

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
3/15/2024

Apply a display filter <Ctrl>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xa3d35b63
2	0.000282	fe80::dead:ca3b::6e3c	fe80::112:1:2	DHCPv6	156	Solicit XID: 0xa0507fc CID: 000100012cda8c3a6c3c8c5a6e0
3	0.210213	172.17.170.151	192.170.24.170	UDP	71	58507 > 443 Len=29
4	0.250603	192.170.24.170	172.17.170.151	UDP	68	443 > 58507 Len=26
5	0.273534	Del1_30_cid	Broadcast	ARP	60	ARP Announcement for 172.17.170.43
6	0.277383	fe80::307d:65c8::ce7c	ff02::1:6	ICMPv6	90	Multicast Listener Report Message v2
7	0.277383	fe80::307d:65c8::ce7c	ff02::1:6	ICMPv6	90	Multicast Listener Report Message v2
8	0.277450	172.17.170.43	224.0.0.22	ICMPv3	60	Membership Report / Leave group 224.0.0.252
9	0.277450	172.17.170.43	224.0.0.22	ICMPv3	60	Membership Report / Leave group 224.0.0.251
10	0.286134	fe80::307d:65c8::ce7c	ff02::1:6	ICMPv6	110	Multicast Listener Report Message v2
11	0.286138	172.17.170.43	224.0.0.22	ICMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
12	0.286138	172.17.170.43	224.0.0.22	ICMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
13	0.286879	172.17.170.142	224.0.0.251	NDNS	118	Standard query response 0x0000 AAAA fe80::4ea2:e6f:cb64:2292 A 172.17.170.142
14	0.286879	172.17.170.151	224.0.0.251	NDNS	118	Standard query response 0x0000 AAAA fe80::f127:6504:7892:1657 A 172.17.170.151
15	0.286879	172.17.170.43	224.0.0.252	NDNS	74	Standard query 0x0000 ANY Rawul-AID-PC-1
16	0.286879	fe80::6790:21ed::b0b6	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::6790:21ed:b0b6:3264 A 172.17.170.137
17	0.286933	172.17.170.43	224.0.0.251	NDNS	80	Standard query 0x0000 ANY Rawul-AID-PC-1.local, "Q" question
18	0.286933	fe80::307d:65c8::ce7c	ff02::fb	NDNS	100	Standard query 0x0000 ANY Rawul-AID-PC-1.local, "Q" question
19	0.286933	172.17.170.137	224.0.0.251	NDNS	118	Standard query response 0x0000 AAAA fe80::7330:cf2:c17:4174 A 172.17.170.139
20	0.286933	fe80::307d:65c8::ce7c	ff02::1:3	LLMNR	94	Standard query 0x0000 ANY Rawul-AID-PC-1
21	0.286933	172.17.170.137	224.0.0.251	NDNS	118	Standard query response 0x0000 AAAA fe80::6790:21ed:b0b6:3264 A 172.17.170.137
22	0.287216	fe80::4ea2:e6f:cb64::f2	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::4ea2:e6f:cb64:2292 A 172.17.170.142
23	0.287316	fe80::7330:cf2:c17::f2	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::7330:cf2:c17:4174 A 172.17.170.139
24	0.287316	172.17.170.150	224.0.0.251	NDNS	118	Standard query response 0x0000 AAAA fe80::1929:7fff:1416:3087 A 172.17.170.150
25	0.287316	fe80::307d:65c8::f748	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::307d:65c8:f748:1647 A 172.17.170.165
26	0.287316	fe80::1902:a:fae4:379a::f2	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::1902:a:fae4:379a:1563 A 172.17.170.160
27	0.287316	fe80::1406:dd0:7f:b51:f56f::f2	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::1406:dd0:7f:b51:f56f A 172.17.170.162
28	0.287316	fe80::4096:f039:165:cccc::f2	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::4096:f039:165:cccc A 172.17.170.159
29	0.287316	fe80::5103:ead3:ff:1647::f2	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::5103:ead3:ff:1647 A 172.17.170.165
30	0.287316	fe80::c80d:60ac:7564:4089::f2	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::c80d:60ac:7564:4089 A 169.254.125.218
31	0.287316	fe80::1085:2d:7a:1068::f2	ff02::fb	NDNS	138	Standard query response 0x0000 AAAA fe80::1085:2d:7a:1068 A 172.17.170.161

Frame 11: 343 bytes on wire (2744 bits), 343 bytes captured (2744 bits) on Interface User-VNMP_156050803-F04E-0585-1752522603FE, Id 0

Ethernet II, Src: Dell_SaTei6a (6c3c8c5a6e0a), Dst:

2. Search for 'gmail' on the internet and log in to your account.

Done

3. Stop capturing the traffic and display 'http' traffic. Then search for tcp and dns too.

The image shows a Wireshark network traffic capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions. The main display area shows a list of captured packets, with the first packet selected. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
8334	66.478247	172.17.170.151	192.229.221.95	HTTP	294	GET /_PEwTzBNFEwSTa38gurDgKcGgUAB8Q50otckX2fH8Zt1N28z8SIP17WEWwDlQQUT11U181V5uJmSgK2f6K2BkS7QYXjkCEAN5skKVVW8d36uH13012Wk30 HTTP/1.1
8348	66.679118	192.229.221.95	172.17.170.151	OCSP	791	Response
8592	71.276238	172.17.170.151	192.229.221.95	HTTP	294	GET /_PEwTzBNFEwSTa38gurDgKcGgUAB8Q50otckX2fH8Zt1N28z8SIP17WEWwDlQQUT11U181V5uJmSgK2f6K2BkS7QYXjkCEAN5skKVVW8d36uH13012Wk30 HTTP/1.1
8598	71.570716	192.229.221.95	172.17.170.151	OCSP	791	Response
28231	127.572524	172.17.170.151	178.79.238.128	HTTP	300	GET /msdownload/update/v3/static/trusted/en/pinrulesstl.cab?0f29b0526c915159 HTTP/1.1
28234	127.698721	178.79.238.128	172.17.170.151	HTTP	353	HTTP/1.1 304 Not Modified

The packet details pane shows the selected packet (Frame 8334) with the following information:

- Frame 8334: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{5605E883-FDAE-4D5E-8B35-27525269C3F0}, Id 0
- Ethernet II, Src: Dell_00:10:10:05 (6c:3c:8c:4b:10:05), Dst: Realtek_00:40:00 (08:97:34:00:40:00)
- Internet Protocol Version 4, Src: 172.17.170.151, Dst: 192.229.221.95
- Transmission Control Protocol, Src Port: 55882, Dst Port: 80, Seq: 1, Ack: 1, Len: 240
- Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the selected packet, including the HTTP GET request and the OCSP response.

At the bottom of the window, there is a status bar showing the number of packets captured (36887) and displayed (6 (0.0%)). The system tray shows the date and time (4:09 PM, 9/18/2024) and the Windows logo.

Http :

*Ethernet 3						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
8334	66.478247	172.17.170.151	192.229.221.95	HTTP	294	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUA
8348	66.679118	192.229.221.95	172.17.170.151	OCSP	791	Response
8592	71.370238	172.17.170.151	192.229.221.95	HTTP	294	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUA
8598	71.570716	192.229.221.95	172.17.170.151	OCSP	791	Response
28231	127.572524	172.17.170.151	178.79.238.128	HTTP	300	GET /msdownload/update/v3/static/
28234	127.698721	178.79.238.128	172.17.170.151	HTTP	353	HTTP/1.1 304 Not Modified

TCP :

*Ethernet 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
8263	65.281208	172.16.100.211	172.17.170.151	TCP	60	53 → 55880 [ACK] Seq=93 Ack=55880
8264	65.281208	172.16.100.211	172.17.170.151	TCP	60	53 → 55880 [FIN, ACK] Seq=93 Ack=55880
8265	65.281272	172.17.170.151	172.16.100.211	TCP	54	55880 → 53 [ACK] Seq=37 Ack=55880
8266	65.328112	172.16.100.211	172.17.170.151	DNS	105	Standard query response 0x0
8267	65.328841	172.17.170.151	172.16.100.211	TCP	54	55879 → 53 [FIN, ACK] Seq=37 Ack=55880
8271	65.329871	172.16.100.211	172.17.170.151	TCP	60	53 → 55879 [ACK] Seq=52 Ack=55879
8272	65.329871	172.16.100.211	172.17.170.151	TCP	60	53 → 55879 [FIN, ACK] Seq=52 Ack=55879
8273	65.329928	172.17.170.151	172.16.100.211	TCP	54	55879 → 53 [ACK] Seq=37 Ack=55879
8313	65.940725	172.17.170.151	20.74.47.205	TCP	66	55881 → 443 [SYN] Seq=0 Win=0 Len=0
8315	66.105459	20.74.47.205	172.17.170.151	TCP	66	443 → 55881 [SYN, ACK] Seq=2921 Ack=55881 Len=0
8316	66.105520	172.17.170.151	20.74.47.205	TCP	54	55881 → 443 [ACK] Seq=1 Ack=55881
8317	66.106192	172.17.170.151	20.74.47.205	TLSv1.2	359	Client Hello
8324	66.269342	20.74.47.205	172.17.170.151	TCP	1514	443 → 55881 [ACK] Seq=1 Ack=55881
8325	66.269342	20.74.47.205	172.17.170.151	TCP	1514	443 → 55881 [ACK] Seq=1461 Ack=55881
8326	66.269342	20.74.47.205	172.17.170.151	TCP	1514	443 → 55881 [ACK] Seq=2921 Ack=55881

DNS :

*Ethernet 3							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
[Icons]							
dns							
No.	Time	Source	Destination	Protocol	Length	Info	
3971	32.365178	172.16.100.211	172.17.170.151	DNS	104	Standard query response	
3973	32.365183	172.16.100.211	172.17.170.151	DNS	113	Standard query response	
4165	32.905798	172.17.170.151	172.16.100.211	DNS	96	Standard query 0xf37f H	
4167	32.905823	172.17.170.151	172.16.100.211	DNS	96	Standard query 0x54fc A	
4172	32.907366	172.16.100.211	172.17.170.151	DNS	114	Standard query response	
4173	32.907366	172.16.100.211	172.17.170.151	DNS	123	Standard query response	
4232	32.984889	172.17.170.151	172.16.100.211	DNS	97	Standard query 0x0356 A	
4234	32.984960	172.17.170.151	172.16.100.211	DNS	97	Standard query 0x6e1c H	
4236	32.986226	172.16.100.211	172.17.170.151	DNS	144	Standard query response	
4238	32.986289	172.16.100.211	172.17.170.151	DNS	185	Standard query response	
5923	35.351087	172.17.170.151	172.16.100.211	DNS	100	Standard query 0x3026 H	
5925	35.351111	172.17.170.151	172.16.100.211	DNS	100	Standard query 0xdc90 A	
5929	35.352385	172.16.100.211	172.17.170.151	DNS	118	Standard query response	
6683	36.688492	172.17.170.151	172.16.100.211	DNS	91	Standard query 0xdc02 H	
6685	36.688512	172.17.170.151	172.16.100.211	DNS	91	Standard query 0xa9f A	

4. Write down the IP address of your machine and the IP address of destination server.

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 8334).

No.	Time	Source	Destination	Protocol	Length	Info
8334	66.478247	172.17.170.151	192.229.221.95	HTTP	294	GET /MFEwTzBNV
8348	66.679118	192.229.221.95	172.17.170.151	OCSP	791	Response
8592	71.370238	172.17.170.151	192.229.221.95	HTTP	294	GET /MFEwTzBNV
8598	71.570716	192.229.221.95	172.17.170.151	OCSP	791	Response
28231	127.572524	172.17.170.151	178.79.238.128	HTTP	300	GET /msdownloa
28234	127.698721					

Wireshark · Packet 8334 · tyhuj.pcapng

...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.17.170.151
Destination Address: 192.229.221.95
Transmission Control Protocol, Src Port: 55882, Dst Port: 80, Seq: 1.
Source Port: 55882
Destination Port: 80
[Stream index: 79]

My machine IP :

172.17.170.151

Destination Server IP :

192.229.221.95

5. Write down source and destination port number of one http packet.

Source Port: 55882

Destination Port: 80

The image shows a close-up of the Wireshark packet details pane. The 'Transmission Control Protocol' section is expanded, showing the source and destination ports.

Source Port: 55882
Destination Port: 80