

Project 2

Wireshark Lab: DNS

By
Shreyas Mohan
1001669806

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

ANSWER: They are sent over UDP.

409	19.180940	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2600:1700:11e1:2b70::1	DNS	92 Standard query 0xb814 AAAA www.ietf.org
410	19.230953	2600:1700:11e1:2b70::1	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	DNS	109 Standard query response 0xf1fb A www.ietf.org
411	19.240662	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2600:1700:11e1:2b70::1	DNS	109 Standard query 0x2292 A nav.smartscreen.micr
412	19.241489	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2600:1700:11e1:2b70::1	DNS	109 Standard query 0xf1fb AAAA nav.smartscreen.m
413	19.246642	2600:1700:11e1:2b70::1	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	DNS	244 Standard query response 0x2292 A nav.smartsc
414	19.246643	2600:1700:11e1:2b70::1	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	DNS	291 Standard query response 0xf1fb AAAA nav.smar
415	19.273294	192.168.1.183	23.101.184.153	TCP	66 62474 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=
416	19.291054	23.101.184.153	192.168.1.183	TCP	66 443 → 62474 [SYN, ACK] Seq=0 Ack=1 Win=8192
417	19.291288	192.168.1.183	23.101.184.153	TCP	54 62474 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len
418	19.296192	192.168.1.183	23.101.184.153	TLS...	262 Client Hello
419	19.318240	23.101.184.153	192.168.1.183	TCP	15... [TCP segment of a reassembled PDU]
420	19.318244	23.101.184.153	192.168.1.183	TCP	15... [TCP segment of a reassembled PDU]
421	19.318245	23.101.184.153	192.168.1.183	TCP	15... [TCP segment of a reassembled PDU]
422	19.318246	23.101.184.153	192.168.1.183	TCP	15... [TCP segment of a reassembled PDU]
423	19.318247	23.101.184.153	192.168.1.183	TLS...	13... Server Hello, Certificate, Certificate Statu
424	19.319360	192.168.1.183	23.101.184.153	TCP	54 62474 → 443 [ACK] Seq=209 Ack=1461 Win=26214

Frame 409: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Ethernet II, Src: c0:b6:f9:72:b8:25 (c0:b6:f9:72:b8:25), Dst: 88:96:4e:2b:52:30 (88:96:4e:2b:52:30)
Internet Protocol Version 6, Src: 2600:1700:11e1:2b70:5095:82c2:e7fb:172f, Dst: 2600:1700:11e1:2b70::1
User Datagram Protocol, Src Port: 64304 (64304), Dst Port: 53 (53)
Source Port: 64304
Destination Port: 53
Length: 38
Checksum: 0xc75d [validation disabled]

Screenshot for DNS Query

429	19.340024	2600:1700:11e1:2b70::1	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	DNS	193 Standard query response 0xb814 AAAA www.ietf.org CNAME www.ietf.org.cdn.cl
430	19.345814	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	86 62476 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
431	19.345902	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	86 62475 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1

Frame 429: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface 0
Ethernet II, Src: 30:52:2b:4e:96:88 (30:52:2b:4e:96:88), Dst: c0:b6:f9:72:b8:25 (c0:b6:f9:72:b8:25)
Internet Protocol Version 6, Src: 2600:1700:11e1:2b70::1, Dst: 2600:1700:11e1:2b70:5095:82c2:e7fb:172f
User Datagram Protocol, Src Port: 53 (53), Dst Port: 64304 (64304)
Source Port: 53
Destination Port: 64304

Screenshot for DNS Response

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

ANSWER:

Destination Port of query message:53

Source Port of response message:53

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:

It is sent to **2600:1700:11e1:2b70::1 (destination of query message)**, which is the IP address of one of my local DNS servers. Hence, **both IP addresses are same.**

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : attlocal.net
Description . . . . . : Intel(R) Wireless-AC 9560
Physical Address. . . . . : C0-B6-F9-72-B8-25
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2600:1700:11e1:2b70::a(Preferred)
Lease Obtained. . . . . : Saturday, November 24, 2018 9:20:14 PM
Lease Expires . . . . . : Monday, November 26, 2018 9:43:03 AM
IPv6 Address. . . . . : 2600:1700:11e1:2b70:9d00:84b3:5425:c646(Preferred)
Temporary IPv6 Address. . . . : 2600:1700:11e1:2b70:6c75:ead8:d193:9f20(Preferred)
Link-local IPv6 Address . . . . : fe80::9d00:84b3:5425:c646%6(Preferred)
IPv4 Address. . . . . : 192.168.1.183(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, November 24, 2018 9:20:02 PM
Lease Expires . . . . . : Monday, November 26, 2018 11:09:08 AM
Default Gateway . . . . . : fe80::8a96:4eff:fe2b:5230%6
                               192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 46184185
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-B0-33-F2-54-BF-64-1E-34-5B
DNS Servers . . . . . : 2600:1700:11e1:2b70::1
                       192.168.1.254

```

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

Answer: Type: **AAAA query (IPv6 address)**. The query message **does not contain any answers**.

```

Domain Name System (query)
[Response In: 429]
Transaction ID: 0xb814
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ www.ietf.org: type AAAA, class IN
    Name: www.ietf.org
    [Name Length: 12]
    [Label Count: 3]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)

```

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

Answer: Three answers are provided. The answers contains **name of the host, type of the address, class, the TTL, data length and the IPv6 address**.

```

> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
▼ Queries
  > www.ietf.org: type AAAA, class IN
▼ Answers
  ▼ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1800
    Data length: 33
    CNAME: www.ietf.org.cdn.cloudflare.net
  ▼ www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:55
    Name: www.ietf.org.cdn.cloudflare.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 300
    Data length: 16
    AAAA Address: 2606:4700:10::6814:55
  ▼ www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:155
    Name: www.ietf.org.cdn.cloudflare.net
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
    Time to live: 300
    Data length: 16
    AAAA Address: 2606:4700:10::6814:155

```

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: The destination IP address of the SYN packet is sent to **2606:4700:10::6814:55**, which **corresponds to the second IP address** in the DNS response message.

429 19.3480924	2600:1700:11e1:2b70::1	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	DNS	193 Standard query response 0xb814 AAAA www.ietf.org CNAME www.ietf.org.cdn.c
430 19.345814	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	86 62476 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
431 19.345902	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	86 62475 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
432 19.347515	192.168.1.183	23.101.184.153	TLS	147 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
433 19.351278	2606:4700:10::6814:55	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	TCP	86 80 → 62476 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1 WS
434 19.351426	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	74 62476 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
435 19.351653	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	HTTP	438 GET / HTTP/1.1
436 19.354973	2606:4700:10::6814:55	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	TCP	86 80 → 62475 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1 WS
437 19.355110	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	74 62475 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
438 19.357913	2606:4700:10::6814:55	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	TCP	74 80 → 62476 [ACK] Seq=1 Ack=365 Win=28672 Len=0
439 19.362488	2606:4700:10::6814:55	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	TCP	784 [TCP segment of a reassembled PDU]
440 19.362489	2606:4700:10::6814:55	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	HTTP	79 HTTP/1.1 302 Found (text/html)
441 19.362863	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	74 62476 → 80 [ACK] Seq=365 Ack=711 Win=261376 Len=0
442 19.363061	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	74 62476 → 80 [ACK] Seq=365 Ack=716 Win=261376 Len=0
443 19.363651	23.101.184.153	192.168.1.183	TLS	105 Change Cipher Spec, Hello Request, Hello Request
444 19.364289	192.168.1.183	23.101.184.153	TCP	54 62474 → 443 [ACK] Seq=302 Ack=7210 Win=260608 Len=0
445 19.370057	2600:1700:11e1:2b70:5095:82c2:e7fb:172f	2606:4700:10::6814:55	TCP	74 62476 → 80 [FIN, ACK] Seq=365 Ack=716 Win=261376 Len=0

```

Domain Name System (response)
[Request In: 409]
[Time: 0.159084000 seconds]
Transaction ID: 0xb814
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
▼ Queries
  > www.ietf.org: type AAAA, class IN
▼ Answers
  > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  > www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:55
  > www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:155

```

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

ANSWER: No, no new queries are issued.

Nslookup on www.mit.edu

```
C:\Users\Shreyas Mohan>nslookup www.mit.edu
Server: dsldevice6.attlocal.net
Address: 2600:1700:11e1:2b70::1

Non-authoritative answer:
Name: user-att-71-136-128-0.e9566.dscb.akamaiedge.net
Addresses: 2600:1404:e000:2b2::255e
           2600:1404:e000:28d::255e
           23.209.76.236
Aliases: www.mit.edu
          www.mit.edu.edgekey.net
          e9566.dscb.akamaiedge.net
```

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

ANSWER: We are supposed to pay attention to the last query for www.mit.edu according to the lab manual. I have 4 queries, where last 2 are similar. I am paying attention to the third query. **Destination port for DNS query is 53 and Source port for DNS response is 53.**

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

ANSWER:

Type: A standard query (Host address). The query message does not contain any answers.

161	18.569718	2600:1700:11e1...	2600:1700:11e1:2b70::1	DNS	91	Standard query 0x0004 A www.mit.edu
162	18.576731	2600:1700:11e1...	2600:1700:11e1:2b70:f5be:e457:fd05:6ed3	DNS	216	Standard query response 0x0004 A www.i
163	18.579332	2600:1700:11e1...	2600:1700:11e1:2b70::1	DNS	91	Standard query 0x0005 AAAA www.mit.ed
164	18.586086	2600:1700:11e1...	2600:1700:11e1:2b70:f5be:e457:fd05:6ed3	DNS	256	Standard query response 0x0005 AAAA w
165	19.272001	86:96:4e:2b:52...	Broadcast	0x7...	118	Ethernet II
166	19.390540	192.168.1.183	192.168.1.79	TCP	171	[TCP segment of a reassembled PDU]
167	19.390547	192.168.1.183	192.168.1.75	TCP	171	[TCP segment of a reassembled PDU]

[Response In: 162]
Transaction ID: 0x0004
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
✓ Queries
 v www.mit.edu: type A, class IN
 Name: www.mit.edu
 [Name Length: 11]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)

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

Answer: **Four answers** are provided. The answers contains **name of the host, type of the address, class, the TTL, data length and the IP address.**

Answer RRs: 4
Authority RRs: 0
Additional RRs: 0
> Queries
Answers
v 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
Data length: 25
CNAME: www.mit.edu.edgekey.net
v 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
Data length: 24
CNAME: e9566.dscb.akamaiedge.net
v e9566.dscb.akamaiedge.net: type CNAME, class IN, cname user-att-71-136-128-0.e9566.dscb.akamaiedge.net
Name: e9566.dscb.akamaiedge.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1
Data length: 24
CNAME: user-att-71-136-128-0.e9566.dscb.akamaiedge.net
v user-att-71-136-128-0.e9566.dscb.akamaiedge.net: type A, class IN, addr 23.209.76.236
Name: user-att-71-136-128-0.e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 20
Data length: 4
Address: 23.209.76.236

I have already provided it.

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

[illegible]

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

ANSWER: This is a **standard type NS query** and it contains no answers.

58	5.429621	2600:1700:11e1:2b70:3590:77a2:c5c9:fc61	2600:1700:11e1:2b70::1	DNS	87 Standard query 0x0003 NS mit.edu
59	5.436524	2600:1700:11e1:2b70::1	2600:1700:11e1:2b70:3590:77a2:c5c9:fc61	DNS	254 Standard query response 0x0003 NS m...
60	6.154332	86:96:4e:2b:52:33	Broadcast	0x7...	118 Ethernet II
61	7.012141	192.168.1.183	192.168.1.79	TCP	171 64113 → 42382 [PSH, ACK] Seq=118 Acl
62	7.012580	192.168.1.183	192.168.1.79	TCP	171 [TCP segment of a reassembled PDU]
63	7.012895	192.168.1.183	192.168.1.79	TCP	171 64114 → 42654 [PSH, ACK] Seq=118 Acl
64	7.013258	192.168.1.183	192.168.1.75	TCP	171 [TCP segment of a reassembled PDU]
65	7.040585	192.168.1.79	192.168.1.183	TCP	171 42382 → 64113 [PSH, ACK] Seq=118 Acl

[Response In: 59]
Transaction ID: 0x0003
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
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)

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?

ANSWER: The response message **does not contain any nameservers**. If they contained, it would be under additional records right under answers, but there is nothing below answers.

59	5.436524	2600:1700:11e1:2b70::1	2600:1700:11e1:2b70:3590:77a2:c5c9:fc61	DNS	254 Standard query response 0x0003 NS mit.edu NS asia1.akam.net NS ns1-37.akam.net NS ns1-173.akam...
60	6.154332	86:96:4e:2b:52:33	Broadcast	0x7...	118 Ethernet II
61	7.012141	192.168.1.183	192.168.1.79	TCP	171 64113 → 42382 [PSH, ACK] Seq=118 Ack=118 Win=253 Len=117
62	7.012580	192.168.1.183	192.168.1.79	TCP	171 [TCP segment of a reassembled PDU]
63	7.012895	192.168.1.183	192.168.1.79	TCP	171 64114 → 42654 [PSH, ACK] Seq=118 Ack=118 Win=253 Len=117
64	7.013258	192.168.1.183	192.168.1.75	TCP	171 [TCP segment of a reassembled PDU]
65	7.040585	192.168.1.79	192.168.1.183	TCP	171 42382 → 64113 [PSH, ACK] Seq=118 Ack=235 Win=346 Len=117

Answer RRs: 8
Authority RRs: 0
Additional RRs: 0
Queries
 mit.edu: type NS, class IN
Answers
 mit.edu: type NS, class IN, ns asia1.akam.net
 mit.edu: type NS, class IN, ns ns1-37.akam.net
 mit.edu: type NS, class IN, ns ns1-173.akam.net
 mit.edu: type NS, class IN, ns asia2.akam.net
 mit.edu: type NS, class IN, ns usw2.akam.net
 mit.edu: type NS, class IN, ns use2.akam.net
 mit.edu: type NS, class IN, ns eur5.akam.net
 mit.edu: type NS, class IN, ns use5.akam.net

19. Provide a screenshot.

Screenshots provided in the answers of each question.

Now repeat the previous experiment, but instead issue the command:
nslookup www.aiit.or.kr bitsy.mit.edu

```
C:\Users\Shreyas Mohan>nslookup http://www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 18.72.0.3

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

C:\Users\Shreyas Mohan>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 18.72.0.3

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

C:\Users\Shreyas Mohan>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 18.72.0.3

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
```

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 I tried doing the nslookup 3 times and all of them timed out. The query is sent to **192.168.1.254** . Yes, it is same as of default local DNS server.

91	6.869682	192.168.1.183	192.168.1.254	DNS	73	Standard query 0xe65a AAAA bitsy.mit.edu
92	6.875280	192.168.1.254	192.168.1.183	DNS	138	Standard query response 0xe65a AAAA bitsy.mit.edu SOA use2.akam.net
93	6.893298	192.168.1.183	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
94	6.914458	2600:1700:11e1...	2600:1700:11e1...	DNS	158	Standard query response 0xe65a AAAA bitsy.mit.edu SOA use2.akam.net
103	8.891549	192.168.1.183	18.72.0.3	DNS	87	Standard query 0x0002 A www.aiit.or.kr.attlocal.net
117	10.896711	192.168.1.183	18.72.0.3	DNS	87	Standard query 0x0003 AAAA www.aiit.or.kr.attlocal.net
140	12.901359	192.168.1.183	18.72.0.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
146	14.906667	192.168.1.183	18.72.0.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
221	28.443592	2600:1700:11e1...	2600:1700:11e1...	DNS	93	Standard query 0x515a AAAA bitsy.mit.edu
222	28.451720	2600:1700:11e1...	2600:1700:11e1...	DNS	158	Standard query response 0x515a AAAA bitsy.mit.edu SOA use2.akam.net
223	28.471562	192.168.1.183	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
230	30.467737	192.168.1.183	18.72.0.3	DNS	87	Standard query 0x0002 A www.aiit.or.kr.attlocal.net
249	32.472283	192.168.1.183	18.72.0.3	DNS	87	Standard query 0x0003 AAAA www.aiit.or.kr.attlocal.net
261	34.476232	192.168.1.183	18.72.0.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr

Frame 91: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
Ethernet II, Src: c0:b6:f9:72:b8:25 (c0:b6:f9:72:b8:25), Dst: 88:96:4e:2b:52:30 (88:96:4e:2b:52:30)
Internet Protocol Version 4, Src: 192.168.1.183, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 62203 (62203), Dst Port: 53 (53)
Domain Name System (query)
[\[Response In: 92\]](#)

```
DNS Servers . . . . . : 2600:1700:11e1:2b70::1
                      192.168.1.254
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                        attlocal.net
```

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

ANSWER: This is a **IPv6 type AAAA query** and it contains no answers.

[Response In: 92]	
Transaction ID: 0xe65a	
> Flags: 0x0100 Standard query	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
v Queries	
v bitsy.mit.edu: type AAAA, class IN	
Name: bitsy.mit.edu	
[Name Length: 13]	
[Label Count: 3]	
Type: AAAA (IPv6 Address) (28)	

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

ANSWER: The response message does not contain any answers.

```
✓ Domain Name System (response)
  [Request In: 91]
  [Time: 0.005598000 seconds]
  Transaction ID: 0xe65a
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
  ✓ Queries
    ✓ bitsy.mit.edu: type AAAA, class IN
      Name: bitsy.mit.edu
      [Name Length: 13]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
```

23. Provide a screenshot.

Screenshots are provided in the answers of each question