

Modulo II: Forense

Ismael Gómez Esquilichi y Alejandro Bermejo Pérez



Índice

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

2. Wireshark

- I. ¿Qué es?
- 2. Ejemplos de uso

3. Autopsy

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



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





I.Volatility – Comandos Básicos (imageinfo)

(urjc BETSIICTF)-[~/Documentos/dump]
_\$ vol.py -f dump.raw imageinfo

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

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

Ismael Gómez y Alejandro Bermejo

I.Volatility – Comandos Básicos (pslist)

•••

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

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

Ismael Gómez y Alejandro Bermejo

5

I.Volatility – Comandos básicos (pstree)

<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	ility –f <u>imagen.v</u>	<u>'mem</u> p	rofile=W	VinXPSF	2x86 pstree	9	
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
<pre> 0x817757f0:svchost.exe</pre>	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**

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	Foundation Volatility	Framework 2.6.1	Pid
Offset(P)	Local Address	Remote Address	
	0.0.0.0:1026		
0x01a25a50		172.16.98.1:6666	1956

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}
0x000000000015ac5c8	1	1	Rrw-	<pre>\Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows.Co</pre>
0x00000000015ac6b0	1	0	Rrw-	<pre>\Device\HarddiskVolume1\WINDOWS\Media\Windows XP Startup.wav</pre>
0x000000000015ac8f0	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>
0x000000000015ad740	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)

Image

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 - Wireshark

¿Qué es Wireshark?

Es una herramienta que intercepta tráfico/sniffer (admite más de 2000 protocolos de red), que muestra en una interfaz sencilla paquete a paquete y todos los datos que contiene..

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 Capture Analyze</u>	Statistics lelephony Wireless Tools Help		
Apply a display filter <ctrl-></ctrl->			
No. Time Source	Destination Protocol	Length Info	
	14/ 192.168.0.115 TCP	$7452670 \rightarrow 80$ [SYN] Seq=0 W1n=64240 Len=0 M	SS=1460 SACK_PERM=1
448 32.24516 192.168.0.	115 192.168.0.147 ICP	$/480 \rightarrow 520/0$ [SYN, ALK] Seq=0 ACK=1 W1N=05	160 Len=0 MSS=1460 SA
449 32.24518 192.108.0	147 192.108.0.115 ICP	$00 52070 \rightarrow 00 [AUK] Seq=1 ACK=1 WIN=04230 L$	en=0 TSVat=1407804982
450 52.24552 192.108.0.	147 192.108.0.115 HTTP 115 192 168 0 147 TCP	$407 \text{ GET / SHELL, PHP HTP/1.1}$ $66.80 \rightarrow 52670 \text{ [ACK] Seg-1 Ack-342 Win-64896}$	len=0 TSval=17019546
451 52.24505 192.100.0.	115 192.100.0.147 TCP	$7453734 \rightarrow 80$ [SVN] Seq-0 Win-64240 Len-0 M	SS-1460 SACK PERM-1 1
452 52.24004 192.100.0.	147 192 168 0 115 TCP	$74.95734 \Rightarrow 660 [STN] 364=0 Win=64240 [en=6.1]$	160 Len=0 MSS=1460 S4
454 32.24908 192.168.0.	115 192.168.0.147 TCP	$66\ 53734 \rightarrow 80\ [ACK]\ Seg=1\ Ack=1\ Win=64256\ L$	en=0 TSval=1701954101
455 32.25470 192.168.0.	115 192.168.0.147 TCP	$17253734 \rightarrow 80$ [PSH, ACK] Seg=1 Ack=1 Win=64	256 Len=106 TSval=176
456 32.25472 192.168.0.	147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seg=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=1
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=17
460 32.27585 192.168.0.	147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seq=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] Seq=360 Ack=1 Win=	64256 Len=12 TSval=17
462 32.27786 192.168.0.	147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seq=1 Ack=372 Win=65024	Len=0 TSval=14078050
463 32.27812 192.168.0.	115 192.168.0.147 TCP	109 53734 → 80 [PSH, ACK] Seq=372 Ack=1 Win=	64256 Len=43 TSval=17
464 32.27813 192.168.0.	147 192.168.0.115 TCP	66 80 → 53734 [ACK] Seq=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] Seq=1 AcK=415 Win=	65024 Len=7 TSval=140
466 36.53792 192.168.0.	115 192.168.0.147 TCP	$bb 53/34 \rightarrow 80 [ACK] Seq=415 ACK=8 W1n=b425b$	Len=0 ISVal=1/01958:
407 30.54057 192.108.0.	115 192.168.0.147 TCP	/5 53734 → 80 [PSH, ALK] Seq=415 ACK=8 W1N=	04250 Len=9 ISVal=1/0
Transmission Control Pro-	tocol, Src Port: 52670, Dst Port	: 80, Seg: 1, Ack: 1, Len: 341	A
- Hypertext Transfer Proto	col		
GET /shell.php HTTP/1.1	1\r\n		
Host: 192.168.0.115\r\r	n		
User-Agent: Mozilla/5.0	0 (X11; Linux x86_64; rv:78.0) Ge	ecko/20100101 Firefox/78.0\r\n	
Accept: text/html,appl	ication/xhtml+xml,application/xm	l;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		
UNI: 1\r\n	0.0. 20.4. b0.ed 08.00.45.00		
	0 0C 29 4a D9 C0 08 00 45 00 0 06 06 fb c0 38 00 03 c0 38	······································	-
0020 00 73 cd be 00 50 01	9 f 1 c bb 87 c6 14 06 80 18	sP	
		5 .	•
😑 🝸 Capture.pcapng		Packets: 907 · Displayed: 907 (100.0%)	Profile: Default

14



II – Wireshark (Follow Stream)

Length Info					
62 3372 → 80 [SYN] Seq=0 Win=876	0 Len=0 MSS=1460 SAC	CK_PERM=1			
62 80 → 3372 [SYN, ACK] Seq=0 Ac	k=1 Win=5840 Len=0 M	1SS=1380 SAC	K_PERM=1		
54 3372 → 80 [ACK] Seq=1 Ack=1 W	in=9660 Len=0				
533 GET /download.html HTTP/1.1	Mark/Upmark Packot	Ctrl+M			
54 80 → 3372 [ACK] Seq=1 Ack=480		Ctrl+M	_		
14 80 → 3372 [ACK] Seq=1 Ack=480	Ignore/Unignore Packet	Ctri+D	of a reassem	bled PDU]	
54 3372 → 80 [ACK] Seq=480 Ack=1	Set/Unset Time Reference	Ctrl+1	_		
14 80 → 3372 [ACK] Seq=1381 Ack	Time Shift	Ctrl+Shift+T	ent of a reas	sembled 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 reas	sembled PDU]	
14 80 → 3372 [PSH, ACK] Seq=414	Apply as Filter	•	segment of a	reassembled	PDU]
54 3372 → 80 [ACK] Seq=480 Ack=	Prepare as Filter	+			
89 Standard query 0x0023 A page	Conversation Filter	•			
14 80 → 3372 [ACK] Seq=5521 Ack	Colorize Conversation	•	ent of a reas	sembled PDUJ	
54 33/2 → 80 [ACK] Seq=480 ACK=	SCTP				
14 80 → 3372 [ACK] Seq=6901 ACK	Follow		ent of a reas	Sempled PDUI	CHAM
188 Standard query response 0x00.	FOILOW		ICF Stream	CUITAILTSHIILT I	CNAM
//S GET /pagead/ads?client=ca-put	Сору	•	UDP Stream	Ctri+Alt+Shift+U	at=46
$54 \ 3372 \rightarrow 80 \ [ACK] \ Seq=480 \ ACK=0$	Protocol Preferences	•	TLS Stream	Ctrl+Alt+Shift+S	
$1480 \rightarrow 3372 \text{ [ACK] Seq=8281 ACK}$	Decode As		HTTP Stream	Ctrl+Alt+Shift+H	
$1400 \rightarrow 5572$ [PSR, ACK] Seq=900.	Show Packet in New <u>W</u> indow		HTTP/2 Stream		00]
$54 \ 3372 \rightarrow 80 \ [ACK] \ Seq=480 \ ACK=1$	1041 WIN=9000 Len=0		QUIC Stream		

Opción muy útil para seguir la conversación HTTP

II – Wireshark (Follow Stream)

<u>•••</u>

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

Petición

_ 🗆 🗙 Wireshark · Follow HTTP Stream (tcp.stream eq 0) · http.cap GET /download.html HTTP/1.1 Host: www.ethereal.com User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1 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 HTTP/1.1 200 OK Date: Thu, 13 May 2004 10:17:12 GMT Server: Apache Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT ETag: "9a01a-4696-7e354b00" Accept-Ranges: bytes Content-Length: 18070 Keep-Alive: timeout=15, max=100 Connection: Keep-Alive Content-Type: text/html; charset=ISO-8859-1 <?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE html Respuesta PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> <head> <title>Ethereal: Download</title> <style type="text/css" media="all"> @import url("mm/css/ethereal-3-0.css"); </style> </head> <body> <div class="top"> Packet 4. 1 client pkt, 1 server pkt, 1 turn. Click to select. Entire conversation (18kB) Show data as ASCII Ŧ Ŧ Find: Find <u>N</u>ext 👯 Help Filter Out This Stream Print Save as... Back X Close

II – Wireshark (Export Objects)

<u>...</u>

Universidad Rey Juan Carlos

Ē	ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> a	apture <u>A</u> nalyze <u>S</u> tatistics	Telephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp
Γ	<u>O</u> pen	Ctrl+O	
	Open <u>R</u> ecent	•	
ļ.	Merge		
ſ	Import from Hex Dump	ρ	stination Protocol
	<u>C</u> lose	Ctrl+W	.208.228.223 TCP
	Save	Ctrl+S	5.254.100.2 TCP
	Save <u>A</u> s	Ctrl+Shift+S	5 254 160 2 TCP
-	File Set	•	208 228 223 TCP
-	Export Specified Packe	ets	5.254.160.2 TCP
	Export Packet Dissection	ons 🕨	5.254.160.2 TCP
	Export Packet Bytes	Ctrl+Shift+X	.208.228.223 TCP
	Export PDUs to File		5.254.160.2 TCP
	Export TLS Session Key	ys	.208.228.223 TCP
	Export Objects	•	DICOM TCP
	Print	Ctrl+P	нттр В ТСР
-	 Ouit	Ctrl+0	ICP
Т	33 / 35626/	145 254 160 2 65	SMB B TCP
	34 4, 496465	65,208,228,223 14	TFTP
	35 4,496465	145.254.160.2 65	5.208.228.223 TCP
•	- 38 4.846969	65.208.228.223 14	L45.254.160.2 HTTP/XML
	39 5.017214	145.254.160.2 65	5.208.228.223 TCP
	40 17.905747	65.208.228.223 14	L45.254.160.2 TCP
	41 17.905747	145.254.160.2 65	5.208.228.223 TCP
	42 30.063228	145.254.160.2 65	55.208.228.223 TCP
	- 43 30.393/04	05.208.228.223 14	145.254.100.2 ICP

Opción útil para exportar objetos de distintos protocolos

17

II – Wireshark (Export Objects)

Wiresharl	k · Export	 HTTP ob 	ject lis
-----------	------------	-----------------------------	----------

Packet Hostname Content Type Size Filename www.msftncsi.com 54 text/plain 14 bytes ncsi.txt 132 api.bing.com text/html 1,305 bytes gsml.aspx?gue 163 api.bing.com text/html 1,346 bytes gsml.aspx?que 177 api.bing.com text/html 1,369 bytes gsml.aspx?gue api.bing.com 1,398 bytes gsml.aspx?gue 198 text/html 212 text/html 219 bytes google.com 226 www.google.com text/html 231 bytes 1,058 bytes url?sa=t&rct= www.google.com text/html 1858 www.bluproducts.com text/html 1904 19 kB www.bluproducts.com 7,321 bytes default iceme 1955 text/css www.bluproducts.com default notis.d text/css 331 bytes 1972 widgetkit-241 2109 www.bluproducts.com text/css 63 kB www.bluproducts.com 2136 application/x-javascript 4,707 bytes core-816de4c 2139 www.bluproducts.com application/x-javascript 657 bytes caption-5e0b3 2280 www.bluproducts.com application/x-javascript widgetkit-34c2 20 kB www.bluproducts.com 2390 application/x-javascript cufon-yui-1d1 18 kB www.bluproducts.com application/x-javascript 2545 95 kB mootools-core 2560 www.bluproducts.com application/x-javascript 93 kB jquery-7ae67c 2689 www.bluproducts.com application/x-javascript 4,784 bytes core.js 2728 platform.linkedin.com text/javascript 3,768 bytes in.js www.bluproducts.com template-897f 2743 text/css 132 kB www.bluproducts.com application/x-javascript 22 kB template-3f20 2784 www.bluproducts.com 19 kB 2898 image/png facebook.png www.bluproducts.com 22 kB Twitter.png 2990 image/png www.bluproducts.com 44 kB googleplus.pn 3060 image/png iui3?d=3p-hbc 3066 s.amazon-adsystem.com image/gif 43 bytes 3145 www.bluproducts.com 19 kB mail.png image/png × Image: A second seco 4 Text Filter: Save All Close Help Save



II – Wireshark (Filtros)

	tp.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: U	SER jenny
	269 4.043289	192.168.0.147	192.168.0.115	FTP	78 Request: U	SER jenny
	273 4.108928	192.168.0.147	192.168.0.115	FTP	81 Request: P	ASS football
	274 4.121641	192.168.0.147	192.168.0.115	FTP	79 Request: P	ASS 000000
	275 4.121775	192.168.0.147	192.168.0.115	FTP	83 Request: P	ASS 1234567890
	276 4.133276	192.168.0.147	192.168.0.115	FTP	81 Request: P	ASS computer
	277 4.139140	192.168.0.147	192.168.0.115	FTP	81 Request: P	ASS superman
	278 4.140089	192.168.0.147	192.168.0.115	FTP	81 Request: P	ASS internet
	279 4.141101	192.168.0.147	192.168.0.115	FTP	84 Request: P	ASS password123
	280 4.141239	192.168.0.147	192.168.0.115	FTP	81 Request: P	ASS 1qaz2wsx
	281 4.143016	192.168.0.147	192.168.0.115	FTP	79 Request: P	ASS monkey
	282 4.143070	192.168.0.147	192.168.0.115	FTP	80 Request: P	ASS michael
	283 4.143117	192.168.0.147	192.168.0.115	FTP	79 Request: P	ASS shadow

Hemos usado dos filtros concatenados con (&&)

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



II – Wireshark (Retos)





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,)



III - Autopsy

Antes de analizar tenemos que crear un caso

I. Nombre del caso

II. Descripción

III. Participantes en la investigación

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.



III - Autopsy (Añadir nueva imagen)

Para agregar una imagen al caso simplemente escribimos la ruta completa al fichero a analizar.

Después, indicar si el fichero es una **imagen de disco entera** o una **partición** (si no estamos seguros lo dejamos en disco)

De método de importación, elegir el que más convenga (por temas de espacio elegí enlace simbólico)

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.

/home/ismael/ragnarok/autopsy_sample.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.

Symlink	• Сору	O Move
	NEXT	
CANCEL	- 4	HELP



III – Autopsy (Analizar disco)

Select a volume to analyze or add a new image file.

mount	name		fs type	
🔿 disk	autopsy_samp]	le.E01-disk	raw	<u>detail</u>
○ C:/	autopsy_samp]	le.E01-63-4095944	fat32	<u>detail</u>
		HELP		
		HELP		



III – Autopsy (Tipos de análisis)



Tenemos varios tipos de análisis:

```
I. File Analysis -> Análisis del sistema de ficheros
```

- II. Keyword Search -> Un "strings" a lo bestia
- III. FileType -> "file" a lo bestia, intenta detectar ficheros con extensión cambiada

IV. MetaData -> Útil para recuperar

V. Data Unit -> Te permite ver datos de distintas formas, como hexdump, dd, etc...

III – Autopsy (File Analysis)

	Directory Seek		u / u	_+01331_/	2009-11-20 10.49.32 (CE1)	2009-11-20 00.00.00 (CE1)	10:49:30 (CET)
> >	Enter the name of a	1	r / r	_54402.EXE	2009-11-20 10:31:36 (CET)	2009-11-20 00:00:00 (CET)	2009-11-20 10:31:34 (CET)
	directory that you want to view.	~	d / d	_604468_/	2009-11-20 10:51:54 (CET)	2009-11-20 00:00:00 (CET)	2009-11-20 10:51:53 (CET)
	V		d / d	Log/	2009-12-07 08:05:22 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:20 (CET)
			r / r	<u>M57biz.jpg</u>	2009-11-17 08:50:26 (CET)	2009-12-07 00:00:00 (CET)	2009-11-17 08:50:25 (CET)
	File Name Search		r / r	<u>patentauto.py</u>	2009-11-17 13:37:00 (CET)	2009-11-17 00:00:00 (CET)	2009-11-16 14:16:49 (CET)
	expression for the file		r / r	<u>patentterms.txt</u>	2009-11-16 14:29:38 (CET)	2009-11-24 00:00:00 (CET)	2009-11-14 17:43:57 (CET)
	names you want to find.		r / r	<u>R54402.EXE</u>	2009-11-20 10:31:44 (CET)	2009-12-07 00:00:00 (CET)	2009-11-20 10:31:34 (CET)
	SEARCH		r / r	TERRYS WORK (Volume Label Entry)	2009-11-17 13:47:24 (CET)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)
	ALL DELETED FILES		r / r	<u>urlscopyright.txt</u>	2009-11-17 10:40:56 (CET)	2009-11-24 00:00:00 (CET)	2009-11-17 10:40:57 (CET)
	EXPAND DIRECTORIES		r / r	<u>urlscryptography.txt</u>	2009-11-16 10:22:50 (CET)	2009-11-24 00:00:00 (CET)	2009-11-16 10:22:51 (CET)
			r / r	<u>urlspatents.txt</u>	2009-11-17 10:40:56 (CET)	2009-11-24 00:00:00 (CET)	2009-11-17 10:40:57 (CET)
			r / r	<u>urlspersona.txt</u>	2009-11-14 17:43:14 (CET)	2009-11-24 00:00:00 (CET)	2009-11-14 17:41:55 (CET)
			r / r	<u>urlstime_machine.txt</u>	2009-11-16 10:22:50 (CET)	2009-11-24 00:00:00 (CET)	2009-11-16 10:22:51 (CET)
			r / r	vnc-4_1_3-x86_win32.exe	2008-10-15 17:14:08 (CEST)	2009-12-07 00:00:00 (CET)	2008-10-15 17:14:08 (CEST)
			r / r	webauto.py	2009-11-16 14:23:38 (CET)	2009-11-24 00:00:00 (CET)	2009-11-14 17:39:19 (CET)
		~	r / r	<u>xpadvancedkeylogger.exe</u>	2009-12-03 09:40:44 (CET)	2009-12-07 00:00:00 (CET)	2009-12-03 09:41:16 (CET)

III – Autopsy (File Analysis)

≞ Ū

Universidad Rey Juan Carlos

Directory Seek Enter the name of a	ASCII (<u>display</u> - <u>report</u>) * Hex (<u>display</u> - <u>report</u>) * ASCII Strings (<u>display</u> - <u>report</u>) * <u>Export</u> * <u>Add Note</u> File Type: Python script, ASCII text executable						
directory that you want to view. C:/	Contents Of File: C:/patentauto.py						
View	<pre>#! /usr/bin/pythonauthor="LCDR Kris Kearton" date = "\$Aug 24 2009 7:42:41 PM\$"</pre>						
File Name Search Enter a Perl regular expression for the file names you want to find.	<pre># class: CS4920 ADOMEX # System info: Running on OS 10.6 python ver 2.6.2 # Setup information: # (1) Install MozRepl Plugin at: # http://wiki.github.com/bard/mozrepl # Once installed, ensure in Firefox under tools MozRepl is started # #</pre>						
SEARCH	# Summary: MozRepl needs to telnet to the browser via port 4242. Once connected the port can program # can issue commands directly to the web browser. This program gets the list of urls from the text file. # Then randomly picks a URL and surfs it for background noise.						
ALL DELETED FILES	<pre>import time import csv import telnetlib import robotparser import os import random</pre>						
	<pre># #connect to MozRepl and fetch HTML # def connect_mozrepl(url_addr): quit = False t = telnetlib.Telnet("localhost", 4242) t.read_until("repl>")</pre>						
<	<pre>#verifies page was accepted rp = robotparser.RobotFileParser() fetched = rp.can_fetch("*", url_addr) print fetched state = True while(state==True): if fetched==True:</pre>						

27

III – Autopsy (File Analysis)

Current Directory: <u>C:/</u> /Log/												
AD		GENERATE MD5 LIST OF FILES										
DEL	Type <u>dir</u> / <u>in</u>	NAME Q	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	Мета			
	d / d	<u>/</u>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4096	0	0	2			
	d / d	<u>/</u>	2009-12-07 08:05:22 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:20 (CET)	643072	0	0	<u>72</u>			
	r / r	2009-12-03.htm	2009-12-03 23:59:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:20 (CET)	441396	0	0	<u>4231</u>			
	r / r	<u>2009-12-03_00036d9f_big.jpg</u>	2009-12-03 19:11:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:21 (CET)	74965	0	0	<u>4235</u>			
	r / r	<u>2009-12-03_00036d9f_small.jpg</u>	2009-12-03 19:11:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:21 (CET)	4369	0	0	<u>4239</u>			
	r / r	<u>2009-12-03_0005425f_big.jpg</u>	2009-12-03 19:13:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:21 (CET)	74958	0	0	<u>4243</u>			
	r / r	<u>2009-12-03_0005425f_small.jpg</u>	2009-12-03 19:13:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:21 (CET)	4369	0	0	<u>4247</u>			
	r / r	<u>2009-12-03_0007171f_big.jpg</u>	2009-12-03 19:15:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:21 (CET)	74971	0	0	<u>4251</u>			
	r / r	<u>2009-12-03_0007171f_small.jpg</u>	2009-12-03 19:15:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:21 (CET)	4369	0	0	<u>4255</u>			
	r / r	<u>2009-12-03_0008ebdf_big.jpg</u>	2009-12-03 19:17:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:22 (CET)	74957	0	0	<u>4259</u>			
	r / r	2009-12-03_0008ebdf_small.jpg	2009-12-03 19:17:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:22 (CET)	4369	0	0	<u>4263</u>			
	r / r	<u>2009-12-03_000ac09f_big.jpg</u>	2009-12-03 19:19:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:22 (CET)	74965	0	0	<u>4267</u>			
	r / r	<u>2009-12-03_000ac09f_small.jpg</u>	2009-12-03 19:19:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:22 (CET)	4369	0	0	<u>4271</u>			
	r / r	<u>2009-12-03_000c955f_big.jpg</u>	2009-12-03 19:21:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:22 (CET)	12663	0	0	<u>4275</u>			
	r / r	<u>2009-12-03_000c955f_small.jpg</u>	2009-12-03 19:21:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:22 (CET)	1186	0	0	<u>4279</u>			
	r / r	2009-12-03_000e6a1f_big.jpg	2009-12-03 19:23:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:22 (CET)	12538	0	0	<u>4283</u>			
	r / r	2009-12-03_000e6a1f_small.jpg	2009-12-03 19:23:10 (CET)	2009-12-07 00:00:00 (CET)	2009-12-07 08:05:23 (CET)	1165	0	0	<u>4287</u>			

Navegación por distintos directorios del disco



Modulo II: Forense

Ismael Gómez Esquilichi y Alejandro Bermejo Pérez

