# 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


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

pe.linkedin.com/in/alonsocaballeroquezada/

# Informática Forense & GNU/Linux

## 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 pude 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

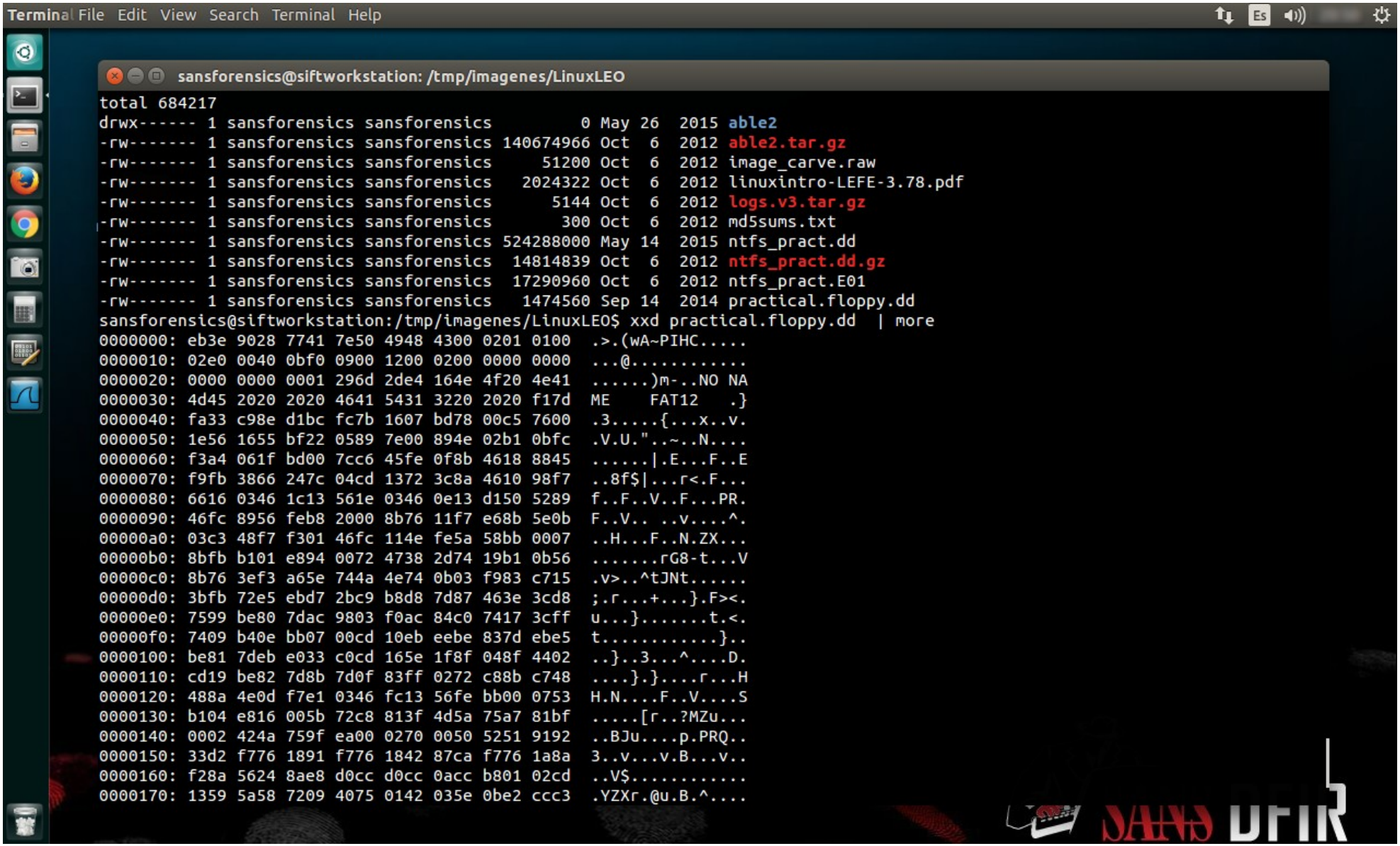
- Crear una imagen forense desde un disco o dispositivo incautado.
- Montar un archivo conteniendo una imagen forense.
- Montar una imagen utilizando el dispositivo loopback.
- Generar un Hash desde un archivo o conjunto de archivos.
- Realizar un análisis forense básico.
- Realizar un listado de archivos.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

* Digital Forensic Process: https://en.wikipedia.org/wiki/Digital_forensic_process

# 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



# 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
E-mail: **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

- Curso Virtual de Hacking Aplicaciones Web

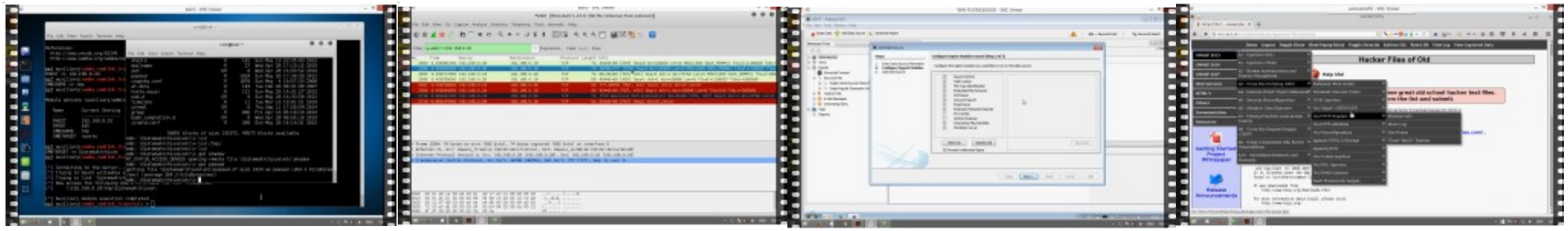
  http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

- Curso Virtual de Informática Forense

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

- 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

# 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

Jueves 21 de Julio del 2016