

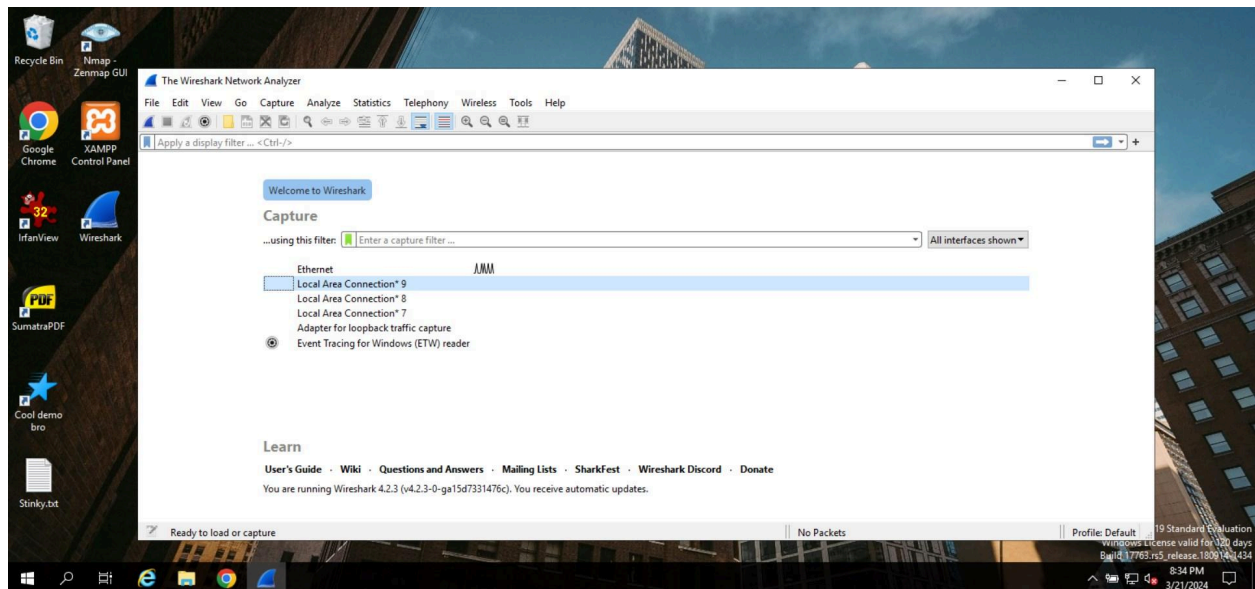
Name: Cristian Barreno

Capturing Packets with Wireshark

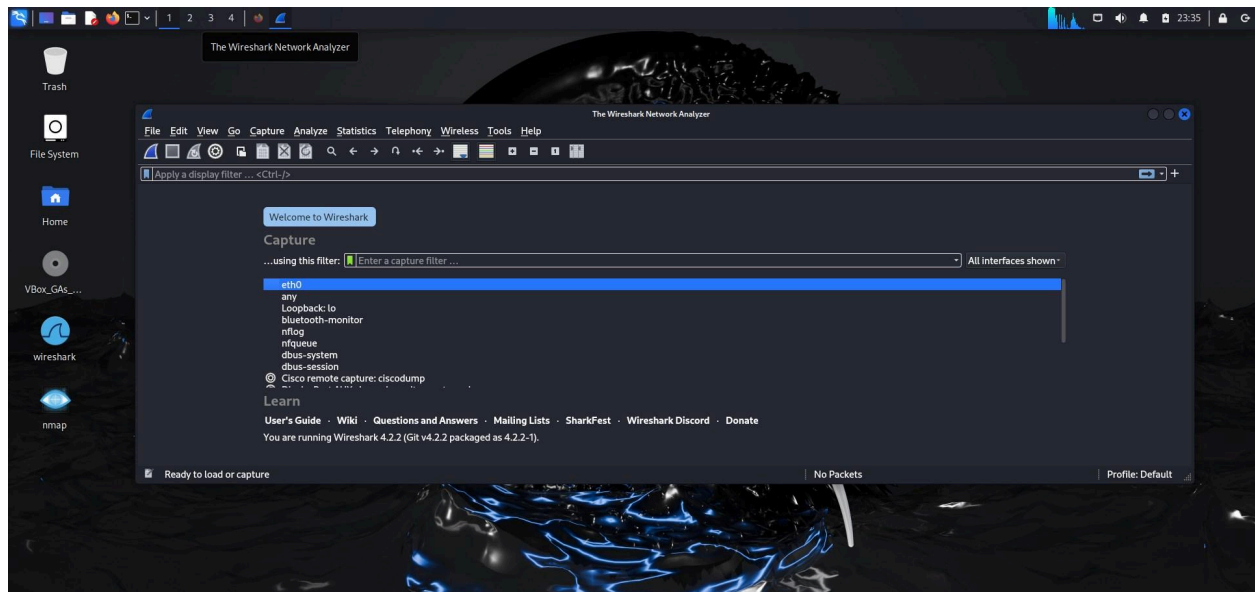
Lab Exercise

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

Wireshark installed in Windows 19

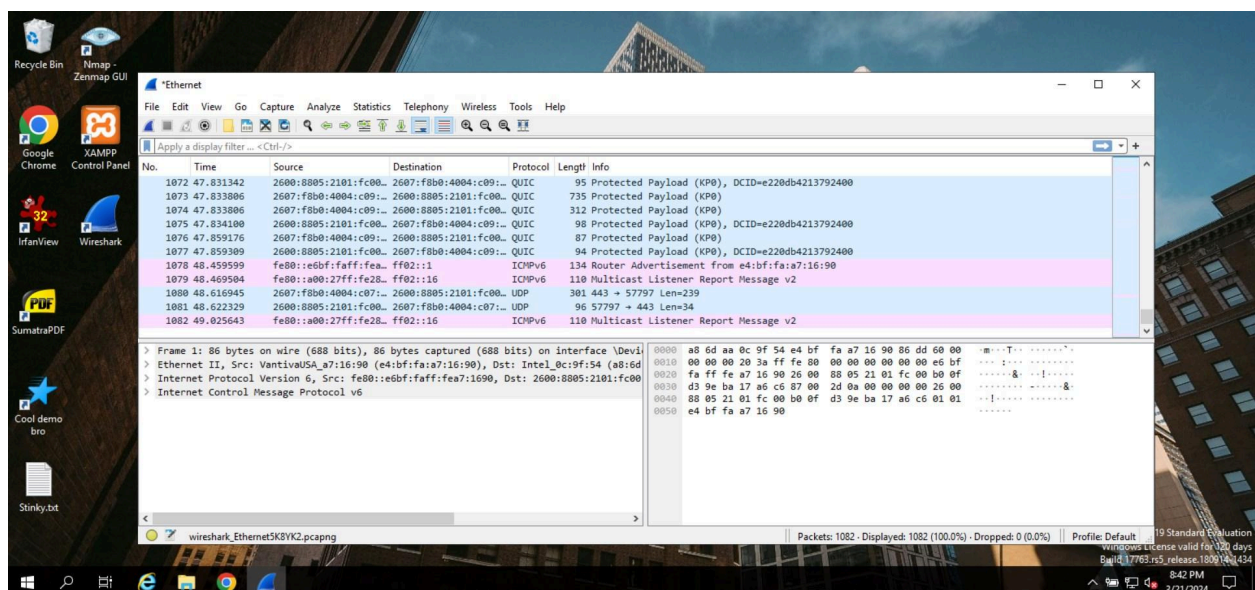


Wireshark installed in Kali Linux

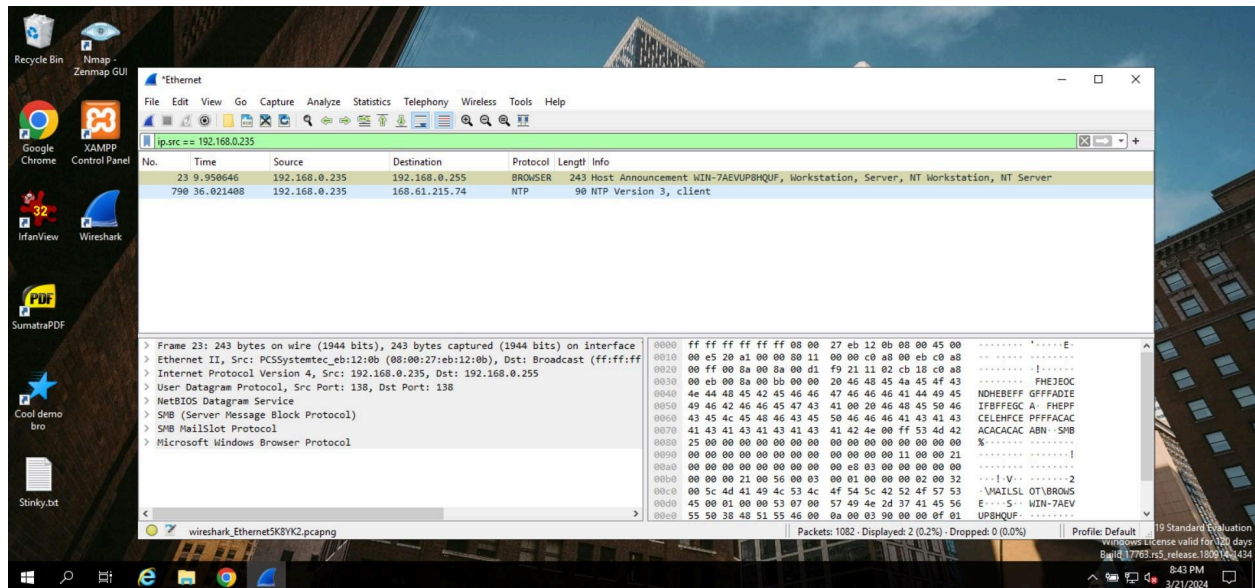


To filter and analyze the captured packets, use Wireshark's display filters.

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.

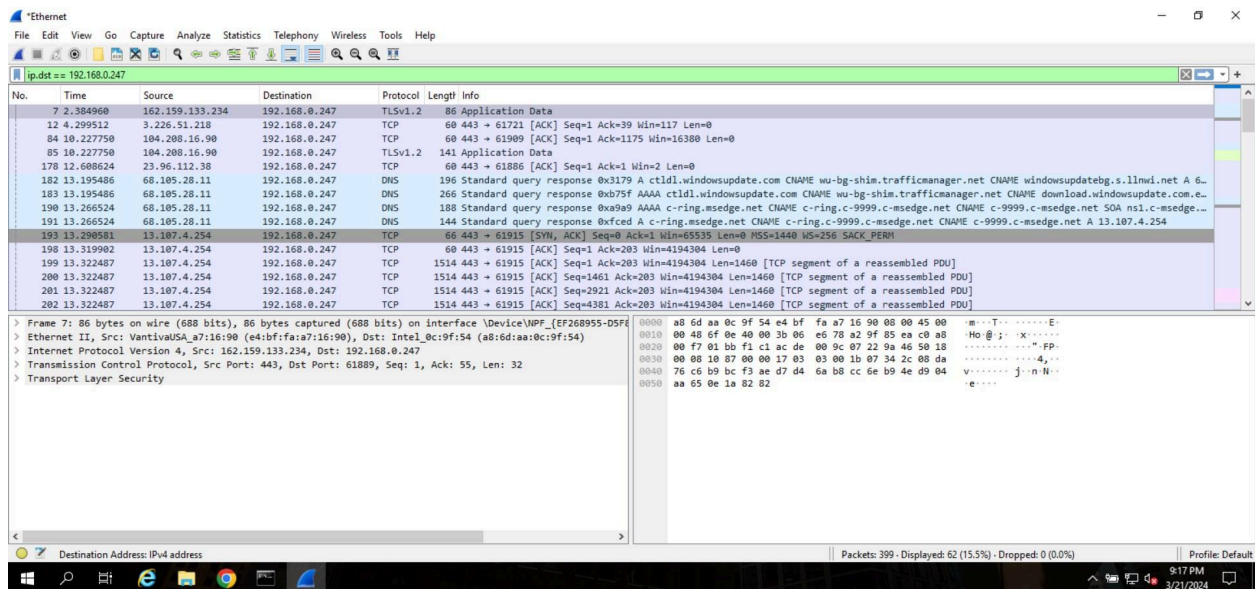


To filter by source IP address: `ip.src == 192.168.X.X` (your scanner IP)



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

The image shows a Wireshark packet capture of an HTTP transaction. The packet list pane shows four packets: a GET request (No. 189), a 304 Not Modified response (No. 197), a TCP reset (No. 214), and an OCSP response (No. 216). The selected packet (No. 189) is expanded to show the Hypertext Transfer Protocol details. The raw packet data pane shows the hexadecimal and ASCII representation of the packet bytes.

No.	Time	Source	Destination	Protocol	Length	Info
189	13.253133	2600:8805:2101:fc00::...	2600:1407:e800:7:1::...	HTTP	360	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?69e4b7eafe0f2468 HTTP/1.1
197	13.295276	2600:1407:e800:7:1::...	2600:8805:2101:fc00::...	HTTP	340	HTTP/1.1 304 Not Modified
214	13.386792	192.168.0.247	192.229.211.108	HTTP	294	/NFewT:BNHeswSTA3gUrDg/KCGuAB8Q50otxk2Fh0Zt1k28:85IP17wEWxdlQUt13UIB1V5ulu5gk2f6X28rk57QYXj:KCEAqpsXKY8RRQeo74ffHuxcX3D HTTP/1.1
216	13.416711	192.229.211.108	192.168.0.247	OCSP	791	Response

Frame 189: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF_{EF268955-D5} Ethernet II, Src: Intel_0c:9f:54 (a8:6d:aa:0c:9f:54), Dst: VantivaUSA_a7:16:90 (e4:bf:fa:a7:16:90)
Internet Protocol Version 6, Src: 2600:8805:2101:fc00:b00f:d39e:ba17:a6c6, Dst: 2600:1407:e800:7:1:221:554
Transmission Control Protocol, Src Port: 61914, Dst Port: 80, Seq: 1, Ack: 1, Len: 286
Hypertext Transfer Protocol

0000 e4 bf fa a7 16 90 a8 6d aa 0c 9f 54 86 dd 60 06m...T...
0010 b8 16 01 32 06 40 26 00 88 05 21 01 fc 00 b0 0f ...2 88...
0020 d3 9e ba 17 a6 c6 26 00 14 07 e8 00 00 07 00 00 ...&...
0030 00 00 17 21 55 eb f1 da 00 50 1a 90 2d cd fd 15 ...U...P...
0040 a0 f5 50 18 02 05 75 a9 00 00 47 45 54 20 2f 6d ...P...u...GET /m
0050 73 64 6f 77 6e 6c 6f 61 64 2f 75 70 64 61 74 65 sdownload/update
0060 2f 76 33 2f 73 74 61 74 69 63 2f 74 72 75 73 74 /v3/stat ic/trust
0070 65 64 72 2f 65 6e 2f 64 69 73 61 6c 6c 6f 77 65 edr/en/disallow
0080 64 63 65 72 74 73 74 6c 2e 63 61 62 3f 36 39 65 dcertstl.cab?69e
0090 34 62 37 65 61 66 65 30 66 32 34 36 38 20 48 54 4b7eafe0 f2468 HT
00a0 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 TP/1.1... Connecti
00b0 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a on: Keep-Alive
00c0 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 49 66 2d Accept: */*...if:
00d0 4d 6f 64 69 66 69 65 64 2d 53 69 6e 63 65 3a 20 Modified-Since:
00e0 54 75 65 2c 20 32 36 20 53 65 70 20 32 30 32 33 Tue, 26 Sep 2023
00f0 20 31 38 3a 30 31 3a 35 31 20 47 4d 54 0d 0a 49 18:01:5 1 GMT...I
0100 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a 20 22 37 f-None-N atch: "7
0110 34 36 37 38 37 61 33 66 30 64 39 31 3a 30 22 0d 46787a3f fd01:0"

ARP

ARP stands for address resolution protocol

The image shows a Wireshark packet capture of an ARP request. The packet list pane shows five packets: two ARP requests (Nos. 322 and 323), and three ARP responses (Nos. 388, 389, and 390). The selected packet (No. 322) is expanded to show the Address Resolution Protocol details. The raw packet data pane shows the hexadecimal and ASCII representation of the packet bytes.

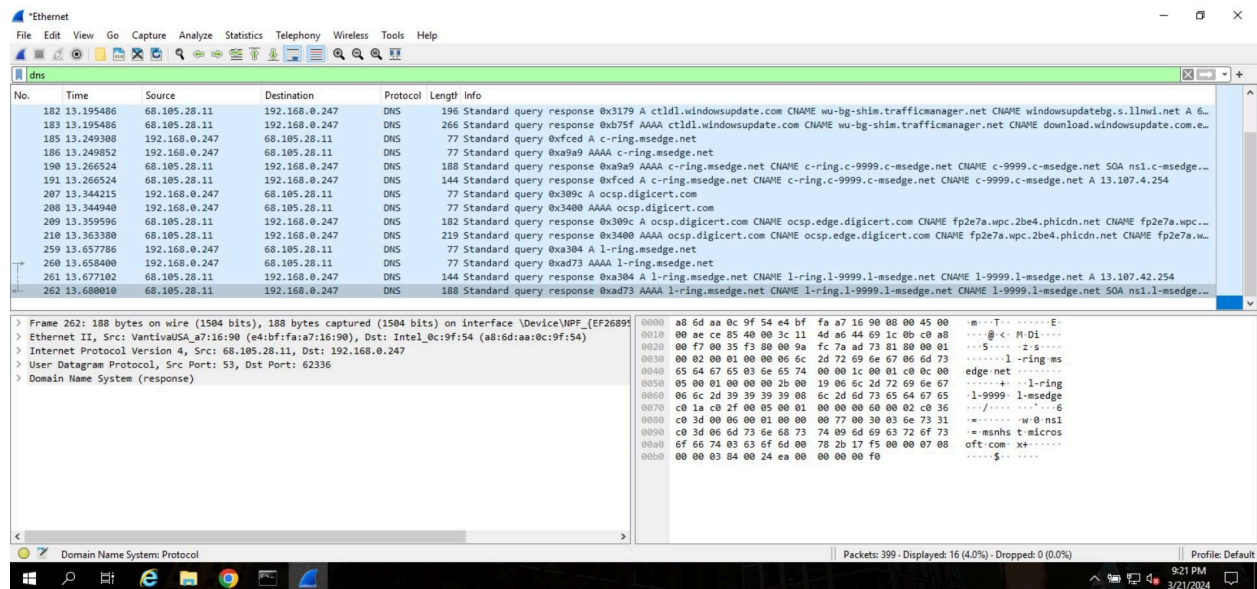
No.	Time	Source	Destination	Protocol	Length	Info
322	15.465936	VantivaUSA_a7:16:90	Broadcast	ARP	60	who has 192.168.0.247? Tell 192.168.0.1
323	15.465936	Intel_0c:9f:54	VantivaUSA_a7:16:90	ARP	60	192.168.0.247 is at a8:6d:aa:0c:9f:54
388	41.391778	Intel_0c:9f:54	PCSSystemtec_eb:12:...	ARP	60	who has 192.168.0.235? Tell 192.168.0.247
389	41.391794	PCSSystemtec_eb:12:...	Intel_0c:9f:54	ARP	42	192.168.0.235 is at 00:00:27:eb:12:00
390	41.494923	PCSSystemtec_eb:12:...	Intel_0c:9f:54	ARP	42	who has 192.168.0.247? Tell 192.168.0.235
391	41.495422	Intel_0c:9f:54	PCSSystemtec_eb:12:...	ARP	60	192.168.0.247 is at a8:6d:aa:0c:9f:54

Frame 322: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{EF268955-D5} Ethernet II, Src: VantivaUSA_a7:16:90 (e4:bf:fa:a7:16:90), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff e4 bf fa a7 16 90 08 06 00 01
0010 08 00 06 04 00 01 e4 bf fa a7 16 90 c0 a8 00 01
0020 00 00 00 00 00 c0 a8 00 f7 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0120 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0150 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0160 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0180 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0190 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
01f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0200 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0210 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0230 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0240 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0250 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0260 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0270 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0280 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0290 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
02f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0300 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0310 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0320 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0330 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0340 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0350 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0360 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0370 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0380 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0390 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
03f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0400 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0410 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0420 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0430 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0440 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0450 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0460 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0470 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0480 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0490 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
04f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0500 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0510 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0520 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0530 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0540 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0550 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0560 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0570 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0580 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0590 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0600 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0610 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0620 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0630 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0640 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0650 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0660 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0670 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0680 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0690 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
06f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0700 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0710 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0720 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0730 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0740 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0750 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0760 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0770 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0780 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0790 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
07f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0800 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0810 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0820 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0830 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0840 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0850 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0860 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0870 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0880 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0890 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
08f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0900 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0910 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0920 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0930 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0940 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0950 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0960 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0970 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0980 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0990 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
09f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a10 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a30 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a50 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a60 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a70 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0a90 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0aa0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ab0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ac0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ad0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0ae0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0af0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b10 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b30 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b50 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b60 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b70 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0b90 00 00

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.

