**🧪 Experiment 4: Analyzing Volatile Memory to Detect Evidence of Attack**

**✅ Step-by-Step Procedure (As Per PDF)**

**🔹 Step 1: Create a Memory Dump of the System**

You need a Windows memory dump (.raw, .mem, or .dmp) to analyze.

📌 **Tool:** Use **DumpIt** or **WinPMEM** on a Windows machine to generate the memory image.

You will get something like:

CopyEdit

WINMEMORY.raw

Transfer this file to your Kali Linux system for analysis.

**🔹 Step 2: Install Volatility**

If not installed, run:

bash

CopyEdit

sudo apt update

sudo apt install volatility -y

Or download it manually:

bash

CopyEdit

git clone https://github.com/volatilityfoundation/volatility.git

**🔹 Step 3: Open Terminal**

bash

CopyEdit

# Open terminal (Ctrl + Alt + T)

**🔹 Step 4: Go to the Directory Where Volatility is Located**

bash

CopyEdit

cd volatility

Or wherever you copied the volatility-master directory (e.g., cd ~/Downloads/volatility-master).

**🔹 Step 5: Use Volatility with the Memory Dump**

The base format is:

bash

CopyEdit

python vol.py <plugin> -f <dump\_file>

📌 Example Commands (from plugin list in PDF):

**🔸 Registry Analysis:**

bash

CopyEdit

python vol.py hivelist -f WINMEMORY.raw

python vol.py printkey -f WINMEMORY.raw --key="Software\\Microsoft\\Windows\\CurrentVersion\\Run"

python vol.py hashdump -f WINMEMORY.raw

**🔸 Process Analysis:**

bash

CopyEdit

python vol.py pslist -f WINMEMORY.raw

python vol.py pstree -f WINMEMORY.raw

python vol.py psscan -f WINMEMORY.raw

**🔸 Code Injection Detection:**

bash

CopyEdit

python vol.py malfind -f WINMEMORY.raw

**🔸 DLLs and Handles:**

bash

CopyEdit

python vol.py dlllist -f WINMEMORY.raw

python vol.py handles -f WINMEMORY.raw

**🔸 File Extraction:**

bash

CopyEdit

python vol.py dumpfiles -f WINMEMORY.raw --dump-dir=dump\_output/

**🔸 Rootkit Detection:**

bash

CopyEdit

python vol.py psxview -f WINMEMORY.raw

python vol.py ssdt -f WINMEMORY.raw

**🧾 Output:**

* Volatility will list processes, dumped files, DLLs, handles, registry entries, etc.
* Evidence like:
  + Suspicious processes
  + Injected code
  + Password hashes
  + Hidden drivers
  + Command-line history
  + Autorun malware