**🧪 Experiment 1: Hard Disk Analysis with Autopsy on Kali Linux**

**✅ Step-by-Step Process on Kali Linux**

**Step 1: Install Autopsy (if not installed)**

bash

CopyEdit

sudo apt update

sudo apt install autopsy sleuthkit -y

This installs both **Autopsy** and **The Sleuth Kit** (backend tools Autopsy uses).

**Step 2: Start Autopsy**

Launch the Autopsy forensic browser using:

bash

CopyEdit

autopsy

You will see an output similar to:

bash

CopyEdit

Opening Autopsy at http://localhost:9999/autopsy

Open your browser and go to <http://localhost:9999/autopsy>

**Step 3: Create a New Case**

1. Click on **“New Case”**
2. Fill in:
   * **Case Name** (e.g., case1)
   * **Base Directory** (e.g., /home/kali/Documents/AutopsyCases)
   * Click **Next**

**Step 4: Enter Case Details**

1. Fill in:
   * **Case Number** (optional)
   * **Examiner Name** (your name)
2. Click **Finish**

**Step 5: Add Host to Case**

You’ll be prompted to **Add a Host**:

* Either:
  + Select **Generate new host name**
  + OR Enter a **custom name**
* Click **Next**

**Step 6: Select Data Source Type**

Choose the data source:

* For example: Disk Image or VM File (for .dd, .img, .E01, etc.)

Click **Next**

**Step 7: Select Data Source File**

1. Browse and select your **disk image file** (e.g., suspect.img)
2. Click **Next**

**Step 8: Configure Ingest Modules**

* Tick the modules you want to use:
  + File Type Identification
  + Hash Lookup
  + Web Artifacts
  + EXIF Metadata
  + Deleted Files Recovery
  + etc.

Click **Next**

**Step 9: Add Data Source**

* Click **Finish**
* Autopsy will start processing and show extracted data:
  + Files
  + Email
  + Web history
  + Images
  + File system info
  + Hash matches, etc.

**🧾 Output**

* Browse the extracted data from the left panel.
* You can **export reports**, view timelines, analyze deleted files, and more.