LAB #1

In this lab, you will run a malware sample in a controlled environment and collect data about its behavior. The goal is to practice safe execution techniques and gather logs and artifacts.

01 **Download a malware sample (in the VM):**

- Go to GitHub
- Search for a macOS malware sample (e.g., XLoader, KeyStealer, etc.)
- Download the sample ZIP file to your VM

02 **Allow full disk access:**

- On your macOS VM, open: System Settings → Privacy & Security → Full Disk Access
- Enable access for Terminal

03 **Disable networking in the VM:**

- Shut down the VM
- In UTM, open the VM Settings → Network
- Remove the network interface (to prevent malware from connecting out)

04 **Run malware and collect logs:**

- Start the VM
- Unzip the malware file
- Open Terminal
- Navigate to the directory where you want to save your logs
- Start eslogger with the following command:

```
sudo eslogger exec create rename unlink tcc_modify open close write fork exit mount unmount signal
kextload kextunload cs_invalidated proc_check > events.json
```

- Run the malware
- Once the malware finishes, stop the logger (press Ctrl + C)

05

Transfer the data out safely:

Step 1: Add a Detachable Disk to the VM

- Shut down the VM
- In UTM, click Edit the VM → Add New Drive
- Choose a size (e.g., 1GB), click Create, and Save

Step 2: Format the Disk

- Start the VM again
- When prompted, click Ignore the new disk warning
- Open Disk Utility
- Select the new disk ("Apple Inc. …")
- Click Erase, use:
  - Name: sharing
  - Format: Mac OS Extended (Journaled)
  - Scheme: GUID Partition Map
- Click Erase

Step 3: Copy the File

- Move events.json onto the newly formatted disk

Step 4: Unmount and Sync

- In Disk Utility, right-click the disk and choose Unmount
- In Terminal, run: sync

Step 5: Mount the Disk on the Host

- Shut down the VM
- On your host machine, run:

```
ls Library/Containers/com.utmapp.UTM/Data/Documents/macOS\ -\ OFTW.utm/Data
```

- Identify the .img file
- Attach it with:

```
hdiutil attach Library/Containers/com.utmapp.UTM/Data/Documents/macOS\ -\ OFTW.utm/Data/<your-image>.img
```

- You should now see the disk mounted on your Mac, and your collected events.json file should be accessible.