Taller Triaje de Datos y Forense Digital (Windows Forensics Analysis)

Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Temario

- Captura de Memoria con FTK Imager
- Captura de Memoria con DumpIT
- Verificar Encriptación del Disco con EDD
- Crear Datos de Triaje con el Replicador de Contenido Personalizado de FTK Imager
- Recolección para Triaje con CyLR
- Montar Imagen Forense con FTK Imager
- Marcas de Tiempo NTFS
- Flujos Alternos de Datos (ADS)
- Volumen Shadow Copy
- Adquirir una Imagen Forense de un Disco con FTK Imager
- Interpretar Metadatos de Archivos con ExifTool
- Reconstrucción de Datos con Photorec

Taller 100% Práctico

Presentación

Este taller abarca el forense digital en los entornos interconectados actuales, y analiza los desafíos asociados con los sistemas operativos Microsoft Windows. El tamaño de los discos duros y medios digitales está incrementando la dificultad, además de consumir más tiempo para manejar apropiadamente los casos digitales. Estar en la capacidad de adquirir datos de manera eficiente y con rigor forense es crucial para todo investigador en la actualidad. En este taller se revisan las técnicas fundamentales, mientras se presentan capacidades para la adquisición basada en triaje y extracción, lo cual incrementa la velocidad y eficiencia del proceso de adquisición.

Inversión

Perú: S/. 95 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: $ 40 Dólares

- Pago mediante PayPal

Escríbeme un mensaje al WhatsApp **https://wa.me/reydes** para proporcionarte los datos pertinentes.

Información

Obtén más información sobre este taller a través de los siguientes mecanismos de contacto.

- WhatsApp: **https://wa.me/reydes**
- Correo electrónico: **reydes@gmail.com**