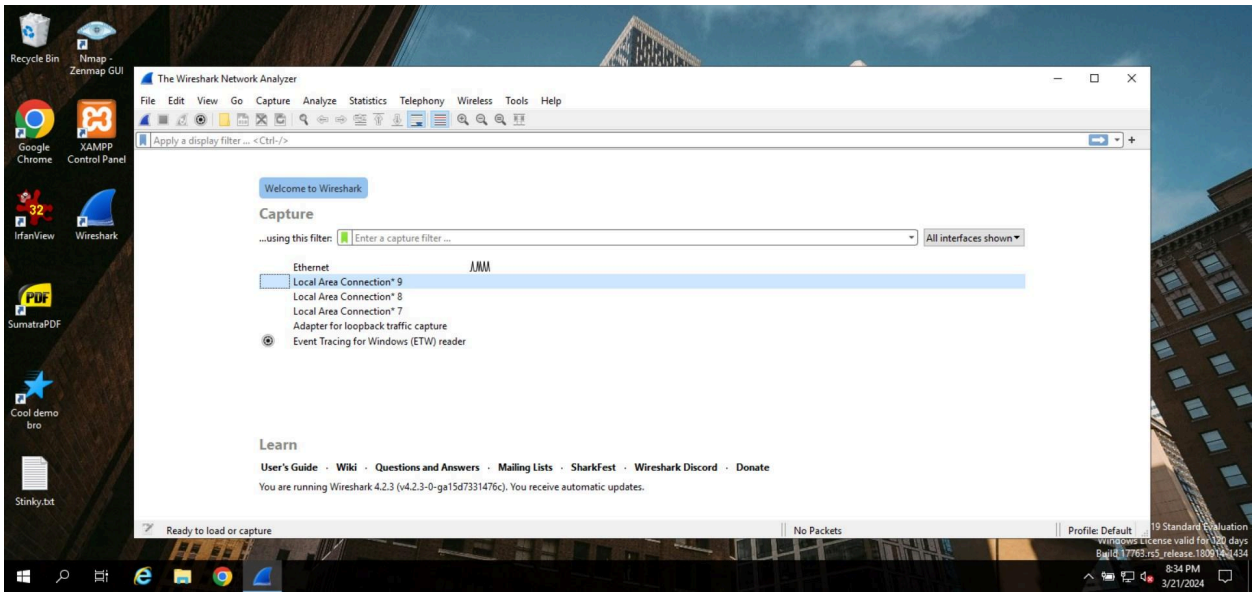
Name: Cristian Barreno

Capturing Packets with Wireshark

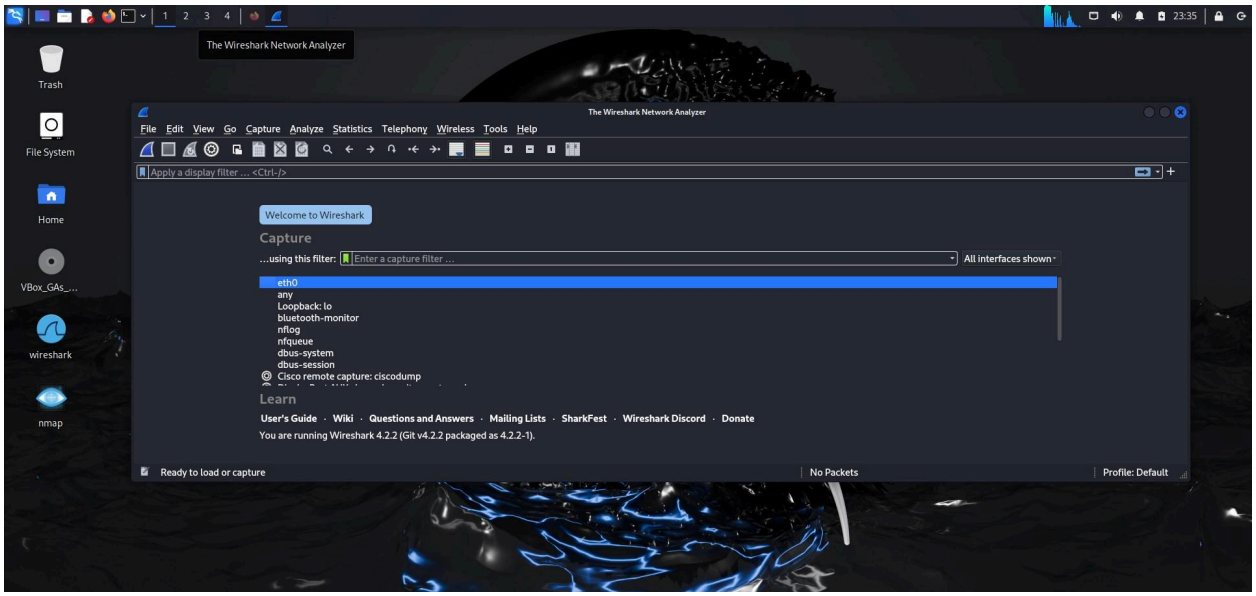
Lab Exercise

I installed Wireshark in both Windows and Linux. Below I posted the screenshots. I also installed nmap and apache.

Wireshark installed in Windows 19

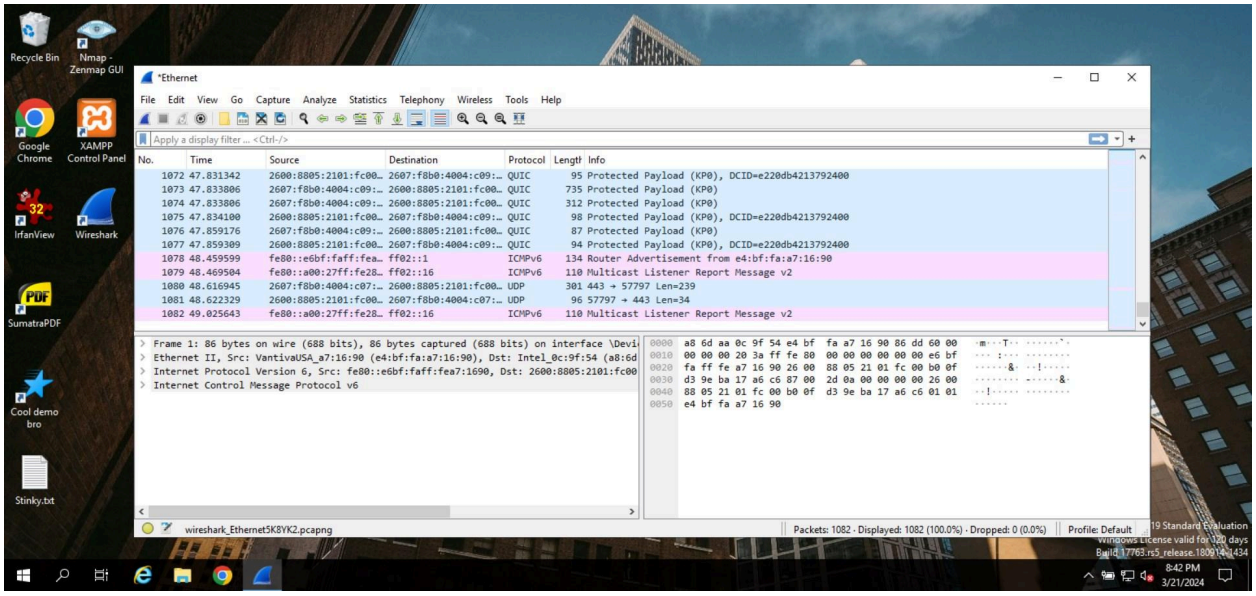


Wireshark installed in Kali Linux

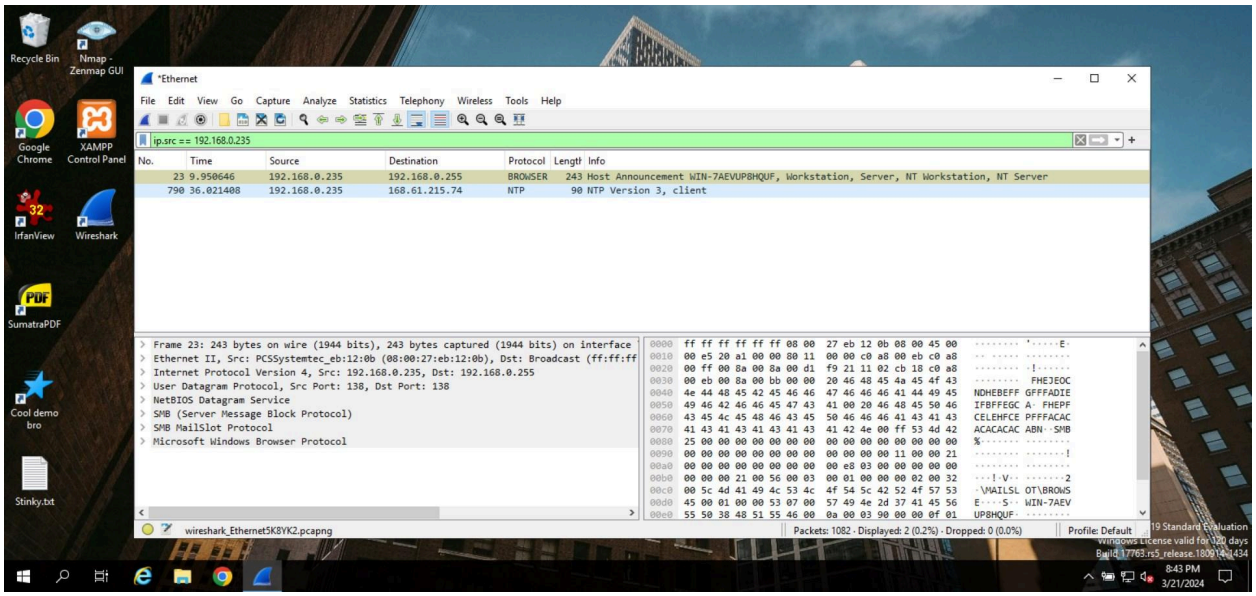


To filter and analyze the captured packets, use Wireshark's display filters.

On my Windows 19 server I opened wireshark, then I clicked on ethernet, then I clicked on the blue fin to start capturing packets. After you collected enough packets, I clicked the red stop button.

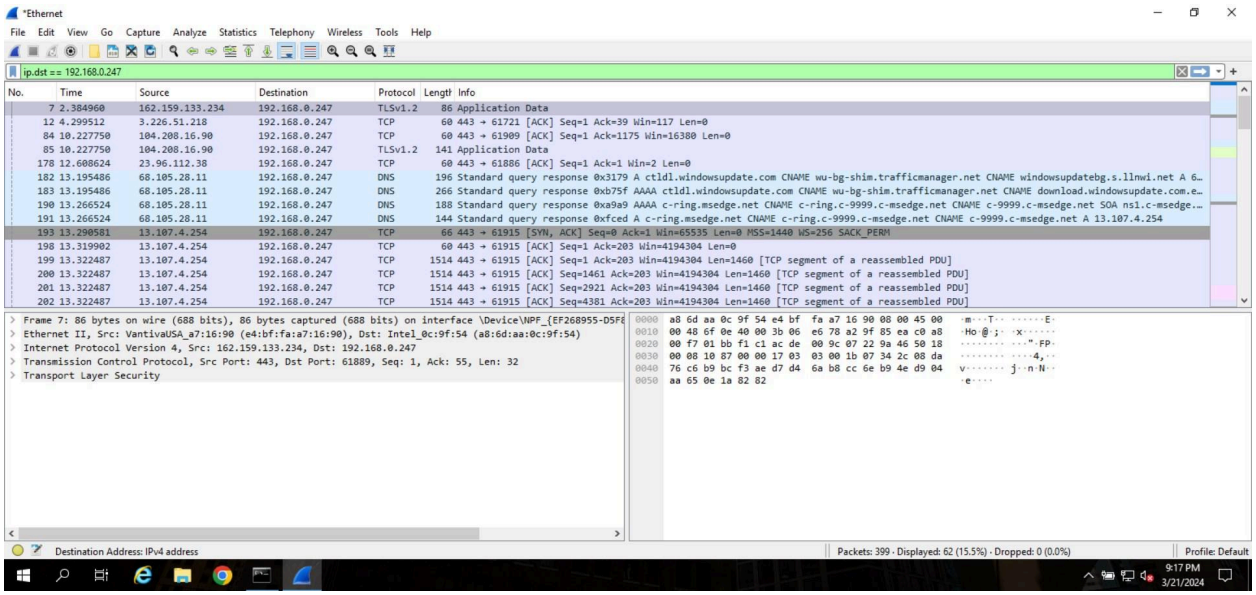


To filter by source IP address: ip.src == 192.168.X.X (your scanner IP)



I entered ip.src == followed by the IPV4 address of my windows 19 server. Inside the big white box in the middle I can see different packets that I captured.

To filter by destination IP address: ip.dst == 192.168.X.X (your target IP)

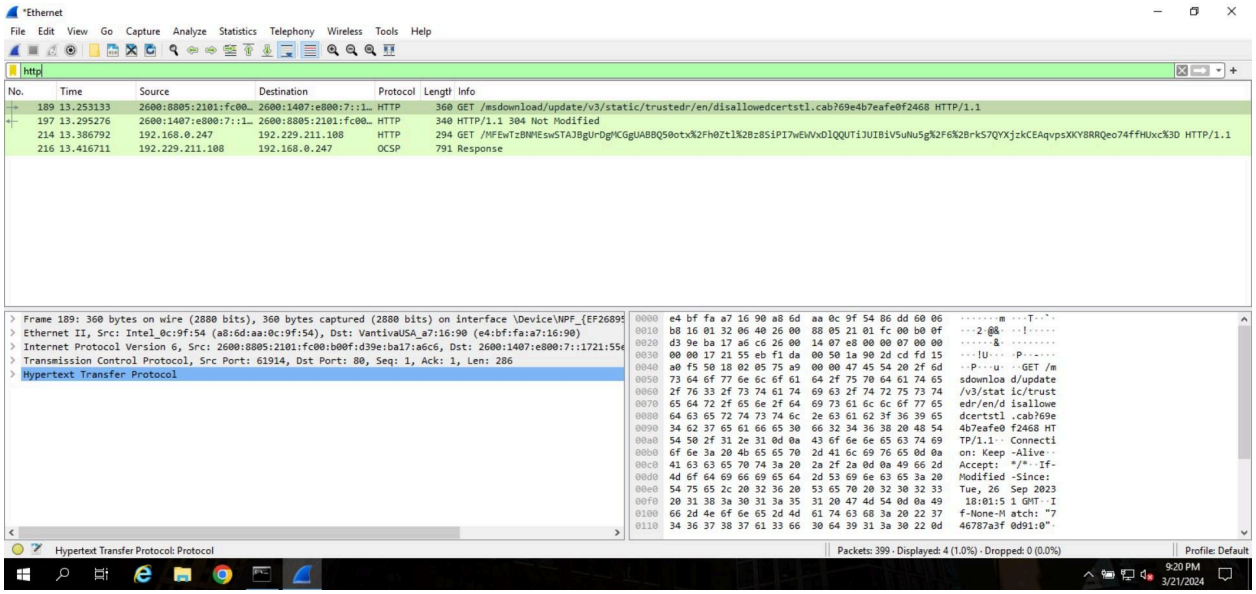


In the screenshot above I entered ip.dst == followed by the destination IP. Wireshark filtered it and populated it in the middle big white box.

To filter by specific protocol: http, arp, dns

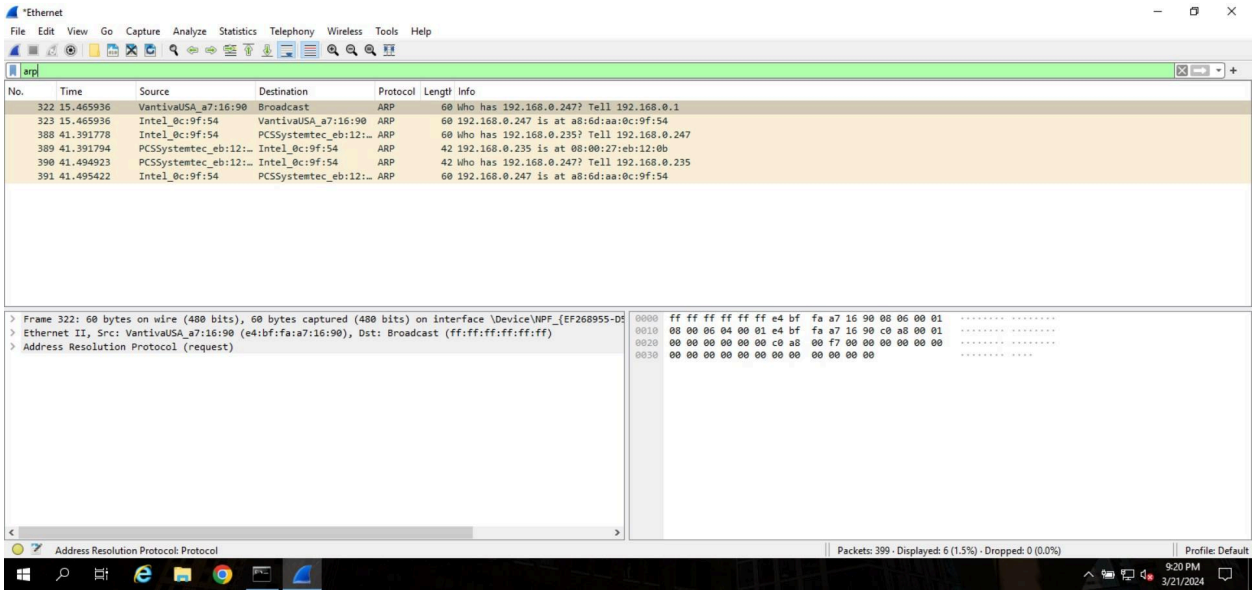
HTTP

HTTP stands for hypertext transfer protocol. HTTPs port is port 80

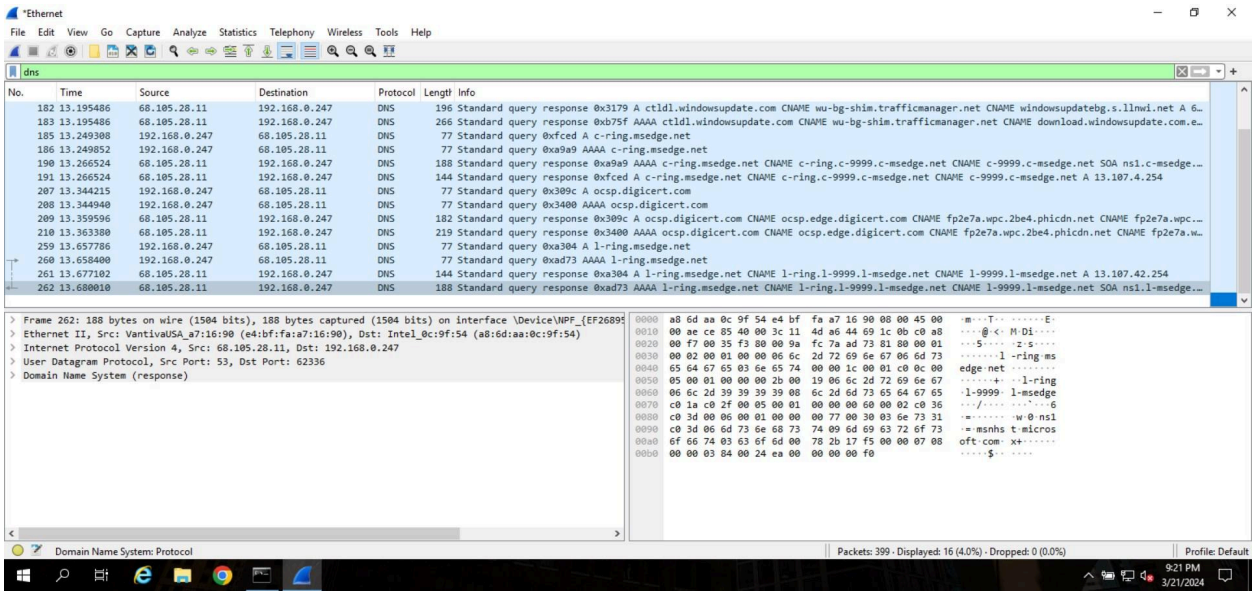


ARP

ARP stands for address resolution protocol



DNS
DNS stands for domain name system. Port 53



BONUS – Run the advanced command to search for http services specifically. To do this you will need to install XAMPP and make sure Apache is running.

Once installed, run the Start packet capture then run the following command
“nmap –script http-title –sV –p80 192.168.0.2”.Then apply filters for “http” and look for information about the web service.