Profesor

Constantino Malagón

Seguridad Informática

Herramientas para el análisis de Imágenes forenses

Universidad Francisco de Vitoria UFV Madrid

Grado en Ingeniería Informática
Escuela Politécnica Superior

Análisis de imágenes forenses

Universidad Francisco de Vitoria UFV Madrid

- Ya hemos visto cómo realizar una imagen de un disco o de una partición mediante varias herramientas (ver práctica 1):
  - Linux: dc3dd, dfcldd y dd en Linux
  - Windows: FTK Imager
- Y bajo qué condiciones se han de hacer para que puedan ser utilizadas como prueba:
  - Partición montada como solo lectura
  - Comprobación de los hashes
- Ahora vamos a ver cómo analizarlas

Sleuth kit

- Sleuth kit
- Colección de aplicaciones para análisis forense
- De estas la más importante es Autopsy
- Open source y gratuito
- Permite:
  - Analizar imágenes de discos
  - Recuperar archivos eliminados de un disco (*file carving*)

Autopsy

- Autopsy es una aplicación que nos va a servir para analizar en un proceso de investigación las imágenes obtenidas en la fase anterior
- Aplicación gratuita
- Instalado por defecto en Kali
- Partiríamos de una imagen ya obtenida mediante dc3dd o FTK Imager por ejemplo (práctica 1)

Analizar emails y el navegador

Universidad Francisco de Vitoria UFV Madrid

- Aunque está en Kali esta vez vamos a usar Autopsy en Windows
- Y en vez de usar nuestras imágenes hechas previamente nos bajaremos imágenes publicadas para poder testearlas y aprender cómo se realiza un análisis forense
- https://digitalcorpora.org/corpora/disk-images - *NPS Test Disk Images are a set of disk images that have been created for testing computer forensic tools*

Universidad Francisco de Vitoria UFV Madrid

Analizar evidencias: emails y actividad del navegador

Analizar emails y el navegador

Universidad Francisco de Vitoria UFV Madrid

- Tenemos una imagen del equipo de un yihadista y queremos saber qué ha estado visitando en Internet.
- Sabemos que ha visitado páginas del gobierno de Estados Unidos y han estado realizando fotos para preparar un atentado

Analizar emails y el navegador

Universidad Francisco de Vitoria UFV Madrid

- Vamos a https://digitalcorpora.org/corpora/disk-images
- Imagen: nps-2009-casper-rw — *An ext3 file system from a bootable USB token that had an installation of Ubuntu 8.10. The operating system was used to browse several US Government websites*
- Ver narrative.txt

Analizar emails y el navegador

Universidad Francisco de Vitoria UFV Madrid

- Descargamos en Windows la imagen que se llama ubnisnt1.casper-rw.gen2.raw
- Lo abro en Autopsy
- Comprobar que el hash es el mismo. Lo veo en el fichero anterior, narrative.txt, y lo comparo con el que se ve en las propiedades de la imagen en Autopsy
- Vamos a Data sources/Imagen ->botón derecho -> View summary information

Analizar emails y el navegador

Universidad Francisco de Vitoria UFV Madrid

- Vamos a Results
- Empezamos por Extracted Content
- Ahí veremos la información extraída por Autopsy de la imagen que hemos cargadom, resumida por tipo de información
  - Historial web
  - Búsquedas webs realizadas
  - Documentos recientemente descargados
  - Cookies

Analizar emails y el navegador

Universidad Francisco de Vitoria UFV Madrid

- Y EXIF Parser
- The EXIF Parser module extracts EXIF (Exchangeable Image File Format) information from ingested pictures. This information can contain geolocation data for the picture, time, date, camera model and settings (exposure values, resolution, etc) and other information (https://sleuthkit.org/autopsy/docs/user-docs/3.1/_e_x_i_f_parser_page.html)

Analizar emails y el navegador

Universidad Francisco de Vitoria UFV Madrid

- Podemos ver las fotos que tenía almacenadas en el disco, y cuándo las hizo
- Podemos ver los correos electrónicos guardados en local → Email messages (aquí no hay muchos)
- Y buscar por palabras en todos los ficheros (Keyword search)

Autopsy

Universidad Francisco de Vitoria UFV Madrid

- Podemos ver las fotos en Timeline.
- Nos dan los datos y ficheros creados pero agrupados por meses (clave en una investigación)
- En el árbol, Views/File types, podemos ver los archivos agrupados por tipos
- Podemos ver también Deleted Files, en Views/deleted files, donde podemos ver los ficheros que han sido borrados