Escuela Colombiana de Ingeniería Julio Garavito

Demo Company

IT Security and Privacy

Digital Forensics

Students:

Laura Sofia Gil Chaves

Teacher:

Ing. Daniel Vela

Business Confidential

December 11th , 2024

Project 01-11

Version 1.0

Table

Assessment Overview

From Thursday, December 5 to Tuesday, December 11 the digital forensic analysis of the Dell CPi computer case, found on 09/20/04, focuses on identifying hacking software, evidence of its use and any data generated during its operation. First, the system should be checked for programs or tools associated with traffic interception activities, such as packet sniffers or software to steal sensitive information (credit card numbers, passwords, etc.). In addition, it is crucial to investigate possible fingerprints connecting the computer to the suspect, G=r=e=e=g S=c=h=a=r=d=t (aka "Mr. Evil"), who is known to intercept traffic on public Wi-Fi hotspots. In analyzing the evidence, we will be looking for any data related to intercepted internet traffic and sensitive data such as credit card numbers or login credentials that could link the suspect to the device. The goal is to determine if this equipment was involved in illegal activities and if a direct link to the suspect can be established based on the information recovered during the forensic analysis.

1.Planning: defined the scope and steps required for forensic analysis of the Dell CPi computer. Using Kali Linux, which is a distribution specialized in penetration testing and forensic analysis.

2.Discovery: began with data collection and analysis in search of relevant evidence.

3.Attacking: checked whether the computer was used for illegal activities and how it relates to the suspect.

4.Reporting: Documentation of attack and possible mitigation options.

Plan → Discovery → Attack →Report

Scope

Assessment	Details
External Penetration Test	Hacking Case (nist.gov)

Scope Exclusions

There will be no scope exclusions regarding Digital Forensics as all testing will be conducted in a secure and controlled laboratory environment.

Client Allowances

The permissions required to perform the tests will be provided by the laboratory teacher, which will allow full access to all necessary files and resources.

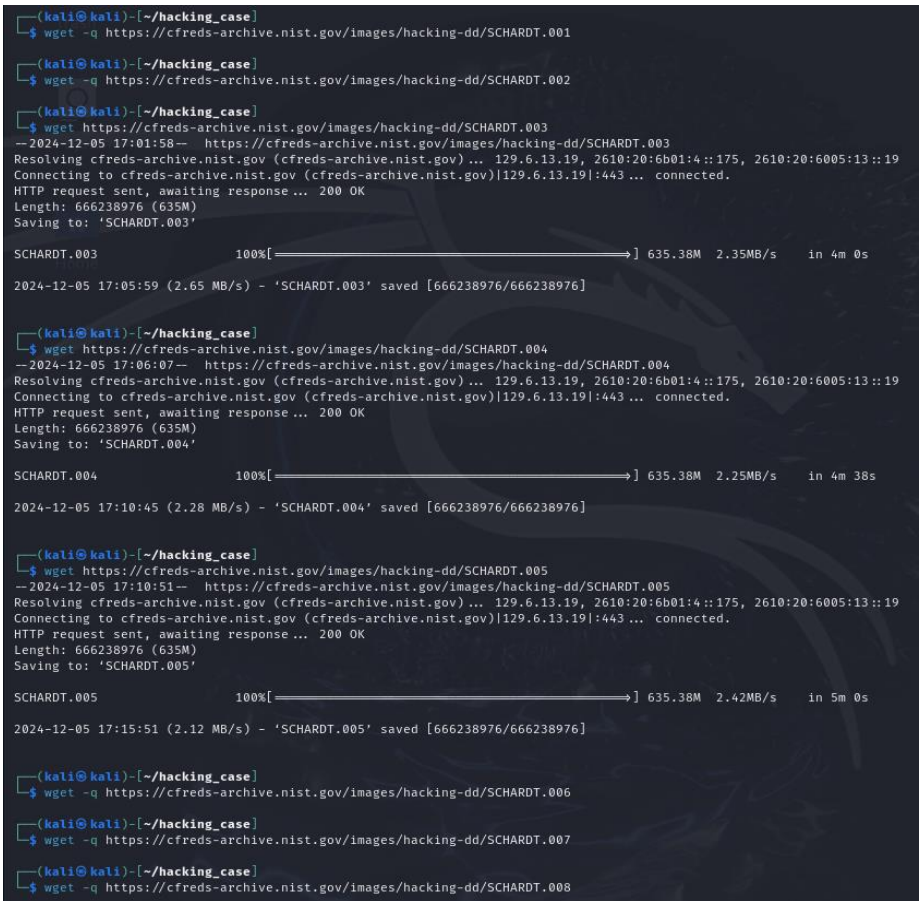
External Penetration Test Findings

External Penetration Test Findings

Description:	forensic analysis of the Dell CPi focuses on identifying hacking software, evidence of traffic interception, and data theft tools. The goal is to link the suspect, Gregg Schardt ("Mr. Evil"), to illegal activities using recovered evidence like intercepted internet traffic or sensitive data.
Impact:	Critical
System:	Windows
References:	Hacking Case (nist.gov)

Exploit proof of contest

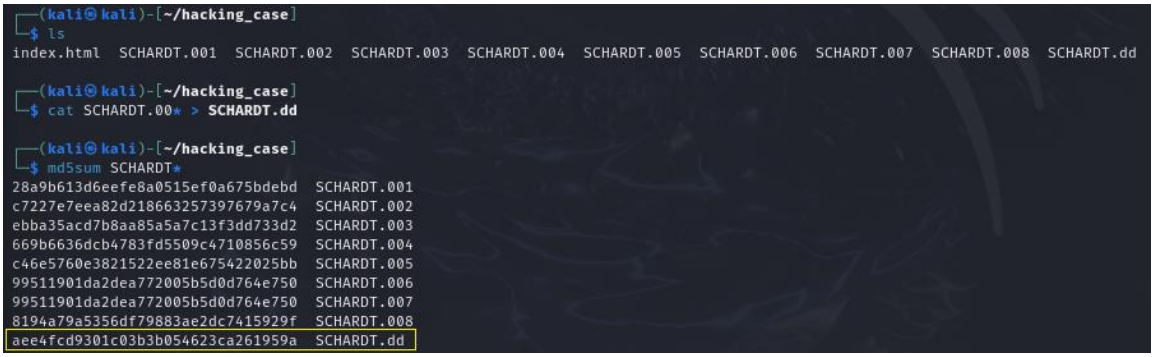
I got the DD images



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

First, I checked if I had the necessary DD images, and then a merge of all of them into a single consolidated DD image was performed. Subsequently, the MD5 checksum was generated and verified to ensure the integrity of the merged data.

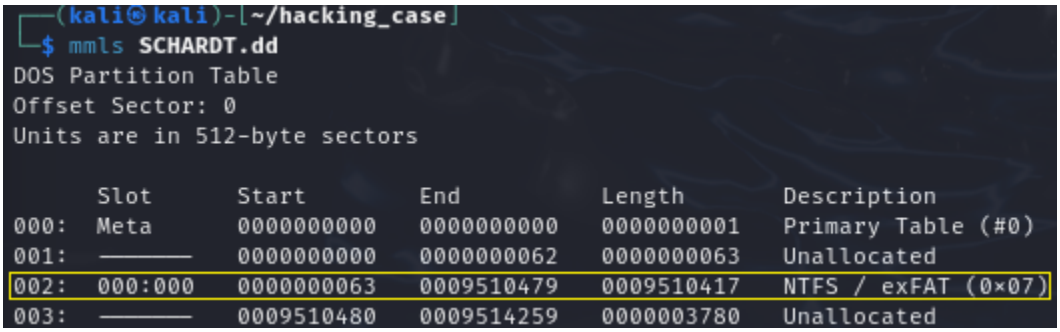
- Image Hash : aee4fcd9301c03b3b054623ca261959a
- the acquisition and verification match correctly.



2. What operating system was used on the computer?

First, I looked at the partitions (NTFS) and unallocated space using mmls command

- mmls: Displays partition layout on a disk image (from The Sleuth Kit).



Extract software, which contains OS information saved in Win registry

fls -rF -o 63 SCHARDT.dd

- fls: Lists the files and directories contained in a forensic image or file system.
- -r: Searches recursively through subdirectories.
- -F: Displays additional details such as file flags.
- -o 63: Indicates that the file system starts at offset 63 (usually used with disk images).
- SCHARDT.dd: Is the forensic image you are analyzing.

Result: Lists all files and directories in the SCHARDT.dd image, searching all subdirectories.

grep -i software

- grep: Filters lines containing the specified text.
- -i: Ignores upper and lower case.
- software: Is the keyword to be searched for.

Result: Filters only the lines containing the word "software" in the output of fls.

icat -o 63 SCHARDT.dd 336 > software

- icat: Extracts a specific file from a forensic image.
- -o 63: Indicates that the file system starts at offset 63.
- SCHARDT.dd: Is the forensic image.
- 336: Is the inode number of the file you want to extract (obtained from the output of fls).
    - ➢ software: Save the extracted file with the name software.

Result: Extracts the file identified with the inode 336 and saves it in the system as software.

- ls software -l

- ls: Lists the files in the current directory.
- -l: Displays extended details such as permissions, size and date.

Result: Displays detailed information about the extracted file named software.

```
┌──(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

┌──(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd > software
Missing image name and/or address
usage: icat [-hrRsvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o imgoffset] image [images] inum[-typ[-id]]
        -h: Do not display holes in sparse files
        -r: Recover deleted file
        -R: Recover deleted file and suppress recovery errors
        -s: Display slack space at end of file
        -i imgtype: The format of the image file (use '-i list' for supported types)
        -b dev_sector_size: The size (in bytes) of the device sectors
        -f fstype: File system type (use '-f list' for supported types)
        -o imgoffset: The offset of the file system in the image (in sectors)
        -P pooltype: Pool container type (use '-P list' for supported types)
        -B pool_volume_block: Starting block (for pool volumes only)
        -S snap_id: Snapshot ID (for APFS only)
        -v: verbose to stderr
        -V: Print version
        -k password: Decryption password for encrypted volumes

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

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls software -l
-rw-r--r-- 1 kali kali 8650752 Dec  8 17:00 software
```

Then, I found regrip plugin and winver mmls

- Regrip plugin: A tool or script (likely for RegRipper) to extract registry information.
- winver: Command to check Windows version.

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -l | grep -i winver

190. winver v.20200525 [Software]

┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/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
```

The operating system used on the computer is Windows XP

3. When was the install date?

The installation date is 08/19/04 22:48:27 PM

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -l | grep -i winver

190. winver v.20200525 [Software]

┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/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
```

4. What is the timezone settings?

First, I search for system, then extract system and then search for the time zone. We use the same commands, except *egrep -i config/system$*, where :

- *egrep:* Is a variant of grep, which allows to use extended regular expressions (that's why the "e" in egrep).
- *i*: Specifies that the search should be case insensitive, i.e., it does not matter if the text is in upper or lower case.
- *config/system$*: This is the pattern you are looking for. The explanation of this pattern is:
- config/system: search for the exact string config/system.
- $: This is a special symbol in regular expressions that means "end of line". This indicates that the string config/system must be at the end of the line.

```
┌──(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 334 > system

┌──(kali㉿kali)-[~/hacking_case]
└─$ cd RegRipper3.0

┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/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)
```

The timezone settings is Central Daylight Time (-05hrs GMT)

5. Who is the registered owner?

The registered owner is Greg Schardt

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -l | grep -i winver

190. winver v.20200525 [Software]

┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/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?

The computer account name is N-1A9ODN6ZXK4LQ

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/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?

I need to do the following:

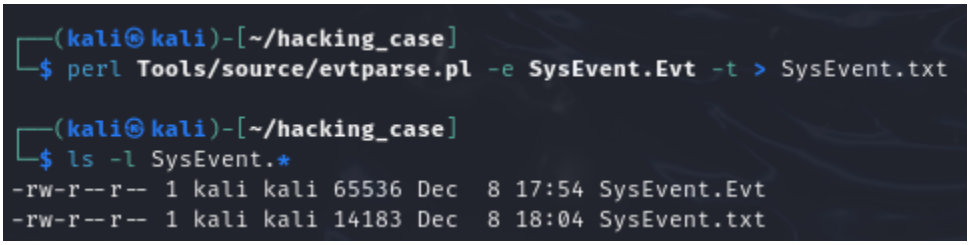
- Search for the workgroup in the system event log and extract the event log: First, the system event log is dumped, then Download evtparse, and then Test evtparse.

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rF -o 63 SCHARDT.dd | egrep -i config/sysevent
r/r 3678-128-1: WINDOWS/system32/config/SysEvent.Evt

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

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls
index.html     SCHARDT.001  SCHARDT.003  SCHARDT.005  SCHARDT.007  SCHARDT.dd  SysEvent.Evt
RegRipper3.0   SCHARDT.002  SCHARDT.004  SCHARDT.006  SCHARDT.008  software    system

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls -l SysEvent.Evt
-rw-r--r-- 1 kali kali 65536 Dec  8 17:54 SysEvent.Evt
```

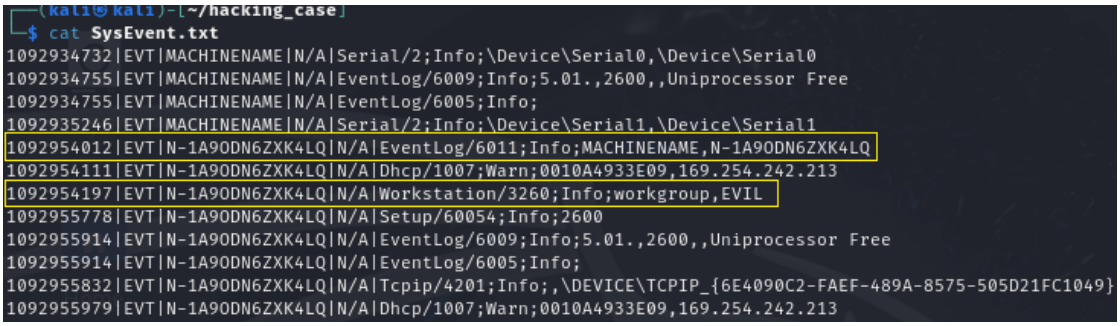
- Find a tool to analyze the event log

```
┌──(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 | 3.81 MiB/s, done.
Resolving deltas: 100% (108/108), done.
Updating files: 100% (67/67), done.

┌──(kali㉿kali)-[~/hacking_case]
└─$ perl Tools/source/evtparse.pl
evtparse [option]
Parse Event log (Win2000, XP, 2003)

  -e file........Event log (full path)
  -d dir.........Directory where .evt files are located
  -s ............Output in sequential format (record number and time
                 generated values ONLY - use to see if system time may
                 have been tampered with)
  -t ............TLN output (default .csv)
  -h ............Help (print this information)

Ex: C:\>evtparse -e secevent.evt -t > timeline.txt
    C:\>evtparse -e sysevent.evt -s

**All times printed as GMT/UTC

copyright 2012 Quantum Analytics Research, LLC
```

The perl command Tools/source/evtparse.pl -e SysEvent.Evt -t > SysEvent.txt runs a Perl script that processes the event file SysEvent.Evt with options -e (specifies the input file) and -t (probably to format the output). It then saves the result to SysEvent.txt.



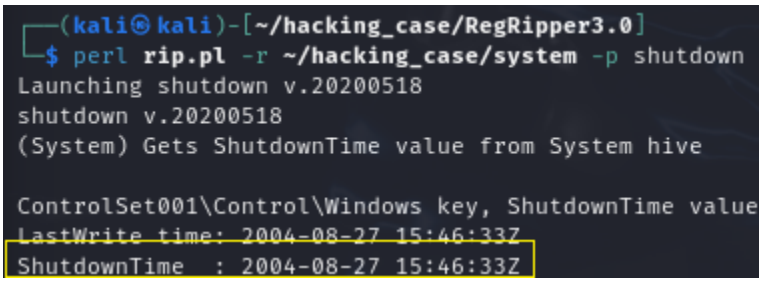
- Find domain information



The primary domain name is Evil

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

The last recorded computer shutdown date/timei s 08/27/04 15:46:33AM



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

All Windows user account names, SIDs (Security Identifiers), login counts, creation dates, last password change dates, groups, and much more can be found in the Windows Registry SAM (Security Account Manager) file.

```
┌──(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/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/SAM -p samparse
Launching samparse v.20220921
samparse v.20220921
(SAM) Parse SAM file for user & group mbrshp info


User Information
--------------------------
Username        : Administrator [500]
SID             : S-1-5-21-2000478354-688789844-1708537768-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Thu Aug 19 16:59:24 2004 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Thu Aug 19 17:17:29 2004 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account

Username        : Guest [501]
SID             : S-1-5-21-2000478354-688789844-1708537768-501
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Thu Aug 19 16:59:24 2004 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password not required
  --> Password does not expire
  --> Normal user account

Username        : HelpAssistant [1000]
SID             : S-1-5-21-2000478354-688789844-1708537768-1000
Full Name       : Remote Desktop Help Assistant Account
User Comment    : Account for Providing Remote Assistance
Account Type    : Custom Limited Acct
Account Created : Thu Aug 19 22:28:24 2004 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Thu Aug 19 22:28:24 2004 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account

Username        : SUPPORT_388945a0 [1002]
SID             : S-1-5-21-2000478354-688789844-1708537768-1002
Full Name       : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
User Comment    : This is a vendor's account for the Help and Support Service
Account Type    : Custom Limited Acct
```

```
Username        : Mr. Evil [1003]
SID             : S-1-5-21-2000478354-688789844-1708537768-1003
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Aug 19 23:03:54 2004 Z
Name            :
Last Login Date : Fri Aug 27 15:08:23 2004 Z
Pwd Reset Date  : Thu Aug 19 23:03:54 2004 Z
Pwd Fail Date   : Never
Login Count     : 15
  ⟶ Password does not expire
  ⟶ Normal user account
```

The total accounts are recorded are 5

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

```
Username        : Mr. Evil [1003]
SID             : S-1-5-21-2000478354-688789844-1708537768-1003
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Aug 19 23:03:54 2004 Z
Name            :
Last Login Date : Fri Aug 27 15:08:23 2004 Z
Pwd Reset Date  : Thu Aug 19 23:03:54 2004 Z
Pwd Fail Date   : Never
Login Count     : 15
  ⟶ Password does not expire
  ⟶ Normal user account
```

The account name of the user who mostly uses the computer is Mr. Evil

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

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/software -p profilelist
Launching profilelist v.20200518
profilelist v.20200518
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList

Path      : %systemroot%\system32\config\systemprofile
SID       : S-1-5-18
LastWrite : 2004-08-19 22:48:26Z

Path      : %SystemDrive%\Documents and Settings\LocalService
SID       : S-1-5-19
LastWrite : 2004-08-27 15:08:21Z

Path      : %SystemDrive%\Documents and Settings\NetworkService
SID       : S-1-5-20
LastWrite : 2004-08-27 15:08:20Z

Path      : %SystemDrive%\Documents and Settings\Mr. Evil
SID       : S-1-5-21-2000478354-688789844-1708537768-1003
LastWrite : 2004-08-27 15:46:23Z

Domain Accounts
```

The last user to logon to the computer is 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?

Approach

- Search "Greg" and check if the name associated with "Evil"
- To search, I need to mount the DD image

First, create a mounting point, then I set up a loop device. With this I can mount dd to the mounting point .

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

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

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls -l loop0*
ls: cannot access 'loop0*': No such file or directory

┌──(kali㉿kali)-[~/hacking_case]
└─$ ls -l /dev/loop0*
brw-rw---- 1 root disk   7, 0 Dec  8 18:49 /dev/loop0
brw-rw---- 1 root disk 259, 0 Dec  8 18:49 /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   COMMAND.COM             hiberfil.sys   NETLOG.TXT      RECYCLER                Temp
 boot.ini       CONFIG.SYS              IO.SYS         ntdetect.com    SETUPLOG.TXT            VIDEOROM.BIN
 BOOTLOG.PRV    DETLOG.TXT              MSDOS.---      ntldr           SUHDLOG.DAT             WIN98
 BOOTLOG.TXT   'Documents and Settings'  MSDOS.SYS     pagefile.sys    SYSTEM.1ST              WINDOWS
 BOOTSECT.DOS   FRUNLOG.TXT             'My Documents' 'Program Files' 'System Volume Information'
```

Now, I search globally for the string “Grep Schardt”

```
┌──(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
```

Observation:

- look@lan is a software because it was installed under the “Program Files” folder
- look@lan has a configuration file named “irunin.ini”
- The initial config file has owner and user name information.
- The config file has a setup log

With this, I can search for the string “evil”

```
┌──(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/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]
└─$ strings '/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/History/History.IE5/index.dat' | grep -i greg

Visited: Mr. Evil@http://edit.yahoo.com/config/id_check?.fn=Greg&.ln=Schardt&.id=mrevil2000&.u=b568cfp0ic6g0

┌──(kali㉿kali)-[~/hacking_case]
└─$ strings '/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/History/History.IE5/MSHist012004081620040823/index.dat' | grep
 -i 'greg'

:2004081620040823: Mr. Evil@http://edit.yahoo.com/config/id_check?.fn=Greg&.ln=Schardt&.id=mrevil2000&.u=b568cfp0ic6g0
```

13. List the network cards used by this computer

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/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
```

Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface) and Compaq WL110 Wireless LAN PC Card are the network cards used by this computer

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

I need to:

- list all files contain IP address and list all files contain MAC address

```
┌──(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/loop/' > 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
```

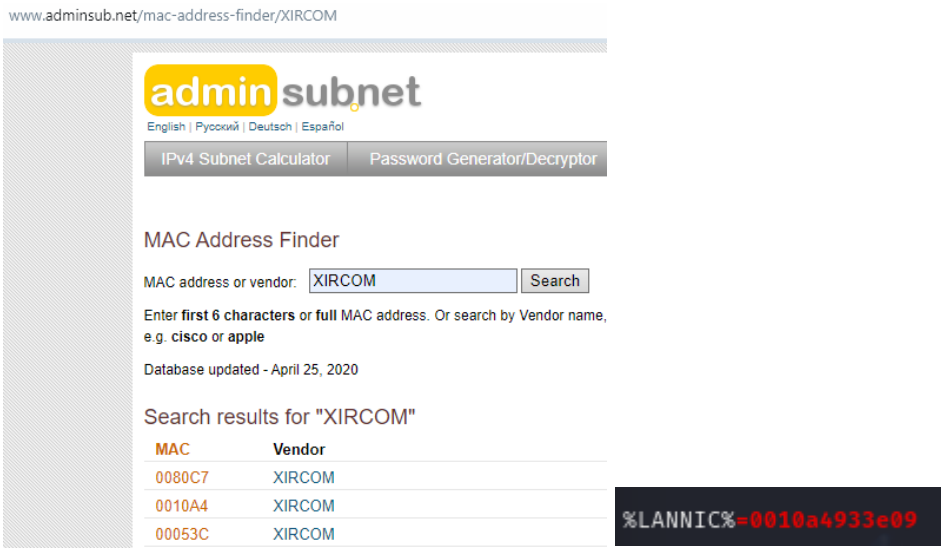
- Find intersection of two files

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

%LANNIC%=0010a4933e09
```

- the IP address: 192.168.1.111
- MAC address : 0010a4933e09

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?



The NIC card was used during the installation and set-up for LOOK@LAN is Xircom

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

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/software -p uninstall
Launching uninstall v.20200525
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

2004-08-27 15:29:19Z
  Ethereal 0.10.6 v.0.10.6

2004-08-27 15:15:19Z
  WinPcap 3.01 alpha

2004-08-27 15:12:15Z
  Network Stumbler 0.4.0 (remove only)

2004-08-25 15:56:11Z
  Look@LAN 2.50 Build 29

2004-08-20 15:13:08Z
  123 Write All Stored Passwords
```

```
2004-08-20 15:09:02Z
  CuteFTP

2004-08-20 15:08:19Z
  Forté Agent

2004-08-20 15:07:25Z
  Faber Toys v.2.4 Build 216

2004-08-20 15:05:58Z
  Cain & Abel v2.5 beta45

2004-08-20 15:05:09Z
  Anonymizer Bar 2.0 (remove only)

2004-08-19 23:04:50Z
  WebFldrs XP v.9.50.5318

2004-08-19 23:04:36Z
  Microsoft NetShow Player 2.0
  MPlayer2
```

The 6 installed programs that may be used for hacking were :

- Cain & Abel v2.5 beta45 (password sniffer & cracker)
- Ethereal (packet sniffer)
- 123 Write All Stored Passwords (finds passwords in registry)
- Anonymizer (hides IP tracks when browsing)
- CuteFTP (FTP software) Look&LAN_1.0 (network discovery tool)
- NetStumbler (wireless access point discovery tool)

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

First, I search for ntuser.data that Contains User Profile Settings, then I extract evil ntuser.data and for the last I search the email pattern.

```
┌──(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

┌──(kali㉿kali)-[~/hacking_case]
└─$ icat -o 63 SCHARDT.dd 345 > NTUSER_Evil.DAT
```

```
┌──(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
```

The SMTP email address for Mr. Evil is whoknowsme@sbcglobal.net

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

To do this, I needed to:

- Find new applications installed

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/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
```

- Find the application installation directory where I searched for installed Forte Agent.

```
┌──(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
```

- Search for configuration files or key words where first I looked for Forte Agent configuration files or data.

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

Now, I found news server configuration

```
┌──(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
```

The NNTP (news server) settings for Mr. Evil is News.dallas.sbcglobal.net

```
┌──(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/{EF086998-1115-4ECD-9B13-9ADC067B
4929}/Microsoft/Outlook Express/cleanup.log
r/r 11443-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B
4929}/Microsoft/Outlook Express/alt.2600.cardz.dbx
r/r 11444-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B
4929}/Microsoft/Outlook Express/alt.2600.codez.dbx
r/r 11445-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B
4929}/Microsoft/Outlook Express/alt.2600.crackz.dbx
r/r 11442-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B
4929}/Microsoft/Outlook Express/alt.2600.dbx
r/r 11539-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B
4929}/Microsoft/Outlook Express/alt.2600.hackerz.dbx
r/r 11446-128-4:        Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B
4929}/Microsoft/Outlook Express/alt.2600.moderated.dbx
```

Find the news server:news.dallas.sbcglobal.net in the .dbx (outlook express format).

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ strings "/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4
929}/Microsoft/Outlook Express/alt.2600.cardz.dbx" | grep -i "news.dallas.sbcglobal.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?

```
┌──(kali㉿kali)-[~/hacking_case/RegRipper3.0]
└─$ perl rip.pl -r ~/hacking_case/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
```

- Outlook Express
- Forte Agent

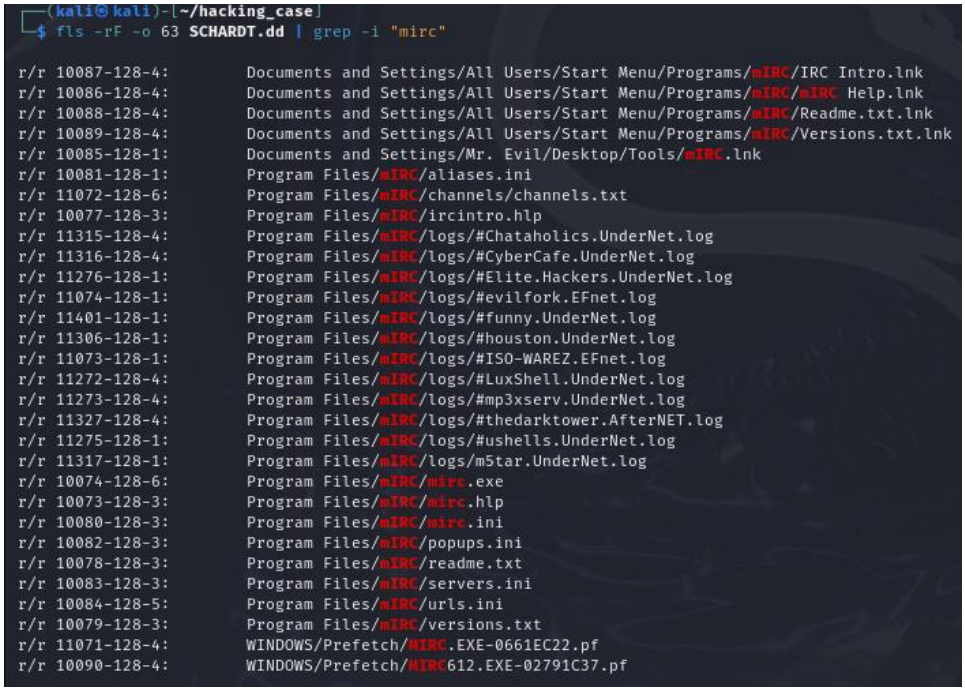
20. List 5 newsgroups that Mr. Evil has subscribed to?

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ ls  "/mnt/loop/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}
/Microsoft/Outlook Express"
 alt.2600.cardz.dbx                  alt.binaries.hacking.utilities.dbx    free.binaries.hacking.beginner.dbx
 alt.2600.codez.dbx                  alt.binaries.hacking.websites.dbx     free.binaries.hacking.computers.dbx
 alt.2600.crackz.dbx                 alt.dss.hack.dbx                      free.binaries.hacking.talentless.troll-haven.dbx
 alt.2600.dbx                        alt.hacking.dbx                       free.binaries.hacking.talentless.troll_haven.dbx
 alt.2600.hackerz.dbx                alt.nl.binaries.hack.dbx              free.binaries.hacking.utilities.dbx
 alt.2600.moderated.dbx              alt.stupidity.hackers.malicious.dbx   free.binaries.hacking.websites.dbx
 alt.2600.phreakz.dbx                cleanup.log                           Inbox.dbx
 alt.2600.programz.dbx              'Deleted Items.dbx'                    Offline.dbx
 alt.binaries.hacking.beginner.dbx   Folders.dbx                          Outbox.dbx
 alt.binaries.hacking.computers.dbx  free.binaries.hackers.malicious.dbx
```

- Alt.2600.phreakz
- Alt.2600
- Alt.2600.cardz
- Alt.2600codez
- Alt.2600.crackz
- Alt.2600.moderated
- Alt.binaries.hacking.utilities
- Alt.stupidity.hackers.malicious
- Free.binaries.hackers.malicious
- Free.binaries.hacking.talentless.troll_haven
- Free.binaries.hacking.talentless.troll-haven
- alt.nl.binaries.hack
- free.binaries.hacking.beginner
- free.binaries.hacking.computers
- free.binaries.hacking.utilities
- free.binaries.hacking.websites
- alt.binaries.hacking.computers
- alt.binaries.hacking.websites
- alt.dss.hack
- alt.binaries.hacking.beginner
- alt.hacking
- alt.2600.programz
- alt.2600.hackerz

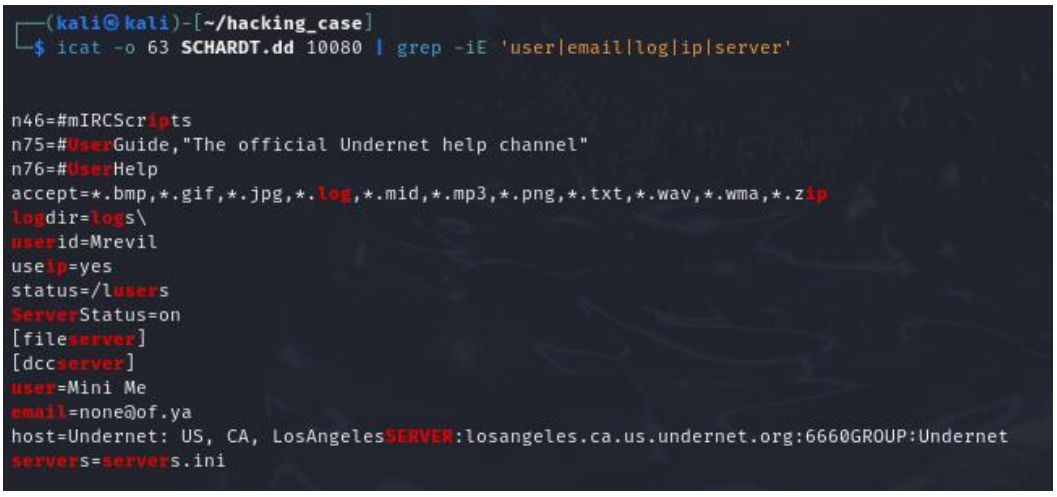
21. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?

Find new applications installed where I found MIRC installed directory



```
┌──(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.lnk
r/r 10086-128-4:        Documents and Settings/All Users/Start Menu/Programs/mIRC/mIRC Help.lnk
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.txt.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
```

Then, I needed to find some important 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
```

The user settings that were shown when the user was online and in a chat channel are:

- user=Mini Me
- email=none@of.ya
- nick=Mr

- anick=mrevilrulez

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

The IRC channels that the user of this computer accessed:

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

- Find the location \Document and Setting\Mr. Evil and then I Searched for TCP packets saved (.pcap)

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

'Application Data'   Desktop     interception       'My Documents'   NTUSER.DAT       ntuser.ini   Recent   'Start Menu'
 Cookies             Favorites  'Local Settings'    NetHood          ntuser.dat.LOG   PrintHood    SendTo    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 (little-endian) - version 2.4 (Ethernet, c
apture length 65535)
```

The name of the file that contains the intercepted data is Interception.

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?

The command that I used is:

- *tshark*: A command line tool for capturing and analyzing network packets (equivalent to Wireshark).
- *-r /mnt/loop/Documents and Settings/Mr.Evil/interception*: Reads a packet capture file (interception), located in the specified path.
- -*Y http.request:* Filters packets to show only those that are HTTP requests.
- *-T fields*: Displays only the fields specified in the output.
- *-e http.user_agent*: Extracts and displays the User-Agent field from HTTP requests, which contains information about the browser or client that made the request.
- *-e http.host*: Extracts and displays the Host field for HTTP requests, which indicates the server to which the request was made.

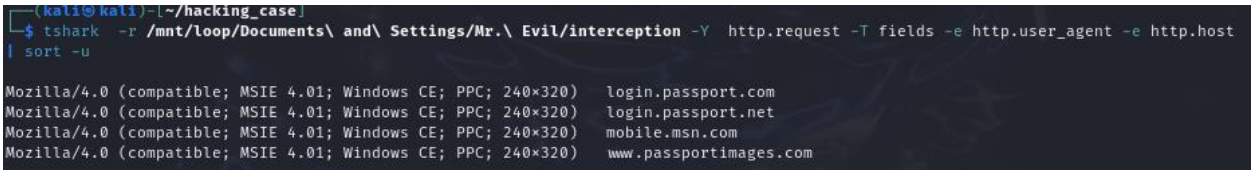
```
┌──(kali㉿kali)-[~/hacking_case]
└─$ tshark  -r /mnt/loop/Documents\ and\ Settings/Mr.\ Evil/interception -Y  http.request -T fields -e http.user_agent -e http.host

Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   www.passportimages.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   login.passport.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   login.passport.net
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   www.passportimages.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   www.passportimages.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   www.passportimages.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   www.passportimages.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240×320)   mobile.msn.com
```

The type of wireless computer was the victim using is Windows CE (Pocket PC)

25. What websites was the victim accessing?

The command that I used is:

- *tshark:* Command line tool for capturing and analyzing network traffic (similar to Wireshark).
- *-r /mnt/loop/Documents and Settings/Mr.\ Evil/interception:* Specifies the traffic capture file to be analyzed (interception), located in the specified path. Backslashes (backslashes) are necessary to escape spaces in file or folder names.
- *Y http.request*: Filter the packets to show only those containing HTTP requests.
- *T fields:* Configures the output to display only the specified fields.
- *-e http.user_agent*: Extracts the User-Agent field from HTTP requests, which describes the client or browser that made the request.
- *-e http.host*: Extracts the Host field, which indicates the server or domain to which the request was made.
- |: Passes the output of the tshark command to the next command in the pipeline.
- *sort -u:*
  sort: Sorts the lines alphabetically. *-u:* Removes duplicate lines, displaying only unique ones.



The websites where the victim access is :

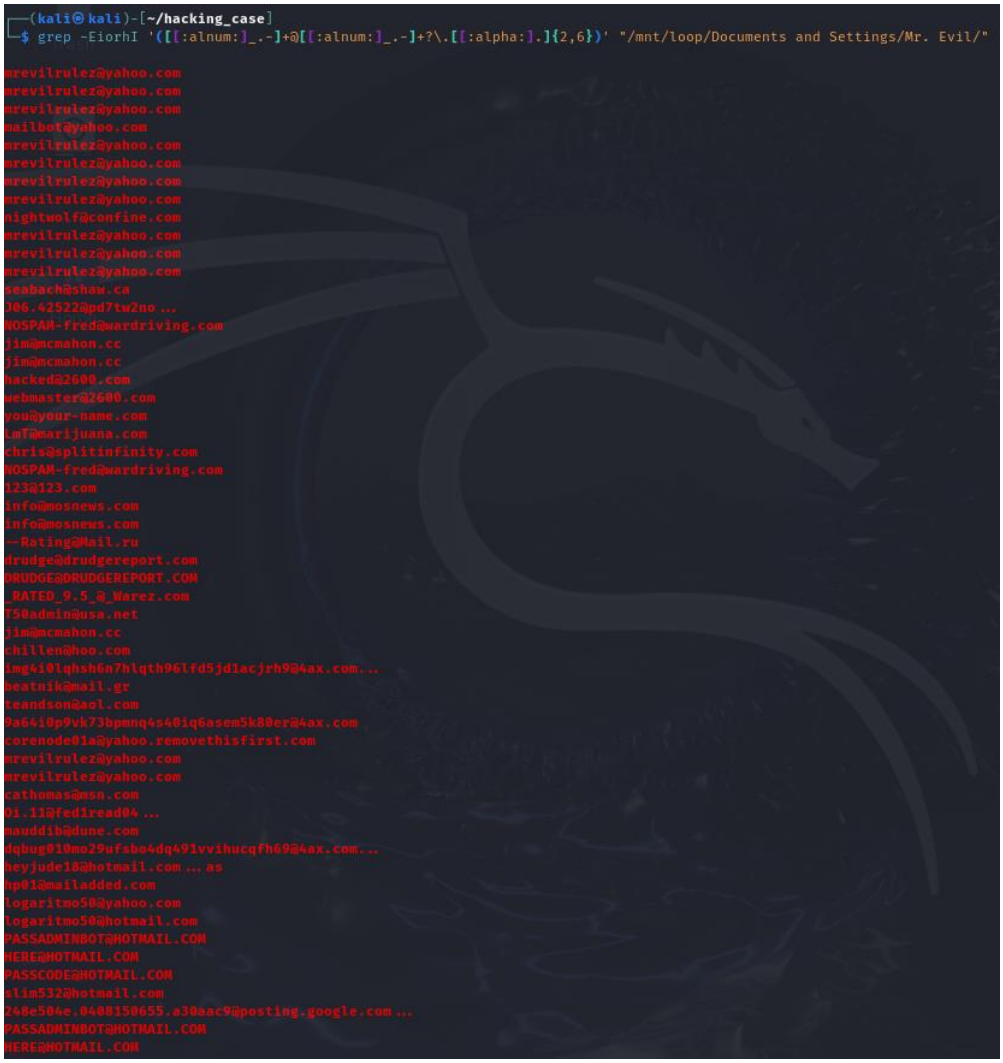
- Mobile.msn.com
- MSN (Hotmail) Email
- Login.passport.com
- Login.passport.net

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

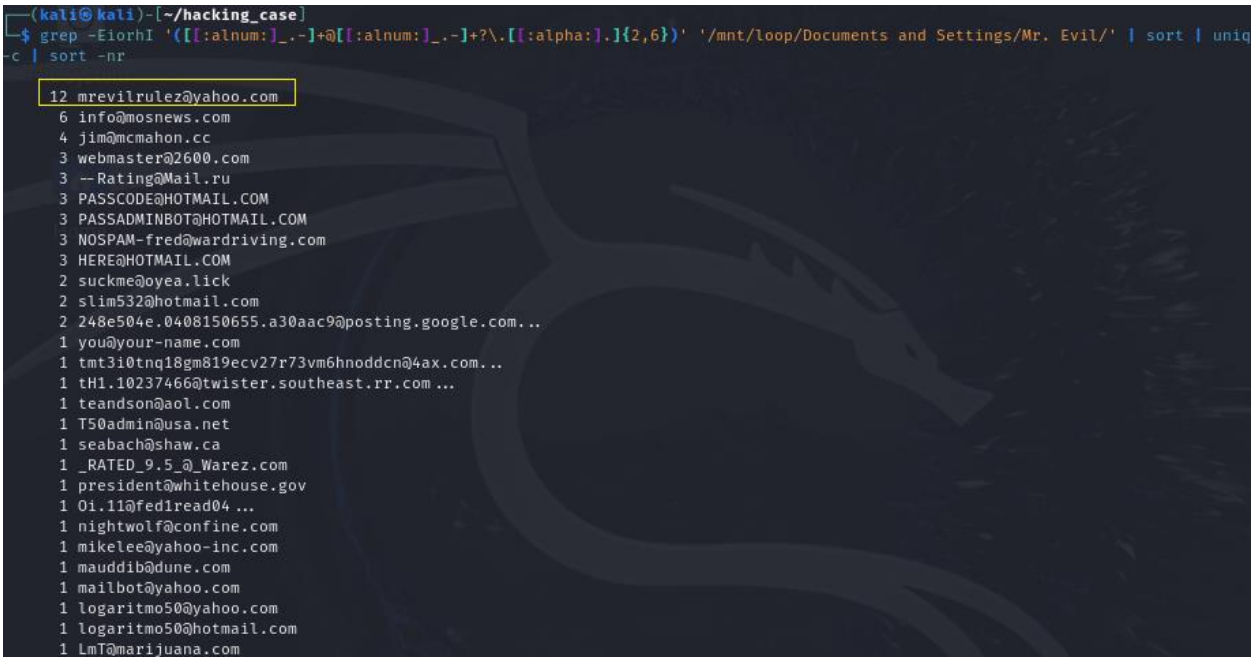
The command that I used is:

- *grep:* It is a command to search for text in files.
- *-E:* Allows the use of extended regular expressions (more advanced than the basic ones).
- *-i*: Makes the search case insensitive.

- *-o*: Displays only the text that matches the pattern, instead of the whole line.
- *-r:* Recursively searches all files and subdirectories within the specified folder.
- *-h*: Avoid displaying file names in the results.
- *-I:* Ignores binary files (only processes text files).
- *'([[:alnum:]_.-]+@[[:alnum:]_.-]+?\.[[:alpha:].]{2,6})':* This is the regular expression that defines the format of email addresses:
- *[[:alnum:]_.-]+:* Searches for alphanumeric characters (letters and numbers), periods (.), underscores (_) and hyphens (-) before the @ symbol.
- *@*: Matches the @ symbol.
- *[[:alnum:]_.-]+?:* Searches for similar characters after the @ (domain name).
- *\alpha:]{2,6}:* Searches for a dot (.) followed by between 2 and 6 letters or dots, such as .com, .org, or .co.uk.
- */mnt/loop/Documents and Settings/Mr. Evil/':* Specifies the directory in which to search for emails.



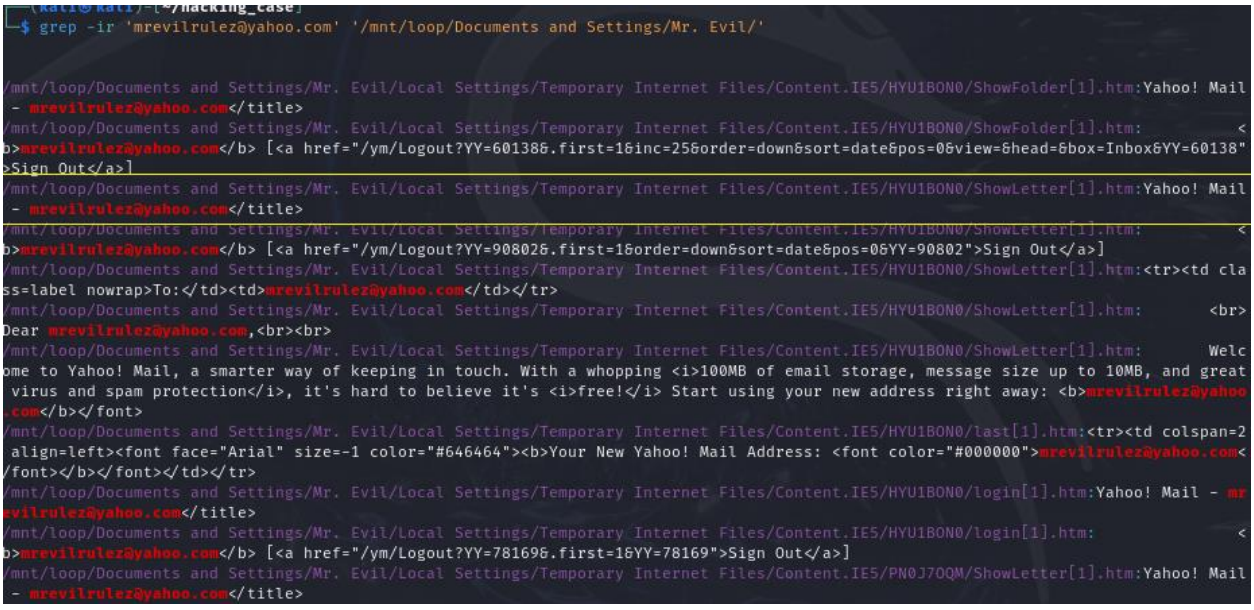
Sort all emails, count them, and sort again based on counts



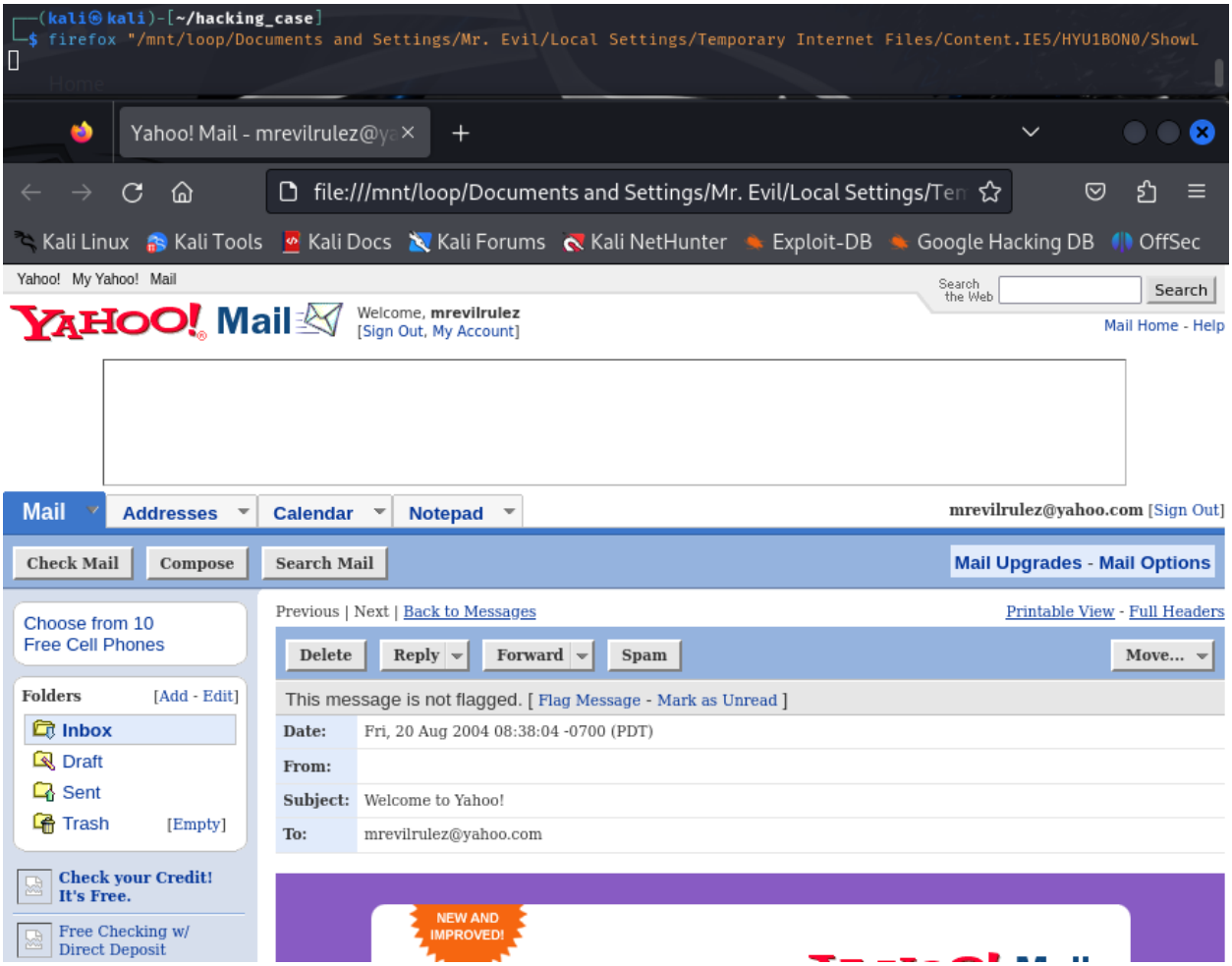
The email address is mrevilrulez@yahoo.com

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

I searched for email under Mr. Evil's account

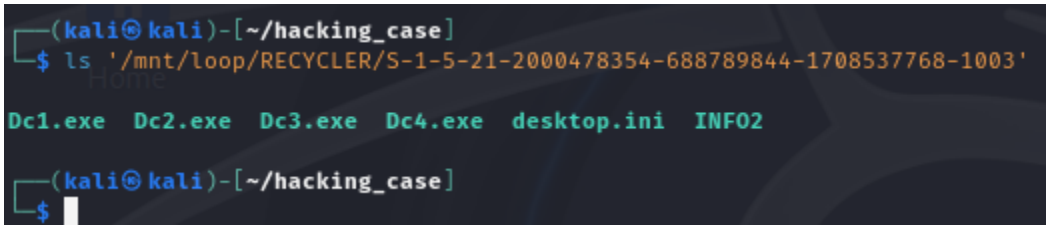


View cached webpages



The file name is Showletter[1].htm

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



The executable files are 4

29. Are these files really deleted?

No. They can be restored with this command:

- *rifiuti2:* It is a tool designed to analyze files in the Recycle Bin of Windows systems. It extracts information about deleted files found in the Recycle Bin.

- *'/mnt/loop/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003/INFO2':* This is the path to a specific file called INFO2. This file is used in older versions of Windows (such as Windows XP) to record metadata about deleted files, such as:
    - Original file name.
    - Full path before deletion.
    - Date of deletion.
    - Size of the file.
- *Command process:*
    - Parses the INFO2 file.
    - Extracts the information mentioned above.
    - It presents a report on the standard output (usually on the terminal).

```
┌──(kali㉿kali)-[~]
└─$ 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?

```
┌──(kali㉿kali)-[~/hacking_case]
└─$ fls -rFd -o 63 SCHARDT.dd | wc -l
365
```

Actually, it reported to be deleted is 365

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

Yes, there any viruses on the computer using this command:

- *clamscan:* This is the main ClamAV command for performing antivirus scans on files and directories.
- *-r (recursive):* Performs a recursive scan, i.e. scans all files and subdirectories within the specified path.
- *-i (infected):* Only shows in the output the files that are infected or suspicious. Clean files will not be listed, which makes the output more concise.

- *"/mnt/loop/":* This is the path to the directory to be scanned. In this case, it appears to be a directory mounted on /mnt/loop/, possibly associated with a forensic image or other drive.