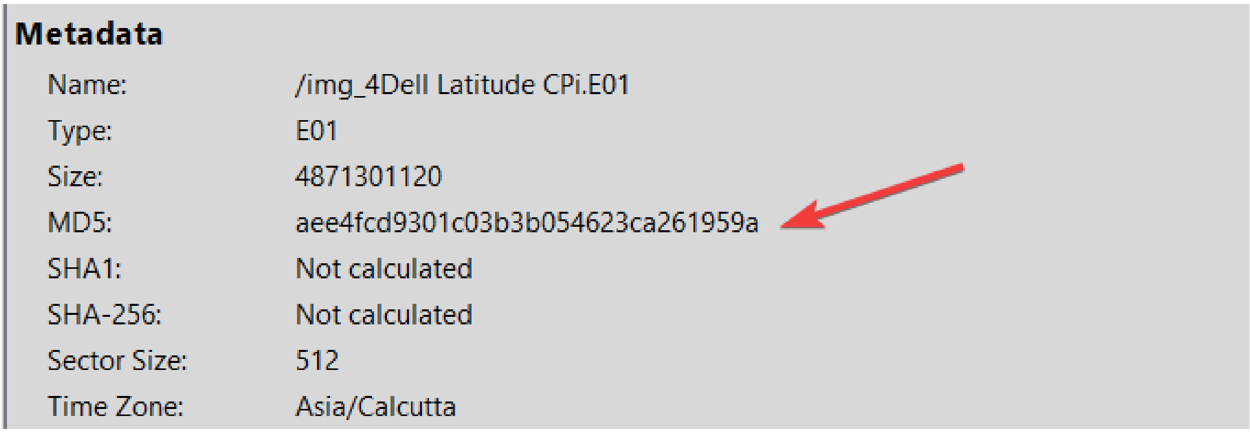
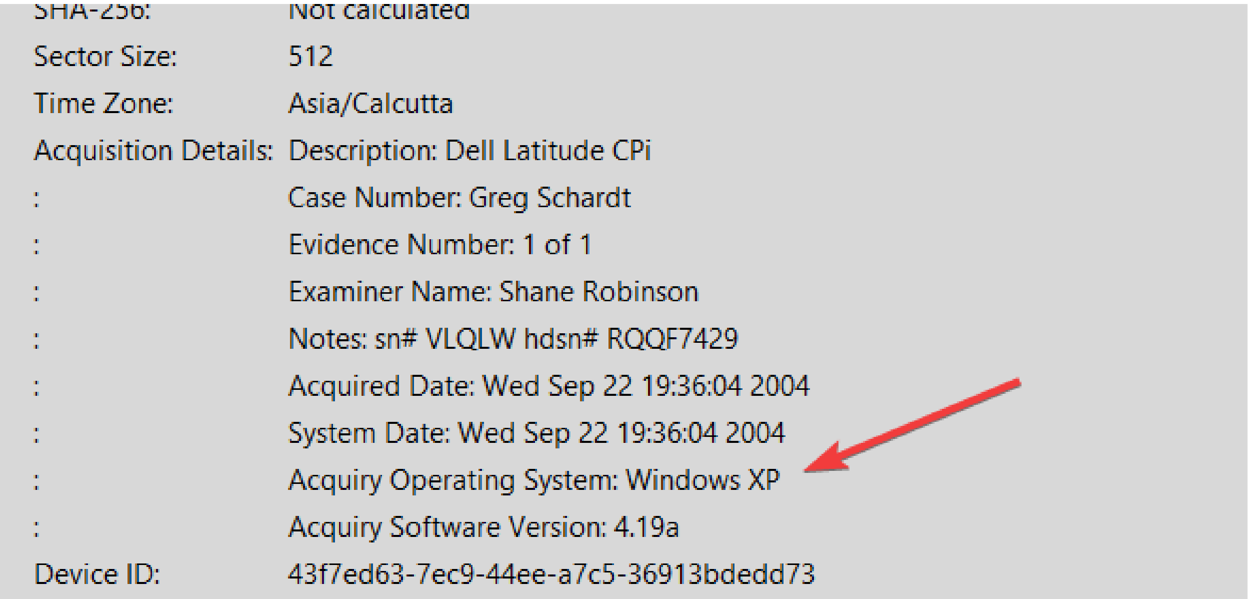
1. What is the image hash? Does the acquisition and verification hash match?
Ans: aee4fcd9301c03b3b054623ca261959a. Yes



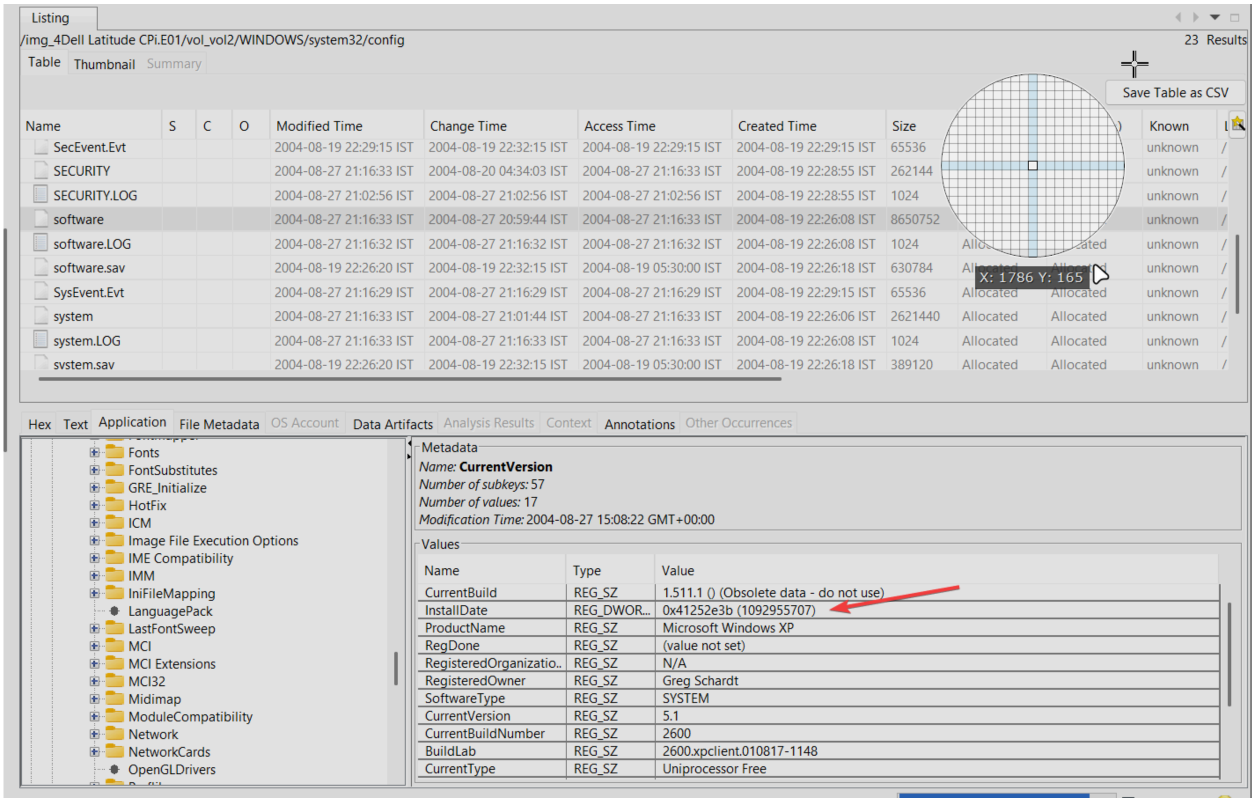
```
Metadata
  Name:               /img_4Dell Latitude CPi.E01
  Type:               E01
  Size:               4871301120
  MD5:                aee4fcd9301c03b3b054623ca261959a
  SHA1:               Not calculated
  SHA-256:            Not calculated
  Sector Size:        512
  Time Zone:          Asia/Calcutta
```

2. What operating system was used on the computer?
Ans: Windows XP



```
SHA-256:              Not calculated
Sector Size:          512
Time Zone:            Asia/Calcutta
Acquisition Details:  Description: Dell Latitude CPi
:                     Case Number: Greg Schardt
:                     Evidence Number: 1 of 1
:                     Examiner Name: Shane Robinson
:                     Notes: sn# VLQLW hdsn# RQQF7429
:                     Acquired Date: Wed Sep 22 19:36:04 2004
:                     System Date: Wed Sep 22 19:36:04 2004
:                     Acquiry Operating System: Windows XP
:                     Acquiry Software Version: 4.19a
Device ID:            43f7ed63-7ec9-44ee-a7c5-36913bdedd73
```

3. When was the install date?
Ans: **Your time zone**: Friday, 20 August 2004 04:18:27 GMT+05:30



/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size		)	Known	L
SecEvent.Evt				2004-08-19 22:29:15 IST	2004-08-19 22:32:15 IST	2004-08-19 22:29:15 IST	2004-08-19 22:29:15 IST	65536			unknown	/
SECURITY				2004-08-27 21:16:33 IST	2004-08-20 04:34:03 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144			unknown	/
SECURITY.LOG				2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:28:55 IST	1024			unknown	/
software				2004-08-27 21:16:33 IST	2004-08-27 20:59:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	8650752			unknown	/
software.LOG				2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-19 22:26:08 IST	1024	Allo	ated	unknown	/
software.sav				2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	630784	Al		unknown	/
SysEvent.Evt				2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated	unknown	/
system				2004-08-27 21:16:33 IST	2004-08-27 21:01:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:06 IST	2621440	Allocated	Allocated	unknown	/
system.LOG				2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated	unknown	/
svstem.sav				2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	389120	Allocated	Allocated	unknown	/

Fonts
FontSubstitutes
GRE_Initialize
HotFix
ICM
Image File Execution Options
IME Compatibility
IMM
IniFileMapping
LanguagePack
LastFontSweep
MCI
MCI Extensions
MCI32
Midimap
ModuleCompatibility
Network
NetworkCards
OpenGLDrivers

Metadata

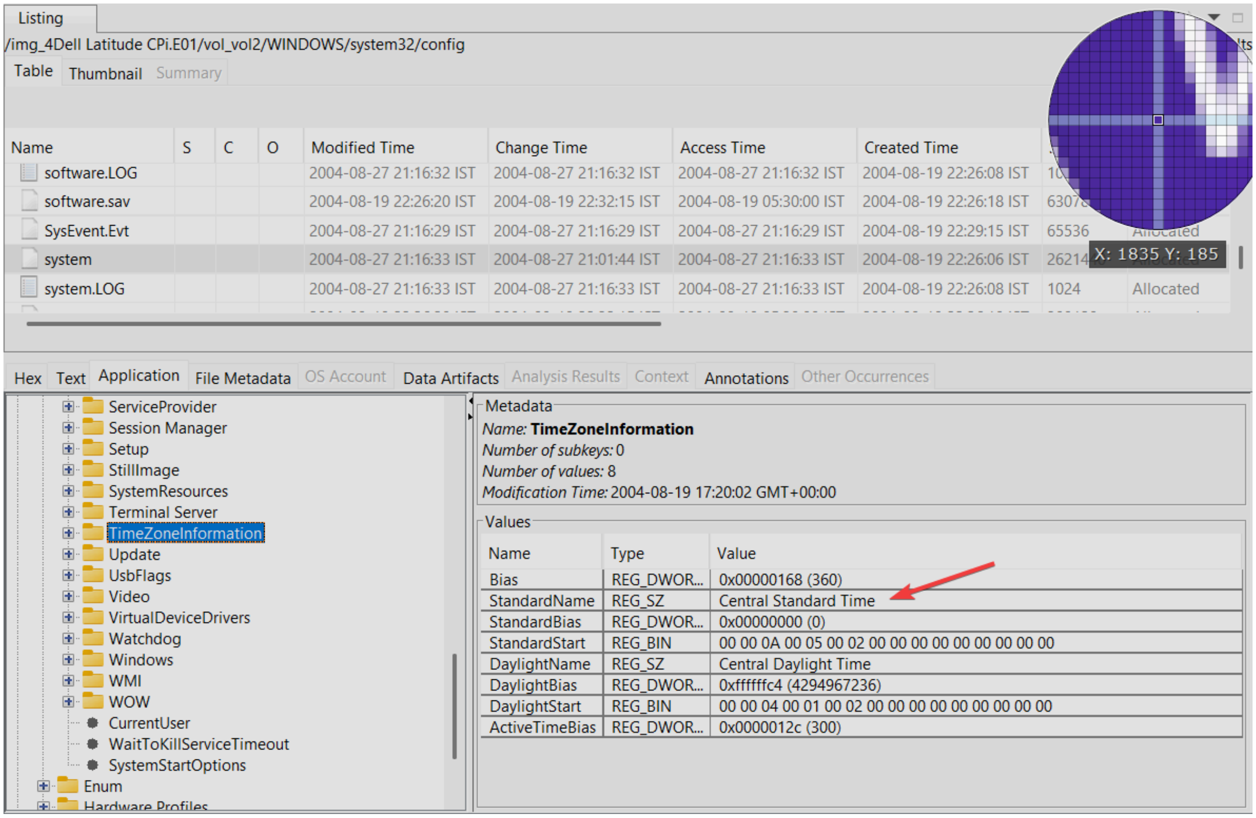
Name: **CurrentVersion**
Number of subkeys: 57
Number of values: 17
Modification Time: 2004-08-27 15:08:22 GMT+00:00

Values

Name	Type	Value
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWOR...	0x41252e3b (1092955707)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganizatio..	REG_SZ	N/A
RegisteredOwner	REG_SZ	Greg Schardt
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpclient.010817-1148
CurrentType	REG_SZ	Uniprocessor Free

4. What is the timezone settings?

Ans: Central Standard Time => Friday, 20 August 2004 04:48:27 GMT+06:00



Listing

/img_4Dell Latitude CPi.E01/vol_vol2/WINDOWS/system32/config

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time		
software.LOG				2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-19 22:26:08 IST	10	
software.sav				2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	6307	
SysEvent.Evt				2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-19 22:29:15 IST	65536	Allocated
system				2004-08-27 21:16:33 IST	2004-08-27 21:01:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:06 IST	26214	
system.LOG				2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	1024	Allocated

X: 1835 Y: 185

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

ServiceProvider
Session Manager
Setup
StillImage
SystemResources
Terminal Server
TimeZoneInformation
Update
UsbFlags
Video
VirtualDeviceDrivers
Watchdog
Windows
WMI
WOW
CurrentUser
WaitToKillServiceTimeout
SystemStartOptions
Enum
Hardware Profiles

Metadata

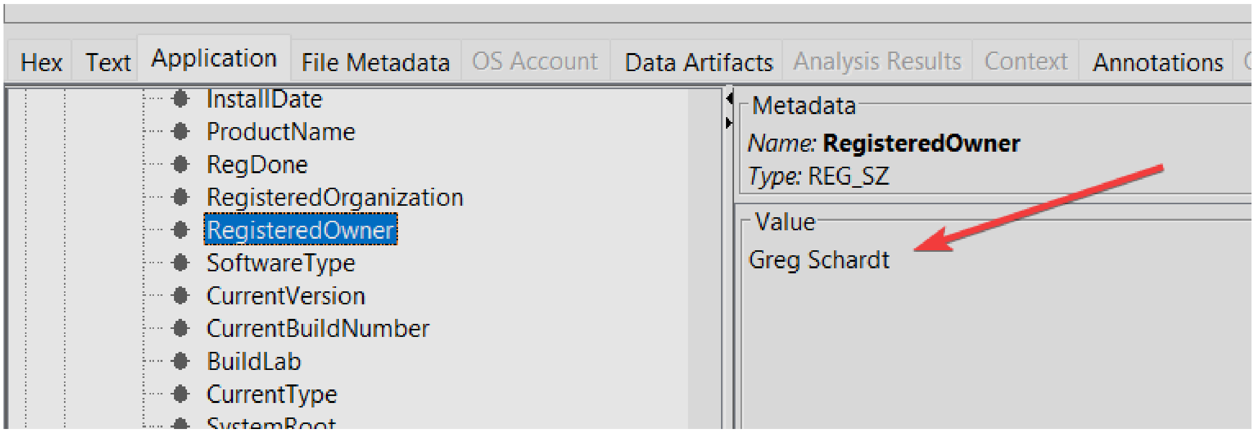
Name: **TimeZoneInformation**
Number of subkeys: 0
Number of values: 8
Modification Time: 2004-08-19 17:20:02 GMT+00:00

Values

Name	Type	Value
Bias	REG_DWOR...	0x00000168 (360)
StandardName	REG_SZ	Central Standard Time
StandardBias	REG_DWOR...	0x00000000 (0)
StandardStart	REG_BIN	00 00 0A 00 05 00 02 00 00 00 00 00 00 00 00 00
DaylightName	REG_SZ	Central Daylight Time
DaylightBias	REG_DWOR...	0xffffffc4 (4294967236)
DaylightStart	REG_BIN	00 00 04 00 01 00 02 00 00 00 00 00 00 00 00 00
ActiveTimeBias	REG_DWOR...	0x0000012c (300)

5. Who is the registered owner?

Ans: Greg Schardt



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

InstallDate
ProductName
RegDone
RegisteredOrganization
RegisteredOwner
SoftwareType
CurrentVersion
CurrentBuildNumber
BuildLab
CurrentType
SystemRoot

Metadata

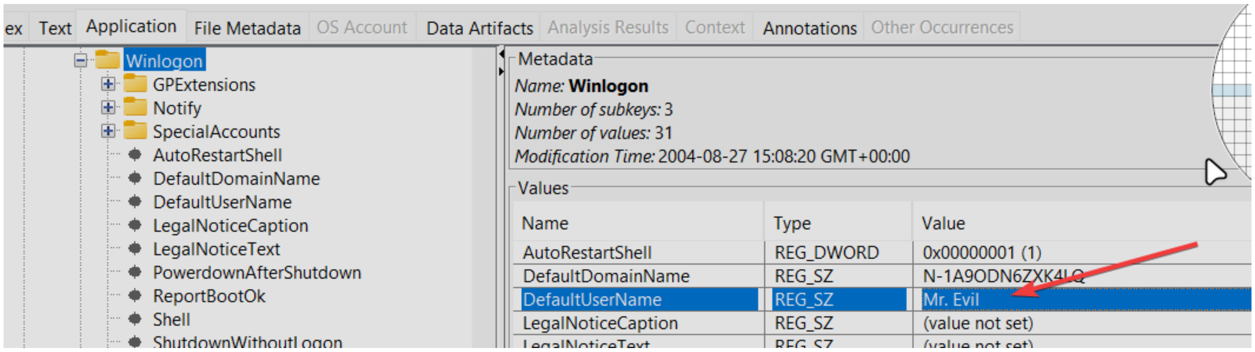
Name: **RegisteredOwner**
Type: REG_SZ

Value

Greg Schardt

6. What is the computer account name?

Ans: Mr. Evil



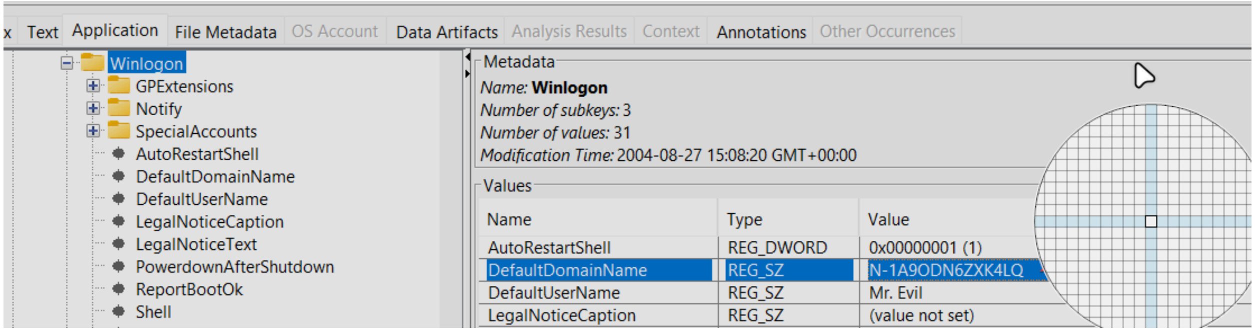
Metadata

Name: **Winlogon**
Number of subkeys: 3
Number of values: 31
Modification Time: 2004-08-27 15:08:20 GMT+00:00

Values

Name	Type	Value
AutoRestartShell	REG_DWORD	0x00000001 (1)
DefaultDomainName	REG_SZ	N-1A9ODN6ZXK4LQ
DefaultUserName	REG_SZ	Mr. Evil
LegalNoticeCaption	REG_SZ	(value not set)
LegalNoticeText	REG_SZ	(value not set)

7. What is the primary domain name?
Ans: N-1A9ODN6ZXK4LQ



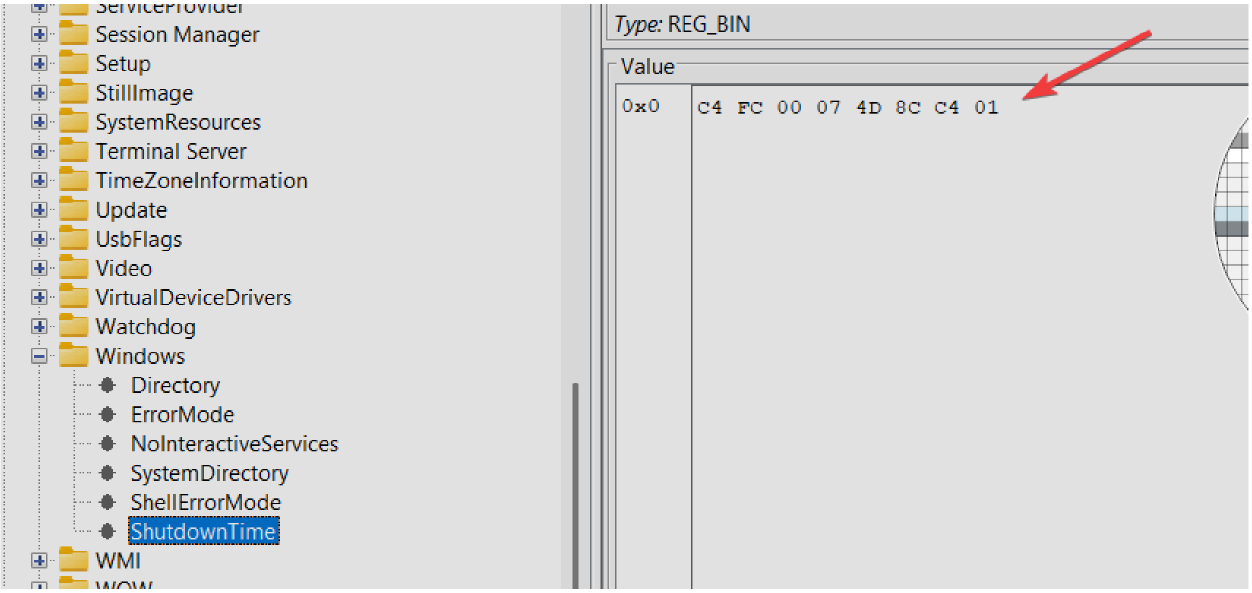
Metadata

Name: **Winlogon**
Number of subkeys: 3
Number of values: 31
Modification Time: 2004-08-27 15:08:20 GMT+00:00

Values

Name	Type	Value
AutoRestartShell	REG_DWORD	0x00000001 (1)
DefaultDomainName	REG_SZ	N-1A9ODN6ZXK4LQ
DefaultUserName	REG_SZ	Mr. Evil
LegalNoticeCaption	REG_SZ	(value not set)

8. When was the last recorded computer shutdown date/time?
Ans: C4 FC 00 07 4D 8C C4 01
Decoded: Friday, 20 August 2004 04:18:27 (UTC)



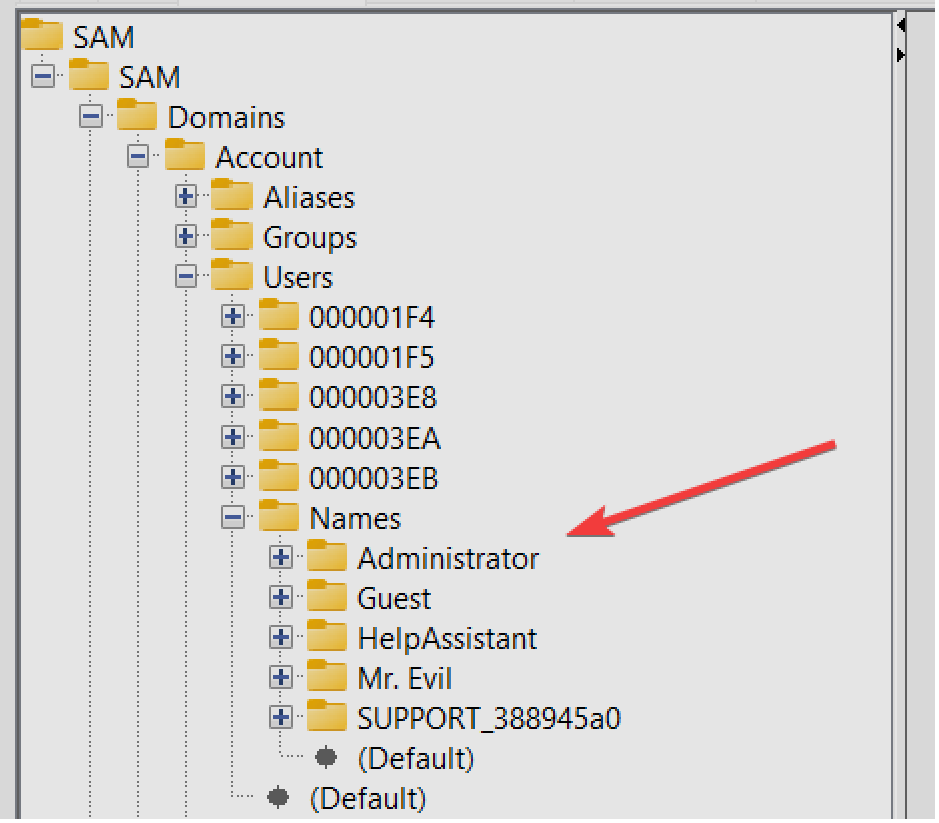
Type: REG_BIN

Value

```
0x0   C4 FC 00 07 4D 8C C4 01
```

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

Ans: 5

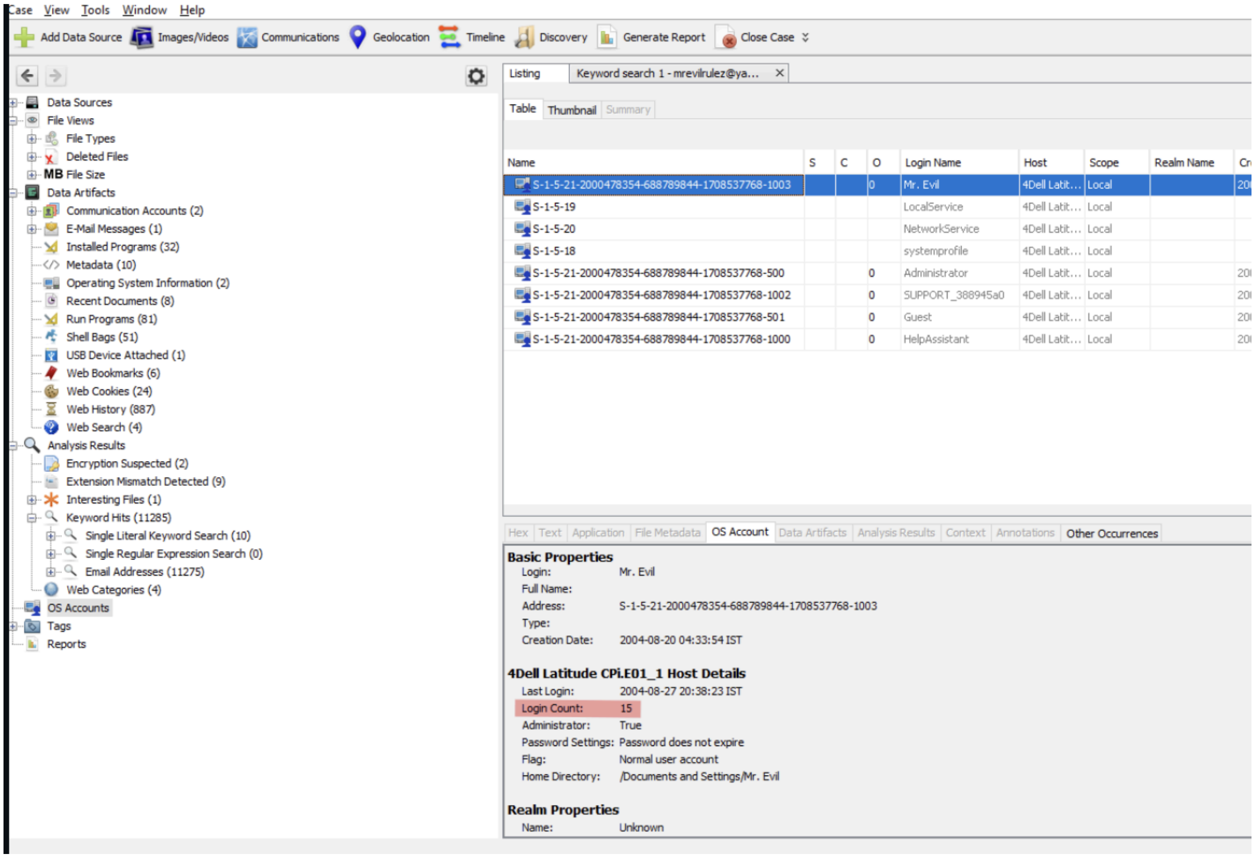


```
SAM
  SAM
    Domains
      Account
        Aliases
        Groups
        Users
          000001F4
          000001F5
          000003E8
          000003EA
          000003EB
          Names
            Administrator
            Guest
            HelpAssistant
            Mr. Evil
            SUPPORT_388945a0
            (Default)
          (Default)
```

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

Ans. Mr. Evil (count 15 times)

This information can be found by going to “OS Accounts” in the left tree structure.



Name	S	C	O	Login Name	Host	Scope	Realm Name	Cr
S-1-5-21-2000478354-688789844-1708537768-1003			0	Mr. Evil	4Dell Latit...	Local		20
S-1-5-19				LocalService	4Dell Latit...	Local		
S-1-5-20				NetworkService	4Dell Latit...	Local		
S-1-5-18				systemprofile	4Dell Latit...	Local		
S-1-5-21-2000478354-688789844-1708537768-500			0	Administrator	4Dell Latit...	Local		20
S-1-5-21-2000478354-688789844-1708537768-1002			0	SUPPORT_388945a0	4Dell Latit...	Local		20
S-1-5-21-2000478354-688789844-1708537768-501			0	Guest	4Dell Latit...	Local		20
S-1-5-21-2000478354-688789844-1708537768-1000			0	HelpAssistant	4Dell Latit...	Local		20

Basic Properties

Login:	Mr. Evil
Full Name:	
Address:	S-1-5-21-2000478354-688789844-1708537768-1003
Type:	
Creation Date:	2004-08-20 04:33:54 IST

4Dell Latitude CPi.E01_1 Host Details

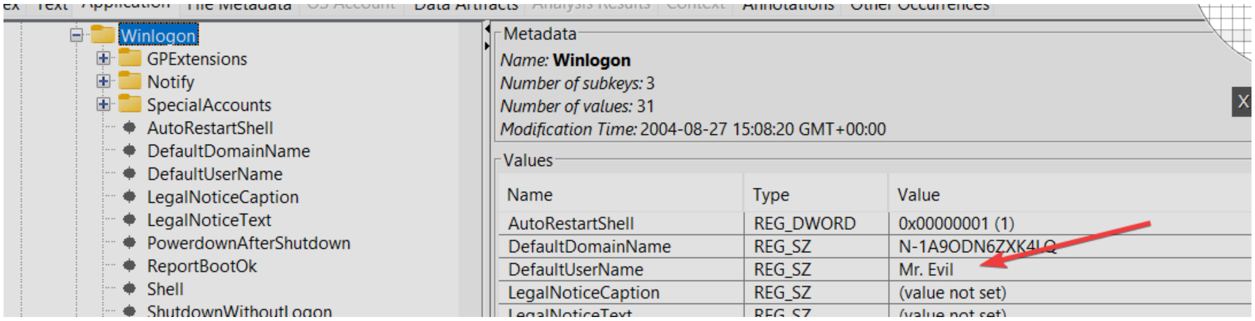
Last Login:	2004-08-27 20:38:23 IST
Login Count:	15
Administrator:	True
Password Settings:	Password does not expire
Flag:	Normal user account
Home Directory:	/Documents and Settings/Mr. Evil

Realm Properties

Name:	Unknown

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

Ans: Mr. Evil



Metadata

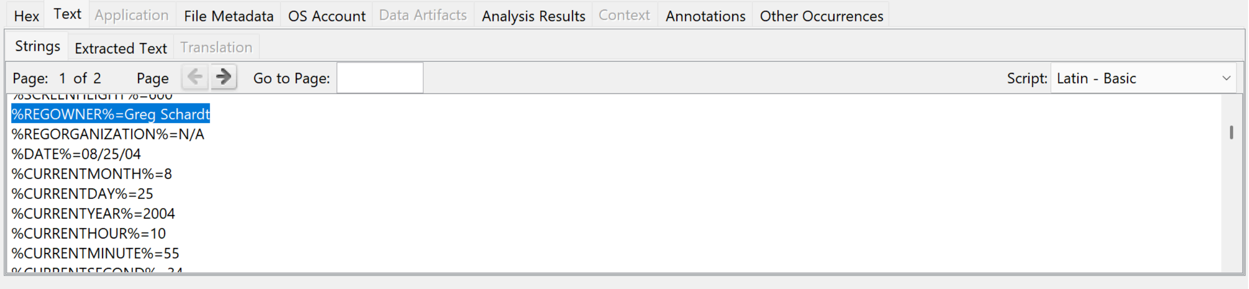
Name: **Winlogon**
Number of subkeys: 3
Number of values: 31
Modification Time: 2004-08-27 15:08:20 GMT+00:00

Values

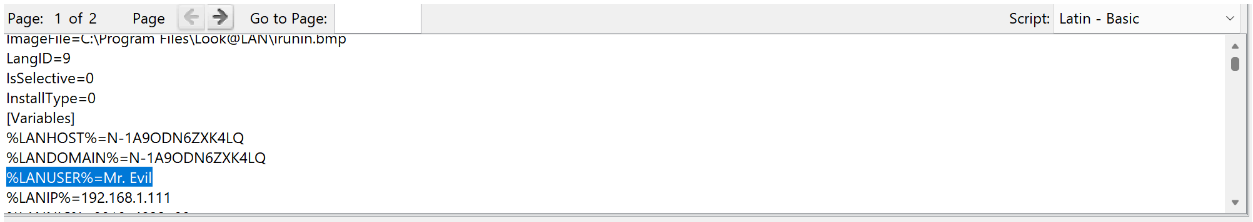
Name	Type	Value
AutoRestartShell	REG_DWORD	0x00000001 (1)
DefaultDomainName	REG_SZ	N-1A9ODN6ZXK4LQ
DefaultUserName	REG_SZ	Mr. Evil
LegalNoticeCaption	REG_SZ	(value not set)
LegalNoticeText	REG_SZ	(value not set)

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?

The file is **`C:\Program Files\Look@LAN\irunin.ini`** — it’s part of the **Look@LAN** LAN-monitoring program (the `irunin.ini` contains entries like `%LANUSER%=Mr. Evil` and `%REGOWNER%=Greg Schardt`).



```
%SCREENHEIGHT%=600
%REGOWNER%=Greg Schardt
%REGORGANIZATION%=N/A
%DATE%=08/25/04
%CURRENTMONTH%=8
%CURRENTDAY%=25
%CURRENTYEAR%=2004
%CURRENTHOUR%=10
%CURRENTMINUTE%=55
%CURRENTSECOND%=34
```



```
ImageFile=C:\Program Files\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
```

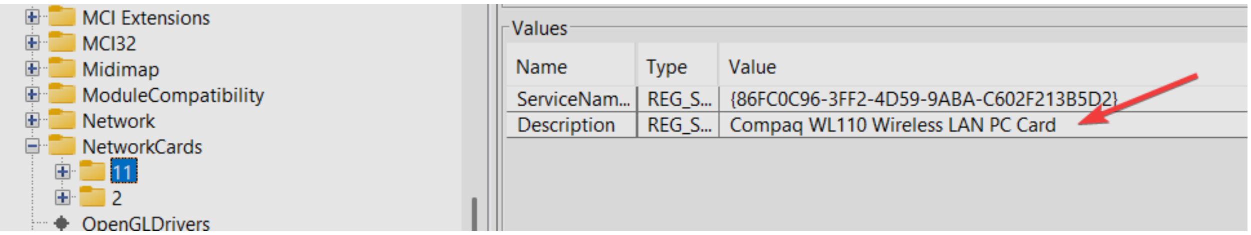
13. List the network cards used by this computer

Ans. There are 2 Network Cards:

First is Compaq WL110 Wireless LAN PC Card

Second is Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)

NOTE:- To find the network card the path is "C:\windows\system32\config\software\Microsoft\Windows NT\CurrentVersion\NetworkCards"



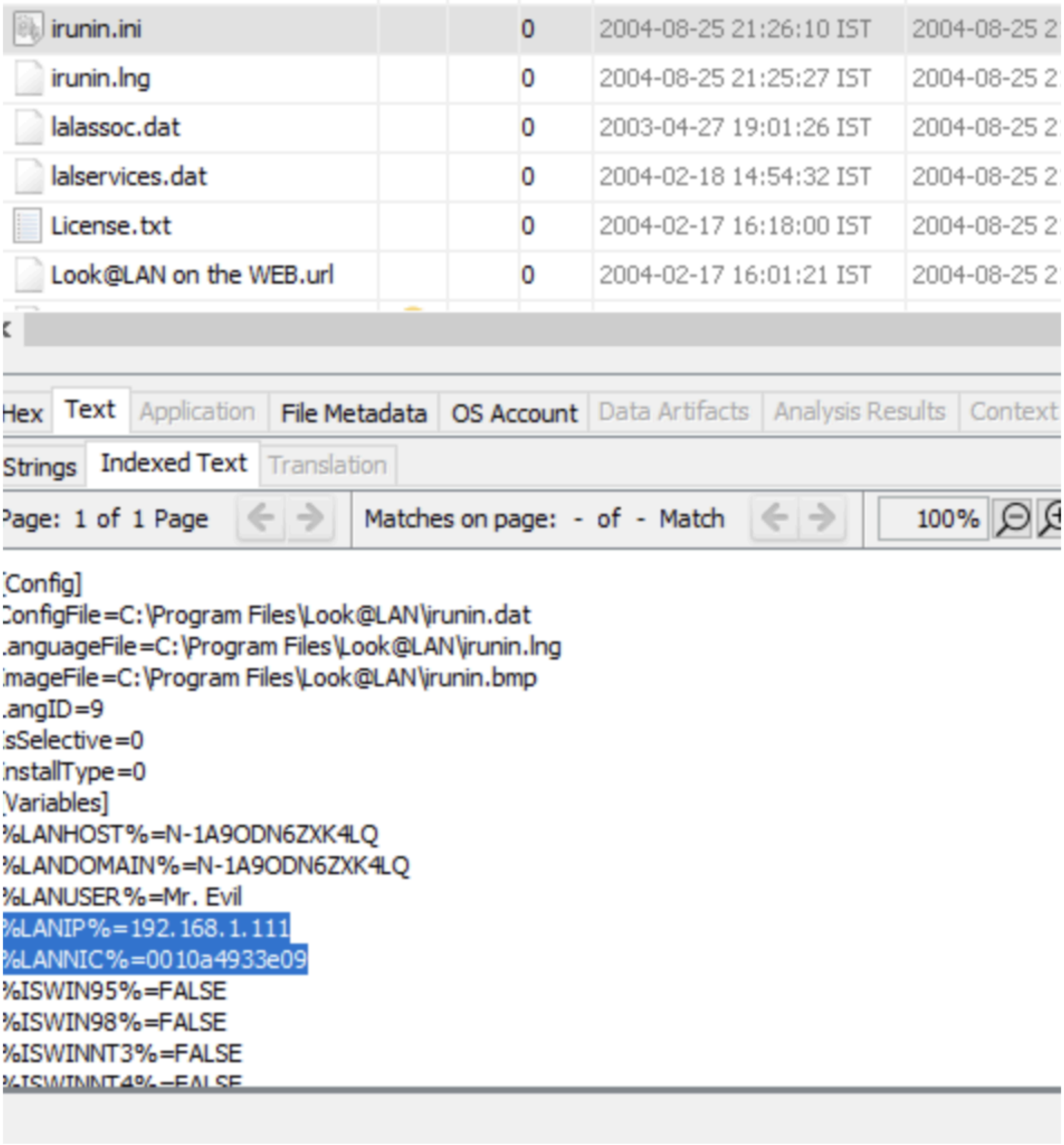
Name	Type	Value
ServiceNam...	REG_S...	{86FC0C96-3FF2-4D59-9ABA-C602F213B5D2}
Description	REG_S...	Compaq WL110 Wireless LAN PC Card

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

Ans. File is "C:\Program Files\Look@LAN\irunin.ini".

IP Address : 192.168.1.111

MAC Address : 00:10:a4:93:3e:09



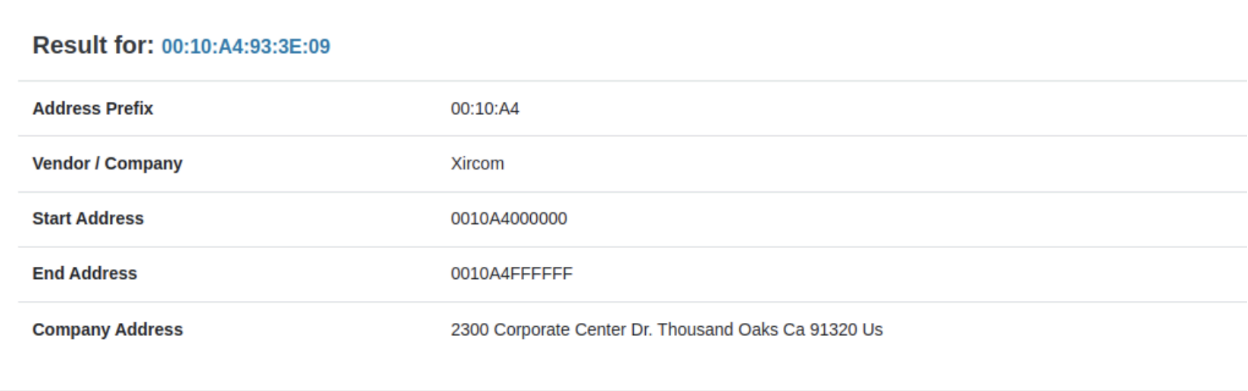
irunin.ini			0	2004-08-25 21:26:10 IST	2004-08-25 2
irunin.lng			0	2004-08-25 21:25:27 IST	2004-08-25 2
lalassoc.dat			0	2003-04-27 19:01:26 IST	2004-08-25 2
lalservices.dat			0	2004-02-18 14:54:32 IST	2004-08-25 2
License.txt			0	2004-02-17 16:18:00 IST	2004-08-25 2
Look@LAN on the WEB.url			0	2004-02-17 16:01:21 IST	2004-08-25 2

```
[Config]
ConfigFile=C:\Program Files\Look@LAN\irunin.dat
LanguageFile=C:\Program Files\Look@LAN\irunin.lng
ImageFile=C:\Program Files\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE
%ISWINNT4%=FALSE
```

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?

Ans. Upon looking on MAC Lookup the company name found was: XIRCOM.

So, the NIC card used for setup the Look@LAN is: Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)



Result for: 00:10:A4:93:3E:09

Address Prefix	00:10:A4
Vendor / Company	Xircom
Start Address	0010A4000000
End Address	0010A4FFFFFF
Company Address	2300 Corporate Center Dr. Thousand Oaks Ca 91320 Us

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

Ans:

a) 123WASP:- Freeware used to get all stored passwords.

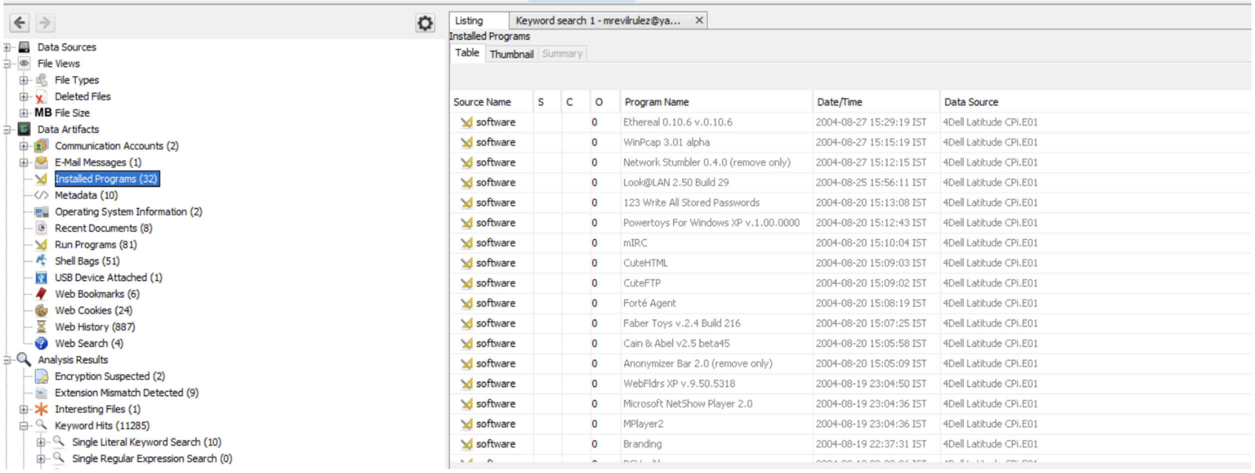
b) Anonymizer:- Tool used to create a proxy.

c) Cain:- Password cracking tool

d) Ethereal:- Packet sniffing tool

e) Look@LAN:- Network monitoring tool

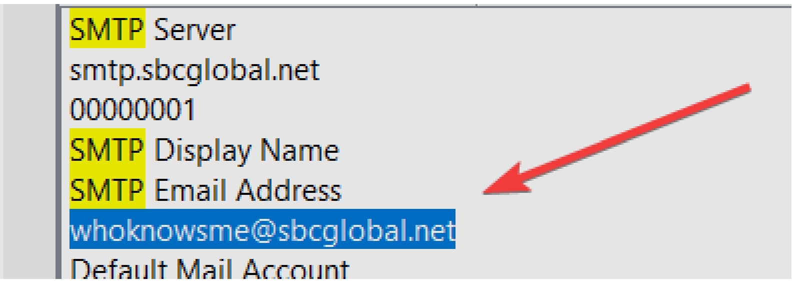
f) NetStumbler:- wireless networking tool to hack wifi password



Installed Programs

Source Name	S	C	O	Program Name	Date/Time	Data Source
software			0	Ethereal 0.10.6 v.0.10.6	2004-08-27 15:29:19 IST	4Dell Latitude CPi.E01
software			0	WinPcap 3.01 alpha	2004-08-27 15:15:19 IST	4Dell Latitude CPi.E01
software			0	Network Stumbler 0.4.0 (remove only)	2004-08-27 15:12:15 IST	4Dell Latitude CPi.E01
software			0	Look@LAN 2.50 Build 29	2004-08-25 15:56:11 IST	4Dell Latitude CPi.E01
software			0	123 Write All Stored Passwords	2004-08-20 15:13:08 IST	4Dell Latitude CPi.E01
software			0	Powertoys For Windows XP v.1.00.0000	2004-08-20 15:12:43 IST	4Dell Latitude CPi.E01
software			0	mIRC	2004-08-20 15:10:04 IST	4Dell Latitude CPi.E01
software			0	CuteHTML	2004-08-20 15:09:03 IST	4Dell Latitude CPi.E01
software			0	CuteFTP	2004-08-20 15:09:02 IST	4Dell Latitude CPi.E01
software			0	Forté Agent	2004-08-20 15:08:19 IST	4Dell Latitude CPi.E01
software			0	Faber Toys v.2.4 Build 216	2004-08-20 15:07:25 IST	4Dell Latitude CPi.E01
software			0	Cain & Abel v2.5 beta45	2004-08-20 15:05:58 IST	4Dell Latitude CPi.E01
software			0	Anonymizer Bar 2.0 (remove only)	2004-08-20 15:05:09 IST	4Dell Latitude CPi.E01
software			0	WebFldrs XP v.9.50.5318	2004-08-19 23:04:50 IST	4Dell Latitude CPi.E01
software			0	Microsoft NetShow Player 2.0	2004-08-19 23:04:36 IST	4Dell Latitude CPi.E01
software			0	MPlayer2	2004-08-19 23:04:36 IST	4Dell Latitude CPi.E01
software			0	Branding	2004-08-19 22:37:31 IST	4Dell Latitude CPi.E01

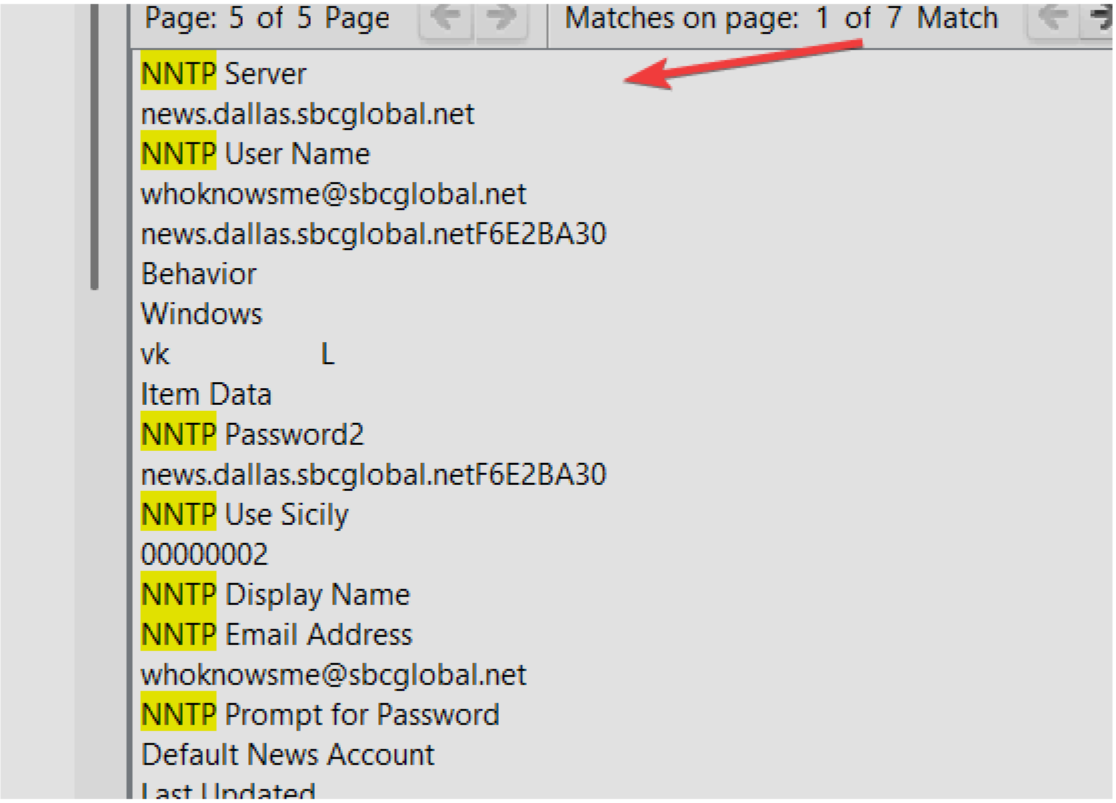
17. What is the SMTP email address for Mr. Evil?



SMTP Server
smtp.sbcglobal.net
00000001
SMTP Display Name
SMTP Email Address
whoknowsme@sbcglobal.net
Default Mail Account

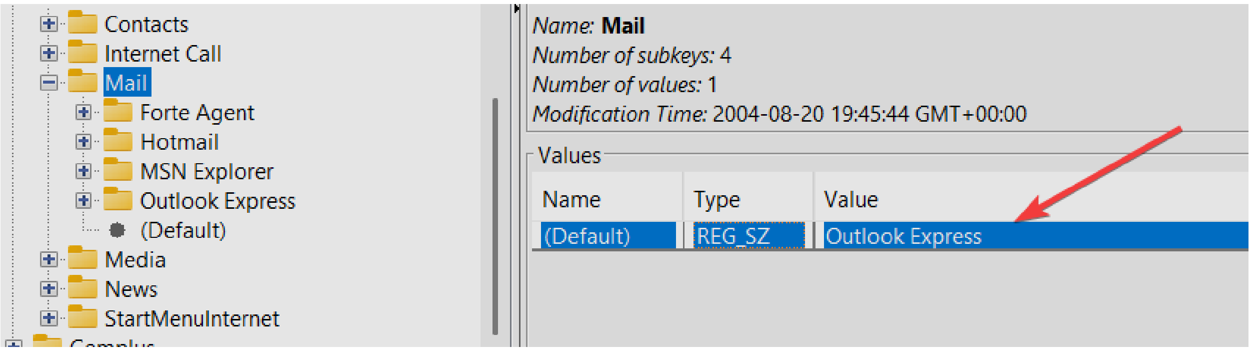
18. What are the NNTP (news server) settings for Mr. Evil?

Ans:
a) server name is “news.dallas.sbcglobal.net”,
b) user name is whoknowsme@sbcglobal.net



```
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
NNTP Use Sicily
00000002
NNTP Display Name
NNTP Email Address
whoknowsme@sbcglobal.net
NNTP Prompt for Password
Default News Account
Last Updated
```

19. What two installed programs show this information?



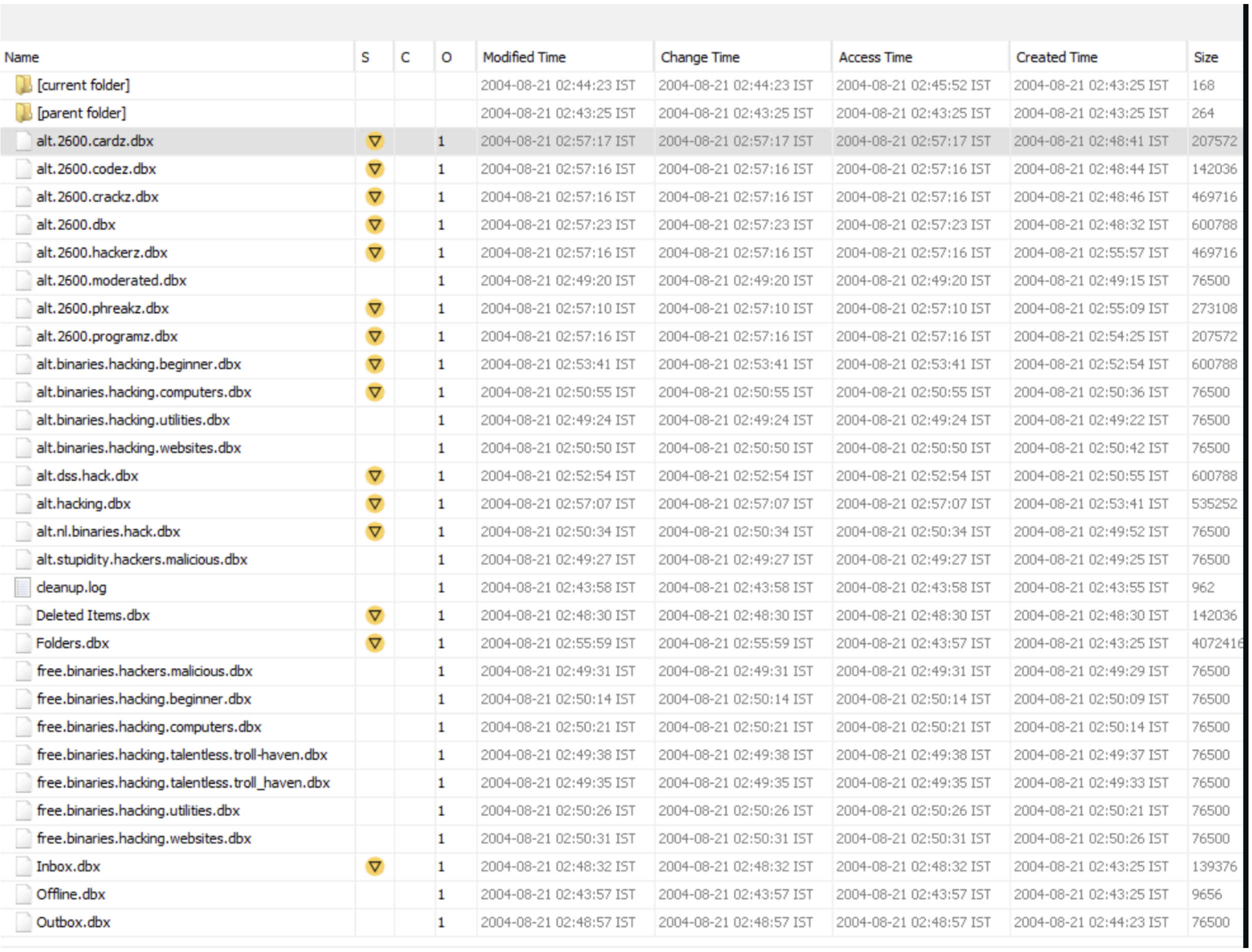
Name: **Mail**
Number of subkeys: 4
Number of values: 1
Modification Time: 2004-08-20 19:45:44 GMT+00:00

Values

Name	Type	Value
(Default)	REG_SZ	Outlook Express

20. List 5 newsgroups that Mr. Evil has subscribed to?
Ans. The answer is in given image.

The newsgroups can be found at the Path: C:\Document and Settings\Mr. Evil\Local Settings\Application Data\Identities\
{EF086998–1115–4ECD-9B13 9ADC067B4929} \Microsoft\Outlook Express

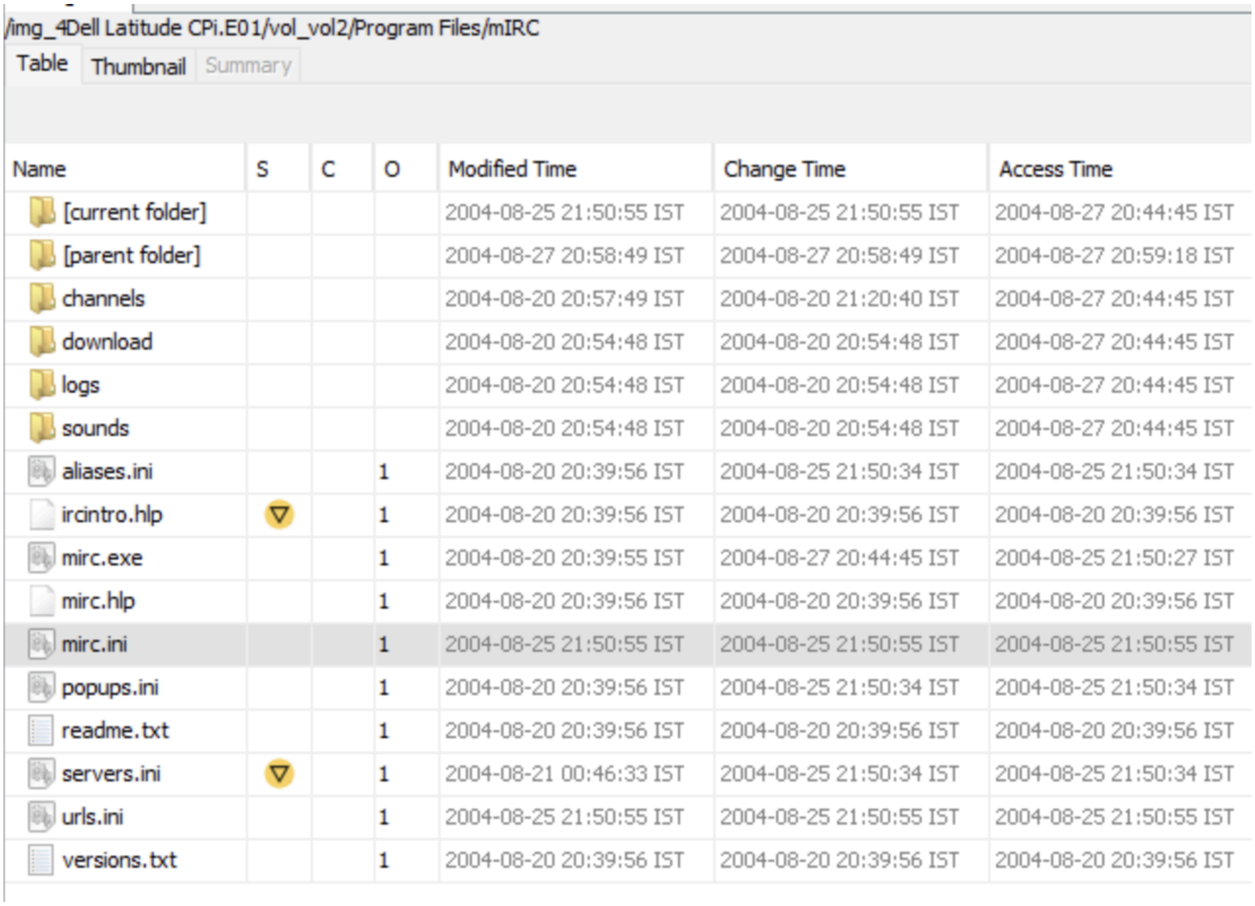


Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2004-08-21 02:44:23 IST	2004-08-21 02:44:23 IST	2004-08-21 02:45:52 IST	2004-08-21 02:43:25 IST	168
[parent folder]				2004-08-21 02:43:25 IST	2004-08-21 02:43:25 IST	2004-08-21 02:43:25 IST	2004-08-21 02:43:25 IST	264
alt.2600.cardz.dbx	▽		1	2004-08-21 02:57:17 IST	2004-08-21 02:57:17 IST	2004-08-21 02:57:17 IST	2004-08-21 02:48:41 IST	207572
alt.2600.codez.dbx	▽		1	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:48:44 IST	142036
alt.2600.crackz.dbx	▽		1	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:48:46 IST	469716
alt.2600.dbx	▽		1	2004-08-21 02:57:23 IST	2004-08-21 02:57:23 IST	2004-08-21 02:57:23 IST	2004-08-21 02:48:32 IST	600788
alt.2600.hackerz.dbx	▽		1	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:55:57 IST	469716
alt.2600.moderated.dbx			1	2004-08-21 02:49:20 IST	2004-08-21 02:49:20 IST	2004-08-21 02:49:20 IST	2004-08-21 02:49:15 IST	76500
alt.2600.phreakz.dbx	▽		1	2004-08-21 02:57:10 IST	2004-08-21 02:57:10 IST	2004-08-21 02:57:10 IST	2004-08-21 02:55:09 IST	273108
alt.2600.programz.dbx	▽		1	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:57:16 IST	2004-08-21 02:54:25 IST	207572
alt.binaries.hacking.beginner.dbx	▽		1	2004-08-21 02:53:41 IST	2004-08-21 02:53:41 IST	2004-08-21 02:53:41 IST	2004-08-21 02:52:54 IST	600788
alt.binaries.hacking.computers.dbx	▽		1	2004-08-21 02:50:55 IST	2004-08-21 02:50:55 IST	2004-08-21 02:50:55 IST	2004-08-21 02:50:36 IST	76500
alt.binaries.hacking.utilities.dbx			1	2004-08-21 02:49:24 IST	2004-08-21 02:49:24 IST	2004-08-21 02:49:24 IST	2004-08-21 02:49:22 IST	76500
alt.binaries.hacking.websites.dbx			1	2004-08-21 02:50:50 IST	2004-08-21 02:50:50 IST	2004-08-21 02:50:50 IST	2004-08-21 02:50:42 IST	76500
alt.dss.hack.dbx	▽		1	2004-08-21 02:52:54 IST	2004-08-21 02:52:54 IST	2004-08-21 02:52:54 IST	2004-08-21 02:50:55 IST	600788
alt.hacking.dbx	▽		1	2004-08-21 02:57:07 IST	2004-08-21 02:57:07 IST	2004-08-21 02:57:07 IST	2004-08-21 02:53:41 IST	535252
alt.nl.binaries.hack.dbx	▽		1	2004-08-21 02:50:34 IST	2004-08-21 02:50:34 IST	2004-08-21 02:50:34 IST	2004-08-21 02:49:52 IST	76500
alt.stupidity.hackers.malicious.dbx			1	2004-08-21 02:49:27 IST	2004-08-21 02:49:27 IST	2004-08-21 02:49:27 IST	2004-08-21 02:49:25 IST	76500
cleanup.log			1	2004-08-21 02:43:58 IST	2004-08-21 02:43:58 IST	2004-08-21 02:43:58 IST	2004-08-21 02:43:55 IST	962
Deleted Items.dbx	▽		1	2004-08-21 02:48:30 IST	2004-08-21 02:48:30 IST	2004-08-21 02:48:30 IST	2004-08-21 02:48:30 IST	142036
Folders.dbx	▽		1	2004-08-21 02:55:59 IST	2004-08-21 02:55:59 IST	2004-08-21 02:43:57 IST	2004-08-21 02:43:25 IST	4072416
free.binaries.hackers.malicious.dbx			1	2004-08-21 02:49:31 IST	2004-08-21 02:49:31 IST	2004-08-21 02:49:31 IST	2004-08-21 02:49:29 IST	76500
free.binaries.hacking.beginner.dbx			1	2004-08-21 02:50:14 IST	2004-08-21 02:50:14 IST	2004-08-21 02:50:14 IST	2004-08-21 02:50:09 IST	76500
free.binaries.hacking.computers.dbx			1	2004-08-21 02:50:21 IST	2004-08-21 02:50:21 IST	2004-08-21 02:50:21 IST	2004-08-21 02:50:14 IST	76500
free.binaries.hacking.talentless.troll-haven.dbx			1	2004-08-21 02:49:38 IST	2004-08-21 02:49:38 IST	2004-08-21 02:49:38 IST	2004-08-21 02:49:37 IST	76500
free.binaries.hacking.talentless.troll_haven.dbx			1	2004-08-21 02:49:35 IST	2004-08-21 02:49:35 IST	2004-08-21 02:49:35 IST	2004-08-21 02:49:33 IST	76500
free.binaries.hacking.utilities.dbx			1	2004-08-21 02:50:26 IST	2004-08-21 02:50:26 IST	2004-08-21 02:50:26 IST	2004-08-21 02:50:21 IST	76500
free.binaries.hacking.websites.dbx			1	2004-08-21 02:50:31 IST	2004-08-21 02:50:31 IST	2004-08-21 02:50:31 IST	2004-08-21 02:50:26 IST	76500
Inbox.dbx	▽		1	2004-08-21 02:48:32 IST	2004-08-21 02:48:32 IST	2004-08-21 02:48:32 IST	2004-08-21 02:43:25 IST	139376
Offline.dbx			1	2004-08-21 02:43:57 IST	2004-08-21 02:43:57 IST	2004-08-21 02:43:57 IST	2004-08-21 02:43:25 IST	9656
Outbox.dbx			1	2004-08-21 02:48:57 IST	2004-08-21 02:48:57 IST	2004-08-21 02:48:57 IST	2004-08-21 02:44:23 IST	76500

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?

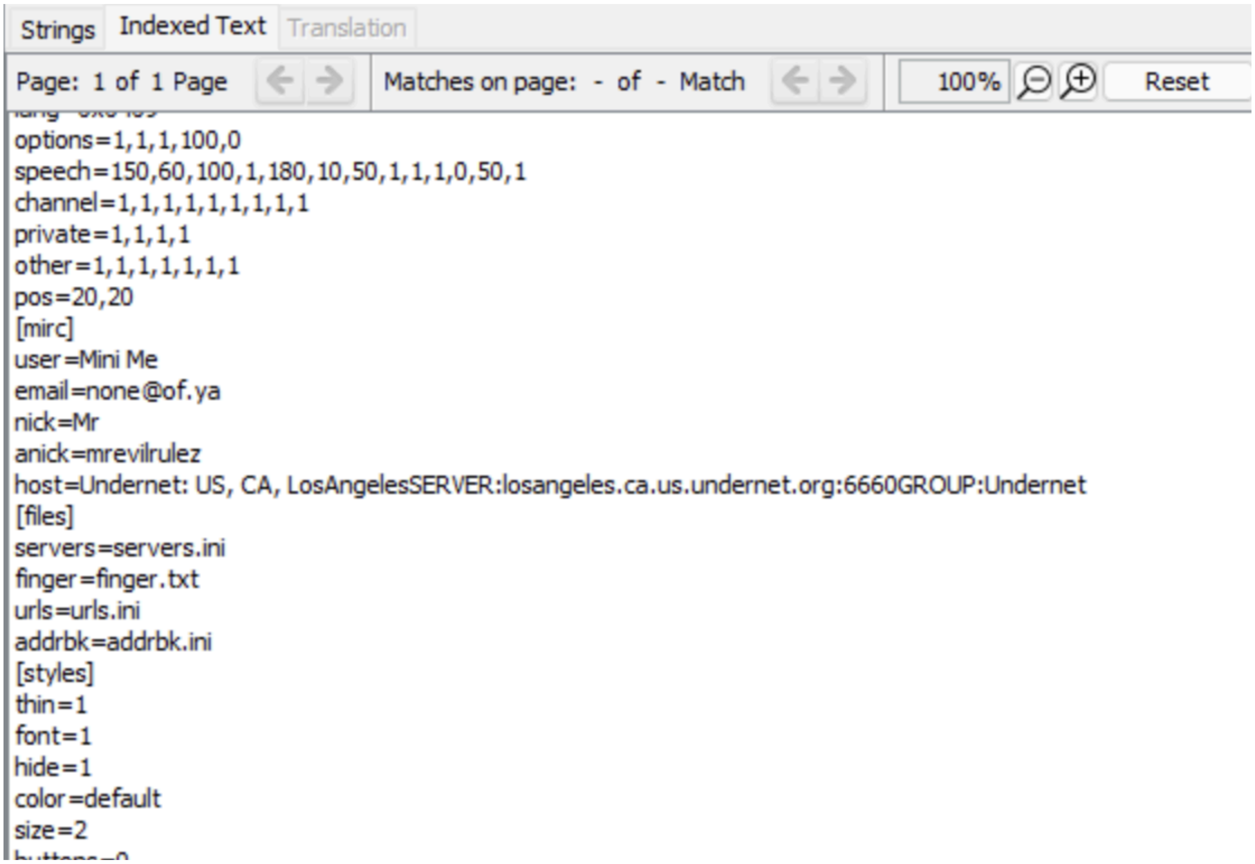
Ans. User = Mini Me
Email = none@of.ya
nick = Mr
anick = mrevilrulez
host = Undernet: US, CA, LosAngelesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet

Can be found at Path: C:\Program Files\mIRC\mirc.ini



/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/mIRC

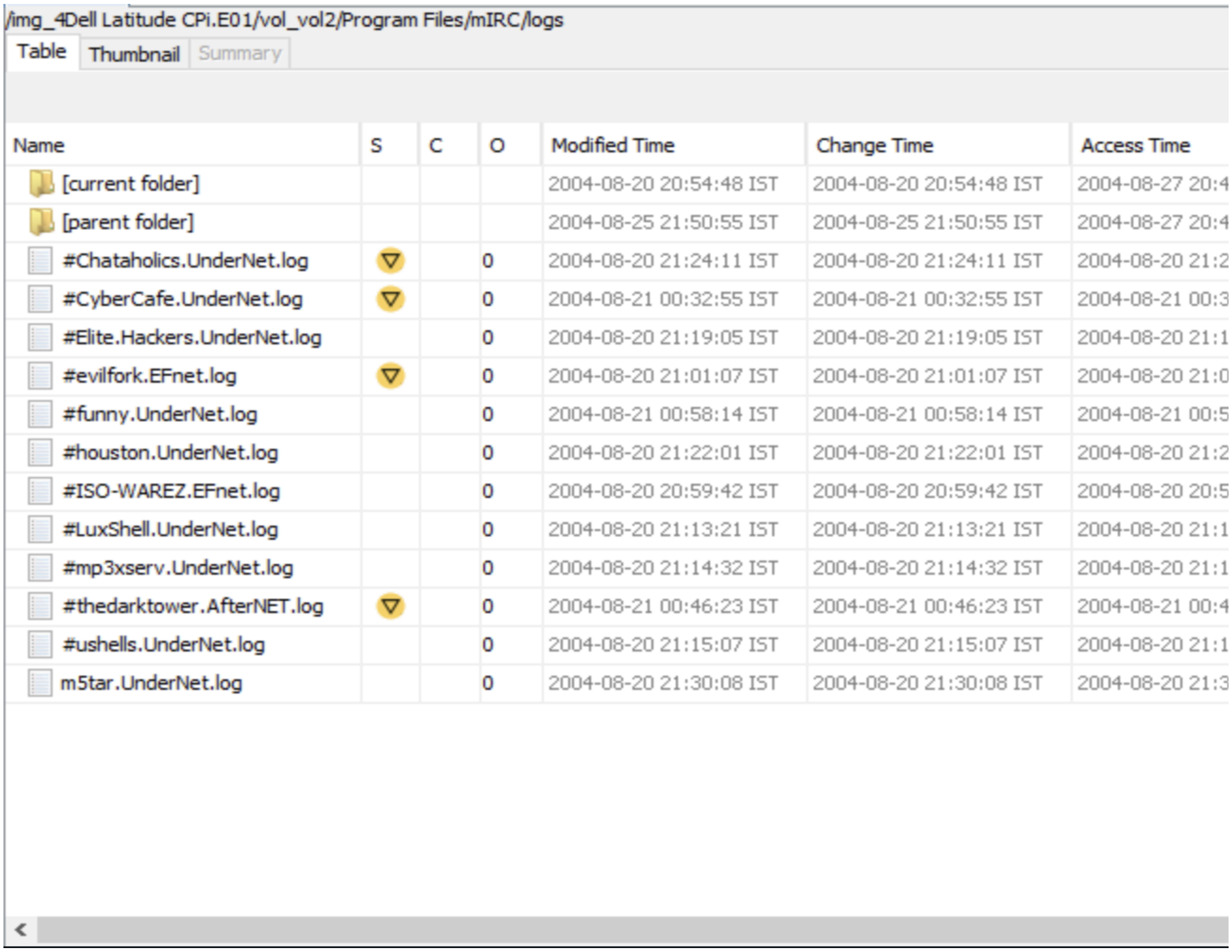
Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-27 20:44:45 IST
[parent folder]				2004-08-27 20:58:49 IST	2004-08-27 20:58:49 IST	2004-08-27 20:59:18 IST
channels				2004-08-20 20:57:49 IST	2004-08-20 21:20:40 IST	2004-08-27 20:44:45 IST
download				2004-08-20 20:54:48 IST	2004-08-20 20:54:48 IST	2004-08-27 20:44:45 IST
logs				2004-08-20 20:54:48 IST	2004-08-20 20:54:48 IST	2004-08-27 20:44:45 IST
sounds				2004-08-20 20:54:48 IST	2004-08-20 20:54:48 IST	2004-08-27 20:44:45 IST
aliases.ini			1	2004-08-20 20:39:56 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST
ircintro.hlp	▽		1	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST
mirc.exe			1	2004-08-20 20:39:55 IST	2004-08-27 20:44:45 IST	2004-08-25 21:50:27 IST
mirc.hlp			1	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST
mirc.ini			1	2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST
popups.ini			1	2004-08-20 20:39:56 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST
readme.txt			1	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST
servers.ini	▽		1	2004-08-21 00:46:33 IST	2004-08-25 21:50:34 IST	2004-08-25 21:50:34 IST
urls.ini			1	2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST
versions.txt			1	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST	2004-08-20 20:39:56 IST



```
options=1,1,1,100,0
speech=150,60,100,1,180,10,50,1,1,1,0,50,1
channel=1,1,1,1,1,1,1,1
private=1,1,1,1
other=1,1,1,1,1,1,1
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
finger=finger.txt
urls=urls.ini
addrbk=addrbk.ini
[styles]
thin=1
font=1
hide=1
color=default
size=2
```

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

Ans. To view the logs, we have to go inside the logs directory of mIRC. The channels that the user has accessed is given in below picture.



/img_4Dell Latitude CPi.E01/vol_vol2/Program Files/mIRC/logs

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2004-08-20 20:54:48 IST	2004-08-20 20:54:48 IST	2004-08-27 20:4
[parent folder]				2004-08-25 21:50:55 IST	2004-08-25 21:50:55 IST	2004-08-27 20:4
#Chataholics.UnderNet.log	▽		0	2004-08-20 21:24:11 IST	2004-08-20 21:24:11 IST	2004-08-20 21:2
#CyberCafe.UnderNet.log	▽		0	2004-08-21 00:32:55 IST	2004-08-21 00:32:55 IST	2004-08-21 00:3
#Elite.Hackers.UnderNet.log			0	2004-08-20 21:19:05 IST	2004-08-20 21:19:05 IST	2004-08-20 21:1
#evilfork.EFnet.log	▽		0	2004-08-20 21:01:07 IST	2004-08-20 21:01:07 IST	2004-08-20 21:0
#funny.UnderNet.log			0	2004-08-21 00:58:14 IST	2004-08-21 00:58:14 IST	2004-08-21 00:5
#houston.UnderNet.log			0	2004-08-20 21:22:01 IST	2004-08-20 21:22:01 IST	2004-08-20 21:2
#ISO-WAREZ.EFnet.log			0	2004-08-20 20:59:42 IST	2004-08-20 20:59:42 IST	2004-08-20 20:5
#LuxShell.UnderNet.log			0	2004-08-20 21:13:21 IST	2004-08-20 21:13:21 IST	2004-08-20 21:1
#mp3xserv.UnderNet.log			0	2004-08-20 21:14:32 IST	2004-08-20 21:14:32 IST	2004-08-20 21:1
#thedarktower.AfterNET.log	▽		0	2004-08-21 00:46:23 IST	2004-08-21 00:46:23 IST	2004-08-21 00:4
#ushells.UnderNet.log			0	2004-08-20 21:15:07 IST	2004-08-20 21:15:07 IST	2004-08-20 21:1
m5tar.UnderNet.log			0	2004-08-20 21:30:08 IST	2004-08-20 21:30:08 IST	2004-08-20 21:3

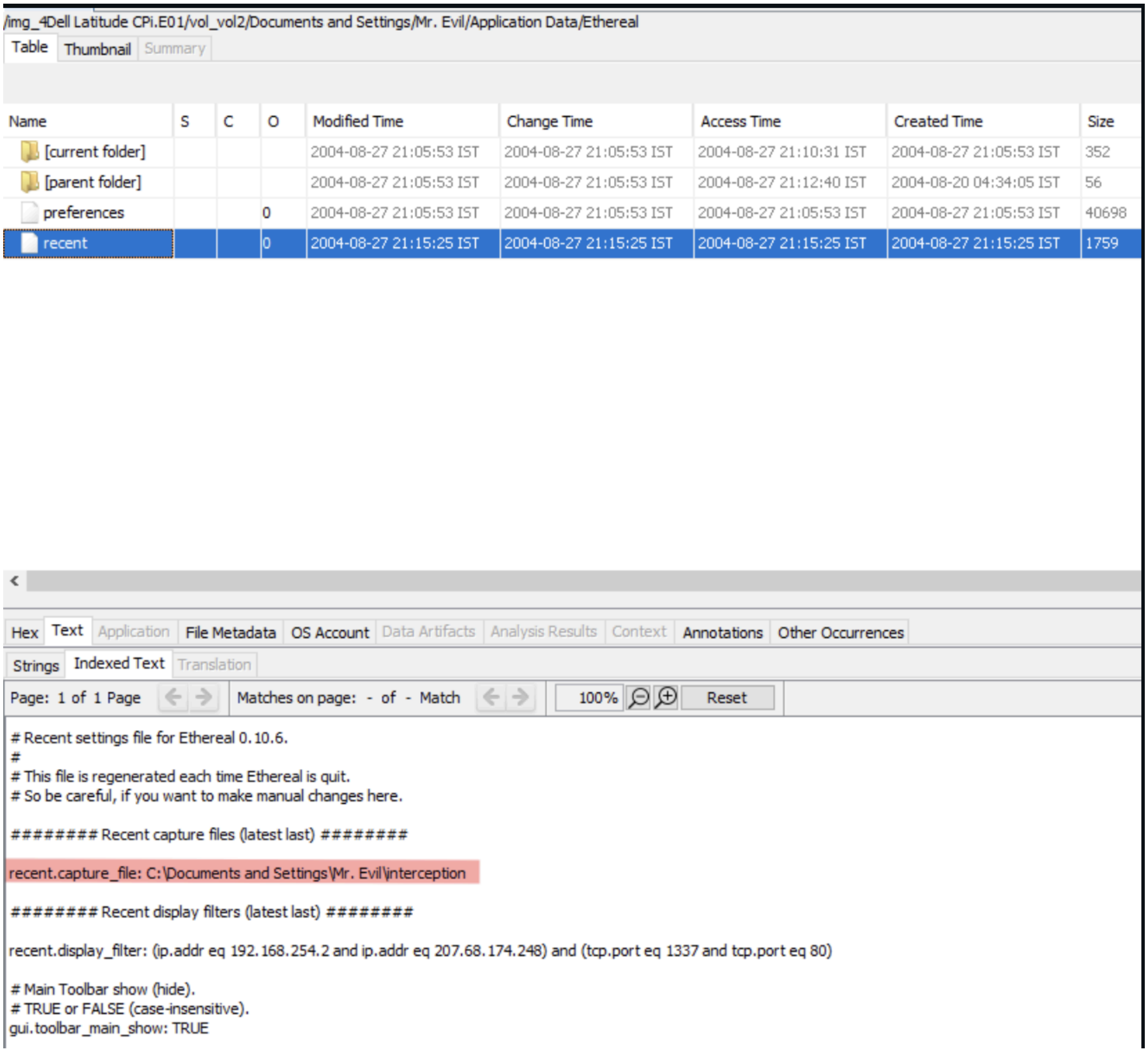
Path is: C:\Program Files\mIRC\logs

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?

Ans. To find the file, we can look to the application data of the Ethereal. The file name is "recent".

Upon looking we can see that the recent capture is "interception".
recent.capture_file: C:\Documents and Settings\Mr. Evil\interception

The path to find the file is : C:\Documents and Settings\Mr. Evil\Application Data\Ethereal\recent



/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settings/Mr. Evil/Application Data/Ethereal

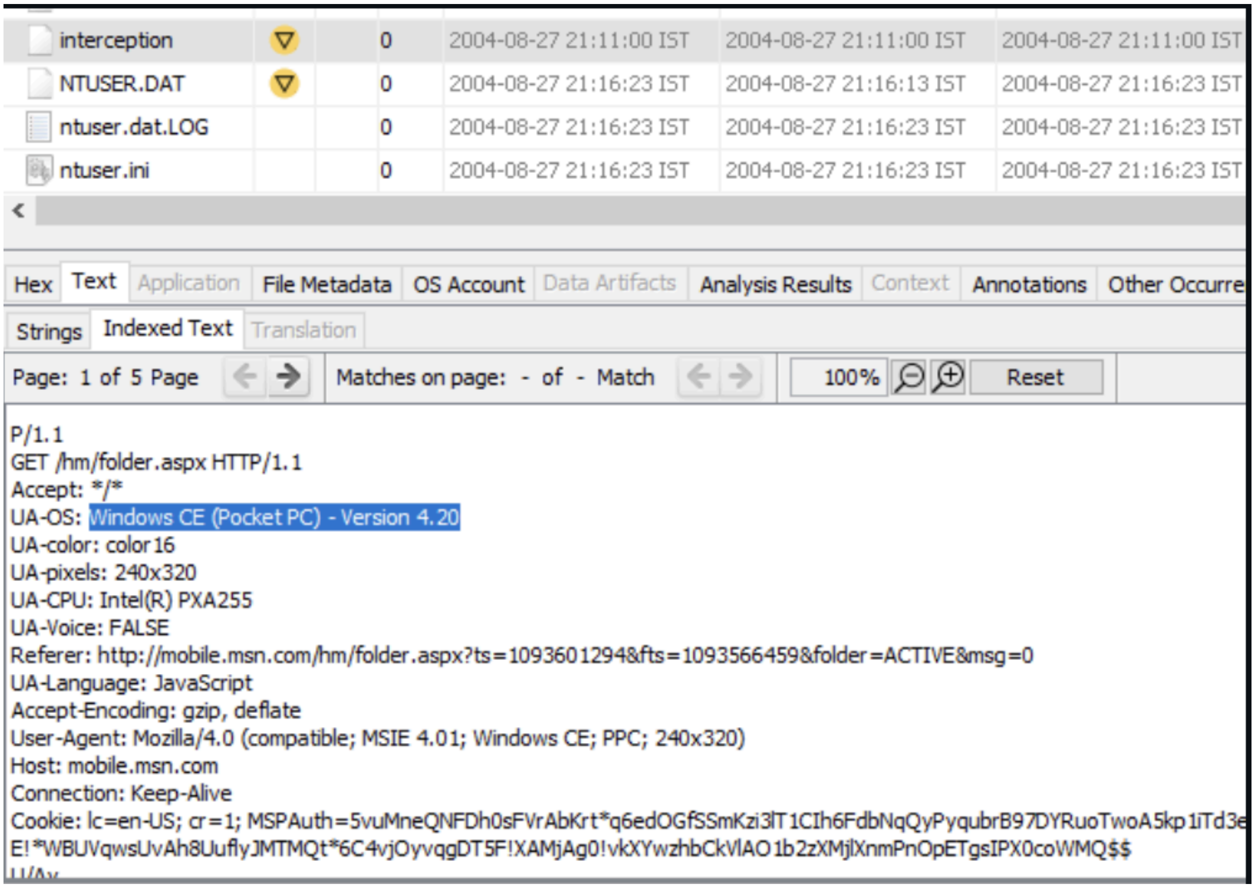
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	2004-08-27 21:10:31 IST	2004-08-27 21:05:53 IST	352
[parent folder]				2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	2004-08-27 21:12:40 IST	2004-08-20 04:34:05 IST	56
preferences			0	2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	40698
recent			0	2004-08-27 21:15:25 IST	2004-08-27 21:15:25 IST	2004-08-27 21:15:25 IST	2004-08-27 21:15:25 IST	1759

```
# 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).
gui.toolbar_main_show: TRUE
```

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?

Ans. To get this data we have look into the file which contains intercepted data which is at "C:\Documents and Settings\Mr. Evil\interception".

The wireless computer used by the victim is: Windows CE (Pocket PC) - Version 4.20



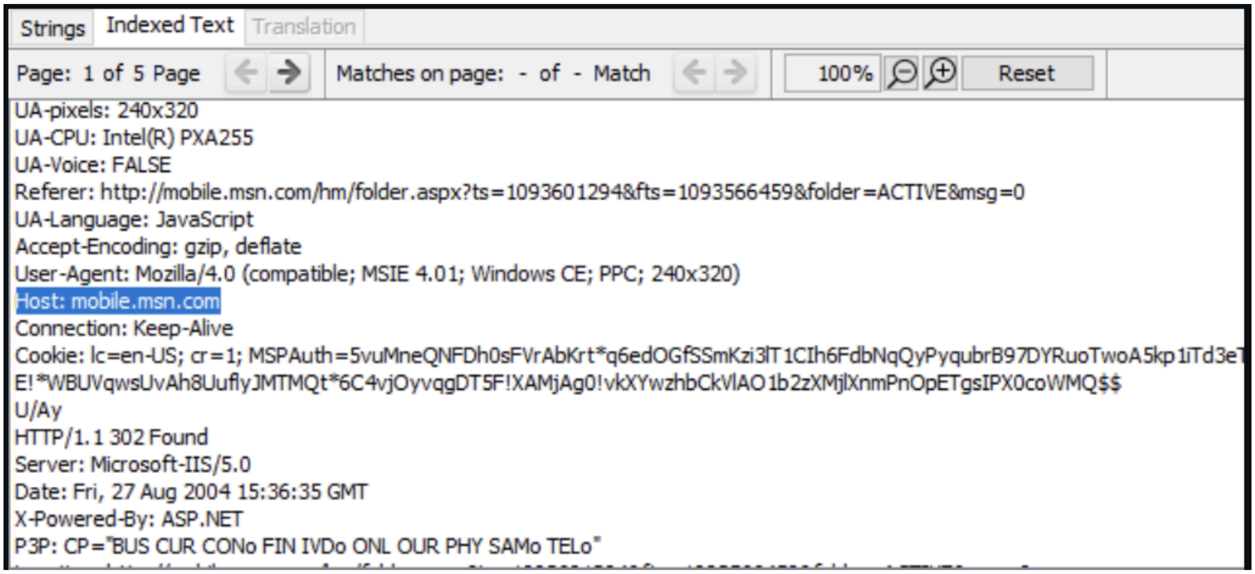
interception	▽	0	2004-08-27 21:11:00 IST	2004-08-27 21:11:00 IST	2004-08-27 21:11:00 IST
NTUSER.DAT	▽	0	2004-08-27 21:16:23 IST	2004-08-27 21:16:13 IST	2004-08-27 21:16:23 IST
ntuser.dat.LOG		0	2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST
ntuser.ini		0	2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST	2004-08-27 21:16:23 IST

```
P/1.1
GET /hm/folder.aspx 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
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*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kp1iTd3e
E!*WBUVqwsUvAh8UuflyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!vkXYwzhbCkVlAO1b2zXMjlXnmPnOpETgsIPX0coWMQ$$
U/Av
```

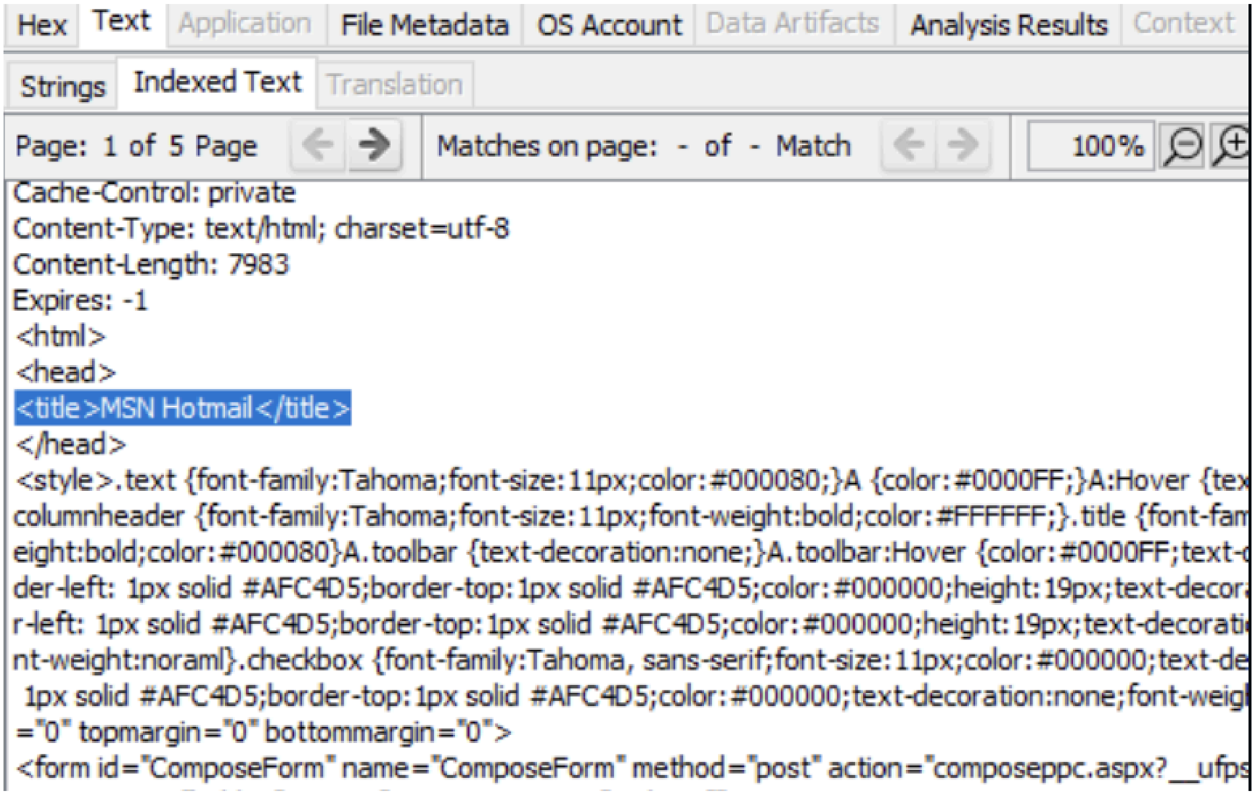
25. What websites was the victim accessing?

Ans. Upon checking the file "interception", the website accessed by user is :

mobile.msn.com, MSN Hotmail Email



```
UA-pixels: 240x320
UA-CPU: Intel(R) PXA255
UA-Voice: FALSE
Referer: http://mobile.msn.com/hm/folder.aspx?ts=109360 1294&fts=1093566459&folder=ACTIVE&msg=0
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*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kp1iTd3eT
E!*WBUVqwsUvAh8UuflyJMTMQt*6C4vjOyvqgDT5F!XAMjAg0!vkXYwzhbCkVlAO1b2zXMjlXnmPnOpETgsIPX0coWMQ$$
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
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
```



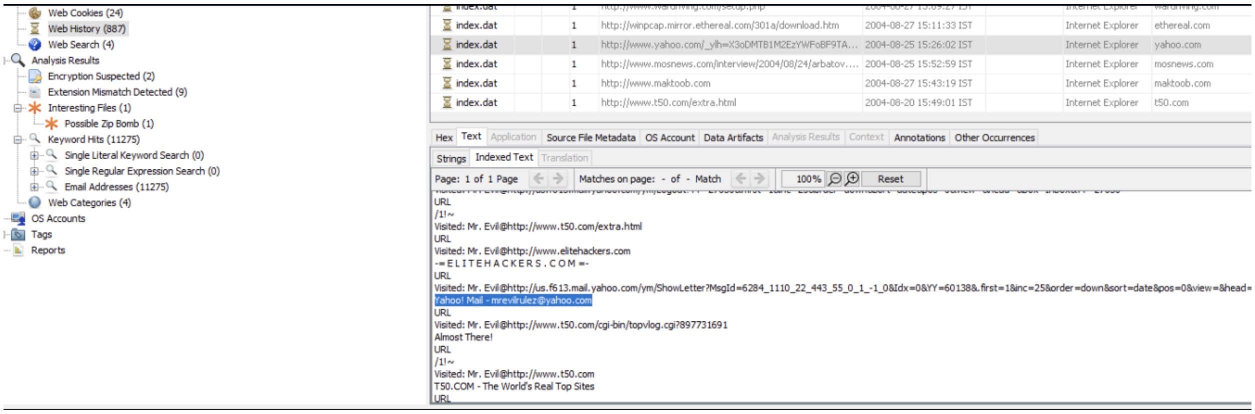
```
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 7983
Expires: -1
<html>
<head>
<title>MSN Hotmail</title>
</head>
<style>.text {font-family:Tahoma;font-size:11px;color:#000080;}A {color:#0000FF;}A:Hover {tex
columnheader {font-family:Tahoma;font-size:11px;font-weight:bold;color:#FFFFFF;}.title {font-fam
eight:bold;color:#000080}A.toolbar {text-decoration:none;}A.toolbar:Hover {color:#0000FF;text-
der-left: 1px solid #AFC4D5;border-top:1px solid #AFC4D5;color:#000000;height:19px;text-decor
r-left: 1px solid #AFC4D5;border-top:1px solid #AFC4D5;color:#000000;height:19px;text-decorati
nt-weight:noraml}.checkbox {font-family:Tahoma, sans-serif;font-size:11px;color:#000000;text-de
 1px solid #AFC4D5;border-top:1px solid #AFC4D5;color:#000000;text-decoration:none;font-weig
="0" topmargin="0" bottommargin="0">
<form id="ComposeForm" name="ComposeForm" method="post" action="composeppc.aspx?__ufps
```

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

Ans. For this, I search in the Web History which is present in Extracted Content.

After searching through all the files, I found a file in which I found that the user has a login to some FTP service using his email id.

Yahoo! Mail - mrevilrulez@yahoo.com



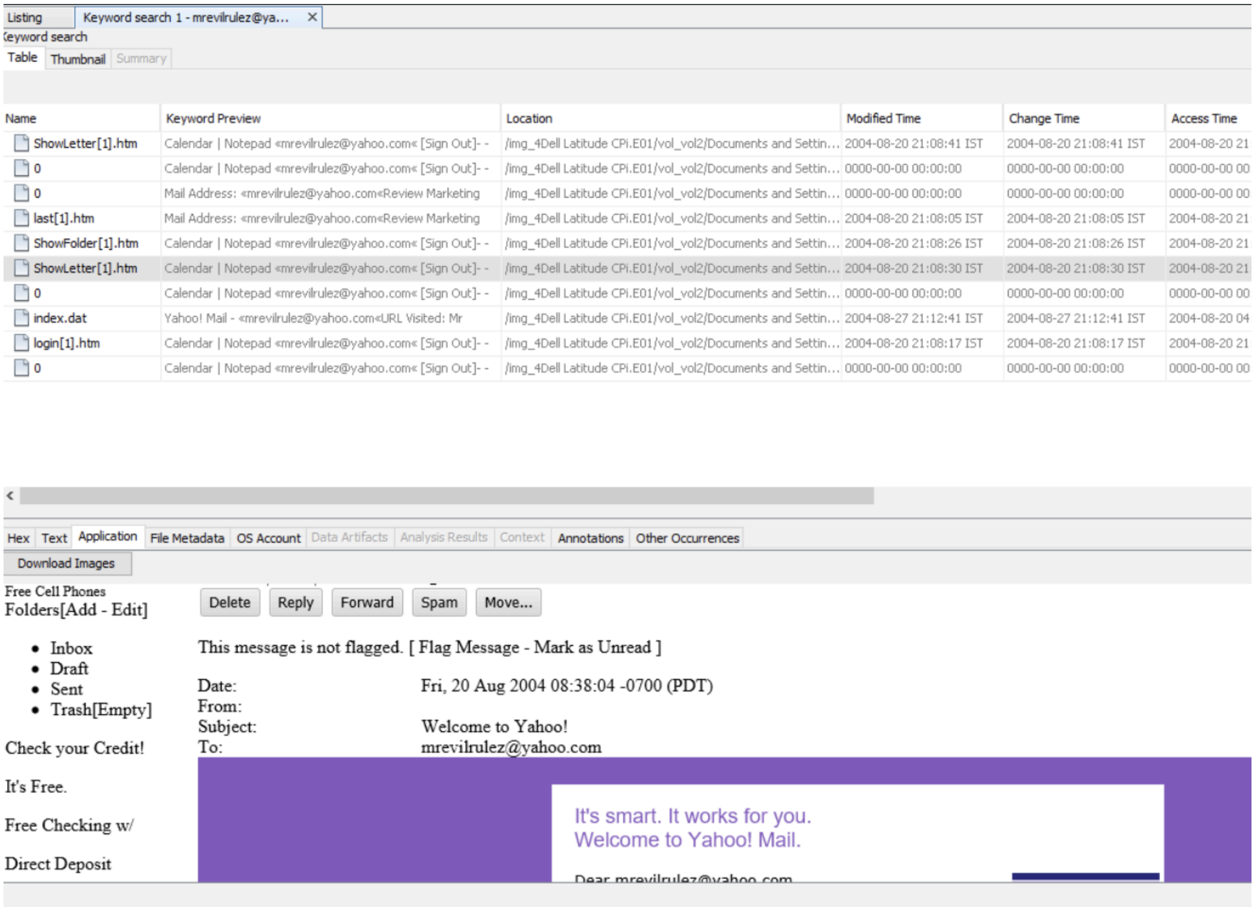
index.dat	1	http://www.wardriving.com/setup.php	2004-08-27 15:09:27 IST	Internet Explorer	wardriving.com
index.dat	1	http://winpcap.mirror.ethereal.com/301a/download.htm	2004-08-27 15:11:33 IST	Internet Explorer	ethereal.com
index.dat	1	http://www.yahoo.com/_ylh=X3oDMTB1M2EzYWFoBF9TA...	2004-08-25 15:26:02 IST	Internet Explorer	yahoo.com
index.dat	1	http://www.mosnews.com/interview/2004/08/24/arbatov....	2004-08-25 15:52:59 IST	Internet Explorer	mosnews.com
index.dat	1	http://www.maktoob.com	2004-08-27 15:43:19 IST	Internet Explorer	maktoob.com
index.dat	1	http://www.t50.com/extra.html	2004-08-20 15:49:01 IST	Internet Explorer	t50.com

```
URL
/1!~
Visited: Mr. Evil@http://www.t50.com/extra.html
URL
Visited: Mr. Evil@http://www.elitehackers.com
-=ELITEHACKERS.COM=-
URL
Visited: Mr. Evil@http://us.f613.mail.yahoo.com/ym/ShowLetter?MsgId=6284_1110_22_443_55_0_1_-1_0&Idx=0&YY=60138&.first=1&inc=25&order=down&sort=date&pos=0&view=&head=
Yahoo! Mail - mrevilrulez@yahoo.com
URL
Visited: Mr. Evil@http://www.t50.com/cgi-bin/topvlog.cgi?897731691
Almost There!
URL
/1!~
Visited: Mr. Evil@http://www.t50.com
T50.COM - The World's Real Top Sites
URL
```

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

Ans. To find the file name, I did the keyword search.

The file found is : ShowLetter[1].htm



Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
ShowLetter[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 21:08:41 IST	2004-08-20 21:08:41 IST	2004-08-20 21
0	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
0	Mail Address: «mrevilrulez@yahoo.com«Review Marketing	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
last[1].htm	Mail Address: «mrevilrulez@yahoo.com«Review Marketing	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 21:08:05 IST	2004-08-20 21:08:05 IST	2004-08-20 21
ShowFolder[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 21:08:26 IST	2004-08-20 21:08:26 IST	2004-08-20 21
ShowLetter[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 21:08:30 IST	2004-08-20 21:08:30 IST	2004-08-20 21
0	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
index.dat	Yahoo! Mail - «mrevilrulez@yahoo.com«URL Visited: Mr	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-27 21:12:41 IST	2004-08-27 21:12:41 IST	2004-08-20 04
login[1].htm	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	2004-08-20 21:08:17 IST	2004-08-20 21:08:17 IST	2004-08-20 21
0	Calendar | Notepad «mrevilrulez@yahoo.com« [Sign Out]- -	/img_4Dell Latitude CPi.E01/vol_vol2/Documents and Settin...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00

Free Cell Phones
Folders[Add - Edit]

- Inbox
- Draft
- Sent
- Trash[Empty]

Check your Credit!

It's Free.

Free Checking w/

Direct Deposit

This message is not flagged. [Flag Message - Mark as Unread]

Date: Fri, 20 Aug 2004 08:38:04 -0700 (PDT)
From:
Subject: Welcome to Yahoo!
To: mrevilrulez@yahoo.com

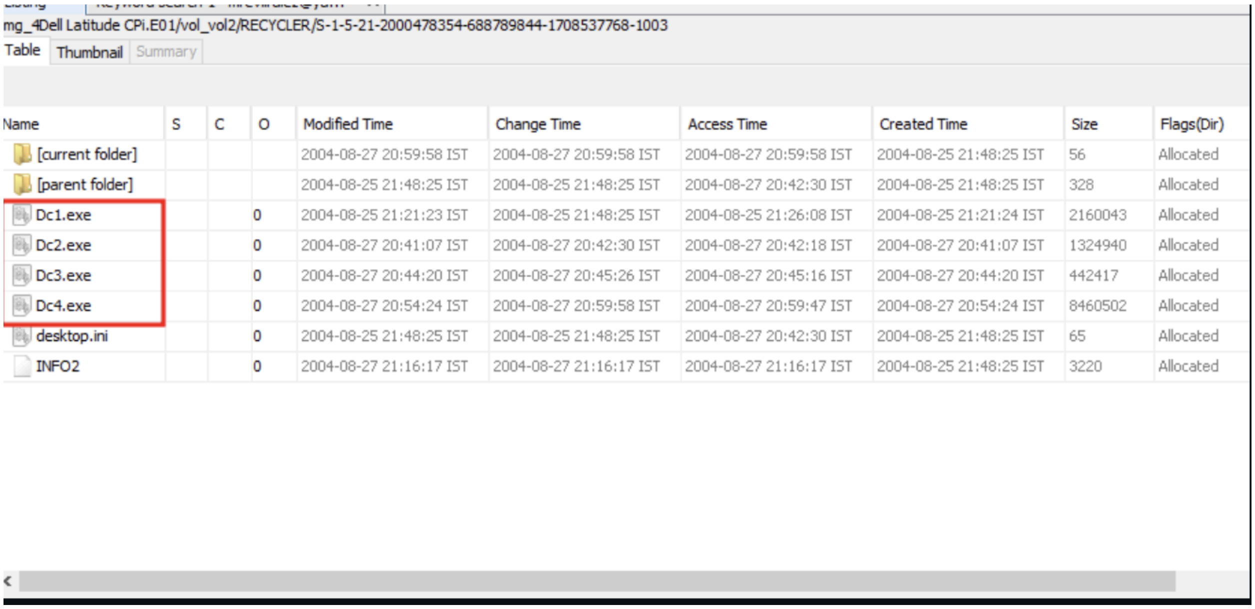
It's smart. It works for you.
Welcome to Yahoo! Mail.

Dear mrevilrulez@yahoo.com

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

Ans. To find the files, we have to look into folder of Recycle Bin.3

Note:- The Path is:
"C:\RECYCLER\S-1–5–21–2000478354–688789844–1708537768–1003\"

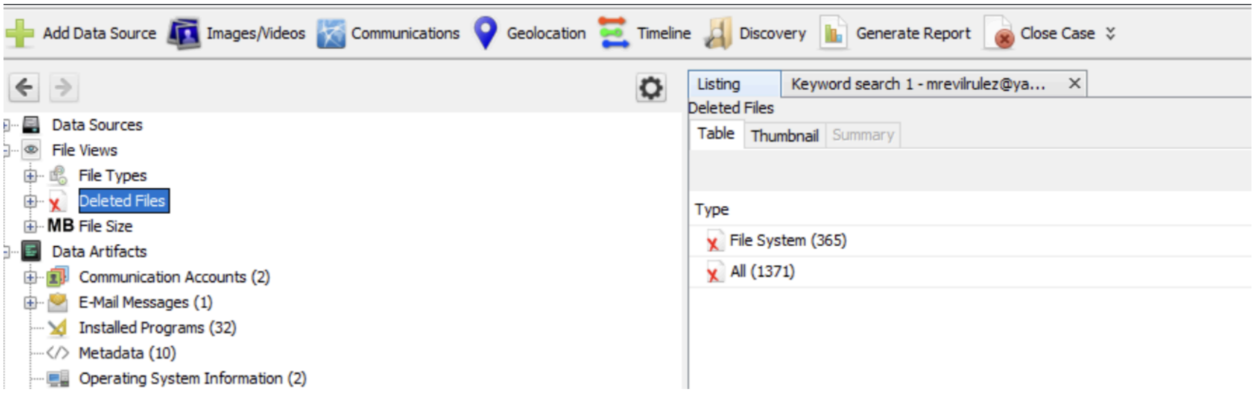


mg_4Dell Latitude CPi.E01/vol_vol2/RECYCLER/S-1-5-21-2000478354-688789844-1708537768-1003

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2004-08-27 20:59:58 IST	2004-08-27 20:59:58 IST	2004-08-27 20:59:58 IST	2004-08-25 21:48:25 IST	56	Allocated
[parent folder]				2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	328	Allocated
Dc1.exe			0	2004-08-25 21:21:23 IST	2004-08-25 21:48:25 IST	2004-08-25 21:26:08 IST	2004-08-25 21:21:24 IST	2160043	Allocated
Dc2.exe			0	2004-08-27 20:41:07 IST	2004-08-27 20:42:30 IST	2004-08-27 20:42:18 IST	2004-08-27 20:41:07 IST	1324940	Allocated
Dc3.exe			0	2004-08-27 20:44:20 IST	2004-08-27 20:45:26 IST	2004-08-27 20:45:16 IST	2004-08-27 20:44:20 IST	442417	Allocated
Dc4.exe			0	2004-08-27 20:54:24 IST	2004-08-27 20:59:58 IST	2004-08-27 20:59:47 IST	2004-08-27 20:54:24 IST	8460502	Allocated
desktop.ini			0	2004-08-25 21:48:25 IST	2004-08-25 21:48:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:48:25 IST	65	Allocated
INFO2			0	2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-25 21:48:25 IST	3220	Allocated

29. Are these files really deleted?

Ans. By looking at Deleted Files in the left pane, the total count of deleted files is: 1371



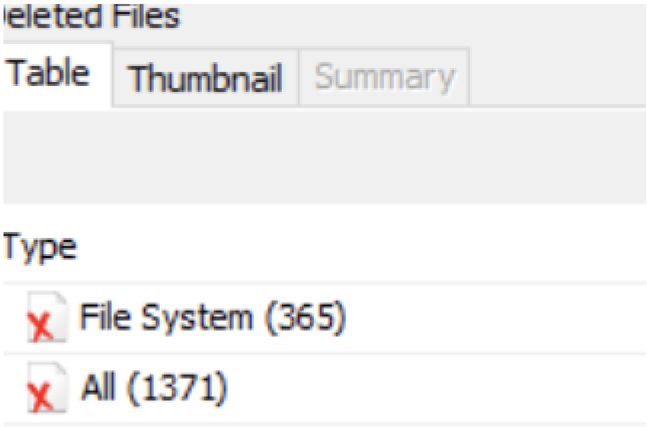
Data Sources
File Views
File Types
Deleted Files
MB File Size
Data Artifacts
Communication Accounts (2)
E-Mail Messages (1)
Installed Programs (32)
Metadata (10)
Operating System Information (2)

Deleted Files

Type
File System (365)
All (1371)

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

Ans. By looking at Deleted Files in the left pane, the files actually reported to be deleted by file system is: 365



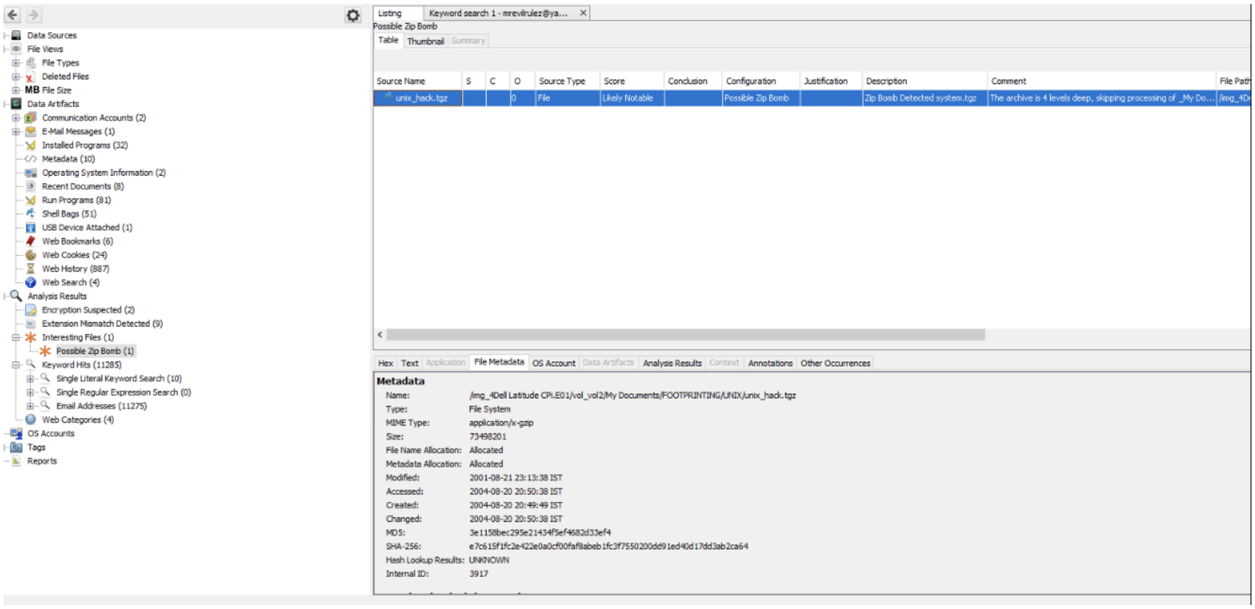
Type
File System (365)
All (1371)

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

Ans. Autopsy itself performs an antivirus check & it shows its result inside Interesting Items (left-side tree structure).

Upon looking at, we find out that there is a zip bomb.

Location of zip bomb: C:\My Documents\FOOTPRINTING\UNIX\unix_hack.tgz



- Data Sources
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Communication Accounts (2)
  - E-Mail Messages (1)
  - Installed Programs (32)
  - Metadata (10)
  - Operating System Information (2)
  - Recent Documents (8)
  - Run Programs (81)
  - Shell Bags (51)
  - USB Device Attached (1)
  - Web Bookmarks (6)
  - Web Cookies (24)
  - Web History (887)
  - Web Search (4)
- Analysis Results
  - Encryption Suspected (2)
  - Extension Mismatch Detected (9)
  - Interesting Files (1)
    - Possible Zip Bomb (1)
  - Keyword Hits (11285)
    - Single Literal Keyword Search (10)
    - Single Regular Expression Search (0)
    - Email Addresses (11275)
  - Web Categories (4)
- OS Accounts
- Tags
- Reports

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Description	Comment	File Path
unix_hack.tgz			0	File	Likely Notable		Possible Zip Bomb		Zip Bomb Detected system.tgz	The archive is 4 levels deep, skipping processing of _My Do...	/img_4D

Metadata

Name:	/img_4Dell Latitude CPi.E01/vol_vol2/My Documents/FOOTPRINTING/UNIX/unix_hack.tgz
Type:	File System
MIME Type:	application/x-gzip
Size:	73498201
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2001-08-21 23:13:38 IST
Accessed:	2004-08-20 20:50:38 IST
Created:	2004-08-20 20:49:49 IST
Changed:	2004-08-20 20:50:38 IST
MD5:	3e1158bec295e21434f5ef4682d33ef4
SHA-256:	e7c615f1fc2e422e0a0cf00faf8abeb1fc3f7550200dd91ed40d17dd3ab2ca64
Hash Lookup Results:	UNKNOWN
Internal ID:	3917