
# Análisis forense en entorno Windows

Trabajo Fin de Máster

Presentado por José Javier León Marcos

Tutorizada por Marco Antonio Lozano Merino

# Índice

# Introducción

Los sistemas informáticos son, cada vez más, parte indispensable para las funciones de una empresa o un particular, y cada vez contienen más información personal de alto valor para un agente malicioso. Actualmente la información posee un valor por sí misma, y exigen diferentes formas de recopilar dicha información mediante ataques directos sobre los equipos que la contienen.

Aunque la prevención sigue siendo la mejor medida para reducir estas incidencias, es imposible protegerse del 100% de las amenazas, cuando día a día aparecen nuevas fallas de seguridad y vulnerabilidades, códigos maliciosos… Para estos casos, el análisis forense se vuelve crítico, ya que nos ofrece la posibilidad de recoger toda la información posible de dicha intromisión con el fin de tomar las medidas pertinentes y evitar un segundo ataque. Un correcto análisis puede indicarnos cómo hemos sido atacados, por qué (o quién), y cómo podemos evitar que ocurra de nuevo.

A día de hoy, Microsoft Windows, en sus diferentes versiones, representa una cuota de mercado superior al 85% de los equipos de escritorio[1,2], sobre todo en el entorno profesional. Esto significa que, aunque sólo sea por superficie de impacto, muchos de los ataques ejecutados actualmente son sobre estos sistemas operativos.

Diferentes tecnologías actuales ofrecen medios para conseguir información relativa a cada posible aspecto de un ataque como rastros en el sistema operativo, la memoria, conexiones de red, etc…

Nuestro objetivo en este trabajo es el de realizar y documentar una búsqueda de evidencias en sistemas Windows, de tal forma que se obtenga una recolección de pruebas en caso de un ataque.

Hay que reseñar que no estamos creando una metodología estándar de análisis forense cuya finalidad sea el rigor judicial, sino la máxima recolección de datos de tal forma que nos ayude a identificar, entender y protegernos en un futuro de dicho ataque.

Al final de este trabajo, habremos de conseguir todos los datos posibles de un equipo que ha sido atacado por un agente externo, y proveer un informe que ofrezca toda la información relativa a dicho incidente.

Un análisis forense es capaz de arrojar información de gran valor sobre qué acciones han sido llevadas a cabo en un equipo. Esto no incluye solamente una infección de un virus, sino si un usuario ha realizado actividades ilícitas desde él, o si han sido herramientas para la fuga de información por parte de un empleado, entre otras muchas posibilidades. En una definición amplia, podríamos decir que el análisis forense es una herramienta orientada a la extracción de información sobre hechos, que buscan dar solidez y base a un argumento. Ciertamente, esta información es prácticamente imposible de averiguar de forma veraz sin el uso de la ciencia forense, ya que esta se basa en acontecimientos objetivos para describir una historia, y no se ve alterada por la versión parcial de un individuo.

# Objetivos

El objetivo principal del TFM es el análisis de un equipo de escritorio Windows del cual se han de extraer todas las evidencias posibles tras un incidente de seguridad. Adicionalmente, requerimos los siguientes puntos para conseguir nuestro objetivo:

- Conocimiento de entornos Windows y su funcionamiento estándar
- Conocimiento de herramientas de evaluación y análisis forense

En un espectro más amplio, el objetivo de cualquier análisis forense de este tipo es la de indagar en el funcionamiento de un sistema informático y ser capaz de crear una línea temporal que nos indique si ha habido alguna acción que comprometiera dicho sistema. Para llevar esta tarea a buen puerto, el analista ha de usar cualquier herramienta que considere necesaria para obtener cualquier información relevante.

# Metodología

Para la recolección de datos se seguirán las etapas generales del análisis forense. Dichas etapas se pueden resumir en los siguientes puntos:

- Identificación de evidencias
- Adquisición de evidencias
- Análisis e investigación
- Informe y conclusión

Estos puntos clave son las fases estándar del análisis forense, y para seguirlas nos regiremos por los principios que podemos encontrar en diferentes metodologías bien aceptadas en los círculos de análisis forense, además de la bibliografía de la asignatura de Análisis Forense de este mismo Máster.

Las fases anteriormente citadas se corresponden con una base común de cualquier análisis forense informático. A pesar de que existen varios protocolos ampliamente conocidos (Modelo DFRWS, Casey, Modelo del Departamento de Justicia de EE.UU.…), todos ellos recogen de una forma u otra las acciones que hemos nombrado, por lo que asumimos que, a pesar de que las exigencias en algunos entornos puedan diferir en cierto rango, las bases son comunes para todos ellos.

Cada uno de estos apartados engloba diferentes tareas a realizar, que pormenorizaremos en el siguiente apartado.

# Tareas

Las fases que se llevarán a cabo son las siguientes, las cuáles van a ser desglosadas en las siguientes tareas:

Etapa 1: Identificación de evidencias

- Aseguramiento de la escena
- Identificación del sistema a analizar
- Identificar evidencias volátiles
- Identificar otros posibles medios que puedan contener información

Etapa 2: Adquisición de evidencias

- Realización de copia bit a bit
- Verificación de integridad de la copia
- Retención de tiempos y fechas
- Documentación de la cadena de custodia, si procede
- Protección y transporte de las evidencias, si procede

Etapa 3: Análisis e investigación

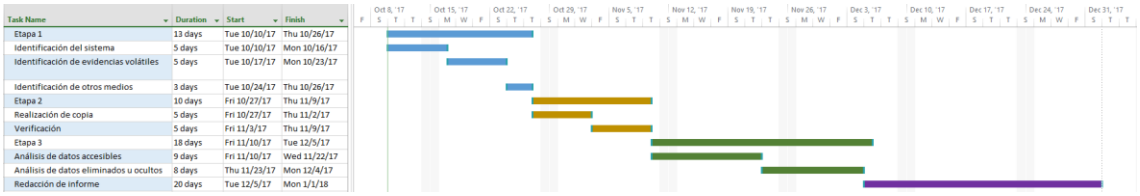
- Análisis de datos accesibles
- Análisis de datos eliminados u ocultos

Etapa 4: Informe y conclusión

Se procurará utilizar recomendaciones de diferentes organismos y normas, como de ISO, UNE, DOJ, NIST o el Instituto SANS

# Planificación

Cada tarea se ha identificado entre paréntesis por sus iniciales a fin de poder identificarlas en el diagrama de Gantt.



| Task Name | Duration | Start | Finish |
|---|---|---|---|
| Etapa 1 | 13 days | Tue 10/10/17 | Thu 10/26/17 |
| Identificación del sistema | 5 days | Tue 10/10/17 | Mon 10/16/17 |
| Identificación de evidencias volátiles | 5 days | Tue 10/17/17 | Mon 10/23/17 |
| Identificación de otros medios | 3 days | Tue 10/24/17 | Thu 10/26/17 |
| Etapa 2 | 10 days | Fri 10/27/17 | Thu 11/9/17 |
| Realización de copia | 5 days | Fri 10/27/17 | Thu 11/2/17 |
| Verificación | 5 days | Fri 11/3/17 | Thu 11/9/17 |
| Etapa 3 | 18 days | Fri 11/10/17 | Tue 12/5/17 |
| Análisis de datos accesibles | 9 days | Fri 11/10/17 | Wed 11/22/17 |
| Análisis de datos eliminados u ocultos | 8 days | Thu 11/23/17 | Mon 12/4/17 |
| Redacción de informe | 20 days | Tue 12/5/17 | Mon 1/1/18 |

## Ejecución

Como nombramos en apartados anteriores, seguiremos diferentes métodos de recolección de datos, condicionados mayormente en las evidencias que nos proponemos extraer. Esto significa que a lo largo del proceso se variará entre diferentes herramientas, métodos de extracción y recomendaciones o estándares.

Haremos uso de entornos virtualizados, ya sea en entornos VMWare o Virtual Box, en los que se simulará el equipo comprometido, sobre los que se ejecutarán herramientas y distribuciones como SIFT de Sans, Bugtrack o Kali.

## Estado del arte

A pesar de que muchas organizaciones de carácter nacional e internacional están trabajando en metodologías de análisis forense, actualmente no se cuenta con ningún procedimiento oficial y universal que nos pueda guiar en este arduo trabajo. La amplitud de posibilidades, así como las legislaciones locales, hacen que sea complicado guiar todos los trabajos de recolección de tal manera que sean aceptados en cualquier lugar y circunstancias.

Aun así, importantes organismos como IETF, ISO o AENOR han detallado parte del proceso dentro de sus estándares, que han de hacer de base para un análisis exhaustivo de cualquier sistema que haya sido comprometido.

En el ámbito no gubernamental, existen también organizaciones interesadas en el análisis forense que procuran arrojar algo de luz sobre esta actividad. Dichas organizaciones están encabezadas por el instituto SANS (SysAdmin Audit, Networking and Security) o Digital Forensics Workshop (DFRWS).

A continuación haremos una breve introducción sobre los aportes de cada uno de los citados:

- IETF: Internet Engineering Task Force aporta su *RFC 3227: Directrices para la recopilación de evidencias y su almacenamiento*, 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.

- ISO: Dentro de la norma ISO 27000 se recogen los estándares de seguridad de los sistemas de información. Dentro de la familia *27K* tenemos dos normas relacionadas con el análisis forense. El estándar *27037: Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas* se nos indican las fases que se debe seguir para el correcto análisis forense. En el estándar *27050: Electronic discovery* la norma hace hincapié en aspectos relacionados con el análisis forense, aunque actualmente sólo se encuentra publicado su primer apartado, encontrándose los demás en fase de desarrollo o aprobación.
- AENOR: La Asociación Española de Normalización han lanzado dos guías relacionadas con el análisis forense. Tanto la *UNE 71505: Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE)* como la *UNE 71506: Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas* tratan de añadir su grano de arena en cuanto a análisis forense se trata.
- NCJRS: A pesar de que no se trata de un organismo internacional, el Departamento de Justicia de los EE.UU. también ejerce como estándar de facto para el análisis de recursos informáticos. Su *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* es material recomendado por muchos medios especializados.
- SANS: El instituto SANS ofrece un abanico de documentación y formación en el ámbito de la ciberseguridad y el análisis forense en su departamento SANS DFIR (Digital Forensics and Incident Response) incluso ofrecen una distribución Linux especialmente orientada al análisis forense.
- DFRWS: Esta comunidad ofrece un amplio espectro de información y recursos donde extraer información, aunque la carencia de un procedimiento completo deja en manos del auditor, y de su capacidad, que el resultado sea satisfactorio.
- INCIBE: Basado en el estándar RFC 3227, Asier Martínez Retenaga propone una metodología a través del Instituto Nacional de Ciberseguridad. *Guía de Toma de Evidencias en Entornos Windows* fue presentado en noviembre de 2014, recogiendo un procedimiento centrado sobre todo en orden de volatilidad, que procura asegurar la toma de datos de forma segura y objetiva.

## Herramientas para el análisis

Actualmente disponemos de una gran variedad de herramientas con las que realizar un estudio forense. Tanto aquellas de código abierto como propietario, es importante que el analista encuentre un set de herramientas con el que se sienta cómodo, y a su vez abarque lo máximo posible el espectro de información que pueda recolectar. Con esta finalidad, haremos un listado de herramientas conocidas, organizándolas por su objetivo principal. Esta lista no es excluyente, ya que aún siguen existiendo muchas más posibilidades que no hemos recogido aquí y son ampliamente utilizada de igual modo.

Debemos tener en cuenta que el propio sistema operativo Windows nos puede dar parte de la información que queremos, pero dado que el sistema está comprometido, no siempre nos podemos fiar de la información que nos muestra, y por ello es especialmente interesante utilizar softwares "objetivos".

## Distribuciones completas

- CAINE: acrónimo de Computer Aided Investigative Environment es una Distribución GNU/Linux original de Italia creada como un Proyecto de Forense Digital. CAINE Ofrece un entorno Linux completo, integrando herramientas de software existentes y con una interfaz gráfica amigable.
- DEFT: Digital Evidence & Forensics Toolkit es una distribución creada para el análisis forense que tiene como objetivo de ser ejecutado de tal manera que asegure la integridad y la no modificación de los elementos estudiados. Incluye la suite DART (Digital Advanced Response Toolkit)
- SIFT: SANS Investigative Forensic Tool es un grupo de herramientas forenses de código abierto que permiten realizar un detallado análisis sobre diferentes sistemas. Su objetivo es demostrar que se puede realizar un análisis forense basándose en herramientas open-source.
- Helix: Esta distribución de e-fense se compone de diferentes suites (Enterprise, pro, live response…) para redes, sistemas, o análisis forense.

Además de las citadas, tenemos muchas otras distribuciones con herramientas forenses como Kali, Digital Forensics Framework, The Sleuth Kit y AutoPsy, o Forensic and Incident Response Environment, todas ellas basadas en Linux, con herramientas que se pueden utilizar para diversos sistemas operativos.

## Análisis de memoria

- DumpIt
- Volatility
- AccessData FTK Imager
- Pd – Process Dumper
- RedLine
- Memorize

## Procesos y servicios

- Tasklist
- PSlist / PSservice
- Volatility

- CurrProcess

## Usuarios de sistema

- Netusers
- PSLoggedon
- LogonSessions

## Análisis de red

- Wireshark
- Snort
- Nmap
- Xplico
- TCPDump
- Windump

## Volcado de disco

- Dd (Linux)
- WinDD
- FTK Imager
- CloneZilla

## Ficheros de sistema

- MBRUtil
- NTFSWalk
- AnalyzeMFT
- MFT tolos
- Prefecth Parser

## Análisis de Malware

- OllyDbg
- Radare
- Volatility Framework con plugins malfind2 y apihooks

# Fase I: Identificación de evidencias

La identificación y preservación de las evidencias es un proceso crítico en la elaboración de un análisis forense. Como primer paso de todo el proceso, resulta crucial que se lleve a cabo con el máximo cuidado, ya que una incorrecta ejecución podría desembocar en la desconsideración o eliminación de una prueba. En la metodología que estamos siguiendo, podríamos definir la identificación como aquellas acciones que garantizan que no se pierdan las evidencias del sistema, además de dotar de información básica sobre las condiciones en las que se encuentra el objetivo del estudio.

En casos genéricos, se vuelve imprescindible asegurar el entorno físico para evitar la posible modificación de evidencias o perdida de las mismas debido a agentes externos, como conexiones de red remotas, golpes que puedan dañar el contenido del disco duro, apagados inesperados o cualquier otro incidente.

Dada la delicadeza de esta fase, debemos tener en cuenta una serie de condiciones que debemos tener en cuenta si queremos que las pruebas sigan teniendo validez cuando nos dispongamos a realizar el análisis:

- No se debe modificar el estado en el que se han encontrado los equipos
- Se comenzará identificando físicamente cada dispositivo, tomando fotografías si fuera necesario para su posterior inclusión en un inventario
- Se asegurará la cadena de custodia de dichos elementos. Se ha de tener un registro de interacciones de cada prueba

Ciertos soportes son más delicados que otros, como dispositivos magnéticos u ópticos. Estas evidencias merecen un tipo de tratamiento especial y deben ser protegidas de campos electromagnéticos o aumentos de tensión que pudieran inhabilitarlo.

## Seguridad física

Como se indicó anteriormente, la seguridad física de la zona a estudiar se vuelve primordial. El analista o grupo de analistas debe poder asegurar la no interferencia de agentes externos sobre el equipamiento a estudiar. Esto significa que cada acción llevada a cabo sobre los sujetos debe estar debidamente documentada y realizada por personal aprobado para dicha finalidad.

Resulta de especial ayuda la documentación gráfica del entorno a analizar. El estado del material, el conexionado… De tal manera que, si fuera necesario, este estado se pueda restaurar en un entorno de pruebas, o por parte de otro analista que deba corroborar nuestros hallazgos. También resulta especialmente útil en este aspecto el etiquetado de los periféricos y demás elementos que interactúen con el equipo, como impresoras, teléfonos IP o cualquier conexión USB como smartphones, discos duros externos…

Por otra parte, para casos de índole judicial, y con el fin de alterar lo menos posible el entorno, se recomienda utilizar medios como guantes de látex para evitar la destrucción de huellas dactilares.

Otro punto importante, una vez que los pasos anteriores han sido llevados a cabo, es comprobar si el sistema muestra algún mensaje que nos pueda ofrecer información, esto sin interferir en su funcionamiento, ya que esta evidencia podría ser volátil y su toma (mediante una fotografía o vídeo) puede ser valiosa más tarde.

## Cadena de custodia

En lo referente a la cadena de custodia, su ejecución puede hacer que se acepte o desestime un hallazgo, no sólo ante un tribunal, sino incluso cuando realizamos un análisis de finalidad privada.

Debido a esto, es importante que, siempre que sea posible, se documenten los agentes que interfieren en la manipulación de las evidencias, así como su actividad con ellas. En un registro de cadena de custodia se debería registrar, al menos, la identificación de la evidencia en cuestión, relación de agentes que han interactuado con ella, la acción en sí (acceso, modificación, borrado…), y el marco temporal en el que se han llevado a cabo dichas acciones, indicando el inicio y el final de las mismas. Esto incluye, por supuesto, el traslado de las evidencias, correspondiendo el mismo nivel de detalle.

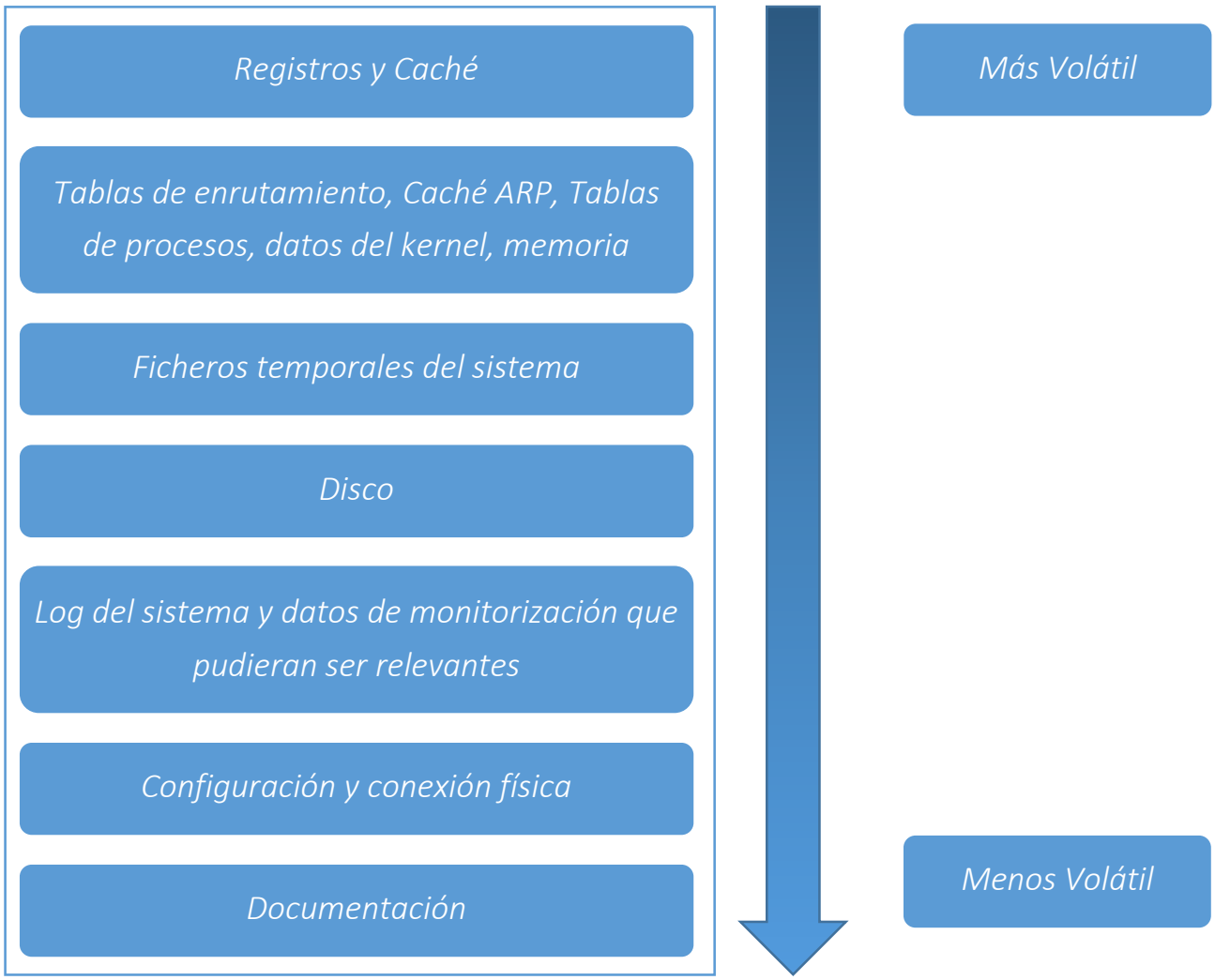
De cara a saber si la cadena ha sido alterada, es recomendable que se documente su estado en el momento de la recolección de información y se compare en el momento del análisis. Esto puede ser llevado a cabo mediante soportes visuales tales como fotografías y video en las evidencias físicas, o mediante valores hash para pruebas virtuales, por ejemplo.

## Identificación de evidencias

En este punto el analista se encuentra ante la primera gran dicotomía. ¿Se debe detener el sistema a analizar, apagarlo ordenadamente, desconectarlo, dejarlo tal y como está? Esta respuesta nunca es sencilla, y ante todo se debe tener en cuenta una serie de factores que son intrínsecos a cada caso. No se puede generalizar una acción, y recaerá sobre el analista la decisión final de si apagar el equipo tan pronto llegamos a él (desconectándolo de la corriente o similar) o si es más valioso intentar obtener las evidencias volátiles a las que nos sería imposible llegar estando apagado.

En lo referente a las evidencias contenidas dentro del sistema a analizar, podemos hacer una diferenciación importante en cuanto a la persistencia de los datos. Por un lado, tenemos los datos no volátiles, que son aquellos contenidos en el disco duro y que no dependen de que el equipo se encuentre en funcionamiento para encontrarlos. Estas evidencias se pueden se pueden analizar mediante herramientas forenses “offline”, lo cual nos permitirá trabajar en un entorno más seguro mediante copias de datos. Por otra parte, contamos con las evidencias volátiles, aquellas que pueden ser modificadas, eliminadas o inaccesibles una vez que el equipo deje de funcionar.

De acuerdo con el RFC 3227, apartado 2.1, el siguiente es un ejemplo clásico de orden por volatilidad:




Mención especial merecen los ficheros de hibernación y paginación (hiberfil.sys y pagefile.sys). Estos equipos conforman un formato especial de memoria, y nos podrían permitir realizar análisis de la memoria incluso cuando el equipo está apagado. El fichero de hibernación contiene una "fotografía" de la memoria RAM la última vez que el equipo cambio su estado a hibernación. Dependiendo de la distancia temporal con este evento, podría ofrecernos una imagen sobre la memoria volátil relativamente actualizada. Con respecto al fichero de paginación, este es un reservado de memoria dónde la RAM vuelca aquellos datos que sobrepasan su capacidad, de tal manera que aquellos datos que la memoria volátil no puede manejar, se pasan al disco duro. Para obtener datos de este fichero debemos hacerlo con el ordenador encendido, o después de un apagado no controlado.

## Almacenamiento de evidencias

Aunque este apartado está estrechamente relacionado con la cadena de custodia, merece hacer una reseña especial en cuanto a la seguridad física de los mismos.

Al ser elementos tan sensibles, el almacenamiento de estas debe ser en un lugar cuyas condiciones no puedan dañar en ningún sentido las evidencias. Se debe procurar que las temperaturas sean estables y cerca de la temperatura óptima para la electrónica (unos 21º-25º), que entorno tenga baja humedad y carente en la medida de lo posible de grandes flujos de polvo o campos electromagnéticos. Para más información acerca de estas condiciones, podemos consultar la norma ISO 17799:2005.

Por razones obvias, el acceso a estos almacenes debe estar de acuerdo con las mismas exigencias de las que hablamos en el apartado de la cadena de custodia.

La retención de estas evidencias debe asegurarse, al menos, durante todo el tiempo que dure la investigación sobre la misma. Además, si por alguna razón esta información fuera utilizada en procesos legales, la retención debe alargarse durante todo el tiempo que estime la legislación local en este sentido.

## Consideraciones Legales

Los diferentes ámbitos legales en los que se puede enmarcar una actividad objeto de análisis puede dificultar la correcta ejecución de las mismas, ya que las exigencias por parte de los organismos judiciales pueden variar de un punto a otro.

Aun así, para poder utilizar cualquier resultado hallado durante el análisis, es indispensable que se demuestre la no alteración delas mismas, y que las acciones han sido realizadas en base al principio de protección y preservación, mediante una cadena de custodia estricta y documentada.

# Fase II: Adquisición de evidencias

En esta fase llevaremos a uso todas las consideraciones y conocimientos que hemos citado en los anteriores apartados.

La recolección de evidencias es un proceso que debe ser ejecutado lo más sistemáticamente posible, reduciendo el número de variables y decisiones no previstas. Aseguraremos que el proceso de toma de datos sea comprobable mediante la repetición de las pruebas que llevemos a cabo, por lo que cada paso debe ser descrito detalladamente.

De acuerdo a la tabla de volatilidad que vimos anteriormente, seguiremos un procedimiento que procure el máximo posible de evidencias tras el estudio.

1. Volcado de registros y caché
2. Volcado del estado de red
3. Volcado de memoria del equipo
4. Volcado de ficheros de paginación e hibernación
5. Copiado bit a bit del disco
6. Estudio del sistema de ficheros

De cada uno de estos pasos, es importante tener registros temporales que indiquen cuando ha sido llevado a cabo la toma de evidencias, de tal manera que nos permita esbozar una línea temporal de cada acción ejecutada sobre el sistema. También es importante evitar la modificación del sistema, procurando no hacer uso de software que modifique las tablas MAC de los ficheros.

# Fase III: Análisis de evidencias

En esta fase llevaremos a cabo un estudio pormenorizado de los hallazgos de la etapa anterior. Es durante el análisis que el responsable del caso identificara aquellos comportamientos, conexiones, ficheros y demás aspectos que puedan ser susceptibles de un uso malintencionado.

Para esto, el analista puede hacer uso de las herramientas que crea conveniente, así como de referencias externas, siempre y cuando no se altere el estado inicial de las pruebas.

Toda la información relevante debe ser recogida y categorizada de tal forma que se pueda añadir posteriormente al informe de manera comprensible y clara.

# Fase IV: Informe

Como fin último del análisis, encontramos el informe. En este apartado el analista volcará los hallazgos encontrados durante la fase de análisis, y ejecutara un veredicto sobre los hallazgos encontrados. El objetivo de esta conclusión no es la de "juzgar" los hechos, sino la de presentar una línea de acontecimientos que desembocaran en los resultados que se han visto en el equipo comprometido.

En muchos casos este informe ha de ser presentado a personal de carácter menos técnico, por lo que debe utilizar un lenguaje sencillo y con claridad en la presentación de las pruebas, sin dar por supuesto ningún conocimiento especializado en el análisis forense.

# Caso Práctico

## Identificación del sistema

Para la ejecución de este estudio, se ha decidido utilizar un entorno virtual ejecutado sobre VMWare Workstation 12. Esto nos aporta un entorno controlado y fácilmente recuperable en caso de desastre mediante el uso de snapshots.

El equipo a analizar se trata de una máquina virtual Windows 10 Enterprise, Build 16299.rs3. Esta imagen se ha obtenido del entorno de desarrolladores de Microsoft, que ofrece imágenes para pruebas por tiempo limitado. Con el fin de identificar totalmente el equipo, se muestra una tabla con los datos más significativos del mismo:

| | |
|---|---|
| Fabricante | VMWare |
| UUID | 56 4d ba ad 2f 68 be b8-db 25 49 4b a4 2b 63 41 |
| Procesador | 2 x Intel(R) Core(TM) i7-2670QM CPU @ 2.20GHz |
| Memoria | 4 GB |
| Nombre de equipo | MSEDGEWIN10 |
| Almacenamiento | VMWare Virtual S SCSI Disk, 40 GB |
| Sistema Operativo | Windows 10 Enterprise Build 16299.rs3 |
| Dirección MAC | 00:0C:29:2B:63:41 |
| Dirección IP | 192.168.86.128 |

En estas condiciones, el aseguramiento de la escena se puede resumir en limitar el alcance de red del equipo, de cara a evitar el despliegue de la amenaza a través de la red. Por otro lado, el hecho de no desconectar la red totalmente nos permitirá realizar un escáner del tráfico de red originado por el dispositivo, lo que podría ayudarnos a identificarlo y analizarlo.

Para este caso concreto carecemos de procedimiento de aseguramiento de la escena física, ya que el entorno es totalmente virtual, y el equipo a analizar se encuentra alojado en el equipo que va a realizar el análisis.

Dado que estamos analizando un equipo virtual en un entorno aislado, no suponemos dispositivos adicionales que puedan añadir información al análisis, ya que no se han conectado dispositivos de almacenamiento USB, unidades de red o discos adicionales.

El planteamiento que llevaremos a cabo de aquí en adelante es el de un sistema en caja negra, en el que se nos ha reportado una posible amenaza, pero desconocemos cuál o de que tipo. La única información con la que contamos es que se ha abierto un fichero aparentemente PDF desde una ubicación no especificada.

# Identificación de evidencias volátiles

El primer paso de todo análisis forense debe ser, en la medida de lo posible, la recolección de evidencias volátiles. Estas evidencias poseen la particularidad de que su disponibilidad es temporal, y normalmente es eliminada tras el apagado del sistema. A continuación, listaremos una serie de estas evidencias que nos ayudarán a completar el análisis.

Como ya sabemos, la información que arroje el sistema no es siempre confiable, por lo que será bueno la comparación con valores externos de referencia, que nos sirvan para saber si estos datos son ciertos o no. Un ejemplo ilustrativo de estos es la fecha del sistema local. Aunque nos sirva para tener una referencia del tiempo transcurrido durante el análisis, o un hándicap que deba ser considerado en las tablas MAC de los ficheros.

Para la comprobación de la integridad de ficheros utilizaremos un hash en algoritmo SHA-512, debido a que MD5 y SHA-1 podrían presentar colisiones.

## *Hora y fecha del sistema*

Usaremos esta primera información para dar inicio a la línea temporal que vertebrará el análisis.

Mediante herramientas propias del sistema infectado haremos que muestre y vuelque en un fichero local la información. En este caso usaremos la suite Powershell, que forma parte del sistema operativo, y ejecutaremos la siguiente orden:

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

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.

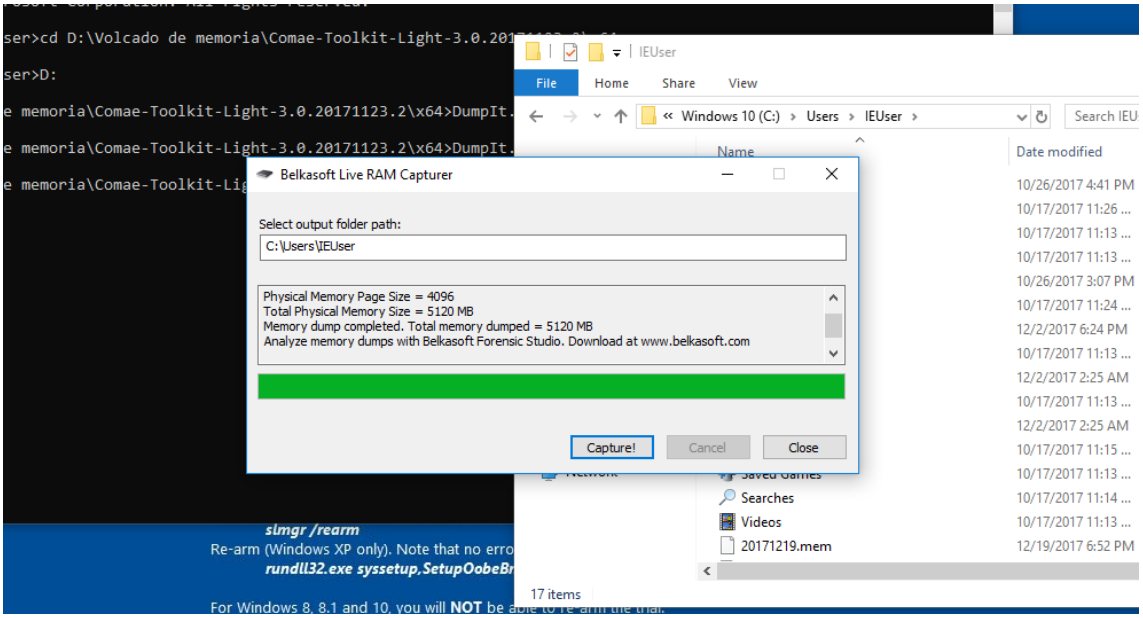
## *Volcado de la memoria*

Este paso puede ser el más delicado de todo el análisis. Normalmente el análisis de la memoria arrojará información relacionada con la mayoría de los malware. En la memoria se almacenan datos de diversas fuentes, como las conexiones establecidas, los procesos, etc… Por lo que en ella se puede encontrar cualquier proceso o instrucción de memoria que este “oculta” al usuario.

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.

En este caso vamos a utilizar la herramienta Belkasoft Live RAM Capturer. Esta aplicación no es posiblemente tan conocida como DumpIt, aunque ofrece una interfaz gráfica simple e intuitiva.




El fichero resultante se denominará 20171219.mem, y su hash SHA-512
55FD6DBBE4050647E2970BD4271E110173B01217805AC359EBF58874AB4ADC107312005544ABCC49B2487F3DBBCF23A11E99AB479C720722A9C01DEF95C735F6

Aparte de la memoria física del sistema, también es de gran interés obtener la memoria virtual, lo que requiere adquirir el fichero de paginación pagefile.sys. Este fichero se encuentra por lo general protegido por el sistema, y dado que obtendremos una imagen completa del sistema en próximas actividades, no hay necesidad de realizar la copia expresa.

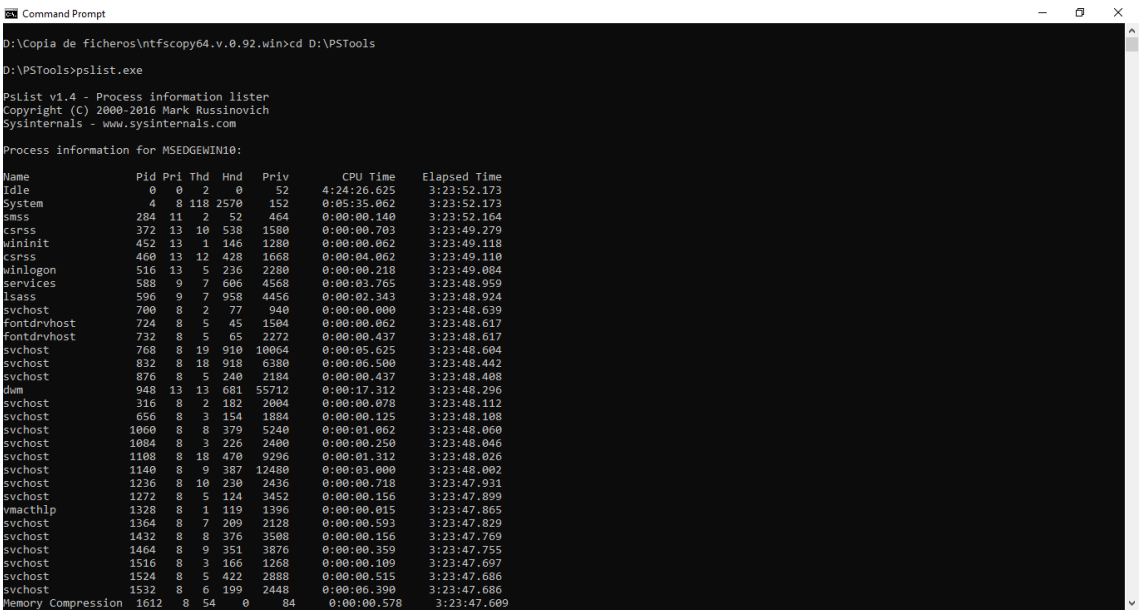
## *Procesos*

El estudio de los procesos nos indicará qué acciones está llevando el equipo en el momento de la extracción. Esto nos puede dar una idea de si hay alguna actividad fuera de lo común ejecutándose en un momento dado.

Para la extracción de los procesos en uso, podemos hacerlo mediante la tarea Volatility, a partir de la imagen de memoria que hemos extraído en el apartado anterior, y también mediante

herramientas específicas para este fin. Dado que este ejercicio tiene una función educativa, realizaremos también este paso por separado.

En este caso haremos uso de una de las herramientas de la suite SysInternals, PSList, y volcaremos dicho resultado a un fichero de texto para su posterior comprobación.

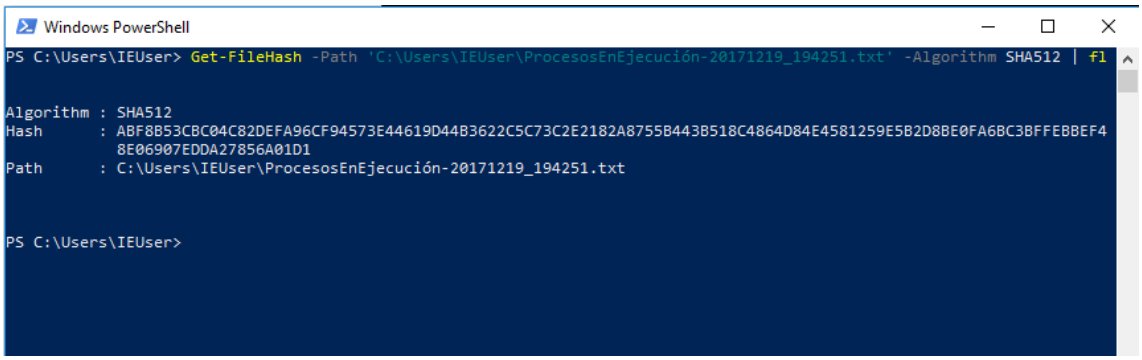



Podemos ver una gran variedad de procesos, utilizaremos la orden de volcado mediante

PSList64.exe > “C:\Users\IEUser\ProcesosEnEjecución-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

El nombre del fichero resultante será ProcesosEnEjecución-20171219_194251.txt y el hash de dicho fichero es

ABF8B53CBC04C82DEFA96CF94573E44619D44B3622C5C73C2E2182A8755B443B518C4864D84E4581259E5B2D8BE0FA6BC3BFFEBBEF48E06907EDDA27856A01D1



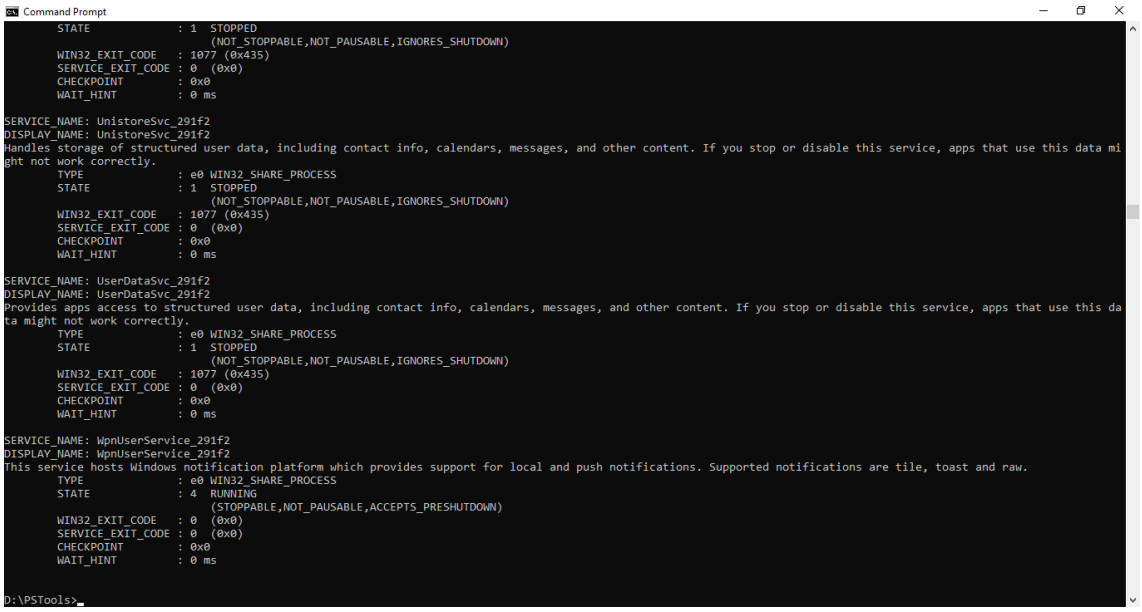
## *Servicios*

Windows utiliza los servicios como componentes del sistema que inician una acción concreta sobre el mismo. En algunos casos, esta lista puede darnos información sobre aplicaciones instaladas, procesos recurrentes… además de relacionarlos con el componente (ejecutable) que inician.

Continuando con las acciones del caso anterior, extraeremos la información de los servicios en ejecución actualmente.

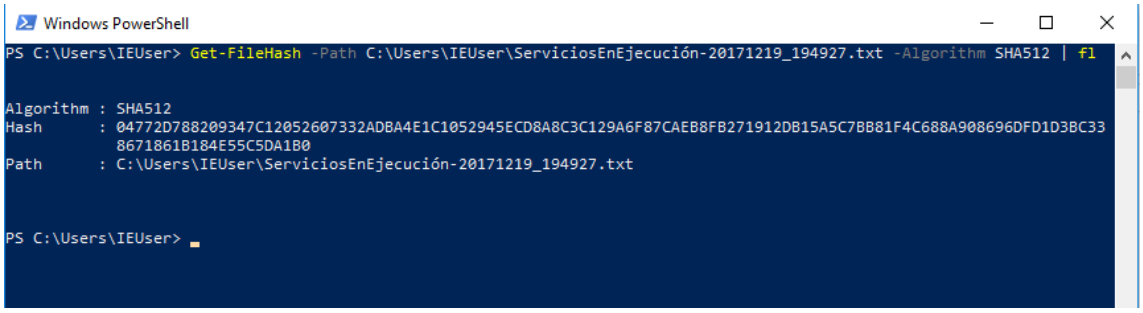
Para ejecutar esta utilidad, debemos iniciar la consola de Windows como administrador y utilizaremos la orden de volcado siguiente

PSService64.exe > "C:\Users\IEUser\ServiciosEnEjecución-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"




El nombre del fichero resultante será ServiciosEnEjecución-20171219_194927.txt y el hash de dicho fichero es

04772D788209347C12052607332ADBA4E1C1052945ECD8A8C3C129A6F87CAEB8FB271912DB15A5C7BB81F4C688A908696DFD1D3BC338671861B184E55C5DA1B0




## *Usuarios*

En algunos casos, ciertos ataques pueden crear cuentas con privilegios de administrador sin el conocimiento del usuario con el fin de tener control sobre la maquina incluso si el usuario no ha iniciado su sesión, como en los sistemas Command & Control (C2).

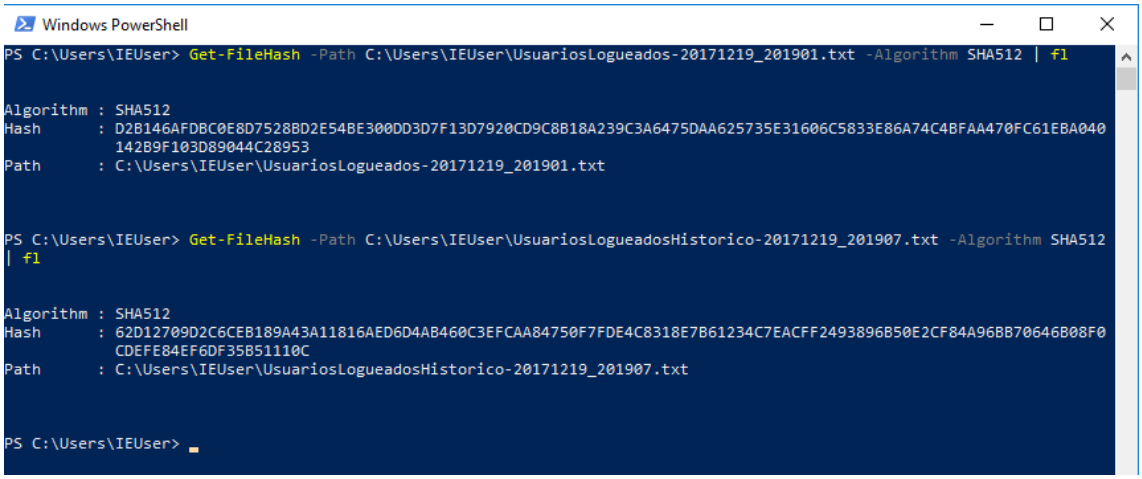
Por otra parte, puede sernos de utilidad saber qué usuarios están actualmente con la sesión iniciada en el sistema, así como aquellos que alguna vez lo hayan hecho. Un malware puede estar haciendo uso de una cuenta creada específicamente para su uso fraudulento, y esta información puede ser de utilidad.

En esta ocasión utilizaremos la aplicación PSLoggedOn, especialmente diseñado para este fin. Usaremos las siguientes órdenes para extraer dicha información.

PSLoggedon.exe > “C:\Users\IEUser\UsuariosLogueados-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"


A continuación, podremos ver el fichero con su nombre final y su valor hash SHA-512:

UsuariosLogueados-20171219_204902.txt con un hash
D2B146AFDBC0E8D7528BD2E54BE300DD3D7F13D7920CD9C8B18A239C3A6475DAA625735E31606C5833E86A74C4BFAA470FC61EBA040142B9F103D89044C28953

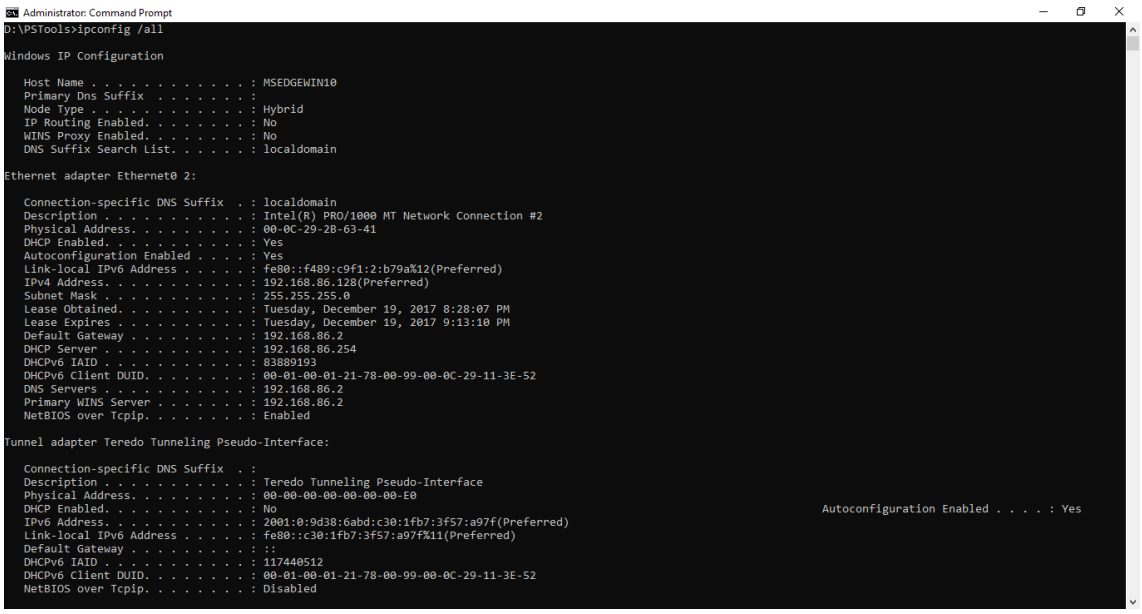



## *Estado de la red*

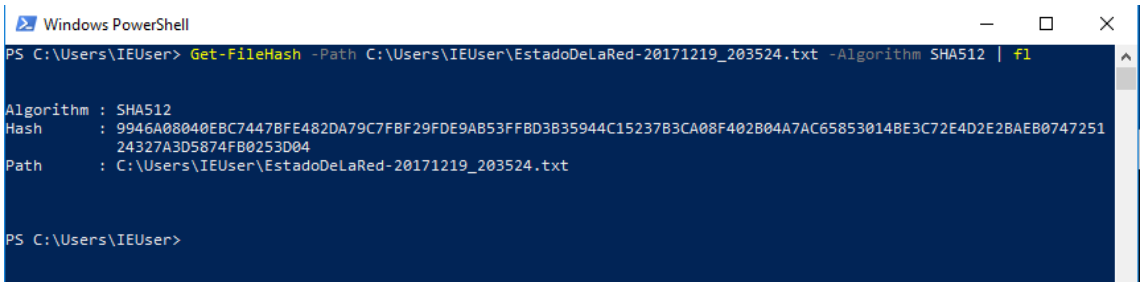
En este paso determinaremos el estado de la red, intentando localizar cualquier comunicación que nos pueda dar una idea de cuál es la amenaza que estamos enfrentando.

Lo primero, y más básico, será identificar nuestro equipo, mediante su dirección IP y lista de interfaces de red. Para esto haremos uso de la utilidad embebida de Windows ipconfig, mediante la siguiente orden

Ipconfig /all > C:\Users\IEUser\EstadoDeLaRed-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt



El resultado será el fichero EstadoDeLaRed-20171219_203524.txt con valor hash
9946A08040EBC7447BFE482DA79C7FBF29FDE9AB53FFBD3B35944C15237B3CA08F402B04A7AC65853014BE3C72E4D2E2BAEB074725124327A3D5874FB0253D04



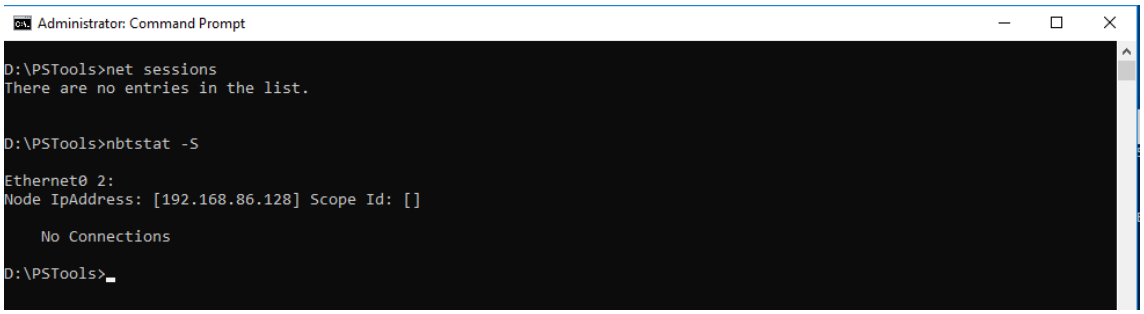

## *Conexiones establecidas*

Podemos generalizar en que la utilidad final de muchos malware pasa por extraer información, o al menos en recibir órdenes de control por parte de un centro de mando. En estos casos, las conexiones de red pueden indicarnos una actividad oculta por parte del equipo a estudiar. También nos indicará si tenemos alguna puerta trasera esperando a ser utilizada para acceder al sistema.

En este caso detectaremos las conexiones establecidas a nivel de NetBIOS, un protocolo Windows para detectar equipos en la red local. Con esta utilidad comprobaremos qué otros equipos están dentro de su radio de acción, y si se han buscado otros objetivos en la red

Nbtstat -S > C:\Users\IEUser\ConexionesNetBIOS-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt

Net sessions > C:\Users\IEUser\SesionesRemotas-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt




Los ficheros resultantes serán los siguientes

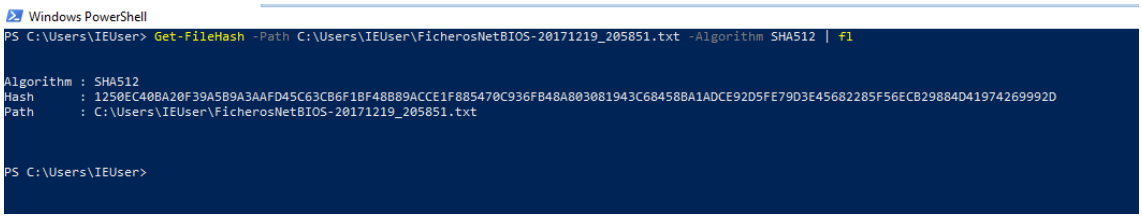
ConexionesNetBIOS-20171219_205409.txt con un hash
A30E8E803223B17249DEAB676EE0DFE782B37C2BED90AE3A7CB892D8C7454EEA19EE9CA0547BD5DF63865D5255A6AAE07F0587D602B6896E9E1E92830F54DBBB

SesionesRemotas-20171219_205409.txt con un hash
1250EC40BA20F39A5B9A3AAFD45C63CB6F1BF48B89ACCE1F885470C936FB48A803081943C68458BA1ADCE92D5FE79D3E45682285F56ECB29884D41974269992D

NetBIOS también cuenta con una tabla de ficheros transferidos por este protocolo, que podría ser útil si queremos trazar un posible esparcimiento de la amenaza. Aunque en este caso sabemos que no ha habido ninguna conexión aparente, realizaremos el estudio igualmente.

Net file > C:\Users\IEUser\FicherosNetBIOS-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt


El volcado de esta información se encontrará en el fichero FicherosNetBIOS-20171219_205851.txt con hash
1250EC40BA20F39A5B9A3AAFD45C63CB6F1BF48B89ACCE1F885470C936FB48A803081943C68458BA1ADCE92D5FE79D3E45682285F56ECB29884D41974269992D

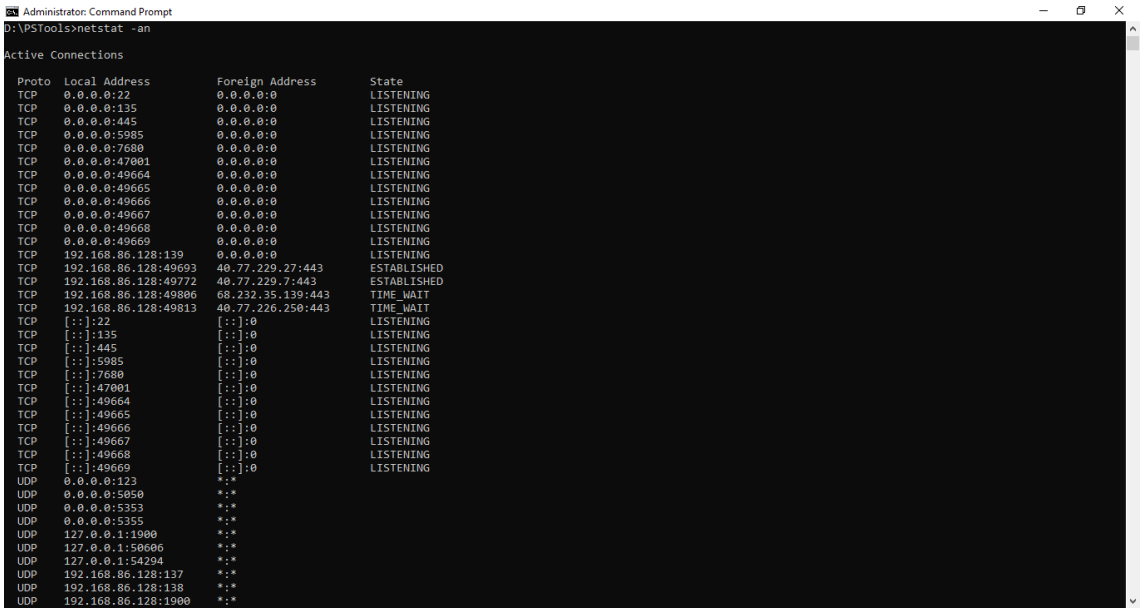



## *Conexiones activas y puertos abiertos*

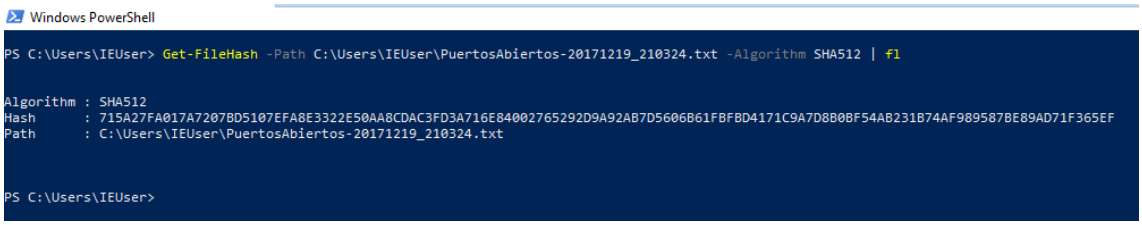
Siguiendo los principios del estudio anterior, buscaremos indicios de puertos en escucha fuera de lo común, que podría estar a la de un “knock-code” o acceso remoto malintencionado.

Seguiremos haciendo uso del comando netstat, y de las herramientas internas del sistema para identificar los puertos abiertos del equipo

netstat -an |findstr /i "state listening established" > C:\Users\IEUser\PuertosAbiertos-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt




Esta información y la que no se incluyó en la captura se encuentran en el fichero PuertosAbiertos-20171219_210324.txt con hash 715A27FA017A7207BD5107EFA8E3322E50AA8CDAC3FD3A716E84002765292D9A92AB7D5606B61FBFBD4171C9A7D8B0BF54AB231B74AF989587BE89AD71F365EF




## *Caché DNS*

En la caché DNS se puede visualizar dicha asociación con respecto a los dominios a los que se ha accedido desde el equipo. Una aplicación malintencionada que utilice un nombre de dominio como objetivo podría guardar en este caché su par nombre-dirección, lo cuál podría ayudarnos para bloquear cualquier comunicación a dicho dominio. Para obtener el listado se puede utilizar el comando ipconfig.

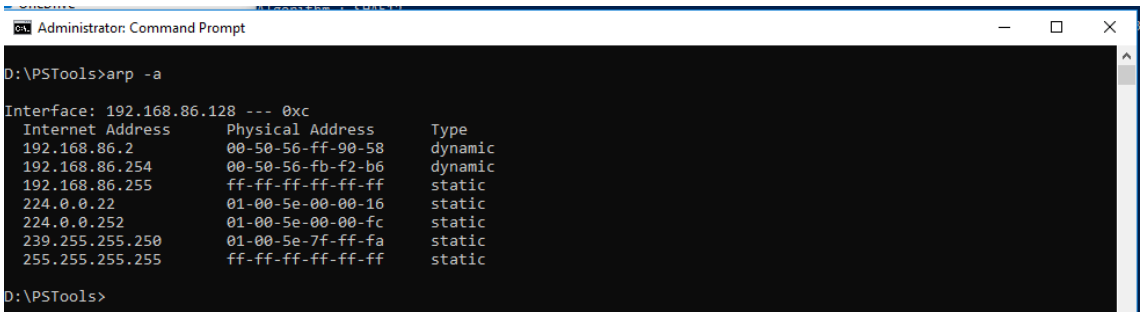
Ipconfig /displaydns > C:\Users\IEUser\DNSCache-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt


A pesar de que actualmente la caché se encuentra vacío, el fichero informe se encuentra igualmente con el nombre DNSCache-20171219_212936.txt, con un hash DE258C2DEF8DD9661FBDA1ECFE5EA66AF0BCED9945154AADDD91CA0DFBA5F400E182646195864C4D1E79D6F6530A7442309D0454BCCAC064C2613528165249EE

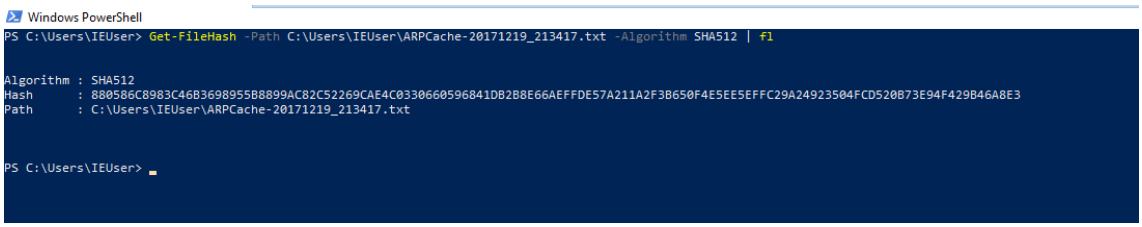
## *Caché ARP*

De modo similar a como hemos hecho con el caché DNS, podemos hacer un proceso similar para investigar la tabla ARP, que contiene la relación entre IP y MAC que el equipo conoce.

arp -a > C:\Users\IEUser\ARPCache-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt




Esta tabla se encuentra contenida en el fichero ARPCache-20171219_213417.txt, con un hash 880586C8983C46B3698955B8899AC82C52269CAE4C0330660596841DB2B8E66AEFFDE57A211A2F3B650F4E5EE5EFFC29A24923504FCD520B73E94F429B46A8E3




Llegados a este punto desconectaremos el equipo de la red con el fin de minimizar la fuga de información.

## *Contraseñas*

Otra de las particularidades que pueden ser interesantes es comprobar las contraseñas almacenadas en el equipo para recursos de red. En esos casos podemos saber si una contraseña ha sido comprometida, y por lo tanto debemos cambiarla. En nuestro caso práctico carecemos de contraseñas de red, web o correo, ya que la imagen se ha instalado de cero.

## *Registros y autoejecutables*

El registro de Windows es una importante herramienta del sistema. Podríamos decir que todo lo que está configurado en el equipo tiene una entrada de registro asociada. Desde la aplicación que ejecuta cierto tipo de fichero a las tareas iniciales de Windows, esta relación de llaves y valores puede describir con lujo de detalles el comportamiento del sistema operativo.

A pesar de que los ficheros de registro no son necesariamente volátiles, ya que normalmente son accesibles desde una imagen forense para su posterior análisis, utilizaremos algunas herramientas que nos puedan añadir información adicional al ser ejecutadas sobre el sistema "vivo", y que principalmente hacen uso del registro para extraer información.

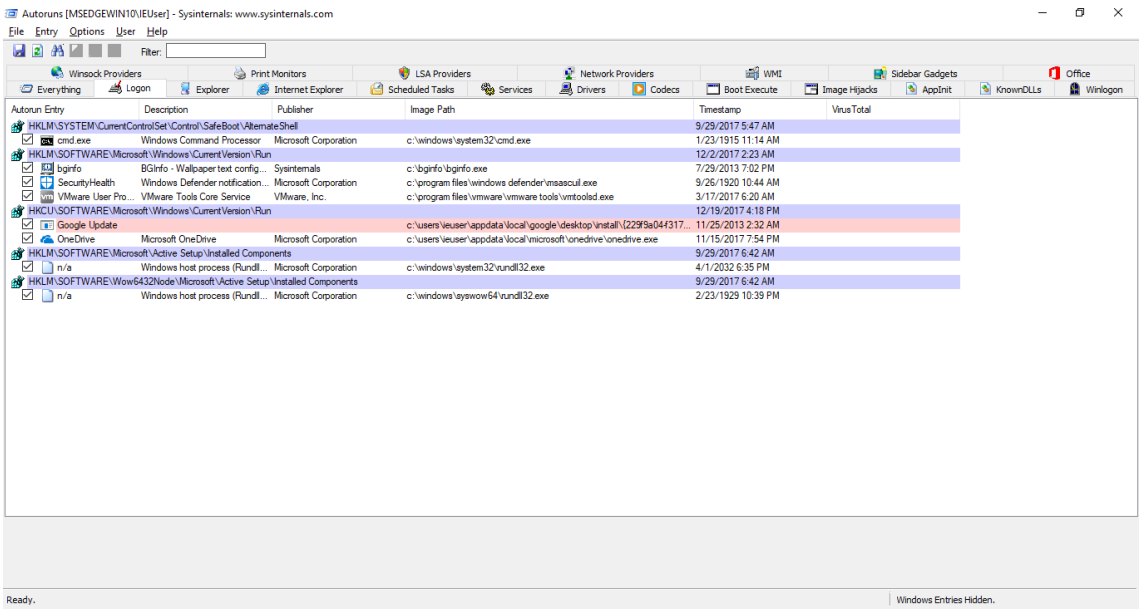
En este caso aplicaremos la utilidad Autoruns de Sysinternals, que nos muestra información como las aplicaciones que se ejecutarán al inicio, las tareas programadas, etc… Una de las utilidades interesantes de esta aplicación es que automáticamente oculta las entradas firmadas por Microsoft y remarca aquellas entradas que son fuera de lo común, o que no son provistas por el sistema o por aplicaciones confiables.

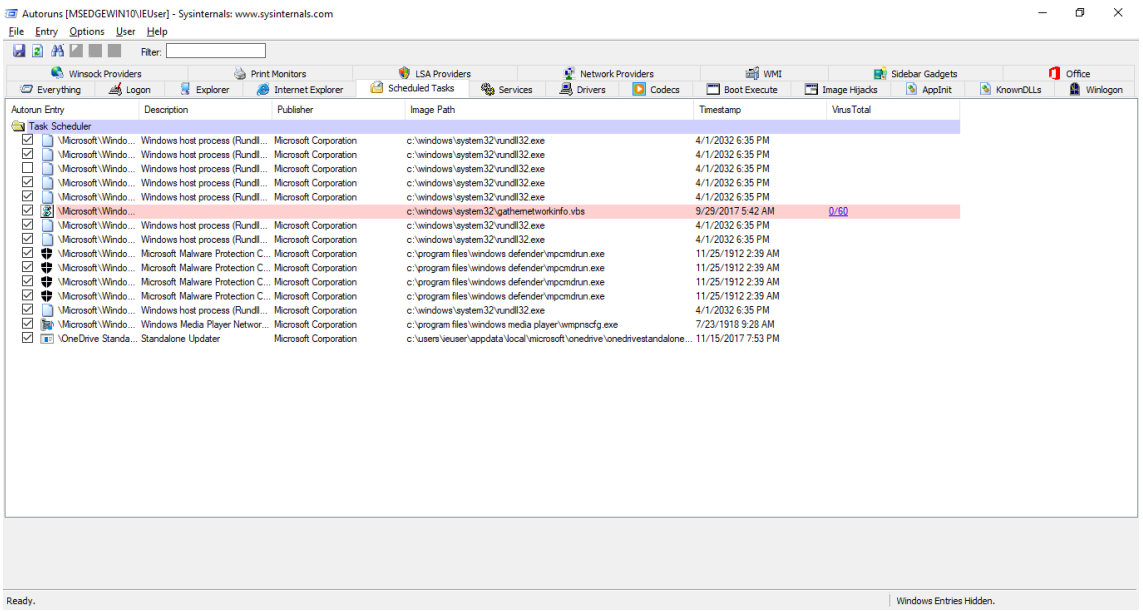
En nuestro análisis hemos encontrados tres datos interesantes mediante esta aplicación:

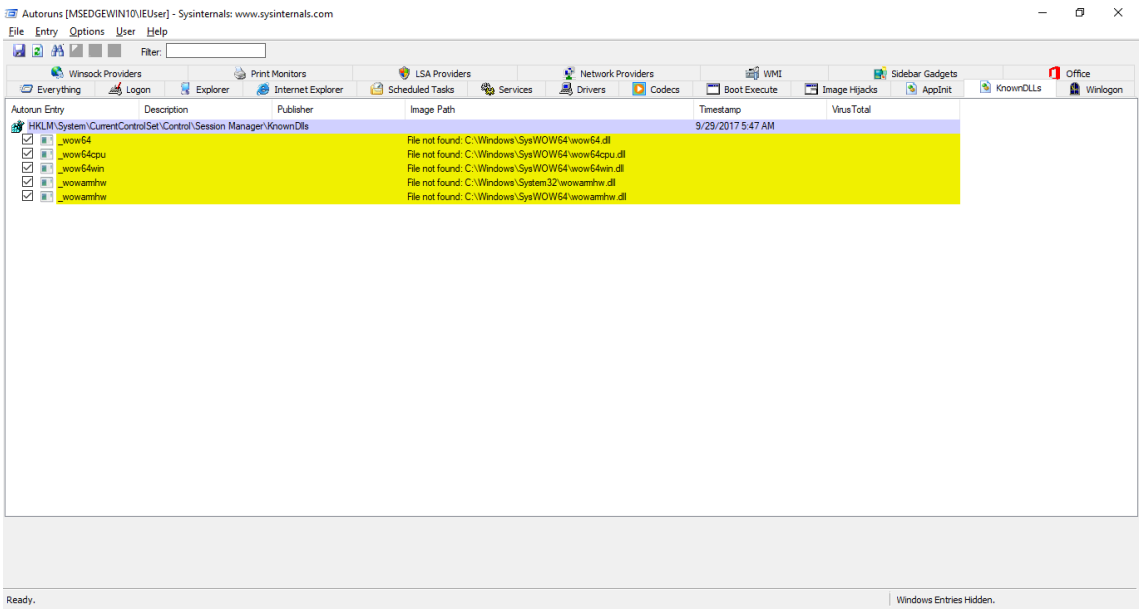
1. Durante el arranque se inicia un proceso llamado "Google Update" pero no ubicado en la carpeta go Google (el cual no está ni siquiera instalado en la máquina virtual), sino en una ubicación oculta dentro del perfil del usuario

2. Se ha creado una tarea programada que ejecuta un script llamado "gathernetworkinfo.vbs" (Recolectar información de la red)

3. La aplicación no es capaz de encontrar una serie de DLL relacionadas con el sistema operativo de 64 bits


Autoruns [MSEDGEWIN10\IEUser] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit KnownDLLs Winlogon
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell 9/29/2017 5:47 AM
cmd.exe Windows Command Processor Microsoft Corporation c:\windows\system32\cmd.exe 1/23/1915 11:14 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 12/2/2017 2:23 AM
bginfo BGInfo - Wallpaper text config... Sysinternals c:\bginfo\bginfo.exe 7/29/2013 7:02 PM
SecurityHealth Windows Defender notification... Microsoft Corporation c:\program files\windows defender\msascuil.exe 9/26/1920 10:44 AM
VMware User Pro... VMware Tools Core Service VMware, Inc. c:\program files\vmware\vmware tools\vmtoolsd.exe 3/17/2017 6:20 AM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 12/19/2017 4:18 PM
Google Update c:\users\ieuser\appdata\local\google\desktop\install\{229f9a04-4317... 11/25/2013 2:32 AM
OneDrive Microsoft OneDrive Microsoft Corporation c:\users\ieuser\appdata\local\microsoft\onedrive\onedrive.exe 11/15/2017 7:54 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 9/29/2017 6:42 AM
n/a Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components 9/29/2017 6:42 AM
n/a Windows host process (Rundll... Microsoft Corporation c:\windows\syswow64\rundll32.exe 2/23/1929 10:39 PM
Ready.
Windows Entries Hidden.


Autoruns [MSEDGEWIN10\IEUser] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
Winsock Providers Print Monitors LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit KnownDLLs Winlogon
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
Task Scheduler
\Microsoft\Windo... Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
\Microsoft\Windo... Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
\Microsoft\Windo... Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
\Microsoft\Windo... Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
\Microsoft\Windo... Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
\Microsoft\Windo... c:\windows\system32\gathernetworkinfo.vbs 9/29/2017 5:42 AM 0/60
\Microsoft\Windo... Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
\Microsoft\Windo... Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
\Microsoft\Windo... Microsoft Malware Protection C... Microsoft Corporation c:\program files\windows defender\mpcmdrun.exe 11/25/1912 2:39 AM
\Microsoft\Windo... Microsoft Malware Protection C... Microsoft Corporation c:\program files\windows defender\mpcmdrun.exe 11/25/1912 2:39 AM
\Microsoft\Windo... Microsoft Malware Protection C... Microsoft Corporation c:\program files\windows defender\mpcmdrun.exe 11/25/1912 2:39 AM
\Microsoft\Windo... Microsoft Malware Protection C... Microsoft Corporation c:\program files\windows defender\mpcmdrun.exe 11/25/1912 2:39 AM
\Microsoft\Windo... Windows host process (Rundll... Microsoft Corporation c:\windows\system32\rundll32.exe 4/1/2032 6:35 PM
\Microsoft\Windo... Windows Media Player Networ... Microsoft Corporation c:\program files\windows media player\wmpnscfg.exe 7/23/1918 9:28 AM
\OneDrive Standa... Standalone Updater Microsoft Corporation c:\users\ieuser\appdata\local\microsoft\onedrive\onedrivestandalone... 11/15/2017 7:53 PM
Ready.
Windows Entries Hidden.



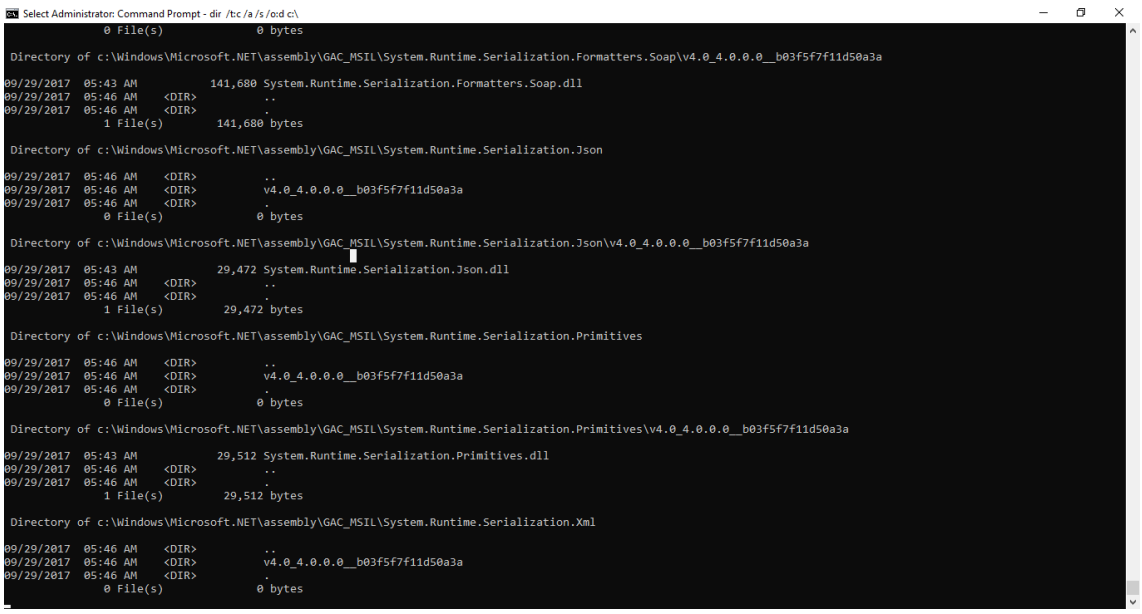

Analizaremos cada uno de estos hallazgos en el apartado de conclusiones, incluyendo su comprobación contra la base de datos virustotal.com, otra de las utilidades que la aplicación tiene incluida.

## *Árbol de directorios*

Aunque también podemos extraer esta información de la imagen forense, utilizaremos las herramientas internas del equipo para extraer el árbol de carpetas mientras el equipo sigue vivo. Desconocemos aún si la amenaza puede destruir datos al apagar el equipo, por lo que todo lo que podamos extraer en este punto será interesante.

Para obtener un mapa del sistema de fichero basado en la fecha de creación, y dado que solo tenemos un volumen, usaremos el siguiente comando de consola

dir /t:c /a /s /o:d c:\ > C:\Users\IEUser\ListadoFicherosPorFechaDeCreacion-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt

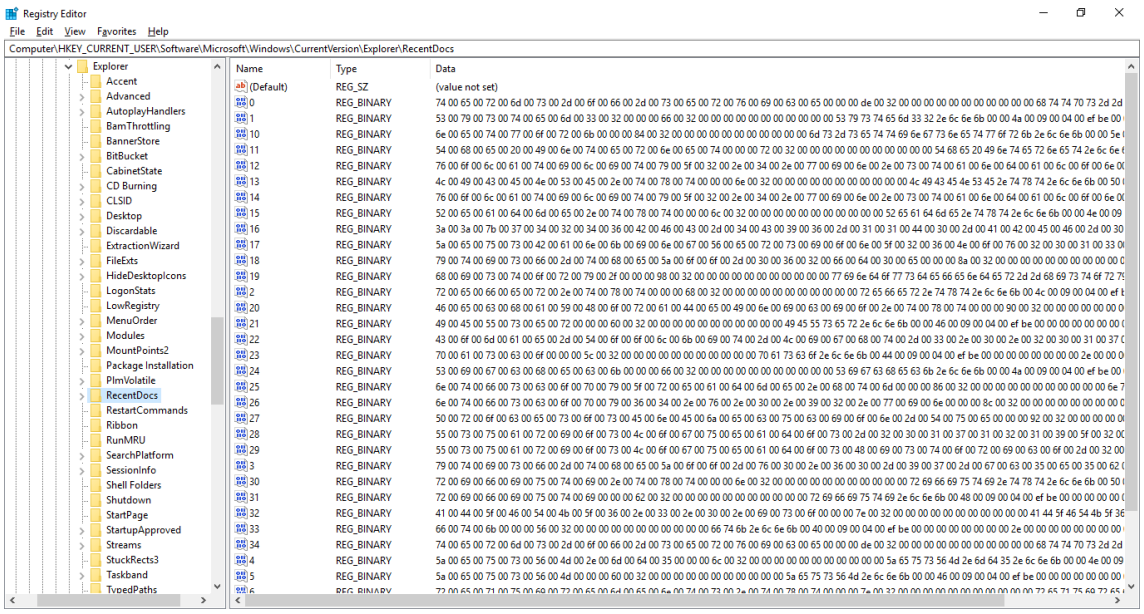



El resultado de este listado se volcará en el fichero ListadoFicherosPorFechaDeCreacion-20171220_041321.txt, cuyo hash es
09D1E52FDD08492819626EE6833A6FE8EC6C254FF726EB4F6433D440D782E6E145733F48F18B071B15108B17F5D7AC631089ACD64A8CED8297DA123097D4E715

## *Ficheros Recientes*

Si sospechamos que el equipo puede haber sido infectado por un malware recientemente, podemos intentar aislar los últimos ficheros abiertos, y tal vez poder recuperar un hilo temporal, o incluso el malware original. Esta información se incluye en el registro y lo exportaremos mediante

reg export "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs" "RecentDocs-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.reg"




El fichero de registro tiene el nombre RecentDocs-20171220_ 50226.reg y un valor hash de 601CABCD8E0712301E7D977446654D9409C1B6CE666DDA3968C6CA1EE18359CD1BE3E21D250CBB188F7971BFA4D9B3761B6851BF75D13A58C41D858B042A20EE

## *Otras Capturas no aplicables*

A pesar de que hemos tomado muestras y datos de varios apartados del sistema, existen algunos otros que pueden ser extraídos mediante técnicas en el sistema operativo, tales como:

- Dispositivos USB conectados
- Listado de redes WIFI a las que se ha conectado un equipo
- Configuración de Windows Security Center / Windows Action Center
- Configuración del firewall de Windows
- Asociaciones de ficheros con depuradores
- MUICache
- LastVisitedMRU / LastVisitedPidlMRU
- OpenSaveMRU
- Browser Helper Objects (BHO)
- Información cacheada de los navegadores
- Histórico de la pantalla de consola

- Información de portapapeles
- Historial de Internet
- Últimas búsquedas
- Cookies
- Volúmenes cifrados
- Unidades mapeadas
- Carpetas compartidas
- Grabaciones pendientes

Todas estas pruebas han sido obviadas, bien porque no eran de aplicación para nuestro entorno o porque no arrojaban información alguna al estudio. Aun así, merece la pena nombrarlos como referencias para cualquier otro estudio fuera de un entorno de laboratorio.

Además, y para evitar ser redundante, diremos que aplicaciones como Autopsy pueden proveernos esta información desde la imagen forense.

# Creación de la imagen forense

Una vez que se ha terminado de tomar todas las evidencias volátiles, el siguiente paso debe ser tomar una imagen forense del equipo a estudiar, de tal manera que todos los trabajos se hagan sobre una copia exacta del volumen inicial, en lugar de sobre el disco comprometido.

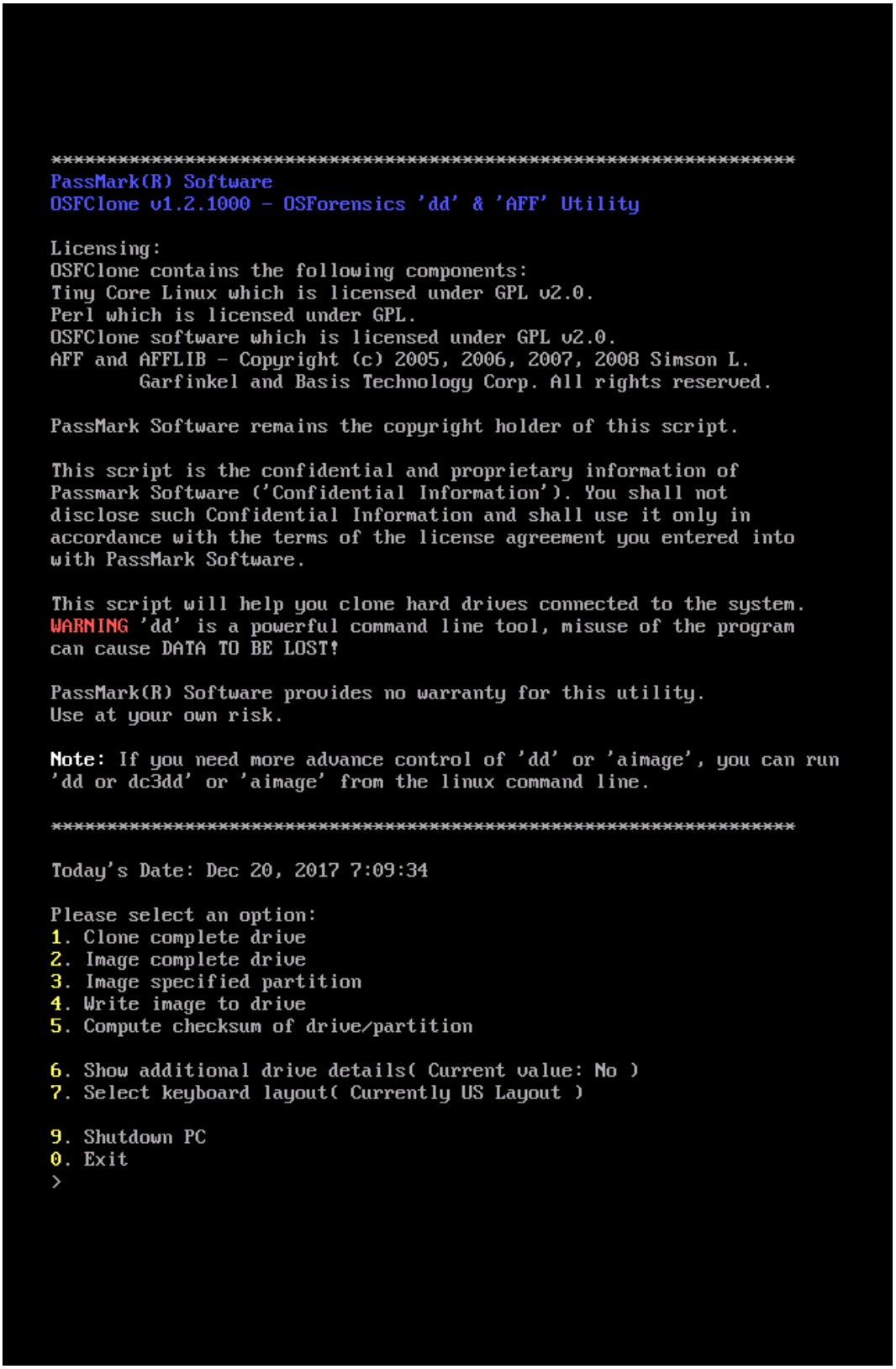
Este volcado del disco duro puede ser llevado a cabo de diferentes maneras, dependiendo de la tecnología que se vaya a utilizar en el análisis:

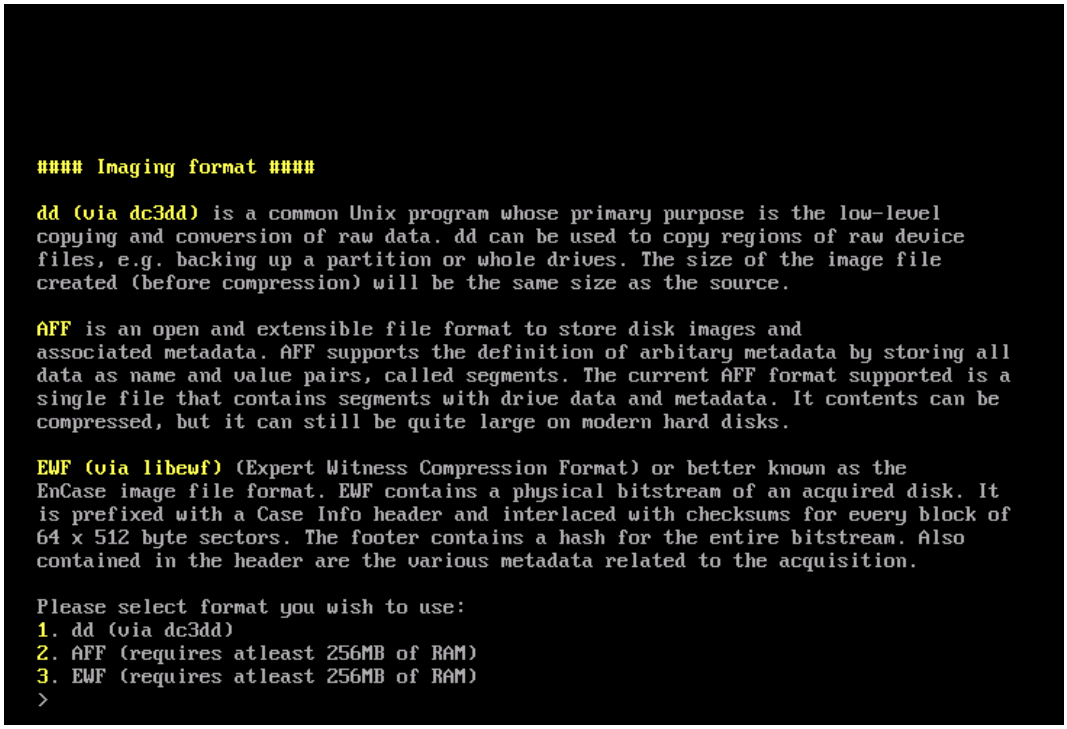
- Copia bit a bit de disco a imagen
- Copia bit a bit de disco a disco
- Exportación de selección de datos

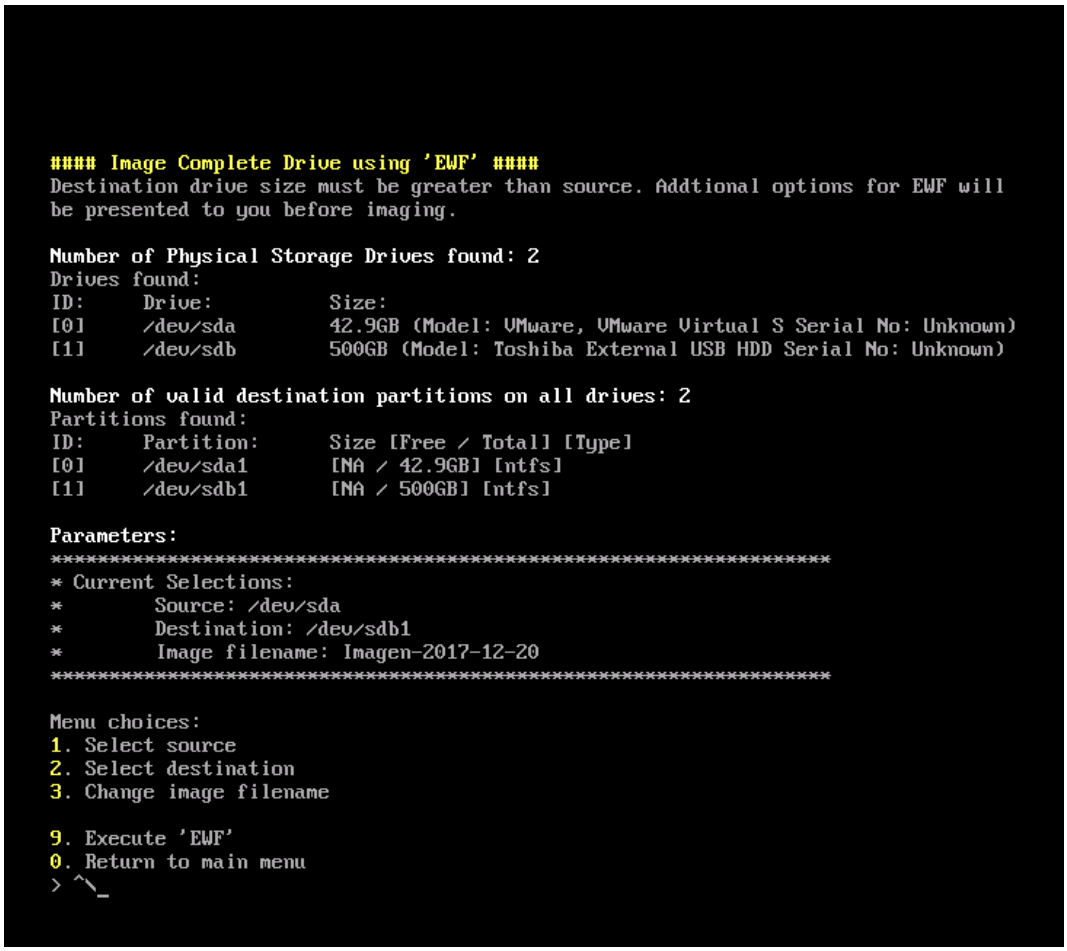
En nuestro caso, y de cara a dar una validez forense a nuestro estudio, nos centraremos en la primera opción. Existen en la actualidad diferentes softwares que permiten realizar una copia bit a bit de un disco, como dd o WinDD, desde un disco live en el sistema comprometido, y también contamos con software más específicos para extraer imágenes forenses, que contienen ya de por si metadatos sobre el análisis. El formato más famoso de este tipo de ficheros es el denominado formato EnCase (.E01…). EnCase es una suite forense de código propietario cuyo formato de imagen sirve como estándar en la tecnología de análisis forense de discos. Aunque EnCase es una solución de pago, también existe software libre que es capaz de comprimir y analizar estos formatos. Para este análisis vamos a utilizar OSFClone de OSForensics (PassMark), una distribución que se ejecuta en Live y con el que se puede extraer fácilmente una imagen en diferentes formatos raw, AFF o EWF (EnCase).

A continuación, veremos el proceso de creación de dicha imagen. Para volcarlo se ha conectado un disco duro a la máquina virtual, y se ha conectado la ISO de OSFClone al lector de CD del equipo virtual comprometido.

1. En la pantalla inicial elegimos realizar una imagen del disco completo (2)
2. Elegimos el formato EWF (3)
3. Seleccionamos el origen y destino de los datos, así como el nombre
4. Se visualiza un resumen de las características de la imagen y se ejecuta


PassMark(R) Software
OSFClone v1.2.1000 - OSForensics 'dd' & 'AFF' Utility
Licensing:
OSFClone contains the following components:
Tiny Core Linux which is licensed under GPL v2.0.
Perl which is licensed under GPL.
OSFClone software which is licensed under GPL v2.0.
AFF and AFFLIB - Copyright (c) 2005, 2006, 2007, 2008 Simson L.
Garfinkel and Basis Technology Corp. All rights reserved.
PassMark Software remains the copyright holder of this script.
This script is the confidential and proprietary information of
Passmark Software ('Confidential Information'). You shall not
disclose such Confidential Information and shall use it only in
accordance with the terms of the license agreement you entered into
with PassMark Software.
This script will help you clone hard drives connected to the system.
WARNING 'dd' is a powerful command line tool, misuse of the program
can cause DATA TO BE LOST!
PassMark(R) Software provides no warranty for this utility.
Use at your own risk.
Note: If you need more advance control of 'dd' or 'aimage', you can run
'dd or dc3dd' or 'aimage' from the linux command line.
Today's Date: Dec 20, 2017 7:09:34
Please select an option:
1. Clone complete drive
2. Image complete drive
3. Image specified partition
4. Write image to drive
5. Compute checksum of drive/partition
6. Show additional drive details( Current value: No )
7. Select keyboard layout( Currently US Layout )
9. Shutdown PC
0. Exit
>


#### Imaging format ####
dd (via dc3dd) is a common Unix program whose primary purpose is the low-level copying and conversion of raw data. dd can be used to copy regions of raw device files, e.g. backing up a partition or whole drives. The size of the image file created (before compression) will be the same size as the source.
AFF is an open and extensible file format to store disk images and associated metadata. AFF supports the definition of arbitary metadata by storing all data as name and value pairs, called segments. The current AFF format supported is a single file that contains segments with drive data and metadata. It contents can be compressed, but it can still be quite large on modern hard disks.
EWF (via libewf) (Expert Witness Compression Format) or better known as the EnCase image file format. EWF contains a physical bitstream of an acquired disk. It is prefixed with a Case Info header and interlaced with checksums for every block of 64 x 512 byte sectors. The footer contains a hash for the entire bitstream. Also contained in the header are the various metadata related to the acquisition.
Please select format you wish to use:
1. dd (via dc3dd)
2. AFF (requires atleast 256MB of RAM)
3. EWF (requires atleast 256MB of RAM)
>

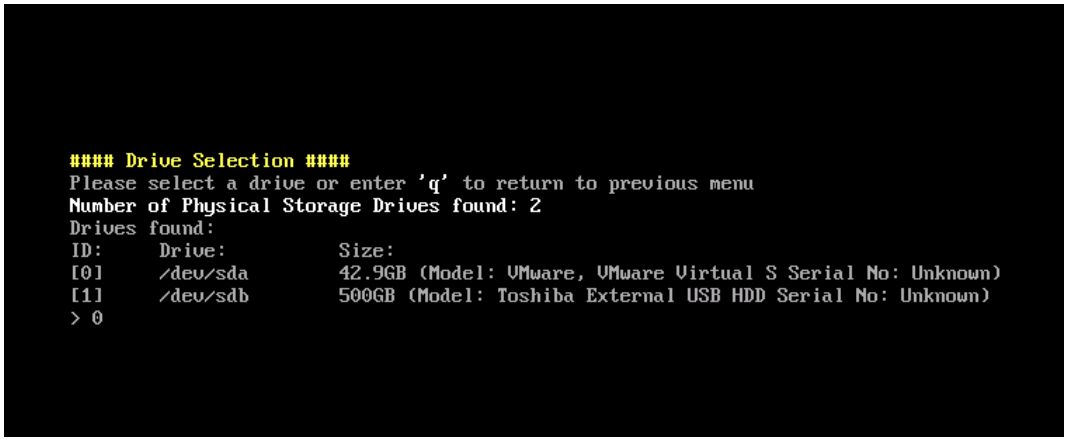

#### Image Complete Drive using 'EWF' ####
Destination drive size must be greater than source. Addtional options for EWF will be presented to you before imaging.
Number of Physical Storage Drives found: 2
Drives found:
ID: Drive: Size:
[0] /dev/sda 42.9GB (Model: VMware, VMware Virtual S Serial No: Unknown)
[1] /dev/sdb 500GB (Model: Toshiba External USB HDD Serial No: Unknown)
Number of valid destination partitions on all drives: 2
Partitions found:
ID: Partition: Size [Free / Total] [Type]
[0] /dev/sda1 [NA / 42.9GB] [ntfs]
[1] /dev/sdb1 [NA / 500GB] [ntfs]
Parameters:
**********
* Current Selections:
* Source: /dev/sda
* Destination: /dev/sdb1
* Image filename: Imagen-2017-12-20
**********
Menu choices:
1. Select source
2. Select destination
3. Change image filename
9. Execute 'EWF'
0. Return to main menu
> ^_

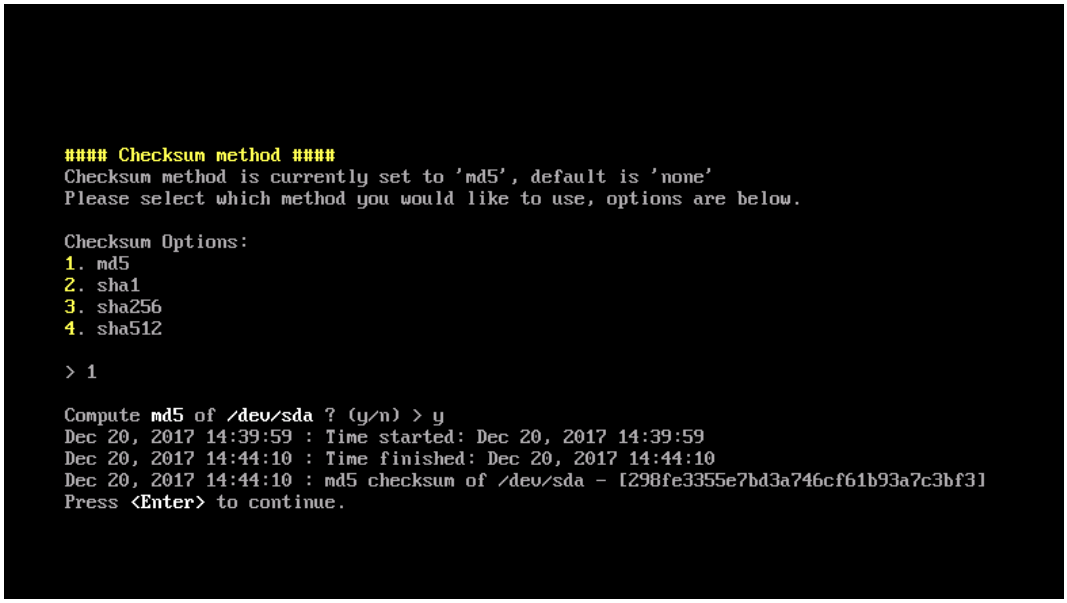
```
#### Image Complete Drive using 'EWF' ####
Destination drive size must be greater than source. Addtional options for EWF will
be presented to you before imaging.

Number of Physical Storage Drives found: 2
Drives found:
ID:     Drive:          Size:
[0]     /dev/sda        42.9GB (Model: VMware, VMware Virtual S Serial No: Unknown)
[1]     /dev/sdb        500GB (Model: Toshiba External USB HDD Serial No: Unknown)

Number of valid destination partitions on all drives: 2
Partitions found:
ID:     Partition:      Size [Free / Total] [Type]
Use EWF file format (ewf, smart, ftk, encase1, encase2, encase3, encase4, encase5, encase6, encase7, encase7-v2, linen5, linen6,
 linen7, ewfx) [encase6]:
Compression method (deflate) [deflate]:
Compression level (none, empty-block, fast, best) [none]:
Start to acquire at offset (0 <= value <= 42949672960) [0]:
The number of bytes to acquire (0 <= value <= 42949672960) [42949672960]:
Evidence segment file size in bytes (1.0 MiB <= value <= 7.9 EiB) [1.4 GiB]:
The number of bytes per sector (1 <= value <= 4294967295) [512]:
The number of sectors to read at once (16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768) [64]:
The number of sectors to be used as error granularity (1 <= value <= 64) [64]:
The number of retries when a read error occurs (0 <= value <= 255) [2]:
Wipe sectors on read error (mimic EnCase like behavior) (yes, no) [no]:

The following acquiry parameters were provided:
Image path and filename:                /mnt/temp/Imagen-2017-12-20.E01
Case number:                            001
Description:                            Imagen Forense para TFM UOC
Evidence number:                        020
Examiner name:                          Javier Leon
Notes:
Media type:                             fixed disk
Is physical:                            no
EWF file format:                        EnCase 6 (.E01)
Compression method:                     deflate
Compression level:                      none
Acquiry start offset:                   0
Number of bytes to acquire:             40 GiB (42949672960 bytes)
Evidence segment file size:             1.4 GiB (1572864000 bytes)
Bytes per sector:                       512
Block size:                             64 sectors
Error granularity:                      64 sectors
Retries on read error:                  2
Zero sectors on read error:             no

Continue acquiry with these values (yes, no) [yes]:
```

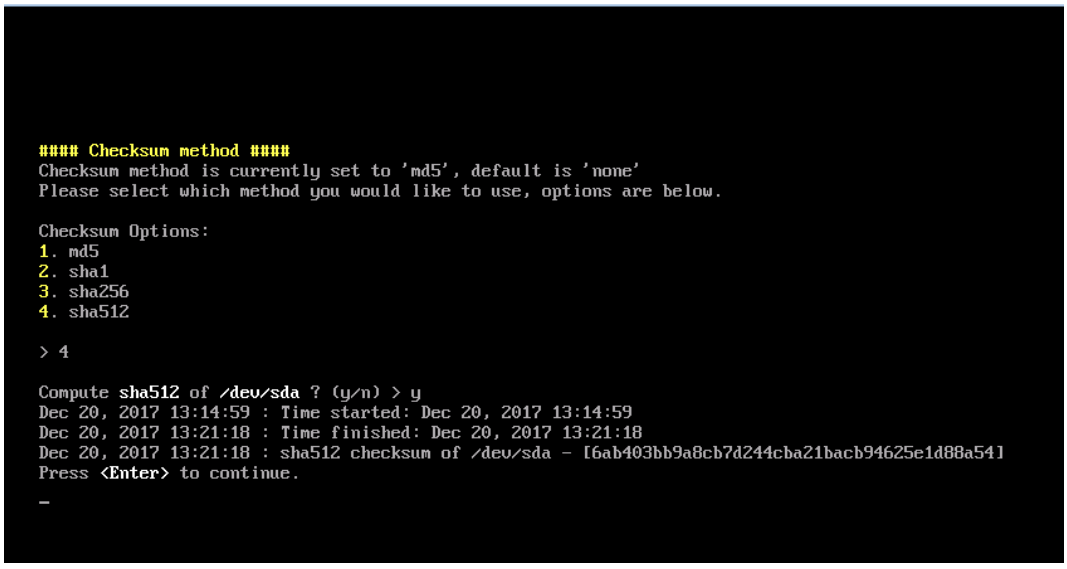
Es importante comprobar que la imagen extraída corresponde con los mismos datos exactamente que la que se encuentra en el disco, si no este proceso sería inútil.

Con esta finalidad, OSFClone ofrece la posibilidad de calcular el hash en diferentes algoritmos para su posterior comparación. Si utilizáramos otra suite sin esta posibilidad, deberíamos hacer al menos tres copias y comprobar que coincidan los hashes de al menos dos de ellas, aunque lo ideal sería que las tres coincidieran.

```
#### Compute Checksum ####

Compute checksum of:
1. Drive
2. Partition

0. Exit
> _
```


#### Drive Selection ####
Please select a drive or enter 'q' to return to previous menu
Number of Physical Storage Drives found: 2
Drives found:
ID: Drive: Size:
[0] /dev/sda 42.9GB (Model: VMware, VMware Virtual S Serial No: Unknown)
[1] /dev/sdb 500GB (Model: Toshiba External USB HDD Serial No: Unknown)
> 0

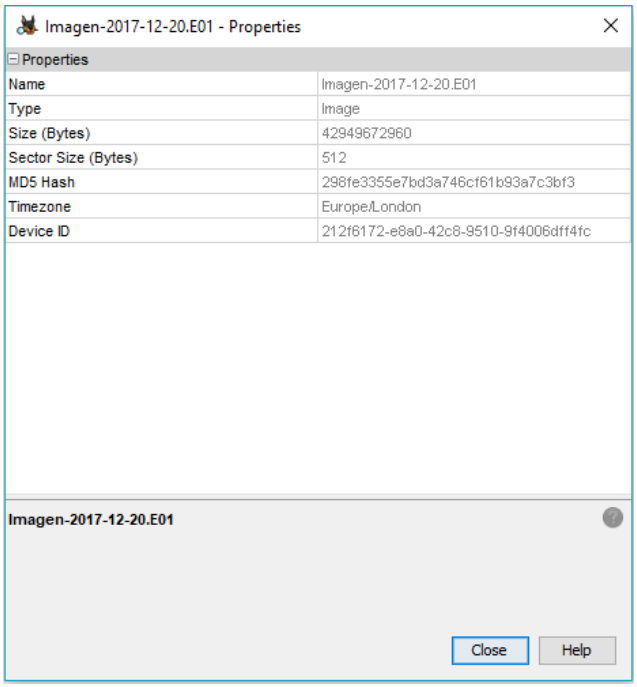

#### Checksum method ####
Checksum method is currently set to 'md5', default is 'none'
Please select which method you would like to use, options are below.
Checksum Options:
1. md5
2. sha1
3. sha256
4. sha512
> 1
Compute md5 of /dev/sda ? (y/n) > y
Dec 20, 2017 14:39:59 : Time started: Dec 20, 2017 14:39:59
Dec 20, 2017 14:44:10 : Time finished: Dec 20, 2017 14:44:10
Dec 20, 2017 14:44:10 : md5 checksum of /dev/sda - [298fe3355e7bd3a746cf61b93a7c3bf3]
Press <Enter> to continue.


#### Checksum method ####
Checksum method is currently set to 'md5', default is 'none'
Please select which method you would like to use, options are below.
Checksum Options:
1. md5
2. sha1
3. sha256
4. sha512
> 4
Compute sha512 of /dev/sda ? (y/n) > y
Dec 20, 2017 13:14:59 : Time started: Dec 20, 2017 13:14:59
Dec 20, 2017 13:21:18 : Time finished: Dec 20, 2017 13:21:18
Dec 20, 2017 13:21:18 : sha512 checksum of /dev/sda - [6ab403bb9a8cb7d244cba21bacb94625e1d88a54]
Press <Enter> to continue.

Los valores hash para el disco que hemos extraído son los siguientes:

- SHA-512: 6ab403bb9a8cb7d244cba21bacb94625e1d88a54
- MD5:298fe3355e7bd3a746cf61b93a7c3bf3

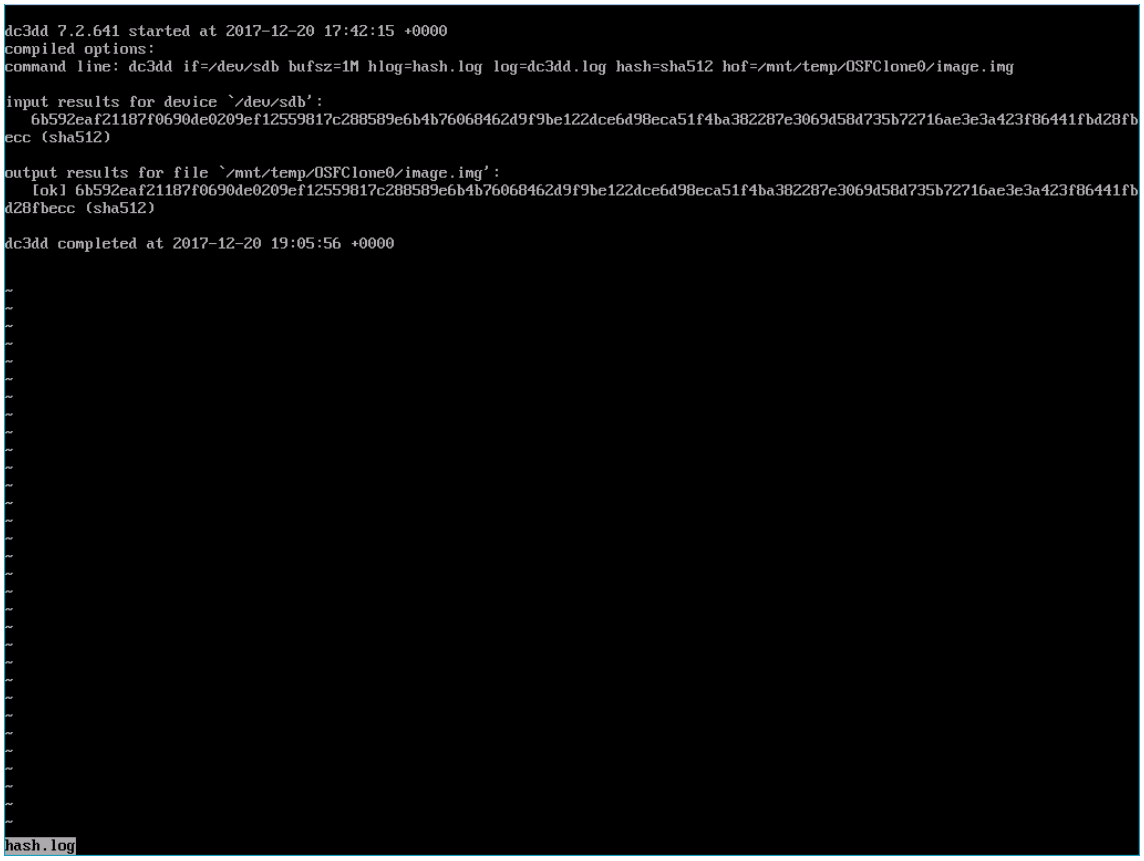
Ahora utilizaremos la herramienta de análisis Autopsy para extraer el hash MD5 de la imagen que hemos creado (desgraciadamente Autopsy aún no ofrece la posibilidad de calcular el checksum en ningún algoritmo de SHA):




Vemos que el hash coincide, por lo que aceptamos que la imagen es correcta, dentro del posible margen de colisión que existe en MD5.

Como modo alternativo, se ha seguido el procedimiento similar para obtener una imagen del disco mediante la herramienta “dd”, volcándolo en un fichero .img. Al contrario que el procedimiento para el formato EnCase, en este modo podemos solicitar que la propia aplicación realice el algoritmo de hash tanto en el equipo como en la imagen y nos lo muestre al finalizar el proceso para comprobar su correcta creación:

```
4. Change image filename

9. Execute 'dd'
0. Return to main menu
> 9
Dec 20, 2017 17:42:06 : STATUS: Checking SRC and DST size.
Dec 20, 2017 17:42:06 : NOTE: When compression is enabled, OSFClone will still perform these steps independently (image then com
press).
Dec 20, 2017 17:42:07 : STATUS: Mounting /dev/sda1 of type ntfs to /mnt/temp
Dec 20, 2017 17:42:08 : STATUS: Unmounting /mnt/temp...
The following 'dd' command will be executed:

        dc3dd if=/dev/sdb of=/dev/sda1/image.img bufsz=1M
        Note: /dev/sda1 will be mounted on /mnt/temp

Continue (y/n) ? > y
Dec 20, 2017 17:42:14 : STATUS: User chose to commence with 'dd'...
Dec 20, 2017 17:42:14 : STATUS: Executing dd, this process can take a while, please wait.
Dec 20, 2017 17:42:14 : STATUS: Start imaging...
Dec 20, 2017 17:42:14 : STATUS: Mounting /dev/sda1 of type ntfs to /mnt/temp

dc3dd 7.2.641 started at 2017-12-20 17:42:15 +0000
compiled options:
command line: dc3dd if=/dev/sdb bufsz=1M hlog=hash.log log=dc3dd.log hash=sha512 hof=/mnt/temp/OSFClone0/image.img
device size: 83886080 sectors (probed),   42,949,672,960 bytes
sector size: 512 bytes (probed)
 42949672960 bytes ( 40 G ) copied ( 100% ), 5022 s, 8.2 M/s
 42949672960 bytes ( 40 G ) hashed ( 100% ), 2772 s, 15 M/s

input results for device `/dev/sdb':
   83886080 sectors in
   0 bad sectors replaced by zeros
   6b592eaf21187f0690de0209ef12559817c288589e6b4b76068462d9f9be122dce6d98eca51f4ba382287e3069d58d735b72716ae3e3a423f86441fbd28fb
ecc (sha512)

output results for file `/mnt/temp/OSFClone0/image.img':
   83886080 sectors out
   [ok] 6b592eaf21187f0690de0209ef12559817c288589e6b4b76068462d9f9be122dce6d98eca51f4ba382287e3069d58d735b72716ae3e3a423f86441fb
d28fbecc (sha512)

dc3dd completed at 2017-12-20 19:05:56 +0000

Dec 20, 2017 19:05:56 : STATUS: Imaging finished.

When viewing the checksum log, use 'up ,down, space bar (next Page) or p (previous page)' keys to navigate.
After viewing press 'q' to quit.
Press <Enter> to continue.
```

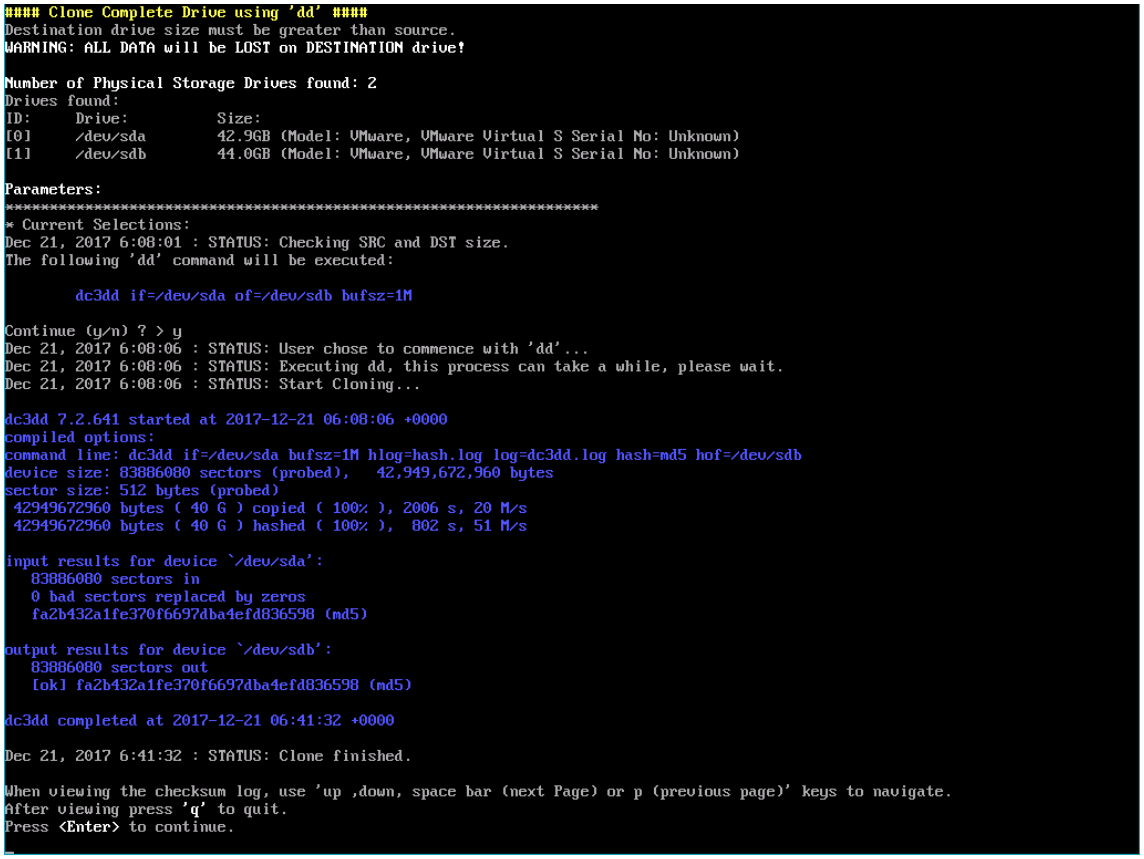



## Extracción de datos no volátiles

Una vez tenemos una copia bit a bit de la imagen, podemos extraer diferentes datos sin riesgo de modificar en modo alguno la imagen inicial, y sin mantener operativa la brecha de seguridad que estamos investigando. También podemos extraer desde la imagen, mediante herramientas como Autopsy o EnCase los ficheros de registro, para ser analizados mediante herramientas en el equipo de análisis, como Windows Registry Recover.

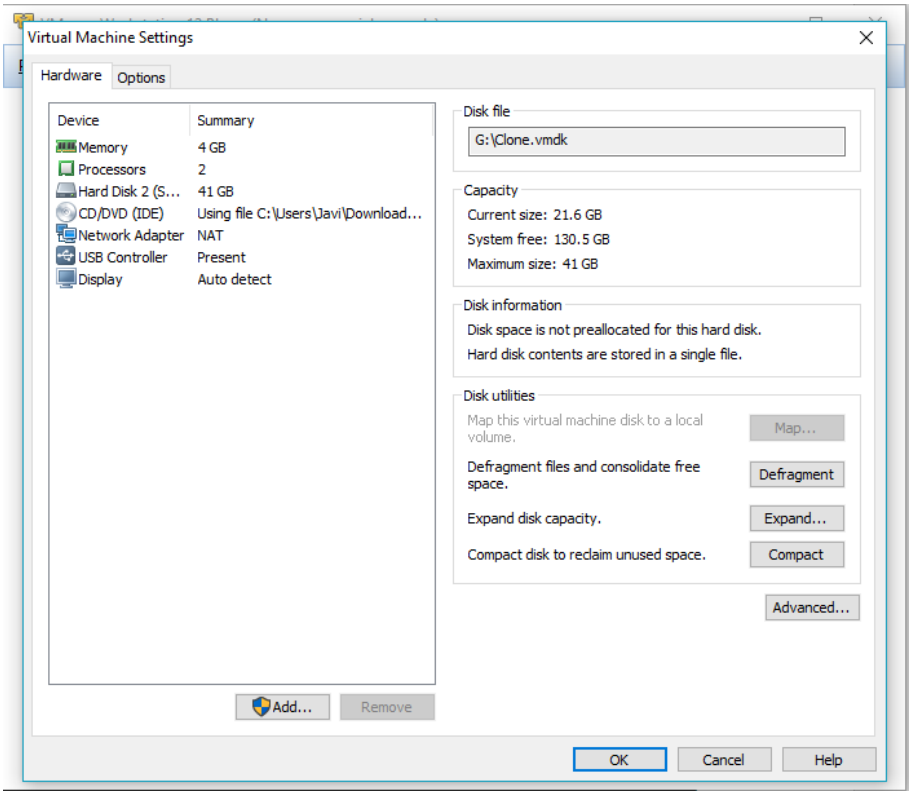
Hay una serie de atributos del sistema que pueden contener información interesante de cara a un análisis forense, como las tablas de sistema (MBR y MFT), tareas programadas y logs. A pesar de que la toma de esos datos puede conllevar el encendido del sistema para ser tomados, lo ideal es tomar la imagen que hemos creado para cargarla en un entorno que nos permita realizar las acciones que debamos sin que estas puedan modificar la imagen inicial.

A partir de este punto todas las tomas serán sobre un disco copiado, dejando el original intacto, y a ser posible desconectado del equipo. Con este fin realizaremos un clon a un disco diferente (opción 1 del OSFClon), y lo conectaremos en lugar del original.


#### Clone Complete Drive using 'dd' ####
Destination drive size must be greater than source.
WARNING: ALL DATA will be LOST on DESTINATION drive!
Number of Physical Storage Drives found: 2
Drives found:
ID: Drive: Size:
[0] /dev/sda 42.9GB (Model: VMware, VMware Virtual S Serial No: Unknown)
[1] /dev/sdb 44.0GB (Model: VMware, VMware Virtual S Serial No: Unknown)
Parameters:
* Current Selections:
Dec 21, 2017 6:08:01 : STATUS: Checking SRC and DST size.
The following 'dd' command will be executed:
dc3dd if=/dev/sda of=/dev/sdb bufsz=1M
Continue (y/n) ? > y
Dec 21, 2017 6:08:06 : STATUS: User chose to commence with 'dd'...
Dec 21, 2017 6:08:06 : STATUS: Executing dd, this process can take a while, please wait.
Dec 21, 2017 6:08:06 : STATUS: Start Cloning...
dc3dd 7.2.641 started at 2017-12-21 06:08:06 +0000
compiled options:
command line: dc3dd if=/dev/sda bufsz=1M hlog=hash.log log=dc3dd.log hash=md5 hof=/dev/sdb
device size: 83886080 sectors (probed), 42,949,672,960 bytes
sector size: 512 bytes (probed)
42949672960 bytes ( 40 G ) copied ( 100% ), 2006 s, 20 M/s
42949672960 bytes ( 40 G ) hashed ( 100% ), 802 s, 51 M/s
input results for device `/dev/sda':
83886080 sectors in
0 bad sectors replaced by zeros
fa2b432a1fe370f6697dba4efd836598 (md5)
output results for device `/dev/sdb':
83886080 sectors out
[ok] fa2b432a1fe370f6697dba4efd836598 (md5)
dc3dd completed at 2017-12-21 06:41:32 +0000
Dec 21, 2017 6:41:32 : STATUS: Clone finished.
When viewing the checksum log, use 'up ,down, space bar (next Page) or p (previous page)' keys to navigate.
After viewing press 'q' to quit.
Press <Enter> to continue.

```
dc3dd 7.2.641 started at 2017-12-21 06:08:06 +0000
compiled options:
command line: dc3dd if=/dev/sda bufsz=1M hlog=hash.log log=dc3dd.log hash=md5 hof=/dev/sdb

input results for device `/dev/sda':
   fa2b432a1fe370f6697dba4efd836598 (md5)

output results for device `/dev/sdb':
   [ok] fa2b432a1fe370f6697dba4efd836598 (md5)

dc3dd completed at 2017-12-21 06:41:32 +0000
```

hash.log



En este modo podremos obtener los siguientes datos extrayéndolos a un dispositivo de almacenamiento externo y asegurándonos que la integridad de la imagen inicial está intacta.

## *Master Boot Record (MBR)*

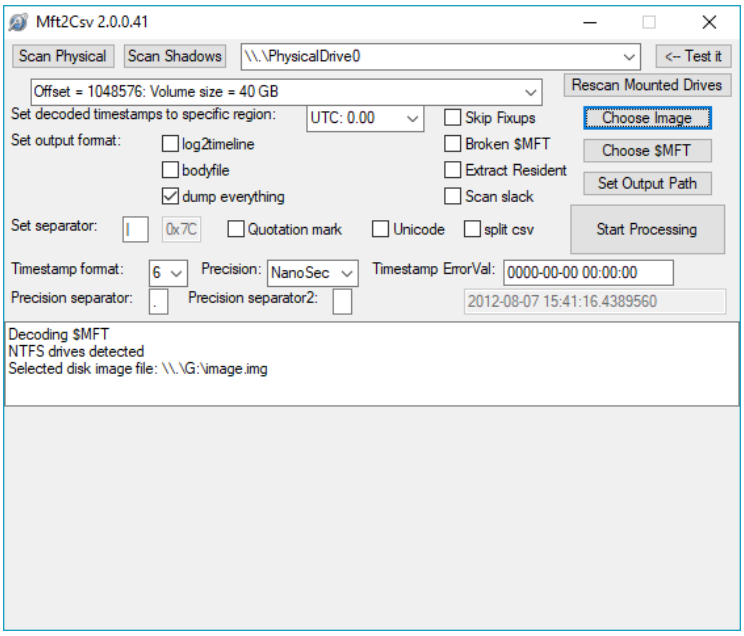
El Master Boot Record es el primer sector de un dispositivo de almacenamiento de datos. En él se incluyen datos como qué particiones hay o su tamaño. Su análisis puede ayudarnos a saber si un equipo ha "ocultado" una partición debido a la infección de un malware, por ejemplo. Para la extracción del Master Boot Record utilizaremos la utilidad MBRUtil.

MBRUtil.exe /S="E:\No-volatil\MBR-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.dat"

Si analizamos los datos obtenidos a través de esta utilidad, podemos ver que al parecer tiene algún problema con la tabla de particiones, ya que arroja el mensaje: "Invalid partition table Error loading operating system Missing operating system". Si lo comprobamos con Autopsy, por ejemplo, vemos un mensaje similar en la primera partición del sistema.

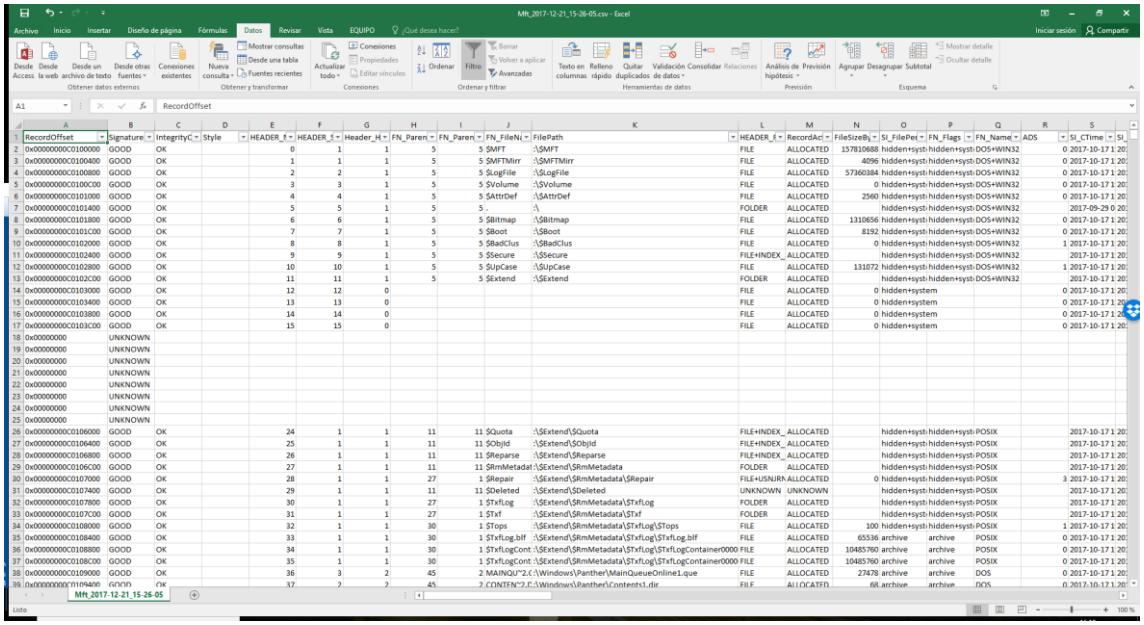
## *Master File Table (MFT)*

Con la tabla de fichero MFT hemos extraído el contenido de la misma a un conjunto de ficheros csv y SQL mediante la utilidad Mft2csv



Una de las características que tiene este software es la posibilidad de escanear una imagen de disco, en lugar de un sistema en vivo, por lo que podemos analizar la imagen obtenida mediante el comando dd en el apartado anterior.

El resultado se nos muestra como una hoja de cálculo donde además de los ficheros que ha encontrado, nos ofrece información útil como su firma, localización, su tabla MAC…



El resultado no arroja ninguna firma mala, aunque sí que existen varias entradas “inidentificables” o de espacio “unallocated”, que se encuentran sobre todo al final de la partición de boot y de la de datos, en sus últimos clústeres (en los offset 18-25 y 153919-154114)

https://github.com/jschicht/Mft2Csv

## *Información de Sistema*

El propio sistema operativo nos puede dar diferente información interesante acerca del hardware, software, actualizaciones o tiempos de actividad mediante la herramienta systeminfo:

Systeminfo > “E:\No-volatil\Systeminfo -%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

```
Host Name:                 MSEDGEWIN10
OS Name:                   Microsoft Windows 10 Enterprise Evaluation
OS Version:                10.0.16299 N/A Build 16299
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Microsoft
Product ID:                00329-20000-00001-AA273
Original Install Date:     10/17/2017, 10:13:29 AM
System Boot Time:          12/21/2017, 6:45:01 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 42 Stepping 7 GenuineIntel ~2201 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 7/2/2015
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,096 MB
Available Physical Memory: 2,897 MB
Virtual Memory: Max Size:  4,800 MB
Virtual Memory: Available: 3,722 MB
Virtual Memory: In Use:    1,078 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\MSEDGEWIN10
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB4048951
                           [02]: KB4049179
                           [03]: KB4054022
                           [04]: KB4054517
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Ethernet0 2
                                 Status:          Media disconnected
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

## *Tareas Programadas*

En algunos casos una incursión o un malware puede crear una tarea programa con el fin de asegurarse su aplicación en todo momento. En estos casos puede resultar útil revisar las tareas programadas del equipo en buscar de actividades fuera de lo común.

schtasks > “E:\No-volatil\Tareas -%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

Para este análisis no existe ningún dato reseñable, por lo que no se incluirán datos en este reporte.

## *Variables de entorno*

Puede ser útil también conocer las variables de entorno del equipo, ya que una variable no estándar podría estar detrás de un malware que ha tomado el equipo.

path > “E:\No-volatil\PATH -%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

El resultado no añade nngún dato Nuevo al análisis, ya que todas las localizaciones de la vista son comunes:

PATH=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\ProgramData\chocolatey\bin;C:\Program Files\Puppet Labs\Puppet\bin;C:\Program Files\OpenSSH\bin;C:\Users\IEUser\AppData\Local\Microsoft\WindowsApps

## *Logs*

Los logs de Windows contienen toda la información relacionada con el equipo, sus actividades, sus conexiones, fallos… Por esto tienen un alto valor en los aspectos forenses, ya que nos muestran un "cuaderno de bitácora" del equipo que estamos investigando.

## *Logs de Windows*

Mediante los siguientes comandos, exportaremos los eventos de Windows a un formato texto, que después podremos manipular mediante el analizador de log que prefiramos. También podemos copiar directamente los ficheros que se encuentran en %systemroot%\system32\config si los preferimos en formato Windows Event Viewer.

PSLoglist –s application > "E:\No-volatil\LogApp -%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

PSLoglist –s system > "E:\No-volatil\LogSys -%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

PSLoglist –s security > "E:\No-volatil\LogSEC -%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

## *Firewall*

En ciertos casos puede resultarnos útil también analizar el log del Firewall, ya que nos puede mostrar un histórico de paquetes que se han rechazado o permitido, y arrojar luz sobre las acciones de red realizadas por el equipo.

Para los sistemas operativos Windows 10 como este, el Firewall de Windows se encuentra embebido en la solución Windows Defender, que se encontraba apagado, por lo que no hemos podido extraer información de este recurso.

## *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.

Si lo utilizamos con una herramienta como WinPrefetchView de NirSoft, podemos identificar las aplicaciones usadas por nuestro sistema de forma relativamente fácil.

Se han encontrado nuevos datos sobre aplicaciones de nombres sospechosos, o cuyo nombre de proceso no se define. Estos datos se incluirán en el apartado de conclusiones en el reporte final.

## *Papelera*

En ciertas ocasiones puede ser útil revisar la papelera de reciclaje en busca de fichero eliminados que pudieran ser una amenaza. Dentro de las carpetas ubicadas en %SystemDrive%\$Recycle.Bin\ por cada fichero eliminado habrá dos ficheros con el mismo nombre excepto la segunda letra. 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.

## *Ejecutables no firmados*

La busqueda de ficheros cuya propiedad no sea verificable también puede ser de utilidad si sospechamos de actividades de malware. Mediante el uso de la utilidad Sigcheck de SysInternals, que compara la firma contra la base de datos de VirusTotal.com, podemos analizar si existe algún fichero sospechoso. Por economía de tiempo y esfuerzo, nos centraremos en las rutas de Windows y del único usuario, de manera recursiva.

Sigcheck64.exe –ct –h –v –vt -s c:\Windows > “E:\No-volatil\FicherosFirmadosWindir-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

Sigcheck64.exe –ct –h –v –vt -s c:\Users\IEUser > “E:\No-volatil\FicherosFirmadosUser-%date:~-4,4%%date:~-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"

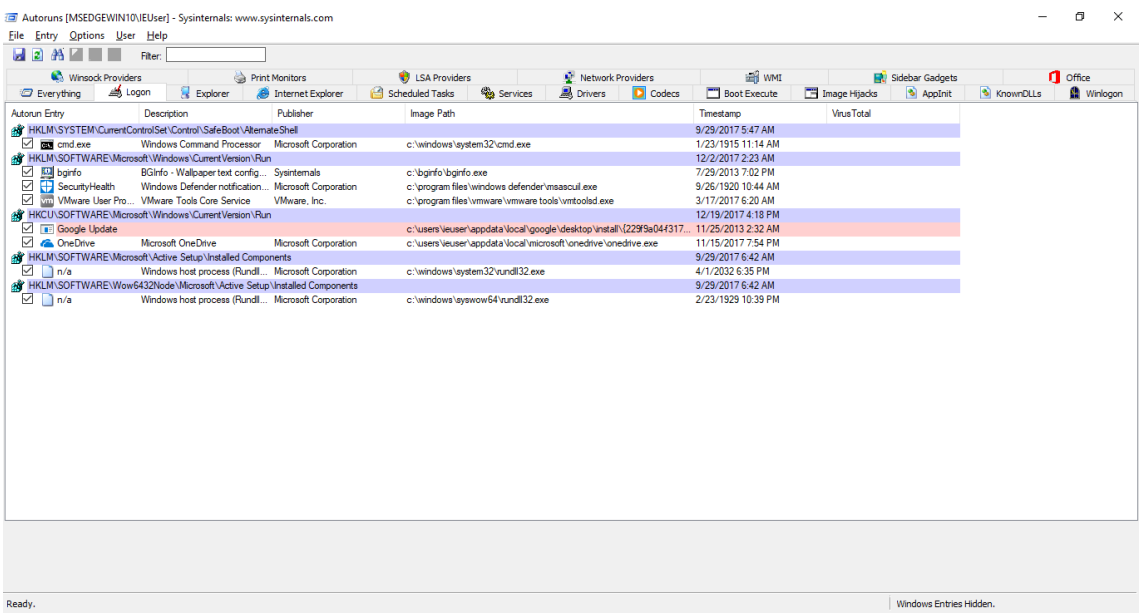
# Conclusiones

En este apartado indicaremos las evidencias significativas que hemos encontrado y toda la información que hayamos podido extraer de las mismas.

A pesar de que se han extraído diferentes evidencias, y varias categorías, han sido especialmente útiles las relacionadas con el inicio de equipo y las aplicaciones, ya que esta información es especialmente útil en casos de infecciones de malware.

## Evidencias en el arranque del equipo

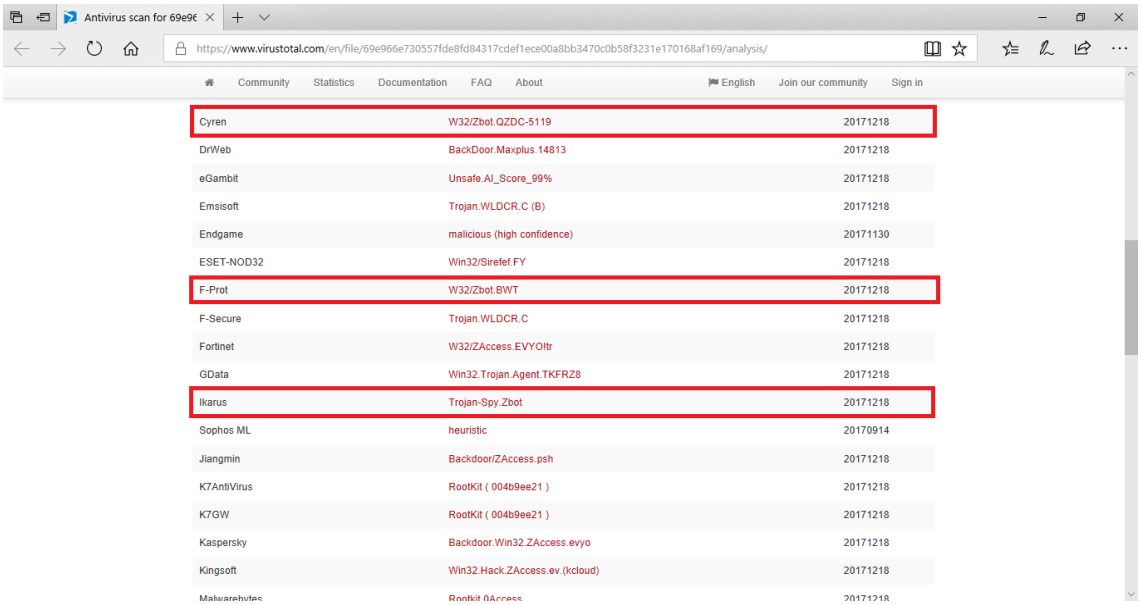
Una de las formas comunes en las que un malware se asegura de ser iniciado después de encender el equipo es añadirse en la lista de acciones en el "start-up". En el análisis de la secuencia de inicio mediante la herramienta Autoruns de Sysinternals, pudimos ver como existe una secuencia bajo el nombre de Google Update que ejecuta un script proveniente de una carpeta oculta en el escritorio del usuario, que no es accesible por ningún usuario. Una de los aspectos llamativos de esta tarea es que carece de descripción o propietario, y que la carpeta a la que hace referencia parece no existir.




Además, hay que reseñar que el equipo comprometido carece de ningún software propiedad de Google, por lo que ningún software confiable pudo crear esta tarea.

Con el fin de poder identificar la amenaza, Autoruns permite lanzar una solicitud directa a los servidores de VirusTotal.com, subiendo el hash del fichero y comparándola con sus bases de datos para comprobar si el objeto puede ser malicioso. Tras realizar esta comprobación, vemos que el fichero que inicia esta tarea se confirma que se trata de un troyano por la gran mayoría de las bases de datos de virus con las que se compara (https://www.virustotal.com/en/file/69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169/analysis/ )

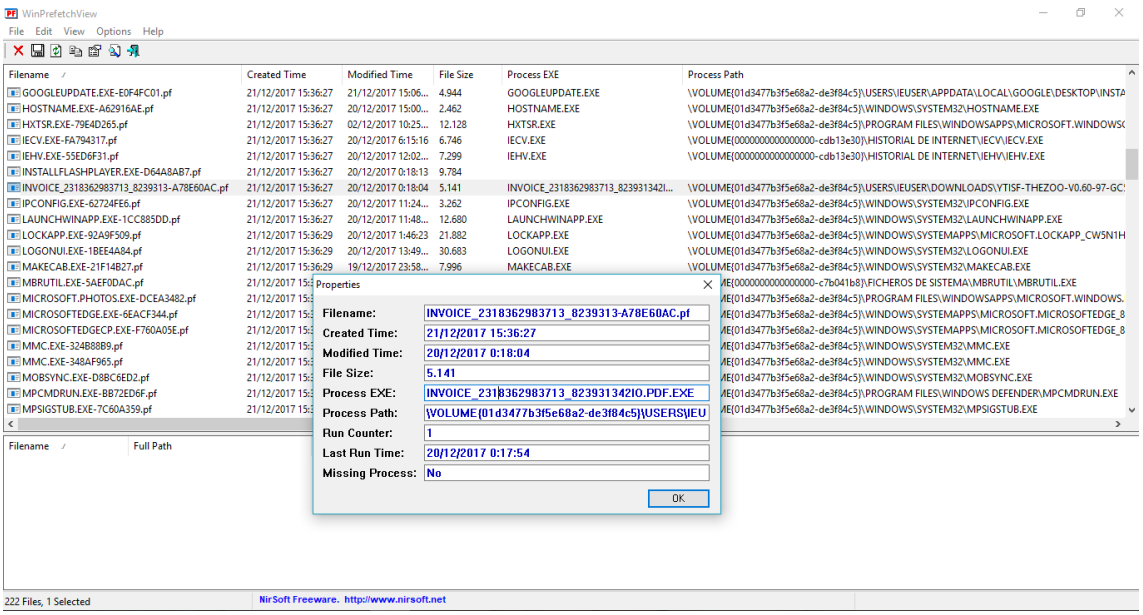
Si observamos los resultados de estos análisis, podemos identificar incluso el tipo de malware que ha infectado el equipo:




ZBot, o también llamado Zeus, lo definiremos al final de este apartado.

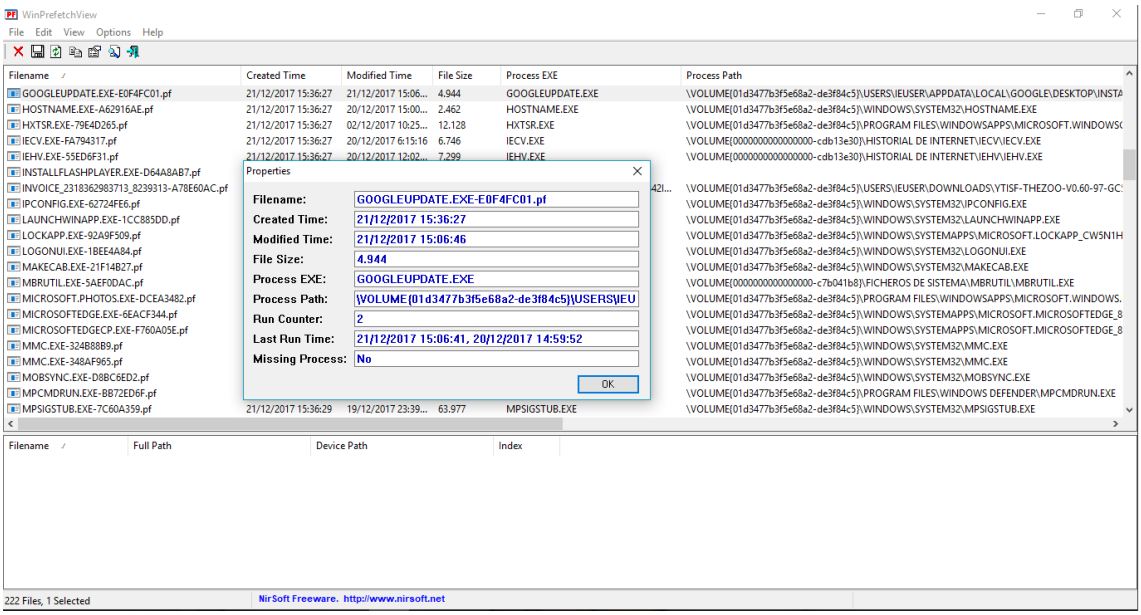
## Aplicaciones en la carpeta prefetch

Por su parte, un análisis detallado de la carpeta prefetch nos muestra que hay algunas aplicaciones con nombre sospechosos, como INVOICE_2318362983713_8239313-A78E60AC.pf, lo que parece un documento de texto y resulta ser una aplicación como podemos ver en su path \VOLUME{01d3477b3f5e68a2-de3f84c5}\USERS\IEUSER\DOWNLOADS\YTISF-THEZOO-V0.60-97-GC5E5BD8\YTISF-THEZOO-C5E5BD8\MALWARES\BINARIES\ZEUSBANKINGVERSION_26NOV2013\ZEUSBANKINGVERSION_26NOV2013\INVOICE_2318362983713_823931342IO.PDF.EXE



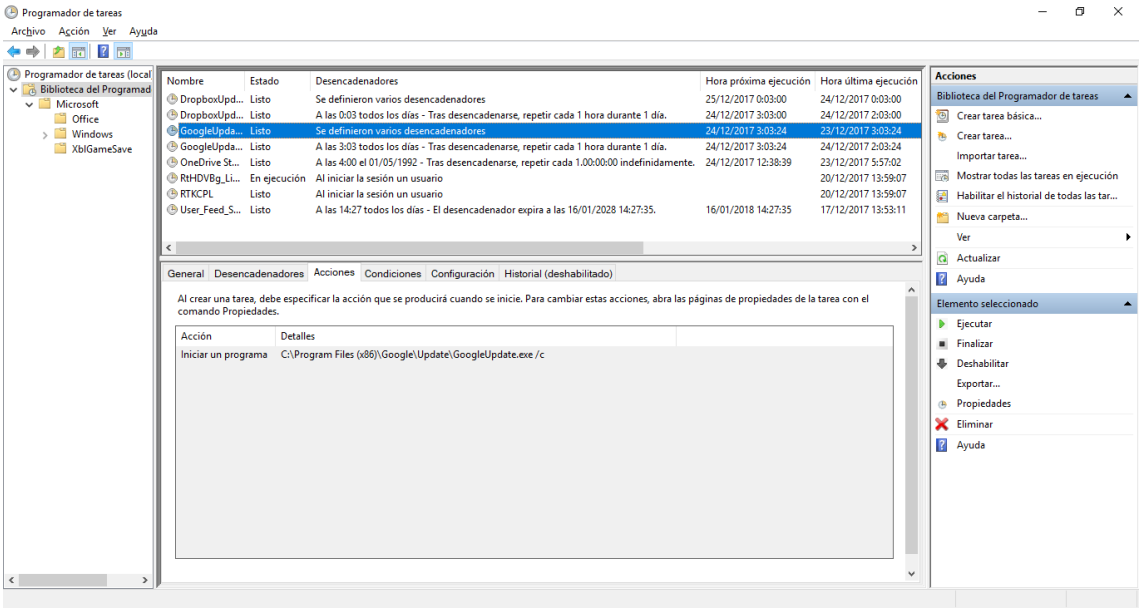

Esta aplicación corresponde al perfil de un atacante que intenta hacer pasar un ejecutable por un documento, con el fin de que el usuario lo abra confiando y resulte infectado por algún troyano o gusano.

Además de la aplicación anterior, en este listado volvemos a encontrar el mismo ejecutable que vimos en la evidencia sobre el inicio del sistema, haciéndose pasar por un actualizador de Google.




Que ejecuta un fichero exe localizado en \VOLUME{01d3477b3f5e68a2-de3f84c5}\USERS\IEUSER\APPDATA\LOCAL\GOOGLE\DESKTOP\INSTALL\{229F9A04-F317-A0E4-ACFD-F1EFB9E8AAA6}\❤⸸»\🔍〰\-DFCA-4E0A-713F-40A9F922{\ؤ EXE.ETADPUELGOOG\}6AAA8E9BFE1F

Si se busca información sobre el servicio de google update (en el caso de que haya algún software de esta compañía en el equipo) este debe encontrarse en C:\Program Files (x86)\Google\Update\




# Conclusión

A la luz de los hallazgos encontrados, podemos inferir que los acontecimientos son los siguientes:

1. El día 20 de Diciembre a las 0:17 hora local del ordenador (UTC), se ejecuta un fichero de origen en el disco local con el nombre INVOICE_2318362983713_823931342IO.PDF.EXE
2. Este fichero a su vez crea una carpeta y la oculta en el escritorio del perfil usuario, posiblemente descargando un payload que ofusca su actividad haciéndose pasar por un complemento de actualización de Google
3. También se crea una tarea programada que ejecuta el payload regularmente

El análisis de este payload lo identifica como un troyano de tipo ZBot, que ha infectado al equipo y ha estado ejecutándose desde la fecha en la que se abrió el supuesto fichero PDF.

# ZBot

Zeus, ZeuS, or Zbot es un malware de tipo troyano que infecta ordenadores con sistema operativo Windows, con el objetivo de robar credenciales bancarias u obtener otro tipo de información relevante. Además, los ordenadores infectados con este malware pasan a ser parte de una botnet, con lo que pueden ser utilizados para cometer acciones criminales o maliciosas.

Este troyano fue diseñado inicialmente para robar información confidencial de los ordenadores infectados, como por ejemplo la información del sistema, las credenciales de los usuarios y sus

datos bancarios. Sin embargo, debido a su alto grado de personalización puede adaptarse para recopilar cualquier tipo de información.

Además, los ordenadores infectados por Zeus son controlados mediante un servidor de comando y control (C&C) y que habilita la posibilidad de que los bots realicen funciones adicionales, como descarga y ejecución de archivos o modificar la configuración del sistema.

Históricamente, es reseñable decir que este botnet fue infiltrado en la red del FBI en 2010 a través de una campaña de correo dirigida a diferentes niveles de esta entidad de seguridad estadounidense.

# ANEXOS

Para evitar la excesiva longitud de este informe, y dado que las evidencias más importantes han sido incluidas en el apartado del informe, se adjuntarán los anexos correspondientes a las otras pruebas realizadas e información extraída en ficheros separados, siguiendo la nomenclatura que se indica en cada uno de los apartados.