Recuperación de Archivos

#CIBERCI

CIBERCI
Comunidad Iberoamericana de Ciberseguridad

Alonso Eduardo Caballero Quezada
Consultor e Instructor en Hacking Ético, Forense Digital y GNU/Linux
Perú

Alonso Eduardo Caballero Quezada

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 diecisiete años de experiencia en el área y desde hace trece años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: https://www.ReYDeS.com

CIBERCI

Agenda :

* Recuperar Archivos
* Cinco Capas (Sistema de Archivos)
* Archivos Borrados en FAT
* Archivos Borrados en NTFS
* Método de Metadatos
* Método Capa de Datos
* Demostraciones
* Preguntas

Recuperar Archivos Borrados

El forense es probablemente más conocido por recuperar archivos perdidos o borrados desde un sistema de archivos.

Frecuentemente la recuperación se limitada a la extracción a nivel de la capa de metadatos. La dificultad es los S.O. modernos reciclan rápidamente estas ubicaciones de metadatos borrados, resultando en la sobrescritura de datos.

Cinco Capas (Sistema de Archivos)

* Física: La unidad por si misma

* Sistema de Archivos: Información sobre partición

* Datos: Clusters

* Metadatos: Información de estructura, FAT, NTFS

* Nombre de Archivo: Nombre del Archivo. Jerarquía de Directorio

Archivos Borrados en FAT

Capa Nombre Archivo: Se preserva el nombre del archivo menos la primera letra

Capa Metadatos: Se preserva Fecha modificación, creación y acceso. Tipo archivo, tamaño, direcciones de cluster

Capa Datos: Cluster son mercados como no asignados, pero los datos son preservados. Existe espacio residual.

Archivos Borrados en NTFS

Capa Nombre Archivo: Se preserva el nombre del archivo

Capa Metadatos: Se preserva Fecha modificación, creación, acceso y cambio MFT. Tipo archivo, permisos, tamaño, direcciones de cluster

Capa Datos: Cluster son mercados como no asignados, pero los datos son preservados. Existe espacio residual.

Método de Metadatos

* Puntero de metadatos hacia datos

* Metadatos incluye: Entradas MFT, Entrada directorio FAT

* Utiliza dirección de inicio de clusters, y longitud de archivos

* Puede manejar archivos fragmentados

Método Capa de Datos

* Cabeceras de los archivos

* Se escanea el cluster de inicio, buscando por una cabecera al inicio del cluster

* Se realiza el mejor trabajo para adivinar el fines del archivo, a menos exista su “pie”. Buscándolo o finalizando a un tamaño máximo

Demostraciones

¿Preguntas?

Alonso Eduardo Caballero Quezada

reydes@gmail.com

Perú, 23 de Agosto de 2023

CIBERCI

¡Muchas gracias!

CIBERCI

Recuperación de Archivos

#CIBERCI

CIBERCI
Comunidad Iberoamericana de Ciberseguridad

Alonso Eduardo Caballero Quezada
Consultor e Instructor en Hacking Ético, Forense Digital y GNU/Linux
Perú