Webinar Gratuito

Recuperar Fotografías Borradas con Photorec

Alonso Eduardo Caballero Quezada

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

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 4 de Marzo del 2021

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.reydes.com

reydes@gmail.com

+51 949 304 030

SIFT

SIFT (SANS Incident Forensic Toolkit), es utilizado en respuesta de incidentes y forense digital, el cual está disponible libremente para toda la comunidad.

SIFT demuestra investigaciones avanzadas y la respuesta a intrusiones, pueden ser realizadas utilizando herramientas open source, las cuales están libremente disponibles y son frecuentemente actualizadas.

- Basado en Ubuntu LTS 16.04
- Sistema base de 64 bits
- Mejor utilización de memoria
- Las últimas herramientas y técnicas forenses
- Compatibilidad entre Linux y Windows
- Opción de instalar un sistema autónomo en línea de comando, etc.

* SIFT: https://digital-forensics.sans.org/community/downloads

Recuperación de Archivos

La recuperación de archivos es uno de los diversos procesos a realizar durante la etapa de análisis forense, correspondiente a un forense de computadoras. La recuperación de archivos depende de varios factores.

- El sistema operativo (Windows, Linux, Mac, etc.)
- El sistema de archivos (FAT, NTFS, extX, etc)
- La acción realizada para borrar el archivo
- El formato del archivo borrado
- Tiempo transcurrido desde el borrado, etc.

Formato JPEG

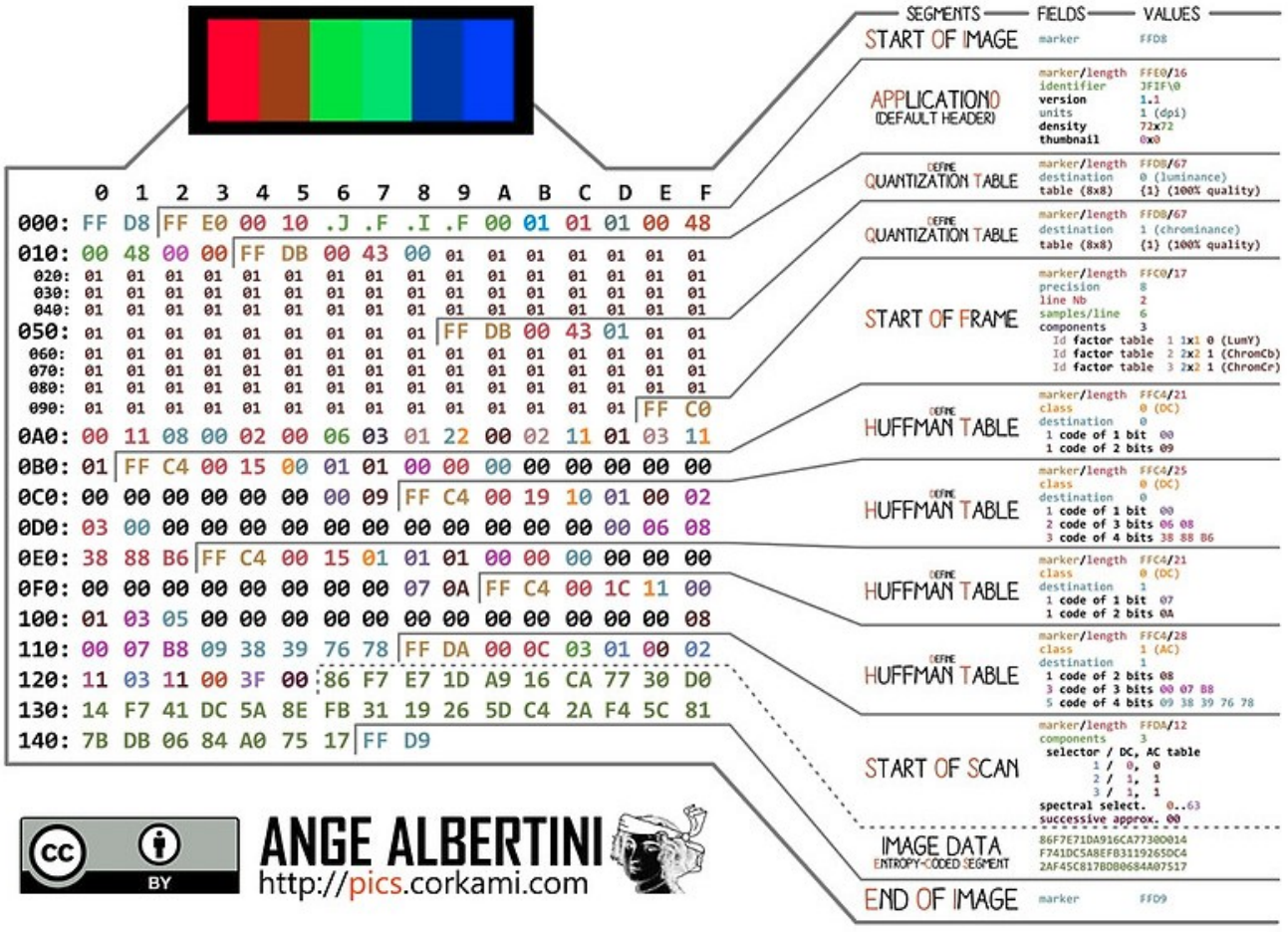
El formato “Joint Photographic Experts Group” es comúnmente utilizado para almacenar imágenes gráficas.

Es un formato de archivo contenedor constituido de una cabecera bien definida, como también algunos metadatos, iconos, tabla de colores, datos comprimidos, y un pie bien definido. Las extensiones comunes son .jpg, .jpeg, .jfif, etc.

Contiene muchos metadatos en diversos formatos, Exif, IPTC, GPS, etc. Existen comandos los cuales pueden extraer y manipular algunos de los metadatos. Herramientas como ExifTool.

* JPEG: https://forensicswiki.xyz/wiki/index.php?title=JPEG
* ExifTool: https://exiftool.org/

Formato JPEG (Cont.)



Photorec

Software diseñado para la recuperación de datos, el cual permite intentar recuperar archivos perdidos, incluyendo videos, documentos, y archivos desde discos duros, CDs, DVDs, y otros dispositivos de almacenamiento, además de imágenes perdidas desde memorias de cámaras digitales.

Photorec ignora el sistemas de archivos, y va hacia los datos subyacentes, de tal manera funciona incluso si el sistema de archivos del medio ha sido severamente dañado.

Para mayor seguridad, Photorec utiliza acceso de solo lectura para manejar la unidad o tarjeta de memoria, desde la cual se intenta recuperar datos.

* Photorec: https://www.cgsecurity.org/wiki/PhotoRec

¿Cómo Funciona Photorec?

Cuando un archivo es borrado, la meta información sobre el archivo se pierde. Pero los datos pueden seguir existiendo en el sistema de archivos, únicamente hasta sean parcial o totalmente sobrescritos por nuevos archivos de datos.

Para recuperar estos archivos, primero se intenta encontrar el tamaño del cluster. Si el sistema de archivos no está dañado, este valor puede ser leído desde el registro del volumen de inicio. De otra manera se lee sector por sector el medio de almacenamiento buscando por los primeros diez archivos, desde los cuales se calcula el tamaño del cluster desde sus ubicaciones. Una vez obtenido se lee cluster por cluster desde el medio de almacenamiento. Esto es verificado contra una base de datos de firmas incluido en Photorec. La herramienta tiene una gran cantidad de archivos los cuales son factibles de recuperar.

* Photorec: https://www.cgsecurity.org/wiki/PhotoRec

¿Cómo Funciona Photorec? (Cont.)

Por ejemplo para archivos JPEG. Si Photorec empieza a recuperar archivos, detiene la recuperación, verifica la consistencia de los archivos cuando es posible, e inicia el guardado del nuevo archivo.

Si los datos no están fragmentados, el archivo recuperado debe ser ya sea idéntico o mayor al archivo original en tamaño. En algunos casos puede aprender del tamaño del archivo original desde la cabecera del archivo, de tal manera el archivo recuperado está truncado hacia el tamaño correcto. En caso el archivo recuperado finaliza siendo más pequeño de lo cual especifica la cabecera, es descartado.

Cuando se recupera exitosamente un archivo, se verifican los bloques de datos previos para ver si se encontró una firma de archivo, pero si el archivo no se recuperó exitosamente, se intenta nuevamente. De esta manera algunos archivos fragmentados se pueden recupera exitosamente.

Curso

Curso Virtual Informática Forense 2021

Domingos 7, 14, 21 y 28 de Marzo del 2021. 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

En la actualidad todas las empresas y organizaciones deben estar preparadas para enfrentar exitosamente diversos tipos de crímenes cibernéticos, los cuales se suscitan y afectan sus sistemas de cómputo y redes. Consecuentemente se ha incrementado la demanda por profesionales forenses debidamente entrenados y experimentados, quienes estén en la capacidad investigar crímenes cibernéticos relacionados a fraudes, amenazas internas, espionaje industrial, inadecuado uso de los empleados, e intrusiones hacia computadoras y redes Las agencias del gobierno a nivel mundial también requieren profesionales forenses debidamente entrenados y con amplia experiencia en el ámbito del forense digital.

Objetivos

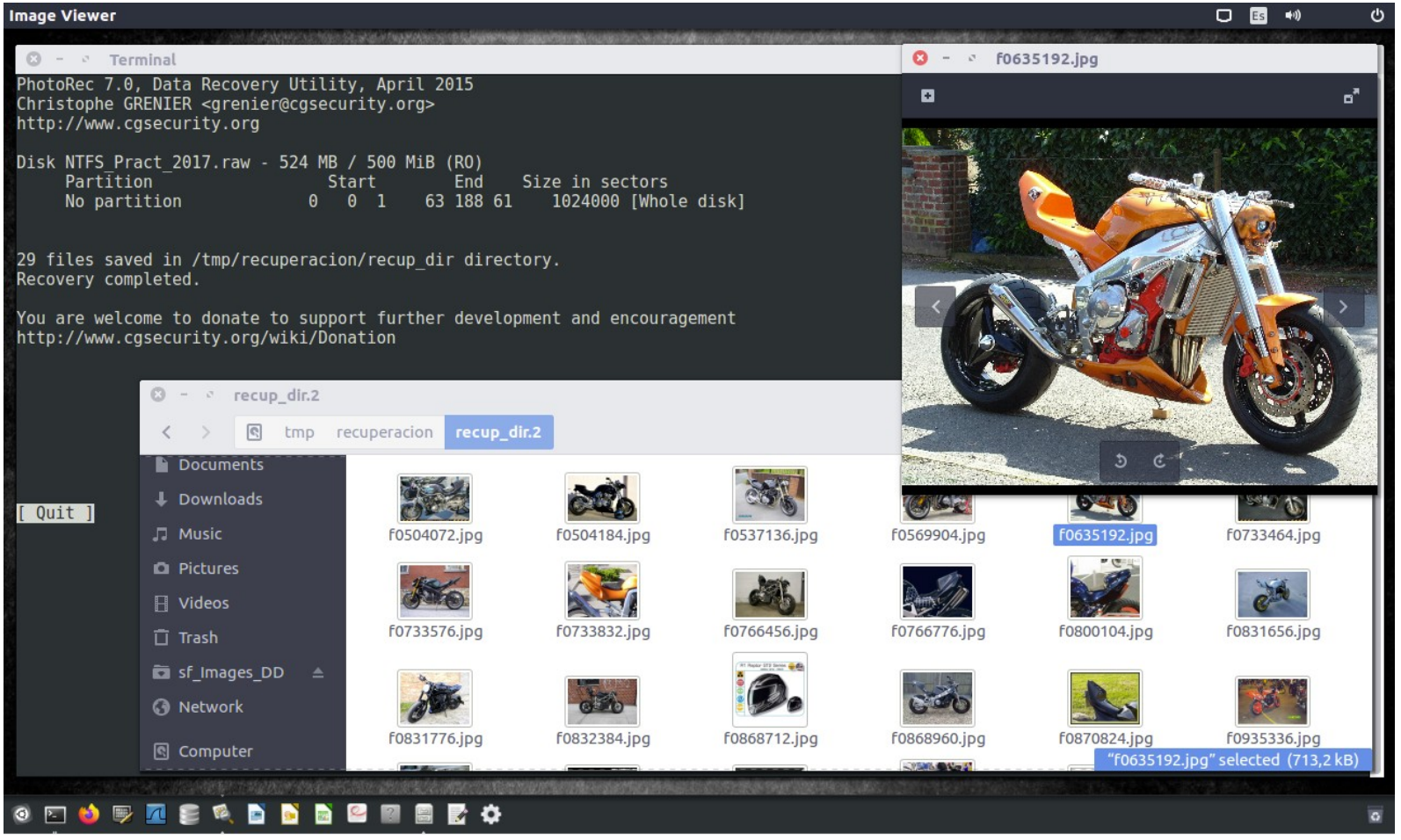
Este curso enseña a los participantes a desarrollar un profundo

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el OWASP LATAM Tour, expositor en

Más Información: https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

e-mail: reydes@gmail.com Sitio Web: https://www.reydes.com

Demostraciones

- 

Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

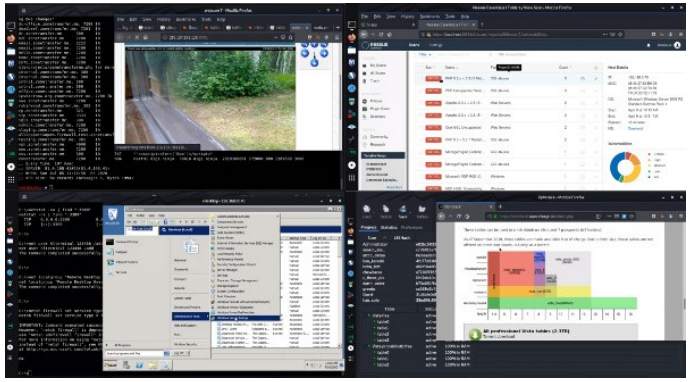
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

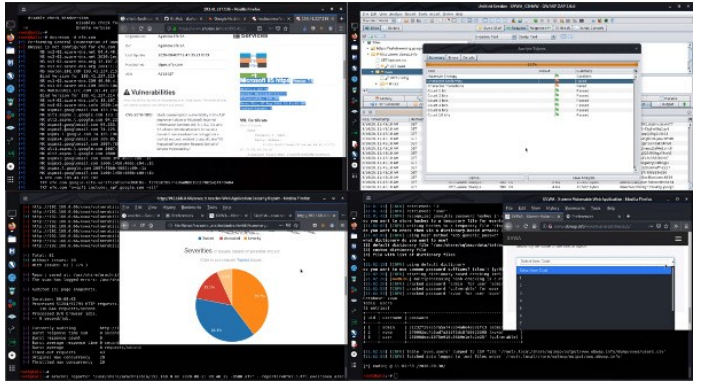
Curso Virtual OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
https://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

https://www.reydes.com/d/?q=cursos





Más Contenidos

Videos de 64 webinars gratuitos

https://www.reydes.com/d/?q=videos

Diapositivas de los webinars gratuitos

https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

https://www.reydes.com/d/?q=documentos

Blog sobre temas de mi interés

https://www.reydes.com/d/?q=blog/1

Webinar Gratuito

Recuperar Fotografías Borradas con Photorec

Alonso Eduardo Caballero Quezada

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

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 4 de Marzo del 2021