ANÁLISIS FORENSE

- El "**Análisis Forense Informático"** es la **agrupación de técnicas científicas y técnicas de análisis especializadas en las infraestructuras tecnológicas**.
- Esas técnicas nos posibilitan realizar una **identificación, preservación, análisis y presentación** de datos y documentación, que pueden ser válidamente aceptados en un proceso legal.

El análisis forense informático es efectivo para las siguientes situaciones:

- · Recuperar la información o la tecnología afectada
- · Asegurar la protección de datos y su cumplimiento
- · Minimizar las pérdidas en un determinado ataque o incidente
- · Prevenir o evitar ciberataques en el futuro
- · Servir de ayuda en el análisis y recolección de pruebas a la autoridad judicial competente
- · Ser una herramienta de peritaje en los sistemas internos de control de una entidad

- Los TTP (Tácticas, Técnicas y Procedimientos) de un atacante son las acciones que realiza y métodos que utiliza a medida que avanza y desarrolla el ataque. Desarrollar un ataque, desde el reconocimiento hasta el logro del objetivo, proporciona información procesable en dos áreas.

Las Tácticas

- Las tácticas representan el objetivo táctico de un adversario, es decir, el vector con el que los ciberdelincuentes buscan desarrollar su actividad y lograr su objetivo. Por ejemplo: escalada de privilegios, movimientos laterales o exfiltración.

Las Técnicas

-
- Las Técnicas representan la manera o los métodos que un atacante utiliza para conseguir alcanzar o realizar una Táctica. También representa lo que el adversario obtiene cuando realiza una acción. Ejemplos de Técnicas son fuerza bruta o manipulación de cuentas.

- Además, cada Táctica puede estar compuesta de varias Técnicas, ya que pueden existir muchas maneras diferentes de alcanzar un objetivo. Por ejemplo, para realizar un movimiento lateral se puede optar por atacar el RDP o usar Técnicas como SSH Hijacking o vulnerar las carpetas de administrador de Windows (como C$)…
- Los Procedimientos
- Los Procedimientos son las implementaciones especificas (como por ejemplo, las herramientas) y los pasos concretos que los atacantes usan para llevar a cabo las Técnicas con las que finalmente alcanzar sus objetivos o estrategias.

Los Procedimientos

-
- Los Procedimientos son las implementaciones especificas (como por ejemplo, las herramientas) y los pasos concretos que los atacantes usan para llevar a cabo las Técnicas con las que finalmente alcanzar sus objetivos o estrategias.

- Los conocimientos de defensa de sistemas informáticos se basan en entender las técnicas utilizadas por los atacantes.
- **Uno de los principales objetivos del Blue Team es reconocer brechas de ciberseguridad y bloquear a los atacantes de la forma más rápida posible**

- **Tenemos un esquema conceptual que sirve para definir el nivel de riesgo de cada acción de un atacante en un sistema comprometido**.

- **Amenazas Avanzadas Persistentes:**
-

- Cuando se habla de APT´s, descrita en inglés: **Advanced Persistent Threat**.

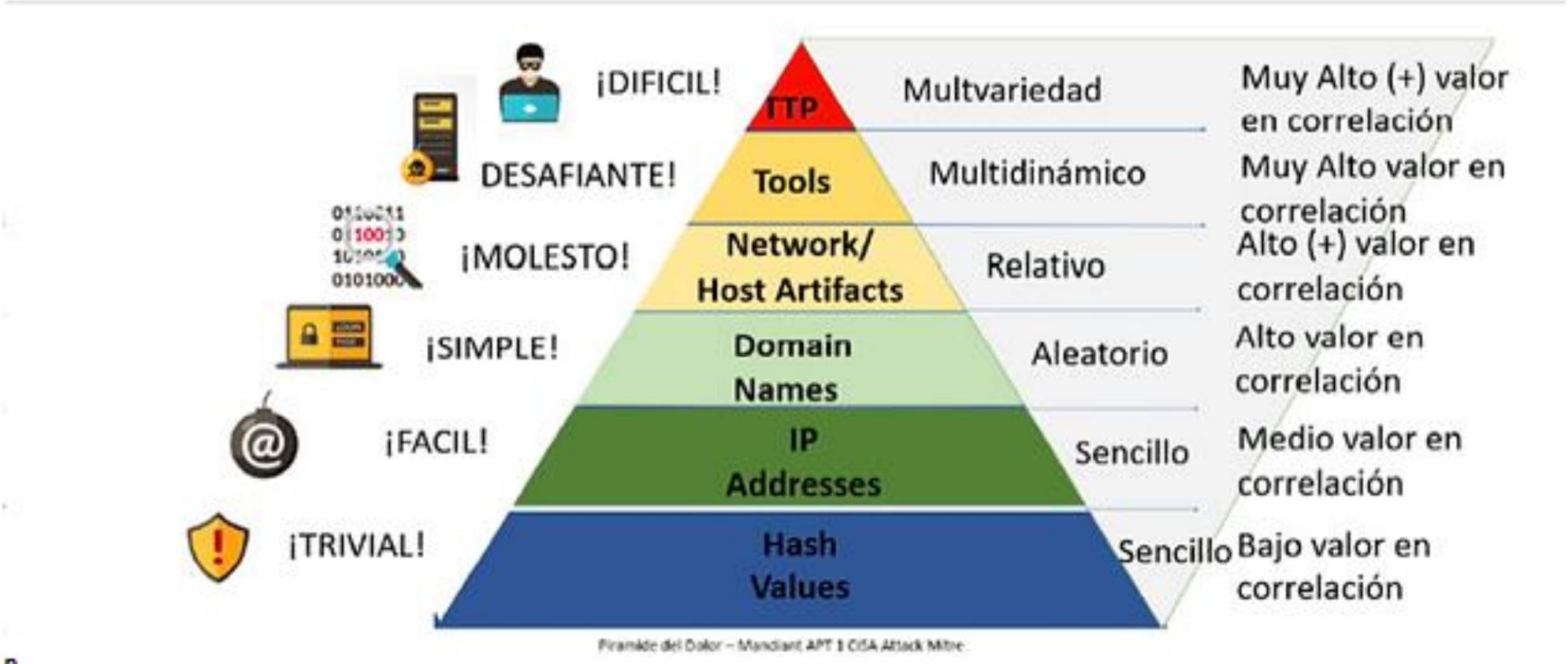
- La amenaza avanzada persistente se logra definir como aquella que debidamente está estructurada y debidamente fundada, la cual posee elementos de intrusión, *tácticas, técnicas y herramientas* avanzadas y puede consecuentemente recibir instrucciones para poder avanzar respecto de un objetivo en específico.
- De tal manera que, los elementos particulares de un APT están debidamente asociados a esa serie de herramientas y técnicas para poder ejecutar determinada labor en el objetivo (victima)

- ***Primera fase - Reconocimiento:*** *Escaneo de la red, mapeo de la red, perfilación de empleados, búsqueda de 6día cero.*
- ***Segunda Fase – Liberar:*** *Búsqueda de Emails, creación de malware (troyanos), creación de URL´s maliciosas, envío de Phishing dirigido*
- ***Tercera fase - Explotación:*** *Liberar el phishing dirigido, explotar la máquina del usuario (victima), obtener las credenciales del usuario, escanear la red interna.*
- ***Cuarta fase - Operación:*** *Localizar los datos objetivo, localizar los usuarios con privilegios, elevar los privilegios de acceso, acceder a datos sensibles.*
- ***Quinta Fase – Colección de datos:*** *Seleccionar servidores intermediarios, trasladar datos sensibles, empaquetar y comprimir los datos, encriptar los datos.*
- ***Sexta fase - Exfiltración:*** *Seleccionar servidores de descarga, establecer canales extensos de Comando y Control, iniciar conexiones externas y extraer la información*.
-

- Estas líneas permiten a los investigadores de ciberseguridad poder tomar las fases del ciclo de vida de un ciberataque y poder determinar un antes, durante y después de poder entender lo mencionado por dentro de las TTP´s , en donde se define cada una de ellas para poder realizar análisis dentro de la pirámide del dolor.
-

Pirámide del dolor

La Pirámide del Dolor refleja la relación entre diferentes tipos de indicadores que pueden llegar a utilizarse para detectar a un adversario, frente al potencial daño que denegar dichos indicadores puede provocar a los atacantes. También refleja la dificultad de conseguir dicha inteligencia para poder usarla contra el adversario.



- **Valores hash: trivial:**
- El acceso a los valores hash de contraseñas y datos de un sistema o aplicación web se considera trivial para la seguridad. **Las funciones hash son algoritmos matemáticos que producen valores únicos, que corresponden directamente a un archivo**. La función hash de un fichero puede hallarse fácilmente a partir del mismo. No obstante, es imposible encontrar un archivo a partir de su valor hash.

- **Direcciones IP: fácil**
- **El rango de direcciones IP que corresponden al sistema de una red corporativa es fácil de encontrar**. Existen páginas web que le permiten a cualquier usuario averiguar esta información y realizar un mapeo de la red. No obstante, es importante recordar que hacer estos mapeos de forma no autorizada es ilegal.
- **Nombres de dominio: simple**
- Encontrar los nombres de dominio, subdominios y subdirectorios de una aplicación son tareas simples si se ejecutan con las herramientas correctas. **MassDNS, por ejemplo, es una potente herramienta para hacer *fuzzing* o fuerza bruta de subdominios**. Estas tareas también están prohibidas para ejecutar en entornos no autorizados, pero no se considera que representen un riesgo alto para el sistema.

- **Redes y equipos: molesto**
- Ahora bien, el **escaneo de redes y equipos sí se considera «molesto», según la pirámide del dolor en ciberseguridad**. Esta tarea se puede ejecutar por medio de *softwares* como Nmap, pero, como hemos dicho anteriormente, no es legal hacerlo sin autorización. Para practicar esta técnica de *pentesting*, es necesario hacerlo en un entorno virtual propio, en juegos CTF o en programas de Bug Bounty.
- **Herramientas: retador**
- **Reconocer las herramientas, es decir, los *softwares* y *hardwares* que se utilizan dentro de una red corporativa**, es retador para el Blue Team de una compañía, ya que esto **le permite a los atacantes indagar sobre si hay fallos de seguridad en la tecnología**. De este modo, se pueden hallar vulnerabilidades de día cero, que son incidentes de seguridad altamente retadores para los equipos de defensa.
- **Técnicas y protocolos: difícil**
- **Cuando los atacantes despliegan técnicas y protocolos para vulnerar el sistema**, se considera que es difícil generar una respuesta, según la pirámide del dolor en ciberseguridad.

- **Redes y equipos: molesto**
- Ahora bien, el **escaneo de redes y equipos sí se considera «molesto», según la pirámide del dolor en ciberseguridad**. Esta tarea se puede ejecutar por medio de *softwares* como Nmap, pero, como hemos dicho anteriormente, no es legal hacerlo sin autorización. Para practicar esta técnica de *pentesting*, es necesario hacerlo en un entorno virtual propio, en juegos CTF o en programas de Bug Bounty.
- **Herramientas: retador**
- **Reconocer las herramientas, es decir, los *softwares* y *hardwares* que se utilizan dentro de una red corporativa**, es retador para el Blue Team de una compañía, ya que esto **le permite a los atacantes indagar sobre si hay fallos de seguridad en la tecnología**. De este modo, se pueden hallar vulnerabilidades de día cero, que son incidentes de seguridad altamente retadores para los equipos de defensa.
- **Técnicas y protocolos: difícil**
- **Cuando los atacantes despliegan técnicas y protocolos para vulnerar el sistema**, se considera que es difícil generar una respuesta, según la pirámide del dolor en ciberseguridad.

- modificar son los dominios. El mayor problema está en el registro, pero entre dominios comprometidos, los servicios de DNS dinámico, y otras diversas posibilidades un atacante puede modificar sus dominios

- Un piso más arriba están los artefactos de red y host. Aquí entramos en un terreno que empieza a suponer un reto para los atacantes, ya que es prácticamente imposible realizar una actividad realmente significativa sin dejar rastro en los logs. A nivel de host podríamos hablar de ficheros, entradas de registro, cadenas en memoria, etc., y a nivel de red tenemos ejemplos en cadenas de user-agent concretas, patrones de URI que se repiten, tamaños de petición y/o respuesta, y otros. Muchos de estos elementos se pueden modificar, pero comienzan a ser muchos los parámetros que deben ser tenidos en cuenta para ocultar su presencia en nuestros sistemas y redes.

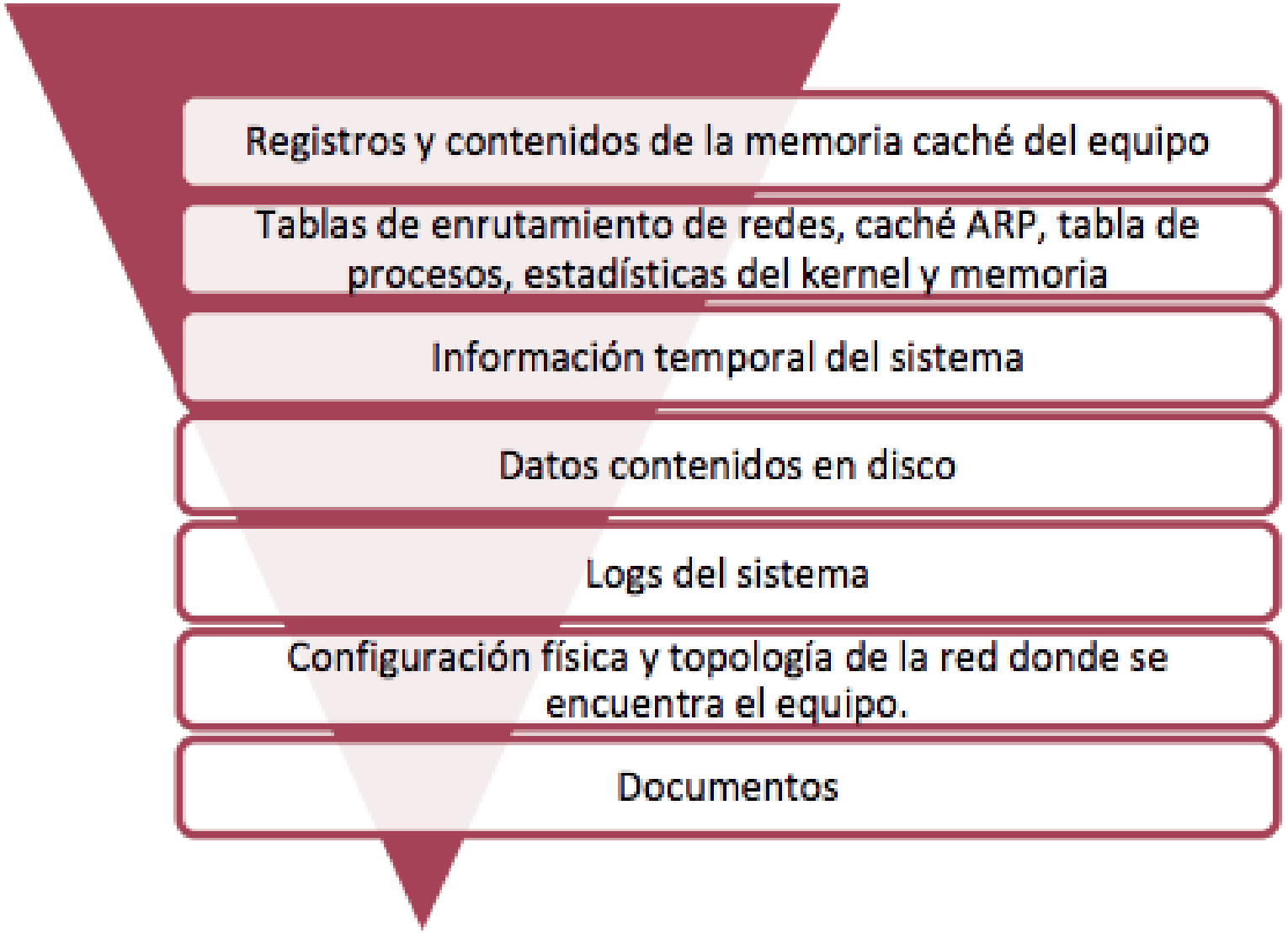
- Denegar el acceso a herramientas es otro paso más en la pirámide del dolor. Observar una y otra vez la misma herramienta te ayuda a generar reglas que te permiten detectarla, aunque el atacante intente realizar cambios sobre ella, modificando su hash e incluso eliminando las firmas para tu propio antivirus. En última instancia, forzamos al atacante a investigar nuevas herramientas o desarrollar una nueva.
-

FASES

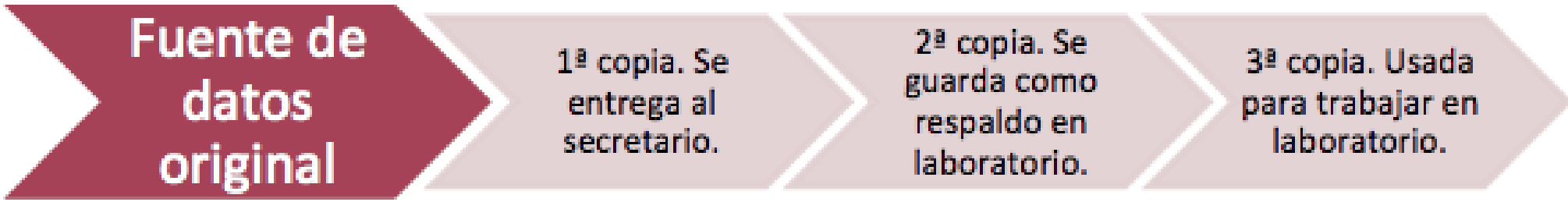
Procesos

- **Asegurar la escena** se trata de la primera fase y no siempre se aplica, su objetivo es impedir que nadie pueda alterar algo.
- **Identificación de evidencias**, se debe constatar qué evidencias deben recogerse para un análisis posterior, se deben identificar los dispositivos y sistemas a analizar y distinguir qué evidencias hay que destacar.
- **Adquisición de datos** se trata de una fase crítica debido a la posibilidad de modificar por error alguna de las evidencias digitales. Un error de este estilo podría invalidar las pruebas en un posible proceso judicial.
- **Análisis de datos** es la etapa en la que se busca información útil en relación a las evidencias, en este punto se estudian los ficheros donde puede estar la información eliminada, registros, logs del sistema, ficheros, etc
- **Presentación e informe de resultados** finalizado el análisis forense se debe redactar un informe pericial con conclusiones y justificación del sistema de trabajo empleado. El informe debe ser claro y conciso ya que puede terminar como prueba en los tribunales.

1.- Identificación de evidencias



2.- Recolección de evidencias



3.- PRESERVACIÓN DE LAS EVIDENCIAS

- La documentación de la cadena de custodia deberá contener también todos los lugares por donde ha pasado la evidencia y quién ha realizado su transporte y su acceso.

4.- ANÁLISIS DE LAS EVIDENCIAS

- Sistema operativo del sistema.
- Programas instalados en el equipo.
- Hardware, accesorios y periféricos que forman parte del sistema.
- Datos relativos a la conectividad del equipo:
  - Si dispone de firewall, ya sea físico o lógico.
  - Si el equipo se encuentra en zonas de red especiales, por ejemplo, DMZ.
  - Si tiene conexión a Internet o utiliza proxies.
- Datos generales de configuración que puedan ser de interés para el investigador para ayudar en la tarea.

Pasos

- En todo caso, se pueden destacar varios pasos, que habrá que adaptar en cada caso:
- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema.

4.1 .- Entorno de trabajo

- Análisis en caliente:
  - Uso de discos originales
- Análisis en frío
  - Usamos máquinas virtuales

4.2.- Creación de línea temporal

- Para crear la línea temporal, lo más sencillo es referirnos a los tiempos MACD de los archivos, es decir, las fechas de modificación, acceso, cambio y borrado, en los casos que aplique. Es importante, como ya se ha indicado en alguna ocasión tener en cuenta los husos horarios y que la fecha y hora del sistema no tienen por qué coincidir con los reales. Este dato es muy importante para poder dar crédito a las pruebas y a la investigación en general.

4.3.- Determinación de actuación

- La investigación sobre la memoria del equipo.
- Es interesante realizar un volcado de memoria para la obtención de cierta información

4.4.- Identificación de autores

4.5 .- Impacto

FASE 5: Redactar informe: INFORME EJECUTIVO:

- Motivos de la intrusión.
  - ¿Por qué se ha producido el incidente?
  - ¿Qué finalidad tenía el atacante?
- Desarrollo de la intrusión
  - ¿Cómo lo ha logrado?
  - ¿Qué ha realizado en los sistemas?
- Resultados del análisis.
  - ¿Qué ha pasado?
  - ¿Qué daños se han producido o se prevén que se producirán?
  - ¿Es denunciable?
  - ¿Quién es el autor o autores?
- Recomendaciones.
- ¿Qué pasos dar a continuación?
- ¿Cómo protegerse para no repetir los hechos?

FASE 5: Redactar informe: INFORME TÉCNICO:

- Antecedentes del incidente.
  - Puesta en situación de cómo se encontraba la situación anteriormente al incidente.
- Recolección de datos.
  - ¿Cómo se ha llevado a cabo el proceso?
  - ¿Qué se ha recolectado?
- Descripción de la evidencia.
  - o Detalles técnicos de las evidencias recolectadas, su estado, su contenido, etc.

FASE 5: Redactar informe: INFORME TÉCNICO:

- Entorno de trabajo del análisis.
  - ¿Qué herramientas se han usado?
  - ¿Cómo se han usado?
- Análisis de las evidencias.
  - Se deberá informar del sistema analizado aportando datos como las características del sistema operativo, las aplicaciones instaladas en el equipo, los servicios en ejecución, las vulnerabilidades que se han detectado y la metodología usada.

FASE 5: Redactar informe: INFORME TÉCNICO:

-
- Descripción de los resultados.
  - ¿Qué herramientas ha usado el atacante?
  - o ¿Qué alcance ha tenido el incidente?
  - o Determinar el origen del mismo y como se ha encontrado.
- Dar la línea temporal de los hechos ocurridos con todo detalle.
- Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado.
- Dar unas recomendaciones sobre cómo proteger los equipos para no repetir el incidente o sobre cómo actuar legalmente contra el autor.

Detección y Análisis

Detección y Análisis - Nivel 1

- MITRE también creó algunos scripts que ayudan a detectar una gran cantidad de técnicas:
  - Proceso y supervisión de la línea de comandos, a menudo recopilados por Sysmon, Windows Event Collection y muchos SIEM y plataformas EDR;
  - Monitoreo de archivos y registros, también recopilados por las mismas herramientas anteriores;
  - Registros de autenticación, como los recopilados del controlador de dominio a través de los registros de eventos de Windows;
  - Captura de paquetes, especialmente captura entre hosts

¿Cómo es un Laboratorio Forense?

¿Cuales Herramientas Forenses se Utilizan?

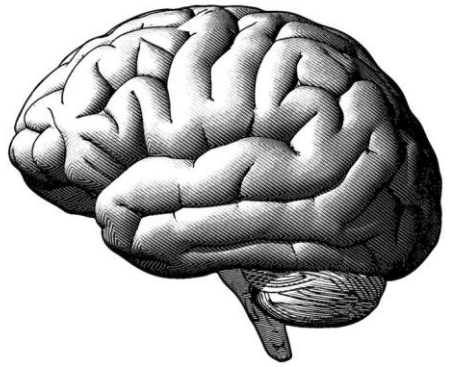
ACCESSDATA
ForensicToolkit (FTK)

EnCase®

MAGNET
FORENSICS®

AUTOPSY
DIGITAL FORENSICS

SIFT



Software usado

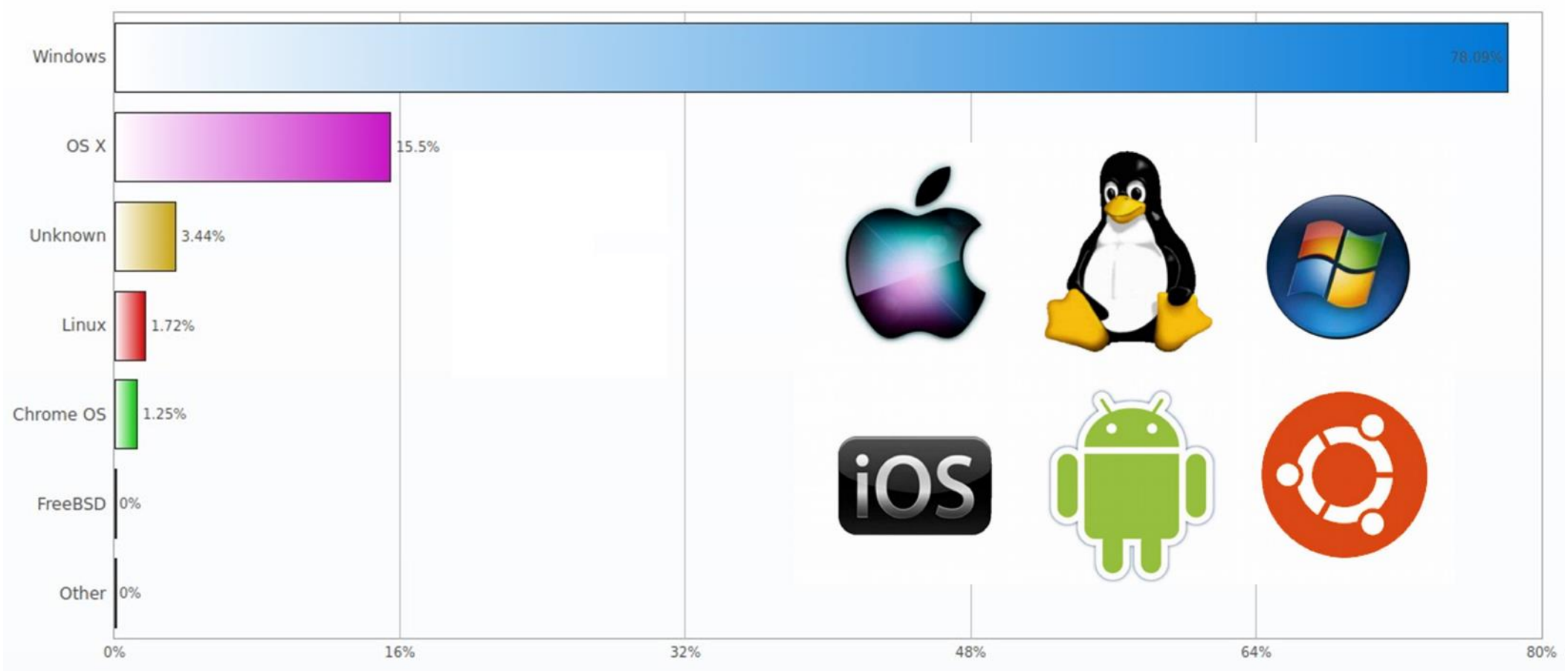
- En la categoría de software con licencia comercial se tiene:
  - FTK.
  - ProDiscover.
  - EnCase.
- en Open Source se tiene:
  - Autopsy.
  - Digital Forensics Framework.
  - Caine Linux.

- * 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

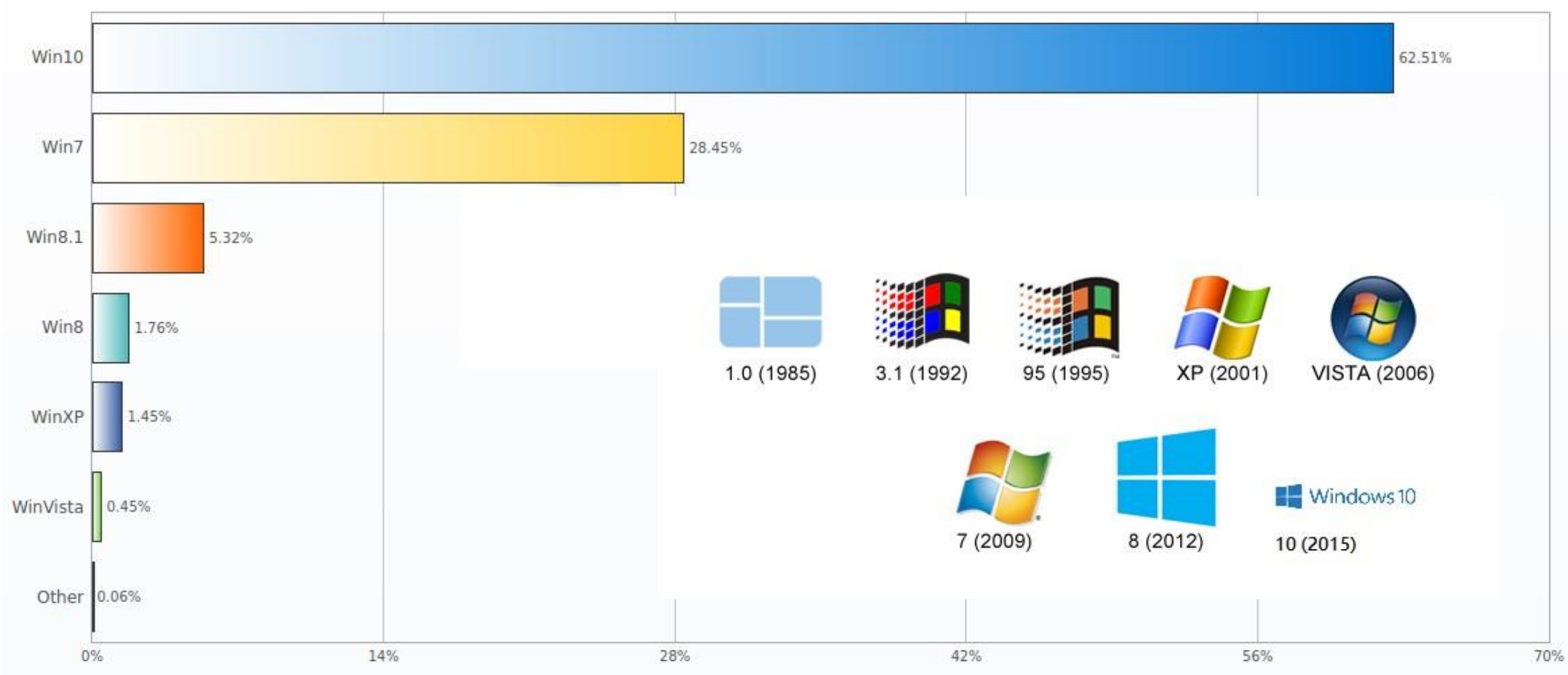
Hardware Forense

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

¿Cuanto se utiliza Windows?



Mercado de Versiones de Windows (abril 2019 - 2020)



¿Qué es SIFT Workstation?

SIFT Workstation: https://digital-forensics.sans.org/community/downloads *

- 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, l as cuales está disponibles libremente y se actualizan frecuentemente.

URLS test

- tipos de malware para descarga con fines de análisis forense
- https://www.hybrid-analysis.com/

Herramientas

- https://geekflare.com/es/forensic-investigation-tools/

Recuperar archivos borrados

- https://noticiasseguridad.com/importantes/21-mejores-herramientas-de-informatica-forense-gratuitas/
- https://www.cleverfiles.com/howto/es/top-5-data-recovery-software-windows.html
- https://www.cleverfiles.com/howto/es/recover-deleted-files-windows10.html

Frameworks seguridad

- https://attack.mitre.org/

Términos

- https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=57.html

Ejemplos de Análisis en un Sistema Windows

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.

- Logs o ficheros de sistema
- Tabla maestra de archivos MFT
- El registro de Windows
- El visor de Eventos
- Los ficheros Prefetch
- Los accesos directos
- La papelera
- Metadatos en imágenes y documentos
- Ficheros de hibernación y memoria
- Copias de seguridad
- Volume Shadow

ARTEFACTOS DE SISTEMA

REGISTROS VARIOS SOBRE LA INSTALACIÓN	
%WINDIR%\setupact.log	Contiene información acerca de las acciones de instalación durante la misma. EVIDENCIAS: Podemos ver fechas de instalación, propiedades de programas instalados, rutas de acceso, copias legales, discos de instalación...

%WINDIR%\setuperr.log	**Contiene información acerca de los errores de instalación durante la misma.** **EVIDENCIAS: Fallos de programas, rutas de red inaccesibles, rutas a volcados de memoria...**
%WINDIR%\WindowsUpdate.log	Registra toda la información de transacción sobre la actualización del sistema y aplicaciones. EVIDENCIAS: Tipos de hotfix instalados, fechas de instalación, elementos por actualizar...

%WINDIR%\Debug\mrt.log	**Resultados del programa de eliminación de software malintencionado de Windows.** **EVIDENCIAS: Fechas, Versión del motor, firmas y resumen de actividad.**
%WINDIR%\security\logs\scecomp.old	Componentes de Windows que no han podido ser instalados. EVIDENCIAS: DLL's no registradas, fechas, intentos de escritura,rutas de acceso...
%WINDIR%\SoftwareDistribution\ReportingEvents.log	Contiene eventos relacionados con la actualización. EVIDENCIAS: Agentes de instalación, descargas incompletas o finalizadas, fechas, tipos de paquetes, rutas...

%WINDIR%\Logs\CBS\CBS.log	Ficheros pertenecientes a 'Windows Resource Protection' y que no se han podido restaurar. EVIDENCIAS: Proveedor de almacenamiento, PID de procesos, fechas, rutas...
%AppData%\Local\Microsoft\Websetup (Windows 8)	Contiene detalles de la fase de instalación web de Windows 8 EVIDENCIAS: URLs de acceso, fases de instalación, fechas de creación, paquetes de programas...

%AppData%\setupapi.log	**Contiene información de unidades, services pack y hotfixes.** **EVIDENCIAS: Unidades locales y extraibles, programas de instalación, programas instalados, actualizaciones de seguridad, reconocimiento de dispositivos conectados...**
%SYSTEMROOT%\$Windows.~BT\Sources\Panther*.log,xml **%WINDIR%\PANTHER*.log,xml**	Contiene información de acciones, errores y estructuras de SID cuando se actualiza desde una versión anterior de windows. EVIDENCIAS: Fechas, rutas, errores , medio de instalación, dispositivos, versiones, reinicio, dispositivos PnP...

%WINDIR%\INF\setupapi.dev.log	**Contiene información de unidades Plug and Play y la instalación de drivers.** **EVIDENCIAS: Versión de SO, Kernel, Service Pack, arquitectura, modo de inicio, fechas, rutas, lista de drivers, dispositivos conectados, dispositivos iniciados o parados...**
%WINDIR%\INF\setupapi.app.log	Contiene información del registro de instalación de las aplicaciones. EVIDENCIAS: Fechas, rutas, sistema operativo, versiones, ficheros, firma digital, dispositivos...

%WINDIR%\Performance\Winsat\winsat.log	Contiene trazas de utilización de la aplicación WINSAT que miden el rendimiento del sistema. EVIDENCIA: Fechas, valores sobre la tarjeta gráfica, CPU, velocidades, puertos USB...

EL.CFG Pid.txt	Estos archivos se usan para automatizar la página de entrada de la clave de producto en el programa de instalación de Windows. EVIDENCIA:Contiene el código de producto y la versión instalada

LOG DE EVENTOS DE WINDOWS	
%WINDIR%\System32\config %WINDIR%\System32\winevt\Logs	Contiene los logs de Windows accesibles desde el visor de eventos. EVIDENCIAS: Casi todas. Entradas, fechas, accesos, permisos, programas, usuario, etc...

MICROSOFT SECURITY ESSENTIALS	
Logs del motor de antimalware **EVIDENCIAS: Fechas, versión del motor, programas analizados, actividad del malware...**	%PROGRAMDATA%\Microsoft\Microsoft Antimalware\Support %PROGRAMDATA%\Microsoft\Microsoft Security Client\Support

ARTEFACTOS LINUX:

- **/etc**
  Equivalente a %SystemRoot%\System32\config
  Directorio principal de configuración del sistema
  Archivos y directorios de configuración independientes para cada aplicación
  /var/log
  Equivalente al Registro de Eventos de Windows
  Registros de seguridad, aplicación, etc.
  Los registros se guardan durante 4-5 semanas
  /home/$USER
  Equivalente a %USERPROFILE%
  Los datos y la información de configuración del usuario

Fichero Información

- /etc/*-release Nombre de la distribución Linux y su versión
  /etc/hostname Nombre del ordenador(también se puede encontrar en losficheros de/var/log)
  /etc/host Dirección IP (asignación estática)
  /var/lib/dhclient
  /var/log/* Dirección IP (DHCP)
  /etc/localtime
  Almacena datos de la zona horario por defecto
  - Ficheros binarios, hay que usar zdump
  - Buscar en /usr/share/zoneinfo
-
  /etc/passwd Información básica de los usuarios.
  Las cuentas con UID=0 tienen permisos de 'root'
  /etc/shadow Hash MD5 de las contraseñas
  (se puede usar John the Ripper)

- /etc/sudoers Puede indicar los usuarios con permiso root
  /etc/group Pertenencia a grupos
  /var/log/wtmp
  Muestra información acerca del usuario, su origen, la hora y durada de una sesión.
  Hay que usar el comando last para verlo
  /var/log/btmp
  /var/log/faillog
  Información sobre los intentos fallados de acceso
  (last -f /var/log/btmp | more)
  /var/log/auth.log
  /var/log/secure
  Información de autorización del sistema, incluido los inicios de sesión de los usuarios, los que no han tenido éxito y el mecanismo de autentificación que se utiliza

- /var/log/daemon.log Mantiene información sobre los servicios en ejecución en background
- /home/<user> La localización más común para las carpetas y ficheros de los usuarios
  /root El directorio del usuario root
  /home/.*
  Los ficheros y directorios "ocultos" empiezan por un punto
  • Contienen información de configuración específica de las aplicaciones
  • En algunos casos se ejecutan al iniciar sesión
  • Es un posible backdoor o mecanismo de persistencia

- Los comandos ejecutadas por el usuario se guardan en $HOME/.bash_history
  Desafortunadamente, es un archivo sin marcas de tiempo
  Puede ser modificado o borrado por el propio usuario
  El histórico de comandos sudo se puede encontrar mirando los archivos
  /var/log/auth.log
  /var/log/sudo.log

NAVEGADORES:

- Los formatos de los ficheros son idénticos que en Windows
  Base de datos en SQLite
  Los ficheros suelen estar en los directorios de los usuarios
  Firefox: $HOME/.mozilla/firefox/*.default
  Chrome: $HOME/.config/chromium/Default