Análisis Forense a Sistemas Windows

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético & Forense Digital

Sitio Web: www.reydes.com / Correo Electrónico: reydes@gmail.com

5 de Mayo del 2020
LATAM

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 y Pen Testing.

Instructor y expositor en OWASP Perú, PERUHACK, 8.8 Lucky Perú. Más de 16 años de experiencia y desde hace 12 años labora 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.

https://twitter.com/Alonso_ReYDeS

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

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

http://www.reydes.com

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

reydes@gmail.com

¿Forense Digital?

Forense Digital

Rama de la ciencia forense abarcando la recuperación e investigación de material encontrado en dispositivos digitales, frecuentemente relacionados con crímenes cometidos por computadoras.

El Forense de computadoras es una rama de la ciencia forense digital, pertinente a la evidencia encontrada en computadoras y medios digitales de almacenamiento.

Su objetivo es examinar medios digitales de una manera “forense”, con el propósito de identificar, preservar, recuperar, analizar, y presentar hechos sobre la información digital.

El análisis forense es la etapa donde se realiza una investigación profunda, cuyo propósito es identificar objetivamente y documentar los culpables, razones, ruta y consecuencias de un incidente de seguridad, violación de las leyes, etc.

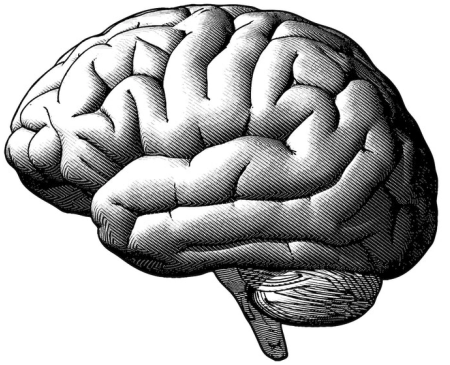
¿Cómo es un Laboratorio Forense?

Un Laboratorio Forense Digital

Alonso Eduardo Caballero Quezada -:- Sitio Web: www.reydes.com -:- Correo Electrónico: reydes@gmail.com

¿Cuales Herramientas Forenses se Utilizan?

Software Forense



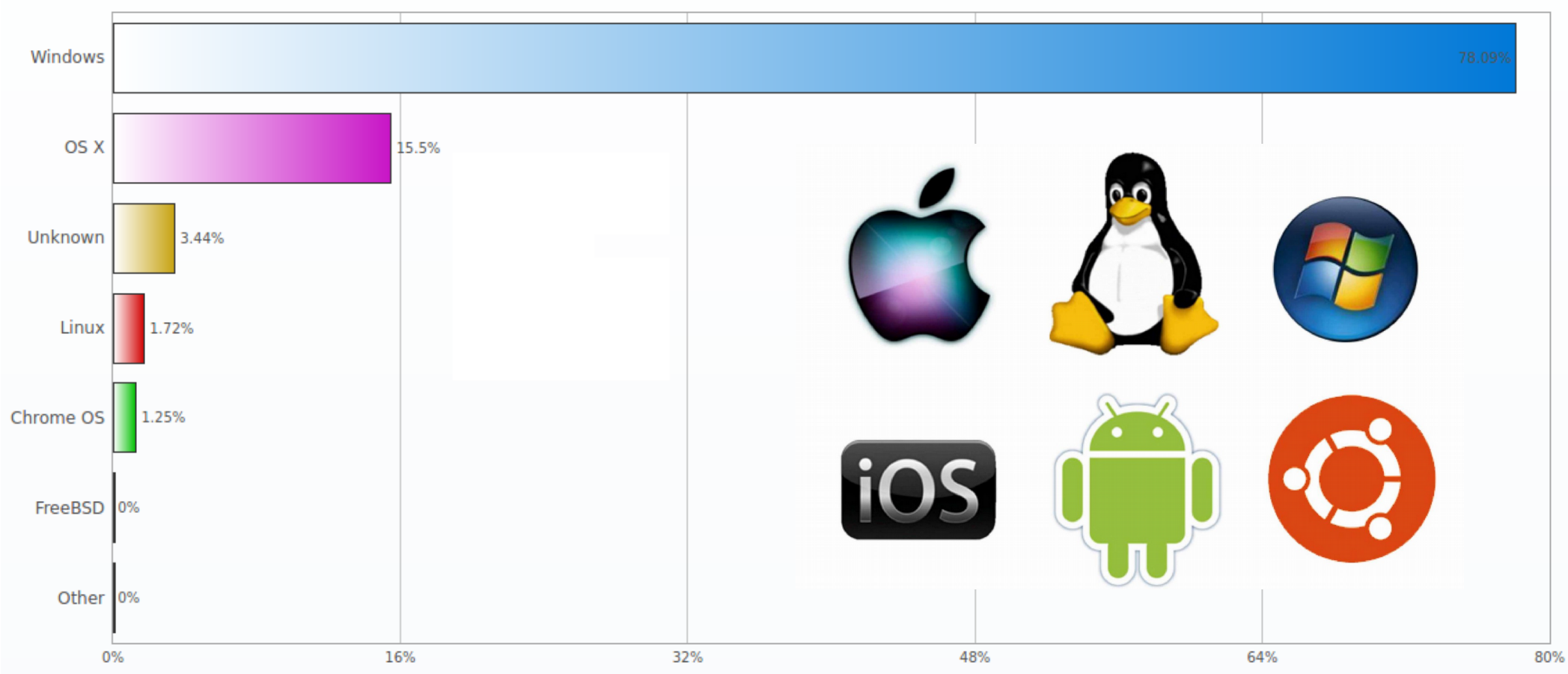
* https://www.guidancesoftware.com/encase-forensic
* https://accessdata.com/products-services/forensic-toolkit-ftk
* https://www.magnetforensics.com/for-forensic-examiners/
* https://www.autopsy.com/
* https://digital-forensics.sans.org/community/downloads

Hardware Forense

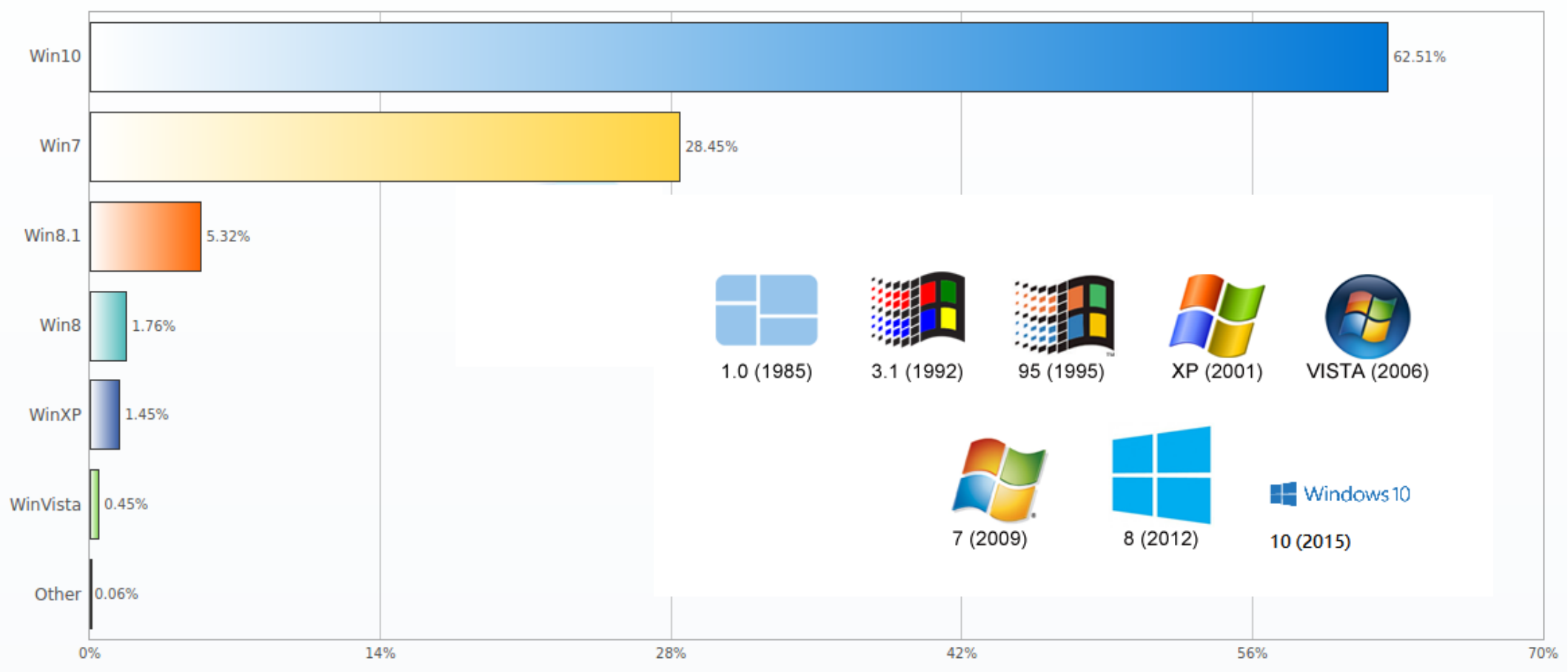
* https://forensicstore.com/all-products/

¿Cuanto se utiliza Windows?

Mercado de Sistemas Operativos de Escritorio (abril 2019 - 2020)



Mercado de Versiones de Windows (abril 2019 - 2020)



Alonso Eduardo Caballero Quezada -:- Sitio Web: www.reydes.com -:- Correo Electrónico: reydes@gmail.com

¿Qué es SIFT Workstation?

SIFT WorkStation

La estación de trabajo SIFT está constituida de un grupo de herramientas open source libres para respuesta de incidentes y forense, siendo diseñado para realizar exámenes forenses digitales detallados en una diversidad de escenarios.

SIFT puede ser utilizado como cualquier suite de herramientas para respuesta de incidentes y forense. Demuestra las capacidades avanzadas para respuesta de incidentes, y las técnicas forenses digitales profundas, las cuales pueden realizarse utilizando herramientas open source de última generación, las cuales está disponibles libremente y se actualizan frecuentemente.

SIFT

* SIFT Workstation: https://digital-forensics.sans.org/community/downloads
* Ubuntu: https://www.ubuntu.com/

Características de SIFT

Es exitosamente utilizado en respuesta de incidentes y forense digital, y está disponible libremente como servicio público. Continúa siendo la herramienta open source más popular de este tipo

- Base Ubuntu LTS 16.04
- Sistema base de 64 bits
- Mejor utilización de memoria
- Actualización automática de paquetes DFIR y personalizaciones
- Las últimas herramientas y técnicas forenses
- Disponible un Appliance VM listo para trabajar en forense
- Compatibilidad cruzada entre Linux y Windows
- Opción para instalar un sistema autónomo mediante un instalador “SIFT-CLI”
- Documentación del proyecto
- Soporte ampliado para sistemas de archivos

* SIFT Documentation: http://sift.readthedocs.io/en/latest/

Herramientas en SIFT

Paquetes: Afterglow, binplist, bulk_extractor, dumppig, flowgrep, libbde, libdata-heify-perl, libesedb, libevt, libetvx, libewf, liblnk, libfile-mork-perl, libfvde, libfwsi, liblightgrep, liblnk, libmac-popertylist-perl, libmsiecf, libolecf, libpff, libqcow, libregf, libsmdev, libmsraw, libvhdi, libvmdk, libvshadow, libxml-entities-perl, log2timeline-perl, mac-robber, maltegoce, mantaray, ntdsxtract, ntopng, pdf-tools, pyelftools, python-bencode, python-construct, python-dfvfs, python-pdkt, python-plaso, python-pyparsing, pytsk, re2, regripper, sleuthkit, volatility, windows-perl, xmount, etc.

Scripts: Denisityscout, extract_mft_record_slack,py, ga_parser.py, java_idx_parser, jobparser.py, page_brute, pe_carver, pescanner.py, shellbags.py, shimchacheparser.py, sqlparser.py, etc.

* SIFT Tools, Commands and Scripts: http://sift.readthedocs.io/en/latest/tools/index.html

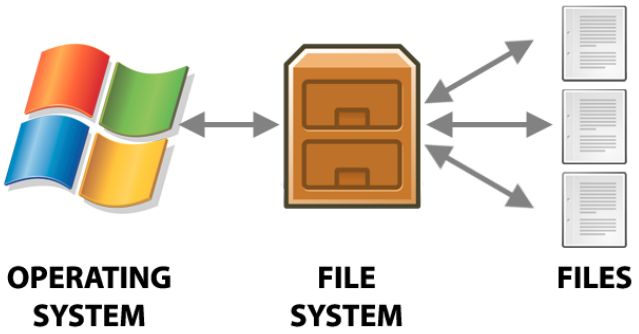
Ejemplos de Análisis en un Sistema Windows

Alonso Eduardo Caballero Quezada -:- Sitio Web: www.reydes.com -:- Correo Electrónico: reydes@gmail.com

Sistema de Archivos en Windows

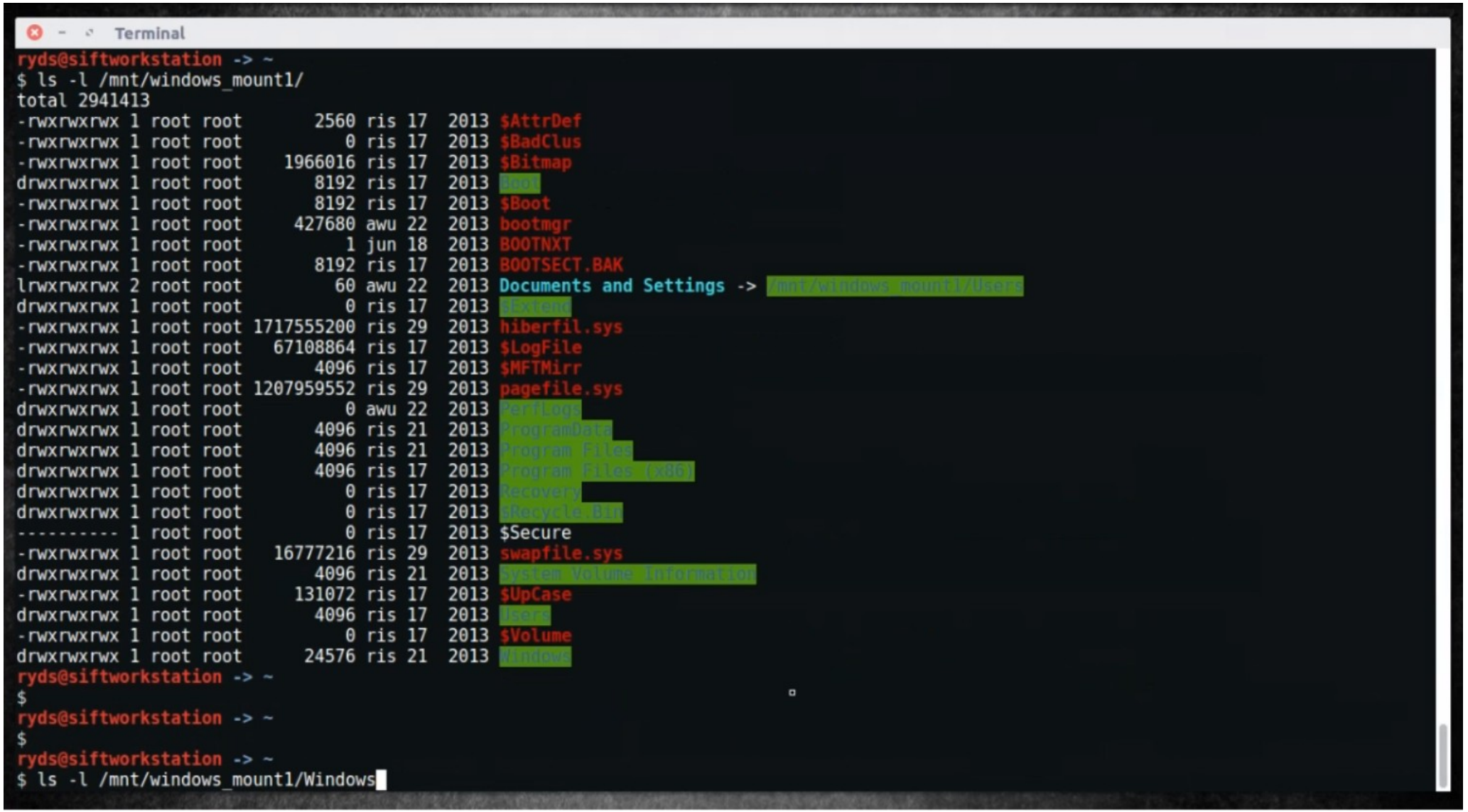
Tiene principalmente dos generaciones de sistemas de archivos. El primer sistema de archivos, FAT (File Allocation Table), fue utilizado en versiones anteriores de los sistemas Windows / MS-DOS, y creció desde sistemas de archivos de 12 bits denominado FAT12, hasta sistemas de archivos de 32 bits denominado FAT32. El segundo sistema de archivos, NTFS (New Technology File System) fue introducido con Windows NT, y es utilizado hasta las versiones más recientes de Windows.

- Master Boot Record
- Sistema de Archivos FAT
- Recuperar Particiones FAT
- Recuperar Particiones NTFS

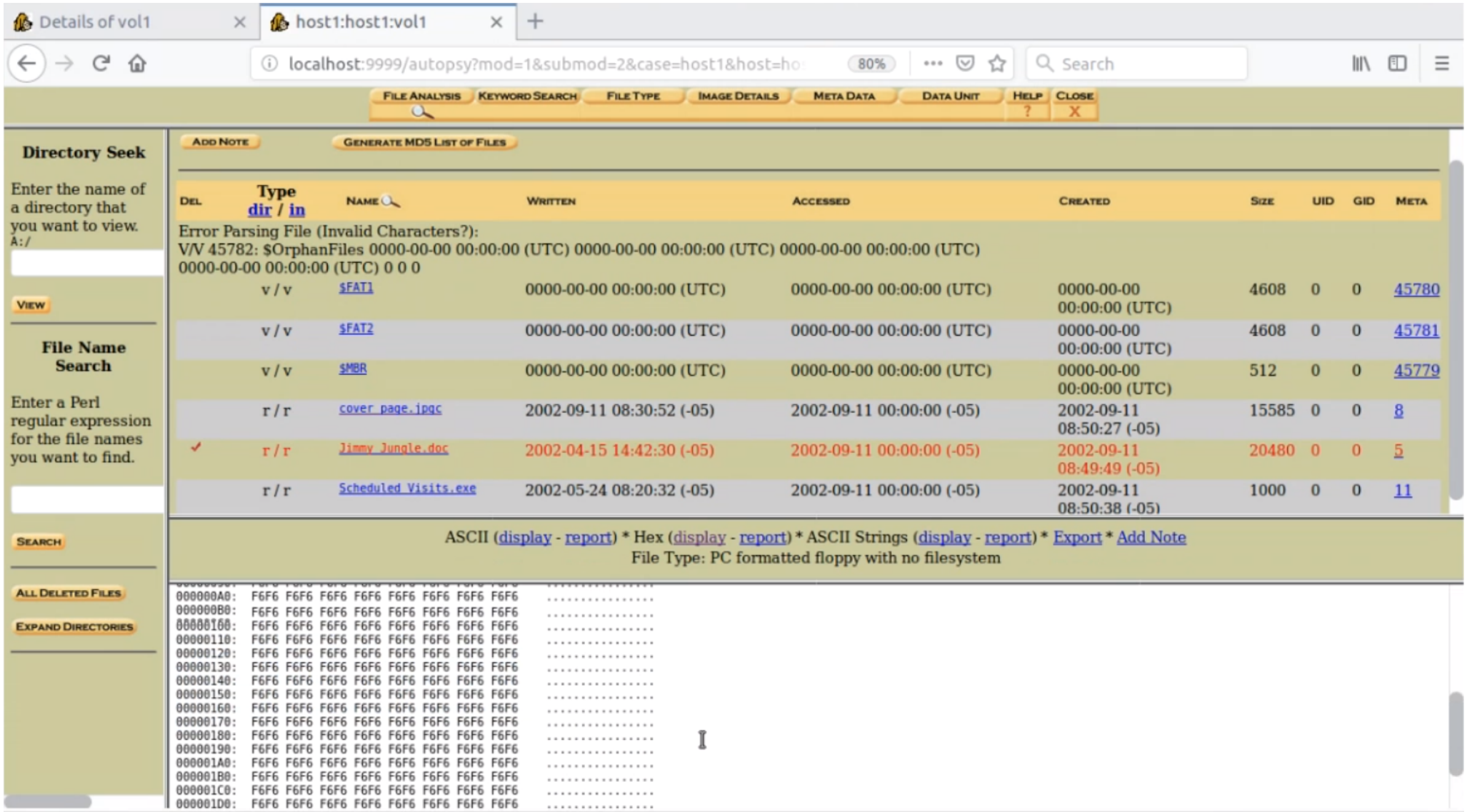


* https://technet.microsoft.com/en-us/library/cc938438.aspx
* https://technet.microsoft.com/en-us/library/cc776720(v=ws.10).aspx
* https://technet.microsoft.com/en-us/library/cc778410(v=ws.10).aspx
* https://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx

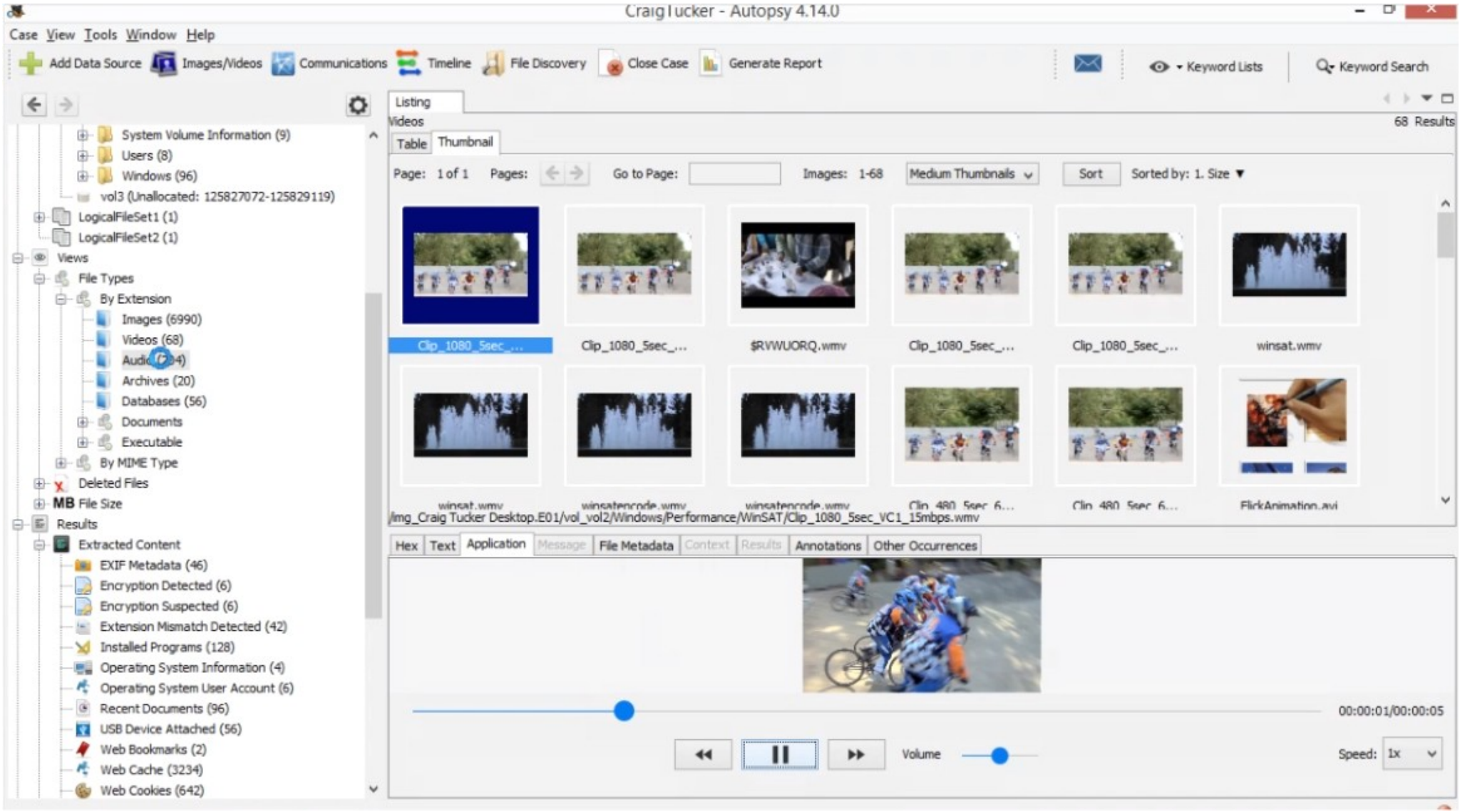
Sistema de Archivos en Windows (Cont.)



Sistema de Archivos en Windows (Cont.)



Sistema de Archivos en Windows (Cont.)



Memoria RAM

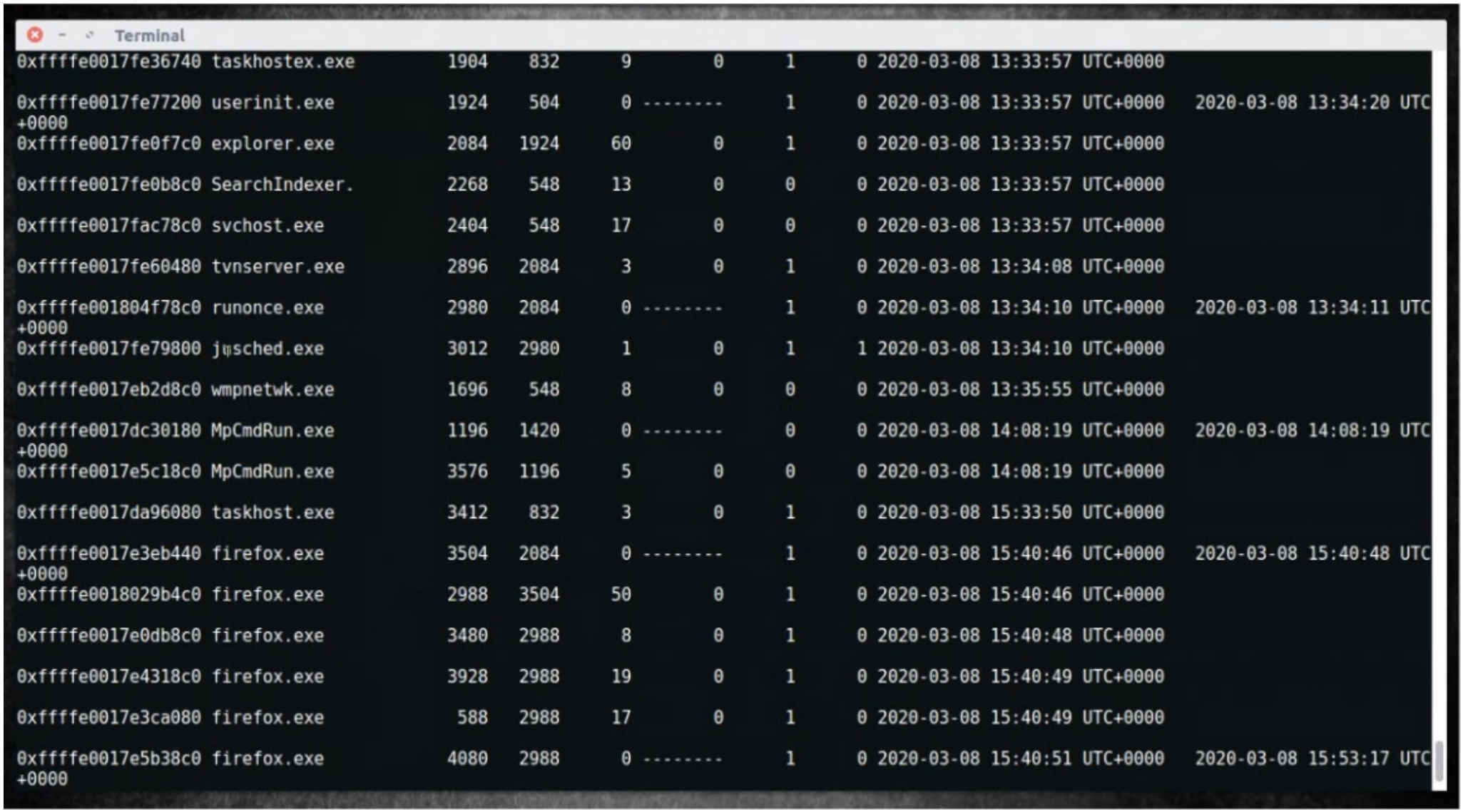
La adquisición de la memoria RAM, se ha convertido en uno de los más importantes cambios en el campo forense de computadoras.

Al responder a incidentes, se requiere recolectar y preservar tanta evidencia volátil como sea posible, incluyendo la memoria RAM.

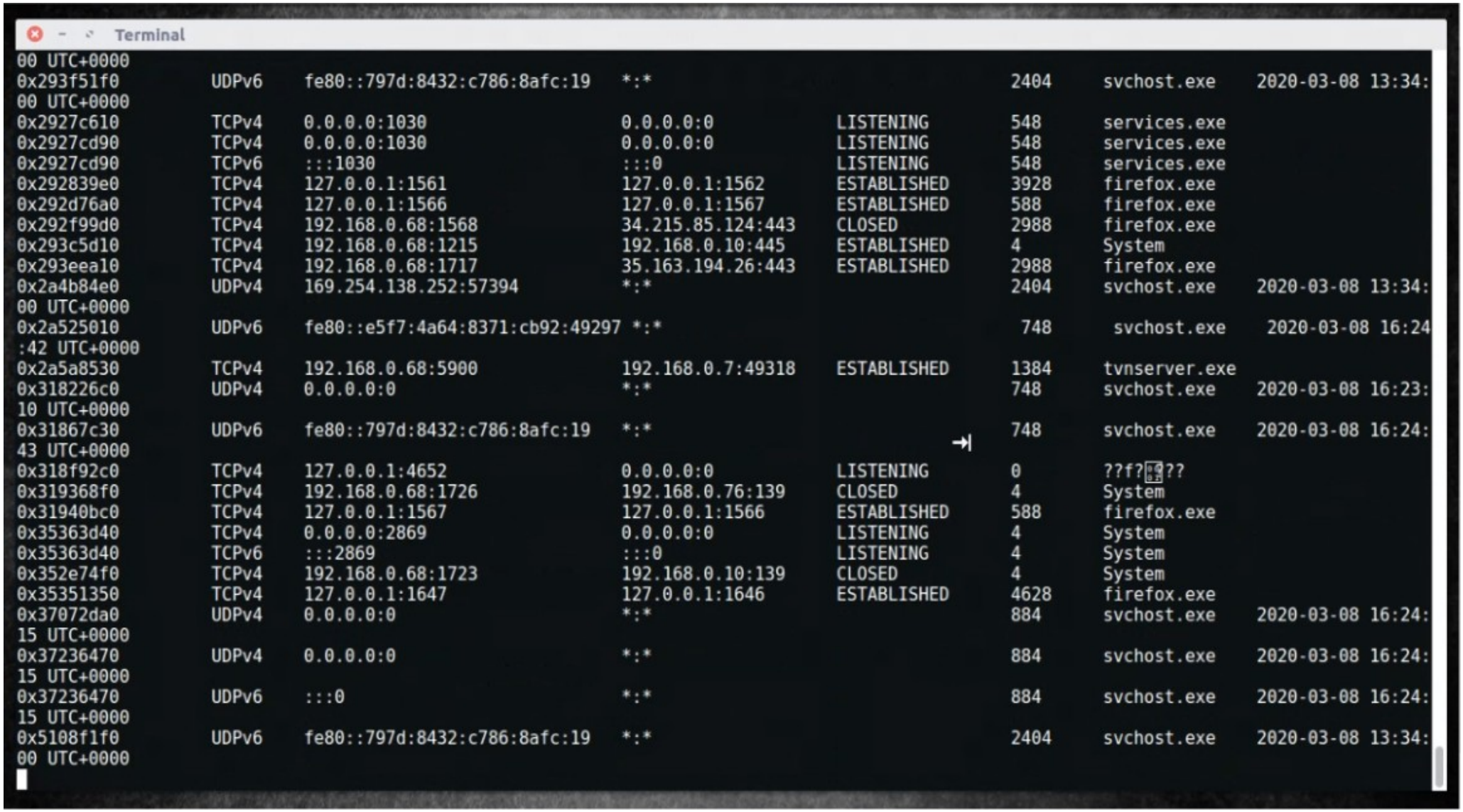
Inevitablemente se realizarán cambios o alteraciones durante este proceso. Pero con el conocimiento y experiencia, también se está en la capacidad de sustentar este accionar.

Los datos volátiles son datos los cuales desaparecerán o serán destruidos una vez el sistema de cómputo sea apagado. Típicamente es la RAM, pero existe más, como conexiones de red activas, aplicaciones en funcionamiento, etc. Muchos de estos datos son extremadamente valiosos para determinar o refutar diversos argumentos.

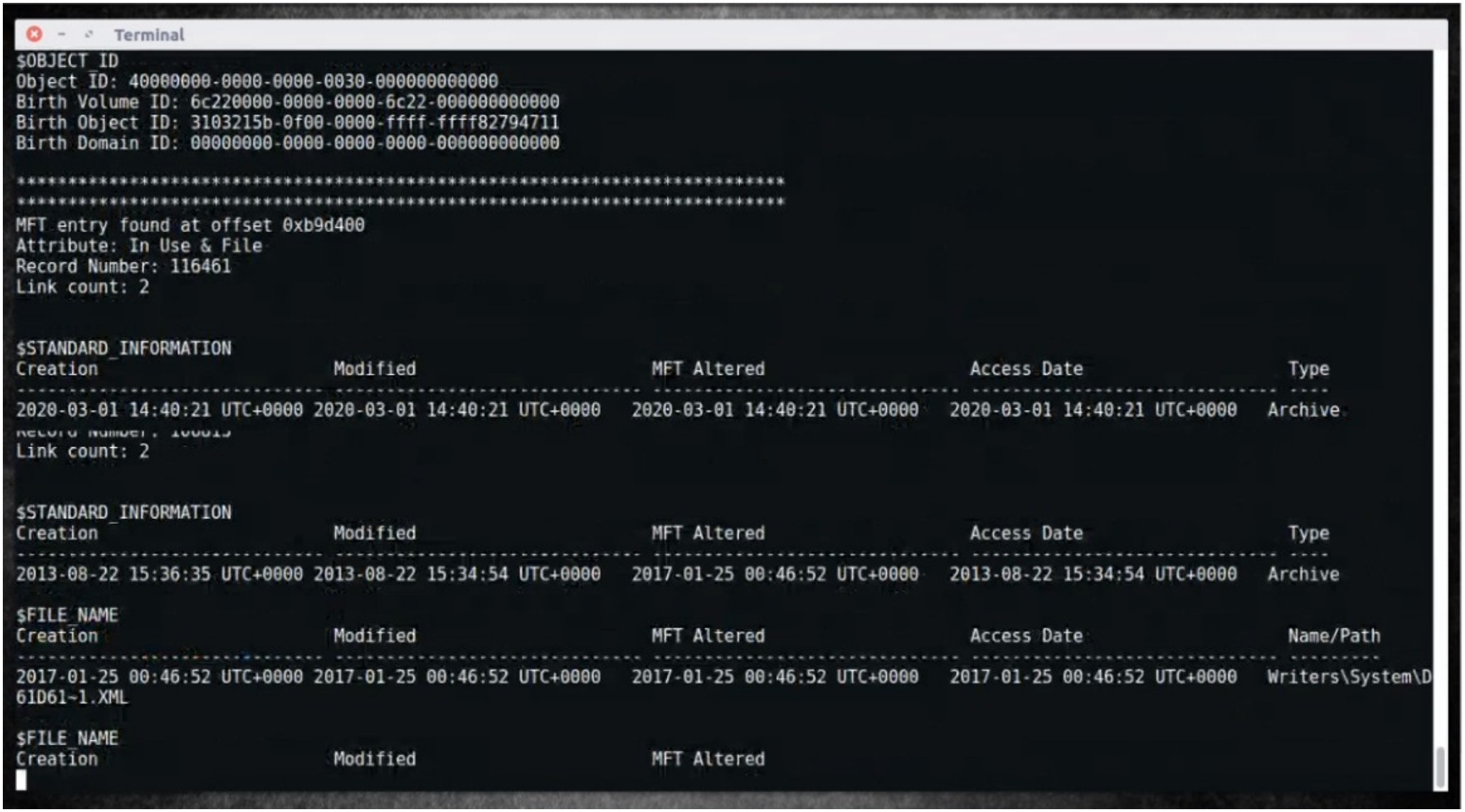
Memoria RAM (Cont.)



Memoria RAM (Cont.)



Memoria RAM (Cont.)



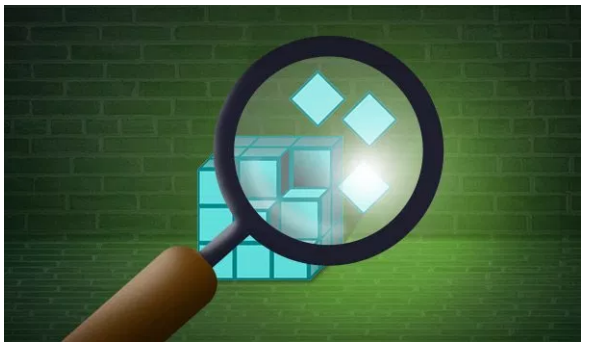
Artefactos de Windows

Al utilizar Windows, se crean, borran, modificación y acceden hacia muchos archivos. Algunos de estos patrones o tipos específicos de cambios, son lo suficientemente únicos para permitir exponer con certeza la comisión de una acción.

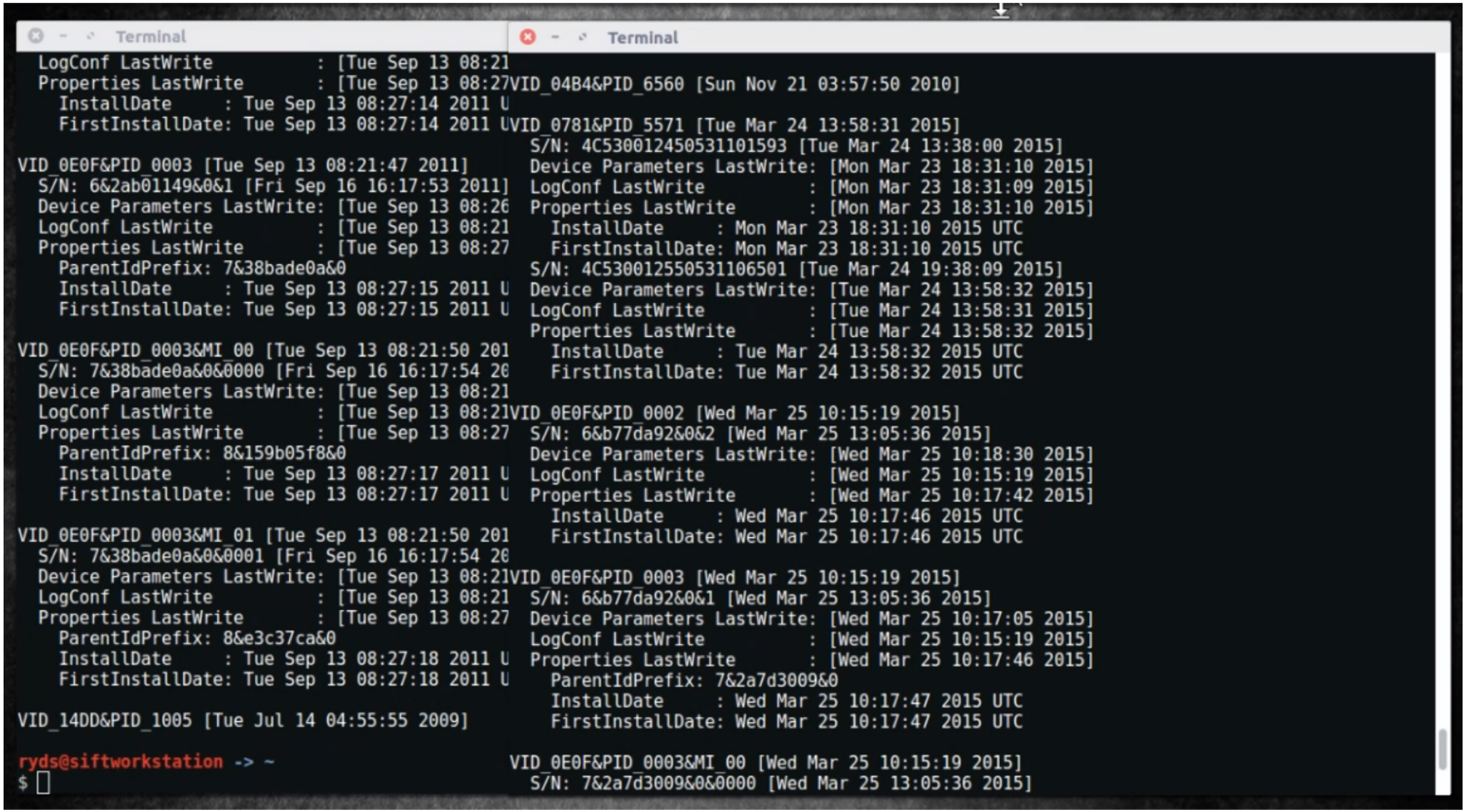
Si se fallase en determinar si existen o no, se podría llegar a conclusiones incorrectas, o no sustentar los argumentos correctos.

Los artefactos de Windows se convierten en puntos clave para una investigación, y conducen hacia la investigación de evidencia.

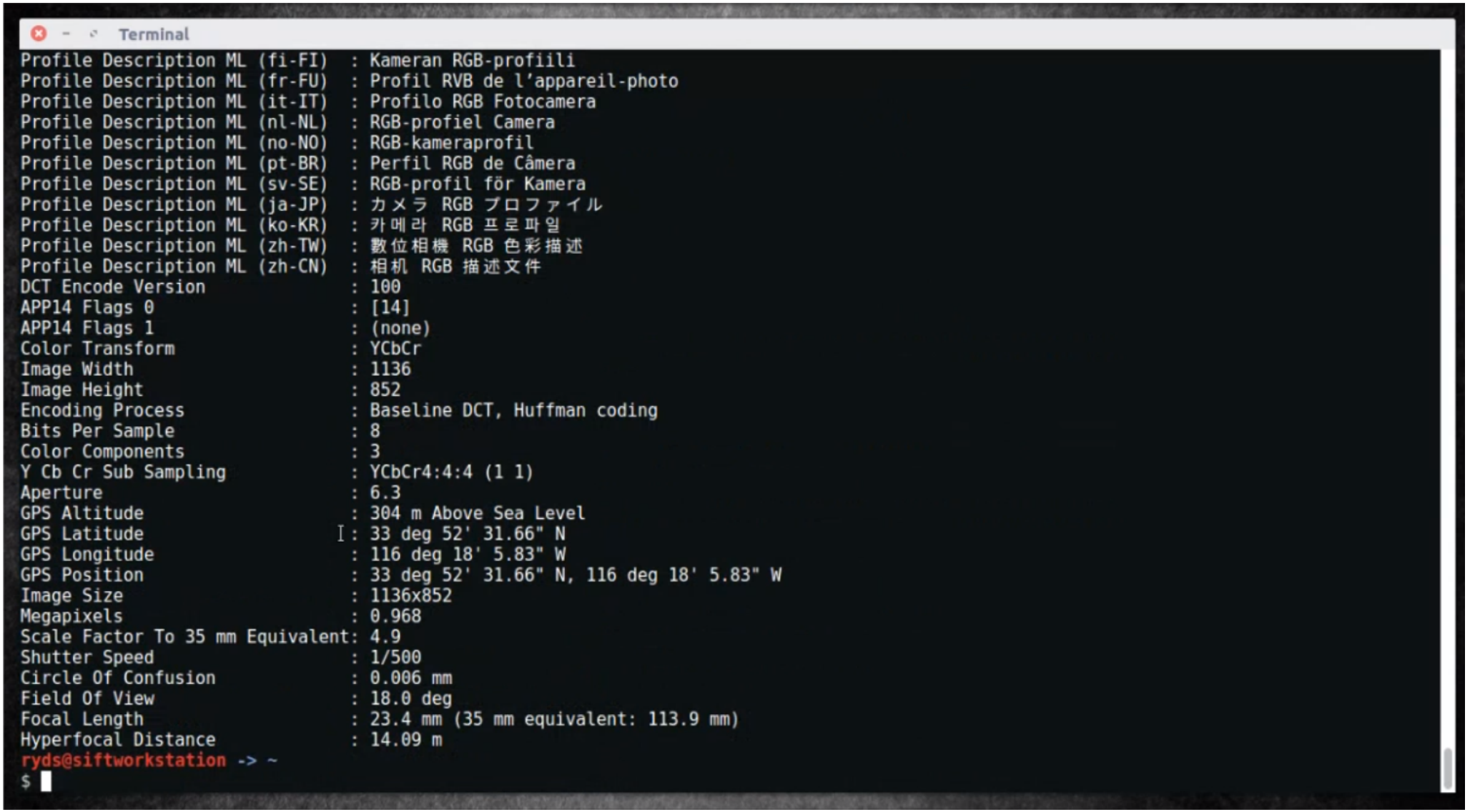
- Papelera de reciclaje
- Archivos LNK
- Dispositivos USB extraíbles
- Metadatos en documentos Office.
- UserAssist, etc.



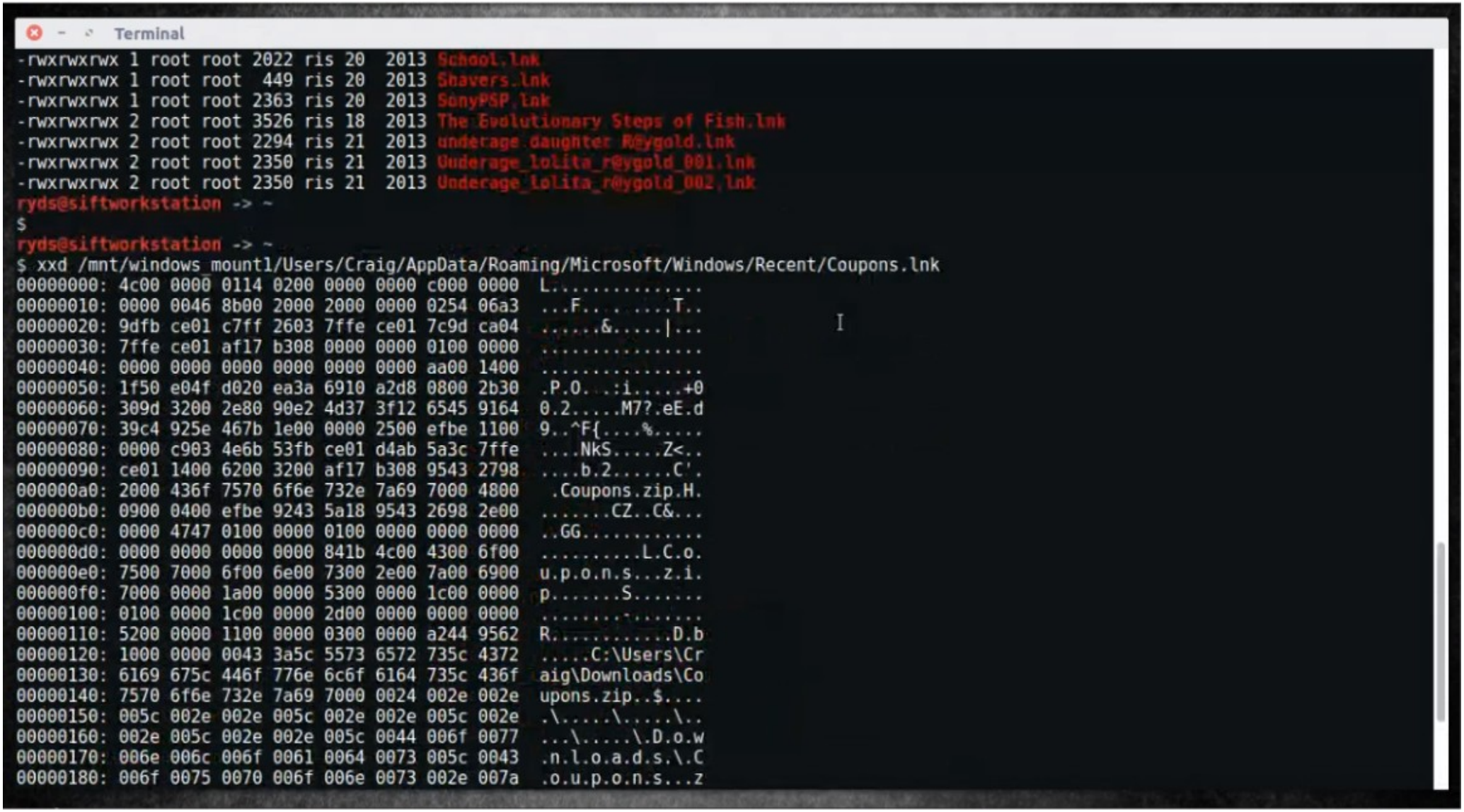
Artefactos de Windows (Cont.)



Artefactos de Windows (Cont.)



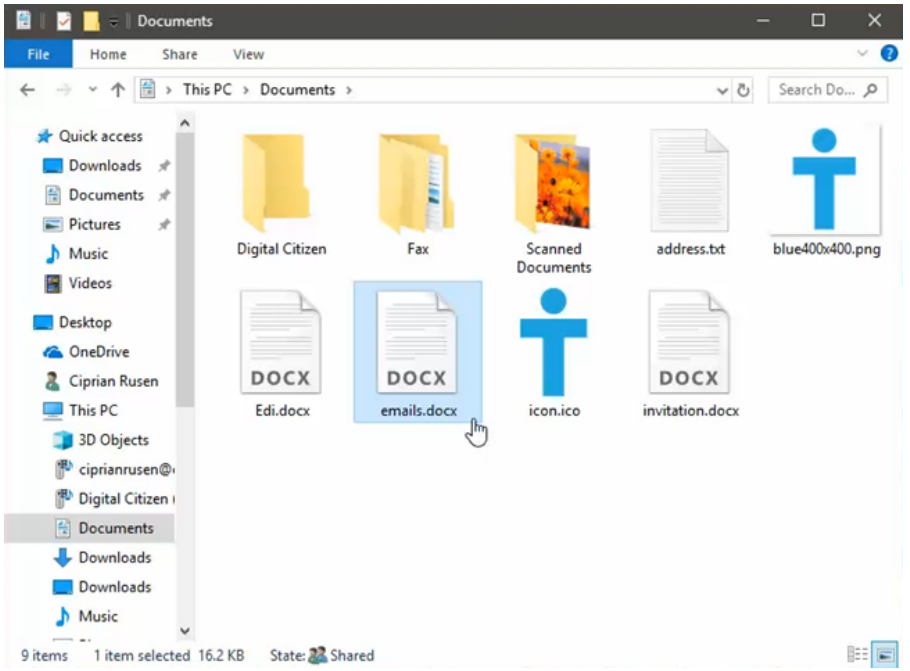
Artefactos de Windows (Cont.)



Pero... ¿Cuanto puede conoer Windows sobre nosotros?

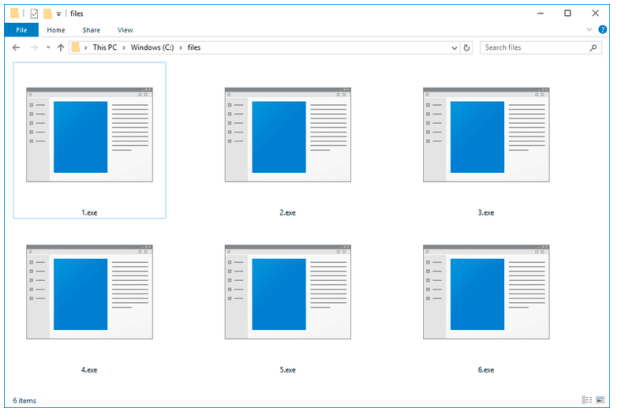
Descarga de Archivos

- Open / Save MRU (Most Recently Used)
- Email Attachments (Adjuntos de correo electrónico)
- Skype History (Historial de Skype)
- Browser Artifacts (Artefactos del navegador web)
- Downloads (Descargas)
- ADS (Alternate Data Stream) Zone.Identifier



Ejecución de Programas

- UserAssist
- Windows 10 Timeline (Cronología de Windows 10)
- RecentApps
- Shimcache
- Jump Lists
- Amcache.hve
- System Resource Usage Monitor - SRUM (Vigilancia de uso de recursos del sistema)
- BAD (Background Activity Moderator) / DAM
- Last-Visited MRU (Most Recently Used)
- Prefetch



Archivos Borrados o Archivos con Conocimiento

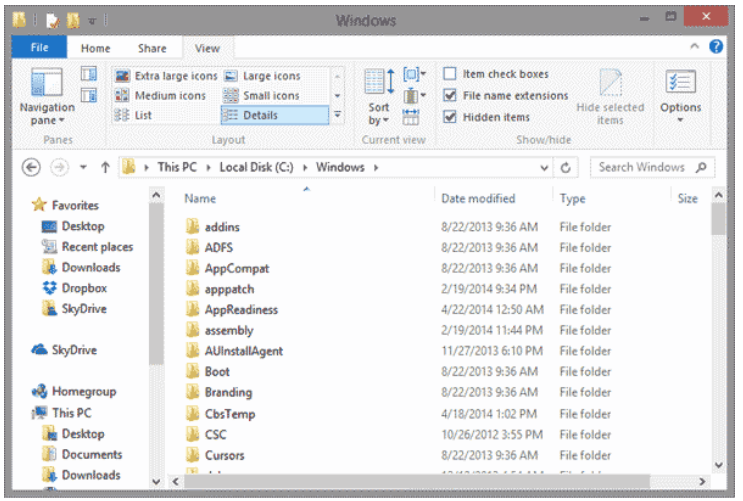
- XP Search - ACMRU
- Thumbcache (Miniaturas)
- Thumbs.db
- IE (Internet Explorer)/Edge file://
- Search - WordWhellQuery
- Win7/8/10 Recycle Bin (Papelera de reciclaje)
- Last-Visited MRU (Most Recently Used)
- XP Recycle Bin (Papelera de Reciclaje)

Actividad de la Red / Ubicación Física

- Timezone (Zona horaria)
- Cookies
- Network History (Historial de red)
- WLAN (Wireless Local Area Network) Event Log (Registro de eventos de WLAN (Redes inalámbricas de área local))
- Browser Search Terms (Términos de búsqueda en el navegador)
- System Resource Usage Monitor - SRUM (Vigilancia de uso de recursos del sistema)

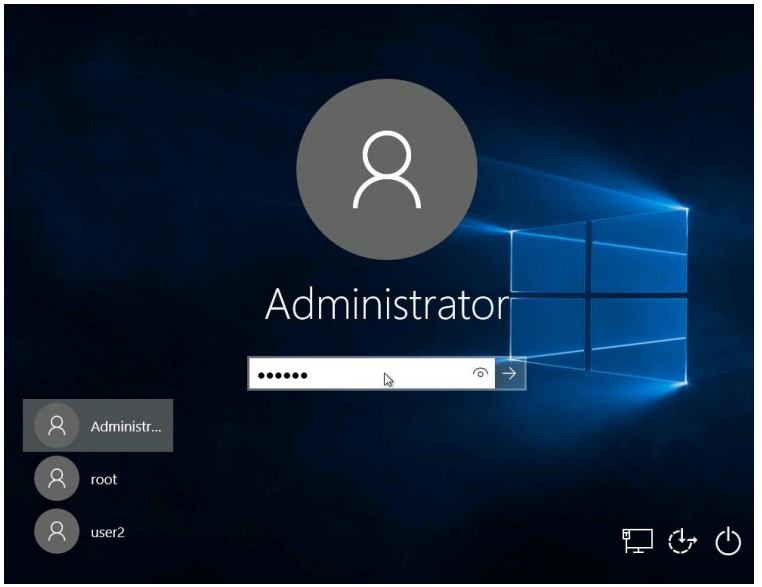
Apertura de Archivos / Carpetas

- Open / Save MRU (Most Recently Used)
- Recent Files (Archivos recientes)
- Jump Lists
- Shell Bags
- Shortcut (LNK) Files (Archivos de enlace)
- Prefetch
- Last-Visited MRU
- IE (Internet Explorer)/Edge file://
- Office Recent Files (Archivos recientes de office)



Utilización de las Cuentas

- Last Login (Último login)
- Last Password Change (Último cambio de la contraseña)
- RDP (Remote Desktop Protocol) Usage (Uso de RDP)
- Services Events (Eventos de servicvios)
- Logon Types (Tipos de login)
- Authentication Events (Eventos de autenticación)
- Success / Fail Logons (Logins fallidos y exitosos)



Utilización USB / Dispositivos Externos

- Key Identification (Identificación de claves)
- First / Last Times (Tiempo inicial y final)
- User (Usuario)
- PnP (Plug and Play) Events (Eventos PnP)
- Volume Serial Number (Número de serie del volumen)
- Drive Letter and Volume Name (Nombre del volumen y letra de unidad)
- Shortcut (LNK) Files (Archivos de enlace)

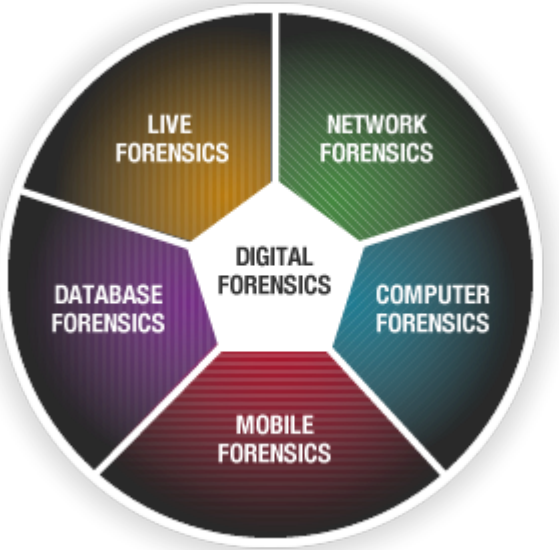
Utilización del Navegador

- History (Historial)
- Cookies
- Cache
- Flash & Super Cookies
- Session Restore (Restauración de sesión)
- Google Analytics Cookies

¿Más Forense Digital?

Otras Áreas del Forense Digital

- Forense de Sistemas Windows
- Respuesta de Incidentes
- Forense de Redes
- Análisis de Malware
- Forense de Sistemas Mac
- Forense de Memoria RAM
- Forense de Teléfonos Inteligentes
- Forense a la Nube, etc...



Curso Virtuales Disponibles en Video

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

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

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

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

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

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

Y todos mis cursos virtuales:

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

Más Contenidos

Videos de 52 webinars gratuitos

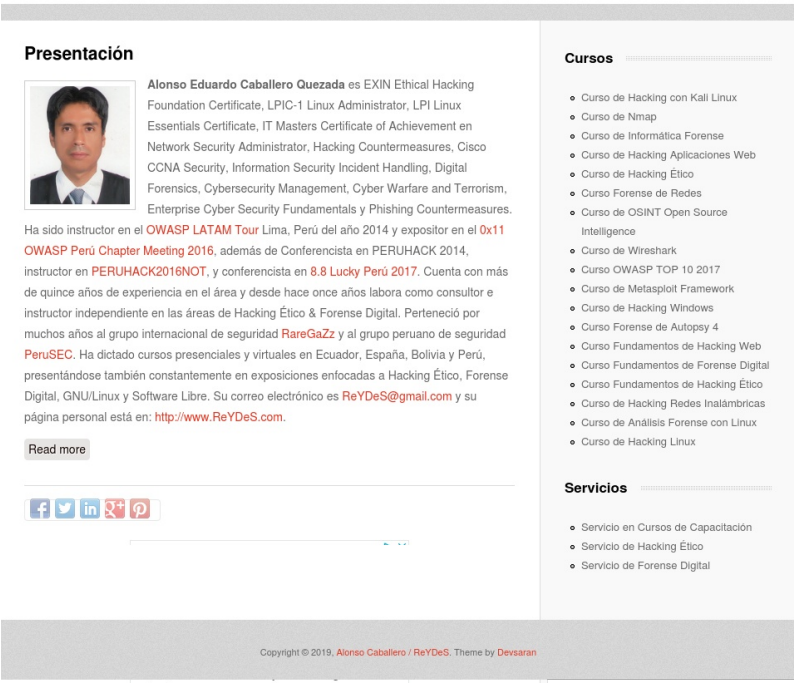
http://www.reydes.com/d/?q=videos

Diapositivas de los webinars gratuitos

http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

http://www.reydes.com/d/?q=node/2



Blog sobre temas de mi interés.

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

¡Muchas Gracias !

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético & Forense Digital

Sitio Web: www.reydes.com / Correo Electrónico: reydes@gmail.com

5 de Mayo del 2020
LATAM