UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

AUTOPSY 2 COMO HERRAMIENTA DE ANÁLISIS FORENSE

MATERIA:

ANÁLISIS DE SISTEMAS

INTEGRANTES:

N°	Apellidos	Nombres	Carnet	Participación
1	Rodríguez Rodríguez	Marbin Antonio	RR01132610	100%
2	González	Oscar Antonio	G01132991	100%
4	Mejia Barahona	Carlos Alberto	MB01132820	100%

DOCENTE:

LIC. JOSÉ LUIS ALVARADO AGUILAR

SAN SALVADOR 1 DE DICIEMBRE DE 2017

PRESENTACIÓN

Este perfil del trabajo final, pretende mostrar todos los aspectos generales que contendrá el documento del proyecto final, como proyecto, se pretende mostrar los aspectos fundamentales que tiene el software “Autopsy”, así como también los pasos a seguir para su correcta instalación y manejo.

Autopsy es una plataforma de interfaz gráfica para las herramientas de análisis forense digital que en sistemas Unix trabajo bajo la linea de comandos, este software es utilizado para investigar lo que sucedió en una computadora, tratar la información de discos duros e incluso se puede utilizar para recuperar información de una memoria USB. Autopsy es una interfaz intuitiva fácil de usar, esta basado en HTML, se puede conectar al servidor de Autopsy usando un navegador y en el se crea una interfaz de tipo ”Administrador de Archivos” que muestra detalles de los datos eliminados y las estructuras del sistema de archivos.

La utilización de un software para el manejo de evidencia forense, como “Autopsy”, permitirá obtener el conocimiento necesario para la gestión de la información de nuestros equipos de computo, así como también profundizar en el conocimiento de nuevas herramientas que nos permitan mantenernos al día con las técnicas que se utilizan en casos reales de delitos informáticos, así como también en el manejo de las evidencias informáticas forenses.

JUSTIFICACIÓN

En nuestros días, es de vital importancia conocer herramientas informáticas que nos permitan estar al tanto de lo que pasa o pasó en nuestros equipos de computo, es de todos sabido que las computadoras son vulnerables a miles de ataques a través de la Internet, ataques que pueden venir desde cualquier parte del mundo sin saber quien los provocó o para que, también no solo,estos ataques pueden venir de la Red, sino que también pueden darse o provocarse en nuestros mismos computadores, simplemente con dejar nuestra computadora encendida estamos siendo vulnerables a que cualquier persona pueda entrar en nuestros sistemas y archivos, y cambiar o modificar nuestros datos.

La utilización de herramientas para tratar las evidencias informáticas forenses, vienen a contribuir al conocimientos de técnicas que podemos poner en practica a la hora de tratar nuestra información en casos en los que queramos comprobar la veracidad de dichos datos, la implementación de un software como “Autopsy” es de gran ayuda para dar seguimiento a una investigación de un delito informático, ya sea que se requiera analizar un disco duro, una memoria o todo el computador, este software cubre con estas necesidades.

En tal sentido, este proyecto permitirá afianzar los conocimientos necesarios para el buen trato de la información en casos de delitos informáticos y también viene a reforzar el uso de herramientas informáticas dedicadas para fines específicos, lo cual abona al conocimiento y desarrollo técnicas para nuestro aprendizaje.

OBJETIVOS

OBJETIVO GENERAL

- Conocer de manera general el funcionamiento del software autopsy y cuales son su aportes a la informática forense.

OBJETIVOS ESPECÍFICOS

- Mostrar como se realiza la instalación del software de informática forense autopsy
- Enumerar las ventajas y desventajas que ofrece autopsy a la informática forense.
- Realizar un análisis básico de informática forense utilizando autopsy

ANTECEDENTES

El campo de la informática forense se inició en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores. En 1984, fue creado un programa del FBI. Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART (CART, del inglés computer analysis and response team), o análisis de informática y equipo de respuesta. Poco después, el hombre al que se le atribuye ser el "padre de la informática forense", comenzó a trabajar en este campo. Su nombre era Michael Anderson, y era un agente especial de la División de Investigación Criminal del IRS. Anderson trabajó para el gobierno en esta capacidad hasta mediados de 1990, tras lo cual fundó New Technologies, Inc., un equipo que lleva la firma forense.

Autopsy es una de las principales plataformas forense digital e interfaz gráfica de extremo a extremo. Construido por Basis Technology con las características que se espera de las herramientas forenses comerciales, Autopsy es una solución de investigación de disco duro rápida, completa y eficiente que evoluciona según sus necesidades.

MATERIALES Y MÉTODOS

1. Área de estudio: La investigación se realizara en las instalaciones de la Universidad Luterana Salvadoreña y en el hogar de cada miembro del equipo de expertos involucrados en al caso.

2. Materiales y equipos:

Materiales y Equipos	Descripción
3 Equipos portátiles	
Sistema Operativos Debian 8	
Autopsy	Herramienta libre que existe para el análisis de evidencia digital.
fdisk	Es un comando para manipular las particiones lógicas de una unidad físicas de almacenamiento.
dd	Es un comando de la familia de los sistemas operativos Unix, que permite copiar y convertir datos de archivos a bajo nivel, se utiliza para crear copias de seguridad de la información en crudo.
SleuthKit	Es una biblioteca y una colección de utilidades basadas en Unix y Windows para facilitar el análisis forense de los sistemas informáticos. Fue escrito y mantenido principalmente por el investigador digital Brian Carrier

3. Métodos y procedimientos:

La metodología a utilizar para la investigación estará basada en las directrices para la recopilación de evidencias y su almacenamiento descritas en el RFC3227.

Que dicta los siguientes procedimientos:

- Capturar una imagen del sistema tan precisa como sea posible.
- Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.
- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
- Recoger la información según el orden de volatilidad (de mayor a menor).
- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

THE SLEUTH KIT (TSK)

The Sleuth Kit (TSK) es una librería y colección de herramientas en línea de comando, la cual permite investigar imágenes de discos. La funcionalidad principal de TSK permite analizar datos del volumen y del sistema de archivos. El plug-in del Framework permite incorporar módulos adicionales para analizar contenidos de archivos y construir sistemas automatizados. La librería puede ser incorporada en herramientas digitales forenses más grandes y la línea de comando puede ser directamente utilizada para encontrar evidencia.

Instalacion: Para instalar The Sleuth Kit en Debian Jessie 8.1 se ejecuta el siguiente comando:

aptitude install sleuthkit

AUTOPSY 2

Autopsy 2 es una interfaz gráfica para las herramientas de análisis de investigación digital **Sleuth Kit** que se ejecuta en el navegador. Juntas estas dos herramientas permiten analizar discos Windows y UNIX, ademas de sistemas de Archivos(BTFS, FAT, EXT2/3).

aptitude install autopsy

COMO FUNCIONA AUTOPSY 2.

Como se ha mencionado anteriormente Autopsy 2 es una interfaz gráfica de la herramienta en lineas de comandos The Sleuth Kit, una vez instaladas ambas herramientas ya se puede realizar el informe forense.

Es necesario aclarar que Autopsy es una herramienta Cliente Servidor es necesario que el Servidor se este ejecutando para que se puede correr en el navegador la interfaz, autopsy escucha en el puerto 9999. Para iniciar el servicio de Autopsy se ejecuta el comando *autopsy* en consola.

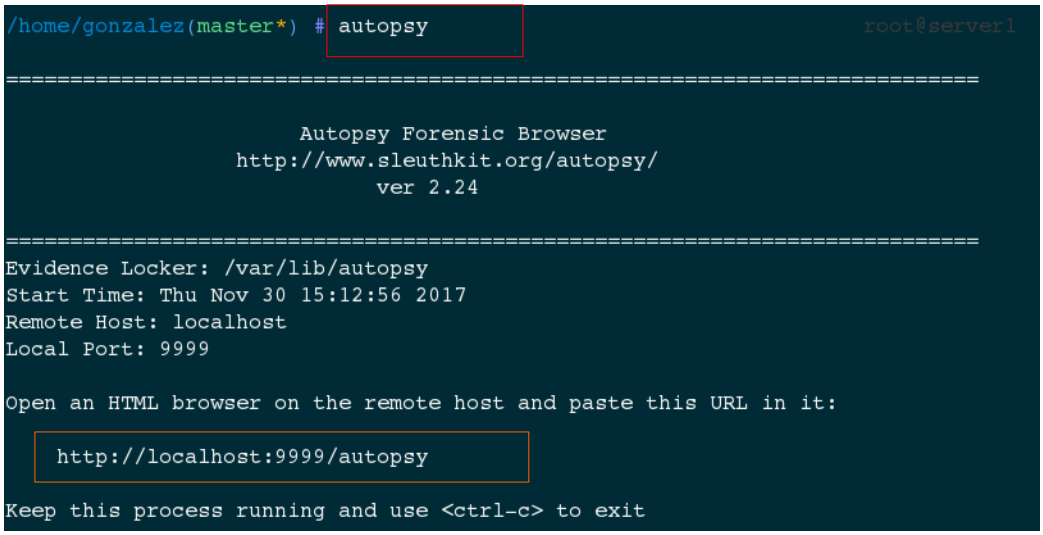


Ilustración 1: Iniciando el servicio Autopsy desde consola

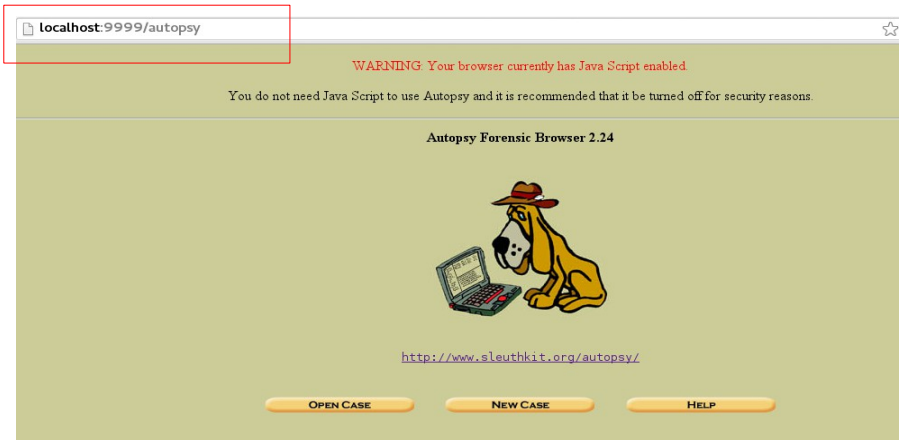


Ilustración 2: Autopsy corriendo en el navegador

RESOLVIENDO UN CASO PRACTICO CON AUTOPSY 2.

Para llevara cabo la resolución del análisis forense con autopsy 2 partamos del punto de que esta herramienta nos servirá para el análisis de datos a nivel de bits, autopsy ofrece una gran cantidad de información del dispositivo o disco que se este analizando pero con una leve desventaja, que es que se necesita tener un conocimiento avanzado de: cadenas hash, codigo ASCII, sectores de disco.

Además nos auxiliaremos de lagunas herramientas ajenas a SleuthKit y Autopsy, dichas herramientas se encuentran disponibles en los sistemas operativos basados en Linux. En este caso trabajaremos con una versión de Debian 8 Jesssie.

Se analizará un dispositivo USB, marca Kingston de 16 gb.

1. Usaremos el comando ***dd*** para clonar una imagen del dispositivo USB, esto con el afan de crear una copia exacta del dispositivo, esto con el afán de conservar la imagen del dispositivo original intacta. Para no cometer errores vemos primero los dispositivos conectados a nuestro equipo con el comando **fdisk.**

```
/home/gonzalez(master*) # fdisk -l

Disco /dev/sda: 232.9 GiB, 250059350016 bytes, 488397168 sectores
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
Tipo de etiqueta de disco: dos
Identificador del disco: 0x057272ce

Device     Boot Start       End   Sectors   Size Id Type
/dev/sda1  *     2048 468555775 468553728 223.4G 83 Linux

Disco /dev/sdb: 14.6 GiB, 15614803968 bytes, 30497664 sectores
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
Tipo de etiqueta de disco: dos
Identificador del disco: 0x00979dc8

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1  *     2048 30497663 30495616 14.6G  c W95 FAT32 (LBA)
```

Ilustración 3: Identificamos el dispositivo a analizar

Una vez identificado el dispositivo que será analizado procedemos a clonar la imagen del dispositivo, para este paso utilizaremos el comando dd.

```
/home/gonzalez(master*) # dd if=/dev/sdb1 of=/home/gonzalez/Recovery/copia_usb.dd
```

Ilustración 4: Clonando el dispositivo /dev/sdb1

Como observamos en la ilustración 4 hemos guardado una copia del dispositivo /dev/sdb1 en el directorio Recovery. La imagen creada se llamara copia_usb.dd y es con esta imagen que realizaremos nuestro trabajo de análisis forense para mantener sin alterar la unidad original.

Antes de iniciar el análisis forense es necesario algunos conceptos fundamentales para poder trabajar con Autopsy.

Tiempo de Modificación: Existe en sistemas de archivos UNIX y NTFS. Muestra la última vez en el cual se modificó el archivo de datos. En otras palabras, cuando fueron por última vez escritos datos hacia las unidades de datos asignadas para el archivo.

Tiempo de Escritura: Existe para sistemas de archivos FAT y es el tiempo cuando el archivo fue escrito por última vez. De los tres tiempo, este es el único valor requerido por la especificación FAT.

Tiempo de Acceso: Contiene el tiempo del último acceso del archivo de datos. Sobre una imagen FAT, este valor es opcional y es solo preciso al día (no horas y segundos).

Tiempo de Cambio: Existe para sistemas de archivos UNIX y NTFS. Es la última vez en el cual se cambió estado del archivo (o metadatos). Esto es diferente al tiempo de modificación, el cual trata con el archivo de datos, y este trata con los datos descriptivos en el inodo o entrada MFT.

Tiempo de Creación: NTFS y FAT. Cuando el archivo fue creado. (Opc).

ANÁLISIS DELA IMAGEN CREADA.

Como primer paso abrimos un nuevo caso en autopsy, dentro del cual importaremos la imagen .dd.
A continuación los pasos más importantes para crear un nuevo caso en Autopsy, dado que existe una enorme cantidad de material sobre como crear un nuevo caso con Autopsy en la red, nos enfocaremos en el análisis e interpretación de los datos que arroja Autopsy.

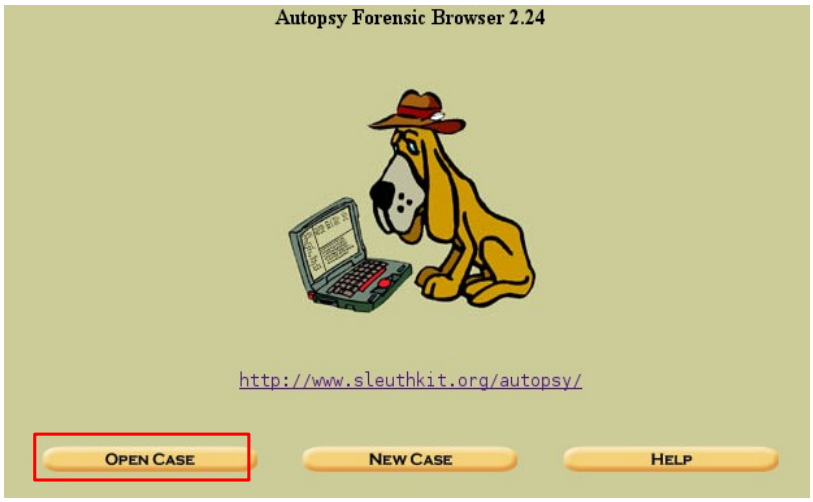
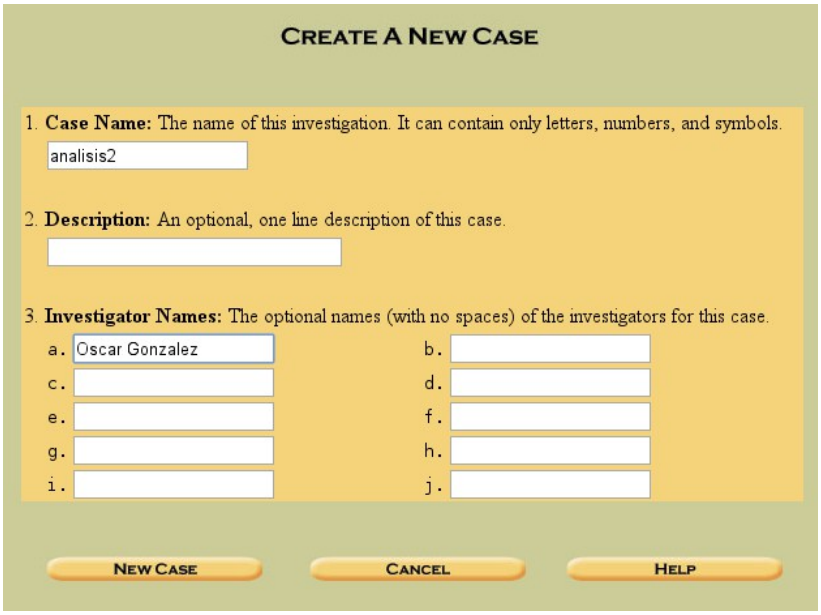


Ilustración 5: Seleccionamos la opción new case para crear un nuevo caso



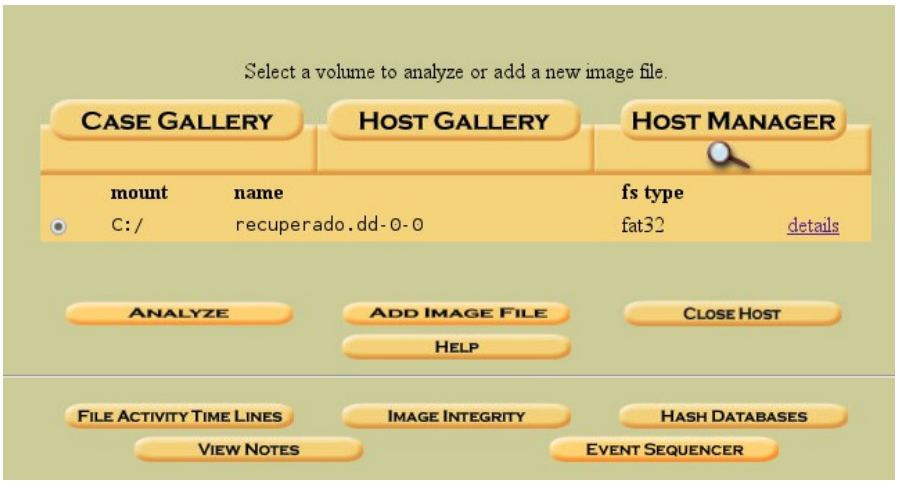


Ilustración 6: Agregamos la imagen forense

Una vez se ha creado un nuevo caso se generan archivos de configuracion y de logs, que pueden resultar muy utiles en el directorio /var/lib/autopsy. Allí encontraremos la información pertinente de cada caso.

```
/home/gonzalez(master*) # cd /var/lib/autopsy
-------------------------------------------------------------------
/var/lib/autopsy # ls
analisis  analisis2  autopsy.log  caso1  CasoPrueba  CasoUSB  demo1  demo2  USB
-------------------------------------------------------------------
/var/lib/autopsy # cd USB
-------------------------------------------------------------------
/var/lib/autopsy/USB # ls
case.aut  case.log  host1  investigators.txt
-------------------------------------------------------------------
```

Ilustración 7: Archivos de configuración e historial de cada caso

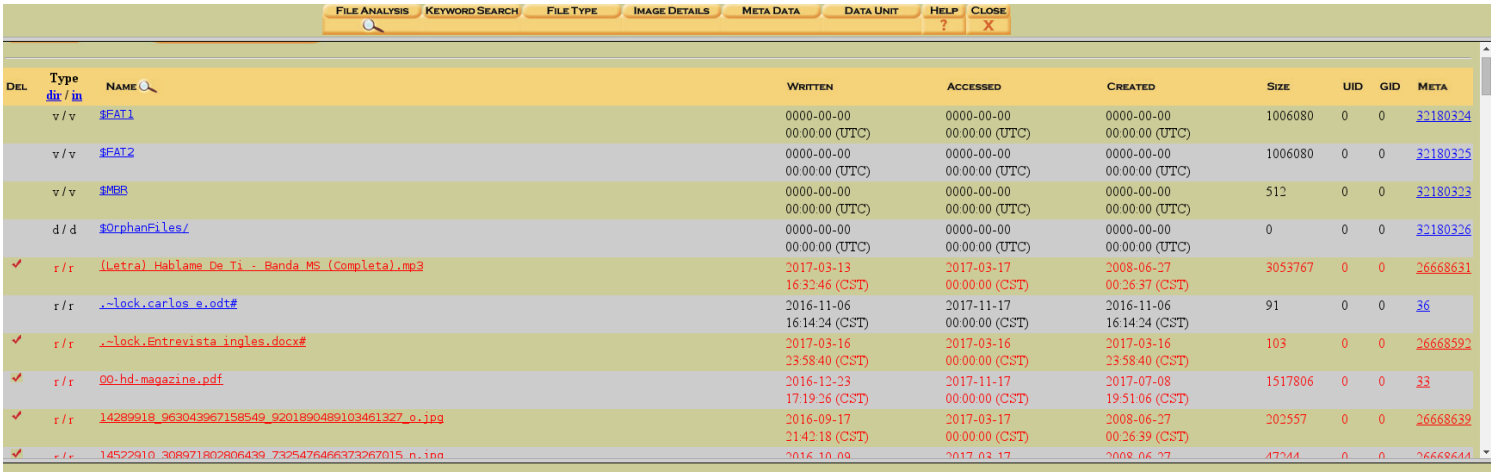


Ilustración 8: interfaz principal de Autopsy

De este modo visualizaremos el la organización de archivos que contiene la imagen que creamos del dispositivo original. Los archivos que aparecen en rojo son los archivos borrados.

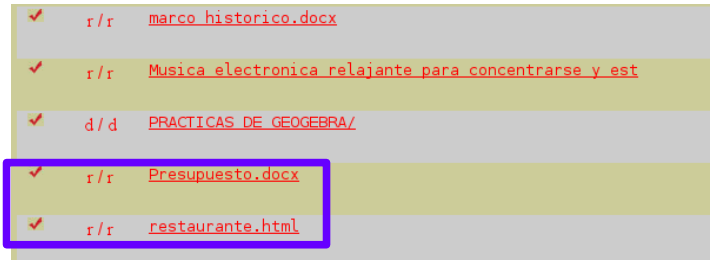


Ilustración 9: Archivo a analizar presupuesto.docx

Para el ejemplo de análisis tomaremos el archivo borrado presupuesto.

Para ver detalles básicos del archivo hacemos clic sobre el y nos dará información básica del elemento al elegir una de las opciones que nos ofrece Autopsy en su panel inferior.

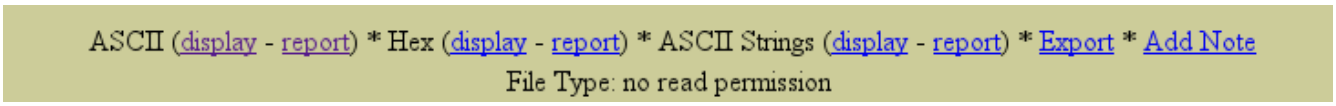


Ilustración 10: Panel de información del elemento

En la ilustración 10 tenemos las opciones en tres formatos distintos: ASCII. HEXADECIMAL Y ASCII strings. Al elegir la ***report*** de la opción ASCII nos mostrará datos como los q podemos ver en la ilustración 11.

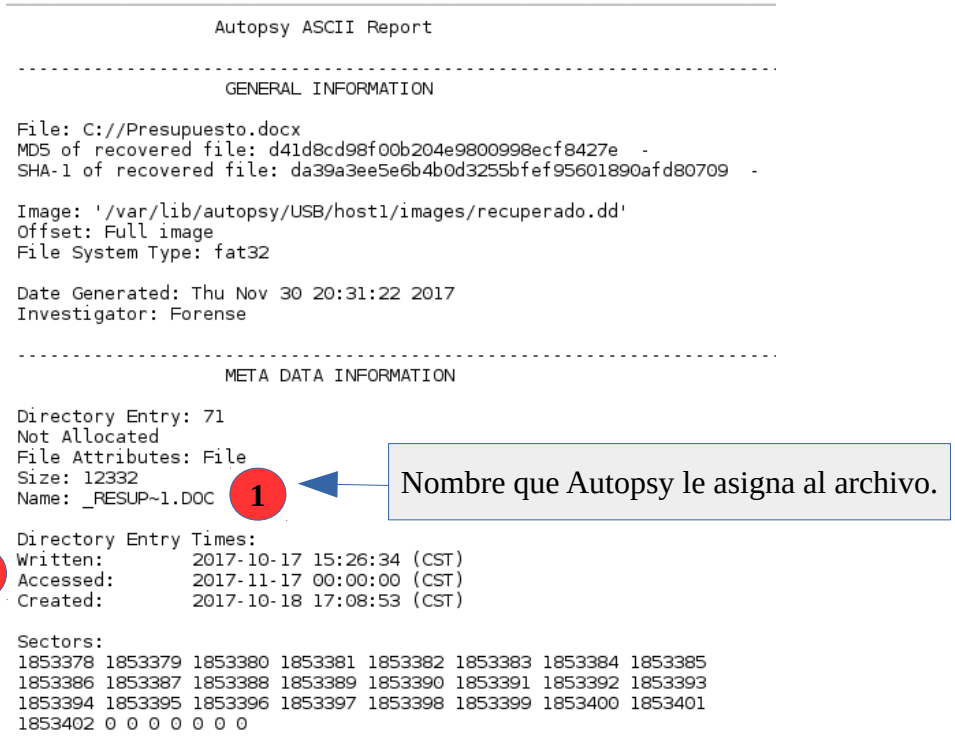


Ilustración 11: Reporte ASCII

Tiempo de Escritura: Tiempo en que se escribió por ultima vez en el fichero.
Acceso: Última vez que se accedió al archivo.
Creación: Fecha en que el elemento fue creado.

Como se ha señalado anteriormente el punto fuerte de Autopsy no es la recuperación de elementos borrados, si no el análisis a nivel de meta datos, en este caso práctico trataremos de recuperar el archivo presupuesto.docx, una de las características es que Autopsy nos permite recuperar incluso aquellos archivos que estén dañanos.

El siguiente paso de nuestro análisis será la revision de metadatos del archivo presupuesto.docx. Eso lo buscamos en la opcion **DATA UNIT,** el resultado sera como el que se muestra en la ilustración 12.

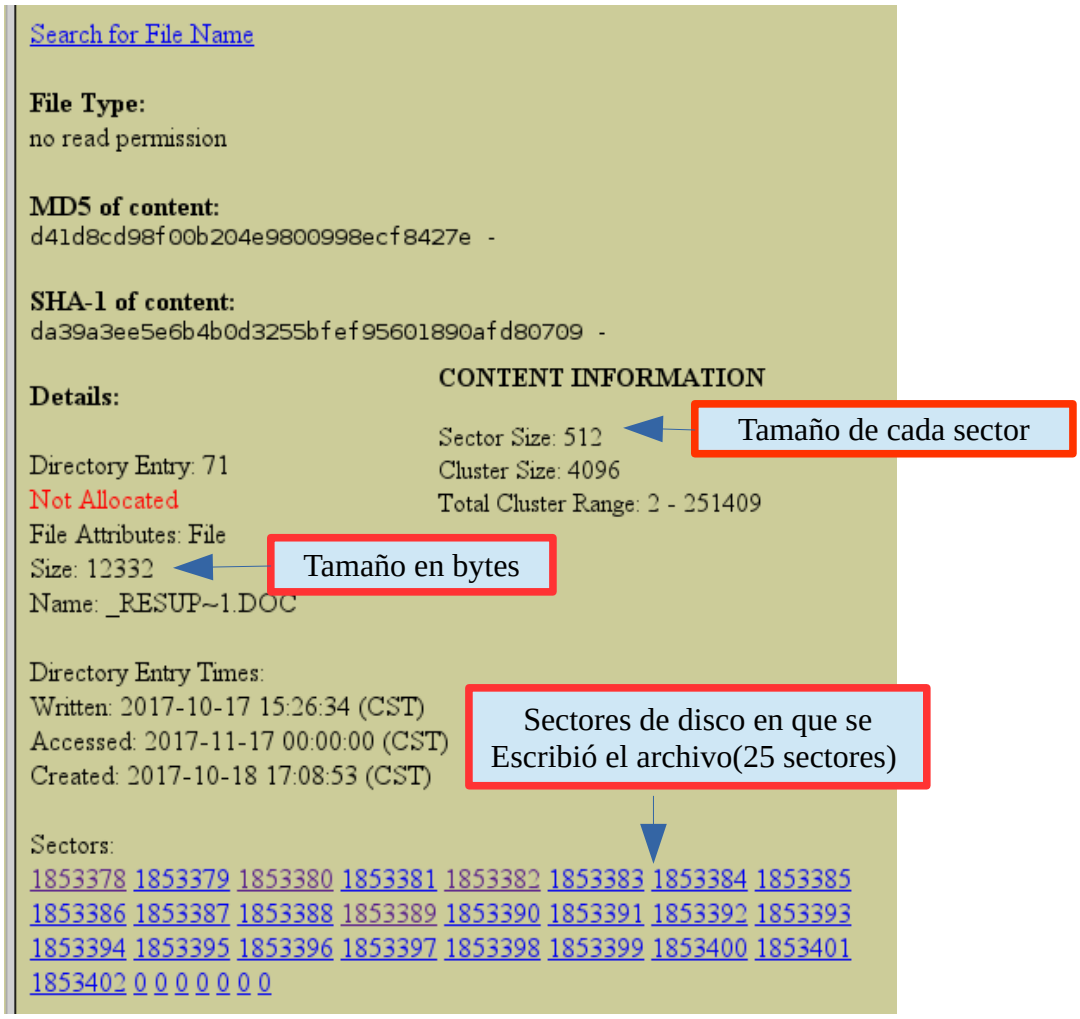


Ilustración 12: Metadatos

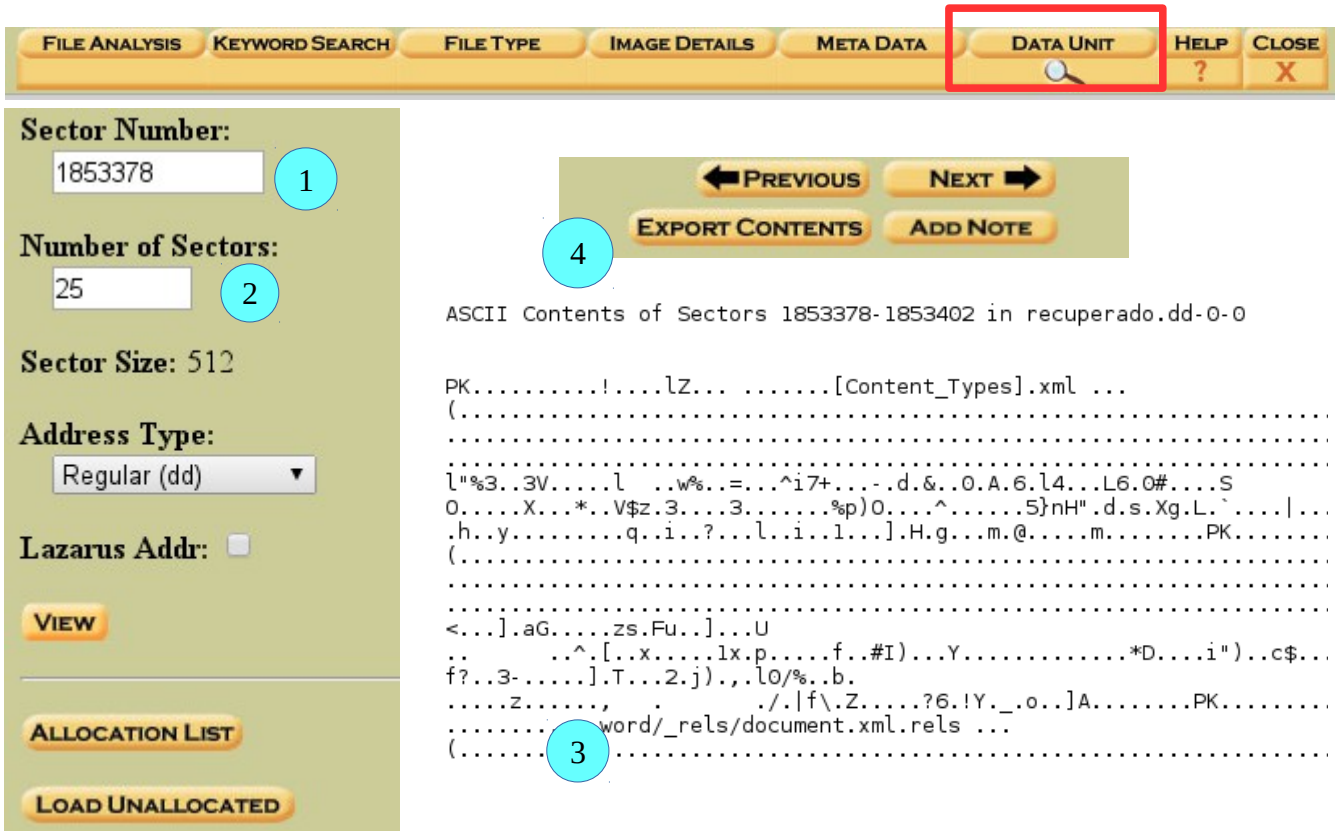
Estos datos son de suma importancia, la imagen muestra en primer lugar el tamaño de cada sector del dispositivo, como se sabe toda unidad de almacenamiento se divide en sectores de almacenamiento. En nuestro caso en particular vemos que cada sector tiene un tamaño de **512 bytes**, y que el archivo que estamos analizando tiene un tamaño de **12332 bytes,** y que esta escrito a partir del sector **1853378** hasta el **1853402.**

Al hacer una simple operación aritmética podemos ver el numero de sectores que ocupa ese archivo. Para ello dividimos el tamaño del archivo entre el tamaño de cada sector.

12332/512=24.0859

Eso es correcto ya que si contamos manualmente vemos que este archivo ocupa **25 sectores**.

Para recuperar un archivo vamos a extraer toda la información contenida en los sectores en que esta escrita la información. Paea esos lo hacemos desde la opción DATA UNIT.



1. Le indicamos a partir de cual sector deseamos extraer información.
2. Cuantos sectores deseamos Extraer.
3. Nos muestra que es un tipo de documento word, esto es importante ya que Autopsy nos exportara la información en un archivo .raw, este formato es un tipo de archivo con información en bruto o en crudo. Luego deberemos cambiar la extensión manualmente, como sabemos que se trata de un documento tipo word lo cambiaremos por un .doc o .docx.

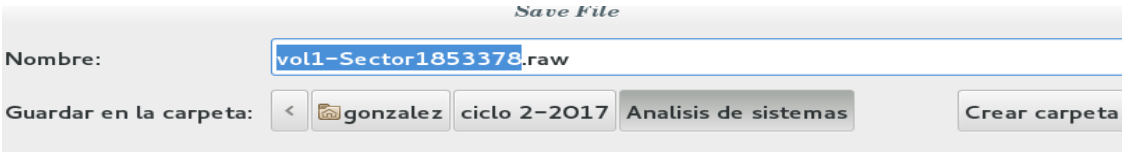
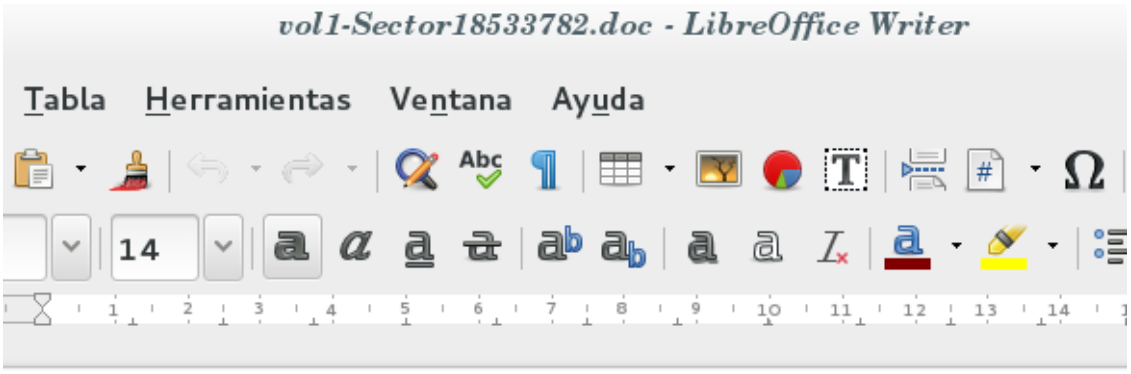


Ilustración 13: Exportando los datos en bruto.

Ilustración 15: Cambiando la extensión

Ilustración 14: Archivo con nueva extensión

Procedemos a verificar la información que contiene el archivo recuperado.



PRESUPUESTO

Fotocopias	$18.00
Horas de navegación	$10.00
Impresiones	$20.00
Anillado	$5.00
Papelería	$4.00
Total	$57.00

Ilustración 16: Archivo recuperado

BIBLIOGRAFÍA

http://software-libre-if.blogspot.com/p/tutorial-de-autopsy.html
http://www.reydes.com/archivos/slides/webinars/AC_WG_AnalisisForenseAutopsy2.pdf
https://www.youtube.com/watch?v=P59W3BNR2U0