Wireshark Setup (Kali Linux)

This document explains the **step-by-step setup of Wireshark** for PCAP-based network traffic analysis. This setup was used for **Project 6 – Network Traffic Analysis (PCAP)**.

---

1. System Requirements

- Operating System: **Kali Linux** (VM or bare metal)
- RAM: Minimum **4 GB** (8 GB recommended)
- Disk Space: ~2 GB free
- Network: Not required for offline PCAP analysis

---

2. Installing Wireshark

Step 1: Update system packages

sudo apt update && sudo apt upgrade -y

Step 2: Install Wireshark

sudo apt install wireshark -y

Step 3: Allow non-root packet capture (recommended)

During installation, you will be prompted:

> *Allow non-superusers to capture packets?*

Select: **Yes**

If skipped, configure manually:

sudo dpkg-reconfigure wireshark-common
sudo usermod -aG wireshark $USER

Reboot the system after this step.

---

3. Verifying Installation

Check Wireshark version:

wireshark --version

Launch Wireshark:

wireshark

Expected result:

- Wireshark GUI opens without errors
- Interfaces and menu options are visible

---

4. PCAP-Based Analysis Setup (Offline Mode)

⚠ Live capture is **not required** for this project

Step 1: Download PCAP files

PCAP files can be downloaded from trusted sources such as:

- Malware Traffic Analysis >>>> >The pcap file used in this project is from this site<<<<<
- Blue Team Labs Online
- Wireshark Sample Captures

Step 2: Open PCAP file

- Open Wireshark
- Click **File → Open**
- Select the `.pcap` file

---

5. Recommended Wireshark Preferences

Navigate to:

Edit → Preferences

Recommended Settings

- **Name Resolution**: Disabled (to avoid DNS noise)
- **Time Format**: Seconds Since Beginning of Capture
- **Layout**: Three-pane default

---

6. Enabling Useful Columns

Right-click any column → **Column Preferences**

Add:

- Time
- Source
- Destination
- Protocol
- Length
- Info

These columns help during DNS, HTTP, and beaconing analysis.

---

7. Important Wireshark Tools Used

Tool	Purpose
Display Filters	Protocol-specific analysis
Statistics → Conversations	Identify top talkers
Statistics → Endpoints	IP activity analysis
Statistics → I/O Graphs	Detect spikes & beaconing
Follow Stream	View HTTP content

---

8. Display Filters Used in Project

dns
http
udp.port == 53
http.request
ip.addr == <suspicious_ip>

---

9. Common Issues & Fixes

Issue: No packets visible

- Ensure PCAP file is loaded
- Clear display filters

Issue: Time duration not visible

- Go to **View → Time Display Format → Seconds Since Beginning of Capture**

Issue: Permission denied

- Ensure user is in `wireshark` group
- Reboot system

---

10. Project Usage Confirmation

Wireshark was used to:

- Analyze DNS queries
- Inspect HTTP requests
- Detect abnormal traffic spikes
- Identify suspicious IP behavior
- Observe potential beaconing patterns

---

11. Conclusion

Wireshark was successfully installed and configured for **offline PCAP analysis**. The setup supports SOC Level 1 and penetration testing fundamentals and aligns with real-world traffic analysis workflows.