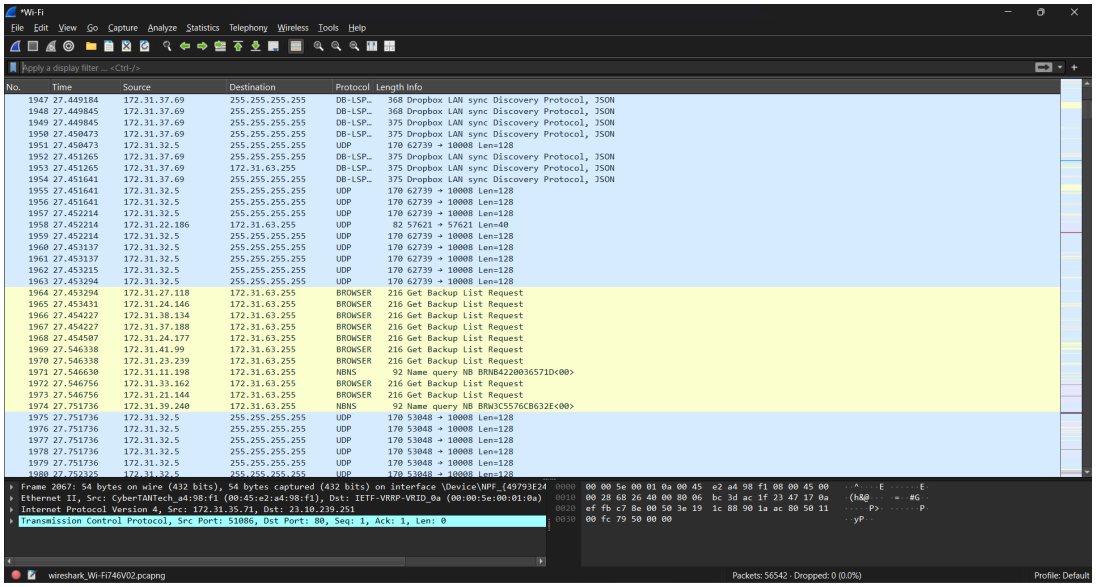
CSL6010 : Cybersecurity
Assignment - III

Name : *Abhay Kashyap*
Roll no : *B22CS001*

---

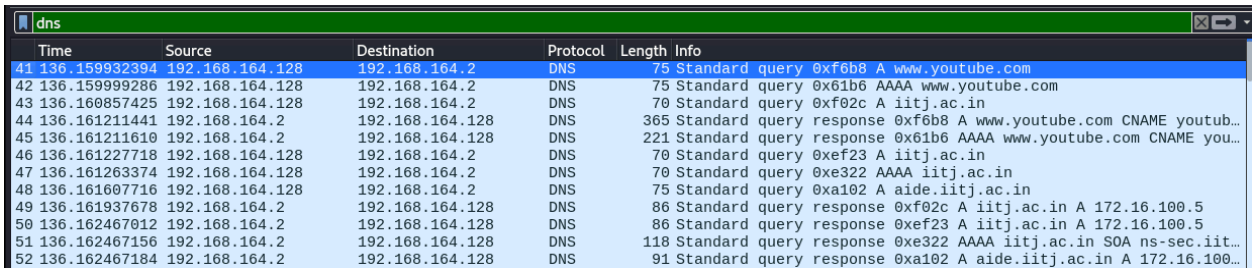
1. Start packet capture in Wireshark on your wireless interface. What do you observe?

This is the traffic overview captured by Wireshark, displaying detailed information such as source and destination addresses, along with the protocols in use. Wireshark serves as a comprehensive tool for analyzing network traffic and diagnosing potential issues in the communication flow.



2. Now visit a local website, say www.iitj.ac.in. Subsequently stop the packet capture and record your observations. Are you able to see the DNS request? What about TCP and HTTP? What is the IP address of the IITJ server? Are you able to see different HTTP requests/responses? Please justify your answer with relevant screenshots.

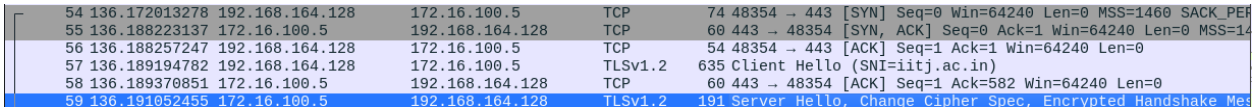
When opening the iitj.ac.in website, we can see the network requesting the IP address of the IITJ server and receiving it in response



dns

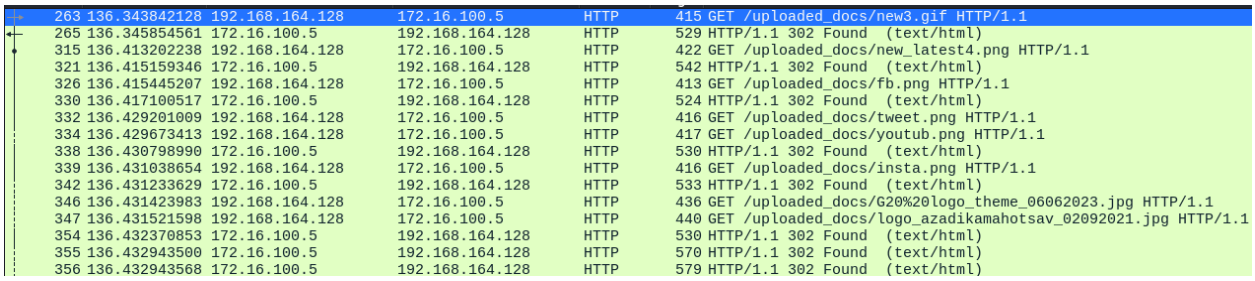
Time	Source	Destination	Protocol	Length	Info
41 136.159932394	192.168.164.128	192.168.164.2	DNS	75	Standard query 0xf6b8 A www.youtube.com
42 136.159999286	192.168.164.128	192.168.164.2	DNS	75	Standard query 0x61b6 AAAA www.youtube.com
43 136.160857425	192.168.164.128	192.168.164.2	DNS	70	Standard query 0xf02c A iitj.ac.in
44 136.161211441	192.168.164.2	192.168.164.128	DNS	365	Standard query response 0xf6b8 A www.youtube.com CNAME youtub…
45 136.161211610	192.168.164.2	192.168.164.128	DNS	221	Standard query response 0x61b6 AAAA www.youtube.com CNAME you…
46 136.161227718	192.168.164.128	192.168.164.2	DNS	70	Standard query 0xef23 A iitj.ac.in
47 136.161263374	192.168.164.128	192.168.164.2	DNS	70	Standard query 0xe322 AAAA iitj.ac.in
48 136.161607716	192.168.164.128	192.168.164.2	DNS	75	Standard query 0xa102 A aide.iitj.ac.in
49 136.161937678	192.168.164.2	192.168.164.128	DNS	86	Standard query response 0xf02c A iitj.ac.in A 172.16.100.5
50 136.162467012	192.168.164.2	192.168.164.128	DNS	86	Standard query response 0xef23 A iitj.ac.in A 172.16.100.5
51 136.162467156	192.168.164.2	192.168.164.128	DNS	118	Standard query response 0xe322 AAAA iitj.ac.in SOA ns-sec.iit…
52 136.162467184	192.168.164.2	192.168.164.128	DNS	91	Standard query response 0xa102 A aide.iitj.ac.in A 172.16.100…

The following screenshot shows the TCP handshake using three packets in sequence :-
SYN (Client to Server)
SYN-ACK (Server to Client)
ACK (Client to Server)



54 136.172013278	192.168.164.128	172.16.100.5	TCP	74	48354 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
55 136.188223137	172.16.100.5	192.168.164.128	TCP	60	443 → 48354 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=14
56 136.188257247	192.168.164.128	172.16.100.5	TCP	54	48354 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
57 136.189194782	192.168.164.128	172.16.100.5	TLSv1.2	635	Client Hello (SNI=iitj.ac.in)
58 136.189370851	172.16.100.5	192.168.164.128	TCP	60	443 → 48354 [ACK] Seq=1 Ack=582 Win=64240 Len=0
59 136.191052455	172.16.100.5	192.168.164.128	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Mes

Here is the HTTP request and response after a successful handshake



263 136.343842128	192.168.164.128	172.16.100.5	HTTP	415	GET /uploaded_docs/new3.gif HTTP/1.1
265 136.345854561	172.16.100.5	192.168.164.128	HTTP	529	HTTP/1.1 302 Found (text/html)
315 136.413202238	192.168.164.128	172.16.100.5	HTTP	422	GET /uploaded_docs/new_latest4.png HTTP/1.1
321 136.415159346	172.16.100.5	192.168.164.128	HTTP	542	HTTP/1.1 302 Found (text/html)
326 136.415445207	192.168.164.128	172.16.100.5	HTTP	413	GET /uploaded_docs/fb.png HTTP/1.1
330 136.417100517	172.16.100.5	192.168.164.128	HTTP	524	HTTP/1.1 302 Found (text/html)
332 136.429201009	192.168.164.128	172.16.100.5	HTTP	416	GET /uploaded_docs/tweet.png HTTP/1.1
334 136.429673413	192.168.164.128	172.16.100.5	HTTP	417	GET /uploaded_docs/youtub.png HTTP/1.1
338 136.430798990	172.16.100.5	192.168.164.128	HTTP	530	HTTP/1.1 302 Found (text/html)
339 136.431038654	192.168.164.128	172.16.100.5	HTTP	416	GET /uploaded_docs/insta.png HTTP/1.1
342 136.431233629	172.16.100.5	192.168.164.128	HTTP	533	HTTP/1.1 302 Found (text/html)
346 136.431423983	192.168.164.128	172.16.100.5	HTTP	436	GET /uploaded_docs/G20%20logo_theme_06062023.jpg HTTP/1.1
347 136.431521598	192.168.164.128	172.16.100.5	HTTP	440	GET /uploaded_docs/logo_azadikamahotsav_02092021.jpg HTTP/1.1
354 136.432370853	172.16.100.5	192.168.164.128	HTTP	530	HTTP/1.1 302 Found (text/html)
355 136.432943500	172.16.100.5	192.168.164.128	HTTP	570	HTTP/1.1 302 Found (text/html)
356 136.432943568	172.16.100.5	192.168.164.128	HTTP	579	HTTP/1.1 302 Found (text/html)

3. What does a packet highlighted in `black' color signify?

Black packets represent some sort of error in the transmission of the packet. Black packets in network analysis tools (such as Wireshark) indicate TCP retransmissions, duplicate ACKs, or lost segments. These events often signal potential network issues like packet loss or congestion, which can degrade network performance.

1. TCP Retransmissions

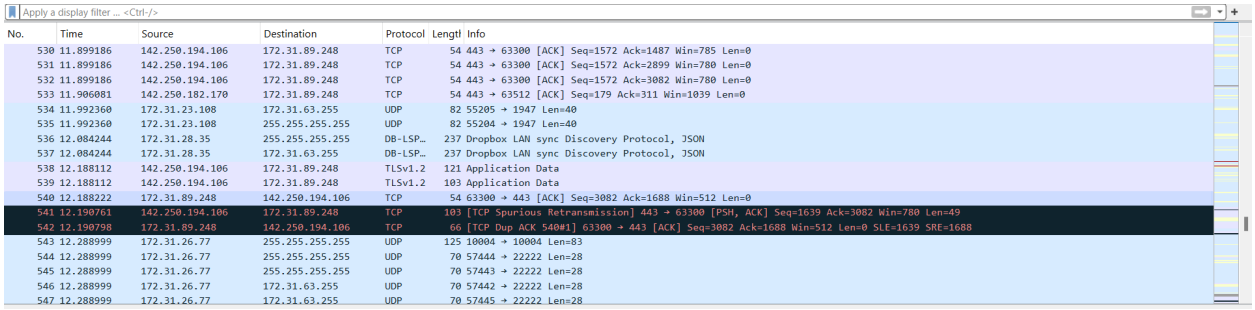
- TCP ensures reliable data transfer by using sequence numbers and acknowledgments (ACKs).
- When a sender transmits a packet, it expects an acknowledgment from the receiver.
- If the sender does not receive an ACK within a specific time (due to packet loss or excessive delay), it retransmits the same packet.
- This retransmission is detected in network analysis as a black packet, indicating that the original packet may have been lost or delayed.

2. Duplicate Acknowledgments (Dup ACKs)

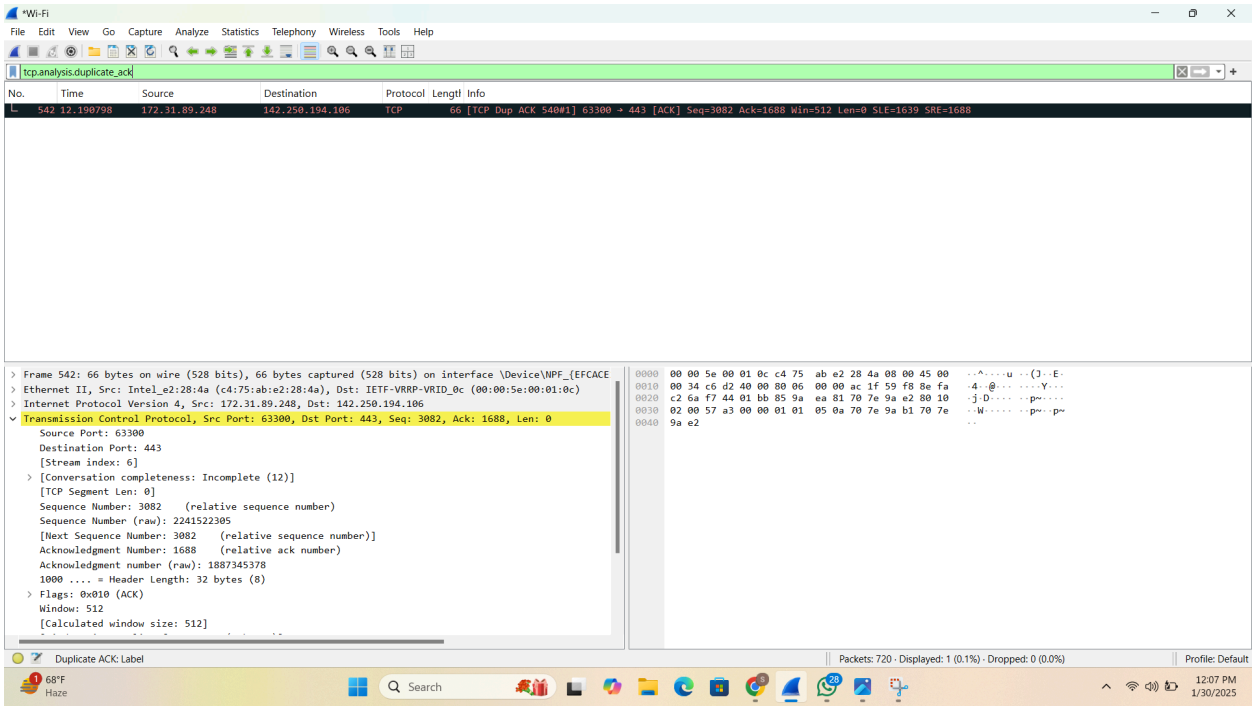
- When a receiver gets an out-of-order segment (because a previous packet was lost), it sends an acknowledgment for the last successfully received packet.
- If the sender receives three consecutive duplicate ACKs, it assumes the missing packet is lost and performs fast retransmission.
- A high number of duplicate ACKs suggests packet loss or network instability.

3. Lost Segments

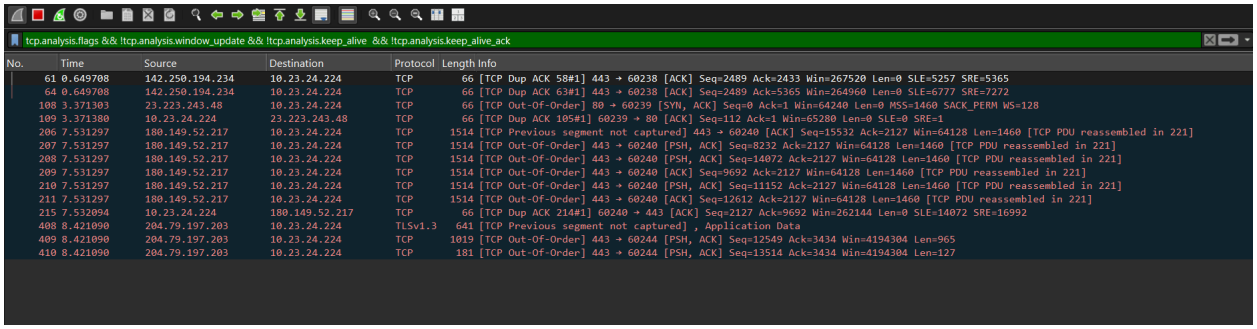
- If a packet is lost in transit (due to congestion or network failure), the sender does not receive an acknowledgment.
- This results in either retransmissions or duplicate ACKs.
- Persistent lost segments can cause slow performance, increased latency, and reduced throughput.



Duplicate Acknowledgment

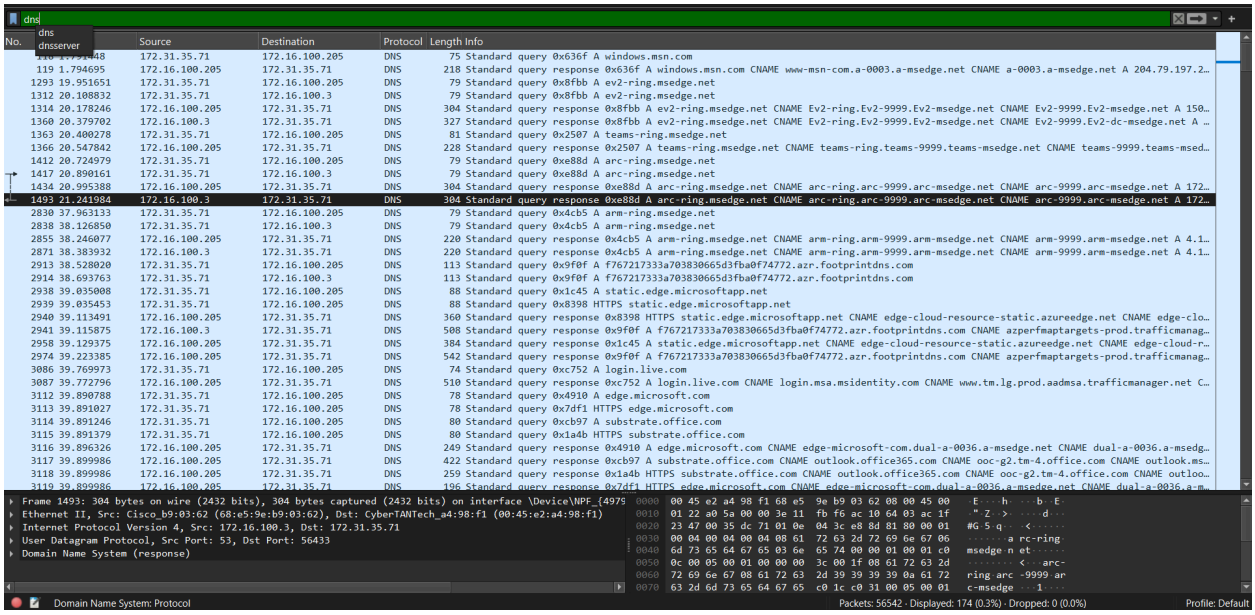


tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ac : Wireshark filter shows TCP packets that are not related to window updates or keep-alive messages. It filters out packets with the *window_update* or *keep_alive* flags, focusing on other types of TCP traffic.

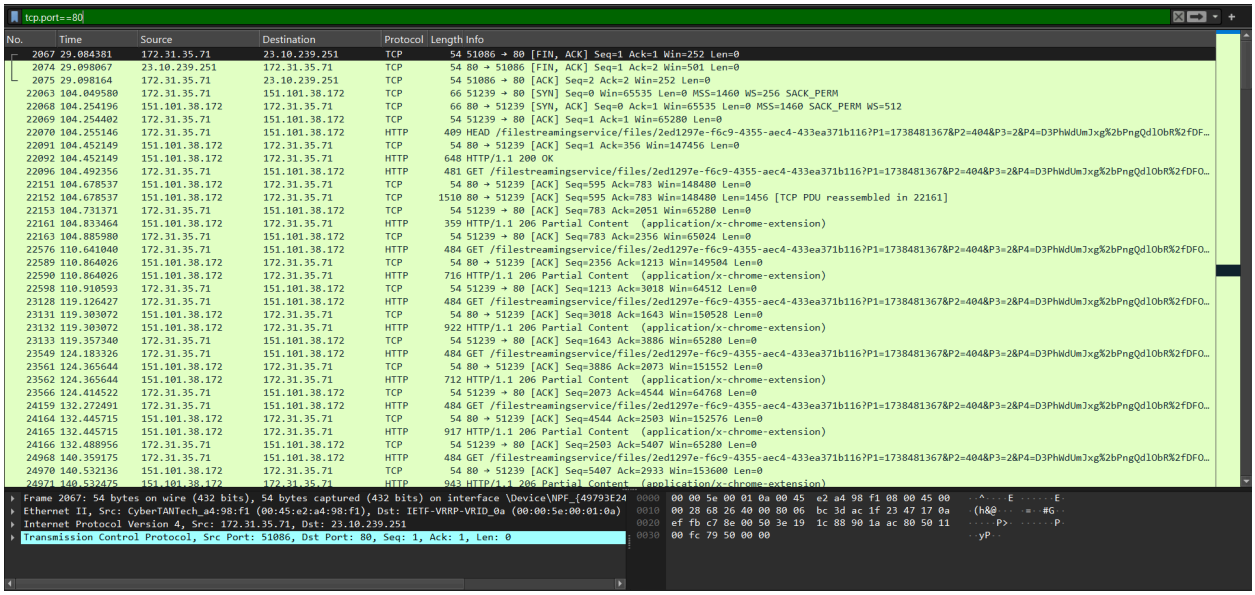


4. Explore at least 5 different filters in Wireshark (https://wiki.wireshark.org/DisplayFilters). Ex. “http” would give you only HTTP traffic.

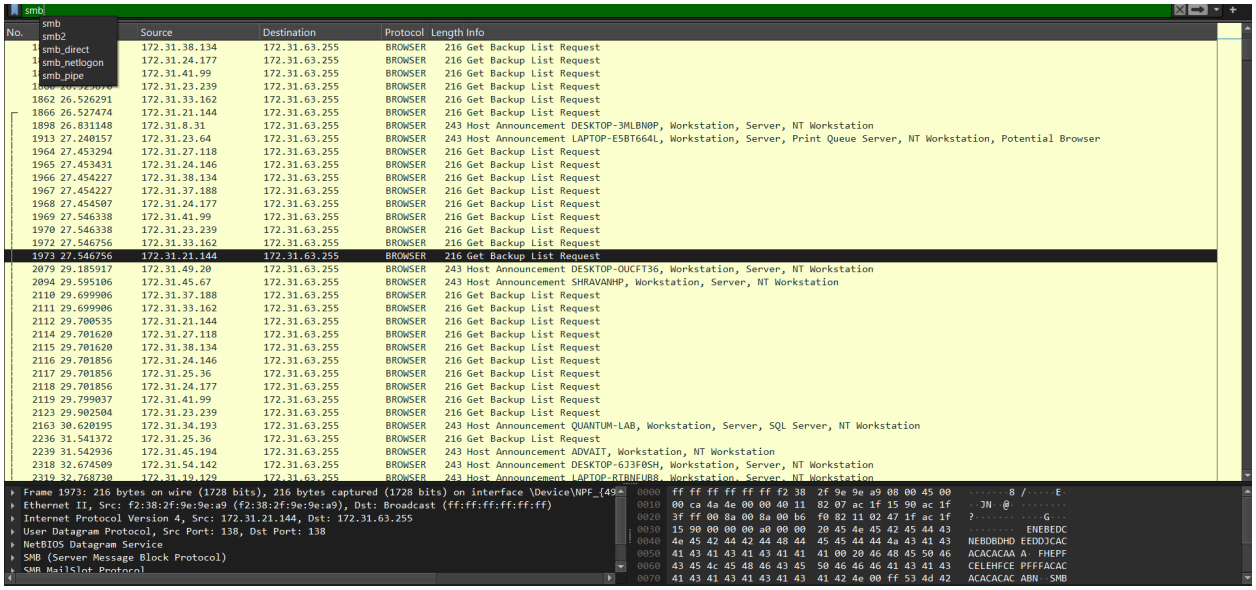
   dns :


dns
dns
dnsserver
No. Source Destination Protocol Length Info
119 1.794695 172.16.100.205 172.31.35.71 DNS 218 Standard query response 0x636f A windows.msn.com CNAME www-msn-com.a-0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.79.197.2…
1293 19.951651 172.31.35.71 172.16.100.205 DNS 79 Standard query 0x8fbb A ev2-ring.msedge.net
1312 20.108832 172.31.35.71 172.16.100.3 DNS 79 Standard query 0x8fbb A ev2-ring.msedge.net
1314 20.178246 172.16.100.205 172.31.35.71 DNS 304 Standard query response 0x8fbb A ev2-ring.msedge.net CNAME Ev2-ring.Ev2-9999.Ev2-msedge.net CNAME Ev2-9999.Ev2-msedge.net A 150…
1360 20.379702 172.16.100.3 172.31.35.71 DNS 327 Standard query response 0x8fbb A ev2-ring.msedge.net CNAME Ev2-ring.Ev2-9999.Ev2-msedge.net CNAME Ev2-9999.Ev2-dc-msedge.net A …
1363 20.400278 172.31.35.71 172.16.100.205 DNS 81 Standard query 0x2507 A teams-ring.msedge.net
1366 20.547842 172.16.100.205 172.31.35.71 DNS 228 Standard query response 0x2507 A teams-ring.msedge.net CNAME teams-ring.teams-9999.teams-msedge.net CNAME teams-9999.teams-msed…
1412 20.724979 172.31.35.71 172.16.100.205 DNS 79 Standard query 0xe88d A arc-ring.msedge.net
1417 20.890161 172.31.35.71 172.16.100.3 DNS 79 Standard query 0xe88d A arc-ring.msedge.net
1434 20.995388 172.16.100.205 172.31.35.71 DNS 304 Standard query response 0xe88d A arc-ring.msedge.net CNAME arc-ring.arc-9999.arc-msedge.net CNAME arc-9999.arc-msedge.net A 172…
1493 21.241934 172.16.100.3 172.31.35.71 DNS 304 Standard query response 0xe88d A arc-ring.msedge.net CNAME arc-ring.arc-9999.arc-msedge.net CNAME arc-9999.arc-msedge.net A 172…
2830 37.963133 172.31.35.71 172.16.100.205 DNS 79 Standard query 0x4cb5 A arm-ring.msedge.net
2838 38.126850 172.31.35.71 172.16.100.3 DNS 79 Standard query 0x4cb5 A arm-ring.msedge.net
2855 38.246077 172.16.100.205 172.31.35.71 DNS 220 Standard query response 0x4cb5 A arm-ring.msedge.net CNAME arm-ring.arm-9999.arm-msedge.net CNAME arm-9999.arm-msedge.net A 4.1…
2871 38.383932 172.16.100.3 172.31.35.71 DNS 220 Standard query response 0x4cb5 A arm-ring.msedge.net CNAME arm-ring.arm-9999.arm-msedge.net CNAME arm-9999.arm-msedge.net A 4.1…
2913 38.528020 172.31.35.71 172.16.100.205 DNS 113 Standard query 0x9f0f A f767217333a703830665d3fba0f74772.azr.footprintdns.com
2914 38.693763 172.31.35.71 172.16.100.3 DNS 113 Standard query 0x9f0f A f767217333a703830665d3fba0f74772.azr.footprintdns.com
2938 39.035008 172.31.35.71 172.16.100.205 DNS 88 Standard query 0x1c45 A static.edge.microsoftapp.net
2939 39.035453 172.31.35.71 172.16.100.205 DNS 88 Standard query 0x8398 HTTPS static.edge.microsoftapp.net
2940 39.113491 172.16.100.205 172.31.35.71 DNS 360 Standard query response 0x8398 HTTPS static.edge.microsoftapp.net CNAME edge-cloud-resource-static.azureedge.net CNAME edge-clo…
2941 39.115875 172.16.100.3 172.31.35.71 DNS 508 Standard query response 0x9f0f A f767217333a703830665d3fba0f74772.azr.footprintdns.com CNAME azperfmaptargets-prod.trafficmanag…
2958 39.129375 172.16.100.205 172.31.35.71 DNS 384 Standard query response 0x1c45 A static.edge.microsoftapp.net CNAME edge-cloud-resource-static.azureedge.net CNAME edge-cloud-r…
2974 39.223385 172.16.100.205 172.31.35.71 DNS 542 Standard query response 0x9f0f A f767217333a703830665d3fba0f74772.azr.footprintdns.com CNAME azperfmaptargets-prod.trafficmanag…
3086 39.769973 172.31.35.71 172.16.100.205 DNS 74 Standard query 0xc752 A login.live.com
3087 39.772796 172.16.100.205 172.31.35.71 DNS 510 Standard query response 0xc752 A login.live.com CNAME login.msa.msidentity.com CNAME www.tm.lg.prod.aadmsa.trafficmanager.net C…
3112 39.890788 172.31.35.71 172.16.100.205 DNS 78 Standard query 0x4910 A edge.microsoft.com
3113 39.891027 172.31.35.71 172.16.100.205 DNS 78 Standard query 0x7df1 HTTPS edge.microsoft.com
3114 39.891246 172.31.35.71 172.16.100.205 DNS 80 Standard query 0xcb97 A substrate.office.com
3115 39.891379 172.31.35.71 172.16.100.205 DNS 80 Standard query 0x1a4b HTTPS substrate.office.com
3116 39.896326 172.16.100.205 172.31.35.71 DNS 249 Standard query response 0x4910 A edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME dual-a-0036.a-msedg…
3117 39.899986 172.16.100.205 172.31.35.71 DNS 422 Standard query response 0xcb97 A substrate.office.com CNAME outlook.office365.com CNAME ooc-g2.tm-4.office.com CNAME outlook.ms…
3118 39.899986 172.16.100.205 172.31.35.71 DNS 259 Standard query response 0x1a4b HTTPS substrate.office.com CNAME outlook.office365.com CNAME ooc-g2.tm-4.office.com CNAME outloo…
3119 39.899986 172.16.100.205 172.31.35.71 DNS 196 Standard query response 0x7df1 HTTPS edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME dual-a-0036.a-m…
Frame 1493: 304 bytes on wire (2432 bits), 304 bytes captured (2432 bits) on interface \Device\NPF_{4975
Ethernet II, Src: Cisco_b9:03:62 (68:e5:9e:b9:03:62), Dst: CyberTANTech_a4:98:f1 (00:45:e2:a4:98:f1)
Internet Protocol Version 4, Src: 172.16.100.3, Dst: 172.31.35.71
User Datagram Protocol, Src Port: 53, Dst Port: 56433
Domain Name System (response)
0000 00 45 e2 a4 98 f1 68 e5 9e b9 03 62 08 00 45 00
0010 01 22 a0 5a 00 00 3e 11 fb f6 ac 10 64 03 ac 1f
0020 23 47 00 35 dc 71 01 0e 04 3c e8 8d 81 80 00 01
0030 00 04 00 04 00 04 08 61 72 63 2d 72 69 6e 67 06
0040 6d 73 65 64 67 65 03 6e 65 74 00 00 01 00 01 c0
0050 0c 00 05 00 01 00 00 00 3c 00 1f 08 61 72 63 2d
0060 72 69 6e 67 08 61 72 63 2d 39 39 39 39 0a 61 72
0070 63 2d 6d 73 65 64 67 65 c0 1c c0 31 00 05 00 01
Domain Name System: Protocol
Packets: 56542 · Displayed: 174 (0.3%) · Dropped: 0 (0.0%)
Profile: Default

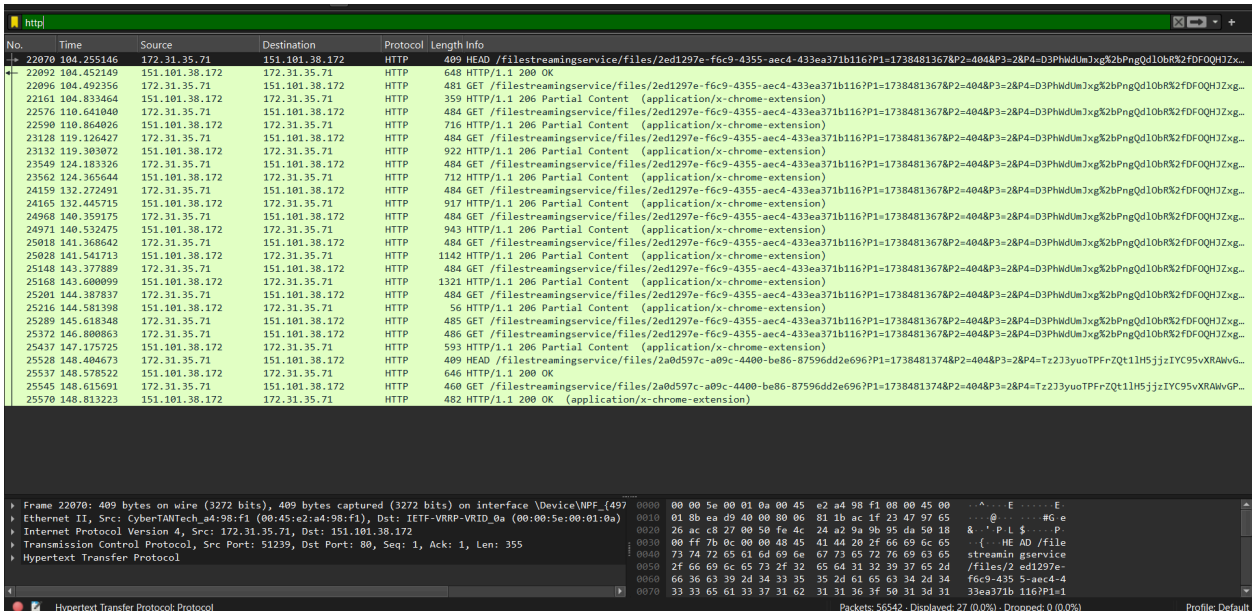
tcp :


tcp.port==80
No. Time Source Destination Protocol Length Info
2067 29.084381 172.31.35.71 23.10.239.251 TCP 54 51086 → 80 [FIN, ACK] Seq=1 Ack=1 Win=252 Len=0
2074 29.098067 23.10.239.251 172.31.35.71 TCP 54 80 → 51086 [FIN, ACK] Seq=1 Ack=2 Win=501 Len=0
2075 29.098164 172.31.35.71 23.10.239.251 TCP 54 51086 → 80 [ACK] Seq=2 Ack=2 Win=252 Len=0
22063 104.049580 172.31.35.71 151.101.38.172 TCP 66 51239 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
22068 104.254196 151.101.38.172 172.31.35.71 TCP 66 80 → 51239 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM WS=512
22069 104.254402 172.31.35.71 151.101.38.172 TCP 54 51239 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
22070 104.255146 172.31.35.71 151.101.38.172 HTTP 409 HEAD /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDF…
22091 104.452149 151.101.38.172 172.31.35.71 TCP 54 80 → 51239 [ACK] Seq=1 Ack=356 Win=147456 Len=0
22092 104.452149 151.101.38.172 172.31.35.71 HTTP 648 HTTP/1.1 200 OK
22096 104.492356 172.31.35.71 151.101.38.172 HTTP 481 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFO…
22151 104.678537 151.101.38.172 172.31.35.71 TCP 54 80 → 51239 [ACK] Seq=595 Ack=783 Win=148480 Len=0
22152 104.678537 151.101.38.172 172.31.35.71 TCP 1510 80 → 51239 [ACK] Seq=595 Ack=783 Win=148480 Len=1456 [TCP PDU reassembled in 22161]
22153 104.731371 172.31.35.71 151.101.38.172 TCP 54 51239 → 80 [ACK] Seq=783 Ack=2051 Win=65280 Len=0
22161 104.833464 151.101.38.172 172.31.35.71 HTTP 359 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
22163 104.885980 172.31.35.71 151.101.38.172 TCP 54 51239 → 80 [ACK] Seq=783 Ack=2356 Win=65024 Len=0
22576 110.641040 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFO…
22589 110.864026 151.101.38.172 172.31.35.71 TCP 54 80 → 51239 [ACK] Seq=2356 Ack=1213 Win=149504 Len=0
22590 110.864026 151.101.38.172 172.31.35.71 HTTP 716 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
22598 110.910593 172.31.35.71 151.101.38.172 TCP 54 51239 → 80 [ACK] Seq=1213 Ack=3018 Win=64512 Len=0
23128 119.126427 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFO…
23131 119.303072 151.101.38.172 172.31.35.71 TCP 54 80 → 51239 [ACK] Seq=3018 Ack=1643 Win=150528 Len=0
23132 119.303072 151.101.38.172 172.31.35.71 HTTP 922 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
23133 119.357340 172.31.35.71 151.101.38.172 TCP 54 51239 → 80 [ACK] Seq=1643 Ack=3886 Win=65280 Len=0
23549 124.183326 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFO…
23561 124.365644 151.101.38.172 172.31.35.71 TCP 54 80 → 51239 [ACK] Seq=3886 Ack=2073 Win=151552 Len=0
23562 124.365644 151.101.38.172 172.31.35.71 HTTP 712 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
23566 124.414522 172.31.35.71 151.101.38.172 TCP 54 51239 → 80 [ACK] Seq=2073 Ack=4544 Win=64768 Len=0
24159 132.272491 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFO…
24164 132.445715 151.101.38.172 172.31.35.71 TCP 54 80 → 51239 [ACK] Seq=4544 Ack=2503 Win=152576 Len=0
24165 132.445715 151.101.38.172 172.31.35.71 HTTP 917 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
24166 132.488956 172.31.35.71 151.101.38.172 TCP 54 51239 → 80 [ACK] Seq=2503 Ack=5407 Win=65280 Len=0
24968 140.359175 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFO…
24970 140.532136 151.101.38.172 172.31.35.71 TCP 54 80 → 51239 [ACK] Seq=5407 Ack=2933 Win=153600 Len=0
24971 140.532475 151.101.38.172 172.31.35.71 HTTP 943 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
Frame 2067: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{49793E24
Ethernet II, Src: CyberTANTech_a4:98:f1 (00:45:e2:a4:98:f1), Dst: IETF-VRRP-VRID_0a (00:00:5e:00:01:0a)
Internet Protocol Version 4, Src: 172.31.35.71, Dst: 23.10.239.251
Transmission Control Protocol, Src Port: 51086, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 00 00 5e 00 01 0a 00 45 e2 a4 98 f1 08 00 45 00
0010 00 28 68 26 40 00 80 06 bc 3d ac 1f 23 47 17 0a
0020 ef fb c7 8e 00 50 3e 19 1c 88 90 1a ac 80 50 11
0030 00 fc 79 50 00 00

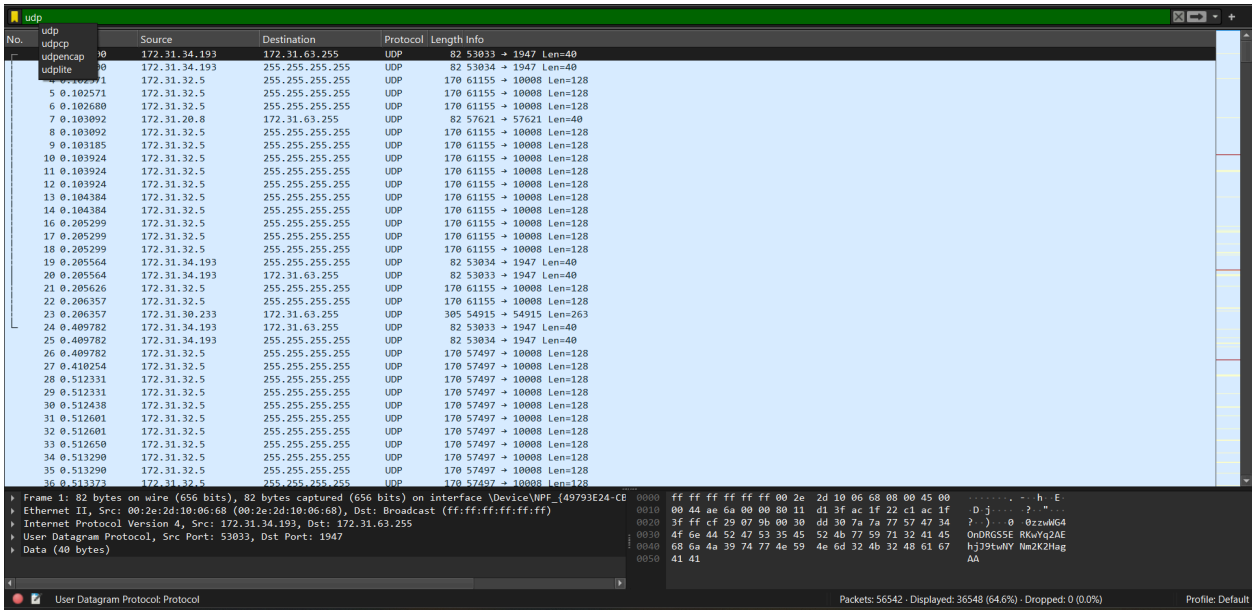
smb :


smb
smb
smb2
smb_direct
smb_netlogon
smb_pipe
No. Source Destination Protocol Length Info
1862 26.526291 172.31.33.162 172.31.63.255 BROWSER 216 Get Backup List Request
1866 26.527474 172.31.21.144 172.31.63.255 BROWSER 216 Get Backup List Request
1898 26.831148 172.31.8.31 172.31.63.255 BROWSER 243 Host Announcement DESKTOP-3MLBN0P, Workstation, Server, NT Workstation
1913 27.240157 172.31.23.64 172.31.63.255 BROWSER 243 Host Announcement LAPTOP-E5BT664L, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser
1964 27.453294 172.31.27.118 172.31.63.255 BROWSER 216 Get Backup List Request
1965 27.453431 172.31.24.146 172.31.63.255 BROWSER 216 Get Backup List Request
1966 27.454227 172.31.38.134 172.31.63.255 BROWSER 216 Get Backup List Request
1967 27.454227 172.31.37.188 172.31.63.255 BROWSER 216 Get Backup List Request
1968 27.454507 172.31.24.177 172.31.63.255 BROWSER 216 Get Backup List Request
1969 27.546338 172.31.41.99 172.31.63.255 BROWSER 216 Get Backup List Request
1970 27.546338 172.31.23.239 172.31.63.255 BROWSER 216 Get Backup List Request
1972 27.546756 172.31.33.162 172.31.63.255 BROWSER 216 Get Backup List Request
1973 27.546756 172.31.21.144 172.31.63.255 BROWSER 216 Get Backup List Request
2079 29.185917 172.31.49.20 172.31.63.255 BROWSER 243 Host Announcement DESKTOP-OUCFT36, Workstation, Server, NT Workstation
2094 29.595106 172.31.45.67 172.31.63.255 BROWSER 243 Host Announcement SHRAVANHP, Workstation, Server, NT Workstation
2110 29.699906 172.31.37.188 172.31.63.255 BROWSER 216 Get Backup List Request
2111 29.699906 172.31.33.162 172.31.63.255 BROWSER 216 Get Backup List Request
2112 29.700535 172.31.21.144 172.31.63.255 BROWSER 216 Get Backup List Request
2114 29.701620 172.31.27.118 172.31.63.255 BROWSER 216 Get Backup List Request
2115 29.701620 172.31.38.134 172.31.63.255 BROWSER 216 Get Backup List Request
2116 29.701856 172.31.24.146 172.31.63.255 BROWSER 216 Get Backup List Request
2117 29.701856 172.31.25.36 172.31.63.255 BROWSER 216 Get Backup List Request
2118 29.701856 172.31.24.177 172.31.63.255 BROWSER 216 Get Backup List Request
2119 29.799037 172.31.41.99 172.31.63.255 BROWSER 216 Get Backup List Request
2123 29.902504 172.31.23.239 172.31.63.255 BROWSER 216 Get Backup List Request
2163 30.620195 172.31.34.193 172.31.63.255 BROWSER 243 Host Announcement QUANTUM-LAB, Workstation, Server, SQL Server, NT Workstation
2236 31.541372 172.31.25.36 172.31.63.255 BROWSER 216 Get Backup List Request
2239 31.542936 172.31.45.194 172.31.63.255 BROWSER 243 Host Announcement ADVAIT, Workstation, NT Workstation
2318 32.674509 172.31.54.142 172.31.63.255 BROWSER 243 Host Announcement DESKTOP-6J3F05H, Workstation, Server, NT Workstation
2319 32.768730 172.31.19.129 172.31.63.255 BROWSER 243 Host Announcement LAPTOP-RTBNEUB8, Workstation, Server, NT Workstation
Frame 1973: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{49
Ethernet II, Src: f2:38:2f:9e:9e:a9 (f2:38:2f:9e:9e:a9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 172.31.21.144, Dst: 172.31.63.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
0000 ff ff ff ff ff ff f2 38 2f 9e 9e a9 08 00 45 00 ·····8 /·····E
0010 00 ca 4a 4e 00 00 40 11 82 07 ac 1f 15 90 ac 1f ··JN··@· ····
0020 3f ff 00 8a 00 8a 00 b6 f0 82 11 02 47 1f ac 1f ?····· ····G···
0030 15 90 00 00 00 00 a0 00 00 20 45 4e 45 42 45 44 43 ····· ENEBEDC
0040 4e 45 42 44 42 44 48 44 45 45 44 44 4a 43 41 43 NEBDBDHD EEDDJCAC
0050 41 43 41 43 41 43 41 41 41 00 20 46 48 45 50 46 ACACACAA A· FHEPF
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43 CELEHFCE PFFFACAC
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 4d 42 ACACACAC ABN··SMB

http :

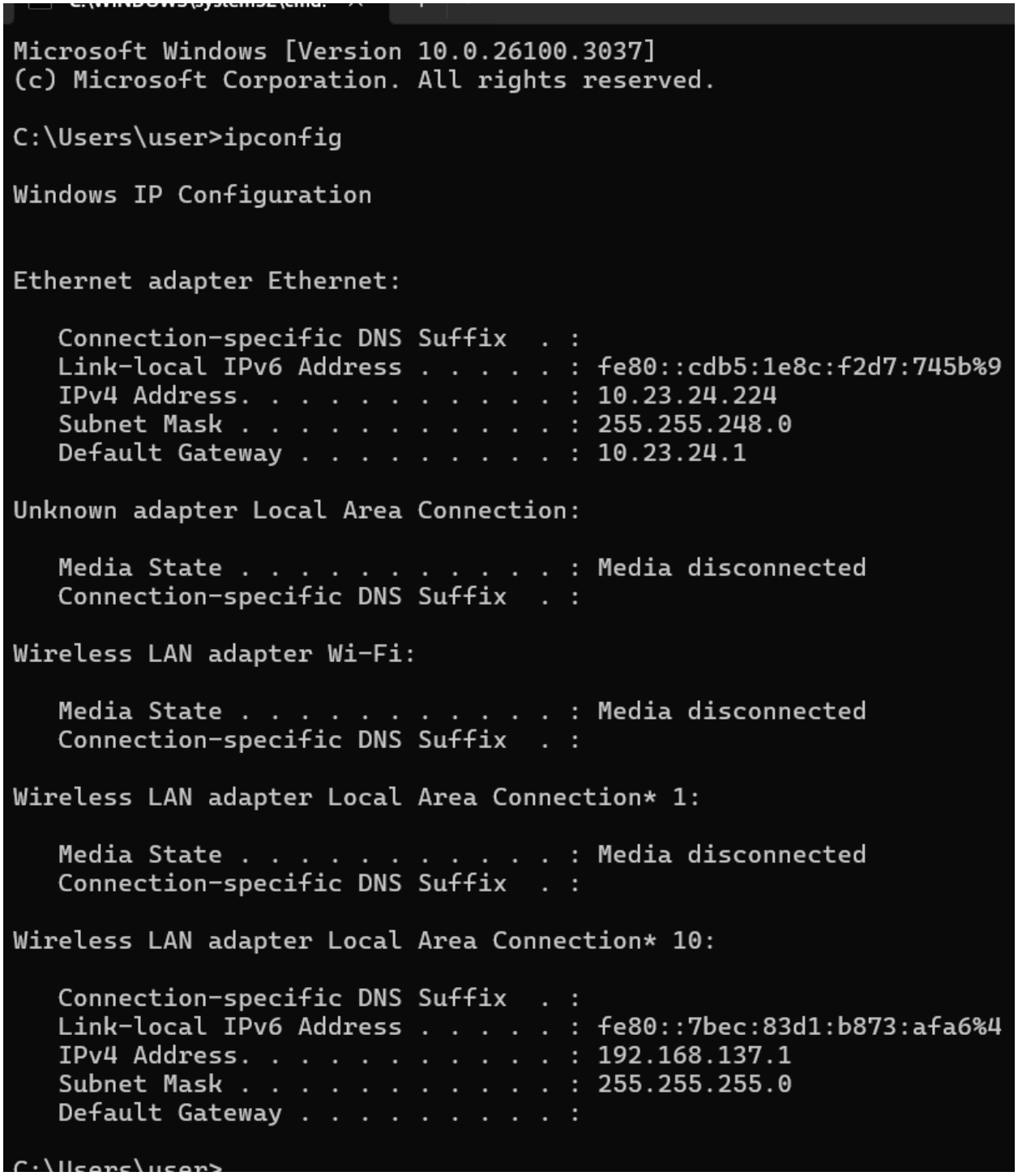

http
No. Time Source Destination Protocol Length Info
22070 104.255146 172.31.35.71 151.101.38.172 HTTP 409 HEAD /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZx…
22092 104.452149 151.101.38.172 172.31.35.71 HTTP 648 HTTP/1.1 200 OK
22096 104.492356 172.31.35.71 151.101.38.172 HTTP 481 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
22161 104.833464 151.101.38.172 172.31.35.71 HTTP 359 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
22576 110.641040 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
22590 110.864026 151.101.38.172 172.31.35.71 HTTP 716 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
23128 119.126427 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
23132 119.303072 151.101.38.172 172.31.35.71 HTTP 922 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
23549 124.183326 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
23562 124.365644 151.101.38.172 172.31.35.71 HTTP 712 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
24159 132.272491 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
24165 132.445715 151.101.38.172 172.31.35.71 HTTP 917 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
24968 140.359175 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
24971 140.532475 151.101.38.172 172.31.35.71 HTTP 943 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
25018 141.368642 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
25028 141.541713 151.101.38.172 172.31.35.71 HTTP 1142 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
25148 143.377889 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
25168 143.600099 151.101.38.172 172.31.35.71 HTTP 1321 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
25201 144.387837 172.31.35.71 151.101.38.172 HTTP 484 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
25216 144.581398 151.101.38.172 172.31.35.71 HTTP 56 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
25289 145.618348 172.31.35.71 151.101.38.172 HTTP 485 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
25372 146.800863 172.31.35.71 151.101.38.172 HTTP 486 GET /filestreamingservice/files/2ed1297e-f6c9-4355-aec4-433ea371b116?P1=1738481367&P2=404&P3=2&P4=D3PhWdUmJxg%2bPngQdlObR%2fDFOQHJZxg…
25437 147.175725 151.101.38.172 172.31.35.71 HTTP 593 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
25528 148.404673 172.31.35.71 151.101.38.172 HTTP 409 HEAD /filestreamingservice/files/2a0d597c-a09c-4400-be86-87596dd2e696?P1=1738481374&P2=404&P3=2&P4=Tz2J3yuoTPFrZQt1lH5jjzIYC95vXRAWvG…
25537 148.578522 151.101.38.172 172.31.35.71 HTTP 646 HTTP/1.1 200 OK
25545 148.615691 172.31.35.71 151.101.38.172 HTTP 460 GET /filestreamingservice/files/2a0d597c-a09c-4400-be86-87596dd2e696?P1=1738481374&P2=404&P3=2&P4=Tz2J3yuoTPFrZQt1lH5jjzIYC95vXRAWvGP…
25570 148.813223 151.101.38.172 172.31.35.71 HTTP 482 HTTP/1.1 200 OK (application/x-chrome-extension)
Frame 22070: 409 bytes on wire (3272 bits), 409 bytes captured (3272 bits) on interface \Device\NPF_{497
Ethernet II, Src: CyberTANTech_a4:98:f1 (00:45:e2:a4:98:f1), Dst: IETF-VRRP-VRID_0a (00:00:5e:00:01:0a)
Internet Protocol Version 4, Src: 172.31.35.71, Dst: 151.101.38.172
Transmission Control Protocol, Src Port: 51239, Dst Port: 80, Seq: 1, Ack: 1, Len: 355
Hypertext Transfer Protocol
0000 00 00 5e 00 01 0a 00 45 e2 a4 98 f1 08 00 45 00 ··^····E ·····E·
0010 01 8b ea d9 40 00 80 06 81 1b ac 1f 23 47 97 65 ····@··· ····#G·e
0020 26 ac c8 27 00 50 fe 4c 24 a2 9a 9b 95 da 50 18 &··'·P·L $·····P·
0030 00 ff 7b 0c 00 00 48 45 41 44 20 2f 66 69 6c 65 ··{···HE AD /file
0040 73 74 72 65 61 6d 69 6e 67 73 65 72 76 69 63 65 streamin gservice
0050 2f 66 69 6c 65 73 2f 32 65 64 31 32 39 37 65 2d /files/2 ed1297e-
0060 66 36 63 39 2d 34 33 35 35 2d 61 65 63 34 2d 34 f6c9-435 5-aec4-4
0070 33 33 65 61 33 37 31 62 31 31 36 3f 50 31 3d 31 33ea371b 116?P1=1
Hypertext Transfer Protocol Protocol
Packets: 56542 · Displayed: 27 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

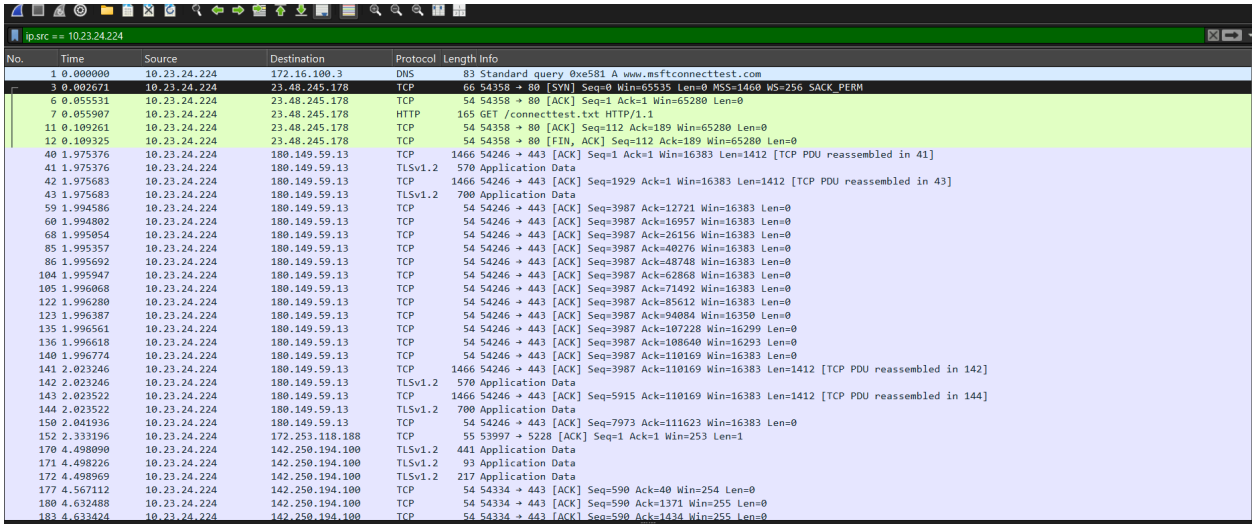
udp :



5. What is the filter command for listing all outgoing traffic?

```
ip.src == your_IP (IP address of the device in use)
```


Microsoft Windows [Version 10.0.26100.3037]
(c) Microsoft Corporation. All rights reserved.
C:\Users\user>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::cdb5:1e8c:f2d7:745b%9
IPv4 Address. . . . . : 10.23.24.224
Subnet Mask . . . . . : 255.255.248.0
Default Gateway . . . . . : 10.23.24.1
Unknown adapter Local Area Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 10:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::7bec:83d1:b873:afa6%4
IPv4 Address. . . . . : 192.168.137.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
C:\Users\user>

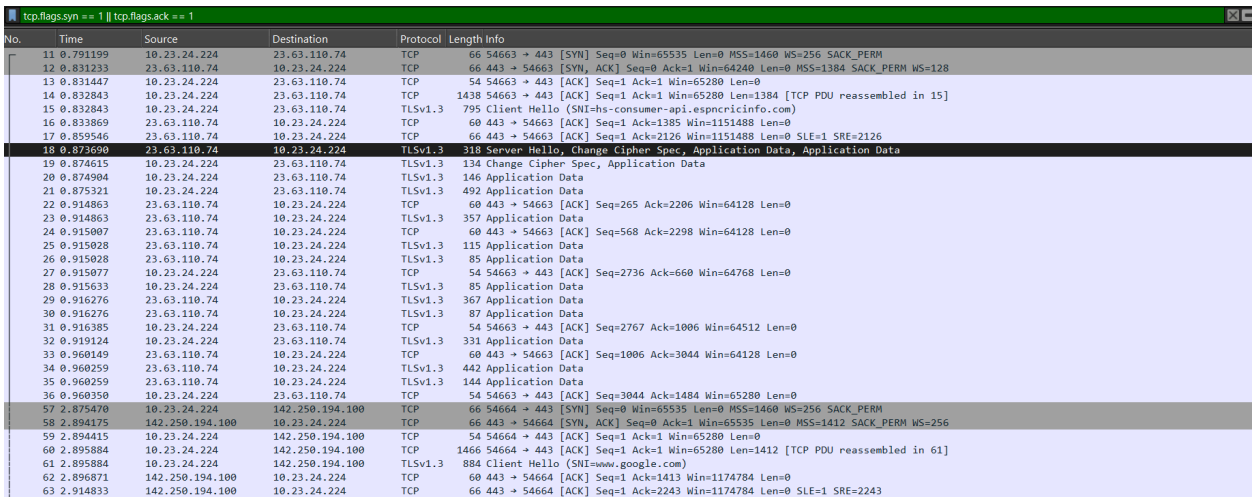


ip.src == 10.23.24.224

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.23.24.224	172.16.100.3	DNS	83	Standard query 0xe581 A www.msftconnecttest.com
3	0.002671	10.23.24.224	23.48.245.178	TCP	66	54358 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
6	0.055531	10.23.24.224	23.48.245.178	TCP	54	54358 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
7	0.055907	10.23.24.224	23.48.245.178	HTTP	165	GET /connecttest.txt HTTP/1.1
11	0.109261	10.23.24.224	23.48.245.178	TCP	54	54358 → 80 [ACK] Seq=112 Ack=189 Win=65280 Len=0
12	0.109325	10.23.24.224	23.48.245.178	TCP	54	54358 → 80 [FIN, ACK] Seq=112 Ack=189 Win=65280 Len=0
40	1.975376	10.23.24.224	180.149.59.13	TCP	1466	54246 → 443 [ACK] Seq=1 Ack=1 Win=16383 Len=1412 [TCP PDU reassembled in 41]
41	1.975376	10.23.24.224	180.149.59.13	TLSv1.2	570	Application Data
42	1.975683	10.23.24.224	180.149.59.13	TCP	1466	54246 → 443 [ACK] Seq=1929 Ack=1 Win=16383 Len=1412 [TCP PDU reassembled in 43]
43	1.975683	10.23.24.224	180.149.59.13	TLSv1.2	700	Application Data
59	1.994586	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=12721 Win=16383 Len=0
60	1.994802	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=16957 Win=16383 Len=0
68	1.995054	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=26156 Win=16383 Len=0
85	1.995357	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=40276 Win=16383 Len=0
86	1.995692	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=48748 Win=16383 Len=0
104	1.995947	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=62868 Win=16383 Len=0
105	1.996068	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=71492 Win=16383 Len=0
122	1.996280	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=85612 Win=16383 Len=0
123	1.996387	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=94084 Win=16350 Len=0
135	1.996561	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=107228 Win=16299 Len=0
136	1.996618	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=108640 Win=16293 Len=0
140	1.996774	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=3987 Ack=110169 Win=16383 Len=0
141	2.023246	10.23.24.224	180.149.59.13	TCP	1466	54246 → 443 [ACK] Seq=3987 Ack=110169 Win=16383 Len=1412 [TCP PDU reassembled in 142]
142	2.023246	10.23.24.224	180.149.59.13	TLSv1.2	570	Application Data
143	2.023522	10.23.24.224	180.149.59.13	TCP	1466	54246 → 443 [ACK] Seq=5915 Ack=110169 Win=16383 Len=1412 [TCP PDU reassembled in 144]
144	2.023522	10.23.24.224	180.149.59.13	TLSv1.2	700	Application Data
150	2.041936	10.23.24.224	180.149.59.13	TCP	54	54246 → 443 [ACK] Seq=7973 Ack=111623 Win=16383 Len=0
152	2.333196	10.23.24.224	172.253.118.188	TCP	55	53997 → 5228 [ACK] Seq=1 Ack=1 Win=253 Len=1
170	4.498090	10.23.24.224	142.250.194.100	TLSv1.2	441	Application Data
171	4.498226	10.23.24.224	142.250.194.100	TLSv1.2	93	Application Data
172	4.498969	10.23.24.224	142.250.194.100	TLSv1.2	217	Application Data
177	4.567112	10.23.24.224	142.250.194.100	TCP	54	54334 → 443 [ACK] Seq=590 Ack=40 Win=254 Len=0
180	4.632488	10.23.24.224	142.250.194.100	TCP	54	54334 → 443 [ACK] Seq=590 Ack=1371 Win=255 Len=0
183	4.633424	10.23.24.224	142.250.194.100	TCP	54	54334 → 443 [ACK] Seq=590 Ack=1434 Win=255 Len=0

6. Start a new packet capture to now visit an external website, say www.cricinfo.com. Can you show the 3-way TCP handshake happening? Can you see your IITJ proxy in between? What is its IP address?

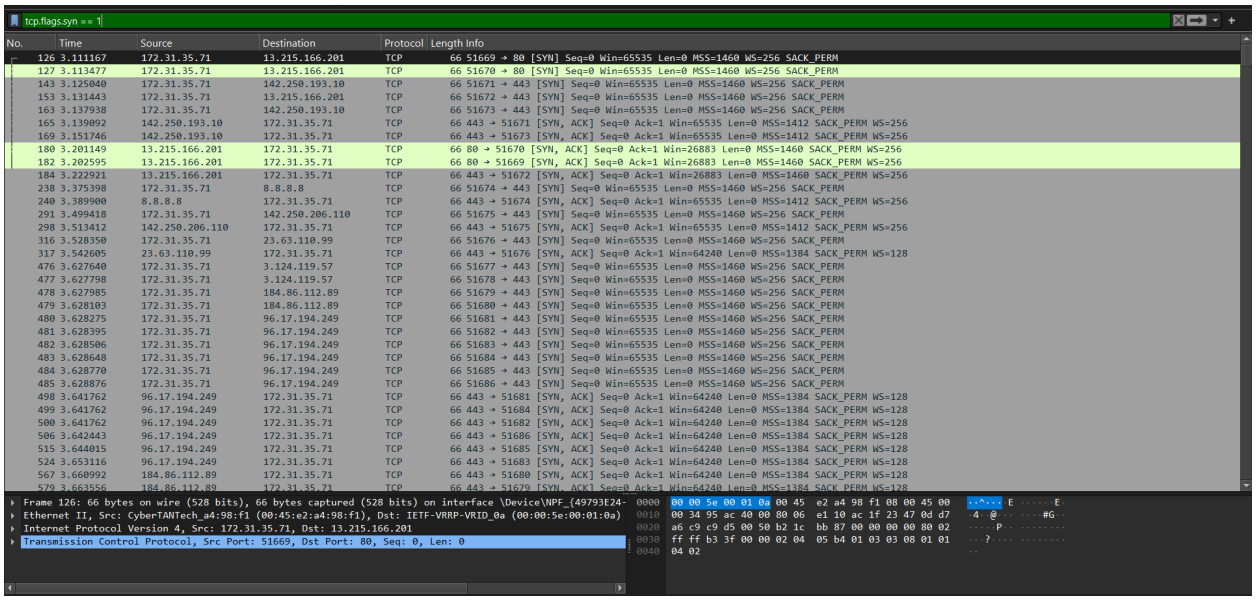
tcp.flags.syn == 1 || tcp.flags.ack == 1 : This filter is used in Wireshark to capture packets involved in the TCP 3-way handshake by focusing on SYN and ACK flags.



tcp.flags.syn == 1 || tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length	Info
11	0.791199	10.23.24.224	23.63.110.74	TCP	66	54663 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
12	0.831233	23.63.110.74	10.23.24.224	TCP	66	443 → 54663 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
13	0.831447	10.23.24.224	23.63.110.74	TCP	54	54663 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
14	0.832843	10.23.24.224	23.63.110.74	TCP	1438	54663 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1384 [TCP PDU reassembled in 15]
15	0.832843	10.23.24.224	23.63.110.74	TLSv1.3	795	Client Hello (SNI=hs-consumer-api.espncricinfo.com)
16	0.833869	23.63.110.74	10.23.24.224	TCP	60	443 → 54663 [ACK] Seq=1 Ack=1385 Win=1151488 Len=0
17	0.859546	23.63.110.74	10.23.24.224	TCP	66	443 → 54663 [ACK] Seq=1 Ack=2126 Win=1151488 Len=0 SLE=1 SRE=2126
18	0.873690	23.63.110.74	10.23.24.224	TLSv1.3	318	Server Hello, Change Cipher Spec, Application Data, Application Data
19	0.874615	10.23.24.224	23.63.110.74	TLSv1.3	134	Change Cipher Spec, Application Data
20	0.874904	10.23.24.224	23.63.110.74	TLSv1.3	146	Application Data
21	0.875321	10.23.24.224	23.63.110.74	TLSv1.3	492	Application Data
22	0.914863	23.63.110.74	10.23.24.224	TCP	60	443 → 54663 [ACK] Seq=265 Ack=2206 Win=64128 Len=0
23	0.914863	23.63.110.74	10.23.24.224	TLSv1.3	357	Application Data
24	0.915007	23.63.110.74	10.23.24.224	TCP	60	443 → 54663 [ACK] Seq=568 Ack=2298 Win=64128 Len=0
25	0.915028	23.63.110.74	10.23.24.224	TLSv1.3	115	Application Data
26	0.915028	23.63.110.74	10.23.24.224	TLSv1.3	85	Application Data
27	0.915077	10.23.24.224	23.63.110.74	TCP	54	54663 → 443 [ACK] Seq=2736 Ack=660 Win=64768 Len=0
28	0.915633	10.23.24.224	23.63.110.74	TLSv1.3	85	Application Data
29	0.916276	23.63.110.74	10.23.24.224	TLSv1.3	367	Application Data
30	0.916276	23.63.110.74	10.23.24.224	TLSv1.3	87	Application Data
31	0.916385	10.23.24.224	23.63.110.74	TCP	54	54663 → 443 [ACK] Seq=2767 Ack=1006 Win=64512 Len=0
32	0.919124	10.23.24.224	23.63.110.74	TLSv1.3	331	Application Data
33	0.960149	23.63.110.74	10.23.24.224	TCP	60	443 → 54663 [ACK] Seq=1006 Ack=3044 Win=64128 Len=0
34	0.960259	23.63.110.74	10.23.24.224	TLSv1.3	442	Application Data
35	0.960259	23.63.110.74	10.23.24.224	TLSv1.3	144	Application Data
36	0.960350	10.23.24.224	23.63.110.74	TCP	54	54663 → 443 [ACK] Seq=3044 Ack=1484 Win=65280 Len=0
57	2.875470	10.23.24.224	142.250.194.100	TCP	66	54664 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
58	2.894175	142.250.194.100	10.23.24.224	TCP	66	443 → 54664 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
59	2.894415	10.23.24.224	142.250.194.100	TCP	54	54664 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
60	2.895884	10.23.24.224	142.250.194.100	TCP	1466	54664 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1412 [TCP PDU reassembled in 61]
61	2.895884	10.23.24.224	142.250.194.100	TLSv1.3	884	Client Hello (SNI=www.google.com)
62	2.896871	142.250.194.100	10.23.24.224	TCP	60	443 → 54664 [ACK] Seq=1 Ack=1413 Win=1174784 Len=0
63	2.914833	142.250.194.100	10.23.24.224	TCP	66	443 → 54664 [ACK] Seq=1 Ack=2243 Win=1174784 Len=0 SLE=1 SRE=2243

Syn packets :



7. Why does DNS follow the UDP stream while HTTP follows the TCP stream?

DNS primarily relies on UDP because it allows for faster query resolution. Since DNS lookups involve small request-and-response messages, using UDP keeps things lightweight and efficient. UDP doesn't require a handshake to establish a connection, reducing latency. Additionally, occasional packet loss is generally acceptable because DNS clients can simply resend the request if needed.

On the other hand, HTTP uses TCP to ensure reliable and ordered delivery of web content. Web pages include various elements like HTML, CSS, and JavaScript, all of which must arrive in the correct sequence to render properly. TCP's three-way handshake and error correction mechanisms make it ideal for delivering web content without corruption or missing data.

8. Execute the socket program (both server and client) to demonstrate TCP communication on different ports. Capture the network packets using Wireshark and analyze them to justify the communication process.

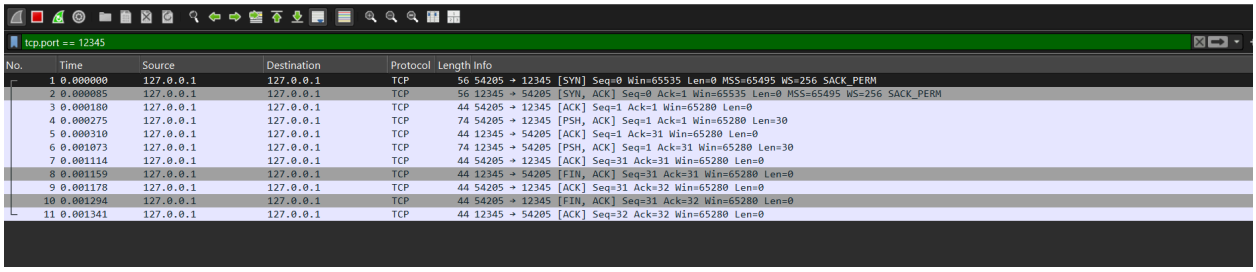
This Wireshark capture documents a local TCP connection (127.0.0.1) between the client (source port 47194) and the server (destination port 12345), demonstrating a standard TCP communication flow.

1. **Packets 6 & 8:** The client transmits application-layer data using **PSH, ACK** flags, ensuring immediate processing by the server. The **ACK** confirms receipt of previous segments.
2. **Packets 7 & 9:** The server acknowledges the client's data transmission with dedicated **ACK** segments, maintaining TCP's reliability mechanism.
3. **Packet 10:** The server initiates a **graceful connection termination** by sending a **FIN, ACK**, signaling that no further data will be transmitted.
4. **Packet 11:** The client responds with an **ACK**, formally completing the **four-way termination handshake**, adhering to TCP's standard teardown procedure.

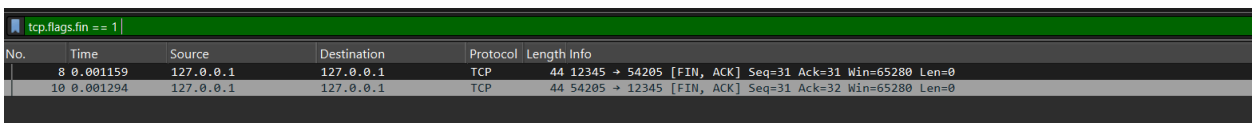
The communication sequence follows the expected **TCP lifecycle**, including **connection establishment, reliable data transfer, and an orderly termination**. Additionally, the **TCP Timestamps (TSval, TSecr)** provide temporal markers, aiding in round-trip time (RTT) analysis and delay assessment.

Note: The client-server architecture was pre-configured in a prior lab session.

tcp.port == 12345 : This filter isolates all TCP packets where either the source or destination port is 12345.



tcp.flags.fin == 1 : This filter captures TCP FIN (Finish) packets, which indicate a connection termination request.



tcp.flags.syn == 1 || tcp.flags.ack == 1 : This filter captures:

- SYN (Synchronization) packets: Used in TCP's three-way handshake to establish a connection.
- ACK (Acknowledgment) packets: Sent to confirm receipt of data.