CAEN
ESCUELA DE POSGRADO

ANÁLISIS FORENSE

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA
CON MENCIÓN EN TRANSFORMACIÓN DIGITAL

SANS FORENSICS INVESTIGATIVE TOOKKIT (SIFT)

- Creada por expertos de la SANS Institute. (USA)
- Usada durante la capacitación sobre Digital Forensics Incident Response (DFIR).
- Comparable a suites comerciales.
- Open-Source con gran soporte.
- Diseñado para operar de manera virtualizada.


Activities
Aug 9 21:16
sansforensics
Zimmerman-Tools-Poster.pdf
Trash
Hunt-Evil.pdf
Poster_Threat-Intelligence-Co...
SIFT-Cheatsheet.pdf
Network-Forensics-Post...
Windows-to-Unix-Cheatshe...
SIFT-REMnux-Poster.pdf
Hex-File-Regex-Cheatsheet.pdf
DFIR-Smartphone-F...
SQLite-Pocket-Reference.pdf
Windows-Forensics-Post...
mount_points
iOS-3rd-Party-Apps-Poster.pdf
cases
SIFT
WORKSTATION

¿Qué tipo de sistemas de archivo soporta?

- ntfs (NTFS)
- iso9660 (ISO9660 CD)
- hfs (HFS+)
- raw (Raw Data)
- swap (Swap Data)
- memory (RAM Data)
- fat12 (FAT12)
- fat16 (FAT16)
- fat32 (FAT32)
- Ext2
- Ext3
- Ext4
- Ufs1
- Ufs2
- vmdk

PRINCIPALES HERRAMIENTAS

- The Sleuth Kit (File system Analysis Tools)
- Plaso/log2timeline (Timeline Generation Tool)
- ssdeep & md5deep (Hashing Tools)
- Foremost/Scalpel (File Carving)
- WireShark (Network Forensics)
- Vinetto (thumbs.db examination)
- Pasco (IE Web History examination)
- Rifiuti (Recycle Bin examination)
- Volatility Framework (Memory Analysis)
- DFLabs PTK (GUI Front-End for Sleuthkit)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)

Adquisición de la evidencia

- Herramientas Linux y Windows (FTK Imager).

Analisis de evidencia

- Volatility
- The Sleuth Kit (File system Analysis Tools)

Presentación

- Entrega de Informe Final.

RECURSOS ADICIONALES

- Registro y Creación de Línea de tiempo de un Sistema de Archivos: https://www.sans.org/blog/digital-forensic-sifting-registry-and-filesystem-timeline-creation/

- Creación de una línea de tiempo con log2timeline: https://www.sans.org/blog/digital-forensic-sifting-super-timeline-creation-using-log2timeline/

- GIAC Certified Forensic Analyst (GCFA): https://www.sans.org/cyber-security-courses/advanced-incident-response-threat-hunting-training/