

Análisis Forense con Autopsy 2

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: ReYDeS@gmail.com

Jueves 5 de Marzo del 2015

Presentación

Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Miembro de Open Web Application Security Project (OWASP).

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de doce años de experiencia en el área y desde hace ocho años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, presentándose también constantemente en exposiciones enfocadas a, Hacking Ético, Informática Forense, GNU/Linux y Software Libre.



@Alonso_ReYDeS



www.facebook.com/alonsoreydes



pe.linkedin.com/in/alonsocaballeroquezada/



The Sleuth Kit

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.



```
sansforensics@siftworkstation:~$ sudo istat -f ntfs -o 8064 /dev/sdc 35-128-1
MFT Entry Header Values:
Entry: 35          Sequence: 2
$LogFile Sequence Number: 16782355
Not Allocated File
Links: 2

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 261 ( )
Created:          2014-05-12 09:04:26 (PET)
File Modified:   2014-03-30 09:23:45 (PET)
MFT Modified:    2014-05-12 09:04:26 (PET)
Accessed:        2014-05-12 09:04:26 (PET)
```

Autopsy 2

Autopsy 2 es una interfaz gráfica para las herramientas de análisis de investigación digital en línea de comando The Sleuth Kit. Juntas pueden analizar discos Windows y UNIX, además de sistemas de archivos (BTFS, FAT, UFS1/2, Ext2/3).

The Sleuth Kit y Autopsy 2 son ambos open source y se ejecutan en plataformas UNIX. Como Autopsy 2 se basa en HTML, se puede conectar al servidor Autopsy desde cualquier plataforma utilizando un navegador HTML. Autopsy proporciona una interfaz como un “Gestor de Archivo”, y muestra detalles sobre datos eliminados y estructuras del sistema de archivos.

Modos de Análisis

- Análisis en Reposo
- Análisis en Vivo



Modos del Navegador

Archivos: Permite navegar el sistema de archivos y visualizar contenidos.

Meta Datos: Permite examinar las estructuras de metadatos.

Unidades de Datos: Permite navegar por número de bloque.

Búsqueda de Palabras Clave: Busca una cadena utilizando grep(1).

Detalles de la Imagen: Detalles sobre el sistema de archivos o volumen.

Integridad de la Imagen: Se puede verificar en cualquier momento.

Cronología sobre Actividad de los Archivos: Cronologías en Base a tiempos (MAC) Modificado, Accedido, Cambiado (Creado en FAT/NTFS).

Categorías por Tipo de Archivo: Ordenar archivos basado en su tipo.

Generación de Reporte: Cada una de las técnicas permite generarlo

Análisis de Archivo (Conceptos)

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 de Meta Datos (Conceptos)

Este modo permite al investigador visualizar los detalles de las estructuras de metadatos. Las estructuras de metadatos sobre las estructuras del disco los cuales contienen los detalles del archivo, como tiempos y punteros hacia las unidades de datos asignadas. Los sistemas de archivos FFS y EXT2FS los llama estructuras inodos, los sistemas de archivos NTFS los llama entradas MFT (Master File Table) o Entradas de de Archivo, y el sistema de archivos FAT los llama entradas de directorios.

Este modo es útil para recuperar datos y obtener una visión detallada del archivo.

Para visualizar el contenido de una estructura únicamente se debe ingresar su dirección.

También es factible visualizar el estado de asignación de estructuras de metadatos en grupos de 500.

Análisis de Unidades de Datos (Conceptos)

Este modo permite al investigador visualizar el contenido de unidades de datos individuales. Las unidades de datos son un término genérico utilizado para describir las áreas del disco utilizadas para almacenar datos. Cada sistema de archivos nombra de manera diferente a una unidad de datos (Por ejemplo, Fragmentos o Clusters).

Este modo es muy útil cuando se requiere recuperar y analizar datos borrados.

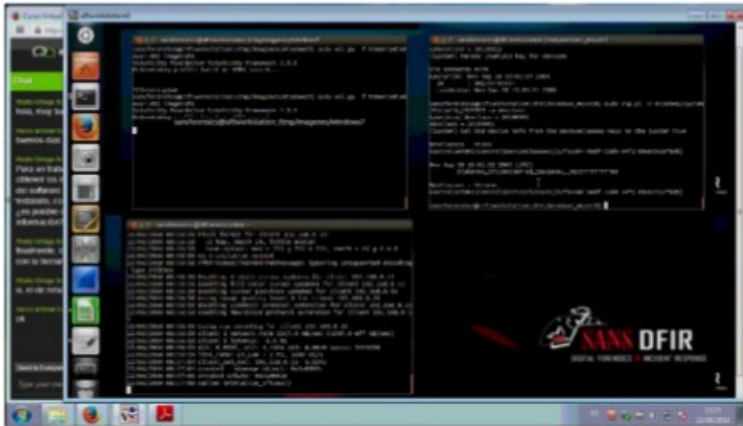
Por defecto solo se mostrará una unidad de datos. Para visualizar más de una unidad consecutiva, definir el número de unidades.

El contenido de las unidades de datos pueden ser visualizados en formatos de cadenas, volcado hexadecimal, o ASCII.

Es factible también mostrar la dirección y nombre de archivo asignada a la unidad, encontrando su estructura de meta datos.

Curso Virtual de Informática Forense

2015



Grupo Sábado:

7, 14, 21 y 28 de Marzo del 2015
De 3:30pm a 7:15pm (UTC -05:00)

Grupo Domingo:

8, 15, 22 y 29 de Marzo del 2015
De 9:00am a 12:45pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:



Más Información: http://www.reydes.com/d/?q=Curso_de_Informatica_Forense

E-mail: caballero.alonso@gmail.com / Sitio Web: <http://www.reydes.com>

Mas Contenidos

Videos de 24 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

<http://www.reydes.com/d/?q=videos>

Diapositivas utilizadas en los Webinars Gratuitos.

<http://www.reydes.com/d/?q=node/3>

Artículos y documentos publicados

<http://www.reydes.com/d/?q=node/2>

Mi Blog sobre temas de mi interés.


<http://www.reydes.com/d/?q=blog/1>



Alonso Caballero Quezada / ReYDeS Documentos Eventos Cursos Blog Contacto

Servicio Independiente de Hacking Ético

Presentación



Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Miembro de Open Web Application Security Project (OWASP). Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de once años de experiencia en el área y desde hace siete años labora como consultor e Instructor Independiente en las áreas de Hacking

Cursos

- Curso de Hacking Ético
- Curso de Hacking Aplicaciones Web
- Curso de Informática Forense
- Curso de Hacking con Kali Linux
- Curso Forense de Autopsy 3

MI Blog

- Crear una Puerta Trasera Persistente utilizando Meterpreter
- Trazado de Rutas en Paralelo utilizando Scapy
- Automatizar un Ataque MITM para Recolectar Credenciales utilizando Subterfuge

Demostraciones

The screenshot displays a web-based forensic analysis tool. The browser address bar shows the URL: `http://localhost:9999/autopsy?mod=1&submod=2&case=IRFDS&host=host1&inv=unknown&vol=v`. The interface includes a navigation menu with tabs for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. The main area is divided into a sidebar and a main content area.

Directory Seek
Enter the name of a directory that you want to view.
C: /

File Name Search
Enter a Perl regular expression for the file names you want to find.

Permissions	File Name	Creation Time	Last Modified	Accessed	Size	Blocks	Used Blocks	File ID
d / d	Archivos de programa/	2011-09-13 09:29:50 (PET)	2011-09-13 09:29:50 (PET)	2011-09-13 09:29:50 (PET)	48	0	0	16924-144-
r / r	autoexec.bat	2009-06-10 16:42:20 (PET)	2009-07-13 21:04:04 (PET)	2011-09-13 04:09:49 (PET)	24	0	0	9738-128-1
d / d	Boot/	2011-09-13 04:20:46 (PET)	2011-09-13 04:20:46 (PET)	2011-09-13 04:20:46 (PET)	56	0	0	42280-144-
r / r	bootmgr	2009-07-13 20:38:58 (PET)	2011-09-13 04:20:45 (PET)	2011-09-13 04:20:45 (PET)	383562	0	0	42333-128-
r / r	BOOTSECT.BAK	2011-09-13 04:20:47 (PET)	2011-09-13 04:20:47 (PET)	2011-09-13 04:20:47 (PET)	8192	0	0	42344-128-
r / r	config.sys	2009-06-10 16:42:20 (PET)	2009-07-13 21:04:04 (PET)	2011-09-13 04:09:49 (PET)	10	0	0	9741-128-1
d / d	Documents and	2009-07-13	2009-07-13	2011-09-13	48	0	0	9743-144-1

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [Add Note](#)

File Type: x86 boot sector, code offset 0x52, OEM-ID "NTFS ", sectors/cluster 8, reserved sectors 0, Media descriptor 0xf8, heads 255, hidden sectors 2048. dos < 4.0 BootSector (0x80)

Hex Contents Of File: C:/BOOTSECT.BAK

```
00000000: EB52 904E 5446 5320 2020 2000 0208 0000   .R.NTFS   .....
00000010: 0000 0000 00F8 0000 3F00 FF00 0008 0000   .....?.....
00000020: 0000 0000 8000 8000 FFEF 7F02 0000 0000   .....
00000030: 0000 0C00 0000 0000 0200 0000 0000 0000   .....
00000040: F600 0000 0100 0000 C028 8ACC 608A CCE8   .....(.....
00000050: 0000 0000 FA33 C08E D0BC 007C FB68 C007   .....3....|.h..
00000060: 1F1E 6866 00CB 8816 0E00 6681 3E03 004E   ..hf.....f.>..N
00000070: 5446 5375 15B4 41BB AA55 CD13 720C 81FB   TFSu..A..U..r...
00000080: 55AA 7506 F7C1 0100 7503 E9DD 001E 83EC   U.u.....u.....
00000090: 1868 1A00 B448 8A16 0E00 8BF4 161F CD13   .h...H.....
000000A0: 9F83 C418 9E58 1F72 E13B 060B 0075 DBA3   ....X.r.;...u..
000000B0: 0F00 C12E 0F00 041E 5A33 DBB9 0020 2BC8   .....Z3...+.
000000C0: 6655 8614 8003 1605 8005 6A55 8616 8005   f
```

Análisis Forense con Autopsy 2

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: ReYDeS@gmail.com