

Q1) What is the purpose of using filter in Wireshark?

Ans: Filters helps you focus on specific types of network traffic, making it easier to analyze and troubleshoot issue without being overwhelmed by all the data.

Q2) Which network interface did you use for capturing packets? Why?

Ans: You would typically use the network interface that is connected to the internet or the local network you want to analyze. This allows you to capture relevant traffic.

Q3) Name at least 3 different protocols you observed during the capture.

→ Common protocols you might observe include

- HTTP (for web traffic)
- DNS (for domain name resolution)
- TCP (for reliable data transmission)

Q4) What is the IP address for your system (Source IP)?

Ans: You can find your system's IP address in Wireshark by looking at the source IP of any particular packet capture. It usually starts with "192.168." or "10.x" for local network.

Q5) What is one destination IP you communicate with during the capture?

Looks for any packet where your system's IP is the source. The destination IP will be the address.

of the server or device you communicate with
(eg: a website's IP)

6) Find a DNS query in your capture. What domain name was being looked up?

Ans Look for ipackets with the DNS protocol. You can find a query that shows a domain name like "example.com" being looked up.

Q7) Pick one HTTP packets and describe its source . . .

Ans Select an HTTP packets and check the details. The source IP is your system's IP, the destination IP is the web server's IP, and most the most Host name is usually found in the HTTP header.

Eg: "Host : www.example.com"):

Q8) Which filter showed the most traffic? why do you think that is ?

Ans The HTTP filter often shows the most traffic because web browsing generates a lot of request and responses. Many user access website frequently leading to high HTTP traffic.

Q9) Did you observe any encrypted traffic . . . ?

Ans Yes, you can tell if traffic is encrypted by looking for packets with the "TLS" or "SSL" protocol. These packet usually indicate secure connections, like HTTPS website.

10) What's the difference between 'ip.addr == x.x.x.x' and 'ip.src == x.x.x.x'?

$ip\cdot addr == x\cdot x\cdot x\cdot x$: This filter shows packets where the IP address is e.g either the source or destination.

$ip\cdot src == x\cdot x\cdot x\cdot x$: This filter shows only packets where the IP address is the source

11) FIND a TCP handshake (SYN, SYN-ACK, ACK)

→ A TCP handshake involves three steps:

1. SYN : your system sends a SYN packet to initiate a connection.
2. SYN - ACK : The server responds with a SYN-ACK packet to acknowledge the request.
3. ACK : your system sends an ACK packet to confirm the connection is established.

12) What's one interesting thing you noticed in your network traffic?

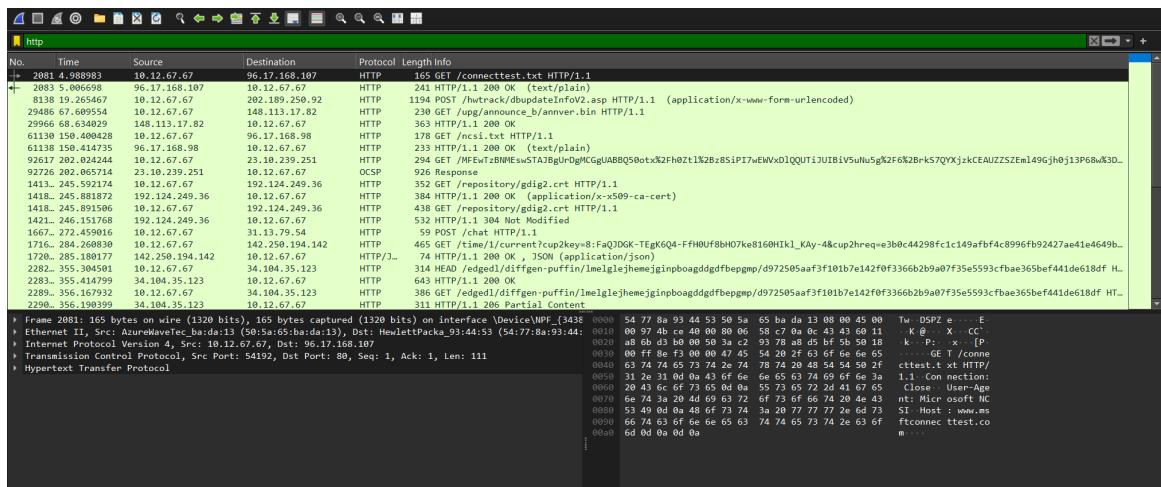
→ You might notice unusual traffic patterns such as a high number of DNS queries, unexpected IP addresses communicating with your system, or a lot of encrypted traffic, which could indicate secure browsing or potential security concerns.

Assignment-12

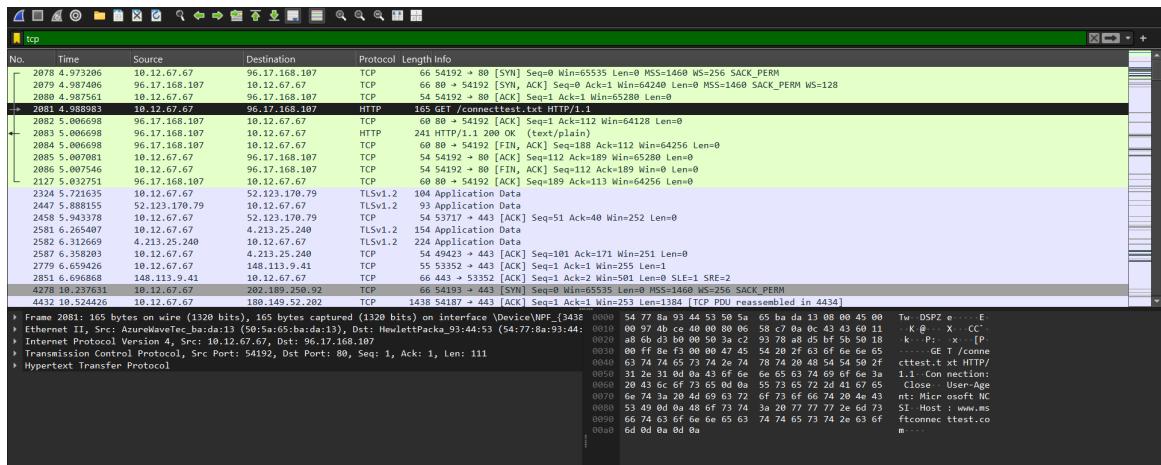
Wireshark display filters :-

1. Protocol-Based Filters

- http – Shows only HTTP traffic



- tcp – Displays only TCP packets



- udp – Displays only UDP packets

No.	Time	Source	Destination	Protocol	Length Info
2061 4.849059	fe80::1:50:9d1:3d8c::ff02::fb	MDNS	156 Standard query 0x0000 TXT Saranya's MacBook Air._companion-link._tcp.local, "QU" question TXT ANKIT's MacBook Air._companion-link._tcp.local, "QU" question TXT Mayank's MacBook Pro (2)._companion-link._tcp.local TXT TXT, cache flush AAAA, cache flush f...		
2062 4.849059	fe80::1:6cbf:8e10::ff02::fb	MDNS	451 Standard query response 0x0000 PTR Soumya's MacBook Pro (2)._companion-link._tcp.local TXT TXT, cache flush AAAA, cache flush f...		
2063 4.849059	10.12.1.66	MDNS	451 Standard query response 0x0000 PTR Soumya's MacBook Pro (2)._companion-link._tcp.local TXT TXT, cache flush AAAA, cache flush f...		
2064 4.849059	10.6.4.45	239.255.255.250	SSDP	489 NOTIFY + HTTP/1.1	
2065 4.849059	fe80::1:7b5::fb77:ddc::ff02::fb	SSDP	521 NOTIFY + HTTP/1.1		
2066 4.849059	10.12.1.66	10.12.1.66	DNS	160 Standard query 0x0000 TXT ANKIT's MacBook Air._companion-link._tcp.local, "QU" question	
2067 4.876747	10.12.1.67	10.2.1.60	DNS	83 Standard query 0x0000 A www.msftconnecttest.com	
2068 4.913626	fe80::1:419::7a00:9b4::ff02::fb	MDNS	223 Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR Ayush's MacBook A...		
2069 4.913626	fe80::1:45c::8500:27a::ff02::fb	MDNS	128 Standard query 0x0000 TXT ANKIT's MacBook Air._companion-link._tcp.local, "QU" question		
2070 4.913626	10.12.1.66	10.12.1.66	DNS	200 Standard query 0x0000 A www.msftncsi.com.edgesuite.net	
2093 5.019380	0.0.0.0	255.255.255.255	DHCP	362 DHCP Request - Transaction ID 0xbFB2328a	
2093 5.019380	10.6.13.1	224.0.0.252	LLMNR	75 Standard query 0x000f ANY LAPTOP-1093V2R	
2094 5.020397	10.12.1.66	239.255.255.250	MDNS	125 Standard query 0x0000 TXT Mayank's MacBook Air (4)._airplay._tcp.local, "QU" question TXT Mayank's Air._airplay._tcp.local, "QU" question	
2096 5.021043	fe80::0054:ffff:feaa::ff02::fb	MDNS	107 Standard query 0x0000 PTR _spotifyconnect._tcp.local, "QU" question		
2097 5.022083	10.6.11.62	224.0.0.251	MDNS	755 Standard query response 0x0000 PTR FABCE4E4B87@amrita's MacBook Pro._raop._tcp.local PTR Amrita's MacBook Pro._companion-link...	
2098 5.022083	fe80::c1:7197::ff02::fb	MDNS	145 Standard query 0x0000 TXT Aryan's MacBook Air (4)._airplay._tcp.local, "QU" question TXT Mayank's Air._airplay._tcp.local, "QU" question		
2099 5.022083	fe80::c1:7197::ff02::fb	MDNS	77 Standard query 0x0000 PTR _spotifyconnect._tcp.local, "QU" question PTR Amrita's MacBook Pro._companion-link...		
2101 5.022083	10.12.41.223	224.0.0.251	MDNS	108 Standard query 0x0000 TXT ANKIT's MacBook Air._companion-link._tcp.local, "QU" question	
2102 5.022083	fe80::1:ceb1bea::697::ff02::fb	MDNS	128 Standard query 0x0000 TXT ANKIT's MacBook Air._companion-link._tcp.local, "QU" question		
2103 5.022083	10.12.45.100	224.0.0.251	MDNS	893 Standard query 0x0000 TXT Mayank's MacBook Pro._raop._tcp.local, "QU" question PTR 468BD0468056565@raop.msnf...	
▼ Frame 2071: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface <devicewpf_{343888c}< td=""><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td></devicewpf_{343888c}<>					
Ethernet II, Src: HewlettPacka_93:44:53 (54:77:8a:93:44:53), Dst: AzureWaveTe_baida13 (50:5a:65:baid:13)					
Internet Protocol Version 4, Src: 10.2.1.60, Dst: 10.12.67.67					
User Datagram Protocol, Src Port: 53, Dst Port: 59534					
Domain Name System (response)					

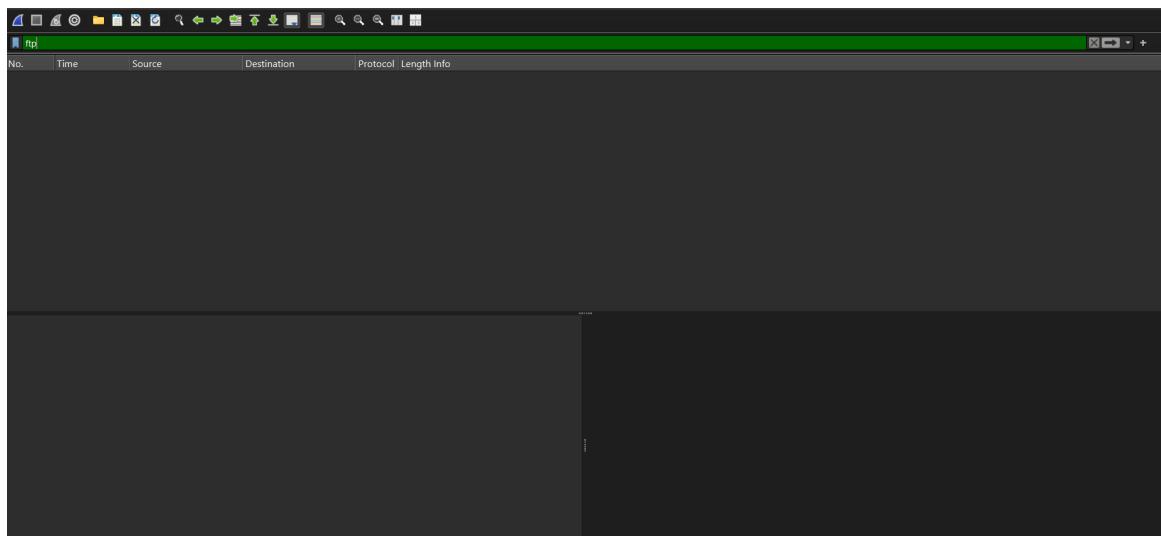
• dns – Shows only DNS traffic

No.	Time	Source	Destination	Protocol	Length Info
2067 4.870674	10.12.67.67	10.2.1.60	DNS	83 Standard query 0x87d3 A www.msftconnecttest.com	
+ 2077 4.870666	10.2.1.68	10.12.67.67	DNS	227 Standard query response 0x87d3 A www.msftconnecttest.com CNAME www.msftncsi.com.edgesuite.net	
+ 4276 10.186359	10.12.67.67	10.2.1.60	DNS	82 Standard query 0x533a A www.computerumbai.com	
+ 4277 10.224247	10.2.1.68	10.12.67.67	DNS	98 Standard query response 0x533a A www.computerumbai.com A 202.189.250.92	
+ 4911 10.863186	10.12.67.67	10.2.1.60	DNS	99 Standard query response 0x9f69 A www.msftncsi.com.edgesuite.net	
+ 4912 11.863186	10.2.1.60	10.12.67.67	DNS	99 Standard query response 0x1669 A zhuo.corpwebcontrol.com A 202.189.250.92	
+ 11034 27.155919	10.12.67.67	10.2.1.60	DNS	91 Standard query 0x9f57 HTTPS teams.events-data.microsoft.com	
+ 11034 27.157722	10.12.67.67	10.2.1.60	DNS	91 Standard query 0xc2f2 HTTPS teams.events-data.microsoft.com	
+ 11034 27.158736	10.12.67.67	10.2.1.60	DNS	79 Standard query 0x9f69 A wpad.DDN.UPEs.AC.IN	
+ 11037 27.201371	10.2.1.60	10.12.67.67	DNS	134 Standard query response 0x9f69 No Such Name A wpad.DDN.UPEs.AC.IN SOA authdn.DDN.UPEs.AC.IN	
+ 11038 27.201371	10.2.1.60	10.12.67.67	DNS	213 Standard query 0x9f69 A www.msftncsi.com.edgesuite.net	
+ 11039 27.218616	10.12.67.67	10.2.1.60	DNS	91 Standard query response 0xc2f2 HTTPS teams.events-data.microsoft.com	
+ 12443 31.209206	10.12.67.67	10.2.1.60	DNS	74 Standard query 0x9e29 A w2l.pnawnet.in	
+ 12507 31.434489	10.2.1.60	10.12.67.67	DNS	98 Standard query response 0x69ee A w2l.pnawnet.in A 146.112.61.106	
+ 12891 32.429626	10.12.67.67	10.2.1.60	DNS	71 Standard query 0x9e29 A w4.pnaw.net	
+ 12976 3.496710	10.2.1.68	10.12.67.67	DNS	87 Standard query response 0x9e29 A w4.pnaw.net A 15.235.218.105	
+ 13358 33.476552	10.12.67.67	10.2.1.60	DNS	82 Standard query 0xb085 A w11.corpwebcontrol.com	
+ 13430 33.476552	10.2.1.60	10.12.67.67	DNS	98 Standard query response 0xb085 A w11.corpwebcontrol.com A 150.242.201.76	
+ 13607 34.300955	10.12.67.67	10.2.1.60	DNS	71 Standard query 0x9e29 A w5.pnaw.net	
+ 13704 34.493355	10.12.67.67	10.12.67.67	DNS	87 Standard query response 0x7398 A w5.pnaw.net A 148.113.17.82	
▼ Frame 2077: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface <devicewpf_{343888c}< td=""><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td></devicewpf_{343888c}<>					
Ethernet II, Src: HewlettPacka_93:44:53 (54:77:8a:93:44:53), Dst: AzureWaveTe_baida13 (50:5a:65:baid:13)					
Internet Protocol Version 4, Src: 10.2.1.60, Dst: 10.12.67.67					
User Datagram Protocol, Src Port: 53, Dst Port: 59534					
Domain Name System (response)					

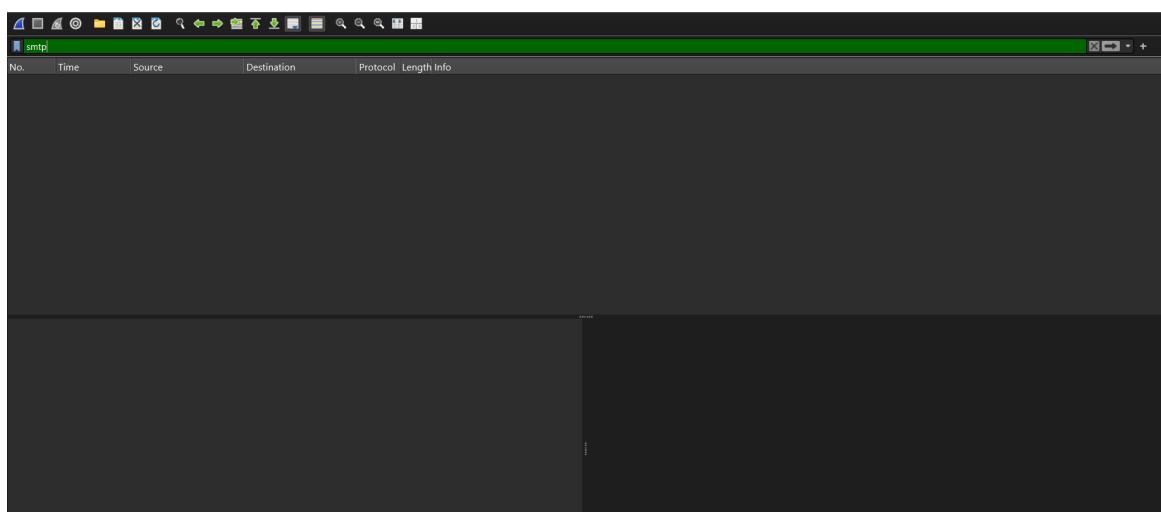
• icmp – Filters ICMP packets (e.g., ping)

No.	Time	Source	Destination	Protocol	Length Info
-+ 3068 9.701165	10.12.67.67	142.250.194.196	ICMP	74 Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 3066)	
-+ 3066 9.701165	142.250.194.196	10.12.67.67	ICMP	74 Echo (ping) reply id=0x0001, seq=22/5632, ttl=117 (request in 3068)	
-+ 3067 9.701165	142.250.194.196	10.12.67.67	ICMP	74 Echo (ping) request id=0x0001, seq=23/5632, ttl=128 (request in 3068)	
-+ 3068 9.701165	142.250.194.196	10.12.67.67	ICMP	74 Echo (ping) reply id=0x0001, seq=23/5632, ttl=117 (request in 3067)	
-+ 3823 11.889435	10.12.67.67	142.250.194.196	ICMP	74 Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 3848)	
-+ 3848 11.889952	142.250.194.196	10.12.67.67	ICMP	74 Echo (ping) reply id=0x0001, seq=24/6144, ttl=117 (request in 3823)	
+ 4136 12.902741	10.12.67.67	142.250.194.196	ICMP	74 Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 4137)	
+ 4137 12.982355	142.250.194.196	10.12.67.67	ICMP	74 Echo (ping) reply id=0x0001, seq=25/6400, ttl=117 (request in 4136)	
▼ Frame 3018: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface <devicewpf_{343888c}< td=""><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td><td data-kind="ghost"></td></devicewpf_{343888c}<>					
Ethernet II, Src: AzureWaveTe_baida13 (50:5a:65:baid:13), Dst: HewlettPacka_93:44:53 (54:77:8a:93:44:53)					
Internet Protocol Version 4, Src: 10.2.1.60, Dst: 10.12.67.67					
Internet Control Message Protocol					

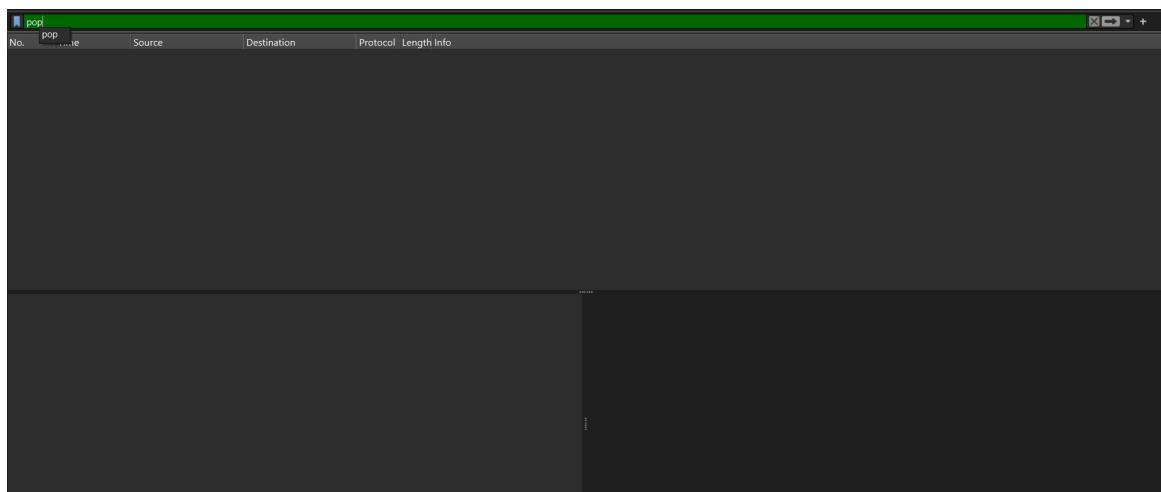
• ftp – Filters FTP traffic



- **smtp** – Filters SMTP (email sending)



- **pop** – Filters POP3 (email receiving)



- **tls or ssl** – Filters encrypted traffic (HTTPS)

No.	Time	Source	Destination	Protocol	Length	Info
2324	5.721639	10.12.67.67	52.123.170.79	TLSv1.2	104	Application Data
2447	5.888155	52.123.170.79	10.12.67.67	TLSv1.2	93	Application Data
2585	6.265407	10.12.67.67	4.213.25.240	TLSv1.2	154	Application Data
2582	6.312669	4.213.25.240	10.12.67.67	TLSv1.2	224	Application Data
4444	10.544246	10.12.67.67	180.149.52.202	TLSv1.2	1249	Application Data, Application Data, Application Data
4446	10.544247	180.149.52.202	10.12.67.67	TLSv1.2	93	Application Data
4462	10.692376	180.149.52.202	10.12.67.67	TLSv1.2	473	Application Data
4463	10.692376	180.149.52.202	10.12.67.67	TLSv1.2	85	Application Data
594	14.274791	10.12.67.67	52.123.169.122	TLSv1.2	111	Application Data
6065	14.462652	52.123.169.122	10.12.67.67	TLSv1.2	100	Application Data
11198	27.511937	10.12.67.67	164.208.16.89	TLSv1.3	450	Client Hello (SNI=teams.events.data.microsoft.com)
11200	27.511937	164.208.16.89	10.12.67.67	TLSv1.3	153	Server Hello, Change Cipher Spec, Client Hello (SNI=teams.events.data.microsoft.com)
11257	27.809168	10.12.67.67	164.208.16.89	TLSv1.3	153	Server Hello, Client Hello (SNI=teams.events.data.microsoft.com)
11258	27.810895	10.12.67.67	164.208.16.89	TLSv1.3	736	Change Cipher Spec, Client Hello (SNI=teams.events.data.microsoft.com)
11360	28.138141	164.208.16.89	10.12.67.67	TLSv1.3	153	HelloRetryRequest, Change Cipher Spec
11362	28.138512	164.208.16.89	10.12.67.67	TLSv1.3	1514	ServerHello
11364	28.138764	164.208.16.89	10.12.67.67	TLSv1.3	620	Application Data
11367	28.142488	10.12.67.67	164.208.16.89	TLSv1.3	673	ChangeCipherSpec, ClientHello (SNI=teams.events.data.microsoft.com)
11368	28.143960	10.12.67.67	164.208.16.89	TLSv1.3	128	Application Data
11369	28.144439	10.12.67.67	164.208.16.89	TLSv1.3	146	Application Data

2. IP Address Filters

- **ip.addr == 192.168.1.1 – Shows all traffic to/from a specific IP**

No.	Time	Source	Destination	Protocol	Length	Info
2067	4.876874	10.12.67.67	10.2.1.68	DNS	83	Standard query 0x87d3 A www.msftconnecttest.com
2077	4.979806	10.2.1.68	10.12.67.67	DNS	27	Standard query response 0x87d3 A www.msftconnecttest.com CNAME www.msftncsi.com.edgesuite.net
2078	4.980285	10.12.67.67	96.17.168.107	TCP	66	54192 > 104 [SYN] Seq=0 Win=65535 MSS=1468 WS=256 SACK_PERM
2079	4.987406	96.17.168.107	10.12.67.67	TCP	54	54192 > 104 [SYN] Seq=0 Win=65535 MSS=1468 WS=256 SACK_PERM
2080	4.987561	10.12.67.67	96.17.168.107	TCP	54	54192 > 104 [ACK] Seq=1 Win=65280 Len=0
2081	4.988983	10.12.67.67	96.17.168.107	HTTP	165	GET /connecttest.txt HTTP/1.1
2082	5.006698	96.17.168.107	10.12.67.67	HTTP	60	80 > 54192 [ACK] Seq=112 Win=64218 Len=0
2083	5.006700	96.17.168.107	10.12.67.67	HTTP	243	401 [Text/Plain]
2084	5.006698	96.17.168.107	10.12.67.67	HTTP	60	80 > 54192 [FIN, ACK] Seq=119 Win=65280 Len=0
2085	5.007081	10.12.67.67	96.17.168.107	TCP	54	54192 > 80 [ACK] Seq=112 Ack=189 Win=65280 Len=0
2086	5.007546	10.12.67.67	96.17.168.107	TCP	54	54192 > 80 [FIN, ACK] Seq=112 Ack=189 Win=0 Len=0
2127	5.032751	96.17.168.107	10.12.67.67	TCP	60	80 > 54192 [ACK] Seq=189 Ack=113 Win=64256 Len=0
2324	5.721639	10.12.67.67	52.123.170.79	TLSv1.2	104	Application Data
2458	5.943378	10.12.67.67	52.123.170.79	TLSv1.2	104	Application Data
2581	6.265407	10.12.67.67	4.213.25.240	TLSv1.2	154	Application Data
2582	6.312669	4.213.25.240	10.12.67.67	TLSv1.2	224	Application Data
2587	6.358203	10.12.67.67	4.213.25.240	TCP	54	54192 > 443 [ACK] Seq=101 Ack=171 Win=251 Len=0
2779	6.659426	10.12.67.67	148.113.9.41	TCP	55	53352 > 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
2781	6.696868	148.113.9.41	10.12.67.67	TCP	66	443 > 5352 [ACK] Seq=1 Ack=2 Win=255 Len=1 SIf=1 SRIf=2

- **ip.src == 192.168.1.1 – Traffic from a specific IP**

No.	Time	Source	Destination	Protocol	Length	Info
2067	4.876874	10.12.67.67	10.2.1.68	DNS	83	Standard query 0x87d3 A www.msftconnecttest.com
2978	4.973296	10.12.67.67	96.17.168.107	TCP	66	54192 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1468 WS=256 SACK_PERM
2080	4.987561	10.12.67.67	96.17.168.107	HTTP	165	GET /connecttest.txt HTTP/1.1
2081	4.988983	10.12.67.67	96.17.168.107	HTTP	60	80 > 54192 [ACK] Seq=112 Ack=189 Win=65280 Len=0
2086	5.007546	10.12.67.67	96.17.168.107	HTTP	243	401 [Text/Plain]
2234	5.721639	10.12.67.67	52.123.170.79	TLSv1.2	104	Application Data
2458	5.943378	10.12.67.67	52.123.170.79	TLSv1.2	104	Application Data
2581	6.265407	10.12.67.67	4.213.25.240	TLSv1.2	154	Application Data
2582	6.312669	4.213.25.240	10.12.67.67	TLSv1.2	224	Application Data
2587	6.358203	10.12.67.67	4.213.25.240	TCP	54	54192 > 443 [ACK] Seq=101 Ack=171 Win=251 Len=0
2779	6.659426	10.12.67.67	148.113.9.41	TCP	55	53352 > 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
4432	10.524426	10.12.67.67	180.149.52.202	TCP	1438	54187 > 443 [ACK] Seq=Ack=1 Win=253 Len=1384 [TCP PDU reassembled in 4434]
4433	10.524426	10.12.67.67	180.149.52.202	TCP	1438	54187 > 443 [ACK] Seq=1385 Ack=1 Win=253 Len=1384 [TCP PDU reassembled in 4434]
4434	10.524426	10.12.67.67	180.149.52.202	TLSv1.2	1249	Application Data, Application Data, Application Data
4435	10.524426	10.12.67.67	180.149.52.202	TCP	54	54192 > 443 [ACK] Seq=Ack=1 Win=251 Len=0
4465	10.759815	10.12.67.67	180.149.52.202	TCP	54	54187 > 443 [ACK] Seq=1384 Ack=1 Win=253 Len=9
4466	10.739805	10.12.67.67	180.149.52.202	TCP	66	[TCP Dup] Seq=44651414187 + 443 [ACK] Seq=39844 Ack=490 Win=252 Len=0 SLF=459 SRF=498
4663	11.248177	10.12.67.67	202.189.250.92	TCP	66	[TCP Retransmission] Seq=44651414187 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1468 WS=256 SACK_PERM

- **ip.dst == 8.8.8.8 – Traffic to a specific IP**

ip.dst = 8.8.8.8

No.	Time	Source	Destination	Protocol	Length Info
31089 66.075437	31.13.79.53	10.12.67.67	TLSv1.3	93 Application Data	
31091 66.107953	31.13.79.53	10.12.67.67	TCP	60 443 → 56834 [SYN, ACK] Seq=1598 Ack=3620 Len=0	
31133 66.177265	20.50.201.200	10.12.67.67	TCP	60 443 → 56810 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
31135 66.177265	20.50.201.200	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56810 [ACK] Seq=24545 Ack=2889 Len=0 SLE=2889 SRE=2889	
31282 68.349325	142.250.182.103	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56895 [ACK] Seq=241484 Ack=5307 Len=0 SLE=5306 SRE=5307	
31284 66.828526	142.250.194.196	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56837 [ACK] Seq=5337480 Ack=102066 Len=0 SLE=102065 SRE=102066	
31287 66.847135	10.2.1.60	10.12.67.67	DNS	133 Standard query response 0x3a0 No such name A upad.DDN.UPEs.AC.IN SOA adcdnn.DDN.UPEs.AC.IN	
31288 66.847135	10.2.1.60	10.12.67.67	DNS	133 Standard query response 0x3a0 No such name A upad.DDN.UPEs.AC.IN SOA adcdnn.DDN.UPEs.AC.IN	
31344 67.277055	142.250.206.142	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56911 [ACK] Seq=13375 Win=267988 Len=0 SLE=3374 SRE=3375	
31349 67.277055	142.250.206.146	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56912 [ACK] Seq=13376 Win=267988 Len=0 SLE=3374 SRE=3374	
31594 68.024319	142.250.206.196	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56925 [ACK] Seq=12414 Ack=2511 Win=267776 Len=0 SLE=2510 SRE=2511	
31529 68.349311	142.250.206.196	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56929 [ACK] Seq=12798 Ack=3739 Win=266496 Len=0 SLE=3738 SRE=3738	
31585 68.849456	172.67.29.97	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56916 [ACK] Seq=94422 Ack=3865 Win=73728 Len=0 SLE=3864 SRE=3865	
31618 69.039164	142.250.194.196	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56936 [ACK] Seq=29715 Ack=3304 Win=266752 Len=0 SLE=3303 SRE=3304	
31620 69.039164	142.250.194.196	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56937 [ACK] Seq=29716 Ack=3305 Win=266756 Len=0 SLE=3305 SRE=3305	
31697 69.551495	142.250.207.234	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56938 [ACK] Seq=12526 Ack=2579 Win=267767 Len=0 SLE=2579 SRE=2579	
31767 69.761925	142.250.207.234	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 56931 [ACK] Seq=26413 Ack=5785 Win=264448 Len=0 SLE=5784 SRE=5785	
31769 69.918111	148.113.9.41	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 → 53352 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=1	
31856 70.081732	13.203.11.146	10.12.67.67	TCP	60 [TCP Keep-Alive] 443 → 56930 [ACK] Seq=0 Ack=7477 Ack=4876 Win=106496 Len=0	

Frame 139: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{34388CA0} (00:00:00:00:00:00) at AzureWaveTec_ba:da:13 (50:5a:65:ba:da:13) Src: 10.2.1.60 Dst: 10.12.67.67
Internet Protocol Version 4, Src: 10.2.1.60, Dst: 10.12.67.67
Transmission Control Protocol, Src Port: 53, Dst Port: 56833, Seq: 0, Ack: 1, Len: 0
0040 03 07

3. Port Filters

- **tcp.port == 80 – Shows HTTP traffic on port 80**

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length Info
2078 4.072206	10.12.67.67	96.17.108.107	TCP	66 54192 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
2079 4.087496	96.17.108.107	10.12.67.67	TCP	66 80 → 54192 [SYN, ACK] Seq=1 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	
2080 4.098561	10.12.67.67	96.17.108.107	TCP	54 54192 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0	
2081 4.098983	10.12.67.67	96.17.108.107	HTTP	165 GET /connecttest.txt HTTP/1.1	
2082 5.006698	96.17.108.107	10.12.67.67	TCP	60 80 → 54192 [ACK] Seq=1 Ack=12 Win=64128 Len=0	
2083 5.006698	96.17.108.107	10.12.67.67	HTTP	165 GET /connecttest.txt HTTP/1.1	
2084 5.006698	96.17.108.107	10.12.67.67	TCP	60 80 → 54192 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0	
2085 5.007081	10.12.67.67	96.17.108.107	TCP	54 54192 → 80 [ACK] Seq=112 Ack=189 Win=65288 Len=0	
2086 5.008754	10.12.67.67	96.17.108.107	TCP	54 54192 → 80 [FIN, ACK] Seq=112 Ack=189 Win=0 Len=0	
2127 5.032751	96.17.108.107	10.12.67.67	TCP	60 80 → 54192 [ACK] Seq=189 Ack=113 Win=64256 Len=0	
4913 11.874659	10.12.67.67	202.189.250.93	TCP	66 54194 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
5334 10.251375	10.12.67.67	202.189.250.93	TCP	66 [TCP Retransmission] 54194 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
6144 14.891154	10.12.67.67	202.189.250.93	TCP	66 [TCP Retransmission] 54194 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
7999 18.899418	10.12.67.67	202.189.250.93	TCP	66 [TCP Retransmission] 54194 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
8102 19.251183	202.189.250.92	10.12.67.67	TCP	66 80 → 54194 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	
8107 19.251373	10.12.67.67	202.189.250.92	TCP	54 54194 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0	
8136 19.251540	10.12.67.67	202.189.250.92	HTTP	164 GET /index.html HTTP/1.1 Content-Type: application/x-www-form-urlencoded	
8149 19.272066	202.189.250.92	10.12.67.67	TCP	60 80 → 54194 [ACK] Seq=118 Win=65280 Len=0	
22799 51.043446	10.12.67.67	202.189.250.92	TCP	54 54194 → 80 [EST, ACK] Seq=114 Ack=1 Win=0 Len=0	
23374 52.989610	10.12.67.67	103.239.171.37	TCP	66 54230 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM	

Frame 2078: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{34388CA0} (00:00:00:00:00:00) at AzureWaveTec_ba:da:13 (54:77:8a:93:44:53) Src: 10.12.67.67 Dst: 10.12.67.67
Internet Protocol Version 4, Src: 10.12.67.67, Dst: 96.17.108.107
Transmission Control Protocol, Src Port: 80, Dst Port: 80, Seq: 0, Ack: 1, Len: 0
0040 04 02

- **udp.port == 53 – Shows DNS traffic over UDP**

No.	Time	Source	Destination	Protocol	Length Info
2067	10.12.67.67	10.2.1.68	10.12.67.67	DNS	22 Standard query 0x07f13 A www.msftconnecttest.com
2077	10.12.67.66	10.2.1.68	10.12.67.67	DNS	22 Standard query 0x07f13 A www.msftconnecttest.com CNAME www.msftncsi.com.edgesuite.net
4276	10.18.6359	10.2.1.68	10.2.1.68	DNS	82 Standard query 0x533a A www.computermumbai.com
4277	10.2.1.68	10.2.1.68	10.12.67.67	DNS	98 Standard query response 0x533a A www.computermumbai.com A 202.189.250.92
4911	11.812453	10.2.1.68	10.2.1.68	DNS	83 Standard query 0x1669 A zvh.corpwebcontrol.com
4912	11.868186	10.2.1.68	10.12.67.67	DNS	99 Standard query response 0x1669 A zvh.corpwebcontrol.com A 202.189.250.92
11834	11.159519	10.2.1.68	10.2.1.68	DNS	91 Standard query 0x0f57 A teams.events.data.microsoft.com
11835	11.159519	10.2.1.68	10.2.1.68	DNS	92 Standard query response 0x0f57 A teams.events.data.microsoft.com
11836	27.158736	10.2.1.68	10.2.1.68	DNS	79 Standard query 0x9f69 A wpad.DDN.UPES.AC.IN
11037	27.201371	10.2.1.68	10.12.67.67	DNS	134 Standard query response 0x9f69 No such name A wpad.DDN.UPES.AC.IN SOA authddn.DDN.UPES.AC.IN
11038	27.219813	10.2.1.68	10.12.67.67	DNS	213 Standard query response 0x0f57 A teams.events.data.microsoft.com CNAME teams-events-data.trafficmanager.net
11039	27.219816	10.2.1.68	10.12.67.67	DNS	91 Standard query response 0x0f57 HTTPS teams.events.data.microsoft.com
12443	10.2.1.68	10.2.1.68	10.12.67.67	DNS	73 Standard query 0x0f57 A w2l.corpwebcontrol.com
12507	31.434489	10.2.1.68	10.12.67.67	DNS	98 Standard query response 0x0f57 A w2l.npavnet.in A 146.112.61.106
12891	32.429629	10.2.1.68	10.2.1.68	DNS	71 Standard query 0x0ca29 A w4.npav.net
12976	32.496719	10.2.1.68	10.12.67.67	DNS	87 Standard query response 0x0ca29 A w4.npav.net A 15.235.218.105
13358	33.476552	10.2.1.68	10.12.67.67	DNS	82 Standard query 0x0eb85 A w11.corpwebcontrol.com
13430	34.476552	10.2.1.68	10.12.67.67	DNS	98 Standard query response 0x0eb85 A w11.corpwebcontrol.com A 150.242.201.76
13493	34.369865	10.2.1.68	10.2.1.68	DNS	71 Standard query 0x2798 A w5.npav.net A 148.113.17.82
13704	34.438345	10.2.1.68	10.12.67.67	DNS	87 Standard query response 0x2798 A w5.npav.net A 148.113.17.82

• tcp.srcport == 443 – HTTPS traffic from server

No.	Time	Source	Destination	Protocol	Length Info
2447	5.888155	4.213.170.79	10.12.67.67	TLSv1.2	93 Application Data
2582	6.312669	4.213.25.240	10.12.67.67	TLSv1.2	224 Application Data
2851	6.696868	148.113.9.41	10.12.67.67	TCP	66 443 > 53352 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
4444	10.549137	180.149.52.202	10.12.67.67	TCP	66 [TCP Keep-Alive] 443 > 54189 [ACK] Seq=1 Ack=3964 Len=0
4445	10.549137	180.149.52.202	10.12.67.67	TCP	66 443 > 54189 [ACK] Seq=1 Ack=3964 Len=0 SLE=1 SRE=2
4446	10.549137	180.149.52.202	10.12.67.67	TLSv1.2	473 Application Data
4462	10.692376	180.149.52.202	10.12.67.67	TLSv1.2	85 Application Data
4463	10.692376	180.149.52.202	10.12.67.67	TLSv1.2	85 Application Data
4464	10.739803	180.149.52.202	10.12.67.67	TCP	85 [TCP Retransmission] 443 > 54187 [PSH, ACK] Seq=459 Ack=3964 Win=1105 Len=31
6063	14.270452	52.123.170.79	10.12.67.67	TLSv1.2	100 Application Data
7150	14.270452	148.113.9.41	10.12.67.67	TCP	66 [TCP Keep-Alive] 443 > 53352 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
10753	26.783831	148.113.9.41	10.12.67.67	TCP	66 [TCP Keep-Alive] 443 > 53352 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
10951	27.064594	180.149.52.218	10.12.67.67	TCP	66 443 > 54189 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
11088	27.308232	20.189.173.1	10.12.67.67	TCP	66 443 > 54188 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
11195	27.508163	180.208.16.89	10.12.67.67	TCP	66 443 > 54189 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
13300	27.508163	180.208.16.89	10.12.67.67	TCP	66 443 > 54189 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
11254	27.800402	104.208.16.89	10.12.67.67	TLSv1.3	153 HelloRetryRequest, ChangeCipherSpec
11309	27.995642	104.208.16.89	10.12.67.67	TCP	66 443 > 54189 [ACK] Seq=109 Ack=2519 Win=4194560 Len=0
11368	28.138141	104.208.16.89	10.12.67.67	TLSv1.3	153 HelloRetryRequest, ChangeCipherSpec
13161	28.138141	104.208.16.89	10.12.67.67	TLSv1.3	1514 Server Hello

• tcp.dstport == 443 – HTTPS traffic to server

No.	Time	Source	Destination	Protocol	Length Info
2350	5.943038	10.12.67.67	52.123.170.79	TLSv1.2	38 Application Data
2459	5.943038	10.12.67.67	52.123.170.79	TCP	54 53373 > 443 [ACK] Seq=51 Ack=40 Win=25 Len=0
2581	6.265407	10.12.67.67	4.213.25.240	TLSv1.2	154 Application Data
2587	6.358203	10.12.67.67	4.213.25.240	TCP	54 49423 > 443 [ACK] Seq=101 Ack=171 Win=251 Len=0
2779	6.659426	10.12.67.67	148.113.9.41	TCP	55 53352 > 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
4278	10.235062	10.12.67.67	20.189.173.1	TCP	66 443 > 54189 [ACK] Seq=103 Ack=1 Win=13400 Len=0 MSS=1440 WS=256 SACK_PERM
4432	10.235062	10.12.67.67	180.149.52.202	TCP	1438 54189 > 443 [ACK] Seq=103 Ack=1 Win=13400 Len=0 MSS=1440 WS=256 SACK_PERM
4443	10.235062	10.12.67.67	180.149.52.202	TCP	1438 54187 > 443 [ACK] Seq=1385 Ack=2535 Win=1384 [TCP PDU reassembled in 4434]
4444	10.235062	10.12.67.67	180.149.52.202	TLSv1.2	1249 Application Data, Application Data, Application Data
4457	10.596864	10.12.67.67	180.149.52.202	TCP	54 54187 > 443 [ACK] Seq=3964 Ack=40 Win=253 Len=0
4465	10.739815	10.12.67.67	180.149.52.202	TCP	54 54187 > 443 [ACK] Seq=3964 Ack=490 Win=252 Len=0
4466	10.739865	10.12.67.67	180.149.52.202	TCP	66 [TCP Dup ACK 4465#1] 54187 > 443 [ACK] Seq=3964 Ack=490 Win=252 Len=0 SLE=1 SRE=2
4683	10.739815	10.12.67.67	20.189.173.1	TCP	66 [TCP Retransmission] 54187 > 443 [ACK] Seq=3964 Ack=490 Win=252 Len=0 MSS=1440 WS=256 SACK_PERM
5353	13.250506	10.12.67.67	20.189.173.1	TCP	54 54193 > 443 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5945	14.274791	10.12.67.67	52.123.168.122	TLSv1.2	311 Application Data
6064	14.518798	10.12.67.67	52.123.168.122	TCP	54 53720 > 443 [ACK] Seq=47 Win=254 Len=0
7147	14.701978	10.12.67.67	148.113.9.41	TCP	55 [TCP Keep-Alive] 53352 > 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
7482	17.258647	10.12.67.67	20.189.173.1	TCP	66 [TCP Retransmission] 54187 > 443 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
7500	17.258647	10.12.67.67	20.189.173.1	TCP	66 [TCP Retransmission] 54187 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
10741	26.738182	10.12.67.67	148.113.9.41	TCP	55 [TCP Keep-Alive] 53352 > 443 [ACK] Seq=1 Ack=1 Win=255 Len=1

4. MAC Address Filters

• eth.addr == 00:11:22:33:44:55 – Traffic to/from a specific MAC address

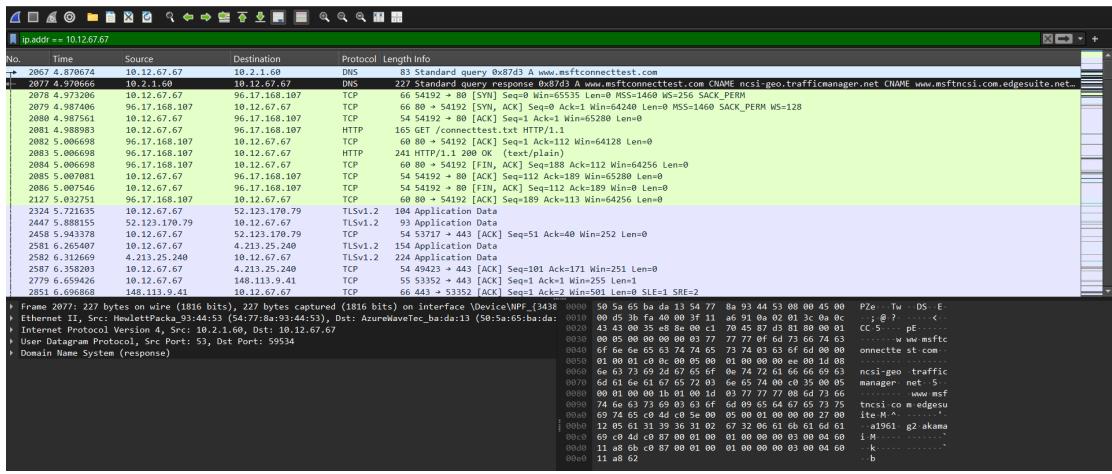
No.	Time	Source	Destination	Protocol	Length	Info
2067	4.570674	10.12.67.67	10.2.1.68	DNS	83	Standard query 0x87d3 A www.msftconnecttest.com
2077	4.570666	10.2.1.68	10.12.67.67	DNS	227	Standard query response 0x87d3 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net
2078	4.573206	10.12.67.67	95.17.168.107	TCP	66	54192 > 80 [SYN] Seq=0 Win=5535 Len=0 MSS=1460 WS=256 SACK_PERM
2079	4.574846	95.17.168.107	10.12.67.67	TCP	66	80 > 54192 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2080	4.575051	10.12.67.67	95.17.168.107	TCP	54	54192 > 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
2081	4.588983	10.12.67.67	95.17.168.107	HTTP	165	GET /Connecttest.txt HTTP/1.1
2082	5.066698	95.17.168.107	10.12.67.67	TCP	60	80 > 54192 [ACK] Seq=1 Ack=112 Win=64128 Len=0
2083	5.066698	95.17.168.107	10.12.67.67	HTTP	241	HTTP/1.1 200 OK (text/plain)
2084	5.066698	95.17.168.107	10.12.67.67	TCP	60	64128 > 54192 [FIN, ACK] Seq=112 Ack=113 Win=64256 Len=0
2085	5.087981	10.12.67.67	95.17.168.107	TCP	54	54192 > 80 [FIN, ACK] Seq=112 Ack=113 Win=65280 Len=0
2086	5.087546	10.12.67.67	95.17.168.107	TCP	54	54192 > 80 [FIN, ACK] Seq=112 Ack=113 Win=6 Len=0
2127	5.932751	95.17.168.107	10.12.67.67	TCP	60	80 > 54192 [ACK] Seq=189 Ack=113 Win=64256 Len=0
2324	5.721635	10.12.67.67	52.123.170.79	TLSv1.2	104	Application Data
2447	5.843661	52.123.170.79	10.12.67.67	TLSv1.2	104	Application Data
2504	5.843738	10.12.67.67	52.123.170.79	TLSv1.2	104	Application Data Seq=51 Ack=40 Win=252 Len=0
2581	6.265487	10.12.67.67	4.213.25.240	TLSv1.2	154	Application Data
2582	6.312669	4.213.25.240	10.12.67.67	TLSv1.2	224	Application Data
2587	6.358203	10.12.67.67	4.213.25.240	TCP	54	49423 > 443 [ACK] Seq=101 Ack=171 Win=251 Len=0
2779	6.659426	10.12.67.67	148.113.9.41	TCP	55	53552 > 443 [ACK] Seq=101 Ack=1 Win=251 Len=0
2801	6.659426	148.113.9.41	10.12.67.67	TCP	66	6423 > 53532 [ACK] Seq=101 Ack=1 Win=501 Len=1 STE=1 SRE=2
F	From: 10.12.67.67	To: 10.2.1.68	83 bytes captured (664 bits), 83 bytes decoded (664 bits) on interface 'Device_WPF_34388BC' (mon0)		54	77 Ba 93 44 53 50 55 65 Ba 13 00 88 45 00 Tw DSP2 e - E
Ethernet II, Src: Arduinokeket [00:5e:65:b2:d1:13], Dst: HewlettPacke_93:44:53 (54:77:8a:03:44:00)				0010	00 00 01 45 60 00 00 88 11 F9 Ba 0a 9c 43 43 02 00 E - E .. CC ..	
Internet Protocol Version 4, Src: 10.12.67.67, Dst: 10.2.1.68				0020	00 01 c8 8e 00 35 00 31 25 4F 87 d3 01 00 00 01 <- 5 30 ..	
User Datagram Protocol, Src Port: 59534, Dst Port: 53				0030	00 00 00 00 00 00 00 03 77 77 0f 6d 73 66 74 63 <- 11 11 ..	
Domain Name System (query)				0040	00 00 00 00 00 00 00 00 75 74 05 65 74 74 63 <- 11 11 ..	
				0050	01 00 01	

- **eth.src == 00:11:22:33:44:55** – Traffic from MAC

- `eth.dst == 00:11:22:33:44:55` – Traffic to MAC

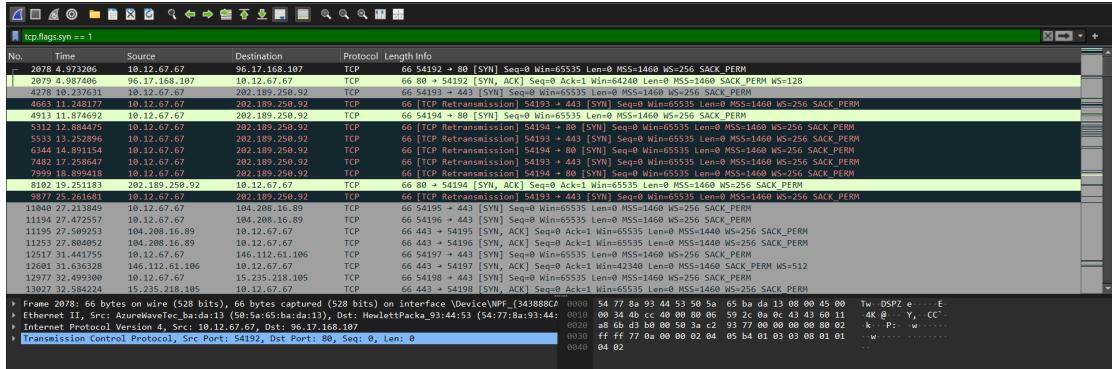
5. Network Filters

- `ip.addr == 192.168.0.0/24` – Traffic within a subnet

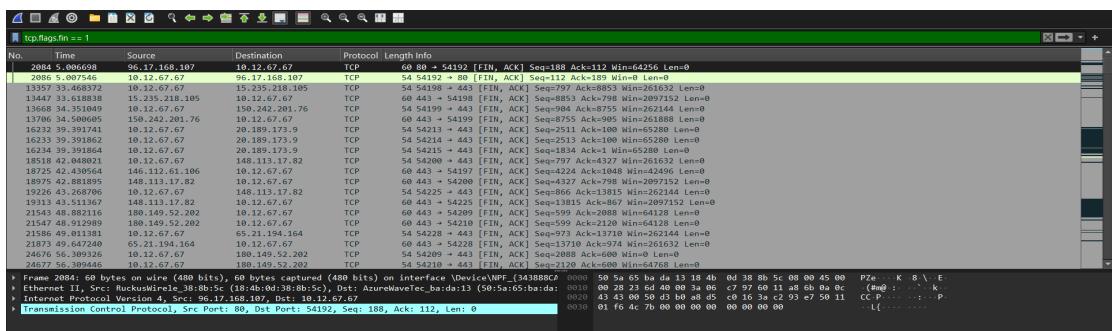


6. TCP Flags

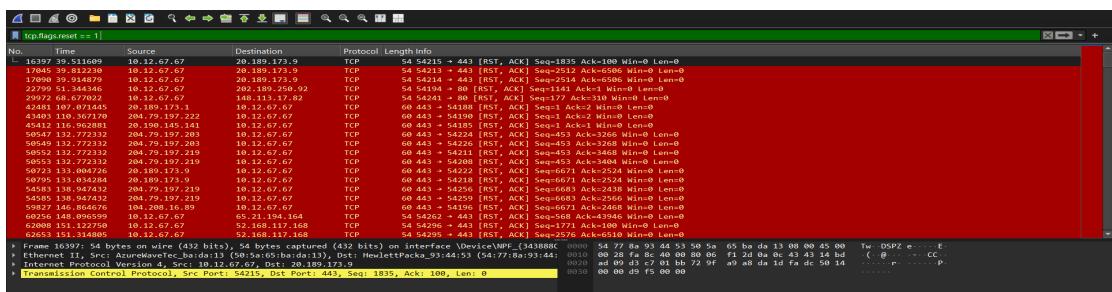
- `tcp.flags.syn == 1` – SYN packets (start of TCP handshake)



- `tcp.flags.fin == 1` – FIN packets (end of session)



- `tcp.flags.reset == 1` – RST packets (reset connection)



7. Other Useful Filters

- frame contains "text" – Packets containing specific text

No.	Time	Source	Destination	Protocol	Length Info
25130	57.09894	10.12.67.67	10.2.1.60	DNS	82 Standard query 0x0f94 A myupes-beta.uptes.ac.in
25131	57.09974	10.12.67.67	10.2.1.60	DNS	82 Standard query 0x452b HTTPS myupes-beta.uptes.ac.in
25133	57.10498	10.12.67.67	10.2.1.60	DNS	82 Standard query 0x0f91 B myupes-beta.uptes.ac.in
25135	57.10525	10.12.67.67	10.2.1.60	DNS	82 Standard query response 0x0f91 B myupes-beta.uptes.ac.in A 135.235.233.234
25136	57.162354	10.2.1.60	10.12.67.67	DNS	82 Standard query response 0x0f52b HTTPS myupes-beta.uptes.ac.in
25161	57.162354	10.2.1.60	10.12.67.67	DNS	82 Standard query response 0x0f91 A myupes-beta.uptes.ac.in A 135.235.233.234
25174	57.19712	10.12.67.67	135.235.233.234	TCP	1444 54236 → 443 [ACK] Seq=1 Win=5228 Len=1390 [TCP PDU reassembled in 25175]
26075	59.02886	10.2.1.60	10.12.67.67	DNS	98 Standard query 0x029b A myupes-beta.uptes.ac.in
26076	59.028892	10.2.1.60	10.12.67.67	DNS	98 Standard query 0x029b A myupes-beta.uptes.ac.in
26089	59.071484	10.2.1.60	10.12.67.67	DNS	98 Standard query response 0x029b A myupes-beta.uptes.ac.in A 135.235.233.234
26886	59.071481	10.2.1.60	10.12.67.67	DNS	98 Standard query response 0x0fde A myupes-beta.uptes.ac.in A 135.235.233.234
26258	59.49368	10.2.1.60	10.12.67.67	DNS	98 Standard query 0x6695 A myupes-beta.uptes.ac.in
26312	59.541538	10.2.1.60	10.12.67.67	DNS	98 Standard query response 0x6695 A myupes-beta.uptes.ac.in A 135.235.233.234
26591	59.92558	10.12.67.67	135.235.233.234	TCP	1444 54248 → 443 [ACK] Seq=1 Win=5228 Len=1390 [TCP PDU reassembled in 26592]
31039	73.09893	10.12.67.67	10.2.1.60	DNS	74 Standard query 0x0293 HTTPS lms.uptes.ac.in
31830	73.097957	10.12.67.67	10.2.1.60	DNS	74 Standard query 0x0293 HTTPS lms.uptes.ac.in
31831	73.099438	10.12.67.67	10.2.1.60	DNS	74 Standard query 0x05e5 A lms.uptes.ac.in
31832	73.091372	10.12.67.67	10.2.1.60	DNS	82 Standard query 0x2f1d A myupes-beta.uptes.ac.in
31843	73.0959402	10.2.1.60	10.12.67.67	DNS	90 Standard query response 0xabad1 lms.uptes.ac.in A 20.207.95.233
31844	73.0959402	10.2.1.60	10.12.67.67	DNS	74 Standard query response 0x0793 HTTPS lms.uptes.ac.in

- tcp.analysis.retransmission – Shows retransmitted packets

No.	Time	Source	Destination	Protocol	Length Info
7482	17.208647	10.12.67.67	202.480.259.92	TCP	66 [TCP Retransmission] 54193 + 443 [SYN] Seq=0 Win=65325 Len=1460 MSS=1460 WS=256 SACK_PERM
7999	18.099418	10.12.67.67	202.489.259.92	TCP	66 [TCP Retransmission] 54194 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
9877	25.261681	10.12.67.67	202.489.259.92	TCP	66 [TCP Retransmission] 54193 + 443 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
15697	38.81131	10.12.67.67	10.12.67.67	TCP	66 [TCP Retransmission] 443 + 54209 [SYN] ACK Seq=0 Win=65335 Len=0 MSS=1384 SACK_PERM WS=128
17265	40.077614	23.32.177.89	10.12.67.67	TCP	739 [TCP Retransmission] 443 + 54221 [PSH, ACK] Seq=17007 Ack=2583 Win=64128 Len=685 [TCP PDU reassembled in 17220]
17846	40.0996179	23.32.177.89	10.12.67.67	TCP	888 [TCP Retransmission] 443 + 54209 [PSH, ACK] Seq=17007 Ack=2583 Win=64128 Len=685 [TCP PDU reassembled in 17220]
20980	40.12.67.67	148.13.17.82	10.12.67.67	TCP	60 [TCP Retransmission] 54227 + 443 [PSH, ACK] Seq=17007 Ack=2583 Win=64128 Len=685
23745	55.995263	10.12.67.67	10.13.199.173	TCP	66 [TCP Retransmission] 54230 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
24456	55.745082	10.12.67.67	20.189.173.9	TCP	89 [TCP Retransmission] 54203 + 443 [PSH, ACK] Seq=167594 Ack=10784 Win=64080 Len=35
24511	55.998651	10.12.67.67	103.239.171.37	TCP	66 [TCP Retransmission] 54230 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
26207	59.208943	10.12.67.67	52.66.36.147	TCP	1514 [TCP Retransmission] 54237 + 443 [PSH, ACK] Seq=17007 Ack=2583 Win=64128 Len=1460 [TCP PDU reassembled in 26149]
26890	59.209441	10.12.67.67	148.13.17.89	TCP	160 [TCP Retransmission] 54237 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
26948	59.311842	52.66.36.147	10.12.67.67	TCP	513 [TCP Spurious Retransmission] 443 + 54237 [PSH, ACK] Seq=47272 Ack=2766 Win=33792 Len=459
26621	60.003842	52.66.36.147	103.239.171.37	TCP	66 [TCP Retransmission] 54230 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
29080	66.438453	10.12.67.67	10.12.67.67	TCP	66 [TCP Retransmission] 443 + 54231 [FIN, ACK] Seq=615 Ack=2153 Win=64128 Len=0
29034	66.580457	10.12.67.67	103.239.171.37	TCP	66 [TCP Retransmission] 443 + 54233 [FIN, ACK] Seq=599 Ack=2152 Win=64128 Len=0
29088	66.686353	10.12.67.67	10.12.67.67	TCP	117 [TCP Spurious Retransmission] 443 + 54233 [FIN, ACK] Seq=595 Ack=2153 Win=64128 Len=63
29090	66.686353	10.12.67.67	10.12.67.67	TCP	66 [TCP Retransmission] 443 + 54234 [FIN, ACK] Seq=596 Ack=2153 Win=64128 Len=63
29091	66.686353	10.12.67.67	10.12.67.67	TCP	66 [TCP Retransmission] 443 + 54235 [FIN, ACK] Seq=597 Ack=2153 Win=64128 Len=0
29116	66.826821	10.12.67.67	10.12.67.67	TCP	117 [TCP Spurious Retransmission] 443 + 54233 [FIN, PSH, ACK] Seq=595 Ack=2152 Win=64128 Len=63
26077	66.826821	10.12.67.67	10.12.67.67	TCP	0 [TCP Control Protocol, Src Port: 54230, Dst Port: 80, Seq: 0, Len: 0]

- tcp.analysis.flags – Flags abnormal TCP behavior

No.	Time	Source	Destination	Protocol	Length Info
20743	46.829983	10.12.67.67	148.113.9.41	TCP	55 [TCP Keep-Alive] 53352 + 443 [ACK] Seq=1 Ack=1 Win=255 Len=1
20744	46.868082	148.113.9.41	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 + 53352 [ACK] Seq=1 Ack=2 Win=50 SLE=1 SRE=2
20838	47.073076	148.113.17.82	10.12.67.67	TCP	66 [TCP Dup ACK 2050081] 443 + 54222 [ACK] Seq=5198 Ack=1143 Win=2096640 Len=0 SLE=539 SRE=1143
21874	49.647414	10.12.67.67	65.21.194.164	TCP	54 [TCP Dup ACK 215851] 54228 + 443 [ACK] Seq=974 Ack=13710 Win=261144 Len=0
23745	55.995263	10.12.67.67	10.13.199.173	TCP	66 [TCP Retransmission] 54187 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
24455	55.745079	10.12.67.67	10.13.199.173	TCP	55 [TCP Retransmission] 54187 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
24456	55.745082	10.12.67.67	10.13.199.173	TCP	66 [TCP Keep-Alive] 443 + 54187 [ACK] Seq=499 Ack=498 Win=2523 Len=0
24455	55.77574	10.12.67.67	10.12.67.67	TCP	66 [TCP Keep-Alive ACK] 443 + 54187 [ACK] Seq=499 Ack=498 Win=64128 Len=0
24456	55.77574	10.12.67.67	20.189.173.9	TCP	1514 [TCP Retransmission] 54203 + 443 [PSH, ACK] Seq=17084 Ack=10784 Win=64080 Len=35
24510	55.994526	20.189.173.9	10.12.67.67	TCP	66 [TCP Dup ACK 2445781] 443 + 54280 [ACK] Seq=17084 Ack=167629 Win=0 SLE=167594 SRE=167629
24511	55.998651	10.12.67.67	103.239.171.37	TCP	66 [TCP Retransmission] 54230 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
24717	56.361481	10.12.67.67	10.12.67.67	TCP	66 [TCP Dup ACK 2471161] 54231 + 80 [SYN] Seq=0 Win=65335 Len=0 MSS=1460 WS=256 SACK_PERM
24718	56.361682	10.12.67.67	180.149.52.202	TCP	66 [TCP Dup ACK 2471161] 54231 + 443 [ACK] Seq=2973 Ack=1 Win=65280 Len=0 SLE=0 SRE=1
24735	56.402355	10.12.67.67	10.12.67.67	TCP	66 [TCP Out-Of-Order] 443 + 54233 [SYN, ACK] Seq=1 Ack=1 Win=64240 Len=0 SLE=0 SRE=1
24736	56.402410	10.12.67.67	10.12.67.67	TCP	66 [TCP Dup ACK 2471981] 54233 + 443 [ACK] Seq=2072 Ack=1 Win=65280 Len=0 SLE=0 SRE=1
24738	56.412878	10.12.67.67	10.12.67.67	TCP	66 [TCP Out-Of-Order] 443 + 54234 [SYN, ACK] Seq=1 Ack=1 Win=64240 Len=0 SLE=0 SACK_PERM WS=128
24740	56.413584	10.12.67.67	10.12.67.67	TCP	66 [TCP Out-Of-Order] 443 + 54235 [SYN, ACK] Seq=1 Ack=1 Win=64240 Len=0 SLE=0 SACK_PERM WS=128
24741	56.413621	10.12.67.67	10.12.67.67	TCP	66 [TCP Dup ACK 2472441] 54232 + 443 [ACK] Seq=2088 Ack=1 Win=64240 Len=0 SLE=0 SRE=1
24934	56.803798	10.12.67.67	10.12.67.67	TCP	66 [TCP Out-Of-Order] 443 + 54235 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
Frame 24511: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface [DeviceWPF_{34388BC} 00000 54 78 93 44 53 50 5a 65 ba da 13 08 00 45 00 Tw DSPZ e E] Ethernet II, Src: AzureWaveTec_ba:da:13 (50:5a:65:ba:da:13), Dst: HewlettPacka_93:44:53 (54:77:8a:93:44:53) Internet Protocol Version 4, Src: 10.12.67.67, Dst: 103.239.171.37 Transmission Control Protocol, Src Port: 54230, Dst Port: 80, Seq: 0, Len: 0	0010 00 34 b9 29 40 00 80 06 e1 36 0a 0c 43 67 ef 4 0) 6 -Cg- 0020 ab 25 d3 d6 00 50 66 60 0d 52 00 00 00 00 80 02 %PF R- 0030 ff c6 d3 00 02 04 05 b4 01 03 03 08 01 01 0040 04 02	...			

- arp – Filters ARP requests/replies

No.	Time	Source	Destination	Protocol	Length/Info
24439	55.706840	ba:69:ad:57:d8:06	Broadcast	ARP	56 Who has 10.12.1.17 Tell 10.12.13.124
24440	55.706618	96:26:3b:88:c1:54	Broadcast	ARP	56 Who has 10.12.3.26? Tell 10.12.14.12
24441	55.707289	3a:f4:f7:30:c1:e5	Broadcast	ARP	56 Who has 10.12.1.1? Tell 10.12.20.82
24442	55.707289	ba:cc:e8:8b:58:08	Broadcast	ARP	56 Who has 10.12.30.165? Tell 10.12.41.46
24443	55.707289	ba:c1:ed:8b:58:08	Broadcast	ARP	56 Who has 10.12.35.31? Tell 10.12.41.46
24444	55.707289	9a:c1:ed:8b:58:08	Broadcast	ARP	56 Who has 10.12.35.31? Tell 10.12.41.46
24459	55.809462	AcmeNetGear-5:s1:a1	Broadcast	ARP	56 Who has 10.6.21.15? Tell 10.6.1.46
24461	55.809833	LiteonTechno_8b:54:c0	Broadcast	ARP	56 Who has 10.6.17.145? Tell 10.6.4.121
24462	55.811188	16:b3:69:2c:3d:f3	Broadcast	ARP	56 Who has 10.12.23.161? Tell 10.12.43.84
24482	55.908919	Intel_6e:6d:07	Broadcast	ARP	56 Who has 10.6.21.15? Tell 10.6.29.3
24557	56.111355	Apple_4b:9c:0b	Broadcast	ARP	56 Who has 10.6.1.17 Tell 10.6.28.217
24564	56.111355	Intel_e7:3e:16	Broadcast	ARP	56 Who has 10.6.1.17 Tell 10.6.4.43
24564	56.114983	Intel_e7:3e:16	Broadcast	ARP	56 Who has 10.6.4.43? (ARP Probe)
24567	56.115122	Intel_e7:3e:16	Broadcast	ARP	56 Who has 10.6.1.17 Tell 10.6.4.43
24568	56.115122	86:87:45:ff:ff:ef	Broadcast	ARP	56 Who has 10.6.18.114? Tell 10.6.17.209
24569	56.115122	aa:61:29:16:44:25	Broadcast	ARP	56 Who has 10.6.1.17 Tell 10.6.4.242
24570	56.115122	4e:3b:4c:1f:56:07	Broadcast	ARP	56 ARP Announcement for 10.6.1.17
24572	56.115122	ba:c8:e8:8b:58:08	Broadcast	ARP	56 ARP Announcement for 10.12.12.41.46
24569	56.219869	ba:c8:e8:8b:58:08	Broadcast	ARP	56 Who has 10.12.1.1? Tell 10.12.41.46
24563	56.219869	4e:a9:6b:13:3a:f8	Broadcast	ARP	56 ARP Announcement for 10.12.29.46