Único Curso del Año 2016

Sábados 17 y 24 de Setiembre del 2016
De 9:00am a 12:00m (UTC -05:00) - 6 Horas en Total

1. Presentación:

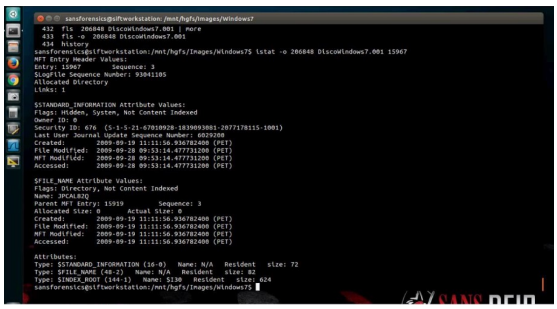
Cuando se habla del sistema operativo Linux, normalmente se refiere al sistema operativo GNU/Linux. Linux por si mismo no es un sistema operativo, es solo un Kernel. El sistema operativo es actualmente una combinación del Kernel de Linux y las utilidades GNU, las cuales permiten al Hardware interactuar con el Kernel.

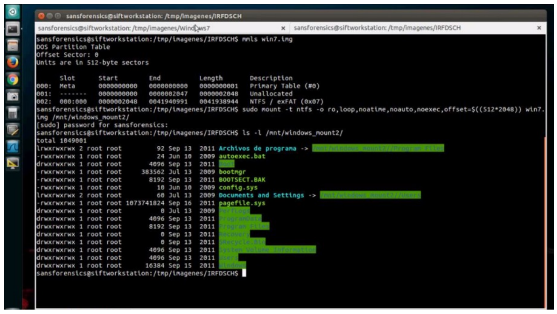
Existen diversas razones para aprender GNU/Linux y utilizarlo como herramienta forense. De hecho en la actualidad ha ganado un gran terreno como plataforma para realizar análisis forense de computadoras. Entre sus atributos principales se pueden enumerar; GNU/Linux proporciona control no únicamente sobre el software forense, sino con todo el sistema operativo y el Hardware. Proporciona flexibilidad; siendo factible iniciar todo un sistema operativo completo desde un DVD o unidad USB, incluyendo soporte para diversos sistemas de archivos, soporte de plataformas, etc. Y cualquier distribución GNU/Linux; es o podría ser una herramienta forense. Otro punto a considerar; el simplemente conocer como Linux funciona se convierte en más y más importante.

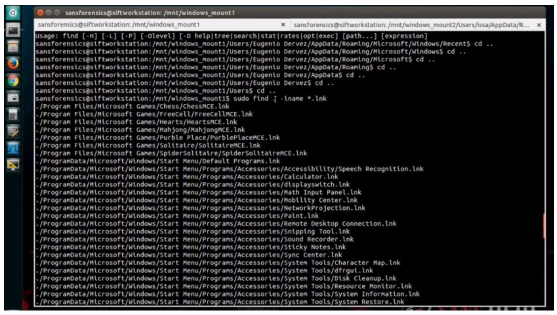
Este curso práctico de análisis forense utilizando GNU/Linux, proporciona a los participantes los conocimientos necesarios sobre el sistema operativo GNU/Linux, para ser utilizado como plataforma forense en investigaciones digitales.

2. Temario:

- Introducción al Análisis Forense utilizando Linux
- Herramientas Forenses incluidas en Linux
- Determinar la Estructura del Disco
- Montar una Imagen Forense
- Crear Hashs desde Archivos
- Proceso de Análisis Forense
- Crear Listados de Todos los Archivos
- Crear Listados por Tipo de Archivos
- Buscar en el Espacio Residual y Espacio no Asignado
- Uso Avanzado de la Línea de Comandos en Linux
- Reconstrucción de Datos con DD
- Reconstrucción de Particiones con DD
- The Sleuth Kit
- Recuperación e Identificación de Archivos Borrados.
- Búsqueda Física de Cadenas y Estado de Asignación
- Extracción y Examen del Espacio no Asignado
- Examen NTFS y Análisis de Archivos
- Examen NTFS y ADS
- Examen NTFS y Ordenamiento de Archivos
- Búsqueda de Firmas en el Espacio no Asignado







3. Material:

Se sugiere al participante tener instalado la máquina virtual SIFT (SANS Investigative Forensic Toolkit) versión 3, Está máquina puede ser descargada desde el siguiente enlace:

SIFT Versión 3: http://digital-forensics.sans.org/community/downloads

Nombre del Archivo: SIFT-Workstation-3-Virtual-Machine-Distro-Version.zip

[*] Si el participante lo requiere se le puede enviar un DVD con todo el material utilizado añadiendo S/. 45 Soles por el concepto de gastos de envío hacia cualquier lugar del Perú.

4. Día y Horario:

La duración total del curso es de 6 (seis) horas. El Curso se dictará en los siguientes días y horarios.

Sábados 17 y 24 de Setiembre del 2016

De 9:00am a 12:00m (UTC -05:00) - 6 Horas en Total

[*] No habrá reprogramaciones. El Curso se dictará **sin** ningún requisito mínimo de participantes.

5. Inversión y Forma de Pago:

El Curso tiene un costo de:

S/. 135 Soles o $ 40 Dólares

El pago del Curso se realiza mediante un depósito bancario en la siguiente cuenta:

ScotiaBank
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

Una vez realizado el depósito, enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: **caballero.alonso@gmail.com**.

Para residentes en otros países por favor escribir un mensaje de correo electrónico para consultar el mecanismo de pago. Confirmado el depósito se enviará al correo electrónico del participante, los datos necesarios para conectarse al sistema y poder participar en el curso.

6. Más Información:

Si desea mayor información sobre el Curso Virtual de Análisis Forense con Linux, tiene a su disposición los siguientes mecanismos de contacto:

Correo electrónico: caballero.alonso@gmail.com

Vía Web: http://www.reydes.com

Celular: (+51) 949304030

7. Sobre el Instructor:

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 del año 2014, y Conferencista en PERUHACK 2014. 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.