

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

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

- **MD5 hash of .dd image (hackingEC14Dell Latitude Cpi):**
28A9B613D6EEFE8A0515EFOA675BDEBD
- This hash value can be found in the “File Metadata” tab on the home screen of the image.

The screenshot shows the FTK Imager interface. On the left, the 'Data Sources' pane lists several hosts, including 'hackingdd1SCHARDT.001_39719 Host'. The main pane displays the 'File Metadata' tab for the selected image. The metadata table shows the following details:

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone
hackingdd1SCHARDT.001	Image	666238976	512	America/New_York

Below the table, the 'Metadata' section provides further details:

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

- **MD5 hash of .E01 image (hackingEC14Dell Latitude Cpi.E01):**
83324509a13d71fe1a202841a3aeceb0.
- This hash value can be found in the “File Metadata” tab on the home screen of the image.

The screenshot shows the FTK Imager interface. On the left, the 'Data Sources' pane lists several hosts, including 'hackingEC14Dell Latitude Cpi.E01_1 Host'. The main pane displays the 'File Metadata' tab for the selected image. The metadata table shows the following details:

Name	ID	Starting Sector	Length in Sectors	Des
vol1 (Unallocated: 0-62)	1	0	63	Una
vol2 (NTFS / exFAT (0x07): 63-9510479)	2	63	9510417	NTF
vol3 (Unallocated: 9510480-9514259)	3	9510480	3780	Una

Below the table, the 'Metadata' section provides further details:

- Name: /img_hackingEC14Dell Latitude Cpi.E01
- Type: E01
- Size: 4871301120
- MD5: 83324509a13d71fe1a202841a3aeceb0
- SHA1: 4c98148c3d813c7c8c66e231b8ebe8f252d9735a
- SHA-256: 525ffe103be690ed4c38715c5b08933d0ea744c11a8bcad790951707db68dd3f
- Sector Size: 512
- Time Zone: America/New_York

2. What operating system was used on the computer?

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

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

Listing						
/img_hackingEC14Dell Latitude CPi.E01/vol_vol2						
Table Thumbnail Summary						
^ Name	S	C	O	Modified Time	Change Time	Access Time
VIDEOROM.BIN			1	2004-08-18 12:54:36 EDT	2004-08-19 13:02:21 EDT	2004-08-18 12:54:36 EDT
WIN98				2004-08-18 12:28:38 EDT	2004-08-18 12:28:38 EDT	2004-08-20 11:26:37 EDT
WINDOWS				2004-08-25 11:56:09 EDT	2004-08-25 11:56:09 EDT	2004-08-27 11:08:06 EDT
[current folder]				2004-08-26 11:46:18 EDT	2004-08-27 11:08:18 EDT	2004-08-27 11:08:05 EDT
boot.ini			1	2004-08-19 18:20:04 EDT	2004-08-19 18:40:19 EDT	2004-08-26 11:51:47 EDT
hiberfil.sys				2004-08-27 11:08:16 EDT	2004-08-27 11:08:16 EDT	2004-08-27 11:08:16 EDT
ntdetect.com			1	2001-08-23 14:00:00 EDT	2004-08-19 13:02:11 EDT	2004-08-18 20:00:00 EDT
ntldr			1	2001-08-23 14:00:00 EDT	2004-08-19 13:02:11 EDT	2004-08-18 20:00:00 EDT
pagefile.sys				2004-08-27 11:08:14 EDT	2004-08-27 11:08:14 EDT	2004-08-27 11:08:14 EDT
<						
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences						
Strings Extracted Text Translation						
Page: 1 of 1 Page < > Matches on page: - of - Match < > 100% ⌕ ⌕ Reset						
[boot loader] timeout=30 default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating systems] multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional" /fastdetect						

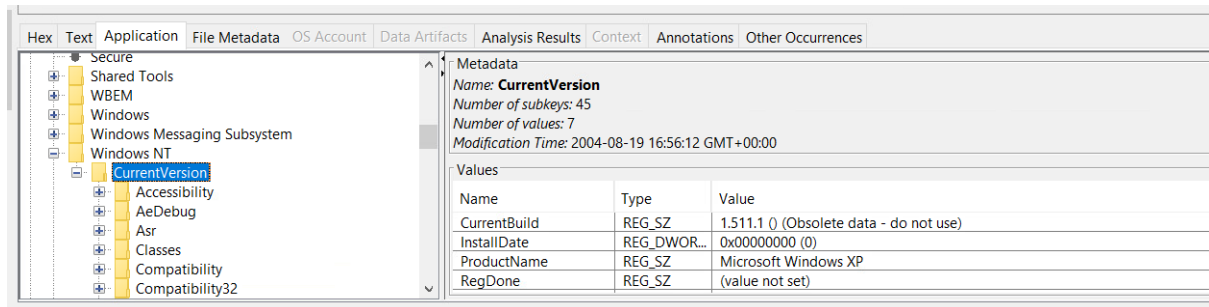
➤ Why “boot.ini” file and not the other file?

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

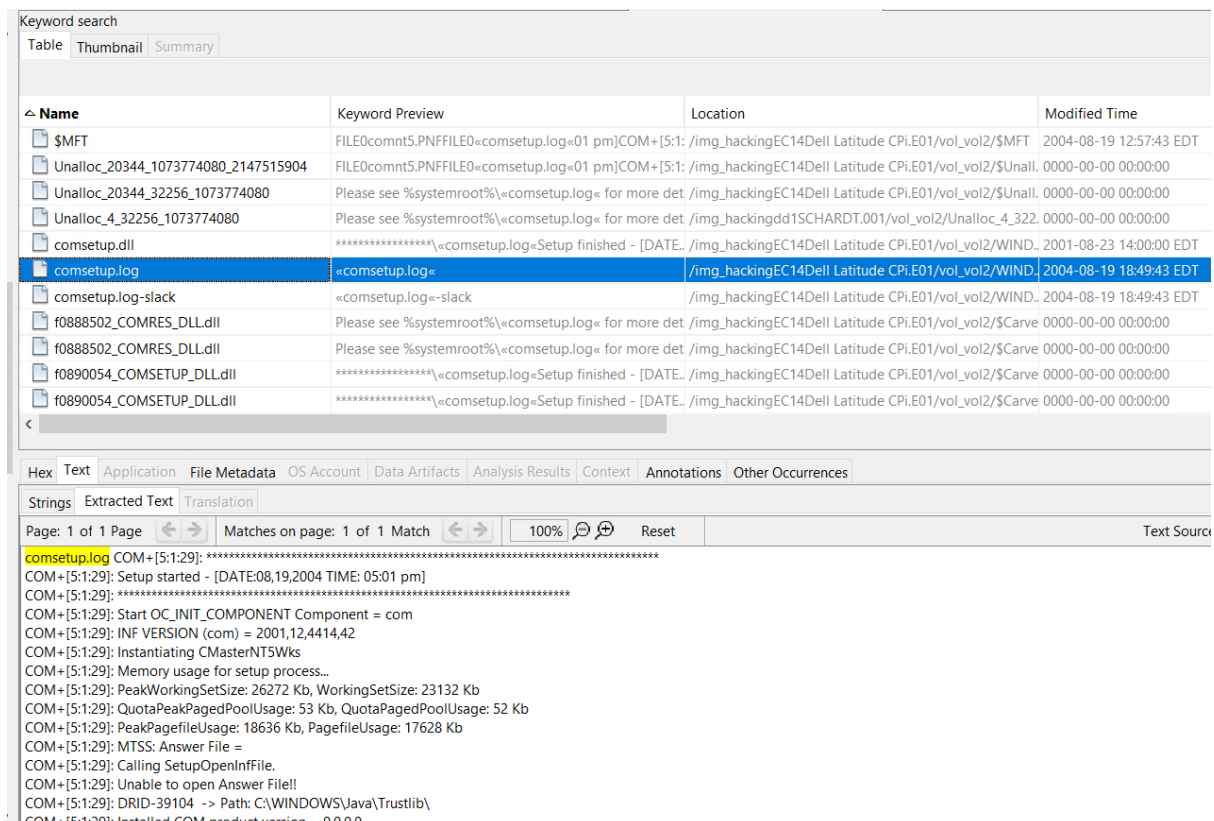
3. When was the install date?

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

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



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



4. What is the time zone settings?

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

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

6. What is the computer account name?

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

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

Listing Keyword search 5 - Mr. Evil x

/img_hackingEC14Dell LatitudeCPi.E01/vol_vol2/WINDOWS

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
sessmgr.setup.log			2	2004-08-19 18:28:27 EDT	2004-08-19 18:28:27 EDT	2004-08-19 18:28:27 EDT	2004-08-19 18:28:22 EDT	1059
setupact.log			2	2004-08-19 18:49:40 EDT	2004-08-19 18:49:40 EDT	2004-08-19 18:49:40 EDT	2004-08-19 12:59:16 EDT	158488
setupapi.log			2	2004-08-27 11:31:44 EDT	2004-08-27 11:31:44 EDT	2004-08-27 11:31:44 EDT	2004-08-19 12:59:29 EDT	175104
setuperr.log				2004-08-19 12:59:16 EDT	2004-08-19 13:02:11 EDT	2004-08-19 12:59:16 EDT	2004-08-19 12:59:16 EDT	0
setuplog.txt			2	2004-08-19 19:03:57 EDT	2004-08-19 19:03:57 EDT	2004-08-19 19:03:57 EDT	2004-08-19 12:59:13 EDT	706832
srchasst				2004-08-19 18:31:27 EDT	2004-08-19 18:31:27 EDT	2004-08-19 18:31:27 EDT	2004-08-19 18:31:21 EDT	56
system				2004-08-19 13:00:45 EDT	2004-08-19 13:00:45 EDT	2004-08-19 18:37:49 EDT	2004-08-19 12:50:37 EDT	56

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

Strings Extracted Text Translation

Page: 24 of 24 Page Matches on page: - of - Match 100% Reset

08/19/2004 18:03:54,d:\xpclient\base\ntsetup\oobe\msobmain\msobmain.cpp,5950,,Create account Mr. Evil in Administrators NTSTATUS(0)
08/19/2004 18:03:54,d:\xpclient\base\ntsetup\oobe\msobmain\msobmain.cpp,5793,,NetUserGetInfo Mr. Evil (0x00000000)
08/19/2004 18:03:55,d:\xpclient\base\ntsetup\oobe\msobmain\msobmain.cpp,5817,,Change Mr. Evil password property from 0x00000201 to 0x00010201 (0x00000000)
08/19/2004 18:03:55,d:\xpclient\base\ntsetup\oobe\msobmain\msobmain.cpp,7786,,COBMain:SetComputerDescription()
08/19/2004 18:03:55,d:\xpclient\base\ntsetup\oobe\msobmain\msobmain.cpp,2860,,START m_pObCommunicationManager->DoFinalTasks
08/19/2004 18:03:55,d:\xpclient\base\ntsetup\oobe\msobmain\msobmain.cpp,2862,,FINISH m_pObCommunicationManager->DoFinalTasks
08/19/2004 18:03:55,d:\xpclient\base\ntsetup\oobe\msobmain\msobmain.cpp,5742,,MainWndProc called PostQuitMessage().
08/19/2004 18:03:56,OOBE Trace 0,PlayStateChange 9
08/19/2004 18:03:56,OOBE Trace 0,PlayStateChange 10

7. What is the primary domain name?

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

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

Why this evidence:

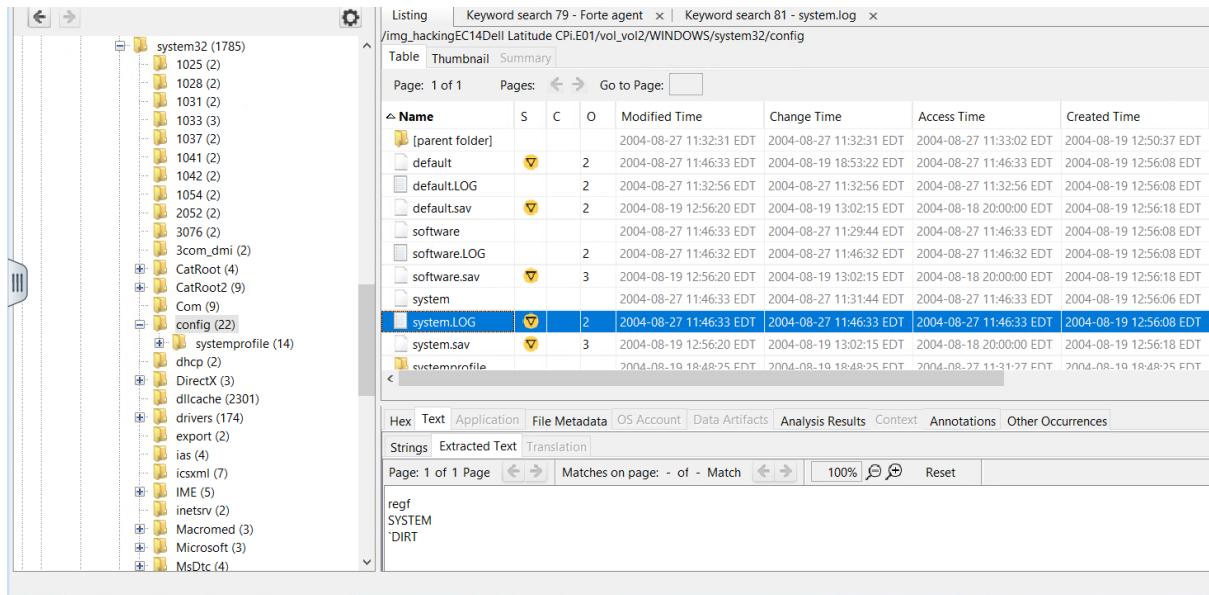
- The file **irunin.ini** appears to be a configuration file for the "Look@LAN" software, which is likely a network monitoring or management tool.
- The variable names %LANHOST% and %LANDOMAIN% strongly suggest they are related to the network environment where the software operates.

/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN							
Table Thumbnail Summary							
△ Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
irunin.bmp			3	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-08-25 11:56:09 EDT	2004-08-25 11:56:09 EDT
irunin.dat			3	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-08-25 11:56:09 EDT	2004-08-25 11:56:09 EDT
irunin.ini			3	2004-08-25 11:56:10 EDT	2004-08-25 11:56:10 EDT	2004-08-25 11:56:10 EDT	2004-08-25 11:56:09 EDT
irunin.lng			3	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-08-25 11:56:09 EDT	2004-08-25 11:56:09 EDT
lalassoc.dat			3	2003-04-27 09:31:26 EDT	2004-08-25 11:56:05 EDT	2004-08-26 11:06:15 EDT	2004-02-16 05:51:14 EST
lalservices.dat				2004-02-18 04:24:32 EST	2004-08-25 11:56:05 EDT	2004-08-26 11:06:18 EDT	2004-02-16 05:51:14 EST
sounds				2004-08-25 11:56:07 EDT	2004-08-25 11:56:07 EDT	2004-08-27 11:14:45 EDT	2004-08-25 11:56:06 EDT
<							
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences							
Strings Extracted Text Translation							
Page: 1 of 1 Page Matches on page: - of - Match 100% Reset							
[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 %ISWIN2000%=FALSE							

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

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

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



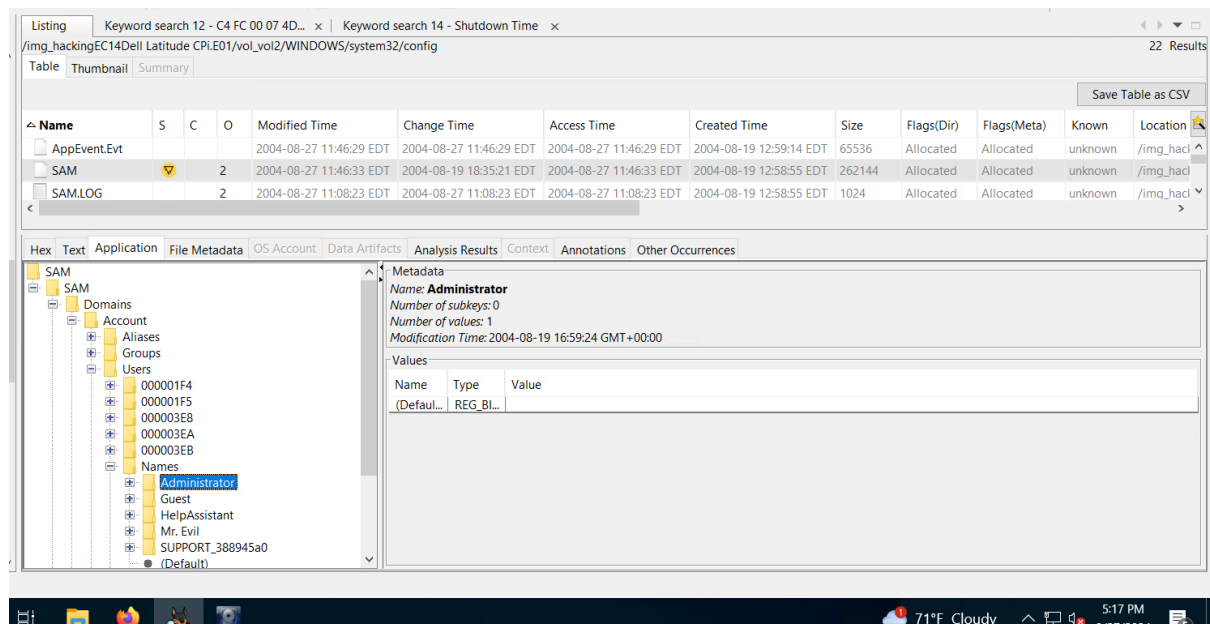
The **system.log** is maintained by the Windows Event Log service. Contains a chronological record of system-level events, including:

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

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

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

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



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

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

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

Listing Keyword search 79 - Forte agent x

Table Thumbnail Summary

Page: Pages: Go to Page:

Name	S	C	O	Login Name	Host	Scope	Realm Name
S-1-5-21-2000478354-688789844-1708537768-500			3	Administrator	hackingEC...	Local	
S-1-5-21-2000478354-688789844-1708537768-1003			3	Mr. Evil	hackingEC...	Local	
S-1-5-21-2000478354-688789844-1708537768-1002			3	SUPPORT_388945a0	hackingEC...	Local	
S-1-5-21-2000478354-688789844-1708537768-501			3	Guest	hackingEC...	Local	
S-1-5-21-2000478354-688789844-1708537768-1000			3	HelpAssistant	hackingEC...	Local	

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

Basic Properties

Login: Mr. Evil

Full Name:

Address: S-1-5-21-2000478354-688789844-1708537768-1003

Type:

Creation Date: 2004-08-19 19:03:54 EDT

Object ID: 20010

hackingEC14Dell Latitude CPi.E01_1 Host Details

Last Login: 2004-08-27 11:08:23 EDT

Login Count: 15

Administrator: True

Password Settings: Password does not expire

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

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

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

Listing Keyword search 79 - Forte agent x

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

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
All Users				2004-08-19 18:33:37 EDT	2004-08-19 18:33:37 EDT	2004-08-27 11:08:06 EDT	2004-08-19 12:59:01 EDT
Default User				2004-08-19 18:38:47 EDT	2004-08-19 18:38:47 EDT	2004-08-20 11:17:59 EDT	2004-08-19 12:59:01 EDT
LocalService				2004-08-19 18:52:00 EDT	2004-08-19 18:52:00 EDT	2004-08-27 11:08:06 EDT	2004-08-19 18:51:58 EDT
Mr. Evil				2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-08-19 19:04:05 EDT
NetworkService				2004-08-19 18:51:58 EDT	2004-08-19 18:51:58 EDT	2004-08-27 11:08:06 EDT	2004-08-19 18:51:55 EDT
[current folder]				2004-08-19 19:04:05 EDT	2004-08-19 19:04:05 EDT	2004-08-27 11:08:05 EDT	2004-08-19 12:59:01 EDT
[parent folder]				2004-08-26 11:46:18 EDT	2004-08-27 11:08:18 EDT	2004-08-27 11:08:05 EDT	2004-08-19 12:57:43 EDT

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

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

➤ **Verification:**

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

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

The screenshot shows a keyword search interface with two tabs: 'Listing' and 'Keyword search'. The 'Keyword search' tab is active, displaying a table with columns: Name, Location, and Keyword Preview. The first result is 'irunin.ini' located at '/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini'. Below the table, there are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The 'Text' tab is selected, showing the extracted text from the file. The text contains various system variables, including '%LANUSER%=Mr. Evil', '%REGOWNER%=Greg Schardt', and '%ISUSERNTADMIN%=TRUE'. The search results show 1 match on page 1 of 1.

Name	Location	Keyword Preview
irunin.ini	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Look@LAN/irunin.ini	HT%=600%REGOWNER%=«Greg Schardt«%REGORGA...

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

Strings Extracted Text Translation

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

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

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

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

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

Keyword search

Table Thumbnail Summary

Name	Location	Modified Time	Change Time
\$MFT	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/\$MFT	2004-08-19 12:57:43 EDT	2004-08-19 12:57:43 EDT
hackingdd1SCHARDT.001	/LogicalFileSet1/hackingdd1SCHARDT.001	0000-00-00 00:00:00	0000-00-00 00:00:00
f0826766_SHELL32_DLL	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/\$Carve	0000-00-00 00:00:00	0000-00-00 00:00:00
Unalloc_19547_32256_1073774080	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/\$Unall.	0000-00-00 00:00:00	0000-00-00 00:00:00
Unalloc_39722_32256_1073774080	/img_hackingdd1SCHARDT.001/vol_vol2/Unalloc_39722	0000-00-00 00:00:00	0000-00-00 00:00:00
f0826766_SHELL32_DLL	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/\$Carve	0000-00-00 00:00:00	0000-00-00 00:00:00
DETLOG.TXT	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/DETLO	2004-08-18 12:50:00 EDT	2004-08-19 18:40:19 EDT
DETLOG.TXT-slack	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/DETLO	2004-08-18 12:50:00 EDT	2004-08-19 18:40:19 EDT

<

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

Strings Extracted Text Translation

Page: 2 of 3 Page < > Matches on page: 1 of 1 Match < > 100% ⌕ ⊕ Reset

Checking for: Parallel Printer Port
QueryIOMem: Caller=DETECTLPT, rcQuery=0
IO=3bc-3be
Checking for: Xircom PE3 Network Adapter (VerifyKey=3bc)
QueryIOMem: Caller=DETECTLPT, rcQuery=0
IO=3bc-3be
Checking for: Trantor T3x8 SCSI Adapter (VerifyKey=3bc)
QueryIOMem: Caller=DETECTLPT, rcQuery=0
IO=3bc-3be

2. Compaq WL110 Wireless LAN PC Card

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

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

The screenshot shows a keyword search interface. At the top, there are tabs for 'Table', 'Thumbnail', and 'Summary'. Below these is a table with three columns: 'Name', 'Location', and 'Modified Time'. The table lists three files: 'f1437462.java', 'f1437462.java', and 'netwv48.inf'. The 'netwv48.inf' file is highlighted. Below the table, there are tabs for 'Hex', 'Text', 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', 'Annotations', and 'Other Occurrences'. The 'Text' tab is selected, showing a list of device descriptions. The list includes various wireless LAN cards and their descriptions, such as 'Dell TrueMobile 1150 Series Wireless LAN Card', 'IBM High Rate Wireless LAN PC Card', 'IBM High Rate Wireless LAN Mini PCI Card', 'IBM Internal High Rate Wireless LAN PC Card', 'ELSA Airlancer MC11 High Rate Wireless LAN PC Card', 'ORINOCO Wireless LAN PC Card (5 volt)', 'ORINOCO Wireless LAN PC Card (3.3 and 5 volt)', 'ORINOCO Wireless LAN PC Card (3.3 volt)', 'Sony PCWA-C100 Wireless PC Card', 'Toshiba Wireless LAN Card', 'Toshiba Wireless LAN Mini PCI Card', 'NCR-WaveLAN Wireless LAN PC Card', 'Buffalo WLI-PCM-L11 Wireless LAN Adapter', and 'RoamAbout 802.11 DS (Cabletron)'.

Name	Location	Modified Time
f1437462.java	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/\$Carve	0000-00-00 00:00:00
f1437462.java	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/\$Carve	0000-00-00 00:00:00
netwv48.inf	/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/WIND..	2001-08-23 14:00:00 EDT

Page: 1 of 1 Page Matches on page: 1 of 15 Match 100% Reset

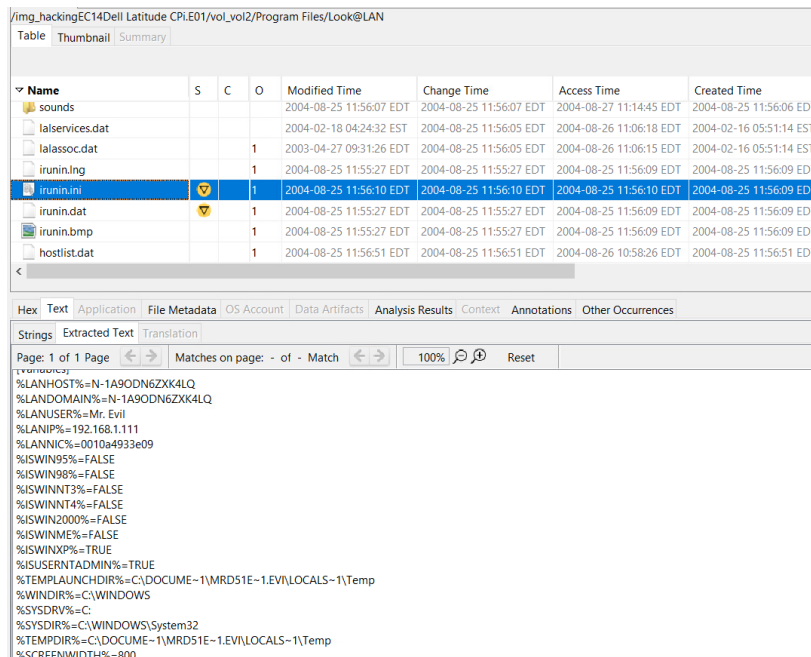
wlde148_LT1.DeviceDesc = "Dell TrueMobile 1150 Series Wireless LAN Card"
wlde148_LT2.DeviceDesc = "Dell TrueMobile 1150 Series Wireless LAN Mini PCI Card"
wlilm48_LT.DeviceDesc = "IBM High Rate Wireless LAN PC Card"
wlilm48_LT2.DeviceDesc = "IBM High Rate Wireless LAN Mini PCI Card"
wlilm48_LT3.DeviceDesc = "IBM Internal High Rate Wireless LAN PC Card"
ELSA.DeviceDesc = "ELSA Airlancer MC11 High Rate Wireless LAN PC Card"
wlluc48.DeviceDesc = "ORINOCO Wireless LAN PC Card (5 volt)"
wlluc48a.DeviceDesc = "ORINOCO Wireless LAN PC Card (3.3 and 5 volt)"
wlluc48b.DeviceDesc = "ORINOCO Wireless LAN PC Card (3.3 volt)"
wlson48_LT.DeviceDesc = "Sony PCWA-C100 Wireless PC Card"
wlto48_TO1.DeviceDesc = "Toshiba Wireless LAN Card"
wlto48_TO2.DeviceDesc = "Toshiba Wireless LAN Mini PCI Card"
wlil11.DeviceDesc = "NCR-WaveLAN Wireless LAN PC Card"
wlil12.DeviceDesc = "Buffalo WLI-PCM-L11 Wireless LAN Adapter"
wlrbt48_EN1.DeviceDesc = "RoamAbout 802.11 DS (Cabletron)"

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

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

Answer: The IP: 192.168.1.111 and MAC: 0010a4933e09

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



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
sounds				2004-08-25 11:56:07 EDT	2004-08-25 11:56:07 EDT	2004-08-27 11:14:45 EDT	2004-08-25 11:56:06 EDT
lalservices.dat				2004-02-18 04:24:32 EST	2004-08-25 11:56:05 EDT	2004-08-26 11:06:18 EDT	2004-02-16 05:51:14 EST
lalasscd.dat			1	2003-04-27 09:31:26 EDT	2004-08-25 11:56:05 EDT	2004-08-26 11:06:15 EDT	2004-02-16 05:51:14 EST
irunin.lng			1	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-08-25 11:56:09 EDT	2004-08-25 11:56:09 EDT
irunin.ini			1	2004-08-25 11:56:10 EDT	2004-08-25 11:56:10 EDT	2004-08-25 11:56:10 EDT	2004-08-25 11:56:09 EDT
irunin.dat			1	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-08-25 11:56:09 EDT	2004-08-25 11:56:09 EDT
irunin.bmp			1	2004-08-25 11:55:27 EDT	2004-08-25 11:55:27 EDT	2004-08-25 11:56:09 EDT	2004-08-25 11:56:09 EDT
hostlist.dat			1	2004-08-25 11:56:51 EDT	2004-08-25 11:56:51 EDT	2004-08-26 10:58:26 EDT	2004-08-25 11:56:51 EDT

Strings	Extracted Text	Translation
Page: 1 of 1 Page		
Matches on page: - of - Match		
100%		
Reset		
<pre>%LANHOST%=N-1A90DN6ZXK4LQ %LANDOMAIN%=N-1A90DN6ZXK4LQ %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\EV\LOCALS~1\Temp %WINDIR%=C:\WINDOWS %SYSDIR%=C: %SYSDIR%=C:\WINDOWS\System32 %TEMPDIR%=C:\DOCUME~1\MRD51E~1\EV\LOCALS~1\Temp %SCREENWIDTH%=800</pre>		

- **Why this file and not others:** The "*irunin.ini*" file appears to be a configuration file for the "Look@LAN" software, which is likely a network monitoring and management tool. Configuration files often store settings related to the network environment, including network interfaces and their addresses. While this file doesn't explicitly name the network card model, the presence of the MAC and IP address variables suggests it's a good place to look for network-related information.
- **Source of evidence:** The *irunin.ini* file provide evidence related to network connectivity:
 - **%LANNIC%=0010a4933e09:** This variable represents the MAC (Media Access Control) address of the network card. A MAC address is a unique identifier assigned to a network interface.


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

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

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

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

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

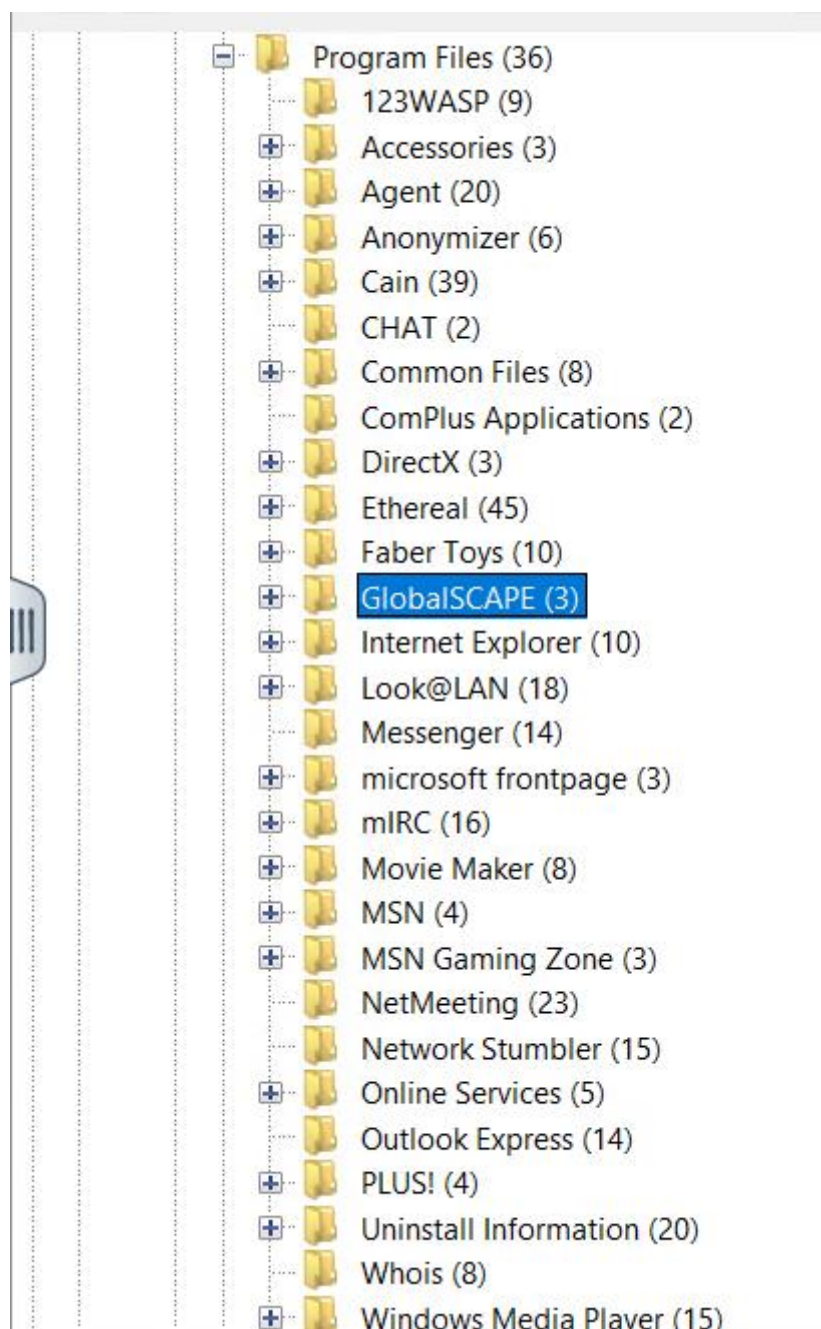

[Database Download](#)
[Lookup](#)
[API](#)
[Generator](#)
[Statistics](#)
[FAQ](#)
[Login](#)
[Sign up](#)

0010A4 MAC address details

Vendor details		Block details		MAC address details	
OUI	00:10:A4	Is registered	True	Is valid	False
Is private	False	Border left	00:10:A4:00:00:00	Virtual Machine	Not detected
Company name	Xircom	Border right	00:10:A4:FF:FF:FF	Transmission type	Unicast
Company address	2300 CORPORATE CENTER DR. THOUSAND OAKS CA 91320 US	Block size	16,777,216	Administration type	UAA
Country code	US	Assignment block size	MA-L	Applications	Not detected
		Date created	13 November 1997	Wireshark notes	Xircom # RealPort 10/100 PC Card
		Date updated	26 September 2015		

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

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



The 6 installed programs are:

1) mIRC: Internet Relay Chat client

mIRC is a popular **Internet Relay Chat** client used by individuals and organizations to communicate, share, play and work with each other on IRC networks around the world. Serving the Internet community for over two decades, mIRC has evolved into a powerful, reliable and fun piece of technology.

[About mIRC](#)[Download mIRC](#)[Register mIRC](#)

Latest News

mIRC v7.77 has been [released](#).

Join our release announcement [mailing list](#) if you would like to be notified by email when a new version of mIRC is released.

Visit our [discussion forums](#) where you can discuss mIRC with other users or post questions if you need help.

2) Look@LAN:



< [HOME](#) | [TUTORIALS](#) | [DONATE](#) | [WEB TOOLS](#) | [YOUTUBE](#) | [NEWSLETTER](#) | [DEALS!](#) | [FORUMS](#)

MajorGeeks.com - Live Fast, Geek Hard

MajorGeeks.Com » Networking » Look@LAN 2.50 Build 35 » Download Now

Look@LAN 2.50 Build 35

Author: Carlo Medas
Date: 10/16/2016
Size: 2.1 MB
License: Freeware
Requires: Win 10 / 8 / 7 / Vista / XP
Downloads: 283531 times

TIP: [Click Here to Repair or Restore Missing Windows Files](#)

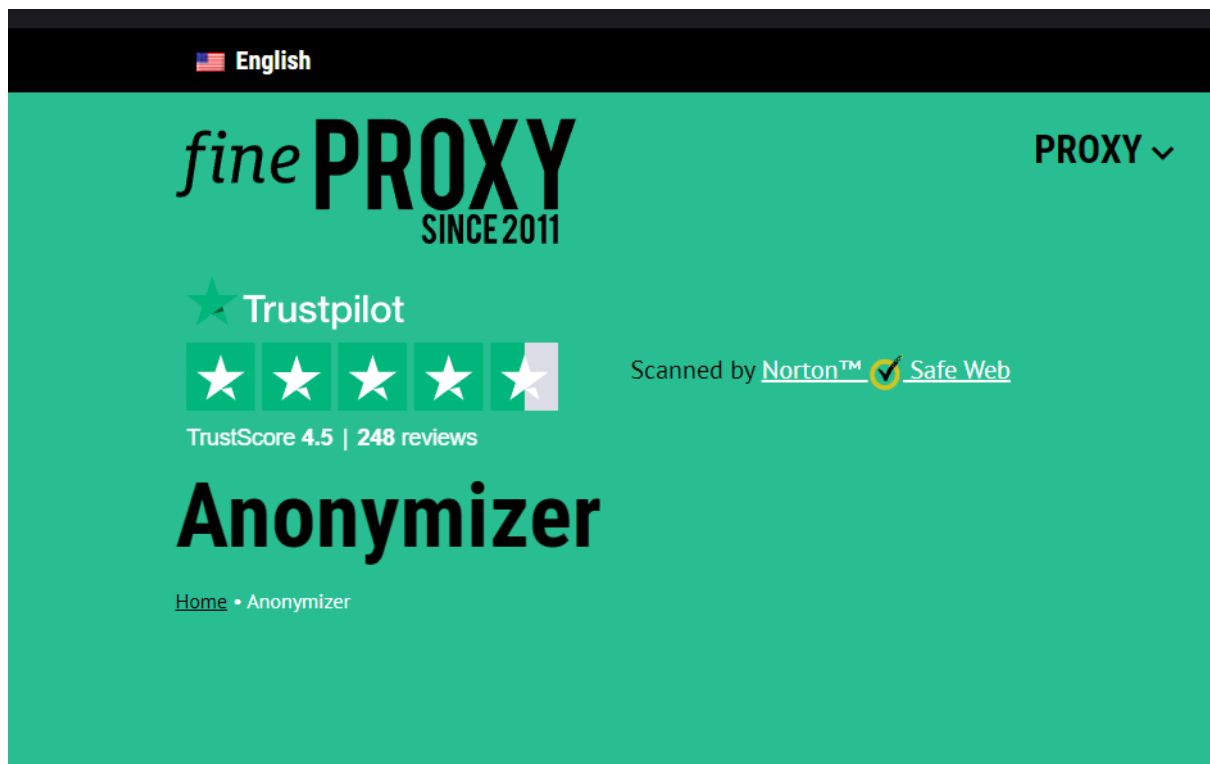


[Download@MajorGeeks](#)
[Download@MajorGeeks](#)

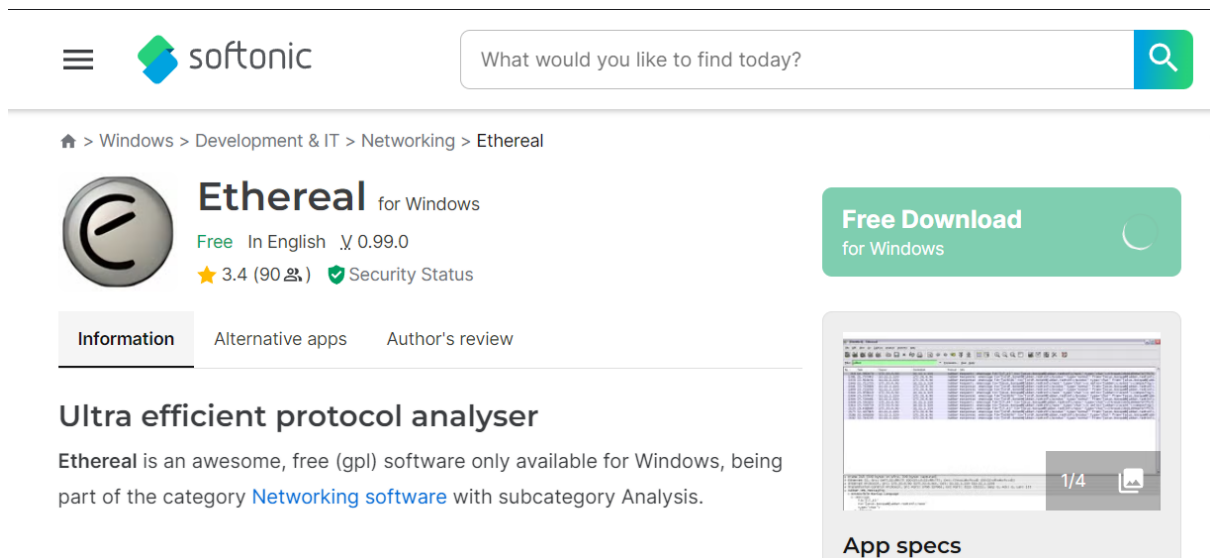
FILES

- All In One Tweaks
- Android
- Antivirus & Malware
- Appearance
- Back Up
- Browsers
- CD\DVD\Blu-Ray
- Covert Ops
- Drivers
- Drives (SSD, HDD, USB)
- Games
- Graphics & Photos
- Internet Tools
- Linux Distros

3) Anonymizer: Proxy tool



4) Ethereal: Packet sniffing tool



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



123 Write All Stored Passwords (WASP) v 2.01

WASP will display all passwords of the currently logged on user that are stored in the Microsoft PWL file.

OVERVIEW | **SPECS**

WASP will display all passwords of the currently logged on user that are stored in the Microsoft PWL file. It allows the supervision / convenient deletion of this file to improve the security / privacy of your PC.

It is also very useful for educational purposes about computer security. In the documentation you also find helpful facts about the Microsoft PWL file in general. This software is free for private and commercial use and does not need to be registered.

[Download Now](#)

TechSpot means tech analysis and advice you can trust.

Last updated: August 19, 2014
Developer: iOpus
License: Freeware
OS: Windows 98, ME
File size: 2.9 MB
Downloads: 8,428

DOWNLOAD

Microsoft E

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



FILES

- All In One Tweaks
- Android
- Antivirus & Malware
- Appearance
- Back Up
- Browsers
- CD\DVD\Blu-Ray
- Covert Ops
- Drivers
- Drives (SSD, HDD, USB)
- Games
- Graphics & Photos
- Internet Tools
- Linux Distros
- MajorGeeks Windows Tweaks
- Multimedia

MajorGeeks.Com » All In One Tweaks » Windows 98, XP, ME & Vista » Faber Toys 2.6 Build 52 » Do

Faber Toys 2.6 Build 52

Author: Fabio Vescarelli.
Date: 10/03/2004
Size: 1.86 MB
License: Freeware
Requires: Win9x/NT/200x/XP/Vista
Downloads: 37982 times

[Download Now](#)

[Download@MajorGeeks](#)
[Download@MajorGeeks](#)

TIP: Click Here to Repair or Restore Missing Windows Files

Major Geeks Special Offer: Save 85% on Advanced SystemCare PRO Super Pack Sale!

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

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

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

Listing Keyword search 26 - Compaq WL110 W... Keyword search 27 - Compaq WL110 W... Keyword search 28 - Xircom CardBus...

/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/Program Files/Agent/Data

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
00000152.DAT	▼			2004-08-25 12:06:15 EDT	2004-08-25 12:06:15 EDT	2004-08-25 12:06:29 EDT	2004-08-25 12:02:56 EDT
00000152.IDX	▼		3	2004-08-25 12:06:29 EDT	2004-08-25 12:06:29 EDT	2004-08-25 12:06:29 EDT	2004-08-25 12:02:56 EDT
00000157.DAT	▼		3	2004-08-25 12:11:47 EDT	2004-08-25 12:11:47 EDT	2004-08-25 12:12:07 EDT	2004-08-25 12:03:02 EDT
00000157.IDX	▼		3	2004-08-25 12:12:07 EDT	2004-08-25 12:12:07 EDT	2004-08-25 12:12:07 EDT	2004-08-25 12:03:02 EDT
00000158.DAT				2004-08-25 12:12:39 EDT	2004-08-25 12:12:39 EDT	2004-08-25 12:13:39 EDT	2004-08-25 12:03:04 EDT
00000158.IDX			3	2004-08-25 12:13:39 EDT	2004-08-25 12:13:39 EDT	2004-08-25 12:13:39 EDT	2004-08-25 12:03:04 EDT
000004AF.DAT				2004-08-25 12:14:31 EDT	2004-08-25 12:14:31 EDT	2004-08-25 12:14:42 EDT	2004-08-25 12:03:06 EDT
000004AF.IDX	▼		3	2004-08-25 12:14:42 EDT	2004-08-25 12:14:42 EDT	2004-08-25 12:14:42 EDT	2004-08-25 12:03:06 EDT
000004B0.DAT	▼		3	2004-08-25 12:03:10 EDT	2004-08-25 12:03:10 EDT	2004-08-25 12:03:10 EDT	2004-08-25 12:03:10 EDT

<

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

Strings Extracted Text Translation

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

enu
Mr Evil <whoknowsme@sbcglobal.net>

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

Answer: The NNTP server information is as follows:

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

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

Listing

Keyword search 39 - news.dallas.sb... x







Keyword search 40 - NNTP Server x

Keyword search

Table

Thumbnail

Summary

Name	Location
 hackingdd1SCHARDT.001	/LogicalFileSet1/hackingdd1SCHARDT.001
 f1107542_iis_u.dll	/img_hackingEC14Dell Latitude Cpi.E01/vol_vol2/\$CarvedFiles/2/f1107542_iis_u.dll
 f1801689.reg	/img_hackingEC14Dell Latitude Cpi.E01/vol_vol2/\$CarvedFiles/4/f1801689.reg
 Unalloc_19547_32256_1073774080	/img_hackingEC14Dell Latitude Cpi.E01/vol_vol2/\$Unalloc/Unalloc_19547_32256_1073774080
 iis.inf	/img_hackingEC14Dell Latitude Cpi.E01/vol_vol2/WINDOWS/inf/iis.inf
 iis.PNF	/img_hackingEC14Dell Latitude Cpi.E01/vol_vol2/WINDOWS/inf/iis.PNF

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 4317 of 6447

Page

←

→

Matches on page: 1 of 1 Match

←

→

100%

🔍

🔍

Reset

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

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

19. What two installed programs show this information?

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

```
➤ Path: /img_hackingEC14Dell Latitude
CPI.E01/vol vol2/$Unalloc/Unalloc 19547 1073774080 2147515904
```

Listing

Keyword search 79 - Forte agent x

/img_hackingEC14DeII Latitude CPi.E01/vol_vol2/\$Unalloc

Table

Thumbnail

Summary

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 89 of 106 Page

◀ ▶

 Matches on page: - of - Match

◀ ▶

 100%

🔍

 Reset

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

/img_hackingEC14DeII Latitude CPi.E01/vol_vol2/\$Unalloc

Table

Thumbnail

Summary

Page: 1 of 1 Pages:

◀ ▶

 Go to Page:

▲ Name

S

C

O

Modified Time

Change Time

Access Time

Created Time

✖

 Unalloc_19547_1073774080_2147515904

▼

 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00

<

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 89 of 106 Page

◀ ▶

 Matches on page: - of - Match

◀ ▶

 100%

🔍

 Reset

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

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

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

The screenshot shows a forensic analysis interface. At the top, there's a 'Listing' tab with a search bar containing 'Keyword search 57 - mreivilrulez'. Below this, the path '/img_hackingEC14Dell Latitude CPi.E01/vol_vol2/\$CarvedFiles/2' is displayed. A table view shows two files: 'f1234109.txt' and 'f1234207.txt'. The 'f1234109.txt' file is selected, and its contents are displayed in the 'Text' view below. The text view shows a list of mIRC configuration settings, including '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=mreivilrulez', '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]', and 'thin=1'.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
f1234109.txt			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	51
f1234207.txt			2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	35

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=mreivilrulez
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

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

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

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

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

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

➤ **Path:**:/img_hackingEC14Dell Latitude
CPI.E01/vol_vol2/\$CarvedFiles/2/f1234109.txt

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

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

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

Table	Thumbnail	Summary							
▲ Name	S	C	O	Modified Time	Change Time	Access Time	Created Time		
#Chataholics.UnderNet.log			3	2004-08-20 11:54:11 EDT	2004-08-20 11:54:11 EDT	2004-08-20 11:54:11 EDT	2004-08-20 11:52:09 EDT		
#CyberCafe.UnderNet.log		▼	3	2004-08-20 15:02:55 EDT	2004-08-20 15:02:55 EDT	2004-08-20 15:02:55 EDT	2004-08-20 11:54:21 EDT		
#Elite.Hackers.UnderNet.log			3	2004-08-20 11:49:05 EDT	2004-08-20 11:49:05 EDT	2004-08-20 11:49:05 EDT	2004-08-20 11:45:34 EDT		
#ISO-WAREZ.EFnet.log			3	2004-08-20 11:29:42 EDT	2004-08-20 11:29:42 EDT	2004-08-20 11:29:42 EDT	2004-08-20 11:29:01 EDT		
#LuxShell.UnderNet.log			3	2004-08-20 11:43:21 EDT	2004-08-20 11:43:21 EDT	2004-08-20 11:43:21 EDT	2004-08-20 11:42:03 EDT		
#evilfork.EFnet.log		▼	3	2004-08-20 11:31:07 EDT	2004-08-20 11:31:07 EDT	2004-08-20 11:31:07 EDT	2004-08-20 11:30:18 EDT		
#funny.UnderNet.log			3	2004-08-20 15:28:14 EDT	2004-08-20 15:28:14 EDT	2004-08-20 15:28:14 EDT	2004-08-20 15:26:18 EDT		
#houston.UnderNet.log			3	2004-08-20 11:52:01 EDT	2004-08-20 11:52:01 EDT	2004-08-20 11:52:01 EDT	2004-08-20 11:48:59 EDT		
#mp3xserv.UnderNet.log			3	2004-08-20 11:44:32 EDT	2004-08-20 11:44:32 EDT	2004-08-20 11:44:32 EDT	2004-08-20 11:43:16 EDT		
#thedarktower.AfterNET.log		▼	4	2004-08-20 15:16:23 EDT	2004-08-20 15:16:23 EDT	2004-08-20 15:16:23 EDT	2004-08-20 15:14:45 EDT		
#ushells.UnderNet.log			3	2004-08-20 11:45:07 EDT	2004-08-20 11:45:07 EDT	2004-08-20 11:45:07 EDT	2004-08-20 11:44:49 EDT		
[current folder]				2004-08-20 11:24:48 EDT	2004-08-20 11:24:48 EDT	2004-08-27 11:14:45 EDT	2004-08-20 11:24:48 EDT		
<div><</div>									
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Strings	Extracted Text	Translation							
Page: 1 of 1 Page <div><></div> Matches on page: - of - Match <div><></div> <div>100%</div> <div></div> <div></div> Reset									
Session Start: Fri Aug 20 10:45:34 2004 Session Ident: #Elite.Hackers									

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

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

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

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

TableThumbnailSummary

△ Name

[current folder]

[parent folder]

preferences

recent

S

C

O

Modified Time

Change Time

Access Time

Created Time

</

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

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

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

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

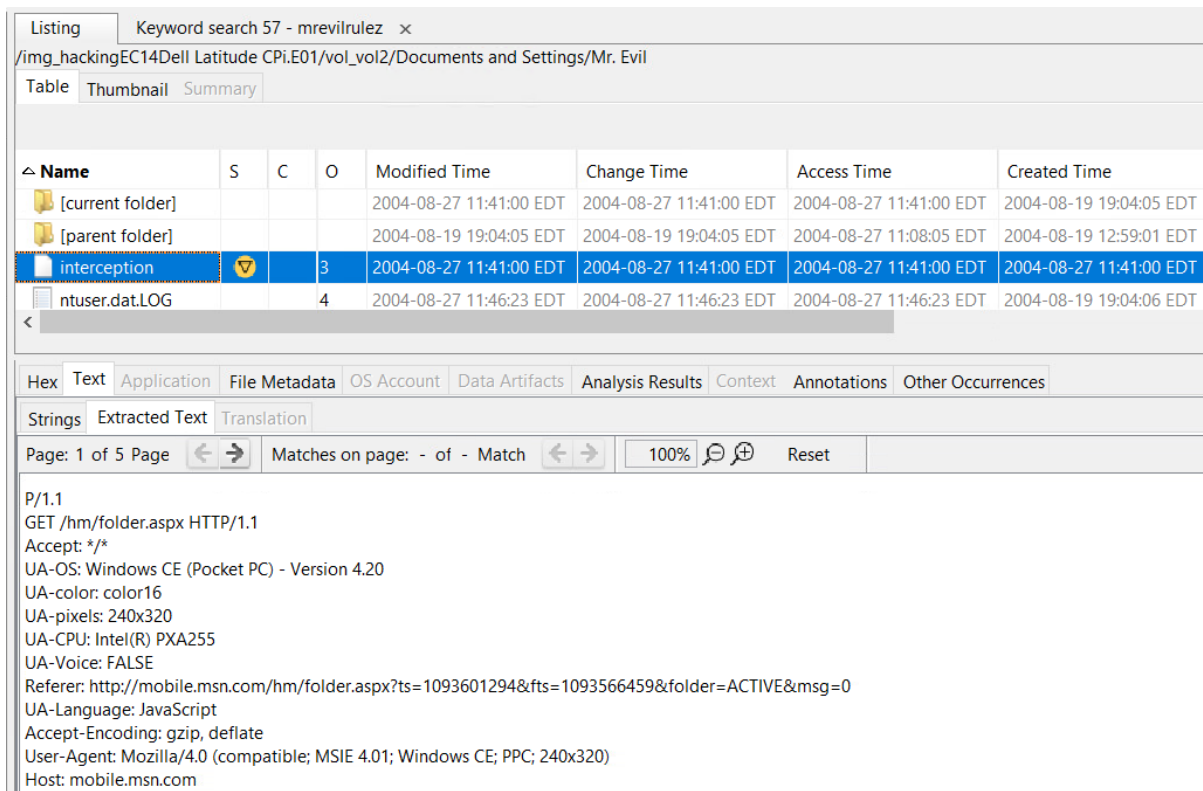
UA-OS: Windows CE (Pocket PC) - Version 4.20

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

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

25. What websites was the victim accessing?

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



Listing Keyword search 57 - mrevilrulez x

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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-08-19 19:04:05 EDT
[parent folder]				2004-08-19 19:04:05 EDT	2004-08-19 19:04:05 EDT	2004-08-27 11:08:05 EDT	2004-08-19 12:59:01 EDT
interception			3	2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT	2004-08-27 11:41:00 EDT
ntuser.dat.LOG			4	2004-08-27 11:46:23 EDT	2004-08-27 11:46:23 EDT	2004-08-27 11:46:23 EDT	2004-08-19 19:04:06 EDT

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

Strings Extracted Text Translation

Page: 1 of 5 Page Matches on page: - of - Match 100% Reset

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

- **mobile.msn.com**

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

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

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

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

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

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

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

Table	Thumbnail	Summary
△ Name	S	C O
[current folder]		2004-08-27 11:41:00 EDT 2004-08-27 11:41:00 EDT 2004-08-27 11:41:00 EDT 2004-08-19 19:04:05 EDT
[parent folder]		2004-08-19 19:04:05 EDT 2004-08-19 19:04:05 EDT 2004-08-27 11:08:05 EDT 2004-08-19 12:59:01 EDT
interception	▼	3 2004-08-27 11:41:00 EDT 2004-08-27 11:41:00 EDT 2004-08-27 11:41:00 EDT 2004-08-27 11:41:00 EDT
ntuser.dat.LOG		4 2004-08-27 11:46:23 EDT 2004-08-27 11:46:23 EDT 2004-08-27 11:46:23 EDT 2004-08-19 19:04:06 EDT

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Strings									
Extracted Text									
Translation									
Page: 1 of 5 Page									
Matches on page: - of - Match									
100% Reset									
<pre> HTTP/1.1 302 Found Server: Microsoft-IIS/5.0 Date: Fri, 27 Aug 2004 15:36:42 GMT X-Powered-By: ASP.NET P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" Location: http://mobile.msn.com/hm/folder.aspx?ts=1093601294&fts=1093566459&folder=ACTIVE&msg=0 Cache-Control: private Content-Type: text/html; charset=utf-8 Content-Length: 214 Expires: -1 <html><head><title>Object moved</title></head><body> <h2>Object moved to here< </body></html> </pre>									

Listing Keyword search 57 - mrevilrulez x

Keyword search

Table Thumbnail Summary

Name	Location	Keyword Preview
f2016858.h	/img_hackingEC14Dell Latitude CPl.E01/vol_vol2/\$CarvedFiles/4/f2016858.h	class="last" > «mrev
hackingdd1SCHARDT.001	/LogicalFileSet1/hackingdd1SCHARDT.001	<title>Yahoo! Mail - «mrevilrulez«@y
0	/img_hackingEC14Dell Latitude CPl.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Ten	Congratulations, the ID«mrevilrulez«is
0	/img_hackingEC14Dell Latitude CPl.E01/vol_vol2/Documents and Settings/Mr. Evil/Local Settings/Ten	Mail Welcome, «mre
Unalloc_19547_32256_1073774080	/img_hackingEC14Dell Latitude CPl.E01/vol_vol2/\$Unalloc/Unalloc_19547_32256_1073774080	<title>Yahoo! Mail - «mrevilrulez«@y

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

Download Images

Yahoo! My Yahoo! Mail

Welcome, **mrevilrulez**
[Sign Out, My Account]

Mail | Addresses | Calendar | Notepad **mrevilrulez@yahoo.com** [Sign Out]

Check Mail - Compose - Search Mail | Mail Upgrades - Mail Options

Choose from 10
Free Cell Phones
Folders[Add - Edit]

Welcome, Greg!

You have **1 unread message:**
Inbox(1)


Today's tip: Stop spammers from knowing you opened an email. Turn on the security preference to "Block HTML graphics." [Learn](#)

0% of 100.0MB


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

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

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



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

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

[Continue to Yahoo! Mail](#)

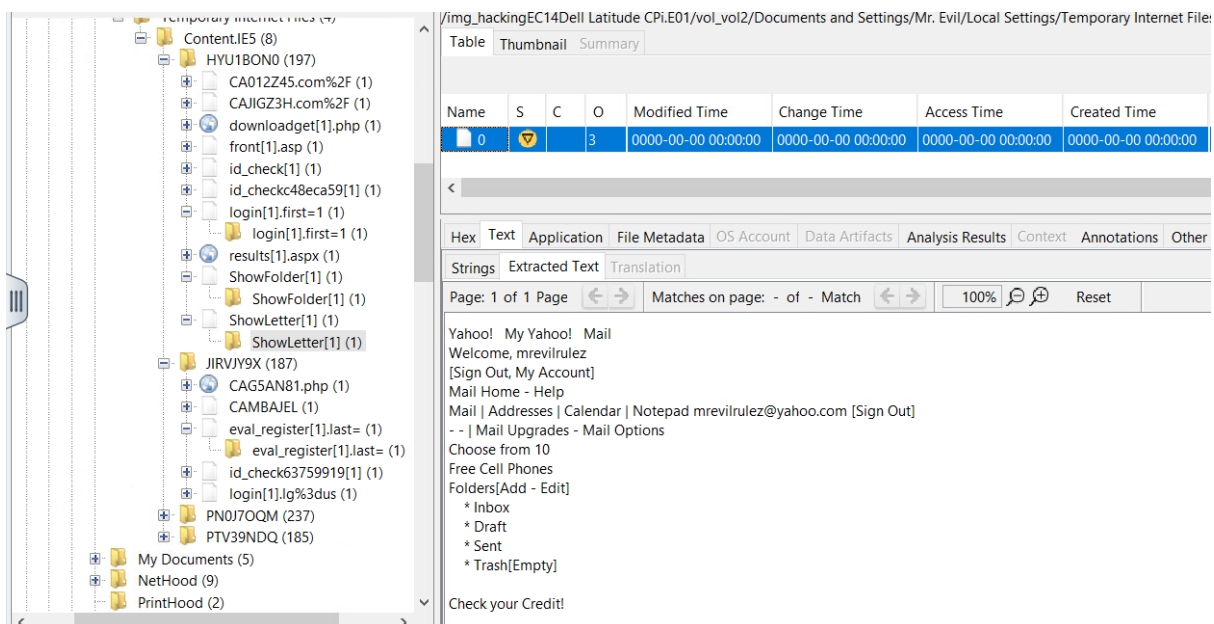
[Review Marketing Preferences:](#)

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

Settings/Temporary Internet

Files/Content.IE5/HYU1BON0/ShowLetter[1]/ShowLetter[1]/0

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



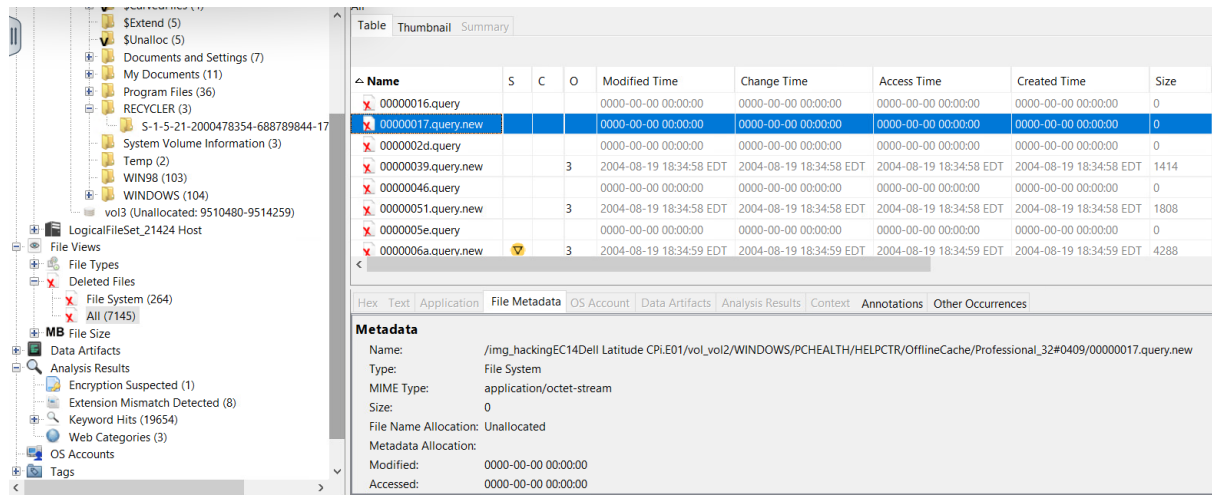
28. How many executable files are in the recycle bin?

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

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

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

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



The screenshot shows a file explorer window with a list of files. The file '00000016.query' is selected. The metadata for this file is displayed on the right side of the window.

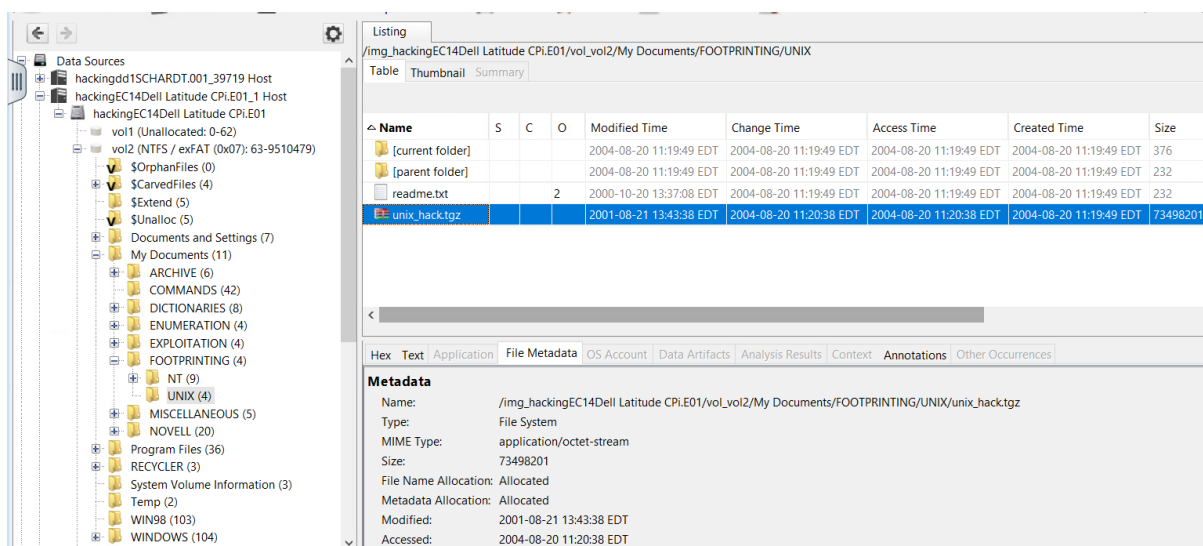
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
00000016.query				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
00000017.query.new				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
0000002d.query				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
00000039.query.new			3	2004-08-19 18:34:58 EDT	2004-08-19 18:34:58 EDT	2004-08-19 18:34:58 EDT	2004-08-19 18:34:58 EDT	1414
00000046.query				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
00000051.query.new			3	2004-08-19 18:34:58 EDT	2004-08-19 18:34:58 EDT	2004-08-19 18:34:58 EDT	2004-08-19 18:34:58 EDT	1808
0000005e.query				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
0000006a.query.new			3	2004-08-19 18:34:59 EDT	2004-08-19 18:34:59 EDT	2004-08-19 18:34:59 EDT	2004-08-19 18:34:59 EDT	4288

Metadata

Name: /img_hackingEC14Dell Latitude Cpi.E01/vol_vol2/WINDOWS/PCHEALTH/HELPCTR/OfflineCache/Professional_32#0409/00000016.query.new
Type: File System
MIME Type: application/octet-stream
Size: 0
File Name Allocation: Unallocated
Metadata Allocation:
Modified: 0000-00-00 00:00:00
Accessed: 0000-00-00 00:00:00

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

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



The screenshot shows a file explorer window with a list of files. The file 'unix_hack.tgz' is selected. The metadata for this file is displayed on the right side of the window.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	376
[parent folder]				2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	232
readme.txt			2	2000-10-20 13:37:08 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	2004-08-20 11:19:49 EDT	232
unix_hack.tgz				2001-08-21 13:43:38 EDT	2004-08-20 11:20:38 EDT	2004-08-20 11:20:38 EDT	2004-08-20 11:19:49 EDT	73498201

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

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

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

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