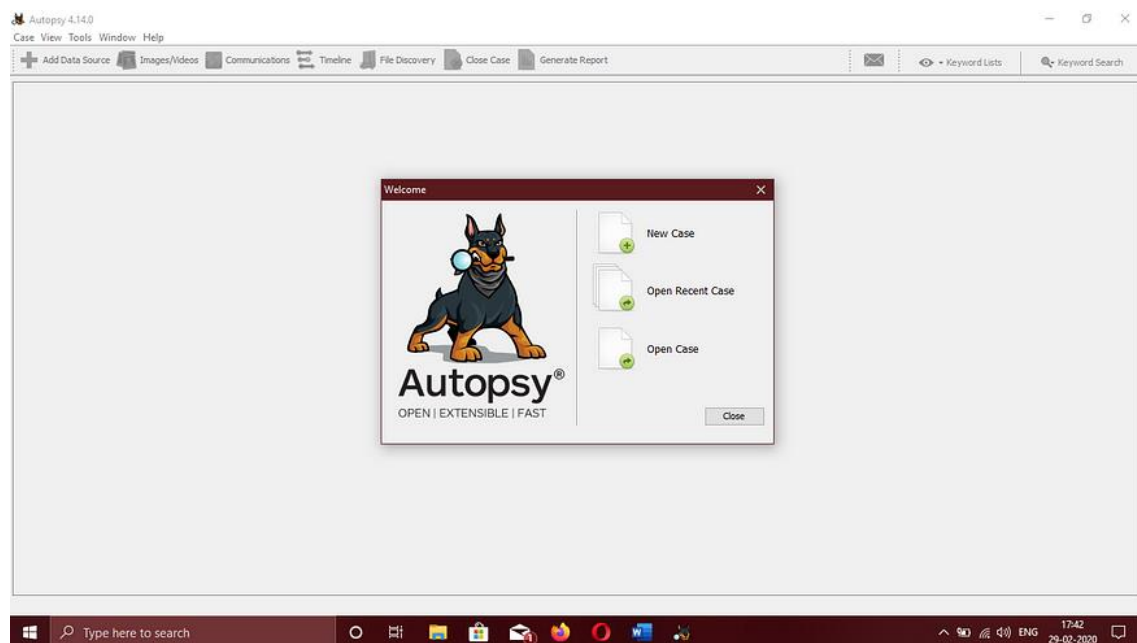


INFORMÁTICA FORENSE: CASO DE HACKING MEDIANTE AUTOPSY

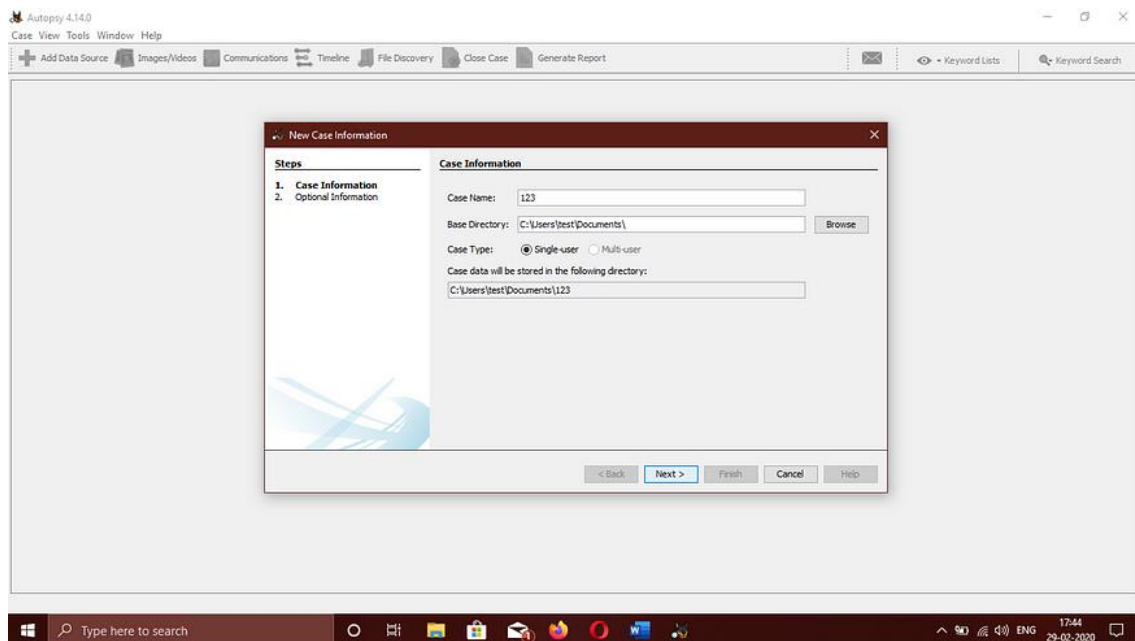
Se sospecha que este ordenador se utilizó con fines de piratería informática, aunque no puede vincularse a un sospechoso de piratería, Greg Schardt. Schardt también se conoce en Internet con el sobrenombre de "Mr. Evil" (Sr. Maldad) y algunos de sus socios han declarado que aparcaba su vehículo dentro del radio de alcance de puntos de acceso inalámbricos donde interceptaba el tráfico de Internet para intentar obtener números de tarjetas de crédito, nombres de usuario y contraseñas. Encuentra cualquier software de pirateo, pruebas de su uso y cualquier dato que pueda haberse generado. Intentar relacionar el ordenador con el sospechoso, Greg Schardt.

Para el análisis de la imagen, estoy utilizando el software de código abierto Autopsy para Windows (no es necesario registrarse para descargarlo): <https://www.autopsy.com/download/>

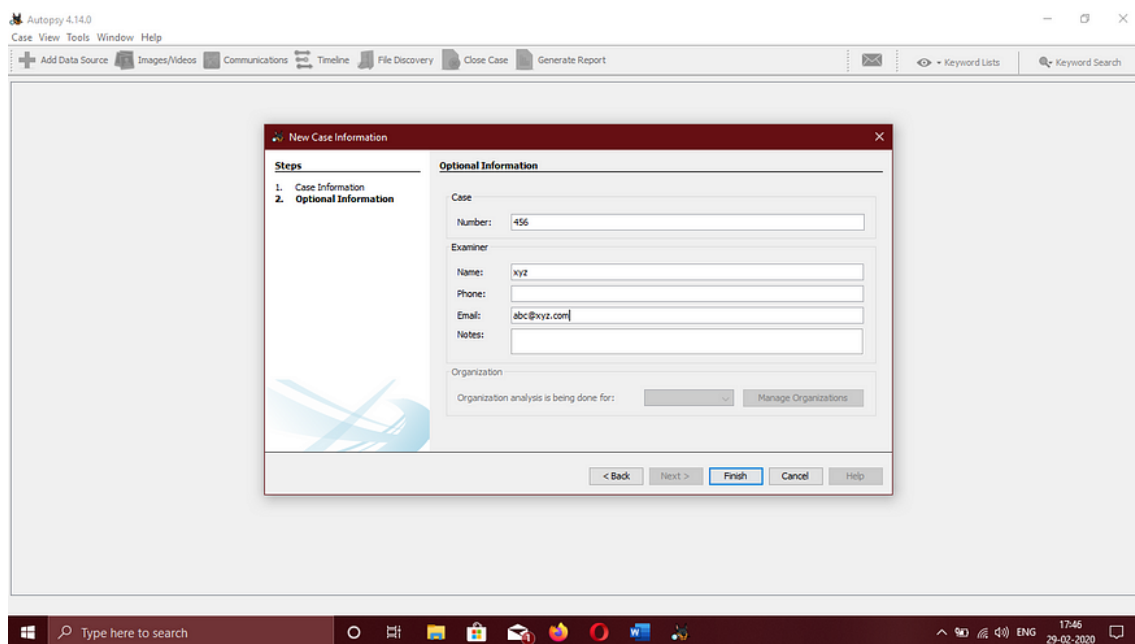
PASO 1: EJECUTE AUTOPSIA Y SELECCIONE NUEVO CASO.



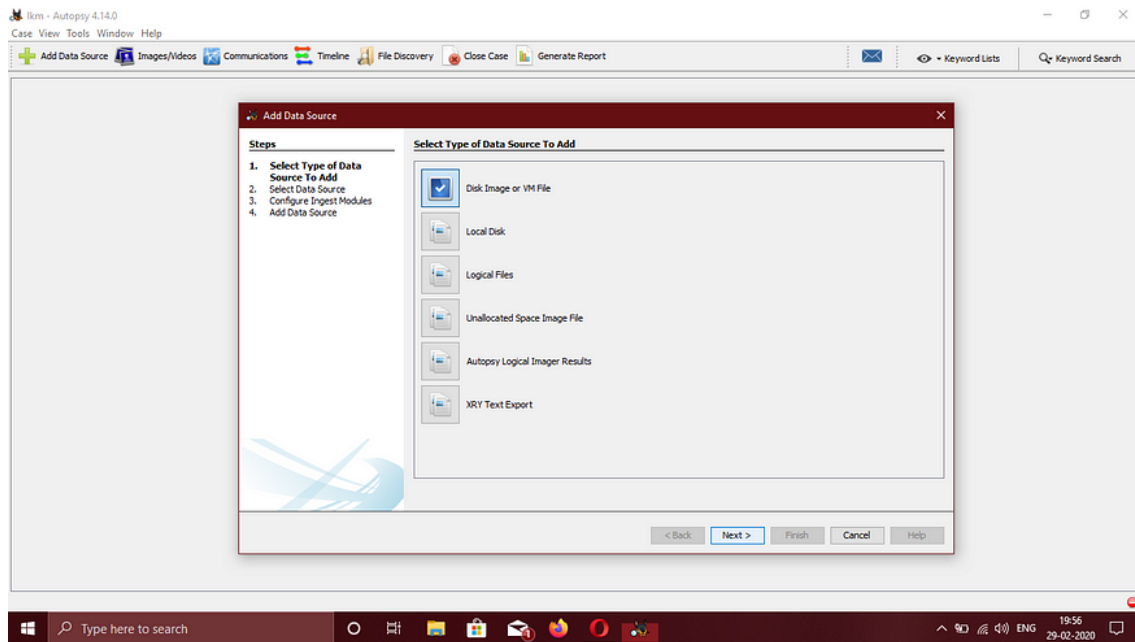
PASO 2: PROPORCIONE EL NOMBRE DEL CASO Y EL DIRECTORIO PARA ALMACENAR EL ARCHIVO DEL CASO. HAGA CLIC EN SIGUIENTE.



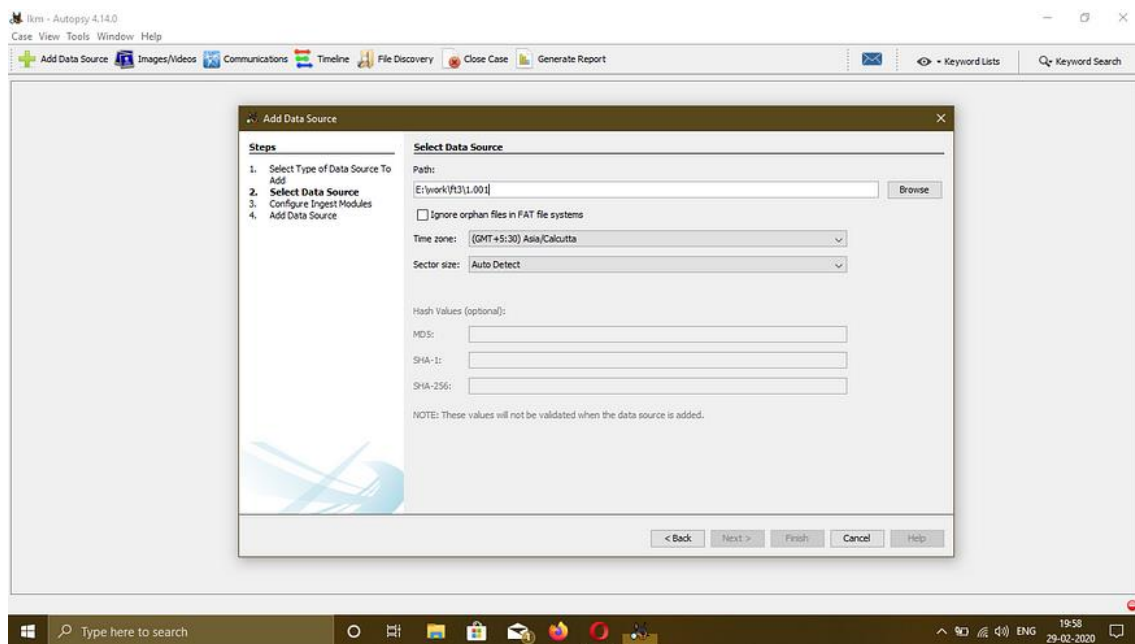
PASO 3: AÑADA EL NÚMERO DE CASO Y LOS DATOS DEL EXAMINADOR Y HAGA CLIC EN FINALIZAR.



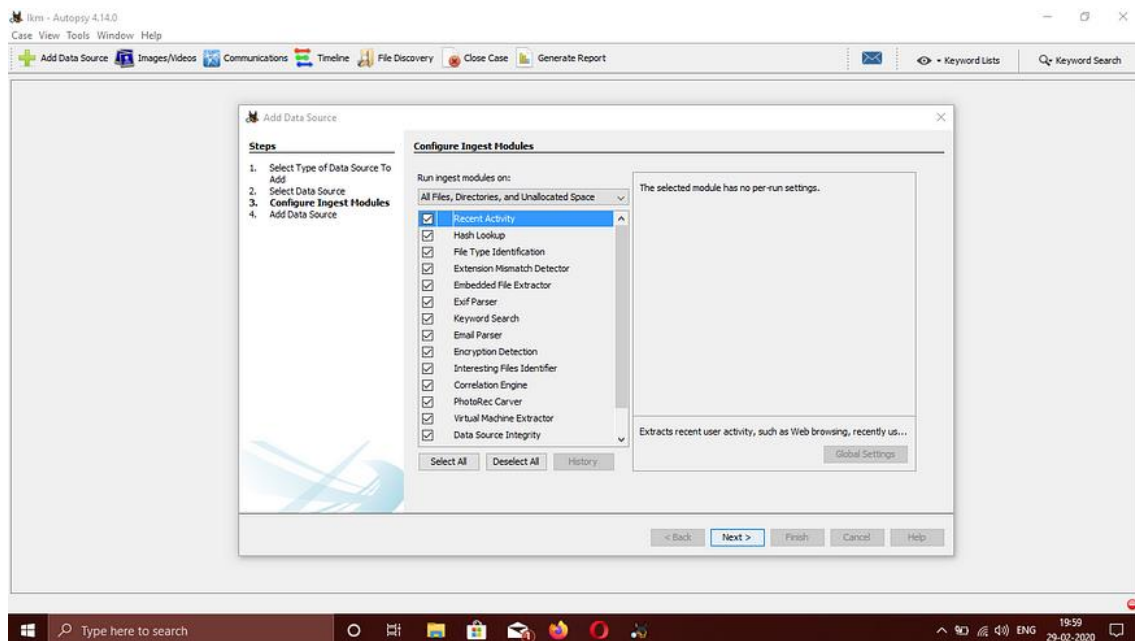
PASO 4: ELIJA EL TIPO DE FUENTE DE DATOS REQUERIDO, EN ESTE CASO IMAGEN DE DISCO Y HAGA CLIC EN SIGUIENTE.



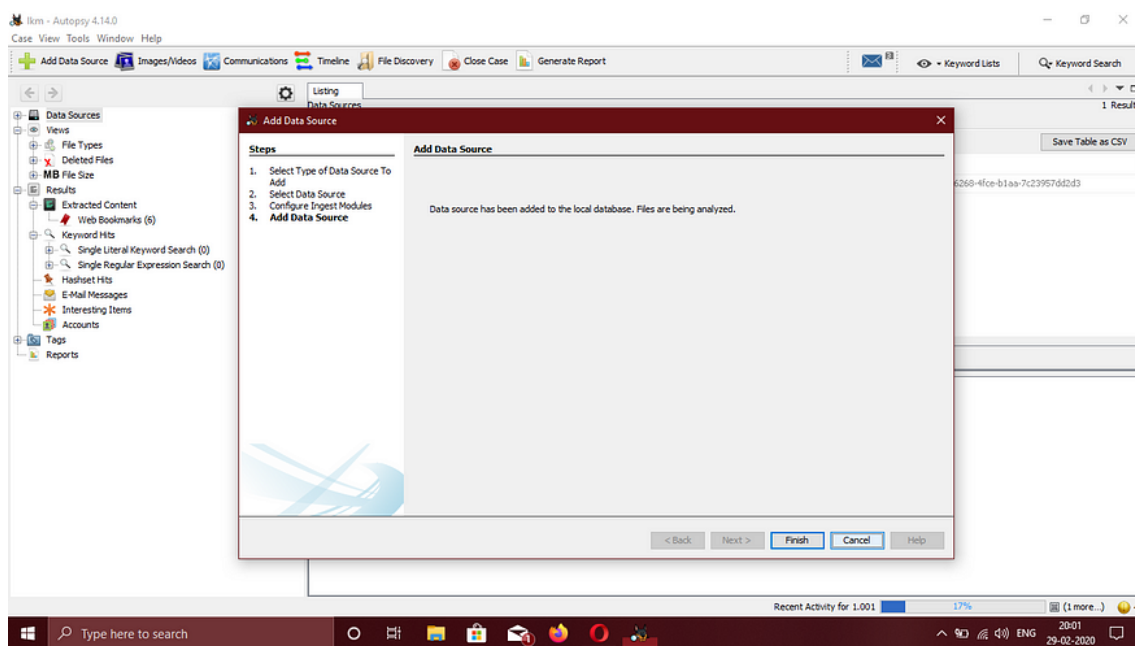
PASO 5: INDIQUE LA RUTA DE LA FUENTE DE DATOS Y HAGA CLIC EN SIGUIENTE.



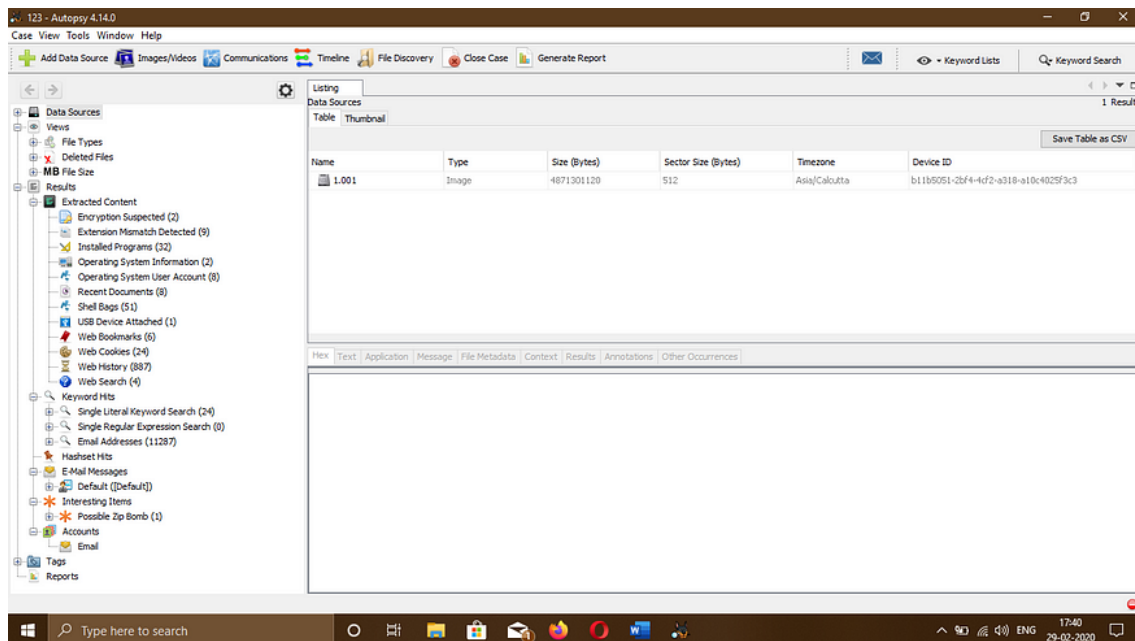
PASO 6: SELECCIONE LOS MÓDULOS NECESARIOS Y HAGA CLIC EN SIGUIENTE.



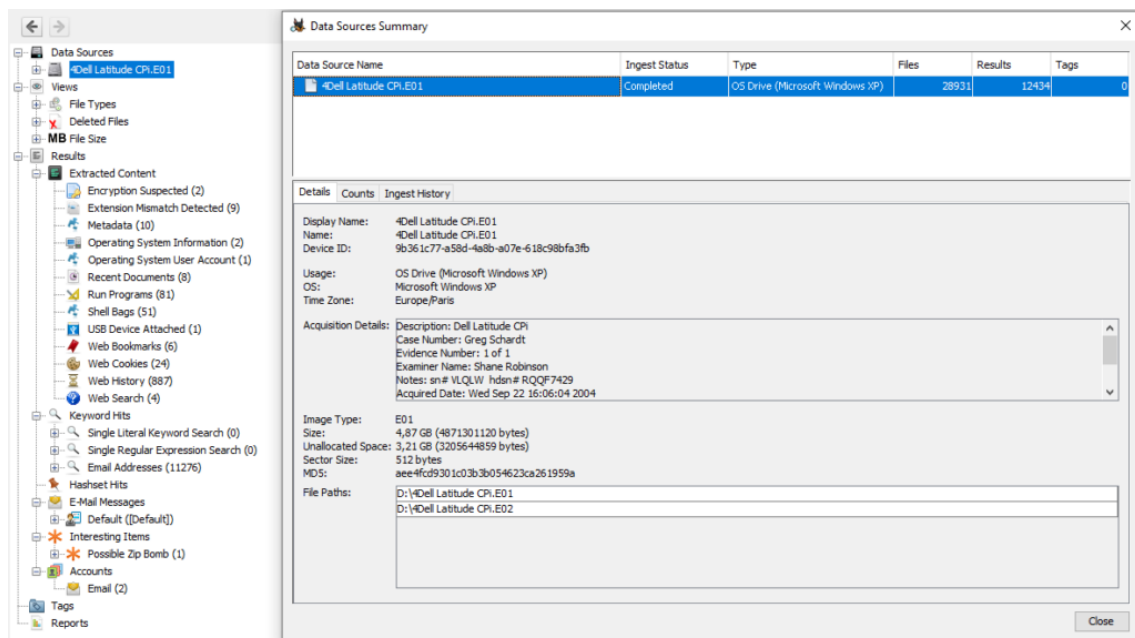
PASO 7: UNA VEZ AÑADIDA LA FUENTE DE DATOS, HAGA CLIC EN FINALIZAR.



PASO 8: SE LLEGA AQUÍ UNA VEZ QUE TODOS LOS MÓDULOS HAN SIDO INGESTADOS. PUEDE EMPEZAR A INVESTIGAR, PERO LE RECOMIENDO QUE ESPERE HASTA QUE FINALICE EL ANÁLISIS Y LA COMPROBACIÓN DE INTEGRIDAD.



La instalación es bastante sencilla. Una vez hecho esto, sólo tienes que iniciar un nuevo "Caso" en Autopsy cargando la imagen forense. Entonces aterrizarás en la pantalla principal de este bonito software. En esta pantalla principal, encontrarás la imagen en la parte superior izquierda. Haz clic con el botón derecho y selecciona "Ver información resumida", y encontrarás información básica que te permitirá responder a las primeras preguntas.



RESPUESTAS

1. ¿Cuál es el hash de la imagen? ¿Coinciden el hash de adquisición y el de verificación?

El hash es un MD5, su valor es AEE4FCD9301C03B3B054623CA261959A. Sólo para recordar, se trata de un identificador único procedente de un cálculo del algoritmo MD5 aplicado al contenido del archivo. Permite una identificación única del fichero de origen

Sin embargo, no se indica el hash de adquisición, por lo que no puedo comparar el hash de adquisición con el de verificación.

2. ¿Qué sistema operativo se utilizó en el ordenador?

Se puede ver inmediatamente que es un sistema operativo Windows XP.

Mirando en el archivo C:\boot.ini, encontramos que es una versión Profesional

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known
boot.ini				2004-08-19 17:35:37 CEST	2004-08-19 17:35:37 CEST	2004-08-19 17:35:37 CEST	2004-08-19 17:35:37 CEST	104	Allocated	Flagged	unknown

3. ¿Cuál fue la fecha de instalación?

Parece que inicialmente se instaló una versión de Windows 98, seguida de una instalación de Windows XP (proceso de actualización) el 19/08/2004 a las 17:35:37 horas

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known
boot.ini				2004-08-19 17:35:37 CEST	2004-08-19 17:35:37 CEST	2004-08-19 17:35:37 CEST	2004-08-19 17:35:37 CEST	104	Allocated	Flagged	unknown

4. ¿Cuál es la configuración de la zona horaria?

Usando Autopsy, podemos navegar a través del registro. Se encuentra en la carpeta WindowsSystem32\Config. En este directorio, podemos navegar a través de los archivos en la ventana superior derecha de Autopsy, que permite que la información del registro se despliegue en la ventana inferior derecha. Allí vamos.

En primer lugar, tenemos una clave de registro del sistema establecido en "Central Standard Time" zona, en system\ControlSet001\Control\TimeZoneInformation :

The screenshot shows the Windows Registry Editor with the path `system32\config\software\Microsoft\Windows NT\CurrentVersion\Time Zones`. The 'Time Zones' value is highlighted, displaying a list of time zones. The 'GMT-06:00' time zone is selected, and its details are shown in the right pane.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known
SECURITY.LOG		3		2004-08-27 17:32:56 CEST	2004-08-27 17:32:56 CEST	2004-08-27 17:32:56 CEST	2004-08-19 18:59:55 CEST	1024	Allocated	Allocated	unknown
software		2		2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	8650752	Allocated	Allocated	unknown
software.sav		3		2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	1024	Allocated	Allocated	unknown
software.sav		3		2004-08-19 18:56:20 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:10 CEST	630784	Allocated	Allocated	unknown
SysEvent.Evt		2		2004-08-27 17:46:29 CEST	2004-08-27 17:46:29 CEST	2004-08-27 17:46:29 CEST	2004-08-19 18:59:15 CEST	65536	Allocated	Allocated	unknown
system		2		2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	2621440	Allocated	Allocated	unknown
system.LOG		3		2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	1024	Allocated	Allocated	unknown
system.sav		3		2004-08-19 18:56:20 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:14 CEST	389120	Allocated	Allocated	unknown
TempKey.LOG		3		2004-08-19 18:56:18 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:14 CEST	1024	Allocated	Allocated	unknown
userdiff		3		2004-08-19 18:56:20 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:08 CEST	262144	Allocated	Allocated	unknown
userdiff.LOG		3		2004-08-19 18:56:20 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:08 CEST	1024	Allocated	Allocated	unknown
userdiff.LOG		0		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	Unallocated		unknown

En segundo lugar, tenemos otra clave de registro importante en `software\Microsoft\Windows NT\CurrentVersion\Time Zones`, que contiene la zona horaria exacta : GMT - 06:00

The screenshot shows the Windows Registry Editor with the path `system32\config\software\Microsoft\Windows NT\CurrentVersion\Time Zones`. The 'Time Zones' value is highlighted, displaying a list of time zones. The 'GMT-06:00' time zone is selected, and its details are shown in the right pane.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known
SAM.LOG		3		2004-08-27 17:08:23 CEST	2004-08-27 17:08:23 CEST	2004-08-27 17:08:23 CEST	2004-08-19 18:58:55 CEST	1024	Allocated	Allocated	unknown
SecEvent.Evt		2		2004-08-19 18:59:15 CEST	2004-08-19 19:02:15 CEST	2004-08-19 18:59:15 CEST	2004-08-19 18:59:15 CEST	65536	Allocated	Allocated	unknown
SECURITY		3		2004-08-27 17:46:33 CEST	2004-08-20 01:04:03 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:59:55 CEST	262144	Allocated	Allocated	unknown
SECURITY.LOG		3		2004-08-27 17:32:56 CEST	2004-08-27 17:32:56 CEST	2004-08-27 17:32:56 CEST	2004-08-19 18:59:55 CEST	1024	Allocated	Allocated	unknown
software		2		2004-08-27 17:46:33 CEST	2004-08-27 17:29:44 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	8650752	Allocated	Allocated	unknown
software.LOG		3		2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	1024	Allocated	Allocated	unknown
software.sav		3		2004-08-19 18:56:20 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:10 CEST	630784	Allocated	Allocated	unknown
SysEvent.Evt		2		2004-08-27 17:46:29 CEST	2004-08-27 17:46:29 CEST	2004-08-27 17:46:29 CEST	2004-08-19 18:59:15 CEST	65536	Allocated	Allocated	unknown
system		2		2004-08-27 17:46:33 CEST	2004-08-27 17:31:44 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	2621440	Allocated	Allocated	unknown
system.LOG		3		2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	1024	Allocated	Allocated	unknown
system.sav		3		2004-08-19 18:56:20 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:14 CEST	389120	Allocated	Allocated	unknown
TempKey.LOG		3		2004-08-19 18:56:18 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:14 CEST	1024	Allocated	Allocated	unknown

5. ¿Quién es el propietario registrado?

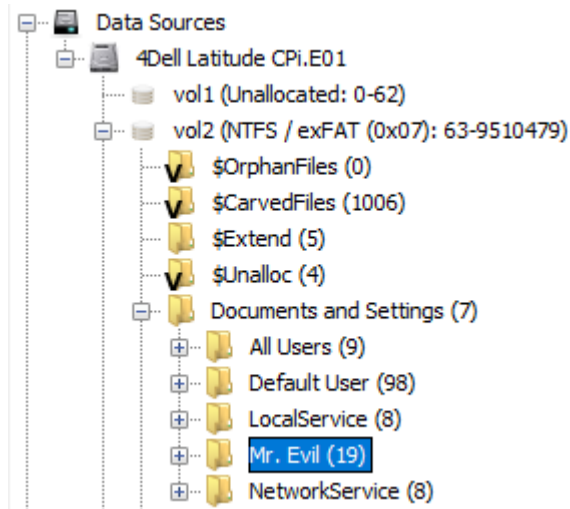
En `software\Microsoft\Windows NT\CurrentVersion`, encontramos que el propietario registrado es Greg Schardt

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
			CurrentVersion				
			Accessibility				
			AeDebug				
			Asr				
			Classes				
			Compatibility				
			Compatibility32				
			Console				
			Drivers				
			drivers.desc				
			Drivers32				
			EFS				
			Embedding				
			Event Viewer				
			File Manager				
			Font Drivers				
			FontDPI				
			FontMapper				
			Fonts				
			FontSubstitutes				
			GRE_Initialize				
			HotFix				
			ICM				
			Image File Execution Options				

Metadata		
Name: CurrentVersion		
Number of subkeys: 57		
Number of values: 17		
Values		
Name	Type	Value
CurrentBuild	REG_SZ	1.511.1 () (Obsolete data - do not use)
InstallDate	REG_DWORD	0x41252e3b (1092955707)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganization	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
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\
PathName	REG_SZ	C:\WINDOWS
ProductId	REG_SZ	55274-640-0147306-23684
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 35 35 32 37 34 2D 36 34...
LicenseInfo	REG_BIN	34 54 AE DC C7 2E 3D E5 8B 15 06 1A 8C 74 A6 55...

6. ¿Cuál es el nombre de la cuenta del ordenador?

Se puede encontrar en Documents and Settings : Mr. Evil



O, también se puede encontrar en el registro, en el archivo SAM


Listing

CPI.E01/vol_vol2/WINDOWS/system32/config

Table
Thumbnail

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
systemprofile				2004-08-20 00:48:25 CEST	2004-08-20 00:48:25 CEST	2004-08-27 17:31:27 CEST	2004-08-20 00:48:25 CEST	56
AppEvent.Evt			2	2004-08-27 17:46:29 CEST	2004-08-27 17:46:29 CEST	2004-08-27 17:46:29 CEST	2004-08-19 18:59:14 CEST	65536
default			3	2004-08-27 17:46:33 CEST	2004-08-20 00:53:22 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	262144
default.LOG			3	2004-08-27 17:32:56 CEST	2004-08-27 17:32:56 CEST	2004-08-27 17:32:56 CEST	2004-08-19 18:56:08 CEST	1024
default.sav			3	2004-08-19 18:56:20 CEST	2004-08-19 19:02:15 CEST	2004-08-19 02:00:00 CEST	2004-08-19 18:56:18 CEST	90112
SAM			3	2004-08-27 17:46:33 CEST	2004-08-20 00:35:21 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:58:55 CEST	262144
SAM.LOG			3	2004-08-27 17:08:23 CEST	2004-08-27 17:08:23 CEST	2004-08-27 17:08:23 CEST	2004-08-19 18:58:55 CEST	1024
SecEvent.Evt			2	2004-08-19 18:59:15 CEST	2004-08-19 19:02:15 CEST	2004-08-19 18:59:15 CEST	2004-08-19 18:59:15 CEST	65536
SECURITY			3	2004-08-27 17:46:33 CEST	2004-08-20 01:04:03 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:58:55 CEST	262144
SECURITY.LOG			3	2004-08-27 17:32:56 CEST	2004-08-27 17:32:56 CEST	2004-08-27 17:32:56 CEST	2004-08-19 18:58:55 CEST	1024
software			2	2004-08-27 17:46:33 CEST	2004-08-27 17:29:44 CEST	2004-08-27 17:46:33 CEST	2004-08-19 18:56:08 CEST	8650752
software.LOG			3	2004-08-27 17:46:32 CEST	2004-08-27 17:46:32 CEST	2004-08-27 17:46:32 CEST	2004-08-19 18:56:08 CEST	1024

Winlogon

GPEExtensions
Notify
SpecialAccounts
AutoRestartShell
DefaultDomainName
DefaultUserName
LegalNoticeCaption
LegalNoticeText
PowerdownAfterShutdown
ReportBootOk
Shell
ShutdownWithoutLogon
System
Userinit
VmApplet
SfcQuota
allocatcdroms
allocatcdasd
allocatfloppies
cachedlogonscount

Metadata
Name: Winlogon
Number of subkeys: 3
Number of values: 31

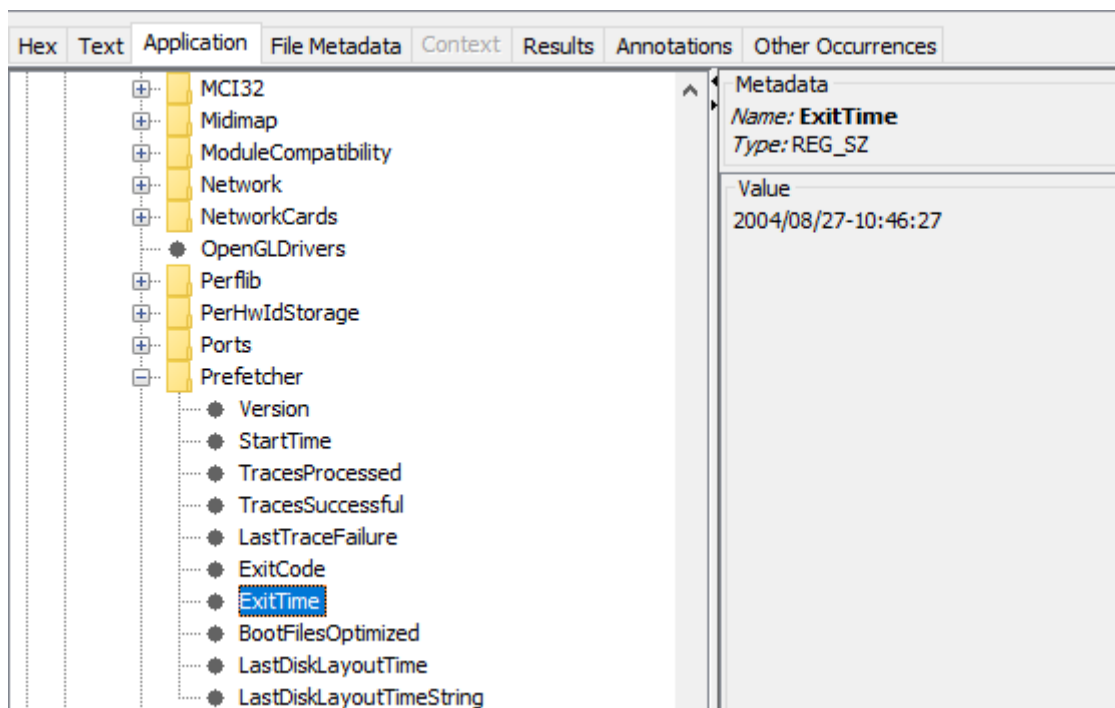
Name	Type	Value
AutoRestartShell	REG_DWORD	0x00000001 (1)
DefaultDomainName	REG_SZ	N-1A9ODN6ZK4LQ
DefaultUserName	REG_SZ	Mr. Evil
LegalNoticeCaption	REG_SZ	(value not set)
LegalNoticeText	REG_SZ	(value not set)
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1
Shell	REG_SZ	Explorer.exe
ShutdownWithoutLogon	REG_SZ	0
System	REG_SZ	(value not set)
Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe,
VmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"
SfcQuota	REG_DWORD	0xffffffff (4294967295)
allocatcdroms	REG_SZ	0
allocatcdasd	REG_SZ	0

8. ¿Cuándo se registró por última vez la fecha/hora de apagado del ordenador?

Para encontrar esto, vamos a la siguiente clave del registro:

software\Microsoft\WindowsNT\CurrentVersion\Prefetcher\ExitTime

Encontramos una fecha/hora de apagado del 27/08/2004-10:46:27



9. ¿Cuántas cuentas hay registradas (número total)?

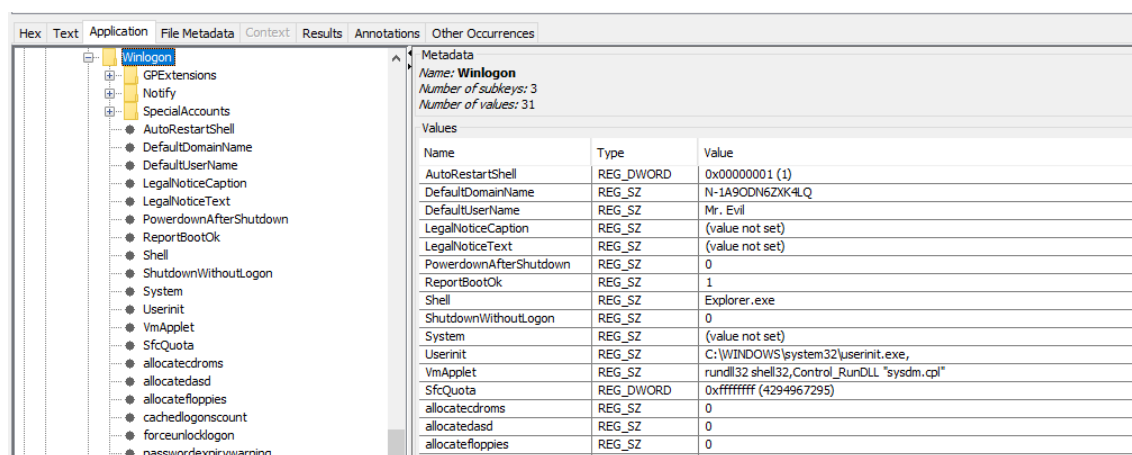
En la pregunta 6, ya habíamos encontrado los 5 nombres de usuario: Administrator, Guest, HelpAssistant, Mr. Evil, SUPPORT_388945a0

10. ¿Cuál es el nombre de cuenta del usuario que más utiliza el ordenador?

Mr. Evil es el único usuario real de este ordenador, como se puede ver en Cuenta de usuario del sistema operativo. (1)

11. ¿Quién fue el último usuario que se conectó al ordenador?

El nombre del último usuario que inició sesión con éxito aparece en la clave DefaultUserName en software\Microsoft\Windows NT\CurrentVersion\Winlogon: ¡es el Sr. Maligno!



12. Una búsqueda por el nombre de "Greg Schardt" revela múltiples resultados. Una de ellas demuestra que Greg Schardt es Mr. Evil y también el administrador de este ordenador. ¿De qué archivo se trata? ¿Con qué programa de software está relacionado este archivo?

Hemos visto que Greg Schardt es el propietario registrado del aparato, mientras que el Sr. Maligno es el único usuario del sistema. Por lo tanto, podemos creer que se trata de la misma persona

La búsqueda del nombre Greg Schardt nos lleva a este resultado:

ListingKeyword search 5 - Greg SchardtX

Keyword search

TableThumbnail

Name	Keyword Preview	Location	Modified Time	Ch
irunin.ini	HT%=<600%REGOWNER%=<Greg Schardt<%REGORGANI...	/img_4Dell Latitude CPE01/vol_vol2/Program Files/Look@L...	2004-08-25 17:56:10 CEST	20K
Unalloc_20050_351232_1683209728	REG_SZValue data = <Greg Schardt<(On Error) User no	/img_4Dell Latitude CPE01/vol_vol2//Unalloc/Unalloc_20...	0000-00-00 00:00:00	00K
Unalloc_20050_1684736000_3639811072	Companyil SoNone<Greg Schardt<C:\WINDOWS\System32...	/img_4Dell Latitude CPE01/vol_vol2//Unalloc/Unalloc_20...	0000-00-00 00:00:00	00K
Look@LAN Setup Log.txt	REG_SZValue data = <Greg Schardt<(On Error) User no	/img_4Dell Latitude CPE01/vol_vol2/WINDOWS/Look@LA...	2004-08-25 17:56:33 CEST	20K
drwtsn32.log	Registered Owner: <Greg Schardt<*-----> Task List <-----*	/img_4Dell Latitude CPE01/vol_vol2/Documents and Sett...	2004-08-20 17:25:48 CEST	20K
software	OoRegisteredOwner<Greg Schardt<26008XxCurriSoft	/img_4Dell Latitude CPE01/vol_vol2/WINDOWS/repair/sof...	2004-08-20 00:49:11 CEST	20K
software	Companyil SoNone<Greg Schardt<C:\WINDOWS\System32...	/img_4Dell Latitude CPE01/vol_vol2/WINDOWS/system32...	2004-08-27 17:46:33 CEST	20K
Operating System Information Artifact	7306-23684Owner : <Greg Schardt<Organization : N/A	/img_4Dell Latitude CPE01/vol_vol2/WINDOWS/system32...	2004-08-27 17:46:33 CEST	20K
AppEvent.Evt	Registered Owner: <Greg Schardt<*-----> Task List <-----*	/img_4Dell Latitude CPE01/vol_vol2/WINDOWS/system32...	2004-08-27 17:46:29 CEST	20K

irunin.ini - Properties

Properties

Name	irunin.ini
Keyword Preview	HT%=<600%REGOWNER%=<Greg Schardt<%REGORGANIZATION%=<N/A
Location	/img_4Dell Latitude CPE01/vol_vol2/Program Files/Look@LAN/irunin.ini
Modified Time	2004-08-25 17:56:10 CEST
Change Time	2004-08-25 17:56:10 CEST
Access Time	2004-08-25 17:56:10 CEST
Created Time	2004-08-25 17:56:09 CEST
Size	18197
Flags(Dir)	Allocated
Flags(Meta)	Allocated
Known	unknown
MD5 Hash	4cae7cbee2c6022cbf9e30874042c091
MIME Type	text/x-ini
Extension	ini

irunin.ini

CloseHelp

Podemos ver, en Archivos de Programa, un programa llamado Look@LAN. Se trata de una aplicación portable que permite al usuario controlar qué clientes están conectados a una red local (LAN = Local Area Network) : <https://www.majorgeeks.com/files/details/looklan.html>

Los Archivos de Programa Look@LANirunin.ini nos vinculan a Mr. Evil como usuario de LAN, ilo que nos prueba el vínculo con Greg Schardt!

Listing










Keyword search 5 - Greg Schardt

X

Keyword search

Table

Thumbnail

Name	Keyword Preview	Location
 irunin.ini	HT%=600%REGOWNER%=«Greg Schardt«%REGORGANI...	/img_4Dell Latitude CPl.E01/vol_vol2/Program Files/Look@L...
 Unalloc_20050_351232_1683209728	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_4Dell Latitude CPl.E01/vol_vol2//\$Unalloc/Unalloc_20...
 Unalloc_20050_1684736000_3639811072	Companyil SoNome«Greg Schardt«C:\WINDOWS\System32...	/img_4Dell Latitude CPl.E01/vol_vol2//\$Unalloc/Unalloc_20...
 Look@LAN Setup Log.txt	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_4Dell Latitude CPl.E01/vol_vol2/WINDOWS/Look@LA...
 drwtsn32.log	Registered Owner: «Greg Schardt«*-----> Task List <----*	/img_4Dell Latitude CPl.E01/vol_vol2/Documents and Sett...
 software	OoRegisteredOwner«Greg Schardt«26008xxCurriSoft	/img_4Dell Latitude CPl.E01/vol_vol2/WINDOWS/repair/sof...
 software	Companyil SoNome«Greg Schardt«C:\WINDOWS\System32...	/img_4Dell Latitude CPl.E01/vol_vol2/WINDOWS/system32...
 Operating System Information Artifact	7306-23684Owner : «Greg Schardt«Organization : N/A	/img_4Dell Latitude CPl.E01/vol_vol2/WINDOWS/system32...
 AppEvent.Evt	Registered Owner: «Greg Schardt«*-----> Task List <----*	/img_4Dell Latitude CPl.E01/vol_vol2/WINDOWS/system32...

<

Hex

Text

Application

File Metadata

Context

Results

Annotations

Other Occurrences

Strings

Indexed Text

Translation

Page: 1 of 1 Page

<

>

Matches on page: 1 of 2 Match

<

>

100%

Reset

```

irunin.ini [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-1A90DN6ZXK4LQ
%RANDOMMAIN%=N-1A90DN6ZXK4LQ
%LANUSER%=Mr. Evil

```

13. Enumera las tarjetas de red utilizadas por este ordenador

Hay 2 tarjetas de red en uso en el software\Microsoft\Windows NT\CurrentVersion\NetworkCards :

Tarjeta PC Compaq WL110 Wireless LAN



Xircom CardBus Ethernet 100 + Módem 56 (Interfaz Ethernet)



14. Este mismo fichero informa de la dirección IP y la dirección MAC del ordenador. ¿Qué son?

La pregunta no es clara de inmediato, pero usted consigue la idea cuando se considera el software Look@LAN supervisa los clientes conectados a la red local. Para buscar de nuevo el archivo que ya hemos abierto en la pregunta 12, basta con escribir en la barra de búsqueda superior derecha, el nombre de archivo irinin.ini

Dentro de este fichero, encontrará fácilmente lo siguiente :

%LANIP%=192.168.1.111 -> normalmente esta IP identifica un PC en una red local (¡así que tiene sentido encontrar esta IP!)

%LANNIC%=0010a4933e09 -> una simple herramienta de búsqueda de direcciones MAC como <https://rst.im/oui/>, confirmará que es una dirección Xircom. ¡Tiene sentido con la pregunta 13 !

15. Una búsqueda en Internet del nombre del proveedor/modelo de las tarjetas NIC por dirección MAC puede utilizarse para averiguar qué interfaz de red se utilizó. En la respuesta anterior, los 3 primeros caracteres hexadecimales de la dirección MAC indican el proveedor de la tarjeta. ¿Qué tarjeta NIC se utilizó durante la instalación y configuración de LOOK@LAN?

El fichero de configuración de LOOK@LAN es irunun.ini. Abramos de nuevo este fichero. Encontramos la siguiente información dentro de este archivo:

```
irunun.ini [Config]
ConfigFile=C:\Program Files\Look@LAN\irunun.dat
LanguageFile=C:\Program Files\Look@LAN\irunun.lng
ImageFile=C:\Program Files\Look@LAN\irunun.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A90DN6ZXX4LQ
%LANDOMAIN%=N-1A90DN6ZXX4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
```

Entonces, está claro que la NIC - Network Interface Card usada durante la instalación y configuración, es la tarjeta con la dirección MAC 0010a4933e09, que es la Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface).

16. Encontrar 6 programas instalados que pueden ser utilizados para la piratería

Buscando en los Archivos de Programa, es bastante fácil encontrar los siguientes programas :

123WASP : <https://www.techspot.com/downloads/107-123-write-all-stored-passwords.html>

Anonymizer : <https://news.hitb.org/content/anonymizer-launches-free-anonymizer-privacy-tool-ms-ie-browser>

Caín : <https://myhackingworld.com/cain-and-abel/>

Ethereal : <https://hackersonlineclub.com/what-is-ethereal-hacking/>

(NB : desde entonces, se ha renombrado en Wireshark, la famosa herramienta de sniffing de paquetes de red <https://www.wireshark.org/download.html>)

Look@LAN : <https://www.techspot.com/community/topics/look-lan.64758/>

NetStumbler : <https://dudehackingtricks.wordpress.com/2014/08/14/netstumbler-hack-wifi-password/>

17. ¿Cuál es la dirección de correo electrónico SMTP de Mr. Evil?

Para encontrar esta información, puedes mirar en el fichero AGENT.INI. Ver más sobre este archivo en versiones anteriores de Windows:

<https://groups.google.com/forum/#!topic/alt.usenet.offline-reader.forte-agent/23uh0mRbq88>

El archivo se encuentra en Archivos de programa\Agent\Data\AGENT.INI

Encontramos la dirección de correo electrónico de Mr. Evil : whoknowsme@sbcglobal.net

18. ¿Cuál es la configuración NNTP (servidor de noticias) de Mr.

NNTP significa Network News Transfer Protocol (Grupo de noticias / Usenet) : <https://ccnatutorials.in/application-layer-of-tcp-ip/nntp-network-news-transfer-protocol/>

De nuevo, una búsqueda en el archivo AGENT.INI te permitirá encontrar la información.

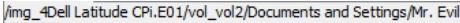
```
[Servers]
NewsServer="news.dallas.sbcglobal.net"
MailServer="smtp.sbcglobal.net"
```

19. ¿Qué dos programas instalados muestran esta información?

Tenemos que buscar el cliente de correo y/o el cliente de Usenet. Una fuente para investigar esto es NTUSER.DAT, que es una fuente forense bien conocida.

Descubrimos que MS Outlook Express revela la dirección de correo electrónico de Mr. Para encontrar esto, usted necesita mirar en NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\UnreadMail

Sólo tienes que escribir NTUSER.DAT en la barra de búsqueda, y navegar en la estructura de archivos



Table

Thumbnail

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
NetHood				2004-08-26 17:08:15 CEST	2004-08-26 17:08:15 CEST	2004-08-26 17:08:15 CEST	2004-08-20 01:04:05 CEST
PrintHood				2004-08-19 19:00:09 CEST	2004-08-20 01:04:06 CEST	2004-08-26 17:07:44 CEST	2004-08-20 01:04:05 CEST
Recent				2004-08-26 17:08:14 CEST	2004-08-26 17:08:14 CEST	2004-08-27 17:14:40 CEST	2004-08-20 01:04:05 CEST
SendTo				2004-08-20 01:04:15 CEST	2004-08-20 01:04:15 CEST	2004-08-20 17:17:59 CEST	2004-08-20 01:04:05 CEST
Start Menu				2004-08-19 19:00:09 CEST	2004-08-20 01:04:06 CEST	2004-08-27 17:08:06 CEST	2004-08-20 01:04:05 CEST
Templates				2004-08-20 00:24:35 CEST	2004-08-20 01:04:06 CEST	2004-08-20 17:17:59 CEST	2004-08-20 01:04:05 CEST
.gtk-bookmarks			0	2004-08-27 17:40:43 CEST	2004-08-27 17:40:43 CEST	2004-08-27 17:40:43 CEST	2004-08-27 17:40:43 CEST
interception			3	2004-08-27 17:41:00 CEST	2004-08-27 17:41:00 CEST	2004-08-27 17:41:00 CEST	2004-08-27 17:41:00 CEST
NTUSER.DAT			2	2004-08-27 17:46:23 CEST	2004-08-27 17:46:13 CEST	2004-08-27 17:46:23 CEST	2004-08-20 01:04:05 CEST
ntuser.dat.LOG			2	2004-08-27 17:46:23 CEST	2004-08-27 17:46:23 CEST	2004-08-27 17:46:23 CEST	2004-08-20 01:04:06 CEST
ntuser.ini			3	2004-08-27 17:46:23 CEST	2004-08-27 17:46:23 CEST	2004-08-27 17:46:23 CEST	2004-08-20 01:04:08 CEST

Hex

Text

Application

File Metadata

Context

Results

Annotations

Other Occurrences

WAB

Windows

CurrentVersion

Applets

Controls Folder

Explorer

Group Policy

GrpConv

Internet

Internet Settings

Policies

Run

Settings

Shell Extensions

Synmgr

Telephony

ThemeManager

Themes

UnreadMail

whoknowsme@sbcglobal.net

MessageCount

TimeStamp

Application

Webcheck

WinTrust

Shell

ShellNoRoam

Windows Help

Windows NT

mIRC

Netscape

Policies

Metadata

Name: whoknowsme@sbcglobal.net

Number of subkeys: 0

Number of values: 3

Values

Name	Type	Value
MessageCount	REG_DWORD	0x00000000 (0)
TimeStamp	REG_BIN	90 0E DC 3D FB 86 C4 01
Application	REG_SZ	msimn

En este momento, no soy capaz de encontrar el segundo programa que revele la misma información... si lo encuentras, ¡por favor, ponlo en la sección de comentarios!

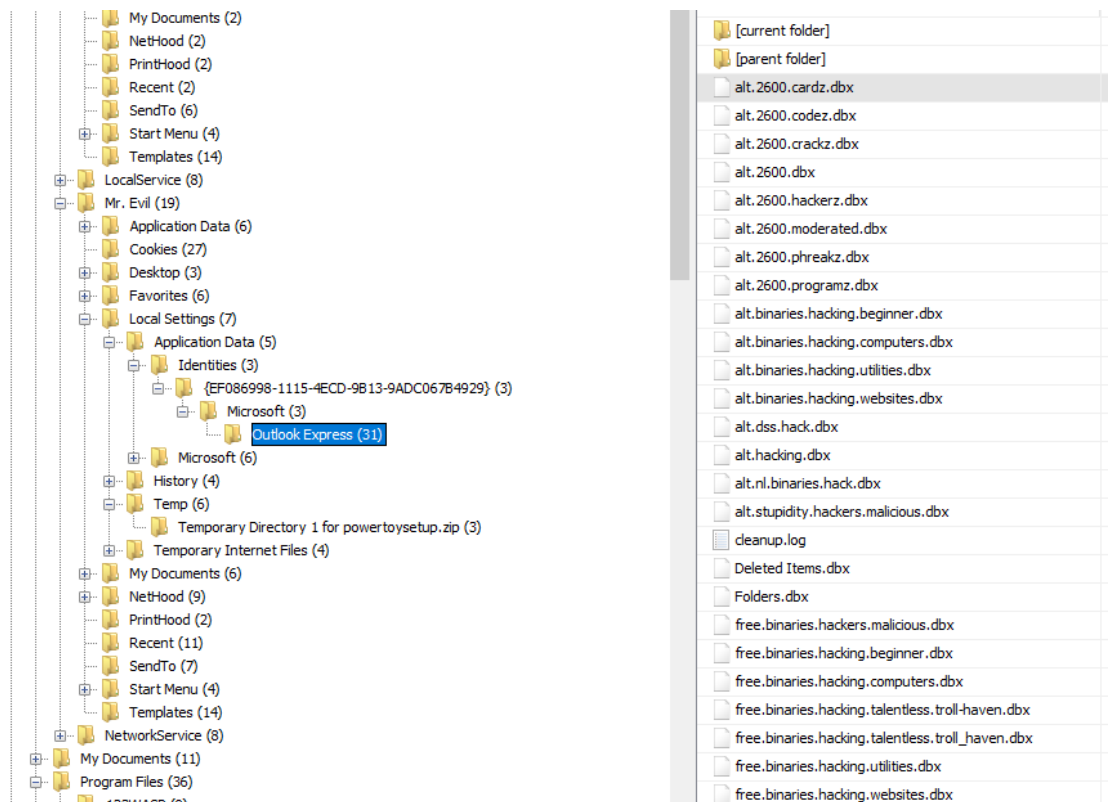
20. ¿Enumera 5 grupos de noticias a los que está suscrito el Sr. Maligno?

Hay un buen artículo para entender el análisis forense de Outlook Express : <https://www.mailxaminer.com/blog/outlook-express-email-forensics/>

Todas las carpetas y mensajes de correo electrónico de Outlook Express, las carpetas IMAP locales y la configuración se almacenan en una carpeta. La ubicación de este directorio es :

Documents and Settings nombre_de_usuario Configuración local Datos de aplicación Identidades Microsoft Outlook Express

Encontramos muchos grupos de noticias a los que el Sr. Maligno se ha suscrito.



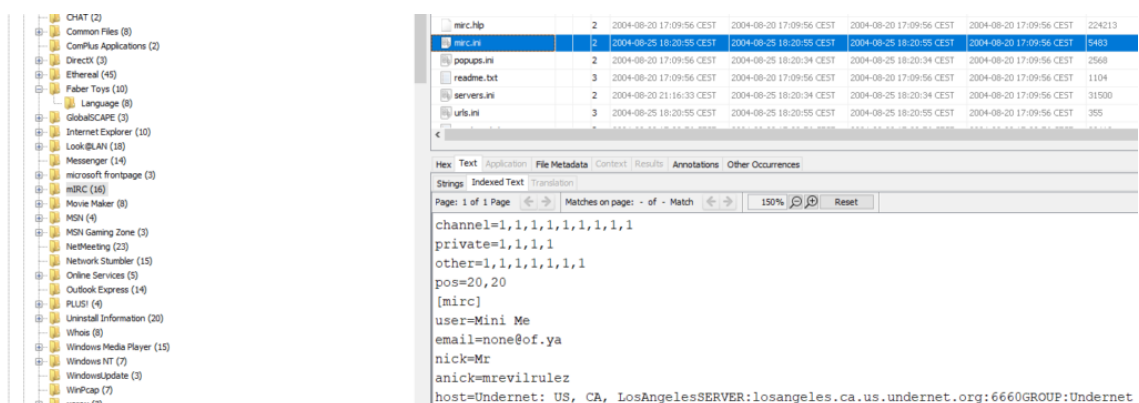
21. Se ha instalado un popular programa de IRC (Internet Relay Chat) llamado MIRC. ¿Cuáles son ¿Cuál es la configuración de usuario que se muestra cuando el usuario está en línea y en un canal de chat?

El programa mIRC (https://www.mirc.com/) se encuentra en los Archivos de Programa.

Sólo tienes que abrir y comprobar a través del mirc.ini y obtendrás la información solicitada

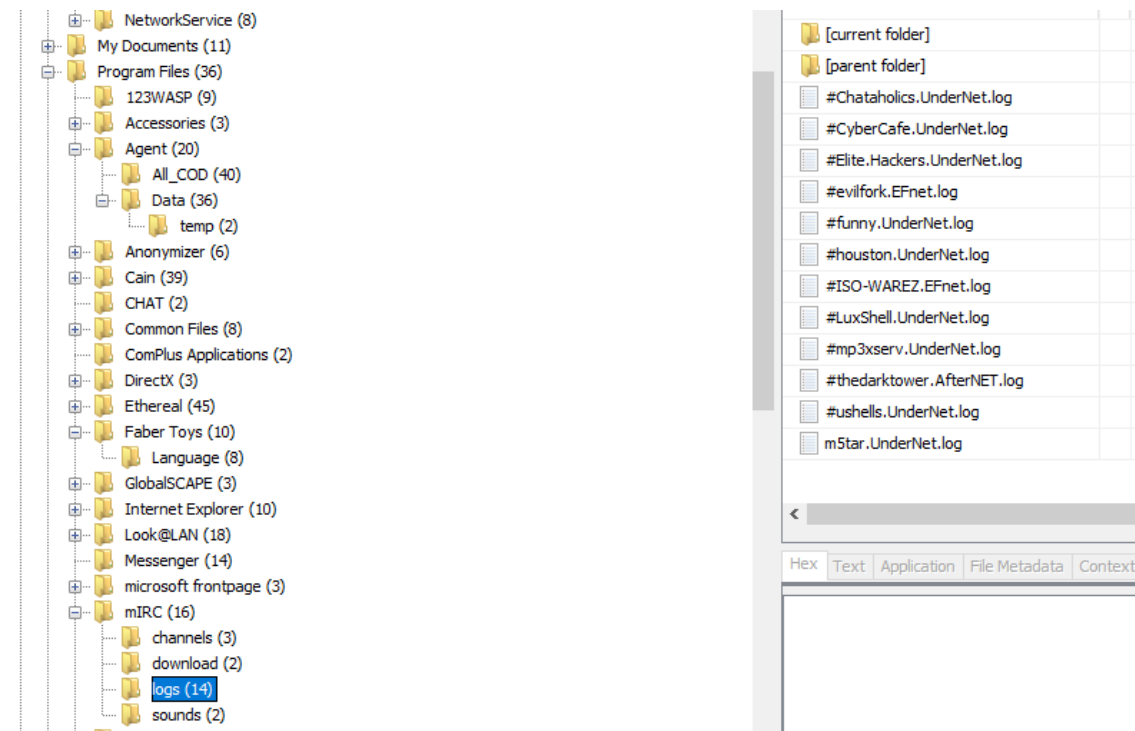
user=Mini
email=none@of.ya
nick=Mr
anick=mrevilrulez

Yo



22. Este programa de IRC tiene la capacidad de registrar sesiones de chat. Enumera 3 canales IRC a los que el usuario de este ordenador accedió.

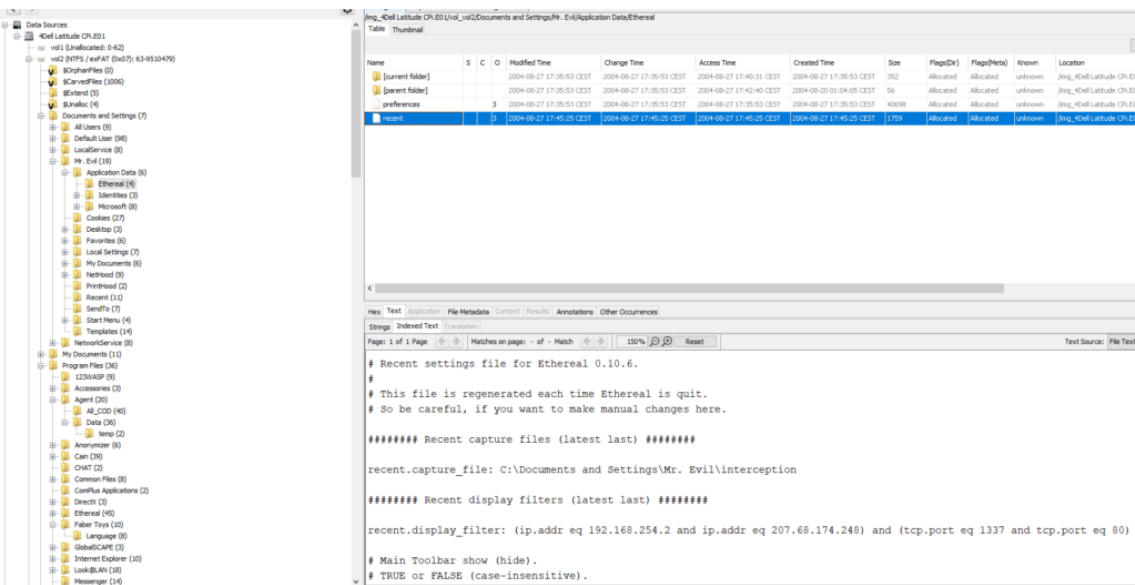
La seccion de log si mIRC en la seccion de Archivos de Programa, revela que hay un directorio "logs". Las sesiones de chat aparecen inmediatamente aquí



23. Ethernet, un popular programa de "sniffing" que puede ser usado para interceptar paquetes de Internet alámbricos e inalámbricos.

paquetes inalámbricos de Internet. Cuando los paquetes TCP son recogidos y reensamblados, el directorio de guardado por defecto es el directorio Mis Documentos del usuario. ¿Cuál es el nombre del archivo que contiene los datos interceptados?

Buscando en el directorio Ethernet, encontramos un archivo "reciente". Al abrir este archivo se revela la información solicitada "intercepción".



24. Ver el archivo en formato de texto revela mucha información sobre quién y qué fue interceptado. ¿Qué tipo de ordenador inalámbrico utilizaba la víctima (la persona a la que se grabó su Internet)?

El archivo de interceptación se puede encontrar escribiendo "interceptación" en la barra de búsqueda de la parte superior derecha de la pantalla de inicio.

ListingKeyword search 7 - interception X

Keyword search

TableThumbnail

Name	Keyword Preview	Location
Words.lst	allow near-silent line <interception> are white.	/img_4Dell Latitude CPI.E01/vol_vol2/My Documents/Dictionary/250MB_WORDLIST.ZIP/Words.lst
Glossary.chm	channel to prevent the <interception> of critical information	/img_4Dell Latitude CPI.E01/vol_vol2/Windows/Help/Glossary.chm
interception	<interception>	/img_4Dell Latitude CPI.E01/vol_vol2/Documents and Settings/Mr. Evil/interception
interception-slack	<interception>-slack	/img_4Dell Latitude CPI.E01/vol_vol2/Documents and Settings/Mr. Evil/interception-slack
test.tab	<interception>	/img_4Dell Latitude CPI.E01/vol_vol2/My Documents/Dictionary/test.zip/test.tab
comexp.chm	applications.<interception>For an object activated	/img_4Dell Latitude CPI.E01/vol_vol2/Windows/Help/comexp.chm

HexTextApplicationFile MetadataContextResultsAnnotationsOther Occurrences

StringsIndexed TextTranslation

Page: 1 of 5 PageMatches on page: 1 of 1 Match150%Reset

interception 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*q6edOGfSSmKzi3lT1CIh6FdbNqQyPyqubrB97DYRuoTwoA5kpliTcf=5ynNj8z2mEi3KQzUnhBOK5dmrXWUam5W2H3bXqJgZE5uFZ7OFVIdTd8rwZLZfLhhQB8q*Sto508d!UJp8ulXjB5g4RJME!*WBUVqwsUvZgDT5F!XAMjAg0!vkXYwzhbCkVlAO1b2zXMj1XnmPnOpETgsIPX0coWMQ\$\$
U/Ay
HTTP/1.1 302 Found

El agente de usuario es un Microsoft Internet Explorer 4.01 que utiliza un Pocket PC con Windows CE, resolución de pantalla 240×320. Te lo dije, ¡es muy vintage!



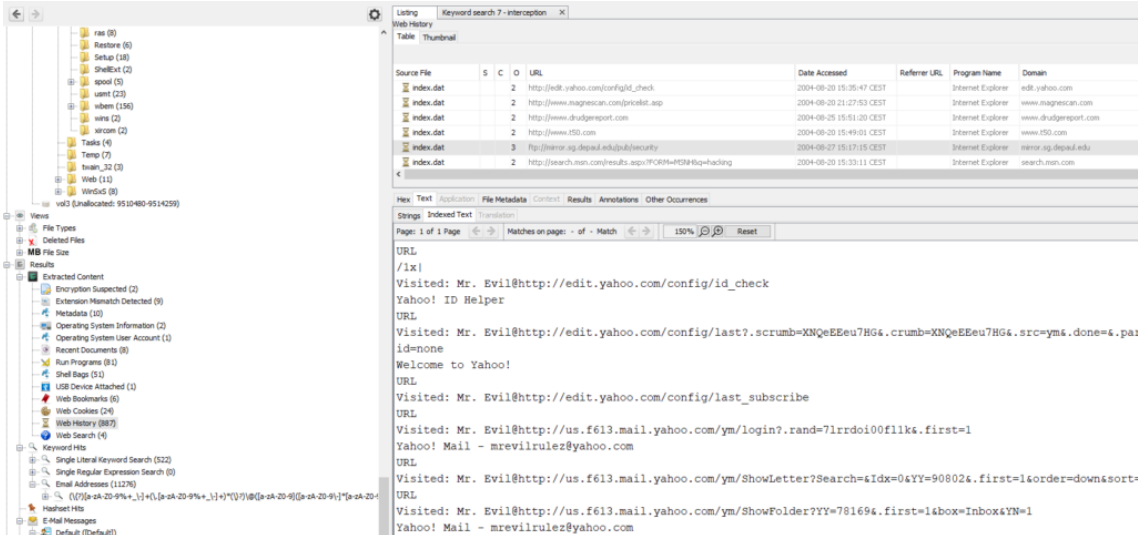
25. ¿A qué sitios web accedía la víctima?

La víctima estaba accediendo a mobile.msn.com, como puede verse en el archivo de interceptación. Más abajo podemos ver que la víctima también estaba utilizando MSN hotmail (correo electrónico).

Host: mobile.msn.com

26. Busca la dirección de correo electrónico del usuario principal. ¿Cuál es?

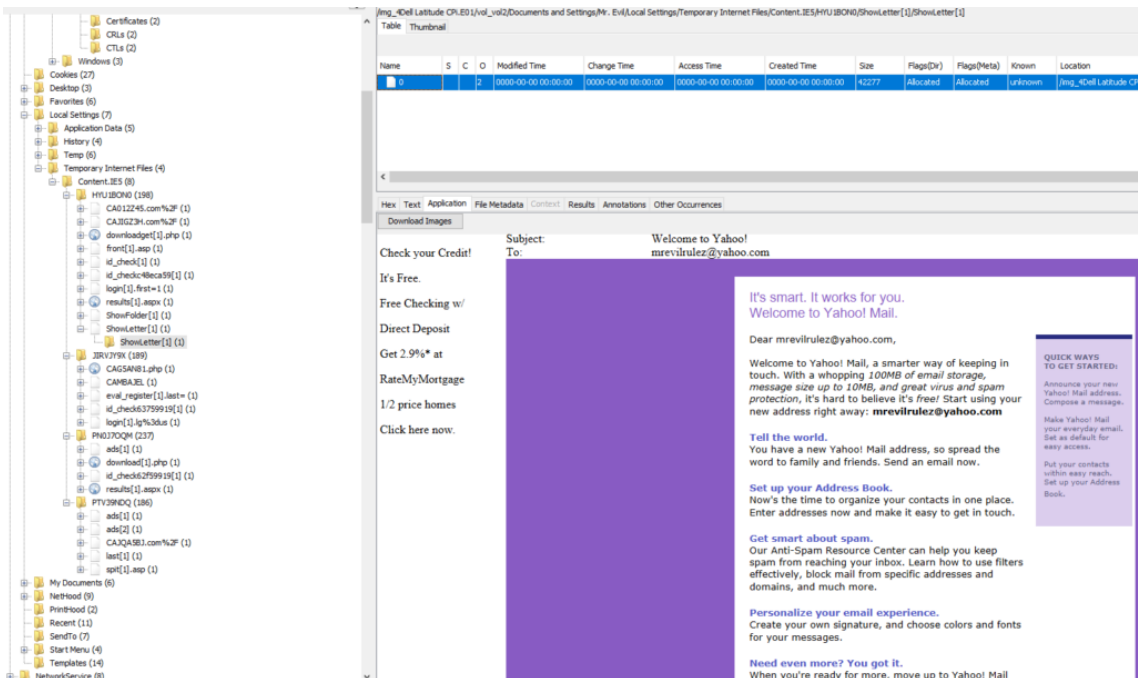
21).



27. Yahoo mail, un popular servicio de correo electrónico basado en la web, guarda copias del correo electrónico bajo ¿qué nombre de archivo?

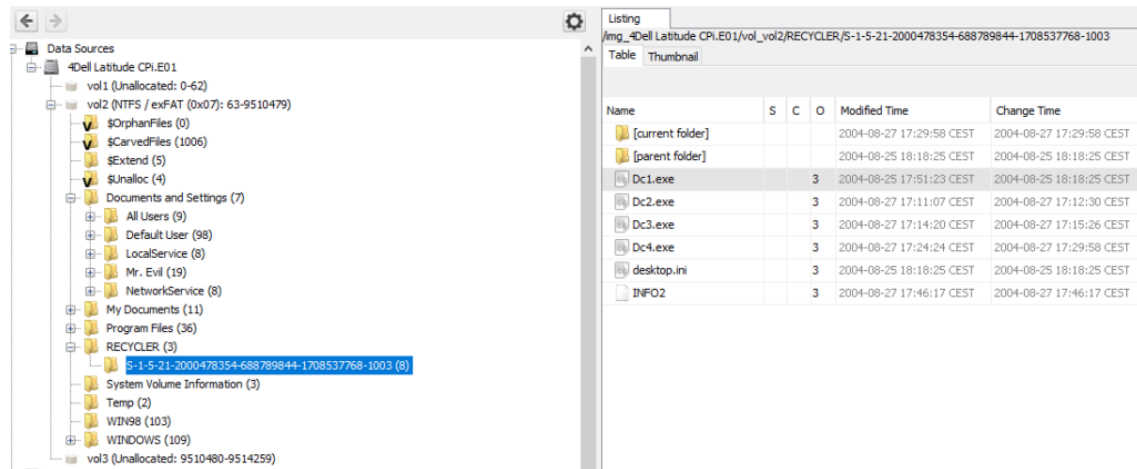
Los correos de Yahoo se guardan en "ShowLetter[1]".

Podemos confirmar la dirección de correo electrónico utilizada por Mr. Evil.



28. ¿Cuántos archivos ejecutables hay en la papelera de reciclaje?

Hay 4 archivos ejecutables en la papelera de reciclaje.

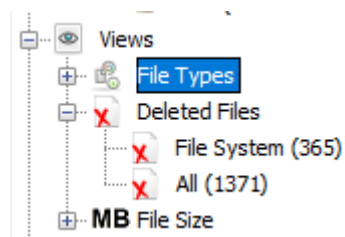


29. ¿Estos archivos son realmente borrados?

¡No, sólo se mueven a la papelera de reciclaje y no se borran...!

30. ¿Cuántos ficheros son realmente borrados por el sistema de ficheros?

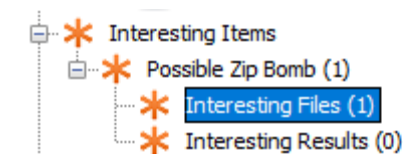
Es muy fácil. Sólo tienes que ir a "Ver" y encontrarás el contador "Todos" -> 1 371 archivos fueron borrados. ¡Gracias a "bobo" por el dato!



31. Realice una comprobación antivirus. ¿Hay algún virus en el ordenador?

Sí, hay una bomba zip presente, unix_hack.tgz

Se encuentra en la sección "Objetos de interés".



Esto es lo que dice Wikipedia sobre las bombas zip

https://en.wikipedia.org/wiki/Zip_bomb ▼

A zip bomb, also known as a zip of death or decompression bomb, is a malicious archive file designed to crash or render useless the program or system reading it. It is often employed to disable antivirus software, in order to create an opening for more traditional viruses.

Overview

Details and use

See also

Rather than hijacking the normal operation of the program, a zip bomb allows the program to work as intended, but the archive is carefully crafted so that unpacking it (e.g. by a virus scanner in order to scan for viruses) requires inordinate amounts of time, disk space or memory. +

Este es un ejemplo de un famoso zip bomb (¡pruébelo con precaución!): <https://www.unforgettable.dk/>

Conclusión:

Después de este escrito, ahora está claro que Greg Schardt y Mr. Evil son una sola persona. El portátil incautado incluye software de hacking que se utilizó para husmear en los datos de las víctimas, chatear en grupos de noticias de hackers e IRC, contener una bomba zip. ¡Así que todas las sospechas sobre Greg Schardt eran ciertas!