

Wireshark packet capture showing DNS and ICMP traffic. The packet list shows a series of DNS queries and responses, and an ICMP Multicast Listener Report Message. The packet details pane shows the structure of the DNS query and response, and the ICMP message. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
9696	89.281486	172.16.103.97	172.16.96.1	DNS	79	Standard query 0x7d86 A fp-as.azureedge.net
9697	89.287202	fe80::5dcb:c004:157...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
9698	89.287247	fe80::5dcb:c004:157...	ff02::1:3	LLMNR	93	Standard query 0x1798 ANY 22PHD0342-SAS
9699	89.299016	Cisco_5c:21:b1	Chongqin_c5:7b:7f	0x3a00	72	Ethernet II
9700	89.315897	fe80::5dcb:c004:157...	ff02::fb	MDNS	137	Standard query response 0x0000 AAAA fe80::5dcb:c004:157e:2f83 A 172.16.103.201
9701	89.356121	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local
9702	89.358396	fe80::454:f6e:a8c:7...	ff02::fb	MDNS	438	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local
9703	89.358396	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
9704	89.358396	fe80::454:f6e:a8c:7...	ff02::fb	MDNS	202	Standard query response 0x0000 TXT OPT
9705	89.358396	172.16.96.1	172.16.103.97	DNS	209	Standard query response 0x7d86 A fp-as.azureedge.net CNAME fp-as.akstd.azureedge.net
9706	89.359511	172.16.103.97	23.46.187.161	TCP	66	62143 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
9707	89.367657	fe80::5dcb:c004:157...	ff02::1:2	DHCPv6	155	Solicit XID: 0x5bb817 CID: 0001000129cad0cd00e04c68bc86
9708	89.372874	23.46.187.161	172.16.103.97	TCP	66	443 → 62143 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
9709	89.372987	172.16.103.97	23.46.187.161	TCP	54	62143 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
9710	89.373514	172.16.103.97	23.46.187.161	TLSv1.2	258	Client Hello
9711	89.386052	23.46.187.161	172.16.103.97	TCP	60	443 → 62143 [ACK] Seq=1 Ack=205 Win=64128 Len=0
9712	89.416753	fe80::5dcb:c004:157...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

Frame 1: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface \Device\NPF\_{D7AF522C-2BC7-43EF-B577-CF2B521ACF49}, id 0

Ethernet II, Src: Apple\_e9:63:e3 (8c:7a:aa:e9:63:e3), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)

Internet Protocol Version 4, Src: 172.16.103.211, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Multicast Domain Name System (query)

```
Ip.addr == 172.16.103.211
```

The figure displays a Wireshark packet capture of DNS traffic. The top pane shows a list of 21 packets, all of which are DNS Standard queries from 172.16.103.211 to 224.0.0.251. The middle pane shows the details of the selected packet (Frame 1), which is a DNS Standard query for PTR records. The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local
2	3.0.000000	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
3	5.0.100370	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local
4	7.0.102191	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
5	13.0.298403	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local
6	15.0.301700	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
7	19.0.398168	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local
8	21.0.399921	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
9	25.0.500940	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local
10	27.0.503063	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
11	30.0.600117	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local
12	32.0.602034	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
13	36.0.701298	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local
14	38.0.705034	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
15	42.0.806012	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local
16	44.0.806367	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
17	49.0.902426	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question PTR _printer._tcp.local, "QU" question PTR _ipp._tcp.local

Frame 1: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface \Device\NPF\_{D7AF522C-2BC7-43EF-B577-CF2B521ACF49}, id 0  
 Ethernet II, Src: Apple\_e9:63:e3 (8c:7a:aa:e9:63:e3), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)  
 Internet Protocol Version 4, Src: 172.16.103.211, Dst: 224.0.0.251  
 User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
 Multicast Domain Name System (query)

0000	28 cd c4 c5 7b 7f 8c 7a aa e9 63 e3 00 00 45 00	{...Z...E...
0010	01 94 76 0d 00 00 ff 11 4f 6c ac 10 67 d3 00 00	W... 01 g...
0020	00 fb 14 e9 14 e9 01 80 d2 02 00 00 00 00 00 11	.....
0030	00 01 00 00 00 01 08 5f 61 69 72 70 6f 72 74 04	....._airport-
0040	5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c 80 01 07	_tcp.local.....
0050	5f 72 64 6c 69 6e 6b c0 15 00 0c 80 01 08 5f 70	_rdlink.....p
0060	72 69 6e 74 65 72 c0 15 00 0c 80 01 06 5f 75 73	rinter.....us
0070	63 61 6e c0 15 00 0c 80 01 04 5f 69 70 70 c0 15	can....._ipp-
0080	00 0c 80 01 07 5f 75 73 63 61 6e 73 c0 15 00 0c	.....us cans...

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows a series of packets, with the selected packet (No. 1) being a DNS query from 172.16.103.211 to 224.0.0.251. The packet details pane shows the structure of the query, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and Multicast Domain Name System (query) header. The packet bytes pane shows the raw data of the packet, with the first few bytes being 28 cd c4 c5 7b 7f 8c 7a aa e9 63 e3 08 00 45 00.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PT...
3	0.000000	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0...
5	0.100370	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PT...
7	0.102191	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0...
13	0.298403	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PT...
15	0.301700	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0...
19	0.398168	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PT...
21	0.399921	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0...
25	0.500940	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PT...
27	0.503063	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0...
30	0.600117	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PT...
32	0.602034	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0...
36	0.701298	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PT...
38	0.705034	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0...
42	0.806012	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PT...
44	0.806367	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0...

> Frame 1: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface \Device\NPF\_{D7AF5...}

> Ethernet II, Src: Apple\_e9:63:e3 (8c:7a:aa:e9:63:e3), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)

> Internet Protocol Version 4, Src: 172.16.103.211, Dst: 224.0.0.251

> User Datagram Protocol, Src Port: 5353, Dst Port: 5353

> Multicast Domain Name System (query)

0000 28 cd c4 c5 7b 7f 8c 7a aa e9 63 e3 08 00 45 00 (---{---z---c---E-

0010 01 94 76 0d 00 00 ff 11 4f 6c ac 10 67 d3 e0 00 --v-----0l--g--

0020 00 fb 14 e9 14 e9 01 80 d2 02 00 00 00 00 00 11 -----

0030 00 01 00 00 00 01 08 5f 61 69 72 70 6f 72 74 04 ----- airport

0040 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c 80 01 07 \_tcp\_loc al-----

0050 5f 72 64 6c 69 6e 6b c0 15 00 0c 80 01 08 5f 70 \_rdlink-----\_p

0060 72 69 6e 74 65 72 c0 15 00 0c 80 01 06 5f 75 73 rinter-----\_us

0070 63 61 6e c0 15 00 0c 80 01 04 5f 69 70 70 c0 15 can-----\_ipp--

0080 00 0c 80 01 07 5f 75 73 63 61 6e 73 c0 15 00 0c -----\_us cans----

0090 80 01 07 5f 69 70 70 75 73 62 c0 15 00 0c 80 01 ----- innu sh-----

## Filter by destination address

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane shows five captured packets, all of which are LLMNR queries from source IP 172.16.103.209 to destination IP 224.0.0.252. The selected packet (No. 802) is expanded in the packet details pane, showing the following layers: Ethernet II (Src: IntelCor\_03:dd:d8, Dst: Chongqin\_c5:7b:7f), Internet Protocol Version 4 (Src: 172.16.103.209, Dst: 224.0.0.252), User Datagram Protocol (Src Port: 60295, Dst Port: 5355), and Link-local Multicast Name Resolution (query). The packet bytes pane shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
802	9.443909	172.16.103.209	224.0.0.252	LLMNR	64	Standard query 0xfe55 A wpa
826	9.865484	172.16.103.209	224.0.0.252	LLMNR	64	Standard query 0xfe55 A wpa
18896	206.576459	172.16.103.209	224.0.0.252	LLMNR	64	Standard query 0xa8f9 A wpa
18919	206.907525	172.16.103.209	224.0.0.252	LLMNR	64	Standard query 0xa8f9 A wpa
41564	471.485870	172.16.103.209	224.0.0.252	LLMNR	75	Standard query 0x77f9 ANY D

Frame 802: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{D7AF522C...}

Ethernet II, Src: IntelCor\_03:dd:d8 (0c:dd:24:03:dd:d8), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)

Internet Protocol Version 4, Src: 172.16.103.209, Dst: 224.0.0.252

User Datagram Protocol, Src Port: 60295, Dst Port: 5355

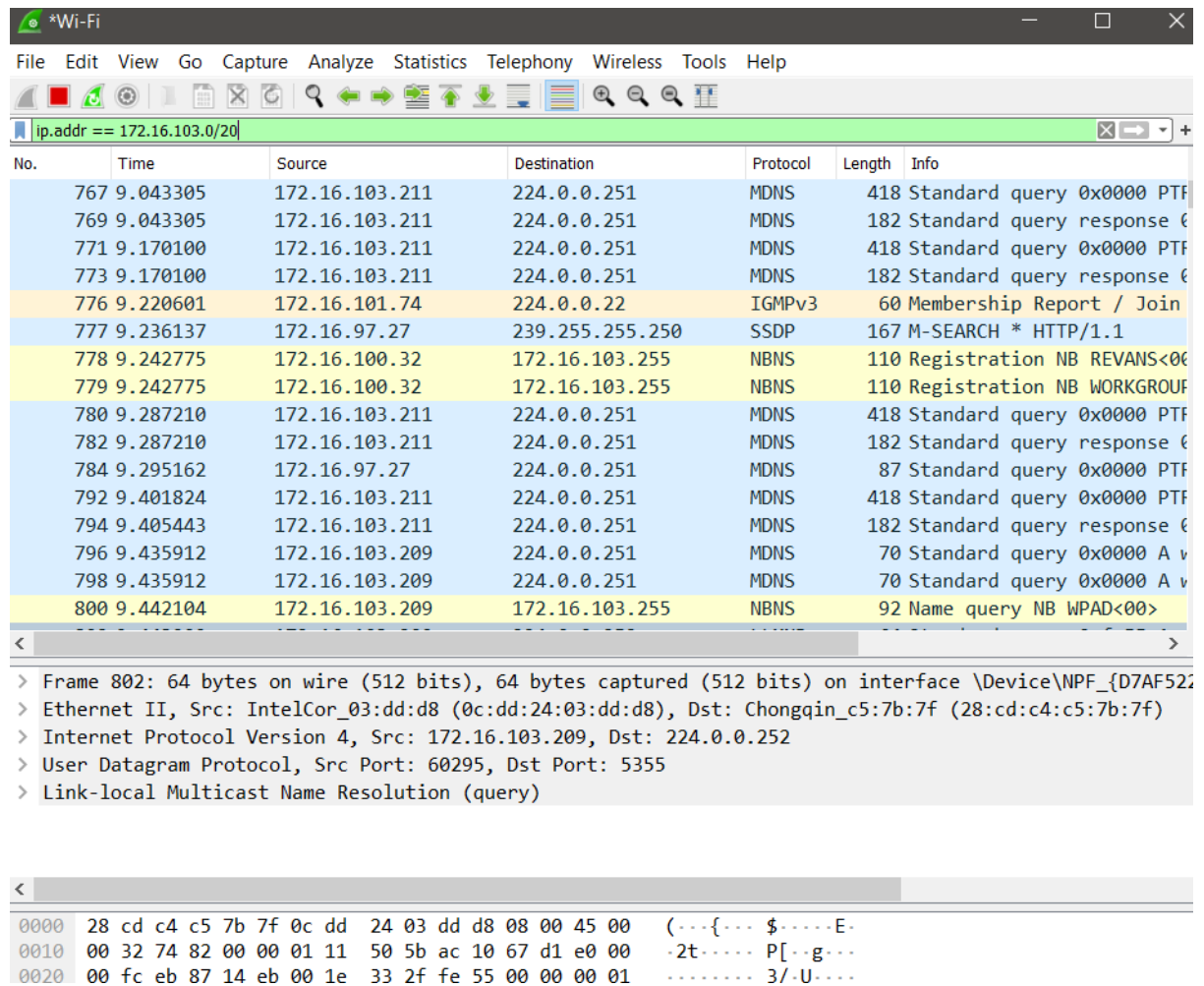
Link-local Multicast Name Resolution (query)

```

0000  28 cd c4 c5 7b 7f 0c dd 24 03 dd d8 08 00 45 00  (---{--- $-----E-
0010  00 32 74 82 00 00 01 11 50 5b ac 10 67 d1 e0 00  -2t----- P[...g...
0020  00 fc eb 87 14 eb 00 1e 33 2f fe 55 00 00 00 01  ..... 3/.U....
0030  00 00 00 00 00 00 04 77 70 61 64 00 00 01 00 01  ....w pad....

```

## Filter by IP subnet



\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.103.0/20

No.	Time	Source	Destination	Protocol	Length	Info
767	9.043305	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTF
769	9.043305	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0
771	9.170100	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTF
773	9.170100	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0
776	9.220601	172.16.101.74	224.0.0.22	IGMPv3	60	Membership Report / Join
777	9.236137	172.16.97.27	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
778	9.242775	172.16.100.32	172.16.103.255	NBNS	110	Registration NB REVANS<00
779	9.242775	172.16.100.32	172.16.103.255	NBNS	110	Registration NB WORKGROU
780	9.287210	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTF
782	9.287210	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0
784	9.295162	172.16.97.27	224.0.0.251	MDNS	87	Standard query 0x0000 PTF
792	9.401824	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTF
794	9.405443	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0
796	9.435912	172.16.103.209	224.0.0.251	MDNS	70	Standard query 0x0000 A v
798	9.435912	172.16.103.209	224.0.0.251	MDNS	70	Standard query 0x0000 A v
800	9.442104	172.16.103.209	172.16.103.255	NBNS	92	Name query NB WPAD<00>

< >

> Frame 802: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{D7AF522...}

> Ethernet II, Src: IntelCor\_03:dd:d8 (0c:dd:24:03:dd:d8), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)

> Internet Protocol Version 4, Src: 172.16.103.209, Dst: 224.0.0.252

> User Datagram Protocol, Src Port: 60295, Dst Port: 5355

> Link-local Multicast Name Resolution (query)

< >

Offset	Hex	ASCII
0000	28 cd c4 c5 7b 7f 0c dd 24 03 dd d8 08 00 45 00	(...{... \$.....E-
0010	00 32 74 82 00 00 01 11 50 5b ac 10 67 d1 e0 00	-2t..... P[...g...
0020	00 fc eb 87 14 eb 00 1e 33 2f fe 55 00 00 00 01	..... 3/U....

## Filter traffic based on protocol

The image displays a Wireshark packet capture of DNS traffic. The packet list shows 20 packets, all DNS queries and responses. The packet details pane shows the structure of a DNS query packet (Frame 6001). The packet bytes pane shows the raw hex and ASCII data.

Source	Destination	Protocol	Length	Info
172.16.96.1	172.16.103.97	DNS	181	Standard query response 0x8360 A edge.microsoft.com CNAME ed
172.16.103.97	172.16.96.1	DNS	83	Standard query 0x1574 A www.msftconnecttest.com
172.16.96.1	172.16.103.97	DNS	219	Standard query response 0x1574 A www.msftconnecttest.com CNA
172.16.103.97	172.16.96.1	DNS	89	Standard query 0x9952 A pagead2.google syndication.com
172.16.96.1	172.16.103.97	DNS	105	Standard query response 0x9952 A pagead2.google syndication.co
172.16.103.97	172.16.96.1	DNS	75	Standard query 0x4aa5 A ssl.gstatic.com
172.16.96.1	172.16.103.97	DNS	91	Standard query response 0x4aa5 A ssl.gstatic.com A 142.250.19
172.16.103.97	172.16.96.1	DNS	83	Standard query 0xd9ee A www.msftconnecttest.com
172.16.96.1	172.16.103.97	DNS	219	Standard query response 0xd9ee A www.msftconnecttest.com CNA
172.16.103.97	172.16.96.1	DNS	75	Standard query 0xb9fe A docs.google.com
172.16.96.1	172.16.103.97	DNS	163	Standard query response 0xb9fe A docs.google.com A 142.250.19
172.16.103.97	172.16.96.1	DNS	83	Standard query 0x002f A www.msftconnecttest.com
172.16.96.1	172.16.103.97	DNS	219	Standard query response 0x002f A www.msftconnecttest.com CNA
172.16.103.97	172.16.96.1	DNS	83	Standard query 0xd705 A www.msftconnecttest.com
172.16.96.1	172.16.103.97	DNS	219	Standard query response 0xd705 A www.msftconnecttest.com CNA
172.16.103.97	172.16.96.1	DNS	77	Standard query 0x3a53 A music.youtube.com
172.16.96.1	172.16.103.97	DNS	439	Standard query response 0x3a53 A music.youtube.com CNAME you
172.16.103.97	172.16.96.1	DNS	83	Standard query 0xb76c A www.msftconnecttest.com
172.16.96.1	172.16.103.97	DNS	219	Standard query response 0xb76c A www.msftconnecttest.com CNA
172.16.103.97	172.16.96.1	DNS	83	Standard query 0x6e38 A www.msftconnecttest.com
172.16.96.1	172.16.103.97	DNS	219	Standard query response 0x6e38 A www.msftconnecttest.com CNA

< >

> Frame 6001: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF\_{D7AF522C-2BC7-43EF...}

> Ethernet II, Src: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor\_c8:07:7c (00:15:17:c8:07:7c)

> Internet Protocol Version 4, Src: 172.16.103.97, Dst: 172.16.96.1

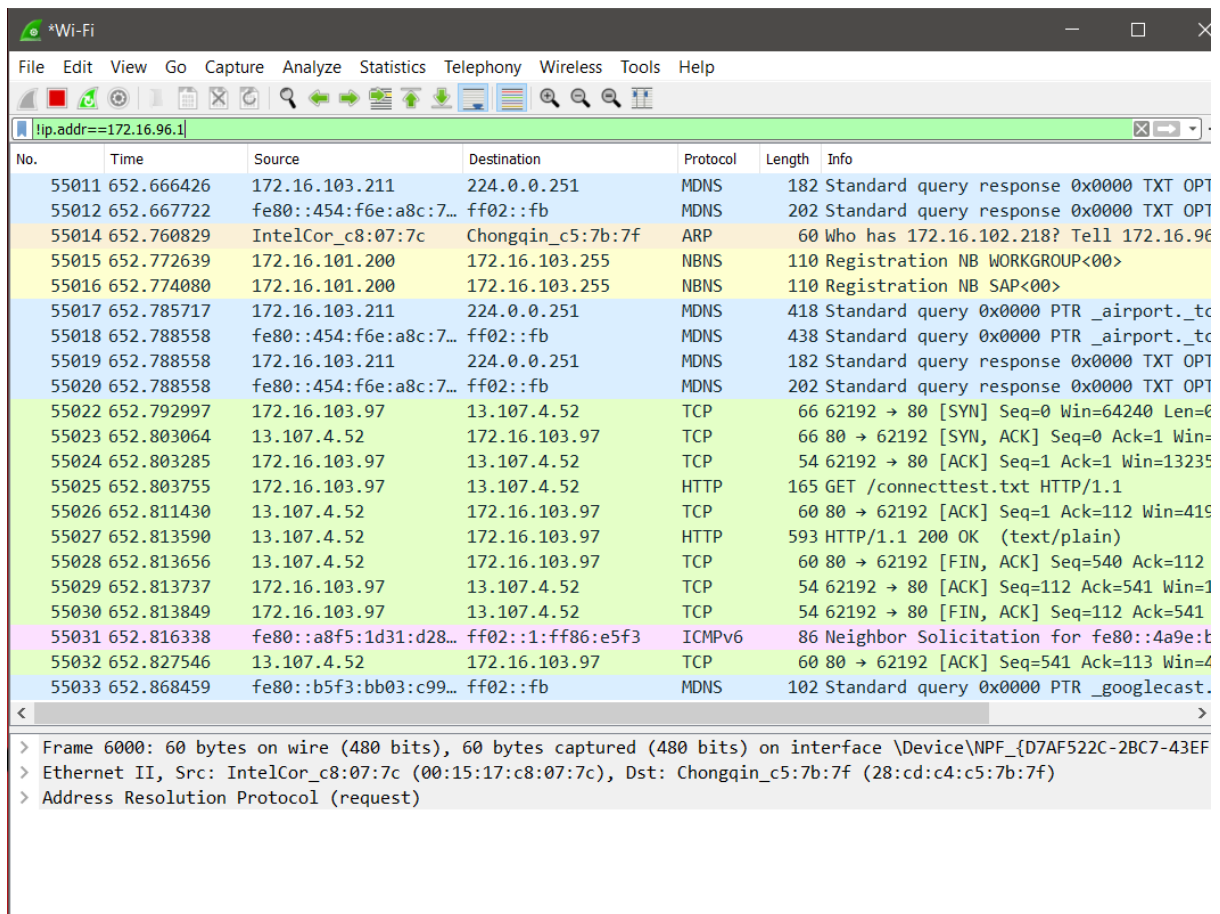
> User Datagram Protocol, Src Port: 65245, Dst Port: 53

> Domain Name System (query)

< >

0000 00 15 17 c8 07 7c 28 cd c4 c5 7b 7f 08 00 45 00 .....|(. .{...E-

## Exclude IP address



\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==172.16.96.1

No.	Time	Source	Destination	Protocol	Length	Info
55011	652.666426	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
55012	652.667722	fe80::454:f6e:a8c:7...	ff02::fb	MDNS	202	Standard query response 0x0000 TXT OPT
55014	652.760829	IntelCor_c8:07:7c	Chongqin_c5:7b:7f	ARP	60	Who has 172.16.102.218? Tell 172.16.96
55015	652.772639	172.16.101.200	172.16.103.255	NBNS	110	Registration NB WORKGROUP<00>
55016	652.774080	172.16.101.200	172.16.103.255	NBNS	110	Registration NB SAP<00>
55017	652.785717	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tc
55018	652.788558	fe80::454:f6e:a8c:7...	ff02::fb	MDNS	438	Standard query 0x0000 PTR _airport._tc
55019	652.788558	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OPT
55020	652.788558	fe80::454:f6e:a8c:7...	ff02::fb	MDNS	202	Standard query response 0x0000 TXT OPT
55022	652.792997	172.16.103.97	13.107.4.52	TCP	66	62192 → 80 [SYN] Seq=0 Win=64240 Len=6
55023	652.803064	13.107.4.52	172.16.103.97	TCP	66	80 → 62192 [SYN, ACK] Seq=0 Ack=1 Win=
55024	652.803285	172.16.103.97	13.107.4.52	TCP	54	62192 → 80 [ACK] Seq=1 Ack=1 Win=13235
55025	652.803755	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
55026	652.811430	13.107.4.52	172.16.103.97	TCP	60	80 → 62192 [ACK] Seq=1 Ack=112 Win=419
55027	652.813590	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
55028	652.813656	13.107.4.52	172.16.103.97	TCP	60	80 → 62192 [FIN, ACK] Seq=540 Ack=112
55029	652.813737	172.16.103.97	13.107.4.52	TCP	54	62192 → 80 [ACK] Seq=112 Ack=541 Win=1
55030	652.813849	172.16.103.97	13.107.4.52	TCP	54	62192 → 80 [FIN, ACK] Seq=112 Ack=541
55031	652.816338	fe80::a8f5:1d31:d28...	ff02::1:ff86:e5f3	ICMPv6	86	Neighbor Solicitation for fe80::4a9e:b
55032	652.827546	13.107.4.52	172.16.103.97	TCP	60	80 → 62192 [ACK] Seq=541 Ack=113 Win=4
55033	652.868459	fe80::b5f3:bb03:c99...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast.

< >

> Frame 6000: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{D7AF522C-2BC7-43EF}

> Ethernet II, Src: IntelCor\_c8:07:7c (00:15:17:c8:07:7c), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)

> Address Resolution Protocol (request)

## Filter on TCP port

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==80

No.	Time	Source	Destination	Protocol	Length	Info
468	6.683274	172.16.103.97	13.107.4.52	TCP	66	62239 → 80 [SYN] Seq=0 Win=64240 Len=0
469	6.692892	13.107.4.52	172.16.103.97	TCP	66	80 → 62239 [SYN, ACK] Seq=0 Ack=1 Win=
470	6.693029	172.16.103.97	13.107.4.52	TCP	54	62239 → 80 [ACK] Seq=1 Ack=1 Win=13235
471	6.693293	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
474	6.713956	13.107.4.52	172.16.103.97	TCP	60	80 → 62239 [ACK] Seq=1 Ack=112 Win=419
475	6.714705	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
476	6.714705	13.107.4.52	172.16.103.97	TCP	60	80 → 62239 [FIN, ACK] Seq=540 Ack=112
477	6.714912	172.16.103.97	13.107.4.52	TCP	54	62239 → 80 [ACK] Seq=112 Ack=541 Win=1
478	6.715053	172.16.103.97	13.107.4.52	TCP	54	62239 → 80 [FIN, ACK] Seq=112 Ack=541
483	6.740328	13.107.4.52	172.16.103.97	TCP	60	80 → 62239 [ACK] Seq=541 Ack=113 Win=4
2305	36.808337	172.16.103.97	13.107.4.52	TCP	66	62240 → 80 [SYN] Seq=0 Win=64240 Len=0
2307	36.858449	13.107.4.52	172.16.103.97	TCP	66	80 → 62240 [SYN, ACK] Seq=0 Ack=1 Win=
2308	36.858651	172.16.103.97	13.107.4.52	TCP	54	62240 → 80 [ACK] Seq=1 Ack=1 Win=13235
2309	36.858952	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
2314	36.869282	13.107.4.52	172.16.103.97	TCP	60	80 → 62240 [ACK] Seq=1 Ack=112 Win=419
2315	36.871492	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
2316	36.871492	13.107.4.52	172.16.103.97	TCP	60	80 → 62240 [FIN, ACK] Seq=540 Ack=112
2317	36.871714	172.16.103.97	13.107.4.52	TCP	54	62240 → 80 [ACK] Seq=112 Ack=541 Win=1
2318	36.871824	172.16.103.97	13.107.4.52	TCP	54	62240 → 80 [FIN, ACK] Seq=112 Ack=541
2319	36.881259	13.107.4.52	172.16.103.97	TCP	60	80 → 62240 [ACK] Seq=541 Ack=113 Win=4
4370	66.934059	172.16.103.97	13.107.4.52	TCP	66	62241 → 80 [SYN] Seq=0 Win=64240 Len=0

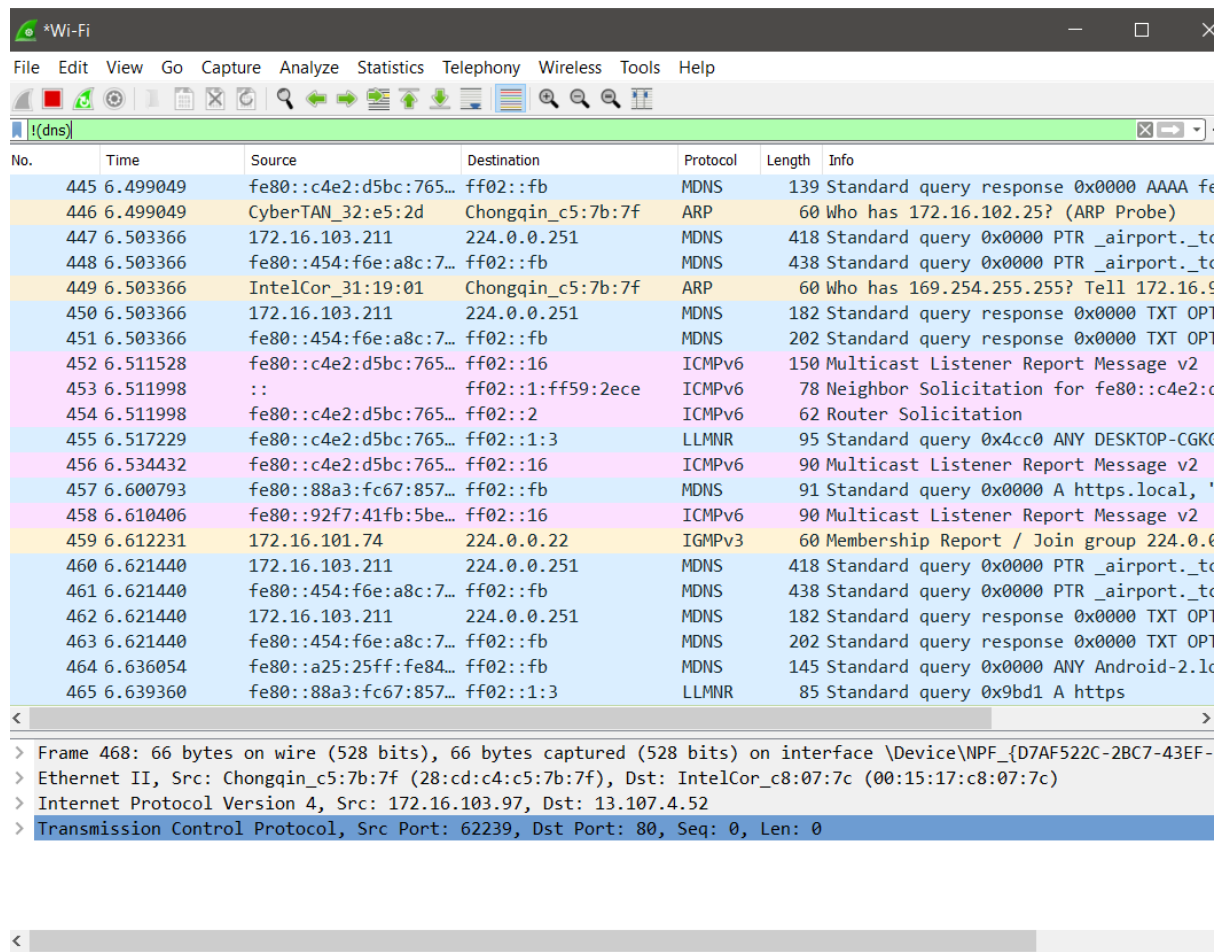
< >

> Frame 468: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{D7AF522C-2BC7-43EF-B  
> Ethernet II, Src: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor\_c8:07:7c (00:15:17:c8:07:7c)  
> Internet Protocol Version 4, Src: 172.16.103.97, Dst: 13.107.4.52  
> Transmission Control Protocol, Src Port: 62239, Dst Port: 80, Seq: 0, Len: 0

< >



## Filter background network noise



Wireshark network traffic capture showing DNS and other protocols. The packet list shows various DNS queries and responses, ARP probes, and ICMPv6 messages. The packet details pane shows the structure of a selected packet (Frame 468).

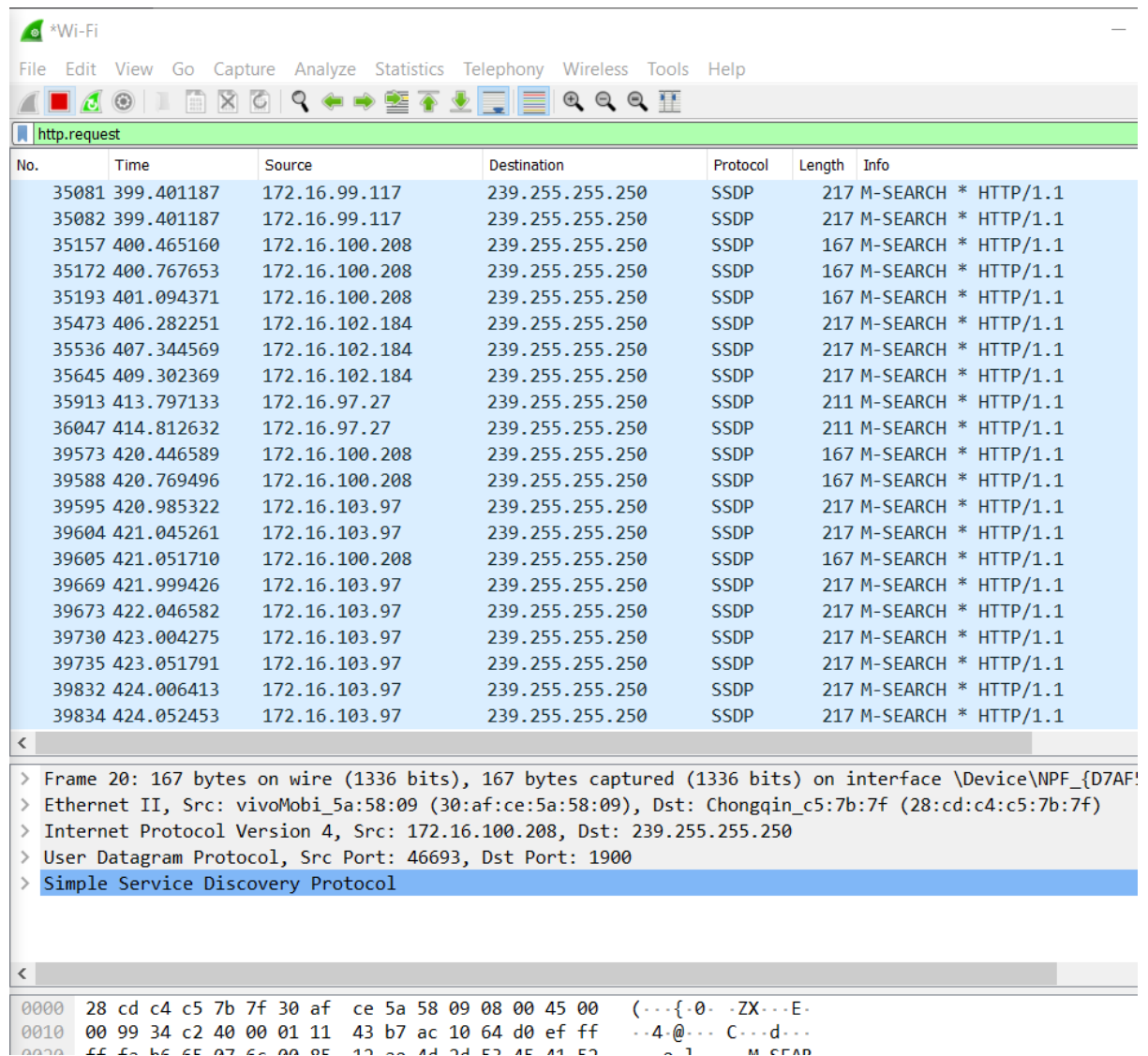
No.	Time	Source	Destination	Protocol	Length	Info
445	6.499049	fe80::c4e2:d5bc:765...	ff02::fb	MDNS	139	Standard query response 0x0000 AAAA fe
446	6.499049	CyberTAN_32:e5:2d	Chongqin_c5:7b:7f	ARP	60	Who has 172.16.102.25? (ARP Probe)
447	6.503366	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tc
448	6.503366	fe80::454:f6e:a8c:7...	ff02::fb	MDNS	438	Standard query 0x0000 PTR _airport._tc
449	6.503366	IntelCor_31:19:01	Chongqin_c5:7b:7f	ARP	60	Who has 169.254.255.255? Tell 172.16.9
450	6.503366	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OP1
451	6.503366	fe80::c454:f6e:a8c:7...	ff02::fb	MDNS	202	Standard query response 0x0000 TXT OP1
452	6.511528	fe80::c4e2:d5bc:765...	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
453	6.511998	::	ff02::1:ff59:2ece	ICMPv6	78	Neighbor Solicitation for fe80::c4e2:c
454	6.511998	fe80::c4e2:d5bc:765...	ff02::2	ICMPv6	62	Router Solicitation
455	6.517229	fe80::c4e2:d5bc:765...	ff02::1:3	LLMNR	95	Standard query 0x4cc0 ANY DESKTOP-CGK
456	6.534432	fe80::c4e2:d5bc:765...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
457	6.600793	fe80::88a3:fc67:857...	ff02::fb	MDNS	91	Standard query 0x0000 A https.local, '
458	6.610406	fe80::92f7:41fb:5be...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
459	6.612231	172.16.101.74	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0
460	6.621440	172.16.103.211	224.0.0.251	MDNS	418	Standard query 0x0000 PTR _airport._tc
461	6.621440	fe80::454:f6e:a8c:7...	ff02::fb	MDNS	438	Standard query 0x0000 PTR _airport._tc
462	6.621440	172.16.103.211	224.0.0.251	MDNS	182	Standard query response 0x0000 TXT OP1
463	6.621440	fe80::454:f6e:a8c:7...	ff02::fb	MDNS	202	Standard query response 0x0000 TXT OP1
464	6.636054	fe80::a25:25ff:fe84...	ff02::fb	MDNS	145	Standard query 0x0000 ANY Android-2.1c
465	6.639360	fe80::88a3:fc67:857...	ff02::1:3	LLMNR	85	Standard query 0x9bd1 A https

< >

> Frame 468: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{D7AF522C-2BC7-43EF-  
> Ethernet II, Src: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor\_c8:07:7c (00:15:17:c8:07:7c)  
> Internet Protocol Version 4, Src: 172.16.103.97, Dst: 13.107.4.52  
> Transmission Control Protocol, Src Port: 62239, Dst Port: 80, Seq: 0, Len: 0

< >

## Filter for all http get requests



The image shows a Wireshark capture of network traffic on a Wi-Fi interface. The filter bar at the top is set to "http.request". The packet list pane displays 20 packets, all of which are SSDP M-SEARCH requests. The packet details pane shows the structure of the selected packet (Frame 20), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Service Discovery Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
35081	399.401187	172.16.99.117	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
35082	399.401187	172.16.99.117	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
35157	400.465160	172.16.100.208	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
35172	400.767653	172.16.100.208	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
35193	401.094371	172.16.100.208	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
35473	406.282251	172.16.102.184	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
35536	407.344569	172.16.102.184	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
35645	409.302369	172.16.102.184	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
35913	413.797133	172.16.97.27	239.255.255.250	SSDP	211	M-SEARCH * HTTP/1.1
36047	414.812632	172.16.97.27	239.255.255.250	SSDP	211	M-SEARCH * HTTP/1.1
39573	420.446589	172.16.100.208	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
39588	420.769496	172.16.100.208	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
39595	420.985322	172.16.103.97	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39604	421.045261	172.16.103.97	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39605	421.051710	172.16.100.208	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
39669	421.999426	172.16.103.97	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39673	422.046582	172.16.103.97	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39730	423.004275	172.16.103.97	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39735	423.051791	172.16.103.97	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39832	424.006413	172.16.103.97	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39834	424.052453	172.16.103.97	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

> Frame 20: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF\_{D7AF...}

> Ethernet II, Src: vivoMobi\_5a:58:09 (30:af:ce:5a:58:09), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)

> Internet Protocol Version 4, Src: 172.16.100.208, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 46693, Dst Port: 1900

> Simple Service Discovery Protocol

0000 28 cd c4 c5 7b 7f 30 af ce 5a 58 09 08 00 45 00 (---{-0- -ZX---E-

0010 00 99 34 c2 40 00 01 11 43 b7 ac 10 64 d0 ef ff --4-@---C---d---

0020 ff 5a b5 65 07 6c 00 85 12 00 4d 2d 52 45 41 52 ---a-1---M-SEARCH

## Filter on three way handshake

The image shows a Wireshark network traffic capture window. The title bar reads '\*Wi-Fi'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. A filter bar at the top displays the filter expression: `tcp.flags.syn==1 or (tcp.seq_raw==1 and tcp.ack==1)`. Below the filter bar is a packet list table with columns: No., Time, Source, Destination, Protocol, Length, and Info. The table contains 24 entries, with alternating rows highlighted in light green and light grey. The selected packet is No. 468, a TCP SYN-ACK from 172.16.103.97 to 13.107.4.52. Below the packet list, the packet details pane shows the following information: Frame 468: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{D7AF522C-2BC7-...}; Ethernet II, Src: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor\_c8:07:7c (00:15:17:c8:07:7c); Internet Protocol Version 4, Src: 172.16.103.97, Dst: 13.107.4.52; Transmission Control Protocol, Src Port: 62239, Dst Port: 80, Seq: 0, Len: 0. At the bottom, the packet bytes pane shows the raw data in hexadecimal and ASCII. The selected packet's bytes are: 00 15 17 c8 07 7c 28 cd c4 c5 7b 7f 08 00 45 00 (ASCII: .....|(. ...{...E.); 00 34 7b f3 40 00 80 06 59 c0 ac 10 67 61 0d 6b (ASCII: -4{.@... Y...ga k); 04 34 f3 1f 00 50 16 95 ef bf 00 00 00 00 80 02 (ASCII: -4...P... ..); fa f0 55 4a 00 00 02 04 05 b4 01 03 03 08 01 01 (ASCII: ..UJ.....).

No.	Time	Source	Destination	Protocol	Length	Info
40438	427.909573	13.107.4.52	172.16.103.97	TCP	66	80 → 62330 [SYN, ACK] Seq=0 Ack=
40750	432.926427	172.16.103.97	20.44.229.112	TCP	66	62331 → 443 [SYN] Seq=0 Win=6424
40757	432.970147	20.44.229.112	172.16.103.97	TCP	66	443 → 62331 [SYN, ACK] Seq=0 Ack=
40997	435.760505	172.16.103.97	52.109.56.83	TCP	66	62332 → 443 [SYN] Seq=0 Win=6424
41003	435.798415	52.109.56.83	172.16.103.97	TCP	66	443 → 62332 [SYN, ACK] Seq=0 Ack=
41049	436.306200	172.16.103.97	52.109.56.83	TCP	66	62333 → 443 [SYN] Seq=0 Win=6424
41055	436.339647	52.109.56.83	172.16.103.97	TCP	66	443 → 62333 [SYN, ACK] Seq=0 Ack=
42441	457.947614	172.16.103.97	13.107.4.52	TCP	66	62334 → 80 [SYN] Seq=0 Win=64240
42446	457.960239	13.107.4.52	172.16.103.97	TCP	66	80 → 62334 [SYN, ACK] Seq=0 Ack=
42476	458.405927	172.16.103.97	34.117.237.239	TCP	66	62335 → 443 [SYN] Seq=0 Win=6424
42479	458.415854	34.117.237.239	172.16.103.97	TCP	66	443 → 62335 [SYN, ACK] Seq=0 Ack=
43585	477.441078	172.16.103.97	104.211.156.162	TCP	66	62336 → 443 [SYN] Seq=0 Win=6424
43586	477.469157	104.211.156.162	172.16.103.97	TCP	66	443 → 62336 [SYN, ACK] Seq=0 Ack=
44245	488.066821	172.16.103.97	13.107.4.52	TCP	66	62337 → 80 [SYN] Seq=0 Win=64240
44248	488.078161	13.107.4.52	172.16.103.97	TCP	66	80 → 62337 [SYN, ACK] Seq=0 Ack=
44758	496.246038	172.16.103.97	157.240.23.11	TCP	66	62338 → 443 [SYN] Seq=0 Win=6424
44764	496.253698	157.240.23.11	172.16.103.97	TCP	66	443 → 62338 [SYN, ACK] Seq=0 Ack=
46104	518.120075	172.16.103.97	13.107.4.52	TCP	66	62339 → 80 [SYN] Seq=0 Win=64240
46105	518.131795	13.107.4.52	172.16.103.97	TCP	66	80 → 62339 [SYN, ACK] Seq=0 Ack=
48083	548.164980	172.16.103.97	13.107.4.52	TCP	66	62340 → 80 [SYN] Seq=0 Win=64240
48094	548.183623	13.107.4.52	172.16.103.97	TCP	66	80 → 62340 [SYN, ACK] Seq=0 Ack=

> Frame 468: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{D7AF522C-2BC7-...}  
> Ethernet II, Src: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor\_c8:07:7c (00:15:17:c8:07:7c)  
> Internet Protocol Version 4, Src: 172.16.103.97, Dst: 13.107.4.52  
> Transmission Control Protocol, Src Port: 62239, Dst Port: 80, Seq: 0, Len: 0

Offset	Hex	ASCII
0000	00 15 17 c8 07 7c 28 cd c4 c5 7b 7f 08 00 45 00	..... (. ...{...E.
0010	00 34 7b f3 40 00 80 06 59 c0 ac 10 67 61 0d 6b	-4{.@... Y...ga k
0020	04 34 f3 1f 00 50 16 95 ef bf 00 00 00 00 80 02	-4...P... ..
0030	fa f0 55 4a 00 00 02 04 05 b4 01 03 03 08 01 01	..UJ.....

## Find executable or other file types

The image shows the Wireshark network protocol analyzer interface. The title bar indicates the capture is on the \*Wi-Fi interface. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like packet list, packet details, packet bytes, and search. The packet list pane shows a single packet, No. 38600, at time 418.689690, from source 157.240.23.25 to destination 172.16.103.97, using the QUIC protocol with a length of 1274 bytes. The packet info pane shows the packet is a Protected Payload (KP0). The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and QUIC IETF. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
38600	418.689690	157.240.23.25	172.16.103.97	QUIC	1274	Protected Payload (KP0)

Packet Details:

- Frame 38600: 1274 bytes on wire (10192 bits), 1274 bytes captured (10192 bits) on interface \Device\NPF\_{D7AF522C-2B0C-408A-8000-000000000000}
- Ethernet II, Src: IntelCor\_c8:07:7c (00:15:17:c8:07:7c), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)
- Internet Protocol Version 4, Src: 157.240.23.25, Dst: 172.16.103.97
- User Datagram Protocol, Src Port: 443, Dst Port: 56689
- QUIC IETF

## Search traffic based on a keyword

The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates the capture is on the \*Wi-Fi interface. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like capture, analysis, and packet manipulation. The packet list pane shows a capture of five packets, all from source 172.16.103.97 to destination 157.240.23.11, using the TLSv1.3 protocol. The packet details pane for the selected packet (No. 5) shows the structure: Frame 5 (144 bytes) on the wire, TLSv1.3 (130 bytes), and Client Hello (130 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
38228	418.116622	172.16.103.97	157.240.23.19	TLSv1.3	571	Client Hello
38236	418.117119	172.16.103.97	157.240.23.11	TLSv1.3	571	Client Hello
39754	423.237011	172.16.103.97	157.240.23.19	TLSv1.3	571	Client Hello
44766	496.254549	172.16.103.97	157.240.23.11	TLSv1.3	571	Client Hello
51373	601.975129	172.16.103.97	157.240.23.11	TLSv1.3	571	Client Hello

```
> Frame 38236: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{D7AF522C-
> Ethernet II, Src: Chongqin_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor_c8:07:7c (00:15:17:c8:07:7c)
> Internet Protocol Version 4, Src: 172.16.103.97, Dst: 157.240.23.11
> Transmission Control Protocol, Src Port: 62328, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Transport Layer Security
```

[illegible]

# Detecting SYN Floods (Possible DDoS attacks)

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 and tcp.flags.ack == 0

No.	Time	Source	Destination	Protocol	Length	Info
24000	308.854279	172.16.103.97	65.9.86.19	TCP	66	62307 → 443 [SYN] Seq=0 Win=64240 Len=
24001	308.854387	172.16.103.97	65.9.86.19	TCP	66	62308 → 443 [SYN] Seq=0 Win=64240 Len=
24002	308.854511	172.16.103.97	65.9.86.19	TCP	66	62309 → 443 [SYN] Seq=0 Win=64240 Len=
24023	308.964153	172.16.103.97	117.18.237.29	TCP	66	62310 → 80 [SYN] Seq=0 Win=64240 Len=0
24024	308.964656	172.16.103.97	117.18.237.29	TCP	66	62311 → 80 [SYN] Seq=0 Win=64240 Len=0
24064	309.010954	172.16.103.97	108.159.15.63	TCP	66	62312 → 443 [SYN] Seq=0 Win=64240 Len=
24066	309.011144	172.16.103.97	108.159.15.63	TCP	66	62313 → 443 [SYN] Seq=0 Win=64240 Len=
24158	309.211927	172.16.103.97	142.250.182.14	TCP	66	62314 → 443 [SYN] Seq=0 Win=64240 Len=
24281	309.642830	172.16.103.97	182.79.221.222	TCP	66	62315 → 443 [SYN] Seq=0 Win=64240 Len=
24313	309.725867	172.16.103.97	142.250.195.35	TCP	66	62316 → 80 [SYN] Seq=0 Win=64240 Len=0
24348	309.983079	172.16.103.97	23.3.70.24	TCP	66	62317 → 80 [SYN] Seq=0 Win=64240 Len=0
24571	310.581119	172.16.103.97	20.190.146.33	TCP	66	62318 → 443 [SYN] Seq=0 Win=65535 Len=
31494	337.639159	172.16.103.97	13.107.4.52	TCP	66	62319 → 80 [SYN] Seq=0 Win=64240 Len=0
31574	339.019093	172.16.103.97	40.79.150.120	TCP	66	62320 → 443 [SYN] Seq=0 Win=65535 Len=
33131	367.692206	172.16.103.97	13.107.4.52	TCP	66	62321 → 80 [SYN] Seq=0 Win=64240 Len=0
34796	395.972337	172.16.103.97	104.46.162.226	TCP	66	62322 → 443 [SYN] Seq=0 Win=64240 Len=
34968	397.778155	172.16.103.97	13.107.4.52	TCP	66	62323 → 80 [SYN] Seq=0 Win=64240 Len=0
36958	416.289335	172.16.103.97	116.119.107.146	TCP	66	62324 → 443 [SYN] Seq=0 Win=64240 Len=
37027	416.391125	172.16.103.97	116.119.107.146	TCP	66	62325 → 443 [SYN] Seq=0 Win=64240 Len=
37203	416.562894	172.16.103.97	116.119.107.146	TCP	66	62326 → 443 [SYN] Seq=0 Win=64240 Len=
38137	417.973969	172.16.103.97	157.240.23.19	TCP	66	62327 → 443 [SYN] Seq=0 Win=64240 Len=

< >

> Frame 38141: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{D7AF522C-2BC7-43EF  
> Ethernet II, Src: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor\_c8:07:7c (00:15:17:c8:07:7c)  
> Internet Protocol Version 4, Src: 172.16.103.97, Dst: 157.240.23.11  
> Transmission Control Protocol, Src Port: 62328, Dst Port: 443, Seq: 0, Len: 0

< >

0000 00 15 17 c8 07 7c 28 cd c4 c5 7b 7f 08 00 45 00 .....|(. ..{...E.  
0010 00 34 64 52 40 00 80 06 ce 04 ac 10 67 61 9d f0 -4dR@... ..ga..

## Part 2:

### Step 1:

The image shows a Wireshark network traffic capture window titled "\*Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The packet list pane displays a series of HTTP GET requests to /connecttest.txt. The packet details pane for the selected packet (No. 11696) shows the following layers: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
11696	27.611868	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
11699	27.646301	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
13551	57.694784	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
13553	57.708138	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
15569	87.783787	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
15578	87.865188	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
17426	117.891920	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
17428	117.936132	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
19234	148.009975	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
19236	148.029160	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
21884	178.075142	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
21887	178.105245	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
24291	208.206798	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
24293	208.217247	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
31636	233.377869	172.16.103.97	141.217.1.160	HTTP	491	GET / HTTP/1.1
31664	233.645251	141.217.1.160	172.16.103.97	HTTP	555	HTTP/1.1 307 Temporary Redirect (text/ht
33806	238.253839	172.16.103.97	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
33813	238.279654	13.107.4.52	172.16.103.97	HTTP	593	HTTP/1.1 200 OK (text/plain)
34128	241.379207	172.16.103.97	141.217.1.160	HTTP	793	GET / HTTP/1.1
34146	241.646186	141.217.1.160	172.16.103.97	HTTP	555	HTTP/1.1 307 Temporary Redirect (text/ht

> Frame 11696: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF\_{D7AF522C-2BC7-431...}

> Ethernet II, Src: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor\_c8:07:7c (00:15:17:c8:07:7c)

> Internet Protocol Version 4, Src: 172.16.103.97, Dst: 13.107.4.52

> Transmission Control Protocol, Src Port: 62390, Dst Port: 80, Seq: 1, Ack: 1, Len: 111

> Hypertext Transfer Protocol

0020 04 34 f3 b6 00 50 b7 45 07 a4 05 4e 20 48 50 18 .4...P.E...N HP.

0030 02 05 f0 8e 00 00 47 45 54 20 2f 63 6f 6e 6e 65 .....GE T /conne

0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f cctest.t xt HTTP/

0050 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 1.1..Con nection:

0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 Close.. User-Age

## Step 2:

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http.host==www.wayne.edu						
No.	Time	Source	Destination	Protocol	Length	Info
31636	233.377869	172.16.103.97	141.217.1.160	HTTP	491	GET / HTTP/1.1
34128	241.379207	172.16.103.97	141.217.1.160	HTTP	793	GET / HTTP/1.1

<

- > Frame 31636: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF\_{D7AF522...}
- > Ethernet II, Src: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f), Dst: IntelCor\_c8:07:7c (00:15:17:c8:07:7c)
- > Internet Protocol Version 4, Src: 172.16.103.97, Dst: 141.217.1.160
- > Transmission Control Protocol, Src Port: 62404, Dst Port: 80, Seq: 1, Ack: 1, Len: 437
- > Hypertext Transfer Protocol

<

0020	01 a0 f3 c4 00 50 18 be 4d f0 89 77 9b de 50 18	...P..M..w..P.
0030	02 01 2e 17 00 00 47 45 54 20 2f 20 48 54 54 50	.....GET / HTTP
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e	/1.1..Host: www.
0050	77 61 79 6e 65 2e 65 64 75 0d 0a 43 6f 6e 6e 65	wayne.ed u..Conne
0060	63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76	ction: keep-aliv
0070	65 0d 0a 55 70 67 73 61 64 65 2d 40 6a 73 65 63	...Header: Trac



# Dns

The image shows a Wireshark network traffic capture window titled "\*Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. The packet list pane on the left shows a list of 20 DNS packets. The packet details pane on the right shows the structure of a DNS response packet (Frame 31609). The packet bytes pane at the bottom shows the raw hex and ASCII data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
34145	241.623714	172.16.103.97	172.16.96.1	DNS	89	Standard query 0x133e A v10.events.
34148	241.657707	172.16.103.97	172.16.96.1	DNS	89	Standard query 0x133e A v10.events.
34153	241.677455	172.16.96.1	172.16.103.97	DNS	220	Standard query response 0x133e A v10.events.
34970	244.222721	172.16.103.97	172.16.96.1	DNS	79	Standard query 0x32a7 A pixel.sites
34990	244.258790	172.16.103.97	172.16.96.1	DNS	79	Standard query 0x32a7 A pixel.sites
35070	244.358441	172.16.96.1	172.16.103.97	DNS	95	Standard query response 0x32a7 A pixel.sites
35737	245.338121	172.16.103.97	172.16.96.1	DNS	74	Standard query 0x1562 A dpm.demdex.
35738	245.339004	172.16.103.97	172.16.96.1	DNS	75	Standard query 0x60f9 A pixel.tapad
35742	245.377770	172.16.103.97	172.16.96.1	DNS	75	Standard query 0x60f9 A pixel.tapad
35743	245.377770	172.16.103.97	172.16.96.1	DNS	74	Standard query 0x1562 A dpm.demdex.
35756	245.424093	172.16.96.1	172.16.103.97	DNS	91	Standard query response 0x60f9 A pixel.tapad
35761	245.424766	172.16.96.1	172.16.103.97	DNS	314	Standard query response 0x1562 A dpm.demdex.
35784	245.433616	172.16.96.1	172.16.103.97	DNS	91	Standard query response 0x60f9 A pixel.tapad
35785	245.433616	172.16.96.1	172.16.103.97	DNS	314	Standard query response 0x1562 A dpm.demdex.
35990	245.710001	172.16.103.97	172.16.96.1	DNS	73	Standard query 0x25f1 A sync.teads.
36020	245.750741	172.16.103.97	172.16.96.1	DNS	73	Standard query 0x25f1 A sync.teads.
36063	245.819520	172.16.103.97	172.16.96.1	DNS	87	Standard query 0x93de A sync.search
36064	245.824794	172.16.96.1	172.16.103.97	DNS	195	Standard query response 0x93de A sync.search
36079	245.859401	172.16.96.1	172.16.103.97	DNS	162	Standard query response 0x25f1 A sync.teads.
36257	246.093955	172.16.103.97	172.16.96.1	DNS	77	Standard query 0x8707 A bh.contextw
36271	246.124581	172.16.96.1	172.16.103.97	DNS	143	Standard query response 0x8707 A bh.contextw

> Frame 31609: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface \Device\NPF\_{D7AF522C-2BC7-43EF-9A9E-0800200C9A66} (08:00:20:0C:9A:66)

> Ethernet II, Src: IntelCor\_c8:07:7c (00:15:17:c8:07:7c), Dst: Chongqin\_c5:7b:7f (28:cd:c4:c5:7b:7f)

> Internet Protocol Version 4, Src: 172.16.96.1, Dst: 172.16.103.97

> User Datagram Protocol, Src Port: 53, Dst Port: 59008

> Domain Name System (response)

```
0000  28 cd c4 c5 7b 7f 00 15 17 c8 07 7c 08 00 45 00  (...{... ..|..E-
0010  00 65 aa ae 00 00 40 11 b0 56 ac 10 60 01 ac 10  .e...@. -V...
0020  67 61 00 35 e6 80 00 51 ea 3e 13 80 81 80 00 01  ga-5...Q ->.....
0030  00 02 00 00 00 00 03 77 77 77 05 77 61 79 6e 65  ....w ww-wayne
0040  03 65 64 75 00 00 01 00 01 c0 0c 00 05 00 01 00  .edu.... ..
```



## Following tcp

The image shows a Wireshark packet capture window titled '\*Wi-Fi'. The main pane displays a list of network packets. The selected packet is number 34128, which is an HTTP GET request. The details pane on the right shows the structure of this packet, including the request line, headers, status line, and the HTML body content.

No.	Time	Source	Destination	Protocol	Length	Info
31610	233.050773	172.16.103.97	141.217.1.160	TCP	66	62404 → 80 [SYN] Seq=0 Win=0 Len=0
31634	233.377331	141.217.1.160	172.16.103.97	TCP	66	80 → 62404 [SYN, ACK] Seq=62404 Win=65535 Len=0
31635	233.377479	172.16.103.97	141.217.1.160	TCP	54	62404 → 80 [ACK] Seq=1177 Win=0 Len=0
31636	233.377869	172.16.103.97	141.217.1.160	HTTP	491	GET / HTTP/1.1
31661	233.645078	141.217.1.160	172.16.103.97	TCP	60	80 → 62404 [ACK] Seq=1177 Win=0 Len=0
31664	233.645251	141.217.1.160	172.16.103.97	HTTP	555	HTTP/1.1 307 Temporary Redirect
31673	233.689354	172.16.103.97	141.217.1.160	TCP	54	62404 → 80 [ACK] Seq=1177 Win=0 Len=0
34128	241.379207	172.16.103.97	141.217.1.160	HTTP	793	GET / HTTP/1.1
34146	241.646186	141.217.1.160	172.16.103.97	HTTP	555	HTTP/1.1 307 Temporary Redirect
34156	241.688679	172.16.103.97	141.217.1.160	TCP	54	62404 → 80 [ACK] Seq=1177 Win=0 Len=0

Wireshark · Follow TCP Stream (tcp.stream eq 23) · Wi-Fi

GET / HTTP/1.1  
Host: www.wayne.edu  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9,ne;q=0.8

HTTP/1.1 307 Temporary Redirect  
Server: nginx  
Date: Mon, 19 Sep 2022 16:30:15 GMT  
Content-Type: text/html; charset=iso-8859-1  
Content-Length: 228  
Connection: keep-alive  
Location: https://wayne.edu/  
Cache-Control: max-age=0  
Expires: Mon, 19 Sep 2022 16:30:15 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>307 Temporary Redirect</title>  
</head><body>  
<h1>Temporary Redirect</h1>  
<p>The document has moved <a href="https://wayne.edu/">here</a>.</p>  
</body></html>

GET / HTTP/1.1