2016

PROPUESTA DE METODOLOGÍA PARA EL ANÁLISIS FORENSE DE SISTEMAS INFORMÁTICOS WINDOWS.

TRABAJO FIN DE MASTER DE SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN.

Universitat Oberta de Catalunya (UOC), Universidad Autónoma de Barcelona (UAB), Rovira i Virgili

AUTOR: JOSÉ MARÍA AMUSATEGUI LÓPEZ

22/12/2016

ÍNDICE

1. INTRODUCCIÓN.

a. Objetivo

b. Extracto

c. Planificación

d. Contexto y normativa

e. Justificación y motivación

2. DISTRIBUCIONES Y HERRAMIENTAS ORIENTADAS AL ANÁLISIS FORENSE.

a. Resumen de distribuciones

b. Resumen de herramientas

3. TIPOLOGÍAS.

a. Tipo de análisis

b. Tipo de evidencia

c. Tipo de delito

4. METODOLOGÍA PROPUESTA.

i. PRESERVACION – IDENTIFICACION.

1. Asegurar la escena y recopilación de información física
2. Cadena custodia
3. Identificación de evidencias y su volatilidad
4. Transporte y manipulación de evidencias
5. Almacenamiento de evidencias

ii. RECOLECCION – ADQUISICION.

1. Consideraciones de privacidad
2. Consideraciones legales
3. Procedimiento de recolección de evidencias
    a. Equipo encendido
        Análisis de red
            TALLER 1. Análisis de red
        Volcado de memoria RAM
        Fecha y hora del sistema
        Histórico del intérprete de comandos
        Pagefile.sys e hiberfile.sys
        Árbol de directorios y ficheros

Historial de internet

Carpetas compartidas

Usuarios que han iniciado sesión y listado de cuentas

Procesos activos

Servicios en ejecución

b. Equipo apagado

TALLER2. Volcado de disco

4. Firmado y validación de copias – Hash

iii. ANALISIS.

1. Información volátil

TALLER 3. Análisis de memoria RAM - Malware

2. Información NO volátil

Disco duro

TALLER 4. Análisis de disco y "timeline" de archivos

Tabla MBR

Tabla MFT

Registro de Windows

TALLER 5. Registro de Windows

Análisis de Malware

TALLER 6. Análisis de malware "keylogger"

Ficheros y directorios importantes NTFS e instalación Windows

Archivos eliminados

Carpeta "prefetch"

Fichero hosts

Tareas programadas

Logs del sistema Windows

Análisis de metadatos

iv. REDACCIÓN DE INFORMES.

1. Informe ejecutivo
2. Informe técnico

5. BIBLIOGRAFÍA

1.- Introducción

1.a)- Objetivo:

El objetivo principal del presente TFM consiste en, mediante el estudio y recopilación actual de métodos y técnicas utilizadas para un análisis forense en entornos Windows, realizar una propuesta de estandarización para este tipo de análisis, buscando el camino más corto posible que a su vez, lleve a recolectar el mayor número posible de evidencias de un dispositivo, preservando siempre la integridad de las mismas.

Para ello, nos basaremos en las normas y estándares actuales que rigen dicha actividad, como son: ISO 27037 (serie ISO 27000:2014 en general), la RFC 3227 o las UNE 71505 y UNE 71506, así como el marco legal, tanto estatal (Español) como Internacional para la recolección, archivado, gestión y manipulación de evidencias digitales.

1.b)- Extracto:

Para el desarrollo del método expuesto en el presente TFM, basaremos el proceso en 4 fases definidas como:

1. **Preservación**: Primera fase, en la que se garantiza la preservación de las pruebas obtenidas para su posterior análisis.

2. **Adquisición**: Fase de recopilación de evidencias. Estas deben poseer las siguientes características: admisibles, auténticas, completas, creíbles y confiables. Se clasifican en dos grandes grupos: físicas y digitales.

3. **Análisis**: Fase en la que analizan en profundidad las pruebas obtenidas atendiendo a su tipología para lograr un análisis lo más exhaustivo posible.

4. **Documentación**: Fase fundamental donde recoger de forma detallada todo el proceso indicando fechas y horas de cada una de las acciones realizadas con las evidencias. La documentación más común en la cadena de custodia de las evidencias. La documentación del proceso y pruebas se recoge en dos informes, el ejecutivo y el técnico.

Se pretende establecer etapas estandarizadas para el análisis forense, diferenciando el árbol de etapas en función de posibles tipologías de ataques.

Como principal objetivo se buscará el camino más corto (con menos pasos) que lleve a recolectar el mayor número de pruebas posibles, siempre tratando de mantener la integridad de las evidencias de forma prioritaria.

Para el proceso de adquisición o recolección de evidencias, el presente TFM se basará en la RFC 3227, la cual trata los siguientes puntos:

- Principios para la recolección de evidencias
- Orden de volatilidad
- Acciones a evitar durante el proceso
- Consideraciones a la privacidad de datos
- Transparencia
- Procedimientos de recolección
- Legalidad
- Cadena de custodia
- Metodologías de almacenamiento de las evidencias

Uno de los aspectos más importantes Lo más importante a la hora de realizar un análisis forense es preservar la originalidad de la muestra, es decir, que esta no sufra modificaciones o alteraciones de ninguna de sus partes ni de su información obtenida debido a la manipulación por parte del analista. Para ello han de establecerse protocolos y firmas que corroboren su integridad y originalidad, así como asegurar la cadena de custodia y que tampoco sufra ningún tipo de modificación a posteriori, a lo largo del tiempo.

Cabe destacar que cualquier herramienta utilizada sobre la memoria volátil del dispositivo a utilizar analizando en caliente, provocará que parte de esta se sobrescriba o modifique, con la consiguiente pérdida de información que esto supone.

1.c)- Planificación:

Metodología TFM: Estado del arte y recopilación de información para su posterior redacción como TFM, identificando y detallando sus diferentes fases (resumidas en el próximo punto), así como video explicativo sobre el TFM y su seguimiento.

Listado de tareas

- Estado del arte y recopilación de información de diferentes fuentes disponibles.
- Redacción del extracto e índice a seguir.
- Estudio sobre herramientas específicas.

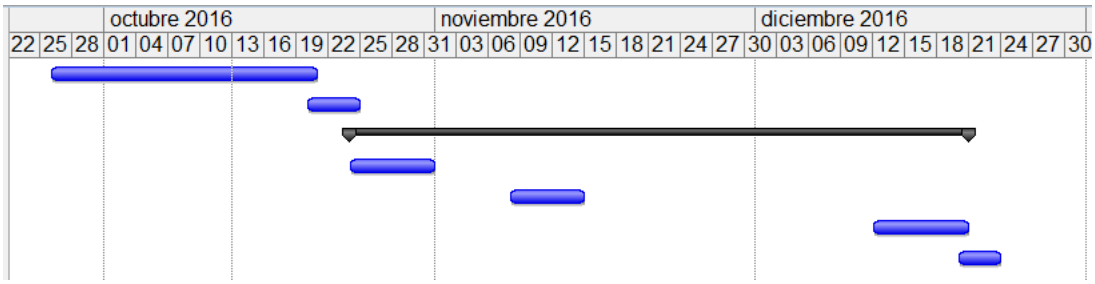
- Taller para puesta en práctica.
- Redacción de contenido teórico.
- Maquetado de teoría + imágenes o gráficos sobre la puesta en práctica y/o demostraciones.
- Realización de video explicativo.

Planificación temporal detallada

- *Estado del arte y recopilación de información de diferentes fuentes disponibles. (20/10/16)*
- *Redacción del extracto e índice a seguir. (20/10/16)*
- *Estudio sobre herramientas específicas. (24/10/16)*
- *Taller para puesta en práctica. (8/11/16)*
- *Redacción de contenido teórico. (13/10/2016 a 9/12/16)*
- *Maquetado de teoría + imágenes o gráficos sobre la puesta en práctica y/o demostraciones. (12/12/16)*
- *Realización de video explicativo. (20/12/16)*

GANTT:

	Nombre de tarea	Duración	Comienzo	Fin
1	Estado del arte y recopilación de información de diferentes fuentes disponibles	19 días?	lun 26/09/16	jue 20/10/16
2	Redacción del extracto e índice a seguir	3 días?	jue 20/10/16	lun 24/10/16
3	**Redacción de contenido teórico**	**42 días?**	**lun 24/10/16**	**mar 20/12/16**
4	Estudio sobre herramientas específicas	6 días?	lun 24/10/16	lun 31/10/16
5	Taller para puesta en práctica	5 días?	mar 08/11/16	lun 14/11/16
6	Maquetado de teoría + imágenes o gráficos sobre la puesta en práctica y/o	7 días?	lun 12/12/16	mar 20/12/16
7	Realización de video explicativo	4 días?	mar 20/12/16	vie 23/12/16



1.d)- Contexto y normativa

El papel de la tecnología en un delito puede darse desde ciertos dispositivos involucrados en un delito hasta ser el propio canal a través del cual se comete el delito. Así mismo, el equipo a analizar puede pertenecer a la víctima o al delincuente.

El análisis forense puede ser utilizado para, gracias al análisis del dispositivo, determinar qué es lo que ha ocurrido.

En este proyecto se pretende desarrollar una guía práctica para el análisis forense de delitos informáticos. La necesidad de la creación de la misma surge ante la falta de normalización y/o estandarización común para este tipo de análisis. Podemos encontrar diferentes trabajos, propuestas y documentos en general, que tratan de recopilar pautas para llevar a cabo una correcta investigación, en este trabajo se recopilarán las más relevantes de todas ellas.

Por este motivo, es oportuno crear una metodología única y definitiva que estandarice los pasos a seguir para realizar un análisis forense meticuloso y de éxito. Teniendo en cuenta todas las premisas de seguridad, las recomendaciones y los estándares ya existentes.

Varias organizaciones han desarrollado documentación al respecto, en las que recogen pautas y consejos para llevar a cabo cierta parte de la investigación. A pesar de ello, seguir esta documentación no supone ninguna garantía ante un tribunal se certifique al 100% la tarea realizada por el analista ni son de aplicación obligatoria. Algunas de ellas contienen directrices e indicaciones que nos serán de utilidad y en las que se basará este trabajo, es el caso de la RFC 3227, serie ISO 27000:2014 y las normas UNE 71505 y UNE 71506, así como el marco legal, tanto estatal (Español) como Internacional para la recolección, archivado, gestión y manipulación de evidencias digitales.

Algunas de las organizaciones que han contribuido son:

- **Engineering Task Force (IETF)**

  The Internet Engineering Task Force (IETF). (https://www.ietf.org)
- **Asociación Española de Normalización y Certificación (AENOR)**

  Asociación Española de Normalización y Certificación. (www.aenor.es)
- **Organización Internacional para la Estandarización (ISO)**

  International Organization for Standardization. (www.iso.org)
- **Cuerpos del estado**
  - Association of Chief Police Officers. [En línea] www.acpo.police.uk.
  - National Criminal Justice Reference Service. (https://www.ncjrs.gov)
- **Departamentos de Justicia (5) de varios países proponen varios documentos**
  - Martínez Retenaga, Asier. Guía de toma de evidencias en entornos Windows: Instituto Nacional de Ciberseguridad, Noviembre 2014.
  - Forensic Examination of Digital Evidence: A Guide for Law Enforcement. 2004.
  - Good Practice Guide for Computer-Based Electronic Evidence.

Entre las contribuciones a propuestas sobre metodologías existentes podemos destacar:

- **Metodología del Departamento de Justicia de Estados Unidos**

El modelo pretende construir un modelo de análisis general que pueda ser aplicado a diferentes dispositivos electrónico, es decir, sin hacer distinción entre si el dispositivo es móvil o PC o en la plataforma o SO utilizados.

- Ventajas:
  - Incluye un diagrama de flujo a seguir para cada una de las etapas. Muy bien definido y claro.
- Desventajas:
  - No cubre la totalidad de las etapas de un análisis forense
  - Se enfoca en SO Windows
  - No establece una cadena de custodia
  - No propone métodos para realizar adquisición de grandes volúmenes de datos
  - No propone métodos de análisis para grandes volúmenes de datos

- **Metodología del Instituto SANS**

El instituto SANS es una organización cooperativa de investigación y educación para profesionales especialistas en seguridad. El manejo adecuado de una investigación es clave para luchar contra la ciber-delincuencia, requiriendo un profundo conocimiento de diversas áreas para poder llevar a cabo una investigación adecuada.

- Ventajas
  - Incluye formatos para establecer la cadena de custodia
  - Define directorios con posible información oculta en Windows y Linux
  - Cubre todas las etapas de una investigación forense
- Desventajas:
  - No propone métodos para realizar adquisición de grandes volúmenes de datos
  - No propone métodos de análisis para grandes volúmenes de datos

- **Digital Forensics Workshop (DFRW)**

Se trata de un grupo que ayuda a definir y enfocar la dirección de la comunidad científica en relación al análisis forense digital.

- Ventajas:
  - Define directorios con posible información oculta en Windows y Linux

        - Provee métodos y actividades para la localización y extracción de información oculta.
        - Cubre todas las etapas de una investigación forense
        - Define todo el universo de dispositivos y plantea formas que puedan ser analizadas dentro de una investigación de cómputo forense.
        - Enfocada a conservar la integridad.
        - Considera métodos para el análisis de grandes volúmenes.
    - Desventajas:
        - No propone un procedimiento específico para la realización de las actividades.

Legislación vigente

Todo profesional de la informática forense debe conocer la legislación vigente a las que se someten sus actividades en el país que ejerza su profesión. Comprendiendo hasta donde pueden llegar sus investigaciones, repercusiones legales sobre ciertas actuaciones y ser consciente de todas ellas para cumplirlas en todo momento durante el proceso de investigación forense, así como identificar correctamente los delitos a estudiar o analizar.

Derechos relativos a la dignidad de la persona humana:

- Derecho a la seguridad jurídica y tutela judicial, la cual nos garantiza un proceso penal con garantías de derecho.
- Derecho al secreto de las comunicaciones.
- Derecho a la vida privada. En este derecho se incluye el derecho a la intimidad, una vida privada, derecho al honor y a la propia imagen. Así como la limitación del uso de la informática para proteger la intimidad.

- Derecho fundamental a la protección de datos.

Constitución Española

Se compone de los siguientes 5 documentos:

- Ley de Enjuiciamiento Civil
- Ley de Protección de Datos de Carácter Personal
- Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.
- Ley de Conservación de Datos Relativos a las Comunicaciones y Redes Públicas.
- Código Penal.

A continuación se comentará el resumen de cada una de ellas:

1. Ley de Enjuiciamiento Civil

Esta Ley establece el marco legal, mediante el cual se regulan los procesos civiles, los tribunales y quienes en ellos intervienen.

2. Ley de Protección de Datos de Carácter Personal

Su propósito es el de regular los datos de carácter personal, redactada en 1999.

Define al responsable del fichero como la persona con el máximo poder sobre este y que deberá seguir unos principios para garantizar la privacidad de los datos. El poseedor de los datos, deberá registrar unas mínimas garantías de seguridad para que los datos contenidos en el fichero no sean públicos y deberá garantizar que se eliminan los datos cuando el titular así lo requiera y siempre que la Ley permita dicha eliminación.

Se detallan tres niveles de seguridad, básico, medio y alto.

- **Básico:** Cualquier sistema con datos personales.
- **Medio:** Incluye los datos del nivel básico, además de los datos sobre comisión de infracciones administrativas o penales, crédito, hacienda pública, servicios financieros, solvencia patrimonial, etc.
- **Alto:** Todos los datos del nivel medio, además de los datos sobre ideología, religión, creencias, origen racial, salud o vida sexual, recabados para fines policiales y violencia de género.

3. Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico

Redactada y aprobada en 2001, la LSSICE regula y protege las relaciones contractuales que se llevan a cabo en Internet.

Obliga a aquellos quienes prestan servicios en Internet a identificarse de modo claro y accesible de modo que la parte contratante sepa en todo caso con quien está negociando.

La presente Ley también prohíbe las comunicaciones no deseadas de publicidad, como por ejemplo el "*spam"*, entre muchas otras formas existentes.

4. Ley de Conservación de Datos Relativos a las Comunicaciones y las Redes Públicas

Con dicha Ley el legislador pretende conservar datos que puedan ser relevantes para rastrear actividades ilícitas y mejorar de esta forma la seguridad de los ciudadanos frente a actividades terroristas.

Los datos que se retienen se dividen en tres categorías, telefonía fija, telefonía móvil y acceso a Internet. Estos datos deben ser todos los necesarios para la trazabilidad de origen a destino de cualquier comunicación telemática.

La conservación de los datos por parte de los prestadores de servicio finaliza a los doce meses de la comunicación. A pesar de que en casos concretos este periodo temporal oscila entre los seis meses y los dos años.

5. Código Penal

El Código Penal concentra aquellas actitudes que se consideran delito en España.

Además de la regulación legislativa estatal que se ha repasado cabe destacar la regulación y propuestas de regulación a nivel europeo sobre aspectos informáticos y que son de igual interés para el profesional de este ámbito.

A continuación se detallan dos directivas del Parlamento Europeo y del Consejo:

Directiva 2006/24/CE

Esta directiva trata sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

En cuando a la información sobre la que trata se centrará en los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. En cambio no se aplicará al propio contenido de las comunicaciones electrónicas ni grabaciones de las mismas.

Directiva 2013/40/UE

Directiva que establece las normas mínimas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información.

Por otra parte, también tiene como fin facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes. Incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciber-delincuencia y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

Normativas y estándares del sector

En este capítulo se repasarán algunas de las normativas y estándares, tanto a nivel nacional como internacional, más relevantes. Por un lado la RFC 3227 y por otro lado la ISO 27037 y las UNE 71505 y UNE 71506. Se tratan de estándares actualmente vigentes más importantes y de los que se hará uso en este trabajo como bibliografía base para la elaboración de la propuesta de metodología para el análisis forense de sistemas informáticos con sistema operativo Windows son.

ISO 27037

Dentro de la seguridad informática cabe destacar una normativa muy conocida, se trata de la familia ISO 27000. Esta serie de normas incluye estándares de seguridad publicados por la

Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Contiene mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

En concreto, dentro de esta serie podemos encontrar una norma dedicada en exclusiva al análisis forense, se trata de la ISO 27037. Para la selección, preservación y adquisición de evidencias se adoptarán como base los conceptos del estándar internacional **ISO/IEC 27037** (*Information Technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence)*.

La norma ISO/IEC 27037 define las siguientes etapas con las respectivas recomendaciones en detalle:

- Identificación.
- Recolección.

- Adquisición.
- Preservación.

El estándar ISO 27037 define dos actores muy importantes dentro de un proceso forense informático:

- **DEFR (Digital Evidence First Responders):** Expertos en primera intervención de evidencias electrónicas. A cargo de las etapas de identificación, recolección y adquisición
- **DES (Digital Evidence Specialists):** Experto en gestión de evidencias electrónicas. Especialista de evidencia digital, es el encargado de continuar con las etapas de preservación, análisis y reporte.

Proporciona orientación para los siguientes dispositivos y circunstancias:

- Medios de almacenamiento digitales utilizados en equipos varios como por ejemplo discos duros, disquetes, discos magneto-ópticos y ópticos y otros similares.
- Teléfonos móviles, PDA's, tarjetas de memoria.
- Sistemas de navegación móvil (GPS).
- Cámaras de video y cámaras digitales (incluyendo circuitos cerrados de televisión).
- Ordenadores estándares con conexiones a redes.
- Redes basadas en protocolos TCP/IP y otros protocolos digitales.
- Otros dispositivos con funcionalidades similares a las descritas anteriormente.

UNE 71505 y UNE 71506

Se trata de dos normas publicadas por la Asociación Española de Normalización y Certificación, cuya finalidad consiste en proporcionar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Estas normas contribuyen a homogeneizar la gestión de las evidencias electrónicas y establecen un marco de referencia de buenas prácticas que contribuye a mejorar la admisibilidad de las pruebas electrónicas en procesos jurisdiccionales siempre que los peritos adopten sus postulados.

La UNE 197001:2011 establece la estructura y los requisitos mínimos de contenido de un dictamen o informe pericial.

La UNE 71506:2013, "Metodología para el análisis forense de las evidencias electrónicas", refleja una visión práctica del análisis forense digital.

RFC 3227

Se trata de un RFC (Request For Comments), documento en el que se recogen propuestas de expertos en una materia concreta.

RFC 3227 es uno de los referentes en cuanto a normativas aplicadas al análisis forense de sistemas informáticos, consiste en un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento.

Estos son los puntos más importantes relacionados con dicho proceso:

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.

Conforme a las pautas establecidas en el RFC 3227, se puede crear la siguiente escala de volatilidad, de mayor a menor:

- 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.

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 para 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.
- 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.

3. Consideraciones sobre la privacidad

- Es muy importante tener en consideración las pautas de la empresa en lo que a privacidad se refiere. Es habitual solicitar una autorización por escrito de quien corresponda para poder llevar a cabo 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 la empresa, o que la disponibilidad de los servicios se vea afectada.
- No hay que entrometerse en la privacidad de las personas sin una justificación. No se deben recopilar datos de lugares a los que normalmente no hay razón para acceder, como ficheros personales, a menos que haya suficientes indicios.

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.

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.

El procedimiento de almacenamiento:

1 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.

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.

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 haber sido comprometidas, principalmente en los casos de malware.
- Se debe procurar utilizar herramientas que alteren lo menos posible el escenario, evitando el uso de herramientas de interfaz gráfico y aquellas que hagan un amplio uso de memoria.
- Los programas que se vayan a utilizar para recolectar las evidencias deben estar ubicados en un dispositivo de sólo lectura, para evitar modificaciones de las pruebas.
- El kit de análisis debe incluir 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.

1.e)- Justificación y motivación

Debido a la falta de estandarización hasta la fecha de una estructura que englobe todo tipo de casos en el análisis forense (para este trabajo en particular entornos Windows) este trabajo pretende dar a conocer una posibilidad lo más completa y actualizada posible para dicho fin.

2. Distribuciones y herramientas orientadas al Análisis Forense

2.2. Resumen de distribuciones

Existen distribuciones destinadas a varias fases dentro de un análisis forense. El ejemplo más claro podemos encontrarlo en CAINE, distribución basada en Linux y ampliamente orientada al análisis forense, en ella podemos encontrar incluidas herramientas utilizadas en el análisis de discos e imágenes, hash, “timelines”, recuperación de datos eliminados, bases de datos, forense móvil, forense red y otros. Algunos ejemplos de aplicaciones incluidas son: Autopsy, foremost, photorec, Fundl, scalpel, testdisk, cryptcat, TheSleuthKit, gparted, md5sum, sha256sum, sha512sum, etc.

CAINE (Computer Aided INvestigative Environment):

Se trata de una distribución GNU/Linux basada en Ubuntu y cuenta con el entorno de escritorio MATE. Los principales objetivos de esta distribución consisten en crear un ambiente interoperable de forma que se apoye al analista durante las fases de la investigación.

Incluye esta vez una herramienta destinada al análisis en vivo de sistemas Windows llamada Win-UFO (Windows - Ultimate Forensic Outflow), que proporcionando un gran conjunto de herramientas útiles separadas en varias categorías.

Para cerciorar el montaje seguro de dispositivos, se han incluido dos utilidades:

- *rbfstab*: se activa automáticamente durante el arranque del sistema o al conectar un dispositivo, de modo que escribe entradas en el archivo /etc/fstab para que los dispositivos sean montados de forma segura en modo de solo lectura
- *mounter*: es una herramienta de montaje con GUI situada en la barra de tareas, desde la cual se podrán seleccionar los dispositivos que se deseen. También permite cambiar la política de montaje con click derecho del ratón sobre el icono del programa

Además de **CAINE**, existen distribuciones o "live CD's", la mayoría basadas en Linux orientadas al análisis forense informático, pasaremos a mencionar algunas de las más conocidas:

DEFT (Digital Evidence & Forensic Toolkit):

La distribución DEFT (Digital Evidence & Forensic Toolkit), basada en Lubuntu y cuya primera versión data de 2005, es actualmente mantenida y desarrollada por Stefano Fratepietro, con el apoyo de Alessandro Rossetti, Massimiliano Dal Cero, Paolo Dal Checco, Valerio Leomporra, Davide Gabrini, Marco Giorgi y Nicodemo Gawronski.

Incluye la suite de aplicaciones DART (Digital Advanced Response Toolkit), destinada a sistemas operativos Windows.

Cuenta con una serie de características destinadas a asegurar la integridad de las posibles evidencias sometidas a análisis. Dichas características son:

- En el arranque, el sistema no hace uso de las particiones swap
- Durante el arranque del sistema, no hay scripts de montaje automáticos
- No hay sistemas automatizados para ninguna actividad durante el análisis de la evidencia
- Todas las herramientas de adquisición de almacenamiento masivo y de tráfico de red no alteran los datos que estuvieran siendo adquiridos

DEFT puede ser utilizado desde sistemas que dispongan de lector de CD/DVD-ROM o puerto USB, con arquitectura x86 y un mínimo de 64 MB de memoria RAM si se quiere arrancar en modo texto o 128 MB si se opta arrancar con la interfaz gráfica de usuario (GUI), en cuyo caso el entorno de escritorio Lightweight X11 Desktop Environment (LXDE) será el utilizado.

Algunas de las herramientas más importantes incorporadas son:

- Explorador de archivos con estado de montaje de disco
- Soporte a discos encriptados con Bitlocker
- The Sleuth Kit
- Digital Forensics Framework
- JD-GUI
- Skype Xtractor
- Maltego

Y otras como Matriux, SIFT (SANS Investigative Forensic Toolkit), NETSECL, Kali Linux, Backtrack, Santoku Linux o Backbox, entre otras.

Además de distribuciones "live", podemos encontrar herramientas y suites (fuera de distribuciones específicas) para su instalación sobre sistemas operativos, con las que realizar diferentes fases dentro del marco de un análisis forense. Uno de los ejemplos más destacados es "Sleuth Kit" o su interfaz de usuario para línea de comandos "Autopsy", esta herramienta de análisis de investigación digital puede analizar los discos de Windows y UNIX, así como imágenes y sistemas de archivos (NTFS, FAT, UFS1 / 2, Ext2 / 3). Permite listar archivos, ver contenido del archivo, comparar archivos creados por el usuario o bases de datos, tipo de archivos, realizar búsquedas de palabras clave, análisis de metadatos. Notas sobre el caso, Imagen de verificación de integridad, Creación de informes, de Auditoría Registro de investigación. Es útil a la hora de analizar un disco de evidencia, modificados, correos enviados, tipo de sistema operativo, entre otros.

Una parte de las herramientas que voy a citar en esta práctica pueden encontrarse tanto para Linux como Windows, no obstante existen herramientas específicas para cada uno de estos sistemas, encontrando un mayor abanico de aplicaciones para sistemas basados en Unix/Linux.

Además de las distribuciones anteriormente mencionadas (que incluyen gran cantidad de herramientas), podemos encontrar las herramientas o "suites" por separado para utilizarlas en nuestro propio sistema operativo o montarnos un sistema propio con aplicaciones preinstaladas para realizar análisis forenses informáticos, móviles o de telecomunicación.

2.1. Resumen de herramientas

A continuación se enumeran herramientas destinadas a ciertos procesos del análisis forense:

Herramientas de disco y recuperación de datos

- **Photorec, Foremost, Magicrescue, ddrescue, Freerecover, Restoration, Scalpel y Recuva**: Destinadas al análisis de ficheros eliminados en imágenes de discos, memorias USB, discos físicos, etc... Con ellas podemos obtener estos ficheros para su posterior análisis, así como realizar recuperaciones de ficheros cifrados o sectores de disco corruptos. También permiten analizar las tablas de formato de los mismos e incluso reestructurarlas., búsqueda de patrones y ficheros con contenido determinado como por ejemplo imágenes, vídeos. Recuperación de particiones y tratamiento de estructuras de discos.
- Herramienta DD: Clonado de disco
- Autopsy: (Explicado anteriormente)
- Guymanager: Creación de imágenes de disco en diversos formatos (RAW (o .dd) como más habitual).
- TestDisk
- RecoverRS – Recupera urls de acceso a sitios web y ficheros.
- NTFS Recovery – Permite recuperar datos y discos aun habiendo formateado el disco.
- Raid Reconstructor – Recuperar datos de un RAID roto, tanto en raid 5 o raid 0. Incluso si no conocemos los parámetros RAID.
- CNWrecovery – Recupera sectores corruptos.
- Rstudio – Recuperación de datos de cualquier sistema de disco NTFS, NTFS5, ReFS, FAT12/16/32, exFAT, HFS/HFS+ (Macintosh), Little y Big Endian en sus distintas variaciones UFS1/UFS2 (FreeBSD/OpenBSD/NetBSD/Solaris) y particiones Ext2/Ext3/Ext4 FS.
- DMDE – Admite FAT12/16, FAT32, NTFS, y trabaja bajo Windows 98/ME/2K/XP/Vista/7/8 (GUI y consola), DOS (consola), Linux (Terminal) e incorpora utilidades de carving.
- IEF – Internet Evidence Finder Realiza carving sobre una imagen de disco buscando más de 230 aplicaciones como chat de Google, Facebook, IOS, memoria RAM, memoria virtual, etc.
- Bulk_extractor – Permite extraer datos desde una imagen.

Procesos y registro

- Proccess explorer: Muestra información de los procesos activos en el sistema.
- LordPE: Herramienta para editar ciertas partes de los ejecutables y volcado de memoria de los procesos ejecutados.
- Regshot: Crea snapshots del registro pudiendo comparar los cambios entre ellos

Utilidades para el sistema de ficheros Windows

- analyzeMFT - Utilidad en python de David Kovar's que permite extraer la tablaMFT y parsearla.
- MFT Extractor- Otra utilidad para la extracción de la tabla MFT.
- INDXParse - Herramienta para los índices y fichero $I30.
- MFT Tools (mft2csv, LogFileParser, etc.) Conjunto de utilidades para el acceso a la tabla MFT
- MFT_Parser - Extrae y analiza la MFT
- Prefetch Parser - Extrae y analiza el directorio prefetch
- Winprefectchview - Extrae y analiza el directorio prefetch
- Fileassassin - Desbloquea ficheros bloqueados por los programas

Memoria RAM

- pd Proccess Dumper: Convierte y guarda un proceso de la memoria a fichero.
- FTK Imager: Permite entre otras cosas volcar la memoria.
- Volatility: Analiza procesos y volcado de información volátil. Se basa en el uso de "plugins" para recopilación de información específica de un sistema o imagen, en este caso imagen de volcado de memoria RAM volátil.

  Un listado de comandos y plugins posibles a utilizar se encuentra en el Github del proyecto Volatilityfundation:

  https://github.com/volatilityfoundation/volatility/wiki/Volatility-Usage

  https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

  Además de estos, cabe la posibilidad de instalar plugins externos para hacer uso de ellos en Volatility.

  - Sus principales plugins son:

    apihooks Detect API hooks in process and kernel memory
    atoms Print session and window station atom tables
    atomscan Pool scanner for _RTL_ATOM_TABLE
    bioskbd Reads the keyboard buffer from Real Mode memory
    callbacks Print system-wide notification routines
    clipboard Extract the contents of the windows clipboard
    cmdscan Extract command history by scanning for _COMMAND_HISTORY
    connections Print list of open connections [Windows XP and 2003 Only]
    connscan Scan Physical memory for _TCPT_OBJECT objects (tcp connections)
    consoles Extract command history by scanning for _CONSOLE_INFORMATION
    crashinfo Dump crash-dump information
    deskscan Poolscaner for tagDESKTOP (desktops)
    devicetree Show device tree

```
dlldump         Dump DLLs from a process address space
dlllist         Print list of loaded dlls for each process
driverirp       Driver IRP hook detection
driverscan      Scan for driver objects _DRIVER_OBJECT
envars          Display process environment variables
eventhooks      Print details on windows event hooks
evtlogs         Extract Windows Event Logs (XP/2003 only)
filescan        Scan Physical memory for _FILE_OBJECT pool allocations
gahti           Dump the USER handle type information
gditimers       Print installed GDI timers and callbacks
gdt             Display Global Descriptor Table
getservicesids  Get the names of services in the Registry and return
Calculated SID
getsids         Print the SIDs owning each process
handles         Print list of open handles for each process
hashdump        Dumps passwords hashes (LM/NTLM) from memory
hibinfo         Dump hibernation file information
hivedump        Prints out a hive
hivelist        Print list of registry hives.
hivescan        Scan Physical memory for _CMHIVE objects (registry
hives)
idt             Display Interrupt Descriptor Table
imagecopy       Copies a physical address space out as a raw DD image
imageinfo       Identify information for the image
impscan         Scan for calls to imported functions
kdbgscan        Search for and dump potential KDBG values
kpcrscan        Search for and dump potential KPCR values
ldrmodules      Detect unlinked DLLs
lsadump         Dump (decrypted) LSA secrets from the registry
malfind         Find hidden and injected code
memdump         Dump the addressable memory for a process
memmap          Print the memory map
messagehooks    List desktop and thread window message hooks
moddump         Dump a kernel driver to an executable file sample
modscan         Scan Physical memory for _LDR_DATA_TABLE_ENTRY
objects
modules         Print list of loaded modules
mutantscan      Scan for mutant objects _KMUTANT
patcher         Patches memory based on page scans
printkey        Print a registry key, and its subkeys and values
procexedump     Dump a process to an executable file sample
procmemdump     Dump a process to an executable memory sample
pslist          Print all running processes by following the EPROCESS lists
psscan          Scan Physical memory for _EPROCESS pool allocations
pstree          Print process list as a tree
psxview         Find hidden processes with various process listings
raw2dmp         Converts a physical memory sample to a windbg crash
dump
screenshot      Save a pseudo-screenshot based on GDI windows
sessions        List details on _MM_SESSION_SPACE (user logon
sessions)
shimcache       Parses the Application Compatibility Shim Cache
```

registry key
sockets Print list of open sockets
sockscan Scan Physical memory for _ADDRESS_OBJECT objects (tcp sockets)
ssdt Display SSDT entries
strings Match physical offsets to virtual addresses (may take a while, VERY verbose)
svcscan Scan for Windows services
symlinkscan Scan for symbolic link objects
thrdscan Scan physical memory for _ETHREAD objects
threads Investigate _ETHREAD and _KTHREADs
timers Print kernel timers and associated module DPCs
userassist Print userassist registry keys and information
userhandles Dump the USER handle tables
vaddump Dumps out the vad sections to a file
vadinfo Dump the VAD info
vadtree Walk the VAD tree and display in tree format
vadwalk Walk the VAD tree
volshell Shell in the memory image
windows Print Desktop Windows (verbose details)
wintree Print Z-Order Desktop Windows Tree
wndscan Pool scanner for tagWINDOWSTATION (window stations)
yarascan Scan process or kernel memory with Yara signatures

- RedLine: Entorno gráfico para la captura memoria y análisis de la misma.
- Memorize: Volcado de RAM para Windows y OSX.
- DumpIt: Realiza volcados de memoria a fichero.
- Responder CE: Captura la memoria volátil y permite analizarla.

Protocolos de red

- WireShark: Herramienta para la captura y análisis de tráfico de red.
- NetworkMiner: Herramienta enfocada a descubrimiento de información de red.
- Network Appliance Forensic Toolkit: Conjunto de utilidades para la adquisición y análisis de la red.
- Xplico: Extrae todo el contenido de datos de red (archivo con extensión .pcap o adquisición en tiempo real). Es capaz de extraer todos los correos electrónicos que llevan los protocolos POP y SMTP, y todo el contenido realizado por el protocolo HTTP.
- Netstat y Nbstat: Análisis de red para Windows.
- Snort: Detector de intrusos y captura de paquetes para su análisis.
- Splunk: Motor para los datos y “logs” que generan los dispositivos, puestos y servidores. Indexa y aprovecha los datos generados por todos los sistemas e infraestructura de IT: ya sea física, virtual o en la nube.

Programas ejecutables y documentos

- PDFStreamDumper: Esta es una herramienta gratuita para el análisis PDFs maliciosos.
- IDA Pro: Depurador de aplicaciones.
- Captura BAT: Permite la monitorización de la actividad del sistema o de un ejecutable.
- OllyDbg: Desemsamblador y depurador de aplicaciones o procesos.
- OfficeMalScanner: Búsqueda de fichores de Office maliciosos.
- Bintext: Extrae el formato ASCII de un fichero.

Análisis de Malware

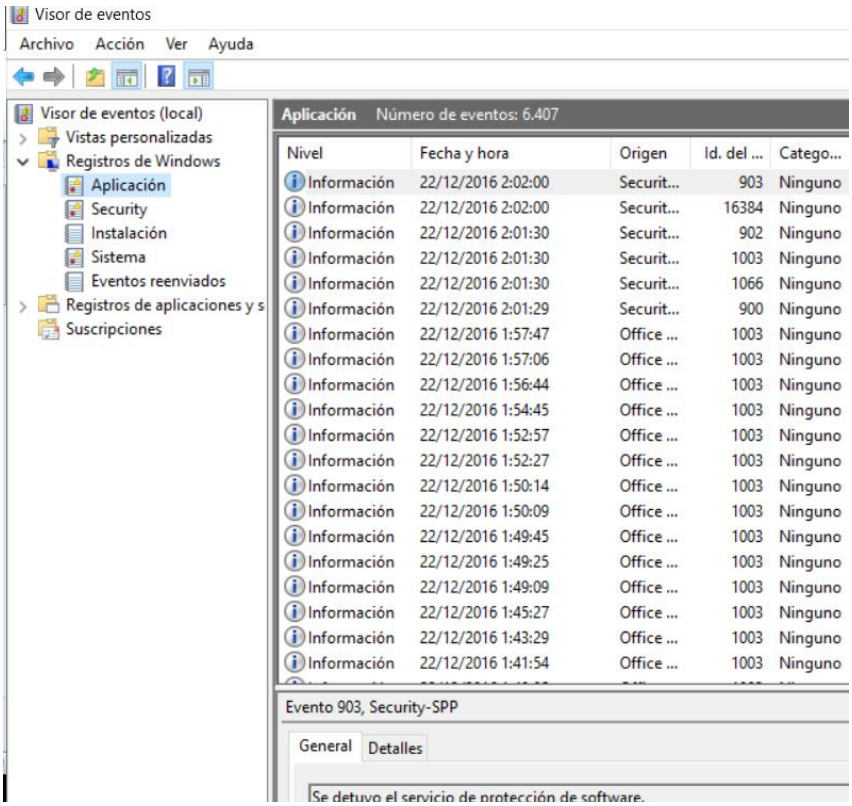
- OllyDbg: Desemsamblador y depurador de aplicaciones o procesos procesos para Windows. Carga y permite realizar "debugs" de DLLs, ejecutables y escaneo de todo tipo de archivos. No requiere instalación así que no creará nuevas entradas en el registro de la máquina donde se instala.
- PDFStreamDumper - Esta es una herramienta gratuita para el análisis PDFs maliciosos.
- Proccess explorer - Muestra información de los procesos.
- Captura BAT - Permite la monitorización de la actividad del sistema o de un ejecutable.
- Regshot - Crea snapshots del registro pudiendo comparar los cambios entre ellos
- Bintext - Extrae el formato ASCII de un ejecutable o fichero.
- LordPE - Herramienta para editar ciertas partes de los ejecutables y volcado de memoria de los procesos ejecutados.
- Firebug - Análisis de aplicaciones web.
- IDA Pro - Depurador de aplicaciones.
- Jsunpack-n - Emula la funcionalidad del navegador al visitar una URL. Su propósito es la detección de exploits
- OfficeMalScanner - Es una herramienta forense cuyo objeto es buscar programas o ficheros maliciosos en Office.
- Radare - Framework para el uso de ingeniería inversa.
- FileInsight - Framework para el uso de ingeniería inversa.
- Volatility Framework con los plugins malfind2 y apihooks.
- shellcode2exe - Conversor de shellcodes en binarios

Frameworks o suites

- PTK – Busca ficheros, genera hash, dispone de “rainbow tables”. Analiza datos de un disco ya montado.
- Log2timeline – Marco para creación de línea temporal.
- Plaso – Evolución de Log2timeline. Framework para la creación automática de líneas de tiempo.
- OSForensics – Busca ficheros, genera hash, dispone de rainbow tables. Analiza datos de un disco ya montado. Puede utilizarse desde un medio extraíble USB de forma portable.
- Autopsy – Muy completo. Reescrito en java totalmente para Windows, multiplataforma. Utilizado para análisis de imágenes de disco y ficheros.
- Suite Sysinternals de Microsoft: Una de las suites más completas para el análisis de entornos Windows, incluye herramientas para todo tipo de análisis principalmente en caliente para un análisis completo del sistema.

Además de las herramientas anteriormente citadas, se pueden usar otras herramientas, incluso herramientas nativas de Windows para obtener información sobre el sistema, procesos activos y demás información de utilidad como se puede observar a continuación:

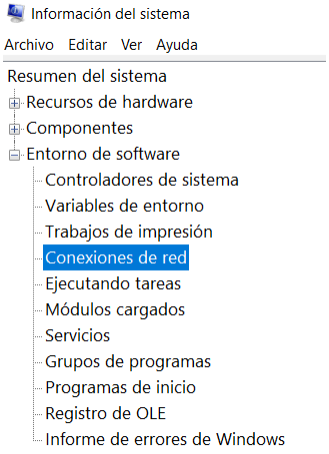
Una de las Herramientas nativas para obtener información detallada de los programas, accesos al equipo, instalaciones, etc. chequear el comportamiento del sistema es **eventvwr** (visor de eventos).



Mediante la herramienta **Tasklist**, se obtendrá un detalle de las tareas que se están ejecutando en el sistema. Cabe destacar que mediante el comando "taskkill" se puede matar cualquier tarea que este ejecutando.

Mediante la herramienta **Systeminfo** se obtiene una gran cantidad de información del equipo, desde la versión de sistema, ubicación de las carpetas principales de Windows, fecha de instalación del sistema, dominio, etc.

Mediante la herramienta **msinfo32** se pueden ver datos de configuración de hardware y software y diversa información del sistema.



3. TIPOLOGIAS

Con el fin de diseccionar los diferentes supuestos que pueden darse en cada caso forense, durante este capítulo se definirán diferentes tipos de análisis, evidencias y delitos o incidentes.

a. Tipo de análisis:

En este punto se describirán principalmente dos tipos de análisis: En frio y en caliente, dependiendo si al llegar a la escena a investigar la máquina se encuentra en estado apagado o encendido respectivamente, no obstante, también se hará hincapié en el análisis de red, del que se realiza un taller en esta propuesta de guía más adelante.

b. Tipo de evidencia:

Existen diferentes tipos de datos en el marco del análisis forense (sistemas de archivos, sistemas operativos, ficheros de diferentes extensiones…). Para este trabajo nos centraremos en entornos con sistema operativo Windows.

Diferenciaremos entre dos tipos principales de evidencias:

Evidencias volátiles y no volátiles

Para llevar a cabo este trabajo, se debe conocer la volatilidad de las pruebas, identificando su prioridad de forma correcta para su posterior orden de recolección, haciendo uso de la RFC 3227.

Entendemos por volatilidad de los datos a cierta información que tiene la propiedad de cambiar o transformarse de forma constante en el tiempo y poco predecible, incluso llegar a desaparecer.

Se trata de información que tiene la propiedad de cambiar o transformarse de forma constante en el tiempo y poco predecible, incluso llegar a desaparecer.

Este tipo de información (o evidencias si se aplica a un caso de análisis forense), son los que se pueden obtener a partir de un análisis en caliente del dispositivo o máquina, sin embargo no es posible obtenerlos a través de un análisis en frio.

Como ejemplo, algunos de los tipos pueden ser: caché del sistema, registros, conexiones, procesos activos o archivos temporales entre otros.

El tipo de evidencia que se nos presente cambiará la forma de actuación sobre la misma, al igual que la topología del delito que se estudie.

c. Tipo de delito / Tipología de incidente:

A continuación se enumeran delitos típicos que se abordan en un análisis forense informático:

- Robo de información:
    - El robo de información privada preocupa desde usuarios hasta empresas, tanto por violar el derecho a la intimidad como por suponer posibles filtraciones de información en el ámbito empresarial. Suele utilizarse este método como medio de extorsión, para obtener beneficio económico o dañar la imagen.

- Fraude:
    - Es uno de los delitos más extendidos en internet, podemos encontrar fraudes de todo tipo: falsas ofertas de empleo, falsos emails (phishing), fraudes de inversión y crédito, falsas facturas, descargas que facturan servicio de SMS Premium, multas por descargas ilegales, malware contenido en webs…

- Malware:
    - El malware es otro de los delitos más comunes. Esto incluye piezas de código malicioso, como son los “rootkits”, troyanos, virus…

- Accesos no autorizados
    - Uno de los mayores problemas que se da en las empresas es el acceso no autorizado a ciertas páginas web. Como sabemos, al conectar con ciertas páginas

web y sin las medidas de protección necesaria (como puede ser un firewall, deshabilitar el complemento Javascript, mantener los programas y SO actualizados… el dispositivo queda expuesto antes cualquier amenaza que pueda existir en la red. Aprovechándose de bugs de las propias aplicaciones instaladas en el dispositivo por una infección online al acceder a una página infectada de acceso no autorizado pueden darse accesos no autorizados a una máquina.

- Uso inapropiado de recursos
    - Suele ser frecuente en las empresas, a la hora de realizar una impresión de documentos personales o descargas personales como programas o películas dentro de una red corporativa.

- Propiedad intelectual
    - Se trata de uno de los mayores motivos de pérdidas en internet a nivel mundial. La piratería ha incrementado en los últimos años, proliferando las web de descargas donde podemos encontrar series, películas, juegos, programas y otro software.

- Escucha de conversaciones/tráfico de red
    - Ataques “Man in the Middle”, líneas pinchadas…

- Denegación de servicio
    - Se trata de un tipo de ataque mediante el cual se deja sin acceso o se impide el acceso a los servicios y recursos de una organización. Existe una variante de tipo distribuida “DDoS”, ataque en auge, en el que se suelen utilizar redes de zombis o “Botnets”.

Además de los mencionados anteriormente, existen otro tipo de incidentes relacionados con la informática y/o internet, como pornografía infantil, apología del terrorismo, extorsión (en este grupo queda incluido, entre otros, el “ciber-acoso”, “ciber-bullying”, o la vulneración de la intimidad), robo de información o el fraude entre otros.

4. METODOLOGÍA

Para la selección de evidencias se tendrán como guía los conceptos del estándar internacional **ISO/IEC 27037** (*Information Technology – Security Techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence).*

La norma ISO/IEC 27037 define las siguientes etapas:

- Identificación.

- Recolección.
- Adquisición.
- Preservación.

Para este T.F.M. se modificarán las fases ligeramente de la siguiente forma:

- Preservación – identificación, escena y pruebas
- Recolección (adquisición)
- Análisis
- Informes

Por tanto, la metodología propuesta en la que se basa este TFM consta de 4 fases: preservación, recolección, análisis e informes. Pasaremos a comentar cada una de ellas en profundidad.

Dado que durante la fase de identificación de las evidencias se hace lógico aprovechar para asegurar su preservación y lo que ello conlleva (manipulación, almacenamiento y transporte correctos). Por el mismo motivo, se han decidido unificar recolección y adquisición de las evidencias en un solo paso y para finalizar y no por ello menos importante, se ha añadido una última fase de informes y presentaciones.

Cabe destacar que este trabajo se formula como propuesta para una metodología en casos de análisis forense informático, que recopila información de diferentes estándares, normalizaciones, políticas y trabajos relacionados hasta la fecha.

En la primera fase, además de la identificación de evidencias, se ha incluido la fase de preservación de las mismas, aunando criterios para una correcta tanto identificación como preservación de las evidencias.

Se ha añadido una nueva fase, la tercera, de análisis de evidencias y por último, la fase de informes y presentación se han unificado.

Siguiendo las directrices de la norma ISO/IEC 27037 y siguiendo la prioridad de recolección de evidencias descrita en el RFC 322, se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales (preservando su validez en un juicio).

Además de esto, durante esta propuesta de guía aseguraremos cumplir la normativa descrita para la legislación vigente tanto Nacional como Internacional, así como basarse en los estándares y normalización vigente. Recogiendo así una guía lo más completa posible sobre recomendaciones para evitar cometer errores en un análisis forense y mediante talleres, como llevar a cabo análisis de forma práctica.

A continuación se realizará un resumen del sistema de archivos de Windows y NTFS, con el fin de comprender la relevancia de los mismos durante la fase de análisis:

Niveles del sistema de archivos en Windows:

En primer lugar tenemos el nombre del fichero, seguido de los metadatos de interés de la estructura del sistema de archivos, como puede ser la tabla MFT o el registro de Windows.

A continuación los datos, que corresponden con varios sectores consecutivos agrupados formando un bloque o clúster.

El Sistema de Archivos contiene la tabla de particiones (MBR – Master Bot Record, primaria activa), información de las particiones de disco y árbol de directorios y archivos que contienen.

Master File Table (MFT)

En el sistema de archivo NTFS cada componente es un archivo, hasta la información del sistema. El archivo más importante es el MFT (Master File Table), es un directorio centralizado que contiene información de todos los archivos del disco incluyéndolo a él mismo.

La tabla maestra de archivos (o $MFT) es el primer archivo de un volumen de tipo NTFS (el tipo más común y estandarizado en sistemas Windows actuales) que contiene todos y cada uno de los archivos que componen un volumen. Si el SO realiza una consulta, en primer lugar se dirige a la $MFT para obtener información del mismo, como por ejemplo tamaño, propiedades, atributos, localización, nombres de archivos… etc.

El archivo $MFT contiene la MFT. Existe una copia llamada $MFTMirr

Durante la creación del volumen es creado el Master File Table (MFT), además de otros archivos de control.

Un MFT almacena los atributos de los archivos y subdirectorios incluyendo el nombre, MAC, permisos, flags de estado, entre otros. Existe una entrada de 1KB en la MFT por cada archivo o directorio en el volumen.

Una entrada MFT tiene una pequeña cabecera fija (42 bytes, 12 campos) y el resto son atributos no previamente definidos.

Los MFT están localizados en la raíz del volumen, comienzan por “$” y no son visibles.

Master Boot Record (MBR)

Posiblemente el más importante en todo lo que concierne al arranque. El MBR se encuentra en el primer sector absoluto de un disco duro, nos informa de las particiones primarias que contiene el disco duro (hasta un máximo de 4) y se asocia normalmente al sector de arranque. El Master Boot Record se encuentra en el primer sector de un disco duro, tiene un tamaño de 512 bytes y como el MBR tiene código que es ejecutado, pues lo voy a definir como un programa que se encarga de ceder el

control al sector de arranque de una partición primaria y que esté activa. El sistema hará uso de MBR o GPT según el firmware de arranque que disponga o tenga instalado:

- BIOS. Sistema básico de entrada y salida. También conocido como registro de arranque maestro (MBR).
- UEFI. Unified Extensible Firmware Interface. También conocido como tabla de particiones GUID (GPT).

Firmware.

Es un programa que es grabado en una memoria ROM y establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo.

La BIOS (Basic Input/Output System),

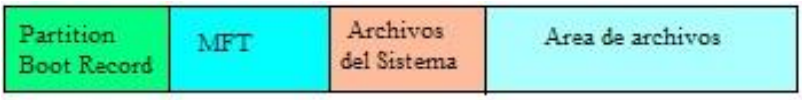
Firmware preinstalado en un circuito integrado de la placa base (memoria ROM) que la maquina carga en memoria RAM, posteriormente localiza y prepara los componentes electrónicos o periféricos de una PC, para comunicarlos con algún sistema operativo que la gobernará. Proporciona funcionalidades básicas: chequeo de la memoria principal y secundaria, comunicación con el usuario vía monitor o teclado y enlace mediante los procesos de arranque con el núcleo del sistema operativo que gobernará el sistema.

Registro de Windows

Se trata de una base de datos que almacena las configuraciones y opciones del sistema operativo Microsoft Windows.
Contiene información, configuraciones e históricos de todo el hardware, software, usuarios, y preferencias del PC.
La Información en el Registro se ordena en un sistema de árbol, normalmente de gran dimensión y su información se guarda en claves.

En la parte de análisis de este trabajo se profundizará en este árbol de registro.

Esquema General - NTFS



Boot Partition Record

Los primeros 8Kb contienen la información sobre el volumen (tipo d partición, largo, etc.), junto con el bloque del código básico para iniciar al sistema operativo.
MTF
La tabla maestra contiene donde y el cómo están almacenados los archivos junto con todos los atributos asociados a estos.
Archivos del Sistema
Contiene la información sobre los datos y operaciones que se realizan sobre el sistema de archivos: espacio libre, log de transaccionalidad, etc…
Área de archivos

Donde se almacena la información de usuario o datos reales.

En la siguiente tabla se describen los componentes de un sistema de archivos NTFS de la arquitectura de un sistema basado en x86 a modo de ejemplo:

Componente	Componente descripción
Disco duro	Contiene una o más particiones.
Arranque sector	Partición de arranque que almacena información acerca de la disposición del volumen y la estructura del sistema de archivos, así como el código de arranque que carga Ntdlr.
Master Boot Record	Contiene código ejecutable que carga el BIOS del sistema en la memoria. El código escanea el MBR para encontrar la tabla de particiones para determinar cuál es la partición activa o de arranque.
Ntldlr.dll	Cambia la CPU a modo protegido, se inicia el sistema de archivos y a continuación lee el contenido del archivo Boot.ini. Esta información determina las opciones de inicio y las selecciones iniciales del menú de arranque.
Ntfs.sys	Controlador del sistema de archivos de NTFS.
Ntoskrnl.exe	Extrae información sobre los controladores de dispositivos del sistema para cargar y el orden de carga.
Modo de núcleo	El modo de procesamiento que permite que el código para tener acceso directo a todo el hardware y la memoria en el sistema.
Modo de usuario	El modo de procesamiento en que las aplicaciones se ejecutan.

i. PRESERVACION

Preservar correctamente las evidencias es una de las partes más importantes durante el proceso de investigación, así como asegurar un uso, transporte y manipulación correctos de las mismas. De ello puede depender una anulación o validación de cierta evidencia o la validez de la misma durante el juicio.

En esta etapa se debe mantener la validez y confiabilidad de todas las pruebas relacionadas con el caso por parte de los técnicos que tienen el primer contacto con la escena. Para ello, se debe utilizar sistemas de almacenaje adecuado como bolsas antiestáticas, soportes estancos contra interferencias y haciendo uso de guantes e indumentaria antiestática adecuada y accesorios como pulsera antiestática.

Se recomienda seguir las siguientes pautas:

- No se alterará el estado en el que se encontraron las evidencias

- Se comenzará etiquetando y fotografiando los dispositivos que serán sometidos a análisis, indicando equipo, marca, modelo, número de serie y código de evidencia, que será el identificador único de dicha evidencia.
- Se garantizará la integridad mediante el mecanismo de cadena de custodia.
- Se hará una distinción entre evidencia física y evidencia digital.

Es importante identificar el propietario y lugar donde fue confiscado el dispositivo.

En función de la naturaleza de las evidencias confiscadas habrá que tomar una serie de medidas adicionales. Para discos ópticos o magnéticos, se deberán proteger contra electricidad estática, por lo que se guardarán en bolsas antiestáticas para evitar pérdida o daño en los datos contenidos.

Mientras los dispositivos a analizar no estén en uso, se deberán almacenar correctamente siguiendo las pautas descritas en esta propuesta de guía, así como identificar correctamente cada una de las mismas y mantener sus cadenas de custodia y documentación.

1. Asegurar la escena y recopilación de información física

Durante cualquier investigación, todos los implicados deben ser responsables y conscientes que cualquier acto de mala praxis o que pueda alterar resultados o las mismas pruebas podría invalidar todo el proceso ante un juez.

El analista debe asegurar la integridad de la escena del crimen, desde el descubrimiento del equipo en cuestión hasta el comienza su análisis. Asegurándose de que la escena no ha sido alterada o modificada durante el proceso completo.

Se deberá llevar una cámara para poder grabar o fotografiar la pantalla del pc en caso de incautar y pillar “con las manos en la masa”, a fin de grabar si se encuentra algún proceso o información útil volátil en la pantalla de la máquina.

Se recogerán fotografías de la escena donde se encuentre el equipo para situarlo físicamente y poder consultar su estado inicial.

En todo momento deben usarse guantes de látex al entrar a la escena para asegurar la integridad de posibles huellas o pruebas físicas que puedan contener.

Se debe anotar fecha y hora de los equipos a la llegada, comienzo de las fases y fin de las mismas.

Otro punto importante a llevar a cabo durante esta etapa del análisis es valorar los periféricos de entrada y salida conectados al equipo como impresoras, teléfonos IP, escáneres…

Identificar el estado de los equipos a analizar, si se encuentran encendidos o apagados para saber qué actuación se va a tomar y con qué prioridad

2. Cadena custodia

La cadena de custodia es el procedimiento controlado aplicable a las evidencias relacionadas con el suceso que recoge y documenta en detalle la manipulación y acceso a las pruebas o

evidencias (elemento que proporciona información de interés para el caso, del cual es posible deducir cierta conclusión o que constituye un hallazgo relacionado con el hecho investigado) que son objeto de una investigación concreta. En ella se recogen todos los accesos a dichas pruebas, detallando fecha, hora y persona que accede a dichas pruebas (no obstante puede incluir más datos, dependiendo de la sensibilidad de las pruebas).

La finalidad de la cadena de custodia es evitar cualquier tipo de manipulación y tener un control absoluto sobre todos los elementos incautados que forman parte de una investigación, quién los manipulado, cómo lo ha realizado, porqué los ha manipulado, para qué lo ha hecho y cuándo ha tenido lugar dicha manipulación.

La documentación de la cadena de custodia deberá contener también todos los lugares por donde ha pasado la evidencia y quién ha realizado su transporte y su acceso o manipulación.

3. Identificación de las evidencias y su volatilidad

Basando esta propuesta de guía en el RFC 3227, se establece el siguiente orden de volatilidad (definida en la tipología de evidencias) y por tanto, orden de recopilación de evidencias, atendiendo a si el tipo de dato/evidencia es volátil o no:

- Volátiles:
    - Registros y contenidos de la caché.
    - Contenidos de la memoria.
    - Estado de las conexiones de red, tablas de rutas.
    - Estado de los procesos en ejecución.

- No volátiles:
    - Contenido del sistema de archivos y de los discos duros.
    - Metadatos archivos
    - Contenido de otros dispositivos de almacenamiento.

Los cuatro primeros puntos representan un tipo de datos, volátil, que se perderán o modificarán si apaga o reinicia el sistema, tanto muy sensibles o fáciles de eliminar de forma inadvertida.

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

1. Registros y contenido de la caché.
2. Análisis de red, Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del *kernel*, memoria RAM.
3. Información temporal del sistema.
4. Disco.

5. Logs y registros del sistema.
6. Configuración física y topología de la red.
7. Documentos.

Dentro de las evidencias volátiles será de interés recuperar los siguientes datos del sistema en tiempo real (Siguiendo la RFC 3227):

- Fecha y hora.
- Análisis de red
- Volcado de memoria RAM
- Fecha y hora del sistema
- Histórico del intérprete de comandos
- Pagefile.sys e hiberfile.sys
- Árbol de directorios y ficheros
- Historial de internet
- Carpetas compartidas
- Usuarios que han iniciado sesión y listado de cuentas
- Procesos activos
- Servicios en ejecución

4. Transporte y manipulación de evidencias

Se tendrá en cuenta proteger las evidencias para el transporte desde el lugar de los hechos hasta el laboratorio con los medios necesarios para evitar golpes y proteger de caídas fortuitas, además de las medidas de preservación anteriormente descritas y manteniendo la cadena de custodia para cada una de ellas.

5. Almacenamiento de evidencias

El lugar de almacenamiento también debe reunir unas mínimas de condiciones de seguridad, no sólo de acceso físico a las evidencias, sino también ambientales. No se podrán almacenar dispositivos electrónicos en sitios húmedos o con temperaturas extremas o con exceso de polvo, suciedad o radiación electromagnética.

Para la gestión de datos en dispositivos de almacenamiento y su transporte (evidencias) se puede consultar y considerar alguna de las recomendaciones contenidas en la ISO 17799:2005 en su apartado 10.7.

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

ii. RECOLECCION

Recolección de evidencias

A lo largo de esta etapa se lleva a cabo la recolección de las evidencias digitales, proceso que requiere un gran conocimiento de los sistemas a estudiar.

Una vez conocido el orden de volatilidad de las pruebas y mediante la tipología del caso a analizar se ha establecido un orden de prioridad sobre las pruebas a recolectar.

Durante esta fase se debe documentar toda la información posible sobre los dispositivos que se encuentran en la escena, listando sus características, usuarios, nombre y contraseña de los usuarios que hacen uso del equipo y la posición espacial de los mismos. También deben identificarse los discos duros, anotando todos sus datos (marca, modelo, capacidad, foto y tamaño), lo mismo ocurre con los discos ópticos y sus unidades lectoras.

Para continuar profundizando en el análisis, se dibujará la topología de la red a la que esté conectada la maquina/s (de estarlo), identificando la posición de cada equipo en la red. Así mismo se deberán anotar todos los puertos y cables/conexiones de las máquinas involucradas conectados a los "routers", para poder reproducir el escenario al detalle en laboratorio en caso de ser necesario, así como puertos y conexiones de periféricos.

A la hora de realizar la recolección de evidencias, debemos tener en cuenta la legislación vigente en todo momento.

1. **Consideraciones de privacidad**

Es importante considerar las pautas de la empresa en cuanto a privacidad. Se suele solicitar autorización por escrito para efectuar la recolección de evidencias. Esto es muy importante ya que en ocasiones se pueden manejar datos confidenciales o incluso llegar a afectar a la disponibilidad de los servicios. Además, a menos que haya indicios suficientes y fundamentados no se deben recopilar ficheros con datos personales.

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.

2. **Consideraciones legales**

Se debe tener en consideración la legislación del país en el que se actúe, dado que no es único para todos, no obstante deben cumplir una serie de características comunes:

- **Admisible**: se debe cumplir las normas de la legislación vigente para que las evidencias tengan validez judicial.
- **Auténtica**: se debe poder probar que la evidencia corresponde al incidente en cuestión y no ha sido modificada.

- **Completa**: debe corresponder a la información completa y no a una visión parcial de la misma.
- **Confiable**: no debe existir ninguna duda acerca del proceso o método de obtención la evidencia y la posterior manipulación.
- **Creíble**: debe de ser verosímil y fácilmente comprensible por un tribunal.

3. **Procedimiento de recolección**

Este procedimiento debe ser lo más detallado y claro posible, reduciendo al mínimo la toma de decisiones y maximizando el número de posibles pruebas obtenidas, para ello el método de recolección de evidencias utilizado durante el caso debe ser reproducible:

Reproducible

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

Y deben seguirse unos pasos básicos durante la recolección de las evidencias:

- Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.
- Listar gente que se encontraba en la escena del crimen, así como lo que estaban haciendo, lo que observaban y como reaccionaron.
- Establecer qué es relevante para el caso.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información (recolección) 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.

Diferenciamos dos tipos de análisis posibles principalmente a la hora de llegar a una escena:

a) <u>Equipo encendido. Análisis en caliente</u>

Hace referencia al dispositivo de interés, del que se desea obtener evidencias o involucrado en un caso que requiere de un análisis forense, cuando éste se encuentra inicialmente en estado arrancado o encendido. Con el dispositivo encendido se pueden obtener datos o evidencias volátiles que no sería posible obtener si este careciese de corriente o se encontrase en el estado opuesto, apagado, como por ejemplo procesos en

ejecución, conexiones de red y su estado. Este tipo de datos se pierden al apagar el dispositivo o desconectarlo de la red eléctrica/fuente de alimentación.

Su principal ventaja radica en la posibilidad de toma de evidencias de ataques que se encuentran activos en ese instante, datos de vital importancia que pueden llegar a identificar el origen de dicho ataque.

Otro tipo de dato volátil de interés es la memoria RAM. Mediante un análisis en caliente puede volcarse la información contenida en ese momento en la memoria RAM, en muchas ocasiones se trata de información de vital importancia.

Al realizar una copia exacta del sistema cuando éste se encuentra encendido, es posible replicar el entorno prácticamente al completo mediante técnicas de virtualización, asegurando siempre que la evidencia original no sufra modificaciones o se ponga en peligro la integridad de la misma.

Durante todo el trabajo presente, seguiremos las recomendaciones recogidas en el RFC 3227 sobre la toma de evidencias, volatilidad y almacenamiento de evidencias para priorizar el orden de recolección de las mismas conforme a su nivel de volatilidad, es decir, comenzaremos recogiendo las evidencias con mayor índice de volatilidad.

En nuestro caso, dado que suponemos un ordenador conectado a la red, primero realizaremos el análisis de red con su correspondiente informe y toma de evidencias para poder desconectarlo de la red y continuar con el procedimiento de volcado de memoria RAM e información volátil del sistema.

A fin de no perder información debido a una actuación remota desde la red o internet (bien debido a un fallo, al propio atacante o a algún sistema de protección-autodestrucción de datos/evidencias) del equipo a analizar y para no perder la información de conexiones abiertas y rutas de la máquina, en primer lugar procederemos a analizar la red

Posteriormente desconectaremos el equipo de toda red y realizaremos el volcado de memoria RAM.

Por último se realizará una copia bit a bit del disco, fase común a ambas tipologías de análisis, tanto en frío como en caliente.

Uno de los datos volátiles más importantes a la hora de realizar un análisis forense (junto al análisis de memoria RAM) se trata del análisis del estado de red, en el que se incluye:

- Información de red: estado, conexiones activas, puertos UDP y TCP abiertos
- Captura de red Wireshark
- Puertos TCP/UDP abiertos y aplicaciones asociadas “a la escucha”
- Carpetas compartidas
- Volúmenes virtuales
- Archivo hosts, cache ARP y otros archivos y logs de red

Para realizar un volcado de memoria RAM sobre un fichero, podemos usar diferentes herramientas, por ejemplo MDD:

mdd_1.3.exe -o fichero_de_volcado.img

TALLER 1. Análisis Red:

Vamos a ver algunas herramientas nativas y la forma de recolectar datos de un determinado sistema Windows. A pesar de que para realizar análisis profesionales, siempre es recomendable utilizar herramientas no nativas (existen cantidad de ellas para cada una de las fases del análisis, por ejemplo en la suite Sysinternals se recopilan un gran número de herramientas o OSForensics, entre otras) y desde un medio extraíble a ser posible con acceso de sólo lectura. Dado que el malware que haya afectado al sistema a analizar podría falsear los resultados que arrojan los programas nativos a la hora de realizar las consultas de nuestro análisis forense informático.

Netstat muestra conexiones abiertas en el equipo, muy utilizado en el análisis de backdoors.

Vamos a ver ahora algunas opciones más del comando **net**:

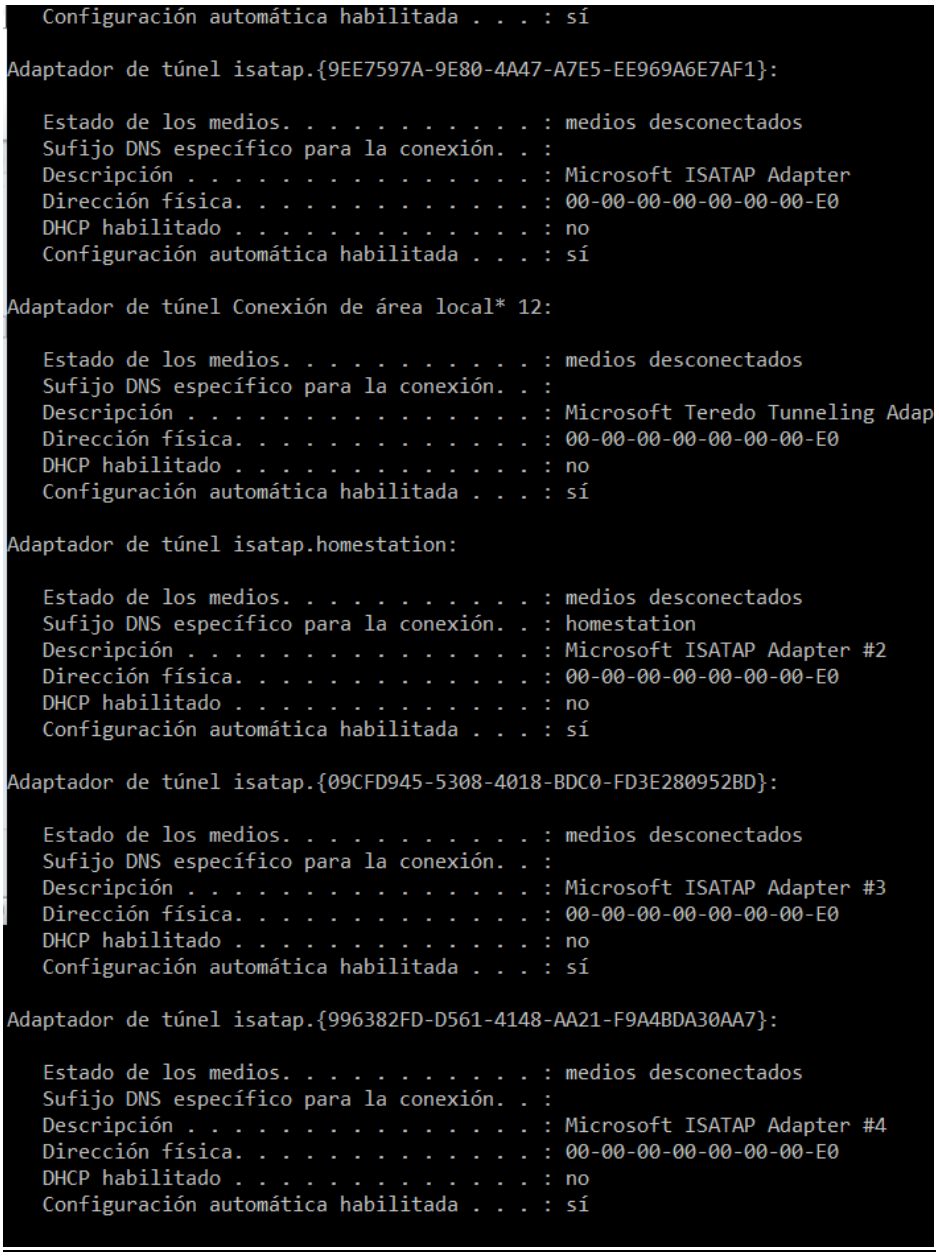
- *net view* : nos muestra información de los equipos de nuestro grupo de trabajo o dominio y ver que se está compartiendo
- *net niew /domain* : nos muestra los distintos dominios
- *net statistics server* : permite recuperar información acerca del uso de la red, como la cantidad de información enviada y recibida, cantidad de archivos a los que se tuvo acceso, sesiones aceptadas, etc.

Algunas opciones del comando **nbtstat**

- *nbtstat –n :* vemos a que recursos están conectados, los valores hexadecimales dicen que servicio tiene buscar tabla
- *nbtstat –c :* con valores hexadecimales y direcciones IP
- *nbtstat –R :* borra la tabla que generamos, dado que el comando almacena en el cache
- *nbtstat -a pc01* : para obtener los valores “hexa”, “tabla” y “macaddress”

Otro comando de interés para obtener información sobre el hardware de red es ipconfig:

Mediante “*ipconfig /all*”, podemos observar la siguiente información:



NetBIOS

Este protocolo de red que permite comunicar equipos dentro de la misma red local asignando un nombre identificativo a cada equipo, lo que facilita compartir recursos o acceder a 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

net sessions

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

net file

Contenido de la caché DNS

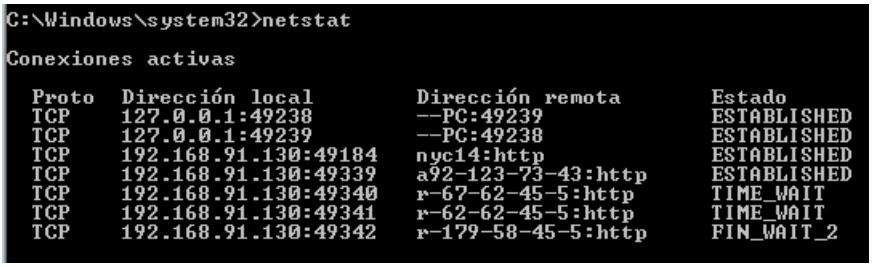
"Domain Name System", se trata de servidores específicos que asocian direcciones IP con nombres de dominio.

Conexiones en Windows

Para obtener el listado de conexiones el comando "netstat".

Para ello, se debe escribir la siguiente instrucción:

netstat



Para obtener la relación entre aplicaciones y puertos abiertos se utiliza la siguiente instrucción:

netstat -anob

ARP caché

En esta tabla se almacena la relación entre dirección física (MAC) y dirección lógica (IP) de los equipos con los que se haya comunicado recientemente el ordenador. Dicha información almacenada será eliminada, en el caso de que no se mantenga la comunicación.

Tráfico de red

Una buena forma de saber lo que ocurre en una red específica, es capturando el tráfico que pasa por la misma, así como para identificar las conversaciones que tiene la máquina objeto de análisis con el exterior o dentro de la propia red. Para ello pueden utilizarse multitud de programas que cuentan con GUI o no, unos de los más conocidos son TShark o Wireshark.

A partir de este punto desconectar el equipo de la red para continuar el análisis

En este punto una vez realizado el análisis de red, procederemos a desconectar físicamente la máquina de la red.

Desconectando o aislando un equipo de la red, podemos lograr que una determinada acción no siga ocurriendo, por ejemplo una descarga de datos no autorizada o el borrado remoto de datos por parte del atacante que podrían dificultar el análisis. Por otra parte, perderemos información sobre posibles conexiones que nos den el origen del incidente o valiosos indicios. Por ello es recomendable realizar el análisis de red previamente.

Volcado de memoria RAM (RAM & "Swap Dumps"):

Consiste en realizar una copia exacta de la memoria RAM o memoria física como partición swap (Linux) y/o ficheros de paginación/pagefile en Windows, del sistema en el momento exacto en el que se incauta o interviene un dispositivo, obteniendo la información instantánea en el momento de este análisis. El volcado de memoria es uno de los aspectos más importantes y críticos de la fase de adquisición. Esta información de volcado incluye datos que pueden llegar a ser de gran importancia como los citados anteriormente para un "análisis en caliente". Mediante este método es posible identificar posibles conexiones, contraseñas introducidas, documentos y archivos temporales y procesos en ejecución entre otros.

Además del análisis de red y volcado de memoria RAM anteriormente descrito, siguiendo la RFC 3772 debemos proceder a recolectar el resto de evidencias volátiles. Aquí se hará uso de herramientas nativas del sistema para algunos ejemplos, no obstante es conveniente utilizar herramientas de terceros almacenadas, en medios extraíbles protegidos contra escritura para asegurar la integridad de las evidencias tomadas (como la "Suite Sysinternals" u "OSForensics"), ya que cualquier proceso que corramos en la memoria del equipo objetivo de análisis puede provocar una sobre escritura de datos y una modificación de la misma, por lo que la prueba tomada quedaría corrupta por el analista:

- **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 o duración del proceso.

  Podemos utilizar los siguientes comandos en una consola de Windows:

  Fecha De Inicio

  date /t

  Hora De Inicio

  time /t

  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 crear una línea temporal del caso y determinar si la fecha establecida en el sistema es correcta o no, y que desviación existe.

  Se debe tener en cuenta 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.

  Una vez finalizado el proceso se deberá ejecutar las mismas instrucciónes para obtener la fecha y hora, pero esta vez de fin y posteriormente documentarlo.

- **Histórico del intérprete de comandos**

  Para consultar un listado de los últimos comandos escritos en consola en Windows se utiliza el siguiente comando:

  doskey /history

- **Pagefile.sys e hiberfile.sys**

  Otros ficheros importantes a recolectar, que pueden resultar de gran interés son los archivos pagefile.sys e hiberfile.sys. Es recomendable obtener estos ficheros siempre que se encuentre la máquina encendida, esta tarea se puede llevar a cabo en las fase de análisis de disco, extrayendo y analizando estos archivos, no obstante es posible perder esta información al desconectar la máquina de la red eléctrica, dependiendo de la configuración del sistema. Existen herramientas específicas para extraer estos ficheros, ya que el sistema operativo hace uso de ellos durante su ejecución, lo que dificulta su copia directa.

- **Árbol de directorios y ficheros**
    - Listado en base a la fecha de modificación.

      dir /t:w /a /s /o:d c:\ > "ListadoBaseFechaMod.txt"

    - Listado en base al último acceso.

      dir /t:a /a /s /o:d c:\ > " ListadoBaseAcceso.txt"

    - Listado en base a la fecha de creación.

      dir /t:c /a /s /o:d c:\ > " ListadoBaseFechaCrea.txt"

- **Historial de internet**

  En ocasiones puede resultar de interés conocer el historial de navegación del sistema y poder analizar la actividad en internet del mismo.

  Para ello se utiliza algún tipo de herramienta como BrowsingHistoryView.

  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"

  - **Internet Explorer**

    Todas las actividades del usuario en Internet Explorer están almacenadas en: C:\Users\%username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5

    Los directorios de Actividad de IE que contienen las actividades de historial sin contenido en caché local: C:\Users\%username%\AppData\Local\Microsoft\Windows\History

    Cookies: C:\Users\%username%\AppData\Local\Microsoft\Windows\Cookies

  - **Chrome**

    El Historial, cookies, caché y favoritos se encuentran especialmente en el directorio: C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default

  - **Firefox**

    La caché está almacenada en C:\Users\%username%\AppData\Local\Mozilla\Firefox\Profiles\umuq8upn.default\Cache

    Cookies: C:\Users\%username%\AppData\Local\Mozilla\Firefox\Profiles\umuq8upn.default\cookies.sqlite

    Historial: C:\Users\%username%\AppData\Local\Mozilla\Firefox\Profiles\umuq8upn.default\places.sqlite

- **Carpetas compartidas**

  Listado de recursos compartidos en la máquina:

- **Usuarios que han iniciado sesión y listado de cuentas de usuario**

  Para obtener un log usuarios que han iniciado sesión en el equipo, incluyendo fechas de sesión, se pueden utilizar diferentes herramientas, una de ellas es netUsers.exe

  Para realizar la consulta se debe escribir la siguiente instrucción:

  netUsers.exe /History

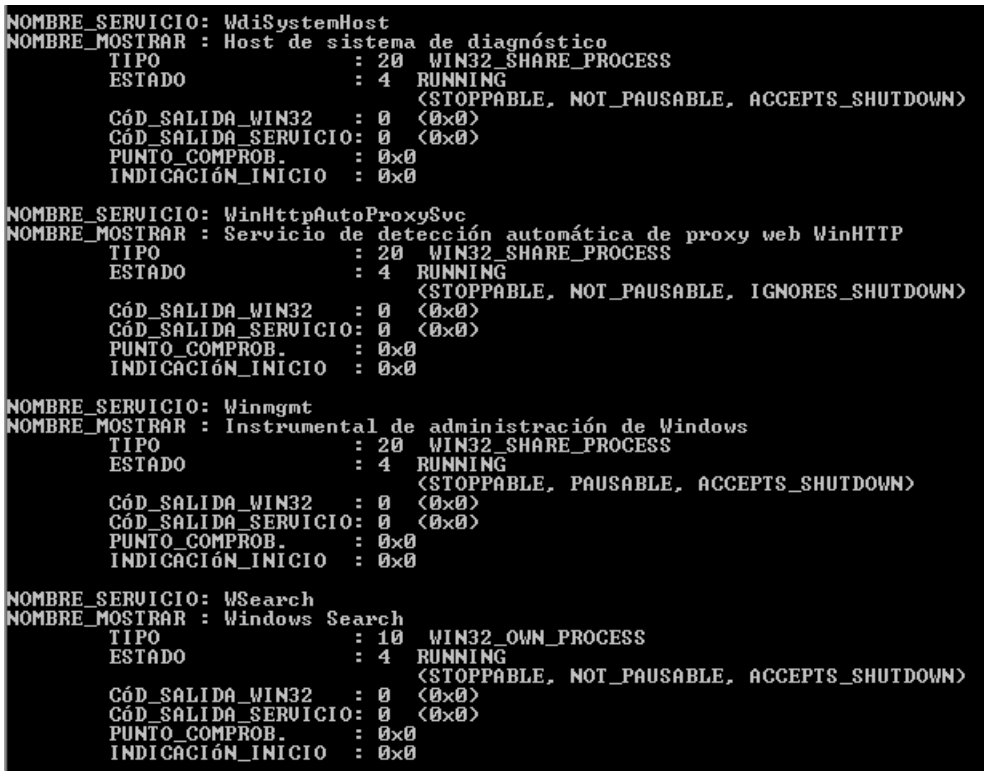
- **Procesos activos o en ejecución.**

  Podemos utilizar el comando "tasklist" para llamar a la herramienta de Windows o utilizar herramientas como Sysinternals de Microsoft desde un medio externo.

- **Servicios en ejecución**

  El siguiente comando se utiliza para obtener el listado de servicios en ejecución e sistemas Windows:

  sc query



Por último realizaremos una copia de disco como se describe en el siguiente punto, para posteriormente poder realizar un análisis sobre la misma.

A partir de este punto, se podrá proceder al apagado de la máquina para su posterior recolección de pruebas mediante una copia bit a bit de disco.

b) **Equipo apagado. Análisis en frio**

Este tipo de análisis, a diferencia del análisis en caliente, puede realizarse de forma más profunda, pero por otra parte se puede perder (o dejar de obtener) pruebas de tipo volátil que pueden llegar a ser de gran importancia para la resolución de un caso. Se realiza partiendo de la copia exacta de un disco (información no volátil del dispositivo), extraída a partir de un equipo en estado apagado. Se trata de un proceso menos intrusivo para la evidencia, evitando alterar la información de esta dado que se trabaja sobre una copia exacta del disco, verificando su integridad a partir de un hash obtenido previamente a la manipulación.

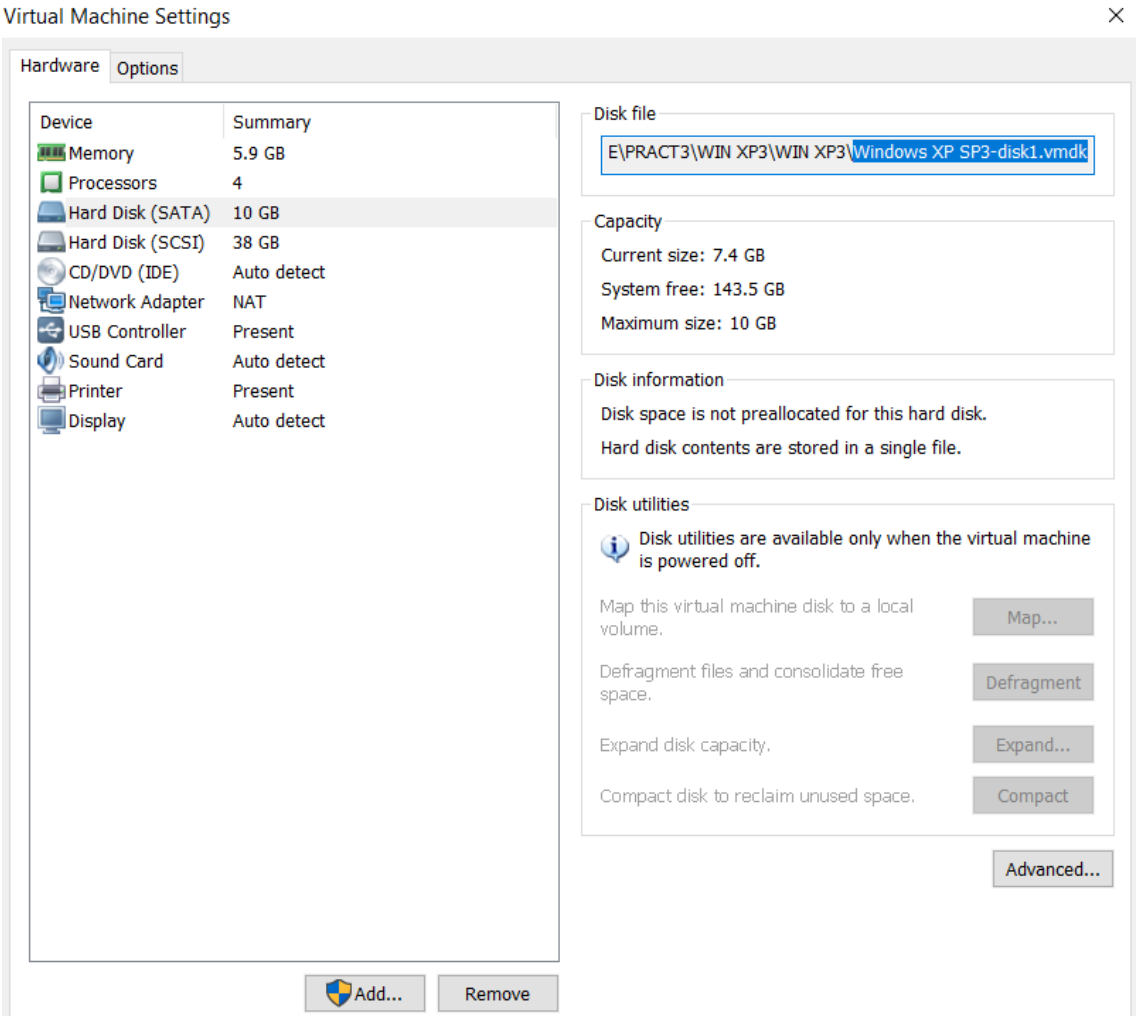
Volcado de disco – TALLER 2

Para este caso haremos uso de una máquina virtual con la distribución CAINE instalada y una copia de un disco duro a analizar.

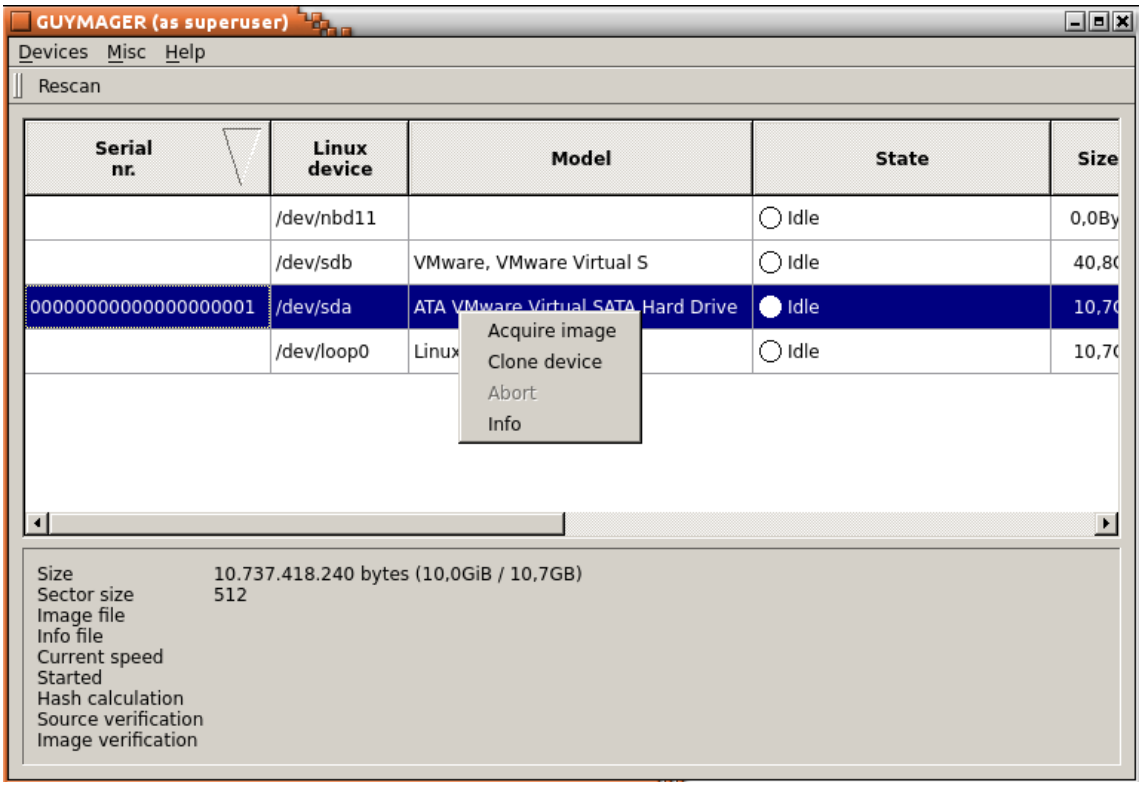
Para realizar este mismo análisis a un medio físico, es decir, a un disco duro en lugar de una imagen de disco, deberemos conectar el disco duro a copiar a través de un dispositivo Hardware o software que proteja al medio contra escritura y conectarlo a nuestro sistema de análisis forense, en nuestro caso CAINE para realizar el volcado de la información, montándolo como medio extraíble a través del Hardware específico de copiado.

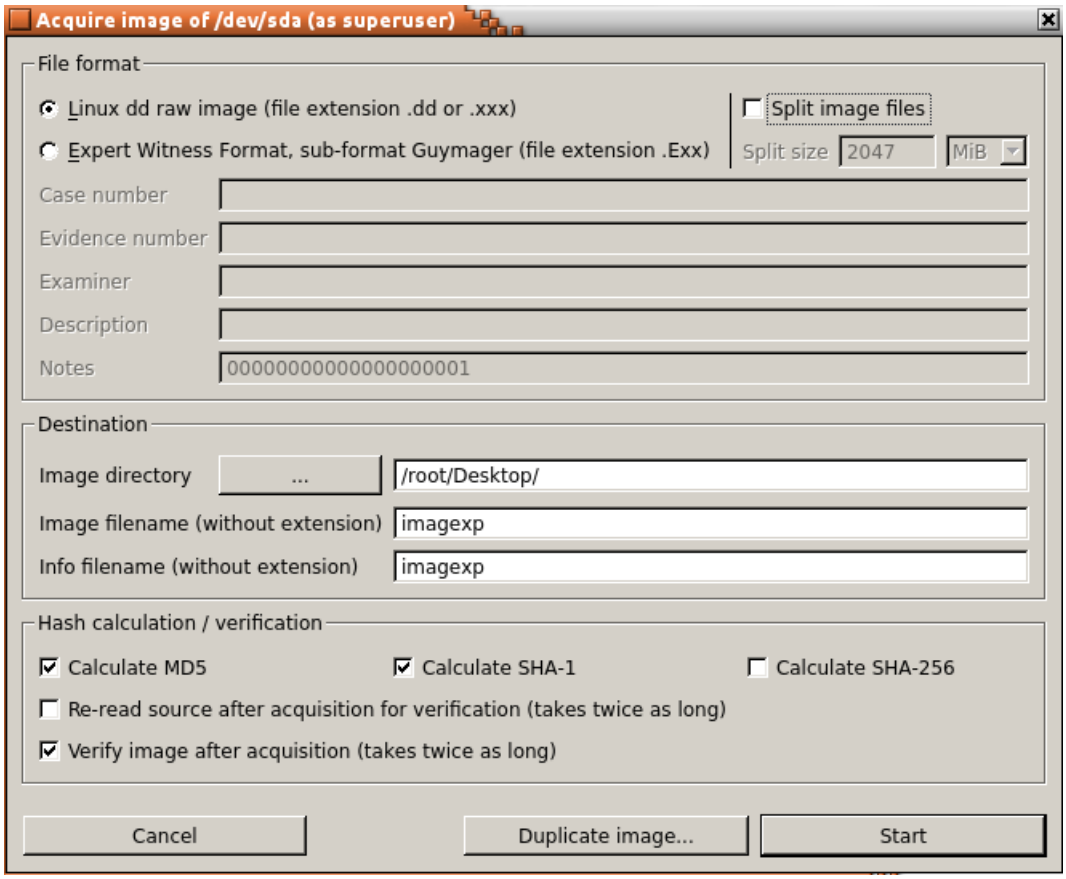
En primer lugar, a fin de preservar la imagen de disco objeto de este análisis, realizaremos una copia del mismo, posteriormente se considera el volcado del disco duro completo (junto a sus "allocated"), en un fichero, asegurándonos de evitar cualquier permiso de escritura sobre el mismo. Mediante este proceso podemos evitar arrancar la máquina virtual entregada en la práctica, manteniéndola intacta, así como su copia, dado que montaremos dicha imagen como disco duro ATA/SATA en una distribución de Linux orientada al análisis forense, para este caso en concreto usaré CAINE 7.0, arrancada de forma virtual a través de virtualización, haciendo uso de la herramienta VMWare para Windows 10.

Creamos una imagen en formato raw (.dd) del disco duro de la máquina virtual. Para ello haremos uso de CAINE instalado virtualmente en VMWare, montando dicha imagen en un disco secundario (dentro de VMWare) con permisos de solo lectura, para asegurar no comprometer la prueba, además se firmará digitalmente mediante hash (MD5+SHA1) o SHA256. Preferiblemente MD5+SHA1, comprobando la integridad mediante comparación de originalidad en ambos valores (MD5+SHA1), ya que de este modo consumiremos menos recursos y ahorraremos tiempo. Se sabe que tanto MD5 como SHA1 son procesos de firmado digital mediante hash débiles, ya que existen vulnerabilidades conocidas en los mismos, no obstante al utilizar ambos al mismo tiempo, se reduce casi por completo un fallo en la comparación de firmas.



Posteriormente pasamos a arrancar CAINE, montamos el disco en modo solo lectura y creamos una copia del disco mediante la herramienta Guymager:


GUYMAGER (as superuser)
Devices Misc Help
Rescan
Serial nr.
Linux device
Model
State
Size
/dev/nbd11
Idle
0,0By
/dev/sdb
VMware, VMware Virtual S
Idle
40,8(
00000000000000000001
/dev/sda
ATA VMware Virtual SATA Hard Drive
Idle
10,7(
/dev/loop0
Linux
Idle
10,7(
Acquire image
Clone device
Abort
Info
Size
10.737.418.240 bytes (10,0GiB / 10,7GB)
Sector size
512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification


Acquire image of /dev/sda (as superuser)
File format
Linux dd raw image (file extension .dd or .xxx)
Expert Witness Format, sub-format Guymager (file extension .Exx)
Split image files
Split size
2047
MiB
Case number
Evidence number
Examiner
Description
Notes
00000000000000000001
Destination
Image directory
...
/root/Desktop/
Image filename (without extension)
imagexp
Info filename (without extension)
imagexp
Hash calculation / verification
Calculate MD5
Calculate SHA-1
Calculate SHA-256
Re-read source after acquisition for verification (takes twice as long)
Verify image after acquisition (takes twice as long)
Cancel
Duplicate image...
Start

Copias seguras de disco y análisis bloqueando escritura, SW o HW.

Se debe realizar una copia bit a bit o a bajo nivel, es decir una copia exacta del contenido de los discos, incluyendo todos los archivos del disco y el espacio sin asignar del mismo para tratar de recuperar archivos eliminados o "desindexizados en memoria" en sectores no sobrescritos. Esta copia se llevará a cabo sobre un soporte limpio mediante un borrado seguro de los datos que pudiera contener anteriormente para evitar así contaminaciones con otros casos.

Esta imagen incluye particiones, espacios del disco que no se hayan utilizado, tabla de particiones, sector de arranque, zonas reservadas que son poco accesibles, utilizadas por el fabricante para incluir información especial o disminuir almacenamiento de un dispositivo.

Para tener una imagen clonada de bajo nivel es necesario que se tenga el acceso de modo lectura únicamente al disco duro a investigar evitar así cualquier operación de escritura sobre disco/evidencia, para realizar estos procedimientos se utilizan herramientas tipo hardware y software que soportan todo tipo de dispositivos de almacenamiento y conexiones.

Una vez se ha realizado la copia del disco, se procede a firmarla digitalmente mediante una función hash o CRC, utilizando algoritmos MD5 o SHA, (recomendado MD5+SHA1 o SHA256), de esta forma se puede validar la integridad de la copia mediante el hash de la muestra original y el de la copia, certificando que ambos son iguales a todos los niveles en un juicio y que no han sufrido alteraciones o modificaciones en la toma ni proceso de análisis. Este hash actúa como un certificado digital para la validación de los elementos adquiridos por el investigador.

Se deberá realizar una segunda copia sobre la primera, verificando su integridad mediante el mecanismo de firmado anteriormente descrito.

Esta clonación se debe realizar en un dispositivo con funciones de formateo a bajo nivel y protección contra escritura de tipo Hardware o Software, para evitar una alteración de la evidencia y tener únicamente acceso de lectura a la misma. Kali Linux.

Teniendo los datos de la persona, del equipo, de los dispositivos de almacenamiento y la clonación, finalmente se tienen que trasportar al centro donde se realizarán las investigaciones.

Teniendo ambas copias entregaremos la primera al secretario judicial o notario responsable del caso y nos quedaremos con la segunda para poder trabajar. La segunda copia será nuestra copia de respaldo en todo momento en el laboratorio y no será para trabajar directamente con ella en ningún caso.

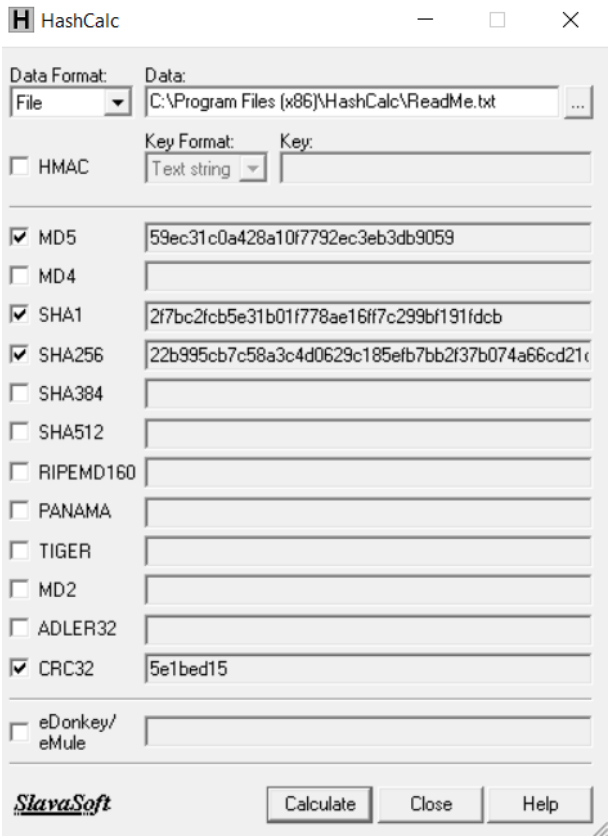
4. Firmado y validación de copias – Hash

El uso del hash MD5, a pesar de su amplio grado de utilización, presenta debilidades en el proceso de firmado, 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 que consideramos firma débil o vulnerable, aunque no igual, es el del SHA-1 por lo que se aconseja que se busquen otras alternativas como SHA-256, SHA-512, etc. O la utilización de una mezcla de dos firmas, como por ejemplo MD5+SHA1.

Existe herramientas para firmado y validación de firmas como por ejemplo HashMyFiles27, MD5deep28 o HashCalc29 a través de las cuales se pueden obtener los distintos hashes de un fichero.

Ejemplo: Obtención de diferentes hash sobre fichero en Windows:



iii. ANALISIS

Esta fase recoge una serie de procesos y tareas sobre las evidencias de las que se disponen en un caso para dar respuesta a las preguntas relacionadas con el incidente investigado, recopilando el máximo número de pruebas e información posibles.

Debe realizarse un análisis basado en la legislación y jurisdicción vigente de cada país y los resultados que se obtengan del proceso han de ser verificables y reproducibles, es decir, podemos montar un laboratorio donde reproducir los hechos y la investigación a fin de demostrar los hechos supuestamente acontecidos.

Durante todo el proceso se trabajará sobre copias de las evidencias entregadas o sus copias, guardando los originales correctamente para asegurar no corromper/modificar la evidencia, usando para confirmar la originalidad de la copia mediante firmado hash (MD5+SHA1 o SHA256) al comienzo del análisis y verificación del mismo al finalizar la fase.

El tipo de análisis a realizar sobre las evidencias dependerá del tipo de incidente/delito.

Durante esta etapa se realiza una búsqueda detallada de información de las evidencias adquiridas en la etapa anterior, como búsqueda detallada de los sistemas de archivos, detección y análisis de malware, análisis de memoria RAM, entre otros.

En el caso de los ficheros del sistema analizado, hay que tener cuidado con las carpetas personales de los usuarios y las leyes que las protegen, por otra parte se debe tener en cuenta que las carpetas en la instalación del sistema operativo por ejemplo creadas por el usuario administrador no se consideran personales.

Uno de los elementos más importantes en la realización de un análisis forense son las marcas de tiempo de los ficheros (MAC Times): MAC (Modificación, Acceso y Creación), que marcan los tiempos de creación, acceso y modificación.

Análisis de las evidencias

1. Información Volátil.

Análisis de memoria RAM – TALLER 3

En este taller trabajaremos en el análisis de una imagen de memoria RAM entregada (volcada previamente de una máquina como evidencia de un caso ficticio).

Los datos sobre el sistema operativo se obtiene a partir del comando/"plugin" "consoles":

caine@caine:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Documents/memoriacp.dd consoles

File type: Microsoft memory crash dump file

Acquisition method: MmMapIoSpace()

Content: Memory manager physical memory block + Very First PFNs

Destination path: C:\Output\memory.dmp

O.S. Version: Microsoft Windows XP Professional Service Pack 2 (build 2600)

Computer name: VMWARE-W2KSP2

Physical memory in use: 63%

Physical memory size: 65008 Kb (63 Mb)

Physical memory available: 24000 Kb (23 Mb)

Paging file size: 250468 Kb (244 Mb)

Paging file available: 189564 Kb (185 Mb)

Virtual memory size: 2097024 Kb (2047 Mb)

Virtual memory available: 2083644 Kb (2034 Mb)

Extented memory available: 0 Kb (0 Mb)

Physical page size: 4096 bytes

Minimum physical address: 0x0000000000002000

Maximum physical address: 0x0000000003FFF000

……

Se trata de un Windows XP SP2 con nombre d equipo vmware-w2ksp2 y perfil principal WinXPSP2x86. Como podemos observar:

O.S. Version: Microsoft Windows XP Professional Service Pack 2 (build 2600)

Computer name: VMWARE-W2KSP2

Enunciado 1. Indicar si la máquina ha sido comprometida. En caso afirmativo indicar, en la medida de lo posible, el código malicioso y comprobar si es posible extraerlo. Evaluar su persistencia en el sistema:

Se procede al análisis de ficheros mediante "filescan":

caine@caine:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Documents/memoriacp.dd filescan --output-file=/home/caine/Desktop/filescan.txt

Offset(P) #Ptr #Hnd Access Name

---------- ------ ------ ------ ----

0x0000000000909700 1 0 R--r-d \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.VC80.MFC_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_3bf8fa05\mfc80u.dll

0x00000000009099e0 1 0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\drivers\audstub.sys

0x0000000000909c10 1 0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\snmpapi.dll

0x0000000000909dd0 1 0 -W-r-d \Device\HarddiskVolume1\WINDOWS\system32\wbem\Logs\wbemprox.log

0x00000000009e33e0 3 1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Testbenutzer\Start Menu

0x0000000000a4a670 1 1 ------ \Device\Afd\Endpoint

0x0000000000a4a820 3 0 RWD--- \Device\HarddiskVolume1\$Directory

0x0000000000a4ab80 1 1 ------ \Device\NamedPipe??kssvc

0x0000000000c9c958 1 0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\wshext.dll

0x0000000000c9cd10 3 0 RWD--- \Device\HarddiskVolume1\$Directory

0x0000000000cb5188 1 0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\tapi32.dll

0x0000000000cb5990 2 1 ------ \Device\NamedPipe\InitShutdown

0x0000000000cb5a68 1 1 ------ \Device\NamedPipe\InitShutdown

0x0000000000d143e0 1 0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\drivers\vmxnet.sys

0x0000000000d147f0 1 0 R--r-d \Device\HarddiskVolume1\Program Files\VMware\VMware Tools\VMwareUser.exe

0x0000000000d14f90 1 0 R--r-d \Device\HarddiskVolume1\Malware\FUto\fu.exe

Donde se puede observar que el fichero principal desde el que se infectó la máquina se encuentra en \Device\HarddiskVolume1\Malware\FUto\fu.exe

Se trata de extraer (tanto el ejecutable como el proceso) mediante comandos de dump:

caine@caine:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Documents/memoriacp.dd procdump --output=text --output-file=/home/caine/Desktop/procdump.txt --dump-dir=/home/caine/Desktop/procdump

Process(V) ImageBase Name Result

---------- ---------- -------------------- ------

0x81233bd0 ---------- System Error: PEB at 0x0 is unavailable (possibly due to paging)

0x810dc368 ---------- smss.exe Error: PEB at 0x7ffd7000 is unavailable (possibly due to paging)

0x810d89a0 0x4a680000 csrss.exe Error: ImageBaseAddress at 0x4a680000 is unavailable (possibly due to paging)

0x810be578 0x01000000 winlogon.exe Error: ImageBaseAddress at 0x1000000 is unavailable (possibly due to paging)

0x810ec620 0x01000000 services.exe OK: executable.664.exe

0xffb78150 0x01000000 lsass.exe OK: executable.676.exe

0xffb538e0 0x00000000 vmacthlp.exe Error: ImageBaseAddress at 0x0 is unavailable (possibly due to paging)

0x810cb1d0 0x01000000 svchost.exe OK: executable.892.exe

0x810d3460 0x01000000 svchost.exe Error: ImageBaseAddress at 0x1000000 is unavailable (possibly due to paging)

0x810d9a78 0x01000000 svchost.exe OK: executable.1068.exe

0x810a2c90 0x01000000 svchost.exe OK: executable.1096.exe

0xffb44638 0x01000000 svchost.exe Error: ImageBaseAddress at 0x1000000 is unavailable (possibly due to paging)

0xffb37278 0x00400000 VMwareService.e OK: executable.1452.exe

0xffb7e4b8 0x01000000 explorer.exe OK: executable.1704.exe

0xffb19228 0x00400000 VMwareTray.exe OK: executable.1780.exe

0xffb17210 0x00400000 VMwareUser.exe Error: ImageBaseAddress at 0x400000 is unavailable (possibly due to paging)

0xffb153c0 0x4ad00000 cmd.exe OK: executable.1012.exe

0x81067da0 0x00400000 win32dd.exe OK: executable.1020.exe

Enunciado 2. ¿Existen procesos, dll's o módulos ocultos en el sistema o direcciones IP a las que se conecte? En caso afirmativo tratar de descubrirlos

En primera instancia, utilizando el comando "sysinfo", se localiza el perfil adecuado y la información del dispositivo a analizar.

Posteriormente se realiza un análisis prácticamente integro de la imagen facilitada, obteniendo principalmente procesos, ficheros, archivos de paginación, sockets, consolas, etc…

En el siguiente ejemplo, se hace uso del "plugin" "pslist", obteniendo la lista de procesos activos, donde podemos ver el archivo de interés para los siguientes análisis (posteriormente confirmaremos que se trata de malware persistente en el archivo win32dd.exe):

caine@caine:/usr/share/caine/pacchetti/volatility$ volatility -f /home/caine/Documents/memoriacp.dd pslist

Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit

---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------

0xffb78150 lsass.exe 676 620 14 268 0 0 2009-10-24 10:48:29 UTC+0000

0xffb538e0 vmacthlp.exe 844 664 1 24 0 0 2009-10-24 10:48:31 UTC+0000

0x810cb1d0 svchost.exe 892 664 6 117 0 0 2009-10-24 10:48:33 UTC+0000

0x810d3460 svchost.exe 960 664 9 193 0 0 2009-10-24 10:48:33 UTC+0000

0x810d9a78 svchost.exe 1068 664 23 463 0 0 2009-10-24 10:48:34 UTC+0000

0x810a2c90 svchost.exe 1096 664 6 60 0 0 2009-10-24 10:48:34 UTC+0000

0xffb44638 svchost.exe 1220 664 10 153 0 0 2009-10-24 10:48:34 UTC+0000

0xffb153c0 cmd.exe 1012 1704 1 20 0 0 2009-10-24 11:01:34 UTC+0000

0x81067da0 win32dd.exe 1020 1012 1 21 0 0

…

Al continuar investigando, se obtiene una dirección del disco sospechosa:

caine@caine:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Documents/memoriacp.dd modscan

Offset(P) Name Base Size File

------------------ -------------------- ---------- ---------- ----

0x000000000111ffa0 imapi.sys 0xfdecb000 0xb000 \SystemRoot\system32\DRIVERS\imapi.sys

0x0000000001120008 ndiswan.sys 0xfdb22000 0x17000 \SystemRoot\system32\DRIVERS\ndiswan.sys

0x00000000011206d8 serial.sys 0xfdebb000 0x10000 \SystemRoot\system32\DRIVERS\serial.sys

0x0000000001120dd8 kbdclass.sys 0xfe0db000 0x6000 \SystemRoot\system32\DRIVERS\kbdclass.sys

0x0000000001120e88 i8042prt.sys 0xfdeab000 0xd000 \SystemRoot\system32\DRIVERS\i8042prt.sys

0x0000000001124628 vmmouse.sys 0xfe327000 0x2000 \SystemRoot\system32\DRIVERS\vmmouse.sys

0x00000000011249b8 mouclass.sys 0xfe0e3000 0x6000 \SystemRoot\system32\DRIVERS\mouclass.sys

0x0000000001127008 serenum.sys 0xfe2af000 0x4000 \SystemRoot\system32\DRIVERS\serenum.sys

0x00000000011270e0 dump_atapi.sys 0xfc526000 0x18000 \SystemRoot\System32\Drivers\dump_atapi.sys

0x0000000001127688 parport.sys 0xfdbaa000 0x14000 \SystemRoot\system32\DRIVERS\parport.sys

0x0000000001127ac0 dump_WMILIB.SYS 0xfe337000 0x2000 \SystemRoot\System32\Drivers\dump_WMILIB.SYS

0x0000000001128638 win32dd.sys 0xfc123000 0xc000 \??\C:\Imagers\Win32dd\win32dd.sys

0x0000000001129008 TDI.SYS 0xfe10b000 0x5000 \SystemRoot\system32\DRIVERS\TDI.SYS

0x000000000112e688 msdirectx.sys 0xfc3b6000 0x10000 \??\C:\Malware\FUto\msdirectx.sys

…

Mediante el “plugin” ”modscan”, obtenemos más información del mismo:

caine@caine:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Documents/memoriacp.dd modscan

Offset(P) Name Base Size File

------------------ -------------------- ---------- ---------- ----

0x0000000001120008 ndiswan.sys 0xfdb22000 0x17000 \SystemRoot\system32\DRIVERS\ndiswan.sys

0x00000000011206d8 serial.sys 0xfdebb000 0x10000 \SystemRoot\system32\DRIVERS\serial.sys

0x0000000001120dd8 kbdclass.sys 0xfe0db000 0x6000 \SystemRoot\system32\DRIVERS\kbdclass.sys

0x0000000001120e88 i8042prt.sys 0xfdeab000 0xd000 \SystemRoot\system32\DRIVERS\i8042prt.sys

0x0000000001124628 vmmouse.sys 0xfe327000 0x2000 \SystemRoot\system32\DRIVERS\vmmouse.sys

0x00000000011249b8 mouclass.sys 0xfe0e3000 0x6000 \SystemRoot\system32\DRIVERS\mouclass.sys

0x0000000001127008 serenum.sys 0xfe2af000 0x4000 \SystemRoot\system32\DRIVERS\serenum.sys

0x00000000011270e0 dump_atapi.sys 0xfc526000 0x18000 \SystemRoot\System32\Drivers\dump_atapi.sys

0x0000000001127688 parport.sys 0xfdbaa000 0x14000 \SystemRoot\system32\DRIVERS\parport.sys

0x0000000001127ac0 dump_WMILIB.SYS 0xfe337000 0x2000 \SystemRoot\System32\Drivers\dump_WMILIB.SYS

0x0000000001128638 win32dd.sys 0xfc123000 0xc000 \??\C:\Imagers\Win32dd\win32dd.sys

0x0000000001129008 TDI.SYS 0xfe10b000 0x5000 \SystemRoot\system32\DRIVERS\TDI.SYS

0x000000000112e688 msdirectx.sys 0xfc3b6000 0x10000 \??\C:\Malware\FUto\msdirectx.sys

…

Al parecer la máquina ha sido comprometida por un malware llamado "C:\Malware\FUto\fu.exe", haciendo uso de la librería "C:\Malware\FUto\msdirectx.sys", como se verá a continuación.

La información obtenida de las conexiones y sockets parece limitada, sin embargo se pueden observar ciertos sockets en acción:

caine@caine:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Documents/memoriacp.dd sockets

Offset(V) PID Port Proto Protocol Address Create Time

---------- -------- ------ ------ --------------- --------------- -----------

0x811523c0 4 138 17 UDP 192.168.150.130 2009-10-24 10:48:37 UTC+0000

0xffb2fa40 1068 123 17 UDP 192.168.150.130 2009-10-24 10:48:38 UTC+0000

0x81066a78 4 445 6 TCP 0.0.0.0 2009-10-24 10:48:21 UTC+0000

0x8109cd80 960 135 6 TCP 0.0.0.0 2009-10-24 10:48:34 UTC+0000

0x8120d508 408 31337 6 TCP 0.0.0.0 2009-10-24 10:56:47 UTC+0000

0xffb2f608 1068 123 17 UDP 127.0.0.1 2009-10-24 10:48:38 UTC+0000

0x81176cc0 1220 1900 17 UDP 192.168.150.130 2009-10-24 10:51:13 UTC+0000

0x8114fbf0 4 139 6 TCP 192.168.150.130 2009-10-24 10:48:37 UTC+0000

0x8112d500 4 137 17 UDP 192.168.150.130 2009-10-24 10:48:37 UTC+0000

0x81067538 1220 1900 17 UDP 127.0.0.1 2009-10-24 10:51:13 UTC+0000

0x81066cc0 4 445 17 UDP 0.0.0.0 2009-10-24 10:48:21 UTC+0000

Se identifica el puerto 31337, no relacionado directamente con servicios conocidos (con protocolo 6 TCP).

caine@caine:/usr/share/caine/pacchetti/volatility$ ./vol.py -f /home/caine/Documents/memoriacp.dd sockscan

Offset(P) PID Port Proto Protocol Address Create Time

---------- -------- ------ ------ --------------- --------------- -----------

0x01020a78 4 445 6 TCP 0.0.0.0 2009-10-24 10:48:21 UTC+0000

0x01020cc0 4 445 17 UDP 0.0.0.0 2009-10-24 10:48:21 UTC+0000

0x01021538 1220 1900 17 UDP 127.0.0.1 2009-10-24 10:51:13 UTC+0000

0x01056d80 960 135 6 TCP 0.0.0.0 2009-10-24 10:48:34 UTC+0000

0x010e7500 4 137 17 UDP 192.168.150.130 2009-10-24 10:48:37 UTC+0000

0x01109bf0 4 139 6 TCP 192.168.150.130 2009-10-24 10:48:37 UTC+0000

0x0110c3c0 4 138 17 UDP 192.168.150.130 2009-10-24 10:48:37 UTC+0000

0x01130cc0 1220 1900 17 UDP 192.168.150.130 2009-10-24 10:51:13 UTC+0000

0x011c7508 408 31337 6 TCP 0.0.0.0 2009-10-24 10:56:47 UTC+0000

0x0264babc 0 7266 8456 - 128.206.46.0 -

0x02a49608 1068 123 17 UDP 127.0.0.1 2009-10-24 10:48:38 UTC+0000

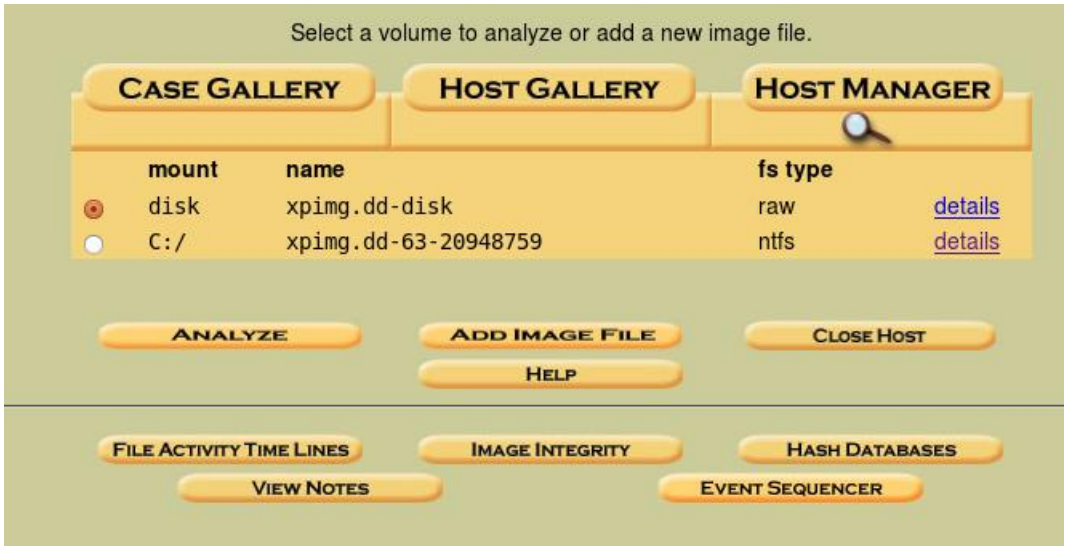
0x02a49a40 1068 123 17 UDP 192.168.150.130 2009-10-24 10:48:38 UTC+0000

1. Información no volátil - Análisis Disco

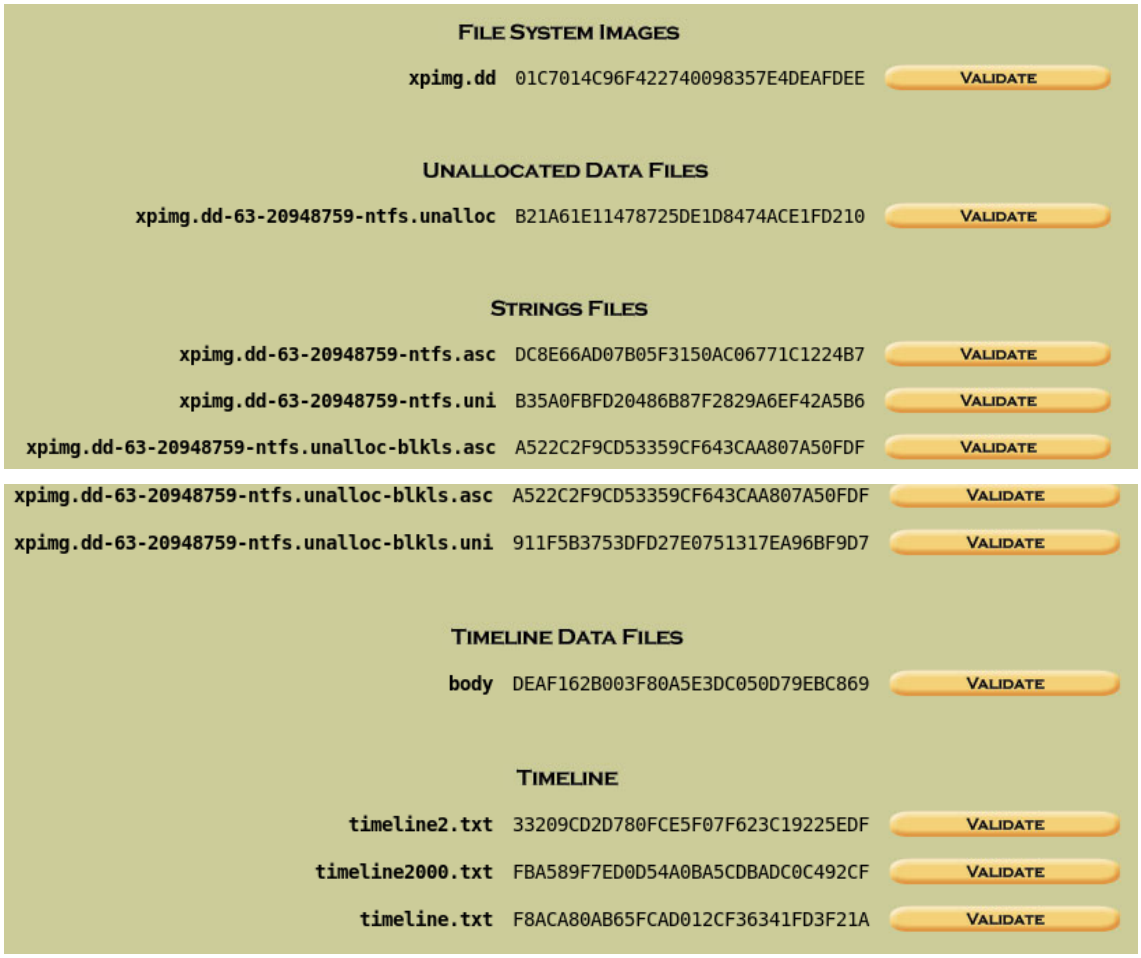
Análisis básico de imagen de disco con Autopsy – <u>TALLER 4</u>

Procedemos a cargar la copia del disco a analizar con la herramienta Autopsy, incluida en la distribución "live CD" CAINE para analizarla, a fin de buscar archivos específicos y volcarlos, analizar metadatos, archivos borrados, línea temporal, realizar búsquedas de ficheros por extensión o nombre, etc…

Para ello, crearemos un nuevo caso:

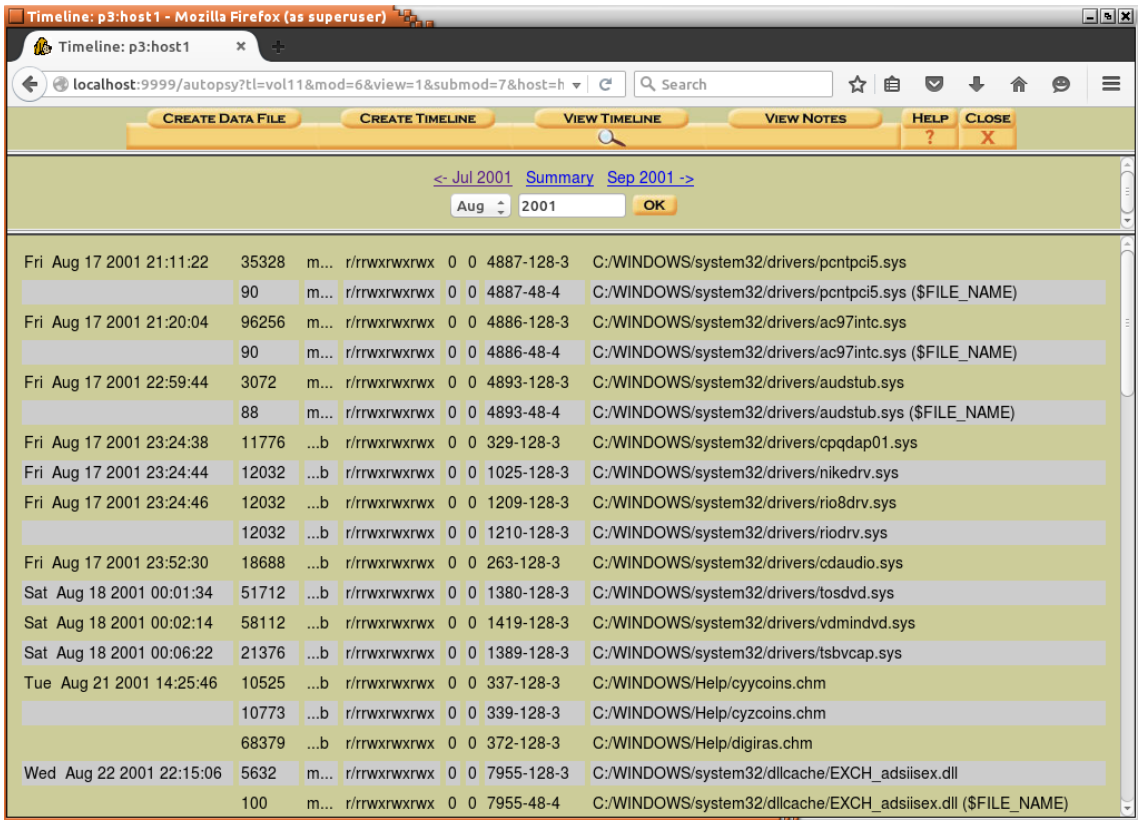


Y calculamos todos las firmas hash para poder verificar la integridad de los datos y la imagen por completo al terminar nuestro análisis. Se muestran a continuación:



Creación de línea temporal – <u>TALLER 4 (CONT.)</u>

A continuación crearemos el “timeline” de archivos del sistema mediante Autopsy, con el que podemos observar creación y modificación de ficheros ordenados por fecha, con posibilidad de exportar a fichero:



Autopsy ofrece plugins mediante los cuales tenemos opciones adicionales para el análisis como:

- Búsqueda de ficheros por nombre o extensión
- Ficheros eliminados (sombreados en rojo)
- Firmado de copias y verificación de las mismas

Master Boot Record (MBR)

MBR corresponden a las siglas del primer sector de un dispositivo de almacenamiento, utilizado para el arranque del sistema operativo y normalmente contiene la tabla de particiones. Comprende los primeros 512 bytes (sector 0), y dentro de él se encuentra la tabla de particiones, alojada a partir del byte 446.

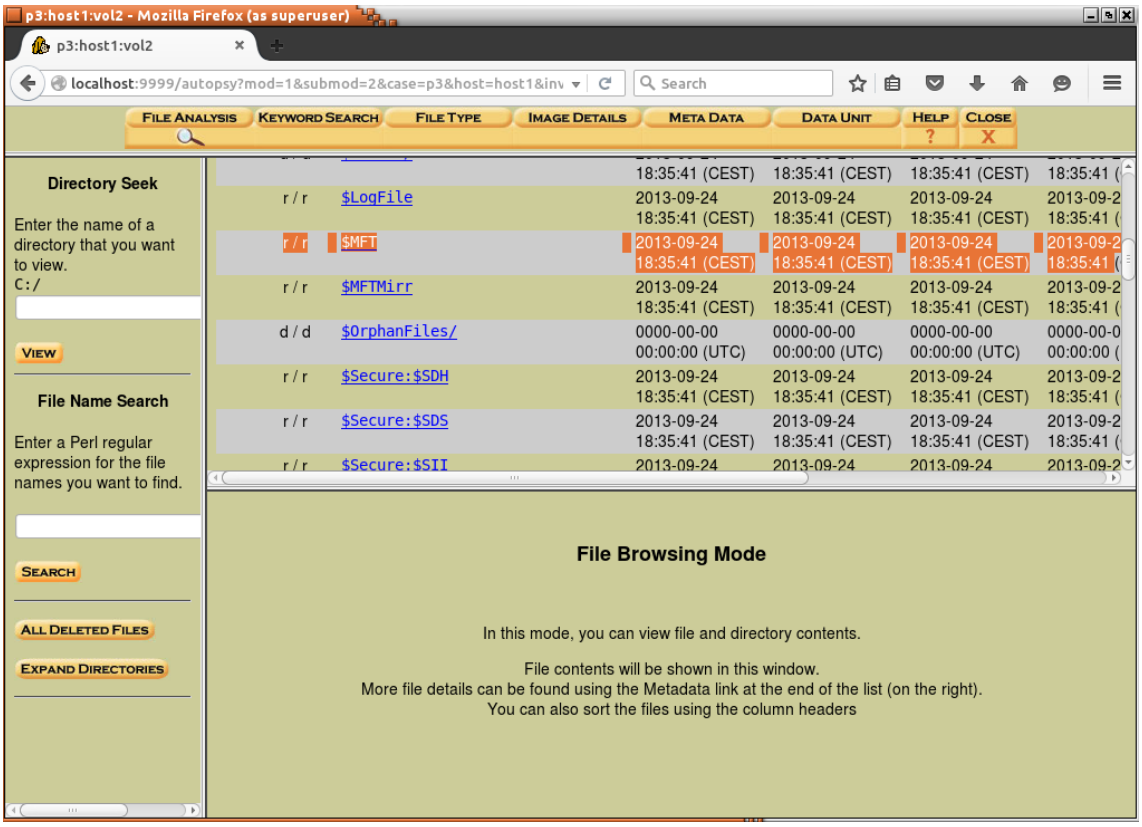
La tabla de particiones ocupa 64 bytes, conteniendo 4 registros de 16 bytes, los cuales definen las particiones primarias (estas a su vez pueden tener particiones extendidas). En ellas se almacena toda la información básica sobre la partición: el formato, el tamaño, si es arrancable o no y el sector de inicio.

Para extraerla se puede utilizar la herramienta MBRutil55, mediante la siguiente instrucción:

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

Master File Table (MFT)

La tabla maestra de archivos (o $MFT) es el primer archivo de un volumen de tipo NTFS (el tipo más común y estandarizado en sistemas Windows actuales) que contiene todos y cada uno de los archivos que componen un volumen. Si el SO realiza una consulta, en primer lugar se dirige a la $MFT para obtener información del mismo, como por ejemplo tamaño, propiedades, atributos, localización, nombres de archivos… etc.



Se volcará o extraerá y "parseará" la tabla desde una imagen de disco el archivo $MFT (Archivo de registro base para un volumen NTFS) haciendo uso de SLEUTHKIT: mmls (averiguar la posición del offset de inicio de Windows) y volcado de información mediante la herramienta: "icat", incluida en SLEUTHKIT a un archivo con extensión ".mft", que posteriormente convertimos a formato CSV mediante la herramienta "analyzeMFT".

Un método alternativo para exportar la Master File Table desde el propio sistema operativo de Windows al realizar un análisis en caliente, es utilizar alguna herramienta como Ntfswalk56, haciendo uso de la siguiente instrucción:

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

Registro de Windows

El Registro de Windows, es una base de datos que almacena las configuraciones y opciones del sistema operativo Microsoft Windows.

Contiene información y configuraciones e históricos de todo el hardware, software, usuarios, y preferencias del PC.

La Información en el Registro se ordena en un sistema de árbol, normalmente de gran dimensión y su información se guarda en claves.

Para analizarlo, podemos utilizar herramientas como “Forensic Registry Editor” (FRED) o la herramienta nativa de Windows “regedit”.

El registro está dividido en 5 secciones:

- HKEY_CURRENT_USER: Contiene la información de configuración del usuario que ha iniciado sesión, carpetas del usuario, los colores de la pantalla y la configuración del Panel de control. Esta clave en ocasiones aparece abreviada como HKCU.
- HKEY_CURRENT_CONFIG: Contiene información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema.
- HKEY_LOCAL_MACHINE: Contiene información de configuración específica del equipo (para cualquier usuario). Esta clave en ocasiones aparece abreviada como HKLM.
- HKEY_CLASSES_ROOT: Relaciona los programas con sus archivos. Contiene la relación entre las extensiones de archivos y los archivos en el sistema. Esta información también se encuentra en HKEY_LOCAL_MACHINE\Software.
- HKEY_USERS: Contiene todos los perfiles de usuario cargados activamente en el equipo. Esta clave en ocasiones aparece abreviada como HKU.

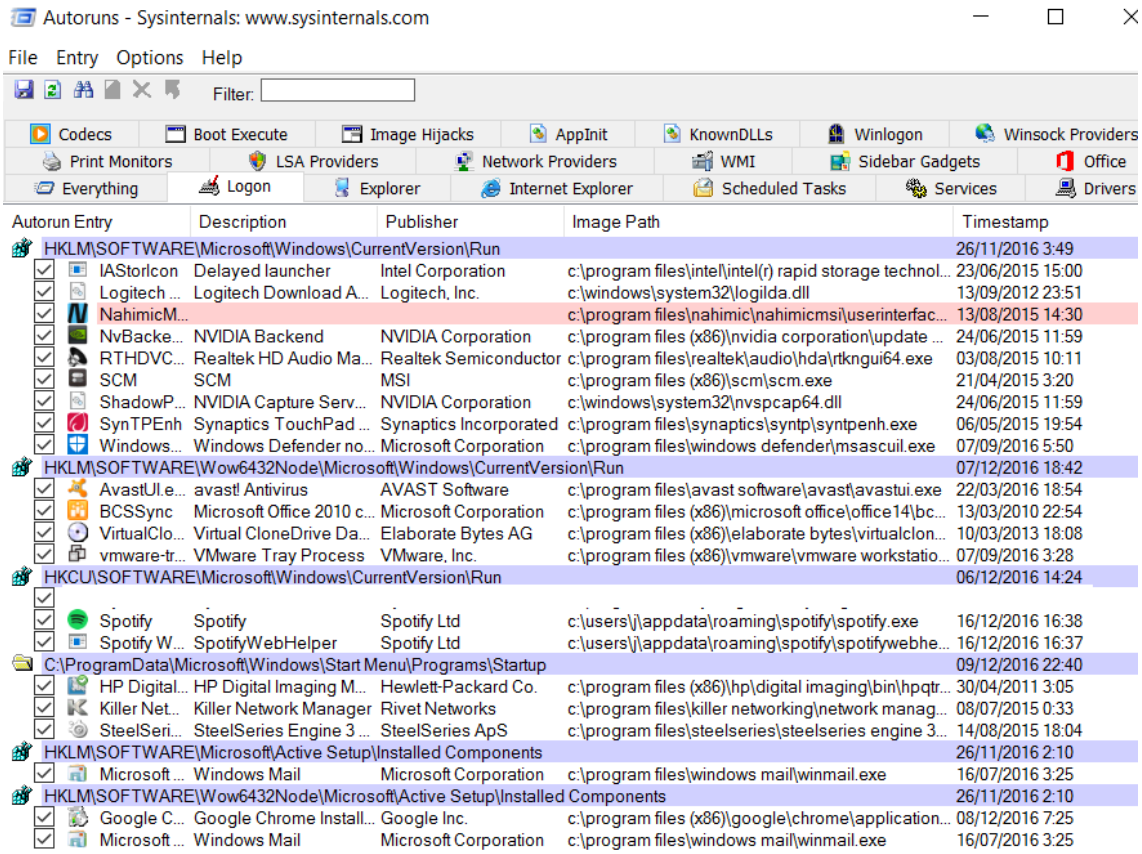
Los siguientes archivos, que se encuentran en el directorio “C:\Windows\System32\config”, contienen datos de las ramas correspondientes:

- Security - HKEY_LOCAL_MACHINE\SECURITY
- Software - HKEY_LOCAL_MACHINE\SOFTWARE
- Sam - HKEY_LOCAL_MACHINE\SAM
- System - HKEY_LOCAL_MACHINE\SYSTEM
- Default - HKEY_USERS\.DEFAULT

En cada carpeta de usuario se encuentra un archivo de nombre Ntuser.dat, que se encuentran en el directorio C:\Users\NombreDeUsuario\Ntuser.dat, y contiene los datos referentes a la rama de dicho usuario como registros de seguimiento y dentro del mismo directorio se localiza otro fichero de interés: C:\Users\NombreDeUsuario\AppData\Local\Microsoft\Windows\UsrClass.dat

AutoRuns

Muestra qué programas están configurados para ejecutarse durante el inicio del sistema o el inicio de sesión, las entradas en el orden en que Windows las procesa. Se puede recolectar información a través de la herramienta nativa "reg.exe" o la herramienta AutoRuns de Sysinternals (Microsoft).



Algunos de los registros a destacar son:

- Se puede consultar el nombre actual del equipo en la siguiente ubicación: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName\ ActiveComputerName
- Encontrar el momento en que el equipo fue apagado la última vez en: HEY_LOCAL_MACHINE\System\ControlSet00x\Control\Windows (Generalmente ControlSet001, o ControlSet002)
- La Información sobre la Zona Horaria se encuentra en: HEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
- Información sobre Nombre del producto, versión, etc.: HEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
- La información sobre recursos compartidos se encuentra en: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\Shares
- El registro del archivo de intercambio se encuentra en: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

- El siguiente registro se encarga de indicar al sistema si debe limpiar el archivo de paginación al apagar la máquina:
  MACHINE/System/CurrentControlSet/Control/Session Manager/Memory Management/ClearPageFileAtShutdown
- La clave MountedDevices almacena información sobre varios dispositivos y volúmenes montados en el sistema de archivo NTFS:
  HKEY_LOCAL_MACHINE\System\MountedDevice

- Las aplicaciones mantienen una lista MRU, que se trata de una lista de los archivos más accedidos recientemente, contenida en la clave:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

- TypedURLs mantiene una lista de URLs que el usuario ha escrito en la barra de direcciones:
  HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

- RunMRU contiene la lista de valores escritos en el cuadro "Ejecutar como":
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

- El siguiente registro mantiene una lista de archivos abiertos o guardados:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU

- La clave Network Drive MRU muestra las Unidades de Red:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Map

- Para consultar los puntos de restauración del sistema se accederá a la clave:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints

- Los ajustes de puntos de restauración se encuentran ubicados en:
  HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore

A la hora de buscar malware, se recomienda revisar también las claves de registro alojadas en las siguientes ubicaciones:

- HKEY_LOCAL_MACHINE\Software\Classes\Exefile\Shell\Open\command
- HKEYE_CLASSES_ROOT\Exefile\Shell\Open\Comand

Cuando un dispositivo USB es identificado, la clave de registro será creada debajo de la clave:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR

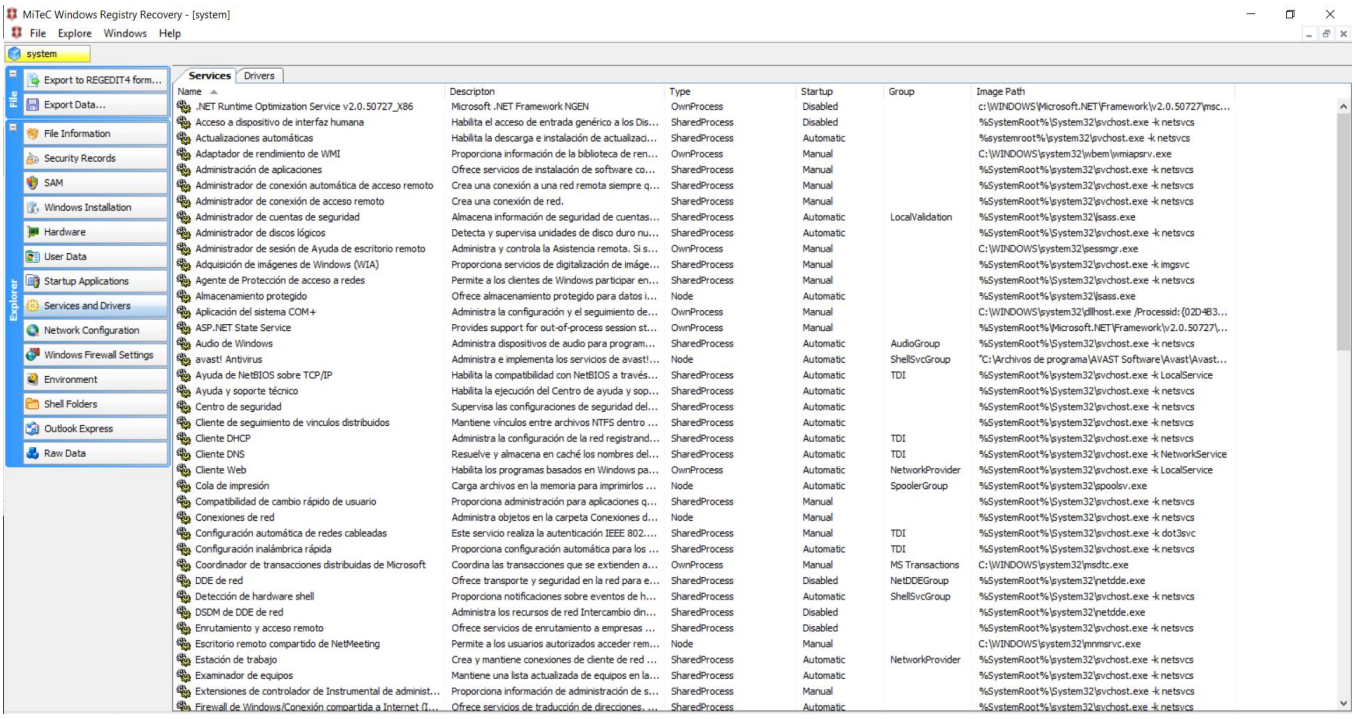
Por último, se resumirán el resto de claves relativas al registro de Windows relevantes:

Clave de Registro	Notas
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Todos los valores de esta clave se ejecutan al Iniciar el Sistema
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce	Todos los valores de esta clave se ejecutan al Iniciar el Sistema una sola vez y posteriormente son eliminados
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\WinLogon	Almacena el último nombre de usuario introducido en el cuadro de diálogo al Iniciar sesión en Windows.
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components	Cada subclave representa un componente instalado.
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\run	Si Explorer y run están presentes, los valores incluidos son ejecutados ejecutarse Explorer
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager	El valor BootExecute contiene archivos de aplicaciones nativas ejecutadas antes de la ejecución de Windows
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services	Contiene una lista de servicios que se ejecutan cuando el Sistema inicia. Si el valor Start es 2, el inicio es automático. Si el valor es 3, el inicio es manual. Si el valor es 4, el servicio está deshabilitado
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog9\Catalog_Entries	Estas claves se destinan a servicios por capas, todos los valores se ejecutan antes de que el Usuario inicie sesión
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run	Todos los valores de esta clave se ejecutan cuando el usuario inicia sesión
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce	Todos los valores de esta clave se ejecutan cuando el usuario inicia sesión y posteriormente eliminados
HKEY_CURRENT_USER\Control Panel\Desktop	Para el usuario específico, el protector de pantalla está habilitado, un valor llamado srnsave.exe está presente.
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows	Para el usuario específico, la cadena especificada en el valor se ejecuta cuando el usuario inicia sesión

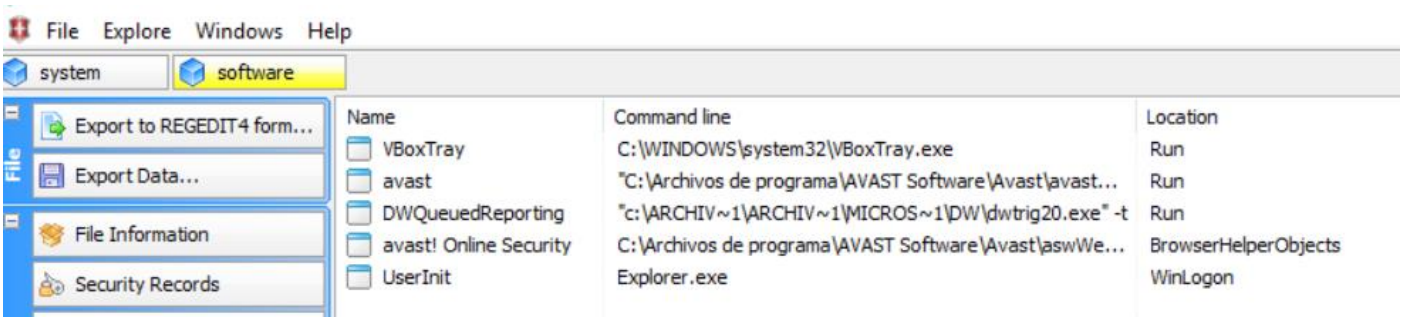
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	Para el usuario específico, la cadena especificada en el valor se ejecuta cuando el usuario inicia sesión
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	El valor Startup será C:\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup donde %username% es el nombre del usuario actual
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	El valor Startup será %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Se encuentran las rutas de le los Documentos, escritorio, etc. públicos

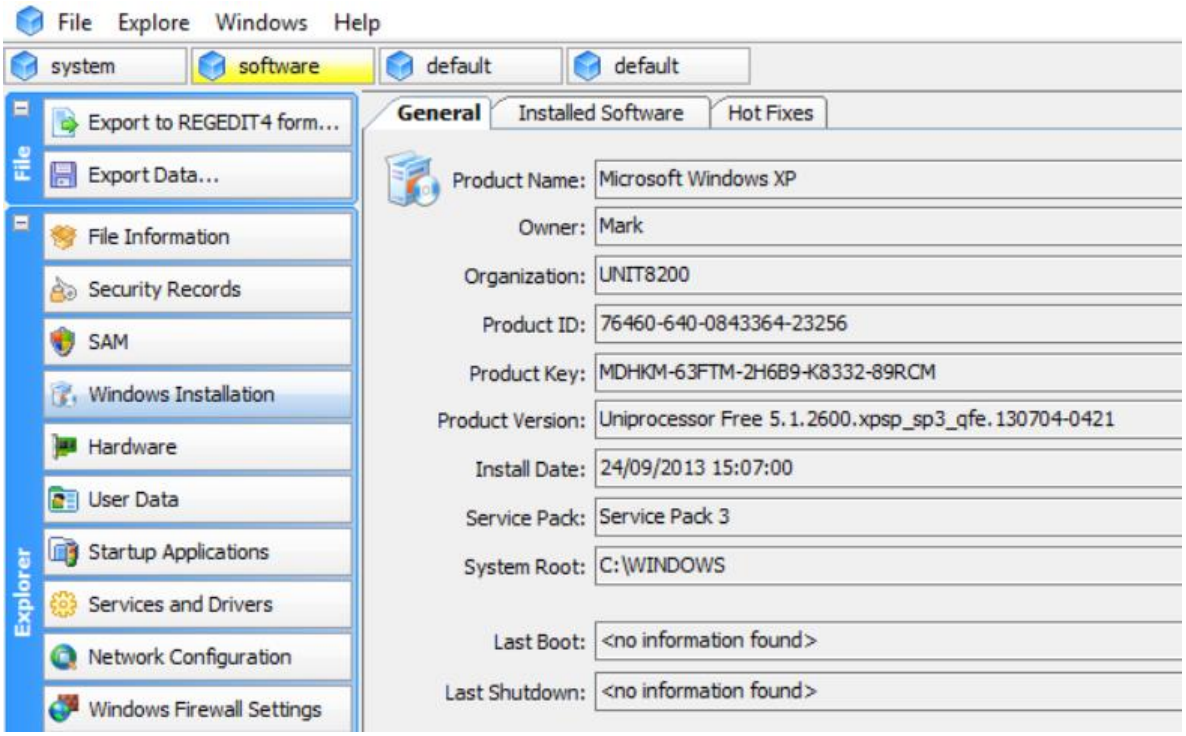
TALLER 5 - **Búsqueda en los archivos de registro de Windows principales** alojados en la carpeta WINDOWS\system32\config y su posterior análisis mediante la herramienta "Windows Registry Recovery". Los siguientes archivos del Registro importantes, con posibilidad de análisis en frio, se encuentran en %SystemRoot%System32Config:

- Sam – HKEY_LOCAL_MACHINESAM
- Security – HKEY_LOCAL_MACHINESECURITY
- Software – HKEY_LOCAL_MACHINESOFTWARE
- System – HKEY_LOCAL_MACHINESYSTEM
- Default – HKEY_USERSDEFAULT
- Userdiff



Aplicaciones en arranque de sistema:





Análisis básico de malware - TALLER 6. Keylogger

Como método alternativo en la búsqueda de malware, además de revisar todos los archivos de interés de Windows mencionados en esta propuesta de guía, se podría hacer uso de una copia del disco, montándola de forma protegida contra escritura, es decir en modo solo lectura a una máquina de análisis. En esta máquina se podrán realizar análisis de malware y antivirus con herramientas convencionales sobre la unidad, así como utilizar la web virustotal.com y similares para analizar los archivos más sospechosos hasta dar con los archivos relativos al malware que se desea descubrir.

Para comenzar el análisis del malware en cuestión, se procede a arrancar la máquina virtual en un entorno controlado (podríamos también realizar un volcado de memoria RAM para posteriormente analizarla con Volatility, fijándose en todos los procesos activos, siendo esta, por lo general, una forma menos intrusiva de análisis).

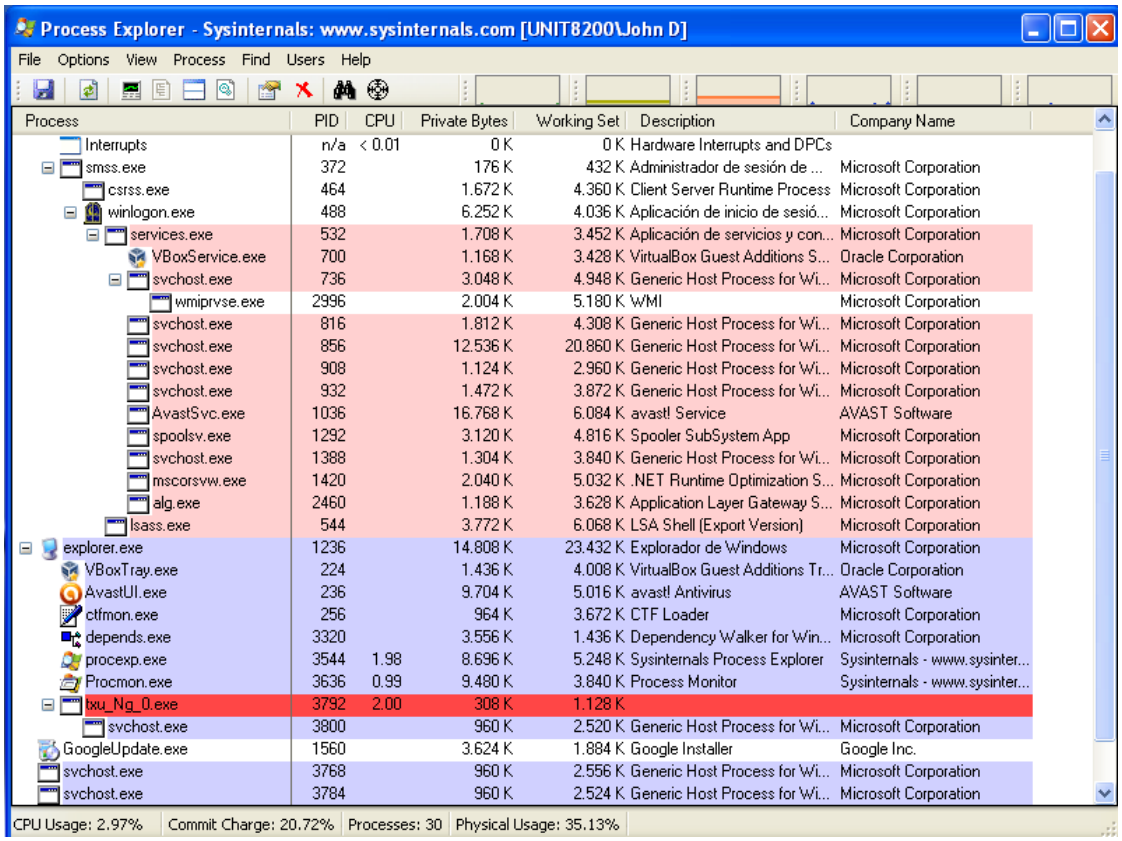
Durante los siguientes párrafos, se realizará un taller en el que se pretende obtener la máxima información posible sobre un malware que ha sido detectado en una máquina con sistema operativo Windows XP (imagen de sistema corriendo sobre VirtualBox a modo de "víctima").

Se comenzará a realizar ingeniería inversa sobre el fichero "txu_Ng_0.exe" sospechoso. Estos métodos específicos se conocen como análisis de malware (tanto dinámico como estático). Para ello, en este caso concreto haremos uso de las herramientas "Process Explorer", "Dependency Walker", y "PEiD".

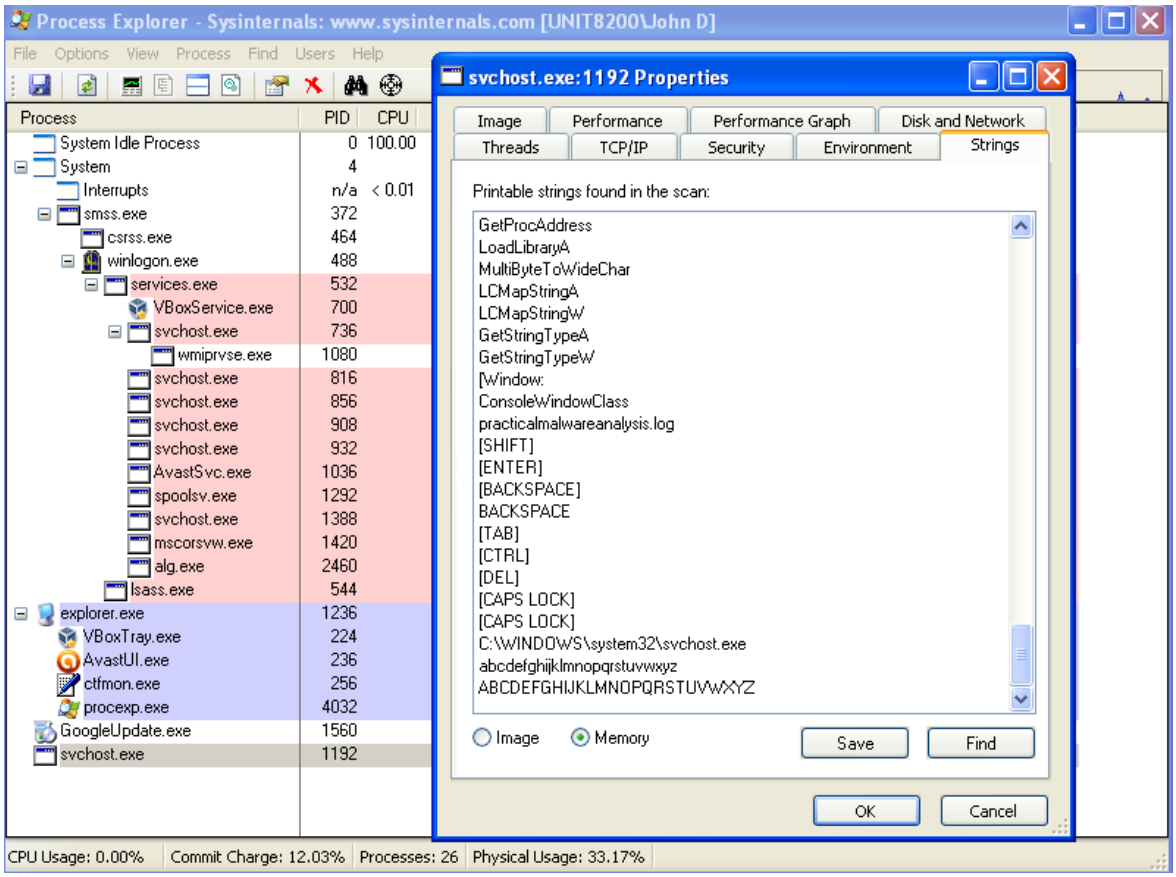
Análisis dinámico de malware

En esta parte analizaremos cómo se comporta el malware al ejecutarlo, de forma dinámica haciendo uso de herramientas específicas y bajo un entorno controlado en el que se ha instalado una copia exacta del sistema operativo original.

Comenzamos analizando mediante "Process Explorer", como podemos ver en la siguiente imagen, al poco tiempo de lanzar el malware, este migra al proceso svchost.exe, desapareciendo txu_Ng_0.exe y quedando en ejecución en memoria el proceso svchost.exe infectado, comportamiento que confirma que se trata de malware:



Mediante esta herramienta, también podemos observar las cadenas del malware, en este caso interesan las alojadas en memoria:

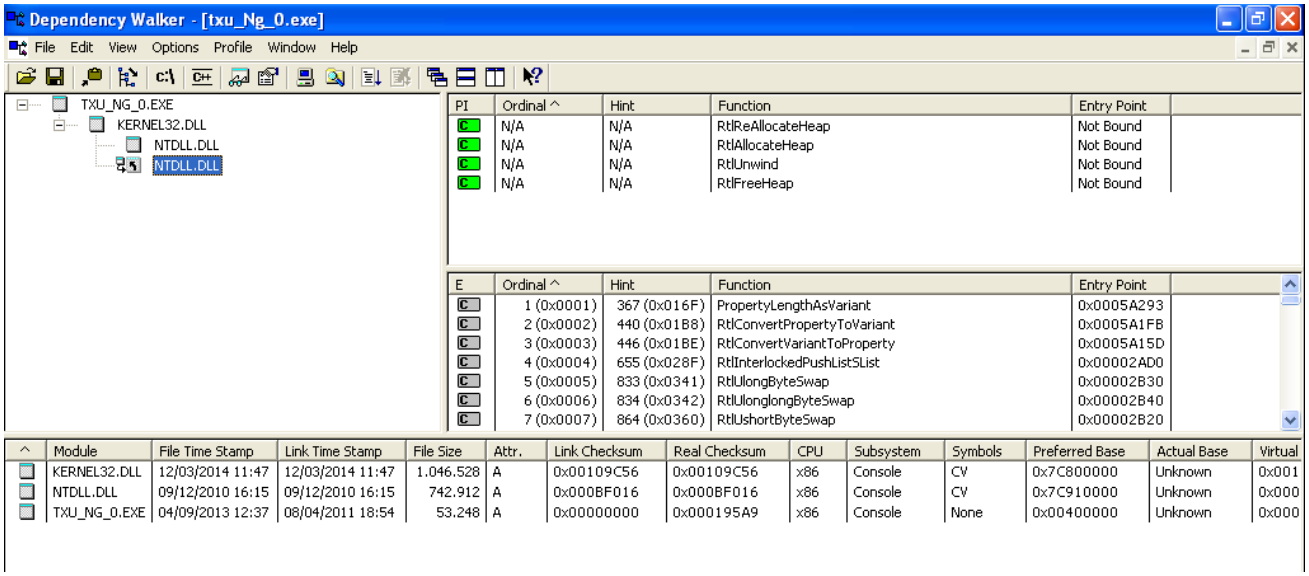


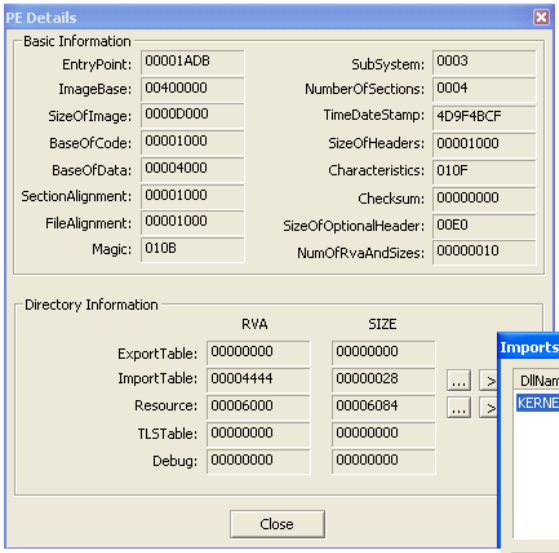
Como vemos recoge en el archivo practicalmalwareanalysis.log todas las pulsaciones del teclado (shift, enter, tab, backspace, del, abcdefghijklmnopqrstvwxyz, ABCDEFGHIJKLMNOPQRSTVWXYZ, etc…), por ello confirmamos que se trata de un malware tipo keylogger.

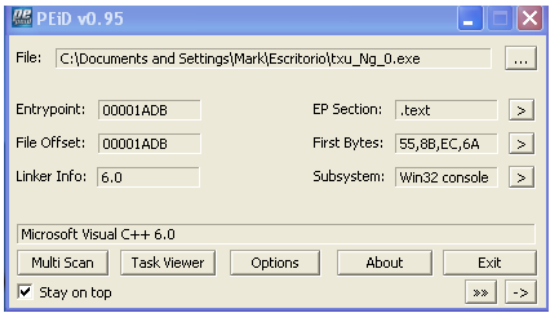
Análisis estático de malware

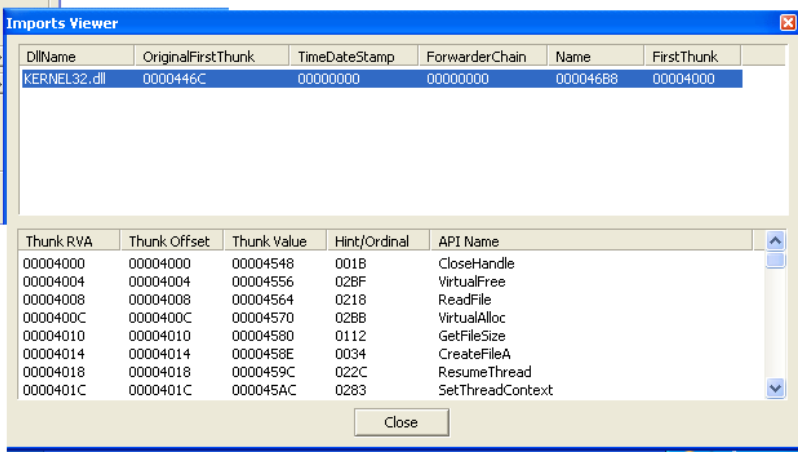
En esta parte se analizará el código del malware mediante herramientas específicas.

Mediante “Dependency Walker” y PEiD, se pueden observar las librerías de las que depende o hace uso el malware, KERNELL32.DLL y su hijo NTDLL.DLL:



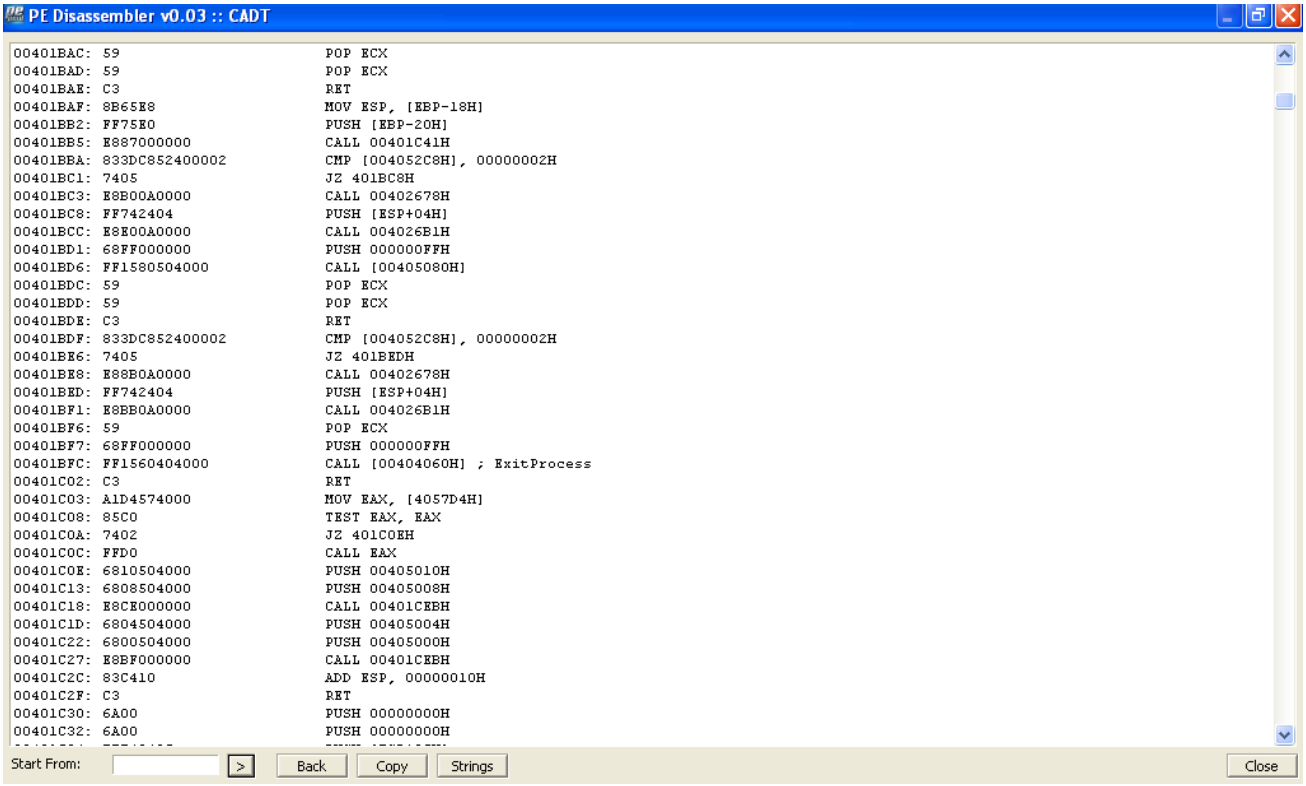


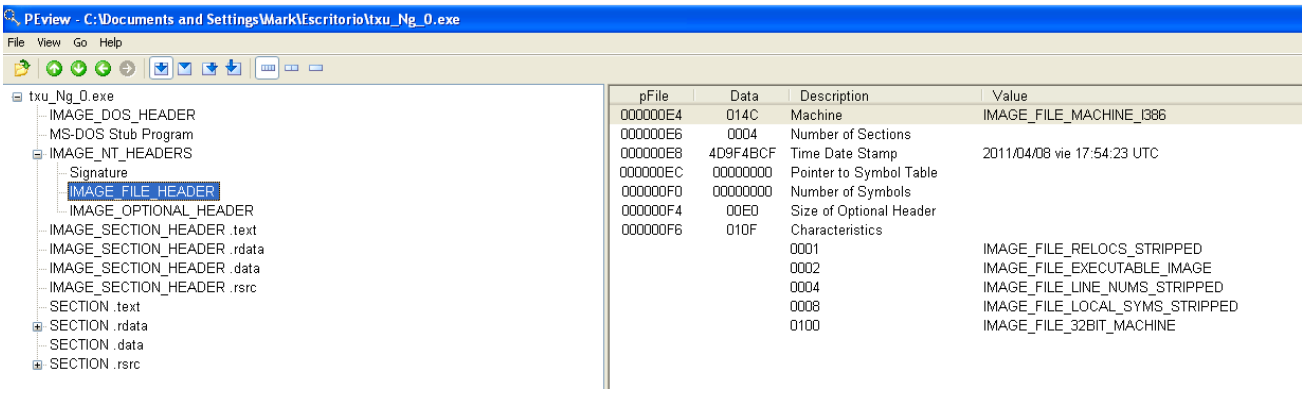




KERNELL32.dll se trata de una librería de Windows muy utilizada por malwares, que incluye funcionalidades como acceso y manipulación de memoria, archivos, así como creación de procesos y hardware.

Por último observamos el archivo desensamblado:





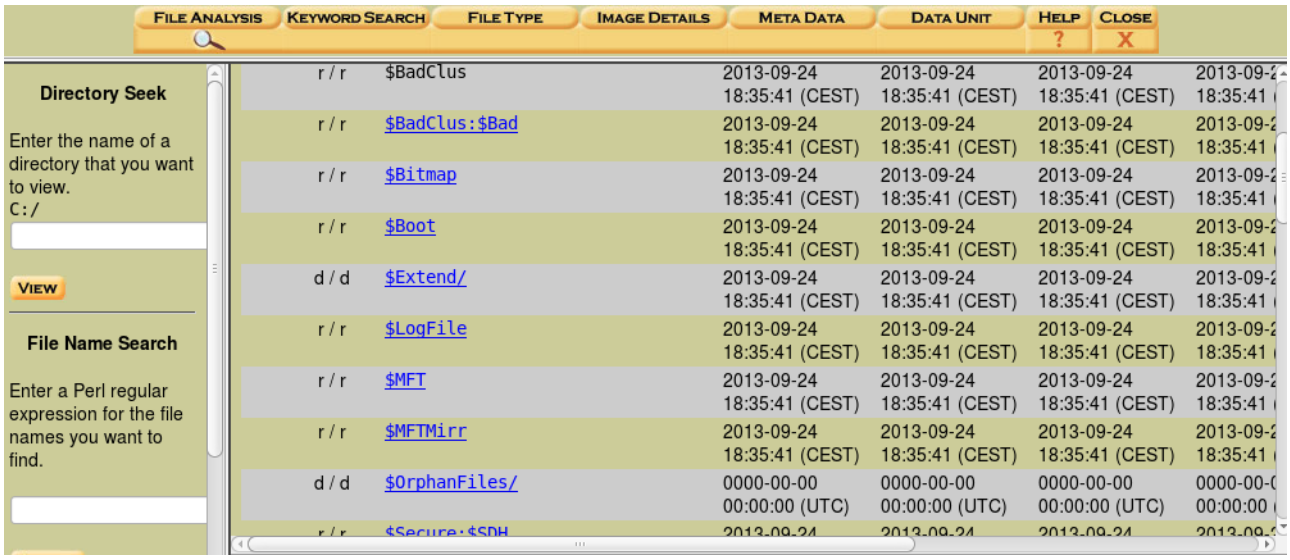
Ficheros y directorios importantes NTFS e instalación Windows

Además de los ficheros mencionados, también se analizaron (puesto que también se consideran importantes), extrayéndolos y revisando tanto su código en hexadecimal como ASCII:

autoexec.nt, config.nt, default, secsetup.inf, setup.log y ntuser.dat (registros de seguimiento de las actividades del usuario).

Así como análisis de pagefile.sys e hiberfile.sys, por ejemplo haciendo uso de la herramienta WinHex u OllyDbg.

También se recomienda analizar los siguientes ficheros de sistema con contenido importante:



Función de los componentes principales dentro de un sistema de archivos NTFS:

- $AttrDef – Lista de atributos de los archivos.
- $BadClus –Lista de clúster o sectores que tienen errores irrecuperables.
- $Bitmap – Lista de disponibilidad y uso de los clústeres.
- $Boot – Utilizado para montar el volumen NTFS durante el proceso de arranque.
- $LogFile –Transacciones previas listadas y almacenadas para posibles restauraciones.
- $MFTMirr – Almacena los primeros cuatro registros del MFT como copia parcial de la MFT primaria.
- $Secure – Lista de control de acceso
- $Volumen –Almacena información relacionada al volumen.
- $Upcase – Utilizado para convertir todos los caracteres en mayúscula a caracteres Unicode minúscula.
- $Extend – Extensiones opcionales como cuotas e identificadores de objetivo.

Archivos eliminados

La propia herramienta Autopsy extrae datos y ficheros eliminados que no hayan sido sobrescritos. Para profundizar en el análisis e ficheros eliminados, podemos utilizar herramientas como Foremost o DDRescue, llegando a recuperar información eliminada (cuyo índice se ha borrado de memoria pero la información sigue en disco sin ser

sobrescrita) de todos los sectores del disco, incluso llegar a reparar sectores o las tablas de particiones.

Carpeta "prefetch"

La carpeta "prefetch" se encuentra en la siguiente ubicación:

%systemroot%prefetch

Podríamos decir que se trata de la cache de Windows para programas de uso frecuente para cargar dichos programas con 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, datos de árbol de directorio, clúster inválidos, etc.

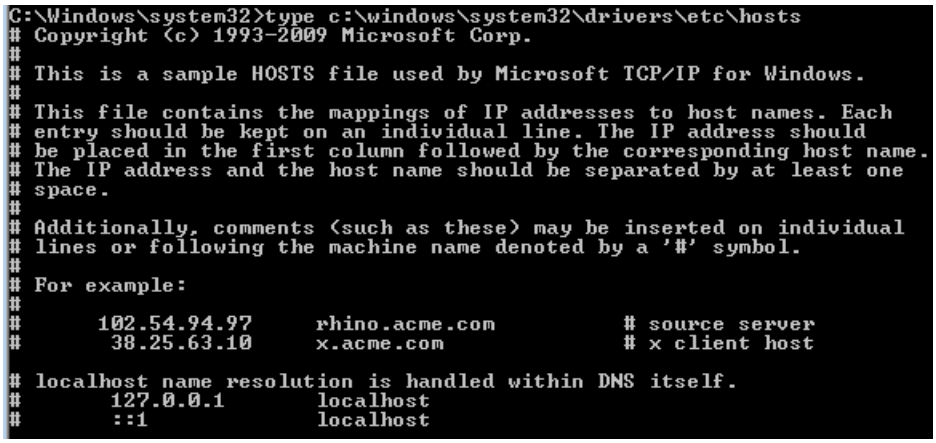
Fichero hosts

Se trata de un fichero sin extensión en texto plano, utilizado por Windows para asociar nombres de dominio con direcciones IP. Si este archivo existe el sistema lo examina antes de hacer una consulta a un servidor DNS.

Puede ser utilizado para redirigir dominios locales o bloquear cierto contenido o direcciones de internet. En muchos sistemas operativos este método es usado preferentemente respecto a otros como el DNS.

Podemos consultarlo de forma rápida mediante la instrucción:

type c:\windows\system32\drivers\etc\hosts



O analizarlo posteriormente desde una imagen de disco, abriendo con un editor el archivo "hosts" ubicado en la carpeta "c:\windows\system32\drivers\etc\".

Tareas programadas

Para visualizar las tareas programadas en Windows se utiliza el siguiente comando:

schtasks

También es útil obtener el fichero schedlgu.txt ubicado en %WinDir%\Tasks, donde se almacena el log de las tareas programadas que se han ejecutado.

Logs de sistema Windows

Estos ficheros de texto almacenan información histórica relevante que ha ocurrido en el sistema.

La clave de registro mantiene la configuración de log de eventos se encuentra en: HEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\<Log del Evento>

Entre los "logs" más importantes en Windows, podemos destacar los siguientes:

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.

Windows Event Logs

Dentro de los logs de eventos de Windows se puede destacar 3 que tienen especial importancia:

a. AppEvent.evt: Registra los sucesos relativos a aplicaciones.
b. SysEvent.evt: Registra los sucesos relativos al sistema.
c. SecEvent.evt: Registra los sucesos relativos a la seguridad.

Ubicados en %systemroot%\system32\winevt\Logs, se pueden exportar mediante la herramienta de Windows "wevtutil" ejecutando las siguientes instrucciones en una consola:

- 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"

El comando wevtutil permite recuperar información sobre los logs de eventos de Windows

wevtutil /?

Ver las opciones del comando

wevtutil el
Lista los registros de eventos disponibles en el Sistema

wevtutil gl log name
Lista la información de configuración sobre un log de evento específico

La información mostrada por este comando está también disponible en HKEY_LOCAL_MACHINE\System\ControlSet00x\Services\EventLog\nombre de log

pfirewall.log

Se encuentra ubicado en la carpeta %WinDir%\System32\LogFiles\Firewall y almacena diferente información correspondiente al firewall de Windows como por ejemplo paquetes perdidos o conexiones que se han realizado correctamente.

Análisis de Metadatos

- **Metadatos descriptivos**: Describe un recurso para propósitos de descubrimiento e identificación. Incluye información como título, abstract, autor, palabras clave.
- **Metadatos estructurales**: Información que facilita la navegación, presentación y recursos electrónicos.
- **Metadatos administrativos**: Provee información para ayudar a administrar un recurso, incluyendo el tipo de archivo y otra información técnica y quién accedió a él.

```
~$ exiftool /home/      /Desktop/vol2-C..WINDOWS.system32.txu_Ng_0.e
xe
ExifTool Version Number         : 9.46
File Name                       : vol2-C..WINDOWS.system32.txu_Ng_0.exe
Directory                       : /home/      /Desktop
File Size                       : 52 kB
File Modification Date/Time     :
File Access Date/Time           :
File Inode Change Date/Time     :
File Permissions                : rw-r--r--
File Type                       : Win32 EXE
MIME Type                       : application/octet-stream
Machine Type                    : Intel 386 or later, and compatibles
Time Stamp                      : 2011:04:08 19:54:23+02:00
PE Type                         : PE32
Linker Version                  : 6.0
Code Size                       : 12288
Initialized Data Size           : 36864
Uninitialized Data Size         : 0
Entry Point                     : 0x1adb
OS Version                      : 4.0
Image Version                   : 0.0
Subsystem Version               : 4.0
Subsystem                       : Windows command line
```

Mediante la herramienta “exiftool”, entre otras de las muchas que podemos encontrar, como por ejemplo FOCA, podemos obtener información sobre el creador, fecha de creación y modificación, tipo de archivo, software utilizado, etc. En imágenes y ficheros de diferentes formatos en ocasiones podemos observar modelos, tiempos de exposición y otros datos de interés de cada fichero de la imagen de disco a analizar, dependiendo del tipo de fichero que se analice se pueden utilizar herramientas específicas para extraer esta información.

IV. Redacción de Informes

En esta fase, que se desarrolla a lo largo de toda la investigación, se redactan los informes que documenten los antecedentes del evento, método seguido y trabajo realizado y conclusiones generadas sobre el caso.

Para ello se redactan dos tipos de informes que en esencia contienen la misma información pero desde diferentes puntos de vista y grado de detalle, el informe técnico y el ejecutivo.

- **En el informe ejecutivo**

  Usará un lenguaje claro y sin tecnicismos, se debe evitar usar terminología propia de la ciencia e ingeniería. Hay que pensar que el público lector de estos informes serán jueces y gerentes que seguramente estén poco relacionados con el tema y además tengan poco tiempo para dedicarle. Se les debe facilitar la tarea de comprensión lectora al máximo.

  Este informe recoge todas las tareas llevadas a cabo con las evidencias, incluyendo motivos del incidente, desarrollo del mismo, resultados obtenidos en el análisis y recomendaciones para protegerse de un incidente de similares características en el futuro.

- **En el informe técnico**

  El público final será técnico y con conocimientos de la materia que se expone. Aquí se detallarán todos los procesos, los programas utilizados, las técnicas, procesos y metodología seguida. Se debe crear un documento que pueda servir de guía para reproducir todo el proceso que se ha realizado si fuese necesario.

  El informe técnico contendrá mucho más detalle que el anterior, incluyendo una exposición muy detallada de todo el análisis en profundidad y las conclusiones obtenidas. Entre los datos básicos que debe tener encontramos: antecedentes del incidente, metodología de recolección de evidencias, descripción de evidencias recolectadas, descripción del entorno de trabajo utilizado durante el

análisis, metodología y pasos llevados a cabo durante la fase de análisis de las evidencias, resultados obtenidos, línea temporal de hechos ocurridos, conclusiones y recomendaciones para protegerse de un incidente de similares características en el futuro.

Una de las normativas recomendadas antes de redactar un informe forense informático es la UNE 197001:2011, titulada "Criterios Generales para la elaboración de informes y dictámenes periciales".

5. BIBLIOGRAFÍA

[1] Forensic Engineering 2nd Edition (2001) - Kenneth L. Carper

[2] Técnicas Anti-Forenses y Seguridad Informática 3ª Edición (2015) - Anónimo

[3] Análisis Forense (2015) - UOC

[4] https://www.certsi.es

[5] ISO AF 27037-2012 (ISOIEC 27037)

[6] INCIBE (instituto Nacional de Ciber Seguridad) https://www.incibe.es

[7] Computer Forensics - CHFI

[8] http://www.flu-project.com

[9] http://stackoverflow.com

[10] https://github.com/sleuthkit/autopsy

[11] Análisis Forense Digital en Entornos Windows 3ª Edición – Juan Garrido Caballero

[12] http://www.securitybydefault.com

[13] http://conexioninversa.blogspot.com.es

[14] http://www.elladodelmal.com

[15] Análisis Forense de Sistemas Informáticos y Respuesta

[16] http://neosysforensics.blogspot.com.es

[17] Seguridad en Equipos Informáticos – A. Gómez Vieites

[18] Comunidad DragonJar (2008) http://www.dragonjar.org

[19] AENOR

[20] IETF

[21] ISO/IEC. (2012). ISO/IEC 27037

[22] Advanced Analysis Techniques for Windows 7 – Harlan Carvey

[23] Boletín Oficial del Estado. Constitución Española, Ley de Enjuiciamiento Civil, Ley de Protección de Datos de Carácter Personal, Código Penal, Directiva 2006/24/CE y Directiva 2013/40/UE. https://www.boe.es/

[24] Microsoft. Windows registry information for advanced users https://support.microsoft.com/