

# 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](mailto:ReYDeS@gmail.com)

# 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)
```

# 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 (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



## 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 numerosas 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.

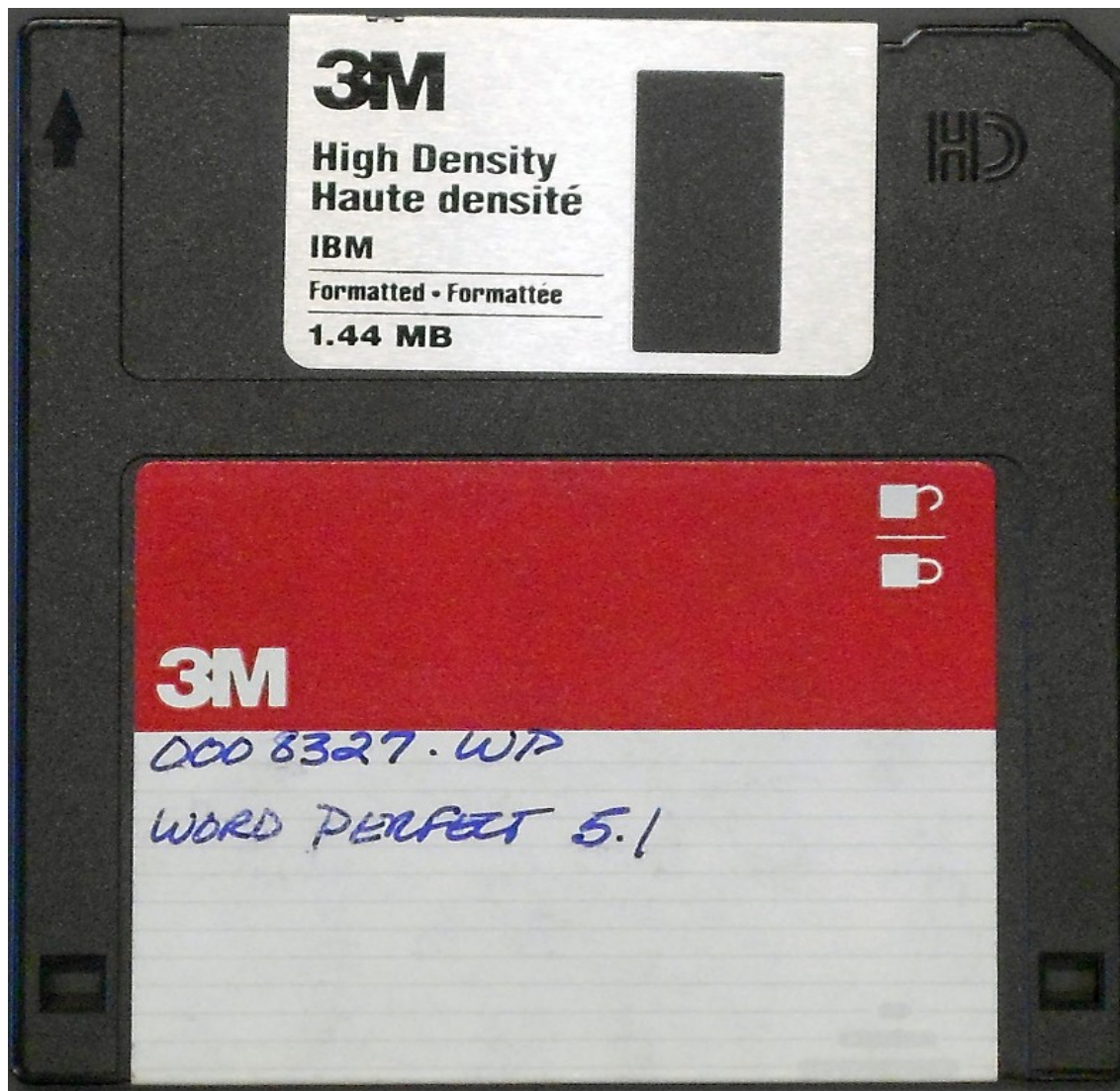
¿Quién es el proveedor de Marihuana de Joe Jacobs y su dirección?

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

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

# Sobre el Caso en Análisis (Cont.)

## Evidencia Capturada



# Demostraciones

The screenshot shows a web-based forensic analysis tool. The browser address bar displays `http://localhost:9999/autopsy?mod=1&submod=2&case=IRFDS&host=host1&inv=unknown&vol=v`. The interface includes several tabs: FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. The main area displays a file list with columns for file type, name, and various timestamps. The selected file is `C:/BOOTSECT.BAK`. Below the file list, there are search options for Directory Seek and File Name Search. At the bottom, the hex contents of the selected file are displayed, showing a boot sector with various strings and offsets.

File Type	File Name	2011-09-13	2011-09-13	2011-09-13	2009-07-13	Size	0	0	Path
d/d	Archivos de programa/	18:41:39 (PET)	18:41:39 (PET)	18:41:39 (PET)	21:07:54 (PET)	48	0	0	16924-144-
r/r	autoexec.bat	09:29:50 (PET)	09:29:50 (PET)	09:29:50 (PET)	09:29:50 (PET)	24	0	0	9738-128-1
d/d	Boot/	16:42:20 (PET)	21:04:04 (PET)	04:09:49 (PET)	21:04:04 (PET)	56	0	0	42280-144-
r/r	bootmgr	04:20:46 (PET)	04:20:46 (PET)	04:20:46 (PET)	04:20:45 (PET)	383562	0	0	42333-128-
r/r	BOOTSECT.BAK	20:38:58 (PET)	04:20:45 (PET)	04:20:45 (PET)	04:20:45 (PET)	8192	0	0	42344-128-
r/r	config.sys	04:20:47 (PET)	04:20:47 (PET)	04:20:47 (PET)	04:20:47 (PET)	10	0	0	9741-128-1
d/d	Documents and	16:42:20 (PET)	21:04:04 (PET)	04:09:49 (PET)	21:04:04 (PET)	48	0	0	9743-144-1

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

```

# ¿Preguntas, Comentarios, Sugerencias?





# Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

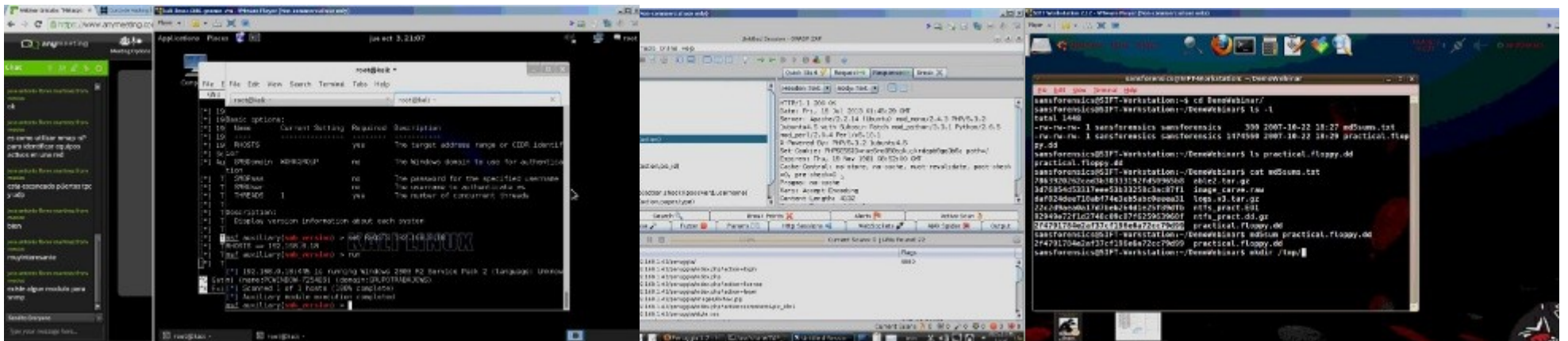
[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Etico](http://www.reydes.com/d/?q=Curso_de_Hacking_Etico)

Curso Virtual de Hacking Aplicaciones Web

[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Aplicaciones\\_Web](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](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>

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

# 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](mailto:ReYDeS@gmail.com)