Hacking Case: FSCS 620

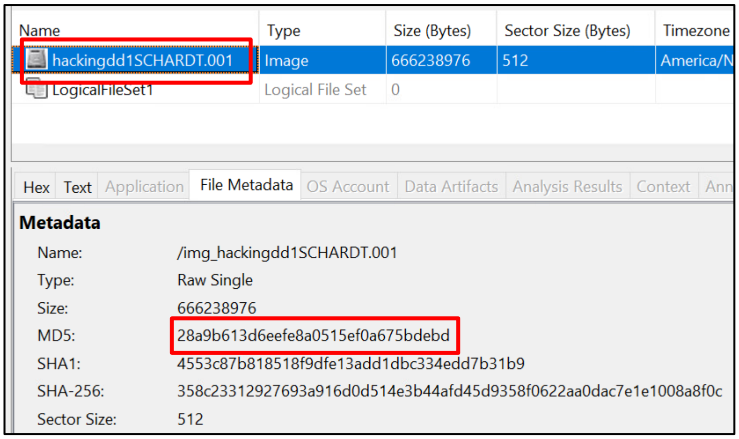
1. What is the image hash? Does the acquisition and verification hash match?

Answer:

Hash: 28a9b613d6eefe8a0515ef0a675bdebd

File: img_hackingdd1SCHARDT.001

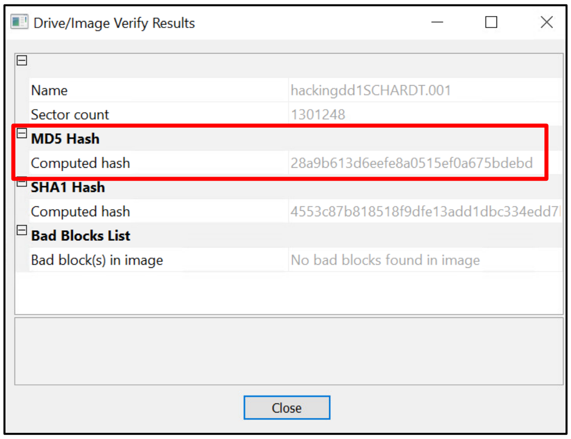
Location: / img_hackingdd1SCHARDT.001 (Metadata)



Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone
hackingdd1SCHARDT.001	Image	666238976	512	America/N
LogicalFileSet1	Logical File Set	0		

Metadata

Name:	/img_hackingdd1SCHARDT.001
Type:	Raw Single
Size:	666238976
MD5:	28a9b613d6eefe8a0515ef0a675bdebd
SHA1:	4553c87b818518f9dfe13add1dbc334edd7b31b9
SHA-256:	358c23312927693a916d0d514e3b44afd45d9358f0622aa0dac7e1e1008a8f0c
Sector Size:	512



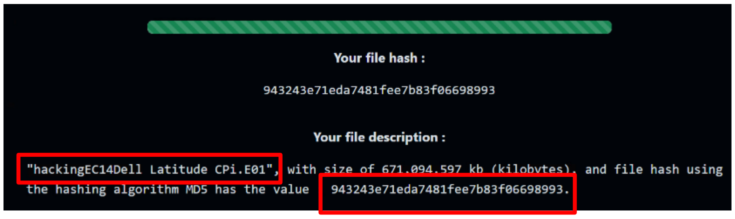
Drive/Image Verify Results

Name	hackingdd1SCHARDT.001
Sector count	1301248
MD5 Hash	
Computed hash	28a9b613d6eefe8a0515ef0a675bdebd
SHA1 Hash	
Computed hash	4553c87b818518f9dfe13add1dbc334edd7
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Hash: 943243e71eda7481fee7b83f06698993

File: hackingEC14Dell Latitude CPi.E01

Location: /hackingEC14Dell Latitude CPi.E01 (Metadata)

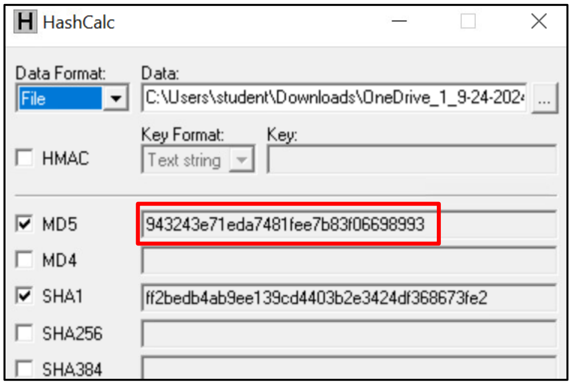


Your file hash :

943243e71eda7481fee7b83f06698993

Your file description :

"hackingEC14Dell Latitude CPi.E01", with size of 671.094.597 kb (kilobytes), and file hash using the hashing algorithm MD5 has the value 943243e71eda7481fee7b83f06698993.



HashCalc

Data Format: File

Data: C:\Users\student\Downloads\OneDrive_1_9-24-202

☐ HMAC

Key Format: Text string

Key:

☑ MD5 943243e71eda7481fee7b83f06698993

☐ MD4

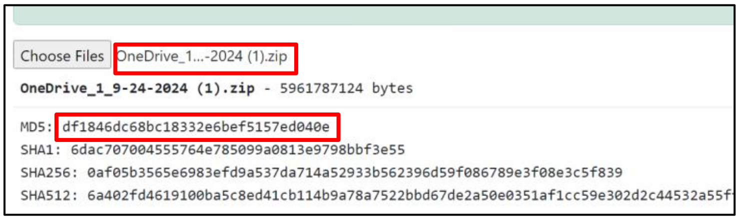
☑ SHA1 ff2bedb4ab9ee139cd4403b2e3424df368673fe2

☐ SHA256

☐ SHA384

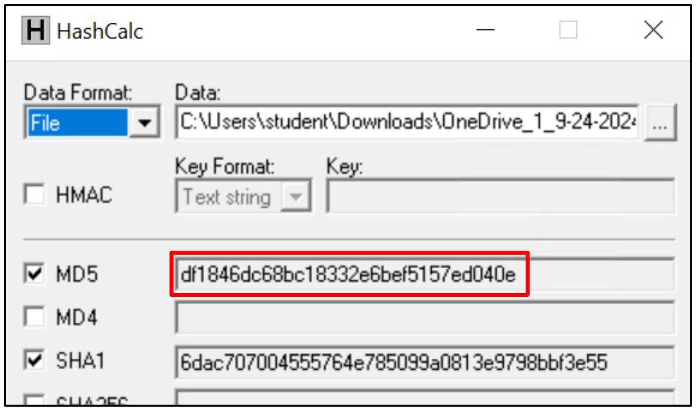
Hash: df1846dc68bc18332e6bef5157ed040e

File: OneDrive_1_9-24-2024 (1).zip



Choose Files OneDrive_1...-2024 (1).zip

```
OneDrive_1_9-24-2024 (1).zip - 5961787124 bytes

MD5: df1846dc68bc18332e6bef5157ed040e
SHA1: 6dac707004555764e785099a0813e9798bbf3e55
SHA256: 0af05b3565e6983efd9a537da714a52933b562396d59f086789e3f08e3c5f839
SHA512: 6a402fd4619100ba5c8ed41cb114b9a78a7522bbd67de2a50e0351af1cc59e302d2c44532a55f
```



HashCalc

Data Format: File

Data: C:\Users\student\Downloads\OneDrive_1_9-24-202

☐ HMAC

Key Format: Text string

Key:

☑ MD5 df1846dc68bc18332e6bef5157ed040e

☐ MD4

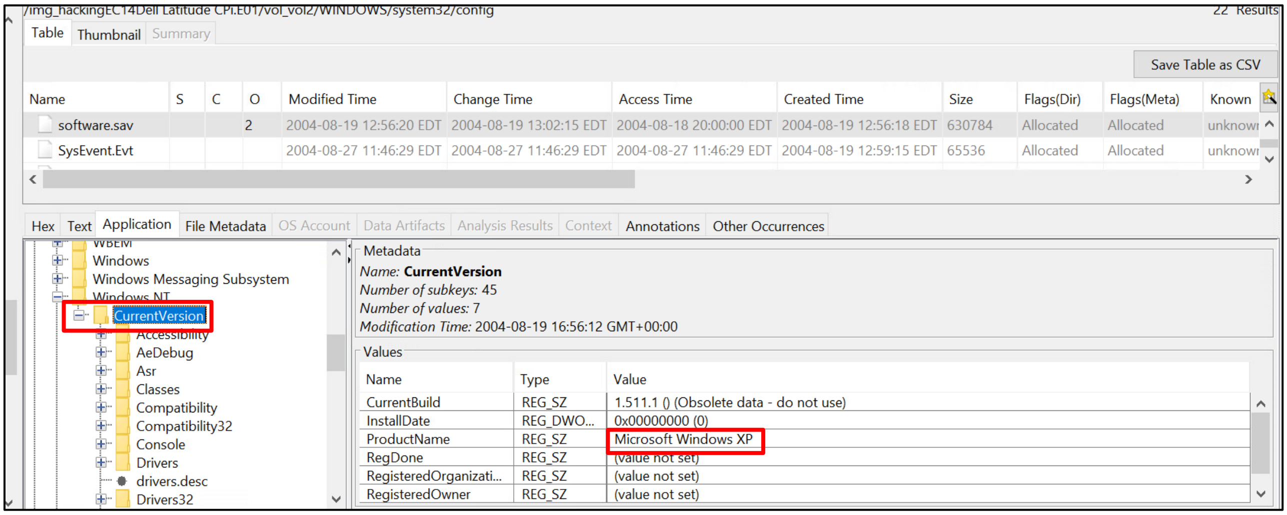
☑ SHA1 6dac707004555764e785099a0813e9798bbf3e55

2. What operating system was used on the computer?

Answer: Windows XP Professional

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/software.sav/Microsoft/WindowsNT/CurrentVersion

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config — 22 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
software.sav			2	2004-08-19 12:56:20 EDT	2004-08-19 13:02:15 EDT	2004-08-18 20:00:00 EDT	2004-08-19 12:56:18 EDT	630784	Allocated	Allocated	unknown
SysEvent.Evt				2004-08-27 11:46:29 EDT	2004-08-27 11:46:29 EDT	2004-08-27 11:46:29 EDT	2004-08-19 12:59:15 EDT	65536	Allocated	Allocated	unknown

Metadata

Name: **CurrentVersion**
Number of subkeys: 45
Number of values: 7
Modification Time: 2004-08-19 16:56:12 GMT+00:00

Values

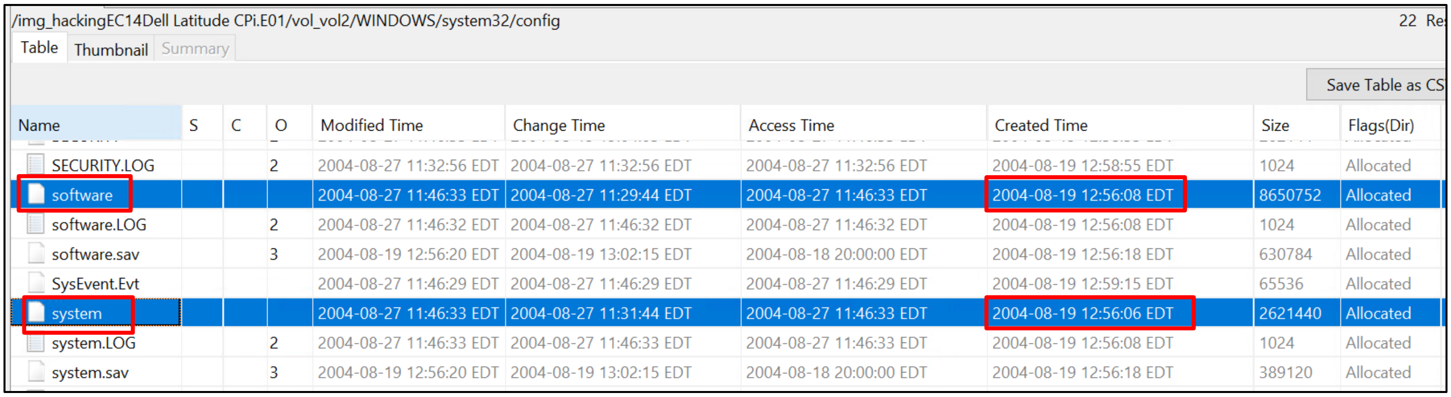
Name	Type	Value
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWO...	0x00000000 (0)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganizati...	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	(value not set)

3. When was the install date?

Answer: 19 August 2004

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config — 22 Re

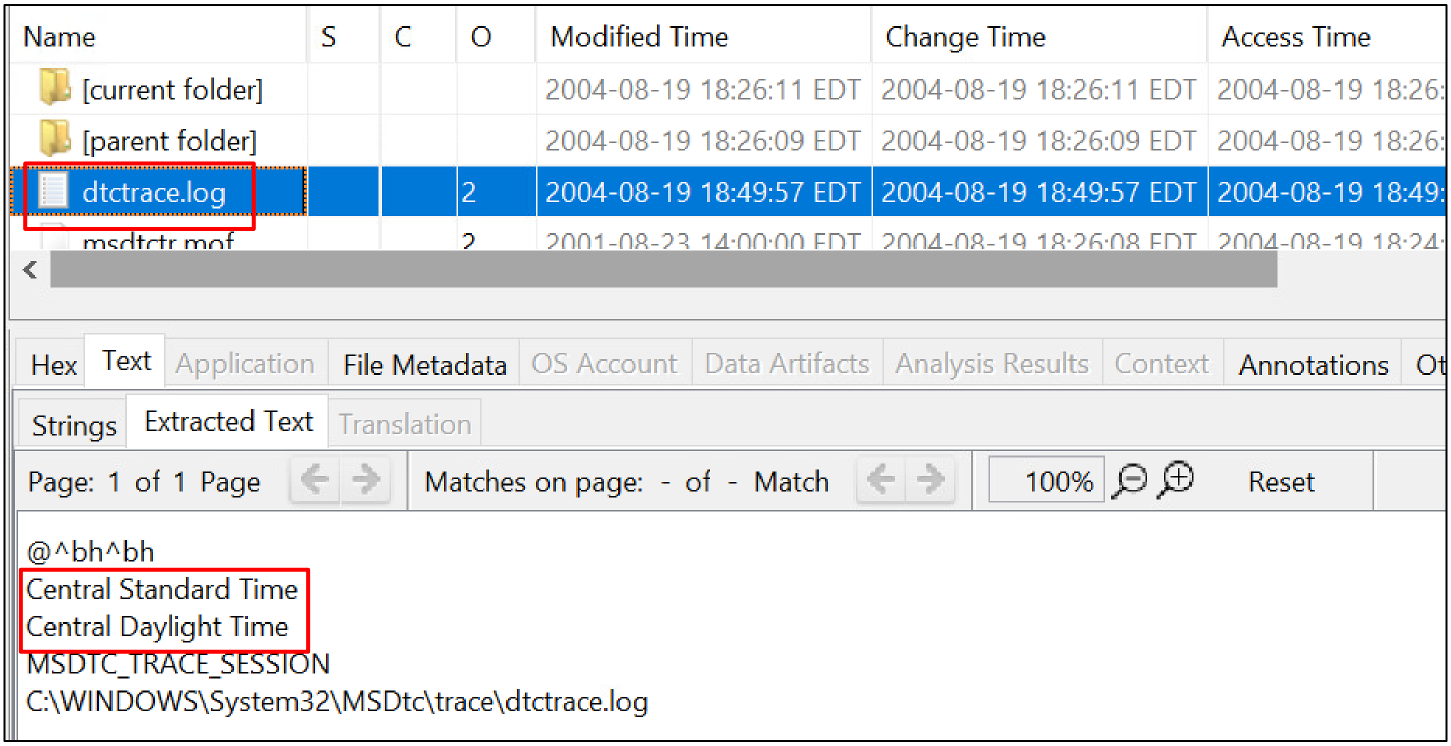
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
SECURITY.LOG			2	2004-08-27 11:32:56 EDT	2004-08-27 11:32:56 EDT	2004-08-27 11:32:56 EDT	2004-08-19 12:58:55 EDT	1024	Allocated
software				2004-08-27 11:46:33 EDT	2004-08-27 11:29:44 EDT	2004-08-27 11:46:33 EDT	2004-08-19 12:56:08 EDT	8650752	Allocated
software.LOG			2	2004-08-27 11:46:32 EDT	2004-08-27 11:46:32 EDT	2004-08-27 11:46:32 EDT	2004-08-19 12:56:08 EDT	1024	Allocated
software.sav			3	2004-08-19 12:56:20 EDT	2004-08-19 13:02:15 EDT	2004-08-18 20:00:00 EDT	2004-08-19 12:56:18 EDT	630784	Allocated
SysEvent.Evt				2004-08-27 11:46:29 EDT	2004-08-27 11:46:29 EDT	2004-08-27 11:46:29 EDT	2004-08-19 12:59:15 EDT	65536	Allocated
system				2004-08-27 11:46:33 EDT	2004-08-27 11:31:44 EDT	2004-08-27 11:46:33 EDT	2004-08-19 12:56:06 EDT	2621440	Allocated
system.LOG			2	2004-08-27 11:46:33 EDT	2004-08-27 11:46:33 EDT	2004-08-27 11:46:33 EDT	2004-08-19 12:56:08 EDT	1024	Allocated
system.sav			3	2004-08-19 12:56:20 EDT	2004-08-19 13:02:15 EDT	2004-08-18 20:00:00 EDT	2004-08-19 12:56:18 EDT	389120	Allocated

4. What is the timezone settings?

Answer: Central Daylight Time

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/MsDtc/Trace/dtctrace.log

Evidence:



Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2004-08-19 18:26:11 EDT	2004-08-19 18:26:11 EDT	2004-08-19 18:26:
[parent folder]				2004-08-19 18:26:09 EDT	2004-08-19 18:26:09 EDT	2004-08-19 18:26:
dtctrace.log			2	2004-08-19 18:49:57 EDT	2004-08-19 18:49:57 EDT	2004-08-19 18:49:
msdtctr.mof			2	2001-08-23 14:00:00 EDT	2004-08-19 18:26:08 EDT	2004-08-19 18:24:

```
@^bh^bh
Central Standard Time
Central Daylight Time
MSDTC_TRACE_SESSION
C:\WINDOWS\System32\MSDtc\trace\dtctrace.log
```

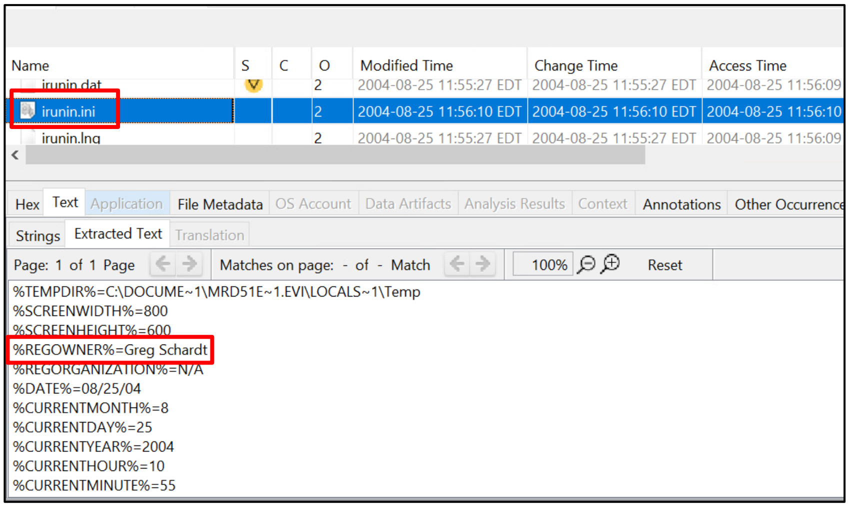
The **dtctrace.log** is a log file generated by the **Microsoft Distributed Transaction Coordinator (MSDTC)** service in Windows operating systems, including Windows XP. The MSDTC service is responsible for coordinating transactions that span multiple resource managers, such as databases, message queues, and file systems. It ensures that distributed transactions are completed either entirely (commit) or not at all (rollback), maintaining consistency across systems.

5. Who is the registered owner?

Answer: Greg Schardt

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini

Evidence:



Name	S	C	O	Modified Time	Change Time	Access Time
irunin.dat	V		2	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-08-25 11:56:09
irunin.ini			2	2004-08-25 11:56:10 EDT	2004-08-25 11:56:10 EDT	2004-08-25 11:56:10
irunin.lng			2	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-08-25 11:56:09

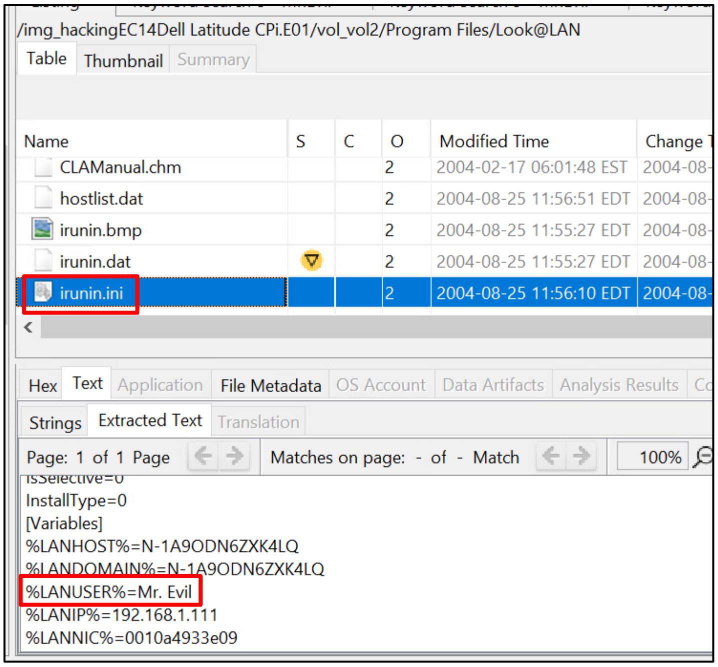
```
%TEMPDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%SCREENWIDTH%=800
%SCREENHEIGHT%=600
%REGOWNER%=Greg Schardt
%REGORGANIZATION%=N/A
%DATE%=08/25/04
%CURRENTMONTH%=8
%CURRENTDAY%=25
%CURRENTYEAR%=2004
%CURRENTHOUR%=10
%CURRENTMINUTE%=55
```

6. What is the computer account name?

Answer: Mr. Evil also N-1A9ODN6ZXK4LQ can be computer name

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN

Name	S	C	O	Modified Time	Change T
CLAManual.chm			2	2004-02-17 06:01:48 EST	2004-08-
hostlist.dat			2	2004-08-25 11:56:51 EDT	2004-08-
irunin.bmp			2	2004-08-25 11:55:27 EDT	2004-08-
irunin.dat	▽		2	2004-08-25 11:55:27 EDT	2004-08-
irunin.ini			2	2004-08-25 11:56:10 EDT	2004-08-

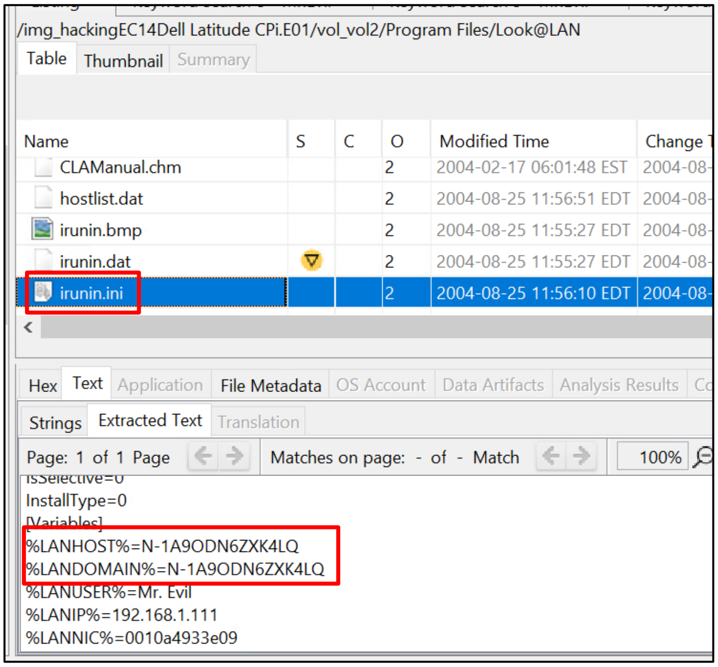
```
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
```

7. What is the primary domain name?

Answer: N-1A9ODN6ZXK4LQ

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN

Name	S	C	O	Modified Time	Change T
CLAManual.chm			2	2004-02-17 06:01:48 EST	2004-08-
hostlist.dat			2	2004-08-25 11:56:51 EDT	2004-08-
irunin.bmp			2	2004-08-25 11:55:27 EDT	2004-08-
irunin.dat	▽		2	2004-08-25 11:55:27 EDT	2004-08-
irunin.ini			2	2004-08-25 11:56:10 EDT	2004-08-

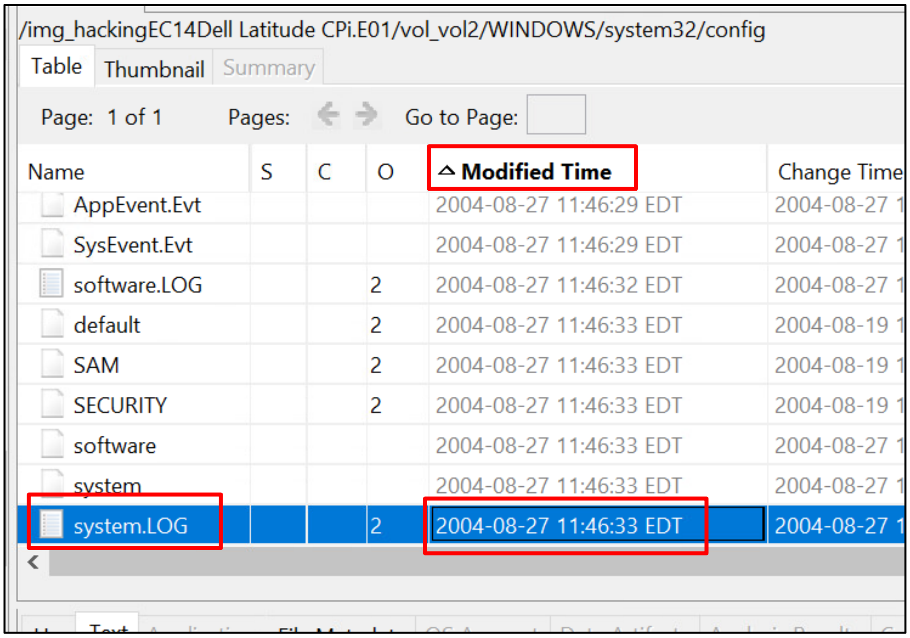
```
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
```

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

Answer: 27 August 2004 (11:46:33 AM EDT) (15:46:33 UTC)

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/system.LOG

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

Name	S	C	O	Modified Time	Change Time
AppEvent.Evt				2004-08-27 11:46:29 EDT	2004-08-27 1
SysEvent.Evt				2004-08-27 11:46:29 EDT	2004-08-27 1
software.LOG			2	2004-08-27 11:46:32 EDT	2004-08-27 1
default			2	2004-08-27 11:46:33 EDT	2004-08-19 1
SAM			2	2004-08-27 11:46:33 EDT	2004-08-19 1
SECURITY			2	2004-08-27 11:46:33 EDT	2004-08-19 1
software				2004-08-27 11:46:33 EDT	2004-08-27 1
system				2004-08-27 11:46:33 EDT	2004-08-27 1
system.LOG			2	2004-08-27 11:46:33 EDT	2004-08-27 1

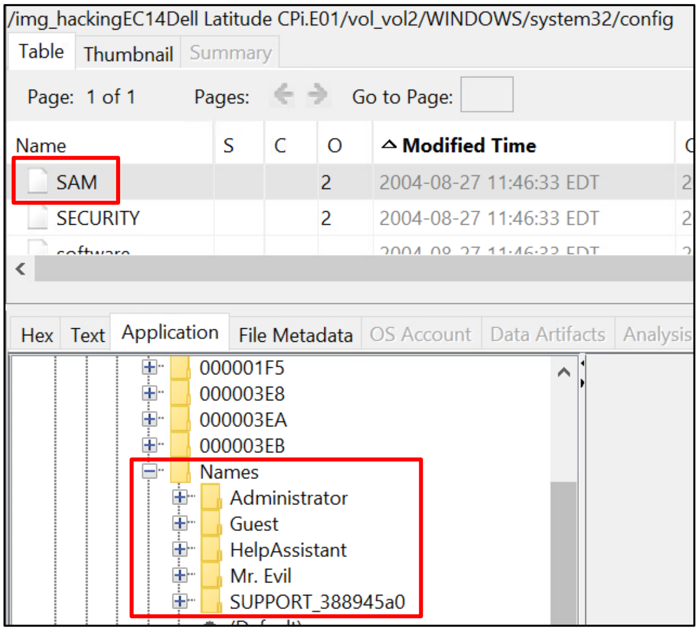
The **system.LOG** file can be considered for identifying the last shutdown or restart time because it records changes to the **SYSTEM** registry hive, which typically happens during a system shutdown or restart. The matching **modified time** of the **SYSTEM** hive and **system.LOG** indicates that the system was last written to during a controlled shutdown or restart, making it a reliable indicator of the system's last recorded shutdown time.

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

Answer: 5 (Administrator, Guest, HelpAssistant, Mr.Evil, SUPPORT_388945a0)

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config/SAM/Domains/Account/Users/Names/

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

Name	S	C	O	Modified Time
SAM			2	2004-08-27 11:46:33 EDT
SECURITY			2	2004-08-27 11:46:33 EDT
software				2004-08-27 11:46:33 EDT

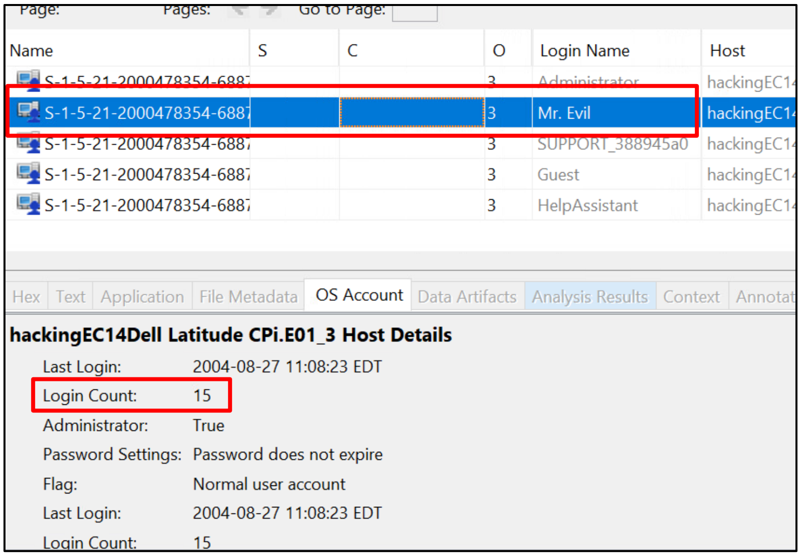
```
000001F5
000003E8
000003EA
000003EB
Names
  Administrator
  Guest
  HelpAssistant
  Mr. Evil
  SUPPORT_388945a0
```

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

Answer: Mr. Evil (15 Count)

Location: Found in OS Account Section

Evidence:



Name	S	C	O	Login Name	Host
S-1-5-21-2000478354-6887			3	Administrator	hackingEC14
S-1-5-21-2000478354-6887			3	Mr. Evil	hackingEC14
S-1-5-21-2000478354-6887			3	SUPPORT_388945a0	hackingEC14
S-1-5-21-2000478354-6887			3	Guest	hackingEC14
S-1-5-21-2000478354-6887			3	HelpAssistant	hackingEC14

hackingEC14Dell Latitude CPi.E01_3 Host Details

Last Login:	2004-08-27 11:08:23 EDT
Login Count:	15
Administrator:	True
Password Settings:	Password does not expire
Flag:	Normal user account
Last Login:	2004-08-27 11:08:23 EDT
Login Count:	15

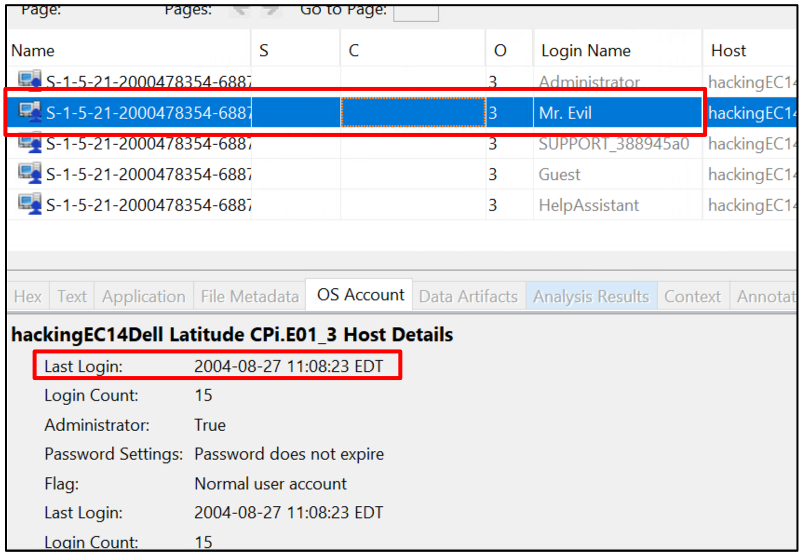
11. Who was the last user to logon to the computer?

Answer: Mr. Evil

(Date and Time Matches with Last Shutdown Date and Time)

Location: Found in OS Account Section

Evidence:



Name	S	C	O	Login Name	Host
S-1-5-21-2000478354-6887			3	Administrator	hackingEC14
S-1-5-21-2000478354-6887			3	Mr. Evil	hackingEC14
S-1-5-21-2000478354-6887			3	SUPPORT_388945a0	hackingEC14
S-1-5-21-2000478354-6887			3	Guest	hackingEC14
S-1-5-21-2000478354-6887			3	HelpAssistant	hackingEC14

hackingEC14Dell Latitude CPi.E01_3 Host Details

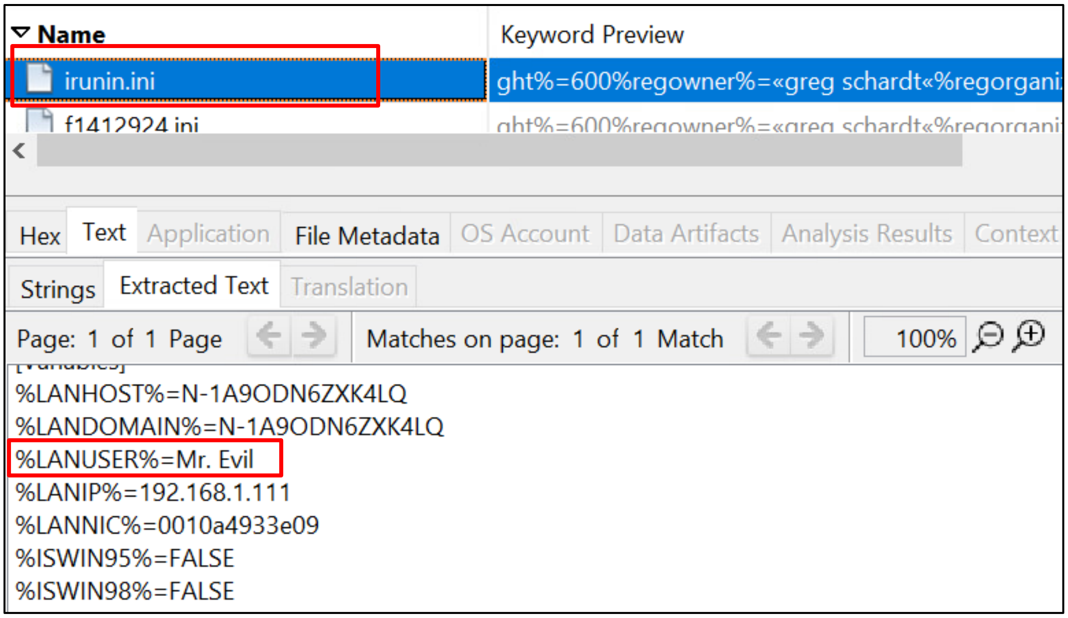
Last Login:	2004-08-27 11:08:23 EDT
Login Count:	15
Administrator:	True
Password Settings:	Password does not expire
Flag:	Normal user account
Last Login:	2004-08-27 11:08:23 EDT
Login Count:	15

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

Answer: irunin.ini

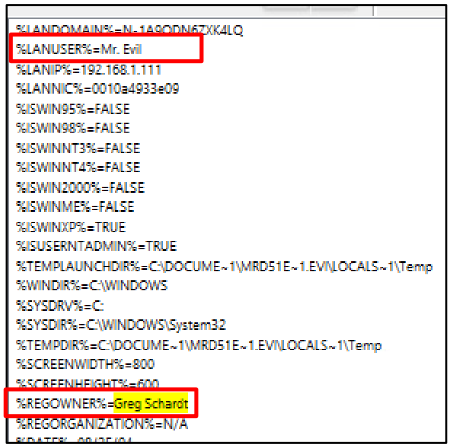
Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini

Evidence:



Name	Keyword Preview
irunin.ini	ght%=600%regowner%=«greg schardt«%regorgani
f1412924.ini	ght%=600%regowner%=«greg schardt«%regorgani

```
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
```



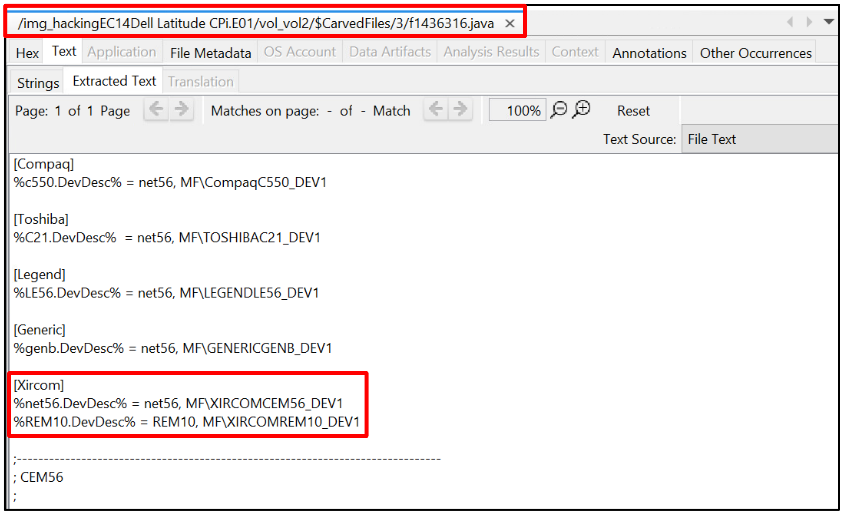
```
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE
%ISWINNT4%=FALSE
%ISWIN2000%=FALSE
%ISWINME%=FALSE
%ISWINXP%=TRUE
%ISUSERNTADMIN%=TRUE
%TEMPLAUNCHDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%WINDIR%=C:\WINDOWS
%SYSDRV%=C:
%SYSDIR%=C:\WINDOWS\System32
%TEMPDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%SCREENWIDTH%=800
%SCREENHEIGHT%=600
%REGOWNER%=Greg Schardt
%REGORGANIZATION%=N/A
```

13. List the network cards used by this computer

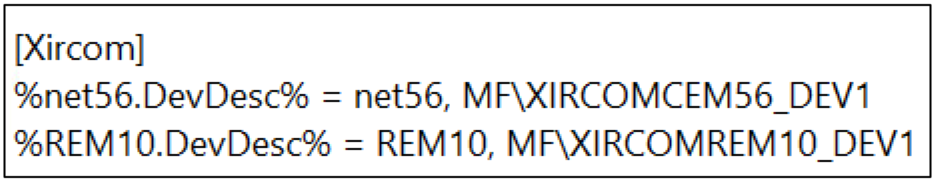
Answer: 2 (Xircom CreditCard Ethernet 10/100 + Modem 56 & Xircom Ethernet + Modem 56)

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$CarvedFiles/3/f1436316.java

Evidence:



```
[Compaq]
%c550.DevDesc% = net56, MF\CompaqC550_DEV1

[Toshiba]
%C21.DevDesc%  = net56, MF\TOSHIBAC21_DEV1

[Legend]
%LE56.DevDesc% = net56, MF\LEGENDLE56_DEV1

[Generic]
%genb.DevDesc% = net56, MF\GENERICGENB_DEV1

[Xircom]
%net56.DevDesc% = net56, MF\XIRCOMCEM56_DEV1
%REM10.DevDesc% = REM10, MF\XIRCOMREM10_DEV1

;------------------------------------------------------------------------------
; CEM56
;
```



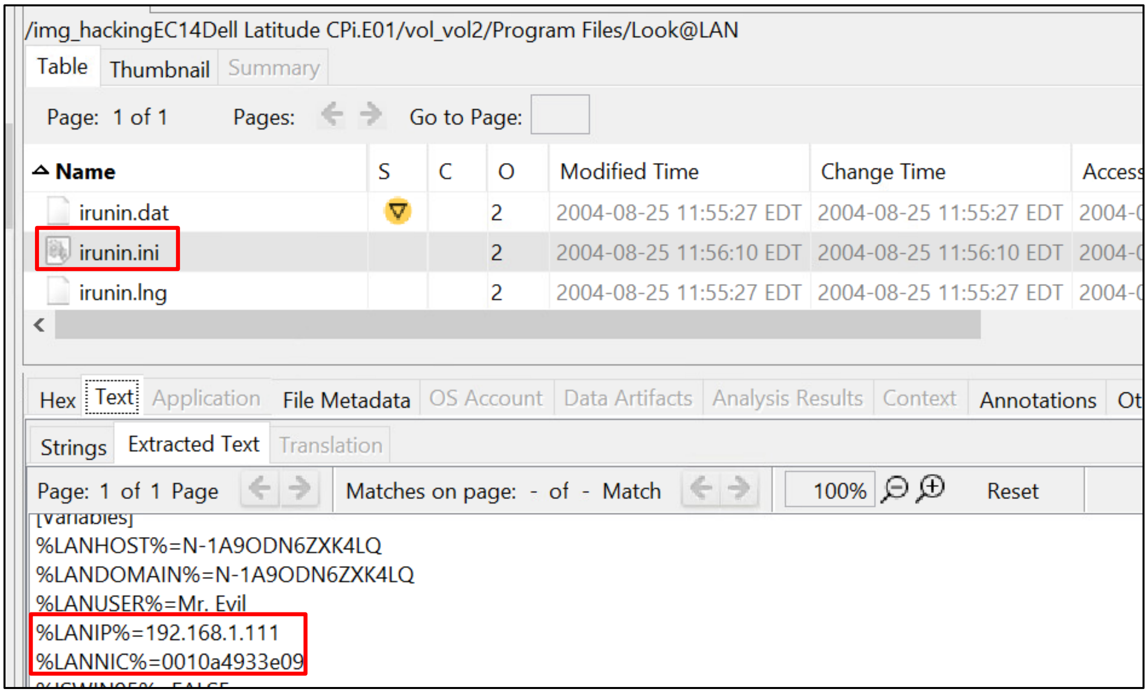
```
[Xircom]
%net56.DevDesc% = net56, MF\XIRCOMCEM56_DEV1
%REM10.DevDesc% = REM10, MF\XIRCOMREM10_DEV1
```

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

Answer: IP: 192.168.1.111 & MAC: 00:10: a4:93:3e:09

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN

Name	S	C	O	Modified Time	Change Time	Access
irunin.dat			2	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-(
irunin.ini			2	2004-08-25 11:56:10 EDT	2004-08-25 11:56:10 EDT	2004-(
irunin.lng			2	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-(

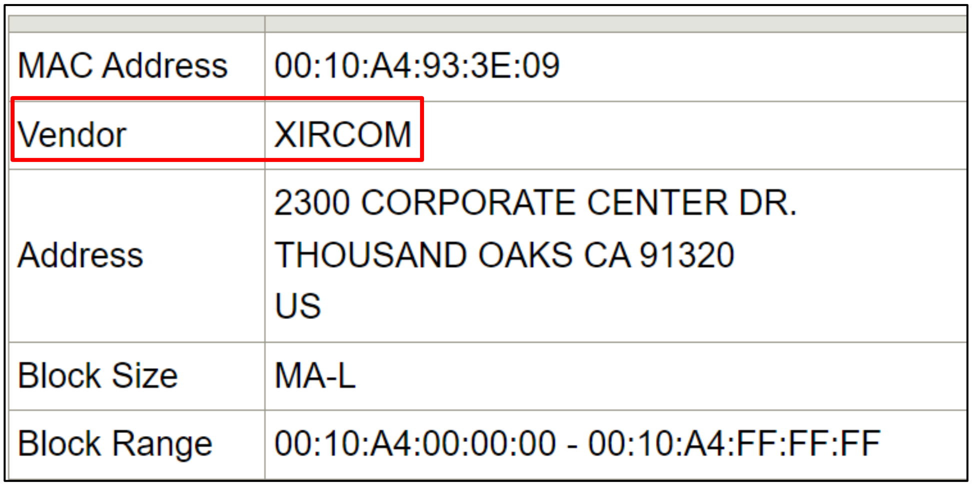
```
[variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
```

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?

Answer: Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)

Location: https://aruljohn.com/mac/0010A4933E09

Evidence:



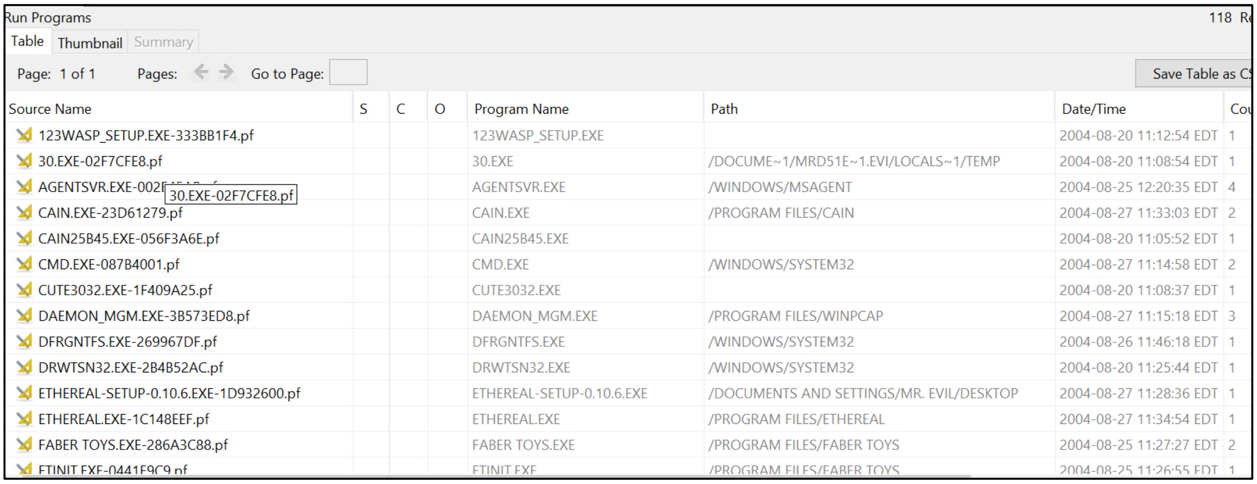
MAC Address	00:10:A4:93:3E:09
Vendor	XIRCOM
Address	2300 CORPORATE CENTER DR. THOUSAND OAKS CA 91320 US
Block Size	MA-L
Block Range	00:10:A4:00:00:00 - 00:10:A4:FF:FF:FF

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

Answer: 123WASP, CAIN, ETHEREAL, LOOK@LAN, NETSTUMBLER, TELNET, WHOIS

Location: Found Under Run Programs

Evidence:



Source Name	S	C	O	Program Name	Path	Date/Time	Cou
123WASP_SETUP.EXE-333BB1F4.pf				123WASP_SETUP.EXE		2004-08-20 11:12:54 EDT	1
30.EXE-02F7CFE8.pf				30.EXE	/DOCUME~1/MRD51E~1.EVI/LOCALS~1/TEMP	2004-08-20 11:08:54 EDT	1
AGENTSVR.EXE-002F				AGENTSVR.EXE	/WINDOWS/MSAGENT	2004-08-25 12:20:35 EDT	4
CAIN.EXE-23D61279.pf				CAIN.EXE	/PROGRAM FILES/CAIN	2004-08-27 11:33:03 EDT	2
CAIN25B45.EXE-056F3A6E.pf				CAIN25B45.EXE		2004-08-20 11:05:52 EDT	1
CMD.EXE-087B4001.pf				CMD.EXE	/WINDOWS/SYSTEM32	2004-08-27 11:14:58 EDT	2
CUTE3032.EXE-1F409A25.pf				CUTE3032.EXE		2004-08-20 11:08:37 EDT	1
DAEMON_MGM.EXE-3B573ED8.pf				DAEMON_MGM.EXE	/PROGRAM FILES/WINPCAP	2004-08-27 11:15:18 EDT	3
DFRGNTFS.EXE-269967DF.pf				DFRGNTFS.EXE	/WINDOWS/SYSTEM32	2004-08-26 11:46:18 EDT	1
DRWTSN32.EXE-2B4B52AC.pf				DRWTSN32.EXE	/WINDOWS/SYSTEM32	2004-08-20 11:25:44 EDT	1
ETHEREAL-SETUP-0.10.6.EXE-1D932600.pf				ETHEREAL-SETUP-0.10.6.EXE	/DOCUMENTS AND SETTINGS/MR. EVIL/DESKTOP	2004-08-27 11:28:36 EDT	1
ETHEREAL.EXE-1C148EEF.pf				ETHEREAL.EXE	/PROGRAM FILES/ETHEREAL	2004-08-27 11:34:54 EDT	1
FABER TOYS.EXE-286A3C88.pf				FABER TOYS.EXE	/PROGRAM FILES/FABER TOYS	2004-08-25 11:27:27 EDT	2
ETINIT.EXE-0441F9C9.pf				ETINIT.EXE	/PROGRAM FILES/FABER TOYS	2004-08-25 11:26:55 EDT	1

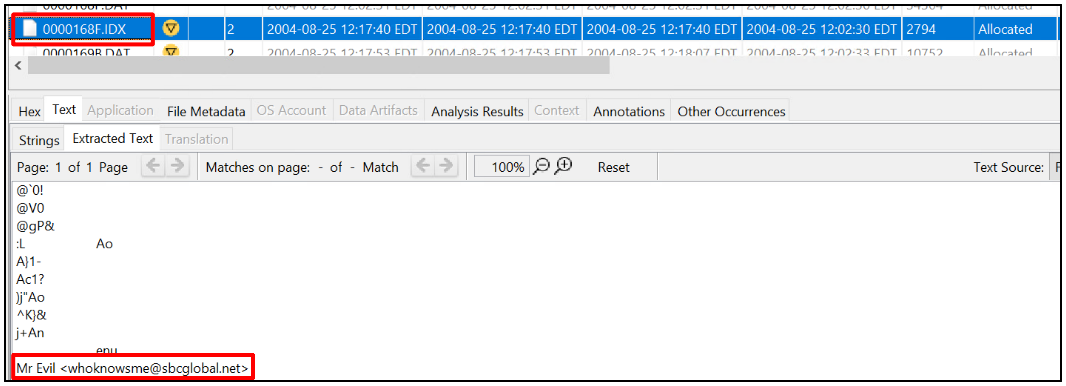
- **123WASP_SETUP.EXE / 123WASP.EXE** - Password recovery tool to retrieve stored passwords.
- **CAIN25B45.EXE / CAIN.EXE** - Cain & Abel, a password recovery and network sniffing tool.
- **ETHEREAL.EXE / ETHEREAL-SETUP-0.10.6.EXE** - Ethereal (now known as Wireshark), a packet sniffing tool.
- **LOOK@LAN.EXE** - A network monitoring tool often used for analyzing and scanning networks.
- **NETSTUMBLER.EXE / NETSTUMBLERINSTALLER_0_4_0.EXE** - A wireless networking tool used to detect Wi-Fi networks, sometimes used for Wi-Fi hacking.
- **TELNET.EXE** - Telnet, which can be used for remote access to servers, sometimes exploited for unauthorized access.
- **WHOIS.EXE** - Whois tool used to gather information about domain names and IP addresses, sometimes used in reconnaissance.

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

Answer: whoknowsme@sbcglobal.net

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data/0000168F.IDX

Evidence:



0000168F.IDX	2	2004-08-25 12:17:40 EDT	2004-08-25 12:17:40 EDT	2004-08-25 12:17:40 EDT	2004-08-25 12:02:30 EDT	2794	Allocated
0000169B.DAT	2	2004-08-25 12:17:53 EDT	2004-08-25 12:17:53 EDT	2004-08-25 12:18:07 EDT	2004-08-25 12:02:33 EDT	10752	Allocated

```
@`0!
@V0
@gP&
:L          Ao
A)1-
Ac1?
)j"Ao
^K)&
j+An
            enu
Mr Evil <whoknowsme@sbcglobal.net>
```

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

Answer:

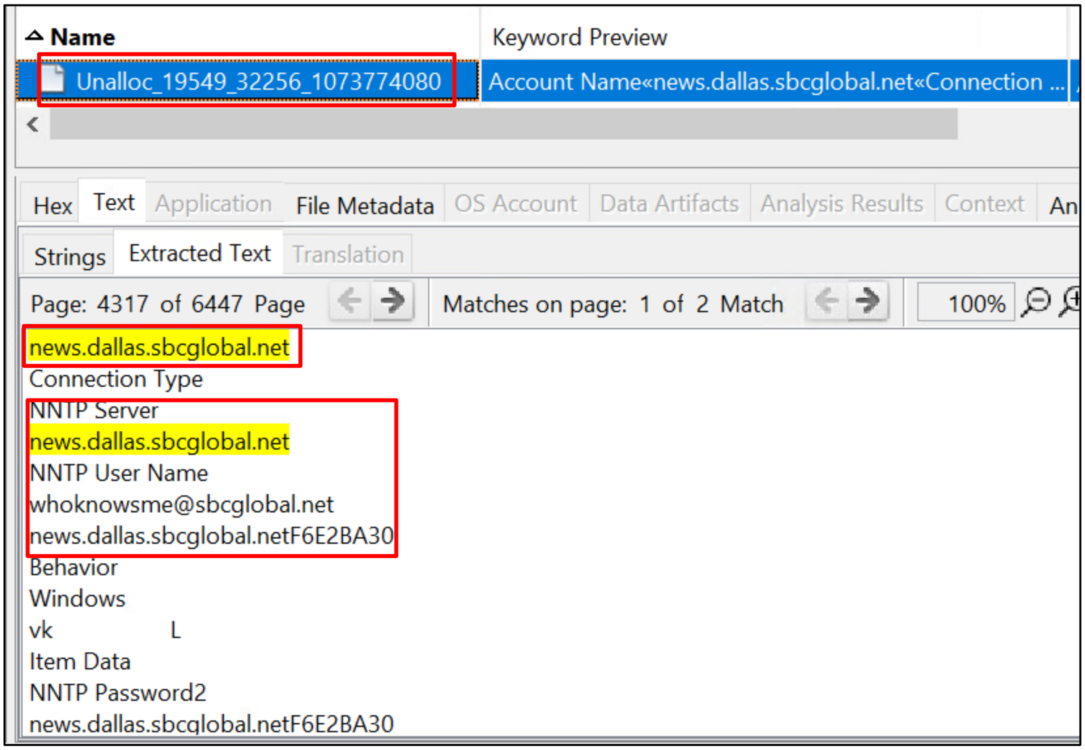
Server Name: news.dallas.sbcglobal.net

Server username: whoknowsme@sbcglobal.net

Server Password: news.dallas.sbcglobal.netF6E2BA30

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_19549_32256_1073774080

Evidence:



```
news.dallas.sbcglobal.net
Connection Type
NNTP Server
news.dallas.sbcglobal.net
NNTP User Name
whoknowsme@sbcglobal.net
news.dallas.sbcglobal.netF6E2BA30
Behavior
Windows
vk              L
Item Data
NNTP Password2
news.dallas.sbcglobal.netF6E2BA30
```

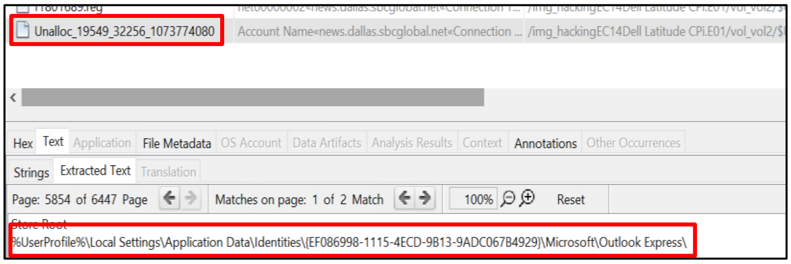
19. What two installed programs show this information?

Answer:

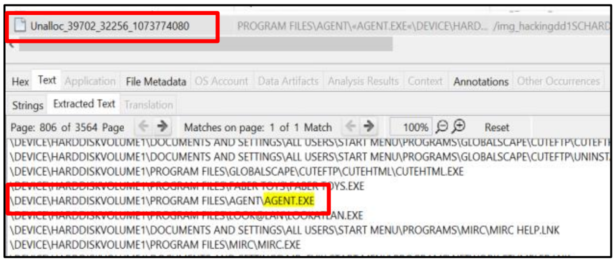
Forte Agent and Outlook Express

Location: /img_hackingdd1SCHARDT.001/vol_vol2/Unalloc_39702_32256_1073774080

Evidence:



```
Store Root
%UserProfile%\Local Settings\Application Data\Identities\{EF086998-1115-4ECD-9B13-9ADC067B4929}\Microsoft\Outlook Express\
```



```
\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\PROGRAMS\GLOBALSCAPE\CUTEFTP\CUTEFT
\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\PROGRAMS\GLOBALSCAPE\CUTEFTP\UNINST
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\GLOBALSCAPE\CUTEFTP\CUTEHTML\CUTEHTML.EXE
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\FABER TOYS\FABER TOYS.EXE
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\AGENT\AGENT.EXE
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\LOOK@LAN\LOOKATLAN.EXE
\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\PROGRAMS\MIRC\MIRC HELP.LNK
\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MIRC\MIRC.EXE
```

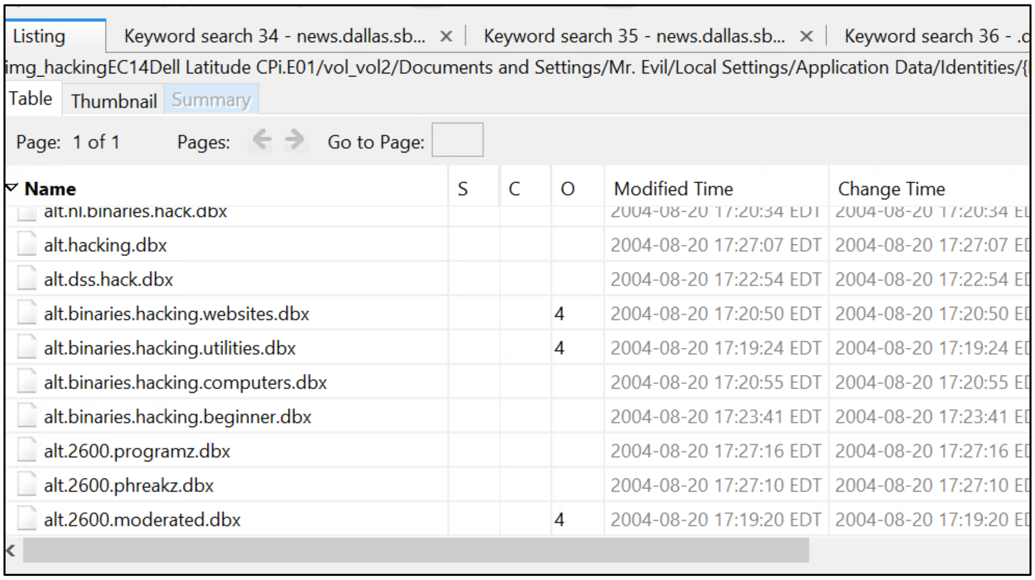
20. List 5 newsgroups that Mr. Evil has subscribed to?

Answer:

Alt.binaries.hacking.utilities
Alt.stupidity.hackers.malicious
Free.binaries.hackers.malicious
Free.binaries.hacking.talentless.troll_haven
alt.dss.hack

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{EF086998-1115-4ECD-9B13-9ADC067B4929}/Microsoft/Outlook Express

Evidence:



img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Application Data/Identities/{

Name	S	C	O	Modified Time	Change Time
alt.nl.binaries.hack.dbx				2004-08-20 17:20:34 EDT	2004-08-20 17:20:34 EI
alt.hacking.dbx				2004-08-20 17:27:07 EDT	2004-08-20 17:27:07 EI
alt.dss.hack.dbx				2004-08-20 17:22:54 EDT	2004-08-20 17:22:54 EI
alt.binaries.hacking.websites.dbx			4	2004-08-20 17:20:50 EDT	2004-08-20 17:20:50 EI
alt.binaries.hacking.utilities.dbx			4	2004-08-20 17:19:24 EDT	2004-08-20 17:19:24 EI
alt.binaries.hacking.computers.dbx				2004-08-20 17:20:55 EDT	2004-08-20 17:20:55 EI
alt.binaries.hacking.beginner.dbx				2004-08-20 17:23:41 EDT	2004-08-20 17:23:41 EI
alt.2600.programz.dbx				2004-08-20 17:27:16 EDT	2004-08-20 17:27:16 EI
alt.2600.phreakz.dbx				2004-08-20 17:27:10 EDT	2004-08-20 17:27:10 EI
alt.2600.moderated.dbx			4	2004-08-20 17:19:20 EDT	2004-08-20 17:19:20 EI

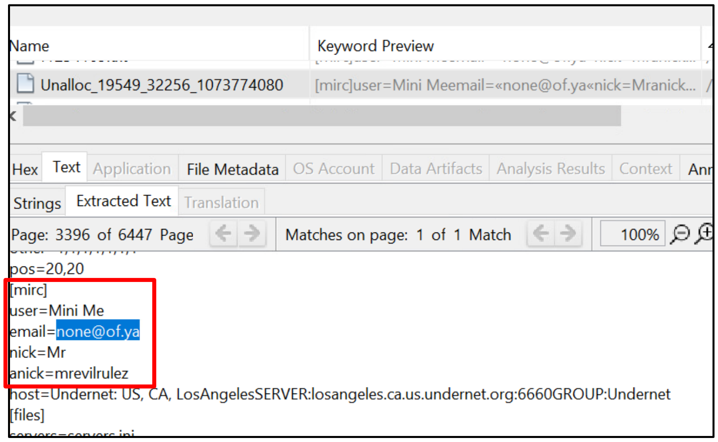
21. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?

Answer:

User: Mini Me
Email: none@of.ya
Nick: Mr
Anic: mrevilrulez

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$Unalloc/Unalloc_19549_32256_1073774080

Evidence:



Name	Keyword Preview
Unalloc_19549_32256_1073774080	[mirc]user=Mini Meemail=«none@of.ya«nick=Mranick...

```
pos=20,20
[mirc]
user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
host=Undernet: US, CA, LosAngelesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet
[files]
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.

Answer:

Chataholics.UnderNet

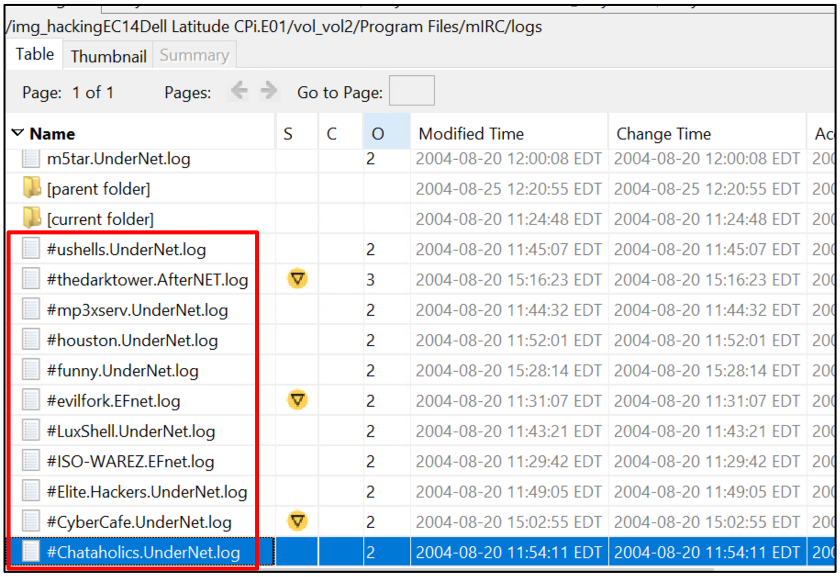
Elite.Hackers.UnderNet

thedarktower.AfterNET

mp3xserv.UnderNet

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/mIRC/logs/

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/mIRC/logs

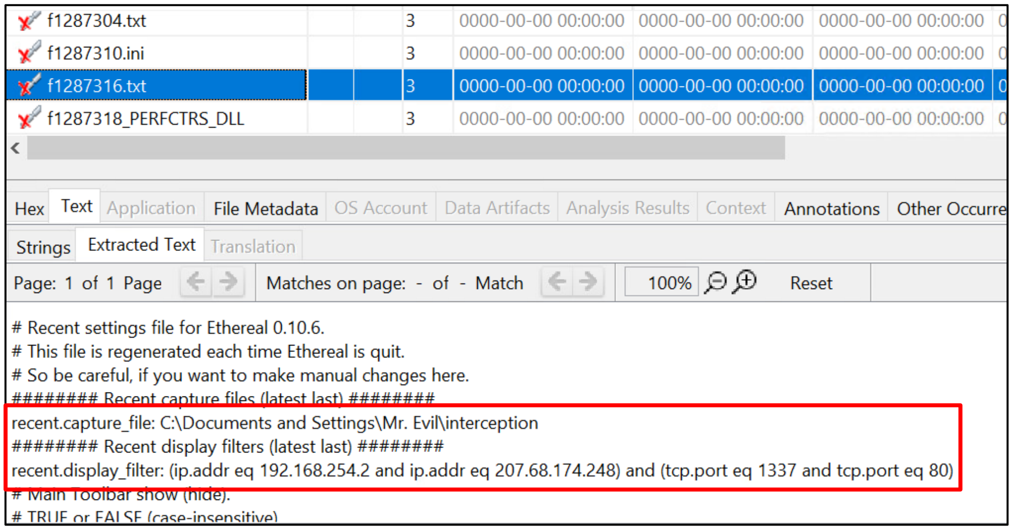
Name	S	C	O	Modified Time	Change Time	Ac
m5tar.UnderNet.log			2	2004-08-20 12:00:08 EDT	2004-08-20 12:00:08 EDT	200
[parent folder]				2004-08-25 12:20:55 EDT	2004-08-25 12:20:55 EDT	200
[current folder]				2004-08-20 11:24:48 EDT	2004-08-20 11:24:48 EDT	200
#ushells.UnderNet.log			2	2004-08-20 11:45:07 EDT	2004-08-20 11:45:07 EDT	200
#thedarktower.AfterNET.log	▽		3	2004-08-20 15:16:23 EDT	2004-08-20 15:16:23 EDT	200
#mp3xserv.UnderNet.log			2	2004-08-20 11:44:32 EDT	2004-08-20 11:44:32 EDT	200
#houston.UnderNet.log			2	2004-08-20 11:52:01 EDT	2004-08-20 11:52:01 EDT	200
#funny.UnderNet.log			2	2004-08-20 15:28:14 EDT	2004-08-20 15:28:14 EDT	200
#evilfork.EFnet.log	▽		2	2004-08-20 11:31:07 EDT	2004-08-20 11:31:07 EDT	200
#LuxShell.UnderNet.log			2	2004-08-20 11:43:21 EDT	2004-08-20 11:43:21 EDT	200
#ISO-WAREZ.EFnet.log			2	2004-08-20 11:29:42 EDT	2004-08-20 11:29:42 EDT	200
#Elite.Hackers.UnderNet.log			2	2004-08-20 11:49:05 EDT	2004-08-20 11:49:05 EDT	200
#CyberCafe.UnderNet.log	▽		2	2004-08-20 15:02:55 EDT	2004-08-20 15:02:55 EDT	200
#Chataholics.UnderNet.log			2	2004-08-20 11:54:11 EDT	2004-08-20 11:54:11 EDT	200

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

Answer: recent.capture_file: C:\Documents and Settings\Mr. Evil\interception

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$CarvedFiles/2/f1287316.txt

Evidence:



f1287304.txt			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
f1287310.ini			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
f1287316.txt			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
f1287318_PERFCTRS_DLL			3	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0

```
# Recent settings file for Ethereal 0.10.6.
# This file is regenerated each time Ethereal is quit.
# So be careful, if you want to make manual changes here.
######## Recent capture files (latest last) ########
recent.capture_file: C:\Documents and Settings\Mr. Evil\interception
######## Recent display filters (latest last) ########
recent.display_filter: (ip.addr eq 192.168.254.2 and ip.addr eq 207.68.174.248) and (tcp.port eq 1337 and tcp.port eq 80)
# Main Toolbar show (hide).
# TRUE or FALSE (case-insensitive).
```

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

Answer:

Computer: Windows CE (Pocket PC) Version-4.20

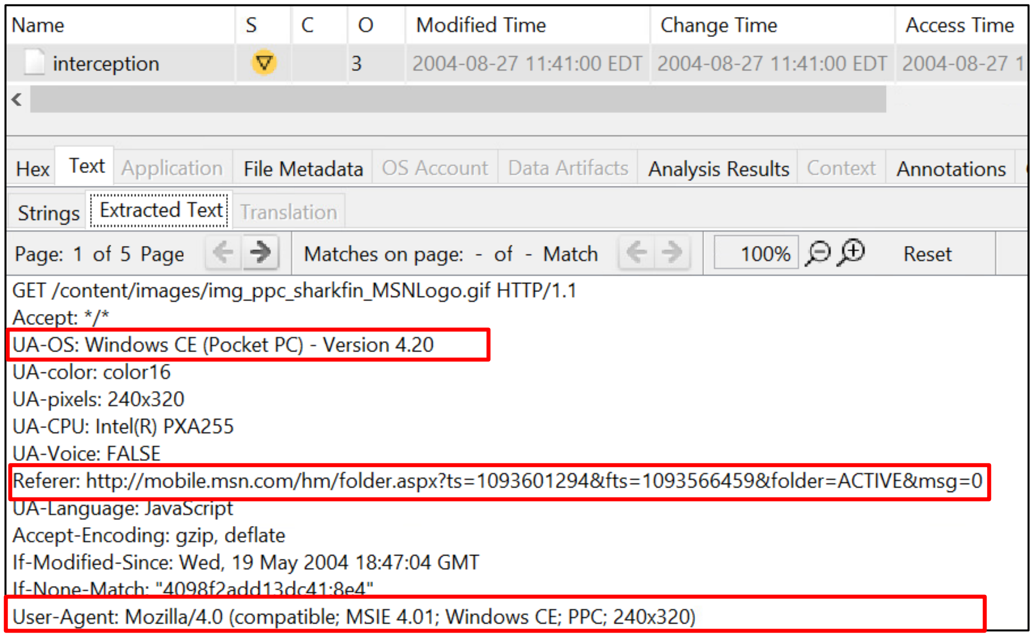
Browser: MS internet explorer 4.01

Intercept 1: Mobile.msn.com

Intercept 2: MSN Hotmail

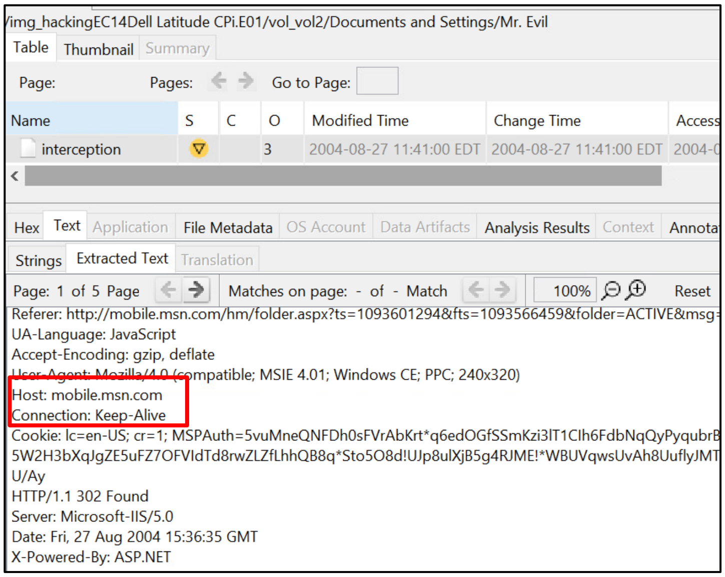
Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/interception

Evidence:



Name	S	C	O	Modified Time	Change Time	Access Time
interception	▽		3	2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-08-27 1

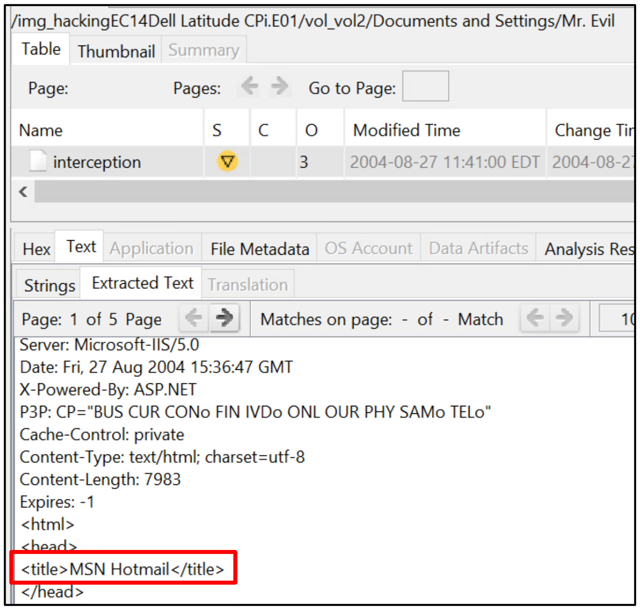
```
GET /content/images/img_ppc_sharkfin_MSNLogo.gif HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
If-Modified-Since: Wed, 19 May 2004 18:47:04 GMT
If-None-Match: "4098f2add13dc41:8e4"
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
```



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

Name	S	C	O	Modified Time	Change Time	Access
interception	▽		3	2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-0

```
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB
5W2H3bXqJgZE5uFZ7OFVIdTd8rwZLZfLhhQB8q*Sto5O8d!UJp8ulXjB5g4RJME!*WBUVqwsUvAh8UuflyJMT
U/Ay
HTTP/1.1 302 Found
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:35 GMT
X-Powered-By: ASP.NET
```



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

Name	S	C	O	Modified Time	Change Ti
interception	▽		3	2004-08-27 11:41:00 EDT	2004-08-2

```
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:47 GMT
X-Powered-By: ASP.NET
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 7983
Expires: -1
<html>
<head>
<title>MSN Hotmail</title>
</head>
```

25. What websites was the victim accessing?

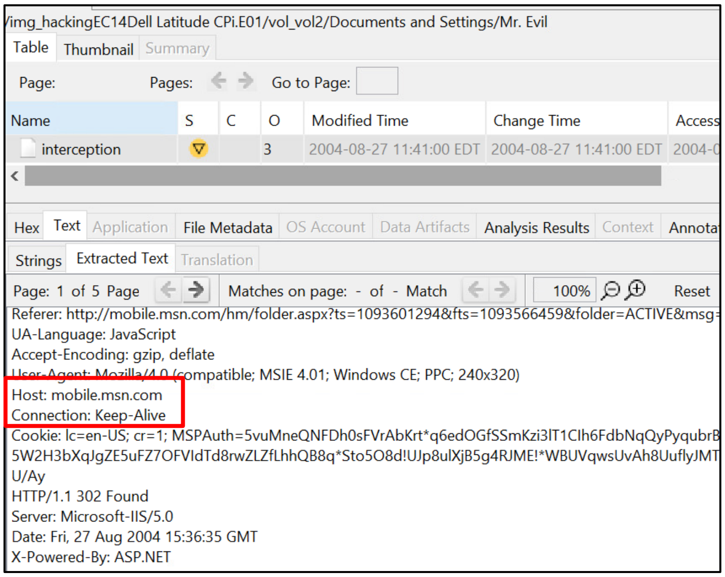
Answer:

Intercept 1: Mobile.msn.com

Intercept 2: MSN Hotmail

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/interception

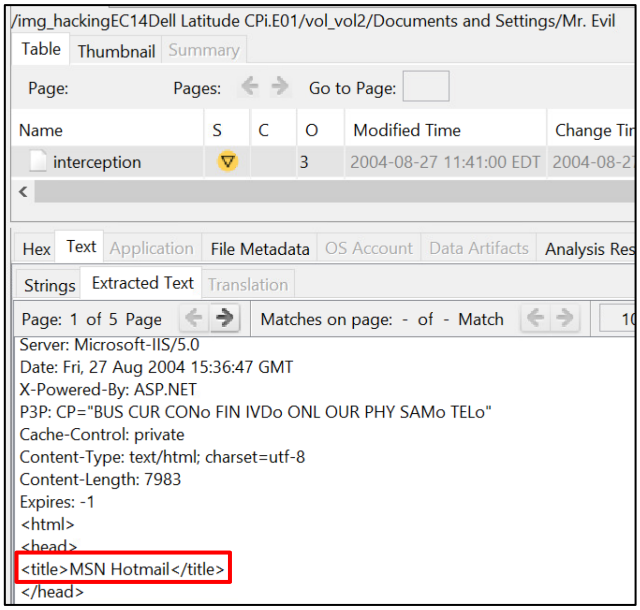
Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

Name	S	C	O	Modified Time	Change Time	Access
interception	▽		3	2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-0

```
Referer: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB
5W2H3bXqJgZE5uFZ7OFVIdTd8rwZLZfLhhQB8q*Sto5O8d!UJp8ulXjB5g4RJME!*WBUVqwsUvAh8UuflyJMT
U/Ay
HTTP/1.1 302 Found
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:35 GMT
X-Powered-By: ASP.NET
```



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil

Name	S	C	O	Modified Time	Change Tir
interception	▽		3	2004-08-27 11:41:00 EDT	2004-08-2

```
Server: Microsoft-IIS/5.0
Date: Fri, 27 Aug 2004 15:36:47 GMT
X-Powered-By: ASP.NET
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 7983
Expires: -1
<html>
<head>
<title>MSN Hotmail</title>
</head>
```

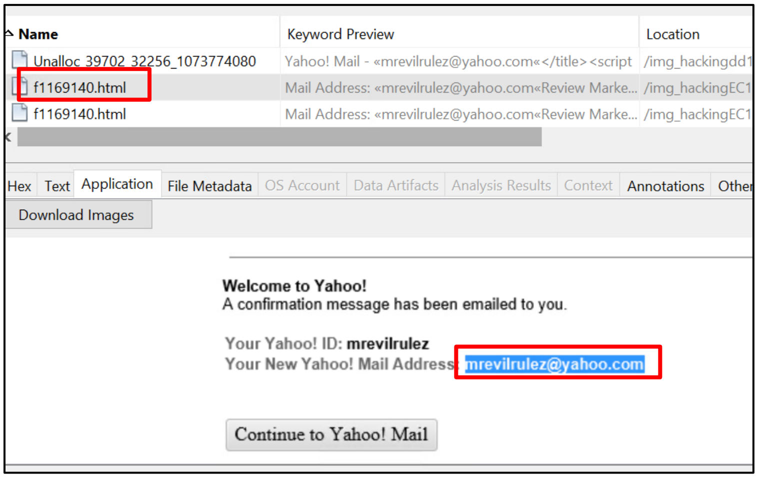
26. Search for the main user's web-based email address. What is it?

Answer: mrevilrulez@yahoo.com

Location 1: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/$CarvedFiles/6/f1169140.html.gz/f1169140.html

Location 2: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/History/History.IE5/MSHist012004081620040823/index.dat

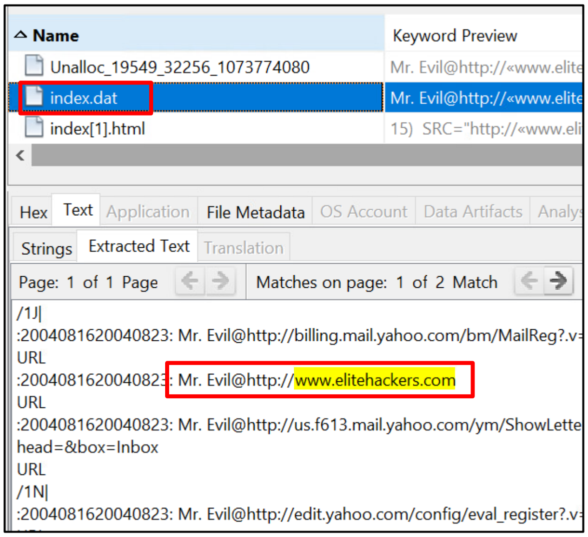
Evidence:



Name	Keyword Preview	Location
Unalloc_39702_32256_1073774080	Yahoo! Mail - «mrevilrulez@yahoo.com«</title><script	/img_hackingdd1
f1169140.html	Mail Address: «mrevilrulez@yahoo.com«Review Marke...	/img_hackingEC1
f1169140.html	Mail Address: «mrevilrulez@yahoo.com«Review Marke...	/img_hackingEC1

Welcome to Yahoo!
A confirmation message has been emailed to you.

Your Yahoo! ID: **mrevilrulez**
Your New Yahoo! Mail Address: mrevilrulez@yahoo.com



Name	Keyword Preview
Unalloc_19549_32256_1073774080	Mr. Evil@http://«www.elite
index.dat	Mr. Evil@http://«www.elite
index[1].html	15) SRC="http://«www.eli

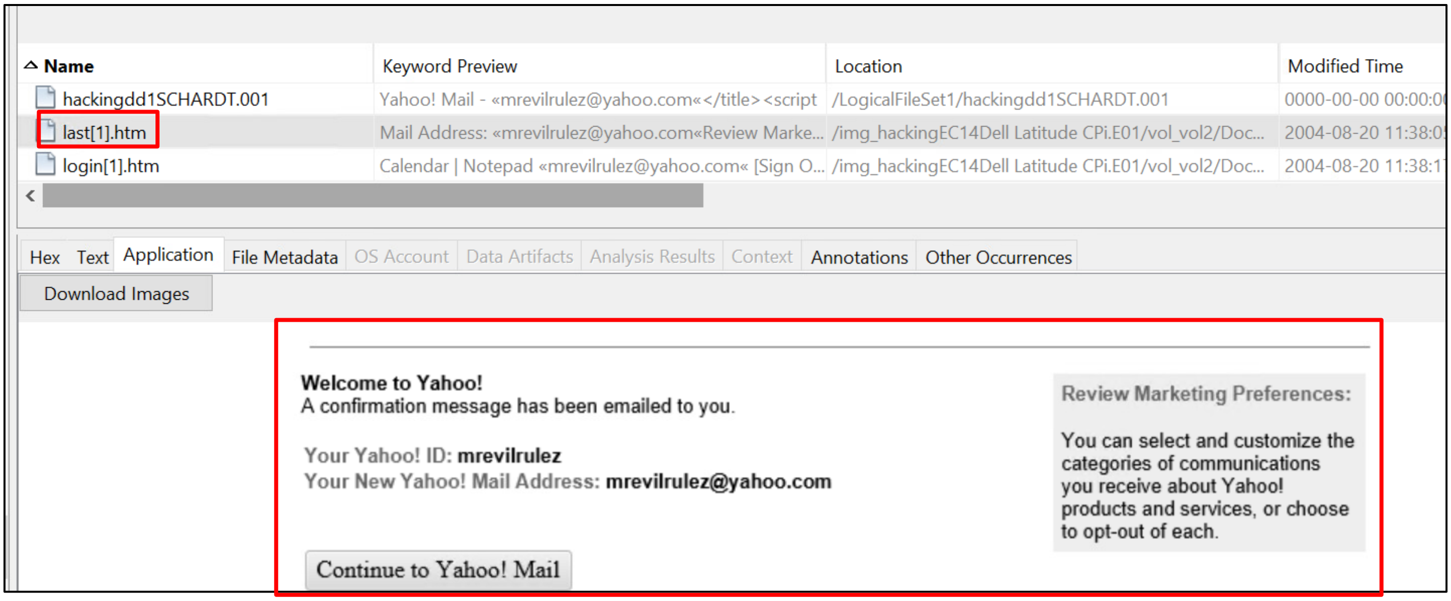
```
/1J|
:2004081620040823: Mr. Evil@http://billing.mail.yahoo.com/bm/MailReg?.v=
URL
:2004081620040823: Mr. Evil@http://www.elitehackers.com
URL
:2004081620040823: Mr. Evil@http://us.f613.mail.yahoo.com/ym/ShowLette
head=&box=Inbox
URL
/1N|
:2004081620040823: Mr. Evil@http://edit.yahoo.com/config/eval_register?.v=
```

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

Answer: last[1].htm

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Temporary Internet Files/Content.IE5/HYU1BON0/last[1].htm

Evidence:



Name	Keyword Preview	Location	Modified Time
hackingdd1SCHARDT.001	Yahoo! Mail - «mrevilrulez@yahoo.com«</title><script	/LogicalFileSet1/hackingdd1SCHARDT.001	0000-00-00 00:00:0
last[1].htm	Mail Address: «mrevilrulez@yahoo.com«Review Marke...	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Doc...	2004-08-20 11:38:0
login[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign O...	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Doc...	2004-08-20 11:38:1

Welcome to Yahoo!
A confirmation message has been emailed to you.

Your Yahoo! ID: **mrevilrulez**
Your New Yahoo! Mail Address: **mrevilrulez@yahoo.com**

Review Marketing Preferences:

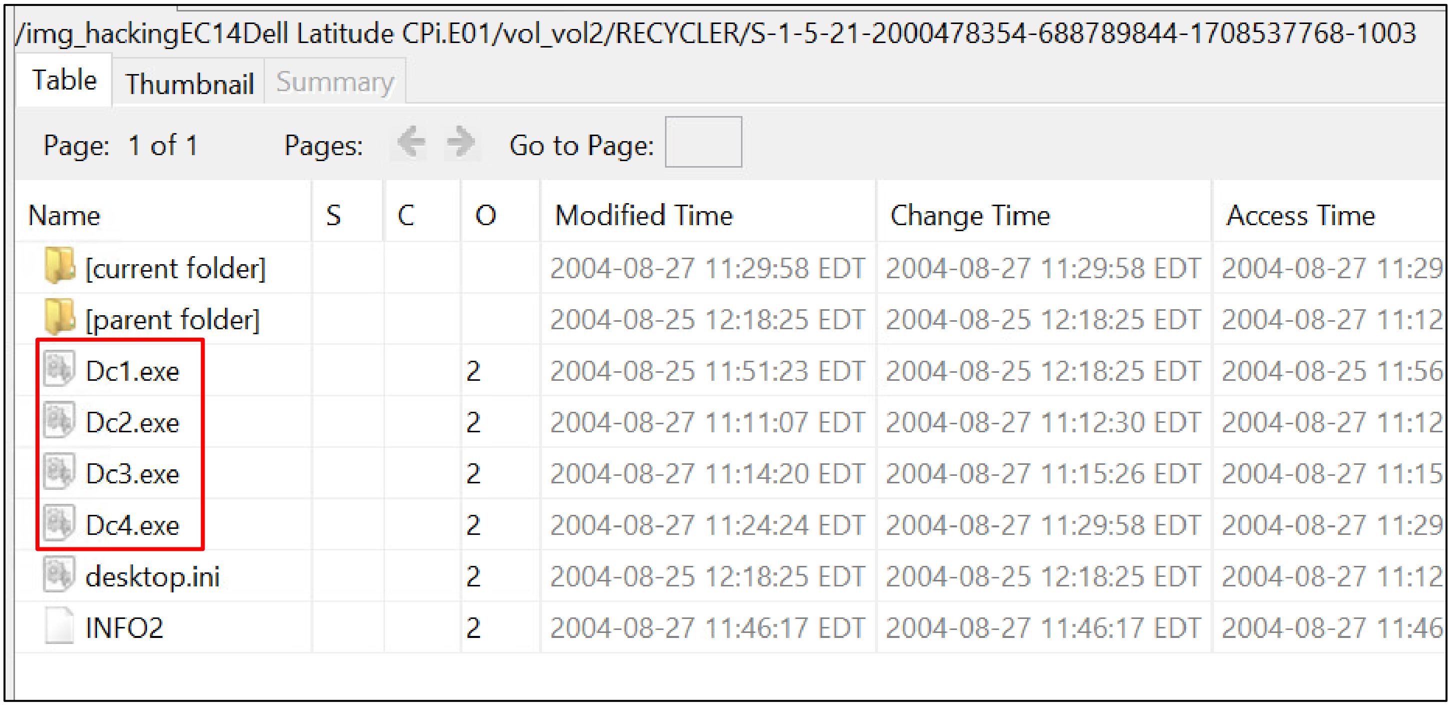
You can select and customize the categories of communications you receive about Yahoo! products and services, or choose to opt-out of each.

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

Answer: 4 Portable Executable files

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

Evidence:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

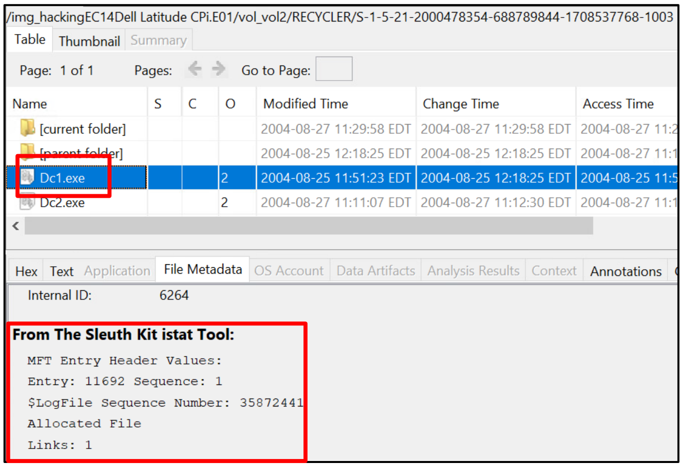
Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2004-08-27 11:29:58 EDT	2004-08-27 11:29:58 EDT	2004-08-27 11:29
[parent folder]				2004-08-25 12:18:25 EDT	2004-08-25 12:18:25 EDT	2004-08-27 11:12
Dc1.exe			2	2004-08-25 11:51:23 EDT	2004-08-25 12:18:25 EDT	2004-08-25 11:56
Dc2.exe			2	2004-08-27 11:11:07 EDT	2004-08-27 11:12:30 EDT	2004-08-27 11:12
Dc3.exe			2	2004-08-27 11:14:20 EDT	2004-08-27 11:15:26 EDT	2004-08-27 11:15
Dc4.exe			2	2004-08-27 11:24:24 EDT	2004-08-27 11:29:58 EDT	2004-08-27 11:29
desktop.ini			2	2004-08-25 12:18:25 EDT	2004-08-25 12:18:25 EDT	2004-08-27 11:12
INFO2			2	2004-08-27 11:46:17 EDT	2004-08-27 11:46:17 EDT	2004-08-27 11:46

29. Are these files really deleted?

Answer: NO

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

Evidence:



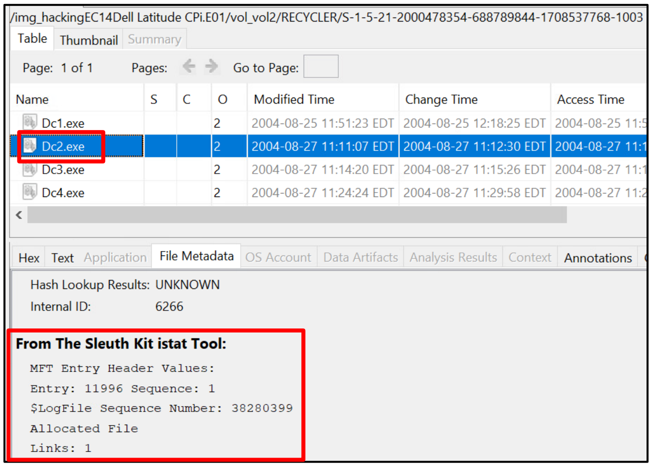
/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2004-08-27 11:29:58 EDT	2004-08-27 11:29:58 EDT	2004-08-27 11:2
[parent folder]				2004-08-25 12:18:25 EDT	2004-08-25 12:18:25 EDT	2004-08-27 11:1
Dc1.exe			2	2004-08-25 11:51:23 EDT	2004-08-25 12:18:25 EDT	2004-08-25 11:5
Dc2.exe			2	2004-08-27 11:11:07 EDT	2004-08-27 11:12:30 EDT	2004-08-27 11:1

Internal ID: 6264

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 11692 Sequence: 1
$LogFile Sequence Number: 35872441
Allocated File
Links: 1
```



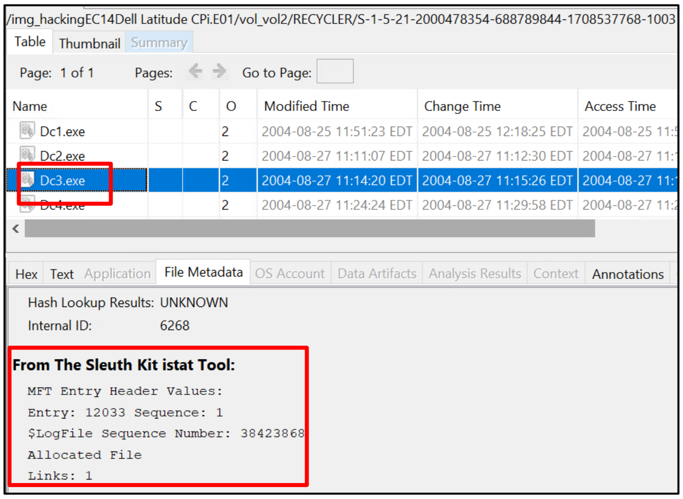
/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

Name	S	C	O	Modified Time	Change Time	Access Time
Dc1.exe			2	2004-08-25 11:51:23 EDT	2004-08-25 12:18:25 EDT	2004-08-25 11:5
Dc2.exe			2	2004-08-27 11:11:07 EDT	2004-08-27 11:12:30 EDT	2004-08-27 11:1
Dc3.exe			2	2004-08-27 11:14:20 EDT	2004-08-27 11:15:26 EDT	2004-08-27 11:1
Dc4.exe			2	2004-08-27 11:24:24 EDT	2004-08-27 11:29:58 EDT	2004-08-27 11:2

Hash Lookup Results: UNKNOWN
Internal ID: 6266

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 11996 Sequence: 1
$LogFile Sequence Number: 38280399
Allocated File
Links: 1
```



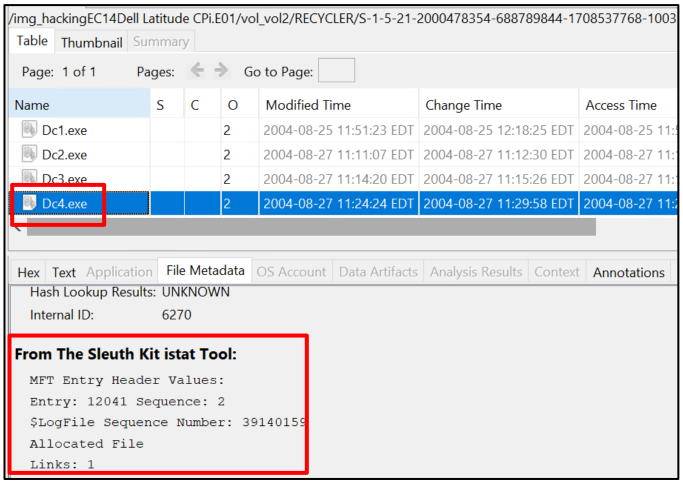
/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

Name	S	C	O	Modified Time	Change Time	Access Time
Dc1.exe			2	2004-08-25 11:51:23 EDT	2004-08-25 12:18:25 EDT	2004-08-25 11:5
Dc2.exe			2	2004-08-27 11:11:07 EDT	2004-08-27 11:12:30 EDT	2004-08-27 11:1
Dc3.exe			2	2004-08-27 11:14:20 EDT	2004-08-27 11:15:26 EDT	2004-08-27 11:1
Dc4.exe			2	2004-08-27 11:24:24 EDT	2004-08-27 11:29:58 EDT	2004-08-27 11:2

Hash Lookup Results: UNKNOWN
Internal ID: 6268

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
Entry: 12033 Sequence: 1
$LogFile Sequence Number: 38423868
Allocated File
Links: 1
```



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

Name	S	C	O	Modified Time	Change Time	Access Time
Dc1.exe			2	2004-08-25 11:51:23 EDT	2004-08-25 12:18:25 EDT	2004-08-25 11:
Dc2.exe			2	2004-08-27 11:11:07 EDT	2004-08-27 11:12:30 EDT	2004-08-27 11:
Dc3.exe			2	2004-08-27 11:14:20 EDT	2004-08-27 11:15:26 EDT	2004-08-27 11:
Dc4.exe			2	2004-08-27 11:24:24 EDT	2004-08-27 11:29:58 EDT	2004-08-27 11:

Hash Lookup Results: UNKNOWN
Internal ID: 6270

From The Sleuth Kit istat Tool:

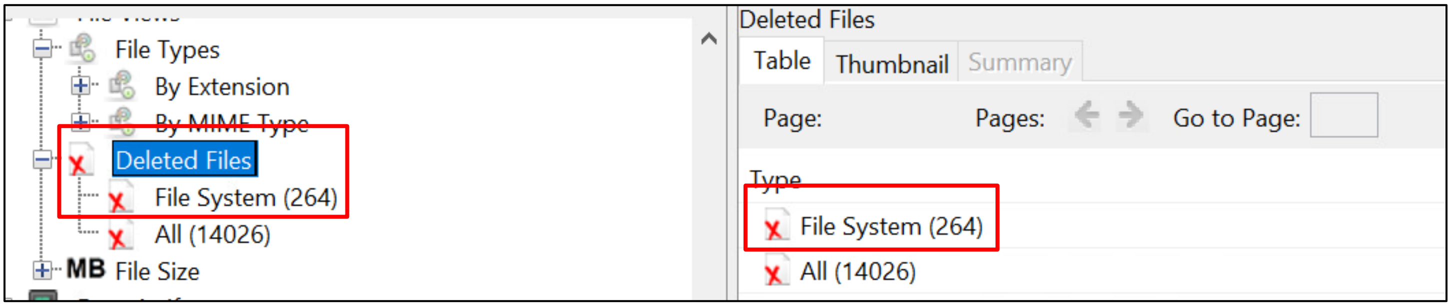
```
MFT Entry Header Values:
Entry: 12041 Sequence: 2
$LogFile Sequence Number: 39140159
Allocated File
Links: 1
```

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

Answer: 264

Location: Found in Deleted Files Section

Evidence:

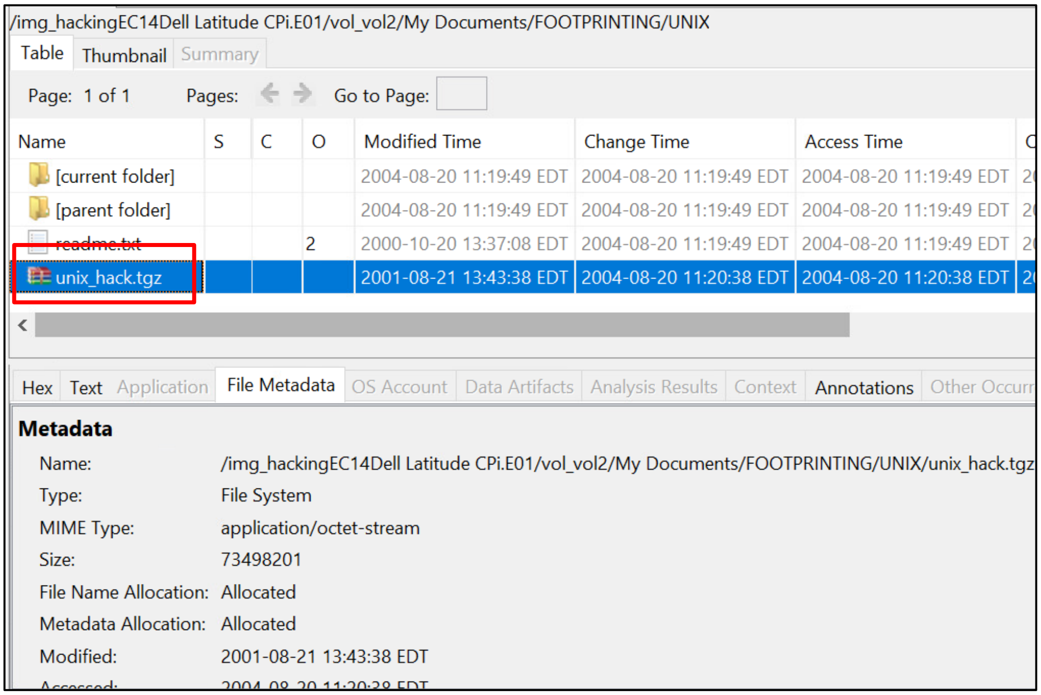


31. Perform an Anti-Virus check. Are there any viruses on the computer?

Answer: Yes (Possible File: unix_hack.tgz)

Location: /img_hackingEC14Dell Latitude CPi.E01/vol_vol2/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz

Evidence:



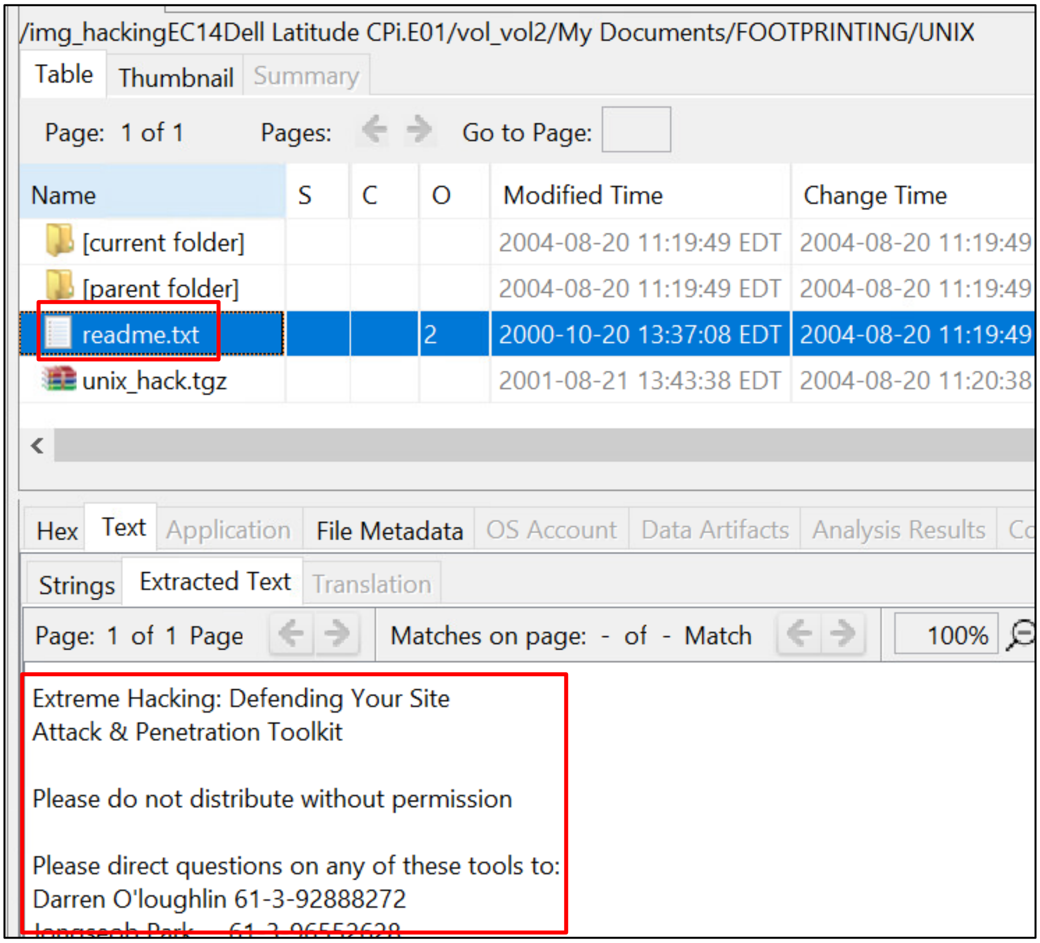
/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/My Documents/FOOTPRINTING/UNIX

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT
[parent folder]				2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT
readme.txt			2	2000-10-20 13:37:08 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT
unix_hack.tgz				2001-08-21 13:43:38 EDT	2004-08-20 11:20:38 EDT	2004-08-20 11:20:38 EDT

Metadata

Name:	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz
Type:	File System
MIME Type:	application/octet-stream
Size:	73498201
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2001-08-21 13:43:38 EDT
Accessed:	2004-08-20 11:20:38 EDT

Instruction about Virus:



/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/My Documents/FOOTPRINTING/UNIX

Name	S	C	O	Modified Time	Change Time
[current folder]				2004-08-20 11:19:49 EDT	2004-08-20 11:19:49
[parent folder]				2004-08-20 11:19:49 EDT	2004-08-20 11:19:49
readme.txt			2	2000-10-20 13:37:08 EDT	2004-08-20 11:19:49
unix_hack.tgz				2001-08-21 13:43:38 EDT	2004-08-20 11:20:38

Extreme Hacking: Defending Your Site
Attack & Penetration Toolkit

Please do not distribute without permission

Please direct questions on any of these tools to:
Darren O'loughlin 61-3-92888272
Jongseob Park 61-3-96552628