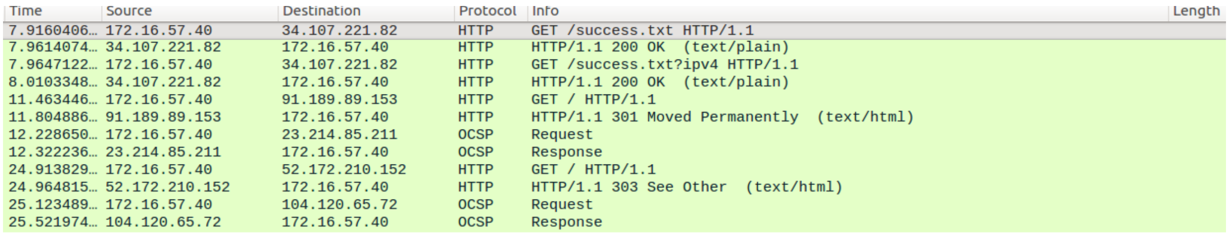
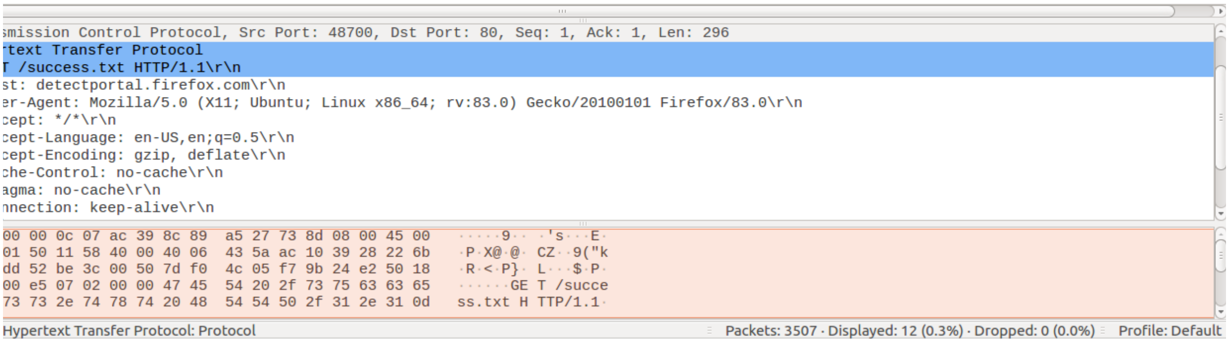
Aditya Pradhan CSE D 180905350

Lab3
Q3.1



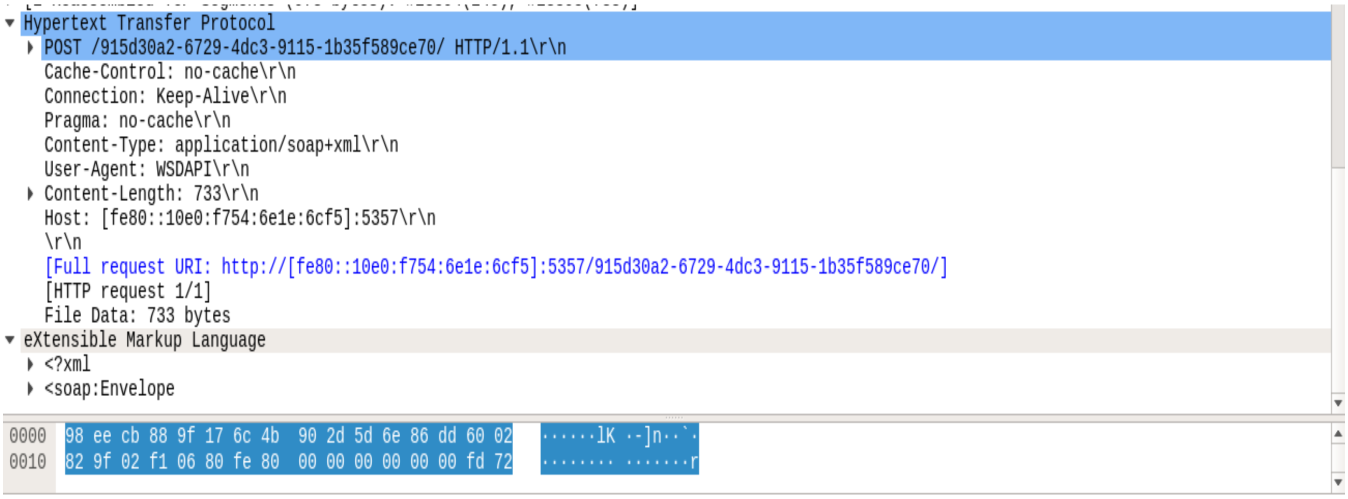
Time	Source	Destination	Protocol	Info	Length
7.9160406…	172.16.57.40	34.107.221.82	HTTP	GET /success.txt HTTP/1.1	
7.9614074…	34.107.221.82	172.16.57.40	HTTP	HTTP/1.1 200 OK (text/plain)	
7.9647122…	172.16.57.40	34.107.221.82	HTTP	GET /success.txt?ipv4 HTTP/1.1	
8.0103348…	34.107.221.82	172.16.57.40	HTTP	HTTP/1.1 200 OK (text/plain)	
11.463446…	172.16.57.40	91.189.89.153	HTTP	GET / HTTP/1.1	
11.804886…	91.189.89.153	172.16.57.40	HTTP	HTTP/1.1 301 Moved Permanently (text/html)	
12.228650…	172.16.57.40	23.214.85.211	OCSP	Request	
12.322236…	23.214.85.211	172.16.57.40	OCSP	Response	
24.913829…	172.16.57.40	52.172.210.152	HTTP	GET / HTTP/1.1	
24.964815…	52.172.210.152	172.16.57.40	HTTP	HTTP/1.1 303 See Other (text/html)	
25.123489…	172.16.57.40	104.120.65.72	OCSP	Request	
25.521974…	104.120.65.72	172.16.57.40	OCSP	Response	



```
smission Control Protocol, Src Port: 48700, Dst Port: 80, Seq: 1, Ack: 1, Len: 296
rtext Transfer Protocol
T /success.txt HTTP/1.1\r\n
st: detectportal.firefox.com\r\n
er-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0\r\n
cept: */*\r\n
cept-Language: en-US,en;q=0.5\r\n
cept-Encoding: gzip, deflate\r\n
che-Control: no-cache\r\n
agma: no-cache\r\n
nnection: keep-alive\r\n
```

```
00 00 0c 07 ac 39 8c 89  a5 27 73 8d 08 00 45 00   ·····9·· ·'s···E·
01 50 11 58 40 00 40 06  43 5a ac 10 39 28 22 6b   ·P·X@·@· CZ··9("k
dd 52 be 3c 00 50 7d f0  4c 05 f7 9b 24 e2 50 18   ·R·<·P}· L···$·P·
00 e5 07 02 00 00 47 45  54 20 2f 73 75 63 63 65   ······GE T /succe
73 73 2e 74 78 74 20 48  54 54 50 2f 31 2e 31 0d   ss.txt H TTP/1.1·
```

Hypertext Transfer Protocol: Protocol   Packets: 3507 · Displayed: 12 (0.3%) · Dropped: 0 (0.0%)   Profile: Default



```
▾ Hypertext Transfer Protocol
  ▸ POST /915d30a2-6729-4dc3-9115-1b35f589ce70/ HTTP/1.1\r\n
    Cache-Control: no-cache\r\n
    Connection: Keep-Alive\r\n
    Pragma: no-cache\r\n
    Content-Type: application/soap+xml\r\n
    User-Agent: WSDAPI\r\n
  ▸ Content-Length: 733\r\n
    Host: [fe80::10e0:f754:6e1e:6cf5]:5357\r\n
    \r\n
    [Full request URI: http://[fe80::10e0:f754:6e1e:6cf5]:5357/915d30a2-6729-4dc3-9115-1b35f589ce70/]
    [HTTP request 1/1]
    File Data: 733 bytes
▾ eXtensible Markup Language
  ▸ <?xml
  ▸ <soap:Envelope
```

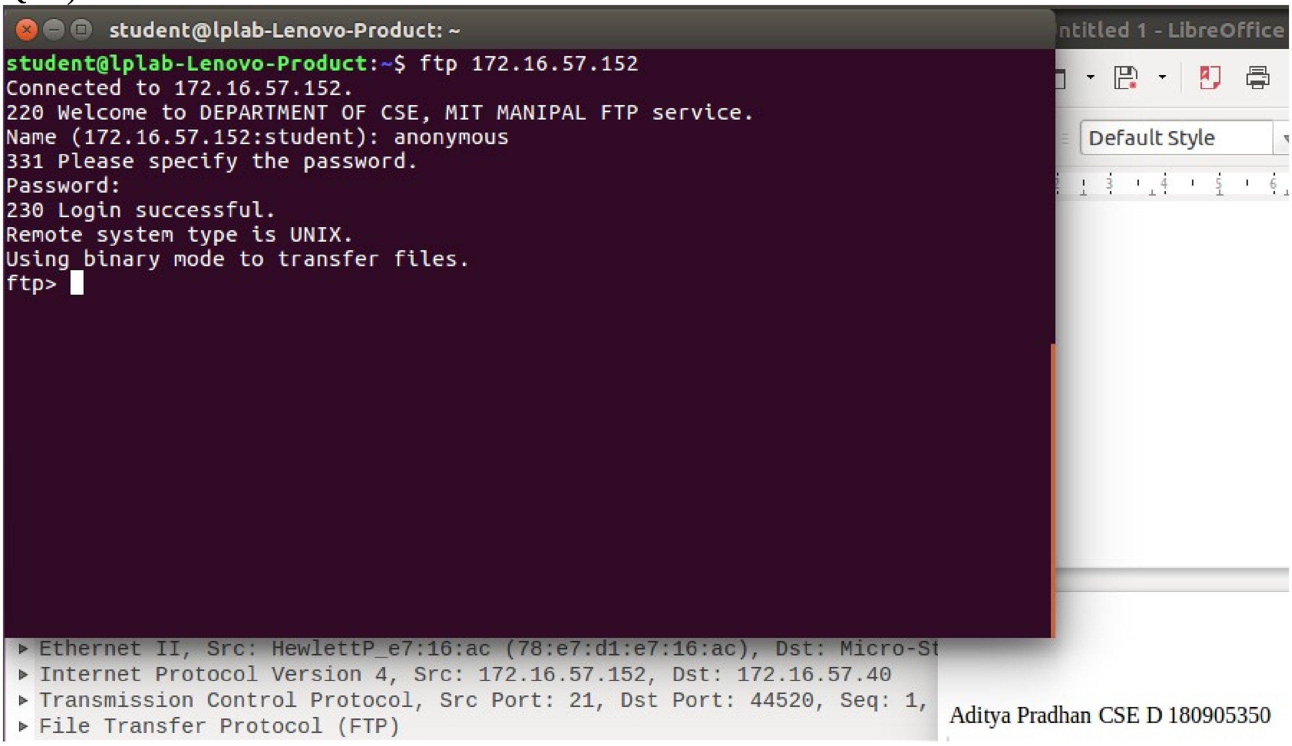
```
0000  98 ee cb 88 9f 17 6c 4b  90 2d 5d 6e 86 dd 60 02   ······lK ·-]n··`·
0010  82 9f 02 f1 06 80 fe 80  00 00 00 00 00 00 fd 72   ········ ·······r
```

Line 1725, my web browser sends a request to the server (a GET request)
Line 1734, server sends an acknowledgement back to my browser.

Most common HTTP methods are GET and POST.
Others are put and delete

Aditya Pradhan CSE D 180905350

Q3.2)

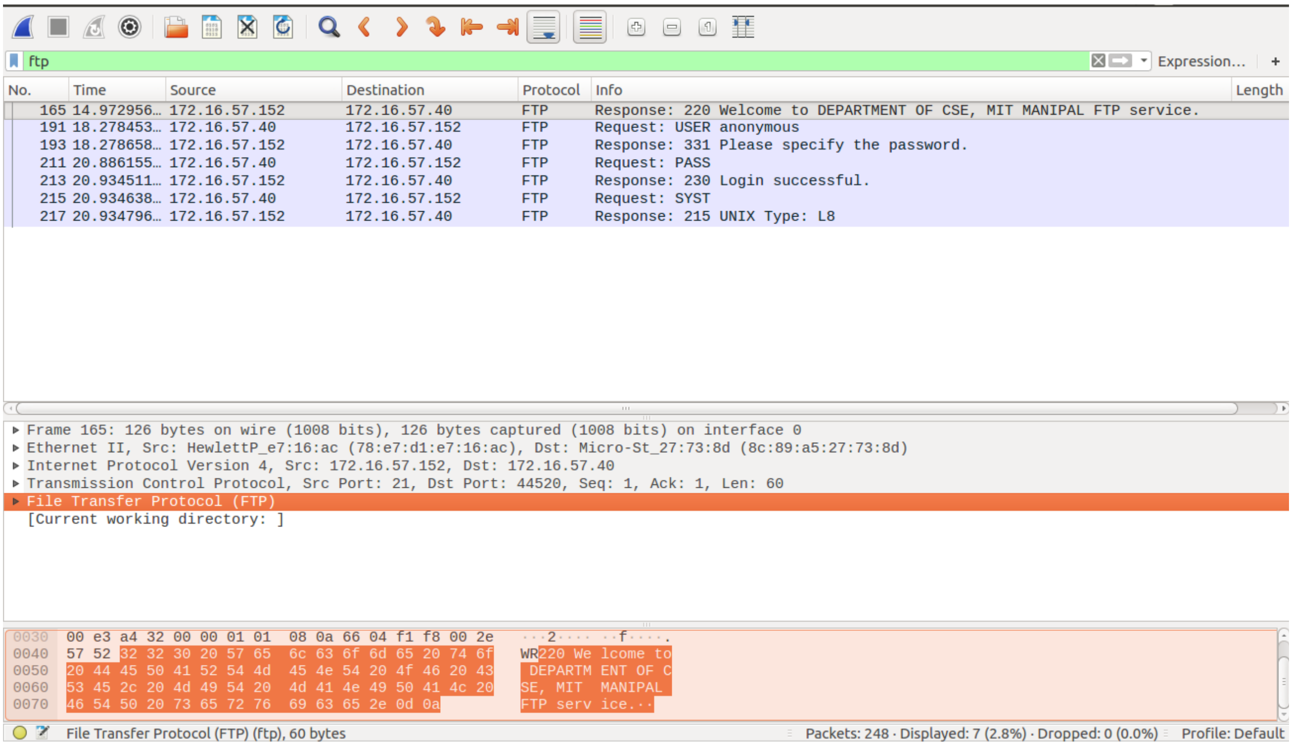


```
student@lplab-Lenovo-Product:~$ ftp 172.16.57.152
Connected to 172.16.57.152.
220 Welcome to DEPARTMENT OF CSE, MIT MANIPAL FTP service.
Name (172.16.57.152:student): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

```
▸ Ethernet II, Src: HewlettP_e7:16:ac (78:e7:d1:e7:16:ac), Dst: Micro-St
▸ Internet Protocol Version 4, Src: 172.16.57.152, Dst: 172.16.57.40
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 44520, Seq: 1,
▸ File Transfer Protocol (FTP)
```

Aditya Pradhan CSE D 180905350

Wireshark



```
No.  Time           Source         Destination    Protocol  Info                                                              Length
165  14.972956…  172.16.57.152  172.16.57.40   FTP       Response: 220 Welcome to DEPARTMENT OF CSE, MIT MANIPAL FTP service.
191  18.278453…  172.16.57.40   172.16.57.152  FTP       Request: USER anonymous
193  18.278658…  172.16.57.152  172.16.57.40   FTP       Response: 331 Please specify the password.
211  20.886155…  172.16.57.40   172.16.57.152  FTP       Request: PASS
213  20.934511…  172.16.57.152  172.16.57.40   FTP       Response: 230 Login successful.
215  20.934638…  172.16.57.40   172.16.57.152  FTP       Request: SYST
217  20.934796…  172.16.57.152  172.16.57.40   FTP       Response: 215 UNIX Type: L8
```

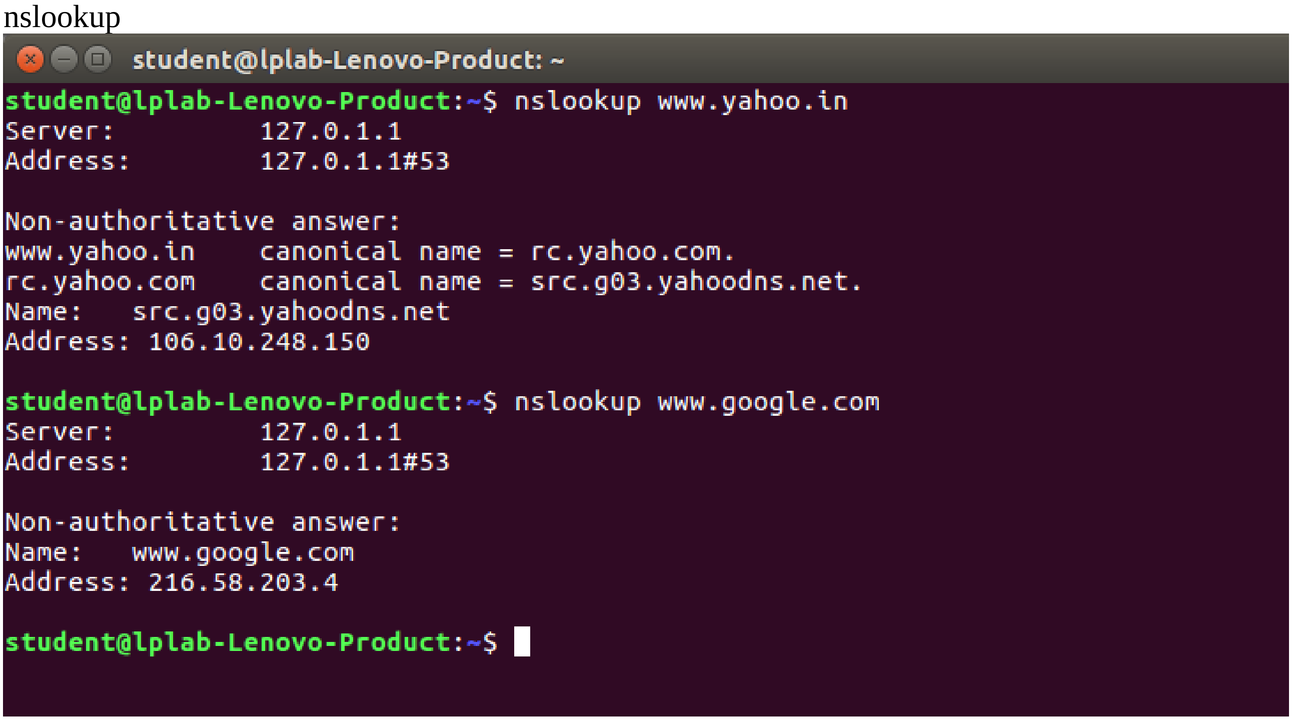
```
▸ Frame 165: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
▸ Ethernet II, Src: HewlettP_e7:16:ac (78:e7:d1:e7:16:ac), Dst: Micro-St_27:73:8d (8c:89:a5:27:73:8d)
▸ Internet Protocol Version 4, Src: 172.16.57.152, Dst: 172.16.57.40
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 44520, Seq: 1, Ack: 1, Len: 60
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0030  00 e3 a4 32 00 00 01 01  08 0a 66 04 f1 f8 00 2e   ···2···· ··f·····.
0040  57 52 32 32 30 20 57 65  6c 63 6f 6d 65 20 74 6f   WR220 We lcome to
0050  20 44 45 50 41 52 54 4d  45 4e 54 20 4f 46 20 43    DEPARTM ENT OF C
0060  53 45 2c 20 4d 49 54 20  4d 41 4e 49 50 41 4c 20   SE, MIT  MANIPAL 
0070  46 54 50 20 73 65 72 76  69 63 65 2e 0d 0a         FTP serv ice.··
```

File Transfer Protocol (FTP) (ftp), 60 bytes   Packets: 248 · Displayed: 7 (2.8%) · Dropped: 0 (0.0%)   Profile: Default

Aditya Pradhan CSE D 180905350

Q3.7)
nslookup



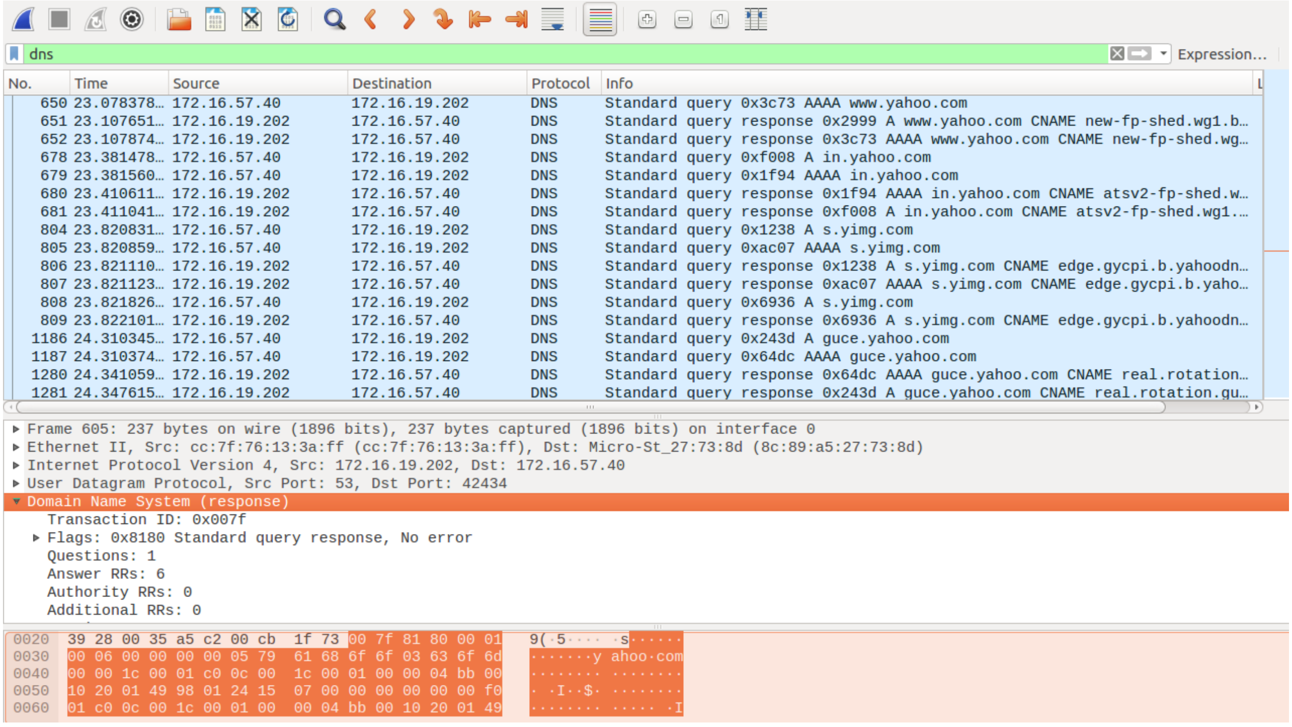
```
student@lplab-Lenovo-Product: ~
student@lplab-Lenovo-Product:~$ nslookup www.yahoo.in
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.yahoo.in    canonical name = rc.yahoo.com.
rc.yahoo.com    canonical name = src.g03.yahoodns.net.
Name:   src.g03.yahoodns.net
Address: 106.10.248.150

student@lplab-Lenovo-Product:~$ nslookup www.google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.203.4

student@lplab-Lenovo-Product:~$ 
```



```
dns

No.  Time          Source         Destination    Protocol Info
 650 23.078378…    172.16.57.40   172.16.19.202  DNS      Standard query 0x3c73 AAAA www.yahoo.com
 651 23.107651…    172.16.19.202  172.16.57.40   DNS      Standard query response 0x2999 A www.yahoo.com CNAME new-fp-shed.wg1.b…
 652 23.107874…    172.16.19.202  172.16.57.40   DNS      Standard query response 0x3c73 AAAA www.yahoo.com CNAME new-fp-shed.wg…
 678 23.381478…    172.16.57.40   172.16.19.202  DNS      Standard query 0xf008 A in.yahoo.com
 679 23.381560…    172.16.57.40   172.16.19.202  DNS      Standard query 0x1f94 AAAA in.yahoo.com
 680 23.410611…    172.16.19.202  172.16.57.40   DNS      Standard query response 0x1f94 AAAA in.yahoo.com CNAME atsv2-fp-shed.w…
 681 23.411041…    172.16.19.202  172.16.57.40   DNS      Standard query response 0xf008 A in.yahoo.com CNAME atsv2-fp-shed.wg1.…
 804 23.820831…    172.16.57.40   172.16.19.202  DNS      Standard query 0x1238 A s.yimg.com
 805 23.820859…    172.16.57.40   172.16.19.202  DNS      Standard query 0xac07 AAAA s.yimg.com
 806 23.821110…    172.16.19.202  172.16.57.40   DNS      Standard query response 0x1238 A s.yimg.com CNAME edge.gycpi.b.yahoodn…
 807 23.821123…    172.16.19.202  172.16.57.40   DNS      Standard query response 0xac07 AAAA s.yimg.com CNAME edge.gycpi.b.yaho…
 808 23.821826…    172.16.57.40   172.16.19.202  DNS      Standard query 0x6936 A s.yimg.com
 809 23.822101…    172.16.19.202  172.16.57.40   DNS      Standard query response 0x6936 A s.yimg.com CNAME edge.gycpi.b.yahoodn…
1186 24.310345…    172.16.57.40   172.16.19.202  DNS      Standard query 0x243d A guce.yahoo.com
1187 24.310374…    172.16.57.40   172.16.19.202  DNS      Standard query 0x64dc AAAA guce.yahoo.com
1280 24.341059…    172.16.19.202  172.16.57.40   DNS      Standard query response 0x64dc AAAA guce.yahoo.com CNAME real.rotation…
1281 24.347615…    172.16.19.202  172.16.57.40   DNS      Standard query response 0x243d A guce.yahoo.com CNAME real.rotation.gu…

▸ Frame 605: 237 bytes on wire (1896 bits), 237 bytes captured (1896 bits) on interface 0
▸ Ethernet II, Src: cc:7f:76:13:3a:ff (cc:7f:76:13:3a:ff), Dst: Micro-St_27:73:8d (8c:89:a5:27:73:8d)
▸ Internet Protocol Version 4, Src: 172.16.19.202, Dst: 172.16.57.40
▸ User Datagram Protocol, Src Port: 53, Dst Port: 42434
▾ Domain Name System (response)
    Transaction ID: 0x007f
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0

0020  39 28 00 35 a5 c2 00 cb  1f 73 00 7f 81 80 00 01   9(·5····  ·s······
0030  00 06 00 00 00 00 05 79  61 68 6f 6f 03 63 6f 6d   ·······y ahoo·com
0040  00 00 1c 00 01 c0 0c 00  1c 00 01 00 00 04 bb 00   ········ ········
0050  10 20 01 49 98 01 24 15  07 00 00 00 00 00 00 f0   · ·I··$· ········
0060  01 c0 0c 00 1c 00 01 00  00 04 bb 00 10 20 01 49   ········ ····· ·I
```

My web browser sends a DNS query to the server. It uses the Ipv4 protocol to do this.