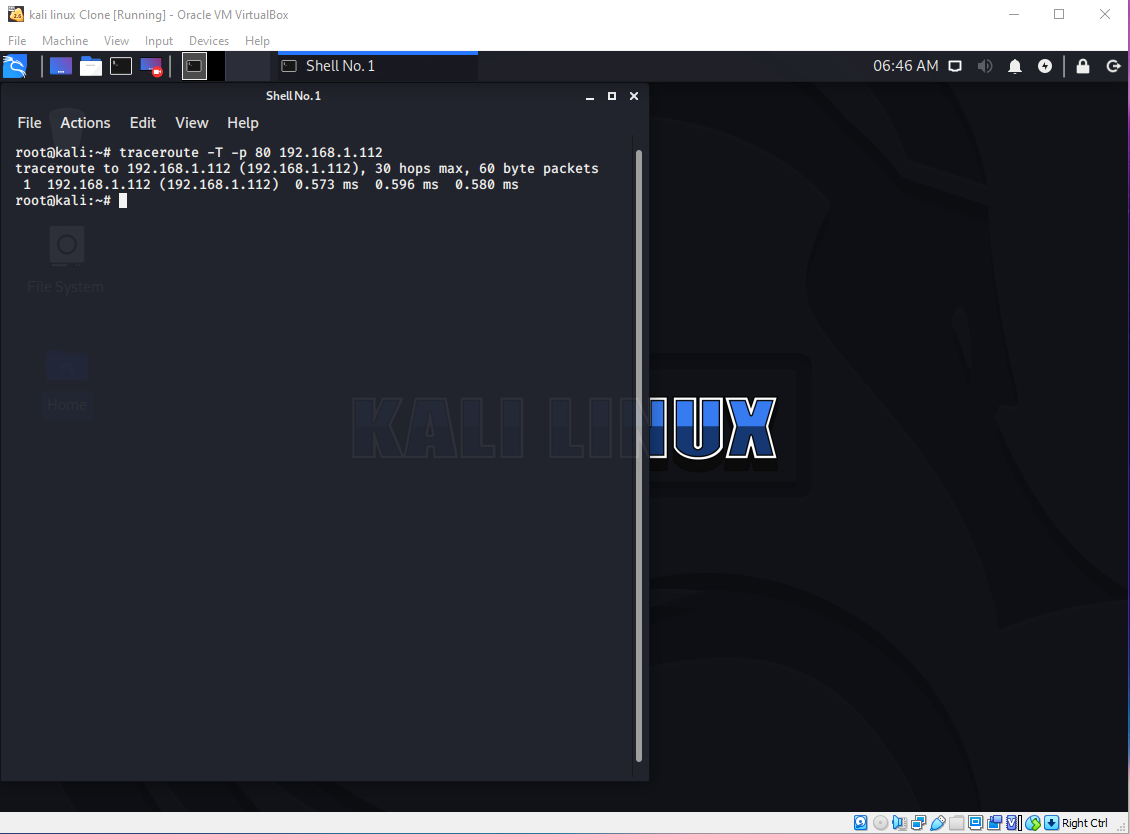
Setup your virtual machines. Add a network rule that blocks all traffic from internal network 1 to internal network 2 except for one port. Use traceroute to show this port is open and that there are no other hosts between your target and PFSense. You should submit the following.

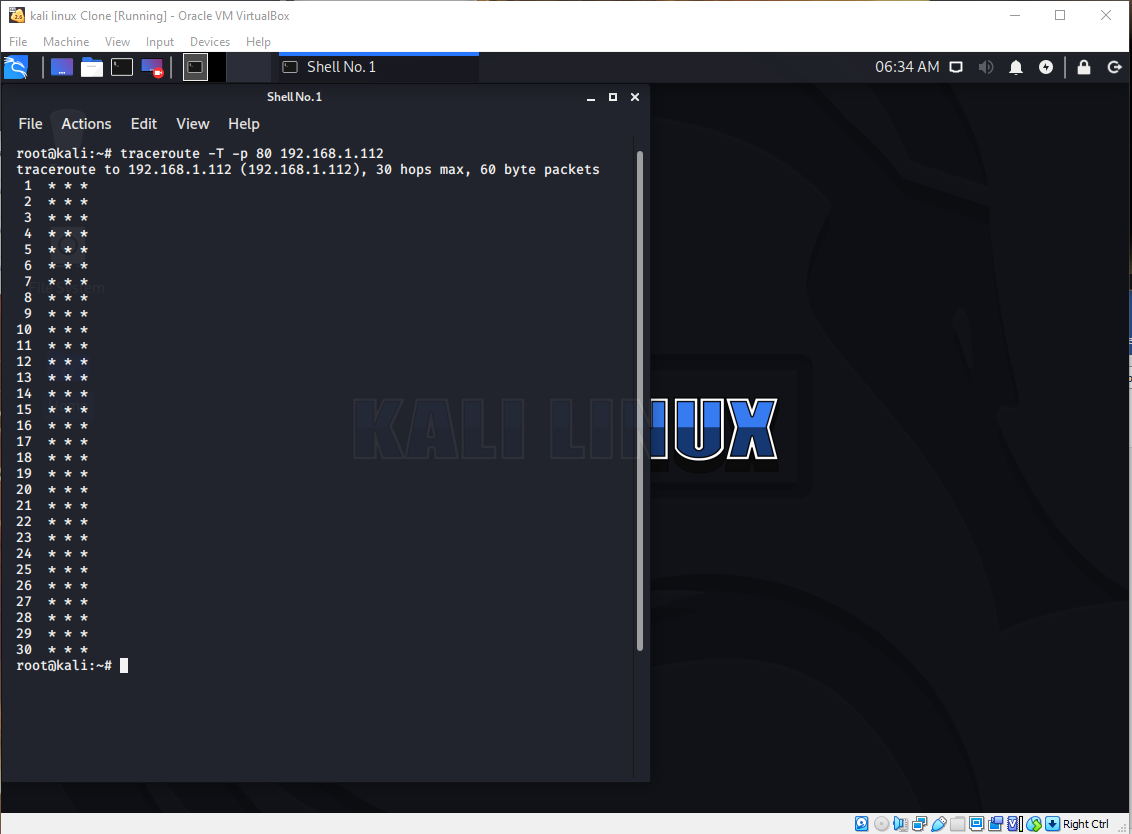
1. A screen shot showing what happens when you use traceroute to the target when the port is open vs when it is closed.

## Sub Task 1

TraceRoute command with port 80 open



TraceRoute command with port 80 closed



## Sub Task 2

Place your two Kali Machines on the same virtual network. Perform the following scans with nmap, while performing a packet capture between the two. Submit the following.

1. A short explanation of each of the following scans, explaining the differences, when you would use them, and referencing the packet capture to illustrate your point.
2. Full Connect
3. Syn Scan
4. Xmas Scan

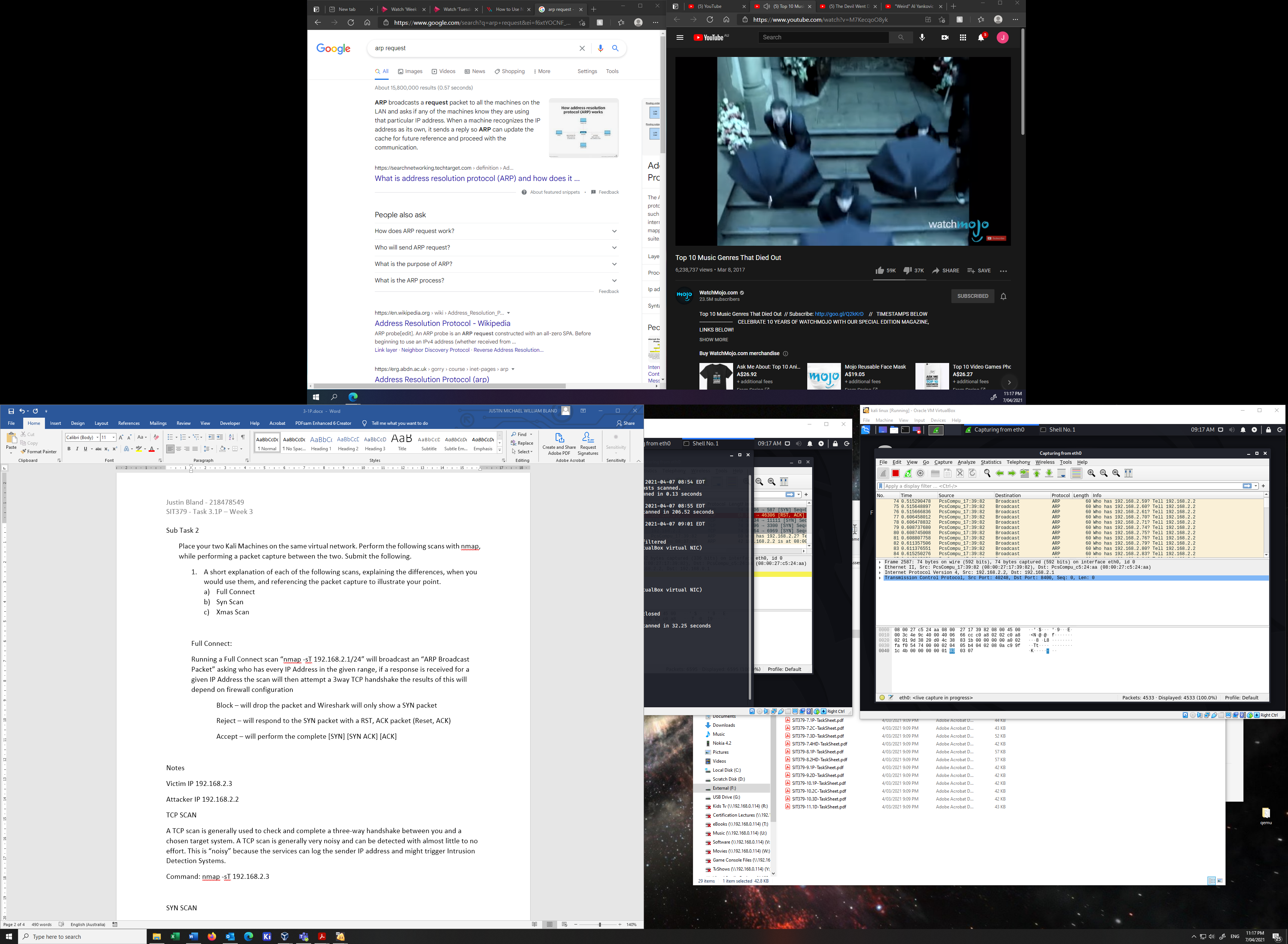
**Full Connect:**

Running a Full Connect scan “nmap -sT 192.168.2.1/24” will broadcast an “ARP Broadcast Packet” asking who has every IP Address in the given range, if a response is received for a given IP Address the scan will then attempt a 3way TCP handshake the results of this will depend on firewall configuration

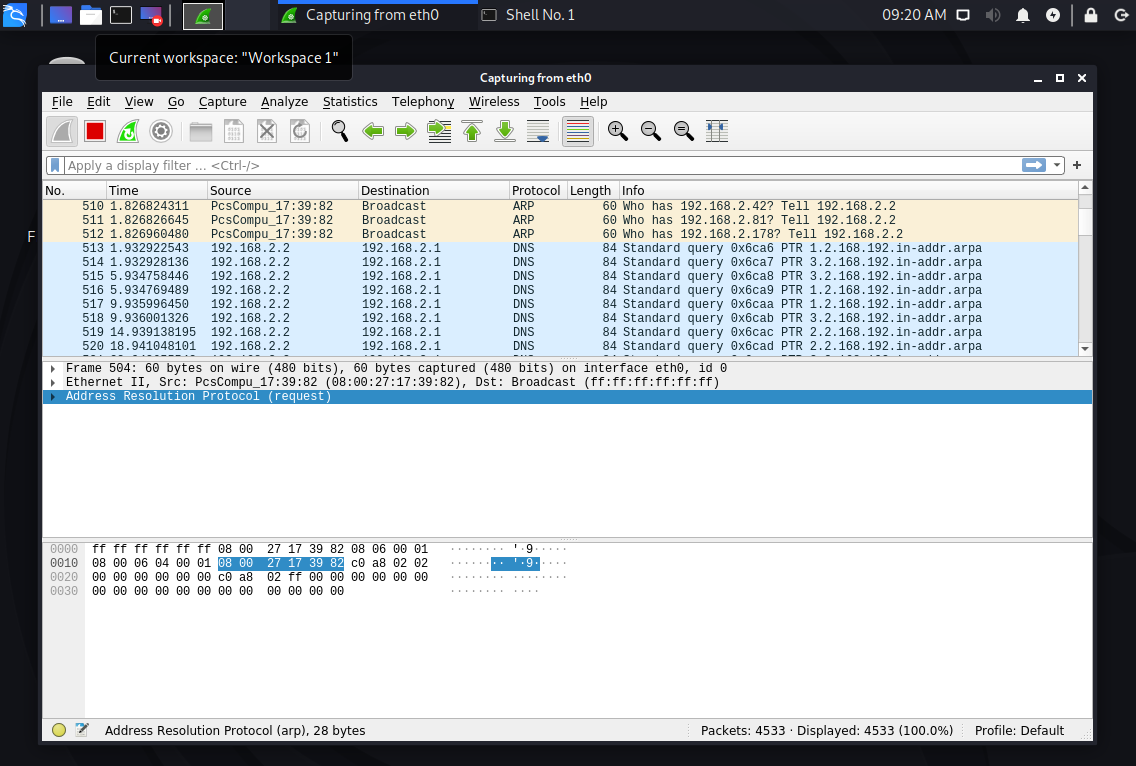
Block – will drop the packet and Wireshark will only show a SYN packet

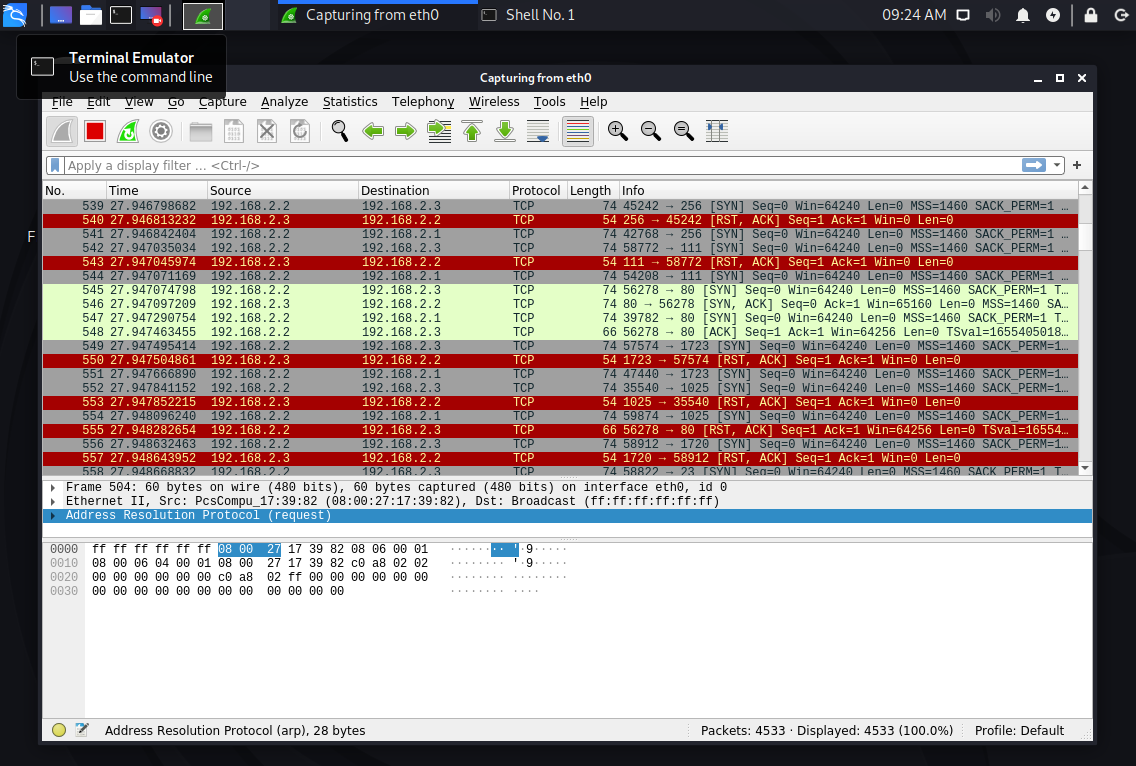
Reject – will respond to the SYN packet with a RST, ACK packet (Reset, ACK)

Accept – will perform the complete [SYN] [SYN ACK] [ACK]



ARP Broadcasts

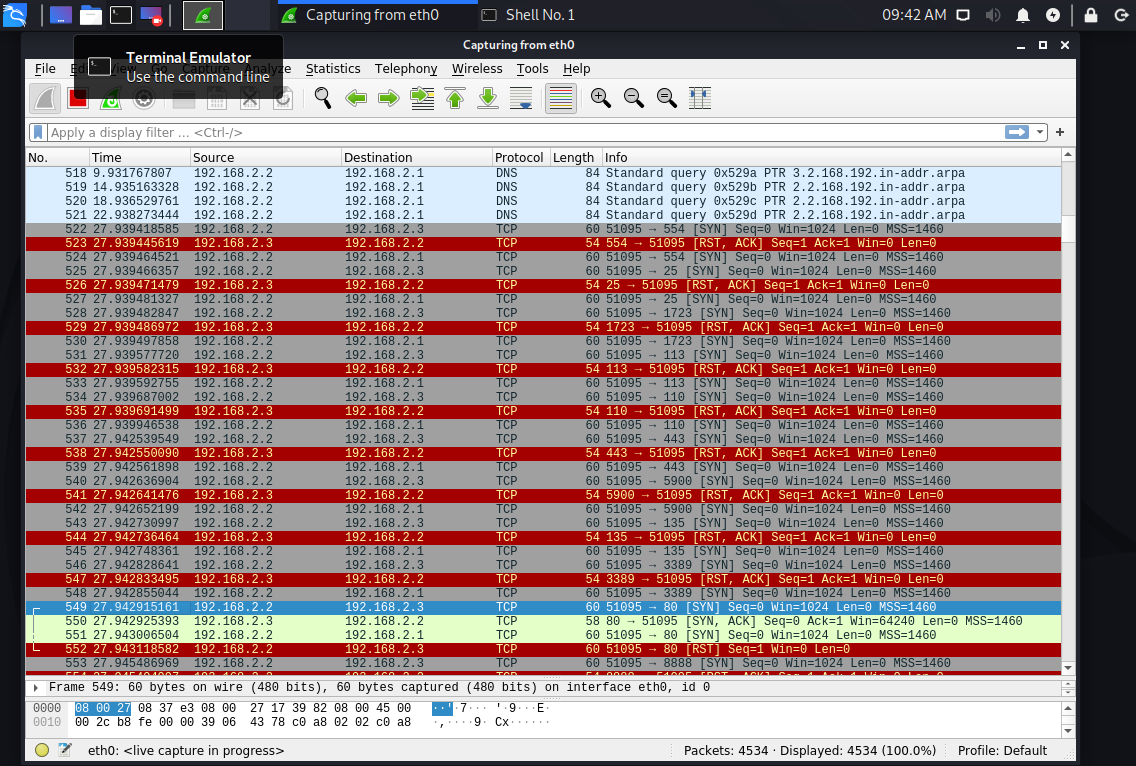


ARP Broadcast Response

TCP 3-Way Handshake

**SYN Scan:**

Running a Full Connect scan “nmap -sS 192.168.2.1/24” for the most part will be the same as the Full Connect Scan, with the exception that during the TCP 3-Way Handshake the connection is never formed, rather Nmap analyses the [SYN ACK] response to produce the results of the scan.



**SYN Scan:**

Running a Full Connect scan “nmap -sX 192.168.2.1/24” starts with an ARP broadcast just as the previous scans then probes the ports of the found IP-Addresses with an unusual packet where the [PSH], [URG], [FIN] flags in the header manipulated, in general due to the way the TCP stack is implemented in the Windows Operating System it is unlikely that this scan will produce usable results on a Windows system.

