

Análisis Forense a Sistemas Windows

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético & Forense Digital

Sitio Web: www.reydes.com / Correo Electrónico: reydes@gmail.com

Alonso Eduardo Caballero Quezada OWASP™

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures y Pen Testing.

Instructor y expositor en OWASP Perú, PERUHACK, 8.8 Lucky Perú. Más de 16 años de experiencia y desde hace 12 años labora como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú.



https://twitter.com/Alonso_ReYDeS



<https://www.facebook.com/alonsoreydes/>



<https://www.linkedin.com/in/alonsocaballeroquezada/>



<https://www.youtube.com/c/AlonsoCaballero>



<http://www.reydes.com>



reydes@gmail.com

¿Forense Digital?

Rama de la ciencia forense abarcando la recuperación e investigación de material encontrado en dispositivos digitales, frecuentemente relacionados con crímenes cometidos por computadoras.

El Forense de computadoras es una rama de la ciencia forense digital, pertinente a la evidencia encontrada en computadoras y medios digitales de almacenamiento.

Su objetivo es examinar medios digitales de una manera “forense”, con el propósito de identificar, preservar, recuperar, analizar, y presentar hechos sobre la información digital.

El análisis forense es la etapa donde se realiza una investigación profunda, cuyo propósito es identificar objetivamente y documentar los culpables, razones, ruta y consecuencias de un incidente de seguridad, violación de las leyes, etc.

¿Cómo es un Laboratorio Forense?

Un Laboratorio Forense Digital



¿Cuales Herramientas Forenses se Utilizan?

Software Forense



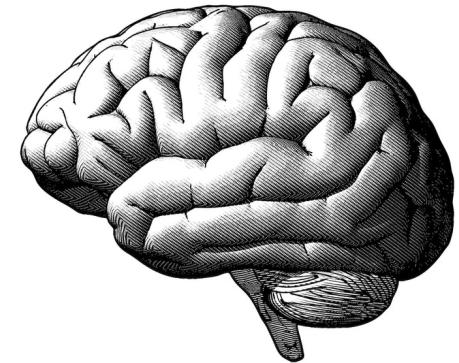
ACCESSDATA
ForensicToolkit (FTK)



MAGNET
FORENSICS®



AUTOPSY
DIGITAL FORENSICS



- * <https://www.guidancesoftware.com/encase-forensic>
- * <https://accessdata.com/products-services/forensic-toolkit-ftk>
- * <https://www.magnetforensics.com/for-forensic-examiners/>
- * <https://www.autopsy.com/>
- * <https://digital-forensics.sans.org/community/downloads>

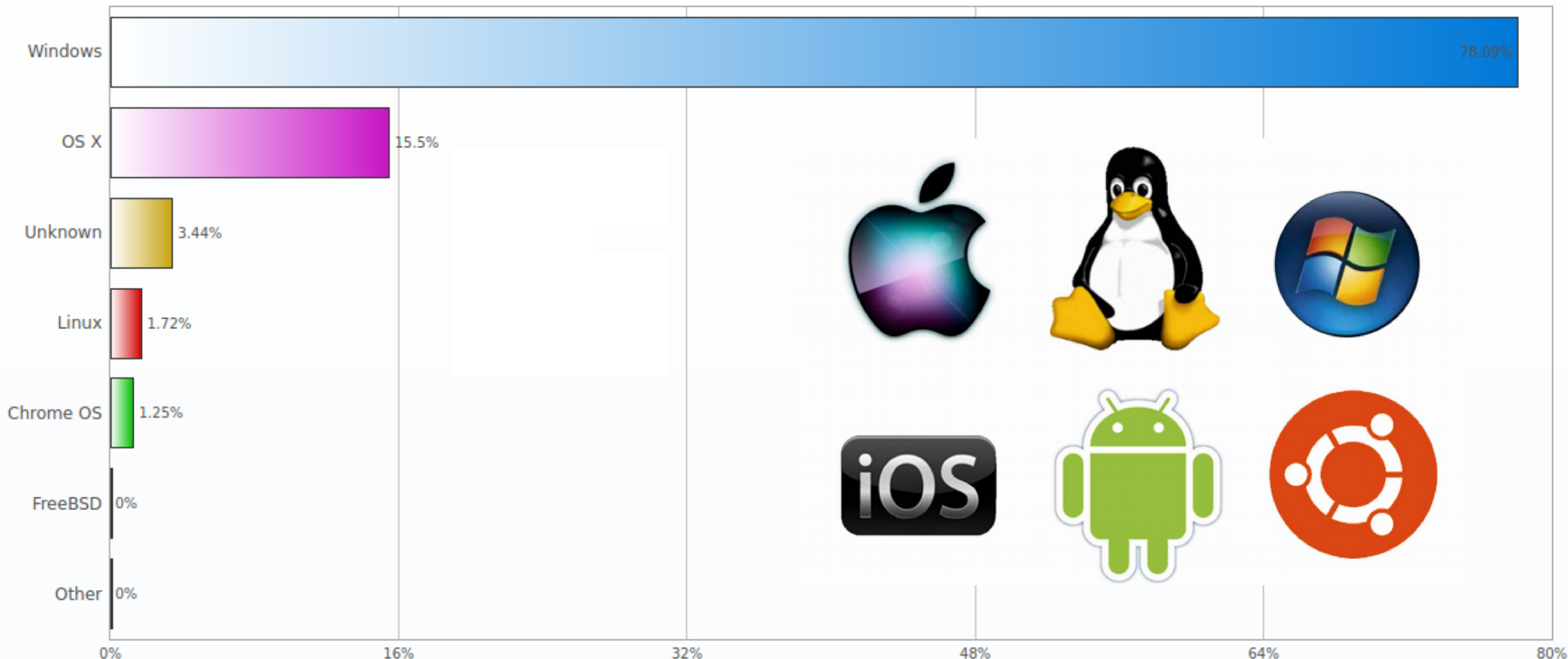
Hardware Forense



* <https://forensicstore.com/all-products/>

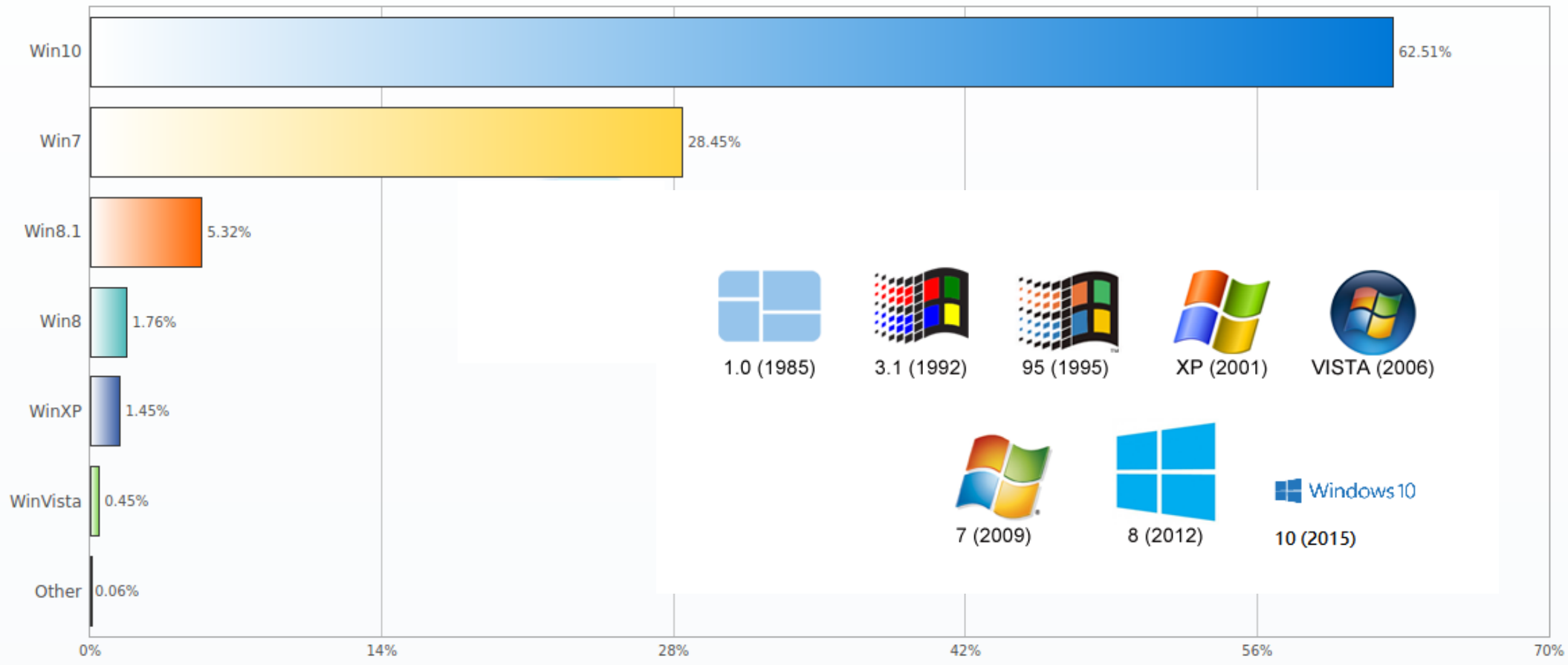
¿Cuanto se utiliza Windows?

Mercado de Sistemas Operativos de Escritorio (abril 2019 - 2020)



Mercado de Versiones de Windows

(abril 2019 - 2020)



¿Qué es SIFT Workstation?

La estación de trabajo SIFT está constituida de un grupo de herramientas open source libres para respuesta de incidentes y forense, siendo diseñado para realizar exámenes forenses digitales detallados en una diversidad de escenarios.

SIFT puede ser utilizado como cualquier suite de herramientas para respuesta de incidentes y forense. Demuestra las capacidades avanzadas para respuesta de incidentes, y las técnicas forenses digitales profundas, las cuales pueden realizarse utilizando herramientas open source de última generación, las cuales están disponibles libremente y se actualizan frecuentemente.



* SIFT Workstation: <https://digital-forensics.sans.org/community/downloads>

* Ubuntu: <https://www.ubuntu.com/>

Es exitosamente utilizado en respuesta de incidentes y forense digital, y está disponible libremente como servicio público. Continúa siendo la herramienta open source más popular de este tipo

- Base Ubuntu LTS 16.04
- Sistema base de 64 bits
- Mejor utilización de memoria
- Actualización automática de paquetes DFIR y personalizaciones
- Las últimas herramientas y técnicas forenses
- Disponible un Appliance VM listo para trabajar en forense
- Compatibilidad cruzada entre Linux y Windows
- Opción para instalar un sistema autónomo mediante un instalador "SIFT-CLI"
- Documentación del proyecto
- Soporte ampliado para sistemas de archivos

* SIFT Documentation: <http://sift.readthedocs.io/en/latest/>

Paquetes: Afterglow, binplist, bulk_extractor, dumppig, flowgrep, libbde, libdata-heify-perl, libesedb, libevt, libetvx, libewf, liblnk, libfile-mork-perl, libfvde, libfws, liblightgrep, liblnk, libmac-propertylist-perl, libmsiecf, libolecf, libpff, libqcow, libregf, libsmdev, libmsraw, libvhdi, libvmdk, libvshadow, libxml-entities-perl, log2timeline-perl, mac-robber, maltegoce, mantaray, ntdsextract, ntopng, pdf-tools, pyelftools, python-bencode, python-construct, python-dfvfs, python-pdkt, python-plaso, python-pyparsing, pytsk, re2, regripper, sleuthkit, volatility, windows-perl, xmount, etc.

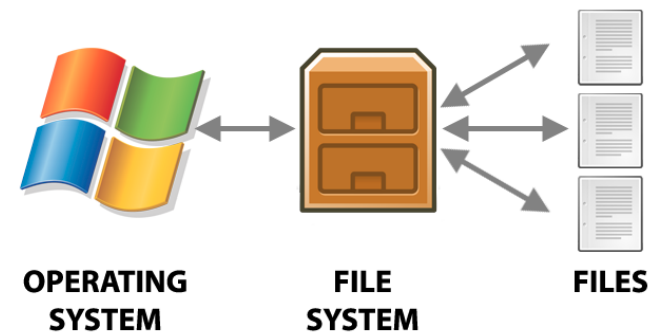
Scripts: Denensityscout, extract_mft_record_slack.py, ga_parser.py, java_idx_parser, jobparser.py, page_brute, pe_carver, pescanner.py, shellbags.py, shimchacheparser.py, sqlparser.py, etc.

* SIFT Tools, Commands and Scripts: <http://sift.readthedocs.io/en/latest/tools/index.html>

Ejemplos de Análisis en un Sistema Windows

Tiene principalmente dos generaciones de sistemas de archivos. El primer sistema de archivos, FAT (File Allocation Table), fue utilizado en versiones anteriores de los sistemas Windows / MS-DOS, y creció desde sistemas de archivos de 12 bits denominado FAT12, hasta sistemas de archivos de 32 bits denominado FAT32. El segundo sistema de archivos, NTFS (New Technology File System) fue introducido con Windows NT, y es utilizado hasta las versiones más recientes de Windows.

- Master Boot Record
- Sistema de Archivos FAT
- Recuperar Particiones FAT
- Recuperar Particiones NTFS



- * <https://technet.microsoft.com/en-us/library/cc938438.aspx>
- * [https://technet.microsoft.com/en-us/library/cc776720\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc776720(v=ws.10).aspx)
- * [https://technet.microsoft.com/en-us/library/cc778410\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc778410(v=ws.10).aspx)
- * [https://technet.microsoft.com/en-us/library/cc781134\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx)

Sistema de Archivos en Windows (Cont.)



```
Terminal
ryds@siftworkstation -> ~
$ ls -l /mnt/windows_mount1/
total 2941413
-rwxrwxrwx 1 root root      2560 ris 17  2013 $AttrDef
-rwxrwxrwx 1 root root         0 ris 17  2013 $BadClus
-rwxrwxrwx 1 root root    1966016 ris 17  2013 $Bitmap
drwxrwxrwx 1 root root      8192 ris 17  2013 $Boot
-rwxrwxrwx 1 root root      8192 ris 17  2013 $Boot
-rwxrwxrwx 1 root root    427680 awu 22  2013 bootmgr
-rwxrwxrwx 1 root root         1 jun 18  2013 BOOTNXT
-rwxrwxrwx 1 root root      8192 ris 17  2013 BOOTSECT.BAK
lrwxrwxrwx 2 root root         60 awu 22  2013 Documents and Settings -> /mnt/windows_mount1/Users
drwxrwxrwx 1 root root         0 ris 17  2013 $Extenc
-rwxrwxrwx 1 root root 1717555200 ris 29  2013 hiberfil.sys
-rwxrwxrwx 1 root root    67108864 ris 17  2013 $LogFile
-rwxrwxrwx 1 root root      4096 ris 17  2013 $MFTMirr
-rwxrwxrwx 1 root root 1207959552 ris 29  2013 pagefile.sys
drwxrwxrwx 1 root root         0 awu 22  2013 PerfLogs
drwxrwxrwx 1 root root      4096 ris 21  2013 ProgramData
drwxrwxrwx 1 root root      4096 ris 21  2013 Program Files
drwxrwxrwx 1 root root      4096 ris 17  2013 Program Files (x86)
drwxrwxrwx 1 root root         0 ris 17  2013 Recovery
drwxrwxrwx 1 root root         0 ris 17  2013 $Recycle.Bin
----- 1 root root         0 ris 17  2013 $Secure
-rwxrwxrwx 1 root root    16777216 ris 29  2013 swapfile.sys
drwxrwxrwx 1 root root      4096 ris 21  2013 System Volume Information
-rwxrwxrwx 1 root root    131072 ris 17  2013 $UpCase
drwxrwxrwx 1 root root      4096 ris 17  2013 Users
-rwxrwxrwx 1 root root         0 ris 17  2013 $Volume
drwxrwxrwx 1 root root     24576 ris 21  2013 Windows
ryds@siftworkstation -> ~
$
ryds@siftworkstation -> ~
$
ryds@siftworkstation -> ~
$ ls -l /mnt/windows_mount1/Windows
```


Sistema de Archivos en Windows (Cont.)



Details of vol1 x host1:host1:vol1 x +

localhost:9999/autopsy?mod=1&submod=2&case=host1&host=ho: 80% ... ? X

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

Directory Seek

Enter the name of a directory that you want to view.
A: /

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

ADD NOTE **GENERATE MD5 LIST OF FILES**

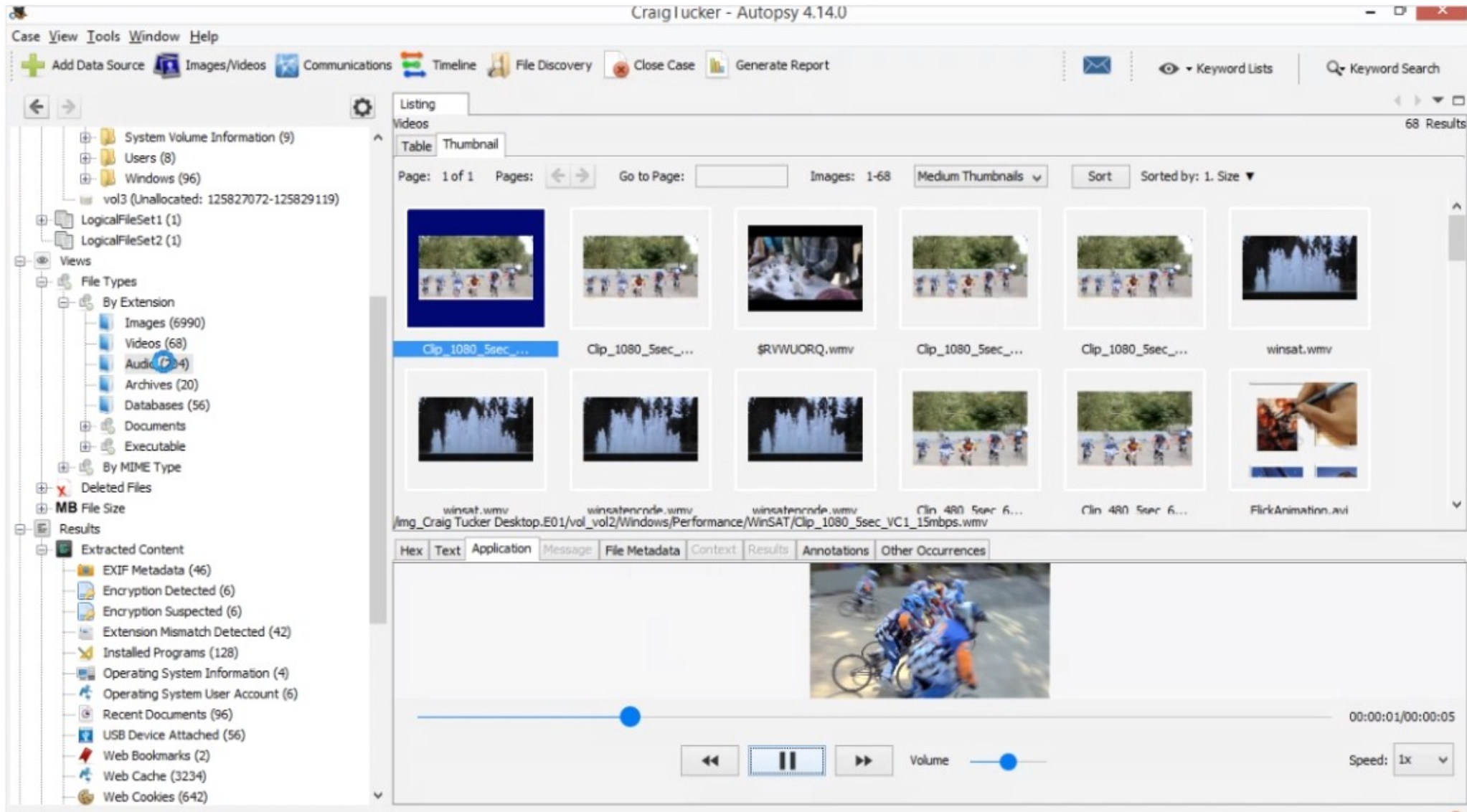
DEL	Type	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	dir / in								
Error Parsing File (Invalid Characters?): V/V 45782: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0									
	v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45780
	v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
	v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
	r / r	cover_page.ipgc	2002-09-11 08:30:52 (-05)	2002-09-11 00:00:00 (-05)	2002-09-11 08:50:27 (-05)	15585	0	0	8
✓	r / r	Jimmy Jungle.doc	2002-04-15 14:42:30 (-05)	2002-09-11 00:00:00 (-05)	2002-09-11 08:49:49 (-05)	20480	0	0	5
	r / r	Scheduled Visits.exe	2002-05-24 08:20:32 (-05)	2002-09-11 00:00:00 (-05)	2002-09-11 08:50:38 (-05)	1000	0	0	11

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [Add Note](#)

File Type: PC formatted floppy with no filesystem

```
00000000: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000008: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000010: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000018: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000020: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000028: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000030: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000038: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000040: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000048: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000050: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000058: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000060: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000068: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000070: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000078: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000080: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000088: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000090: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
00000098: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
000000A0: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
000000B0: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
000000C0: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
000000D0: F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 F6F6 .....
```


Sistema de Archivos en Windows (Cont.)



La adquisición de la memoria RAM, se ha convertido en uno de los más importantes cambios en el campo forense de computadoras.

Al responder a incidentes, se requiere recolectar y preservar tanta evidencia volátil como sea posible, incluyendo la memoria RAM.

Inevitablemente se realizarán cambios o alteraciones durante este proceso. Pero con el conocimiento y experiencia, también se está en la capacidad de sustentar este accionar.

Los datos volátiles son datos los cuales desaparecerán o serán destruidos una vez el sistema de cómputo sea apagado. Típicamente es la RAM, pero existe más, como conexiones de red activas, aplicaciones en funcionamiento, etc. Muchos de estos datos son extremadamente valiosos para determinar o refutar diversos argumentos.

Memoria RAM (Cont.)



0xffffe0017fe36740	taskhost.exe	1904	832	9	0	1	0	2020-03-08 13:33:57 UTC+0000	
0xffffe0017fe77200	userinit.exe	1924	504	0	-----	1	0	2020-03-08 13:33:57 UTC+0000	2020-03-08 13:34:20 UTC
0xffffe0017fe0f7c0	explorer.exe	2084	1924	60	0	1	0	2020-03-08 13:33:57 UTC+0000	
0xffffe0017fe0b8c0	SearchIndexer.	2268	548	13	0	0	0	2020-03-08 13:33:57 UTC+0000	
0xffffe0017fac78c0	svchost.exe	2404	548	17	0	0	0	2020-03-08 13:33:57 UTC+0000	
0xffffe0017fe60480	tvnserver.exe	2896	2084	3	0	1	0	2020-03-08 13:34:08 UTC+0000	
0xffffe001804f78c0	runonce.exe	2980	2084	0	-----	1	0	2020-03-08 13:34:10 UTC+0000	2020-03-08 13:34:11 UTC
0xffffe0017fe79800	jpsched.exe	3012	2980	1	0	1	1	2020-03-08 13:34:10 UTC+0000	
0xffffe0017eb2d8c0	wmpnetwk.exe	1696	548	8	0	0	0	2020-03-08 13:35:55 UTC+0000	
0xffffe0017dc30180	MpCmdRun.exe	1196	1420	0	-----	0	0	2020-03-08 14:08:19 UTC+0000	2020-03-08 14:08:19 UTC
0xffffe0017e5c18c0	MpCmdRun.exe	3576	1196	5	0	0	0	2020-03-08 14:08:19 UTC+0000	
0xffffe0017da96080	taskhost.exe	3412	832	3	0	1	0	2020-03-08 15:33:50 UTC+0000	
0xffffe0017e3eb440	firefox.exe	3504	2084	0	-----	1	0	2020-03-08 15:40:46 UTC+0000	2020-03-08 15:40:48 UTC
0xffffe0018029b4c0	firefox.exe	2988	3504	50	0	1	0	2020-03-08 15:40:46 UTC+0000	
0xffffe0017e0db8c0	firefox.exe	3480	2988	8	0	1	0	2020-03-08 15:40:48 UTC+0000	
0xffffe0017e4318c0	firefox.exe	3928	2988	19	0	1	0	2020-03-08 15:40:49 UTC+0000	
0xffffe0017e3ca080	firefox.exe	588	2988	17	0	1	0	2020-03-08 15:40:49 UTC+0000	
0xffffe0017e5b38c0	firefox.exe	4080	2988	0	-----	1	0	2020-03-08 15:40:51 UTC+0000	2020-03-08 15:53:17 UTC

Memoria RAM (Cont.)

Terminal							
00 UTC+0000							
0x293f51f0	UDPv6	fe80::797d:8432:c786:8afc:19	*:*		2404	svchost.exe	2020-03-08 13:34:
00 UTC+0000							
0x2927c610	TCPv4	0.0.0.0:1030	0.0.0.0:0	LISTENING	548	services.exe	
0x2927cd90	TCPv4	0.0.0.0:1030	0.0.0.0:0	LISTENING	548	services.exe	
0x2927cd90	TCPv6	:::1030	:::0	LISTENING	548	services.exe	
0x292839e0	TCPv4	127.0.0.1:1561	127.0.0.1:1562	ESTABLISHED	3928	firefox.exe	
0x292d76a0	TCPv4	127.0.0.1:1566	127.0.0.1:1567	ESTABLISHED	588	firefox.exe	
0x292f99d0	TCPv4	192.168.0.68:1568	34.215.85.124:443	CLOSED	2988	firefox.exe	
0x293c5d10	TCPv4	192.168.0.68:1215	192.168.0.10:445	ESTABLISHED	4	System	
0x293eea10	TCPv4	192.168.0.68:1717	35.163.194.26:443	ESTABLISHED	2988	firefox.exe	
0x2a4b84e0	UDPv4	169.254.138.252:57394	*:*		2404	svchost.exe	2020-03-08 13:34:
00 UTC+0000							
0x2a525010	UDPv6	fe80::e5f7:4a64:8371:cb92:49297	*:*		748	svchost.exe	2020-03-08 16:24:
:42 UTC+0000							
0x2a5a8530	TCPv4	192.168.0.68:5900	192.168.0.7:49318	ESTABLISHED	1384	tvnserver.exe	
0x318226c0	UDPv4	0.0.0.0:0	*:*		748	svchost.exe	2020-03-08 16:23:
10 UTC+0000							
0x31867c30	UDPv6	fe80::797d:8432:c786:8afc:19	*:*		748	svchost.exe	2020-03-08 16:24:
43 UTC+0000							
0x318f92c0	TCPv4	127.0.0.1:4652	0.0.0.0:0	LISTENING	0	??f?g??	
0x319368f0	TCPv4	192.168.0.68:1726	192.168.0.76:139	CLOSED	4	System	
0x31940bc0	TCPv4	127.0.0.1:1567	127.0.0.1:1566	ESTABLISHED	588	firefox.exe	
0x35363d40	TCPv4	0.0.0.0:2869	0.0.0.0:0	LISTENING	4	System	
0x35363d40	TCPv6	:::2869	:::0	LISTENING	4	System	
0x352e74f0	TCPv4	192.168.0.68:1723	192.168.0.10:139	CLOSED	4	System	
0x35351350	TCPv4	127.0.0.1:1647	127.0.0.1:1646	ESTABLISHED	4628	firefox.exe	
0x37072da0	UDPv4	0.0.0.0:0	*:*		884	svchost.exe	2020-03-08 16:24:
15 UTC+0000							
0x37236470	UDPv4	0.0.0.0:0	*:*		884	svchost.exe	2020-03-08 16:24:
15 UTC+0000							
0x37236470	UDPv6	:::0	*:*		884	svchost.exe	2020-03-08 16:24:
15 UTC+0000							
0x5108f1f0	UDPv6	fe80::797d:8432:c786:8afc:19	*:*		2404	svchost.exe	2020-03-08 13:34:
00 UTC+0000							

Memoria RAM (Cont.)

```
Terminal
$OBJECT ID
Object ID: 40000000-0000-0000-0030-000000000000
Birth Volume ID: 6c220000-0000-0000-6c22-000000000000
Birth Object ID: 3103215b-0f00-0000-ffff-ffff82794711
Birth Domain ID: 00000000-0000-0000-0000-000000000000

*****
*****
MFT entry found at offset 0xb9d400
Attribute: In Use & File
Record Number: 116461
Link count: 2

$STANDARD_INFORMATION
Creation              Modified              MFT Altered              Access Date              Type
-----
2020-03-01 14:40:21 UTC+0000 2020-03-01 14:40:21 UTC+0000 2020-03-01 14:40:21 UTC+0000 2020-03-01 14:40:21 UTC+0000 Archive
Record Number: 100013
Link count: 2

$STANDARD_INFORMATION
Creation              Modified              MFT Altered              Access Date              Type
-----
2013-08-22 15:36:35 UTC+0000 2013-08-22 15:34:54 UTC+0000 2017-01-25 00:46:52 UTC+0000 2013-08-22 15:34:54 UTC+0000 Archive

$FILE_NAME
Creation              Modified              MFT Altered              Access Date              Name/Path
-----
2017-01-25 00:46:52 UTC+0000 2017-01-25 00:46:52 UTC+0000 2017-01-25 00:46:52 UTC+0000 2017-01-25 00:46:52 UTC+0000 Writers\System\
61D61-1.XML

$FILE_NAME
Creation              Modified              MFT Altered
```

Al utilizar Windows, se crean, borran, modificación y acceden hacia muchos archivos. Algunos de estos patrones o tipos específicos de cambios, son lo suficientemente únicos para permitir exponer con certeza la comisión de una acción.

Si se fallase en determinar si existen o no, se podría llegar a conclusiones incorrectas, o no sustentar los argumentos correctos.

Los artefactos de Windows se convierten en puntos clave para una investigación, y conducen hacia la investigación de evidencia.

- Papelera de reciclaje
- Archivos LNK
- Dispositivos USB extraíbles
- Metadatos en documentos Office.
- UserAssist, etc.



Artefactos de Windows (Cont.)



```
Terminal
LogConf LastWrite      : [Tue Sep 13 08:21
Properties LastWrite    : [Tue Sep 13 08:27
  InstallDate          : Tue Sep 13 08:27:14 2011 U
  FirstInstallDate: Tue Sep 13 08:27:14 2011 U
VID 0E0F&PID 0003 [Tue Sep 13 08:21:47 2011]
  S/N: 6&2ab01149&0&1 [Fri Sep 16 16:17:53 2011]
  Device Parameters LastWrite: [Tue Sep 13 08:26
  LogConf LastWrite      : [Tue Sep 13 08:21
  Properties LastWrite    : [Tue Sep 13 08:27
  ParentIdPrefix: 7&38bade0a&0
  InstallDate          : Tue Sep 13 08:27:15 2011 U
  FirstInstallDate: Tue Sep 13 08:27:15 2011 U
VID 0E0F&PID 0003&MI 00 [Tue Sep 13 08:21:50 201
  S/N: 7&38bade0a&0&0000 [Fri Sep 16 16:17:54 20
  Device Parameters LastWrite: [Tue Sep 13 08:21
  LogConf LastWrite      : [Tue Sep 13 08:21
  Properties LastWrite    : [Tue Sep 13 08:27
  ParentIdPrefix: 8&159b05f8&0
  InstallDate          : Tue Sep 13 08:27:17 2011 U
  FirstInstallDate: Tue Sep 13 08:27:17 2011 U
VID 0E0F&PID 0003&MI 01 [Tue Sep 13 08:21:50 201
  S/N: 7&38bade0a&0&0001 [Fri Sep 16 16:17:54 20
  Device Parameters LastWrite: [Tue Sep 13 08:21
  LogConf LastWrite      : [Tue Sep 13 08:21
  Properties LastWrite    : [Tue Sep 13 08:27
  ParentIdPrefix: 8&e3c37ca&0
  InstallDate          : Tue Sep 13 08:27:18 2011 U
  FirstInstallDate: Tue Sep 13 08:27:18 2011 U
VID_14DD&PID_1005 [Tue Jul 14 04:55:55 2009]
ryds@siftworkstation -> ~
$

Terminal
VID_04B4&PID_6560 [Sun Nov 21 03:57:50 2010]
  S/N: 4C530012450531101593 [Tue Mar 24 13:38:00 2015]
  Device Parameters LastWrite: [Mon Mar 23 18:31:10 2015]
  LogConf LastWrite      : [Mon Mar 23 18:31:09 2015]
  Properties LastWrite    : [Mon Mar 23 18:31:10 2015]
  InstallDate          : Mon Mar 23 18:31:10 2015 UTC
  FirstInstallDate: Mon Mar 23 18:31:10 2015 UTC
  S/N: 4C530012550531106501 [Tue Mar 24 19:38:09 2015]
  Device Parameters LastWrite: [Tue Mar 24 13:58:32 2015]
  LogConf LastWrite      : [Tue Mar 24 13:58:31 2015]
  Properties LastWrite    : [Tue Mar 24 13:58:32 2015]
  InstallDate          : Tue Mar 24 13:58:32 2015 UTC
  FirstInstallDate: Tue Mar 24 13:58:32 2015 UTC
VID 0E0F&PID 0002 [Wed Mar 25 10:15:19 2015]
  S/N: 6&b77da92&0&2 [Wed Mar 25 13:05:36 2015]
  Device Parameters LastWrite: [Wed Mar 25 10:18:30 2015]
  LogConf LastWrite      : [Wed Mar 25 10:15:19 2015]
  Properties LastWrite    : [Wed Mar 25 10:17:42 2015]
  InstallDate          : Wed Mar 25 10:17:46 2015 UTC
  FirstInstallDate: Wed Mar 25 10:17:46 2015 UTC
VID 0E0F&PID 0003 [Wed Mar 25 10:15:19 2015]
  S/N: 6&b77da92&0&1 [Wed Mar 25 13:05:36 2015]
  Device Parameters LastWrite: [Wed Mar 25 10:17:05 2015]
  LogConf LastWrite      : [Wed Mar 25 10:15:19 2015]
  Properties LastWrite    : [Wed Mar 25 10:17:46 2015]
  ParentIdPrefix: 7&2a7d3009&0
  InstallDate          : Wed Mar 25 10:17:47 2015 UTC
  FirstInstallDate: Wed Mar 25 10:17:47 2015 UTC
VID 0E0F&PID 0003&MI 00 [Wed Mar 25 10:15:19 2015]
  S/N: 7&2a7d3009&0&0000 [Wed Mar 25 13:05:36 2015]
```

Artefactos de Windows (Cont.)



```
Terminal
Profile Description ML (fi-FI) : Kameran RGB-profiili
Profile Description ML (fr-FU) : Profil RVB de l'appareil-photo
Profile Description ML (it-IT) : Profilo RGB Fotocamera
Profile Description ML (nl-NL) : RGB-profiel Camera
Profile Description ML (no-NO) : RGB-kameraprofil
Profile Description ML (pt-BR) : Perfil RGB de Câmera
Profile Description ML (sv-SE) : RGB-profil för Kamera
Profile Description ML (ja-JP) : カメラ RGB プロファイル
Profile Description ML (ko-KR) : 카메라 RGB 프로파일
Profile Description ML (zh-TW) : 數位相機 RGB 色彩描述
Profile Description ML (zh-CN) : 相机 RGB 描述文件
DCT Encode Version : 100
APP14 Flags 0 : [14]
APP14 Flags 1 : (none)
Color Transform : YCbCr
Image Width : 1136
Image Height : 852
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)
Aperture : 6.3
GPS Altitude : 304 m Above Sea Level
GPS Latitude : 33 deg 52' 31.66" N
GPS Longitude : 116 deg 18' 5.83" W
GPS Position : 33 deg 52' 31.66" N, 116 deg 18' 5.83" W
Image Size : 1136x852
Megapixels : 0.968
Scale Factor To 35 mm Equivalent: 4.9
Shutter Speed : 1/500
Circle Of Confusion : 0.006 mm
Field Of View : 18.0 deg
Focal Length : 23.4 mm (35 mm equivalent: 113.9 mm)
Hyperfocal Distance : 14.09 m
ryds@siftworkstation -> ~
$
```


Artefactos de Windows (Cont.)



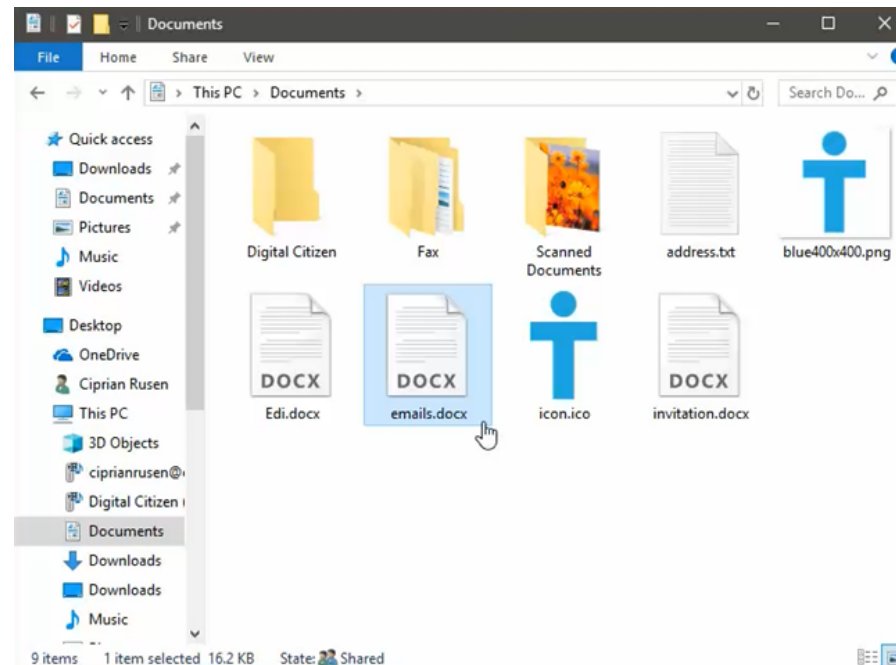
```
Terminal
-rwxrwxrwx 1 root root 2022 ris 20 2013 School.lnk
-rwxrwxrwx 1 root root 449 ris 20 2013 Shavers.lnk
-rwxrwxrwx 1 root root 2363 ris 20 2013 SonyPSP.lnk
-rwxrwxrwx 2 root root 3526 ris 18 2013 The Evolutionary Steps of Fish.lnk
-rwxrwxrwx 2 root root 2294 ris 21 2013 underage_daughter_R@ygold.lnk
-rwxrwxrwx 2 root root 2350 ris 21 2013 Underage_lolita_r@ygold_001.lnk
-rwxrwxrwx 2 root root 2350 ris 21 2013 Underage_lolita_r@ygold_002.lnk
ryds@siftworkstation -> ~
$
ryds@siftworkstation -> ~
$ xxd /mnt/windows mount1/Users/Craig/AppData/Roaming/Microsoft/Windows/Recent/Coupons.lnk
00000000: 4c00 0000 0114 0200 0000 0000 c000 0000  L.....
00000010: 0000 0046 8b00 2000 2000 0000 0254 06a3  ...F.....T..
00000020: 9dfb ce01 c7ff 2603 7ffe ce01 7c9d ca04  ....&.....|...
00000030: 7ffe ce01 af17 b308 0000 0000 0100 0000  ....
00000040: 0000 0000 0000 0000 0000 0000 aa00 1400  ....
00000050: 1f50 e04f d020 ea3a 6910 a2d8 0800 2b30  .P.O...:i....+0
00000060: 309d 3200 2e80 90e2 4d37 3f12 6545 9164  0.2.....M7?.eE.d
00000070: 39c4 925e 467b 1e00 0000 2500 efbe 1100  9..^F{....%....
00000080: 0000 c903 4e6b 53fb ce01 d4ab 5a3c 7ffe  ....NkS.....Z<..
00000090: ce01 1400 6200 3200 af17 b308 9543 2798  ....b.2.....C'.
000000a0: 2000 436f 7570 6f6e 732e 7a69 7000 4800  .Coupons.zip.H.
000000b0: 0900 0400 efbe 9243 5a18 9543 2698 2e00  ....CZ..C&...
000000c0: 0000 4747 0100 0000 0100 0000 0000 0000  ..GG.....
000000d0: 0000 0000 0000 0000 841b 4c00 4300 6f00  ....L.C.o.
000000e0: 7500 7000 6f00 6e00 7300 2e00 7a00 6900  u.p.o.n.s...z.i.
000000f0: 7000 0000 1a00 0000 5300 0000 1c00 0000  p.....S.....
00000100: 0100 0000 1c00 0000 2d00 0000 0000 0000  ....
00000110: 5200 0000 1100 0000 0300 0000 a244 9562  R.....D.b
00000120: 1000 0000 0043 3a5c 5573 6572 735c 4372  ....C:\Users\Cr
00000130: 6169 675c 446f 776e 6c6f 6164 735c 436f  aig\Downloads\Co
00000140: 7570 6f6e 732e 7a69 7000 0024 002e 002e  upons.zip..$.
00000150: 005c 002e 002e 005c 002e 002e 005c 002e  .\.....\.....\..
00000160: 002e 005c 002e 002e 005c 0044 006f 0077  ...\.D.o.w
00000170: 006e 006c 006f 0061 0064 0073 005c 0043  .n.l.o.a.d.s.\.C
00000180: 006f 0075 0070 006f 006e 0073 002e 007a  .o.u.p.o.n.s...Z
```

Pero... ¿Cuanto puede conocer
Windows sobre nosotros?

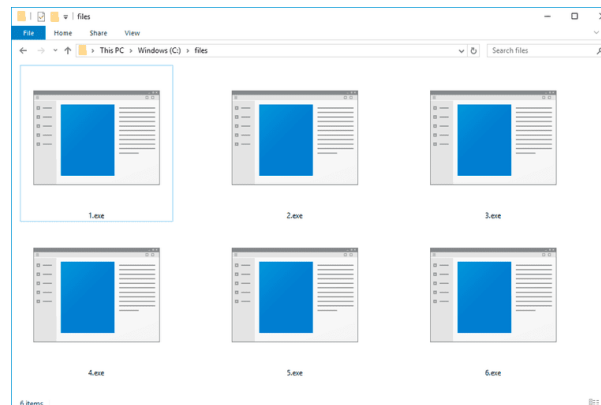
Descarga de Archivos



- Open / Save MRU (Most Recently Used)
- Email Attachments (Adjuntos de correo electrónico)
- Skype History (Historial de Skype)
- Browser Artifacts (Artefactos del navegador web)
- Downloads (Descargas)
- ADS (Alternate Data Stream) Zone.Identifier



- UserAssist
- Windows 10 Timeline (Cronología de Windows 10)
- RecentApps
- Shimcache
- Jump Lists
- Amcache.hve
- System Resource Usage Monitor - SRUM (Vigilancia de uso de recursos del sistema)
- BAD (Background Activity Moderator) / DAM
- Last-Visited MRU (Most Recently Used)
- Prefetch



Archivos Borrados o Archivos con Conocimiento



- XP Search - ACMRU
- Thumbcache (Miniaturas)
- Thumbs.db
- IE (Internet Explorer)/Edge file://
- Search - WordWhellQuery
- Win7/8/10 Recycle Bin (Papelera de reciclaje)
- Last-Visited MRU (Most Recently Used)
- XP Recycle Bin (Papelera de Reciclaje)



Actividad de la Red / Ubicación Física



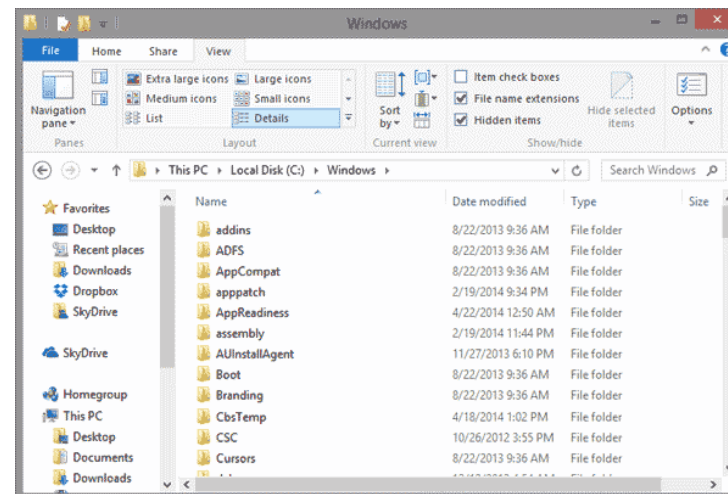
- Timezone (Zona horaria)
- Cookies
- Network History (Historial de red)
- WLAN (Wireless Local Area Network) Event Log (Registro de eventos de WLAN (Redes inalámbricas de área local))
- Browser Search Terms (Términos de búsqueda en el navegador)
- System Resource Usage Monitor - SRUM (Vigilancia de uso de recursos del sistema)



Apertura de Archivos / Carpetas



- Open / Save MRU (Most Recently Used)
- Recent Files (Archivos recientes)
- Jump Lists
- Shell Bags
- Shortcut (LNK) Files (Archivos de enlace)
- Prefetch
- Last-Visited MRU
- IE (Internet Explorer)/Edge file://
- Office Recent Files (Archivos recientes de office)



Utilización de las Cuentas



- Last Login (Último login)
- Last Password Change (Último cambio de la contraseña)
- RDP (Remote Desktop Protocol) Usage (Uso de RDP)
- Services Events (Eventos de servicios)
- Logon Types (Tipos de login)
- Authentication Events (Eventos de autenticación)
- Success / Fail Logons (Logins fallidos y exitosos)



Utilización USB / Dispositivos Externos

- Key Identification (Identificación de claves)
- First / Last Times (Tiempo inicial y final)
- User (Usuario)
- PnP (Plug and Play) Events (Eventos PnP)
- Volume Serial Number (Número de serie del volumen)
- Drive Letter and Volume Name (Nombre del volumen y letra de unidad)
- Shortcut (LNK) Files (Archivos de enlace)



Utilización del Navegador



- History (Historial)
- Cookies
- Cache
- Flash & Super Cookies
- Session Restore (Restauración de sesión)
- Google Analytics Cookies



Opera



Google Chrome



Safari



Mozilla Firefox



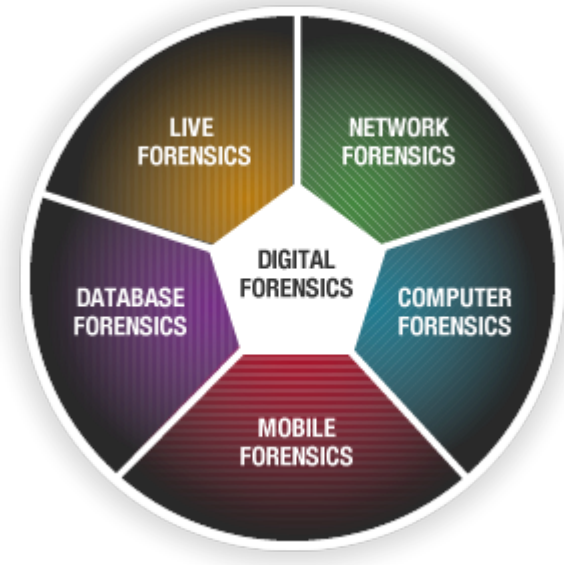
Internet Explorer



Microsoft Edge

¿Más Forense Digital?

- Forense de Sistemas Windows
- Respuesta de Incidentes
- Forense de Redes
- Análisis de Malware
- Forense de Sistemas Mac
- Forense de Memoria RAM
- Forense de Teléfonos Inteligentes
- Forense a la Nube, etc...



Curso Virtuales Disponibles en Video OWASP™

Curso Virtual de Hacking Ético

http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

http://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Curso Virtual Hacking con Kali Linux

http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence

http://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes

http://www.reydes.com/d/?q=Curso_Forense_de_Reddes

Y todos mis cursos virtuales:

<http://www.reydes.com/d/?q=cursos>

Más Contenidos



Videos de 52 webinars gratuitos

<http://www.reydes.com/d/?q=videos>

Diapositivas de los webinars gratuitos

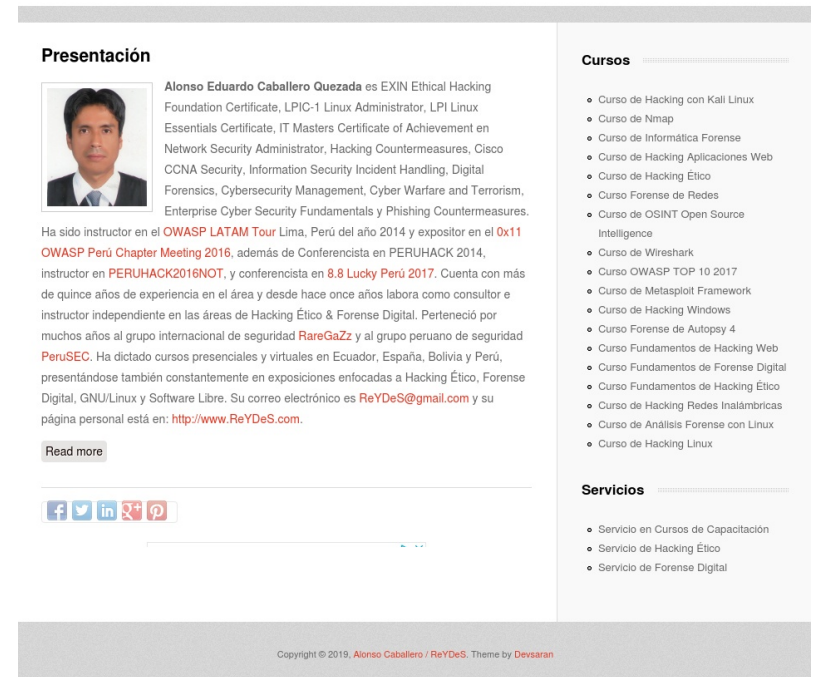
<http://www.reydes.com/d/?q=node/3>

Artículos y documentos publicados

<http://www.reydes.com/d/?q=node/2>

Blog sobre temas de mi interés.

<http://www.reydes.com/d/?q=blog/1>



¡Muchas Gracias !

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético & Forense Digital

Sitio Web: www.reydes.com / Correo Electrónico: reydes@gmail.com