

# Módulo II: Forense

#### Ismael Gómez, Inés Martín y Carlos Barahona



# Índice

### I. Análisis de RAM: Volatility

- I. ¿Qué es?
- 2. Comandos básicos
- 3. Dumpeo de archivos

### 2. Análisis de tráfico: Wireshark

- I. ¿Qué es?
- 2. Ejemplos de uso

### 3. Análisis de discos: Autopsy

- I. ¿Qué es?
- 2. Abrir un caso
- 3. Tipos de análisis



#### I - Análisis de RAM

•••

Universidad Rey Juan Carlos

Análisis de RAM

Análisis de memoria volátil

Sólo tiene contenido cuándo está conectada a la corriente y cuando se apaga el ordenador, Ciao datos.

Se almacenan de forma temporal todos los programas, procesos, librerías, etc...





### I.Volatility- ¿Qué es?

#### ¿Qué es Volatility?

Es una colección de herramientas que nos ayudan a analizar **"dumps" de memoria volátil (RAM**)

Fácil de ejecutar ya que está implementada en Python

Preinstalada en la máquina del curso

\$ cd Documentos
\$ cd volatility
\$ python2 vol.py





## I.Volatility – Comandos Básicos (imageinfo)

(urjc@ETSIICTF)-[~/Documentos/dump] vol.py -f dump.raw imageinfo (urjc@ETSIICTF)-[~/Documentos/dump] vol.py -f dump.raw imageinfo vol.py -f dump.raw imageinfo Volatility Foundation Volatility Framework 2<sub>aw</sub>) INFO : volatility.debug · Determining Suggested Profile(s) : Win7SP1×64, Image Type (Service rack) · 1

El plugin "imageinfo" nos da información sobre el dump que vamos a comenzar a analizar Lo más importante es quedarnos con el "profile"



# II. Volatility (help)

E N

#### Python2 vol.py -h

0

#### https://github.com/volatilityfoundation /volatility/wiki/Command-Reference

ueva pestaña 🚬 🔟 Separar vista	izquierda/derecha 🛛 🗧 Separar vista arriba/abajo 🛛 Cargar una nueva pes
handles hashdump hibinfo hivedump	Print list of open handles for each process Dumps passwords hashes (LM/NTLM) from memory Dump hibernation file information Prints out a hive
hivelist hivescan	Print list of registry hives. Pool scanner for registry hives
hpakextract	Extract physical memory from an HPAK file
idt	Display Interrupt Descriptor Table
imagecopy	Copies a physical address space out as a raw DD image
imageinfo impscan	Identify information for the image Scan for calls to imported functions
joblinks	Print process job link information
kpcrscan	Search for and dump potential KPCR values
ldrmodules lsadump	Detect unlinked DLLs Dump (decrypted) LSA secrets from the registry
machoinfo malfind	Dump Mach-O file format information Find hidden and injected code
mbrparser	Scans for and parses potential Master Boot Records (MBRs)
memmap	Print the memory map
mftparser	Scans for and parses potential MFT entries
moddump modscan	Dump a kernel driver to an executable file sample Pool scanner for kernel modules
modules multiscan	Print list of loaded modules Scan for various objects at once
mutantscan	Pool scanner for mutex objects
notepad objtypescan	List currently displayed notepad text Scan for Windows object type objects
patcher poolpeek	Patches memory based on page scans Configurable pool scanner plugin
printkey	Print a registry key, and its subkeys and values
procdump	Dump a process to an executable file sample
pscisc	Pool scanner for process objects
pstree psxview	Print process list as a tree Find hidden processes with various process listings
qemuinfo raw2dmp	Dump Qemu information Converts a physical memory sample to a windbg crash dump
screenshot	Save a pseudo-screenshot based on GDI windows
sessions	List details on _MM_SESSION_SPACE (user logon sessions)
shellbags shimcache	Prints ShellBags info Parses the Application Compatibility Shim Cache registry key
shutdowntime sockets	Print ShutdownTime of machine from registry Print list of open sockets



•••

Universidad Rey Juan Carlos

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64 Start
0×fffffa801afe1b30	firefox.exe	3312	3692	33	353	1	1 2020-06-12 16:16:16 UTC+0000
0×fffffa801a811520	firefox.exe	3084	3692	39	381	1	1 2020-06-12 16:16:16 UTC+0000
0×fffffa801af39b30	firefox.exe	2784	3692	25	307	1	1 2020-06-12 16:16:21 UTC+0000
0×fffffa801aa10270	notepad.exe	3060	1928	2	58	1	0 2020-06-12 16:16:34 UTC+0000
0×fffffa8019dc1b30	sppsvc.exe	3000	512	5	164	0	0 2020-06-12 16:17:13 UTC+0000
0×fffffa801aff97d0	svchost.exe	3656	512	13	351	0	0 2020-06-12 16:17:13 UTC+0000
0×fffffa8018faf630	7zFM.exe	868	1184	4	149	1	0 2020-06-12 16:17:32 UTC+0000
0×fffffa8018f7e060	SearchProtocol	2256	1036	8	287	1	0 2020-06-12 16:18:24 UTC+0000
0×fffffa801ace08a0	SearchFilterHo	2320	1036	6	103	0	0 2020-06-12 16:18:24 UTC+0000
0×fffffa801a9d5b30	SearchProtocol	1960	1036	8	284	0	0 2020-06-12 16:18:24 UTC+0000
0×fffffa8019011b30	MRCv120.exe	1376	1928	16	319	1	1 2020-06-12 16:18:50 UTC+0000
0×fffffa8019096060	WMIADAP.exe	1184	888	6	98	0	0 2020-06-12 16:19:13 UTC+0000
0×fffffa8019066060	WmiPrvSE.exe	1400	648	8	126	0	0 2020-06-12 16:19:13 UTC+0000

Inés Martín y Carlos Barahona

## I.Volatility – Comandos básicos (pstree)

<pre>// Content in the second second</pre>						
Name	Pid	PPid	Thds	Hnds Time		
0x819cc830:System	4	 0	· 55	162 1970-01-01 00:00:00 UTC+0000		
. 0x81945020:smss.exe	536	4	3	21 2011-10-10 17:03:56 UTC+0000		
0x816c6020:csrss.exe	608	536	11	355 2011-10-10 17:03:58 UTC+0000		
0x813a9020:winlogon.exe	632	536	24	533 2011-10-10 17:03:58 UTC+0000		
0x816da020:services.exe	676	632	16	261 2011-10-10 17:03:58 UTC+0000		
0x817757f0:svchost.exe	916	676	9	217 2011-10-10 17:03:59 UTC+0000		
<pre> 0x81772ca8:vmacthlp.exe</pre>	832	676	1	24 2011-10-10 17:03:59 UTC+0000		
0x816c6da0:svchost.exe	964	676	63	1058 2011-10-10 17:03:59 UTC+0000		
<pre> 0x815c4da0:wscntfy.exe</pre>	1920	964	1	27 2011-10-10 17:04:39 UTC+0000		
0x815e7be0:wuauclt.exe	400	964	8	173 2011-10-10 17:04:46 UTC+0000		
<pre> 0x8167e9d0:svchost.exe</pre>	848	676	20	194 2011-10-10 17:03:59 UTC+0000		
0x81754990:VMwareService.e	1444	676	3	145 2011-10-10 17:04:00 UTC+0000		
0x8136c5a0:alg.exe	1616	676	7	99 2011-10-10 17:04:01 UTC+0000		
0x813aeda0:svchost.exe	1148	676	12	187 2011-10-10 17:04:00 UTC+0000		
0x817937e0:spoolsv.exe	1260	676	13	140 2011-10-10 17:04:00 UTC+0000		
0x815daca8:svchost.exe	1020	676	5	58 2011-10-10 17:03:59 UTC+0000		
0x813c4020:lsass.exe	688	632	23	336 2011-10-10 17:03:58 UTC+0000		
0x813bcda0:explorer.exe	1956	1884	18	322 2011-10-10 17:04:39 UTC+0000		

# Con este comando podemos listar los **procesos en forma de árbol**

Inés Martín y Carlos Barahona

# I.Volatility – Comandos básicos (cmdline)

# (urjc ETSIICTF)-[~/Documentos/dump] \$ vol.py -f dump.raw --profile="Win7SP1×64" cmdline

svchost.exe pid: 3656

Command line : C:\Windows\System32\svchost.exe -k secsvcs

7zFM.exe pid: 868

Command line : "C:\Program Files\7-Zip\7zFM.exe" "C:\Users\Admin\Desktop\ficheroSecreto.7z"

# Obtenemos los **comandos** que se ejecutaron en la máquina Windows

# I.Volatility – Comandos básicos (consoles)

#### volatility -f imagen.vmem --profile=WinXPSP2x86 consoles

C:\Documents and Settings\Administrator>sc query malware							
SERVICE_NAME: malware							
ТҮРЕ	: 1 KERNEL_DRIVER						
STATE	: 4 RUNNING						
	(STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)						
WIN32_EXIT_CODE	: 0 (0×0)						
SERVICE_EXIT_CODE	: 0 (0×0)						
CHECKPOINT	: 0×0						
WAIT_HINT	: 0×0						

Con este plugin encuentra **comandos** que un atacante puede haber ejecutado en **cmd.exe** 



# I.Volatility – Comandos básicos (connscan)

#### volatility -f imagen.vmem --profile=WinXPSP2x86 connscan

Volatility Offset(P)	Foundation Volatility Local Address	Framework 2.6.1 Remote Address	Pid
0x01a25a50	0.0.0.0:1026	1/2.10.98.1:0000	1920

# Listamos las **conexiones** que estaban en el momento de la captura

# I.Volatility – Comandos básicos (filescan)

#### volatility -f imagen.vmem --profile=WinXPSP2x86 filescan

Offset(P)	#Ptr	#Hnd Access	Name
0x000000000156bcb0	2	1	\Device\Afd\Endpoint
0×000000000156f100	1	1	\Device\NamedPipe\W32TIME
0x00000000015a9a70	1	0	\Device\KSENUM#0000002\{9B365890-165F-11D0-A195-0020AFD156E4}
0x00000000015ac5c8	1	1 Rrw-	<pre>\Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.C</pre>
0x00000000015ac6b0	1	0 Rrw-	<pre>\Device\HarddiskVolume1\WINDOWS\Media\Windows XP Startup.wav</pre>
0x00000000015ac8f0	1	0 Rr-d	<pre>\Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.VC80.MFC_</pre>
0x00000000015ad318	1	0 Rr-d	<pre>\Device\HarddiskVolume1\WINDOWS\system32\webcheck.dll</pre>
0x00000000015ad740	1	0 Rr-d	<pre>\Device\HarddiskVolume1\WINDOWS\system32\themeui.dll</pre>

# Con este comando podemos listar los **archivos** que se encontraban en la máquina

# I.Volatility – Comandos básicos (dumpfile)

Imagen.vmem--profile=WinXPSP2x86 filescan | grep .wavVolatility Foundation Volatility Framework 2.6.10x0000000015ac6b010 R--rw- \Device\HarddiskVolume1\WINDOWS\Media\Windows XP Startup.wav0x0000000018d82c010 R--rw- \Device\HarddiskVolume1\WINDOWS\Media\Windows XP Balloon.wav

Volatility Foundation Volatility Framework 2.6.1 Volatility Foundation Volatility Framework 2.6.1 DataSectionObject 0x015ac6b0 None \Device\HarddiskVolume1\WINDOWS\Media\Windows XP Startup.wav

## Con este comando podemos dumpear/extraer archivos concretos que se encontraban en la máquina

# I.Volatility – Comandos básicos (hashdump)

(urjc ETSIICTF) - [~/Documentos/dump] \$ vol.py -f dump.raw --profile="Win7SP1x64" hashdump Volatility Foundation Volatility Framework 2.6.1 Administrador: 500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: Admin:1000:aac3b435b51404eeaad3b435b51404ee:62234517c6b66dc7839f0da943bd29ee:::

# Con este comando podemos dumpear/extraer los hashes de los usuarios de la máquina



#### II – Análisis de tráfico

#### Análisis de tráfico

Análisis de las actividades de la red para descubrir el origen de ataques, virus, intrusiones o infracciones de seguridad que se producen en una red.

Involucra las redes informáticas y los protocolos de red.



#### Permitirá descubrir:

- Navegación en páginas web
  - Exfiltraciones de datos
  - Conexiones maliciosas
- Credenciales en texto plano

. . .



#### II – Wireshark

#### ¿Qué es Wireshark?

Es un "sniffer" o herramienta que intercepta tráfico. Muestra en una interfaz sencilla paquete a paquete y todos los datos que contienen. Admite más de 2000 protocolos de red.

Las capturas de tráfico se guardan en ficheros .pcap, que es con lo que vamos a trabajar mayoritariamente en CTFs

(la captura nos la dan)





#### II – Wireshark

	Capture.pcapng
<u>File Edit View Go</u> Capture <u>A</u> nalyze <u>Statistics</u> Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
■ ⊿ ⊗ = 🖹 🕅 🙆 ۹ 🗢 ⇒ ≌ 🗿 🖳 📃 🔍 ۹ ۹	. 🎹
Apply a display filter <ctrl-></ctrl->	
Io. Time Source Destination Protocol	Lengt
– 447 32.24296… 192.168.0.147 192.168.0.115 TCP	74 52670 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 <sup>-</sup>
448 32.24516 192.168.0.115 192.168.0.147 TCP	74 80 → 52670 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 S/
449 32.24518 192.168.0.147 192.168.0.115 TCP	66 52670 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1407804984
450 32.24552… 192.168.0.147 192.168.0.115 HTTP	407 GET /shell.php HTTP/1.1
451 32.24589 192.168.0.115 192.168.0.147 TCP	66 80 → 52670 [ACK] Seq=1 Ack=342 Win=64896 Len=0 TSval=17019540
452 32.24864 192.168.0.115 192.168.0.147 TCP	74 53734 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 $^{-1}$
453 32.24867 192.168.0.147 192.168.0.115 TCP	74 80 → 53734 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 S/
454 32.24908 192.168.0.115 192.168.0.147 TCP	66 53734 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=170195410:
455 32.25470 192.168.0.115 192.168.0.147 TCP	172 53734 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=106 TSval=170
456 32.25472 192.168.0.147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seq=1 Ack=107 Win=65152 Len=0 TSval=14078049
457 32.27156 192.168.0.115 192.168.0.147 TCP	265 53734 → 80 [PSH, ACK] Seq=107 Ack=1 Win=64256 Len=199 TSval=:
458 32.27159 192.168.0.147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seq=1 Ack=306 Win=65024 Len=0 TSval=14078050
459 32.27581 192.168.0.115 192.168.0.147 TCP	120 53734 → 80 [PSH, ACK] Seq=306 Ack=1 Win=64256 Len=54 TSval=1
460 32.27585 192.168.0.147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seg=1 Ack=360 Win=65024 Len=0 TSval=14078050
461 32.27781 192.168.0.115 192.168.0.147 TCP	78 53734 → 80 [PSH, ACK] Seg=360 Ack=1 Win=64256 Len=12 TSval=1
462 32.27786 192.168.0.147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seg=1 Ack=372 Win=65024 Len=0 TSval=1407805(
463 32.27812 192.168.0.115 192.168.0.147 TCP	109 53734 → 80 [PSH, ACK] Seg=372 Ack=1 Win=64256 Len=43 TSval=1
464 32.27813 192.168.0.147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seg=1 Ack=415 Win=65024 Len=0 TSval=14078050
465 36.53758 192.168.0.147 192.168.0.115 TCP	73 80 → 53734 [PSH. ACK] Seg=1 Ack=415 Win=65024 Len=7 TSval=14(
466 36.53792 192.168.0.115 192.168.0.147 TCP	66 53734 → 80 [ACK] Seg=415 Ack=8 Win=64256 Len=0 TSval=1701958
467 36 54057 192 168 0 115 192 168 0 147 TCP	$7553734 \rightarrow 80$ [PSH] ACK] Seq=415 Ack=8 Win=64256 Len=9 TSval=170
407 50.54657# 152.100.0.115 152.100.0.147 161	
Transmission Control Protocol, Src Port: 52670, Dst Port: 80,	Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol	
→ GET /shell.php HTTP/1.1\r\n	
Host: 192.168.0.115\r\n	
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/2	20100101 Firefox/78.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.	.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n	
Accept-Encoding: gzip, deflate\r\n	
DNT: 1\r\n	
0000 08 00 27 92 a2 af 00 0c 29 4a b9 cd 08 00 45 00 ·····	)JE.
0010 01 89 b0 1d 40 00 40 06 06 fb c0 a8 00 93 c0 a8 ····@·	@· · · · · · · ·
0020 00 73 cd be 00 50 01 9f 1c bb 87 c6 14 06 80 18 ·s···P	0
Capture pcappg	Packets: 907 · Displayed: 907 (100.0%)
appeared people and a second s	Tacked, 507 Displayed, 507 (100.070)



## II – Wireshark (follow stream)

#### Seguir flujo HTTP

						+
Length Info						-
62 3372 → 80 [SYN] Seq=0 Win=8760	) Len=0 MSS=1460 SAC	K_PERM=1				- 1
62 80 → 3372 [SYN, ACK] Seq=0 Ack	k=1 Win=5840 Len=0 №	SS=1380 SAC	K_PERM=1			
54 3372 → 80 [ACK] Seq=1 Ack=1 Wi	n=9660 Len=0					
533 GET /download.html HTTP/1.1	Mark/Upmark Packet	Ctrl+M				
54 80 → 3372 [ACK] Seq=1 Ack=480		Cul+M				
14 80 → 3372 [ACK] Seq=1 Ack=480	Ignore/Unignore Packet	Ctri+D	of a reassemb	led PDU]		
54 3372 → 80 [ACK] Seq=480 Ack=1	Set/Unset Time Reference	Ctrl+T				
14 80 → 3372 [ACK] Seq=1381 Ack	Time Shift	Ctrl+Shift+T	ent of a reass	embled PDU]		
54 3372 → 80 [ACK] Seq=480 Ack=1	Packet Comment	Ctrl+Alt+C				
14 80 → 3372 [ACK] Seq=2761 Ack=	Edit Resolved Name		ent of a reass	embled PDU]		
14 80 → 3372 [PSH, ACK] Seq=414	Apply as Filter	•	segment of a	reassembled	PDU]	
54 3372 → 80 [ACK] Seq=480 Ack=	Prenare as Filter					
89 Standard query 0x0023 A pagea	Conversation Filter					
14 80 → 3372 [ACK] Seq=5521 Ack=			ent of a reass	embled PDU]		
54 3372 → 80 [ACK] Seq=480 Ack=0	Colorize Conversation	•				
14 80 → 3372 [ACK] Seq=6901 Ack	SCTP	•	ent of a reass	embled PDU1	_	
188 Standard query response 0x00	Follow	•	TCP Stream	Ctrl+Alt+Shift+T	CNAME	
775 GET /pagead/ads?client=ca-pul	Сору	•	UDP Stream	Ctrl+Alt+Shift+U	at=468;	
54 3372 → 80 [ACK] Seq=480 Ack=8	Protocol Preferences	•	TLS Stream	Ctrl+Alt+Shift+S		
14 80 → 3372 [ACK] Seq=8281 Ack=	Decode As		HTTP Stream	Ctrl+Alt+Shift+H		
14 80 → 3372 [PSH, ACK] Seq=966	Show Packet in New Window		HTTP/2 Stream		DU]	
54 3372 → 80 [ACK] Seq=480 Ack=	U41 WIII=9000 Leli=0		OUIC Stream			
14… 80 → 3372 [ACK] Seq=11041 Ack=	=480 Win=6432 Len=13	80 [TCP seg	ment of a reas	sempled PDUJ		-
					► I	

Petición

# II – Wireshark (follow stream)

GET /download.ntml HTTP/1.1		
Host: www.ethereal.com		
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gec	ko/20040113	
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,	<pre>text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1</pre>	-
Accept-Language: en-us,en;q=0.5		
Accept-Encoding: gzip,deflate		
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7		
Keep-Alive: 300		
Connection: keep-alive		
Referer: http://www.ethereal.com/development.html		
ITTP/1.1 200 OK		
Date: Thu, 13 May 2004 10:17:12 GMT		
Server: Apache		
ast-Modified: Tue, 20 Apr 2004 13:17:00 GMT		
Tag: "9a01a-4696-7e354b00"		
ccept-Ranges: bytes	1	
ontent-Length: 18070		
<pre>keep-Alive: timeout=15, max=100</pre>		
Connection: Keep-Alive		
.ontent-Type: text/ntml; charset=150-8859-1		
<pre><?xml version="1.0" encoding="UTF-8"?></pre>	R	
<pre>cloctype html</pre>	Kespuesta	
PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"		
"DTD/xhtmll-strict.dtd">		
<pre><html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml"></html></pre>		
<title>Ethereal: Download</title>		
<style media="all" type="text/css"></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td>@import url("mm/css/ethereal-3-0.css");</td><td></td><td></td></tr><tr><td>@import url("mm/css/ethereal-3-0.css"); </style>		
@import url("mm/css/ethereal-3-0.css");  		
@import url("mm/css/ethereal-3-0.css");   <body></body>		
@import url("mm/css/ethereal-3-0.css");   <body> <div class="top"> <table "0"="" border="" collopscing="0" collopsdding="0" cumm<="" td="" width="100%"><td>2.51-11</td><td></td></table></div></body>	2.51-11	
@import url("mm/css/ethereal-3-0.css");  <body> <div class="top"> <table border="0" cellpadding="0" cellspacing="0" summ<="" td="" width="100%"><td>ary=""&gt;</td><td></td></table></div></body>	ary="">	
@import url("mm/css/ethereal-3-0.css");  <body> <div class="top"></div></body>	ary="">	
<pre>@import url("mm/css/ethereal-3-0.css");   <body> <div class="top">   acket 4.1 client pkt.1 server pkt.1 turn. Click to select.</div></body></pre>	ary="">	
<pre>@import url("mm/css/ethereal-3-0.css");  <body> <div class="top"> <td.valion="middle" width="1"> acket 4. 1 client pkt, 1 server pkt, 1 turn. Click to select. Entire conversation (18kB)</td.valion="middle"></div></body></pre>	ary="">	
<pre>@import url("mm/css/ethereal-3-0.css");  <body> <div class="top"> acket 4. 1 client pkt, 1 server pkt, 1 turn. Click to select. Entire conversation (18kB)</div></body></pre>	ary=""> Show data as ASCII	



## II – Wireshark (export objects)

#### **Exportar objetos**

Ē	le <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> a	pture <u>A</u> nalyze <u>S</u> tatistics	Telephony <u>W</u> ireless	<u>T</u> ools <u>H</u> elp			
	<u>O</u> pen	Ctrl+O	🔿 堅 🚡 👲		ΘΘ		
	Open <u>R</u> ecent	*				 	
	Merge						
	Import from Hex Dump	1	stination	Protocol			
	<u>C</u> lose	Ctrl+W	.208.228.223	ТСР			
-	Save	Ctrl+S	5.254.160.2	TCP			
	Save <u>A</u> s	Ctrl+Shift+S	.208.228.223				
-	File Set	•	-2.224.10U.2				
-	Export Specified Packet	te	5 254 160 2				
	Export Specified Packet	LS	5 254 160 2				
	Export Packet Dissectio	ons /	208 228 223	тср			
	Export Packet Bytes	Ctri+Snitt+X	5 254 160 2	тср			
	Export PDUs to File		208 228 223	тср			
	Export TLS Session Key	/S	F 2F4 100 2	тср			
	Export Objects	•	DICOM	тср			
	<u>P</u> rint	Ctrl+P	HTTP	ТСР			
	<u>Q</u> uit	Ctrl+Q	IMF	ТСР			
Τ	33 4,356264	145.254.160.2 65	SMB B	TCP			
÷.	34 4.496465	65.208.228.223 14	TFTP	ТСР			
	35 4.496465	145.254.160.2 65	5.208.228.223	ТСР			
•	38 4.846969	65.208.228.223 14	45.254.160 <u>.2</u>	HTTP/XML			
	39 5.017214	145.254.160.2 65	5.208.228.223	ТСР			
	40 17.905747	65.208.228.223 14	45.254.160.2	TCP			
	41 17.905747	145.254.160.2 65	5.208.228.223	TCP			

## II – Wireshark (export objects)

	Wires	hark · Export · HTTP object list		
Packet	▼ Hostname	Content Type	Size	Filename 🔺
54	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
132	api.bing.com	text/html	1,305 bytes	qsml.aspx?qu(
163	api.bing.com	text/html	1,346 bytes	qsml.aspx?qu
.77	api.bing.com	text/html	1,369 bytes	qsml.aspx?que
98	api.bing.com	text/html	1,398 bytes	qsml.aspx?qu(
212	google.com	text/html	219 bytes	<i>i</i>
26	www.google.com	text/html	231 bytes	/
858	www.google.com	text/html	1,058 bytes	url?sa=t&rct=
904	www.bluproducts.com	text/html	19 kB	1
955	www.bluproducts.com	text/css	7,321 bytes	default_iceme
972	www.bluproducts.com	text/css	331 bytes	default_notjs.c
109	www.bluproducts.com	text/css	63 kB	widgetkit-241
136	www.bluproducts.com	application/x-javascript	4,707 bytes	core-816de4c
139	www.bluproducts.com	application/x-javascript	657 bytes	caption-5e0b3
280	www.bluproducts.com	application/x-javascript	20 kB	widgetkit-34c2
390	www.bluproducts.com	application/x-javascript	18 kB	cufon-yui-1d1
545	www.bluproducts.com	application/x-javascript	95 kB	mootools-core
560	www.bluproducts.com	application/x-javascript	93 kB	jquery-7ae67c
689	www.bluproducts.com	application/x-javascript	4,784 bytes	core.js
728	platform.linkedin.com	text/javascript	3,768 bytes	in.js
743	www.bluproducts.com	text/css	132 kB	template-897f
784	www.bluproducts.com	application/x-javascript	22 kB	template-3f20
898	www.bluproducts.com	image/png	19 kB	facebook.png
990	www.bluproducts.com	image/png	22 kB	Twitter.png
060	www.bluproducts.com	image/png	44 kB	googleplus.pn
066	s.amazon-adsystem.com	image/gif	43 bytes	iui3?d=3p-hbg
145	www.bluproducts.com	image/png	19 kB	mail.png 📃 💌
				•
ext Filte	er:			
Help		Sav	/e All <u>C</u> lose	Save



## II – Wireshark (filters)

#### Filtros de Wireshark

Podemos filtrar los paquetes en base a diferentes campos:

#### **Direcciones IP**

- IP: ip.addr == 10.10.50.1
- Origen: ip.src == 10.10.50.1
- Destino: ip.dest == 10.10.50.1
- Subred: ip.addr == 10.10.50.1/24

#### **Protocolos**

tcp

• udp

• dns

• http

ftp

. . .

•

#### **Operadores**

- and o &&
- or o ||
- xor o ^^
- not o !
  - <u>Texto</u>
- Edit  $\rightarrow$  Find packet  $\rightarrow$  String



## II – Wireshark *(filters)*

#### Ejemplo

	ftp.request && ip.src ==	192.168.0.147				
No.	Time	Source	Destination	Protocol	Length Info	
	241 4.035759	192.168.0.147	192.168.0.115	FTP	78 Request: USER	jenny
	269 4.043289	192.168.0.147	192.168.0.115	FTP	78 Request: USER	jenny
	273 4.108928	192.168.0.147	192.168.0.115	FTP	81 Request: PASS	football
	274 4.121641	192.168.0.147	192.168.0.115	FTP	79 Request: PASS	000000
	275 4.121775	192.168.0.147	192.168.0.115	FTP	83 Request: PASS	1234567890
	276 4.133276	192.168.0.147	192.168.0.115	FTP	81 Request: PASS	computer
	277 4.139140	192.168.0.147	192.168.0.115	FTP	81 Request: PASS	superman
	278 4.140089	192.168.0.147	192.168.0.115	FTP	81 Request: PASS	internet
	279 4.141101	192.168.0.147	192.168.0.115	FTP	84 Request: PASS	password123
	280 4.141239	192.168.0.147	192.168.0.115	FTP	81 Request: PASS	lqaz2wsx
	281 4.143016	192.168.0.147	192.168.0.115	FTP	79 Request: PASS	monkey
	282 4.143070	192.168.0.147	192.168.0.115	FTP	80 Request: PASS	michael
	283 4.143117	192.168.0.147	192.168.0.115	FTP	79 Request: PASS	shadow

Hemos usado dos filtros concatenados con (&&)

I. ftp.request  $\rightarrow$  Nos muestra todas las "request" del protocolo ftp

II. Ip.src == 192.168.0.147 → Nos muestra todos los paquetes que vienen de la IP "192.168.0.147"

••••

Universidad Rey Juan Carlos

#### Jerarquía de protocolos

Estadísticas  $\rightarrow$  Jerarquía de protocolo

ocolo	Porcent	aje de paquetes	Paquetes	Porcent	taje de bytes	Bytes	Bits/s	End Packets	End Bytes	End Bit
Frame		100.0	85634		100.0	18726049	62k	0	0	0
<ul> <li>Linux cooked-mode capture</li> </ul>		100.0	85634		7.3	1370144	4600	0	0	0
Internet Protocol Version 6		0.1	86		0.0	3440	11	0	0	0
<ul> <li>Internet Protocol Version 4</li> </ul>		64.5	55272		5.9	1105964	3713	0	0	0
<ul> <li>User Datagram Protocol</li> </ul>		0.5	444		0.0	3552	11	0	0	0
Simple Service Discovery Protocol		0.0	11		0.0	3008	10	11	3008	10
QUIC IETF		0.2	166		0.5	88082	295	119	50692	170
<ul> <li>NetBIOS Datagram Service</li> </ul>		0.0	3		0.0	603	2	0	0	0
> SMB (Server Message Block Protocol)		0.0	3		0.0	357	1	0	0	0
Domain Name System		0.4	309		0.3	58393	196	309	58393	196
Data		0.0	2		0.0	600	2	2	600	2
<ul> <li>Transmission Control Protocol</li> </ul>		63.9	54687		81.4	15242898	51k	24794	4335343	14k
Transport Layer Security		2.1	1815		12.7	2383885	8004	1791	2241486	7525
Malformed Packet		0.0	7		0.0	0	0	7	0	0
<ul> <li>Hypertext Transfer Protocol</li> </ul>		25.2	21573		45.6	8533837	28k	10312	1584477	5319
Portable Network Graphics		0.0	5		0.1	12319	41	5	12319	41
Online Certificate Status Protocol		0.0	16		0.0	4348	14	16	4348	14
Media Type		0.0	22		6.8	1264094	4244	22	902661	3030
Line-based text data		12.5	10700		30.6	5723438	19k	10700	4916620	16k
JPEG File Interchange Format		0.0	6		3.2	603766	2027	6	604920	2031
HTML Form URL Encoded		0.6	492		0.1	22856	76	492	142144	477
eXtensible Markup Language		0.0	8		0.1	20896	70	8	20896	70
Compuserve GIF		0.0	12		0.0	2486	8	12	2486	8
> FTP Data		0.1	72		7.1	1330793	4468	0	0	0
File Transfer Protocol (FTP)		5.3	4573		0.5	93259	313	4573	0	0
Data	- I	2.2	1877		0.2	39960	134	1877	39960	134
Internet Group Management Protocol		0.2	131		0.0	1048	3	131	1048	3
<ul> <li>Internet Control Message Protocol</li> </ul>		0.0	10		0.0	1816	6	8	1144	3
Data		0.0	2		0.0	600	2	2	600	2
Address Resolution Protocol		35.4	30276	I	4.6	854442	2868	30276	854442	2868
ay filtro de visualización.										



# II – Wireshark (Retos)





#### Análisis de discos

Extracción de información forense de los medios de almacenamiento digital, como pueden ser discos duros, dispositivos USB, unidades flash, CDs o DVDs...



Inés Martín y Carlos Barahona

## III – Análisis de discos: ¿qué buscar?

Jniversidad Lev Iuan Carlos

#### Artefactos

- Datos de navegación: historial, cookies, credenciales guardadas...
  - **Descarga de archivos:** navegador, adjuntos de emails...
    - Ejecución de programas
  - **Borrado de archivos:** papelera de reciclaje, file carving...
- Uso de cuentas: ¿quién fue el último usuario en loguearse? ¿qué hizo? ...
  - Apertura de archivos/carpetas recientes

...



### III – Autopsy

#### ¿Qué es Autopsy?

Autopsy es una herramienta utilizada en el ámbito forense que sirve para analizar imágenes de **disco**, tanto de Windows como de sistemas UNIX

(NTFS, Fat, Ext3/4, ....)





•••

Universidad Rey Juan Ca<u>rlos</u>

#### Instalación y uso



https://www.autopsy.com/download/





\$ sudo apt-get install autopsy (preinstalada en la VM del curso)



# III – Autopsy: primeros pasos

#### I. Crear un caso



Habrá que rellenar información que describa el caso que ha a analizar: nombre del caso, descripción, nombre de los investigadores...

😹 New Case Information	×
Steps	Optional Information
<ol> <li>Case Information</li> <li>Optional Information</li> </ol>	Case Number:
	Name:       Phone:       Email:       Notes:
	Organization Organization analysis is being done for: Not Specified  Manage Organizations
	< Back Next > Finish Cancel Help

#### **CREATE A NEW CASE** 1. Case Name: The name of this investigation. It can contain only letters, numbers, and symbols. 2. Description: An optional, one line description of this case. 3. Investigator Names: The optional names (with no spaces) of the investigators for this case. ь. d. f. e. h. NEW CASE CANCEL HELP



## III – Autopsy: primeros pasos

#### II.Agregar una imagen



- Location: ruta completa al fichero a analizar.
- Type: si el fichero es una imagen de disco entera o una partición (si no estamos seguros lo dejamos en disco)
- Método de importación: elegir el más conveniente

#### ADD A NEW IMAGE 1. Location Enter the full path (starting with /) to the image file. If the image is split (either raw or EnCase), then enter '\*' for the extension. /kali/Downloads/charlie-work-usb-2009-12-11.E01 2. Type Please select if this image file is for a disk or a single partition. O Disk O Partition 3. Import Method To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt. O Symlink Move Opv NEXT CANCEL HELP







Select a volume to analyze or add a new image file. **CASE GALLERY** HOST GALLERY HOST MANAGER 0 fs type mount name disk details charlie-work-usb-2009-12-11.E01-disk raw C:/ ntfs details charlie-work-usb-2009-12-11.E01-1-2068479 **CLOSE HOST** ANALYZE ADD IMAGE FILE HELP FILE ACTIVITY TIME LINES HASH DATABASES **IMAGE INTEGRITY** VIEW NOTES EVENT SEQUENCER





- File analysis: análisis del sistema de ficheros.
- Keyword search: búsqueda de texto. Admite expresiones regulares.
- File type: categoriza los archivos por su extensión. Intenta además detectar aquellos archivos que tengan su extensión cambiada.
- Meta data: detalles sobre entradas MFT en el sistema de archivos.
- **Data unit:** permite ver datos de distintas formas (hexadecimal, por ejemplo).







## III – Autopsy: primeros pasos

#### II.Agregar una imagen



- Elegir tipo de imagen
- Elegir la ruta del archivo

#### Tipos de imágenes soportadas

- Disk Image/VM file: <u>imágenes</u> que son una copia exacta de un disco duro, o una máquina virtual.
- Local disk: disco duro, pendrive, tarjeta de memoria...
- > Logical files: carpetas o archivos locales.
- Unallocated space image file: espacio no asignado.

😹 Add Data Source	×
Steps	Select Data Source Type
Select Host     Select Data Source Type     Select Data Source     Configure Ingest     Add Data Source	Disk Image or VM File
5. Add Data Source	Local Disk
	Logical Files
	Unallocated Space Image File
	Autopsy Logical Imager Results
	Memory Image File (Volatility)
	XRY Text Export
	< Back Next > Finish Cancel Help
elect Data Source	
ath:	
:\RetoNCL\dump.E01	Browse
Ignore orphan files in FAT	file systems



••••

Universidad Rey Juan Carlos



😹 Add Data Source	>
Steps	Configure Ingest
<ol> <li>Select Host</li> <li>Select Data Source Type</li> <li>Select Data Source</li> <li>Configure Ingest</li> <li>Add Data Source</li> </ol>	Run ingest modules on:       Image: All Files, Directories, and Unallocated Space         Image: All Files, Directories, and Unallocated Space       Image: The selected module has no per-run settings.         Image: All Files, Directories, and Unallocated Space       Image: The selected module has no per-run settings.         Image: All Files, Directories, and Unallocated Space       Image: The selected module has no per-run settings.         Image: All Files, Directories, and Unallocated Space       Image: The selected module has no per-run settings.         Image: All Files, Directories, and Unallocated Space       Image: The selected module has no per-run settings.         Image: All Files, Directories, and Unallocated Space       Image: The selected module has no per-run settings.
¡Plugins!	Image: Second
	<ul> <li>Email Parser</li> <li>Encryption Detection</li> <li>Interesting Files Identifier</li> <li>Central Repository</li> <li>PhotoRec Carver</li> </ul>
	Virtual Machine Extractor         Data Source Integrity         Select All         Deselect All         History
	< Back Next > Finish Cancel Help



Información

#### III – Autopsy: análisis del disco



₩ urjc ctf - Autopsy 4.19.1 Case View Tools Window Help												- 0	
Add Data Source 📠 Images/Videos 📉 Communicat	tions 💡 Geolocation 🗮 Timeline 縜 Discovery 🗽	Generate	Report	Slose Case						⊙ - Keyword	Lists	Q- Keyword	Search
Data Sources     Data fources     Arallework-usb-2009-12-11.E01_1 Host	Listing /mg_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth Table Thumbnail Summary	er										Cave Tabl	15 Res
Charlie-work-usb-2009-12-11.E01           vol1 (Unallocated: 0-0)	A Name	s (	. 0	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Known	MD5 Hash	SHA
□ □ vol2 (NTFS / exFAT (0x07): 1-2068479)	Charlie 2009-12-07 1142 Sent.txt			/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:38:25 CET	2009-12-10 23:38:25 CET	2009-12-10 23:38:25 CET	2009-12-10 23:38:25 CET	375	Allocated	unknown	THE STREET	- Silk
SorphanFiles (0)	Charlie_2009-12-07_1144_Sent.txt			/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:37:16 CET	2009-12-10 23:37:17 CET	2009-12-10 23:37:16 CET	2009-12-10 23:37:16 CET	199	Allocated	unknown		
\$Unalloc (1)	Charlie_2009-12-07_1144_Sent_microscope 1.jpg	-		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:29:38 CET	2009-12-10 23:37:59 CET	2009-12-10 23:29:38 CET	2009-12-10 23:29:37 CET	136274	Allocated	unknown		
🖨 🖟 Email (91)	Charlie_2009-12-07_1255_Sent.txt	▽		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:36:12 CET	2009-12-10 23:36:12 CET	2009-12-10 23:36:12 CET	2009-12-10 23:36:12 CET	307	Allocated	unknown		
uther (15)	Charlie_2009-12-08_1259_Sent.txt	V		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:38:40 CET	2009-12-10 23:38:40 CET	2009-12-10 23:38:40 CET	2009-12-10 23:38:40 CET	368	Allocated	unknown		
Eile Viewe	Charlie_2009-12-08_1418_Sent.txt	V		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:36:50 CET	2009-12-10 23:36:50 CET	2009-12-10 23:36:50 CET	2009-12-10 23:36:50 CET	287	Allocated	unknown		
🗄 📽 File Types	Charlie_2009-12-10_1418_Sent.txt	▽		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	412	Allocated	unknown		
🗈 😠 Deleted Files	Great Lunch.txt	▽		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:28:55 CET	2009-12-10 23:35:43 CET	2009-12-10 23:28:55 CET	2009-12-10 23:28:55 CET	307	Allocated	unknown		
B File Size	Hey.txt	▽		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:29:06 CET	2009-12-10 23:36:25 CET	2009-12-10 23:29:06 CET	2009-12-10 23:29:06 CET	287	Allocated	unknown		
Data Artifacts	Picture.eml.txt	▽		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:28:17 CET	2009-12-10 23:36:56 CET	2009-12-10 23:28:17 CET	2009-12-10 23:28:17 CET	199	Allocated	unknown		
Analysis Results	QC Project.eml.txt	▽		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:28:05 CET	2009-12-10 23:37:22 CET	2009-12-10 23:28:05 CET	2009-12-10 23:28:05 CET	375	Allocated	unknown		
🗄 💁 Keyword Hits (293)	Vacation time.txt	$\bigtriangledown$		/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:29:01 CET	2009-12-10 23:38:28 CET	2009-12-10 23:29:01 CET	2009-12-10 23:29:01 CET	368	Allocated	unknown		
OS Accounts	When's it coming.txt			/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:29:11 CET	2009-12-10 23:38:44 CET	2009-12-10 23:29:11 CET	2009-12-10 23:29:11 CET	412	Allocated	unknown		
Tags	🖟 [current folder]			/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	2009-12-10 23:27:49 CET	56	Allocated	unknown		
E Reports	🖟 [parent folder]			/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:27:55 CET	2009-12-10 23:27:55 CET	2009-12-10 23:29:38 CET	2009-12-03 22:16:59 CET	56	Allocated	unknown		



<u></u>

Universidad Rey Juan Carlos



△ Name	s	С	0	Location	Modified Time	Change Time	Access Time	Created Time	Size
Charlie_2009-12-07_1142_Sent.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:38:25 CET	2009-12-10 23:38:25 CET	2009-12-10 23:38:25 CET	2009-12-10 23:38:25 CET	375
Charlie_2009-12-07_1144_Sent.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:37:16 CET	2009-12-10 23:37:17 CET	2009-12-10 23:37:16 CET	2009-12-10 23:37:16 CET	199
Charlie_2009-12-07_1144_Sent_microscope1.jpg				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:29:38 CET	2009-12-10 23:37:59 CET	2009-12-10 23:29:38 CET	2009-12-10 23:29:37 CET	1362
Charlie_2009-12-07_1255_Sent.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:36:12 CET	2009-12-10 23:36:12 CET	2009-12-10 23:36:12 CET	2009-12-10 23:36:12 CET	307
Charlie_2009-12-08_1259_Sent.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:38:40 CET	2009-12-10 23:38:40 CET	2009-12-10 23:38:40 CET	2009-12-10 23:38:40 CET	368
Charlie_2009-12-08_1418_Sent.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:36:50 CET	2009-12-10 23:36:50 CET	2009-12-10 23:36:50 CET	2009-12-10 23:36:50 CET	287
Charlie_2009-12-10_1418_Sent.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	412
Great Lunch.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:28:55 CET	2009-12-10 23:35:43 CET	2009-12-10 23:28:55 CET	2009-12-10 23:28:55 CET	307
Hey.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:29:06 CET	2009-12-10 23:36:25 CET	2009-12-10 23:29:06 CET	2009-12-10 23:29:06 CET	287
Picture.eml.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:28:17 CET	2009-12-10 23:36:56 CET	2009-12-10 23:28:17 CET	2009-12-10 23:28:17 CET	199
QC Project.eml.txt	▽			/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:28:05 CET	2009-12-10 23:37:22 CET	2009-12-10 23:28:05 CET	2009-12-10 23:28:05 CET	375
Vacation time.txt	$\bigtriangledown$			/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:29:01 CET	2009-12-10 23:38:28 CET	2009-12-10 23:29:01 CET	2009-12-10 23:29:01 CET	368
When's it coming.txt				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:29:11 CET	2009-12-10 23:38:44 CET	2009-12-10 23:29:11 CET	2009-12-10 23:29:11 CET	412
退 [current folder]				/img_charlie-work-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	2009-12-10 23:39:09 CET	2009-12-10 23:27:49 CET	56
🔑 [parent folder]				/img_ch/ork-usb-2009-12-11.E01/vol_vol2/Email/oth	2009-12-10 23:27:55 CET	2009-12-10 23:27:55 CET	2009-12-10 23:29:38 CET	2009-12-03 22:16:59 CET	56
: Hex Text Application File Metadata OS Account Strings Indexed Text Translation	Data Ari	tifacts	Anal	ysis Results   Context   Annotations   Other Occurrences					
Page: 1 of 1 Page	of - Ma	atch	€ 3	100% 💭 🕀 Reset					
Jubject: jreat Lunch 'rom: 'harlie <charlie@m57.biz> Jate: Mon, 07 Dec 2009 12:55:40 -0800 To: Tat McGoo <pat@m57.biz>, Terry Johnson <terry@m57.< td=""><td>7.biz&gt;, :</td><td>Jo Smi</td><td>th <io≬< td=""><td>₽m57.biz&gt;</td><td></td><td></td><td></td><td></td><td></td></io≬<></td></terry@m57.<></pat@m57.biz></charlie@m57.biz>	7.biz>, :	Jo Smi	th <io≬< td=""><td>₽m57.biz&gt;</td><td></td><td></td><td></td><td></td><td></td></io≬<>	₽m57.biz>					





#### Navegación por directorios



#### Categorización de archivos + Información relevante

File Views 🖨 🖧 File Types 🚊 🖧 By Extension Images (10) Videos (0) Audio (0) Archives (3) tabases () 🖶 🗟 Documents HTML (0) Office (1) PDF (6) Plain Text (88) Rich Text (0) 🗄 🧟 Executable 🗄 🗟 By MIME Type 🖶 χ Deleted Files File System (2) ..... 🗙 🛛 All (2) • MB File Size Data Artifacts Metadata (8) -- 🔍 Analysis Results Keyword Hits (293)
 Keyword Hits ( - 🖳 OS Accounts S Tags Reports

#### Búsqueda de texto





#### III – Autopsy: para practicar



**Disk Analysis & Autopsy** 

Inés Martín y Carlos Barahona



# Módulo II: Forense

#### Ismael Gómez, Inés Martín y Carlos Barahona

