**Informe de forensia digital**

**Grupo** viernes

**Objetivo:**

* encontrar todos los datos ya sea imágenes, videos, audio, textos, archivos eliminados etc. Con el fin de detectar el rastro creado en nuestra imagen forense.

**Alcance:**

corresponde con un conjunto de técnicas destinadas a extraer información valiosa de discos, sin alterar el estado de los mismos. Esto permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información.

**Metodología:**

Se utilizo las siguientes herramientas gratuitas en el ámbito de forensia digital:

* AccesDataFTK
* MultiHashers
* Autopsy
* WinHex

**Procedimiento:**

**Primero** realizamos una imagen forense con la herramienta AccesDataFTK, procurando mantener la original integra y sin alterar su contenido.

**Segundo** luego de realizar la imagen procedemos a verificar los hashes MD5 y SHA-1 con la herramienta MultiHashers para comprobar que el original no a sido manipulado de ninguna manera y luego trabajaremos con la imagen. También usamos WinHex para verificar los datos hexadecimales.

**Tercero** utilizamos la herramienta Autopsy para visualizar los datos, archivos borrados entre otras para dar con hallazgos digitales. Buscamos detenidamente siempre documentando lo que se ve, se hace y encuentra.

**Hallazgos:**

7 imagens, 1 office, 124 plain text, 1 msword, 2 gif, 132 archivos borrados. Algunos datos tienen informacion sobre Ella un gif se vio sospechoso.

**Conclusiones:**

Podemos entender que aunque tomemos algo sutilmente digital siempre habrá un rastro en el que podremos descubrir al ladrón y ver que se filtró. Con unas buenas herramientas y el conocimiento adecuado poner un orden.