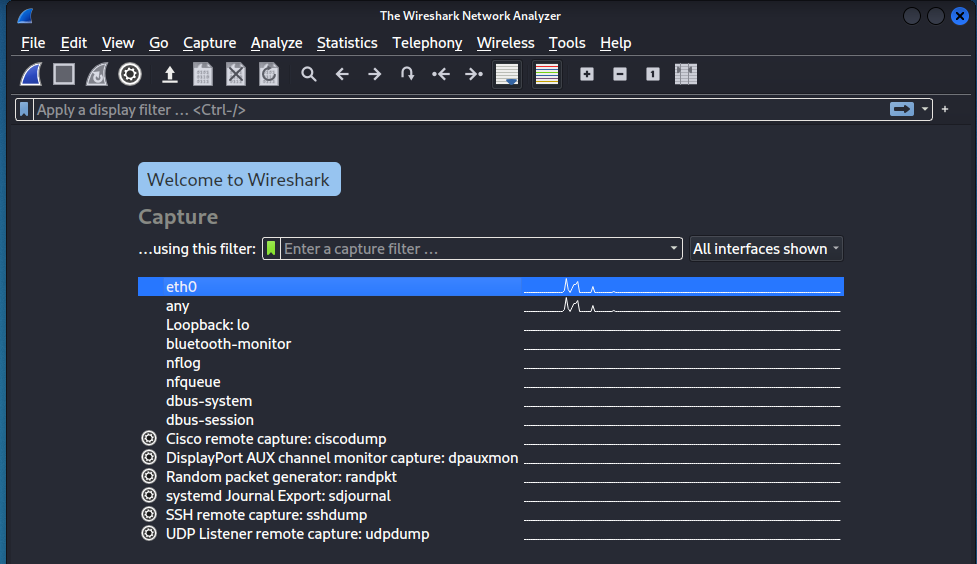
Network Forensics

Part I Traffic Analysis using Wireshark

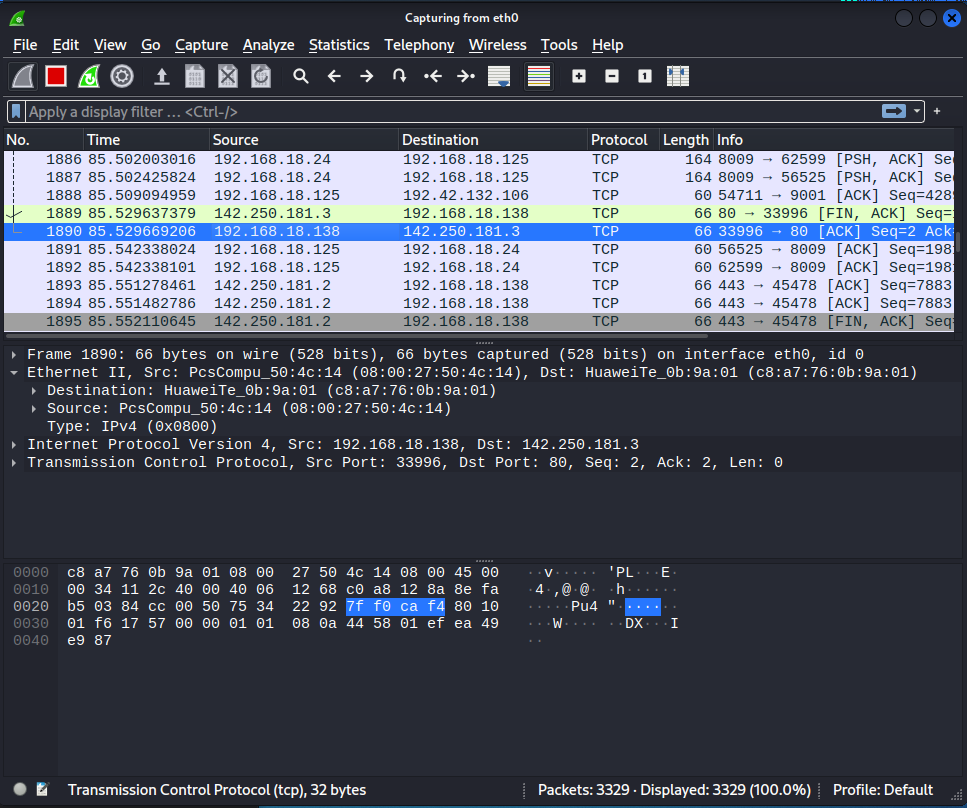
**Step 1**

Wireshark is one of the most popular tools in the world of network forensics. It is used for network troubleshooting and packet analysis. In kali linux it comes pre-installed. You need to write in terminal “**wireshark**” to start it. Below is the screenshot for the interface that you need to choose to capture the type of traffic.



**Step 2 & 3**

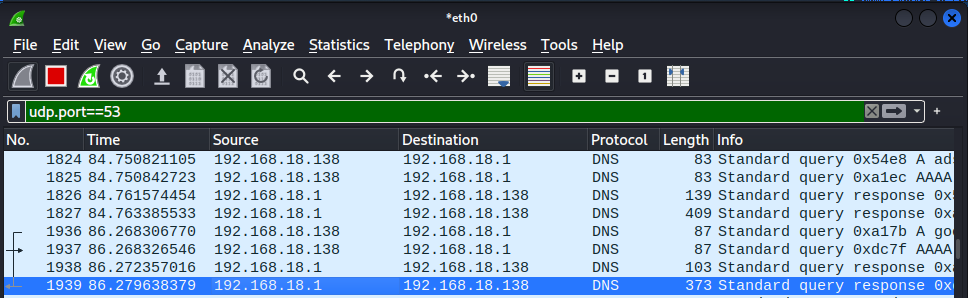
I selected eth0 interface to capture the traffic that is passing through my device. Below is the screenshot for further analyzing each packet that occurs during transmission. We can see **Source**, **Destination** and the **Protocol** that tells important information about the specific packet



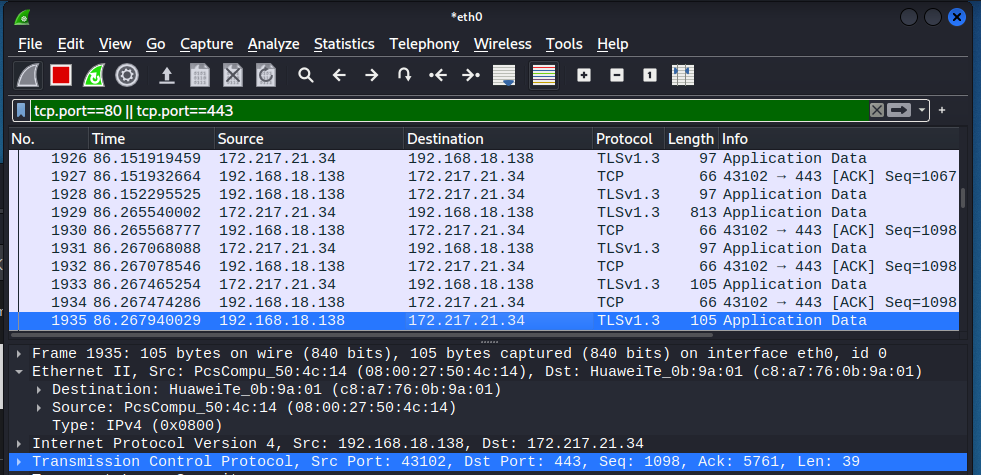
**Step 4**

Wireshark is capable of using filters to find out specific packet in no time, it is very useful as it saves a lot of time. You can type the filter in the “Apply a display filter” field shown in the below screenshot:

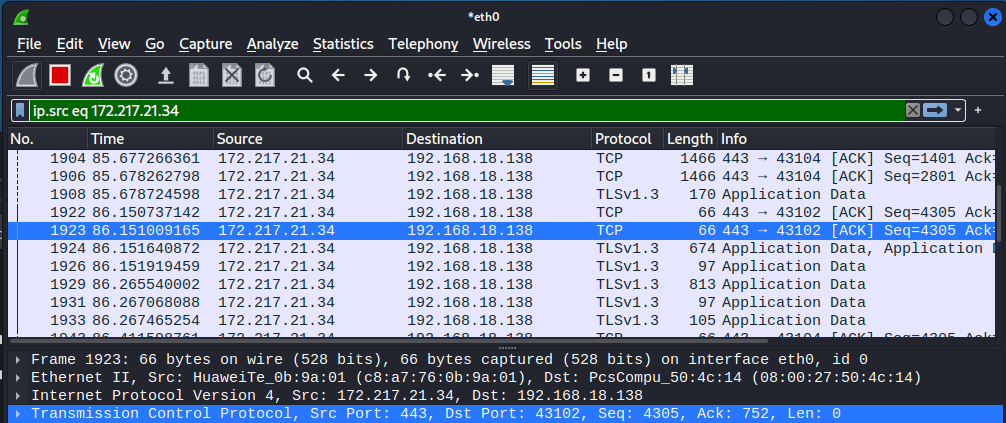
**udp.port==53**



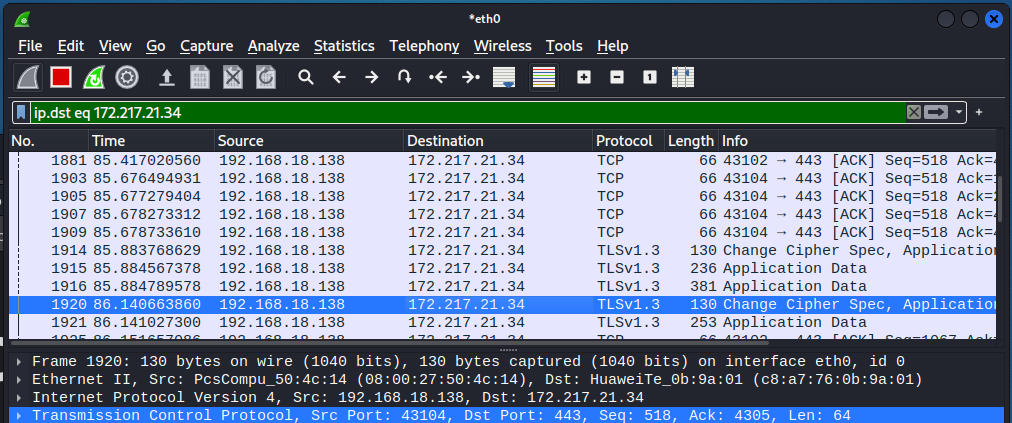
**tcp.port==80 || tcp.port==443**



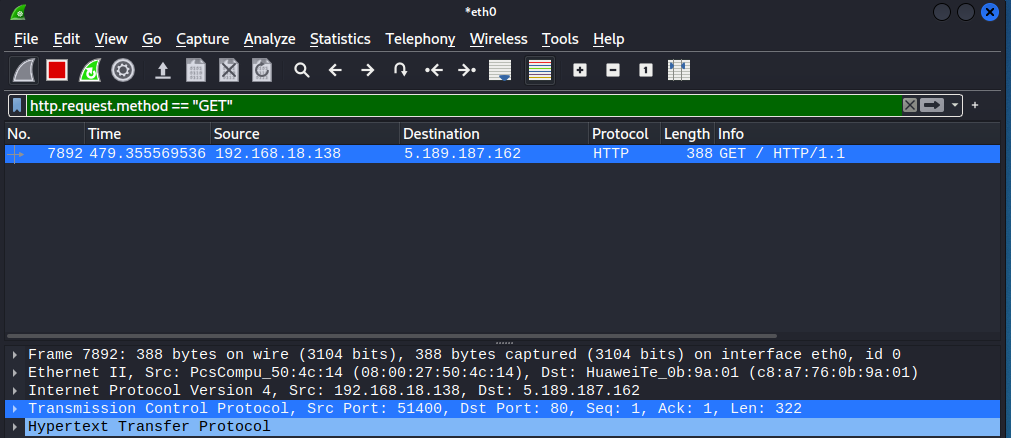
**ip.src eq 172.217.21.34**



**ip.dst eq 172.217.21.34**



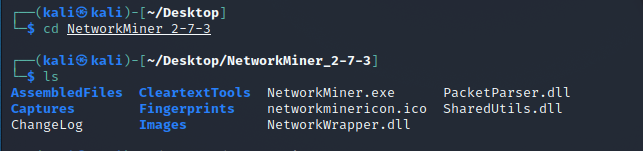
**http.request.method == "GET"**

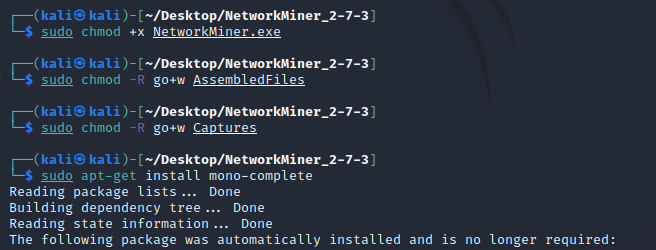


Part II: NetworkMiner Packer Viewer

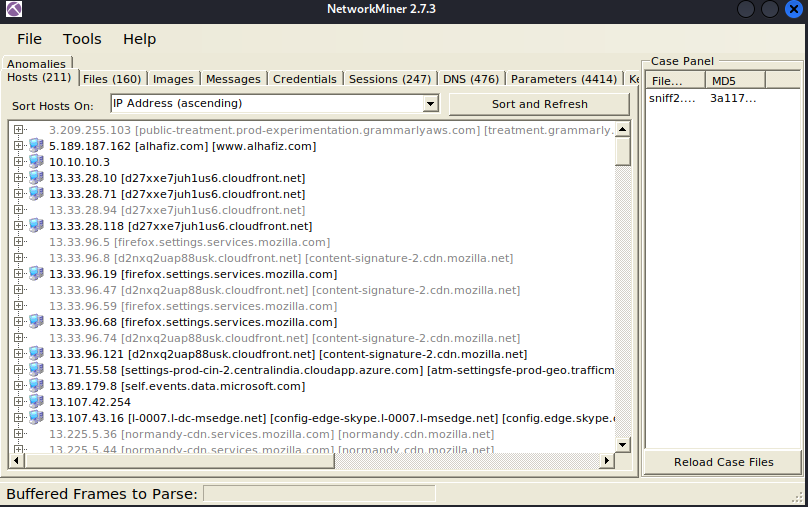
Installing **NetworkMiner** which is another great tool. It is GUI compared to wireshark but is cable to read .pcap files.

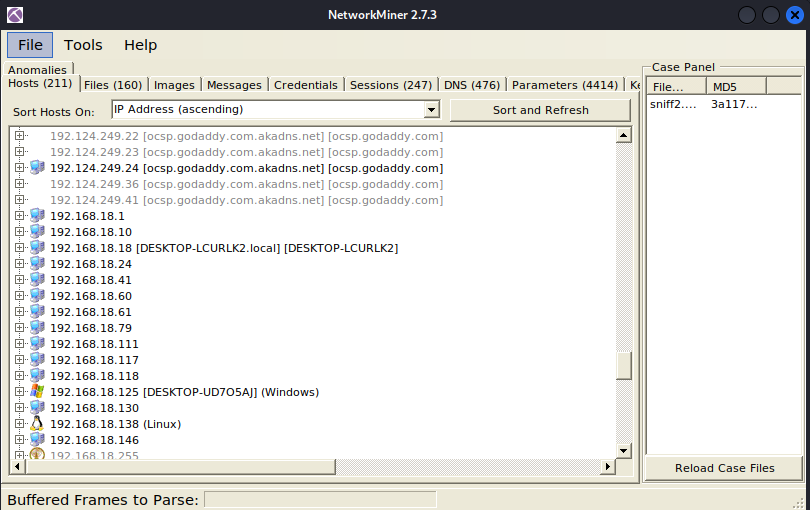






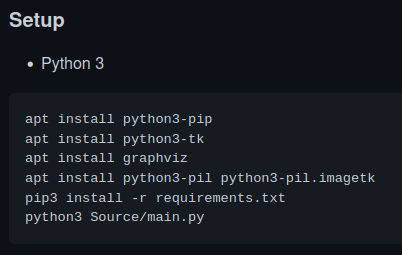
Using **Network Miner** to read .pcap file that was generated and captured by Wireshark, it gives us GUI based feature which is easier to use.

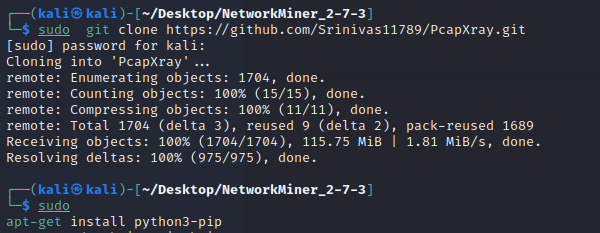


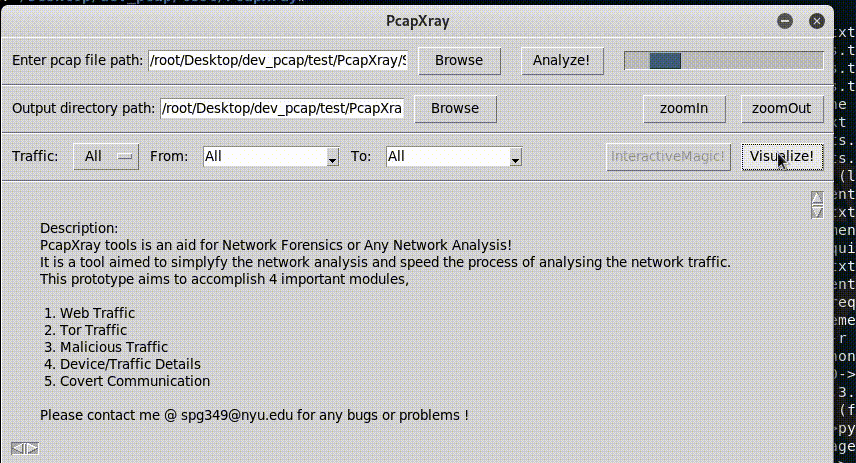


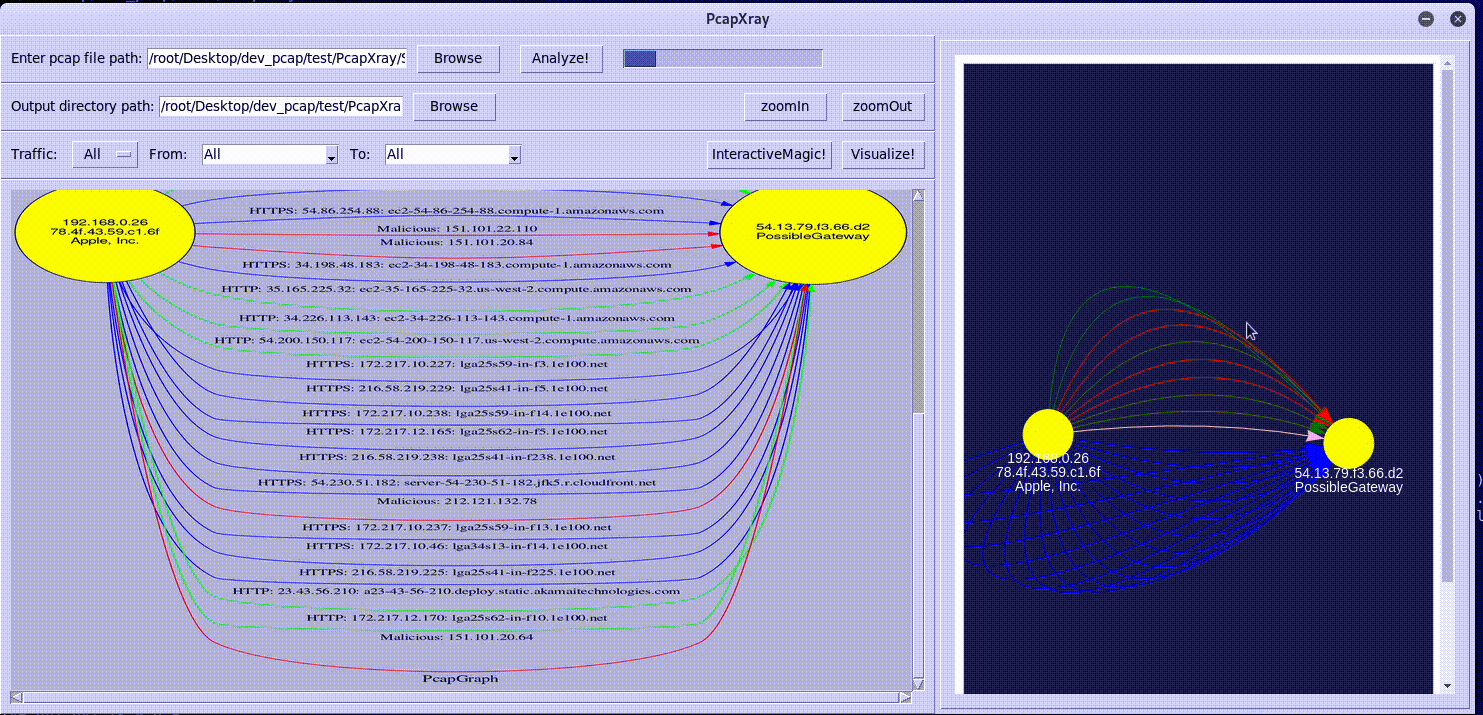
Part III: Packet Visualization and Analysis using PcapXray

A Network Forensics Tool - To visualize a Packet Capture offline as a Network Diagram including device identification, highlight important communication and file extraction









SUMMARY

This lab was all about learning **Network Forensics** from analyzing data transmission packets using wireshark to using PcapXray (**Packet Visualization**). In the First part, we learned how to sniff packets across the network not only that but also to read those packets, Further more we used filters to make our job easy. In the Second part, we learned about **NetworkMiner Packet Viewer,** it is a graphical user interface version of wireshark and used to read the packets captured by Wireshark. It is easy compared to wireshark. In the Third part, we used **PcapXray**, which is another amazing tool for reading data across the network, it extracts graph from wireshark pcap files and one can track each packet and endpoint nodes.