5 Evidencias Digitales en la Investigación Forense Informática

10

15

ESPOCH 2019

EVIDENCIAS DIGITALES EN LA INVESTIGACIÓN FORENSE INFORMÁTICA

20

EVIDENCIAS DIGITALES EN LA INVESTIGACIÓN FORENSE INFORMÁTICA

35

30





Evidencias Digitales en la Investigación Forense Informática

 45 © 2019 Escuela Superior Politécnica del Chimborazo Panamericana Sur, kilómetro 1 ¹/₂ Dirección de Publicaciones Científicas Riobamba, Ecuador Teléfono: 593 (3) 2 998200
 50 Código Postal: EC060155

Aval ESPOCH

Este libro se sometió a arbitraje bajo el sistema de doble ciego (peer review).

55

Corrección y diseño:

El presente libro recopila información sobre la extracción y restauración de las diferentes evidencias digitales en la investigación forense informática como son documentos, ficheros, registros, datos, etc., contenido en un soporte informático y es susceptible de tratamiento digital; las imágenes han sido generadas en la realización de prácticas desarrolladas, mientras se encontraba en proceso de elaboración el presente libro.

Impreso en Ecuador

70 Prohibida la reproducción de este libro, por cualquier medio, sin la previa autorización por escrito de los propietarios del Copyright.

CDU: _____ Evidencias Digitales en la Investigación Forense Informática

Riobamba: Escuela Superior Politécnica de Chimborazo Dirección de Publicaciones, año 2019 186 pp. vol.: 17 x 24 cm ISBN: _____

- 1. Introducción
- 2. Artefactos
- 3. Framework Forense
- 4. Herramientas para extracción de la memoria volátil

PRÓLOGO

- 75 Las evidencias digitales en la investigación forense informática, involucran documentos, ficheros, registros, datos, etc., contenido en un soporte informático y siendo susceptible de tratamiento digital.
- 80 Para abordar las evidencias digitales en la investigación forense informática en el presente libro, se trabajó con ejemplos reales y con el software recomendable a utilizarse, ya que las leyes y reglas de administración de justicia sobre informática forense y evidencias digitales son de origen europeo y específicamente en
 85 Ecuador no existe ninguna ley ni reglamento para la misma. El texto consta de cuatro capítulos; el primero versará sobre la introducción a la informática forense y examinación de los medios digitales de manera válida, con el propósito de analizar los resultados obtenidos. El segundo hace referencia a los artefactos y es todo aquello que
 90 puede obtener una evidencia. El tercero se refiere al framework forense que dispone de utilidades y programas con la finalidad de

facilitar la tarea forense, en todos sus aspectos como adquisición,

preservación y análisis. En el cuarto capítulo, se versará sobre las herramientas para extracción de la memoria volátil y tipos de técnicas para recuperar información.

ÍNDICE GENERAL

	PRÓLOGO	VI
	ÍNDICE GENERAL	VIII
100	ÍNDICE DE FIGURAS	XI
	ÍNDICE DE TABLAS	XVI
	CAPÍTULO I	17
	INTRODUCCIÓN	17
	1.1. Análisis Forense Informático	17
105	1.2. El perito informático	
	1.2.1. Perito	
	1.2.2. Perito Judicial o Perito Forense	
	1.3. Forense informático	24
	1.4. Evidencia Digital	
110	1.4.1. Características de la evidencia digital	
	1.5. Admisibilidad de la evidencia digital	
	1.5.1. Autenticidad	
	1.5.2. Confiabilidad	
	1.5.3. Suficiencia	
115	1.5.4. Conformidad con las leyes y reglas de la administración de justicia	
	1.6. Determinar la relevancia de la evidencia	
	1.7. Herramientas forenses	
120	 1.8. Confiablidad de las herramientas forenses en i 40 	nformática
	CAPÍTULO II	43

	ARTEFACTOS	43
	2.1. Shellbags	44
	2.2. Registros HIVE	45
125	2.2.1. Windows Registry Recovery	52
	2.2.2RegRipper	62
	2.2.3. Bulk Extractor.	69
	2.2.4La papelera	75
	2.2.5. RecoverMyFiles	78
130	2.2.6. Prefetch	80
	2.2.7Winprefetchview	83
	2.2.8. USBDeview	89
	2.2.9. Endpoint Protector	96
	2.3. Artefactos y contraseñas	98
135	2.3.1. Dialupass	98
	2.3.2. Network Password Recovery	99
	2.3.3. MessenPass	99
	2.4. Navegadores	. 100
	2.4.1. Chrome	100
140	2.4.2. iExplore	101
	2.4.3. Firefox	103
	2.5. Herramientas para la obtención de contraseñas en los navegadores	; 104
	2.5.1. WebBrowserPassView	104
145	2.5.2. MailPassView	105
	2.5.3. Metadatos	106
	2.5.4. Document Metadata Extraction	107
	2.5.5. Accesos directos	107
	2.5.6. MiTec E-mail History Browser	111

150	2.6. Creación de un Timeline	113
	CAPÍTULO III	118
	FRAMEWORK FORENSE	118
	3.1. Digital Forensics Framework	118
	3.2. Xplico	119
155	3.3. Autopsy	121
	3.4. Volatility	123
	3.5. ReKall Memory Forensic Framework	126
	3.6. Mimikatz	127
	3.7. NetworkMiner 2.0	128
160	CAPÍTULO IV	136
	HERRAMIENTAS PARA EXTRACCIÓN DE LA M	MEMORIA
	VOLÁTIL	136
	4.1. La Memoria	
	4.2. Técnicas de volcado	
165	4.3. Herramientas de volcado de memoria	
	4.3.1. Dumpit	
	4.3.2. RamCapturer	141
	4.3.3. FTK Imager lite	
	4.4. Procesos de Análisis de Memoria	145
170	4.5. Memoria Pagefile	149
	GLOSARIO DE TÉRMINOS	170
		100
	GLOSARIO DE SIGLAS	

ÍNDICE DE FIGURAS

	Fig. 2.1. Registry Path Ficheros HIVE.	47
	Fig. 2.2. El Registro del Computador	47
	Fig. 2.3. Access Data FTK Imager	50
180	Fig. 2.4. HIVE copiados en la carpeta REGISTRO	51
	Fig. 2.5. Ubicación del lugar de donde se conecta en la Pc	52
	Fig. 2.6. Ejecución del Windows Registry Recovery en la carpo	eta
	REGISTRO	53
	Fig. 2.7. Instalación de programas en WRR.	54
185	Fig. 2.8. Logotipo de la Herramienta RegRipper	62
	Fig. 2.9. Herramienta RegRipper	63
	Fig. 2.10. Ejecución RegRipper sobre "rr.exe"	64
	Fig. 2.11. Informe de Software en el archivo SW.txt	66
	Fig. 2.12. Regripper – Timeline.	68
190	Fig. 2.13. Regripper – USB	69
	Fig. 2.14. Bulk Extractor	70
	Fig. 2.15. Ejecución de una máquina clonada y obtención de	
	información	71
	Fig. 2.16. Run bulk_extractor sobre Image file.	73
195	Fig. 2.17. Extracción de información con Bulk Extractor	74
	Fig. 2.18. Extracción de información – números telefónicos co	on
	Bulk Extractor	74
	Fig. 2.19. Extracción de información de correos electrónicos o	con
	Bulk Extractor	75

XI

200	Fig. 2.20. Papelera de Reciclaje76
	Fig. 2.21. Papelera de Reciclaje de la carpeta \$Recycle.Bin77
	Fig. 2.22. Papelera de Reciclaje con los \$I y \$R78
	Fig. 2.23. RecoverMyFiles
	Fig. 2.24. Registros HIVE del Prefetch 81
205	Fig. 2.25. Archivo Prefetch
	Fig. 2.26. Herramienta WinPrefetchView
	Fig. 2.27. Información USB
	Fig. 2.28. USBDeview combinado con el visor de eventos de
	Windows
210	Fig. 2.29. Conexión a un fichero SYSTEM de forma externa 92
	Fig. 2.30. Información que se guarde en una página HTML 95
	Fig. 2.31. Información de ficheros USBDeview guardada en una
	página Web95
	Fig. 2.32. Herramienta para varios sistemas operativos
215	Fig. 2.33. Artefacto Dialupass
	Fig. 2.34. Artefacto Network Password Recovery
	Fig. 2.35. Artefacto MessenPass
	Fig. 2.36. Navegadores de internet 100
	Fig. 2.37. Navegador Chrome 100
220	Fig. 2.38. Navegador Internet Explorer
	Fig. 2.39. Navegador Firefox
	Fig. 2.40. Herramienta WebBrowserPassView para obtener las
	contraseñas 105
	Fig. 2.41. Herramienta Mail PassView para obtener contraseñas

	Fig. 2.42. Herramienta que permite obtener la información de
	metadatos que está dentro de un archivo106
	Fig. 2.43. Herramienta para obtener los Metadatos 107
	Fig. 2.44. Herramienta WFA para obtener los accesos directos.108
230	Fig. 2.45. Ubicación de los accesos directos e información
	relevante para el análisis de los accesos directos 109
	Fig. 2.46. Ubicación exacta de los archivos utilizando Windows
	File Analizer
	Fig. 2.47. Acceso al histórico del correo por medio de MíTec E-
235	mail History Browser
	Fig. 2.48. Acceso al histórico de correo de Outlook Express,
	Windows Mail, Windows Live Mail, Mozilla Thunderbird y
	visualiza los correos sin entrar en el fichero 111
	Fig. 2.49. Hitos de una persona para ir del Parque
240	Sesquicentenario a la ESPOCH114
	Fig. 2.50. Carta figurativa utilizaba Napoleón para todas sus
	batallas
	Fig. 2.51. Línea de Tiempo o Cronograma para Citadel botnet con
	clave de acceso 4DF1 ACE3 115
245	Fig. 2.52. Listado de un timeline el disco duro de todos los
	subdirectorios en Excel
	Fig. 3.1. Digital Forensics Framework
	Fig. 3.2. Framework Xplico 119
	Fig. 3.3. Interfaz Xplico
250	Fig. 3.4. Geolocalización con Xplico
	Fig. 3.5. Herramienta Autopsy 121

	Fig. 3.6. Análisis con Autopsy 12	2
	Fig. 3.7. Autopsy en Windows	3
	Fig. 3.8. Volatility	4
255	Fig. 3.9. Imágenes de Windows, MAC, Linux, Android 124	4
	Fig. 3.10. Ejecución de Volatility	5
	Fig. 3.11. ReKall Memory Forensic Framework 12	7
	Fig. 3.12. Mimikatz	8
	Fig. 3.13. Logotipo NetworkMiner 2.012	9
260	Fig. 3.14. Herramienta Wireshark	0
	Fig. 3.15. Herramienta Wireshark en archivo pcap 13	1
	Fig. 3.16. Herramienta NetworkMiner	2
	Fig. 3.17. Análisis DNS en NetworkMiner	2
	Fig. 3.18. Análisis Files en NetworkMiner	3
265	Fig. 3.19. Análisis parámetros en NetworkMiner134	4
	Fig. 4.1. Herramienta DumpIt	9
	Fig. 4.2. Ejecución de Dumpit	9
	Fig. 4.3. Extracción del archivo.raw del volcado de memoria14	0
	Fig. 4.4. Volcado de memoria	1
270	Fig. 4.5. Volcado de memoria con RamCapturer 14	1
	Fig. 4.6. Fichero de memoria.mem con RamCapturer14	2
	Fig. 4.7. Herramienta FTK Imager lite	4
	Fig. 4.8. Progreso de Captura de memoria con FTK Imager 14.	5
	Fig. 4.9. Proceso de Volcado de memoria usando Trapkit 14	6
275	Fig. 4.10. Web de movistar para el envío de mensajes por SMS.14	7
	Fig. 4.11. Código fuente de la página de la web de movistar 14	8
	Fig. 4.12. TM_LOGIN del usuario de la página web14	8

	Fig. 4.13. TM_LOGIN del usuario de la página web con su
	contraseña
280	Fig. 4.14. Obtención fichero de paginación modo encendido 152
	Fig. 4.15. Ubicación archivo paginación e hibernación152
	Fig. 4.16. Exportación fichero de paginación pagefile.sys 152
	Fig. 4.17. Ubicación del fichero pagefile.sys
	Fig. 4.18. Comandos para extraer el fichero de paginación 154
285	Fig. 4.19. Fichero de paginación transformado en texto 155
	Fig. 4.20. Extracción información que contiene ftp://155
	Fig. 4.21. Clonación del Disco Duro mediante el aplicativo DD.
	150
	Fig. 4.22. Copia del disco duro origen con FTK Imager 159
290	Fig. 4.22. Copia del disco duro origen con FTK Imager
290	 Fig. 4.22. Copia del disco duro origen con FTK Imager
290	 Fig. 4.22. Copia del disco duro origen con FTK Imager
290	 Fig. 4.22. Copia del disco duro origen con FTK Imager
290	 Fig. 4.22. Copia del disco duro origen con FTK Imager
290 295	 Fig. 4.22. Copia del disco duro origen con FTK Imager
290 295	Fig. 4.22. Copia del disco duro origen con FTK Imager

ÍNDICE DE TABLAS

Tabla 2.1. Algunos elementos de los Artefactos. 43
Tabla 2.2. Opción línea de comandos para
Habilitar/Deshabilitar/Eliminar dispositivos USBs91
Tabla 2.3. Opciones de Grabar información de dispositivos USBs
con Línea de Comandos93
Tabla 2.4. Monitorización en modo hardware o virtual para los
dispositivos
Tabla 4.1. Características del equipo afectado

CAPÍTULO I

INTRODUCCIÓN

La evidencia digital o la prueba electrónica es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio. Antes de aceptar la evidencia digital un tribunal determinará si la prueba es pertinente, auténtica, si es un rumor y si es aceptable
una copia o el original es requerido.

1.1. Análisis Forense Informático.

Se considera que el Análisis Forense Informático consiste en 325 la aplicación de técnicas científicas y analíticas especializadas a una infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal (Santos Tello, 2013). 330 Cuando se requiere de servicios profesionales para ejecutar un análisis forense o peritaje, es prioritario salvaguardar toda la información, que luego será o no judicializada.

El conocimiento del informático forense abarca aspectos no 335 solo del software, sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información.

Es muy importante tener clara la diferencia entre informática forense, seguridad informática y auditoría, para evitar confusiones 340 como la que vincula a la primera con la prevención de delitos, cuando la que se encarga de esto es la seguridad informática.

1.2. El perito informático

345 1.2.1. Perito

Con la creación del Real Decreto del 17 de agosto de 1901 de Romanones surge una nueva profesión con el título de Perito. Posteriormente aparecen los títulos de perito informático y perito 350 forense (Delgado, 1994). Ejemplo: Si un habitante de una colina es experto en minerales o simplemente conoce bien la zona, pudiera actuar como perito judicial o forense en el caso de que ocurriera algún problema. No es imprescindible tener una titulación, pero sí experiencia en la actividad que se realiza a diario, aunque evidentemente lo más recomendable sería alcanzar certificaciones o titulaciones que potencien el trabajo que se lleva a cabo.

1.2.2. Perito Judicial o Perito Forense

355

360 Es el profesional dotado de conocimientos especializados y reconocidos a través de sus estudios, que suministra información u opinión con fundamentos a los tribunales de justicia, sobre cuestiones relacionadas con sus conocimientos en caso de ser requeridos como expertos. Se puede decir que es la persona que
365 funciona como vínculo entre la parte técnica y la parte judicial (Sánchez Cordero, Introducción al Análisis Forense Informático, 2014).

Existen dos tipos de peritos: los nombrados judicialmente y370 los propuestos por una o ambas partes y luego aceptados por el juez o fiscal. Los peritos judiciales son capaces de ejecutar, aplicar y

utilizar todas las técnicas y recursos de una forma científica para una adecuada administración de los requerimientos de su campo laboral (recolección de pruebas, aseguramiento, preservación, manejo de la

375 cadena de custodia necesaria para esclarecer la verdad, etc.).

Peritos Judiciales según la Ley de Enjuiciamiento Civil L.E.C artículo 340.1

Los peritos deberán poseer el título oficial que corresponda a 380 la materia objeto del dictamen y a la naturaleza de éste, por lo tanto, en la Ley de Enjuiciamiento Criminal, en su artículo 457 contempla que los Peritos Judiciales pueden ser o no titulares.

Cuando no hay peritos judiciales se nombran personas 385 expertas sobre el tema, que pueden ser:

- Peritos que tienen título oficial en la naturaleza del peritaje requerida por el juzgado.
- En ausencia de peritos titulados, se puede nombrar personas entendidas o expertas sobre el tema que, a pesar de carecer de título oficial, posean conocimientos o prácticas especiales en alguna ciencia o arte.

El perito suministra al juez el peritaje u opinión sobre determinadas ramas del conocimiento que el juez no está obligado a dominar, a efecto de suministrarle argumentos o razones para la

formación de su convencimiento (Arsuaga Cortázar, 2010).

Funciones de un perito informático

395

Entre las funciones que puede realizar un perito se encuentran 400 (Hidalgo Cajo, 2014):

- Asesoría técnica contra el ciber-crimen, considerando que se pueden presentar problemas por la existencia de un malware que afecte una entidad financiera y, por ende, a sus clientes.
- Localización de evidencias electrónicas, es decir, de los ficheros
- 405 que han sido borrados y cuya ubicación se requiere determinar.
 - Auditorías y seguridad informática forense mediante test de penetración.
 - Valoración y tasación de equipos tecnológicos.
- Certificaciones y homologaciones.
 - Recuperación de datos.

- Asesoría informática y formación de profesionales del derecho, la administración pública, de cuerpos y fuerzas de seguridad del estado, y también como detectives privados.
- 415 Contraespionaje informático.

- Supervisión de actividad laboral informática.
- Detección y asesoría en casos de infidelidad empresarial, que se da cuando un trabajador se separa de una empresa y se lleva consigo información que no le pertenece como, por ejemplo, una base de datos de todos los clientes.
- Seguimiento de correos anónimos, autores de publicaciones, propietarios de páginas web.
- Análisis informático forense de videos, imágenes digitales y audio.
- Asesoría sobre falsificación de correos, imágenes, violaciones de seguridad, infiltraciones, doble contabilidad, fraude financiero y de sistemas informáticos, robo de claves, información sensible, secretos industriales, errores en la cadena de custodia.
- 430 Para realizar su labor, el perito debe entender bien la naturaleza del problema, en dependencia del tipo de organización.

Es importante que tenga una formación adecuada porque se han observado casos de mal manejo de la información. Por ejemplo, se puede citar el caso específico de un perito que era electricista, y al

435 realizar un peritaje informático, hizo copias de discos duros con el xCopy, lo que imposibilitó posteriormente la lectura o la copia del informe. Este tipo de inconvenientes son irreversibles.

Para lograr una buena formación es imprescindible contar con
una buena preparación previa en informática, que no implique solamente el manejo de la ofimática, sino los conocimientos básicos y generales sobre temas de desarrollo, ingeniería de software, base de datos, y bases de sistemas.

445 Con esta base se impone la especialización en Seguridad Informática, la que está conformada por varios campos: la auditoría, el hacking ético, la parte de defensa y análisis forense, para hacer una analogía podría usarse el ejemplo de un médico general que según la patología que detecte en su paciente, lo remite al médico especialista
450 que pueda dar un diagnóstico y un tratamiento más fiable.

La seguridad es una especialización dentro de la informática, y el análisis forense una subespecialización de la misma, por lo tanto, se podrá contar con diferentes criterios y puntos de vista.

455

1.3. Forense informático.

El forense informático es el experto en el campo informático y que dirige la investigación orientado al descubrimiento de información cuando se ha cometido un mal proceso o crimen 460 relacionado con el área de la informática (Navarro Clérigues, 2014). Inicialmente fue considerada como una materia, pero no está regulada, sin embargo, cuenta con una norma de metodología para el análisis forense de las evidencias electrónicas (http://www.ietf.org/rfc/rfc3227.txt) que apoyan al Forense 465 informático.

Se reconoce generalmente a los creadores del Foresis Toolkit, Dan Farmer y Dietes Venema, como los pioneros de la informática 470 forense. Actualmente, Brian Carrier es probablemente uno de los mayores expertos mundiales en el tema.

475 No existen estándares aceptados, aunque algunos proyectos están en desarrollo, como el C4PDF (Código de Prácticas para Análisis Forense Digital), de Roger Carhuatocto, el Open Source Computer Forensics Manual, de Matías Bevilacqua Trabado, y las Training Standards and Knowledge Skills and Abilities de la
480 International Organization on Computer Evidence, que mantiene en la web varias conferencias interesantes.

La norma internacional vigente no se usa mucho, sin embargo, en el caso de España, el analista forense cuenta desde junio de 2013, con la norma UNE (Una Norma Española), en la cual se define claramente cómo se debe realizar, tratar y gestionar un análisis forense de una evidencia digital. Hasta el 2013 se realizaba un procedimiento forense basado únicamente en conocimientos empíricos y sin la seguridad adecuada, lo que podía provocar 490 inconvenientes como que se obtuvieran diferentes tipos de evidencias luego de realizar un mismo procedimiento. Para evitar estos problemas es muy importante disponer de una metodología, como la norma española (UNE-71506, Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas., 2013)

1.4. Evidencia Digital

495

Casey define la evidencia de digital como "cualquier dato que
puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar una enlace (link) entre un crimen y su víctima o un crimen y su autor" (Casey, Handbook of Computer Crime Investigation, 2001)

- 505 A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia
- 510 (Sánchez Cordero, Conexión Inversa, 2014)

Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.

515

520

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso,

para esto se utilizan varias tecnologías, como por ejemplo checksums o hash MD5 (Deering, s.f.).

Cuando ha sucedido un incidente, generalmente, las personas
525 involucradas en el crimen intentan manipular y alterar la evidencia digital, tratando de borrar cualquier rastro que pueda dar muestras del daño. Sin embargo, este problema es mitigado con algunas características que posee la evidencia digital (Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the
530 Internet, 2004).

- La evidencia digital puede ser duplicada de forma exacta y se puede obtener una copia para ser examinada como si fuera la original. Esto se hace generalmente para no manejar los originales y evitar el riesgo de dañarlos.
- Actualmente, con las herramientas existentes, es muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.
- La evidencia digital es muy difícil de eliminar. Aun cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.
 - Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

545

1.4.1. Características de la evidencia digital

La evidencia digital posee las siguientes características:

1. Volátil

550 2. Anónima

- 3. Duplicable
- **4.** Alterable y modificable
- 5. Eliminable
- 555 Estas características hacen de la evidencia digital un constante desafío para la identificación y el análisis, que exige al grupo de seguridad y auditoría la capacitación tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia en una escena del delito.
- 560 Antes de realizar el proceso de análisis forense el equipo de seguridad o auditoría debe considerar los siguientes elementos para mantener la idoneidad del procedimiento forense.
 - La evidencia altamente volátil, se versará lo siguiente:
- 565 CPU (Registros, Caché), Memoria de Video. Usualmente la información en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de la memoria del sistema.
 - La evidencia medianamente volátil, se puede mencionar:

- 570 La memoria RAM, donde se incluye información sobre los procesos en ejecución, el hecho de capturarla hace que cambie. Además, se requiere conocimiento especializado para poder reconstruirla, pero no se demanda mucho conocimiento para hacer una búsqueda de palabras clave. Las tablas del kernel (Procesos en ejecución),
- 575 permiten analizar los procesos que pueden ser evidencia de actividades no autorizadas.

• La evidencia poco volátil, se indicará

Los medios fijos (discos duros), incluye área de swap, colas,
directorios temporales, directorios de registros. La información recolectada en el área de swap y las colas permite analizar los procesos y la información de los mismos en un punto del tiempo en particular. Los directorios permiten reconstruir eventos.

585 1.5. Admisibilidad de la evidencia digital

La evidencia digital (representada en todas las formas de registro magnético u óptico generadas por las organizaciones) debe avanzar hacia una estrategia de formalización que ofrezca un cuerpo 590 formal de evaluación y análisis que deba ser observado por el ordenamiento judicial de un país. En general, las legislaciones y las instituciones de justicia han fundado sus reflexiones sobre la admisibilidad de la evidencia en cuatro conceptos (Casey, Handbook of Computer Crime Investigation, 2001) (IOCE, 2000),
595 que a continuación se detallan:

1.5.1. Autenticidad

Sugiere ilustrar a las partes que la evidencia ha sido generada
y registrada en los sitios relacionados con el caso, particularmente en la escena del posible ilícito o lugares establecidos en la diligencia de levantamiento de evidencia.

De la misma manera, la autenticidad es entendida como 605 aquella característica que muestra la no alterabilidad de los medios originales y busca confirmar que los registros aportados correspondan a la realidad evidenciada en la fase de identificación y recolección. En los medios digitales, dada la volatilidad y alta capacidad de manipulación que se presenta en el almacenamiento electrónico. Si bien estas características también son, de alguna manera, inherentes a las vías tradicionales, el detalle se encuentra en que existe una serie de procedimientos asociados con el manejo y control de los mismos
en las organizaciones, mientras que para los registros magnéticos aún no se tiene la misma formalidad.

Verificar la autenticidad de los registros digitales requiere, de manera complementaria, a la directriz general establecida por la
620 organización sobre éstos, el desarrollo y configuración de mecanismos de control de integridad de archivos, es decir, necesita que una arquitectura exhiba mecanismos que aseguren la integridad de los registros y el control de cambios de los mismos.

625 Al establecer una arquitectura de cómputo con la que se fortalezca la protección de los medios digitales de registro y el procedimiento asociado para su verificación, aumenta sustancialmente la veracidad de las pruebas recolectadas y aportadas. En consecuencia, la información que se identifique en una

630 arquitectura con estas características tendrá mayor fuerza y solidez, no sólo por lo que su contenido ofrezca, sino por las condiciones de generación, control y revisión de los registros electrónicos.

En otras palabras, al contar con mecanismos y 635 procedimientos de control de integridad, se disminuye la incertidumbre sobre la manipulación no autorizada de la evidencia aportada y se concentra el proceso en los hechos y no en errores técnicos de control de la evidencia digital bajo análisis.

640 1.5.2. Confiabilidad

Es otro factor relevante para asegurar la admisibilidad de la misma. La confiabilidad nos dice si, efectivamente, los elementos probatorios aportados vienen de fuentes que son creíbles y 645 verificables y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue. En medios digitales podríamos relacionar este concepto a ¿cómo se recogen y analizan las evidencias digitales?, son preguntas cuyas respuestas buscan demostrar que poseen una manera confiable para ser identificados, recopilados y verificados.

Cuando se logra que una arquitectura de cómputo ofrezca mecanismos de sincronización de eventos y una centralización de registros de sus actividades (los cuales, de manera complementaria, soportan estrategias de control de integridad), se ha avanzado en la formalización de la confiabilidad de la evidencia digital.

655

Asimismo, en el desarrollo de software o diseño de programas es necesario incluir, desde las primeras fases de la creación de aplicaciones, un momento para la configuración de logs o registros

de auditoría del sistema ya que, de no hacerlo, se corre el riesgo de perder trazabilidad de las acciones de los usuarios en el sistema y, por tanto, crear un terreno fértil para la ocurrencia de acciones no autorizadas, es decir, se sugiere que la confiabilidad de la evidencia en una arquitectura de cómputo estará en función de la manera
como se sincronice la inscripción de las acciones de los usuarios y de un registro centralizado e íntegro de los mismos. Esto reitera la necesidad de un control de integridad de los registros del sistema para mantener su autenticidad.

670 1.5.3. Suficiencia

675

Es la presencia de toda la evidencia necesaria para adelantar el caso; esta característica, al igual que las anteriores, es factor crítico de éxito en las investigaciones en procesos judiciales. Con frecuencia, la falta de pruebas o insuficiencia de elementos

probatorios ocasiona la dilación o terminación de procesos que podrían haberse resuelto. En este sentido, los abogados reconocen que, mientras mayores fuentes de análisis y pruebas se tengan, habrá más posibilidades de avanzar en la defensa o acusación en un 680 proceso judicial.

Desarrollar estas particularidades en arquitecturas de cómputo requiere afianzar y manejar destrezas de correlación de eventos en registros de auditoría, es decir, si se cuenta con una arquitectura con 685 mecanismos de integridad, sincronización y centralización, es posible establecer patrones de análisis que muestren la imagen completa de la situación bajo revisión.

La correlación de hechos (definida como el establecimiento de 690 relaciones coherentes y consistentes entre diferentes fuentes de

datos para establecer y conocer eventos ocurridos en una arquitectura o proceso) sugiere una manera de probar y verificar la suficiencia de los datos entregados en un juicio.

695 Si analizamos esta posibilidad, es viable establecer relaciones entre los datos y los sucesos presentados, canalizando las inquietudes y afirmaciones de las partes sobre comportamientos y acciones de los involucrados, sustentando dichas conexiones con acontecimientos o registros que previamente han sido asegurados y 700 sincronizados.

Con esto en mente, la correlación se convierte en factor aglutinante de las características anteriores referenciadas para integridad y confiabilidad de la evidencia, lo que propone un 705 panorama básico requerido en las arquitecturas de cómputo para validar las condiciones solicitadas por la ley en relación con las pruebas.

Es decir, que la correlación de sucesos (como una función 710 entre la centralización del registro de eventos y el debido control de
integridad de los mismos) se soporta en una sincronización formal de tiempo y eventos que deben estar disponibles por la arquitectura de cómputo para asegurar la suficiencia del análisis de la información presente en una arquitectura de cómputo.

715

1.5.4. Conformidad con las leyes y reglas de la administración de justicia

Hace referencia a los procedimientos internacionalmente
aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital. Si bien están previstos en el código de procedimiento penal las actividades mínimas requeridas para aportar evidencia a los procesos existen en medios digitales iniciativas internacionales donde se establecen lineamientos de acción y
parámetros que cobijan el tratamiento de la evidencia en medios

electrónicos, los cuales deben ser revisados y analizados en cada uno de los contextos nacionales para su posible incorporación.

1.6. Determinar la relevancia de la evidencia

730

El estándar en esta fase establece valorar las evidencias de tal manera que se identifiquen las mejores evidencias que permitan presentar de manera clara y eficaz los elementos que se desean aportar en el proceso y en el juicio que se lleve. El objetivo es que el ente que valore las pruebas aportadas observe en sus análisis y

aportes los objetos de prueba más relevantes para el esclarecimiento de los hechos en discusión.

En este sentido el estándar sugiere dos criterios para tener en 740 cuenta a saber:

- a. Valor probatorio: que establece aquel registro electrónico que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación, confiabilidad del sistema.
- b. Reglas de la evidencia: que establece que se han seguido los
 procedimientos, reglas establecidas para la adecuada recolección y manejo de la evidencia.

1.7. Herramientas forenses

735

750 Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento

- 755 del equipo de seguridad que las utiliza. Estos dos elementos hacen del uso de las herramientas, una constante reflexión y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.
- 760 Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas para conocimiento general, que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática.
- 765 Si bien las herramientas forenses informáticas son licenciadas y sus precios oscilan entre los 600 y los 5000 euros, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código abierto.

770

Las herramientas forenses utilizadas en el presente libro son totalmente gratuitas y podrán ser utilizadas y validadas en un peritaje.

1.8. Confiablidad de las herramientas forenses en informática775

Para la computación Forense, otro reto emergente son las herramientas tecnológicas que los investigadores utilizan para adelantar sus pericias. Por un lado, las herramientas son licenciadas, propiedad de firmas desarrolladoras de software para forense digital, establecen un nicho de negocio que exige de los informáticos forenses en informática una importante inversión, tanto en

hardware y software, para darles mayor formalidad y certeza a las partes involucradas en un caso de la evidencia digital.

780

Dichas inversiones no solo son en la adquisición, sino en el mantenimiento y la actualización de las mismas, lo que hace que los especialistas forenses deben constantemente reforzar sus habilidades en el uso de estos programas y mantenerse notificados de posibles errores, propios de las mismas y sus maneras de
mitigarlos pues saben que un caso basado en la confiabilidad de las mismas se puede o no decidir.

Por otra parte, se encuentran las herramientas forenses de código abierto o también llamadas software libre, las cuales aún no **795** son cuestionadas en tribunales y poco se recomiendan como herramientas de uso formal para presentar en audiencias, por su condición de herramientas revisadas y analizadas por una comunidad de la cual poco se conoce de sus pruebas, de las personas que adelantan las mismas, ni el control de los errores.

800

Sin embargo, otra corriente defiende estas herramientas frente a las licenciadas, diciendo que el mundo de código abierto todo está para la investigación de un tercero, que las pruebas se pueden adelantar con mayor confianza que en las abiertas, y que el nivel de

805 confiabilidad es mayor, dado que son muchos "ojos" los que están tratando de mejorarla.

Mientras esta disyuntiva continua, se adelanta importantes esfuerzos formales para probar las herramientas forenses como el 810 proyecto de National Institute of Standars and Tecnology "NIST" cuyo objetivo es establecer una metodología para probar

aplicaciones forenses en informática a través de la especificación general de herramientas.

815 En este contexto, las pruebas que realicen a los programas y dispositivos de hardware serán útiles para dar cumplimiento a las exigencias propias del test de Deubert prueba de referencia generalizada para establecer la confiabilidad de las herramientas en computación forense.

820

En este sentido, los programas o las herramientas de computación forense requieren estudios y análisis detallados para contar con un nivel de aceptación de los mismos.

CAPÍTULO II

ARTEFACTOS

Artefacto es "todo aquello que puede obtener una evidencia"

830 (Sánchez Cordero, Análisis Forense Informático, 2015), y cabe recalcar que son los diferentes ficheros, cadenas de registro, rutas de acceso y configuraciones que pueden determinar la actividad de un malware o de un usuario malicioso, así como las evidencias necesarias para una prueba.

835

_

Un artefacto puede contener todo lo siguiente (Tabla 2.1.):

Arte	factos
• Logs o ficheros de sistema	• La papelera
• Tabla maestra de archivos	• Metadatos en imágenes
MFT	
• El registro de Windows	• Ficheros de hibernación y
	memoria
• El visor de Eventos	• Copias de seguridad
• Los ficheros Prefetch	• Volume Shadow Copies
• Los accesos directos	
Fuente: <u>http://conexioninversa.blog</u>	<u>spot.com/2013/12/artefactos-forenses-</u>
i.l	html

Tabla 2.1. Algunos elementos de los Artefactos.

840 2.1. Shellbags.

Se considera artefacto shellbags, aquellos lugares donde el sistema operativo almacena información relacionada con las preferencias de visualización de contenidos en Windows Explorer, tales como: tamaño de la ventana, posición de ésta en la pantalla,

845 modo de visualización y elementos visibles, por mencionar algunos ejemplos. Si se requiere observar a las shellbags en operación, lo adecuado sería hacer doble clic sobre "Mi PC", cerrar la ventana y volver a abrir. Las preferencias de visualización se han guardado (Hernando, 2011).

850

El interés forense de las shellbags procede de su naturaleza, solo existen si una ventana se ha abierto y cerrado al menos una vez, con lo que pueden ser utilizadas para trazar la actividad de los usuarios. Esto es debido a la información que almacenan, lo que **855** incluye los timestamps temporales que pueden finalmente entender si un usuario determinado abrió o no una carpeta específica en una fecha y hora definida.

860 HKEY_USERS\\Software\Microsoft\Windows\Shell
HKEY_USERS\\Software\Microsoft\Windows\ShellNoR oam
Ambas son idénticas en estructura; la única diferencia es que

En el caso de Windows, las shellbags, son principalmente dos:

- la primera almacena información relacionada con carpetas
 remotas (roaming) y la segunda custodia información relacionada con contenidos locales (sin roaming).
 - Se recomienda utilizar ERUNT para la copia en vivo.

2.2. Registros HIVE.

- 870 Son importantes por la información que se encuentra en un análisis forense; es decir, el sistema operativo Windows, si se cambia el fondo de pantalla para colocar una fotografía a continuación se reiniciará y la fotografía aparece otra vez (Tocados Cano, 2015). Lo que sucedió es que se ha guardado un valor, un parámetro en el
- 875 registro de Windows y el valor guardado, hace que el equipo cuando se encienda recupere la información que se almacenó.

Un HIVE es la estructura del registro que cuando se apaga el equipo se almacena la información sobre ficheros.

El editor del registro no muestra solo la estructura local;
 existen varias claves y subclaves que están almacenadas sobre ficheros en el disco duro; es decir, cuando se apaga el ordenador hay ficheros que desaparecen, hay partes que son volátiles por ejemplo la dirección IP o cuando cambia la misma, se menciona la posición de una ventana, eso es volátil
 885 y aparecerá la dirección de la última posición que se haya guardado.

Estos ficheros (Fig. 2.1.) son llamados "hives".

890

• El sistema a estos ficheros "los mima" estableciendo copias de seguridad para su posterior utilización en caso de que el sistema falle en el inicio del sistema operativo. Las claves del registro que se asocian a los 'hives' son HKLM y HKU.

HKLM\SAM> SAM, SAM.LOG
HKLM\SECURITY> SECURITY, SECURITY.LOG
HKLM\SOFTWARE> software, software LOG, software sav
HKLM\SYSTEM> system, system.LOG, system.sav
HKLM\HARDWARE> (Dinamico/Volatil Hive)
HKU\DEFAULT> default, default.LOG, default.sav
HKU\SID> NTUSER.DAT
HKU\SID_CLASSES> UsrClass.dat, UsrClass.dat.LOG

Fig. 2.1. Registry Path Ficheros HIVE.

895 *Fuente:* Curso de Informàtica forense i evidències digitals, realizada por Pedro Sánchez Cordero, Universitat Rovira i Virgili, Catalunya-España, 2015.

Cuando se apaga el equipo, los ficheros físicos históricos se localizan

en la raíz del sistema operativo (Fig.2.2.).



Fig. 2.2. El Registro del Computador.

HKEY_CLASSES_ROOT: Es todo lo que está relacionado con

el software y el hardware de la máquina.

905

HKEY_CURRENT_USER: Es todo lo que está afín con el usuario que ha iniciado la sesión, es decir si se inició la sesión en la máquina como usuario *Iván*, pues todo lo que se haga como *Iván* se va a grabar en esta clave de registro.

HKEY_LOCAL_MACHINE: Todo lo que tenga que ver con el software y el hardware de este usuario, sería una combinación de los ficheros HKEY_CLASSES_ROOT y HKEY_CURRENT_USER, y es el lugar donde se va a guardar la información, es decir en este lugar se tienen las claves de los usuarios).

HKEY_USERS: Todos los demás usuarios se guardarán en este fichero; ejemplo: se combina el usuario *Iván* y el usuario *Diego* cuando haga una combinación en la parte de usuario *Iván* se
almacenará en el HKEY_CURRENT_USER y cuando inicie la sesión *Diego* remotamente se referirá en el HKEY_USERS que es donde se ubican los demás usuarios.

HKEY_CURRENT_CONFIG: Si se realiza una configuración
925 de pantalla, de parámetros o de colores se almacenará en este lugar. Editor del registro → Equipo → HKEY_LOCAL_MACHINE →
SAM → SAM y en esta clave del registro, que aparentemente está vacía, se encuentran las cuentas de los usuarios. Cuando se crea un usuario, se viene a esta parte del registro; ejemplo: se crea el usuario

930 Saul y se va a: Editor del registro \rightarrow Equipo \rightarrow HKEY_LOCAL_MACHINE \rightarrow Software \rightarrow Microsoft \rightarrow Notepad; se encuentra vacío y no se puede observar.

Se puede gestionar con el administrador de cuentas de usuario,
pero ciertamente se va a grabar en: Editor del registro → Equipo → HKEY_LOCAL_MACHINE → Software → Microsoft → Windows → CurrentVersion; en este lugar se guarda el software, cuentas por defecto, Microsoft, ODBC, si se tiene conexiones.

940 En la ubicación Editor del registro → Equipo → HKEY_LOCAL_MACHINE → Software → Microsoft → Windows → CurrentVersion → Run; se observa que todo lo que se irá a cambiar; se va a almacenar en el registro, por ejemplo: en este lugar se tiene la clave Windows Current Version y es la ruta de
945 carpetas que tiene el usuario, en este registro se iniciará el computador. Si se desea arrancar un programa se tendrá que crear una clave, colocar la ruta del programa y automáticamente arrancará. Cuando se detiene el disco, estas claves se almacenan en una parte de un fichero del disco duro C:\Windows\System32\config y se

- 950 marcan los archivos: *DEFAULT, SAM, SECURITY, SOFTWARE, SYSTEM,* estos archivos se llaman por defecto ficheros HIVE (ficheros que cuando se apaga el equipo, se guardan como registros de Windows y se pueden acceder). No se puede acceder a estos archivos, debido a que el computador se encuentra
- 955 encendido y como no se puede copiar la información se puede aplicar la utilidad *Access Data FTK Imager* para hacer el clonado con el computador encendido; y lo que se hace es añadir un ítem (Fig. 2.3.).



960

965

Fig. 2.3. Access Data FTK Imager.

En este momento se plantea una interrogante acerca de que se va a realizar con el disco duro, unidad lógica, fichero de imagen o la carpeta, es decir extraer los ficheros *HIVE*. Se elige una unidad lógica ya que se encuentra encendido el equipo y se escoge la partición C: la agregan; y se procede a buscar la información que se localiza en C:\Windows\System32\config; cuando se despliega la pantalla se pulsa el botón derecho y se exportan los archivos a la carpeta donde se requiere copiar; ahora ya se dispone de los HIVE copiados en la carpeta REGISTRO (Fig. 2.4.).

$\leftarrow \rightarrow - \uparrow$	→ REGISTRO		
Nombre	Fecha de modificación	Tipo	Tamaño
DEFAULT	10/03/2018 11:52 p.m.	Archivo	1,024 KB
SAM	03/03/2018 12:07 p.m.	Archivo	48 KB
SECURITY	10/03/2018 11:52 p.m.	Archivo	56 KB
SOFTWARE	10/03/2018 11:52 p.m.	Archivo	111,360 KB
SYSTEM	10/03/2018 11:52 p.m.	Archivo	26,112 KB

970

Fig. 2.4. HIVE copiados en la carpeta REGISTRO.

Para continuar con el proceso es necesario ir a un navegador web
975 y encontrar una utilidad, para saber la ubicación desde donde se conecta al computador, la URL es: <u>http://www.mitec.cz/</u>, (Fig. 2.5.):



Fig. 2.5. Ubicación del lugar de donde se conecta en la Pc. Fuente: <u>http://www.mitec.cz/</u>

2.2.1. Windows Registry Recovery

980

985 Se descarga el artefacto Windows Registry Recovery (http://ww.mitec.cz/wrr.html), desde la cual se obtiene numerosa información acerca de diferentes herramientas forenses, se procede a descargar el que se denomina Windows Registry Recovery; a continuación, se ejecuta porque no necesita instalación y se abren
990 los archivos de REGISTRO; después se procede a seleccionar todos los archivos y se pulsa la opción Abrir (Fig. 2.6.).



Fig. 2.6. Ejecución del Windows Registry Recovery en la carpeta REGISTRO.

995

Esta herramienta va a interpretar el contenido de los *HIVE* que es lo mismo que el registro de Windows, por ejemplo: al ubicarse en la pestaña **SOFTWARE;** y si desea observar que instalación de Windows, se procede a dar clic sobre *Windows* **1000** *Installation* y en la pestaña *Installed Software* (el registro más grande de los HIVE) se puede ver que software tiene con la fecha de instalación (Fig. 2.7.).

EFAULT 👩 SAM	SECURITY SOFTWARE	SYSTEM			
Export to REGEDIT4 form	General Installed Software	lot Fixes			
Everet Data	Name	Version	Company	Datetme	Uninstal
Coper rootern	Intell() Management Engine Co	11.0.0.1167	Intel Corporation	20160415	MSEREC.exe /1(PBC 0P91A-800E-4405-ASP2-824AA8)0063C)
File Information	Actualización de NVIDIA 2, 11, 6,0	2.11.4.0	NVIDIA Cremor	20160708	Hatesteckee (1(2)1/0-69-4001-5/02-0-30/00 (000000)
Security Records	AutoCAO 2015 - English	20.0.51.0	Autodesk	20160708	
	AutoCAD 2015 - English	20.0.51.0	Autodesk	20160708	C: Yrogram Files/Autodesk/AutoCAD 2015/Setup/en-us/Setup/Setup.exe /P (5783F2D7-E001-0000-0102-0060B0CE58BA) /M ACAD
5AM	AutoCAD 2015 Language Pack	20.0.51.0	Autodesk	20160708	
Windows Installation	Autodesk 360	5.0.27.1100	Autodesk	20160708	MaExec.exe /X(556966D9/F7F6-4218-9707-D07901604DDF)
	Autodesk AutoCAD 2015 - English	20.0.51.0	Autodesk	08/07/2016	C:\Program Files\Autodesk\AutoCAD 2015\Setup\en-us\Setup\Setup.exe /P (5783F2D7-E001-0000-0102-0050B0CE58BA) /M ACAD
Hardware	Autodesk BIM 360 Glue AutoCA	3.32.3004	Autodesk	20160708	MsExec.exe (X(50589081-AFC2-4932-9071-AC585AC1EA83)
User Data	Autodesk ReCap	1.3.1.39	Autodesk	20160708	
The second second second second	Autodesk ReCap	1.3.1.39	Autodesk	08/07/2016	C: Yrogram Piles (Autodesk (Autodesk ReCapit)etup (etup (etu (etup (etup (etup (etup (etup (etup (etup (etu (etu) (etup (etu))
scarcup Applications	B COmment	3.0.0.10	Apple Inc.	20160415	MSEXEC.exe (A (bc.)o 1852-4300-4500-6503-65050-680)
Services and Drivers	Common Desistrice Accent	1.67.0	CEM	20120608	Melliner, ava. N/INTLANE14-0411-4197-0777-16 10878178144481
Network Configuration	R CyberLink PhotoDirector	5.0.6.7006	Nombre de su o	20160415	"C: Procent Files (x66)UnstallSheid Installation Information//SA454ECS-2178-43a5-BCE1-2000C4E20E013/Setup eve" /z-uninstall
	CyberLink PowerDirector 12	12.0.5.4601	Nombre de su o	20160415	"Cr Program Files (x86) UnstallSheld Installation Information (2):1646825-0391-4240-9344-27/481004093) (Setup exe" /z-uninstall
Windows Firewall Settings	DisableMSDefender	1.0.0	Hewlett-Packar	20160415	NoExec.exe ///74PE3940-FB76-47CD-846A-91E288817EF2}
Environment	ELAN Touchped 15.2.1.1_X64	15.2.1.1	ELAN Microelec		NProgramFiles%/Elantech/ETDUn_inst.exe
	Energy Star	1.0.9	Hewlett-Packer	20160415	MsExec.exe //(465CA286-98AF-Æ77-8E22-A908C3-889EC)
Shell Folders	15 HP Documentation		HP		CMD /C "C: Program Files HP Documentation Doc_Uninstall.ond"
Outlook Express	HP ePrint Windows Driver	4.8.84.16	HP	20160415	MsExec.exe /f(38C36736-6685-4C48-AF0A-C41C335A8C80)
	HP Welcome	1.0	HP Inc.		c:@rogram Files/HP/HP Welcome/uninstal.bat
Raw Data	BM SPSS Statistics 19	19.0.0	SPSS Inc., an I	20160918	MsExec.exe /f(06C43FAA-7226-41EF-A09E-9AE0AA849FFE)
	5 IBM SPSS Statistics 19 Help Packs	19.0.0	SPSS Inc.	20160918	MsExec.exe /[/F1E691EA-CAA6-4427-87C7-C94308C686EC]
	BM SPSS Statistics 23	23.0.0.0	IBM Corp	20170320	MsExec.exe /1(C38A73A4-2A45-4036-8541-#F5F81460788)
	5 Intel(R) Chipset Device Software	10.1.1.9	Intel Corporation	20160415	MaExec.exe (ft(55398EAC+58E-#19-8553 8DF889EFD839)
	Intel(R) Management Engine Co	1.0.0.0	Intel Corporation	20160415	MsExec.exe (1(7ESC90F9-4883-49CE-8381-449E952078D1)
	Intel(R) Management Engine Co	11.0.0.1167	Intel Corporation		"CriProgramDatal@nteliPackage Cache\{ICEAC85D-2990-4760-800F-80E5E91F3700}\Setup.exe" -uninstal
	Intel(R) ME UninstalLegacy	1.0.1.0	Intel Corporation	20160415	MsExec.exe (E(0873CCF5-A7CF-H137-A90C-184ACE1C85A3)
	5 Intel(R) Rapid Storage Technology	14.5.2.1088	Intel Corporation		"C: ProgramData(Intel/Package Cache\{409CB30E-E457-4008-981A-ED189EA21140})(Setup.exe" -uninstall
	5. Intel(R) Rapid Storage Technology	14.5.2.1088	Intel Corporation	20160415	NoExec.exe (1/303CSCD6-2525-49C5-9E49-08D92F9F638D)

Fig. 2.7. Instalación de programas en WRR.

1005

En **SAM**, se ubica la pestaña donde se encuentra *Groups and User;* que son los usuarios en la computadora, contiene a su vez información con los metadatos: de cuando fue el último logon, la última vez que se cambió la contraseña, la fecha que expira la **1010** contraseña, el último logon incorrecto y los grupos que tiene la máquina.

En **SYSTEM**, sobre la pestaña Network Configuration se puede observar acerca de TCP/IP; *Windows Firewalls Settings* y se pregunta la configuración de Red; al ubicarse en las pestañas **1015** *Hardware*, sobre *DeviceMap*, y *RefreshCurrent* se obtendrá que IPs tenía la máquina, Gateway, DNS; se podrán saber también si tiene Reglas en el Firewall, que reglas tenía editadas, las aplicaciones; además se identificará que hardware estaba utilizando, que unidades y discos duros poseía en funcionamiento; es decir, si alguien copió la 1020 información aquí se identifica el modelo que tenía el dispositivo en la pestaña *Service and Drivers*, en el sistema operativo Windows queda todo el historial de lo que se realiza.

Se desconoce lo que se copió al pendrive, pero se mantiene un 1025 historial, donde también se puede saber los servicios y drivers que tenía la máquina, si estaban en inicio automático.

Toda la información se puede observar en el REGEDIT, viendo las claves, llevando los ficheros en el pendrive; para ser 1030 analizados desde la casa ubicado en uno de los apartados forense más generales, que permite analizar el registro de Windows, que es la base de datos de configuraciones volátiles y no volátiles del entorno del sistema operativo y aplicaciones.

1035 La cadena HKLM se ubica en:%SYSTEMROOT%\System32\config\ (%SYSTEMROOT%)

Normalmente referido a:

C:\WINDOWS\HKLM\HARDWARE

Este fichero "hive" es dinámico y se crea en tiempo de ejecución en

1040 el inicio del sistema, copiándose en memoria (Russinovich, 1999).

HKU\.DEFAULT corresponde a:

%SYSTEMROOT%\System32\config\default.HKU\SID; normalmente se encuentra en el directorio por defecto del usuario

1045 (home directory), en %USERPROFILE%\NTUSER.DAT, y

HKU\SID_CLASSES que corresponde a:

%USERPROFILE%\Local Settings \Application

 $Data \backslash Microsoft \backslash Windows \backslash UsrClass.dat.$

1050 Las claves con valores forenses se las puede mencionar de la siguiente manera:

HKCU\Software\Microsoft\Windows\CurrentVersion\Expl orer\ComDlg32\OpenSaveMRU MRU es la abreviatura de "Most-Recently-Used". Esta clave

1055 mantiene los ficheros guardados o abiertos normalmente desde el explorador de ficheros o bien utilizando la caja de abrir o guardar ficheros (por ejemplo, Excel), igualmente se encuentran aquellos ficheros que se abren desde el Internet Explorer.

HKCU\Software\Microsoft\Windows\CurrentVersion\Expl orer\ComDlg32\LastVisitedMRU

1060

Esta clave corresponde a las aplicaciones más utilizados o actualizados; es decir, los documentos más recientes.

HKCU\Software\Microsoft\Windows\CurrentVersion\Expl orer\RecentDocs

1065 Esta clave mantiene la lista de ficheros ejecutados o abiertos desde Explorer. Corresponde a %USERPROFILE%\Recent. La clave contiene tanto los ficheros locales como de red, incluido ficheros no ejecutables.

HKCU\Software\Microsoft\Windows\CurrentVersion\Expl

Esta clave mantiene una lista de entradas de comandos utilizados desde el menú: Inicio \rightarrow Ejecutar \rightarrow cmd

HKCU\Software\Microsoft\Windows\CurrentVersion\Expl orer\MountPoints2\CPC\Volume\

1075 Contiene las unidades montadas y asociadas físicamente a un disco o unidad de red, incluidas Dvd's y Usb's

HKCU \Software\Microsoft\Search Assistant\ACMru

La clave contiene las búsquedas más recientes del buscador de ficheros de Windows. La subclave 5603 contiene los términos de

1080 búsqueda de las carpetas y ficheros, así como la subclave 5604, que contiene palabras y frases que se buscan en los contenidos de ficheros.

HKCU\Software\Microsoft\Windows\CurrentVersion\Expl orer\UserAssist

1085 La clave contiene una lista de objetos como accesos directos, acceso al Panel de Control, por ejemplo: La subclave GUID con el carácter "5E6" que corresponde a la barra de Internet Explorer y el "750" al Active Desktop.

HKCU\Software\Microsoft\Internet Explorer\

1090 Contiene las últimas 25 Url's (fichero o path) que se ha escrito en el Internet Explorer (IE) o en la barra de Windows Explorer.

HKLM \SYSTEM\MountedDevices

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

1095 Esta clave es de vital importancia ya que da amplia información acerca de los Usb's y tarjetas de memoria que fueron conectadas al sistema.

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

1100 La clave donde se ubica el fichero de paginación y su configuración. Es importante desde el punto de vista que se puede comprobar si está configurado para su borrado "ClearPagefileAtShutdown".

HKLM\SYSTEM\CurrentControlSet\Services\

Contiene los servicios de la máquina.

1105 HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Para meters\Interfaces\GUID

Contiene la configuración de los adaptadores de red, IP, Gateway... etc.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Uninstall

La clave representa los programas que constan instalados en el equipo. Se debe estar alerta a las fechas, ya que esa información se encuentra almacenada en esta clave.

HKLM\ SOFTWARE

1110

1115 \Microsoft\Windows\CurrentVersion\Run

HKLM\ SOFTWARE

\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\ SOFTWARE

\Microsoft\Windows\CurrentVersion\RunOnceEx

1120 HKLM\ SOFTWARE

\Microsoft\Windows\CurrentVersion\RunServices

HKLM\ SOFTWARE

\Microsoft\Windows\CurrentVersion\RunServicesOnce

Contiene los "paths" a las aplicaciones que automáticamente se

1125 ejecutan durante el inicio del sistema sin intervención del usuario, en esta ubicación están numerosas pistas sobre malware.

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersi on\Winlogon

La ubicación especifica cuál es el entorno de ejecución de las 1130 ventanas; por defecto es Explorer.exe. Algunos malware modifican esta clave por otros valores en el "Shell=Explorer.exe %system%\System32.exe"

HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Int erfaces\GUID

1135 Contiene la configuración de las redes wifi

HKCU\Software\Microsoft\Windows\CurrentVersion\Expl orer\Map Network Drive MRU

HKCU\Software\Microsoft\Windows\CurrentVersion\Expl

1140 orer\MountPoints2

Las claves mantienen la lista de unidades de red mapeadas a caracteres, es decir, por ejemplo, M: F:

2.2.2. RegRipper

1145

Es una herramienta (Fig. 2.8.), que puede monitorear todo de una manera accesible; sin entorno gráfico, pero va a permitir encriptar (Arnedo Blanco, 2014). RegRipper, va a posibilitar poder parsear, obtener un informe de una forma rápida y cómoda a modo **1150** de script. RegRipper en la versión 2,5 está orientada a Windows XP y RegRipper en la versión 2,8 dirigida a Windows en su versión 7, 8 y 10. Se puede descargar directamente desde el siguiente enlace: <u>https://github.com/keydet89/RegRipper2.8</u>



1155

Fig. 2.8. Logotipo de la Herramienta RegRipper. Fuente: <u>http://resources.infosecinstitute.com/windows-registry-analysis-</u> regripper-hands-case-study-2/#gref Una vez que se ha descargado desde el sitio web donde se 1160 obtienen los ficheros ejecutables (.exe), y una serie de ficheros (.pl), al cual .*pl* es el código fuente por si se lo desea reprogramar y mejorar su versión, si no se desea modificar se tiene el ejecutable rr.exe, el rip.exe y el pb.exe que es para la base de datos (Fig. 2.9.).

Nombre Fecha de modificación Tipo Tamaño plugins 12/03/2018 04:25 a. m. Carpeta de archivos . . gitattributes 12/03/2018 04:25 a. m. Archivo GITATTRIBUTES 1 KB . gitignore 12/03/2018 04:25 a. m. Archivo GITATTRIBUTES 1 KB . gitignore 12/03/2018 04:25 a. m. Archivo GITIGNORE 1 KB copying.txt 12/03/2018 04:25 a. m. Documento de texto 35 KB icense.txt 12/03/2018 04:25 a. m. Documento de texto 1 KB p2x5124.dll 12/03/2018 04:25 a. m. Extensión de la aplicación 417 KB P2x5124.dll 12/03/2018 04:25 a. m. Archivo MD 1 KB regripper.pdf 12/03/2018 04:25 a. m. Archivo MD 1 KB rip.exe 12/03/2018 04:25 a. m. Archivo PL 10 KB rip.pl 12/03/2018 04:25 a. m. Archivo PL 10 KB rip.pl 12/03/2018 04:25 a. m. Archivo PL 10 KB rip.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB rip.pl 12/03/2018 04:25 a. m	$\leftarrow \rightarrow \checkmark \uparrow$	> RegRipper2.8-master		
plugins 12/03/2018 04:25 a. m. Carpeta de archivos gitattributes 12/03/2018 04:25 a. m. Archivo GITATTRIBUTES 1 KB gitignore 12/03/2018 04:25 a. m. Archivo GITATTRIBUTES 1 KB gitignore 12/03/2018 04:25 a. m. Archivo GITATTRIBUTES 1 KB gitignore 12/03/2018 04:25 a. m. Documento de texto 35 KB gitignore 12/03/2018 04:25 a. m. Documento de texto 1 KB gozying.bt 12/03/2018 04:25 a. m. Documento de texto 1 KB gozying.bt 12/03/2018 04:25 a. m. Extensión de la aplicación 417 KB gozying.bt 12/03/2018 04:25 a. m. Archivo MD 1 KB gregripper.pdf 12/03/2018 04:25 a. m. Adobe Acrobat Document 157 KB gip.exe 12/03/2018 04:25 a. m. Aplicación 1,741 KB gip.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB gip.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB gip.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB	Nombre	Fecha de modificación	Tipo	Tamaño
i.gitattributes 12/03/2018 04:25 a. m. Archivo GITATTRIBUTES 1 KB i.gitignore 12/03/2018 04:25 a. m. Archivo GITIGNORE 1 KB icopying.txt 12/03/2018 04:25 a. m. Documento de texto 35 KB icense.txt 12/03/2018 04:25 a. m. Documento de texto 1 KB icense.txt 12/03/2018 04:25 a. m. Documento de texto 1 KB icense.txt 12/03/2018 04:25 a. m. Documento de texto 1 KB icense.txt 12/03/2018 04:25 a. m. Extensión de la aplicación 417 KB icense.txt 12/03/2018 04:25 a. m. Archivo MD 1 KB iperper.pdf 12/03/2018 04:25 a. m. Archivo MD 1 KB rip.exe 12/03/2018 04:25 a. m. Adobe Acrobat Document 157 KB rip.exe 12/03/2018 04:25 a. m. Aplicación 1,741 KB rip.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB rr.r.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB	plugins	12/03/2018 04:25 a.m.	Carpeta de archivos	
□.gitignore 12/03/2018 04:25 a. m. Archivo GITIGNORE 1 KB □ copying.txt 12/03/2018 04:25 a. m. Documento de texto 35 KB □ license.txt 12/03/2018 04:25 a. m. Documento de texto 1 KB ☑ p2x5124.dll 12/03/2018 04:25 a. m. Documento de texto 1 KB ☑ p2x5124.dll 12/03/2018 04:25 a. m. Extensión de la aplicación 417 KB ☑ README.md 12/03/2018 04:25 a. m. Archivo MD 1 KB ☑ regripper.pdf 12/03/2018 04:25 a. m. Archivo MD 1 KB ☑ rip.exe 12/03/2018 04:25 a. m. Adobe Acrobat Document 157 KB □ rip.exe 12/03/2018 04:25 a. m. Aplicación 1,741 KB □ rip.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB □ rr.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB □ rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB ☑ sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB □ shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB □ time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB	.gitattributes	12/03/2018 04:25 a.m.	Archivo GITATTRIBUTES	1 KB
□ copying.txt 12/03/2018 04:25 a. m. Documento de texto 35 KB □ license.txt 12/03/2018 04:25 a. m. Documento de texto 1 KB ☑ p2x5124.dll 12/03/2018 04:25 a. m. Extensión de la aplicación 417 KB ☑ p2x5124.dll 12/03/2018 04:25 a. m. Extensión de la aplicación 417 KB ☑ README.md 12/03/2018 04:25 a. m. Archivo MD 1 KB ☑ regripper.pdf 12/03/2018 04:25 a. m. Adobe Acrobat Document 157 KB □ rip.exe 12/03/2018 04:25 a. m. Adobe Acrobat Document 1741 KB □ rip.pl 12/03/2018 04:25 a. m. Aplicación 1,741 KB □ rr.exe 12/03/2018 04:25 a. m. Aplicación 2,379 KB □ rr.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB □ rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB □ sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB □ shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB □ time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB □ updates.txt 12/03/2018 04:25 a. m. Archivo PL	.gitignore	12/03/2018 04:25 a.m.	Archivo GITIGNORE	1 KB
■ license.txt 12/03/2018 04:25 a. m. Documento de texto 1 KB ■ p2x5124.dll 12/03/2018 04:25 a. m. Extensión de la aplicación 417 KB ■ README.md 12/03/2018 04:25 a. m. Archivo MD 1 KB ■ regripper.pdf 12/03/2018 04:25 a. m. Archivo MD 1 KB ■ regripper.pdf 12/03/2018 04:25 a. m. Adobe Acrobat Document 157 KB ■ rip.exe 12/03/2018 04:25 a. m. Adobe Acrobat Document 1741 KB ■ rip.pl 12/03/2018 04:25 a. m. Aplicación 1,741 KB ■ rip.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB ■ rr.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB ■ rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB ■ sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB ■ shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB ■ time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB ■ updates.txt 12/03/2	copying.txt	12/03/2018 04:25 a.m.	Documento de texto	35 KB
§ p2x5124.dll 12/03/2018 04:25 a. m. Extensión de la aplicación 417 KB § README.md 12/03/2018 04:25 a. m. Archivo MD 1 KB ¶ regripper.pdf 12/03/2018 04:25 a. m. Archivo MD 1 KB ¶ regripper.pdf 12/03/2018 04:25 a. m. Adobe Acrobat Document 157 KB ¶ rip.pl 12/03/2018 04:25 a. m. Adobe Acrobat Document 1,741 KB ¶ rip.pl 12/03/2018 04:25 a. m. Archivo PL 10 KB ¶ rr.exe 12/03/2018 04:25 a. m. Archivo PL 10 KB ¶ rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB ¶ sample.txt 12/03/2018 04:25 a. m. Archivo PL 12 KB ¶ sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB ¶ shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB ↓ time.pl 12/03/2018 04:25 a. m. Archivo PL	license.txt	12/03/2018 04:25 a.m.	Documento de texto	1 KB
Image: Second	p2x5124.dll	12/03/2018 04:25 a.m.	Extensión de la aplicación	417 KB
Tegripper.pdf 12/03/2018 04:25 a. m. Adobe Acrobat Document 157 KB rip.exe 12/03/2018 04:25 a. m. Aplicación 1,741 KB rip.pl 12/03/2018 04:25 a. m. Aplicación 1,741 KB rip.pl 12/03/2018 04:25 a. m. Archivo PL 10 KB rr.exe 12/03/2018 04:25 a. m. Aplicación 2,379 KB rr.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB time.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB updates.txt 12/03/2018 04:25 a. m. Documento de texto 6 KB	README.md	12/03/2018 04:25 a.m.	Archivo MD	1 KB
a rip.exe 12/03/2018 04:25 a. m. Aplicación 1,741 KB rip.pl 12/03/2018 04:25 a. m. Archivo PL 10 KB a rr.exe 12/03/2018 04:25 a. m. Archivo PL 10 KB i rr.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB i rr.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB i rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB i sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB i shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB i time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB i updates.txt 12/03/2018 04:25 a. m. Documento de texto 6 KB	🗾 regripper.pdf	12/03/2018 04:25 a.m.	Adobe Acrobat Document	157 KB
□ rip.pl 12/03/2018 04:25 a. m. Archivo PL 10 KB □ rr.exe 12/03/2018 04:25 a. m. Aplicación 2,379 KB □ rr.pl 12/03/2018 04:25 a. m. Aplicación 2,379 KB □ rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB □ sample.bxt 12/03/2018 04:25 a. m. Documento de texto 416 KB □ shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB □ time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB □ updates.txt 12/03/2018 04:25 a. m. Archivo PL 3 KB	rip.exe	12/03/2018 04:25 a.m.	Aplicación	1,741 KB
a rr.exe 12/03/2018 04:25 a. m. Aplicación 2,379 KB rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB shellitems.pl 12/03/2018 04:25 a. m. Documento de texto 416 KB time.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB updates.txt 12/03/2018 04:25 a. m. Documento de texto 6 KB	📄 rip.pl	12/03/2018 04:25 a.m.	Archivo PL	10 KB
□ rr.pl 12/03/2018 04:25 a. m. Archivo PL 12 KB □ sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB □ shellitems.pl 12/03/2018 04:25 a. m. Documento de texto 416 KB □ shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB □ time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB □ updates.txt 12/03/2018 04:25 a. m. Documento de texto 6 KB	rr.exe	12/03/2018 04:25 a.m.	Aplicación	2,379 KB
image: sample.txt 12/03/2018 04:25 a. m. Documento de texto 416 KB image: shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB image: time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB image: updates.txt 12/03/2018 04:25 a. m. Documento de texto 6 KB	📄 rr.pl	12/03/2018 04:25 a.m.	Archivo PL	12 KB
□ shellitems.pl 12/03/2018 04:25 a. m. Archivo PL 27 KB □ time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB □ updates.txt 12/03/2018 04:25 a. m. Documento de texto 6 KB	📄 sample.txt	12/03/2018 04:25 a.m.	Documento de texto	416 KB
□ time.pl 12/03/2018 04:25 a. m. Archivo PL 3 KB □ updates.txt 12/03/2018 04:25 a. m. Documento de texto 6 KB	📄 shellitems.pl	12/03/2018 04:25 a.m.	Archivo PL	27 KB
updates.txt 12/03/2018 04:25 a.m. Documento de texto 6 KB	📄 time.pl	12/03/2018 04:25 a.m.	Archivo PL	3 KB
	updates.txt	12/03/2018 04:25 a.m.	Documento de texto	6 KB

1165

1170

Fig. 2.9. Herramienta RegRipper.

En caso de editar el archivo *rr.pl*, se lo puede abrir por ejemplo con la herramienta Notepad++, *rr.pl* contiene el código fuente, donde se observa las llamadas, el menú, los campos, y se obtiene una carpeta muy importante que es los *plugins*. Los plugins son diferentes programas que permiten parsear los ficheros *HIVE*, por tanto RegRipper va a elegir los ficheros HIVE, parsear y pasará por los plugins, por ejemplo: si se usa el

1175 navegador Internet Explorer (ie_main.pl), que tipo de configuración están usando (ie_settings.pl), conexiones a yahoo (yahoo_cu.pl), si se tiene outlook (outlook2.pl), sí disponen de las pstools.pl, se tiene documentación office (officedocs.pl), que tipo de winlogon.pl están realizando, y si se está haciendo bakuprestore.pl, la lista de red
1180 networklist_tln.pl. La ejecución del programa es sencilla al presionar sobre el fichero rr.exe (Fig. 2.10.).

RegRipper, v.2.8	- 🗆 ×
<u>F</u> ile <u>H</u> elp	
Hive File:	Browse
Report File:	Browse
Profile:	
	~
	Rip It Close
Profile List Populated.	//

Fig. 2.10. Ejecución RegRipper sobre "rr.exe".

- Al seleccionar la opción Hive File \rightarrow muestra cuántos usuarios 1185 tiene la máquina, seguidamente se presentara automáticamente la opción SAM (permite que el hive que se desea se analice), y visualizará cuál va ser el Report File \rightarrow en la que asignará un nombre que puede ser INFORME DE USUARIOS (este generará un 1190 reporte) y Profile \rightarrow va a escoger el SAM y realizar un Rip It que crea un registro log y un .txt, este indicará todos los usuarios del computador, por ejemplo: el usuario administrador, fecha de creación, último login, última vez que se ha reseteado el password, última vez que ha fallado. Una política en Login Count nos verifica la cuenta deshabilitada, el usuario puede ser Normal y es lo mismo 1195 que se podrá obtener con el programa MiTeC Windows Registry Recovery - [SAM], pero en MíTeC, al ser en entorno gráfico, no permite ingresar dentro a su código fuente.
- 1200 Al realizar el análisis con el RegRipper se escoge un archivo clonado y se obtiene la información directamente en un fichero .bat.

En el RegRipper (Fig. 2.11.), al escoger SOFTWARE, se genera un archivo que se podrá denominar SW.txt, donde el plugin SOFTWARE se analizará en Rip-It, el cual tardará en ejecutar debido a que va a filtrarse por todos los plugins en modo texto, el mismo proceso se puede realizar en modo comando que se dispone de la utilidad RegRipper.



1210

Fig. 2.11. Informe de Software en el archivo SW.txt.

Por ejemplo, en la figura anterior (Fig. 2.12.), se describe la siguiente

información:

1215 Sun Mar 11 18:09:36 2018 (UTC)

Wireshark.exe - C:\Program Files\Wireshark\Wireshark.exe

Las líneas anteriores detallan de manera individual las fechas de instalación, path, claves del registro, entre otros, es decir, cuando se han creado y todos los cambios ocurridos por los plugins.

1220

Por otro lado, el siguiente registro "Microsoft\Windows\CurrentVersion\Installer\UserDat", describe el TemStant de aplicaciones: ¿Qué?, ¿Cuándo? -que programa y cuando se instaló-.

- 1225 "Classes\Installer\Products" describe los productos instalados, así como la cadena de desinstalación, y más información. El software que está montado en la máquina va a mostrar toda la información sobre el formato y tiempo que se instaló, se permitirá observar los datos con RegRipper y analizarlos. RegRipper funciona a manera de
- 1230 comandos, por lo tanto, se puede programar un script y proyectar a cualquier hora así se podrá usar un HIVE de una máquina local que esté encendida o una HIVE de una máquina clonada, por ejemplo: si se extraen los datos del sistema, se obtendrá: el tipo de sistema operativo, el directorio, las fechas, las carpetas, que procesador, que

1235 tipo de aplicaciones están instaladas en el siguiente registro "Microsoft\WindowsNT\CurrentVersion"

Regripper Aplicaciones Instaladas

Regripper – Timeline:

1240 Extrae un marco del tiempo fecha (Fig. 2.12.).

SW.txt: Bloc de not	as	022		×
Archivo Edición Fo	rmato Ver Ayuda			
Launching inst	aller v.20120917			
(Software) Det	ermines product install information			
Installer				
Microsoft\Wind	lows\CurrentVersion\Installer\UserData			
User SID: S-1-	5-18			
Key : 000	061091E00A0C000000000000F01FEC			
LastWrite: Sat	: Mar 3 17:06:53 2018			
20160614 - Mic	rosoft Office OSM MUI (Spanish) 2016 16.0.4266.1001 (Microsoft Co	rpora	tion)	
Key : 000	061096100000000000000000000000000000000			
LastWrite: Sat	: Mar 3 17:06:53 2018			
20180314 - Mic	rosoft Excel 2016 16.0.4266.1001 (Microsoft Corporation)			
Key : 000	061096100A0C000000000000000F01FEC			
LastWrite: Sat	Mar 3 17:06:53 2018			
20180314 - Mic	rosoft Excel MUI (Spanish) 2016 16.0.4266.1001 (Microsoft Corpora	tion)		
Key : 000	06109810000000000000000000F01FEC			
LastWrite: Sat	Mar 3 17:06:54 2018			
20180314 - Mic	rosoft PowerPoint 2016 16.0.4266.1001 (Microsoft Corporation)			
Key : 000	061098100A0C000000000000000F01FEC			
LastWrite: Sat	: Mar 3 17:06:54 2018			
20180314 - Mic	rosoft PowerPoint MUI (Spanish) 2016 16.0.4266.1001 (Microsoft Co	rpora	tion)	6
Key : 000	06109A20000000100000000F01FEC			
LastWrite: Sat	Mar 3 17:06:54 2018			
20180314 - Mic	rosoft Office 64-bit Components 2016 16.0.4266.1001 (Microsoft Com	rpora	tion)	

Fig. 2.12. Regripper – Timeline.

Regripper – Redes

1245 Describe las redes instaladas o configuradas en la máquina, el

Gateway y el IP, clave "Network key"

Regripper - USB

USBs, que se tienen instalados. Esto permite de una forma muyrápida obtener una información relativamente automatizada (Fig.

2.13.).

SW.txt: Blog	c de	notas — 🗆	×
Archivo Edici	ón	Formato Ver Ayuda	
RemovDev			
Microsoft	W/	indows Portable Devices\Devices	
LastWrite	T	ime Tue Mar 13 21:16:42 2018 (UTC)	
Device	:	DISK&VEN_&PROD_&REV_1.00	
LastWrite	:	Sat Mar 3 16:15:32 2018 (UTC)	
SN	:	6&8BC5DC8&0&&0	
Drive	:	JANETA-3D	
Device	:	DISK&VEN_ADATA&PROD_USB_FLASH_DRIVE&REV_0.00	
LastWrite	:	Sat Mar 3 16:15:32 2018 (UTC)	
SN	:	6&F475396&0&DAD53D9379C192&0	
Drive	:	F:\	
Device	:	DISK&VEN_ADATA&PROD_USB_FLASH_DRIVE&REV_1100	
LastWrite	:	Sat Mar 3 16:15:32 2018 (UTC)	
SN	2	262051931021015F&0	
Drive	:	ISABEL PROA	
Device	:	DISK&VEN_ADATA&PROD_USB_FLASH_DRIVE&REV_1100	
LastWrite	:	Sat Mar 3 16:15:32 2018 (UTC)	
SN	2	2680703301640013&0	
Drive	:	ADATA UFD	
Device	2	DISK&VEN_ADATA&PROD_USB_FLASH_DRIVE&REV_1100	
LastWrite	:	Sat Mar 3 16:15:32 2018 (UTC)	
SN	:	272111612004004E&0	
Drive	•	ADATA UFD	
Device		DISK&VEN_GENERAL&PROD_UDISK&REV_5.00	
LastWrite	:	Sat Mar 3 16:15:32 2018 (UTC)	
SN	:	1411141708347778962502&0	

Fig. 2.13. Regripper – USB.

1255 2.2.3. Bulk Extractor.

(http://digitalcorpora.org/downloads/bulk_extractor/); es la herramienta que va a permitir obtener una gran cantidad de artefactos de forma automatizada, además dispone de una serie de 1260 perfiles montados que permite extraer la información sin mayor conocimiento previo.

Bulk Extractor (Fig. 2.14.) permite, de una manera muy rápida, útil y práctica obtener: números de teléfono, números de tarjetas de 1265 crédito, dominios, correos. Esta sería la unidad y el programa.

🚽 Bulk E	xtractor v0.1.2		-	
assword:	Softpedia			Stopped
Extract to:				cropped
Status		Archive		

Fig. 2.14. Bulk Extractor.

Lo que va a permitir que se ejecute una máquina clonada y que

1270 se obtenga información de esta.

El comando que se utiliza es:

bulk_extractor –o

C:\Users\HIDALGO\Desktop\REGISTRO -e Facebook outlook -e wordlist

1275 C:\Users\HIDALGO\Desktop\REGISTRO\LinuxRedhatRelease.img

Se visualiza la extracción de la información y se procede a guardar en la carpeta REGISTRO; es decir extraer el Facebook, Outlook y lista de archivos de este fichero LinuxRedHatRelease.img (Fig. 2.15.).

1280



Fig. 2.15. Ejecución de una máquina clonada y obtención de información.

Al ubicarse sobre Inicio →Programas y al ejecutar el programa

1285 Bulk Extractor 1.5.5, seleccione la opción BEViewer with Bulk Extractor 1.5.5 (64 bit), visualizara la herramienta en sí en entorno gráfico. Al acceder a menú *Tools* y pulsar sobre la opción Runbulk_extractor; se presentará varias opciones y se escogerá Image File.

A continuacion se elegirá la información que se desea extraer: facebook, outlook, wordlist; además se podrá obtener archivos .gps, .gzip, ficheros de correo electronico, contraseña con Aes, ficheros de hibernación hiberfile, ficheros .rar, .pdf, .net, etiquetas de contactos vcard en caso de existir, base de datos en sqlite;
proporciona información automatizada y para finalizar se da clic sobre el botón Submit Run (Fig. 2.16.). La extracción de un archivo de tamaño 5 GB tarda aproximadamente 1 hora.
Required Parameters						Scanners
Scan: Image File File	Raw Devi	ce O	Directory	of Files		base 16
Image file	ile ILGO \Desktop \REGISTRO \LinuxRedHatRelease.img					Facebook
Output Feature Directory C	put Feature Directory C:\Users\HIDALGO\Desktop\REGISTRO					hashdb
General Ontions						🗹 outlook
Use Banner File						sceadan
Use Alert List File	-					wordlist
Use Stop List File	-					🗌 xor
Use Find Regex Text File						accts
Use Find Regex Text	-					🗹 aes
Use Random Sampling	-					☑ base64
	L					elf
Tuning Parameters			-			🖂 email
Use Context Window Size	•	16				exif
Use Page Size		167772	16			🗹 find
Use Margin Size		4194304	1			gps
Use Block Size		512				🗹 gzip
Use Number of Threads		4				✓ hiberfile
Use Maximum Recursion D	Depth	7				M httplogs
Use Wait Time		60				json
Darallelizing						🖂 kml
Use start processing at o	ffset		1			🗹 net
Use process range offset	01-02		_			🗹 pdf
Use add offset to reporte	ed featur	e offsets	_			🗹 rar
						🖂 sqlite
Debugging Options						vcard
Start on Page Number	0					windirs
Use Debug Mode Number	1					🗹 winlnk
Erase Output Directory						🖂 winpe
						>

Fig. 2.16. Run bulk_extractor sobre Image file.

Bulkextractor, retorna la carpeta REGISTRO que ha extraído con todos los archivos, describiendo fecha, tipo, tamaño y los archivos .txt, .pcap (Fig. 2.17.).

Nombre	Fecha de modificación	Tipo	Tamaño
alerts.txt	16/03/2018 04:26 p.m.	Documento de texto	715 KB
ccn.bxt	16/03/2018 04:27 p.m.	Documento de texto	514 KB
ccn_histogram.txt	16/03/2018 04:22 p.m.	Documento de texto	0 KE
ccn_track2.txt	16/03/2018 04:01 p.m.	Documento de texto	0 KE
ccn_track2_histogram.txt	16/03/2018 04:22 p.m.	Documento de texto	0 KE
domain.txt	16/03/2018 04:21 p.m.	Documento de texto	726 KE
domain_histogram.txt	16/03/2018 04:22 p.m.	Documento de texto	2 KE
elf.txt	16/03/2018 04:01 p.m.	Documento de texto	0 KE
email.txt	16/03/2018 04:26 p.m.	Documento de texto	29 KE
email_domain_histogram.txt	16/03/2018 04:22 p. m.	Documento de texto	1 KE
email_histogram.txt	16/03/2018 04:22 p.m.	Documento de texto	1 KE
ether.txt	16/03/2018 04:01 p.m.	Documento de texto	0 KE
ether_histogram.txt	16/03/2018 04:22 p.m.	Documento de texto	0 KI
exif.txt	16/03/2018 04:22 p.m.	Documento de texto	15 KE
facebook.txt	16/03/2018 04:28 p.m.	Documento de texto	8 KE
find.txt	16/03/2018 04:01 p.m.	Documento de texto	0 KE
find_histogram.txt	16/03/2018 04:22 p. m.	Documento de texto	0 KI
] gps.txt	16/03/2018 04:01 p.m.	Documento de texto	0 KI
httplogs.txt	16/03/2018 04:01 p.m.	Documento de texto	0 KI
ip.txt	16/03/2018 04:28 p. m.	Documento de texto	5 KI
ip_histogram.txt	16/03/2018 04:28 p. m.	Documento de texto	2 KI
jpeg_carved.txt	16/03/2018 04:22 p.m.	Documento de texto	35 KE

1310

Fig. 2.17. Extracción de información con Bulk Extractor.

Los números de teléfonos no se distinguirá fácilmente, pero se podrá detectar algún número o fax, el investigador forense informático, sabrá diferenciar ágilmente que está buscando. (Fig. 2.18.).

🗐 telephone.txt: Bloc o	le notas			1000		×
Archivo Edición For	mato Ver Ayuda					
542564253	Tel: +41 22 999 01	70 6 Gland, Su	iza(Tel: +41 22 999 0170,Fax: +41 22 99			^
542564275	Fax: +41 22 999 0	69 41 22 999	0170, Fax: +41 22 999 0169, E-mailx13 HYPER			
551275311Fax: 986	81 21 16 o: 986 1	81 21 00 Fax: 9	986 81 21 16\x0DE-mail:jitel05			
608895635	Tel: 2971310	Diaz Chap	arro.\x0ATel: 2971310\x94\x00\x00Confec\xElmaras\x0A			
608902596	Tel 4442120	Vicepresid	ente\x0ATel: 4442120p\xO0\x00Atender y sub			
608905028	Fax: 5658671	57649 - 50	501095\x0AFax: 5658671\0AFax: 5658671\x0A\xDD\xO0\x0	0Direcc	ixF3n	ge
608905178	Tel 5601095	anticorrupo	hxF3n\x0ATel 5601095, 5657649\x0Aleonpu			
608910808	Tel.: 596 0300	llo Social -	. \x0ATel.: 596 0300 - 566 3666 \x0Awe			
608911048tel: 33600	11 Roberto	Molano. tel: 3	360011 ext 1114.\x0A\x0ADeleg			
584985969-ZIP-395	67 701 70	11126	P PGUID b f 700 701 701 1126\x09 0\x09 0\x09 0\x09 0\x09 0\x09	0		
584985969-ZIP-397	55 701 70	1 1129	P PGUID b f 700 701 701 1129\x09 0\x09 0\x09 0\x09 0\x09 0\x09	0		
584985969-ZIP-406	95 701 70	1 1116	P PGUID b f 700 700 701 1116\x09 0\x09 0\x09 0\x09 0\x09 0\x09	0		
584985969-ZIP-409	83 700 70	1 1119	P PGUID b f 701 700 701 1119\x09 0\x09 0\x09 0\x09 0\x09 0\x09	0		
584999073-ZIP-270	167 603 60	3 2281	ftfi3 2281 "603 303 2281" mull_mull_			
684407137	Mobile 2800+	C AMD A	thlon XP Mobile 2800+ Socket A (Socket			
558770743-PDF-35	72 Fax: +3	4 91 369 70 3	1 +34 91 369 70 30Fax: +34 91 369 70 31www.trendmicro-e			
715113946Mobile 28	800+ CAME	Athlon XP Me	bile 2800+ Socket 754 SiS 7			~

Fig. 2.18. Extracción de información – números telefónicos con Bulk

Extractor.

La Fig. 2.19., refleja los correos electrónicos repetidos evidentemente, pero con la ayuda de un procesador de hojas de 1315 cálculo se podrá filtrar y organizar; es una forma de obtener información.

🧾 email.txt: E	Bloc de notas	<u></u> %		×
Archivo Edic	ión Formato Ver Ayuda			
345249473	ingo@mysql.com	/11/15 18:02:31 ingo@mysql.com +0 -0\x0D\x0A	Auto	~
345249561	ingo@mysql.com	/11/15 18:02:31 ingo@mysql.com +0 -0\x0D\x0A	Auto	
345249650	ingo@mysql.com	/11/15 18:02:31 ingo@mysql.com +0 -0\x0D\x0A	Auto	
345249749	ingo@mysql.com	/11/15 18:02:31 ingo@mysql.com +0 -0\x0D\x0A	Auto	
345249832	ingo@mysql.com	/11/15 18:01:30 ingo@mysql.com +1 -0\x0D\x0A1	Bug#14	
345250006	ingo@mysql.com	/11/15 18:01:26 ingo@mysql.com +1 -1\x0D\x0A	Bug#	
345250169	bell@sanja.is.com.ua	/11/15 18:14:53 bell@sanja.is.com.ua +2 -0\x0D\x	0A Test	£
345250330	bell@sanja.is.com.ua	/11/15 18:14:51 bell@sanja.is.com.ua +9 -0\x0D\x	0A Test	
345250447	bell@sanja.is.com.ua	/11/15 18:14:50 bell@sanja.is.com.ua +7 -0\x0D\x	0A Test	
345250330	bell@sanja.is.com.ua	/11/15 18:14:51 bell@sanja.is.com.ua +9 -0\x0D\x	0A Test	
345250549	ingo@mysql.com	/11/15 16:07:05 ingo@mysql.com +3 -0\x0D\x0A	Merge	
345250718	ingo@mysql.com	/11/15 16:07:02 ingo@mysql.com +3 -1\x0D\x0A	Bug#	
345250891	ingo@mysql.com	/11/15 16:07:02 ingo@mysql.com +1 -1\x0D\x0A	Bug#	
345251066	ingo@mysql.com	/11/15 16:07:01 ingo@mysql.com +1 -1\x0D\x0A	Bug#	
345251226	bar@mysql.com	/11/14 16:36:06 bar@mysql.com +4 -0\x0D\x0A	Bug#	
	• · · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · ·	-	

Fig. 2.19. Extracción de información de correos electrónicos con Bulk Extractor.

1320 Se podrá observar el contenido de los ficheros .ZIP - zip.txt, los dominios - domain.txt (Passport.net, usado en pornografía infantil kids.passport.net), registros - register.msnia.passport, adobe, sql, sai, IPs internas, las URL - url.txt (para lo cual se podría navegar por las url que se obtienen).

1325 2.2.4. La papelera

De la papelera (Fig. 2.20.) se van a distinguir varios conceptos.



Es un artefacto del que se puede obtener información, cuyo funcionamiento es sencillo. En el sistema de archivos donde se encuentra instalado el sistema operativo en la partición C:\>, se identifica una carpeta con el nombre \$Recycle.Bin.

- Esta carpeta representa el área de la Papelera de Reciclaje; es decir, el contenido de lo que se borra; se puede decir que es un área de almacenamiento donde se guardan archivos y carpetas previas a su eliminación definitiva.
- 1340 Cada vez que el usuario borra un archivo o tiene al menos un archivo en su papelera de reciclaje, por ejemplo, C:\\$Recycle.Bin se crea una carpeta con el SID del usuario. El SID de usuario es el identificador que le pone Windows a un usuario; es decir, si tenemos el usuario Iván, la nomenclatura va a iniciar como S-1-5-21 y una serie de números

 NUM, si el NUM es 500 significa que es Administrador y si es 1000 es Usuario Normal. En otras palabras, si 2 usuarios del sistema tuvieran archivos en su papelera de reciclaje, la carpeta \$Recycle.Bin tendría 2 carpetas del estilo S-1-5-21 (Fig. 2.21.).



Fig. 2.21. Papelera de Reciclaje de la carpeta \$Recycle.Bin.

En el interior de la carpeta de cada usuario se encontrarán
2 tipos de archivos: los que inician por \$I y \$R.

1355

1360

 Los que inician con \$I contienen la ruta original del archivo y algunos datos propios del fichero, mientras, los que inician con \$R incluyen en el interior el contenido del archivo original (Fig. 2.22.). Cuando se vacía la Papelera de Reciclaje, y se eliminan los \$I y \$R; no se borran en su totalidad, sino que se marcan como eliminados y luego se pueden recuperar con una herramienta forense informática de recuperación.



Fig. 2.22. Papelera de Reciclaje con los \$I y \$R.

Los archivos eliminados se pueden recuperar con la siguiente herramienta forense, **RECUVA** que se puede descargar en el siguiente enlace: <u>https://www.piriform.com/recuva</u>.

1370 2.2.5. RecoverMyFiles

Es una herramienta con licencia propia con un costo módico y se puede descargar en el siguiente enlace: <u>http://www.recovermyfiles.com/es/</u>, tiene un alto grado de recuperación de información, es robusto y dispone de las siguientes

1375 características:

- Recupera discos duros formateados incluso si ha reinstalado el sistema operativo Windows.
- Recupera sus archivos después de un fallo físico del disco duro.

- Recupera los archivos de un error al realizar una partición.
- 1380 Recupera documentos, fotos, video, música y correos electrónicos.
 - Recupera datos de un disco duro, una tarjeta de cámara, un medio de almacenamiento usb, una unidad Zip flexible o cualquier otro medio (Sánchez Cordero, Análisis Forense Informático, 2015).

1390

Al aplicar la herramienta se recuperan las evidencias de una forma estructurada, si se requiere archivos .gif, páginas html, .mov; muestra el contenido organizado y categorizado, es decir, se obtienen los metadatos (Fig. 2.23.).



Fig. 2.23. RecoverMyFiles.

Se pueden encontrar una variedad de herramientas, según las utilidades que se requieran, en el siguiente enlace:

1395 www.conexioninversa.blogspot.com.es/2013/09/forensicspowertools-listado-de.html

2.2.6. Prefetch

Es un artefacto que permite conocer en un momento 1400 determinado cuantas veces el ordenador ha ejecutado un programa (Pato Rodríguez , 2006), por ejemplo: permite obtener información de una aplicación conociendo si se encontraba instalada en la máquina y las veces que fue utilizada. Entonces el *Prefetch* es un artefacto desde Windows Xp, hasta Windows 7 se llama Prefetch y 1405 a partir de Windows 7 se llama SuperPrefetch, la cual admite registrar la información que se encuentra en la máquina o cuando un usuario ejecuta las aplicaciones; significa, si se ejecuta Excel automáticamente la aplicación del sistema operativo va a ejecutar la aplicación y obtener los elementos que más utiliza y los va a registrar.

1410

Para ejecutar esta herramienta se dirigen a la siguiente ubicación del disco duro C:\Windows\Prefetch y se sitúan sobre el fichero archivos .pf; de tal manera que se observarán en el equipo las aplicaciones más utilizadas con un detalle importante de las mismas
1415 (Fig. 2.24.); es decir, en un apartado del sistema operativo existe un directorio donde se almacenan todas las aplicaciones registradas que se utilizan en el sistema, estas aplicaciones son susceptibles de ser observadas ante un peritaje o un análisis forense.

Nombre ~	Fecha de modificación	Тіро	Tamaño
ReadyBoot	11/03/2018 12:00 a.m.	Carpeta de archivos	
7ZG.EXE-F49B3D46.pf	12/03/2018 10:44 a.m.	Archivo PF	9 K
ACRORD32.EXE-F7519AA2.pf	13/03/2018 11:08 p.m.	Archivo PF	33 K
ACTIVEHEALTH.EXE-4DD7F4F4.pf	14/03/2018 04:04 p.m.	Archivo PF	30 K
ADDINUTIL.EXE-38D7B022.pf	14/03/2018 05:48 p. m.	Archivo PF	15 K
ADOBEARM.EXE-F9223367.pf	13/03/2018 11:08 p.m.	Archivo PF	7 K
AgAppLaunch.db	03/03/2018 11:16 a.m.	Data Base File	327 K
AgCx_SC1.db	14/03/2018 09:02 p.m.	Data Base File	239 K
AgCx_SC1.db.trx	14/03/2018 09:01 p.m.	Archivo TRX	208
AgCx_SC2.db	13/03/2018 03:19 p.m.	Data Base File	187 1
AgCx_SC5.db	14/03/2018 04:02 p.m.	Data Base File	2561
AgGIFaultHistory.db	14/03/2018 09:06 p.m.	Data Base File	732 1
AgGIFgAppHistory.db	14/03/2018 09:06 p.m.	Data Base File	1,523
AgGIGlobalHistory.db	14/03/2018 09:06 p.m.	Data Base File	2,850 1
AgGIUAD_P_S-1-5-21-1731920651-1631437389-121688643-1001.db	14/03/2018 05:52 p.m.	Data Base File	158 1
AgGIUAD_S-1-5-21-1731920651-1631437389-121688643-1001.db	14/03/2018 05:52 p.m.	Data Base File	1,260 1
AgRobust.db	14/03/2018 09:06 p.m.	Data Base File	637 8
APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf	14/03/2018 04:35 p.m.	Archivo PF	151
ATBROKER.EXE-5CD29207.pf	13/03/2018 11:27 p. m.	Archivo PF	10 1
AUDIODG.EXE-AB22E9A6.pf	14/03/2018 04:36 p.m.	Archivo PF	111
AVIRA.SYSTRAY.EXE-C50E5413.pf	14/03/2018 04:02 p.m.	Archivo PF	31 1

Fig. 2.24. Registros HIVE del Prefetch.

En la Fig. 2.25., se detalla el equipo con todas las aplicaciones que se han abierto y utilizado con su respectiva información de uso así como la ubicación del directorio en el sistema operativo.

→ ★ ↑ Ste equipo > WINDOWS (C:) > Windows > Prefetch					
Nombre	~	Fecha de modificación	Тіро	Tamaño	
ReadyBoot		11/03/2018 12:00 a.m.	Carpeta de archivos		
7ZG.EXE-F49B3D46.pf		12/03/2018 10:44 a.m.	Archivo PF	9 KB	
ACRORD32.EXE-F7519AA2.pf		13/03/2018 11:08 p. m.	Archivo PF	33 KB	
ACTIVEHEALTH.EXE-4DD7F4F4.pf		14/03/2018 04:04 p.m.	Archivo PF	30 KB	
ADDINUTIL.EXE-38D7B022.pf		14/03/2018 05:48 p.m.	Archivo PF	15 KB	
ADOBEARM.EXE-F9223367.pf		13/03/2018 11:08 p.m.	Archivo PF	7 KB	

Fig. 2.25. Archivo Prefetch.

El Prefetch es una de las herramientas que permite conocer cuando una aplicación se encuentra instalada y las veces que ha sido 1430 ejecutado un determinado programa en el ordenador (Sánchez Cordero, Conexión Inversa, 2014).

El Prefetch es una de las herramienta como Windows Prefetch que están diseñadas para acelerar el proceso de inicio de la 1435 aplicación; de esta manera se puede mencionar que:

- Contienen el nombre del ejecutable, una lista Unicode de archivos DLL utilizados por dicho ejecutable, un recuento de las veces que el ejecutable se ha ejecutado, y una marca de tiempo que indica la última vez que se ejecutó el programa.
- Hasta 128 archivos Prefetch se almacenan en el % SystemRoot% \
 Prefetch. Cada archivo en ese directorio debe contener el

nombre de la aplicación, un guion y luego un hash de ocho caracteres de la ubicación desde la que se ejecuta la aplicación, y una extensión .pf

Si una aplicación se ejecuta desde dos lugares diferentes en el disco duro (es decir, que el usuario ejecute C: \ md5deep.exe y
 C: \ APPS \ Hashing \ md5deep.exe), obtendrán dos archivos Prefetch diferentes en la carpeta Prefetch.

1450 2.2.7. Winprefetchview

Es una herramienta muy útil:

(http://www.nirsoft.net/utils/win prefetch view.html), cómoda, sencilla, y se suele emplear en problemas de propiedad intelectual. No necesita de instalación, es un ejecutable; se abre 1455 automáticamente el Prefetch, por ejemplo: si se contrata el servicio de peritaje o un análisis forense de un ordenador donde se ha instalado el Autocad con la licencia en regla, por tanto el problema es si una máquina tenía instalado un software, lo más fácil es ir al Panel de Control y examinar, o buscar evidencias en el disco duro, 1460 como puede ser, un archivo de Autocad o el nombre del ejecutable; pero, lo sería elegir el Prefetch abrir y automáticamente, ha extraído todo la información del Prefetch en la aplicación. En la parte superior izquierda se ilustra una columna con el nombre del archivo marcado con la extensión .7zip, .pf, al seleccionarlo en la parte

1465 inferior mostrará una variedad de ficheros que son las librerías y ejecutables que están registrados en esta aplicación; es decir, todos estos ficheros se encuentran registrados dentro del Prefetch, lo que significa que cuando se ejecutó la primera vez un Windows, la instalación es lenta, en Windows 7 y Windows 8. En el proceso de
1470 instalación se ilustra el siguiente mensaje "instalando programas"; es decir lo que se está realizando es creando el Prefetch, cuando arranca la máquina y se torna sumamente rápido ejecutando programas

como Excel, Power Point o cualquier utilidad de manera eficaz, esto es debido al Prefetch o SuperPrefetch.

1475

1480

Lo importante es saber si se cargó el directorio; ya que la máquina va a reducir su funcionamiento (lenta) y se puede confundir que tiene algún tipo de virus o troyano. Por lo tanto, se ven directorios llenos de .pf y si se los borra empieza a degradarse la ejecución de la máquina, porque el sistema operativo intentará

volver a crear un sistema de Prefetch, la solución es no borrar los archivos .pf.

En el caso de que un usuario ingrese a la máquina y borre, se
1485 verán diferentes técnicas sobre la ejecución del programa, por ejemplo: Autocad se indica que en reemplazo de *7zip*, aparecerá el *Autocad*, al igual que la fecha que se instaló el programa, la fecha de modificación (la última vez que se ejecutó), el tamaño, proceso, Patch, porque se imagina que ocultando el nombre el usuario
1490 infiltrado no lo encontrará, el Prefetch expresará donde exactamente se encuentra la utilidad. Es importante la columna *Run Counter* porque indica las veces que se ha ejecutado el programa.

En el caso de que se elimine el programa, se puede encontrar en el Prefetch, por lo tanto, es una herramienta muy útil a la hora de buscar un elemento de estas características que se indicarán en la parte derecha (Fig. 2.26.) de la última vez que se ejecutó. En un caso dado que manifieste que el Autocad no se instaló o ejecutó; la

herramienta proporcionará información sobre si el programa se 1500 encontraba en el ordenador.

En la tercera posición se encuentra la columna *Filename* que es un fichero temporal, que se puede confundir con un malware, troyano, que además posee en las propiedades un tamaño pequeño y que se ejecuta varias veces, es importante investigar previamente ya que nos referimos al Prefetch que, en combinación con otras herramientas, permite la resolución de temas de propiedad intelectual (Fig. 2.26.).

Eile Edit View Options	delp							
× 🖬 🖻 🗞 📽 🖏 🤻								
Filename /		Created Time	Modified Time	File Size	Process EXE	Process Path	Ru	Last Run Time
72 72G.EXE-F4983D46.pf		12/03/2018 10:41:19 a.m.	12/03/2018 10:44:47 a.m.	8,547	7ZG.EXE	C\PROGRAM FILES\7-Zip\7zG.exe	3	12/03/2018 10:44:47 a.m., 12/03/2018 10:41:40 a.m., 12/03/20
ACRORD32.EXE-F7519AA2.p	1	03/03/2018 12:05:58 p.m.	13/03/2018 11:08:33 p. m.	33,036	ACRORD32.EXE	C:\PROGRAM FILES (X86)\Adobe\ACRO8	29	13/03/2018 11:08:22 p. m., 13/03/2018 05:29:08 p. m., 13/03/20
ACTIVEHEALTHLEXE-4DD7F4	IF4.pf	13/03/2018 08:38:17 p.m.	14/03/2018 04:04:18 p. m.	30,263	ACTIVEHEALTH.EXE	C:\PROGRAM FILES (X86)\HEWLETT-PAC	2	14/03/2018 04:03:55 p. m., 13/03/2018 08:38:07 p. m.
ADDINUTILEXE-38D7B022.p	f.	14/03/2018 04:28:37 p.m.	14/03/2018 05:48:56 p.m.	14,825	ADDINUTILEXE	C:\Windows\MICROSOFT.NET\FRAMEW	10	14/03/2018 05:48:56 p. m., 14/03/2018 05:48:55 p. m., 14/03/20
ADOBEARM.EXE-F9223367.p	f	13/03/2018 11:08:57 p.m.	13/03/2018 11:08:57 p.m.	6,539	ADOBEARM.EXE	C:\PROGRAM FILES (X86)\COMMON FIL	1	13/03/2018 11:08:57 p. m.
E APPLICATIONFRAMEHOSTJ	EXE-BCE9A1EE.pf	06/03/2018 06:08:44 p. m.	14/03/2018 04:35:14 p. m.	14,949	APPLICATIONFRA	C:\Windows\System32\APPLICATIONFR	13	14/03/2018 04:35:04 p. m., 14/03/2018 08:36:08 a. m., 12/03/20
ATBROKER.EXE-5CD29207.pt	E.	12/03/2018 10:46:50 a.m.	13/03/2018 11:27:44 p. m.	9,487	ATBROKER.EXE	C:\Windows\System32\AtBroker.exe	27	13/03/2018 11:27:43 p. m., 13/03/2018 08:03:52 p. m., 13/03/20
AUDIODG.EXE-A822E9A6.pf		13/03/2018 03:23:23 p. m.	14/03/2018 04:36:49 p. m.	11,052	AUDIODG.EXE	Ci\Windows\System32\audiodg.exe	6	14/03/2018 04:36:39 p. m., 14/03/2018 04:08:20 p. m., 14/03/20
AVIRA.SYSTRAY.EXE-C50E54	13.pf	14/03/2018 08:20:06 a.m.	14/03/2018 04:02:30 p. m.	31,341	AVIRA.SYSTRAY.EXE	C:\PRDGRAM FILES (X86)\Avira\Launche	2	14/03/2018 04:02:20 p. m, 14/03/2018 08:19:56 a. m.
AVIRA.SYSTRAYSTARTTRIGG	ER.EXE-1721E2F	14/03/2018 08:19:22 a.m.	14/03/2018 04:01:48 p. m.	6,215	AVIRA.SYSTRAYST	C:\PROGRAM FILES (X86)\Avira\Launche	2	14/03/2018 04:01:38 p. m., 14/03/2018 08:19:12 a. m.
AVUPDATE.EXE-FF796A51.pf		13/03/2018 08:05:06 p.m.	14/03/2018 09:32:41 p. m.	8,776	AVUPDATE.EXE	C:\rei\AV\avupdate.exe	2	14/03/2018 09:32:41 p. m., 13/03/2018 08:05:00 p. m.
BACKGROUNDTASKHOST E	E-478EA968.pf	13/03/2018 11:51:26 a.m.	13/03/2018 03:17:58 p. m.	9,848	BACKGROUNDTAS	C:\Windows\System32\BACKGROUNDTA	2	13/03/2018 03:17:47 p. m., 13/03/2018 11:51:18 a. m.
BACKGROUNDTASKHOST E	E-A4828DE4.pf	03/03/2018 04:24:35 p.m.	14/03/2018 04:36:46 p.m.	17,357	BACKGROUNDTAS	C:\Windows\System32\BACKGROUNDTA	87	14/03/2018 04:36:36 p. m, 14/03/2018 04:01:12 p. m, 14/03/20
BROWSER_BROKER.EXE-EEC	8D935.pf	13/03/2018 11:10:37 p.m.	13/03/2018 11:10:37 p.m.	7,429	BROWSER_BROKE	C:\Windows\System32\BROWSER_BROK	1	13/03/2018 11:10:32 p. m.
BTSERVER.EXE-EF30FDB9.pf		14/03/2018 08:19:02 a.m.	14/03/2018 04:01:28 p. m.	13,768	BTSERVER.EXE	C:\PROGRAM FILES (X86)\Realtek\REALT	2	14/03/2018 04:01:16 p. m., 14/03/2018 08:18:52 a. m.
BUBBLES.SCR-6885EE86.pf		07/03/2018 10:09:34 p. m.	13/03/2018 07:24:01 a.m.	9,013	BUBBLES.SCR	C:\Windows\System32\Bubbles.scr	13	13/03/2018 07:23:58 a.m., 11/03/2018 07:38:12 p.m., 11/03/20
BULK EXTRACTOR32.EXE-05	7BD3F8.pf	13/03/2018 08:49:05 p.m.	13/03/2018 08:49:05 p. m.	4.978	BULK EXTRACTOR	CI/USERS/HIDALGO/DESKTOP/NUEVA C	1	13/03/2018 08:49:05 e. m.
Filename	Full Path		Device Pat	ы X				Index
CLIET	CALIFORNIA		TVACUALA MOLINACI	014164207	7.4705 - 0.4724-555 58.6	T.		45
27.041	CARROCRAM	COULD CARTON COULD INC IN	MOLDER MOLDING	014164307	24285-04724-560 000	CD A&A ER ED. 7. 700 77 PUL		21
TTC EVE	CARROGRAM	ELES 7- Zip 7-G eve	SUCHIME	014164297	2+7285+-0+73/+560 PP/	ICE AM EN ES 7. 200 72/0 EVE		4
ELASTACTIVITYVEW 77	CALIFERDAIDA	CONDESCIORU ASTACTIN	TVMEW 77 WOLLINGE	014164207	74785+ 0+734+5601108	PS HIDALGO DESKTOPLASTACTIVATIVAEW 7	7	0
ASTACTAUTIVERI CEG	CALIFERSHID	CONDESCIORU ASTACTIN	TVAENALA MOLUME	014164207	2+225> 0+728>5601105	PO HIDALGO DESKTOP LOGTACTIVITYUEAN	ACTA/	TAITAIN AT
ASTACTIVITY/JEW CHM	CAUSERSWIDA	U GOLDESKTOPU ASTACTIV	TYVEWIA WOULDED	014164207	2#205a-0#732a560116E	PS/MIDALGO/DESKTOP/LASTACTIVITY//PAN/	ACTAC	TWITWIEW 44
A STACTIVITY/JEW EVE	CAUSERSHIDA	LIGOLDESKTOP LIASTACTIN	TYMEWIA WOULD	014164307	24/285a-0473/45601108	PS/HIDALGO/DESKTOP/LASTACTIVITY/JEAAL	ASTAC	TAITWIEW AR
PEADAGE TYT	CALISERS HID	I GOI DESCTORU ASTACTIN	TWAENARE WOLDING	014164207	24/205+ 04/24+5601102	E TYT 46		
SYSMAIN SDR	CiWindowsia	annat/h\susmain sdh	VVOLUME	014164397	2ad285a-9e734a560 Will	IDOWS APPRATCH SYSMAIN SDR		55
STATICCACHE.DAT	C\Windows\Fe	ants/STATICCACHE.DAT	VVOLUME:	01d16d397	2#285a-9+734+561.WIR	DOWS/FONTS/STATICCACHE.DAT		36
SORTOFFAULT NLS	C/Windows\G	ORALIZATION Section SO	RTDEFAULT WOLUME	014164397	2#255a-9#734a565.W/h	DOWS GLOBALIZATION SORTING SORTDER	URTN	15 35
ADVAPR2 DI I	C-Windows S	stem2/aduani22 dll	VOLUME	01/16/397	2ad285a-9e734a568.With	IDOWS/SYSTEMR2/ADVARIA2 DI L		22
APPINE P DI I	C/Windows/S	atem 27 annhein dil	VOI UME	014164397	2#225a-0#734a560 Will	IDOWS/SYSTEM12/ APPHELP DLL		54
53 Files 1 Selected		NirSoft Freeware.	http://www.nirsoft.net					

1505

Fig. 2.26. Herramienta WinPrefetchView.

En Windows, por defecto cuando un usuario externo coloca un pendrive no se conoce que se copió o revisó, a excepción que este activado el sistema de auditoría (Windows desde sus versiones

1515 más antiguas; desde Windows Xp dispone de un sistema de auditoría que permite verificar tanto las aplicaciones como la seguridad, a la vez presenta diferentes escenarios como la ejecución de programas, borrado de ficheros, etc.).

1520 Ventajas:

En un entorno empresarial, se recomienda activar el sistema de auditoría, y luego se puede mejorar; es decir, que el sistema de auditoría en un principio va a estar instalado en la máquina, y cuando se tiene una incidencia es uno de los primeros registros que normalmente se suele mirar; pero puede ocurrir que se presente un caso en el que los logs se empiezan a llenar, porque la actividad de usuario es muy amplia, esta situación se podría mejorar ya que es un sistema de log centralizado, en donde los productos que se escriben son registros en el log y automáticamente se están escribiendo en el 1530 servidor. Se permite que el usuario en el caso que borre los registros, automáticamente se obtendrá la evidencia en el servidor, el usuario conseguirá la información referente a lo que ha realizado, permitiendo tener un respaldo ante posibles incidentes; para los registros HIVE y los artefactos, el log es muy importante, por

ejemplo: si un gerente de una empresa se cambia a otra empresa, automáticamente lo que haría es llevarse toda la información de la misma directamente en un pendrive.

1540

1535

Por lo tanto, se va a "saber" que, con una combinación entre el registro de Windows, el log y una serie de programas, si un usuario se ha llevado información en una USB, Windows no registra lo que se copia a un dispositivo externo, es decir si Byron realiza una copia 1545 al pendrive, Windows solamente registrará el ingreso del pendrive; si además se tiene activada la auditoría se conocerá la fecha, hora y el tipo de dispositivo en el que Byron realizó la copia.

2.2.8. USBDeview

1550 USBDeview, extrae toda una estadística de los discos duros externos, pendrive o sistemas de almacenamiento, que se han insertado en la máquina desde que Windows fue instalado por primera vez en el computador, no desde que una sesión fue iniciada (Sofer, 2001) (Fig. 2.27.).

\leftarrow \rightarrow \checkmark \uparrow \square << Disco local (C:) \rightarrow Windows	> System32	v ひ Buscar en System	132	P
Nombre	Y Fecha de modificación	Тіро	Tamaño	^
Windows.Devices.SerialCommunication.dll	18/3/2017 15:58	Extensión de la aplicación	164 KB	
Windows.Devices.SmartCards.dll	18/3/2017 15:57	Extensión de la aplicación	901 KB	
Windows.Devices.SmartCards.Phone.dll	18/3/2017 15:58	Extensión de la aplicación	416 KB	
Windows.Devices.Usb.dll	18/3/2017 15:58	Extensión de la aplicación	417 KB	
Windows.Devices.WiFi.dll	18/3/2017 15:58	Extensión de la aplicación	187 KB	
Windows.Devices.WiFiDirect.dll	18/3/2017 15:58	Extensión de la aplicación	483 KB	
Windows.Energy.dll	18/3/2017 15:58	Extensión de la aplicación	191 KB	~

1555

Fig. 2.27. Información USB.

USBDeview combinado con el visor de eventos de Windows, es propicio porque se puede obtener un timeline completo de lo que 1560 se está buscando, pero si solamente se tiene esta información y no el registro de Windows, el visor de eventos va a extraer el dispositivo que es útil porque muestra suficiente información (Fig. 2.28.).

Se puede descargar la desde:

http://nirsoft.net/utils/usb_devices_view.html y no necesita 1565 instalación.

USBDeview										-	0)	×
File Edit View Option	s <u>H</u> elp											
X 🎯 🔹 🔹 [- C - C - C - A											
Device Name /	Description	Device Type	Connected	Safe To Unpl	Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Unplug	VendorlD	^
0000.0014.0000.002.00	USB Input Device	HID (Human Interface D	No	Yes	No	No			20/7/2018 8:37:08	20/7/2018 8:37:08	0458	
@ 0000.0014.0000.002.00	USB Input Device	HID (Human Interface D	No	Yes	No	No			20/7/2018 8:37:08	20/7/2018 8:37:08	0458	
@ 0000.0014.0000.002.00	USB Input Device	HID (Human Interface D	No	Yes	No	No			20/7/2018 8:37:08	20/7/2018 8:37:08	0458	
0000.0014.0000.003.00	USB Video Device	Video	Yes	Yes	No	No			26/7/2018 11:16:41	11/6/2018 8:07:55	04/2	
@ 0000.0014.0000.003.00	USB Video Device	Video	No	Yes	No	No			23/7/2018 6:31:27	23/7/2018 6:31:27	1bcf	
© 0000.0014.0000.006.00	USB Input Device	HID (Human Interface D	No	Yes	No	No			24/7/2018 14:26:10	24/7/2018 14:26:10	045e	
@ 0000.0014.0000.006.00	USB Input Device	HID (Human Interface D	No	Yes	No	No			24/7/2018 14:26:10	24/7/2018 14:26:10	045e	
@ 0000.0014.0000.006.00	USB Input Device	HID (Human Interface D	No	Yes	No	No			24/7/2018 14:26:10	24/7/2018 14:26:10	045e	
© 0000.0014.0000.006.00	SM-J200M	Unknown	No	Yes	No	No			25/7/2018 22:04:43	20/7/2018 13:12:20	04e8	
@ 0000.0014.0000.006.00	Dispositivo serie USB	Communication	No	Yes	No	No	COM3		25/7/2018 22:04:43	20/7/2018 13:12:07	04e8	
© 0000.0014.0000.006.00	ADB Device	Vendor Specific	No	No	No	No			25/7/2018 22:04:39	20/7/2018 13:12:06	04e8	
Microsoft® Nano Tra	USB Composite Device	Unknown	Yes	Yes	No	No			25/7/2018 14:20:21	11/6/2018 8:02:55	045e	
Microsoft® Nano Tra	USB Input Device	HID (Human Interface D	Ves	Yes	No	No			25/7/2018 14:20:22	25/7/2018 14:20:22	045e	
Microsoft® Nano Tra	USB Input Device	HID (Human Interface D	Yes	Yes	No	No			25/7/2018 14:20:22	25/7/2018 14:20:22	045e	
Microsoft® Nano Tra	USB Input Device	HID (Human Interface D	Yes	Yes	No	No			25/7/2018 14:20:22	25/7/2018 14:20:22	045e	
@ Port #0001.Hub #0001	Sony Storage Media USB Device	Mass Storage	No	Yes	No	No		4C070D428452863	11/7/2018 11:21:18	11/7/2018 9:39:07	054c	

Fig. 2.28. USBDeview combinado con el visor de eventos de Windows.

Al analizar la información de la última vez que se introdujo el
1570 USB al PC, el atributo *VendorID* muestra en *Driver Description* y la *Instance ID*, toda la información que se puede ubicar en un informe, por ejemplo: si se tuviera el registro de Windows, el visor de eventos se podría ubicar con las fechas, si los atributos *Create Date* y el *Last Plug/Unplug* coinciden, esto asegura que existió una copia, aunque no se pueda garantizar que fue lo que se copió.

Existe una serie de comandos que van a permitir al USBDeview, buscar de forma remota la información de los dispositivos conectados en el equipo (Tabla 1.2.).

Tabla 2.2. Opción línea de comandos para Habilitar/Deshabilitar/Eliminar dispositivos USBs.

Comandos para Habilitar/Deshabilitar/Eliminar para USB

- /disable {\\RemoteComputer} <Device Name>
- /disable_by_serial {\\RemoteComputer} <Device Name>
- /disable_by_drive {\\RemoteComputer} < Device Name>
- /disable_by_class {\\RemoteComputer} < USB Class;USB SubClass;USB Protocol>
- /disable_by_pid {\\RemoteComputer} <\VendorID;ProductID>
- /disable_all {\\RemoteComputer}
- /enable {\\RemoteComputer} <Device Name>
- /enable_by_serial {\\RemoteComputer} <Device Name>
- /enable_by_drive {\\RemoteComputer} <Device Name>
- /enable_by_class {\\RemoteComputer} <USB Class;USB SubClass;USB Protocol>
- /enable_by_pid {\\RemoteComputer} <\VendorID;ProductID>
- /enable_all {\\RemoteComputer}
- /disable_enable {\\RemoteComputer} <Device Name>
- /disable_enable_by_serial {\\RemoteComputer} <Device Name>
- /disable_enable_by_drive {\\RemoteComputer} <Device Name>
- /disable_enable_by_class {\\RemoteComputer} <USB Class;USB SubClass;USB Protocol>
- /disable_enable_by_pid {\\RemoteComputer} <\VendorID;ProductID>
- /disable_enable_all {\\RemoteComputer}
- /remove {\\RemoteComputer} < Device Name>
- /remove_by_serial {\\RemoteComputer} < Device Name>
- /remove_by_drive {\\RemoteComputer} <Device Name>
- /remove_by_class {\\RemoteComputer} <USB Class;USB SubClass;USB Protocol>
- /remove_by_pid {\\RemoteComputer} <\VendorID;ProductID>
- /remove_all {\\RemoteComputer}
- /remove_all_connected Quita todos los dispositivos USB conectados.
- /remove_all_disconnected Retirar todos los dispositivos USB desconectados.
- 1585
- *Fuente:* <u>http://nirsoft.net/utils/usb_devices_view.html</u>

Conectar a un fichero SYSTEM de forma externa

• USBDeview.exe /regfile "c:\hives\SYSTEM"

Si se ubica USBDeview en el fichero SYSTEM va a devolver 1590 de una máquina clonada que dispositivos tenía conectados, lo que realiza, es cambiar las rutas porque no va a coincidir.

> Al ejecutar la consola cmd, como usuario Administrador, se obtiene automáticamente de la máquina que dispositivos se encontraban conectados (Fig. 2.29.).

I- CI/User	s\HIDALGO\Desktop\FORE	INSICS												~ 0	Buscar er	- P
Nombre	Fecha de modificación	Tipo	0 4 .0	Tamaño												
USBDeview.ene	04/03/2018 01:03 p.m.	Aplicación		180 KB												
WFA.exe	06/05/2016 08:02 p.m.	Aplicación		2,930 KB												
MinPrefetchView.exe	12/01/2016 11:23 a.m.	Aplicación		110 KB												
SYSTEM	10/03/2018 11:52 p.m.	Archivo		26,112 KB												
USEDeview da	23/03/2018 01:51 e.m.	Archive CEG		2 8/8												
Malamantar Lalamanta	alaccinanda 15 5 8 40															63
				10 K. 10 M 10								_	_			-
The second se				- PI - U	And the second sec											
Administradoc Simbolo de	d sistema				+ itikCerne										-	0
Administradoc Simbolo de	il sistema		-	X	the late late of the	- 59										0
Administradee Simbole de \Usens\HIDALGO\Desk	l sistema top\FORENSICS>USBD	eview.exe /r	regfile "C:\User	rs\HIDALGO\	A Difference										ē.	0
Administradee Simbole de \Users\HIDALGO\Desk sktop\FORENSICS\SYS	l pidema top\FORENSICS>USBD TÉM®	eview.exe /r	regfile "C:\User	rs\HIDALGO\	€ tildbene Jie jat yne gyte X Q ● ● ● Deca here	n 5% ⊒356204	Device Loss	Convected	latina.	Dutied	1994	Dividate	Josef Namber	Control Dates	Lat Pro Unive	
Administradoc Simbolo de \Users\HIDALGO\Desk sktop\FORENSICS\SYS	l potema top\FORENSICS>USBD TEM*	≥view.exe /r	regfile "C:\User	S/HIDALGO/	tillCoune (n går ynn gefer XQ ♦ ● ● Dougstang	~ 59 월급 15 년 10 4 Decement	Decker Type	Canvected	lating	Dubid	1244	Divi Lette	Southerte	Contribut	Lat Pro Dalve	. 100
Administrador Simbola de \Users\HIDALGO\Desk sktop\FORENSICS\SYS \Users\HIDALGO\Desk	I USEEMA top\FORENSICS>USBD TEM* top\FORENSICS>	≫view.exe /r	regfile "C:\User	rs/HIDALGO/	titlevene titlevene title (de Vene Option X @ • • • • • • • • • • • • • • • •	n (59) ⊒ 3 % 2 Q 4 Decaytor Converting	Device Type RCD Startes Machine C.	Convected Too	Sectoray No.	Dubid	127-14	Divi Lette	Join/Turnle	Created Dates	Lat Pug Urging 2000 C C C C C	0 100
Administrator Simbold de \Users\HIDALGO\Desk sktop\FORENSICS\SYS \Users\HIDALGO\Desk	l Unterna top\FORENSICS>USBD TEM" top\FORENSICS>	Deview.exe ∕r	regfile "C:\User	rs/HIDALGO/	the Contract of the Contr	n gra Deciptor College Coll College College College College College College College College	Device Type 102 Starrey Models 2 102 Flance Harfwell, 102 Flance Harfwell,	Carried and Tax	Sections In The	Dutied No. No.	1244	Division	Seaffunde	Cranat Date Sciciliti A Local Sciciliti A Local Sciciliti A Local Sciciliti A Local	Lat Phy Diphy. 2000 Billion 2010 Billion 2010 Billion 2010 Billion	0 NO NU NU
Administradec Simbele de LUSers\HIDALGO\Desk sktop\FORENSICS\SYS LUSers\HIDALGO\Desk	d Disterna top\FORENSICS>USBD TEM" top\FORENSICS>	eview.exe /r	regfile "C:\User	□ × rs\HIDALGO\ A	Intervene Fill [All Year Option No. Option Device Name Intervene Intervene <	n (219) Decaytors Decaytors CER Page Decise CER Page Decise CER Page Decise CER Page Decise CER Page Decise	Derice Type NG Overset Hocker D. NG Planas Hocker D. NG Planas Hocker D. Nder	Canneched Na Na Na Na	Sele Torringe Tel Tel Tel Tel Tel Tel Tel Tel Tel Te	Dutied No. No. No.	157 mail Tas Tas Tas	Divi Litte	Selafikande	Control Day Detroited Advice 2011/2014 Advice 2011/2014 Advice Advice 2011/2014 Advice Advice 2011/2014 Advice Adv	Lat Pug Diplog 2010/2018 all 10 2010/2018 all 10 2010/2018 all 10 114/2018 all 10	0 NO NU NU NU
Administradoc Simbole de \Users\HIDALGO\Desk sktop\FORENSICS\SYS \Users\HIDALGO\Desk	l Disterna top\FORENSICS>USBD TEM" top\FORENSICS>	eview.exe //	egfile "C:\User		Intervene Filt See Split Intervene See Split Intervene Statistics Statistics Intervene Statistics Statistics Statistics	In para Description Total Input Conce Total Input Conce	Device Type MC Process Monacolo MC Process Monacolo MC Process Monacolo Water Video	Cannechael Nac Nac Nac Nac Nac Nac	Sectory No. No. No. No.	Dubled No. No. No. No. No.	15744 In In In In	Divi Litter	Selafikande	Control Day Device A Line 2010/09/00/00 2010/09/00/09 2010/09/00/07 2010/09/00/07	Lat Pilg Graing 2010/2018 81/108 2011/2018 81/108 114/2018 81/108 2011/2018 81/108	0 100 100 100 100 100
Administrator Simbole de NUSers \HIDAL GO\Desk sktop \FORENSICS \SYS \USers \HIDAL GO\Desk	d bioterny top\FORENSICS>USBD TEM" top\FORENSICS>	≥eview.exe /r	-egfile "C:\User	P\$\HEOALGO\	Image: Control of the second	n (199) 2013 No (2) (2) (4) 2013 No (2) (2) (4) 101 Not 2014 101 Not	Device Type IRC: Monree Hoffscrift IRC: Plana V Hoffscrift HC: Haras Hoffscrift Video Video HC: Planas Hoffscrift	Cannechal Na Na Na Na Na Na Na		Dubled No. No. No. No. No. No.	157 %44 14 14 15 15 15 15	Divi Litter	Selflande	Created Date Sectors a server 2011 Director and 2011 Director and 2011 Director and 2011 Director and 2011 Director and	Let Pug Unplug 2010/2010 EXTUR 2010/2010 EXTUR 2010/2010 EXTUR 2010/2010 EXTUR 2010/2010 EXTUR	0 80 80 80 80 80 80 80 80 80 80 80 80 80
Administrator Simbole de NUsers\HIDALGO\Desk sktop\FORENSICS\SYS \Users\HIDALGO\Desk	l bitema top\FORENSICS>USBD TEN" top\FORENSICS>	Deview.exe ∕r		II X	Image: Control of the contro	 Strip Strip (2) (2) (4) Becaptore Becap	Device Type HC - Hannes Medican D. HC - Hannes Medican D. HC - Hannes Medican D. Web Voles HC - Hannes Medican D. HC - Hannes Medican D.	Carriedad Tas Tas Tas Tas Tas Tas Tas		Dutied No. No. No. No. No. No.	1214	DiviLine	Selfante	Control Date Sector R Annal 2010/07/2010 2010/07/2010 2010/07/2010 2010/07/2010 2010/07/2010 2010/07/2010 2010/07/2010	Lat Pug Ungling Software street 2010/09/812/19/8 2010/91/81/09 10/2019/81/07 2010/91/82/07 2010/91/82/07 2010/91/82/07 2010/91/82/07	
Admentsdon Smoole de \Users\HIDALGO\Desk sktop\FORENSICS\SYS \Users\HIDALGO\Desk	H WISEMA top\FORENSICS>USBD TEN" top\FORENSICS>	Devlew.exe /r		PS/HIOALGO/	€ 1020cmms [M = [M = [M = [M = [M = [M	The Second Secon	Device Type MC Process Montace D. MC Process Montace D.	Carriedad Na Na Na Na Na Na Na	Sectorary No. No. No. No. No. No. No. No. No. No.	Dubled No. No. No. No. No. No. No.	152 Hut Inc. Inc. Inc. Inc. Inc. Inc. Inc.	Drive Letter	Seaffante	Costel Day 2010/001100/00 2010/001010 2010/00101060 2010/00101060 2010/001060 2010/001060 2010/001060 2010/001060	Lat Poylogies 2010201 Store 201020 Store 201020 Store 201020 Store 201020 Store 201020 Store 201020 Store 201020 Store	
Administration Simbole de Visens WIDAL (60) Desk sktop \FORENSICS\SYS \Usens\HIDAL60\Desk	d USEEMA top\FORENSICS>USBD TEM [™] top\FORENSICS>	Deview.exe ∕r		S HIDALGO	Image: Control of the contro	Total Sectors	Device Type IEC: Promote Microsofte Microsofte Microsofte Microsofte Microsofte Microsofte Microsofte Microsofte Devices Market Discover Devices D	Cannochel Res Res Res Res Res Res Res Res Res Res		Dutied No. No. No. No. No. No. No. No. No. No.		Divi Lietur	Seatharde	Control Date 2010/00112000 2010/0012000 2010/0012000 2010/0012000 2010/0012000 2010/0012000 2010/0012000 2010/00120000 2010/00120000	Lat Phy Orphy. 2012091 Endler 2012091 Endler 2012091 Endler 2012091 Endler 2012091 Endler 2012091 Endler 2012091 Endler	0 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3
Administration Semble do USers (HIDALGO) Desk sktop (FORENSICS) SYS (Users (HIDALGO) Desk	d ustema top:ForensICS>USBD TEM" top:ForensICS>	Deview.exe /r		S (HIOALGO)		The Difference of the Differen	Delat Typ RC Jonas Hofesch HC Hanas Hofesch HC Hanas Hofesch HC Hanas Hofesch HC Hanas Hofesch HC Hanas Hofesch HC Hanas Hofesch Lanasyndhes Lanasin	Connected Ros Ros Ros Ros Ros Ros Ros Ros Ros Ros				Divisions (134)	SetThete	Control Date 2010/07/07/07/07/07/07/07/07/07/07/07/07/07	Lat Pug Unglog 2010/2018 and 2010/2018 and 2	C E E S D E E E E E E E E
Users HIDALGO\Desk sktop\F0RENSICS\SYS Users\HIDALGO\Desk	d USEEMA top\FORENSICS>USBD TEM [®] top\FORENSICS>	Deview.exe /r	-egfîle "C:\User	S HIDALGO	♥ 100 cont № 24 cont № 24 cont № 24 cont ♥ 24 cont ♥ <td>DP DP DP</td> <td>Zecks Type INC Source Markets MC Shares Hardwords MC Hares Hardwords Hitter Hitter Hitter Shares Indexed Distance Conservations Index Systems Techniques Index Shares Indexed Distance Same</td> <td>Convected The The The The The The The The The The</td> <td></td> <td>Dubled The The The The The The The The The The</td> <td></td> <td>Disi Leta</td> <td>Seaffante</td> <td>Control Date 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014</td> <td>Lat Pag Orging 2012/09/88/2018 2012/09/88/2018 2012/09/88/2018 2012/09/88/2018 2012/09/88/2018 2012/09/81/2018 2012/09/81/2018 2012/09/81/2018 2012/09/81/2018 2012/09/81/2018</td> <td>0 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2</td>	DP	Zecks Type INC Source Markets MC Shares Hardwords MC Hares Hardwords Hitter Hitter Hitter Shares Indexed Distance Conservations Index Systems Techniques Index Shares Indexed Distance Same	Convected The The The The The The The The The The		Dubled The The The The The The The The The The		Disi Leta	Seaffante	Control Date 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014 2010/09/2014	Lat Pag Orging 2012/09/88/2018 2012/09/88/2018 2012/09/88/2018 2012/09/88/2018 2012/09/88/2018 2012/09/81/2018 2012/09/81/2018 2012/09/81/2018 2012/09/81/2018 2012/09/81/2018	0 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Administration Semble do Utsers (HIDALGO) Desk sktop (FORENSICS) SYS (Users (HIDALGO) Desk	d bitterna top\FORENSICS>USBD TEM* top\FORENSICS>	Deview.exe ∦r			Image: Strategy and S	 DP December <lidecember< li=""> December December</lidecember<>	Point Type Colores Michaels	Convected The The The The The The The The The The	Sections No. No. No. No. No. No. No. No. No. No.	Dubled No. No. No. No. No. No. No. No. No. No.		Distants CDM	Southante	Costal Data 2010/07/07/07/07/07/07/07/07/07/07/07/07/07	Lat Pug Unglog 2012/06 11:00 2012/06 11:00	
Users (HIDALGO/Desk sktop/FDRENSICS/SYS (Users (HIDALGO/Desk	d bitterna top\FORENSICS>USBD TEM" top\FORENSICS>	Deview.exe /r	-egfîle "C:\User	C ×	Image: State State Image: State	DPF D	Device Type Tel: Source Indiversity Tel: Statuse Indianase. Hild: Statuse Indianase. Hild: Statuse Indianase. Hild: Statuse Indianase. Statuse Indianase. Statu	Connected Bas Bas Bas Bas Bas Bas Bas Bas Bas Bas	Sections No. No. No. No. No. No. No. No. No. No.	Dubled The The The The The The The The The The		Dec Lifes CDMJ	Set/fambe	Costel Date 2010/02/01/02/02/02/02/02/02/02/02/02/02/02/02/02/	Lat Pug Unglag. 2010/09 81/10 2010/09 81/10	0 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 5 5 5 5 5
USers\HIALGO\Desk VSers\HIALGO\Desk Attop\fPREIS(S\SYS \Users\HIALGO\Desk	d Bisterna top\FORENSICS>USBD TEM" top\FORENSICS>	Devieu.exe /r	 regfile "C:\User	C ×	Image: Strategy and S	20% 20%	Point Spir Colores Michaels Michaels Michaels Michael Michaels Mic	Connected Ros Ros Ros Ros Ros Ros Ros Ros Ros Ros	lak formu Ni Ni Ni Ni Ni Ni Ni Ni Ni Ni Ni Ni Ni	Dublid No No No No No No No No No No No No No		Distints (114)	Seaffante	Costed Date 2010/2018 11/00 2010/2018 11/00 2010/2018 11/00 2010/2018 11/00 2010/2018 11/00 2010/2018 12/00 2010/2018	Last Play Graphig. 2010;2018;2019 2010;2018;2019 2010;2018;2019 2010;2018;2019 2010;2018;2019 2010;2018;2019 2010;2019;2029 2010;2019;2019 2010;2019 2010;2019;2019 2010;2019	0 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2

Fig. 2.29. Conexión a un fichero SYSTEM de forma externa.

Se puede grabar toda la información recopilada en diferentes formatos (Tabla 2.3.):

1600

Tabla 2.3. Opciones de Grabar información de dispositivos USBs con Línea de Comandos.

Comando	Descripción
/stext <filename></filename>	Guarda la lista de todos los dispositivos USB en un archivo de texto normal:
/stab <filename></filename>	Guarda la lista de todos los dispositivos USB en un archivo de texto delimitado por tabuladores
/scomma <filename></filename>	Guarda la lista de todos los dispositivos USB en un archivo de texto delimitado por comas.
/stabular <filename></filename>	Guarda la lista de todos los dispositivos USB en un archivo de texto tabular.
/shtml <filename></filename>	Guarda la lista de todos los dispositivos USB en un archivo HTML (Horizontal).
/sverhtml <filename></filename>	Guarda la lista de todos los dispositivos USB en un archivo HTML (Vertical).
/sxml <filename></filename>	Guarda la lista de todos los dispositivos USB en un archivo XML.
	Esta opción de línea de comandos se puede utilizar con otras opciones de guardar para ordenar por la columna deseada.
/sort <column></column>	Si no especifica esta opción, la lista se clasifica de acuerdo con el último tipo que ha creado desde la interfaz de usuario. El parámetro <column> puede especificar el índice de columna (0 para la primera columna, 1 para la segunda columna, etc.) o el nombre de la columna, como "Nombre del dispositivo" y "Descripción".</column>
	Puede especificar el carácter de prefijo '~' (por ejemplo: "~ Descripción") si desea ordenar en orden descendente. Puede poner múltiples / ordenar en la línea de comandos si desea ordenar por varias columnas.
	Ejemplos:

	USBDeview.exe /shtml "f:\temp\usb-list.html" /sort 2 /sort ~1
/nosort	USBDeview.exe /shtml "f:\temp\usb-list.html" /sort "Tipo de dispositivo " /sort "Nombre del dispositivo " Cuando especifique esta opción de línea de comandos, la lista se guardará sin ninguna
/DisplayDisconnected <0 1>	ordenacion. Especifica si se muestran los dispositivos desconectados. $0 = No$, $1 = Si$.
/DisplayNoPortSerial <0 1>	Especifica si se muestran los dispositivos sin número de puerto / serie. $0 = No$, $1 = Si$.
/DisplayNoDriver <0 1>	Especifica si se muestran los dispositivos sin controlador. $0 = No$, $1 = Si$.
/DisplayHubs <0 1>	Especifica si se mostrarán los concentradores USB. 0 = No, 1 = Sí.
/RetrieveUSBPower <0 1>	Especifica si se recupera la información de la alimentación / versión USB.
/MarkConnectedDevices	Especifica si marca los dispositivos conectados.
/TrayIcon <0 1>	Especifica si se debe iniciar USBDeview con un icono de bandeja.
/AddExportHeaderLine <0 1>	Especifica si se debe agregar una línea de encabezado al exportar la información USB a un archivo delimitado por csv / tab.

Fuente: <u>http://nirsoft.net/utils/usb_devices_view.html</u>

1605

Toda la información que se recopiló se puede guardar en una

página .html (Fig. 2.30.), y disponer de manera centralizada o en una

aplicación web (Fig. 2.31.).



Fig. 2.30. Información que se guarde en una página HTML.

← → C D C:/Users/Ivan/Desktop/REGI	5TRO/INFORME.html							
USB Devices List								
Created by using <u>USBDeview</u>								
Device Name	Description	Device Type	Connected	Safe To Unplug	Disabled	USB Hub	Drive Letter	Serial ?
0000.0014.0000.002.000.000.000.000.000	USB Input Device	HID (Human Interface Device)	No	Yes	No	No		
0000.0014.0000.002.000.000.000.000.000	USB Input Device	HID (Human Interface Device)	No	Yes	No	No		
0000.0014.0000.002.000.000.000.000.000	USB Input Device	HID (Human Interface Device)	No	Yes	No	No		
0000.0014.0000.003.000.000.000.000.000	USB Video Device	Video	Yes	Yes	No	No		
0000.0014.0000.003.000.000.000.000.000	USB Video Device	Video	No	Yes	No	No		
0000.0014.0000.006.000.000.000.000.000	USB Input Device	HID (Human Interface Device)	No	Yes	No	No		
0000.0014.0000.006.000.000.000.000.000	USB Input Device	HID (Human Interface Device)	No	Yes	No	No		
0000.0014.0000.006.000.000.000.000.000	USB Input Device	HID (Human Interface Device)	No	Yes	No	No		
0000.0014.0000.006.000.000.000.000.000	SM-J200M	Unknown	No	Yes	No	No		
0000.0014.0000.006.000.000.000.000.000	Dispositivo serie USB	Communication	No	Yes	No	No	COM3	
0000.0014.0000.006.000.000.000.000.000	ADB Device	Vendor Specific	No	No	No	No		
Microsoft® Nano Transceiver v1.0	USB Composite Device	Unknown	Yes	Yes	No	No		
Microsoft® Nano Transceiver v1.0	USB Input Device	HID (Human Interface Device)	Yes	Yes	No	No		

Fig. 2.31. Información de ficheros USBDeview guardada en una página Web.

1615

La herramienta combinada con el visor de eventos permite controlar las fugas de información y que algún usuario se lleve un archivo de la empresa, por lo que se debería utilizar una tecnología de pago o comercial.

1620 USBDeview.exe /regfile

"C:\windows\system32\config\SYSTEM"

2.2.9. Endpoint Protector

1630

1625 La herramienta proviene de una empresa rumana (Fig. 2.32.) y se puede descargar desde el siguiente enlace <u>http://www.endpointprotector.com/</u>



Fig. 2.32. Herramienta para varios sistemas operativos. Fuente: <u>http://www.endpointprotector.es/</u>

La herramienta es multiplataforma diseñada para Windows,
OSx, Ubuntu, openSUSE, Mac, iOS, Android, prácticamente un 90
a 95% de los sistemas operativos; es decir, dispone de los
1635 dispositivos que reconoce usarlo en modo hardware o virtual, y lo protege, *Resourses → Data Sheets*

(http://www.endpointprotector.com/support/pdf/datasheet/Dat a Sheet Endpoint Protector 4 CoSoSys ES.pdf); este es capaz de monitorear (Tabla 2.4.) todos los dispositivos como:

Dispositivos hardwar	e o virtuales
• Dispositivos USB	Clientes de correo electrónico
• Unidades USB* (normales, U3)	o Outlook
• Tarjetas de Memoria (SD, CF, etc.)	o Lotus Notes
• CD/DVD	o Thunderbird, etc.
• Quemadores (int., ext.)	• Navegadores Web
• HDDs externos (incl. SATA)	o Internet Explorer
• Impresoras	o Firefox
• Unidades Floppy	o Chrome, etc.
• Lectores de Tarjeta (int., ext.)	• Mensajería Instantánea
• Cámaras web	o Skype, etc.
• Tarjetas de red WiFi	o Microsoft
	Communicator
 Cámaras Digitales 	o Yahoo Messenger,
• iPhones / iPads / iPods	Aplicaciones de compartir archivos
• Smartphones/BlackBerry/PDAs	o Dropbox
• Unidades FireWire	o BitTorrent
• Reproductor MP3/Reproductores Media	o Kazaa, etc.
Dispositivos Biométricos	• Otras Aplicaciones
Dispositivos Bluetooth	o iTunes
• Unidades ZIP	o Samsung Kies
• Tarjetas Express (SSD)	o Windows DVD Maker
• USB inalámbrico	o Total Commander
Puerto Serie	o FileZilla
• Placa Teensy	o Team Viewer
• Dispositivos de almacenamiento PCMCIA	o EasyLock, y muchos mas

Fuente:

<u>http://www.ireo.com/fileadmin/docs/documentacion_de_productos/cososys/</u> Datasheet_Endpoint_Protector_4.pdf Actualmente existe una variedad de herramientas que brindan

1645 seguridad en temas de auditorías para todos los ficheros de una empresa, es cuestión de inversión y que productos prefiera adquirir el administrador.

2.3. Artefactos y contraseñas

1650

2.3.1. Dialupass

Se lo puede descargar desde:

(http://nirsoft.net/utils/dialupass.html), este artefacto permite extraer todas las conexiones de acceso remoto de una máquina, por
1655 ejemplo: si un administrador de una empresa ha renunciado y se desconocen las contraseñas, se procede a la caja de herramientas en donde se ejecuta la aplicación y automáticamente en la pantalla se va

a exponer el usuario y la contraseña (Fig. 2.33.).

Dialupass						
<u>File E</u> dit <u>V</u> iev	v Options <u>H</u> elp					
- E 🔛 😰 🛙	è f 🔕 🖪					
Entry 🛆	Phone / Host	User N	Password	Domain	Password Owner	Password Owne
atgtatat	10.10.20.20	Hello01	hffy3427fG	Dom01	VM-XP\Administ	S-1-5-21-199396
書 Internet01	10.10.0.1	nsft8	1234RRFF		All Users	
🛃 NirSoft	192.168.22.11	nirs02	NBG56712		All Users	
<						>
2 item(c) 1 Selec	ted		NirSoft Fr	eeware, http://www	v.nirsoft.net	



2.3.2. Network Password Recovery

Se lo puede descargar desde:

1665 (<u>http://nirsoft.net/utils/network password recovery.html</u>), se pueden obtener las contraseñas de red, las veces necesarias utilizando la herramienta Network Password Recovery que permitirá la recuperación de las contraseñas de red (Fig. 2.34.), siempre y cuando estén almacenadas en el equipo a ejecutar.

<u>File E</u> dit ⊻iew <u>H</u> e	p		
🔜 🖻 🖻 🔮) - 1 1		
Item Name 🛛 🛆	Туре	User	Password
192.168.3.35	Domain Password	srv\admin1	hyyu7TRF5
Server05	Domain Password	Server05\User01	6tgR51
Server08	Domain Password	domain\nirsoft	hy1tRerr5
41			

1670

Fig. 2.34. Artefacto Network Password Recovery. Fuente: <u>http://nirsoft.net/utils/network_password_recovery.html</u>

2.3.3. MessenPass

1675 Se lo puede descargar desde:

(http://nirsoft.net/utils/mspass.html), se pueden extraer las contraseñas de Messenger, América Live, Yahoo (Fig. 2.35.). Evidentemente se debe tener acceso físico a la máquina o remoto con alguna conexión administrativa, el MessenPass permitirá extraer

1680 el usuario y la contraseña.

💉 MessenPass			- 0
<u>File E</u> dit <u>V</u> iew <u>H</u> elp			
🗀 🔜 🙆 🖻 🖆 📲			
Software 🔺	Protocol	User	Password
Miranda	Jabber	jaber12345	K8mnj61
MSN Messenger	MSN Messenger	nhhggttf@hotmail.com	1Plki98W2
Netscape-AOL Instant Messenger	AOL Instant Messenger	aol26612	PO65TfRh
Trillian	MSN Messenger	msnh765	OiJJhygtr
Trillian	Yahoo! Messenger	yahoo123d	kijUsce
Yahoo Messenger	Yahoo! Messenger	nirsoft821	AcGG6tyrr

Fig. 2.35. Artefacto MessenPass. Fuente: <u>http://nirsoft.net/utils/mspass.html</u>

1685 2.4. Navegadores

Los navegadores web (Fig. 2.36.), poseen las rutas de los diferentes sistemas operativos y versiones posteriores, donde se localiza los navegadores de internet como Chrome, Explorer, Firefox, y al utilizar una herramienta específica se obtendrá las contraseñas almacenadas en los mismos.



Fig. 2.36. Navegadores de internet.

2.4.1. Chrome.



1695

En Linux

/ Home / \$ USER / .config / google-chrome / Default / Preferences

1700

En MacOS-X

/ Users / \$ USER / Library / Application Support / Google / Chrome / Default / Preferences

1705 En Windows XP

C: \ Documents and Settings \ % USERNAME% \ Configuración local \ Datos de programa \ Google \ Chrome \ User Data \ Default \ Preferences

En Windows Vista y versiones posteriores



2.4.2. iExplore.



Fig. 2.38. Navegador Internet Explorer.

1715 En Windows 95/98, estos archivos estarán ubicados en los

siguientes lugares:

%% Systemdir \ Temporary Internet Files \ Content.IES % \ Cookies systemdir %% Systemdir \ Historia \ History.ie5

1720

En Windows 2000/XP las ubicaciones de los archivos han

cambiado:

	%% Systemdir $\ $ Documents and Settings $\ $ % username% $\ $ Local Settings $\$
	Temporary Internet Files \ Content.IES
1725	%% Systemdir $\ Documents and Settings \ % username% \ Cookies$
	%% Systemdir $\ Documents and Settings \ % username% \ Configuracion$
	local \ Historia \ history.ie5

En Windows Vista / 7

1730

%%Systemdir \ Users \ % username% \ AppData \ Local \ Microsoft \
 Windows \ Temporary Internet Files \

%%Systemdir $\ \$ Users $\ \$ wername% $\ \$ AppData $\ \$ Local $\ \$ Microsoft $\$

Windows \setminus Temporary Internet Files $\setminus \setminus$ Low

Internet Explorer igualmente mantiene registros de historial diarios,

semanales y mensuales que se encuentran en las carpetas dé %%
 systemdir \ Documents and Settings \%

2.4.3. Firefox.



Fig. 2.39. Navegador Firefox.

En Linux

1740

÷	_	_			_	_					_				_	_	-	_				-	_	_				_			_	_		 	-	
I.																																				1
I.		/	ho	m	e/1	\$U	JS	El	R/	'.n	10	zil	la	/f	ire	efc)X	/\$	\mathbf{P}	R(DF	Π	٦E	.d	ef	au	lt/	pl	ac	es.	sql	lite	5			1
I.																												1			1					- !
-	-	_				-	-				-	-				-	-	_	-	-				-	-				_			-	-	 		

1745 En MacOS-X

/Users/\$USER/Library/Application Support/Firefox/Profiles/\$PROFILE.default/places.sqlite

En Windows XP

C:\DocumentsandSettings\%USERNAME%\ApplicationData\Mozilla\Firefo 1750 x\Profiles\%PROFILE%.default\places.sqlite

En Windows Vista, 7

C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\% PROFILE%.default\places.sqlite

1755 2.5. Herramientas para la obtención de contraseñas en los navegadores

2.5.1. WebBrowserPassView

La herramienta:

(http://www.nirsoft.net/utils/web_browser_password.html),

1760 permite saber dónde se encuentran las rutas y la ubicación para obtener las contraseñas.

Además, reconoce todas las contraseñas que se han introducido y las que el usuario ha guardado, por ejemplo, cuándo 1765 se inicia una sesión en una sitio o aplicación web aparece una ventana solicitando ¿desea guardar la contraseña?, la próxima vez que ingrese se almacenará las contraseñas (Fig. 2.40.).

WebBrowserPassView						- 0	×
File Edit View Options Help							-
URL	Web Browser	User Na	P. /	Password	User Name Field	Password Field	^
http://deac.espoch.edu.ec:8085/SIEDD_11/validarusuario.jsp	Chrome	0603370_	Soloy	Strong	UserName	Password	
http://estacademico.espoch.edu.ec/OAS_SitioWeb/LogIn.aspx	Chrome	0603370	Soloy	Strong	txtiDUsuario	txtContrasena	
http://utei.espoch.edu.ec:8085/SIEDD1/	Chrome	0603370	Soloy	Strong	UserName	Password	
https://accounts.google.com/SignUp	Chrome	ceacc.fs	Soloy	Strong	GmailAddress		
https://accounts.google.com	Firefox 32+	ceace.fs	Soloy	Strong	identifier	password	
https://accounts.google.com	Firefox 32+	ceacc.fs	Soloy	Strong	identifier	password	
https://login.microsoftonline.com/	Chrome	ceacc_fs	Soloy	Strong	loginfmt	passwd	
https://login.microsoftonline.com	Firefox 32+	ceace_fs	Soloy	Strong	login	passwd	
O https://login.microsoftonline.com/common/oauth2/authorize	Opera	ceacc_fs	Soloy	Strong	login	pesswd	
https://www.facebook.com	Firefox 32+		Soloy	Very Strong		pass	
https://elearning.espoch.edu.ec/login/index.php	Chrome	0603370	Soloy	Very Strong	usemame	pessword	
https://recursos.espoch.edu.ec/homeg.php	Chrome	0603370	Soloy	Very Strong	user_	pwd_	
https://repositorioeva.espoch.edu.ec/	Chrome	0603370	Soloy	Very Strong	usemame	password	
O https://accounts.google.com/ServiceLogin	Opera	espoch.f_	Soloy	Very Strong	Email	Passwd	
https://accounts.google.com/signin/v2/sl/pwd	Chrome	espoch.f	Soloy	Very Strong	identifier	password	
https://zoom.us/activate	Chrome	Hidalgo	Soloy	Very Strong	lastName		
https://secure.urkund.com/account/signup/invite	Chrome	ihidalgo	Soloy	Very Strong	UsernameOrEmail	Password	
http://eujournal.org/index.php/esj/user/register	Chrome	ihidalgo	Soloy	Very Strong	usemame	password	
http://journals.epistemopolis.org/index.php/hmedicas/user/register	Chrome	ihidalgo	Soloy	Very Strong	usemame		
Shttps://ebookcentral.proquest.com/auth/lib/espochsp/newAccou	Chrome	ihidalgo	Soloy	Very Strong	usemame	password	
https://www.brilliantdownload.com/en/signup.html	Chrome	ihidalgo	Soloy	Very Strong			
Shttps://zoom.us/signin	Chrome	ihidalgo	Soloy	Very Strong	email		
https://www.tarjetasbancopichincha.com/wps/portal/PortalPichin	Chrome	NanHid	Soloy	Very Strong	pbns_Z7_8ALG1282KGT1D0AMBRES7K3087_:	pbns_Z7_8ALG1282KGT1D0AMBRES7K3087_:_viewRoot:formLoginId:j_id11	
https://dialnet.unirioja.es/servlet/alta	Chrome	ivanmhi	Soloy	Very Strong	login	pess	
https://accounts.google.com/ServiceLogin	Chrome	ivanmhi	Soloy	Very Strong	identifier	password	
https://www.canva.com/signup	Chrome	ivanmhi	Soloy	Very Strong	emailConfirmation	password	
https://accounts.google.com	Firefox 32+	ivanmhi	Soloy	Very Strong	Email	Passwd	
https://login.live.com/login.srf	Chrome	soft_wor_	Soloy	Very Strong	loginfmt	pesswd	
https://twitter.com/edutec2018	Chrome	soft_wor_	Soloy	Very Strong	session[username_or_email]	session[password]	- 11
https://www.slideshare.net	Firefox 32+		Soloy	Very Strong		password	
https://login.microsoftonline.com/login.srf	Chrome	ihidalgo	Soloy	Very Strong	loginfmt	passwd	

Fig. 2.40. Herramienta WebBrowserPassView para obtener las contraseñas.

1775

2.5.2. MailPassView

La herramienta MailPassView:

(<u>http://www.nirsoft.net/utils/mailpv.html</u>) permite obtener las contraseñas del Outlook; es decir, si se ha cambiado la contraseña y se desconoce la misma, esta utilidad permite conseguir las contraseñas del usuario (Fig. 2.41.).

😹 Mail Pass¥i	ew					_ 🗆 >
<u>File Edit View</u>	v <u>H</u> elp					
🖬 🔮 🖦 I	f					
Name 🔺	Application	Email	Server	Type	User	Password
🖂 Mr. Bean	Eudora	mrbean@mrbean.com	10.10.10.10	IMAP	bean	BlueCar
🖾 Nir Sofer	Outlook Express	nirsoft@abcdefg.com	mail.abcdefg.com	POP3	nirsoft	126abf1P
🖾 Rainbow	IncrediMail	rainbow@test.com	192.168.12.12	SMTP	rainbow	tornado
📉 Test User	IncrediMail	test@test.com	192.168.10.10	POP3	test	BigDog86
۹						
4 item(s), 1 Sele	cted					

Fig. 2.41. Herramienta Mail PassView para obtener contraseñas del Outlook. Fuente: http://wnw.nirsoft.net/utils/mailpv.html

2.5.3. Metadatos

Los metadatos es la información que se encuentra localizada dentro de un archivo y que está oculta (Fig. 2.42.), por ejemplo: 1785 cuando se va a un archivo y se ejecuta *Propiedades* luego a *Detalles* y se coloca *Ouitar Propiedades*.



Fig. 2.42. Herramienta que permite obtener la información de metadatos que está dentro de un archivo.

1790

Con diferentes utilidades por ejemplo *FOCA* (se emplea más para Hacking que para Forense), se podría obtener información de los metadatos de un archivo; es decir, permite obtener un directorio y extraer todos los metadatos de los ficheros como: autor, cuantas 1795 revisiones se han hecho, si ha existido algún tipo de modificación, cuando se hizo la modificación. Foca lo devolverá directamente.

2.5.4. Document Metadata Extraction

En el siguiente enlace se ubican varias herramientas (Fig.

1800 2.43.), que extraerán metadatos de archivos:

http://www.forensicswiki.org/wiki/Document Metadata Extract



Fig. 2.43. Herramienta para obtener los Metadatos.

1805

2.5.5. Accesos directos

Esta herramienta se puede descargar de:

(http://www.mitec.cz/wfa.html), es un conjunto de todas las herramientas que se han visto en el presente libro, por ejemplo: se

1810 busca miniaturas de Google, miniaturas de Bases de Datos, elPrefetch, y lo que se va a analizar es Accesos Directos, el

Index.DAT, la Papelera, una herramienta que analice los accesos directos (Shortcut Analizer).

1815 Permite obtener los accesos directos, al ejecutar el archivo WFA.exe. En una máquina clonada solamente se haría el montaje virtual; es decir, dirigirse a la carpeta y seleccione la ruta de esta, el sistema operativo que se tiene va a hacer un recorrido por toda la RAM (Fig. 2.44.).

🅞 Wi	indows File Analyzer - [SA - Recent]					- 0	×	
🙆 F	ile Windows Help						. 0	×
	🔊 🏊 📾 🖬 🖶 🔜 🙆							
SA 🥥	A - Recent							
0	Shortcut Analysis					Re	port	
	Unectory: C: Users (PSP-01AL02A)	21 Abbinata (koaming Microsoft (Windows (Kecent						
	volume senal: 8C22-929C							
	Volume label:							
Filena	me veniduurk	Linked path	Created	Written	Last Accessed A	Size [B]	Vol Typ	æ
03	-RB (D).Ink	D:\	1/1/1980	1/1/1980	1/1/1980	0	Remo	^
Uni	idad USB (D).lnk	D:\	1/1/1980	1/1/1980	1/1/1980	0	Remo	
SE	RIAL-Ink	D:\SERIAL.txt	25/1/2018 8:10:54	25/1/2018 10:45:25	25/1/2018 8:10:54	135	Remo	
CE	DA_X64FREV_ES-ES_DV5 (D).Ink	D:\	23/1/2018 11:04:56	25/1/2018 11:08:23	25/1/2018 11:08:23	8192	Remo	
🗉 Dis	co local (C) (2).ink	C:)	18/3/2017 6:40:20	25/1/2018 12:09:27	25/1/2018 12:09:27	4096	Fixed	
🗉 SW	DVD5_Visio_Std_2016_64Bit_Spanis	C:\Service\SW_DVD5_Visio_Std_2016_64Bit_Spanish_ML	25/1/2018 12:09:31	5/2/2016 16:42:06	25/1/2018 12:09:31	593371136	Fixed	
€ SW	_DVD5_Project_Pro_2016_64Bit_Spa	C:\Service\SW_DVD5_Project_Pro_2016_64Bit_Spanish	25/1/2018 12:10:54	11/11/2016 17:00:16	25/1/2018 12:10:54	525744128	Fixed	
H 15	ALUD PUBLICA.Ink	C:\Service\1 SALUD PUBLICA.jpg	25/1/2018 12:15:29	27/1/2016 9:47:01	25/1/2018 12:15:29	3811852	Fixed	
🗉 log	o_espoch.ink	C:\Service\logo_espoch.png	25/1/2018 12:15:30	22/6/2016 15:27:56	25/1/2018 12:15:30	1115886	Fixed	
🗉 Ser	rvice.lnk	C:\Service	25/1/2018 12:09:21	25/1/2018 12:18:21	25/1/2018 12:18:21	4096	Fixed	
	03960535.lnk	D:\27ENERO\SESION 3\0603960535	27/1/2018 20:09:01	27/1/2018 20:09:02	27/1/2018	0	Remo	
E SES	SION 3 (2).lnk	D:\27ENERO\SESION 3	27/1/2018 19:35:19	27/1/2018 19:35:20	27/1/2018	0	Remo	
E SES	SION 3.Ink	D:\27ENERO\SESION 3	27/1/2018 19:35:19	27/1/2018 19:35:20	27/1/2018	0	Remo	
17	_00_0603960535_20180127_2001.lnk	C:\Users\FSP-UINL02N21\Documents\17_00_060396053	27/1/2018 20:01:01	27/1/2018 20:01:41	27/1/2018 20:01:01	7243	Fixed	
060	04391763.lnk	D:\enero 28\SESION11\0604391763	28/1/2018 11:26:47	28/1/2018 11:26:48	28/1/2018	0	Remo	
H 07.	Ink	D:\DATOS\07	28/1/2018 15:12:34	28/1/2018 15:12:36	28/1/2018	0	Remo	
	ENERO.Ink	D:\27ENERO	27/1/2018 10:33:46	27/1/2018 10:33:48	28/1/2018	0	Remo	
DA	TOS.Ink	D:\DATOS	28/1/2018 15:03:48	28/1/2018 15:03:50	28/1/2018	0	Remo	
ene	ero 28.ink	D:\enero 28	28/1/2018 9:54:12	28/1/2018 9:54:14	28/1/2018	0	Remo	
SES	SION 11. Ink	D:\enero 28\SESION11	28/1/2018 10:31:19	28/1/2018 10:31:20	28/1/2018	0	Remo	
Do	cumentos.Ink	C:\Users\FSP-UINL02N21\Documents	25/1/2018 11:53:31	28/1/2018 20:04:44	28/1/2018 20:04:44	4096	Fixed	
Nu	eva carpeta.lnk	C:\Users\FSP-UINL02N21\Documents\Nueva carpeta	28/1/2018 20:04:44	28/1/2018 20:04:44	28/1/2018 20:04:44	0	Fixed	
EZ	Analyze3.lnk	C:\Users\FSP-UINL02N21\Downloads\EZAnalyze3.xls	29/1/2018 9:02:18	29/1/2018 9:02:20	29/1/2018 9:02:18	1361920	Fixed	
🗄 EZ/	Analyze3 (2).lnk	C:\Users\FSP-UINL02N21\AppData\Roaming\Microsoft\C	29/1/2018 9:02:49	29/1/2018 9:02:53	29/1/2018 9:02:49	898560	Fixed	
🗉 Co	mplementos.Ink	C:\Users\FSP-UINL02N21\AppData\Roaming\Microsoft\C	25/1/2018 12:35:29	29/1/2018 9:02:53	29/1/2018 9:02:53	0	Fixed	
De	ecargae lok	Criticere/ESPJ IINI 02021/Downloade	25/1/2018 11:53:31	20/1/2018 0-00-07	29/1/2018 9:09:07	4006	Eived	

1820

Fig. 2.44. Herramienta WFA para obtener los accesos directos.

Un acceso directo a una aplicación o a un dato, significa que no tendrá que dirigirse a la ruta del original. Entonces si alguien
- 1825 desinstala un programa puede ocurrir que el acceso directo no se borre o que otro usuario escoja un programa y lo suprima manualmente y los accesos directos se quedan. Un acceso directo así quede huérfano va a permitir sacar los metadatos que contenía de la aplicación original, por ejemplo, si un archivo .lnk contiene
- 1830 información, tiene todos los metadatos con los archivos que los creó o la aplicación que los generó.

La Fig. 2.45., ilustra la información, sobre dónde está ubicado el archivo original, y muestra en detalle la información como: fecha
1835 de creación, fecha de escritura, cuando se accedió por última vez a la aplicación, convirtiéndose en un tema de propiedad intelectual.

Windows File Analyzer - [SA - Recent]				- 0	×
				-	0
🖼 • 🔟 🔹 🛍 • 🗟 • 🔝 🙆					
SA - Recent					
				Report	
Shortcut Analysis				Nepor	Lass
Directory: C: Users/FSP-UBNL02	(21)AppData (Roaming (Microsoft (Windows (Recent				
Volume senal: 8C22-929C					
Volume label:					
filename	Linked path	Created	Written	Last Accessed 🔺	
DJ-RB (D).ink	P:\	1/1/1980	1/1/1980	1/1/1980	
Unidad USB (D).Ink	D:/	1/1/1980	1/1/1980	1/1/1980	
SERIAL.ink	D:\SERIAL.txt	25/1/2018 8:10:54	25/1/2018 10:45:25	25/1/2018 8:10:54	
CEDA X6#REV ES-ES DVS (D).ink	P:\	23/1/2018 11:04:56	25/1/2018 11:08:23	25/1/2018 11:08:23	
Disco local (C) (2).Ink	CI	18/3/2017 6:40:20	25/1/2018 12:09:27	25/1/2018 12:09:27	
SW DVD5 Visio Std 2016 64Bit Spanis.	C:\Service\SW DVD5 Visio Std 2016 64Bit Spanish MLF X20-42809.ISO	25/1/2018 12:09:31	5/2/2016 16:42:06	25/1/2018 12:09:31	
SW DVDS Project Pro 2016 648it Spa.	C:\Service\SW_DVD5_Project_Pro_2016_648it_Spanish_MLF_X20-42706.ISO	25/1/2018 12:10:54	11/11/2016 17:00:16	25/1/2018 12:10:54	
1 SALUD PUBLICA.Ink	C:\Service\1 SALUD PUBLICA.ipg	25/1/2018 12:15:29	27/1/2016 9:47:01	25/1/2018 12:15:29	
logo_espoch.ink	C:\Service\Jogo_espoch.png	25/1/2018 12:15:30	22/6/2016 15:27:56	25/1/2018 12:15:30	
Service.Ink	C:\Service	25/1/2018 12:09:21	25/1/2018 12:18:21	25/1/2018 12:18:21	
0603960535.lnk	D: \27ENERO \SESION 3\(0603960535	27/1/2018 20:09:01	27/1/2018 20:09:02	27/1/2018	
SESION 3 (2).Ink	D: \27ENERO \SESION 3	27/1/2018 19:35:19	27/1/2018 19:35:20	27/1/2018	
SESION 3.Ink	D:\27ENERO\SESION 3	27/1/2018 19:35:19	27/1/2018 19:35:20	27/1/2018	
17_00_0603960535_20180127_2001.lnk	C:\Users\FSP-UINL02N21\Documents\17_00_0603960535_20180127_2001.pdf	27/1/2018 20:01:01	27/1/2018 20:01:41	27/1/2018 20:01:01	
0604391763.lnk	D:\enero 28\SESION11\0604391763	28/1/2018 11:26:47	28/1/2018 11:26:48	28/1/2018	
07.lnk	D:\DATOS\07	28/1/2018 15:12:34	28/1/2018 15:12:36	28/1/2018	
27ENERO.ink	D:\27ENERO	27/1/2018 10:33:46	27/1/2018 10:33:48	28/1/2018	
DATOS.Hk	D: VDATOS	28/1/2018 15:03:48	28/1/2018 15:03:50	28/1/2018	
enero 28.ink	D: lenero 28	28/1/2018 9:54:12	28/1/2018 9:54:14	28/1/2018	
SESION11.ink	D: jenero 28/SESION11	28/1/2018 10:31:19	28/1/2018 10:31:20	28/1/2018	
Documentos.Ink	C: Users/FSP-UINL02N21/Documents	25/1/2018 11:53:31	28/1/2018 20:04:44	28/1/2018 20:04:44	
Nueva carpeta.ink	C:\Users\FSP-UINL02N21\Documents\Nueva carpeta	28/1/2018 20:04:44	28/1/2018 20:04:44	28/1/2018 20:04:44	
EZAnalyze3.lnk	C: {Users {FSP-UINL02N21}Downloads {EZAnalyze 3.xls	29/1/2018 9:02:18	29/1/2018 9:02:20	29/1/2018 9:02:18	
EZAnalyze3 (2).lnk	C: Users/FSP-UDIL02N21/AppData/Roaming/Microsoft/Complementos/EZAnaly	29/1/2018 9:02:49	29/1/2018 9:02:53	29/1/2018 9:02:49	
Complementos.Ink	C: Users/FSP-UINL02N21/AppData/Roaming/Microsoft/Complementos	25/1/2018 12:35:29	29/1/2018 9:02:53	29/1/2018 9:02:53	
Descarpas lok	C:\Users\FSP-UDIL02N21\Downloads	25/1/2018 11:53:31	29/1/2018 9:09:07	29/1/2018 9:09:07	

Fig. 2.45. Ubicación de los accesos directos e información relevante para el análisis de los accesos directos.

De igual manera al mismo tiempo, se informará en donde está la carpeta ubicada, es decir Windows File Analizer, tiene la función de analizar los accesos directos. (Fig. 2.46.). Si tiene acceso a la carpeta Register igualmente se puede obtener toda la información.

📼 - 🖻 🌲 📾 - 🕿 - 🖂 🧑					
SA - Recent					
Shortcut Analysis				Repor	t
Directory: C: Users (FSP-UDNL02NG	11 AppData (Roaming (Microsoft (Windows (Recent				
Volume serial: 8C22-929C					
Volume label:					
Flename	Linked path	Created	Written	Last Accessed	
DJ-RB (D).Ink	D:\	1/1/1980	1/1/1980	1/1/1980	
Unidad US8 (D).Ink	D:\	1/1/1980	1/1/1980	1/1/1980	
SERIALink	D:\SERIAL.bxt	25/1/2018 8:10:54	25/1/2018 10:45:25	25/1/2018 8:10:54	
CEDA_X64FREV_ES-ES_DV5 (D).hk	D:\	23/1/2018 11:04:56	25/1/2018 11:08:23	25/1/2018 11:08:23	
Disco local (C) (2).Ink	C:\	18/3/2017 6:40:20	25/1/2018 12:09:27	25/1/2018 12:09:27	
SW_DVD5_Visio_Std_2016_64Bit_Spanis	C:\Service\SW_DVD5_Visio_Std_2016_648it_Spanish_MLF_X20-42809.tSD	25/1/2018 12:09:31	5/2/2016 16:42:06	25/1/2018 12:09:31	
SW_DVD5_Project_Pro_2016_64Bit_Spa	C:\Service\SW_DVD5_Project_Pro_2016_64Bit_Spanish_MLF_X20-42706.ISO	25/1/2018 12:10:54	11/11/2016 17:00:16	25/1/2018 12:10:54	
1 SALUD PUBLICA.Ink	C:\Service\1 SALUD PUBLICA.jpg	25/1/2018 12:15:29	27/1/2016 9:47:01	25/1/2018 12:15:29	
E logo_espech.lnk	C:\Service\jogo_espoch.png	25/1/2018 12:15:30	22/6/2016 15:27:56	25/1/2018 12:15:30	
E Service.Ink	C:\Service	25/1/2018 12:09:21	25/1/2018 12:18:21	25/1/2018 12:18:21	
0603960535.lvk	D:\27ENERO\SESION 3\0603960535	27/1/2018 20:09:01	27/1/2018 20:09:02	27/1/2018	
E SESION 3 (2).Ink	D:\27ENERO\SESION 3	27/1/2018 19:35:19	27/1/2018 19:35:20	27/1/2018	
E SESTON 3.Ink	D:\27ENERO\SESION 3	27/1/2018 19:35:19	27/1/2018 19:35:20	27/1/2018	
17_00_0603960535_20180127_2001.lnk	C:\Users\FSP-UINL02N21\Documents\17_00_0603960535_20180127_2001.pdf	27/1/2018 20:01:01	27/1/2018 20:01:41	27/1/2018 20:01:01	
0604391763.lnk	D:/enero 28/SESTON11/0604391763	28/1/2018 11:26:47	28/1/2018 11:25:48	28/1/2018	
E 07.lnk	D:\DATOS\07	28/1/2018 15:12:34	28/1/2018 15:12:36	28/1/2018	
27ENERO.Ink	D:\27ENERO	27/1/2018 10:33:46	27/1/2018 10:33:48	28/1/2018	
0 DATOS.ink	D:\DATOS	28/1/2018 15:03:48	28/1/2018 15:03:50	28/1/2018	
enero 28.lnk	D:\enero 28	28/1/2018 9:54:12	28/1/2018 9:54:14	28/1/2018	
SESION11.Ink	D:\enero 28\SESION11	28/1/2018 10:31:19	28/1/2018 10:31:20	28/1/2018	
Documentos.ink	C:\Lisers\PSP-LIIN.02N21\Documents	25/1/2018 11:53:31	28/1/2018 20:04:44	28/1/2018 20:04:44	
Nueva carpeta.ink	C:\Users\PSP-UINL02N21\Documents\Nueva carpeta	28/1/2018 20:04:44	28/1/2018 20:04:44	28/1/2018 20:04:44	
EZAnalyze3.lnk	C:\Users\PSP-UINL02N21\Downloads\EZAnalyze3.xls	29/1/2018 9:02:18	29/1/2018 9:02:20	29/1/2018 9:02:18	
EZAnalyze3 (2).lnk	C: \Users\FSP-UINL02N21\AppData\Roaming\Microsoft\Complementos\EZAnaly	29/1/2018 9:02:49	29/1/2018 9:02:53	29/1/2018 9:02:49	
£ Complementos.Ink	C: \Users\PSP-UINL02N21\AppData\Roaming\Microsoft\Complementos	25/1/2018 12:35:29	29/1/2018 9:02:53	29/1/2018 9:02:53	
Descargas.ink	C:\Lisers\FSP-UIN.02N21\Downloads	25/1/2018 11-53-31	29/1/2018 9:09:07	29/1/2018 9-09-07	

1845

Fig. 2.46. Ubicación exacta de los archivos utilizando Windows File Analizer.

2.5.6. MiTec E-mail History Browser



1850 *Fig. 2.47.* Acceso al histórico del correo por medio de MiTec E-mail History Browser.

Permite acceder al historial del correo Outlook Express, Windows Mail, Windows Live Mail, Mozilla Thunderbird; y 1855 posibilita visualizar los correos sin entrar en el fichero (Fig. 2.48.); lo que realiza es una extracción.



Fig. 2.48. Acceso al histórico de correo de Outlook Express, Windows Mail, Windows Live Mail, Mozilla Thunderbird y visualiza los correos sin entrar en el fichero.

Si el usuario no está utilizando el correo, se realiza una extracción en modo lectura, evidentemente se obtiene las cabeceras y se podrá observar: correos, fechas, tamaños que se consigue del

1865 historial; es muy importante si se encuentra un tcp y no se desea abrirlo ver las cabeceras y elegir los correos necesarios.

En resumen sobre los Artefactos, se destaca RegRipper, por su versatilidad a la hora de parsear cualquier fichero del registro; Windows Recovery Registry por ser simple, permite imprimir 1870 pantallas que los usuarios observen y no accede a un intérprete de un archivo, Bulk Extractor por su parte evita buscar cosas que estén en el disco duro, por ejemplo correos electrónicos; sobre la Papelera de Reciclaje se enfatiza su utilidad porque no hay muchas herramientas que permiten recuperar ficheros borrados, etc., lo 1875 importante es saber la función de la herramienta, el Prefetch funciona para todo el tema de propiedad intelectual. Por otra parte, el USBDeview en combinación con otras herramientas, permite tener un control exhaustivo de lo que hay en las máquinas, por ejemplo; en cuanto a las fugas de información, así como los 1880

Artefactos y Contraseñas; Dialupass, Network Password Recovery, Messenger, MessenPass y Navegadores, el WebBrowserPassView y temas de correo MailPassView, como Metadatos se destaca Shortcut Analizer, en la cual se observa la cantidad de Artefactos que están en funcionamiento.

2.6. Creación de un Timeline

1885

Una línea de tiempo es una forma de plasmar una lista de eventos en orden cronológico, a veces descrito como un hito del proyecto. Es típicamente un diseño gráfico que muestra una línea con anotaciones de fechas, junto a los eventos marcados en los puntos donde habrían ocurrido, por ejemplo: se ha realizado un viaje, y se tienen hitos de donde se detuvieron, en donde se alimentaron, donde se realizó una llamada de teléfono, en qué lugar se cargó la gasolina. Estos corresponden a diferentes hitos en una cronología de tiempo (Fig. 2.49.).



Fig. 2.49. Hitos de una persona para ir del Parque Sesquicentenario a la ESPOCH. Fuente: <u>http://www.mapsdirections.info/mapea-mi-ruta/</u>

Se dispone de una carta figurativa como la que utilizó Napoleón Bonaparte (Fig. 2.50.), para las batallas y estrategias que 1905 implementaba, así se tenía definido una línea de tiempo establecida que especificaba: donde paraba, donde tenía que comer, donde correspondía atacar y evidentemente al trasportar los datos al mundo actual permite conocer los puntos cronológicos que ocuparon.



Fig. 2.50. Carta figurativa utilizaba Napoleón para todas sus batallas. *Fuente:*

https://upload.wikimedia.org/wikipedia/commons/2/29/Minard.png

Cabe indicar que, al pasar estos datos a digital, o al mundo de los ordenadores; se tendrá un timeline, especificando cuando ingresó, que países y que fechas (Fig. 2.51.).



1915 *Fig. 2.51.* Línea de Tiempo o Cronograma para Citadel botnet con clave de acceso 4DF1... ACE3.

Fuente: <u>http://oa.upm.es/38772/1/PFC_EDUARDO_RUIZ_AZOFRA_20</u> <u>15.pdf</u>

1920

1910

Un timeline se lo puede efectuar de ficheros, permisos, usuarios, Máster File Table (Tabla Maestra de Archivos), por ejemplo: se va a realizar la creación de un timeline con Excel, para 1925 los cual se debe tener en cuenta las ventajas e inconvenientes, los datos que permiten recoger la información y realizar cálculos son:

- Posibilidad infinita de cálculo
- Gráficos
- Estadísticas
- 1930 Programación
 - Integración

Algunos inconvenientes que se podrán observar son:

- Limitación a los recursos por hardware
- No es una base de datos, así que el inconveniente es trabajar con una línea de tiempo muy grande.
 - Limitación por hoja 1.048.576 filas por 16.384 columnas.

Ejemplo: Extraer un listado de todos los subdirectorios del disco

- 1940 duro, como se indica en la Fig. 2.52., es decir se utiliza la combinación de teclas "/q" lo que permitirá obtener quién es el propietario del fichero así como filtrar por fechas y se guardarán en un archivo que se llama resultado.txt, así que una vez que se posea este fichero en Excel, se dispone de una tabla dinámica que en la
- 1945 parte izquierda se llama Informe de Actividad (Etiquetas de fila, Cuenta de Fichero), y en la parte derecha se dispone la gráfica de cuantos Administradores, ficheros y totales se tiene; todo esto es un timeline básico pero muy funcional y se podrá ubicar macros así como la opción Imprimir.





Fig. 2.52. Listado de un timeline el disco duro de todos los subdirectorios en Excel.

CAPÍTULO III

FRAMEWORK FORENSE

Un framework forense es un entorno de trabajo que dispone de utilidades y programas con objeto de facilitar la tarea forense, en 1960 todos sus aspectos como: adquisición, preservación y análisis (Gervilla Rivas, 2014). Varios de los framework se ofertan con el código fuente y el lenguaje de programación en Python.

3.1. Digital Forensics Framework

- 1965 El framework más conocido es el Digital Forensics Framework (www.digital-forensic.org); dispone de dos versiones: una gratuita (Fig. 3.1.) y otra de pago que dispone de soporte y permite, en todo momento, trabajar en un entorno gráfico en base a comandos y botones para poder hacer una adquisición de un disco
- 1970 duro; que se puede clonar, hacer revisión para ver el sistema de ficheros y buscar los hive.



3.2. Xplico

El framework Xplico (<u>www.xplico.org</u>); nos permite capturar el tráfico de red (Fig. 3.2.).

Xplico es un framework que permite obtener de un tráfico de

1980 red los correos electrónicos que circulan (Fig. 3.3.), una especie de filtrado y en consola gráfico se ilustra el resultado.



Fig. 3.2. Framework Xplico. Fuente: <u>http://www.xplico.org/</u>

1985

El resultado al realizar con el framework Xplico se podrá observar la información clasificada de las páginas web, los .html, las imágenes que circulan por la red como videos, audio, ftp, así como geolocalizarlo (Fig. 3.4.). Se incorpora un script que permite 1990 convertir a fichero .kml para ejecutarlo desde networking.

Xplico Ir	nterface				User: d
leip Log	out				
Cases	Search:		Go		
Sols	Date	Subject	Sender	Receivers	Size
-	2007-08-14 11:06:50	*****SPAM***** Magic is real	"Shannon Palacios" < shraga.davenpo	<into@iserm.com></into@iserm.com>	22907
Email	2007-08-14 11:03:50	*****SPAM***** Ladies will love you	"Tania Moreno" <pkcensorial@mone< td=""><td>"15cd67a3" <15cd67a3@iserm.com></td><td>3692</td></pkcensorial@mone<>	"15cd67a3" <15cd67a3@iserm.com>	3692
Sip	2007-08-14 11:02:50	Sony for being late	"Bridgett" <tajnireiwfcs@advantexm< td=""><td>"Cleo Sanchez" <yoke@iserm.com></yoke@iserm.com></td><td>2393</td></tajnireiwfcs@advantexm<>	"Cleo Sanchez" <yoke@iserm.com></yoke@iserm.com>	2393
Moh	2007-08-14 08:24:10	This basic strategic insight supplied the factics t	"Daniel Perth" < Daniel836@ecomme	a618f5cf@iserm.com	2303
web	2007-08-14 08:20:35	You would have been a formidable team.	"Carmela Fomenko" < Fomenkowig@	<yoke@iserm.com></yoke@iserm.com>	5660
Images	2007-08-14 08:18:34	They talked for five or ten minutes and then I h	Gustavo Breck" <gustavo_breck@< td=""><td><howledabstracted@iserm.com></howledabstracted@iserm.com></td><td>2378</td></gustavo_breck@<>	<howledabstracted@iserm.com></howledabstracted@iserm.com>	2378
Printer	2007-08-14 08:12:29	Accept Credit Cards on Your Web Site Today.	"Julie Amomonpon" <julie_amomon< td=""><td><outplaying@iserm.com></outplaying@iserm.com></td><td>2240</td></julie_amomon<>	<outplaying@iserm.com></outplaying@iserm.com>	2240
	2007-08-14 08:04:58	This report indicates which shows were watch	"Kingman Mulchan" <mulchan@stef< td=""><td>beforehand@iserm.com</td><td>2285</td></mulchan@stef<>	beforehand@iserm.com	2285
нtр	2007-08-14 08:04:41	Returned mail: see transcript for details	Mail Delivery Subsystem <mailer-d <="" td=""><td><hucsotrmv@iserm.com></hucsotrmv@iserm.com></td><td>5021</td></mailer-d>	<hucsotrmv@iserm.com></hucsotrmv@iserm.com>	5021
Mms	2007-08-14 08:04:34	Returned mail: see transcript for details	Mail Delivery Subsystem <mailer-d <="" td=""><td><pafthsmqc@iserm.com></pafthsmqc@iserm.com></td><td>5342</td></mailer-d>	<pafthsmqc@iserm.com></pafthsmqc@iserm.com>	5342
Cooldon	2007-08-14 08:04:33	Re: Hallo!	"Abel Chaney" <a-1 @adultcashflow.<="" td=""><td><solace@iserm.com></solace@iserm.com></td><td>1377</td></a-1>	<solace@iserm.com></solace@iserm.com>	1377
Seowap	2007-08-14 08:04:31	Delivery Status Notification (Failure)	"Mail Delivery System" <mailer-dae< td=""><td>zylqsps@iserm.com</td><td>4552</td></mailer-dae<>	zylqsps@iserm.com	4552
	2007-08-14 08:04:31	*****SPAM***** But the way SATA has been der	"melica soo" <sooltjg@photoesc.com< td=""><td><a618f5cf@iserm.com></a618f5cf@iserm.com></td><td>8125</td></sooltjg@photoesc.com<>	<a618f5cf@iserm.com></a618f5cf@iserm.com>	8125
	2007-08-14 08:04:30	*****SPAM***** The girl eluded us.	"Mellissa Goedde" <goeddejenx@we< td=""><td><pre><perishedcloudiness@iserm.com></perishedcloudiness@iserm.com></pre></td><td>4229</td></goeddejenx@we<>	<pre><perishedcloudiness@iserm.com></perishedcloudiness@iserm.com></pre>	4229
	2007-08-14 08:04:28	About last night	"Crystal Hamilton" <arismenidezory< td=""><td>"Steve" <has@iserm.com></has@iserm.com></td><td>2398</td></arismenidezory<>	"Steve" <has@iserm.com></has@iserm.com>	2398
	2007-08-14 08:04:28	*****SPAM***** Fwd: Thanks, we are accepting	"Drew Christensen" <lgnaciomercur< td=""><td><howledabstracted@iserm.com></howledabstracted@iserm.com></td><td>6263</td></lgnaciomercur<>	<howledabstracted@iserm.com></howledabstracted@iserm.com>	6263
	2007-08-14 08:04:28	Webster, Nesta - "World Revolution", London,	("wandersom Nyland" <wandersom@< td=""><td> deforehand@iserm.com></td><td>5258</td></wandersom@<>	 deforehand@iserm.com>	5258
	2007-08-14 08:04:26	Just keep in touch	"Goldie Sanchez" <balstoreoamm@< td=""><td>"Lisandra" <guyanayoke@iserm.cor< td=""><td>2268</td></guyanayoke@iserm.cor<></td></balstoreoamm@<>	"Lisandra" <guyanayoke@iserm.cor< td=""><td>2268</td></guyanayoke@iserm.cor<>	2268
	2007-08-14 08:04:24	AUTHENTIC VIAGRA AND CIALIS	"Sales Department" <sales@design< td=""><td>"Luiz Everson" <kxtvwy@iserm.com< td=""><td>1387</td></kxtvwy@iserm.com<></td></sales@design<>	"Luiz Everson" <kxtvwy@iserm.com< td=""><td>1387</td></kxtvwy@iserm.com<>	1387
	2007-08-14 08:04:24	*****SPAM***** Fwd: Thank you, we are ready t	"Heath Randall" <demetriuselastom< td=""><td><outplaying@iserm.com></outplaying@iserm.com></td><td>6109</td></demetriuselastom<>	<outplaying@iserm.com></outplaying@iserm.com>	6109
	2007-08-14 08:04:23	Undeliverable: Thanks, we are ready to lend yo	"System Administrator" <administra< td=""><td><jjowiagwstl@iserm.com></jjowiagwstl@iserm.com></td><td>4962</td></administra<>	<jjowiagwstl@iserm.com></jjowiagwstl@iserm.com>	4962

Fig. 3.3. Interfaz Xplico. Fuente: <u>http://www.xplico.org/wp-</u> <u>content/uploads/2008/11/xwi_emails_list.png</u>

1995



Fig. 3.4. Geolocalización con Xplico. Fuente: <u>http://www.xplico.org/wp-</u> content/uploads/2008/11/xwi_geomap.png

3.3. Autopsy

La herramienta Autopsy (<u>www.sleuthkit.org/autopsy/</u>), es una plataforma forense digital e interfaz gráfica de The Sleuth Kit y

2000 otras herramientas forenses digitales. Es utilizada por los encargados de hacer cumplir la ley, militares y examinadores corporativos para investigar lo que sucedió en una computadora. Incluso puede usarlo para recuperar fotos de la tarjeta de memoria de su cámara (SleuthKit-Autopsy, 2003), su uso es destinado en el sistema
2005 operativo Linux (Fig. 3.5. y Fig. 3.6.).



Fig. 3.5. Herramienta Autopsy.

CASE	ALLERY	HOST GALLER	HOST	MANAGER	
o /	t name heneype	b ot.hdo8.dd-0-0	fs type oxt	details	
O /boot/	heneyp	ot.hdal.dd.0-0	ext	dotails	
(hose/	heneya	ot.hda6.dd-0-0	ext	details	
G /usr/	hanaya	ot.hda5.dd-0-0	ext	details	
🔿 /var/	heneye	at.hda7.dd+0+0	oxt	details	
🔿 амар	heneyp	ot.hdo9.dd+0+0	swap	details	
AN	LYZE		• <u> </u>	ORE HORT	

Fig. 3.6. Análisis con Autopsy.

2010 Autopsy en Windows (Fig. 3.7.), tiene las imágenes clonadas y se puede observar la estructura de directorios como si fuera un FTK y agrupar; es decir se puede extraer por tipo de ficheros, imágenes, videos, audio; capaz de pre visualizar y buscar toda información para extraer los bookmarks, cookies, el historial de web, las descargas que
2015 se han realizado desde ese ordenador o máquina clonada, los documentos recientes, los programas instalados y con un visualizador hexadecimal; así se podrá ir creando y generando informes o reportes.

xpinbox1 - Autopsy 3.0.0b3		- -					Inc. Min	- ×
ile Edit View Jools Window Help								
👩 Close Case 📥 Add Image 🚡 Generate Repor	t		4	• Keyword	Lists - Scorch			Q.
e >	Directory Listing						in.	
anages	Vip-sp3-v4.001/vol2 Table View Thumbnal View							15 Resul
⊕ ∰ xp-sp3-v4.001	Name	Mod. Time	Change Time	Access Time	Created Time	Size	Hags(Dr)	Pied
 iii vol1 (Unallocated: 0-62) iii vol3 (MTRF (In-075) 47, 810 3140) 	floot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:02		8192	Allocated	Alect
Stard	Sectord .	2012-01-20 12 09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Alto
Documents and Settings	R or Fig	2012/01/02 12:00:02	1012-01-20 12:00:02	2012-01-20 12:00:02	20112-01-2012205-02	10002764	Allocated	Abres
🕀 🎉 Program Mies	- ANY IS		2012-01-10 12-09-00	2012-01-20 12-09-00			Abused	1
- 🐊 System Volume Information	- Beer					10007116	HILLOU	1
IB D WINDOWS	- Brit-Thett	2012-01-20 12:09:00	2012-01-20 12:09:00	2012-01-20 12:09:05	2912-01-2012:09:03	40%	Allocated	ARCO
SCrphanFiles	sSecure:\$505	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Altro:
iii vol3 (Unaliocated: 8193150-10485215)	BUpCase	2012-01-20 12:09:00	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20-12:09:00		Allocated	Alco
- Weves	Svolume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09(08	2012-01-20 12:09-03	0	Allocated	Aloca
Inson	AUTOEXEC.BAT	2012/01/20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alter
Videos	bootani	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Alco
- Audo	CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alto
II- 🖏 Documents	Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:45	2012-01-20 12:10:41	.56	Allocated	Altor
E Recent Ples	10.515	2012-01-20 12:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49		Allocated	Alere
- B Final Day	MEDICE EVE	2012-01-20 17:20-49	2012-01-20 17:20-49	2012-01-20 17:20:48	2010-01-20 17:20-40		Alicated	Alera
Final Day - 1	Recounts	LULC OF NO TRADITS	2012-01-00 17:20/17	DULCOV SU L'OLDEVY	2012-04-20 17:04-17	Provide State	HECOLD .	
e Pinal Day - 2	MIDEIDELCOM	2006-04-13 22:13:04	2012-01-2012/11/07	Tang-at-sh remains	2010-04-10 22110-04	14/004	witcosed	TALCO.
Final Day - 3	ntdr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2358-04-14 00:01:44	250048	Allocated	Alcci
8 Final Day - 5	pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Alco
Pinal Day - 6	Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Alter
Results	🐊 System Volume Information	2012-01-20 17:21:37	2012-01-20 17 21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alter
🖶 🔟 Extracted Content	WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:45	2012-01-20 12:09:08	56	Allocated	Alco
- 💐 Bookmarks (174)	BOrohanFiles	0000-00-00 00:00:00	0000-00-00 00-00-00	0000-00-00 00:00:00	0000-00-00 00:00 00	0	Allocated	Alect
- 🍪 Cookies (1911)	()							
Web History (1218)	Transformer I May May Transform	Christel Harris						
Operationals (30) Recent Documents (72)	Page: 1 of 3	age (Go to	Pages					
Sintake Program (72) Government Attached (9) Government Attached (9) Government Hits Government Hits Government Hits Hanhaet Hits	Buccoccc: 46 55 46 55 Buccoccc: 70 00 46 55 46 55 Buccoccc: 70 00 46 55 46 46 7 56 56 56 <td>P EC 66 FD X5 7 85 FD A4 C1 8 64 85 45 0C 8 64 85 45 1C 2 64 76 84 52 2 64 70 64 84 2 64 70 64 84 2 64 70 64 84 2 64 70 64 84 7 76 64 70 30 8 76 64 88 10 9 80 64 88 30 </td> <td>FF FF 00 00 25 04 8.2 02 00 00 52 01 04 8.2 02 01 05 00 00 52 01 04 8.5 06 82 01 05 01 00 06 80 06 8.1 66 82 64 00 00 00 00 00 06 80 00 00 00 06 80 00 00 00 06 80 00 00 00 06 80 00 00 00 07 08 60 42 06 07 08 60 83 83</td> <td>11 0.6 6.6 5.3 0.3 0.1 7.0 2.6 0.0 3.0 0.5 0.4 0.0 0.0 6.6 3.9 7.5 1.4 0.0 6.6 3.3 7.5 1.4 0.0 0.0 6.6 3.3 7.6 4.6 0.0 <</td> <td>rus.s. rvv. f. f. f. f. f. f. v. f. N. f. v. f. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. f</td> <td>23 </td> <td></td> <td></td>	P EC 66 FD X5 7 85 FD A4 C1 8 64 85 45 0C 8 64 85 45 1C 2 64 76 84 52 2 64 70 64 84 2 64 70 64 84 2 64 70 64 84 2 64 70 64 84 7 76 64 70 30 8 76 64 88 10 9 80 64 88 30	FF FF 00 00 25 04 8.2 02 00 00 52 01 04 8.2 02 01 05 00 00 52 01 04 8.5 06 82 01 05 01 00 06 80 06 8.1 66 82 64 00 00 00 00 00 06 80 00 00 00 06 80 00 00 00 06 80 00 00 00 06 80 00 00 00 07 08 60 42 06 07 08 60 83 83	11 0.6 6.6 5.3 0.3 0.1 7.0 2.6 0.0 3.0 0.5 0.4 0.0 0.0 6.6 3.9 7.5 1.4 0.0 6.6 3.3 7.5 1.4 0.0 0.0 6.6 3.3 7.6 4.6 0.0 <	rus.s. rvv. f. f. f. f. f. f. v. f. N. f. v. f. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. rvs.rvv. f	23 		

Fig. 3.7. Autopsy en Windows.

Fuente: <u>http://www.sleuthkit.org/autopsy/images/v3/overview.png</u>

2020 3.4. Volatility

Es una colección de herramientas:

(http://www.volatilityfoundation.org/25); implementado en Python bajo la GNU (Fig. 3.8.), para la extracción de recursos digitales de la memoria volátil (RAM).

2025

Las técnicas de extracción se realizan completamente independiente del sistema que está siendo investigado, pero ofrecen visibilidad del estado de ejecución del sistema. • volatility foundation • Fig. 3.8. Volatility. Fuente: <u>http://www.volatilityfoundation.org/</u>

2030

2045

Es un framework que solamente es capaz de analizar la memoria RAM, funciona para diferentes sistemas operativos (Fig. 2035 3.9.), muy amplio.



Fig. 3.9. Imágenes de Windows, MAC, Linux, Android. Fuente: <u>https://github.com/volatilityfoundation/volatility/wiki</u>

2040 Volatility no es gráfico; al ejecutar el volatility juntamente con el lenguaje de programación Python con "-f" que significa extraer las características del fichero de memoria "vol.py" y sacar el árbol de procesos.

Con volatility se extrae directamente la información de un fichero de memoria (Fig. 3.10.).

Name	Pid	PPid	Thds	Hnds	Time	
0x810b1660:System	4	0	58	379	1970-01-01	00:00:00
. 0xff2ab020:smss.exe	544		3	21	2010-08-11	06:06:21
0xff1ec978:winlogon.exe	632	544	24	536	2010-08-11	06:06:23
0xff255020:lsass.exe	688	632	21	405	2010-08-11	86:86:24
0xff247020:services.exe	676	632	16	288	2010-08-11	06:06:24
0xff1b8b28:vmtoolsd.exe	1668	676	5	225	2010-08-11	06:06:35
0xff224020:cmd.exe	124	1668	0		2010-08-15	19:17:55
0x80ff88d8:svchost.exe	856	676	29	336	2010-08-11	06:06:24
0xff1d7da0:spoolsv.exe	1432	676	14	145	2010-08-11	06:06:26
0x80fbf910:svchost.exe	1028	676	88	1424	2010-08-11	06:06:24
0x80f60da0:wuauclt.exe	1732	1028		189	2010-08-11	86:07:44
0x80f94588:wuauclt.exe	468	1028		142	2010-08-11	06:09:37
0xff364310:wscntfy.exe	888	1028		40	2010-08-11	06:06:49
0xff217560:svchost.exe	936	676		288	2010-08-11	86:86:24
0xff143b28:TPAutoConnSvc.e	1968	676		106	2010-08-11	06:06:39
0xff38b5f8:TPAutoConnect.e	1084	1968		68	2010-08-11	06:06:52
0xff22d558:svchost.exe	1088	676		93	2010-08-11	06:06:25
0xff218230:vmacthlp.exe	844	676		37	2010-08-11	06:06:24
0xff25a7e0:alg.exe	216	676		120	2010-08-11	06:06:39
0xff203b80:svchost.exe	1148	676	15	217	2010-08-11	06:06:26
0xff1fdc88:VMUpgradeHelper	1788	676		112	2010-08-11	06:06:38
0xfflecda0:csrss.exe	608	544	10	410	2010-08-11	06:06:23
0xff3865d0:explorer.exe	1724	1708	13	326	2010-08-11	06:09:29
. 0xff374980:VMwareUser.exe	452	1724	8	207	2010-08-11	06:09:32
. 0xff3667e8:VMwareTray.exe	432	1724		60	2010-08-11	06:09:31

Fig. 3.10. Ejecución de Volatility.

Fuente: Curso de Informàtica forense i evidències digitals, realizada por Pedro Sánchez Cordero, Universitat Rovira i Virgili, Catalunya-España, 2015.

2050

La información relevante se puede localizar en el siguiente enlace:

http://conexioninversa.blogspot.com.es/2009/02/forensics-con-

volatility.html

- 2055 Entre las características que se pueden extraer están las siguientes:
 - Procesos que se estaban ejecutando.
 - Tipo de sistema, fecha y hora.
 - Puertos abiertos.
- **2060** Puertos conectados.
 - Claves del registro utilizadas en los procesos.

- Módulos del Kernel.
- Extracción de ejecutables.
- Mapa físico de offsets a direcciones virtuales.
- Direccionamiento de memoria por proceso.
 - DLLs cargadas por proceso.
 - Ficheros cargados por procesos.

En conclusión, hay varios frameworks en entorno gráfico, de 2070 los cuales se mencionan los más utilizados, sin entorno gráfico, Volatility se utiliza en temas de adquisición y análisis de memoria, Digital Forensics Framework es utilizado para temas de tráfico de red, Xplico para todo lo referente a Windows.

2075 3.5. ReKall Memory Forensic Framework.-

2080

(www.rekall-forensic.com); es un framework forense de memoria que proporciona una solución integral para los que responden a incidentes y analistas forenses. Desde herramientas de adquisición de vanguardia hasta el framework de análisis de memoria de código abierto más avanzado. Rekall es la única herramienta de análisis de memoria de código abierto que puede funcionar con el archivo de página de Windows y los archivos asignados (Fig. 3.11.).

2085 Rekall igualmente incluye una solución de adquisición completa (en el complemento aff4acquire) que permite la adquisición del archivo de paginación y todos los archivos mapeados relevantes, lo hace al ejecutar una rutina de triage durante la adquisición (Darknet, 2018).



2090

Fig. 3.11. ReKall Memory Forensic Framework. Fuente: <u>http://www.rekall-forensic.com/</u>

3.6. Mimikatz

2095 Mimikatz (<u>http://blog.gefntilkiwi.com/mimikatz</u>); es un framework que permite trabajar (Fig. 3.12.), pero utilizando un

entorno propio, muy parecido a Volatilitity que extrae procesos de memoria, obtiene contraseñas, etc. Es un framework, que va a permitir obtener información muy relevante.



Fig. 3.12. Mimikatz. Fuente: <u>http://blog.gentilkiwi.com/mimikatz</u>

2105 3.7. NetworkMiner 2.0.-

Una rama de la informática forense se encarga del estudio de las comunicaciones y redes, con el fin de lograr una captura de tráfico, registros y análisis de eventos de red para descubrir el origen de un incidente o ataque o ser utilizado luego como evidencia digital

2110 (Paus, 2016). Este análisis puede ser realizado en tiempo real o mediante el análisis de los archivos capturados (.caps). A partir de este estudio se pueden entender características de la red, quien está usándola, identificar picos de tráficos, actividad maliciosa, uso de protocolos inseguros o cualquier comportamiento anómalo.

2100

En su primera versión, NetwokMiner se instauró como una de las herramientas más utilizadas para el sniffing y análisis de capturas en distintas entidades judiciales y CERT del mundo. En esta última versión, 2.0, agrega otras funcionalidades (Fig. 3.13.).



Fig. 3.13. Logotipo NetworkMiner 2.0.

El entorno dependiendo del ambiente en que se realice la captura, se podrán plantear distintos escenarios; en ocasiones será 2125 necesario utilizar dispositivos que posean Port Mirroring o SPAN (en plataformas Cisco), generando un ARP poisoning o utilizando un TAP de red.

Si es usuario de Microsoft Windows se puede descargar 2130 (https://www.netresec.com/?download=NetworkMiner), y es necesario tener que instalar ".NET Framework 3.5". Esta aplicación se puede ejecutar en Linux, Mac OS X y FreeBSD (welivesecurity, 2016). Ejemplo: Realizar un análisis forense de redes con Wireshark,
2135 NetworkMiner 2.0 para analizar un archivo PCAP; como se indica en la Fig. 3.14., se logrará capturar el tráfico de la red (sniffer), se utilizará la herramienta Wireshark.



Fig. 3.14. Herramienta Wireshark.

2140

Inicialmente, se selecciona la interfaz de red y al dar clic sobre

Start (Fig. 3.15.).

RedHidalgo.pcap					- 0	×
File Edit View Go	Capture Analyze Statis	tics Telephony Wireless	Tools He			
	X 0 9 + + *		9.17			
Apply a deplay filter	<pre>chri-/></pre>				Expressio	an +
No. Time	Course	Destination	Orotocal	anoth tota		-
2017 29.570521	192, 168, 2, 112	34, 196, 194, 115	TI Sv1.2	231 Application Data		
2018 22 570525	192.168.2.112	34 106 104 135	T15v1.2	278 Application Date		
2010 29.570505	192.168.2.112	34, 196, 194, 135	T1.5v1.2	92 Application Data		
2020 29,612225	209.85.144.94	192,168,2,112	TCP	54 443 + 55488 [ACK] Seg=128683 Ack=2102 bin=49408 Len=0		
2021 29,664596	192,168,2,112	35,158,73.6	TOP	185 [TCP Retransmission] 55499 + 443 [PSH, ACK] Seg-225 Ack+145 Win+17152 Len+51		
2022 29.695928	35,158,73,6	192.168.2.112	TCP	54 443 + 55499 [ACX] Seg=146 Ack=277 Win=20160 Len=0		
2023 29.695967	34.196.194.135	192.168.2.112	TLSv1.2	92 Application Data		
2024 29,699345	34,196,194,135	192,168,2,112	TCP	54 443 + 55523 [ACK] Seg-3421 Ack=758 Win=30200 Len=0		1000
2025 29.704741	34,196,194,135	192.168.2.112	TLSv1.2	277 Application Data		
2026 29.704777	192.168.2.112	34.196.194.135	TCP	54 55523 + 443 [ACK] Seq+758 Ack+3644 Win+16640 Len+0		
2027 29.718356	34,196.194.135	192.168.2.112	TL5v1.2	92 Application Data		
2028 29.764870	192.168.2.112	34.196.194.135	TCP	54 55523 + 443 [ACK] Seq=758 Ack=3682 Win=16640 Len=0		
2029-29.881663	35.158.73.0	192,168.2.112	TCP	66 [TCP Dup ACK 202201] 443 - 55499 [ACK] Seq=146 Ack=277 Win=20160 Len=0 5LE=226 SRE=277		
2030 30.220023	192.168.2.112	13.32.80.50	TLSv1.2	85 Encrypted Alert		
2031 30.220687	192.168.2.112	13.32.80.50	TCP	54 55485 + 443 [FIN, ACK] Seq-367 Ack-3711 Win-16384 Len-0		
2032 30.316897	13.32.80.50	192.168.2.112	TCP	54 443 + 55485 [FIN, ACK] Seq-3711 Ack-367 Win-30464 Len-0		
2033 30.316954	192.168.2.112	13.32.80.50	TCP	54 55485 + 443 [ACK] Seq=368 Ack=3712 Win=16384 Len=8		
2034 30.317021	13.32.80.50	192.168.2.112	TCP	54 443 + 55485 [ACK] Seq=3712 Ack=368 Win=30464 Len=0		
2035 30.466337	D-LinkIn_c4:9d:76	HonHaiPr_66:66:f3	ARP	42 Who has 192.168.2.112? Tell 192.168.2.1		
2036 30.466370	HonHaiPr_66:66:f3	D-LinkIn_c4:9d:76	ARP	42 192.168.2.112 is at 68:14:01:66:66:f3		
2037 32.224113	192.168.2.112	54.149.200.38	TLSv1.2	85 Encryoted Alert		
 Frame 1: 1024 byt Ethernet II, Src. Internet Protocol User Datagram Pro QUIC (Quick UDP 1) 	tes on wire (8192 bits) HonHaiPr_66:66:f3 (68 Version 4, Src: 192.1 Itocol, Src Port: 53953 Internet Connections)	n, 1024 bytes captures 1:14:01:66:66:f3}, Dst 68.2.112, Dst: 200.8 5, Dst Port: 443	(8192 bit) 1: D-LinkIn 1:144.147) on interface 0 (4:98:76 (c0:40:56:c4:96:76)		
0000 c0 a0 bb c4 5	d 76 68 14 01 66 66 f	3 88 88 45 88	vhff			-
0010 03 f2 04 ba 4	H0 00 80 11 cd 3f c0 a	8 82 78 d1 55	p.	0		
0020 90 93 d2 c1 t	n of 14 Re ad Ra R3 c	2 84 83 22 46		22		
0010 16 at 88 fe 1	5 b9 65 1b 89 be f9 3	3 fb 22 d9 #2				
0050 af cd bd 78 4	48 33 0d 4d f8 be a9 7	d f0 28 08 7e	B.M]. (No. Contraction of the second s		
0060 d8 8f 4c 42 c	8 d6 1f 5e e2 1f 42 f	5 e6 4b ca c3LB.	BK.			
8878 45 d1 f9 96 2	13 97 48 38 Se fa 3b c	b bb 67 e8 02 E4	.HS ^.j8			
10000 f3 fe 34 ea 8	2 65 92 05 87 39 81 5	4 31 c0 e2 e54.		A		~
🔘 🖉 Redhidalgo				Packets: 2043 - Daplayed: 2043 (100.0%)	Profi	ie: Default

Fig. 3.15. Herramienta Wireshark en archivo pcap.

Para generar nuestro archivo PCAP, presionamos sobre \checkmark y para detener la captura de paquetes pulsamos \blacksquare , inmediatamente se teclea File \rightarrow Save o Save As... y se obtiene el archivo PCAP.

2150 Una vez seleccionada la interfaz que se va a utilizar para la captura, se ubican sobre NetworkMiner, File → Open, se selecciona el archivo y lo abren, La herramienta procederá a analizarlo y se podrá mostrar la información detallada, como se advierte en la siguiente imagen (Fig. 3.16.):



Fig. 3.16. Herramienta NetworkMiner.

Al consultar la etiqueta DNS se puede observar las peticiones 2160 que se han realizado sobre la red, lo cual puede ser muy útil para el análisis de malware, como por ejemplo en la detección de paneles de control estando en presencia de un bot (Fig. 3.17.).

ile Jos	ols Help											
Poap: Re	altek PCIe GBE Family Controller	(0.0.0.0) (35754968-F588-	451D-8348-0	CC 7E3CF187	F)							v 👂 Stert 🕼 Sa
osto (84)	Files (45) Images Messages	Credentials (4) Sessions (8	(DNS (18	0) Parameter	to (1012) Key	words A	inomalies				Case Panel	
iter keywa	ed.							Case sensitiv	e ExactPhrase v An	y column ~ Clear Apply	Rietane MD5	MD5
tane nr.	Tinestanp	Clent	Client Pot	Server	Server Port	IP TTL	ONS TTL time)	Transaction 10	Type	DNS Guery	NedHidalgo pcap	3b-4b 95b 352 deeb 0446 3e 916b 4d dod 742
,	2018-03-11 13:54:44 UTC-05	192 168 2 112	62950	192 168 2 1	53	64	00-02-20	0x1070	0x0005 (CNAME)	www.googleadservices.c		
6	2018-03-11 13 54 44 UTC-05	192 168 2 112	62960	152 168 2.1	53	64	00.02.28	Dx1070	De0001 (Host Address)	papead I doublectick net		
20	2018-03-11 13:54:45 UTC-05	192 168 2 112	53751	192,158,2,1	53	64	00:04:51	0x20AF	0x0005 (CNAME)	fonts astatic.com		
10	2018-03-11 13:54:46 UTC-05	192 168 2 112	53751	192 168 2.1	53	64	00:04:51	0x20AF	Dr0001 (Host Address)	ostaticades! I concile corr		
22	2018-03-11 13:54:46 UTC-05	192.168.2.112	59555	152 168 2.1	53	64	00.02.23	Dx4F3A	Di0005 (CINAME)	play google com		
1	2018-03-11 13:54:46 UTC-05	192 158 2 112	59655	192,168,2,1	53	64	00:04:58	Dx4F3A	Dr0001 (Host Address)	play I google.com		
15	2018-03-11 13:54:55 UTC-05	192.168.2.112 (Windows)	61875	192.168.2.1	53	64	00.18:30	0x695A	Di0005 (CNAME)	roaming officeapps live.c		
15	2018-03-11 13:54:55 UTC-05	192.168.2.112 (Windows)	61875	152.168.2.1	53	64	00.00.16	0x695A	De0005 (CINAME)	prod roaning 1 live com a		
5	2018-03-11 13:54:55 UTC-05	192 168 2 112 (Mindoes)	61875	192,158,2,1	13	64	00:01:48	Dx695A	0x0001 (Host Address)	us1 roaming1 live com al		
113	2018-03-11 13:54:56 UTC-05	192.168.2.112 (Windows)	64347	192.168.2.1	53	64	00:01:26	0x8978	0x0005 (CNAME)	templateservice office cc		
113	2018-03-11 13:54:56 UTC-05	192.168.2.112 (Windows)	64347	152 168 2.1	53	64	00.00.05	Gx8978	0x0005 (CN4ME)	prod omeotemplates live		
113	2018-03-11 13:54:56 UTC-05	192 168 2 112 (Windows)	64347	192,168,2,1	53	64	00.35.43	0x8978	0x0005 (CTVAME)	weu-001 onextemplates.		
113	2018-03-11 13:54:56 UTC-05	192 168 2 112 (Windows)	64347	192 168 2.1	53	64	00-00-38	0x8978	0x0001 04ost Address)	osiprod-weu-plum-001.ck		
131	2018-03-11 13:54:56 UTC-05	192.168.2.112 (Windows)	62041	152,168,2,1	53	64	00:52:31	0x8823	GL0005 (CINAME)	omentemplates content c		
121	2018-03-11 13:54:56 UTC-05	192.168.2.112 (Mindowa)	62041	192 168 2.1	53	64	02.25.02	0x5823	D-0005 (CNAME)	omextemplates content c		
131	2018-03-11 13:54:56 UTC-05	192 168 2 112 (Windows)	62041	192.168.2.1	53	64	00:00:14	0x8823	Ox0001 (Host Address)	e584 g akamaledge net		
1085	2018-03-11 13:55:06 UTC-05	192.168.2.112 (Mindows)	51175	152.168.2.1	53	64	00.00.07	Dv6DC5	0x0005 (CNAME)	detectportal firefox.com		
085	2018-03-11 13:55:06 UTC-05	192 168 2 112 (Windows)	51175	192,168,2,1	53	64	01:17:55	DisDC5	D-0005 (CNAME)	detectportal firefox com s		
085	2018-03-11 13:55:06 UTC-05	192 168 2 112 (Windows)	51175	192,168,2,1	53	64	00:00:14	DeEDC5	0x0001 (Host Address)	a 1009 diakama inet		
1085	2018-03-11 13:55:06 UTC-05	192.168.2.112 (Windows)	51175	152,168,2,1	53	64	00.00.14	Dv6DC5	Ge0001 (Host Address)	a 1009 diakamalinet		
098	2018-03-11 13:55:06 UTC-05	192 168 2 112 (Mindoers)	60683	192 168 2.1	53	64	00:01 58	0-CFEF	De0001 (Host Address)	www.google.com.ec		
102	2018-03-11 13:55:06 UTC-05	192.168.2.112 (Windows)	50570	192.168.2.1	53	64	00:00:14	0x3FB3	Dx0001 (Host Address)	a 1009.d.akamai net		
102	2018-03-11 13:55:06 UTC-05	192,168,2,112 (Windows)	50570	192,168,2,1	53	64	00:00:14	0x3F83	Ge0001 (Host Address)	e1009 diskamalinet		
107	2018-03-11 13:55:06 UTC-05	192.168.2.112 (Windows)	63203	192.168.2.1	53	64	00.00.00	0x946D	Dx0000	a 1009 d.ak.amai.net		
118	2018-03-11 13:55:07 UTC-05	192.168.2.112 (/lindows)	57998	192.168.2.1	53	64	00:00:13	0xF439	Di0005 (CNAME)	push services mosila.cor		
1118	2018-03-11 13:55:07 UTC-05	192,168,2,112 (Windows)	57998	152 168 2 1	53	64	00.00:17	0xF439	Ge0001 (Host Address)	autopush prod mozawa r		
120	2018-03-11 13:55:07 UTC-05	192.168.2.112 (Windows)	62193	152.168.2.1	53	64	00.00.17	DxBES1	De0001 (Host Address)	autopush prod mezawa r		
123	2018-03-11 13:55:07 UTC-05	192.168.2.112 (Windows)	56109	192.168.2.1	53	64	00:00:00	0x4D03	Dx0000	autopush prod mozaws r		
137	2018-03-11 13:55:08 UTC-05	192 168 2 112 (Windows)	57821	192,168,2,1	53	64	01:12:01	0x3069	(HO005 (CNAME)	cosp digicert.com		
137	2018-03-11 13:55:08 UTC-05	192.168.2.112 (Mindosea)	57821	152.163.2.1	53	64	00.13.01	0x3069	De0001 (Host Address)	cs9 was phildh net		
141	2018-03-11 13:55:08 UTC-05	192.168.2.112 (Windows)	59472	192,168,2,1	53	64	00:00:18	DKASEC	Dr0005 (CTVAME)	tiles services mozilia com *		
										,		Reload Case Files

Fig. 3.17. Análisis DNS en NetworkMiner.

2165

Sin embargo, si se analizan los archivos PCAP que pueden contener malware, se recomienda llevar a cabo el análisis sobre algún otro sistema operativo que no sea en el que se ejecuta el malware, es decir, mayormente en plataformas Linux.

2170

2175

En la solapa de anomalías se podrá encontrar información muy valiosa que puede ayudar al analista a deducir rápidamente de qué forma sucedió un determinado incidente. En la solapa Files se encuentran todos los ficheros que se están ejecutando en ese momento (Fig. 3.18.):

Networ	kt/liner 2.2									- 0	×
Ble In	ools Help										
WePcap R	eabek PCIe GBE Family Controller (0.0.0	0.0) (15754 96 8-F	588-4\$1D-	8348-CCC7E3CF187F)						v 👂 Start	III Step
Hosts (84)	Files (43) Images Messages Ciede	ritals (4) Sessie	ns (54) 0	NS (180) Parameters (1012) Keywords Anonalies					Case Panel		
Filter keyw	vord			Any column	- Clear Apply	Flenane	MDS				
Frame nr.	Flenarse	Edension	Sae	Source host	S.pot.	Destination host	D.pot	Protocol *	неснизадо розр	354034030239403445343740403	00/42
1132	push services modila com cer	cer	13968	34,208,23,114 (autopush prodimozaws net) (push services	TCP 443	192,158,2,112 (Windows)	TCP 55475	ToCetficate			
1132	DigCet SHA2 Secure Server cer	cer	1175.8	34.208.23.114 (autopush prod mozawa net) (push services	TCP 443	192,168.2.112 (Windows)	TCP 55479	ToCetticate			
1145	index html posp-response	ocsp-response	4718	192, 16:58.8 (os9 was phioth.net) (cosp.digicet.com)	TCP 80	192.168.2.112 (Windows)	TCP 55482	HtpGetNomal			
1171	services mobila con cer	oer	13758	52,41.78 152 bles r53-2 services mozila com bles service	TCP 443	192 168 2 112 (Windows)	TCP 55483	TeCetficate			
1171	DigCet SH42 Secure Server .per	cer	11768	52.41 78.152 bies r53-2 services mopila com bies service.	TCP 443	192.168.2.112 (Windows)	TCP 55483	ToCetficate			
1173	index.html[1].oosp-response	ocap-response	4718	192.16.58.8 (cs9 was phildrin ret) (cosp digloet.com)	TCP 80	192.168.2.112 (Windows)	TCP 55482	HtpGetNomal			
1185	services modila con(1) cer	oer	13798	52,41 78,752 bles r53-2 services mozila com) bles service.	TCP 443	192 168 2 112 (Windows)	TCP 55484	ToCetficate			
1185	DgCet SHA2 Secure Server [1].cer	Cer	11768	52.41 78.152 bles r53-2 services motils com bles service	TCP 443	192.168.2.112 (Windows)	TCP 55484	TeCetficate			
1208	odn.modila.net.cer	cer	13368	13.32.80 50 (dokyfu fmðufei cioudfront net) (ties-cioudfro	TCP 443	192.168.2.112 (Windows)	TCP 55405	ToCetticate			
1208	DigCet SHA2 Secure Server cer	cer	11768	13.32.80 50 (dokyfu/ImBuliel cloudfront net) (blen-cloudfro.	TCP 443	192.168.2.112 (Windows)	TCP 55485	TeCetficate			
1250	google con wo cer	cer	1 199 8	209.85 144.94 (www.google.com.ec)	TCP 443	192.168.2.112 (Windows)	TCP 55408	TeCetficate			
1250	Google Internet Authority G3 cer	Cer	1 120 B	205.85.144.54 (www.google.com.ec)	TCP 443	192.168.2.112 (Windows)	TCP 55488	TaCetticate			
1267	GTSGIAG3.ccp-response	ocap-response	463 B	172.217.2.206 [play I google con] [play google com] [www.	TCP 80	192.168.2.112 (Windows)	TCP 55491	HtpGetNomal			
1281	Index Heri FDCD355D Heri	htesi	3 230 8	185 123 227 13 (wither avera corr) (cm avera corr)	TCP 80	192.155.2.112 (Westewa)	TCP 55492	HtpGetOunke			
1338	index Hani scap-response	ocap-wapores	472.8	178.255.83 1 (scap correctoca correl	TCP 80	192.158.2 112 (Windows)	TCP 55495	HtpGatNormal			
1411	cdh.evta.con.cer	Cer	1858 B	23.47.68.194 [e11356.g akamaladge rwt] [cdn avits com e.	TCP 443	192.158.2.112 (Windows)	TCP 55500	TaCetficate			
1411	GeoTrust SSL CA - G3.cer	Cer	11078	23.47.63 194 (e11396 g alcenaedge rvet) (och avra con e.	TCP 443	192.158.2.112 (Windows)	TCP 55500	ToCatificate			
1390	index.html[1].ocsp-response	ocap-response	4718	178.255.83.1 (scap comodoca com)	TCP 80	192.168.2.112 (Windowa)	TCP 55496	HtpGatNormal			
1487	index Hani pcap response	ocap-response	1416B	23.4.43.27 [e8218.decb1.akamaledge.net] [ocep-ds.we.sy	TCP 80	192.168.2.112 (Windows)	TCP 55506	HtpGetNomal			
1672	goode con cer	OW	19278	216 St. 192 35 Swere getatic core]	TCP 443	192.168.2.112 (Westewa)	TCP 55507	ToCetRcate			
1672	Google Internet Authority G2.cer	Cer	1058 B	216.58 192.35 [www.gatatic.com]	TCP 443	192.168.2.112 (Windows)	TCP \$5507	TsCetficate			
1672	GeoTruit Global CAper	cer	897.8	216 58 192 35 Inverse gatatic core1	TCP 443	192,158,2,112 (Windows)	TCP 55507	TeCetficate			
1657	index HariEZLocsp response	ocso-response	472.8	178 255 83 1 jocsp. comodoca.com/	TCP 80	192.168.2.112 (Windowe)	TCP 55508	HtpGetNormal			
1703	ocap ocap response	ocap response	463 B	216.58 192.46 [clients google.com] [clients] google.com]	TCP 80	192.168.2.112 (Windows)	TCP 55511	HtpGetNomal			
1767	mispanel con cer	oer	1 203 B	169 54 129 21 lapi mispanel conti	TCP 443	192,168,2,112 (Windows)	TCP 55510	ToCerficate			
1767	RapidSSL RSA CA 2018 cer	cer	1 205 8	169.54 129 21 [api milpanel.com]	TCP 443	192,158,2,112 (Windows)	TCP 55510	ToCetficate			
1783	shavar services riscalla core cer	cer	1440 8	35.165.158.113 (shavar prod mozaws net) (shavar services	TCP 443	192.168.2.112 (Windows)	TCP 55513	ToCetificate			
1783	DigCet SHA2 Secure Server cer	cer	11768	35.165.158.113 Inhavar.prod mozaws netil Ishavar services.	TCP 443	192,158,2,112 (Windows)	TCP 55513	TsCetficate			
1011	index html52.oosp response	ocap-response	4718	192 15 58 8 los9 was phiodn net! loosp digicet con] btat.	TCP 80	192,155,2,112 (Windows)	TCP 55516	HtpGetNormal			
1821	index html/III.ocsp response	ocap-response	4718	192, 16 58,8 lost was phiods net! looso discert conil littat	TCP 80	192 168 2 112 (Windows)	TCP 55517	HtpGetNama			
1864	googleapis con cer	oer	10548	216.58 192.42 Isafebrowoing googleapis com	TCP 443	192,158,2,112 (Windows)	TCP 55518	ToCetficate 4			
<										Reload Case Files	

Fig. 3.18. Análisis Files en NetworkMiner.

Esta versión también permite encontrar dentro de la solapa 2180 parámetros información referida a métodos de petición HTTP, códigos de estado HTTP de respuesta, cabeceras HTTP y SMB (recursos compartidos), (Fig. 3.19.). Esto podría darnos indicios de una fuga de información o inclusive de algún código malicioso como el ransomware que esté cifrando recursos compartidos.

NetworkMiner 2.2			- a ×
File Tools Help			
MnPcap: Reatek PCIe GBE Family Controller (0.0.0.0) (357545	69 F568 461D 834B CCC7E3CF187F)		✓ ▶ Start ■ Start
Hosts (54) Files (45) Images Messages Condentials (4) 5	ansing (54) DNS (180) [Parameters (1012] Keywords Anomalies	Case Panel	
Filter keyword	Cose sensitive ExactPhrase V Any column V Clear Apply	Fienane	MD5
Parameter name	Parameter value	RedHidalgo pcap	5b4b96b382deeb04468e916b4ddod742
TI S Securi Name	manipa officiants has con		
Catificate School CN	maning and against his cost		
Catificate Issuer CN	Monavit IT IS C & 1		
Contribute Income OIL	Managed (T		
Catificate Issuer O	Monado Campation		
Cetificate Inner I	Redmond		
Catificate Insuer S	Washington		
Catificate Issuer C	1/5		
Cetticate Hash	DB41ED978229 VEDU145 VDER 205EEE VHERSERNIN		
Catificate unlif from	10/12/2017 16/20 C = n		
Catificate valid to	19/12/01/05/22/00 m		
Castilizate Secol	14 1000000 455755 15984 (C 10210000000000 45		
28 20 28 Upped a la viena	The share of the state of the share of the share of the state of the s		
2.5.29 17 like majorade de clause	Intra legal, choose de conteste dans perio Betantine dal classificatione de la secolarización del asocidar (136155731)		
2.5.23.37 Oldo Heljonado de Carves	Automation de cente (1.3.5.1.3.5.7.3.2) Automation de service (1.3.5.1.3.5.7.3.1) Nades Differenties de cente ha cente facelle d'altére de cente de cente d'activité d'activité de cente de cente		
2.5.29.17 Honore atemativo del studar	The provide the second se		
2.5.25.14 Identification de clave de studied entrese	CONFICULTIVED FORCE FALSE CONFICTION FORCE FORCE 74		
2.5.23.35 Identificador de clave de entidad entitora	10. de Darwinsonscherber 20 voluzier / Hamber de Destantarian Nacher annalder Presente 100 date / Hamber de Destantarian Internet de Service 100		
2.5.29.31 Puntos de desebución CPL	(There are approved and the second of the se		
1.3.5.1.3.3.7.1.1 Access a la momación de ensora ensora	[1] CODED & Information on automatic, metodo de acceso-consor de a create de contraction (1.3.5.1.3.3.7.45.2). Nontre atemativo,		
1.3.5.1.4.1.311.21.7 Internacion de pareira de centroaco	Padman 1.3 6 1.4 1.31 21.6 16 3500 2 10 00 0 3 30 100 3 20 304 1 12 00 0 2 2 13 44 22 30 44 10 Autreto de vendon majori 10 / Autreto de		
2.5.29.32 Directivas del certificado	[[Decova of contractor, inervision of decova+1.3.11.4.1.31142.1, [1.] promation of centration of decova. It de centration		
1.3.5.1.4.1.311.21.10 Unectival of apicadon	Tipreciva de centricado de la apicadon, lo entricado de descrita-Auenticado de la encado de la apicadon, lo		
Catholic School CN	Honord (TT) 5 / 4 3		
Centrate Subject CN	None T		
Continues Suger CO	Manager 11		
Configure Dated 1	Party of Control Contr		
Contribute School S	respectively and the second seco		
Continues Integral II	and a second		
Centrole augent C	V2 Editors CoherText Red		
Carthoate Islaer CN	Balancie Goar Inde Hoot		
Vermulat nove VV	UND THE T		

2185

Fig. 3.19. Análisis parámetros en NetworkMiner.

Se puede concluir que, en determinadas ocasiones los analistas de red se encuentran con un problema de capturas de gran tamaño, 2190 lo cual hace muy compleja la tarea de visualizar de forma clara todos los parámetros. Esta herramienta resulta particularmente útil y ágil debido a que el uso de columnas ordena toda la información. Tanto parámetros y DNS como mensajes y sesiones pueden visualizarse fácilmente. De este modo, esta herramienta se presenta como una 2195 excelente opción a otras aplicaciones como Wireshark, Bro o Xplico.

CAPÍTULO IV

2200 HERRAMIENTAS PARA EXTRACCIÓN DE LA MEMORIA VOLÁTIL

La memoria es un elemento (aunque es volátil) que va a proporcionar suficiente información a la hora de buscar evidencias. Todo se centraliza en la memoria (Sánchez Cordero, Conexión 2205 Inversa, 2014); por ejemplo, si se escribe una tarea, si se realiza un cálculo o si se abre un fichero grande, todo esto se grabará automáticamente en la memoria, aparte de que se encuentre en el disco duro.

2210 Uno de los problemas más relevantes para las imágenes de memoria, es comprobar que la imagen se ha creado correctamente; es decir, la verificación que refleja el contenido actual de la memoria en el momento de su creación; el análisis de la memoria puede revelar si los contenidos de la imagen son consistentes con la
2215 disposición conocida y la estructura de un sistema operativo determinado, pero no se puede responder si la imagen refleja con

precisión el sistema de la que fue tomada, como es el proceso de recopilación de información, para eso se observarán algunos tipos de técnicas.

2220

4.1. La Memoria

Uno de los problemas más acuciantes para las imágenes de los discos duros de memoria es comprobar que la imagen del disco se ha creado correctamente, es decir el análisis de la memoria puede

2225 revelar si los contenidos de la imagen son consistentes con la disposición conocida y la estructura de un sistema operativo determinado.

4.2. Técnicas de volcado

2230

Entre las diferentes técnicas de volcado se pueden mencionar:

- Utilización de ficheros de paginación o hiberfil.sys. Este archivo se puede analizar y descomprimir para obtener la imagen de memoria.
- Volcado LiveKD por uso de herramientas.

- MoonSols DumpIt es una fusión de win32dd y win64dd en un ejecutable, es decir al realizar solamente doble clic sobre el ejecutable es suficiente para generar una copia de la memoria física en el directorio actual. DumpIt es la utilidad perfecta para desplegar en una llave USB, una rápida operación de respuesta a incidente.
 - Volcados por fallo configurando el sistema operativo para crear un volcado de memoria completa de Windows (también conocida como pantalla azul o kernel panic)

2240

4.3. Herramientas de volcado de memoria

4.3.1. Dumpit

 DumpIt o MoonSols Windows Memory Toolkit es la
 2250 herramienta para tomar muestras de la memoria RAM en Ambientes Windows, a diferencia de WinPMEM, DumpIT es de pago, aunque tiene una versión gratuita limitada para sistemas de 32 bits (Fig. 4.1.).

→ × ↑ 🔒 > FORENSICS > Dumpl	t		
Nombre	Fecha de modifica	Тіро	Tamaño
📙 dumps	22/03/2010 11:22 a	Carpeta de archivos	
📊 logs	22/03/2010 06:16	Carpeta de archivos	
scripts	19/03/2010 08:52 a	Carpeta de archivos	
in2dmp.exe	17/01/2013 12:03	Aplicación	81 KB
📧 dmp2bin.exe	17/01/2013 12:03	Aplicación	74 KB
🔣 Dumplt.exe	03/05/2011 12:41 a	Aplicación	203 KB
iii hibr2bin.exe	17/01/2013 12:03	Aplicación	74 KB
📧 hibr2dmp.exe	17/01/2013 12:03	Aplicación	81 KB
MWMT-v1.4.zip	30/03/2018 02:02	Archivo WinRAR Z	265 KB
README.txt	11/02/2011 06:57	Documento de tex	5 KB

Fig. 4.1. Herramienta DumpIt.

Dumpit permite hacer un volcado de la memoria RAM y convertirla en un fichero, luego se parsea para convertirla en algo legible; es decir, primero hace un volcado y lo convierte en archivo (http://www.moonsols.com/2011/07/18/moonsols-dumpit-

2260 goes-mainstream/), el volcado de memoria se realizará siempre en un equipo encendido, la memoria tiene una limitación, no es lo mismo 8 GB que 1 Tera (Fig. 4.2.). En la nube se podrá hacer un volcado de memoria, solamente si se tiene un permiso judicial.

C:\Users\HIDALGO\Desktop\Analisis	C:\Users\HIDALGO\Desktop\AnalisisForense\Dumplt-Free\Dumplt.exe						
DumpIt - v1.3.2.20110401 - Copyright (c) 2007 - 2011, Copyright (c) 2010 - 2011,	One click memory memory dumper Matthieu Suiche <http: www.msuiche.net=""> MoonSols <http: www.moonsols.com=""></http:></http:>						
Address space size: Free space size:	10779361280 bytes (10280 Mb) 34592817152 bytes (32990 Mb)						
<pre>* Destination = \??\C:\U</pre>	sers\HIDALGO\Desktop\AnalisisForense\DumpIt-Free\HIDALGO-20180311	-07032	8.raw				
> Are you sure you wan + Processing	t to continue? [y/n] y						

2265

Fig. 4.2. Ejecución de Dumpit.

Al observar *Destination* es la ruta de donde se ha ejecutado, y donde se ubica HIDALGO-**20180311-070328**.raw (añomesdía – horadelsistema); y si se desea continuar, al pulsar "**y**" retorna un volcado de memoria. El tamaño del archivo será proporcional a la memoria RAM, pues es un procedimiento para realizar un volcado de memoria. Todo se realiza en modo de comando para lo cual se puede hacer scripting, es decir permite optimizar y obtener el volcado de memoria "HIDALGO-20180311-070328.raw" (Fig.

2275 4.3.).

→ AnalisisForense → Dumplt-Free			
Nombre	Fecha de modifica	Tipo	Tamaño
📕 Dumplt.exe	22/01/2014 02:12	Aplicación	203 KB
HIDALGO-20180311-070328.raw	11/03/2018 02:05 a	Archivo RAW	10,526,720 KB
README.txt	22/01/2014 02:12	Documento de tex	1 KB

Fig. 4.3. Extracción del archivo.raw del volcado de memoria.

Finalmente se puede observar el volcado de memoria en un archivo

2280 HIDALGO-20180330-191924.raw (Fig. 4.4.)

← → ֊ ↑ 🔒 > FORENSICS > Dump	t	~	ල් Buscar er
Nombre ^	Fecha de modifica	Тіро	Tamaño
📙 dumps	22/03/2010 11:22 a	Carpeta de archivos	
logs	22/03/2010 06:16	Carpeta de archivos	
scripts	19/03/2010 08:52 a	Carpeta de archivos	
📧 bin2dmp.exe	17/01/2013 12:03	Aplicación	81 KB
📧 dmp2bin.exe	17/01/2013 12:03	Aplicación	74 KB
📕 Dumplt.exe	03/05/2011 12:41 a	Aplicación	203 KB
📧 hibr2bin.exe	17/01/2013 12:03	Aplicación	74 KB
📧 hibr2dmp.exe	17/01/2013 12:03	Aplicación	81 KB
🗹 🖻 HIDALGO-20180330-191924.raw	30/03/2018 02:22	Archivo RAW	10,526,720 KB
MWMT-v1.4.zip	30/03/2018 02:02	Archivo WinRAR Z	265 KB
README.txt	11/02/2011 06:57	Documento de tex	5 KB

Fig. 4.4. Volcado de memoria.

4.3.2. RamCapturer

2285 (http://download.cnet.com/Belkasoft-RAM-Capturer-64-

bit/3001-2094 4-75946114.html), funciona en modo gráfico y

texto, en dónde se va a realizar el volcado (Fig. 4.5.).

 Belkasoft Live RAM Capturer 			-		×
Calasta da de Calas antes					
Select output rolder path:					
C:\Users\HIDALGO\Desktop\AnalisisForense\64bit					
Loading device driver Physical Memory Page Size = 4096 Total Physical Memory Size = 10280 MB					^
	Capture!	Can	cel	Clo	se

Fig. 4.5. Volcado de memoria con RamCapturer.

2290

Al reservar un espacio en el disco duro y volcar en ese espacio,

algunas veces hace una parada y si lo hace es sobrescribiéndolo,

haciéndolo más rápido, se completa y finalmente se obtiene el fichero en memoria (Fig. 4.6.).

🔒 > AnalisisForense > 64bit										
Nombre	Fecha de modifica	Tipo	Tamaño							
20180311.mem	11/03/2018 12:19 a	Archivo MEM	10,526,720 KB							
msvcp110.dll	23/07/2016 03:12 a	Extensión de la apl	646 KB							
🖄 msvcr110.dll	23/07/2016 03:12 a	Extensión de la apl	830 KB							
🦔 RamCapture64.exe	03/08/2016 07:37 a	Aplicación	50 KB							
RamCaptureDriver64.sys	03/08/2016 07:37 a	Archivo de sistema	12 KB							

2295

Fig. 4.6. Fichero de memoria.mem con RamCapturer.

4.3.3. FTK Imager lite

FTK Imager de AccessData es una herramienta para realizar
réplicas y visualización previa de datos, la cual permite una evaluación rápida de evidencia electrónica para determinar si se garantiza un análisis posterior con una herramienta forense como AccessData Forensic Toolkit. FTK Imager también puede crear copias perfectas (imágenes forenses) de datos de computadora sin realizar cambios en la evidencia original (Quezada, 2014).

Es importante mencionar el uso de un bloqueador de escritura al utilizar FTK Imager para crear la imagen forense desde un disco duro u otro dispositivo electrónico. Esto asegura que el sistema

142

2310 operativo no alterará la unidad fuente original cuando se le adjunte a la computadora.

Para prevenir la manipulación accidental o intencional de la evidencia original, FTK Imager realiza una imagen duplicada bit a 2315 bit del medio. La imagen forense es idéntica en cualquier forma al original, incluyendo espacio de holgura o residual y espacio sin asignar o espacio libre de la unidad. Esto permite almacenar el medio original en un lugar seguro de daño mientras se procede con la investigación utilizando la imagen forense (ReYDeS, 2018). Se

2320 puede descargar desde:

http://www.accessdata.com/support/product-downloads, al ejecutar FTK (Fig. 4.7.),

Elle View Mode Help		000) 🗈	56	200		Dei HE	<u>e</u> '	8.										
vidence Tree	×	File List																	
		Name						Size	Туре						Date Modified				
		SLogFile					65,	536	Regular File							22/02/2016 06:22:47 a.m.			
		SMFT				1,	147,	392	Regula	ar Fil	le					22/0	2/2016 06:22:4	7 a. m.	
FI C SExtend			r				4		Regular File						22/0	2/2016 06:22:4	7 a. m.		
🗄 🫅 \$Recycle.Bin		Secure						1	Regular File						22/02/2016 06:22:47 a.m.				
-tr \$Secure								1	NTFS Logged Utility Stream					m	2//03/2018 04:57:12 a.m.				
-te SUpCase		Supcase						128	Regular File						22/02/2016 06:22:47 a.m.				
⊞ i 3590F75ABA9E485486C100C1A9D4F								1	Regular File						22/02/2010 00:22:4/ a.m.				
3590F /5ABA9E485486C100C1A9D4	3	dates listenes tot						0	Regular File						10/02/2017 06:30:00 p. m.				
3590F75ABA9E485486C100C1A9D4		hiberfil.s	vs			3	289	432	Regula	ar Fil	e					30/0	3/2018 12:02:5	6 a. m.	
Config.Msi		a nagefile.svs				7.	510.	588	Regula	ar Fil	e					27/03/2018 06:55:31 p. m.			
🕀 🫅 Horarios		resultado.txt					15,	185	Regular File							19/03/2017 03:32:32 a.m			
🖻 🚞 hp		swapfile.	sys				262,	144	Regula	ar Fil	le					21/0	3/2018 04:23:2	3 p. m.	
inetpub intel	~	url_settin	g_def	nitio	ns.tx	t		35	Regula	ar Fil	le					02/0	3/2018 05:13:4	9 p. m.	
< >		00000000	57 4	1 4B	45	09	00	00	00-74	A6	00	00	DS	03	00	00	WAKE ···· t		
Custom Content Sources	×	00000010	5D 0	6 11	00	00	00	00	00-00	10	00	00	00	00	00	00	1		
Evidence Ele Sustem Dath Ele Onting		00000020	81 6	4 31	FB	B7	C7	D3	01-88	46	DC	41	34	08	00	00	·dlû ·Ç0 · · F	UA4 · ·	
Evidence: File System Paur (File Opdons	-	00000030	00 0	0 48	BD 8C	01	BD	FF	FF-30	3F	00	00	F8	66	00	00	Y2		
		00000050	32 5	8 00	00	00	00	00	00-21	B3	00	00	00	00	00	00	2X! 3		
		00000060	00 0	0 00	00	00	00	00	00-13	00	00	00	00	00	00	00			
		00000070	83 6	A 00	00	00	00	00	00-03	39	04	00	00	00	00	00	·j · · · · · · 9		
		00000080	AC C	9 FB	00	00	00	00	00-28	A4	62	2A	06	00	00	00	(P	Dx	
		000000a0	F8 1	2 82	47	06	00	00	00-6C	E4	08	97	16	00	00	00	ø · · G · · · · 1ä		
		00000000	D2 8	B C8	00	00	00	00	00-1C	06	6C	18	00	00	00	00	Ò ·È · · · · · ·	1	
		000000c0	F6 D	0 EE	05	00	00	00	00-00	00	00	00	00	00	00	00	öÐî		
		0000000d0	1C D	9 DC	BA	13	02	00	00-00	00	00	00	00	00	00	00	.00°		
		0000000000	00 0	0 00	00	00	00	00	00-00	00	00	00	00	00	00	00			
		00000100	00 0	0 00	00	00	00	00	00-00	00	00	00	00	00	00	00			
<	>	00000110	00 0	0 00	00	00	00	00	00-00	00	00	00	00	00	00	00			
New Edit Remove Remove All Greate Image		00000120	00 0	0 00	00	00	00	00	00-00 00-00	00	00	00	00	00	00	00			
Properties Hex Value Int Custom Conte		Cursor pos =	0; du:	5 = 11	1079	987;	log s	ec =	888638	96									

Fig. 4.7. Herramienta FTK Imager lite.

Al realizar un clic sobre File \rightarrow Capture Memory... \rightarrow Destination Path \rightarrow Include paquefile \rightarrow Capture Memory; es decir se tiene diferentes herramientas que permiten en un momento determinado tener el volcado de memoria.

2330

Todo lo realizado es interesante desde el punto de vista forense; cabe mencionar que cuando la máquina está encendida lo principal es sacar todas las evidencias volátiles y principalmente la
memoria RAM, ante un troyano, o algo externo. Se realiza unvolcado de la memoria completo de lo ocupado y lo no ocupado (Fig. 4.8.).

Memory Progr	ess				
Destination:	C:\Users\HIDALGO\Desktop\memdump.mem				
Status:	Dumping RAM: 4GB/10GB [37%]				
Cancel					

Fig. 4.8. Progreso de Captura de memoria con FTK Imager.

2340 Finalmente se ilustra el volcado de memoria en un archivo memdump.mem.

Además la herramienta se puede ejecutar remotamente con psexee. Para analizar los resultados de la memoria se dispone de un 2345 conjunto de utilidades, que van a permitir obtener desde temas de malware hasta ficheros de texto.

4.4. Procesos de Análisis de Memoria

Hay algunas maneras para analizar la memoria, se puede usarpara la información almacenada dentro de los volcados de proceso

realizados con Process Dumper (pd). Los procesos de análisis extraen las diferentes asignaciones de procesos en el disco y luego se puede usar como espacio de trabajo central para análisis posteriores. En la memoria se encuentra toda la información (o casi de todo) (Fig. 4.9).

2355

C:>pd pd, version 1.1 tk 2006, www.trapkit.de Usage: pd [-v] -p pid Options: -v - be verbose Examples pd -p pid > pid.dump pd -p pid | nc 10.0.0.1 7000

Fig. 4.9. Proceso de Volcado de memoria usando Trapkit.

Por ejemplo: Se puede dar el caso de que un usuario quiera
recuperar las contraseñas de acceso a una aplicación o sitio web de un computador que anteriormente ha iniciado la sesión. Depende de la aplicación o del navegador las puede almacenar en disco, cifrando el contenido de las contraseñas, por lo cual este método de recuperación no es válido. (se entiende que el usuario no recuerda la contraseña).

Para ello utilizamos la siguiente 'tool': pd, disponible en la web '<u>http://www.trapkit.de</u>' Pd es una utilidad que permite extraer de la memoria un 2370 determinado proceso basándose en el identificador de proceso (PID) que el sistema le asigna y poder volcarlo a disco. De esta forma no tenemos que 'dumpear' toda la memoria para hacer lo mismo.

En este caso se necesita recuperar las contraseñas de acceso a la web de movistar para el envío de mensajes por SMS (Fig. 4.10) (desde un puesto de trabajo Linux y con navegador Firefox)
(Telefónica Móviles España, s.f.).

€ → C	B Es seguro https://enviamensajes.movistar.es/EnviaMensajes;/#	x 51 🖬 1
Envial	Mensajes	附 movistar
EnviaNem	sajes es la forma más fácil y rápida de enviar mensajes de texto SMS y mensajes multimedia MMS desde tu PC. Silo necesitas un ordenetor con conexión a Intern	et y una linea mévil moviatar.
D Pode	as aprovechar toda la capacidad del PC para enviar mensajes desde tu linea móvil escribe el mensaje utilizando el teclado completo, alfadele contenidos multime ne de tu entorno de trabajo. Mucho más corocol:	dia con un click, almacena aún más mensajes y todo sin
Envia	Mericajes te permites	
Envis Date Para i	Story of general sectors and the sector of t	
\bigtriangledown	Version Week week week a Version da la propertie de la propertie de la propertie de la construction de la co	
	Envoltenasjes en el Decritoris de la PC. Entrela la aplicación en la PC y Jola al caso de la Escritorio para enviar managin.	

2380

Fig. 4.10. Web de movistar para el envío de mensajes por SMS.

Fuente: <u>https://enviamensajes.movistar.es/EnviaMensajes/#</u>

Si vemos el código fuente de la página nos encontramos con las posibles variables a buscar entre ellas (TM_LOGIN, TM_PASSWORD, TM_ACTION) (Fig. 4.11).



Fig. 4.11. Código fuente de la página de la web de movistar. *Fuente:* <u>https://enviamensajes.movistar.es/EnviaMensajes/#</u>

2390 En el sistema operativo Linux:

pd -p 19323 > firefox.dump (donde 19323 es el PID de firefox)

Extraigo el texto del fichero binario a otro fichero más humano (txt)

strings -el firefox.dump > memorystrings.txt

Editamos el fichero TXT y buscamos las cadenas anteriormente

2395 citadas

2385

Al encontrarse con la cadena TM_LOGIN, lleva asociado un

número (deducimos que es un teléfono), mientras que las demás

cadenas no muestran nada coherente (Fig. 4.12).

hEP	hEP	pEP	р
TM_LOG	IN620664	4566	1

Fig. 4.12. TM_LOGIN del usuario de la página web.

Detenidamente si se busca por el número de teléfono, nos muestra suficiente información, agendas, otros números de contacto, etc. y, sobre todo la posible contraseña (Fig. 4.13.).



Fig. 4.13. TM_LOGIN del usuario de la página web con su contraseña.

Este procedimiento es idéntico para Windows con la misma herramienta.

2410

2405

4.5. Memoria Pagefile

Este archivo es muy especial y lo usa Windows para almacenar temporalmente datos los cuales son intercambiados entre la 2415 memoria RAM y éste, con el fin de disponer de un bloque más grande de memoria, a ésta se le conoce como **MEMORIA VIRTUAL** (Copyleft, 2018).

El nombre del archivo es **pagefile.sys** y se crea en el 2420 momento de la instalación de Windows en la unidad raíz (normalmente C:\>) donde se encuentra el boot del sistema y sus atributos son ocultos.

El tamaño de archivo pagefile.sys normalmente es 1.5 veces 2425 más grande que la memoria RAM del sistema. (Por ejemplo, si se tiene 1 GB de RAM, el archivo debería pesar algo como 1.5 GB, si tiene 256 MB, el archivo debería pesar algo como 384 B, y así, etc.).

El fichero de paginación ocurre cuando se va llenando la

2430 memoria RAM, lo que hace el sistema operativo es volcarlo al fichero pagefile.sys; y una vez que lo vuelca, va a permitir tener una memoria virtual. En un equipo encendido el volcado sería que después de haber producido el volcado de memoria con los artefactos antes estudiados, se procede a desenchufar el cable y
2435 como no se ha apagado correctamente el computador, disponemos del fichero pagefile.sys; pero si se apaga correctamente, es decir *Inicio* → *Apagar*, el fichero pagefile.sys se borra y en el fichero pagefile.sys; lo que no cabe en la memoria RAM va directo al fichero pagefile.sys

y este fichero hay que tenerlo previsto para el tema de la paginacióny evidencias.

Para obtener el fichero de paginación en una máquina encendida se puede usar el FTK Imager \rightarrow Add Evidence Item \rightarrow Logical Drive \rightarrow C:\> (Fig. 4.14)





Fig. 4.14. Obtención fichero de paginación modo encendido.

Si tenemos más de un disco duro lo recomendable sería tener en otro disco duro o partición el fichero de paginación para lo cual 2450 se dispondrá proceder a ubicar sobre el directorio root para obtener el archivo de paginación e hibernación (Fig. 4.15).

vidence Tree	×	File List														
⊒- @ C:\		Name			1		Size	Type					1	Date	Modified	
🖻 📴 WINDOWS [NTFS]		SLogFile				6	5,536	Regul	ar Fil	e				22/0	2/2016 06:22:4	47 a. m.
[root]		SMFT				1,14	7,392	Regul	ar Fil	e				22/0	2/2016 06:22:4	47 a. m.
SBadClus		SMFTMin	r				4	Regul	ar Fil	e				22/0	2/2016 06:22:4	47 a. m
E Consula Dia		Secure \$					1	Regul	ar Fil	e				22/0	2/2016 06:22:4	47 a. m
ht Secure		STXF_DA	TA				1	NTFS	Logg	ed U	tility !	Strea	m	27/0	3/2018 04:57:	12 a. m
SUpCase		SUpCase					128	Regular File				22/0	2/2016 06:22:4	47 a. m		
3590F75ABA9E485486C100	C1A9D4F	SVolume					0	Regular File					22/02/2016 06:22:47 a.m. 30/10/2015 07:18:34 a.m. 19/02/2017 06:30:09 p.m.			
3590F75ABA9E485486C100	C1A9D4F	BOOTNX	Т				1	Regular File Regular File								
3590F75ABA9E485486C100	C1A9D4F	datos_list	tener.txt	ŧ.			0									
3590F75ABA9E485486C100	C1A9D4F	hiberfil.sys		3,289,432 F		Regular File				30/03/2018 12:02:56 a.m.						
- Config.Msi		pagefile.	sys			7,510	0,588	Regul	ar Fil	e				27/0	3/2018 06:55:3	31 p. m
🕀 🧰 Horarios		resultado	.txt			15,185		Regular File			19/03/2017 03:32:32 a.m					
🕀 🧰 hp		Swapfile.	sys			26	2,144	Regul	ar Fil	e				21/0	3/2018 04:23:2	23 p. m
🖽 🧰 inetpub		url_settin	g_defin	ition	s.txt		35	Regul	ar Fil	e				02/0	3/2018 05:13:4	49 p. m
i 🕂 🧰 Intel	~															
		00000000	57 41	4B	45 1	09 00	00 0	00-74	A6	00	00 D8	3 03	00	00	WAKE	
Sustom Content Sources	×	00000010	SD 06	31	FR I	30 00	7 03	01-99	10	DC 1	41 3/	1 08	00	00	.d10.có	FÍDA
Evidence:File System Path IFile	Options	00000030	FF BF	9B	BD B	ED 04	1 00	00-01	00	00 1	00 00	7 00	00	00	V: 351	
n en de la constante de la cons		00000040	00 00	48	8C (01 BI) FF	FF-30	3E	00 0	00 F8	66	00	00	···H··35990:	>··øf·
		00000050	32 58	00	00 1	00 00	00 0	00-21	B3	00 (00 00	00	00	00	2X · · · · · !	3
		00000060	00 00	00	00 0	00 00	00 0	00-13	00	00 0	00 00	00 0	00	00		
		00000070	83 6A	00	00 0	00 00	00 0	00-03	39	04 1	00 00	00 00	00	00	·j	9
		00000080	AC C/	FR	00 0	30 00	00 0	00-28	A4	73	2A 04	00	00	00	4.8	RD*···
		000000000	F8 12	82	47	06 00	0 00	00-60	E4	08	97 14	5 00	00	00	g G 14	y
		000000b0	D2 8B	C8	00 1	00 00	00 0	00-1C	06	6C :	18 00	00	00	00	Ò.È	1
		000000c0	F6 D0	EE	05 1	00 00	00 0	00-00	00	00 1	00 00	0 00	00	00	öÐ1 · · · · ·	
		000000d0	1C D9	DC	BA :	13 02	00 2	00-00	00	00 (00 00	0 00	00	00	.)Úܰ	
		000000e0	00 00	00	00 (00 00	00 0	00-00	00	00 0	00 00	0 00	00	00		• • • • • •
		0000000f0	00 00	00	00 0	00 00	00 0	00-00	00	00 1	00 00	00 00	00	00	221000000	
		00000100	00 00	00	00 0	00 00	00 0	00-00	00	00 0		00 0	00	00	0.000.000.000	0.020.00
<	>	00000110	00 00	00	00 0	10 00	00	00-00	00	00		00	00	00		
								00-00		1414						

Fig. 4.15. Ubicación archivo paginación e hibernación.

El archivo de paginación es el que se localiza en la máquina encendida y el de hibernación se encuentra en el computador en modo suspendido o hibernación y se lo puede volcar; de esta manera en modo vivo o encendido se realiza con el FTK Imager lite porque no se puede copiar directamente el fichero pagefile.sys, y de esa
2460 manera se puede exportar el archivo en *Export File...* (Fig. 4.16)

Export Files	×
Copying files	
C:\Users\HIDALGO\Desktop\FORENSICS\pagefile.sys	
Cancel	

Fig. 4.16. Exportación fichero de paginación pagefile.sys.

La ubicación del fichero pagefile.sys (Fig. 4.17)



Fig. 4.17. Ubicación del fichero pagefile.sys.

Para tratar la información del fichero pagefile.sys, se hace uso de la herramienta strings.exe (https://docs.microsoft.com/en2470 us/sysinternals/downloads/strings), que va permitir parsear la información que está en un archivo y permitirá convertir el contenido del archivo de paginación en un archivo de texto (Fig. 4.18.). Para el volcado de memoria del fichero pagefile.sys se puede usar los siguientes comandos:

- findstr "password" pagefile.txt > contraseñas.txt
- findstr "password" pagefile.txt > passwd.txt

- findstr "net user" pagefile.txt > netuser.txt
- findstr /C:"reg add" pagefile.txt > reg.txt
- **2480** findstr "UPDATE" pagefile.txt
 - findstr "ipconfig" pagefile.txt
 - findstr "html" pagefile.txt > dochtml.htm
 - findstr "msnmsgr" pagefile.txt > messenger.htm
 - findstr "INVITE" pagefile.txt > invite_messenger.htm
- 2485 findstr /c:"conectado" pagefile.txt
 - findstr /c:"MSNSLP" pagefile.txt
 - findstr /c:".doc" pagefile.txt
 - findstr /c:"CONTENT" pagefile.txt



Fig. 4.18. Comandos para extraer el fichero de paginación.

En la Fig. 4.19, disponemos del fichero transformado en texto

y se lo puede analizar.



Fig. 4.19. Fichero de paginación transformado en texto.

Ya extraído el contenido del archivo pagefile.sys, se procede analizarlo con el editor de texto Notepad++, y permitirá obtener 2500 información relevante, además se procede a buscar lo que desea, por ejemplo todas los "<u>ftp://</u>" del archivo de paginación y del resultado se extrae la línea o líneas que contiene dicha información, de esa manera se puede buscar la información que desee (Fig. 4.20).



2505

2495

Fig. 4.20. Extracción información que contiene ftp://

Caso Práctico: A continuación, se permitirá determinar con claridad y certeza la aplicabilidad de diversas herramientas de software en la investigación de delitos informáticos. Cabe
2510 mencionar que se asumen como realizados los pasos relacionados con el aseguramiento y cadena de custodia de las evidencias digitales identificadas en el caso práctico que a continuación se tratará, ya que

se centra en la ejecución de herramientas de software, su funcionalidad y su aplicabilidad de acuerdo con el objetivo de investigación planteado.

Un cracker aprovechándose de sus conocimientos y experiencia, se aprovechó al tener acceso a recursos computacionales adecuados viola el sistema de seguridad informático de una clínica, accediendo a un servidor con sistema operativo Linux CentOS y robando información confidencial de los pacientes atendidos en los últimos diez años, alimentada en una hoja de cálculo con tablas dinámicas, la cual publicó en internet en un blog anónimo.

2525

2515

Se requiere investigar el origen del incidente, posibles delincuentes, herramientas informáticas utilizadas, daños ocasionados, fallas que permitieron el ilícito y correcciones a corto plazo.

2530

La Investigación Forense versa que el día 14 de octubre de 2013 un funcionario informa a sus superiores de la clínica Medical Center Valledupar (Colombia) que el equipo HP destinado a alojar la base de datos de los pacientes tratados en los últimos años, 2535 soportada en una hoja de cálculo con tablas dinámicas, presenta registros borrados. El administrador descubre esta incidencia porque al consultar el archivo la información estaba incompleta. En la Tabla 4.1, se ilustra las características del equipo afectado:

Tabla 4.1. Características del equipo afectado.

Fabricante	HP
Modelo	Deskpro
Número de serie	978978978
Procesador	Intel [®] Pentium [®] i7 (4 núcleos, 2,9 GHz, 3 MB, 55 W)
Memoria	8 GB DDR3
Disco Duro	Marca: HP Capacidad: 750 GB Tecnología: SATA Serial: XYZ7890
Sistema Operativo	CentOS 6.5
Nombre del equipo	Servidor CM1
IP	192.168.1.1

Luego de pasadas las fases de análisis del problema, recolección de evidencias digitales y preservación de las mismas, se 2545 continua con la fase de evaluación de estas evidencias.

Las novedades encontradas en la consecución de este delito:

Computador de escritorio simple sirviendo como Servidor de aplicaciones, con sistema operativo CentOS v6.5, sin implementación de Herramientas de Seguridad a nivel de hardware o software (Tipo Firewall, IDS, etc.).

Las evidencias digitales adquiridas en la consecución de este delito:

- 2555 Adquisición de la memoria RAM a través del aplicativo DumpIT
 - Clonación del Disco Duro mediante el aplicativo DD, previa generación del hash del disco original (Fig. 4.21).

🌲 DataRescue DD			(
Dai	Pyright © 2001-2008 DataRes		1.0.0 rved.	(Build 11225)
Source			Destination	
New Volume (D:) NTFS 750 GB	Refresh	\My Documents\imag	je.dd Bro	wse
	Opt	ons		
Start	Size		End	
100000		175000	275000 😂	MBs
20000000	3	5000000 😂	550000000 🗢	Sectors
	Read direction: 🔘	O		
Time		Message		
11:11:20 Please wait (11:11:20 1 drives four	while searching for drives			
Last log				

2560

Fig. 4.21. Clonación del Disco Duro mediante el aplicativo DD.

 Creación de dos imágenes del disco duro mediante el software FTK Imager y se realiza la validación hash, resultado verificado (Fig. 4.22).





Fig. 4.22. Copia del disco duro origen con FTK Imager.

Inicialmente se selecciona uno de los equipos de la entidad, los cuales tienen las mismas características que el servidor y se clona 2570 una de las copias al disco duro de éste, luego se realiza una validación hash para comprobar la integridad del clonado, se verifica, valida y se arranca el sistema.

Se loguea con el usuario *root*, credenciales facilitados por el 2575 usuario del equipo atacado en la entidad, que inexplicablemente su contraseña es *admin01*, lo que da a entender la poca gestión de seguridad aplicada.

Se valida que software se ha instalado recientemente con el 2580 comando: rpm -qa --last

Lo que ilustra el siguiente resultado:

xchat-2.8.8-0 lun 09 sep 2013 22:10:15 COT sudo-1.6.3p6-1 mar 01 ene 2013 17:00:59 COT

- 2585 stunnel-3.13-3 mar 01 ene 2013 17:00:59 COT strace-4.2.20010119-3 mar 01 ene 2013 17:00:59 COT anonftp-4.0-4 mar 01 ene 2013 16:57:29 COT xinetd-2.1.8.9pre14-6 mar 01 ene 2013 16:57:28 COT zlib-devel-1.1.3-22 mar 01 ene 2013 17:00:59 COT
- 2590 texinfo-4.0-20 mar 01 ene 2013 17:00:59 COT wu-ftpd-2.6.1-16 mar 01 ene 2013 16:57:28 COT kudzu-devel-0.98.10-1 mar 01 ene 2013 16:56:07 COT urw-fonts-2.0-12 mar 01 ene 2013 16:57:28 COT telnet-server-0.17-10 mar 01 ene 2013 16:57:28 COT
 2595 glibc-common-2.2.2-10 mar 01 ene 2013 16:56:07 COT man-pages-es-0.6a-7 mar 01 ene 2013 16:56:09 COT

man-pages-1.35-5 mar 01 ene 2013 16:56:08 COT mailcap-2.1.4-2 mar 01 ene 2013 16:56:07 COT indexhtml-7.1-2 mar 01 ene 2013 16:56:07 COT

2600

Se puede apreciar la instalación el día 09 de septiembre de 2013 de un software de mensajería instantánea IRC denominado xchat. Lo que trae consigo graves problemas ya que, si no existe otro usuario en el servidor además del root, significa que la persona que 2605 ha instalado el software de IRC lo ha hecho con este usuario y lo más seguro se ha conectado a canales de Chat desde ese perfil. Luego de esta conectado es muy fácil encontrar su dirección ip para otro usuario que este en el mismo canal mediante el comando /whois, el cual se puede ejecutar desde el mismo software XCHAT,
2610 sin necesidad de instalar nada adicional.

Se observa los logs fallidos en /var/log/faillog, o con el comando *faillog –u root* y se observa que el día del incidente se dieron innumerables conexiones infructuosas al servidor con el usuario root antes de ser accedido.

Username	Failures	Maximum	Latest
root	17	99	

Y con el comando last se observa los últimos logins correctos:

2620	last -20		
	root tty7	Sat Oct 10 06:57	still logged in
	root tty8	Sat Oct 10 08:26	still logged in

	root	tty7	Sat Oct 10 17:37	still logged in
	root	tty8	Sat Oct 10 22:56	still logged in
2625	root	tty7	Sat Oct 11 06:57	still logged in
	root	tty8	Sat Oct 11 09:46	still logged in
	root	tty7	Sat Oct 11 12:57	still logged in
	root	tty8	Sat Oct 11 23:02	still logged in
	root	tty7	Sat Oct 12 06:47	still logged in
2630	root	tty8	Sat Oct 12 17:56	still logged in
	root	tty7	Sat Oct 12 23:07	still logged in
	root	tty8	Sat Oct 13 06:48	still logged in
	root	tty7	Sat Oct 13 23:02	still logged in
	root	tty8	Sat Oct 14 07:46	still logged in
2635	root	tty7	Sat Oct 14 09.27	still logged in
	root	tty8	Sat Oct 14 12:36	still logged in
	root	tty7	Sat Oct 14 14:37	still logged in
	root	tty8	Sat Oct 14 17:22	still logged in
	root	tty7	Sat Oct 14 20:04	still logged in
2640	root	tty8	Sat Oct 14 22:51	still logged in

Se observa que existe unas horas comunes de logins correctos, entre las 06:46 y las 06:57 y entre las 22:56 y 23:07. Se entiende el acceso en horas de la mañana porque la política de seguridad **2645** implementada en la empresa estipula copias de seguridad todos los días antes de las 8:00 que empiezan labores, pero no se tiene claro los accesos nocturnos, más aún cuando el usuario de la base de datos trabaja hasta las 18:00 y las conexiones se dan localmente.

2650 Se mira el historial de comandos que se guardan en el archivo ~/.bash_bistory y se observa que el programa de chat se ejecuta todos los días en ese periodo de tiempo.

3433 su

3435 xchat

2655

4041 su

4042 xchat

Se examina el archivo volcado de la memoria RAM del 2660 archivo atacado, al analizar con el software WINHEX (**Fig. 4.23**), se encuentra que en horas de la noche existe navegación a páginas para adultos y de chat (**Fig. 4.24**).





Fig. 4.23. Análisis de la RAM con el software WINHEX.

Winflex - [MantraPortable.e.	(e]	Contract - Mandan - Male	
Prie Eak Search Navigetion	New Tools Specia		- 01
	MantraPortable.exe		
File Edit	Offset	1 2 3 4 5 6 7 8 9 A B C D E F	Langedistan
	00001220 F 00001230 4	8B C8 8B 45 E0 83 F8 0C 77 69 FF 24 85 18 32 yiEtEAte wiy5t 2 00 03 F9 EB 5E 2B F9 EB 5A 0F AF F9 EB 55 3B 0 ue*+ueZ_ueU:	MantraPortable.exe D:\PENTEST\MantraPortable
	00001240 C 00001250 0	74 07 8B C7 99 F7 F9 EB 1E 33 FF C7 45 FC 01 Et tCt+ue 3yCEu 00 00 EB 3F 0B F9 EB 3B 23 F9 EB 37 33 F9 EB eP ue73ue	File size: 2251
	00001260 3 00001270 3	33 CO 3B FB OF 94 CO 8B F8 EB 28 3B FB 75 04 33Å,û låløe(;ûu CB 74 09 33 FF 47 EB 1B 3B FB 75 F3 33 FF EB ;Et 39Ge ;ûud3ye	DOS name: MANTRA~1.D
	00001280 1 00001290 E	3B CB 74 C5 8B C7 99 F7 F9 8B FA EB 06 D3 E7 :EtAlC1+utue Oc 02 D3 FF 57 E9 43 12 00 00 6A 01 E8 BB F5 FF e OyVeC j enery	Delaut Edit Mode State: modifi
	000012R0 P 000012B0 4 000012C0 4	64 02 59 88 F8 E8 98 F5 FF FF 50 57 55 FF 15 93 T1@01099F0V9 82 40 00 E9 D2 FC FF FF 8B 45 DC 8B 3D C0 B0 H1@ 00099FUU=Å 00 3B C3 74 5E 48 3B FF 74 0A 8B 3F 3B C3 75 Ø Åt'N 9t 17 Åu	Undo level Undo reverses keyboard in
	000012D0 F 000012E0 0	3B FB 75 22 FF 75 DC 68 F4 89 40 00 E8 22 45 8:uu*yuUhat€ e*E 00 59 59 68 10 00 20 00 6A E8 53 E8 75 4A 00 YYh jeSeuJ	Creation time: 29/08/20 06.33
	000012F0 0 00001300 5 00001310 F	50 E9 45 FD FF FF 83 C7 04 57 BE C8 B0 40 00 PEEyyy[C WAE'9 E8 64 42 00 00 A1 C0 B0 40 00 83 C0 04 50 57 VedB iÅ'9 IÅ PV 55 42 00 00 A1 C0 B0 40 00 56 92 C0 04 50 F2 A110 iÅ'9 VA De	Last write time: 29/08/20 06:33
	00001320 2	OF 00 00 3B CB 74 2B 3B FB 75 10 68 D0 89 40 Et+: tu hB10 E8 CE 44 00 00 59 E9 D7 FA FF FF 8D 47 04 50 EID Yexuyy G P	Attributes: Icons:
	00001340 5 00001350 0	E8 24 42 00 00 8B 07 A3 C0 B0 40 00 57 E9 34 Ve8B 1 \$A*# Ve4 00 00 68 0C 40 00 00 6A 40 FF 15 24 81 40 00 h # j#y \$ #	Mode: To Character set CP 12
	00001360 F 00001370 B	75 D4 88 F0 8D 46 04 50 E8 F8 49 00 00 A1 C0 yu018 F PemJ iA 40 00 89 06 89 35 C0 B0 40 00 E9 63 11 00 00 '0 ∎ 15Å'0 ec	Offsetz: hexadecia Bytes per page: 29x16-4
	00001380 F	FF FF F6 45 E8 01 09 45 08 74 0A 6A 33 E8 B9 0yybEe [E t j3e]	Window II Not of windows
	000013B0 F 000013C0 8	FF FF 89 45 08 83 7D D0 21 75 4A 33 C9 41 E8 cyylE 1)BluJ3EAe F4 FF FF 6A 02 59 8B F8 E8 78 F4 FF FF 8B 4D [cyyl YimexcyylH	C 8 B# (s) 119
	000013D0 E	C1 F9 02 3B CB 74 1E 8D 55 F8 52 51 53 FF 75 eÅu Et UeROSyu FF 75 CC 50 57 FF 15 4C 82 40 00 F7 D8 1B C0 +ulPV+ L10 +0 Å +1	T 16 B4 (±) 30583 3 32 B# (±) 779581303

Fig. 4.24. Información de la RAM con el software WINHEX.

2670

Se encuentra un pendrive usb conectado al servidor, se analiza y entre otras cosas se ubica un archivo con el nombre amigoschat.doc, lo llevamos a un equipo con sistema Windows, se trata de abrir con el aplicativo ofimático Microsoft Word y no es posible porque está protegido con contraseña. Se ejecuta el software

2675 Passware, que se encarga entre otras cosas de descubrir las contraseñas en archivos ofimáticos protegidos (Fig. 4.25).



Fig. 4.25. Análisis software Passware.

2680 Se ubica el documento protegido con contraseña, el software Passware descubre la contraseña, el cual es el número 123456, solo seis caracteres, lo que facilitó su consecución.

Contraseña	?	×
Contraseña para abrir C:\Users\Ivan\Desktop\ ••••••	el archivo contactos9.	docx
Acepta	r Car	ncelar

Fig. 4.26. Extracción contraseña documento Word con Passware.

Al abrir el archivo se encuentra un documento con nombres, correos electrónicos y alias de personas. Se supone que son personas habituales a los foros de los canales activos en el programa *xchat*.

Autoguardado 💽 🖳				ss9.docx				
hivo Inicio Insertar	Diseño Disposición	Referencias Correspo	ndencia Revisar Vi	sta Zolero Ayuda	Nitro Pro 10 🔎 ¿Qué dese	a hacer?	🖻 Compartir	Comentar
Gernar Ger • ✓ Copiar • ✓ Copiar formato	Calibri (Cuerpt * $ 11 + A^{\circ} A^{\vee}$ N K <u>S</u> + elb x, x ² A -	Aa+ Ap IΞ+IΞ+ ℓ Δ IΞ Ξ	E·EE2 2↓ ¶ ≣ E· &·⊞·	AaBbCcDr T Normal T Sin espa	AaBbCc AaBbCcc AaB Titulo 1 Titulo 2 Titulo	AaBbCcC + Subtitulo +	, O Buscar → G ^b _c Reemplazar D Seleccionar→	Dictar
Portapapeles ra	Fuente	ra l	Párrato ra		Estilos	5	Edición	Voz
	Lin Tai Lui	ia <u>Gonzalez</u> nia <u>Perez</u> isa <u>Scoth</u>	27 años 19 años 21 años	México Venezuela Estados Unidos	linag@gmail.com tania.perez@hotmail.com luisascotch@gmail.com	n		
	Ga	briela Montes	22 años	Venezuela	gscmontes@gmail.com	mailto:sandraperez Ctrl+clic para segu	Ogmail.com ir vinculo	
	Sa	nora <u>Peres</u> Arroyave	21 anos 20 años	Colombia	sangraperez@gmail.com			
	Sa	ndra	22 años	Colombia	sandracolombianita			

2690

Fig. 4.27. Archivo Word analizar.

Se investiga con el jefe de personal y menciona que en la noche solo se queda el vigilante, que no hay más nadie dentro de las instalaciones de la entidad a esa hora.

2695

Se le pregunta al usuario afectado si existe la posibilidad de que el vigilante supiera la clave del usuario root del equipo afectado y reconoce que sí, que él se la dio un día para que consultara algo en internet ya que los demás computadores estaban ocupados. Se ejecuta el software Wireshark y se deja activo toda la noche, para que capture el tráfico que se en la red en esas horas (Fig. 4.28).



Fig. 4.28. Ejecución software Wireshark.

2705

Al día siguiente se analiza el tráfico y se encuentran trazas con los nombres de los contactos registrados en el archivo de Word, desprotegido anteriormente. Se concluye que esa noche el vigilante volvió a ingresar a la plataforma de Chat XCHAT, confirmando que 2710 es la persona que por su actuación indebida a ingresado desde el servidor a portales web peligrosas, ha propiciado el incidente de seguridad al servidor, la falta de gestión en la seguridad del servidor por parte de la persona responsable de ello (Fig. 4.29).

λ	Сар	turir	ng fr	om N	licro	soft:	\Dev	/ice\	NPF_	{579	3621	0-66	551-4	890-l	ACC-	EF63	71653/	\B6}	[Wires	shark	1.8.4	I (SVN	(Re	/ 4625	0 fror	n/tru	k-1.8)]				Ð	_ 5	×
E	e	Edit	Ую	N G	0 9	japtur	e é	ynaly:	28 9	<u>tatist</u>	ics	Telepi	hony	Ioo	s įni	ternak	s <u>H</u> elp																	
	()	al I	24	e (1	8	в (×	3	8	9	4	- 6)	4) T	2			0	Q	0	•		1	5	*	H						
Fi	er:															v	Expres	ssion	Gtat			Save												
No.		1	ime			Soun	ce .					Desti	nation				Proto	col (L	ength	Info														-
		21 7	75.1	7131	680	192	.16	8.0	.22			217	.14	5.6.	3		TCP		54	td	-pos	tman	1 >	5938	[AC	K] 5	2q=49	AC	k=49	win	=32702	Len	-0	
		22 8	38.	7960	400	192	.16	8.0	0.1			224	.0.0	0.1			IGM	IPv2	42	2 Mer	nber	ship	QU	iery,	gen	eral								
		23 1	38.	7970	0770	192	.10	8.0	0.1			224	.0.1	0.1			IGM	IPV3	46	5 Mer	nber	ship	QU	iery,	gen	eral								
		24 8	59.1	213	1890	192	.10	8.0	. 22			239	.25	0.25	5.25	0	IGM	PV2	40	o mer	nber	snip	Re	port	gro	up 2	19.23	0.2	55.2	50				
		25 8	59.	214:	060	192	.10	8.0	. 22			224	.0.1	0.25	2		IGM	PV2	40	o me	nper	snip	Re	port	gro	up 2.	4.0.	0.2	52	50				
		27 1	20 3	21 7/	1214	107	10	0.0	26			224	0.0	2.25	2		TCM	EV2	44	Mar	abar	chin	De	port	gro	up 21	24 0	0.2	52	50				
		28 0	00	2521	770	1 97	16	8.0	1.20			216	52	233	171		TIS	1.7	82	3 An	alic	atio		ata	gru	up 2.		0.2	32					
		29 0	0.	475	800	216	. 52	. 23	3.1	71		192	.16	B. O.	22		TLS	v1.2	88	3 AD	alic	atio	n c	ata										
		30 9	90.	6758	3680	192	.16	8.0	. 22			216	. 52	233	.171		TCP		54	da	nf-a	k2 >	ht	tps	EACK	1 Se	=137	AC	k=13	7 Wi	n=4040	Len	=0	
		31 9	95.3	213	970	Hor	наі	Pr_	84 :	03:b	5	Hon	Hail	Pr_6	7:07	:0e	ARP		42	2 wh	o ha	s 19	2.1	68.0	.1?	теТ	192	2.16	8.0.	22				
		32 9	95.3	2153	860	Hor	на1	Pr_	67:	07:0)e	Hon	на1	Pr_8	4:03	:b5	ARP		42	2 19	2.16	8.0.	11	s at	9c:	2a:7	:67:	:07:	0e					1
€																																	•	ſ
Ð	Fra	ame	1:	88	byt	es i	on v	vine	e (7	04	bits	э.	88	byte	s ca	ptu	red (704 k	oits)	on	int	erfa	ce	0										-
ŧ	Eth	nerr	net	II,	Sr	C: 1	Hone	lair	Pr_8	4:0	3:b:	5 (9	0:4	c:e5	:84:	03:1	05),	Dst:	HonH	aiP	_67	:07:	0e	(9c:	2a:7	0:67:	07:0	(e)						
ŧ	Int	terr	net	Pro	too	01	ver:	sion	n 4,	Sr	c: 1	192.	168	. 0. 2	2 (1	.92.3	168.0	.22),	, Dst	: 23	16.5	2.23	3.1	71 (216.	52.23	3.17	1)						
ŧ	Tra	ansr	115:	sior	CC	ntri	ol a	Prot	toco	1, :	Src	Por	t: I	danf	-ak2	2 (1)	341),	Dst	Port	: h	tps	(44	3),	Seq	: 1,	Ack:	1,	Len	: 34					
Đ	Sev	sune	? S(ock (ts	Lay	er																											
1																																		
																	_	_																_
00	00	90	2a	70	67	07	0e	90	4c	eS	84	03	bs (0 8 0	45	00	:"	pg	-		Ε.							_	_					-
00	20	69	be ab	04	a5 11	40	00 hh	64	05	10	45	64	a8 0	10 1	5 08	34 19	1,11	a. e	يار ز		-4													
00	ŝŏ	ōf	ea	d8	d6	ŏõ	00	17	03	ô3	00	1d	8d 9	2 b	i c8	cc																		
00	40	87	ca	89	82	61	43	69	b9	68	08	d6	e5 2	4 4	5 79	3f		aci	. h.	\$F	y?													
00	50	0b	55	28	d1	89	ua	21	16								. 01	(/																
1																																		
		_																																_
\odot	Y.	Micro	soft:	Dev	icely	PF_(5	7936	2F0-4	6651-	4890-	BAC	Pack	ets: 3	2 Displ	ayed:	32 Ma	rked: 0								Pro	ile: Del	aut							

Fig. 4.29. Análisis disco duro con Wireshark.

2715

Se concluye que, a través del programa de chat, alguien logro detectar la dirección ip y penetrar el sistema por tener un usuario root con una contraseña trivial. Se deduce que debieron utilizar un software de ataque por fuerza bruta, ya que el día del incidente se dieron más de dieciséis intentos de conexión fallidos, antes de la conexión satisfactoria utilizando el protocolo ssh. В

Bot: Es un programa informático que efectúa automáticamente tareas repetitivas a través de Internet, cuya realización por parte de una persona sería imposible o muy tediosa. Algunos ejemplos de

2730 bots son los rastreadores web de los motores de búsqueda de Internet, que recorren los sitios web de forma automática y recopilan información de los mismos de manera mucho más rápida y efectiva de lo que lo haría una persona.

Bookmark: Un marcador de Internet es la localización almacenada
2735 de una página web de forma que puede ser revisitada más adelante.
La localización de una página web suele expresarse con una URL.
Todos los navegadores web modernos incorporan como característica la posibilidad de catalogar y acceder fácilmente a las webs que el usuario ya ha visitado y guardado.

2740 C

Clonado: Proceso de copia, a bajo nivel y firmada digitalmente, de la información original por el cual se traslada ésta a un nuevo soporte de almacenamiento digital, preservando la inalterabilidad de la información en el sistema o soporte de origen y asegurando laidentidad total entre aquella y la extraída.

COMMIT: Es la idea de confirmar un conjunto de cambios provisionales de forma permanente.

Cookie: Es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador.

Cracker: Son las personas que rompen o vulneran algún sistema de seguridad1 de forma ilícita.

Cracking: Es una conducta delictiva en donde un individuo denominado cracker altera, modifica, elimina, borra los datos de un
programa informático o de un documento con la finalidad de obtener un beneficio de dicha alteración; puede referirse a varias prácticas similares, o al conjunto de ellas

D

2750

Dumpear: Registro no estructurado del contenido de la memoria
en un momento concreto, generalmente utilizado para depurar un programa que ha finalizado su ejecución incorrectamente.

Ε

ERUNT: La Utilidad de Recuperación de Emergencia NT, es una utilidad que se puede usar para respaldar y restaurar el Registro de

2765 Windows. Esta herramienta tiene la capacidad de realizar una copia de seguridad completa y restaurar el Registro de Windows, incluida la sección de seguridad para que los permisos se respalden y se restauren correctamente.

Evidencia: Cada uno de los datos digitales recogidos en la escena2770 de interés susceptible de ser analizados con una metodología forense.

F

Firewall: Un cortafuego (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no
autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

2780 Framework: Un framework, entorno de trabajo o marco de trabajo es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.

2785 **G**:

Gateway: Es una 'puerta de enlace' (equipo para interconectar redes).

Η

Hacking: El hacking informático recurre a la manipulación de la
conducta normal de un equipo y de los sistemas que tiene conectados. Esto se hace generalmente mediante scripts o programas que manipulan los datos que pasan a través de una conexión de red con el fin de acceder a la información del sistema. Las técnicas de hacking incluyen el uso de virus, gusanos, Troyanos,

2795 ransomware, secuestros del navegador, rootkits y ataques de denegación de servicio.

Hardware: Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

2800 Hash: Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.

I

Informática forense: Es la ciencia de adquirir, preservar, obtener y

2805 presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

IP: Es un número que identifica, de manera lógica y jerárquica, a una interfaz en red (elemento de comunicación/conexión de un dispositivo (computadora, Tablet, portátil, Smartphone) que utilice el protocolo IP).

K

2810

Kernel: Es un software que constituye una parte fundamental del sistema operativo, y se define como la parte que se ejecuta en modo privilegiado (conocido también como modo núcleo).

2815 L

Live: Es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD, que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora.

Μ

2820 Malware: Hace referencia a cualquier tipo de software maligno que trata de afectar a un ordenador, a un teléfono celular u otro dispositivo.

Р

Parsear: Recorrer todos los registros de una base de datos.

2825 Path: Es una variable de entorno de los sistemas operativos POSIX y los sistemas de Microsoft, en ella se especifican las rutas en las cuales el intérprete de comandos debe buscar los programas a ejecutar.

Plugins: Es una aplicación (o programa informático) que se
2830 relaciona con otra para agregarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la

aplicación principal e interactúan por medio de la interfaz de programación de aplicaciones.

Programa: Secuencia de instrucciones que una computadora puede2835 interpretar y ejecutar.

R

Ransomware: Es un tipo de virus que impide o limita el acceso del usuario a su propio sistema informático.

Regedit: Es el nombre de la herramienta que permite editar el
2840 registro del sistema operativo Windows. Este registro es la base de datos donde se guardan las preferencias del usuario en materia de configuraciones.

Registro: Conjunto de datos que almacena la información y configuraciones de todo el hardware, software, usuarios y
2845 preferencias de un sistema de información.

Roaming: Refiere a la capacidad de un teléfono de efectuar y de recibir llamados más allá del área de servicio local de la empresa que brinda la prestación. De este modo, haciendo uso del roaming, un

usuario puede comunicarse en países extranjeros o en regiones 2850 donde su compañía de telefonía no opera.

S

Sistema de Archivos: Es un método para el almacenamiento y organización de archivos de computadora y los datos que estos contienen, para hacer más fácil la tarea encontrarlos y accederlos.

2855 Sistema de ficheros: Organización lógica de un dispositivo.

Sniffing: Un sniffer es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

Software: Es el conjunto de los programas de cómputo,
procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación.

Spam: Los términos correo basura, correo no solicitado y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido (o incluso correo anónimo o de falso

2865 remitente), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de

alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

Swap: El espacio de intercambio de un disco.

2870 T

Tap de red: Los TAPs de red (Terminal Access Point por sus siglas en inglés) son el dispositivo de hardware más común a la hora de capturar tráfico de red. Un TAP de red es básicamente un hardware diseñado para acceder al tráfico entre dos nodos de red y reflejarlo

2875 en un puerto de monitor donde podemos conectar una herramienta de análisis de terceros para escuchar.

TCP: Es la capa intermedia entre el protocolo de red (IP) y la aplicación, algunas veces las aplicaciones necesitan que la comunicación a través de la red sea confiable.

2880 Test de Deubert: Es un conjunto de reglas extraídas de la sentencia de la Corte Suprema de Justicia Estadounidense

Timestamps: Conocida también como registro de tiempo **que** es una secuencia de caracteres que denotan la hora y fecha (o alguna de ellas) en la/s que ocurrió determinado evento. **2885 Trazabilidad:** Capacidad de seguimiento y reconstrucción de acciones efectuadas por los usuarios en un sistema.

Troyano: Es un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

V

Memoria volátil: Es aquella memoria cuya información se pierde al interrumpirse el flujo eléctrico

2895

2890

GLOSARIO DE SIGLAS

A

2905	ARP: Address Resolution Protocol
	С
	CERT: Community Emergency Response Team
	CD: Compact Disk
	CMD: Command prompt
2910	D
	DLL: Dynamic-Link Library
	DNS: Domain Name System
	DVD: Digital Versatile Disc
	F
2915	FTP: File Transfer Protocol
	G
	GB: Gigabyte
	Н
HIVE: Hierarchy of International Vengeance and Extermination

2920 HKLM: HKEY_LOCAL_MACHINE

HKU: HKEY_USERS

HTML: HyperText Markup Language

HTTP: Hypertext Transfer Protocol

I

2925 IE: Internet Explorer

IP: Internet Protocol

M

MFT: Máster File Table

Р

2930 PC: Personal Computer

Pd: Process Dumper

PID: Identificador de proceso

R

RAM: Random Access Memory

S

	SAM: Sequential Access Memory
	SID: Standard Instrumental Departure
	SD: Secure Digital
	SMB: Server Message Block
2940	SMS: Safety Management System
	SO: Sistema operativo
	Т
	TAP: Terminal Access Point
	TCP: Protocolo de Control de Transmisión
2945	U
	URL: Uniform Resource Locator
	USB: Universal Serial Bus
	W
	WWW: World Wide Web
2950	

BIBLIOGRAFÍA

	Arnedo Blanco, P. (2014). Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos. Valledupar.
2955	Arsuaga Cortázar, D. J. (2010). La Prueba Pericial en la Ley de Enjuiciamiento Civil (Ley 1/2000). Santander.
	Casey, E. (2001). Handbook of Computer Crime Investigation. Academic Press.
	Casey, E. (2004). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
2960	Copyleft. (2018). Archivo Pagefile.sys . Obtenido de https://www.elhacker.net/archivo-pagefile-sys.html
	Darknet. (2018). Hacking Tools, Hacker News & Cyber Security. Obtenido de https://www.darknet.org.uk/2015/11/rekall- memory-forensic-framework/
2965	Deering, B. (s.f.). <i>Data Validation Using The Md5 Hash</i> . Obtenido de http://www.forensics-intl.com/art12.html
	Delgado, B. (1994). La Educación en la España Contemporánea. Madrid: Morata.
2970	Gervilla Rivas, C. (2014). <i>Metodología para un Análisis Forense</i> . Barcelona.
2975	Hernando, S. (11 de Julio de 2011). Analisis forense de perfiles de usuario en Windows. Introducción a las Shellbags. Obtenido de http://www.sahw.com/wp/archivos/2011/07/11/analisis -forense-de-perfiles-de-usuario-en-windows-introduccion- a-las-shellbags/
2373	Hidalgo Cajo, I. (2014). Análisis preliminar y Diseño de una Herramienta de toma de decisiones como soporte para las tareas de Análisis Forense Informático. Tarragona.
2980	IOCE. (2000). International Organization of Computer Evidence. Obtenido de http://www.ioce.org

2985	Navarro Clérigues, J. (2014). <i>Guía actualizada para futuros peritos</i> <i>informáticos. Últimas herramientas de análisis forense digital. Caso</i> <i>práctico.</i> Obtenido de http://www.pensamientopenal.com.ar/system/files/2016/ 05/doctrina43429.pdf
	Pato Rodríguez , A. (2006). <i>Metodología para realizar el manejo de incidentes de seguridad de TI mediante actividades de forénsica digital.</i> Caracas.
2990	Paus, L. (2 de Marzo de 2016). <i>Análisis forense de redes con</i> <i>NetworkMiner 2.0 para identificar anomalías</i> . Obtenido de https://www.welivesecurity.com/la- es/2016/03/02/analisis-forense-de-redes-networkminer/
2995	Quezada, A. C. (05 de Febrero de 2014). <i>Crear La Imagen Forense Desde Una Unidad Utilizando FTK Imager</i> . Obtenido de http://www.reydes.com/d/?q=Crear_la_Imagen_Forense _desde_una_Unidad_utilizando_FTK_Imager
3000	ReYDeS, A. C. (2018). Crear La Imagen Forense Desde Una Unidad Utilizando FTK Imager. Obtenido de http://www.reydes.com/d/?q=Crear_la_Imagen_Forense _desde_una_Unidad_utilizando_FTK_Imager
	Russinovich, M. (1999). Inside The Registry. ITProWindows.
3005	Sánchez Cordero, P. (Enero de 2014). <i>Conexión Inversa</i> . Obtenido de http://conexioninversa.blogspot.com/2014/01/artefactos -forenses-ii-prefetch-y.html
	Sánchez Cordero, P. (2014). Introducción al Análisis Forense Informático. Barcelona, Barcelona, España.
	Sánchez Cordero, P. (2015). Análisis Forense Informático. Barcelona.
3010	Santos Tello, J. D. (2013). PROCEDIMIENTOS EN LA INVESTIGACIÓN, RECOLECCIÓN Y MANEJO DE LA EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN. Huehuetenango.

	SleuthKit-Autopsy. (2003). Open Source Digital Forensics. Obtenido de https://www.sleuthkit.org/autopsy/
3015	Sofer, N. (2001). <i>NirSoft</i> . Obtenido de http://www.nirsoft.net/utils/usb_devices_view.html
	Telefónica Móviles España, S. (s.f.). <i>Movistar</i> . Obtenido de http://conexioninversa.blogspot.com.es/2008/10/ceregu mil-concentrado.html
3020	Tocados Cano, J. (2015). <i>Metodología para el desarrollo de procedimientos periciales en el ámbito de la informática forense</i> . La Mancha.
	UNE-71506. (2013). <i>Metodología para el análisis forense de las evidencias electrónicas</i> . Madrid: AENOR.
3025	UNE-71506. (Julio de 2013). Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas. Obtenido de http://www.aenor.es/aenor/normas/normas/fichanorma.
	asp?tipo=N&codigo=N0051414#.Wor0yajOXIU welivesecurity. (02 de Marzo de 2016). Análisis forense de redes con
3030	NetworkMiner 2.0 para identificar anomalías. Obtenido de https://www.welivesecurity.com/la- es/2016/03/02/analisis_forense-de-redes-networkminer/
3030	<i>NetworkMiner 2.0 para identificar anomalías.</i> Obtenido de https://www.welivesecurity.com/la- es/2016/03/02/analisis-forense-de-redes-networkminer.

3035 "Las evidencias digitales en la investigación forense informática son cualquier documento, fichero, registro, dato, etc., contenido en un soporte informático y que es susceptible de tratamiento digital".

- Iván Mesias Hidalgo Cajo, Máster Universitario en Ingeniería
 Informática: Seguridad Informática y Sistemas Inteligentes, Universidad Rovira i Virgili, España; Ingeniero en Sistemas Informáticos, ESPOCH, Ecuador, Tecnólogo en Informática: Programación y Análisis de Sistemas, Instituto Tecnológico Superior Harvard Comput, Ecuador.
- 3045 Su especialización en Seguridad Informática e Inteligencia Artificial se ha inducido por la Informática Forense y la detección de intrusiones, actualmente es docente universitario en las asignaturas de seguridad y pertenece a un grupo de investigación en España sobre la Inteligencia Artificial, Robótica y Visión, desempeñándose
- 3050 en trabajos relacionados en el campo de la seguridad, participa anualmente en los cursos que desarrolla las universidades de Europa sobre Peritaje Informático e Informática Forense en los cuales existen cyber-ejercicios de desarrollo y desarrollan una serie de metodologías, pruebas, clasificaciones, y ven los impactos, defensas.
- **3055** Proporciona conferencias a nivel nacional e internacional sobre la cyber-seguridad.

Byron Geovanny Hidalgo Cajo, Máster Universitario en Ingeniería Computacional y Matemática, Universidad Rovira i Virgili, España, Magister en Docencia Universitaria e Investigación

- 3060 Educativa, UTPL, Ecuador, Diploma Superior las Nuevas Tecnologías de la Información y Comunicación y su aplicación en la Práctica Docente Ecuatoriana, UTPL, Ecuador, Ingeniero en Computación y Ciencias de la Informática, ESPOJ, Ecuador.
- Saul Yasaca Pucuna, Magíster en Informática Educativa,
 3065 ESPOCH, Ecuador, Ingeniero en Sistemas Informáticos, ESPOCH, Ecuador.

Diego Patricio Hidalgo Cajo, Magíster en Educación Matemática, UNACH, Ecuador, Licenciado en Ciencias de la Educación profesor de Ciencias Exactas, UNACH, Ecuador.

3070 Jessica Janeth Aragadbay Ola, Abogada de los Tribunales y Juzgados de la República, UNACH, Ecuador, Ingeniera en Gestión de Gobiernos Seccionales, ESPOCH, Ecuador.

ISBN Código Barras

186