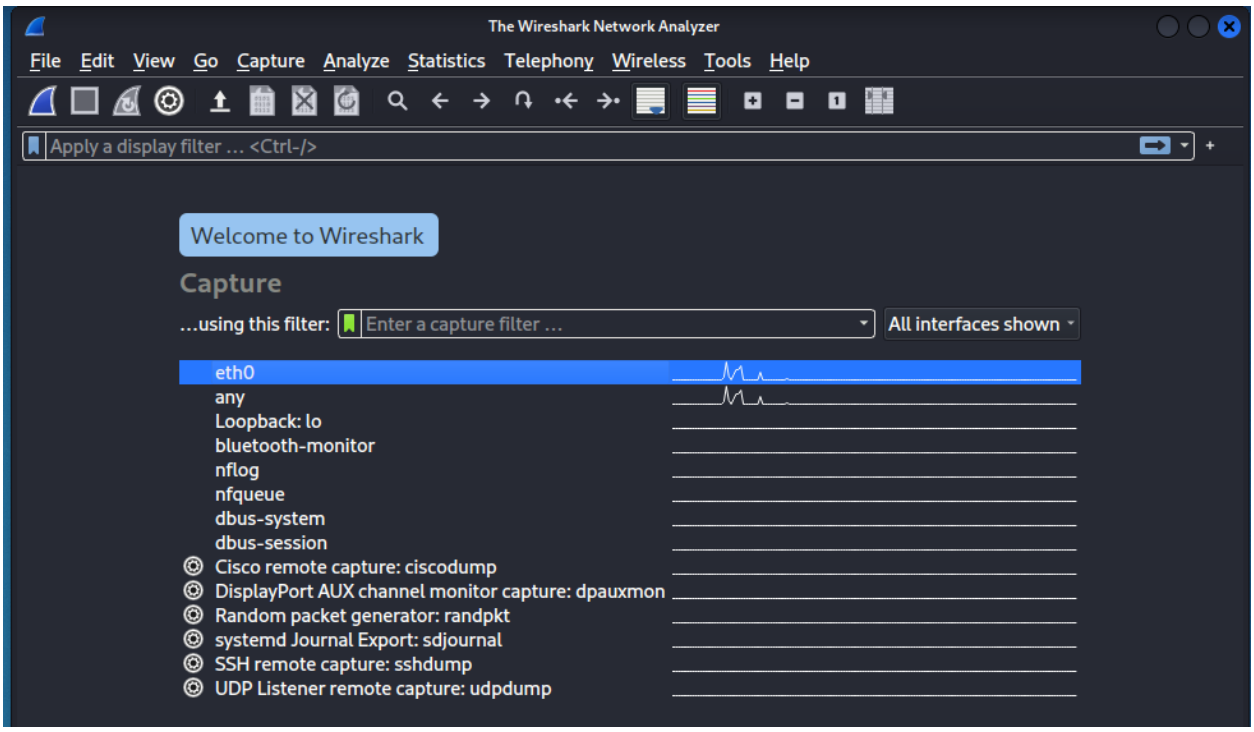
PART I TRAFFIC ANALYSIS USING WIRESHARK

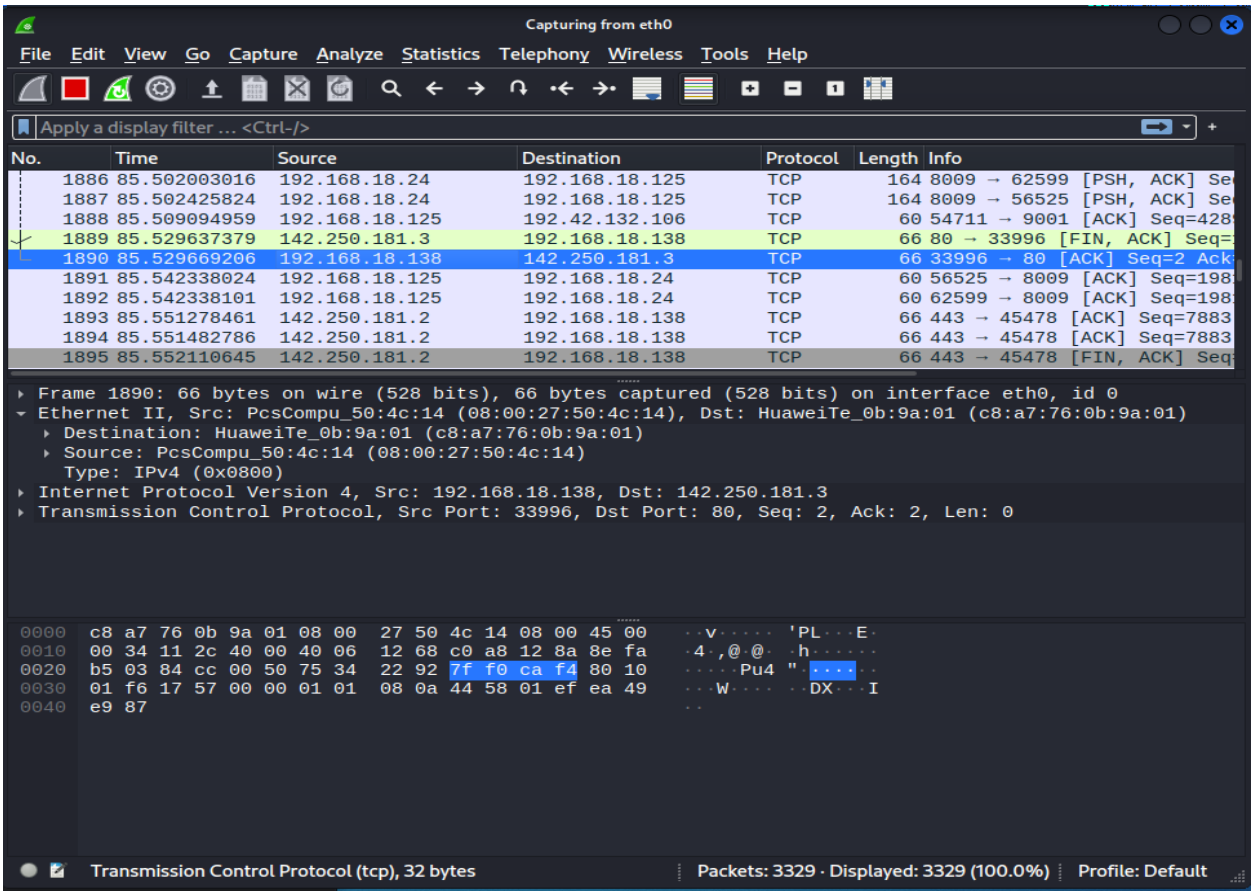
Step 1

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

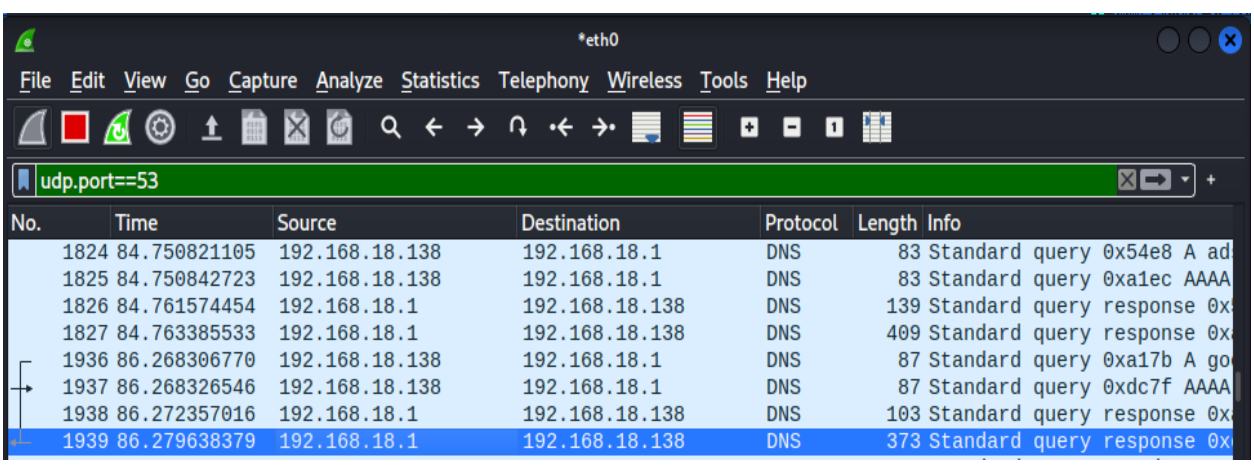
I selected eth0 interface to capture the traffic that is passing through my device. Below is the screenshot for further analyzing each packet that occurs during transmission. We can see **Source**, **Destination** and the **Protocol** that tells important information about the specific packet



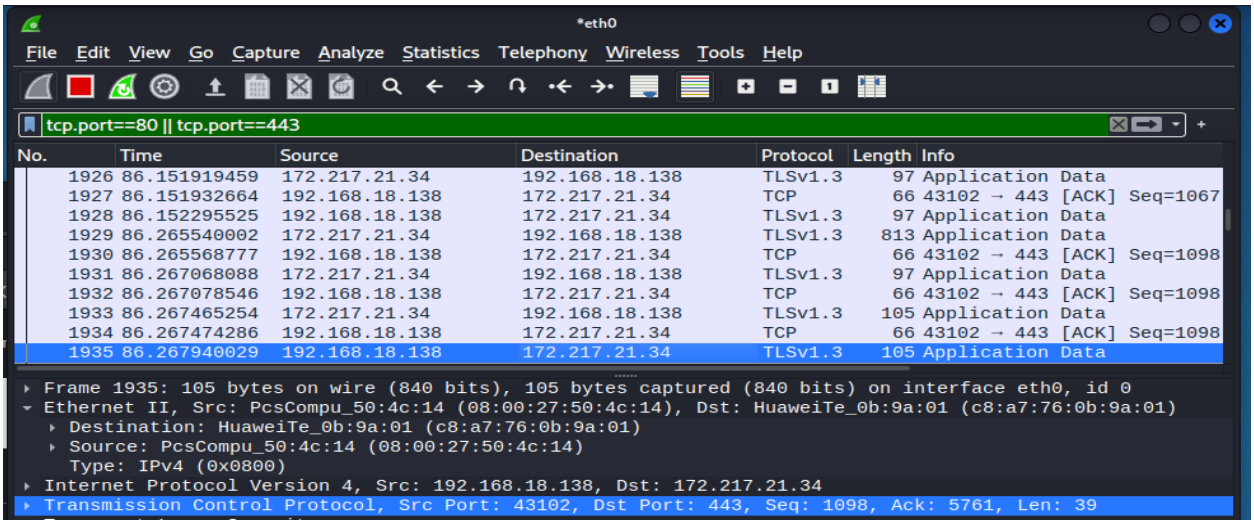
Step 4

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:

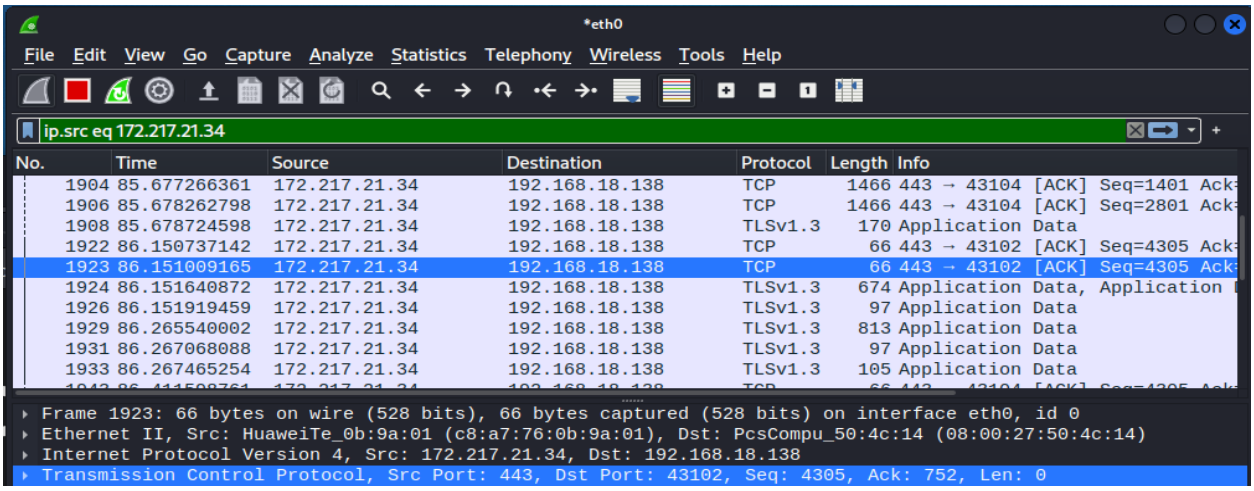
udp.port==53



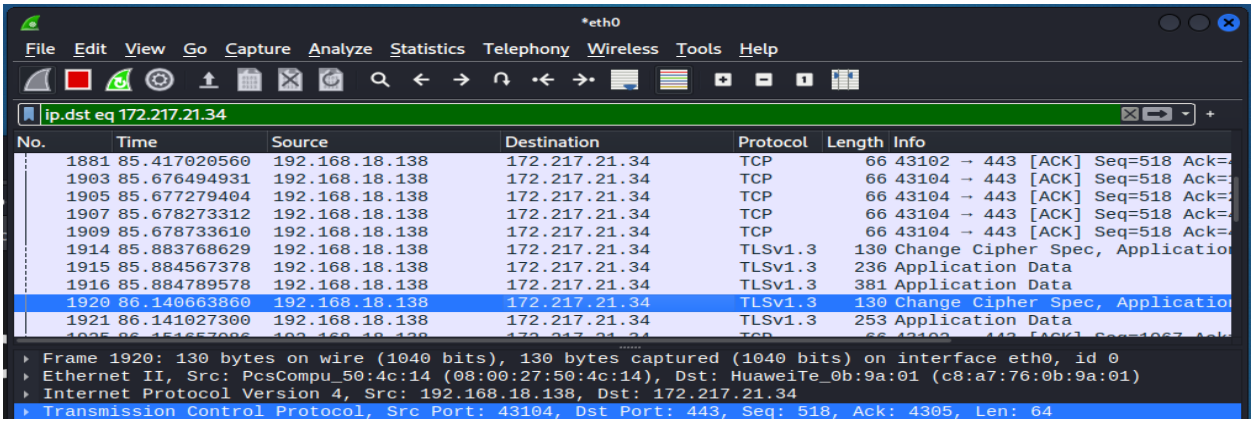
tcp.port==80 || tcp.port==443



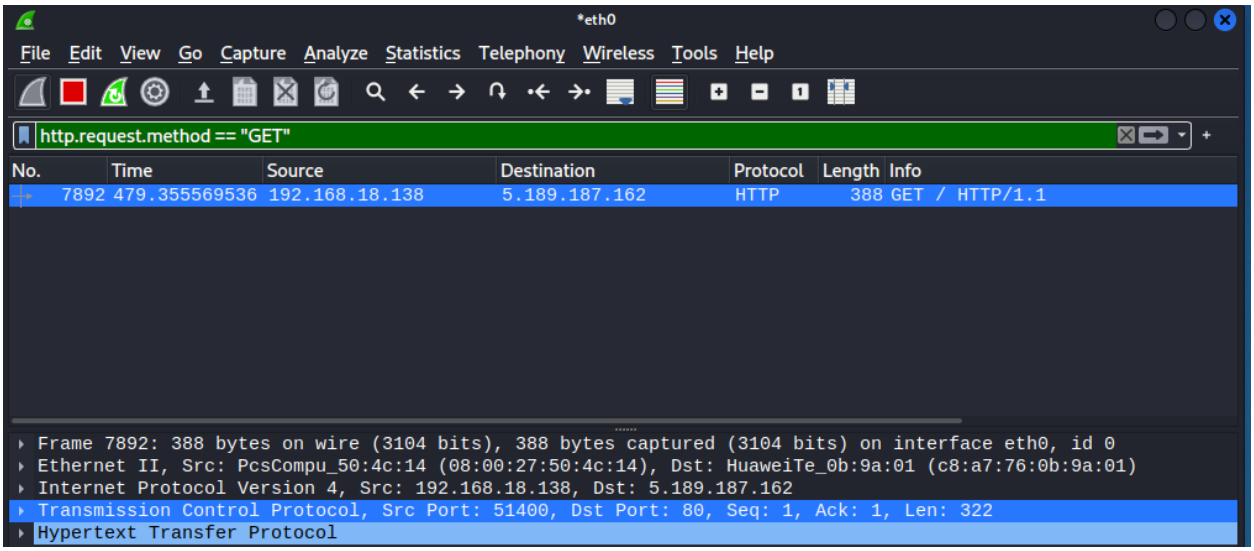
ip.src eq 172.217.21.34



ip.dst eq 172.217.21.34



http.request.method == "GET"



PART II: NETWORKMINER PACKER VIEWER

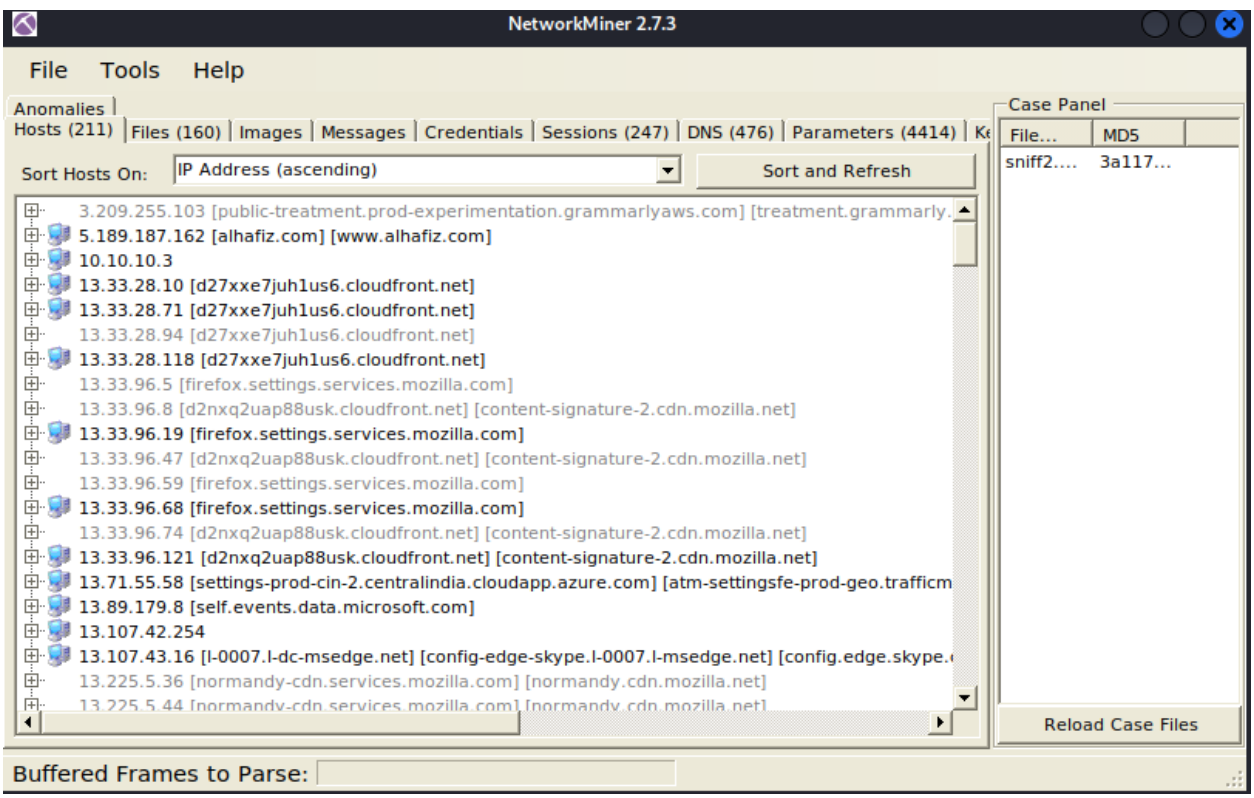
Installing **NetworkMiner** which is another great tool. It is GUI compared to wireshark but is cable to read .pcap files.

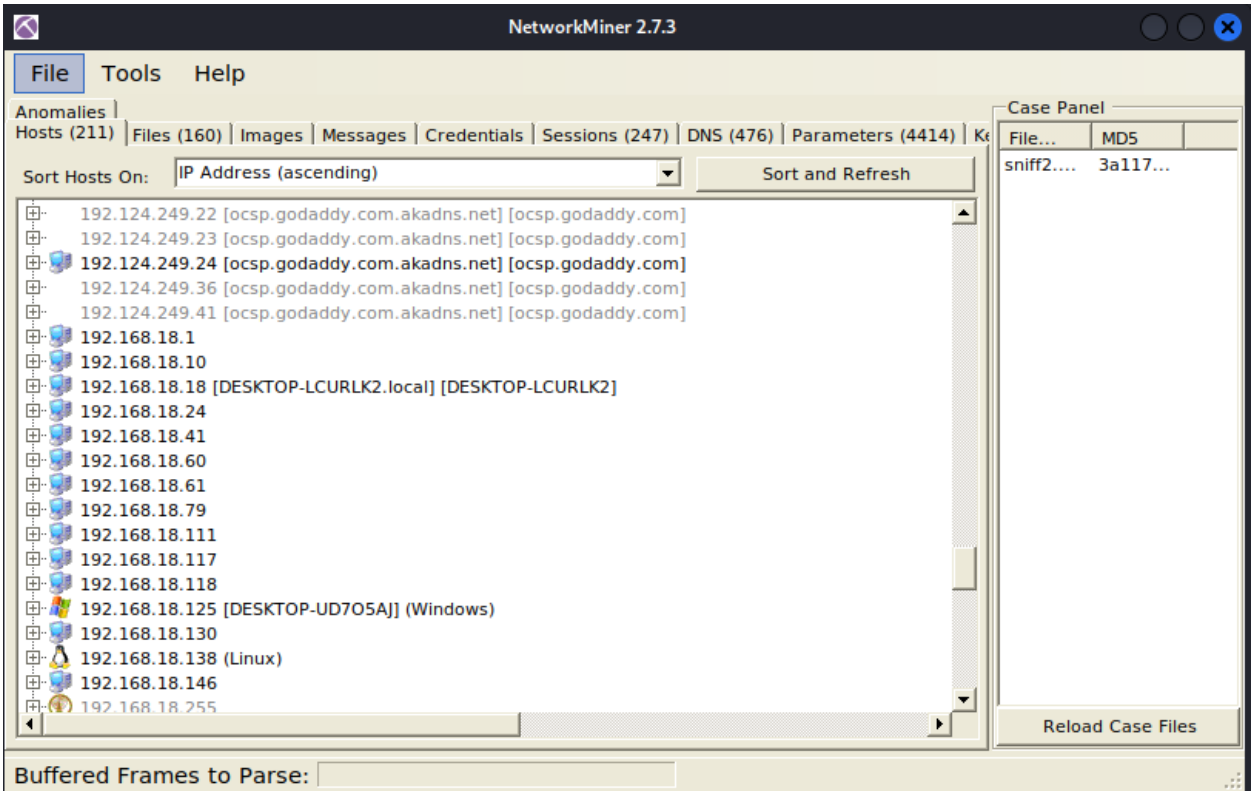
```
┌──(kali㉿kali)-[~/Desktop]
└─$ wget www.netresec.com/?download=NetworkMiner -O nm.zip
--2022-04-17 09:09:16--  http://www.netresec.com/?download=NetworkMiner
Resolving www.netresec.com (www.netresec.com)... 81.95.105.80, 2a02:4a8:ac24:137::105:80
Connecting to www.netresec.com (www.netresec.com)|81.95.105.80|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.netresec.com/?download=NetworkMiner [following]
--2022-04-17 09:09:17--  https://www.netresec.com/?download=NetworkMiner
Connecting to www.netresec.com (www.netresec.com)|81.95.105.80|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2728854 (2.6M) [application/octet-stream]
Saving to: 'nm.zip'

nm.zip                  100%[===================================>]   2.60M   702KB/s    in 4.1s

2022-04-17 09:09:22 (647 KB/s) - 'nm.zip' saved [2728854/2728854]


┌──(kali㉿kali)-[~/Desktop]
└─$ sudo unzip nm.zip
[sudo] password for kali:
Archive:  nm.zip
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd NetworkMiner 2-7-3

┌──(kali㉿kali)-[~/Desktop/NetworkMiner_2-7-3]
└─$ ls
AssembledFiles  CleartextTools  NetworkMiner.exe      PacketParser.dll
Captures        Fingerprints    networkminericon.ico  SharedUtils.dll
ChangeLog       Images          NetworkWrapper.dll
```

```
┌──(kali㉿kali)-[~/Desktop/NetworkMiner_2-7-3]
└─$ sudo chmod +x NetworkMiner.exe

┌──(kali㉿kali)-[~/Desktop/NetworkMiner_2-7-3]
└─$ sudo chmod -R go+w AssembledFiles

┌──(kali㉿kali)-[~/Desktop/NetworkMiner_2-7-3]
└─$ sudo chmod -R go+w Captures

┌──(kali㉿kali)-[~/Desktop/NetworkMiner_2-7-3]
└─$ sudo apt-get install mono-complete
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
```

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

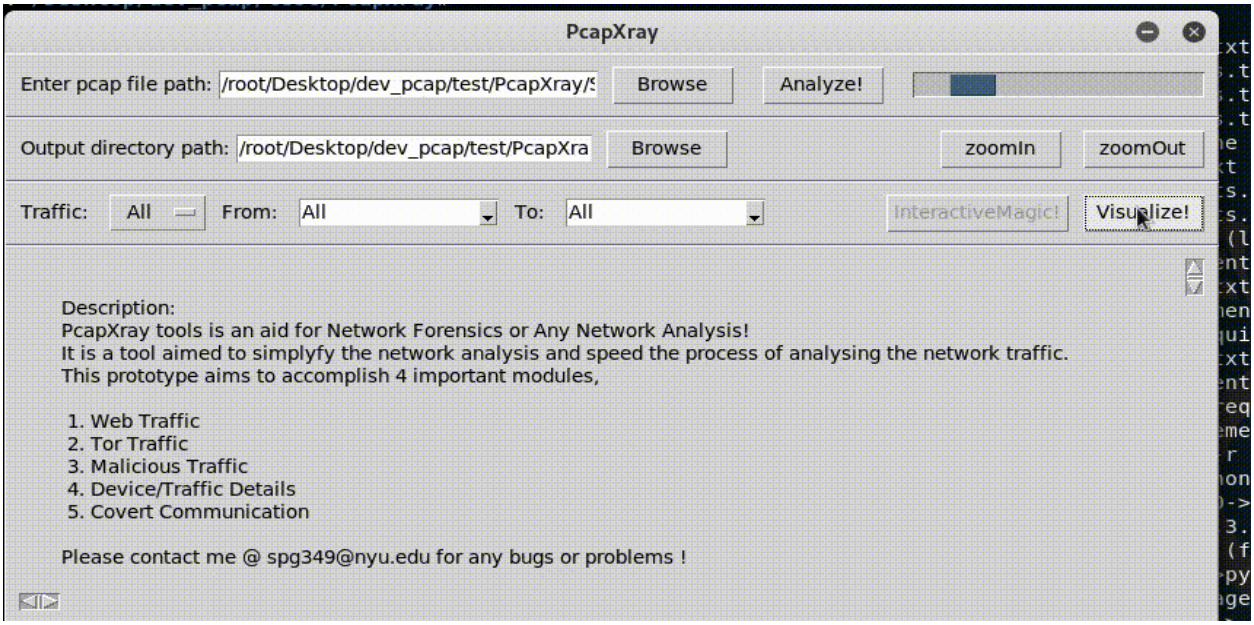
A Network Forensics Tool - To visualize a Packet Capture offline as a Network Diagram including device identification, highlight important communication and file extraction

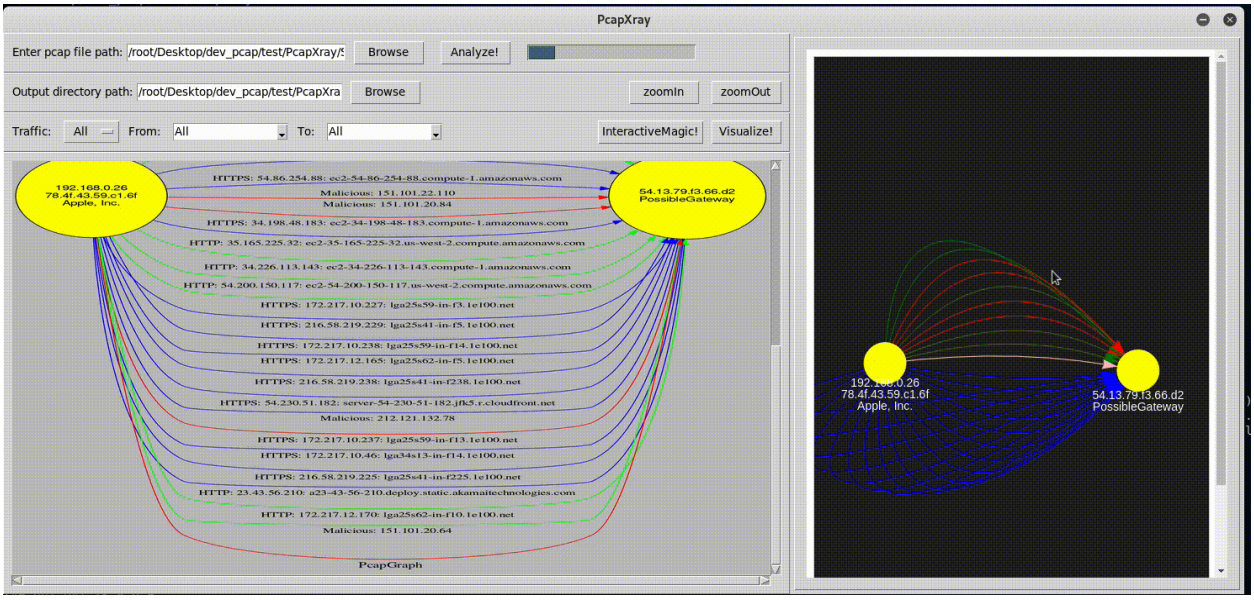
Setup

- Python 3

```
apt install python3-pip
apt install python3-tk
apt install graphviz
apt install python3-pil python3-pil.imagetk
pip3 install -r requirements.txt
python3 Source/main.py
```

```
┌──(kali㉿kali)-[~/Desktop/NetworkMiner_2-7-3]
└─$ sudo  git clone https://github.com/Srinivas11789/PcapXray.git
[sudo] password for kali:
Cloning into 'PcapXray'...
remote: Enumerating objects: 1704, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 1704 (delta 3), reused 9 (delta 2), pack-reused 1689
Receiving objects: 100% (1704/1704), 115.75 MiB | 1.81 MiB/s, done.
Resolving deltas: 100% (975/975), done.

┌──(kali㉿kali)-[~/Desktop/NetworkMiner_2-7-3]
└─$ sudo
apt-get install python3-pip
```





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.