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 Mazo 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)
```

* http://www.sleuthkit.org/sleuthkit/

Autopsy 2

Autopsy 2 es una interfaz gráfica para las herramientas de análisis de investigación digital en linea 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

* http://www.sleuthkit.org/autopsy/v2/

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

* http://www.sleuthkit.org/autopsy/help/index.html

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.

* http://www.sleuthkit.org/autopsy/help/meta_mode.html

Análisis de Unidades de Datos (Conceptos)

Este modo permite al investigador visualiza el contenido de unidades de datos individuales. Las unidades de datos son un termino 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.

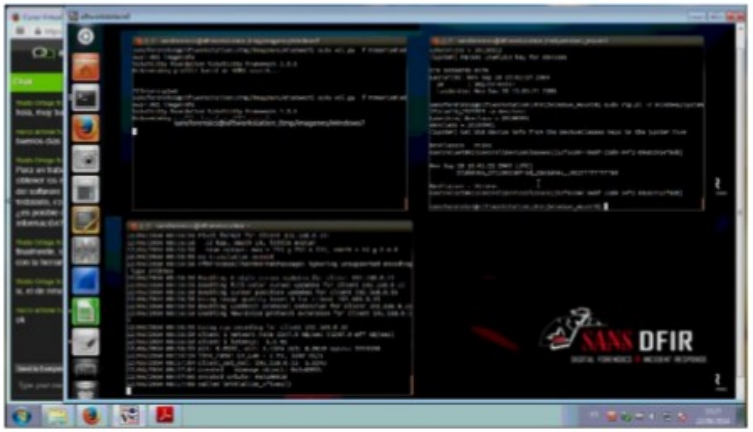
Es factible también mostrar la dirección y nombre de archivo asignada a la unidad, encontrando su estructura de meta datos.

* http://www.sleuthkit.org/autopsy/help/data_mode.html

Curso Virtual de Informática Forense

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

Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

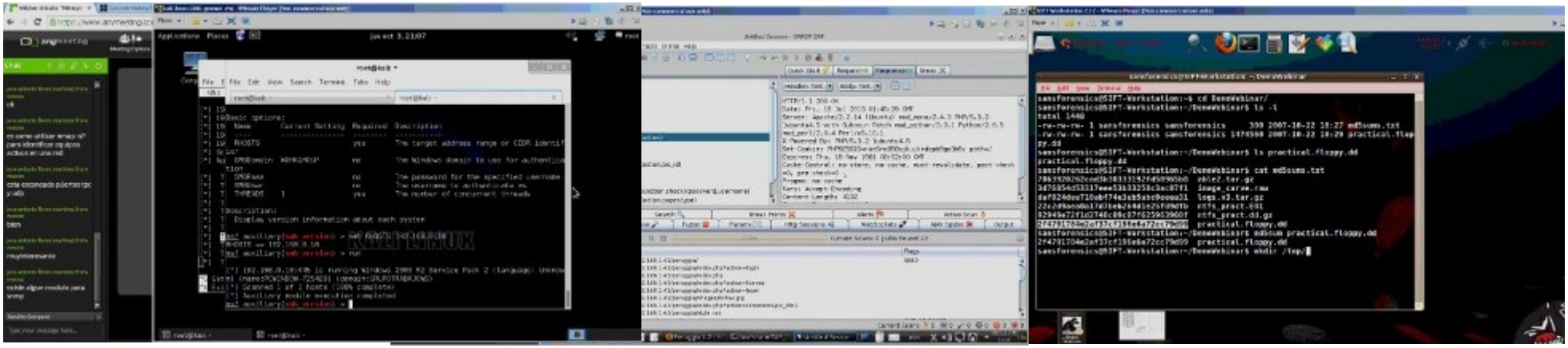
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

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



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.

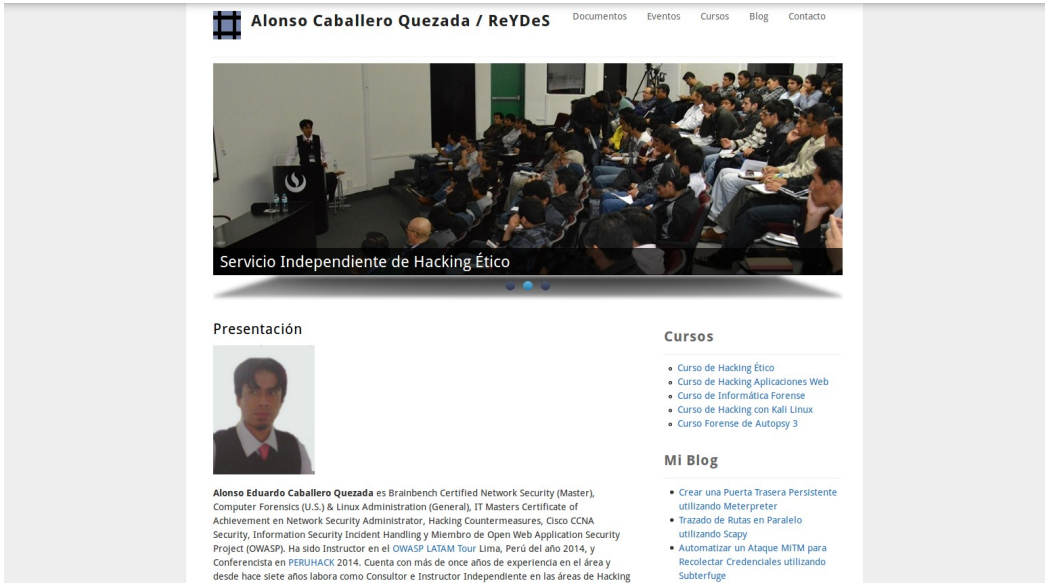
http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

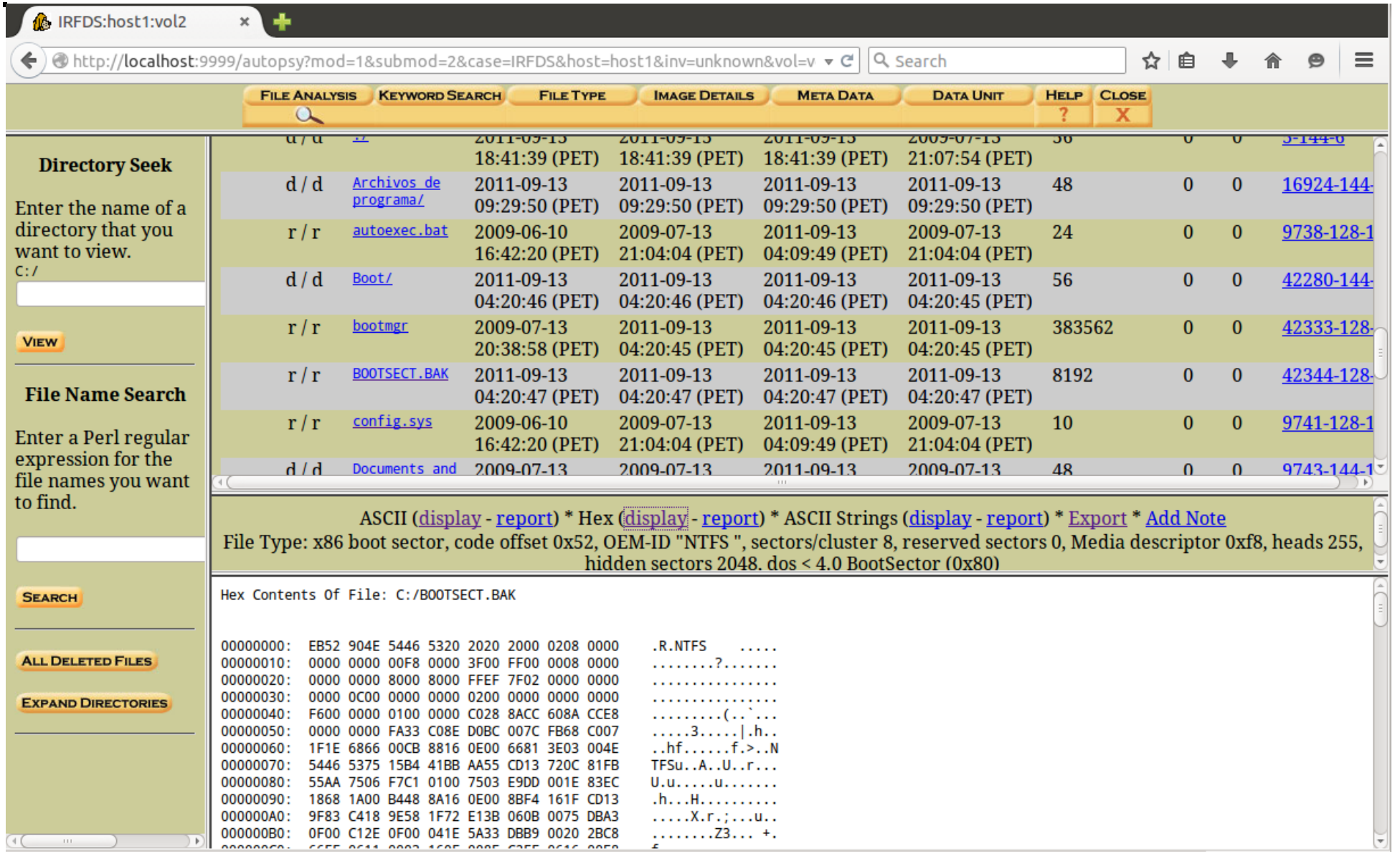
http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

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



Demostraciones



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

Jueves 5 de Mazo del 2015