

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

ANS:

```
krishna@krishna-HP-G42-Notebook-PC: ~  
krishna@krishna-HP-G42-Notebook-PC:~$ nslookup www.livedoor.jp  
Server:          127.0.1.1  
Address:         127.0.1.1#53  
  
Non-authoritative answer:  
www.livedoor.jp canonical name = www.livedoor.com.  
Name:   www.livedoor.com  
Address: 125.6.149.67  
  
krishna@krishna-HP-G42-Notebook-PC:~$
```

The IP address of the server is 125.6.149.67

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

ANS:

University of Cambridge was the target of this nslookup at <http://www.cam.ac.uk>.

```
krishna@krishna-HP-G42-Notebook-PC: ~  
krishna@krishna-HP-G42-Notebook-PC:~$ nslookup -type=NS www.cam.ac.uk  
Server:          127.0.1.1  
Address:         127.0.1.1#53  
  
Non-authoritative answer:  
*** Can't find www.cam.ac.uk: No answer  
  
Authoritative answers can be found from:  
cam.ac.uk  
    origin = ipreg.csi.cam.ac.uk  
    mail addr = hostmaster.cam.ac.uk  
    serial = 1478919106  
    refresh = 1800  
    retry = 900  
    expire = 604800  
    minimum = 3600  
  
krishna@krishna-HP-G42-Notebook-PC:~$
```

The authoritative DNS server for Cambridge is ipreg.csi.cam.ac.uk

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?

ANS:

```
krishna@krishna-HP-G42-Notebook-PC: ~  
krishna@krishna-HP-G42-Notebook-PC:~$  
krishna@krishna-HP-G42-Notebook-PC:~$ nslookup ipreg.csi.cam.ac.uk mail.yahoo.com  
;; connection timed out; no servers could be reached  
krishna@krishna-HP-G42-Notebook-PC:~$
```

The connection timed out.

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

ANS:

ip.addr=192.168.0.81						
No.	Time	Source	Destination	Protocol	Length	Info
24	16:25:33.921314671	192.168.0.81	209.18.47.62	DNS	72	Standard query 0x37f8 AAAA www.ietf.org
25	16:25:33.922200153	ArrisGro_93:3c:17	Universa_fb:36:2d	ARP	56	Who has 192.168.0.81? Tell 192.168.0.1
26	16:25:33.922212949	Universa_fb:36:2d	ArrisGro_93:3c:17	ARP	42	192.168.0.81 is at e0:2a:82:fb:36:2d
27	16:25:33.974888265	209.18.47.62	192.168.0.81	DNS	156	Standard query response 0x628d A www.ietf.org CNAME www.ietf.org
28	16:25:33.974966311	209.18.47.62	192.168.0.81	DNS	180	Standard query response 0x37f8 AAAA www.ietf.org CNAME www.ietf.org
29	16:25:33.976407568	192.168.0.81	5.135.181.213	TCP	609	55360->9222 [PSH, ACK] Seq=1 Ack=1 Win=3630 Len=543 TSval=52...
30	16:25:34.103672234	5.135.181.213	192.168.0.81	TCP	66	9222->55360 [ACK] Seq=1 Ack=544 Win=1392 Len=0 TSval=3075529...
31	16:25:34.181482766	5.135.181.213	192.168.0.81	TCP	609	9222->55360 [PSH, ACK] Seq=1 Ack=544 Win=1392 Len=543 TSval=...
32	16:25:34.182343631	192.168.0.81	5.135.181.213	TCP	609	55360->9222 [PSH, ACK] Seq=544 Ack=544 Win=3630 Len=543 TSva...
33	16:25:34.469674712	5.135.181.213	192.168.0.81	TCP	66	9222->55360 [ACK] Seq=544 Ack=1087 Win=1392 Len=0 TSval=3075...
34	16:25:34.471807668	5.135.181.213	192.168.0.81	TCP	1514	9222->55360 [ACK] Seq=544 Ack=1087 Win=1392 Len=1448 TSval=3...
Frame 27: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface 0						
Ethernet II, Src: ArrisGro_93:3c:17 (00:ac:e0:93:3c:17), Dst: Universa_fb:36:2d (e0:2a:82:fb:36:2d)						
Internet Protocol Version 4, Src: 209.18.47.62, Dst: 192.168.0.81						
User Datagram Protocol, Src Port: 53, Dst Port: 23450						
Source Port: 53						
Destination Port: 23450						
Length: 122						
Checksum: 0x6494 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 4]						
Domain Name System (response)						

The query and response messages are sent via UDP.

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

ANS:

The destination port is port 23450, and the source port is port 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?

ANS:

```
krishna@krishna-HP-G42-Notebook-PC: ~  
IP4.DNS[1]: 209.18.47.61  
IP4.DNS[2]: 209.18.47.62  
IP6.ADDRESS[1]: 2605:6000:8a45:1e00:fc9a:dd34:c71e:162f/  
64  
IP6.ADDRESS[2]: 2605:6000:8a45:1e00:d666:5808:e1af:3e42/  
64  
IP6.ADDRESS[3]: fe80::d356:2104:2e65:aac5/64  
IP6.GATEWAY: fe80::2ac:e0ff:fe93:3c17
```

The DNS query message was sent to 209.18.47.61 This is the same IP address as the local DNS server.

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

ANS:

```
▼ Domain Name System (response)  
  [Request In: 23]  
  [Time: 0.053731735 seconds]  
  Transaction ID: 0x628d  
  ► Flags: 0x8180 Standard query response, No error  
    Questions: 1  
    Answer RRs: 3  
    Authority RRs: 0  
    Additional RRs: 0  
  ▼ Queries  
    ► www.ietf.org: type A, class IN
```

This query was a type A query. It did not contain any “answers”.

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

ANS:

```
▼ Queries
  ▶ www.ietf.org: type A, class IN
▼ Answers
  ▼ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare-dnssec.net
    Name: www.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1471
    Data length: 40
    CNAME: www.ietf.org.cdn.cloudflare-dnssec.net
  ▼ www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.0.85
    Name: www.ietf.org.cdn.cloudflare-dnssec.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300
    Data length: 4
    Address: 104.20.0.85
  ▼ www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.1.85
    Name: www.ietf.org.cdn.cloudflare-dnssec.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 300
    Data length: 4
    Address: 104.20.1.85
```

This DNS response message provided three answer. The answer contains the address of the website that it was queried for.

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?

ANS:

The destination IP address of the SYN packet corresponds to the address provided by the DNS response, 104.20.1.85

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

ANS:

No

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

ANS:

```
▼ User Datagram Protocol, Src Port: 14672, Dst Port: 53
  Source Port: 14672
  Destination Port: 53
  Length: 37
  Checksum: 0xd1af [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
```

The destination port for the DNS query message is port 53. The source port of the DNS response message is also port 14672.

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

ANS:

The DNS query message is sent to IP 209.18.47.61. This is the same IP address of my local DNS server.

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

ANS:

```
▼ Queries
  ► www.mit.edu: type A, class IN
```

This message is of type A. This query contains no answers.

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

ANS:

The first DNS response message contains no answer.

15. Provide a screenshot.

ANS:

The screenshot shows a Wireshark packet capture of a network interface. The top bar indicates the filter is 'ip.addr==192.168.0.81'. The packet list shows a series of packets, with packet 10 (a DNS query) selected. The packet details pane shows the structure of the DNS query, including the transaction ID, flags, and the query for 'www.mit.edu'. The packet bytes pane shows the raw data of the query, with the domain name 'www.mit.edu' visible in the hex and ASCII representation.

No.	Time	Source	Destination	Protocol	Length	Info
9	17:25:06.626814818	192.168.0.81	69.18.50.35	TCP	66	55632-443 [ACK] Seq=902 Ack=886 Win=685 Len=0 TSval=6154276...
10	17:25:07.351720129	192.168.0.81	209.18.47.61	DNS	71	Standard query 0xe07a A www.mit.edu
11	17:25:07.389952886	209.18.47.61	192.168.0.81	DNS	160	Standard query response 0xe07a A www.mit.edu CNAME www.mit...
12	17:25:08.326955293	192.168.0.81	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
13	17:25:08.352270121	fe80::2ac:e0ff:f...	ff02::1	ICMPv6	110	Router Advertisement from 00:ac:e0:93:3c:17
14	17:25:08.558536228	192.168.0.20	224.0.0.251	MDNS	304	Standard query response 0x0000 SRV, cache flush 0 0 8770 Ma...
15	17:25:08.562385174	fe80::a299:9bff:...	ff02::fb	MDNS	324	Standard query response 0x0000 SRV, cache flush 0 0 8770 Ma...
16	17:25:08.564720445	192.168.0.81	224.0.0.251	MDNS	92	Standard query 0x0000 SRV MacBook Pro._sftp-ssh._tcp.local,...
17	17:25:08.762981253	192.168.0.20	224.0.0.251	MDNS	231	Standard query response 0x0000 SRV, cache flush 0 0 22 MacB...
18	17:25:08.765565968	fe80::a299:9bff:...	ff02::fb	MDNS	251	Standard query response 0x0000 SRV, cache flush 0 0 22 MacB...
19	17:25:08.929464100	fe80::2ac:e0ff:f...	2605:6000:8a45:...	ICMPv6	86	Neighbor Solicitation for 2605:6000:8a45:1e00:fc9a:dd34:c71...

Frame 10: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
Ethernet II, Src: Universa_fb:36:2d (e0:2a:82:fb:36:2d), Dst: ArrisGro_93:3c:17 (00:ac:e0:93:3c:17)
Internet Protocol Version 4, Src: 192.168.0.81, Dst: 209.18.47.61
User Datagram Protocol, Src Port: 14672, Dst Port: 53
Domain Name System (query)
[Response In: 11]
Transaction ID: 0xe07a
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.mit.edu: type A, class IN

0000 00 ac e0 93 3c 17 e0 2a 82 fb 36 2d 08 00 45 00<.* ..6...E.
0010 00 39 1a 89 40 00 40 11 5e e2 c0 a8 00 51 d1 12 .9..@. ^...Q..
0020 2f 3d 39 50 00 35 00 25 d1 af e0 7a 01 00 00 01 /=9P.5.% ..z....
0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65w ww.mit.e
0040 64 75 00 00 01 00 01 du....

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

ANS:

```
Server: dns-cac-lb-01.rr.com
Address: 209.18.47.61

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

The IP address that the DNS query message is sent to 209.18.47.61, which is the same as my local DNS server.

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

ANS:

```
▼ Queries
  ▼ mit.edu.tx.rr.com: type NS, class IN
    Name: mit.edu.tx.rr.com
    [Name Length: 17]
    [Label Count: 5]
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
```

It is a type NS DNS query that contains no answers.

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?

ANS:

There are no response messages.

19. Provide a screenshot

ANS:

The screenshot shows a Wireshark packet capture of a network interface. The filter is set to `ip.addr==192.168.0.29`. The packet list shows several packets, with packet 9 selected. The packet details pane shows the following information:

- Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: Universa_fb:36:2d (e0:2a:82:fb:36:2d), Dst: Netgear_5b:b0:fa (a0:63:91:5b:b0:fa)
- Internet Protocol Version 4, Src: 192.168.0.29, Dst: 209.18.47.61
- User Datagram Protocol, Src Port: 64346, Dst Port: 53
- Domain Name System (query)
 - [Response In: 10]
 - Transaction ID: 0x0003
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0

The packet bytes pane shows the raw data of the DNS query:

```
0000 a0 63 91 5b b0 fa e0 2a 82 fb 36 2d 08 00 45 00 .c.[...* ..6...E.
0010 00 3c 3c 98 00 00 80 11 3d 04 c0 a8 00 1d d1 12 .<<.....=.....
0020 2f 3d fb 5a 00 35 00 28 28 51 00 03 01 00 00 01 /=.Z.5.( (Q.....
0030 00 00 00 00 00 03 6d 69 74 03 65 64 75 02 72 .....m it.edu.r
0040 72 03 63 6f 6d 00 00 02 00 01 r.com... ..
```

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?

ANS:

38	3.534646	192.168.0.29	18.72.0.3	DNS	84	Standard query 0x0002 A www.aiit.or.kr.tx.rr.com
42	5.537684	192.168.0.29	18.72.0.3	DNS	84	Standard query 0x0003 AAAA www.aiit.or.kr.tx.rr.com

The DNS query message is sent to 18.72.0.3 which is not the same as my local DNS server. This IP address corresponds to www.aiit.or.kr.

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

ANS:

```
▼ Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    > www.aiit.or.kr.tx.rr.com: type A, class IN
```

The DNS query message is a type A, and does not contain any answers.

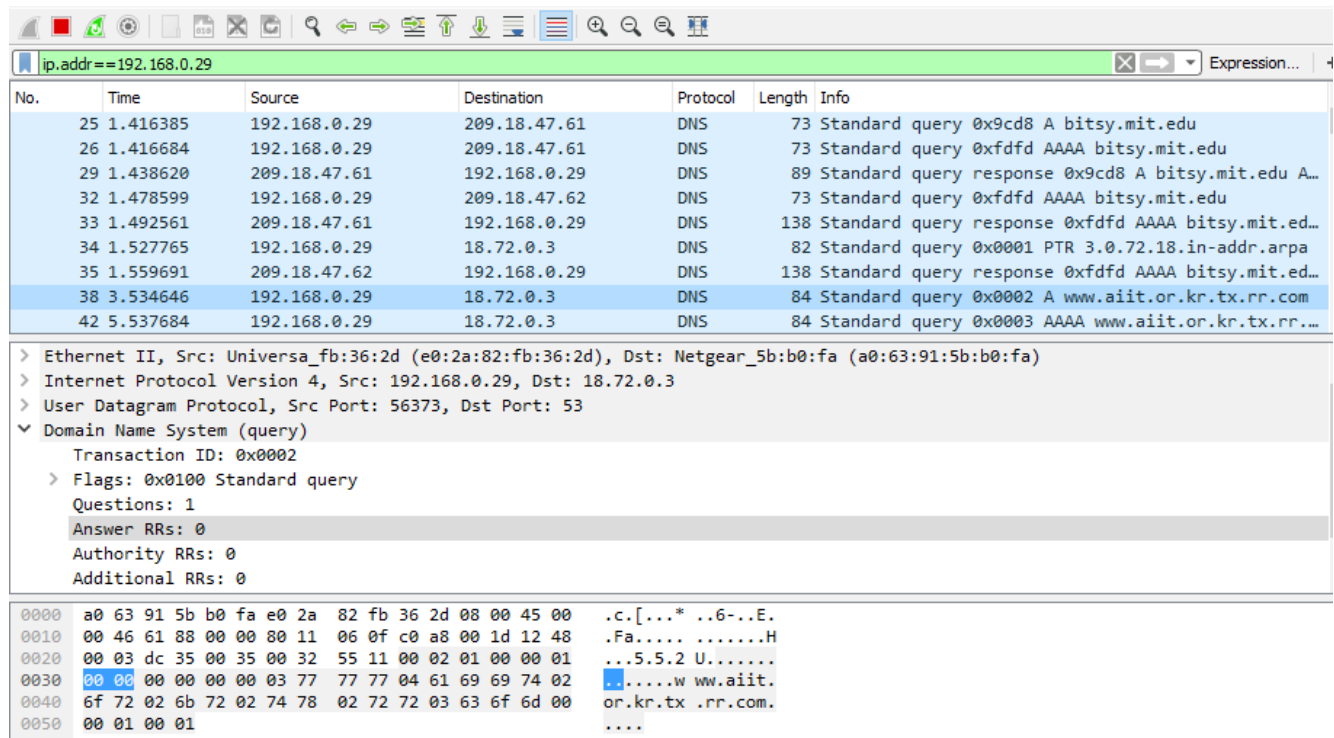
22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

ANS:

There are no response messages.

23. Provide a screenshot.

ANS:



The screenshot shows a Wireshark packet capture interface. The top toolbar includes icons for file operations, network analysis, and search. The filter bar at the top displays the filter `ip.addr==192.168.0.29`. The packet list pane shows a series of DNS packets. Packet 38 is selected, showing a standard query for `www.aiit.or.kr.tx.rr.com`. The packet details pane below shows the protocol stack: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The DNS section shows a transaction ID of `0x0002`, flags of `0x0100`, and one question. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII, including the domain name `www.aiit.or.kr.tx.rr.com`.

No.	Time	Source	Destination	Protocol	Length	Info
25	1.416385	192.168.0.29	209.18.47.61	DNS	73	Standard query 0x9cd8 A bitsy.mit.edu
26	1.416684	192.168.0.29	209.18.47.61	DNS	73	Standard query 0xfdfd AAAA bitsy.mit.edu
29	1.438620	209.18.47.61	192.168.0.29	DNS	89	Standard query response 0x9cd8 A bitsy.mit.edu A...
32	1.478599	192.168.0.29	209.18.47.62	DNS	73	Standard query 0xfdfd AAAA bitsy.mit.edu
33	1.492561	209.18.47.61	192.168.0.29	DNS	138	Standard query response 0xfdfd AAAA bitsy.mit.ed...
34	1.527765	192.168.0.29	18.72.0.3	DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
35	1.559691	209.18.47.62	192.168.0.29	DNS	138	Standard query response 0xfdfd AAAA bitsy.mit.ed...
38	3.534646	192.168.0.29	18.72.0.3	DNS	84	Standard query 0x0002 A www.aiit.or.kr.tx.rr.com
42	5.537684	192.168.0.29	18.72.0.3	DNS	84	Standard query 0x0003 AAAA www.aiit.or.kr.tx.rr...

> Ethernet II, Src: Universa_fb:36:2d (e0:2a:82:fb:36:2d), Dst: Netgear_5b:b0:fa (a0:63:91:5b:b0:fa)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 18.72.0.3
> User Datagram Protocol, Src Port: 56373, 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

0000 a0 63 91 5b b0 fa e0 2a 82 fb 36 2d 08 00 45 00 .c.[...* ..6--E.
0010 00 46 61 88 00 00 80 11 06 0f c0 a8 00 1d 12 48 .Fa.....H
0020 00 03 dc 35 00 35 00 32 55 11 00 02 01 00 00 01 ...5.5.2 U.....
0030 00 00 00 00 00 03 77 77 77 04 61 69 69 74 02w ww.aiit.
0040 6f 72 02 6b 72 02 74 78 02 72 72 03 63 6f 6d 00 or.kr.tx .rr.com.
0050 00 01 00 01