

# Informática Forense & GNU/Linux

## Webinar Gratuito

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Informática Forense &  
GNU/Linux

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

e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Jueves 21 de Julio del 2016

# 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 y Digital Forensics.

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú y Conferencista en PERUHACK. Cuenta con más de trece años de experiencia en el área y desde hace nueve 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](http://www.facebook.com/alonsoreydes) 

[pe.linkedin.com/in/alonsocaballeroquezada/](http://pe.linkedin.com/in/alonsocaballeroquezada/) 

## Linux

Cuando hablamos del Sistema Operativo Linux, nos estamos refiriendo a GNU/Linux. Una combinación del Kernel Linux y utilidades GNU.

### ¿Porqué GNU/Linux?

- **Control:** No únicamente sobre el software forense, sino también sobre el sistema operativo y el hardware adjunto.
- **Flexibilidad:** Se puede iniciar Linux desde un CD/DVD/USB (Un sistema operativo completo), soporte de sistemas de archivos, soporte plataformas, etc.
- **Poder:** Una distribución de Linux es (o puede ser) una herramienta forense muy completa.

\* The Linux Kernel Archives: <https://www.kernel.org/>

\* GNU: <https://www.gnu.org>

# Tareas Forense Comunes utilizando GNU/Linux

- Crear una imagen forense desde un disco o dispositivo incautado.
- Montar un archivo conteniendo una imagen forense.
- Montar una imagen utilizando el dispositivo loopback.
- Generar un Hash desde un archivo o conjunto de archivos.
- Realizar un análisis forense básico.
- Realizar un listado de archivos.
- Realizar un listado por tipos de archivo.
- Visualizar archivos de texto o binarios.
- Buscar texto en el espacio de holgura o sin asignar

# Herramientas Forenses Incluidas en GNU/Linux

- **dd:** Comando utilizado para copiar desde un archivo o dispositivo de entrada hacia un archivo o dispositivo de salida. Réplica sencilla de flujo de bits.
- **sfdisk / fdisk:** Utilizado para determinar la estructura de un disco.
- **grep:** Busca archivos por coincidencias de una expresión o patrón.
- **Dispositivo loop:** Permite asociar archivos regulares con nodos de dispositivo. Este permite montar una imagen de flujo de bits sin la obligación de reescribir la imagen hacia un disco.
- **md5sum / sha1sum:** Crean y almacenan un Hash ya sea MD5 o SHA-1 desde un archivo o lista de archivos (incluyendo dispositivos).
- **file:** Lee la información desde la cabecera de los archivos en un intento de acertar su tipo, sin relación al nombre o extensión.
- **xxd:** Herramienta en línea de comando para visualizar un archivo en modo hexadecimal.

# Demostraciones

```
Terminal File Edit View Search Terminal Help
sansforensics@siftworkstation: /tmp/imagenes/LinuxLEO
total 684217
drwx----- 1 sansforensics sansforensics      0 May 26  2015 able2
-rw----- 1 sansforensics sansforensics 140674966 Oct  6  2012 able2.tar.gz
-rw----- 1 sansforensics sansforensics   51200 Oct  6  2012 image_carve.raw
-rw----- 1 sansforensics sansforensics 2024322 Oct  6  2012 linuxintro-LEFE-3.78.pdf
-rw----- 1 sansforensics sansforensics    5144 Oct  6  2012 logs.v3.tar.gz
-rw----- 1 sansforensics sansforensics     300 Oct  6  2012 md5sums.txt
-rw----- 1 sansforensics sansforensics 524288000 May 14  2015 ntfs_pract.dd
-rw----- 1 sansforensics sansforensics 14814839 Oct  6  2012 ntfs_pract.dd.gz
-rw----- 1 sansforensics sansforensics 17290960 Oct  6  2012 ntfs_pract.E01
-rw----- 1 sansforensics sansforensics 1474560 Sep 14  2014 practical.floppy.dd
sansforensics@siftworkstation:/tmp/imagenes/LinuxLEO$ xxd practical.floppy.dd | more
00000000: eb3e 9028 7741 7e50 4948 4300 0201 0100  .>.(wA~PIHC....
00000010: 02e0 0040 0bf0 0900 1200 0200 0000 0000  ...@.....
00000020: 0000 0000 0001 296d 2de4 164e 4f20 4e41  .....)m-..NO NA
00000030: 4d45 2020 2020 4641 5431 3220 2020 f17d  ME  FAT12  .}
00000040: fa33 c98e d1bc fc7b 1607 bd78 00c5 7600  .3.....{...x..v.
00000050: 1e56 1655 bf22 0589 7e00 894e 02b1 0bfc  .V.U."...~.N....
00000060: f3a4 061f bd00 7cc6 45fe 0f8b 4618 8845  .....|.E...F..E
00000070: f9fb 3866 247c 04cd 1372 3c8a 4610 98f7  ..8f$|...r<.F...
00000080: 6616 0346 1c13 561e 0346 0e13 d150 5289  f..F..V..F...PR.
00000090: 46fc 8956 feb8 2000 8b76 11f7 e68b 5e0b  F..V.. ..v....^
000000a0: 03c3 48f7 f301 46fc 114e fe5a 58bb 0007  ..H...F..N.ZX...
000000b0: 8bfb b101 e894 0072 4738 2d74 19b1 0b56  .....rG8-t...V
000000c0: 8b76 3ef3 a65e 744a 4e74 0b03 f983 c715  .v>..^tJNT.....
000000d0: 3bfb 72e5 ebd7 2bc9 b8d8 7d87 463e 3cd8  ;.r...+...}.F><.
000000e0: 7599 be80 7dac 9803 f0ac 84c0 7417 3cff  u...}.....t.<.
000000f0: 7409 b40e bb07 00cd 10eb eebe 837d ebe5  t.....}..
0000100: be81 7deb e033 c0cd 165e 1f8f 048f 4402  ..}..3...^....D.
0000110: cd19 be82 7d8b 7d0f 83ff 0272 c88b c748  ....}.}....r...H
0000120: 488a 4e0d f7e1 0346 fc13 56fe bb00 0753  H.N...F..V....S
0000130: b104 e816 005b 72c8 813f 4d5a 75a7 81bf  ....[r...?MZu...
0000140: 0002 424a 759f ea00 0270 0050 5251 9192  ..BJu....p.PRQ..
0000150: 33d2 f776 1891 f776 1842 87ca f776 1a8a  3..v...v.B...v..
0000160: f28a 5624 8ae8 d0cc d0cc 0acc b801 02cd  ..V$.
0000170: 1359 5a58 7209 4075 0142 035e 0be2 ccc3  .YZXr.@u.B.^....
```



# Curso Virtual de Informática Forense

## Curso Virtual de Informática Forense 2016

Domingos 24, 31 de Julio, 7 y 14 de Agosto del 2016. De 9:00 am a 12:15 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:



### Presentación:

Todas las organizaciones deben prepararse para crímenes cibernéticos ocurriendo en sus sistemas de cómputo y dentro de sus redes. Se ha incrementado la demanda actual de analistas quienes puedan investigar crímenes como fraudes, amenazas internas, espionaje industrial, inadecuado uso de los empleados, e intrusiones de computadoras. Las agencias del gobierno también requieren personal debidamente entrenado para analizar sistemas windows.

### Objetivos:

Este curso se enfoca en construir un profundo conocimiento en forense digital del sistema operativo microsoft windows. No se puede proteger aquello desconocido, por lo tanto entender las capacidades forenses y artefactos es un componente clave en la seguridad de la información. Aprender a recuperar, analizar y autenticar datos forenses sobre sistemas windows. Entender como rastrear actividad detallada del usuario sobre la red, y como organizar sus hallazgos para ser utilizado en una respuesta de incidentes, investigaciones internas y litigios civiles o penales. Utilizar los nuevos conocimientos adquiridos para validar las herramientas de seguridad mejorando las evaluaciones de seguridad, identificar amenazas internas, rastrear hackers, y mejorar políticas de seguridad. Aunque se conozca o no, windows silenciosamente registra una cantidad inimaginable de datos sobre los usuarios. Este curso enseña la manera de obtener y analizar toda esta ingente cantidad de datos.



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, Digital Forensics y Cybersecurity Management. Ha sido Instructor en el OWASP LATAM Tour Lima, Perú y Conferencista en PERUHACK. Cuenta con más de trece años de experiencia en el área y desde hace nueve 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. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: <http://www.ReYDeS.com>.

Más Información: [http://www.reydes.com/d/?q=Curso\\_de\\_Informatica\\_Forense](http://www.reydes.com/d/?q=Curso_de_Informatica_Forense)

E-mail: [caballero.alonso@gmail.com](mailto:caballero.alonso@gmail.com) / Sitio Web: <http://www.reydes.com>

# Cursos Virtuales 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

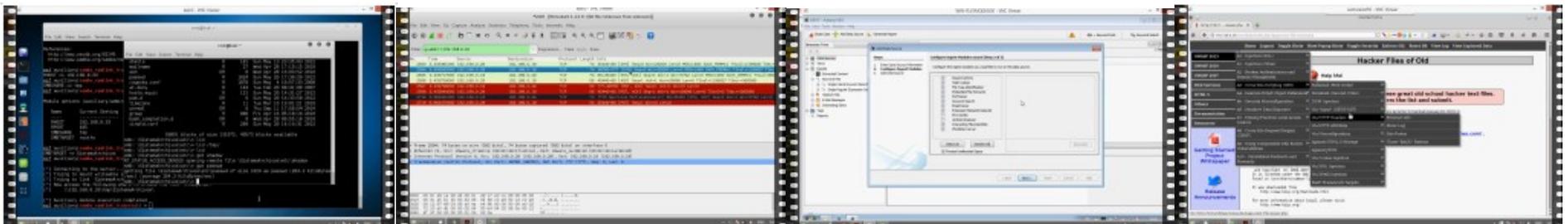
[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Aplicaciones\\_Web](http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web)

- 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)

- Y muchos más Cursos:

<http://www.reydes.com/d/?q=node/8>



# Más Contenidos

Videos de 30 Webinars Gratuitos

<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 Cursos Videos Blog Eventos Contacto



Servicio Independiente de Hacking Ético

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

Cursos

- Curso de Informática Forense
- Curso de Hacking Windows
- Curso OWASP TOP 10
- Curso de Hacking Linux
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso de Hacking con Kali Linux 2.0
- Curso Forense de Autopsy 4
- Curso de Metasploit Framework
- Curso de Nmap
- Curso Forense de Windows XP

# Informática Forense & GNU/Linux

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Informática Forense &  
GNU/Linux

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

e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)