

Name :Izaan Mohtashim

Roll No: P20-0613

Sec : 5A

Computer Networks

Lab Homework 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 of slate 115.186.60.92

```
lycan@Lycan: ~  
lycan@Lycan:~$ www.slate.nu.edu.pk  
www.slate.nu.edu.pk: command not found  
lycan@Lycan:~$ nslookup www.slate.nu.edu.pk  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
www.slate.nu.edu.pk    canonical name = slate.nu.edu.pk.  
Name:   slate.nu.edu.pk  
Address: 115.186.60.92  
  
lycan@Lycan:~$
```

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

ip address of Mit 192.168.18.1

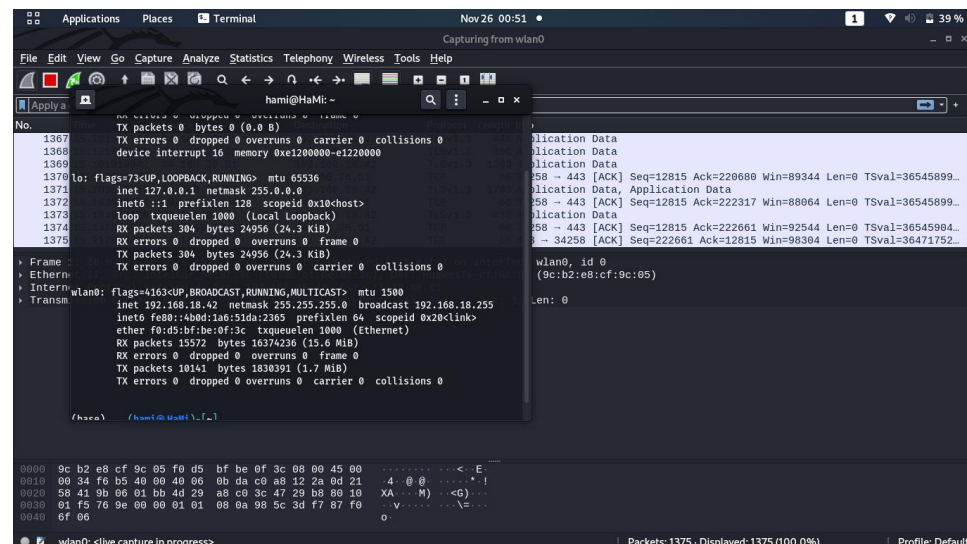
```
lycan@Lycan: ~  
lycan@Lycan:~$ nslookup -type=NS mit.edu  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
mit.edu nameserver = use2.akam.net.  
mit.edu nameserver = asia1.akam.net.  
mit.edu nameserver = eur5.akam.net.  
mit.edu nameserver = usw2.akam.net.  
mit.edu nameserver = asia2.akam.net.  
mit.edu nameserver = ns1-37.akam.net.  
mit.edu nameserver = use5.akam.net.  
mit.edu nameserver = ns1-173.akam.net.  
  
Authoritative answers can be found from:  
usw2.akam.net    internet address = 184.26.161.64  
use5.akam.net    internet address = 2.16.40.64  
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  
ns1-173.akam.net internet address = 193.108.91.173  
asia1.akam.net   internet address = 95.100.175.64  
use5.akam.net    has AAAA address 2600:1403:a::40  
ns1-173.akam.net has AAAA address 2600:1401:2::ad
```

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?

Ip address of yahoo is 87.248.119.252

Tracing DNS with Wireshark

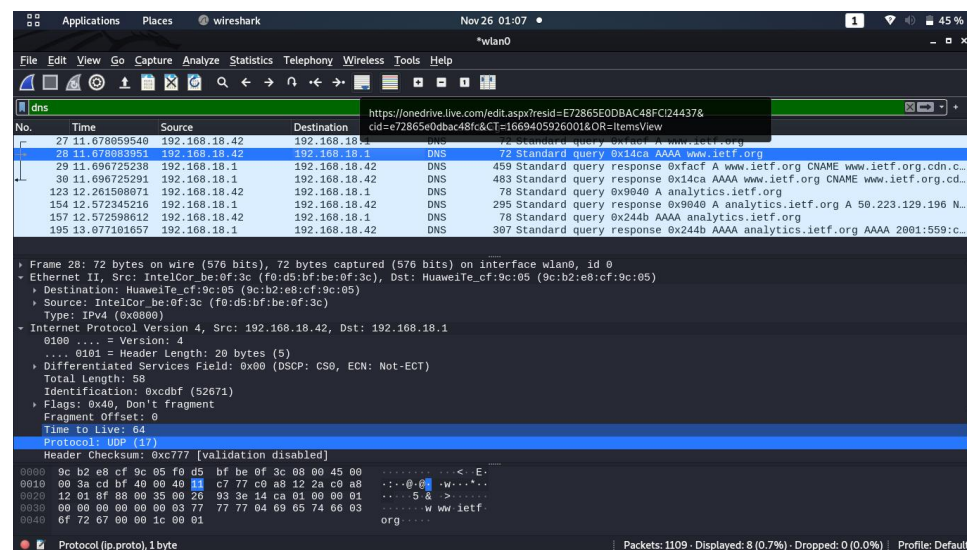
Ip address of my device -> 192.168.18.42



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

The DNS query and response messages are sent over UDP.

Using UDP



Applications Places wireshark Nov 26 01:07 wlan0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
27	11.678059540	192.168.18.42	192.168.18.1	DNS	72	Standard query 0xfacf A www.ietf.org
28	11.678083951	192.168.18.42	192.168.18.1	DNS	72	Standard query 0x14ca AAAA www.ietf.org
29	11.696725238	192.168.18.1	192.168.18.42	DNS	459	Standard query response 0xfacf A www.ietf.org CNAME www.ietf.org.cdn.c.
30	11.696725291	192.168.18.1	192.168.18.42	DNS	483	Standard query response 0x14ca AAAA www.ietf.org CNAME www.ietf.org.cdn.c.
123	12.261508071	192.168.18.42	192.168.18.1	DNS	78	Standard query 0x9040 A analytics.ietf.org
154	12.572345216	192.168.18.1	192.168.18.42	DNS	295	Standard query response 0x9040 A analytics.ietf.org A 50.223.129.196 N.
157	12.572598612	192.168.18.42	192.168.18.1	DNS	78	Standard query 0x244b AAAA analytics.ietf.org
195	13.077101657	192.168.18.1	192.168.18.42	DNS	307	Standard query response 0x244b AAAA analytics.ietf.org AAAA 2001:559:c...

Frame 29: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface wlan0, id 0

Ethernet II, Src: HuaweiTe_cf:9c:05 (9c:b2:e8:cf:9c:05), Dst: IntelCor_be:0f:3c (f0:d5:bf:be:0f:3c)

Destination: IntelCor_be:0f:3c (f0:d5:bf:be:0f:3c)

Source: HuaweiTe_cf:9c:05 (9c:b2:e8:cf:9c:05)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.18.1, Dst: 192.168.18.42

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 445

Identification: 0x5c10 (23568)

Flags: 0x40, Don't fragment

Fragment Offset: 0

Time to Live: 64

Protocol: UDP (17)

Header Checksum: 0x37a4 [validation disabled]

0010 01 bd 5c 10 40 00 40 11 37 a4 c0 a8 12 01 c0 a8 ... \-@-0 7-.....

0020 12 2a 00 35 8f 88 01 a9 bd b7 fa cf 81 00 00 01 ... 5.....

0030 00 03 00 05 00 0a 03 77 77 77 04 69 65 74 66 03w ww.ietf.

0040 6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00 ... org.....

0050 06 53 00 21 03 77 77 77 04 69 65 74 66 03 6f 72 ... S! ww.ietf.or

Protocol (p.proto), 1 byte

Packets: 1109 - Displayed: 8 (0.7%) - Dropped: 0 (0.0%) | Profile: Default

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

Dns query

Port 53

Applications Places wireshark Nov 26 01:09 wlan0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
27	11.678059540	192.168.18.42	192.168.18.1	DNS	72	Standard query 0xfacf A www.ietf.org
28	11.678083951	192.168.18.42	192.168.18.1	DNS	72	Standard query 0x14ca AAAA www.ietf.org
29	11.696725238	192.168.18.1	192.168.18.42	DNS	459	Standard query response 0xfacf A www.ietf.org CNAME www.ietf.org.cdn.c.
30	11.696725291	192.168.18.1	192.168.18.42	DNS	483	Standard query response 0x14ca AAAA www.ietf.org CNAME www.ietf.org.cdn.c.
123	12.261508071	192.168.18.42	192.168.18.1	DNS	78	Standard query 0x9040 A analytics.ietf.org
154	12.572345216	192.168.18.1	192.168.18.42	DNS	295	Standard query response 0x9040 A analytics.ietf.org A 50.223.129.196 N.
157	12.572598612	192.168.18.42	192.168.18.1	DNS	78	Standard query 0x244b AAAA analytics.ietf.org
195	13.077101657	192.168.18.1	192.168.18.42	DNS	307	Standard query response 0x244b AAAA analytics.ietf.org AAAA 2001:559:c...

Frame 28: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface wlan0, id 0

Ethernet II, Src: IntelCor_be:0f:3c (f0:d5:bf:be:0f:3c), Dst: HuaweiTe_cf:9c:05 (9c:b2:e8:cf:9c:05)

Destination: HuaweiTe_cf:9c:05 (9c:b2:e8:cf:9c:05)

Source: IntelCor_be:0f:3c (f0:d5:bf:be:0f:3c)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.18.42, Dst: 192.168.18.1

User Datagram Protocol, Src Port: 36744, Dst Port: 53

Source Port: 36744

Destination Port: 53

Length: 38

Checksum: 0x933e [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

[Timestamps]

UDP payload (38 bytes)

Domain Name System (query)

0000 0c b2 e8 cf 9c 05 f0 d5 bf be 0f 3c 00 00 45 00 ... <-@-0 7-.....

0010 00 3a cd bf 40 00 40 11 c7 77 c9 a8 12 2a c0 a8 ... @-0 7-.....

0020 12 01 8f 88 00 35 00 26 93 3e 14 ca 01 00 00 01 ... 5 & >.....

0030 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03w ww.ietf.

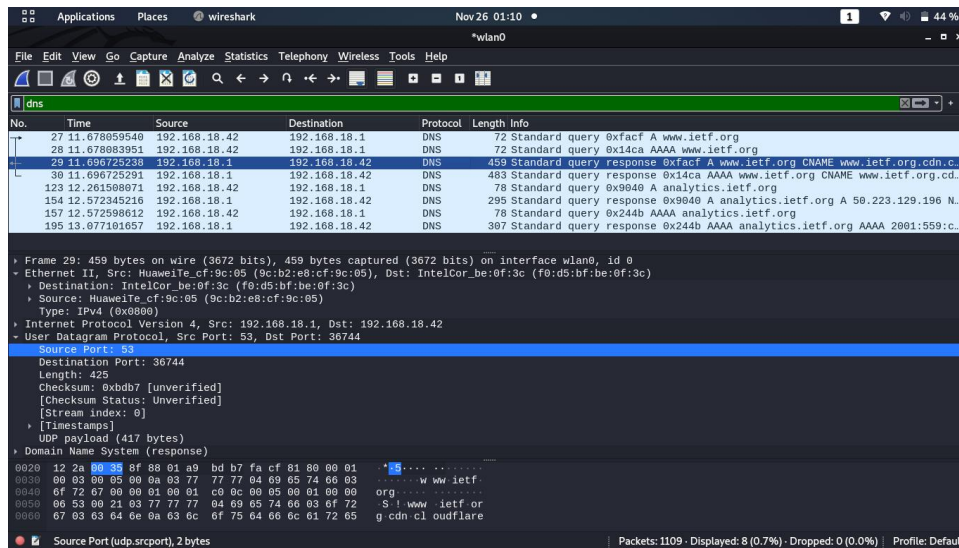
0040 6f 72 67 00 00 1c 00 01 ... org.....

Destination Port (udp.dstport), 2 bytes

Packets: 1109 - Displayed: 8 (0.7%) - Dropped: 0 (0.0%) | Profile: Default

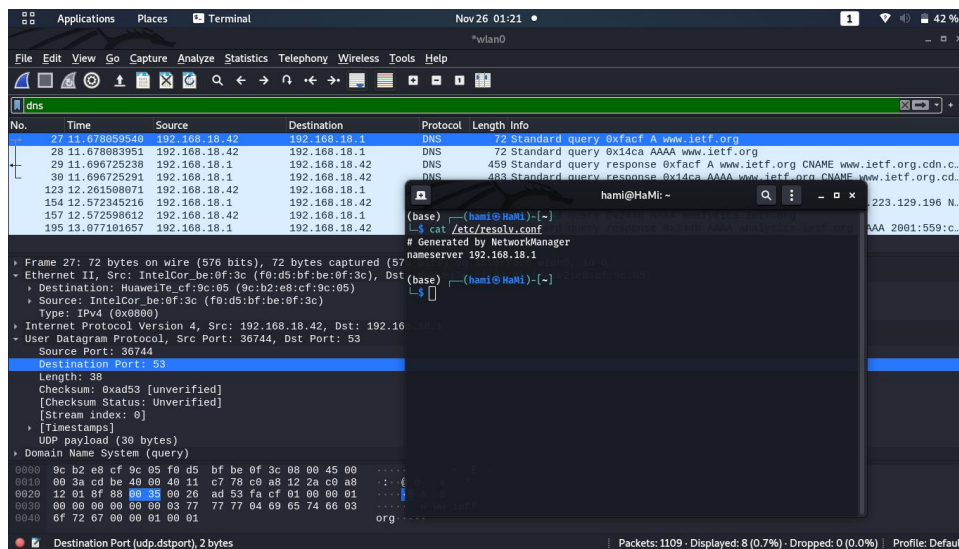
Dns response

Port 53



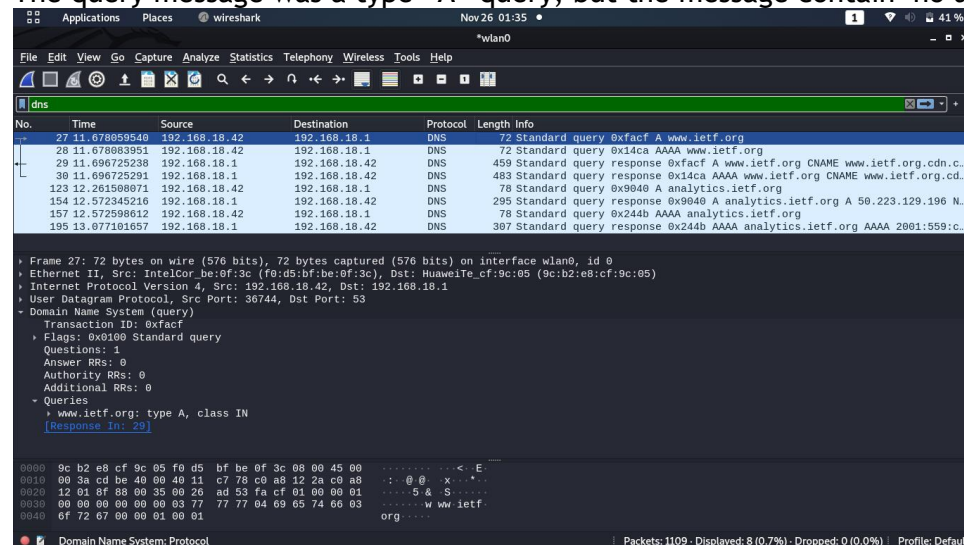
3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Both are same



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

The query message was a type “A” query, but the message contain no answers

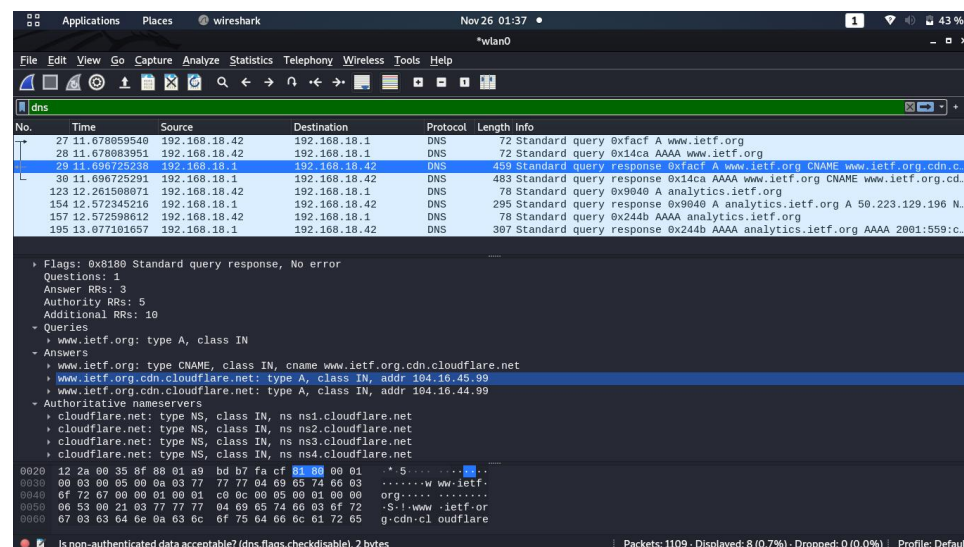


5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

3 Ans

Authority servenames : 5

Additional inforamtion : 10



6. 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 of the SYN packet is 50.223.129.196 , the same address that was provided in the DNS response message as the type “A” address of the webpage.

No.	Time	Source	Destination	Protocol	Length	Info
27	11.678059540	192.168.18.42	192.168.18.1	DNS	72	Standard query 0xfacf A www.ietf.org
28	11.678083951	192.168.18.42	192.168.18.1	DNS	72	Standard query 0x14ca AAAA www.ietf.org
29	11.696725238	192.168.18.1	192.168.18.42	DNS	459	Standard query response 0xfacf A www.ietf.org CNAME www.ietf.org.cdn.c...
30	11.696725291	192.168.18.1	192.168.18.42	DNS	483	Standard query response 0x14ca AAAA www.ietf.org CNAME www.ietf.org.cdn.c...
123	12.261588071	192.168.18.42	192.168.18.1	DNS	78	Standard query 0x9040 A analytics.ietf.org
124	12.572598612	192.168.18.42	192.168.18.1	DNS	225	Standard query response 0x9040 A analytics.ietf.org A 50.223.129.196 N...
157	12.572598612	192.168.18.42	192.168.18.1	DNS	78	Standard query 0x244b AAAA analytics.ietf.org
195	13.077101657	192.168.18.1	192.168.18.42	DNS	307	Standard query response 0x244b AAAA analytics.ietf.org AAAA 2001:559:c...

Queries

- analytics.ietf.org: type A, class IN
 - Name: analytics.ietf.org
 - Label count: 31
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

Answers

- analytics.ietf.org: type A, class IN, addr 50.223.129.196
 - Authoritative nameservers
 - ietf.org: type NS, class IN, ns ns1.hkg1.afilias-nst.info
 - ietf.org: type NS, class IN, ns ns1.ams1.afilias-nst.info
 - ietf.org: type NS, class IN, ns ns1.yyz1.afilias-nst.info
 - ietf.org: type NS, class IN, ns ns1.mia1.afilias-nst.info
 - ietf.org: type NS, class IN, ns ns1.sea1.afilias-nst.info
 - ietf.org: type NS, class IN, ns ns0.ams1.com

0040 04 69 65 74 66 03 6f 72 67 00 00 01 00 01 00 00 .ietf-or g-----
 0050 00 01 00 01 00 00 00 5a 00 04 32 df 61 64 c9 162.....
 0060 00 02 00 01 00 00 00 59 00 1b 03 6e 73 31 04 68V...nsi-h
 0070 6b 67 31 0b 01 66 09 6e 69 61 73 2d 0e 73 74 04 kg1:afilias-nst-
 0080 69 6e 66 6f 00 c0 16 00 02 00 01 00 00 0d 59 00 info.....Y.

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

Now let's play with nslookup4.

- Start packet capture.
- Do an nslookup on www.mit.edu
- Stop packet capture.

Yes, my host did issue new DNS queries before the images were retrieved. For example, one such query was for an image from open-stand.org. The image corresponding to the page was not returned until this query was made

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

Destination Port: 53

No.	Time	Source	Destination	Protocol	Length	Info
2	0.817999561	192.168.18.42	192.168.18.1	DNS	71	Standard query 0x6095 A www.mit.edu
3	0.817999561	192.168.18.1	192.168.18.42	DNS	484	Standard query response 0x0093 A www.mit.edu CNAME www.mit.edu.edgekey...
4	0.819273094	192.168.18.42	192.168.18.1	DNS	85	Standard query 0x7781 AAAA e9566.dscb.akamaiedge.net
7	0.871750246	192.168.18.1	192.168.18.42	DNS	465	Standard query response 0x7781 AAAA e9566.dscb.akamaiedge.net AAAA 260...

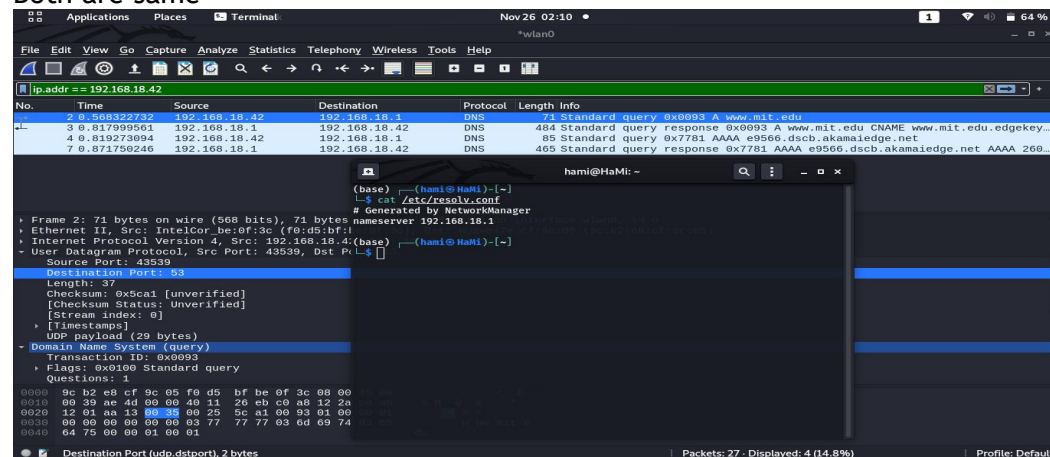
Frame 2: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface wlan0, id 0

- Ethernet II, Src: IntelCor_be:0f:3c (f0:d5:bf:be:0f:3c), Dst: HuaweiTe_cf:9c:05 (9c:b2:e8:cf:9c:05)
- Internet Protocol Version 4, Src: 192.168.18.42, Dst: 192.168.18.1
- User Datagram Protocol, Src Port: 43539, Dst Port: 53
 - Source Port: 43539
 - Destination Port: 53
 - Length: 37
 - Checksum: 0x5ca1 [unverified]
 - Checksum Status: Unverified
 - Stream index: 0
 - Timestamps
 - UDP payload (29 bytes)
 - Domain Name System (query)
 - Transaction ID: 0x0093
 - Flags: 0x0100 Standard query
 - Questions: 1

0000 9c b2 e8 cf 9c 05 f0 d5 bf be 0f 3c 08 00 45 00<...E
 0010 00 39 ae 4d 00 00 40 11 26 eb c0 a8 12 2a c0 a8 9 M @ &
 0020 12 01 aa 13 00 00 00 25 5c a1 00 93 01 00 00 01 5 % \
 0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65w w w mit e
 0040 64 75 00 00 01 00 01 du.....

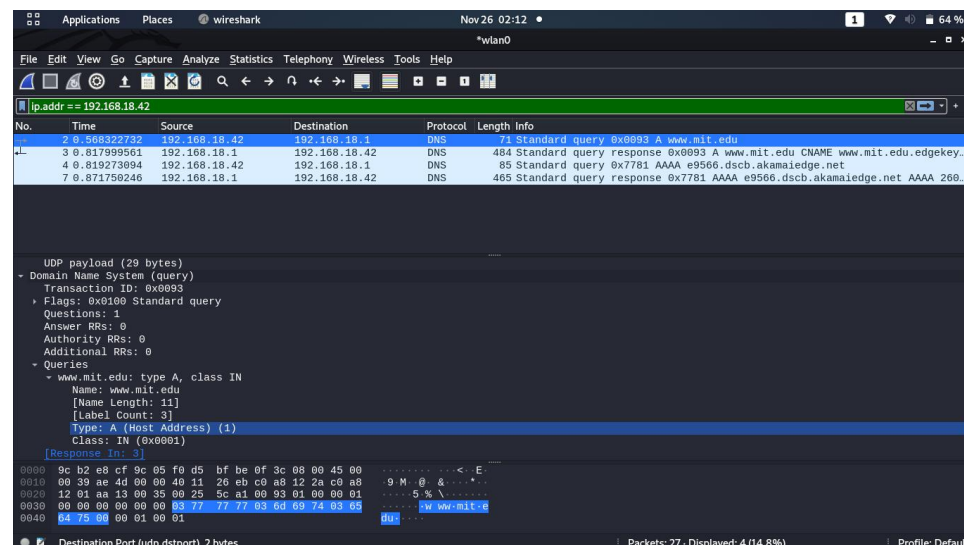
9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Both are same



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

The DNS query message is a type “A” query, containing only one question and not containing any answers.

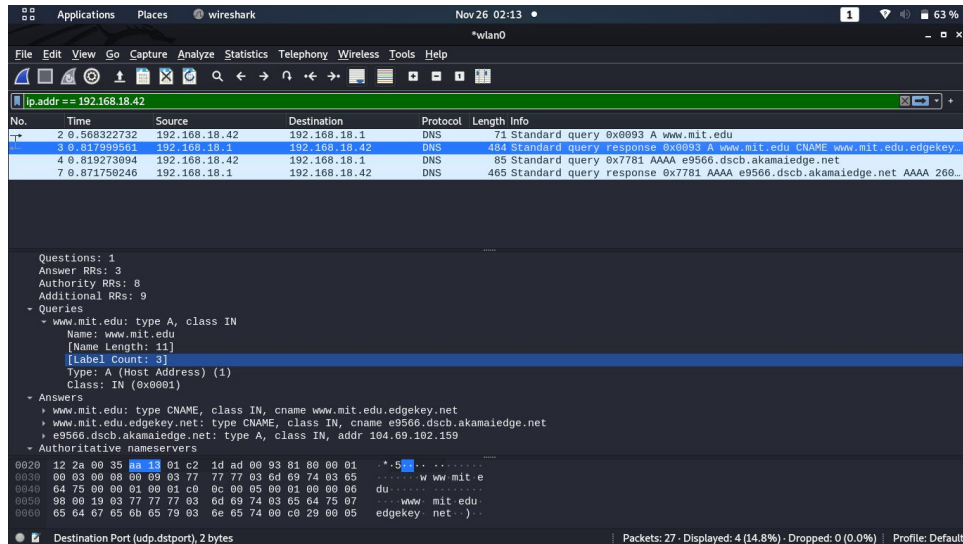


11. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer RRs: 3

Authority RRs: 8

Additional RRs: 9



12. Provide a screenshot.

