Guía de toma de evidencias

en entornos Windows®

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Autor

Asier Martínez Retenaga

Esta guía ha sido elaborada con la colaboración de Daniel Fírvida Pereira y Jesús Díaz Vico.

Noviembre 2014

ÍNDICE

1 SOBRE LA GUÍA

Este documento proporciona información relacionada con el análisis forense digital, y en concreto en entornos Windows. Se centra en el proceso de toma de evidencias, realizándose las pruebas sobre Windows XP (pese a que haya finalizado su soporte, aún tiene una cuota de mercado importante), Windows 7, Windows 8 y 8.1, si bien los ejemplos indicados son aplicables en muchos casos a otras versiones del sistema operativo al tener una estructura similar.

Ofrece tanto una visión global acerca del proceso, explicando en qué consiste, para qué sirve, las fases que lo componen, las metodologías para llevarlo a cabo, etc., como una visión específica en lo que a la obtención de evidencias se refiere. Es importante tener presente que pese a que la guía realiza una primera aproximación al proceso de análisis forense digital, se centra principalmente en la fase de obtención de evidencias, y ese es su objetivo.

El público objetivo del documento son profesionales del sector informático: técnicos de soporte IT, administradores de sistemas, administradores de redes, analistas de malware, etc., que tienen conocimientos informáticos pero no están familiarizados con el proceso de análisis forense digital y que pudieran acabar enfrentándose a algún tipo de incidente que requiera realizar uno.

El documento pretende ser una guía práctica de los pasos a seguir en el caso de que surja un incidente con el fin de recopilar las evidencias necesarias para realizar un posterior análisis que derive en una solución para el propio incidente, este análisis posterior esta fuera del ámbito de este documento.

Se van a utilizar herramientas gratuitas con el fin de que dicho procedimiento no suponga un coste adicional en cuanto a licencias se refiere.

1.1. NOTACIONES UTILIZADAS

En el documento se utilizan las siguientes notaciones:

Ejemplo	Secciones o apartados del documento en los que se desee realizar una demostración de en qué casos puede resultar práctica la información explicada.
¡Importante!	Resalta cierta información de notable relevancia y que debe tenerse especialmente en cuenta.
Nota	Informa acerca de algún aspecto a tener en cuenta.
Otras utilidades	Indica otras herramientas con similares características o funcionalidades a la que se ha sido previamente indicada.

2 INTRODUCCIÓN AL ANÁLISIS FORENSE

El concepto de análisis forense digital hace referencia a un conjunto de procedimientos de recopilación y análisis de evidencias que se realizan con el fin de responder a un incidente relacionado con la seguridad informática y que, en ocasiones, deben de servir como pruebas ante un tribunal. Mediante este procedimiento se pretende responder a las siguientes preguntas: *¿qué?, ¿dónde?, ¿cuándo?, ¿por qué?, ¿quién? y ¿cómo?*

Esta ciencia está adquiriendo un papel muy importante en los últimos años ya que cada día es más habitual tener que hacer frente a diferentes incidentes relacionados con la seguridad informática como por ejemplo: intrusiones, robos de información, infecciones, etc.

Su uso está extendido por muy diversos campos, entre los que destacan:

- Persecución de delitos como fraude financiero, evasión de impuestos, acoso o pornografía infantil.
- Casos de discriminación o acoso.
- Investigación de seguros.
- Recuperación de ficheros eliminados.
- Casos de robo de la propiedad intelectual.
- Ciberterrorismo.
- Asegurar la resiliencia de las empresas, es decir, la capacidad de recuperación frente a ataques.

A lo largo del documento se detallará la manera de proceder, ya que es fundamental tener claras las pautas que se deben seguir a la hora de realizar un análisis forense digital con el fin de no destruir pruebas que imposibiliten resolver el incidente de una manera satisfactoria. Un incidente es resuelto de manera satisfactoria cuando se extraen conclusiones que permiten responder a las preguntas anteriormente planteadas.

2.1. PRINCIPIO DE LOCARD

A la hora de realizar un análisis forense digital es fundamental tener presente el principio de intercambio de Locard, el cuál sentó las bases de la ciencia forense, y que dice lo siguiente: "*siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto*". Esto significa que cualquier tipo de delito, incluidos los relacionados con la informática que son los que nos atañen, dejan un rastro por lo que mediante el proceso de análisis forense se pueden obtener evidencias.

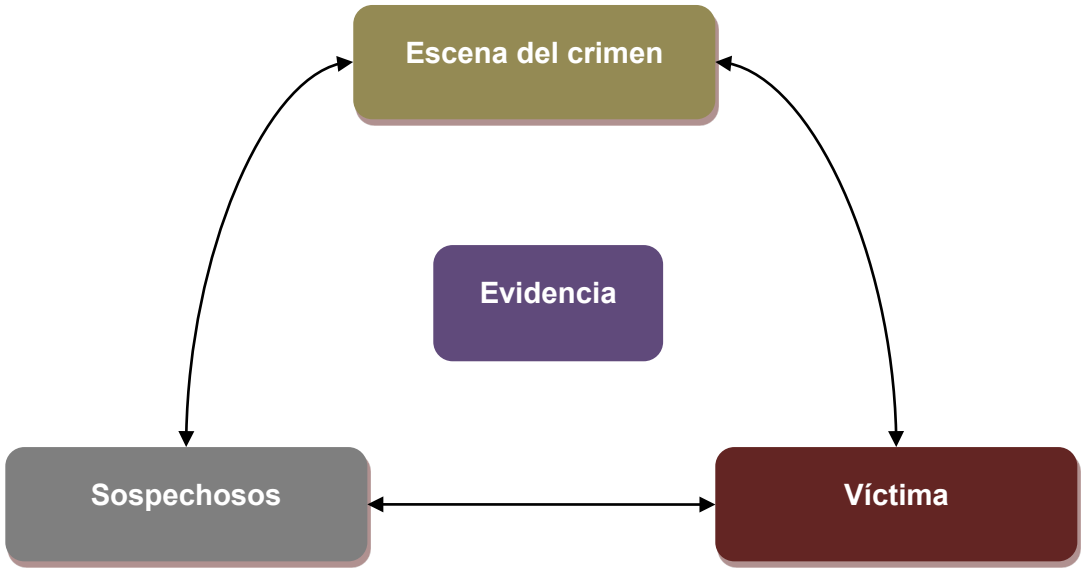

Ilustración 1: Principio de intercambio de Locard

¡Importante!

Del mismo modo, se cumple el principio de Locard a la hora de realizar el propio análisis forense por lo que hay que ser especialmente cuidadoso para que el sistema se vea afectado en la menor medida posible y que las evidencias adquiridas no se vean alteradas.

2.2. TIPOS DE ANÁLISIS FORENSE

Se puede crear una clasificación de tipos de análisis forense en base a qué estén orientados a analizar. Teniendo en cuenta este aspecto se pueden identificar tres tipos de análisis:

- Análisis forense de sistemas: tanto sistemas operativos Windows, como OSX, GNU/Linux, etc.
- Análisis forense de redes.
- Análisis forense de sistemas embebidos.
- Análisis forense de memoria volátil.

Esta guía, como su propio nombre indica y se ha comentado anteriormente, se centra en la toma de evidencias en entornos Windows, si bien el proceso, desde un punto de vista global, es similar para todos los tipos.

2.3. CARACTERÍSTICAS

El procedimiento de análisis forense debe poseer las siguientes características:

- **Verificable**: se debe poder comprobar la veracidad de las conclusiones extraídas a partir de la realización del análisis.
- **Reproducible**: se deben poder reproducir en todo momento las pruebas realizadas durante el proceso.
- **Documentado:** todo el proceso debe estar correctamente documentado y debe realizarse de manera comprensible y detallada.
- **Independiente:** las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología utilizada.

2.4. FASES

El procedimiento de análisis forense consta de las siguientes fases:

Ilustración 2: Fases del análisis forense digital.

- **Preservación**: corresponde a la fase en la que se debe garantizar que no se pierdan las evidencias que deben ser recopiladas para su posterior análisis. El desconocimiento puede provocar que se pierda información relevante y que podría resultar decisiva para la resolución del incidente. Aspectos críticos como que no se apaguen los equipos para poder preservar la información volátil o la correcta rotulación de los elementos a analizar se realizan durante esta fase.

  Así mismo, se debe mantener un registro continuo de las operaciones que se van realizando sobre el material a analizar con el fin de mantener la validez jurídica de las evidencias que se recopilen a posteriori, en el caso de que sea necesario. Si los materiales deben ser transportados, se debe realizar con sumo cuidado, evitando que la información sea alterada o que se vea expuesta a temperaturas extremas o campos electromagnéticos.

- **Adquisición**: Esta es la fase en la que se centra esta guía, y la que se explicará con mayor detalle, y corresponde a la etapa en la que se recopilan las evidencias. Una evidencia puede ser definida como cualquier prueba que pueda ser utilizada en un proceso legal, aunque no siempre sea así.

  Características de las evidencias:

  - **Admisible**: debe tener valor legal.
  - **Auténtica**: debe ser verídica y no haber sufrido manipulación alguna. Para ello, deben haberse sacado los correspondientes hashes con el fin de asegurar la integridad.

  - **Completa**: debe representar la prueba desde un punto de vista objetivo y técnico, sin valoraciones personales, ni prejuicios.
  - **Creíble**: debe ser comprensible.
  - **Confiable**: las técnicas utilizadas para la obtención de la evidencia no deben generar ninguna duda sobre su veracidad y autenticidad.

Pueden ser clasificadas en dos tipos:

- *Evidencia física:* hace referencia al material informático como por ejemplo: discos duros, *pendrives*, etc.
- *Evidencia digital*: corresponde a la información almacenada en las evidencias electrónicas.

  Algunos ejemplos de evidencias digitales son:

  - Fichero en disco.
  - Proceso en ejecución.
  - Log.
  - Archivos temporales.
  - Entradas de registro.

- **Análisis**: a la hora de realizar el análisis de la información recopilada se debe tener presente el tipo de incidente al que se pretende ofrecer respuesta. Dependiendo del caso puede resultar útil analizar en profundidad diferentes aspectos como:

  - **MFT o *Master File Table***: corresponde a la tabla que almacena información sobre los ficheros almacenados en el disco. Almacena información como el nombre, fechas de acceso, creación y modificación, ubicación de los datos en disco, etc.
  - **Archivo de paginación** (*Pagefile.sys*): es un fichero que permite optimizar el uso de la memoria RAM ya que el sistema operativo envía ahí temporalmente la información que no sea necesaria en ese momento para los procesos en ejecución y posteriormente la recupera en el caso de que alguno la solicite.
  - **Papelera de reciclaje**.
  - **Espacio no asignado**: corresponde al espacio en disco disponible para almacenar información. Cuando se elimina un fichero en Windows, el sistema operativo elimina la referencia a dicha información pero no la información en sí, sino que sólo la marca como sobre escribible. Es por ello que tal información puede ser recuperada mediante diferentes métodos.
  - **Registro de Windows**: en el registro de Windows se almacena muy diversa información como por ejemplo las redes a las que se ha conectado el equipo, el listado de páginas visitadas, los archivos abiertos recientemente, las aplicaciones instaladas, el histórico de dispositivos USB conectados, etc.
  - ***Slack Space***: hace referencia al espacio libre que queda en un *clúster* (conjunto contiguo de sectores que componen la unidad más pequeña de almacenamiento de información en un disco) tras almacenar un fichero.

  - **Tráfico de red**.
  - **Procesos del sistema**.
  - **Logs del sistema**: como por ejemplo el registro de sucesos relativos al sistema, a la seguridad o a las aplicaciones.

  Es fundamental que todo el proceso sea realizado desde un punto de vista objetivo, sin descartar lo que para el analista pueda ser considerado como obvio.

- **Documentación**: un aspecto fundamental en el proceso del análisis forense es el de la documentación por lo que se debe realizar dicha fase de una manera muy metódica y detallada. Se pueden realizar, entre otras, las siguientes acciones:
  - Fotografiar las pruebas.
  - Cadena de custodia.
  - Documentar todos y cada uno de los pasos realizados durante el proceso, manteniendo una bitácora con fechas y horas de cada acción realizada sobre las evidencias.
  - Elaborar dos tipos de informe de conclusiones: uno ejecutivo y uno técnico.
- **Presentación**: la fase de presentación de la información es tan importante o más que las anteriores ya que se deben hacer accesibles y comprensibles las conclusiones que se han obtenido del proceso del análisis forense.

  Para ello, es recomendable seguir las siguientes pautas:
  - Preparar una presentación de manera pedagógica que sea fácilmente comprensible.
  - Detallar las conclusiones.
  - Explicar de manera clara el proceso que se ha llevado para la obtención de las evidencias.
  - Evitar las afirmaciones no demostrables o los juicios de valor.
  - Elaborar las conclusiones desde un punto de vista objetivo.

Hay que tener presente que las fases no son secuenciales sino que están entrelazadas entre sí. Por ejemplo, la fase de documentación comienza en la fase de preservación.

2.5. METODOLOGÍAS Y GUÍAS

Existen diferentes metodologías o guías a la hora de realizar un análisis forense, si bien todas tienen aspectos comunes. Como referencia para este documento se va a tomar el *RFC 3227*[1] «*directrices para la recopilación de evidencias y su almacenamiento*», el cual refleja de una manera completa el proceso de actuación y las pautas que se deben seguir a la hora de realizar un análisis de éste tipo.

[1] http://www.ietf.org/rfc/rfc3227.txt

A continuación, se mencionan otra serie de guías que pueden servir de referencia para aquellos lectores interesados en profundizar en el tema:

- *Guidelines for the best practices in the forensic examination of digital technology*[2]
- *Electronic Crime Scene Investigation: A Guide for First Responders*[3]
- Forensic Examination of Digital Evidence: A Guide for Law Enforcement[4]
- *UNE 71506 - Metodología para el análisis forense de las evidencias electrónicas*[5]
- *ISO/IEC 27037:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence*[6]

[2] http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html
[3] https://www.ncjrs.gov/pdffiles1/nij/187736.pdf
[4] https://www.ncjrs.gov/pdffiles1/nij/199408.pdf
[5] http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414&PDF=Si#.UmTshXC8B5H
[6] http://www.iso.org/iso/catalogue_detail?csnumber=44381

3 TIPOLOGÍAS DE UN INCIDENTE

Existe una gran cantidad de incidentes relacionados con la seguridad informática:

Atendiendo a aquellos a los que con mayor probabilidad se va a enfrentar el público objetivo de esta guía, y teniendo en cuenta que algunos de ellos pueden tener relación entre sí, se pueden identificar los siguientes:

- **Robo de información**: El robo de información privada es una las preocupaciones mayores tanto para usuarios como para empresas. Existen multitud de prácticas que permiten el robo de información como por ejemplo la monitorización del tráfico de red mediante un *sniffer*, la intercepción de emails o simplemente mediante la inserción de un pendrive y la copia información privada, etc. Dicha información se utiliza principalmente para obtener un beneficio económico, si bien en algunos casos se usa únicamente para dañar la imagen del afectado.
- **Fraude**: Existen multitud de ejemplos de fraudes a través de Internet, entre los que destacan:
  - Falsas ofertas de empleo[7].

[7] http://www.osi.es/es/actualidad/blog/2013/05/07/fraudes-online-iv-ofertas-falsas-de-trabajo

- Estafas de loterías y sorteos[8].
- Falsas herencias.
- Fraudes de inversiones y créditos.
- Falsos correos para donaciones a alguna ONG[9].
- Falsas facturas de servicios de mensajería.
- Descargas que facturan servicio de SMS Premium[10].
- Multas por descargas ilegales.

A lo largo del año se realizan un gran número de campañas, aprovechando fechas significativas o acontecimientos importantes, para propagar este tipo de amenazas.

- **Malware**: El malware es otro de los incidentes más habituales a los que se puede enfrentar un analista forense. La profesionalización del mercado desde hace varios años ha generado un aumento muy importante en lo que al volumen de este tipo de amenazas se refiere, alcanzando en algunos casos unos niveles de sofisticación muy importantes. Algunos de los datos más significativos son los siguientes:
  - Hay alrededor de 170 millones de muestras de malware, de las cuales cerca de 70 millones han surgido en 2013[11].
  - En el año 2012 el número de ficheros correspondientes a malware firmados digitalmente alcanzó los 2 millones[12].
  - En el año 2012 el número de malware correspondiente a ransomware alcanzó las 700.000 muestras[13].
  - El cibercrimen ha generado pérdidas de 87.000 millones euros 2013[14].
  - Kaspersky en el tercer trimestre del 2013 ha catalogado más de 120.000 muestras de malware para móviles[15].
  - McAfee cataloga diariamente más de 100.000 muestras[16].
- **Accesos no autorizados**: Según un estudio de ThreatTrack Security[17] el acceso no autorizado a páginas de contenido sexual es uno de los principales motivos de infección en ordenadores corporativos. Otro ejemplo, a la orden del día, es el aprovechamiento de las vulnerabilidades del software para obtener privilegios y así poder acceder a carpetas o documentos de información confidencial.
- **Uso inapropiado de recursos**: La utilización de recursos de manera inapropiada es una práctica bastante habitual en las empresas: imprimir documentos personales o descargar contenido audiovisual como películas o series son algunos de los ejemplos más habituales.

---

[8] http://www.osi.es/es/actualidad/blog/2013/06/28/fraudes-online-vi-has-ganado-un-premio
[9] http://www.osi.es/es/actualidad/blog/2013/12/13/los-5-fraudes-navidenos-mas-tipicos-que-no-te-enganen
[10] http://www.osi.es/es/actualidad/blog/2013/02/15/identificando-banners-enganosos
[11] http://www.av-test.org/en/statistics/malware/
[12] http://www.scmagazine.com/the-state-of-malware-2013/slideshow/1255/#3
[13] http://www.scmagazine.com/the-state-of-malware-2013/slideshow/1255/#5
[14] http://www.rtve.es/noticias/20131105/cibercrimen-generado-perdidas-87000-millones-euros-ultimo-ano/784565.shtml
[15] http://www.securelist.com/en/analysis/204792312/IT_Threat_Evolution_Q3_2013#14
[16] http://www.mcafee.com/au/resources/reports/rp-quarterly-threat-q1-2013.pdf
[17] http://www.threattracksecurity.com/documents/malware-analysts-study.pdf

- **Propiedad intelectual**: La vulneración de la propiedad intelectual supone un coste anual muy importante. Según un estudio realizado por McAfee sobre el impacto económico del cibercrimen, éste provoca, a nivel mundial, pérdidas de hasta 400.000 millones de dólares y uno de los principales motivos es el robo de la propiedad intelectual. Existen gran cantidad de páginas desde las cuales se pueden descargar películas, música, software, etc. y que tienen un impacto directo en estas pérdidas.
- **Denegación de servicio**: Un ataque de denegación de servicio pretende impedir el acceso a los servicios y recursos de una organización. Este tipo de ataques son normalmente cometidos mediante la utilización de botnets[18] (redes de ordenadores infectados) y han sufrido un incremento notable en los últimos tiempos, y en ocasiones motivados por acciones hacktivistas.

Pese a toda esta diversidad de incidentes, el procedimiento a seguir durante el proceso de toma de evidencias es común en la mayoría de los casos. Si bien hay que tener muy presente que el posterior análisis será específico dependiendo del tipo de incidente.

Existen otro tipo de incidentes, principalmente relacionados con pornografía infantil, apología del terrorismo, extorsión (en este grupo queda incluido, entre otros, el ciberacoso, *ciberbullying*, *grooming*, *sexting* o la vulneración de la intimidad), etc. que deben ser puestos en conocimiento de las autoridades pertinentes con el fin de inicien una investigación y tomen las medidas que consideren oportunas. Este tipo de incidentes están fuera del alcance del documento. Incluso, algunos de los descritos en el punto puede ser necesario ponerlos en conocimiento de las autoridades como por ejemplo los relacionados con el robo de información o el fraude. Para todos ellos, hay que ponerse en contacto con el **Grupo de delitos telemáticos**[19] o el **Cuerpo Nacional de Policía**[20] y seguir los pasos que se indican.

[18] http://www.incibe.es/file/p9cSCisIwwtRK6a0e7iZKg
[19] https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
[20] http://www.policia.es/bit/index.htm

4 DIRECTRICES PARA LA RECOLECCIÓN DE EVIDENCIAS Y SU ALMACENAMIENTO

El *RFC 3227*[21] es un documento que recoge las «*directrices para la recopilación de evidencias y su almacenamiento*» y puede llegar a servir como estándar de facto para la recopilación de información en incidentes de seguridad.

Dicho documento recoge los siguientes apartados:

4.1. PRINCIPIOS DURANTE LA RECOLECCIÓN DE EVIDENCIAS

- Capturar una imagen del sistema tan precisa como sea posible.
- Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.
- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
- **Recoger la información según el orden de volatilidad (de mayor a menor**).
- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

4.1.1. Orden de volatilidad

El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información. Por este motivo se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor.

De acuerdo a esta escala se puede crear la siguiente lista en orden de mayor a menor volatilidad:

- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del *kernel*, memoria.
- Información temporal del sistema.
- Disco.
- Logs del sistema.
- Configuración física y topología de la red.
- Documentos.

[21] http://www.ietf.org/rfc/rfc3227.txt

4.1.2. Acciones que deben evitarse

Se deben evitar las siguientes acciones con el fin de no invalidar el proceso de recolección de información ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan ser utilizados en un juicio en el caso de que sea necesario:

- No apagar el ordenador hasta que se haya recopilado toda la información volátil.
- No confiar en la información proporcionada por los programas del sistema ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido como se explicará más adelante.
- No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

4.1.3. Consideraciones de privacidad

Hay que asegurarse que toda la información recopilada durante el proceso sea tratada dentro del marco legal establecido, manteniendo la privacidad exigida. Los ficheros log están incluidos en este apartado ya que pueden almacenar patrones de comportamiento del usuario del equipo.

4.1.4. Consideraciones legales

Se debe tener presente que la legislación es diferente en cada país por lo que las evidencias pueden ser admitidas en un país y en otro no. En todo caso dichas evidencias deben tener una serie de características comunes:

- **Admisible**: se debe cumplir las normas de la legislación vigente con el fin de que las evidencias tengan validez judicial.
- **Auténtica**: se debe poder probar que la evidencia corresponde al incidente en cuestión.
- **Completa**: debe corresponder a la información completa y no a una visión parcial.
- **Confiable**: no debe existir ninguna duda acerca de cómo se ha obtenido la evidencia y la posterior manipulación que pueda arrojar dudas sobre su autenticidad y veracidad.
- **Creíble**: debe de ser verosímil y fácilmente comprensible por un tribunal.

4.2. PROCEDIMIENTO DE RECOLECCIÓN

El procedimiento de recolección debe de ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones.

4.2.1. Reproducible

Los métodos utilizados para recolectar evidencias deben de ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos usados, y que dichos métodos hayan sido testados por expertos independientes.

4.2.2. Pasos

- ¿Dónde está la evidencia? Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.

- Establecer qué es relevante. En caso de duda es mejor recopilar mucha información que poca.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información de acuerdo al orden establecido.
- Comprobar el grado de sincronización del reloj del sistema.
- Según se vayan realizando los pasos de recolección preguntarse qué más puede ser una evidencia.
- Documentar cada paso.
- No olvidar a la gente involucrada. Tomar notas sobre qué gente estaba allí, qué estaban haciendo, qué observaron y cómo reaccionaron.

4.3. PROCEDIMIENTO DE ALMACENAMIENTO

4.3.1. Cadena de custodia

La cadena de custodia debe estar claramente documentada y se deben detallar los siguientes puntos:

- ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.
- ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.
- ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?
- En el caso de que la evidencia cambie de custodia indicar cuándo y cómo se realizó el intercambio, incluyendo número de albarán, etc.

4.3.2. Dónde y cómo almacenarlo

Se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados.

4.4. HERRAMIENTAS NECESARIAS

Existen una serie de pautas que deben de ser seguidas a la hora de seleccionar las herramientas con las que se va a llevar a cabo el proceso de recolección:

- Se deben utilizar herramientas ajenas al sistema ya que éstas pueden haberse visto comprometidas.
- Se debe procurar utilizar herramientas que alteren lo menos posible el escenario, evitando, en la medida de lo posible, el uso de herramientas de interfaz gráfico y aquellas cuyo uso de memoria sea grande.
- Los programas que se vayan a utilizar para recolectar las evidencias deben estar ubicados en un dispositivo de sólo lectura (CDROM, USB, etc.).
- Se debe preparar un conjunto de utilidades adecuadas a los sistemas operativos con los que se trabaje.
- El kit de análisis debe incluir, entre otros, los siguientes tipos de herramientas:
  - Programas para listar y examinar procesos.
  - Programas para examinar el estado del sistema.
  - Programas para realizar copias bit a bit.

4.5. CONCLUSIONES

A la hora de realizar el proceso de recolección de información en un sistema que haya sufrido un incidente de seguridad hay que tener muy claro las acciones que se deben realizar, siendo muy meticuloso y detallando en todo momento dicho proceso de manera muy minuciosa. Así mismo, se debe realizar el proceso procurando ser lo menos intrusivo posible con el fin de preservar el sistema en su estado original.

5 TOMA DE EVIDENCIAS

Uno de los retos principales a la hora de realizar un análisis forense es tener bien claro el tipo de incidente al que nos enfrentamos y a partir de él ver qué información es necesaria recopilar y la manera de proceder. Si bien hay aspectos comunes, no es lo mismo realizar un análisis forense en un caso de malware que en un caso de fraude ya que los puntos donde debe focalizarse el investigador para localizar evidencias son distintos.

Obviamente, puede que no sean necesarios algunos de los pasos que a continuación se indican como que no vaya a requerirse que las pruebas sean presentadas ante un tribunal por lo que la documentación no deba ser muy exhaustiva, no obstante es recomendable realizar el proceso desde un punto de vista profesional e íntegro y que sea lo más completo posible. Queda a juicio del lector determinar qué aspectos debe tener en cuenta, en función de la propia situación que deba analizar, y que pautas debe seguir.

El proceso de toma de evidencias se puede realizar mediante diferentes enfoques: utilizando metodologías basadas en software o metodologías basadas en hardware. Existen un gran número de dispositivos hardware diseñados expresamente para realizar este tipo de tareas y que tienen un muy alto grado de eficiencia, si bien la guía pretende ser de ayuda a la mayor cantidad de público posible por lo que se va a utilizar el enfoque basado en software, y como se ha indicado anteriormente software libre y gratuito con el fin de que dicha tarea no suponga un sobrecoste en lo que a licencias se refiere.

5.1. CONSIDERACIONES PREVIAS

Existen una serie de consideraciones previas que se deben tener en cuenta antes de comenzar el proceso de toma de evidencias:

- En primera instancia, no tocar el ordenador, dejarlo exactamente como está: ni abrir ficheros, ni ejecutar programas, ni borrar carpetas, etc. En el caso de que esté encendido, no apagarlo y en el caso de que esté apagado, no encenderlo. Hay que tener presente que existe gran cantidad de información volátil, es decir que desaparece al apagar el ordenador por lo que hacerlo podría suponer la pérdida de información muy significativa. Del mismo modo, si está apagado el hecho de encenderlo podría suponer la modificación de fechas o la ocultación de ficheros en el caso de que haya un *rootkit*.
- Establecer de manera global los pasos que se van a seguir con el fin de tener una guía operativa del proceso y que no se nos olvide ningún aspecto.
- A partir del punto anterior, se debe concretar de manera detallada los pasos que se van a seguir. En este punto se tienen en cuenta diferentes aspectos como el tiempo estimado de duración del análisis, la urgencia del mismo o los recursos necesarios para llevarlo a cabo.
- Prever y minimizar los riesgos con el fin de que si se presenta algún problema no afecte significativamente de manera negativa al proceso.
- Valorar si la persona responsable de realizar el proceso tiene las habilidades y conocimientos necesarios para ello. En el caso de que se tengan dudas sobre la capacidad para llevarlo a cabo es mejor consultar a alguien con experiencia y conocimientos

contrastados con el fin de que asesore el proceso y que no se destruyan pruebas accidentalmente.

- Obtener una autorización por escrito de quien corresponda para poder llevar a cabo el análisis y la recolección de evidencias. Este es un aspecto fundamental ya que puede darse el caso de que se trabaje con información confidencial o de vital importancia para una empresa, o que la disponibilidad de los servicios se vea afectada por el trabajo de investigador forense. En cierto tipo de incidentes será necesario solicitar una autorización judicial con el fin de que asegurar la validez de las pruebas recogidas en un futuro juicio.
- Solicitar las contraseñas necesarias para acceder a ficheros o volúmenes cifrados.
- Tener preparado un kit lo más completo posible de utilidades siguiendo las pautas que se indican en el punto 4.4.
- Preparar una lista de personas a las que se deba informar y mantener al tanto del proceso, incluyendo el nombre, email y cualquier otro tipo de información que pueda resultar relevante.

  A modo de ejemplo se adjunta el modelo indicado en el «ANEXO 1 – Personas de contacto».

Una vez valoradas todas las consideraciones previas que ayuden a tener claro el tipo de incidente al que nos enfrentamos y los pasos que se deben seguir para solucionarlo. Por lo que comienza el proceso de recolección de evidencias.

5.2. INICIO DEL PROCESO

Se comienza etiquetando, inventariando y fotografiando todos los dispositivos que se van a analizar: discos duros, *pendrives*, cámaras, etc. Incluso, dependiendo del tipo de incidente, puede ser necesario incluir *routers*, escáneres, impresoras, etc. Se debe anotar la marca, modelo, número de serie, tipo de conexión (USB, *firewire*, etc.) de todos ellos. Así mismo, se deben tomar los datos de la persona responsable del equipo y del usuario o los usuarios que trabajen en él, y cualquier otra información que se considere que puede resultar relevante. La cadena de custodia es fundamental, ya que demuestra que las pruebas obtenidas no han sido manipuladas, por lo que se debe ser especialmente meticuloso en este aspecto. Para ello es imprescindible documentar todas y cada una de las evidencias obtenidas.

A modo de ejemplo se indica una plantilla disponible en el **«**ANEXO 2 – Cadena de custodia de evidencias**».**

En el apartado de observaciones es importante justificar el motivo por el que se han recopilado dichas evidencias. El fin de esta tarea es facilitar el trabajo del analista en el caso de que no sea el propio investigador el que vaya a realizar dicho papel.

Una vez etiquetados, inventariados y fotografiados todos los dispositivos se procede a la recopilación de las evidencias. De forma genérica se puede clasificar el tipo de información a recopilar en dos grandes grupos: información volátil e información no volátil. Así mismo, se puede hablar de «*live acquisition*», que corresponde a la obtención de información en un sistema en funcionamiento, o «*static acquisition*», que corresponde a la obtención de información de un sistema que está apagado.

¡Importante!

Para realizar una correcta obtención de evidencias es importante el uso de software no invasivo y que se encuentre en dispositivos protegidos contra escritura (pendrive, cd-rom, etc.), y en el caso de que sospeche que el sistema se ha visto comprometido con malware, que obtenga la información mediante sus propios métodos implementados y no a través de la API del sistema ya que la integridad de ésta puede haberse visto comprometida y no reflejar los resultados reales.

A continuación, se indican una serie de kits especializados en este tipo de tareas, aunque lo más recomendable es crearse uno de acuerdo a las necesidades de cada uno.

Tabla 1: Listado de kits open source de utilidades de análisis forense.

Nombre	URL
Caine	http://www.caine-live.net
Digital Forensics Framework	http://www.digital-forensic.org
The Sleuth Kit y AutoSpy	http://www.sleuthkit.org
Helix Live CD	http://www.e-fense.com
Forensic and Incident Response Environment (F.I.R.E)	http://fire.dmzs.com
Digital Evidence & Forensic Toolkit	http://www.deftlinux.net

Nota

Habitualmente se suele realizar únicamente el volcado de memoria y el volcado de disco, y a partir de ahí se trabaja sobre diferentes copias para obtener el resto de evidencias. A continuación se indica la obtención concreta de diferentes evidencias ya que dependiendo del caso, puede no ser necesario realizar un volcado completo de la información, sino que será suficiente con realizar un análisis específico.

5.3. INFORMACIÓN VOLÁTIL

Como se ha indicado anteriormente la información volátil puede resultar muy importante a la hora de realizar un análisis forense ya que puede contener evidencias de conexiones, de procesos en ejecución, etc. La pérdida de este tipo de información puede suponer que el análisis forense no se complete satisfactoriamente o dificultar en gran medida el proceso. Es

por ello que, como indica el *RFC 3227*, se deben tomar en primer lugar las evidencias volátiles y después las que no lo son. A continuación se indica la metodología que se debe seguir y se indican algunos ejemplos de incidentes donde puede resultar útil hacerlo, de modo que la persona que lleve a cabo el proceso realizará los pasos que considere oportunos tomando como base la información facilitada.

5.3.1. Hora y fecha del sistema

En cuanto a la información volátil lo primero que se debe obtener es la fecha y hora del sistema para poder establecer una línea temporal de recopilación de evidencias, duración del proceso, etc.

Para ello, se puede escribir la siguiente instrucción desde una Shell segura del intérprete de comandos, pudiendo realizarlo mediante alguna utilidad como **PowerShell** o **WMIC**:

```
date /t > FechaYHoraDeInicio.txt &time /t >> FechaYHoraDeInicio.txt
```

Se debe comparar la fecha obtenida con el tiempo universal coordinado (UTC), estándar de tiempo por el cual se regula la hora nivel mundial, para determinar si la fecha establecida en el sistema es correcta o no, y que desviación existe.

También hay que tener presente que los sistemas FAT almacenan los valores de tiempo en base al tiempo local del ordenador, mientras que los sistemas NTFS los almacenan en formato UTC. Esto significa que mientras que los NTFS no se ven afectados por los cambios en la zona horaria o el horario de verano, los FAT tendrán distinto valor si se visualizan en una región u otra con diferente franja horaria, o en verano con respecto a invierno.

Así mismo, una vez finalizado el proceso se deberá ejecutar la misma instrucción cambiando el fichero de destino a `FechaYHoraFin.txt`.

5.3.2. Volcado de memoria

El volcado de memoria es uno de los aspectos más importantes y críticos de la fase de adquisición. Como se ha indicado anteriormente, en la memoria se almacenan evidencias significativas como las conexiones establecidas, los procesos en ejecución, contraseñas de volúmenes cifrados, etc. Realizar un correcto volcado de memoria puede suponer la diferencia entre la resolución del incidente o no. Debido a ello se debe ser muy cuidadoso durante el proceso.

A la hora de obtener la memoria se deben tener en cuenta 2 tipos de memoria: la memoria física y la memoria virtual. La memoria física corresponde a la memoria real del sistema mientras que la memoria virtual corresponde normalmente al fichero de paginación pagefile.sys. Como se ha indicado anteriormente la memoria virtual permite optimizar el uso de la memoria RAM ya que el sistema operativo envía ahí temporalmente la información que no sea necesaria en ese momento para los procesos en ejecución y posteriormente la recupera en el caso de alguno se la solicite.

Existen un gran número de utilidades que permiten realizar un volcado de memoria, pero entre todas destaca **DumpIt**[22] por su sencillez y compatibilidad con las distintas versiones de Windows. Con ejecutar la aplicación desde el intérprete de comandos es suficiente. Realiza un volcado de memoria en formato RAW en el mismo directorio desde donde se ejecute el programa.

Un ejemplo de uso del programa es la Ilustración 3:

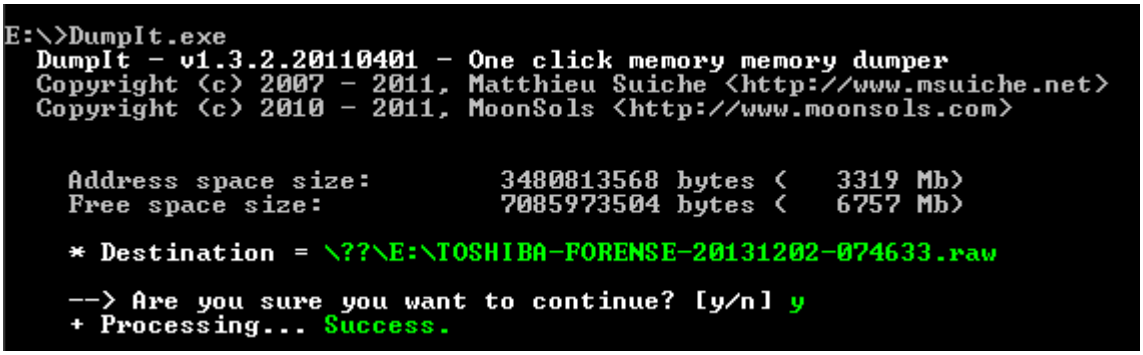

Ilustración 3: DumpIt

Otras utilidades

Volatility	https://code.google.com/p/volatility
AccessData FTK Imager	http://www.accessdata.com
Memoryze	http://www.mandiant.com/resources/download/memoryze
MDD	http://sourceforge.net/projects/mdd/
Belkasoft Live RAM Capturer	http://forensic.belkasoft.com/en/ram-capturer

Otra manera de obtener la memoria física es mediante un "***crash dump***", el cual corresponde a un fallo del que el sistema no puede recuperarse. Cuando se produce este tipo de fallos se genera un fichero, que puede ser un ***minidump*** (volcado parcial de la memoria física) o, en el caso de configurarlo[23], un volcado completo de la memoria física (`%SystemRoot%\Memory.dmp`), y que posteriormente pueden ser analizados mediante la herramienta correspondiente. Este tipo de fallos pueden ser provocados mediante herramientas como **NotMyFault**[24] o quitando directamente el cable de corriente del

[22] http://www.moonsols.com
[23] http://blogs.technet.com/b/plataformas/archive/2008/08/22/como-configurar-mi-m-quina-para-obtener-un-dump-de-memoria.aspx
[24] http://download.sysinternals.com/files/NotMyFault.zip

ordenador, si es uno de sobremesa, y la batería y el cable de corriente en un portátil. En el caso de obtener la memoria mediante este método es recomendable verificar la integridad del fichero mediante alguna utilidad como **Dumpchk**[25].

Para ello, se debe escribir la siguiente instrucción:

```
dumpchk.exe Memory.dmp
```

En el caso de que la integridad del fichero esté afectada mostrará un mensaje de error y en el caso de que la integridad del fichero sea correcta mostrará el mensaje: "*Finished dump check*".

Puede darse el caso de que por diferentes motivos, como que no se tenga acceso físico al equipo al que se va a realizar la toma de evidencias, sea necesario realizar el proceso de manera remota. Para ello es posible utilizar de alguna herramienta como **psexec**[26] gracias a la cual se puede realizar dicho proceso de una manera eficaz y sin necesidad de instalar ningún componente en el equipo remoto.

Una vez obtenida la imagen correspondiente al volcado de memoria física es necesario obtener un hash de la misma que será anotado en la documentación de la cadena de custodia para asegurar que dicha imagen no sea modificada a posteriori y garantizar la integridad de la misma. Un hash es un valor que identifica datos de forma "unívoca". Existen distintos tipos de hashes: MD5, SHA-1, SHA-2, etc.

¡Importante!

El uso del hash MD5, pese al alto grado de utilización, presenta el problema de que pueden surgir colisiones, es decir, puede darse el caso de que ficheros diferentes tengan el mismo MD5, por lo que puede quedar en entredicho la validez de las pruebas. Es por ello que es recomendable que vaya cayendo en desuso.

Un caso similar, aunque no igual, es el del SHA-1 por lo que se aconseja que se busquen otras alternativas como SHA-256, SHA-512, etc.

Hay un gran número de herramientas como por ejemplo **HashMyFiles**[27], **MD5deep**[28] o **HashCalc**[29] a través de las cuales se pueden obtener los distintos hashes de un fichero. Un ejemplo de uso del programa **HashMyFiles** es la Ilustración 4

[25] http://technet.microsoft.com/es-es/library/ee424340%28v=ws.10%29.aspx
[26] http://technet.microsoft.com/es-es/sysinternals/bb897553.aspx
[27] http://www.nirsoft.net/utils/hash_my_files.html
[28] http://md5deep.sourceforge.net
[29] http://www.slavasoft.com/hashcalc/

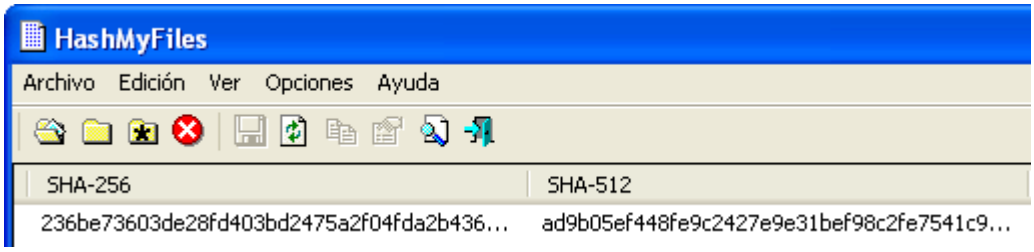

Ilustración 4: HashMyFiles

También puede resultar de gran interés para el análisis forense la obtención de la memoria virtual, por lo que es recomendable adquirir el fichero ***pagefile.sys*** siempre que sea posible. Para ello se puede utilizar alguna herramienta especializada como **NTFSCopy**[30] o bien, sería necesario apagar el ordenador, extraer el disco duro y conectarlo en otro ordenador para que dicho fichero no esté en uso y poder así copiarlo, corriendo el riesgo de que si el sistema tiene configurada la opción de borrar el archivo de paginación de la memoria virtual al apagar el equipo, perdamos la información.

En el caso de realizar la adquisición del fichero de paginación con la herramienta indicada, tan sólo es necesario ejecutar el programa desde una consola del intérprete de comandos.

Un ejemplo de utilización es la siguiente instrucción:

```
NTFSCopy.exe c:\pagefile.sys g:\pagefile.sys -raw -MD5
```

Se indica a la herramienta que realice una copia de fichero de paginación pagefile.sys ubicado en C: y que la almacene en la unidad G:,añadiéndole el MD5 al nombre.

Otras utilidades

AccessData FTK Imager	http://www.accessdata.com
Hobocopy	https://github.com/candera/hobocopy
ShadowCopy	http://www.runtime.org/shadow-copy.htm

¡Importante!

No es necesario obtener el fichero pagefile.sys si se va a realizar un volcado de disco a posteriori ya que de este modo ya se está obteniendo el propio fichero de

[30] https://tzworks.net/prototype_page.php?proto_id=9

paginación, por lo que la persona que vaya a realizar el análisis de las evidencias no tendrá ningún problema en extraerlo de la propia imagen de disco.

Este mismo caso se aplica al fichero de hibernación (***hiberfil.sys***), el cual almacena una imagen exacta del ordenador justo antes de que hiberne con el fin de poder restaurar dicha imagen cuando se abandone el estado de hibernación. En el caso de que la hibernación no esté configurada por defecto, es posible hacerlo mediante la utilidad **Powercfg**[31] y posteriormente forzar el estado con la utilidad **PsShutdown**[32] o desde *Inicio – Apagar - Hibernar*.

En ocasiones puede que no sea necesario, por el tipo de incidente, volcar toda la memoria, sino que con obtener cierto tipo de información será suficiente. A continuación se indican algunas evidencias significativas que puede ser necesario recopilar en incidentes concretos.

5.3.2.1. Procesos en ejecución.

Para obtener el listado de procesos en ejecución se puede utilizar la utilidad **tasklist**.

Para ello, se debe escribir la siguiente instrucción:

```
tasklist > "ProcesosEnEjecución-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 5:

```
Nombre de imagen              PID Nombre de sesión Núm. de  Uso de memor
========================= ====== ================ ======== ============
System Idle Process             0 Console                0         28 KB
System                          4 Console                0        240 KB
smss.exe                      612 Console                0        436 KB
csrss.exe                     660 Console                0      9.608 KB
winlogon.exe                  684 Console                0      8.292 KB
services.exe                  728 Console                0      5.100 KB
lsass.exe                     740 Console                0      2.812 KB
svchost.exe                   928 Console                0      5.228 KB
svchost.exe                   996 Console                0      4.892 KB
psksvc.exe                   1092 Console                0        124 KB
pavsrvx86.exe                1132 Console                0        996 KB
AVENGINE.EXE                 1176 Console                0      3.984 KB
svchost.exe                  1312 Console                0     30.100 KB
svchost.exe                  1416 Console                0      5.168 KB
svchost.exe                  1484 Console                0      4.544 KB
spoolsv.exe                  1612 Console                0      5.420 KB
svchost.exe                  1716 Console                0      3.896 KB
atchksrv.exe                 1812 Console                0      1.936 KB
dirmngr.exe                  1848 Console                0      4.080 KB
jqs.exe                      1924 Console                0      1.388 KB
```

Ilustración 5: Procesos en ejecución

Otras utilidades

[31] http://technet.microsoft.com/es-es/library/cc748940(v=ws.10).aspx
[32] http://technet.microsoft.com/en-us/sysinternals/bb897541.aspx

Pslist	http://technet.microsoft.com/es-es/sysinternals/bb896682.aspx
Volatility	https://code.google.com/p/volatility
CurrProcess	http://www.nirsoft.net/utils/cprocess.html

Nota

En casos concretos, principalmente los relacionados con malware, puede resultar útil volcar el contenido en memoria de un proceso en ejecución, sospecho de ser utilizado por el malware. Para ello, se pueden utilizar diferentes herramientas como **PMDump**[33] o **Process Dumper**[34], o a partir de Windows 7 desde el administrador de tareas crear archivo de volcado.

5.3.2.2. Servicios en ejecución.

Para obtener el listado de servicios en ejecución se puede utilizar la utilidad **sc query**.

Para ello, se debe escribir la siguiente instrucción:

```
sc query > "ServiciosEnEjecución-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 6:

```
SERVICE_NAME: wscsvc
DISPLAY_NAME: Centro de seguridad
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: wuauserv
DISPLAY_NAME: Actualizaciones automßticas
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: WZCSVC
DISPLAY_NAME: Configuraci¾n inalßmbrica rßpida
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
```

Ilustración 6: Servicios en ejecución

[33] http://ntsecurity.nu/toolbox/pmdump/
[34] http://www.trapkit.de/research/forensic/pd/

Otras utilidades

PsService	http://technet.microsoft.com/es-es/sysinternals/bb897542.aspx
Volatility	https://code.google.com/p/volatility

5.3.2.3. Usuarios que han iniciado sesión y listado de cuentas de usuario.

Para obtener el listado usuarios actualmente han iniciado sesión en el equipo se pueden utilizar diferentes herramientas como **netusers**[35].

Para ello se debe escribir la siguiente instrucción:

```
netUsers.exe > "UsuariosActualmenteLogueados-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Con la misma herramienta, se pueden saber los usuarios que alguna vez se han iniciado sesión en la máquina y cuándo fue la última vez que lo hicieron. Para ello se debe escribir la siguiente instrucción:

```
netUsers.exe /History > "HistoricoUsuariosLogueados-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Otras utilidades

Psloggedon	http://technet.microsoft.com/es-es/sysinternals/bb897545.aspx
LogonSessions	http://technet.microsoft.com/es-es/sysinternals/bb896769.aspx

5.3.3. Información de red: estado, conexiones activas, puertos UDP y TCP abiertos

5.3.3.1. Estado de la red

Para obtener el estado de la red, los adaptadores de red, su configuración, etc. se puede utilizar el comando **ipconfig**.

Para ello, se debe escribir la siguiente instrucción:

```
ipconfig /all > "EstadoDeLaRed-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

[35] http://www.systemtools.com/cgi-bin/download.pl?NetUsers

Y el resultado obtenido es la Ilustración 7:

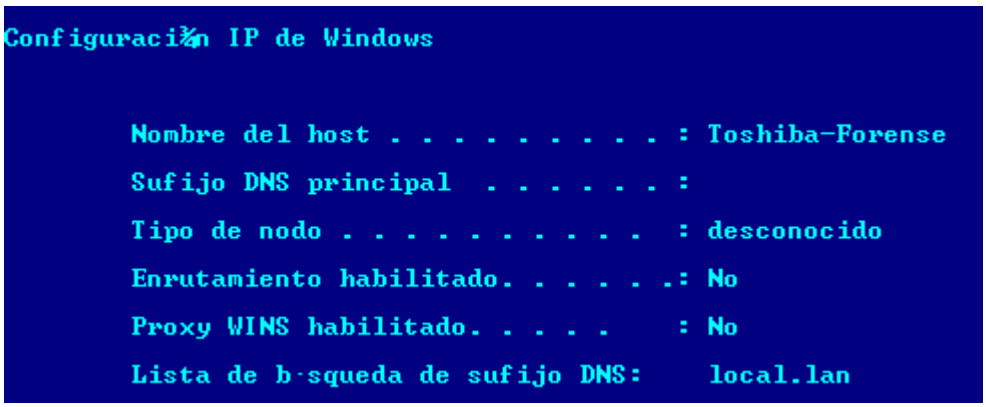

Ilustración 7: Configuración IP de Windows

Nota

Puede ocurrir que, por diversos motivos, como una infección por malware, el equipo esté funcionando como un *sniffer* en modo promiscuo, es decir, que esté capturando todo el tráfico de la red. Para detectar este tipo de práctica se puede utilizar alguna herramienta como **Promiscdetect**[36].

Para ello, se debe ejecutar la siguiente instrucción:

```
Promiscdetect > "Promiscdetect-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

5.3.3.2. Conexiones NetBIOS establecidas

NetBIOS es un protocolo utilizado por Windows, y que normalmente funciona sobre TCP/IP, el cual permite comunicar equipos dentro de la misma red local. Para ello, NetBIOS asigna un nombre identificativo a cada equipo. De este modo, se puede acceder a través de la red mediante el nombre o la IP a los recursos compartidos de un equipo.

NetBIOS almacena en una tabla el registro de todos los accesos. Para visualizarlos se puede utilizar el comando **nbtstat** o el **net**:

```
nbtstat -S > "ConexionesNetBIOSEstablecidas-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

O bien,

```
net sessions > "SesionesRemotasEstablecidas-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 8:

[36] http://ntsecurity.nu/toolbox/promiscdetect/

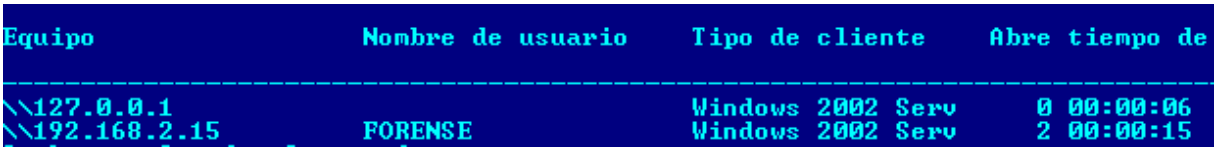

Ilustración 8: Conexiones NetBIOS establecidas

5.3.3.3. Ficheros transferidos recientemente mediante NetBIOS

NetBIOS también almacena temporalmente en una tabla el registro de todos los ficheros copiados mediante este protocolo. Para visualizarlos se puede escribir la siguiente instrucción:

```
net file > "FicherosCopiadosMedianteNetBIOS-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 9:

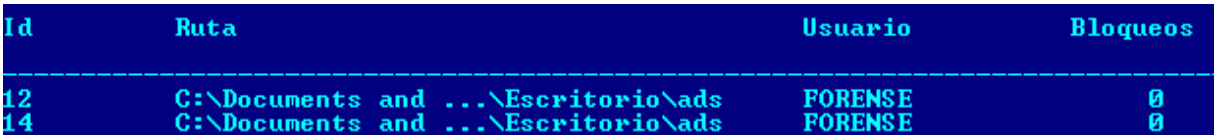

Ilustración 9: Ficheros transferidos recientemente mediante NetBIOS

5.3.3.4. Conexiones activas o puertos abiertos

Para obtener el listado de conexiones activas se puede utilizar el comando **netstat**.

Para ello, se debe escribir la siguiente instrucción:

```
netstat -an |findstr /i "estado listening established" >
"PuertosAbiertos-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 10:

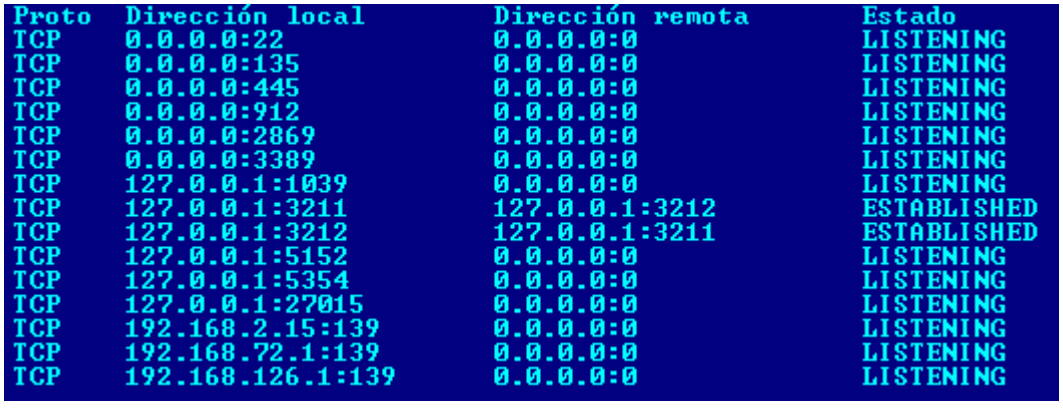

Ilustración 10: Conexiones activas o puertos abiertos

Así mismo, se puede obtener la relación entre aplicaciones y puertos abiertos. Para ello, se debe escribir la siguiente instrucción:

```
netstat -anob > "AplicacionesConPuertosAbiertos-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Otras utilidades

Fport	http://www.mcafee.com/es/downloads/free-tools/fport.aspx

5.3.3.5. Contenido de la caché DNS

El protocolo DNS (*Domain Name System* o Sistema de Nombres de Dominio) permite asociar direcciones IP con nombres de dominio ya que éstos últimos son más sencillos de recordar. En la caché DNS se puede visualizar dicha asociación con respecto a los dominios a los que se ha accedido desde el equipo. Pata obtener el listado se puede utilizar el comando **ipconfig**.

Para ello, se puede escribir la siguiente instrucción:

```
ipconfig /displaydns > "DNSCache-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 11:

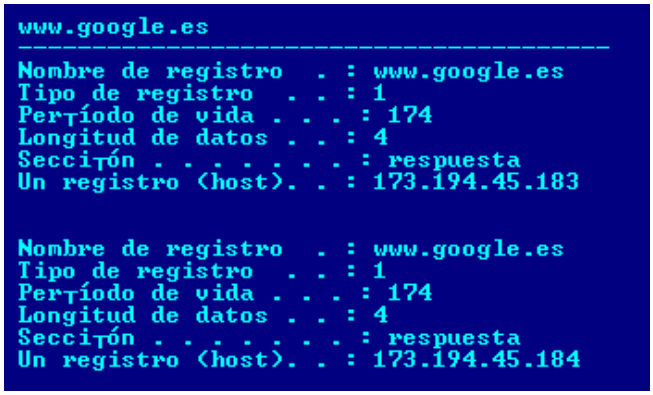

Ilustración 11: Contenido de la caché DNS

5.3.3.6. ARP caché

La tabla ARP almacena la relación entre dirección física (MAC) y dirección lógica (IP) de los equipos con los que se haya comunicado recientemente el ordenador. Hay que tener presente que la información almacenada es temporal y que, en el caso de que no se mantenga la comunicación, la entrada correspondiente será eliminada en un breve espacio de tiempo.

Para obtener la caché de la tabla ARP se debe utilizar el comando **arp**.

Para ello, se puede escribir la siguiente instrucción:

```
arp -a > "ArpCache-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 12:

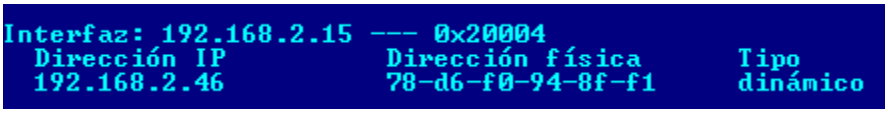

Ilustración 12: ARP Cache

5.3.3.7. Tráfico de red

Además de la información anteriormente indicada correspondiente al estado de la red, conexiones activas, etc. conviene capturar el tráfico durante un cierto espacio de tiempo para que pueda ser analizado posteriormente. En dicho análisis se puede descubrir tráfico generado por malware, conexiones con servidores C&C, recepción de paquetes malformados, etc.

Para ello, se recomienda utilizar alguna herramienta como **tshark**[37] o **dumpcap**[38], las cuales permiten capturar el tráfico en modo promiscuo (en el caso de que la tarjeta de red lo permita), es decir, soportan la monitorización de todo el tráfico que circula por la red independientemente de que el origen o destino sea el host que se está analizando.

Un ejemplo de utilización de la herramienta sería el siguiente.

```
tshark -w "CapturaRed-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.pcap"
```

O bien,

```
dumpcap -w "CapturaRed-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.pcap"
```

Otras utilidades

Tcpdump	http://www.tcpdump.org
Wireshark	http://www.wireshark.org
Netsleuth	http://www.netgrab.co.uk
Windump	http://www.winpcap.org/windump
NetWitness	http://www.emc.com/security/rsa-netwitness.htm

Nota

En el caso de que se sospeche que existe riesgo de una posible exfiltración de información sensible como es el caso de malware

[37] http://www.wireshark.org/docs/man-pages/tshark.html
[38] http://www.wireshark.org/docs/man-pages/dumpcap.html

perteneciente a alguna botnet, es recomendable redirigir el tráfico del equipo a una vlan aislada sin salida a Internet.

Ejemplo

Un caso práctico corresponde a un equipo en el que el acceso a internet funcionaba con extrema lentitud y se realizó una captura del tráfico de red. En un posterior análisis se observó la Ilustración 13:

Destination	Protocol	Length	Info
173.194.67.26	SMTP	88	C: RCPT TO:
173.194.67.26	SMTP	84	C: RCPT TO:
167.206.4.79	SMTP	87	C: RCPT TO:
65.55.92.168	SMTP	86	C: RCPT TO:
66.196.118.33	SMTP	83	C: RCPT TO:
98.136.216.25	SMTP	84	C: RCPT TO:
98.139.214.154	SMTP	90	C: RCPT TO:
98.136.216.25	SMTP	89	C: RCPT TO:
64.236.64.226	SMTP	92	C: RCPT TO:
65.54.188.126	SMTP	86	C: RCPT TO:
98.136.216.25	SMTP	87	C: RCPT TO:
209.86.93.229	SMTP	88	C: RCPT TO:
209.181.247.105	SMTP	89	C: RCPT TO:
68.142.202.129	SMTP	86	C: RCPT TO:
65.55.92.184	SMTP	88	C: RCPT TO:
98.136.217.192	SMTP	88	C: RCPT TO:

Ilustración 13: Envío masivo de Spam

El equipo enviaba masivamente emails de spam como la Ilustración 14:

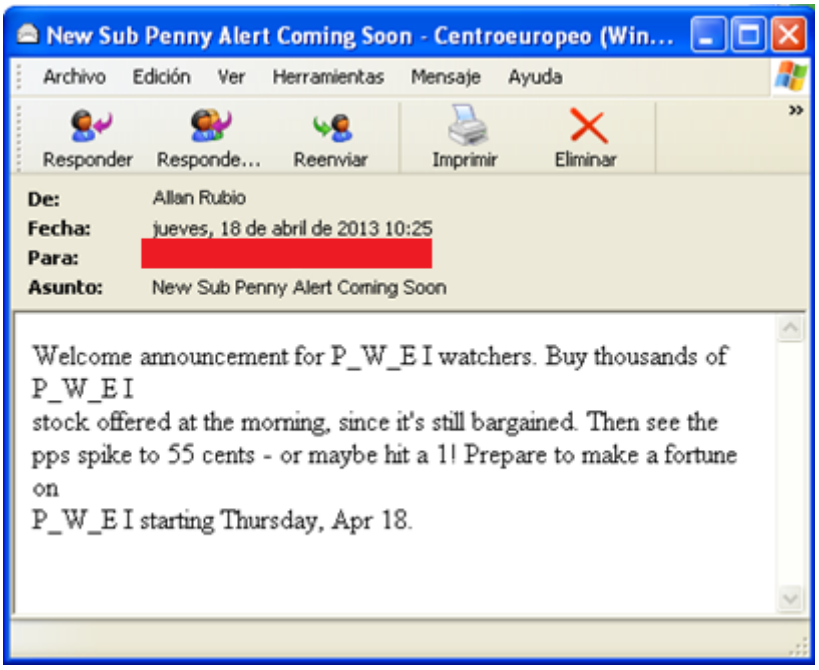

Ilustración 14: Email de Spam

En algunos de los correos se observó que se adjuntaba un fichero con nombre **newbos3.exe** que correspondía a un malware catalogado como **Adware/SystemTool**.

5.3.4. Registro de Windows

El registro almacena información de gran interés para un investigador forense (programas que se cargan al iniciar el equipo, perfiles de usuario, configuraciones de acceso a redes inalámbricas, histórico de dispositivos USB conectados al equipo, etc.) por lo que es necesario realizar una copia del mismo para su posterior análisis.

En la siguiente tabla se pueden visualizar las claves de registro junto con la información que contienen.

Tabla 2: Entradas del registro e información que contienen [9].

Clave de registro	Abreviatura	Información que contiene
HKEY_CLASSES_ROOT	HKCR	Garantiza que cuando abra un archivo con el Explorador de Windows se abrirá el programa correcto.
HKEY_CURRENT_USER	HKCU	Configuración del usuario que ha iniciado sesión.
HKEY_LOCAL_MACHINE	HKML	Información de configuración específica del equipo (para cualquier usuario).
HKEY_USERS	HKU	Perfiles de usuario cargados activamente en el equipo.
HKEY_CURRENT_CONFIG	HKCC	Información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema.

Para exportarlas se deben ejecutar las siguientes instrucciones (Estructura: `reg export Clave\Subclave` fichero):

```
reg export HKEY_CLASSES_ROOT "HKCR-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export HKEY_CURRENT_USER "HKCU-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export HKEY_LOCAL_MACHINE "HKLM-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export HKEY_USERS "HKU-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export HKEY_CURRENT_CONFIG "HKCC-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

Así mismo, existen una serie de ficheros que pueden ser recopilados y que sirven de respaldo para las claves de registro. En la siguiente tabla se pueden visualizar las correspondencias entre ficheros y entradas de registro:

Tabla 3: Entradas del registro y ficheros asociados [9].

Entrada de registro	Ficheros asociados
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\SECURITY	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\SOFTWARE	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\SYSTEM	System, System.log, System.alt, System.sav
HKEY_CURRENT_CONFIG	System, System.log, System.alt, System.sav
HKEY_CURRENT_USER	Ntuser.dat y Ntuser.dat.log
HKEY_USERS\.DEFAULT	Default, Default.log, Default.sav

Los ficheros se almacenan en `%SystemRoot%\System32\Config\` (Windows NT/2000/XP) o `%SystemRoot%\System32\Config\Regback\` (Windows 7/8), a excepción de *Ntuser.dat* y *Ntuser.dat*.log que se encuentran en *%HomePath%*.

Otras utilidades

RegRipper	https://code.google.com/p/regripper
RegFileExport	http://www.nirsoft.net/utils/registry_file_offline_export.html
Forensic Registry EDitor (fred)	https://www.pinguin.lu/index.php
Registry Decoder	https://code.google.com/p/registrydecoder

Puede darse el caso de que no sea necesario, por el tipo de incidente, exportar todo el registro, sino que con ciertas claves sea suficiente. A continuación se indican algunas evidencias significativas del registro que puede ser necesario recopilar en incidentes concretos.

5.3.4.1. Dispositivos USB conectados.

Con cada conexión de un nuevo dispositivo USB al equipo se crea su correspondiente entrada de registro en la que se almacena información del mismo, como el fabricante o un número único identificativo. Es por ello que puede resultar relevante exportar las entradas de registro que se indican a continuación, en el caso de que el incidente lo requiera. Para ello se deben ejecutar las siguientes instrucciones:

```
reg export "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR"
"USBSTOR-%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USB" "USB-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\DeviceClasses"
"DeviceClasses-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_LOCAL_MACHINE\System\MountedDevices" "MountedDevices-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"
```

Así mismo, *setupapi.log* (Windows XP) o *setupapi.dev.log* (a partir de Windows Vista) ubicado en la carpeta `%WinDir%` y `%WinDir%\inf` contiene información relativa a los dispositivos instalados y almacena registros tales como el nombre del dispositivo, el número de serie, la fecha correspondiente a la primera vez que se conectó al equipo, etc.

Ejemplo

Un caso práctico corresponde a una empresa en la que estaba establecida una directiva para prohibir el uso de *pendrives* propios por parte de los trabajadores por temas de seguridad. Un equipo de la empresa, sin acceso a la red local ni a Internet, se infectó con un malware y mediante el análisis de dicha entrada se observó la Ilustración 15:

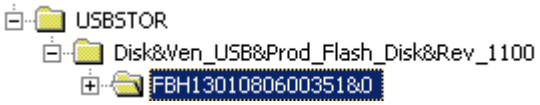

Ilustración 15: Dispositivos USB conectados

Como se ha indicado previamente en el registro se puede obtener, entre otra información:

- El número que identifica la clase del dispositivo (*Device Class ID*, en formato *Disk&Vendedor&Producto&Version*, en este caso *Disk&Ven_USB&Prod_Flash_Disk&Rev_1100*.
- El número de identificador único (*Unique Instance ID*), en este caso *FBH1301080600351&0*. En el caso de que el segundo carácter del identificador sea un & indica que el dispositivo no tiene un número de serie identificativo propio y que el sistema operativo le ha asignado uno.

De este modo se demostró que se había infringido la normativa y que se había conectado un dispositivo USB al equipo.

Otras utilidades

USB History Dump	http://sourceforge.net/projects/USBhistory/

5.3.4.2. Listado de redes WIFI a las que se ha conectado un equipo:

En el caso de un portátil puede resultar interesante conocer a qué redes WIFI se ha conectado y la configuración de las mismas. En Windows XP se deben ejecutar las siguientes instrucciones para exportar las entradas de registro correspondientes:

```
reg export
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces"
"ListadoRedesWifi-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters\I
nterfaces" "ConfiguraciónRedesWifi-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

En el caso de Windows 7/8 ya no se almacena esa información en el registro sino que se crean en disco ficheros con extensión XML en la carpeta *C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces* correspondientes a las configuraciones de las redes WIFI a las que se ha conectado el equipo, por lo que habría que copiar el contenido de la misma o exportarlos mediante las siguientes instrucciones:

```
netsh wlan show profiles > "PerfilesWifi-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"

netsh wlan show all > "ConfiguraciónPerfilesWifi-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Otra opción sería exportar los propios perfiles mediante la siguiente instrucción:

```
netsh wlan export profile
```

Ejemplo

Un caso práctico corresponde a un usuario que se sospechaba que había realizado una intrusión desde su portátil con Windows XP a una red inalámbrica por lo que se realizó una exportación de la entrada de registro anteriormente indicada.

El posterior análisis de dicha entrada reveló que el usuario sí que se había conectado a la red con SSID (*Service Set IDentifier*) "*CIBER NOMBRE FICTICIO*", como se puede observar en la Ilustración 16.

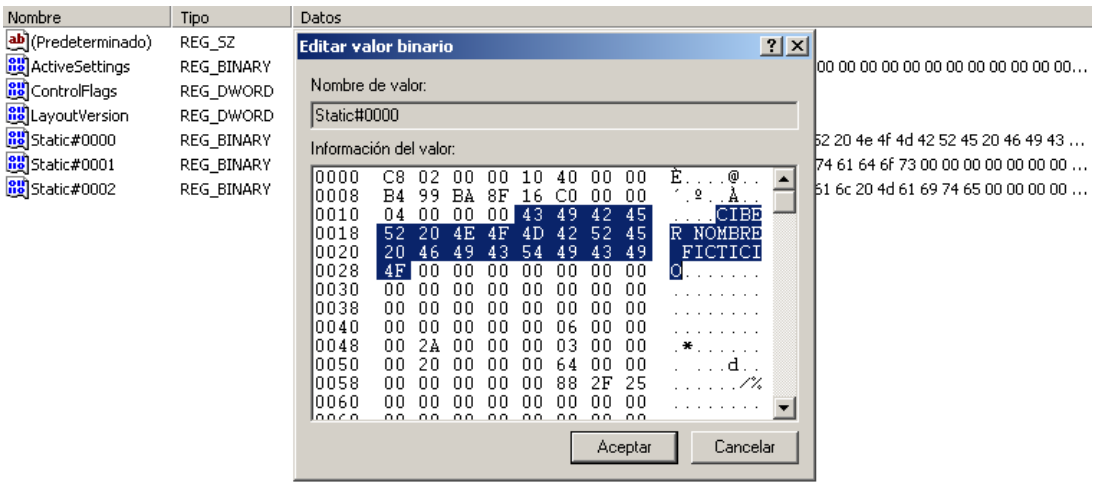

Ilustración 16: Listado de redes WIFI a las que se ha conectado el equipo

Otras utilidades

WirelessNetConsole	http://www.nirsoft.net/utils/wireless_net_console.html

5.3.4.3. Configuración de Windows Security Center / Windows Action Center

Microsoft, a partir del *Service Pack* 2 de Windows XP, incluyó el *Security Center*, que en versiones posteriores del sistema operativo ha pasado a llamarse *Action Center*. Dicho componente es un panel informativo donde se pueden visualizar y configurar los principales aspectos relacionados con la seguridad del propio sistema: *firewall*, actualizaciones automáticas, notificaciones, etc.

En el registro se almacena la configuración de este componente y puede ser importante conocer dicha configuración en algunos incidentes. Para exportar las claves de registro correspondientes se deben ejecutar las siguientes instrucciones:

En Windows XP:

```
reg export "HKEY_LOCAL_MACHINE\Software\Microsoft\Security Center"
"HKLM-SecurityCenter-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

En Windows 7/8:

```
reg export "HKEY_LOCAL_MACHINE\Software\Microsoft\Security Center"
"HKLM-SecurityCenter-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action
Center" "HKLM-ActionCenter-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

5.3.4.4. Configuración del firewall de Windows.

En la configuración del *firewall* de Windows se almacenan las aplicaciones permitidas, los puertos abiertos y demás información relacionada con el propio *firewall*.

Para exportar dicha información se debe ejecutar la siguiente instrucción:

```
reg export
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Param
eters\FirewallPolicy" "HKLM-FirewallPolicy-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"
```

Ejemplo

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
C:\WINDOWS\system32\dfsdasdcxz.exe	REG_SZ	C:\WINDOWS\system32\dfsdasdcxz.exe:*:Enabled:dfsdasdcxz.exe

Ilustración 17: Excepción de malware en el firewall de Windows

Un caso práctico corresponde a un equipo en el que había ocurrido una fuga de información correspondiente a datos bancarios del propietario del mismo y tras analizar dicha entrada de registró se constató que en el firewall había establecida una excepción para que el programa *dfsdasdcxz.exe* pudiera conectar con el exterior, como se puede observar en la Ilustración 17. Tras una investigación posterior del propio fichero se determinó que era un malware que tenía funciones de *keylogger* y que enviaba la información recopilada a un servidor externo.

5.3.4.5. Programas que se ejecutan al iniciar el sistema operativo.

Las principales entradas de registro donde se almacenan el listado de programas que se ejecutan al iniciar el sistema operativo son las siguientes:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager

Es por ello que se recomienda exportar estas claves de registro mediante las siguientes instrucciones:

```
reg export
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Sh
ell Folders" "HKCU-ShellFolders-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Us
er Shell Folders" "HKCU-UserShellFolders-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" "HKCU-
Run-%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce"
"HKCU-RunOnce-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CURRENT_USER\Software\Microsoft\Windows
NT\CurrentVersion\Windows" "HKCU-Windows-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\S
hell Folders" "HKLM-ShellFolders-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\U
ser Shell Folders" "HKLM-UserShellFolders-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\E
xplorer" "HKLM-Explorer-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
"HKLM-Run-%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce"
"HKLM-RunOnce-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager" "HKLM-SessionManager-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

Ejemplo

Un caso práctico corresponde a un equipo infectado con un falso antivirus, Ilustración 18, que mostraba constantes notificaciones y que, entre otras cosas, impedía ejecutar el Administrador de Tareas.

Ilustración 18: Falso antivirus

Tras analizar las claves de registro exportadas se determinó que había creado el siguiente valor en el registro en `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, como se puede observar en la Ilustración 19, por lo que se ejecutaba automáticamente al iniciar sesión el usuario en el equipo.

Ilustración 19: Falso antivirus ejecutándose en la carga del sistema operativo

Otras utilidades

Autoruns	http://technet.microsoft.com/es-es/sysinternals/bb963902.aspx
WhatInStartup	http://www.nirsoft.net/utils/what_run_in_startup.html

5.3.4.6. Extensiones de ficheros y programas asociados para abrirlos.

Windows almacena en el registro las asociaciones entre tipos de fichero según la extensión y programas que se deben utilizar para abrirlos. En ciertos incidentes, principalmente relacionados con malware, éste modifica estas entradas de registro con el fin de ejecutarse automáticamente cuando se ejecute un fichero.

Con el fin de exportar las entradas correspondientes para poder realizar un posterior análisis se deben ejecutar las siguientes instrucciones:

```
reg export "HKEY_CLASSES_ROOT\batfile\shell\open\command" "HKCR-batfile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\cmdfile\shell\open\command" "HKCRcmdfile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\comfile\shell\open\command" "HKCRcomfile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\exefile\shell\open\command" "HKCRexefile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\htafile\shell\open\command" "HKCRhtafile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\https\shell\open\command" "HKCRhttps-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\JSEfile\shell\open\command" "HKCRJSEfile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\piffile\shell\open\command" "HKCRpiffile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\regfile\shell\open\command" "HKCRregfile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\scrfile\shell\open\command" "HKCRscrfile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\txtfile\shell\open\command" "HKCRtxtfile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\VBSfile\shell\open\command" "HKCRVBSfile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export "HKEY_CLASSES_ROOT\WSFFile\shell\open\command" "HKCRWSFFile-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\software\Classes\batfile\shell\open\command"
"HKLMbatfile-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\software\Classes\comfile\shell\open\command"
"HKLMcomfile-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\software\Classes\exefile\shell\open\command"
"HKLMexefile-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"

reg export
"HKEY_LOCAL_MACHINE\software\Classes\piffile\shell\open\command"
"HKLMpiffile-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

O bien, ejecutar el siguiente archivo de procesamiento por lotes:

```
@echo off

for %%t in (batfile cmdfile comfile exefile htafile https JSEfile
piffile regfile scrfile txtfile VBSfile WSFFile) do (

reg export "HKEY_CLASSES_ROOT\%%t\shell\open\command" "HKCR-%%t-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

)

for %%t in (batfile comfile exefile piffile) do (

reg export "HKEY_LOCAL_MACHINE\software\Classes\%%t\shell\open\command"
"HKLM-%%t-%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"

)
```

5.3.4.7. Asociaciones de ficheros con depuradores.

En el registro de Windows hay una serie de entradas gracias a la cuales se puede indicar al sistema operativo que abra un programa listo para ser depurado. Hay malware que aprovecha estas entradas para ejecutarse automáticamente por lo que es recomendable ejecutar la siguiente instrucción en este tipo de incidentes con el fin de exportar la entrada de registro correspondiente.

```
reg export "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options" "HKLM-IFEO-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"
```

5.3.4.8. Browser Helper Objects (BHO)

Los *Browser Helper Objects* son complementos que permiten añadir funcionalidades al navegador. En ocasiones, algunos programas crean BHOs con el fin de monitorizar las páginas visitadas, mostrar ventanas emergentes de publicidad, modificar el resultado en los diferentes motores de búsqueda, etc. Es por ello que en cierto tipo de incidentes resulta de utilidad exportar la entrada de registro correspondiente a estos complementos. Para exportar dicha información se debe ejecutar la siguiente instrucción (válido hasta Windows 7):

```
reg export
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\B
rowser Helper Objects" "BHOs-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

Ejemplo

Un caso práctico corresponde a un equipo que se sospechaba que estaba infectado ya que mostraba constantes ventanas de publicidad por lo que se realizó una exportación de dicha clave de registro, como se puede observar en la Ilustración 20.

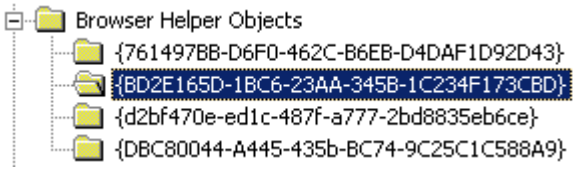

Ilustración 20: Browser Helper Objects

Al analizar la exportación se comprobó que el BHO seleccionado tenía asociado una librería (DLL) que correspondía a un malware conocido como **Adware.BHO.NAP**, como se observa en la Ilustración 21.

Ilustración 21: Análisis de Virustotal de un fichero asociado a una BHO

5.3.4.9. MUICache

Cada vez que un usuario ejecuta por primera vez un programa se almacena en el registro una entrada que guarda el nombre del programa. Dicha clave se encuentra en:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache` en Windows XP.
- `HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache` en Windows 7/8.

Para exportar dicha información se debe ejecutar la siguiente instrucción:

Windows XP

```
reg export
"HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache"
"MUICache-%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"
```

Windows 7/8

```
reg export "HKEY_CURRENT_USER\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\MuiCache" "MUICache-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.reg"
```

Otras utilidades

MUICacheView http://www.nirsoft.net/utils/muicache_view.html

5.3.4.10. LastVisitedMRU / LastVisitedPidlMRU

En el registro de Windows se almacena el listado de aplicaciones utilizadas recientemente. Dicha información puede resultar interesante en ciertos tipos de incidentes por lo que para exportarla se debe ejecutar la siguiente instrucción:

Windows XP

```
reg export
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVi
sitedMRU" "LastVisitedMRU-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

Windows 7/8

```
reg export
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVi
sitedPidlMRU" "LastVisitedPidlMRU-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

5.3.4.11. OpenSaveMRU

La entrada de registro *OpenSaveMRU* contiene el listado de ficheros abiertos o guardados desde la ventana correspondiente al cuadro de diálogo que utilizan la mayor parte de las aplicaciones, como se observa en la Ilustración 22.

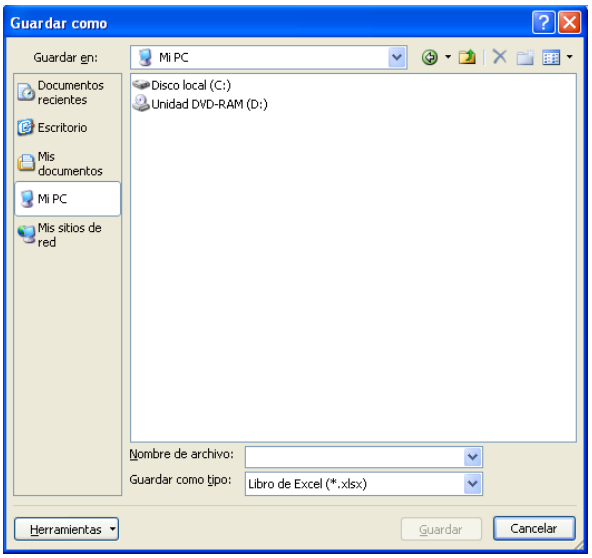

Ilustración 22: Cuadro de diálogo correspondiente a la entrada OpenSaveMRU

Para exportar esta información se debe ejecutar la siguiente instrucción:

Windows XP

```
reg export
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSa
```

```
veMRU" "OpenSaveMRU-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

Windows 7/8 (No válido en Windows 8.1)

```
reg export
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSa
vePidlMRU" "OpenSavePidlMRU-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

5.3.4.12. Ficheros abiertos recientemente

La entrada *RecentDocs* almacena el listado de ficheros abiertos recientemente. Para exportar esta información se debe ejecutar la siguiente instrucción:

```
reg export
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs"
"RecentDocs-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

Ejemplo

En este ejemplo se simula un posible caso de acceso a información indebida como es el fichero Cuentas Generales Empresa Ficticia.pdf desde el equipo analizado, como se observa Ilustración 23.

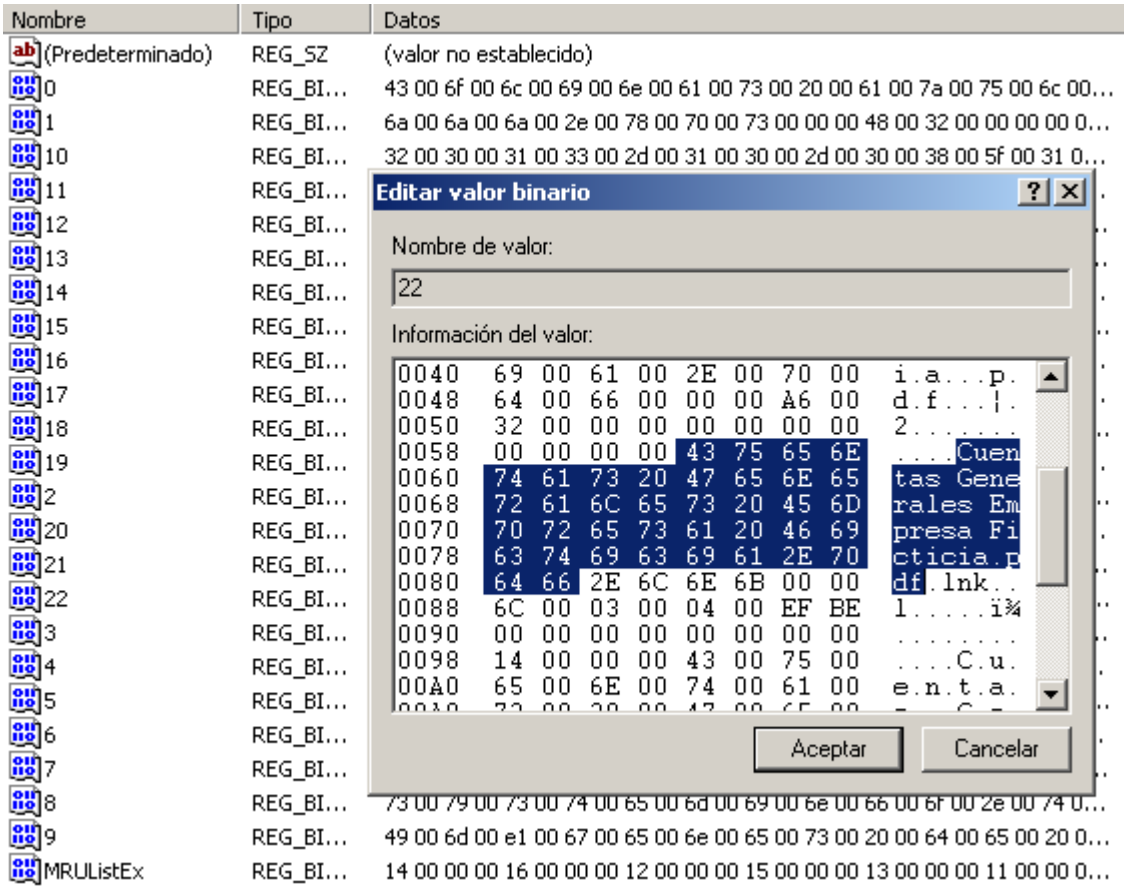

Ilustración 23: Ficheros abiertos recientemente

5.3.4.13. Software instalado.

Windows almacena en el registro el listado del software instalado junto con su información. Para exportar esta información se debe ejecutar la siguiente instrucción:

```
reg export
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall"
"SoftwareInstalado-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.reg"
```

5.3.5. Contraseñas

En ciertos incidentes puede resultar muy útil conocer los diferentes nombres de usuario y contraseñas almacenadas en el equipo, así que es recomendable su recopilación siempre y cuando se haya obtenido previamente una autorización expresa, y se traten de acuerdo a la legislación vigente sobre protección de datos.

Existen multitud de contraseñas que pueden estar almacenadas en el equipo, de diferentes servicios como correo electrónico, banca online, servicios de compra-venta, etc. y un gran número de programas para recopilarlas. A continuación se indican una selección de los más habituales:

- **WebBrowserPassView**[39]: Recopila las contraseñas almacenadas en los principales navegadores: Internet Explorer (Versión 4.0 - 10.0), Mozilla Firefox (todas las versiones), Google Chrome, Safari, y Opera.

```
WebBrowserPassView /stab "ContraseñasNavegadores-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

- **Network Password Recovery**[40]: Recopila las contraseñas correspondientes a los recursos de red a los que está conectado el usuario actual.

```
Netpass /stab "NetworkPasswordRecovery-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

- **Mail PassView**[41]: Recopila las contraseñas de los principales gestores de correo.

```
mailpv /stab "MailPassView-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

5.3.6. Información cacheada en los navegadores (direcciones, historial de descargas)

- En el caso de Google Chrome se debe copiar el fichero *Web data* mediante el siguiente comando:

Windows XP

```
copy %UserProfile%\Configuracion local\Datos de
programa\Google\Chrome\User Data\Default\Web Data  WebData
```

Windows 7/8

```
copy %UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Web
Data WebData
```

Dicho fichero corresponde a una base de datos en formato SQLITE que puede ser visualizada mediante diferentes utilidades como SQLite Database Browser[42]. En el propio directorio es posible localizar diferentes ficheros que almacenan información como los marcadores o el historial, entre otros, por lo que puede resultar interesante realizar una copia completa del mismo dependiendo del incidente.

- En el caso de Mozilla Firefox se debe copiar el fichero *formhistory.sqlite* mediante el siguiente comando:

Windows XP

[39] http://www.nirsoft.net/utils/web_browser_password.html
[40] http://www.nirsoft.net/utils/network_password_recovery.html
[41] http://www.nirsoft.net/utils/mailpv.html
[42] http://sourceforge.net/projects/sqlitebrowser/

```
copy %UserProfile%\Configuracion local\Datos de programa\
\Mozilla\Firefox\Profiles\<random>.default\formhistory.sqlite
formhistory.sqlite
```

Windows 7/8

```
copy %UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\
<random>.default\formhistory.sqlite formhistory.sqlite
```

Donde <*random*> es el nombre aleatorio que asigna Firefox a la carpeta del usuario. Para conocerlo previamente será necesario listar el contenido del directorio *Profiles*. Al igual que en otros navegadores, en la ruta del perfil del usuario se almacena otro tipo de información.

- En el caso de Internet Explorer es posible utilizar la herramienta **IECacheView**[43]. Para ello, basta con utilizar la siguiente instrucción:

```
IECacheView /stab "IECache-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

5.3.7. Árbol de directorios y ficheros

Puede resultar interesante conocer el árbol de directorios y ficheros con el fin de poder comprobar la existencia de ficheros sospechosos. Para ello, se deben obtener 3 listados mediante las siguientes instrucciones, y que corresponden a los tiempos MAC (Modificación, Acceso, Creación) de los ficheros:

- Listado en base a la fecha de modificación.

```
dir /t:w /a /s /o:d c:\ > "ListadoFicherosPorFechaDeModificacion-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

- Listado en base al último acceso.

```
dir /t:a /a /s /o:d c:\ > "ListadoFicherosPorUltimoAcceso-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

- Listado en base a la fecha de creación.

```
dir /t:c /a /s /o:d c:\ > "ListadoFicherosPorFechaDeCreacion-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Nota

En el caso de que existan varios discos duros o particiones se deberá ejecutar la instrucción por cada disco o partición, es decir, habría que ejecutar el comando tantas veces como fuera necesario cambiando el directorio sobre el que se hace el listado, en este caso c:

[43] http://www.nirsoft.net/utils/ie_cache_viewer.html

y cambiando a su vez el nombre del fichero que almacenará el listado.

Otras utilidades

MacMatch	http://ntsecurity.nu/toolbox/macmatch/

5.3.8. Histórico del intérprete de comandos

En el caso de que al realizar el proceso de toma de evidencias haya una ventana abierta del intérprete de comandos, se puede obtener el histórico de comandos ejecutados mediante la siguiente instrucción:

```
doskey /history > "HistoricoCMD-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

5.3.9. Capturas de pantalla

En el caso de que la persona responsable de realizar la adquisición de evidencias desee obtener alguna captura de pantalla porque haya observado algo significativo y que debe ser recopilado, puede utilizar alguna herramienta por línea de comandos como por ejemplo **screenshot-cmd**[44].

Para ello, se debe escribir la siguiente instrucción:

```
Screenshot-cmd -o "Screenshot-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%%time:~6,2%.png"
```

5.3.10. Información del portapapeles

En el portapapeles se almacena información que puede resultar de interés: URLS, contraseñas, fragmentos de texto, etc. Es por ello que se recomienda comprobar su contenido. Para ello se puede utilizar alguna herramienta como **InsideClipboard**[45]:

```
InsideClipboard /saveclp "Portapapeles-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.clp"
```

5.3.11. Historial de internet

El historial de internet puede resultar un foco muy importante de información en algunos incidentes, principalmente los relacionados con algún tipo de infección por malware provocado por el acceso a páginas web infectadas. En los últimos tiempos, los creadores de malware han intensificado el aprovechamiento de vulnerabilidades en los navegadores, en las tecnologías con las que se desarrollan páginas web o en los servidores sobre los que se alojan

[44] https://code.google.com/p/screenshot-cmd/
[45] http://www.nirsoft.net/utils/inside_clipboard.html

para infectar a un gran número de usuarios de Internet. Este incremento en la explotación de este tipo de vulnerabilidades es provocado debido a que es una manera sencilla y eficiente de llegar a gran cantidad de usuarios. Es por todo ello que en muchos casos es recomendable obtener la información referente al historial para poder analizar la actividad en Internet.

Por comodidad, ya que soporta los principales navegadores (Internet Explorer, Mozilla Firefox, Google Chrome, y Safari) y versiones de los mismos, es recomendable utilizar algún tipo de herramienta como **BrowsingHistoryView**[46].

```
BrowsingHistoryView.exe /HistorySource 2 /LoadIE 1 /LoadFirefox 1
/LoadChrome 1 /LoadSafari 1 /stab Historial-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Otras utilidades

Browser History Spy	http://securityxploded.com/browser-history-spy.php
IEHistoryView	http://www.nirsoft.net/utils/iehv.html
MozillaHistoryView	http://www.nirsoft.net/utils/mozilla_history_view.html
ChromeHistoryView	http://www.nirsoft.net/utils/chrome_history_view.html
Pasco	http://www.mcafee.com/es/downloads/free-tools/pasco.aspx
Mandiant Redline	https://www.mandiant.com/resources/download/redline

Ejemplo

Un caso práctico corresponde a un equipo infectado por malware. Tras exportar y analizar el historial se observó la Ilustración 24:

Ilustración 24: URL correspondiente a un malware en el historial de un equipo infectado

Dicho ejecutable, clasificado como **Trj/Lineage.JAE**, era el responsable de la infección y gracias a la exportación del historial se obtuvo el foco de infección.

[46] http://www.nirsoft.net/utils/browsing_history_view.html

5.3.12. Últimas búsquedas

Conocer las últimas búsquedas en los principales motores de búsqueda puede resultar de interés dependiendo del tipo de incidente. Para recopilar toda esta información se pueden utilizar herramientas como **MyLastSearch**[47], la cual obtiene todas las búsquedas realizadas en los principales motores de búsqueda (Google, Yahoo y MSN) y en varias redes sociales como por ejemplo Twitter, Facebook, MySpace, etc.

```
MyLastSearch /stab "MyLastSearch-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

5.3.13. Cookies

Las cookies son pequeños ficheros de texto que permiten, entre otras cosas, mantener la sesión iniciada en un sitio web, realizar un seguimiento de la misma, almacenar las preferencias de visualización, etc. A partir de ellas se puede obtener cierta información que puede ser relevante en un proceso forense como direcciones de páginas web, nombres de usuario, fechas, etc. Por este motivo, puede resultar de interés obtenerlas para poder analizarlas en el caso de que sea necesario.

Existen diferentes utilidades dependiendo del navegador para poder visualizar de una manera sencilla las cookies. Entre todas ellas, destacan **ChromeCookiesView**[48], **MozillaCookiesView**[49] y **IECookiesView**[50]. Su funcionamiento es similar:

Otras utilidades

Galleta	http://www.mcafee.com/es/downloads/free-tools/galleta.aspx
Mandiant Redline	https://www.mandiant.com/resources/download/redline

5.3.14. Volúmenes cifrados

Cada vez es más habitual utilizar herramientas de cifrado con el fin de añadir cierto nivel de privacidad y seguridad a la información. Puede resultar de interés en un proceso forense identificar volúmenes cifrados ya que es probable que almacenen información relevante. Para ello se pueden utilizar herramientas como **Encrypted Disk Detector**[51], la cual analiza las unidades de almacenamiento del ordenador y determina si alguna de ellas corresponde a un volumen cifrado con las principales herramientas, como TrueCrypt, PGP®, Safeboot, o Bitlocker®.

Para ello, se debe escribir la siguiente instrucción:

[47] http://www.nirsoft.net/utils/my_last_search.html
[48] http://www.nirsoft.net/utils/chrome_cookies_view.html
[49] http://www.nirsoft.net/utils/mzcv.html
[50] http://www.nirsoft.net/utils/iecookies.html
[51] http://info.magnetforensics.com/encrypted-disk-detector/

```
EDD.exe > "VolumenesEncriptados-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

5.3.15. Unidades mapeadas

Para obtener el listado de unidades mapeadas se debe ejecutar la siguiente instrucción:

```
net use > "UnidadesMapeadas-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 25:

Ilustración 25: Unidades mapeadas

5.3.16. Carpetas compartidas

Con el fin de obtener el listado de recursos compartidos se debe ejecutar la siguiente instrucción:

```
net share > "CarpetasCompartidas-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 26:

Ilustración 26: Carpetas compartidas

5.3.17. Grabaciones pendientes

A partir de Windows XP, los sistemas operativos poseen la capacidad de grabar CDs sin necesidad de utilizar software adicional. Dicha funcionalidad debe ser tenida en cuenta en algunos incidentes como por ejemplo los relacionados con el robo de información en el caso de que se pille al infractor con “las manos en la masa”. Pese a que la forma más habitual de realizar esta práctica sea mediante la utilización de *pendrives* o el envío de emails, no se debe descartar esta posibilidad. Por este motivo, se debe comprobar la existencia de compilaciones pendientes con el fin de poder analizar qué ficheros se pretendían grabar.

Para ello se debe acceder la siguiente instrucción desde una ventana del intérprete de comandos, la cual exporta el listado de ficheros pendientes de grabación.

En Windows XP

```
dir "%UserProfile%\Configuración local\Application Data\Microsoft\CD
Burning" > "GrabacionesPendientes-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

En Windows 7/8

```
dir "%UserProfile%\AppData\Local\Microsoft\Windows\Burn" >
"GrabacionesPendientes-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Nota

Es posible sustituir la variable de entorno `%UserProfile%` por la ruta correspondiente al directorio del perfil del usuario.

5.4. INFORMACIÓN NO VOLÁTIL

Una vez recopilada la información volátil, se procede a la recolección de aquellas evidencias que no lo son, pero no por ello tienen menor importancia.

5.4.1. Volcado de disco

Algunos factores a tener en cuenta a la hora de realizar la toma de evidencias son la rapidez de dicha toma y la integridad de la misma. Hoy en día el volumen de los discos es muy amplio por lo que el proceso puede resultar costoso en cuanto a tiempo y a recursos. Se debe tener bien claro qué tipo de volcado se va a realizar, y podemos clasificarlos en 3 tipos:

- **Crear una copia *bit stream* de disco a imagen**: es el método más habitual y más rápido. Además, permite realizar tantas copias como sea necesario de una manera fácil y sencilla para la fase de análisis. Para crear una copia *bit stream* de disco a imagen se puede utilizar alguna utilidad como **FTK Imager**[52] (versión de línea de comandos). Para ello tan sólo es necesario seguir los siguientes pasos:

```
ftkimager.exe \\.\PHYSICALDRIVE0 g:\ImagenHD --verify
```

  En el caso de realizar un volcado de un disco duro que no sea el principal, o si existen varias particiones, se puede realizar un listado de las unidades disponibles mediante el siguiente parámetro:

```
ftkimager.exe -list-drives
```

Otras utilidades

[52] http://www.accessdata.com/support/product-downloads

WinDD	http://sourceforge.net/projects/windd/
Clonezilla	http://clonezilla.org
OSFClone	http://www.osforensics.com/tools/create-disk-images.html

- **Crear una copia bit stream de disco a disco**: es el método utilizado en el caso de que no sea posible realizar una copia bit stream de disco a imagen.

  Del mismo modo que el método anterior se puede realizar tantas copias como discos dispongamos. La realización de un clonado mediante un dispositivo hardware conlleva una mayor fiabilidad y rapidez. Sin embargo, como se ha indicado anteriormente, en esta guía se ha optado por la utilización de software libre y gratuito con el fin de que dicha tarea no suponga un sobrecoste en lo que a licencias se refiere.

  Para crear una copia *bit stream* de disco a disco se puede utilizar alguna utilidad como **Clonezilla**[53]. Para ello tan sólo es necesario arrancar el equipo con la utilidad y seguir los pasos que indican.

Otras utilidades

DC3DD	http://sourceforge.net/projects/dc3dd/
OSFClone	http://www.osforensics.com/tools/create-disk-images.html
dd	Disponible en la distribuciones con Linux
FOG	http://sourceforge.net/projects/freeghost/
AIR - Automated Image and Restore	http://sourceforge.net/projects/air-imager/

Nota

Cuando se trata de crear una copia *bit stream* de disco a imagen o de disco a disco, en los discos duros de estado sólido (SSD) *Solid State Drive*, hay que tener en cuenta lo siguiente:

Los discos SSD no funcionan de igual de modo que los discos magnéticos. Además, los fabricantes implementaron el comando TRIM gracias al cual se prolonga la vida útil de los SSD e impide la degradación de su rendimiento. Dicho comando permite informar qué celdas ya no están en uso al controlador, el cual a su vez, notifica al recolector de basura

[53] http://clonezilla.org

para que vaya borrando electrónicamente el contenido de esas celdas y las prepare para futuras operaciones de escritura. Es muy importante tener claro que no es posible evitar el proceso de recolección de basura en el caso de que el comando TRIM esté activado, ni si quiera cambiando el disco SSD a otro equipo, ni poniendo un bloqueador de escritura, ya que un disco SSD únicamente con tener corriente iniciará dicho proceso de manera automática.

Esto quiere decir que si un usuario elimina un fichero, y el comando TRIM está activado, la evidencia desaparecerá para siempre. Este hecho no afecta a los volúmenes cifrados como TrueCrypt, BitLocker, etc por lo que deben ser recopilados para un posterior análisis.

Así mismo, hay que tener en cuenta que este hecho afecta a la hora de sacar el hash de un disco SDD, el cual puede ser distinto, ya que el proceso que desencadena el comando TRIM corre en un segundo plano y pese a que aparentemente dicho disco no haya sufrido ninguna modificación, en realidad sí que haya sufrido cambios.

- **Creación de una copia de datos dispersos de una carpeta o archivo:** es decir, realizar una copia selectiva: ya que en muchas ocasiones dependiendo del tipo de incidente puede no ser necesario volcar todo el disco y sea suficiente copiar ciertas carpetas o ficheros.

  Para ello basta con utilizar alguna herramienta como **Teracopy**[54]. Un ejemplo de utilización es el siguiente:

```
TeraCopy.exe Copy "D:\Info" F:\Backup
```

Mediante esta herramienta es posible comprobar si el proceso de copiado se ha realizado correctamente ya que calcula hashes de los ficheros y sus respectivas copias y los compara.

Otras utilidades

Robocopy	http://technet.microsoft.com/es-es/library/cc733145(v=ws.10).aspx
Copy	Disponible en sistemas operativos Windows.
Xcopy	Disponible en sistemas operativos Windows.
ForensicCopy	http://sandersonforensics.com/forum/content.php?121-ForensicCopy

¡Importante!

[54] http://codesector.com/teracopy

En los tres casos descritos, independientemente del que se haya llevado a cabo, será obligatorio trabajar durante el análisis sobre las copias realizadas, manteniendo intacta la información original y preservando en todo momento su integridad.

5.4.2. Master Boot Record (MBR)

El *Master Boot Record* hace referencia al primer sector, sector 0, de un dispositivo de almacenamiento de datos, como por ejemplo un disco duro. Posee un tamaño de 512 bytes y almacena información relativa a cómo iniciar el sistema, qué tipo de particiones hay en el dispositivo y el tamaño de las mismas, etc.

En cierto tipo de incidentes, principalmente relacionados con malware, puede resultar de interés extraerlo para que en un posterior análisis determinar si está infectado.

Para ello, es recomendable la utilización de alguna herramienta como **MBRutil**[55], la cual permite exportar el MBR ejecutando la siguiente instrucción:

```
MBRutil /S="MBR-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.dat"
```

Así mismo, es posible realizar el proceso con las herramientas anteriormente mencionadas **DC3DD** y **dd**.

5.4.3. Master File Table (MFT)

La *Master File Table* es una tabla que almacena información relevante de todos los ficheros y carpetas de una unidad o disco. Contiene, entre otra, información como nombre, tamaño, fecha, hora, o permisos, incluso de ficheros que hayan sido eliminados hasta el momento en el que dicho espacio sea necesario y se sobrescriba.

Para exportar la *Master File Table* se pueden utilizar alguna herramienta como **Ntfswalk**[56]. Para ello, se debe escribir la siguiente instrucción:

```
Ntfswalk –partition c -csv > "MFT-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.csv"
```

5.4.4. Información del sistema

Desde el intérprete de comandos mediante la instrucción **systeminfo** se puede obtener información referente al *hardware*, *software*, *hotfixes*, versiones, tiempo de actividad, etc.

Para ello, se debe escribir la siguiente instrucción:

```
systeminfo > "InformaciónDelSistema-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

[55] http://www.symantec.com/business/support/index?page=content&id=TECH93277
[56] https://tzworks.net/prototype_page.php?proto_id=12

Y el resultado obtenido es la Ilustración 27:

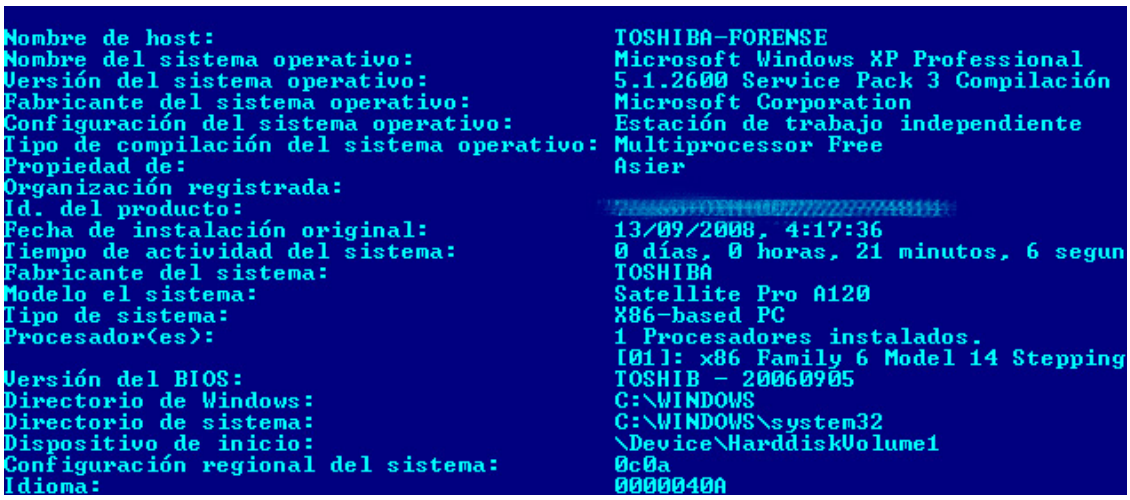

Ilustración 27: Información del sistema

Así mismo, es posible realizar dicho proceso mediante otras herramientas como **psinfo**[57].

5.4.5. Tareas programadas

Mediante el comando **schtasks** se pueden visualizar las tareas programadas en el sistema operativo.

Para ello, se debe escribir la siguiente instrucción:

```
schtasks > "TareasProgramadas-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Así mismo, es útil obtener el fichero **schedlgu.txt** ubicado en `%WinDir%` en Windows XP y en `%WinDir%\Tasks` en Windows 7/8, el cual almacena las tareas programadas que se han ejecutado, si lo han hecho correctamente o no, la hora de ejecución, etc.

Ejemplo

Un caso práctico corresponde a un equipo que se sospechaba que estaba infectado por lo que, entre mucha otra información, se obtuvo el listado de tareas programadas. Tras analizarlas se concluyó que el malware había creado una tarea programada para lanzar un componente adicional que realizaba ciertas acciones en el equipo infectado.

5.4.6. Ficheros impresos

Es posible recuperar los ficheros enviados a imprimir en el caso de que se haya marcado la opción de "*Conservar los documentos después de su impresión*" en las propiedades de la impresora, ya que Windows crea ficheros de almacenamiento intermedio con extensión *.SPL (metadatos: propietario, método de impresión, etc) y *.SHD (datos a imprimir) en la carpeta

[57] http://technet.microsoft.com/es-es/sysinternals/bb897550.aspx

`%WinDir%\system32\spool\printers` cada vez que enviamos un documento a imprimir. Una vez finalizado el proceso de impresión dichos ficheros son eliminados salvo que se haya indicado lo contrario, como ocurre al marcar la opción anteriormente indicada.

5.4.7. Variables de entorno

Para conocer todas las variables de entorno, es decir, aquellas que están en el *path* se deben ejecutar la siguiente instrucción:

```
path > "VariablesDeEntorno-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

Y el resultado obtenido es la Ilustración 28:

```
00000000: 50 41 54 48-3D 43 3A 5C-57 49 4E 44-4F 57 53 5C  PATH=C:\WINDOWS\
00000010: 73 79 73 74-65 6D 33 32-3B 43 3A 5C-57 49 4E 44  system32;C:\WIND
00000020: 4F 57 53 3B-43 3A 5C 57-49 4E 44 4F-57 53 5C 53  OWS;C:\WINDOWS\S
00000030: 79 73 74 65-6D 33 32 5C-57 62 65 6D-3B 43 3A 5C  ystem32\Wbem;C:\
00000040: 41 72 63 68-69 76 6F 73-20 64 65 20-70 72 6F 67  Archivos de prog
00000050: 72 61 6D 61-5C 49 6E 74-65 6C 5C 44-4D 49 58 3B  rama\Intel\DMIX;
00000060: 43 3A 5C 41-72 63 68 69-76 6F 73 20-64 65 20 70  C:\Archivos de p
00000070: 72 6F 67 72-61 6D 61 5C-41 72 63 68-69 76 6F 73  rograma\Archivos
00000080: 20 63 6F 6D-75 6E 65 73-5C 52 6F 78-69 6F 20 53   comunes\Roxio S
00000090: 68 61 72 65-64 5C 44 4C-4C 53 68 61-72 65 64 5C  hared\DLLShared\
000000A0: 3B 43 3A 5C-41 72 63 68-69 76 6F 73-20 64 65 20  ;C:\Archivos de
000000B0: 70 72 6F 67-72 61 6D 61-5C 41 72 63-68 69 76 6F  programa\Archivo
000000C0: 73 20 63 6F-6D 75 6E 65-73 5C 52 6F-78 69 6F 20  s comunes\Roxio
000000D0: 53 68 61 72-65 64 5C 44-4C 4C 53 68-61 72 65 64  Shared\DLLShared
000000E0: 5C 3B 43 3A-5C 41 72 63-68 69 76 6F-73 20 64 65  \;C:\Archivos de
000000F0: 20 70 72 6F-67 72 61 6D-61 5C 41 72-63 68 69 76   programa\Archiv
00000100: 6F 73 20 63-6F 6D 75 6E-65 73 5C 52-6F 78 69 6F  os comunes\Roxio
00000110: 20 53 68 61-72 65 64 5C-39 2E 30 5C-44 4C 4C 53   Shared\9.0\DLLS
00000120: 68 61 72 65-64 5C 3B 43-3A 5C 57 49-4E 44 4F 57  hared\;C:\WINDOW
00000130: 53 5C 73 79-73 74 65 6D-33 32 5C 57-69 6E 64 6F  S\system32\Windo
00000140: 77 73 50 6F-77 65 72 53-68 65 6C 6C-5C 76 31 2E  wsPowerShell\v1.
00000150: 30 3B 43 3A-5C 50 79 74-68 6F 6E 33-33 3B 43 3A  0;C:\Python33;C:
00000160: 5C 44 6F 63-75 6D 65 6E-74 73 20 61-6E 64 20 53  \Documents and S
```

Ilustración 28: Variables de entorno

5.4.8. Logs del sistema

Los logs son ficheros de texto que almacenan información relevante como conexiones remotas, eventos del sistema, etc. Existen varios que son de gran interés forense y que deben ser recopilados.

5.4.8.1. Windows Event Logs

Dentro de los logs de eventos de Windows hay 3 que tienen especial importancia:

- *AppEvent.evt(x)*: Registra los sucesos relativos a aplicaciones.
- *SysEvent.evt(x)*: Registra los sucesos relativos al sistema.
- *SecEvent.evt(x)*: Registra los sucesos relativos a la seguridad.

En Windows XP están ubicados en `%systemroot%\system32\config` se pueden exportar utilizando algún programa como **psloglist**[58]:

[58] http://technet.microsoft.com/en-us/sysinternals/bb897544

```
psloglist -s application > "Application-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"

psloglist -s system > "System-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"

psloglist -s security > "Security-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.txt"
```

En Windows 7/8 están ubicados en `%systemroot%\system32\winevt\Logs` y, además de la utilidad anteriormente indicada, se pueden exportar mediante la utilidad de sistema **wevtutil**. Para ello se deben ejecutar las siguientes instrucciones:

```
wevtutil epl application "Application-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.evtx"

wevtutil epl system "System-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.evtx"

wevtutil epl security "Security-%date:~6,4%%date:~3,2%%date:~0,2%-
%time:~0,2%%time:~3,2%.evtx"
```

Mediante dicha utilidad se pueden exportar gran cantidad de logs del sistema operativo. Para obtener la lista completa se debe ejecutar la siguiente instrucción:

```
wevtutil el
```

Otras utilidades

MyEventViewer	http://www.nirsoft.net/utils/my_event_viewer.html

5.4.8.2. WindowsUpdate.log

El fichero *WindowsUpdate.log*, ubicado en la carpeta `%WinDir%`, almacena el listado de actualizaciones correspondientes al sistema operativo que se han llevado a cabo en el equipo.

Ejemplo

Un caso práctico corresponde a un equipo que había sido víctima de una intrusión remota y gracias al fichero WindowsUpdate.log se constató que el atacante había aprovechado ciertas vulnerabilidades del sistema operativo que no habían sido parcheadas.

5.4.8.3. pfirewall.log

El fichero *pfirewall.log*, ubicado en la carpeta `%WinDir%` (Windows XP) y en `%WinDir%\System32\LogFiles\Firewall` (Windows 7/8), almacena diferente información correspondiente al firewall de Windows como por ejemplo paquetes perdidos o conexiones que se han realizado correctamente.

5.4.8.4. Otros logs

Existen otra serie de logs que pueden estar presentes en el equipo u otros equipos del sistema, y que pueden resultar de interés dependiendo del tipo de incidente, por lo que es conveniente su recopilación. Algunos de ellos pueden ser los siguientes:

- Servidores Web como Internet Information Server (IIS), Apache, etc.
- Utilidades de acceso remoto como WinVNC, pcAnywhere, etc.
- Clientes FTP como Filezilla, WinSCP, etc.
- Firewalls o sistemas de detección de intrusos.
- Logs DHCP.
- Logs de programas de mensajería como Skype.
- Fichero de sincronización de dropbox (.dbx).

5.4.9. Archivos .pst y .ost

Los archivos PST (*personal storage file*) corresponden a copias de seguridad de los emails, entradas del calendario, etc. de Microsoft Outlook.

Los archivos OST corresponden a archivos de datos de Outlook sin conexión y almacenan, en el caso de que se haya configurado, los mensajes de correo electrónico, los elementos del calendario, etc.

Las principales diferencias entre estos dos tipos de archivos de datos de Outlook son:

- Los archivos PST se utilizan para cuentas POP3, IMAP y basadas en Web y permiten realizar copias de seguridad de las carpetas de Outlook y los elementos del equipo, incluidas las cuentas Exchange.
- Los archivos OST se utilizan en los casos en los que esté configurada una cuenta de Exchange y se desee trabajar sin conexión.

La mayoría de los gestores de correo electrónico permiten también realizar copias de seguridad en formato PST por lo que es aconsejable obtener estos ficheros ya que, en cierto tipo de incidentes, puede resultar interesante el posterior análisis debido a que pueden contener por ejemplo el registro de conversaciones, intercambio de información, registros de fugas de información, etc. Por defecto, en Windows XP y Windows 7, los ficheros están almacenadas en la carpeta Archivos de Outlook en Mis Documentos, y en Windows 8 en `%UserProfile%\AppData\Local\Microsoft\Outlook`.

5.4.10. Carpeta prefetch

En esta carpeta se almacenan los programas que se abren habitualmente y es utilizada por el sistema operativo para cargarlos en memoria con una mayor rapidez. Cada programa utilizado habitualmente tiene asociado un fichero con extensión PF que almacena información como el nombre del ejecutable, el número de veces que se ha ejecutado, librerías asociadas, etc.

Se pueden visualizar accediendo a la carpeta `%WinDir%\Prefetch`, como se observa en la Ilustración 29.

Nombre	Tamaño de C...	Tipo	Fecha de modificación
CHROME.EXE-11BAD832.pf	38 KB	Archivo PF	10/12/2013 15:46
CHROME.EXE-127CD585.pf	56 KB	Archivo PF	05/12/2013 13:35
CHROME.EXE-38321E8B.pf	117 KB	Archivo PF	04/12/2013 11:14
CHROME.EXE-6051491A.pf	61 KB	Archivo PF	10/12/2013 15:41
CLIPBRD.EXE-1B911FB5.pf	15 KB	Archivo PF	04/12/2013 16:14
CMD.EXE-087B4001.pf	12 KB	Archivo PF	05/12/2013 16:28
CMD.EXE-339B0F65.pf	11 KB	Archivo PF	10/12/2013 13:41
CONTROL.EXE-013DBFB5.pf	19 KB	Archivo PF	10/12/2013 12:09
DEFRAG.EXE-273F131E.pf	16 KB	Archivo PF	10/12/2013 11:46
DFRGNTFS.EXE-269967DF.pf	38 KB	Archivo PF	10/12/2013 11:46
DOTNETFX45_FULL_X86_X64...	55 KB	Archivo PF	04/12/2013 15:48

Ilustración 29: Contenido carpeta Prefetch

Ejemplo

Un caso práctico corresponde a un equipo de una empresa que se sospechaba había sido víctima de una intrusión remota. Al comprobar los ficheros *prefetch* se constató que había ciertos programas que se habían ejecutado en horas fuera del horario de oficina.

5.4.11. Papelera de reciclaje

Es posible obtener información de los elementos eliminados que hayan sido enviados a la papelera de reciclaje. Para ello se debe de tener en cuenta la siguiente tabla:

Tabla 4: Rutas de la papelera de reciclaje según versión del sistema operativo.

Sistema operativo	Localización
Windows XP	`%SystemDrive%\Recycler`
Windows 7/8	`%SystemDrive%\$Recycle.Bin\`

En las rutas indicadas se almacenan carpetas con el siguiente formato S-1-5-21-299502267-1677128483-839522115-1003, correspondiente al identificador de Windows del usuario que lo ha borrado.

En el caso de Windows XP, dentro de dichas carpetas están los ficheros eliminados renombrados junto con un fichero de nombre INFO2, el cual almacena información correspondiente a la fecha de eliminación, el tamaño y la ruta donde se almacenaba dicho fichero.

A continuación, en la Ilustración 30, se indica la estructura de dicho fichero y la manera de obtener la información anteriormente indicada.

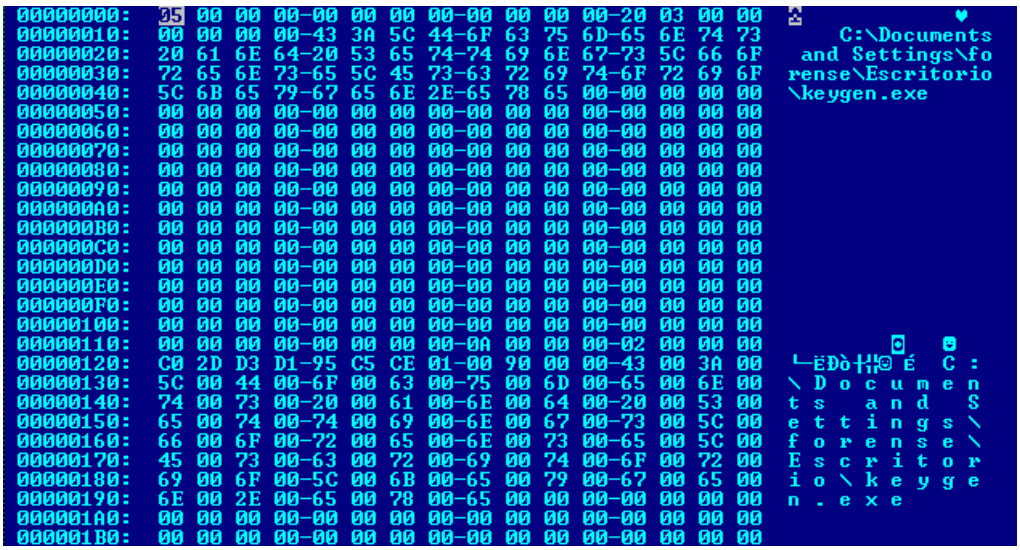

Ilustración 30: Estructura de los ficheros de la papelera de reciclaje

Los *bytes* comprendidos entre el 0 y F corresponden a la cabecera del fichero, y, dentro de ellos, los *bytes* 12 y 13 (20 03) al tamaño de cada registro de INFO2. Por cada fichero eliminado se crea un registro en el fichero. El valor está en hexadecimal, así que hay que realizar una conversión a decimal para hacerlo más comprensible, teniendo en cuenta que el valor está en *Little Endian*[59], es decir, 2003 = 0320 = 800 *bytes*.

El nombre del fichero o ficheros eliminados aparece dos veces, primero en ASCII y después en UNICODE. En este caso sólo hay un fichero eliminado cuyo nombre es keygen.exe y estaba ubicado en el escritorio del usuario.

La fecha de eliminación del fichero se puede ver en la Ilustración 31 desde el byte 272 al 279 (*offset* 0x10), teniendo en cuenta que se encuentra el formato *FILETIME*, *Little Endian* y Hexadecimal por lo que se debe convertir a un formato comprensible.

[59] http://es.wikipedia.org/wiki/Endianness

Ilustración 31: Fecha de eliminación de los ficheros de la papelera de reciclaje

En este caso, el valor es C0 2D D3 D1 95 C5 CE 01 = 01 CE C5 95 D1 D3 2D C0 = 130258686501400000 = Jueves, 10 de octubre de 2013 08:50:50

El tamaño del fichero eliminado se obtiene desde el byte 280 al 283 (offset 0x10), como se puede observar en la Ilustración 32. Para ello, se debe realizar una conversión de hexadecimal a decimal, teniendo nuevamente en cuenta el formato *Little Endian*, es decir, 00 90 00 00 = 00 00 90 00 = 36864 *bytes*.

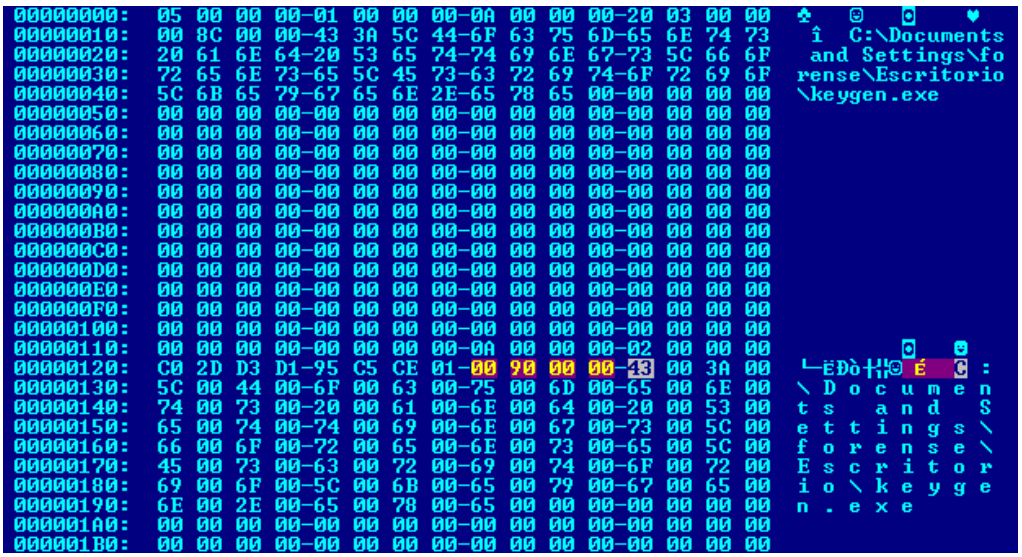

Ilustración 32: Tamaño de los ficheros de la papelera de reciclaje

El tamaño del fichero debe ser múltiplo de tamaño del clúster, en este caso 4096.

Con el fin de facilitar la interpretación del fichero INFO2 es recomendable la utilización de alguna herramienta como **rifiuti**[60].

[60] http://www.mcafee.com/es/downloads/free-tools/rifiuti.aspx

En el caso de Windows 7/8, dentro de las carpetas ubicadas en `%SystemDrive%\$Recycle.Bin\` por cada fichero eliminado habrá dos ficheros con el mismo nombre excepto la segunda letra, como se puede observar en la Ilustración 33. El que tiene la letra L como segunda letra almacena la ruta original del fichero borrado y el que tiene la letra R como segunda letra almacena el propio fichero borrado.

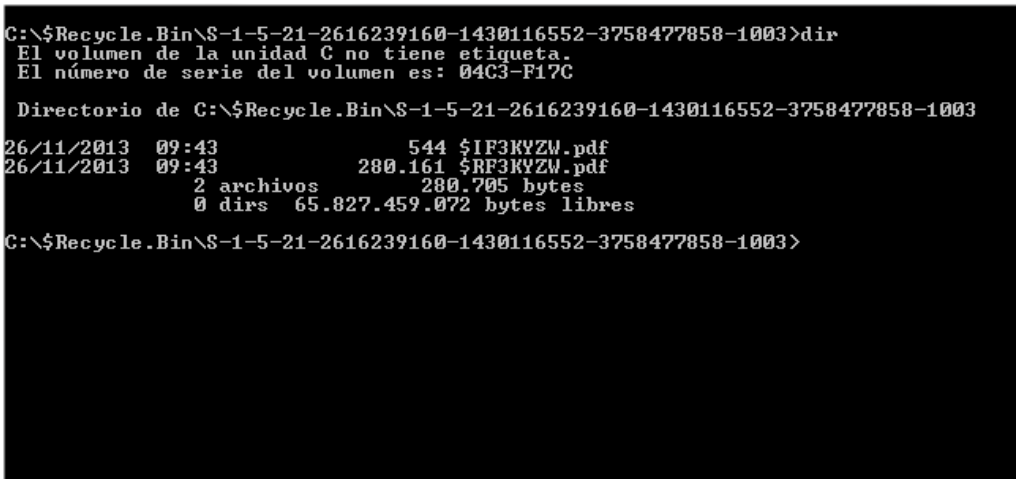

Ilustración 33: Papelera de reciclaje a partir de Windows 7

5.4.12. Fichero hosts

El funcionamiento del fichero hosts es el siguiente: cuando un usuario introduce una URL en el navegador, el sistema consulta en primer lugar el fichero hosts. En el caso de que el fichero contenga alguna asociación para dicha URL, se redirigirá a la dirección que tenga configurada y en el caso de que la URL no aparezca en el fichero hosts se realizará una consulta al ISP (*Internet Service Provider*) para solicitarle la dirección a la que debe ser redirigido.

Consultar el fichero hosts puede resultar una práctica conveniente en ciertas ocasiones ya que es habitual que en los casos de infección el malware modifique el fichero hosts con el fin de impedir que el usuario pueda acceder a ciertas páginas web, principalmente aquellas que corresponden a antivirus, suites de seguridad o actualizaciones de este tipo de software.

Para conocer obtener el contenido del fichero hosts se debe ejecutar la siguiente instrucción:

```
type c:\windows\system32\drivers\etc\hosts > "FicheroHosts-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Ejemplo

Un caso práctico corresponde a un equipo de un particular cuyo antivirus no se actualizaba y el usuario tampoco podía acceder a algunas páginas. Al comprobar el fichero host se observó la Ilustración 34:

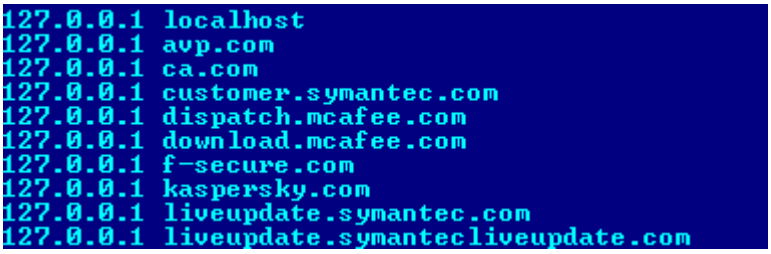

Ilustración 34: Fichero Host modificado por un malware

Contenía redirecciones para algunas compañías de antivirus con el fin de imposibilitar al usuario acceder a ellas.

5.4.13. Comprobar los ejecutables que no estén firmados

Dependiendo del tipo de incidente, y principalmente en aquellos relacionados con malware, resulta útil comprobar los ficheros no firmados de ciertas carpetas. Para ello se puede utilizar herramientas como **sigcheck**[61].

Para ello, se debe escribir la siguiente instrucción:

```
sigcheck -ct -h -vn -vt c:\Windows > "FicherosFirmados-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"

sigcheck -ct -h -vn -vt c:\Windows\System32 > "FicherosFirmadosWindows-
%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

5.4.14. Ficheros LNK

Los ficheros con extensión LNK corresponden a accesos directos. Estos ficheros almacenan gran cantidad de información que puede resultar relevante en un incidente:

- Ruta del fichero al que enlazan.
- Tiempos MAC tanto del propio fichero como del fichero que enlaza.
- Información de la unidad donde está almacenado (nombre, número de serie, dirección MAC, etc).
- Información de la red, en el caso de que referencie a un fichero almacenado en una ubicación remota.
- Tamaño del fichero.

Para recopilar todos estos ficheros se pueden emplear diferentes utilidades como **lnk-parser** o **Windows LNK Parsing Utility**. Un ejemplo de utilización de lnk-parser es el siguiente:

```
lnk_parser_cmd.exe -o listadoLNKs -w -s C:
```

[61] http://technet.microsoft.com/es-es/sysinternals/bb897441.aspx

6 RESUMEN

Como se ha indicado al principio del documento, el concepto de análisis forense digital hace referencia al conjunto de procedimientos de recopilación y análisis de evidencias que se realizan con el fin de responder a un incidente relacionado con la seguridad informática y que, en algunas ocasiones, pueden servir como pruebas ante un tribunal. Mediante este procedimiento se pretende responder a las siguientes preguntas: ¿qué?, ¿dónde?, ¿cuándo?, ¿por qué?, ¿quién? y ¿cómo?

Esta ciencia está adquiriendo un papel muy importante en los últimos años ya que cada día es más habitual tener que hacer frente a diferentes incidentes relacionados con la seguridad informática como por ejemplo: intrusiones, robos de información, infecciones, etc., y es por ello que su uso se está extendiendo por muy diversos campos.

Existen diferentes metodologías que se pueden seguir para realizar dicho proceso, si bien todas ellas se basan en aspectos bastante similares y tienen pautas y fases comunes. Una de las más destacadas, como se ha descrito y detallado en el documento, es el *RFC3227*. Entre los más aspectos más importantes que se deben tener en cuenta, y sobre el que hace un especial énfasis el *RFC3227,* es el orden de volatilidad de las evidencias, indicando que se deben recopilar en primer lugar aquellas que vayan a estar disponibles durante el menor período de tiempo

De forma genérica se obtienen el volcado de memoria y el volcado de disco, y a partir de ahí se trabaja sobre diferentes copias para obtener el resto de evidencias. Sin embargo, a la hora de realizar el proceso, es muy importante tener bien claro el tipo de incidente al que nos enfrentamos y a partir de él ver qué información es necesaria recopilar y la manera de proceder.

Finalmente, indicar que todo el proceso debe realizarse de manera muy rigurosa y meticulosa con el fin de mantener la integridad y validez del mismo.

7 GLOSARIO

- **Resiliencia:** En seguridad informática, es la capacidad de soportar y recuperarse de un incidente que afecte a la seguridad del sistema.
- ***Sniffer*:** Un *sniffer* es una utilidad que permite monitorizar y analizar el tráfico de una red.
- ***Offset*:** un offset dentro de un *array* u otra estructura de datos es un entero que indica la distancia (desplazamiento) desde el inicio del objeto hasta un punto o elemento dado.
- **Modo promiscuo**: permite monitorizar todo el tráfico que circula por la red independientemente de que el origen o destino sea el host que se está analizando.
- **%WinDir% o %SystemRoot%**: son variables de entorno que corresponden al directorio de instalación del sistema operativo, normalmente c:\Windows.
- **%SystemDrive%**: es la variable de entorno que corresponde a la unidad donde se ha instalado el sistema operativo, normalmente c:\
- **%UserProfile% o %HomePath%**: son variables de entorno que corresponden al directorio del usuario actualmente logueado en el sistema. `Normalmente c:\Document and settings\Nombre de Usuario` en Windows XP y `c:\Users\Nombre de Usuario` en Windows 7/8.

8 REFERENCIAS

[1] Using IOC (Indicators of Compromise) in Malware Forensics. Junio de 2012, disponible en https://www.sans.org/reading-room/whitepapers/incident/ioc-indicators-compromise-malware-forensics-34200.

[2] ANTI-CARTEL ENFORCEMENT MANUAL CARTEL WORKING GROUP Subgroup 2: Enforcement Techniques. Marzo de 2010, disponible en http://www.internationalcompetitionnetwork.org/uploads/library/doc627.pdf.

[3] Analysis of the incident handling six-step process. Octubre de 2012, disponible en http://www.giac.org/cissp-papers/17.pdf

[4] An introduction to the malware attribute enumeration and characterization white paper. Febrero de 2008, disponible en https://maec.mitre.org/about/docs/Introduction_to_MAEC_white_paper.pdf

[5] Auditando puertos USB y otros dispositivos. Registro de windows y software dedicado. Mayo de 2010, disponible en http://seguridadyredes.wordpress.com/2010/05/19/auditando-puertos-USB-y-otros-dispositivos-registro-de-windows-y-software-dedicado/

[6] Técnicas Anti-Forenses en Informática: Ingeniería Reversa Aplicada a TimeStomp. Septiembre de 2009, disponible en http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6(3).pdf

[7] Computer forensics: Evidence Collection & Preservation. Disponible en http://ictc.aeoi.org.ir/sites/default/files/Evidence_Collection_Preservation.pdf

[8] Análisis forense de sistemas informáticos. Agosto de 2009, disponible en http://webs.uvigo.es/jlrivas/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf

[9] Información del Registro de Windows para usuarios avanzados**.** Disponible en http://support.microsoft.com/kb/256986/es

[10] La informática forense, una herramienta para combatir la ciberdelincuencia. Diciembre de 2009 disponible en http://www.minseg.gob.ar/download/file/fid/893

[11] Digital Forensics with Open Source Tools. Marzo de 2011, disponible en http://www.amazon.es/Digital-Forensics-Open-Source-Tools-ebook/dp/B004W7DO78/ref=sr_1_1?ie=UTF8&qid=1410770257&sr=8-1&keywords=Digital+Forensics+with+Open+Source+Tools

[12] Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. Enero de 2011, disponible en http://www.amazon.es/Windows-Registry-Forensics-Advanced-Forensic-ebook/dp/B004JN0CDO/ref=sr_1_11?ie=UTF8&qid=1410770470&sr=8-11&keywords=Digital+Forensics

[13] The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Julio de 2014, disponible en http://www.amazon.es/Art-Memory-Forensics-Detecting-Malware-ebook/dp/B00JUUZSQC/ref=sr_1_6?ie=UTF8&qid=1410770470&sr=8-6&keywords=Digital+Forensics

ANEXO 1 – PERSONAS DE CONTACTO

Número de caso:

Tipo de incidente: _____

_____

_____

_____

_____

_____

Empresa afectada:

Dirección:

Teléfono:

Fecha y Hora: / / 20 :

Investigador:

Observaciones

_____

_____

_____

_____

_____

_____

_____

PERSONAS DE CONTACTO

Listado de personas

Número de caso:

Número de página

Nombre y Apellidos	Email	Teléfono	Cargo

Imprimir esta página las veces que sea necesario.

ANEXO 2 – CADENA DE CUSTODIA DE EVIDENCIAS

Número de caso:

Tipo de incidente: _____

_____

_____

_____

_____

_____

Empresa afectada:

Dirección:

Teléfono:

Fecha y Hora: / / 20 :

Investigador:

Observaciones

_____

_____

_____

_____

_____

_____

_____

CADENA DE CUSTODIA DE EVIDENCIAS

Listado de evidencias

Número de caso: | | | | | | | | | | |

Número de página | | | | | | | | | | |

Evidencia (Código)	Cantidad	Descripción del artículo (Marca, Modelo, Número de serie, estado, etc).

Imprimir esta página las veces que sea necesario

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS