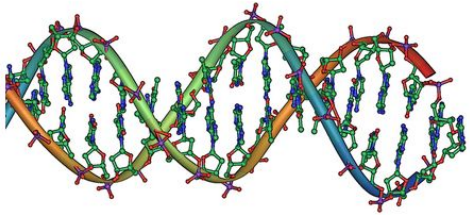
Análisis Forense I
Comandos, Versionamiento y Recuperación de Datos

CC5325 - Taller de Hacking Competitivo

Imágenes de dominio público en Wikimedia Commons

Ciencia forense

Aplicación de método científico para recopilar evidencia en casos criminales.



Íconos por Freepik en https://flaticon.com

¿Y en CTFs?

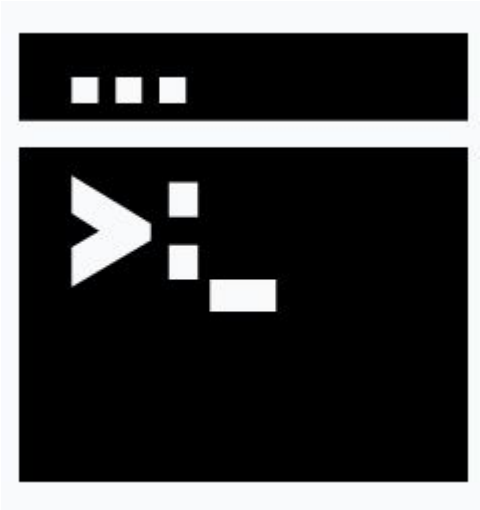
El término se usa en general para técnicas de recuperación de información en categorías como las siguientes:

- Recuperación de archivos o dispositivos borrados o dañados.
- Análisis de logs de redes o equipos.

Ícono por Freepik en https://flaticon.com

Comandos Interesantes

- **find**: Encontrar un archivo en un árbol de carpetas
- **grep**: Encontrar contenido dentro de uno o maś archivos
- **awk**: Procesar documentos
- **sed**: Reemplazar texto en un archivo
- **tr**: Transponer texto en un archivo
- **sort**: Ordenar alfabéticamente las líneas de un archivo
- **uniq**: Eliminar líneas repetidas en un archivo ordenado



Íconos por Flaticon en https://flaticon.com

Archivos de Log y Configuración

Logs

- Detallan estado de servicios corriendo en el computador
- Generalmente en **/var/log**
- **Ubicación configurable**

Configuraciones

- Generalmente en **/etc/**
- Ubicación puede buscarse con **find**

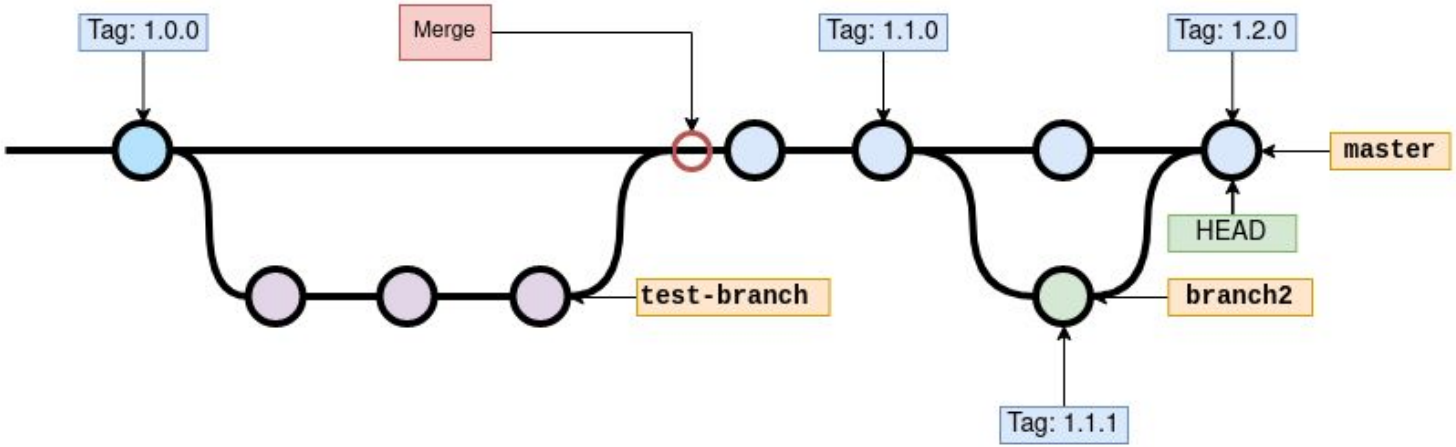
Versionamiento

- ¿Cómo llevar un historial de cambios en un proyecto de código? (VCS)
- A veces se registran más datos de los que se debiesen (como llaves secretas). **Si se borran, no desaparecen del historial del VCS.**

Logos de git, subversion y mercurial de los respectivos proyectos.

Git

VCS distribuido y de código abierto creado el 2005 por Linus Torvalds para manejar el código del kernel de Linux.



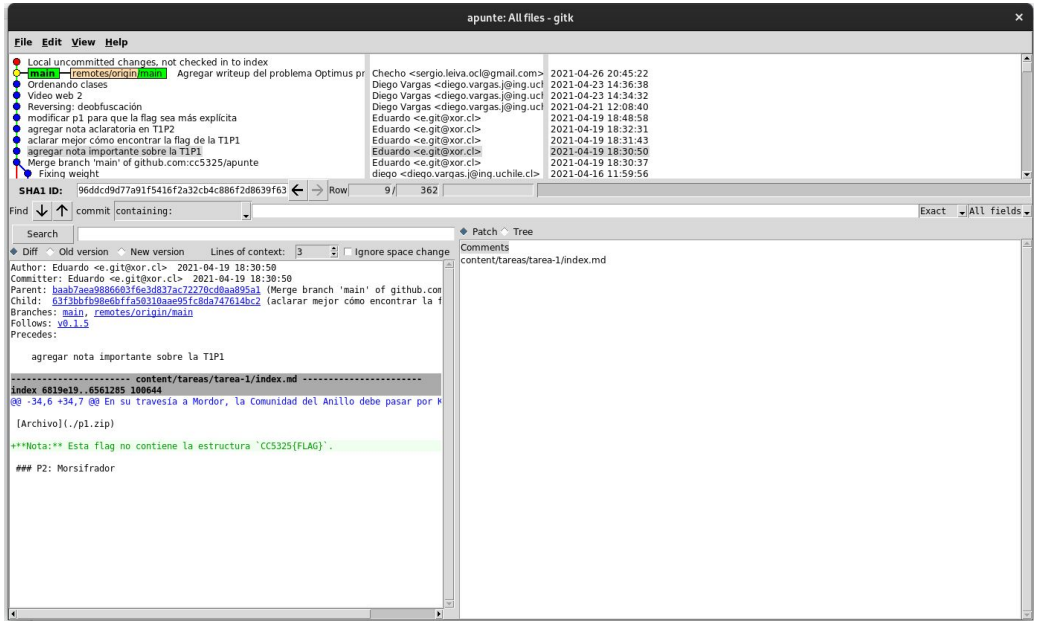
Comandos y Herramientas Útiles

Comandos:

- **git log:** Ver historial de cambios
- **git checkout HEAD^:** Cambiar a commit anterior

Herramientas

- **gitk**: Cliente gráfico de Git



Ícono por Flaticon en https://flaticon.com

Recuperación de Datos

Archivos Dañados:

- Depende el tipo de archivo y de daño, puede ser recuperado de forma parcial o total
- ¿Daño de headers? A veces son regenerables o copiables de otro archivo similar.
- ¿Daño de contenido? Revisar si el formato tiene corrección de errores o si existe un respaldo temporal creado por el programa que lo abrió.

¿Herramienta?

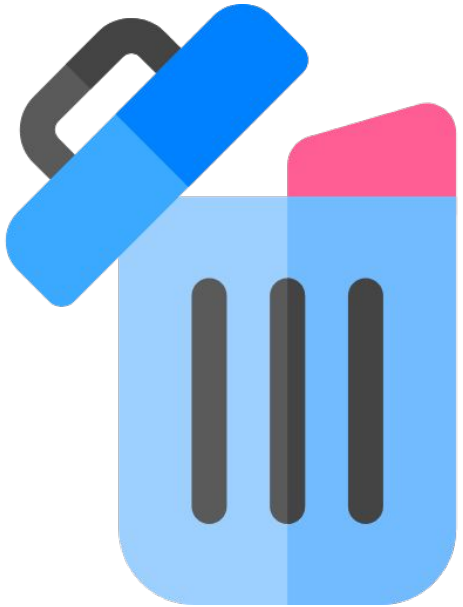
Depende

Ícono por Flaticon en https://flaticon.com

Recuperación de Datos

Archivos Eliminados:

- Archivos no son eliminados realmente de un sistema de archivos, en general **solo se elimina su entrada en el índice del sist. de archivos.**
- Escaneo completo al espacio de almacenamiento del dispositivo podría permitir encontrar el archivo, **siempre y cuando otro archivo no haya reclamado ya ese espacio.**



¿Herramienta?

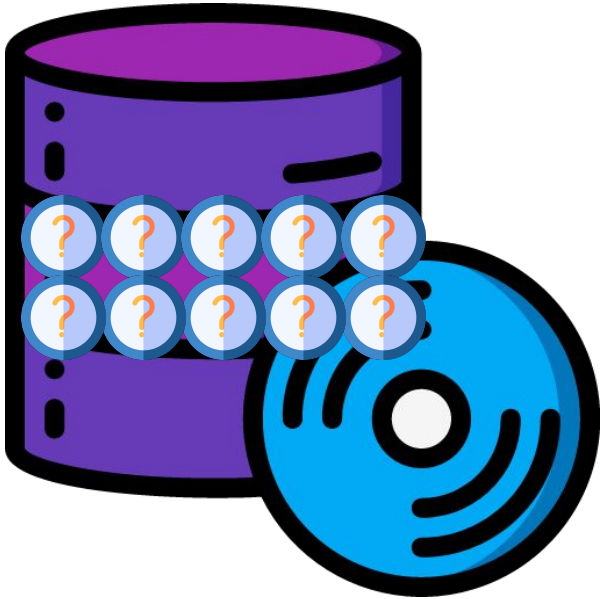
TestDisk

Ícono por smashicons en https://flaticon.com

Recuperación de Datos

Problemas en sistema de archivos

- **Herramientas permiten regenerar partes importantes del sistema de archivos** o copiar los sectores válidos del disco.
- **Se recomienda respaldar disco antes de intentar recuperarlo**, por si el proceso de recuperación afecta a los datos almacenados.



¿Herramientas?

fsck
ddrescue

Ícono por smashicons en https://flaticon.com

Otros tipos de recuperación de información

- **Dumps de RAM del estado de una máquina virtual.**
- **Se requiere analizar los procesos abiertos con herramientas especiales, y buscar en la memoria de uno la flag**
- **Herramienta: Volatility**