Webinar Gratuito
FTK Imager

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 Junio del 2014

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavín de Huantar 2012.
- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.
- Más de 11 años de experiencia en el área.
-  @Alonso_ReYDeS
-  pe.linkedin.com/in/alonsocaballeroquezada/

¿Qué es FTK Imager?

FTK Imager es una herramienta para previsualizar datos, la cual permite también realizar réplicas o imágenes. De esta manera se puede evaluar rápidamente evidencia electrónica y determinar si se requiere realizar un análisis más profundo con una herramienta como AccessData Forensics ToolKit.

FTK Imager también puede crear copias perfectas (imágenes forenses) de datos residentes en computadoras sin realizar cambios en la evidencia original.

Importante:

Cuando se utilice FTK Imager para crear imágenes forenses desde un disco duro u otro dispositivo electrónico, se debe utilizar un bloqueador de escritura basado en hardware. Esto asegura que el sistema operativo no alterará la unidad fuente original cuando se anexe a la computadora.

* http://www.accessdata.com/support/product-downloads
* http://www.accessdata.com/products/digital-forensics/ftk

¿Qué se puede realizar con FTK Imager?

- Crear imágenes forenses de discos duros locales, CDs, DVDs, USBs, de carpetas, o archivos individuales del medio.
- Previsualizar archivos y carpetas de discos duros locales, unidades de red, CD, DVDs, USBs, etc.
- Previsualizar el contenido de las imágenes forenses almacenadas en la máquina local o en una unidad de red.
- Montar una imagen forense para visualizarla en “solo-lectura”, lo cual permite al navegador de Windows ver los contenidos.
- Exportar archivos o carpetas desde las imágenes forenses.
- Ver y recuperar archivos borrados desde la papelera de reciclaje.
- Crear hashes de archivos utilizando MD5 o SHA-1.
- Generar reportes de hashes para archivos regulares e imágenes

FTK Imager

Para prevenir la manipulación accidental o intencional de la evidencia original, FTK Imager realiza una imagen duplicado bit a bit del medio. La imagen forense es idéntica en cualquier forma al original, incluyendo el espacio de holgura o residual, y el espacio sin asignar o el espacio libre en la unidad. Esto permite almacenar la evidencia original en un lugar seguro de daño mientras procede la investigación.

Después de crear la imagen de los datos, se puede utilizar AccessData Forensic Toolkit (FTK) para realizar un examen forense completo y profundo, para luego crear un reporte de los hallazgos.

AccessData Forensics Toolkit

Es una plataforma para investigaciones forenses digitales construida para ser rápida, estable y de fácil uso.

* http://www.accessdata.com/products/digital-forensics/ftk

Curso Virtual de Informática Forense

Días:

Grupo 1: Sábados 7, 14, 21 y 28 de Junio del 2014
Grupo 2: Domingos 8, 15, 22 y 29 de Junio del 2014

Horario:

De 9:00am a 12:30m (UTC -05:00)

Más Información:

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


caballero.alonso@gmail.com

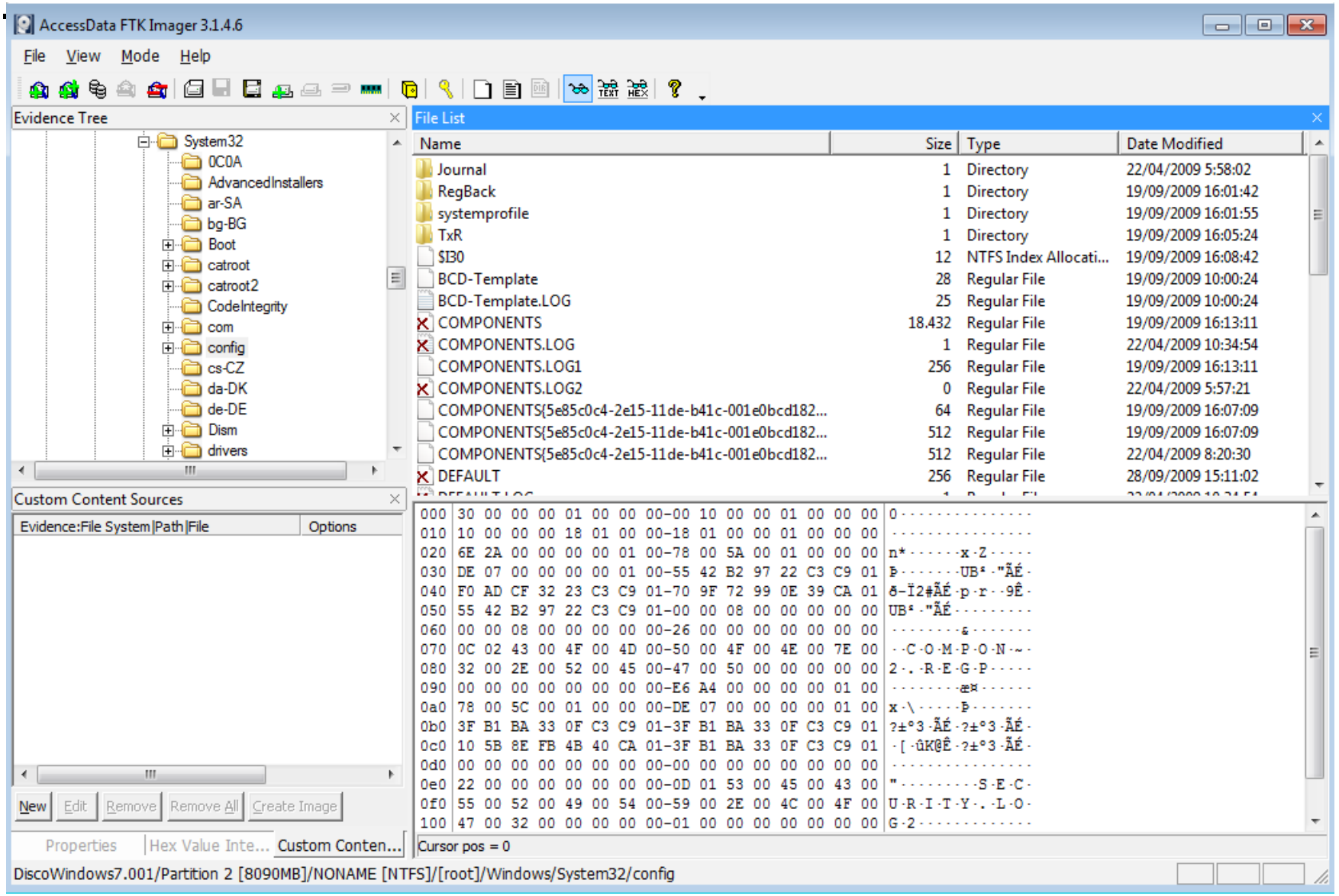
@Alonso_ReYDeS 


http://pe.linkedin.com/in/alonsocaballeroquezada/


ReYDeS


http://www.reydes.com

Demostraciones



Más Material

Videos de 21 Webinars Gratuitos que he dictado sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

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

Todas las diapositivas utilizadas en los Webinars Gratuitos las encuentran en la siguiente página.

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

Todos los artículos y documentos que he publicado.

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

Mi Blog sobre temas de mi interés.

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

¡Muchas Gracias!

FTK Imager

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 Junio del 2014