PRÁCTICA 3: ADQUISICIÓN DE EVIDENCIAS EN CALIENTE.

Análisis en caliente es el análisis que se lleva a cabo de un sistema que se presume ha sufrido un incidente o está sufriendo un incidente de seguridad. En este caso, se suele emplear un CD/DVD/flash drive con las herramientas de Respuesta ante Incidentes y Análisis Forense compiladas de forma que no realicen modificaciones en el sistema. Una vez hecho este análisis en caliente, y confirmado el incidente, se realiza el análisis post-mortem.

Supongamos que un cliente está trabajando en una estación de trabajo y se ve envuelto en un incidente de seguridad. Para realizar la adquisición de las evidencias digitales en caliente, usaremos herramientas como:

1) OSF (windows)

2) FTK imager (windows)

3) Belkasoft RAM capturer (windows)

4) Microsoft AVML (linux)

Objetivos principales de la práctica:

- **Recopilación de pruebas en caliente causando el mínimo impacto en el sistema informático.-**

Se pide:

- Crear dos máquinas virtuales donde instalar un sistema operativo Windows (XP,7,10) y linux (la distribución que prefieras)
- ¿Dónde puedo obtener las herramientas citadas anteriormente?.
    - Ten en cuenta que cumpla con los requisitos del sistema (windows/linux 32/64 bits)
- Realizar una extracción de las evidencias digitales volátiles (RAM) y documentar el proceso.
    - Ten en cuenta que deberás añadir un VDI (disco duro virtual) extra a las máquinas virtuales que hará las veces de flash drive y/o disco duro externo.
    - Calcula los HASH de las evidencias extraídas (comando sha512sum)
- Por último, justifica cuál de las herramientas piensas que es más adecuada desde el punto de vista de mínimo impacto en el sistema informático.