

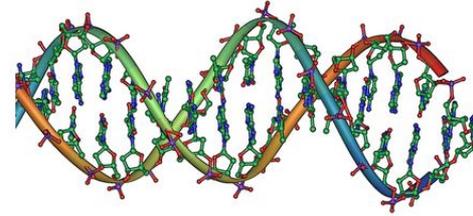
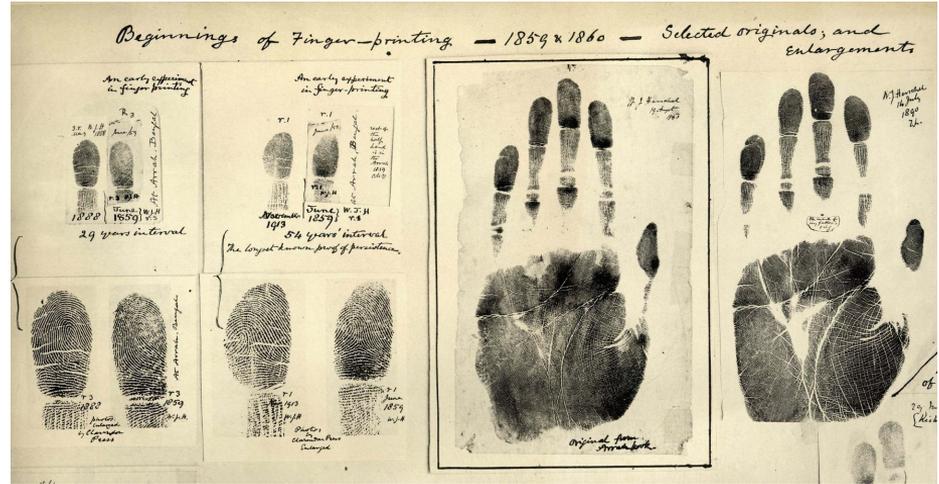
Análisis Forense I

Comandos, Versionamiento y Recuperación de Datos

CC5325 - Taller de Hacking Competitivo

Ciencia forense

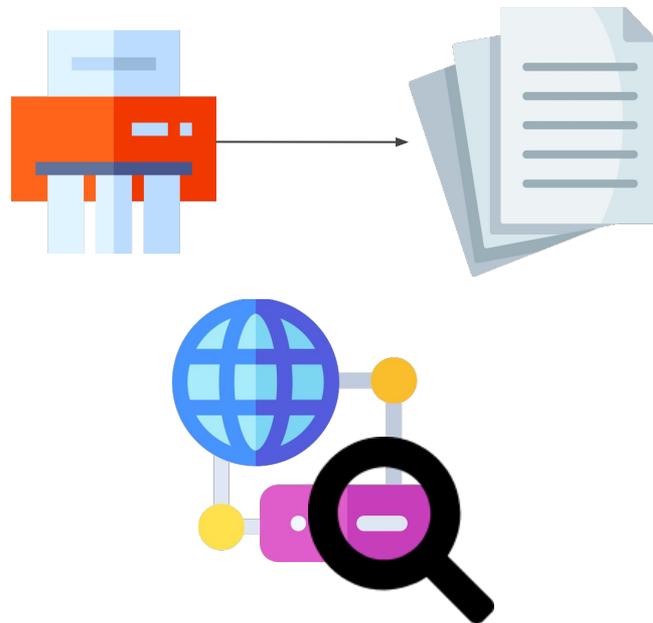
Aplicación de método científico para recopilar evidencia en casos criminales.



¿Y en CTFs?

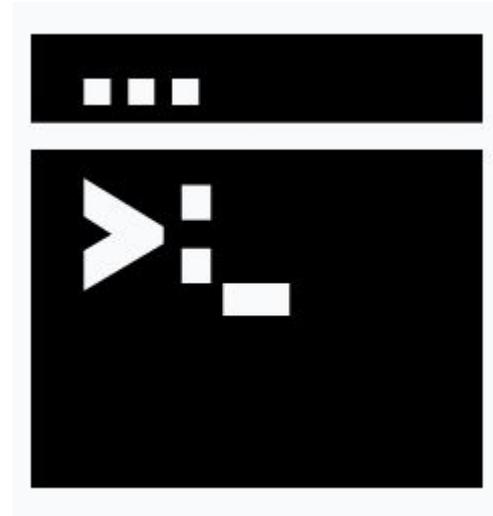
El término se usa en general para técnicas de recuperación de información en categorías como las siguientes:

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



Comandos Interesantes

- **find**: Encontrar un archivo en un árbol de carpetas
- **grep**: Encontrar contenido dentro de uno o más 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



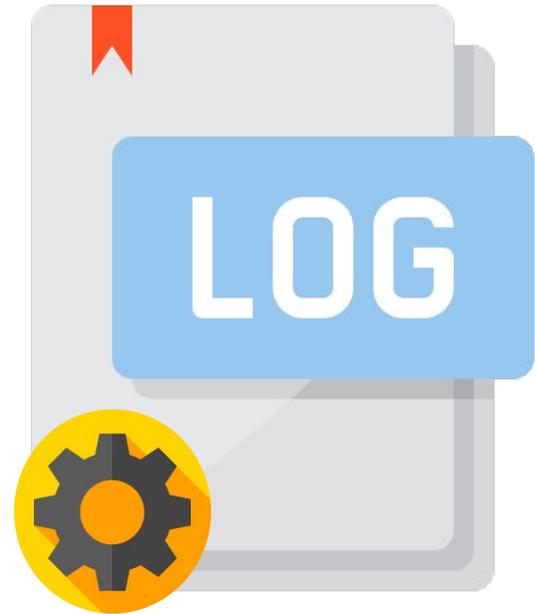
Archivos de Log y Configuración

Logs

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

Configuraciones

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



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

Versionamiento

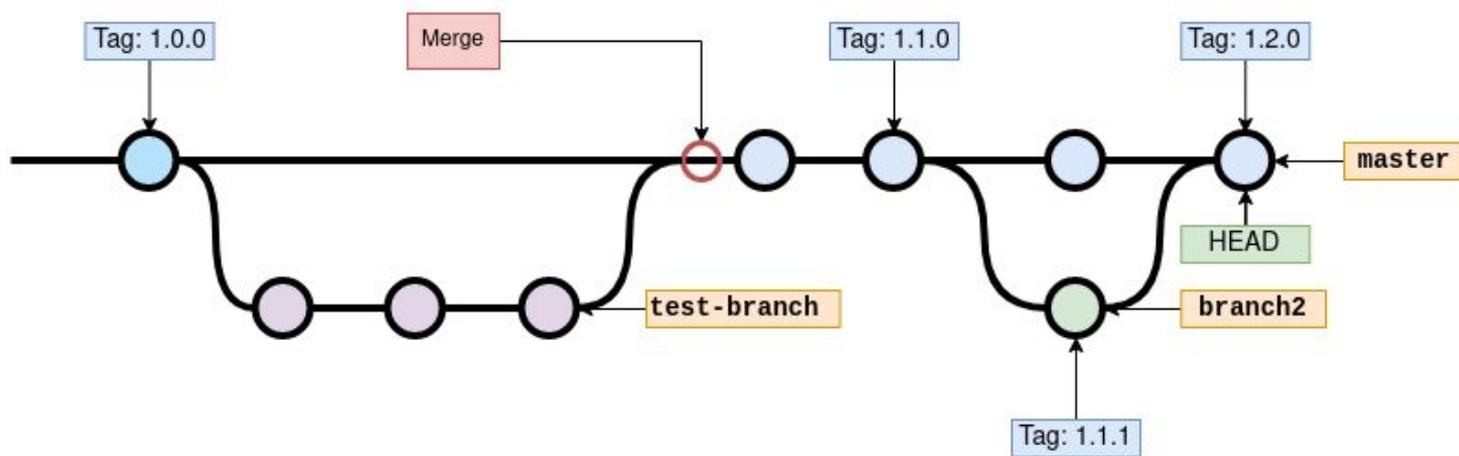
- ¿Cómo llevar un historial de cambios en un proyecto de código? (VCS)
- A veces se registran más datos de los que se debiesen (como llaves secretas). **Si se borran, no desaparecen del historial del VCS.**



Git



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



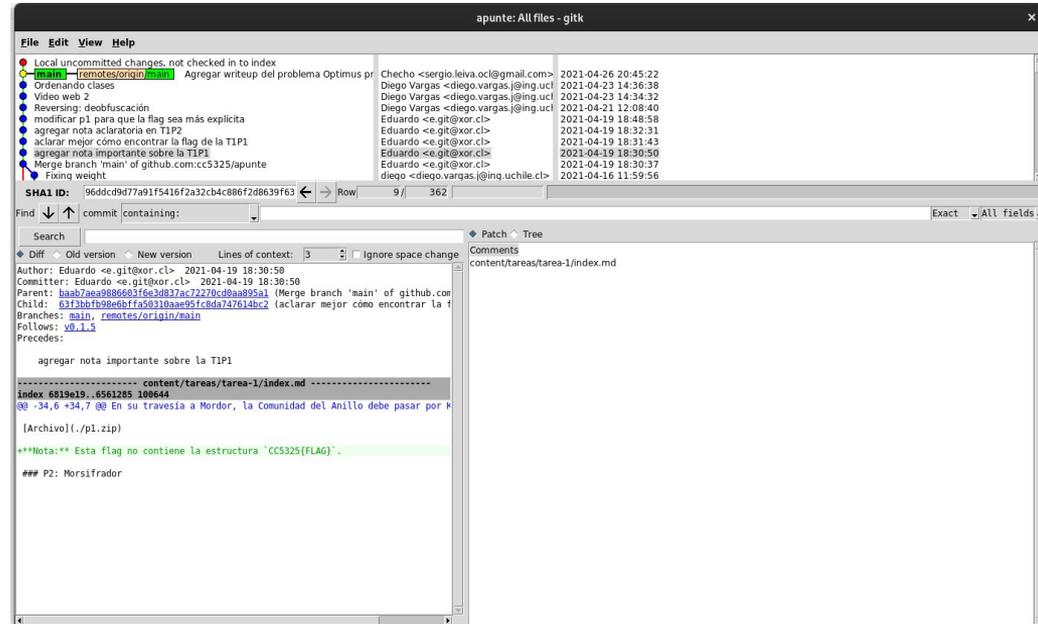
Comandos y Herramientas Útiles

Comandos:

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

Herramientas

- **gitk:** Cliente gráfico de Git



The screenshot shows the gitk graphical interface. At the top, there's a menu bar with 'File', 'Edit', 'View', and 'Help'. Below it, a commit history table is visible with columns for commit type, commit message, author, and date. The current commit is highlighted in green. Below the table, the 'SHA1 ID' and 'commit containing:' fields are shown. The main area displays a diff view for the file 'content/tareas/tarea-1/index.md'. The diff shows the current version (index 6819e19) and the previous version (index 4561285). The diff content includes a note about a flag structure and a reference to a Morsifrador.

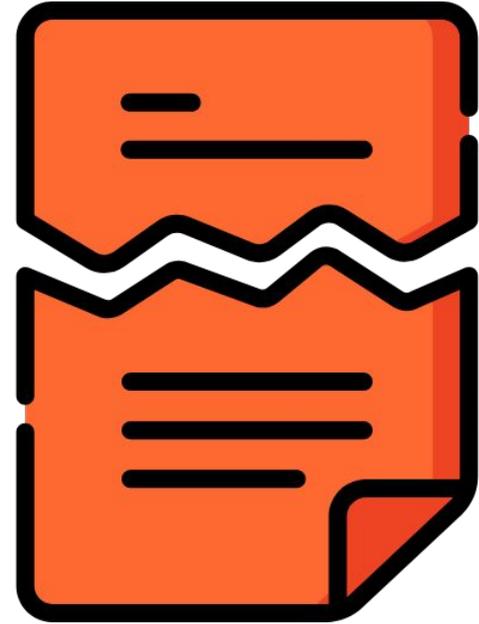
```
Local uncommitted changes, not checked in to index
- main - remotes/origin/main  Agregar writeup del problema Optimus p... Checho <sergio.leiva.oc@gmail.com> 2021-04-26 20:45:22
+ Ordenando clases Diego Vargas <diego.vargas.j@ing.uc... 2021-04-23 14:36:38
+ Video web 2 Diego Vargas <diego.vargas.j@ing.uc... 2021-04-23 14:34:32
+ Reversing: deobfuscación Diego Vargas <diego.vargas.j@ing.uc... 2021-04-21 12:08:40
+ modificar p1 para que la flag sea más explícita Eduardo <e.git@xor.cl> 2021-04-19 18:48:58
+ agregar nota aclaratoria en T1P2 Eduardo <e.git@xor.cl> 2021-04-19 18:32:31
+ aclarar mejor cómo encontrar la flag de la T1P1 Eduardo <e.git@xor.cl> 2021-04-19 18:31:43
+ agregar nota importante sobre la T1P1 Eduardo <e.git@xor.cl> 2021-04-19 18:30:50
+ Merge branch 'main' of github.com:cc5325/apunte Eduardo <e.git@xor.cl> 2021-04-19 18:30:37
+ Fixing weight diego <diego.vargas.j@ing.uchile.cl> 2021-04-16 11:59:56

SHA1 ID: 96ddcd9d77a91f5416f2a32cb4c886f2d8639f63 Row: 9 / 362
Find commit containing:
Search
Diff Old version New version Lines of context: 3 Ignore space change
Author: Eduardo <e.git@xor.cl> 2021-04-19 18:30:50
Committer: Eduardo <e.git@xor.cl> 2021-04-19 18:30:50
Parent: baab7aea9886603f6e3d837ac72270c0baa895a1 (Merge branch 'main' of github.com)
Child: 63f3bbfb98e6b7fa58310aae95f8da747614bc2 (aclarar mejor cómo encontrar la f
Follows: v0.1.5
Precedes:
+ agregar nota importante sobre la T1P1
----- content/tareas/tarea-1/index.md -----
index 6819e19..4561285 100644
@@ -34,6 +34,7 @@ En su travesía a Mordor, la Comunidad del Anillo debe pasar por K
[Archivo](./p1.zip)
+***Nota:** Esta flag no contiene la estructura 'CC5325(FLAG)'.
+## P2: Morsifrador
```

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

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.**



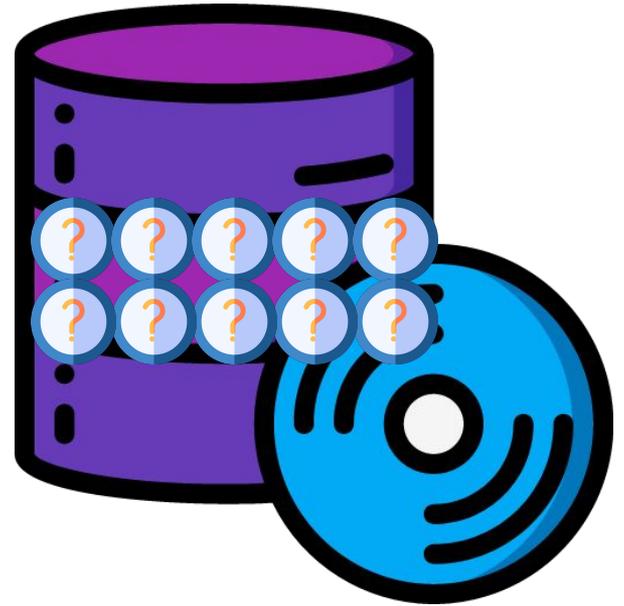
¿Herramienta?

TestDisk

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

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

