

TASK-05

WIRESHARK TRAFFIC CAPTURING

1. WIFI MONITORING

The screenshot shows a Wireshark traffic capture on a Windows 11 system. The capture is titled "Wi-Fi" and shows a list of packets in the packet list pane. The selected packet is packet 20, which is a TCP Reset (RST) from 2a03:2880:f26e:c9:f to 2409:40c4:15:db2f:a. The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 6, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2620:1ec:33:1::11	2409:40c4:15:db2f:a	TCP	74	443 → 50358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2	0.619484	64:ff9b::34bb:4f6d	2409:40c4:15:db2f:a	TLSv1.2	133	Application Data
3	0.620237	2409:40c4:15:db2f:a	64:ff9b::34bb:4f6d	TLSv1.2	140	Application Data
4	0.692789	64:ff9b::34bb:4f6d	2409:40c4:15:db2f:a	TCP	74	443 → 50080 [ACK] Seq=60 Ack=67 Win=251 Len=0
5	1.921853	2409:40c4:15:db2f:a	2405:200:1607:2820::	TCP	86	50474 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
6	1.940322	64:ff9b::14bd:ad0d	2409:40c4:15:db2f:a	TCP	74	443 → 50296 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	1.984091	2409:40c4:15:db2f:a	2603:1010:3:b::1c	TLSv1.2	124	Application Data
8	2.265258	2603:1010:3:b::1c	2409:40c4:15:db2f:a	TLSv1.2	113	Application Data
9	2.310603	2409:40c4:15:db2f:a	2603:1010:3:b::1c	TCP	74	49786 → 443 [ACK] Seq=51 Ack=40 Win=254 Len=0
10	2.563327	2603:1010:3:b::1c	2409:40c4:15:db2f:a	TCP	113	[TCP Spurious Retransmission] 443 → 49786 [PSH, ACK] Seq=1 Ack=51 Win=16385 Len=39
11	2.563391	2409:40c4:15:db2f:a	2603:1010:3:b::1c	TCP	86	[TCP Dup ACK 9#1] 49786 → 443 [ACK] Seq=51 Ack=40 Win=254 Len=0 SLE=1 SRE=40
12	2.922212	2409:40c4:15:db2f:a	2405:200:1607:2820::	TCP	86	[TCP Retransmission] 50474 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
13	4.933560	2409:40c4:15:db2f:a	2405:200:1607:2820::	TCP	86	[TCP Retransmission] 50474 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
14	5.464733	2409:40c4:15:db2f:a	2a03:2880:f26e:c9:f	TCP	74	50469 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
15	5.572495	2a03:2880:f26e:c9:f	2409:40c4:15:db2f:a	TCP	74	443 → 50469 [ACK] Seq=1 Ack=2 Win=265 Len=0
16	5.948268	2a03:2880:f26e:c9:f	2409:40c4:15:db2f:a	TCP	74	443 → 50469 [FIN, ACK] Seq=1 Ack=2 Win=265 Len=0
17	5.948342	2409:40c4:15:db2f:a	2a03:2880:f26e:c9:f	TCP	74	50469 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
18	5.985239	2a03:2880:f26e:c9:f	2409:40c4:15:db2f:a	TCP	74	[TCP Retransmission] 443 → 50469 [FIN, ACK] Seq=1 Ack=2 Win=265 Len=0
19	5.985297	2409:40c4:15:db2f:a	2a03:2880:f26e:c9:f	TCP	74	[TCP ZeroWindow] 50469 → 443 [ACK] Seq=2 Ack=2 Win=0 Len=0
20	6.022587	2a03:2880:f26e:c9:f	2409:40c4:15:db2f:a	TCP	74	443 → 50469 [RST] Seq=2 Win=0 Len=0

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{136A70FC-0E-40-40-80-00} (00:00:00:00:00:00)
> Ethernet II, Src: fa:15:5f:32:fb:15 (fa:15:5f:32:fb:15), Dst: AzureWaveTec_3a:02:c0 (10:60:30:3a:02:c0)
> Internet Protocol Version 6, Src: 2620:1ec:33:1::11, Dst: 2409:40c4:15:db2f:ad01:42e8:94da:71c
> Transmission Control Protocol, Src Port: 443, Dst Port: 50358, Seq: 1, Ack: 1, Len: 0

Packets: 1168 - Dropped: 0 (0.0%) Profile: Default

2. TCP FILTER

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
131	10.744526	2409:40c4:15:db2f:a...	2405:200:1607:2820::	TCP	86	[TCP Retransmission] 50675 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
132	10.770839	2409:40c4:15:db2f:a...	2409:40c4:15:db2f:a...	ICMPv6	78	Neighbor Advertisement 2409:40c4:15:db2f::f0 (rtr, sol)
133	11.467925	fa:15:5f:32:fb:15	AzureWaveTec_3a:02::	ARP	42	Who has 192.168.227.172? Tell 192.168.227.131
134	11.467958	AzureWaveTec_3a:02::	fa:15:5f:32:fb:15	ARP	42	192.168.227.172 is at 10:68:38:3a:02:c0
135	13.306892	2603:1063:27:2::14	2409:40c4:15:db2f:a...	TCP	74	443 → 50648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
136	16.060345	192.168.227.131	224.0.0.251	MDNS	82	Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question
137	16.060702	fe80::f815:5fff:fe3...	ff02::fb	MDNS	102	Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question
138	16.061050	fe80::f815:5fff:fe3...	ff02::fb	MDNS	123	Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _8E6C866D._sub._googlecast._tcp.local, "QU" question
139	16.061330	192.168.227.131	224.0.0.251	MDNS	119	Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _674A0243._sub._googlecast._tcp.local, "QU" question PTR _8E6C8...
140	16.061505	fe80::f815:5fff:fe3...	ff02::fb	MDNS	139	Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _674A0243._sub._googlecast._tcp.local, "QU" question PTR _8E6C8...
141	17.907491	192.168.227.131	224.0.0.251	MDNS	119	Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C8...
142	17.907876	fe80::f815:5fff:fe3...	ff02::fb	MDNS	139	Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _674A0243._sub._googlecast._tcp.local, "QM" question PTR _8E6C8...
143	18.752408	2409:40c4:15:db2f:a...	2405:200:1607:2820::	TCP	86	[TCP Retransmission] 50675 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
144	20.676958	64:ff9b::d294:551e	2409:40c4:15:db2f:a...	TCP	74	[TCP Keep-Alive] 443 → 50678 [ACK] Seq=489 Ack=1084 Win=81024 Len=0
145	20.677054	2409:40c4:15:db2f:a...	64:ff9b::d294:551e	TCP	74	[TCP Keep-Alive ACK] 50678 → 443 [ACK] Seq=1084 Ack=490 Win=65024 Len=0
146	20.987828	2409:40c4:15:db2f:a...	2603:1046:900:40::2	TCP	74	50649 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
147	21.070814	2603:1046:900:40::2	2409:40c4:15:db2f:a...	TCP	74	443 → 50649 [FIN, ACK] Seq=1 Ack=2 Win=16386 Len=0
148	21.070894	2409:40c4:15:db2f:a...	2603:1046:900:40::2	TCP	74	50649 → 443 [ACK] Seq=2 Ack=2 Win=1023 Len=0
149	25.755675	2409:40c4:15:db2f:a...	2405:200:1607:2820::	TCP	86	50682 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
150	26.105404	fe80::f815:5fff:fe3...	2409:40c4:15:db2f:a...	ICMPv6	86	Neighbor Solicitation for 2409:40c4:15:db2f:ad01:42e8:94da:71c from fa:15:5f:32:fb:15
151	26.105536	2409:40c4:15:db2f:a...	fe80::f815:5fff:fe3...	ICMPv6	86	Neighbor Advertisement 2409:40c4:15:db2f:ad01:42e8:94da:71c (sol, ovr) is at 10:68:38:3a:02:c0
152	26.763285	2409:40c4:15:db2f:a...	2405:200:1607:2820::	TCP	86	[TCP Retransmission] 50682 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM

> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{136A70FC-0000} fa:15:5f:32:fb:15 10 68 38 3a 02 c0 86 dd 60 07 ...2...h 8:....
> Ethernet II, Src: AzureWaveTec_3a:02:c0 (10:68:38:3a:02:c0), Dst: fa:15:5f:32:fb:15 (fa:15:5f:32:fb:15) 0010 cc ba 00 15 06 3f 24 09 40 c4 00 15 db 2f ad 0125 @:....
> Internet Protocol Version 6, Src: 2409:40c4:15:db2f:ad01:42e8:94da:71c, Dst: 2620:1ec:33:1::254 0020 42 e8 94 da 07 1c 26 20 01 ec 00 33 00 01 00 00 B.....& ...3:....
> Transmission Control Protocol, Src Port: 50654, Dst Port: 443, Seq: 1, Ack: 1, Len: 1 0030 00 00 00 02 54 c5 de 01 bb 8f 5c 34 6d 60 6eT... ..4m'n
0040 cb d9 50 10 00 fc 00 a6 00 00 00 ..P.....

Transmission Control Protocol: Protocol Packets: 228 Profile: Default

3. DNS FILTER

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Source	Destination	Protocol	Length	Info
72	2409:40c4:15:db2f:a...	2404:6800:4009:81e:...	UDP	94	60457 → 443 Len=32
76	2404:6800:4009:81e:...	2409:40c4:15:db2f:a...	UDP	86	443 → 60457 Len=24
77	2404:6800:4009:81e:...	2409:40c4:15:db2f:a...	UDP	83	443 → 60457 Len=21
69	5.299583	2409:40c4:15:db2f:a...	UDP	95	60457 → 443 Len=33
76	6.046790	192.168.227.172	DNS	70	Standard query 0x5107 A c.pki.goog
77	6.047235	192.168.227.172	DNS	70	Standard query 0xbc39 AAAA c.pki.goog
78	6.079754	2409:40c4:15:db2f:a...	DNS	90	Standard query 0x5107 A c.pki.goog
79	6.079754	2409:40c4:15:db2f:a...	DNS	90	Standard query 0xbc39 AAAA c.pki.goog
80	6.098809	192.168.227.131	DNS	121	Standard query response 0x5107 A c.pki.goog CNAME pki-goog.l.google.com A 142.251.220.3
81	6.098809	192.168.227.131	DNS	133	Standard query response 0xbc39 AAAA c.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4009:805::2003
83	6.106023	2409:40c4:15:db2f:a...	DNS	153	Standard query response 0xbc39 AAAA c.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4009:80a::2003
84	6.113228	2409:40c4:15:db2f:a...	DNS	141	Standard query response 0x5107 A c.pki.goog CNAME pki-goog.l.google.com A 142.251.220.3
90	6.242116	192.168.227.172	DNS	74	Standard query 0x2136 A x1.c.lencr.org
91	6.242447	192.168.227.172	DNS	74	Standard query 0x6437 AAAA x1.c.lencr.org
93	6.282676	2409:40c4:15:db2f:a...	DNS	94	Standard query 0x6437 AAAA x1.c.lencr.org
94	6.282676	2409:40c4:15:db2f:a...	DNS	94	Standard query 0x2136 A x1.c.lencr.org
95	6.288738	192.168.227.131	DNS	179	Standard query response 0x2136 A x1.c.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.net CNAME e8652.dscx.akamaiedge.net A 49...
96	6.288738	192.168.227.131	DNS	219	Standard query response 0x6437 AAAA x1.c.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.net CNAME e8652.dscx.akamaiedge.net AA...
98	6.329267	2409:40c4:15:db2f:a...	DNS	199	Standard query response 0x2136 A x1.c.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.net CNAME e8652.dscx.akamaiedge.net A 49...
99	6.329267	2409:40c4:15:db2f:a...	DNS	239	Standard query response 0x6437 AAAA x1.c.lencr.org CNAME crl.root-x1.letsencrypt.org.edgekey.net CNAME e8652.dscx.akamaiedge.net AA...
110	6.644418	192.168.227.172	DNS	83	Standard query 0x5dba A ctldl.windowsupdate.com
111	6.644746	192.168.227.172	DNS	83	Standard query 0x17a3 AAAA ctldl.windowsupdate.com

> Frame 84: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface \Device\NPF_{136A7E...}

> Ethernet II, Src: fa:15:5f:32:fb:15 (fa:15:5f:32:fb:15), Dst: AzureNaveTec_3a:02:c0 (10:68:38:3a:02:c0)

> Internet Protocol Version 6, Src: 2409:40c4:15:db2f::f0, Dst: 2409:40c4:15:db2f:ad01:42e8:94da:71c

> User Datagram Protocol, Src Port: 53, Dst Port: 59981

> Domain Name System (response)

0000 10 68 38 3a 02 c0 fa 15 5f 32 fb 15 86 dd 60 01 :h8:.... 2....

0010 d8 73 00 57 11 40 24 09 40 c4 00 15 db 2f 00 00 :sW@ @.../..

0020 00 00 00 00 00 f0 24 09 40 c4 00 15 db 2f ad 01 :.....\$ @...f..

0030 42 e8 94 da 07 1c 00 35 ea 4d 00 57 60 bd 51 07 :B.....5 -M'W'Q

0040 01 80 00 01 00 02 00 00 00 00 01 63 03 70 6b 69 :.....c.pki

0050 04 67 6f 6f 67 00 00 01 00 01 c0 0c 00 05 00 01 :.goog:.....

0060 00 00 01 01 00 17 08 70 6b 69 24 67 6f 6f 01 01 :.....pki:goog:

0070 6c 06 67 6f 6f 67 6c 65 03 63 6f 6d 00 c0 28 00 :l.google.com: (

0080 01 00 01 00 00 01 01 00 04 8e fb dc 03 :.....

User Datagram Protocol Protocol Packets: 537 - Displayed: 126 (23.5%) Profile: Default

4. IP ADDRESS OF WEBSITE

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.227.172

No.	Time	Source	Destination	Protocol	Length	Info
267	54.297884	192.168.227.172	192.168.227.131	DNS	79	Standard query 0xc53 AAAA graph.microsoft.com
270	54.349581	192.168.227.131	192.168.227.172	DNS	243	Standard query response 0xc53 AAAA graph.microsoft.com CNAME ags.privatelink.asidentity.com CNAME www.tm.prd.ags.akadns.net AAAA 2...
273	54.586519	192.168.227.131	192.168.227.172	DNS	207	Standard query response 0xc74 A graph.microsoft.com CNAME ags.privatelink.asidentity.com CNAME www.tm.prd.ags.akadns.net A 20.198...
290	54.758563	192.168.227.172	49.44.79.236	TCP	60	[TCP Reset/Transmission] Seq=50976 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=0
331	61.626087	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
332	61.637584	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
335	61.671939	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
337	61.672472	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
339	61.672997	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
341	61.673892	192.168.227.172	224.0.0.252	LLMNR	69	Standard query 0x08a8 ANY priyu1618
343	62.086317	192.168.227.172	224.0.0.252	LLMNR	69	Standard query 0x08a8 ANY priyu1618
344	62.143922	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
348	64.625381	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
349	64.644790	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
352	64.659196	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
354	64.659445	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
356	64.659954	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
358	64.661806	192.168.227.172	224.0.0.252	LLMNR	69	Standard query 0x08c5 ANY priyu1618
362	65.081482	192.168.227.172	224.0.0.252	LLMNR	69	Standard query 0x08c5 ANY priyu1618
363	65.144166	192.168.227.172	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
373	71.017832	192.168.227.172	192.168.227.131	DNS	72	Standard query 0x29f8 AAAA nephobox.com
374	71.040136	192.168.227.131	192.168.227.172	DNS	100	Standard query response 0x29f8 AAAA nephobox.com AAAA 64:ff9b:6262:e1c8

> Frame 35: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{136A70FC-...}

> Ethernet II, Src: AzureWaveTec_3a:02:c0 (10:68:38:3a:02:c0), Dst: fa:15:5f:32:fb:15 (fa:15:5f:32:fb:15)

> Internet Protocol Version 4, Src: 192.168.227.172, Dst: 98.98.225.200

> Transmission Control Protocol, Src Port: 50976, Dst Port: 443, Seq: 0, Len: 0

0000 fa 15 5f 32 fb 15 10 68 38 3a 02 c0 08 00 45 00 ...2...h B:....E:
0010 00 34 07 3d 60 00 80 06 0b 07 c0 a8 e3 ac 62 62 ...4-@...-...bb
0020 e1 c8 c7 1d 01 bb 23 09 cc cd 00 00 00 00 00 02 ...-...-...-...
0030 ff ff cd e0 00 00 02 04 05 b4 01 03 03 08 01 01 ...-...-...-...
0040 04 02 ...

wireshark-Wi-FiZ46662.pcapng Packets: 402 · Displayed: 69 (17.2%) Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.227.131

No.	Time	Source	Destination	Protocol	Length	Info
793	190.699126	192.168.227.131	192.168.227.172	TCP	54	53 → 51003 [ACK] Seq=1 Ack=3 Win=65536 Len=0
794	190.699126	192.168.227.131	192.168.227.172	TCP	54	53 → 51003 [ACK] Seq=1 Ack=57 Win=65536 Len=0
796	190.777446	192.168.227.131	192.168.227.172	TCP	55	53 → 51004 [PSH, ACK] Seq=1 Ack=57 Win=65536 Len=1 [TCP PDU reassembled in 801]
797	190.777446	192.168.227.131	192.168.227.172	TCP	55	53 → 51005 [PSH, ACK] Seq=1 Ack=57 Win=65536 Len=1 [TCP PDU reassembled in 802]
798	190.882393	192.168.227.131	192.168.227.172	TCP	55	53 → 51003 [PSH, ACK] Seq=1 Ack=57 Win=65536 Len=1 [TCP PDU reassembled in 810]
799	190.820371	192.168.227.172	192.168.227.131	TCP	54	51004 → 53 [ACK] Seq=57 Ack=2 Win=65280 Len=0
800	190.820421	192.168.227.172	192.168.227.131	TCP	54	51005 → 53 [ACK] Seq=57 Ack=2 Win=65280 Len=0
801	190.824177	192.168.227.131	192.168.227.172	DNS	239	Standard query response 0x3544 A functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME oned...
802	190.824177	192.168.227.131	192.168.227.172	DNS	290	Standard query response 0x3bfe HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME ...
803	190.824492	192.168.227.172	192.168.227.131	TCP	54	51005 → 53 [FIN, ACK] Seq=57 Ack=238 Win=65280 Len=0
804	190.824684	192.168.227.172	192.168.227.131	TCP	54	51004 → 53 [FIN, ACK] Seq=57 Ack=187 Win=65280 Len=0
805	190.828829	192.168.227.131	192.168.227.172	TCP	54	53 → 51005 [FIN, ACK] Seq=238 Ack=58 Win=65536 Len=0
806	190.828829	192.168.227.131	192.168.227.172	TCP	54	53 → 51004 [FIN, ACK] Seq=187 Ack=58 Win=65536 Len=0
807	190.828873	192.168.227.172	192.168.227.131	TCP	54	51005 → 53 [ACK] Seq=58 Ack=239 Win=65280 Len=0
808	190.828927	192.168.227.172	192.168.227.131	TCP	54	51004 → 53 [ACK] Seq=58 Ack=188 Win=65280 Len=0
809	190.851483	192.168.227.172	192.168.227.131	TCP	54	51003 → 53 [ACK] Seq=57 Ack=2 Win=65280 Len=0
810	190.855659	192.168.227.131	192.168.227.172	DNS	255	Standard query response 0x9e0d AAAA functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME o...
811	190.855915	192.168.227.172	192.168.227.131	TCP	54	51003 → 53 [FIN, ACK] Seq=57 Ack=203 Win=65280 Len=0
812	190.861178	192.168.227.131	192.168.227.172	TCP	54	53 → 51003 [FIN, ACK] Seq=203 Ack=58 Win=65536 Len=0
815	190.861248	192.168.227.172	192.168.227.131	TCP	54	51003 → 53 [ACK] Seq=58 Ack=204 Win=65280 Len=0
820	190.876621	192.168.227.172	192.168.227.131	DNS	72	Standard query 0x2cbe A nephobox.com
821	190.898012	192.168.227.131	192.168.227.172	DNS	88	Standard query response 0x2cbe A nephobox.com A 98.98.225.200

> Frame 138: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{136A70FC-...}

> Ethernet II, Src: AzureWaveTec_3a:02:c0 (10:68:38:3a:02:c0), Dst: fa:15:5f:32:fb:15 (fa:15:5f:32:fb:15)

> Internet Protocol Version 4, Src: 192.168.227.172, Dst: 192.168.227.131

> Transmission Control Protocol, Src Port: 50976, Dst Port: 53, Seq: 0, Len: 0

0000 fa 15 5f 32 fb 15 10 68 38 3a 02 c0 08 00 45 00 ...2...h B:....E:
0010 00 34 06 b3 40 00 80 06 45 8f c0 a8 e3 ac c0 a8 ...41@...E:.....
0020 e3 83 c7 1f 00 15 68 b9 1e 85 00 00 00 00 02 ...-Sh.....
0030 ff ff d7 fb 00 00 02 04 05 b4 01 03 03 08 01 01 ...-...-...-...
0040 04 02 ...

wireshark-Wi-FiZ46662.pcapng Packets: 913 · Displayed: 172 (18.8%) Profile: Default