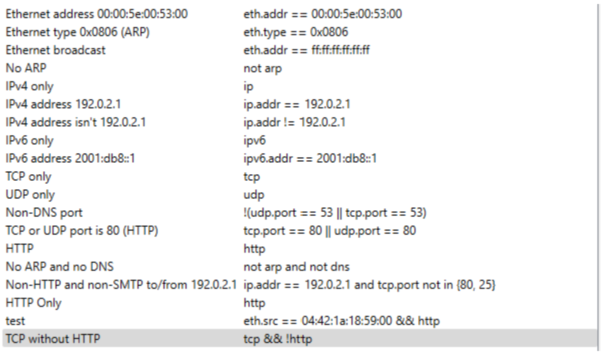
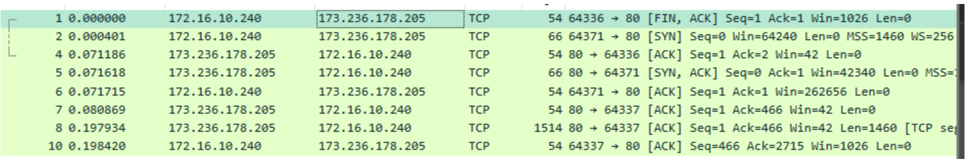
Question 1, part A



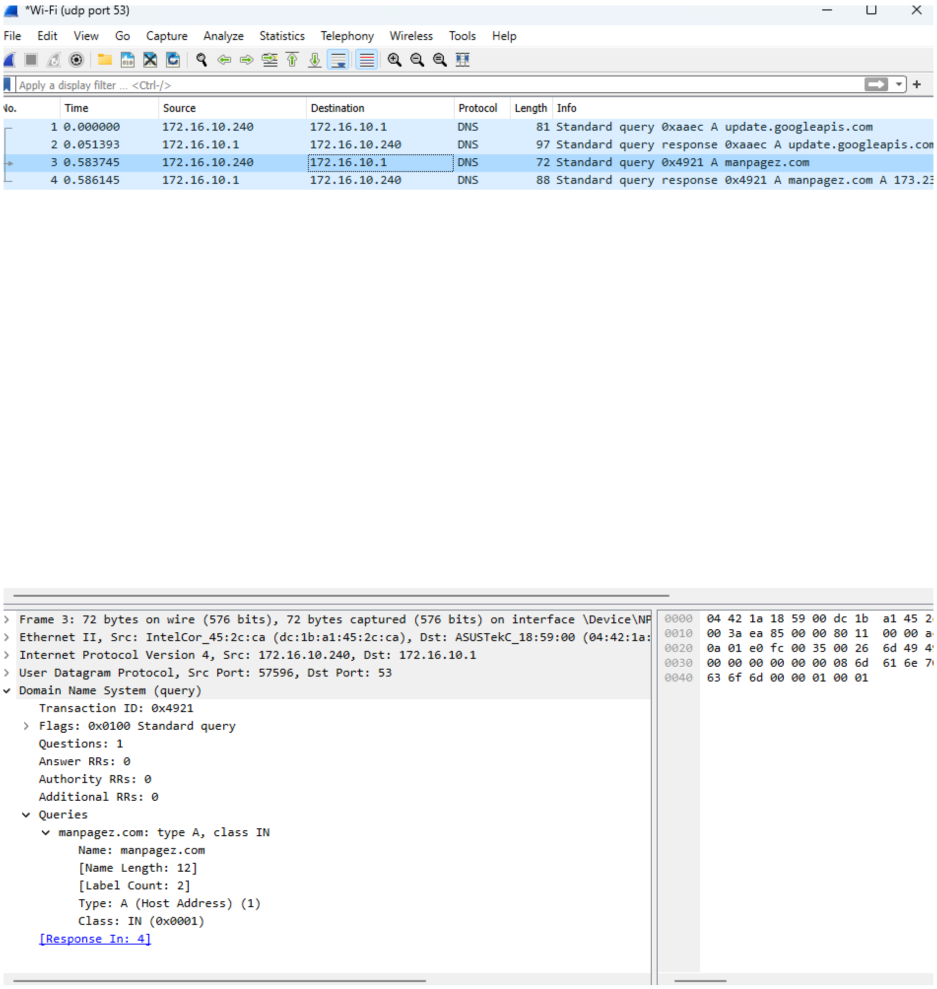
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1	ip.addr != 192.0.2.1
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS port	!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
HTTP	http
No ARP and no DNS	not arp and not dns
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and tcp.port not in {80, 25}
HTTP Only	http
test	eth.src == 04:42:1a:18:59:00 && http
TCP without HTTP	tcp && !http

Question 1, part B



```
 1 0.000000   172.16.10.240    173.236.178.205  TCP      54 64336 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
 2 0.000401   172.16.10.240    173.236.178.205  TCP      66 64371 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
 4 0.071186   173.236.178.205  172.16.10.240    TCP      54 80 → 64336 [ACK] Seq=1 Ack=2 Win=42 Len=0
 5 0.071618   173.236.178.205  172.16.10.240    TCP      66 80 → 64371 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=
 6 0.071715   172.16.10.240    173.236.178.205  TCP      54 64371 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
 7 0.080869   173.236.178.205  172.16.10.240    TCP      54 80 → 64337 [ACK] Seq=1 Ack=466 Win=42 Len=0
 8 0.197934   173.236.178.205  172.16.10.240    TCP    1514 80 → 64337 [ACK] Seq=1 Ack=466 Win=42 Len=1460 [TCP se
10 0.198420   172.16.10.240    173.236.178.205  TCP      54 64337 → 80 [ACK] Seq=466 Ack=2715 Win=1026 Len=0
```

Question 2

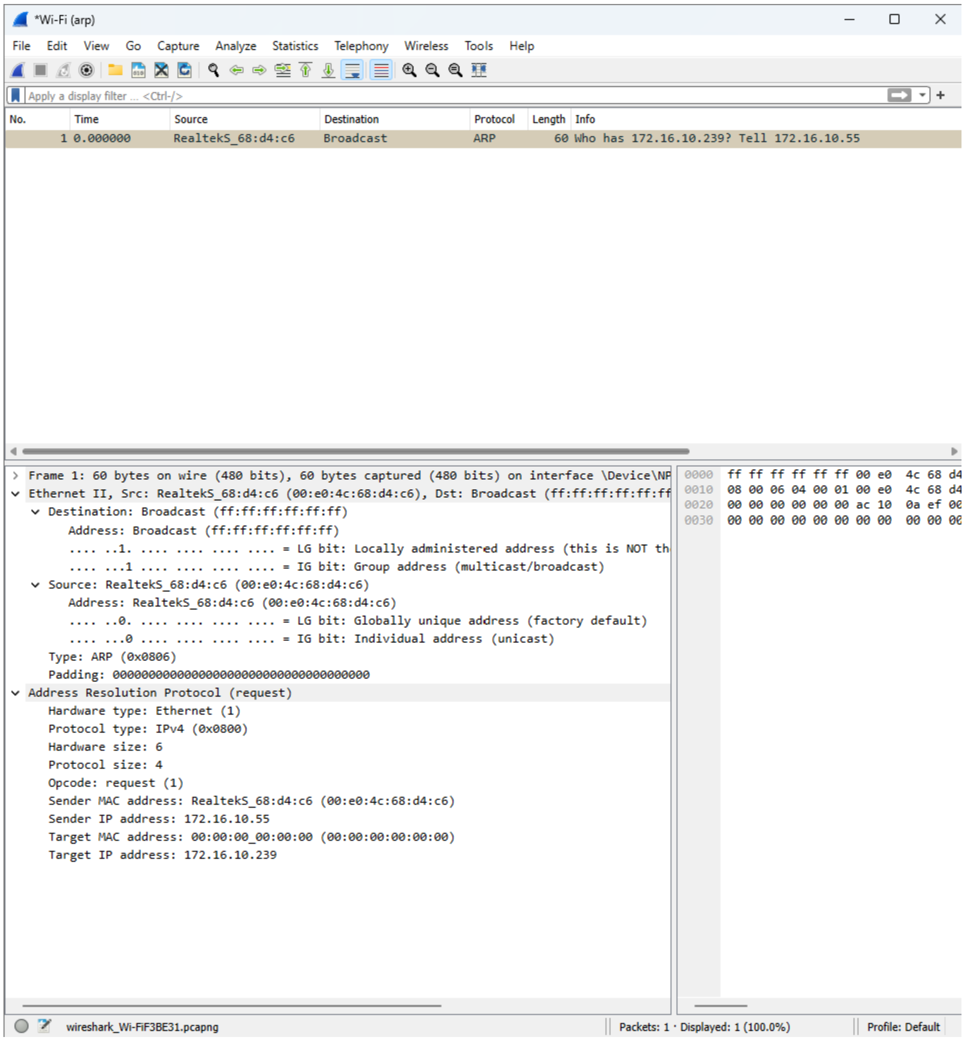


```
No.   Time       Source          Destination     Protocol  Length Info
    1 0.000000   172.16.10.240   172.16.10.1     DNS       81 Standard query 0xaaec A update.googleapis.com
    2 0.051393   172.16.10.1     172.16.10.240   DNS       97 Standard query response 0xaaec A update.googleapis.com
    3 0.583745   172.16.10.240   172.16.10.1     DNS       72 Standard query 0x4921 A manpagez.com
    4 0.586145   172.16.10.1     172.16.10.240   DNS       88 Standard query response 0x4921 A manpagez.com A 173.23
```

```
> Frame 3: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NP
> Ethernet II, Src: IntelCor_45:2c:ca (dc:1b:a1:45:2c:ca), Dst: ASUSTekC_18:59:00 (04:42:1a:
> Internet Protocol Version 4, Src: 172.16.10.240, Dst: 172.16.10.1
> User Datagram Protocol, Src Port: 57596, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x4921
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v manpagez.com: type A, class IN
        Name: manpagez.com
        [Name Length: 12]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 4]
```

```
0000  04 42 1a 18 59 00 dc 1b  a1 45 2
0010  00 3a ea 85 00 00 80 11  00 00 a
0020  0a 01 e0 fc 00 35 00 26  6d 49 4
0030  00 00 00 00 00 00 08 6d  61 6e 7
0040  63 6f 6d 00 00 01 00 01
```

Question 3



*Wi-Fi (arp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source              Destination   Protocol  Length  Info
    1 0.000000    RealtekS_68:d4:c6   Broadcast     ARP           60  Who has 172.16.10.239? Tell 172.16.10.55
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NP
v Ethernet II, Src: RealtekS_68:d4:c6 (00:e0:4c:68:d4:c6), Dst: Broadcast (ff:ff:ff:ff:ff:ff
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT th
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: RealtekS_68:d4:c6 (00:e0:4c:68:d4:c6)
      Address: RealtekS_68:d4:c6 (00:e0:4c:68:d4:c6)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: RealtekS_68:d4:c6 (00:e0:4c:68:d4:c6)
    Sender IP address: 172.16.10.55
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.10.239
```

```
0000  ff ff ff ff ff ff 00 e0  4c 68 d4
0010  08 00 06 04 00 01 00 e0  4c 68 d4
0020  00 00 00 00 00 00 ac 10  0a ef 00
0030  00 00 00 00 00 00 00 00  00 00 00
```

wireshark_Wi-FiF3BE31.pcapng | Packets: 1 · Displayed: 1 (100.0%) | Profile: Default