

4DELL VAKA ANALİZ RAPORU

- Hash değeri

The screenshot displays a forensic analysis tool interface. On the left, a tree view shows various data sources and results. The main pane on the right shows a table of data sources. Below this, a detailed view of a file's metadata is shown, including its name, type, size, and various hash values. The MD5 hash is highlighted in blue.

Name	Type
4Dell Latitude CPL.E01	Image

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
	Name		/img_4Dell Latitude CPL.E01				
	Type		E01				
	Size		4871501120				
	MD5		aee4fcd9301c03b3b054623ca261959a				
	SHA1		Not calculated				
	SHA256		Not calculated				
	Sector Size		512				
	Time Zone		Asia/Istanbul				
	Acquisition Details		Description: Dell Latitude CPI				
			Case Number: Greg Schardt				
			Evidence Number: 1 of 1				
			Examiner Name: Shane Robinson				

Hash değerini bulmak için imaj dosyasının dosya meta verilerine bakıyoruz. Burada hash değerinin md5 formatında “aee4fcd9301c03b3b054623ca261959a” olduğunu görüyoruz.

- İşletim sistemi

The screenshot shows a forensic analysis tool interface. On the left, a tree view displays the file system structure of a Dell Latitude CPiE01. The selected volume is vol2 (NTFS / exFAT (0x07): 63-9510479). The right pane shows a list of files with columns: Name, S, C, Modified Time, Change Time, and Access Time. The file boot.ini is highlighted. Below the list, a search bar shows the string "Microsoft Windows XP Professional" and the file path "multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\".

Name	S	C	Modified Time	Change Time	Access Time
\$Secure:\$SDS			2004-08-19 19:57:43 EEST	2004-08-19 19:57:43 EEST	2004-08-19 19:57
\$UpCase			2004-08-19 19:57:43 EEST	2004-08-19 19:57:43 EEST	2004-08-19 19:57
\$Volume			2004-08-19 19:57:43 EEST	2004-08-19 19:57:43 EEST	2004-08-19 19:57
AUTOEXEC.BAT			2004-08-18 19:53:36 EEST	2004-08-19 20:02:10 EEST	2004-08-19 03:00
boot.ini			2004-08-20 01:20:04 EEST	2004-08-20 01:40:19 EEST	2004-08-26 18:51
BOOTLOG.PRV			2004-08-18 19:56:12 EEST	2004-08-20 01:40:19 EEST	2004-08-18 03:00
BOOTLOG.TXT			2004-08-19 18:39:26 EEST	2004-08-20 01:40:19 EEST	2004-08-19 03:00
BOOTSECT.DOS			2004-08-19 19:47:34 EEST	2004-08-20 01:40:19 EEST	2004-08-19 03:00
COMMAND.COM			1999-04-24 01:22:00 EEST	2004-08-20 01:40:19 EEST	2004-08-18 03:00
CONFIG.SYS			2004-08-18 19:54:56 EEST	2004-08-19 20:02:10 EEST	2004-08-20 01:38
DETLG.TXT			2004-08-18 19:50:00 EEST	2004-08-20 01:40:19 EEST	2004-08-18 03:00
FRUNLOG.TXT			2004-08-18 19:46:48 EEST	2004-08-19 20:02:21 EEST	2004-08-18 03:00
hiberfil.sys			2004-08-27 18:08:16 EEST	2004-08-27 18:08:16 EEST	2004-08-27 18:08
IO.SYS			1999-04-24 01:22:00 EEST	2004-08-19 20:02:21 EEST	2004-08-18 03:00
MSDOS---			2004-08-18 19:31:34 EEST	2004-08-20 01:40:19 EEST	2004-08-18 03:00
MSDOS.SYS			2004-08-18 19:50:14 EEST	2004-08-19 20:02:21 EEST	2004-08-18 03:00
NETLOG.TXT			2004-08-18 19:53:16 EEST	2004-08-20 01:40:19 EEST	2004-08-18 03:00
ntdetect.com			2001-08-23 21:00:00 EEST	2004-08-19 20:02:11 EEST	2004-08-19 03:00
ntldr			2001-08-23 21:00:00 EEST	2004-08-19 20:02:11 EEST	2004-08-19 03:00
pagefile.sys			2004-08-27 18:08:14 EEST	2004-08-27 18:08:14 EEST	2004-08-27 18:08
SETUPLOG.TXT			2004-08-18 19:53:16 EEST	2004-08-20 01:40:19 EEST	2004-08-18 03:00
SUHDLOG.DAT			2004-08-18 19:40:56 EEST	2004-08-20 01:40:19 EEST	2004-08-18 03:00

NTFS dosya sisteminde boot.ini dosyasına baktığımızda Microsoft Windows XP işletim sistemini ve Professional sürümünün kullanıldığı buluyoruz.

- Kurulum tarihi

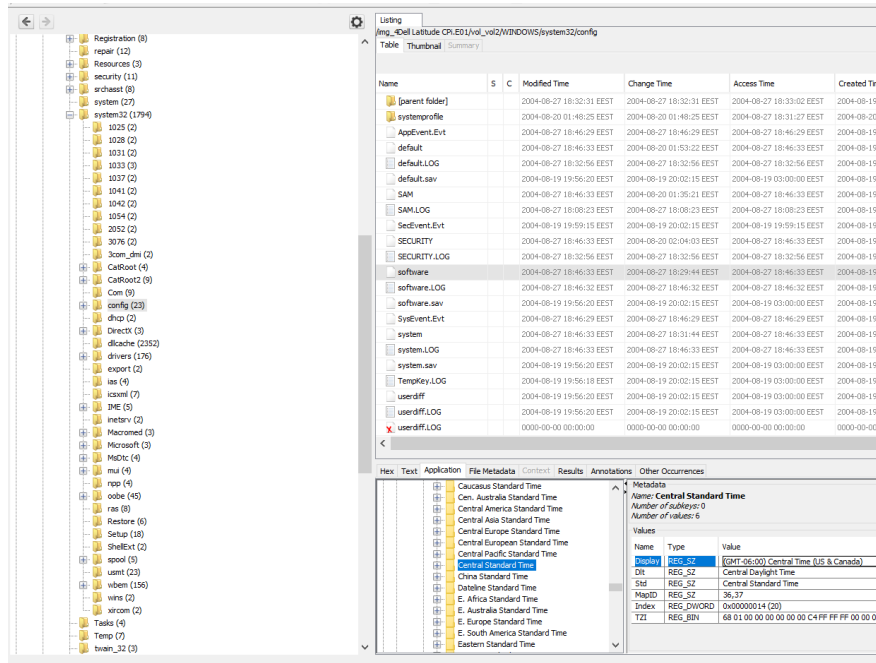
The screenshot shows a forensic analysis tool interface. On the left, a tree view displays the file system structure of a Dell Latitude CPiE01. The selected volume is vol2 (NTFS / exFAT (0x07): 63-9510479). The right pane shows a list of files with columns: Name, S, C, Modified Time, and Ch. The file Windows Update.log is highlighted. Below the list, a search bar shows the string "Microsoft Windows XP Professional" and the file path "multi(0)disk(0)rdisk(0)partition(1)\WINDOWS\".

Name	S	C	Modified Time	Ch
twain_32.dll			2001-08-23 21:00:00 EEST	20C
twain_16.exe			2001-08-23 21:00:00 EEST	20C
twain_32.exe			2001-08-23 21:00:00 EEST	20C
vb.ini			2004-08-20 01:26:28 EEST	20C
vbaddin.ini			2004-08-20 01:26:28 EEST	20C
vmmreg32.dll			2001-08-23 21:00:00 EEST	20C
wiadebug.log			2004-08-19 20:08:50 EEST	20C
wiaservc.log			2004-08-19 20:08:51 EEST	20C
win.ini			2004-08-20 01:38:20 EEST	20C
Windows Update.log			2004-08-20 01:35:37 EEST	20C
WindowsShell.Manifest			2004-08-20 01:32:26 EEST	20C
winhelp.exe			2001-08-23 21:00:00 EEST	20C
winhlp32.exe			2001-08-23 21:00:00 EEST	20C
winnit.bmp			2001-08-23 21:00:00 EEST	20C
winnit256.bmp			2001-08-23 21:00:00 EEST	20C
WMSysPrx.prx			2004-08-20 01:38:02 EEST	20C
Zapotec.bmp			2001-08-23 21:00:00 EEST	20C
regopt.log			0000-00-00 00:00:00	00C
vb.ini			0000-00-00 00:00:00	00C
~GLC0000.TMP			0000-00-00 00:00:00	00C
~GLH0000.TMP			0000-00-00 00:00:00	00C
~GLH0001.TMP			0000-00-00 00:00:00	00C

Kurulum tarihini öğrenmek için Windows klasöründeki Windows update.log kayıtlarına bakıyoruz.

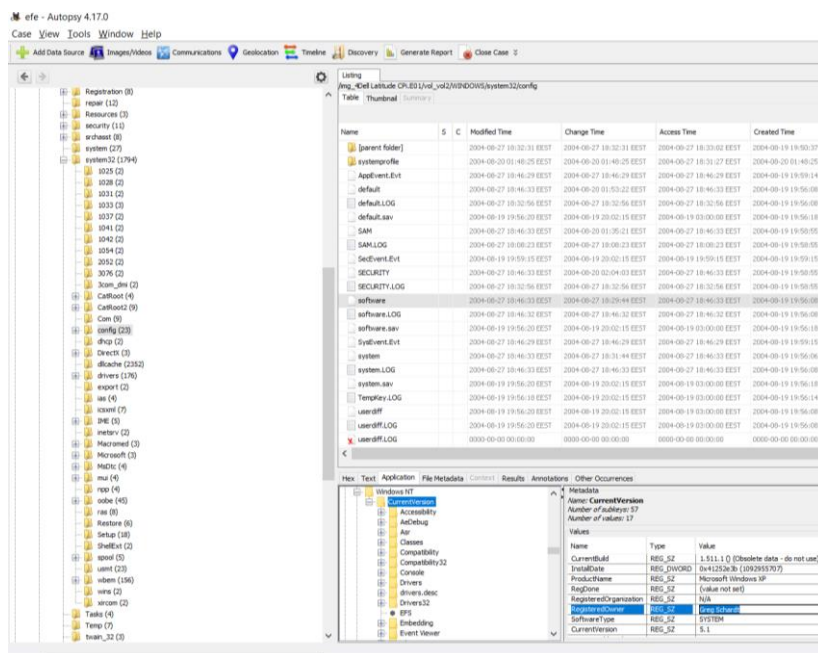
Buradan 2004-08-19 17:35:37 gibi bir sonuçla karşılaşıyoruz. Önceki sürümden Windows XP'ye 19 ağustos 2004 tarihinde saat 17:35 de güncellendiğini görüyoruz.

- Saat dilimi



Saat dilimini öğrenmek için Windows/system32 dosyasında bulunan software'ye giriyoruz. Ardından Microsoft\Windows NT\CurrentVersion\Time Zones'un içerisinde GMT-06:00 saat dilimi kullanıldığını buluyoruz.

- Cihaz sahibi

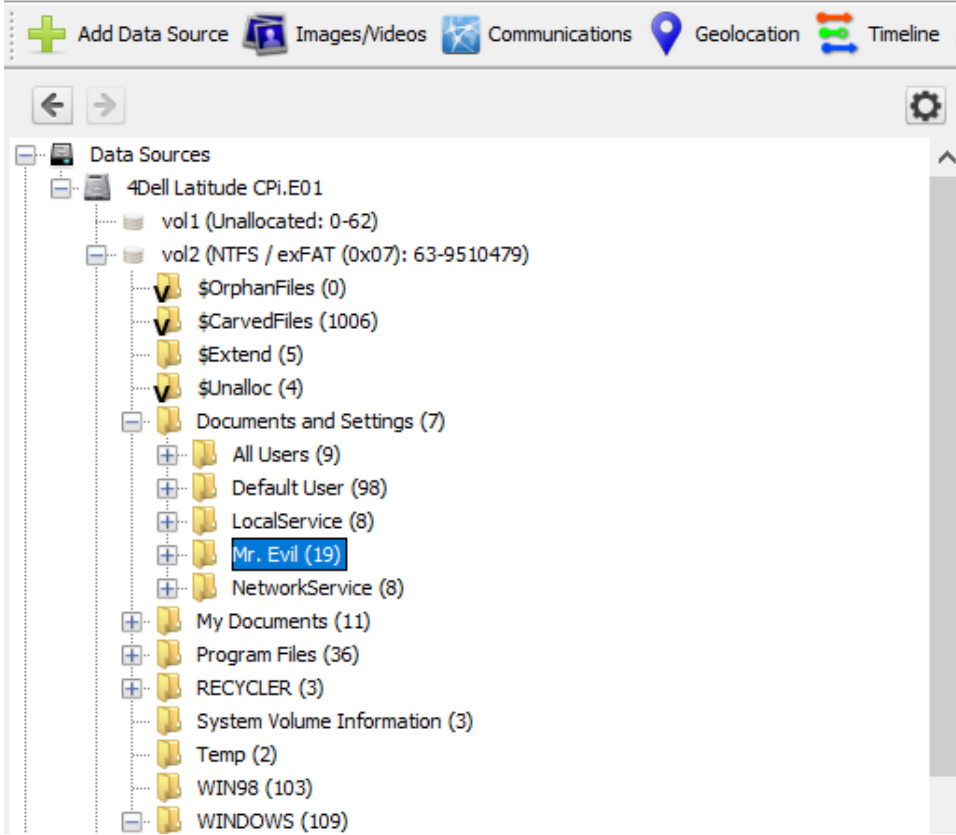


Saat dilimini öğrenirken girdiğimiz dosya konumunda bu kez CurrentVersion'un içerisinde Greg Schardt isimli kişinin kayıtlı kişi olduğunu öğreniyoruz.

- Hesap ismi

Autopsy 4.17.0

Case View Tools Window Help



Hesap isminin ise Documents and Setting bölümünden “Mr. Evil” yani bay kötü olduğunu öğreniyoruz.

- Cihazın son kapanma zamanı

system.LOG		2004-08-27 18:46:33 EEST	2004-08-27 18:46:33 EEST	200
system.sav		2004-08-19 19:56:20 EEST	2004-08-19 20:02:15 EEST	200
TempKey.LOG		2004-08-19 19:56:18 EEST	2004-08-19 20:02:15 EEST	200
userdiff		2004-08-19 19:56:20 EEST	2004-08-19 20:02:15 EEST	200
userdiff.LOG		2004-08-19 19:56:20 EEST	2004-08-19 20:02:15 EEST	200
userdiff.LOG		0000-00-00 00:00:00	0000-00-00 00:00:00	000

The screenshot shows the Autopsy 4.17.0 interface. The 'Prefetcher' file is selected in the file tree. The 'ExitTime' field in the 'Metadata' pane is highlighted, showing the value '2004/08/27-10:46:27'.

Cihaz sahibini öğrenmek için girdiğimiz CurrentVersion dosyasında bu sefer Prefetcher dosyasına giriyoruz buradaki ExitTime bölümünden son kapanma zamanını şu şekilde buluyoruz: 27/08/2004–10:46:27

- Kullanıcı sayısı

The screenshot shows the Autopsy 4.17.0 interface. The 'system32\config\SAM' file is selected in the file tree. The 'Name' field in the 'Metadata' pane is highlighted, showing the value 'SAM'.

Cihazda bulunan kullanıcı sayısını bulmak için system32 dosyasında bulunan config dosyasındaki SAM

dosyasına giriyoruz.SAM/SAM/Domains/Account/Users/Names bölümünde Sadet kullanıcı yer aldığını görebiliyoruz.

- Oturum açan son kullanıcı

The screenshot shows a file explorer window with a directory tree on the left and a metadata window on the right. The directory tree includes folders like 'software', 'system', and 'userdiff', each containing a '.LOG' file. The metadata window is for 'NetworkCards' and shows details for 'Compaq WL110 Wireless LAN PC Card'.

Name	Type	Value
ServiceName	REG_SZ	{86FC0C96-3FF2-4D59-9ABA-C602F21365D2}
Description	REG_SZ	Compaq WL110 Wireless LAN PC Card

Cihazda oturum açan son kullanıcıyı bulmak için CurrentVersion'daki Winlogon dosyasına bakıyoruz ve son giriş yapan kullanıcının Mr. Evil olduğunu görüyoruz.

- Kullanılan ağ kartları

The screenshot shows a file explorer window with a directory tree on the left and a metadata window on the right. The directory tree includes folders like 'software', 'system', and 'userdiff', each containing a '.LOG' file. The metadata window is for 'NetworkCards' and shows details for 'Xircom CardBus Ethernet 100 + Modem 56 (Ether...'.

Name	Type	Value
ServiceName	REG_SZ	{6E4090C2-FAEF-489A-8575-505D21FC1049}
Description	REG_SZ	Xircom CardBus Ethernet 100 + Modem 56 (Ether...

Bu cihazdaki kullanılan ağ kartlarını öğrenmek için CurrentVersion içerisinde yer alan NetworkCards dosyasını inceliyoruz ve Compaq WL110 Wireless LAN PC Card Xircom ve CardBus Ethernet 100 + Modem 56 (Ether... ağ kartlarını görüyoruz.

- IP adresi ve MAC adresi

☛ efs - Autopsy 4.17.0

Case View Tools Window Help

The screenshot shows the Autopsy 4.17.0 interface. On the left, the 'Data Sources' pane shows a tree structure of files. The 'Program Files' folder is expanded, showing 'Look@LAN' and 'irunin.ini'. On the right, the 'Listing' pane shows a table of files. The 'irunin.ini' file is selected, and its contents are displayed in the bottom pane. The contents of 'irunin.ini' are as follows:

```
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-LA90DN62XK4LQ
%LANDONMAIN%=N-LA90DN62XK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANZC%=0010a4933e09
%ISWIN95%=FALSE
```

Program Files dosyasından Look@LAN dosyasındaki irunun.ini'yi incelediğimiz zaman ip adresini 192.168.1.111 olduğunu ve MAC adresinin 0010a4933e09 olduğunu görüyoruz.

- E-posta adresi

The screenshot shows the Autopsy 4.17.0 interface. On the left, the 'Data Sources' pane shows a tree structure of files. The 'Program Files' folder is expanded, showing 'Look@LAN' and 'AGENT.INI'. On the right, the 'Listing' pane shows a table of files. The 'AGENT.INI' file is selected, and its contents are displayed in the bottom pane. The contents of 'AGENT.INI' are as follows:

```
AGENT.INI
;For information about the settings in this file,
;search for AGENT.INI in the online help.
[Profile]
Fullname="Mr. Evil"
EmailAddress="0010a4933e09@lookatlan.com"
EmailAddressFormat=""
ReplyTo=""
Organization="Mr. Evil"
DukeAuthorization=1
DataAssessment=1
```


Program Files/Agent/Data/AGENT.INI'yi incelediğimiz zaman Mr. Evil'in e-posta adresinin whoknowsme@sbcglobal.net olduğunu görüyoruz.

- Abonelikler

The screenshot shows the Autopsy 4.17.0 interface. On the left, the file system tree is expanded to 'Application Data (5)' > 'Identities (5)' > 'Microsoft (3)' > 'Outlook Express (31)'. The main pane displays a list of files with columns: Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dr), Flags(Meta), Known, and Location. The file 'alt2600.phreaker.dbx' is highlighted in the list.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
[current folder]			2004-09-21 00:14:23 EEST	2004-09-21 00:14:23 EEST	2004-09-21 00:15:02 EEST	2004-09-21 00:13:25 EEST	168	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
[current folder]			2004-09-21 00:13:25 EEST	2004-09-21 00:13:25 EEST	2004-09-21 00:13:25 EEST	2004-09-21 00:13:25 EEST	264	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
[current folder]			2004-09-21 00:27:17 EEST	2004-09-21 00:27:17 EEST	2004-09-21 00:27:17 EEST	2004-09-21 00:18:41 EEST	207572	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.codes.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:18:44 EEST	143206	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.codes.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:18:46 EEST	469716	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.dbx			2004-09-21 00:27:23 EEST	2004-09-21 00:27:23 EEST	2004-09-21 00:27:23 EEST	2004-09-21 00:18:32 EEST	600780	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.hackers.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:25:57 EEST	469716	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.moderated.dbx			2004-09-21 00:19:20 EEST	2004-09-21 00:19:20 EEST	2004-09-21 00:19:20 EEST	2004-09-21 00:19:15 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.phreaker.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:25:59 EEST	277188	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.programs.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:24:25 EEST	207572	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.binaries.hacking.beginner.dbx			2004-09-21 00:23:41 EEST	2004-09-21 00:23:41 EEST	2004-09-21 00:23:41 EEST	2004-09-21 00:22:54 EEST	680780	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.binaries.hacking.computers.dbx			2004-09-21 00:20:55 EEST	2004-09-21 00:20:55 EEST	2004-09-21 00:20:55 EEST	2004-09-21 00:20:36 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.binaries.hacking.utilities.dbx			2004-09-21 00:19:24 EEST	2004-09-21 00:19:24 EEST	2004-09-21 00:19:24 EEST	2004-09-21 00:19:22 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.binaries.hacking.utilities.dbx			2004-09-21 00:20:50 EEST	2004-09-21 00:20:50 EEST	2004-09-21 00:20:50 EEST	2004-09-21 00:20:42 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.das.hack.dbx			2004-09-21 00:22:54 EEST	2004-09-21 00:22:54 EEST	2004-09-21 00:22:54 EEST	2004-09-21 00:20:55 EEST	680780	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.hacking.dbx			2004-09-21 00:27:07 EEST	2004-09-21 00:27:07 EEST	2004-09-21 00:27:07 EEST	2004-09-21 00:23:41 EEST	535252	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.hackers.hack.dbx			2004-09-21 00:20:34 EEST	2004-09-21 00:20:34 EEST	2004-09-21 00:20:34 EEST	2004-09-21 00:19:52 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.hackers.hacking.malicious.dbx			2004-09-21 00:19:27 EEST	2004-09-21 00:19:27 EEST	2004-09-21 00:19:27 EEST	2004-09-21 00:19:25 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
cleanlog			2004-09-21 00:13:58 EEST	2004-09-21 00:13:58 EEST	2004-09-21 00:13:58 EEST	2004-09-21 00:13:55 EEST	962	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
Deleted Items.dbx			2004-09-21 00:18:30 EEST	2004-09-21 00:18:30 EEST	2004-09-21 00:18:30 EEST	2004-09-21 00:18:30 EEST	143206	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
Folders.dbx			2004-09-21 00:25:59 EEST	2004-09-21 00:25:59 EEST	2004-09-21 00:13:57 EEST	2004-09-21 00:13:25 EEST	4072416	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
free.binaries.hackers.malicious.dbx			2004-09-21 00:19:31 EEST	2004-09-21 00:19:31 EEST	2004-09-21 00:19:31 EEST	2004-09-21 00:19:29 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...

Mr. Evil'in abone olduğu grupları görmek için Documents and Settings\Mr. Evil\Local Settings\Application Data\Identities\Microsoft\Outlook Express konumunu inceliyoruz. Burada bir çok hack grubuna abone olduğunu öğreniyoruz.

- Mirc kullanıcı bilgileri

The screenshot shows the Autopsy 4.17.0 interface. On the left, the file system tree is expanded to 'Application Data (5)' > 'Identities (5)' > 'Microsoft (3)' > 'Outlook Express (31)'. The main pane displays a list of files with columns: Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dr), Flags(Meta), Known, and Location. The file 'alt2600.phreaker.dbx' is highlighted in the list.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
[current folder]			2004-09-21 00:14:23 EEST	2004-09-21 00:14:23 EEST	2004-09-21 00:15:02 EEST	2004-09-21 00:13:25 EEST	168	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
[current folder]			2004-09-21 00:13:25 EEST	2004-09-21 00:13:25 EEST	2004-09-21 00:13:25 EEST	2004-09-21 00:13:25 EEST	264	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
[current folder]			2004-09-21 00:27:17 EEST	2004-09-21 00:27:17 EEST	2004-09-21 00:27:17 EEST	2004-09-21 00:18:41 EEST	207572	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.codes.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:18:44 EEST	143206	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.codes.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:18:46 EEST	469716	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.dbx			2004-09-21 00:27:23 EEST	2004-09-21 00:27:23 EEST	2004-09-21 00:27:23 EEST	2004-09-21 00:18:32 EEST	600780	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.hackers.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:25:57 EEST	469716	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.moderated.dbx			2004-09-21 00:19:20 EEST	2004-09-21 00:19:20 EEST	2004-09-21 00:19:20 EEST	2004-09-21 00:19:15 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.phreaker.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:25:59 EEST	277188	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.2600.programs.dbx			2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:27:16 EEST	2004-09-21 00:24:25 EEST	207572	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.binaries.hacking.beginner.dbx			2004-09-21 00:23:41 EEST	2004-09-21 00:23:41 EEST	2004-09-21 00:23:41 EEST	2004-09-21 00:22:54 EEST	680780	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.binaries.hacking.computers.dbx			2004-09-21 00:20:55 EEST	2004-09-21 00:20:55 EEST	2004-09-21 00:20:55 EEST	2004-09-21 00:20:36 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.binaries.hacking.utilities.dbx			2004-09-21 00:19:24 EEST	2004-09-21 00:19:24 EEST	2004-09-21 00:19:24 EEST	2004-09-21 00:19:22 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.binaries.hacking.utilities.dbx			2004-09-21 00:20:50 EEST	2004-09-21 00:20:50 EEST	2004-09-21 00:20:50 EEST	2004-09-21 00:20:42 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.das.hack.dbx			2004-09-21 00:22:54 EEST	2004-09-21 00:22:54 EEST	2004-09-21 00:22:54 EEST	2004-09-21 00:20:55 EEST	680780	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.hacking.dbx			2004-09-21 00:27:07 EEST	2004-09-21 00:27:07 EEST	2004-09-21 00:27:07 EEST	2004-09-21 00:23:41 EEST	535252	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.hackers.hack.dbx			2004-09-21 00:20:34 EEST	2004-09-21 00:20:34 EEST	2004-09-21 00:20:34 EEST	2004-09-21 00:19:52 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
alt.hackers.hacking.malicious.dbx			2004-09-21 00:19:27 EEST	2004-09-21 00:19:27 EEST	2004-09-21 00:19:27 EEST	2004-09-21 00:19:25 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
cleanlog			2004-09-21 00:13:58 EEST	2004-09-21 00:13:58 EEST	2004-09-21 00:13:58 EEST	2004-09-21 00:13:55 EEST	962	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
Deleted Items.dbx			2004-09-21 00:18:30 EEST	2004-09-21 00:18:30 EEST	2004-09-21 00:18:30 EEST	2004-09-21 00:18:30 EEST	143206	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
Folders.dbx			2004-09-21 00:25:59 EEST	2004-09-21 00:25:59 EEST	2004-09-21 00:13:57 EEST	2004-09-21 00:13:25 EEST	4072416	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...
free.binaries.hackers.malicious.dbx			2004-09-21 00:19:31 EEST	2004-09-21 00:19:31 EEST	2004-09-21 00:19:31 EEST	2004-09-21 00:19:29 EEST	76508	Allocated	Allocated	unknown	Img_K0ell Latitude CH.E01\...

Bu bilgiler erişmek için mIRC dosyasındaki mirc.ini'yi incelememiz yeterli olacaktır ve aşağıdaki bilgilere erişeceğiz.

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

- Mirc kanalları

Autopsy 4.17.0 interface showing a file listing of logs in the Application Data directory. The table displays columns for Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dr), Flags(Meta), Known, and Location. The logs are listed in chronological order, with the most recent at the top.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
[current folder]			2004-08-20 18:24:40 EEST	2004-08-20 18:24:40 EEST	2004-08-27 18:14:45 EEST	2004-08-20 18:24:40 EEST	56	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
[parent folder]			2004-08-25 19:20:55 EEST	2004-08-25 19:20:55 EEST	2004-08-27 18:14:45 EEST	2004-08-20 18:09:53 EEST	56	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#ChorusLike.UnderNet.log			2004-08-20 18:54:11 EEST	2004-08-20 18:54:11 EEST	2004-08-20 18:54:11 EEST	2004-08-20 18:52:39 EEST	868	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#CircusLike.UnderNet.log			2004-08-20 22:02:55 EEST	2004-08-20 22:02:55 EEST	2004-08-20 22:02:55 EEST	2004-08-20 18:54:21 EEST	9273	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#Ella.Hackers.UnderNet.log			2004-08-20 18:49:05 EEST	2004-08-20 18:49:05 EEST	2004-08-20 18:49:05 EEST	2004-08-20 18:45:34 EEST	464	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#EvilFork.Phrnet.log			2004-08-20 18:31:07 EEST	2004-08-20 18:31:07 EEST	2004-08-20 18:31:07 EEST	2004-08-20 18:30:18 EEST	335	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#Funny.UnderNet.log			2004-08-20 22:28:14 EEST	2004-08-20 22:28:14 EEST	2004-08-20 22:28:14 EEST	2004-08-20 22:26:18 EEST	263	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#Houton.UnderNet.log			2004-08-20 18:52:01 EEST	2004-08-20 18:52:01 EEST	2004-08-20 18:52:01 EEST	2004-08-20 18:48:59 EEST	265	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#ISO-WAREZ.Phrnet.log			2004-08-20 18:29:42 EEST	2004-08-20 18:29:42 EEST	2004-08-20 18:29:42 EEST	2004-08-20 18:29:01 EEST	149	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#LuxShell.UnderNet.log			2004-08-20 18:43:21 EEST	2004-08-20 18:43:21 EEST	2004-08-20 18:43:21 EEST	2004-08-20 18:42:03 EEST	589	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#mp3man.UnderNet.log			2004-08-20 18:44:20 EEST	2004-08-20 18:44:20 EEST	2004-08-20 18:44:20 EEST	2004-08-20 18:43:18 EEST	1283	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#Phreakt0wer.AStarNET.log			2004-08-20 22:16:23 EEST	2004-08-20 22:16:23 EEST	2004-08-20 22:16:23 EEST	2004-08-20 22:14:45 EEST	578	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#uhells.UnderNet.log			2004-08-20 18:45:07 EEST	2004-08-20 18:45:07 EEST	2004-08-20 18:45:07 EEST	2004-08-20 18:44:49 EEST	294	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log
#Star.UnderNet.log			2004-08-20 19:00:08 EEST	2004-08-20 19:00:08 EEST	2004-08-20 19:00:08 EEST	2004-08-20 18:54:55 EEST	285	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Program Files/mIRC.log

Bu kanallara erişmek için mIRC içerisinde yer alan logs dosyasına bakıyoruz ve bir çok kanalın yer aldığını görüyoruz.

- Şüpheli uygulama

Autopsy 4.17.0 interface showing a file listing of logs in the Application Data directory. The table displays columns for Name, S, C, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dr), Flags(Meta), Known, and Location. The logs are listed in chronological order, with the most recent at the top.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
[current folder]			2004-08-27 18:35:53 EEST	2004-08-27 18:35:53 EEST	2004-08-27 18:40:31 EEST	2004-08-27 18:35:53 EEST	352	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Documents and Settings/...
[parent folder]			2004-08-27 18:35:53 EEST	2004-08-27 18:35:53 EEST	2004-08-27 18:42:40 EEST	2004-08-20 02:04:05 EEST	56	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Documents and Settings/...
[record]			2004-08-27 18:45:25 EEST	2004-08-27 18:45:25 EEST	2004-08-27 18:45:25 EEST	2004-08-27 18:45:25 EEST	1788	Allocated	Allocated	unknown	/img_4c0d Latitude CH.E331/vol_02/Documents and Settings/...

Recent settings file for Ethereal 0.10.4.

This file is regenerated each time Ethereal is quit.
So be careful, if you want to make manual changes here.

Recent capture files (latest last) #####

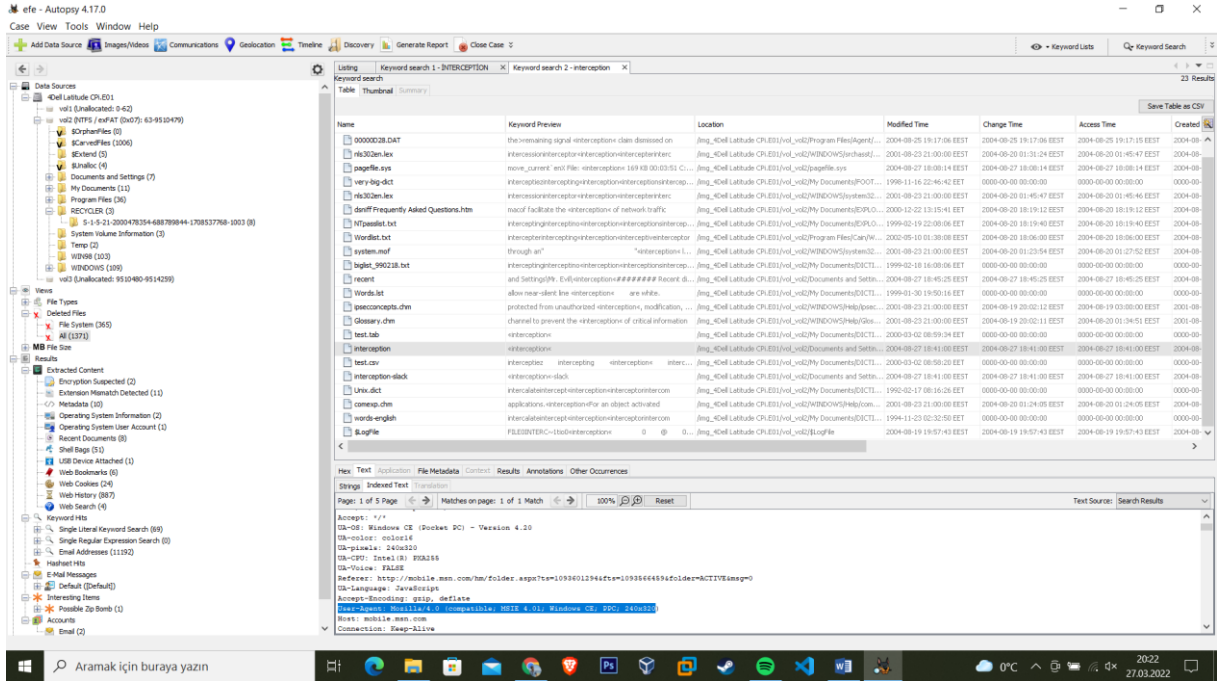
Recent capture file: C:\Documents and Settings\Mr. Evil\Interception

Recent display filters (latest last) #####

Recent display filter: !ip_addr eq 192.168.254.2 and ip_addr eq 207.68.174.248 and !tcp.port eq 1337 and tcp.port eq 80

Mr. Evil dosyası içerisindeki Application Data klasöründe Ethereal programının yer aldığını görüyoruz. Bu program internet paketlerini kesmek için kullanılır. Recentte ise programın kullanıldığını ve işlemlerin başarılı olduğunu görüyoruz.

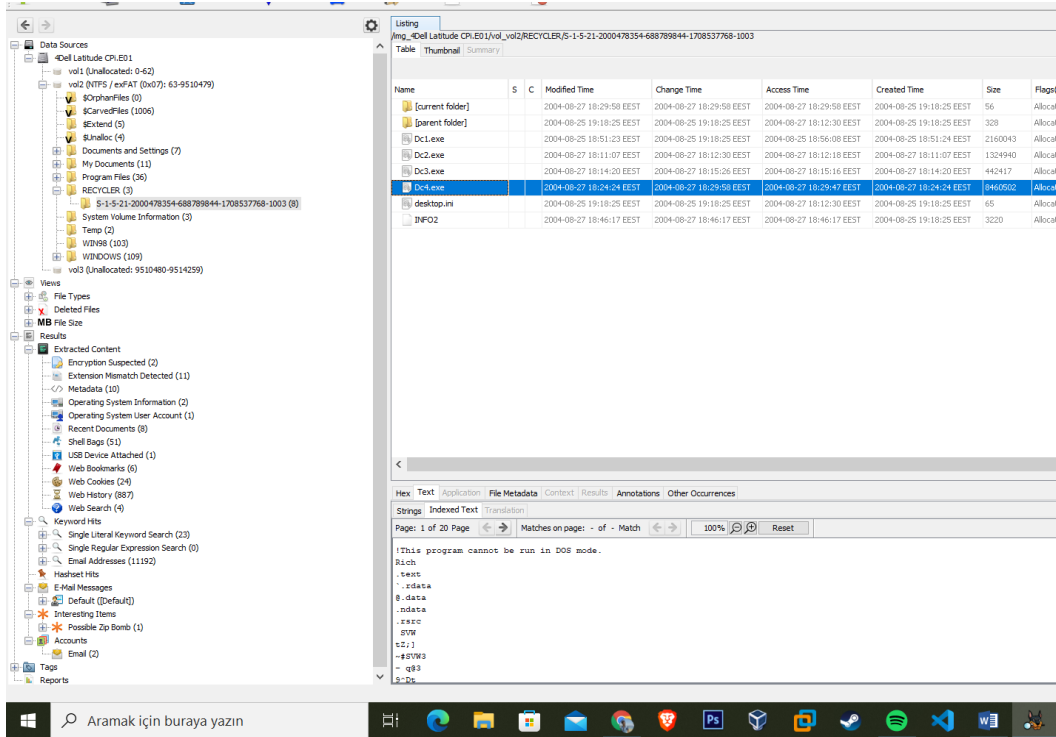
- Mağdurun bilgileri



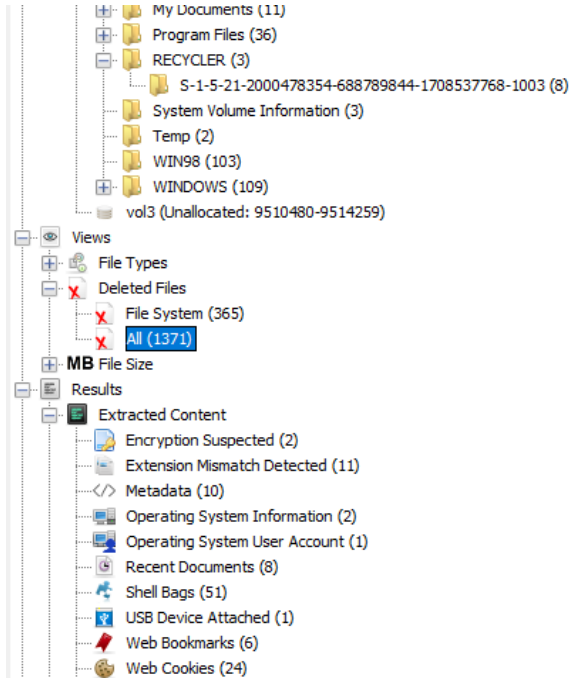
Kelime araması kısmında “interception”u aratıyoruz ve çıkan interception dosyasını inceliyoruz buradan mağdur kişinin Windows ce isimli bir cihazdan Mozilla 4.0 tarayıcısından giriş yaptığı görülüyor.

Ayrıca mağdur kişi mobile.msn.com a erişiyormuş.

- Silinen dosyalar

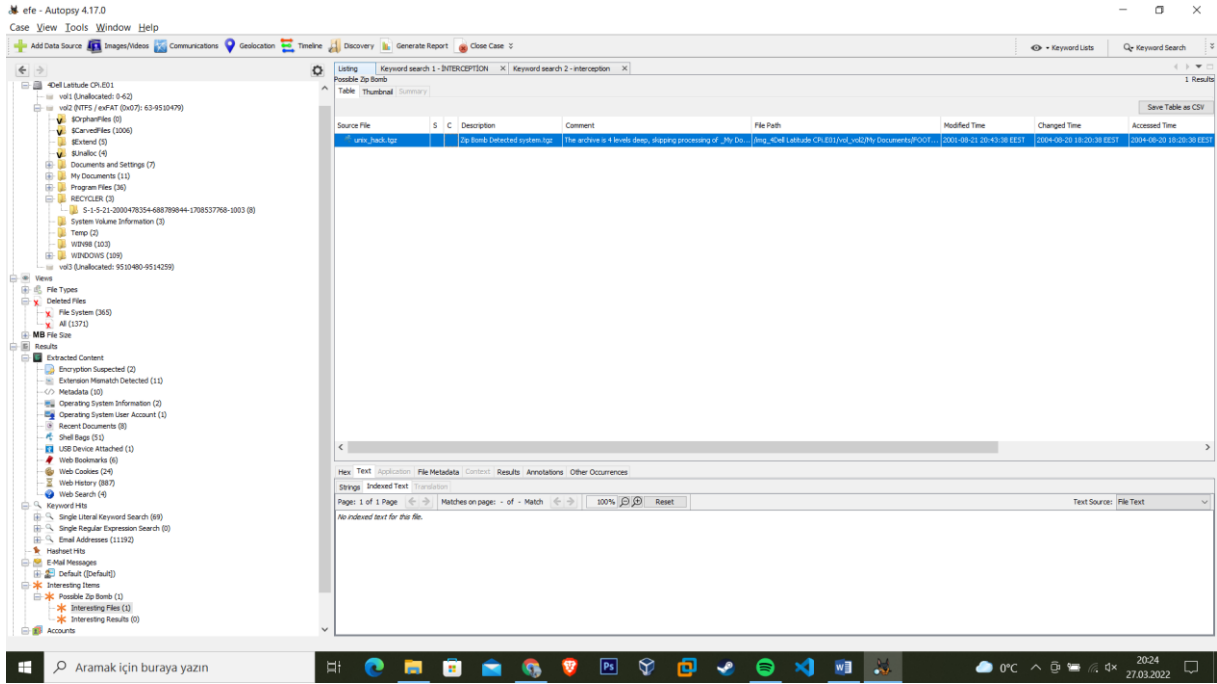


Geri dönüşüm kutusuna gönderilen 4 adet exe dosyası mevcut.



Gerçekten silinen ise 1371 adet dosya vardır.

- Cihazda Virüs var mı?



İlginç dosyalara baktığımız zaman bir adet zip bombası olduğunu görüyoruz.

Efekan ACAR 200509047