

Computer Networks 1

Lab 2b

Wireshark Lab: DNS v8.0

Student Name: Nguyễn Quý Hải

Student No.: 2052974

1. nslookup

- Q1: Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

Answer: nslookup mybk.hcmut.edu.vn

```
C:\Users\dell>nslookup mybk.hcmut.edu.vn
Server:  cachingdns2.vnpt.vn
Address: 123.26.26.26

Non-authoritative answer:
Name:    mybk.hcmut.edu.vn
Address: 221.133.13.124
```

- Q2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

Answer:

```
C:\Windows\system32>nslookup www.ox.ac.uk
Server:  cachingdns2.vnpt.vn
Address: 123.26.26.26

Non-authoritative answer:
Name:    www.ox.ac.uk
Addresses: 151.101.130.216
           151.101.194.216
           151.101.66.216
           151.101.2.216
```

- Q3. 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:

```
C:\Windows\system32>nslookup www.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 2406:2000:9c:800::12

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
```

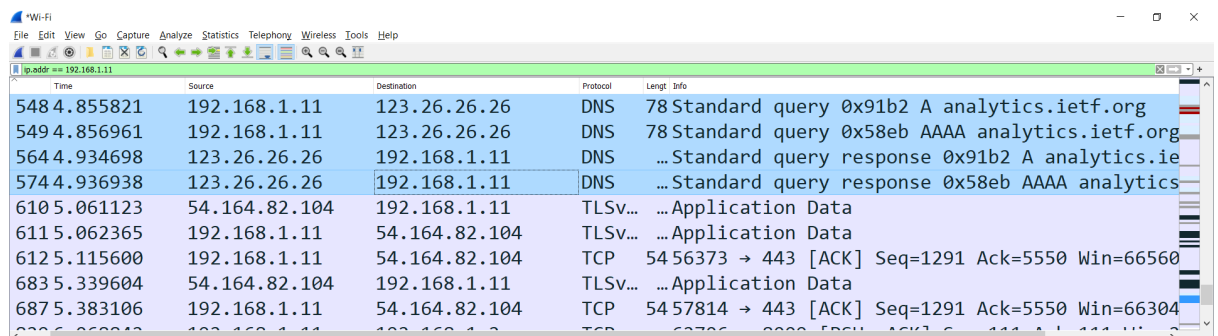
2. ipconfig

Do the command as instruction in the pdf

3. Tracing DNS with Wireshark

- Q4: Locate the DNS query and response messages. Are they sent over UDP or TCP?

Answer: They are all sent over UDP



Time	Source	Destination	Protocol	Length	Info
548.4.855821	192.168.1.11	123.26.26.26	DNS	78	Standard query 0x91b2 A analytics.ietf.org
549.4.856961	192.168.1.11	123.26.26.26	DNS	78	Standard query 0x58eb AAAA analytics.ietf.org
564.4.934698	123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x91b2 A analytics.ietf.org
574.4.936938	123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x58eb AAAA analytics.ietf.org
610.5.061123	54.164.82.104	192.168.1.11	TLSv1	...	Application Data
611.5.062365	192.168.1.11	54.164.82.104	TLSv1	...	Application Data
612.5.115600	192.168.1.11	54.164.82.104	TCP	54	56373 → 443 [ACK] Seq=1291 Ack=5550 Win=66560
683.5.339604	54.164.82.104	192.168.1.11	TLSv1	...	Application Data
687.5.383106	192.168.1.11	54.164.82.104	TCP	54	57814 → 443 [ACK] Seq=1291 Ack=5550 Win=66304

- Q5. What is the destination port for the DNS query message? What is the source port of DNS response messages?

Answer: Source port: 53152, Destination port: 53

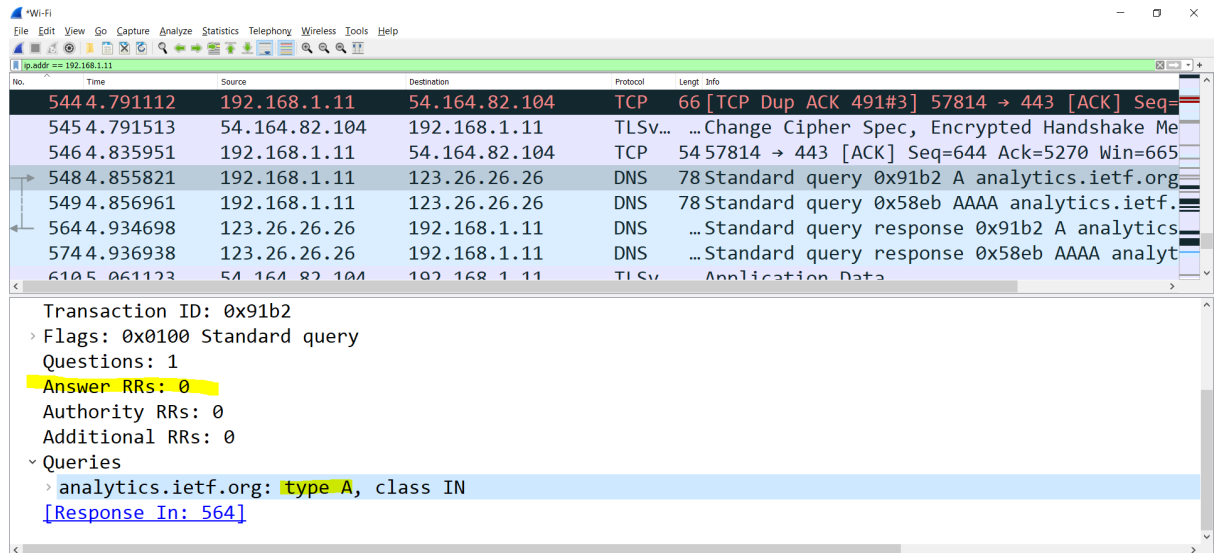
```
> Frame 548: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{A90544A8-4}
> Ethernet II, Src: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b), Dst: Vnptech_a4:6a:08 (a0:65:18:a4:6a:08)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 123.26.26.26
> User Datagram Protocol, Src Port: 53152, Dst Port: 53
> Domain Name System (query)
```

- Q6. 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: DNS query message sent to 192.168.1.11 and it is the same as my local DNS server.

- Q7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: Type A and it does not contain any answers.

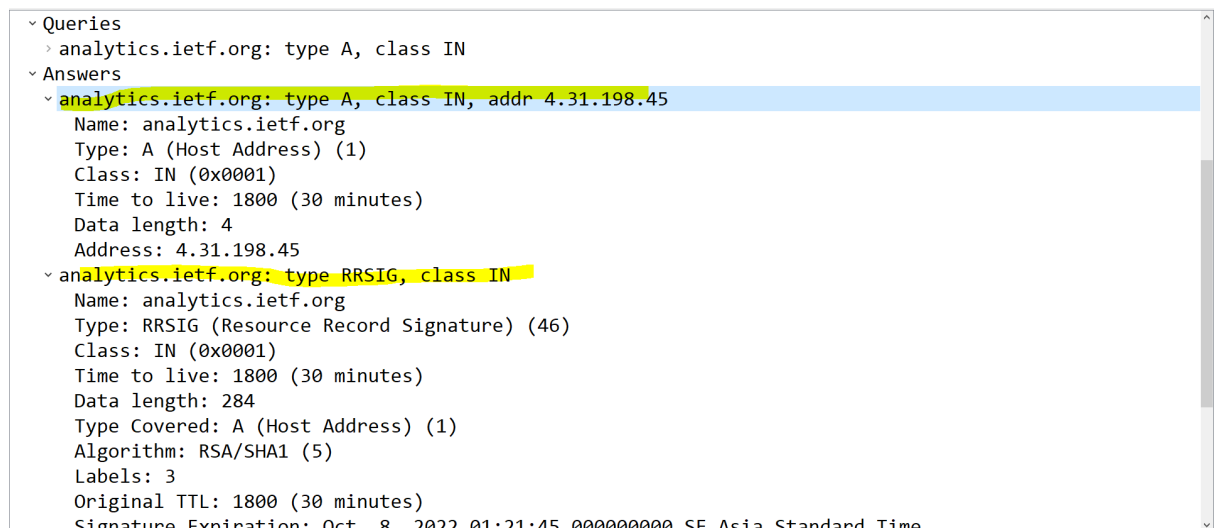


Transaction ID: 0x91b2
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 > analytics.ietf.org: type A, class IN
 [Response In: 564]

- Q8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer: 2 answers.

- +First answer contains address
- +Second answer contains algorithm, signature



Queries
 > analytics.ietf.org: type A, class IN
 Answers
 > analytics.ietf.org: type A, class IN, addr 4.31.198.45
 Name: analytics.ietf.org
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 1800 (30 minutes)
 Data length: 4
 Address: 4.31.198.45
 > analytics.ietf.org: type RRSIG, class IN
 Name: analytics.ietf.org
 Type: RRSIG (Resource Record Signature) (46)
 Class: IN (0x0001)
 Time to live: 1800 (30 minutes)
 Data length: 284
 Type Covered: A (Host Address) (1)
 Algorithm: RSA/SHA1 (5)
 Labels: 3
 Original TTL: 1800 (30 minutes)
 Signature Expiration: Oct 8, 2022 01:21:45.000000000 SF Asia Standard Time

- Q9: 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: Destination IP address of packet is 54.164.82.104 and it corresponds to the address of the answer in the figure above

- Q10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Answer: No, we don't need any more DNS queries because images have all already been loaded in ietf.org.

- Q11: What is the destination port for the DNS query message? What is the source port of DNS response messages?

Answer: Source port: 53, Destination port: 54285

151	20.816316	192.168.1.11	192.168.1.11	TCP	...8009 → 53043 [PSH, ACK] Seq=331 Ack=441 Win=255
152	20.869937	192.168.1.11	192.168.1.2	TCP	5453043 → 8009 [ACK] Seq=441 Ack=255 Win=255
153	21.564635	192.168.1.11	123.26.26.26	DNS	85 Standard query 0x0001 PTR 26.26.26.123.in-
154	21.574396	123.26.26.26	192.168.1.11	DNS	...Standard query response 0x0001 PTR 26.26.2
155	21.578921	192.168.1.11	123.26.26.26	DNS	76 Standard query 0x0002 A www.mit.edu.Home
156	21.623908	123.26.26.26	192.168.1.11	DNS	...Standard query response 0x0002 No such nam
157	21.625033	192.168.1.11	123.26.26.26	DNS	76 Standard query 0x0003 AAAA www.mit.edu.Hom
158	21.635962	123.26.26.26	192.168.1.11	DNS	...Standard query response 0x0003 No such nam
159	21.637354	192.168.1.11	123.26.26.26	DNS	71 Standard query 0x0004 A www.mit.edu
160	21.782284	123.26.26.26	192.168.1.11	DNS	...Standard query response 0x0004 A www.mit.e

Frame 154: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{A90544A...}
 Ethernet II, Src: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08), Dst: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
 Internet Protocol Version 4, Src: 123.26.26.26, Dst: 192.168.1.11
 User Datagram Protocol, Src Port: 53, Dst Port: 54285
 Domain Name System (response)
 Transaction ID: 0x0001
 Flags: 0x8180 Standard query response, No error
 Questions: 1

- Q12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer: DNS query message sent to 123.26.26.26. Obviously this is the IP address of my default local DNS server.

153	21.564635	192.168.1.11	123.26.26.26	DNS	85 Standard query 0x0001 PTR 26.26.26.123.in-
154	21.574396	123.26.26.26	192.168.1.11	DNS	...Standard query response 0x0001 PTR 26.26.2
155	21.578921	192.168.1.11	123.26.26.26	DNS	76 Standard query 0x0002 A www.mit.edu.Home
156	21.623908	123.26.26.26	192.168.1.11	DNS	...Standard query response 0x0002 No such nam
157	21.625033	192.168.1.11	123.26.26.26	DNS	76 Standard query 0x0003 AAAA www.mit.edu.Hom
158	21.635962	123.26.26.26	192.168.1.11	DNS	...Standard query response 0x0003 No such nam
159	21.637354	192.168.1.11	123.26.26.26	DNS	71 Standard query 0x0004 A www.mit.edu

```

Administrator: Command Prompt

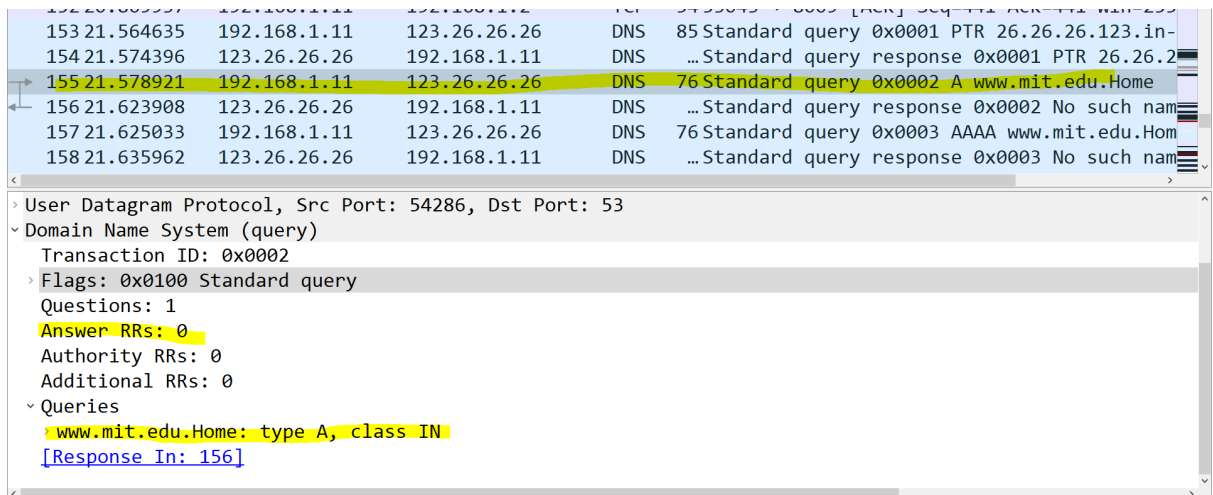
Description . . . . . : Qualcomm QCA9377 802.11ac Wireless Adapter
Physical Address. . . . . : A4-97-B1-E3-90-0B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:ee0:5271:5950:3dfb:5720:63ac:e526(Preferred)
Temporary IPv6 Address. . . . . : 2001:ee0:5271:5950:d1b3:5a8a:e339:103c(Preferred)
Link-local IPv6 Address . . . . . : fe80::3dfb:5720:63ac:e526%16(Preferred)
IPv4 Address. . . . . : 192.168.1.11(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, October 15, 2021 7:54:06 PM
Lease Expires . . . . . : Monday, October 18, 2021 8:03:08 AM
Default Gateway . . . . . : fe80::a265:18ff:fea4:6a08%16
                             192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 178558897
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-9E-19-B6-30-D0-42-2C-3B-1A
DNS Servers . . . . . : 123.26.26.26
                             123.23.23.23
NetBIOS over Tcpi. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

```

- Q13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: Type A with no answers



```

153 21.564635 192.168.1.11 123.26.26.26 DNS 85 Standard query 0x0001 PTR 26.26.26.123.in-
154 21.574396 123.26.26.26 192.168.1.11 DNS ... Standard query response 0x0001 PTR 26.26.2
155 21.578921 192.168.1.11 123.26.26.26 DNS 76 Standard query 0x0002 A www.mit.edu.Home
156 21.623908 123.26.26.26 192.168.1.11 DNS ... Standard query response 0x0002 No such nam
157 21.625033 192.168.1.11 123.26.26.26 DNS 76 Standard query 0x0003 AAAA www.mit.edu.Hom
158 21.635962 123.26.26.26 192.168.1.11 DNS ... Standard query response 0x0003 No such nam

User Datagram Protocol, Src Port: 54286, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.mit.edu.Home: type A, class IN
[Response In: 156]

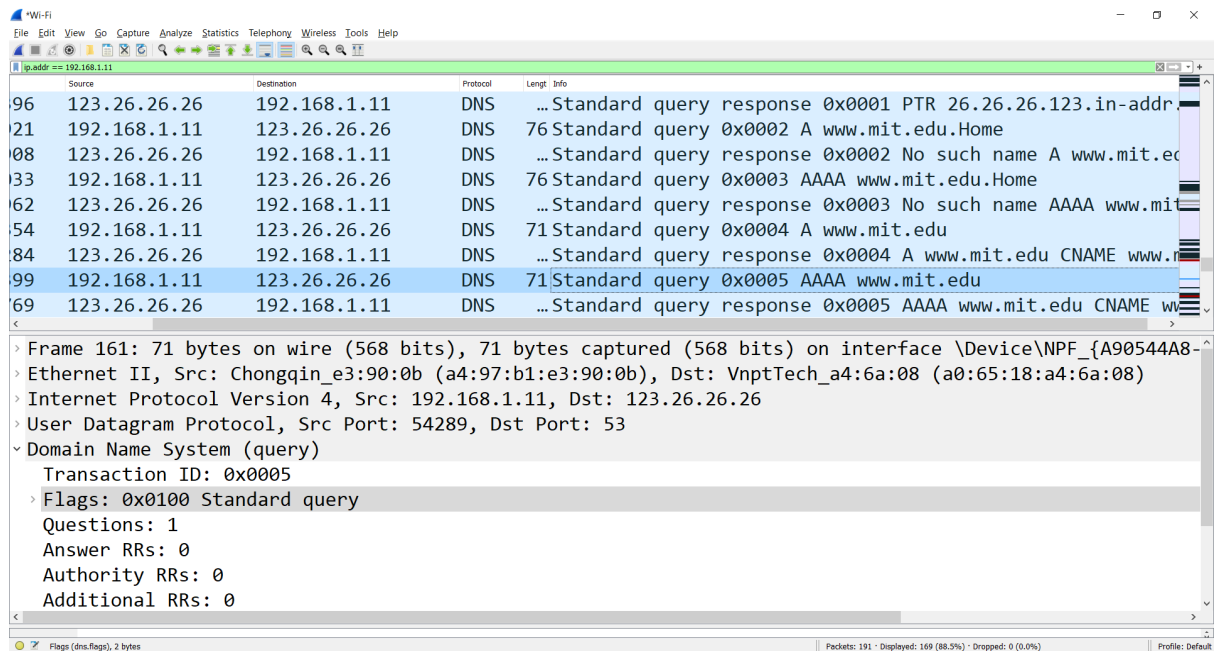
```

- Q14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer: 3 answers. 2 CNAME and 1 address.

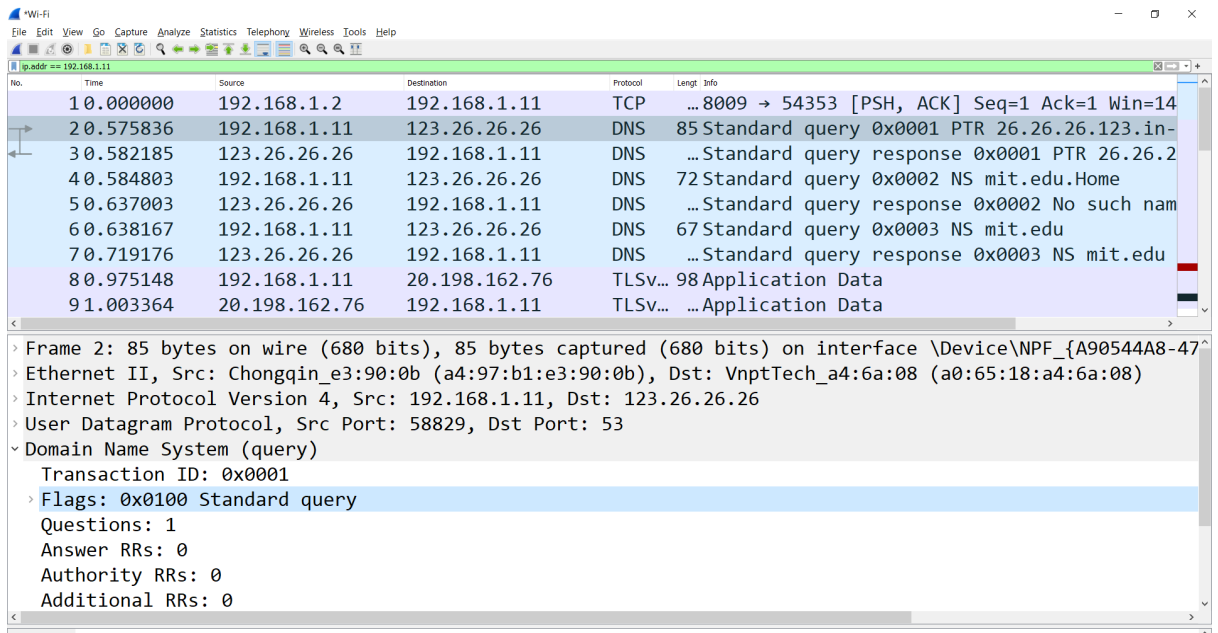
```
Additional RRs: 1
Queries
  > www.mit.edu: type A, class IN
Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    Name: www.mit.edu
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 25
    CNAME: www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    Name: www.mit.edu.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 60 (1 minute)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.7.172.76
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 20 (20 seconds)
```

- Q15. Provide a screenshot.



- Q16: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer: DNS query was sent to 123.26.26.26. This is my default DNS server's IP address.



No.	Time	Source	Destination	Protocol	Length	Info
10.000000		192.168.1.2	192.168.1.11	TCP	...	8009 → 54353 [PSH, ACK] Seq=1 Ack=1 Win=14
20.575836		192.168.1.11	123.26.26.26	DNS	85	Standard query 0x0001 PTR 26.26.26.123.in-
30.582185		123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x0001 PTR 26.26.2
40.584803		192.168.1.11	123.26.26.26	DNS	72	Standard query 0x0002 NS mit.edu.Home
50.637003		123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x0002 No such nam
60.638167		192.168.1.11	123.26.26.26	DNS	67	Standard query 0x0003 NS mit.edu
70.719176		123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x0003 NS mit.edu
80.975148		192.168.1.11	20.198.162.76	TLSv...	98	Application Data
91.003364		20.198.162.76	192.168.1.11	TLSv...	...	Application Data

Frame 2: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{A90544A8-47...}

Ethernet II, Src: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b), Dst: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)

Internet Protocol Version 4, Src: 192.168.1.11, Dst: 123.26.26.26

User Datagram Protocol, Src Port: 58829, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0001

Flags: 0x0100 Standard query

Questions: 1

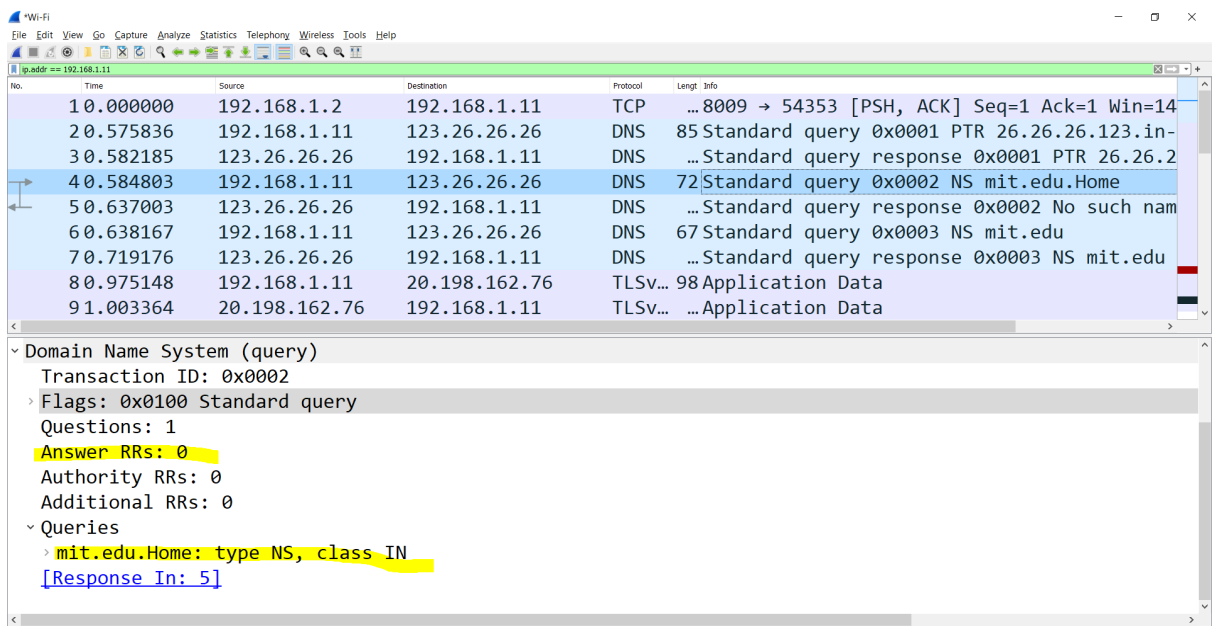
Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

- Q17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: Type NS, no answers.



No.	Time	Source	Destination	Protocol	Length	Info
10.000000		192.168.1.2	192.168.1.11	TCP	...	8009 → 54353 [PSH, ACK] Seq=1 Ack=1 Win=14
20.575836		192.168.1.11	123.26.26.26	DNS	85	Standard query 0x0001 PTR 26.26.26.123.in-
30.582185		123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x0001 PTR 26.26.2
40.584803		192.168.1.11	123.26.26.26	DNS	72	Standard query 0x0002 NS mit.edu.Home
50.637003		123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x0002 No such nam
60.638167		192.168.1.11	123.26.26.26	DNS	67	Standard query 0x0003 NS mit.edu
70.719176		123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x0003 NS mit.edu
80.975148		192.168.1.11	20.198.162.76	TLSv...	98	Application Data
91.003364		20.198.162.76	192.168.1.11	TLSv...	...	Application Data

Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

mit.edu.Home: type NS, class IN

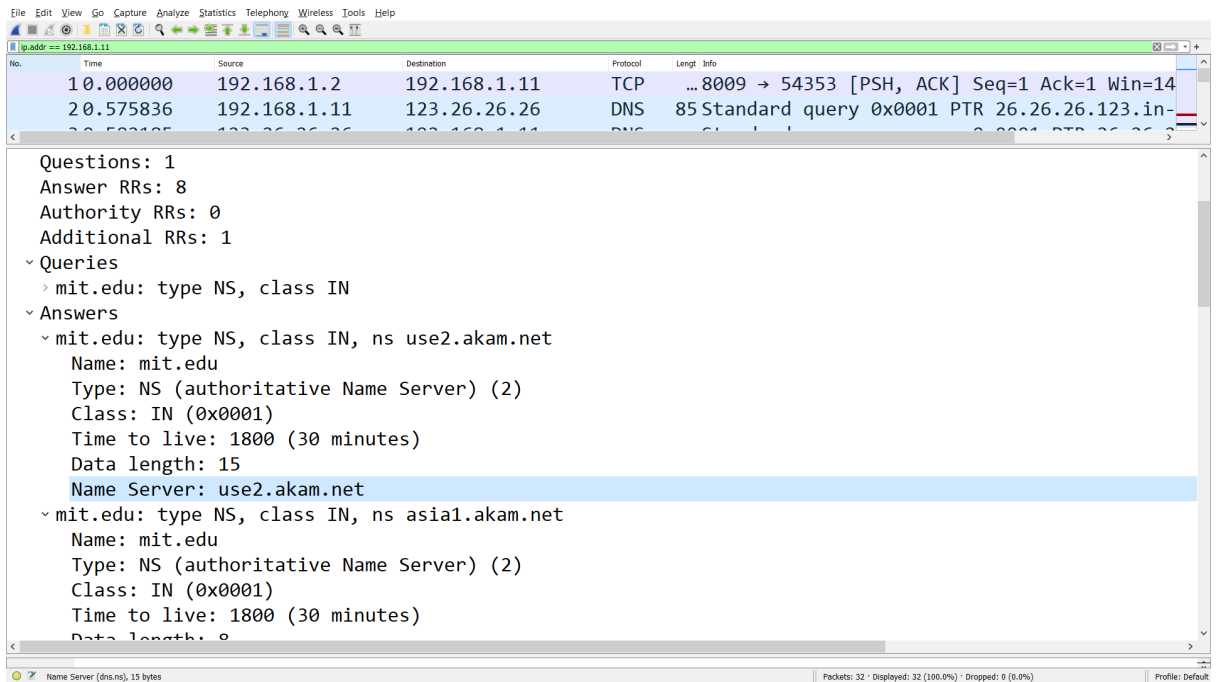
[Response In: 5]

- Q18. 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 namesers?

Answer: Altogether, response message provides 8 nameservers, these are:

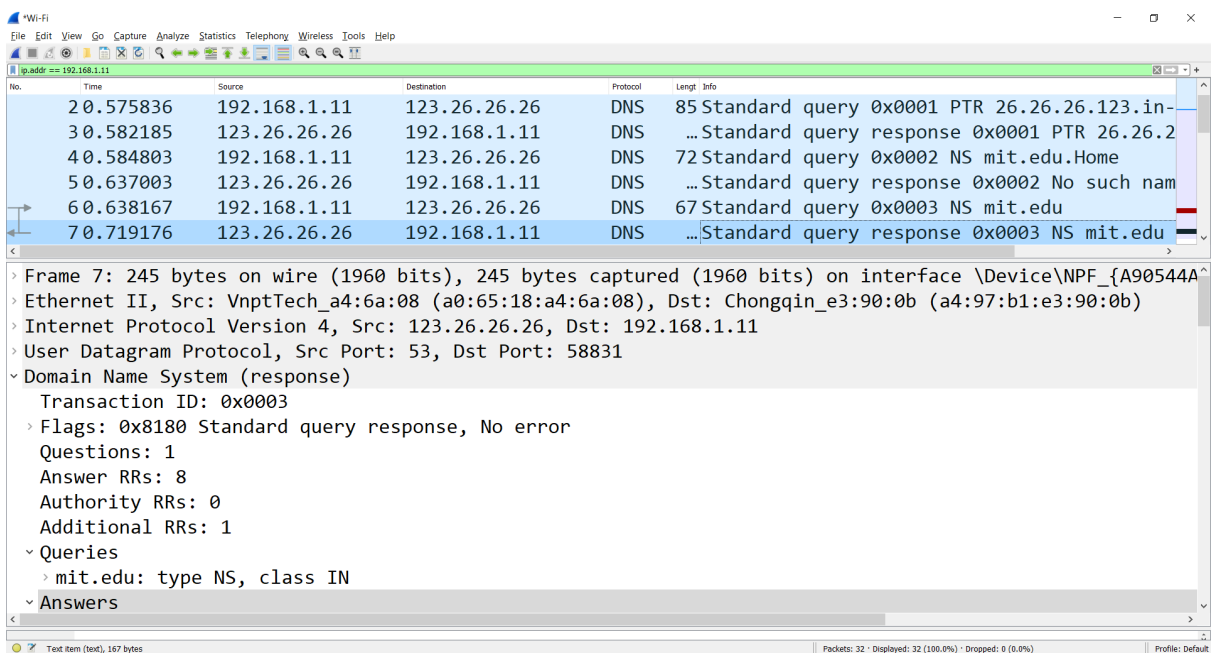
- use2.akam.net
- asia1.akam.net
- usw2.akam.net

- ns1-173.akam.net
- eur5.akam.net
- use5.akam.net
- ns1-37.akam.net
- asia2.akam.net



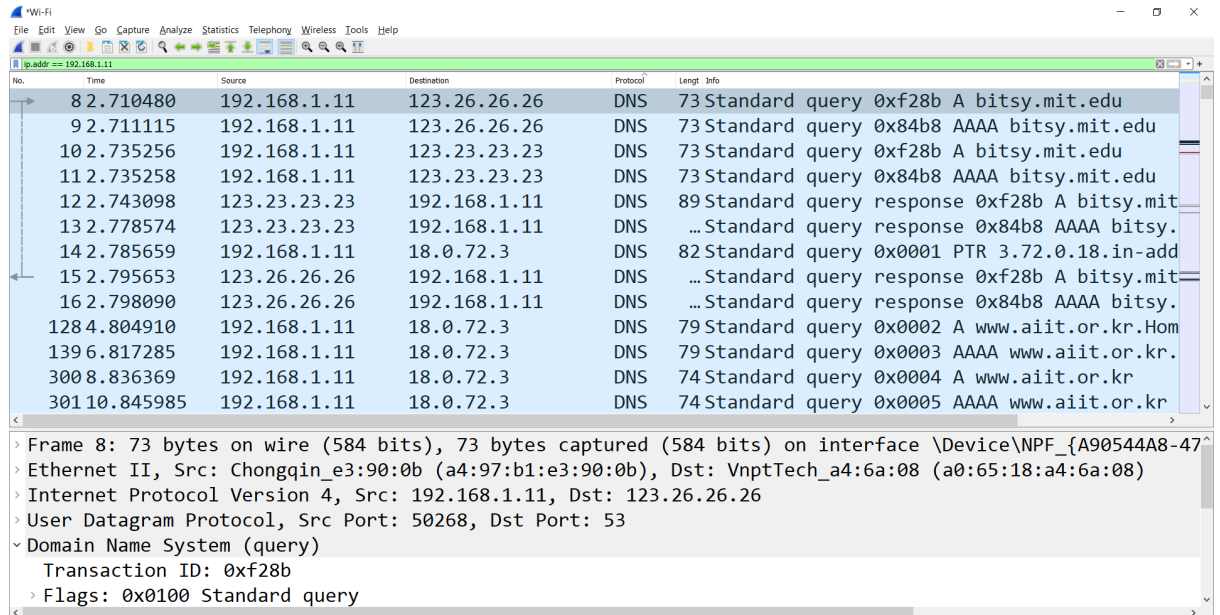
- Q19. Provide a screenshot.

Answer:



- Q20: 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: 123.26.26.26 and once again, it is my default local DNS server's IP addr.



No.	Time	Source	Destination	Protocol	Length	Info
8	2.710480	192.168.1.11	123.26.26.26	DNS	73	Standard query 0xf28b A bitsy.mit.edu
9	2.711115	192.168.1.11	123.26.26.26	DNS	73	Standard query 0x84b8 AAAA bitsy.mit.edu
10	2.735256	192.168.1.11	123.23.23.23	DNS	73	Standard query 0xf28b A bitsy.mit.edu
11	2.735258	192.168.1.11	123.23.23.23	DNS	73	Standard query 0x84b8 AAAA bitsy.mit.edu
12	2.743098	123.23.23.23	192.168.1.11	DNS	89	Standard query response 0xf28b A bitsy.mit.edu
13	2.778574	123.23.23.23	192.168.1.11	DNS	...	Standard query response 0x84b8 AAAA bitsy.mit.edu
14	2.785659	192.168.1.11	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
15	2.795653	123.26.26.26	192.168.1.11	DNS	...	Standard query response 0xf28b A bitsy.mit.edu
16	2.798090	123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x84b8 AAAA bitsy.mit.edu
128	4.804910	192.168.1.11	18.0.72.3	DNS	79	Standard query 0x0002 A www.aiit.or.kr
139	6.817285	192.168.1.11	18.0.72.3	DNS	79	Standard query 0x0003 AAAA www.aiit.or.kr
300	8.836369	192.168.1.11	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
301	10.845985	192.168.1.11	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Frame 8: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{A90544A8-47B...}

Ethernet II, Src: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b), Dst: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)

Internet Protocol Version 4, Src: 192.168.1.11, Dst: 123.26.26.26

User Datagram Protocol, Src Port: 50268, Dst Port: 53

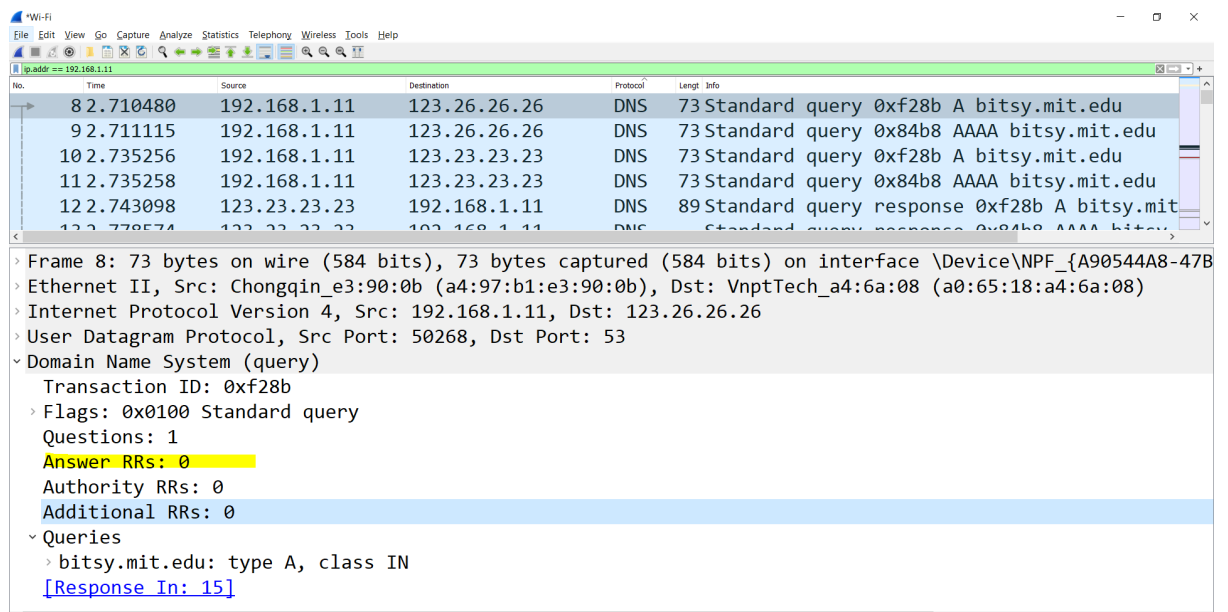
Domain Name System (query)

Transaction ID: 0xf28b

Flags: 0x0100 Standard query

- Q21: Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: Type A. No answers.



No.	Time	Source	Destination	Protocol	Length	Info
8	2.710480	192.168.1.11	123.26.26.26	DNS	73	Standard query 0xf28b A bitsy.mit.edu
9	2.711115	192.168.1.11	123.26.26.26	DNS	73	Standard query 0x84b8 AAAA bitsy.mit.edu
10	2.735256	192.168.1.11	123.23.23.23	DNS	73	Standard query 0xf28b A bitsy.mit.edu
11	2.735258	192.168.1.11	123.23.23.23	DNS	73	Standard query 0x84b8 AAAA bitsy.mit.edu
12	2.743098	123.23.23.23	192.168.1.11	DNS	89	Standard query response 0xf28b A bitsy.mit.edu
13	2.778574	123.23.23.23	192.168.1.11	DNS	...	Standard query response 0x84b8 AAAA bitsy.mit.edu

Frame 8: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{A90544A8-47B...}

Ethernet II, Src: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b), Dst: VnptTech_a4:6a:08 (a0:65:18:a4:6a:08)

Internet Protocol Version 4, Src: 192.168.1.11, Dst: 123.26.26.26

User Datagram Protocol, Src Port: 50268, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xf28b

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

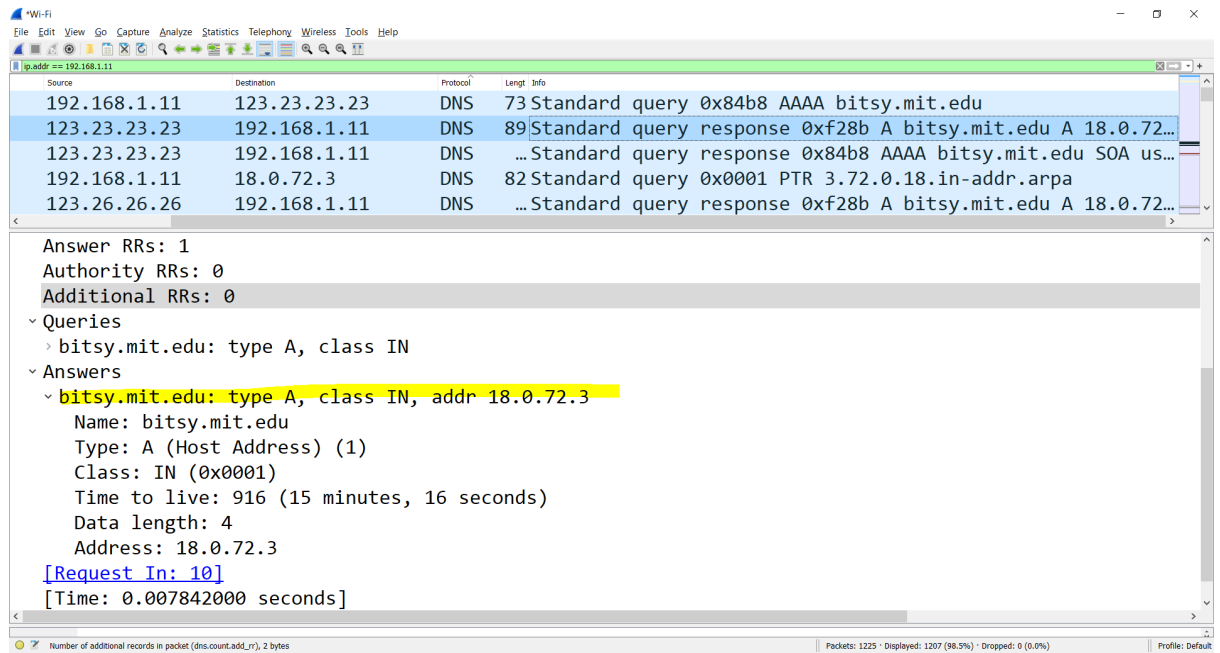
Queries

bitsy.mit.edu: type A, class IN

[Response In: 15]

- Q22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Answer: 1 answer. It contains Address: 18.0.72.3



Wireshark packet capture analysis of DNS traffic. The packet list shows a query from 192.168.1.11 to 123.23.23.23 for bitsy.mit.edu. The packet details pane shows the query response with the IP address 18.0.72.3.

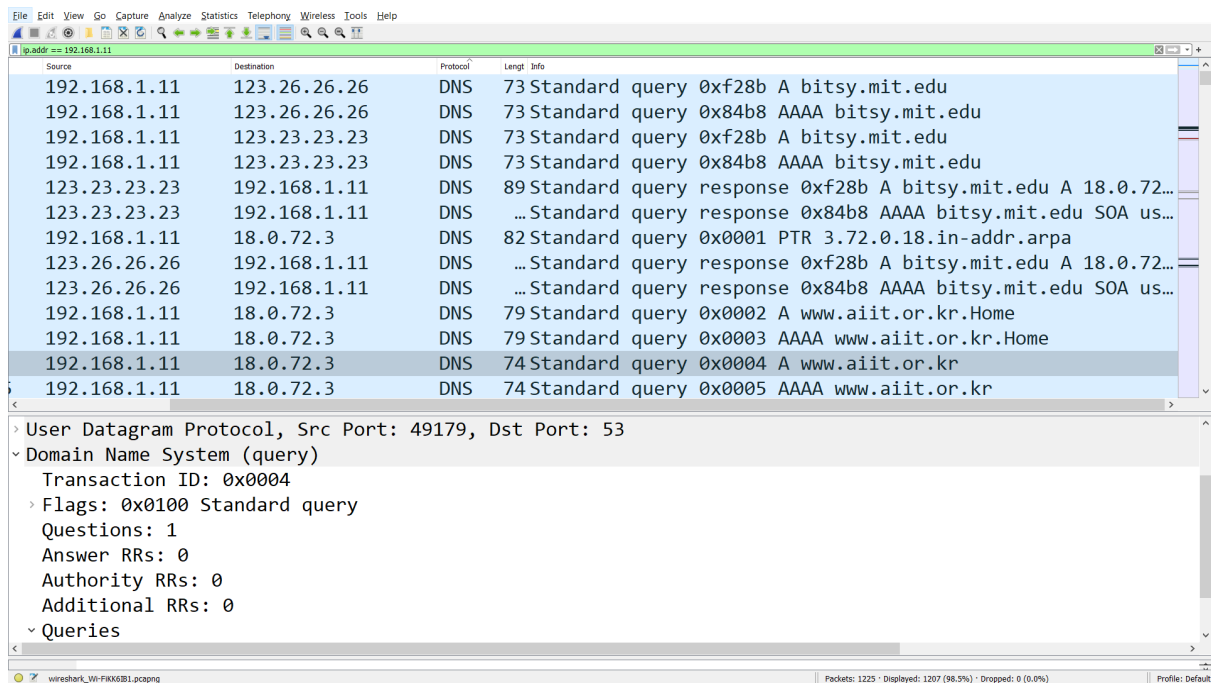
Source	Destination	Protocol	Length	Info
192.168.1.11	123.23.23.23	DNS	73	Standard query 0x84b8 AAAA bitsy.mit.edu
123.23.23.23	192.168.1.11	DNS	89	Standard query response 0xf28b A bitsy.mit.edu A 18.0.72...
123.23.23.23	192.168.1.11	DNS	...	Standard query response 0x84b8 AAAA bitsy.mit.edu SOA us...
192.168.1.11	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
123.26.26.26	192.168.1.11	DNS	...	Standard query response 0xf28b A bitsy.mit.edu A 18.0.72...

Answer RRs: 1
Authority RRs: 0
Additional RRs: 0

Queries
> bitsy.mit.edu: type A, class IN

Answers
> bitsy.mit.edu: type A, class IN, addr 18.0.72.3
Name: bitsy.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 916 (15 minutes, 16 seconds)
Data length: 4
Address: 18.0.72.3
[Request In: 10]
[Time: 0.007842000 seconds]

- Q23. Provide a screenshot.



Wireshark packet capture analysis of DNS traffic. The packet list shows a query from 192.168.1.11 to 123.26.26.26 for bitsy.mit.edu. The packet details pane shows the query response with the IP address 18.0.72.3.

Source	Destination	Protocol	Length	Info
192.168.1.11	123.26.26.26	DNS	73	Standard query 0xf28b A bitsy.mit.edu
192.168.1.11	123.26.26.26	DNS	73	Standard query 0x84b8 AAAA bitsy.mit.edu
192.168.1.11	123.23.23.23	DNS	73	Standard query 0xf28b A bitsy.mit.edu
192.168.1.11	123.23.23.23	DNS	73	Standard query 0x84b8 AAAA bitsy.mit.edu
123.23.23.23	192.168.1.11	DNS	89	Standard query response 0xf28b A bitsy.mit.edu A 18.0.72...
123.23.23.23	192.168.1.11	DNS	...	Standard query response 0x84b8 AAAA bitsy.mit.edu SOA us...
192.168.1.11	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
123.26.26.26	192.168.1.11	DNS	...	Standard query response 0xf28b A bitsy.mit.edu A 18.0.72...
123.26.26.26	192.168.1.11	DNS	...	Standard query response 0x84b8 AAAA bitsy.mit.edu SOA us...
192.168.1.11	18.0.72.3	DNS	79	Standard query 0x0002 A www.aiit.or.kr.Home
192.168.1.11	18.0.72.3	DNS	79	Standard query 0x0003 AAAA www.aiit.or.kr.Home
192.168.1.11	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
192.168.1.11	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

User Datagram Protocol, Src Port: 49179, Dst Port: 53

Domain Name System (query)
Transaction ID: 0x0004
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

Queries