Lab 3

CSC154

Daniel Hammon

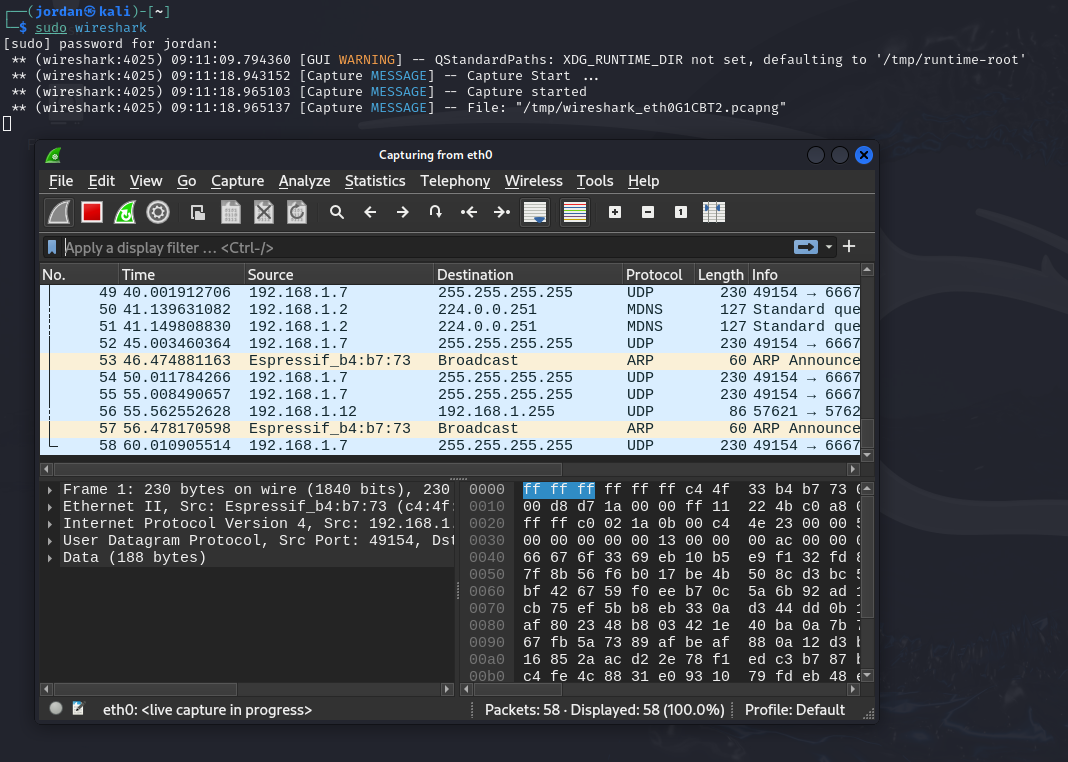
TTH 5:30pm

Jordan Penaloza

Lab 3 Overview:

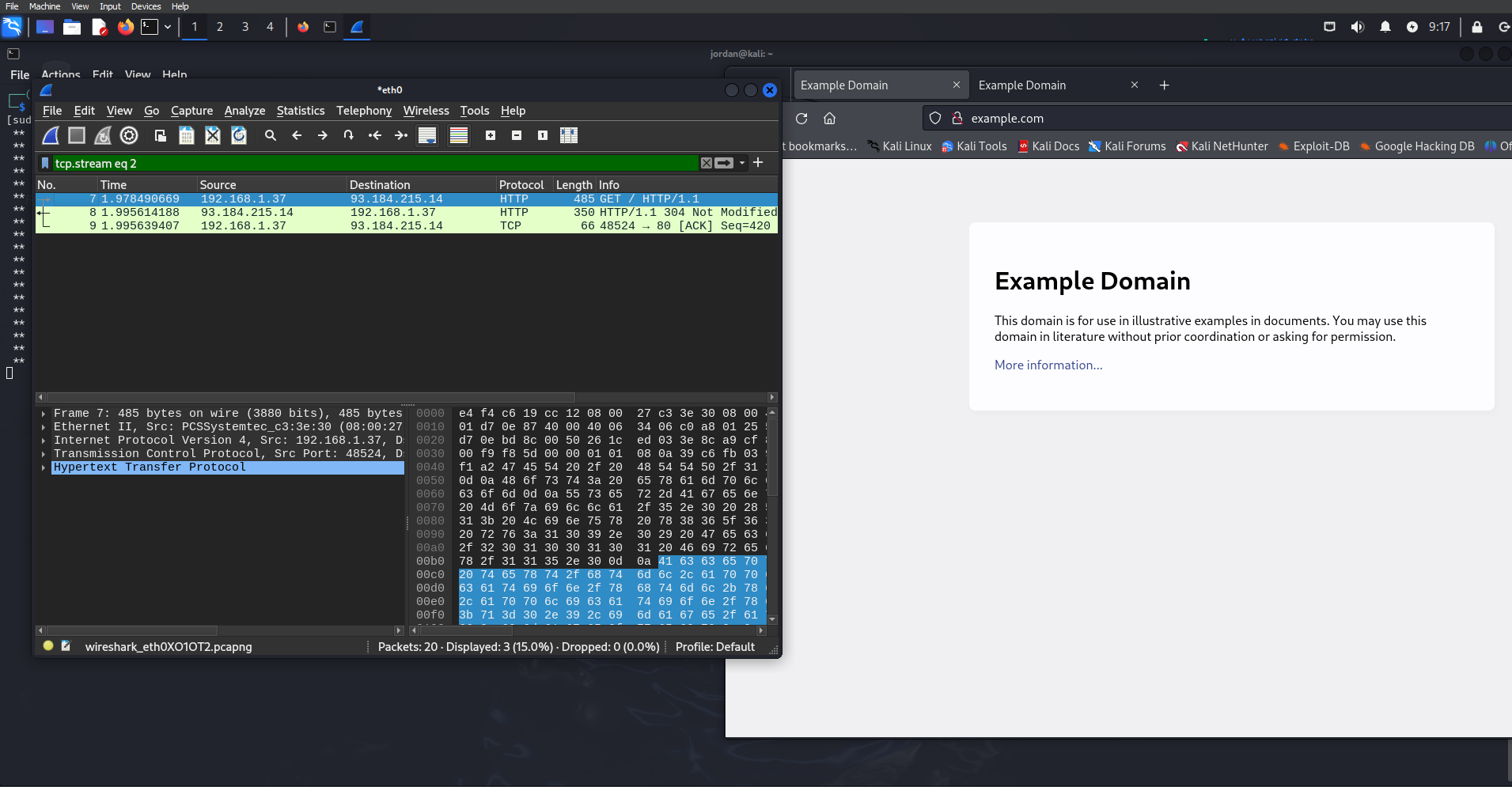
The goal of this lab is to become proficient in network security. We will be learning how to utilize packet capturing tools like wire shark and various network utilities. We will also learn about host and service discovery as well as WEP cracking.

Step 1/2: Launch Wireshark and Start Packet Capture

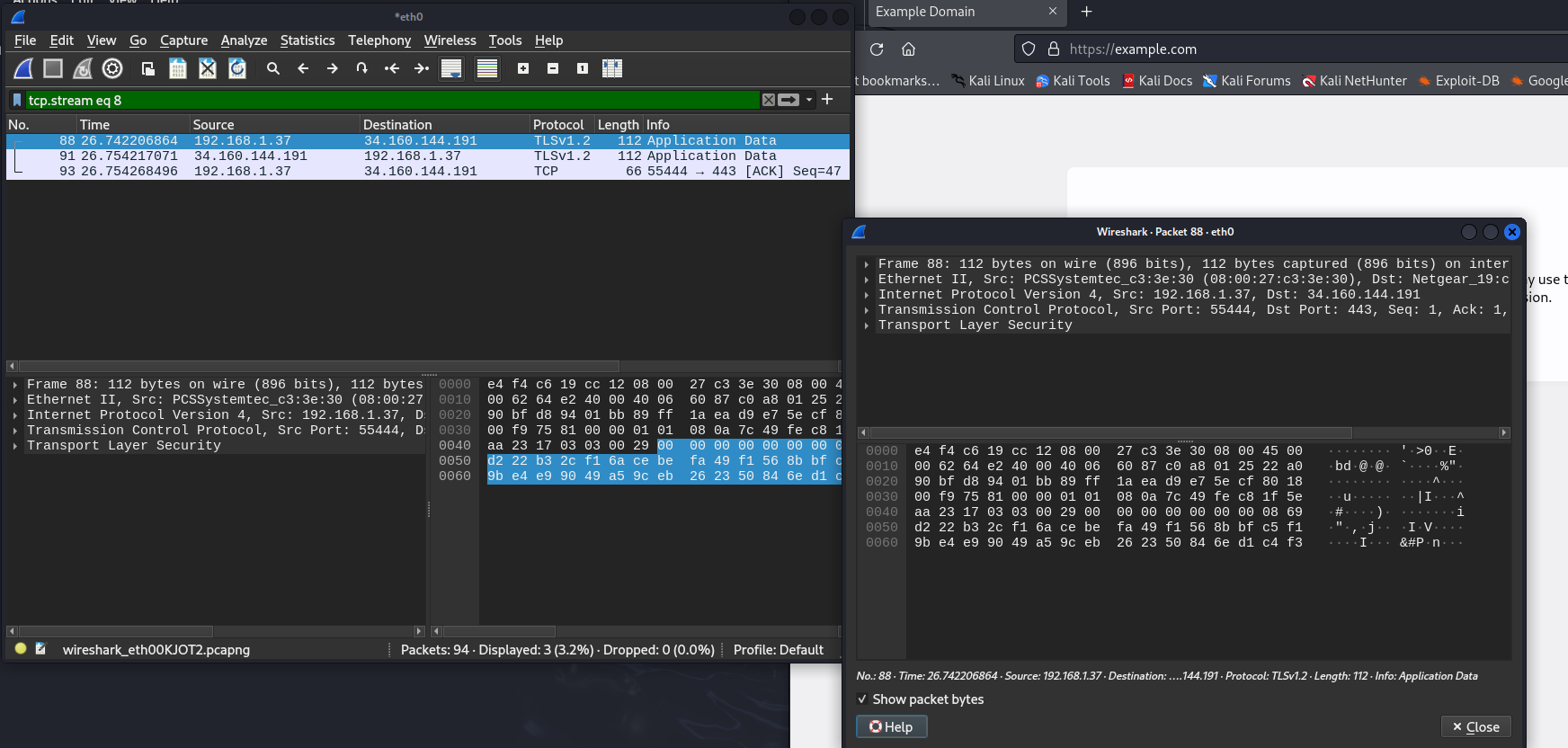


Here I opened wireshark through the terminal and began a packet capture. So far it seems like there is a lot of traffic.

Step 3: Packet Analysis

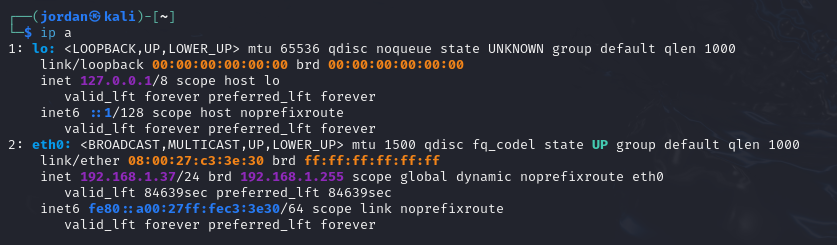


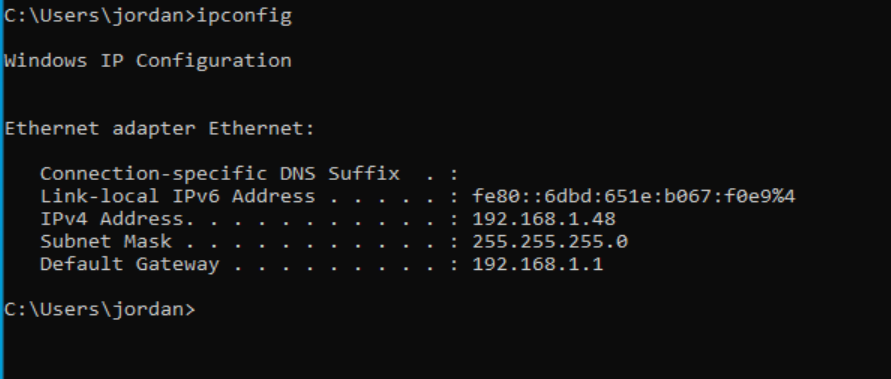
After following the HTTP stream for the http page we were able to filter out lal of the clutter and get the traffic for the http page.



Here is the traffic fore the HTTPS page, something interesting about this one is that we aren’t able to view the payload in plaintext like we could with the HTTP page, probably because it’s encrypted.

3.2 Network Utilities:

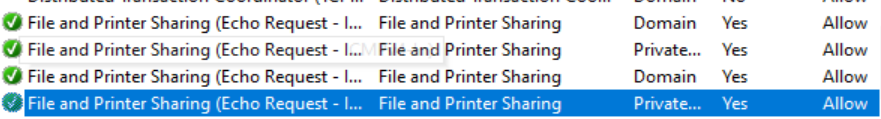




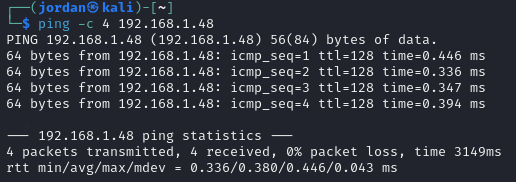
IP configurations for kali and windows machines

Kali: 192.168.1.37

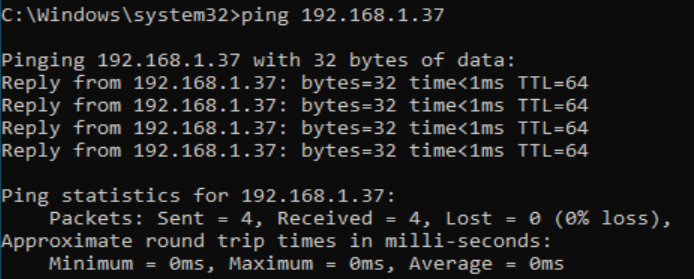
Windows: 192.168.1.48



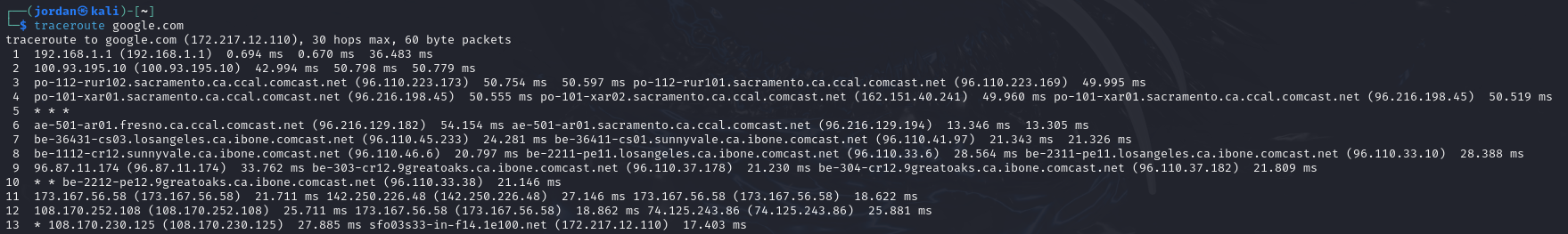
Here I have allowed the file and printer sharing firewall rules.



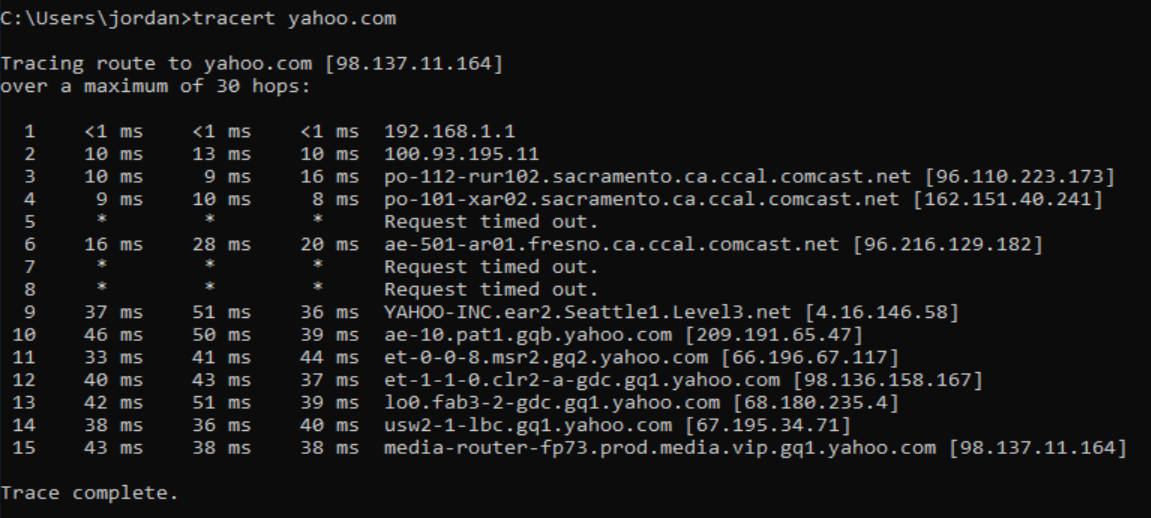
Looks like we are able to ping the windows machine from kali!



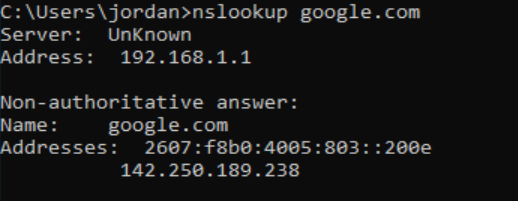
Ping to kali from windows

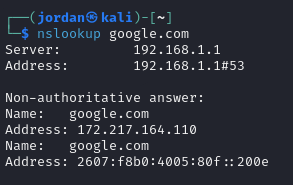


Traceroute from kali machine to google servers

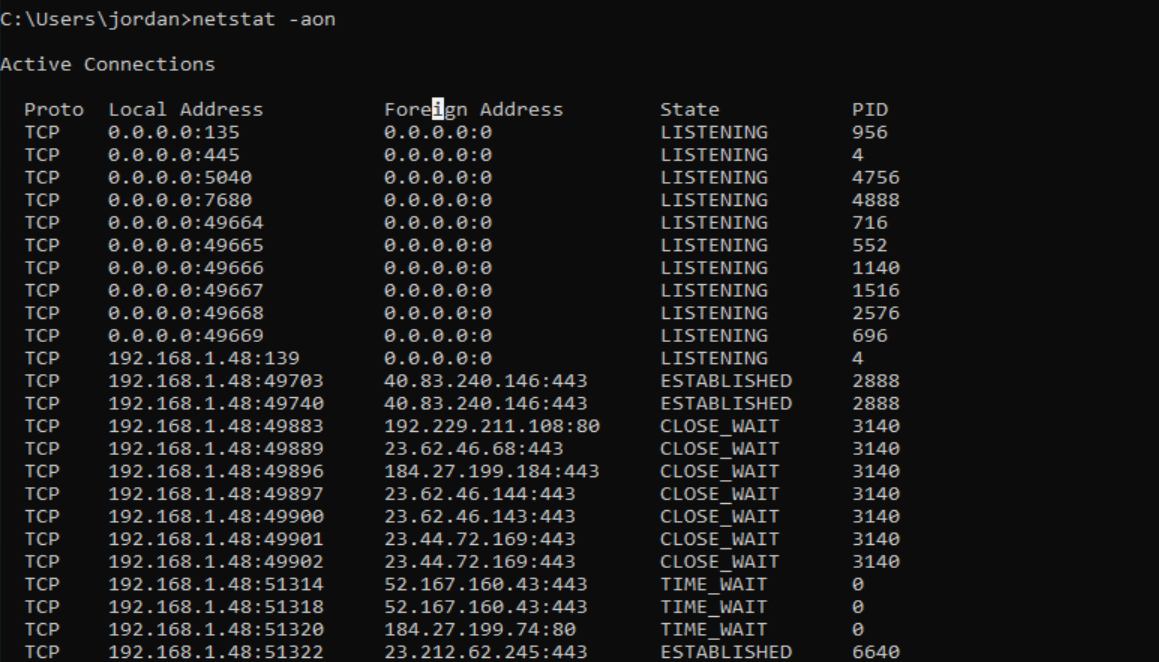


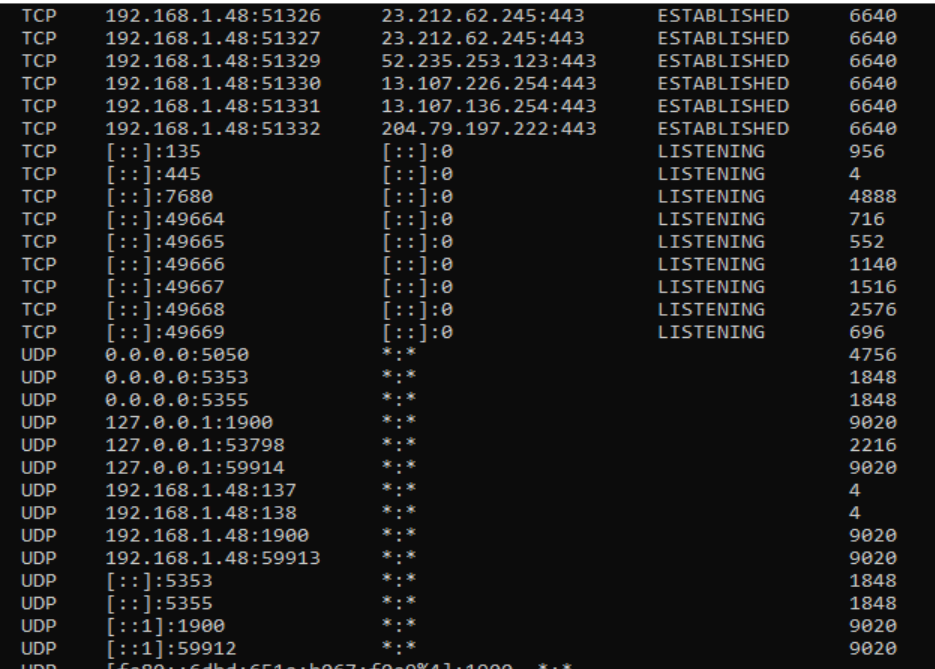
Windows tracert to yahoo.com





Nameserver lookup





We see port 135 is open which is Microsoft RPC (remote procedure call) service, it is used for allowing windows apps to communicate with each other over the network.

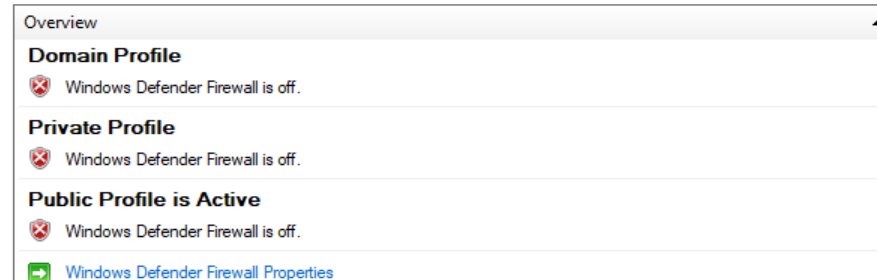
Port 445 is SMB (server message block) which allows file sharing and printer sharing

Port 5040 is used by microsoft forefront threat management gateway for secure web and network traffic filtering

Port 7680 is Delivery Optimization which is used for p2p sharing of apps and updates

Port 49664–49675 are just temp connections for short term connections like browsing

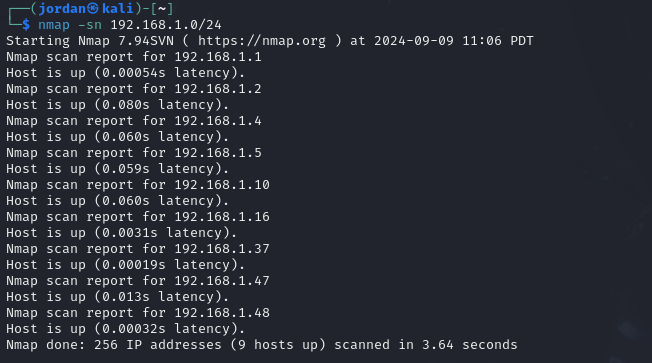
3.3 - Host and Service Discovery



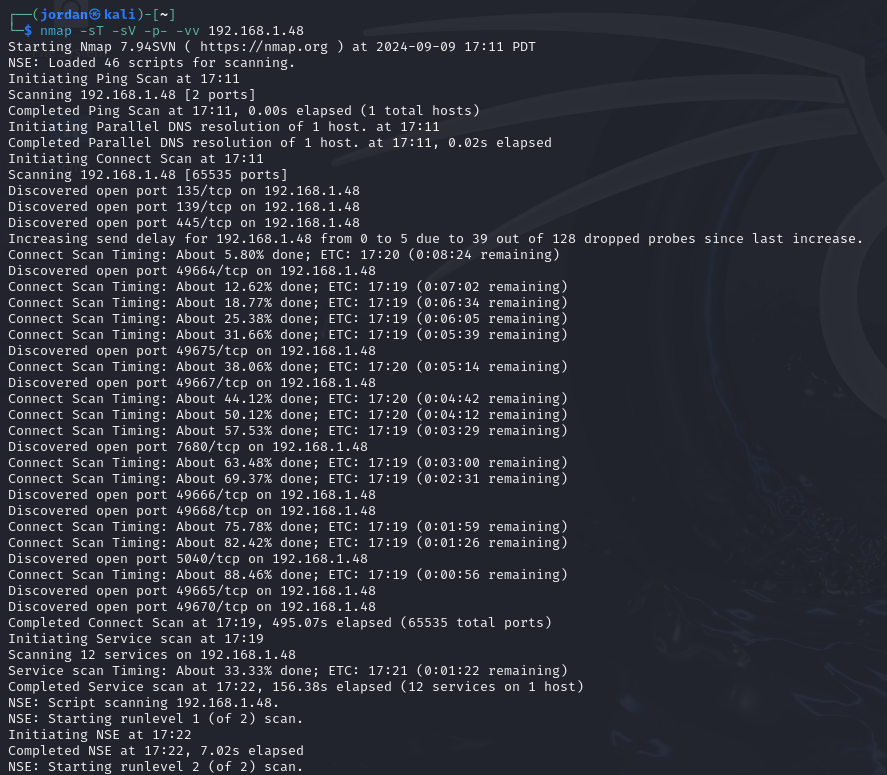
Disabling windows firewall

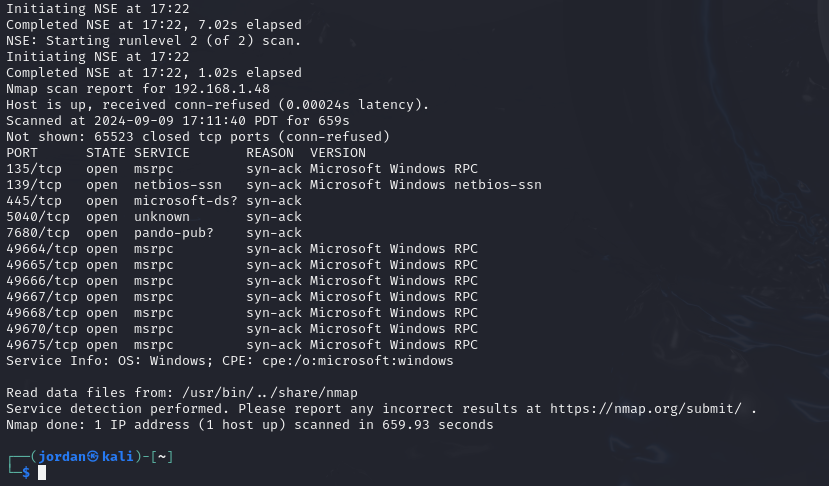
Kali: 192.168.1.37/24

Windows: 192.168.1.48/24



Found the windows IP in ping sweep 192.168.1.48

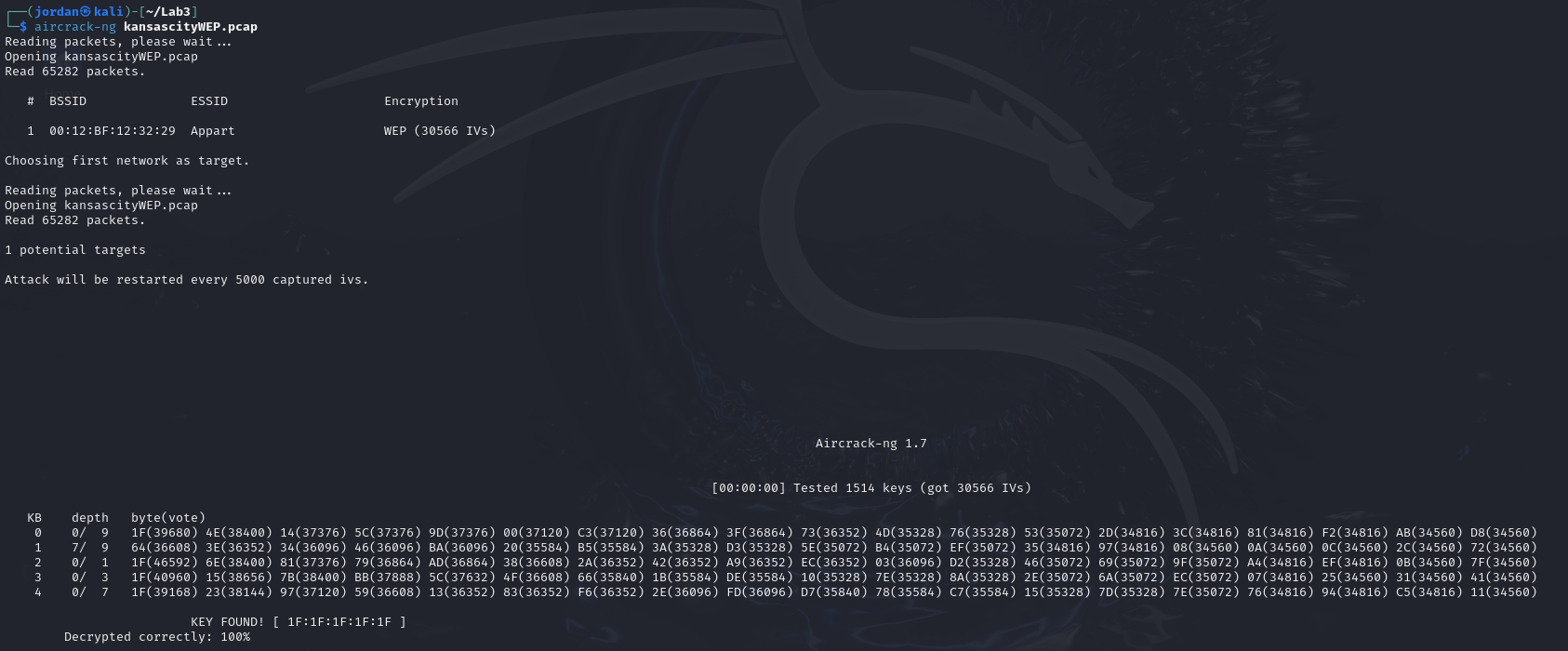




Nmapping the windows machine gave the above open ports.

3.4 - WIFI WEP Cracking

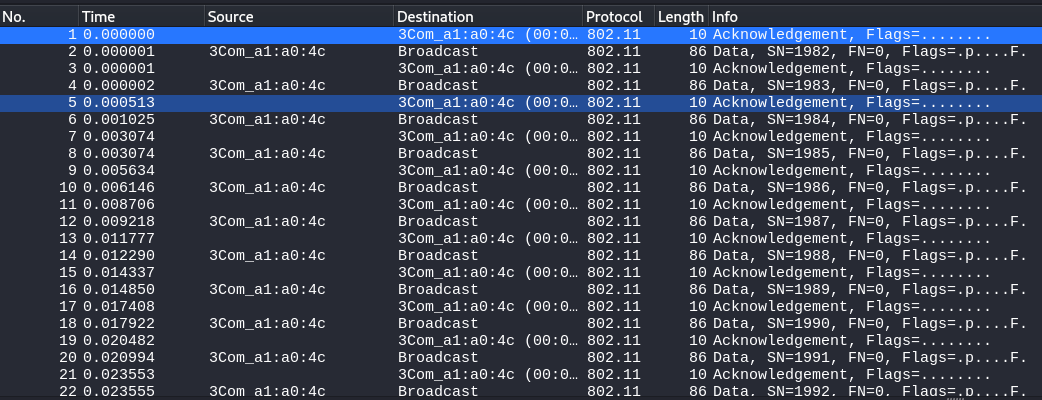
We will now be performing a crack on a WEP service



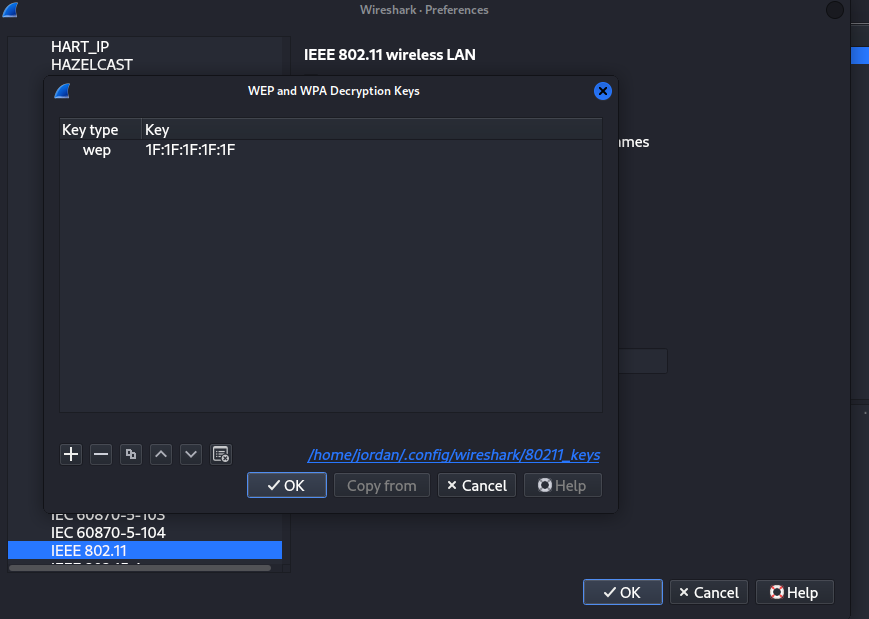
Used aircrack-ng kansascityWEP.pcap on pcap file to crack

KEY FOUND! [ 1F:1F:1F:1F:1F ]

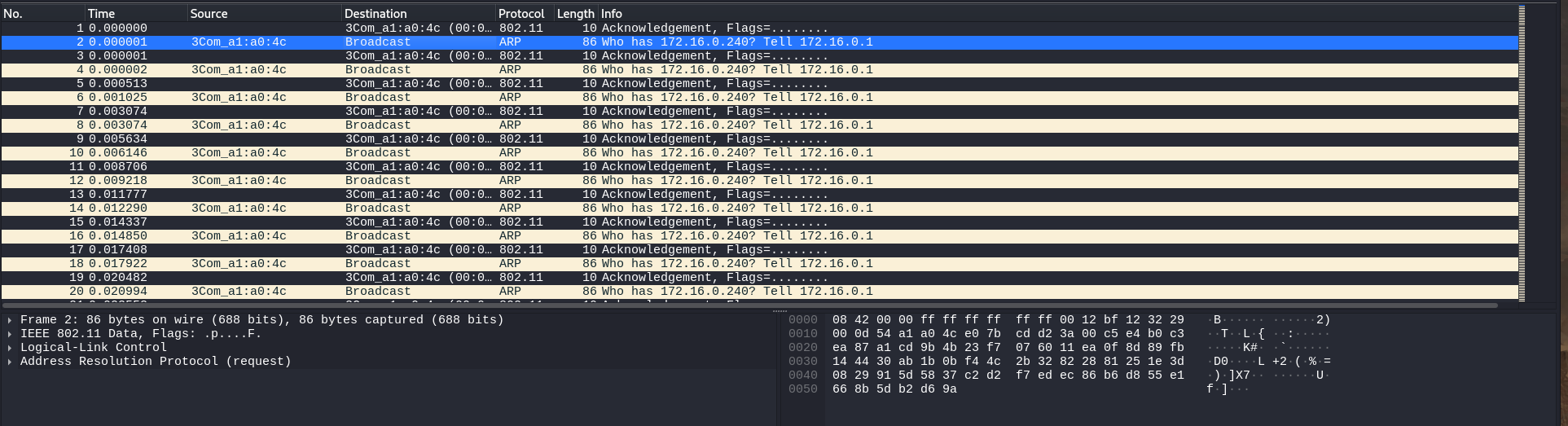
After opening the pcap file in wireshark,



We can see all of this encrypted traffic



Here, I added the key we found using the WEP crack tool



Now all of the traffic is decrypted!