



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/>



<http://www.reydes.com>



ReYDeS

Demostraciones

AccessData FTK Imager 3.1.4.6

File View Mode Help

Evidence Tree

- System32
 - 0C0A
 - AdvancedInstallers
 - ar-SA
 - bg-BG
 - Boot
 - catroot
 - catroot2
 - CodeIntegrity
 - com
 - config
 - cs-CZ
 - da-DK
 - de-DE
 - Dism
 - drivers

File List

Name	Size	Type	Date Modified
Journal	1	Directory	22/04/2009 5:58:02
RegBack	1	Directory	19/09/2009 16:01:42
systemprofile	1	Directory	19/09/2009 16:01:55
TxR	1	Directory	19/09/2009 16:05:24
\$B0	12	NTFS Index Allocati...	19/09/2009 16:08:42
BCD-Template	28	Regular File	19/09/2009 10:00:24
BCD-Template.LOG	25	Regular File	19/09/2009 10:00:24
COMPONENTS	18.432	Regular File	19/09/2009 16:13:11
COMPONENTS.LOG	1	Regular File	22/04/2009 10:34:54
COMPONENTS.LOG1	256	Regular File	19/09/2009 16:13:11
COMPONENTS.LOG2	0	Regular File	22/04/2009 5:57:21
COMPONENTS{5e85c0c4-2e15-11de-b41c-001e0bcd182...}	64	Regular File	19/09/2009 16:07:09
COMPONENTS{5e85c0c4-2e15-11de-b41c-001e0bcd182...}	512	Regular File	19/09/2009 16:07:09
COMPONENTS{5e85c0c4-2e15-11de-b41c-001e0bcd182...}	512	Regular File	22/04/2009 8:20:30
DEFAULT	256	Regular File	28/09/2009 15:11:02
DEFAULT.LOG	1	Regular File	22/04/2009 10:34:54

Custom Content Sources

Evidence:File System Path File	Options

New Edit Remove Remove All Create Image

Properties Hex Value Inte... Custom Conten...

Cursor pos = 0

DiscoWindows7.001/Partition 2 [8090MB]/NONAME [NTFS]/[root]/Windows/System32/config

```

000 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0
010 10 00 00 00 18 01 00 00-18 01 00 00 01 00 00 00
020 6E 2A 00 00 00 00 01 00-78 00 5A 00 01 00 00 00
030 DE 07 00 00 00 00 01 00-55 42 B2 97 22 C3 C9 01
040 F0 AD CF 32 23 C3 C9 01-70 9F 72 99 0E 39 CA 01
050 55 42 B2 97 22 C3 C9 01-00 00 08 00 00 00 00 00
060 00 00 08 00 00 00 00 00-26 00 00 00 00 00 00 00
070 0C 02 43 00 4F 00 4D 00-50 00 4F 00 4E 00 7E 00
080 32 00 2E 00 52 00 45 00-47 00 50 00 00 00 00 00
090 00 00 00 00 00 00 00 00-E6 A4 00 00 00 00 01 00
0a0 78 00 5C 00 01 00 00 00-DE 07 00 00 00 01 00 00
0b0 3F B1 BA 33 0F C3 C9 01-3F B1 BA 33 0F C3 C9 01
0c0 10 5B 8E FB 4B 40 CA 01-3F B1 BA 33 0F C3 C9 01
0d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0e0 22 00 00 00 00 00 00 00-0D 01 53 00 45 00 43 00
0f0 55 00 52 00 49 00 54 00-59 00 2E 00 4C 00 4F 00
100 47 00 32 00 00 00 00 00-01 00 00 00 00 00 00 00
    
```

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