Wireshark Network Traffic Capture and Analysis Report - Kali Linux

1. Introduction

This report provides a step-by-step guide on capturing and analyzing network traffic using Wireshark on Kali Linux. Wireshark is a widely-used network protocol analyzer that allows you to monitor and inspect packets in real time. This document covers installation, capture, filtering, and basic analysis techniques.

2. Installation of Wireshark on Kali Linux

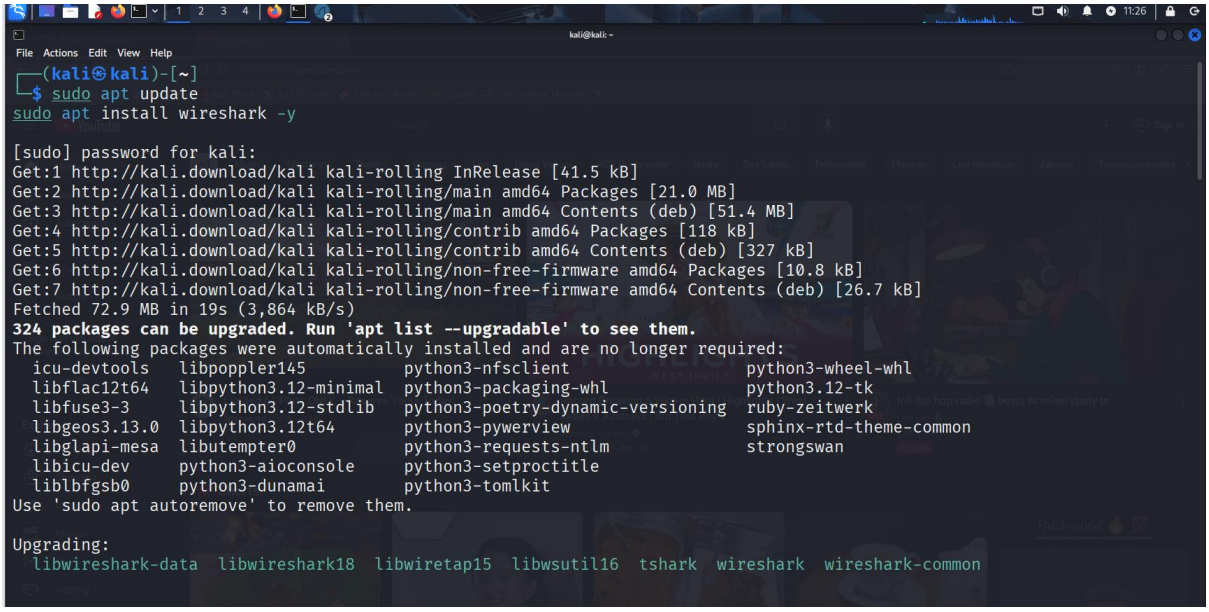
Open a terminal and run the following commands:

sudo apt update

sudo apt install wireshark -y

During installation, select **Yes** if prompted to allow non-superusers to capture packets. Then, add your user to the wireshark group

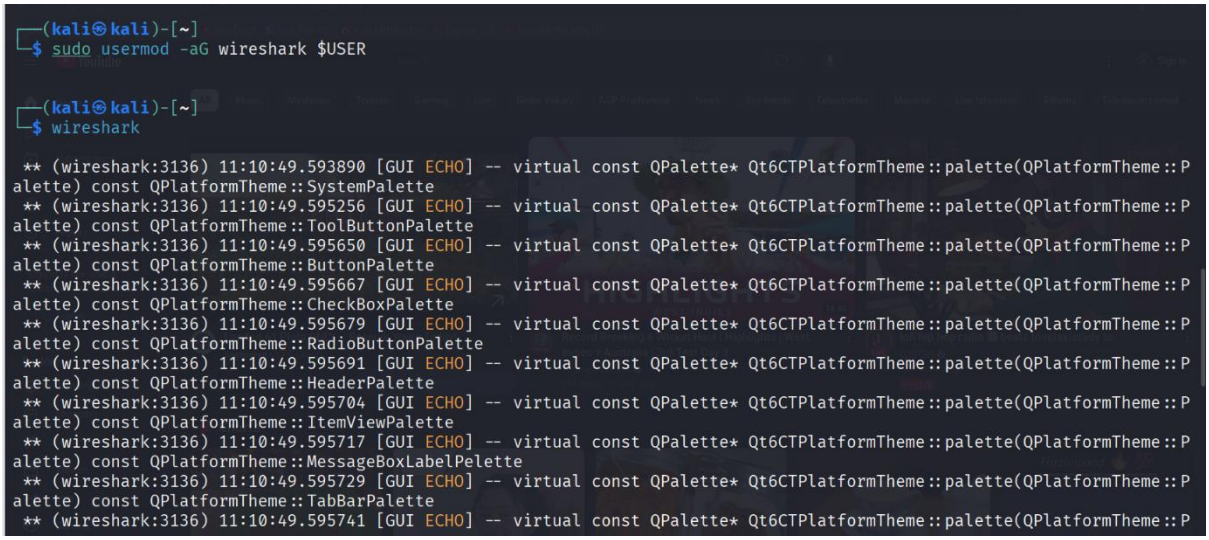
sudo usermod -aG wireshark $USER



3. Launching Wireshark

Start Wireshark via terminal:

wireshark

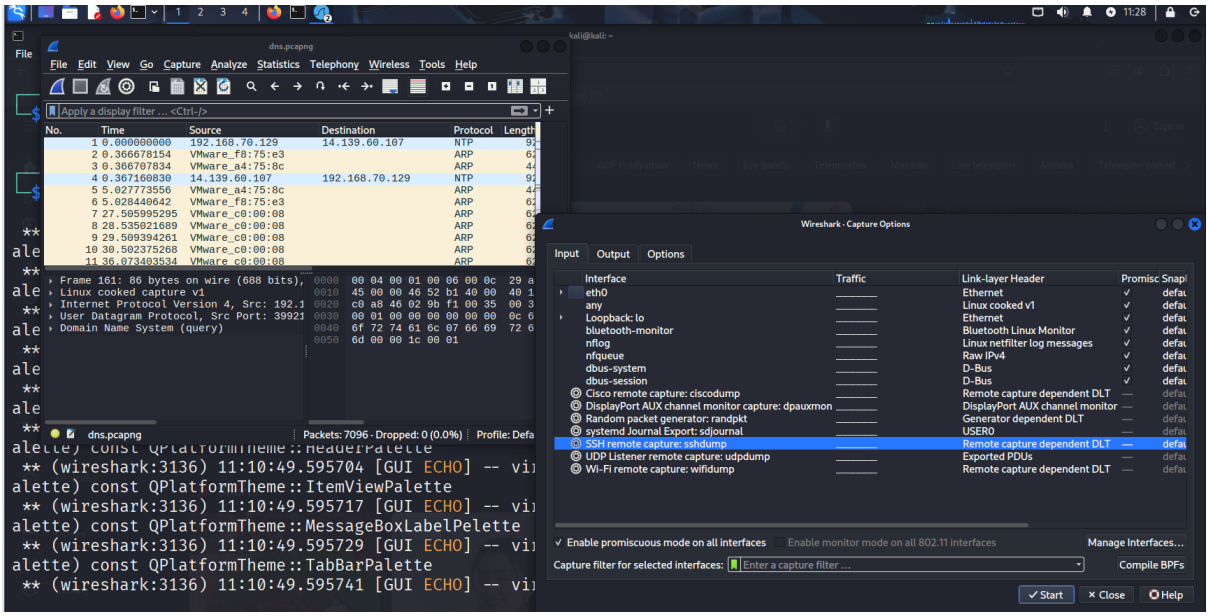


4. Capturing Network Traffic

- Choose the appropriate interface (e.g., eth0 for Ethernet, wlan0 for Wi-Fi).
- Click the interface to start capturing packets.

Optional Capture Filters:

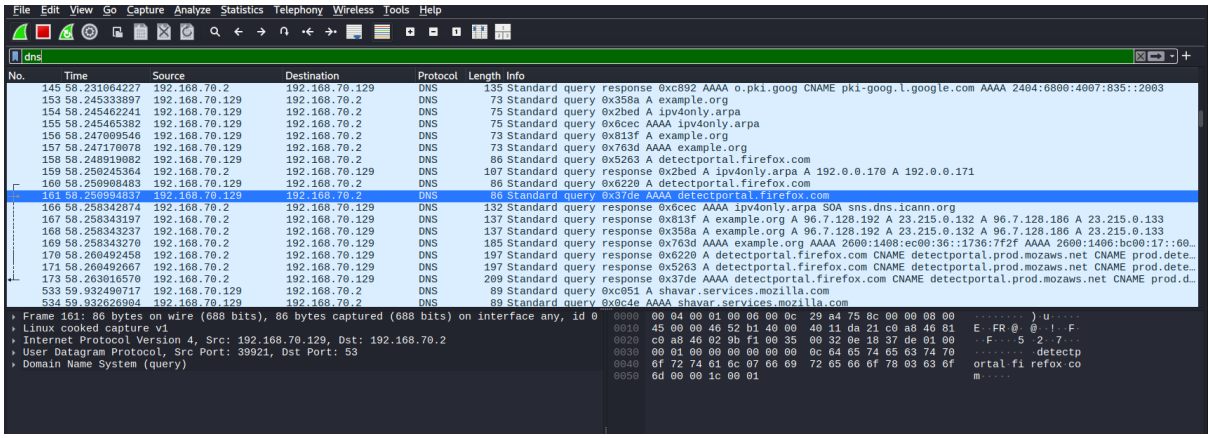
- Capture HTTP traffic: port 80
- Capture traffic from a specific IP: host 192.168.1.10

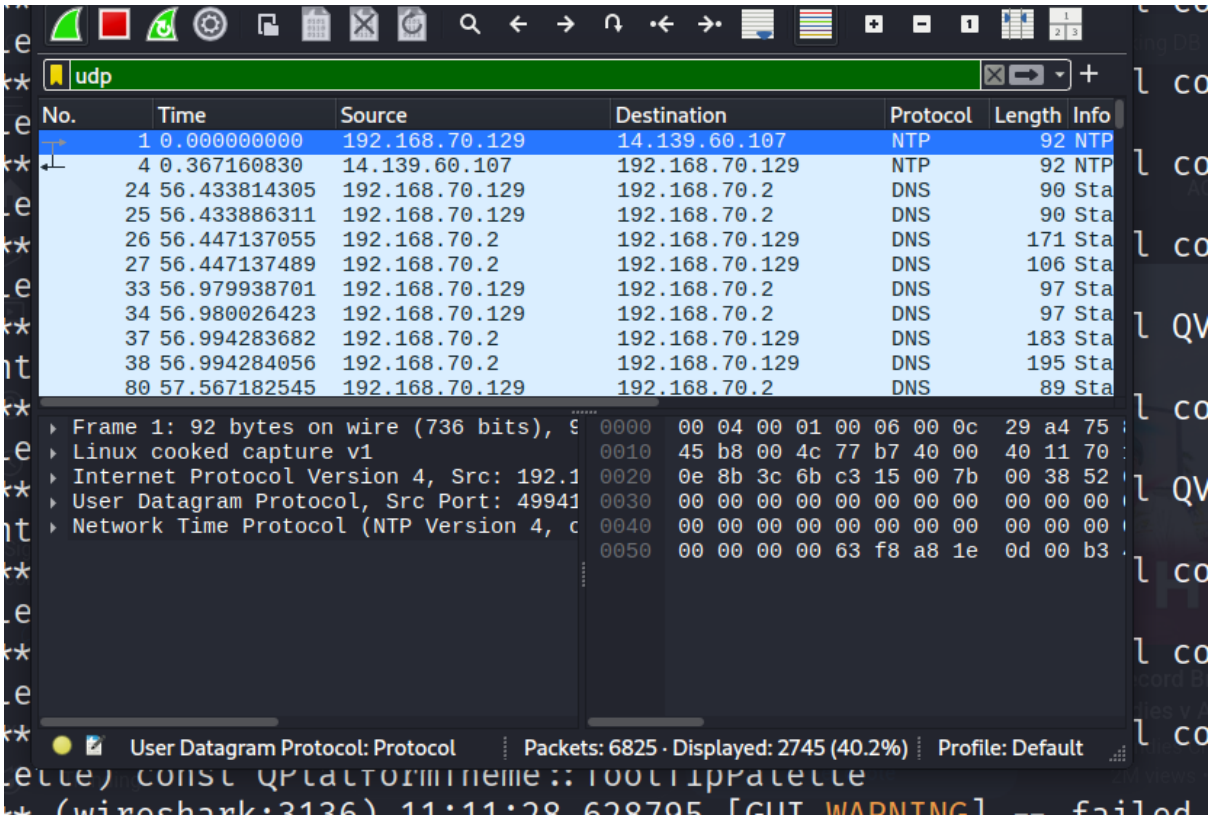


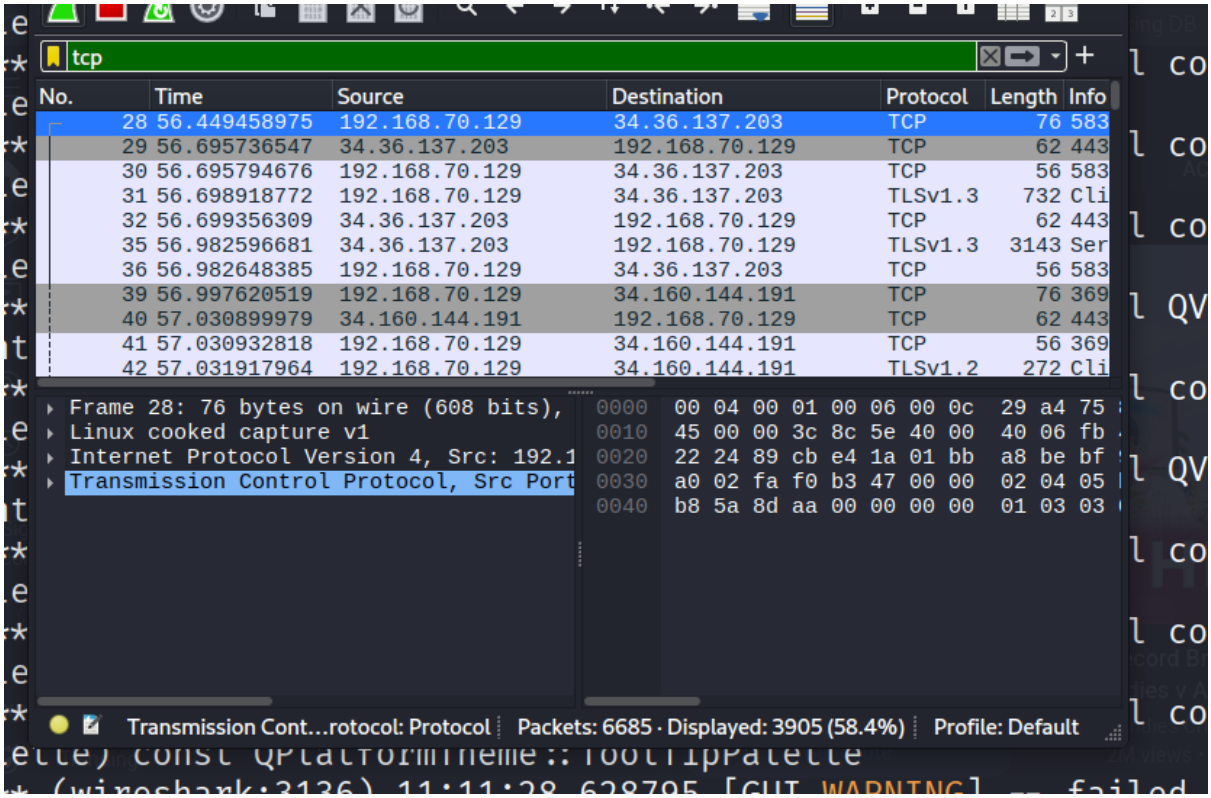
Analyzing Captured Packets

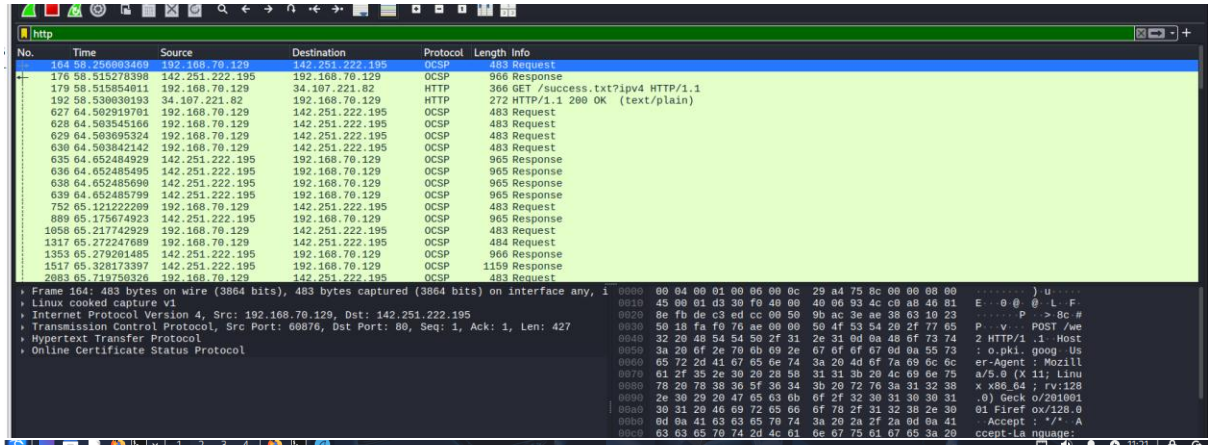
Common protocols to analyze:

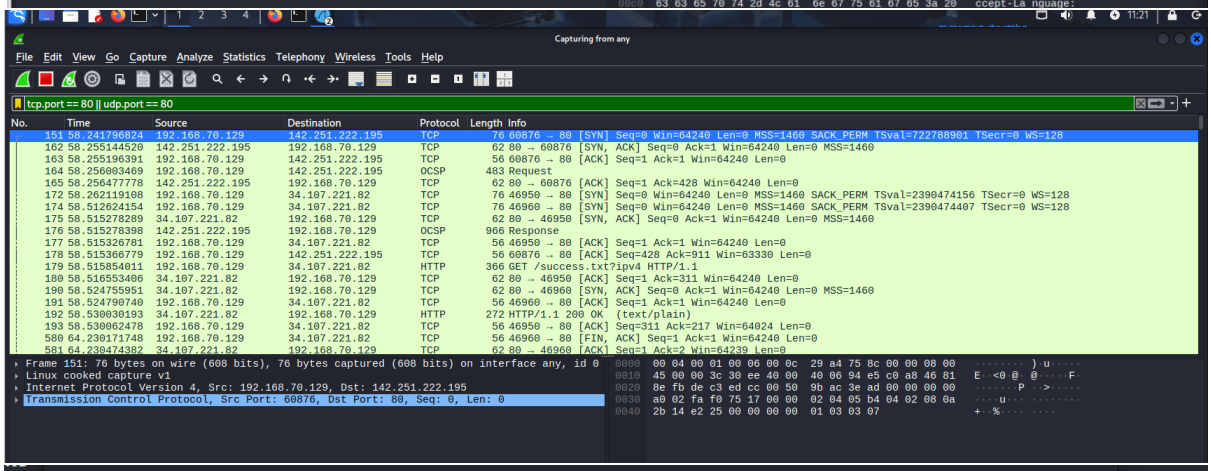
- **HTTP** – Inspect requests and responses
- **DNS** – View name resolution
- **TCP/UDP** – Observe ports and data flow
- **ICMP** – Analyze ping packets

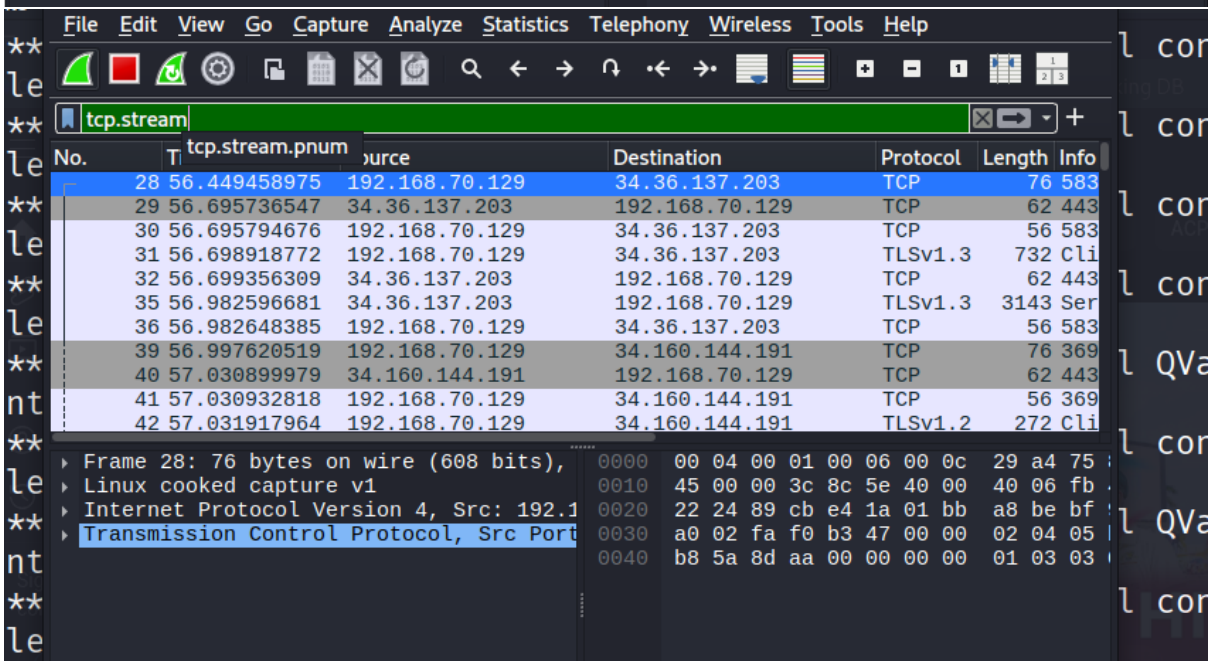





tcp
No. Time Source Destination Protocol Length Info
28 56.449458975 192.168.70.129 34.36.137.203 TCP 76 583
29 56.695736547 34.36.137.203 192.168.70.129 TCP 62 443
30 56.695794676 192.168.70.129 34.36.137.203 TCP 56 583
31 56.698918772 192.168.70.129 34.36.137.203 TLSv1.3 732 Cli
32 56.699356309 34.36.137.203 192.168.70.129 TCP 62 443
35 56.982596681 34.36.137.203 192.168.70.129 TLSv1.3 3143 Ser
36 56.982648385 192.168.70.129 34.36.137.203 TCP 56 583
39 56.997620519 192.168.70.129 34.160.144.191 TCP 76 369
40 57.030899979 34.160.144.191 192.168.70.129 TCP 62 443
41 57.030932818 192.168.70.129 34.160.144.191 TCP 56 369
42 57.031917964 192.168.70.129 34.160.144.191 TLSv1.2 272 Cli
Frame 28: 76 bytes on wire (608 bits),
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.1
Transmission Control Protocol, Src Port
0000 00 04 00 01 00 06 00 0c 29 a4 75
0010 45 00 00 3c 8c 5e 40 00 40 06 fb
0020 22 24 89 cb e4 1a 01 bb a8 be bf
0030 a0 02 fa f0 b3 47 00 00 02 04 05
0040 b8 5a 8d aa 00 00 00 00 01 03 03
Transmission Cont...rotocol: Protocol
Packets: 6685 · Displayed: 3905 (58.4%)
Profile: Default







5. Stopping the Capture

Click the red square **Stop** button in the toolbar to end the capture.

Conclusion

Wireshark is a powerful tool for network traffic capture and analysis. Mastering its filters, stream tracking, and protocol analysis enables in-depth understanding of network behavior and threat detection.