

LAB 1

What to hand in

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

TCP, HTTP, ARP, TLSv1.2, MDNS

The screenshot shows the Wireshark interface with a packet capture. The packet list pane on the left displays a list of captured packets. The packet details pane on the right shows the selected packet's structure. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2265	21:49:41.649055	192.168.1.16	128.119.245.12	TCP	66	49861 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2266	21:49:41.676113	157.55.212.205	192.168.1.16	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2267	21:49:41.676185	192.168.1.16	157.55.212.205	TCP	54	49860 → 443 [ACK] Seq=334 Ack=7085 Win=261888 Len=0
2268	21:49:41.676770	192.168.1.16	157.55.212.205	TLSv1.2	543	Application Data
2269	21:49:41.676888	192.168.1.16	157.55.212.205	TCP	1494	49860 → 443 [ACK] Seq=823 Ack=7085 Win=261888 Len=1440 [TCP segment of a reassembled PDU]
2270	21:49:41.676888	192.168.1.16	157.55.212.205	TLSv1.2	430	Application Data
2271	21:49:41.702560	128.119.245.12	192.168.1.16	TCP	66	80 → 49861 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2272	21:49:41.702560	128.119.245.12	192.168.1.16	TCP	66	80 → 49862 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2273	21:49:41.702560	157.55.212.205	192.168.1.16	TCP	54	443 → 49860 [ACK] Seq=7085 Ack=2263 Win=262656 Len=0
2274	21:49:41.702722	192.168.1.16	128.119.245.12	TCP	54	49861 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2275	21:49:41.702801	192.168.1.16	128.119.245.12	TCP	54	49862 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2276	21:49:41.718572	192.168.1.16	128.119.245.12	HTTP	473	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2277	21:49:41.722673	157.55.212.205	192.168.1.16	TLSv1.2	747	Application Data
2278	21:49:41.722739	192.168.1.16	157.55.212.205	TCP	54	49860 → 443 [ACK] Seq=2639 Ack=7779 Win=261376 Len=0
2279	21:49:41.722823	192.168.1.16	157.55.212.205	TCP	54	49860 → 443 [FIN, ACK] Seq=2639 Ack=7779 Win=261376 Len=0
2280	21:49:41.750069	157.55.212.205	192.168.1.16	TCP	54	443 → 49860 [ACK] Seq=7779 Ack=2640 Win=262400 Len=0
2281	21:49:41.766364	128.119.245.12	192.168.1.16	TCP	54	80 → 49861 [ACK] Seq=1 Ack=420 Win=30336 Len=0
2282	21:49:41.780744	128.119.245.12	192.168.1.16	HTTP	491	HTTP/1.1 200 OK (text/html)
2283	21:49:41.780836	192.168.1.16	128.119.245.12	TCP	54	49861 → 80 [ACK] Seq=420 Ack=438 Win=261632 Len=0
2284	21:49:42.453291	192.168.1.3	224.0.0.251	MDNS	136	Standard query 0x0018 PTR _9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM" question PTR _googlec...
2285	21:49:42.453899	192.168.1.7	224.0.0.251	MDNS	400	Standard query response 0x0000 PTR Google-Home-Mini-25da0aff2c3323ec7af2dc5d4c7ee8b3._googlecast._tcp.local TXT, cache flush...
2286	21:49:42.515271	HewlettP_7f:e8:f5	Broadcast	ARP	60	Who has 169.254.58.47? (ARP Probe)
2287	21:49:43.538803	HewlettP_7f:e8:f5	Broadcast	ARP	60	Who has 169.254.58.47? (ARP Probe)
2288	21:49:43.957868	fe80::684f:bbaf:a66... ff02::2		ICMPv6	70	Router Solicitation from 74:46:a0:7f:e8:f5
2289	21:49:44.563993	HewlettP_7f:e8:f5	Broadcast	ARP	60	Who has 169.254.58.47? (ARP Probe)
2290	21:49:44.711755	192.168.1.16	130.211.26.229	TCP	1434	49810 → 443 [ACK] Seq=9014 Ack=7476 Win=129792 Len=1380 [TCP segment of a reassembled PDU]
2291	21:49:44.711755	192.168.1.16	130.211.26.229	TCP	1434	49810 → 443 [ACK] Seq=10394 Ack=7476 Win=129792 Len=1380 [TCP segment of a reassembled PDU]
2292	21:49:44.711755	192.168.1.16	130.211.26.229	TCP	1434	49810 → 443 [ACK] Seq=11774 Ack=7476 Win=129792 Len=1380 [TCP segment of a reassembled PDU]
2293	21:49:44.711755	192.168.1.16	130.211.26.229	TLSv1.3	842	Application Data
2294	21:49:44.714869	130.211.26.229	192.168.1.16	TCP	54	443 → 49810 [ACK] Seq=7476 Ack=10394 Win=83968 Len=0
2295	21:49:44.714869	130.211.26.229	192.168.1.16	TCP	54	443 → 49810 [ACK] Seq=7476 Ack=11774 Win=86784 Len=0
2296	21:49:44.715665	130.211.26.229	192.168.1.16	TCP	54	443 → 49810 [ACK] Seq=7476 Ack=13154 Win=89600 Len=0
2297	21:49:44.715665	130.211.26.229	192.168.1.16	TCP	54	443 → 49810 [ACK] Seq=7476 Ack=13942 Win=92160 Len=0
2298	21:49:44.723383	130.211.26.229	192.168.1.16	TLSv1.3	93	Application Data
2299	21:49:44.764357	192.168.1.16	130.211.26.229	TCP	54	49810 → 443 [ACK] Seq=13942 Ack=7515 Win=129792 Len=0

Frame 2284: 136 bytes on wire (1088 bits) captured (1088 bits) on interface \Device\NPF{0A5A0000-45AD-A65E-8550-33E983A0A1A1} id 0

0000 04 e3 33 b0 5c b6 c8 f2 30 de f9 1d 08 00 45 00 ...3... 0....E.

0010 00 7a 92 6f 40 00 ff 11 46 5c c0 a8 01 03 e0 00 ...z.o@... F.....

0020 00 fb 14 e9 14 e9 00 66 2f 87 00 18 00 00 00 02f /.....

Wireshark_Wi-Fi_20200707214909_e12640.pcapng

Packets: 2340 · Displayed: 2340 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

LAB 1

- How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

HTTP GET request was sent at - 21:49:41.718572

HTTP OK reply was received at – 21:49:41.780744

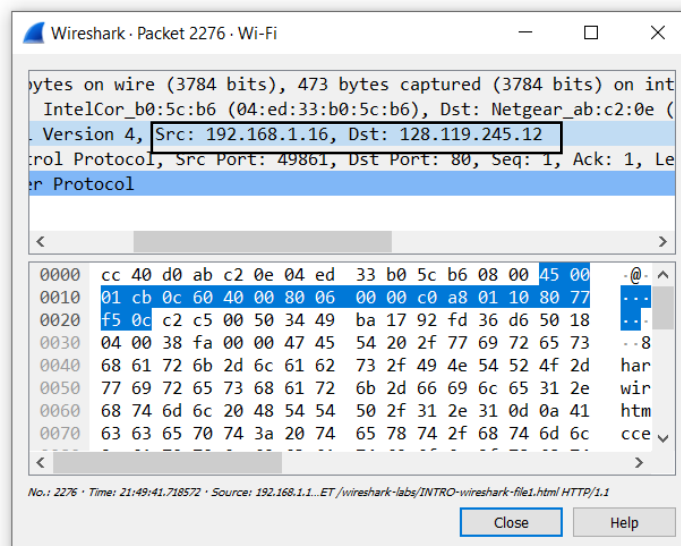
Time elapsed - 21:49:41.780744 – 21:49:41.718572 = 00:00:0.62172 Seconds

No.	Time	Source	Destination	Protocol	Length	Info
409	21:49:15.022444	192.168.1.16	192.168.1.12	HTTP	293	GET /dial/dd.xml HTTP/1.1
472	21:49:15.212759	192.168.1.12	192.168.1.16	HTTP/X...	1356	HTTP/1.1 200 OK
952	21:49:17.758861	192.168.1.16	5.62.48.18	HTTP	200	GET /v1/info HTTP/1.1
977	21:49:17.792894	5.62.48.18	192.168.1.16	HTTP	566	HTTP/1.1 200 OK (application/json)
2243	21:49:38.735723	77.234.46.107	192.168.1.16	HTTP	235	HTTP/1.1 200 OK
2276	21:49:41.718572	192.168.1.16	128.119.245.12	HTTP	473	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2282	21:49:41.780744	128.119.245.12	192.168.1.16	HTTP	491	HTTP/1.1 200 OK (text/html)
2326	21:49:48.190588	192.168.1.16	77.234.46.108	HTTP	340	GET /R/A20KIGJknjhMWN1ZDJKNTQzZmM5ZTBhNTVhYjA4YzMSYzcxEGQEBwcgGkKwCIgh-KggTB8DhoZaAASoHCAMQpoi-fjjqkpCgAUIGZK2d86FXHpLtrupHorS7D88...
2331	21:49:48.952504	77.234.46.108	192.168.1.16	HTTP	1463	HTTP/1.1 200 OK
2332	21:49:48.964156	192.168.1.16	77.234.46.108	HTTP	360	GET /R/A3oKIGJknjhMWN1ZDJKNTQzZmM5ZTBhNTVhYjA4YzMSYzcxEGQEBwcgG0EBIGh-KggTB8Dro5aAASoHCAMQpoi-fjILCAQQ660NgAEYgAo46pKQoAFCIGStnQe...

- What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

Internet address of the gaia.cs.umass.edu – **128.119.245.12 (Destination IP)**

Internet address of your computer – **192.168.1.16 (Source IP)**



LAB 1

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

No.	Time	Source	Destination	Protocol	Length	Info
2276	21:49:41.718572	192.168.1.16	128.119.245.12	HTTP	473	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 2276: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0

Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)

Internet Protocol Version 4, Src: 192.168.1.16, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 49861, Dst Port: 80, Seq: 1, Ack: 1, Len: 419

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
2282	21:49:41.780744	128.119.245.12	192.168.1.16	HTTP	491	HTTP/1.1 200 OK (text/html)

Frame 2282: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0

Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.16

Transmission Control Protocol, Src Port: 80, Dst Port: 49861, Seq: 1, Ack: 420, Len: 437

Hypertext Transfer Protocol

Line-based text data: text/html (3 lines)

PFA - Text file for the same

LAB 1

PART - 2

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

IP Address – 184.168.131.241

C:\Users\nanag>nslookup www.flipkart.in

Server: www.routerlogin.com

Address: 192.168.1.1

Non-authoritative answer:

Name: flipkart.in

Address: 184.168.131.241

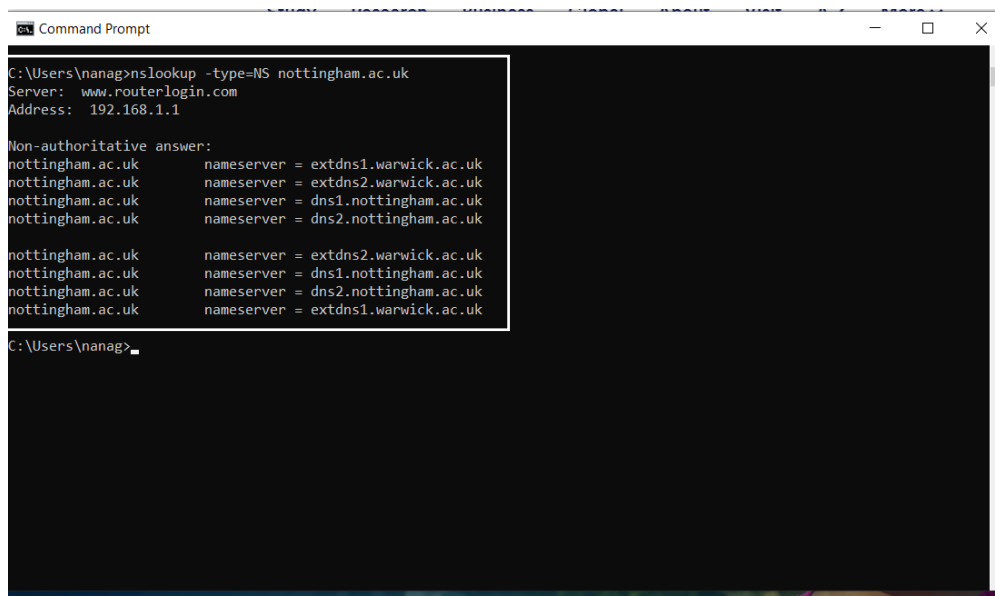
Aliases: www.flipkart.in



```
Command Prompt
C:\Users\nanag>nslookup www.flipkart.in
Server: www.routerlogin.com
Address: 192.168.1.1

Non-authoritative answer:
Name: flipkart.in
Address: 184.168.131.241
Aliases: www.flipkart.in
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.



```
Command Prompt
C:\Users\nanag>nslookup -type=NS nottingham.ac.uk
Server: www.routerlogin.com
Address: 192.168.1.1

Non-authoritative answer:
nottingham.ac.uk nameserver = extdns1.warwick.ac.uk
nottingham.ac.uk nameserver = extdns2.warwick.ac.uk
nottingham.ac.uk nameserver = dns1.nottingham.ac.uk
nottingham.ac.uk nameserver = dns2.nottingham.ac.uk

nottingham.ac.uk nameserver = extdns2.warwick.ac.uk
nottingham.ac.uk nameserver = dns1.nottingham.ac.uk
nottingham.ac.uk nameserver = dns2.nottingham.ac.uk
nottingham.ac.uk nameserver = extdns1.warwick.ac.uk

C:\Users\nanag>
```

LAB 1

4.) Locate the DNS query and response messages. Are then sent over UDP or TCP?

UDP

Wireshark packet capture showing DNS traffic. The packet list shows a query from 192.168.1.16 to 192.168.1.1. The packet details pane shows the query for www.google.com. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
231	23:30:50.747722	192.168.1.16	192.168.1.1	DNS	74	Standard query 0x00a3 A www.google.com
274	23:30:50.756093	192.168.1.1	192.168.1.16	DNS	194	Standard query response 0x00a3 A www.google.com A 172.217.9.4 NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns1.g...
322	23:30:50.928966	192.168.1.16	192.168.1.1	DNS	85	Standard query 0x1b1f A lh3.googleusercontent.com
326	23:30:50.932498	192.168.1.16	192.168.1.1	DNS	77	Standard query 0xeac7 A fonts.gstatic.com
388	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	146	Standard query response 0x1b1f A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 216.58.194.129 A 172...
389	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	129	Standard query response 0xeac7 A fonts.gstatic.com CNAME.gstaticadssl.l.google.com A 172.217.6.163
390	23:30:50.947680	192.168.1.16	192.168.1.1	DNS	75	Standard query 0x3ad2 A www.gstatic.com
398	23:30:50.953243	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0x3ad2 A www.gstatic.com A 172.217.1.227
485	23:30:54.453594	192.168.1.16	192.168.1.1	DNS	80	Standard query 0xa1c5 A beacons.gcp.gvt2.com
488	23:30:54.457575	192.168.1.1	192.168.1.16	DNS	126	Standard query response 0xa1c5 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 108.177.122.94
562	23:30:55.117027	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xedbe A apis.google.com
563	23:30:55.117109	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xc8 A ssl.gstatic.com
616	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	216	Standard query response 0xedbe A apis.google.com CNAME plus.l.google.com A 172.217.6.142 NS ns1.google.com NS ns4.google.com...
617	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0xc8 A ssl.gstatic.com A 172.217.6.163
1011	23:31:05.716522	192.168.1.16	192.168.1.1	DNS	79	Standard query 0xad5b A uta.instructure.com
1014	23:31:05.740734	192.168.1.1	192.168.1.16	DNS	219	Standard query response 0xad5b A uta.instructure.com CNAME cluster38.instructure.com CNAME canvas-iad-prod-c38-830190408.us...
1041	23:31:06.132977	192.168.1.16	192.168.1.1	DNS	72	Standard query 0x825a A www.ietf.org
1045	23:31:06.171575	192.168.1.1	192.168.1.16	DNS	149	Standard query response 0x825a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
1465	23:31:06.698810	192.168.1.16	192.168.1.1	DNS	78	Standard query 0x9359 A analytics.ietf.org
1782	23:31:06.816675	192.168.1.1	192.168.1.16	DNS	108	Standard query response 0x9359 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
1837	23:31:08.620957	192.168.1.16	192.168.1.1	DNS	92	Standard query 0x257f A protection-toolbar.urban-vpn.com
1838	23:31:08.620957	192.168.1.16	192.168.1.1	DNS	153	Standard query response 0x257f A protection-toolbar.urban-vpn.com CNAME protection-toolbar.urban-vpn.com A 200.126.102.128

Frame 231: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
> Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 63474, Dst Port: 53
> Domain Name System (query)

5. What is the destination port for the DNS query message? What is the source port of DNS response message?

The destination port for the DNS query message – 53

The source port of DNS response message – 53

Wireshark packet capture showing DNS traffic. The packet list shows a query from 192.168.1.16 to 192.168.1.1. The packet details pane shows the query for www.google.com. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
231	23:30:50.747722	192.168.1.16	192.168.1.1	DNS	74	Standard query 0x00a3 A www.google.com
274	23:30:50.756093	192.168.1.1	192.168.1.16	DNS	194	Standard query response 0x00a3 A www.google.com A 172.217.9.4 NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns1.g...
322	23:30:50.928966	192.168.1.16	192.168.1.1	DNS	85	Standard query 0x1b1f A lh3.googleusercontent.com
326	23:30:50.932498	192.168.1.16	192.168.1.1	DNS	77	Standard query 0xeac7 A fonts.gstatic.com
388	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	146	Standard query response 0x1b1f A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 216.58.194.129 A 172...
389	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	129	Standard query response 0xeac7 A fonts.gstatic.com CNAME.gstaticadssl.l.google.com A 172.217.6.163
390	23:30:50.947680	192.168.1.16	192.168.1.1	DNS	75	Standard query 0x3ad2 A www.gstatic.com
398	23:30:50.953243	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0x3ad2 A www.gstatic.com A 172.217.1.227
485	23:30:54.453594	192.168.1.16	192.168.1.1	DNS	80	Standard query 0xa1c5 A beacons.gcp.gvt2.com
488	23:30:54.457575	192.168.1.1	192.168.1.16	DNS	126	Standard query response 0xa1c5 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 108.177.122.94
562	23:30:55.117027	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xedbe A apis.google.com
563	23:30:55.117109	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xc8 A ssl.gstatic.com
616	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	216	Standard query response 0xedbe A apis.google.com CNAME plus.l.google.com A 172.217.6.142 NS ns1.google.com NS ns4.google.com...
617	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0xc8 A ssl.gstatic.com A 172.217.6.163
1011	23:31:05.716522	192.168.1.16	192.168.1.1	DNS	79	Standard query 0xad5b A uta.instructure.com
1014	23:31:05.740734	192.168.1.1	192.168.1.16	DNS	219	Standard query response 0xad5b A uta.instructure.com CNAME cluster38.instructure.com CNAME canvas-iad-prod-c38-830190408.us...
1041	23:31:06.132977	192.168.1.16	192.168.1.1	DNS	72	Standard query 0x825a A www.ietf.org
1045	23:31:06.171575	192.168.1.1	192.168.1.16	DNS	149	Standard query response 0x825a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
1465	23:31:06.698810	192.168.1.16	192.168.1.1	DNS	78	Standard query 0x9359 A analytics.ietf.org
1782	23:31:06.816675	192.168.1.1	192.168.1.16	DNS	108	Standard query response 0x9359 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
1837	23:31:08.620957	192.168.1.16	192.168.1.1	DNS	92	Standard query 0x257f A protection-toolbar.urban-vpn.com
1838	23:31:08.620957	192.168.1.16	192.168.1.1	DNS	153	Standard query response 0x257f A protection-toolbar.urban-vpn.com CNAME protection-toolbar.urban-vpn.com A 200.126.102.128

Frame 231: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
> Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 63474, Dst Port: 53
> Domain Name System (query)

LAB 1

No.	Time	Source	Destination	Protocol	Length	Info
231	23:30:50.747722	192.168.1.16	192.168.1.1	DNS	74	Standard query 0x00a3 A www.google.com
274	23:30:50.756093	192.168.1.1	192.168.1.16	DNS	194	Standard query response 0x00a3 A www.google.com A 172.217.9.4 NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns1.g...
322	23:30:50.928066	192.168.1.16	192.168.1.1	DNS	85	Standard query 0x1b1f A lh3.googleusercontent.com
326	23:30:50.932498	192.168.1.16	192.168.1.1	DNS	77	Standard query 0xeac7 A fonts.gstatic.com
388	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	146	Standard query response 0x1b1f A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 216.58.194.129 A 172...
389	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	129	Standard query response 0xeac7 A fonts.gstatic.com CNAME gstaticadssl1.l.google.com A 172.217.6.163
390	23:30:50.947680	192.168.1.16	192.168.1.1	DNS	75	Standard query 0x3ad2 A www.gstatic.com
398	23:30:50.953243	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0x3ad2 A www.gstatic.com A 172.217.1.227
485	23:30:54.453594	192.168.1.16	192.168.1.1	DNS	80	Standard query 0xalc5 A beacons.gcp.gvt2.com
488	23:30:54.457575	192.168.1.1	192.168.1.16	DNS	126	Standard query response 0xalc5 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 108.177.122.94
562	23:30:55.117027	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xedbe A apis.google.com
563	23:30:55.117109	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xccc8 A ssl.gstatic.com
616	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	216	Standard query response 0xedbe A apis.google.com CNAME plus-1.google.com A 172.217.6.142 NS ns1.google.com NS ns4.google.com...
617	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0xccc8 A ssl.gstatic.com A 172.217.6.163
1011	23:31:05.716522	192.168.1.16	192.168.1.1	DNS	79	Standard query 0xad5b A uta.instructure.com
1014	23:31:05.740734	192.168.1.1	192.168.1.16	DNS	219	Standard query response 0xad5b A uta.instructure.com CNAME cluster38.instructure.com CNAME canvas-lad-prod-c38-830190408.us...
1041	23:31:06.132977	192.168.1.16	192.168.1.1	DNS	72	Standard query 0x825a A www.ietf.org
1045	23:31:06.171575	192.168.1.1	192.168.1.16	DNS	149	Standard query response 0x825a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
1465	23:31:06.698810	192.168.1.16	192.168.1.1	DNS	78	Standard query 0x9359 A analytics.ietf.org
1782	23:31:06.816675	192.168.1.1	192.168.1.16	DNS	108	Standard query response 0x9359 A analytics.ietf.org CNAME ietf.org A 172.217.1.227

> Internet Protocol Version 4, Src Port: 53, Dst Port: 53, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 53, Dst Port: 63474
Domain Name System (query)

6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

YES, Both the IP Addresses are Same – 192.168.1.1

```
Command Prompt

C:\Users\lanag>ipconfig /all

Windows IP Configuration

Host Name . . . . . : LAPTOP-3IHJ273H
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 04-ED-33-B0-5C-B7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 06-ED-33-B0-5C-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Wireless-AC 9560 160MHz
Physical Address. . . . . : 04-ED-33-B0-5C-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::195e:6dcd:2061:2ccb%3(Preferred)
IPv4 Address. . . . . : 192.168.1.16(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, July 7, 2020 9:48:19 PM
Lease Expires . . . . . : Wednesday, July 8, 2020 9:48:19 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 56654515
DHCPv6 Client DUID . . . . . : 00-01-00-01-25-B0-5B-49-04-ED-33-B0-5C-B6
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

LAB 1

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
231	23:30:50.747722	192.168.1.16	192.168.1.1	DNS	74	Standard query 0x00a3 A www.google.com
274	23:30:50.756093	192.168.1.1	192.168.1.16	DNS	194	Standard query response 0x00a3 A www.google.com A 172.217.9.4 NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns1.g...
322	23:30:50.928966	192.168.1.16	192.168.1.1	DNS	85	Standard query 0x1b1f A lh3.googleusercontent.com
326	23:30:50.932498	192.168.1.16	192.168.1.1	DNS	77	Standard query 0xeac7 A fonts.gstatic.com
388	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	146	Standard query response 0x1b1f A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 216.58.194.129 A 172...
389	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	129	Standard query response 0xeac7 A fonts.gstatic.com CNAME.gstaticadssl.l.google.com A 172.217.6.163
390	23:30:50.947680	192.168.1.16	192.168.1.1	DNS	75	Standard query 0x3ad2 A www.gstatic.com
398	23:30:50.953243	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0x3ad2 A www.gstatic.com A 172.217.1.227
485	23:30:54.453594	192.168.1.16	192.168.1.1	DNS	80	Standard query 0xa1c5 A beacons.gcp.gvt2.com
488	23:30:54.457575	192.168.1.1	192.168.1.16	DNS	126	Standard query response 0xa1c5 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 108.177.122.94
562	23:30:55.117027	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xedbe A apis.google.com
563	23:30:55.117109	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xcc8 A ssl.gstatic.com
616	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	216	Standard query response 0xedbe A apis.google.com CNAME plus.l.google.com A 172.217.6.142 NS ns1.google.com NS ns4.google.com...
617	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0xcc8 A ssl.gstatic.com A 172.217.6.163
1011	23:31:05.716522	192.168.1.16	192.168.1.1	DNS	79	Standard query 0xad5b A uta.instructure.com
1014	23:31:05.740734	192.168.1.1	192.168.1.16	DNS	219	Standard query response 0xad5b A uta.instructure.com CNAME cluster38.instructure.com CNAME canvas-iad-prod-c38-830190408.us...
1041	23:31:06.132977	192.168.1.16	192.168.1.1	DNS	72	Standard query 0x825a A www.ietf.org
1045	23:31:06.171575	192.168.1.1	192.168.1.16	DNS	149	Standard query response 0x825a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
1465	23:31:06.698810	192.168.1.16	192.168.1.1	DNS	78	Standard query 0x9359 A analytics.ietf.org
1782	23:31:06.816675	192.168.1.1	192.168.1.16	DNS	108	Standard query response 0x9359 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
1837	23:31:08.620957	192.168.1.16	192.168.1.1	DNS	92	Standard query 0x257f A protection-toolbar.urban-vpn.com
1838	23:31:08.620957	192.168.1.1	192.168.1.16	DNS	152	Standard query response 0x257f A protection-toolbar.urban-vpn.com CNAME protection-toolbar.urban-vpn.com A 200.136.102.120

> Frame 231: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0

> Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)

> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 63474, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x00a3

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> www.google.com: type A, class IN

[Response In: 274]

7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

DNS Query – TYPE- A

No query message contains 0 Answers

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
231	23:30:50.747722	192.168.1.16	192.168.1.1	DNS	74	Standard query 0x00a3 A www.google.com
274	23:30:50.756093	192.168.1.1	192.168.1.16	DNS	194	Standard query response 0x00a3 A www.google.com A 172.217.9.4 NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns1.g...
322	23:30:50.928966	192.168.1.16	192.168.1.1	DNS	85	Standard query 0x1b1f A lh3.googleusercontent.com
326	23:30:50.932498	192.168.1.16	192.168.1.1	DNS	77	Standard query 0xeac7 A fonts.gstatic.com
388	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	146	Standard query response 0x1b1f A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 216.58.194.129 A 172...
389	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	129	Standard query response 0xeac7 A fonts.gstatic.com CNAME.gstaticadssl.l.google.com A 172.217.6.163
390	23:30:50.947680	192.168.1.16	192.168.1.1	DNS	75	Standard query 0x3ad2 A www.gstatic.com
398	23:30:50.953243	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0x3ad2 A www.gstatic.com A 172.217.1.227
485	23:30:54.453594	192.168.1.16	192.168.1.1	DNS	80	Standard query 0xa1c5 A beacons.gcp.gvt2.com
488	23:30:54.457575	192.168.1.1	192.168.1.16	DNS	126	Standard query response 0xa1c5 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 108.177.122.94
562	23:30:55.117027	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xedbe A apis.google.com
563	23:30:55.117109	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xcc8 A ssl.gstatic.com
616	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	216	Standard query response 0xedbe A apis.google.com CNAME plus.l.google.com A 172.217.6.142 NS ns1.google.com NS ns4.google.com...
617	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0xcc8 A ssl.gstatic.com A 172.217.6.163
1011	23:31:05.716522	192.168.1.16	192.168.1.1	DNS	79	Standard query 0xad5b A uta.instructure.com
1014	23:31:05.740734	192.168.1.1	192.168.1.16	DNS	219	Standard query response 0xad5b A uta.instructure.com CNAME cluster38.instructure.com CNAME canvas-iad-prod-c38-830190408.us...
1041	23:31:06.132977	192.168.1.16	192.168.1.1	DNS	72	Standard query 0x825a A www.ietf.org
1045	23:31:06.171575	192.168.1.1	192.168.1.16	DNS	149	Standard query response 0x825a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85
1465	23:31:06.698810	192.168.1.16	192.168.1.1	DNS	78	Standard query 0x9359 A analytics.ietf.org
1782	23:31:06.816675	192.168.1.1	192.168.1.16	DNS	108	Standard query response 0x9359 A analytics.ietf.org CNAME ietf.org A 4.31.198.44
1837	23:31:08.620957	192.168.1.16	192.168.1.1	DNS	92	Standard query 0x257f A protection-toolbar.urban-vpn.com
1838	23:31:08.620957	192.168.1.1	192.168.1.16	DNS	152	Standard query response 0x257f A protection-toolbar.urban-vpn.com CNAME protection-toolbar.urban-vpn.com A 200.136.102.120

> Frame 231: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0

> Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)

> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 63474, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x00a3

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> www.google.com: type A, class IN

[Response In: 274]

LAB 1

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

ANSWERS = 2

Each answer contains NAME, TYPE, Class, Time to Live, Data length, CNAME, Address

The image shows a Wireshark capture of DNS traffic. The top pane displays a list of captured packets, with the 485th packet selected. The bottom pane provides a detailed view of this packet's structure.

No.	Time	Source	Destination	Protocol	Length	Info
231	23:30:50.747722	192.168.1.16	192.168.1.1	DNS	74	Standard query 0x00a3 A www.google.com
274	23:30:50.756093	192.168.1.1	192.168.1.16	DNS	194	Standard query response 0x00a3 A www.google.com A 172.217.9.4 NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns1.g...
322	23:30:50.928966	192.168.1.16	192.168.1.1	DNS	85	Standard query 0x1b1f A lh3.googleusercontent.com
326	23:30:50.932498	192.168.1.16	192.168.1.1	DNS	77	Standard query 0xeac7 A fonts.gstatic.com
388	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	146	Standard query response 0x1b1f A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 216.58.194.129 A 172...
389	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	129	Standard query response 0xeac7 A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 172.217.6.163
390	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	75	Standard query 0x3ad2 A www.gstatic.com
398	23:30:50.953243	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0x3ad2 A www.gstatic.com A 172.217.1.227
485	23:30:54.453594	192.168.1.16	192.168.1.1	DNS	80	Standard query 0xalc5 A beacons.gcp.gvt2.com
488	23:30:54.457575	192.168.1.1	192.168.1.16	DNS	126	Standard query response 0xalc5 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 108.177.122.94
562	23:30:55.117027	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xedbe A apis.google.com
563	23:30:55.117109	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xcc8 A ssl.gstatic.com
616	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	216	Standard query response 0xedbe A apis.google.com CNAME plus.l.google.com A 172.217.6.142 NS ns1.google.com NS ns4.google.com...
617	23:30:55.128398	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0xcc8 A ssl.gstatic.com A 172.217.6.163
1011	23:31:05.716522	192.168.1.16	192.168.1.1	DNS	79	Standard query 0xad5b A uta.instructure.com
1014	23:31:05.740734	192.168.1.1	192.168.1.16	DNS	219	Standard query response 0xad5b A uta.instructure.com CNAME cluster38.instructure.com CNAME canvas-iad-prod-c38-830190408.us-...

Packet 488 Details:

- Answer RRs: 2
- Authority RRs: 0
- Additional RRs: 0
- Queries
 - > beacons.gcp.gvt2.com: type A, class IN
- Answers
 - > beacons.gcp.gvt2.com: type CNAME, class IN, cname beacons-handoff.gcp.gvt2.com
 - Name: beacons.gcp.gvt2.com
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 229 (3 minutes, 49 seconds)
 - Data length: 18
 - CNAME: beacons-handoff.gcp.gvt2.com
 - > beacons-handoff.gcp.gvt2.com: type A, class IN, addr 108.177.122.94
 - Name: beacons-handoff.gcp.gvt2.com
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 229 (3 minutes, 49 seconds)
 - Data length: 4
 - Address: 108.177.122.94

[Request in: 485]
[Time: 0.003981000 seconds]

LAB 1

9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message – **YES, local IP – 192.168.1.16**

```
Command Prompt
C:\Users\nanag>ipconfig /all

Windows IP Configuration

Host Name . . . . . : LAPTOP-3IHJ273H
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 04-ED-33-B0-5C-B7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 06-ED-33-B0-5C-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) Wireless-AC 9560 160MHz
Physical Address. . . . . : 04-ED-33-B0-5C-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::195e:6dcd:2061:2ccb%3(Preferred)
IPv4 Address. . . . . : 192.168.1.16(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, July 7, 2020 9:48:19 PM
Lease Expires . . . . . : Wednesday, July 8, 2020 9:48:19 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 50654515
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-B0-58-49-04-ED-33-B0-5C-B6
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\nanag>ipconfig /flushdns
```

The image shows a Wireshark packet capture on the Wi-Fi interface. The packet list on the left shows a series of packets, with packet 397 highlighted in green. The packet details pane on the right shows the structure of this packet, which is a TCP SYN packet. The packet bytes pane at the bottom shows the raw data of the packet.

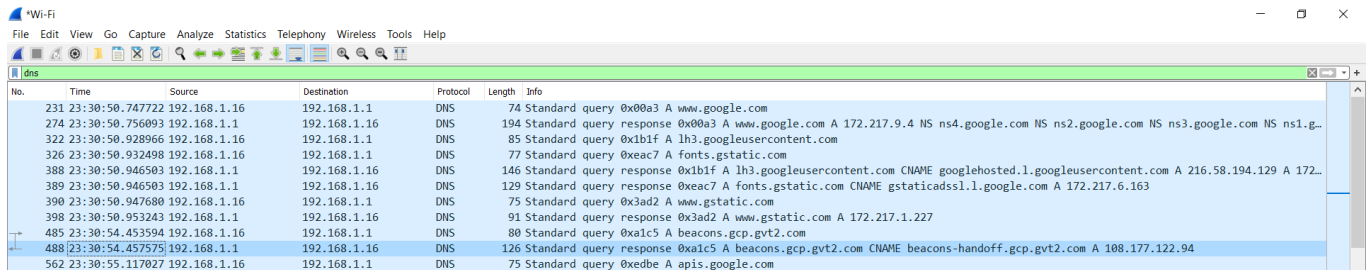
No.	Time	Source	Destination	Protocol	Length	Info
382	23:30:50.941251	216.58.193.131	192.168.1.16	TLSv1.2	1484	Application Data, Application Data
383	23:30:50.941251	216.58.193.131	192.168.1.16	TLSv1.2	1484	Application Data [TCP segment of a reassembled PDU]
384	23:30:50.941251	216.58.193.131	192.168.1.16	TLSv1.2	1484	Application Data [TCP segment of a reassembled PDU]
385	23:30:50.941657	192.168.1.16	216.58.193.131	TCP	54	50947 → 443 [ACK] Seq=484 Ack=70307 Win=512 Len=0
386	23:30:50.943201	216.58.193.131	192.168.1.16	TLSv1.2	324	Application Data, Application Data
387	23:30:50.943437	192.168.1.16	216.58.193.131	TCP	54	50947 → 443 [ACK] Seq=484 Ack=70577 Win=511 Len=0
391	23:30:50.947919	192.168.1.16	172.17.0.129	TCP	54	50979 → 80 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
392	23:30:50.948172	192.168.1.16	172.17.0.129	TCP	66	50982 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
393	23:30:50.948454	192.168.1.16	172.17.0.129	TLSv1.2	54	Application Data
394	23:30:50.951035	172.17.0.129	192.168.1.16	TCP	54	443 → 50944 [ACK] Seq=278681 Ack=339 Win=256 Len=0
395	23:30:50.952524	172.17.0.129	192.168.1.16	TLSv1.2	93	[TCP Previous segment not captured], Application Data
396	23:30:50.952574	192.168.1.16	172.17.0.129	TCP	66	[TCP Dup ACK 261#1] 50944 → 443 [ACK] Seq=339 Ack=278681 Win=2048 Len=0 SLE=278966 SRE=279005
397	23:30:50.953243	172.17.0.129	192.168.1.16	TCP	66	443 → 50982 [SYN, ACK] Seq=0 Ack=1 Win=50720 Len=0 MSS=1380 SACK_PERM=1 WS=256
399	23:30:50.953310	192.168.1.16	172.17.0.129	TCP	54	50982 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
400	23:30:50.954041	172.17.0.129	192.168.1.16	TCP	128	[TCP Out-Of-Order] 443 → 50944 [PSH, ACK] Seq=278681 Ack=339 Win=256 Len=74
401	23:30:50.954041	172.17.0.129	192.168.1.16	TCP	265	[TCP Out-Of-Order] 443 → 50944 [PSH, ACK] Seq=278755 Ack=339 Win=256 Len=211
402	23:30:50.954118	192.168.1.16	172.17.0.129	TCP	54	50944 → 443 [ACK] Seq=339 Ack=279005 Win=2047 Len=0
403	23:30:50.954402	192.168.1.16	216.58.193.131	TLSv1.2	93	Application Data
404	23:30:50.954881	192.168.1.16	172.17.0.129	TLSv1.2	93	Application Data
405	23:30:50.956106	192.168.1.16	216.58.193.131	TLSv1.2	150	Application Data
406	23:30:50.959072	216.58.193.131	192.168.1.16	TCP	54	443 → 50947 [ACK] Seq=70577 Ack=619 Win=311 Len=0
407	23:30:50.960873	216.58.193.131	192.168.1.16	TLSv1.2	128	Application Data

> Frame 397: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
> Ethernet II, Src: Netgear_abic2:0e(cc:40:40:ab:c2:0e), Dst: Totalcon_b0:5c:b6(04:ed:33:b0:5c:b6)
> Internet Protocol Version 4, Src: 172.17.0.129, Dst: 192.168.1.16
✚ Transmission Control Protocol, Src Port: 50982, Seq: 0, Ack: 1, Len: 0

LAB 1

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

NO it does not issue new DNS queries.



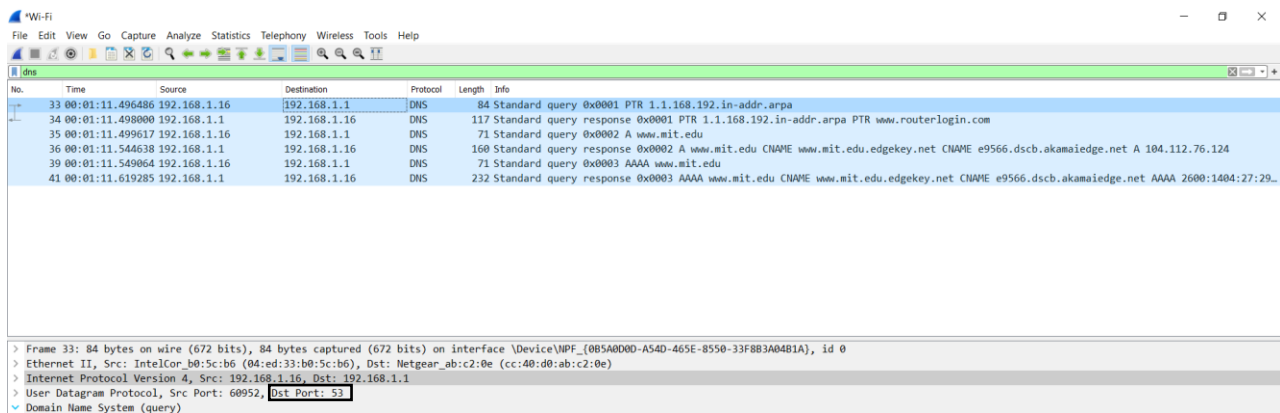
Wireshark capture of DNS traffic. The table below shows the captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
231	23:30:50.747722	192.168.1.16	192.168.1.1	DNS	74	Standard query 0x00a3 A www.google.com
274	23:30:50.750993	192.168.1.1	192.168.1.16	DNS	194	Standard query response 0x00a3 A www.google.com A 172.217.9.4 NS ns4.google.com NS ns2.google.com NS ns3.google.com NS ns1.g...
322	23:30:50.928966	192.168.1.16	192.168.1.1	DNS	85	Standard query 0x1b1f A lh3.googleusercontent.com
326	23:30:50.932498	192.168.1.16	192.168.1.1	DNS	77	Standard query 0xeac7 A fonts.gstatic.com
388	23:30:50.946503	192.168.1.1	192.168.1.16	DNS	146	Standard query response 0x1b1f A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 216.58.194.129 A 172...
389	23:30:50.946503	192.168.1.16	192.168.1.1	DNS	129	Standard query response 0xeac7 A fonts.gstatic.com CNAME.gstaticadssl1.l.google.com A 172.217.6.163
390	23:30:50.947680	192.168.1.16	192.168.1.1	DNS	75	Standard query 0x3ad2 A www.gstatic.com
398	23:30:50.953243	192.168.1.1	192.168.1.16	DNS	91	Standard query response 0x3ad2 A www.gstatic.com A 172.217.1.227
485	23:30:54.453594	192.168.1.16	192.168.1.1	DNS	80	Standard query 0xa1c5 A beacons.gcp.gvt2.com
498	23:30:54.457575	192.168.1.1	192.168.1.16	DNS	126	Standard query response 0xa1c5 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 108.177.122.94
562	23:30:55.117027	192.168.1.16	192.168.1.1	DNS	75	Standard query 0xedbe A apis.google.com

11. What is the destination port for the DNS query message? What is the source port of DNS response message?

The destination port for the DNS query message – **53**

The source port of DNS response message – **53**

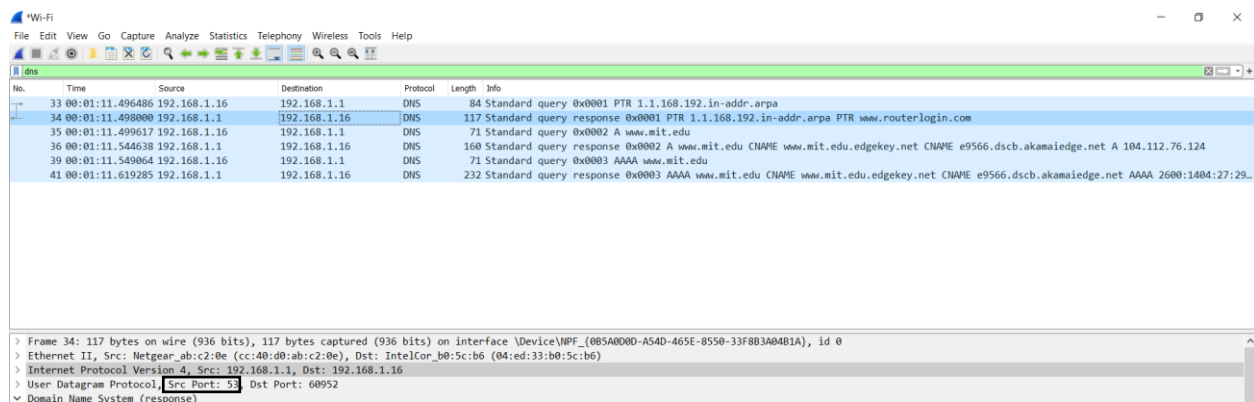


Wireshark capture of DNS traffic. The table below shows the captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
33	00:01:11.496486	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
34	00:01:11.498000	192.168.1.1	192.168.1.16	DNS	117	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR www.routerlogin.com
35	00:01:11.499617	192.168.1.16	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
36	00:01:11.544638	192.168.1.1	192.168.1.16	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.112.76.124
39	00:01:11.549064	192.168.1.16	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
41	00:01:11.619285	192.168.1.1	192.168.1.16	DNS	232	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:1404:27:29...

Packet details for Frame 33:

- Frame 33: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
- Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)
- Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 60952, Dst Port: 53
- Domain Name System (query)



Wireshark capture of DNS traffic. The table below shows the captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
33	00:01:11.496486	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
34	00:01:11.498000	192.168.1.1	192.168.1.16	DNS	117	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR www.routerlogin.com
35	00:01:11.499617	192.168.1.16	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
36	00:01:11.544638	192.168.1.1	192.168.1.16	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.112.76.124
39	00:01:11.549064	192.168.1.16	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
41	00:01:11.619285	192.168.1.1	192.168.1.16	DNS	232	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:1404:27:29...

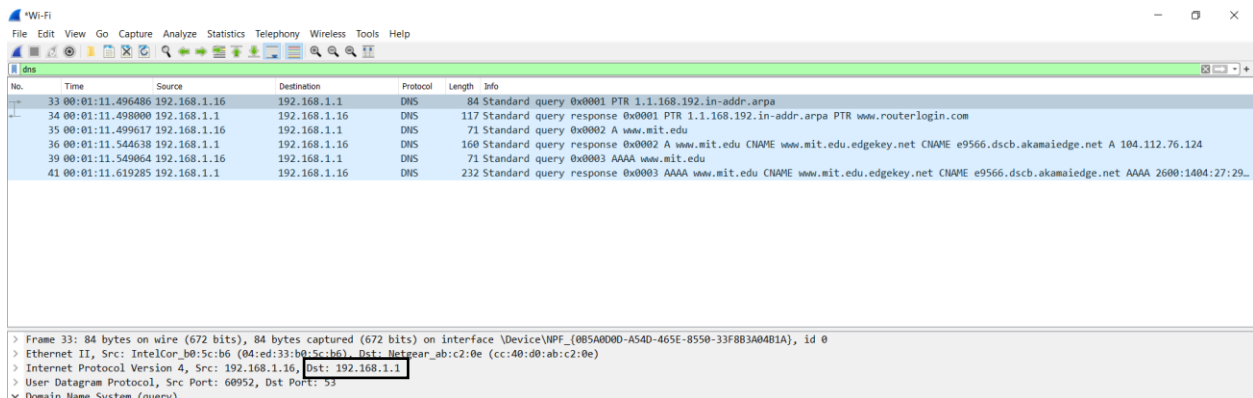
Packet details for Frame 34:

- Frame 34: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{0B5A0D0D-A54D-465E-8550-33F8B3A04B1A}, id 0
- Ethernet II, Src: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.16
- User Datagram Protocol, Src Port: 53, Dst Port: 60952
- Domain Name System (response)

LAB 1

12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

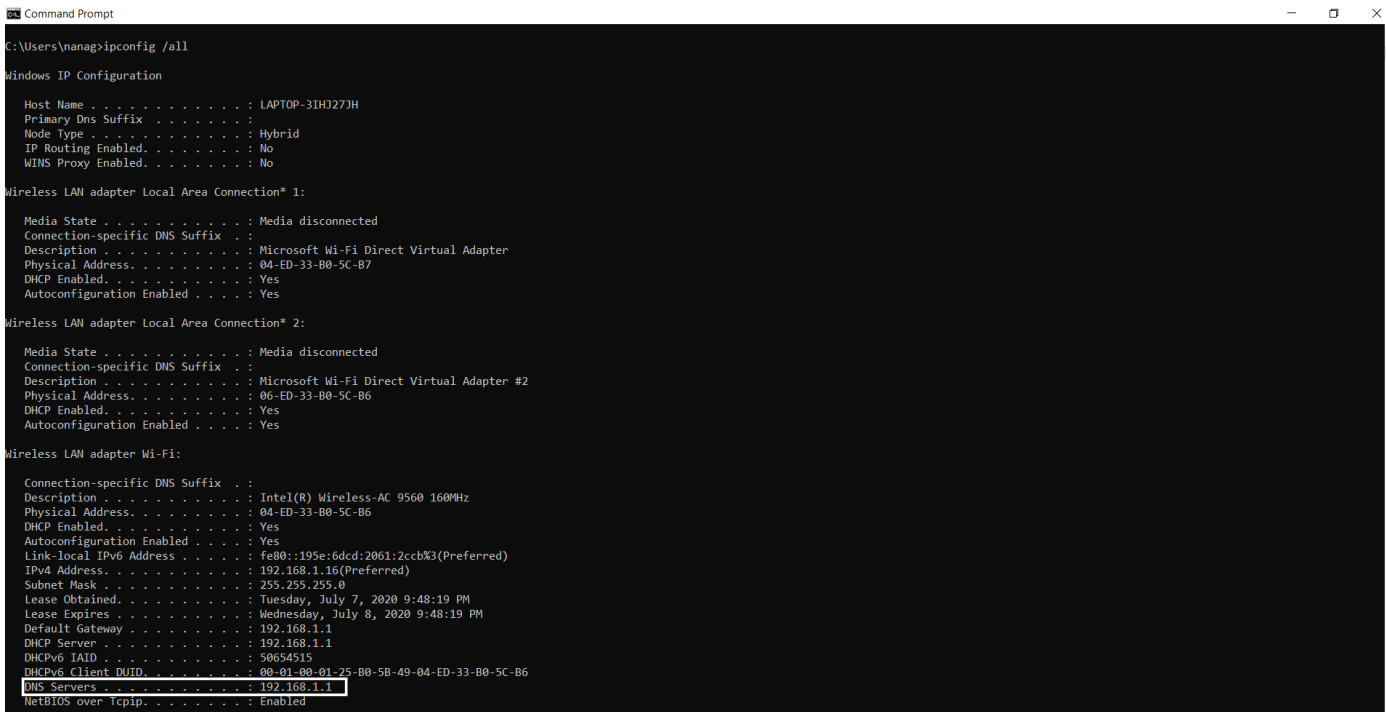
DNS query message IP address sent And the IP address of your default local DNS server are same – **192.168.1.1**



The image shows a Wireshark packet capture window titled '*Wi-Fi'. The packet list pane shows several DNS packets. The selected packet is packet 41, a 'Standard query response' from 192.168.1.1 to 192.168.1.1. The packet details pane shows the 'Domain Name System (query)' section, with the 'Destination' field highlighted as '192.168.1.1'.

No.	Time	Source	Destination	Protocol	Length	Info
33	00:01:11.496486	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
34	00:01:11.498000	192.168.1.1	192.168.1.16	DNS	117	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR www.routerlogin.com
35	00:01:11.499617	192.168.1.16	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
36	00:01:11.544638	192.168.1.1	192.168.1.16	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.112.76.124
39	00:01:11.549064	192.168.1.16	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
41	00:01:11.619285	192.168.1.1	192.168.1.16	DNS	232	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2600:1404:27:29...

> Frame 33: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{0B5A0D00-A54D-465E-8550-33F8B3A04B1A}, id 0
> Ethernet II, Src: IntelCor_b0:5c:b6 (04:ed:33:b0:5c:b6), Dst: Netgear_ab:c2:0e (cc:40:d0:ab:c2:0e)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 60952, Dst Port: 53
v Domain Name System (query)



The image shows a Windows Command Prompt window displaying the output of the 'ipconfig /all' command. The output shows the configuration for the 'Wireless LAN adapter Wi-Fi' interface, which is the active network connection. The 'DNS Servers' field is highlighted, showing the IP address '192.168.1.1'.

```
C:\Users\nanag>ipconfig /all

Windows IP Configuration

Host Name . . . . . : LAPTOP-3IHJ27JH
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 04-ED-33-B0-5C-B7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 06-ED-33-B0-5C-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) Wireless-AC 9560 160MHz
Physical Address. . . . . : 04-ED-33-B0-5C-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::195e:6dcd:2061:2ccb%3(Preferred)
IPv4 Address. . . . . : 192.168.1.16(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, July 7, 2020 9:48:19 PM
Lease Expires . . . . . : Wednesday, July 8, 2020 9:48:19 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 50654515
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-B0-5B-49-04-ED-33-B0-5C-B6
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

LAB 1

13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

TYPE – AAAA

No query message does not contain any Answers. Answers = 0

The image shows a Wireshark packet capture of a DNS query. The packet list pane shows several DNS packets. Packet 39 is selected, which is a standard query for the AAAA record of www.mit.edu. The packet details pane shows the following structure:

- Domain Name System (query)
 - Transaction ID: 0x0003
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.mit.edu: type AAAA, class IN

The packet bytes pane shows the raw data of the query.

14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

ANSWERS = 4

Each answer contains NAME, TYPE, Class, Time to Live, Data length, CNAME, Address

The image shows a Wireshark packet capture of a DNS response. The packet list pane shows several DNS packets. Packet 41 is selected, which is a standard query response for the AAAA record of www.mit.edu. The packet details pane shows the following structure:

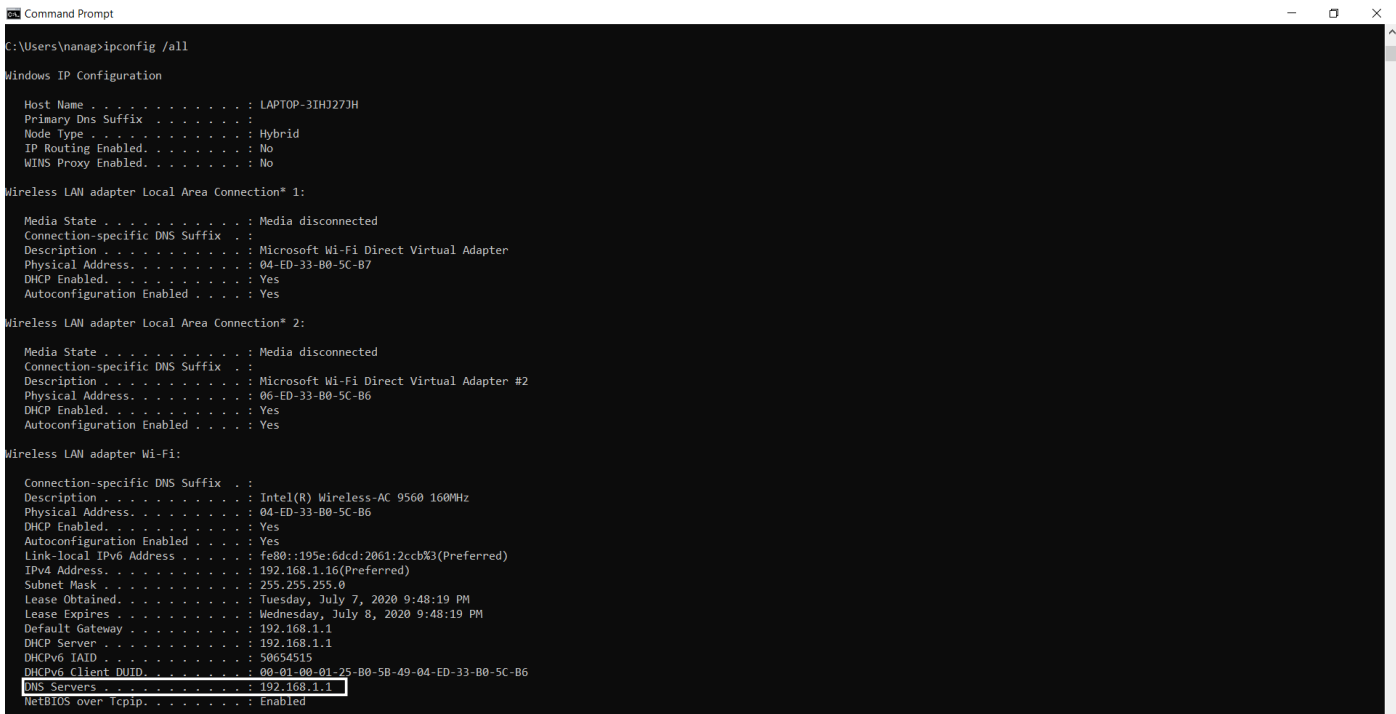
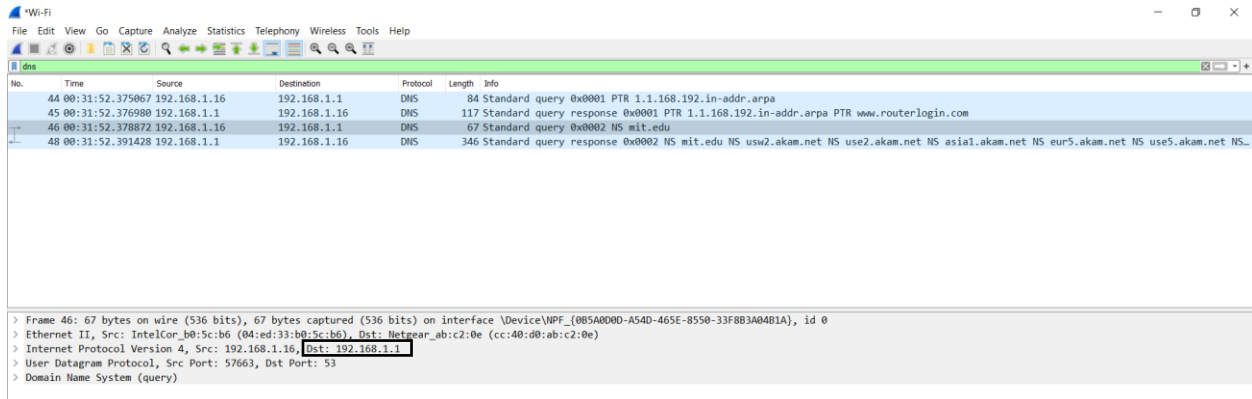
- Domain Name System (response)
 - Transaction ID: 0x0003
 - Flags: 0x8100 Standard query response, No error
 - Questions: 1
 - Answer RRs: 4
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.mit.edu: type AAAA, class IN
 - Answers
 - www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 - Name: www.mit.edu
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 1709 (28 minutes, 29 seconds)
 - Data length: 25
 - CNAME: www.mit.edu.edgekey.net
 - www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 - e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1404:5400:1971:255e
 - e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1404:5400:1811:255e

The packet bytes pane shows the raw data of the response.

LAB 1

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

YES, IP address the DNS query message is sent is same as my default local DNS server-

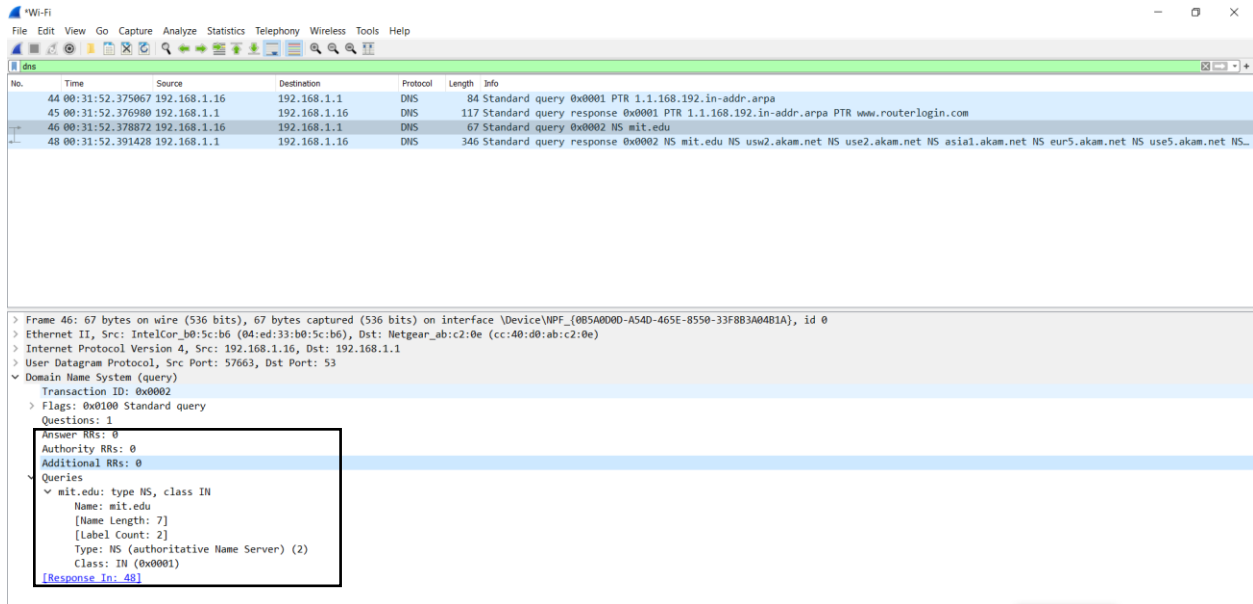


LAB 1

17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

TYPE – NS

No query message does not contain any Answers. Answers = 0



18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

usw2.akam.net
asia1.akam.net
eur5.akam.net
use5.akam.net
ns1-173.akam.net
asia2.akam.net
ns1-37.akam.net
use2.akam.net

YES, it does provide IP address of MIT nameservers

LAB 1

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

1 dns

No.	Time	Source	Destination	Protocol	Length	Info
44	00:31:52.375067	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
45	00:31:52.376980	192.168.1.1	192.168.1.16	DNS	117	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR www.routerlogin.com
46	00:31:52.378872	192.168.1.16	192.168.1.1	DNS	67	Standard query 0x0002 NS mit.edu
48	00:31:52.391428	192.168.1.1	192.168.1.16	DNS	346	Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS use2.akam.net NS asia1.akam.net NS eur5.akam.net NS use5.akam.net NS...

> User Datagram Protocol, Src Port: 53, Dst Port: 57663

▼ Domain Name System (response)

Transaction ID: 0x0002

> Flags: 0x8100 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 0

▼ Queries

- mit.edu: type NS, class IN
 - Name: mit.edu
 - [Name Length: 7]
 - [Label Count: 2]
 - Type: NS (authoritative Name Server) (2)
 - Class: IN (0x0001)

▼ Answers

- mit.edu: type NS, class IN, ns usw2.akam.net
 - Name: mit.edu
 - Type: NS (authoritative Name Server) (2)
 - Class: IN (0x0001)
 - Time to live: 1833 (17 minutes, 13 seconds)
 - Data length: 15
 - Name Server: usw2.akam.net
- mit.edu: type NS, class IN, ns use2.akam.net
 - Name: mit.edu
 - Type: NS (authoritative Name Server) (2)
 - Class: IN (0x0001)
 - Time to live: 1833 (17 minutes, 13 seconds)
 - Data length: 7
 - Name Server: use2.akam.net
- mit.edu: type NS, class IN, ns asia1.akam.net
 - Name: mit.edu