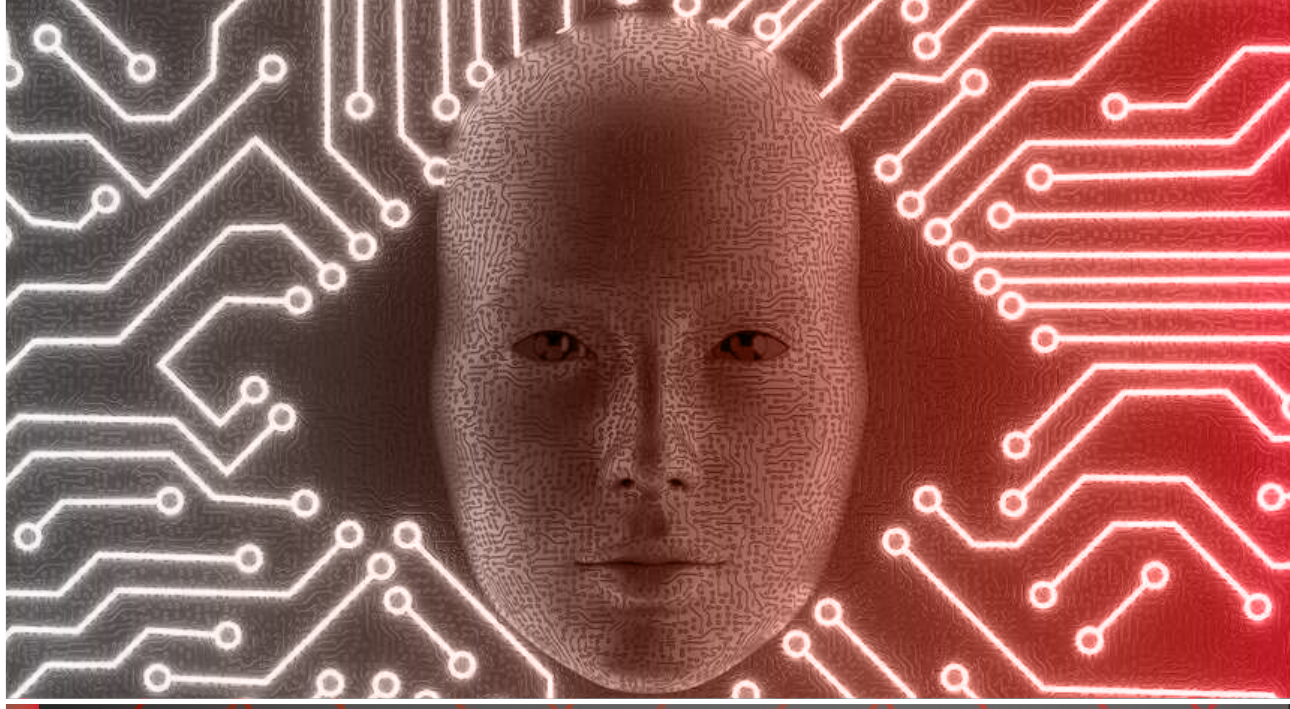
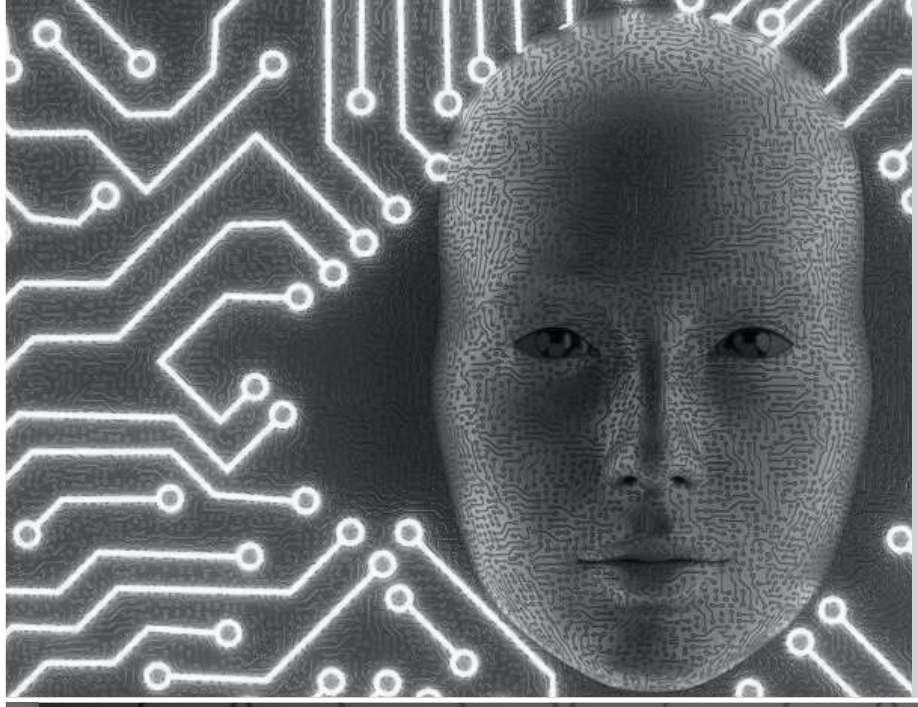


Informática Forense II

Prueba Indiciaria Informático Forense

1era Edición

SciELa



Computer Forensics II

Informative Forensic Evidence

1st Edition

SciELa

Autores:

- Hidalgo Cajo Iván Mesias
- Hidalgo Cajo Byron Geovanny
- Hidalgo Olmedo Byron Geovanny
- Latorre Benalcázar Nelly Baltazara

ISBN: 978-9942-7221-5-7

Primera Edición, Junio 2024

Informática Forense II: Prueba Indiciaria Informático Forense

ISBN digital: 978-9942-7221-5-7
DOI: https://doi.org/10.62131/978-9942-7221-5-7

Editado por:

Sello editorial:

© Editorial Investigativa Latinoamericana (SciELa)

Quevedo, Los Rios, Ecuador

E-mail: admin@editorial-sciela.org
Código Postal: 120303
WEB: https://editorial-sciela.org

Este libro se sometió a arbitraje bajo el sistema de doble ciego (peer review) y antiplágio. Este producto investigativo cumple con la Declaración de Principios de Budapest, San Francisco, México, Helsinki y Firma del Marco del MIT

Dirección editorial:
Lic. Alexander Fernando Haro, MSI.

Revisor (1):
Ing. Fabián Gallardo Gonzaga, Mg.

Revisor (2):
Ing. Johnny Triviño Sánchez, Mg.

Sistema de clasificación decimal DEWEY

005 - Programación. programas. datos de computadores

Clasificación comercial internacional - THEMA

U - Computación y tecnologías de la Información

UR - Seguridad Informática

URH - Fraude informático y "hacking"

| AUTORES |

Iván Mesias Hidalgo Cajo

https://orcid.org/0000-0002-9059-0272

ihidalgo@espoch.edu.ec

Escuela Superior Politécnica de Chimborazo - ESPOCH

Doctor (PhD) en Tecnología Educativa, Universidad Rovira i Virgili, España; Master 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 Informática e Inteligencia Artificial y pertenece a un grupo de investigación sobre la Inteligencia Artificial,

Joan M. Hidalgo C.

Byron Geovanny Hidalgo Cajo

https://orcid.org/0000-0002-5526-1676

bhidalgo@unach.edu.ec

Universidad Nacional de Chimborazo - UNACH

Ph.D. en Tecnología Educativa por la Universitat Lleida – España, Ph.D. en Ingeniería de Sistema e Informática por la Universidad Nacional Mayor de San Marcos – Perú, Máster en Ingeniería Computacional y Matemática por la Universitat Rovira i Virgili - España. Magister en Docencia Universitaria e Investigación Educativa por la Universidad Nacional de Loja - Ecuador. Magíster en Estadística Aplicada por la Politécnica Estatal del Carchi, Ingeniero en Computación y Ciencias de la Informática por la Universidad Javeriana . Investigador Agregado 1 acreditado por la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT REG-INV-20-04593), Docente - Investigador de la Universidad Nacional de Chimborazo, Escuela Superior Politécnica de Chimborazo.

Byron G. Hidalgo C.

Byron Geovanny Hidalgo Olmedo

https://orcid.org/0009-0005-6225-9442

bghidalgo.fiag@unach.edu.ec

Universidad Nacional de Chimborazo - UNACH

Magister en Estadística Aplicada, UPEC, Ecuador, Magister en Agroindustria mención: Sistemas Agroindustriales, UEA, Ecuador, Ingeniero Agroindustrial, UNACH, Ecuador.

Byron G. Hidalgo O.

Nelly Baltazara Latorre Benalcázar

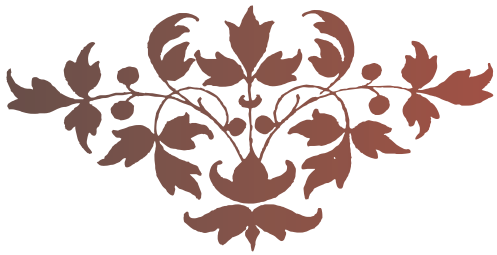
https://orcid.org/0000-0003-2618-7814

nelly.latorre@educacion.gob.ec

Ministerio de Educación - MINEDUC

Magister en Educación Básica, UNACH, Ecuador, Licenciada en Ciencias de la Educación profesora de Educación Básica, UNACH, Ecuador.

Nelly B. Latorre B.



ÍNDICE

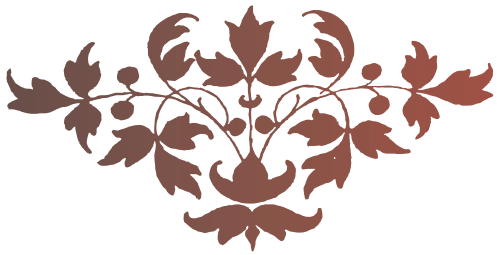
CAPÍTULO II.
METODOLOGÍA APLICADA EN LA INFORMÁTICA FORENSE II

CAPÍTULO III.
PROTOCOLOS DETALLADOS EN LA TOMA DE DECISIONES DE CADA UNA DE LAS FASES EN EL ANÁLISIS FORENSE INFORMÁTICO

Capítulo IV.

Comprendiendo Terminología Sobre Informática Forense

RECURSOS



PRÓLOGO

Recopilar pruebas digitales legalmente admisibles

La informática forense involucra la recolección, preservación, identificación, extracción, documentación e interpretación de datos informáticos, se aborda el problema de la falta de herramientas para el soporte de los procesos de toma de decisiones durante el análisis forense informático. Se realiza el estudio preliminar, diseño y prototipado de una herramienta de toma de decisiones aplicable al análisis de equipos informáticos personales, así como de sistemas en red. Se estudian también otros dispositivos, detallando de forma particular el análisis de computadoras personales de escritorio.

Para abordar la Informática Forense II (Prueba Indiciaria Informático Forense) en el presente libro, se trabajó con ejemplos reales y con el software recomendable. 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 pro-

pósito de identificar, preservar, analizar y documentar los resultados obtenidos. El segundo se refiere a la Metodología aplicada en el Informática Forense II (Prueba Indiciaria Informático Forense) referente a la Captura/Adquisición de las evidencias tratando de no alterarlas o dañarlas en la que se mantiene la integridad de la evidencia obtenida y se establece la cadena de custodia. En el tercer capítulo se versará sobre los protocolos detallados en la toma de decisiones de cada una de las fases en el Análisis Forense Informático.

Capítulo I

Introducción al análisis forense informático

CAPÍTULO I

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 ésta 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, 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 reconoci-

dos 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).

1.2.3. 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 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 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 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, 2013).

1.4. Metodología para el Análisis Forense de Evidencias Digitales

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

- 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.

- 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 proce-

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

- 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.

- 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.

- 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.

- Preservación de la evidencia

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

- 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.

- 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:

- 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.

- 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.

- 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 de 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.

- 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.).

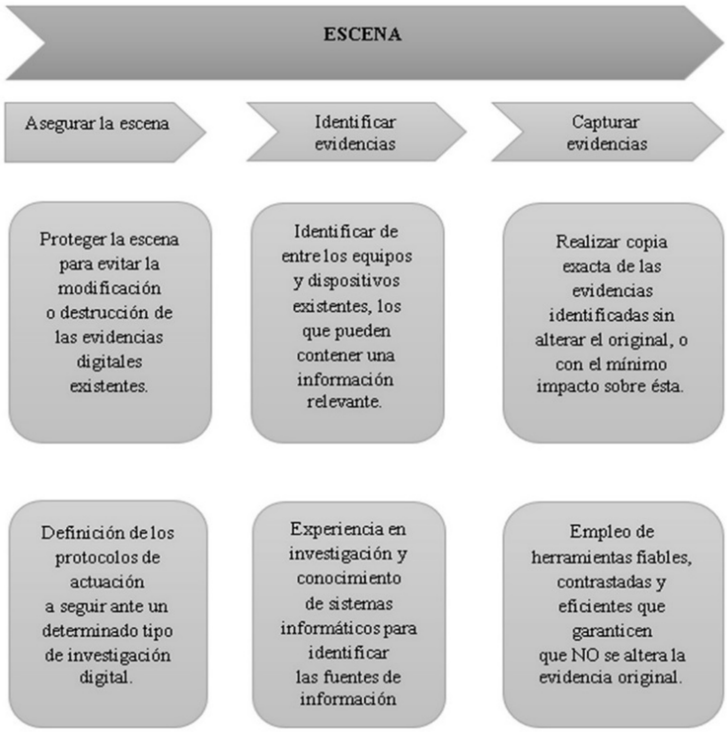


Fig. 1.1. Metodología para el Análisis Forense de Evidencias Digitales.

Capítulo II

Metodología aplicada en la informática forense II

CAPÍTULO II

Metodología aplicada en la informática forense II

En el presente capítulo se define la metodología y se toma en cuenta algunas las diferentes fases que se realiza en la misma, haciendo énfasis en la "Prueba Indiciaria Informático Forense", que tendría una aplicación operacional en cuanto a las cuestiones fundamentales en la fase de Captura/Adquisición, y en el desarrollo de ésta fase ayudará a los procesos que enfrenta un analista en informática forense. (Hidalgo Cajo, 2014)

Teniendo claro que en cada fase de la metodología forense se debe detallar, los procedimientos, técnicas, actividades y demás estrategias metodológicas requeridas, se ha desarrollado en la cada fase de la metodología los workflows respectivo, centrándonos en la fase de "Captura/Adquisición" los respectivos workflows necesarios para el desarrollo de la misma, se deberá indicarse el proceso a seguir en la recolección o captura de la información, así como en la organización, sistematización

y análisis de los datos.

A continuación, se describen las etapas de la metodología básica aplicada al peritaje informático, como se ilustra en la Fig. 2.1.

Fig. 2.1. Metodología de trabajo para análisis informático forense

Al respecto entre las diferentes actividades, el primer aspecto a tomar en cuenta es el análisis visual a cargo de la autoridad respectiva y el forense investigador, para estar en condiciones de documentar, todo lo que corresponde, orientando como primera seguridad que no haya alteración alguna de todo cuanto se relaciona con el objeto del acto ilícito y el estado del lugar donde se va a realizar el respectivo análisis forense.

2.1. Preservación

En la presente fase el análisis de la información digital exige preservar las evidencias (UNE-71506, 2013) originales para que éstas no pierdan en ningún momento su validez y confiabilidad y se debe garantizar la reproducibilidad de los estudios efectuados por cualquier entorno de análisis forense (López Delgado, 2007) o laboratorio designado para su análisis, caso de existir contraanálisis o contra-pericias sobre esta

misma información; en la Fig. 2.2., podemos observar los pasos de manera general de la Fase de Preservación de Análisis Forense.

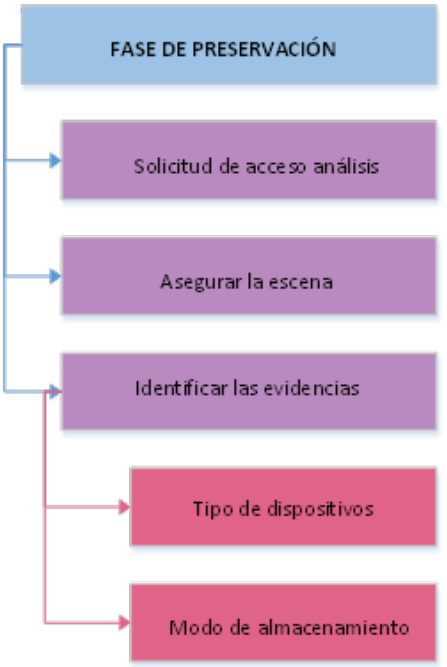


Fig. 2.2. Componentes Fase de Preservación

2.1.1. Definir debidamente el planteamiento del problema.

El perito en Informática Forense deberá ser un experto en la materia que podrá definir de una manera clara y concisa el motivo de su intervención, orientando a la autoridad competente sobre cómo debe plantear su discusión, así como haciéndole saber su competencia y límites

Para ello se tendrá que hacer lo siguiente:

- Identificar de forma general el tipo de intervención a efectuar.
- Razonar la información de interés (evidencia (Judicatura, 2020)) por parte de la autoridad competente y determinar si es competencia de la especialidad de informática o no; por ejemplo, se le solicita al analista forense informático analicé un CPU, (relacionado con la falsificación de documentos oficiales) a efecto de sustraer todos los documentos públicos y privados que se encuentran almacenados en su disco duro y determinar si son falsos. En este caso, al analista forense informático si le corresponde realizar la sustracción de to-

dos los formatos con tales características especificadas, pero no así el de determinar si son auténticos o falsos, y esto sería tarea de un especialista en documentos copia.

2.1.2. Valorar la disponibilidad de los recursos con los que se cuenta.

Es a partir de esta fase que el perito en analista Informático Forense: evaluará la disponibilidad de los recursos con los que cuenta y los que le serán necesarios, sean estos palpables o impalpables como el tiempo, esto es, a partir de esta etapa se estará en posibilidades de realizar un requerimiento pericial; es decir si lo que se solícita es viable o es demasiado subjetivo, por ejemplo si lo que se solicita es: determinar el deterioro de un software (ARIMETRICS, 2023), se le podrá solicitar que sea más objetivo el motivo de estudio o cuestionamiento.

Ahora, algunos de los recursos a evaluar dentro de esta actividad serán los siguientes:

- Recursos Humanos (factorial, 2023)
- Recursos Materiales (Guerrero Z y Flores H., 2009)
- Recursos Organizacionales (Escobar, 2010)
- Recursos Temporales (Zambrano, 2017)

Continuando con la Fase De Preservación de la evidencia (factorial, 2023), se debe determinar entre otras cosas el tipo de información que está disponible, así también como puede llevarse de manera segura y finalmente determinar que forma parte de la evidencia (Rodriguez Vega y Traipe Castro, 2023); entre las diferentes diligencias urgentes, ocupa el primer plano la realización de la inspección ocular a cargo de la autoridad competente u órgano investigador, para estar en condiciones

de documentar, todo cuanto le corresponde, disponiendo como primera medida que no haya alteración alguna de todo cuanto se relaciona con el objeto del acto ilícito y el estado del lugar donde se cometió.

Una vez que la autoridad competente ha adoptado todas las medidas adecuadas para que no se altere nada relacionado con el objeto del crimen y el estado del lugar donde se cometió, debe arbitrar los medios para facilitar la inmediata intervención del equipo de sus auxiliares directos (peritos, policía judicial, policía preventiva, servicio médico forense etc.), para que sean ellos los primeros en visitar la escena del delito en procurar de los indicios que les suministraron "los testigos mudos", tendientes a constatar que realmente se ha cometido un hecho considerado delictuoso por la legislación penal vigente y todo aquello que conduzca a la positiva identificación de su autor o autores.

Ese equipo de auxiliares del órgano investigador no actúa en forma indiscriminada, sino siguiendo un ordenamiento, que permita su actuación ponderable y eficaz para alcanzar el mejor de los resultados. A continuación, se hace referencia al orden de expertos que intervendrán bajo un hipotético casó (posterior a su denuncia), en que esté involucrado un medio informático, el orden será el siguiente:

- Perito Criminalista (Darahuge y Arellano González, 2014)
- Perito en Dactiloscopia (Darahuge y Arellano González, 2014)
- Perito Fotógrafo (Darahuge y Arellano González, 2014)

Después de estas intervenciones, entraría en escena el perito en Informática forense, si el caso involucra computadoras. En el caso de la realización de toma fotográfica este podrá solicitar todas las que la crea conveniente.

Satisfechas las tareas preliminares el perito en Informática Forense pro-

cederá a identificar los elementos que necesita para su caso (elementos de estudio); tener en cuenta que sin pruebas realmente lo que se tiene no es más que una opinión; para cada caso es diferente, así que es probable que se necesiten diferentes tipos de pruebas para cada proceso. Una premisa esencial es tomar todo lo necesario. Desafortunadamente, existen cuestiones legales y logísticas relacionadas con este enfoque. El perito en Informática Forense debe ser muy cauteloso en el ejercicio de sus funciones, por cuanto la extralimitación en el encargo pericial puede traducirse fácilmente en un delito electrónico.

Apegarse estrictamente a la cadena de custodia6, normas, así como etiquetar todo tal y como sea removido, conexiones etc.; en la Fig. 2.3. se muestra a manera de ilustración la variedad de dispositivo a analizar y en la Fig. 2.4., se ilustra una manera de cómo se identificaría a los diferentes dispositivos objeto de estudio:

Fig. 2.3. Variedad de dispositivo a analizar
Tomado de: https://elmundoecativodelfururo.blogspot.com/2015/11/34-dispositivos-de-almacenamiento.html

Fig. 2.4. Forma en que se identifica un posible material objeto de estudio, el mismo que será detallado en el respectivo documento Final. Tomado de: Metodología para el Análisis Forense Informático en Sistemas de redes y equipos de cómputo personal

Cuando se accede al lugar de los hechos o donde presuntamente se haya cometido algún delito, se deberá mirar todo cuidadosamente, partiendo del hecho de que ya, se hallan fijado los elementos de interés así como del visto bueno de la autoridad competente, solo así y haciendo uso de guantes de látex (Hobbs y Mann, 2013), cuando se estará en condiciones para tomar algún objeto, con el fin de recabar algún dato relevante tal como: el número de serie del equipo de cómputo, modelo, etc.; como se observa en la Fig. 2.5.

Hay que considerar que el lugar de los hechos se clasifica en tres tipos; de acuerdo con sus condiciones y características pueden ser:

- Lugares cerrados
- Lugares abiertos, y
- Mixtos

Fig. 2.5. Posible lugar de los hechos a realizar la investigación respectiva. Tomado de: Metodología para el Análisis Forense Informático en Sistemas de redes y equipos de cómputo personal

De manera posible siempre documentar el lugar de los hechos con toma fotográfica o video, a este proceso se le llama fijación (Fig. 2.6.). No debe olvidarse que los buenos objetivos no sustituyen a la experiencia y al adiestramiento; la fotografía adecuada en este tipo de trabajo requiere la intervención de un experto provisto de un equipo adecuado. Es preferible esperar una o varias horas y lograr su cooperación a confiar en una persona sin

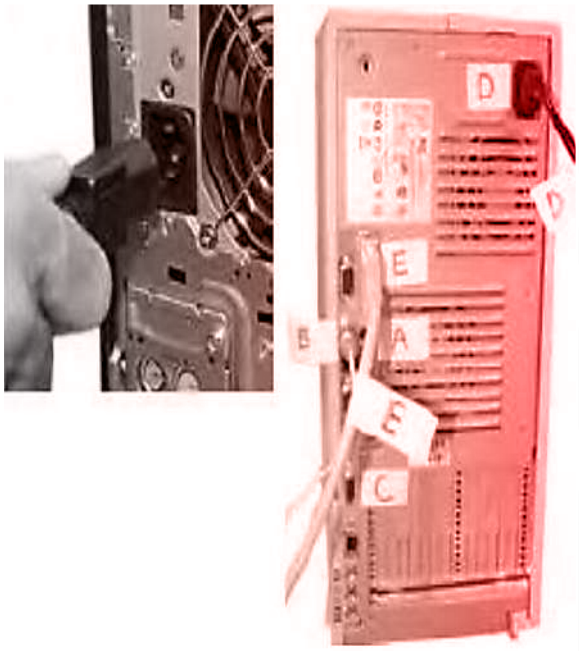


Fig. 2.6. Imagen en la que se ilustra una posible manera de etiquetar las conexiones de un equipo de cómputo a analizar. Tomado de: Metodología para el Análisis Forense Informático en Sistemas de redes y equipos de cómputo personal

experiencia.

El registró y documentación fotográfica de una escena del delito y sus proximidades, debe hacerse cubriendo las mismas etapas señaladas al hablar de los procedimientos escritos; tal operación debe llevarse a cabo desde afuera hacia adentro y en sentido de las agujas del reloj, en forma piramidal, tratando de documentar todas las etapas cubiertas por el delincuente.

Se debe realizar dibujos, croquis o bocetos de conexiones, y escritos haciendo descripciones de lo que se vea (por ejemplo si un equipo se encuentra en tal recámara o área de estudio, apagado o encendido si es esto último que programas se están ejecutando o cuales archivos fueron los más recientes etc.), de igual manera se tendrá que tener en cuenta alguna nota al lado del teclado o cercano al equipo de cómputo donde posiblemente exista información relacionada con la investigación o contraseñas.

Las notas que se tomaron y fotografías (de preferencia con una cámara digital del archivo o archivos se deberán obtener su hash (Hobbs y Mann, 2013) o dibujos, juntos forman la primera encuesta sobre el sitio. Conforme avance la investigación esta información recabada nos dará más pistas sobre donde poder buscar más evidencias (Judicatura, 2020), por ejemplo, el mouse se encontró en posición para zurdos, hora en el sistema bajo estudio, hora en la que se efectúo la diligencia etc.

2.2. Captura/Adquisición

En la presenta fase se debe definir los equipos y herramientas determinadas para llevar a cabo la investigación y lograr un entorno de trabajo adecuado para el análisis y la investigación; para lo cual se procederá a seguir los pasos que se ilustra en la Fig. 2.7.

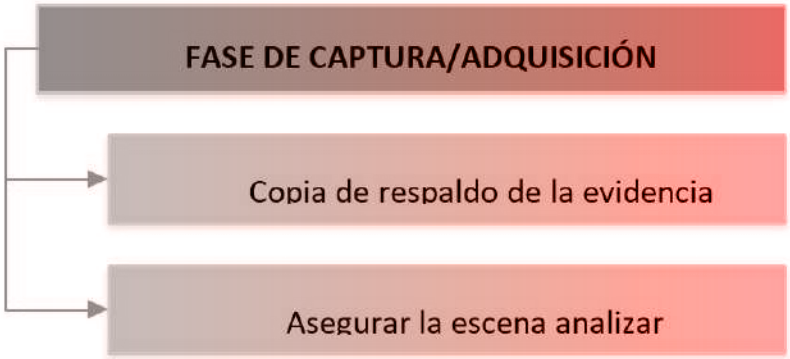


Fig. 2.7. Componentes Fase de Captura/Adquisición

Inicialmente, se inicia una secuencia de pasos que nos permita documentar de manera precisa de identificar y autenticar los datos que se recogen, tipo:

- ¿Quién realiza la acción y por qué lo hicieron?
- ¿Qué estaban tratando de lograr?
- ¿Cómo se realiza la acción, incluidas las herramientas que utilizaban y los procedimientos que siguieron?
- Cuando se realizó la acción (fecha y hora) y los resultados.

De igual forma, se toman otras fuentes de información de los sistemas vivos, los datos volátiles como:

- Cache del Sistema
- Archivos temporales
- Registros (Cedeño Barcia y Pacheco Cervantes, 2017) de sucesos.
- Registros (Cedeño Barcia y Pacheco Cervantes, 2017) de internos y externos que los dispositivos de red, tales como firewalls (Smith y Petreski, 2008), routers (Muñoz, 2021), servidores proxy, etc.

- Logs del sistema, Aplicaciones.
- Tablas de enrutamiento (Arp (Address Resolution Protocol), cache de Netbios, lista de procesos, información de la memoria y el kernel)
- Registros remotos (Winter, 2017) e información de monitoreo relevante

Realizar copia imagen de los dispositivos (bit a bit), con una herramienta apropiada y firmar su contenido con un hash (Hobbs y Mann, 2013) de MD5 o SHA1, generando así el segundo original, a partir de este se generarán las copias para el Análisis de datos, cada copia debe ser comprobada con firmas digitales nuevamente de MD5 o SHA1. Documente la evidencia (Triana-Fuentes y BALLESTEROS-RICAURTE, 2016) con el documento del embalaje (y cadena de custodia (Solana Aguilar y Flores Aguilar, 2023)) que puedan garantizar que se incluye información acerca de sus configuraciones. Por ejemplo, anote el fabricante y modelo, configuración de los puentes, y el tamaño del dispositivo. Además, tenga en cuenta el tipo de interfaz y de la condición de la unidad; aquí es importante considerar las buenas prácticas para conservar la información y la evidencia (Judicatura, 2020).

- Asegurar de manera física un lugar para almacenar los datos, evitando su manipulación. No olvide documentarlo.
- Proteger los equipos de almacenamiento de los campos magnéticos (estática).
- Realice mínimo el segundo original y una copia del segundo original para el análisis y almacene el segundo original en un sitio seguro
- Hay que asegurar que la evidencia (Judicatura, 2020) está protegido digital y físicamente (por ejemplo, en una caja fuerte, asignar una contraseña a los medios de almacenamiento).

- Nuevamente, no olvide actualizar el documento de Cadena de custodia (Solana Aguilar y Flores Aguilar, 2023) (incluye información como el nombre de la persona que examina la evidencia (Judicatura, 2020), la fecha exacta y el tiempo que echa un vistazo a las pruebas, y la fecha exacta y hora en que lo devuelva).

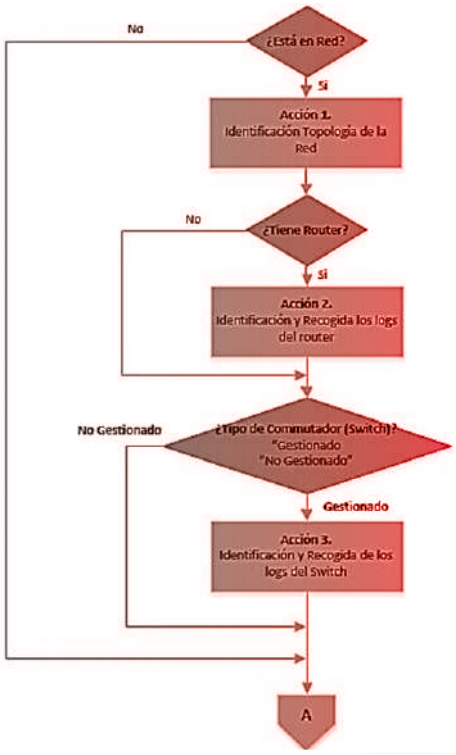


Fig. 2.8. Captura/Adquisición

Se pretende que esta información sea:

- Auténtica
- Correcta
- Completa
- Convincente

Los pasos para realizar la Captura/Adquisición en los diferentes escenarios se ilustra en la siguiente Fig. 2.8.:

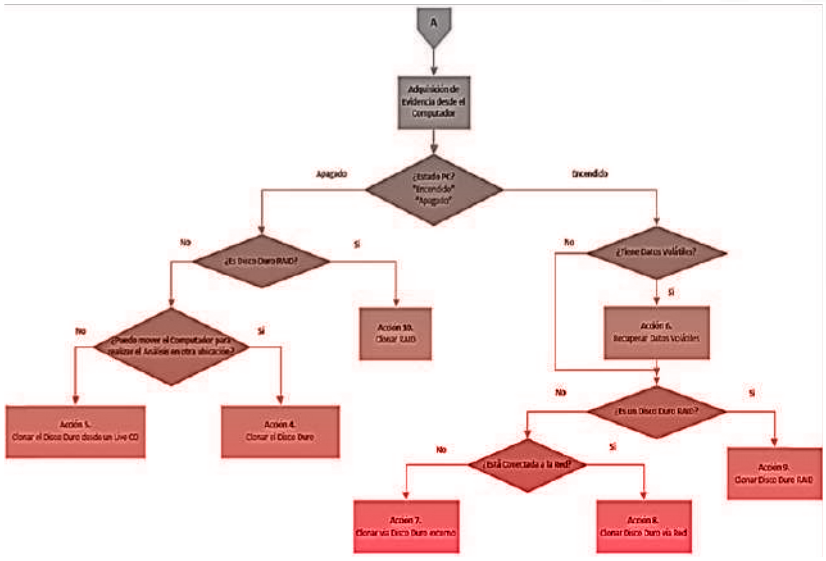


Fig. 2.8. Captura/Adquisición

2.3. Análisis

La Fase de Análisis tienen como fin dar respuesta a preguntas relacionadas con el tiempo de intrusión, su origen, lista de sistemas afectados, métodos de intrusión usados, así como la lista de activos alterados y/o accedidos, y cualquier otra actividad realizada; Las tareas a seguir en la etapa de Análisis son las que se ilustra en la Fig. 2.9.

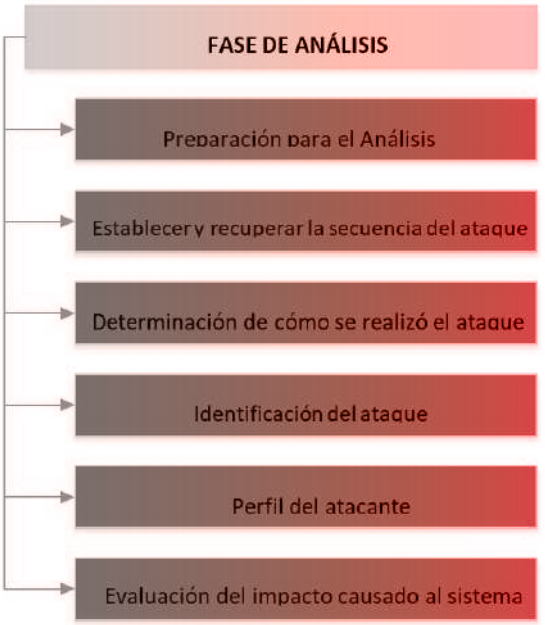


Fig. 2.9. Componentes Fase de Análisis

- Se debe dar una orientación sobre aquellos aspectos relacionados con los requisitos a cumplir por parte del personal técnico, equipos y documentación
- Tareas metódicas, auditables, repetibles y defendibles

Acciones previas:

- Comprobar que el objeto y alcance de lo que se precisa estudiar está dentro de la competencia del laboratorio o entorno forense;
- Estudiar la documentación adjunta a las evidencias electrónicas para componer un mapa contextual de las mismas, estableciéndose las relaciones que pudiera haber entre las distintas evidencias electrónicas entre sí y de éstas con los distintos actores implicados;

- Supervisar la cadena de custodia (Sánchez Cordero, Introducción al Análisis Forense Informático, 2014) previa hasta la llegada de las evidencias (Judicatura, 2020) al entorno de análisis forense (CASEY, 2005) (qué, quién, dónde y cuándo). Identificación del responsable y lugar de almacenado hasta su llegada al lugar de análisis;
- Solicitar las autorizaciones necesarias, según la legislación vigente a nivel
- Comprobar que las evidencias (Judicatura, 2020) no están deterioradas y son susceptibles de su estudio forense;
- Es posible que aparezcan nuevas evidencias (Judicatura, 2020) que no habían sido contempladas en un principio durante la toma u obtención de las mismas allí donde estaban ubicadas originariamente (ej. aparición en los distintos dispositivos lectores/grabadores de los equipos informáticos, de tarjetas de memoria, CD, disquetes, etc.). Debe iniciarse nuevamente la reseña de éstas, generándose un nuevo proceso de gestión, custodia y trazabilidad63 de estas evidencias (Judicatura, 2020) según la Norma UNE 71505. Se debe notificar de forma oportuna la existencia de las mismas a quién solicitó el análisis del resto, requiriendo los permisos correspondientes para su estudio, en caso de ser necesario;
- Especificar la hora de la BIOS del equipo informático donde van instalados los distintos discos duros o soportes digitales que contienen la información de interés, a los efectos de poder ser comparada con la fecha del momento en que se active el análisis forense de la información;
- Establecer criterios de prioridades

2.4. Reporting

En la presente fase debe ser todo documentado y con la fecha respectiva desde que se descubre el evento hasta que finaliza el proceso de análisis forense, con esto permitirá ser más eficiente y efectivo al tiempo que se reducirá las posibilidades de error al momento de formalizar los reportes respectivos; el respectivo Reporting considerado será como se ilustra en la Fig. 2.10.

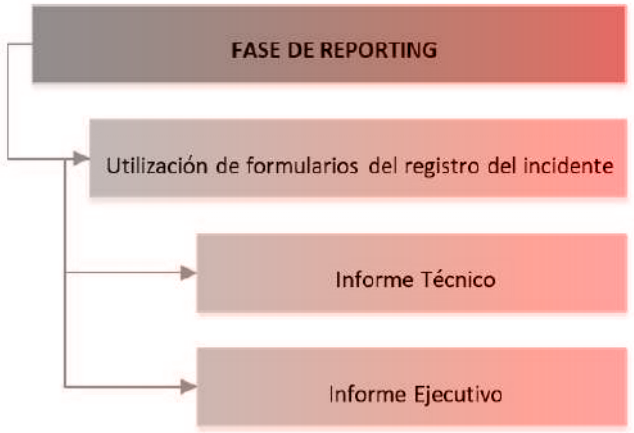


Fig. 2.10. Componentes Fase de Reporting

2.4.1. Presentación resultados

- El análisis forense realizado se debe materializar en un informe pericial (Darahuge y Arellano González, 2014), el cual debe compaginar los términos técnicos con un lenguaje de fácil comprensión dirigido al organismo o entidad que solicitó dicho estudio
- Una vez redactado el informe pericial (Darahuge y Arellano González, 2014) correspondiente, se deben devolver al organismo solicitante del estudio los equipos y soportes digitales estudiados, yendo estos acompañados del correspondiente recibo o documento de control de evidencias (Judicatura, 2020).

- Se mantiene la trazabilidad (Medina et al., 2017) y se transfiere la cadena de custodia6 de las evidencias (Judicatura, 2020)

A continuación, se ilustra la Estructura del Informe en base a la Norma UNE 197001 de AENOR de España.

• **Base**: Norma UNE 197001

• **Estructura**:

o **Asunto**: Se deben especificar los estudios solicitados, identificación del entorno de análisis forense (Sánchez Cordero, Introducción al Análisis Forense Informático, 2014) o en su caso, laboratorio que emite el informe y los datos identificativos de forma nominal de los peritos que han efectuado el análisis de los distintos soportes digitales, reseñando igualmente la fecha de inicio y fin de estos estudios.

o **Evidencias/muestras recibidas**: Reseña de todas las muestras (Cadeño Andalia et al., 2005) objeto de análisis, las cuales se deben visualizar en un Tabla fotográfico o videográfico que debe acompañar al cuerpo del informe en una Tabla.

o **Estudios efectuados sobre las evidencias**: Es la parte principal del informe. Debe incluir:

o Descripción del proceso de clonado (Santo Orcero, 2001) bit a bit de la información original (Pérez-Teruel et al., 2014) o procedimiento seguido para obtener los datos copia que han servido para el estudio de las evidencias (Judicatura, 2020).

o Análisis de las particiones y sistemas de ficheros.

o Proceso de recuperación de archivos borrados, si ha lugar.

o Estudio del sistema operativo y usuarios del mismo.

o Estudio de la seguridad implementada.

o Análisis detallado e individualizado, para cada soporte digital, de los indicios encontrados de interés de las distintas evidencias electrónicas. Se deben reseñar a lo largo de este análisis, en las Tablas correspondientes, los indicios encontrados perfectamente clasificados, con sus rutas de ubicación en los soportes originales.

• Situación final de las evidencias: Especificar el destino final que se dará a las evidencias (Judicatura, 2020) una vez concluido su análisis, reseñando para todas ellas el medio utilizado para la puesta a disposición del organismo o entidad solicitante de esta pericial

• Conclusiones: Los resultados del informe pericial (Darahuge y Arellano González, 2014) deben de responder a las expectativas de quien lo solicitó, siendo claros y concisos. Para ello se debe usar un lenguaje llano sin tecnicismos ni ambigüedades

• Tablas: Toda la información de interés se debe adjuntar en las correspondientes Tablas, bien en formato papel o en formato electrónico. En este último caso, a los soportes con los datos de interés se les debe realizar un resumen digital o “hash” (Dominguez Perez et al., 2019) para garantizar la no alterabilidad de los mismos.

Capítulo III

Protocolos detallados en la toma de decisiones de cada una de las fases en el análisis forense informático

CAPÍTULO III

Protocolos detallados en la toma de decisiones de cada una de las fases en el análisis forense informático

En el presente capítulo se define los Protocolos de manera detallada en la toma de decisiones en la fase de Análisis/Captura en la "Prueba Indiciaria Informático Forense", en los diferentes procesos que enfrenta un analista en informática forense.

3.1. Preservación

En esta fase se llevará a cabo la delimitación clara y precisa del objeto de la investigación; es decir consiste en revelarle al perito en Informática Forense si su proyecto de investigación es viable, dentro de sus tiempos y recursos disponibles (Bordón y Crespo, 2022).

Llevar a cabo la Preservación del material objeto de estudio, el conocer los datos, donde están localizados y cómo están almacenados:

Ahora, se describirá las actividades de esta fase con mayor detalle:

De lo expuesto con antelación se puede expandir que la presente fase permite tener un panorama general del caso a investigar; por lo que se deben de realizar las acciones que a continuación detallo, presentándolas de forma desglosada y ordenada para una mejor apreciación:

3.1.1. Asegurar el material motivo de estudio y consideraciones generales.

Se refiere a que todo material que sea considerado como evidencia (Judicatura, 2020) se deberá resguardarse adecuadamente bajo las más estrictas medidas de seguridad.

- *a. Establecer el perímetro o área de protección del equipo equipos afectados.*

En esta actividad es evitar que la evidencia (Judicatura, 2020) original sea alterada por las personas que intervienen en el lugar de los hechos o bien ajenas a esta Fig. 3.1.

Fig. 3.1. Se debe prohibir el acceso al lugar de los hechos al personal no autorizado al mismo

- *b. Tener la capacidad para poder determinar lo que ha sucedido y reconstruir los hechos.*

Es imprescindible estudiar el lugar del hecho, así como la recolección de todos los indicios, lo cual es materialmente imposible cuando el sitio del suceso no ha sido protegido y conservado adecuadamente, por lo que se deberá restringir el acceso al lugar de los hechos, tanto de personas, como de acceso a otros equipos.

- *c. Preservar toda impresión dactilar ubicada en el lugar de los hechos (huella dactilar latente).*

Nos permitirá facilitar la identificación del supuesto sospechoso o sospechosos. Razón por la cual es recomendable el uso de guantes de látex (Adams R. , 2012), con el fin de evitar contaminar los equipos o dispositivos a ser investigados

- *d. Emplear brazaletes antiestáticos.*

Nos permite evitar alterar la evidencia (Judicatura, 2020) por cargas electrostáticas de aquellas personas que manipulen los equipos o dispositivos, para lo cual será conveniente contar con bolsas antiestáticas para un adecuado y seguro embalaje de la evidencia (Judicatura, 2020)

- *e. Determinar el incidente ocurrido y de su impacto.*

Es con el fin de proveerle a la autoridad competente de una idea general de lo acontecido y tratar de determinar el tipo de incidente suscitado de acuerdo a la experiencia del investigador en informática forense, de esta manera el jefe de la investigación podrá determinar el rumbo que tome la misma

- *f. Considerar todos los componentes que pueden estar relacionados de alguna forma con la computadora y/o elemento cuestionado.*

Se deben considerar todos los elementos relacionados con la especialidad informática y que forman parte de la cadena de eventos que conducen al hecho denunciado, ya que, con la unión de todo el equipo involucrado, se incrementa el área para realizar la investigación, es decir con mayor información proporcionada y obviamente obtener más evidencias (Judicatura, 2020) durante el caso a investigar

- *g. Conocer las fortalezas, debilidades y otros conocimientos relacionados a las fuentes, incluyendo factores humanos y electrónicos.*

Ahora se estará en la posibilidad de identificar el área probable donde se pudo haber presentado el incidente y dar una respuesta acertada a lo ocurrido, está información se le proporcionará ya una idea al titular de la investigación del tiempo que requiere el análisis que está solicitando.

- *h. Estar consciente de las limitaciones de sus capacidades científicas, técnicas o temporales ante el caso expuesto.*

De esta manera se podrá evitar que la evidencia (Judicatura, 2020) sea alterada por el mal manejo de está (por ejemplo, si no se cuenta con material adecuado para respaldar la información), así como el de obtener resultados poco confiables o no tenerlos en tiempo y forma, considerando que muchas veces se contará con sospechosos detenidos relacionados con los hechos que se investigan.

- *i. Realizar una evaluación de los recursos (en el ámbito de la información y acceso a la misma, por ejemplo, la determinación del origen de una intrusión en un pc), alcance y objetivos necesarios para realizar la investigación*
- *j. Contar con un laboratorio de informática forense que permita realizar el proceso de obtención y análisis.*

Esto con la intención de dar un alto valor a la evidencia digital entrega-

da en lo que se refiere a su manejo y custodia, es recomendable tener un área de acceso restringido con caja fuerte para el resguardo del material motivo de estudio. Debe considerarse, además, que la información digital es sensible a la temperatura, y en algunos casos a los campos electromagnéticos.

- *k. Obtener por escrito la autorización para iniciar la intervención pericial en Informática Forense, (ya sea por parte de la juez o del dueño del equipo cuestionado).*

- *l. Documentar todas las acciones y antecedentes que preceden la Investigación. Los acontecimientos y decisiones que se adoptaron durante el incidente y su respuesta al incidente.*

Esto determinará el curso de acción a seguir en la Investigación. Se deberá anotar la fecha, la hora exacta en que se recibió la llamada solicitando la intervención pericial en informática, medio por el cual se recibió la llamada. Al llegar al lugar de los hechos se deberá anotar: la hora exacta de llegada, la dirección correcta, nombre de la autoridad que encabeza la investigación y la persona que le pone a la vista el equipo cuestionado (Adams R. , 2012)

- *m. Organizar y definir el equipo de Investigación.*

Establecer límites, funciones y responsabilidades (por ejemplo, en el caso de intrusión en un pc, contar con un oficio emitido por la autoridad competente en la que se autorice la intervención del pc; para lo cual será indispensable que de fe la autoridad competente o él dueño de la misma (esto es que la autoridad se encuentre presente y que tal acción obre en el expediente), para validar el análisis efectuado

- *n. Realizar una Investigación preliminar.*

Esta misma que se podrá incluir en el Dictamen en Informática en un

apartado como Antecedentes (documentar) que le permita describir la situación actual, si se realizó un traslado a un lugar, que persona lo atendió, quien le puso a la vista el equipo, hechos, las partes afectadas, posibles causantes, gravedad y criticidad de la situación, infraestructura afectada, para lograr una compresión total y mejor de la situación actual del incidente y definir un curso de acción acorde a la situación (Baryamureeba y Tushabe, 2004)

- *o. Analizar el Impacto de los negocios a través de la investigación del Incidente.*

Esto cobra relevancia en los casos en donde el incidente afecta a empresas las cuales sufren de tiempos de inactividad o sufren la perdida u ocultación de información confidencial o la intrusión en el pc. De igual manera resulta importante el determinar el posible costo de un equipo afectado o dañado.

- *p. Identificar la topología de red (Berón et al., 2004) y tipología de red, equipos afectados (servidores, estaciones de trabajo, Sistemas Operativos, Router, Switches (Jaime Toruño et al., 2015), etc.).*
- *q. Identificar los dispositivos de almacenamiento o elementos informáticos.*

Tales dispositivos de almacenamiento pueden ser: Discos Duros, Pen drive, memorias, tarjetas Flash, Zip Disk, Discos Ópticos CDs y DVDs, Disquetes, etc., que se consideren comprometidos o cuestionados y sean determinados como evidencia (Judicatura, 2020), su marca, modelo, características, seriales, etc.; así como fijarlos fotográficamente, como se ilustra en la Fig. 3.2.

Fig. 3.2. Fijación fotográfica del material objeto de estudio, teniendo mayor relevancia el disco duro asociado a la computadora cuestionada

- *r. Ejecutar adecuadamente los procedimientos sobre sistemas vivos; para no perder la continuidad en producción de los equipos y su uso en las instalaciones, evitando la pérdida de los datos volátiles. Es decir, se procederá de acuerdo con el criterio del forense informático acorde a las circunstancias*
- *s. Identificar los posibles implicados o funcionarios que tengan relación con la investigación o que pudieran aportar mayor información. En este punto bien cabe la posibilidad de efectuar entrevistas, ya sea con usuarios o administradores responsables de los sistemas (administrador en general), documentar todo y tratar de lograr un conocimiento total de la situación*
- *t. Realizar una recuperación de los logs de los equipos de comunicación y dispositivos de red, involucrados en la topología de la red.*
- *u. Responder a las preguntas: ¿Dónde?, ¿Cuándo? y ¿Quién es el primero que tiene la evidencia (Judicatura, 2020)?*
- *v. Responder a las preguntas: ¿Dónde?, ¿Cuándo? y ¿Quién examinó la evidencia (Judicatura, 2020)? (Si anterior a nuestra intervención, intervino alguien más, por ejemplo, la policía cibernética).*

- *w. Responder a las preguntas: ¿Quién va a tener custodia de la evidencia (Judicatura, 2020)? y ¿Por cuánto tiempo la tendrá? Documentar a detalle cada acción.*
- *x. Responder a las preguntas: ¿Quién? y ¿Cómo se embaló y/o almacenó la evidencia (Judicatura, 2020)? Documentar de manera detallada cada caso.*

Documentar turno, personal que está preservando la evidencia (Judicatura, 2020).

Ahora se realizará una evaluación del caso:

Aquí el perito en Informática forense valora la información por su importancia la evidencia (Judicatura, 2020)

- *a. Situar el estado del caso que el perito en Informática Forense investigará. Aquí se determina qué sentido tomará la investigación, definiéndose si es simplemente la violación de una política, normas, lineamientos o bien se trate de un delito*

1. Conocer detalles sobre el caso.

El investigador forense antes de llegar a la escena del delito donde se presentó el incidente debe conocer la mayor cantidad de detalles, tanto del área, equipos, personal, sistemas operativos que se manejan (plataforma), dispositivos, etc., para saber ante que se encontrará y acudir con la herramienta y software (López Luque, 2019) necesario para la investigación.

2. Definir el tipo de evidencia (Judicatura, 2020) a manejar.

Se refiere al tipo de dispositivo o equipo a investigar, por ejemplo: CD, DVD, disco duro, USB, computadoras, por ejemplo, hacer la diferencia entre un chip y una micro memoria para equipo fotográfico, etc. Ele-

mentos que podrían estar relacionados de alguna forma con los hechos a investigar.

3. Evaluar de manera inicial respecto al caso.

Esto se refiere a que los forenses informáticos, deben hacer preguntas a las personas relacionadas con el caso, a los administradores de red y a los encargados de seguridad para posteriormente documentar las respuestas obtenidas y relacionarlas o vincularlas con el incidente. Por ejemplo, si para la realización de una acción determinada basta con una cuenta de usuario o se tienen otros candados u otras cuentas para autorizar tal acción.

4. Rastrear fuentes de información en la estructura organizacional.

- Perfiles de usuario.
- Investigación en progreso de un determinado lugar o un análisis nuevo. Se deben de verificar las políticas de uso de equipos o dispositivos de cómputo, así como manuales operativos, para determinar los perfiles de usuarios y verificar que pueden o no hacer, así como también, ver quiénes pueden acceder al sistema de manera remota, y con esto delimitar el área de investigación o determinar otra área para llevarla a cabo. Lo anterior, se ve claramente en los casos de intrusión en un pc.

5. Ubicar, ¿Cuáles son las fuentes de información?

Localización lógica o física de la evidencia (Judicatura, 2020). El perito en Informática Forense puede hacer uso de alguna herramienta gráfica, ejemplo: un administrador de archivos (previa utilización de un bloqueador de escritura, para no alterar los metadatos 28 de los archivos), un visualizador de archivos, etc. usados normalmente en una computadora, un análisis físico desde el punto de vista forense es puramente

físico, en este no se considera el sistema de archivos (Adams R. , 2012). Se debe de determinar donde se ubica la evidencia (Judicatura, 2020) que se está buscando, por ejemplo, si fue cometido el delito por la intrusión de información en un pc.

6. Identificar las fuentes de información

Tanto de personas, como de aquellas que se encuentran almacenadas de manera lógica. Se realiza para delimitar el área de búsqueda.

7. Determinar el diseño preliminar o enfoque del caso.

En este punto se prepara un resumen general para hacer la investigación de manera acotada (podría servir como un avance de Dictamen Pericial) (Carrier y Spafford, Fall 2003)

8. Fijar el lugar de los hechos con toma fotográfica y grabaciones de diferentes ángulos

En el área del lugar de los hechos antes de la recolección de la evidencia (Judicatura, 2020). Esta acción se hace para verificar en ellas si algo no fue considerado durante la intervención pericial y además es de utilidad como evidencia (Judicatura, 2020) de lo encontrado

9. Fijar fotográficamente los periféricos (CASEY, 2005) (teclado, mouse, impresora, escáner, etc.), que se encuentran en el lugar de los hechos.

Ayuda a mantener una correlación de eventos y proporciona mayor oportunidad de encontrar la evidencia (Judicatura, 2020).

10. Fijar fotográficamente las conexiones físicas del equipo motivo de estudio.

Esto servirá para demostrar cómo se encontró el equipo a ser investigado.

11. Documentar la información observable.

Debe de anotarse de manera estructurada la información observable por parte del perito en informática forense, con la intención de juntar todas las ideas y escribir en el Dictamen pericial lo observado desde el inicio del proceso de la investigación.

12. Identificar si el equipo se encuentra encendido o apagado.

Ayuda a determinar los pasos a seguir para la etapa de obtención.

13. Reconocer el sistema operativo (sistema de archivos (Serna et al., 2012)) del dispositivo del cual se obtendrá la información.

Ayuda a determinar la estructura de archivos y permite definir el tipo de software (Rueda, 2009) a utilizar

14. Documentar la fecha y hora del sistema

Para demostrar la hora en la que se dio inicio a la investigación. Por ejemplo, si se trata de una intrusión en un pc chequear la zona horaria, está información cobra relevancia en los casos de alguna intrusión de otro lado del continente o en el caso en el que se discute la fecha de creación de un archivo.

15. Interrumpir las conexiones de la red de cómputo.

Se lleva a la práctica para evitar que alguien de manera remota altere la evidencia (Judicatura, 2020).

16. Realizar movimientos con el mouse (ratón) de forma periódica.

Lo anterior, siempre y cuando el investigador acceda a la escena del delito y el equipo de cómputo cuestionado se encuentre encendido. Considerar, que algunos equipos cuentan con contraseña en el protector de pantalla por lo que será necesario realizar movimientos de mouse a efecto de fijar la pantalla que se encuentra activa, así como programas

ejecutados y archivos abiertos, en la etapa de adquisición se describirá el orden de obtención de información volátil.

17. Preparar un diseño detallado.

- Ajuste a nivel detallado de las necesidades actuales.
- Consideración de la preparación del tiempo estimado, y los recursos requeridos para completar cada caso.

18. Determinación de recursos requeridos para la investigación con respecto al hardware (Rodríguez et al., 2014), software (Zambrano, 2017) y herramientas de informática forense

19. Marco legal relacionado al incidente

- Detalles generales a nivel internacional
- Detalles generales de la jurisdicción federal
- Detalles generales de la jurisdicción común

Este punto es muy importante, ya que deben considerarse antes de proceder con la obtención de información y ver a qué delito corresponde, así como si es de una jurisdicción común o federal.

Recordando que uno de los mayores inconvenientes que presentan los delitos informáticos es la frecuente extraterritorialidad que traen aparejados, ya que los delitos pueden ser cometidos por una persona que se encuentra físicamente en un país y los efectos pueden producirse en otro, instalando interrogantes sobre la autoridad competente para juzgar dichos delitos.

20. Enumerar los pasos a ser realizados durante la investigación, previa información obtenida.

Una vez asegurado el lugar de los hechos y obtenida la información

relacionada al incidente, se prepara el procedimiento a seguir para la obtención de información, cuyo propósito es poder reconstruir los eventos realizados durante la Fase de Captura/Adquisición, por lo que se requiere que éste sea documentado en cada uno de los pasos a seguir.

21. Corroborar diseño de investigación.

Se hace con el propósito de verificar que los pasos decididos son correctos, acordes y justificados con la situación del incidente.

22. Identificar el riesgo implicado.

Se orienta a que el forense informático debe documentar los problemas que espera encontrarse o que obliga a que puedan ocurrir, se podrá incluir en el correspondiente dictamen un apartado de consideraciones técnicas.

Por ejemplo; cuando el material motivo de estudio es la intrusión de un pc; para lo cual no se contó con las respectivas seguridades en la misma. El producto final de esta fase debe proporcionarle al peritaje que se está llevando a cabo, la información que permita definir un punto de inicio para la adquisición de datos y para la elaboración del documento final.

3.2. Captura/Adquisición

En esta Fase se procede a adquirir la evidencia (Judicatura, 2020) sin alterarla o dañarla, la misma que sea auténtica e igual a la original.

Aquí se juega un papel muy importante durante el proceso legal de la informática forense, en la que se mantiene la integridad de la evidencia (Judicatura, 2020) obtenida y se establece la cadena de custodia (Carrier y Spafford, Fall 2003) para demostrar el manejo que le fue dado a la evidencia digital por parte del forense informático que realiza la investigación.

Se deberán definir los equipos y herramientas determinadas para llevar a cabo la Investigación. Lograr un entorno de trabajo adecuado para el análisis y la investigación.

3.2.1. Efectuar consideraciones previas.

De no contar con lo necesario para conservar intacta la información digital y/o desahogar el estudio requerido (por ejemplo: si el perito en informática forense requiere para emitir su Dictamen, el acceso a algún equipo o base datos, se le deberá permitir el mismo), informarlo a la autoridad competente, suspendiendo por el momento el estudio requerido.

Se deberá tener especial cuidado en las implicaciones legales al intervenir y obtener información de un medio electrónico (el Ministerio Público tendrá que dar fe del análisis), así como el de no alterar los metadatos (Marciszack et al., 2009) de la información almacenada.

3.2.2. Instruirse de la mejor manera posible

Las condiciones que se presentan previas a la adquisición de la evidencia (Judicatura, 2020).

- Implicaciones legales de la adquisición de datos, (metodología aplicada en la obtención de información, para su debida legalidad y autenticidad).
- Documentar la cadena de custodia (Carrier y Spafford, Fall 2003).

El perito en Informática Forense, después de haber cubierto la Fase de Preservación, debe tomar en cuenta estas consideraciones para mantener la cadena de custodia (Carrier y Spafford, Fall 2003) y estar en posibilidades de garantizar la individualización, seguridad y preservación de los elementos materiales y evidencias (Judicatura, 2020) (en el caso

particular evidencia digital), recolectados de acuerdo a su naturaleza o incorporados en toda investigación, destinados a garantizar su autenticidad para los efectos del proceso.

3.2.3. Requisito por escrito la autorización, para realizar el análisis forense en informática

Este punto es recomendable que se tenga resuelto ya sea antes de proceder con la obtención de la imagen forense (CASEY, 2005) o bien antes de empezar con el análisis en vivo sobre el dispositivo informático analizarse.

3.2.4. Documentar la configuración y características del hardware del sistema

Este punto, tiene como fin el de lograr la plena identificación del material objeto de estudio, evitando con esto que se dude de la autenticidad de un equipo, dichas características deben de anotarse dentro del formato u oficio de la cadena de custodia (CASEY, 2005)

3.2.5. Elaborar el plan de adquisición de la evidencia digital

- Información adquirida a través de toma fotográfica.
- Información obtenida durante la intervención del perito en informática forense e investigación en curso.

En esta Fase se considera la metodología (métodos y/o técnicas), con la que se llevará a cabo la adquisición de datos, identificando que es lo

más conveniente de acuerdo con las características del incidente, priorizando la obtención de datos volátiles del dispositivo y posteriormente aquellos que no lo son.

Tomándose como base las condiciones presentes del equipo o dispositivos a ser analizados, se prepara la guía que determinará cuál será la fuente inicial de obtención de información, misma que tratará de no ser alterada por el perito en Informática Forense y debe considerar, además, que ésta puede variar de un momento a otro por los procesos que se están ejecutando dentro del equipo o dispositivo.

El orden que debe seguirse es de lo más volátil a lo menos volátil. Cabe señalar que al momento de obtener evidencia (Judicatura, 2020) de medios magnéticos tales como discos duros, será indispensable el uso de bloqueadores de escritura con el fin de preservar y no alterar la evidencia (Judicatura, 2020). Esto puede observarse cuando se accede a un archivo y se modifican sus metadatos (Marciszack et al., 2009) tales como la fecha de modificación.

Los pasos para realizar la Captura/Adquisición de Información para cada Escenario; lo detallamos a continuación:

Tabla 3.1. Identificación Topología de la Red

ACCIÓN 1 - TÍTULO: Identificación Topología de la Red
PROTOCOLO DE ACTUACION:
1. Identificar los diferentes componentes de red como son Router (donde se vaya a obtener información de los registros “logs”), switch, placas de interfaz de red (NIC), estaciones de trabajo (Pc); recursos y periféricos compartidos (impresoras y unidades de disco ópticos, los trazadores); medios de transmisión (cable de

transmisión, wifi, bluetooth).

2. Estructura de la red

3. Direccionamiento

- ¿Hay Sistemas de Monitorización y Seguridad?

  Si, Identificar el "Firewall" que usa, en:

  Hardware ¿Cuál es el hardware que usa?

  Software ¿Cuál es el software que usa?

  Identificar los IDS (Sistema de Detección de Intrusos) que usa, en:

  Hardware ¿Cuál es el hardware que usa?

  Software ¿Cuál es el software que usa?

  De aquí obtengo los logs o registros de red y las alarmas que generan.

- Hay monitores de tráfico de red (sniffer)

  Si, Ver los logs de acceso

COMANDOS DEL SISTEMA: Windows

Con NETSH que nos permite capturar tráfico de red Para iniciar una captura de tráfico solo es necesario ejecutar:

C:\> netsh trace start capture=yes tracefile=PathToFile

Donde **PathToFile** sea la ruta del archivo. ETL en que vamos a almacenar los datos capturados

- Para detener la captura de tráfico ejecutar

  C:\>netsh trace stop

Existen una cantidad de parámetros adicionales que podemos definir para personalizar la captura de acuerdo con las necesidades del caso, de los cuales los más comunes son:

- **maxSize=** (tamaño máximo del archivo.etl resultante expresado en MB, el valor por defecto es 250)

- **fileMode**=single|circular|append (define si utilizaremos archivos sucesivos o solo uno que se sobreescribe, en combinación con maxSize)

COMANDOS DEL SISTEMA: LINUX

Trabajar como [root]

[] tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [-C

file_size]

[-E algo:secret] [-F file] [-i interface] [-M secret]

[-r file] [-s snaplen] [-T type] [-w file]

[-W filecount] [-y datalinktype] [-Z user]

[expression]

-A: Imprime cada paquete en ASCII

-D: Imprime la lista de interfaces disponibles

-n: No convierte las direcciones de salida

-p: No utiliza la interfaz especificada en modo promiscuo

-t: No imprime la hora de captura de cada trama

-x: Imprime cada paquete en hexadecimal

-X: Imprime cada paquete en hexadecimal y código ASCII

-c count: Cierra el programa tras recibir 'count' paquetes

-C file_size

-E algo:secret

-F file

-i interface: Escucha en la interfaz especificada

-M secret

-r file

-s snaplen

-T type

-w file: Guarda la salida en el archivo 'file'

-W filecount

-y datalinktype

-Z user

COMANDOS DEL SISTEMA: Mac OS_X

Rastrear para capturar un paquete en OS X Lion y Mac OS X v10.6 Snow Leopard

Nombre del dispositivo BSD para la interfaz de AirPort es "en1", el Nombre del dispositivo BSD para Ethernet es "en0"

Si estás utilizando una interfaz de red AirPort, escribe o pega este comando (si utilizas un Mac Pro puede que necesites cambiar de en1 a en2):

[] sudo tcpdump -i en1 -s 0 -B 524288 -w

~/Desktop/DumpFile01.pcap

Si estás utilizando una interfaz de red Ethernet, escribe o pega este comando (si utilizas un Mac Pro puede que necesites cambiar de en1 a en2 como se mencionó anteriormente):

[] sudo tcpdump -i en0 -s 0 -B 524288 -w

~/Desktop/DumpFile01.pcap

Si estás utilizando una interfaz VPN, escribe o pega este comando:

[] sudo tcpdump -i ppp0 -s 0 -B 524288 -w

~/Desktop/DumpFile01.pcap

Terminal debería mostrar "tcpdump: listening on…". Accede a la función de red para la que deseas capturar y déjala que se ejecute hasta el final.

Una vez que se haya completado, regresa a Terminal y pulsa Control-C para completar la captura del rastreo de paquete.

En el escritorio aparecerá un archivo nombrado "DumpFile01. pcap" que contendrá el rastreo de paquete. Si deseas que se muestre el contenido, utiliza este comando en Terminal:

[] tcpdump -s 0 -n -e -x -vvv -r

~/Desktop/DumpFile01.pcap

Nota: para las capturas de rastreo de paquete posteriores, aumenta el número que aparece en el nombre del archivo, por ejemplo, DumpFile02.pcap, DumpFile03.pcap, etc.

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows:

- **Wireshark**

www.wireshark.org/download.html

Linux

- **Firewall Analyzer**

(http://www.manageengine.com/products/firewall/download.html)

Mac OS_X

- **Bastgille**

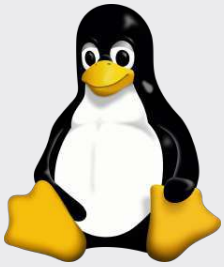
(http://bastille-linux.sourceforge.net/running_bastille_on.htm)

OTRAS HERRAMIENTAS FORENSES: Windows

- **Netcat** (http://joncraton.org/blog/46/netcat-for-windows/)
- **Putty** (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html)

- **pstools** (http://technet.microsoft.com/es-es/sysinternals/bb896649.aspx)
- **Nessus** (http://www.tenable.com/products/nessus/select-your-operating-system)
- **Snort** (https://www.snort.org/start/download)
- **Netcat** (http://joncraton.org/blog/46/netcat-for-windows/)
- **TCPDump / WinDump** (http://www.winpcap.org/windump/install/)
- **Fport** (http://www.mcafee.com/es/downloads/free-tools/fport.aspx)
- **Network Stumbler** (http://www.netstumbler.com/downloads/)
- **Sam Spade** (http://www.majorgeeks.com/files/details/sam_spade.html)
- **LibNet** (http://libnet.sourceforge.net/)

OTRAS HERRAMIENTAS FORENSES:
Linux



- **TCP Wrappers** (http://linux.softpedia.com/progDownload/tcpwrappers-Download-14011.html)
- **Tcptraceroute** (https://packages.debian.org/es/sid/tcptraceroute)
- **Caine** (http://www.caine-live.net/page5/page5.html)
- **Deft linux** (http://www.deftlinux.net/download/)

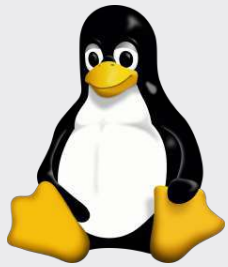
- **Hping2** (http://www.hping.org/download.html)
- **Lids** (http://www.lids.org/)

OTRAS HERRAMIENTAS FORENSES:

Mac OS X

- **Nessus** (http://www.tenable.com/products/nessus/select-your-operating-system)
- **wireshark** (http://www.wireshark.org/download.html)
- **Snort** (https://www.snort.org/start/download)
- **Hping2** (http://www.hping.org/download.html)

EJEMPLO:



Linux usando Wireshark

No permite esta herramienta administrar la red para comprobar el tráfico de paquetes y saber cómo gestionar una red.

Instalación:

Escribimos en una terminal; como se muestra en la Fig. 3.3.

```
sudo apt-get install wireshark
```

Fig. 3.3. Instalación de wireshark

Luego escribimos para arrancar la herramienta; como se muestra en la Fig. 3.4.

```
sudo wireshark
```

Fig. 3.4. Arrancar wireshark

Nos mostrará una ventana; como se muestra en la Fig. 3.5.

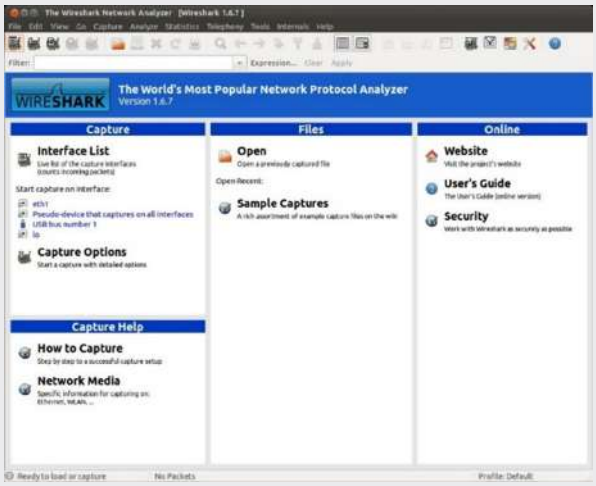


Fig. 3.5. Arranque de wireshark

Modo avanzado:

Podemos o especificar qué tipo de paquetes queremos capturar, (TCP, ARP, HTTP...) y especificar si queremos captar los paquetes de una red entera o de un host concreto.

Para ello debemos pulsar el segundo botón de arriba; como se muestra en la Fig. 3.6.

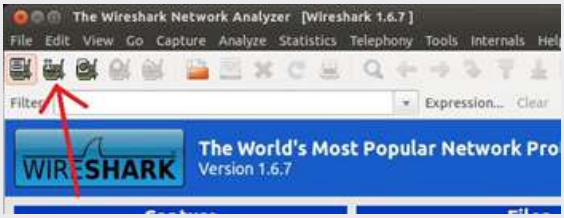


Fig. 3.6. Marcamos que paquetes queremos capturar

Al pulsar el botón indicado arriba nos aparecerá una ventana como la de la imagen de abajo, que nos permitirá elegir la tarjeta de red que queremos utilizar, el tipo de paquete, el destino; como se muestra en la Fig. 3.7.

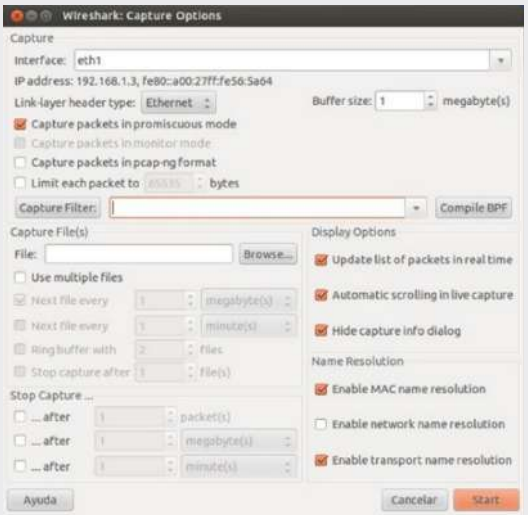


Fig. 3.7. Elegir el tipo de NIC, el tipo de paquete y destino que queremos capturar

Modo básico:

La otra opción más sencilla de empezar a capturar paquetes es pulsando en la ventana principal del programa, donde pone interfaz list, la interfaz que queremos utilizar, de ese modo directamente empezará a capturar todos los paquetes de la red donde se encuentre; como se muestra en la Fig. 3.8.

Fig. 3.8. Capturar paquetes de manera automática

Así es como nos mostrará los paquetes capturados; como se muestra en la Fig. 3.9.

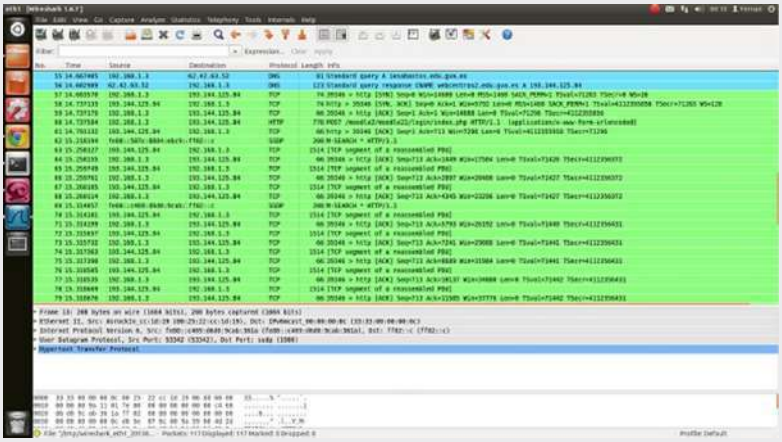


Fig. 3.9. Paquetes capturados con wireshark

Nota: Si lo que buscas son contraseñas, debes filtrar los paquetes http, y buscar la petición de login.

Se ha utilizado de ejemplo un moodle de una universidad de Ecuador (Espoch), no usa https, así que es posible capturar el usuario y la contraseña.

Primero filtrar los paquetes http escribiendo http arriba donde pone filter, y pulsando enter; como se muestra en la Fig. 3.10.

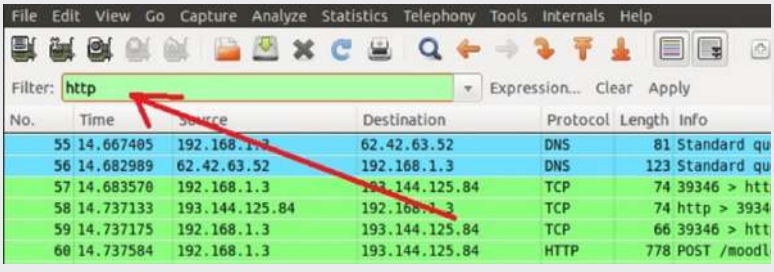


Fig. 3.10. Ejemplo de captura de usuario y contraseña de un usuario de una página web

Ahora buscar el paquete con el login; como se muestra en la Fig. 3.11.

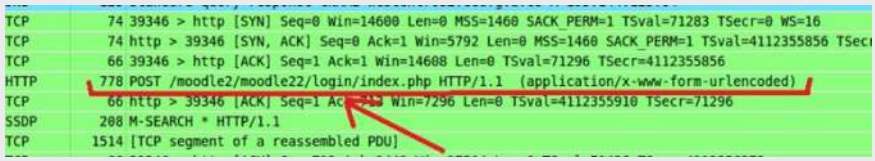


Fig. 3.11. Búsqueda del login de la web

Se selecciona, se le hace click derecho y se pulsa sobre Follow TCP Stream; como se muestra en la Fig. 3.12.

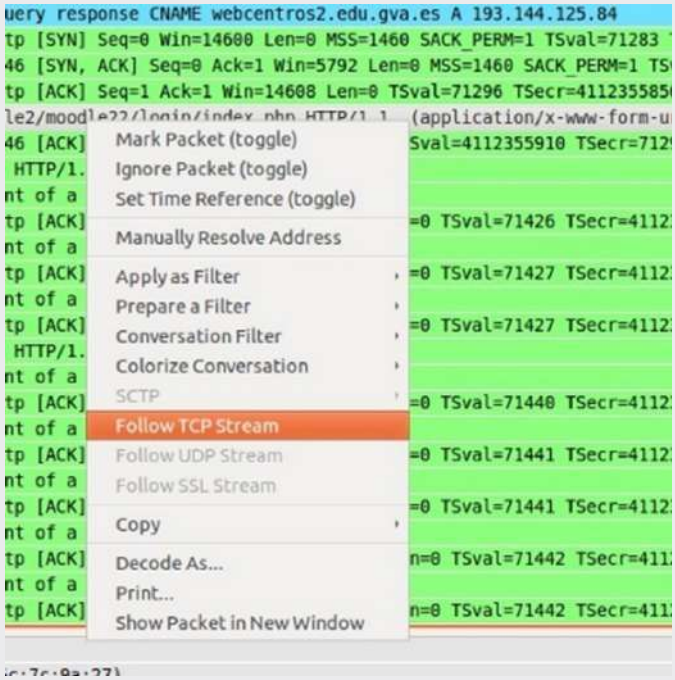


Fig. 3.12. Señalar con el click derecho sobre la dirección http

Abrirá una ventana con la de abajo donde nos aparecerá el login y la contraseña como se muestra en la Fig. 3.13.

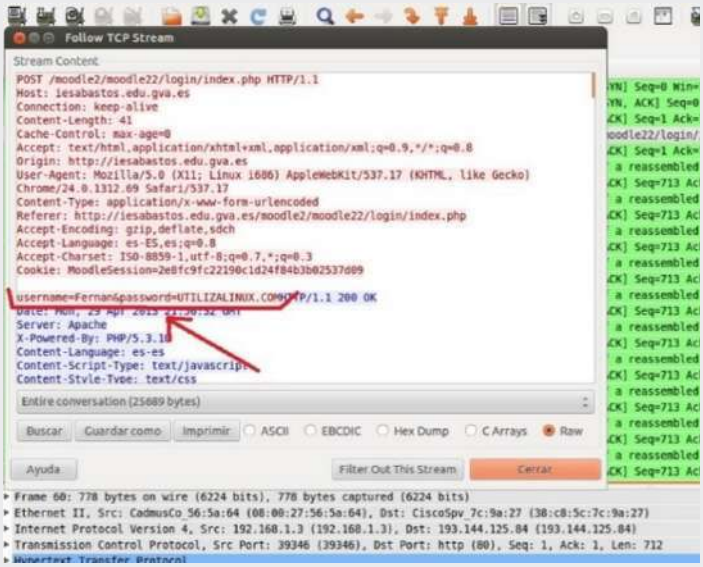


Fig. 3.13. Podemos observar el login y contraseña

Linux con comandos

Captura de paquetes

• Capturar tráfico cuya dirección IP de origen sea 192.168.3.1

[] tcpdump src host 192.168.3.1

• Capturar tráfico cuya dirección origen o destino sea 192.168.3.2

[] tcpdump host 192.168.3.2

• Capturar tráfico con destino a la dirección MAC 50:43:A5:AE:69:55

[] tcpdump ether dst 50:43:A5:AE:69:55

• Capturar tráfico con red destino 192.168.3.0

[] tcpdump dst net 192.168.3.0

• Capturar tráfico con red origen 192.168.3.0/28

[] tcpdump src net 192.168.3.0 mask 255.255.255.240

[] tcpdump src net 192.168.3.0/28

• Capturar tráfico con destino el puerto 23

[] tcpdump dst port 23

• Capturar tráfico con origen o destino el puerto 110

[] tcpdump port 110

• Capturar los paquetes de tipo ICMP

[] tcpdump ip proto \\icmp

• Capturar los paquetes de tipo UDP

[] tcpdump ip proto \\udp

[] tcpdump udp

• Capturar el tráfico Web

[] tcpdump tcp and port 80

• Capturar las peticiones de DNS

[] tcpdump udp and dst port 53

• Capturar el tráfico al puerto telnet o SSH

[] tcpdump tcp and \(port 22 or port 23\)

• Capturar todo el tráfico excepto el web

[] tcpdump tcp and not port 80

• Otra forma:

[] tcpdump tcp and ! port 80

Capturar todo el tráfico a host 10.168.1.100 puerto 80, en full verbose mode, full snap length, sin ponerla en modo promiscuo, sin convertir las direcciones de salida, imprimir en ASCII y volcar todo el dump en un file

[] tcpdump -vvv -n -s 65535 -A -p -w /tmp/tcpdump host 10.168.1.100 and port 80

Windows y Linux con Firewall Analyzer (Proxy Log Analyzer)

Analiza logs de firewalls, servidores proxy, IDS, IPS y VPN

Informes dinámicos

Los informes dinámicos muestran para cada dispositivo proxy el tráfico saliente mínimo, máximo y promedio durante períodos específicos. Es posible obtener la información sobre el tráfico del último día, semana, mes y año con una granularidad promedio de 5 minutos, 30 minutos, 2 horas y 1 día respectivamente.

El ancho de banda saliente se expresa en Kbps.

Informes de principales transmisores de información; podemos observar la Fig. 3.14.

Fig. 3.14. Informes de principales transmisores de información

Los informes de principales transmisores de información muestran cuáles son los principales hosts y usuarios que generan tráfico en LAN y WAN. Podrá detallar estos informes para saber cuáles son los principales sitios web, URL, y mucho más.

Informes de detalles de websites; podemos observar en la Fig. 3.15.

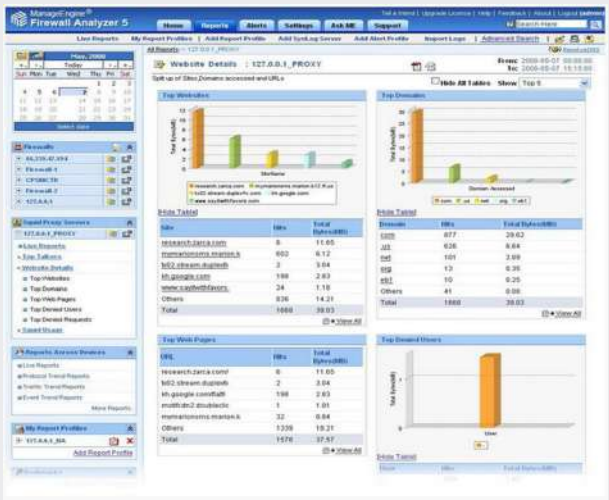


Fig. 3.15. Informes de detalles de websites

Los informes de detalles de websites dan a conocer los principales dominios, sitios web y páginas web a las que se accedió. Si detalla los gráficos podrá obtener más información de cada informe, por ejemplo, sobre principales usuarios, principales URL y códigos de caché de Squid.

Informe resumen de uso de Squid; podemos observar en la Fig. 3.16.

Fig. 3.16. Informe resumen de uso de Squid

El informe resumen de uso de Squid presenta información sobre el servidor proxy Squid. Podrá ver los principales códigos caché generados, códigos de estado peer y códigos de estado HTTP, y a su vez ampliar la información sobre hosts y URL que generan el código.

Tabla 3.2. Identificación y Recogida los logs del router

ACCIÓN 2 TÍTULO: Identificación y Recogida los logs del router

PROTOCOLO DE ACTUACION:

1. Identificar el modelo y fabricante del router

2. Identificar la dirección IP

3. Identificar la máscara de red

4. Acceder a recoger los registros o logs que tiene el router.

- Abrir sesión de un navegador de internet.
- Ingresar a la dirección IP del router a analizar
- Ingresar el nombre de usuario y contraseña
- Abrir la interfaz del router en la ventana del navegador de internet.
- Ingresar al menú del Router a la opción de “Registros” “Datos” u otro término similar en la interfaz basada en el navegador.

COMANDOS DEL SISTEMA: Windows:

C:\> ipconfig

Escojo donde dice “Puerta de enlace predeterminado”, copio y pego en mi barra de direcciones de mi navegador y me conduce a la configuración de mi router.

COMANDOS DEL SISTEMA: Linux:

Trabajar como [root]

[] netstat -rn

Escojo donde dice "Puerta de enlace predeterminado", copio y pego en mi barra de direcciones de mi navegador y me conduce a la configuración de mi router.

COMANDOS DEL SISTEMA: Mac OS X

[] netstat –rn

Escojo donde dice "Puerta de enlace predeterminado", copio y pego en mi barra de direcciones de mi navegador y me conduce a la configuración de mi router.

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **Pstools** (http://technet.microsoft.com/es-es/sysinternals/bb896649.aspx)

Linux

• **Coroner´s Toolkit(TCT)** (http://technet.microsoft.com/es-es/sysinternals/bb896649.aspx)

Mac OS_X

• **Wireshark** (http://www.wireshark.org/download.html)

OTRAS HERRAMIENTAS FORENSES:

Windows

• **pwdump3** (http://www.governmentsecurity.org/forum/topic/1037-pwdump3/)

• **Bastille** (http://bastille-linux.sourceforge.net/running_bastille_on.htm)

• **Hfnetchk** (http://www.petri.co.il/hfnetchk.htm)

• **snoop** (https://snoopwpf.codeplex.com/releases/view/87261)

Linux

• **Lids** (http://www.lids.org/)

• **Visual Route** (http://visualroute.en.softonic.com/mac)

• **Bastille** (http://bastille-linux.sourceforge.net/running_bastille_on.htm)

Mac OS_X

• **Bastille** (http://bastille-linux.sourceforge.net/running_bastille_on.htm)

EJEMPLO:

Router TP-LINK en Windows

Escribimos ipconfig y apretamos enter.

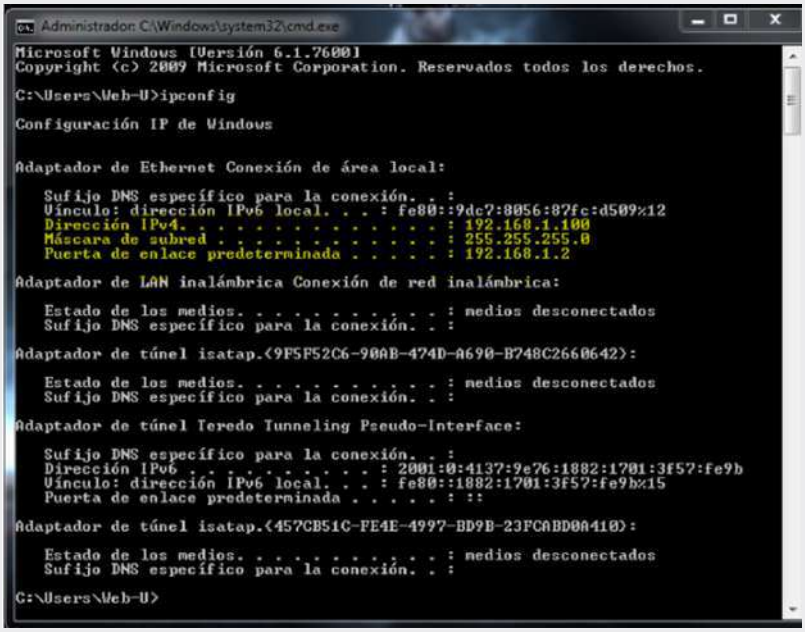


Fig. 3.17. Pantalla con nuestra dirección Ip

Lo que está en amarillo es lo que nos servirá. Lo que dice Puerta de enlace predeterminada tenemos que anotarlo tal cual para después escribirlo en otra parte (Fig. 3.17.)

Si ocupan WIFI tendrán que sacar el número de puerta de enlace predeterminada donde dice Adaptador de LAN inalámbrica. Abrimos el explorador en mi caso Chrome y escribimos en el URL el número que anotamos 192.168.1.2

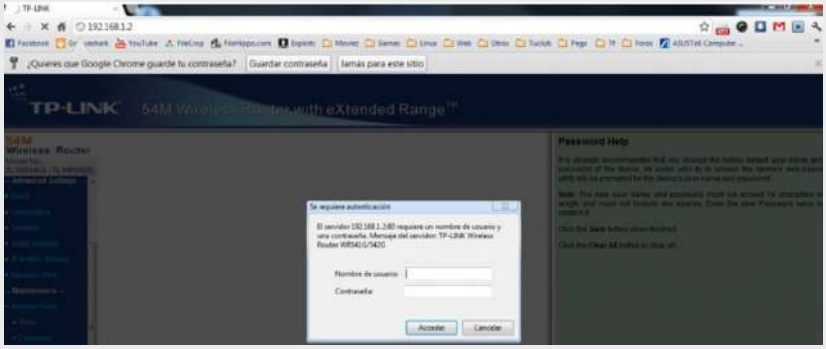


Fig. 3.18. Manera que debemos escribir nuestro Login y Password

Nos saldrá un aviso que pedirá que coloquemos Nombre de usuario y Contraseña (Fig. 3.18.)

Bueno los router por defecto; el usuario es “admin” y la password “admin; si no es así busque el manual en internet o el modelo sale mucha información o simplemente dar vuelta el router y atrás sale el usuario y password.

Luego de colocar la password y el admin estamos listos para ver todo lo de nuestro router (Fig. 3.19.).

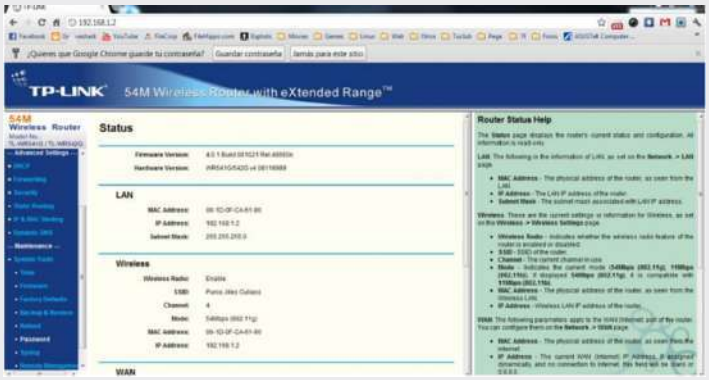


Fig. 3.19. Información de nuestro router

Tabla 3.3. Identificación y Recogida los logs del switch

ACCIÓN 3 TÍTULO: Identificación y Recogida los logs del switch

PROTOCOLO DE ACTUACION:

1. Identificar el modelo y fabricante del switch

2. Identificar la dirección IP

3. Identificar la máscara de red

4. Acceder a recoger los registros o logs que tiene el switch.

- Abrir sesión de un navegador de internet.
- Ingresar a la dirección IP del switch a analizar
- Ingresar el nombre de usuario y contraseña
- Abrir la interfaz del switch en la ventana del navegador de internet.
- Ingresar al menú del Switch a la opción de “Registros” “Datos” u otro término similar en la interfaz basada en el navegador.

COMANDOS DEL SISTEMA:

Windows:

C:\> ipconfig

Escojo donde dice “Puerta de enlace predeterminado”, copio y pego en mi barra de direcciones de mi navegador y me conduce a la configuración de mi switch.

Linux:

Trabajar como [root]

[] netstat -rn

Escojo donde dice “Puerta de enlace predeterminado”, copio y pego en mi barra de direcciones de mi navegador y me conduce a la configuración de mi switch.

Mac OS X

[] netstat –rn

Escojo donde dice “Puerta de enlace predeterminado”, copio y pego en mi barra de direcciones de mi navegador y me conduce a la configuración de mi switch.

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **Pstools** (http://technet.microsoft.com/es-es/sysinternals/bb896649.aspx)

Linux

• **Coroner´s Toolkit(TCT)** (http://technet.microsoft.com/es-es/sysinternals/bb896649.aspx)

Mac OS_X

• **Wireshark** (http://www.wireshark.org/download.html)

OTRAS HERRAMIENTAS FORENSES:

Windows

• **pwdump3** (http://www.governmentsecurity.org/forum/topic/1037-pwdump3/)

• **Bastille** (http://bastille-linux.sourceforge.net/running_bastille_on.htm)

• **Hfnetchk** (http://www.petri.co.il/hfnetchk.htm)

• **snoop** (https://snoopwpf.codeplex.com/releases/view/87261)

Linux

• **Lids** (http://www.lids.org/)

• **Visual Route** (http://visualroute.en.softonic.com/mac)

• **Bastille** (http://bastille-linux.sourceforge.net/running_bastille_on.htm)

Mac OS_X

• **Bastille** (http://bastille-linux.sourceforge.net/running_bastille_on.htm)

EJEMPLO:

Switch Netgear en Windows

• Ingresar a ver mi puerta de enlace predeterminado

C:\>ipconfig

• Abre una sesión en un navegador de Internet.

• Teclea la dirección de protocolo de Internet (IP) de tu router en la barra de direcciones. Pulsa la tecla "Intro". La dirección IP en mi caso

"192.168.1.1"

• Teclea el nombre de usuario y contraseña del switch en la ventana emergente de acceso. Normalmente, el usuario es "admin" y la contraseña "password" (Fig. 3.20).

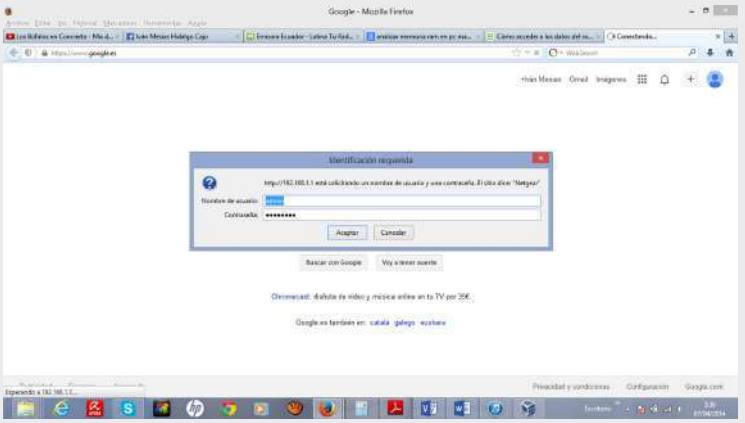


Fig. 3.20. Introducir nombre de usuario y contraseña

• Haz clic en el botón "OK" y pulsa "Intro" en el teclado para abrir el interfaz del switch en la ventana del navegador de Internet.

• Haz clic en la opción del menú del switch relacionado con el "Registro", "Datos" u otro término similar en la interfaz basada en navegador. Por ejemplo, el registro está en la sección "Seguridad" en el panel izquierdo. Hacer clic en el enlace "Registro de seguridad" de esa sección mostrará los datos registrados en el panel derecho (Fig. 3.21).

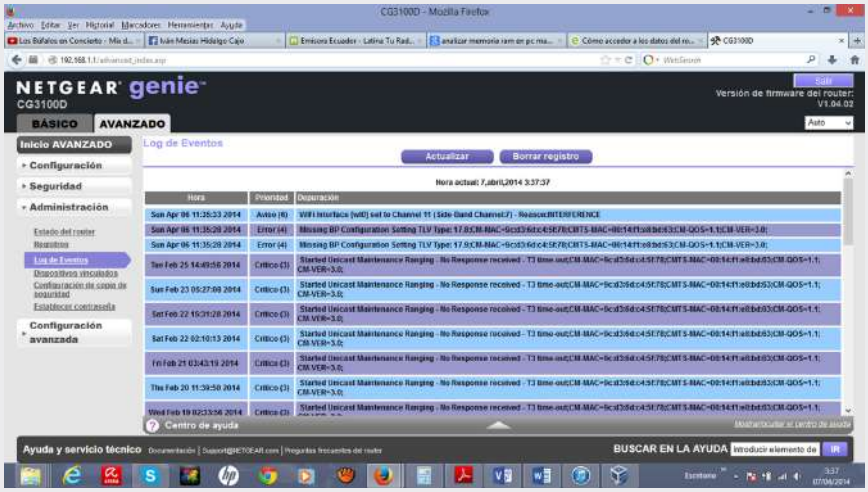


Fig. 3.21. Información de los logs del switch

Tabla 3.4. Clonar el Disco Duro

ACCIÓN 4 TÍTULO: Clonar el Disco Duro

PROTOCOLO DE ACTUACION:

1. Anotar fecha y hora exacta del Análisis del disco duro

2. Usar brazaletes antiestáticos

3. Sacar el disco duro copia de la bolsa antiestática

4. El disco duro copia debe ser de mayor o igual tamaño al disco duro del Pc a analizar

5. El disco duro copia debe ser sometido a un borrado seguro y estar dentro de su vida útil

6. Usar dispositivos que eviten la escritura involuntaria de algún

dato ya almacenado en el disco duro copia

7. Realizar un HASH del disco duro copia de manera simultánea al clonado del disco duro usando alguna herramienta hardware o software de análisis forense.

8. Realizar un HASH al finalizar la copia del disco duro copia para comprobar que el tamaño previo y posterior coinciden.

9. El disco duro copia debe volver a la bolsa antiestática y ser nuevamente sellado y almacenado en algún lugar seguro (caja fuerte) donde estaba guardado

COMANDOS DEL SISTEMA:

Windows:

C:\>ROBOCOPY D:\ E:\ /E

Sustituye D: por la letra asignada al disco cuyo contenido se va a copiar. Sustituye E: por la letra asignada al disco donde se va a pegar la información.

Linux:

Trabajar como [root]

[] dd if=[disco_duro_origen] of=[disco_duro_ destino]

[] dd if=/dev/hda of=/dev/hdb bs=1M con esto clonaríamos el disco hda en hdb. (discos IDE)

[] dd if=/dev/sda of=/dev/sdb bs=1M para discos (discos SATA)

Con bs=1M, estamos diciendo que tanto la lectura como la escritura se haga en bloques de 1 megabyte (menos, sería más lento, pero más seguro, y con más nos arriesgamos a perder datos por el camino).

Hay que tener en cuenta que de esta forma grabarás el disco "tal cual", MBR, tabla de particiones, espacio vacío, etc., por lo que sólo podrás grabar en un disco del mismo o mayor tamaño

Mac OS X

[] dd if=[disco_duro_origen] of=[disco_duro_destino]

[] $ dd if=/dev/hda of=/dev/hdb bs=1M con esto clonaríamos el disco hda en hdb. (discos IDE)

[] $ dd if=/dev/sda of=/dev/sdb bs=1M para discos (discos SATA)

Con bs=1M, estamos diciendo que tanto la lectura como la escritura se haga en bloques de 1 megabyte (menos, sería más lento, pero más seguro, y con más nos arriesgamos a perder datos por el camino).

Hay que tener en cuenta que de esta forma grabarás el disco "tal cual", MBR, tabla de particiones, espacio vacío, etc., por lo que sólo podrás grabar en un disco del mismo o mayor tamaño.

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **FTK Imager** (http://www.accessdata.com/ftk-3-2)

Linux

•**SleunthKit** (http://www.sleuthkit.org/sleuthkit/download.php)

Mac OS_X

• **OndataRecoverySoft** (http://www.ondata-recoverysoft.com/)

OTRAS HERRAMIENTAS FORENSES:

Windows

• EnCase (http://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx)

• DC3DD (http://www.dc3.mil)

• Forensic Replicator (http://www.paraben.com/forensic-replicator.html)

• X-Ways Forensics (http://www.x-ways.com)

• X-Ways Imager (http://www.x-ways.com)

Linux

• DC3DD (http://www.dc3.mil)

Mac OS_X

• DC3DD (http://www.dc3.mil)

• MacQuisition (https://www.blackbagtech.com/software-products/macquisition-1/macquisition.html

EJEMPLO:

Windows usando FTK Imager

1. Iniciar FTK Imager (Fig. 3.22)

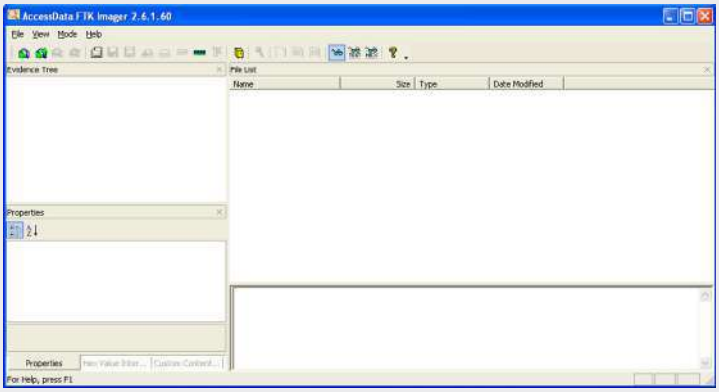


Fig. 3.22. Inicio de FTK Imager

2. Hacer clic en el icono Create Disk Image (Fig. 3.23).

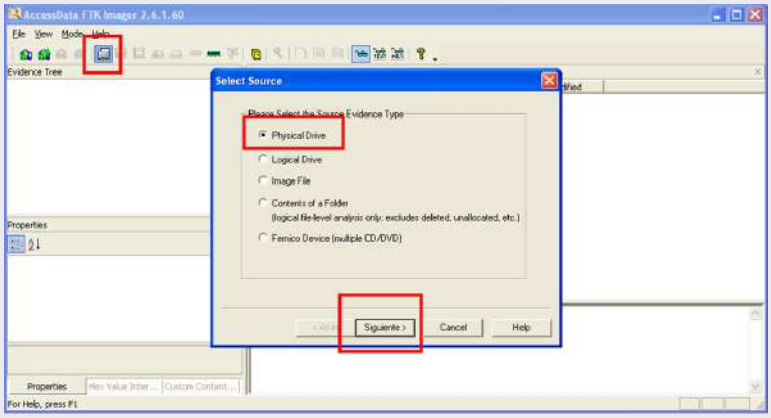


Fig. 3.23. Pulsar en el icono Create Disk Image

2. Crear la imagen de todo el disco físico, se hace clic en este ítem y siguiente (Fig. 3.24.).

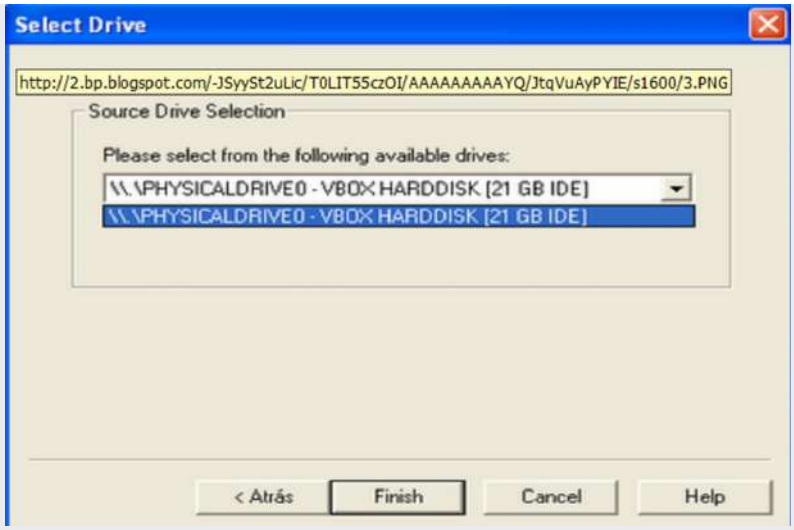


Fig. 3.24. Crear la imagen de todo el disco físico

1. Posterior a ello se hace clic en Add y a continuación se selecciona el tipo de imagen que se está creando, que en este caso es una imagen SMART y se hace clic en siguiente (Fig. 3.25.).

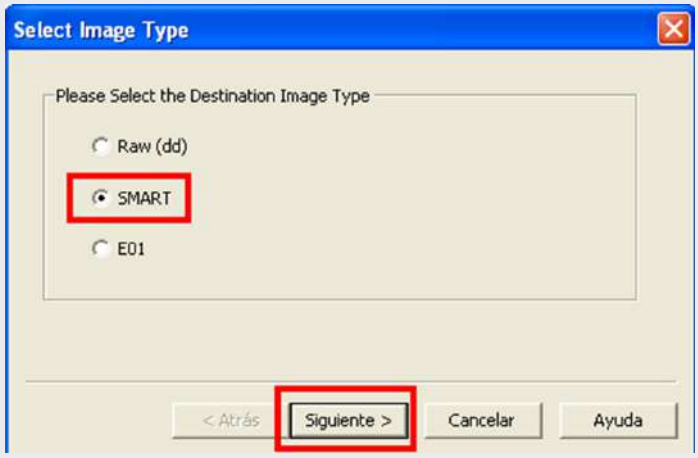


Fig. 3.25. Selecciona el tipo de imagen que se está creando

2. Introducir información sobre la unidad y la investigación, número de caso y de prueba son de uso propio; pero es recomendable asignar a cada investigación un número y a cada

prueba que se obtenga un número diferente (Fig. 3.26.).

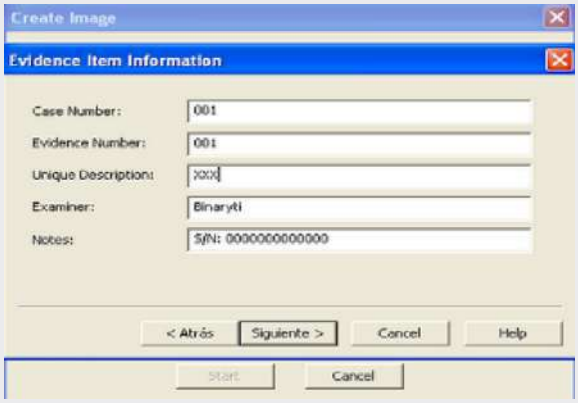


Fig. 3.26. Introducir información sobre la unidad y la investigación

3. En este punto le tendrá que dar la ubicación donde desea guardar la imagen forense, entendiendo que siempre debe ser en una unidad externa "disco duro copia" (Fig. 3.27.).

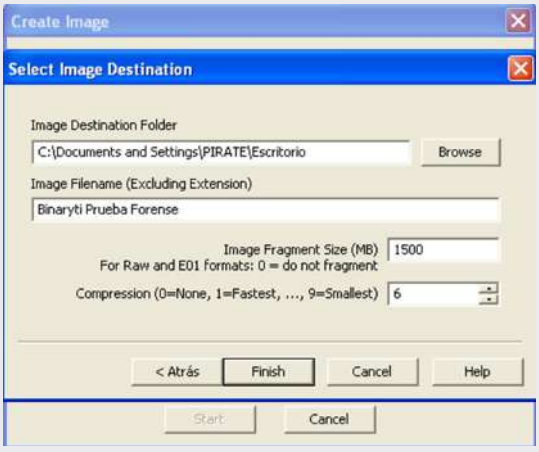


Fig. 3.27. Ubicación donde desea guardar la imagen forense

4. Al dar iniciar aparecerá la pantalla de progreso de la imagen y mostrara cuando ha finalizado (Fig. 3.28.).

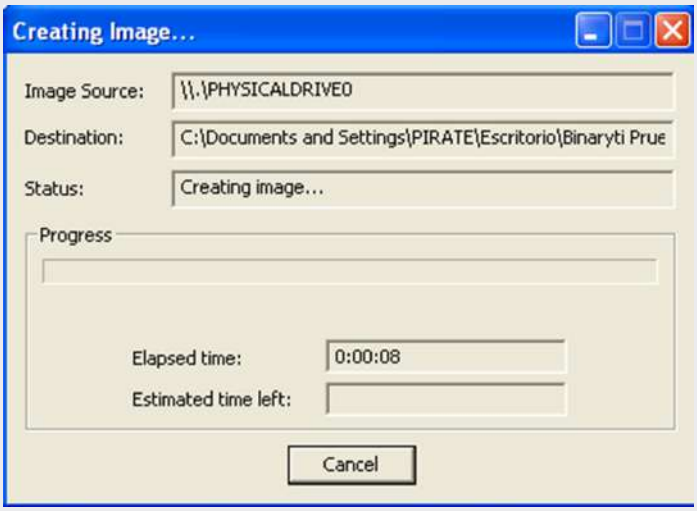


Fig. 3.28. Pantalla de progreso de la imagen y finalización

Ahora ya tenemos la imagen del disco duro original.

Tabla 3.5. Clonar el Disco Duro desde un Live CD

ACCIÓN 5 TÍTULO: Clonar el Disco Duro desde un Live CD

PROTOCOLO DE ACTUACION:

1. Anotar fecha y hora exacta del Análisis del disco duro
2. Usar brazaletes antiestáticos
3. Sacar el disco duro copia de la bolsa antiestática
4. El disco duro copia debe ser de mayor o igual tamaño al disco duro del Pc a analizar

5. El disco duro copia debe ser sometido a un borrado seguro y estar dentro de su vida útil

6. Usar dispositivos que eviten la escritura involuntaria de algún dato ya almacenado en el disco duro copia

7. Arrancar desde un medio de almacenamiento diferente al disco duro original que se va a realizar la imagen.

8. Colocar un Live CD en la unidad del CD-Rom

9. Reiniciar el ordenador y pulsar la tecla “Intro” o “Sup” para arrancar con las opciones por defecto y colocar la primera opción del arranque desde el Cd.

10. Ya arrancado y abierto la consola de administrador, montamos el “dispositivo de almacenamiento” puede ser otro disco duro. en el que guardaremos el fichero imagen diferente al disco duro original que se está preservando.

11. Es necesario asegurarse que nadie va a acceder al disco duro mientras se realiza la imagen.

12. Realizar la imagen del disco duro original

13. Realizar un HASH al finalizar la copia del disco duro copia para comprobar que el tamaño previo y posterior coinciden.

14. El disco duro copia debe volver a la bolsa antiestática y ser nuevamente sellado y almacenado en algún lugar seguro (caja fuerte) donde estaba guardado

COMANDOS DEL SISTEMA:

Utilizamos otro disco duro de la misma Pc y montamos la imagen del disco duro original clonado

[] mkdir /mnt/imagen

[] mount /dev/hdb1 /mnt/imagen (discos IDE)

[] mount /dev/sda1 /mnt/imagen (discos SATA)

Escribe el siguiente comando, sustituyendo ORIGEN con el nombre de tu unidad de origen y DESTINO con el nombre de tu unidad de destino:

[] sudo dd rescue-v /dev/ORIGEN /dev/DESTINO

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **BartPE** (http://www.nu2.nu/pebuilder/download/)

Linux

• **Clonezilla** (http://clonezilla.org/downloads.php)

Mac OS_X

• **Tiger** (http://download.cnet.com/Apple-Mac-OS-X-Tiger/3000-18513_4-10203618.html)

OTRAS HERRAMIENTAS FORENSES:

Windows

• **Ultimate Boot CD** (http://www.ubcd4win.com/)

Linux

• **Knoppix** (http://knopper.net/knoppix-mirrors/index-en.html)

• **Ubuntu Desktop** (http://www.ubuntu.com/download/desktop)

• **Gnoppix** (http://iso.linuxquestions.org/gnoppix/)

• **Suse Live** (http://software.opensuse.org/131/es)

• **Slax** (https://www.slax.org/es/download.php)

Mac OS_X

• **Leopard** (http://www.apple.com/support/leopard/)

• **Snow Leopard** (http://store.apple.com/us/product/MC573Z/A/mac-os-x-106-snow-leopard)

• **Lion** (https://www.macupdate.com/app/mac/39487/os-x-lion)

• **Mountain Lion** (http://kickass.to/mac-os-x-10-8-mountain-lion-iso-untouched-t8036829.html)

• **Mavericks** (https://itunes.apple.com/es/app/os-x-mavericks/id675248567?mt=12)

EJEMPLO:

Linux usando Clonezilla

1. Iniciar tu pc con el cd de clonezilla usando la primera opción, en el momento en que haya cargado todo el sistema nos mostrará una ventana en consola donde se podrá elegir el idioma en que se usará clonezilla (Fig. 3.29.).

Fig. 3.29. Inicio de clonezilla

2. Luego de esto escoge la opción "No tocar mapa del teclado" (Fig. 3.30.).

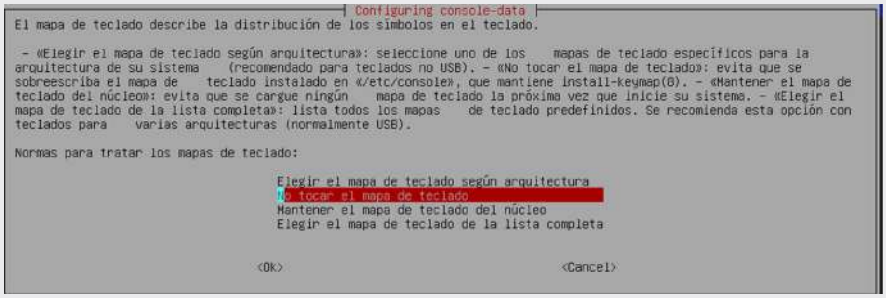


Fig. 3.30. Escoger una opción

3. Una vez hallas conFig.do esto inicia clonezilla aunque si eres un usuario avanzado puedes usar el shell es decir la consola (Fig. 3.31.).

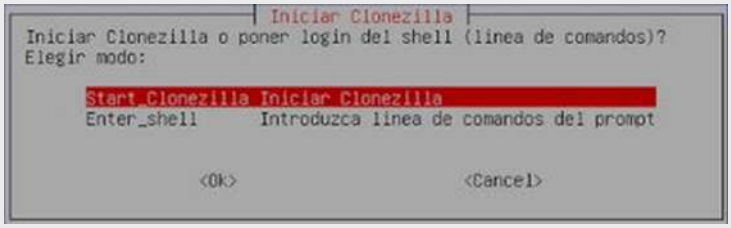


Fig. 3.31. Inicio configuración de clonezilla

4. Para este ejemplo elegiré la opción device-image, la cual se usa para clonar particiones, si lo que quieres es clonar un disco completo usa la opción device-device (Fig. 3.32.).

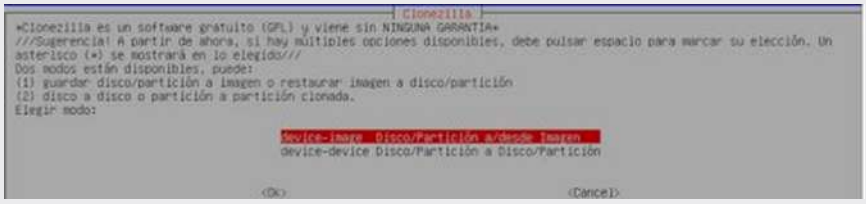


Fig. 3.32. Clonar particiones con la opción device-image

5. Luego de esto aparecerá una pantalla para elegir si deseas usar el modo "experto" o el modo "novato", por supuesto vas a escoger el modo novato ya que hasta ahora estas aprendiendo (Fig. 3.33.).

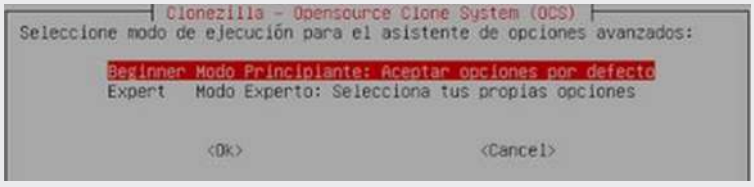


Fig. 3.33. Elegir el modo "experto" o el modo "novato"

6. Este menú te muestra las opciones que ofrece clonezilla para clonar el disco, en dicho menú debes indicar el lugar donde se guardará la imagen que será creada a partir del disco/partición que desees clonar (Fig. 3.34.).

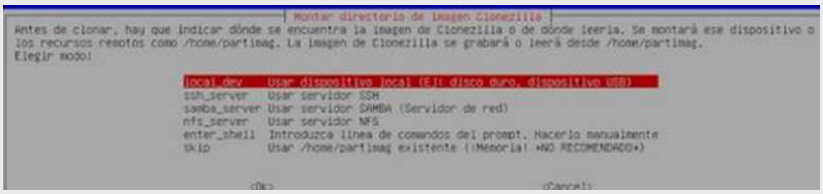


Fig. 3.34. Opciones de clonezilla para clonar el disco

7. Si la partición o el disco que elegiste contiene algunas carpetas te preguntará en cuál de ellas quieres que se guarde la imagen (Fig. 3.35.).

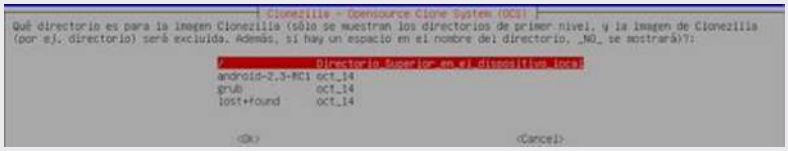


Fig. 3.35. Lugar donde guardar la imagen

8. Después del paso anterior debes indicar si lo que quieres es copiar un disco completo alguna de las particiones del disco (Fig. 3.36.).

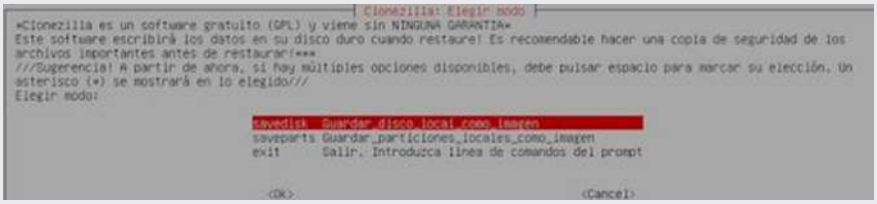


Fig. 3.36. Copiar un disco completo alguna de las particiones del disco.

9. Dale un nombre a la imagen del disco (Fig. 3.37.).

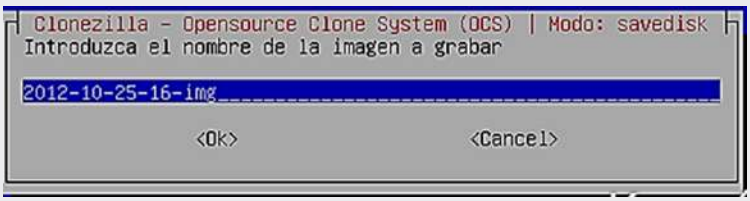


Fig. 3.37. Asignar un nombre a la imagen del disco

10. Indica cual es la partición o disco en donde se va a montar la carpeta /home/partimg, recuerda que debe ser distinta a la partición/disco a clonar (Fig. 3.38.).

Fig. 3.38. Lugar en donde se va a montar la carpeta

11. Ahora ya puedes elegir cual es la partición que quieres clonar (Fig. 3.39.).

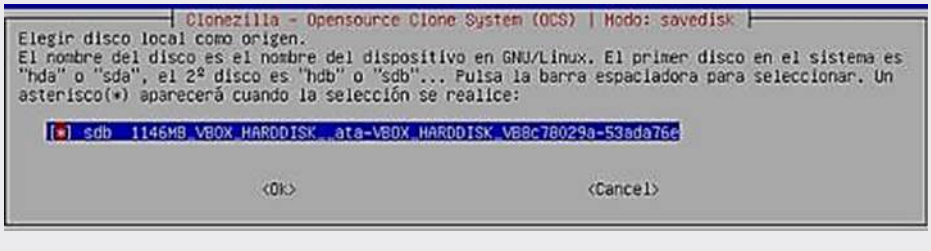


Fig. 3.39. Elegir cual es la partición que deseamos clonar

12. Luego de esto empezara el proceso de clonado, esperamos un momento porque generalmente los procesos en disco son de mucho tiempo.

13. Si quieres restaurar la imagen creada puedes iniciar nuevamente clonezilla, repetir el proceso hasta el paso 7, elige la carpeta donde guardaste la imagen, el siguiente paso será entrar a la opción "restoreparts" (Fig. 3.40.).

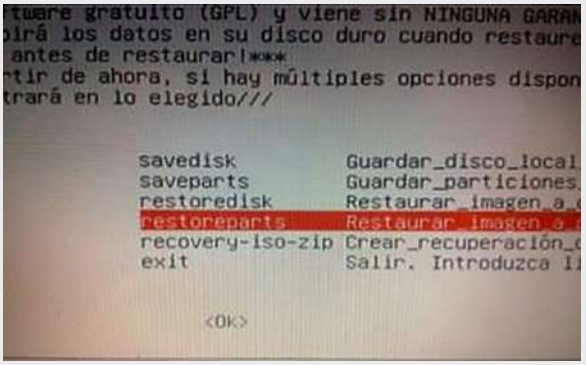


Fig. 3.40 .Si deseamos restaurar la imagen creada

14. Elige la imagen y la partición en donde la vas a copiar (Fig. 3.41).

Fig. 3.41. Seleccionar la imagen y la partición en donde la vas a copiar

Luego de terminar la copia reinicia el pc y listo, tendrás tu disco/ partición clonada.

Tabla 3.6. Recuperar Datos Volátiles

ACCIÓN 6: Recuperar Datos Volátiles

PROTOCOLO DE ACTUACION:

1. No apagar la Pc.
2. Insertar un Live CD que es lo recomendable
3. Analizar los datos volátiles desde el Live CD
4. Analizar los Registros, cache‖ (es una parte de la memoria de la memoria principal que se puede utilizar como buffer) para guardar temporalmente los datos transferidos con el disco).
5. Tabla de procesos, estadísticas del kernel
6. Tablas de ruteo (Para mostrar la tabla de enrutamiento IP en equipos que ejecutan sistemas operativos Windows Server 2003, puede escribir --route print" (comando que se ejecuta) en el símbolo del sistema. También puede examinarse la tabla de ruteo de una máquina con el comando netstat. La opción -r del mismo muestra la tabla de ruteo (la opción -n es para no convertir números en nombres)
7. Cache ARP# (ADDRESS RESOLUTION PROTOCOL, tabla donde se almacenan las direcciones IP de internet, ARP convierte un protocolo de Internet (IP) a su dirección física de red correspondiente).
8. Sesiones abiertas.
9. Configuración de la red.

10. Memoria RAM (RAM son las siglas en ingles de Random Access Memory, un tipo de memoria de computadora a la que se puede acceder aleatoriamente; es decir, se puede acceder a cualquier byte de memoria sin acceder a los bytes precedentes. La memoria RAM es el tipo de memoria más común en computadoras y otros dispositivos como impresoras).
11. Directorios temporales del sistema.
12. Estado de la red.
13. Directorios abiertos.
14. Archivos abiertos.

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **Volatility** (http://code.google.com/p/volatility/downloads/detail?name=volatility2.2.standalone.exe&can=2&q=)

Linux

• **Pd** (http://www.trapkit.de/research/forensic/pd/)

Mac OS_X

• **Memorize** (https://www.mandiant.com/resources/download/memoryze)

OTRAS HERRAMIENTAS FORENSES:

Windows

• **FTK Imager** (http://www.accessdata.com/support/technical-customer-support/product-downloads)

• Redline (http://www.mandiant.com/resources/download/redline/)

• **FTK Imager** (http://www.accessdata.com/support/product-downloads#FTKImager)

• **Responder CE** (http://www.hbgary.com/free-tools)

• **Volatility** (https://www.volatilesystems.com/default/volatility)

• **Pd** (http://www.trapkit.de/research/forensic/pd/)

Linux

• Dump (https://developers.google.com/freebase/data)

Mac OS_X

• **Memtest86** (http://www.memtest86.com/download.htm)

EJEMPLO:

Windows usando Volatility

Analizar la memoria RAM de Windows. Para obtener la RAM de Windows.

Para utilizar la herramienta en Linux habrá que llamarla por la línea de comandos introduciendo el fichero de la memoria con

el comando “-f” y a continuación llamar al plugin que queremos utilizar.

Pslist: Lista los procesos que había activos en el momento (Fig. 3.42.).

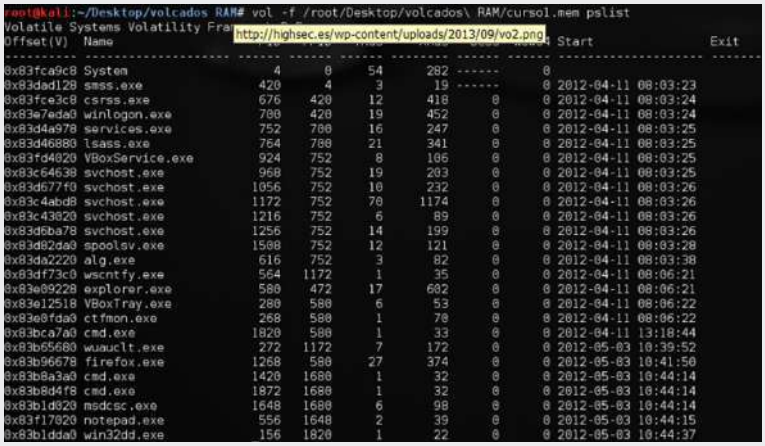


Fig. 3.42. Lista los procesos con Pslist

Consoles: Te muestra un histórico de la terminal. En la parte de abajo de la foto aparece primero los comandos que se introdujeron, y después aparece la consola con los comandos introducidos y la respuesta de la máquina (Fig. 3.43.).

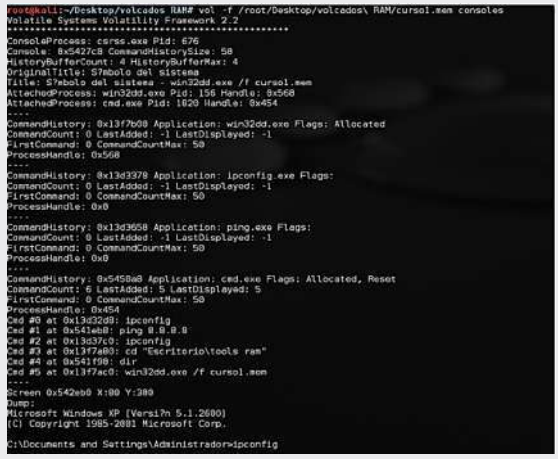


Fig. 3.43. Muestra la información del comando Consoles

Connections: Listado de las conexiones que estaban abiertas (Fig. 3.44. y Fig. 3.45.).

```
root@kali:~/Desktop/volcados RAM# vol -f /root/Desktop/volcados\ RAM/cursol.mem connections
Volatile Systems Volatility Framework 2.2
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ------
0x83b951f8 127.0.0.1:1160           127.0.0.1:1159           1268
0x83ba46f8 127.0.0.1:1162           127.0.0.1:1161           1268
0x83ba6868 127.0.0.1:1159           127.0.0.1:1160           1268
0x83c6aa08 127.0.0.1:1161           127.0.0.1:1162           1268
0x83b88e68 192.168.0.106:1241       50.22.180.168:80         1268
0x83c21008 192.168.0.106:1165       184.164.135.171:80       1268
0x83b1a328 192.168.0.106:1248       78.54.19.110:1604        1648
0x83b882f8 192.168.0.106:1244       74.125.230.217:80        1268
0x83b92b58 192.168.0.106:1240       74.125.230.205:80        1268
0x83ae42e0 192.168.0.106:1243       50.22.180.158:80         1268
0x83b3f008 192.168.0.106:1167       184.164.135.171:80       1268
0x83b1d368 192.168.0.106:1202       173.194.34.40:80         1268
```

Fig. 3.44. Listado de las conexiones que estaban abiertas, con el comando Connections.

```
root@kali:~/Desktop/volcados RAM# vol -f /root/Desktop/volcados\ RAM/cursol.mem sockets
Volatile Systems Volatility Framework 2.2
Offset(V)     PID   Port  Proto Protocol        Address         Create Time
---------- ------ ------ ------ --------------- --------------- -----------
0x83b92008   1268   1243      6 TCP             0.0.0.0         2012-05-03 10:44:20
0x83d88d08   1172   1025     17 UDP             127.0.0.1       2012-04-11 08:03:35
0x83d9de98    764    500     17 UDP             0.0.0.0         2012-04-11 08:03:35
0x83daa008   1172    123     17 UDP             192.168.0.106   2012-04-11 13:19:11
0x83b337c0   1268   1162      6 TCP             0.0.0.0         2012-05-03 10:41:52
0x83d52d00      4    445      6 TCP             0.0.0.0         2012-04-11 08:03:22
0x83d67008   1056    135      6 TCP             0.0.0.0         2012-04-11 08:03:26
0x83ecaaa0   1268   1240      6 TCP             0.0.0.0         2012-05-03 10:44:20
0x83e20450   1268   1244      6 TCP             0.0.0.0         2012-05-03 10:44:20
0x83b26008   1648   1248      6 TCP             0.0.0.0         2012-05-03 10:44:38
0x83bbe898   1216   1133     17 UDP             0.0.0.0         2012-04-11 13:20:35
0x83d839e8   1216   1102     17 UDP             0.0.0.0         2012-04-11 13:18:42
0x83b50470   1268   1167      6 TCP             0.0.0.0         2012-05-03 10:42:06
0x83b888d0   1268   1202      6 TCP             0.0.0.0         2012-05-03 10:42:15
0x83ba9620   1256   1900     17 UDP             192.168.0.106   2012-04-11 13:19:11
0x83be1620   1172    123     17 UDP             127.0.0.1       2012-04-11 13:19:11
0x83da5e98    764      0    255 Reserved        0.0.0.0         2012-04-11 08:03:35
0x83b348a8   1268   1161      6 TCP             127.0.0.1       2012-05-03 10:41:52
0x83b89a38   1268   1241      6 TCP             0.0.0.0         2012-05-03 10:44:20
0x83d8ea78      4    139      6 TCP             192.168.0.106   2012-04-11 13:19:13
0x83b9e898   1216   1130     17 UDP             0.0.0.0         2012-04-11 13:20:27
0x83f178b0   1268   1160      6 TCP             0.0.0.0         2012-05-03 10:41:51
0x83bcb898      4    137     17 UDP             192.168.0.106   2012-04-11 13:19:13
0x83ba7620   1256   1900     17 UDP             127.0.0.1       2012-04-11 13:19:11
0x83da7220    764   4500     17 UDP             0.0.0.0         2012-04-11 08:03:35
0x83b8f2c0   1268   1165      6 TCP             0.0.0.0         2012-05-03 10:42:05
0x83d528d8      4    445     17 UDP             0.0.0.0         2012-04-11 08:03:22
0x83b33008   1216   1178     17 UDP             0.0.0.0         2012-05-03 10:42:10
0x83b561f0   1268   1159      6 TCP             127.0.0.1       2012-05-03 10:41:51
0x83d51c10      4    138     17 UDP             192.168.0.106   2012-04-11 13:19:13
```

Fig. 3.45. Listado con el comando sockets

Pstree: Imprime la lista de procesos en forma de árbol (Fig. 3.46.).

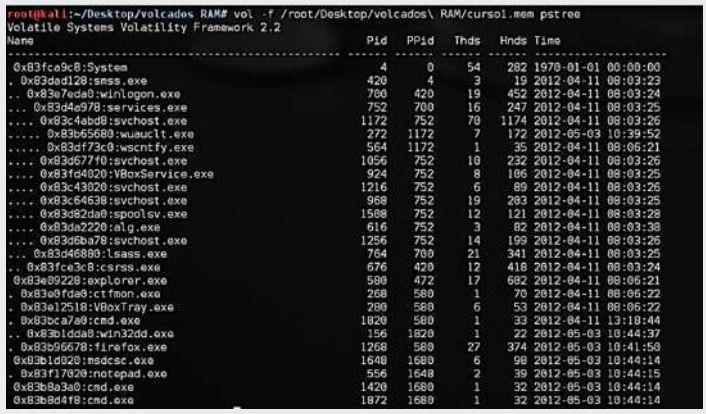


Fig. 3.46. Lista la información del comando Pstree

Svcscan: Muestra los servicios que estaban activos (Fig. 3.47.).

Fig. 3.47. Lista la información del comando Svcscan

Hashdump: Imprime los hashes (LM/NTLM) de la memoria. Para utilizar esta herramienta es necesario ejecutar antes del plugin Hivelist para obtener las posiciones de memoria de SYSTEM y SAM. Si nos fijamos en el principio de la foto, si ejecutamos el plugin "hashdump" sin argumentos de entrada, nos mostrará un error y nos pide la posición de memoria de SYSTEM y de SAM. Para saber los argumentos de entada de estos plugins que necesitan argumentos solo tienes que ver su ayuda: "vol -h hashdump". Entonces podemos ver como en la foto se ha seleccionado la posición de memoria de la SAM para pasarselo al plugin "hashdump" (Fig. 3.48.).

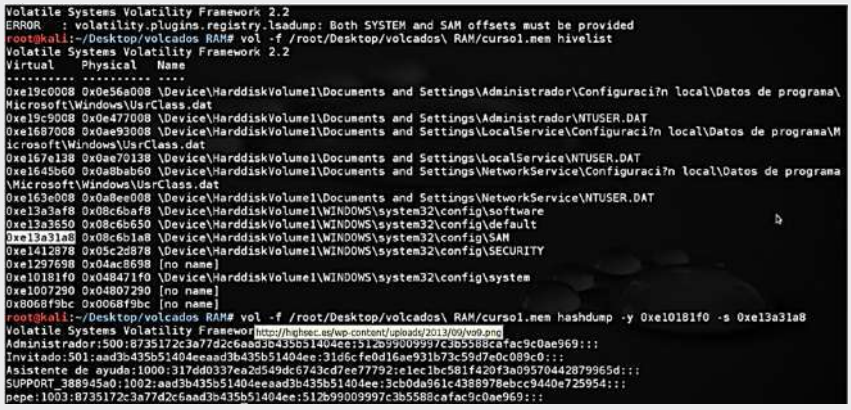


Fig. 3.48. Lista la información del comando Hashdump

Pues estos son solo algunos de los plugins que tiene esta potente herramienta de análisis de RAM. Si muestras la ayuda "vol -h" podrás ver todos los plugins que trae incorporados.

Extraer Password de la RAM desde Windows usando FTK Imager

Procedemos a realizar una copia bit a bit de la memoria RAM.

Para hacer esto nos dirigimos a la lista de botones que tiene la herramienta justo abajo de las pestañas y buscamos uno que ponga "Capture Memory" (verde con forma rectangular de memoria RAM). Seleccionamos el destino de la copia y procedemos.

Una vez terminada la copia de la memoria RAM nos vamos a la pestaña File y dentro de esta pulsamos en "Add evidence item". En la ventana que nos aparece seleccionamos la opción "Image file" y pulsamos siguiente. Ahora seleccionamos la copia donde la tengamos y ya está.

Podemos ver cómo nos aparece el volcado de memoria en la herramienta, es normal que las primeras posiciones estén a cero (Fig. 3.49.).

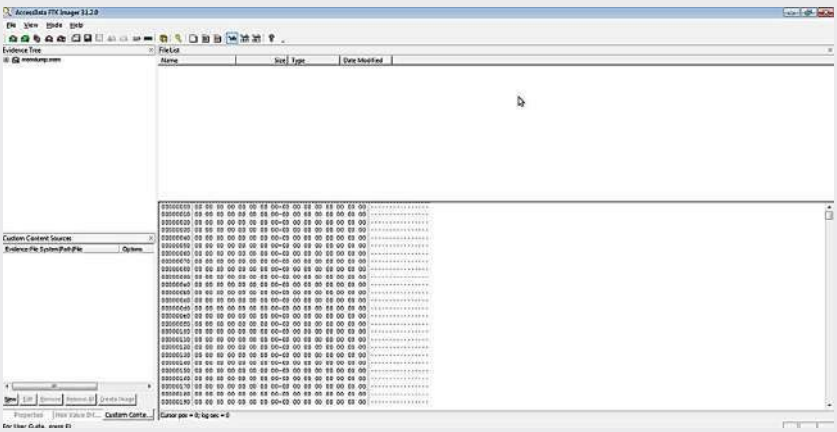


Fig. 3.49. Observar el volcado de memoria en la herramienta FTK Imager

Ahora para buscar aquí pulsaremos CONTROL+F y tenemos muchas formas de buscar. Como sabemos que la contraseña de Gmail se guarda con el prefijo "&Passwd=" delante, haremos una búsqueda de "&Passwd=". El primer resultado que aparece puede no ser el correcto, asi que seguiremos avanzando con F3 hasta dar con el mail y la contraseña. Y como se observa en la imagen

para la cuenta apuntes.tutoriales@gmail.com la contraseña es "pruebadeconcepto" (Fig. 3.50.).

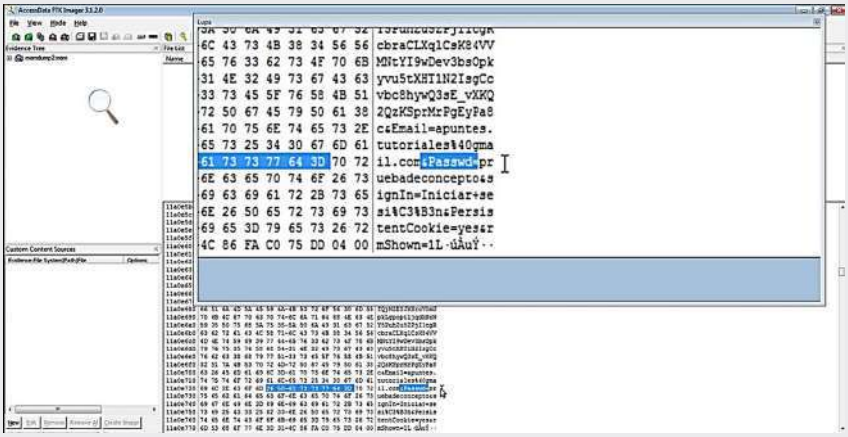


Fig. 3.50. Muestra la contraseña de la cuenta de correo

¡Pues ahí está la contraseña de la cuenta de correo!

Linux:

Para recoger estos datos, es muy importante que, en el equipo atacado, no ejecutemos ningún comando o herramienta por peligro a que pueda haber sido troyanizada. Para ello procederemos a ejecutar los binarios compilados estáticamente directamente desde un CD-ROM.

Para empezar, utilizaremos un equipo no comprometido para el almacenamiento de las pruebas en red, esto lo haremos ejecutando el siguiente comando en el equipo:

nc -l -p 9000 > data.dat

Así, pondremos a la escucha un puerto donde le iremos enviando la información desde la máquina comprometida.

Procederemos a listar los ficheros abiertos por los procesos para así

detectar algún proceso/fichero sospechoso:

/mnt/cdrom/lsof -n | /mnt/cdrom/nc -w 3 IP 9000

Listamos las conexiones establecidas por los procesos:

/mnt/cdrom/netstat -nap | /mnt/cdrom/nc -w 3 IP 9000

Además, listamos la tabla de rutas:

/mnt/cdrom/netstat -nr | /mnt/cdrom/nc -w 3 IP 9000

Es importante hacer un análisis de puertos desde una máquina externa y compararla con la salida de netstat para poder asegurarnos de que no hemos perdido de vista ningún proceso escuchando en ningún puerto, para ello usaremos nmap:

nmap -sS -p 1- IP_COMPROMETIDO

Listamos los ficheros que han sido eliminados pero que aún siguen abiertos por algún proceso en ejecución.

Ahora usamos **The Coroner's Toolkit**:

/mnt/cdrom/ils -o /dev/hda1 | /mnt/cdrom/nc -w 3 IP 9000

Listamos los procesos en ejecución:

/mnt/cdrom/ps -el | /mnt/cdrom/nc -w 3 IP 9000

Si mediante la orden anterior, encontráramos algún proceso sospechoso, podríamos

/mnt/cdrom/pcat | /mnt/cdrom/nc -w 3 IP 9000

Listaremos los usuarios conectados en el sistema:

/mnt/cdrom/who -uHl | /mnt/cdrom/nc -w 3 IP 9000

Para finalizar guardamos el proc, en el cual obtendremos información acerca de los procesos:

/mnt/cdrom/tar cf - /proc | /mnt/cdrom/nc -w 3 IP 9000

Con estos pasos, se lograría haber recopilado mucha información volátil.

Tabla 3.7. Clonar vía Disco Duro externo

ACCIÓN 7 TÍTULO: Clonar vía Disco Duro externo

PROTOCOLO DE ACTUACION:

1. Anotar fecha y hora exacta del Análisis del disco duro
2. Usar brazaletes antiestáticos
3. Sacar el disco duro copia de la bolsa antiestática
4. El disco duro copia debe ser de mayor o igual tamaño al disco duro del Pc a analizar
5. El disco duro copia debe ser sometido a un borrado seguro y estar dentro de su vida útil
6. Usar dispositivos que eviten la escritura involuntaria de algún dato ya almacenado en el disco duro copia
7. No apagar la Pc
8. Usar una herramienta forense (bloqueador de escritura)
9. Calcular el hash del disco duro original

10. Conectar el disco duro copia al Pc

11. Obtener la imagen del disco duro original

12. Guardar la imagen adquirida en el disco duro copia

13. Verificamos si el HASH del disco duro original y del disco duro copia es del mismo tamaño, lo cual nos permitirá corroborar que la imagen forense es una copia duplicada bit a bit del disco suro original

14. Guardar en un archivo plano de preferencia .txt para presentarlo si es requerido.

15. Registrar cualquier anomalía o circunstancia inusual encontrada durante la creación de la imagen por medio de algún formato (capturas de pantalla)

16. Retirar el disco duro copia si me permite manipularlo en caliente caso contrario no retirarlo; y cuando lo retire guardarlo en una bolsa antiestática y ser nuevamente sellado y almacenado en algún lugar seguro (caja fuerte) donde estaba guardado

COMANDOS DEL SISTEMA:

Windows:

C:\>ROBOCOPY D:\ E:\ /E

Sustituye D: por la letra asignada al disco cuyo contenido se va a copiar.

Sustituye E: por la letra asignada al disco donde se va a pegar la información.

Linux:

Trabajar como [root]

[] dd if=[disco_duro_origen] of=[disco_duro_ destino]

[] dd if=/dev/hda of=/dev/hdb bs=1M con esto clonaríamos el disco hda en hdb. (discos IDE)

[] dd if=/dev/sda of=/dev/sdb bs=1M para discos (discos SATA)

Con bs=1M, estamos diciendo que tanto la lectura como la escritura se haga en bloques de 1 megabyte (menos, sería más lento, pero más seguro, y con más nos arriesgamos a perder datos por el camino).

Mac OS X

[] dd if=[origen] of=[destino]

[] dd if=/dev/hda of=/dev/hdb bs=1M con esto clonaríamos el disco hda en hdb (discos IDE)

[] dd if=/dev/sda of=/dev/sdb bs=1M para discos (discos SATA)

Con bs=1M, estamos diciendo que tanto la lectura como la escritura se haga en bloques de 1 megabyte (menos, sería más lento, pero más seguro, y con más nos arriesgamos a perder datos por el camino).

Hay que tener en cuenta que de esta forma grabarás el disco “tal

cual", MBR, tabla de particiones, espacio vacío, etc., por lo que sólo podrás grabar en un disco del mismo o mayor tamaño

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **Systesternals Acronis** (http://es.kioskea.net/download/descargar-735-acronis-true-image)

Linux

• **Forensic ToolKit FTK de Access Data** (http://www.accessdata.com)

Mac OS_X

• **Carbon Copy Cloner** (http://carbon-copy-cloner-ccc.softonic.com/mac)

OTRAS HERRAMIENTAS FORENSES:

Windows

• **Helix 1.9** (http://www.linux23.com/search/helix+1.9+live+cd)

• **XWay Forensics** (http://www.x-ways.com)

• **HD Clone** (http://es.kioskea.net/download/descargar-2556-hdclone)

Linux

• **Norton Ghost** (http://es.norton.com/downloads-trial-norton-online-backup)

• **EnCase** (http://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx)

Mac OS_X

• **Snow Leopard** (http://snow-leopard.en.softonic.com/mac)

• **OndataRecoverySoft** (http://www.ondata-recoverysoft.com/)

EJEMPLO:

Linux usando Carbon Copy Cloner

1. Formatear el disco externo donde vamos a realizar la copia de seguridad desde Utilidad de Discos, seleccionando tal como aparece en la imagen el formato Mac Os Plus (con registro) (Fig. 3.51.).

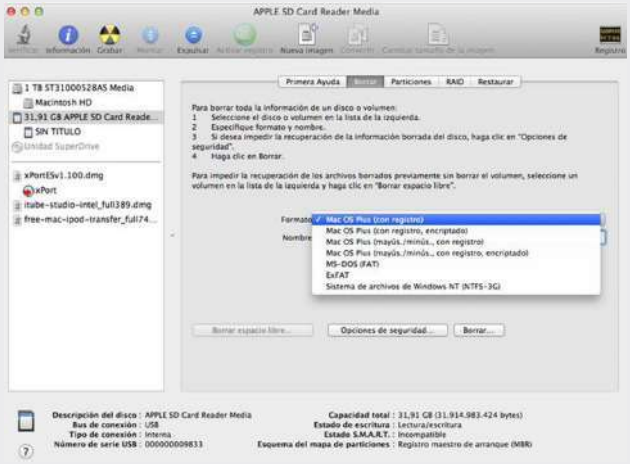


Fig. 3.51. Formatea el disco externo donde vamos a realizar la copia de seguridad desde Utilidad de Discos

2. Abrimos Carbon Copy Cloner, y en la parte izquierda (Source) seleccionamos la unidad donde tenemos el sistema operativo, en

la imagen “Macintosh HD” y en la derecha (Destination)la unidad de destino. Presionamos Clone y dejamos que el programa haga el resto hasta que finalice la clonación (Fig. 3.52.).

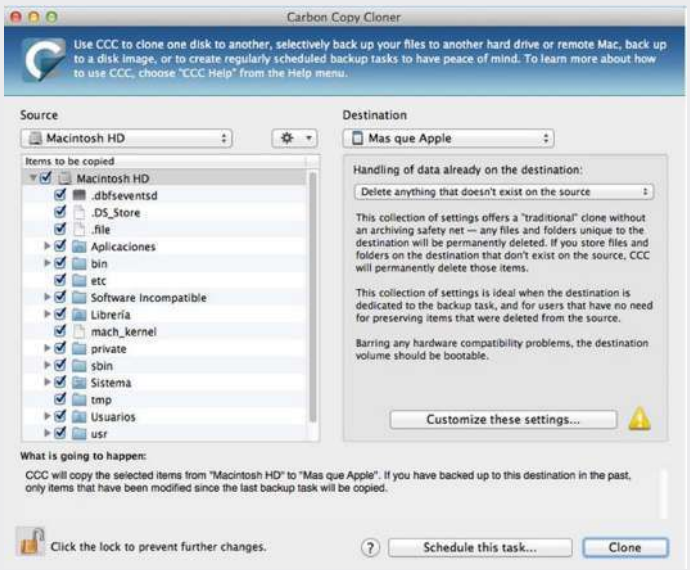


Fig. 3.52. Clonamos el disco

Listo tendremos una copia exacta del disco duro

Tabla 3.8. Clonar Disco Duro vía Red

ACCIÓN 8 TÍTULO: Clonar Disco Duro vía Red

PROTOCOLO DE ACTUACION:

1. Anotar fecha y hora exacta del Análisis del disco duro
2. Usar brazaletes antiestáticos
3. Sacar el disco duro copia de la bolsa antiestática
4. El disco duro copia de la Pc destino debe ser de mayor o igual

tamaño al disco duro del Pc origen.

5. El disco duro copia debe ser sometido a un borrado seguro y estar dentro de su vida útil

6. Usar dispositivos que eviten la escritura involuntaria de algún dato ya almacenado en el disco duro copia Pc destino

7. Configurar la Pc Origen como Máster

8. Ingresar la dirección IP de la Pc que tiene el disco destino y de esta manera se establecerá la comunicación entre las dos máquinas con las que vamos a trabajar.

9. Configuradas las dos máquinas y establecida la comunicación se procede a realizar los pasos tal y como fuese una clonación común

10. Es necesario asegurarse que nadie va a acceder al disco duro mientras se realiza la imagen.

11. Realizar la imagen del disco duro original y copiar al disco duro destino.

12. Realizar un HASH al finalizar la copia del disco duro copia para comprobar que el tamaño previo y posterior coinciden.

13. El disco duro copia debe volver a la bolsa antiestática y ser nuevamente sellado y almacenado en algún lugar seguro (caja fuerte) donde estaba guardado

COMANDOS DEL SISTEMA:

Windows:

Comprobar que las 2 Pc de disco duro origen y

destino hay comunicación

C:\>ping dirección_IP_de_host_local_maestro

C:\>ping dirección_IP_de_host_local_esclavo

Realizar la copia del disco duro original

C:\>ROBOCOPY D:\ E:\ /E

Sustituye D: por la letra asignada al disco cuyo contenido se va a copiar.

Sustituye E: por la letra asignada al disco donde se va a pegar la información.

Linux:

Comprobar que las 2 Pc de disco duro origen y destino hay comunicación

[] ping dirección_IP_de_host_local_maestro

[] ping dirección_IP_de_host_local_esclavo

Trabajar como [root]

[] dd if=[origen] of=[destino]

[] dd if=/dev/hda of=/dev/hdb bs=1M con esto clonaríamos el disco hda en hdb. (discos IDE)

[] dd if=/dev/sda of=/dev/sdb bs=1M para discos (discos SATA)

Con bs=1M, estamos diciendo que tanto la lectura como la

escritura se haga en bloques de 1 megabyte (menos, sería más lento, pero más seguro, y con más nos arriesgamos a perder datos por el camino).

Hay que tener en cuenta que de esta forma grabarás el disco "tal cual", MBR, tabla de particiones, espacio vacío, etc., por lo que sólo podrás grabar en un disco del mismo o mayor tamaño

Mac OS X

Comprobar que las 2 Pc de disco duro origen y destino hay comunicación

[] ping dirección_IP_de_host_local_maestro

[] ping dirección_IP_de_host_local_esclavo

[] dd if=[origen] of=[destino]

[] $ dd if=/dev/hda of=/dev/hdb bs=1M con esto clonaríamos el disco hda en hdb. (discos IDE).

[] $ dd if=/dev/sda of=/dev/sdb bs=1M para discos (discos SATA)

Con bs=1M, estamos diciendo que tanto la lectura como la escritura se haga en bloques de 1 megabyte (menos, sería más lento, pero más seguro, y con más nos arriesgamos a perder datos por el camino).

Hay que tener en cuenta que de esta forma grabarás el disco "tal cual", MBR, tabla de particiones, espacio vacío, etc., por lo que sólo podrás grabar en un disco del mismo o mayor tamaño

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **FTK Imager** (http://www.accessdata.com/ftk-3-2)

Linux

• **DRBL 2.0.2-5** (http://drbl.org/download/live-table/changelog.php)

Mac OS_X

• **OndataRecoverySoft** (http://www.ondata-recoverysoft.com/)

OTRAS HERRAMIENTAS FORENSES:

Windows

• **EnCase** (http://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx)

• **DC3DD** (http://www.dc3.mil)

• **Forensic Replicator** (http://www.paraben.com/forensic-replicator.html)

• **X-Ways Forensics** (http://www.x-ways.com)

• **X-Ways Imager** (http://www.x-ways.com)

• **Norton Ghost 15.0.0.35659** (http://norton-ghost.softonic.com/)

• **Driver Backup 2.1** (http://drivershelper.net/drivers/index.html)

• **Cobian Backup 10.1.1.816** (http://www.cobiansoft.com/cobianbackup.htm)

• **CopyPod 8.6** (http://www.crackserialcodes.com/crack-copypod-8.6-serial-keygen.html)

• **Driver Genius Professional Edition 2005 6.1.2518** (http://driver-genius-professional-edition-2005.pcfiles.com/images/)

• **Casper XP 7.0.2230** (http://casper.uptodown.com/)

• **R-Drive Image 3.0 build 3029** (http://r-drive-image.pcfiles.com/)

Linux

• **SleunthKit** (http://www.sleuthkit.org/sleuthkit/download.php)

• **DC3DD** (http://www.dc3.mil)

Mac OS_X

• **DC3DD** (http://www.dc3.mil)

• **MacQuisition** (https://www.blackbagtech.com/software-products/macquisition-1/macquisition.html)

EJEMPLO:

Linux usando DRBL 2.0.2-5

Procedemos a crear la imagen del disco duro origen Este paso solo sería necesario la primera vez (o cuando deseamos crear una nueva imagen).

Hacemos doble click en “Clonezilla live” (Fig. 3.53.).

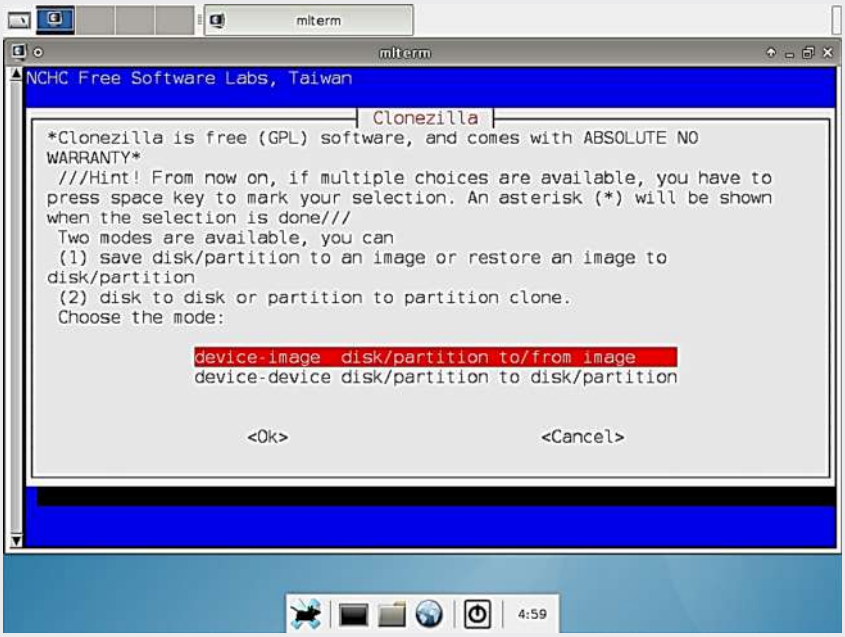


Fig. 3.53. Crear la imagen del disco duro origen

Deseamos crear una imagen de un dispositivo (device-image) o clonar directamente desde un disco/partición a otro (device-device). Seleccionamos la primera opción y pulsamos “enter” para seleccionar la opción) (Fig. 3.54.).

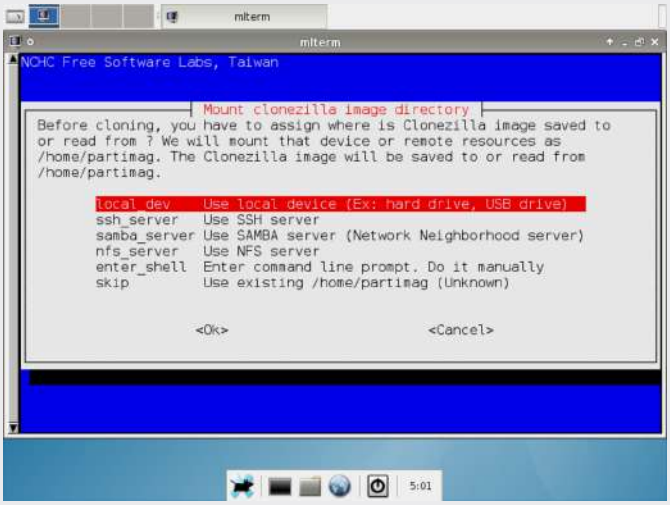


Fig. 3.54. Crear una imagen de un dispositivo (device-image) o clonar directamente desde un disco/partición a otro (device-device)

Escogemos el lugar donde deseamos guardar nuestra copia del disco duro original y escogemos en el disco duro copia (Fig. 3.55.).

Escogemos la opción ssh_server porque así clono la máquina origen y la grabo en el servidor (Pc destino) (Fig. 3.55., Fig. 3.,56 Fig. 3.57, Fig. 3.58, Fig. 3.59, Fig. 3.60, y Fig. 3.61.).

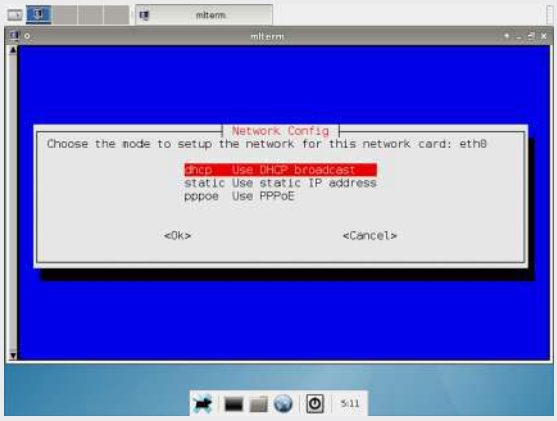


Fig. 3.55. Mostrar el lugar donde deseamos guardar nuestra copia del disco duro original y escogemos en el disco duro copia

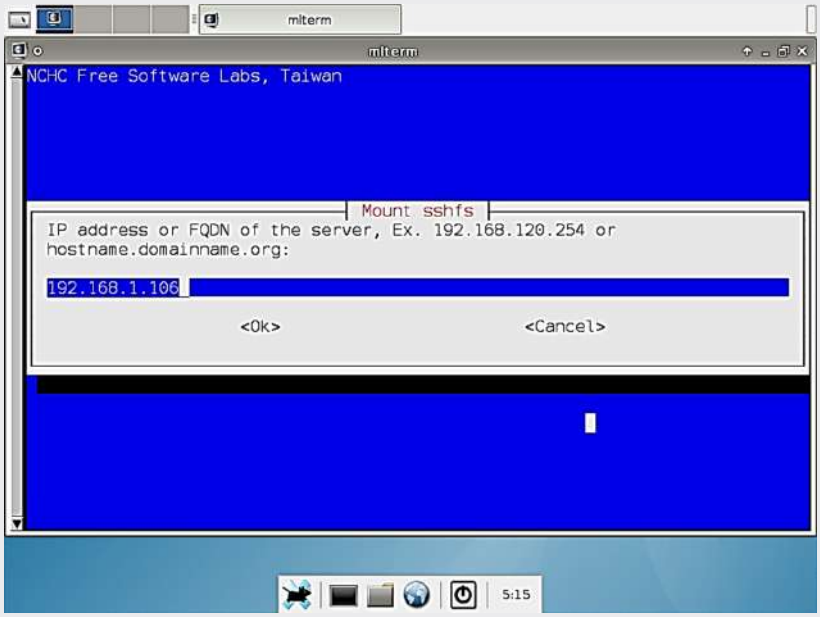


Fig. 3.56. Escogemos la opción ssh_server

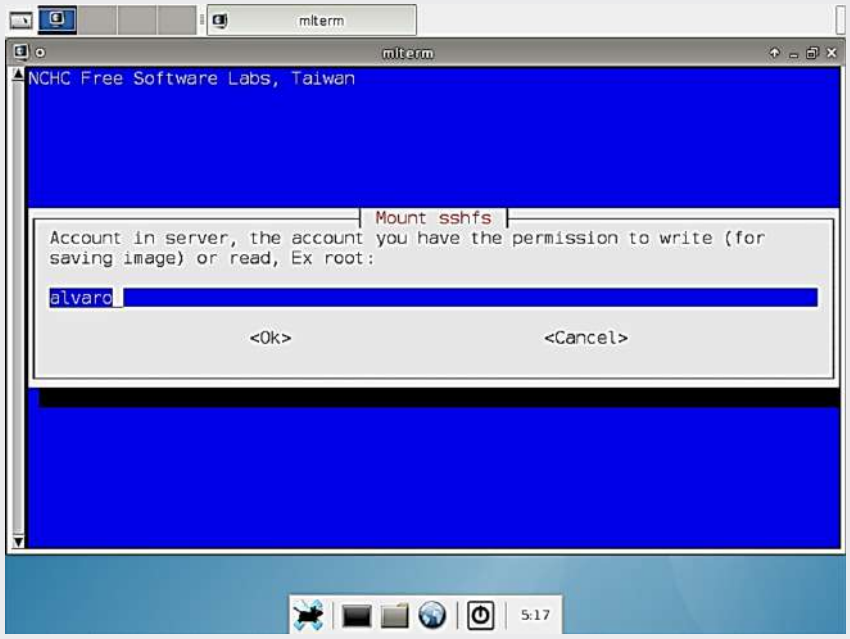


Fig. 3.57. Montar sshfs

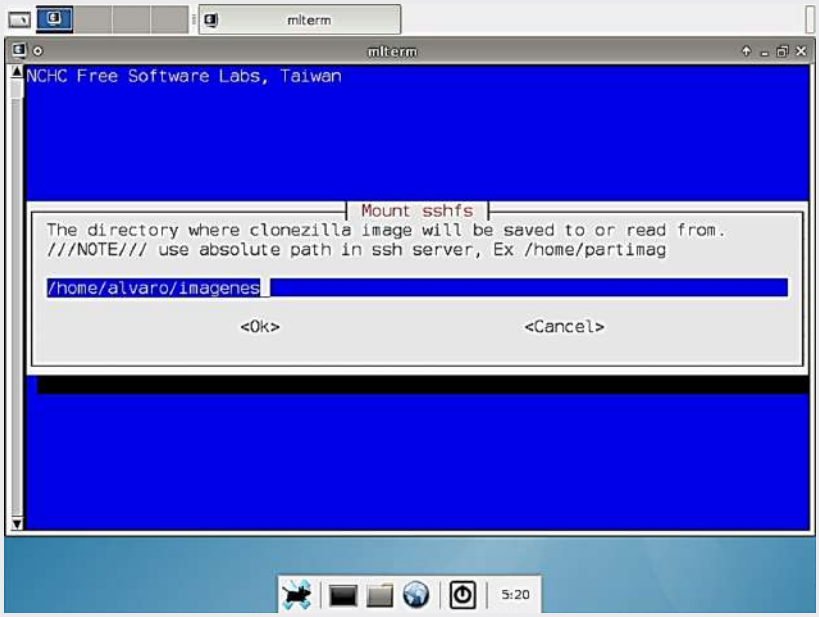


Fig. 3.58. Ubicación donde montamos sshfs

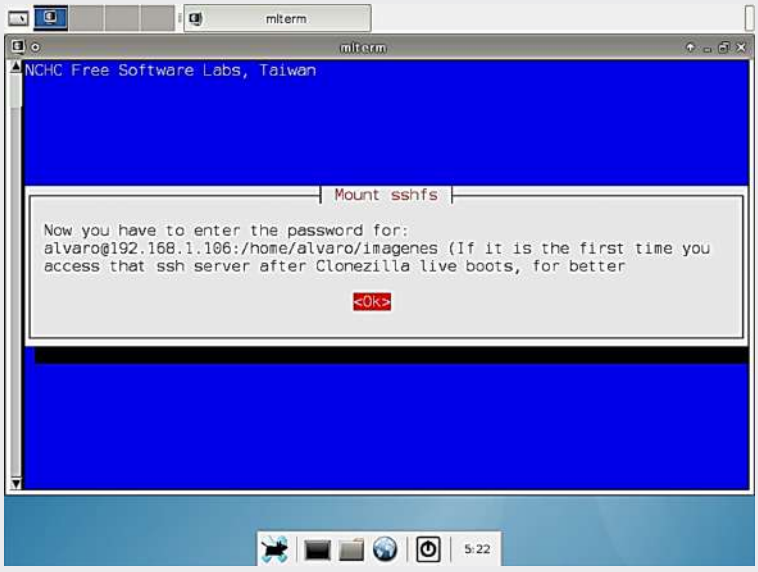


Fig. 3.59. Ahora está montada nuestro sshfs

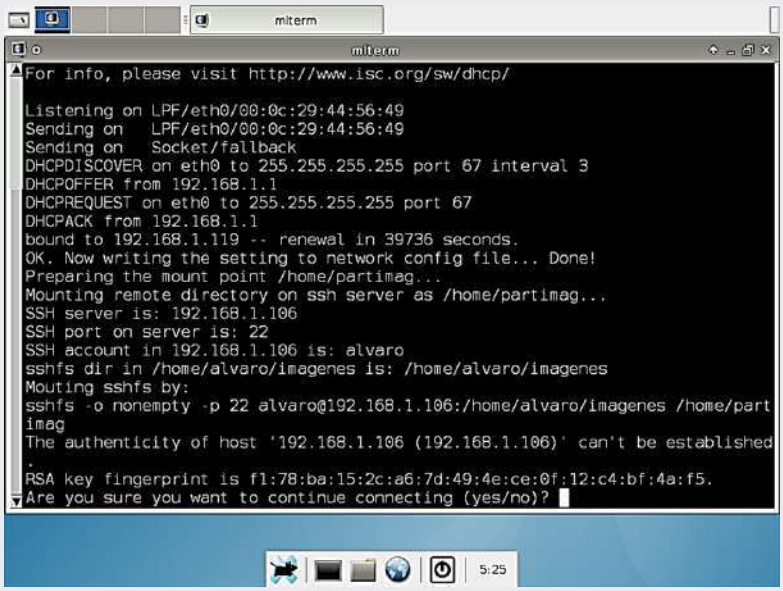


Fig. 3.60. Continuamos con el establecimiento de la conexión

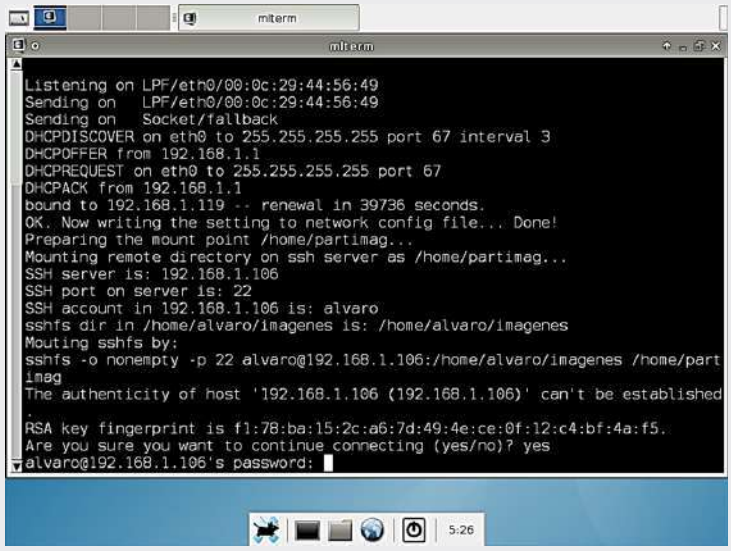


Fig. 3.61. Seguimos con el establecimiento de la conexión

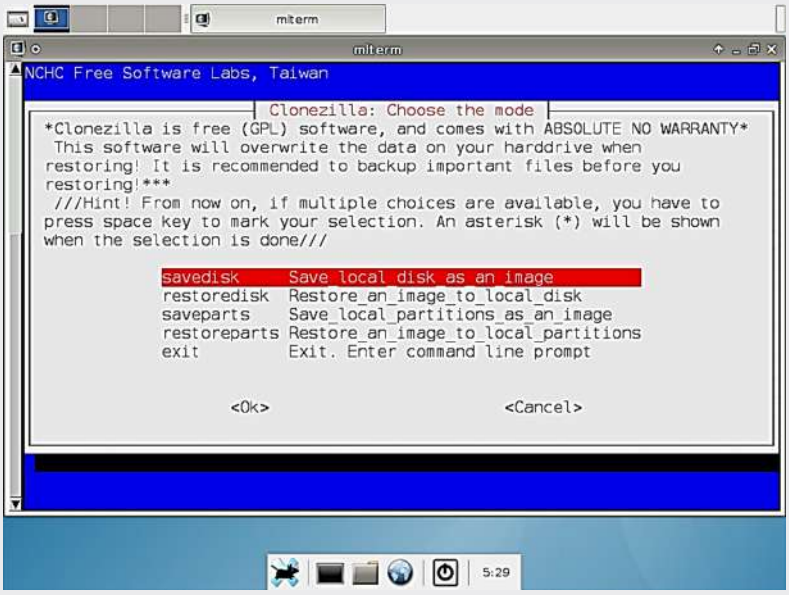


Fig. 3.62. Grabamos la imagen del disco duro local

Escojo la opción savedisk porque me permite crear la imagen del disco duro entero (Fig. 3.62.).

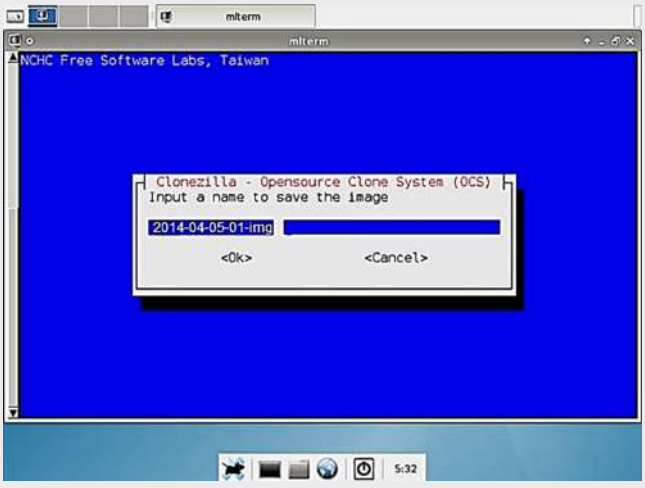


Fig. 3.63. Introducimos un nombre a nuestra imagen

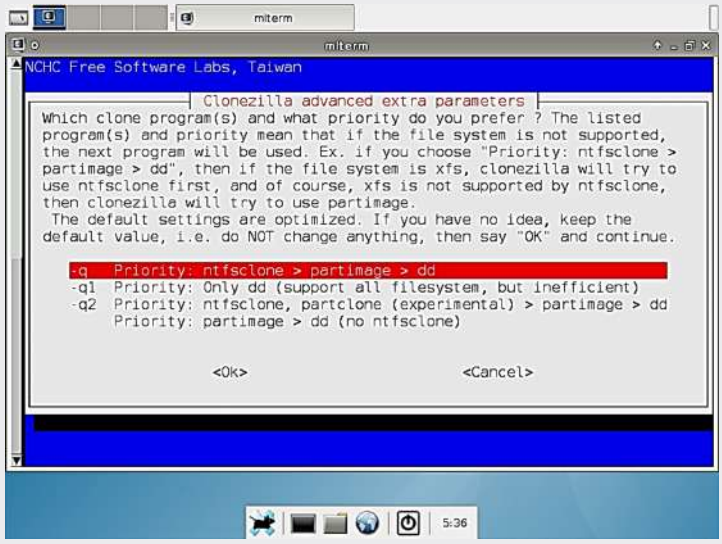


Fig. 3.64. Escogemos la prioridad a grabar

Aquí nos pregunta cómo queremos crear la imagen y escojo -q ya que es una forma estándar, y recomiendo usar esta ya que la imagen también se comprime (Fig. 3.63. y Fig. 3.64.)

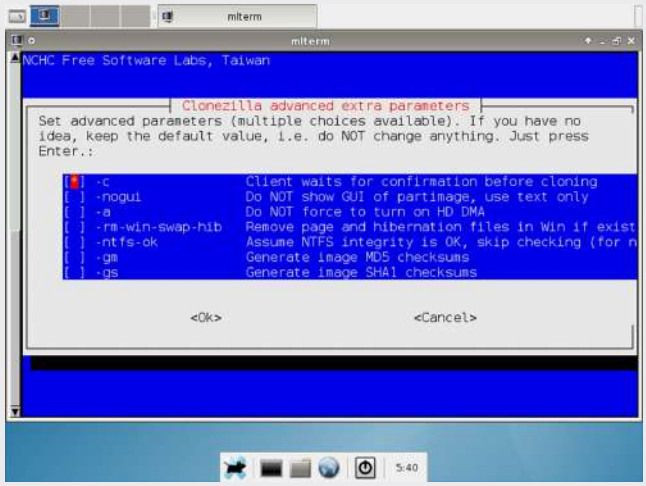


Fig. 3.65. Esperamos la confirmación para clonar nuestro disco duro

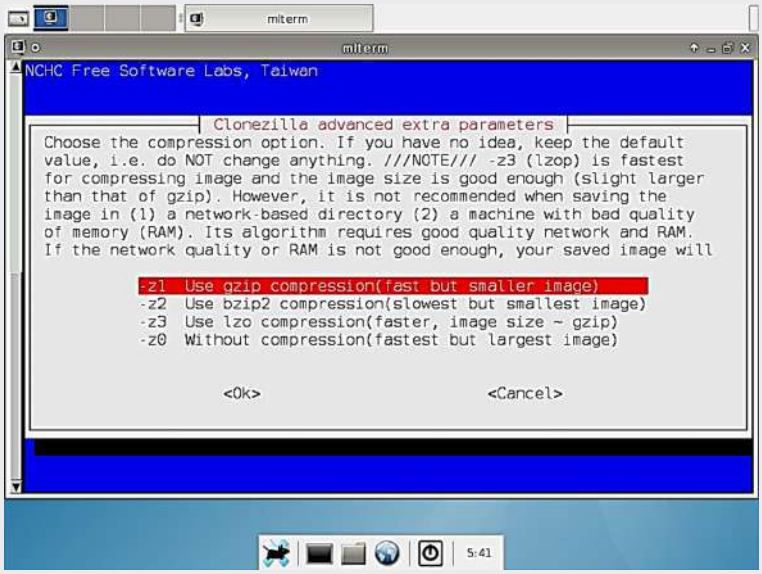


Fig. 3.66. Escojo la opción –Z1 para comprimir la imagen

Escojo la opción -Z1 ya que usa gzip para comprimir la imagen, tarda un tiempo razonable y la compresión también lo es (Fig. 3.65 y Fig. 3.66)

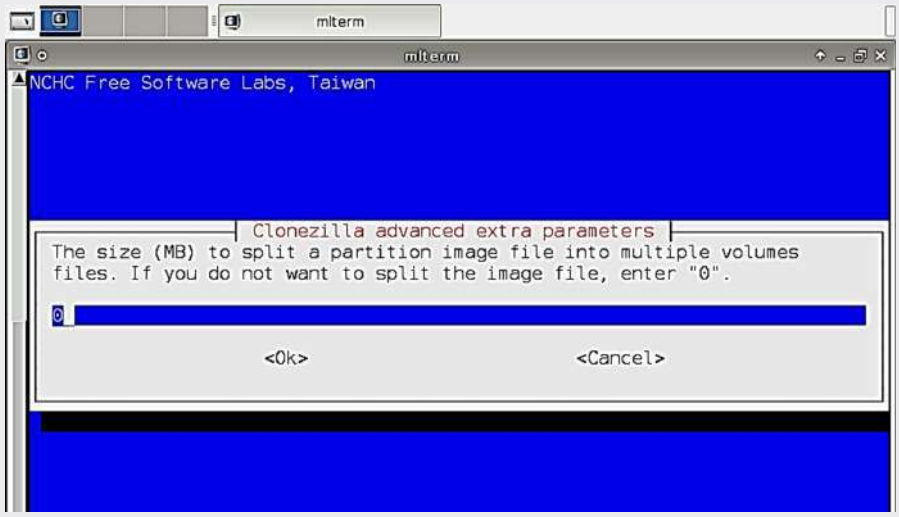


Fig. 3.67. Continuamos en la clonación

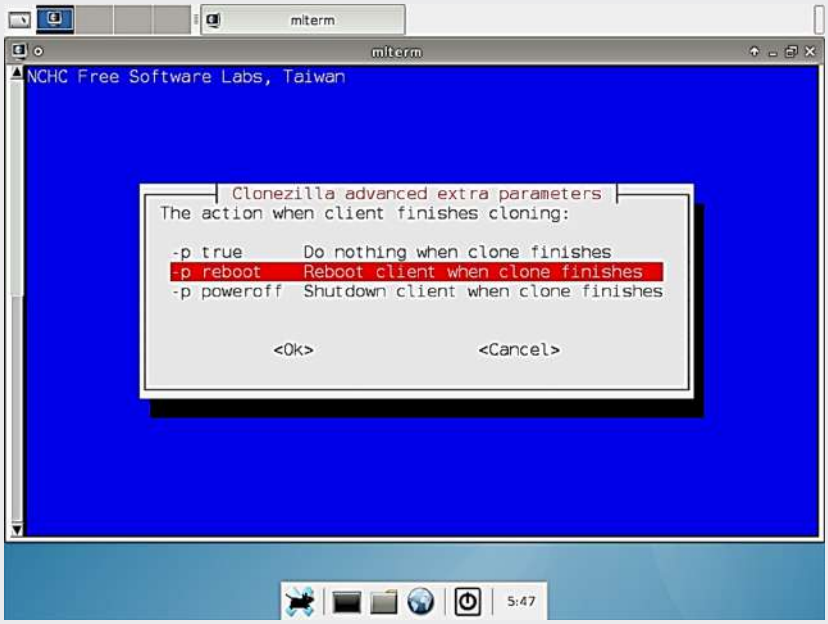


Fig. 3.68. Escoger la opción –p para reiniciar cuando finalice la copia

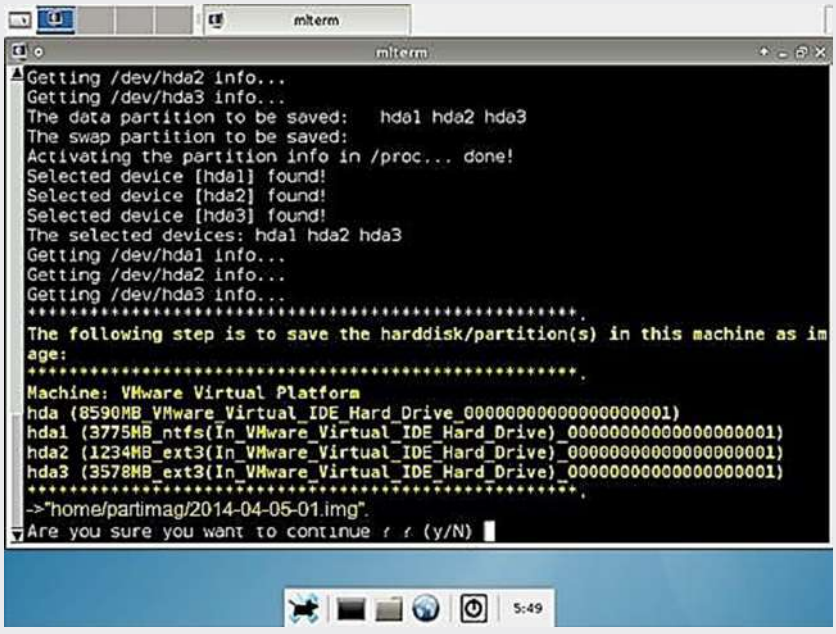


Fig. 3.69. Confirmamos el reinicio

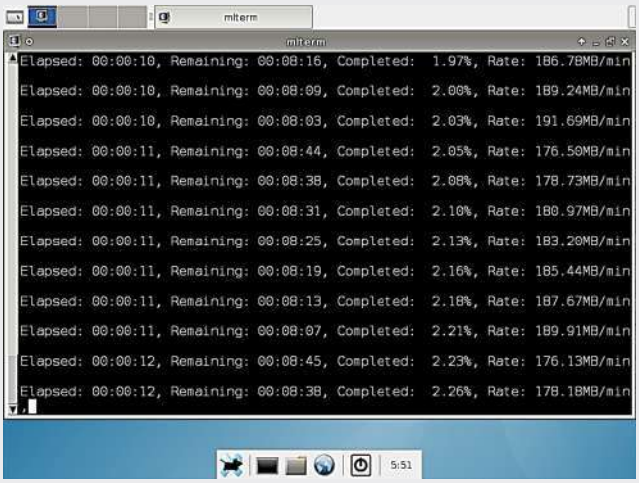


Fig. 3.70. Reinicio de pc

Una vez ya terminado el sistema se reiniciará solo (ya que elegimos esa opción). Volvemos a seleccionar la primera opción en el menú de arranque (Fig. 3.67, Fig. 3.68, Fig. 3.69, y Fig. 3.70).

Una vez cargado el escritorio hacemos doble click en el icono "Clonezilla

Server". Repetimos el proceso de configuración de la red (lo de DHCP y eso) igual que antes. Ahora nos salen muchas letras amarillas (Fig. 3.71. y Fig. 3.72.).

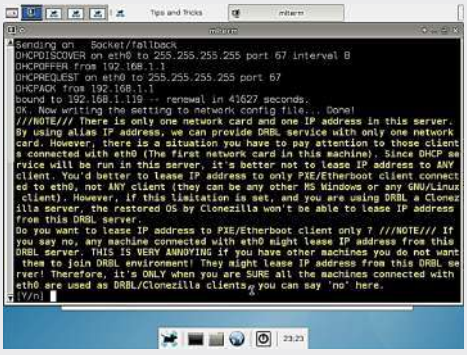


Fig. 3.71. Configuración de red (DHCP)

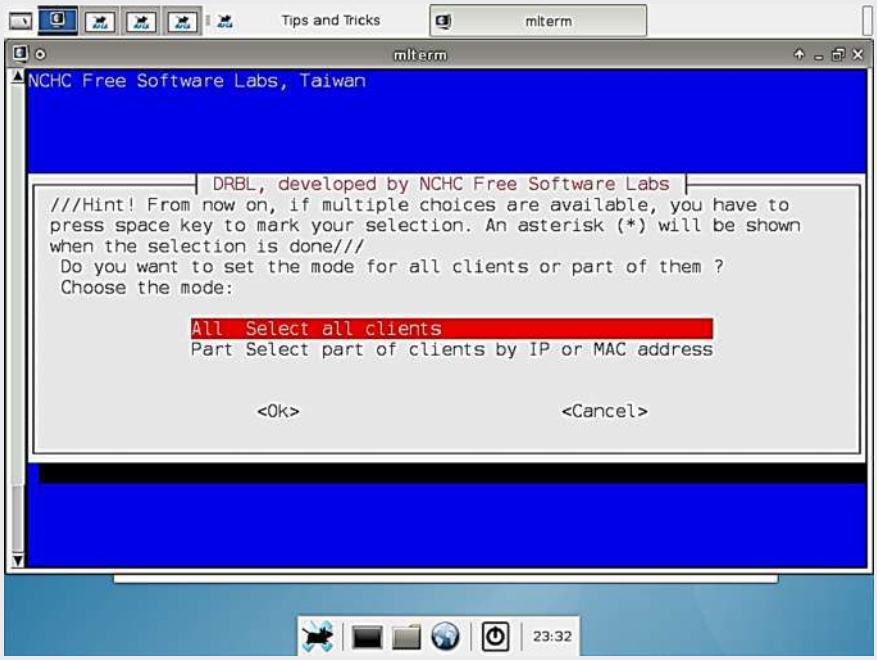


Fig. 3.72. Seleccionamos la opción para todos los clientes

Ahora nos pregunta que donde está la imagen, el menú es como el que hicimos antes donde seleccionamos "ssh_server", posteriormente la IP del servidor, el puerto, el usuario y la ruta de la imagen. Recuerda que es la ruta absoluta de la localización de la imagen en el servidor que en mi caso es "/home/alvaro/imagenes" (la misma ruta que pusimos antes). Remarco este punto porque he visto que es la parte que más confusión causa. Después te mostrará un par de confirmaciones (dar enter y punto) y configurará la red. No se asuste si por ahí algún failed, es simplemente porque apaga algún servicio (como el DHCP) antes de encenderlo para asegurarse de que estaba apagado antes de que el script lo inicie para que cargue la configuración (Fig. 3.73. y Fig. 3.74.).

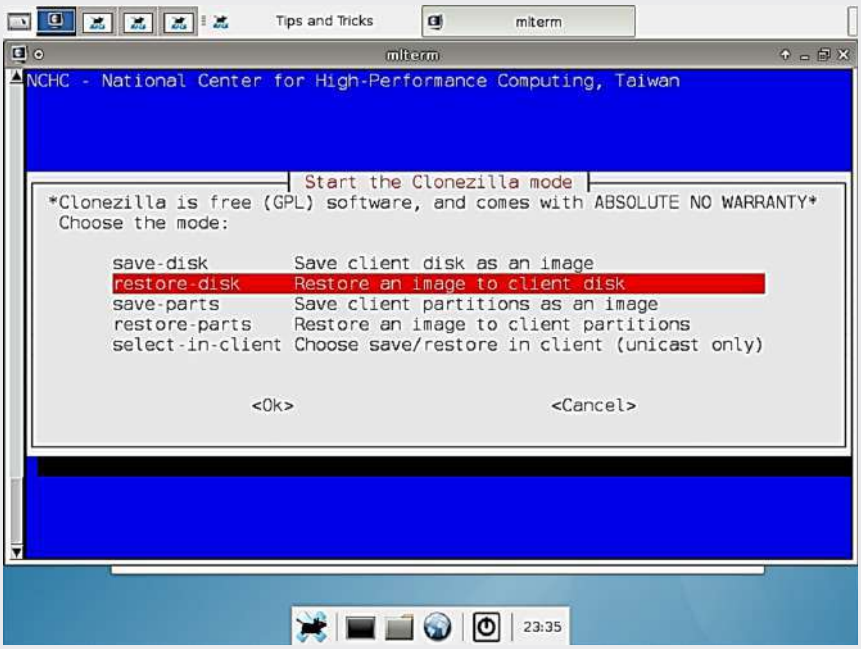


Fig. 3.73. Restaurar la imagen del disco

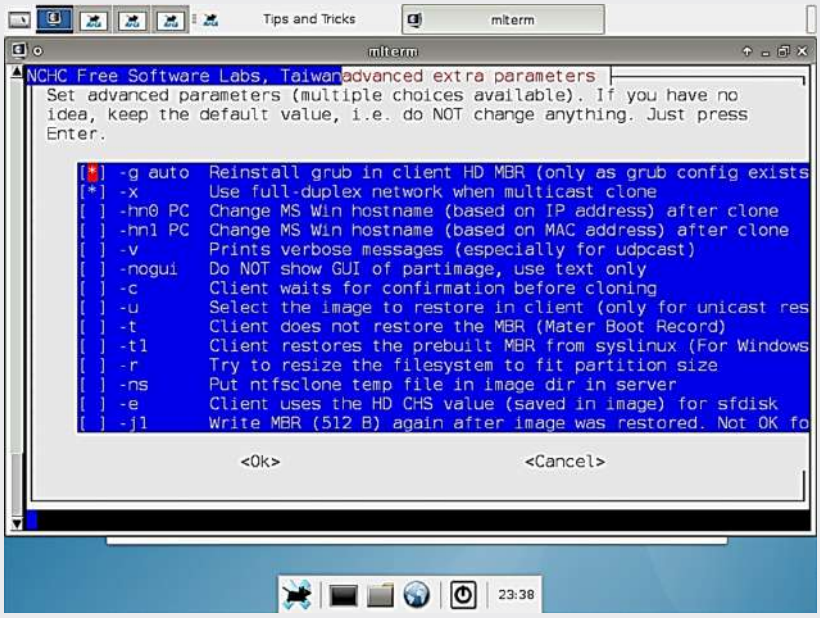


Fig. 3.74. Opciones predeterminadas y continuamos

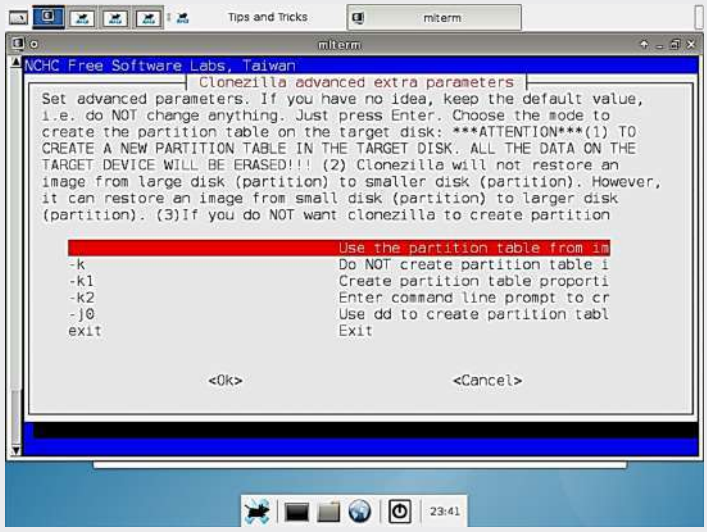


Fig. 3.75. Escogemos usar la tabla de particiones

Este menú es interesante, pero yo escojo la opción por defecto: Usa la tabla de particiones de la imagen (Fig. 3.75).

En nuestro caso usaremos ésta porque hemos hecho una réplica de todo el disco (Fig. 3.76., Fig. 3.77, Fig. 3.78, Fig. 3.79 y Fig. 3.80.).

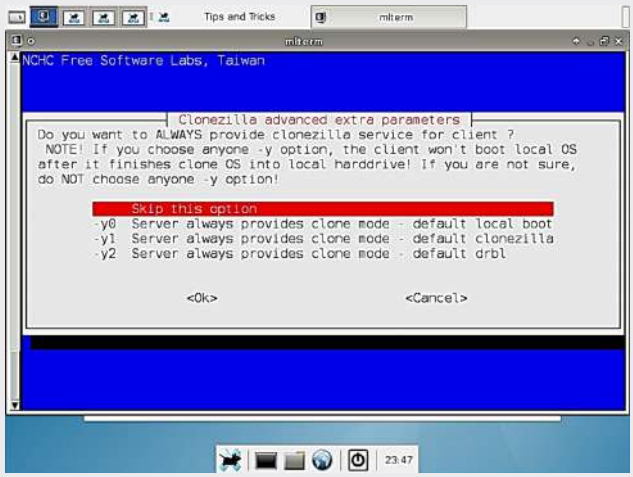


Fig. 3.76. Seleccionamos una opción

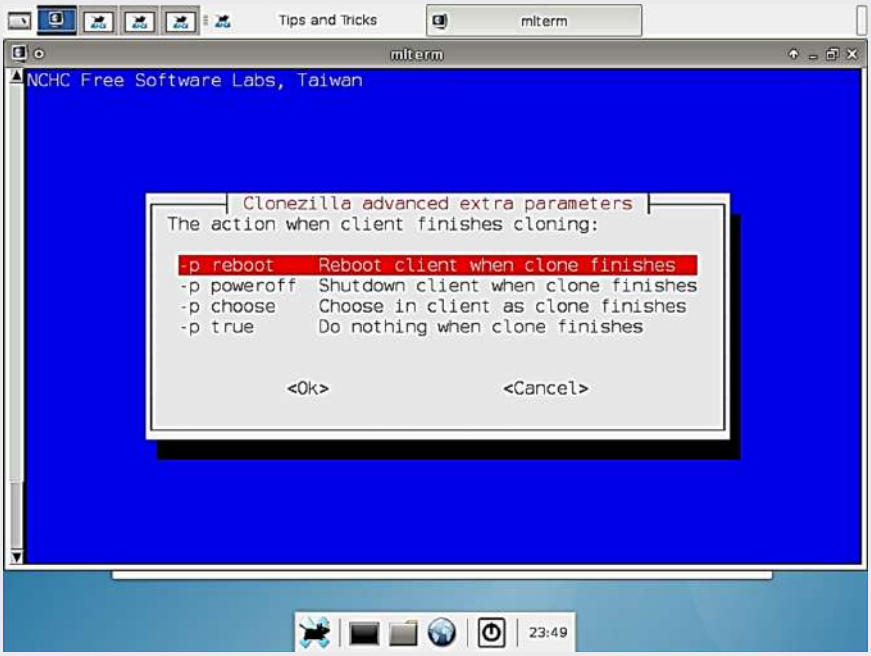


Fig. 3.77. Reinicio cuando termine la clonación

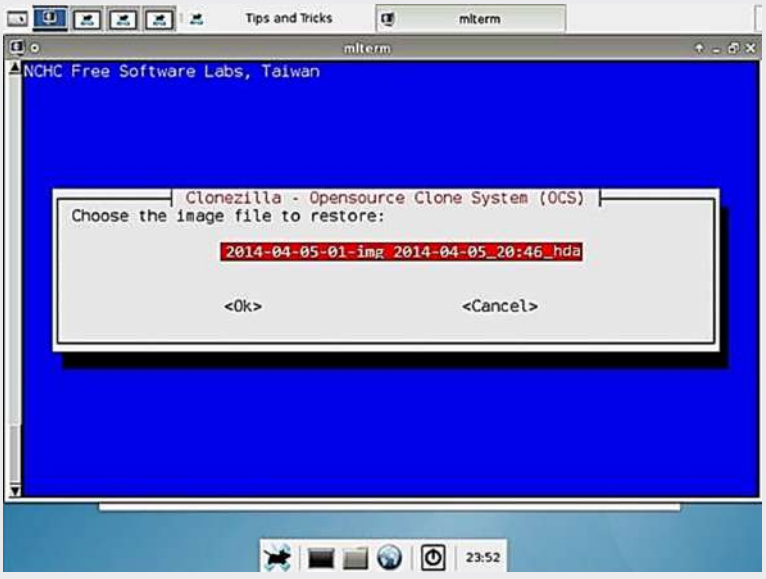


Fig. 3.78. Selección de la imagen a restaurarse

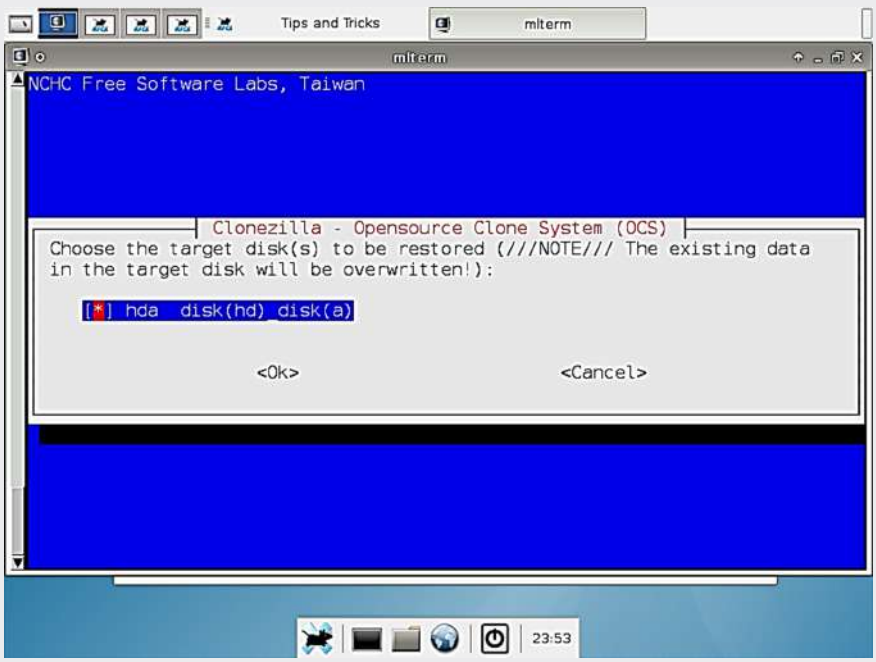


Fig. 3.79. Escogemos la ubicación del disco a restaurarse

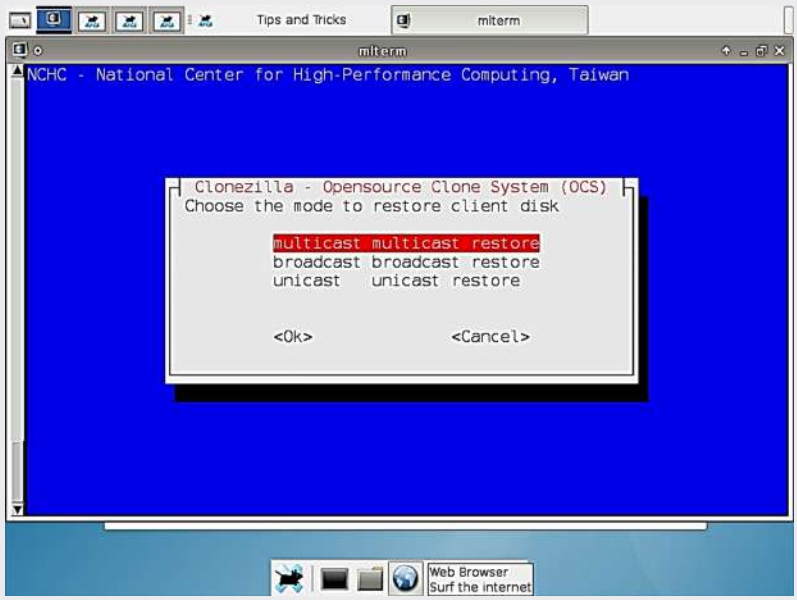


Fig. 3.80. Seleccionamos el modo a clonar nuestro disco

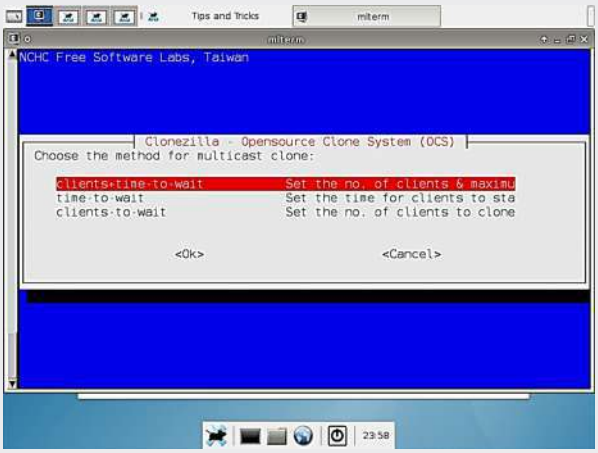


Fig. 3.81. Seleccionamos por el número de clientes a los que tiene que esperar o un tiempo máximo

Escojo la primera opción, clients+time-to-wait pues nos preguntara por el número de clientes a los que tiene que esperar o un tiempo máximo, lo que antes suceda es decir si tengo 40 clientes espere a los 40 o si alguno se atasca, pues que inicie el proceso sin él (Fig. 3.81., Fig. 3.82., Fig. 3.83. y Fig. 3.84.).

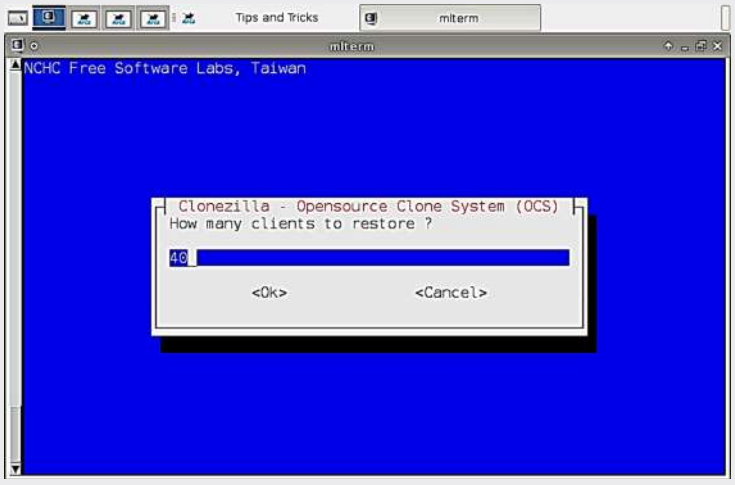


Fig. 3.82. Pulsamos la cantidad de clientes

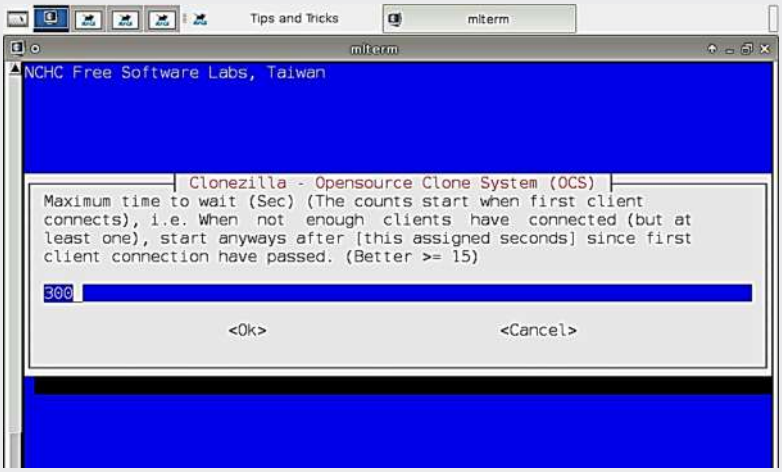


Fig. 3.83. Colocamos la cantidad de tiempo en segundos

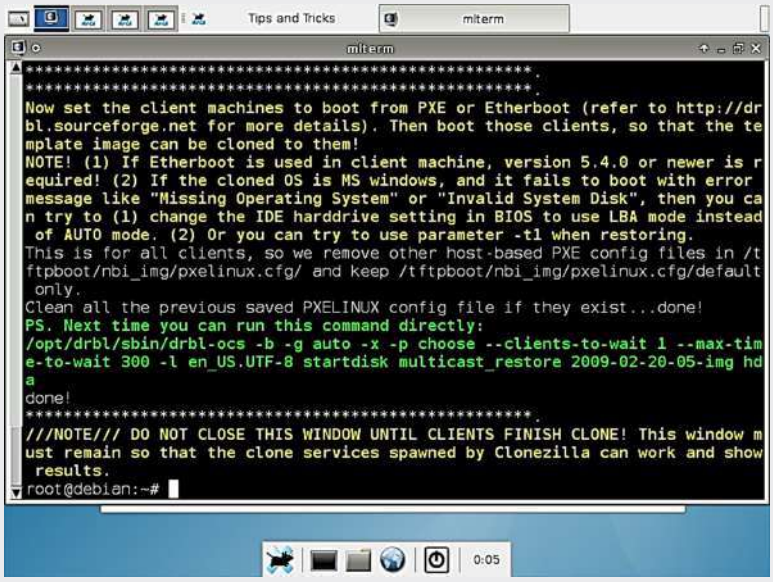


Fig. 3.84. Finalizado nuestra clonación

Si tenemos wake on lan y arranque por red (y activado en la bios) no tenemos más que usar el comando “sudo etherwake direccion_mac” y esperar. Si no, vamos metiendo un cd en cada ordenador y lo arrancamos seleccionando l un cd en cada ordenador y lo arrancamos seleccionando la última opción “Network boot via

etherboot" a última opción "Network boot via etherboot" esperar. Si no, vamos metiendo (Fig. 3.85., Fig. 3.86. y Fig. 3.87.)

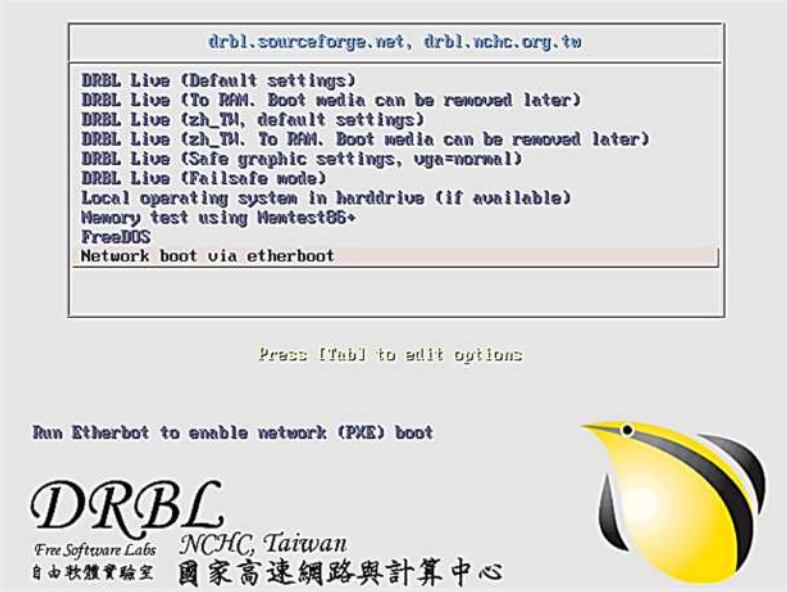


Fig. 3.85. Seleccionar la opción "Network boot via etherboot"

Fig. 3.86. Continuamos la restauración con clonezilla

Fig. 3.87. Pantalla de espera

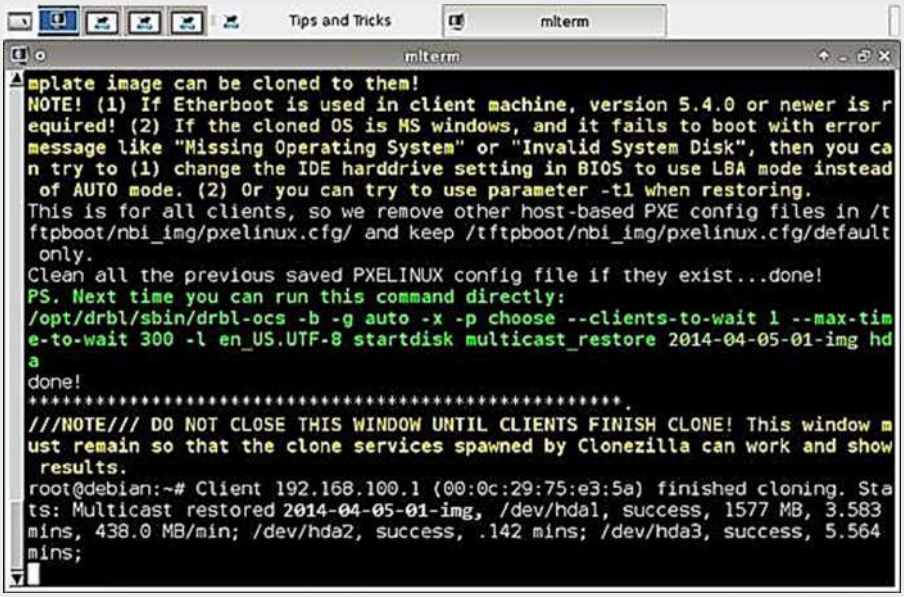


Fig. 3.88. Finalizado el proceso de clonación

Por fin terminamos. Ahora nuestra máquina virtual tiene el mismo sistema operativo y todo igual (Fig. 3.88.).

Tabla 3.9. Clonar Disco Duro RAID

ACCIÓN 9 TÍTULO: Clonar Disco Duro RAID

PROTOCOLO DE ACTUACION:

1. Conectar el disco duro USB con software de recuperación al Servidor

2. Reiniciar el servidor con el disco duro USB conectado

3. Si no se despliega la pantalla; se requiere modificar el BIOS de arranque para que se inicie por el disco duro USB

4. Copiar disco duro RAID a imagen

5. Asignar un nombre a la imagen y guardar

6. Retirar el disco duro USB

COMANDOS DEL SISTEMA:

Instalación de paquetes

Los paquetes necesarios para implementar un RAID en conjunción con un LVM serán los siguientes:

• **mdadm**

Para instalarlos teclee en una terminal de BASH lo siguiente:

[BASH]# yum install mdadm

Instalación y configuración del RAID

El principal requisito para implementar un RAID será disponer de dos discos duros de la misma capacidad. Estos discos duros

deberán tener asignadas las siguientes particiones: El disco duro numero 1 contendrá dos particiones

• sda1 será para la /

• sda2 será para la SWAP

El disco duro numero 2 deberá contener igualmente dos particiones

• sdb1 del mismo tamaño que sda1

• sdb2 del mismo tamaño que sda2

Estas particiones pueden ser creadas con la ayuda de fdisk,. Una vez creadas las particiones solo restara asignar el identificador correspondiente a particiones tipo RAID, para hacerlo haga lo siguiente: Abra una terminal y

teclee:

[BASH]# fdisk /dev/[h|s] d [a|b|c]

Donde:

h La letra 'h' hace referencia a un disco duro SATA.

Ejemplo: hd

s La letra 's' hace referencia a un disco duro SATA.

Ejemplo: sd

a La letra 'a' hace referencia al primer disco duro del equipo

b La letra 'b' hace referencia al segundo disco duro del equipo

c La letra 'c' hace referencia al tercer disco duro del equipo

En nuestro caso, contamos con un solo disco duro SATA en el equipo, por lo que ejecutaremos fdisk de la siguiente manera:

[BASH]# fdisk /dev/hdb

Una vez que la aplicación esta iniciada, se nos presenta el siguiente mensaje:

Command (m for help):

Si usted presiona la tecla 'm' se imprimirá el menú con las herramientas propias del comando fdisk. Estas herramientas son:

Tabla 3.10. Herramientas del comando fdisk

a	Conmuta el indicador de iniciable
b	Modifica la etiqueta de disco bsd
c	Conmuta el indicador de compatibilidad con DOS
d	Suprime una partición
l	Lista los tipos de particiones conocidos
m	Imprime este menú
n	Añade una nueva partición
o	Crea una nueva tabla de particiones DOS vacía
p	Imprime la tabla de particiones
q	Sale sin guardar los cambios
s	Crea una nueva etiqueta de disco Sun
t	Cambia el identificador de sistema de una partición
u	Cambia las unidades de visualización/entrada
v	Verifica la tabla de particiones
w	Escribe la tabla en el disco y sale
x	Funciones adicionales (sólo para usuarios avanzados)

Como podemos notar, con la opción "m" podemos imprimir nuevamente este menú. Seleccione del menú, la opción **"Cambiar el identificador de sistema de una partición"**, para ello teclee la letra 't', esto nos mostrara la distribución actual de nuestras particiones en nuestro disco duro.

fdisk, nos preguntara a que partición queremos cambiar el ID, estas particiones

serán:

• sdb1

• sdb2

Como no conocemos el código hexadecimal para las particiones RAID lanzamos la ayuda para poder visualizar todos los códigos hexadecimales disponibles, para ello teclee la letra 'L' y localiza el código hexadecimal para las particiones RAID. El código hexadecimal para las particiones RAID es el siguiente:

fd Linux raid auto

Una vez localizado el código hexadecimal, solo restara teclearlo. Para guardar los cambios al disco teclee la letra 'w' El siguiente paso sera asignar y crear el RAID. En una terminal de BASH teclee lo siguiente:

- [BASH]# mdadm --create /dev/md0 --level=1 --raid-disks=2 missing /dev/sdb1
- [BASH]# mdadm --create /dev/md1 --level=1 --raid-disks=2 missing /dev/sdb2

En donde:

Tabla 3.11. Opciones RAID

create /dev/ md0	Sera el nombre del RAID que estamos creando
level=1	Le indicamos que tipo de RAID estamos creando, en este caso RAID1
raid-disks=2	El número de dispositivos que forman el RAID
/dev/sda [] / dev/sdb[]	La lista de dispositivos que forma parte del RAID

Estos RAID los crearemos en modo degradado, de momento solo añadiremos al RAID los discos que hemos formateado, por lo que las entradas que corresponden al disco /dev/sda las dejamos en missing El siguiente paso será darles formato a las particiones RAID, para ello teclee lo siguiente (Recuerde que esta acción debe hacerse en nivel de ejecución 1).

[BASH]# mkfs.ext3 /dev/md0

[BASH]# mkswap /dev/md1}}}

Una vez hecho esto tenemos que modificar el fichero

/etc/mdadm.conf

para ello ejecutaremos

[BASH]# mdadm --examine --scan

Que nos devuelve información de nuestro RAID. De dicha información se deberá agregar las siguientes líneas al final del

fichero mdadm.conf

ARRAY /dev/md0 level=raid1 num-devices=2 UUI...

ARRAY /dev/md1 level=raid1 num-devices=2 UUI...}}}

Montaje del RAID

La siguiente acción será crear los puntos de montaje en donde serán alojadas nuestras particiones RAID. Para ello crearemos dos carpetas dentro de la ruta /mnt como se muestra a continuación.

[BASH]# mkdir /mnt/md0

[BASH]# mkdir /mnt/md1}}} Y luego de crearlas monte sobre ellas las particiones RAID creadas anteriormente

[BASH]# mount /dev/md0 /mnt/md0

[BASH]# mount /dev/md0 /mnt/md1}}} Ahora modificaremos el archivo

/etc/fstab

Para que nos monte las particiones RAID como RAIZ y SWAP, para ello deberá sustituir las siguientes líneas:

/dev/sda1 / ext3 defaults,errors=remount-ro 0 1

/dev/sda2 none swap sw 0 0}}} Por estas:

/dev/md0 / ext3 defaults,errors=remount-ro 0 1

/dev/md1 none swap sw 0 0}}} También se debe modificar el fichero

/etc/mtab

Hacemos lo mismo, sustituimos dentro del fichero /dev/sda1 por /dev/md0

Modificando el boteo de Linux

Ahora editaremos el menú del grub para que arranque el sistema operativo desde la partición RAID que hemos creado, para ello abra el fichero:

/boot/grub/menu.lst

Y duplica las líneas que hacen referencia a la partición en donde se encuentra los ficheros de boteo de Linux, en nuestro caso debe ser algo similar a esto:

title Centos 5.3, kernel 2.6.24-17-generic

root (hd0,0) kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/sda1 ro quiet

splash initrd /boot/initrd.img-2.6.24-17-generic quiet}}}

Y modificamos el primero para que apunte a /dev/md0 en el disco (hd1,0). El segundo lo dejamos apuntando a nuestra partición raíz actual por si no arranca correctamente desde /dev/md0. Al final nuestro fichero deberá quedar de la siguiente manera:

title Centos 5.3, kernel 2.6.24-17-generic

root (hd1,0) kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/md0

ro quiet

splash initrd /boot/initrd.img-2.6.24-17-generic quiet

title Centos 5.3, kernel 2.6.24-17-generic root (hd0,0) kernel /boot/vmlinuz2.6.24-17-generic

root=/dev/sda1 ro quiet splash initrd /boot/initrd.img-2.6.2417-generic quiet}}}

A continuación, actualizaremos el ramdisk Ramdisk es una porción de memoria ram la cual se utiliza como si fuera un disco duro. Los discos RAM tienen tamaños establecidos que son como una partición de disco. Los tiempos de acceso para un disco RAM son mucho más rápidos que en un disco físico, Sin embargo, cualquier información guardad en un ram disk se pierde cuando el sistema se apaga o reinicia. Pero son un buen lugar para almacenamiento temporal de datos. Desde la versión 2.4 del kernel de linux se puede encontrar soporte para ramdisks, por lo cual se puede encontrar en cualquier distribución moderna de linux Para hacer la actualización teclearemos lo siguiente en consola:

[BASH]# update-initramfs -u

Ya solo faltaría copiar todos los datos de / a la nueva partición desde la que va a arrancar ahora, para hacerlo teclee lo siguiente:

[BASH]# cp -dpRx / /mnt/md0

Donde:

Tabla 3.12. Opciones BASH

dp	Preserva los atributos de los ficheros (enlaces simbólicos, permisos, modos de lectura)
R	Copia recursivamente el contenido de las carpetas
x	Le indica que debe adaptarse al sistema de ficheros nuevo

Además de todos los pasos antes descritos debemos activar el grub en los dos discos duros, para ello teclee lo siguiente en una terminal de BASH:

[BASH]# grub

grub> root (hd1,0) grub> setup (hd1)

grub> root (hd0,0) grub> setup (hd0) exit}}}

Los siguiente será reiniciar el equipo el cual ya tiene que arrancar desde el RAID que como recordara se encuentra funcionando en modo degradado ya que solo dispone de un disco duro. Lo podemos verificar con el siguiente comando

[BASH]# df -h

Recuerde la partición /dev/md0 debe estar montada en /. Ahora que hemos conseguido arrancar el sistema desde el segundo disco duro es hora de preparar las particiones del primer disco para añadirlo al RAID, para hacerlo se tiene que modificar el identificador de estas particiones que al igual que lo hicimos con /dev/sdb1 y /dev/sdb2, se deberá hacer con /dev/sda1 y /dev/sda2. Luego de haber hecho el paso anterior añadiremos las particiones del disco duro 1 al RAID.

[BASH]# mdadm --add /dev/md0 /dev/sda1

[BASH]# mdadm --add /dev/md1 /dev/sda2}}}

Si compruebas ahora el fichero /proc/mdstat veras que se está sincronizando el RAID, hay que esperar hasta que finalice:

[BASH]# more /proc/mdstat

---------- Personalities : [raid1]

md2 : active raid1 sda1[2] sdb1[1] 8702093 blocks [2/1] [_U]
[=====>.....] recovery = 37.3% (3245881/8702093)
finish=2.4min speed=67433K/sec

md1 : active raid1 sda2[0] sdb2[1] 197920 blocks [2/2] [UU]}}}

Al finalizar el proceso nos debería arrojar un resultado como este:

Personalities: [raid1]

md2: active raid1 sda1[0] sdb1[1] 8702093 blocks [2/2] [UU]

md1: active raid1 sda2[0] sdb2[1] 197920 blocks [2/2] [UU]}}}

Lo cual nos quiere decir que ya lo tenemos correctamente sincronizando Volveremos a modificar el fichero

/etc/mdadm.conf

al cual tendremos que eliminar las lineas que habíamos añadido anteriormente y sustituirlas por las que nos devuelve ahora la ejecución del siguiente comando:

[BASH]# mdadm --examine --scan

En particular las siguientes lineas:

... ...

ARRAY /dev/md0 level=raid1 num-devices=2 UUI... ARRAY / dev/md1 level=raid1 num-devices=2 UUI...}}}

Debemos modificar de nuevo el grub para que la entrada que apunta todavía a /dev/sda1 apunte a /dev/md0 en el disco (hd0,0). Para hacerlo abra el fichero /boot/grub/menu.lst y cambie esta línea

kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/sda1 ro quiet splash

por esta otra

kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/md0 ro quiet splash

al final deberá lucir de la siguiente manera

title Centos 5.3, kernel 2.6.24-17-generic

root (hd1,0) kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/md0 ro quiet splash initrd /boot/initrd.img-2.6.24-17-generic quiet

title Centos 5.3, kernel 2.6.24-17-generic root (hd0,0) kernel /boot/ vmlinuz2.6.24-17-generic root=/dev/md0 ro quiet splash initrd / boot/initrd.img-2.6.2417-generic

quiet}}}

Con esto el sistema arrancara por defecto desde el disco hd1 y en el caso de que este disco falle deberemos indicarle anualmente que arranque desde la otra partición.

Para que el sistema arranque automáticamente desde el segundo disco si falla el primero debemos añadir fallback justo debajo de default en el fichero /boot/grub/menu.lst

... ...

default 0 fallback 1 ...}}} O sea, que arranque por defecto de la entrada 0 (la primera del listado) y en caso de error que arranque de la entrada 1 (la segunda del listado). Finalmente volvemos a actualizar el ramdisk

[BASH]# update-initramfs -u

Y por último reiniciamos el equipo

Comprobación final del RAID

Ahora el sistema debe ser capaz de arrancar desde cualquiera de los dos discos, aunque falle uno de ellos, puedes hacer pruebas desconectando uno de los discos para ver si todo sigue funcionando correctamente. Si no quieres abrir el equipo puedes simular un fallo de discos de la siguiente manera:

[BASH]# mdadm --manage /dev/md0 --fail /dev/sdb1

[BASH]# mdadm --manage /dev/md0 --remove /dev/sdb1}}}
Reiniciar y ahora el equipo deberá arrancar con el RAID en modo degradado.

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **Paragon Advanced Recovery CD** (http://www.paragon-software.com/home/br-free/download.html)

Linux

• **Clonezilla** (http://clonezilla.org/)

MAC OS_X

• **Clonezilla** (http://clonezilla.org/)

OTRAS HERRAMIENTAS FORENSES:

• **Acronis** (https://ac7-downloads.phpnuke.org/en/c62630/acronis-trueimage-home-free-download-full-review)

• **Ghost** (http://es.norton.com/downloads-trial-norton-online-backup)

EJEMPLO:

Mac OSX con Lion

En equipos Apple con el sistema operativo Snow Leopard (actualmente sustituido por Lion) pero ampliamente utilizado, se puede realizar un sistema RAID por software y utilizando 2 o más discos duros, particiones o dispositivos de almacenamiento externo.

Para configurar dos Discos como RAID necesitamos la aplicación 'Utilidad de Disco' que viene ya integrada con el sistema operativo y ubicada en la carpeta 'utilidades' (Fig. 3.89.).

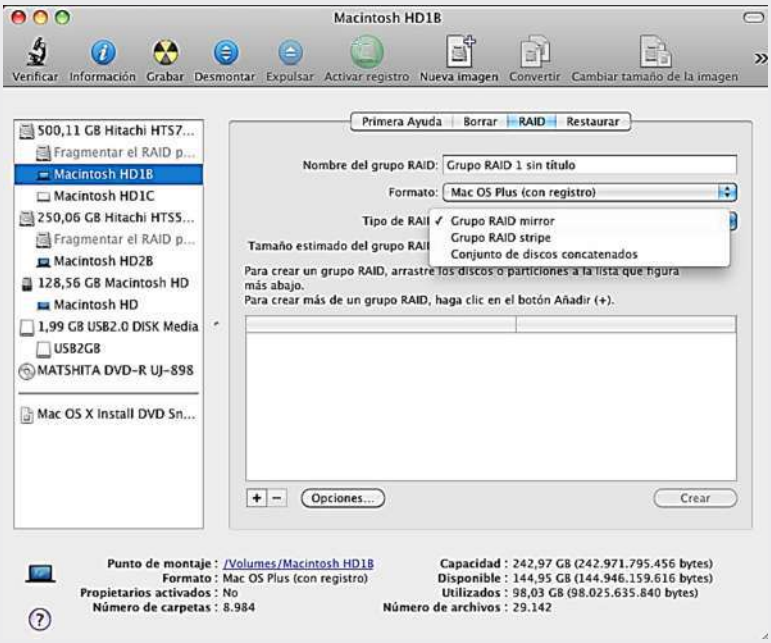


Fig. 3.89. Configuración de dos Discos como RAID

Cuando seleccionamos un disco duro o partición con la que queremos hacer un RAID, tenemos una pestaña llamada 'RAID'

donde tendremos todas las opciones disponibles:

• **Grupo RAID mirror:** Conocido también como RAID 1, proporciona seguridad al copiar en dos o más discos simultáneamente la información, de tal manera que si uno de los discos del grupo mirror se desconecta o falla el ordenador tiene acceso a los datos contenidos en el resto de Discos del Grupo.

• **Ventaja:** Conseguimos seguridad, los datos están duplicados en cada disco.

• **Desventaja:** La velocidad de escritura disminuye (discos diferentes) o se mantiene prácticamente igual en el mejor de los casos (discos iguales)

• **Grupo RAID stripe:** Conocido también como RAID 0, proporciona velocidad de acceso a los datos, lo que se hace es guardar la información repartida entre los discos que con forman el grupo stripe, de tal manera que el acceso es mucho más rápido al estar cada disco en canales diferentes, se pueden usar discos duros o particiones de igual o diferente tamaño (las mejores prestaciones se consiguen si son del mismo tamaño y características).

• **Ventaja:** Conseguimos velocidad de acceso (según discos se puede llegar al doble).

• **Desventaja:** Los datos están repartidos, si falla un disco perderemos la información

• **Conjunto de discos concatenados:** Sirve para crear un Disco de mayor tamaño, a partir de Discos más pequeños, similar en funcionamiento a RAID stripe pero la velocidad de acceso es menor, si los discos son de similar tamaño es mejor usar stripe.

También sirve para, a partir de un Raid 0 y un Raid 1 crear un Raid 10, con lo que conseguiríamos velocidad y seguridad (en este caso se necesitan 4 discos duros o particiones que estén en diferente puerto cada una para obtener todos los beneficios).

Para comprobar el funcionamiento del sistema RAID, he cogido una partición de cada Disco duro (de igual tamaño, 128GB) y le he aplicado RAID mirror, en mi caso al contener una de las particiones el sistema operativo he tenido que realizar una copia se seguridad previamente.

A tener en cuenta:

• Si la partición o disco duro que va a formar parte de RAID es con el que hemos arrancado, no nos permitirá añadirlo, deberemos de iniciar el sistema desde el DVD de instalación (que también contiene 'Utilidad de discos') o una instalación que tengamos en otro disco duro que no participe en la formación de RAID.

• Las particiones o discos duros con los que se vaya a formar RAID serán formateados por lo que hay que hacer copia de seguridad si contienen datos que no queramos perder.

Denotar que en este caso uno de los Discos duros es de 7200rpm y da velocidades de escritura/lecturas sostenidas de alrededor de 80MB/s, sin embargo, el otro Disco duro es de 5200rpm y las lecturas de escritura/lectura son de alrededor de 40MB/s. Tras la creación del RAID constato lo siguiente:

• La velocidad de escritura disminuye y es algo más rápida que el más lento.

• La velocidad de lectura es similar o un poco más rápida que el

más rápido.

En otra prueba he utilizado 2 tarjetas SD de 2GB iguales, le he aplicado la opción mirror y después la opción stripe y he comparado resultados con un programa de test de discos duros (Fig. 3.90., Fig. 3.91. y Fig. 3.92.).

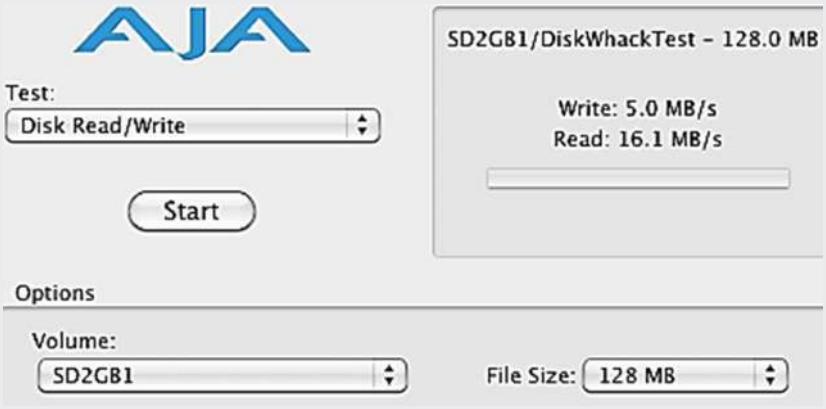


Fig. 3.90. Seleccionamos SD2GB1

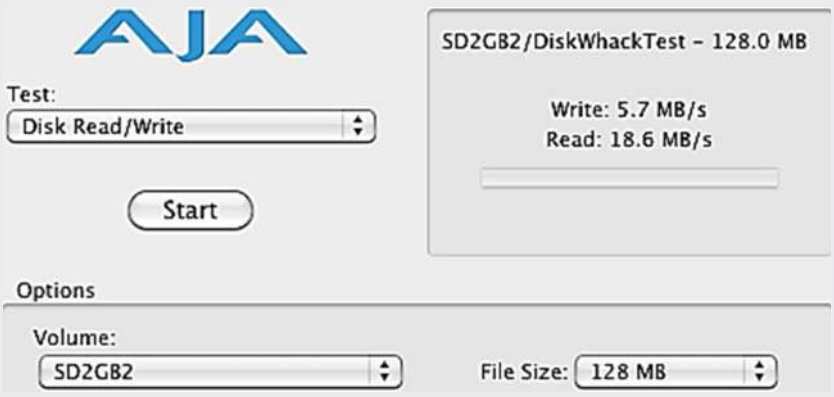


Fig. 3.91. Seleccionamos SD2GB2

Fig. 3.92. Confirmamos que deseamos crear grupo RAID

Nota: A la hora de crear el Grupo RAID marcamos la opción "Reconstruir Grupos RAID mirror automáticamente" de tal manera que cuando falle uno y/o reemplazamos o se desconecte y lo volvamos a conectar, el sistema lo reconstruya con la información del existente y lo incorpore al conjunto, si no lo hacemos no pasa nada, porque con la utilidad de discos tenemos la opción también para hacerlo de forma manual

A esta pantalla accedemos dando click en 'opciones' (Fig. 3.93.):

Fig. 3.93. Seleccionamos "Reconstruir Grupos RAID mirror automáticamente"

Tras el proceso se crea el conjunto RAID que aparecerá con el nombre que le hemos asignados (aparece de forma independiente cada disco y después el conjunto) (Fig. 3.94.):

Fig. 3.94. Crea el conjunto RAID que aparecerá con el nombre que le hemos asignados

Se ejecuta el Test y se comprueban resultados (Fig. 3.95.):

Fig. 3.95. Ejecución del Test y se comprueban resultados

Como se aprecia la velocidad de escritura es algo más lento y la velocidad de lectura se ha incrementado.

En RAID mirror se gana en seguridad al estar los datos duplicados en ambos discos, esto lo vamos a confirmar guardando un archivo y desconectando uno de los discos a ver qué pasa:

• En esta imagen se puede ver el archivo copiado y como los discos están en línea (Fig. 3.96.).

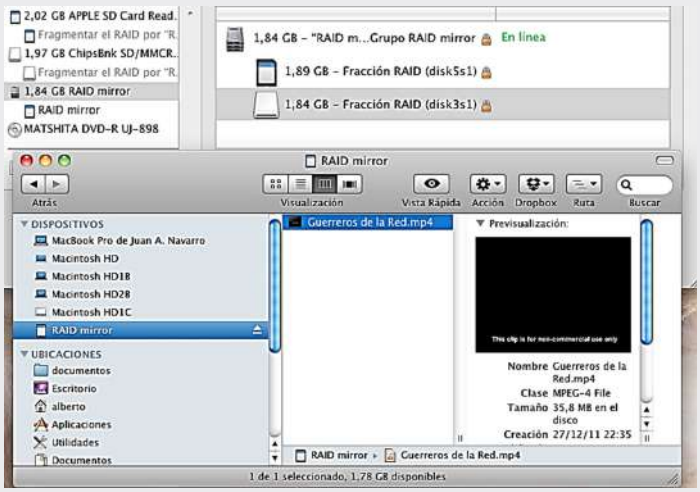


Fig. 3.96. Ver el archivo copiado y como los discos están en línea

Si retiramos de forma intempestiva uno de los discos, aún sigue apareciendo el conjunto RAID en Utilidad de disco, pero indicando un fallo.

En el explorador aparece el disco y el archivo sigue estando, en este caso contiene un vídeo, que si lo ejecutamos se visualiza correctamente (Fig. 3.97.).

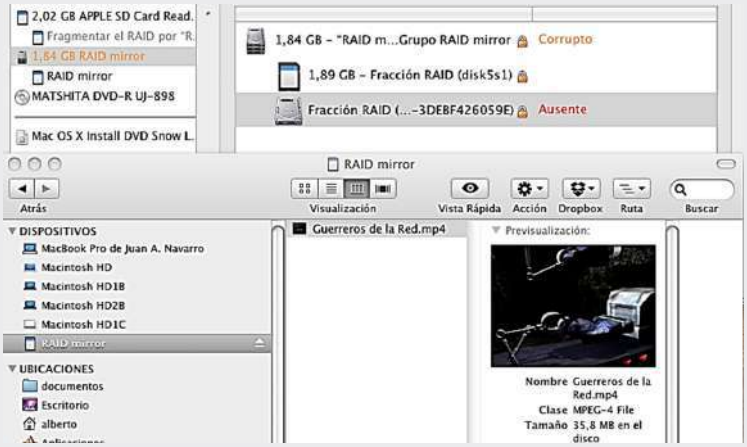


Fig. 3.97. Observamos el explorador aparece el disco y el archivo sigue estando

Si conectamos el Disco de nuevo el disco lo reconstruye automáticamente con la información del que está operativo (Fig. 3.98.).

Fig. 3.98. Reconstruye automáticamente con la información del que está operativo

Ya sea automáticamente si se ha marcado a la opción o manualmente con 'Utilidad de Discos', el proceso se realiza en segundo plano, por lo que podemos en nuestro caso seguir visualizando el vídeo contenido en la unidad.

Nota: Si eliminamos el Grupo RAID mirror, lo que pasa es que el sistema vuelve a dejarnos las dos unidades separadas como al principio, pero con los datos intactos y duplicados en los dos discos.

Como se puede ver en la siguiente imagen (Fig. 3.99.):

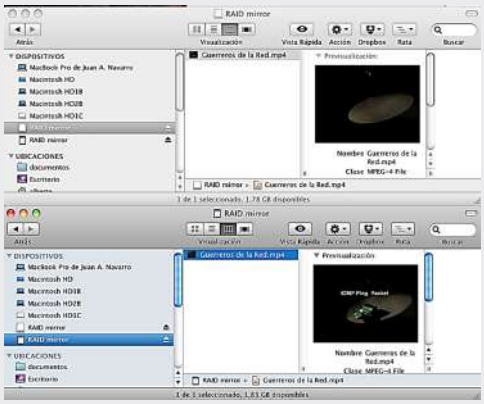


Fig. 3.99. Eliminamos el Grupo RAID mirror

Creamos el Grupo RAID stripe: Mismo procedimiento que el caso anterior, pero con la opción stripe (llamamos al conjunto 'RAID stripe', pero le podemos llamar como queramos) (Fig. 3.100.):

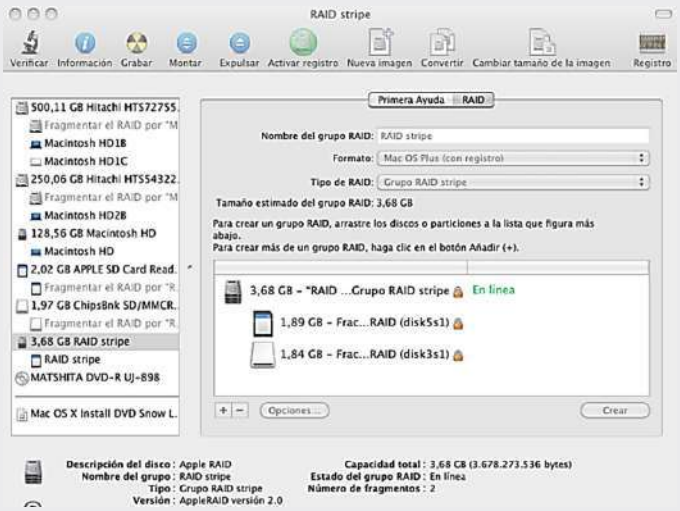


Fig. 3.100. Creación del Grupo RAID stripe

Nota: en este caso no tenemos la opción 'Reconstruir Grupos RAID mirror automáticamente', que como indica su nombre solo es válida para la opción mirror.

Se ejecuta el Test y se comprueban resultados (Fig. 3.101.):

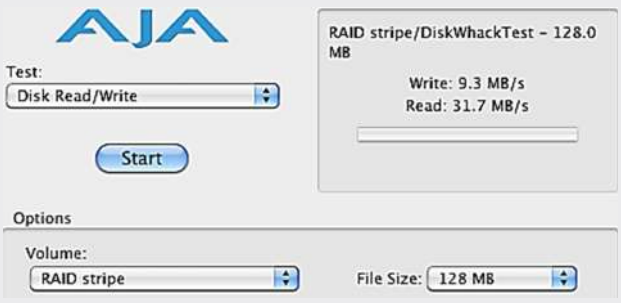


Fig. 3.101. Ejecución el Test y se comprueban resultados

Se puede apreciar como la velocidad de escritura prácticamente se duplica y la velocidad de lectura también mejora con respecto a la opción 'mirror' y por supuesto a si estuvieran como unidades normales.

Si retiramos de forma intempestiva uno de los discos, ya no aparece en el explorador de archivos (Finder en OS X) y en utilidad de Disco no avisa de la desconexión, esto es porque los datos están repartidos en ambos dispositivos y solo se puede reconstruir la información si ambos están presentes (Fig. 3.102.).

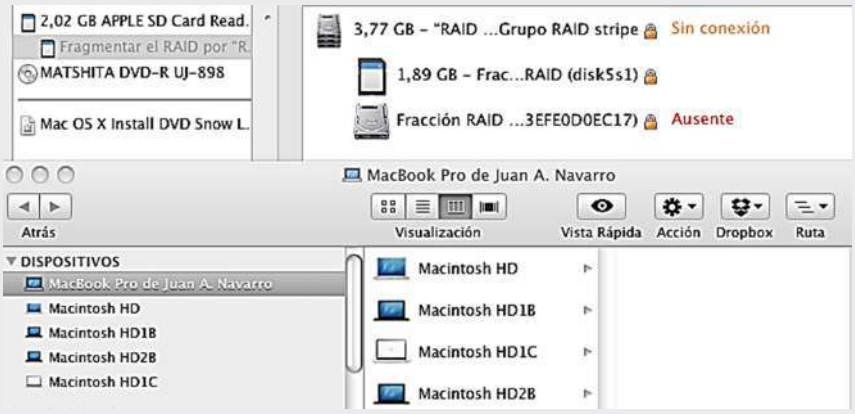


Fig. 3.102. Se aprecia como prácticamente la velocidad de escritura y lectura se duplican.

En este caso lo hemos desconectado cuando no estábamos realizando ninguna acción sobre el dispositivo y al volver a conectarlo todo vuelve a la normalidad.

Nota: Si eliminamos el Grupo RAID stripe perdemos todos los datos que contengan los dispositivos que lo formen y tendremos que volver a darles formato.

En función de las necesidades utilizaremos mirror o stripe, cada uno tiene ventajas e inconvenientes que deberemos valorar.

Tabla 3.13. Clonar RAID

ACCIÓN 10 TÍTULO: Clonar RAID

PROTOCOLO DE ACTUACION:

1. Conectar el disco duro USB con software de recuperación al Servidor

2. Encender el servidor con el disco duro USB conectado

3. Si no se despliega la pantalla; se requiere modificar el BIOS de arranque para que se inicie por el disco duro USB

4. Copiar disco duro RAID a imagen

5. Asignar un nombre a la imagen y guardar

6. Retirar el disco duro USB

COMANDOS DEL SISTEMA:

Instalación de paquetes

Los paquetes necesarios para implementar un RAID en conjunción con un LVM serán los siguientes:

• **mdadm**

Para instalarlos teclee en una terminal de BASH lo siguiente:

[BASH]# yum install mdadm

Instalación y configuración del RAID

El principal requisito para implementar un RAID será disponer de dos discos duros de la misma capacidad. Estos discos duros deberán tener asignadas las siguientes particiones: El disco duro numero 1 contendrá dos particiones

• sda1 será para la /

• sda2 será para la SWAP

El disco duro numero 2 deberá contener igualmente dos particiones

• sdb1 del mismo tamaño que sda1

• sdb2 del mismo tamaño que sda2

Estas particiones pueden ser creadas con la ayuda de fdisk. Una vez creadas las particiones solo restara asignar el identificador correspondiente a particiones tipo RAID, para hacerlo haga lo siguiente: Abra una terminal y teclee:

[BASH]# fdisk /dev/[h|s] d [a|b|c]

Donde:

Tabla 3.14. Herramientas del comando fdisk

h	La letra 'h' hace referencia a un disco duro-SATA. Ejemplo: hd
s	La letra 's' hace referencia a un disco duro-SATA. Ejemplo: sd
a	La letra 'a' hace referencia al primer disco duro del equipo
b	La letra 'b' hace referencia al segundo disco duro del equipo
c	La letra 'c' hace referencia al tercer disco duro del equipo

En nuestro caso, contamos con un solo disco duro-SATA en el equipo, por lo que ejecutaremos fdisk de la siguiente manera:

[BASH]# fdisk /dev/hdb

Una vez que la aplicación esta iniciada, se nos presenta el siguiente mensaje:

Command (m for help):

Si usted presiona la tecla 'm' se imprimirá el menú con las herramientas propias del comando fdisk. Estas herramientas son:

Tabla 3.15. Herramientas propias del comando fdisk

a	Conmuta el indicador de iniciable
b	Modifica la etiqueta de disco bsd
c	Conmuta el indicador de compatibilidad con DOS
d	Suprime una partición
l	Lista los tipos de particiones conocidos
m	Imprime este menú
n	Añade una nueva partición
o	Crea una nueva tabla de particiones DOS vacía
p	Imprime la tabla de particiones
q	Sale sin guardar los cambios
s	Crea una nueva etiqueta de disco Sun
t	Cambia el identificador de sistema de una partición
u	Cambia las unidades de visualización/entrada
v	Verifica la tabla de particiones
w	Escribe la tabla en el disco y sale
x	Funciones adicionales (sólo para usuarios avanzados)

Como podemos notar, con la opción "m" podemos imprimir nuevamente este menú. Seleccione del menú, la opción **"Cambiar el identificador de sistema de una partición"**, para ello teclee la letra 't', esto nos mostrara la distribución actual de nuestras particiones en nuestro disco duro.

fdisk, nos preguntara a que partición queremos cambiar el ID, estas particiones serán:

• sdb1

• sdb2

Como no conocemos el código hexadecimal para las particiones RAID lanzamos la ayuda para poder visualizar todos los códigos hexadecimales disponibles, para ello teclee la letra 'L' y localiza el código hexadecimal para las particiones RAID. El código hexadecimal para las particiones RAID es el siguiente:

fd Linux raid auto

Una vez localizado el código hexadecimal, solo restara teclearlo. Para guardar los cambios al disco teclee la letra 'w' El siguiente paso sera asignar y crear el RAID. En una terminal de BASH teclee lo siguiente:

```
[BASH]# mdadm --create /dev/md0 --level=1 --raid-disks=2
missing /dev/sdb1

[BASH]# mdadm --create /dev/md1 --level=1 --raid-disks=2
missing /dev/sdb2
```

En donde:

Tabla 3.16. Opciones RAID

create /dev/ md0	Sera el nombre del RAID que estamos creando
level=1	Le indicamos que tipo de RAID estamos creando, en este caso RAID1
raid-disks=2	El número de dispositivos que forman el RAID
/dev/sda [] / dev/sdb[]	La lista de dispositivos que forma parte del RAID

Estos RAID los crearemos en modo degradado, de momento solo añadiremos al RAID los discos que hemos formateado, por lo que las entradas que corresponden al disco /dev/sda las dejamos en missing El siguiente paso será darles formato a las particiones RAID, para ello teclee lo siguiente (Recuerde que esta acción debe hacerse en nivel de ejecución 1).

[BASH]# mkfs.ext3 /dev/md0

[BASH]# mkswap /dev/md1}}}

Una vez hecho esto tenemos que modificar el fichero

/etc/mdadm.conf

para ello ejecutaremos

[BASH]# mdadm --examine --scan

Que nos devuelve información de nuestro RAID. De dicha información se deberá agregar las siguientes lineas al final del fichero **mdadm.conf**

ARRAY /dev/md0 level=raid1 num-devices=2 UUI...

ARRAY /dev/md1 level=raid1 num-devices=2 UUI...}}}

Montaje del RAID

La siguiente acción será crear los puntos de montaje en donde serán alojadas nuestras particiones RAID. Para ello crearemos dos carpetas dentro de la ruta /mnt como se muestra a continuación.

[BASH]# mkdir /mnt/md0

[BASH]# mkdir /mnt/md1}}} Y luego de crearlas monte sobre ellas las particiones RAID creadas anteriormente

[BASH]# mount /dev/md0 /mnt/md0

[BASH]# mount /dev/md0 /mnt/md1}}} Ahora modificaremos el archivo

/etc/fstab

Para que nos monte las particiones RAID como RAIZ y SWAP, para ello deberá sustituir las siguientes líneas:

/dev/sda1 / ext3 defaults,errors=remount-ro 0 1

/dev/sda2 none swap sw 0 0}}} Por estas:

/dev/md0 / ext3 defaults,errors=remount-ro 0 1

/dev/md1 none swap sw 0 0}}} También se debe modificar el fichero

/etc/mtab

Hacemos lo mismo, sustituimos dentro del fichero /dev/sda1 por /dev/md0

Modificando el boteo de Linux

Ahora editaremos el menú del grub para que arranque el sistema operativo desde la partición RAID que hemos creado, para ello abra el fichero:

/boot/grub/menu.lst

Y duplica las líneas que hacen referencia a la partición en donde se encuentra los ficheros de boteo de Linux, en nuestro caso debe ser algo similar a esto:

title Centos 5.3, kernel 2.6.24-17-generic

root (hd0,0) kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/sda1 ro quiet

splash initrd /boot/initrd.img-2.6.24-17-generic quiet}}}

Y modificamos el primero para que apunte a /dev/md0 en el disco (hd1,0). El segundo lo dejamos apuntando a nuestra partición raíz actual por si no arranca correctamente desde /dev/md0. Al final nuestro fichero deberá quedar de la siguiente manera:

title Centos 5.3, kernel 2.6.24-17-generic

root (hd1,0) kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/md0 ro quiet

splash initrd /boot/initrd.img-2.6.24-17-generic quiet

title Centos 5.3, kernel 2.6.24-17-generic root (hd0,0) kernel /boot/ vmlinuz2.6.24-17-generic

root=/dev/sda1 ro quiet splash initrd /boot/initrd.img-2.6.2417-generic quiet}}}

A continuación, actualizaremos el ramdisk Ramdisk es una porción de memoria ram la cual se utiliza como si fuera un disco duro. Los discos RAM tienen tamaños establecidos que son como una partición de disco. Los tiempos de acceso para un disco RAM son mucho más rápidos que en un disco físico, Sin embargo, cualquier información guardad en un ram disk se pierde cuando el sistema se apaga o reinicia. Pero son un buen lugar para almacenamiento temporal de datos. Desde la versión 2.4 del kernel de linux se puede encontrar soporte para ramdisks, por lo cual se puede encontrar en cualquier distribución moderna de linux Para hacer la actualización teclearemos lo siguiente en consola:

[BASH]# update-initramfs -u

Ya solo faltaría copiar todos los datos de / a la nueva partición desde la que va a arrancar ahora, para hacerlo teclee lo siguiente:

[BASH]# cp -dpRx / /mnt/md0

Donde:

Tabla 3.17. Opciones BASH

dp	Preserva los atributos de los ficheros (enlaces simbólicos, permisos, modos de lectura)
R	Copia recursivamente el contenido de las carpetas
x	Le indica que debe adaptarse al sistema de ficheros nuevo

Además de todos los pasos antes descritos debemos activar el grub en los dos discos duros, para ello teclee lo siguiente en una terminal de BASH:

[BASH]# grub

grub> root (hd1,0) grub> setup (hd1)

grub> root (hd0,0) grub> setup (hd0) exit}}}

Los siguiente será reiniciar el equipo el cual ya tiene que arrancar desde el RAID que como recordara se encuentra funcionando

en modo degradado ya que solo dispone de un disco duro. Lo podemos verificar con el siguiente comando

[BASH]# df -h

Recuerde la partición /dev/md0 debe estar montada en /. Ahora que hemos conseguido arrancar el sistema desde el segundo disco duro es hora de preparar las particiones del primer disco para añadirlo al RAID, para hacerlo se tiene que modificar el identificador de estas particiones que al igual que lo hicimos con /dev/sdb1 y /dev/sdb2, se deberá hacer con /dev/sda1 y /dev/sda2. Luego de haber hecho el paso anterior añadiremos las particiones del disco duro 1 al RAID.

[BASH]# mdadm --add /dev/md0 /dev/sda1

[BASH]# mdadm --add /dev/md1 /dev/sda2}}}

Si compruebas ahora el fichero /proc/mdstat veras que se está sincronizando el RAID, hay que esperar hasta que finalice:

[BASH]# more /proc/mdstat

---------- Personalities : [raid1]

md2 : active raid1 sda1[2] sdb1[1] 8702093 blocks [2/1] [_U]

[=====>.....] recovery = 37.3% (3245881/8702093)
finish=2.4min speed=67433K/sec

md1 : active raid1 sda2[0] sdb2[1] 197920 blocks [2/2] [UU]}}}
Al finalizar el proceso nos debería arrojar un resultado como este:

Personalities: [raid1]

md2: active raid1 sda1[0] sdb1[1] 8702093 blocks [2/2] [UU]

md1: active raid1 sda2[0] sdb2[1] 197920 blocks [2/2] [UU]}}}

Lo cual nos quiere decir que ya lo tenemos correctamente sincronizando Volveremos a modificar el fichero

/etc/mdadm.conf

al cual tendremos que eliminar las lineas que habíamos añadido anteriormente y sustituirlas por las que nos devuelve ahora la ejecución del siguiente comando:

[BASH]# mdadm --examine --scan

En particular las siguientes lineas:

... ...

ARRAY /dev/md0 level=raid1 num-devices=2 UUI... ARRAY /dev/md1 level=raid1 num-devices=2 UUI...}}}

Debemos modificar de nuevo el grub para que la entrada que apunta todavía a /dev/sda1 apunte a /dev/md0 en el disco (hd0,0). Para hacerlo abra el fichero /boot/grub/menu.lst y cambie esta línea

kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/sda1 ro quiet splash

por esta otra

kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/md0 ro quiet splash

al final deberá lucir de la siguiente manera

title Centos 5.3, kernel 2.6.24-17-generic

root (hd1,0) kernel /boot/vmlinuz-2.6.24-17-generic root=/dev/md0 ro quiet splash initrd /boot/initrd.img-2.6.24-17-generic quiet

title Centos 5.3, kernel 2.6.24-17-generic root (hd0,0) kernel /boot/vmlinuz2.6.24-17-generic root=/dev/md0 ro quiet splash initrd /boot/initrd.img-2.6.2417-generic quiet}}}

Con esto el sistema arrancara por defecto desde el disco hd1 y en el caso de que este disco falle deberemos indicarle anualmente que arranque desde la otra partición. Para que el sistema arranque automáticamente desde el segundo disco si falla el primero debemos añadir fallback justo debajo de default en el fichero /boot/grub/menu.lst

... ...

default 0 fallback 1 ...}}} O sea, que arranque por defecto de la entrada 0 (la primera del listado) y en caso de error que arranque de la entrada 1 (la segunda del listado). Finalmente volvemos a actualizar el ramdisk

[BASH]# update-initramfs -u

Y por último reiniciamos el equipo

Comprobación final del RAID

Ahora el sistema debe ser capaz de arrancar desde cualquiera de

los dos discos, aunque falle uno de ellos, puedes hacer pruebas desconectando uno de los discos para ver si todo sigue funcionando correctamente. Si no quieres abrir el equipo puedes simular un fallo de discos de la siguiente manera:

[BASH]# mdadm --manage /dev/md0 --fail /dev/sdb1

[BASH]# mdadm --manage /dev/md0 --remove /dev/sdb1}}}

Reiniciar y ahora el equipo deberá arrancar con el RAID en modo degradado.

HERRAMIENTAS FORENSES RECOMENDADAS:

Windows

• **Paragon Advanced Recovery CD** (http://www.paragon-software.com/home/br-free/download.html)

Linux

• **Clonezilla** (http://clonezilla.org/)

MAC OS_X

• **Clonezilla** (http://clonezilla.org/)

OTRAS HERRAMIENTAS FORENSES:

• **Acronis** (https://ac7-downloads.phpnuke.org/en/c62630/acronis-trueimage-home-free-download-full-review)

• **Ghost** (http://es.norton.com/downloads-trial-norton-online-backup)



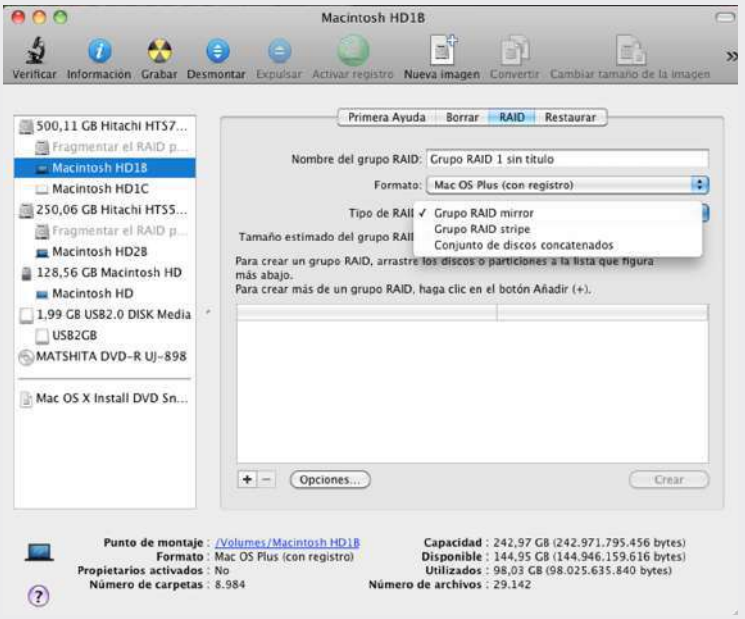
EJEMPLO:

MAC OSX con Lion

En equipos Apple con el sistema operativo Snow Leopard (actualmente sustituido por Lion) pero ampliamente utilizado, se puede realizar un sistema RAID por software y utilizando 2 o más discos duros, particiones o dispositivos de almacenamiento externo.

Para conFig.r dos Discos como RAID necesitamos la aplicación 'Utilidad de Disco' que viene ya integrada con el sistema operativo y ubicada en la carpeta 'utilidades' (Fig. 3.103.).

Fig. 3.103. Configuración de dos Discos como RAID



Cuando seleccionamos un disco duro o partición con la que queremos hacer un RAID, tenemos una pestaña llamada 'RAID' donde tendremos todas las opciones disponibles:

• **Grupo RAID mirror:** Conocido también como RAID 1, proporciona seguridad al copiar en dos o más discos simultáneamente la información, de tal manera que si uno de los discos del grupo mirror se desconecta o falla el ordenador tiene acceso a los datos contenidos en el resto de los discos del Grupo.

o Ventaja: Conseguimos seguridad, los datos están duplicados en cada disco.

o Desventaja: La velocidad de escritura disminuye (discos diferentes) o se mantiene prácticamente igual en el mejor de los casos (discos iguales).

• **Grupo RAID stripe:** Conocido también como RAID 0, proporciona velocidad de acceso a los datos, lo que se hace es guardar la información repartida entre los discos que con forman el grupo stripe, de tal manera que el acceso es mucho más rápido al estar cada disco en canales diferentes, se pueden usar discos duros o particiones de igual o diferente tamaño (las mejores prestaciones se consiguen si son del mismo tamaño y características).

o Ventaja: Conseguimos velocidad de acceso (según discos se puede llegar al doble).

o Desventaja: Los datos están repartidos, si falla un disco perderemos la información.

• **Conjunto de discos concatenados:** Sirve para crear un Disco de mayor tamaño, a partir de Discos más pequeños, similar en funcionamiento a RAID stripe pero la velocidad de acceso es menor, si los discos son de similar tamaño es mejor usar stripe.

También sirve para, a partir de un Raid 0 y un Raid 1 crear un Raid 10, con lo que conseguiríamos velocidad y seguridad (en este caso se necesitan 4 discos duros o particiones que estén en diferente puerto cada una para obtener todos los beneficios).

Para comprobar el funcionamiento del sistema RAID, he cogido una partición de cada Disco duro (de igual tamaño, 128GB) y le he aplicado RAID mirror, en mi caso al contener una de las particiones el sistema operativo he tenido que realizar una copia se seguridad previamente.

A tener en cuenta:

• Si la partición o disco duro que va a formar parte de RAID es con el que hemos arrancado, no nos permitirá añadirlo, deberemos de iniciar el sistema desde el DVD de instalación (que también contiene 'Utilidad de discos') o una instalación que tengamos en otro disco duro que no participe en la formación de RAID.

• Las particiones o discos duros con los que se vaya a formar RAID serán formateados por lo que hay que hacer copia de seguridad si contienen datos que no queramos perder.

• Apuntar que en este caso uno de los Discos duros es de 7200rpm y da velocidades de escritura/lecturas sostenidas de alrededor de 80MB/s, sin embargo, el otro Disco duro es de 5200rpm y las lecturas de escritura/lectura son de alrededor de 40MB/s. Tras la creación del RAID constato lo siguiente:

• La velocidad de escritura disminuye y es algo más rápida que el más lento.

• La velocidad de lectura es similar o un poco más rápida que el más rápido.

En otra prueba he utilizado 2 tarjetas SD de 2GB iguales, le he aplicado la opción mirror y después la opción stripe y he comparado resultados con un programa de test de discos duros (Fig. 3.104. y Fig. 3.105.).

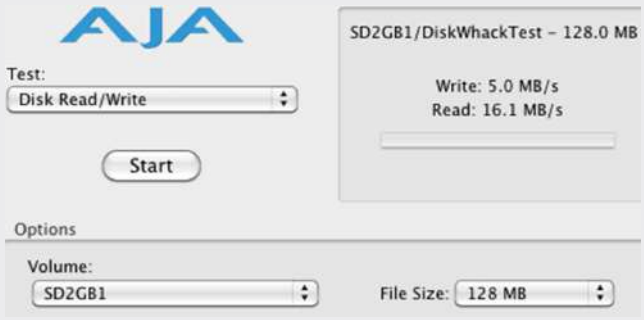


Fig. 3.104. Seleccionamos SD2GB1

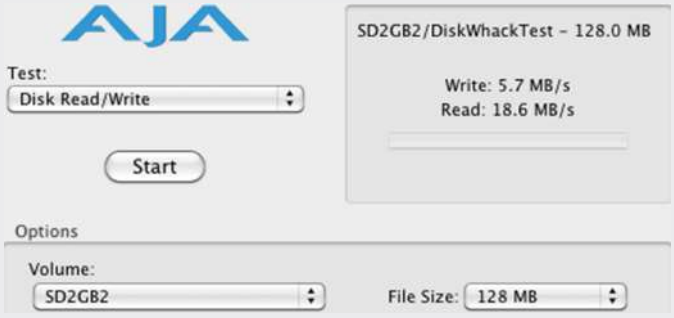


Fig. 3.105. Seleccionamos SD2GB2

Nos da una media de 5MB/s en escritura y 16MB/s en lectura.

Creo el Grupo RAID mirror (recordar que este proceso elimina los datos de los discos, como ya se ha comentado anteriormente) (Fig. 3.106.).

Fig. 3.106. Confirmamos que deseamos crear grupo RAID

Nota: A la hora de crear el Grupo RAID marcamos la opción "Reconstruir Grupos RAID mirror automáticamente" de tal manera que cuando falle uno y lo reemplazamos o se desconecte y lo volvamos a conectar, el sistema lo reconstruya con la información del existente y lo incorpore al conjunto, si no lo hacemos no pasa nada, porque con la utilidad de discos tenemos la opción también para hacerlo de forma manual.

A esta pantalla accedemos pinchando en 'opciones' (Fig. 3.107.):

Fig. 3.107. Seleccionamos "Reconstruir Grupos RAID mirror automáticamente"

Tras el proceso se crea el conjunto RAID que aparecerá con el nombre que le hemos asignados (aparece de forma independiente cada disco y después el conjunto) (Fig. 3.108.):

Fig. 3.108. Crea el conjunto RAID que aparecerá con el nombre que le hemos asignados

Se ejecuta el Test y se comprueban resultados (Fig. 3.109.):

Fig. 3.109. Ejecución del Test y se comprueban resultados

Como se aprecia la velocidad de escritura es algo más lento y la velocidad de lectura se ha incrementado.

En RAID mirror se gana en seguridad al estar los datos duplicados en ambos discos, esto lo vamos a confirmar guardando un archivo y desconectando uno de los discos a ver qué pasa:

• En esta imagen se puede ver el archivo copiado y como los discos están en línea (Fig. 3.110.)

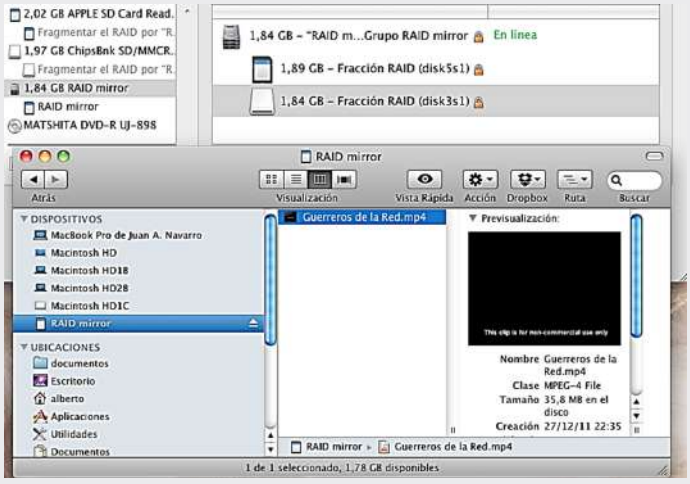


Fig. 3.110. Ver el archivo copiado y como los discos están en línea

Si retiramos de forma intempestiva uno de los discos, aún sigue apareciendo el conjunto RAID en Utilidad de disco, pero indicando un fallo.

En el explorador aparece el disco y el archivo sigue estando, en este caso contiene un vídeo, que si lo ejecutamos se visualiza correctamente (Fig. 3.111.).

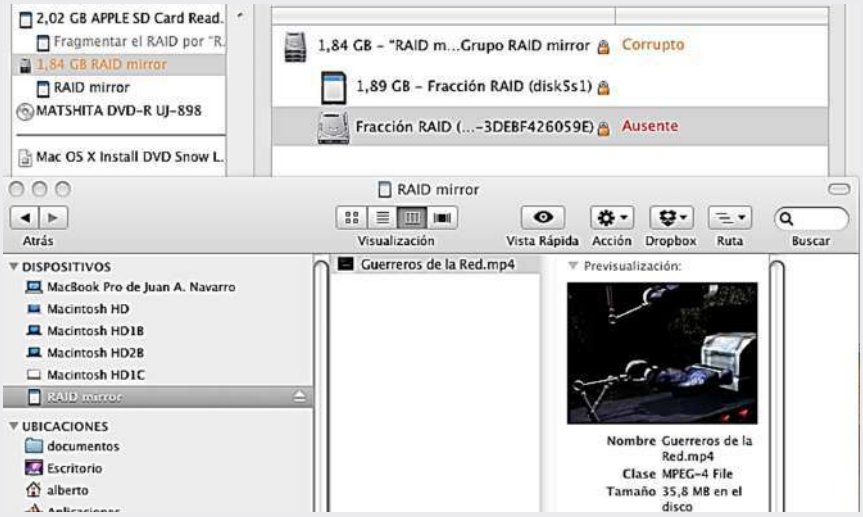


Fig. 3.111. Observamos el explorador aparece el disco y el archivo sigue estando

Si conectamos el Disco de nuevo el disco lo reconstruye automáticamente con la información del que está operativo (Fig. 3.112.).

Fig. 3.112. Reconstruye automáticamente con la información del que está operativo

Ya sea automáticamente si se ha marcado a la opción o manualmente con 'Utilidad de Discos', el proceso se realiza en segundo plano, por lo que podemos en nuestro caso seguir visualizando el vídeo contenido en la unidad.

Nota: Si eliminamos el Grupo RAID mirror, lo que pasa es que el sistema vuelve a dejarnos las dos unidades separadas como al principio, pero con los datos intactos y duplicados en los dos discos.

Como se puede ver en la siguiente imagen (Fig. 3.113.):

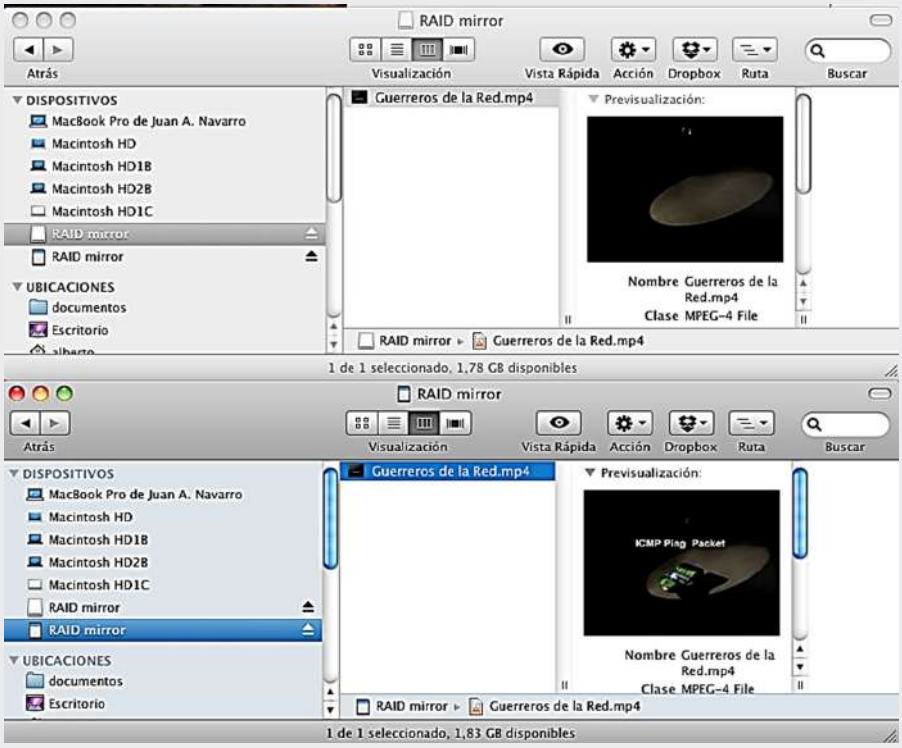


Fig. 3.113. Eliminamos el Grupo RAID mirror

Creamos el Grupo RAID stripe: Mismo procedimiento que el caso

anterior, pero con la opción stripe (llamamos al conjunto 'RAID stripe', pero le podemos llamar como queramos) (Fig. 3.114.):

Fig. 3.114. Creación del Grupo RAID stripe

Nota: en este caso no tenemos la opción 'Reconstruir Grupos RAID mirror automáticamente', que como indica su nombre solo es válida para la opción mirror.

Se ejecuta el Test y se comprueban resultados (Fig. 3.115.):

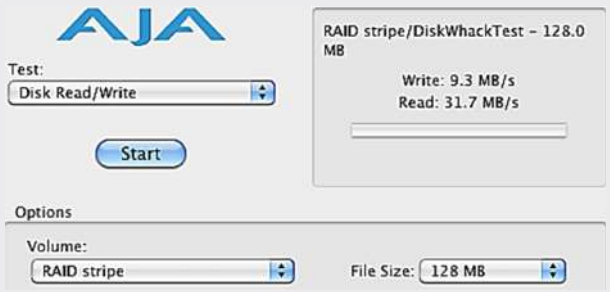


Fig. 3.115. Ejecución el Test y se comprueban resultados

Se puede apreciar como la velocidad de escritura prácticamente se duplica y la velocidad de lectura también mejora con respecto a la opción 'mirror' y por supuesto a si estuvieran como unidades normales.

Si retiramos de forma intempestiva uno de los discos, ya no aparece en el explorador de archivos (Finder en OS X) y en utilidad de Disco no avisa de la desconexión, esto es porque los datos están repartidos en ambos dispositivos y solo se puede reconstruir la información si ambos están presentes (Fig. 3.116.).

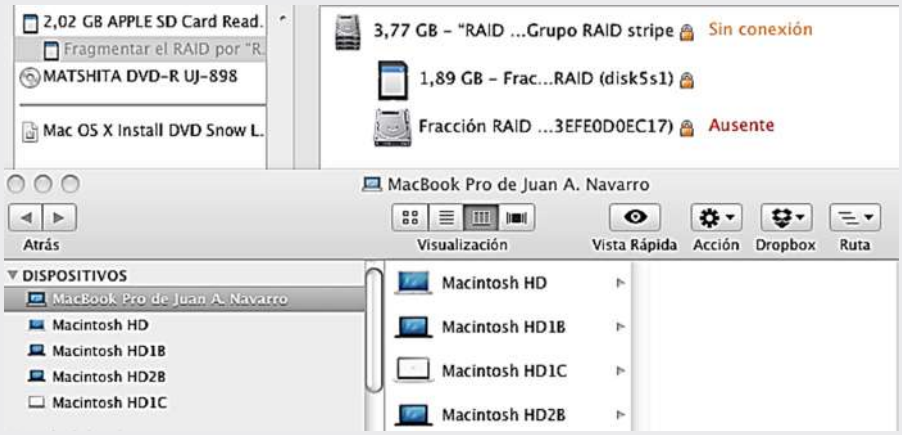


Fig. 3.116. Se aprecia como prácticamente la velocidad de escritura y lectura se duplican

En este caso lo hemos desconectado cuando no estábamos realizando ninguna acción sobre el dispositivo y al volver a conectarlo todo vuelve a la normalidad.

Nota: Si eliminamos el Grupo RAID stripe perdemos todos los datos que contengan los dispositivos que lo formen y tendremos que volver a darles formato.

En función de las necesidades utilizaremos mirror o stripe, cada uno tiene ventajas e inconvenientes que deberemos valorar.

3.3. Análisis

Antes de iniciar con esta fase se deben preparar las herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo para iniciar el análisis forense sobre las evidencias (Judicatura, 2020) obtenidas o presentadas por el administrador. Una vez que se dispone de las evidencias digitales recopiladas y almacenadas de forma adecuada, se inicia la fase más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quien o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc. En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

3.3.1. Preparación para el análisis

Antes de comenzar el análisis de las evidencias (Judicatura, 2020) se deberá:

- a. Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar.

- b. Trabajar con las imágenes que se recopiló como evidencias (Judicatura, 2020), o mejor aún con una copia de éstas, tener en cuenta que es necesario montar las imágenes tal cual estaban en el sistema comprometido.

- c. Si se dispone de recursos suficientes preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.

- d. Instalar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias (Judicatura, 2020). En esta misma estación de trabajo y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos (Medina et al., 2017) En otro equipo instalar un sistema operativo configuración exactamente igual que el equipo atacado, además mantener nuevamente la misma estructura de particiones y archivos en sus discos duros. La idea es utilizar este segundo equipo para realizar pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

Si no se dispone de estos recursos, se puede utilizar software (Adams R. , 2012) como VMware (Irrazábal et al., 2019), que permitirá crear una plataforma de trabajo con varias máquinas virtuales. También se puede utilizar una versión LIVE (Bard, 2018) de sistemas operativos como Linux, que permitirá interactuar con las imágenes montadas, pero sin modificarlas. Si se está muy seguro de las posibilidades y de lo que va a hacer, se puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis en caliente del sistema, se deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones Linux, MAC_OSx o Windows.

3.3.2. Reconstrucción de la secuencia temporal del ataque

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

a. Crear una línea temporal o timeline de sucesos, para ello se debe recopilar la siguiente información sobre los archivos:

- Marcas de tiempo MACD (Cruz Cuéllar, 2014) (fecha y hora de modificación, acceso, creación y borrado)
- Ruta completa.
- Tamaño en bytes y tipo de archivo.
- Usuarios y grupos a quien pertenece.
- Permisos de acceso.
- Si fue borrado o no.

Sin duda esta será la información que más tiempo llevará recopilar, pero será el punto de partida para el análisis, podría plantearse aquí el dedicar un poco de tiempo a preparar un script que automatizase el proceso de creación del timeline, empleando los comandos que proporciona el sistema operativo y las herramientas utilizadas.

b. Ordenar los archivos por sus fechas MAC, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los archivos nuevos, fechas MAC muy distintas a las de los archivos más antiguos.

La idea es buscar archivos y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Hay que pensar que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus 'aplicaciones' en lugares donde no se acostumbra a buscar, como por ejemplo en los directorios temporales.

Primero hay que centrarse en buscar los archivos de sistema modificados tras la instalación del sistema operativo, averiguar después la ubicación de los archivos ocultos, de qué tipo son, identificar también los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros (CASEY, 2005) borrados por los atacantes. Aquí cabe destacar la importancia de realizar imágenes de los discos, pues se puede acceder al espacio residual que hay detrás de cada archivo, (recordar que los archivos se almacenan por bloques cuyo tamaño de clúster depende del tipo de sistema de archivos (Darahuge y Arellano González, 2014) que se emplee), y leer en zonas que el sistema operativo no ve; por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar su fecha de borrado y compararla con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

c. Comenzar a examinar con más detalle los archivos logs y registros (Sánchez Cordero, Introducción al Análisis Forense Informático, 2014) que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una similitud temporal entre eventos. Pensar que los archivos log y de registro (Sánchez Cordero, Introducción al Análisis Forense Informático, 2014) son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que se tendrá que buscar

entradas extrañas y compararlas con la actividad de los archivos. Editar también el archivo de contraseñas y buscar la creación de usuarios y cuentas extrañas sobre la hora que se considere como inicio del ataque en el sistema.

d. Examinar los fragmentos del archivo /var/log/messages (LINUX), que es donde se detectan y registran los accesos FTP, esto nos permitirá descubrir si sobre esa fecha y hora se crearon varios archivos bajo el directorio /var/ftp de la máquina comprometida, además se debe tener presente que este directorio puede ser borrado por el atacante y deberá ser recuperado.

3.3.3. Determinación de cómo se realizó el ataque

Una vez obtenida la cadena de acontecimientos que se han producido, se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal vulnerabilidad.

Estos datos, al igual que en el caso anterior, se deberán obtener de forma metódica, empleando una combinación de consultas a archivos de logs, registros (Darahuge y Arellano González, 2014), claves, cuentas de usuarios, etc. El siguiente proceso permitirá conocer que acciones realizó el atacante.

a. Revisar los servicios y procesos abiertos que se recopilaron como evidencia (Judicatura, 2020) volátil, así como los puertos TCP/UDP (Barrionuevo et al., 2017) y conexiones que estaban abiertas cuando el sistema estaba aún funcionando. Examinar con más detalle aquellas circunstancias que resultan sospechosas cuando se buscó indicios sobre el

ataque, y realizar una búsqueda de vulnerabilidades a través de Internet, emplear algún buscador en la web o utilizar páginas específicas donde se encuentran perfectamente documentadas ciertas vulnerabilidades.

b. Si ya se tiene claro cuál fue la vulnerabilidad que dejó el sistema desprotegido, es necesario ir un paso más allá y buscar en Internet algún exploit (Plociennik, 2014) anterior a la fecha del incidente, que utilice esa vulnerabilidad. Generalmente se encontrará en forma de rootkit (Gibellini et al., Modalidad virtual, 4 al 8 de octubre de 2021) y un buen lugar donde comenzar la búsqueda es, nuevamente, en algún buscador en la web, aunque también será de ayuda utilizar la información presentada en la corrección de vulnerabilidades sobre reportes de este tipo.

c. Reforzar cada una de las hipótesis empleando una formulación causa efecto, también es el momento de arrancar y comenzar a utilizar la máquina preparada como 'juego de pruebas'. Probar sobre la máquina los exploits (Dominguez Perez et al., 2019) que se encontró, recordar que en el análisis forense un antecedente es que los hechos han de ser reproducibles y sus resultados verificables, por lo tanto, comprobar si la ejecución de este exploit (Dominguez Perez et al., 2019) sobre una máquina igual que la afectada, genere los mismos eventos que ha encontrado entre sus evidencias (Judicatura, 2020).

Una forma de ganar experiencia y estar listos ante cualquier eventualidad es recurrir a las bases de datos sobre ataques de los honeypots (Casanovas et al., 2017), herramientas de seguridad informática, cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los ataques, esto permite recoger información sobre los atacantes y las técnicas empleadas.

3.3.4 Identificación del atacante

Si ya se logró averiguar cómo entraron en el sistema, es hora de saber quién o quiénes lo hicieron. Para este propósito será de utilidad consultar nuevamente algunas evidencias (Judicatura, 2020) volátiles que se recopiló en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

Si se tiene pensado llevar a cabo acciones legales o investigaciones internas, se debe realizar este proceso caso contrario se debe saltar y empezar con la recuperación completa del sistema atacado y mejorar su seguridad. Pero si se decide perseguir a los atacantes, se deberá realizar algunas investigaciones como parte del proceso de identificación.

Primero intentar averiguar la dirección IP del atacante, para ello revisar con detenimiento los registros (Baryamureeba y Tushabe, 2004) de conexiones de red y los procesos y servicios que se encontraban a la escucha. También se podría encontrar esta información en fragmentos de las evidencias (Judicatura, 2020) volátiles, la memoria virtual o archivos temporales y borrados, como restos de correo electrónico, conexiones fallidas, etc.

a. Al tener una IP sospechosa, comprobarla en el registro (Baryamureeba y Tushabe, 2004) RIPE NCC (Aguilar Alvarado y Chávez Cruz, 2014) a quién pertenece. Pero por ningún motivo hay que apresurarse y sacar conclusiones prematuras, muchos atacantes falsifican la dirección IP con técnicas de spoofing (Darahuge y Arellano González, 2014). Otra técnica de ataque habitual consiste en utilizar ‘equipos zombis’, éstos son comprometidos en primera instancia por el atacante y posteriormente son utilizados para realizar el ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar

al atacante se tendrá que verificar y validar la dirección IP obtenida.

b. Utilizar técnicas hacker, pero solo de forma ética, para identificar al atacante, por si el atacante dejó en el equipo afectado una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas. Aquí entra en juego nuevamente el equipo 'juego de pruebas'.

c. Si se procede de esta forma, se puede usar una de las herramientas como NMAP (Franco, 2015), para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando y muchas más características que poseen los equipos.

3.3.5 Perfil del atacante

Otro aspecto muy importante es el perfil de los atacantes, y sin entrar en muchos detalles se podrá encontrar los siguientes tipos:

- Hackers (CASEY, 2005)
- ScriptKiddies (Darahuge y Arellano González, 2014)
- Profesionales (CASEY, 2005)

3.3.6 Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el compromi-

so de los equipos y realizar una estimación del impacto causado.

Generalmente se pueden dar dos tipos de ataques:

- Ataques pasivos y Activos.

Se deberá tener en cuenta, además otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados. Por ejemplo, ataques a los cortafuegos, el router de conexión a Internet o Intranet, tendrán diferente repercusión según el tipo de servicio que presta la empresa o institución y las relaciones de dependencia entre los usuarios

3.4. Reporting

Es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finaliza el proceso de análisis forense, esto permitirá ser más eficiente y efectivo al tiempo que se reducirá las posibilidades de error a la hora de gestionar el incidente.

3.4.1. Utilización de formularios de registro del incidente

Es importante que durante el proceso de análisis se mantenga informados a los administradores de los equipos y que tras la resolución del incidente se presenten los informes Técnico y Ejecutivo. El empleo de formularios puede ayudar bastante en este propósito. Éstos deberán ser completados por los departamentos afectados o por el administrador de los equipos. Alguno de los formularios que se deben preparar son:

Tabla 3.18. Lista de Control de Hardware en la Inspección Ocular

Id	Tipo	N° de Serie/Marca/Modelo/Capacidad/Velocidad	Estado	Observaciones
1	Monitor			
2	Teclado			
3	Mouse			
4	Gabinete			
5	Impresora			
6	Unidad de Zip			
7	Unidad de Jazz			
8	PenDrive			
9	Cámara			
10	Parlantes			
11	Discos Externos			
12	Disco Rígido			
13	Diskettes			
14	CD-ROM			
15	DVD			
16	Hub			
17	Switch			
18	Router			
19	Computadora Portátil			
20	Modem			
21	Placa de red			
22	Celular			
23	Teléfono			
24	UPS			

Tomado de: Lista de control del equipo del Perito Informático Forense:

Tabla 3.19. Lista de control del equipo del Perito Informático Forense

Elementos	OBSERVACIONES
Generales	
1. Guantes	
2. Cámara fotográfica y/o firmadora	
3. Cuaderno de notas	
4. Marcadores, lapiceros	
5. Formularios y Listas de Control para:	
a) Inspección Ocular	
b) Recolección de Evidencia	
c) Análisis de Evidencia	
d) Acta de secuestro de elementos	
e) Informe Pericial	
6. Rótulos para las evidencias autoadhesivos	
7. Bolsas plásticas antiestáticas	
8. Sobres de papel	
9. Cajas para el transporte seguro de la evidencia	
10. Rollo de cinta adhesiva	
Hardware	
1. Computadora Portátil, con lecto-grabadora de CD o DVD, placa de red, modem, dispositivo para conexiones inalámbricas, interfaces pcmla, firewire, usb.	
2. Dispositivos específicos de hardware para la copia de dispositivos de almacenamiento (tipo MASSter Solo Forensic).	
a) Disco rígido sin datos de xGB (acorde al caso).	
b) Convertidor IDE de 3.5" para notebook	
3. Impresora	
4. Cables	
a) Plano IDE de 40 pines	
b) Plano IDE de 80 pines	
c) De alimentación IDE	
d) Centronics a 68 pines SCSI	
e) 68 pines a 68 pines SCSI	
f) 68 pines a 50 pines SCSI	
g) De red, UTP directo y cruzado. Coaxial	
h) De consola (roll-over)	
i) De interconexión entre computadoras (de puerto serial y paralelo)	
5. De alimentación eléctrica	
6. Conector eléctrico múltiple	
7. Dispositivo de alimentación eléctrica ininterrumpible. Baterías	
8. Concentrador o Hub Ethernet, con conector coaxial	

9. Transceptores y convertidores	
10. Modem Externo	
11. Unidad de Zip o Jazz externa	
12. Disco rígido externo	
13. PenDrive	
14. Diskettes en blanco	
15. CD-RW o DVD en blanco	
16. Zip en blanco	
17. Conjunto de herramientas (destornilladores, medidor de tensión, medidor de cables de red)	
Software	
1. Diskette, CD-ROM, ZIP, PenDrive de arranque de:	
a) De diferentes marcas de discos rígidos	
b) De Linux, con el comando dd	
c) De DOS, con fdisk, format	
d) De Windows, Linux o MAC_OSx	
e) De Encase	
2. Cd con alguna herramienta forense	
3. Diskette o CD-ROM con la utilidad Partinfo	
4. Diskette o CD-ROM con herramientas forenses para Linux, Windows o MAC_OSx	
5. CD-ROM Sleuth Forensics de herramientas	
6. CD-ROM con herramientas forenses para sistemas operativos Microsoft Windows	
7. Disco rígido con Linux y software Encase	
8. Disco rígido con Windows y software Encase	
9. Software de diferentes placas madre	

Tomado de: Lista de control del equipo del Perito Informático Forense:

Tabla 3.20. Formulario de Registro de evidencia

Organismo	Formulario de Registro de Evidencia de la Computadora			IF-Nro:
Caso Nro.		Juzgado		Lugar y fecha
Especificaciones de la computadora				
Marca				
Modelo				
Nro. De Serie				
Garantía				
Placa Madre Marca/Modelo				
Microprocesador Marca/Modelo/Velocidad				
Memoria Ram				
Memoria Cache				
Almacenamiento Secundario, Fijo y/o Removible				
Cantidad	Tipo Disketera- CD-ROM-DVD-Disco Rígido-IDE-SCSI-USB-Zip-Jazz-Pendrive	Marca/Modelo	Velocidad/Capacidad	Nro. De Serie
Accesorios y Periféricos				
Cantidad	Tipo Placa de red, modem, cámara, tarjeta de acceso, impresora, etc	Marca/Modelo	Velocidad/Capacidad	Nro. De Serie
Observaciones:				
Perito Informático Forense			Lugar	Fecha
Firma:				
Aclaración:				

Tomado de: https://www.evidenciainformatica.com.ec/

Tabla 3.21. Formulario – Recibo de Efectos

Fecha	Organismo	Caso Nro.
Requiere Consentimiento - SI NO	Firma del responsable del consentimiento - - -	Rótulo
Descripción del elemento		
Modelo		
P/N		
S/N		
Entrega Conforme		Firma
Recibe Conforme		Firma

Tomado de: Formulario – Recibo de Efectos

Tabla 3.22. Formulario para la cadena de custodia

Cadena de Custodia de la Evidencia					
Nro.	Ubicación Actual	Fecha	Razón de traslado	Sitio a donde se traslada	Observaciones
Lugar de depósito final de la evidencia:					Fecha:

Tomado de: Manual de informática forense II (Prueba indiciaria Informática Forense)

Tabla 3.23. Lista de Control de Respuesta a incidentes

Fecha y hora:	**Nro. de Incidente:**
Lugar:	
Perito Informático Forense:	
Datos del responsable del reporte del incidente	
Nombre y Apellido:	**DNI/Legajo:**
Dirección:	**Localidad:**
Provincia:	**País:**
Área/Departamento/Oficina:	
Particular/Empresa/Organismo:	
Teléfono:	

Fax:		
Celular:		
Pager:		
Dirección de Correo Electrónico:		
Fecha y hora aproximada del incidente:		
Descripción del incidente:		
Recolección de datos del incidente		
Tipo de red		
LAN	**MAN**	**WAN**
Topología física de la red		
Estrella	**Anillo**	**Bus**
Malla	**Otra**	
Tecnología de Acceso al Medio		
Ethernet	**Token Ring**	**FDDI**
Otra		
Tipo de Cableado		
Estructurado	**Fibra Optica**	**Coaxial**
Inalámbrica	**Satelital**	**Microondas**
Servicios de la red		
Intranet	**DMZ**	**Internet**
VPN		
Tipo de Sistema operativo		
Nombre de o los equipos		
Dirección MAC del equipo		
Dirección IP del equipo		

Tabla 3.24. Lista de Control de Análisis de Discos

Lista de Control de Análisis de Discos			
Rutina	**SI**	**NO**	**OBSERVACIONES**
Actividades Preliminares			
1. Efectuar imagen del disco o medio de almacenamiento bit a bit			
2. Generar la autenticación matemática de los datos a través del algoritmo de hash			
3. Registrar la fecha y hora del sistema			
4. Generar una lista de palabras claves			
Actividades en la imagen del disco			
5. Trabajar sobre la imagen del disco, efectuar autenticación matemática en cada uno de los datos analizados a través del algoritmo de hash.			
6. En el disco analizar:			
a) Tipo del Sistema Operativo			
b) Versión del Sistema Operativo			
c) Número de particiones			
d) Tipo de particiones			
e) Esquema de la tabla de particiones			
f) Registrar nombre de archivos, fecha y hora			
i. Correlación con 3			
g) Evaluar el espacio descuidado o desperdiciado			
i. Incluido el MBR			
ii. Incluida la tabla de particiones			
iii. Incluida la partición de inicio del sistema y los archivos de comandos			
h) Evaluar el espacio no asignado			
i) Evaluar el espacio de intercambio			
j) Recuperar archivos eliminados			
k) Buscar archivos ocultos con las palabras claves en el:			
i. Espacio desperdiciado			
ii. Espacio No Asignado			
iii. Espacio de Intercambio			
iv. MBR y tabla de particiones			
l) Listar todas las aplicaciones existentes en el sistema			
i. Examinar programas ejecutables sospechosos			
m) Identificar extensiones de archivos sospechosas			

i. Examinar las extensiones de los archivos y la coherencia con las aplicaciones que los ejecutan o generan			
n) Examinar archivos en busca de datos ocultos (esteganografía) ya sean de tipo gráficos, imágenes, de texto, comprimidos o de cualquier otro tipo de extensión			
o) Examinar los archivos protegidos con claves, descifrando la clave previamente			
p) Examinar el contenido de los archivos de cada usuario en el directorio raíz y si existen, en los subdirectorios			
q) Evaluar el comportamiento del sistema operativo			
i. Integridad de los comandos			
ii. Integridad de los módulos			
r) Evaluar el funcionamiento de los programa de aplicaciones			
s) Registrar los hallazgos			
i. Capturar pantallas			
t) Generar la autenticación matemática de los datos a través del algoritmo de hash al finalizar el análisis			
i. Comparar resultados obtenidos de 2 y 6.p			
u) Conservar copias del software utilizado			

a. Informe Técnico

Este informe consiste en una explicación detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. Un ejemplo de Informe técnico, podemos ver a continuación:

Tabla 3.25. Ejemplo de Informe Técnico

INFORME PERICIAL

Base: Norma UNE 197001 (AENOR España)

Datos Informativos

1. **Asunto**

   Se deben especificar los estudios solicitados, identificación del entorno de análisis forense o en su caso, laboratorio que emite el informe y los datos identificativos de forma nominal de los peritos que han efectuado el análisis de los distintos soportes digitales, reseñando igualmente la fecha de inicio y fin de estos estudios

2. **Evidencias/muestras recibidas**

   Se deben reseñar todas las muestras objeto de análisis, las cuales se deben visualizar en un anexo fotográfico o video-gráfico que debe acompañar al cuerpo del informe en un anexo.

3. **Resolución o estudios efectuados sobre las evidencias/muestras:**

   Constituye el cuerpo del informe pericial propiamente dicho. Aquí se den incluir todos los análisis previos descritos en esta norma así como en detalle, el apartado correspondiente al análisis de los datos, reflejándose, por tanto, los siguientes subapartados:

   3.1 *Descripción del proceso de clonado bit a bit de la información original o procedimiento seguido para obtener los datos copia que han servido para el estudio de las evidencias correspondientes.*

   3.2 *Análisis de las particiones y sistemas de ficheros.*

   3.3 *Proceso de recuperación de archivos borrados, si ha lugar.*

3.4 *Estudio del sistema operativo y usuarios del mismo.*

3.5 *Estudio de la seguridad implementada.*

3.6 *Análisis detallado e individualizado, para cada soporte digital, de los indicios encontrados de interés de las distintas evidencias electrónicas. Se deben reseñar a los largo de éste análisis, en los anexos correspondientes, los indicios encontrados perfectamente clasificados, con sus rutas de ubicación en los soportes originales.*

4. **Situación final de las evidencias/muestras**

Una vez finalizados los estudios reflejados en el apartado anterior, se debe especificar el destino final que se dará a las evidencias una vez concluido su análisis, reseñando para todas ellas el medio utilizado para la puesta a disposición del organismo o entidad solicitante de esta pericial.

5. **Conclusiones**

Se debe extractar las principales conclusiones que se determinen de los estudios efectuados sobre las evidencias electrónicas. Los resultados del informe pericial deben de responder a las expectativas de quien lo solicitó, siendo claros y concisos. Para ello se debe usar un lenguaje llano sin tecnicismos ni ambigüedades.

b. Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado, pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido al personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos

Humanos (Montiel Pérez et al., 2012), Administración e incluso algunos directivos. Un ejemplo del Informe Ejecutivo, podemos observar a continuación.

Tabla 3.26. Ejemplo de Informe Ejecutivo

INFORME EJECUTIVO
Datos Informativos

- **Introducción**
  Descripción del objetivo del análisis del sistema previamente atacado y comprometido, también se incluye la información de la evidencia (Judicatura, 2020) proporcionada.

- **Análisis**
  Descripción del entorno de trabajo y de las herramientas de análisis forense seleccionadas, así como la cantidad de tiempo empleado en el mismo.

- **Sumario del incidente**
  Resumen del incidente tras el análisis de la evidencia (Judicatura, 2020) aportada.

- **Principales Conclusiones del análisis**
  Detalle de las conclusiones a las que se llegó una vez terminado el proceso de análisis.

- **Solución al incidente**
  Descripción de la solución para recuperación del incidente.

- **Recomendaciones finales**
  Pasos que se deben realizar para garantizar la seguridad de los equipos y que el incidente no vuelva a suceder.

Capítulo IV

Comprendiendo Terminología Sobre Informática Forense

CAPÍTULO IV

Comprendiendo Terminología Sobre Informática Forense

4.1 Glosario de términos

Acceso Multimedia Universal:

[https://es.wikipedia.org/wiki/Acceso_Multimedia_Universal], El Acceso Multimedia Universal (Universal Multimedia Access - UMA) es la capacidad de un sistema o aplicación de acceder a contenido multimedia desde cualquier terminal a través de cualquier red. La tecnología UMA pretende poner a disposición de los usuarios diferentes representaciones de la misma información de forma transparente, adaptándola

a diferentes terminales, redes de acceso y preferencias de usuario. La información sólo se crea una vez y el sistema UMA se encarga de personalizar el contenido deseado de la forma más rápida posible. El objetivo es satisfacer una petición de contenido de forma eficaz y con garantía de obtener la versión más adecuada en función de las condiciones de acceso

Auténtica:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Satisfacer a una corte en que los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa

Bluejacking:

[https://es.wikipedia.org/wiki/Bluejacking], En seguridad informática, el término bluejacking se refiere a una técnica consistente en enviar mensajes no solicitados entre dispositivos Bluetooth, como por ejemplo teléfonos móviles, PDAs o portátiles. La tecnología Bluetooth tiene un alcance limitado de unos 10 metros normalmente en dispositivos pequeños (como teléfonos móviles) aunque otros aparatos más grandes (como portátiles) con transmisores más potentes pueden alcanzar los 100 metros.

Bluetooth:

[https://es.wikipedia.org/wiki/Bluetooth], Es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita

la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz. Los principales objetivos que se pretenden conseguir con esta norma son: -Facilitar las comunicaciones entre equipos móviles. -Eliminar los cables y conectores entre éstos. -Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales. Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a sectores de las telecomunicaciones y la informática personal, como PDA, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras o cámaras digitales.

Cadena de custodia:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], 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:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], 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.

Entorno de análisis forense:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], 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:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Cada uno de los datos digitales recogidos en la escena de interés susceptibles de ser analizados con una metodología forense.

Exploit:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico.

Firewall:

[https://es.wikipedia.org/wiki/Firewall], Un cortafuegos (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 conFig.dos para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios

Guantes De Látex:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Sirven para preservar toda impresión dactilar, que no se haya tomado

Hackers:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Son los más populares y se trata de personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos. Sus ataques tienen motivaciones de tipo ideológico (pacifistas, ecologistas, anti globalización, anti Microsoft,

etc.) o simplemente lo consideran como un desafío intelectual.

Hardware:

[https://es.wikipedia.org/wiki/Hardware], Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.

Hash:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.)

Hijacking:

[https://es.wikipedia.org/wiki/Hijacking], Significa "secuestro" en inglés y en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo (generalmente información) por parte de un atacante. Es por tanto un concepto muy abierto y que puede aplicarse a varios ámbitos, de esta manera podemos encontramos con el secuestro de conexiones de red, sesiones de terminal, servicios, modems y un largo etcétera en cuanto a servicios informáticos se refiere.

IDS:

[https://es.wikipedia.org/wiki/IDS], Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a

una red. Estos accesos pueden ser ataques de habilidosos crackers, o de Script Kiddies que usan herramientas automáticas. El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Imagen forense:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Es el producto de realizar un clonado de cualquier evidencia electrónica en un formato de fichero, sin tener en cuenta el soporte que la contiene.

Información original:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Conjunto organizado de datos que mantiene su integridad desde el inicio hasta el final del fichero o soporte informático que los contiene.

Informe pericial:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], 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.

Live:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], 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.

MAC flooding:

[https://en.wikipedia.org/wiki/MAC_flooding] En las redes de computadoras, inundaciones MAC es una técnica utilizada para comprometer la seguridad de los conmutadores de red

MACD:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Modification date and time, Access, Creation, Deleted

Metadato:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Información que describe el contenido de un dato.

Muestra:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Parte representativa o significativa de una evidencia.

NMAP:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Mapeador de redes de código abierto, sirve para exploración de redes y auditoría de seguridad

Parches y/o actualizaciones de software:

[https://es.wikipedia.org/wiki/Parche_%28software%29], Un parche consta de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo, etc.

Periféricos:

[https://es.wikipedia.org/wiki/Perif%C3%A9ricos], Se denomina periféricos a los aparatos y/o dispositivos auxiliares e independientes conectados a la unidad central de procesamiento de una computadora. Se consideran periféricos tanto a las unidades o dispositivos a través de los cuales la computadora se comunica con el mundo exterior, como a los sistemas que almacenan o archivan la información, sirviendo de memoria auxiliar de la memoria principal.

Perito Criminalista:

[Leopoldo Alberto Galindo Soria, 'Metodología para el análisis foren-

se informático en sistemas de redes y equipos de cómputo personal', México, 2010] Dentro de sus funciones está la de intervenir para tomar por sí y verificar todas las medidas que le permitan confeccionar con exactitud y fidelidad los diversos croquis que, completándose con la fotografía, brindaran a la autoridad competente y a las partes, todo cuanto sea de utilidad para alcanzar la verdad en el proceso penal.

Perito en Dactiloscopia:

[Leopoldo Alberto Galindo Soria, 'Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal', México, 2010] Para examinar todos los objetos o lugares idóneos para captar y preservar las impresiones dactilares producidas por las crestas papilares que se localizan en los pulpejos de los dedos de las manos, con el fin de identificar científicamente a una persona. Es conveniente enfatizar que estas impresiones dactilares fueron posiblemente dejadas por el delincuente y que conducirán a establecer su identidad por medios directos

Perito Fotógrafo:

[Leopoldo Alberto Galindo Soria, 'Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal', México, 2010] Para documentar fidedignamente todo cuanto se relaciona con el lugar de los hechos y sus adyacencias, antes de que se toque o remueva nada; porque de lo contrario, difícilmente se podrán de acuerdo el personal interviniente para determinar qué lugar ocupa cada cosa removida antes de su documentación fotográfica total o en detalle.

Profesionales:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Son personas con muchísimos co-

nocimientos en lenguajes de programación, en redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo UNIX. Este tipo de criminales realizan los ataques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo, realizando un estudio minucioso de todo el proceso que llevará a cabo, recopilando toda la información posible sobre sus objetivos, se posicionará estratégicamente cerca de ellos, realizará unas pruebas con ataques en los que no modificará nada ni dejará huellas cuando lo tenga todo bien definido entonces atacará, este tipo de atacantes se encuentra muy poco y además se dedica a dar grandes golpes.

Prueba electrónica:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Es la demostración en un procedimiento judicial de los hechos que fundamentan la aplicación de requerimientos formales, procesales y/o legales.

Recursos Humanos:

[Leopoldo Alberto Galindo Soria, 'Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal', México, 2010] Toda vez que habrá ocasiones en las que se requiera la intervención de más de un especialista trabajando en el caso objeto de estudio

Recursos Materiales:

[Leopoldo Alberto Galindo Soria, 'Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal', Mé-

xico, 2010] Este punto hace referencia al Hardware que necesite el especialista forense informático, que por lo general siempre será diferente y acorde al caso bajo estudio.

Recursos Organizacionales:

[Leopoldo Alberto Galindo Soria, 'Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal', México, 2010] Este recurso cobra relevancia en intervenciones, en donde se requiera un alto nivel organizacional, por ejemplo cuando es necesario realizar varias visitas, a una determinada empresa en un horario definido, con el fin de realizar un análisis a determinados equipos, que por necesidades de la empresa no puedan salir de la misma ni ser apagados

Recursos Temporales:

[Leopoldo Alberto Galindo Soria, 'Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal', México, 2010] Recordar que el factor tiempo en cualquier intervención pericial dentro de un proceso legal es de suma importancia.

Registro:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Conjunto de datos que almacena la información y conFig.ciones de todo el hardware, software, usuarios y preferencias de un sistema de información.

RIPE NCC:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], El Centro de Coordinación de redes IP europeas (Réseaux IP Européens Network Coordination Centre (RIPE NCC)) es el Registro Regional de Internet (RIR) para Europa,

Oriente Medio y partes de Asia Central.

Rootkit:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

Routers:

[https://es.wikipedia.org/wiki/Router], Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante bridges), y que por tanto tienen prefijos de red distintos.

ScriptKiddies:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Son delincuentes informáticos muy jóvenes, que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y ver qué pasa. Su nombre viene de su corta edad y del uso de los scripts, guías de ataques que encuentran por Internet.

Sistema De Archivos:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], 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:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Organización lógica de un dispositivo.

Sniffers:

[http://www.govannom.org/index.php/seguridad/16-sniffing/395sniffers-que-son-y-como-funcionan], Como un programa que lo que hace es capturar todos los datos que pasan a través de una tarjeta de red. Para ello se basa en un defecto del protocolo Ethernet (el que se usa normalmente en las redes locales). Este protocolo lo que hace es mandar la información a todos los ordenadores de la red, aunque no vaya dirigida a ellos, luego son los propios ordenadores los que basándose en la cabecera del paquete Ethernet aceptan el paquete o no, según vaya dirigido a ellos o no. Normalmente todas las redes tienen este defecto, aunque se puede evitar

Software:

[IEEE Std, IEEE Software Engineering Standard: Glossary of Software Engineering Terminology. IEEE Computer Society Press, 1993], 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.

Spoofing:

[https://es.wikipedia.org/wiki/Spoofing] En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Switch:

[https://es.wikipedia.org/wiki/Conmutador_%28dispositivo_de_red%29], Un conmutador o switch es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

TCP/UDP:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Protocolos de transporte de datos, TCP (orientado a conexión), UDP (protocolo no orientado a conexión), los 2 pertenecen a la capa de transporte del modelo TCP/IP.

Topología de red:

[Castells, Manuel (1.997). La era de la información. Economía, socie-

dad y cultura (Vol I: La sociedad red). Alianza Editorial. Madrid. pp. 506. ISBN 84-206-4247-9], La topología de red se define como una familia de comunicación usada por los computadores que conforman una red para intercambiar datos. En otras palabras, la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente, depende del tipo de redes a que nos refiramos.

Trazabilidad:

[UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de evidencias electrónicas], Propiedad de la información de ser rastreada o reconstruida hasta su origen.

VMware:

[Andrés Collaguazo Ll., 'Metodología para la implementación de informática forense en sistemas operativos Windows y Linux', Universidad Técnica del Norte, Ecuador, 2011], Es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico con unas características de hardware determinadas.

Wi-Fi:

[https://es.wikipedia.org/wiki/Wi-Fi], Es un mecanismo de conexión de

dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: un ordenador personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (o hotspot) tiene un alcance de unos 20 metros en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso. Wi-Fi es una marca de la Wi-Fi Alliance.

Wireless Application Protocol:

o WAP (protocolo de aplicaciones inalámbricas), [https://es.wikipedia.org/wiki/Wireless_Application_Protocol], Es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, p.ej. acceso a servicios de Internet desde un teléfono móvil. Se trata de la especificación de un entorno de aplicación y de un conjunto de protocolos de comunicaciones para normalizar el modo en que los dispositivos inalámbricos, se pueden utilizar para acceder a correo electrónico, grupo de noticias y otros.

4.2 Glosario de siglas

AENOR: Asociación Española de Normalización y Certificación

AFI: Análisis Forense Informático

ASCII: American Standard Code for Information Interchange

ARP: Address Resolution Protocol

BIOS: Basic Input/Output System

BSD: Berkeley Software Distribution

C4PDF: Código de Prácticas para Análisis Forense Digital

CD: Compact Disk

CMD: Command prompt

CPU: Central Processing Unit

DLL: Dynamic-Link Library

DNS: Domain Name System

DOS: Disk Operating System

DVD: Disco Versatil Digital

ETL: Extract, Transform, Load

ESPOCH: Escuela Superior Politécnica de Chimborazo

FTP: File Transfer Protocol

GB: Gigabyte

HD: High Definition

HTML: HyperText Markup Language

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

ICMP: Internet Control Message Protocol

IDS: Sistema de Detección de Intrusos

IE: Internet Explorer

IP: Internet Protocol

IPS: Image Packaging System

LAN: Local Area Network

LEC: Ley de Enjuiciamiento Criminal

Mac OS_X: Macintosh operating system

MD5: Message-Digest Algorithm 5

MFT: Master File Table

NIC: New Internet Computer

NTFS: New Technology File System

PC: Personal Computer

RAID: Redundant array of independent disks

RAM: Random Access Memory

RRHH: Recursos Humanos

SATA: Serial Advanced Technology Attachment

SD: Secure Digital

SHA1: Secure Hash Algorithm 1

SID: Standard Instrumental Departure

SSH: Secure Shell

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

UNE: Una Norma Española

URL: Uniform Resource Locator

USB: Universal Serial Bus

VPN: Virtual private network

WAN: Wide area network

WBEM: Web-Based Enterprise Management

WIFI: Wi-Fi Alliance

WWW: World Wide Web

Referencias Bibliográficas

Adams, R. (2012). The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice.

Adams, R. (2012). The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice. PhD thesis,. Murdoch University.

Adams, R. (2012). The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensics Practice. PhD Thesis, Murdoch University, Perth, Australia.

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

Aguilar Alvarado, A., y Chávez Cruz, L. (2014). Análisis del direccionamiento IPv6 y estudio comparativo entre los protocolos de enrutamiento orientados a IPv6 . (Bachelor's thesis).

ARIMETRICS. (21 de 05 de 2023). Somos Arimetrics, Agencia Digital. https://www.arimetrics.com/glosario-digital/software

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

Bard, J. (2018). Colaboración en las ciencias de computación: Trabajemos juntos (Collaboration in Computer Science: Working Together). The Rosen Publishing Group, Inc.

Barrionuevo, M., Lopresti, M., Miranda, N., y Piccoli, F. (2017). Un modelo de detección de anomalías en una LAN usando K-NN y técnicas de computación de alto desempeño. In XXIII Congreso Argentino de Ciencias de la Computación (La Plata, 2017).

Baryamureeba, V., y Tushabe, F. (2004). Standard Guide for Forensic Digital Image Processing. In: Proceedings of the fourth digital foren-

sic research workshop (DFRWS). Baltimore, MD United States: ASTM E2825-12.

Berón, M., Gagliardi, E., y Hernández Peñalver, G. (2004). Evaluación de algoritmos de ruteo de paquetes en redes de computadoras. VI Workshop de Investigadores en Ciencias de la Computación. http://sedici.unlp.edu.ar/handle/10915/21307

Bordón, P., y Crespo, F. (2022). NLHPC: La experiencia de trabajar usando recursos de computación de alto desempeño. Observatorio Económico, 166, 14-15. https://doi.org/https://doi.org/10.11565/oe.vi166.448

Cadeño Andalia, R., Ramos Ochoa, R., y Guerrero Pupo, J. (2005). La Informática, la Computación y la Ciencia de la Información: una alianza para el desarrollo. ACIMED, 13(5). https://doi.org/1024-9435

Carrier, B., y Spafford, E. (Fall 2003). Getting Physical with the Investigative Process. International Journal of Digital Evidence, 2(2).

Casanovas, E., Tapia, C., Alasia, S., y Polanco, F. (2017). HoneyPots Web como Herramientas de Análisis de Ciberataques sobre una Red de Telefonía Móvil.

CASEY, E. (2005). Handook of Computer Investigation. Elsevier Academia Press, 8.

Cedeño Barcia, R., y Pacheco Cervantes, A. (18 de 07 de 2017). Diseño e implementacion de un sistema integral para la administracion, planificacion y registros de los modulos de computacion de la FIEC. http://www.dspace.espol.edu.ec/xmlui/handle/123456789/39673

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

Cruz Cuéllar, J. (2014). Marco metodológico para el análisis forense al

navegador web Internet Explorer. (Bachelor's thesis, Universidad Piloto de Colombia).

Darahuge, M., y Arellano González, L. (2014). Manual de informática forense II (Prueba indiciaria Informática Forense). ERREPAR S.A. https://doi.org/978-987-01-1682-0

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

Dominguez Perez, L., Gomez Trujillo, L., Cruz Cortes, N., y Rodríguez Henríquez, F. (2019). Sobre el impacto del colisionador SHA-1 en las firmas digitales. Computación y Sistemas, 23(5), 1181-1190. https://doi.org/10.13053/CyS-23-4-3103

El Mundo Educativo Del Futuro. (28 de 11 de 2015). https://elmundoecativodelfururo.blogspot.com/2015/11/34-dispositivos-de-almacenamiento.html

Escobar, D. S. (2010). Presupuesto y análisis de la rentabilidad de las Inversiones en Seguridad Informática. https://www.aacademica.org/escobards/50

factorial. (11 de 12 de 2023). factorial. https://factorialhr.es/blog/que-son-recursos-humanos-definicion/

Franco, J. (2015). Evaluación desde la óptica de la computación forense del bug openssl-heartbleed. Revista Ingeniería, Matemáticas y Ciencias de la Información, 2(4), 97-106.

Gibellini, F., Gibellini, S., Parisi, G., Zea Cárdenas, M., Ciceri, L., Bertola, F., . . . Ruhl, A. (Modalidad virtual, 4 al 8 de octubre de 2021). Monitoreo de llamadas al sistema como método de prevención de malware. In XXVII Congreso Argentino de Ciencias de la Computación (CACIC).

Guerrero Z, T., y Flores H., H. (06 de 2009). Teorías del aprendizaje y la instrucción en el diseño de materiales didácticos informáticos. https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1316-49102009000200008

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.

Hobbs, V., y Mann, G. (2013). The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice. https://doi.org/https://www.researchgate.net/publication/258224615

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

Irrazábal, V., Morales, C., Pluas, E., y Moya, J. (2019). Infraestructura centralizada para laboratorios de computación con escritorios virtuales. Ciencia Digital, 3(3.4.), 75-90.

Jaime Toruño, D., García Machado, H., y Aguilar Zapata, W. (2015). Propuestas de prácticas de laboratorios de switching, routing y servicios de red con IPv6 para la asignatura" Despliegue de IPv6" correspondiente a la electiva X de la carrera de Ingeniería en Telemática del Departamento de Computación de la UNAN-León. Doctoral dissertation.

Judicatura, P. a. (01 de 01 de 2020). Evidencia Informática. https://www.evidenciainformatica.com.ec/

López Delgado, M. (06 de 2007). Análisis Forense Digital. https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

López Luque, N. (2019). HERRAMIENTA DE APOYO A REVISIONES SISTEMÁTICAS DE LA. Santiago de Chile.

Marciszack, M., Maldonado, C., Martínez Spessot, C., Muñoz, R., Navarro, A., Peretti, J., y Roggero, L. (2009). Prometeo: una herramienta para el aprovechamiento de metadatos de base de datos relacionales. In XI Workshop de Investigadores en Ciencias de la Computación. La Plata-Argentina. http://sedici.unlp.edu.ar/handle/10915/19793

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

Medina, O. C., Marciszack, M. M., y Groppo, M. A. (2017). Traceability and validation for functional requirements of information systems using conceptual model transformation. ReCIBE, Revista electrónica de Computación, Informática, Biomédica y Electrónica, 5(1), 1-19. https://doi.org/https://doi.org/10.32870/recibe.v5i1.53

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

Montiel Pérez, J., Hernández Rubio, E., y López Bonilla, J. (2012). Computación móvil. Ingeniare. Revista chilena de ingeniería, 3(20), 282-283.

Muñoz, A. (09 de 2021). REDES CASERAS: VIRTUALIZACIÓN DE ROUTERS. https://riuma.uma.es/xmlui/bitstream/handle/10630/16539/Virtualizacio%20n.pdf?sequence=1

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

Palacios Ugalde, A. (2010). Metodología para el Análisis Forense Informático en Sistemas de redes y equipos de cómputo personal. Instituto Politécnico Nacional, México D.F.

Pérez-Teruel, K., Leyva-Vázquez, M., Espinilla, M., y Estrada-Sentí, V. (2014). Computing with words in decision making using fuzzy cognitive maps. Revista Cubana de Ciencias Informáticas, 8(2), 1-16. https://doi.org/2227-1899

Plociennik, M. (2014). Acceso uniforme a recursos de e-ciencia para la explotación de e-infraestructuras:= Exploitation of e-infrastructures providing seamless access to e-science environments. (Doctoral dissertation, Universidad de Cantabria).

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

Rodriguez Vega, A., y Traipe Castro, L. (10 de 2023). Computer vision syndrome: current evidence-based management. Revista Médica Clínica Las Condes, 34(5), 315-321. https://doi.org/https://doi.org/10.1016/j.rmclc.2023.08.001

Rodríguez, R., Vera, P., Martínez, M., y Verbel de La Cruz, L. (2014). Aprovechamiento del hardware de los dispositivos móviles para la construcción de nuevas aplicaciones. In XVI Workshop de Investigadores en Ciencias de la Computación. La Plata-Argentina. http://sedici.unlp.edu.ar/handle/10915/42655

Rueda, F. (2009). ¿ Qué es la computación en la nube. Revista Sistemas(112), 72-80.

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.

Santo Orcero, D. (2001). El modelo de concurrencia de Mosix: computación en red. Mundo Linux: Sólo programadores Linux, 36, 20-25.

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

Serna, A., Rivera, O., y Morales, J. (2012). Framework para la computación forense en Colombia. 3(2), 61-69.

Smith, D., y Petreski, S. (2008). A New Approach to Digital. https://media.defcon.org/DEF%20CON%2018/DEF%20CON%2018%20presentations/DEF%20CON%2018%20-%20Smith-SPM-Digital-Forensic-Methodlogy.pdf

Solana Aguilar, E., y Flores Aguilar, A. (2023). METODOLOGÍA PARA EL LLENADO DEL REGISTRO DE CADENA DE CUSTODIA DE LA GNCC. Gaceta Internacional de Ciencias Forenses(49), 49-66. https://doi.org/2174-9019

Triana-Fuentes, J. J., y BALLESTEROS-RICAURTE, J. A. (2016). Evidencia forense digital en equipos de cómputo, redes y computación en la nube. Ventana Informática, 34(16), 9-24. https://doi.org/https://doi.org/10.30554/ventanainform.34.1705.2016

UNE-197001. (2011). Criterios generales para la laboración de infórmes y dictámenes periciales. AENOR 2011.

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

Winter, L. B. (2017). Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015. https://doi.

org/1989-4767

Zambrano, D. M. (2017). Software para la evaluaci´on de habilidades investigativas en la. Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 1(2), 27-33.


ISBN: 978-9942-7221-5-7
9 789942 722157