Práctica 1. Análisis forense en la nube.

Extracción de evidencias de la nube.

Se puede acceder a los servicios que ofrece la nube a través de navegadores o aplicaciones cliente en dispositivos en red, como computadoras de escritorio, portátiles, tabletas y teléfonos inteligentes, que generalmente se conocen como dispositivos finales (endpoint devices).

Los datos relevantes para las investigaciones forenses pueden almacenarse en dispositivos finales y/o en proveedores de servicios en la nube. Cuando a los servicios en la nube se accede desde un dispositivo final, se crean varios archivos y carpetas en el dispositivo que son de interés desde el punto de vista forense. Además, un investigador forense digital puede acceder a los datos utilizando una interfaz de programación de aplicaciones (API) puesta a disposición por un proveedor de servicios en la nube para obtener información forense de la nube relacionada con objetos, eventos y archivos metadatos asociados con un usuario de la nube.

Objetivos:

- Tomar conciencia de las posibilidades que nos ofrece la nube a la hora de obtener evidencias forenses.
- Instalar, configurar, extraer evidencias y analizar los sistemas en la nube más utilizados.

Materiales

- Cualquier distribución Windows con la que cuentes en tu sistema informático.
- Clientes onedrive, google drive y dropbox.

Se pide:

1) Lee el documento “A Taxonomy of Cloud Endpoint Forensic Tools” y contesta a las siguientes preguntas:

    a) ¿Qué es el análisis forense de la nube?

    b) ¿Cuales son las fuentes de evidencias digitales que nos encontramos específicamente cuando trabajamos en la nube?
    c) ¿Qué posibilidades nos ofrece explotar las API que nos ofrecen los proveedores de servicios en la nube? Explica los metadatos que se pueden obtener haciendo uso de las API.
    d) Enumera el software cliente más utilizado a la hora de acceder a servicios en la nube (ver tablas 1,2 y 3)

2) Instala y configura los clientes OneDrive, Google Drive y Dropbox.

3) Analiza los clientes anteriores y determina:
    a) Identifica donde se instala los servicios y su configuración
    b) Localiza dónde se sitúan las carpetas que se sincroniza en la nube
    c) Encuentra los metadatos generan y qué información podemos extraer de ellos.