1. What is the IP address of www.upd.edu.ph?

The IP address is 202.92.128.226

```
C:\Programming\BIND9.10.6-P1.x64>nslookup www.upd.edu.ph
Server: 8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
www.upd.edu.ph canonical name = upd.edu.ph.
Name: upd.edu.ph
Address: 202.92.128.226
```

2. What are the authoritative DNS servers for upd.edu.ph?

The authoritative DNS servers are as follows:

```
ns01.upd.edu.ph
ns02.upd.edu.ph
ns03.upd.edu.ph
```

```
C:\Programming\BIND9.10.6-P1.x64>nslookup -type=NS upd.edu.ph
Server: 8.8.8.8
Address: 8.8.8#53

Non-authoritative answer:
upd.edu.ph nameserver = ns01.upd.edu.ph.
upd.edu.ph nameserver = ns02.upd.edu.ph.
upd.edu.ph nameserver = ns03.upd.edu.ph.
```

3. What are the hostname and IP address of the mail servers for @upd.edu.ph?

The hostnames and IP addresses of the mail servers are as follows:

mailc.upd.edu.ph and 202.92.128.138

mailc01.upd.edu.ph and 202.92.128.137

```
fsfbayani@agila:~$ nslookup -type=MX upd.edu.ph
Server:
               172.16.1.130
Address:
               172.16.1.130#53
Non-authoritative answer:
               mail exchanger = 10 mailc.upd.edu.ph.
upd.edu.ph
upd.edu.ph
               mail exchanger = 20 mailc01.upd.edu.ph.
Authoritative answers can be found from:
upd.edu.ph nameserver = ns01.upd.edu.ph.
upd.edu.ph
              nameserver = ns02.upd.edu.ph.
upd.edu.ph nameserver = ns03.upd.edu.ph.
mailc.upd.edu.ph
                       internet address = 202.92.128.138
mailc01.upd.edu.ph internet address = 202.92.128.137
ns01.upd.edu.ph internet address = 202.92.128.248
ns02.upd.edu.ph internet address = 202.92.128.249
ns03.upd.edu.ph internet address = 202.92.130.1
```

4. What are the IP addresses of www.yahoo.com?

IPv4 Addresses:

106.10.178.36

106.10.178.37

IPv6 Addresses:

2406:2000:e4:200::3007

2406:2000:e4:200::3006

```
fsfbayani@agila:~$ dig www.yahoo.com A +short
atsv2-fp.wgl.b.yahoo.com.
106.10.178.36
106.10.178.37
fsfbayani@agila:~$ dig www.yahoo.com AAAA +short
atsv2-fp.wgl.b.yahoo.com.
2406:2000:e4:200::3007
2406:2000:e4:200::3006
```

5. Is www.yahoo.com a canonical name or an alias? If it's an alias, then what is the canonical name?

The canonical name as atsv2-fp.wgl.b.yahoo.com

fsfbayani@agila:~\$ dig www.yahoo.com PTR +short atsv2-fp.wgl.b.yahoo.com.

6. What are the names and IP addresses of the authoritative name servers of yahoo.com?

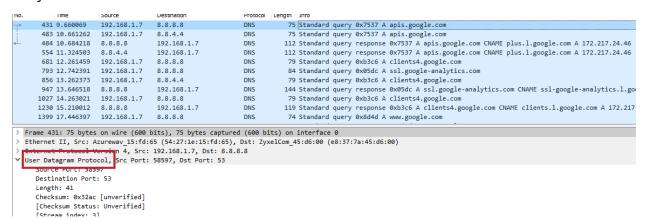
The names and IP addresses of the authoritative name servers of yahoo.com are as follows:

```
yf1.yahoo.com 68.142.254.15
yf2.yahoo.com 68.180.130.15
yf3.al.b.yahoo.net 203.84.209.160
yf4.al.b.yahoo.net 183.177.82.12
```

```
fsfbayani@agila:~$ dig www.yahoo.com
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27278
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 5
;; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.yahoo.com.
                                IN
                                        Α
;; ANSWER SECTION:
                                IN
                                        CNAME
                                                atsv2-fp.wgl.b.yahoo.com.
www.yahoo.com.
                        933
atsv2-fp.wgl.b.yahoo.com. 60
                                IN
                                        Α
                                                106.10.178.36
atsv2-fp.wgl.b.yahoo.com. 60
                                IN
                                        Α
                                                106.10.178.37
;; AUTHORITY SECTION:
                                                yf2.yahoo.com.
wgl.b.yahoo.com.
                        124911 IN
                                        NS
                        124911 IN
                                        NS
wgl.b.yahoo.com.
                                                yfl.yahoo.com.
wgl.b.yahoo.com.
                        124911
                                IN
                                        NS
                                                yf4.al.b.yahoo.net
wgl.b.yahoo.com.
                        124911 IN
                                        NS
                                                yf3.al.b.yahoo.net
;; ADDITIONAL SECTION:
fl.yahoo.com.
                        38461
                                IN
                                        Α
                                                68.142.254.15
yf2.yahoo.com.
                        38461
                                IN
                                        Α
                                                68.180.130.15
                        38461
                                IN
                                                203.84.209.160
yf3.al.b.yahoo.net.
                                        Α
                        38461 IN
                                        Α
yf4.al.b.yahoo.net.
                                                183.177.82.12
;; Query time: 41 msec
;; SERVER: 172.16.1.130#53(172.16.1.130)
;; WHEN: Sat Feb 10 22:51:09 +08 2018
  MSG SIZE rcvd: 253
```

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

They are sent over UDP.



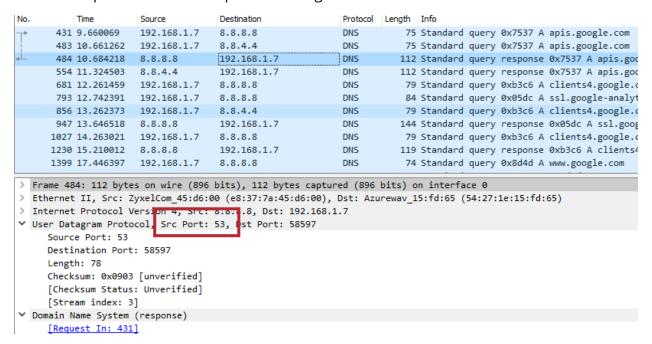
8. What is the destination port for the DNS query message? What is the source port of DNS response message?

The destination port of the DNS query message is 53.

```
INO.
                     Source
                                  Desunation
                                                         Protocol Length Into
      431 9.660069 192.168.1.7 8.8.8.8
                                                          DNS
                                                                    75 Standard query 0x7537
      483 10.661262 192.168.1.7 8.8.4.4
                                                          DNS
                                                                    75 Standard query 0x7537
      484 10.684218 8.8.8.8 192.168.1.7
554 11.324503 8.8.4.4 192.168.1.7
                                                                   112 Standard query respons
                                                          DNS
                                                                   112 Standard query respons
                                                         DNS
      681 12.261459 192.168.1.7 8.8.8.8
                                                         DNS
                                                                   79 Standard query 0xb3c6
      793 12.742391 192.168.1.7 8.8.8.8
                                                        DNS
                                                                    84 Standard query 0x05dc
      856 13.262373 192.168.1.7 8.8.4.4
                                                        DNS
                                                                    79 Standard query 0xb3c6
      947 13.646518 8.8.8.8
                                 192.168.1.7
                                                        DNS
                                                                   144 Standard query respons
      1027 14.263021 192.168.1.7 8.8.8.8
                                                                    79 Standard query 0xb3c6
                                                         DNS
                                                          DNS
      1230 15.210012 8.8.8.8
                                   192.168.1.7
                                                                    119 Standard query response
      1399 17.446397 192.168.1.7 8.8.8.8
                                                          DNS
                                                                    74 Standard query 0x8d4d
> Frame 431: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
> Ethernet II, Src: Azurewav 15:fd:65 (54:27:1e:15:fd:65), Dst: ZyxelCom 45:d6:00 (e8:37:7a:45:d6
> Internet Protocol Version 4, Src: 192.160.1.7, Data 0.6.8.8

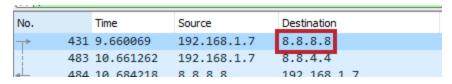
✓ User Datagram Protocol, Src Port: 58597 Dst Port: 53
     Source Port: 58597
     Destination Port: 53
     Length: 41
     Checksum: 0x32ac [unverified]
```

The source port of the DNS response message is also 53.



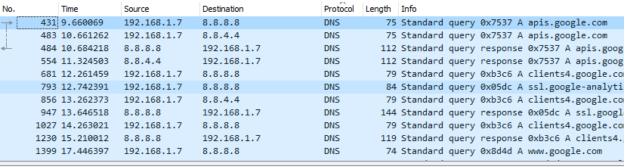
9. To what IP address is the DNS query message sent? Is this the same as your local DNS server?

The DNS query message was sent to 8.8.8.8. This is not the same as my local DNS server.



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

The query message was a "type A" query, and it did not contain any "answers".



```
[Response In: 484]
  Transaction ID: 0x7537

▼ Flags: 0x0100 Standard query

    0... - Response: Message is a query
    .000 0... = Opcode: Standard query (0)
     .... ..0. .... = Truncated: Message is not truncated
     .... ...1 .... = Recursion desired: Do query recursively
     .... = Z: reserved (0)
     .... .... ... O .... = Non-authenticated data: Unacceptable
  Ouestions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
     apis.google.com: type A, class IM
       Name, apis.googie.com
       [Name Length: 15]
       [Label Count: 3]
```

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

They contain the IP address 172.217.24.46.

```
112 Standard query response 0x7537 A apis.google.com CNAME plus.l.google.com A 172.217.24.46
112 Standard query response 0x7537 A apis.google.com CNAME plus.l.google.com A 172.217.24.46
                                  192.168.1.7
 484 10.684218
                  8.8.8.8
 554 11.324503
                                  192.168.1.7
 681 12.261459
                 192.168.1.7
                                  8.8.8.8
                                                           DNS
                                                                       79 Standard query 0xb3c6 A clients4.google.com
  793 12.742391
                                                                        84 Standard query 0x05dc A ssl.google-analytics.com
 856 13.262373
                 192.168.1.7
                                  8.8.4.4
                                                           DNS
                                                                       79 Standard query 0xb3c6 A clients4.google.com
 947 13.646518
                  8.8.8.8
                                  192.168.1.7
                                                           DNS
                                                                      144 Standard query response 0x05dc A ssl.google-analytics.com CNAME ssl-google-analytics.l.go
1027 14.263021
                 192.168.1.7
                                                                        79 Standard query 0xb3c6 A clients4.google.com
                                  192.168.1.7
1230 15.210012
                 8.8.8.8
                                                           DNS
                                                                      119 Standard query response 0xb3c6 A clients4.google.com CNAME clients.l.google.com A 172.217
1399 17.446397
                 192.168.1.7 8.8.8.8
                                                                       74 Standard query 0x8d4d A www.google.com
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0

y apis.google.com: type CNAME, class IN, cname plus.l.google.com

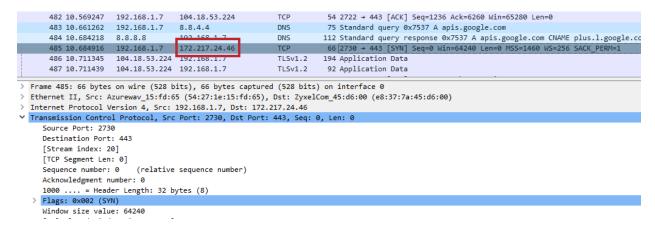
      Name: apis.google.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 21599
     Data length: 9
CNAME: plus.l.google.com

▼ plus.l.google.com: type A, class IN, addr 172.217.24.46

      Name: plus.l.google.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 299
      Data length: 4
```

12. 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?

Yes, it does correspond to **172.217.24.46**.



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

Yes.

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

The destination port of the DNS query message is 53.

```
218 88.966918 8.8.8.8
                                      192.168.1./
                                                                          165 Standard query response 0xdae5 No such name A C:ProgrammingBl
       225 94.367837 192.168.1.7
                                      8.8.8.8
                                                               DNS
                                                                           78 Standard query 0xb012 A berdugo.upm.edu.ph
      227 95.367681 192.168.1.7
                                                                           78 Standard query 0xb012 A berdugo.upm.edu.ph
                                    8.8.4.4
                                                              DNS
      228 95.445833 8.8.8.8
                                      192.168.1.7
                                                              DNS
                                                                           94 Standard query response 0xb012 A berdugo.upm.edu.ph A 202.92.
      229 96.428894 8.8.4.4
                                    192.168.1.7
                                                              DNS
                                                                          94 Standard query response 0xb012 A berdugo.upm.edu.ph A 202.92.
> Frame 225: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: ZyxelCom_45:d6:00 (e8:37:7a:45:d6:00)
> Internet Protocol Version 4, Src: 192.160-1-7, Bate 9

V User Datagram Protocol, Src Port: 64274 Dst Port: 53
                                                            .8.8
     Source Port: 64274
     Destination Port: 53
     Length: 44
     Checksum: 0x0293 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 6]

✓ Domain Name System (query)

     [Response In: 228]
```

The source port of the DNS response message is 53.

```
228 95.445833
                                                                              94 Standard query response 0xb012 A berdugo.upm.edu.ph A 202.92.148.162
                       8.8.8.8
                                        192.168.1.7
       229 96.428894 8.8.4.4
                                                                              94 Standard query response 0xb012 A berdugo.upm.edu.ph A 202.92.148.162
> Frame 228: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
> Ethernet II, Src: ZyxelCom_45:d6:00 (e8:37:7a:45:d6:00), Dst: Azurewav_15:fd:65 (54:27:1e:15:fd:65)
> Internet Protocol Version 4 Spc. 8 8 8.8, Dst: 192.168.1.7

V User Datagram Protocol Spc Port: 53, st Port: 64274
     Source Port: 53
     Destination Port: 64274
     Length: 60
     Checksum: 0x5143 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 6]

✓ Domain Name System (response)

     [Request In: 225]
```

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

It was sent to **8.8.8.8** (Google's Public DNS), this is not the address of my default local DNS server.

```
218 88.966918 8.8.8.8 192.168.1.7 DNS 165 Standard query response 0xdae5 No such name A C:Progra 225 94.367837 192.168.1.7 8.8.8.8 DNS 78 Standard query 0xb012 A berdugo.upm.edu.ph 227 95.367681 192.168.1.7 8.8.4.4 DNS 78 Standard query 0xb012 A berdugo.upm.edu.ph 228 95.445833 8.8.8.8 192.168.1.7 DNS 94 Standard query response 0xb012 A berdugo.upm.edu.ph A
```

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

It is a "type A", with no answers.

```
225 94.367837 192.168.1.7 8.8.8.8 DNS 78 Standard query 0xb012 A berdugo.upm.edu.ph
                                                          DNS 78 Standard query 0xb012 A berdugo.upm.edu.ph
DNS 94 Standard query response 0xb012 A berdugo.up
DNS 94 Standard query response 0xb012 A berdugo.up
DNS 94 Standard query response 0xb012 A berdugo.up
DNS 93 Standard query 0x1068 A v20.vortex-win.data
     227 95.367681 192.168.1.7 8.8.4.4
    228 95.445833 8.8.8.8 192.168.1.7
229 96.428894 8.8.4.4 192.168.1.7
    411 254.761062 192.168.1.7 8.8.8.8
    412 255.760986 192.168.1.7 8.8.4.4 DNS 93 Standard query 0x1068 A v20.vortex-win.data
    413 256.015306 8.8.8.8 192.168.1.7 DNS 210 Standard query response 0x1068 A v20.vortex 417 256.848576 8.8.4.4 192.168.1.7 DNS 210 Standard query response 0x1068 A v20.vortex 448 287.544450 192.168.1.7 8.8.8.8 DNS 87 Standard query 0x4b0f A roaming.officeapps.
   [Response In: 228]
   Transaction ID: 0xb012

▼ Flags: 0x0100 Standard query

      0... .... = Response: Message is a query
      .000 0... = Opcode: Standard query (0)
      .... ..0. .... = Truncated: Message is not truncated
      .... ...1 .... = Recursion desired: Do query recursively
      .... = Z: reserved (0)
      .... .... 0 .... = Non-authenticated data: Unacceptable
   Ouestions: 1
 Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0

✓ Queries

✓ berdugo.upm.edu.ph: type A class IN

          Name: berdugo.upm.edu.ph
```

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

Only one answer was provided, the answer contains an IP address.

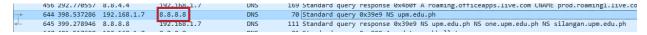
```
22/ 95.36/681 192.168.1./
                                    8.8.4.4
                                                           DNS
                                                                       אס Standard query שאסטוב A perdugo.upm.edu.pn
      228 95.445833 8.8.8.8
                                     192.168.1.7
                                                           DNS
                                                                       94 Standard query response 0xb012 A berdugo.upm.edu.ph A 202.92.148.162
      229 96.428894
                     8.8.4.4
                                    192.168.1.7
                                                           DNS
                                                                       94 Standard query response 0xb012 A berdugo.upm.edu.ph A 202.92.148.162
      411 254.761062 192.168.1.7 8.8.8.8
                                                           DNS
                                                                      93 Standard guery 0x1068 A v20.vortex-win.data.microsoft.com
      412 255.760986 192.168.1.7
                                    8.8.4.4
                                                                       93 Standard query 0x1068 A v20.vortex-win.data.microsoft.com
     [Checksum Status: Unverified]
     [Stream index: 6]

✓ Domain Name System (response)

     [Request In: 225]
     [Time: 1.077996000 seconds]
     Transaction ID: 0xb012
  > Flags: 0x8180 Standard query response, No error
     Answer RRs: 1
     Authority RRs: 0
     Additional RRs: 0
     ∨ berdugo.upm.edu.ph: type A, class IN, addr 202.92.148.162
          Name: berdugo.upm.edu.ph
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 4508
          Data length: 4
          Address: 202.92.148.162
```

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

It was sent to **8.8.8.8** (Google's Public DNS), this is not the address of my default local DNS server.



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

It is a "type NS" DNS query, for nameservers. It does not contain any answers.

```
644 398.537286 192.168.1.7 8.8.8.8
                                                                                            DNS 70 Standard query 0x39e9 NS upm.edu.ph
         645 399.278946 8.8.8.8 192.168.1.7 DNS 111 Standard query response 0x39e9 NS upm 647 401.517698 192.168.1.7 8.8.8.8 DNS 81 Standard query 0xc999 A update.pushbu
         648 402.436252 8.8.8.8 192.168.1.7 DNS 113 Standard query response 0xc999 A upda 681 431.402888 192.168.1.7 8.8.8.8 DNS 81 Standard query 0x76a4 A config.edge.s 682 431.402895 192.168.1.7 8.8.8.8 DNS 91 Standard query 0x8cb2 A client-office 685 432.259117 8.8.8.8 192.168.1.7 DNS 202 Standard query response 0x8cb2 A clie 687 432.264278 8.8.8.8 192.168.1.7 DNS 130 Standard query response 0x76a4 A conf
       Destination Port: 53
        Checksum: 0xde47 [unverified]
        [Checksum Status: Unverified]
        [Stream index: 22]

✓ Domain Name System (query)

       [Response In: 645]
        Transaction ID: 0x39e9
    > Flags: 0x0100 Standard query
        Ouestions: 1
       Answer RRs: 0
        Authority RRs: 0
       Additional RRs: 0

✓ Queries

        ∨ upm.edu.ph: type NS, class IN
               Name: upm.edu.ph
                [Name Length: 10]
```

20. Examine the DNS response message. What name servers does the response provide?

The name servers provided are **one.upm.edu.ph** and **silangan.upm.edu.ph**.

