METODOLOGÍA PARA UN ANÁLISIS FORENSE

Trabajo de Final de Máster

Nombre Estudiante: Carles Gervilla Rivas

Programa: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Nombre Consultor: Marco Antonio Lozano Merino

Centro: Universitat Oberta de Catalunya

INCIBE (Instituto Nacional de Ciberseguridad) (INTECO)

Fecha de entrega: Diciembre 2014

Diciembre 2014

FICHA DEL TRABAJO FINAL

Título del trabajo:	Metodología para un Análisis Forense
Nombre del autor:	Carles Gervilla Rivas
Nombre del consultor:	Marco Antonio Lozano Merino
Fecha de entrega:	Diciembre 2014
Área del Trabajo Final:	Análisis Forense
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Resumen del Trabajo

El objetivo del presente Trabajo de Final de Máster es dar una metodología de análisis forense que sea válido en el mayor espectro posible de situaciones que se pueden dar en este campo.

Para ello se basa en guías y estándares que existen en la actualidad, como por ejemplo la ISO 27037, la RFC 3227 o las UNE 71505 y UNE 71506. También hace un repaso a la normativa legal vigente tanto a nivel español como internacional. A la vista de los estándares y guías existentes se hace patente la necesidad de una uniformidad en los procedimientos de análisis.

La metodología presentada se basa en un proceso de cinco fases. La primera fase resume cómo asegurar la escena donde se ha producido el ataque. La segunda fase explica cómo identificar y recolectar las evidencias que se hallen. En la tercera fase se explica cómo preservar dichas evidencias asegurando la cadena de custodia. En la cuarta fase se dan consejos sobre el análisis de las evidencias. Finalmente la quinta y última fase se basa en los informes que se deben presentar y la diferencias entre los dos tipos, el técnico y el ejecutivo.

En base al estudio realizado queda patente que es muy difícil dar una metodología única y que resultaría útil diversificar la metodología en varías guías en un trabajo futuro.

Abstract

The goal of this Final Master's Project is obtain a methodology for a forensics analysis. This methodology should be valid in most of the situations in which an investigator can be involved.

To do this, it is based on present guidelines and standards like ISO 27037, RFC 3227 or UNE 71505 and UNE 71506. This work also gives an overview to national and international laws related to this field. Reviewing these guidelines and standards is evident the need for uniformity the existing methods.

The methodology presented in this paper is based on five stages. The first one for assure the attack's scene. The second stage gives details about how to identify and collect evidences found at the scene. The third stage is about the custody chain and how to assure it. The fourth stage explain some tips and procedures to analyse evidences found at the scene. The last stage, the fifth, explains how to write the main reports and its differences. In one hand the executive report and in the other hand the technical one.

Due to the work and the analyses done it is easy to see the difficulty of give just one methodology for all scenarios. It will be very interesting write as methodologies as main possible situations can be found.

Palabras clave

Análisis forense

Informática forense

Cadena de custodia

Evidencias digitales

Metodología de análisis

Informe ejecutivo

Informe técnico

ÍNDICE

ÍNDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

1.1. CONTEXTO Y JUSTIFICACIÓN

Este Trabajo de Final de Máster correspondiente al Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de la Comunicaciones se centra en el ámbito del análisis forense de evidencias digitales.

Actualmente los procesos de análisis de este tipo no están estandarizados ni siguen una pauta o pasos descritos en ningún documento, ni de ámbito nacional ni internacional. Aun así, distintas organizaciones como la *Internet Engineering Task Force (IETF)* (1), la Asociación Española de Normalización y Certificación (AENOR) (2) o la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) (3), así como Policías (4) y Departamentos de Justicia (5) de varios países proponen varios documentos (6), (7), (8), en los que recogen alguna pautas y consejos para llevar a cabo este tipo de investigaciones sin que ello suponga una obligación en los procedimientos ni una garantía delante de ningún tribunal de que habiendo seguido esos pasos se certifique al 100% la tarea.

Ilustración 1: Logotipos ISO y AENOR

Por todo esto la única opción que le queda al investigador es seguir las mejores prácticas de todos estos documentos y aunar sus esfuerzos para no cometer errores que puedan ser aprovechados por otros para destruir todo el trabajo realizado.

La justificación de este trabajo pues, se basa en intentar determinar una metodología para este tipo de investigaciones reuniendo en una sola guía todos los consejos y mejores prácticas que ya se encuentran repartidos en otros documentos. Sería muy interesante que la guía fuera adoptada con el tiempo como un estándar y permitiera tener un marco común para todos.

1.2. OBJETIVOS DEL TRABAJO

Si bien la investigación forense puede variar mucho de una situación a otra, por ejemplo, en función del tipo de investigación que se requiera, sea con fines judiciales o meramente auditores, o bien en el plano técnico, no es lo mismo analizar un equipo con sistema operativo Windows que uno con Linux, en este trabajo se pretende orientar al investigador con unas pautas generalizadas que intenten abarcar la mayoría de los caminos posibles que puede tomar una investigación.

Así, el objetivo de este Trabajo de Final de Máster es dar una metodología para el análisis forense de evidencias digitales que pueda ser útil en la mayoría de casos, salvando las particularidades de cada caso y de cada investigación.

1.3. ENFOQUE Y METODOLOGÍA SEGUIDA

Para la realización de este trabajo nos basaremos en dos aspectos.

Por un lado, las prácticas de análisis forense en entornos Windows que, como asignatura del Máster, nos ayudarán a ver qué pasos son los más habituales en este tipo de situaciones. También nos ayudará a recabar cierta información, como herramientas útiles del sector, metodologías básicas y principios a respetar.

Por otro lado, a caballo de lo anterior, nos basaremos en las metodologías, guías, estándares y otras normas y recomendaciones que ya existen en este momento.

Con toda esta información trataremos de realizar un compendio de pasos y mejores prácticas para resolver la mayoría de casos en los que se pueda encontrar un investigador forense.

1.4. PRODUCTO OBTENIDO

En este Trabajo de Final de Máster el producto que se va a obtener será, como ya se ha ido explicando en los apartados anteriores, una metodología de análisis forense para investigadores de este ramo. Así pues, se dará una guía y unos consejos intentado abarcar el máximo posible de situaciones.

1.5. DESCRIPCIÓN DE LA ESTRUCTURA DEL TRABAJO

El presente Trabajo de Final de Máster contiene tres capítulos más aparte del de introducción.

En el segundo capítulo se dará un repaso a la situación actual de la informática forense, para ello se dará una definición sobre esta ciencia definiendo sus finalidades y sus principios básicos.

A continuación se detallará el estado actual en cuanto a regulación estatal e internacional. En el ámbito nacional aparecen la Constitución, la Ley de Enjuiciamiento Civil, la Ley de Protección de Datos de Carácter Personal, la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico, la Ley de Conservación de Datos Relativos a las Comunicaciones y las Redes Públicas y finalmente el Código Penal. En cuanto a la regulación internacional cabe destacar la Directiva 2006/24/CE de conservación de datos relativos a comunicaciones y la directiva 2013/40/UE que define sanciones para los ataques sufridos contra sistemas de información.

Se dará un repaso a las herramientas más utilizadas para realizar un análisis forense. Para ello se dividirán las herramientas en función del ámbito de aplicación, por ejemplo, para el análisis de las redes de comunicaciones, el análisis de los discos de los equipos

intervenidos, el análisis de los dispositivos de memoria, análisis de aplicaciones y finalmente las suites de herramientas que contienen paquetes con herramientas para varias finalidades.

En el segundo capítulo también se repasará la literatura relativa a normativas y estándares del sector. En este caso se verá la RFC 3227 que recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo. También se expondrá la ISO 27037, dentro de la familia 27000, que recoge las 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). Finalmente, dentro de los estándares nacionales, se repasan las normas UNE 71505 y la UNE 71506 que tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Finalmente se darán unas consideraciones sobre la necesidad de una metodología común para el análisis forense.

En el tercer capítulo se entrará de lleno en la metodología para el análisis forense. Para ello se divide en cinco fases.

En la primera fase se explicará cómo se debe asegurar la escena para evitar que se altere la misma con el acceso del personal.

En la segunda se darán directrices para identificar las pruebas que se localizan en la escena y posteriormente como recolectarlas con garantías.

En la tercera fase se explicará cómo preservar las pruebas recolectadas para evitar contaminaciones, tener una trazabilidad de estas y mantener la cadena de custodia.

En la cuarta fase se entrará de lleno en el análisis de las pruebas. Para ello se propondrán consejos y directrices en cuanto a la preparación del entorno de trabajo en el laboratorio, cómo crear una línea temporal dónde ubicar los hechos, determinar cómo se actuó, identificar al autores o autores de los hechos y finalmente valorar el impacto causado.

La quinta fase, se centrará en redactar los informes con todo el trabajo realizado. Para ello se diferenciará entre el informe técnico y el ejecutivo.

El cuarto y último capítulo se centrará básicamente en las conclusiones después del trabajo realizado. Se expondrá lo que se haya obtenido y se dará alguna referencia de trabajo futuro a partir de este mismo.

2. SITUACIÓN ACTUAL DE LA INFORMÁTICA FORENSE

2.1. INTRODUCCIÓN

En este capítulo se analizará la situación actual de la informática forense para situarnos en el contexto que nos ocupa y poder establecer unas bases para la creación de una metodología para el análisis forense.

De entrada se analizará qué es la informática forense pasando por su importancia hoy en día donde los equipos de información se hayan en cualquier punto. Se revisarán los fines de la informática forense, por ejemplo, fines preventivos, fines correctivos, fines probatorios y fines auditores. Finalmente, en este apartado se hará un resumen de los principios mínimos de calidad que debe cumplir la informática forense.

A continuación se hará un repaso a la regulación estatal en cuanto al marco jurídico, pasando por la Constitución, el Código Penal, o el conjunto de Leyes que todo profesional del sector debe conocer cuando se enfrenta a un análisis forense.

También se revisará la normativa internacional relacionada, concretamente dos directivas del Parlamento Europeo y del Consejo.

Se hará una revisión a las herramientas más utilizadas para estos fines con una breve descripción para comprender mejor su utilización. Las herramientas se han clasificado en función de su finalidad, a saber, análisis de red, de discos, de memoria, de aplicaciones y conjuntos o *suites* de aplicaciones con distintas finalidades.

Finalmente se hará un repaso al estándar ISO 27037, única norma ISO relacionada con el análisis forense pero que tampoco aporta lo que buscamos en este trabajo. Además también se repasará la RFC3227 y las UNE 71505 y UNE 71506, tal vez más cercanas a nuestro propósito.

Así, el capítulo concluye con unas breves consideraciones acerca de porqué es importante la creación de una metodología para el análisis informático y que aportaría esta metodología al sector.

2.2. QUÉ ES LA INFORMÁTICA FORENSE

La informática forense es una ciencia, de reciente aparición, que se encarga de asegurar, identificar, preservar, analizar y presentar un conjunto de datos, también llamados, prueba digital, de tal modo que ésta pueda llegar a ser aceptada en un proceso legal y/o judicial.

Más concretamente, esta ciencia y su conjunto de herramientas y técnicas permiten o facilitan, en la medida de lo posible, una reconstrucción del equipo informático afectado, el examen de los datos que se han podido recabar, la autenticación de los mismos, entre muchos otros menesteres.

El sujeto pasivo analizado no se resume tan sólo a un equipo informático entendiendo como tal un ordenador por ejemplo, si no que es mucho más amplio. Se puede tratar de redes completas de equipos, ya sean cableados o inalámbricas. También podemos hablar de

sistemas embebidos en otros más grandes, como por ejemplo pequeños equipos de control en sistemas de seguridad, equipos industriales, automóviles o incluso electrodomésticos.

Más actualmente, debido al auge de los sistemas de información que se pueden encontrar en cualquier sitio y su interés estratégico, la informática forense se puede aplicar al instante anterior al del fin criminal. Se puede utilizar la informática forense con finalidades de prevención, es decir, analizar un conjunto de equipos para analizar a qué riesgos potenciales están expuestos y mitigar así un posible ataque o incidente informático.

Así podemos encontrar que la informática forense es de aplicación en distintos objetivos, a saber, preventivos, correctivos, probatorios y auditores.

A continuación vamos a repasar brevemente de qué se trata cada uno de ellos.

Fines preventivos: Como ya se apuntaba anteriormente, la informática forense puede ayudar a prevenir posibles incidentes informáticos, formando parte del sistema de seguridad. En este caso, los responsables de seguridad de la empresa u organización pertinente, utilizarán las herramientas de la informática forense para verificar y auditar que los sistemas cumplen con los objetivos descritos en sus estándares de seguridad. Los resultados de estos estudios aportarán información valiosa de cara a mejorar los sistemas de seguridad, implementar nuevas metodologías en la organización o mantener los existentes.

Fines correctivos: En relación con el caso anterior, una organización puede detectar posibles fallos de seguridad informática, antes de cualquier incidente. Esta detección debe iniciar automáticamente una comisión que se encargue de corregir los fallos detectados e implemente las soluciones de seguridad que sean más convenientes para evitar que un usuario malintencionado pueda poner en riesgo la organización.

Fines probatorios: Esta es la finalidad de la informática forense que más nos interesa a tenor del tema que se trata en este trabajo. La informática forense con fines probatorios permite, que tras el registro de un incidente informático, se pueda recabar información sobre la intrusión en el sistema, descubrir qué daños se han producido, si ha habido robo de información o destrucción de la misma, etc. Entre otros, se puede llegar a descubrir el o los causantes del incidente, su origen, si se han comprometido más equipos o sólo el que se analiza. Finalmente, con todos los datos recabados, organizados y bien preservados de posibles manipulaciones ulteriores, se pueden presentar los datos ante un juzgado aportando una prueba con validez legal que permita la persecución y pena del hecho delictivo.

Fines auditores: Otro campo de interés de la informática forense es la auditoría de sistemas informáticos. Relacionado con los fines correctivos, se pueden programar auditorias de seguridad, que llevan a cabo empresas especializadas, o incluso un equipo dentro de la propia organización interesada, que verifiquen periódicamente que los sistemas de información cumplen todos los requisitos de seguridad y que los usuarios mantienen unos mínimos de cuidados y prácticas de seguridad entorno a esos equipos.

Como en cualquier otra ciencia, la informática forense debe asegurar unos principios mínimos de calidad para asegurar que todos los resultados que obtiene son de calidad y no han sido manipulados en ningún momento, por ello debe asegurar que:

- Se evita la contaminación de las pruebas recogidas en el escenario. Hay que verificar que el equipo que se va a analizar no se modifica de ninguna manera ni se manipula, de igual forma con las copias de datos que se realicen. Para ello existen técnicas que prueban que una copia realizada es fiel a su original y contiene exactamente la misma información sin que haya variado ni tan siquiera un bit.
- Se debe actuar metódicamente. Hay que seguir unos pasos y seguirlos de manera correcta, se debe estar muy atento en todo momento a los detalles y no permitir que cualquier error o negligencia den al traste con todo el trabajo.
- Se debe controlar la prueba obtenida y evitar manipulaciones. Hay que realizar un registro de quién o quiénes han tenido en cada momento las pruebas y qué se ha hecho con ellas. De este modo nunca se podrá decir que las pruebas han sido manipuladas haciendo que pierdan su finalidad probativa en un proceso judicial.

2.3. REGULACIÓN ESTATAL

Cualquier persona que se dedique profesionalmente a la informática forense debe conocer la legislación vigente a la que se someten sus actos como profesional. De este modo entenderá hasta donde pueden llegar sus investigaciones, qué repercusiones legales pueden tener unas actuaciones u otras y actuar consecuentemente para no acabar siendo acusado durante la investigación de cualquier hecho delictivo. Además podrá conocer si los actos que descubre por razón de su investigación constituyen o no faltas administrativas o delitos penales.

A continuación se repasaran las leyes más importantes en el ámbito que nos ocupa dentro de la jurisdicción española.

Ilustración 2: Esquema de normativa legal vigente en España

Constitución Española (9)

En este caso nos centraremos sobre todo en los derechos relativos a la dignidad de la persona humana y concretamente en los siguientes:

- 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. Asimismo se incluye la limitación del uso de la informática para proteger la intimidad.
- Derecho fundamental a la protección de datos. El Tribunal Constitucional crea el derecho fundamental a la protección de datos como un derecho diferente al de la intimidad.

Ley de Enjuiciamiento Civil (10)

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

Ley de Protección de Datos de Carácter Personal (11)

Esta Ley fue redactada en 1999 con el propósito de regular los datos de carácter personal que manejan, sobre personas físicas, empresas y organismos sean públicos o privados.

Para ello se 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. Además de asegurar su origen y verificar que tiene permiso para almacenar los datos deberá registrar unas mínimas garantías de seguridad para que los datos contenidos en el fichero no sean públicos. Además deberá garantizar que se eliminan los datos cuando el titular así lo requiera y siempre que la Ley permita dicha eliminación.

El perito que esté analizando un equipo deberá tener mucho cuidado con no publicar datos de carácter personal que pudiesen estar contenidos en los equipos analizados, ya sea por error u omisión y mantener el secreto profesional en todo caso.

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

- **Básico:** Todos los sistemas con datos personales.
- **Medio:** Todos los datos del nivel básico, además de los datos sobre comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, solvencia patrimonial y crédito y conjuntos de datos suficientes que permitan obtener una evaluación de la personalidad del individuo.
- **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.

Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (12)

Redactada y aprobada un par de años después, 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.

Ley de Conservación de Datos Relativos a las Comunicaciones y las Redes Públicas (13)

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. Aunque en casos concretos este periodo temporal oscila entre los 6 meses y 2 años.

Código Penal (14)

El Código Penal concentra aquellas actitudes que se consideran delito en España. A continuación se relacionan las acciones consideradas como delitos:

- Corrupción de menores:
    - Exhibicionismo y provocación sexual (art. 186)
    - Prostitución (art. 187 y 189.1)

- Apología del delito:
    - Concepto (art. 18.1, párrafo 2º)
    - Apología del genocidio (art. 608.2)

- Delitos contra el honor (art. 211):
    - Calumnias (art. 205)
    - Injurias (art. 208)

- Delitos contra la intimidad (art. 197):

- Defraudación electrónica:
    - Estafa (art. 248.2)

- Apropiación indebida (art. 252)

- Uso ilegal de terminales (art. 256)
- Daños a ficheros informáticos (art. 264.2)
- Piratería informática (art. 270)
- Delitos documentales:
    - Falsedad documental (arts. del 390 al 400)
    - Infidelidad en la custodia (arts. del 413 al 416)
- Protección de la contraseña (art. 414.2)

2.4. REGULACIÓN INTERNACIONAL

Además de la regulación 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 (15)

Esta directiva del Parlamento Europeo y del Consejo 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.

Así la directiva se 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 contenido de las comunicaciones electrónicas.

Directiva 2013/40/UE (16)

En este caso la directiva 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.

También tiene por objeto 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 (17), Europol (18) y su Centro Europeo contra la Ciberdelincuencia (19) y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) (20).

2.5. HERRAMIENTAS MÁS HABITUALES

Actualmente existen multitud de aplicaciones destinadas al análisis forense que trabajan sobre distintos aspectos de la máquina a analizar, por ejemplo, sobre las memorias, los discos de almacenamiento, los protocolos de red, las aplicaciones, etc.

También existen *suites* que ofrecen el análisis sobre varios de estos puntos ofreciendo herramientas verdaderamente potentes y útiles. No obstante, no existe ni la herramienta definitiva ni aquella aprobada y validada por ningún estándar. A continuación se hará un repaso de las herramientas más populares con una breve descripción y su ámbito de trabajo.

2.5.1. Herramientas de análisis de red

Snort (21)**:** Es un sistema de detección de intrusiones basado en red aunque también se utiliza como analizador. Permite generar un registro de todos los sucesos que afecten al sistema que se está analizando. Funciona mediante filtros que se deben configurar de una manera u otra en función de nuestro objetivo.

Ilustración 3: Logo Snort

Nmap (22)**:** Este *software* es un potente analizador de puertos muy utilizado tanto a nivel de auditorías de seguridad como para extraer evidencias en una investigación forense.

Wireshark (23)**:** Utilidad muy extendida que permite analizar protocolos de red y analizar el tráfico que se captura en una red. Genera reportes que son exportados a archivos de texto para un posterior análisis forense.

Ilustración 4: Logo Wireshark

Xplico (24)**:** Es un *framework* forense para realizar tareas de análisis de datos recopilados en capturas de red, soporta múltiples protocolos. Según cuenta en su página web, permite analizar archivos de captura de datos, en formato PCAP, y los separa en función de los distintos protocolos. Este método ayuda a una mejor comprensión de los datos capturados. Además es posible analizar archivos de gran tamaño. Destaca la funcionalidad de previsualizar las imágenes que hayan sido accedidas durante el periodo de captura. También es de destacar el análisis de peticiones DNS que permiten analizar a qué sitios web se accedieron.

2.5.2. Herramientas para tratamiento de discos

Dcdd3 (25)**:** Utilidad que permite trabajar sobre el disco del equipo que se quiere analizar. Permite realizar copias a bajo nivel para proteger el original. Entre sus características permite copiar grandes imágenes de discos en partes más pequeñas para un traslado y posterior análisis más cómodo.

Mount Manager (26)**:** Es otra herramienta para trabajar con discos. En este caso permite detectar, montar y desmontar, examinar y administrar unidades de almacenamiento conectadas a disco duro.

Guymager (27)**:** Permite la copia bit a bit o réplicas de imagen de disco.

2.5.3. Herramientas para tratamiento de memoria

Volatility (28)**:** Es un conjunto de herramientas desarrolladas en Python. Permite hacer volcados de memoria de máquinas con sistemas operativos Windows, Linux, Mac OSX e incluso Android. Trabaja con versiones tanto de 32 como de 64 bits. Es capaz de analizar volcados con datos en *raw*, *crash dumps* de sistemas Microsoft Windows, etc. A partir de los datos se pueden extraer, por ejemplo, tipo de sistema, fecha y hora, puertos abiertos, ficheros cargados por procesos, así como DLL, módulos del *kernel*, direccionamiento de memoria por procesos, claves de registro utilizadas en los procesos, etc.

Ilustración 5: Logo Volatility

Memoryze (29): Permite la captura de memoria RAM en equipos con sistemas operativos Windows y OSX.

RedLine (30)**:** Como la aplicación anterior, también permite la captura de memoria y su posterior análisis. Además dispone de entorno gráfico.

2.5.4. Herramientas para el análisis de aplicaciones

OllyDbg (31)**:** Esta aplicación permite desensamblar y depurar aplicaciones o procesos para Windows. Carga y permite debugar DLLs 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.

OfficeMalScanner (32)**:** Es una utilidad que permite escanear archivos de la *suite Office*, en busca de códigos maliciosos, por ejemplo, en macros, conectores OLE o ficheros encriptados.

Radare (33)**:** Aplicación multiplataforma, Linux, Android, OSX, Windows e incluso Solaris que permite aplicar ingeniería inversa para analizar código de una aplicación maliciosa que se ha ejecutado.

Process explorer (34)**:** Muestra información de los procesos que hay abiertos en un máquina. Es una herramienta útil para la localización de problemas de versión de DLL o pérdidas de identificadores. También ofrece detalles internos acerca del funcionamiento de Windows y aplicaciones.

PDFStreamDumper (35): Permite el análisis de código malicioso dentro de archivos de tipo PDF. Trabaja con código javascript ofuscado y *shellcodes.*

2.5.5. *Suites* de aplicaciones

DEFT (36)**:** Es una distribución Linux, basada en Ubuntu que permite al análisis forense de terminales móviles y dispositivos con Android o iOS. Contiene herramientas útiles para el análisis de ficheros de diferentes tipos, búsqueda de *rootkits*, virus, *malware*, etc. También permite la recuperación de ficheros del sistema, así como aplicaciones que facilitan la obtención de información asociada a usuarios y su actividad con el equipo. Posee herramientas para la recuperación de contraseñas del sistema mediante distintas técnicas. Finalmente comentar que tiene herramientas que facilitan las tareas de generación de informes y obtención de evidencias.

ForLEx (37)**:** Es otra distribución Linux orientada a aplicaciones de informática forense. Incluye FTK Imager que permite crear imágenes de los sistemas para su posterior análisis forense. Permite agregar más herramientas a las que ya presenta por defecto.

CAINE *(Computer Aided INvestigate Environment)* (38)**:** Otra herramienta basada en Ubuntu. Entre sus características destacan un entorno de trabajo orientado a completar las fases de un análisis forense, una interfaz gráfica bastante amigable y un proceso semiautomático para generar informes a partir de los resultados obtenidos.

Autopsy (39)**:** Es un conjunto de aplicaciones muy útiles para el análisis forense. Una de las herramientas más completas y más utilizadas. Permite un análisis de la línea de tiempo para ayudar a identificar la actividad. Permite búsquedas de palabras sobre todo el equipo. Analiza el registro del sistema operativo Windows. Extrae datos EXIF de las imágenes, permite visualizar miniaturas de las mismas así como clasificación de los archivos del sistema por tipo, entre muchas otras opciones y herramientas.

Ilustración 6: Logo Autopsy

2.6. 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 (40) y por otro lado la ISO 27037 (41) y las UNE 71505 (42) y UNE 71506 (43).

2.6.1. ISO 27037

Dentro de la seguridad informática cabe destacar una normativa ampliamente conocida, es la familia ISO 27000. Esta serie de normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Esta serie contiene diversas normas todas relacionadas con las 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).

Concretamente, existe una norma dedicada en exclusiva al análisis forense, se trata de la ISO 27037 Directrices para la identificación, recolección, adquisición y preservación de la prueba digital.

Esta norma ofrece orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de las pruebas digitales. Además define dos roles especialistas:

- **DEFR *(Digital Evidence First Responders)***: Expertos en primera intervención de evidencias electrónicas.
- **DES *(Digital Evidence Specialists):*** Experto en gestión de evidencias electrónicas.

ISO 27037 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, PDAs, 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.

Resumiendo, se puede destacar que esta norma ofrece orientación sobre el manejo de las pruebas digitales. Siguiendo las directrices de esta norma se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales para facilitar su aportación en juicios y procesos legales. Además cabe destacar que cubre una amplia gama de tipos de dispositivos y situaciones, por lo que la orientación dentro de la norma es ampliamente aplicable.

2.6.2. RFC 3227

Otra norma destacable para mencionar es la RFC 3227. Este documento publicado por la *Internet Engineering Task Force (IETF)* recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo.

En cuanto a los principios para la recolección de evidencias destacan básicamente tres, el orden de volatilidad de los datos, las acciones que deben evitarse y las consideraciones sobre la privacidad.

Relativo al procedimiento de recolección destaca que debe ser detallado, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones.

Sobre el procedimiento de almacenamiento tiene en cuenta la cadena de custodia de las pruebas recogidas anteriormente y dónde y cómo se deben almacenar estas para que estén a buen recaudo.

Para acabar detalla qué tipo de herramientas son las más útiles y qué características deben tener para evitar conflictos, haciendo hincapié en que las herramientas deben alterar lo menos posible el escenario. Según este documento el kit de análisis debe incluir las siguientes herramientas:

- Programas para listar y examinar procesos.
- Programas para examinar el estado del sistema.
- Programas para realizar copias bit a bit.

Todas estas recomendaciones tienen como epicentro el principio de intercambio de Locard, que señala que: “siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto”.

2.6.3. UNE 71505 y UNE 71506

Estas normas, publicadas por la Asociación Española de Normalización y Certificación tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Según la asociación esta norma debe dar respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades. Con la obtención de dichas pruebas digitales, que serán más robustas y fiables siguiendo la normativa, se podrá discernir si su causa tiene como origen un carácter intencional o negligente.

Estas normativas son de aplicación a cualquier organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito. Se dirige especialmente a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas.

2.7. NECESIDAD DE UNA METODOLOGÍA

A tenor de todo lo expuesto en este capítulo, marco legal en España y Unión Europea, herramientas más utilizadas en el sector y estándares nacionales e internacionales relativos al análisis forense, queda claro que no existe ninguna metodología para que los profesionales del sector pueden realizar sus tareas siguiendo un marco único. Aunque algunas de ellas dan buenas directrices e indicaciones que nos serán de mucha utilidad, es el caso de la RFC 3227 y las normas UNE 71505 y UNE 71506.

Por este motivo, es oportuno crear una metodología única y definitiva que pueda aportar al sector una guía práctica de los pasos a seguir para realizar un análisis forense con garantías de éxito. Teniendo en cuenta todas las premisas de seguridad, las recomendaciones y los estándares ya existentes.

Si dicha metodología se hace extensiva y de aplicación generalizada por todo el sector conllevará una mejora en la calidad del peritaje y del análisis forense, evitando así situaciones de riegos, errores en el manejo de los dispositivos y de las pruebas y en general procedimientos que pongan en riesgo toda una investigación.

Desde el punto de vista jurídico, el hecho que una investigación haya seguido unas pautas aceptadas y aprobadas por un ente superior, facilitarían la tarea de jueces y magistrados, que no tendrían que entrar en detalles de si los procesos se han llevado a cabo de manera correcta.

Así pues, resumiendo, se puede decir que la creación, uso y aprobación de una metodología de análisis forense aportaría el más alto grado de seguridad y garantías en todo el proceso que nos ocupa, no dando lugar a interpretaciones laxas, errores u omisiones graves.

3. DESARROLLO DE UNA METODOLOGÍA PARA EL ANÁLISIS FORENSE

3.1. ESTUDIO DE LAS FASES DE UN ANÁLISIS FORENSE

Con el análisis realizado sobre las normas y estándares que existen tanto a nivel nacional como internacional se ha podido ver que hay un conjunto de puntos importantes a tener en cuenta para realizar un análisis forense exitosamente. Por ejemplo, la mayoría recalcan la importancia de preservar el entorno de pruebas, no modificando el escenario encontrado. También aluden a la importancia de cómo se guardan las pruebas, su transporte, conservación, etcétera. Posteriormente se centran en cómo analizar las pruebas para obtener el máximo rendimiento de las mismas y poder esclarecer al máximo los hechos ocurridos. Finalmente, la importancia de unos buenos informes que sean claros, concisos y que sirvan, por ejemplo en caso de juicio, para que una persona no entendida en el tema sea capaz de comprender lo ocurrido y lo que le queremos transmitir sin influir en una posterior decisión.

Así pues, atendiendo a estas recomendaciones y consejos, más o menos extendidos en toda la literatura sobre este asunto, parece oportuno dividir en distintas fases la metodología para un análisis forense exitoso. Esta será la estructura del presente capítulo. Se analizarán las siguientes fases:

1. Asegurar la escena
2. Identificar y recolectar las evidencias
3. Preservar las evidencias
4. Analizar las evidencias obtenidas
5. Redactar informes sobre los resultados

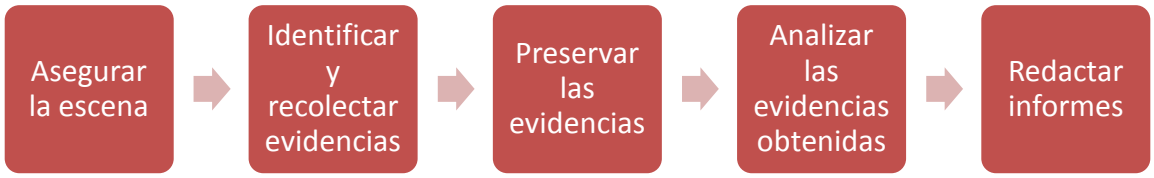


Ilustración 7: Fases de un análisis forense

En cada una de las fases se darán las mejores recomendaciones y los pasos más habituales para no cometer ningún error. Obviamente no todos los análisis forenses se producen ante hechos criminales, y por lo tanto no todos van a acabar en manos de jueces y abogados. Como ya se ha ido indicando el análisis forense tiene muchas más finalidades, puede ser simplemente una auditoría, reconstruir un sistema dañado, un proceso de aprendizaje o la toma de medidas para que no se reproduzca un determinado problema.

En todo caso, la finalidad judicial parece ser la más restrictiva y con la que más problemas nos podemos encontrar, así pues, será esta la que presente más dificultades y con la que se tenga que tener más prudencia.

3.2. 1ª FASE: ASEGURAR LA ESCENA

Tal vez esta fase tenga su máxima expresión en casos criminales. No obstante, quizás con menor rigor, es importante en cualquier análisis forense. Es importante recalcar que el investigador no sólo se tiene que centrar en un análisis técnico del equipo o equipos implicados en el incidente, también debe asegurarse que la escena donde se ha producido el incidente no haya sido alterada, desde el descubrimiento del mismo hasta el inicio de su análisis. Todos los implicados en la investigación deben ser conscientes que cualquier acto que lleven a cabo puede comportar unas consecuencias posteriores, así no deben hacer nada que no tengan claro y que pueda alterar los resultados. Lo mejor es trabajar consensuando la actuación y anotando todo lo realizado en la escena.

Es recomendable realizar fotografías del entorno del equipo para evidenciar el estado original de la escena, identificando así el perímetro de la escena a analizar y protegiéndolo de accesos de personal no autorizado.

Una vez dentro del perímetro de seguridad cabe destacar que hay que proteger las huellas dactilares que pueda haber en los equipos para que los demás cuerpos y unidades de policía e investigadores puedan realizar su tarea. Es por lo tanto recomendable el uso de guantes de látex o similar para esta finalidad.

Hay que anotar la hora y fecha de los equipos implicados que no tiene por qué coincidir con la real, esto es importante para la investigación posterior y para la realización de una línea temporal con todos los sucesos que han ocurrido. En caso de haber desfase entre la hora del equipo y la real, este desfase se tiene que documentar para tenerlo en cuenta posteriormente. La captura de la hora y fecha se puede realizar fotografiando la pantalla o grabando un vídeo de la misma, siempre y cuando no haya que manipular el equipo para ello.

Debemos ver si en pantalla hay algún proceso que nos aporte información útil sobre lo que esté pasando en directo, en ese caso, grabar todo lo que ocurre. Es importante valorar las entradas y salidas de los equipos, pues nos pueden aportar pistas importantes. De igual modo con otros periféricos de entrada/salida, tales como impresoras, teléfonos IP, escáneres, etcétera.

Llegados a este punto hay que centrarse sobre la desconexión de los equipos tanto de la red como de la alimentación eléctrica. Estas desconexiones pueden alterar la investigación y por lo tanto debe documentarse exactamente lo que se ha realizado y lo que lo ha motivado. En cuanto a la desconexión de red, si se realiza, podemos lograr que un determinado hecho siga realizándose, por ejemplo una descarga de datos no autorizada o el borrado remoto de datos que podrían dificultar el análisis. En cambio, perderemos información sobre posibles conexiones que nos den el origen del incidente o valiosos indicios.

De igual forma, habrá que valorar qué repercusiones tendrá la desconexión del fluido eléctrico. Una desconexión evitará que algún proceso siga escribiendo en disco o incluso eliminando datos, aunque también podría provocar alguna escritura de datos en disco si el equipo tiene alguna configuración programada para fallos eléctricos. También se podría haber planificado un borrado de datos en caso de desconexión del equipo y entonces se perdería parte o toda la información del equipo dando al traste con la investigación. Así,

habrá que ser muy cuidadoso con este punto y valorar qué opción nos es más útil en cada caso, no todas las investigaciones que se hagan se resolverán del mismo modo.

Una vez finalizada la primera fase, y con la escena bien asegurada teniendo en cuenta todos los puntos expuestos anteriormente, se podrá pasar a la segunda fase de la metodología. A continuación nos enfrontaremos a la identificación y recolección de pruebas.

3.3. 2ª FASE: IDENTIFICACIÓN Y RECOLECCIÓN DE EVIDENCIAS

Para un mayor detalle la segunda fase se subdividirá en dos apartados, por un lado la parte relativa a la identificación de las evidencias y por otro lado la parte relativa a la recolección de las mismas.

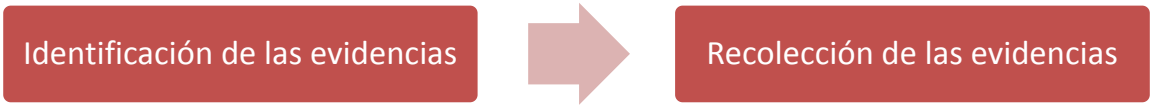


Ilustración 8: Fases de identificación y recolección

3.3.1. Identificación de las evidencias

Llegados a este punto hay que tener en cuenta una serie de principios acerca de la identificación de las evidencias y más específicamente sobre la volatilidad de las mismas. Es vital conocer qué datos son más o menos volátiles, identificarlos correctamente y posteriormente proceder a su recolección.

Entendemos por volatilidad de los datos el período de tiempo en el que estarán accesibles en el equipo. Por lo tanto, se deberán recolectar previamente aquellas pruebas más volátiles. Según la RFC 3227, el que se presenta a continuación, es un posible orden de volatilidad de mayor a menor:

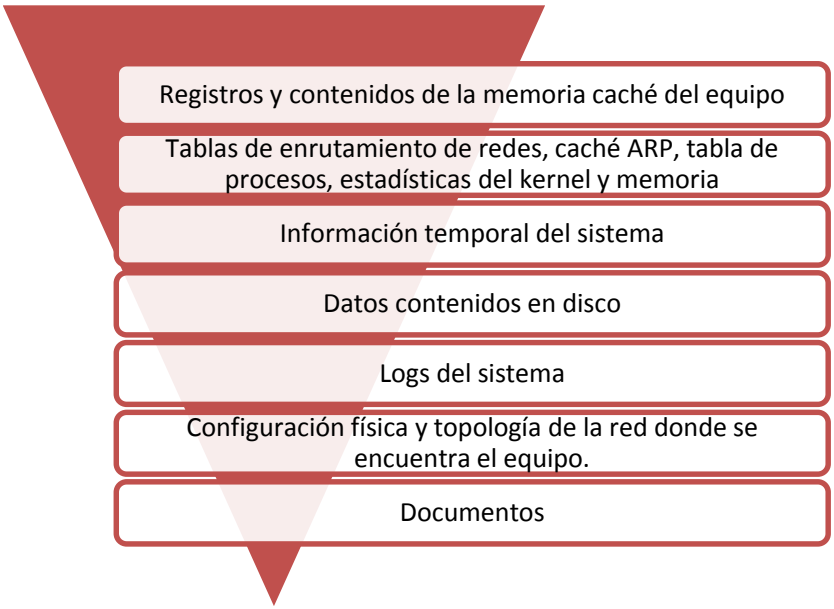


Ilustración 9: Orden de volatilidad

Conocidas las ubicaciones del sistema con mayor y menor volatilidad e identificadas las evidencias que pueda contener habrá que valorar hasta qué punto cuáles son útiles y necesarias y se deberán recolectar.

En esta fase es muy útil documentar ciertos aspectos del sistema y de los dispositivos que se observan en la escena así como aquellos que no se llevarán al laboratorio de análisis.

Se deberán listar los equipos y sus características que estén implicados en los hechos. Así mismo también se deberá hacer un listado con las personas implicadas en los equipos. Será útil recoger su nombre, identificación, contraseñas de los sistemas y acciones que hayan realizado desde el conocimiento del incidente, entre otras.

Será útil, en caso de varios equipos conectados en red, dibujar la estructura de la misma, es decir, su topología, con la identificación de cada equipo en ella. Además también es importante identificar todos los cables y los puertos donde están conectados los distintos periféricos del equipo para poder realizar una posterior conexión en laboratorio en caso de ser necesario.

Los discos duros también deben ser identificados correctamente, pues conforman el núcleo duro, en la mayoría de los casos, de nuestra investigación. Esto incluye anotar marca y modelo, número de serie, capacidad, posición de los *jumpers* y documento gráfico que lo pruebe. Lo mismo ocurre con los discos ópticos y sus unidades lectoras, como DVD, CD, etcétera.

Ilustración 10: Detalle etiqueta disco duro

Finalmente, y no menos importante, hay que recalcar unas indicaciones, a caballo entre la identificación y la recolección de las pruebas relacionadas con la privacidad. Hemos repasado en un capítulo especial la legislación legal vigente sobre este aspecto.

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 que la disponibilidad de los servicios quede afectada. Además, a menos que haya indicios suficientes y fundamentados no se deben recopilar datos de lugares a los que no se accede normalmente, como por ejemplo ficheros con datos personales.

3.3.2. Recolección de evidencias

Tras la correcta identificación de las evidencias se puede proceder a su recolección, para ello se pueden seguir los siguientes pasos:

Copia *bit* a *bit* de los discos que se quieran analizar, es decir, se requiere una copia exacta del contenido de los discos incautados. Esto incluye todos los archivos del disco, por ejemplo los temporales, los ocultos, los de configuración, los eliminados y no sobrescritos y la información relativa a la parte del disco no asignada, es lo que se conoce como copia a bajo nivel.

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.

Una vez realizada la copia se debe verificar la integridad de la misma. Para ello se calcula el *hash* o CRC de la copia, normalmente los equipos destinados al clonado de discos ya incorporan esa característica. Así con el *hash* del disco original y el de la copia se puede certificar que ambos son idénticos a todos los niveles y ante un juez, por ejemplo, quedará probado que no se ha manipulado de ningún modo. Con este procedimiento también nos aseguraremos que no se han producido errores en la copia.

Con la primera copia realizada y comprobada procedemos a realizar una segunda copia sobre la primera. En este caso también se comprobará que el contenido es idéntico mediante el mismo proceso descrito anteriormente. 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. Para realizar el análisis se deberá realizar una tercera copia, comprobar su integridad y trabajar sobre ella, de tal modo que en caso de cualquier desastre o alteración de los datos siempre tengamos la segunda copia exacta al original de donde poder volver a realizar otra copia para analizar.

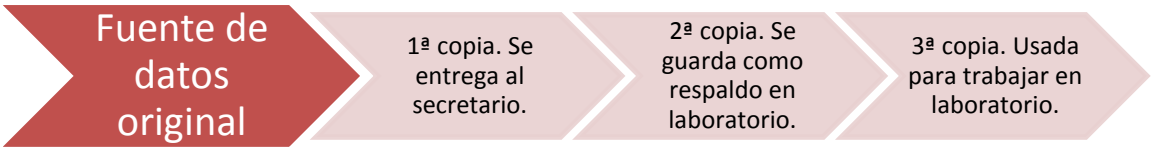


Ilustración 11: Orden de copias para pruebas recolectadas

Se podría considerar que hasta aquí llega la tarea de campo. La siguiente fase tendrá lugar a caballo entre la escena y el laboratorio, es la fase de preservación de las evidencias. Las siguientes tendrán lugar en el laboratorio de análisis forense, serán las de análisis y redacción de informes.

3.4. 3ª FASE: PRESERVACIÓN DE LAS EVIDENCIAS

Una mala preservación de las evidencias, un mal uso o una mala manipulación pueden invalidar toda la investigación que se lleva a cabo delante de un tribunal, este es un factor muy importante que se va repitiendo a lo largo de toda la metodología.

La cadena de custodia es el procedimiento controlado aplicable a las evidencias relacionadas con el suceso, desde el momento en que se encuentran en la escena hasta su análisis en el laboratorio. La finalidad de la cadena de custodia es evitar cualquier tipo de manipulación y tener un control absoluto sobre todos los elementos incautados, quién los ha

manipulado, cómo lo ha realizado, porqué los ha manipulado, para qué lo ha hecho y cuándo ha tenido lugar dicha manipulación.

Es importante realizar todas las anotaciones descritas en la fase de identificación de las evidencias para que esta fase sea aún más sólida. Con todos los elementos documentados será mucho más fácil tener un control de todas las evidencias que disponemos y poder realizar una traza de todas las pruebas adquiridas.

Mientras los dispositivos estén en el laboratorio y no se estén manipulando es importante tenerlos embalados con etiquetas informativas que contengan al menos datos como un identificador único para cada elemento, nombre del técnico responsable del material, la descripción del mismo. También es relevante el propietario del mismo y en qué lugar fue confiscado, así como fecha y hora del evento. Finalmente se podrán anotar otras observaciones que puedan resultar útiles para los investigadores y que aporten cualquier otro dato.

En función de la naturaleza de los equipos confiscados habrá que tomar una serie de cuidados adicionales. En caso de discos ópticos o magnéticos, por ejemplo discos duros, CD, cintas de copias de seguridad o similares, estos se deberán proteger contra electricidad estática y se guardarán en bolsas antiestáticas para evitar pérdida o daño en los datos contenidos. Se procederá de la misma forma con placas electrónicas que pudieren verse afectadas por descargas de electricidad estática o sean sensibles a la manipulación.

Además se tendrá en cuenta de proteger los bienes para el transporte desde el lugar de los hechos hasta el laboratorio con los medios necesarios para evitar golpes o proteger de caídas fortuitas.

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 y suciedad.

Para la gestión de datos en dispositivos de almacenamiento y su transporte se puede consultar y considerar alguna de las recomendaciones contenidas en la ISO 17799:2005 (44) en su apartado 10.7.

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.

3.5. 4ª FASE: ANÁLISIS DE LAS EVIDENCIAS

La fase de análisis no termina hasta que no se puede determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en el sistema, etc. Es decir, es el núcleo duro de la investigación y tiene que concluir con el máximo de información posible para poder proceder a elaborar unos informes con todo el suceso bien documentado.

Antes de empezar el análisis, es importante recordar unas premisas básicas que todo investigador debe tener presente en el momento de enfrontarse al incidente. Como ya se ha explicado nunca se debe trabajar con datos originales y se debe respetar cada una de las

leyes vigentes en la jurisdicción donde se lleve a cabo la investigación. Los resultados que se obtengan de todo el proceso han de ser verificables y reproducibles, así que en cualquier momento debemos poder montar un entorno donde reproducir la investigación y mostrarlo a quién lo requiera. Es importante también disponer de una documentación adicional con información de diversa índole, por ejemplo:

- Sistema operativo del sistema.
- Programas instalados en el equipo.
- Hardware, accesorios y periféricos que forman parte del sistema.
- Datos relativos a la conectividad del equipo:
    - Si dispone de *firewall*, ya sea físico o lógico.
    - Si el equipo se encuentra en zonas de red especiales, por ejemplo, *DMZ.*
    - Si tiene conexión a Internet o utiliza *proxies.*
- Datos generales de configuración que puedan ser de interés para el investigador para ayudar en la tarea.

Para ayudar al desarrollo de esta fase del análisis forense podemos centrarnos en varias subfases o puntos importantes que generalmente siempre deben realizarse. Cabe recordar que no existe ningún proceso estándar que ayude a la investigación y habrá que estudiar cada caso por separado teniendo en cuentas las diversas particularidades que nos podamos encontrar. No será lo mismo analizar un equipo con sistema operativo Windows o con Linux. Tampoco será lo mismo un caso de intrusión en el correo electrónico de alguien o un ataque de denegación de servicio a una institución. De igual forma no actuaremos con los mismos pasos en un caso de instalación de un *malware* que destruya información de una ubicación de disco o un *malware* que envíe todo lo que se teclea en un equipo.

En todo caso, se pueden destacar varios pasos, que habrá que adaptar en cada caso:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema.

3.5.1. Preparar un entorno de trabajo

Antes de empezar el análisis propiamente, se debe preparar un entorno para dicho análisis. Es el momento de decidir si se va a hacer un análisis en caliente o en frío.

En caso de un análisis en caliente se hará la investigación sobre los discos originales, lo que conlleva ciertos riesgos. Hay que tomar la precaución de poner el disco en modo sólo lectura, esta opción sólo está disponible en sistemas operativos Linux pero no en Windows. Si se opta por esta opción hay que operar con sumo cuidado pues cualquier error puede ser fatal y dar al traste con todo el proceso, invalidando las pruebas.

Si se opta por un análisis en frío, lo más sencillo es preparar una máquina virtual con el mismo sistema operativo del equipo afectado y montar una imagen del disco. Para ello,

previamente habremos creado la imagen a partir de las copias que se hicieron para el análisis. En este caso podremos trabajar con la imagen, ejecutar archivos y realizar otras tareas sin tanto cuidado, pues siempre cabe la opción de volver a montar la imagen desde cero en caso de problemas.

La opción del análisis en frío resulta muy atractiva pues en caso de *malwares* se podrán ejecutar sin miedo, reproducir lo que ocurre y desmontar la imagen sin que la copia original resulte afectada. De este modo tal vez se pueda ir un poco más allá en la investigación y ser un poco más agresivo.

Existen varios programas gratuitos para crear y gestionar máquinas virtuales, por ejemplo, Oracle VM VirtualBox (45), que ofrecen muy buenas prestaciones.

3.5.2. Creación de la línea temporal

Sea cual sea el tipo de análisis que se va a llevar a cabo, el primer paso suele ser crear una línea temporal dónde ubicar los acontecimientos que han tenido lugar en el equipo desde su primera instalación.

Para crear la línea temporal, lo más sencillo es referirnos a los tiempos MACD de los archivos, es decir, las fechas de modificación, acceso, cambio y borrado, en los casos que aplique. Es importante, como ya se ha indicado en alguna ocasión tener en cuenta los husos horarios y que la fecha y hora del sistema no tienen por qué coincidir con los reales. Este dato es muy importante para poder dar crédito a las pruebas y a la investigación en general.

Para empezar, lo mejor es determinar la fecha de instalación del sistema operativo, para ello se puede buscar en los datos de registro. Además la mayoría de ficheros del sistema compartirán esa fecha. A partir de aquí puede ser interesante ver qué usuarios se crearon al principio, para ver si hay discrepancias o usuarios fuera de lo común en últimos instantes del equipo. Para ver esta información también es útil acudir al registro del sistema operativo.

Teniendo ya los datos iniciales del sistema, ahora se puede proceder a buscar más información en los ficheros que se ven “a simple vista”. Lo importante es localizar que programas fueron los últimos en ser instalados y qué cambios repercutieron en el sistema. Lo más habitual es que estos programas no se instalen en los lugares habituales, sino que se localicen en rutas poco habituales, por ejemplo en archivos temporales o mezclados con los archivos y librerías del sistema operativo. Aquí se puede ir creando la línea temporal con esos datos.

Alternativamente es útil pensar que no todos los archivos están a la vista. Se puede encontrar información en archivos normales, pero también en temporales, ocultos, borrados o usando técnicas como la esteganografía, no se puede obviar ninguna posibilidad.

Habitualmente los sistemas operativos ofrecen la opción de visualizar los archivos ocultos y también las extensiones. Es útil activar estas opciones para detectar posibles elementos ocultos y extensiones poco habituales que nos resulten extrañas.

Para los archivos borrados se utilizaran programas especiales capaces de recuperar aquellos datos que se hayan eliminado del disco pero sobre los cuales aún no se haya sobrescrito nada. Es posible que el atacante elimine archivos o registros varios en afán de esconder lo que ha ocurrido, si estos no han sido sobrescritos se podrán recuperar y se

podrán situar en la línea temporal relacionándolos con el conjunto de sucesos. Para recuperar información oculta mediante esteganografía también se deberán usar programas concretos. Es posible que el atacante ocultara información sobre otros archivos, tales como imágenes o audio para enviarlos posteriormente o tenerlos almacenados sin llamar la atención. Habitualmente hallaremos más información en ubicaciones ocultas que en los lugares más habituales.

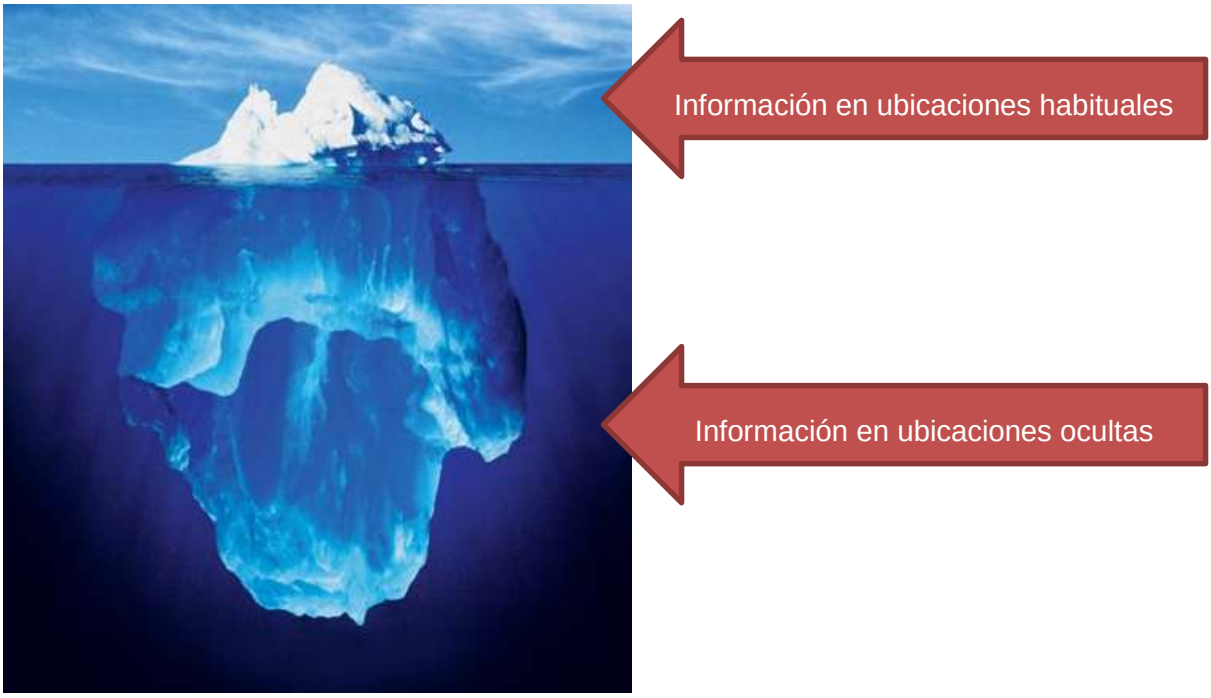


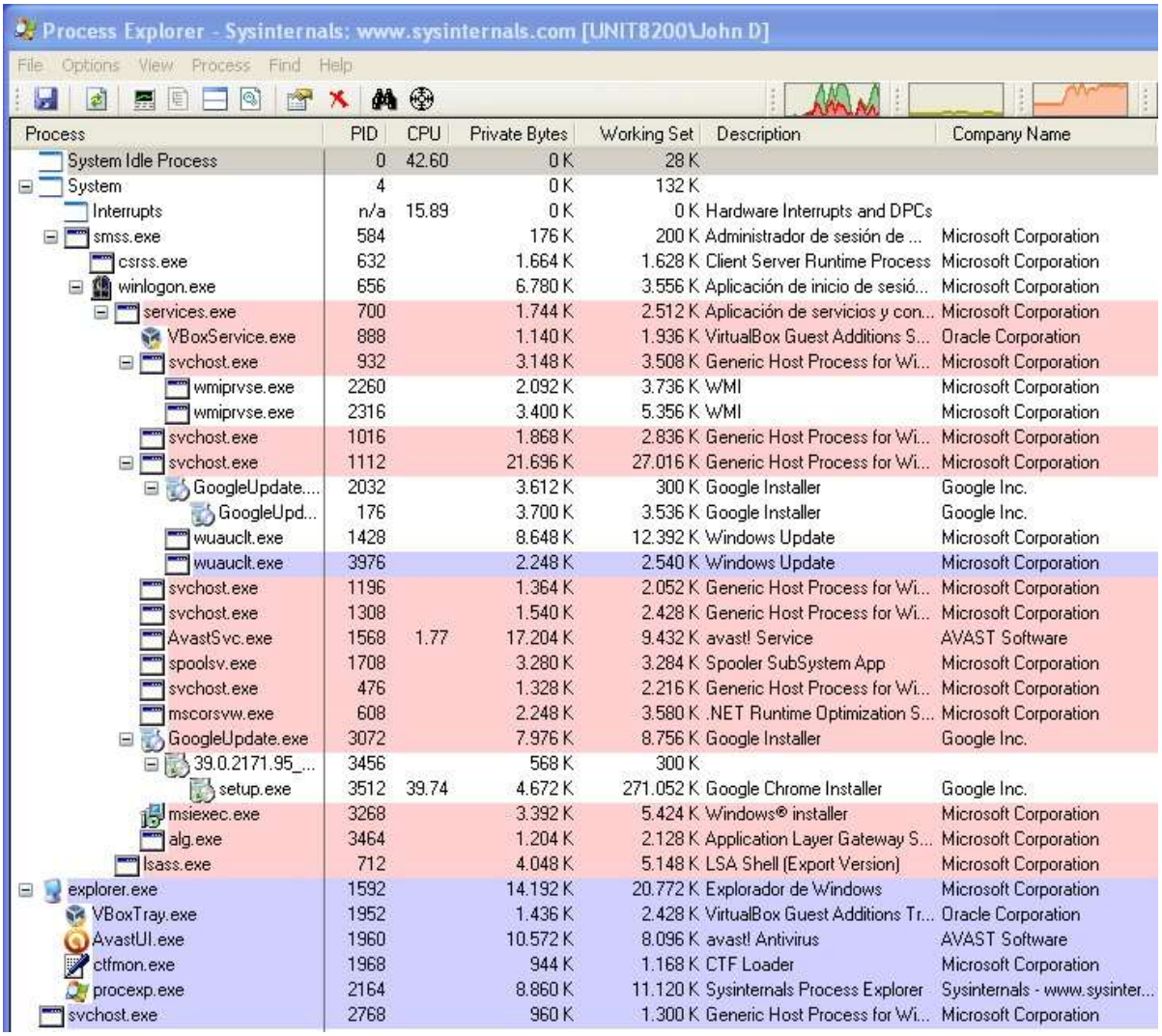
Ilustración 12: Ubicación de la información en el sistema

Con todos estos datos se debería poder crear un esbozo de los puntos clave en el tiempo tales como la instalación del sistema, el borrado de determinados archivos, la instalación de los últimos programas, etcétera.

3.5.3. Determinar cómo se actuó

Para determinar cómo se actuó es importante llevar a cabo una investigación sobre la memoria del equipo. Es interesante realizar un volcado de memoria para la obtención de cierta información. Con programas destinados a tal fin podremos ver que procesos se están ejecutando en el momento concreto y también aquellos que hayan sido ocultados para no levantar sospechas. Con esta información podremos saber qué ejecutables inician los procesos en ejecución y qué librerías se ven involucradas. Llegados aquí se puede proceder a realizar volcados de los ejecutables y de dichas librerías para poder analizar si contienen cadenas sospechosas o si, por lo contrario, son archivos legítimos. Sabiendo los procesos que se ejecutan y su naturaleza podemos obtener pistas de cómo se actuó para comprometer el equipo.

A menudo nos deberemos fijar en procesos en ejecución aparentemente inofensivos, habituales y legítimos en los sistemas operativos. No es extraño que determinados procesos con fines malintencionados se camuflen con procesos legítimos. Para ello deberemos observar que muchas veces estos se encuentran sin un proceso padre, cuando lo más habitual es que dependan de otros. En otras ocasiones simplemente se camuflan con nombres muy parecidos a otros para pasar desapercibidos.



Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	42.60	0 K	28 K		
System	4		0 K	132 K		
Interrupts	n/a	15.89	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	584		176 K	200 K	Administrador de sesión de ...	Microsoft Corporation
csrss.exe	632		1.664 K	1.628 K	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	656		6.780 K	3.556 K	Aplicación de inicio de sesió...	Microsoft Corporation
services.exe	700		1.744 K	2.512 K	Aplicación de servicios y con...	Microsoft Corporation
VBoxService.exe	888		1.140 K	1.936 K	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe	932		3.148 K	3.508 K	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe	2260		2.092 K	3.736 K	WMI	Microsoft Corporation
wmiprvse.exe	2316		3.400 K	5.356 K	WMI	Microsoft Corporation
svchost.exe	1016		1.868 K	2.836 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1112		21.696 K	27.016 K	Generic Host Process for Wi...	Microsoft Corporation
GoogleUpdate....	2032		3.612 K	300 K	Google Installer	Google Inc.
GoogleUpd...	176		3.700 K	3.536 K	Google Installer	Google Inc.
wuauclt.exe	1428		8.648 K	12.392 K	Windows Update	Microsoft Corporation
wuauclt.exe	3976		2.248 K	2.540 K	Windows Update	Microsoft Corporation
svchost.exe	1196		1.364 K	2.052 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1308		1.540 K	2.428 K	Generic Host Process for Wi...	Microsoft Corporation
AvastSvc.exe	1568	1.77	17.204 K	9.432 K	avast! Service	AVAST Software
spoolsv.exe	1708		3.280 K	3.284 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	476		1.328 K	2.216 K	Generic Host Process for Wi...	Microsoft Corporation
mscorsvw.exe	608		2.248 K	3.580 K	.NET Runtime Optimization S...	Microsoft Corporation
GoogleUpdate.exe	3072		7.976 K	8.756 K	Google Installer	Google Inc.
39.0.2171.95_...	3456		568 K	300 K		
setup.exe	3512	39.74	4.672 K	271.052 K	Google Chrome Installer	Google Inc.
msiexec.exe	3268		3.392 K	5.424 K	Windows® installer	Microsoft Corporation
alg.exe	3464		1.204 K	2.128 K	Application Layer Gateway S...	Microsoft Corporation
lsass.exe	712		4.048 K	5.148 K	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1592		14.192 K	20.772 K	Explorador de Windows	Microsoft Corporation
VBoxTray.exe	1952		1.436 K	2.428 K	VirtualBox Guest Additions Tr...	Oracle Corporation
AvastUI.exe	1960		10.572 K	8.096 K	avast! Antivirus	AVAST Software
ctfmon.exe	1968		944 K	1.168 K	CTF Loader	Microsoft Corporation
procexp.exe	2164		8.860 K	11.120 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
svchost.exe	2768		960 K	1.300 K	Generic Host Process for Wi...	Microsoft Corporation

Ilustración 13: Captura de Process Explorer

Ciertos programas también nos darán información sobre las cadenas del ejecutable en cuestión. Con ellas podremos ver si mutan su contenido cuando se ejecutan en memoria y cuál es su contenido. En ocasiones, cierta información de las cadenas nos puede dar pistas muy valiosas, como por ejemplo, cadenas dónde encontrar *logs*, o enlaces a direcciones de Internet. También nos puede dar pistas sobre el tipo de *malware* al que nos enfrentamos. Si por ejemplo encontramos cadenas con alfabetos o teclas concretas del teclado, es probable que nos encontremos ante un *keylogger.*

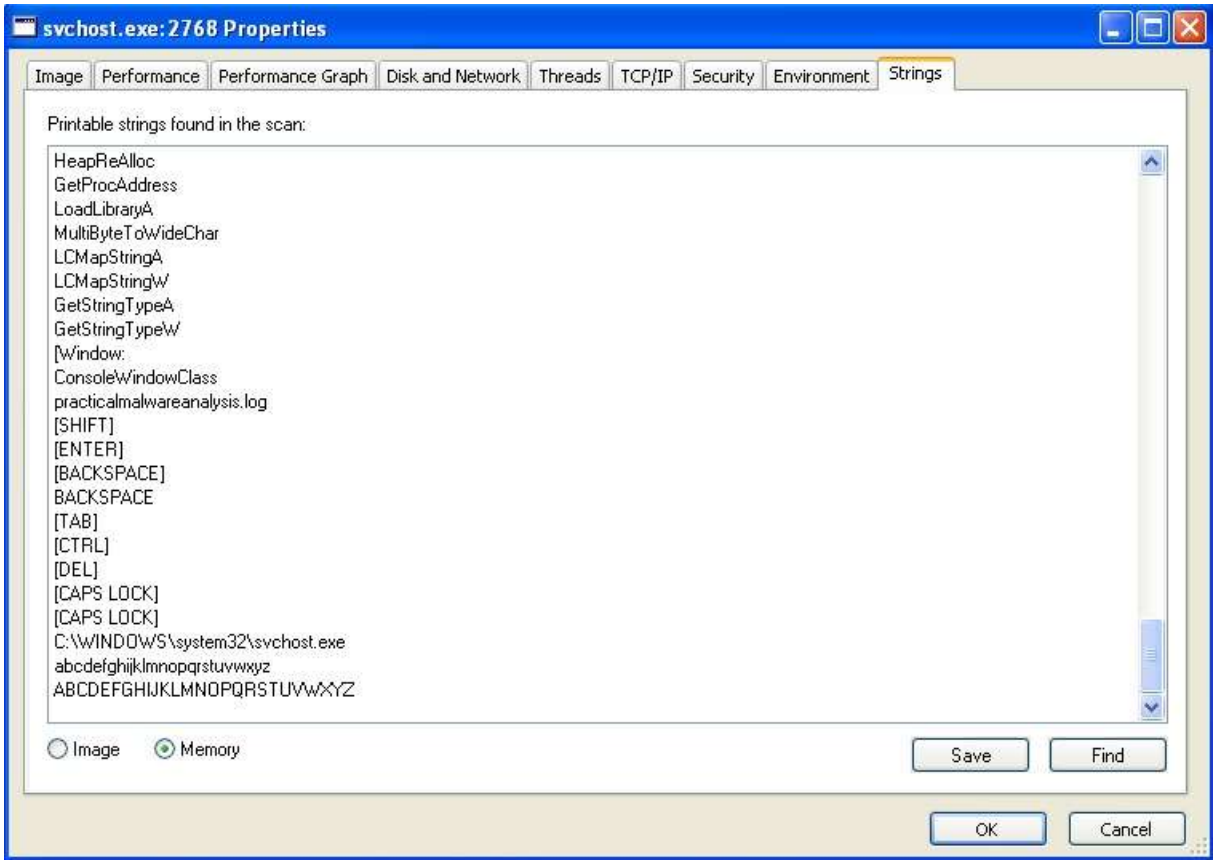


***Ilustración 14: Captura de* strings *de una aplicación* malware**

Finalmente, otra práctica interesante para determinar cómo se actuó es leer la secuencia de comandos escrita por consola. Para ello procederemos con el volcado de memoria y podremos obtener dicha información. De este modo podremos leer que comandos se hicieron por consola y sabremos si se ejecutó algún proceso de este modo. Debemos excluir nuestras propias instrucciones pues seguramente aparecerán los comandos del volcado de memoria que se hicieron en su momento.

3.5.4. Identificación de autores

Para poder realizar una identificación del autor o autores del incidente, otra información importante que nos puede dar el volcado de memoria son las conexiones de red abiertas y las que están preparadas para enviar o recibir datos. Con esto podremos relacionar el posible origen del ataque buscando datos como la dirección IP en Internet.

Hay que actuar con prudencia puesto que en ocasiones se utilizan técnicas para distribuir los ataques o falsear la dirección IP. Hay que ser crítico con la información que se obtiene y contrastarla correctamente. No siempre se obtendrá la respuesta al primer intento y posiblemente en ocasiones sea muy difícil averiguar el origen de un incidente.

Es interesante recapacitar en los distintos perfiles de atacantes que se pueden dar hoy día en este ámbito para intentar mimetizarse y entender quién pudo ser el autor.

Por un lado podemos encontrar organizaciones y criminales que actúan por motivaciones económicas. Su finalidad es robar cierta información, ya sea empresarial o personal, para una vez obtenida venderla o sacar un rendimiento oneroso de la información.

Por otro lado está quién sólo busca acceder a sistemas por mero prestigio y reconocimiento en su ambiente cibernético. Accediendo a sistemas mal configurados y publicando datos que prueben su fechoría incrementará su notoriedad y se dará a conocer más en las redes.

En este punto es importante analizar dos vertientes. En caso que se esté realizando un peritaje con fines inculpatorios, o sea, judiciales, se deberá intentar resolver quién es el autor o al menos aportar pistas fiables para que otros investigadores puedan llevar a cabo otras investigaciones de otros ámbitos.

En cambio, si es con fines correctivos lo más interesante seguramente será obviar esta fase y proceder con el estudio del impacto causado y estudiar las mejoras que se pueden implantar para evitar episodios similares.

3.5.5. Impacto causado

El impacto causado se puede calcular en base a distintos factores y no hay un método único para su cálculo, ni una fórmula que nos dé un importe económico. Aun así para estos cálculos puede servir ayudarse de métodos como BIA (*Business Impact Analysis)* que determinan el impacto de ciertos eventos ayudando a valorar los daños económicamente.

A la larga cualquier incidente ocurrido devengará en unos gastos económicos que habrá que cuantificar en función de los ítems afectados tras el suceso. En ocasiones el coste económico resultará de tener que reemplazar una máquina o dispositivo que ha quedado inservible tras un ataque o bien las horas de empleado de tener que reinstalar el sistema. En este caso, el cálculo no supone mayor dificultad y se resuelve fácilmente.

En otras ocasiones, por ejemplo, los daños pueden deberse al robo de una información de secreto industrial en el que habrá que cuantificar no sólo qué supone reponer el sistema sino, a la larga, en qué se verá afectada la empresa. Los datos robados pueden ser para publicar cierta información sobre la empresa y poner en la opinión pública datos con intenciones de crear mala imagen, lo cual supone un daño incalculable y muy elevado para la empresa.

El impacto no sólo se puede calcular en base económica. Como ya se ha comentado al inicio de esta sección también existen otros factores, es el caso del tiempo de inactividad. Si el incidente ha supuesto paralizar la producción de una planta automatizada de fabricación esto supone muchas horas en que la producción es nula, por lo tanto no se trabajará. Evidentemente, a la larga también supondrá un problema económico pues no se podrán servir los pedidos pendientes de los clientes. Si la paralización afecta a una oficina, tal vez no se pare la producción de bienes pero sí el trabajo de los empleados que verán retrasado todo su trabajo.

3.6. 5ª FASE: REDACCIÓN DE INFORMES

La última fase de un análisis forense queda para redactar los informes que documenten los antecedentes del evento, todo el trabajo realizado, el método seguido y las conclusiones e impacto que se ha derivado de todo el incidente.

Para ello se redactarán dos informes, a saber, el informe técnico y el ejecutivo. En esencia en ambos informes se explican los mismos hechos pero varía su enfoque y el grado de detalle con que se expone el asunto.

- En el informe ejecutivo se usará un lenguaje claro y sin tecnicismos, se debe evitar usar terminología propia de la ciencia e ingeniería y expresiones confusas para gente no ducha en el tema. 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 al máximo.
- En el informe técnico, por el contrario, 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, etcétera. Debemos crear un documento que pueda servir de guía para repetir todo el proceso que se ha realizado en caso necesario.

3.6.1. El informe ejecutivo

Entrando más en detalle en este tipo de informes, cabe destacar que será un resumen de toda la tarea que se ha llevado a cabo con las evidencias digitales. Aunque será un documento de poca extensión, al menos comparado con el informe técnico, éste deberá contener al menos los siguientes apartados:

- Motivos de la intrusión.
  - ¿Por qué se ha producido el incidente?
  - ¿Qué finalidad tenía el atacante?
- Desarrollo de la intrusión.
  - ¿Cómo lo ha logrado?
  - ¿Qué ha realizado en los sistemas?
- Resultados del análisis.
  - ¿Qué ha pasado?
  - ¿Qué daños se han producido o se prevén que se producirán?
  - ¿Es denunciable?
  - ¿Quién es el autor o autores?
- Recomendaciones.
  - ¿Qué pasos dar a continuación?
  - ¿Cómo protegerse para no repetir los hechos?

3.6.2. El informe técnico

El informe técnico será más largo que el anterior y contendrá mucho más detalle. Se hará una exposición muy detallada de todo el análisis con profundidad en la tecnología usada y los hallazgos. En este caso se deberá redactar, al menos:

- Antecedentes del incidente.
    - Puesta en situación de cómo se encontraba la situación anteriormente al incidente.
- Recolección de datos.
    - ¿Cómo se ha llevado a cabo el proceso?
    - ¿Qué se ha recolectado?
- Descripción de la evidencia.
    - Detalles técnicos de las evidencias recolectadas, su estado, su contenido, etc.
- Entorno de trabajo del análisis.
    - ¿Qué herramientas se han usado?
    - ¿Cómo se han usado?
- Análisis de las evidencias.
    - Se deberá informar del sistema analizado aportando datos como las características del sistema operativo, las aplicaciones instaladas en el equipo, los servicios en ejecución, las vulnerabilidades que se han detectado y la metodología usada.
- Descripción de los resultados.
    - ¿Qué herramientas ha usado el atacante?
    - ¿Qué alcance ha tenido el incidente?
    - Determinar el origen del mismo y como se ha encontrado.
- Dar la línea temporal de los hechos ocurridos con todo detalle.
- Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado.
- Dar unas recomendaciones sobre cómo proteger los equipos para no repetir el incidente o sobre cómo actuar legalmente contra el autor.

4. CONCLUSIONES

En este último capítulo vamos a repasar tanto el trabajo realizado como el posible trabajo futuro que se podría derivar de este. También destacaremos los principales problemas encontrados a lo largo del mismo y a qué conclusiones se puede llegar.

4.1. TRABAJO REALIZADO Y PROBLEMAS SURGIDOS

Como ya se ha visto a la largo de todo el trabajo, en la actualidad, no hay ninguna guía oficial, ni ningún estándar publicado que detalle todos y cada uno de los pasos que debe dar un investigador a lo largo de un caso. Esto provoca que cada profesional trabaje de un modo distinto y que cada uno aplique sus normas y conocimientos de la mejor manera posible o según los recursos de que disponga.

Aun así, existen varios documentos publicados por organismos de certificación y también por entidades dedicadas a la seguridad informática, así como departamentos de policía y de justicia que han publicado diversos documentos que pueden servir de ayuda y referencia para los profesionales investigadores forenses.

Son ejemplos de estos documentos, la RFC 3227, las UNE 71505 y 71506 o incluso la ISO 27037 que pueden servir de guía para determinados casos y resultar un buen punto de partida para determinadas situaciones.

En este trabajo, tras el análisis de la situación actual y viendo la necesidad de una metodología para el análisis forense se ha determinado la necesidad de crear dicha metodología de trabajo y para ello se ha partido de las consideraciones y ayudas de muchos de estos documentos.

Uno de los problemas que han surgido para la elaboración de esta metodología ha sido la gran variedad de situaciones que se dan en un análisis forense. Resulta casi imposible analizar todas y cada una de estas situaciones y por lo tanto se ha optado por intentar describir las situaciones más habituales que se pueden dar en función del tipo de investigación, sea con unos fines u otros. La idea es generar una metodología de análisis lo más versátil posible y que se pueda adaptar al máximo de situaciones posibles. La metodología creada se basa en un análisis de 5 fases, a saber, asegurar la escena, identificar y recolectar las evidencias, preservarlas, analizar las evidencias obtenidas y redactar los informes pertinentes con los resultados obtenidos.

En base a esta consideración no cabe decir que ha resultado imposible, por la extensión y tiempo de dedicación de este Trabajo de Final de Máster, realizar un examen exhaustivo de todas las posibles variantes y como solucionar o afrontar todas ellas.

En este trabajo también se ha realizado un repaso a la normativa legal vigente, en el momento de redacción del trabajo, de las leyes, tanto nacionales como internacionales, que vale la pena conocer en este ámbito. El conocimiento de la legislación es importante de cara al investigador puesto que ayuda a conocer los límites de la investigación así como determinar qué casos pueden, o no, ser constitutivos de delito.

Del mismo modo, se ha realizado una pequeña investigación sobre los programas más utilizados en la investigación forense organizándolos en base a sus usos, por ejemplo, análisis de memorias, de discos, de redes u otros. Este resumen de aplicaciones es vigente en el momento de redacción de esta guía pero hay que recordar que la evolución del *software* y la aparición y desaparición de éste es constante.

4.2. TRABAJO FUTURO

En vista de las dificultades surgidas en cuanto a la gran diversidad de casos que se presentan en un análisis forense, un posible trabajo futuro sería crear un conjunto de guías en función de cada finalidad de la investigación.

En base a la clasificación realizada en el apartado 2.2. se podrían generar guías para cada finalidad, a saber, preventiva, correctiva, probatoria y auditoria. Además se podría ampliar sustancialmente para los análisis probatorios en función de los equipos involucrados, los sistemas operativos, si hay redes involucradas o no, tipo de ataque sufrido, etcétera.

Posiblemente cada una de estas metodologías detalladas podría dar lugar a varios trabajos de estas características.

5. GLOSARIO DE TERMINOLOGÍA UTILIZADA

A

Agencia Europea de Seguridad de las Redes y de la Información (ENISA): El objetivo de ENISA es mejorar las redes y la seguridad de la información en la Unión Europea. La agencia tiene que contribuir al desarrollo de una cultura de red y seguridad de la información para el beneficio de los ciudadanos, consumidores, empresas y organizaciones del sector público de la Unión Europea, y por tanto contribuirá a mejorar el funcionamiento interno de la UE.

B

BIA (*Business Impact Analysis):* Es un informe que muestra el coste ocasionado por la interrupción de los procesos de negocio.

Bits: El bit es la unidad de información empleada en informática, en cualquier dispositivo digital o en la teoría de la información.

C

Crash dumps: Volcado de memoria con su contenido que ocurre en caso de error. Es un registro de datos.

CRC (Código de Redundancia cíclica): Es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos.

Centro Europeo contra la Ciberdelincuencia: Es el punto central de la lucha de la UE contra la delincuencia cibernética, contribuyendo a una reacción más rápida a los delitos en línea.

Conectores OLE: Es una tecnología desarrollada por Microsoft usada para tener acceso a diferentes fuentes de información, o bases de datos, de manera uniforme.

D

DLL *(Dynamic-Link Library)*: Se refiere a los archivos con código ejecutable que se cargan bajo demanda de un programa por parte del sistema operativo. Es una denominación exclusiva de sistemas operativos Windows.

DMZ (*Demilitarized zone):* Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

DNS *(Domain Name System)*: Es un Sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

E

Encriptado: Es el procedimiento que utiliza un algoritmo de cifrado con cierta clave para transformar un mensaje, sin atender a su estructura lingüística o

significado, de tal forma que sea incomprensible o, al menos, difícil de comprender para quienes no tengan la clave privada.

ENISA: Ver Agencia Europea de Seguridad de las Redes y de la Información.

Eurojust: Es un órgano de la UE encargado del refuerzo de la cooperación judicial entre los Estados miembros, mediante la adopción de medidas estructurales que facilitan la mejor coordinación de las investigaciones y las actuaciones judiciales que cubren el territorio de más de un Estado miembro.

Europol: Es el órgano encargado de facilitar las operaciones de lucha contra la delincuencia en el seno de la UE.

EXIF *(Exchangeable Image File Format)*: Es una especificación para formatos de archivos de imagen usado por las cámaras digitales.

F

Firewall: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

H

Hash* o funciones *hash: Es una función que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte en un rango de salida finito, normalmente de longitud fija.

I

Ingeniería inversa: El objetivo es obtener información o un diseño a partir de un producto, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado.

(IETF) Internet Engineering Task Force: Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

J

Javascript: Es un lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico.

Jumper: Es un elemento que permite interconectar dos terminales de manera temporal sin tener que efectuar una operación que requiera una herramienta adicional.

K

***Kernel*:** Término que proviene del germánico *Kern*. Es la parte fundamental del Sistema operativo, y se define como la parte que se ejecuta en modo privilegiado.

L

***Log*:** Es un registro de eventos durante un rango de tiempo particular.

M

MACD: Es un conjunto de metadatos de un fichero que aportan información sobre las fechas y horas en que el archivo ha sido modificado, accedido, creado o eliminado.

Macro: Conjunto de instrucciones que se almacenan para que se ejecuten de manera secuencial mediante una sola llamada.

Malware: Del inglés *malicious software*, es un tipo de *software* que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de sus propietario.

P

Proxy: En una red informática, es un servidor que sirve de intermediario en las peticiones de recursos que realiza un cliente u otro servidor.

Python: Es un lenguaje de programación interpretado cuya filosofía hace hincapié en una sintaxis que favorezca un código legible.

R

RAM *(Random Access Memory)*: Es un tipo de memoria de trabajo para el sistema operativo, los programas y la mayor parte del software.

Raw: Término que se refiere a formatos de archivos con compresión de datos per sin pérdida de información.

Rootkit: Permite un acceso de privilegio continuo a una computadora pero mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

S

Shellcode: Permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del Sistema operativo o de otras aplicaciones.

Spam: Término que hace referencia a todas aquellas comunicaciones cuyo contenido es no deseado, no solicitado o se desconoce su remitente. Aunque lo más habitual es que estos mensajes lleguen por correo electrónico también pueden ser en forma de llamadas telefónicas, redes sociales, foros, blogs, wikis o cualesquiera otros métodos.

6. BIBLIOGRAFÍA Y REFERENCIAS

1. **The Internet Engineering Task Force (IETF). [En línea] https://www.ietf.org.**

2. Asociación Española de Normalización y Certificación. [En línea] www.aenor.es.

3. International Organization for Standardization. [En línea] www.iso.org.

4. Association of Chief Police Officers. [En línea] www.acpo.police.uk.

5. National Criminal Justice Reference Service. [En línea] https://www.ncjrs.gov.

6. Martínez Retenaga, Asier. *Guía de toma de evidencias en entornos Windows.* s.l. : Instituto Nacional de Ciberseguridad, Noviembre 2014.

7. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* 2004.

8. *Good Practice Guide for Computer-Based Electronic Evidence.*

9. Boletín Oficial del Estado. *Constitución Española.* [En línea] https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229&b=17&tn=1&p=19781229#a13.

10. Boletín Oficial del Estado. *Ley de Enjuiciamiento Civil.* [En línea] https://www.boe.es/buscar/act.php?id=BOE-A-2000-323.

11. Boletín Oficial del Estado. *Ley de Protección de Datos de Carácter Personal.* [En línea] https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750.

12. Boletín Oficial del Estado. *Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.* [En línea] https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

13. Boletín Oficial del Estado. *Ley de Conservación de Datos Relativos a las Comunicaciones y las Redes Públicas.* [En línea] https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243.

14. Boletín Oficial del Estado. *Código Penal.* [En línea] https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

15. Boletín Oficial del Estado. *Directiva 2006/24/CE.* [En línea] https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

16. Boletín Oficial del Estado. *Directiva 2013/40/UE.* [En línea] http://www.boe.es/diario_boe/txt.php?id=DOUE-L-2013-81648.

17. Eurojust. *The European Union's Judicial Cooperation Unit.* [En línea] http://www.eurojust.europa.eu/Pages/home.aspx.

18. Europol. [En línea] https://www.europol.europa.eu/.

19. European Cybercrime Centre. *Europol.* [En línea] https://www.europol.europa.eu/ec3.

20. European Union Agency for Network and Information Security. *ENISA.* [En línea] http://www.enisa.europa.eu/.

21. Snort. [En línea] https://www.snort.org/.

22. Nmap. [En línea] nmap.org.

23. Wireshark. [En línea] https://www.wireshark.org/.

24. Xplico. [En línea] http://www.xplico.org/.

25. Back|Track-linux. [En línea] http://www.backtrack-linux.org/.

26. MountManager. [En línea] https://code.google.com/p/linuxtuner/.

27. Guymanager. [En línea] http://guymager.sourceforge.net/.

28. Volatility. [En línea] https://code.google.com/p/volatility/.

29. Memoryze Mandiant. [En línea] https://www.mandiant.com/resources/download/memoryze.

30. Redline Mandiant. [En línea] https://www.mandiant.com/resources/download/redline.

31. OllyDbg. [En línea] http://www.ollydbg.de/.

32. OfficeMalScanner. [En línea] http://www.aldeid.com/wiki/OfficeMalScanner.

33. Radare. [En línea] https://github.com/radare/radare2.

34. Windows Sysinternals Process Explorer. [En línea] http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx.

35. PDF Stream Dumper. [En línea] http://sandsprite.com/blogs/index.php?uid=7&pid=57.

36. DEFT Linux. [En línea] http://www.deftlinux.net/.

37. ForLEx Linux. [En línea] http://www.forlex.it/.

38. Computer Forensics Linux Live Distro. *CAINE.* [En línea] http://www.caine-live.net/.

39. Autopsy. *SleuthKit.* [En línea] http://www.sleuthkit.org/autopsy/.

40. Brezinski, D. y Killalea, T. *RFC 3227.* s.l. : IETF, 2002.

41. ISO/IEC 27037:2012. [En línea] http://www.iso.org/iso/catalogue_detail?csnumber=44381.

42. AENOR. *UNE 71505-1:2013.* [En línea] http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051411#.VJMhnXtG-NA.

43. AENOR. *UNE 71506:2013.* [En línea] http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414#.VJMhvntG-NA.

44. ISO/IEC 17799:2005. [En línea] http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612.

45. Oracle VirtualBox. [En línea] https://www.virtualbox.org/.

46. Wikipedia. Cadena de custodia. [En línea] http://es.wikipedia.org/wiki/Cadena_de_custodia

47. INCIBE. RFC 3227 – Directrices para la recopilación de evidencias y su almacenamiento. [En línea] https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/rfc3227

48. Whos. White Hat and Other Stuff. [En línea] http://wh0s.org/category/analisis-forense/

49. MaTTica. [En línea] http://mattica.com/como-asegurar-la-evidencia-forense-digital/

50. La contaminación de la cadena de custodia invalida las pruebas periciales informáticas. [En línea] http://tecnologia.elderecho.com/tecnologia/internet_y_tecnologia/contaminacion-custodia-invalida-periciales-informaticas_11_556555001.html

51. Evidencia Digital: Casos Reales. [En línea] http://www.presman.com.ar/admin/archivospublicaciones/archivos/Curso%20PGN_20100706100513.pdf

52. Análisis Forense. [En línea] http://www.angelalonso.es/doc-presentaciones/AF_v3.pdf

53. Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0. [En línea] http://www.oas.org/juridico/english/cyb_pan_manual.pdf

54. Fases de la Informática Forense [En línea] http://dspace.ups.edu.ec/bitstream/123456789/546/4/CAPITULO3.pdf

55. Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital. Tomás Marqués-Arpa; Jordi Serra-Ruiz. [En línea] http://web.ua.es/en/recsi2014/documentos/papers/cadena-de-custodia-en-el-analisis-forense-implementacion-de-un-marco-de-gestion-de-la-evidencia-digital.pdf

56. Análisis Forense Digital. Miguel López Delgado. [En línea] http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

57. La importancia de la evidencia y el análisis forense digital. [En línea] http://www.bsecure.com.mx/opinion/la-importancia-de-la-evidencia-y-el-analisis-forense-digital/

58. Perfiles de atacantes y delincuentes en Internet. [En línea] http://blog.segu-info.com.ar/2011/01/perfiles-de-atacantes-y-delincuentes-en.html

59. El impacto económico de los ataques de seguridad. [En línea] http://www.redseguridad.com/opinion/articulos/el-impacto-economico-de-los-ataques-de-seguridad

60. Ataques informáticos. [En línea] https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

ANEXO

En el presente anexo se incluyen las prácticas realizadas en la asignatura “Prácticas Profesionalizadoras” del Máster. De este modo se pueden leer ejemplos prácticos y como se desarrolla la investigación.

En anexo de distribuye en dos ejemplos.

1ER EJEMPLO

Enunciado

En esta ocasión, nos ha llegado un ordenador de un ministerio que se supone está comprometido con un archivo malicioso. Se trata de un portátil utilizado por un agente de seguridad infiltrado que ha sido descubierto por un delincuente implicado en la trama que se investigaba, y se sospecha que ha sido por un malware que le han instalado en el ordenador que utilizaba.

Para esta ocasión se nos ha encomendado la tarea de realizar un análisis sobre el equipo afectado (máquina virtual). Este equipo se le ha revocado el acceso a la VPN ya que se sospecha que el compromiso ha sido total y hasta que no se extraigan todos los detalles de la intrusión volverá a estar “on-line” en dicha red.

Inicialmente y para conocer esta pericia, el análisis que se nos pide es de tipo “black-box” (sin ningún tipo de pista).

1. ¿Existe un malware en el equipo investigado? Extraer el nombre y contestar a las siguientes preguntas:

- ¿Se clasifica dentro de algún grupo?
- Cuándo se compiló
- ¿Migra el proceso cuando se ejecuta el archivo? ¿A cuál?
- ¿Cambia el ejecutable dependiendo de si se ejecuta en memoria o en disco?
- ¿Cuándo se ejecuta en memoria, el ejecutable tiene alguna cadena sospechosa?
- ¿Qué tipo de malware es?
- ¿Genera algún tipo de log donde guarde la información?

2. En alguna parte del HD del equipo comprometido hay una serie de logs que el agente infiltrado consiguió antes de ser descubierto, pero ante las prisas no recuerda donde lo metió. Menciona que lo guardó junto a una captura de red, es un *.txt y ambos están en el mismo directorio. Una vez encontrada los log:

- ¿Qué protocolo se usa según el archivo?
- ¿Es TCP o UDP?
- ¿Con que herramienta parece haber sido obtenido y cuál es el objetivo de esta herramienta?
- ¿Se puede obtener algún tipo de geolocalización a partir del log?

3. Ya puestos, aprovechamos para analizar la captura de red:

- ¿Qué protocolos se incluyen en la captura?
- ¿Se obtuvo acceso a algún archivo del servidor? ¿Con qué credenciales?
- ¿Se puede obtener algo más de la captura? En caso afirmativo indicar qué.

Resolución

Para la resolución de esta investigación se ha empezado por descargar la imagen que nos han proporcionado sobre el equipo afectado. Una vez descargada se ha realizado una copia sobre la que se ha trabajado manteniendo siempre la versión descargada, intacta, por si ocurría algún problema.

Posteriormente se ha ejecutado la máquina virtual, con sistema operativo Windows XP Service Pack 3. A partir de aquí se han realizado los siguientes pasos:

1. Volcado de memoria sin ejecutar ninguna aplicación para ver qué procesos están activos. También se buscan procesos ocultos y conexiones de red abiertas o puertos en escucha. Esta vía de análisis no arroja ningún resultado positivo. A simple vista no hay ningún proceso *malware* en ejecución ni conexiones sospechosas.
2. Volcado de memoria directamente de la imagen del sistema sin arrancar la máquina virtual. Esta opción está disponible ejecutando por consola de comandos Oracle VM VirtualBox. Con esta opción tampoco se detectan procesos ni ejecutables sospechosos.
3. Se intenta abrir la imagen del sistema con el *software* Autopsy pero este parece no reconocer la imagen y no carga nada. Se convierte el formato VMDK en RAW e IMG con el *software* “qemu” pero Autopsy tampoco carga la imagen. Se abandona esta vía de análisis.

Hasta el momento se han intentado vías de análisis poco intrusivas con el equipo evitando al máximo las escrituras en disco. Como consecuencia del poco éxito en la búsqueda se decide ejecutar los programas que hay en el equipo y realizar las búsquedas con el buscador del sistema operativo.

1. Se ejecuta el antivirus del sistema, Avast, aun sabiendo que puede estar afectado por cualquier *malware.* No arroja ninguna amenaza.
2. Se utiliza el buscador del sistema operativo para buscar archivos de texto TXT y capturas de red PCAP. Las búsquedas no aportan ningún resultado.
3. Se decide ir directamente a directorios dónde habitualmente se esconden *malwares,* por ejemplo, carpetas de archivos temporales, carpeta SYSTEM32, carpeta WINDOWS, etc. Al intentar acceder a esta última el contenido está vacío a simple vista. Al parecer hay un problema con el sistema de archivos.
4. Reiniciamos el equipo para ver si se corrige y al cargar de nuevo el sistema operativo se solventan, aparentemente, todos los archivos de esa ubicación. Seguimos disponiendo de una copia sin tocar por si esto ha ido mal.
5. Volvemos a buscar todos los archivos TXT y se encuentra el *log* con la captura PCAP en el mismo directorio. Están en C:\WINDOWS\Stole_logs, los archivos son:
    a. logs_honeypot_VoIP.txt
    b. VoIP attack.pcap

6. A modo de prueba ejecutamos el antivirus del equipo para ver si nos puede ayudar. Efectivamente nos indica que hay un archivo *malware.* Su ruta: C:\WINDOWS\system32\txu_Ng_0.exe

A partir de aquí podemos empezar a responder las cuestiones planteadas haciendo uso de varias utilidades, tanto instaladas en el propio equipo, como otras de análisis forense y páginas web, tales como virustotal.com

En cuanto al *malware* podemos decir que el ejecutable es de tipo troyano, compilado, según virustotal.com, en fecha 08/04/2011 a las 17:54:23. Se puede observar que cuando se ejecuta carga dos procesos. Por un lado svchost.exe e hijo de este txu_Ng_0.exe. Al poco tiempo de lanzar la ejecución desaparece txu_Ng_0.exe quedando sólo en ejecución svchost.exe, sin padre. Esta forma de actuación es sintomática de *malwares* ya que este tipo de procesos siempre dependen de otros en el sistema. Así pues se confirma que el ejecutable migra cuando se ejecuta.

Analizando las cadenas del ejecutable en memoria podemos ver varias de ellas que son sospechosas:

- [SHIFT]
- [ENTER]
- [TAB]
- abc…xyz
- ABC…XYZ

Estas cadenas son típicas de *keyloggers*, que son aplicaciones que capturan todas las pulsaciones del teclado para saber lo que se ha escrito durante la ejecución.

Lo más habitual es que todo lo que capturen se guarde en un registro. Sucede lo mismo en este caso. En las cadenas del ejecutable podemos ver “practicalmalwareanalysis.log”. Se localiza en la ruta: C:\WINDOWS\system32\practicalmalwareanalysis.log y en su contenido podemos leer, entre otros:

```
[Window:  Sin título - Bloc de notas]

 to mark@mccd20132mde

[ENTER]Mark

[ENTER]no he podido completar mi mision creo q BACKSPACE   BACKSPACE   BACKSPACE
BACKSPACE  BACKSPACE  BACKSPACE  reo que me han descubierto

[ENTER]no tengo tiempo debo irme

[ENTER]he recogido cierta informacion sobre los

[ENTER]logs de los honeypot en la unit2BACKSPACE  8200

Junto con [ENTER] captura de trafico pcap

[ENTER]que me hacen pensar que la unit8200 posee algunos sistemas vulnerables
BACKSPACE    quizas sea debido a la BACKSPACE  s modificaciones recientes en los
sistemas de voip. He generado un diccionario passwords.txt que seguramente permita
crackear algunas extensiones de la centralita de VoIP. Lo he probado con la mayor
extensión de 4 dígitos y funciona.

[ENTER]También he dejado una grabacion oculta a mark en el server de voip que
podria darnos acceso BACKSPACE    BACKSPACE    BACKSPACE    BACKSPACE    BACKSPACE
```

```
BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE
BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE
BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE a los sBACKSPACE
objetivos elint e imint…Ahhh se me olvidaba, la password de acceso de admin al
servicio de call manager  VoIP por telnet  la he cambiado a un nombre de un país
que tú sabes…..

[ENTER][ENTER]end
```

En cuanto al *log* que se guardó en la ubicación C:\WINDOWS\Stole_logs podemos ver que entre otros se usa el protocolo SIP *(Session Initiation Protocol)* que es un protocolo de señalización para VoIP. El otro protocolo que también se aprecia en el archivo es el conocido UDP, sobre el cual funciona el anterior.

Mirando el archivo parece que se ha usado una herramienta llamada "sipvicious". Si buscamos un poco por Internet se encuentra su web dónde pone que SIPVicious es un conjunto de herramientas que pueden ser usadas para auditar sistema VoIP. Entre sus varias funciones encontramos un escáner SIP, un identificador de extensiones, un *cracker* de contraseñas, etc.

En cuanto a las direcciones IP y su geolocalización encontramos los siguientes datos, haciendo uso de cualquier *whois* en Internet:

- 147.237.72.71: Ministerio de Economía de Israel
- 210.184.120.120: Hong Kong
- 89.42.194.10: Romania

Finalmente en cuanto a la captura de red encontrada, usando Wireshark podemos ver los protocolos implicados en cada captura. En mayor o menor medida se incluyen HTTP, TCP, UDP, RTCP, ICMP, RTP y SIP.

Analizando la captura, concretamente el paquete número 1279 vemos como se accedió al archivo de configuración *sip_custom.conf*. Para acceder se puede ver como se usaron las credenciales de usuario "maint" y password "password". `Credentials: maint:password`

Finalmente, Wireshark nos da la opción de descodificar las conversaciones VoIP, para ello *Telephony -> VoIP Calls -> Player -> Decode* se seleccionan los dos audios y se escucha la conversación. En ella se puede escuchar que la palabra clave, correspondiente al país que anteriormente se hablaba en otro *log* es México.

2º EJEMPLO

Enunciado

En este caso, hemos recibido un encargo urgente de una instancia de una máquina virtualizada sobre un servidor de un Ministerio, que se presume ha sido comprometido. Por nuestra parte nos toca realizar el análisis de la memoria. Para ello utilizaremos la herramienta Volatility ya que nos han indicado que el sistema era Windows.

Las tareas que debemos realizar:

1. Instalar volatility
2. Conocer las opciones que nos serán de utilidad
3. Implementar un informe que dé respuesta a las siguientes preguntas:
    - ¿De qué sistema operativo se trata?
    - Indicar si la máquina ha sido comprometida. En caso afirmativo indicar, en la medida de lo posible extraerlo. Evaluar su persistencia en el sistema.
    - ¿Existen procesos, dll's o módulos ocultos en el sistema o direcciones IP a las que se conecte? En caso afirmativo tratar de descubrirlos.

Resolución

Para la realización del informe se ha usado la herramienta de análisis de memoria "Volatility". El contenido del fichero *memoria.dd* a analizar se corresponde con el volcado de la memoria de una máquina virtual con sistema operativo Windows.

El primer paso para solventar la práctica es la instalación de la herramienta. En este caso se va a utilizar la versión 2.3.1 y más concretamente el ejecutable que no requiere instalación de la herramienta. Esta herramienta se puede ejecutar directamente desde consola mediante los comandos que necesitemos para ir desgranando la información que buscamos.

El siguiente paso consiste en analizar que comandos están disponibles en la aplicación y que datos nos da cada uno. Para ello ejecutamos la herramienta como sigue:

```
volatility-2.3.1.standalone.exe –h
```

Lo cual nos da como salida la siguiente lista de comandos y su breve explicación:

```
      Supported Plugin Commands:

            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
            dumpcerts           Dump RSA private and public SSL keys
            dumpfiles           Extract memory mapped and cached files
            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)
             hpakextract         Extract physical memory from an HPAK file
             hpakinfo            Info on an HPAK file
             idt                 Display Interrupt Descriptor Table
             iehistory           Reconstruct Internet Explorer cache / history
             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
             machoinfo           Dump Mach-O file format information
             malfind             Find hidden and injected code
             mbrparser           Scans for and parses potential Master Boot Records (MBRs)
             memdump             Dump the addressable memory for a process
             memmap              Print the memory map
             messagehooks        List desktop and thread window message hooks
             mftparser           Scans for and parses potential MFT entries
             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
             privs               Display process privileges
             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)
             shellbags           Prints ShellBags info
             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
```

```
timeliner           Creates a timeline from various artifacts in memory
timers              Print kernel timers and associated module DPCs
unloadedmodules     Print list of unloaded modules
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
vboxinfo            Dump virtualbox information
vmwareinfo          Dump VMware VMSS/VMSN information
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
```

Empezamos averiguando de qué sistema operativo se trata. Sabemos que es Windows pero desconocemos su versión y *service pack* instalado. Ejecutamos el comando siguiente para obtener dicha información.

```
volatility-2.3.1.standalone.exe –f memoria.dd imageinfo
```

Esto nos da los siguientes datos:

```
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (E:\UOC\Pràctiques\P2\memoria.dd)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054c760L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2009-10-24 11:01:36 UTC+0000
     Image local date and time : 2009-10-24 11:01:36 +0000
```

De lo cual se desprende que se trata de Windows XP con *service pack 2* ó *service pack 3*. También podemos ver a qué hora se hizo el volcado de memoria, así como el número de procesadores del equipo entre otros datos técnicos de la memoria.

A continuación puede ser interesante ver que procesos se estaban ejecutando en el momento del volcado de memoria, para ello ejecutaremos:

```
volatility-2.3.1.standalone.exe –f memoria.dd pslist
```

Que nos da las siguientes pistas:

```
Offset(V)  Name                PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- ---------------- ------ ------ ------ -------- ------ ----- -------------------
0x81233bd0 System                4      0     49      234 ------     0
0x810dc368 smss.exe            524      4      3       19 ------     0 2009-10-24 10:48:21
```

```
0x810d89a0 csrss.exe            596      524      10      231       0      0 2009-10-24 10:48:26
0x810be578 winlogon.exe         620      524      18      491       0      0 2009-10-24 10:48:27
0x810ec620 services.exe         664      620      14      235       0      0 2009-10-24 10:48:28
0xffb78150 lsass.exe            676      620      14      268       0      0 2009-10-24 10:48:29
0xffb538e0 vmacthlp.exe         844      664       1       24       0      0 2009-10-24 10:48:31
0x810cb1d0 svchost.exe          892      664       6      117       0      0 2009-10-24 10:48:33
0x810d3460 svchost.exe          960      664       9      193       0      0 2009-10-24 10:48:33
0x810d9a78 svchost.exe         1068      664      23      463       0      0 2009-10-24 10:48:34
0x810a2c90 svchost.exe         1096      664       6       60       0      0 2009-10-24 10:48:34
0xffb44638 svchost.exe         1220      664      10      153       0      0 2009-10-24 10:48:34
0xffb37278 VMwareService.e     1452      664       3      129       0      0 2009-10-24 10:48:37
0xffb7e4b8 explorer.exe        1704     1680      12      274       0      0 2009-10-24 10:51:05
0xffb19228 VMwareTray.exe      1780     1704       1       26       0      0 2009-10-24 10:51:07
0xffb17210 VMwareUser.exe      1788     1704       4       72       0      0 2009-10-24 10:51:07
0xffb153c0 cmd.exe             1012     1704       1       20       0      0 2009-10-24 11:01:34
0x81067da0 win32dd.exe         1020     1012       1       21       0      0 2009-10-24 11:01:34
```

De esta lista se desprende que se estaban ejecutando los servicios propios del sistema operativo así como los relativos a la máquina virtual, que al parecer es “VM Ware”. También podemos ver que se ejecutó la consola “cmd.exe” y acto seguido “win32dd.exe”. Esta aplicación sirve para hacer volcados de memoria y corresponde con la hora que antes se ha visto con `imageinfo`, a las 11:01:34 – 11:01:36.

Según esta información parece que no hay ningún proceso en ejecución fuera de lo normal, al menos en el momento del volcado de memoria. Para asegurarnos de esto ejecutaremos la siguiente instrucción que nos dará como resultado todos los procesos del sistema aunque estén ocultos por cualquier motivo.

```
volatility-2.3.1.standalone.exe –f memoria.dd psxview
```

Nos da la siguiente información:

```
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- ---
0x010a6620 services.exe            664 True   True   True     True   True  True    True
0x004038e0 vmacthlp.exe            844 True   True   True     True   True  True    True
0x02dfd278 VMwareService.e        1452 True   True   True     True   True  True    True
0x03da03c0 cmd.exe                1012 True   True   True     True   True  True    True
0x02086638 svchost.exe            1220 True   True   True     True   True  True    True
0x00ae3850 nc.exe                  408 False  True   True     False  True  True    True
0x0108d460 svchost.exe             960 True   True   True     True   True  True    True
0x0105cc90 svchost.exe            1096 True   True   True     True   True  True    True
0x03e4a228 VMwareTray.exe         1780 True   True   True     True   True  True    True
0x009e3150 lsass.exe               676 True   True   True     True   True  True    True
0x01093a78 svchost.exe            1068 True   True   True     True   True  True    True
0x01021da0 win32dd.exe            1020 True   True   True     True   True  True    True
0x010851d0 svchost.exe             892 True   True   True     True   True  True    True
0x03b6d210 VMwareUser.exe         1788 True   True   True     True   True  True    True
0x01078578 winlogon.exe            620 True   True   True     True   True  True    True
0x00d144b8 explorer.exe           1704 True   True   True     True   True  True    True
0x010929a0 csrss.exe               596 True   True   True     True   False True    True
0x01096368 smss.exe                524 True   True   True     True   False False   False
0x011edbd0 System                    4 True   True   True     True   False False   False
```

Analizando estos datos vemos que nos aparece el proceso “nc.exe” que anteriormente no aparecía, efectivamente indica *false* en la columna *pslist.* Una breve búsqueda en la red nos da información sobre este ejecutable que corresponde con la herramienta *netcat*. *Netcat* permite la ejecución remota de comandos a través de consola y abrir y cerrar puertos y conexiones en equipos remotos.

Con esta información la línea de investigación puede proseguir por dos caminos. Por un lado, ver si existen conexiones abiertas en la máquina que se está analizando. Por otro lado ver el contenido de la consola del equipo para ver si se ha digitado algún comando que pueda aportar más datos.

Vamos primero con el análisis de conexiones abiertas. Para ello ejecutaremos la siguiente opción:

```
volatility-2.3.1.standalone.exe –f memoria.dd connscan
```

Esta ejecución no nos devuelve ningún resultado lo cual indica que en el momento del volcado de memoria no existía ninguna conexión activa. Ello no quiere decir que no se puedan realizar conexiones, de hecho, esta es la utilidad de netcat, poder establecer comunicaciones con la máquina comprometida. Con la siguiente instrucción veremos si hay puertos abiertos esperando comunicación:

```
volatility-2.3.1.standalone.exe –f memoria.dd sockets
```

La salida de este comando es la siguiente:

```
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
```

En ella podemos ver que el PID 408, que corresponde con la ejecución de la aplicación “nc.exe” tiene abierto el puerto 31337, a la espera de conexiones usando el protocolo TCP. Según la información que dan los dos anteriores comandos parece ser que no hay ninguna dirección IP conectada, pero sí que la máquina que estamos analizando está comprometida ya que tiene puertos abiertos a la espera de posibles conexiones, además de haber ocultado el proceso en memoria para no levantar sospechas.

A continuación podemos analizar el contenido de los últimos comandos escritos por la consola del equipo comprometido para ver si podemos obtener alguna información más y acabar de ligar todo lo que ya se ha encontrado. Para ello disponemos de la siguiente opción:

```
volatility-2.3.1.standalone.exe –f memoria.dd cmdscan
```

Ello nos devuelve lo siguiente:

```
**************************************************
CommandProcess: csrss.exe Pid: 596
CommandHistory: 0x4e50d8 Application: cmd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x2a4
Cmd #0 @ 0xfc32d8: Nd \Malware\FUto
Cmd #1 @ 0x4e2328: Ntart nc -d -L -p 31337 -e cmd.exe
Cmd #2 @ 0x4e2a10: N?N?
Cmd          #3          @          0x4e9068:          Netstat          -a          -
```

```
??N???N?N
Cmd #4 @ 0x4e91a0: ??
Cmd #5 @ 0x4e9cf8: in32dd.exe
Cmd #6 @ 0x4e1eb8: N?N?
Cmd #7 @ 0x4e2ce8: N?N-phd msdirectx.sys
Cmd #8 @ 0x4e9e38: md.exe
**************************************************
CommandProcess: csrss.exe Pid: 596
CommandHistory: 0xfcf400 Application: win32dd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x330
```

De esta información podemos recalcar tres puntos. El primero es la llamada al *malware FUto*. Buscando por la red se puede leer que se trata de un *rootkit* que oculta procesos en memoria para dificultar la tarea de un posterior análisis forense. Ello explicaría porque no aparece el proceso en la lista de procesos en ejecución.

A continuación vemos la llamada a la aplicación “nc.exe” y la abertura del puerto 31337 que ya hemos visto relacionado con los puertos abiertos. Lo cual confirma que la máquina está comprometida ya que está a la espera de recibir comandos desde ese puerto.

Finalmente comentar la aparición del archivo “msdirectx.sys” que también está relacionado con el *malware Futo* y la ejecución de “nc.exe”.

Con todos estos datos vamos a intentar extraer el código del ejecutable y del módulo oculto. Para esta tarea contamos con la instrucción `procexedump` que necesita como parámetro el PID del ejecutable, el offset en memoria del mismo y un directorio donde volcar el código. Ejecutamos pues:

```
volatility-2.3.1.standalone.exe –f memoria.dd procexedump –p 408 –o 0x00ae3850 –
dump exedump
```

Obteniendo la siguiente salida:

```
Process(V) ImageBase  Name         Result
---------- ---------- ------------ ------
0xffaf6850 0x00400000 nc.exe        Error: ImageBaseAddress at 0x400000 is paged
```

En este caso no se puede obtener el código del ejecutable ya que se ha paginado la memoria en esas direcciones. Vamos a probar con “msdirectx.sys”. En este caso disponemos de `moddump` que requiere la dirección base y un directorio donde volcar el código. Ejecutamos como sigue:

```
volatility-2.3.1.standalone.exe -f memoria.dd moddump -base=0xfc3b6000 -dump dlldump
```

Obteniendo:

```
Module Base Module Name          Result
----------- -------------------- ------
0x0fc3b6000 UNKNOWN              OK: driver.fc3b6000.sys
```

En este caso sí que podemos obtener el código del módulo. Cabe destacar que nuestro *software* antivirus del equipo donde se desarrolla esta práctica detecta el archivo como potencialmente peligroso y lo elimina inmediatamente para evitar su ejecución.

Así pues, tras toda la información que se ha obtenido con la aplicación *volatility* y tal como se ha ido explicando durante todo el análisis podemos llegar a las siguientes conclusiones.

- Se han ejecutado programas para dificultar la detección de otros programas maliciosos.
- Se ha detectado la presencia de puertos abiertos preparados para ejecutar comandos remotamente.
- Se ha detectado una aplicación oculta esperando peticiones por los puertos anteriores.
- Se ha detectado un módulo potencialmente peligroso y se ha podido extraer su contenido.
- Se concluye que la máquina analizada está actualmente comprometida y que su uso no es seguro.