Informática Forense

Iván M. Hidalgo Cajo
Saul Yasaca Pucuna
Luis Á. Lema Ayala
Byron G. Hidalgo Cajo

ESPOCH
2018

INFORMÁTICA FORENSE

INFORMÁTICA FORENSE

Iván Mesias Hidalgo Cajo
Saul Yasaca Pucuna
Luis Ángel Lema Ayala
Byron Geovanny Hidalgo Cajo

DIRECCIÓN DE PUBLICACIONES

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

INFORMÁTICA FORENSE

Panamericana Sur, kilómetro 1 ½
Dirección de Publicaciones Científicas
Riobamba, Ecuador
Teléfono: 593 (3) 2 998200
Código Postal: EC060155

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
Riobamba: Escuela Superior Politécnica de Chimborazo
Dirección de Publicaciones, año 2017
72 pp. vol: 17 x 24 cm
ISBN: 978-9942-35-224-8

1. Informática
2. *Hardware*
3. *Software*
4. Introducción al análisis forense
2. Adquisición, clonación
3. Integridad

CONTENIDO GENERAL

ÍNDICE DE FIGURAS

“La informática forense involucra la recolección, preservación, identificación, extracción, documentación e interpretación de datos informáticos”.

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 sobre la Inteligencia Artificial, Robótica y Visión, desempeñándose en trabajos relacionados en el campo de la seguridad, participa anualmente en los cursos que desarrollan 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 y defensas. Proporciona conferencias a nivel nacional e internacional sobre la cyber-seguridad.

Saul Yasaca Pucuna, Magíster en Informática Educativa, ESPOCH, Ecuador; Ingeniero en Sistemas Informáticos, ESPOCH, Ecuador.

Luis Ángel Lema Ayala, Magíster en Seguridad Telemática, ESPOCH, Ecuador; Ingeniero de Sistemas y Computación, PUCE, Ecuador.

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; Tecnólogo en Informática, ITSPAN, Ecuador; Técnico Superior en Programación de Sistemas, ITSPAN, Ecuador; Tecnólogo en Contabilidad de Costos, Instituto Tecnológico Superior Harvard Comput, Ecuador.

PRÓLOGO

La informática forense involucra la recolección, preservación, identificación, extracción, documentación e interpretación de datos informáticos, y es usada para investigaciones criminales, corporativas o institucionales, evaluación de daños y análisis post-mortem como el fraude, el tráfico de droga, la pornografía infantil, el espionaje, los ataques cibernéticos, la infracción de *copyright*, la recuperación de datos eliminados y la detección de intrusiones con sus mecanismos y técnicas. El análisis forense se refiere a casos en los que se ha producido un delito real en los que la computadora ha sido la víctima.

Para abordar el Análisis Forense Informático, en el presente libro se trabajó con ejemplos reales y con el *software* recomendable para usar en la Unión Europea. El texto consta de tres capítulos: el primero hace referencia a la introducción del Análisis Forense Informático y se dirige a examinar los medios digitales de manera válida, con el propósito de identificar, preservar, analizar y documentar los resultados obtenidos. El segundo se refiere a la adquisición de las evidencias tratando de no alterarlas o dañarlas y a la clonación durante el proceso legal de la informática forense, en la que se mantiene la integridad de la evidencia obtenida y se establece la cadena de custodia. Al tercer capítulo versará sobre la integridad que consiste en disponer de una huella digital única e inequívoca de los dispositivos originales.

CAPÍTULO 1. INTRODUCCIÓN AL ANÁLISIS FORENSE INFORMÁTICO

El Análisis Forense Informático se deriva del peritaje y cabe recalcar que son dos conceptos diferentes. Mediante el peritaje se buscan evidencias, pruebas y se efectúa en base a procedimientos técnicos y científicos que conforman el análisis informático. En la seguridad informática es importante tener en cuenta que la posibilidad de ver ciertos datos no significa necesariamente que esta exista en verdad; de acuerdo con esto, se puede asegurar que toda información puede provenir de muchos otros sitios (Hidalgo Cajo, 2014).

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, podría 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, 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 este, por lo tanto, en la Ley de Enjuiciamiento Criminal, en su artículo 457 se contempla que los peritos judiciales pueden ser o no titulares.

Cuando no hay peritos judiciales se nombran a 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 sub-especialización 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 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 Forensics Toolkit, Dan Farmer y Wietse 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 desa-

rrollo, 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, 2013).

1.4. Metodología para el análisis forense de evidencias digitales

La metodología empleada se basa en el estudio de (Sánchez Cordero, 2014), la misma se desglosa en ocho puntos:

1. **Identificación del incidente**

Cuando se ingresa a una escena del crimen para ejecutar el peritaje correspondiente y se encuentra una persona abatida en el suelo, se procede a identificar valores como: si conserva la ropa en el cuerpo o no, si aún respira, si existe sangre en la escena, o si en la misma se detectan anomalías de otro tipo como cristales rotos.

En el mundo informático el proceder es similar. En el caso de un fraude es necesario observar aspectos como los ordenadores, su tipo, la sala en la que se encuentran y su sistema operativo. Esto permitirá identificar el contexto de la situación dada.

2. **Requisitoria pericial**

Si al contratar los servicios de una empresa se sospecha de un empleado, es obligatorio actuar mediante conceptos legales. No se puede intervenir deliberadamente el ordenador o el dispositivo de una persona y luego acusarla, sino que se debe contar con una serie de garantías procesales. Entonces la requisitoria pe-

ricial incluye todo lo relacionado con las partes judicial y legal. A la hora de hacer un análisis forense hay que hacer cumplir las leyes.

3. Entrevista aclaratoria

Como su nombre lo indica, la entrevista aclaratoria consiste en el encuentro del perito con los personajes involucrados. Con el objetivo de evitar malentendidos, en este paso se dan a conocer varios tipos de conceptos: "quién soy", "qué hago", "cuál es mi código ético". Esta acción debe estar regida por el concepto de imparcialidad, aunque el perito haya sido contratado por una primera o tercera empresa. Por ejemplo, si en los ficheros borrados o eliminados de un ordenador se encuentra pornografía infantil, el perito tiene la obligación de realizar la denuncia respectiva.

¿Qué son los personajes? Se considera así a las personas que actúan o que están dentro del proceso de investigación, ya sean los empleados de los que se sospecha, el representante de los trabajadores o de la empresa. En un mismo proceso de investigación pueden confluir diferentes personajes o escenarios.

4. Inspección ocular

Se aplicaría en la zona donde están los servidores, ordenadores, pero si ya se ha hecho la identificación del incidente, está de más efectuar este paso.

5. Recopilación de evidencias

Si continuamos con la analogía, obtener las evidencias consistiría en algo parecido a lo que se hace en la escena de un crimen: comprobar los valores de la víctima, si está viva o no, si necesita atención. En la informática, se recogen un conjunto de pruebas de la máquina que luego se compararán con una línea base.

6. Preservación de la evidencia

Las cadenas de custodia están enfocadas a la conservación de la información para evitar su manipulación.

7. Análisis de la evidencia

Una vez recopilada y preservada la evidencia, se puede empezar a trabajar con las copias obtenidas anteriormente. Es el momento de realizar el análisis y la exploración de la información, para obtener las conclusiones definitivas que serán presentadas en la documentación y la presentación.

8. Documentación y presentación de los resultados

Los resultados de la investigación se presentarán en dos informes: uno ejecutivo y otro técnico.

1.4.1. Principales puntos de la Metodología de análisis forense digital

Entre los principales puntos de la metodología para el análisis forense de evidencias digitales se pueden destacar los siguientes:

1. **Identificación**

Es muy importante conocer los antecedentes del bien informático, su identificación, su uso dentro de la red, el inicio de la cadena de custodia, el entorno legal que protege al bien y el apoyo para la toma de decisiones con respecto al siguiente paso.

2. **Preservación**

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta que permita mantener la integridad de la evidencia y la cadena de custodia que se requiere.

3. **Análisis**

En este proceso se aplican técnicas científicas y analíticas que permiten ejecutar la indagación sobre cadenas de caracteres, acciones específicas de los usuarios de la máquina como el uso de dispositivos USB (marca, modelo), sitios visitados ,además de la búsqueda de archivos específicos, la recuperación e identificación de correos electrónicos y del caché del navegador de internet.

4. **Presentación**

Es la recopilación de toda la información que se obtuvo a partir del análisis para realizar el informe y la presentación de resultados (Fig. 1.1).

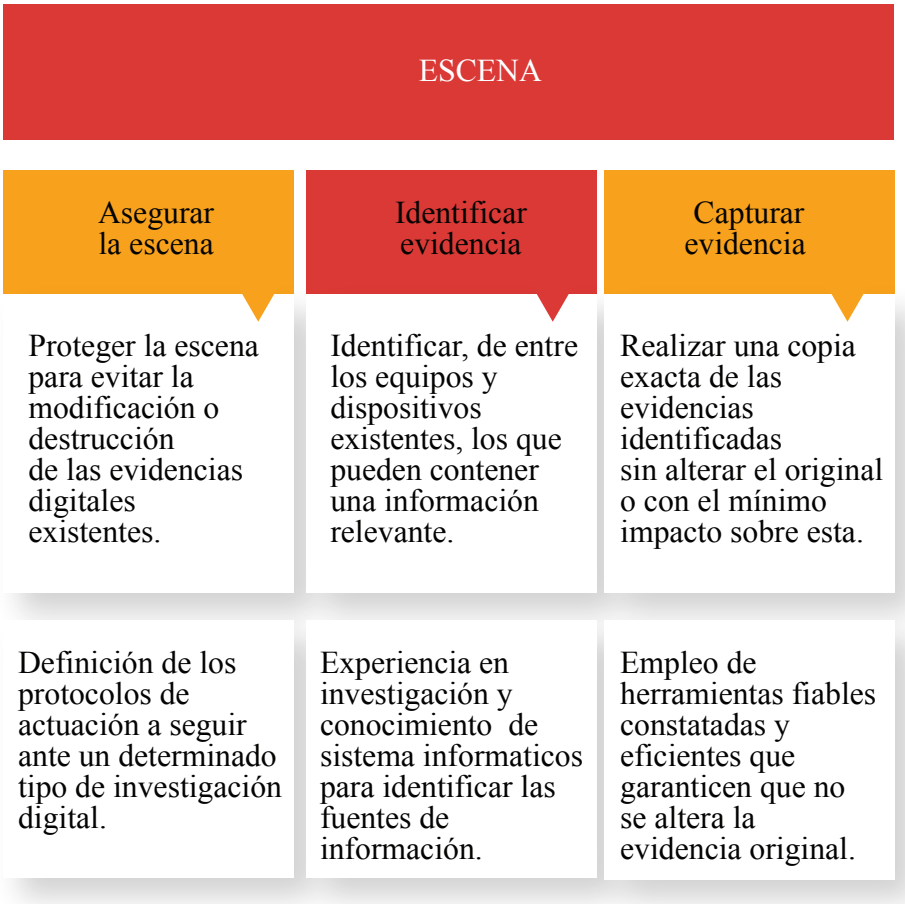

Fig. 1.1. Metodología para el análisis forense de evidencias digitales.

Para fundamentar la Metodología se recurre a Una Norma Europea (UNE-71506, 2013).

CAPÍTULO 2. ADQUISICIÓN, CLONACIÓN

En el presente capítulo se van a definir las herramientas y equipos necesarios para llevar a cabo la investigación en un entorno de trabajo adecuado. En la adquisición de la evidencia se debe garantizar la autenticidad y la originalidad de la misma, además de evitar que sufra alteraciones o daños. En esta fase tan importante del proceso legal de la informática forense se mantiene la integridad de la evidencia obtenida y se establece la cadena de custodia. (Hidalgo Cajo, 2014)

2.1. Adquisición

Si esta primera fase del peritaje se ejecuta de forma errónea, se corre el riesgo de perder el caso.

Cuando una empresa requiere los servicios de un peritaje informático, en la máquina donde se piensa que se ha cometido el fraude, se pueden encontrar diferentes escenarios (Sánchez Cordero, Análisis Forense Informático, Adquisición, Clonación., 2014):

1.Equipo modo encendido:

Esto se entiende como modo *live*. La regla de oro en este caso consiste en no apagarlo si está encendido.

La idea es obtener los datos volátiles del equipo que se analiza; estos son aquellos que persisten en la memoria y que se perderían si se apagara la máquina. Hay cientos de datos volátiles, entre ellos los del sistema operativo. De ellos se puede obtener información sobre las aplicaciones que se estaban usando, sobre la posición de las ventanas, los colores o las veces que se ha ejecutado un determinado programa. Por tanto, apagar el equipo implicaría la invalidación de las pruebas.

¿Qué sería invalidar las pruebas?

En este procedimiento se podrían invalidar las pruebas en dependencia de los comandos que se utilicen y se podrían obtener las evidencias volátiles. Por ejemplo, si se requieren algunos datos de los usuarios se accede a la información que contiene la memoria RAM, pero al ingresar a un programa automáticamente se modifica parte de la estructura de ficheros del sistema en el que se coloca el

programa. Esto supone un problema por la manipulación del fichero o del sistema operativo de origen. Teniendo en cuenta esto, debe ser un procedimiento debidamente documentado y la recolección de datos volátiles normalmente se llevará a cabo utilizando un pendrive externo, como caja de herramientas en la que se colocará toda la información.

2.Equipo Modo Apagado:

Esto se entiende como equipo muerto o modo *sleep*. Extraer el disco duro y clonarlo resulta el modo más recomendado. Aunque de esta forma se pierde todo lo que contenía la memoria RAM en el fichero de paginación. Sin embargo, se puede lograr el acceso a todo lo que estaba en el disco.

3.Virtualización:

Es el modo más recomendable. Actualmente muchas empresas tienen todo virtualizado vía web porque les resulta más cómodo, por lo tanto, se puede clonar la máquina y la memoria RAM. De esta forma se admiten los modos encendido y apagado.

4.Equipo modo nube:

Es conocido como modo cloud, es el más complicado y difícil porque para acceder a una información de una empresa que está en la nube se tiene que hacer con orden judicial. Si se tiene un incidente con una empresa, se le pide a Google que retire los datos y se le entrega la información sobre por qué y en dónde está la orden judicial. Por ejemplo, Amazon cuenta con una herramienta para hacer clonados en dependencia de la compañía o institución que lo requiera. A veces, como en el caso de Google, solo proporciona datos específicos y no el clonado exacto porque es imposible implementar un servidor dedicado a cada persona o empresa. Una base de datos distribuida en cien mil ordenadores ayuda a proporcionar los datos necesarios, pero no a clonar las máquinas. Como consecuencia, se pierde mucha información. Para Microsoft, por orden judicial, normalmente se proporciona una herramienta pagada con anterioridad en función de ejecutar el clonado. Por lo tanto, se infiere que Google es el más afectado porque en otros casos como Amazon y Microsoft pueden usar herramientas que no son baratas, pero al menos se puede contar con ellas.

2.1.1. Adquisición de datos volátiles

Existen algunos comandos del sistema operativo que, al ser ejecutados, permiten obtener información. Por ejemplo, el netcat puede abrir un puerto y direccionar a un fichero de texto. También se puede disponer de otros comandos como el tlis o el netstat. (Tabla 2.1).

Información	Código
Tras establecer el listener en la máquina remota, podemos pasarle información a través de la red desde la máquina sospechosa de haber sido comprometida:	nc –L –p 7777 >\datos_listener.txt
Código:	tlist.exe -c | nc <ip_remota> 7777 -w 5 tlist.exe -t | nc <ip_remota> 7777 -w 5 tlist.exe -s | nc <ip_remota> 7777 -w 5 netstat -naob |nc <ip_remota> 7777 -w 5 tcpvcon -can |nc <ip_remota> 7777 -w 5
Fecha y hora actual del sistema	((date /t)&(time /t))>%DIR%\SystemTime.txt
Uptime de la máquina:	(systeminfo | find “Boot Time”) >%DIR%\ uptime.txt ipconfig /all >%DIR%\ipconfigNICs.txt netstat -rn >%DIR%\TablaEnrutamiento.txt nbtstat -c >%DIR%\CacheNombresNetbios. txt
Árbol de procesos en ejecución (SysInternals): Descubrir DLLs maliciosas cargadas por procesos en ejecución, por ejemplo un keylogger:	pslist -t >%DIR%\ArbolProcesos.txt listdlls >%DIR%\DLLs.txt handle -a >%DIR%\handles.txt

Tabla 2.1. Ejemplo con el netcat y diferentes comandos.
Tomado de: Curso de Informática forense i evidències digitals, realizada por Pedro Sánchez Cordero, Universitat Rovira i Virgili, Catalunya-España, 2015.

Triage (Adquisición de datos volátiles). - Son todos aquellos comandos nativos del sistema operativo o archivos ejecutables disponibles en un dispositivo de almacenamiento externo que se pueden ejecutar en una máquina remota, para obtener toda la información posible de la parte volátil, es decir, con los comandos se accede a determinada información, pero solo el concepto de *triage* es el que permite automatizar.

La Fig. 2.1 representa un *pendrive* que se enchufa a cualquier máquina o se inserta en una red de servidores y automáticamente se tiene acceso a una caja de herramientas que al automatizarse provee la información necesaria. Entonces se pudiera resumir que el *triage* permite:

- Automatizar tareas.
- Utilización de métodos de adquisición mediante scripts.
- Utilizar el lenguaje o los comandos del sistema a analizar. Si es posible se recomienda guardar una copia de los comandos en un USB. (En Windows existen, por ejemplo, los comandos propios cmd y netstat).
- Para usar un USB se debe prever que el mismo disponga de dos particiones, una protegida en modo lectura (la que tendría los comandos), y la otra con los permisos correspondientes de escritura para las evidencias. También es importante tener en cuenta la arquitectura del sistema operativo (computadoras de 32 bits y 64 bits).
- Se requiere tener permisos de administrador.

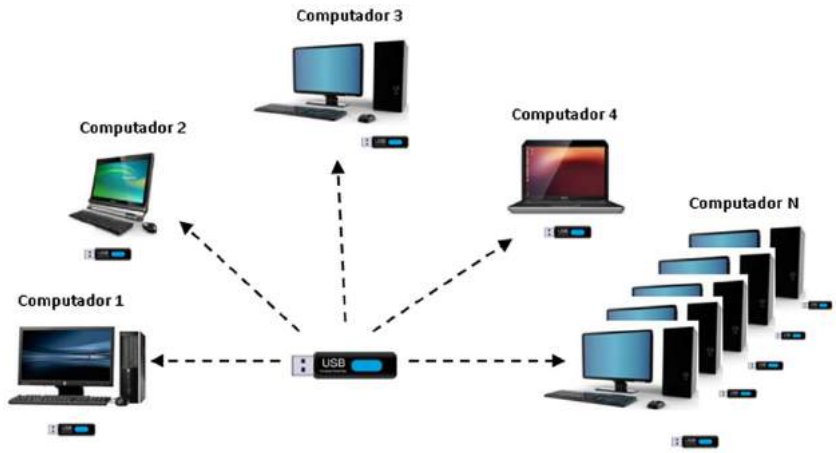

Fig. 2.1. Pendrive en un conjunto de PCs.

- Es importante la utilización de lenguajes nativos del sistema operativo, entre los cuales se encuentran (Fig. 2.2):

  - Windows
    - CDM - BATCH
    - WSH (vba. Js)
    - WMIC
    - POWERSHELL
    - Otros lenguajes muy a la medida como pueden ser (.NET, Java, C#)
  - Linux
    - BASH
    - Perl
    - C
    - Python
    - Otros (Ruby, Java, PHP)

El *triage* incluye todos los comandos del sistema operativo que se pueden automatizar con un lenguaje que permite obtener información.

Fig. 2.2. Lenguajes de programación.
Tomado de: https://www.emaze.com/@ACZRTWOZ/LENGUAJES-DE-PROGRAMACION

Triage en uno o varios equipos. Entre las ventajas que ofrece un *triage* se pueden citar:

- Su efectividad y funcionalidad.
- Capacidad de control ante un problema; por ejemplo, si se lanza un script y este o el cmd se paran, se puede tener el control según la cantidad de máquinas.
- La posibilidad del copy & paste desde diferentes fuentes y la de arreglar el problema en un momento determinado. Si el cmd no funciona, se puede hacer de forma manual.

Las desventajas que puede presentar un *triage* son:

- Un pendrive se hace imprescindible.
- No resulta válido para muchos equipos (redes grandes) porque se tiene que lanzar en un equipo, esperar que acabe y lanzar al siguiente, o tener un clonado de 100 USB y ponerlos en cada máquina, pero eso no quita que se deben tener 100 USB y que se tienen que analizar.
- Es un proceso lento, dependiendo de los sistemas operativos y de lo que está analizando.
- El *script* se actualiza constantemente y si se trata de uno o de dos equipos no pasa nada, pero si son cientos de equipos para usar el *script*, se hace más complicado.

En el ejemplo siguiente (Fig. 2.3) se observa un *scripting* basado en cmd y lo que se hace es lo siguiente:

Se genera un cuadrante de variables del sistema operativo que luego se van a utilizar como las variables de memoria RAM, datos volátiles y datos de disco. Luego se crean las rutas y renombrado la letra, la unidad a limpio donde se quiere que se almacene esta información (W:) que debe ser en un disco externo, lo que facilitará la programación.

La idea es que se pueda advertir que el USB contiene la caja de herramientas. Cuando se inserta se puede comenzar a trabajar en las rutas. En la línea 28 se ejecuta un programa win32dd y se vuelca la memoria RAM a fichero (a fichero o a un fichero, no sería lo mismo). Luego, en la línea 29 se copia una estructura de ficheros que se llama Prefetch para sacar el registro de Windows en memoria registro, responsable de ejecutar comandos que están en el propio pendrive y que a su vez devuelve una serie de ficheros con información. Cabe aclarar que ninguno de estos tres programas son nativos del sistema operativo. En otro bloque se tienen los artefactos (son los diferentes objetos, 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 (Sánchez Cordero, Introducción al Análisis Forense Informático, 2014)); por ejemplo, en la línea 34 se pueden ver con el artefacto la lista de procesos que corre en memoria; en la línea 35, la lista de procesos en uso, la lista de tareas, los procesos mapeados, y los programas pslist, handle, listdlls, netstat, ipconfig, el netstat con diferentes parámetros, el comando net y los arp.

Fig. 2.3. Scripting basado en CMD

En la línea 60 se continúa con el clonado de disco, del cual se va a adquirir y hacer un dd para volcarlo en dependencia de si cabe o no. Para esto se deberá contar con un disco externo de mucha capacidad. Luego, el registro de Windows, el Registry y el RawCopy de la línea 71 a la 75 copian la última configuración buena conocida de Windows. A partir de la línea 79 se ejecutan más parámetros. Si hay tareas, inmediatamente se copian, se hace una consulta a las Querys, y se copia el editor de visor de Windows de la línea 86 a la 91. Se copian todos los *logs*. Por último, en la línea 93 se hace una lista de las políticas del grupo, teniendo en cuenta que se están llevando al sistema operativo cosas que este no lleva, pero que han sido recuperadas de la memoria USB como herramientas para descriptar y poder lanzarlo. A continuación, se muestra un ejemplo de automatización completa de un proceso. (Fig. 2.4).

Fig. 2.4. Automatización completa de un proceso.

Práctica:

Ejecutar el Triage:

"Complete_Windows_Live_Response.bat" que está ubicado dentro del archivo **"Windows_Live_Response.7z"** ubicado en la siguiente dirección web:(https://drive.google.com/file/d/0B9zYUTbcEyHYM2t1Rkp6VjdHcm8/view?usp=sharing), y se obtenga toda la información del computador con la cual se creará una carpeta bajo el nombre del PC involucrado que contenga toda la información de la misma, es decir el volcado de la memoria RAM.

Herramientas forenses gratuitas

Las herramientas forenses gratuitas pueden ser descargadas desde:

- Sysinternals, es un servicio que permite ejecutar herramientas directamente desde la web sin tener que buscarlas y descargarlas manualmente (https://technet.microsoft.com/es-es/sysinternals/bb545021.aspx).
- Las siguientes herramientas están destinadas para las pruebas de seguridad, *hackear* en un entorno de laboratorio, entre otros (http://ntsecurity.nu/toolbox/).
- El sitio web NirSoft ofrece una colección única de utilidades para software que se distribuye de manera gratuita por tiempo ilimitado (http://www.nirsoft.net/).

Triage en una red

Este proceso complejo tiene entre sus ventajas las siguientes:

- Único punto de control.
- Uso de las posibilidades de Active Directory y gestión remota.
- Se llega a toda la red.

Entre las desventajas de un *triage* en red se pueden mencionar las siguientes:

- Analizar demasiadas máquinas es un proceso lento.
- Necesidad de una permanente actualización del script, para poder actualizarlo en todas las máquinas. Evidentemente, si no se cuenta con una red que permita el trabajo en el análisis se complica bastante.
- Más trabajo para el análisis.

Para todo esto se puede usar el WMI (Windows Management Instrumentation) que es la implementación de WBEM (Web-Based Enterprise Management) de Microsoft, una iniciativa que pretende establecer normas estándar para tener acceso y compartir la información de administración a través de la red de una empresa; además, proporciona compatibilidad integrada para el Modelo de Información Común (CIM, Common Information Model), y que describe los objetos existentes en un entorno de administración (Microsoft, 2017). A la hora de hacer un *triage* en una red grande y si se desea obtener información volátil, uno de los principales problemas que aparecen es la definición de qué *software* se va a utilizar. Se puede usar, por ejemplo, el PowerShell, pero como en Windows XP no hay PowerShell, este se debe instalar.

Una de las grandes ventajas de realizar el *triage* es la utilización del WMI, considerando que el mismo es un componente de toda la arquitectura de Windows que responde y que se puede consultar ante cualquier evento del sistema.

En el ejemplo de la Fig. 2.5, aparece en la línea 7 el nombre del ordenador y en las líneas 8 y 9, una consulta, en la que se pide que se indique cuál es el sistema operativo; entonces se puede decir que WMI permite acceder a cualquier información que posea el sistema operativo, como cuánto queda de batería, de CPU, cuáles fueron los últimos picos, que devuelva un registro de Windows, la cantidad de los usuarios que están conectados, del espacio, los procesos que están corriendo.

```
' VARIABLES

Separador="----------------------"
Salida = "" & vbcrlf
Salida2 = "" & vbcrlf
Ordenador = "192.168.1.17"
Consultawmi = "SELECT * FROM Win32_OperatingSystem"
Consultawmi2 = "SELECT * FROM Win32_ComputerSystem"

' CONECTOR

Set Conector = CreateObject("WbemScripting.SWbemLocator")
Set ObjetoWbem = Conector.ConnectServer _
    (Ordenador, "root\cimv2", _
    "administrador", " Hewlett_Packard")

' CONSULTA 1

Set ListaDeProcesos = ObjectWbem.ExecQuery( _
    consultawmi)
For Each ObjetoProceso in ListaDeProcesos
Salida = Salida & ObjetoProceso.csname & "," & ObjetoProceso.caption & "," & ObjetoProceso.BuildNumber
Next


Set ListaDeProcesos2 = ObjetoWbem.ExecQuery( _
    consultawmi2)
For Each ObjetoProceso2 in ListaDeProcesos2
Salida = Salida & ObjetoProceso2.username & vbcrlf
Next

EscribirFichero

' SUB Escribir

Sub EscribirFichero
Dim ObjetoFSO, ObjetoFichero, Escritorio
Set Escritorio = CreateObject("wscript.shell")
Escritorio = Escritorio.specialFolders("desktop")
Set objetoFSO = CreateObject("scripting.filesystemobject")
Set ObjetoFichero = objetoFSO.openTextFILE(Escritorio & "\" & "INFORMACIÓN-SISTEMA-SP.txt", 8, True)
ObjetoFichero.write "IP: " & Ordenador & vbCrLf & Separador & vbCrLf & "INFORMACIÓN: " & vbCrLf & Salida
End sub
```

Fig. 2.5. WMI (I)

En red automáticamente se puede ver toda la información (Fig. 2.6 y Fig. 2.7).

```
On Error Resume Next

'IPInicio = 19
'IPFin = 21
'subred = "192.168.1."

'For i = IPInicio to IPFin
    'strComputer = subred & i
   strComputer = "192.168.1.17"
' ======================================================================
Set objSWbemLocator = CreateObject("WbemScripting.SWbemLocator")
Set objSWbemServices = objSWbemLocator.ConnectServer _
    (strComputer, "root\cimv2", _
    "administrator", "Hewlett_Packard")
Set colProcessList = objSWbemServices.ExecQuery( _
    "Select * from Wim32_Process Where Name = 'cmd.exe'")
For Each objProcess in colProcessList

    CScript.Echo "======================================================================"
    CScript.Echo strComputer
    CScript.Echo "======================================================================"
    CScript.Echo "Nombre proceso: " & objProcess.Name
    CScript.Echo "Titulo: " & objProcess.Caption
    CScript.Echo "Fecha de creación: " & objProcess.CreationDate
    CScript.Echo "Controlador: " & objProcess.Handle
    CScript.Echo "Proceso Padre: " & objProcess.ParentProcessId
    CScript.Echo "ID: " & objProcess.ProcessId

Next

    subWriteToFile
Sub SubWriteToFile
Dim objFSO, objFile, strDeskTop
Set strDeskTop = CreateObject("wscript.shell")
strDesktop = strDesktop.specialFolders("desktop")
Set objFSO = CreateObject("scripting.filesystemobject")
Set objFILE = objFSO.openTextFILE(strDeskTop & "\" & "servicesOUT.txt", 8, True)
objFile.write objProcess & vbcrlf

End sub
```

Fig. 2.6. WMI (II).

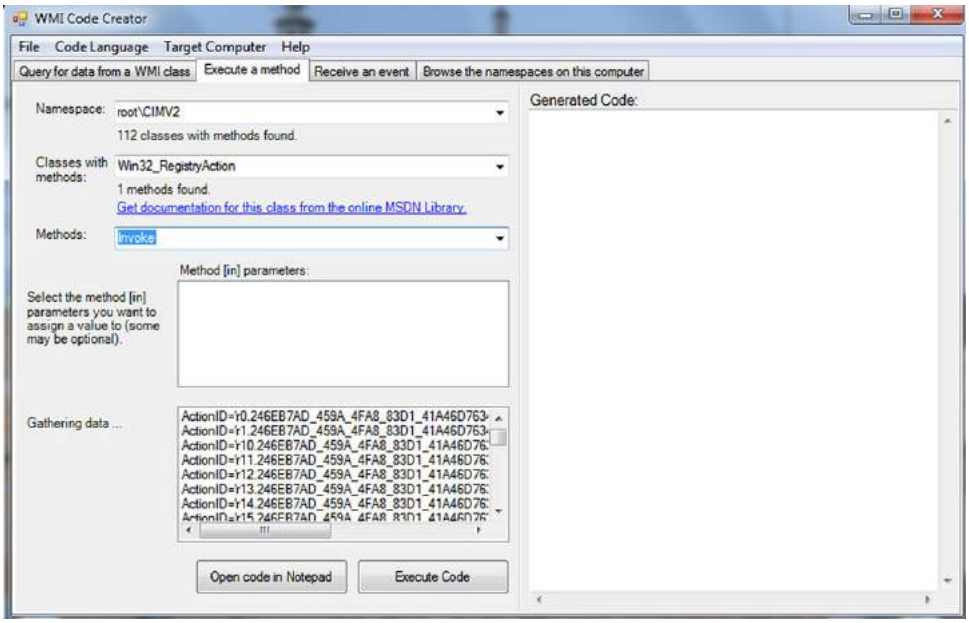

Fig. 2.7. WMI (III)

Tomado de: https://www.google.com.ec/search?tbm=isch&q=wmi+%2B+forensics&spell=1&sa=X&ved=0ahUKEwjfkrPu3o3YAhUD34MKHUoUCjAQvwUIIigA&biw=1517&bih=685&dpr=0.9#imgrc=BZ7JPzxLyqw7RM:

2.2. Clonación

Si la máquina está encendida, se coloca un *pendrive* y se ejecutan las herramientas para realizar una extracción. Una vez que esta se ha realizado se vuelcan los procesos a la memoria, es decir, los parámetros que son importantes y que luego se analizarán. Al tirar del cable que alimenta de energía al ordenador, se apaga el equipo de una forma diferente y no ordenada, pues de lo contrario un *hacker* o algún proceso raro podrían causar daño y borrar datos importantes del ordenador. En este caso es muy oportuno el siguiente axioma: si la máquina está encendida no se debe apagar hasta que se recojan las evidencias, y si está apagada lo conveniente es no encenderla.

Cuando ya se han recogido las evidencias y después de desconectar el cable quedará el fichero de paginación, ficheros abiertos, temporales y todo eso va devolver información, por lo tanto, al culminar esta acción ya se podría hacer el clonado.

2.2.1. Clonación de discos

El clonado es muy importante dentro del proceso de adquisición, porque sin él no se podría obtener casi nada.

Consiste en la copia exacta "bit a bit" de un disco, incluyendo errores o sectores defectuosos. Es importante recordar que si se toma una aplicación, el comando xCopy no sería válido porque es capaz de copiar los datos, pero no copia ningún sector del disco; o sea, hay formatos que se pueden guardar en determinados sectores del disco, lo que hace posible la utilización de algunos sectores del mismo que en principio no haya sido utilizado. Un xCopy no lo detectaría; mientras que el Clonezilla que es un programa de *software* libre, usado para la clonación de discos y particiones (Clonezila, 2018), tampoco lo notaría. Se tendrá que usar la opción de modo avanzado para que pueda clonar bit a bit.

Tipos de clonados

Existen múltiples formas y herramientas:

Por software:

- DD
- Live CD
- OSForensics
- EnCase

Por hardware

- Clonadoras

Fig. 2.8. Clonación de discos por *software*.
Tomado de: https://qloudea.com/blog/clonar-disco-duro/

Se puede clonar por medio del comando típico de Linux "dd", que permite realizar una copia bit a bit, luego desconectar el cable, abrir el ordenador, sacar el disco duro y hacer un clonado a otro disco de igual tamaño (Fig. 2.8). No es imprescindible que sea del mismo modelo ni de la misma marca, pero sí de idéntico tamaño. Por ejemplo, si se cuenta con un tera, el resultado de la copia deberá ser igualmente de un tera.

Es importante tener en cuenta los siguientes detalles:

El disco A y el disco B, en el cual se copiará el primero, deben estar conectados a la PC de la siguiente manera:

El disco A será el máster (maestro o principal) mientras que el B funcionará como *slave* (esclavo o secundario), de manera que el disco A quedará como hda o sda y el B como hdb o sdb; el hdX se utiliza para discos IDE donde X indica el orden de estos. Lógicamente, el hda está primero que el hdb, lo mismo para con sdX, ya que el sd se utiliza para discos SATA y USB, y X al igual que hd se utiliza para indicar cuál es *master*, maestro o primario, y *slave*, esclavo o secundario.

Para saber cuál es primario o el orden de los discos se escribe el siguiente comando:

- df –h

Para copiar:

- dd if=[disco_duro_origen] of=[disco_duro_destino]
- dd if=/dev/hda of=/dev/hdb bs=1M; con esto se clonaría el disco hda en hdb. (discos IDE).
- dd if=/dev/sda of=/dev/sdb bs=1M para discos (discos SATA).

LIVE CD's

Contienen todo el sistema operativo necesario para arrancar y ejecutar programas de adquisición de datos y clonado de discos (Fig. 2.9); se debe arrancar desde el Live CD o desde la USB donde se encuentre el sistema operativo.

Fig. 2.9. Clonado de discos por *software*
Tomado de: http://informaticaforenseviviana.blogspot.com/2015/05/herramientas-de-informatica-forense2.html

Entre los diferentes *software* se tienen los siguientes:

CAINE (http://www.caine-live.net/). Viene con una gran variedad de herramientas con un entorno gráfico y muy fácil de utilizar, sobre todo los que vienen habituados del mundo Windows. Para trabajar con él no es necesario arrancar del sistema operativo que esté descargado por debajo de la PC. Estas herramientas van a permitir ingresar al disco, hacer la extracción y el clonado, o sea básicamente todo; y si se ingresa en la lista de herramientas de CAINE se tienen una gran variedad de componentes. Se puede arrancar del CD live y ofrece la posibilidad de crear un reporte de todo lo que hay en el sistema operativo instalado (Fig. 2.10). Permite hacer una adquisición básica.

Fig. 2.10. Herramienta CAINE.
Tomado de: https://raulespinola.wordpress.com/2009/02/28/caine-gnulinux-livecd-para-informatica-forense/

Deft Linux (www.deftlinux.net).Resulta un poco más complicado que CAINE, pero contiene una gran variedad de herramientas útiles para la adquisición y la clonación, por lo que también es recomendable. Lleva un entorno gráfico que es muy cómodo y el dart, conjunto de herramientas que permiten hacer la clonación (Fig. 2.11).

Fig. 2.11. Herramienta dart.
Tomado de: http://www.deftlinux.net/2015/04/24/deft-zero-rc1-ready-for-download/

También es recomendable porque se emplea para otros temas de seguridad, como es Kali Linux.

Kali Linux, antiguo BackTrack (www.kali.org) que cuenta con una variedad de herramientas para seguridad y temas forenses, por lo cual es muy recomendable (Fig. 2.12).

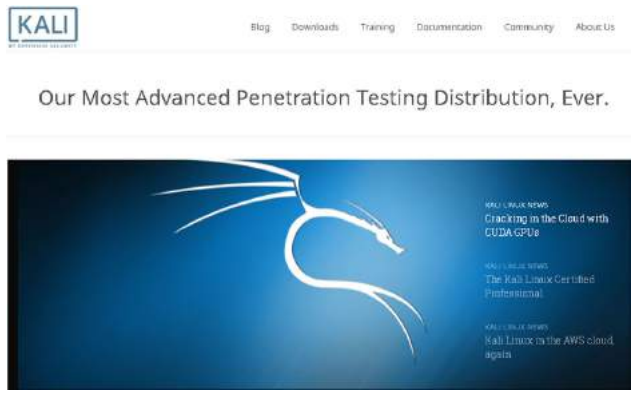

Fig. 2.12. Herramienta Kali Linux.
Tomado de: https://www.kali.org/

Helix (www.e-fense.com/helix/) es una distribución personalizada de Knoppix. Es mucho más que un Live CD Booteable, puesto que contiene kernels personalizados de Linux, una excelente detección de h ardware y una gran cantidad de aplicaciones dedicadas a la respuesta a incidentes e informática forense. Fue designado con mucho cuidado para no tocar el equipo host en cualquier forma, requisito básico en la informática forense. Helix no monta ni el espacio en Swap ni los dispositivos conectados a él de forma automática (http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Autenticacion.php#H, 2016).(Fig. 2.13).

Fig. 2.13. Herramienta Helix.
Tomado de: https://www.efense.com/store/index.php?_a=viewProd&productId=11

Existen otros productos como:

FTK Imager Lite (http://www.accessdata.com/support/product-downloads) 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. FTK Imager también puede crear copias perfectas (imágenes forenses) de datos de computadora sin realizar cambios en la evidencia original (ReYDeS, 2016). (Fig. 2.14).

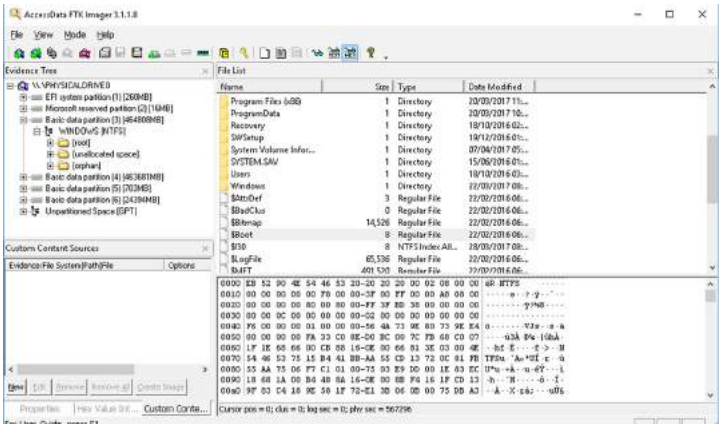

Fig. 2.14. Herramienta FTK Imager Lite.

El OSFClone (http://www.osforensics.com/tools/create-disk-images.html) es gratuito y permite clonar, pero en vez de utilizar un entorno gráfico se maneja en modo consola y puede utilizar los números del 1 al 5 para hacer un clonado bit a bit. (Fig. 2.15).

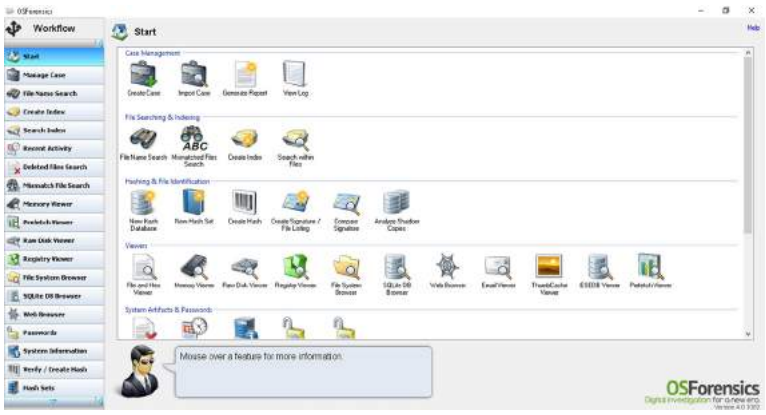

Fig. 2.15. OSFCloneT.

Al hacer un clonado usando *software* libre hay que tener en cuenta el rendimiento que va generar: será mucho menor que si se utilizaran herramientas dedicadas. Al realizar un clonado con cualquiera de las herramientas que se han visto anteriormente con un tamaño de 3 terabytes, tomará alrededor de 4 a 5 días. Si se va reduciendo a 1 tera, se reducirán también los días, pero es importante precisar la cantidad de tiempo que hay que dedicarle. Si se va a hacer un clonado delante de un juez y se ha contratado un notario de la empresa para que esté presente, entonces se haría el clonado. El notario cobraría por la cantidad de días que in-

vertiría en estar pendiente del proceso, aunque no siempre de forma presente. Si se dedican al peritaje hay que tener en cuenta el costo extra del notario y, por lo tanto, es necesario aclarar si está en el presupuesto todo lo mencionado, para que posteriormente el cliente asuma el pago.

Los procedimientos que se deben tener en consideración son:

1. Rendimiento, para hacer un disco duro de 800 megas o de 1 tera estas herramientas son muy útiles, pero en el momento en que sea necesario trabajar con más de un disco duro, los clonadores por *software* no son suficientes y se debe prestar especial atención a la máquina en la que se va a arrancar el cd Live, porque si se hace desde un DVD con el CAIN van arrancar la máquina y luego se empezará a pulsar las teclas Supr, F12, F2, esc y ctrl porque no se ha definido bien cuál será la tecla de arranque. Al arrancar el sistema Windows y no conocer la tecla indicada podría invalidarse, cambiarían las fechas del sistema, los parámetros del registro, el *stand* de fechas y podría levantar sospechas de que ha sido modificado. Si se va arrancar y se va hacer un clonado de un disco de un portátil, es necesario tener claros el modelo y la marca. Esta información puede encontrarse en internet; por ejemplo, si es una HP se puede buscar por internet cuál es la tecla que activa el DVD, porque no todas son iguales. Cuando se va hacer un clonado de este estilo se intenta documentar, pero como no se garantiza nada, se desenchufa el cable de alimentación y se quita la batería, si se observa que la tecla que se está pulsando no arranca. De esta manera se quita la batería, se apaga el equipo y se vuelve a observar cuál es, por eso nunca se debe confiar en el método de arranque de un DVD.

Clonación de discos por medio de hardware

Para la clonación de discos se podrá utilizar la tecnología de los clonadores.

Fig. 2.16. Clonación de discos por medio de *hardware*.
Tomado de: https://qloudea.com/icybox-ib-121cl-6g

Un clonador (Fig. 2.16) es un dispositivo *hardware*, considerado como una herramienta orientada a la copia de discos exclusivamente. Como un *hardware* típico con sus chips tiene su propia CPU y evidentemente sus buses de alta velocidad.

En la (Fig. 2.17) se observa inicialmente un disco duro pequeño. Se ha de copiar a otro disco duro diferente, como se aprecia en la imagen; es sencillo: disco duro 1, disco duro 2, una alimentación y los botones de copiar y calcular hash. Automáticamente dirá: correcto, ha funcionado.

Es rápido, eficaz, sencillo, no intrusivo. De acuerdo a la velocidad se ha reducido bastante, recordemos que podría tomar de 4 a 5 días clonar 3 teras. Se reduciría prácticamente entre 6 u 8 horas. Entonces se está hablando ya de otro modelo, recomendable cuando se tienen que clonar muchos discos. A pesar de que el precio de estas herramientas es muy alto, vale la pena invertir en estos productos.

Fig. 2.17. Herramientas orientadas a la copia de discos duros.
Tomado de: https://www.xataka.com/perifericos/century-kd2535pro-una-ayuda-para-clonar-un-disco-duro

El HardCopy versión III (Fig. 2.18) es un producto israelita y es el que utilizan los analistas forenses para ver el hash de la huella de los dos discos; luego se muestra un clonador de móviles (Fig. 2.19) (http://lang.cellebrite.com/es/) y se enchufa un móvil a un lado y un móvil al otro lado, se da clic en el botón y se logra un clonado automático. Se salta directamente las protecciones si se tiene PIN.

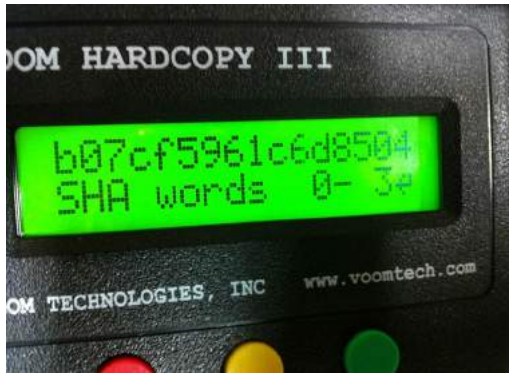

Fig. 2.18. Hardcopy versión III.
Tomado de: http://conexioninversa.blogspot.com/2010/11/hardware-forensics.html

Se puede observar en la pantalla de la Fig. 2.19 la extracción lógica de datos de la sim, del sistema de archivos, de contraseñas, el clonado de la sim física. A pesar de ser un producto excelente, su precio es considerable.

Fig. 2.19. Extracción lógica de datos de la SIM.
Tomado de: http://conexioninversa.blogspot.com/2010/11/hardware-forensics.html

Esto permitirá que cualquier dispositivo móvil se pueda clonar, pero aunque funciona perfectamente no siempre es aplicable por la cantidad de dinero involucrado. Por lo tanto, se trabajará con herramientas gratuitas y comerciales, y todas las que se adjuntan en este libro son admitidas judicialmente (Fig. 2.20).

Fig. 2.20. Análisis forense de dispositivos móviles.
Tomado de: http://lang.cellebrite.com/es/mobile-forensics/products/pc-based/ufed-4pc-ultimate

Actualmente, cuando ya se dispone de los clonadores es necesario tener en cuenta lo siguiente:

Si se tiene que hacer un clonado para un juzgado, se trabajaría con el disco duro original que sería abierto por un secretario general judicial, responsable de dar fe del proceso que se realizaría. El original queda en poder del juzgado y la copia se entrega al señor juez para que sea entregado a otro perito.

Si se contrata una empresa y se tiene la sospecha de que un empleado está haciendo fraude desde alguno de estos ordenadores, el procedimiento cambiaría. Como en esto no intervendría el juzgado, se tendrían que tomar determinadas medidas.

En el proceso de clonado tiene que estar un representante de los trabajadores (comisiones y obreros), un representante de la empresa (recursos humanos, dirección, dirección técnica, alguien que represente la empresa), la persona si es el caso que se le acusa o la víctima, porque tienen que ver qué información se va tocar o tomar de ese ordenador, y el perito informático que dará fe de todo el proceso para colaborar así con el notario. Si no se tienen estas precauciones, se podría modificar el original. Lo que se busca es marcar una serie de garantías procesales que son el conjunto de personas que darán fe de la actividad que se va a realizar independientemente de la acción del notario. Este último levanta el acta y empieza a escribir parte del proceso de clonación. Una vez que se tengan el disco original y el clonado, es posible que se requiera una copia para la empresa que contrata o que se necesiten más copias porque el original se lo lleva el juzgado o lo guardará el notario para mantener la cadena de custodia. Sin embargo, también

puede pedir una copia el empleado del que se sospecha, para buscar otro perito. De esta forma se pueden tener tres discos duros clonados. Si es de 3 teras requerirá demasiado tiempo para copiar, por lo cual es muy recomendable disponer de una clonadora porque ayudaría mucho en la reducción del tiempo.

La cadena de custodia puede presentar obstáculos como el impedimento de que el ordenador salga de la institución. Si esto ocurriera, por ejemplo en Amazon o en un comercio electrónico, en un *rack* de servidores en el que no se pueden clonar los discos duros o en algo más grande como un entorno SAP que está distribuido en varias máquinas o en varios *racks*, y no se pueda clonar los discos, se procede con una extracción de los discos o una especie de clonado, pero concentrado solo en la información que se está buscando. Esto es más complejo porque ya se hace con herramientas comerciales; como los discos duros originales no se puede sacar ni llevar al juzgado o a una entidad financiera que tenga una caja fuerte, se contrataría un servicio de vigilancia, es decir, se ponen los servidores con una cinta y se llama a seguridad para que ellos le pongan una serie de monitores dentro del CPU. Con esto garantizan que nadie pueda ingresar a los teclados ni a los equipos. Esta grabación se realiza online y se va a depositar en este proveedor; aparte se implementaría una serie de alarmas biométricas para evitar algún tipo de acceso más extraño que pueda saltarse las alarmas. Esto constituye un proceso de adquisición de la información más complejo, por lo que tiene un costo evidentemente más elevado y funciona como cadena de custodia.

En resumen, un clonado aparentemente sencillo precisa definir si lleva alguna información, si se puede hacer por *software*, *hardware* o si se corre el riesgo de que se pueda presentar el problema de que sea un RACK o un sistema mucho más grande. La extracción sería en vivo y se le tiene que documentar. Cuando no sea posible cumplir los pasos imprescindibles para hacer un clonado, lógicamente no se obtendrá toda la información, pero sí la memoria, el archivo de paginación, y se puede documentar que dadas las características del servicio que se está ofreciendo, este es el único procedimiento. El dueño de la empresa accederá porque esta no puede cerrar para hacer eso. De esta manera se evitan inconvenientes y si esto va a otro perito para que este evalúe el trabajo que se ha realizado, sabrá lidiar con la situación porque está acostumbrado a hacer este tipo de procedimientos.

CAPÍTULO 3. INTEGRIDAD

La integridad se fundamenta en disponer de una huella digital única e inequívoca de los dispositivos originales que sean iguales a los clonados. Esta huella es producto de la operación de un algoritmo (Hidalgo Cajo, 2014).

3.1.Hash

Un *hash* (también llamado resumen y de manera informal un *checksum*) es una especie de firma de un flujo de datos que representa el contenido; y esto va a devolver un número único que coincidirá con el *checksum* realizado, lo que significaría que es íntegro y que no existió manipulación del origen ni del destino. Lo más cerca de la vida real es "un precinto de seguridad en un paquete de *software*, si se abre la caja (y se cambia el archivo), este será detectado; ejemplo: una vez que se ha terminado el proceso de clonado de un disco duro, se realiza el de *hash*. Aunque parezca simple, un *hash* de un disco duro de 3 teras necesitará al menos de 4 horas para su copia y verificación. En el caso de que no sea un disco duro, sino la extracción de una carpeta, antes de tocarla se debe realizar un *hash* de su contenido y una copia verificar que el origen y el destino del *hash* sean el mismo. Otro ejemplo puede ser el de un fichero pst de Outlook que contiene 3 gb; antes de abrirlo, tocarlo, o manipularlo, se debe realizar un *hash*. Una vez realizado el *hash* se copiar ese fichero en el disco duro y se hace otro *hash*. Todo se documenta con capturas de la pantalla y se pone en la documentación por si alguien quiere verificarlo.

3.2. MD5

MD5 (Message Digest Algorithm 5, Algoritmo de Resumen del Mensaje) es un algoritmo que se utiliza como una función de codificación o huella digital de un archivo. De esta forma, a la hora de descargar un determinado archivo como puede ser un instalador, el código generado por el algoritmo, también llamado *hash*, viene “unido” al archivo. Un hash MD5 está compuesto por 32 caracteres hexadecimales y una codificación de 128 bits (Martínez, 2018).

3.2.1. El problema del MD5

Entre los diferentes problemas que se pueden encontrar con el MD5, se pueden mencionar los siguientes:

- Es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT que se está usando para el cálculo de huellas.
- A pesar de su amplia difusión actual, la sucesión de problemas de seguridad detectados desde que se anunciase una colisión de Hash plantea una serie de dudas acerca de su uso futuro.
- Tiene un problema llamado colisiones.
- Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

3.2.2. ¿Qué son y qué pasa con las colisiones?

Las colisiones se dan cuando zonas de diferentes datos producen el mismo valor *hash*, es decir, que se puede manipular. No es recomendable aplicar el MD5 a un disco duro, solo en España le darían paso. Ejemplo: unos programas de diferentes contenidos contienen el mismo *hash*; un documento Word de 10 páginas tiene el mismo *hash* que otro de 500 y esto no debería pasar porque, al ser diferentes, deberían tener diferente hash. Aquí se calcula el *hash* del programa hello.exe y de erase.exe que son el mismo; sin embargo, si se ejecuta el "hello" sale un texto y si se ejecuta el "erase" sale otro, lo cual significa que los programas son diferentes, pero el *hash* es el mismo. Por lo tanto, el MD5 no es recomendable (Fig. 3.1).

- MD5SUM
- MD5.ZIP

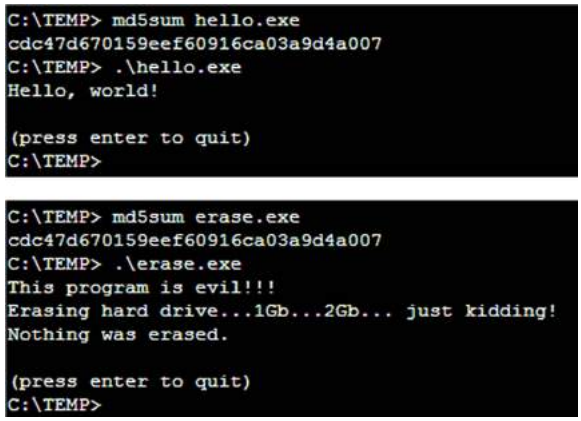

Fig. 3.1. Distintos archivos con el mismo *hash* utilizando MD5.

3.3. Sha-1

Secure Hash Algorithm 1 (Algoritmo de Hash Seguro 1) transforma un mensaje a una larga ristra de números y letras que sirven como huella criptográfica (*hash*) para ese mensaje. El problema es cuando ese mismo valor de *hash* es producido para dos mensajes diferentes, lo cual puede ser explotado para falsificar firmas digitales y poder interceptar y descifrar comunicaciones cifradas con este cifrado. Esto es lo que se conoce como una colisión de *hash*, o ataque de colisión. Básicamente, con esto se pueden alterar funciones *hash* para que coincidan con cualquier otra y poder, por ejemplo, acceder a cualquier cuenta que use cifrado SHA-1 (ADSLZONE, 2018).

3.4.Herramientas criptográficas hash

Dentro de las diversas herramientas que se pueden utilizar, están el HashMyFiles y el HashGenerator que no solo calculan el MD5, sino que también realizan combinaciones utilizando el Sha-1. Cuando se ejecuta un clonado ofrece una opción si se está hablando de una clonadora, de elegir el algoritmo, y si se está hablando de un HashGenerator lo pueden realizar con el Sha-1. Se pueden crear *hashes* de un directorio, de una lista de ficheros de todo el disco duro, de todo lo que se encuentre en el *software* del PC (Fig. 3.2).

Fig. 3.2. Herramientas para calcular el MD5.

Este punto es primordial porque se recogen los datos que se tienen en el *pendrive*; se realiza la adquisición en vivo y se obtendrá el clonado completo. Una vez que ya se tienen las dos clonaciones, la adquisición en el *pendrive* y el clonado se busca sacar la información de ese conjunto.

Ejemplo: El caso a resolver se encuentra en la página web www.honeynet.org que presenta diferentes métodos para el análisis forense de la información. A continuación, un ejercicio práctico sobre la temática:

- Análisis forense informático de un sistema Linux comprometido

La información sobre el incidente:

El sistema ejecutaba una instalación predeterminada de Red Hat Linux 6.2 Server. La zona horaria del sistema se configuró en GMT-0600 (CST). El IDS (snort) de la organización señaló y registró lo siguiente:

Nov 7 23:11:06 lisa snort[1260]:

RPC Info Query: 216.216.74.2:963 -> 172.16.1.107:111

Nov 7 23:11:31 lisa snort[1260]: spp_portscan: portscan status from 216.216.74.2: 2 connections across 1 hosts: TCP(2), UDP(0)

Nov 7 23:11:31 lisa snort[1260]: IDS08 - TELNET - daemon-active: 172.16.1.101:23 -> 216.216.74.2:1209

Nov 7 23:11:34 lisa snort[1260]: IDS08 - TELNET - daemon-active:172.16.1.101:23 -> 216.216.74.2:1210

Nov 7 23:11:47 lisa snort[1260]: spp_portscan: portscan status from

216.216.74.2: 2 connections across 2 hosts: TCP(2), UDP(0)

Nov 7 23:11:51 lisa snort[1260]: IDS15 - RPC - portmap-request-status:216.216.74.2:709 -> 172.16.1.107:111

Nov 7 23:11:51 lisa snort[1260]: IDS362 - MISC - Shellcode X86 NOPS-UDP:216.216.74.2:710 -> 172.16.1.107:871

11/07-23:11:50.870124 216.216.74.2:710 -> 172.16.1.107:871 UDP TTL:42 TOS:0x0 ID:16143 Len: 456

Se obtuvo una copia de imagen de bits de las particiones activas, como se detalla:

/dev/hda8	/
/dev/hda1	/boot
/dev/hda6	/home
/dev/hda5	/usr
/dev/hda7	/var
/dev/hda9	swap

MD5 Checksums:

a1dd64dea2ed889e61f19bab154673ab	honeypot.hda1.dd
c1e1b0dc502173ff5609244e3ce8646b	honeypot.hda5.dd
4a20a173a82eb76546a7806ebf8a78a6	honeypot.hda6.dd
1b672df23d3af577975809ad4f08c49d	honeypot.hda7.dd
8f244a87b8d38d06603396810a91c43b	honeypot.hda8.dd
b763a14d2c724e23ebb5354a27624f5f	honeypot.hda9.dd

ANÁLISIS DE LA INTRUSIÓN DEL SISTEMA

Al ingresar a la herramienta Autopsy se montan las imágenes de cada una de las particiones del disco duro (Fig. 3.3).

Fig. 3.3. Imágenes montadas de las particiones del disco duro.

Seguidamente se procede al cálculo del valor Hash MD5 de cada partición montada; de honeypot.hda1.dd como se observa (Fig. 3.4):

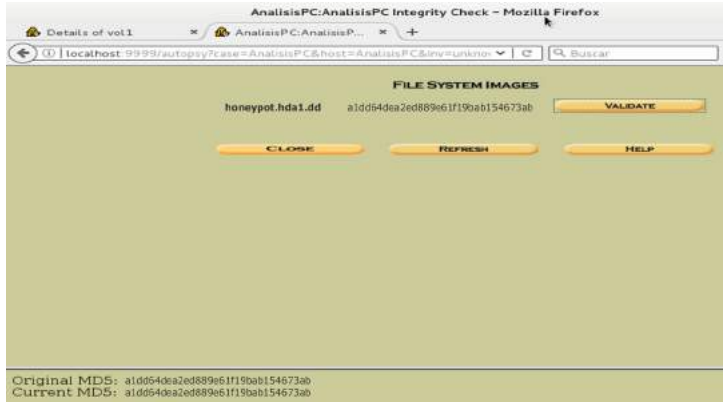

Fig. 3.4. Valor Hash MD5 de honeypot.hda1.dd.

La partición honeypot.hda5.dd que se muestra (Fig. 3.5):

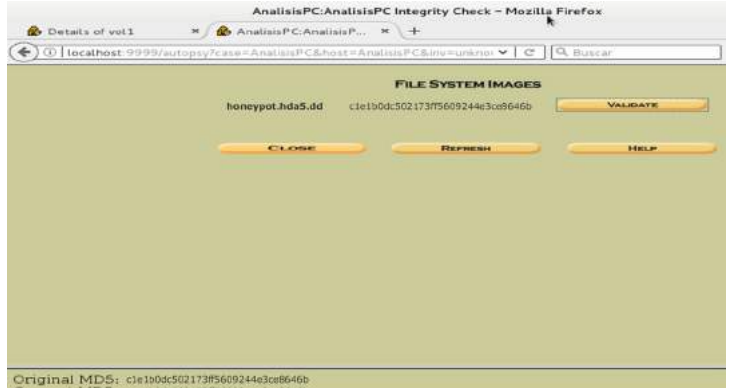

Fig. 3.5. Valor Hash MD5 de honeypot.hda5.dd.

La partición honeypot.hda6.dd como se observa (Fig. 3.6):

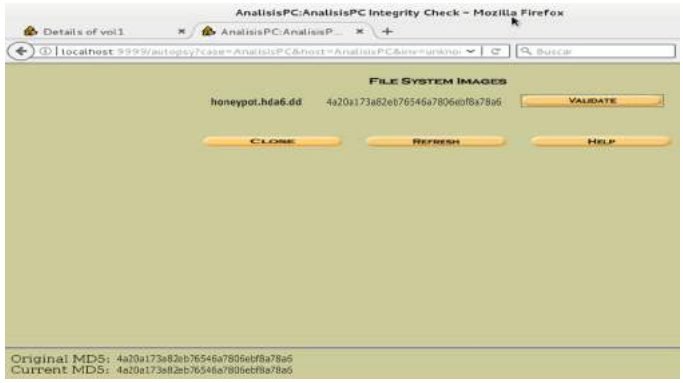

Fig. 3.6. Valor Hash MD5 de honeypot.hda6.dd.

La partición honeypot.hda7.dd como se observa (Fig. 3.7):

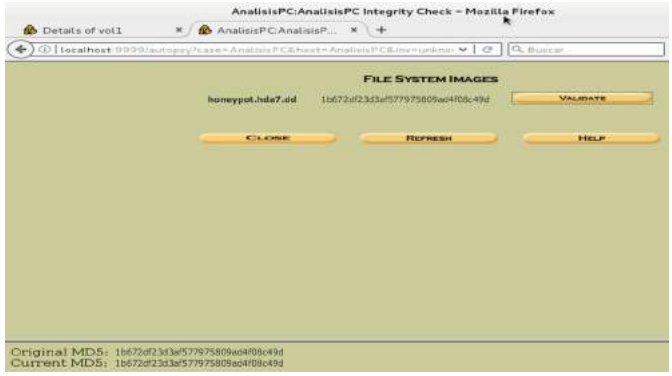

Fig. 3.7. Valor Hash MD5 de honeypot.hda7.dd.

La partición honeypot.hda8.dd como se observa (Fig. 3.8):

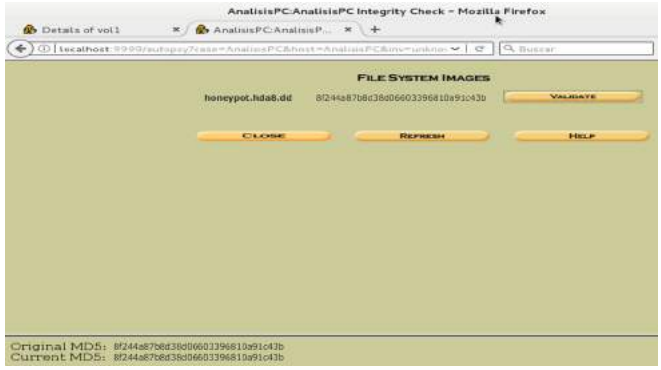

Fig. 3.8. Valor Hash MD5 de honeypot.hda8.dd.

La partición honeypot.hda9.dd como se observa (Fig. 3.9):

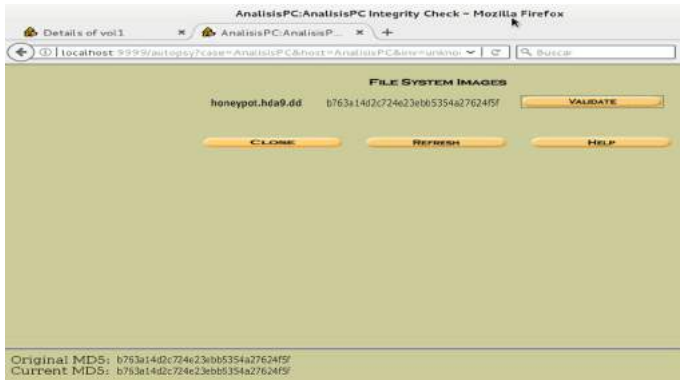

Fig. 3.9. Valor Hash MD5 de honeypot.hda9.dd.

Se procede al análisis de la imagen montada /var (Fig. 3.10).

Fig. 3.10. Partición montada /var.

Se observa que al arrancar el sistema el 06 de noviembre y al finalizar el 08 de noviembre, se obtiene una sesión de ftp cerrada, dando como resultado la existencia de pocos eventos, por lo que es necesario proceder a analizar los *logs* del sistema (Fig. 3.11).

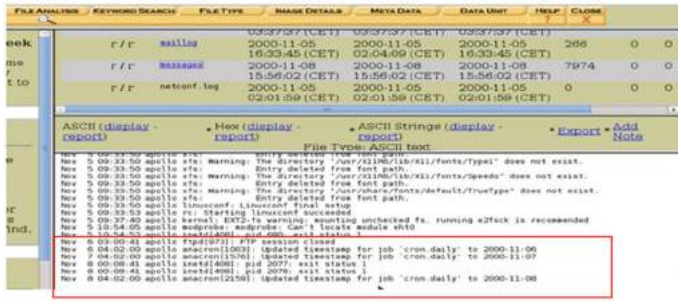

Fig. 3.11. Arranque del sistema.

En el directorio /var/boot.log se localiza el arranque del sistema y en var/log/cron se encuentran los archivos del sistema que se ejecutan a cada hora (Fig. 3.12).

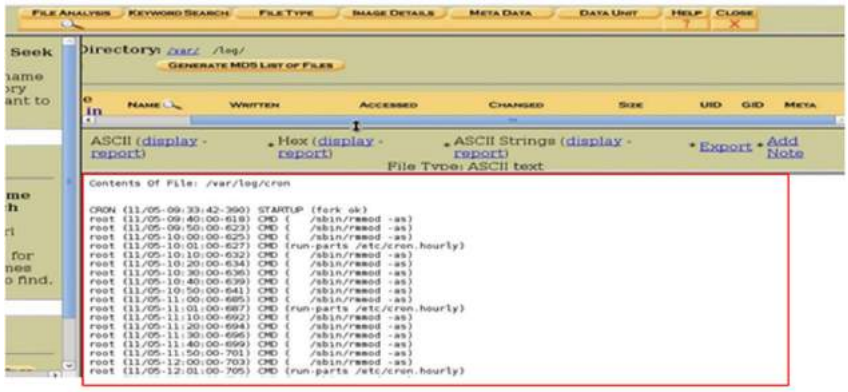

Fig. 3.12. Localización de los archivos del sistema al arrancar.

Se puede observar el directorio /var/log/lastlog, con la última conexión que se ha realizado en el computador http://c871553-b.jffsn1.mo.home.com; el cual informa que existió una conexión remotamente (Fig. 3.13).

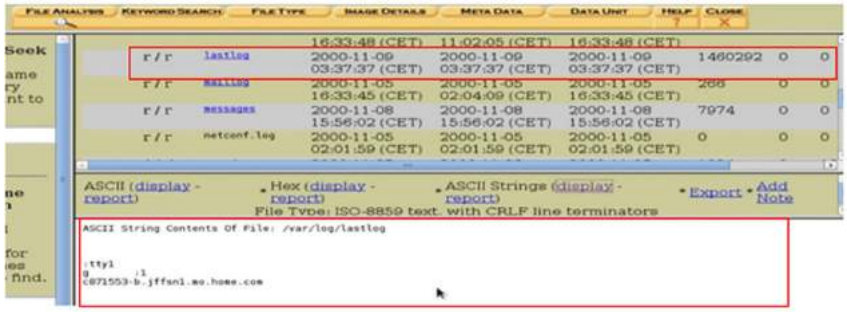

Fig. 3.13. Última conexión en el computador.

En el directorio /var/log/maillog se encuentra la información del servidor de correo (Fig. 3.14).

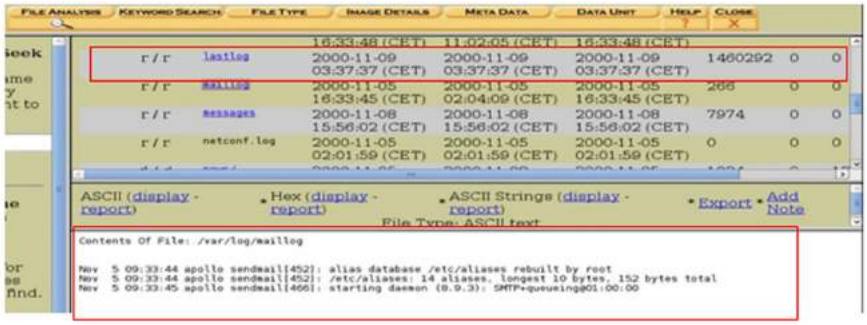

Fig. 3.14. Información del servidor de correo.

En el directorio /var/log/secure encontramos conexiones que se realizaron con ftp y telnet (Fig. 3.15).

Fig. 3.15. Conexiones con ftp y telnet.

En el directorio /var/log/wtmp se observa el número de intentos de ingreso al usuario root (cuenta del administrador) (Fig. 3.16).

Fig. 3.16. Ingresos fallidos con el usuario root.

Al analizar el directorio raíz/ (Fig. 3.17).

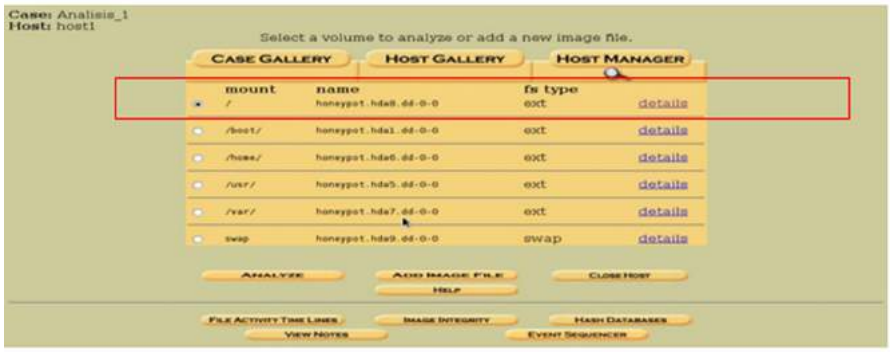

Fig. 3.17. Imagen montada raíz /

Al ingresar al directorio /etc/passwd se muestra la siguiente información (Fig. 3.18):

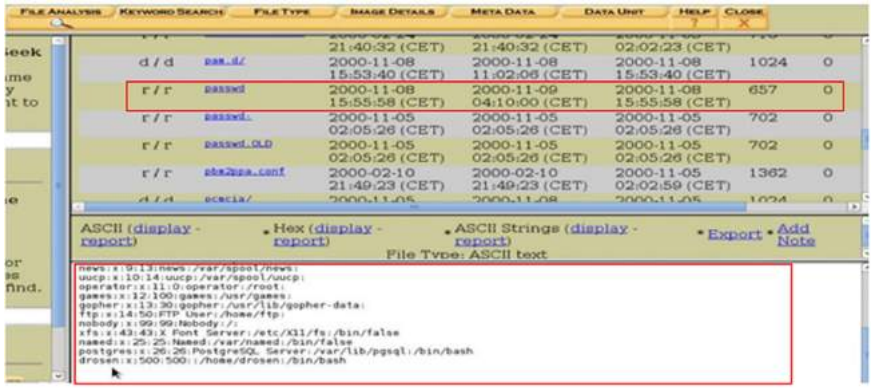

Fig. 3.18. Información del directorio /etc/passwd

En el directorio /etc/passwd- se observa la siguiente información (Fig. 3.19):

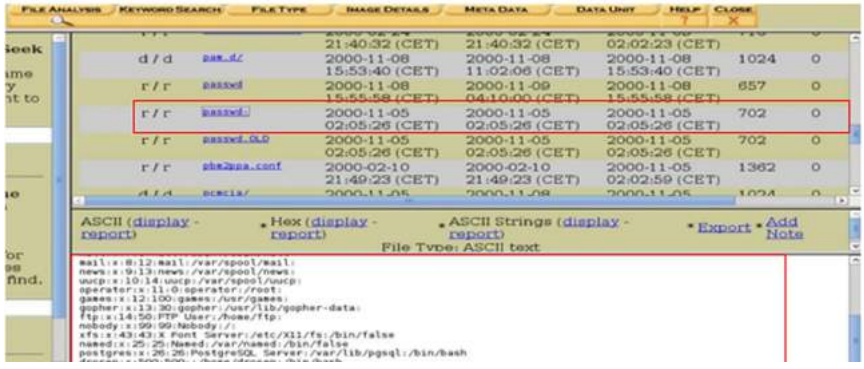

Fig. 3.19. Información del directorio /etc/passwd-.

En el análisis del directorio /etc/passwd.OLD es idéntico a /etc/passwd (Fig. 3.20).

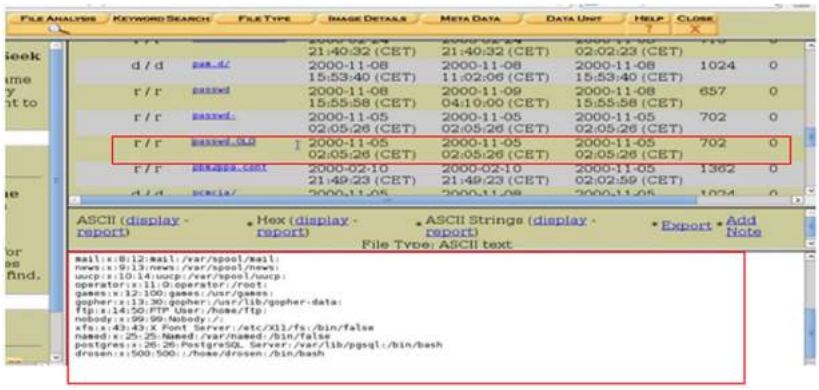

Fig. 3.20. Análisis del directorio /etc/passwd.OLD y /etc/passwd.

Al proceder con el análisis del directorio /home (Fig. 3.21).

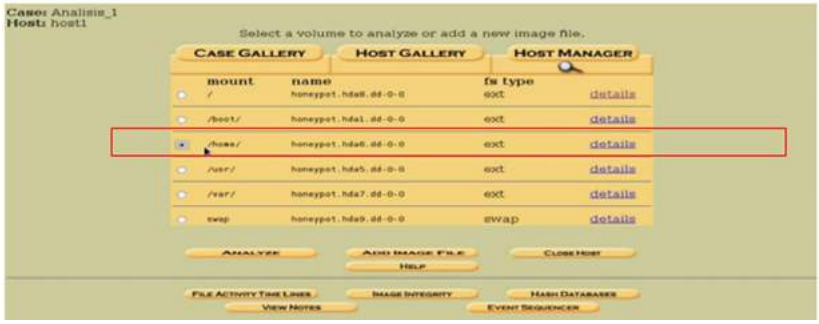

Fig. 3.21. Imagen montada /home.

el directorio /home/drosen se localizan las secuencias del usuario drosen que ha realizado. En él .bash_history existen directorios comprimidos y la instalación de programas (Fig. 3.22).

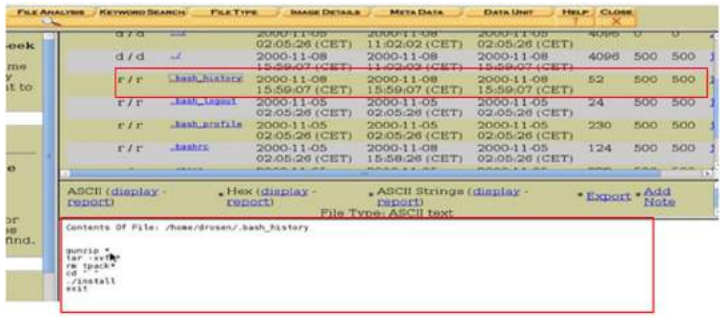

Fig. 3.22. Secuencias directorio /home/drosen/.bash_history.

Se puede crear la Línea de t iempo para analizar cronológicamente todos los directorios (Fig. 3.23.).

Fig. 3.23. Línea de tiempo.

Al realizar el análisis cronológico se detalla que, en el año 2000, mes de noviembre, se ha cambiado 36855 archivos; además, el sistema reinicia la máquina, en su defecto se instaló nuevamente el sistema operativo (Fig. 3.24).

Fig. 3.24. Análisis cronológico.

En el directorio /home/boot/log existe poca información; el análisis cronológico de la línea de tiempo describe un directorio /.Ci, dentro del directorio /man, e identifica que existió una intrusión, en la cual un usuario creó ese directorio y se han instalado varios archivos (Fig. 3.25).

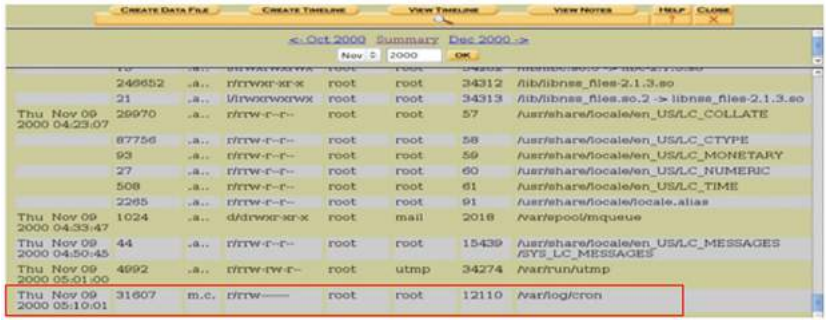

Fig. 3.25. Instalación archivos intruso.

El directorio /root/.bash_history, direcciona a una papelera y cuando el usuario borra un archivo definitivo pasa por dev/null; generalmente cuando realizan estas acciones se detecta una intrusión (Fig. 3.26).

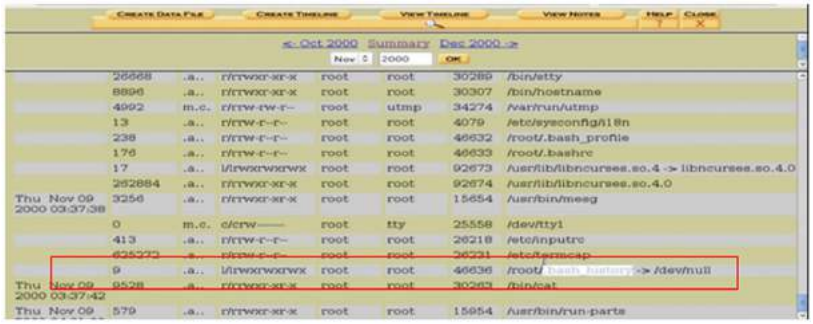

Fig. 3.26. Información acciones intrusión.

El directorio /root/.bash_logout; ingresa a un archivo cuando el usuario root se desconecta (Fig. 3.27).

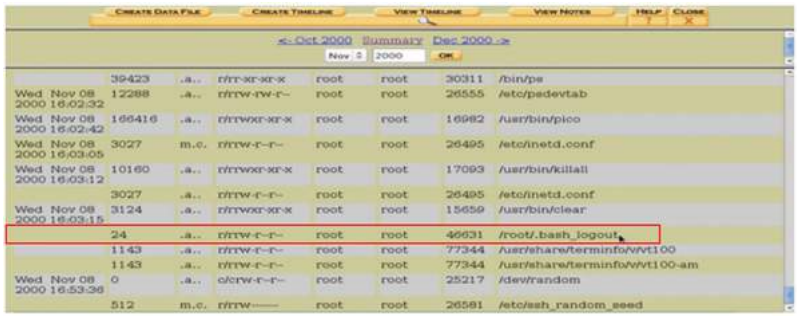

Fig. 3.27. Desconexión del usuario root.

Al analizar el directorio /usr/ (Fig. 3.28).

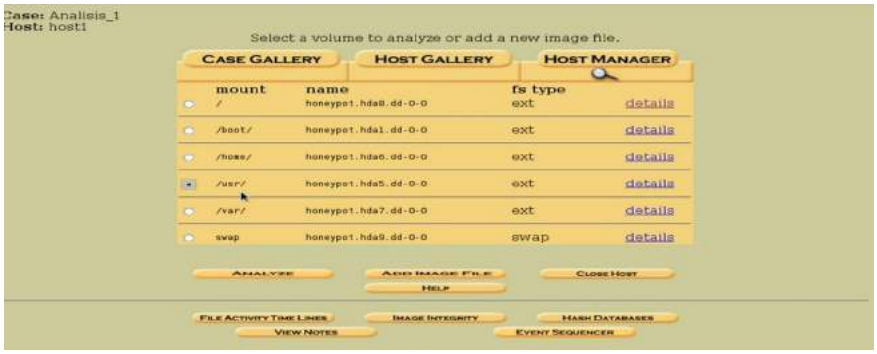

Fig. 3.28. Imagen montada /usr/.

Al ubicarse sobre el directorio /usr/man/.Ci se encuentra al usuario y los comandos del sistema (Fig. 3.29).

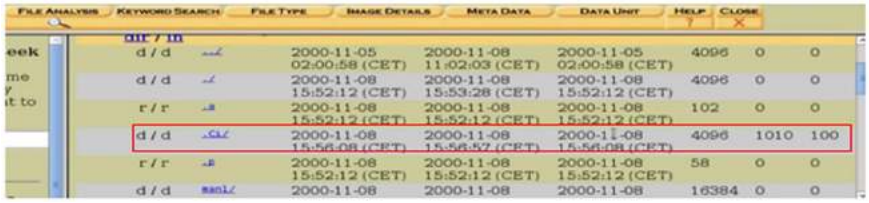

Fig. 3.29. Ubicación directorio /usr/man/.Ci.

Dentro del directorio/usr/man/.Ci se encuentran los comandos (Fig. 3.30).

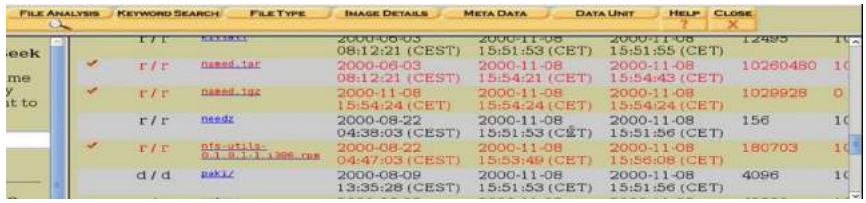

Fig. 3.30. Información directorio/usr/man/.Ci.

Al ingresar a *backup* se tiene comandos del sistema que no deberían estar ahí; los cuales constan con la misma fecha: el 08 de noviembre del 2000 (Fig. 3.31).

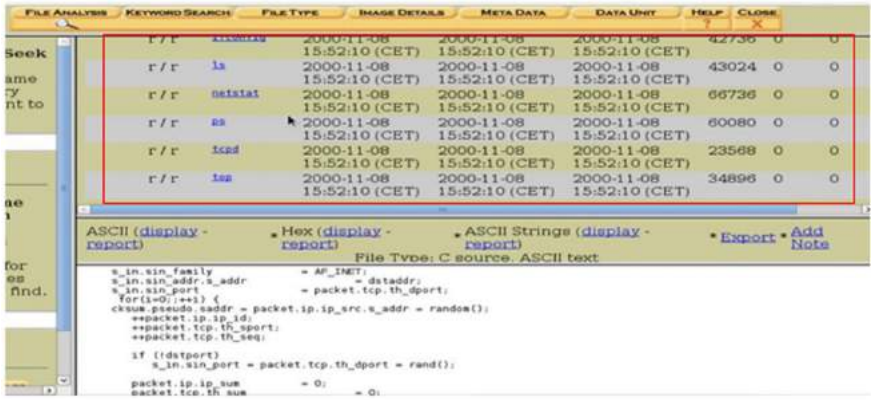

Fig. 3.31. Información *backup*

Al interior del directorio: /usr/man/.Ci/scan/port/strobe/INSTALL se realiza un escaneo de puertos y se observa que existe una vulnerabilidad del sistema (Fig. 3.32).

Fig. 3.32. Escaneo de puertos.

En base al análisis, realice las siguientes actividades:

1. Identifique el método de intrusión, su fecha y hora (suponga que el reloj del IDS estaba sincronizado con una fuente de tiempo de referencia NTP).

Al realizar el montaje de las diferentes particiones en el Autopsy (Fig. 3.33).

Fig. 3.33. Imagen montada /var/.

Se puede observar que en el directorio /var/log/boot.log, el arranque del sistema operativo (Fig. 3.34).

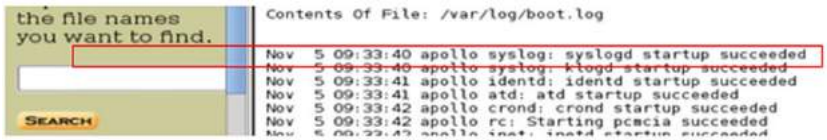

Fig. 3.34. Información directorio /var/log/boot.log.

Se analiza los log del sistema, en donde existió dos conexiones telnetd en noviembre 8, a las 00:08:40 y acceden desde el IP: 216.216.74.2, y se puede aseverar que hay vulnerabilidad al sistema (Fig. 3.35).

Fig. 3.35. Análisis *logs* del sistema.

En el directorio /var/log/messages, se encuentra la misma información de acceso que existió en el computador (Fig. 3.36).

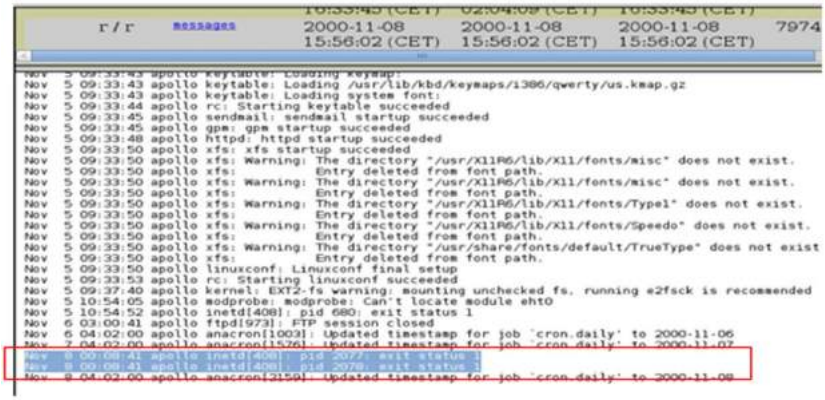

Fig. 3.36. Información directorio /var/log/messages.

Al realizar la extracción de los *strings*, se ilustra la información de la conexión del computador y se concluye que existe vulnerabilidad (Fig. 3.37).

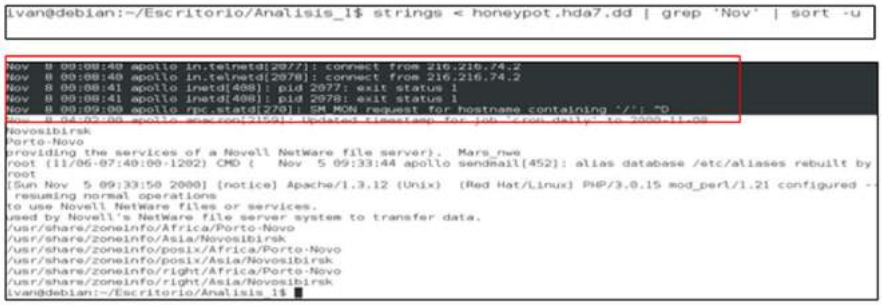

Fig. 3.37. Información de la extracción de los *strings*.

2. Identifique tanto como sea posible sobre el intruso o los intrusos.

La última conexión se ilustra en el directorio /var/log/lastlog, en donde se ubica el código ASCII (Fig. 3.38.) y convirtiéndolo a código hexadecimal corresponde a la dirección de una página web: http://c871553-b.jffsn1.mo.home.com desde donde se realizó la intrusión al sistema (Fig. 3.39).

Fig. 3.38. Información directorio /var/log/lastlog.

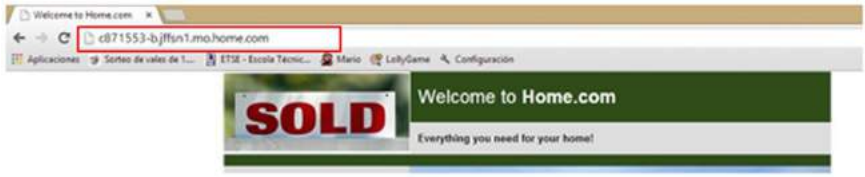

Fig. 3.39. Página web de donde se realizó la intrusión al sistema.

3. Se instaló un programa de captura de husos horarios (hora mundial) o contraseñas, de ser así ¿dónde y qué archivos están asociados?

El sniffer /usr/man/.Ci/snif es iniciado en la red y luego se crean dos archivos, un archivo /usr/man/.Ci/sniff.pid y /usr/man/.Ci/tcp.log (Fig. 3.40).

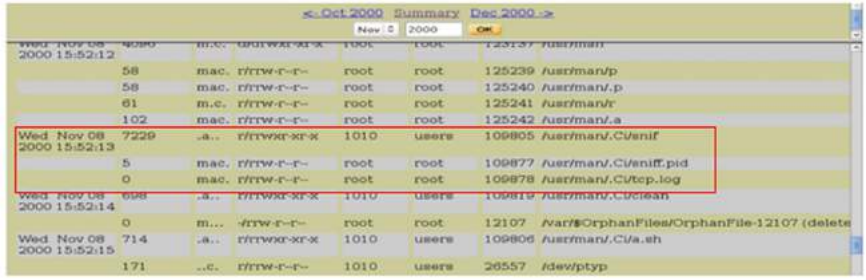

Fig. 3.40. Creación de archivos vulnerados

4. ¿Proporcione un informe adecuado para la gestión o los medios informativos? (Aspectos generales de la intrusión sin datos de identificación específicos).

Todas las conexiones se deberían mostrar pero los *logs* no se detallan; es decir, alguien modificó previamente el comando para ocultar información.

Con la información mencionada se describe que existió una intrusión en el sistema, la vulnerabilidad indica que no hubo daños causados, además el intruso usr/man/.Ci instaló algunos programas para poder ingresar por una puerta secundaria, y que el sistema está funcionando desde el 5 de noviembre del 2000.

5. Proporcionar un aviso para su uso dentro de la organización da lugar a explicar los aspectos claves de la vulnerabilidad explotada. ¿Cómo detectar y defenderse contra esta vulnerabilidad y cómo determinar si otros sistemas se vieron comprometidos de manera similar?

Sistema: apollo.honey.edu

Sistema Operativo: Red Hat Linux versión 6,2 se ha analizado que existe una vulnerabilidad en el sistema, el mismo que posee un directorio oculto /usr/man/.Ci, que contiene algunos kits, como sniffer, troyanos, una posible solución es reinstalar el sistema operativo para evitar que existan nuevos ataques.

C

Cadena de custodia: Procedimiento de trazabilidad controlado que se aplica a las evidencias, desde su adquisición hasta su análisis y presentación final, el cual tiene como fin no alterar la integridad y autenticidad de las mismas, asegurando en todo este proceso que los datos originales no son alterados.

Clonado: Proceso de copia, a bajo nivel y firmada digitalmente, de la información original por el cual se traslada esta 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.

E

Entorno de análisis forense: Lugar físico aislado del resto de actividades de la empresa u organismo donde se analiza la información electrónica, dotado de medios técnicos para los trabajos forenses asociados a las nuevas tecnologías.

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

H

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

Imagen forense: Es el producto de realizar un clonado de cualquier evidencia electrónica en un formato de directorio, sin tener en cuenta el soporte que la contiene

Información original: Conjunto organizado de datos que mantiene su integridad desde el inicio hasta el final del directorio o soporte informático que los contiene.

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

Informe pericial: Documento donde se recogen todas las tareas realizadas en las diferentes fases del análisis forense, así como las conclusiones extraídas en base a los hallazgos encontrados.

L

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

M

Metadato: Información que describe el contenido de un dato.

Muestra: Parte representativa o significativa de una evidencia.

P

Prueba electrónica: Es la demostración en un procedimiento judicial de los hechos que fundamentan la aplicación de requerimientos formales, procesales y legales.

Perito: Que es entendido o experto en determinada materia.

R

Recursos humanos: Toda vez que habrá ocasiones en las que se requiera la intervención de más de un especialista trabajando en el caso objeto de estudio

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

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 directorios: Organización lógica de un dispositivo.

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.

T

Trazabilidad: Propiedad de la información de ser rastreada o reconstruida hasta su origen.

V

Virtualización: Método consistente en la simulación del funcionamiento de una máquina física con su sistema operativo.

GLOSARIO DE SIGLAS

A

AFI: Análisis Forense Informático

ASCII: American Standard Code for Information Interchange

C

CD: Compact Disk

CIM: Common Information Model

CMD: Command Prompt

CPU: Central Processing Unit

CSI: Crime Scene Investigation

C#: Lenguaje de Programación Orientado a Objetos

D

DLL: Dynamic-Link Library

DNS: Domain Name System

DVD: Disco Versatil Digital

F

FTP: File Transfer Protocol

G

GB: Gigabyte

H

HD: High Definition

HTML: HyperText Markup Language

I

IE: Internet Explorer

IP: Internet Protocol

L

LEC: Ley de Enjuiciamiento Criminal

M

MD5: Message-Digest Algorithm 5

MFT: Master File Table

N

NTFS: New Technology File System

O

ONU: Organización de las Naciones Unidas

P

PC: Personal Computer

PCMCIA: Personal Computer Memory Card International Association

R

RAM: Random Access Memory

RRHH: Recursos Humanos

S

SAI: Sistema de Alimentación Ininterrumpida

SATA: Serial Advanced Technology Attachment

SD: Secure Digital

SID: Standard Instrumental Departure

SQL: Structured Query Language

U

UNE: Una Norma Española

URL: Uniform Resource Locator

USB: Universal Serial Bus

W

WBEM: Web-Based Enterprise Management

WMI: Windows Management Instrumentation

WMIC: Windows Management Instrumentation Command-Line

WSH: Windows Script Host

WWW: World Wide Web

BIBLIOGRAFÍA

DSLZONE. (2018). DISQUS. Obtenido de https://www.adslzone.net/2017/02/23/cifrado-sha-1-ya-no-seguro-google-lo-ha-roto-despues-22-anos/

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

Clonezila. (2018). Clonezilla. Obtenido de https://clonezilla.org/

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

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.

http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Autenticacion.php#H. (2016). Universidad Nacional Autónoma de México.

Martínez, I. (2018). Rootear. Obtenido de https://rootear.com/seguridad/md5-como-funciona-usos

Microsoft. (2017). Developer Network. Obtenido de https://msdn.microsoft.com/en-us/library/aa394582(v=vs.85).aspx

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

ReYDeS, A. E. (2016). http://www.reydes.com/d/?q=Crear_la_Imagen_Forense_desde_una_Unidad_utilizando_FTK_Imager.

Sánchez Cordero, P. (2014). Análisis Forense Informático, Adquisición, Clonación. Barcelona.

Sánchez Cordero, P. (2014). Introducción al Análisis Forense Informático., (pág. 10). Barcelona.

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

Santos Tello, J. D. (2013). Procedimientos en la investigación, recolección y manejo de la evidencia digital en la escena del crimen. Huehuetenango.

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

La informática forense involucra la recolección, preservación, identificación, extracción, documentación e interpretación de datos informáticos, y es usada para investigaciones criminales, corporativas o institucionales, evaluación de daños y análisis post-mortem como el fraude, el tráfico de droga, la pornografía infantil, el espionaje, los ataques cibernéticos, la infracción de *copyright*, la recuperación de datos eliminados y la detección de intrusiones con sus mecanismos y técnicas. El análisis forense se refiere a casos en los que se ha producido un delito real en los que la computadora ha sido la víctima.

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.

Saul Yasaca Pucuna, Magíster en Informática Educativa, ESPOCH, Ecuador; Ingeniero en Sistemas Informáticos, ESPOCH, Ecuador.

Luis Ángel Lema Ayala, Magíster en Seguridad Telemática, ESPOCH, Ecuador; Ingeniero de Sistemas y Computación, PUCE, Ecuador.

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; Tecnólogo en Informática, ITS- PAN, Ecuador; Técnico Superior en Programación de Sistemas, ITSPAN, Ecuador; Tecnólogo en Contabilidad de Costos, Instituto Tecnológico Superior Harvard Comput, Ecuador.

ISBN: 978-9942-35-224-8