ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

MODELO PARA LA TOMA DE DECISIONES MULTICRITERIO COMO SOPORTE PARA EL ANÁLISIS FORENSE EN DISPOSITIVOS DE ALMACENAMIENTO DIGITAL

AUTOR: LUIS ÁNGEL LEMA AYALA

Trabajo de Titulación modalidad proyecto de investigación y desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de Magister en Seguridad Telemática

RIOBAMBA-ECUADOR

NOVIEMBRE, 2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado "MODELO PARA LA TOMA DE DECISIONES MULTICRITERIO COMO SOPORTE PARA EL ANÁLISIS FORENSE EN DISPOSITIVOS DE ALMACENAMIENTO DIGITAL", de responsabilidad del Sr. Luis Ángel Lema Ayala ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Fredy Proaño Ortiz, Ph.D. **PRESIDENTE**	**FIRMA**
Ing. Iván Mesias Hidalgo Cajo, M.Sc. **DIRECTOR**	**FIRMA**
Ing. Cristhy Nataly Jiménez Granizo, M.Sc. **MIEMBRO**	**FIRMA**
Ing. Ruth Genoveva Barba Vera, M.Sc. **MIEMBRO**	**FIRMA**

Riobamba, noviembre 2016

DERECHOS INTELECTUALES

Yo, Luis Ángel Lema Ayala, con cédula de identidad 0603168188 declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Luis Ángel Lema Ayala
0603168188

DECLARACIÓN DE AUTENTICIDAD

Yo, Luis Ángel Lema Ayala, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, noviembre de 2016

_____

Luis Ángel Lema Ayala
0603168188

AGRADECIMIENTO

Agradezco a la Escuela Superior Politécnica de Chimborazo, Instituto de Posgrado, al Director de mi tesis Ing. Iván Hidalgo, por el apoyo brindado en la realización de este trabajo de titulación.

Luis

TABLA DE CONTENIDO

PORTADA
CERTIFICACIÓN……...i
DERECHOS INTELECTUALES……ii
DECLARACIÓN DE AUTENTICIDAD……iii
AGRADECIMIENTO……iv
TABLA DE CONTENIDO v
ÍNDICE DE FIGURAS viii
ÍNDICE DE GRÁFICOS xiv
ÍNDICE DE TABLAS xv
ABSTRACT xvii
CAPÍTULO I 1
1. INTRODUCCIÓN 1
1.1. Problema de Investigación 1
1.1.1. ***Planteamiento del Problema*** 1
1.1.2. ***Formulación del Problema*** 2
1.1.3. ***Sistematización del Problema*** 2
1.2. Justificación de la Investigación 2
1.2.1. ***Justificación teórica*** 2
1.2.2. ***Justificación metodológica*** 3
1.2.3. ***Justificación práctica*** 4
1.3. Objetivos 4
1.3.1. ***General*** 4
1.3.2. ***Específicos*** 5
1.4. Hipótesis 5
CAPITULO II 6
2. MARCO DE REFERENCIA 6
2.1. Definiciones 6
2.1.1. ***Computación Forense*** 6
2.1.2. ***Protocolo*** 6
2.1.3. ***Incidente Informático*** 6
2.1.4. ***Cadena de custodia*** 7
2.1.5. ***Evidencia Digital*** 7

2.1.6. ***Copia bit a bit*** 7
2.1.7. ***Informe Pericial*** 8
2.2. **Delitos Informáticos** 8
2.2.1. ***Definición*** 8
2.2.2. ***Características*** 8
2.2.3. ***Clasificación de Delitos Informáticos*** 9
2.2.3.1. *Falsificación Informática* 9
2.2.3.2. *Fraude Informático* 9
2.2.3.3. *Pornografía Infantil* 9
2.2.3.4. *Propiedad intelectual y derechos afines* 10
2.2.4. ***Delitos informáticos en el Ecuador*** 10
2.2.5. ***Estadísticas de Delitos Informáticos en Ecuador*** 11
2.3. **Metodología de análisis forense** 12
2.3.1. ***Preservación*** 13
2.3.2. ***Adquisición*** 13
2.3.3. ***Análisis*** 14
2.3.4. ***Presentación de resultados*** 14
2.4. **Herramientas de Análisis Forense** 15
2.4.1. ***Herramientas de Hardware*** 15
2.4.1.1. *FRED System* 15
2.4.1.2. *FRED - L* 15
2.4.1.3. *UltraKit* 16
2.4.2. ***Herramientas de Software*** 16
2.4.2.1. *Herramientas Comerciales* 16
2.4.2.2. *Herramienta Gratuitas* 17
2.5. **Trabajos Relacionados** 18
CAPÍTULO III 20
3. **DISEÑO DE INVESTIGACIÓN** 20
3.1. **Diagrama de flujo para la toma de decisiones** 20
3.1.1. ***Diagrama de flujo para cuando el computador se encuentra conectado a una red*** 20
3.1.2. ***Diagrama de flujo para cuando el computador no se encuentra conectado a una red*** 22
3.2. **Análisis de Herramientas** 23

3.2.1. ***Herramientas para captura de tráfico de red*** 24
3.2.2. ***Herramientas para adquisición de información volátil*** 24
3.2.3. ***Herramientas para adquisición de información no volátil*** 26
3.2.4. ***Herramientas para montaje y análisis de discos duros*** 27
3.2.5. ***Distribuciones Linux para seguridad informática*** 28
3.3. Protocolos de Actuación 29
3.3.1. ***Acción Número 1*** 30
3.3.2. ***Acción Número 2*** 31
3.3.3. ***Acción Número 3*** 38
3.3.4. ***Acción Número 4*** 43
3.3.5. ***Acción Número 5*** 50
3.3.6. ***Acción Número 6*** 68
3.3.7. ***Acción Número 7*** 78
3.3.8. ***Acción Número 8*** 88
3.3.9. ***Acción Número 9*** 99
3.3.10. ***Acción Número 10*** 109
3.3.11. ***Acción Número 11*** 119
3.4. Análisis de la imagen de un disco duro 127
3.4.1. ***Escenario*** 127
3.4.2. ***Proceso de análisis*** 128
3.5. Aplicación Web 144
3.6.1. ***Escenario propuesto*** 150
3.6.2. ***Población y muestra*** 150
CAPÍTULO IV 152
4. RESULTADOS Y DISCUSIÓN 152
4.1. Resultado de la prueba 152
4.2. Comprobación de la hipótesis 154
4.3. Propuesta de trabajo futuro 156
CONCLUSIONES 157
RECOMENDACIONES 158
BIBLIOGRAFÍA
ANEXOS

ÍNDICE DE FIGURAS

Figura 1-2: Estadísticas de Delitos Informáticos en Ecuador 12
Figura 2-2: Metodología Análisis Forense 13
Figura 1-3: Parte frontal Router 32
Figura 2-3: Parte trasera Router 32
Figura 3-3: Dirección IP de Router 33
Figura 4-3: Dirección IP de Router 34
Figura 5-3: Página de ingreso a Router 34
Figura 6-3: Página de inicio Router 35
Figura 7-3: Descarga archivo de configuración Router 35
Figura 8-3: Direccionamiento IP Router 36
Figura 9-3: Static Routing 36
Figura 10-3: Dynamic Routing 36
Figura 11-3: IPv6 Static Routing 37
Figura 12-3: ACL Router 37
Figura 13-3: Log Router 38
Figura 14-3: Parte trasera Switch 39
Figura 15-3: Modo Privilegiado Switch 40
Figura 16-3: startup-config Switch 41
Figura 17-3: show vlan Switch 42
Figura 18-3: Tabla cam Switch 42
Figura 19-3: Logs Switch 43
Figura 20-3: Wireshark – Ventana Principal 44
Figura 21-3: Wireshark – Elección Interfaz 45
Figura 22-3: Wireshark – Captura de tráfico 45
Figura 23-3: Wireshark – Parar captura de tráfico 46
Figura 24-3: Wireshark – Filtro por http 46
Figura 25-3: Wireshark – Filtro por IP destino 47
Figura 26-3: Wireshark – Filtro por http e IP destino 47
Figura 27-3: Wireshark – Follow TCP Stream 48
Figura 28-3: Wireshark – Follow TCP Stream- Info. Paquete 48
Figura 29-3: Wireshark 49
Figura 30-3: Hora y Fecha del Sistema – date & time 51

Figura 31-3: Usuarios Logueados - PsLoggedon 52
Figura 32-3: Usuarios Logueados net sessions 52
Figura 33-3: Archivo Abiertos - net file 53
Figura 34-3: Archivos Abiertos - psfile 53
Figura 35-3: Información Procesos - tasklist 53
Figura 36-3: Información Procesos – pslist 54
Figura 37-3: Información Procesos – Listdlls 54
Figura 38-3: Mapeo de procesos a puertos – netstat 54
Figura 39-3: Historial Comandos – doskey /history 55
Figura 40-3: Ventana Win-UFO 56
Figura 41-3: Ventana WinAudit 57
Figura 42-3: Vista General WinAudit 57
Figura 43-3: Usuarios Logueados – logonsessions.exe 58
Figura 44-3: Archivos abiertos – OpenedFilesView 58
Figura 45-3: Información Procesos – ProcessActivityView 59
Figura 46-3: Información Procesos – CurrProcess 59
Figura 47-3: Mapeo de puertos – cports 60
Figura 48-3: Ventana FTK imager 61
Figura 49-3: FTK imager - memory capture 61
Figura 50-3: FTK Imager – elección de destino 62
Figura 51-3: FTK imager – copiado de memoria 62
Figura 52-3: HashMyFile – Cálculo valor hash 63
Figura 53-3: Win-UFO 64
Figura 54-3: Hora y Fecha del Sistema – date 64
Figura 55-3: Usuarios Logueados – who 65
Figura 56-3: Usuarios Logueados – whoami 65
Figura 57-3: Archivos abiertos – lsof 65
Figura 58-3: Información Procesos – ps aux 66
Figura 59-3: Mapeo de procesos a puertos – netstat -apn 66
Figura 60-3: Historial – history 67
Figura 61-3: memoria – dd 67
Figura 62-3: memdump.mem – dd 68
Figura 63-3: fdisk - m 71
Figura 64-3: códigos hexadecimales 71

Figura 65-3: Instalación de mdadm 77
Figura 66-3: Archivo a ser copiado 79
Figura 67-3: Hashmyfile origen 80
Figura 68-3: Carpeta compartida - evidencia 80
Figura 69-3: net use 80
Figura 70-3: Uso de robocopy 81
Figura 71-3: archivo copiado - robocopy 81
Figura 72-3: Hashmyfile - destino 81
Figura 73-3: robocopy 82
Figura 74-3: remoto- fdisk –l 83
Figura 75-3: remoto – netcat y hash - investigador 84
Figura 76-3: remoto – netcat y hash - objetivo 84
Figura 77-3: remoto – cat hashdisco - investigador 85
Figura 78-3: remoto – netcat imgdisco - investigador 85
Figura 79-3: remoto – Creación imagen disco - objetivo 86
Figura 80-3: remoto – Archivos escritorio - investigador 86
Figura 81-3: remoto – Calculo hash imagen - investigador 87
Figura 82-3: remoto – Comparación valores hash - investigador 87
Figura 83-3: netcat 88
Figura 84-3: FTK imager – Ventana Principal 90
Figura 85-3: FTK imager – Create disk image 90
Figura 86-3: FTK imager – Physical Drive 91
Figura 87-3: FTK imager – Select Drive 91
Figura 88-3: FTK imager – Add 92
Figura 89-3: FTK imager – Select Image Type 92
Figura 90-3: FTK imager – Evidence Item Infomation 93
Figura 91-3: FTK imager – Image Destination 93
Figura 92-3: FTK imager – Creating Image 94
Figura 93-3: FTK imager – Verifying 94
Figura 94-3: FTK imager – Verify Results 95
Figura 95-3: FTK imager 96
Figura 96-3: fdisk –l 97
Figura 97-3: Cálculo hash – sha1sum 97
Figura 98-3: Creación imagen disco - dd 98

Figura 99-3: Cálculo hash imagen – sha1sum 98
Figura 100-3: Comparación valores hash – cat 99
Figura 101-3: fdisk – m a9 102
Figura 102-3: códigos hexadecimales a9 103
Figura 103-3: instalación de mdadm a9 109
Figura 104-3: boot- CD-ROM 112
Figura 105-3: boot- CD-ROM confirmación 113
Figura 106-3: Kali Linux modo Live CD 113
Figura 107-3: Kali Linux pantalla pricipal 114
Figura 108-3: Kali Linux - fdisk 115
Figura 109-3: Cálculo hash Kali Linux – sha1sum 115
Figura 110-3: Creación imagen disco Kali Linux - dd 116
Figura 111-3: Cálculo hash imagen Kali Linux – sha1sum 117
Figura 112-3: Comparación valores hash Kali Linux – cat 117
Figura 113-3: Kali Linux 118
Figura 114-3: boot- CD-ROM a11 121
Figura 115-3: boot- CD-ROM confirmación a11 121
Figura 116-3: Kali Linux modo Live CD a11 122
Figura 117-3: Kali Linux pantalla principal a11 122
Figura 118-3: Kali Linux – fdisk a11 123
Figura 119-3: Cálculo hash Kali Linux – sha1sum a11 124
Figura 120-3: Creación imagen disco Kali Linux - dd a11 124
Figura 121-3: Cálculo hash imagen Kali Linux – sha1sum a11 125
Figura 122-3: Comparación valores hash Kali Linux – cat a11 126
Figura 123-3: Kali Linux a11 127
Figura 124-3: Imagen forense 127
Figura 125-3: Valor hash1 de imagen forense 128
Figura 126-3: Iniciación de Autopsy 128
Figura 127-3: Página inicio Autopsy 129
Figura 128-3: Autopsy – New Case 129
Figura 129-3: Autopsy – Creating Case 130
Figura 130-3: Autopsy – Add Host 130
Figura 131-3: Autopsy – Host añadido 131
Figura 132-3: Autopsy – Add Image 131

Figura 133-3: Autopsy – Add New Image 132
Figura 134-3: Autopsy – Image file details 132
Figura 135-3: Autopsy – Resumen imagen 133
Figura 136-3: Autopsy – Selección partición 133
Figura 137-3: Autopsy – Opciones análisis 134
Figura 138-3: Autopsy – Análisis de ficheros boot 134
Figura 139-3: Autopsy – Análisis de ficheros root 134
Figura 140-3: Autopsy – Análisis de ficheros swap 135
Figura 141-3: Autopsy – Análisis de ficheros usr 135
Figura 142-3: Autopsy – S.O y versión 136
Figura 143-3: Autopsy – Direccion IP 137
Figura 144-3: Autopsy – Puerta de enlace 137
Figura 145-3: Autopsy – Log del sistema 138
Figura 146-3: Autopsy – lastlog 138
Figura 147-3: Autopsy – log messages 139
Figura 148-3: Autopsy – messages.4 139
Figura 149-3: Autopsy – messages.3 140
Figura 150-3: Autopsy – messages.2 140
Figura 151-3: Autopsy – messages 140
Figura 152-3: Autopsy – messages.1 1 141
Figura 153-3: Autopsy – messages.1 2 141
Figura 154-3: Autopsy – messages.1 3 141
Figura 155-3: Autopsy – messages.1 ftp anónimo 142
Figura 156-3: Autopsy – secure.1 142
Figura 157-3: Autopsy – wtmp 142
Figura 158-3: Autopsy – Keyword search 143
Figura 159-3: Autopsy – Enter Keyword search 143
Figura 160-3: Autopsy – Keyword search wuftpd 143
Figura 161-3: Autopsy –wuftpd configuración 144
Figura 162-3: Página principal – app web 145
Figura 163-3: Página Diagrama Red parte 1 – app web 146
Figura 164-3: Página Diagrama Red parte 2 – app web 146
Figura 165-3: Página toma de decisión– app web 147
Figura 166-3: Página acción 4– app web 147

Figura 167-3: Página acción 4 ejemplo– app web..... 148
Figura 168-3: Página acción 4 secciones– app web 149

ÍNDICE DE GRÁFICOS

Gráfico 1-3: Computador conectado a Red 21
Gráfico 2-3: Computador no conectado a Red 22
Gráfico 1-4: Porcentaje de sujetos que tomaron la decisión correcta..... 152
Gráfico 2-4: Calificación obtenida en la realización de la prueba..... 153
Gráfico 3-4: Dificultad en la realización de la tarea..... 154

ÍNDICE DE TABLAS

Tabla 1-2: Delitos Informáticos en Ecuador 10
Tabla 1-3: Herramientas de captura de tráfico 24
Tabla 2-3: Herramientas de adquisición volátil 25
Tabla 3-3: Herramientas de adquisición no volátil 26
Tabla 4-3: Herramientas para montaje y análisis de discos duros 27
Tabla 5-3: Distribuciones Linux para seguridad informática 29
Tabla 1-4: Calificación obtenida en la realización de la prueba 155

RESUMEN

En procesos legales donde se pretenden esclarecer incidentes informáticos delictivos, la evidencia digital recolectada debe ser confiable y manejarse bajo políticas basadas en estándares para que sea considerada como válida en un juicio. Actualmente no existe un modelo de análisis forense que contenga protocolos de actuación detallados con ejemplos que guíen a los forenses informáticos y que faciliten la toma de decisiones, por lo se ha propuesto un modelo basado en la normativa española UNE 71506: 2013 que pretende ser un soporte en el análisis forense de dispositivos de almacenamiento digital. Este modelo se implementó en un prototipo de aplicación web basado en HTML, CSS y desarrollado con DreamWeaver, la aplicación indica cómo realizar la adquisición y análisis de evidencia siguiendo un diagrama de toma de decisiones, tiene acciones a seguir dependiendo de los escenarios con los que se pueda encontrar el investigador forense, también se detalló un protocolo de actuación con su respectivo ejemplo que indica la forma correcta de cómo se recolecta la evidencia e indica una herramienta recomendada para esta tarea. Para comprobar la facilidad en la toma de decisiones, adquisición y análisis de información mediante la aplicación del modelo con el uso de la interfaz web, se utilizó chi cuadrado y se concluyó que en un 80% se facilitó la adquisición y análisis de información recolectada con la aplicación del modelo. Se recomienda utilizar metodologías y herramientas flexibles que se adapten al continuo cambio de la informática forense.

PALABRAS CLAVE: < TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <INFORMÁTICA>, <INFORMÁTICA FORENSE>, <TOMA DE DECISIONES>, <PROTOCOLO DE ACTUACIÓN>, <MODELO FORENSE>, <EVIDENCIA DIGITAL>.

ABSTRACT

In legal processes where informatics incidents are pretended to be clarified, the recollected digital evidence should be trustworthy and managed under policies based on standards in order to be considered as valid in a trial. Currently it does not exist a forensic analysis model containing detailed updated protocols with examples that can guide the informatics forensics to make decisions, for this reason a model base on the UNE 71506:2013 Spanish legislation has been proposed which pretends to be a support in the forensic analysis of digital storage devices. This model was implemented in a prototype web application based on HTML, CSS and developed through Dream Weaver, the application shows how to perform the acquisition and analysis of evidence following a decision-making diagram. It has actions to be performed depending on the scenarios that can be found by the forensic investigator, also an action protocol with its example was detailed to show the correct way of collecting evidence and indicates a recommended tool for this task. To probe the easiness of the decision-making, acquisition and information analysis through the application of the model with the use of the web interface, the chi square was used and it was concluded that the acquisition and analysis of collected information was eased in an 80% with the application of the model. It is recommended to use flexible methodologies and tools that can be adapted to the continuous change of forensic informatics.

KEY WORDS: < TECHNOLOGY AND ENGINEERING SCIENCES>, <INFORMATICS>, <FORENSIC INFORMATICS>, <DECISION-MAKING>, <ACTION PROTOCOL>, <FORENSIC MODEL>, <DIGITAL EVIDENCE>.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Problema de Investigación

1.1.1. Planteamiento del Problema

En la actualidad con el crecimiento de la ciberdelicuencia las empresas y gobiernos buscan estar preparados para neutralizar incidentes informáticos, ya que estos pueden poner en riesgo su infraestructura tecnológica o afectar directamente a su reputación.

Una manera de contrarrestar estos incidentes informáticos es crear un plan o modelo multicriterio como soporte para el análisis forense. Con el que se identificará la mejor alternativa para el problema de manejo de evidencias digitales, ya que el manejo incorrecto de estas evidencias haría que los resultados obtenidos no fueran admisibles (Acurio, 2009) tanto para demostrar delitos a la interna de una empresa o en un juicio legal.

Para realizar un análisis forense se deben ejecutar cuatro tareas principales: preservación, adquisición, análisis y presentación de resultados. (UNE:71506, 2013).

Actualmente se han realizado varias investigaciones previas sobre temas relacionados con análisis forense informático, entre ellas están:

- La tesis de doctorado "The advanced data acquisition model (adam): a process model for digital forensic practice" ADAM que se centra en el fase de adquisición de Información (Adams, Hobbs, & Mann, 2014).

- La investigación "Getting Physical with the Digital Investigation Process" (Carrier & Spafford, 2003). Los autores exponen que con el uso de modelos y procedimientos del mundo forense físico se añadirá credibilidad al análisis realizado en forense digital.

- La tesis “Diseño y plan de implementación de un Laboratorio de Ciencias Forenses” (Calderón, Guzmán, Margarita, & Aranda, 2012)que propone la implementación de un laboratorio forense digital en la Escuela Superior Politécnica del Litoral.

Por lo que el componente innovador de la presente investigación es que propone la creación de protocolos de actuación detallados de cada parte de las fases de adquisición y análisis de evidencia en dispositivos de almacenamiento digital. El tema planteado pretende ser una guía que les permitirá a investigadores forenses experimentados o novatos tomar decisiones y ejecutar acciones correctas en estas etapas específicas del análisis forense, dependiendo del escenario que encuentren.

1.1.2. Formulación del Problema

¿Cómo un modelo de toma decisiones multicriterio facilitará la recolección y análisis de evidencia en dispositivos de almacenamiento digital?

1.1.3. Sistematización del Problema

- ¿Qué metodologías existen para el análisis forense de dispositivos de almacenamiento digital?
- ¿Cuáles son las ventajas y desventajas de las metodologías existentes?
- ¿Qué herramientas forenses gratuitas existen para la adquisición y análisis de evidencias en dispositivos de almacenamiento digital?
- ¿Cómo ayuda al análisis forense la creación de protocolos de actuación?

1.2. Justificación de la Investigación

1.2.1. Justificación teórica

Cuando se comete un delito informático uno de los principales elementos que deben ser recolectados y analizados son los dispositivos de almacenamiento masivo digital. Es

importante que este proceso se realice siguiendo políticas definidas por la empresa o algún estándar internacional, ya que si se hace de manera incorrecta toda la evidencia recolectada y los resultados obtenidos no tendrán validez alguna al momento de ser presentados ante una corte de justicia o a la interna de la empresa.

A diferencia de las metodologías y modelos existentes que explican los pasos a seguir para realizar un análisis forense digital de manera general, se propone un modelo para la toma de decisiones que contendrá protocolos de actuación que detallan una serie de pasos a seguir, para que investigadores experimentados o novatos puedan realizar una adquisición y análisis de evidencia forense adecuado de dispositivos de almacenamiento dependiendo del escenario que encuentren.

Los protocolos de actuación además contendrán análisis de que comandos de sistema operativo o herramientas gratuitas pueden ser utilizadas en cada paso de las fases de adquisición y análisis de evidencia, independientemente de la plataforma que use el equipo comprometido.

Los beneficios que van a tener tanto investigadores expertos como novatos al seguir este modelo, es que se garantizará que la adquisición y análisis de evidencias en los dispositivos de almacenamiento digital se realizará siguiendo varios protocolos de actuación según la escena encontrada, que los resultados obtenidos serán ciento por ciento confiables ya que no habrá ningún tipo de manipulación en la evidencia original ni copia de la misma y que estos resultados servirán como evidencia para esclarecer el incidente informático investigado.

1.2.2. Justificación metodológica

Para el análisis forense existen pocas metodologías definidas entre las principales se encuentran:

- Normativa UNE 71506: 2013 que es de origen español.
- Metodología ADAM creada en Australia.
- NIST SP 800-86 que es la metodología de Norte América.

Para la creación del modelo se eligió la normativa española UNE 71506: 2013 que es la que mejor se adapta las necesidades de la investigación, ya que cuenta con una descripción exacta de todas las etapas de una investigación forense, además esta normativa se puede aplicar en cualquier organización con independencia de su tamaño o de la actividad a la que se dedique, así como también puede ser usada por cualquier persona con conocimientos en informática e investigación forense.

Uno de los objetivos principales al desarrollar este modelo, es que cualquier persona competente pueda usarlo en cualquier circunstancia y momento, sea en un ambiente laboral o privado, y que los resultados que obtenga sean los correctos.

1.2.3. Justificación práctica

El modelo propuesto será implementado en una aplicación web para que pueda ser accedido por cualquier persona que necesite saber cómo realizar la adquisición y análisis de evidencia, ya sea alguien que no conoce absolutamente nada de informática forense o alguien con experiencia.

El análisis de herramientas y el caso de estudio se realizan en un ambiente de pruebas ya que la creación de un laboratorio específico para análisis forense lleva demasiado tiempo y el costo es elevado.

El laboratorio de pruebas consta de una laptop que contendrá todas las herramientas forenses a ser analizadas y donde se realizará el análisis forense de los dispositivos de almacenamiento digital y máquinas virtuales en las cuales se realizará el proceso de adquisición de evidencia.

1.3. Objetivos

1.3.1. General

Elaborar un modelo para la toma de decisiones multicriterio como soporte en el análisis forense de dispositivos de almacenamiento digital.

1.3.2. Específicos

- Analizar las diferentes metodologías existentes para informática forense y seleccionar una como base para el estudio.
- Elaborar protocolos de actuación detallados dependiendo del escenario que se presente, para las etapas de adquisición y análisis de evidencia en dispositivos de almacenamiento digital.
- Analizar las diversas herramientas forenses gratuitas para la adquisición y análisis de evidencia en dispositivos de almacenamiento digital.
- Desarrollar una aplicación web para la implementación del modelo de toma de decisiones multicriterio.

1.4. Hipótesis

La implementación de un modelo como soporte para el análisis forense facilitará la toma de decisiones multicriterio en la recolección y análisis en dispositivos de almacenamiento digital.

CAPITULO II

2. MARCO DE REFERENCIA

2.1. Definiciones

2.1.1. Computación Forense

La metodología de computación forense es una serie de técnicas y procedimientos para la adquisición de evidencias de información desde equipos informáticos, varios dispositivos de almacenamiento y medios digitales, que puede ser presentada en una corte de justicia en un formato coherente y significativo. (Dr. H.B.Wolfe, 2003) (EC-Council:CHFI, V8)

2.1.2. Protocolo

Un protocolo puede ser un documento o una normativa que establece cómo se debe actuar en ciertos procedimientos. De este modo, recopila conductas, acciones y técnicas que se consideran adecuadas ante ciertas situaciones (http://www.definición.de/protocolo, 2008).

2.1.3. Incidente Informático

Se define como cualquier evento adverso sea este real o supuesto en relación a la seguridad de un sistema de computación o una red de computadoras. (EC-Council:CHFI, V8).

Entre los principales incidentes informáticos de seguridad se encuentran:

- Denegaciones de servicio
- Ataques web (sqlinjection, xss, etc)
- Accesos no autorizados o intentos repetidos de ingreso los servicios que requieren autenticación.

- Ingeniería social
- Virus, malware
- Evidencia de manipulación de datos

2.1.4. Cadena de custodia

La cadena de custodia "es el procedimiento de control documentado que se aplica a la evidencia física, para garantizar y demostrar la identidad, integridad, preservación, seguridad, almacenamiento, continuidad y registro de la misma." (Calderón, Guzmán, Margarita, & Aranda, 2012).

2.1.5. Evidencia Digital

Son los todos los datos digitales recogidos en la escena de interés y que son susceptibles a ser analizados con una metodología forense. (UNE:71506, 2013). Algunos ejemplos de evidencia digital son los siguientes:

- Dispositivos de almacenamiento digital
- Correos electrónicos
- Imágenes
- Logs de sistemas
- Contenido de Archivos
- Historial de navegación de Internet
- Software Ilegal
- Paquetes de Red

2.1.6. Copia bit a bit

Es una copia total de la información que va a ser analizada, este proceso de copiado se debe realizar siempre ya que los análisis nunca deben ser hechos en la evidencia original porque se puede alterar la misma y quedar invalidada como prueba judicial.

Existen varios tipos de herramientas que ayudan a esta tarea tanto gratuita como pagada.

Para comprobar que la copia realizada es igual a la original se debe sacar un hash de las dos partes para probar que son exactamente iguales una vez hecho esto se procede a los análisis respectivos en la copia.

2.1.7. Informe Pericial

“Es un 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,” (UNE:71506, 2013).

2.2. Delitos Informáticos

2.2.1. Definición

Citando al Profesor chileno Renato Leiva quien menciona en su obra “Chile, La protección penal a la Intimidad y el Delito Informático” un delito informático es “… toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma.” (Leiva Renato, 1992, p 225).

2.2.2. Características

Entre las principales características de los delitos informáticos estan:

- Son en muchas ocaciones dificiles de demostrar ya que no existen suficientes pruebas.
- Se los puede cometer desde cualquier parte del mundo sin necesidad de encontrarse físicamente en el lugar del crimen.
- Las técnicas utilizadas para comerter el delito son cada vez mas sofisticadas.
- Pueden producir grandes perdidas económicas a las victimas.
- Son denunciasdos muy pocas veces ya sea por falta de conocimiento por parte del afectado o por miedo a que su reputación se vea afectada.
- Muchas de las veces son cometidos por error y no intencionalmente.

- Son cada vez más comunes ya que muchos de los negocios y transacciones son realizados por Internet.

2.2.3. Clasificación de Delitos Informáticos

Según el convenio sobre ciberdelincuencia del consejo de Europa celebrado en Budapest el 1 de noviembre de 2001 los delitos informáticos se clasifican en:

2.2.3.1. *Falsificación Informática*

Dentro de este delito se considera la introducción, alteración y borrado ilegítimo de datos informáticos con el fin de generar datos no auténticos que sean luego utilizados como auténticos independientemente de que sean o no legibles. (Convenio sobre la Ciberdelincuencia, 2001)

Un ejemplo sería el borrado fraudulento de datos o la corrupción de ficheros.

2.2.3.2. *Fraude Informático*

Se considera fraude informático los actos deliberados que causen perjuicio patrimonial a otra persona mediante:

- La introducción, borrado o alteración de datos informáticos.
- Cualquier interferencia en el funcionamiento de un sistema informático.

Esto con el objetivo de obtener de forma ilegítima beneficios económicos para uno mismo o para un tercero. (Convenio sobre la Ciberdelincuencia, 2001).

2.2.3.3. *Pornografía Infantil*

Los siguientes actos son considerados delitos:

- Producción de pornografía infantil
- Ofertar pornografía infantil
- Difusión de pornografía infantil
- Adquisición de pornografía infantil
- Posesión de pornografía infantil

Todo lo anterior debe haberse realizado a través de un sistema informático. (Convenio sobre la Ciberdelincuencia, 2001)

2.2.3.4. Propiedad intelectual y derechos afines

Un ejemplo clásico de este delito es la piratería informática que consiste en la copia y distribución ilegal de software licenciado.

2.2.4. Delitos informáticos en el Ecuador

En el Código Orgánico Integral Penal (COIP) del Ecuador también existen penas para los delitos cometidos por medios informáticos. Entre los artículos que contemplan la penalización a estos delitos están (Ministerio de Justicia, Derechos Humanos y Cultos, 2014):

Tabla 1-2: Delitos Informáticos en Ecuador contemplados en el COIP

DELITO	ARTÍCULO EN EL COIP	PENA POR EL DELITO
Posesión de pornografía infantil	Artículo 103	Pena privativa de libertad de 13 a 16 años.
Violación a la Intimad, que se refiere a la intercepción, reproducción o difamación de información personal.	Artículo 178	Pena privativa de libertad de 1 a 3 años.
Apropiación fraudulenta por medios electrónicos.	Artículo 190	Pena privativa de libertad de 1 a 3 años.

Revelación ilegal de base de datos	Artículo 122	Pena privativa de libertad de 1 a 3 años.
Intercepción ilegal de datos	Artículo 230	Pena privativa de libertad de 3 a 5 años.
Transferencia electrónica de activo patrimonial, que se refiere a la apropiación ilegal de un activo patrimonial mediante el uso de un sistema informático.	Artículo 231	Pena privativa de libertad de 3 a 5 años.
Ataque a la integridad de sistemas informáticos.	Artículo 232	Pena privativa de libertad de 3 a 5 años.
Delitos contra la información pública.	Artículo 234	Pena privativa de libertad de 3 a 5 años.
Accesos nos consentidos a sistemas informáticos.	Artículo 234	Pena privativa de libertad de 3 a 5 años.

Fuente: Ministerio de Justicia, Derechos Humanos y Cultos, 2014
Realizado por: Luis Lema, 2016

2.2.5. Estadísticas de Delitos Informáticos en Ecuador

El siguiente gráfico muestra la cantidad anual de delitos informáticos denunciados desde el año 2009 hasta el mes de junio de 2014 (Fiscalía General del Estado, 2015). Se puede ver que hay una cantidad importante de delitos denunciados, pero hay muchos otros que no se denuncian ya sea por falta de conocimiento del proceso de denuncia o por temor a perder reputación en caso de una empresa.

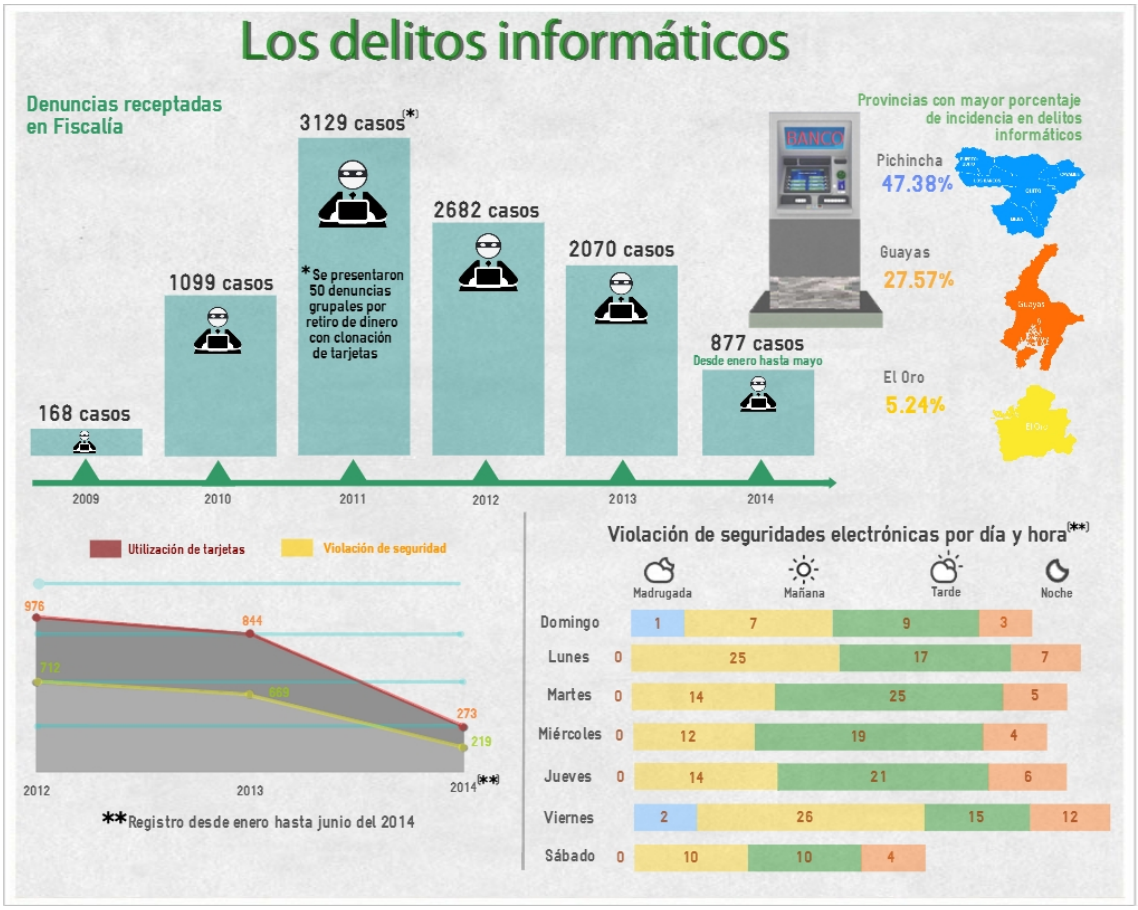


Figura 1-2: Estadísticas de Delitos Informáticos en Ecuador

Fuente: www.fiscalia.gob.ec

2.3. Metodología de análisis forense

La metodología más usada en el mundo de habla hispana es la normativa UNE 71506 que puede ser usada en cualquier organización independiente de su actividad o tamaño.

Esta normativa ha sido elaborada para ayudar en el proceso de análisis forense informático de evidencias electrónicas complementando todos aquellos otros procesos que conforman dicho sistema de gestión de las evidencias electrónicas. (UNE:71506, 2013)

La normativa UNE 71506 consta de cuatro fases principales: Preservación, Adquisición, Análisis y Presentación de Resultados. En la figura 2.2 se presentan las fases de la metodología.

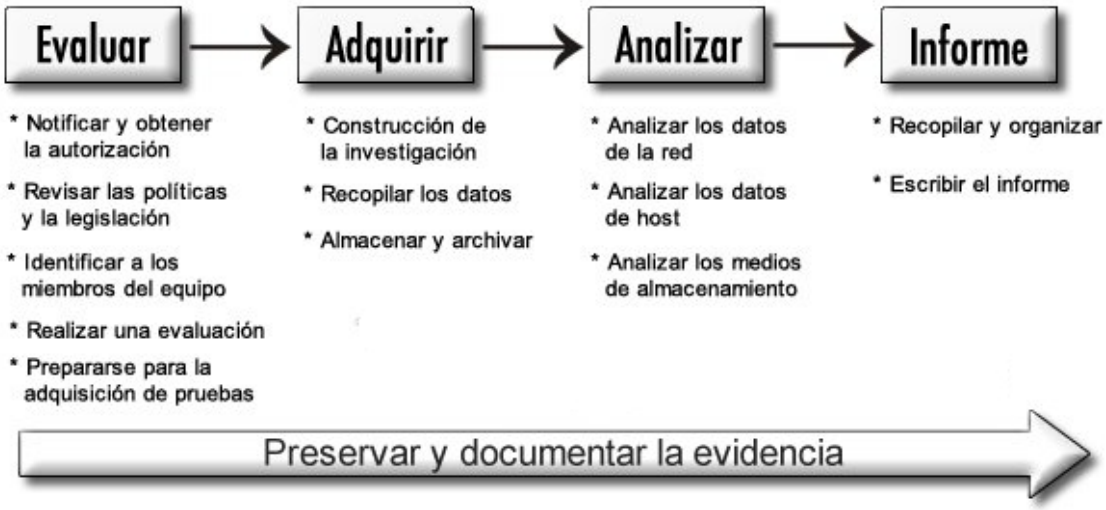


Figura 2-2: Metodología Análisis Forense

Fuente: www.drangonjar.org

2.3.1. Preservación

Cuando se realiza un análisis forense se deben preservar las evidencias originales para que estás no pierdan su validez y confiabilidad. Las principales tareas que se deben realizar en esta fase son:

- Colocar cinta y sellar las evidencias en soportes adecuados.
- Se deben almacenar las evidencias en un lugar seguro hasta el final de la investigación. (UNE:71506, 2013)

2.3.2. Adquisición

Para el proceso de recolección de evidencia se deben tener en cuenta varios aspectos entre los principales están:

- Para preservar la integridad física de la evidencia todas las piezas deben ser manejadas cautelosamente.
- Los elementos identificados deben ser claramente etiquetados. (EC-Council:CHFI, V8)

Dependiendo del escenario con el que se encuentre el investigador se deberán tomar diferentes acciones ya que no es lo mismo recolectar evidencia de un computador que se encuentra encendido o apagado, también se debe tener en cuenta si se encuentra conectado a una red o internet.

Independiente del escenario con el que el investigador se encuentre se deben realizar las siguientes acciones:

- Fotografiar y guardar en video la escena.
- Realizar copias bit a bit de la evidencia encontrada.
- Prestar atención a la hora y fecha del sistema ya que puede no estar sincronizada.
- Documentar todas las acciones tomadas. (EC-Council:CHFI, V8) (Calderón, Guzmán, Margarita, & Aranda, 2012)

2.3.3. Análisis

El proceso de análisis tiene como objetivo responder a las siguientes preguntas:

- ¿Qué?: Determinar la naturaleza de los incidentes.
- ¿Cuándo?: Reconstruir el tiempo de intrusión, la secuencia temporal.
- ¿Cómo?: Identificar que herramientas y técnicas fueron utilizadas para cometer el delito, y cualquier otra actividad realizada.
- ¿Quién?: Reunir información sobre todos los posibles involucrados. (Calderón, Guzmán, Margarita, & Aranda, 2012).

2.3.4. Presentación de resultados

Consiste en la presentación de los informes finales con todas las evidencias encontradas. Estos informes deben ser presentados en forma clara y sin utilizar lenguaje técnico ya que deben pueden ser presentados en corte.

2.4. Herramientas de Análisis Forense

Es necesario contar con herramientas especializadas tanto para la adquisición como el análisis de evidencia digital dentro de la escena donde se ha cometido un delito informático. Por esta razón existen varias herramientas creadas para este fin y según su tipo se clasifican en: Herramientas de Hardware y Herramientas de Software.

2.4.1. Herramientas de Hardware

A continuación, se presenta un listado de algunas de estas herramientas junto con una breve descripción.

2.4.1.1. *FRED System*

FRED significa Forensic Recovery of Evidence Device, es un sistema de laboratorio no portátil optimizado para la adquisición y análisis de evidencia. Su utilización es muy sencilla ya que solo basta con sacar los dispositivos de almacenamiento comprometidos, insertarlos en FRED y sacar la imagen bit a bit.

Este sistema soporta muchos de los diferentes tipos de dispositivos de almacenamientos como son discos duros (IDE/EIDE/ ATAISATAIATAPIISCSI IISCSIll ISCSIlll), DVD, CD, Tarjetas de memoria externa de varios tipos.

Este sistema tiene una gran capacidad de almacenamiento y procesamiento por lo que su costo puede llegar a ser muy elevado. (Hazan, Mahmood, & Raghav, 2012)

2.4.1.2. *FRED - L*

Es un sistema FRED en una Laptop y además viene incluido un UltraKit por lo que es ideal para realizar tareas forenses en sitio, que se refiere a ejecutar adquisición o análisis de evidencia en la escena del crimen.

Al igual que el sistema FRED es una máquina con altas prestaciones en almacenamiento y procesamiento, además tiene tarjeta de red Wireless y soporta varias velocidades de conexión Ethernet. (Hazan, Mahmood, & Raghav, 2012)

2.4.1.3. UltraKit

Es un kit portable que contiene una gran variedad de herramientas de hardware entre las que se encuentran:

- Bloqueadores de escritura
- Cables de diferentes tipos
- Adaptadores
- Baterías de energía

Todas estas herramientas son necesarias para la adquisición de evidencia en el campo, crear por ejemplo copias bit a bit en el lugar donde sucedió el delito informático. UltraKit trabaja conjuntamente con FRED – L por lo que el trabajo del investigador forense en la escena del crimen se ve facilitado en gran manera. (Hazan, Mahmood, & Raghav, 2012)

2.4.2. Herramientas de Software

Las herramientas de software se especializan dependiendo de la investigación que se vaya a realizar, aunque también hay varias que son de utilidad para varias etapas de la investigación forense. A estas herramientas se las puede clasificar en comerciales y gratuitas.

2.4.2.1 Herramientas Comerciales

Algunas de las herramientas comerciales que se pueden utilizar están:

- Encase Forensic: Es la suite para investigación forense más conocida a nivel mundial. Es muy completa ya que se puede utilizar en todas las fases de una investigación forense.
- OxygenForensic: Herramienta especializada para dispositivos móviles.
- SafeBack: Es usada principalmente para obtener imágenes de discos duros y restaurarlas en otro disco duro.
- VogonForensic: Es un producto que ofrece software para la creación de imágenes y análisis de evidencia.

2.4.2.2. *Herramienta Gratuitas*

En lo que se refiere a Herramientas Gratuitas existen algunas distribuciones sobre todo basadas en Linux, que incluyen mucho del software más utilizado para investigación forense. Las distribuciones incluyen software gratuito o versiones de prueba para todas las etapas de la metodología de análisis forense.

Entre las distribuciones más populares están:

- CAINE (Computer Aided INvestigative Environment): Es una distribución que viene en Live DVD y contiene numerosas herramientas y scripts para realizar una investigación forense completa.
  Entre las principales características de CAINE es que tiene una interfaz gráfica muy amigable y el proceso de generación de informes es semiautomático.
- DEFT Linux: Es una distribución de Linux para análisis forense informático basada en Ubuntu que incluye herramientas para el análisis forense de móviles y/o dispositivos con iOS o Android.
- Santoku: Es una distribución orientada a la seguridad móvil, incluye varias herramientas open source que ayudarán al investigador en análisis de malware y test de seguridad en general.
- Kali Linux: Es una distribución basada en Debian que tiene como objetivo facilitar el Test de Penetración y Auditorias de Seguridad. Contiene muchas herramientas destinas para la realización de un Test de Penetración pero también tiene una sección entera dedicada al análisis forense.

De igual manera se pueden utilizar herramientas de software de manera individual para una tarea específica y no necesariamente usar una distribución completa, incluso existe software que sirve para realizar más de una tarea.

A continuación se lista algunas de las herramientas gratuitas más conocidas para investigación forense, varias de estas herramientas vienen en versiones para Windows (Sanchez, 2013), y Linux:

- Autopsy: Es un framework muy completo que cumple sirve principalmente para la fase de análisis de evidencias.
- ExifTool: Sirve para analizar metadatos de varios formatos de archivos.
- FTK Imager: Su función principal es permitir montar imágenes obtenidas de discos duros, también se puede obtener un adquirir una copia de la memoria que se encuentra corriendo en ese momento.
- Volatility: Analiza la memoria adquirida, también tiene plugins para realizar análisis de malware.
- Recuva: Es una utilidad que ayuda en la recuperación de archivos borrados.
- RegRipper: Es una aplicación que sirve para analizar el registro de Windows.
- Wireshark: Es una herramienta para la captura y análisis de paquetes en una red.
- OphCrack: Sirve para la recuperación de contraseñas.

2.5. Trabajos Relacionados

A continuación, se resumen los trabajos realizados previamente sobre temas relacionados con análisis forense informático, entre ellos están:

- La tesis de doctorado "The advanced data acquisition model (adam): a process model for digital forensic practice" (Adams, Hobbs, & Mann, 2014) presenta un modelo genérico para la actividad de adquisición de evidencia digital, identificando los procesos clave de alto nivel dejando la implementación de políticas detalladas y procesos de bajo nivel a los expertos en forense digital. Como ventaja de ADAM es que hace uso de diagramas UML para la

descripción de procesos dentro de la etapa de adquisición, los autores indican que los diagramas permiten estandarizar y entender mejor estos procesos. Además, el modelo pone bastante énfasis en la parte de documentación de todas las etapas del análisis forense digital.

- La investigación "Getting Physical with the Digital Investigation Process" (Carrier & Spafford, 2003) define un modelo para la investigación forense usando la teoría y técnicas del mundo investigación forense física, considera al computador como la escena del crimen en sí y no solo como una evidencia física más.

  Este modelo identifica los requerimientos técnicos por cada fase que deben ser desarrollados y la interacción entre la investigación física y digital. Los autores exponen que con el uso de modelos y procedimientos del mundo forense físico añadirá credibilidad al análisis realizado en el mundo de análisis forense digital.

- A nivel nacional existe un trabajo realizado por estudiantes de la ESPOL titulado "Diseño y plan de implementación de un Laboratorio de Ciencias Forenses" (Calderón, Guzmán, Margarita, & Aranda, 2012) que propone la implementación de un laboratorio forense digital en la Universidad, además hace un resumen de la metodología usada para un análisis forense.

CAPÍTULO III

3. DISEÑO DE INVESTIGACIÓN

3.1. Diagrama de flujo para la toma de decisiones

El siguiente diagrama muestra diferentes caminos y acciones que pueden tomar los investigadores dependiendo el escenario que encuentren, al momento de realizar la adquisición de información a dispositivos de almacenamiento digital.

El diagrama contempla situaciones como, por ejemplo: si el computador se encuentra o no conectado a una red, si está conectado a algún dispositivo de red como un switch o un router, si está encendido o apagado, si el tipo de disco duro es IDE/SATA o RAID, etc.

El diagrama de flujo se encuentra divido en 2 partes: para cuando el computador se encuentra conectado a una red y para cuando no lo está, esto para facilitar el proceso de toma de decisiones. A continuación, se muestran los dos diagramas de flujo mencionados.

3.1.1. Diagrama de flujo para cuando el computador se encuentra conectado a una red

En este primer diagrama de flujo se pueden observar las decisiones y acciones que se pudieran tomar, cuando el computador en el cuál se va a realizar la investigación forense se encuentra conectado a una red.

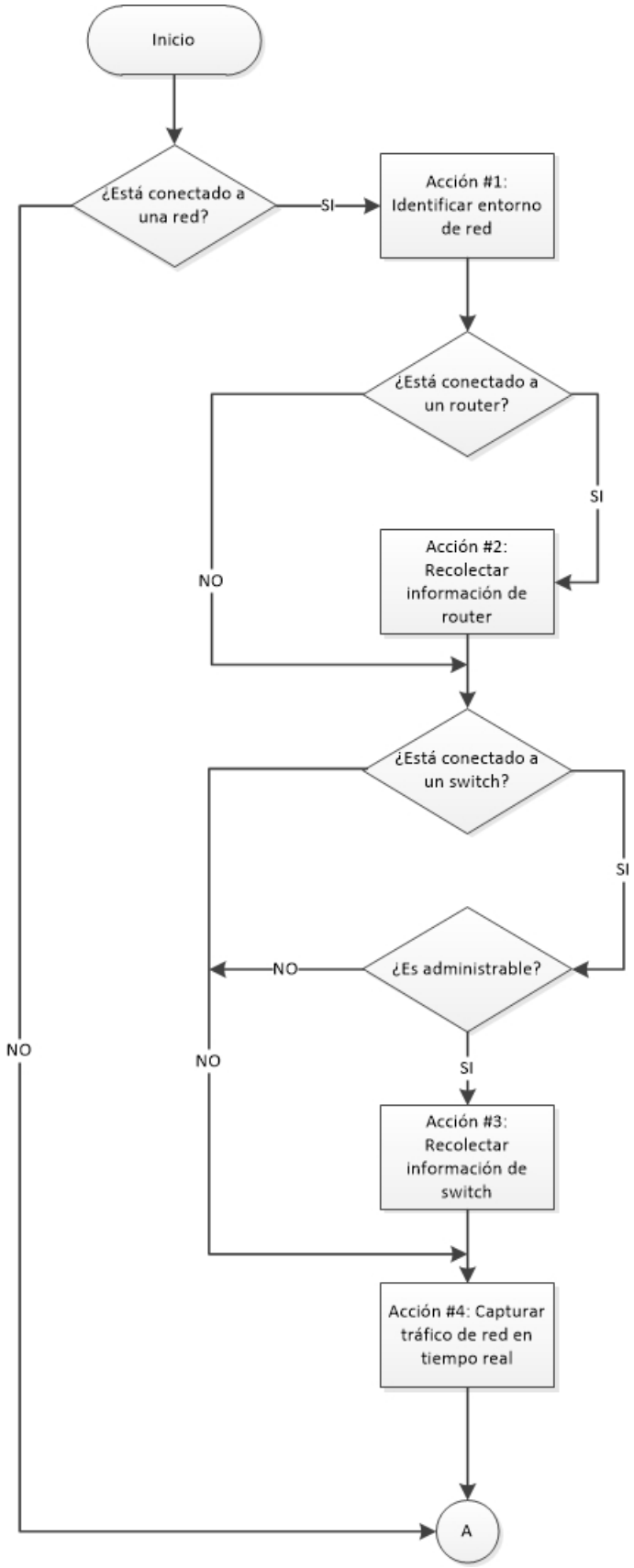


Gráfico 1-3: Computador conectado a Red

Realizado por: Luis Lema, 2016

3.1.2. Diagrama de flujo para cuando el computador no se encuentra conectado a una red

El siguiente diagrama de flujo muestra las decisiones y acciones que se pueden tomar cuando el computador no se encuentra conectado a una red:

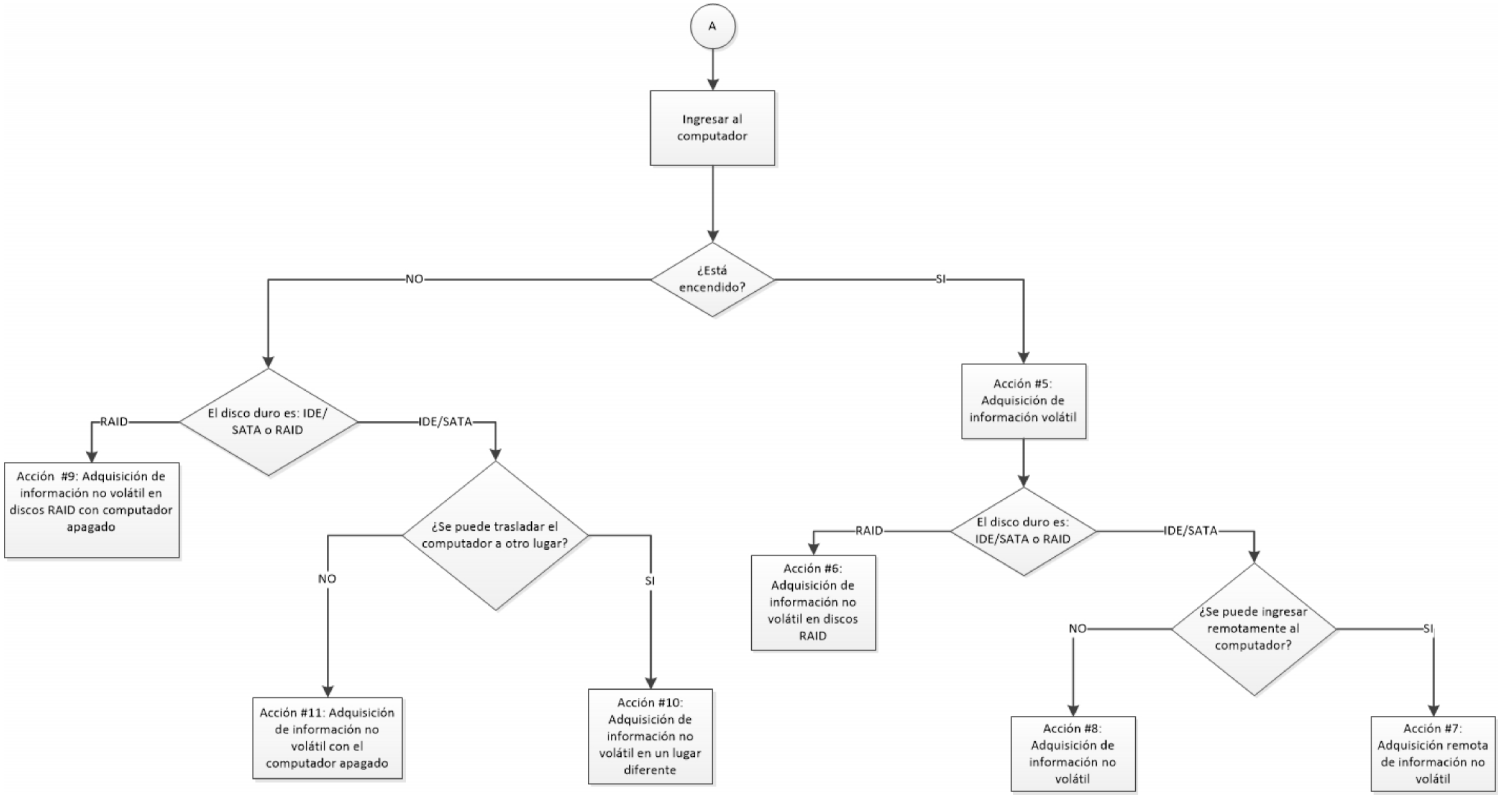


Gráfico 2-3: Computador no conectado a Red

Realizado por: Luis Lema, 2016

3.2. Análisis de Herramientas

Para este análisis se revisaron varias de las herramientas de software forense gratuitas disponibles tanto para sistemas operativos Linux como Windows. Pero ya que existen un gran número de estas herramientas y en la actualidad siguen apareciendo nuevas, para el análisis se eligieron dos o tres herramientas de las más conocidas en el ámbito forense, y se las dividió dependiendo de la función que cumplen.

Entre los parámetros e indicadores que se tomaron en cuenta al momento de realizar el análisis están:

- Idioma en que se encuentra disponible la herramienta.
    - Inglés
    - Español
    - Varios

- Sistemas operativos en los que funciona.
    - Multiplataforma
    - Windows
    - Linux

- Dificultad de uso.
    - Baja
    - Media
    - Alta

- Y otros indicadores dependiendo de la función que cumple.

A continuación, se muestran las matrices donde se comparan las diferentes herramientas analizadas y se indica cuál es la recomendada.

3.2.1. Herramientas para captura de tráfico de red

Para el proceso de capturar tráfico de red en tiempo real se eligieron las siguientes herramientas:

- Wireshark
- Capsa Free
- Tcpdump

Tabla 1-3: Herramientas de captura de tráfico

Software	Idioma	Sistemas Operativos	Dificultad de uso	Filtrado de paquetes	Multiformato	Interfaz
Wireshark	Inglés	Multiplataforma	Media	Si	Si	Gráfica
Capsa Free Network Analyzer	Inglés	Windows	Media	Si	No	Gráfica
Tcpdump	Inglés	Linux	Alta	SI	No	Línea de comandos

Realizado por: Luis Lema, 2016

Como conclusión se puede decir que Wireshark es la mejor herramienta para realizar capturas de tráfico en red, ya que entre varias de las ventajas que tiene sobre las otras opciones de software además de las observadas en la tabla están: la gran cantidad de información detallada que muestra de cada protocolo, la facilidad para personalizar los resultados mostrados y sobre todo que permite leer y crear archivos de captura en varios formatos, por lo que se puede importar y exportar capturas desde y hacia otras herramientas.

3.2.2. Herramientas para adquisición de información volátil

Para la adquisición de información no volátil se analizaron solo herramientas para la plataforma Windows, ya que para realizar este proceso en sistemas operativos Linux, solamente se deberían usar binarios compilados por el mismo investigador de los comandos necesarios para adquirir la información necesaria.

Para esta tarea se van a analizar solamente dos herramientas y una utilidad, ya que no se puede encontrar software gratuito que recoja toda la información volátil necesaria.

Además, se debe tener en cuenta que el software aquí mostrado no es más que una recopilación de utilidades individuales que cumplen diferentes funciones. Estas dos herramientas muestran una interfaz gráfica que facilita la el proceso de adquisición de información.

Las herramientas y la utilidad analizadas son:

- Win – UFO (Ultimate Forensics Outflow)
- LFT (Live Forensic Toolkit)
- Command Prompt Portable

Tabla 2-3: Herramientas de adquisición volátil

Software	Idioma	Sistemas Operativos	Dificultad de uso	Cantidad de información adquirida	Funcionamiento de las utilidades	Interfaz
Win – UFO	Inglés	Windows	Baja	Media	Todas	Gráfica
LFT	Inglés	Windows	Baja	Baja	Algunas fallan	Gráfica
Command Prompt	Inglés	Windows	Media	Total	No aplica	Línea de comandos

Realizado por: Luis Lema, 2016

En este caso la mejor herramienta que se puede utilizar para adquirir información volátil es Win – UFO, ya que se con ella se puede recolectar variada cantidad y tipo de información, entre ella ciertas partes de la volátil como: hora y fecha de sistema, información de procesos, puertos abiertos, etc. Una gran ventaja de Win – UFO es que al ser portable no realiza cambios al registro del sistema operativo (Gupta & Mehtre, 2013), lo que asegura que no se alterando la integridad del mismo.

Se escogió a Win – UFO sobre el Command Prompt Portable porque la principal desventaja de este último, es que se necesita que el investigador posea a más del programa en sí, los ejecutables de los binarios necesarios. Aunque gran cantidad de

binarios están disponibles en la página oficial de Microsoft siguen siendo independientes de la utilidad principal.

3.2.3. Herramientas para adquisición de información no volátil

La adquisición de información no volátil se refiere principalmente al clonado forense de discos duros, por lo que para este análisis se tomaron como referencia herramientas que permiten esta tarea.

Cuando se hace el clonado de discos duros con el computador prendido

Las herramientas que se analizaron son:

- FTK Imager
- OSFClone
- GuyMager

Tabla 3-3: Herramientas de adquisición no volátil

Software	Idioma	Sistemas Operativos	Dificultad de uso	Calcula valor Hash	Versión portable para Windows	Interfaz
FTK Imager	Inglés	Multiplataforma	Baja	Si	Si	Gráfica
OSFClone	Inglés	Multiplataforma	Media	Si	No	Línea de comandos
GuyMager	Inglés	Multiplataforma	Baja	Si	No	Gráfica

Realizado por: Luis Lema, 2016

Como conclusión se puede decir que cuando se vaya a realizar la adquisición de información no volátil con el computador apagado, las tres herramientas son muy buenas y de gran utilidad, ya que las tres realizan copiados bit a bit y calculan los valores hash para comprobar que haya integridad en la imagen obtenida.

La diferencia que tiene FTK imager es que posee una versión portable para el sistema operativo Windows, por lo que el clonado forense del disco duro, cualquier unidad de almacenamiento externa e incluso archivos y carpetas individuales se puede realizar

mientras el computador está encendido, esto ahorra mucho tiempo al investigador. Las otras dos herramientas están desarrolladas especialmente para Linux, aunque de igual manera se puede crear imágenes de cualquier disco duro, la principal desventaja es que se debe apagar el computador y bootear el software desde una unidad externa.

3.2.4. Herramientas para montaje y análisis de discos duros

Para el proceso de montado de imágenes de discos duros existen algunas herramientas gratuitas, pero que además de eso permitan realizar el análisis forense de las mismas hay muy pocas. Por esta razón para este punto se analizaron las dos herramientas más conocidas que son:

- FTK Imager en su versión Lite gratuita
- Autopsy

Tabla 4-3: Herramientas para montaje y análisis de discos duros

Software	Idioma	Sistemas Operativos	Dificultad de uso	Proporciona valores Hash	Documentación Disponible	Personalizable
FTK Imager	Inglés	Multiplataforma	Media	Si	Baja	No
Autopsy	Inglés	Multiplataforma	Media	Si	Alta	Si

Realizado por: Luis Lema, 2016

FTK imager Lite y Autopsy son dos muy buenas herramientas para el montaje y análisis de imágenes de discos duros, pero la desventaja de FTK imager Lite es que en su versión gratuita no cuenta con varias opciones que tiene en su versión pagada. En cambio Autopsy incluso al ser gratuita cuenta con un gran número de opciones para el análisis como son: búsqueda por palabra clave, soporte a imágenes de discos duros de varios formatos, soporte a múltiple sistema de archivos, detección de tipo de archivos, miniaturas de imágenes y videos, etc.

Otro punto importante es que la documentación y soporte para Autopsy es muy amplia ya que al ser gratuita y libre, son los mismos usuarios los que se encargan de crear tutoriales, manuales y soporte en general. Para tener el mismo servicio de documentación y soporte para FTK imager se debe adquirir la versión pagada.

3.2.5. Distribuciones Linux para seguridad informática

En la actualidad existen varias distribuciones Linux que están especialidades en la seguridad informática, auditoría de sistemas y análisis forense. Para elegir a las mejores hay que tener en cuenta factores como por ejemplo que los repositorios siempre estén actualizados y la cantidad de herramientas disponibles.

Para este análisis se van a tomar en cuenta los siguientes parámetros:

- Dificultad de uso
    - Baja
    - Media
    - Alta

- Soporte de la comunidad
    - Bajo
    - Medio
    - Alto

- Cantidad de herramientas preinstaladas
    - Baja
    - Media
    - Alta

- Frecuencia de actualizaciones
    - Baja
    - Media
    - Alta

- Programa de recompensa por encontrar bugs
    - Si
    - No

Se eligieron tres de las distribuciones más conocidas y utilizadas en la seguridad informática:

- Kali Linux
- Caine
- BackBox

Tabla 5-3: Distribuciones Linux para seguridad informática

Distribución	Dificultad de uso	Soporte de la comunidad	Cantidad herramientas preinstaladas	Frecuencia de actualizaciones	Programa de recompensa
Kali Linux	Media	Alto	Alta	Alta	Si
Caine	Media	Medio	Media	Alta	No
BackBox	Media	Medio	Media	Alta	No

Realizado por: Luis Lema, 2016

La gran diferencia entre en Kali Linux y las demás distribuciones, es la gran cantidad de herramientas preinstaladas que este tiene (más de 300), además del programa de recompensa por encontrar errores, este programa asegura a los usuarios que los desarrolladores siempre están corrigiendo bugs dentro de la distribución.

Por estas y más razones Kali Linux es de las distribuciones Linux para seguridad informática más utilizada a nivel mundial, ya sea por investigadores independientes o grandes empresarios.

3.3. Protocolos de Actuación

Los protocolos de actuación son una serie de pasos que el investigador forense debe seguir, para lograr adquirir y/o analizar de manera adecuada la información contenida en una unidad de almacenamiento digital.

El protocolo de actuación y los ejemplos están contenidos dentro de “Acciones”, que llevan por nombre el proceso que se debe realizar dependiendo del escenario y la decisión que tome el investigador forense, como se puede observar en los diagramas de flujo del punto anterior.

Estos protocolos de actuación en su mayoría y cuando es posible contienen: los pasos a seguir para la adquisición y análisis de información, listado de herramientas de software gratuitos necesarios para llevar a cabo la acción, una herramienta o comando recomendado y un ejemplo ya sea con el uso de comandos de sistema y/o herramientas de software, tanto para plataformas Linux como Windows.

3.3.1. Acción Número 1

NOMBRE: Identificar entorno de red

PROTOCOLO DE ACTUACIÓN:

1.- Determinar la topología o estructura de la red.

2.- Listar recursos de red que puedan contener evidencia, como por ejemplo:

- Routers
- Switches
- Firewalls
- IPS/IDS
- Web Proxie
- Servidores de Logs
- Medios inalámbricos
- Cables Físicos
- VPNs
- Sniffers
- Servidores, Pcs

3.- Describir las características de los recursos identificados:

- En caso de ser Hardware:
    - Marca

    - Modelo
    - Serie

- En caso de ser Software:
    - Marca
    - Modelo
    - Breve descripción de lo que hace

4.- Documentar todos los hallazgos.

3.3.2. Acción Número 2

NOMBRE: Recolectar información de router

PROTOCOLO DE ACTUACIÓN:

1.- Describir características físicas:

- Marca
- Modelo
- Serie
- Número de Puertos
- Tipos de Puertos

2.- Describir características de configuraciones:

- Configuraciones de arranque
- Direccionamiento IP
- Tabla de enrutamiento
- Listas de acceso (si tiene)
- Logs generados.

Nota: Para poder recolectar las características de configuración del equipo, se deben contar con las credenciales de autenticación, estas de ser posible pueden ser pedidas al dueño o al administrador de la red.

EJEMPLO PARA PLATAFORMAS LINUX Y WINDOWS:

Herramientas:

- Navegador Web
- Consola de línea de comandos

1.- Características Físicas

Los datos de las características físicas del router se pueden encontrar en la parte externa del dispositivo, por lo que se debe tener acceso al mismo.

Figura 1-3: Parte frontal Router

Fuente: www.configuratuequio.com

Figura 2-3: Parte trasera Router

Fuente: www.configuratuequio.com

- **Marca:** Huawei
- **Modelo:** HGS532s

- **Serie:** ##########
- **No. De puertos:** 6
- **Tipo de puertos:** 4 LAN, 1 ASDL, 1USB

2.- Características de configuraciones

Para acceder a las configuraciones del Router tanto en Windows como en Linux, solamente se necesita conocer la dirección IP del mismo y un navegador Web.

2.1.- Obtención dirección IP

Windows

- ipconfig

La dirección IP que aparece a la derecha de "Puerta de enlace predetermina" es la dirección IP del router.

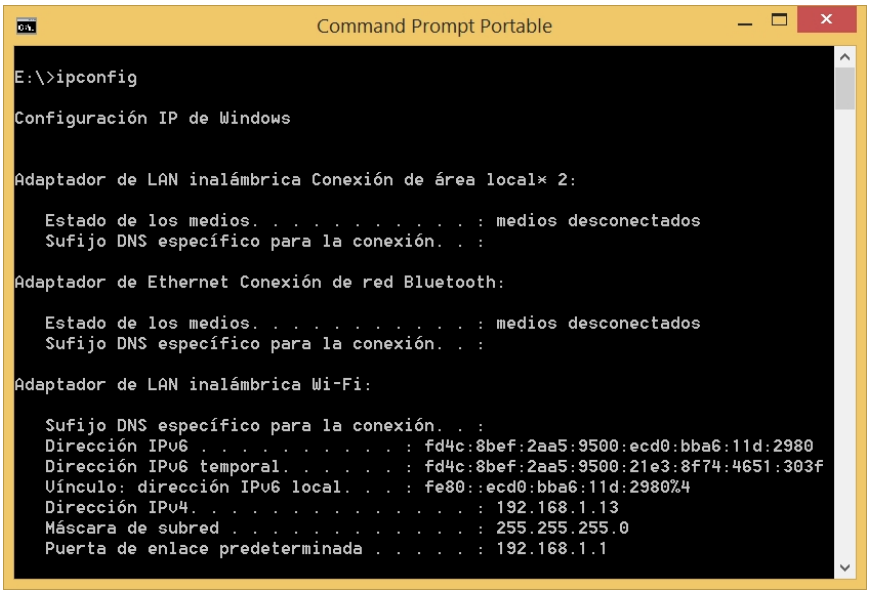


Figura 3-3: Dirección IP de Router

Realizado por: Luis Lema, 2016

Linux

- route –n

La dirección IP debajo de “Gateway”, es la IP del router.

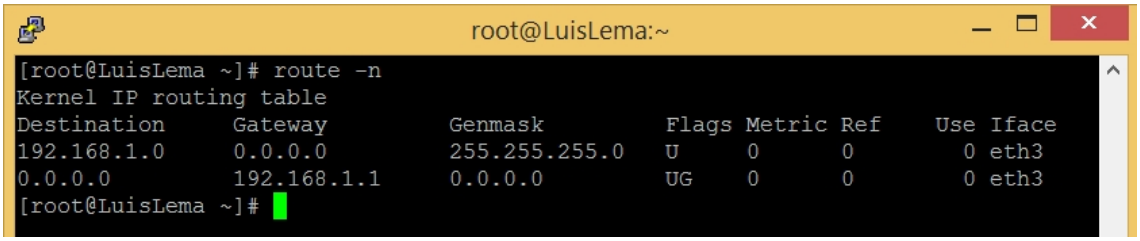


Figura 4-3: Dirección IP de Router

Realizado por: Luis Lema, 2016

2.2.- Ingresar al Router

El procedimiento de ingreso al router es el mismo en Windows y Linux:

Primero se debe abrir un navegador Web y escribir en la barra de direcciones la dirección IP que se obtuvo en el paso anterior. Para este ejemplo se ingresará a un Router Huawei, ingresar el nombre de usuario y password correspondientes.

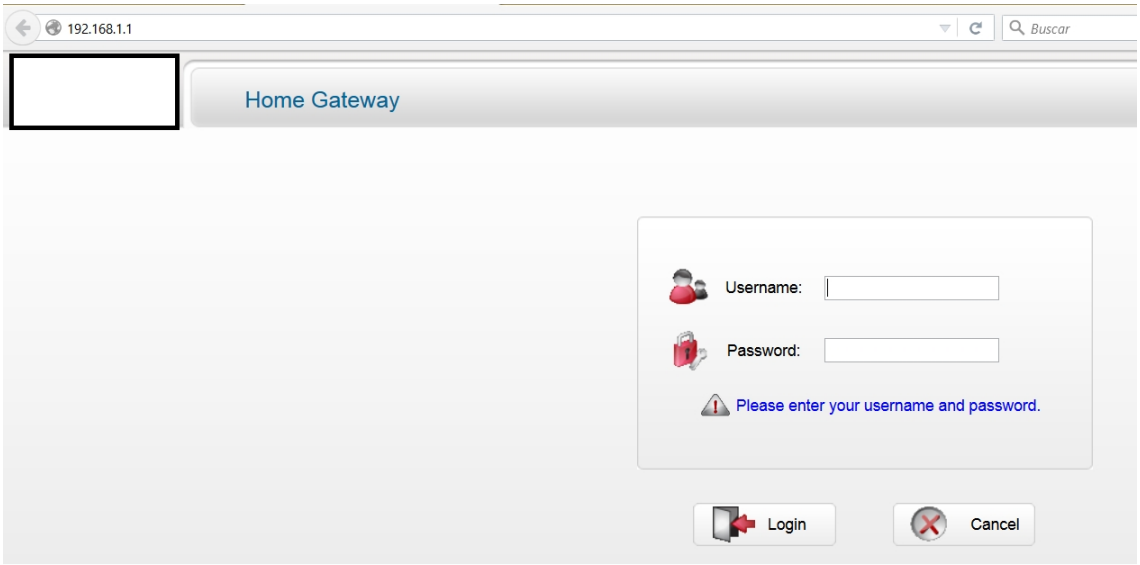


Figura 5-3: Página de ingreso a Router

Realizado por: Luis Lema, 2016

Una vez que se ingresa al Router aparece la siguiente pantalla:

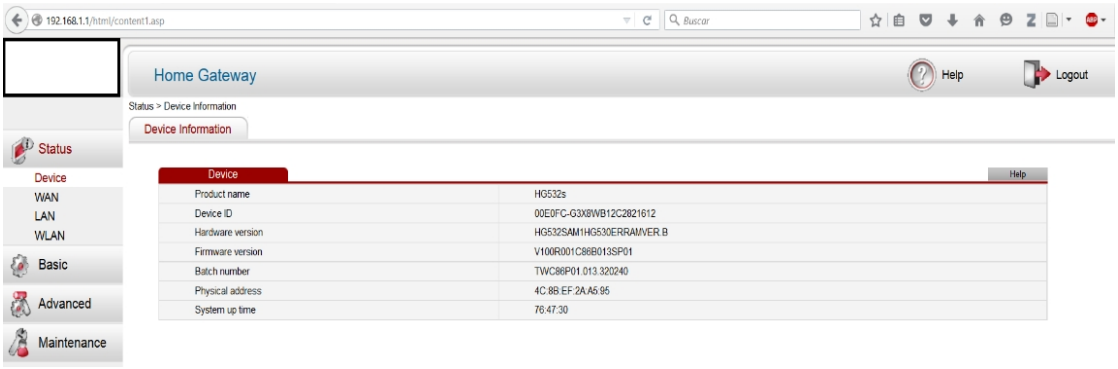


Figura 6-3: Página de inicio Router

Realizado por: Luis Lema, 2016

Para adquirir la información de configuración de arranque, en el caso del ejemplo se debe seguir el siguiente camino: Maintenance -> Device, luego escoger la pestaña "Configuration File" aquí se encuentra el botón "Download Configuration file" que al momento de dar clic en él se descargará el archivo de configuración del dispositivo.

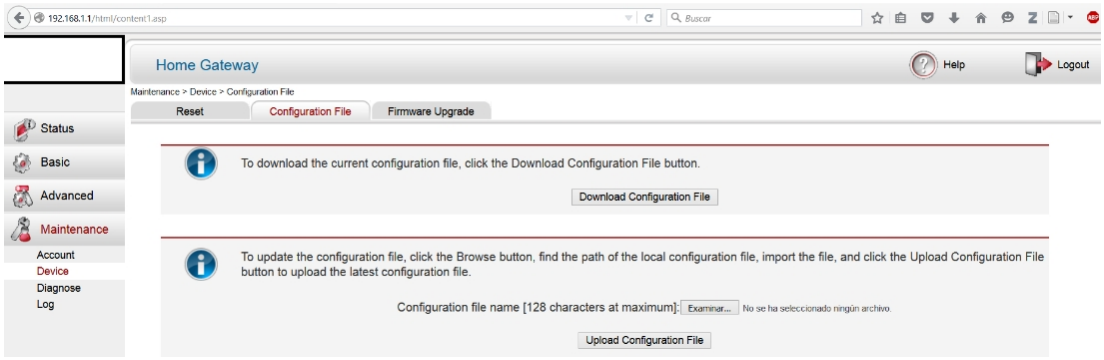


Figura 7-3: Descarga archivo de configuración Router

Realizado por: Luis Lema, 2016

Para obtener el direccionamiento IP se debe seguir el siguiente camino: Basic -> LAN, en la pestaña "DCHP", se encuentra la información requerida.

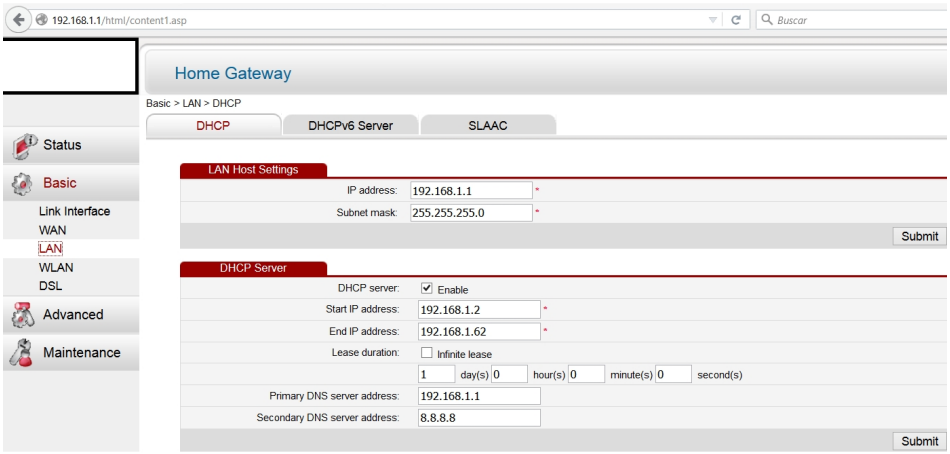


Figura 8-3: Direccionamiento IP Router

Realizado por: Luis Lema, 2016

La tabla de enrutamiento se puede obtener siguiendo el siguiente camino: Advanced -> Routing, en las tres pestañas disponibles: "Static Routing", "Dynamic Routing" y "IPv6 Static Routing" se puede conseguir información sobre enrutamiento.

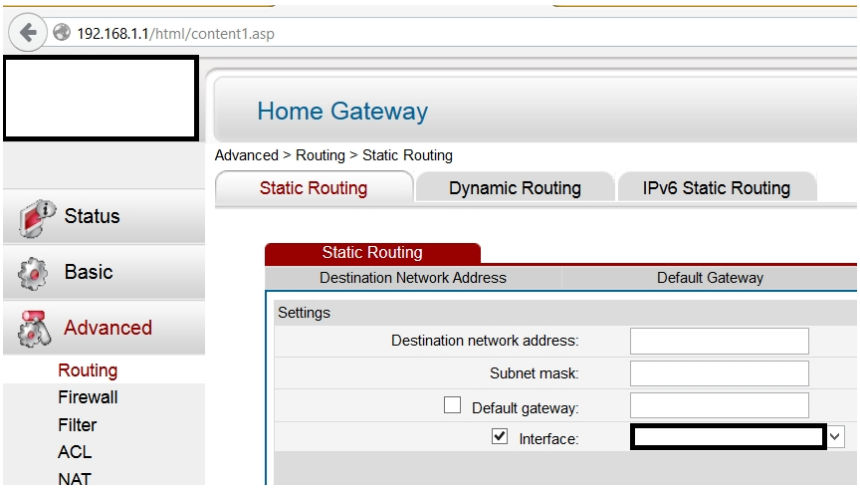


Figura 9-3: Static Routing

Realizado por: Luis Lema, 2016

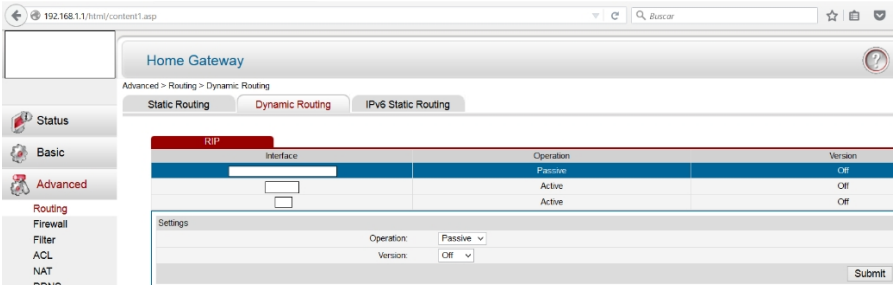


Figura 10-3: Dynamic Routing

Realizado por: Luis Lema, 2016

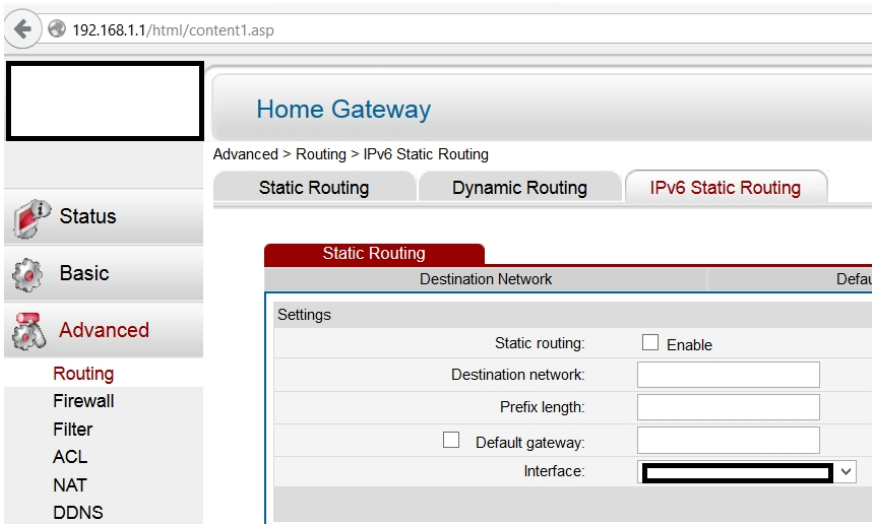


Figura 11-3: IPv6 Static Routing

Realizado por: Luis Lema, 2016

La información de Listas de Acceso (ACL) se encuentra en: Advanced -> ACL.

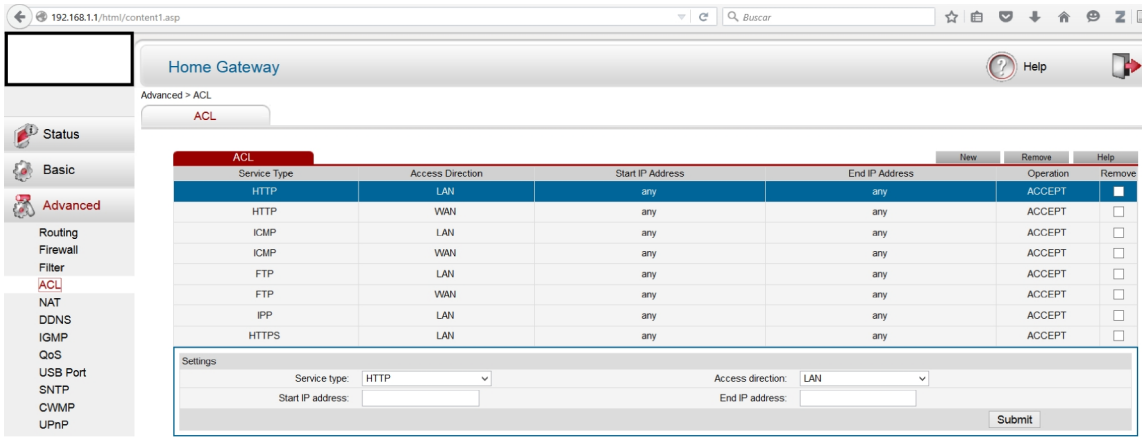


Figura 12-3: ACL Router

Realizado por: Luis Lema, 2016

Para observar los Logs generados por el Router se debe seguir el siguiente camino: Maintenace -> Log, en la pestaña “Displaying Logs” se encuentra la información que se busca.

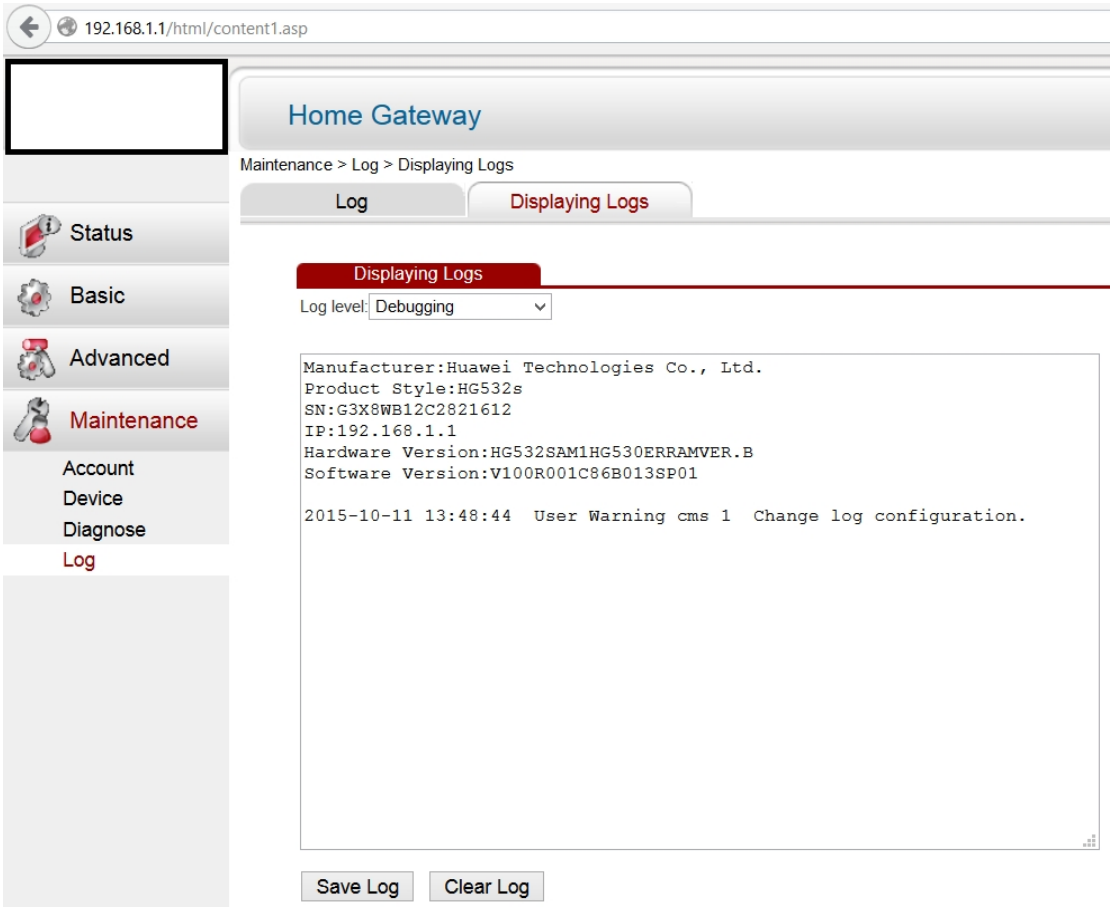


Figura 13-3: Log Router

Realizado por: Luis Lema, 2016

3.3.3. Acción Número 3

NOMBRE: Recolectar información de Switch

PROTOCOLO DE ACTUACIÓN:

1.- Describir características físicas:

- Marca
- Modelo
- Serie
- Número de Puertos
- Tipos de Puertos

2.- Describir características de configuraciones:

- Configuraciones de arranque
- VLANs
- Tabla CAM
- Logs generados

Nota: Para poder recolectar las características de configuración del equipo, se deben contar con las credenciales de autenticación, estas de ser posible pueden ser pedidas al dueño o al administrador de la red.

EJEMPLO PARA PLATAFORMAS WINDOWS Y LINUX:

En este caso se va a recolectar la información necesaria directamente desde el switch, por lo que es necesario tener acceso físico al dispositivo y poder entrar a las configuraciones del mismo. Por lo que no es necesario contar con herramientas de software.

Para este ejemplo se va a utilizar un Switch marca CISCO.

1.- Características Físicas

Los datos de las características físicas del switch se pueden encontrar en la parte externa del dispositivo, por lo que se debe tener acceso al mismo.

Figura 14-3: Parte trasera Switch

Fuente: www.twenga.es

- **Marca:** Cisco
- **Modelo:** Catalyst 2960
- **Serie:** ###########
- **No. De puertos:** 24+2
- **Tipo de puertos:** 24 FaE, 2 GiE

2.- Características de configuraciones

Para acceder a las configuraciones del Switch tanto en Windows como en Linux, solamente se necesita conocer la dirección IP administrativa del mismo y un cliente de Telnet o SSH.

2.1.- Configuraciones de arranque

Para obtener las configuraciones de arranque debemos ingresar al modo privilegiado del switch mediante el siguiente comando:

- enable

Ingresar la contraseña para ingresar al modo privilegiado si es solicitada.

```
Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


ALS1>ena
ALS1>enable
Password:
ALS1#
```

Figura 15-3: Modo Privilegiado Switch

Realizado por: Luis Lema, 2016

A continuación, para desplegar las configuraciones con las que inicia el switch ejecutar el comando:

- show startup-config

```
ALS1#show  startup-config
Using 1290 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ALS1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
 --More--
```

Figura 16-3: startup-config Switch

Realizado por: Luis Lema, 2016

Para seguir observando más configuraciones presionar la tecla “Enter” o la barra espaciadora.

2.2.- VLANs

La información de VLANs se puede obtener ejecutando el siguiente comando en modo privilegiado:

- show vlan

```
ALS1# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
100  Payroll                           active    Fa0/6
200  Engineering                       active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
100  enet  100100     1500  -      -      -        -    -        0      0
200  enet  100200     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
ALS1#
```

Figura 17-3: show vlan Switch

Realizado por: Luis Lema, 2016

2.3.- Tabla CAM

Para adquirir la información almacenada en la tabla CAM del switch se debe ejecutar el siguiente comando:

- show mac address-table

```
ALS1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9628.4701    DYNAMIC     Fa0/1
   1    0090.2b00.cc0b    DYNAMIC     Fa0/11
 100    0001.9628.4701    DYNAMIC     Fa0/1
 200    0001.9628.4701    DYNAMIC     Fa0/1
ALS1#
```

Figura 18-3: Tabla cam Switch

Realizado por: Luis Lema, 2016

2.4.- Logs generados

Para observar los Logs generados en el switch se debe ejecutar el comando:

- show logging

```
ALS1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 7 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level informational, 7 message lines logged
ALS1#
```

Figura 19-3: Logs Switch

Realizado por: Luis Lema, 2016

3.3.4. Acción Número 4

NOMBRE: Capturar tráfico de red en tiempo real

PROTOCOLO DE ACTUACIÓN:

1.- Elegir una herramienta para capturar el tráfico en la red.

2.- Conectar la máquina del investigador a la red donde se encuentra conectada la máquina sospechosa.

3.- Capturar el tráfico que pase por la tarjeta de red de la máquina del investigador en tiempo real.

4.- Filtrar la información que se desee obtener.

Nota: La captura de tráfico debe realizarse en una máquina diferente a la que está siendo investigada, para evitar alterar la información de la misma.

EJEMPLO PARA PLATAFORMAS WINDOWS Y LINUX:

Herramientas para capturar tráfico de red:

- Wireshark (Windows y Linux), disponible en: https://www.wireshark.org/#download
- Capsa Free Network Analyzer (Windows), disponible en: http://www.colasoft.com/download/products/capsa_free.php
- Tcpdump (Linux), disponible en: http://www.tcpdump.org/release/tcpdump-4.7.4.tar.gz

Ejemplo:

El primer paso es abrir la herramienta Wireshark, desde Windows dando doble clic en el ícono de acceso directo, desde Linux escribiendo wireshark en línea de comandos.

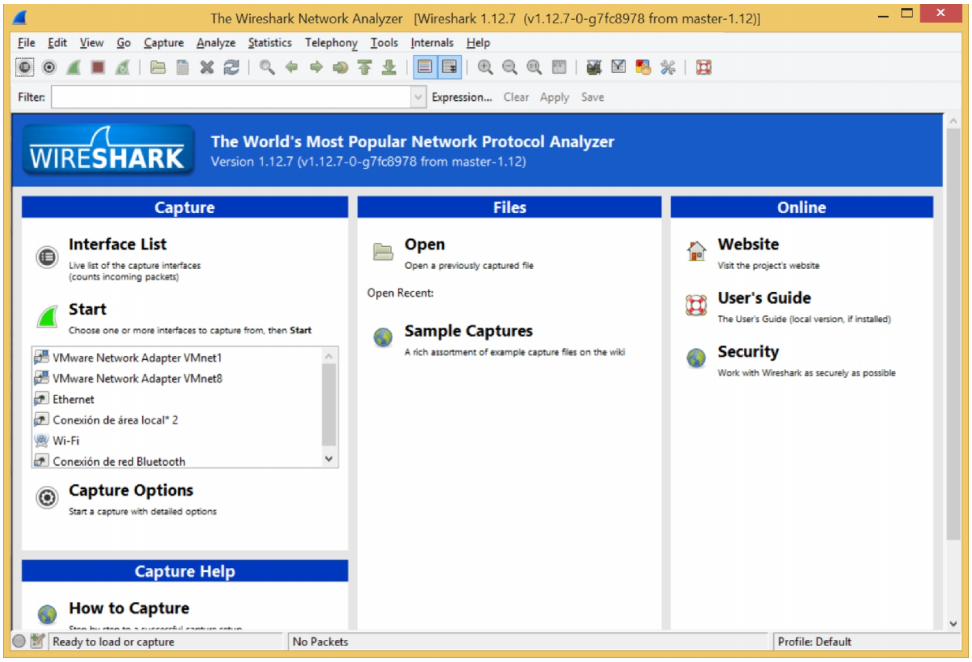


Figura 20-3: Wireshark – Ventana Principal

Realizado por: Luis Lema, 2016

De todas las interfaces que se encuentran listadas, elegir la interfaz que se encuentra conectada a la red de la que se va a capturar el tráfico. Para este ejemplo se utilizará la interfaz inalámbrica.

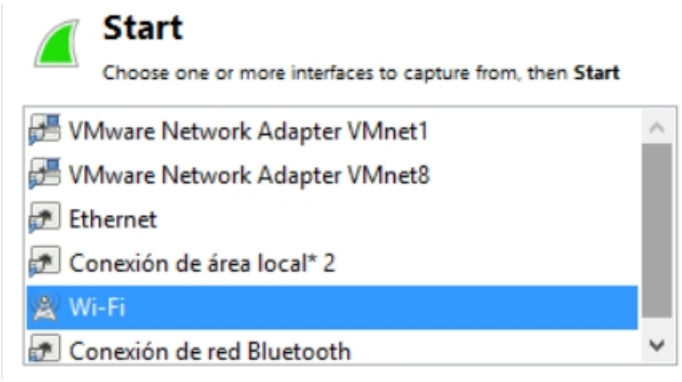


Figura 21-3: Wireshark – Elección Interfaz

Realizado por: Luis Lema, 2016

Luego de haber elegido la interfaz dar clic en el botón "Start", la herramienta empezará a capturar todo el tráfico que está pasando por la tarjeta Wireless.

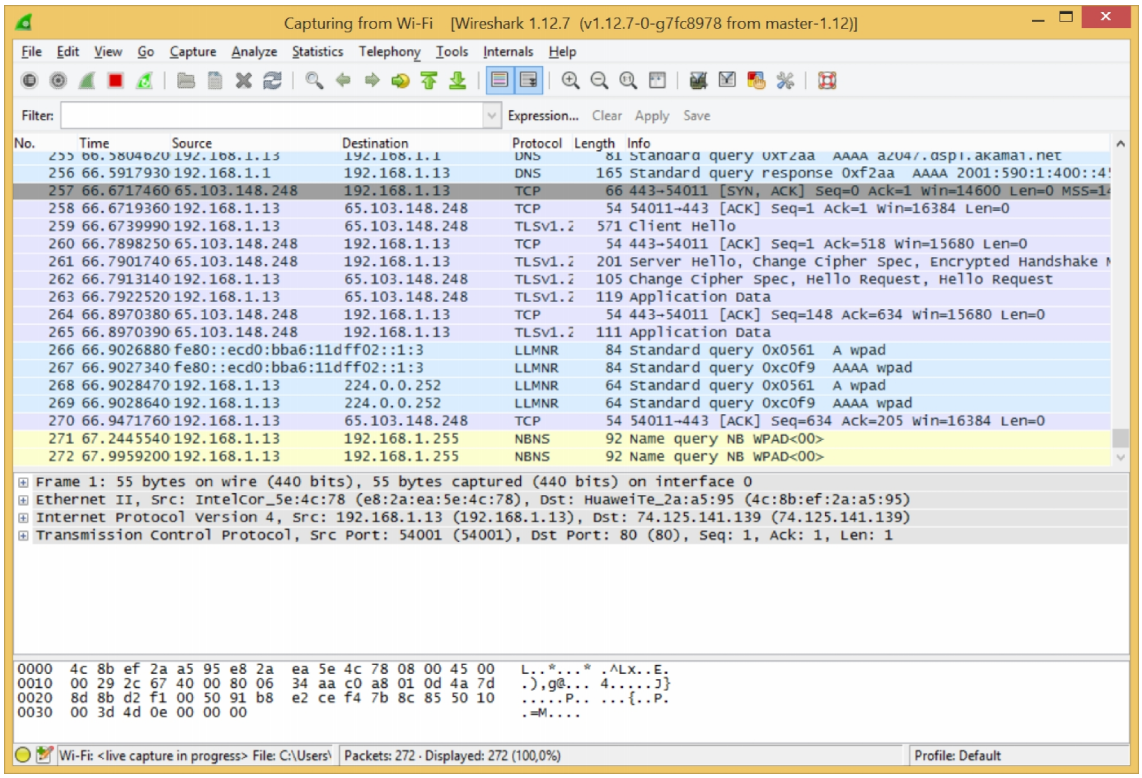


Figura 22-3: Wireshark – Captura de tráfico

Realizado por: Luis Lema, 2016

Una vez que se haya capturado la cantidad de tráfico necesario (puede ser pocos o varios minutos), para terminar la captura se debe dar clic en el botón cuadrado rojo que se encuentra en la parte superior.

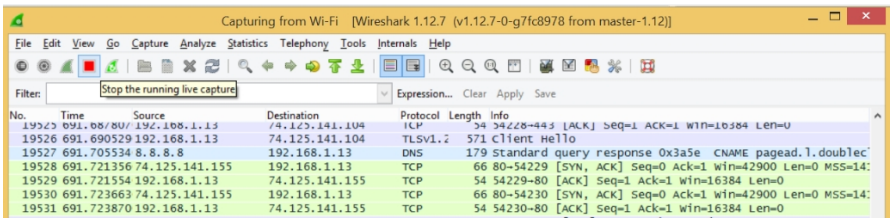


Figura 23-3: Wireshark – Parar captura de tráfico

Realizado por: Luis Lema, 2016

Finalmente, cuando se ha terminado la captura de paquetes, para poder obtener información que sea útil, se pueden filtrar los paquetes dependiendo del protocolo que se desee analizar, como por ejemplo: HTTP, TCP, UDP, DNS, ARP, etc. También se pueden filtrar los paquetes por la IP de origen o destino y realizar varias combinaciones de filtros.

Para este ejemplo, se va a filtrar paquetes correspondientes al protocolo HTTP, para lo cual se debe escribir en la barra llamada "Filter" la palabra http. En la parte de la mitad de la ventana se puede ver más información del paquete señalado por capa, en la imagen se puede ver información de capa 4 como son puertos de origen y destino.

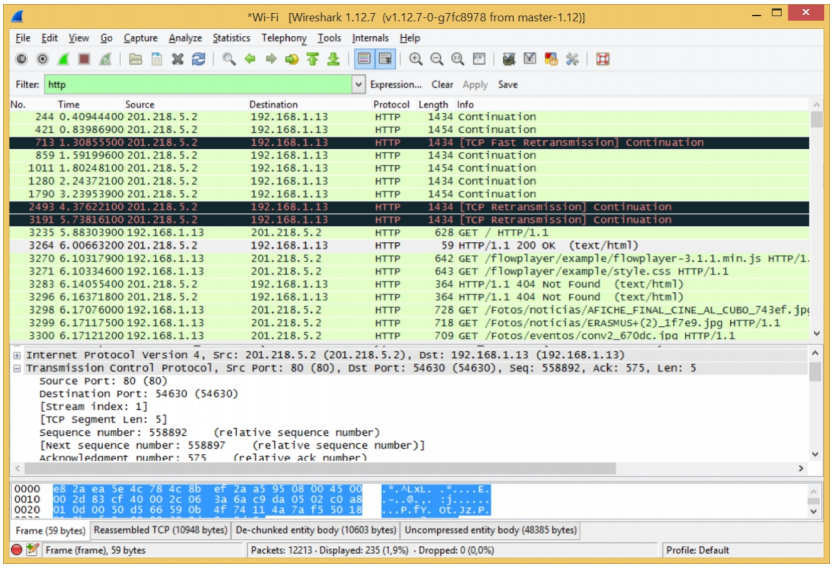


Figura 24-3: Wireshark – Filtro por http

Realizado por: Luis Lema, 2016

Otro filtro que se puede aplicar es por la IP de origen y/o destino, para este ejemplo se utilizará la IP de destino: 201.218.5.2 que es la dirección IP de la página web de la ESPOCH.

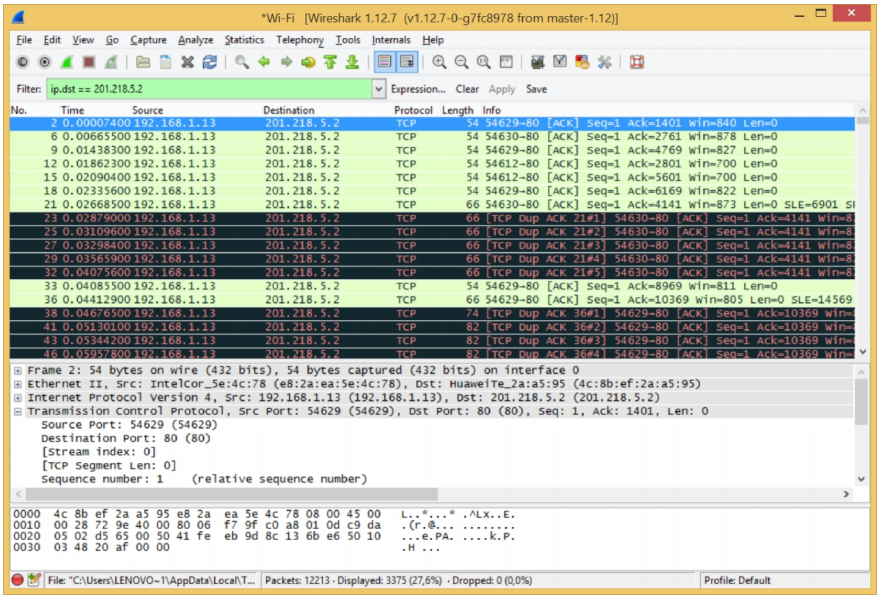


Figura 25-3: Wireshark – Filtro por IP destino

Realizado por: Luis Lema, 2016

Con wireshark es posible capturar incluso inicios de sesión que se realizan en páginas web que no son seguras, para eso solamente se puede aplicar el filtro: (http) && (ip.dst == 201.218.5.22). La dirección IP de destino es del sistema elearnig.espoch.edu.ec.

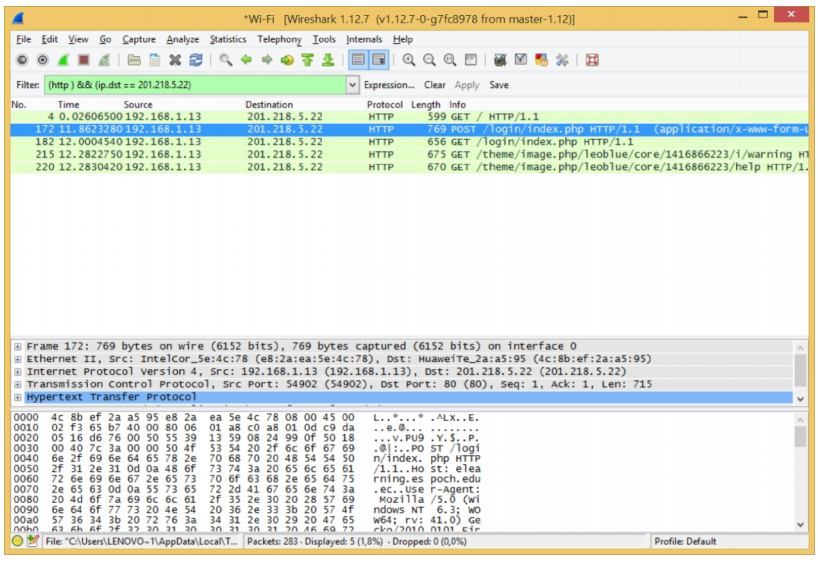


Figura 26-3: Wireshark – Filtro por http e IP destino

Realizado por: Luis Lema, 2016

Una vez aplicado el filtro se debe seleccionar el paquete que contiene la información de LOGIN, en este ejemplo es el segundo paquete, dar clic derecho sobre el mismo y elegir la opción “Follow TCP Stream”.

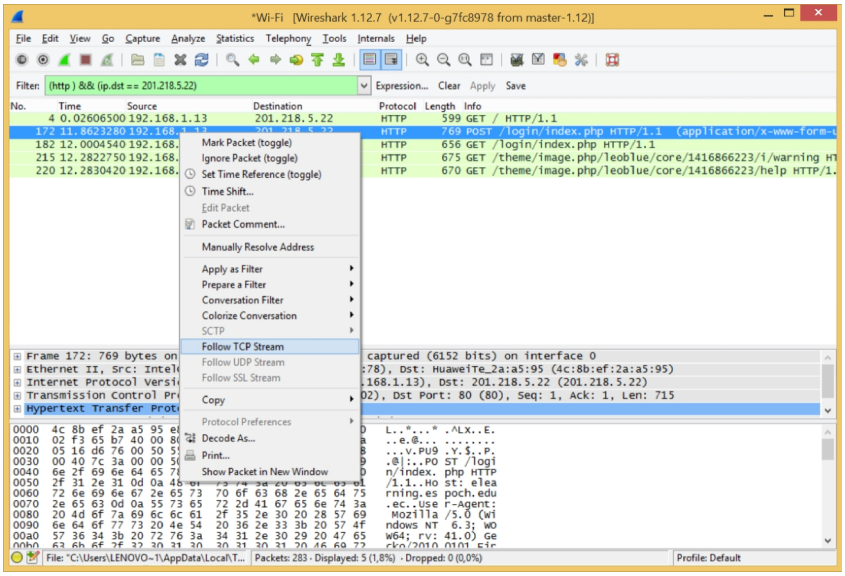


Figura 27-3: Wireshark – Follow TCP Stream

Realizado por: Luis Lema, 2016

Finalmente, se abrirá una ventana con toda la información del paquete, en la que se incluye el nombre de usuario y contraseña que se ingresó en el formulario de LOGIN.

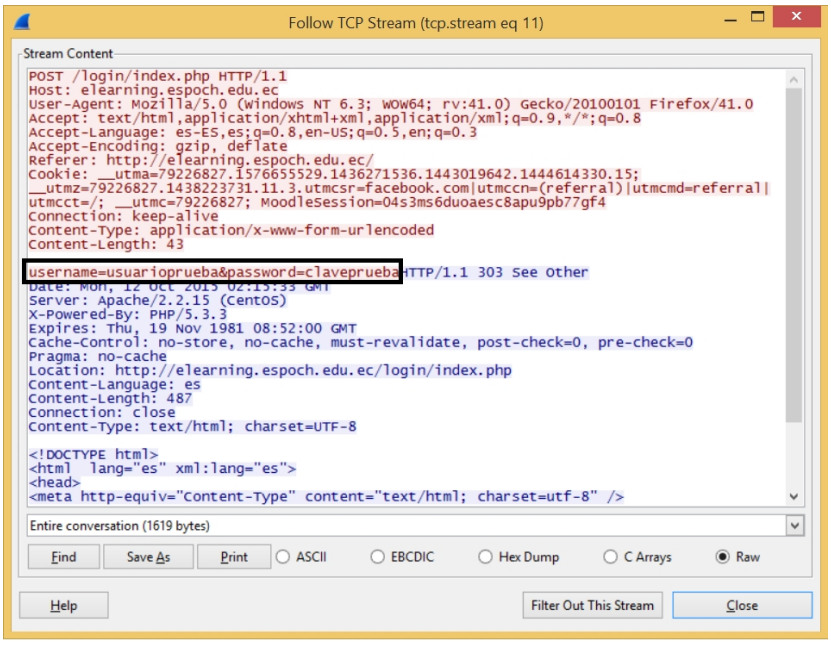


Figura 28-3: Wireshark – Follow TCP Stream- Info. Paquete

Realizado por: Luis Lema, 2016

Herramienta Recomendada:

Para este ejemplo se ha elegido la herramienta de captura de tráfico Wireshark, ya que sirve tanto para Windows como Linux y en las dos plataformas tiene la misma interfaz gráfica. Wireshark se puede descargar desde: https://www.wireshark.org/#download.

Entre las principales características de esta herramienta están:

- Se encuentra disponible para Linux y Windows.
- Muestra información bastante detallada de los paquetes capturados.
- Se puede importar y exportar paquetes capturados desde y hacia varios programas de captura diferentes.
- Filtrar paquetes por varios criterios.
- Personalizar con colores los resultados.
- Captura de paquetes en vivo.

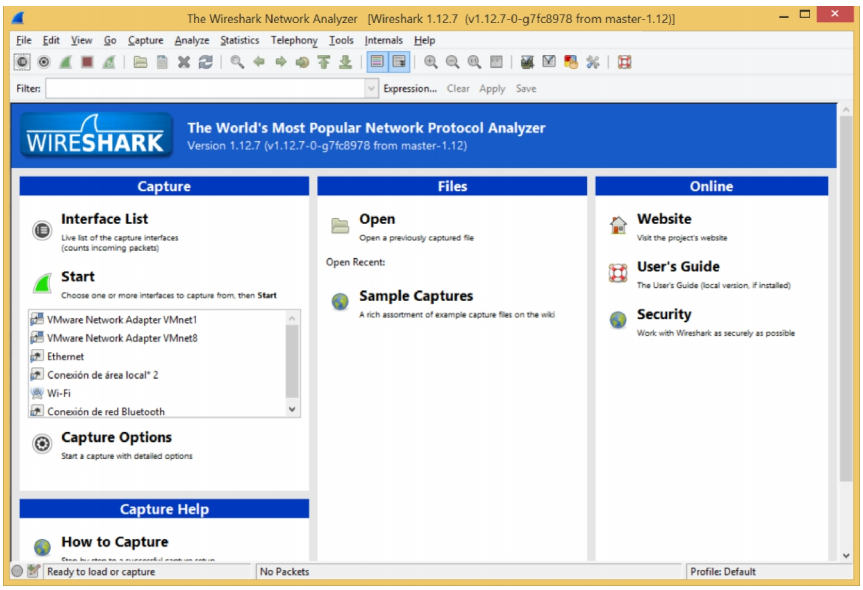


Figura 29-3: Wireshark

Realizado por: Luis Lema, 2016

3.3.5. Acción Número 5

Nombre: Adquisición de información volátil

PROTOCOLO DE ACTUACIÓN:

Nota: Para la adquisición de información volátil utilizar siempre guantes de látex y manilla antiestática.

1.- No apagar o reiniciar el equipo de donde se va a recolectar la información.

2.- Fotografiar la escena donde se está investigando, eso incluye tomar fotografía de la pantalla y de los periféricos que están conectados (mouse, impresora, cámaras, etc).

3.- Si la pantalla está encendida tomar fotografía de la misma.

4.- Si la pantalla esta con salvapantallas o en blanco, mover lentamente el mouse sin aplastar ningún botón y tomar fotografía a la pantalla.

5.- Identificar el sistema operativo que correo en la máquina comprometida.

6.- Recolectar la información volátil importante:

- Hora y Fecha del Sistema
- Usuarios Logueados
- Archivos Abiertos
- Información de procesos corriendo en memoria
- Puertos abiertos y la aplicación que los está usando
- Historial de comandos

7.- Realizar un volcado de la Memoria RAM en otro dispositivo de almacenamiento. Calcular valor hash del archivo resultante del volcado de memoria. Se recomienda no

utilizar el algoritmo MD5 ya que no es seguro, en su lugar se puede usar SHA1, SHA-256, CRC32, etc.

8.- Cuando se vaya a realizar la adquisición de la información volátil, no utilizar las herramientas administrativas propias del sistema operativo, ya que pueden estar comprometidas. Se recomienda recopilar las herramientas (binarios) y guardarlas en un medio externo.

9.- Alterar el sistema lo menos posible.

10.- Crear un informe completo con todos los pasos y acciones seguidas.

EJEMPLO PARA PLATAFORMA WINDOWS VÍA COMANDOS Y HERRAMIENTAS DE SOFTWARE:

Ejemplo vía comandos:

1.- Hora y fecha del sistema

- date /t & time /t

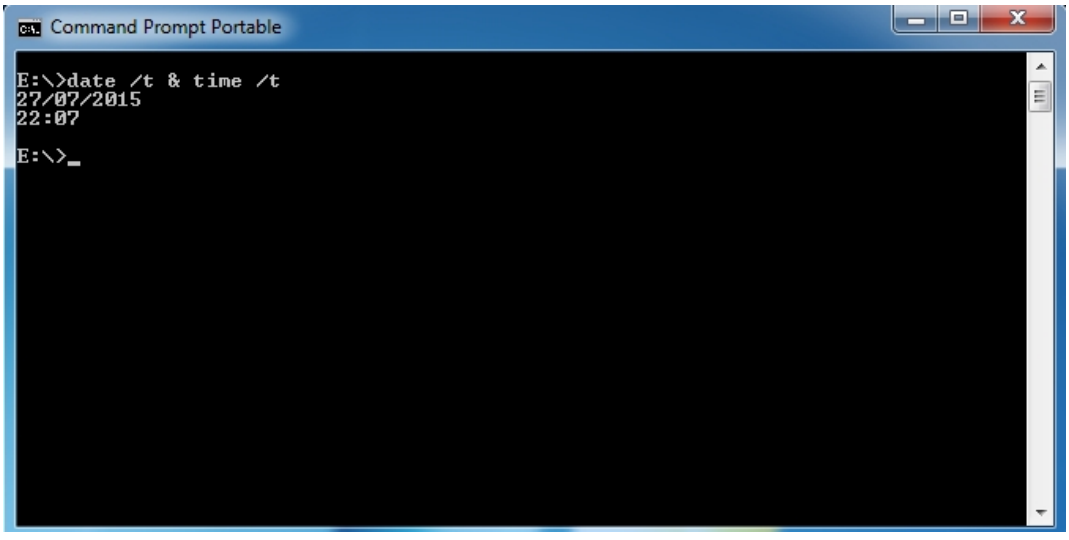


Figura 30-3: Hora y Fecha del Sistema – date & time

Realizado por: Luis Lema, 2016

2.- Usuarios Logueados

- PsLoggedon.exe
- net sessions

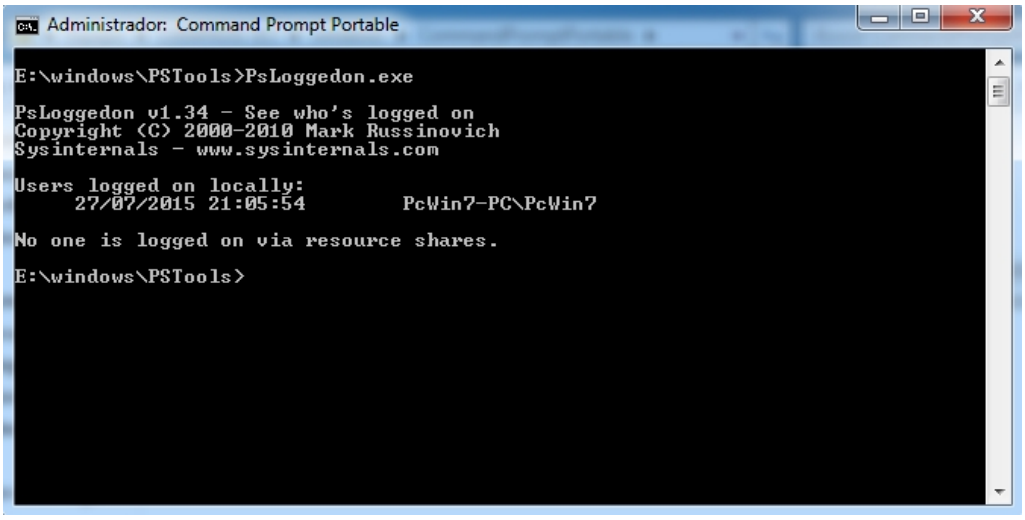


Figura 31-3: Usuarios Logueados - PsLoggedon

Realizado por: Luis Lema, 2016

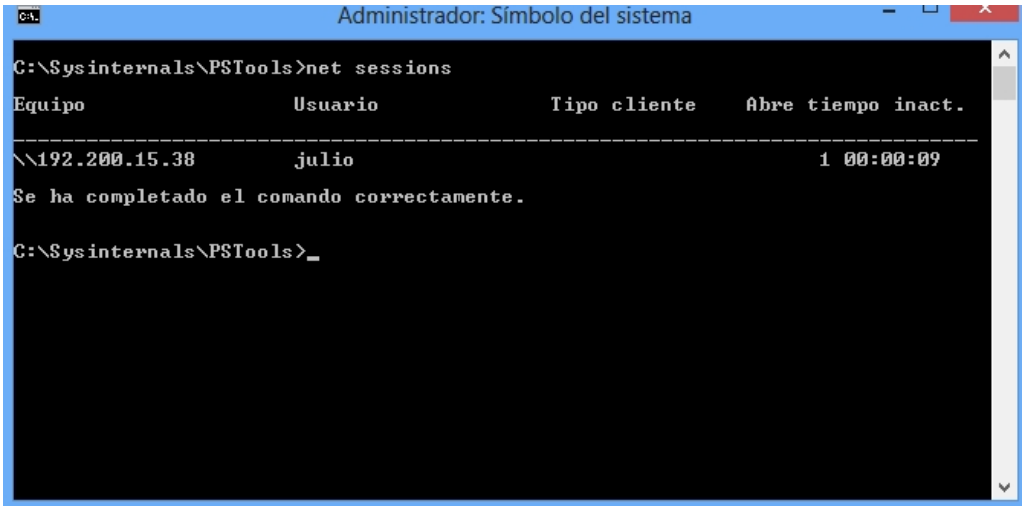


Figura 32-3: Usuarios Logueados net sessions

Fuente: Windows forensics

Autor: Julio Iglesias, 2013

3.- Archivos Abiertos

- net file
- psfile

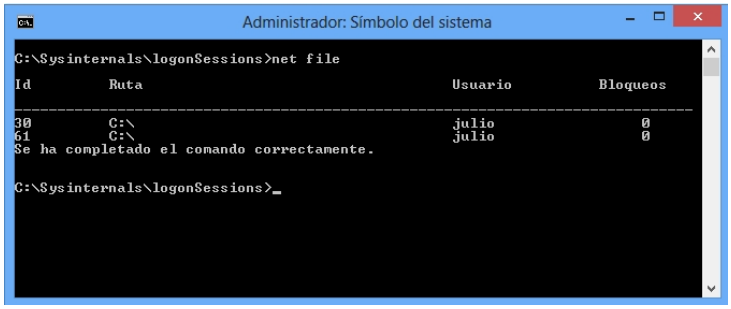


Figura 33-3: Archivo Abiertos - net file

Fuente: Windows forensics

Autor: Julio Iglesias, 2013

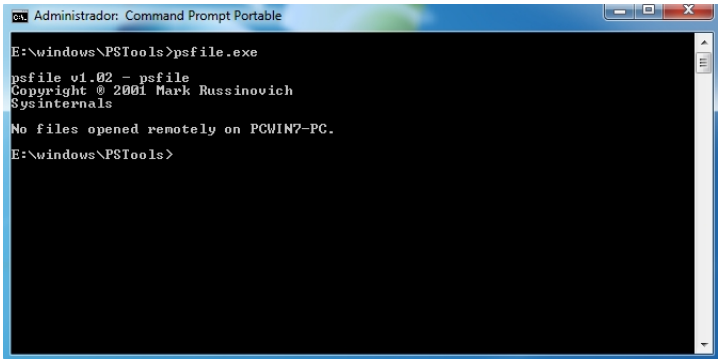


Figura 34-3: Archivos Abiertos - psfile

Realizado por: Luis Lema, 2016

4.- Información de Procesos

- tasklist
- Pslist.exe
- Listdlls.exe

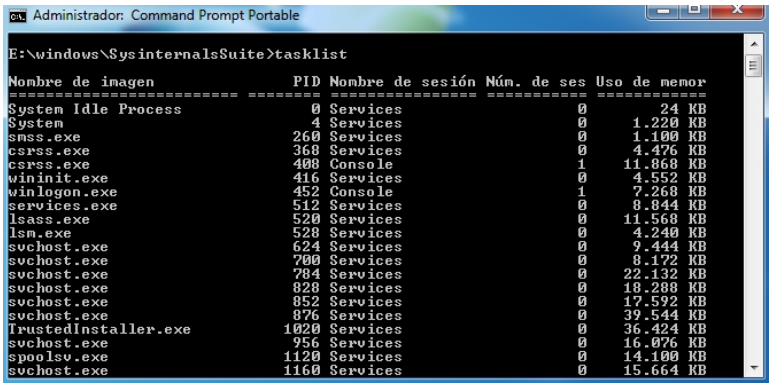


Figura 35-3: Información Procesos - tasklist

Realizado por: Luis Lema, 2016

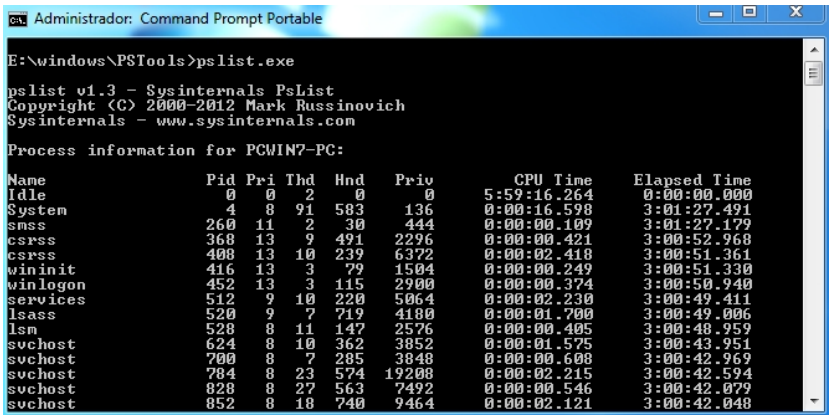


Figura 36-3: Información Procesos – pslist

Realizado por: Luis Lema, 2016

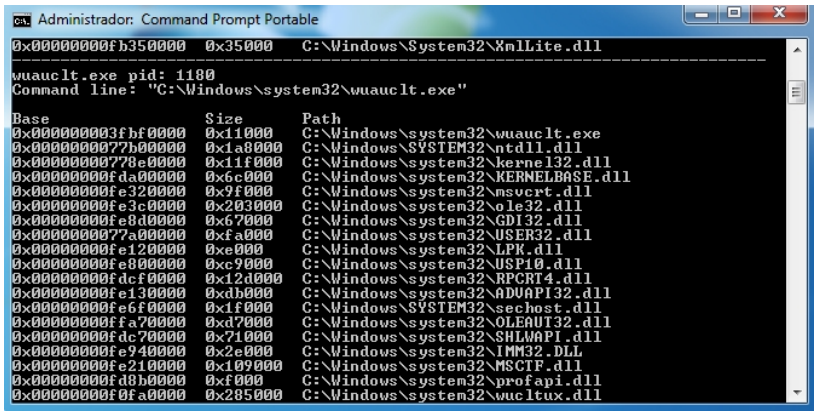


Figura 37-3: Información Procesos – Listdlls

Realizado por: Luis Lema, 2016

5.- Puertos abiertos y aplicación que los está usando

- netstat -o

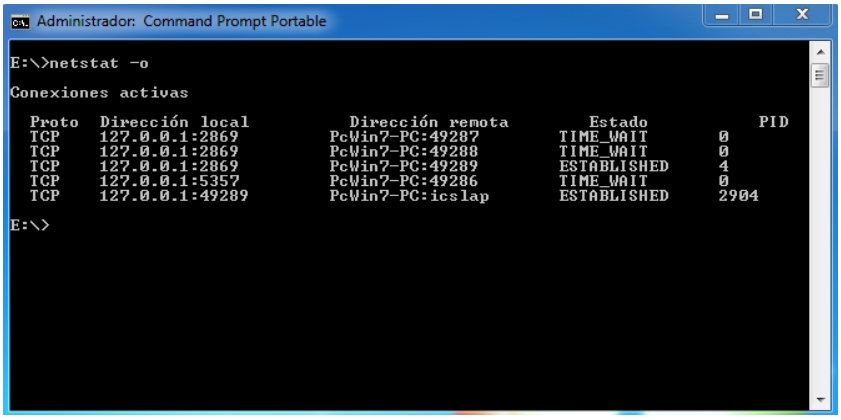


Figura 38-3: Mapeo de procesos a puertos – netstat

Realizado por: Luis Lema, 2016

6.- Historial de comandos

- doskey /history

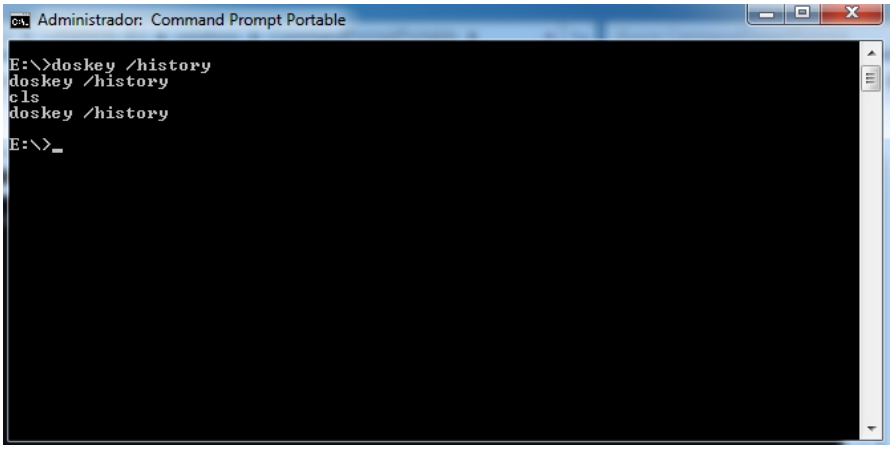


Figura 39-3: Historial Comandos – doskey /history

Realizado por: Luis Lema, 2016

7.- Volcado de Memoria

En Windows se deben utilizar herramientas para realizar esta tarea.

Herramientas para la adquisición de información Volátil:

- Win–UFO (Ultimate Forensics Outflow), disponible en: http://win-ufo.org/downloads.shtml

- logonsessions.exe, disponible en: https://technet.microsoft.com/en-us/sysinternals/bb896769.aspx

- OpenedFilesView, disponible en: http://www.nirsoft.net/utils/opened_files_view.html

- CurrPorts, disponible en: http://www.nirsoft.net/utils/cports.html

- FTK imager, disponible en: http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1

- HashMyFiles, disponible en: http://www.nirsoft.net/utils/hash_my_files.html

Ejemplo con herramientas de Software:

1.- Hora y fecha del sistema

Para esta tarea se utilizara el programa Win–UFO (Ultimate Forensics Outflow), la cual cuenta con la herramienta WinAudit que entrega mucha información sobre la máquina que se está revisando, entre la que se encuentra hora y fecha de sistema.

Primero abrir Win-UFO desde el medio donde esté instalado y dirigirse a la pestaña de "REPORTS". Se puede descargar desde http://win-ufo.org/downloads.shtml

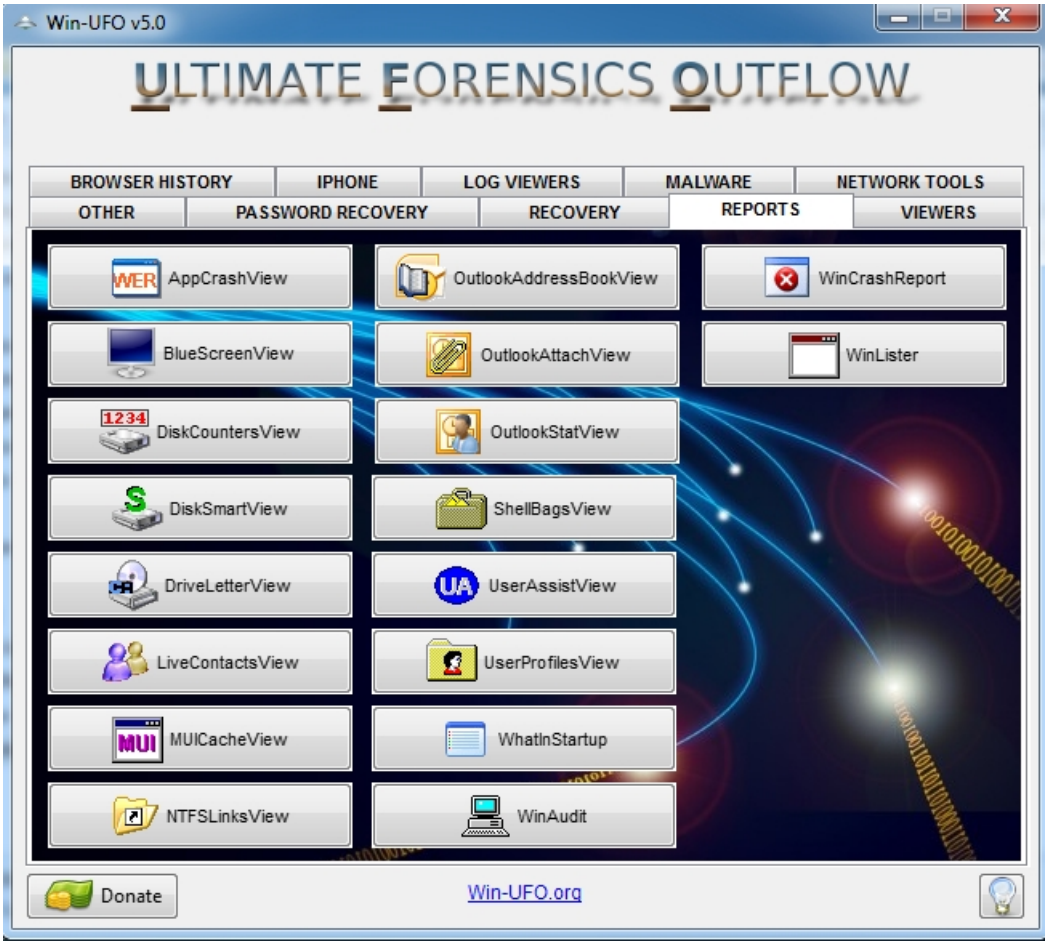


Figura 40-3: Ventana Win-UFO

Realizado por: Luis Lema, 2016

Dar click en el ícono llamado “Winaudit”, se abrirá otra ventana emergente en la que se debe dar click al enlace “Aquí” para que empiece a tomar la información del sistema.

Figura 41-3: Ventana WinAudit

Realizado por: Luis Lema, 2016

Finalmente aparecerá la información que la herramienta tomó del sistema, entre las que se incluye la fecha y hora del sistema. Se recomienda revisar las demás pestañas ya que contienen información extra.

Vista General

Item	Value
Computer Name	PCWIN7-PC
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server, Potential Browser
Description	
Operating System	Microsoft Windows 7 Professional 64-bit
Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Serial Number	VMware-56 4d bd bc 7f 75 c6 75-d7 dc c8 b8 8d 37 9f e4
Asset Tag	No Asset Tag
Number Of Processors	1
Processor Description	Intel(R) Core(TM) i7-4710HQ CPU @ 2.50GHz
Total Memory	3104MB
Total Hard Drive	59.9GB
Display	1366 x 768 pixels, true colour
BIOS Version	_ASUS_ - 6040000 PhoenixBIOS 4.0 Release 6.0
User Account	PcWin7
System Uptime	0 Days, 3 Hours, 19 Minutes
Local Time	2015-07-28 18:40:59

Figura 42-3: Vista General WinAudit

Realizado por: Luis Lema, 2016

2.- Usuarios Logueados:

Para recoger esta información se puede utilizar la utilidad logonsessions.exe. Se ejecuta directamente desde línea de comandos. Se puede descargar desde https://technet.microsoft.com/en-us/sysinternals/bb896769.aspx.

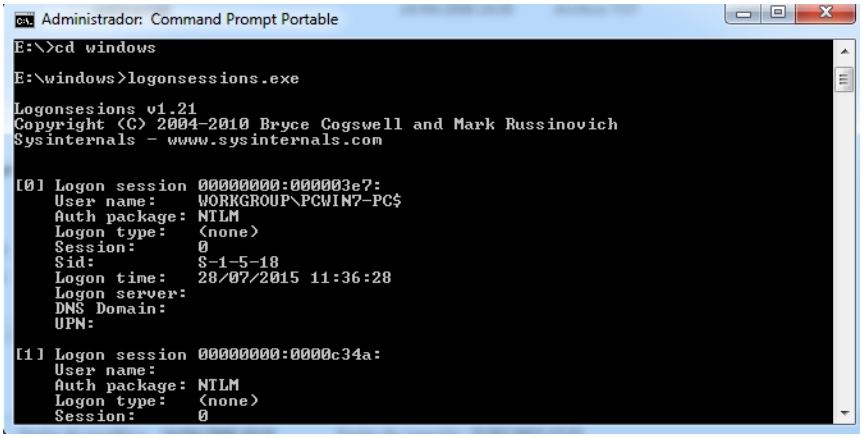


Figura 43-3: Usuarios Logueados – logonsessions.exe

Realizado por: Luis Lema, 2016

3.- Archivos abiertos:

Para ver los archivos abiertos se puede utilizar la herramienta OpenedFilesView. Se puede descargar desde http://www.nirsoft.net/utils/opened_files_view.html.

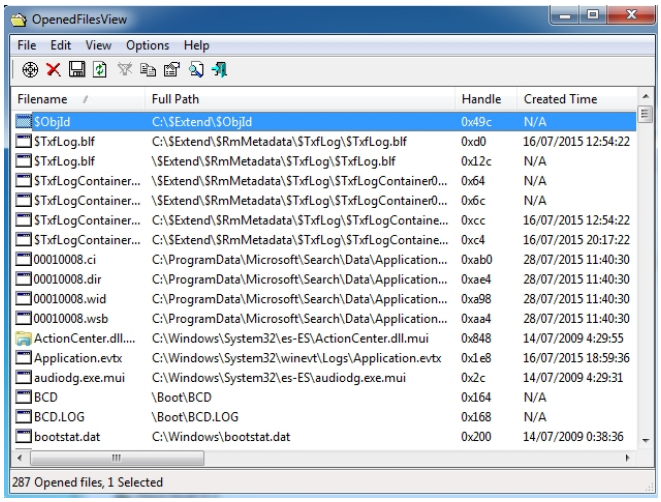


Figura 44-3: Archivos abiertos – OpenedFilesView

Realizado por: Luis Lema, 2016

4.- Información de Procesos:

Para obtener información de los procesos corriendo en el sistema se puede utilizar nuevamente el programa Win–UFO (Ultimate Forensics Outflow) la cual cuenta con la herramienta "ProcessActivityView", se encuentra en la pestaña "OTHER".

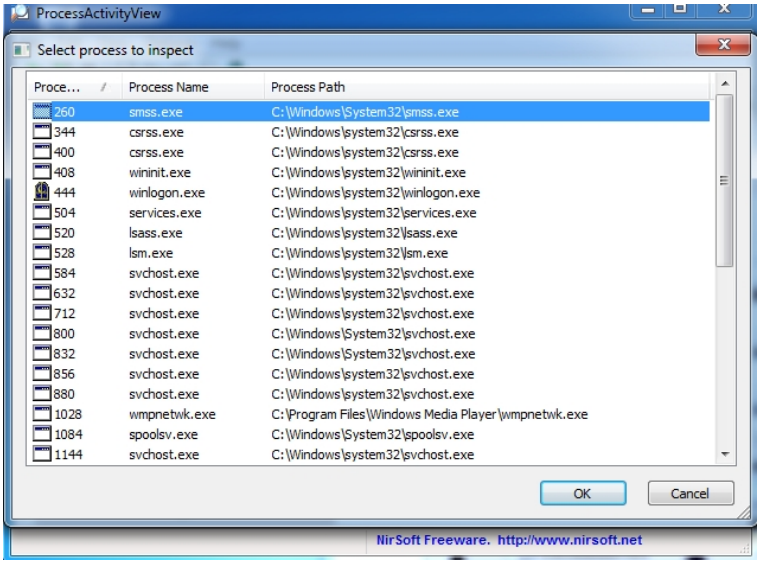


Figura 45-3: Información Procesos – ProcessActivityView

Realizado por: Luis Lema, 2016

En la misma pestaña de "OTHER" se encuentra la herramienta "CurrProcess", que muestra las aplicaciones abierta en ese momento e información de las mismas.

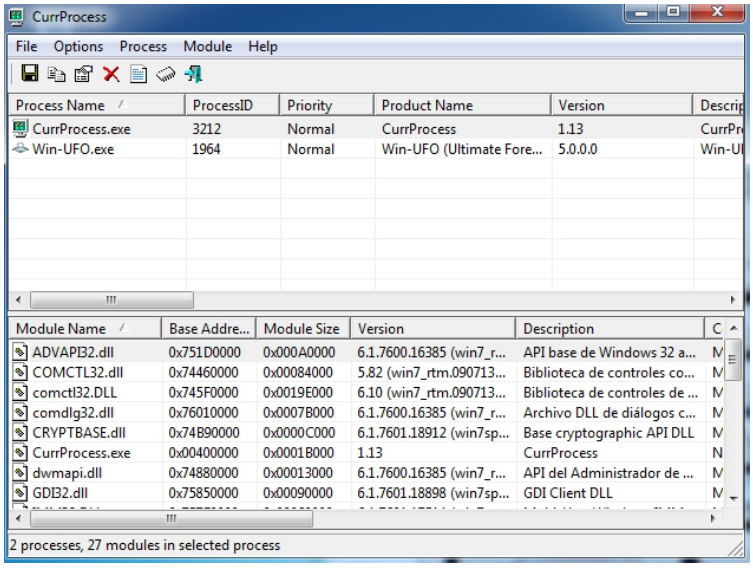


Figura 46-3: Información Procesos – CurrProcess

Realizado por: Luis Lema, 2016

5.- Puertos abiertos y aplicación que los está usando

Para el mapeo de puertos se puede utilizar la herramienta "cports" que se encuentra disponible en http://www.nirsoft.net/utils/cports.html.

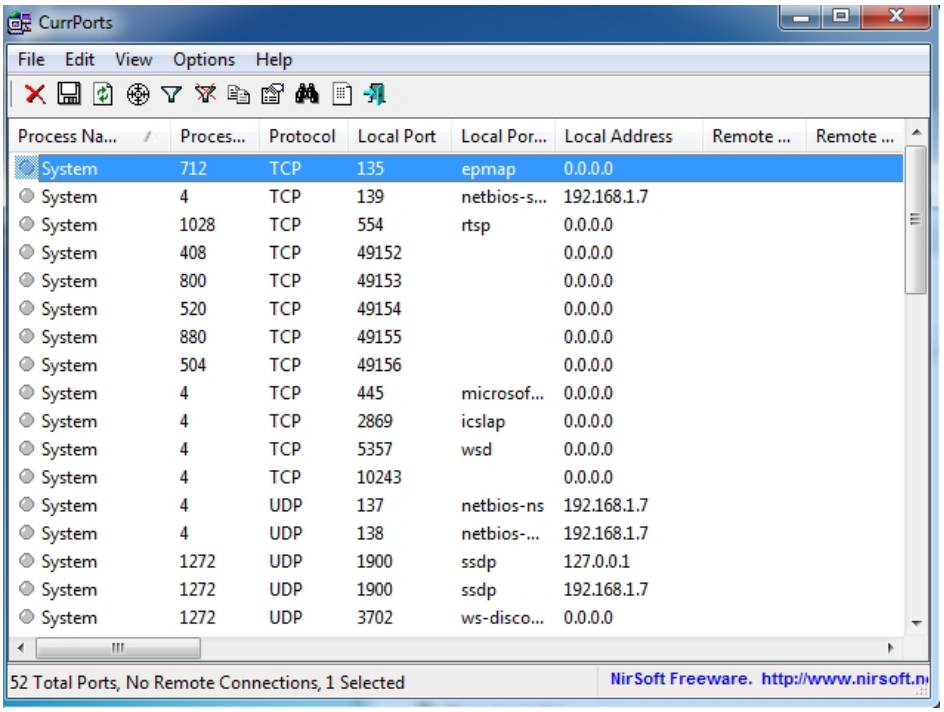


Figura 47-3: Mapeo de puertos – cports

Realizado por: Luis Lema, 2016

6.- Volcado de Memoria

Windows:

Para realizar el volcado de memoria de un sistema Windows se puede utilizar la herramienta FTK imager, la cual tiene la opción de permitir crear una copia exacta bit a bit de la memoria RAM. Esta herramienta puede obtenerse desde http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1.

Primero se debe abrir el programa y a continuación dar click en el ícono de "capture memory".

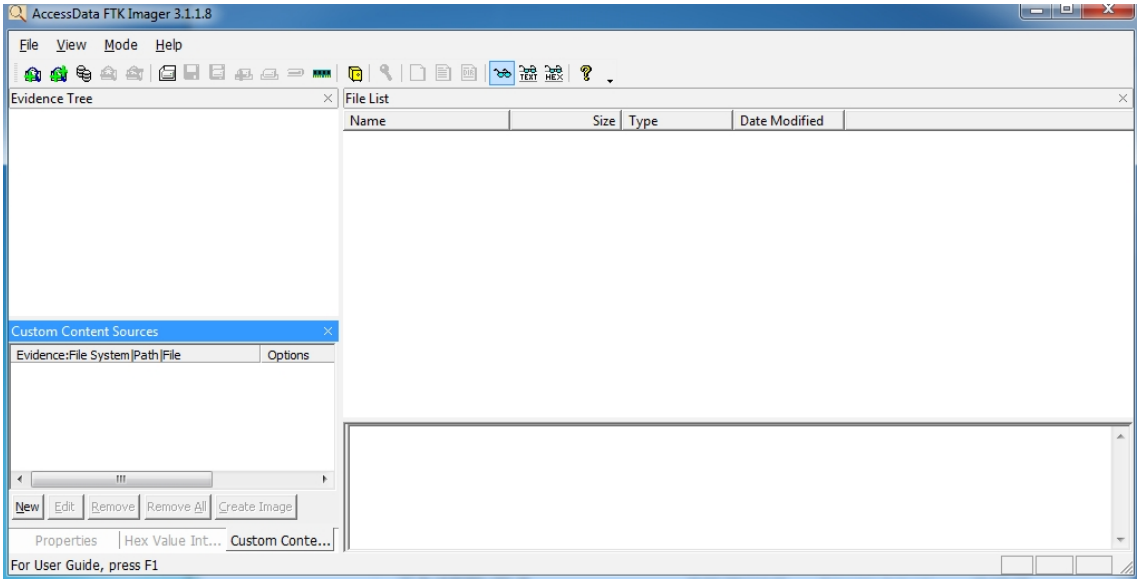


Figura 48-3: Ventana FTK imager

Realizado por: Luis Lema, 2016

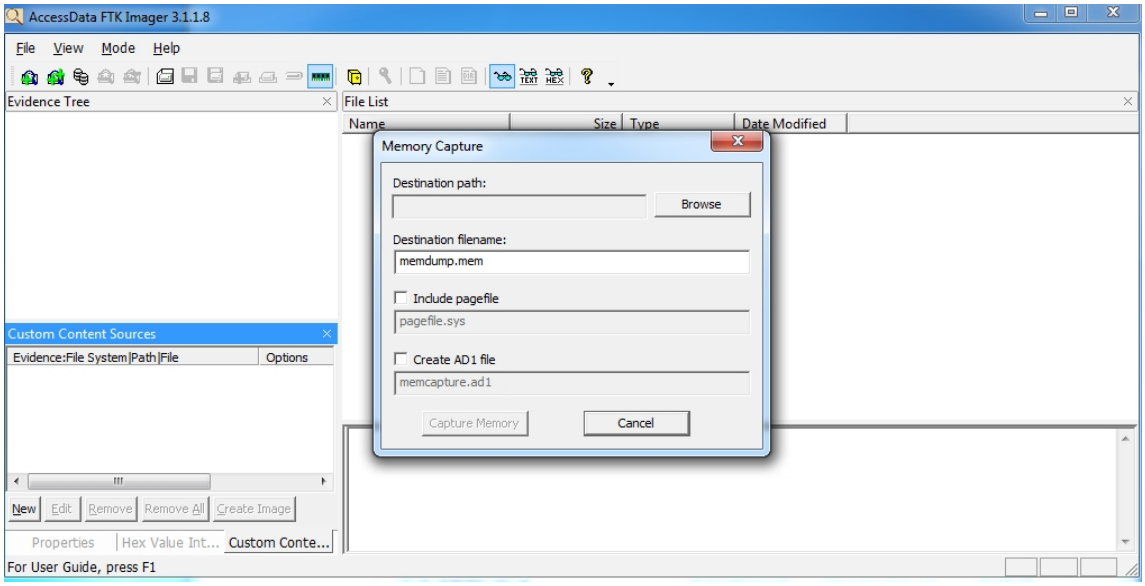


Figura 49-3: FTK imager - memory capture

Realizado por: Luis Lema, 2016

Luego elegir el destino donde se guardará la captura de memoria, el dispositivo de destino debe tener mayor capacidad que el total de memoria RAM a ser capturada.

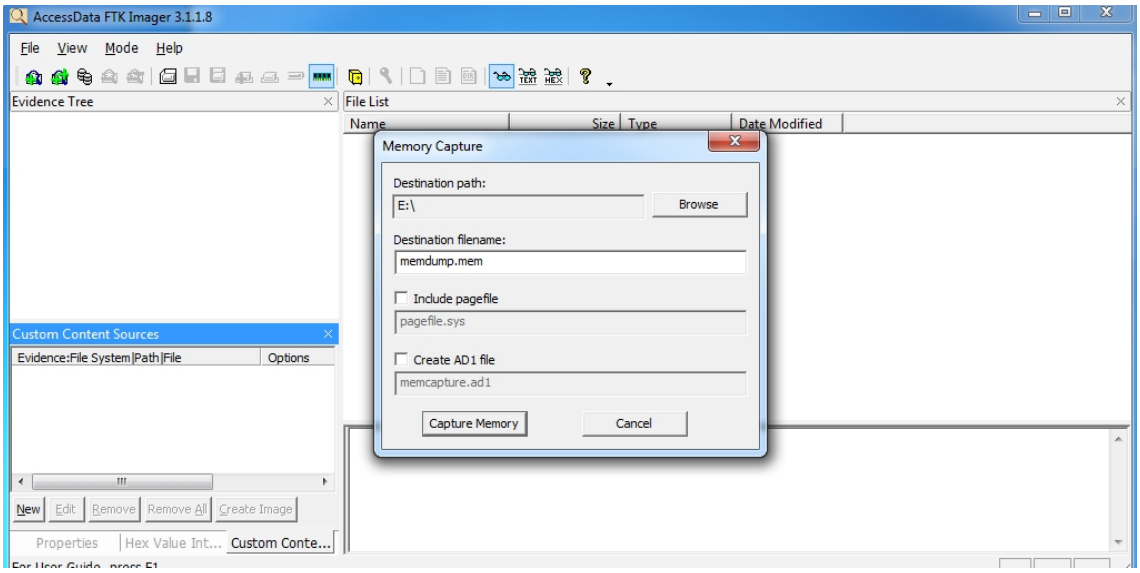


Figura 50-3: FTK Imager – elección de destino

Realizado por: Luis Lema, 2016

Finalmente, dar click en el botón "Capture Memory", y el proceso de copiado bit a bit se llevará a cabo.

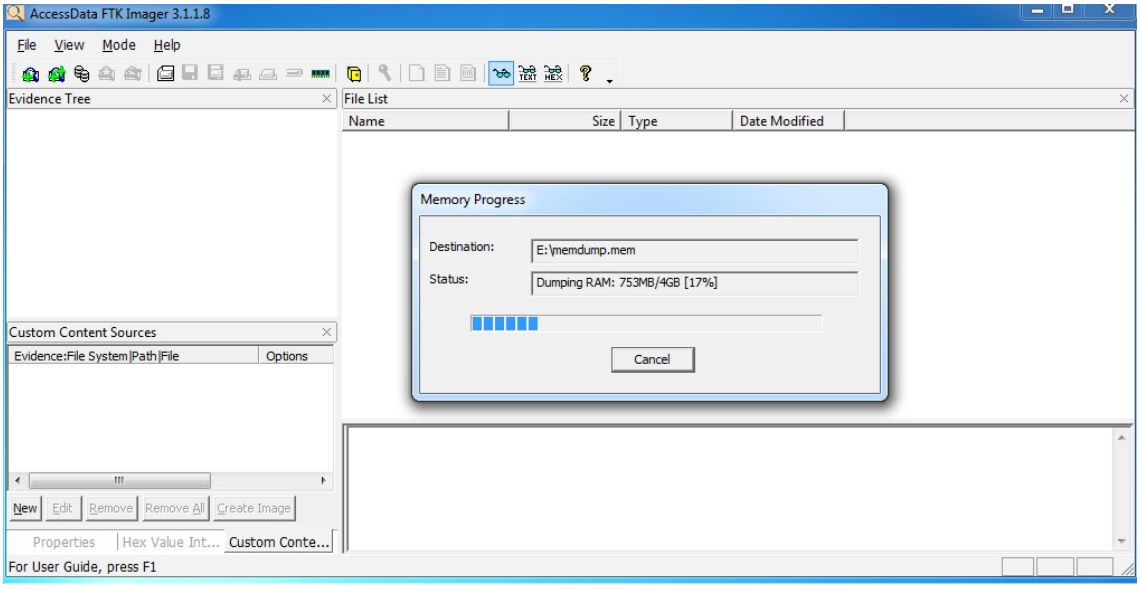


Figura 51-3: FTK imager – copiado de memoria

Realizado por: Luis Lema, 2016

Una vez que se ha terminado de crear el archivo, se puede utilizar la herramienta "HashMyFiles" para calcular el valor hash, esta herramienta tiene la ventaja que calcula varios algoritmos hash entre los que están: MD5, SHA-1, SHA-256, CRC32, etc. "HashMyFiles" está disponible en http://www.nirsoft.net/utils/hash_my_files.html.

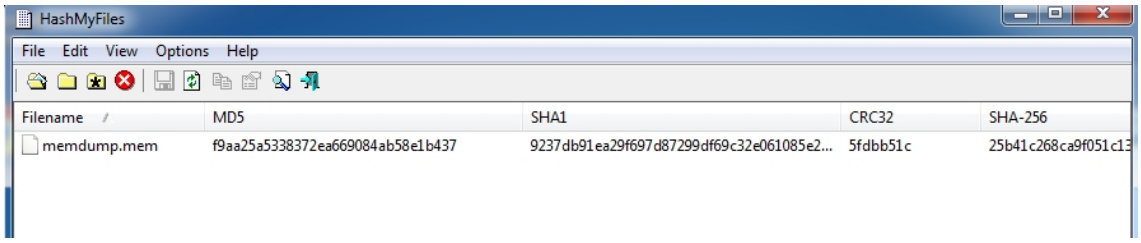


Figura 52-3: HashMyFile – Cálculo valor hash

Realizado por: Luis Lema, 2016

Herramienta Recomendada:

Win–UFO (Ultimate Forensics Outflow), disponible en: http://win-ufo.org/downloads.shtml

Es una herramienta de adquisición de datos en vivo que permite a investigadores forenses adquirir diferentes tipos de información, entre las que destaca:

- Realizar una auditoría a Windows con lo que se obtiene mucha información del sistema operativo.
- Información de Procesos
- Ver historial de Internet
- Búsqueda de palabras clave que se han buscado en Internet
- Recuperación de archivos borrados
- Análisis de malware
- Ver que archivos de video se han visto
- Muchas opciones más

Una ventaja de Win-UFO es que no necesita ser instalada en el sistema que se está investigando, al ser una herramienta portable al momento de correr no realizará cambios al registro del sistema operativo. Además, corre en varias versiones de Windows (XP, Vista, Win7, Win8).

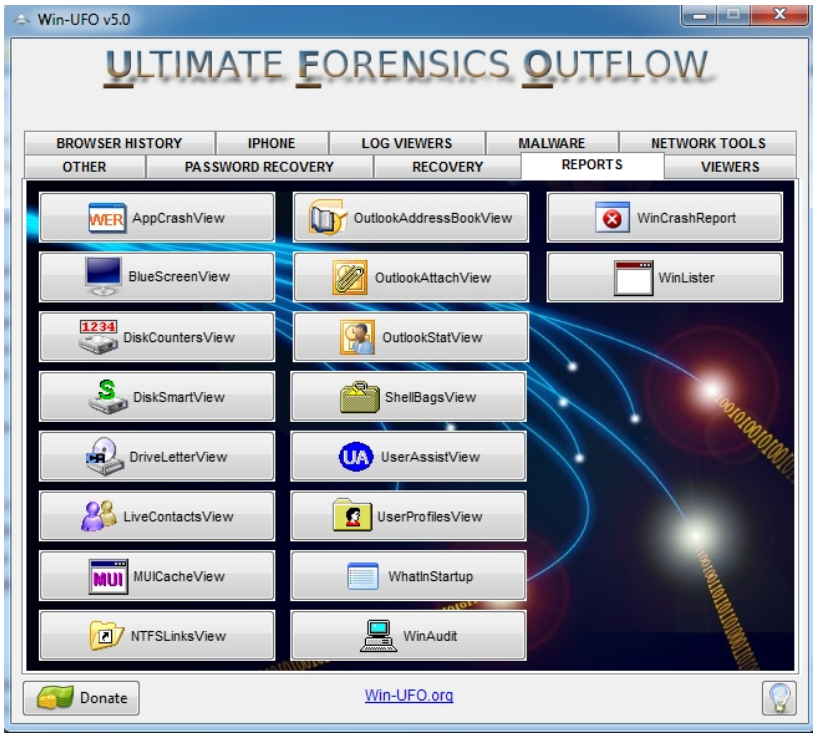


Figura 53-3: Win-UFO

Realizado por: Luis Lema, 2016

EJEMPLO PARA PLATAFORMA LINUX VÍA COMANDOS:

1.- Hora y fecha del sistema

- date

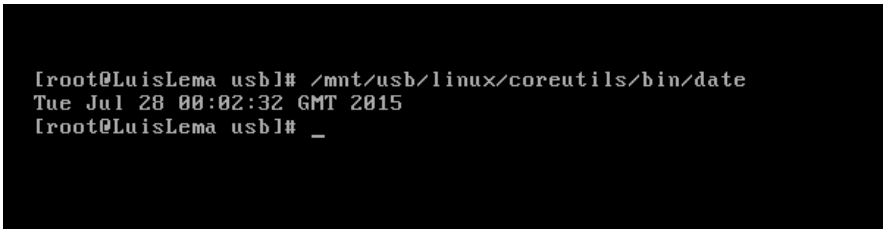


Figura 54-3: Hora y Fecha del Sistema – date

Realizado por: Luis Lema, 2016

2.- Usuarios Logueados

- who
- whoami

```
[root@LuisLema usb]# /mnt/usb/linux/coreutils/bin/who
root     tty1         2015-07-28 06:05
[root@LuisLema usb]# _
```

Figura 55-3: Usuarios Logueados – who

Realizado por: Luis Lema, 2016

```
[root@LuisLema usb]# /mnt/usb/linux/coreutils/bin/whoami
root
[root@LuisLema usb]# _
```

Figura 56-3: Usuarios Logueados – whoami

Realizado por: Luis Lema, 2016

3.- Archivos Abierto

- lsof

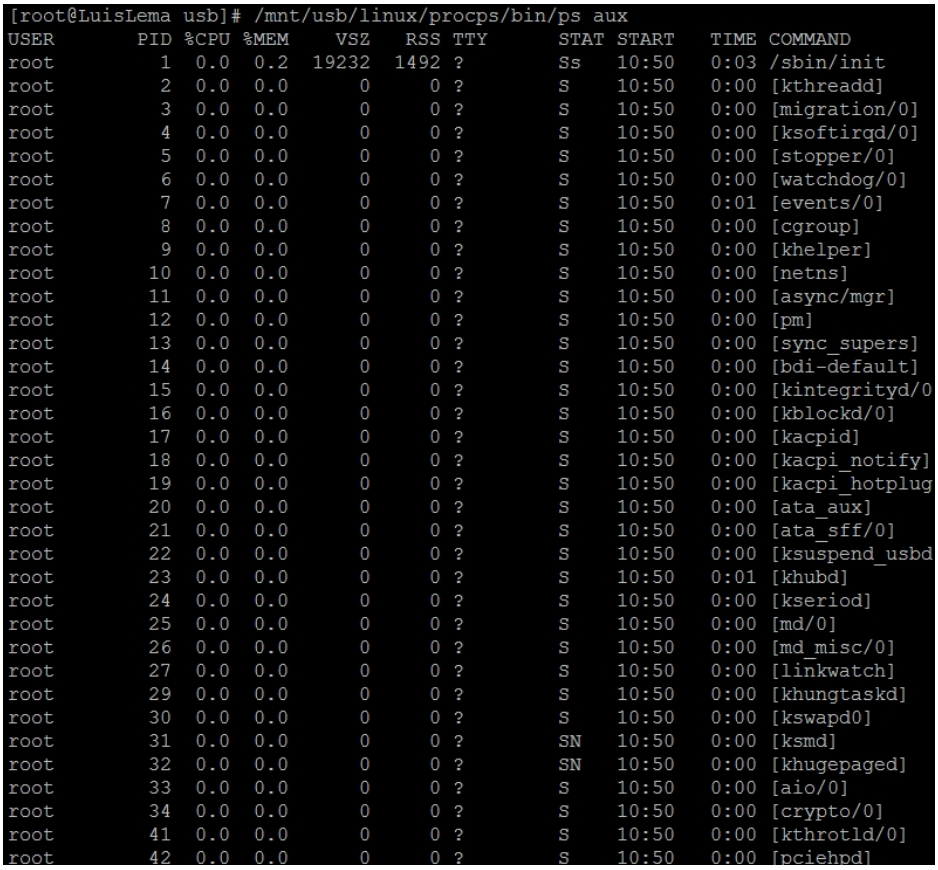
```
[root@LuisLema usb]# /mnt/usb/linux/lsof/usr/bin/lsof
COMMAND    PID  TID     USER   FD   TYPE             DEVICE SIZE/OFF       NODE NAME
init         1          root  cwd    DIR                8,3     4096          2 /
init         1          root  rtd    DIR                8,3     4096          2 /
init         1          root  txt    REG                8,3   150352     132321 /sbin/init
init         1          root  mem    REG                8,3    65928     131031 /lib64/libnss_files-2.12.so
init         1          root  mem    REG                8,3  1921176     131015 /lib64/libc-2.12.so
init         1          root  mem    REG                8,3    90880     128014 /lib64/libgcc_s-4.4.7-20120601.so.1
init         1          root  mem    REG                8,3    43880     131043 /lib64/librt-2.12.so
init         1          root  mem    REG                8,3   142640     131039 /lib64/libpthread-2.12.so
init         1          root  mem    REG                8,3   265728     132051 /lib64/libdbus-1.so.3.4.0
init         1          root  mem    REG                8,3    39896     132317 /lib64/libnih-dbus.so.1.0.0
init         1          root  mem    REG                8,3   101920     132319 /lib64/libnih.so.1.0.0
init         1          root  mem    REG                8,3   154624     131008 /lib64/ld-2.12.so
init         1          root    0u   CHR                1,3      0t0       4165 /dev/null
init         1          root    1u   CHR                1,3      0t0       4165 /dev/null
init         1          root    2u   CHR                1,3      0t0       4165 /dev/null
init         1          root    3r  FIFO                0,8      0t0       7088 pipe
init         1          root    4w  FIFO                0,8      0t0       7088 pipe
init         1          root    5r   DIR               0,10        0          1 inotify
init         1          root    6r   DIR               0,10        0          1 inotify
init         1          root    7u  unix 0xffff88002ecb7400      0t0       7089 socket
kthreadd     2          root  cwd    DIR                8,3     4096          2 /
kthreadd     2          root  rtd    DIR                8,3     4096          2 /
migration    3          root  cwd    DIR                8,3     4096          2 /
migration    3          root  rtd    DIR                8,3     4096          2 /
ksoftirqd    4          root  cwd    DIR                8,3     4096          2 /
ksoftirqd    4          root  rtd    DIR                8,3     4096          2 /
stopper/0    5          root  cwd    DIR                8,3     4096          2 /
stopper/0    5          root  rtd    DIR                8,3     4096          2 /
watchdog/    6          root  cwd    DIR                8,3     4096          2 /
```

Figura 57-3: Archivos abiertos – lsof

Realizado por: Luis Lema, 2016

4.- Información de Procesos

- ps aux



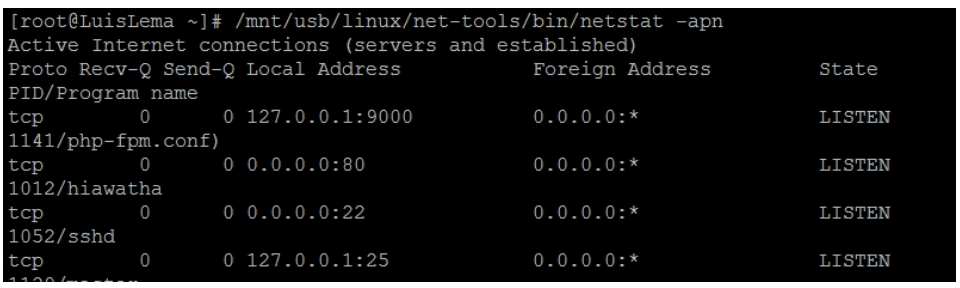
```
[root@LuisLema usb]# /mnt/usb/linux/procps/bin/ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.2  19232  1492 ?        Ss   10:50   0:03 /sbin/init
root         2  0.0  0.0      0     0 ?        S    10:50   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    10:50   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S    10:50   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S    10:50   0:00 [stopper/0]
root         6  0.0  0.0      0     0 ?        S    10:50   0:00 [watchdog/0]
root         7  0.0  0.0      0     0 ?        S    10:50   0:01 [events/0]
root         8  0.0  0.0      0     0 ?        S    10:50   0:00 [cgroup]
root         9  0.0  0.0      0     0 ?        S    10:50   0:00 [khelper]
root        10  0.0  0.0      0     0 ?        S    10:50   0:00 [netns]
root        11  0.0  0.0      0     0 ?        S    10:50   0:00 [async/mgr]
root        12  0.0  0.0      0     0 ?        S    10:50   0:00 [pm]
root        13  0.0  0.0      0     0 ?        S    10:50   0:00 [sync_supers]
root        14  0.0  0.0      0     0 ?        S    10:50   0:00 [bdi-default]
root        15  0.0  0.0      0     0 ?        S    10:50   0:00 [kintegrityd/0
root        16  0.0  0.0      0     0 ?        S    10:50   0:00 [kblockd/0]
root        17  0.0  0.0      0     0 ?        S    10:50   0:00 [kacpid]
root        18  0.0  0.0      0     0 ?        S    10:50   0:00 [kacpi_notify]
root        19  0.0  0.0      0     0 ?        S    10:50   0:00 [kacpi_hotplug
root        20  0.0  0.0      0     0 ?        S    10:50   0:00 [ata_aux]
root        21  0.0  0.0      0     0 ?        S    10:50   0:00 [ata_sff/0]
root        22  0.0  0.0      0     0 ?        S    10:50   0:00 [ksuspend_usbd
root        23  0.0  0.0      0     0 ?        S    10:50   0:01 [khubd]
root        24  0.0  0.0      0     0 ?        S    10:50   0:00 [kseriod]
root        25  0.0  0.0      0     0 ?        S    10:50   0:00 [md/0]
root        26  0.0  0.0      0     0 ?        S    10:50   0:00 [md_misc/0]
root        27  0.0  0.0      0     0 ?        S    10:50   0:00 [linkwatch]
root        29  0.0  0.0      0     0 ?        S    10:50   0:00 [khungtaskd]
root        30  0.0  0.0      0     0 ?        S    10:50   0:00 [kswapd0]
root        31  0.0  0.0      0     0 ?        SN   10:50   0:00 [ksmd]
root        32  0.0  0.0      0     0 ?        SN   10:50   0:00 [khugepaged]
root        33  0.0  0.0      0     0 ?        S    10:50   0:00 [aio/0]
root        34  0.0  0.0      0     0 ?        S    10:50   0:00 [crypto/0]
root        41  0.0  0.0      0     0 ?        S    10:50   0:00 [kthrotld/0]
root        42  0.0  0.0      0     0 ?        S    10:50   0:00 [pciehpd]
```

Figura 58-3: Información Procesos – ps aux

Realizado por: Luis Lema, 2016

5.- Puertos abiertos y aplicación que los está usando

- netstat –apn



```
[root@LuisLema ~]# /mnt/usb/linux/net-tools/bin/netstat -apn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:9000          0.0.0.0:*               LISTEN
1141/php-fpm.conf)
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
1012/hiawatha
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1052/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
```

Figura 59-3: Mapeo de procesos a puertos – netstat -apn

Realizado por: Luis Lema, 2016

6.- Historial de comandos

- history

```
[root@LuisLema ~]# /mnt/usb/linux/coreutils/bin/cat ~/ .bash_history
/mnt/usb/linux/coreutils/bin/cat: /root/: Is a directory
ifconfig
dhclient
ifconfig
clear
ifconfig
yum update
ifconfig
ifconfig
yum update
yum install nano
nano /etc/sysconfig/network-scripts/ifcfg-eth0
nano /etc/sysconfig/selinux
shutdown -r now
echo marica
clear
exit
ifconfig
clear
cp /bin/ls /home/
/home/ls
mount -o remount,noexec /home
/home/ls
nano /etc/fstab
mount -o remount,noexec /home
/home/ls
mount -o remount,noexec /var
/var/ls
clear
mount -o remount /home
```

Figura 60-3: Historial – history

Realizado por: Luis Lema, 2016

7.- Volcado de Memoria

- dd if=/dev/mem of=/usb/linux/memdump.mem

Donde if= origen y of= destino.

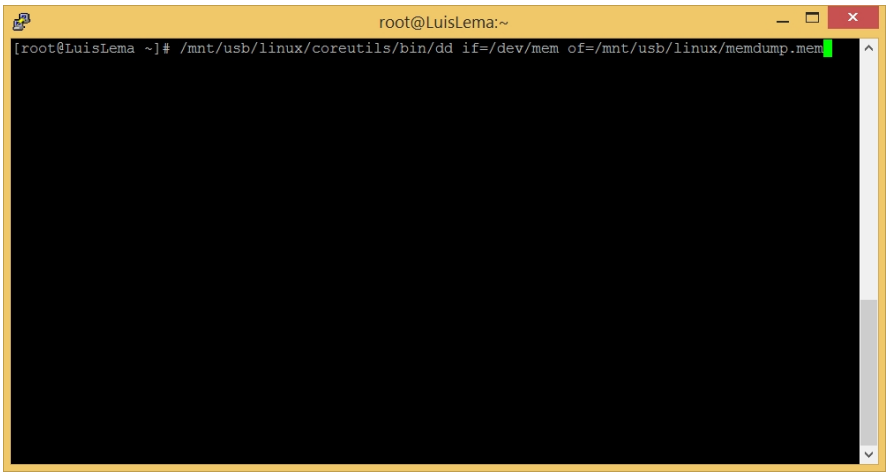


Figura 61-3: memoria – dd

Realizado por: Luis Lema, 2016

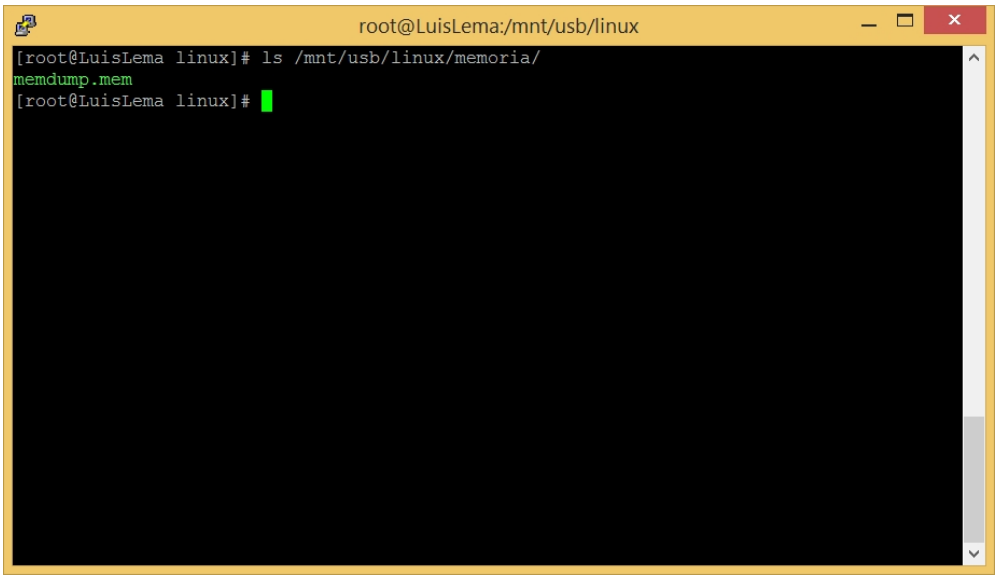


Figura 62-3: memdump.mem – dd

Realizado por: Luis Lema, 2016

Comando Recomendado:

El comando dd, viene incluida en la mayoría de distribuciones Linux, pero de no ser el caso puede ser descargada desde el repositorio de la distribución.

Es una herramienta muy sencilla de utilizar que permite copiar datos, archivos, particiones a bajo nivel.

La sintaxis básica es la siguiente:

- dd if=[origen] of=[destino]
- Para discos SATA: dd if=/dev/sda of=[destino]
- Para discos IDE: dd if=/dev/hda of=[destino]

3.3.6. Acción Número 6

NOMBRE: Adquisición de información no volátil en RAID

PROTOCOLO DE ACTUACIÓN:

Consideraciones previas:

- Identificar el tipo de RAID que está siendo utilizado.
- Cantidad de almacenamiento externo que se necesitará para crear la imagen.
- Tener una herramienta adecuada para crear la imagen de un RAID.
- Para la adquisición de información no volátil utilizar siempre guantes de látex y manilla antiestática.

1.- Conectar al computador comprometido un disco duro USB con software de recuperación.

2.- Arrancar el computador comprometido con el disco duro USB conectado.

3.- Crear una copia del disco duro RAID de la máquina que está siendo analizada en una imagen. Asegurarse que la capacidad de la unidad externa donde se va a crear el nuevo RAID sea mayor o igual al tamaño del disco duro.

4.- Nunca trabajar en el disco duro original. Siempre realizar las pruebas necesarias en la imagen obtenida previamente.

5.- Alterar el sistema lo menos posible.

6.- Crear un informe completo con todos los pasos y acciones seguidas.

EJEMPLO VÍA COMANDOS PARA PLATAFORMAS LINUX:

El primer paso es instalar los paquetes necesarios para la implementación de un RAID en conjunto con LVM, ejecutar el siguiente comando:

- yum install mdadm

Luego se debe instalar y configurar el RAID, para lo que se necesita tener dos discos duros con la misma capacidad. Las particiones de esos discos duros serán de la siguiente manera:

Disco duro 1:

- sda1 para “/”
- sda2 para “Swap”

Disco duro 2:

- sdb1de igual tamaño que sda1
- sdb2 de igual tamaño que sda2

Las particiones pueden ser creadas con fdisk, una vez creadas las particiones solo queda asignar el identificador correspondiente al tipo de partición RAID. Ejecutar el siguiente comando:

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

Donde:
“h” se refiere a un disco duro SATA.
“s” se refiere a un disco duro IDE.
“a” es el primer disco duro del equipo.
“b” es el segundo disco duro del equipo.
“c” es el tercer disco duro del equipo.

En este se usa un disco duro SATA por lo que el comando queda de la siguiente forma:

- fdisk /dev/hdb

Una vez ingresado el comando indicado, la aplicación fdisk se inicia:

Command (m for help):

Al presionar la letra m apare el siguiente menú de opciones:

```
Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help):
```

Figura 63-3: fdisk - m

Realizado por: Luis Lema, 2016

A continuación elegir la opción "t" que es: "Cambiar el id de una partición del sistema", fdisk, preguntara a que partición se desea cambiar el ID, estas particiones serán:

- sdb1
- sdb2

Luego, se debe ingresar el código hexadecimal para particiones RAID, como no se conoce este código en el menú de ayuda ingresar "l" y se mostrará la siguiente lista:

```
Command (m for help): l

 0  Empty           24  NEC DOS         81  Minix / old Lin bf  Solaris
 1  FAT12           39  Plan 9          82  Linux swap / So c1  DRDOS/sec (FAT-
 2  XENIX root      3c  PartitionMagic  83  Linux           c4  DRDOS/sec (FAT-
 3  XENIX usr       40  Venix 80286     84  OS/2 hidden C:  c6  DRDOS/sec (FAT-
 4  FAT16 <32M      41  PPC PReP Boot   85  Linux extended  c7  Syrinx
 5  Extended        42  SFS             86  NTFS volume set da  Non-FS data
 6  FAT16           4d  QNX4.x          87  NTFS volume set db  CP/M / CTOS / .
 7  HPFS/NTFS       4e  QNX4.x 2nd part 88  Linux plaintext de  Dell Utility
 8  AIX             4f  QNX4.x 3rd part 8e  Linux LVM       df  BootIt
 9  AIX bootable    50  OnTrack DM      93  Amoeba          e1  DOS access
 a  OS/2 Boot Manag 51  OnTrack DM6 Aux 94  Amoeba BBT      e3  DOS R/O
 b  W95 FAT32       52  CP/M            9f  BSD/OS          e4  SpeedStor
 c  W95 FAT32 (LBA) 53  OnTrack DM6 Aux a0  IBM Thinkpad hi eb  BeOS fs
 e  W95 FAT16 (LBA) 54  OnTrackDM6      a5  FreeBSD         ee  GPT
 f  W95 Ext'd (LBA) 55  EZ-Drive        a6  OpenBSD         ef  EFI (FAT-12/16/
10  OPUS            56  Golden Bow      a7  NeXTSTEP        f0  Linux/PA-RISC b
11  Hidden FAT12    5c  Priam Edisk     a8  Darwin UFS      f1  SpeedStor
12  Compaq diagnost 61  SpeedStor       a9  NetBSD          f4  SpeedStor
14  Hidden FAT16 <3 63  GNU HURD or Sys ab  Darwin boot     f2  DOS secondary
16  Hidden FAT16    64  Novell Netware  af  HFS / HFS+      fb  VMware VMFS
17  Hidden HPFS/NTF 65  Novell Netware  b7  BSDI fs         fc  VMware VMKCORE
18  AST SmartSleep  70  DiskSecure Mult b8  BSDI swap       fd  Linux raid auto
1b  Hidden W95 FAT3 75  PC/IX           bb  Boot Wizard hid fe  LANstep
1c  Hidden W95 FAT3 80  Old Minix       be  Solaris boot    ff  BBT
1e  Hidden W95 FAT1
```

Figura 64-3: códigos hexadecimales

Realizado por: Luis Lema, 2016

El código para RAID es: “fd Linux raid auto”, ingresar el código y teclear “w” para guardar.

Para crear y asignar el RAID ejecutar los siguientes comandos:

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

Donde:

“create /dev/md0”, es el nombre del RAID que se está creando.
“level=1”, es el tipo de RAID que se está creando en este caso RAID 1.
“raid-disks=2”, es el número de dispositivos que forman el RAID.
“/dev/sda /dev/sdb”, es lista de dispositivos que forma parte del RAID.

Estos RAID se están creando en modo degradado, por lo que se solo se deben añadir al RAID los discos que se han formateado, por lo que las entradas que corresponden al disco /dev/sda se deja en missing El siguiente paso será darles formato a las particiones RAID, ejecutar el siguiente comando:

- mkfs.ext3 /dev/md0
- mkswap /dev/md1

Una vez hecho esto se debe modificar e fichero: mdadm.conf ejecutando el siguiente comando:

- mdadm --examine –scan

Este comando devuelve información sobre el RAID que se está creando, se deben 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...

A continuación se deben crear los puntos de montaje donde irán las particiones del RAID, ejecutar los siguientes comandos:

- mkdir /mnt/md0
- mkdir /mnt/md1

Montar las particiones RAID ejecutando los siguientes comandos:

- mount /dev/md0 /mnt/md0
- mount /dev/md1 /mnt/md1

Para que las particiones del RAID se monten como "/" y "swap" se debe modificar el archivo de configuración "/etc/fstab", sustituyendo lo siguiente:

- /dev/sda1 / ext3 defaults,errors=remount-ro 0 1
- /dev/sda2 none swap sw 0 0

Por las siguientes líneas:

- /dev/md0 / ext3 defaults,errors=remount-ro 0 1
- /dev/md1 none swap sw 0 0

De igual manera modificar el archivo "/etc/mtab" sustiyendo "/dev/sda1" por "/dev/md0".

El siguiente paso es modificar el grub del sistema operativo para que arranque desde la paritción RAID, el fichero es: "/boot/grub/menu.lst"

Se deben reemplazar las siguientes líneas:

- 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

Por las siguientes líneas:

- 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

También aumentar la siguiente línea:

- 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

Una vez actualizado el fichero, se debe actualizar el ramdisk mediante el siguiente comando:

- update-initramfs –u

Lo siguiente es copiar los archivos de "/" a la nueva partición desde la que se va arrancar, ejecutar el siguiente comando:

- cp -dpRx / /mnt/md0

Además de todos los pasos antes descritos se debe activar el grub en los dos discos duros, mediante los comandos:

- grub
- grub> root (hd1,0) grub> setup (hd1)
- grub> root (hd0,0) grub> setup (hd0) exit

Reiniciar el equipo el cual ya debe arrancar desde el RAID, ejecutar:

- df –h

Ahora el sistema ha arrancado desde el segundo disco duro se debe 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 se hizo con /dev/sdb1 y /dev/sdb2, se deberá hacer con /dev/sda1 y /dev/sda2. Luego de haber hecho el paso anterior añadir las particiones del disco duro 1 al RAID.

- mdadm --add /dev/md0 /dev/sda1
- mdadm --add /dev/md1 /dev/sda2

Revisar el fichero /proc/mdstat para ver que el RAID se esté sincronizando, esperar hasta que finalice:

- more /proc/mdstat

Una vez sincronizado modificar el fichero "/etc/mdadm.conf", primero ejecutar el comando:

- mdadm --examine –scan

Se deben eliminar las lineas que se añadieron anteriormente y sustituirlas por las que devuelve ahora la ejecución del comando anteriormente ejecutado.

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

Modificar de nuevo el grub para que la entrada que apunta a /dev/sda1 apunte a /dev/md0 en el disco (hd0,0). Para hacerlo abrir el fichero /boot/grub/menu.lst y cambiar 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:

- 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/vmlinuz-2.6.24-17-generic root=/dev/md0 ro quiet splash initrd /boot/initrd.img-2.6.24-17-generic quiet

Así, el sistema arrancara por defecto desde el disco hd1 y en el caso de que este disco falle se debe añadir fallback debajo de default en el fichero /boot/grub/menu.lst para que arranque desde el segundo disco duro.

- default 0 fallback 1

Actualizar nuevamente el ramdisk mediante el comando:

- update-initramfs –u

Por último reiniciar el equipo.

Finalmente, comprobar que el RAID funcionando simulando el fallo de uno de los discos ejecutando los siguientes comandos:

- mdadm --manage /dev/md0 --fail /dev/sdb1
- mdadm --manage /dev/md0 --remove /dev/sdb1

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

Comando/Herramienta Recomendado:

El conjunto de herramientas mdadm, está disponible en: https://www.kernel.org/pub/linux/utils/raid/mdadm/.

Este conjunto de herramientas mdadm (Multiple Device ADMinistrator), permite la administración de discos duros RAID a través de software. (Alcance Libre, 2013)

Entre las principales características están:

- Es una solución de muy bajo costo ya que no necesita costosos dispositivos de hardware.
- Configuración basada sobre el núcleo del sistema.
- Permite portar de manera transparente los arreglos entre sistemas GNU/Linux sin necesidad de reconstruir éstos.
- Aprovecha de mejor manera los recursos del sistema.
- Soporte hot-swap.
- Detecta automáticamente el número de núcleos del microprocesador para así aprovechar mejor los recursos del sistema. (Alcance Libre, 2013)

Soporta los siguientes tipos de arreglos RAID: RAID 0, RAID 1, RAID 4, RAID 5, RAID 6, RAID 10.

Si por algún motivo no viene instalado en el sistema operativo se instala de la siguiente manera:

```
yum -y install mdadm
```

Figura 65-3: Instalación de mdadm

Fuente: www.alcancelibre.org/staticpages/index.php/como-mdadm

NOTA: Al momento de realizar este trabajo no se encontraron herramientas forenses gratuitas de manejo para RAID en Windows.

3.3.7. Acción Número 7

NOMBRE: Adquisición remota de información no volátil

PROTOCOLO DE ACTUACIÓN:

Consideraciones previas:

- Conectar la máquina del investigador a la red donde se encuentra conectada la máquina sospechosa.
- Para la adquisición de información no volátil utilizar siempre guantes de látex y manilla antiestática.

1.- Calcular el valor hash del disco duro comprometido. Se recomienda no utilizar el algoritmo MD5 ya que no es seguro, en su lugar se puede usar SHA1, SHA-256, CRC32, etc.

2.- Crear una copia remota bit a bit (imagen) del disco duro de la máquina que está siendo analizada en una unidad de almacenamiento externa o el computador del investigador. Asegurarse que la capacidad de la unidad externa sea mayor al tamaño del disco duro.

3.- Calcular el valor hash de la imagen de disco duro resultante.

4.- Comparar el valor hash del disco duro original con el de la imagen resultante. Deben ser iguales.

5.- Nunca trabajar en el disco duro original. Siempre realizar las pruebas necesarias en la imagen obtenida previamente.

6.- Alterar el sistema lo menos posible.

7.- Crear un informe completo con todos los pasos y acciones seguidas.

EJEMPLO VÍA COMANDOS Y HERRAMIENTAS PARA PLATAFORMAS WINDOWS

Herramientas para la adquisición remota de información no volátil:

- Net use, disponible en el mismo Sistema Operativo.
- Robocopy, disponible en: https://www.microsoft.com/en-us/download/details.aspx?id=17657
- HashMyFiles, disponible en: http://www.nirsoft.net/utils/hash_my_files.html

Ejemplo vía comandos y herramientas:

Para este ejemplo se realizará la copia de un archivo que posiblemente contiene evidencia y está almacenado en una máquina con Windows 7, el proceso para copiar el disco duro entero es el mismo solamente cambia el origen en la sintaxis del comando robocopy.

El primer paso es identificar el origen de donde se copiaran los archivos en el equipo objetivo de la cual se va a realizar la copia:

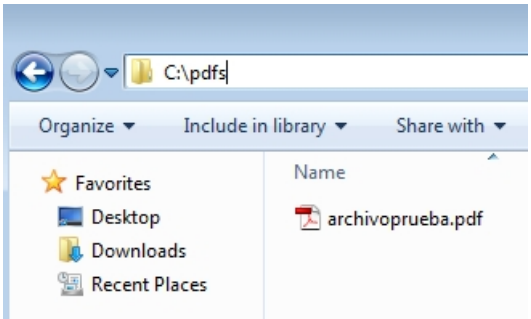


Figura 66-3: Archivo a ser copiado

Realizado por: Luis Lema, 2016

El siguiente paso es calcular el valor hash del archivo a ser copiado, se utilizará la herramienta hashmyfile que está disponible en http://www.nirsoft.net/:

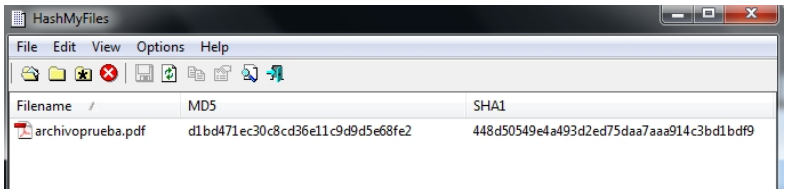


Figura 67-3: Hashmyfile origen

Realizado por: Luis Lema, 2016

En la máquina del investigador crear una carpeta compartida y dar los permisos necesarios de escritura y lectura:

- Para este ejemplo se creará una carpeta llamada "evidencia" en el disco duro D:

Figura 68-3: Carpeta compartida - evidencia

Realizado por: Luis Lema, 2016

Desde la máquina que está siendo investigada abrir una consola de comandos y escribir los siguientes comandos:

- Net use \\ip_maquina_investigador\IPC$ /u:nombre_de_usuario contraseña
- robocopy C:\archivoprueba \\ip_maquina_investigador /e

Donde net use se usa para autenticarse en la máquina del investigador, robocopy "C:\" es el origen de donde se va a copiar, D:\evidencia es el destino donde se almacenara la copia y /e es la opción que permite copiar todos los archivos desde el origen.

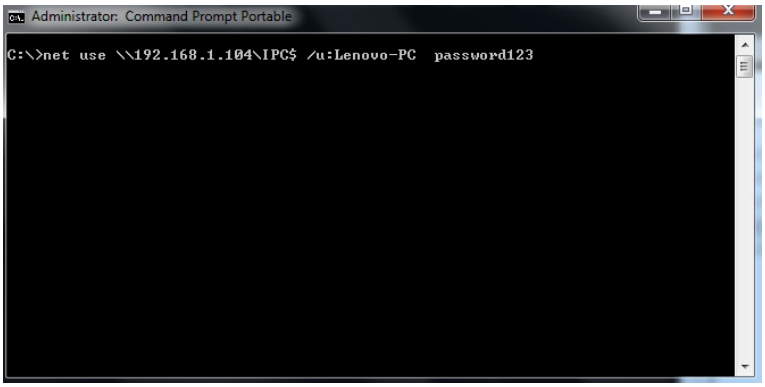


Figura 69-3: net use

Realizado por: Luis Lema, 2016

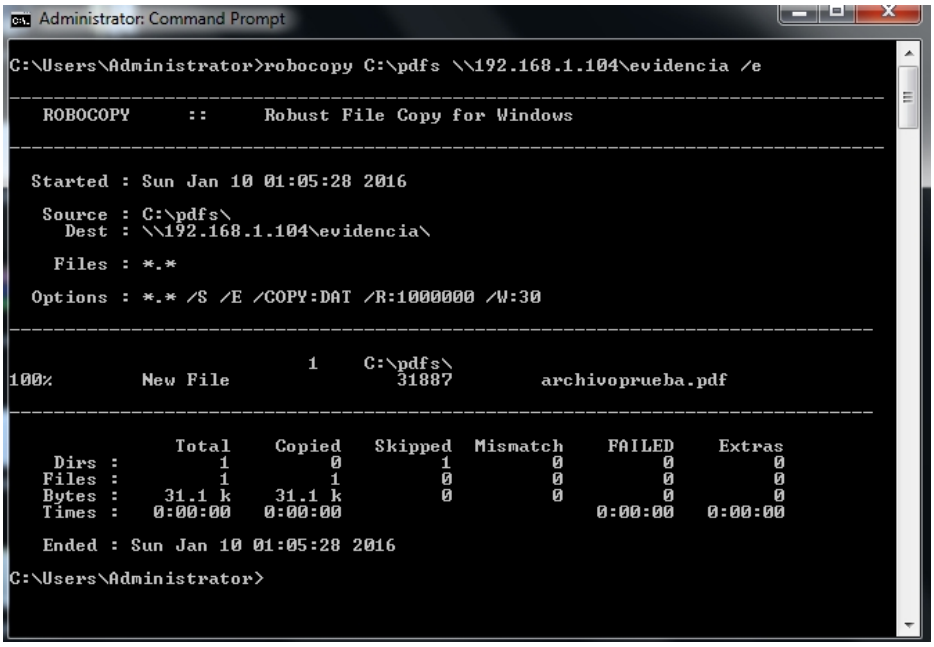


Figura 70-3: Uso de robocopy

Realizado por: Luis Lema, 2016

En la máquina del investigador comprobar que esté copiado el archivo:

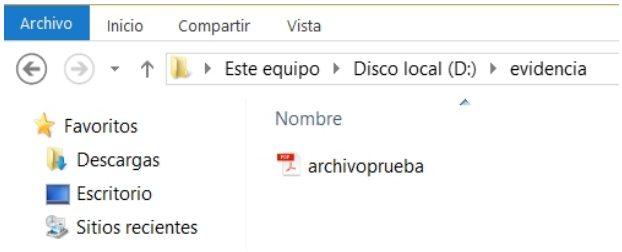


Figura 71-3: archivo copiado - robocopy

Realizado por: Luis Lema, 2016

Finalmente calcular el valor hash del archivo copiado y comparar que sea el mismo valor que el del original:

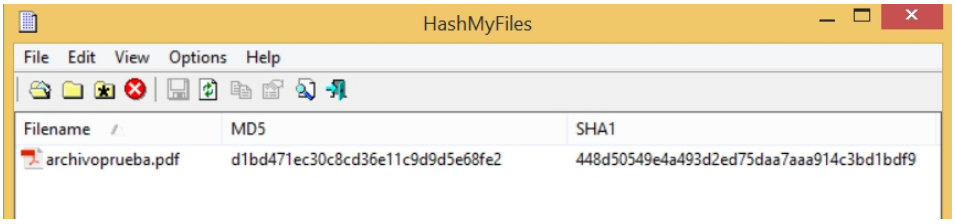


Figura 72-3: Hashmyfile - destino

Realizado por: Luis Lema, 2016

Herramienta Recomendada:

La herramienta robocopy, viene incluida en el sistema operativo Windows o se puede descargar desde: https://www.microsoft.com/en-us/download/details.aspx?id=17657

Es una herramienta/comando que se encuentra disponible en la línea de comandos, y que permite copiar archivos, carpetas o directorios en un computador local o en una red. Entre las ventajas del uso de robocopy están:

- Tolera interrupciones en la copia de archivos.
- Realiza reintentos automáticos si no se logra acceder al archivo que se está copiando.
- Permite copiado de grandes cantidades de archivos.
- Copia correctamente toda la información del archivo.

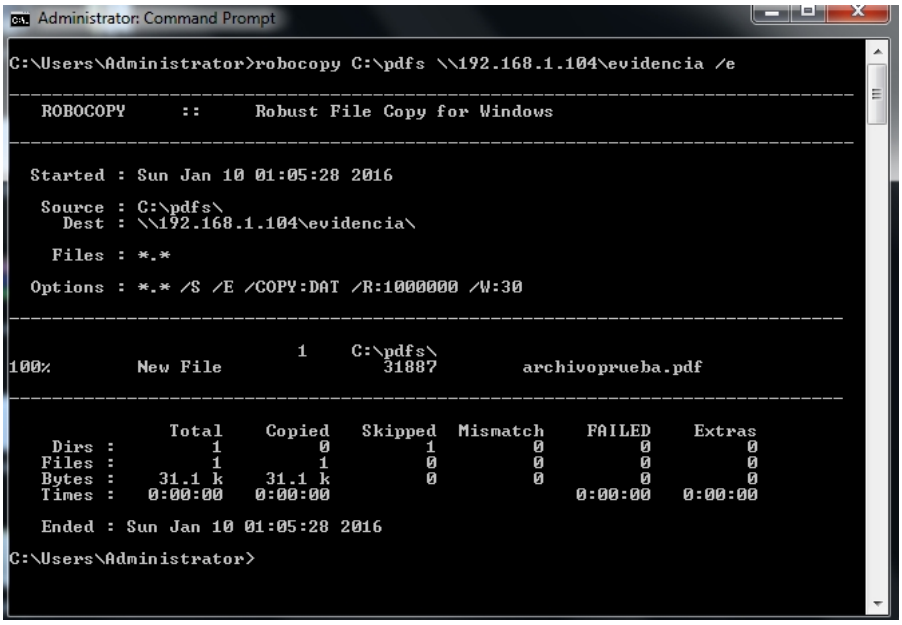


Figura 73-3: robocopy

Realizado por: Luis Lema, 2016

EJEMPLO VÍA COMANDOS Y HERRAMIENTAS PARA PLATAFORMAS LINUX:

Herramientas para la adquisición remota de información no volátil:

- netcat, viene incluida en la mayoría de distribuciones Linux, pero de no ser el caso está disponible en:: http://netcat.sourceforge.net/download.php
- kali linux (máquina invetigador), disponible en: https://www.kali.org/downloads/
- dd, viene incluida en las distribuciones Linux.
- sha1sum, viene incluida en las distribuciones Linux.

Ejemplo vía comandos y herramientas:

El primer paso es observar las características del disco duro del que se va a crear la imagen en la máquina objetivo, utilizar el comando:

- fdisk –l

En este caso se va a realizar la imagen de un disco duro SATA, ya que como se puede ver la nomenclatura es /dev/sda.

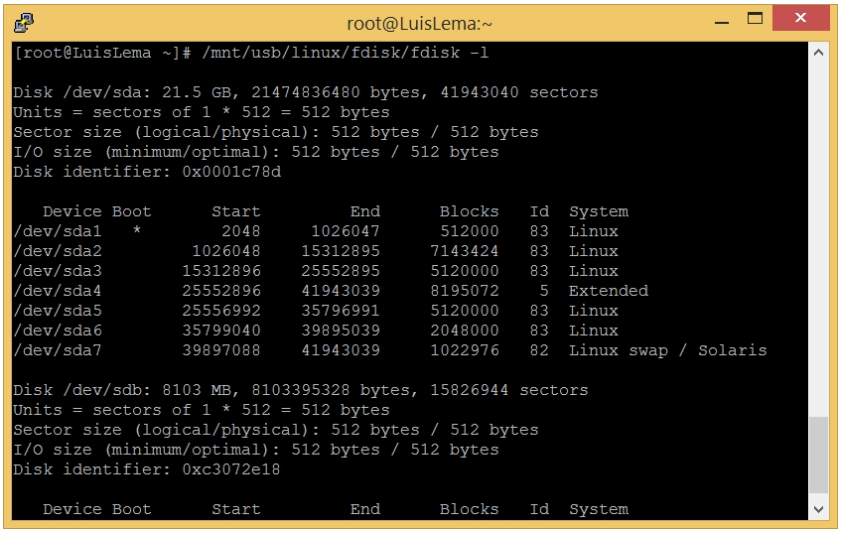


Figura 74-3: remoto- fdisk –l

Realizado por: Luis Lema, 2016

Calcular el valor hash del disco duro comprometido con los siguientes comandos en las máquinas objetivo y la del investigador y guardarlo en un archivo:

Máquina investigador:

- netcat –l –p 1234 > Desktop/hashdisco.txt

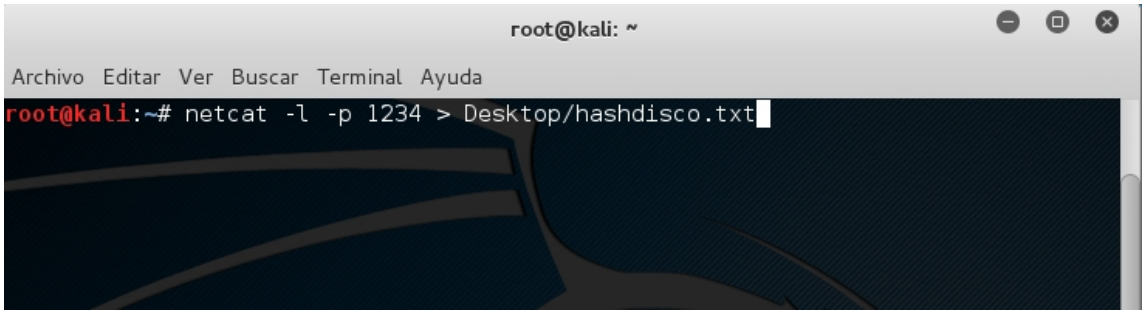


Figura 75-3: remoto – netcat y hash - investigador

Realizado por: Luis Lema, 2016

Máquina objetivo:

- Si se trata de un disco duro SATA: sha1sum /dev/sda | nc ip_maquina_investigador 1234
- Si se trata de un disco duro IDE: sha1sum /dev/hda > hashdisco.txt | nc ip_maquina_investigador 1234

Para este ejemplo se realizará la copia de la partición /dev/sda1, ya que realizar la copia de todo el disco duro lleva demasiado tiempo.

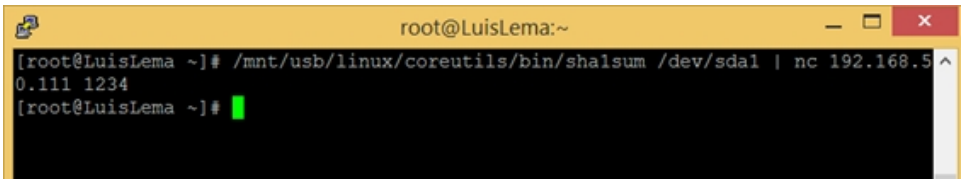


Figura 76-3: remoto – netcat y hash - objetivo

Realizado por: Luis Lema, 2016

Para ver el valor hash calculado, se debe ingresar el siguiente comando en la máquina del investigador:

- cat Desktop/hashdisco.txt

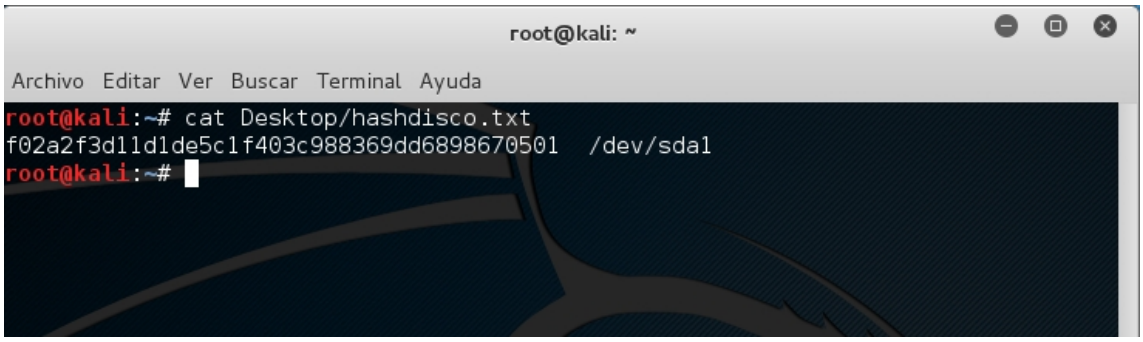


Figura 77-3: remoto – cat hashdisco - investigador

Realizado por: Luis Lema, 2016

Crear la imagen forense del disco duro con los comandos "dd" y "netcat":

Máquina investigador:

- netcat –l –p 1234 > Desktop/imgdisco.img

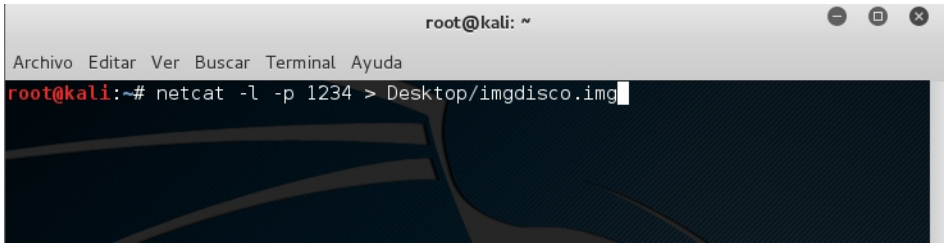


Figura 78-3: remoto – netcat imgdisco - investigador

Realizado por: Luis Lema, 2016

Máquina objetivo:

- Si se trata de un disco duro SATA: dd if=/dev/sda | nc ip_maquina_investigador 1234

- Si se trata de un disco duro IDE: dd if=/dev/hda | nc ip_maquina_investigador 1234

Como en este caso se hace la imagen de una partición lógica se debe reemplazar "sda" por "sda1".

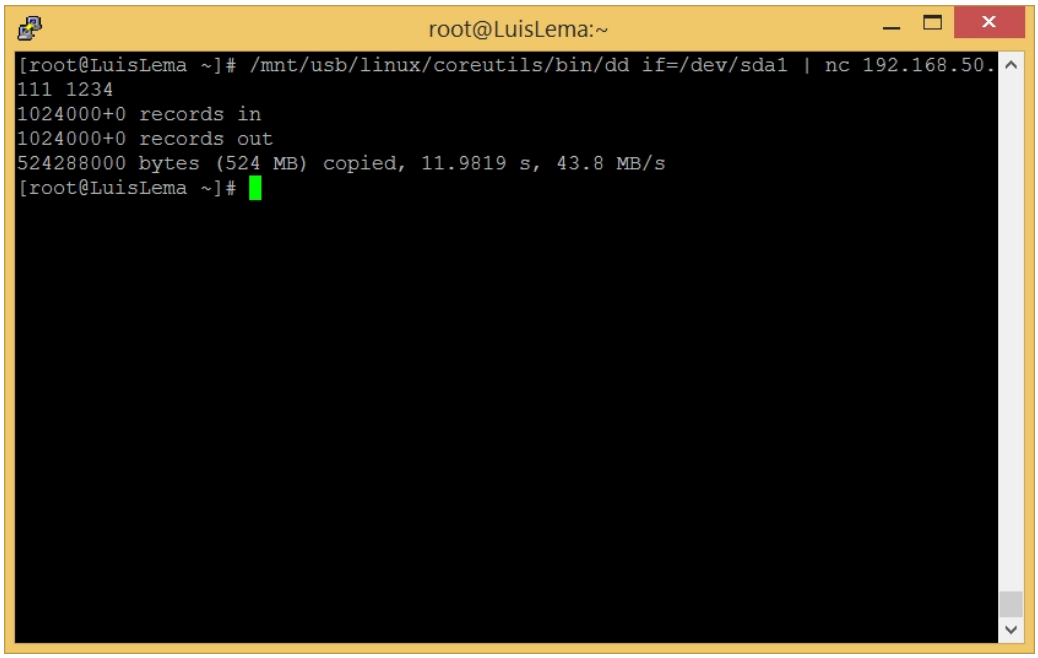


Figura 79-3: remoto – Creación imagen disco - objetivo

Realizado por: Luis Lema, 2016

En la siguiente imagen se puede ver como en la máquina del investigador se encuentran guardados los archivos de hashdisco.txt e imgdisco.img en el Escritorio.

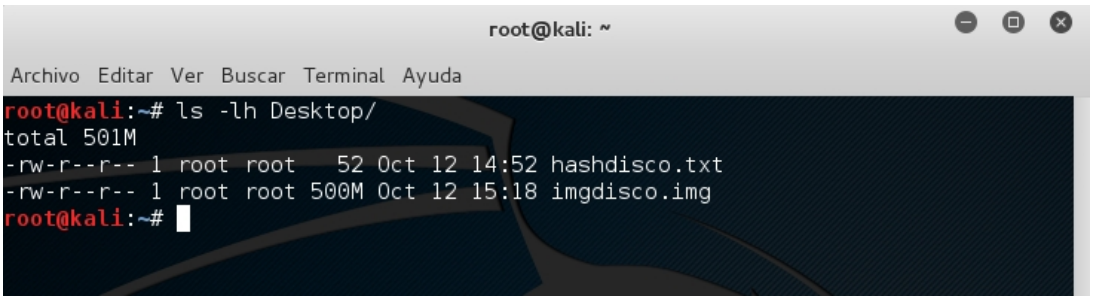


Figura 80-3: remoto – Archivos escritorio - investigador

Realizado por: Luis Lema, 2016

A continuación se debe calcular el valor hash de la imagen obtenida. Usar el siguiente comando y guardarlo en un archivo:

Máquina investigador:

- sha1sum Desktop /imgdisco.img > Desktop/hashimg.txt

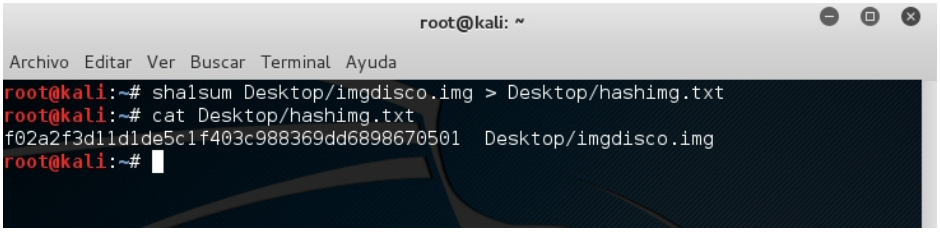


Figura 81-3: remoto – Calculo hash imagen - investigador

Realizado por: Luis Lema, 2016

Finalmente se debe compara el hash de la unidad original con el hash de la imagen, estos valores deben ser iguales.

Máquina investigador:

- cat Desktop/hashdisco.txt ; cat Desktop/hashimg.txt

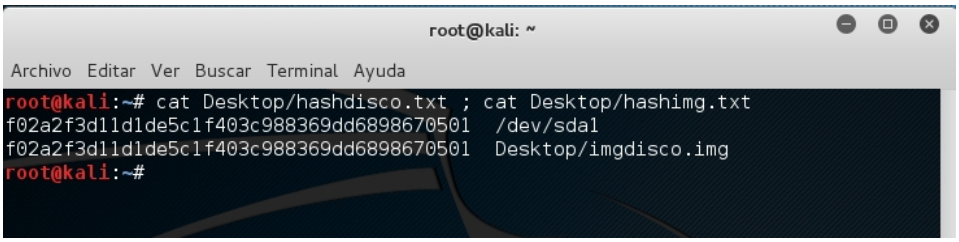


Figura 82-3: remoto – Comparación valores hash - investigador

Realizado por: Luis Lema, 2016

Herramienta Recomendada:

netcat, viene incluida en la mayoría de distribuciones Linux, pero de no ser el caso puede ser descargada desde: http://netcat.sourceforge.net/download.php

Es una herramienta de red que permite la lectura y escritura de datos a través de una conexión de red, utilizando del protocolo TCP/IP.

Entre las principales características de netcat están:

- Conexiones de entrada y salida de red por TCP o UDP desde y hacia cualquier puerto.

- Es de fácil uso.

- Tiene varios parámetros por lo que es una herramienta potente.

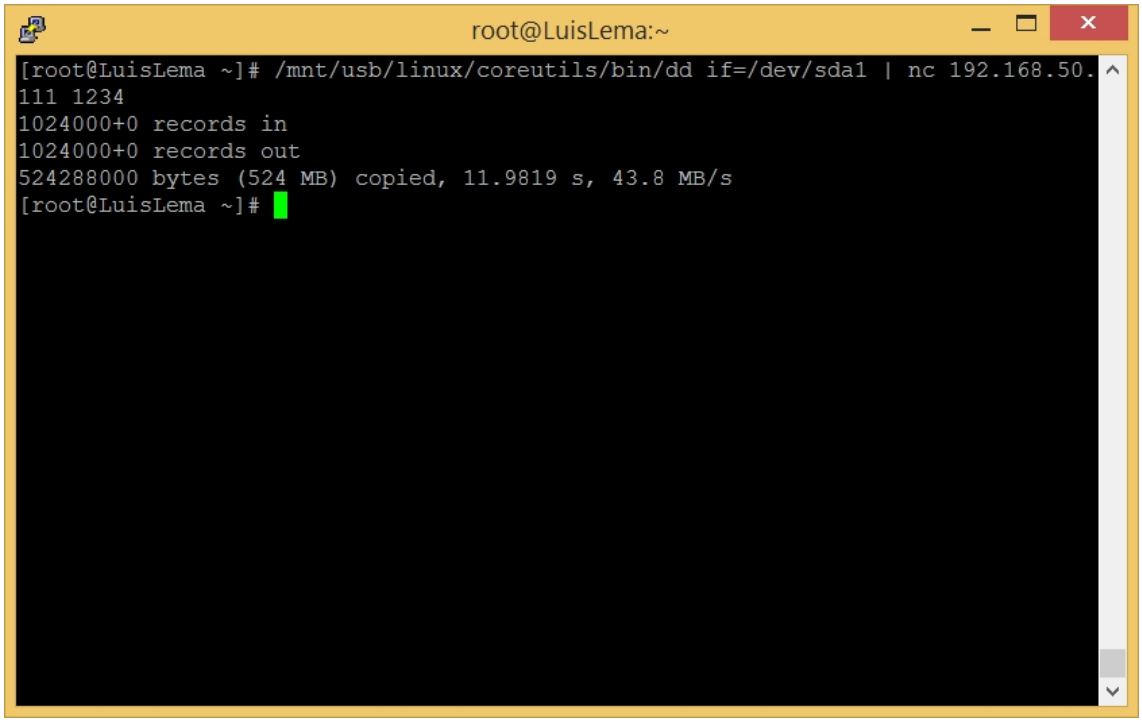


Figura 83-3: netcat

Realizado por: Luis Lema, 2016

3.3.8. Acción Número 8

NOMBRE: Adquisición de información no volátil

PROTOCOLO DE ACTUACIÓN:

Nota: Para la adquisición de información no volátil utilizar siempre guantes de látex y manilla antiestática.

1.- Calcular el valor hash del disco duro comprometido. Se recomienda no utilizar el algoritmo MD5 ya que no es seguro, en su lugar se puede usar SHA1, SHA-256, CRC32, etc.

2.- Crear una copia bit a bit (imagen) del disco duro de la máquina que está siendo analizada en una unidad de almacenamiento externa. Asegurarse que la capacidad de la unidad externa sea mayor al tamaño del disco duro.

3.- Calcular el valor hash de la imagen de disco duro resultante.

4.- Comparar el valor hash del disco duro original con el de la imagen resultante. Deben ser iguales.

5.- Nunca trabajar en el disco duro original. Siempre realizar las pruebas necesarias en la imagen obtenida previamente.

6.- Alterar el sistema lo menos posible.

7.- Crear un informe completo con todos los pasos y acciones seguidas.

EJEMPLO VÍA HERRAMIENTAS DE SOFTWARE PARA LA ADQUISICIÓN DE INFORMACIÓN NO VOLÁTIL:

Herramientas para la adquisición de información no Volátil:

- FTK imager, disponible en: http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1

- HashMyFiles, disponible en: http://www.nirsoft.net/utils/hash_my_files.html

Ejemplo:

Para crear la imagen del disco duro se va a utilizar la herramienta FTK imager.

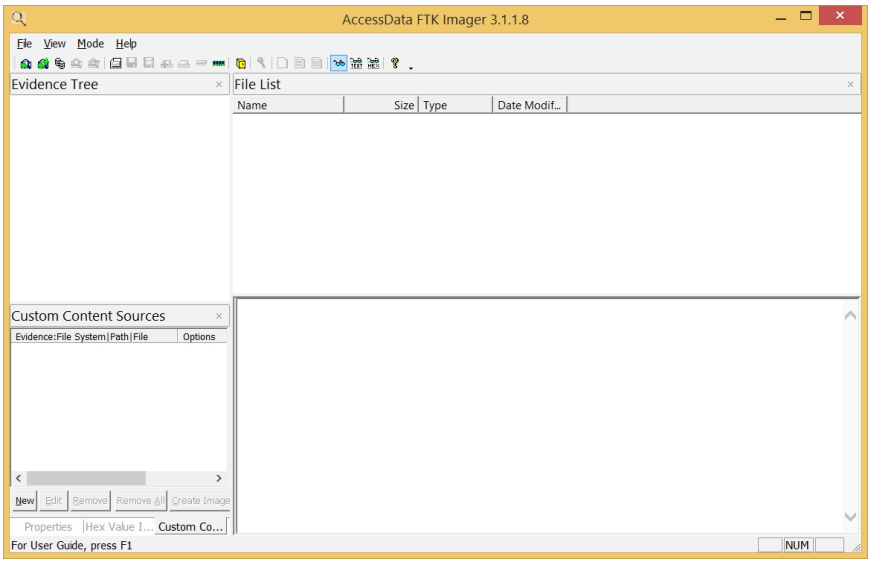


Figura 84-3: FTK imager – Ventana Principal

Realizado por: Luis Lema, 2016

Dar click en la pestaña "File" y elegir la opción "Create disk image".

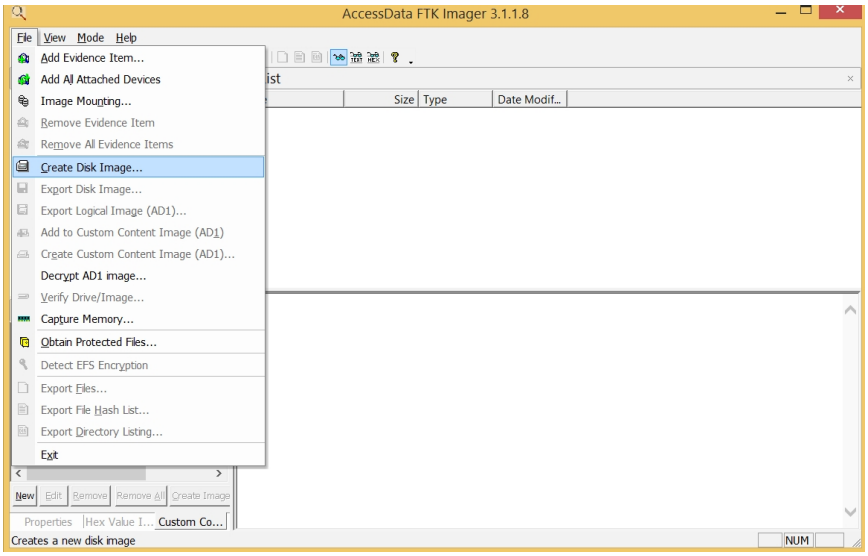


Figura 85-3: FTK imager – Create disk image

Realizado por: Luis Lema, 2016

En la ventana que aparece se debe escoger la opción de "Physical Drive", ya que se va a realizar la imagen de toda una unidad física que puede ser un Disco Duro o un USB, etc. Si se desea hacer una imagen de una partición se debería elegir "Logical Drive", luego dar click a siguiente.

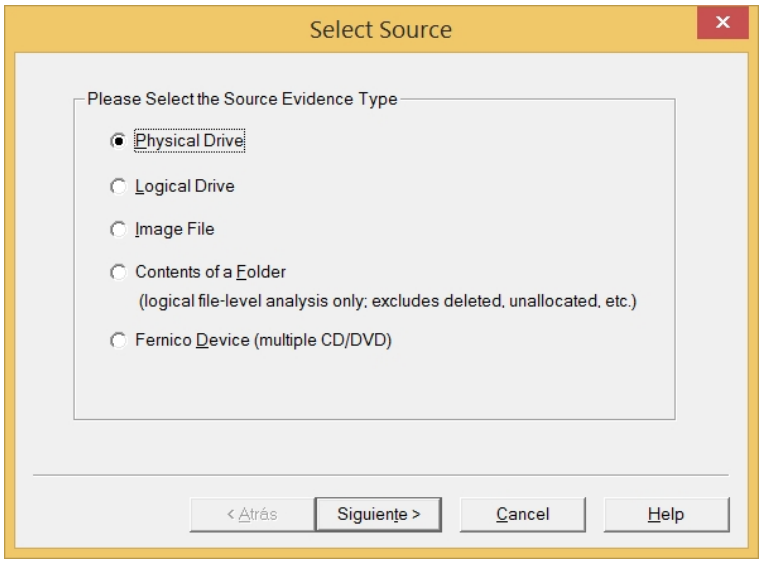


Figura 86-3: FTK imager – Physical Drive

Realizado por: Luis Lema, 2016

En el menú desplegable que se muestra en esta ventana se debe elegir la unidad física de la que se va a realizar la imagen, puede ser el disco duro entero pero para esta demostración será una unidad USB de 8GB.

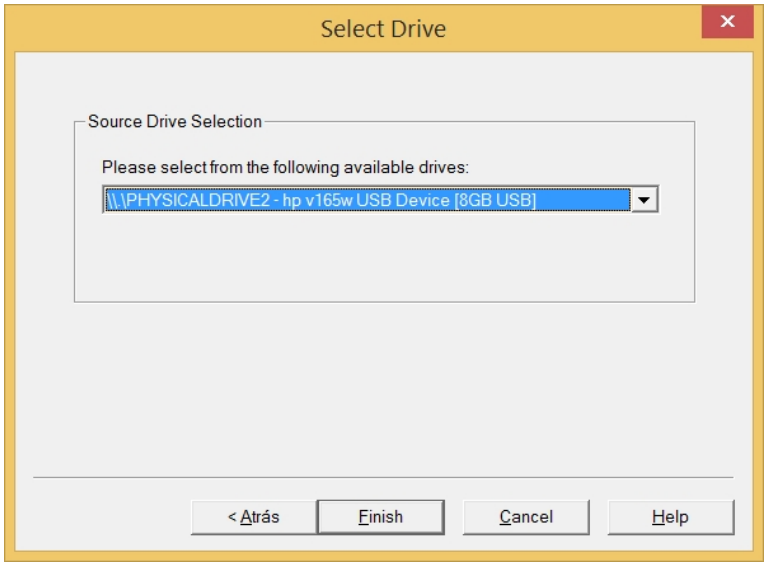


Figura 87-3: FTK imager – Select Drive

Realizado por: Luis Lema, 2016

A continuación se debe elegir el destino donde se almacenará la imagen que se va a crear dando click al botón "Add". Tener en cuenta que la casilla de "Verify images after they are created" este marcada, ya que esta opción permitirá que se realice el cálculo de valores hash de la unidad origen y la imagen resultante.

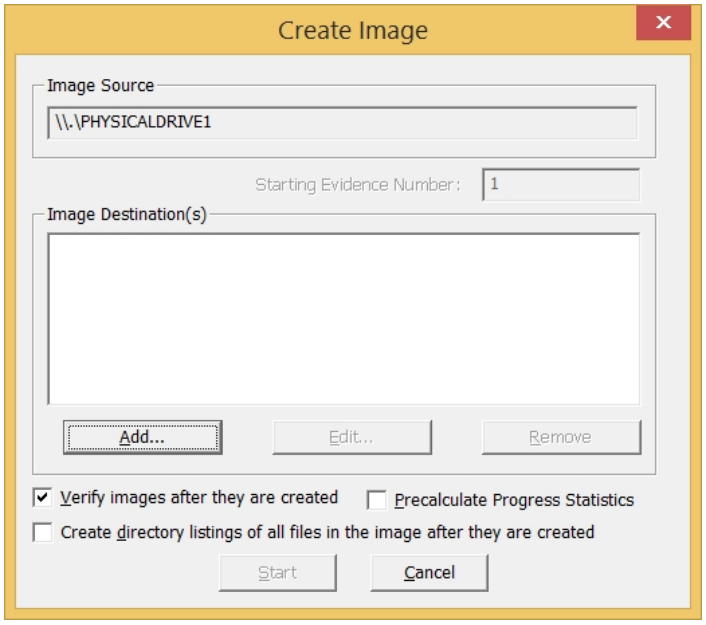


Figura 88-3: FTK imager – Add

Realizado por: Luis Lema, 2016

Se debe seleccionar el tipo de imagen que se va a crear, seleccionar la opción "Raw (dd)", luego dar click a siguiente.

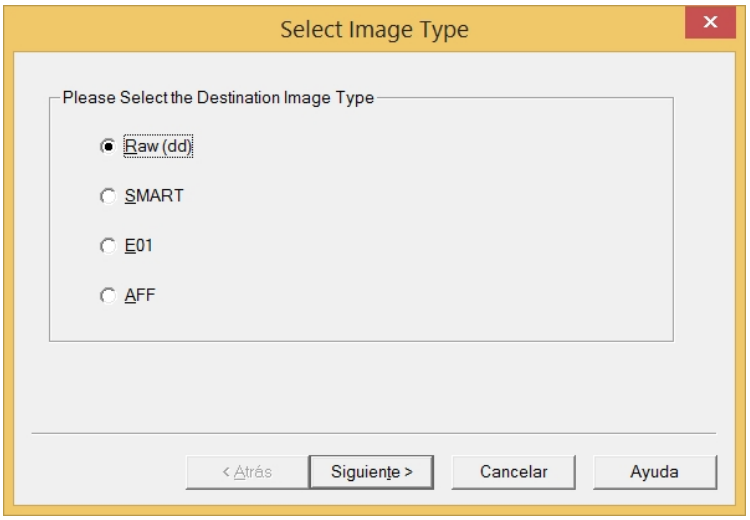


Figura 89-3: FTK imager – Select Image Type

Realizado por: Luis Lema, 2016

En esta ventana se debe ingresar información sobre el caso que se está investigando. Dar click a siguiente.

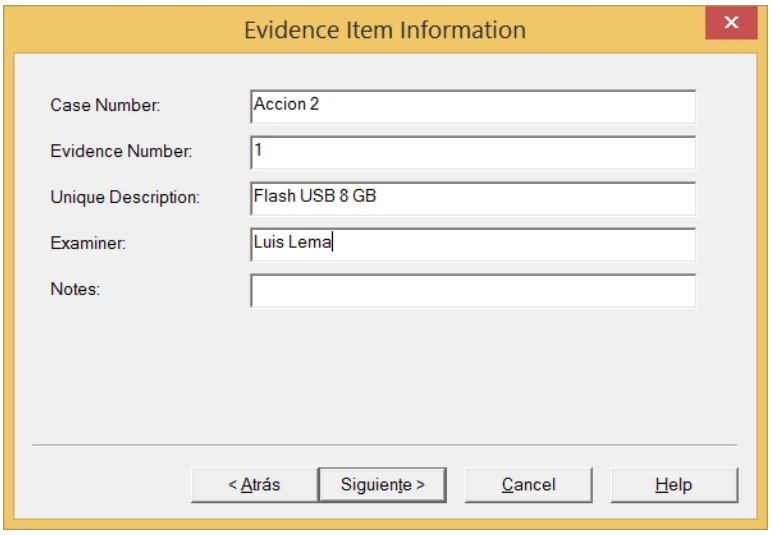


Figura 90-3: FTK imager – Evidence Item Infomation

Realizado por: Luis Lema, 2016

Es necesario escoger el destino de la imagen a crear, se puede ingresar la ruta manualmente o elegir dando click en el botón "Browse", también se debe da un nombre a la imagen, y algo muy importante es decidir si fragmentar o no, para este ejemplo no se va a fragmentar por lo que en "Image Fragment Size" se debe poner 0, caso contrario se debe poner el tamaño en megas del fragmento de la imagen. Dar click en el botón "Finish".

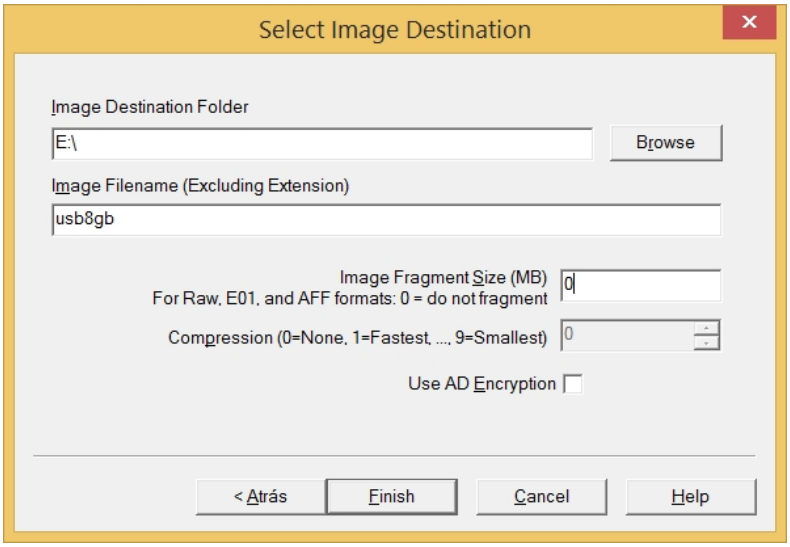


Figura 91-3: FTK imager – Image Destination

Realizado por: Luis Lema, 2016

Para iniciar con la creación de la imagen dar click en "Start".

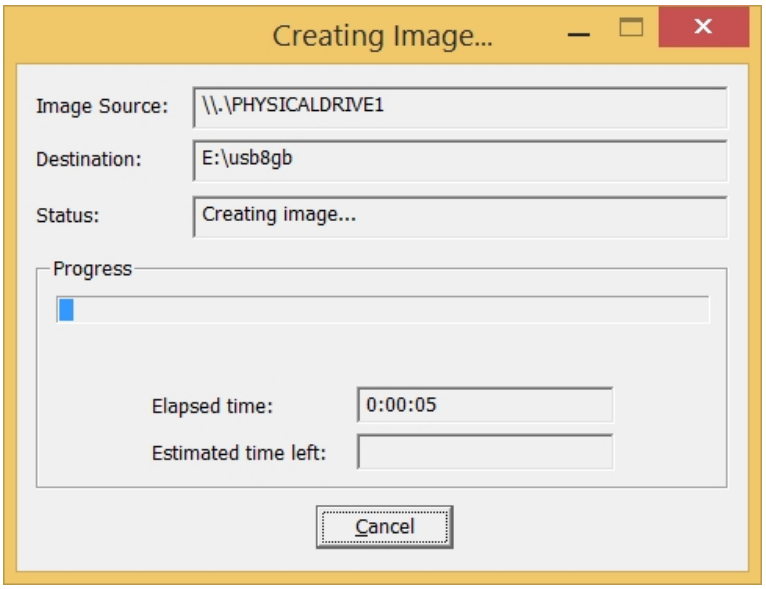


Figura 92-3: FTK imager – Creating Image

Realizado por: Luis Lema, 2016

Al terminar la creación de la imagen empieza el proceso de verificación:

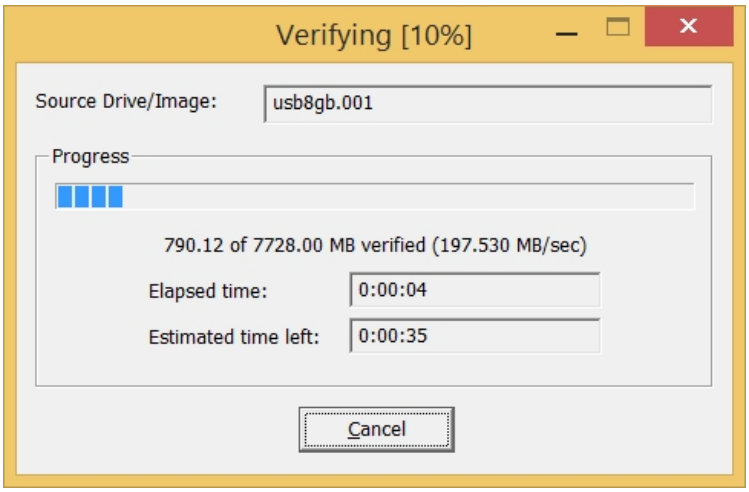


Figura 93-3: FTK imager – Verifying

Realizado por: Luis Lema, 2016

Finalmente se muestra los resultados de la verificación, si la creación de la imagen fue exitosa los valores hash calculados por FTK imager serán los mismos y tendrán la palabra "Match", además indicará que no se han hallado sectores malos.

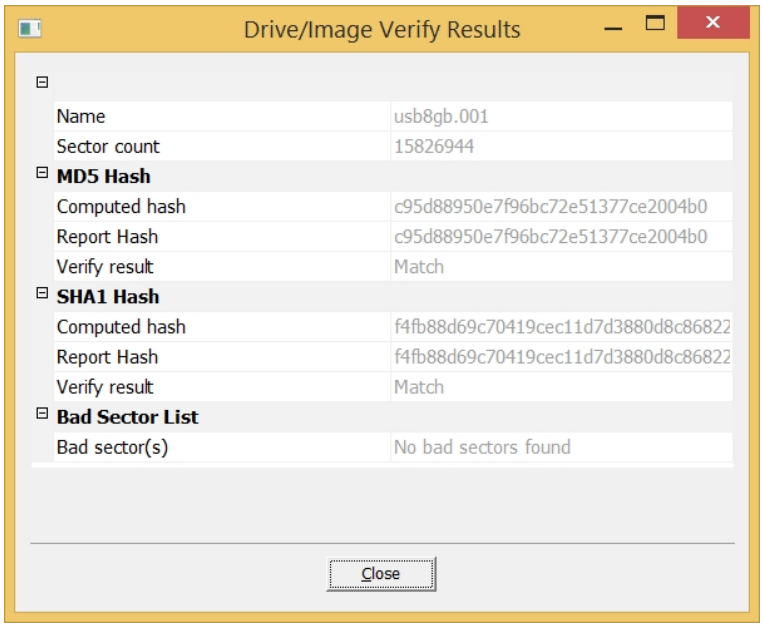


Figura 94-3: FTK imager – Verify Results

Realizado por: Luis Lema, 2016

Herramienta Recomendada:

FTK imager , disponible en: http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1

Es una herramienta forense que permite crear imágenes de diferentes tipos de discos duros para luego ser analizados, entre las principales características de esta herramienta gratuita están:

- Creación de imágenes forenses de discos duros, CD rooms, DVDs, carpetas o incluso archivos individuales.

- Permite montar una imagen para observar la unidad original.

- Crear diferentes tipos de funciones hash.

- Volcado de memoria RAM entre otras. Para más información visitar la página del fabricante: http://accessdata.com/.

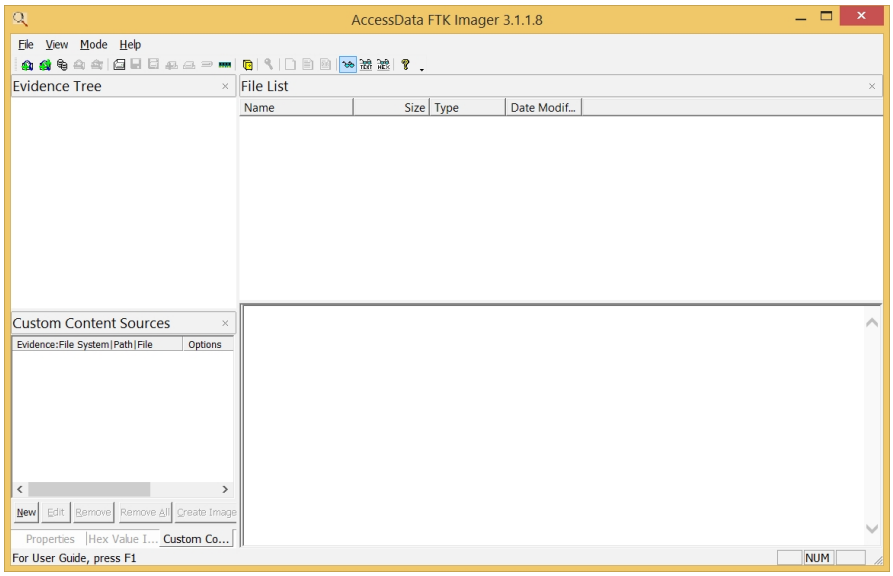


Figura 95-3: FTK imager

Realizado por: Luis Lema, 2016

EJEMPLO VÍA COMANDOS PARA LA ADQUISICIÓN DE INFORMACIÓN NO VOLÁTIL:

Comandos para la adquisición de información no volátil:

- dd, viene incluida en la mayoría de distribuciones Linux, pero de no ser el caso puede ser descargada desde el repositorio de la distribución.

- dcfldd, disponible en: http://dcfldd.sourceforge.net/#download

- sha1sum, viene incluida en la mayoría de distribuciones Linux, pero de no ser el caso puede ser descargada desde el repositorio de la distribución.

Ejemplo:

El primer paso es observar las características del disco duro del que se va a crear la imagen, utilizar el comando:

- fdisk –l

En este caso se va a realizar la imagen de un disco duro SATA, ya que como se puede ver la nomenclatura es /dev/sda.

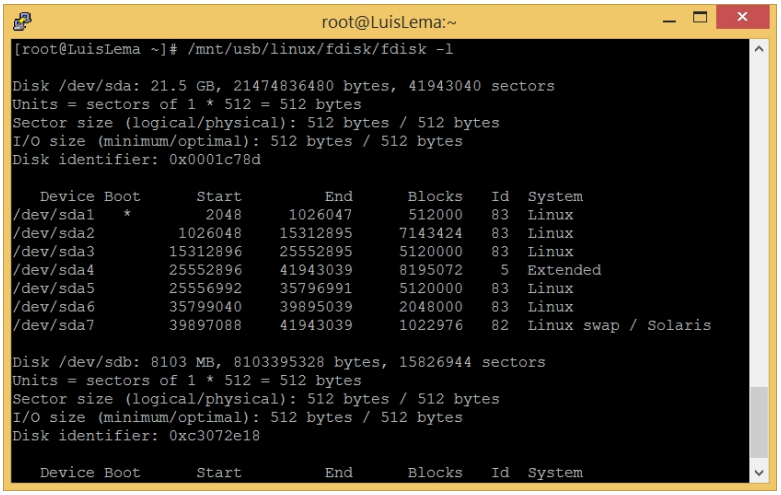


Figura 96-3: fdisk –l

Realizado por: Luis Lema, 2016

Calcular el valor hash del disco duro comprometido con los siguientes comandos y guardarlo en un archivo:

- Si se trata de un disco duro SATA: sha1sum /dev/sda > hashdisco.txt
- Si se trata de un disco duro IDE: sha1sum /dev/hda > hashdisco.txt

Para este ejemplo se realizará la copia de la partición /dev/sda1, ya que realizar la copia de todo el disco duro lleva demasiado tiempo.

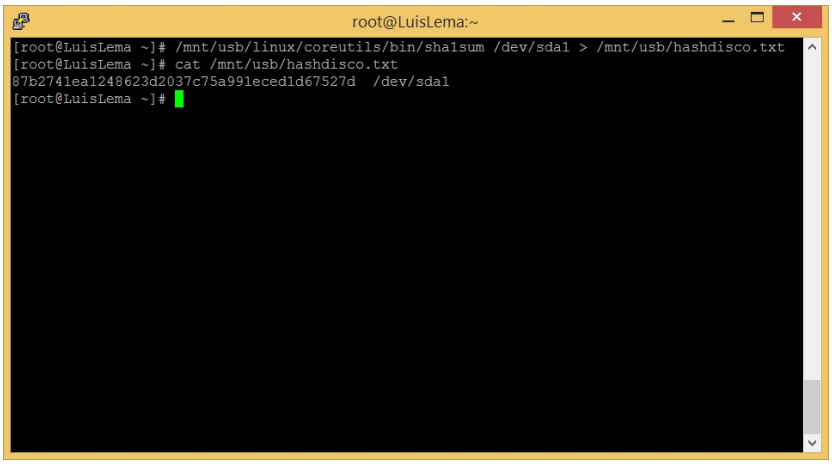


Figura 97-3: Cálculo hash – sha1sum

Realizado por: Luis Lema, 2016

Crear la imagen forense del disco duro con el comando “dd”:

- Si se trata de un disco duro SATA: dd if=/dev/sda of=/evidencia/imgdisco.img
- Si se trata de un disco duro IDE: dd if=/dev/hda of=/evidencia/imgdisco.img

Como en este caso se hace la imagen de una partición lógica se debe reemplazar “sda” por “sda1”.

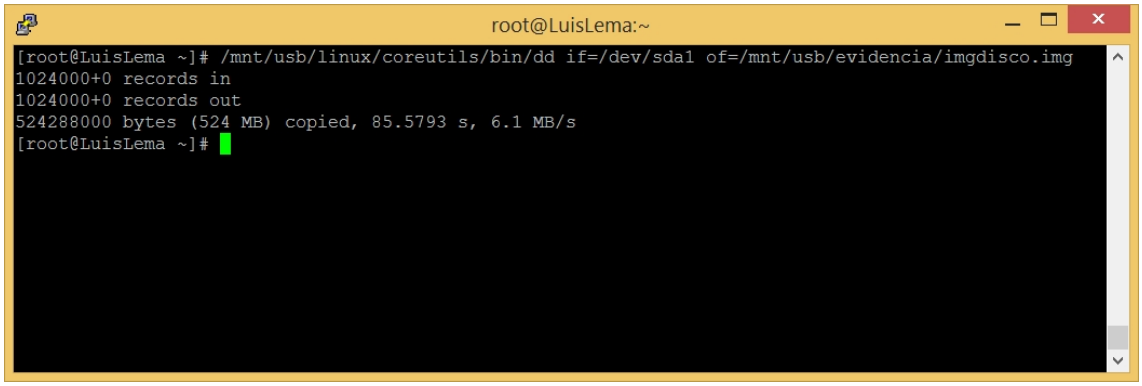


Figura 98-3: Creación imagen disco - dd

Realizado por: Luis Lema, 2016

A continuación, se debe calcular el valor hash de la imagen obtenida. Usar el siguiente comando y guardarlo en un archivo:

- sha1sum /evidencia/imgdisco.img > /evidencia/hashimg.txt

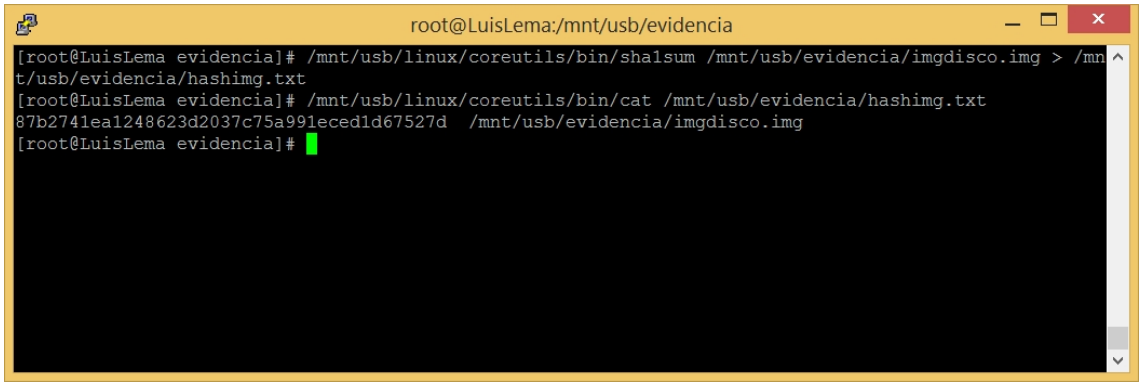


Figura 99-3: Cálculo hash imagen – sha1sum

Realizado por: Luis Lema, 2016

Finalmente se debe comparar el hash de la unidad original con el hash de la imagen, estos valores deben ser iguales.

- cat hashdisco.txt ; cat /evidencia/hashimg.txt

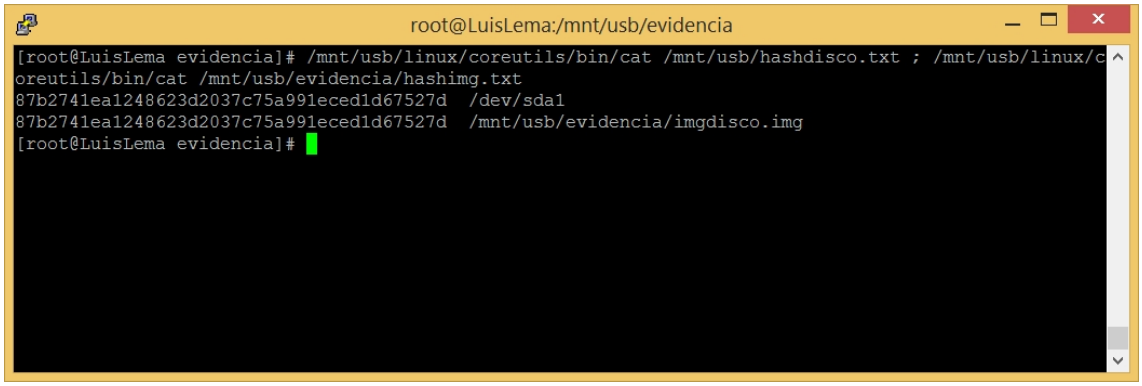


Figura 100-3: Comparación valores hash – cat

Realizado por: Luis Lema, 2016

Comando Recomendado:

dd, viene incluida en la mayoría de distribuciones Linux, pero de no ser el caso puede ser descargada desde el repositorio de la distribución.

Es una herramienta muy sencilla de utilizar que permite copiar datos, archivos, particiones a bajo nivel.

La sintaxis básica es la siguiente:

- dd if=[origen] of=[destino]
- Para discos SATA: dd if=/dev/sda of=[destino]
- Para discos IDE: dd if=/dev/hda of=[destino]

3.3.9. Acción Número 9

NOMBRE: Adquisición de información no volátil en Discos RAID con computador apagado.

Nota: Este protocolo es el mismo de la acción número 6, por lo que los pasos a seguir y el ejemplo son el mismo. Trabajar con discos duros RAID es un caso especial por esa razón todo el proceso es el mismo en las dos acciones.

PROTOCOLO DE ACTUACIÓN:

Consideraciones previas:

- Identificar el tipo de RAID que está siendo utilizado.
- Cantidad de almacenamiento externo que se necesitará para crear la imagen.
- Tener una herramienta adecuada para crear la imagen de un RAID.
- Para la adquisición de información no volátil utilizar siempre guantes de látex y manilla antiestática.

1.- Conectar al computador comprometido un disco duro USB con software de recuperación.

2.- Arrancar el computador comprometido con el disco duro USB conectado.

3.- Crear una copia del disco duro RAID de la máquina que está siendo analizada en una imagen. Asegurarse que la capacidad de la unidad externa donde se va a crear el nuevo RAID sea mayor o igual al tamaño del disco duro.

4.- Nunca trabajar en el disco duro original. Siempre realizar las pruebas necesarias en la imagen obtenida previamente.

5.- Alterar el sistema lo menos posible.

6.- Crear un informe completo con todos los pasos y acciones seguidas.

EJEMPLO VÍA COMANDOS PARA PLATAFORMAS LINUX:

El primer paso es instalar los paquetes necesarios para la implementación de un RAID en conjunto con LVM, ejecutar el siguiente comando:

- yum install mdadm

Luego se debe instalar y configurar el RAID, para lo que se necesita tener dos discos duros con la misma capacidad. Las particiones de esos discos duros serán de la siguiente manera:

Disco duro 1:

- sda1 para "/"
- sda2 para "Swap"

Disco duro 2:

- sdb1de igual tamaño que sda1
- sdb2 de igual tamaño que sda2

Las particiones pueden ser creadas con fdisk, una vez creadas las particiones solo queda asignar el identificador correspondiente al tipo de partición RAID. Ejecutar el siguiente comando:

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

Donde:
"h" se refiere a un disco duro SATA.
"s" se refiere a un disco duro IDE.
"a" es el primer disco duro del equipo.
"b" es el segundo disco duro del equipo.
"c" es el tercer disco duro del equipo.

En este se usa un disco duro SATA por lo que el comando queda de la siguiente forma:

- fdisk /dev/hdb

Una vez ingresado el comando indicado, la aplicación fdisk se inicia:

Command (m for help):

Al presionar la letra m apare el siguiente menú de opciones:

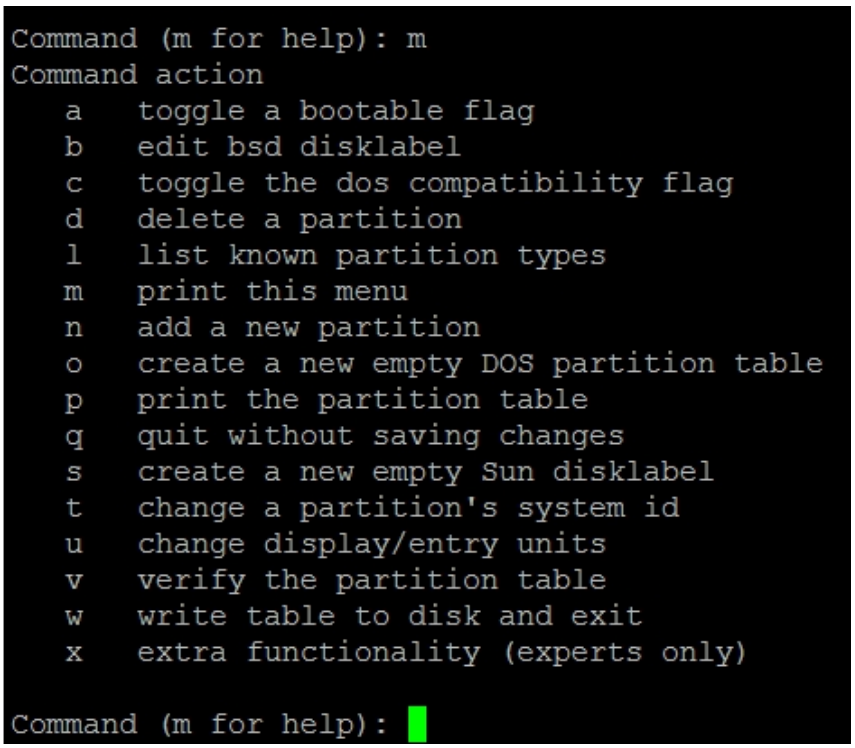


Figura 101-3: fdisk – m a9

Realizado por: Luis Lema, 2016

A continuación, elegir la opción "t" que es: "Cambiar el id de una partición del sistema".

fdisk, preguntara a que partición se desea cambiar el ID, estas particiones serán:

- sdb1
- sdb2

Luego, se debe ingresar el código hexadecimal para particiones RAID, como no se conoce este código en el menú de ayuda ingresar "l" y se mostrará la siguiente lista:

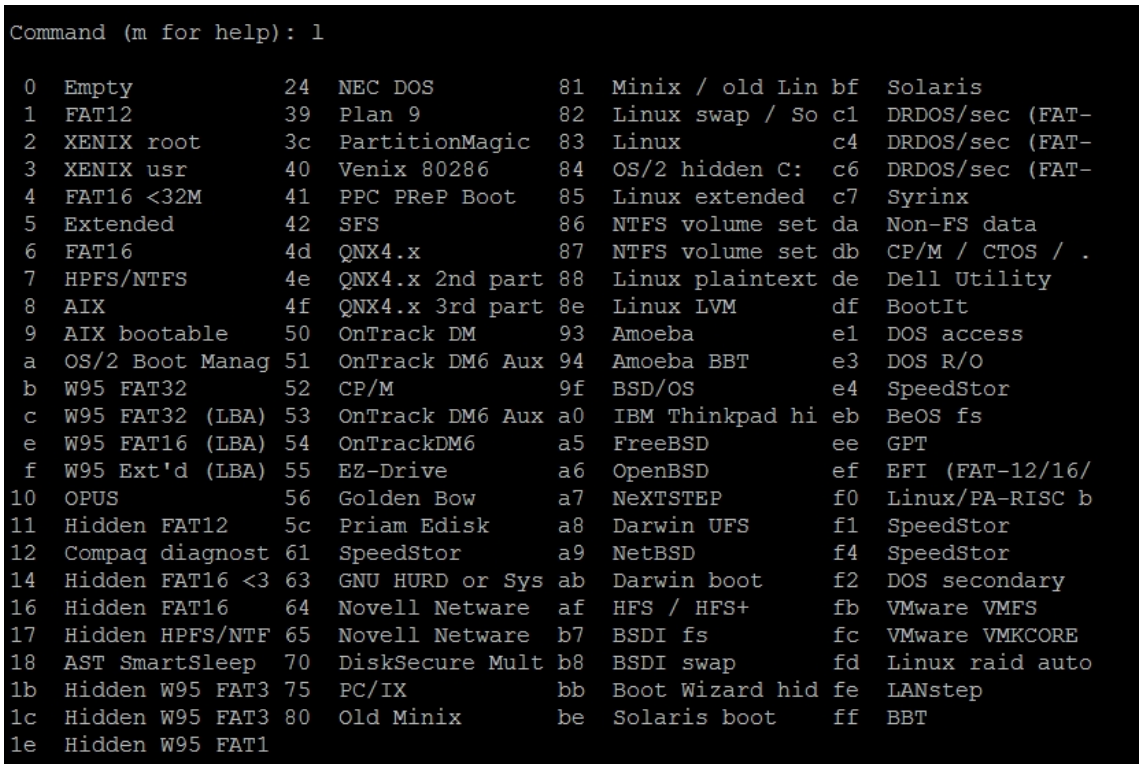


Figura 102-3: códigos hexadecimales a9

Realizado por: Luis Lema, 2016

El código para RAID es: “fd Linux raid auto”, ingresar el código y teclear “w” para guardar.

Para crear y asignar el RAID ejecutar los siguientes comandos:

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

Donde:

“create /dev/md0”, es el nombre del RAID que se está creando.
“level=1”, es el tipo de RAID que se está creando en este caso RAID 1.
“raid-disks=2”, es el número de dispositivos que forman el RAID.
“/dev/sda /dev/sdb”, es lista de dispositivos que forma parte del RAID.

Estos RAID se están creando en modo degradado, por lo que se solo se deben añadir al RAID los discos que se han formateado, por lo que las entradas que corresponden al

disco /dev/sda se deja en missing El siguiente paso será darles formato a las particiones RAID, ejecutar el siguiente comando:

- mkfs.ext3 /dev/md0
- mkswap /dev/md1

Una vez hecho esto se debe modificar e fichero: mdadm.conf ejecutando el siguiente comando:

- mdadm --examine –scan

Este comando devuelve información sobre el RAID que se está creando, se deben 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...

A continuación se deben crear los puntos de montaje donde irán las particiones del RAID, ejecutar los siguientes comandos:

- mkdir /mnt/md0
- mkdir /mnt/md1

Montar las particiones RAID ejecutando los siguientes comandos:

- mount /dev/md0 /mnt/md0
- mount /dev/md1 /mnt/md1

Para que las particiones del RAID se monten como “/” y “swap” se debe modificar el archivo de configuración “/etc/fstab”, sustituyendo lo siguiente:

- /dev/sda1 / ext3 defaults,errors=remount-ro 0 1
- /dev/sda2 none swap sw 0 0

Por las siguientes líneas:

- /dev/md0 / ext3 defaults,errors=remount-ro 0 1
- /dev/md1 none swap sw 0 0

De igual manera modificar el archivo "/etc/mtab" sustiyendo "/dev/sda1" por "/dev/md0".

El siguiente paso es modificar el grub del sistema operativo para que arranque desde la paritción RAID, el fichero es: "/boot/grub/menu.lst"

Se deben reemplazar las siguientes líneas:

- 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

Por las siguientes líneas:

- 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

También aumentar la siguiente línea:

- 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

Una vez actualizado el fichero, se debe actualizar el ramdisk mediante el siguiente comando:

- update-initramfs –u

Lo siguiente es copiar los archivos de "/" a la nueva partición desde la que se va arrancar, ejecutar el siguiente comando:

- cp -dpRx / /mnt/md0

Además de todos los pasos antes descritos se debe activar el grub en los dos discos duros, mediante los comandos:

- grub
- grub> root (hd1,0) grub> setup (hd1)
- grub> root (hd0,0) grub> setup (hd0) exit

Reiniciar el equipo el cual ya debe arrancar desde el RAID, ejecutar:

- df –h

Ahora el sistema ha arrancado desde el segundo disco duro se debe 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 se hizo con /dev/sdb1 y /dev/sdb2, se deberá hacer con /dev/sda1 y /dev/sda2. Luego de haber hecho el paso anterior añadir las particiones del disco duro 1 al RAID.

- mdadm --add /dev/md0 /dev/sda1
- mdadm --add /dev/md1 /dev/sda2

Revisar el fichero /proc/mdstat para ver que el RAID se esté sincronizando, esperar hasta que finalice:

- more /proc/mdstat

Una vez sincronizado modificar el fichero "/etc/mdadm.conf", primero ejecutar el comando:

- mdadm --examine –scan

Se deben eliminar las lineas que se añadieron anteriormente y sustituirlas por las que devuelve ahora la ejecución del comando anteriormente ejecutado.

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

Modificar de nuevo el grub para que la entrada que apunta a /dev/sda1 apunte a /dev/md0 en el disco (hd0,0). Para hacerlo abrir el fichero /boot/grub/menu.lst y cambiar 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:

- 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/vmlinuz-2.6.24-17-generic root=/dev/md0 ro quiet splash initrd /boot/initrd.img-2.6.24-17-generic quiet

Así, el sistema arrancara por defecto desde el disco hd1 y en el caso de que este disco falle se debe añadir fallback debajo de default en el fichero /boot/grub/menu.lst para que arranque desde el segundo disco duro.

- default 0 fallback 1

Actualizar nuevamente el ramdisk mediante el comando:

- update-initramfs –u

Por último reiniciar el equipo.

Finalmente, comprobar que el RAID funcionando simulando el fallo de uno de los discos ejecutando los siguientes comandos:

- mdadm --manage /dev/md0 --fail /dev/sdb1
- mdadm --manage /dev/md0 --remove /dev/sdb1

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

Comando/Herramienta Recomendado:

El conjunto de herramientas mdadm, está disponible en: https://www.kernel.org/pub/linux/utils/raid/mdadm/.

Este conjunto de herramientas mdadm (Multiple Device ADMinistrator), permite la administración de discos duros RAID a través de software. (Alcance Libre, 2013)

Entre las principales características están:

- Es una solución de muy bajo costo ya que no necesita costosos dispositivos de hardware.

- Configuración basada sobre el núcleo del sistema.

- Permite portar de manera transparente los arreglos entre sistemas GNU/Linux sin necesidad de reconstruir éstos.

- Aprovecha de mejor manera los recursos del sistema.

- Soporte hot-swap.

- Detecta automáticamente el número de núcleos del microprocesador para así aprovechar mejor los recursos del sistema. (Alcance Libre, 2013)

Soporta los siguientes tipos de arreglos RAID: RAID 0, RAID 1, RAID 4, RAID 5, RAID 6, RAID 10.

Si por algún motivo no viene instalado en el sistema operativo se instala de la siguiente manera:

```
yum -y install mdadm
```

Figura 103-3: instalación de mdadm a9
Fuente: www.alcancelibre.org/staticpages/index.php/como-mdadm

3.3.10. Acción Número 10

NOMBRE: Adquisición de información no volátil en un lugar diferente

PROTOCOLO DE ACTUACIÓN:

1.- Etiquetar adecuadamente la evidencia antes de ser transportada, incluir en el etiquetado:

- Número de caso
- Número de evidencia, se sugiere utilizar el formato aaa/ddmmyyy/nnnn/zz donde:
    - aaaa: Son las iniciales del investigador forense, o de la persona que realiza la incautación de la evidencia.
    - ddmmyyy: Es la fecha cuando se realiza la incautación.
    - nnnn: Número secuencial que se le da a la evidencia, empieza en 0001.

    - zz: Número secuencial para partes de la misma evidencia.
- Marca
- Modelo
- Número de serie
- Tipo

2.- Empaquetado de la evidencia:

- Empaquetar los medios magnéticos en bolsas antiestáticas.
- Evitar doblar o raspar las evidencias que sean sensibles.
- Asegurarse que todos los contenedores estén correctamente etiquetados.

3.- Mantener la evidencia lejos de fuentes de electromagnetismo mientras es transportada.

4.- Evitar almacenar la evidencia en vehículos por tiempo prolongado.

5.- Almacenar la evidencia en un Área segura, lejos de la humedad y altas temperaturas.

6.- Mantener en todo momento la cadena de custodia de la evidencia transportada. (EC-Council:CHFI, V8)

Nota: Cuando se esté transportando un computador evitar llevarlo en un vehículo donde se puedan dar cambios dramáticos de temperatura o humedad, también se debe tener en cuenta que el mejor lugar para transportar un computador en un vehículo es en el asiento trasero colocado de manera que si hay un frenado improvisado este no se caiga. (EC-Council:CHFI, V8)

Una vez que el computador se encuentre en el lugar donde se va a realizar la investigación se deben seguir estos pasos:

7.- Arrancar el computador comprometido con un Live CD de una distribución Linux que tenga disponible: herramientas/comandos para realizar copias bit a bit de particiones y/o discos duros, y para calcular valores hash.

8.- Calcular el valor hash del disco duro comprometido. Se recomienda no utilizar el algoritmo MD5 ya que no es seguro, en su lugar se puede usar SHA1, SHA-256, CRC32, etc.

9.- Crear una copia bit a bit (imagen) del disco duro de la máquina que está siendo analizada en una unidad de almacenamiento externa. Asegurarse que la capacidad de la unidad externa sea mayor al tamaño del disco duro.

10.- Calcular el valor hash de la imagen de disco duro resultante.

11.- Comparar el valor hash del disco duro original con el de la imagen resultante. Deben ser iguales.

12.- Nunca trabajar en el disco duro original. Siempre realizar las pruebas necesarias en la imagen obtenida previamente.

13.- Alterar el sistema lo menos posible.

14.- Crear un informe completo con todos los pasos y acciones seguidas.

EJEMPLO VÍA HERRAMIENTAS DE SOFTWARE PARA PLATAFORMAS WINDOWS Y LINUX:

Herramientas de software:

- kali linux, disponible en: https://www.kali.org/downloads
- Caine, disponible en: http://caine.mirror.garr.it/mirrors/caine/caine7.0.iso
- SANS SIFT, disponible en: http://digital-forensics.sans.org/community/downloads

Ejemplo:

Para este ejemplo se utilizará como víctima una máquina con Windows 7 y un Live CD con la distribución Kali Linux, si la máquina victima fuera una con Linux el procedimiento de creación de imagen forense del disco duro, sería exactamente el mismo.

El primer paso es encender la máquina víctima e ingresar a la BIOS para elegir la opción que arranque desde el lector de CD:

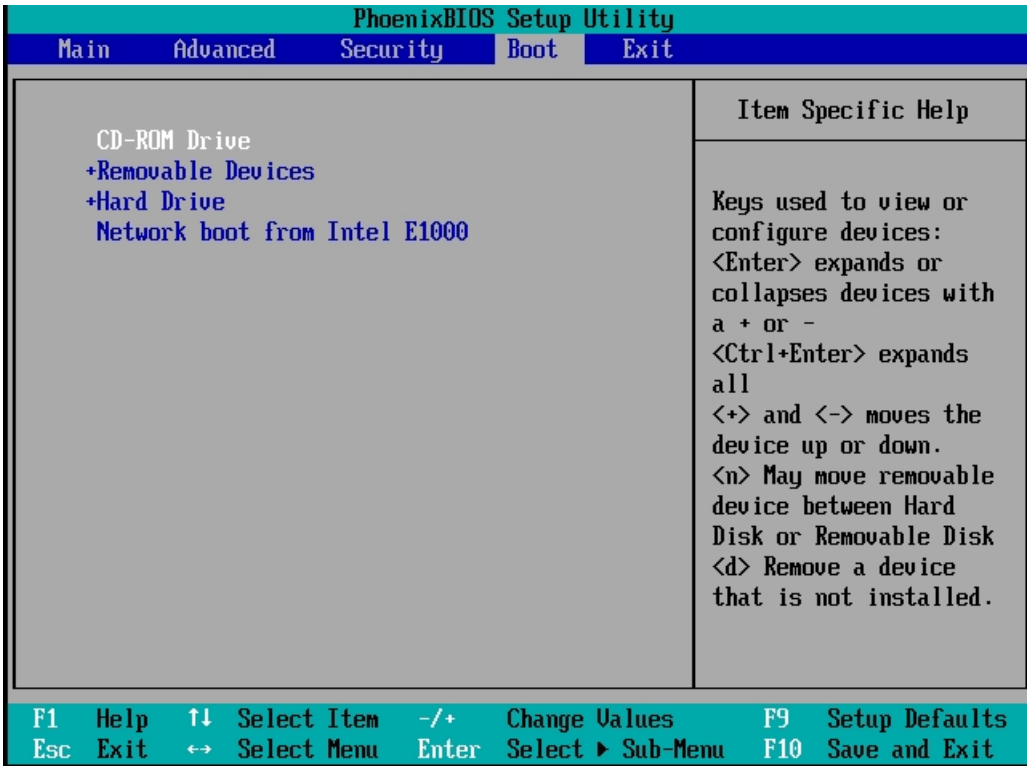


Figura 104-3: boot- CD-ROM

Realizado por: Luis Lema, 2016

En ese momento insertar el Live CD en el computador, presionar la tecla F10 y presionar la tecla Enter en la opción “Yes”:

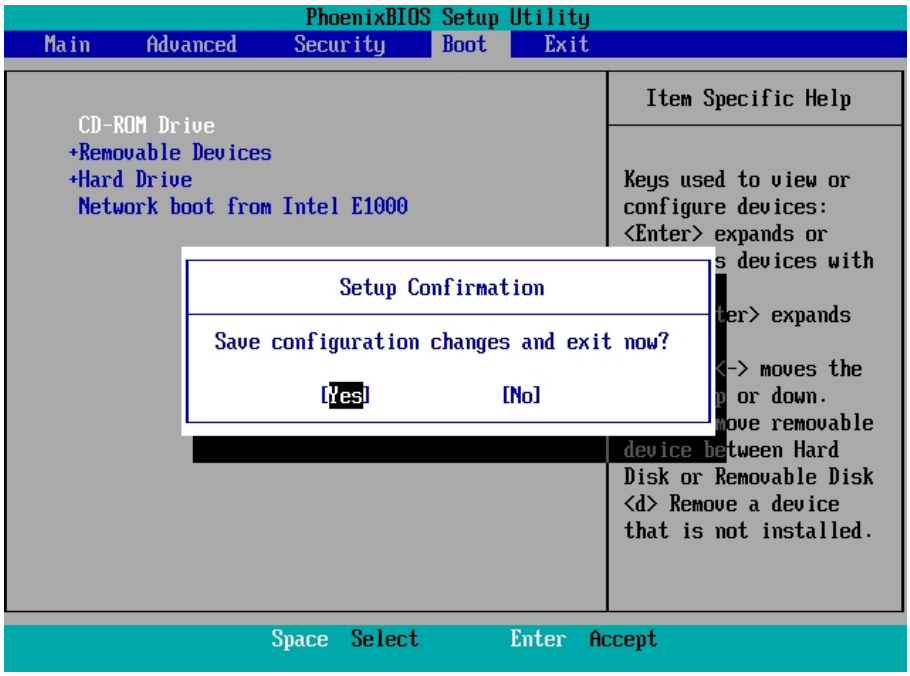


Figura 105-3: boot- CD-ROM confirmación

Realizado por: Luis Lema, 2016

A continuación, aparecerá un menú para elegir el modo en que se desea iniciar kali Linux, ya sea en modo de Live CD o instalarlo directamente en el sistema, para este ejemplo se debe elegir la primera opción:

Figura 106-3: Kali Linux modo Live CD

Realizado por: Luis Lema, 2016

Esperar a que arranque el sistema en modo Live CD, una vez que se ha terminado este proceso se puede observar la pantalla principal de Kali Linux:

Figura 107-3: Kali Linux pantalla pricipal

Realizado por: Luis Lema, 2016

A continuación, abrir un terminal para observar las características del disco duro del que se va a crear la imagen, utilizar el comando:

- fdisk –l

En este caso se va a realizar la imagen de un disco duro SATA, ya que como se puede ver la nomenclatura es /dev/sda

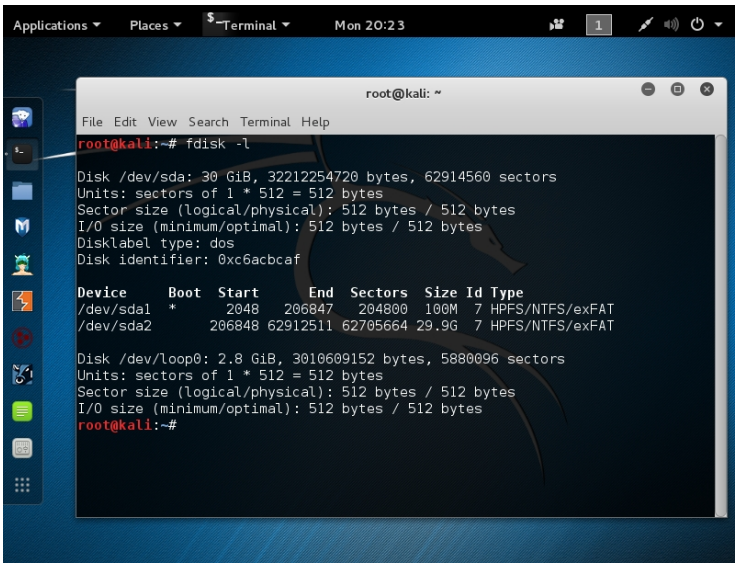


Figura 108-3: Kali Linux - fdisk

Realizado por: Luis Lema, 2016

Calcular el valor hash del disco duro comprometido con los siguientes comandos y guardarlo en un archivo:

- Si se trata de un disco duro SATA: sha1sum /dev/sda > Desktop/hashdisco.txt
- Si se trata de un disco duro IDE: sha1sum /dev/hda > Desktop/hashdisco.txt

Para este ejemplo se realizará la copia de la partición /dev/sda1, ya que realizar la copia de todo el disco duro lleva demasiado tiempo.

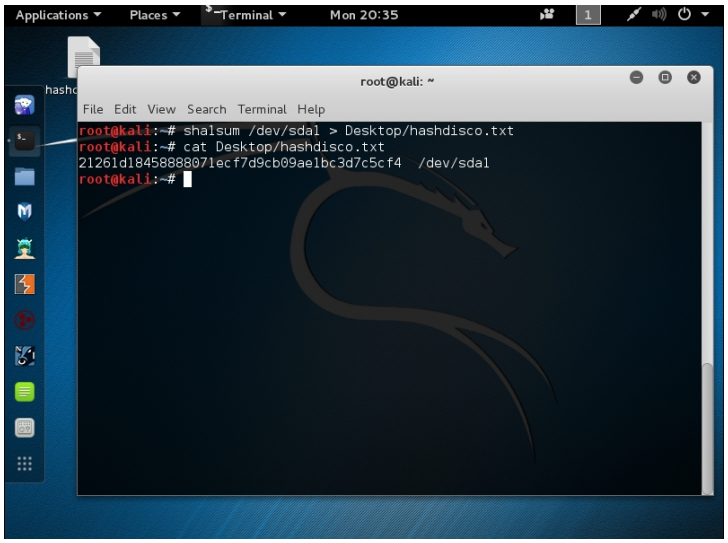


Figura 109-3: Cálculo hash Kali Linux – sha1sum

Realizado por: Luis Lema, 2016

Crear la imagen forense del disco duro con el comando “dd”:

- Si se trata de un disco duro SATA: dd if=/dev/sda of= Desktop/imgdisco.img
- Si se trata de un disco duro IDE: dd if=/dev/hda of= Desktop/imgdisco.img

Como en este caso se hace la imagen de una partición lógica se debe reemplazar “sda” por “sda1”.

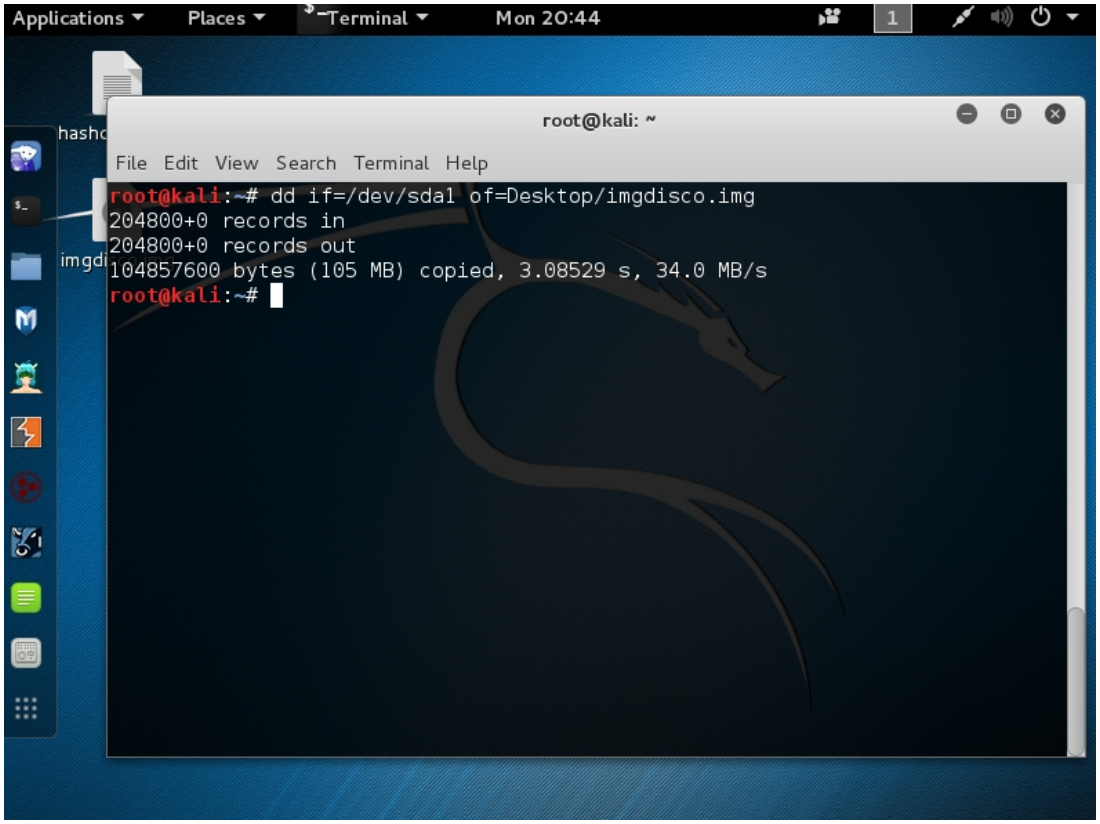


Figura 110-3: Creación imagen disco Kali Linux - dd

Realizado por: Luis Lema, 2016

A continuación, se debe calcular el valor hash de la imagen obtenida. Usar el siguiente comando y guardarlo en un archivo:

- sha1sum Desktop/imgdisco.img > Desktop/hashimg.txt

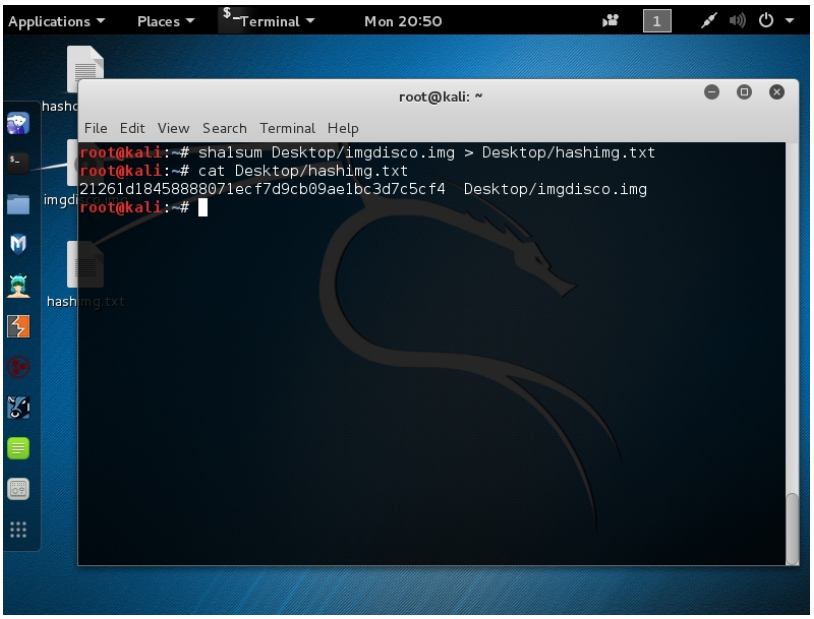


Figura 111-3: Cálculo hash imagen Kali Linux – sha1sum

Realizado por: Luis Lema, 2016

Finalmente comparar el hash de la unidad original con el hash de la imagen, estos valores deben ser iguales. Se deben guardar los documentos generados y la imagen del disco duro, en una unidad de almacenamiento externa.

- cat Desktop/hashdisco.txt ; cat Desktop/hashimg.txt

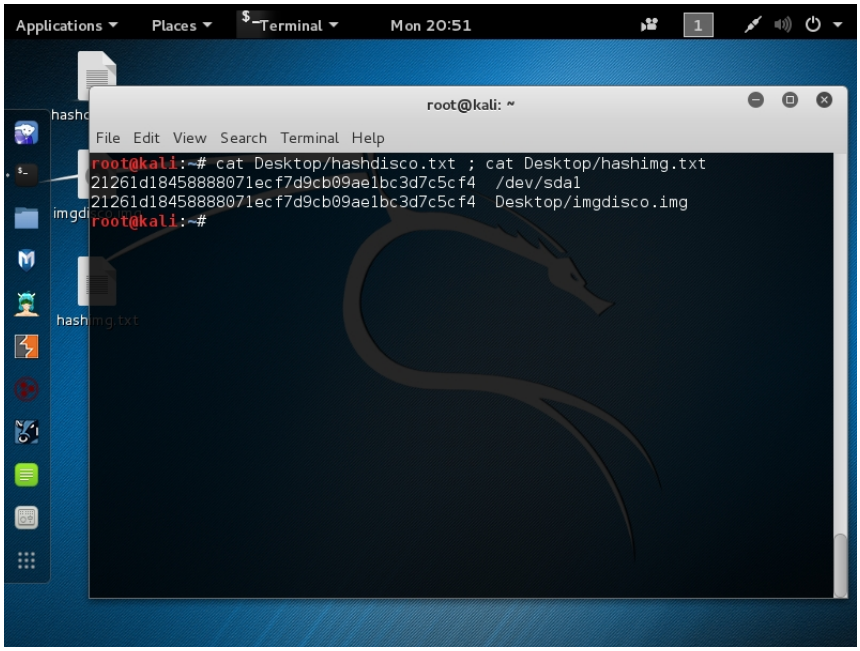


Figura 112-3: Comparación valores hash Kali Linux – cat

Realizado por: Luis Lema, 2016

Herramienta Recomendada:

Kali Linux , disponible en: https://www.kali.org/downloads

Kali Linux es una distribución de Linux basada en Debian que entre varias cosas sirve para realizar pruebas de penetración y auditorías de seguridad informática, entre las principales características están:
Tiene más de 300 herramientas para pruebas de penetración.

- Es totalmente gratuito
- De código abierto
- Es totalmente personalizable
- Todos los paquetes y repositorios son firmados con PGP.
- Las herramientas vienen en varios lenguajes.

Figura 113-3: Kali Linux

Realizado por: Luis Lema, 2016

3.3.11. Acción Número 11

NOMBRE: Adquisición de información no volátil con el computador apagado

Nota: El ejemplo para esta acción es el mismo que el de la acción número 10, ya que solamente cambia el protocolo de actuación, en la acción 10 se detalla el procedimiento para transportar la evidencia de un lugar a otro, en cambio en la acción 11 se realiza la adquisición de información no volátil en la misma escena de la investigación y ese proceso es igual en los dos casos.

PROTOCOLO DE ACTUACIÓN:

Nota: Para la adquisición de información no volátil utilizar siempre guantes de látex y manilla antiestática.

1.- Arrancar el computador comprometido con un Live CD de una distribución Linux que tenga disponible: herramientas/comandos para realizar copias bit a bit de particiones y/o discos duros, y para calcular valores hash.

2.- Calcular el valor hash del disco duro comprometido. Se recomienda no utilizar el algoritmo MD5 ya que no es seguro, en su lugar se puede usar SHA1, SHA-256, CRC32, etc.

3.- Crear una copia bit a bit (imagen) del disco duro de la máquina que está siendo analizada en una unidad de almacenamiento externa. Asegurarse que la capacidad de la unidad externa sea mayor al tamaño del disco duro.

4.- Calcular el valor hash de la imagen de disco duro resultante.

5.- Comparar el valor hash del disco duro original con el de la imagen resultante. Deben ser iguales.

6.- Nunca trabajar en el disco duro original. Siempre realizar las pruebas necesarias en la imagen obtenida previamente.

7.- Alterar el sistema lo menos posible.

8.- Crear un informe completo con todos los pasos y acciones seguidas.

EJEMPLO VÍA HERRAMIENTAS DE SOFTWARE PARA PLATAFORMAS WINDOWS Y LINUX:

Herramientas de software:

- kali linux, disponible en: https://www.kali.org/downloads
- Caine, disponible en: http://caine.mirror.garr.it/mirrors/caine/caine7.0.iso
- SANS SIFT, disponible en: http://digital-forensics.sans.org/community/downloads

Ejemplo:

Para este ejemplo se utilizará como víctima una máquina con Windows 7 y un Live CD con la distribución Kali Linux, si la máquina victima fuera una con Linux el procedimiento de creación de imagen forense del disco duro, sería exactamente el mismo.

El primer paso es encender la máquina víctima e ingresar a la BIOS para elegir la opción que arranque desde el lector de CD:

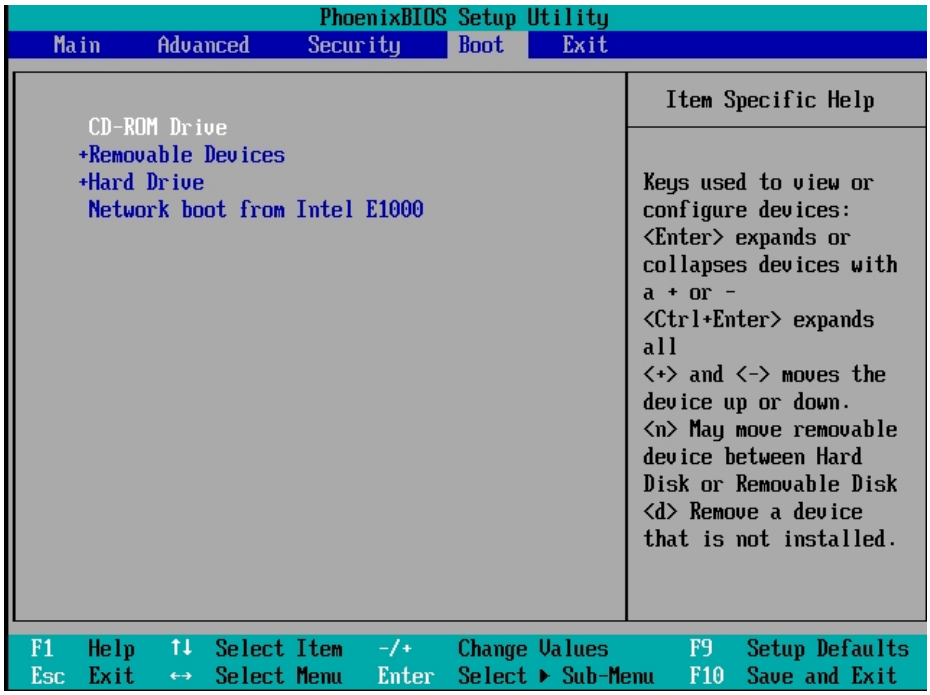


Figura 114-3: boot- CD-ROM a11

Realizado por: Luis Lema, 2016

En ese momento insertar el Live CD en el computador, presionar la tecla F10 y presionar la tecla Enter en la opción "Yes":

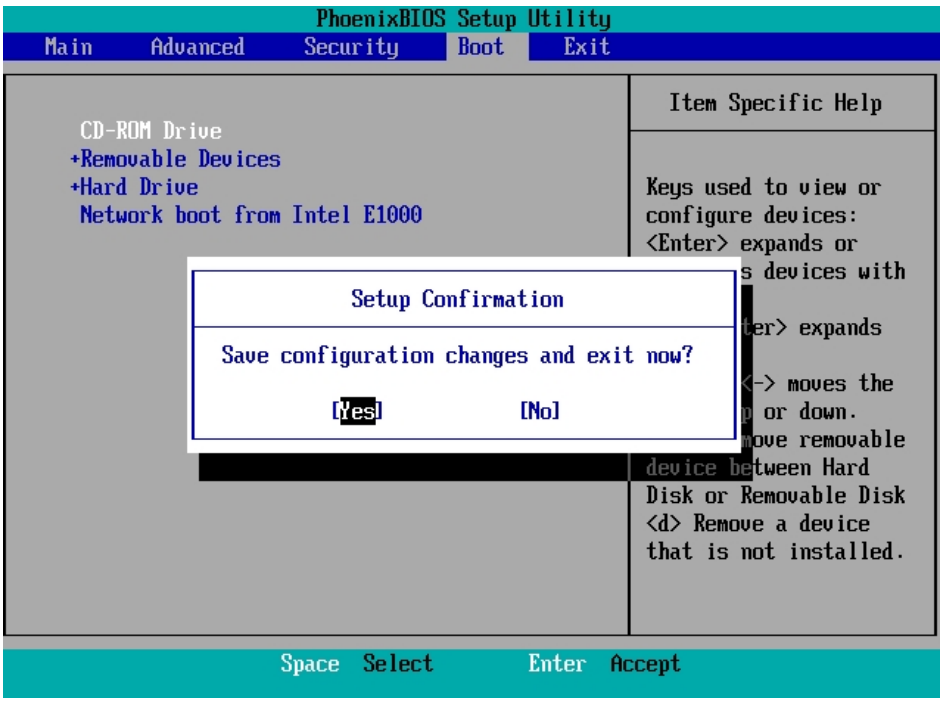


Figura 115-3: boot- CD-ROM confirmación a11

Realizado por: Luis Lema, 2016

A continuación, aparecerá un menú para elegir el modo en que se desea iniciar kali Linux, ya sea en modo de Live CD o instalarlo directamente en el sistema, para este ejemplo se debe elegir la primera opción:

Figura 116-3: Kali Linux modo Live CD a11

Realizado por: Luis Lema, 2016

Esperar a que arranque el sistema en modo Live CD, una vez que se ha terminado este proceso se puede observar la pantalla principal de Kali Linux:

Figura 117-3: Kali Linux pantalla principal a11

Realizado por: Luis Lema, 2016

A continuación, abrir un terminal para observar las características del disco duro del que se va a crear la imagen, utilizar el comando:

- fdisk –l

En este caso se va a realizar la imagen de un disco duro SATA, ya que como se puede ver la nomenclatura es /dev/sda

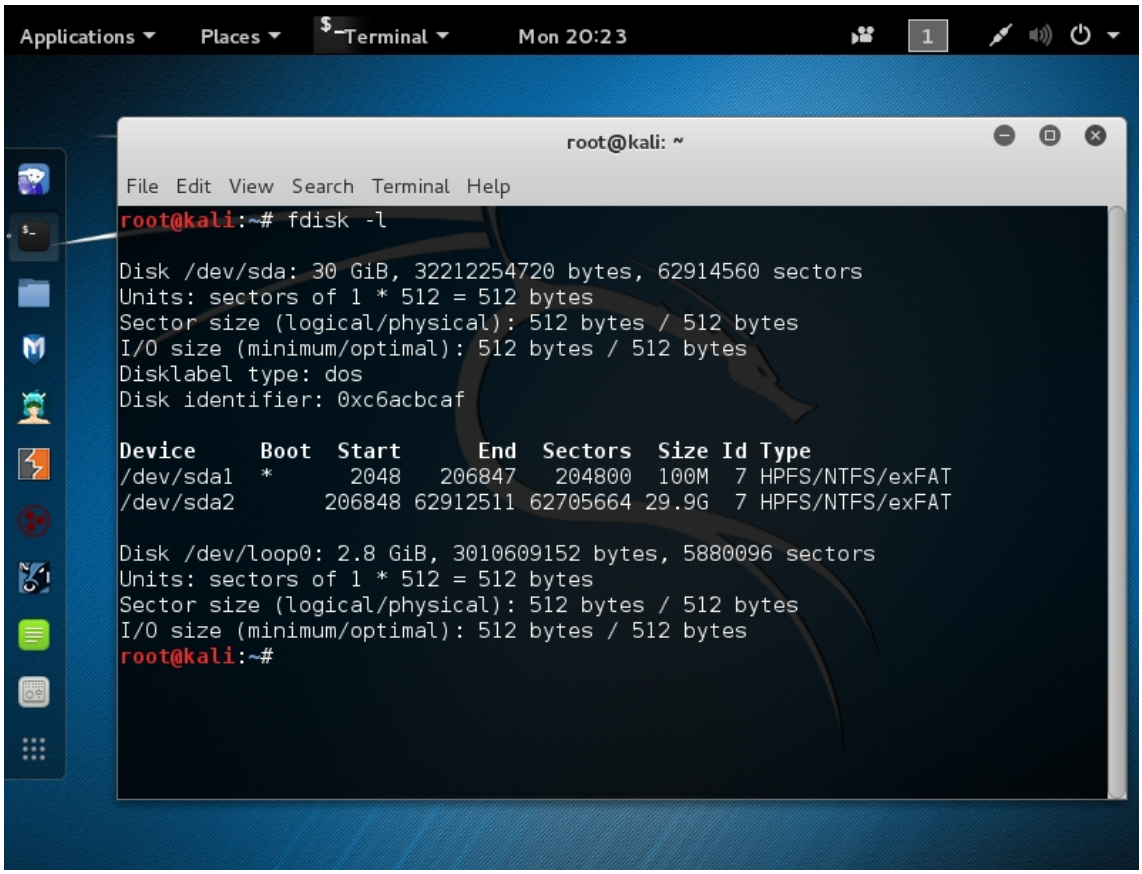


Figura 118-3: Kali Linux – fdisk a11

Realizado por: Luis Lema, 2016

Calcular el valor hash del disco duro comprometido con los siguientes comandos y guardarlo en un archivo:

- Si se trata de un disco duro SATA: sha1sum /dev/sda > Desktop/hashdisco.txt
- Si se trata de un disco duro IDE: sha1sum /dev/hda > Desktop/hashdisco.txt

Para este ejemplo se realizará la copia de la partición /dev/sda1, ya que realizar la copia de todo el disco duro lleva demasiado tiempo.

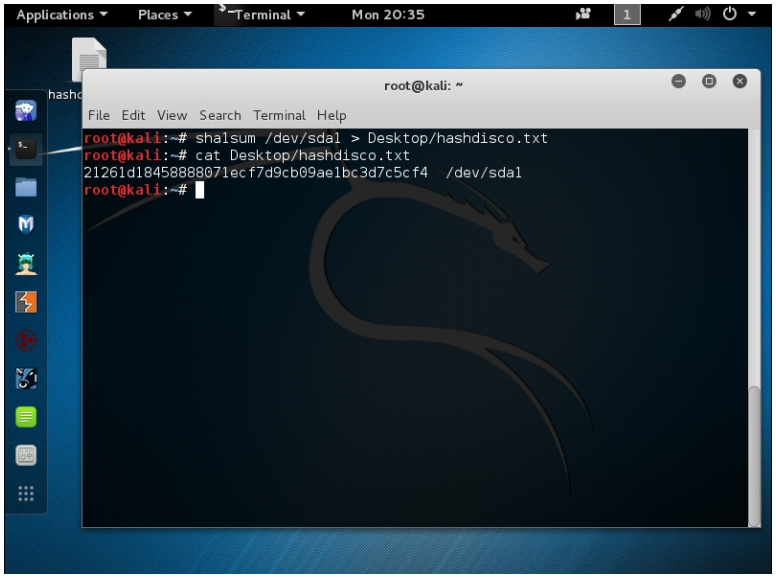


Figura 119-3: Cálculo hash Kali Linux – sha1sum a11

Realizado por: Luis Lema, 2016

Crear la imagen forense del disco duro con el comando "dd":

- Si se trata de un disco duro SATA: dd if=/dev/sda of= Desktop/imgdisco.img
- Si se trata de un disco duro IDE: dd if=/dev/hda of= Desktop/imgdisco.img

Como en este caso se hace la imagen de una partición lógica se debe reemplazar "sda" por "sda1".

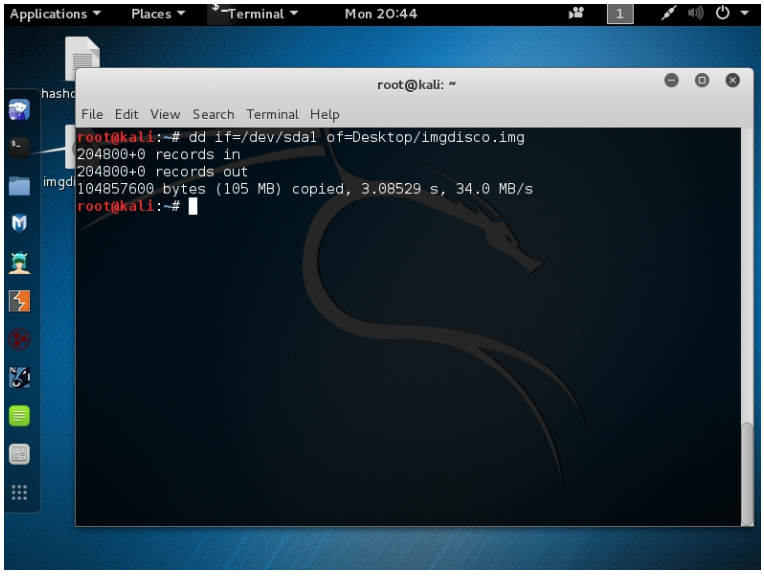


Figura 120-3: Creación imagen disco Kali Linux - dd a11

Realizado por: Luis Lema, 2016

A continuación, se debe calcular el valor hash de la imagen obtenida. Usar el siguiente comando y guardarlo en un archivo:

- sha1sum Desktop/imgdisco.img > Desktop/hashimg.txt

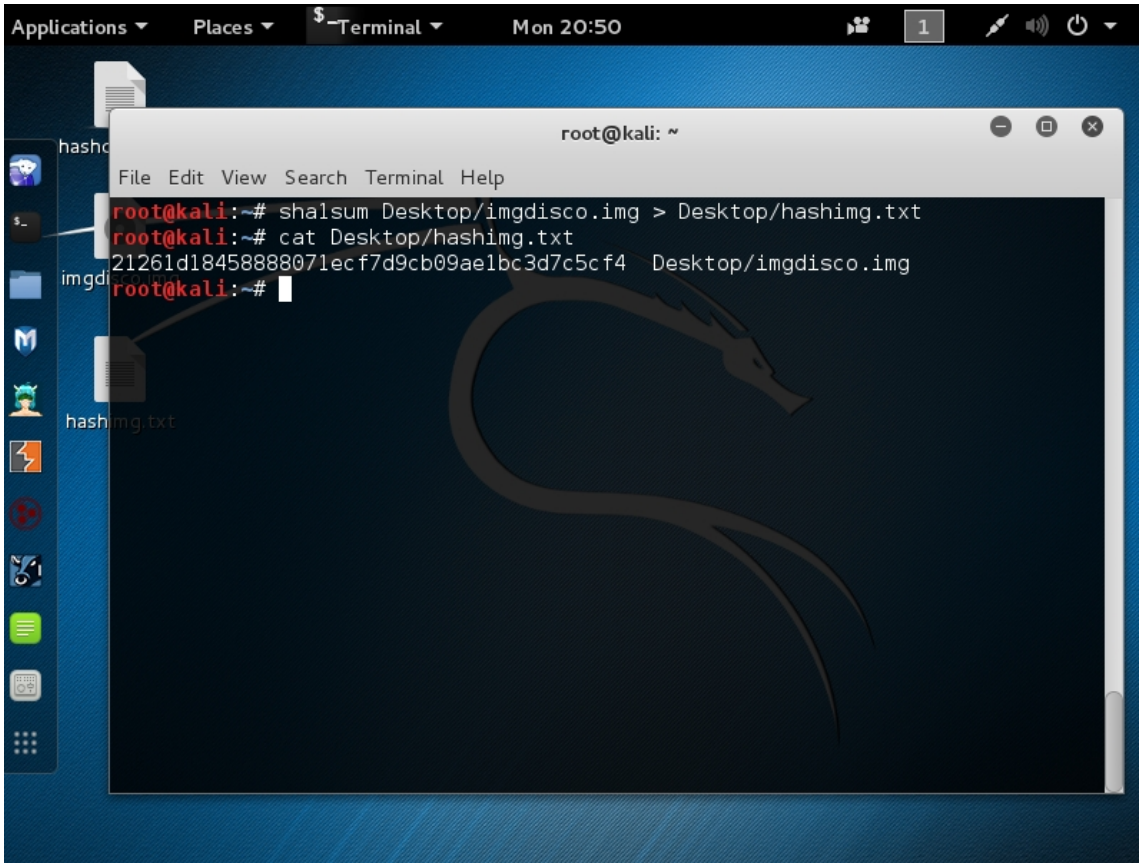


Figura 121-3: Cálculo hash imagen Kali Linux – sha1sum a11

Realizado por: Luis Lema, 2016

Finalmente comparar el hash de la unidad original con el hash de la imagen, estos valores deben ser iguales. Se deben guardar los documentos generados y la imagen del disco duro, en una unidad de almacenamiento externa.

- cat Desktop/hashdisco.txt ; cat Desktop/hashimg.txt

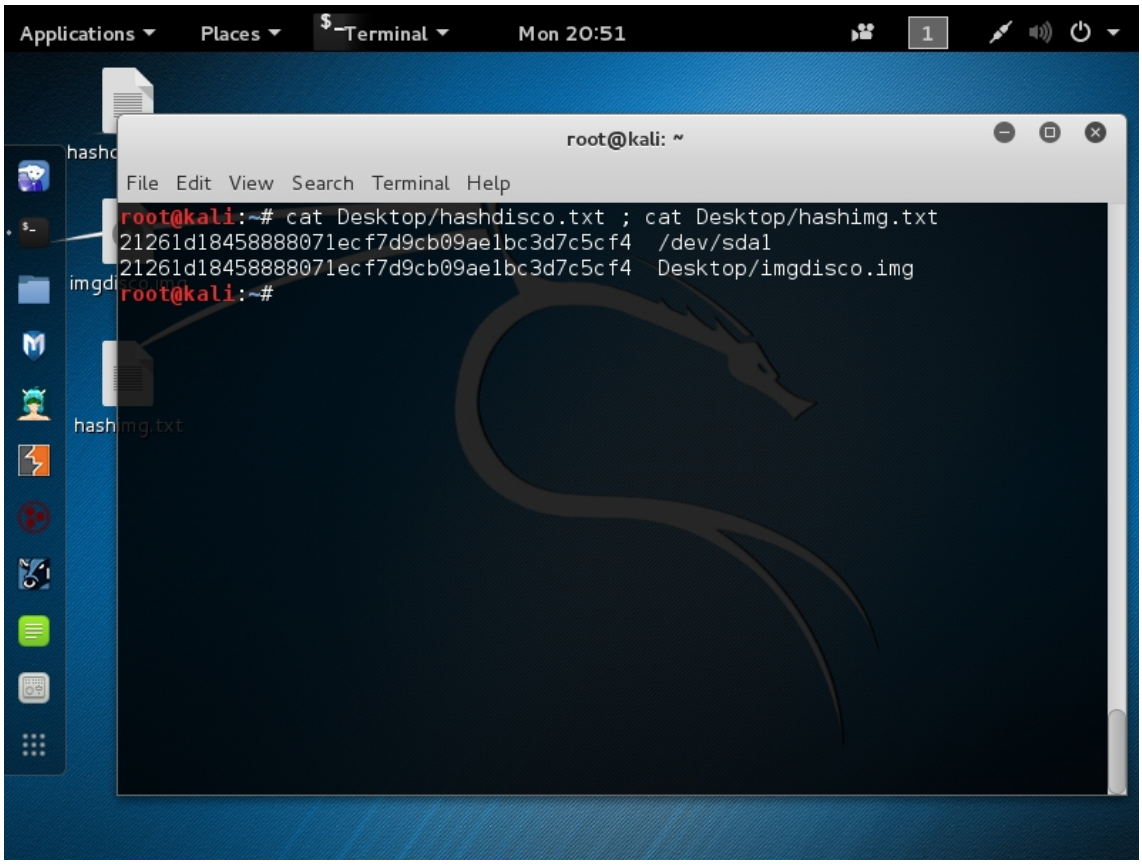


Figura 122-3: Comparación valores hash Kali Linux – cat a11

Realizado por: Luis Lema, 2016

Herramienta Recomendada:

Kali Linux , disponible en: https://www.kali.org/downloads

Kali Linux es una distribución de Linux basada en Debian que entre varias cosas sirve para realizar pruebas de penetración y auditorías de seguridad informática, entre las principales características están:
Tiene más de 300 herramientas para pruebas de penetración.

- Es totalmente gratuito
- De código abierto
- Es totalmente personalizable

- Todos los paquetes y repositorios son firmados con PGP.

- Las herramientas vienen en varios lenguajes.

Figura 123-3: Kali Linux a11

Realizado por: Luis Lema, 2016

3.4. Análisis de la imagen de un disco duro

3.4.1. Escenario

Para este punto se va analizar una imagen forense llamada "HDimage.dd", que pertenece a un disco duro de una máquina que tiene instalado un sistema operativo Linux.

Figura 124-3: Imagen forense

Realizado por: Luis Lema, 2016

Lo único que se conoce es que el administrador del equipo sospecha es que hubo un acceso no autorizado.

3.4.2. Proceso de análisis

El primer paso es calcular el valor Hash de la imagen forense y guardarlo en un documento de texto, esto se lo puede realizar con el comando "sha1sum" desde un equipo con Linux, en este caso se utilizará un computador con Kali Linux:

- sha1sum HDimage.dd > HashImagen.txt

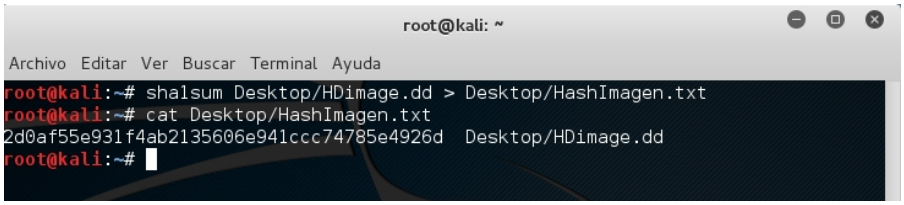


Figura 125-3: Valor hash1 de imagen forense

Realizado por: Luis Lema, 2016

Una vez obtenido el valor hash de la imagen, abrir una terminal y escribir "Autopsy", de esta manera se iniciará el Framework:

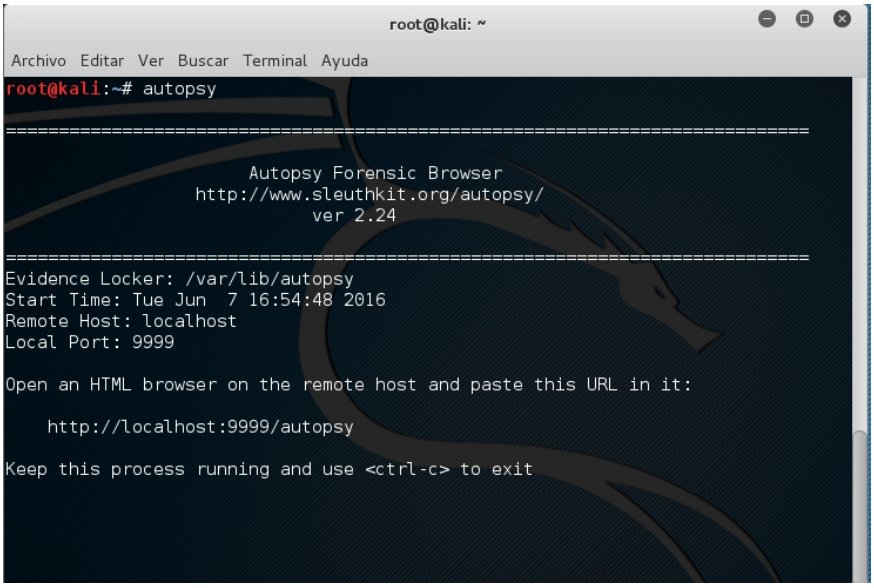


Figura 126-3: Iniciación de Autopsy

Realizado por: Luis Lema, 2016

Como se puede observar en la imagen anterior, pide que se ingrese a un navegador y se escriba la dirección URL:

- http://localhost:9999/autopsy

Una vez hecho esto aparece la siguiente pantalla:

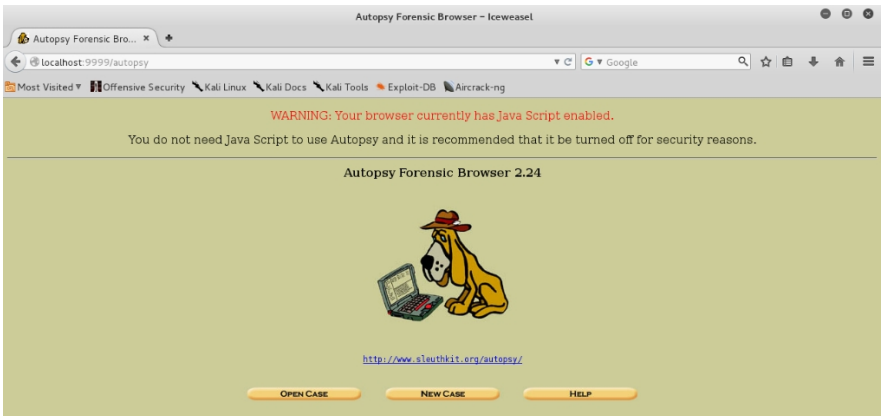


Figura 127-3: Página inicio Autopsy

Realizado por: Luis Lema, 2016

A continuación, dar click en "New Case" y llenar los datos solicitados:

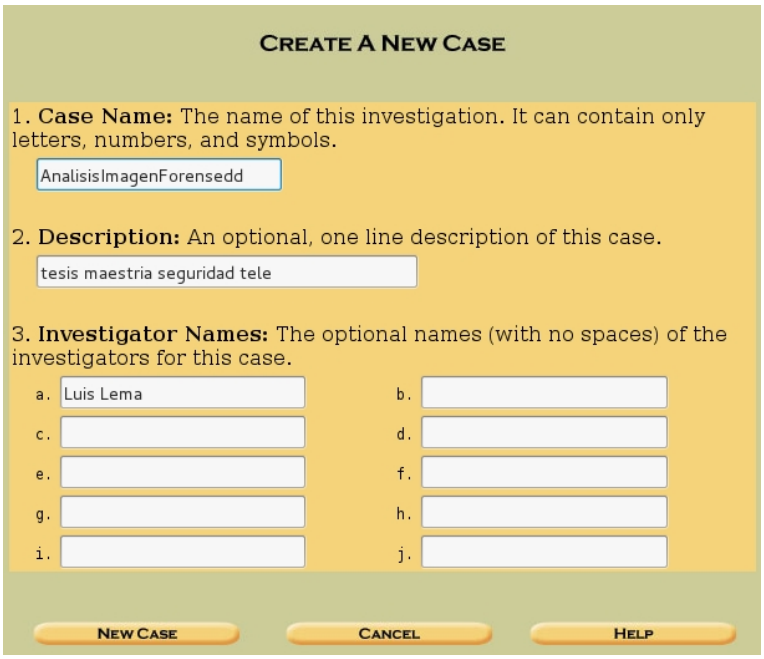


Figura 128-3: Autopsy – New Case

Realizado por: Luis Lema, 2016

Una vez ingresados los datos necesarios dar click al botón de “New Case”, aparecerá una pantalla de confirmación de la creación del nuevo caso, dar click a “Add Host”:

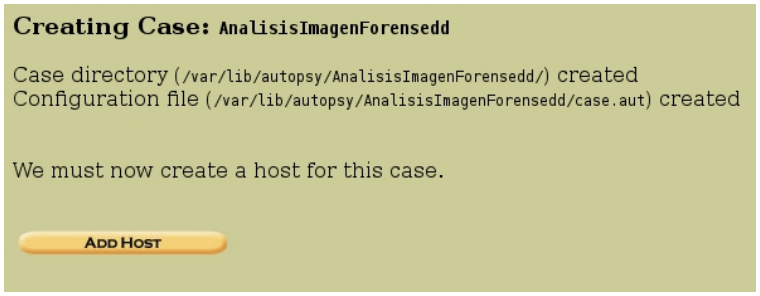


Figura 129-3: Autopsy – Creating Case

Realizado por: Luis Lema, 2016

En esta pantalla pide el ingreso de varios datos, pero solamente es necesario ingresar el nombre del host y lo demás se puede dejar vació, luego dar click al botón de “Add Host”:

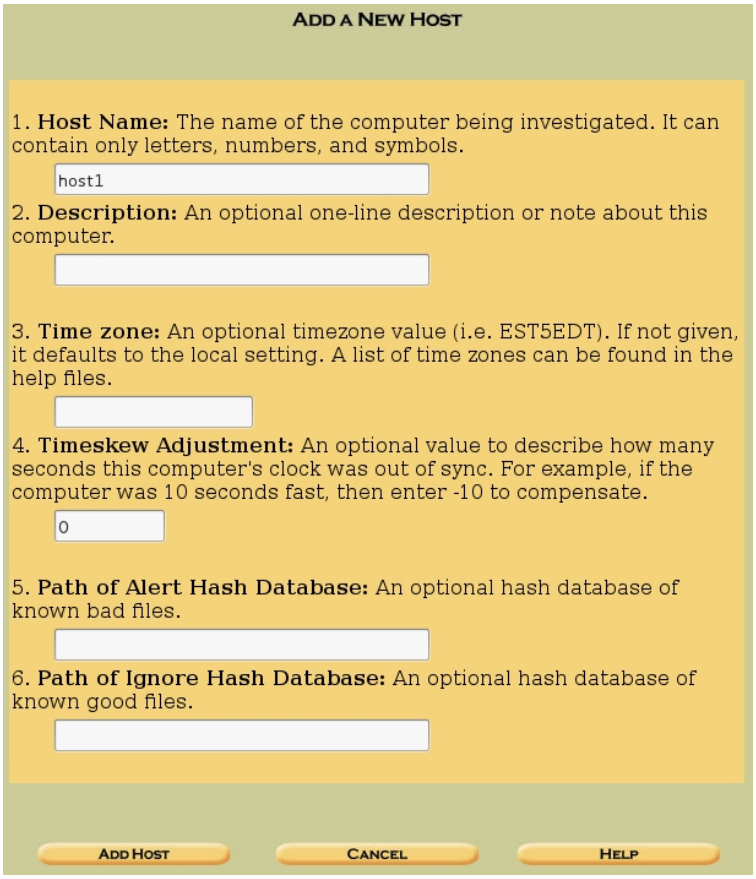


Figura 130-3: Autopsy – Add Host

Realizado por: Luis Lema, 2016

Luego se muestra la pantalla de confirmación de que el host ha sido añadido:

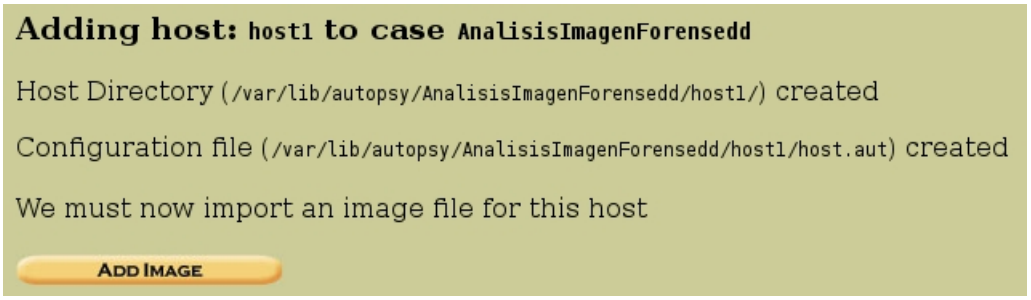


Figura 131-3: Autopsy – Host añadido

Realizado por: Luis Lema, 2016

Después del que el host fue añadido, el sistema pide añadir la imagen que se va analizar, para eso dar click en el botón "Add Image File":

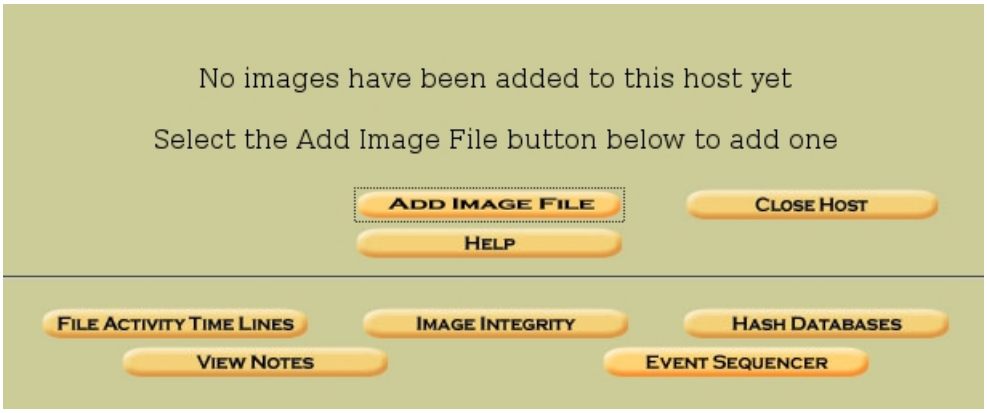


Figura 132-3: Autopsy – Add Image

Realizado por: Luis Lema, 2016

En la siguiente pantalla ingresar la ruta donde está localizada dicha imagen, la opción 2 que dice "Type" se la debe dejar marcada como "Disk" ya que se va analizar un disco duro entero y no una partición, para la opción 3 que es el "Import Method" método de importación de igual manera se le puede dejar marcada la opción "Symlink", luego dar click a "Next":

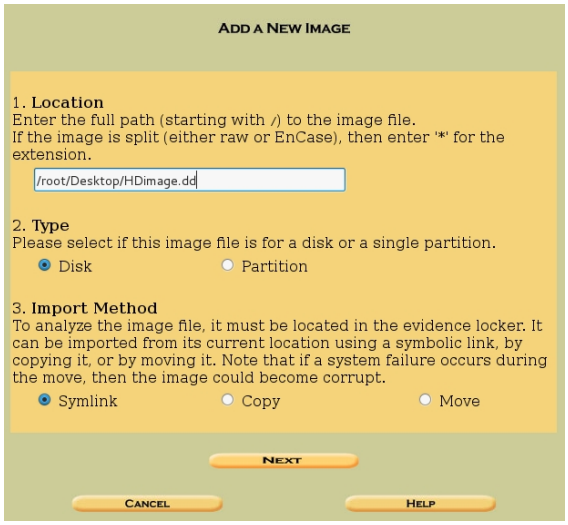


Figura 133-3: Autopsy – Add New Image

Realizado por: Luis Lema, 2016

A continuación, aparece una opción para calcular el valor hash MD5 de la imagen, se puede o no utilizar esta opción ya que anteriormente se calculó el hash sha1, más abajo se muestran los detalles de las particiones encontradas como: rango del sector donde empieza y termina, tipo de sistema de archivo y el punto de montaje, después de revisar esta información dar click a "Add":

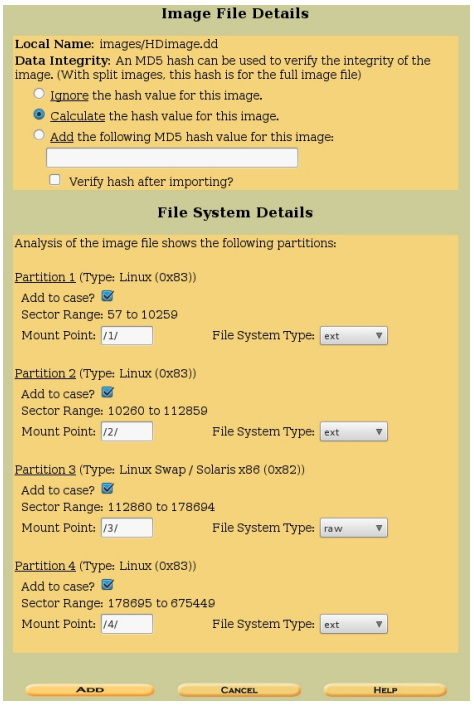


Figura 134-3: Autopsy – Image file details

Realizado por: Luis Lema, 2016

En la siguiente pantalla se puede observar un resumen de la imagen añadida, contiene el valor hash calculado y detalles de las particiones encontradas, dar click al botón “Ok”:

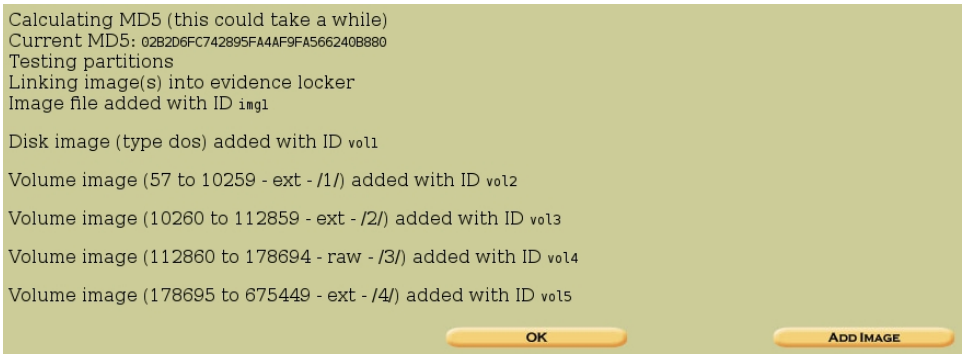


Figura 135-3: Autopsy – Resumen imagen

Realizado por: Luis Lema, 2016

Para iniciar el análisis, primero se debe elegir una de las particiones y dar click en el botón “Analyze”:

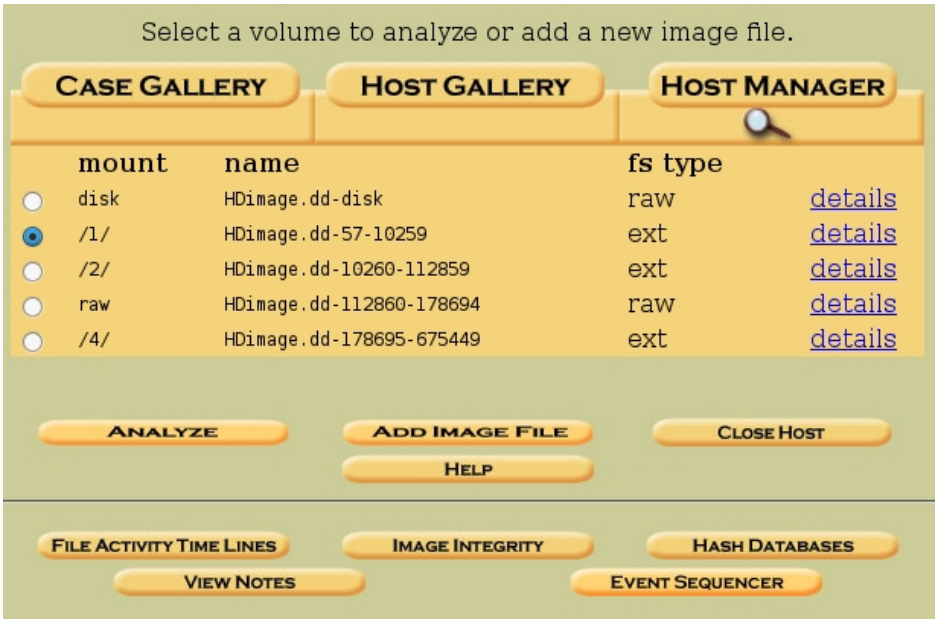


Figura 136-3: Autopsy – Selección partición

Realizado por: Luis Lema, 2016

Se pueden elegir varias opciones, la primera es “File Analize”, y es la que se va a elegir en este caso para tratar de definir qué partición es la que esta con el punto de montaje “/1/”:

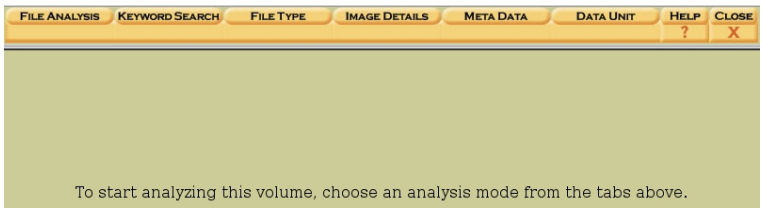


Figura 137-3: Autopsy – Opciones análisis

Realizado por: Luis Lema, 2016

Dentro de esta partición se pueden encontrar directorios como: lost+found/, vmlinuz y otros varios de boot, por lo que se podría concluir que este volumen pertenece a "/boot":

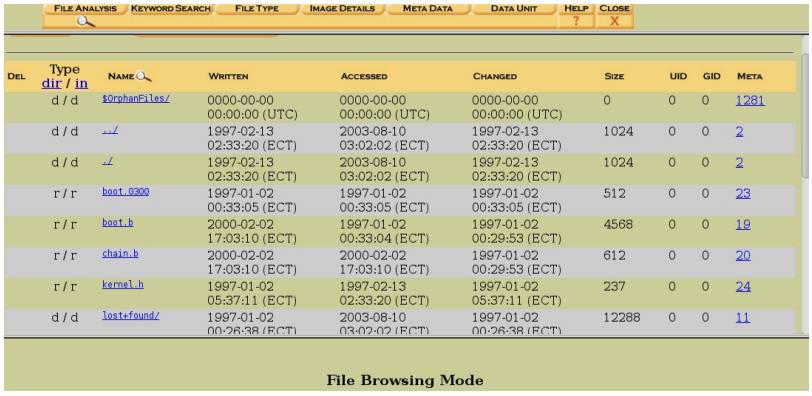


Figura 138-3: Autopsy – Análisis de ficheros boot

Realizado por: Luis Lema, 2016

De igual manera se debe realizar el mismo proceso con las demás particiones, en el caso de la segunda se puede observar el directorio "home/" y otros directorios principales como: "dev/", "etc/", "mnt/", etc, por lo que se puede concluir que esta partición pertenece a "/root":

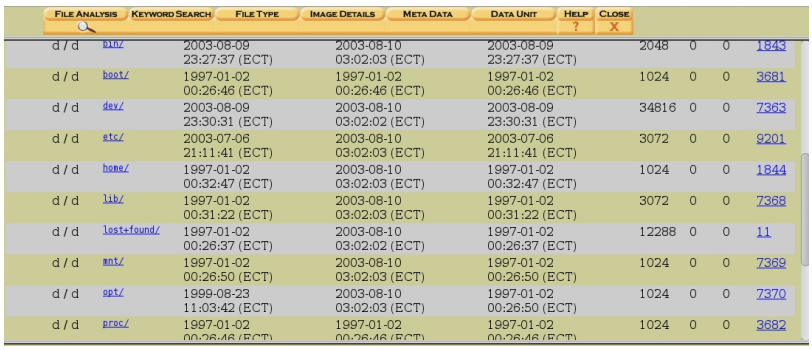


Figura 139-3: Autopsy – Análisis de ficheros root

Realizado por: Luis Lema, 2016

En la tercera partición con el nombre de "/raw/", como se vio en la imagen 3.1232 es de tipo "Linux Swap", por lo que es fácil concluir que es "swap" además como se puede ver no se puede hacer un análisis de archivos:

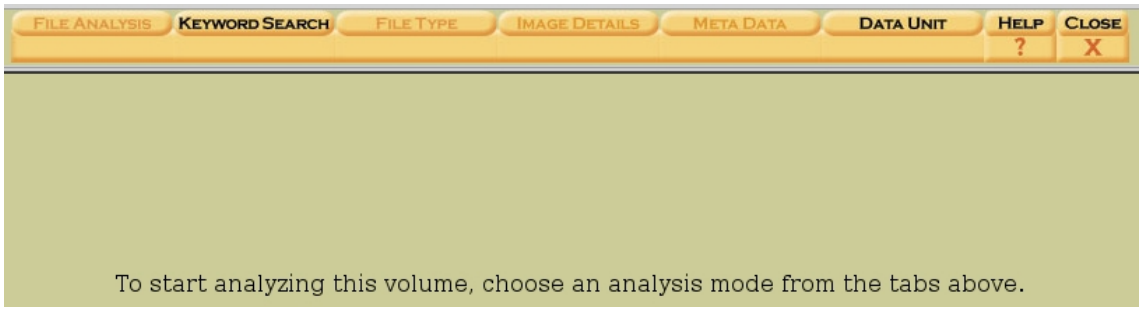
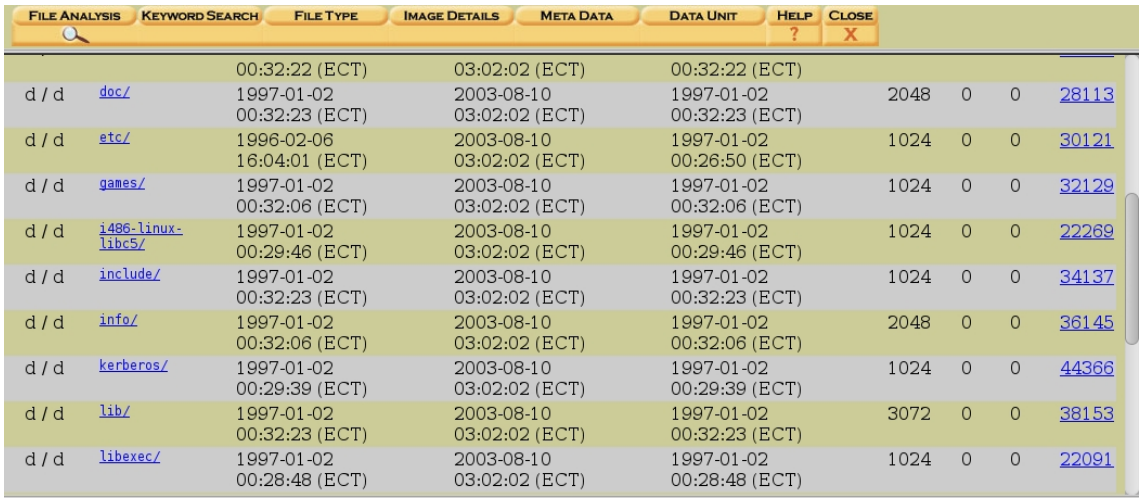


Figura 140-3: Autopsy – Análisis de ficheros swap

Realizado por: Luis Lema, 2016

En la última partición se puede ver el directorio "games/" y otros como "lib/", "libexec/", por lo que se puede decir que se trata de la partición "/usr":



		00:32:22 (ECT)	03:02:02 (ECT)	00:32:22 (ECT)				
d / d	doc/	1997-01-02 00:32:23 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:32:23 (ECT)	2048	0	0	28113
d / d	etc/	1996-02-06 16:04:01 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:26:50 (ECT)	1024	0	0	30121
d / d	games/	1997-01-02 00:32:06 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:32:06 (ECT)	1024	0	0	32129
d / d	i486-linux-libc5/	1997-01-02 00:29:46 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:29:46 (ECT)	1024	0	0	22269
d / d	include/	1997-01-02 00:32:23 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:32:23 (ECT)	1024	0	0	34137
d / d	info/	1997-01-02 00:32:06 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:32:06 (ECT)	2048	0	0	36145
d / d	kerberos/	1997-01-02 00:29:39 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:29:39 (ECT)	1024	0	0	44366
d / d	lib/	1997-01-02 00:32:23 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:32:23 (ECT)	3072	0	0	38153
d / d	libexec/	1997-01-02 00:28:48 (ECT)	2003-08-10 03:02:02 (ECT)	1997-01-02 00:28:48 (ECT)	1024	0	0	22091

Figura 141-3: Autopsy – Análisis de ficheros usr

Realizado por: Luis Lema, 2016

Recolección Evidencia

Una vez que se han identificado todas las particiones del disco duro, el siguiente paso es identificar el Sistema Operativo instalado y la versión del mismo. Esta información se puede encontrar en la partición "/root" en el directorio:

- /root/etc/issue

Como se puede observar se trata de un sistema operativo Red Hat Linux en su versión 6.2.

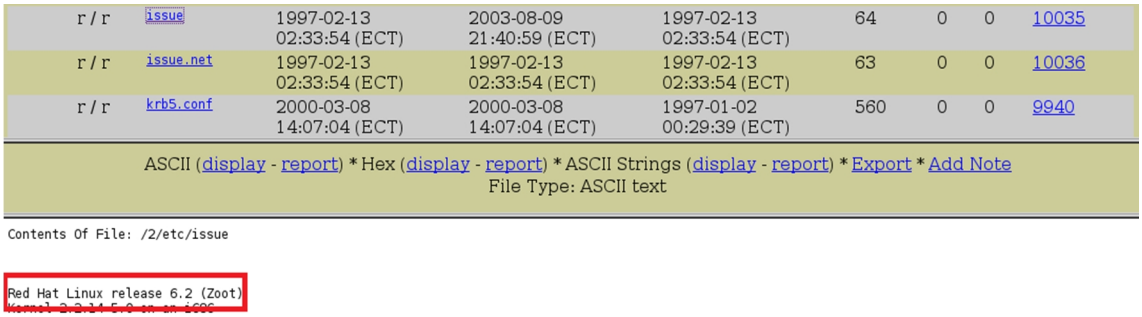


Figura 142-3: Autopsy – S.O y versión

Realizado por: Luis Lema, 2016

Cuando ya se tiene el Sistema Operativo y su versión se deben buscar sus vulnerabilidades y errores de configuración más conocidos, ya que así el investigador puede tener una mejor idea de que ataques pudo haber sufrido el computador que está siendo investigado, además sabrá que buscar en los logs del sistema, ya que al haber tanta información ahí almacenada es difícil poder identificar posibles ataques.

Para este caso se encontraron dos vulnerabilidades muy conocidas y una posible falla de configuración para Red Hat en su versión 6.2:

- Vulnerabilidad en el programa servidor de impresión "lpd": permite a un atacante remoto ganar privilegios en el sistema afectado. (CVE, 2016)
- Vulnerabilidad en Samba, puede permitir que se ejecute código arbitrario y permitir ejecutar comandos con privilegios de superusuario. (CVE, 2016)
- Posibles problemas con configuraciones en el protocolo FTP.

Otro dato importante que se debe obtener el direccionamiento IP de la máquina de donde se obtuvo la imagen del disco duro, esta información se puede obtener en la siguiente ruta:

- /root/etc/sysconfig/network-scripts/ifcfg-eth0

Como se puede ver hay solamente una interfaz de red configurada, de lo contrario se debería revisar la configuración de las demás interfaces.

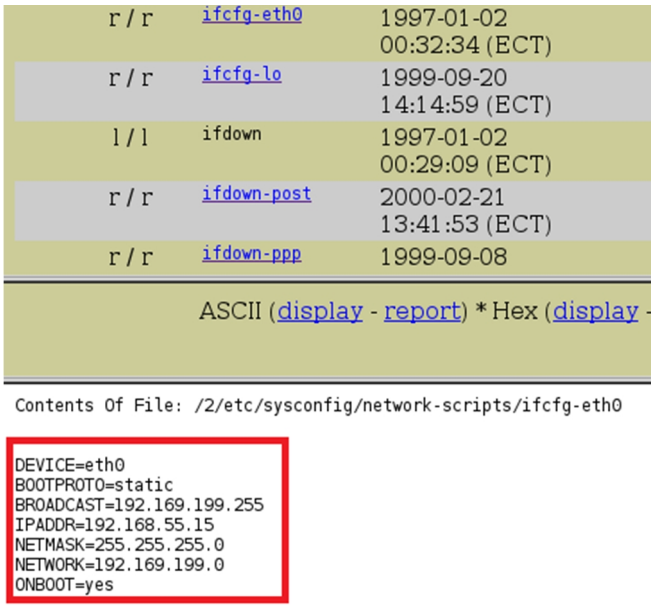


Figura 143-3: Autopsy – Direccion IP

Realizado por: Luis Lema, 2016

Para obtener la información de la puerta de enlace, ir a la siguiente ruta:

- /root/etc/sysconfig/network

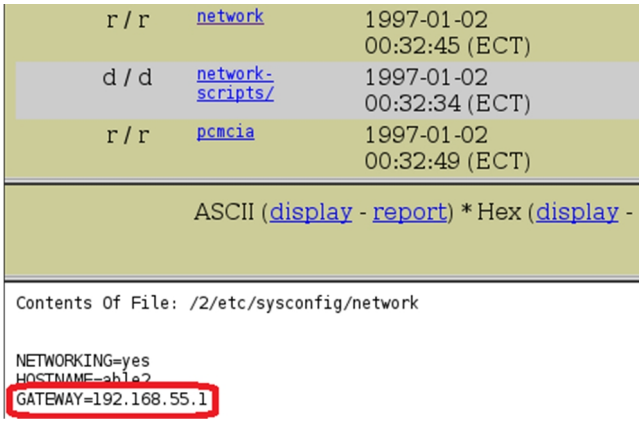


Figura 144-3: Autopsy – Puerta de enlace

Realizado por: Luis Lema, 2016

Una vez que se tiene la información de posibles vulnerabilidades y/o fallas de configuración del sistema y el direccionamiento IP, el siguiente paso es revisar los "log" del sistema.

Para eso se debe ir a la siguiente ruta:

- /root/etc/var/log

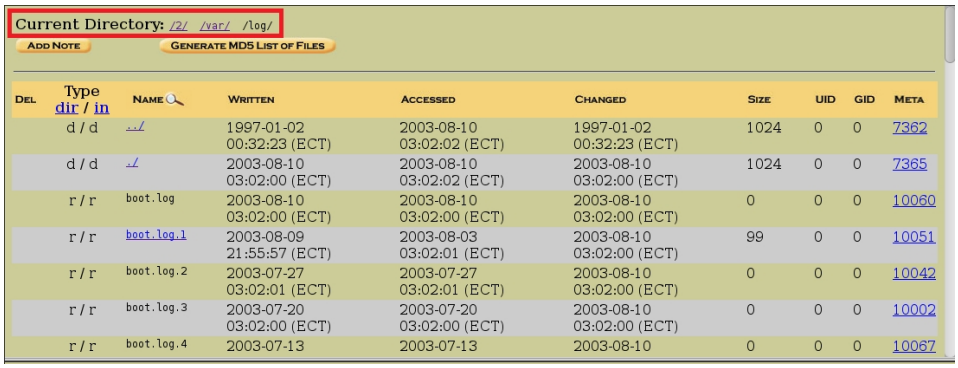


Figura 145-3: Autopsy – Log del sistema

Realizado por: Luis Lema, 2016

En esta ubicación se encuentran varios ficheros que contienen diversa información, para este análisis se van a revisar algunos que pueden contener información útil.

El primero que se va a revisar es "lastlog", que muestra información del último o últimos usuarios logueados, se encuentra en la ruta:

- /root/etc/var/log/lastlog

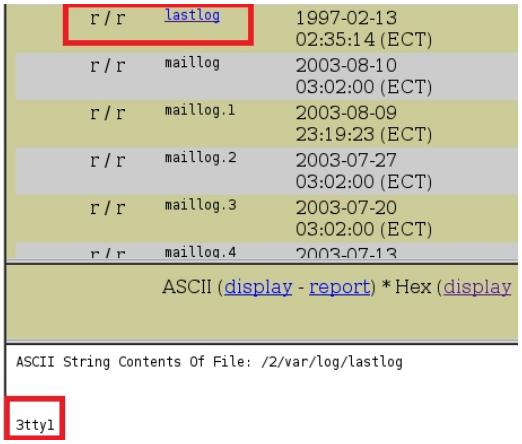


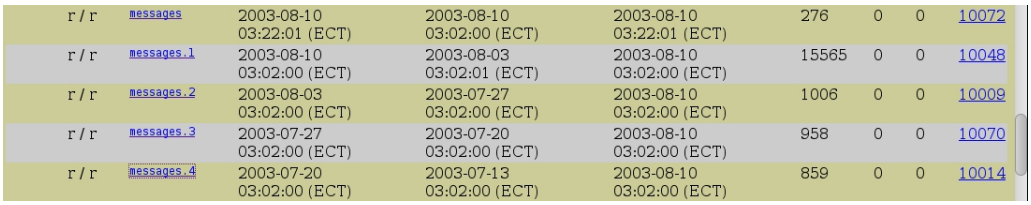
Figura 146-3: Autopsy – lastlog

Realizado por: Luis Lema, 2016

Se puede observar que se realizó una conexión vía terminal, pero tiene fecha del año 1997 y hay ficheros con fechas mucho más actuales con diferencia de varios años por lo que esta información no resulta de utilidad.

Los siguientes ficheros que se van a revisar son los que están denominados como "messages", como se puede observar en la siguiente figura son varios, están localizados en la ruta:

- /root/etc/var/log/messages."x"



r / r	messages	2003-08-10 03:22:01 (ECT)	2003-08-10 03:02:00 (ECT)	2003-08-10 03:22:01 (ECT)	276	0	0	10072
r / r	messages.1	2003-08-10 03:02:00 (ECT)	2003-08-03 03:02:01 (ECT)	2003-08-10 03:02:00 (ECT)	15565	0	0	10048
r / r	messages.2	2003-08-03 03:02:00 (ECT)	2003-07-27 03:02:00 (ECT)	2003-08-10 03:02:00 (ECT)	1006	0	0	10009
r / r	messages.3	2003-07-27 03:02:00 (ECT)	2003-07-20 03:02:00 (ECT)	2003-08-10 03:02:00 (ECT)	958	0	0	10070
r / r	messages.4	2003-07-20 03:02:00 (ECT)	2003-07-13 03:02:00 (ECT)	2003-08-10 03:02:00 (ECT)	859	0	0	10014

Figura 147-3: Autopsy – log messages

Realizado por: Luis Lema, 2016

Se ve en la figura anterior que existen 5 ficheros del tipo messages, están ordenados desde el más reciente con el nombre "messages", hasta el más antiguo con el nombre "messages.4".

En los ficheros messages.4, messages.3, messages.2 y messages se puede observar que hay pocos eventos, la mayoría son tareas programadas e incluso con días de diferencia entre unos y otros, por lo que se puede concluir que en esos ficheros no existe ningún tipo de activada sospechosa:

```
Contents Of File: /2/var/log/messages.4

Jul 13 04:02:00 able2 syslogd 1.3-3: restart.
Jul 13 04:02:00 able2 syslogd 1.3-3: restart.
Jul 13 04:02:00 able2 syslogd 1.3-3: restart.
Jul 13 04:22:00 able2 anacron[5215]: Updated timestamp for job `cron.weekly' to 2003-07-13
Jul 14 04:02:00 able2 anacron[6741]: Updated timestamp for job `cron.daily' to 2003-07-14
Jul 15 04:02:00 able2 anacron[7238]: Updated timestamp for job `cron.daily' to 2003-07-15
Jul 16 04:02:00 able2 anacron[7735]: Updated timestamp for job `cron.daily' to 2003-07-16
Jul 17 04:02:01 able2 anacron[8232]: Updated timestamp for job `cron.daily' to 2003-07-17
Jul 18 04:02:01 able2 anacron[8729]: Updated timestamp for job `cron.daily' to 2003-07-18
Jul 19 04:02:00 able2 anacron[9230]: Updated timestamp for job `cron.daily' to 2003-07-19
Jul 20 04:02:00 able2 anacron[9727]: Updated timestamp for job `cron.daily' to 2003-07-20
```

Figura 148-3: Autopsy – messages.4

Realizado por: Luis Lema, 2016

```
Contents Of File: /2/var/log/messages.3

Jul 20 04:02:00 able2 syslogd 1.3-3: restart.
Jul 20 04:02:00 able2 syslogd 1.3-3: restart.
Jul 20 04:02:00 able2 syslogd 1.3-3: restart.
Jul 20 04:02:00 able2 syslogd 1.3-3: restart.
Jul 20 04:02:00 able2 syslogd 1.3-3: restart.
Jul 20 04:22:00 able2 anacron[9882]: Updated timestamp for job `cron.weekly' to 2003-07-20
Jul 21 04:02:00 able2 anacron[11408]: Updated timestamp for job `cron.daily' to 2003-07-21
Jul 22 04:02:01 able2 anacron[11905]: Updated timestamp for job `cron.daily' to 2003-07-22
Jul 23 04:02:01 able2 anacron[12402]: Updated timestamp for job `cron.daily' to 2003-07-23
Jul 24 04:02:00 able2 anacron[12899]: Updated timestamp for job `cron.daily' to 2003-07-24
Jul 25 04:02:00 able2 anacron[13396]: Updated timestamp for job `cron.daily' to 2003-07-25
Jul 26 04:02:00 able2 anacron[13893]: Updated timestamp for job `cron.daily' to 2003-07-26
Jul 27 04:02:00 able2 anacron[14390]: Updated timestamp for job `cron.daily' to 2003-07-27
```

Figura 149-3: Autopsy – messages.3

Realizado por: Luis Lema, 2016

```
Contents Of File: /2/var/log/messages.2

Jul 27 04:02:00 able2 syslogd 1.3-3: restart.
Jul 27 04:02:00 able2 syslogd 1.3-3: restart.
Jul 27 04:02:01 able2 syslogd 1.3-3: restart.
Jul 27 04:02:01 able2 syslogd 1.3-3: restart.
Jul 27 04:22:01 able2 anacron[14545]: Updated timestamp for job `cron.weekly' to 2003-07-27
Jul 28 04:02:00 able2 anacron[16071]: Updated timestamp for job `cron.daily' to 2003-07-28
Jul 29 04:02:01 able2 anacron[16568]: Updated timestamp for job `cron.daily' to 2003-07-29
Jul 30 04:02:00 able2 anacron[17065]: Updated timestamp for job `cron.daily' to 2003-07-30
Jul 31 04:02:00 able2 anacron[17562]: Updated timestamp for job `cron.daily' to 2003-07-31
Aug  1 04:02:00 able2 anacron[18059]: Updated timestamp for job `cron.daily' to 2003-08-01
Aug  1 04:42:00 able2 anacron[18205]: Updated timestamp for job `cron.monthly' to 2003-08-01
Aug  2 04:02:00 able2 anacron[18561]: Updated timestamp for job `cron.daily' to 2003-08-02
Aug  3 04:02:00 able2 anacron[19066]: Updated timestamp for job `cron.daily' to 2003-08-03
```

Figura 150-3: Autopsy – messages.2

Realizado por: Luis Lema, 2016

```
Contents Of File: /2/var/log/messages

Aug 10 04:02:00 able2 syslogd 1.3-3: restart.
Aug 10 04:02:00 able2 syslogd 1.3-3: restart.
Aug 10 04:02:00 able2 syslogd 1.3-3: restart.
Aug 10 04:02:00 able2 syslogd 1.3-3: restart.
Aug 10 04:22:01 able2 anacron[25089]: Updated timestamp for job `cron.weekly' to 2003-08-10
```

Figura 151-3: Autopsy – messages

Realizado por: Luis Lema, 2016

En el fichero "messages.1" es donde se puede observar que existen actividades sospechosas, como peticiones consecutivas que están siendo bloqueadas por el firewall del sistema operativo a los puertos 23 (Telnet), 79 (Finger) y al 80 (http):

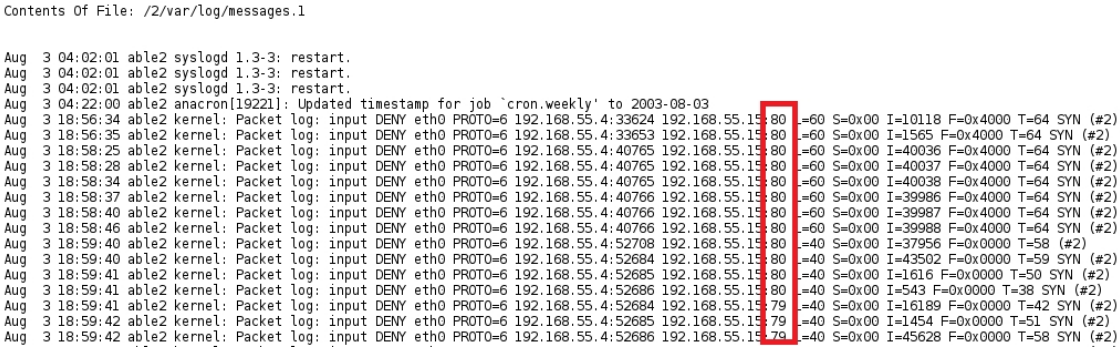


Figura 152-3: Autopsy – messages.1 1

Realizado por: Luis Lema, 2016

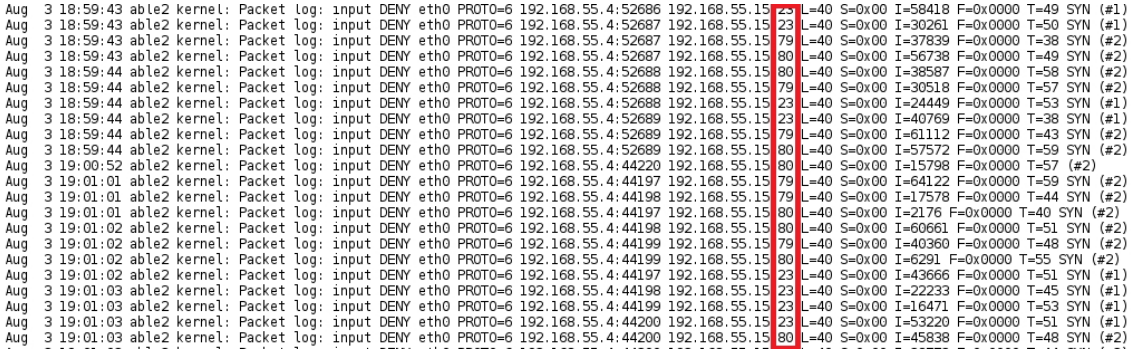


Figura 153-3: Autopsy – messages.1 2

Realizado por: Luis Lema, 2016

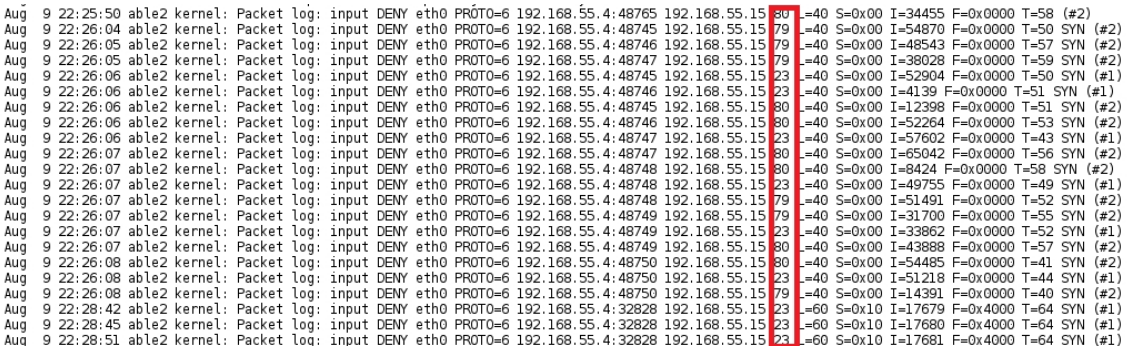


Figura 154-3: Autopsy – messages.1 3

Realizado por: Luis Lema, 2016

Se puede ver que estas peticiones se repiten las fechas 3 de agosto y 9 de agosto, lo que se puede concluir es que hubo intentos de conexión repetidos por parte de la máquina con IP 192.168.55.4 hacia la máquina con IP 192.168.55.4, a los puertos 23,79 y 80, pero estos intentos fueron rechazados por el firewall, al ser tan repetidos los intentos de conexión pudo tratarse de un intento de Denegación de Servicio (DOS).

En el mismo fichero “messages.1” se puede observar una conexión anónima al servicio de FTP por parte de la máquina con IP 192.168.55.4:

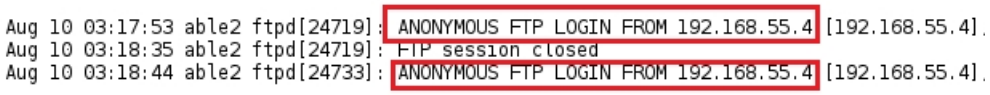


Figura 155-3: Autopsy – messages.1 ftp anónimo

Realizado por: Luis Lema, 2016

Esta conexión se realizó el 10 de agosto un día después de los intentos fallidos de denegación de servicio, esta información de que hubo una conexión por parte de la máquina sospechosa de los ataques se podría corroborar en los ficheros de log “secure” y “wtmp”, estos dos ficheros contienen información de usuarios logueados en el sistema, en el caso de secure indica información de autenticaciones exitosas o fallidas y wtmp información de quién o quienes están logueados en el sistema:

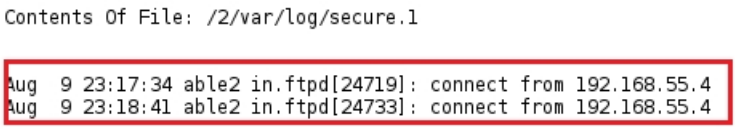


Figura 156-3: Autopsy – secure.1

Realizado por: Luis Lema, 2016

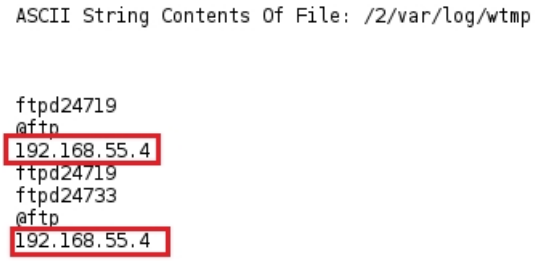


Figura 157-3: Autopsy – wtmp

Realizado por: Luis Lema, 2016

Una vez que se ha comprobado que existió un ingreso anónimo al servicio de FTP, el siguiente paso es identificar si efectivamente está activado el login anónimo.

Para esto lo primero que se puede hacer es una búsqueda de la palabra clave “ftp” en la partición “/root”, así se puede identificar que servidor ftp está instalado en el sistema, en el menú superior existe un botón llamado “Keyword Search” dar click ahí:

Figura 158-3: Autopsy – Keyword search

Realizado por: Luis Lema, 2016

En la siguiente pantalla aparece un cuadro de texto en el que se debe ingresar la palabra a buscar, en este caso es "ftp", a continuación, dar click en "search":

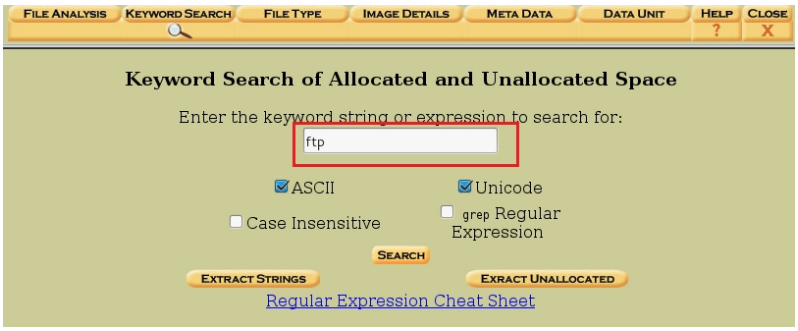


Figura 159-3: Autopsy – Enter Keyword search

Realizado por: Luis Lema, 2016

Al lado izquierdo de la pantalla aparece los resultados de la búsqueda, y como se puede ver en la siguiente imagen hay varias coincidencias que contienen la palabra "wuftpd", que hace referencia a un servidor ftp gratuito llamado "wuarchive-ftpd":

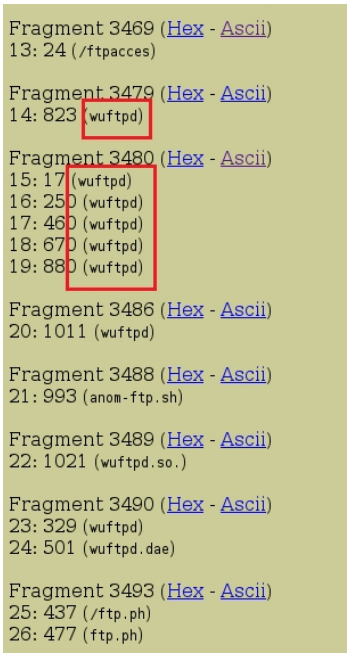


Figura 160-3: Autopsy – Keyword search wuftpd

Realizado por: Luis Lema, 2016

Una vez identificado el servidor ftp se debe revisar el archivo de configuración del mismo, que se encuentra en la ubicación:

- /root/etc/ftpaccess

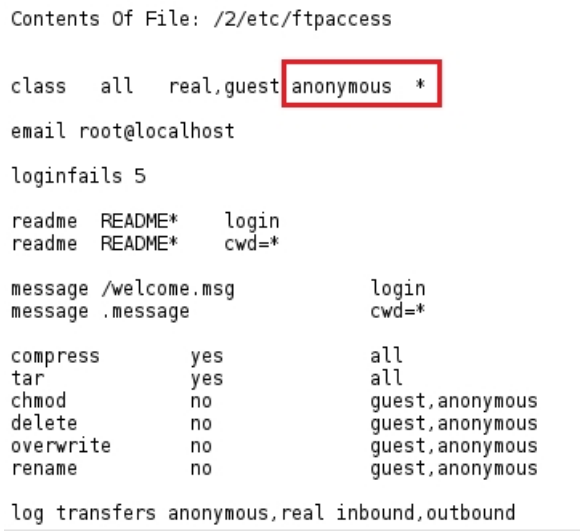


Figura 161-3: Autopsy –wuftpd configuración

Realizado por: Luis Lema, 2016

En el archivo de configuración se puede observar que está habilitado el login anónimo lo cual es una falla de configuración ya que permite que cualquier usuario, ya sea este autorizado o no tenga acceso a este servicio.

Finalmente, se puede concluir que hubo un acceso anónimo al servicio FTP por parte de la máquina con dirección IP 192.168.55.4, así como indicios de un posible intento de denegación de servicio ya que hubo varios intentos de conexión fallidos a diferentes puertos en la máquina siendo analizada.

3.5. Aplicación Web

El desarrollo de esta aplicación web tiene como objetivo que el modelo para la toma de decisiones multicriterio como soporte para el análisis forense en dispositivos de almacenamiento digital, este disponible para ser usado por cualquier investigador forense en cualquier momento y en cualquier lugar. Contiene la siguiente información:

- Diagramas de flujo para la toma de decisiones cuando un computador se encuentra o no conectado a una red.
- Protocolos de actuación dependiendo del escenario elegido.
- Ejemplos de las acciones a realizar para las plataformas Windows y Linux por medio de comandos y/o herramientas de software.
- Herramienta de software y/o comando recomendado para la realización de la tarea indicada.
- Ejemplo de un análisis forense a una imagen de un disco duro.

En la creación de esta Aplicación se utilizaron las siguientes herramientas de programación y software:

- Html
- CSS
- Dreamweaver

Uso de la aplicación Web

La página principal contiene el logo de la ESPOCH, pestañas con accesos directos a los diagramas de flujo para la toma de decisiones, y de contenido solamente el título del trabajo y el autor y director del mismo:

Figura 162-3: Página principal – app web

Realizado por: Luis Lema, 2016

Para acceder al diagrama de flujo cuando el computador se encuentra en red, dar click en la pestaña “Diagrama de Red” o al enlace que se encuentra en la parte inferior llamado “Siguiente”, aparecerá una pantalla donde se podrá seguir elegir entre una acción o una decisión dependiendo del escenario con el que se encuentre el investigador.

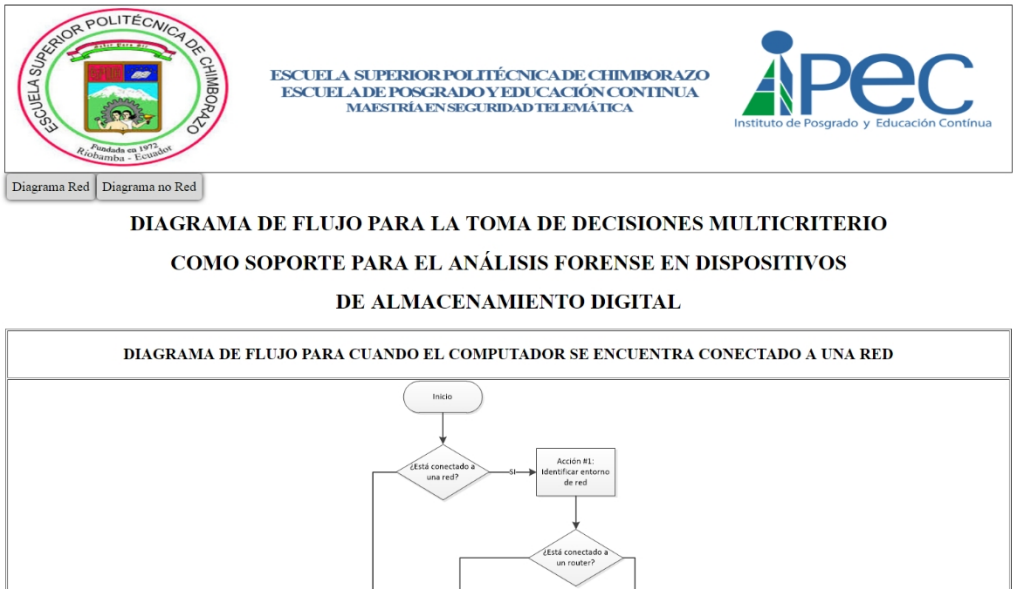


Figura 163-3: Página Diagrama Red parte 1 – app web

Realizado por: Luis Lema, 2016

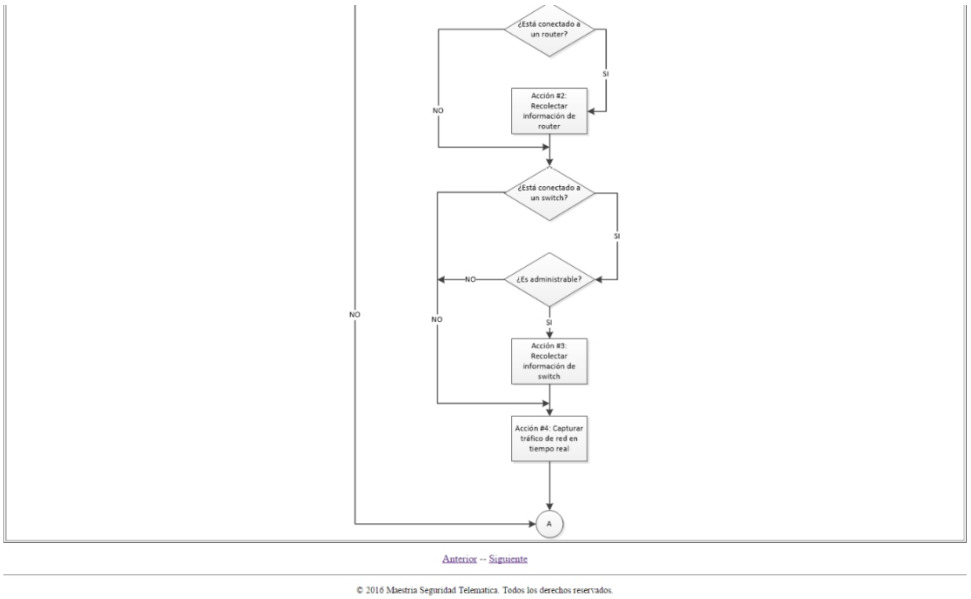


Figura 164-3: Página Diagrama Red parte 2 – app web

Realizado por: Luis Lema, 2016

En el gráfico del diagrama de flujo cada símbolo de decisión es un enlace hacia otra página, donde se puede elegir una respuesta entre "SI" o "NO", dependiendo de la respuesta que se elija, se irá a una nueva página ya sea de una acción o de otra toma de decisión. Por ejemplo, al dar click en el primer símbolo de toma de decisión llamado "¿Está conectado a una red?", aparece la siguiente pantalla:

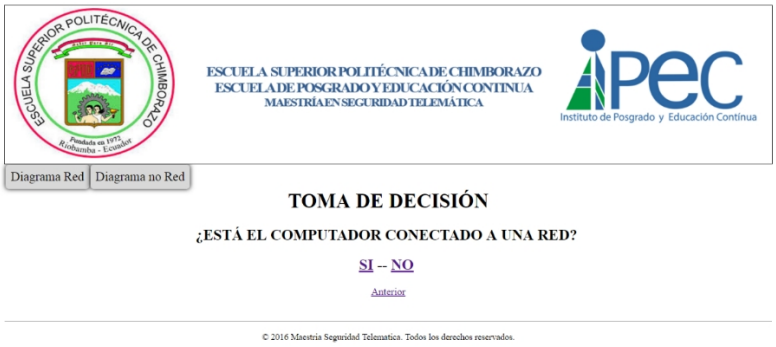


Figura 165-3: Página toma de decisión– app web

Realizado por: Luis Lema, 2016

Si se elige la opción "SI" se irá a la página donde se encuentra la acción 1, si se elige "NO" se irá a la página donde está el diagrama de flujo para cuando el computador no está conectado a una red.

También está la posibilidad de elegir directamente una acción que se desee realizar, por ejemplo se puede dar click en el símbolo con la acción número 4 "Capturar tráfico de red en tiempo real", con lo que aparecerá la siguiente pantalla:

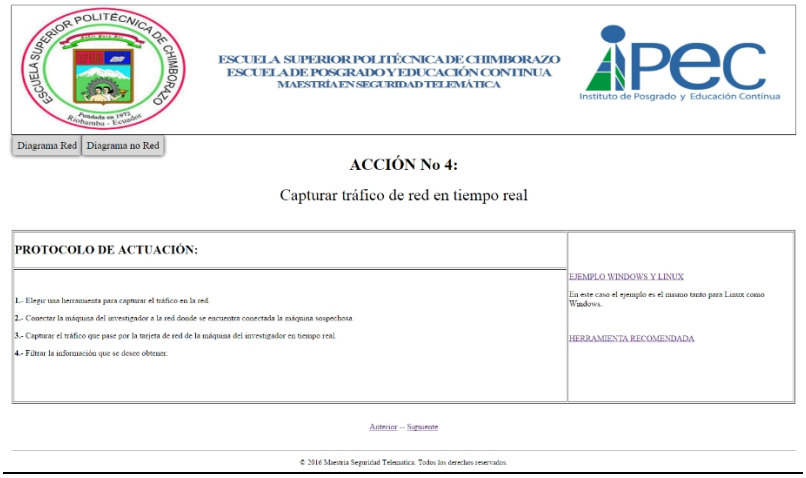


Figura 166-3: Página acción 4– app web

Realizado por: Luis Lema, 2016

En esta página se encuentra el protocolo de actuación correspondiente a la acción y al lado derecho enlaces para el ejemplo tanto para plataformas Windows y Linux, dependiendo del caso el ejemplo puede servir para las dos plataformas, también se encuentra el enlace a la página de la herramienta recomendada. En las siguientes imágenes se omitirán partes del contenido ya que es muy largo para mostrar.

Figura 167-3: Página acción 4 ejemplo– app web

Realizado por: Luis Lema, 2016

En la sección de "herramientas para captura de tráfico de red", se puede dar click en los enlaces proporcionados para descargar la herramienta mostrada.

En la sección del ejemplo se encuentran enlaces para dirigirse en la misma página a la parte especificada indicada, por ejemplo si se da clik al enlace "Capturar el tráfico que pase por la tarjeta de red de la máquina del investigador en tiempo real" se dirigirá a la sección correspondiente:

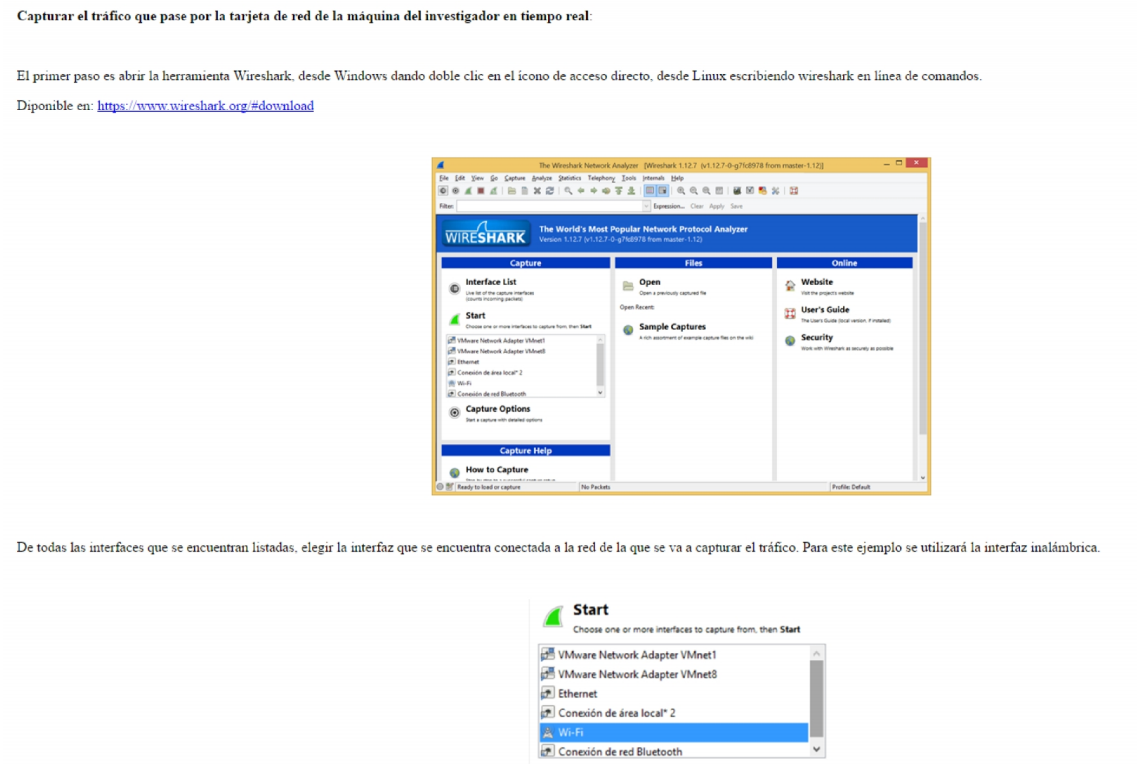


Figura 168-3: Página acción 4 secciones– app web

Realizado por: Luis Lema, 2016

Así es el funcionamiento de toda la aplicación web, dependiendo de la decisión o acción que se elija se abrirá una u otra página donde estará el protocolo de actuación, los ejemplos y la herramienta recomendada.

3.6. Definición de los escenarios de pruebas

Para el desarrollo de la prueba que a posterior comprobará o negará la hipótesis planteada, se tomaron en cuenta sus dos aspectos principales que son, la facilidad en la toma de decisiones y de la recolección y análisis de información.

La prueba consiste en dos partes: la primera en la revisión y análisis del "modelo para la toma de decisiones multicriterio como soporte para el análisis forense en dispositivos de almacenamiento digital" que se encuentra implementado en una aplicación web, por parte de los sujetos de prueba, la segunda parte consiste en realizar la acción correcta dependiendo del escenario que se plantee.

Hay que recalcar que a la segunda parte de la prueba pasarán solamente los sujetos, que una vez presentado el escenario tomen la decisión correcta de que acción realizar

basándose en la revisión y análisis previo que hicieron al modelo de análisis forense propuesto.

3.6.1. Escenario propuesto

El escenario que se creó para la implementación de la prueba fue el siguiente:

- Máquina conectada a una red privada donde se tenía solo acceso a los computadores y no a otros dispositivos como: switches, routers u otros computadores.
- Sistema operativo instalado Linux, en su distribución Fedora.
- Computador y monitor encendidos.

Los sujetos de prueban tendrán 15 minutos para revisar la aplicación web donde se encuentra implementado el modelo para toma decisiones multicriterio como soporte para el análisis forense en dispositivos de almacenamiento digital, una vez que han revisado el modelo deben elegir que acción realizar para el escenario propuesto, dependiendo de su elección podrán o no seguir a la siguiente fase, para este caso la respuesta correcta es la acción número 4 (Adquisición de información volátil), ya que no se cuentan con los permisos necesarios para poder extraer información de switches o router ni tampoco se cuenta con otra máquina que tenga una tarjeta de red, ni el software necesario para realizar una captura de tráfico en tiempo real.

El tiempo dado para la segunda fue de 20 minutos teniendo en cuenta que esta tarea consta de 7 pasos que debían ser completados en su totalidad.

3.6.2. Población y muestra

Uno de los requisitos indispensables para elegir a la población es que los sujetos a ser sometidos a la prueba, tengan conocimientos sólidos de informática sobre todo redes y sistemas operativos, y que además tengan conocimientos ya sea teóricos o prácticos sobre lo que trata la informática forense.

Por lo que la población considera para esta investigación fueron un grupo de 25 estudiantes de 4to semestre de la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo, ya que se entiende que ellos tienen conocimientos sólidos de informática, y además conocimientos básicos sobre informática forense ya que recibieron un módulo de este tema en la materia de Sistemas Operativos que fue dictada por el director de esta investigación.

En este caso al ser la población pequeña se decidió realizar la prueba a las 25 personas, por lo que N=25.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Resultado de la prueba

De las 25 personas que participaron en la primera fase se obtuvo el siguiente resultado:

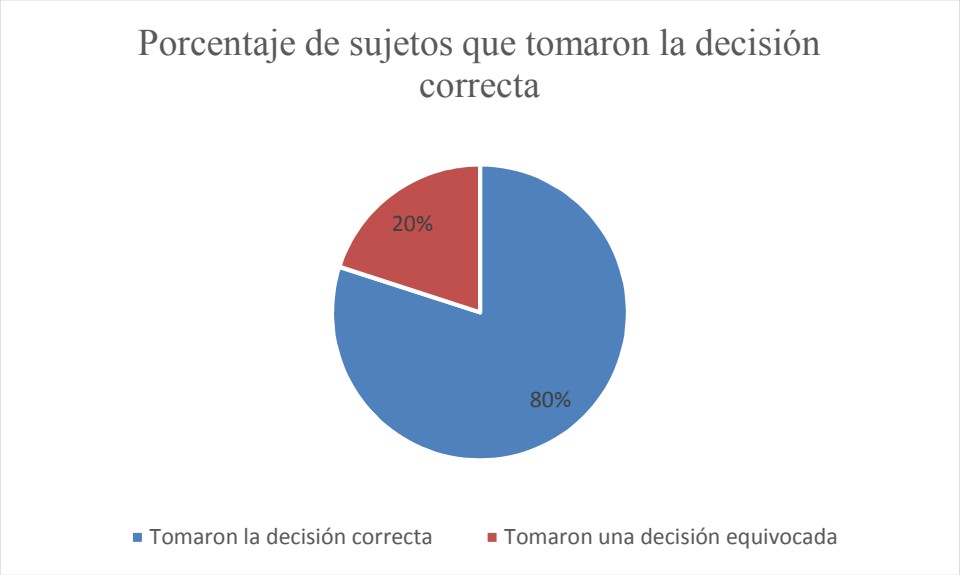


Gráfico 1-4: Porcentaje de sujetos que tomaron la decisión correcta

Realizado por: Luis Lema, 2016

Como se puede observar en el gráfico el 80% de los sujetos que revisaron la aplicación tomaron la decisión correcta de realizar la acción número 5, por lo que la segunda parte la realizaron solamente 20 personas.

Con las 20 persona que se realizaron la segunda parte se obtuvieron los siguientes resultados:

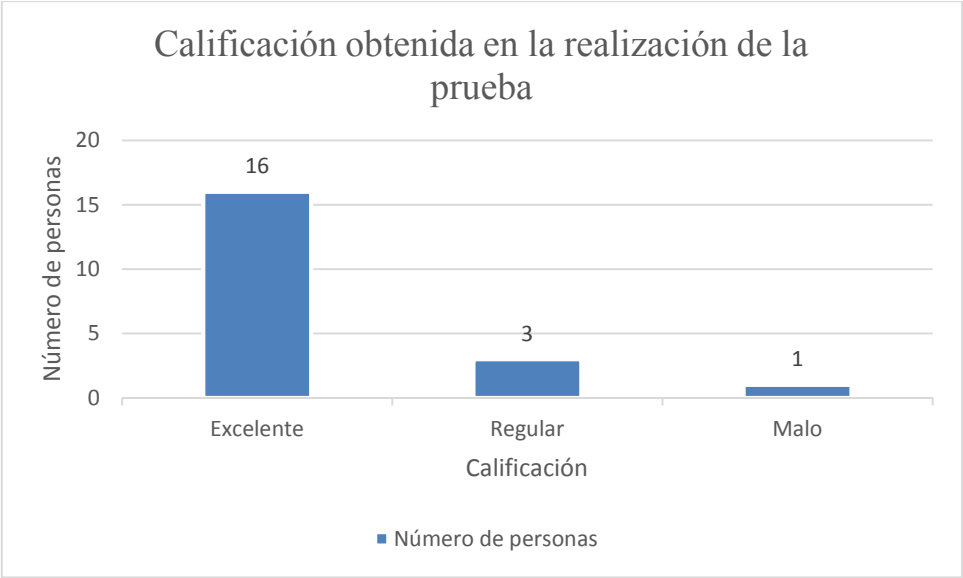


Gráfico 2-4: Calificación obtenida en la realización de la prueba

Realizado por: Luis Lema, 2016

La calificación se refiere al número de pasos que las personas terminaron de la tarea asignada, en este caso la acción número 5 (Adquisición de información volátil) consta de 7 pasos, por la que se dio la siguiente evaluación:

- Excelente, de 6 a 7 pasos completados.
- Regular, de 4 a 5 pasos completados.
- Malo, 3 o menos pasos completados.

Como podemos ver en el gráfico 16 personas obtuvieron una calificación excelente, eso equivale al 80% de los participantes evaluados, completaron los pasos de la tarea con un tiempo promedio de 14 minutos, el 15% que son 3 personas obtuvieron una calificación regular con tiempo promedio de 15 minutos.

También se preguntó a cada estudiante al finalizar la prueba el grado de dificultad en la realización de la tarea, obteniendo los siguientes resultados:

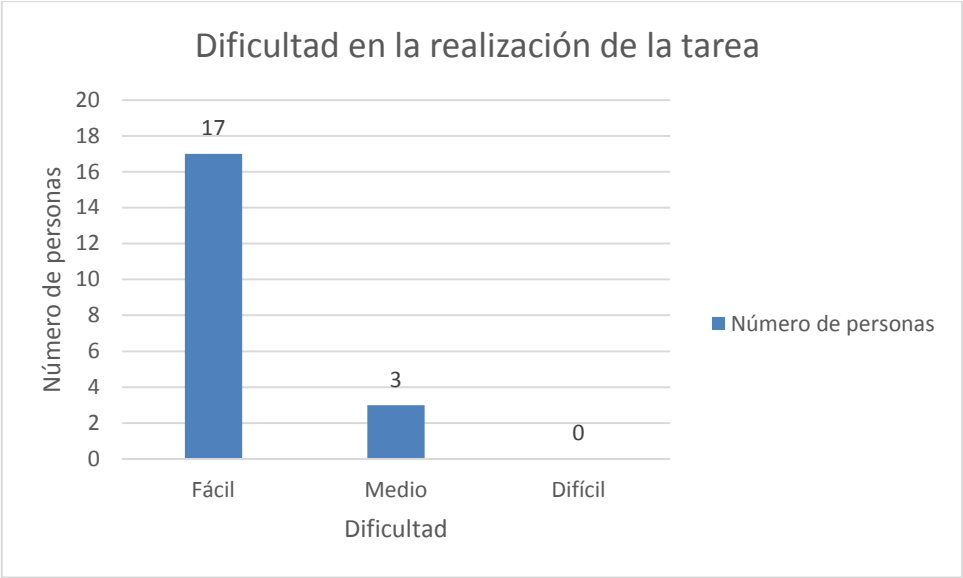


Gráfico 3-4: Dificultad en la realización de la tarea

Realizado por: Luis Lema, 2016

Se puede observar en el gráfico 17 personas respondieron que les pareció fácil realizar la tarea siguiendo los pasos que se encuentran en la aplicación en la web, y solamente 3 personas opinaron que tenía una complejidad media.

4.2. Comprobación de la hipótesis

Para la comprobación de la hipótesis planteada: "La implementación de un modelo como soporte para el análisis forense facilitará la toma de decisiones multicriterio en la recolección y análisis en dispositivos de almacenamiento digital", se aplicó el Chi Cuadrado, luego de haber realizado un análisis de los resultados obtenidos de la prueba aplicada a los estudiantes de la Facultad de Informática y Electrónica de la ESPOCH, se determinó que:

H_0: La implementación de un modelo como soporte para el análisis forense facilitará la toma de decisiones multicriterio en la recolección y análisis en dispositivos de almacenamiento digital.

H_1: La implementación de un modelo como soporte para el análisis forense **no** facilitará la toma de decisiones multicriterio en la recolección y análisis en dispositivos de almacenamiento digital.

Prueba de chi cuadrado:

Tabla 1-4: Calificación obtenida en la realización de la prueba

CALIFICACIÓN	Excelente	Regular	Malo	TOTAL
NÚMERO DE PERSONAS	16	3	1	20

Realizado por: Lui Lema, 2016.

Se desea probar para un nivel de significancia del 5%, $\alpha = 0.05$

Grados de libertad, df = (k-1)

$$\chi^2 = \frac{(f_0 - f_e)^2}{f_e}$$

$$f_e = P_i n = \frac{1}{3} * 20 = 6.6$$

$$\chi^2 = \frac{(16 - 6.6)^2}{6.6} + \frac{(3 - 6.6)^2}{6.6} + \frac{(1 - 6.6)^2}{6.6}$$

$$\chi^2 = 0.030$$

Según el valor chi calculado $\chi^2 = 0.030$ es menor que, el valor critico (5.99) con: df= (3-1)= 2, por lo que se acepta la hipótesis nula es decir: La implementación de un modelo como soporte para el análisis forense facilitará la toma de decisiones multicriterio en la recolección y análisis en dispositivos de almacenamiento digital.

La probabilidad:

El valor p = 0.10 es mayor que $\alpha = 0.05$, se acepta la hipótesis nula es decir: La implementación de un modelo como soporte para el análisis forense facilitará la toma de decisiones multicriterio en la recolección y análisis en dispositivos de almacenamiento digital.

4.3. Propuesta de trabajo futuro

En el presente trabajo se desarrolló una propuesta que aplica los conocimientos adquiridos durante la Maestría en Seguridad Telemática, para su realización han sido fundamental lo aprendido en las asignaturas que componen el plan de estudios de la misma. Dada la temática de este trabajo, las asignaturas que han contribuido de forma más notoria fueron: Seguridad en Sistemas Operativos, Auditoría y Delitos Informáticos y Computación Forense. También se desarrolló un prototipo simple de aplicación web basado en su mayoría en HTML, que contiene las acciones y tomas de decisiones para un análisis forense.

Como trabajo futuro se propone la creación de una herramienta de software que soporte la toma de decisiones basada en el uso de un motor de workflows como por ejemplo BONITA BPM (http://es.bonitasoft.com/). Para aumentar la efectividad y fiabilidad de una herramienta de este tipo, se podría complementarla con un sistema de análisis de decisión multicriterio, que facilite la optimización del proceso de análisis en función del valor potencial de la información obtenida y del costo asociado a su obtención.

CONCLUSIONES

- La aplicación del modelo para la toma de decisiones multicriterio como soporte para el análisis forense en dispositivos de almacenamiento digital, permitió que el 80% de la población que fue puesta a prueba logre completar las tareas que fueron asignadas, además el 85% calificó como de fácil uso a la guía que fue proporcionada.

- Emplear una metodología como la UNE 71506:2013 (Metodología para el análisis forense de las evidencias electrónicas) permite tener una referencia de trabajo estándar que facilita las tareas de análisis y adquisición de elementos informáticos dentro de un sistema de computación, que en lo posterior pueden ser usados como elementos en un peritaje.

- El desarrollo de una herramienta web como soporte al proceso de toma de decisiones en un análisis forense, ayuda asegurar que se aplique una correcta metodología al momento de recolectar información, por la que los resultados obtenidos después del análisis tendrán una gran solidez, esto de gran importancia ya que en un caso judicial estas pruebas deberán ser técnicamente validadas y sustentadas.

- Utilizar herramientas de software forense gratuitas revisadas previamente y garantizar que estas realicen las funciones que se desee, ya que al ser desarrolladas normalmente por otros investigadores y no empresas especializadas o dedicadas a la seguridad informática y/o forense, existe la posibilidad que realicen otro tipo de funciones que pueden perjudicar a la investigación.

RECOMENDACIONES

- Se recomienda utilizar metodologías estándares y herramientas flexibles, que se adapten al continuo cambio y actualización al que está sujeta la computación forense.

- Para tener acceso constante al modelo aquí propuesto se recomienda subir la aplicación web a un servicio de hosting al que se pueda acceder desde cualquier lugar de la web.

- No utilizar herramientas de software de dudosa procedencia ya que pueden contener virus e infectar la máquina que se está investigando.

- Cuando se esté adquiriendo información de un sistema Windows tratar de usar herramientas ejecutables ya que no alteran el registro del sistema, en el caso de Linux procurar usar binarios compilados por el mismo autor y no los del mismo sistema.

BIBLIOGRAFÍA:

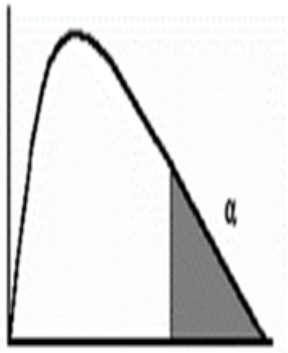
- **Acurio, S.** (2009). *Perfil Sobre los Delitos Informáticos en el Ecuador- Perfil de los Delitos Informaricos Ecuador*. Obtenido de http://app.ute.edu.ec/content/3254-42-10-1-6-7/Perfil%20de%20los%20Delitos%20Informaricos%20%20Ecuador%20-%20Fiscalia.pdf
- **Adams, R., Hobbs, V., & Mann, G.** (2014). The advanced data acquisition model (adam): a process model for digital forensic practice. *Journal of Digital Forensics, Security and Law*, pp. 25-48.
- **Alcance Libre.** (2013). *Gestión de RAID a través de MDADM*. Obtenido de www.alcancelibre.org/staticpages/index.php/como-mdadm
- **Calderón, R., Guzmán, G., Margarita, J., & Aranda, A.** (2012). *Diseño y plan de implementación de un Laboratorio de Ciencias Forenses.* Guayaquil: ESPOL. Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/17064/1/paper_laboratorio_forense_digital.pdf
- **Carrier, B., & Spafford, E.** (2003). Getting Physical with the Digital Investigation Process . *International Journal of Digital Evidence*, pp. 1-20.
- **Council of Europe.** (1 de Noviembre de 2001). Convenio sobre la Ciberdelincuencia. Budapest, Hungria. Obtenido de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c
- **CVE.** (2016). *Common Vulnerabilities and Exposures*. Obtenido de http://cve.mitre.org/
- **DragonJar.** (s.f.). *Foro Informatica Forense DragonJar*. Recuperado el Junio de 2015, de http://comunidad.dragonjar.org/f157/
- **EC-Council:CHFI.** (2015). *Computer Hacking Forensics Investigator v8*. Obtenido de https://www.eccouncil.org/
- **Fiscalía General del Estado.** (13 de Junio de 2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Obtenido de www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-informáticos-van-desde-el-fraude-hasta-el-espionaje.html

- **forensicswiki**. (1 de Julio de 2015). *Tools:Memory Imaging*. Obtenido de http://www.forensicswiki.org/wiki/Tools%3aMemory_Imaging
- **Gupta, D., & Mehtre, B.** (2013). Recent Trends in Collection of Software Forensics Artifacts: Issues and Challenges. En *Security in Computing and Comunications*. Springer Berlin Heidelberg. pp. 303-312
- **Hazan, R., Mahmood, S., & Raghav, A.** (2012). Overview on Computer Forensics Tools. *Control (CONTROL), UKACC International Conference on* Cardiff: IEEE. pp 400-403.
- **Iglesias Pérez, J.** (2013). *Windows Forense*. Obtenido de http://julioiglesiasp.blogspot.com/2013/09/windows-forense.html
- **López, J.** (2015). *minos-static*. Obtenido de https://github.com/minos-org/minos-static
- **Ministerio de Justicia, Derechos Humanos y Cultos.** (2014). Código Orgánico Integral Penal. *Código Orgánico Integral Penal*. Quito, Ecuador.
- **NirSoft.** (2015). *Freeware Utilities for Windows*. Obtenido de http://www.nirsoft.net/utils/index.html
- **RFC3227, I.** (Febrero de 2002). *Guidelines for Evidence Collection and Archiving*. Recuperado el 14 de Mayo de 2015, Obtenido de https://www.ietf.org/rfc/rfc3227.txt
- **Saari, E., & Jantan, A.** (2011). F-IDS: A Technique for Simplifying Evidence Collection in Network Forensics. En *Software Engineering and Computer Systems* Springer Berlin Heidelberg. pp. 693-701.
- **Sanchez, P.** (2013). *Forensics PowerTools (Listado de herramientas forenses)*. Obtenido de http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html
- **Symantec.** (2004). *Forensic Analysis of a Live Linux System*. Obtenido de http://www.symantec.com/connect/articles/forensic-analysis-live-linux-system-pt-1
- **UNE:71506.** (2013). *Metodología para el análisis forense de las evidencias electrónicas*. España.
- **Universidad de Washington.** (2015). *Basic Steps in Forensic Analysis of Unix Systems*. Obtenido de https://staff.washington.edu/dittrich/misc/forensics/

ANEXOS

ANEXO A:

Chi Cuadrado



Grados de libertad	α=.995	α=.99	α=.975	α=.95	α=.90	α=.10	α=.05	α=.025	α=.01	α=.005
1	0.0000	0.0002	0.0010	0.0039	0.0158	2.7055	3.8415	5.0239	6.6349	7.8794
2	0.0100	0.0201	0.0506	0.1026	0.2107	4.6052	5.9915	7.3778	9.2103	10.597
3	0.0717	0.1148	0.2158	0.3518	0.5844	6.2514	7.8147	9.3484	11.345	12.838
4	0.2070	0.2971	0.4844	0.7107	1.0636	7.7794	9.4877	11.143	13.277	14.860
5	0.4117	0.5543	0.8312	1.1455	1.6103	9.2364	11.070	12.833	15.086	16.750
6	0.6757	0.8721	1.2373	1.6354	2.2041	10.645	12.592	14.449	16.812	18.548
7	0.9893	1.2390	1.6899	2.1673	2.8331	12.017	14.067	16.013	18.475	20.278
8	1.3444	1.6465	2.1797	2.7326	3.4895	13.362	15.507	17.535	20.090	21.955
9	1.7349	2.0879	2.7004	3.3251	4.1682	14.684	16.919	19.023	21.666	23.589

ANEXO B:

PRUEBA PARA MEDICIÓN DE HIPÓTESIS:

TAREA:
Adquisición de información volátil.

La información volátil se refiere a los datos que se perderán o modificarán si se apaga o se reinicia el sistema.

INFORMACIÓN A RECOLECTAR:

No apagar o reiniciar el equipo de donde se va a recolectar la información.

La información que se necesita adquirir es la siguiente:

1.- Hora y Fecha del Sistema
2.- Usuarios Logueados
3.- Archivos Abiertos
4.- Información de procesos corriendo en memoria
5.- Puertos abiertos y la aplicación que los está usando
6.- Historial de comandos
7.- Realizar un volcado de la Memoria RAM.

PASOS A SEGUIR:

Para esta tarea la adquisición de información volátil se realizará en un sistema operativo Linux. Se necesita que se guarden los resultados obtenidos en un documento de texto.

Creación documento de texto:

Ingresar el comando “touch” seguido del nombre del documento de texto:

- touch resultados.txt

```
[root@LuisLema ~]# touch resultados.txt
```

Para comprobar que esta creado ingresar el comando “ls”:

- ls

```
[root@LuisLema ~]# ls
anaconda-ks.cfg              install.log         pruebas
anku-release-8-1.noarch.rpm  install.log.syslog  resultados.txt
```

Editar el documento e ingresar el texto “RESULTADOS OBTENIDOS”:

- echo "RESULTADOS OBTENIDOS" >> resultados.txt

```
[root@LuisLema ~]# echo "RESULTADOS OBTENIDOS" >> resultados.txt
```

Para ver el contenido del documento ingresar el comando “nano”, “vi” o “cat”

- cat resultados.txt

```
[root@LuisLema ~]# cat resultados.txt
RESULTADOS OBTENIDOS
```

Comandos:

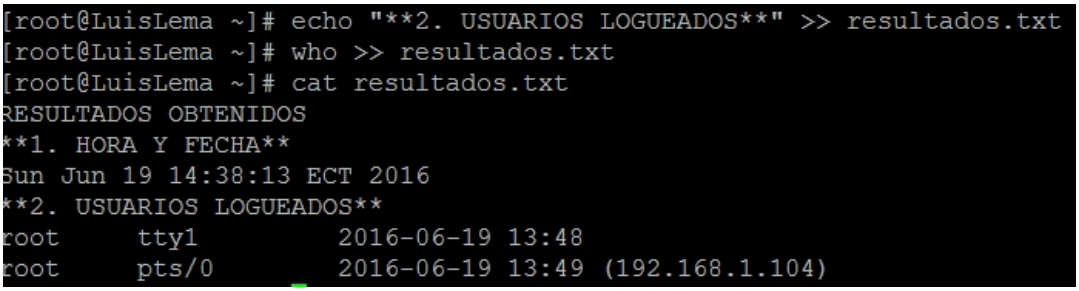
1.- Hora y fecha del sistema

- echo “**1. HORA Y FECHA**” >> resultados.txt
- date >> resultados.txt
- cat resultados.txt

```
[root@LuisLema ~]# echo "**1. HORA Y FECHA**" >> resultados.txt
[root@LuisLema ~]# date >> resultados.txt
[root@LuisLema ~]# cat resultados.txt
RESULTADOS OBTENIDOS
**1. HORA Y FECHA**
Sun Jun 19 14:38:13 ECT 2016
```

2.- Usuarios Logueados

- echo “**2. USUARIOS LOGUEADOS**” >> resultados.txt
- who >> resultados.txt
- cat resultados.txt

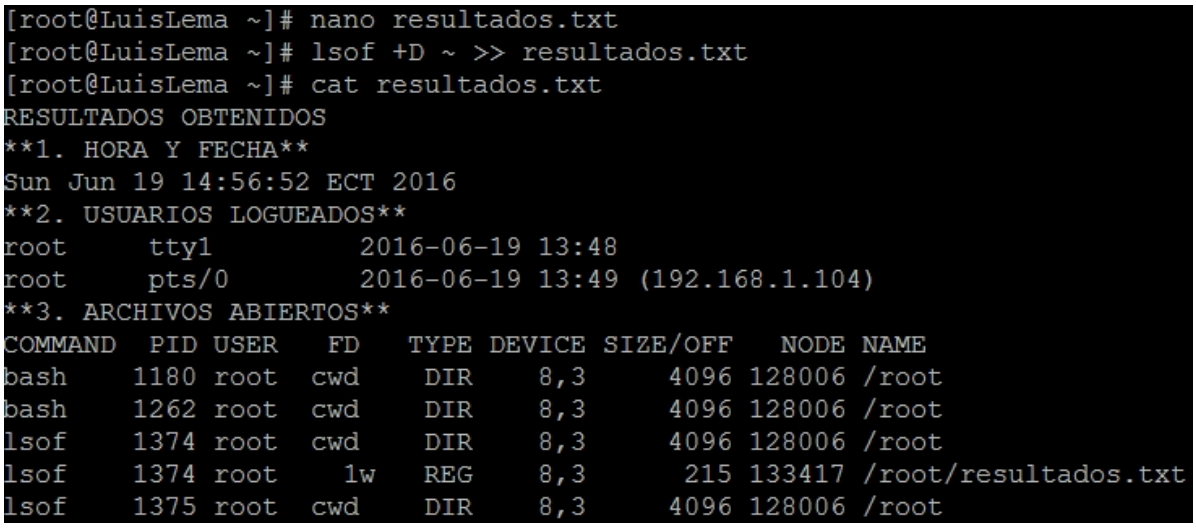


3.- Archivos Abiertos

En este caso se van a revisar los archivos abiertos en el home del usuario actual:

- echo “**3. ARCHIVOS ABIERTOS**” >> resultados.txt
- lsof +D ~ >> resultados.txt
- cat resultados.txt

La tilde de la ñ (~) se obtiene presionando alt+126



4.- Información de Procesos

- echo “**4. PROCESOS**” >> resultados.txt
- ps aux >> resultados.txt
- cat resultados.txt

```
[root@LuisLema ~]# echo "**4. PROCESOS**" >> resultados.txt
[root@LuisLema ~]# ps aux >> resultados.txt
[root@LuisLema ~]# cat resultados.txt
```

Ya que el archivo de texto cada vez es más grande y difícil de mostrar, a partir de este momento en las imágenes solo se mostrará parte del resultado.

```
**4. PROCESOS**
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root          1  0.0  0.2  19232  1496 ?        Ss   13:45   0:00 /sbin/init
root          2  0.0  0.0      0     0 ?        S    13:45   0:00 [kthreadd]
root          3  0.0  0.0      0     0 ?        S    13:45   0:00 [migration/0]
root          4  0.0  0.0      0     0 ?        S    13:45   0:00 [ksoftirqd/0]
root          5  0.0  0.0      0     0 ?        S    13:45   0:00 [stopper/0]
```

5.- Puertos abiertos y aplicación que los está usando

- echo “**5. PUERTOS ABIERTOS**” >> resultados.txt
- netstat -apn >> resultados.txt
- cat resultados.txt

```
[root@LuisLema ~]# echo "**5. PUERTOS ABIERTOS**" >> resultados.txt
[root@LuisLema ~]# netstat -apn >> resultados.txt
[root@LuisLema ~]# cat resultados.txt
```

```
**5. PUERTOS ABIERTOS**
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             Stat
e       PID/Program name
tcp        0      0 127.0.0.1:9000              0.0.0.0:*                   LIST
EN      1134/php-fpm
tcp        0      0 0.0.0.0:80                  0.0.0.0:*                   LIST
EN      1005/hiawatha
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LIST
EN      1045/sshd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LIST
```

6.- Historial de comandos

- echo “**6. HISTORIAL COMANDOS**” >> resultados.txt

- history >> resultados.txt
- cat resultados.txt

```
[root@LuisLema ~]# echo "**6. HISTORIAL COMANDOS**" >> resultados.txt
[root@LuisLema ~]# history >> resultados.txt
[root@LuisLema ~]# cat resultados.txt
```

```
**6. HISTORIAL COMANDOS**
    1  ifconfig
    2  dhclient
    3  ifconfig
    4  clear
    5  ifconfig
    6  yum update
    7  ifconfig
    8  ifconfig
    9  yum update
   10  yum install nano
   11  nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

7.- Volcado de Memoria

Para esta tarea no se va a guardar el resultado en el archivo de texto sino en otro fichero, ingresar los siguientes comandos, SE NECESITA PERMISOS DE ROOT:

- dd if=/dev/mem of=memoria.mem

Donde if= origen y of= destino, si no especifica un destino el archivo se guardara en el directorio que se está trabajando.

```
[root@LuisLema ~]# dd if=/dev/mem of=memoria.mem
dd: reading `/dev/mem': Operation not permitted
2056+0 records in
2056+0 records out
1052672 bytes (1.1 MB) copied, 0.0073549 s, 143 MB/s
```

Para comprobar que el archivo está guardado:

- ls

```
[root@LuisLema ~]# ls
anaconda-ks.cfg              install.log         memoria.mem  p.txt
anku-release-8-1.noarch.rpm  install.log.syslog  pruebas      resultados.txt
```

Finalmente capturar otra vez la hora y fecha del sistema:

- echo “**HORA FINAL**” >> resultados.txt
- date >> resultados.txt