Workflow

1. Preparation

- Identify the system requiring evidence preservation (e.g., Windows VM).
- Ensure write-blocking and isolation from production network.
- Create an evidence folder structure:
- Start a Chain-of-Custody (CoC) document.

2. Volatile Data Collection (Velociraptor)

- Run Velociraptor client locally on the VM
- Artifact: Windows.Network.Netstat
- Query: SELECT * FROM netstat
- Save results as netstat.csv

3. Memory Dump Collection

- Artifact: Artifact.Windows.Memory.Acquisition
- Query: SELECT * FROM Artifact.Windows.Memory.Acquisition
- Run hash on the memory dump:
- Get-FileHash .\memory.raw -Algorithm SHA256
- Save it in hash.txt

4. Chain of Custody Documentation

- Log each action with date/time, signature (your name), and description.
- Ensure CoC is never modified without traceable entries.
- Include:
    - Who collected the evidence
    - How it was collected
    - Where it was stored
    - Transfer records