# Evidencias digitales en la investigación forense informática

Iván Mesías Hidalgo Cajo
Byron Geovanny Hidalgo Cajo
Saul Yasaca Pucuna
Diego Patricio Hidalgo Cajo
Jessica Janeth Aragadbay Ola

ESPOCH
2020

# Evidencias digitales en la investigación forense informática

# Evidencias digitales en la investigación forense informática

Iván Mesías Hidalgo Cajo
Byron Geovanny Hidalgo Cajo
Saul Yasaca Pucuna
Diego Patricio Hidalgo Cajo
Jessica Janeth Aragadbay Ola

DIRECCIÓN DE PUBLICACIONES

**Evidencias digitales en la investigación forense informática**


Panamericana Sur, kilómetro 1 ½
Instituto de Investigaciones
Dirección de Publicaciones Científicas
Riobamba, Ecuador
Teléfono: 593 (03) 2 998-200
Código Postal: EC0600155

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

Corrección y diseño:
La Caracola Editores

Impreso en Ecuador



CDU: 004 + 004.3 + 004.7
Evidencias digitales en la investigación forense informática
Riobamba: Escuela Superior Politécnica de Chimborazo
Dirección de Publicaciones, año 2020
187 pp. vol: 17,6 x 25 cm
ISBN: 978-9942-38-013-5
1. Introducción
2. Artefactos
3. *Framework* forense
4. Herramientas para extracción de la memoria volátil

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# PRÓLOGO

Las evidencias digitales en la investigación forense informática, involucran documentos, ficheros, registros, datos, etc., contenido en un soporte informático y siendo susceptible de tratamiento digital.

Para abordar las evidencias digitales en la investigación forense informática en el presente libro, se trabajó con ejemplos reales y con el software recomendable a utilizarse, ya que las leyes y reglas de administración de justicia sobre informática forense y evidencias digitales son de origen europeo y específicamente en Ecuador no existe ninguna ley ni reglamento para la misma. El texto consta de cuatro capítulos; el primero versará sobre la introducción a la informática forense y examinación de los medios digitales de manera válida, con el propósito de analizar los resultados obtenidos. El segundo hace referencia a los artefactos y es todo aquello que puede obtener una evidencia. El tercero se refiere al framework forense que dispone de utilidades y programas con la finalidad de facilitar la tarea forense, en todos sus aspectos como adquisición,

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

# CAPÍTULO I

## INTRODUCCIÓN

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

### 1.1. Análisis Forense Informático.

Se considera que el Análisis Forense Informático consiste en la aplicación de técnicas científicas y analíticas especializadas a una infraestructura tecnológica que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal (Santos Tello, 2013).

Cuando se requiere de servicios profesionales para ejecutar un análisis forense o peritaje, es prioritario salvaguardar toda la información, que luego será o no judicializada.

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

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

## 1.2. El perito informático

### 1.2.1. Perito

Con la creación del Real Decreto del 17 de agosto de 1901 de Romanones surge una nueva profesión con el título de Perito. Posteriormente aparecen los títulos de perito informático y perito forense (Delgado, 1994). Ejemplo: Si un habitante de una colina es

experto en minerales o simplemente conoce bien la zona, pudiera actuar como perito judicial o forense en el caso de que ocurriera algún problema. No es imprescindible tener una titulación, pero sí experiencia en la actividad que se realiza a diario, aunque evidentemente lo más recomendable sería alcanzar certificaciones o titulaciones que potencien el trabajo que se lleva a cabo.

### 1.2.2. Perito Judicial o Perito Forense

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

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

utilizar todas las técnicas y recursos de una forma científica para una adecuada administración de los requerimientos de su campo laboral (recolección de pruebas, aseguramiento, preservación, manejo de la cadena de custodia necesaria para esclarecer la verdad, etc.).

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

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

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

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

El perito suministra al juez el peritaje u opinión sobre determinadas ramas del conocimiento que el juez no está obligado a dominar, a efecto de suministrarle argumentos o razones para la formación de su convencimiento (Arsuaga Cortázar, 2010).

**Funciones de un perito informático**

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

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

- Asesoría informática y formación de profesionales del derecho, la administración pública, de cuerpos y fuerzas de seguridad del estado, y también como detectives privados.
- Contraespionaje informático.
- Supervisión de actividad laboral informática.
- Detección y asesoría en casos de infidelidad empresarial, que se da cuando un trabajador se separa de una empresa y se lleva consigo información que no le pertenece como, por ejemplo, una base de datos de todos los clientes.
- Seguimiento de correos anónimos, autores de publicaciones, propietarios de páginas web.
- Análisis informático forense de videos, imágenes digitales y audio.
- Asesoría sobre falsificación de correos, imágenes, violaciones de seguridad, infiltraciones, doble contabilidad, fraude financiero y de sistemas informáticos, robo de claves, información sensible, secretos industriales, errores en la cadena de custodia.

Para realizar su labor, el perito debe entender bien la naturaleza del problema, en dependencia del tipo de organización.

Es importante que tenga una formación adecuada porque se han observado casos de mal manejo de la información. Por ejemplo, se puede citar el caso específico de un perito que era electricista, y al realizar un peritaje informático, hizo copias de discos duros con el xCopy, lo que imposibilitó posteriormente la lectura o la copia del informe. Este tipo de inconvenientes son irreversibles.

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

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

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

### 1.3. Forense informático.

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

Se reconoce generalmente a los creadores del Foresis Toolkit, Dan Farmer y Dietes Venema, como los pioneros de la informática forense.

Actualmente, Brian Carrier es probablemente uno de los mayores expertos mundiales en el tema.

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

La norma internacional vigente no se usa mucho, sin embargo, en el caso de España, el analista forense cuenta desde junio de 2013, con la norma UNE (Una Norma Española), en la cual se define claramente cómo se debe realizar, tratar y gestionar un análisis forense de una evidencia digital. Hasta el 2013 se realizaba un procedimiento forense basado únicamente en conocimientos empíricos y sin la seguridad adecuada, lo que podía provocar inconvenientes como que se obtuvieran diferentes tipos de evidencias luego de realizar un mismo procedimiento. Para evitar

estos problemas es muy importante disponer de una metodología, como la norma española (UNE-71506, Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas., 2013)

### 1.4. Evidencia Digital

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

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

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

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo checksums o hash MD5 (Deering, s.f.).

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

- La evidencia digital puede ser duplicada de forma exacta y se puede obtener una copia para ser examinada como si fuera la original. Esto se hace generalmente para no manejar los originales y evitar el riesgo de dañarlos.
- Actualmente, con las herramientas existentes, es muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.

- La evidencia digital es muy difícil de eliminar. Aun cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.
- Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

### 1.4.1. Características de la evidencia digital

La evidencia digital posee las siguientes características:

1. Volátil
2. Anónima

**3.** Duplicable

**4.** Alterable y modificable

**5.** Eliminable

Estas características hacen de la evidencia digital un constante desafío para la identificación y el análisis, que exige al grupo de seguridad y auditoría la capacitación tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia en una escena del delito. Antes de realizar el proceso de análisis forense el equipo de seguridad o auditoría debe considerar los siguientes elementos para mantener la idoneidad del procedimiento forense.

- La evidencia altamente volátil, se versará lo siguiente:

CPU (Registros, Caché), Memoria de Video. Usualmente la información en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de la memoria del sistema.

- La evidencia medianamente volátil, se puede mencionar:

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

- La evidencia poco volátil, se indicará

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

### 1.5. Admisibilidad de la evidencia digital

La evidencia digital (representada en todas las formas de registro magnético u óptico generadas por las organizaciones) debe avanzar hacia una estrategia de formalización que ofrezca un cuerpo

formal de evaluación y análisis que deba ser observado por el ordenamiento judicial de un país. En general, las legislaciones y las instituciones de justicia han fundado sus reflexiones sobre la admisibilidad de la evidencia en cuatro conceptos (Casey, Handbook of Computer Crime lnvestigation, 2001) (IOCE, 2000), que a continuación se detallan:

### 1.5.1. Autenticidad

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

De la misma manera, la autenticidad es entendida como aquella característica que muestra la no alterabilidad de los medios originales y busca confirmar que los registros aportados correspondan a la realidad evidenciada en la fase de identificación y recolección.

En los medios digitales, dada la volatilidad y alta capacidad de manipulación que se presenta en el almacenamiento electrónico. Si bien estas características también son, de alguna manera, inherentes a las vías tradicionales, el detalle se encuentra en que existe una serie de procedimientos asociados con el manejo y control de los mismos en las organizaciones, mientras que para los registros magnéticos aún no se tiene la misma formalidad.

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

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

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

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

### 1.5.2. Confiabilidad

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

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

Asimismo, en el desarrollo de software o diseño de programas es necesario incluir, desde las primeras fases de la creación de aplicaciones, un momento para la configuración de logs o registros de auditoría del sistema ya que, de no hacerlo, se corre el riesgo de perder trazabilidad de las acciones de los usuarios en el sistema y, por tanto, crear un terreno fértil para la ocurrencia de acciones no autorizadas, es decir, se sugiere que la confiabilidad de la evidencia en una arquitectura de cómputo estará en función de la manera como se sincronice la inscripción de las acciones de los usuarios y de un registro centralizado e íntegro de los mismos. Esto reitera la necesidad de un control de integridad de los registros del sistema para mantener su autenticidad.

### 1.5.3. Suficiencia

Es la presencia de toda la evidencia necesaria para adelantar el caso; esta característica, al igual que las anteriores, es factor crítico de éxito en las investigaciones en procesos judiciales. Con frecuencia, la falta de pruebas o insuficiencia de elementos probatorios ocasiona la dilación o terminación de procesos que podrían haberse resuelto. En este sentido, los abogados reconocen que, mientras mayores fuentes de análisis y pruebas se tengan, habrá más posibilidades de avanzar en la defensa o acusación en un proceso judicial.

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

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

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

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

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

Es decir, que la correlación de sucesos (como una función entre la centralización del registro de eventos y el debido control de

integridad de los mismos) se soporta en una sincronización formal de tiempo y eventos que deben estar disponibles por la arquitectura de cómputo para asegurar la suficiencia del análisis de la información presente en una arquitectura de cómputo.

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

Hace referencia a los procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital. Si bien están previstos en el código de procedimiento penal las actividades mínimas requeridas para aportar evidencia a los procesos existen en medios digitales iniciativas internacionales donde se establecen lineamientos de acción y parámetros que cobijan el tratamiento de la evidencia en medios electrónicos, los cuales deben ser revisados y analizados en cada uno de los contextos nacionales para su posible incorporación.

## 1.6. Determinar la relevancia de la evidencia

El estándar en esta fase establece valorar las evidencias de tal manera que se identifiquen las mejores evidencias que permitan

presentar de manera clara y eficaz los elementos que se desean aportar en el proceso y en el juicio que se lleve. El objetivo es que el ente que valore las pruebas aportadas observe en sus análisis y aportes los objetos de prueba más relevantes para el esclarecimiento de los hechos en discusión.

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

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

## 1.7. Herramientas forenses

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

de la aplicación de las mismas, como la formación y conocimiento del equipo de seguridad que las utiliza. Estos dos elementos hacen del uso de las herramientas, una constante reflexión y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas para conocimiento general, que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática.

Si bien las herramientas forenses informáticas son licenciadas y sus precios oscilan entre los 600 y los 5000 euros, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código abierto.

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

## 1.8. Confiablidad de las herramientas forenses en informática

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

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

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

Sin embargo, otra corriente defiende estas herramientas frente a las licenciadas, diciendo que el mundo de código abierto todo está para la investigación de un tercero, que las pruebas se pueden adelantar con mayor confianza que en las abiertas, y que el nivel de confiabilidad es mayor, dado que son muchos "ojos" los que están tratando de mejorarla.

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

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

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

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

# CAPÍTULO II

## ARTEFACTOS

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

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

***Tabla 2.1.*** *Algunos elementos de los Artefactos.*

| **Artefactos** | |
|---|---|
| • Logs o ficheros de sistema | • La papelera |
| • Tabla maestra de archivos MFT | • Metadatos en imágenes |
| • El registro de Windows | • Ficheros de hibernación y memoria |
| • El visor de Eventos | • Copias de seguridad |
| • Los ficheros Prefetch | • Volume Shadow Copies |
| • Los accesos directos | |

***Fuente:*** *http://conexioninversa.blogspot.com/2013/12/artefactos-forenses-i.html*

## 2.1. Shellbags.

Se considera artefacto shellbags, aquellos lugares donde el sistema operativo almacena información relacionada con las preferencias de visualización de contenidos en Windows Explorer, tales como: tamaño de la ventana, posición de ésta en la pantalla, modo de visualización y elementos visibles, por mencionar algunos ejemplos. Si se requiere observar a las shellbags en operación, lo adecuado sería hacer doble clic sobre "Mi PC", cerrar la ventana y volver a abrir. Las preferencias de visualización se han guardado (Hernando, 2011).

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

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

- HKEY_USERS\\Software\Microsoft\Windows\Shell
- HKEY_USERS\\Software\Microsoft\Windows\ShellNoRoam
- Ambas son idénticas en estructura; la única diferencia es que la primera almacena información relacionada con carpetas remotas (roaming) y la segunda custodia información relacionada con contenidos locales (sin roaming).
- Se recomienda utilizar ERUNT para la copia en vivo.

## 2.2. Registros HIVE.

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

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

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

Estos ficheros (Fig. 2.1.) son llamados “hives”.

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

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

***Fig. 2.1.*** *Registry Path Ficheros HIVE.*

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

Cuando se apaga el equipo, los ficheros físicos históricos se localizan en la raíz del sistema operativo (Fig.2.2.).


***Fig. 2.2.*** *El Registro del Computador.*

**HKEY_CLASSES_ROOT:** Es todo lo que está relacionado con el software y el hardware de la máquina.

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

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

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

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

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

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

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

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

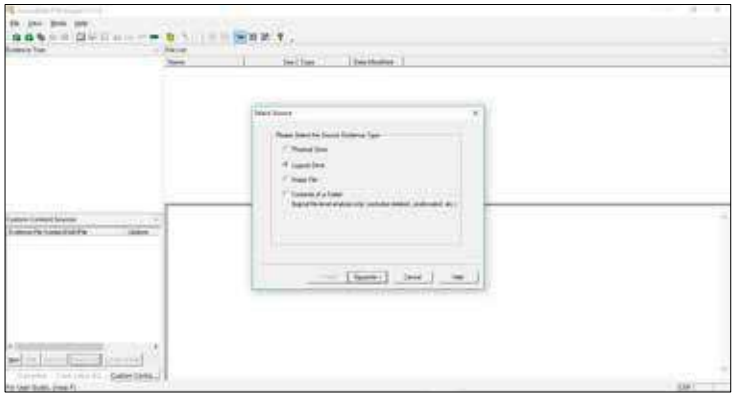


***Fig. 2.3.*** *Access Data FTK Imager.*

En este momento se plantea una interrogante acerca de que se va a realizar con el disco duro, unidad lógica, fichero de imagen o la carpeta, es decir extraer los ficheros *HIVE*. Se elige una unidad lógica ya que se encuentra encendido el equipo y se escoge la

partición C: la agregan; y se procede a buscar la información que se localiza en **C:\Windows\System32\config;** cuando se despliega la pantalla se pulsa el botón derecho y se exportan los archivos a la carpeta donde se requiere copiar; ahora ya se dispone de los HIVE copiados en la carpeta REGISTRO (Fig. 2.4.).

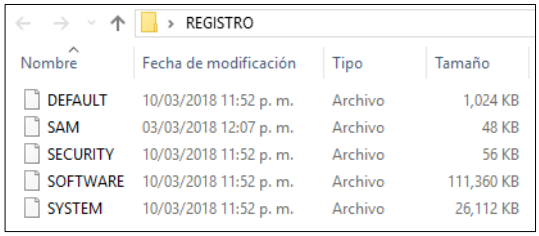



***Fig. 2.4.*** *HIVE copiados en la carpeta REGISTRO.*

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


***Fig. 2.5.*** *Ubicación del lugar de donde se conecta en la Pc.*

*Fuente: http://www.mitec.cz/*

### 2.2.1. Windows Registry Recovery

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

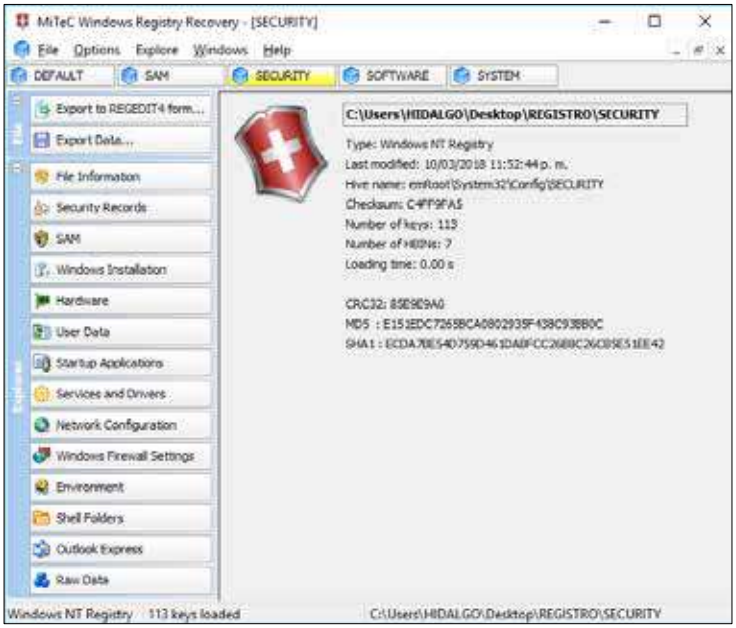



***Fig. 2.6****. Ejecución del Windows Registry Recovery en la carpeta REGISTRO.*

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

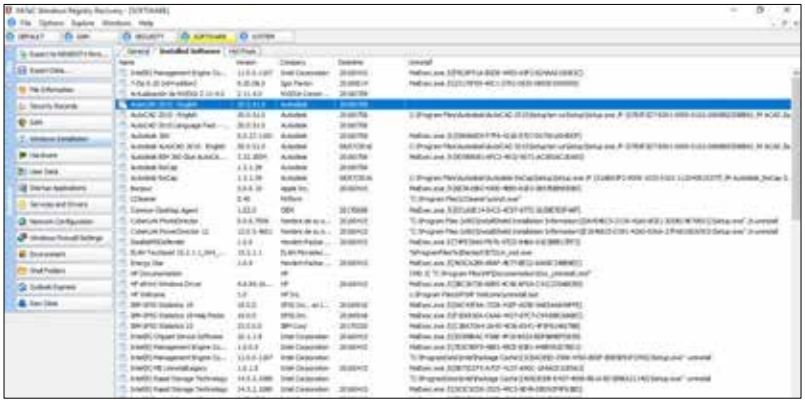


***Fig. 2.7.*** *Instalación de programas en WRR.*

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

En **SYSTEM**, sobre la pestaña Network Configuration se puede observar acerca de TCP/IP; *Windows Firewalls Settings* y se pregunta la configuración de Red; al ubicarse en las pestañas *Hardware*, sobre *DeviceMap*, y *RefreshCurrent* se obtendrá que IPs tenía la máquina, Gateway, DNS; se podrán saber también si tiene Reglas en el Firewall, que reglas tenía editadas, las aplicaciones; además se identificará que hardware estaba utilizando, que unidades y discos

duros poseía en funcionamiento; es decir, si alguien copió la información aquí se identifica el modelo que tenía el dispositivo en la pestaña *Service and Drivers,* en el sistema operativo Windows queda todo el historial de lo que se realiza.

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

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

La cadena HKLM se ubica en:

%SYSTEMROOT%\System32\config\ (%SYSTEMROOT%)

Normalmente referido a:

C:\WINDOWS\HKLM\HARDWARE

Este fichero "hive" es dinámico y se crea en tiempo de ejecución en el inicio del sistema, copiándose en memoria (Russinovich, 1999).

HKU\.DEFAULT corresponde a:

%SYSTEMROOT%\System32\config\default.HKU\SID; normalmente se encuentra en el directorio por defecto del usuario (home directory), en %USERPROFILE%\NTUSER.DAT, y

HKU\SID_CLASSES que corresponde a:

%USERPROFILE%\Local Settings \Application Data\Microsoft\Windows\UsrClass.dat.

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

**HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU**

MRU es la abreviatura de "Most-Recently-Used". Esta clave mantiene los ficheros guardados o abiertos normalmente desde el explorador de ficheros o bien utilizando la caja de abrir o guardar ficheros (por ejemplo, Excel), igualmente se encuentran aquellos ficheros que se abren desde el Internet Explorer.

**HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU**

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

**HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

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

**HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**

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

**HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume**

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

**HKCU \Software\Microsoft\Search Assistant\ACMru**

La clave contiene las búsquedas más recientes del buscador de ficheros de Windows. La subclave 5603 contiene los términos de búsqueda de las carpetas y ficheros, así como la subclave 5604, que contiene palabras y frases que se buscan en los contenidos de ficheros.

**HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist**

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

**HKCU\Software\Microsoft\Internet Explorer**

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

**HKLM \SYSTEM\MountedDevices**

**HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR**

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

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

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

**HKLM\SYSTEM\CurrentControlSet\Services**

Contiene los servicios de la máquina.

**HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID**

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

**HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall**

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

**HKLM\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run**

**HKLM\ SOFTWARE \Microsoft\Windows\CurrentVersion\RunOnce**

**HKLM\ SOFTWARE \Microsoft\Windows\CurrentVersion\RunOnceEx**

**HKLM\ SOFTWARE \Microsoft\Windows\CurrentVersion\RunServices**

**HKLM\ SOFTWARE**

**\Microsoft\Windows\CurrentVersion\RunServicesOnce**

Contiene los "paths" a las aplicaciones que automáticamente se ejecutan durante el inicio del sistema sin intervención del usuario, en esta ubicación están numerosas pistas sobre malware.

**HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon**

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

**HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\GUID**

Contiene la configuración de las redes wifi

**HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU**

**HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**

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

### 2.2.2. RegRipper

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


***Fig. 2.8.*** *Logotipo de la Herramienta RegRipper.*
***Fuente:*** *http://resources.infosecinstitute.com/windows-registry-analysis-regripper-hands-case-study-2/#gref*

Una vez que se ha descargado desde el sitio web donde se obtienen los ficheros ejecutables (.exe), y una serie de ficheros (.pl), al cual *.pl* es el código fuente por si se lo desea reprogramar y mejorar su versión, si no se desea modificar se tiene el ejecutable rr.exe, el rip.exe y el pb.exe que es para la base de datos (Fig. 2.9.).

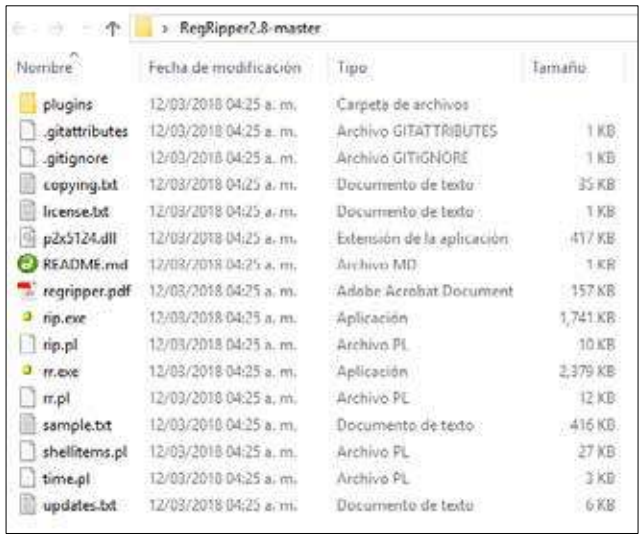



***Fig. 2.9.*** *Herramienta RegRipper.*

En caso de editar el archivo *rr.pl,* se lo puede abrir por ejemplo con la herramienta Notepad++, *rr.pl* contiene el código fuente, donde se observa las llamadas, el menú, los campos, y se obtiene una carpeta muy importante que es los *plugins.*

Los plugins son diferentes programas que permiten parsear los ficheros *HIVE* , por tanto RegRipper va a elegir los ficheros HIVE, parsear y pasará por los plugins, por ejemplo: si se usa el navegador Internet Explorer (ie_main.pl), que tipo de configuración están usando (ie_settings.pl), conexiones a yahoo (yahoo_cu.pl), si se tiene outlook (outlook2.pl), sí disponen de las pstools.pl, se tiene documentación office (officedocs.pl), que tipo de winlogon.pl están realizando, y si se está haciendo bakuprestore.pl, la lista de red networklist_tln.pl. La ejecución del programa es sencilla al presionar sobre el fichero rr.exe (Fig. 2.10.).

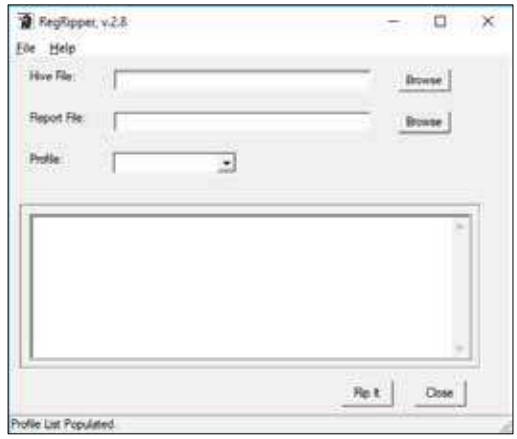



***Fig. 2.10.*** *Ejecución RegRipper sobre "rr.exe".*

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

Al realizar el análisis con el RegRipper se escoge un archivo clonado y se obtiene la información directamente en un fichero .bat.

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


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

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

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

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

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

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

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

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

**Regripper Aplicaciones Instaladas**

**Regripper – Timeline:**

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

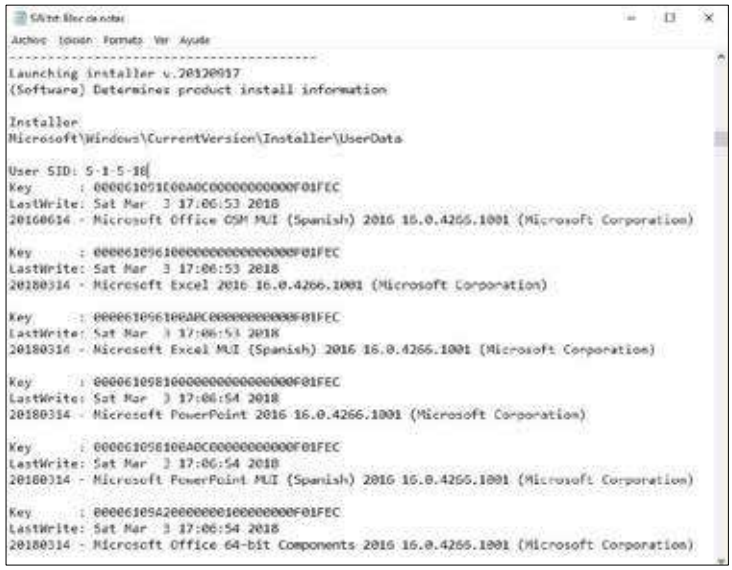



***Fig. 2.12.*** *Regripper – Timeline.*

**Regripper – Redes**

Describe las redes instaladas o configuradas en la máquina, el Gateway y el IP, clave **"Network key"**

**Regripper – USB**

USBs, que se tienen instalados. Esto permite de una forma muy rápida obtener una información relativamente automatizada (Fig. 2.13.).

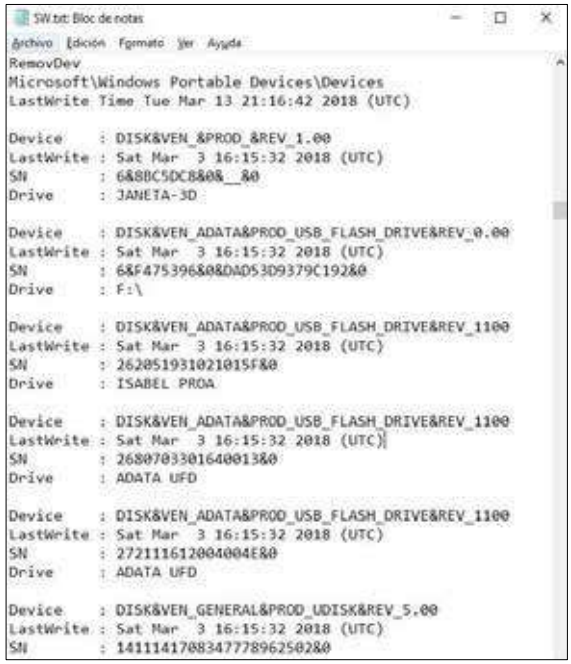



***Fig. 2.13.*** *Regripper – USB.*

### 2.2.3. Bulk Extractor.

(http://digitalcorpora.org/downloads/bulk_extractor/); es la herramienta que va a permitir obtener una gran cantidad de artefactos de forma automatizada, además dispone de una serie de

perfiles montados que permite extraer la información sin mayor conocimiento previo.

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


***Fig. 2.14****. Bulk Extractor.*

Lo que va a permitir que se ejecute una máquina clonada y que se obtenga información de esta.

El comando que se utiliza es:

*bulk_extractor –o*

*C:\Users\HIDALGO\Desktop\REGISTRO –e Facebook outlook –e wordlist C:\Users\HIDALGO\Desktop\REGISTRO\LinuxRedhatRelease.img*

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

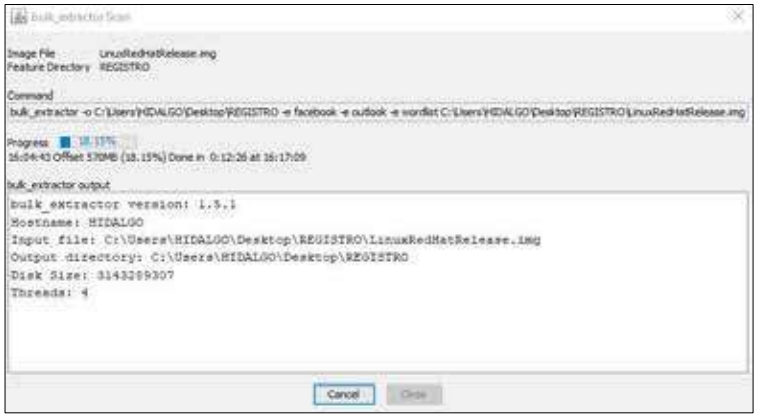



***Fig. 2.15****. Ejecución de una máquina clonada y obtención de información.*

Al ubicarse sobre *Inicio →Programas* y al ejecutar el programa *Bulk Extractor 1.5.5*, seleccione la opción *BEViewer with Bulk Extractor 1.5.5 (64 bit),* visualizara la herramienta en sí en entorno

gráfico. Al acceder a menú *Tools* y pulsar sobre la opción *Runbulk_extractor;* se presentará varias opciones y se escogerá *Image File.*

A continuacion se elegirá la información que se desea extraer: facebook, outlook, wordlist; además se podrá obtener archivos .gps, .gzip, ficheros de correo electronico, contraseña con Aes, ficheros de hibernación hiberfile, ficheros .rar, .pdf, .net, etiquetas de contactos vcard en caso de existir, base de datos en sqlite; proporciona información automatizada y para finalizar se da clic sobre el botón Submit Run (Fig. 2.16.). La extracción de un archivo de tamaño 5 GB tarda aproximadamente 1 hora.


***Fig. 2.16.*** *Run bulk_extractor sobre Image file.*

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

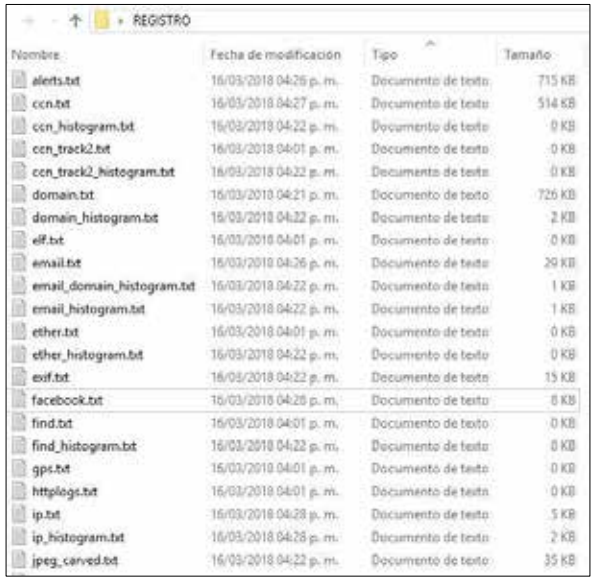



***Fig. 2.17.*** *Extracción de información con Bulk Extractor.*

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

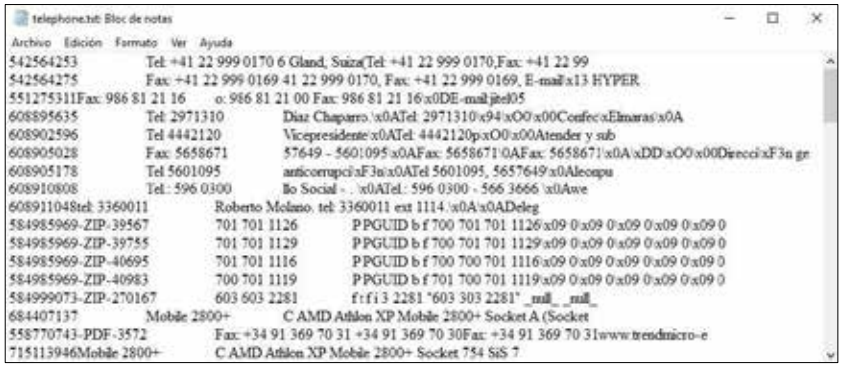



***Fig. 2.18.*** *Extracción de información – números telefónicos con Bulk Extractor.*

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


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

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

### 2.2.4. La papelera

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

***Fig. 2.20.*** *Papelera de Reciclaje.*

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

- Esta carpeta representa el área de la Papelera de Reciclaje; es decir, el contenido de lo que se borra; se puede decir que es un área de almacenamiento donde se guardan archivos y carpetas previas a su eliminación definitiva.

Cada vez que el usuario borra un archivo o tiene al menos un archivo en su papelera de reciclaje, por ejemplo, C:\$Recycle.Bin se crea una carpeta con el SID del usuario. El SID de usuario es el identificador que le pone Windows a un usuario; es decir, si tenemos el usuario Iván, la nomenclatura va a iniciar como S-1-5-21 y una serie de números

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


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

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

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

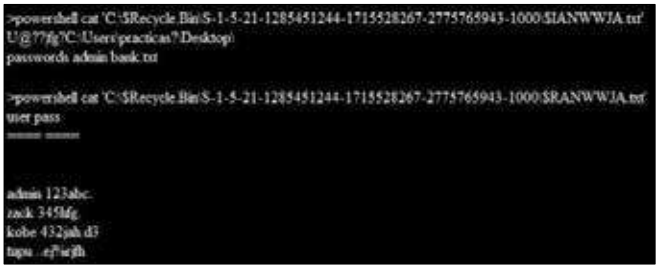



***Fig. 2.22.*** *Papelera de Reciclaje con los $I y $R.*

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

### 2.2.5. RecoverMyFiles

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

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

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

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

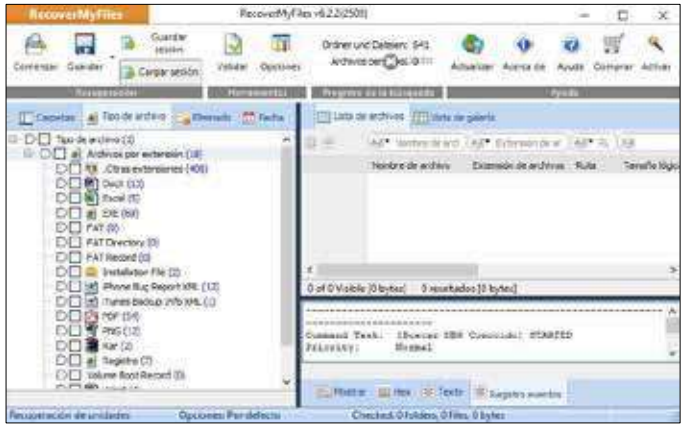



***Fig. 2.23.*** *RecoverMyFiles.*

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

www.conexioninversa.blogspot.com.es/2013/09/forensics-powertools-listado-de.html

### 2.2.6. Prefetch

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

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

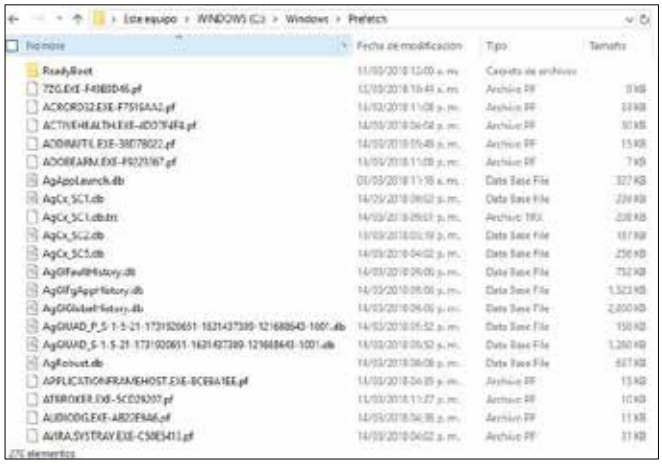


***Fig. 2.24.*** *Registros HIVE del Prefetch.*

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

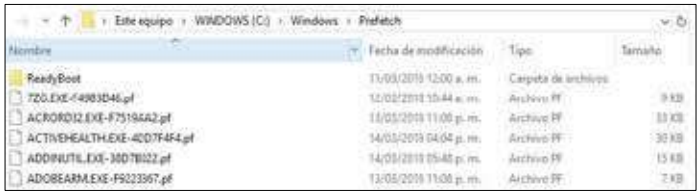



***Fig. 2.25.*** *Archivo Prefetch.*

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

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

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

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

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

### 2.2.7. Winprefetchview

Es una herramienta muy útil: (http://www.nirsoft.net/utils/win_prefetch_view.html), cómoda, sencilla, y se suele emplear en problemas de propiedad intelectual. No necesita de instalación, es un ejecutable; se abre automáticamente el Prefetch, por ejemplo**:** si se contrata el servicio de peritaje o un análisis forense de un ordenador donde se ha instalado el Autocad con la licencia en regla, por tanto el problema es si una máquina tenía instalado un software, lo más fácil es ir al Panel de Control y examinar, o buscar evidencias en el disco duro, como puede ser, un archivo de Autocad o el nombre del ejecutable; pero, lo sería elegir el *Prefetch* abrir y automáticamente, ha extraído

todo la información del Prefetch en la aplicación. En la parte superior izquierda se ilustra una columna con el nombre del archivo marcado con la extensión .7zip, .pf, al seleccionarlo en la parte inferior mostrará una variedad de ficheros que son las librerías y ejecutables que están registrados en esta aplicación; es decir, todos estos ficheros se encuentran registrados dentro del Prefetch, lo que significa que cuando se ejecutó la primera vez un Windows, la instalación es lenta, en Windows 7 y Windows 8. En el proceso de instalación se ilustra el siguiente mensaje "instalando programas"; es decir lo que se está realizando es creando el Prefetch, cuando arranca la máquina y se torna sumamente rápido ejecutando programas como Excel, Power Point o cualquier utilidad de manera eficaz, esto es debido al Prefetch o SuperPrefetch.

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

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

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

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

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

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

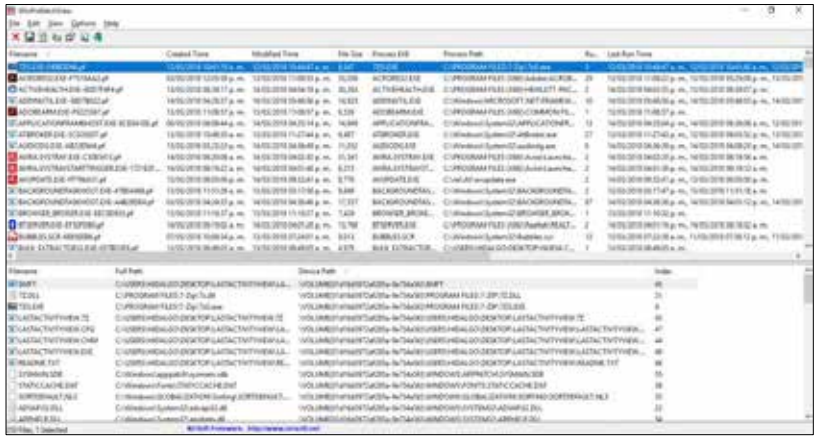


***Fig. 2.26.*** *Herramienta WinPrefetchView.*

En Windows, por defecto cuando un usuario externo coloca un pendrive no se conoce que se copió o revisó, a excepción que este activado el sistema de auditoría (Windows desde sus versiones más antiguas; desde Windows Xp dispone de un sistema de auditoría que permite verificar tanto las aplicaciones como la seguridad, a la vez presenta diferentes escenarios como la ejecución de programas, borrado de ficheros, etc.).

**Ventajas:**

En un entorno empresarial, se recomienda activar el sistema de auditoría, y luego se puede mejorar; es decir, que el sistema de auditoría en un principio va a estar instalado en la máquina, y cuando se tiene una incidencia es uno de los primeros registros que normalmente se suele mirar; pero puede ocurrir que se presente un caso en el que los logs se empiezan a llenar, porque la actividad de usuario es muy amplia, esta situación se podría mejorar ya que es un sistema de log centralizado, en donde los productos que se escriben son registros en el log y automáticamente se están escribiendo en el servidor.

Se permite que el usuario en el caso que borre los registros, automáticamente se obtendrá la evidencia en el servidor, el usuario conseguirá la información referente a lo que ha realizado, permitiendo tener un respaldo ante posibles incidentes; para los registros HIVE y los artefactos, el log es muy importante, por ejemplo: si un gerente de una empresa se cambia a otra empresa, automáticamente lo que haría es llevarse toda la información de la misma directamente en un pendrive.

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

### 2.2.8. USBDeview

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


***Fig. 2.27.*** *Información USB.*

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

Se puede descargar la desde: http://nirsoft.net/utils/usb_devices_view.html y no necesita instalación.

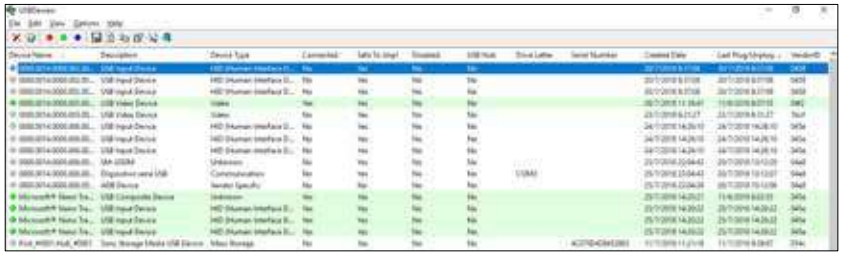


***Fig. 2.28.*** *USBDeview combinado con el visor de eventos de Windows.*

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

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

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

| **Comandos para Habilitar/Deshabilitar/Eliminar para USB** |
|---|
| • /disable {\\RemoteComputer} <Device Name> |
| • /disable_by_serial {\\RemoteComputer} <Device Name> |
| • /disable_by_drive {\\RemoteComputer} <Device Name> |
| • /disable_by_class {\\RemoteComputer} <USB Class;USB SubClass;USB Protocol> |
| • /disable_by_pid {\\RemoteComputer} <VendorID;ProductID> |
| • /disable_all {\\RemoteComputer} |
| • /enable {\\RemoteComputer} <Device Name> |
| • /enable_by_serial {\\RemoteComputer} <Device Name> |
| • /enable_by_drive {\\RemoteComputer} <Device Name> |
| • /enable_by_class {\\RemoteComputer} <USB Class;USB SubClass;USB Protocol> |
| • /enable_by_pid {\\RemoteComputer} <VendorID;ProductID> |
| • /enable_all {\\RemoteComputer} |
| • /disable_enable {\\RemoteComputer} <Device Name> |
| • /disable_enable_by_serial {\\RemoteComputer} <Device Name> |
| • /disable_enable_by_drive {\\RemoteComputer} <Device Name> |
| • /disable_enable_by_class {\\RemoteComputer} <USB Class;USB SubClass;USB Protocol> |
| • /disable_enable_by_pid {\\RemoteComputer} <VendorID;ProductID> |
| • /disable_enable_all {\\RemoteComputer} |
| • /remove {\\RemoteComputer} <Device Name> |
| • /remove_by_serial {\\RemoteComputer} <Device Name> |
| • /remove_by_drive {\\RemoteComputer} <Device Name> |
| • /remove_by_class {\\RemoteComputer} <USB Class;USB SubClass;USB Protocol> |
| • /remove_by_pid {\\RemoteComputer} <VendorID;ProductID> |
| • /remove_all {\\RemoteComputer} |
| • /remove_all_connected - Quita todos los dispositivos USB conectados. |
| • /remove_all_disconnected - Retirar todos los dispositivos USB desconectados. |

***Fuente:*** *http://nirsoft.net/utils/usb_devices_view.html*

**Conectar a un fichero SYSTEM de forma externa**

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

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

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

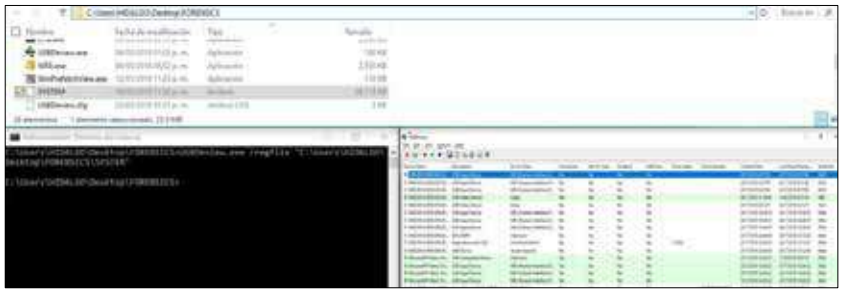


***Fig. 2.29.*** *Conexión a un fichero SYSTEM de forma externa.*

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

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

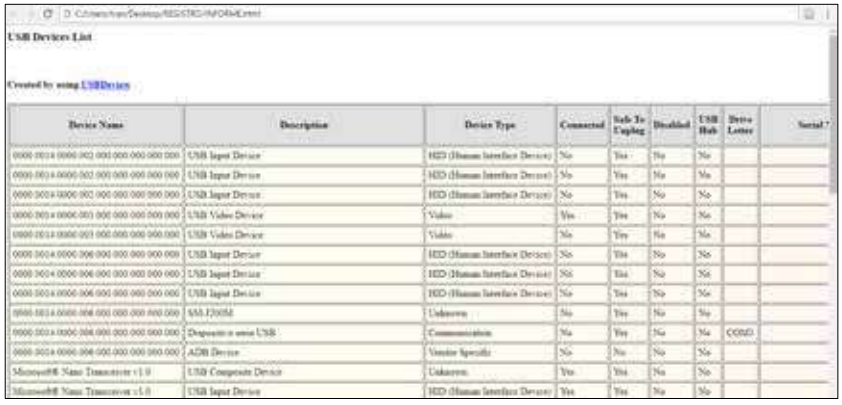
| Comando | Descripción |
|---|---|
| /stext <Filename> | Guarda la lista de todos los dispositivos USB en un archivo de texto normal: |
| /stab <Filename> | Guarda la lista de todos los dispositivos USB en un archivo de texto delimitado por tabuladores |
| /scomma <Filename> | Guarda la lista de todos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

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

***Fuente:*** *http://nirsoft.net/utils/usb_devices_view.html*

Toda la información que se recopiló se puede guardar en una página .html (Fig. 2.30.), y disponer de manera centralizada o en una aplicación web (Fig. 2.31.).

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



USB Devices List

| Device Name | Description | Device Type | Connected | Safe To Unplug | Disabled | USB Hub | Drive Letter | Serial ? |
|---|---|---|---|---|---|---|---|---|
| 0000 001a 0000 002 000 000 000 000 000 | USB Input Device | HID (Human Interface Device) | No | Yes | No | No | | |
| 0000 001a 0000 002 000 000 000 000 000 | USB Input Device | HID (Human Interface Device) | No | Yes | No | No | | |
| 0000 001a 0000 002 000 000 000 000 000 | USB Input Device | HID (Human Interface Device) | No | Yes | No | No | | |
| 0000 001a 0000 003 000 000 000 000 000 | USB Video Device | Video | Yes | Yes | No | No | | |
| 0000 001a 0000 003 000 000 000 000 000 | USB Video Device | Video | No | Yes | No | No | | |
| 0000 001a 0000 006 000 000 000 000 000 | USB Input Device | HID (Human Interface Device) | No | Yes | No | No | | |
| 0000 001a 0000 006 000 000 000 000 000 | USB Input Device | HID (Human Interface Device) | No | Yes | No | No | | |
| 0000 001a 0000 006 000 000 000 000 000 | USB Input Device | HID (Human Interface Device) | No | Yes | No | No | | |
| 0000 001a 0000 008 000 000 000 000 000 | SM-J200M | Unknown | No | Yes | No | No | | |
| 0000 001a 0000 008 000 000 000 000 000 | Dispositivo serie USB | Communication | No | Yes | No | No | COM3 | |
| 0000 001a 0000 008 000 000 000 000 000 | ADB Device | Vendor Specific | No | No | No | No | | |
| Microsoft® Nano Transceiver v1.0 | USB Composite Device | Unknown | Yes | Yes | No | No | | |
| Microsoft® Nano Transceiver v1.0 | USB Input Device | HID (Human Interface Device) | Yes | Yes | No | No | | |

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

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

USBDeview.exe /regfile

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

### 2.2.9. Endpoint Protector

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

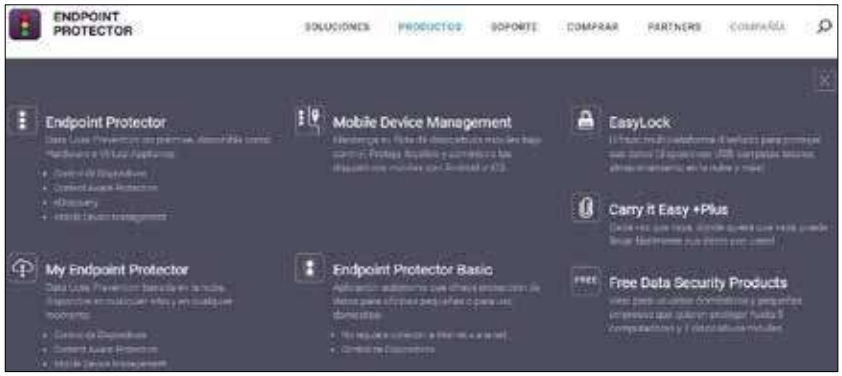



***Fig. 2.32.*** *Herramienta para varios sistemas operativos.*
*Fuente: http://www.endpointprotector.es/*

La herramienta es multiplataforma diseñada para Windows, OSx, Ubuntu, openSUSE, Mac, iOS, Android, prácticamente un 90 a 95% de los sistemas operativos; es decir, dispone de los dispositivos que reconoce usarlo en modo hardware o virtual, y lo protege, *Resourses* → *Data Sheets* (http://www.endpointprotector.com/support/pdf/datasheet/Data_Sheet_Endpoint_Protector_4_CoSoSys_ES.pdf); este es capaz de monitorear (Tabla 2.4.) todos los dispositivos como:

***Tabla 2.4.*** *Monitorización en modo hardware o virtual para los dispositivos.*

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

***Fuente:***
*http://www.ireo.com/fileadmin/docs/documentacion_de_productos/cososys/Datasheet_Endpoint_Protector_4.pdf*

Actualmente existe una variedad de herramientas que brindan seguridad en temas de auditorías para todos los ficheros de una empresa, es cuestión de inversión y que productos prefiera adquirir el administrador.

## 2.3. Artefactos y contraseñas

### 2.3.1. Dialupass

Se lo puede descargar desde: (http://nirsoft.net/utils/dialupass.html), este artefacto permite extraer todas las conexiones de acceso remoto de una máquina, por ejemplo: si un administrador de una empresa ha renunciado y se desconocen las contraseñas, se procede a la caja de herramientas en donde se ejecuta la aplicación y automáticamente en la pantalla se va a exponer el usuario y la contraseña (Fig. 2.33.).


***Fig. 2.33.*** *Artefacto Dialupass.*
***Fuente:*** *http://nirsoft.net/utils/dialupass.html*

### 2.3.2. Network Password Recovery

Se lo puede descargar desde: (http://nirsoft.net/utils/network_password_recovery.html), se pueden obtener las contraseñas de red, las veces necesarias utilizando la herramienta Network Password Recovery que permitirá la recuperación de las contraseñas de red (Fig. 2.34.), siempre y cuando estén almacenadas en el equipo a ejecutar.

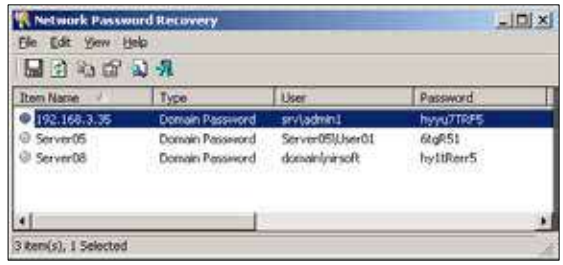



***Fig. 2.34.*** *Artefacto Network Password Recovery.*
***Fuente:*** *http://nirsoft.net/utils/network_password_recovery.html*

### 2.3.3. MessenPass

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

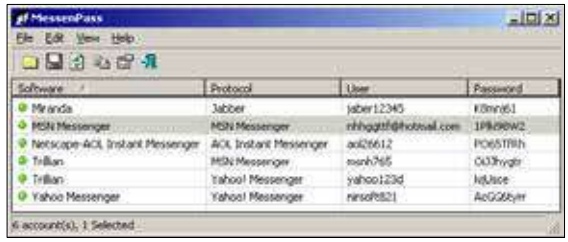



***Fig. 2.35.*** *Artefacto MessenPass.*
***Fuente:*** *http://nirsoft.net/utils/mspass.html*

## 2.4. Navegadores

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

***Fig. 2.36.*** *Navegadores de internet.*

### 2.4.1. Chrome.

***Fig. 2.37.*** *Navegador Chrome.*

### En Linux

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

### En MacOS-X

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

### En Windows XP

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

### En Windows Vista y versiones posteriores

C: \ Users \ % username% \ AppData \ Local \ Google \ Chrome \ Datos de usuarios \ Default \ Preferences

## 2.4.2. iExplore.

***Fig. 2.38.*** *Navegador Internet Explorer.*

**En Windows 95/98, estos archivos estarán ubicados en los siguientes lugares:**

%% Systemdir \ Temporary Internet Files \ Content.IES

% \ Cookies systemdir

%% Systemdir \ Historia \ History.ie5

**En Windows 2000/XP las ubicaciones de los archivos han cambiado:**

%% Systemdir \ Documents and Settings \ % username% \ Local Settings \ Temporary Internet Files \ Content.IES

%% Systemdir \ Documents and Settings \ % username% \ Cookies

%% Systemdir \ Documents and Settings \ % username% \ Configuracion local \ Historia \ history.ie5

**En Windows Vista / 7**

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

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

Internet Explorer igualmente mantiene registros de historial diarios, semanales y mensuales que se encuentran en las carpetas dé %% systemdir \ Documents and Settings \%

### 2.4.3. Firefox.

***Fig. 2.39.*** *Navegador Firefox.*

**En Linux**

/ home/$USER/.mozilla /firefox/$PROFILE.default/places.sqlite

**En MacOS-X**

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

**En Windows XP**

C:\DocumentsandSettings\%USERNAME%\ApplicationData\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite

**En Windows Vista, 7**

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

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

### 2.5.1. WebBrowserPassView

La herramienta: (http://www.nirsoft.net/utils/web_browser_password.html), permite saber dónde se encuentran las rutas y la ubicación para obtener las contraseñas.

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

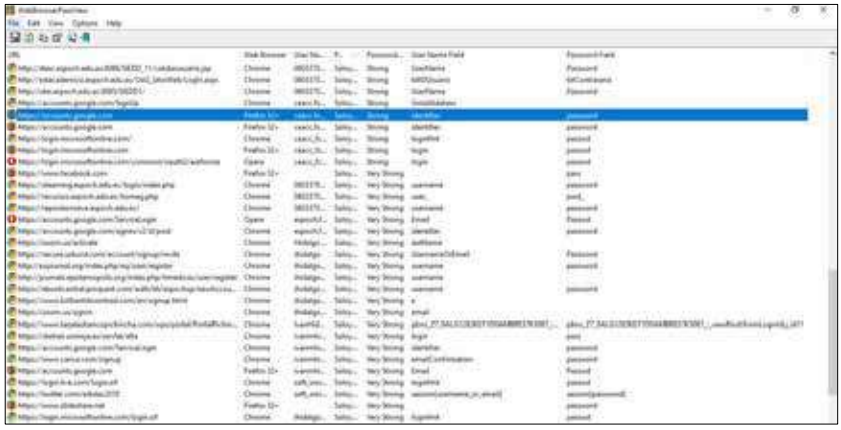


***Fig. 2.40.*** *Herramienta WebBrowserPassView para obtener las contraseñas.*

### 2.5.2. MailPassView

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

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

### 2.5.3. Metadatos

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

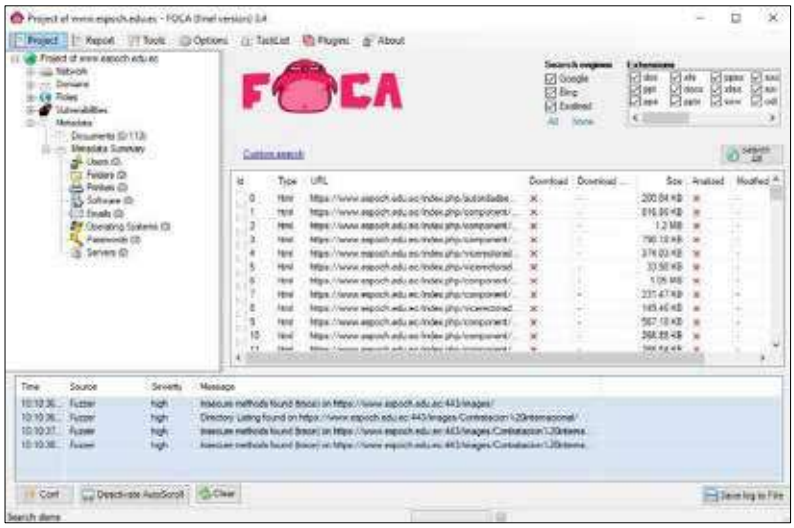



***Fig. 2.42.*** *Herramienta que permite obtener la información de metadatos que está dentro de un archivo.*

Con diferentes utilidades por ejemplo ***FOCA*** (se emplea más para Hacking que para Forense), se podría obtener información de los metadatos de un archivo; es decir, permite obtener un directorio y extraer todos los metadatos de los ficheros como: autor, cuantas

revisiones se han hecho, si ha existido algún tipo de modificación, cuando se hizo la modificación. Foca lo devolverá directamente.

### 2.5.4. Document Metadata Extraction

En el siguiente enlace se ubican varias herramientas (Fig. 2.43.), que extraerán metadatos de archivos:

http://www.forensicswiki.org/wiki/Document_Metadata_Extraction


***Fig. 2.43.*** *Herramienta para obtener los Metadatos.*

### 2.5.5. Accesos directos

Esta herramienta se puede descargar de:

(http://www.mitec.cz/wfa.html), es un conjunto de todas las herramientas que se han visto en el presente libro, por ejemplo: se busca miniaturas de Google, miniaturas de Bases de Datos, el Prefetch, y lo que se va a analizar es Accesos Directos, el

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

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

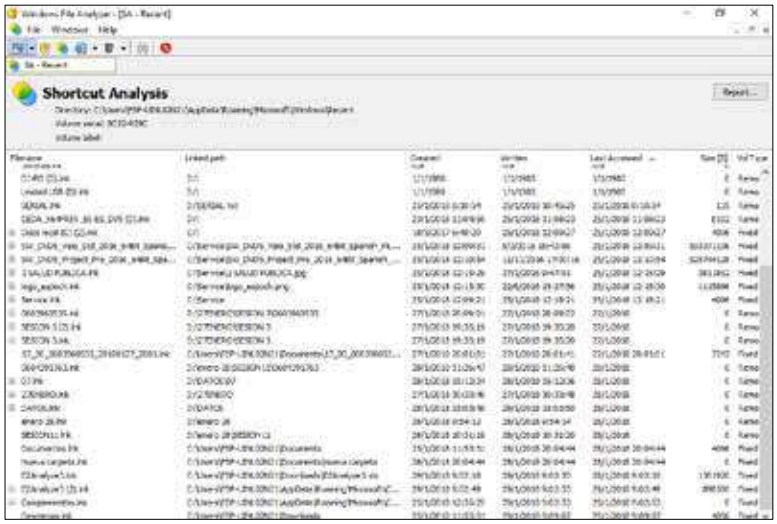



***Fig. 2.44.*** *Herramienta WFA para obtener los accesos directos.*

Un *acceso directo* a una aplicación o a un dato, significa que no tendrá que dirigirse a la ruta del original. Entonces si alguien

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

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

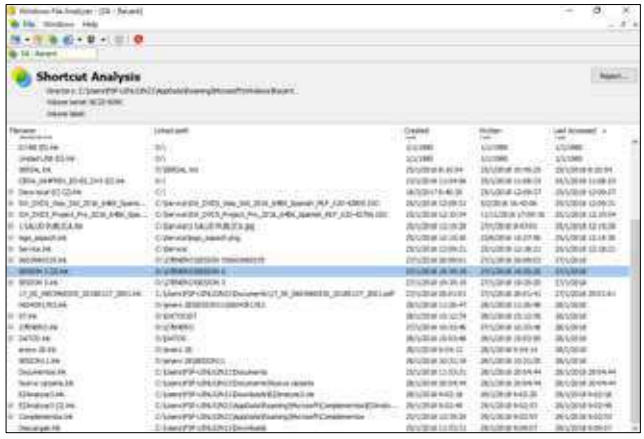



***Fig. 2.45.*** *Ubicación de los accesos directos e información relevante para el análisis de los accesos directos.*

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

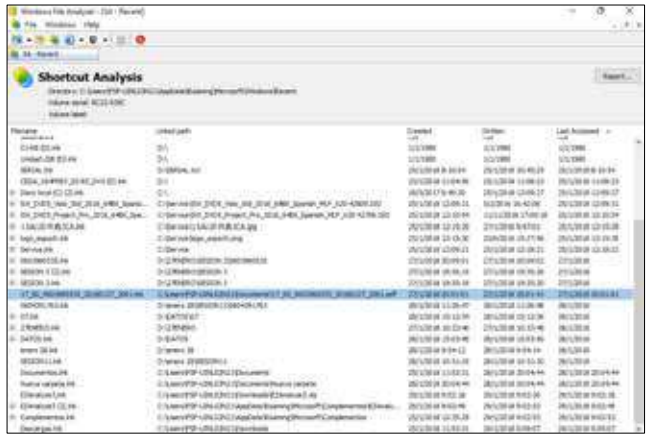



***Fig. 2.46.*** *Ubicación exacta de los archivos utilizando Windows File Analizer.*

### 2.5.6. MiTec E-mail History Browser

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

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

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

Si el usuario no está utilizando el correo, se realiza una extracción en modo lectura, evidentemente se obtiene las cabeceras y se podrá observar: correos, fechas, tamaños que se consigue del historial; es muy importante si se encuentra un tcp y no se desea abrirlo ver las cabeceras y elegir los correos necesarios.

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

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

## 2.6. Creación de un Timeline

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


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

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

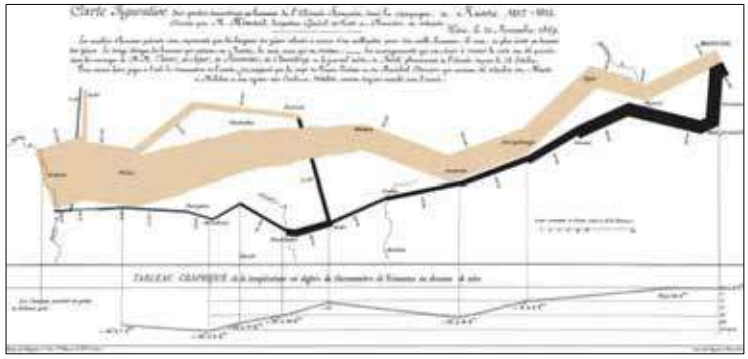


***Fig. 2.50.*** *Carta figurativa utilizaba Napoleón para todas sus batallas.*
***Fuente:***
*https://upload.wikimedia.org/wikipedia/commons/2/29/Minard.png*

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

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

***Fuente:***
*http://oa.upm.es/38772/1/PFC_EDUARDO_RUIZ_AZOFRA_2015.pdf*

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

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

Algunos inconvenientes que se podrán observar son:

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

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

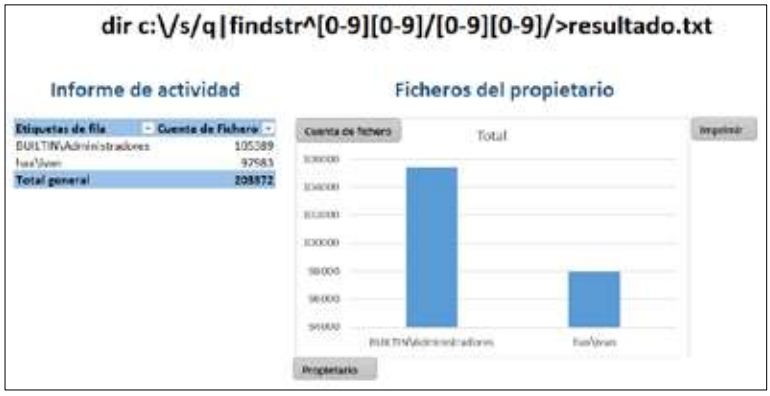



***Fig. 2.52.*** *Listado de un timeline el disco duro de todos los subdirectorios en Excel.*

.

# CAPÍTULO III

## FRAMEWORK FORENSE

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

### 3.1. Digital Forensics Framework

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


***Fig. 3.1.*** *Digital Forensics Framework.*
*Fuente: www.digital-forensic.org*

## 3.2. Xplico

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

Xplico es un framework que permite obtener de un tráfico de red los correos electrónicos que circulan (Fig. 3.3.), una especie de filtrado y en consola gráfico se ilustra el resultado.


***Fig. 3.2.*** *Framework Xplico.*
***Fuente:*** *http://www.xplico.org/*

El resultado al realizar con el framework Xplico se podrá observar la información clasificada de las páginas web, los .html, las imágenes que circulan por la red como videos, audio, ftp, así como

geolocalizarlo (Fig. 3.4.). Se incorpora un script que permite convertir a fichero .kml para ejecutarlo desde networking.

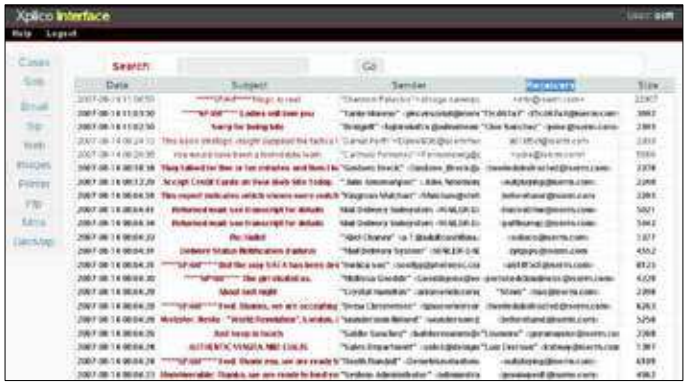



***Fig. 3.3.*** *Interfaz Xplico.*
***Fuente:*** *http://www.xplico.org/wp-content/uploads/2008/11/xwi_emails_list.png*

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

### 3.3. Autopsy

La herramienta Autopsy (www.sleuthkit.org/autopsy/), es una plataforma forense digital e interfaz gráfica de The Sleuth Kit y otras herramientas forenses digitales. Es utilizada por los encargados de hacer cumplir la ley, militares y examinadores corporativos para investigar lo que sucedió en una computadora. Incluso puede usarlo para recuperar fotos de la tarjeta de memoria de su cámara (SleuthKit-Autopsy, 2003), su uso es destinado en el sistema operativo Linux (Fig. 3.5. y Fig. 3.6.).


***Fig. 3.5.*** *Herramienta Autopsy.*


***Fig. 3.6.*** *Análisis con Autopsy.*

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

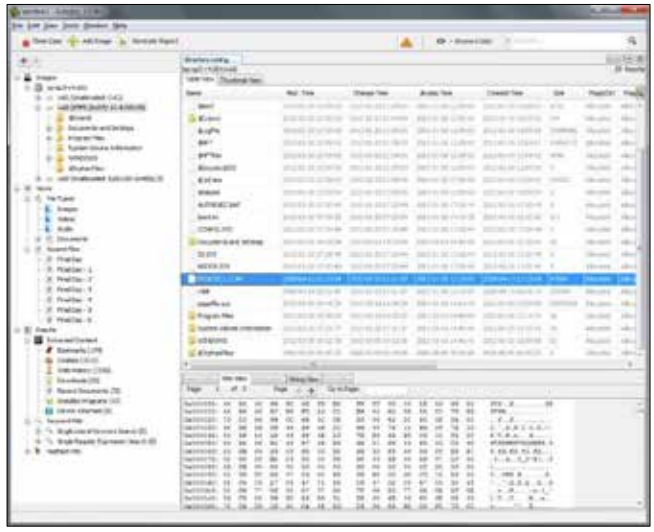


***Fig. 3.7.*** *Autopsy en Windows.*

***Fuente:*** *http://www.sleuthkit.org/autopsy/images/v3/overview.png*

### 3.4. Volatility

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

Las técnicas de extracción se realizan completamente independiente del sistema que está siendo investigado, pero ofrecen visibilidad del estado de ejecución del sistema.


***Fig. 3.8.*** *Volatility.*
*Fuente: http://www.volatilityfoundation.org/*

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

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

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

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

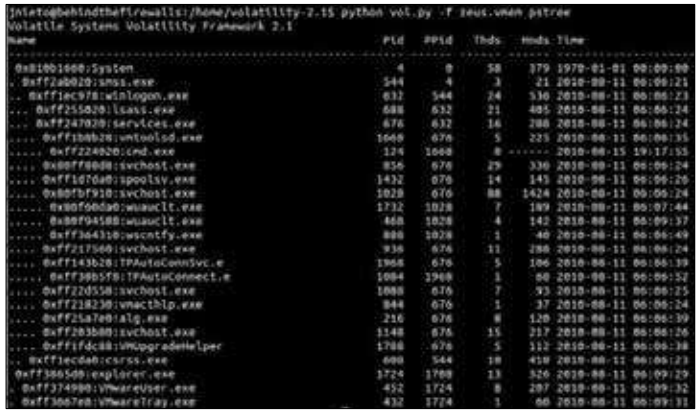



***Fig. 3.10.*** *Ejecución de Volatility.*
***Fuente:*** *Curso de Informàtica forense i evidències digitals, realizada por Pedro Sánchez Cordero, Universitat Rovira i Virgili, Catalunya-España, 2015.*

La información relevante se puede localizar en el siguiente enlace:

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

Entre las características que se pueden extraer están las siguientes:

- Procesos que se estaban ejecutando.
- Tipo de sistema, fecha y hora.
- Puertos abiertos.
- Puertos conectados.
- Claves del registro utilizadas en los procesos.

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

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

### 3.5. ReKall Memory Forensic Framework.-

(www.rekall-forensic.com); es un framework forense de memoria que proporciona una solución integral para los que responden a incidentes y analistas forenses. Desde herramientas de adquisición de vanguardia hasta el framework de análisis de memoria de código abierto más avanzado. Rekall es la única

herramienta de análisis de memoria de código abierto que puede funcionar con el archivo de página de Windows y los archivos asignados (Fig. 3.11.).

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


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

### 3.6. Mimikatz

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

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

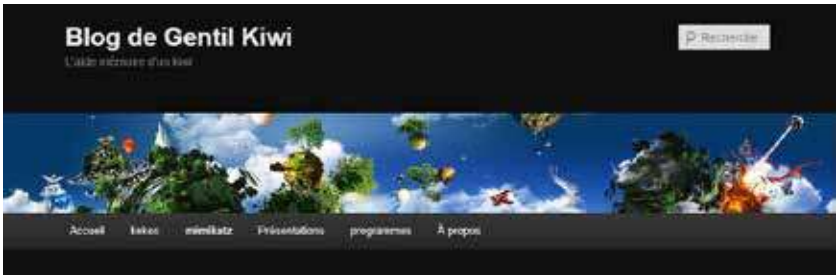



***Fig. 3.12.*** *Mimikatz.*
***Fuente:*** *http://blog.gentilkiwi.com/mimikatz*

### 3.7. NetworkMiner 2.0.-

Una rama de la informática forense se encarga del estudio de las comunicaciones y redes, con el fin de lograr una captura de tráfico, registros y análisis de eventos de red para descubrir el origen de un incidente o ataque o ser utilizado luego como evidencia digital (Paus, 2016). Este análisis puede ser realizado en tiempo real o mediante el análisis de los archivos capturados (.caps). A partir de este estudio se pueden entender características de la red, quien está usándola, identificar picos de tráficos, actividad maliciosa, uso de protocolos inseguros o cualquier comportamiento anómalo.

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

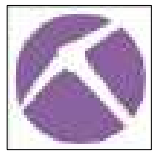


***Fig. 3.13.*** *Logotipo NetworkMiner 2.0.*

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

Si es usuario de Microsoft Windows se puede descargar (https://www.netresec.com/?download=NetworkMiner), y es necesario tener que instalar ".NET Framework 3.5". Esta aplicación se puede ejecutar en Linux, Mac OS X y FreeBSD (welivesecurity, 2016).

**Ejemplo:** Realizar un análisis forense de redes con Wireshark, NetworkMiner 2.0 para analizar un archivo PCAP; como se indica en la Fig. 3.14., se logrará capturar el tráfico de la red (sniffer), se utilizará la herramienta Wireshark.

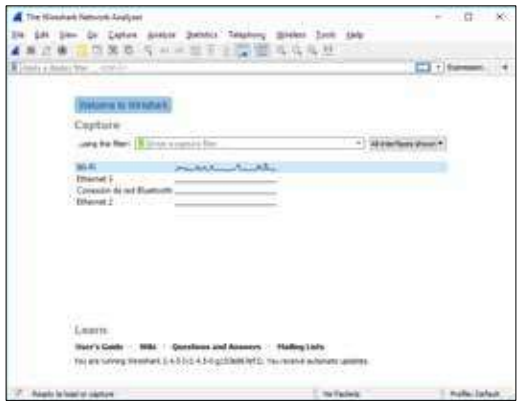


***Fig. 3.14.*** *Herramienta Wireshark.*

Inicialmente, se selecciona la interfaz de red y al dar clic sobre *Start* (Fig. 3.15.).

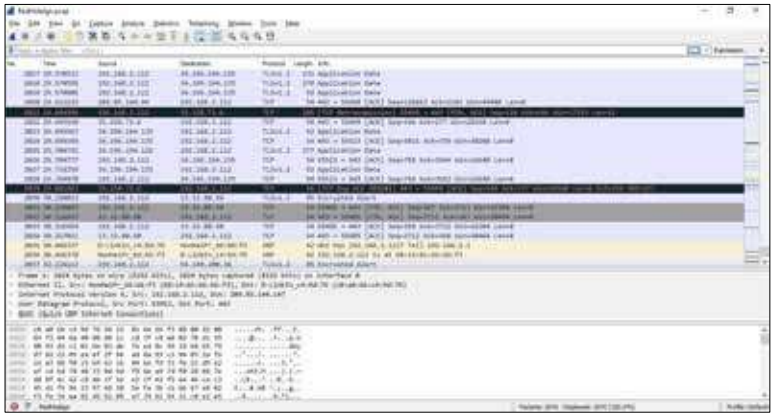


***Fig. 3.15.*** *Herramienta Wireshark en archivo pcap.*

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

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

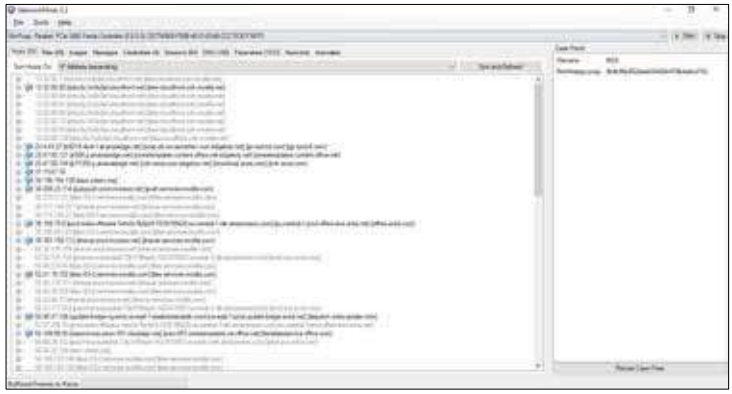


***Fig. 3.16.*** *Herramienta NetworkMiner.*

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

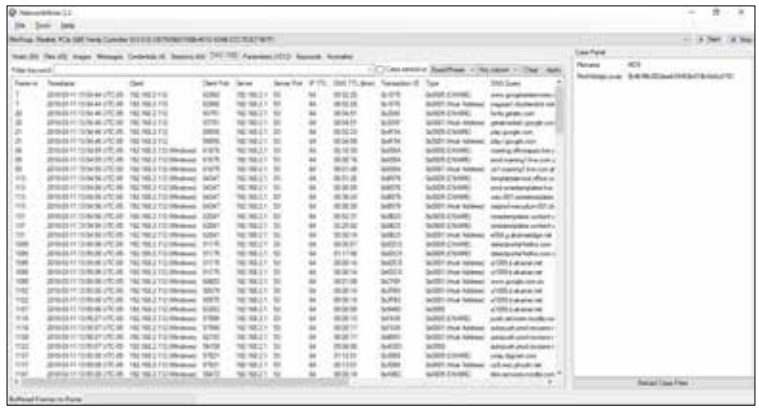


***Fig. 3.17.*** *Análisis DNS en NetworkMiner.*

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

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

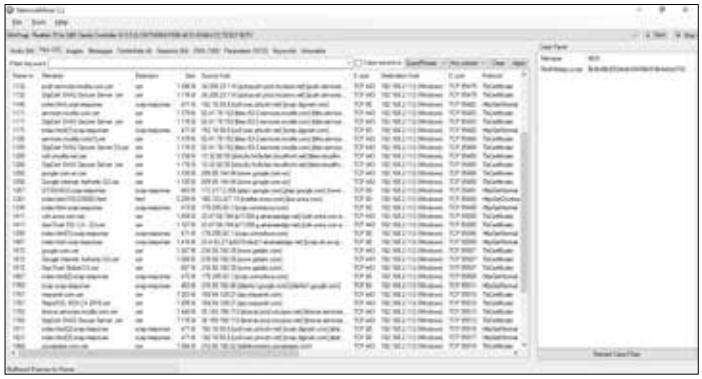


***Fig. 3.18.*** *Análisis Files en NetworkMiner.*

Esta versión también permite encontrar dentro de la solapa parámetros información referida a métodos de petición HTTP,

códigos de estado HTTP de respuesta, cabeceras HTTP y SMB (recursos compartidos), (Fig. 3.19.). Esto podría darnos indicios de una fuga de información o inclusive de algún código malicioso como el ransomware que esté cifrando recursos compartidos.

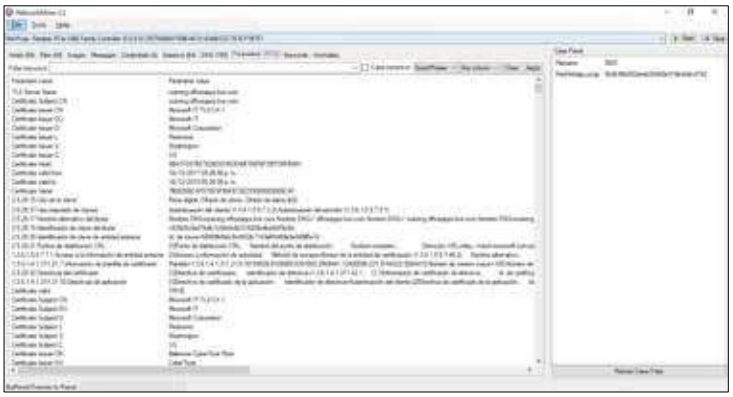


***Fig. 3.19.*** *Análisis parámetros en NetworkMiner.*

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

excelente opción a otras aplicaciones como Wireshark, Bro o Xplico.

# CAPÍTULO IV

## HERRAMIENTAS PARA EXTRACCIÓN DE LA MEMORIA VOLÁTIL

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

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

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

### 4.1. La Memoria

Uno de los problemas más acuciantes para las imágenes de los discos duros de memoria es comprobar que la imagen del disco se ha creado correctamente, es decir el análisis de la memoria puede revelar si los contenidos de la imagen son consistentes con la disposición conocida y la estructura de un sistema operativo determinado.

### 4.2. Técnicas de volcado

Entre las diferentes técnicas de volcado se pueden mencionar:

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

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

## 4.3. Herramientas de volcado de memoria

### 4.3.1. Dumpit

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

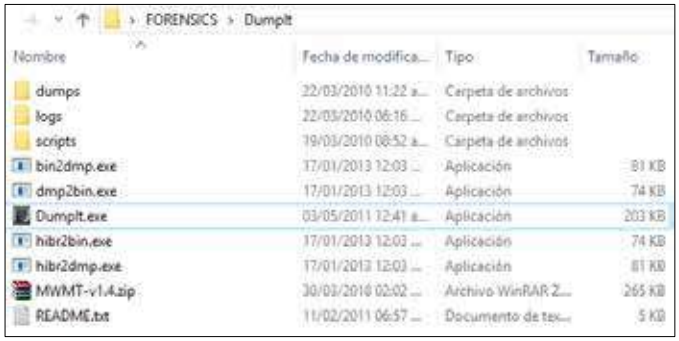



***Fig. 4.1.*** *Herramienta DumpIt.*

Dumpit permite hacer un volcado de la memoria RAM y convertirla en un fichero, luego se parsea para convertirla en algo legible; es decir, primero hace un volcado y lo convierte en archivo (http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/), el volcado de memoria se realizará siempre en un equipo encendido, la memoria tiene una limitación, no es lo mismo 8 GB que 1 Tera (Fig. 4.2.). En la nube se podrá hacer un volcado de memoria, solamente si se tiene un permiso judicial.


***Fig. 4.2.*** *Ejecución de Dumpit.*

Al observar *Destination* es la ruta de donde se ha ejecutado, y donde se ubica HIDALGO-**20180311-070328**.raw (añomesdía – horadelsistema); y si se desea continuar, al pulsar "***y"*** retorna un volcado de memoria. El tamaño del archivo será proporcional a la memoria RAM, pues es un procedimiento para realizar un volcado de memoria. Todo se realiza en modo de comando para lo cual se puede hacer scripting, es decir permite optimizar y obtener el volcado de memoria "HIDALGO-20180311-070328.raw" (Fig. 4.3.).

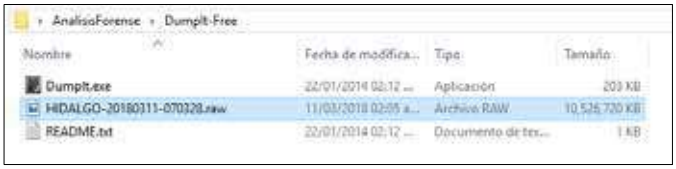



***Fig. 4.3****. Extracción del archivo.raw del volcado de memoria.*

Finalmente se puede observar el volcado de memoria en un archivo HIDALGO-20180330-191924.raw (Fig. 4.4.)

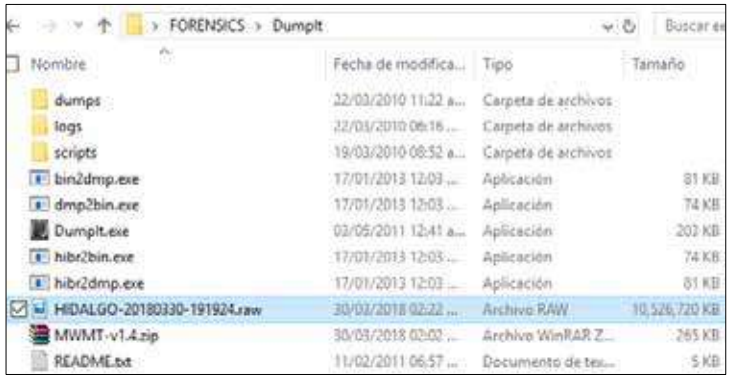



***Fig. 4.4.*** *Volcado de memoria.*

### 4.3.2. RamCapturer

(http://download.cnet.com/Belkasoft-RAM-Capturer-64-bit/3001-2094_4-75946114.html), funciona en modo gráfico y texto, en dónde se va a realizar el volcado (Fig. 4.5.).


***Fig. 4.5.*** *Volcado de memoria con RamCapturer.*

Al reservar un espacio en el disco duro y volcar en ese espacio, algunas veces hace una parada y si lo hace es sobrescribiéndolo,

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

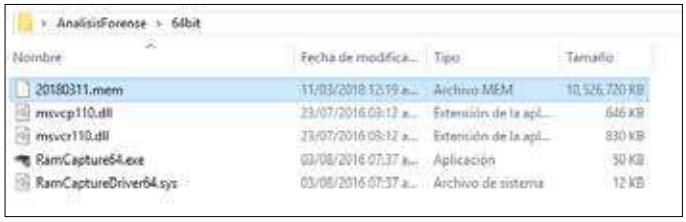



***Fig. 4.6.*** *Fichero de memoria.mem con RamCapturer.*

### 4.3.3. FTK Imager lite

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

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

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

Para prevenir la manipulación accidental o intencional de la evidencia original, FTK Imager realiza una imagen duplicada bit a bit del medio. La imagen forense es idéntica en cualquier forma al original, incluyendo espacio de holgura o residual y espacio sin asignar o espacio libre de la unidad. Esto permite almacenar el medio original en un lugar seguro de daño mientras se procede con la investigación utilizando la imagen forense (ReYDeS, 2018). Se puede descargar desde: http://www.accessdata.com/support/product-downloads, al ejecutar FTK (Fig. 4.7.),

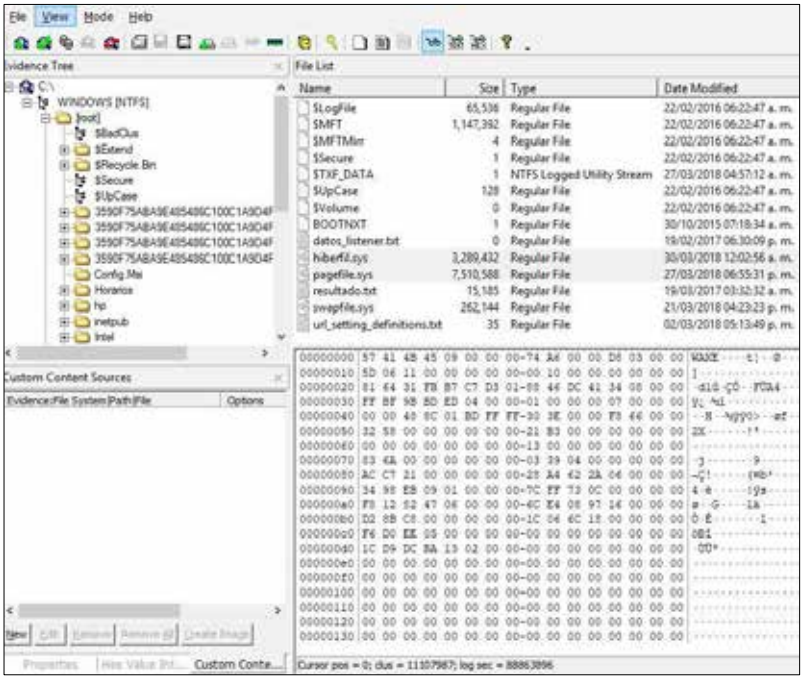



***Fig. 4.7.*** *Herramienta FTK Imager lite.*

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

Todo lo realizado es interesante desde el punto de vista forense; cabe mencionar que cuando la máquina está encendida lo principal es sacar todas las evidencias volátiles y principalmente la

memoria RAM, ante un troyano, o algo externo. Se realiza un volcado de la memoria completo de lo ocupado y lo no ocupado (Fig. 4.8.).


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

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

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

## 4.4. Procesos de Análisis de Memoria

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

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

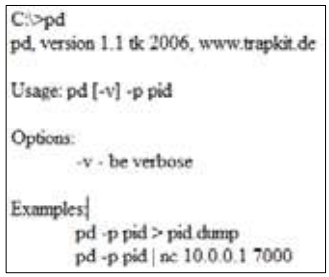



***Fig. 4.9.*** *Proceso de Volcado de memoria usando Trapkit.*

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

Para ello utilizamos la siguiente 'tool': pd, disponible en la web 'http://www.trapkit.de'

Pd es una utilidad que permite extraer de la memoria un determinado proceso basándose en el identificador de proceso (PID) que el sistema le asigna y poder volcarlo a disco. De esta forma no tenemos que 'dumpear' toda la memoria para hacer lo mismo.

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


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

***Fuente:** https://enviamensajes.movistar.es/EnviaMensajes/#*

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

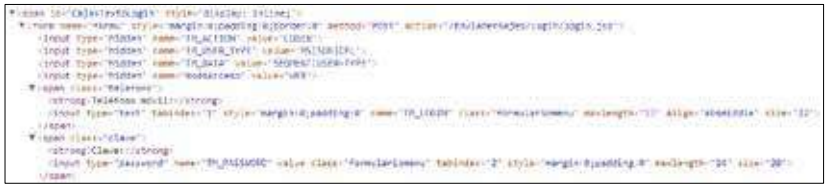


***Fig. 4.11.*** *Código fuente de la página de la web de movistar.*
***Fuente:*** *https://enviamensajes.movistar.es/EnviaMensajes/#*

En el sistema operativo Linux:

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

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

strings -el firefox.dump > memorystrings.txt

Editamos el fichero TXT y buscamos las cadenas anteriormente citadas

Al encontrarse con la cadena TM_LOGIN, lleva asociado un número (deducimos que es un teléfono), mientras que las demás cadenas no muestran nada coherente (Fig. 4.12).


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

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


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

Este procedimiento es idéntico para Windows con la misma herramienta.

## 4.5. Memoria Pagefile

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

El nombre del archivo es **pagefile.sys** y se crea en el momento de la instalación de Windows en la unidad raíz

(normalmente C:\>) donde se encuentra el boot del sistema y sus atributos son ocultos.

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

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

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

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

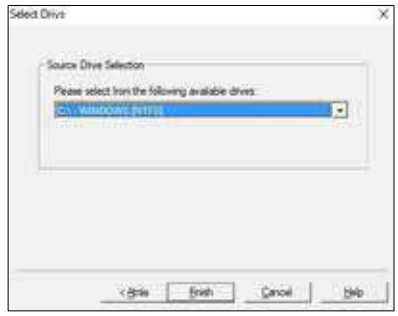



***Fig. 4.14.*** *Obtención fichero de paginación modo encendido.*

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

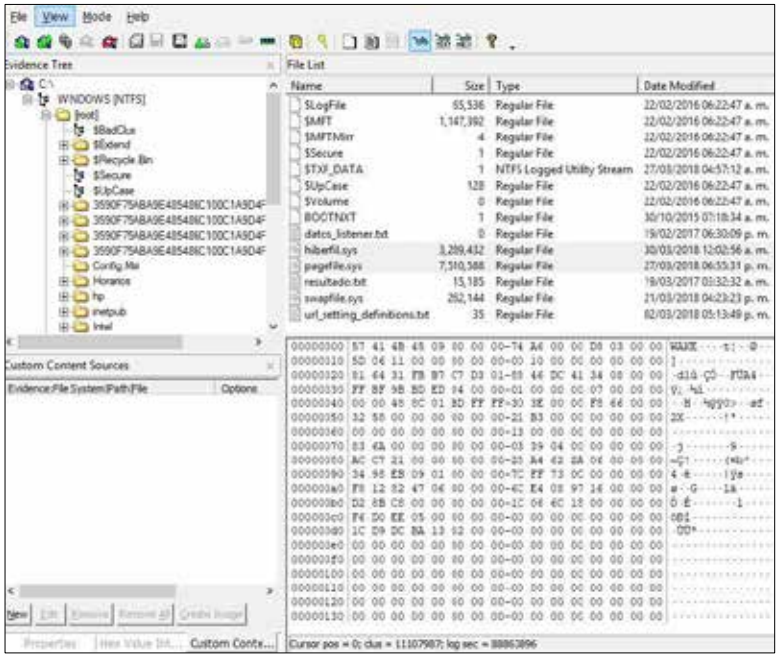



***Fig. 4.15.*** *Ubicación archivo paginación e hibernación.*

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


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

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


***Fig. 4.17.*** *Ubicación del fichero pagefile.sys.*

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

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

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


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

En la Fig. 4.19, disponemos del fichero transformado en texto y se lo puede analizar.


***Fig. 4.19.*** *Fichero de paginación transformado en texto.*

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


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

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

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

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

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

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

***Tabla 4.1.*** *Características del equipo afectado.*

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

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

Las novedades encontradas en la consecución de este delito:

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

Las evidencias digitales adquiridas en la consecución de este delito:

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


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

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

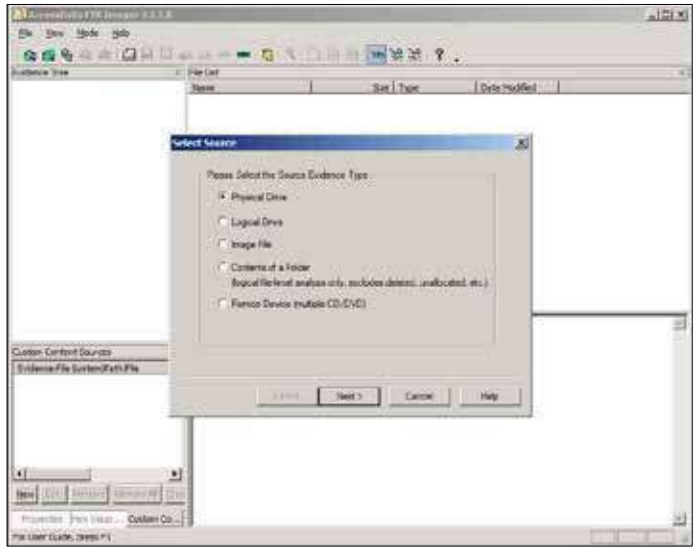


***Fig. 4.22.*** *Copia del disco duro origen con FTK Imager.*

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

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

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

Lo que ilustra el siguiente resultado:

*xchat-2.8.8-0 lun 09 sep 2013 22:10:15 COT*

*sudo-1.6.3p6-1 mar 01 ene 2013 17:00:59 COT*

*stunnel-3.13-3 mar 01 ene 2013 17:00:59 COT*

*strace-4.2.20010119-3 mar 01 ene 2013 17:00:59 COT*

*anonftp-4.0-4 mar 01 ene 2013 16:57:29 COT*

*xinetd-2.1.8.9pre14-6 mar 01 ene 2013 16:57:28 COT*

*zlib-devel-1.1.3-22 mar 01 ene 2013 17:00:59 COT*

*texinfo-4.0-20 mar 01 ene 2013 17:00:59 COT*

*wu-ftpd-2.6.1-16 mar 01 ene 2013 16:57:28 COT*

*kudzu-devel-0.98.10-1 mar 01 ene 2013 16:56:07 COT*

*urw-fonts-2.0-12 mar 01 ene 2013 16:57:28 COT*

*telnet-server-0.17-10 mar 01 ene 2013 16:57:28 COT*

*glibc-common-2.2.2-10 mar 01 ene 2013 16:56:07 COT*

*man-pages-es-0.6a-7 mar 01 ene 2013 16:56:09 COT*

*man-pages-1.35-5 mar 01 ene 2013 16:56:08 COT*

*mailcap-2.1.4-2 mar 01 ene 2013 16:56:07 COT*

*indexhtml-7.1-2 mar 01 ene 2013 16:56:07 COT*

Se puede apreciar la instalación el día 09 de septiembre de 2013 de un software de mensajería instantánea IRC denominado xchat. Lo que trae consigo graves problemas ya que, si no existe otro usuario en el servidor además del root, significa que la persona que

ha instalado el software de IRC lo ha hecho con este usuario y lo más seguro se ha conectado a canales de Chat desde ese perfil. Luego de esta conectado es muy fácil encontrar su dirección ip para otro usuario que este en el mismo canal mediante el comando /whois, el cual se puede ejecutar desde el mismo software XCHAT, sin necesidad de instalar nada adicional.

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

| *Username* | *Failures* | *Maximum* | *Latest* |
|---|---|---|---|
| *root* | *17* | *99* | |

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

*last -20*

*root tty7 Sat Oct 10 06:57 still logged in*

*root tty8 Sat Oct 10 08:26 still logged in*

*root tty7 Sat Oct 10 17:37 still logged in*

*root tty8 Sat Oct 10 22:56 still logged in*

*root tty7 Sat Oct 11 06:57 still logged in*

*root tty8 Sat Oct 11 09:46 still logged in*

*root tty7 Sat Oct 11 12:57 still logged in*

*root tty8 Sat Oct 11 23:02 still logged in*

*root tty7 Sat Oct 12 06:47 still logged in*

*root tty8 Sat Oct 12 17:56 still logged in*

*root tty7 Sat Oct 12 23:07 still logged in*

*root tty8 Sat Oct 13 06:48 still logged in*

*root tty7 Sat Oct 13 23:02 still logged in*

*root tty8 Sat Oct 14 07:46 still logged in*

*root tty7 Sat Oct 14 09.27 still logged in*

*root tty8 Sat Oct 14 12:36 still logged in*

*root tty7 Sat Oct 14 14:37 still logged in*

*root tty8 Sat Oct 14 17:22 still logged in*

*root tty7 Sat Oct 14 20:04 still logged in*

*root tty8 Sat Oct 14 22:51 still logged in*

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

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

*3433 su*

*3435 xchat*

…..

*4041 su*

*4042 xchat*

Se examina el archivo volcado de la memoria RAM del archivo atacado, al analizar con el software WINHEX (**Fig. 4.23**),

se encuentra que en horas de la noche existe navegación a páginas para adultos y de chat (**Fig. 4.24**).

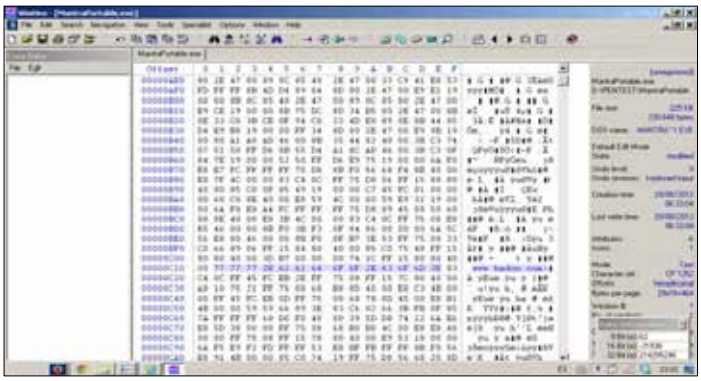


***Fig. 4.23.*** *Análisis de la RAM con el software WINHEX.*

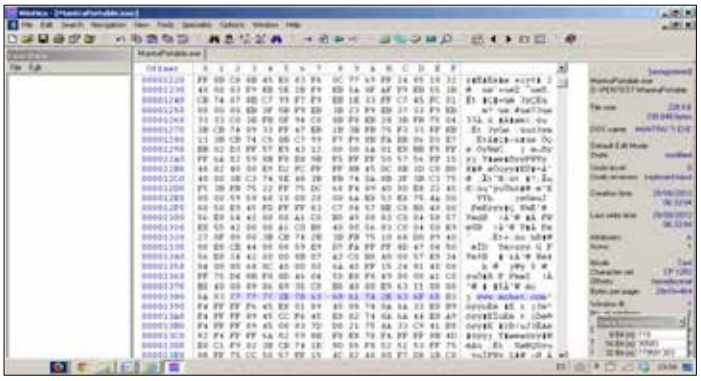


***Fig. 4.24.*** *Información de la RAM con el software WINHEX.*

Se encuentra un pendrive usb conectado al servidor, se analiza y entre otras cosas se ubica un archivo con el nombre

amigoschat.doc, lo llevamos a un equipo con sistema Windows, se trata de abrir con el aplicativo ofimático Microsoft Word y no es posible porque está protegido con contraseña. Se ejecuta el software Passware, que se encarga entre otras cosas de descubrir las contraseñas en archivos ofimáticos protegidos (**Fig. 4.25**).

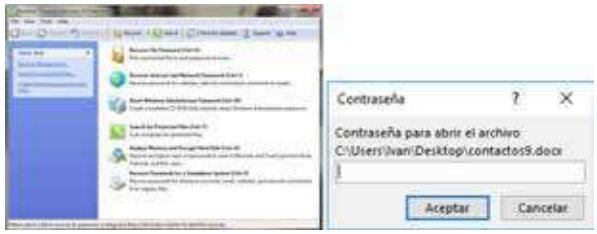



***Fig. 4.25.*** *Análisis software Passware.*

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

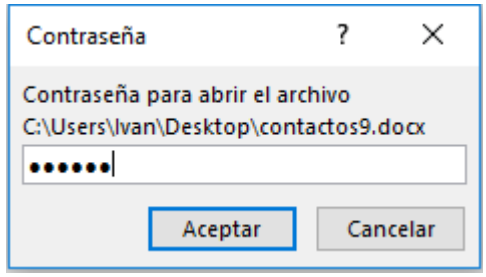



***Fig. 4.26.*** *Extracción contraseña documento Word con Passware.*

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

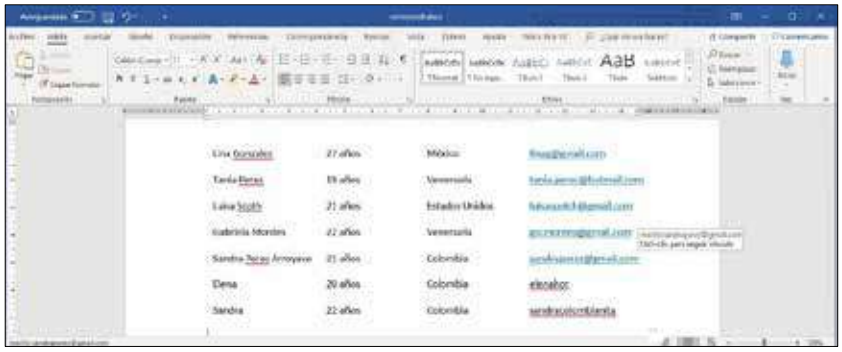


***Fig. 4.27.*** *Archivo Word analizar.*

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

Se le pregunta al usuario afectado si existe la posibilidad de que el vigilante supiera la clave del usuario root del equipo afectado y reconoce que sí, que él se la dio un día para que consultara algo en internet ya que los demás computadores estaban ocupados.

Se ejecuta el software Wireshark y se deja activo toda la noche, para que capture el tráfico que se en la red en esas horas (Fig. 4.28).

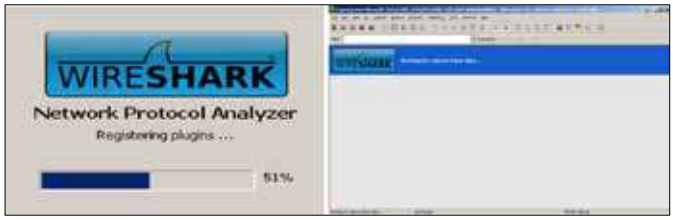



***Fig. 4.28.*** *Ejecución software Wireshark.*

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

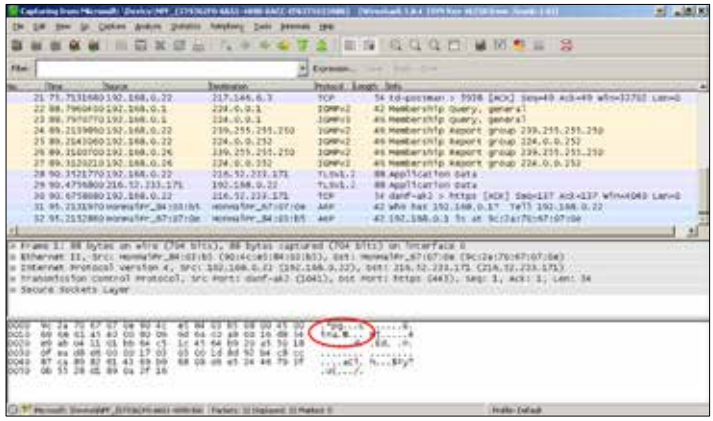


***Fig. 4.29.*** *Análisis disco duro con Wireshark.*

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

# GLOSARIO DE TÉRMINOS

## B

**Bot:** Es un programa informático que efectúa automáticamente tareas repetitivas a través de Internet, cuya realización por parte de una persona sería imposible o muy tediosa. Algunos ejemplos de bots son los rastreadores web de los motores de búsqueda de Internet, que recorren los sitios web de forma automática y recopilan información de los mismos de manera mucho más rápida y efectiva de lo que lo haría una persona.

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

## C

**Clonado:** Proceso de copia, a bajo nivel y firmada digitalmente, de la información original por el cual se traslada ésta a un nuevo soporte de almacenamiento digital, preservando la inalterabilidad de

la información en el sistema o soporte de origen y asegurando la identidad total entre aquella y la extraída.

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

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

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

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

**D**

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

**E**

**ERUNT:** La Utilidad de Recuperación de Emergencia NT, es una utilidad que se puede usar para respaldar y restaurar el Registro de Windows. Esta herramienta tiene la capacidad de realizar una copia de seguridad completa y restaurar el Registro de Windows, incluida la sección de seguridad para que los permisos se respalden y se restauren correctamente.

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

**F**

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

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

**G:**

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

**H**

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

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

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

**I**

**Informática forense:** Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

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

**K**

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

**L**

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

**M**

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

**P**

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

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

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

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

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

**R**

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

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

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

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

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

**S**

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

**Sistema de ficheros:** Organización lógica de un dispositivo.

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

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

**Spam:** Los términos correo basura, correo no solicitado y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido (o incluso correo anónimo o de falso remitente), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de

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

**Swap:** El espacio de intercambio de un disco.

**T**

**Tap de red:** Los TAPs de red (Terminal Access Point por sus siglas en inglés) son el dispositivo de hardware más común a la hora de capturar tráfico de red. Un TAP de red es básicamente un hardware diseñado para acceder al tráfico entre dos nodos de red y reflejarlo en un puerto de monitor donde podemos conectar una herramienta de análisis de terceros para escuchar.

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

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

**Timestamps:** Conocida también como registro de tiempo que es una secuencia de caracteres que denotan la hora y fecha (o alguna de ellas) en la/s que ocurrió determinado evento.

**Trazabilidad:** Capacidad de seguimiento y reconstrucción de acciones efectuadas por los usuarios en un sistema.

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

**V**

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

## GLOSARIO DE SIGLAS

**A**

**ARP:** Address Resolution Protocol

**C**

**CERT:** Community Emergency Response Team

**CD:** Compact Disk

**CMD:** Command prompt

**D**

**DLL:** Dynamic-Link Library

**DNS:** Domain Name System

**DVD:** Digital Versatile Disc

**F**

**FTP:** File Transfer Protocol

**G**

**GB:** Gigabyte

**H**

**HIVE:** Hierarchy of International Vengeance and Extermination

**HKLM:** HKEY_LOCAL_MACHINE

**HKU:** HKEY_USERS

**HTML:** HyperText Markup Language

**HTTP:** Hypertext Transfer Protocol

**I**

**IE:** Internet Explorer

**IP:** Internet Protocol

**M**

**MFT:** Máster File Table

**P**

**PC:** Personal Computer

**Pd:** Process Dumper

**PID:** Identificador de proceso

**R**

**RAM:** Random Access Memory

**S**

**SAM:** Sequential Access Memory

**SID:** Standard Instrumental Departure

**SD:** Secure Digital

**SMB:** Server Message Block

**SMS:** Safety Management System

**SO:** Sistema operativo

**T**

**TAP:** Terminal Access Point

**TCP:** Protocolo de Control de Transmisión

**U**

**URL:** Uniform Resource Locator

**USB:** Universal Serial Bus

**W**

**WWW:** World Wide Web

## BIBLIOGRAFÍA


Arnedo Blanco, P. (2014). *Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos.* Valledupar.

Arsuaga Cortázar, D. J. (2010). *La Prueba Pericial en la Ley de Enjuiciamiento Civil ( Ley 1/2000 ).* Santander.

Casey, E. (2001). *Handbook of Computer Crime Investigation.* Academic Press.

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press.

Copyleft. (2018). *Archivo Pagefile.sys* . Obtenido de https://www.elhacker.net/archivo-pagefile-sys.html

Darknet. (2018). *Hacking Tools, Hacker News & Cyber Security.* Obtenido de https://www.darknet.org.uk/2015/11/rekall-memory-forensic-framework/

Deering, B. (s.f.). *Data Validation Using The Md5 Hash.* Obtenido de http://www.forensics-intl.com/art12.html

Delgado, B. (1994). *La Educación en la España Contemporánea.* Madrid: Morata.

Gervilla Rivas, C. (2014). *Metodología para un Análisis Forense.* Barcelona.

Hernando, S. (11 de Julio de 2011). *Analisis forense de perfiles de usuario en Windows. Introducción a las Shellbags.* Obtenido de http://www.sahw.com/wp/archivos/2011/07/11/analisis-forense-de-perfiles-de-usuario-en-windows-introduccion-a-las-shellbags/

Hidalgo Cajo, I. (2014). *Análisis preliminar y Diseño de una Herramienta de toma de decisiones como soporte para las tareas de Análisis Forense Informático.* Tarragona.

IOCE. (2000). *International Organization of Computer Evidence.* Obtenido de http://www.ioce.org

Navarro Clérigues, J. (2014). *Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico.* Obtenido de http://www.pensamientopenal.com.ar/system/files/2016/05/doctrina43429.pdf

Pato Rodríguez , A. (2006). *Metodología para realizar el manejo de incidentes de seguridad de TI mediante actividades de forénsica digital.* Caracas.

Paus, L. (2 de Marzo de 2016). *Análisis forense de redes con NetworkMiner 2.0 para identificar anomalías*. Obtenido de https://www.welivesecurity.com/la-es/2016/03/02/analisis-forense-de-redes-networkminer/

Quezada, A. C. (05 de Febrero de 2014). *Crear La Imagen Forense Desde Una Unidad Utilizando FTK Imager*. Obtenido de http://www.reydes.com/d/?q=Crear_la_Imagen_Forense_desde_una_Unidad_utilizando_FTK_Imager

ReYDeS, A. C. (2018). *Crear La Imagen Forense Desde Una Unidad Utilizando FTK Imager*. Obtenido de http://www.reydes.com/d/?q=Crear_la_Imagen_Forense_desde_una_Unidad_utilizando_FTK_Imager

Russinovich, M. (1999). Inside The Registry. *ITProWindows*.

Sánchez Cordero, P. (Enero de 2014). *Conexión Inversa*. Obtenido de http://conexioninversa.blogspot.com/2014/01/artefactos-forenses-ii-prefetch-y.html

Sánchez Cordero, P. (2014). Introducción al Análisis Forense Informático. Barcelona, Barcelona, España.

Sánchez Cordero, P. (2015). *Análisis Forense Informático.* Barcelona.

Santos Tello, J. D. (2013). *PROCEDIMIENTOS EN LA INVESTIGACIÓN, RECOLECCIÓN Y MANEJO DE LA EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN*. Huehuetenango.

SleuthKit-Autopsy. (2003). *Open Source Digital Forensics*. Obtenido de https://www.sleuthkit.org/autopsy/

Sofer, N. (2001). *NirSoft*. Obtenido de http://www.nirsoft.net/utils/usb_devices_view.html

Telefónica Móviles España, S. (s.f.). *Movistar*. Obtenido de http://conexioninversa.blogspot.com.es/2008/10/ceregumil-concentrado.html

Tocados Cano, J. (2015). *Metodología para el desarrollo de procedimientos periciales en el ámbito de la informática forense*. La Mancha.

UNE-71506. (2013). *Metodología para el análisis forense de las evidencias electrónicas*. Madrid: AENOR.

UNE-71506. (Julio de 2013). *Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas*. Obtenido de http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414#.Wor0yajOXIU

welivesecurity. (02 de Marzo de 2016). *Análisis forense de redes con NetworkMiner 2.0 para identificar anomalías*. Obtenido de https://www.welivesecurity.com/la-es/2016/03/02/analisis-forense-de-redes-networkminer/

Las evidencias digitales en la investigación forense informática, involucran documentos, ficheros, registros, datos, etc., contenido en un soporte informático y siendo susceptible de tratamiento digital. Para abordar las evidencias digitales en la investigación forense informática en el presente libro, se trabajó con ejemplos reales y con el software recomendable a utilizarse, ya que las leyes y reglas de administración de justicia sobre informática forense y evidencias digitales son de origen europeo y específicamente en Ecuador no existe ninguna ley ni reglamento para la misma. El texto consta de cuatro capítulos; el primero versará sobre la introducción a la informática forense y examinación de los medios digitales de manera válida, con el propósito de analizar los resultados obtenidos. El segundo hace referencia a los artefactos y es todo aquello que puede obtener una evidencia. El tercero se refiere al framework forense que dispone de utilidades y programas con la finalidad de facilitar la tarea forense, en todos sus aspectos como adquisición, preservación y análisis. En el cuarto capítulo, se versará sobre las herramientas para extracción de la memoria volátil y tipos de técnicas para recuperar información.

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

**Byron Geovanny Hidalgo Cajo**, máster universitario en Ingeniería Computacional y Matemática, Universidad Rovira i Virgili, España, magister en Docencia Universitaria e Investigación Educativa, UTPL, Ecuador, diploma superior las Nuevas Tecnologías de la Información y Comunicación y su aplicación en la Práctica Docente Ecuatoriana, UTPL, Ecuador, ingeniero en Computación y Ciencias de la Informática, ESPOJ, Ecuador.

**Saul Yasaca Pucuna**, magíster en Informática Educativa, ESPOCH, Ecuador, ingeniero en Sistemas Informáticos, ESPOCH, Ecuador.

**Diego Patricio Hidalgo Cajo**, magíster en Educación Matemática, UNACH, Ecuador, licenciado en Ciencias de la Educación profesor de Ciencias Exactas, UNACH, Ecuador.

**Jessica Janeth Aragadbay Ola**, abogada de los Tribunales y Juzgados de la República, UNACH, Ecuador, ingeniera en Gestión de Gobiernos Seccionales, ESPOCH, Ecuador.

ISBN: 978-9942-38-013-5