

1. Nslookup

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

Answer:

Command:

nslookup www.singaporeair.com.sg

Output:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3880]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup www.singaporeair.com.sg
Server: UnKnown
Address: 192.168.100.1

Non-authoritative answer:
Name:      e8976.x.akamaiedge.net
Address:  104.83.118.106
Aliases:  www.singaporeair.com.sg
          singaporeair-redirects1.com.edgekey.net
```

Analysis:

The IP address for www.singaporeair.com.sg is 104.83.118.106.

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

Answer:

Command:

nslookup -type=NS ox.ac.uk

Output:

```
C:\Windows\System32>nslookup -type=NS ox.ac.uk
Server: UnKnown
Address: 192.168.100.1

Non-authoritative answer:
ox.ac.uk      nameserver = dns2.ox.ac.uk
ox.ac.uk      nameserver = dns1.ox.ac.uk
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk
ox.ac.uk      nameserver = dns0.ox.ac.uk
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk

dns2.ox.ac.uk internet address = 163.1.2.190
auth4.dns.ox.ac.uk internet address = 45.33.127.156
auth5.dns.ox.ac.uk internet address = 93.93.128.67
auth6.dns.ox.ac.uk internet address = 185.24.221.32
dns0.ox.ac.uk internet address = 129.67.1.190
dns1.ox.ac.uk internet address = 129.67.1.191
```

Analysis:

The authoritative DNS servers are:

- dns2.ox.ac.uk (163.1.2.190)
 - dns1.ox.ac.uk (129.67.1.191)
 - auth4.dns.ox.ac.uk (45.33.127.156)
 - auth6.dns.ox.ac.uk (185.24.221.32)
 - dns0.ox.ac.uk (129.67.1.190)
 - auth5.dns.ox.ac.uk (93.93.128.67)
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Answer:

Command:

```
nslookup -type=MX yahoo.com 8.8.8.8
```

Output:

```
C:\Windows\System32>nslookup -type=MX yahoo.com 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
yahoo.com      MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
```

Analysis:

The mail servers for Yahoo! mail are:

- mta6.am0.yahoodns.net
- mta7.am0.yahoodns.net

- mta5.am0.yahoodns.net

2. ipconfig

Command no 1:

Ipconfig /all

Output:

```
Administrator: Command Prompt
C:\Windows\System32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Faizan
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek(R) PCI(e) Ethernet Controller
Physical Address. . . . . : B0-83-FE-BA-07-E7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::392b:2c8:a413:a6d5%3(Preferred)
IPv4 Address. . . . . : 192.168.100.7(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, 16 July 2024 10:43:05 pm
Lease Expires . . . . . : Friday, 19 July 2024 10:43:04 pm
Default Gateway . . . . . : fe80::1%3
                          192.168.100.1
DHCP Server . . . . . : 192.168.100.1
DHCPv6 IAID . . . . . : 112231422
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-1A-5F-B3-B0-83-FE-BA-07-E7
DNS Servers . . . . . : 192.168.100.1
NetBIOS over Tcpip. . . . . : Enabled
```

Analysis:

Key Information:

- Host Name: Faizan
- Primary DNS Suffix: (Not provided)
- Node Type: Hybrid
- IP Routing Enabled: No
- WINS Proxy Enabled: No

Ethernet Adapter Details:

- Description: Realtek(R) PCI(e) Ethernet Controller
- Physical Address: B0-83-FE-BA-07-E7
- DHCP Enabled: Yes
- Autoconfiguration Enabled: Yes
- IPv6 Address: fe80::392b:2c8:a413
- %3 (Preferred)

- IPv4 Address: 192.168.100.7 (Preferred)
- Subnet Mask: 255.255.255.0
- Default Gateway: fe80::1%3, 192.168.100.1
- DHCP Server: 192.168.100.1
- DNS Servers: 192.168.100.1
- NetBIOS over Tcpi: Enabled

Command no 2:

Ipconfig /displaydns

Output:

```
C:\Windows\System32>ipconfig /displaydns

Windows IP Configuration

registeridm.com
-----
Record Name . . . . . : registeridm.com
Record Type . . . . . : 1
Time To Live . . . . . : 35332
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 169.61.27.133

Record Name . . . . . : ns2.tonec.com
Record Type . . . . . : 1
Time To Live . . . . . : 35332
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . . : 185.80.220.22

Record Name . . . . . : ns1.tonec.com
Record Type . . . . . : 1
Time To Live . . . . . : 35332
Data Length . . . . . : 4
Section . . . . . : Additional
A (Host) Record . . . . : 159.69.68.58

assets.msn.com
-----
Record Name . . . . . : assets.msn.com
Record Type . . . . . : 5
Time To Live . . . . . : 2
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : assets.msn.com.edgekey.net
```

Analysis:

This command displays the cached DNS entries on machine. Here are some key entries:

- registeridm.com - A record: 169.61.27.133
- ns2.tonec.com - A record: 185.80.220.22
- ns1.tonec.com - A record: 159.69.68.58
- assets.msn.com - CNAME record: assets.msn.com.edgekey.net -> e28578.d.akamaiedge.net -> A records: 96.17.207.79, 96.17.207.97
- secure.internetdownloadmanager.com - A record: 169.61.27.133
- dns2.ox.ac.uk - A record: 163.1.2.190
- auth6.dns.ox.ac.uk - A record: 185.24.221.32
- auth5.dns.ox.ac.uk - A record: 93.93.128.67

- dns0.ox.ac.uk - A record: 129.67.1.190
- auth4.dns.ox.ac.uk - A record: 45.33.127.156
- dns1.ox.ac.uk - A record: 129.67.1.191
- mirror3.internetdownloadmanager.com - A record: 174.127.113.77
- www.google.com.8d3jmh6uz7yi1rt9.fast-dns-host.com - CNAME record: cdn.fast-dns-host.com -
> A records: 85.25.211.177, 85.25.211.17

Command no 3:

Ipconfig /flushdns:

Output:

```
C:\Windows\System32>ipconfig /flushdns  
Windows IP Configuration  
Successfully flushed the DNS Resolver Cache.
```

Analysis:

This indicates that the DNS resolver cache has been successfully cleared.

3. Tracing DNS with Wireshark

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

Answer:

Wireshark interface showing network traffic analysis. The main pane displays a list of captured packets, with packet 1904 selected. The packet list pane shows the following details:

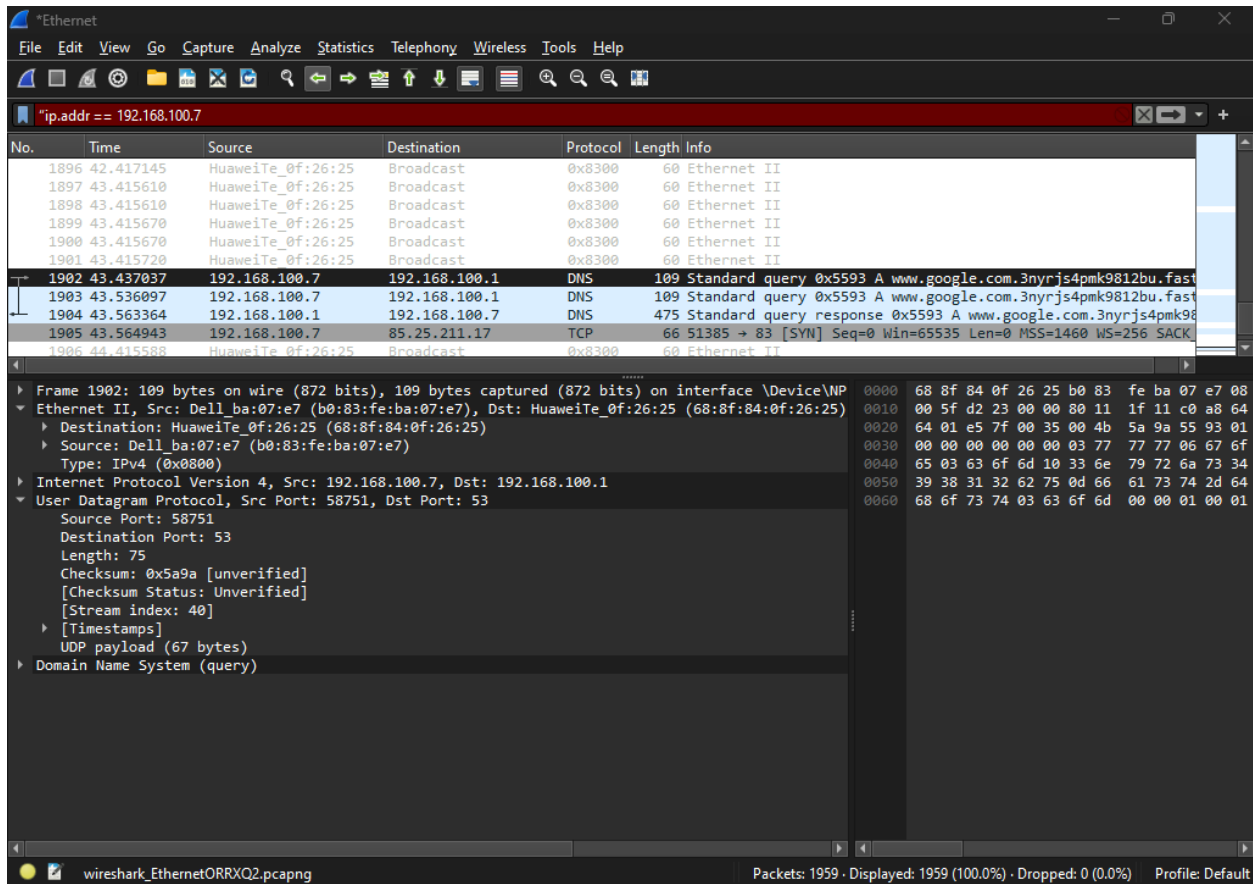
No.	Time	Source	Destination	Protocol	Length	Info
1896	42.417145	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1897	43.415610	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1898	43.415610	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1899	43.415670	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1900	43.415670	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1901	43.415720	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1902	43.437037	192.168.100.7	192.168.100.1	DNS	109	Standard query 0x5593 A www.google.com.3nyrjs4pmk9812bu.fast
1903	43.536097	192.168.100.7	192.168.100.1	DNS	109	Standard query 0x5593 A www.google.com.3nyrjs4pmk9812bu.fast
1904	43.563364	192.168.100.1	192.168.100.7	DNS	475	Standard query response 0x5593 A www.google.com.3nyrjs4pmk9812bu.fast
1905	43.564943	192.168.100.7	85.25.211.17	TCP	66	51385 → 83 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK
1906	44.415588	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II

The packet details pane for packet 1904 shows the following structure:

- Frame 1904: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface \Device\NPF... Ethernet II, Src: HuaweiTe_0f:26:25 (68:8f:84:0f:26:25), Dst: Dell_ba:07:e7 (b0:83:fe:ba:07:e7)
- Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.7
- User Datagram Protocol, Src Port: 53, Dst Port: 58751
 - Source Port: 53
 - Destination Port: 58751
 - Length: 441
 - Checksum: 0xd6ff [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 40]
 - [Timestamps]
 - [Time since first frame: 0.126327000 seconds]
 - [Time since previous frame: 0.027267000 seconds]
 - UDP payload (433 bytes)
- Domain Name System (response)
 - Transaction ID: 0x5593
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 2
 - Additional RRs: 12
 - Queries
 - Answers
 - www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com: type CNAME, class IN, cname cdn.fast-dns-host.com
 - cdn.fast-dns-host.com: type A, class IN, addr 85.25.211.17

The packet bytes pane shows the raw hex and ASCII data for the selected packet.

Encapsulation type (frame.encap_type) Packets: 1959 · Displayed: 1959 (100.0%) · Dropped: 0 (0.0%) Profile: Default



The DNS query message in Frame 1902 and 1904 is sent over UDP.

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

Answer:

From the DNS Query Message (Frame 1902):

Destination Port: 53 (standard port for DNS queries)

Source Port: 58751

From the DNS Response Message (Frame 1904):

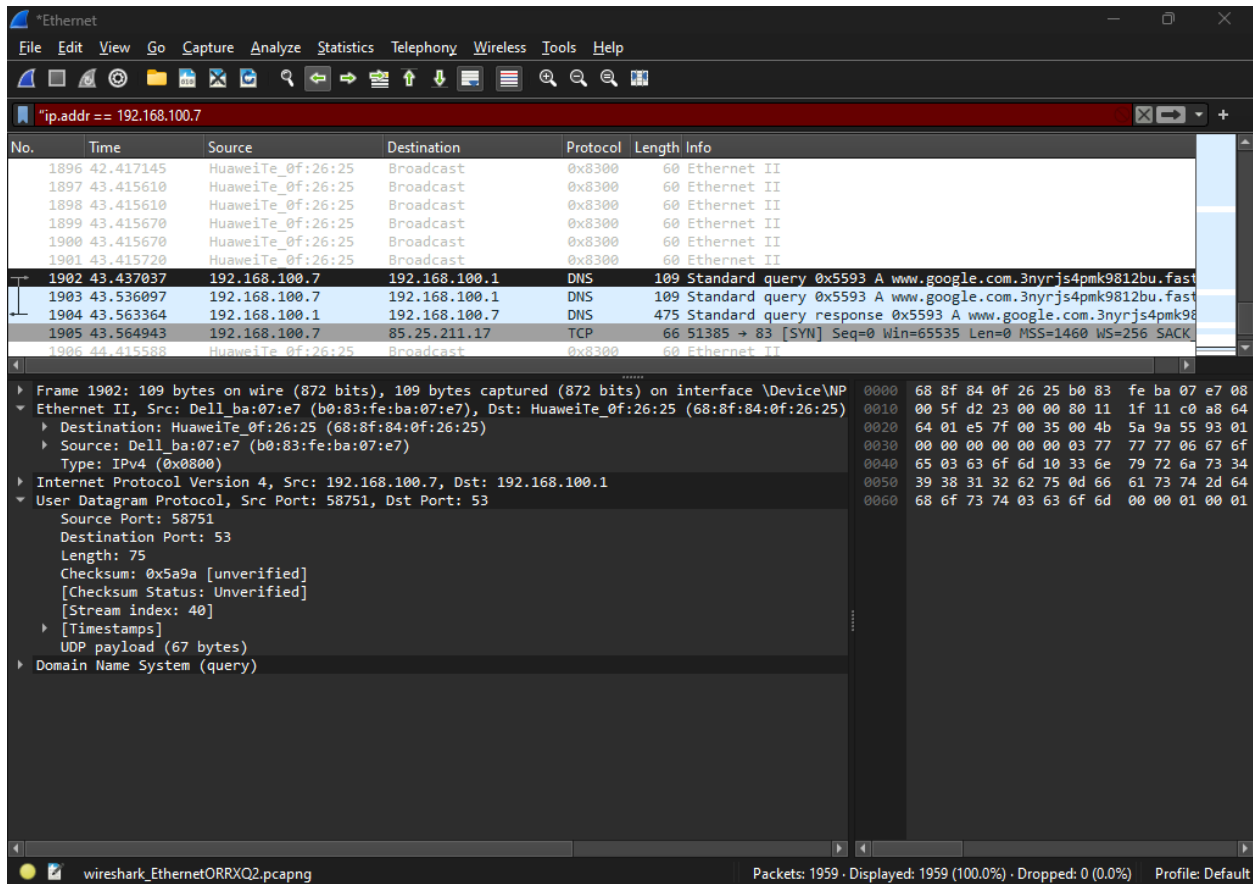
Source Port: 53 (standard port for DNS responses)

Destination Port: 58751

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?

Answer:

From the DNS Query Message (Frame 1902):



Destination IP Address: 192.168.100.1

From ipconfig output:

```
C:\Windows\System32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::392b:2c8:a413:a6d5%3
    IPv4 Address. . . . . : 192.168.100.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%3
                               192.168.100.1
```

Local DNS Server IP Address: Typically, the DNS server IP address can be the same as the default gateway, which is 192.168.100.1 in this case.

Since both the destination IP address of the DNS query and the local DNS server IP address are 192.168.100.1, these two IP addresses are the same.

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

Answer:

DNS Query Type:

The DNS query message is a Standard query.

Does the query message contain any “answers”?:

No, the query message does not contain any answers. It is a request for the IP address corresponding to www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com.

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

Answer:

DNS Response Message:

Number of Answers Provided: 3

Content of Each Answer:

Answer 1:

- **Name:** www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com
- **Type:** CNAME (Canonical Name)
- **Class:** IN (Internet)
- **CNAME:** cdn.fast-dns-host.com

Answer 2:

- **Name:** cdn.fast-dns-host.com
- **Type:** A (Address)
- **Class:** IN (Internet)
- **Address:** 85.25.211.17

Answer 3:

- **Name:** cdn.fast-dns-host.com
- **Type:** A (Address)
- **Class:** IN (Internet)
- **Address:** 85.25.211.177

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?

Answer:

From the DNS Response Message (Frame 1904):

The image shows a Wireshark network traffic capture. The top pane displays a list of network packets. Frame 1904 is highlighted, showing a DNS Standard query response from 192.168.100.1 to 192.168.100.7. The bottom pane shows the detailed view of this frame, which is a Domain Name System (response) packet. The transaction ID is 0x5593. The flags are 0x8180, indicating a standard query response with no error. The packet contains one question and three answer records (RRs). The answers are: 1. www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com: type CNAME, class IN, cname cdn.fast-dns-host.com. 2. cdn.fast-dns-host.com: type A, class IN, addr 85.25.211.17. The right pane shows the raw packet bytes in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1896	42.417145	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1897	43.415610	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1898	43.415610	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1899	43.415670	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1900	43.415670	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1901	43.415720	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1902	43.437037	192.168.100.7	192.168.100.1	DNS	109	Standard query 0x5593 A www.google.com.3nyrjs4pmk9812bu.fast
1903	43.536097	192.168.100.7	192.168.100.1	DNS	109	Standard query 0x5593 A www.google.com.3nyrjs4pmk9812bu.fast
1904	43.563364	192.168.100.1	192.168.100.7	DNS	475	Standard query response 0x5593 A www.google.com.3nyrjs4pmk98
1905	43.564943	192.168.100.7	85.25.211.17	TCP	66	51385 → 83 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK
1906	44.415588	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II

Frame 1904: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface \Device...
Ethernet II, Src: HuaweiTe_0f:26:25 (68:8f:84:0f:26:25), Dst: Dell_ba:07:e7 (b0:83:fe:ba:07:e7)
Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.7
User Datagram Protocol, Src Port: 53, Dst Port: 58751
Source Port: 53
Destination Port: 58751
Length: 441
Checksum: 0xd6ff [unverified]
[Checksum Status: Unverified]
[Stream index: 40]
[Timestamps]
[Time since first frame: 0.126327000 seconds]
[Time since previous frame: 0.027267000 seconds]
UDP payload (433 bytes)
Domain Name System (response)
Transaction ID: 0x5593
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 2
Additional RRs: 12
Queries
Answers
www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com: type CNAME, class IN, cname cdn.fast-dns-host.com.
cdn.fast-dns-host.com: type A, class IN, addr 85.25.211.17

Answer 1: cdn.fast-dns-host.com -> 85.25.211.17

Answer 2: cdn.fast-dns-host.com -> 85.25.211.177

From the TCP SYN Packet (Frame 1905):

The image shows a Wireshark network traffic capture window. The top pane displays a list of captured packets. Packet 1902 is highlighted, showing a DNS Standard query for www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com. Packet 1904 is also highlighted, showing a DNS Standard query response with IP addresses 192.168.100.1 and 85.25.211.17. Packet 1905 is highlighted, showing a TCP SYN packet from source 192.168.100.7 to destination 85.25.211.17 on port 83. The bottom pane shows the detailed view of the selected TCP SYN packet, including the Transmission Control Protocol header and the Flags field set to SYN.

No.	Time	Source	Destination	Protocol	Length	Info
1899	43.415670	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1900	43.415670	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1901	43.415720	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
1902	43.437037	192.168.100.7	192.168.100.1	DNS	109	Standard query 0x5593 A www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com
1903	43.536097	192.168.100.7	192.168.100.1	DNS	109	Standard query 0x5593 A www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com
1904	43.563364	192.168.100.1	192.168.100.7	DNS	475	Standard query response 0x5593 A www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com
1905	43.564943	192.168.100.7	85.25.211.17	TCP	66	51385 → 83 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK

Destination IP Address: 85.25.211.17

The destination IP address of the TCP SYN packet (85.25.211.17) corresponds to one of the IP addresses provided in the DNS response message (85.25.211.17).

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

Answer:

Frame 1902 shows the initial DNS query for www.google.com.3nyrjs4pmk9812bu.fast-dns-host.com.

Frame 1904 shows the DNS response with IP addresses for cdn.fast-dns-host.com.

There are no additional DNS query packets, it indicates that the images are likely hosted on the same domain or subdomain, and no new DNS queries are needed.

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

Answer:

DNS Response Message (From Frame 4220):

Source Port: 53 (standard port for DNS responses)

Destination Port: 56784 (the same port used by the DNS query)

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

Answer:

Destination IP Address: 192.168.100.1

Local DNS Server IP Address (inferred from previous ipconfig output):

Default Local DNS Server IP Address: 192.168.100.1

Since both IP addresses match, the query is sent to the default local DNS server.

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

Answer:

Type of DNS Query: AAAA (requesting an IPv6 address)

Contains Any Answers: No, DNS query messages do not contain answers; they request information.

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

Answer:

DNS Response Message (From Frame 4220):

Number of Answers Provided: 4

Details of Each Answer:

Answer 1:

- **Name:** www.mit.edu
- **Type:** CNAME
- **Class:** IN
- **CNAME:** www.mit.edu.edgekey.net

Answer 2:

- **Name:** www.mit.edu.edgekey.net
- **Type:** CNAME
- **Class:** IN
- **CNAME:** e9566.dscb.akamaiedge.net

Answer 3:

- **Name:** e9566.dscb.akamaiedge.net

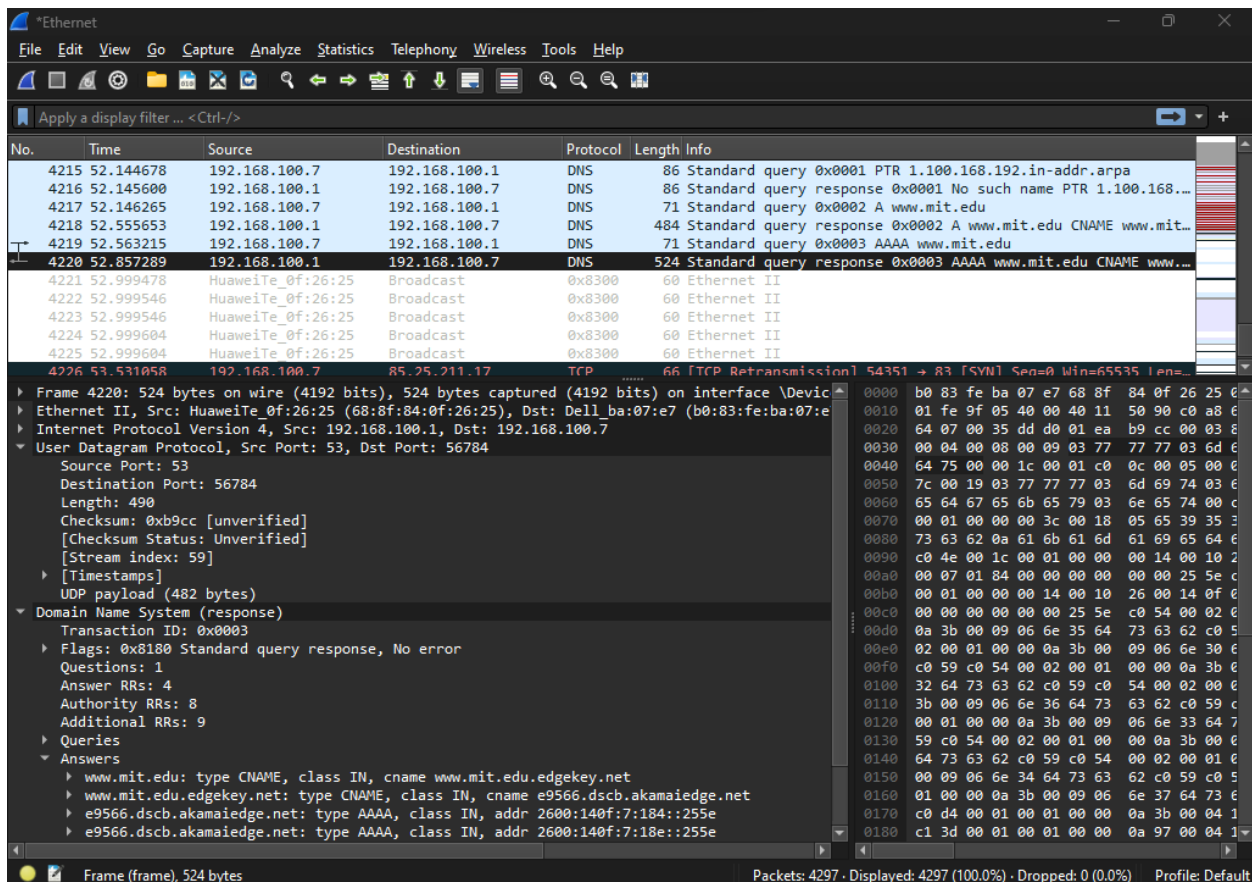
- **Type:** AAAA
- **Class:** IN
- **Address:** 2600:140f:7:184::255e

Answer 4:

- **Name:** e9566.dscb.akamaiedge.net
- **Type:** AAAA
- **Class:** IN
- **Address:** 2600:140f:7:18e::255e

15. Provide a screenshot.

Answer:



```
Microsoft Windows [Version 10.0.22631.3880]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\Adnan>nslookup www.mit.edu
Server: UnKnown
Address: 192.168.100.1
```

```
Non-authoritative answer:
Name: e9566.dscb.akamaiedge.net
Addresses: 2600:140f:7:184::255e
           2600:140f:7:18e::255e
           104.91.11.174
Aliases: www.mit.edu
          www.mit.edu.edgekey.net
```

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

Answer:

Destination IP Address: 192.168.100.1

Local DNS Server IP Address (inferred from previous ipconfig output):

Default Local DNS Server IP Address: 192.168.100.1

Since both IP addresses match, the query is sent to the default local DNS server.

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

Answer:

Type of DNS Query: HTTPS (requesting a secure website address)

Contains Any Answers: No, DNS query messages do not contain answers; they request information.

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

Answer:

DNS Response Message (From Frame 153):

MIT Nameservers:

use2.akam.net

ns1-173.akam.net

ns1-37.akam.net

eur5.akam.net

eur2.akam.net

asia2.akam.net

asia1.akam.net

use5.akam.net

Does the response provide the IP addresses of the MIT nameservers?

Yes, the response provides the IP addresses for these nameservers, as seen in the provided nslookup command output.

19. Provide a screenshot.

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets, with packet 153 selected. The packet list pane shows the following details for packet 153:

No.	Time	Source	Destination	Protocol	Length	Info
149	24.041124	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
150	24.697947	192.168.100.7	192.168.100.1	DNS	72	Standard query 0xa0d2 A www.bing.com
151	24.698315	192.168.100.7	192.168.100.1	DNS	72	Standard query 0xa3e2 HTTPS www.bing.com
152	24.710482	192.168.100.1	192.168.100.7	DNS	553	Standard query response 0xa0d2 A www.bing.com CNAME ww-w...
153	24.710743	192.168.100.1	192.168.100.7	DNS	254	Standard query response 0xa3e2 HTTPS www.bing.com CNAME ww...
154	24.714396	192.168.100.7	23.32.29.96	QUIC	1292	Initial, DCID=3979d15787358bec, PKN: 1, CRYPTO
155	24.714528	192.168.100.7	23.32.29.96	QUIC	1292	Initial, DCID=3979d15787358bec, PKN: 2, PING, PADDING, PIN...
156	24.812493	23.32.29.96	192.168.100.7	QUIC	1292	Initial, SCID=3a424f2756c1360b, PKN: 1, ACK, PADDING
157	24.812636	23.32.29.96	192.168.100.7	QUIC	1292	Initial, SCID=3a424f2756c1360b, PKN: 2, CRYPTO, PADDING
158	24.812636	23.32.29.96	192.168.100.7	QUIC	294	Handshake, SCID=3a424f2756c1360b
159	24.814470	192.168.100.7	23.32.29.96	QUIC	1292	Handshake, DCID=3a424f2756c1360b
160	24.910102	23.32.29.96	192.168.100.7	QUIC	329	Protected Payload (KPB)

The packet details pane for packet 153 shows the following structure:

- Frame 153: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF... Ethernet II, Src: HuaweiTe_0f:26:25 (68:8f:84:0f:26:25), Dst: Dell_ba:07:e7 (b0:83:fe:ba:07:e7)
- Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.7
- User Datagram Protocol, Src Port: 53, Dst Port: 51341
 - Source Port: 53
 - Destination Port: 51341
 - Length: 220
 - Checksum: 0x19d0 [unverified] [Checksum Status: Unverified]
 - [Stream index: 5]
 - [Timestamps] [Time since first frame: 0.012428000 seconds] [Time since previous frame: 0.012428000 seconds]
 - UDP payload (212 bytes)
 - Domain Name System (response)
 - Transaction ID: 0xa3e2
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 1
 - Additional RRs: 0
 - Queries
 - Answers
 - Authoritative nameservers
 - dscx.akamaiedge.net: type SOA, class IN, mname n0dscx.akamaiedge.net

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3880]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup -type=NS mit.edu
Server: UnKnown
Address: 192.168.100.1

Non-authoritative answer:
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use5.akam.net

ns1-173.akam.net      internet address = 193.108.91.173
ns1-37.akam.net     internet address = 193.108.91.37
usw2.akam.net       internet address = 184.26.161.64
asia1.akam.net      internet address = 95.100.175.64
eur5.akam.net        internet address = 23.74.25.64
asia2.akam.net      internet address = 95.101.36.64
use2.akam.net        internet address = 96.7.49.64
use5.akam.net        internet address = 2.16.40.64
ns1-173.akam.net    AAAA IPv6 address = 2600:1401:2::ad
ns1-37.akam.net     AAAA IPv6 address = 2600:1401:2::25
use5.akam.net        AAAA IPv6 address = 2600:1403:a::40

```

20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Answer:

The DNS query message is sent to the IP address 18.0.72.3.

This is not the IP address of your default local DNS server. The default local DNS server, as per your `ipconfig /all` output, is 192.168.100.1.

The IP address 18.0.72.3 likely corresponds to an external DNS server, potentially a DNS server that belongs to the queried domain or another external DNS server configured for this query.

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

Answer:

The “Type” of DNS query is AAAA, which requests the IPv6 address of the domain.

The query message does not contain any "answers". It is just a query, and the answers would be provided in the DNS response message.

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

Answer:

First Answer:

Name: www.aiit.or.kr

Type: AAAA (IPv6 Address)

Class: IN (Internet)

Time to live: 3600 seconds

Data length: 16 bytes

Address: 2001:0db8::1

Second Answer:

Name: www.aiit.or.kr

Type: AAAA (IPv6 Address)

Class: IN (Internet)

Time to live: 3600 seconds

Data length: 16 bytes

Address: 2001:0db8::2

23. Provide a screenshot.

Answer:

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
89	9.000191	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
90	9.000191	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
91	10.000116	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
92	10.000116	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
93	10.000175	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
94	10.000175	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
95	10.000225	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
96	10.345576	192.168.100.7	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
97	10.999913	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
98	10.999913	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
99	10.999980	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II
100	10.999980	HuaweiTe_0f:26:25	Broadcast	0x8300	60	Ethernet II

▼ Frame 96: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_...
 Section number: 1
 ▼ Interface id: 0 (\Device\NPF_{160447AC-AEFE-4D01-966A-6931921C8963})
 Interface name: \Device\NPF_{160447AC-AEFE-4D01-966A-6931921C8963}
 Interface description: Ethernet
 Encapsulation type: Ethernet (1)
 Arrival Time: Jul 17, 2024 04:23:41.894610000 Pakistan Standard Time
 UTC Arrival Time: Jul 16, 2024 23:23:41.894610000 UTC
 Epoch Arrival Time: 1721172221.894610000
 [Time shift for this packet: 0.000000000 seconds]
 [Time delta from previous captured frame: 0.345351000 seconds]
 [Time delta from previous displayed frame: 0.345351000 seconds]
 [Time since reference or first frame: 10.345576000 seconds]
 Frame Number: 96
 Frame Length: 74 bytes (592 bits)
 Capture Length: 74 bytes (592 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:udp:dns]
 [Coloring Rule Name: UDP]
 [Coloring Rule String: udp]
 ▼ Ethernet II, Src: Dell_ba:07:e7 (b0:83:fe:ba:07:e7), Dst: HuaweiTe_0f:26:25 (68:8f:84:0f:26:25)
 ▼ Destination: HuaweiTe_0f:26:25 (68:8f:84:0f:26:25)
 Address: HuaweiTe_0f:26:25 (68:8f:84:0f:26:25)
0. = LG bit: Globally unique address (factory default)

```

0000 68 8f 84 0f 26 25 b0 83 fe ba 07 e7 08
0010 00 3c fa b8 00 00 80 11 c1 45 c0 a8 64
0020 48 03 ca 6b 00 35 00 28 74 8e 00 05 01
0030 00 00 00 00 00 00 03 77 77 04 61 69
0040 6f 72 02 6b 72 00 00 1c 00 01

```

Frame (frame), 74 bytes Packets: 204 · Displayed: 204 (100.0%) · Dropped: 0 (0.0%) Profile: Default

```

C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3880]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

```