Análisis Forense

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Viernes 16 de Octubre del 2015

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, 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.

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 y al Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, 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 (NTFS, 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 hacia el servidor Autopsy desde cualquier plataforma utilizando un navegador HTML. Autopsy 2 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/

Sobre el Caso en Análisis

Scan of The Month 24

Joe Jacobs de 28 años fue arrestado por cargos de vender drogas ilegales a estudiantes de secundaria. Ha sido visto en numeras ocasiones pasando por varios estacionamientos de escuelas secundarias alrededor de las 2:30 de la tarde, tiempo en el cual usualmente el día escolar termina. La policía necesita ayuda para determinar si el acusado ha vendido drogas a estudiantes de otras escuelas aparte de Smith Hill.

Preguntas a responder.

¿Quién es el proveedor de Mariguana de Joe Jacobs y su dirección?

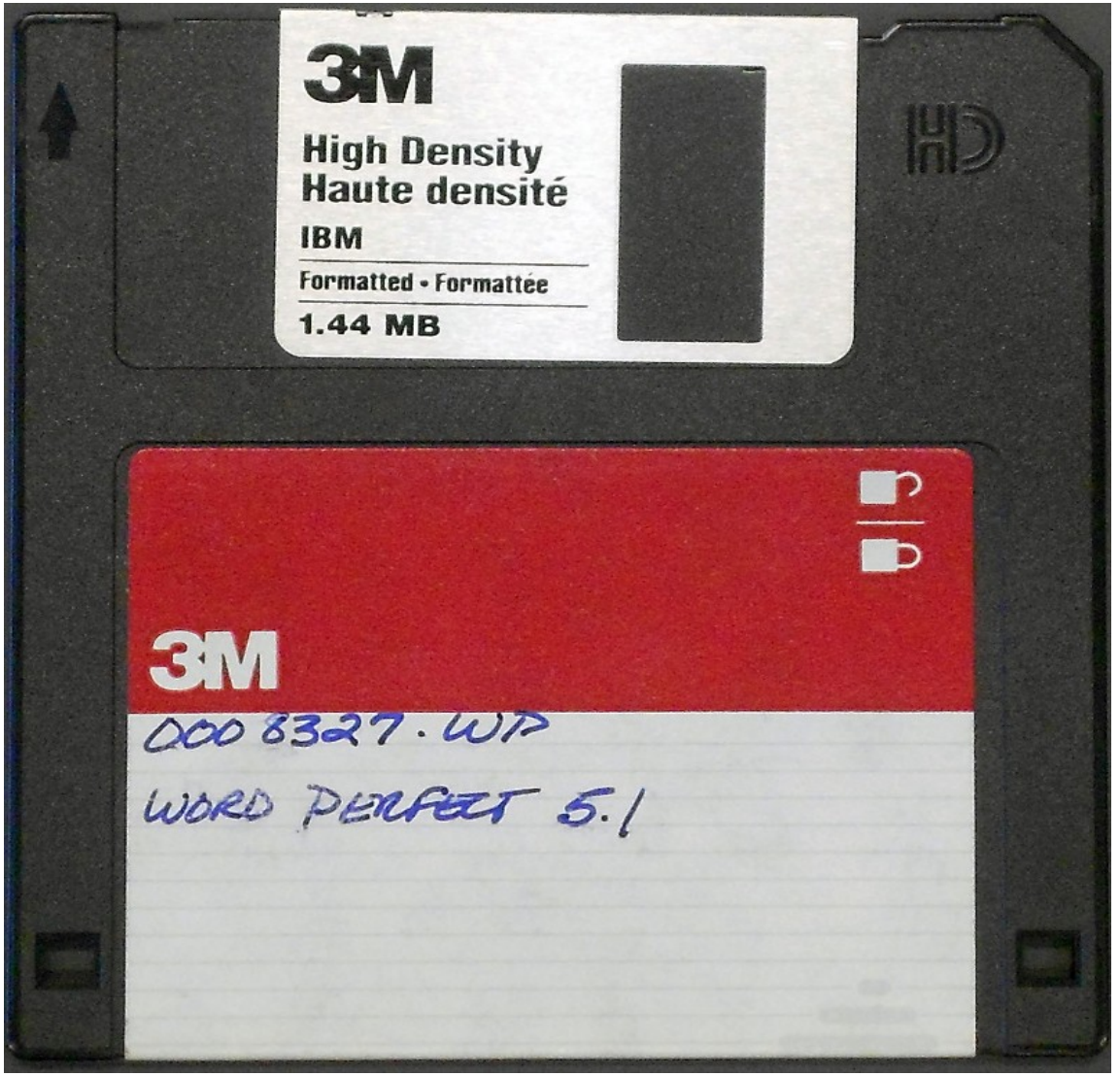
¿Qué datos cruciales están disponibles en el archivo coverpage.jpg y porque son cruciales?

¿Cuales otras escuelas aparte de Smith Hills el acusado frecuentaba?

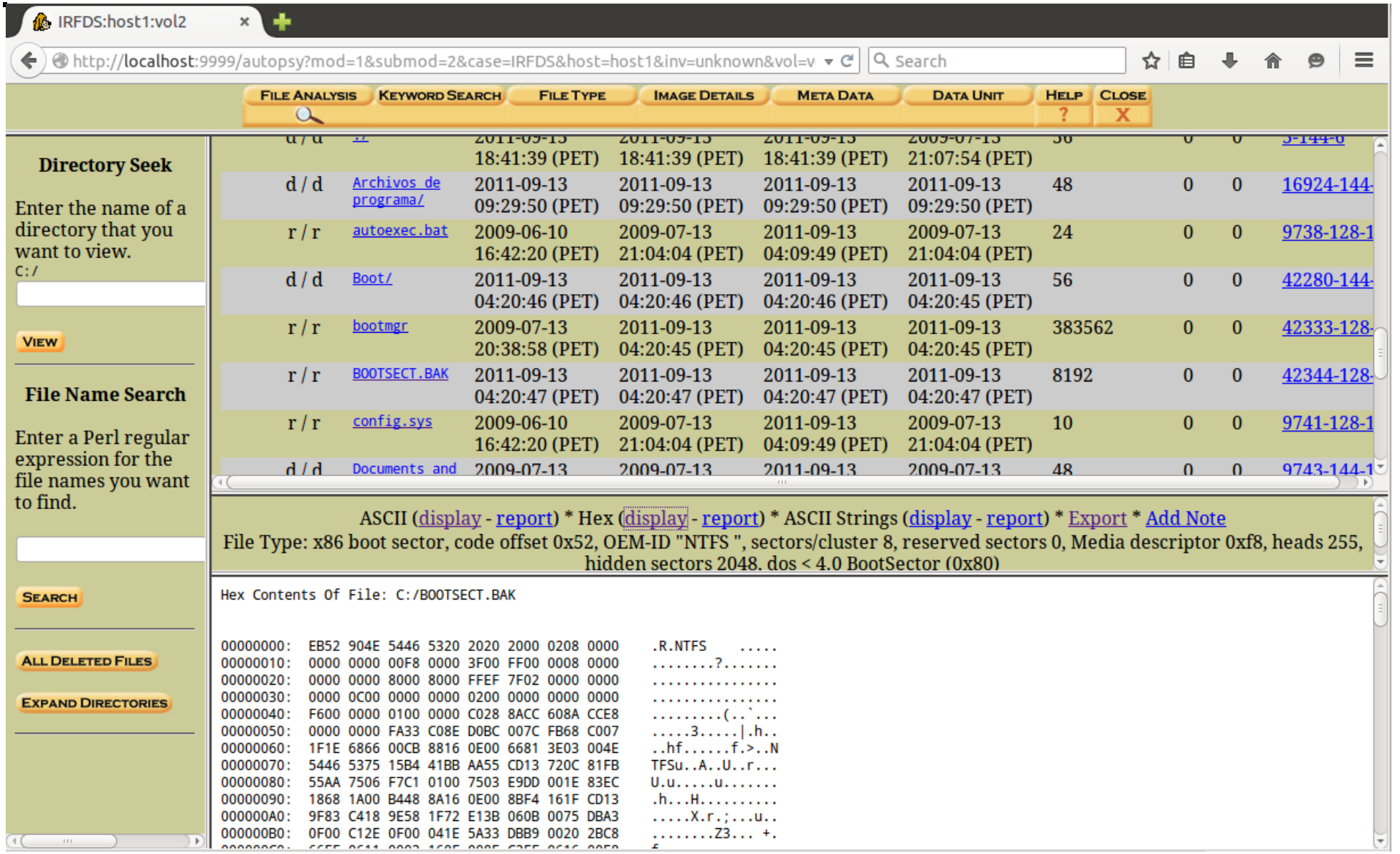
* http://old.honeynet.org/scans/scan24/

Sobre el Caso en Análisis (Cont.)

Evidencia Capturada



Demostraciones



¿Preguntas, Comentarios, Sugerencias?

.

Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

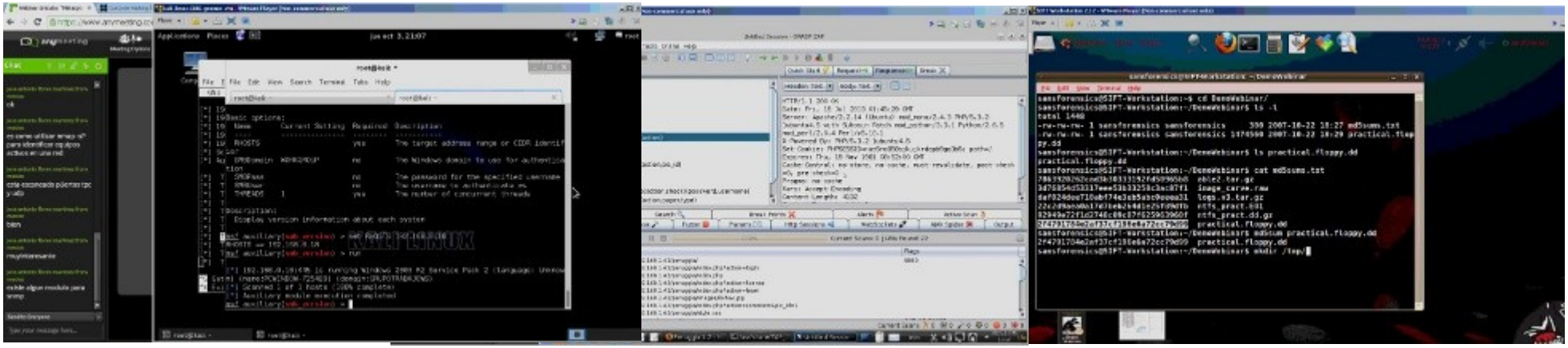
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

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

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

Diapositivas utilizadas en los Webinars Gratuitos.

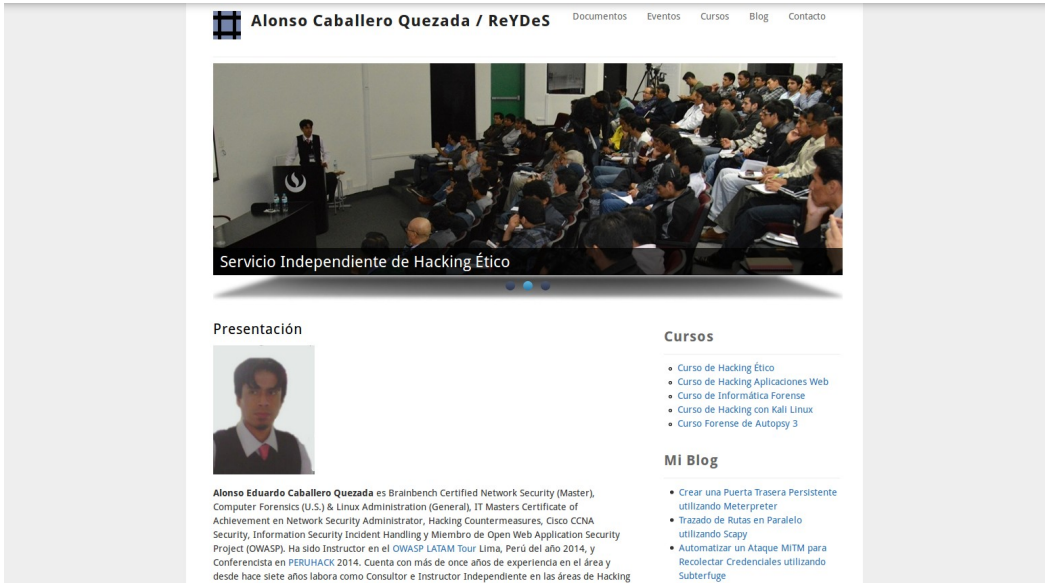
http://www.reydes.com/d/?q=node/3

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



Análisis Forense

¡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

Viernes 16 de Octubre del 2015