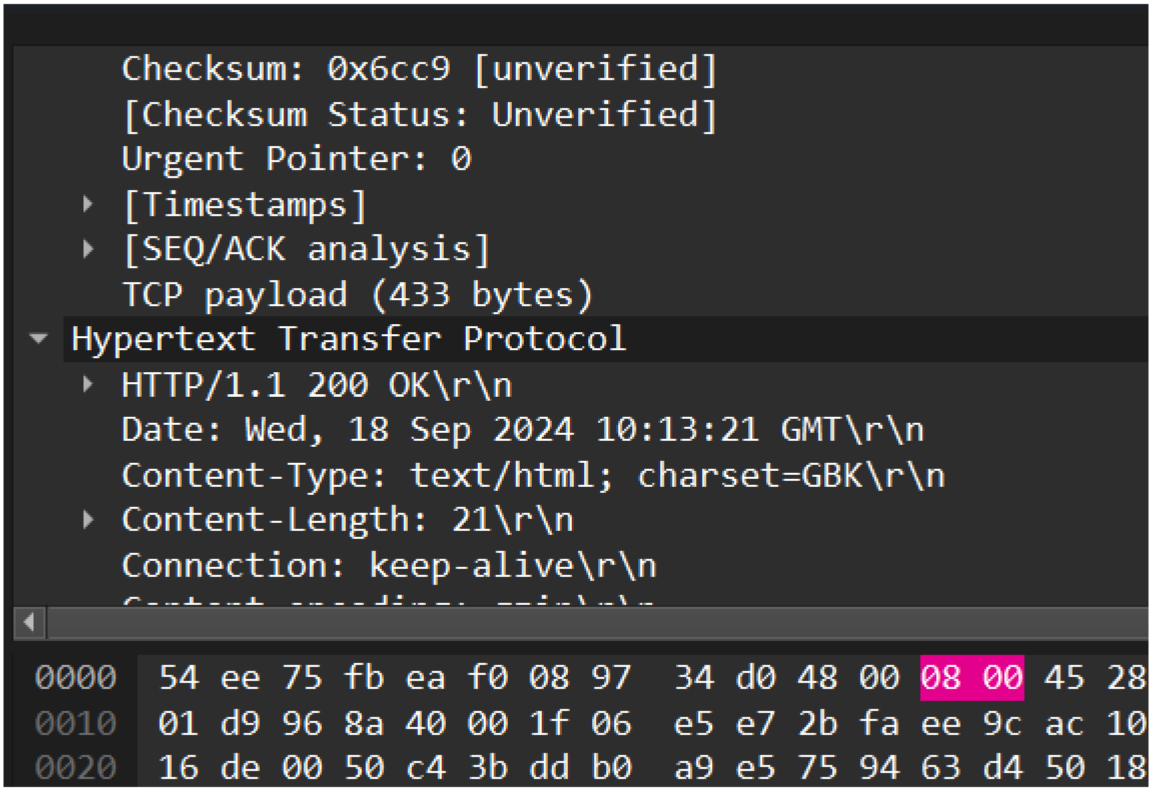
CNET – LAB 5

Maria Naeem ~ i220812 ~ SECTION K

Question 1

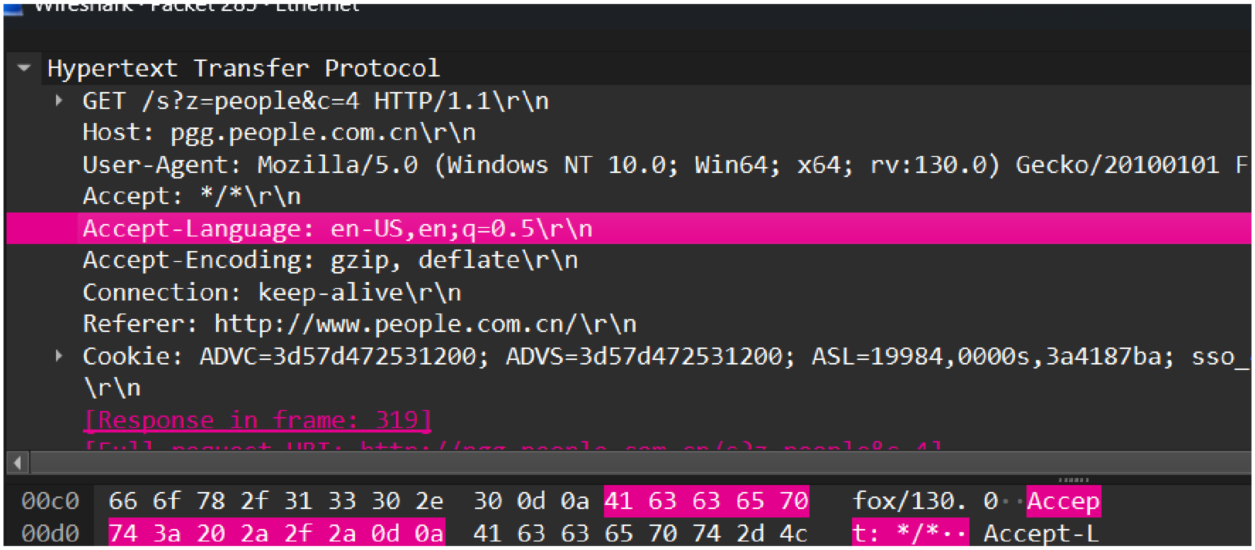


```
      Checksum: 0x6cc9 [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
    ▸ [Timestamps]
    ▸ [SEQ/ACK analysis]
      TCP payload (433 bytes)
  ▾ Hypertext Transfer Protocol
    ▸ HTTP/1.1 200 OK\r\n
      Date: Wed, 18 Sep 2024 10:13:21 GMT\r\n
      Content-Type: text/html; charset=GBK\r\n
    ▸ Content-Length: 21\r\n
      Connection: keep-alive\r\n
      Content-encoding: gzip\r\n

0000  54 ee 75 fb ea f0 08 97  34 d0 48 00 08 00 45 28
0010  01 d9 96 8a 40 00 1f 06  e5 e7 2b fa ee 9c ac 10
0020  16 de 00 50 c4 3b dd b0  a9 e5 75 94 63 d4 50 18
```

http 1.1 as shown above

Question 2

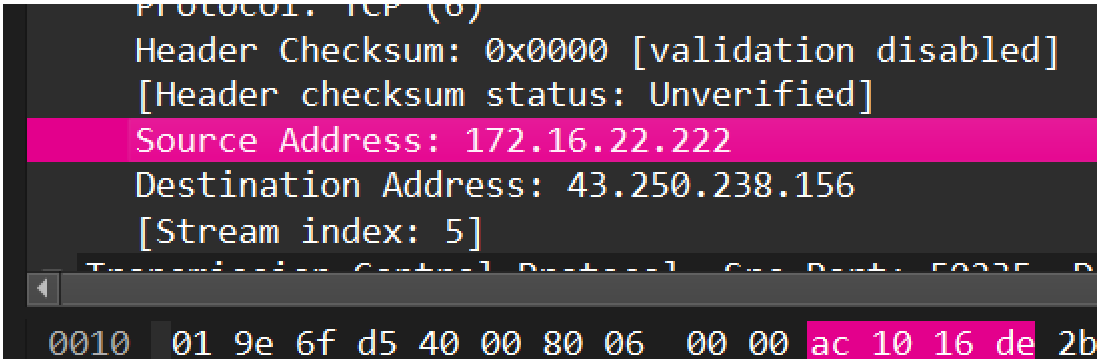


```
Wireshark · Packet 285 · Ethernet

Hypertext Transfer Protocol
  GET /s?z=people&c=4 HTTP/1.1\r\n
  Host: pgg.people.com.cn\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 F
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Referer: http://www.people.com.cn/\r\n
  Cookie: ADVC=3d57d472531200; ADVS=3d57d472531200; ASL=19984,0000s,3a4187ba; sso_
  \r\n
  [Response in frame: 319]
  [Full request URI: http://pgg.people.com.cn/s?z=people&c=4]

00c0  66 6f 78 2f 31 33 30 2e  30 0d 0a 41 63 63 65 70   fox/130. 0··Accep
00d0  74 3a 20 2a 2f 2a 0d 0a  41 63 63 65 70 74 2d 4c   t: */*·· Accept-L
```

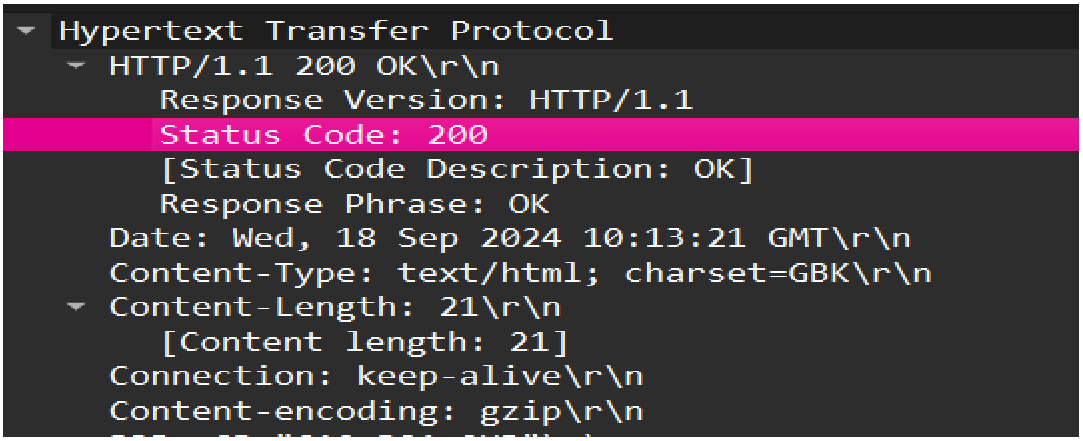
Question 3



```
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.22.222
    Destination Address: 43.250.238.156
    [Stream index: 5]
Transmission Control Protocol, Src Port: 50235, D

0010  01 9e 6f d5 40 00 80 06  00 00 ac 10 16 de 2b
```

Question 4

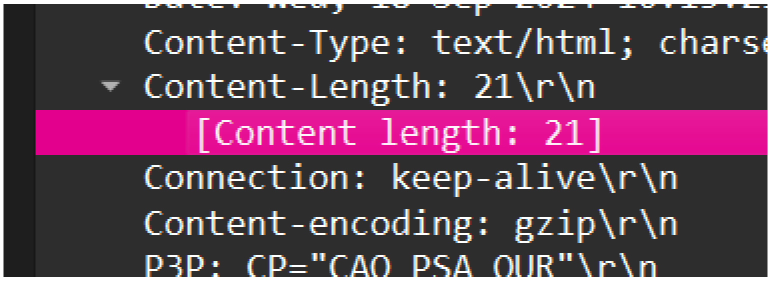


```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Wed, 18 Sep 2024 10:13:21 GMT\r\n
  Content-Type: text/html; charset=GBK\r\n
  Content-Length: 21\r\n
    [Content length: 21]
  Connection: keep-alive\r\n
  Content-encoding: gzip\r\n
```

Question 5

NOT FOUND

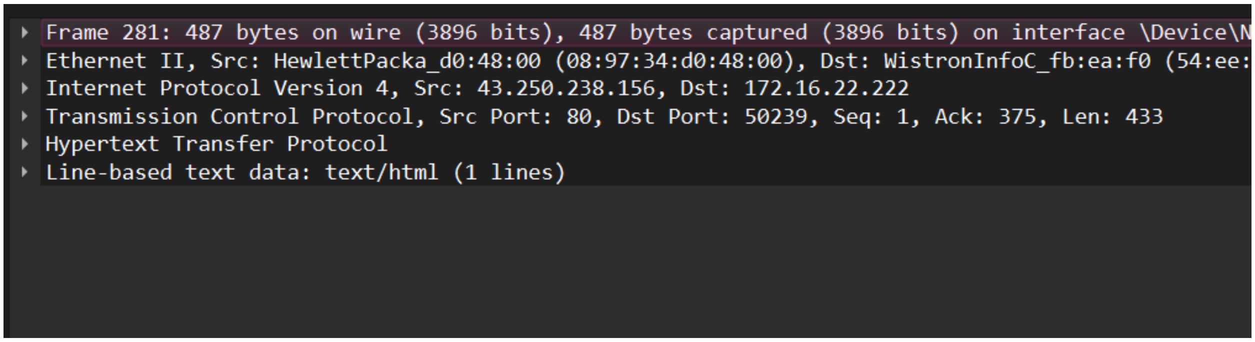
Question 6



```
    Content-Type: text/html; charse
  ▾ Content-Length: 21\r\n
        [Content length: 21]
    Connection: keep-alive\r\n
    Content-encoding: gzip\r\n
    P3P: CP="CAO PSA OUR"\r\n
```

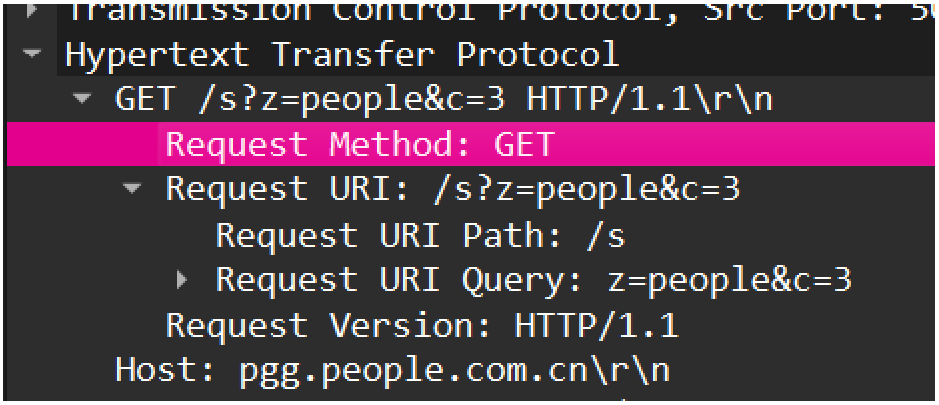
Question 7

None Found, all headers available



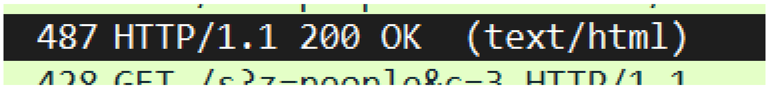
```
▸ Frame 281: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface \Device\N
▸ Ethernet II, Src: HewlettPacka_d0:48:00 (08:97:34:d0:48:00), Dst: WistronInfoC_fb:ea:f0 (54:ee:
▸ Internet Protocol Version 4, Src: 43.250.238.156, Dst: 172.16.22.222
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 50239, Seq: 1, Ack: 375, Len: 433
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (1 lines)
```

Question 8



```
▸ Transmission Control Protocol, Src Port: 5
▾ Hypertext Transfer Protocol
  ▾ GET /s?z=people&c=3 HTTP/1.1\r\n
        Request Method: GET
      ▾ Request URI: /s?z=people&c=3
            Request URI Path: /s
          ▸ Request URI Query: z=people&c=3
        Request Version: HTTP/1.1
    Host: pgg.people.com.cn\r\n
```

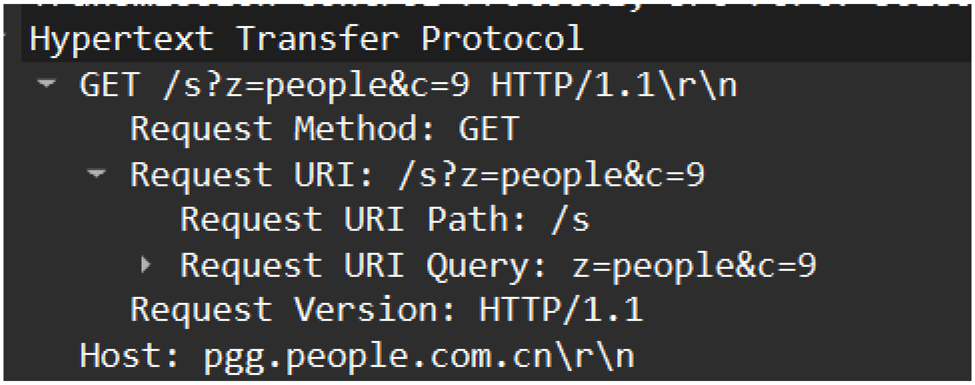
Question 9



```
487 HTTP/1.1 200 OK  (text/html)
428 GET /s?z=people&c=3 HTTP/1.1
```

200 OK

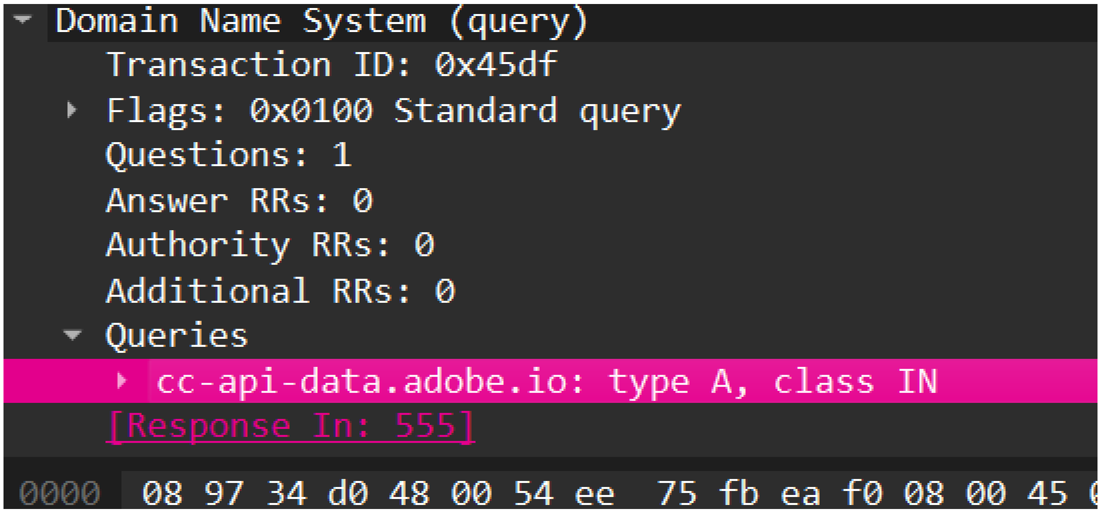
Question 10



```
Hypertext Transfer Protocol
  GET /s?z=people&c=9 HTTP/1.1\r\n
     Request Method: GET
   Request URI: /s?z=people&c=9
        Request URI Path: /s
      Request URI Query: z=people&c=9
     Request Version: HTTP/1.1
  Host: pgg.people.com.cn\r\n
```

In the 2nd GET request, there was nothing extra added in the GET request

Question 11

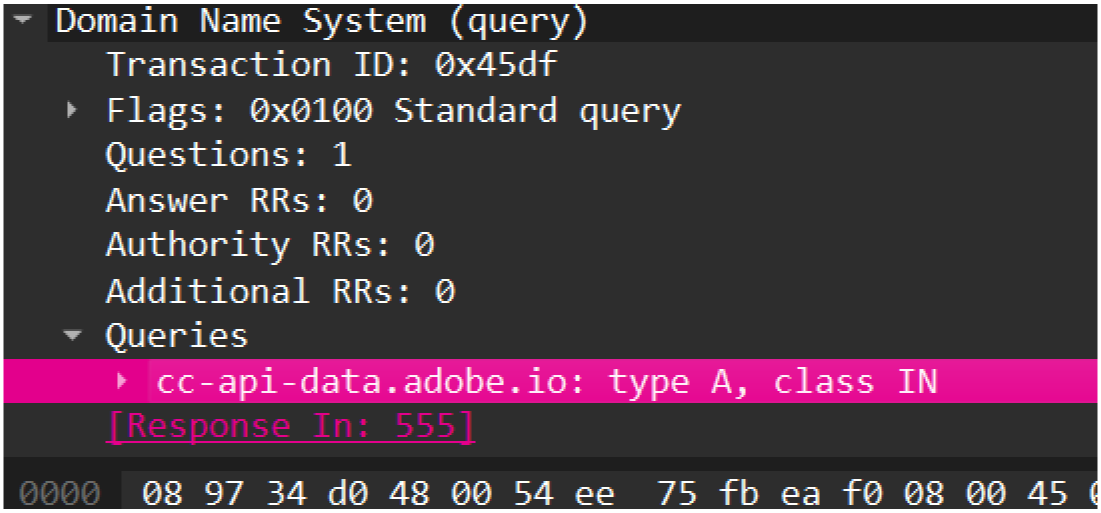


```
Domain Name System (query)
     Transaction ID: 0x45df
   Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   Queries
       cc-api-data.adobe.io: type A, class IN
     [Response In: 555]

0000  08 97 34 d0 48 00 54 ee  75 fb ea f0 08 00 45
```

TYPE : A

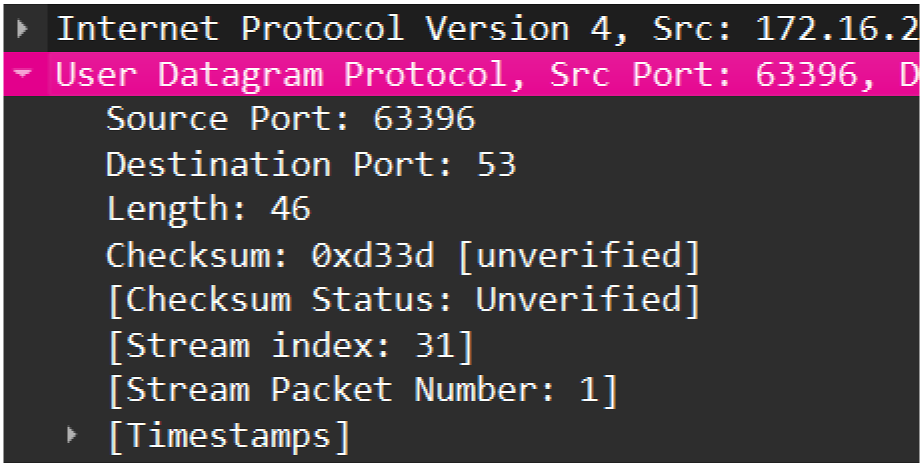
Question 12



```
Domain Name System (query)
    Transaction ID: 0x45df
  Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
      cc-api-data.adobe.io: type A, class IN
    [Response In: 555]
0000  08 97 34 d0 48 00 54 ee  75 fb ea f0 08 00 45
```

cc-api-data.adobe.io

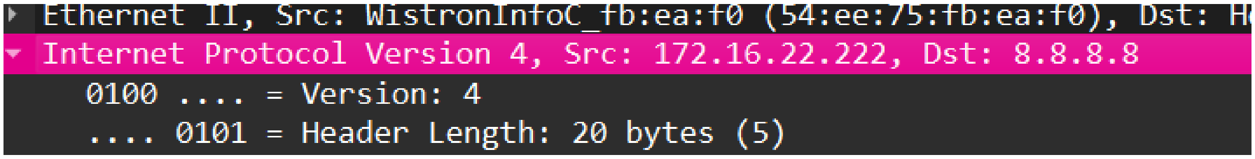
Question 13



```
Internet Protocol Version 4, Src: 172.16.2
User Datagram Protocol, Src Port: 63396, D
    Source Port: 63396
    Destination Port: 53
    Length: 46
    Checksum: 0xd33d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 31]
    [Stream Packet Number: 1]
  [Timestamps]
```

UDP is being used

Question 14

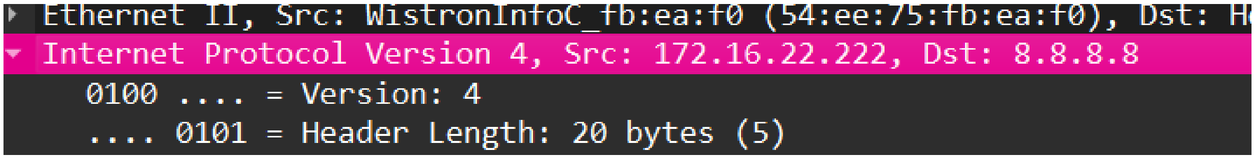


```
Ethernet II, Src: WistronInfoC_fb:ea:f0 (54:ee:75:fb:ea:f0), Dst: H
Internet Protocol Version 4, Src: 172.16.22.222, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

172.16.22.222

Question 15

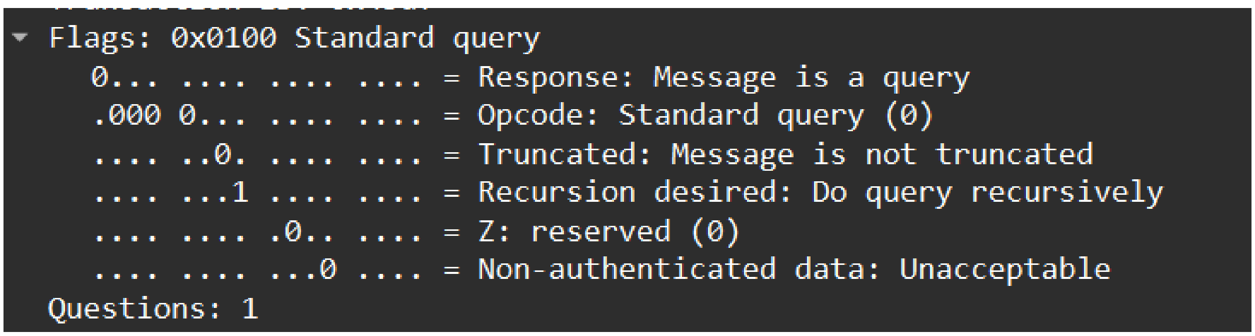
Yes



```
▸ Ethernet II, Src: WistronInfoC_fb:ea:f0 (54:ee:75:fb:ea:f0), Dst: H
▾ Internet Protocol Version 4, Src: 172.16.22.222, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
```

Question 16

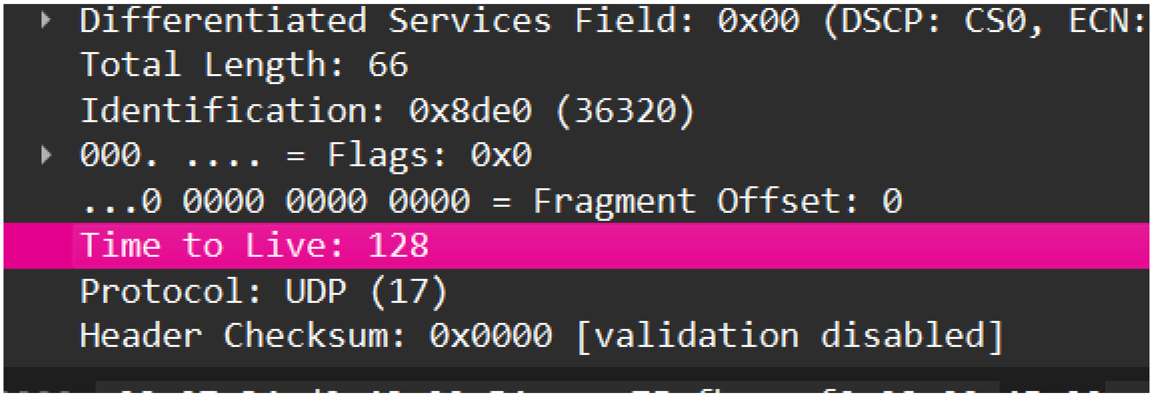
Yes



```
▾ 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
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
  Questions: 1
```

Truncated : Message is not Truncated

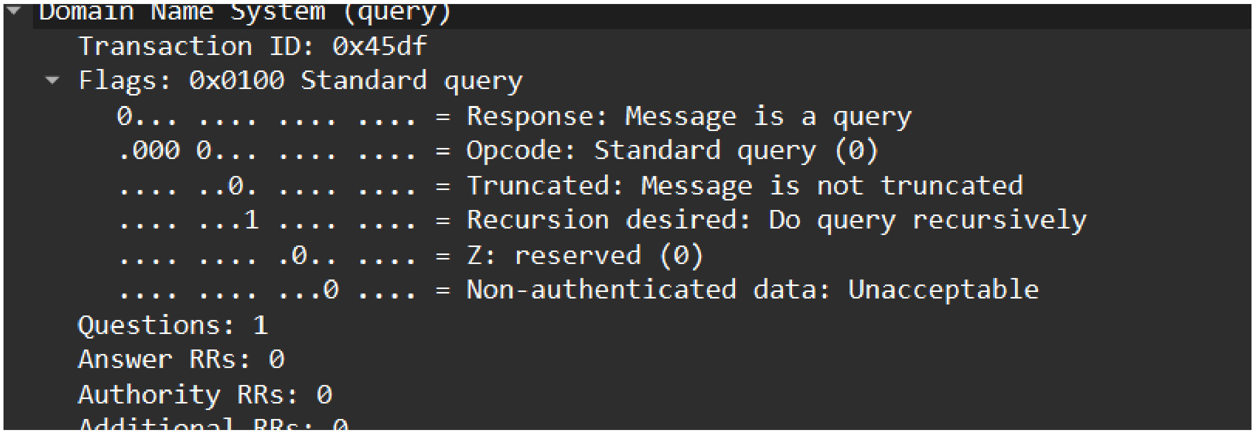
Question 17



```
▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN:
  Total Length: 66
  Identification: 0x8de0 (36320)
▸ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x0000 [validation disabled]
```

128

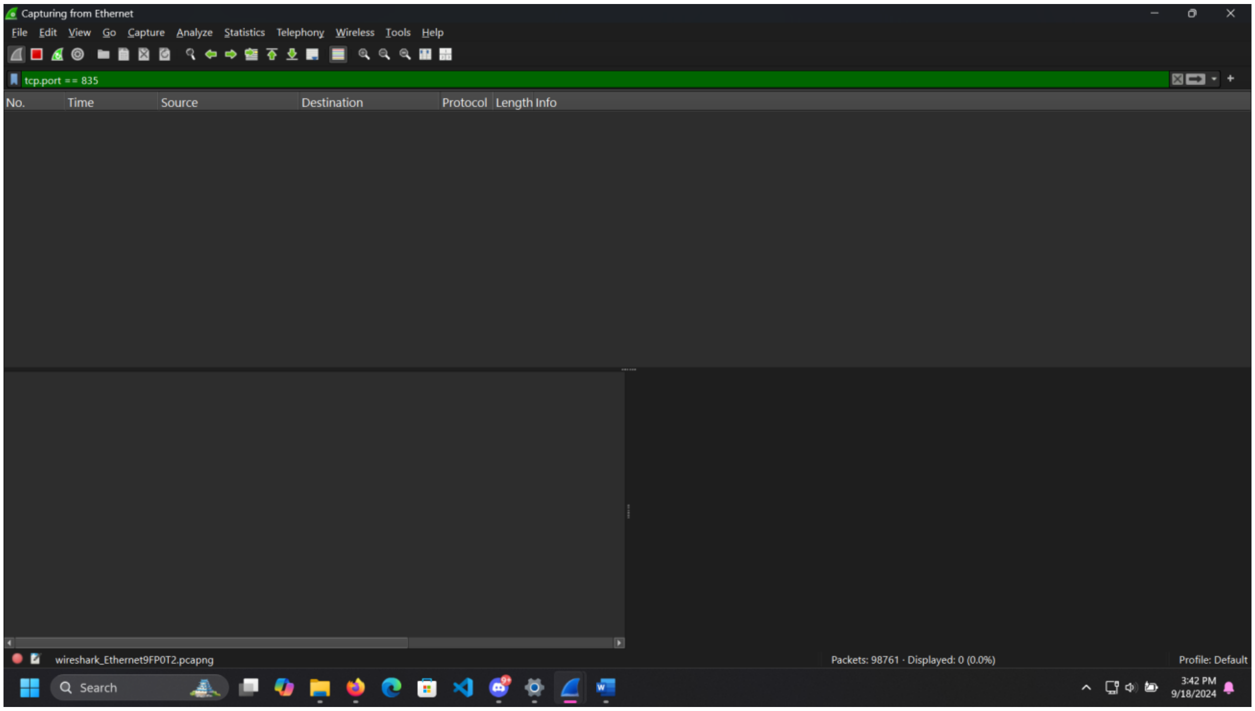
Question 18



```
▾ Domain Name System (query)
    Transaction ID: 0x45df
  ▾ 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
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

NO

Question 19



Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

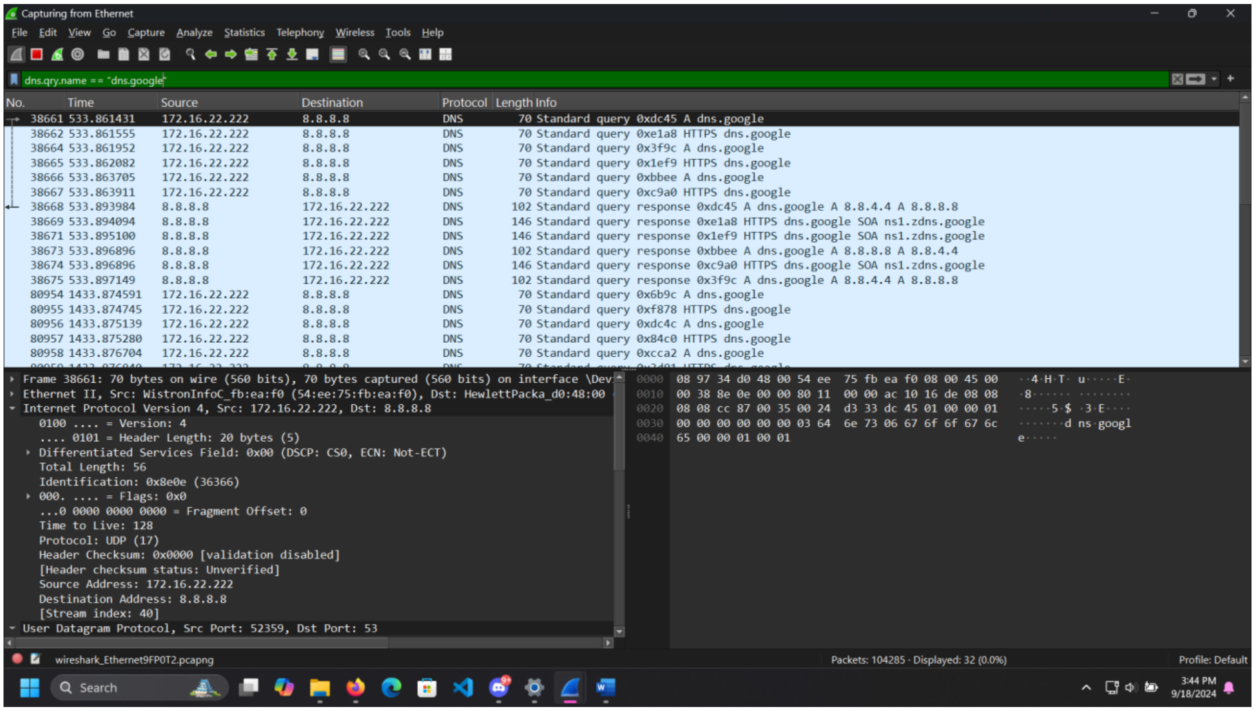
```
tcp.port == 835
```

No.	Time	Source	Destination	Protocol	Length	Info

wireshark_Ethernet9FP0T2.pcapng   Packets: 98761 · Displayed: 0 (0.0%)   Profile: Default

None found

Question 20


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Search

dns.qry.name == "dns.google"

```
No.   Time         Source         Destination    Protocol Length Info
38661 533.861431   172.16.22.222  8.8.8.8        DNS       70 Standard query 0xdc45 A dns.google
38662 533.861555   172.16.22.222  8.8.8.8        DNS       70 Standard query 0xe1a8 HTTPS dns.google
38664 533.861952   172.16.22.222  8.8.8.8        DNS       70 Standard query 0x3f9c A dns.google
38665 533.862082   172.16.22.222  8.8.8.8        DNS       70 Standard query 0x1ef9 HTTPS dns.google
38666 533.863705   172.16.22.222  8.8.8.8        DNS       70 Standard query 0xbbee A dns.google
38667 533.863911   172.16.22.222  8.8.8.8        DNS       70 Standard query 0xc9a0 HTTPS dns.google
38668 533.893984   8.8.8.8        172.16.22.222  DNS      102 Standard query response 0xdc45 A dns.google A 8.8.4.4 A 8.8.8.8
38669 533.894094   8.8.8.8        172.16.22.222  DNS      146 Standard query response 0xe1a8 HTTPS dns.google SOA ns1.zdns.google
38671 533.895100   8.8.8.8        172.16.22.222  DNS      146 Standard query response 0x1ef9 HTTPS dns.google SOA ns1.zdns.google
38673 533.896896   8.8.8.8        172.16.22.222  DNS      102 Standard query response 0xbbee A dns.google A 8.8.8.8 A 8.8.4.4
38674 533.896896   8.8.8.8        172.16.22.222  DNS      146 Standard query response 0xc9a0 HTTPS dns.google SOA ns1.zdns.google
38675 533.897149   8.8.8.8        172.16.22.222  DNS      102 Standard query response 0x3f9c A dns.google A 8.8.4.4 A 8.8.8.8
80954 1433.874591  172.16.22.222  8.8.8.8        DNS       70 Standard query 0x6b9c A dns.google
80955 1433.874745  172.16.22.222  8.8.8.8        DNS       70 Standard query 0xf878 HTTPS dns.google
80956 1433.875139  172.16.22.222  8.8.8.8        DNS       70 Standard query 0xdc4c A dns.google
80957 1433.875280  172.16.22.222  8.8.8.8        DNS       70 Standard query 0x84c0 HTTPS dns.google
80958 1433.876704  172.16.22.222  8.8.8.8        DNS       70 Standard query 0xcca2 A dns.google
```

```
Frame 38661: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Dev
Ethernet II, Src: WistronInfoC_fb:ea:f0 (54:ee:75:fb:ea:f0), Dst: HewlettPacka_d0:48:00
Internet Protocol Version 4, Src: 172.16.22.222, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x8e0e (36366)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.22.222
    Destination Address: 8.8.8.8
    [Stream index: 40]
User Datagram Protocol, Src Port: 52359, Dst Port: 53
```

```
0000  08 97 34 d0 48 00 54 ee  75 fb ea f0 08 00 45 00   ··4·H·T· u·····E·
0010  00 38 8e 0e 00 00 80 11  00 00 ac 10 16 de 08 08   ·8······ ········
0020  08 08 cc 87 00 35 00 24  d3 33 dc 45 01 00 00 01   ·····5·$ ·3·E····
0030  00 00 00 00 00 00 03 64  6e 73 06 67 6f 6f 67 6c   ·······d ns·googl
0040  65 00 00 01 00 01                                  e·····
```

wireshark_Ethernet9FP0T2.pcapng

Packets: 104285 · Displayed: 32 (0.0%)

Profile: Default

3:44 PM
9/18/2024