Webinar Gratuito

Crear Imágenes Forenses

Alonso Eduardo Caballero Quezada

| Hacking | Forense | Linux | OSINT | Ciberseguridad |

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Lunes 17 de Febrero 2025

Alonso Eduardo Caballero Quezada

Alonso Eduardo Caballero Quezada. ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, 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, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). Cuento con más de dieciocho años de experiencia en el área y desde hace catorce años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital.

Redes Sociales

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

https://x.com/Alonso_ReYDeS

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

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

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

+51 949 304 030

@ReYDeS

Imagen de Disco

Las imágenes de disco suelen ser copias bloque por bloque desde la fuente de datos original.

Según la fuente de datos, los bloques pueden ser bytes, sectores, clusters, páginas, o similares.

El formato para imagen de disco puede mejorarse aún más con información adicional, como detección de errores, corrección de errores, resumen de datos (hash) y compresión.

Existen varios tipos de formatos para imagen de disco.

* Disk Imagen: https://forensics.wiki/disk_images/

Formato de Imagen en Bruto (Raw)

El formato de imagen RAW es básicamente una copia bit a bit de los datos en bruto del disco o del volumen, sin adiciones ni eliminaciones.

No existen metadatos almacenados dentro de los archivos en formato de imagen RAW. Sin embargo algunas veces los metadatos se almacenan en archivos adicionales.

El formato de imagen RAW fue utilizado originalmente con la herramienta **dd**, pero la mayoría de las aplicaciones en forense de computadoras lo admiten., como la herramienta **dcfldd** y similares.

* Raw image format: https://forensics.wiki/raw_image_format/

DCFLDD

Fue inicialmente desarrollada por Department of Defense Computer Forensics Lab (DCFL). Se basa en **dd** con las siguientes características adicionales:

- Hashing al vuelo: Genera hash a datos de entrada conforme son transferidos, lo cual ayuda a garantizar la integridad de datos.
- Estado de salida: Puede actualizar al usuario sobre el progreso en términos de cantidad de datos transferidos, y cuanto tiempo tomará la operación.
- Limpieza flexible de discos: Se puede utilizar para limpiar discos rápidamente y con un patrón conocido si es requerido.
- Verificación de imagen/borrado: Puede verificar una unidad de destino coincide bit a bit con el archivo de entrada o patrón especificado.

DCFLDD (Cont.)

- Múltiples salidas: Puede generar salidas en varios archivos o discos al unísono.
- Salida dividida: Puede dividir la salida hacia múltiples archivos con más configuración comparado con el comando split.
- Salida y logs canalizados: Puede enviar todos los datos logs y salida a comandos, así como a archivos de manera nativa.
- Cuando dd usa un tamaño de bloque predeterminado (bs, ibs, obs) de 512 bytes, dcfldd usa 32768 bytes (32 KiB), lo cual es mucho más eficiente.
- Las siguientes opciones están en dcfldd (no dd): ALGORITHMlog:, errlog, hash, hashconv, hashformat, hashlog, hashlog:, hashwindow, limit, of:, pattern, sizeprobe, split, splitformat, statusinterval, textpattern, totalhashformat, verifiedlog, verifiedlog:, vf.

Curso Informática Forense

Curso Informática Forense 2025

18, 20, 25, 27 de Febrero, 4, 6, 11, 13 de Marzo 2025. De 8:00 pm a 9:30 pm (UTC -05:00)

Las clases en vivo se quedan grabadas en el aula virtual

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 profundo conocimiento sobre forense digital aplicado a Microsoft Windows. Es fundamental comprender sus capacidades forenses y artefactos. Aprender a identificar, capturar, autenticar, y analizar datos forenses. Entender como rastrear detalladamente la actividad realizada del usuario a través de la red, además de organizar hallazgos para ser utilizado en una respuesta de incidentes, investigaciones internas, y litigios civiles o penales. Utilizar los conocimientos adquiridos para validar las herramientas de seguridad, identificar amenazas internas, rastrear atacantes, y mejorar las políticas de seguridad. Aunque se conozca o no, el sistema operativo Windows silenciosamente registra una gran cantidad de datos sobre el propio sistema y los usuarios. Este curso enseña una metodología para forense de computadoras con etapas de identificación, preservación, análisis y documentación. Se exponen técnicas y procedimientos de investigación manuales, también se utilizan herramientas forenses.

Fechas & Horarios

Duración:

Catorce (14) horas. Una (1) sesión previamente grabada de dos (2) horas, y ocho (8) sesiones en vivo de una hora y media (1,5) de duración cada una.

Fechas:

18, 20, 25, 27 de Febrero, 4, 6, 11 y 13 de Marzo 2025

Horario:

De 8:00 pm a 9:30 pm (UTC -05:00)

Alonso Eduardo Caballero Quezada.

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, 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, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), y Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). Cuento con más de veintiún años de experiencia en el área, y desde hace diecisiete años laboro como consultor e instructor en Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: www.ReYDeS.com

Más Información

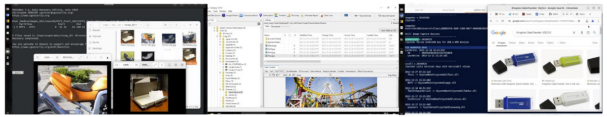
Para obtener más información sobre este curso, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

reydes@gmail.com

WhatsApp: https://wa.me/51949304030

Sitio Web: www.reydes.com



Temario

- Proceso Investigación Forense
- Evolución del Sistema de Archivos Windows
- FTK Imager
- Adquisición de la Memoria RAM
- Evidencia Encriptada
- Obtener Archivos Protegidos
- Imagen con Contenidos Personalizado
- Discos de Estado Sólido (SSD)
- Nivelación de Uso y SSD Trim
- Artefactos Forenses en SSD
- Adquisición de un USB y Disco Duro
- Montar una Imagen
- Visualización Previa de una Unidad
- Recuperar Archivos Borrados
- The Sleuth Kit (TSK)
- Flujos de Datos Alternativos
- Volume Shadow Copy
- Autopsy
- Búsqueda de Cadenas
- Reconstrucción de Datos
- Análisis Forense a la Memoria RAM
- Volatility Framework
- Forense de Correos Electrónicos
- Forense al Registro de Windows
- Lo Esencial del Registro
- Análisis de Información de Usuarios y Grupos
- Análisis de la Configuración del Sistema
- Análisis de la Actividad del Usuario
- Análisis de la Actividad USB
- Archivos de Enlace
- Metadatos en Documentos Office
- Metadatos en Documentos PDF
- Metadatos en Archivos de Medios (EXIF)
- Análisis de Miniaturas
- Análisis de la Papelera de Reciclaje
- Análisis de Archivos Prefetch
- Fundamentos del Registro de Eventos
- Análisis del Registro de Eventos (Logs)
- Registro de Eventos en Windows
- Forense al Navegador Web
- Fundamentos de los Navegadores
- Internet Explorer
- Archivos del Historial Cache / Archivos Temporales
- Cookies, Historial de Descarga

Material

- SIFT Workstation
- Imágenes Forenses Windows
- Herramientas Windows

Beneficios e Inversión

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las cuatro (4) sesiones
- Acceso libre a las sesiones en vivo del siguiente curso a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría en vivo personalizada por videoconferencia
- Libro "Fundamentos de Forense Digital" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 24 horas

S/. 450 Soles o $ 140 Dólares

El pago del curso se realiza:

Residentes en Perú

Depósito bancario Scotiabank

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

O también pagos con Yape o Plin. Escriba un mensaje a reydes@gmail.com para proporcionarle los datos pertinentes.

Residentes en otros países

Pago a través de Paypal PayPal

O también transferencia de dinero mediante Western Union y MoneyGram

Escriba un mensaje a reydes@gmail.com para proporcionarle los datos.

Confirmado el pago se enviará los datos para conectar su participación en el curso.

Certificados

Certificados; constancias de participación y aprobación; expedidos a nombre de la empresa Peruana MILESEC EIRL.

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

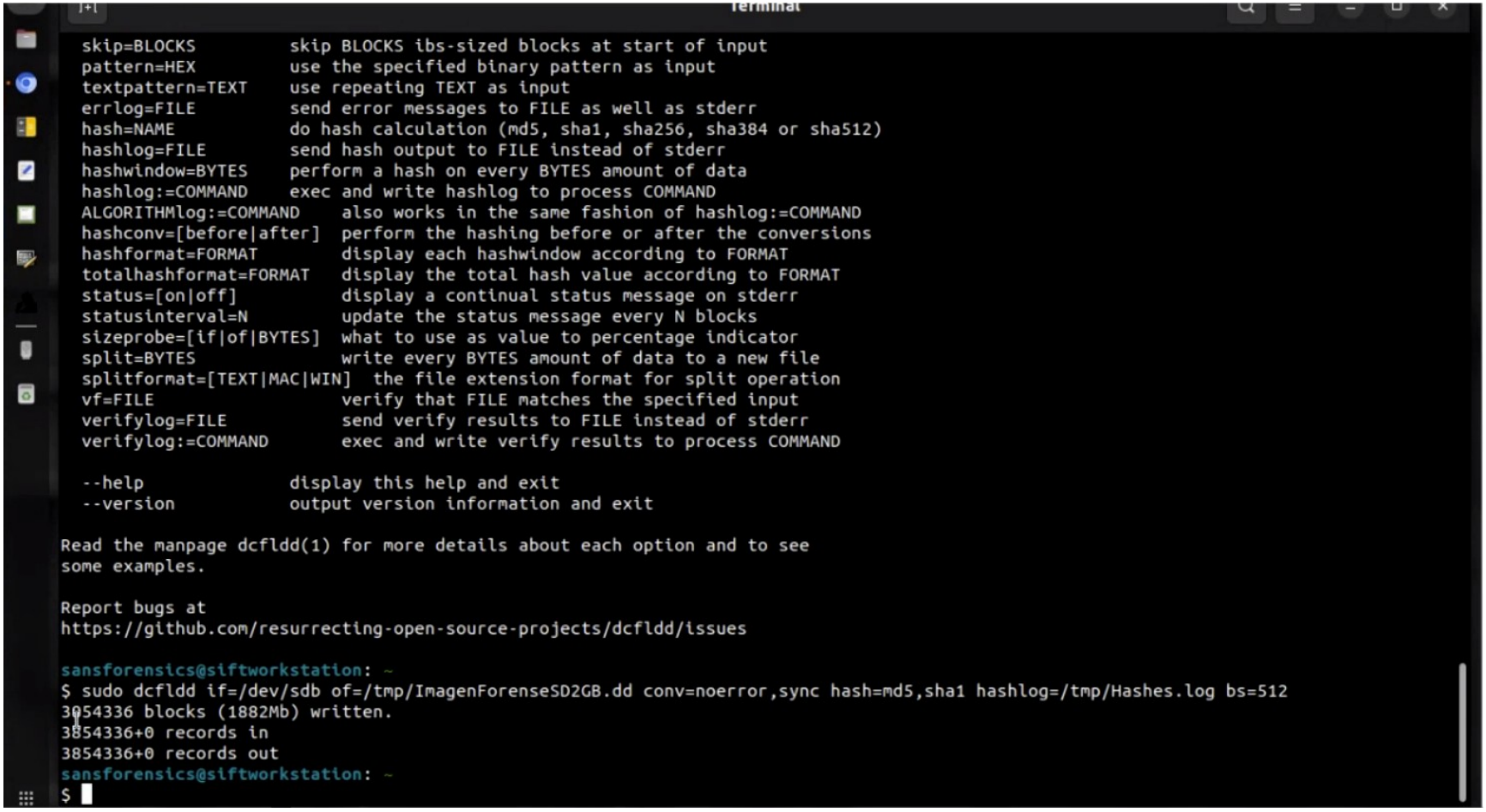
WhatsApp:

https://wa.me/51949304030

Más Información:

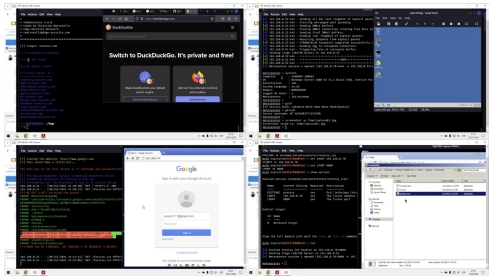
https://www.reydes.com/e/Curso_de_Informatica_Forense

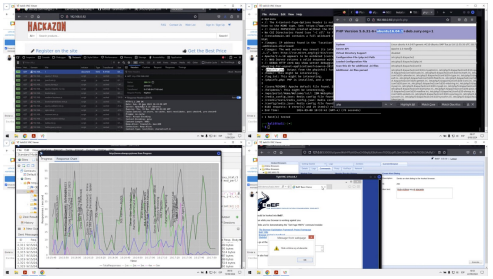
Prácticas

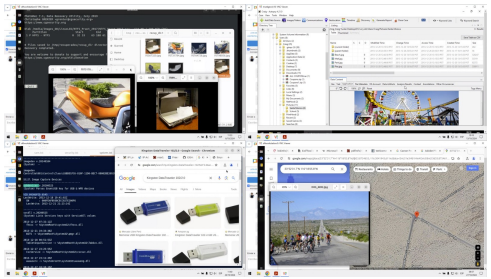

Terminal
skip=BLOCKS skip BLOCKS ibs-sized blocks at start of input
pattern=HEX use the specified binary pattern as input
textpattern=TEXT use repeating TEXT as input
errlog=FILE send error messages to FILE as well as stderr
hash=NAME do hash calculation (md5, sha1, sha256, sha384 or sha512)
hashlog=FILE send hash output to FILE instead of stderr
hashwindow=BYTES perform a hash on every BYTES amount of data
hashlog:=COMMAND exec and write hashlog to process COMMAND
ALGORITHMlog:=COMMAND also works in the same fashion of hashlog:=COMMAND
hashconv=[before|after] perform the hashing before or after the conversions
hashformat=FORMAT display each hashwindow according to FORMAT
totalhashformat=FORMAT display the total hash value according to FORMAT
status=[on|off] display a continual status message on stderr
statusinterval=N update the status message every N blocks
sizeprobe=[if|of|BYTES] what to use as value to percentage indicator
split=BYTES write every BYTES amount of data to a new file
splitformat=[TEXT|MAC|WIN] the file extension format for split operation
vf=FILE verify that FILE matches the specified input
verifylog=FILE send verify results to FILE instead of stderr
verifylog:=COMMAND exec and write verify results to process COMMAND
--help display this help and exit
--version output version information and exit
Read the manpage dcfldd(1) for more details about each option and to see
some examples.
Report bugs at
https://github.com/resurrecting-open-source-projects/dcfldd/issues
sansforensics@siftworkstation: ~
$ sudo dcfldd if=/dev/sdb of=/tmp/ImagenForenseSD2GB.dd conv=noerror,sync hash=md5,sha1 hashlog=/tmp/Hashes.log bs=512
3854336 blocks (1882Mb) written.
3854336+0 records in
3854336+0 records out
sansforensics@siftworkstation: ~
$

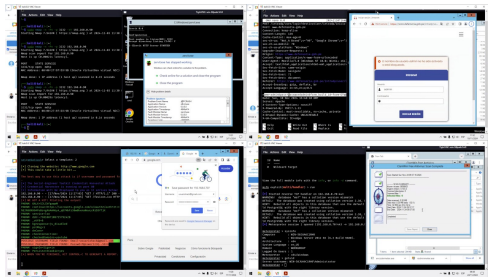
Cursos (Aula Virtual)

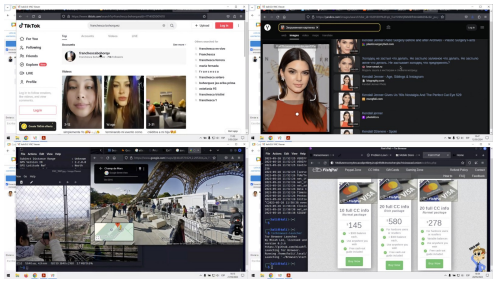
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Bug Bounty
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego CE
- Y más...

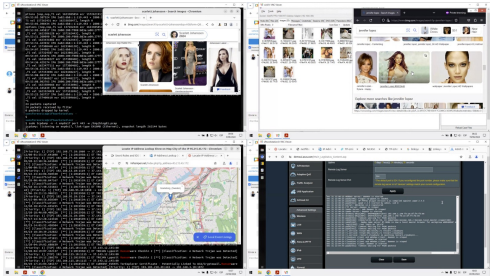












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Más Contenidos

Videos de webinars

https://www.reydes.com/e/videos

Diapositivas de webinars

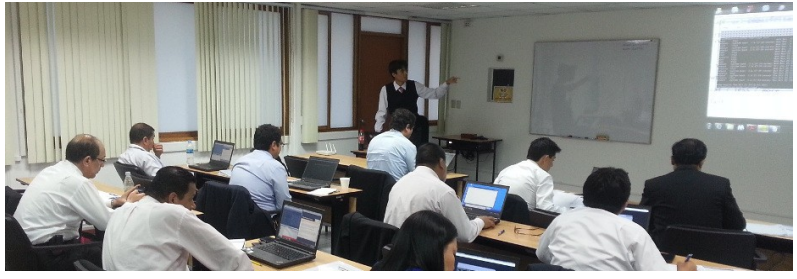
https://www.reydes.com/e/eventos

Libros y artículos

https://www.reydes.com/e/documentos

Blog

https://www.reydes.com/e/blog



Webinar Gratuito

Crear Imágenes Forenses

Alonso Eduardo Caballero Quezada

| Hacking | Forense | Linux | OSINT | Ciberseguridad |

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Lunes 17 de Febrero 2025