# PRÁCTICA 1: La volatilidad en Windows

Como bien sabemos, hay dos tipos de análisis forense: en vivo y post mortem.

El primero ocurre cuando el sistema todavía está activo durante el análisis. En este escenario, es posible adquirir datos volátiles, como RAM, procesos en ejecución, conexiones a Internet y archivos temporales. Si se utiliza el cifrado de disco, con este análisis, el sistema de archivos se puede descifrar con la clave en caché. Por otro lado, este tipo de análisis requiere más experiencia y el sistema modifica constantemente sus datos, lo que puede perjudicar la admisibilidad judicial.

El analista tampoco debe confiar en ninguna herramienta proporcionada en el sistema, dado que puede haberse manipulado deliberadamente.

## APARTADO A)

**Objetivo:**

- Elaborar una herramienta forense, compuesta por comandos ejecutables de extracción de evidencias y un fichero de procesamiento por lotes para lanzar los anteriores, desde donde obtener las evidencias más interesantes que se estudiaron en clase.

**Materiales**

- Sysinternals suite
- Nirsoft
- ntsecurity.nu
- Comandos de microsoft
- Otro software que tu consideres oportuno

La idea es confeccionar un USB-STICK donde estén almacenadas las herramientas y un fichero de procesamiento por lotes. El fichero BATCH se lanzará en la máquina que se pretenda peritar. Este BAT realizará funciones como copiar registros a la unidad USB externa y recopilar información como fecha, hora, usuarios registrados, árbol de procesos, tiempo de actividad del sistema, etc.

## APARTADO B)

**Objetivo:**

- Preparar y utilizar la herramienta de triage gráfica Wintriage para la adquisición rápida y estructurada de evidencias forenses en sistemas Windows, permitiendo la recolección de información relevante de forma controlada durante un análisis forense en vivo.

Wintriage es una herramienta forense gráfica diseñada para facilitar la recopilación inicial de evidencias en sistemas Windows comprometidos. Su enfoque principal es el triage forense, es decir, la obtención rápida de información clave que permita al analista evaluar el estado del sistema y decidir los pasos posteriores de la investigación.

Para su utilización, la herramienta debe ejecutarse preferiblemente desde un medio externo (por ejemplo, un USB forense), minimizando así la alteración del sistema analizado y evitando el uso de herramientas locales que pudieran haber sido manipuladas. Wintriage permite seleccionar de manera sencilla los artefactos a recolectar y almacenar los resultados en un directorio previamente definido.

Prepara la herramienta, aprende a configurarla y haz una prueba de obtención de evidencias digitales en caliente.

## APARTADO C)

Nos han proporcionado una captura de RAM a la que tenemos que realizar un análisis forense completo.

Objetivos principales de la práctica:

- **Analizar memoria RAM**
- **Instalar y aprender a utilizar la herramienta VOLATILITY**

Detalla (comando empleado y captura de pantalla de la salida del mismo) el proceso para obtener esta información.

Se nos pide obtener información de:

- Perfil del sistema operativo
- Listado de procesos
- Historial de comandos
- Información detallada del sistema operativo
- Ficheros cargados en memoria
- Conexiones activas