🧪 Steps to Perform the Experiment:

Step 1: Install Mono Framework (if not already installed)

Open Terminal and run:

bash

Copy

Edit

sudo apt update

sudo apt install mono-complete

Step 2: Download NetworkMiner

Go to the official website: 📎 https://www.netresec.com/?page=NetworkMiner

Click on “NetworkMiner Professional (Free Edition)” → Download the ZIP file.

Alternatively, use wget in terminal:

bash

Copy

Edit

wget https://www.netresec.com/?download=NetworkMiner -O NetworkMiner.zip

Step 3: Extract NetworkMiner

bash

Copy

Edit

unzip NetworkMiner.zip -d NetworkMiner

cd NetworkMiner/NetworkMiner\_\*

Step 4: Run NetworkMiner

bash

Copy

Edit

sudo mono NetworkMiner.exe

NetworkMiner will open with its GUI on Kali Linux.

Step 5: Use a PCAP File or Capture Live Traffic

You can drag and drop a .pcap file into NetworkMiner OR

Use a tool like tcpdump or Wireshark to capture live traffic:

bash

Copy

Edit

sudo tcpdump -i eth0 -w capture.pcap

Then load the file in NetworkMiner using the "File" > "Open" option.

Step 6: Analyze Artifacts

Once the PCAP is loaded:

Go to the Files tab to see extracted files.

Go to Credentials to see usernames/passwords.

View Host details, sessions, DNS info, etc.

Step 7: Report Creation

Take screenshots of the findings and include them in your lab report. Add notes for:

IP addresses involved

Types of files captured

Detected credentials (if any)

Any anomalies or signs of malware