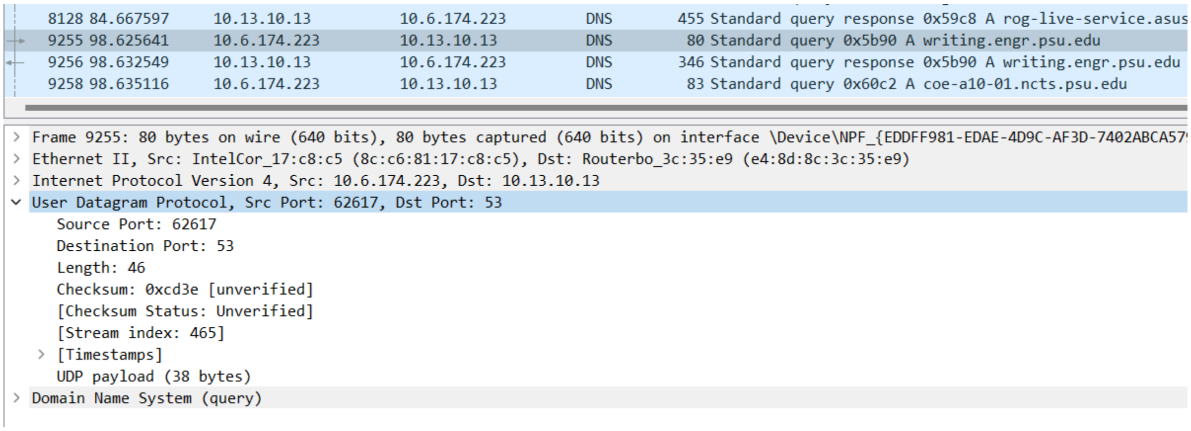
Name : Ramzy Izza Wardhana
NIM : 21/472698/PA/20322
Class : IUP CS B – Lab SKJ

Activity 5.2 – Lab SKJ

5. Locate the first DNS query message resolving the name writing.engr.psu.edu. What is the packet number3 in the trace for the DNS query message? Is this query message sent over UDP or TCP?

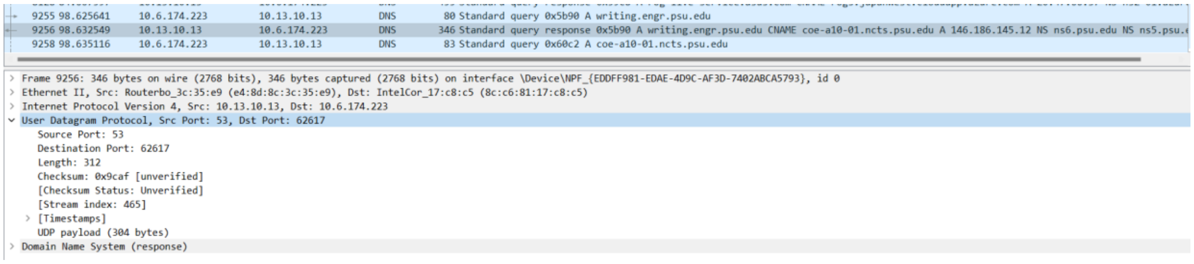


```
8128 84.667597   10.13.10.13     10.6.174.223    DNS   455 Standard query response 0x59c8 A rog-live-service.asus
9255 98.625641   10.6.174.223    10.13.10.13     DNS    80 Standard query 0x5b90 A writing.engr.psu.edu
9256 98.632549   10.13.10.13     10.6.174.223    DNS   346 Standard query response 0x5b90 A writing.engr.psu.edu
9258 98.635116   10.6.174.223    10.13.10.13     DNS    83 Standard query 0x60c2 A coe-a10-01.ncts.psu.edu

> Frame 9255: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{EDDFF981-EDAE-4D9C-AF3D-7402ABCA57
> Ethernet II, Src: IntelCor_17:c8:c5 (8c:c6:81:17:c8:c5), Dst: Routerbo_3c:35:e9 (e4:8d:8c:3c:35:e9)
> Internet Protocol Version 4, Src: 10.6.174.223, Dst: 10.13.10.13
v User Datagram Protocol, Src Port: 62617, Dst Port: 53
    Source Port: 62617
    Destination Port: 53
    Length: 46
    Checksum: 0xcd3e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 465]
  > [Timestamps]
    UDP payload (38 bytes)
> Domain Name System (query)
```

The packet number : 9255
Query message sent over UDP, proven by the screenshot above (highlighted in blue)

6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?



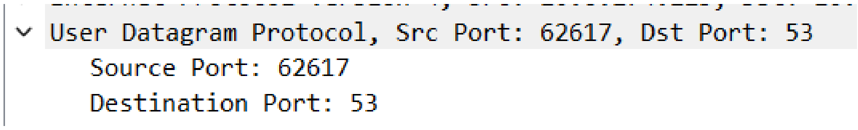
```
9255 98.625641   10.6.174.223    10.13.10.13     DNS    80 Standard query 0x5b90 A writing.engr.psu.edu
9256 98.632549   10.13.10.13     10.6.174.223    DNS   346 Standard query response 0x5b90 A writing.engr.psu.edu CNAME coe-a10-01.ncts.psu.edu A 146.186.145.12 NS ns6.psu.edu NS ns5.psu.
9258 98.635116   10.6.174.223    10.13.10.13     DNS    83 Standard query 0x60c2 A coe-a10-01.ncts.psu.edu

> Frame 9256: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface \Device\NPF_{EDDFF981-EDAE-4D9C-AF3D-7402ABCA5793}, id 0
> Ethernet II, Src: Routerbo_3c:35:e9 (e4:8d:8c:3c:35:e9), Dst: IntelCor_17:c8:c5 (8c:c6:81:17:c8:c5)
> Internet Protocol Version 4, Src: 10.13.10.13, Dst: 10.6.174.223
v User Datagram Protocol, Src Port: 53, Dst Port: 62617
    Source Port: 53
    Destination Port: 62617
    Length: 312
    Checksum: 0x9caf [unverified]
    [Checksum Status: Unverified]
    [Stream index: 465]
  > [Timestamps]
    UDP payload (304 bytes)
> Domain Name System (response)
```

The Packet Number (Response) : 9256
Query message sent over UDP, proven b the screenshot above (highlighted in blue)

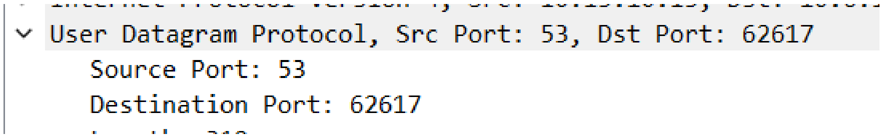
7. What is the destination port for the DNS query message? What is the source port of the DNS response message?

Destination Port of query message: 53



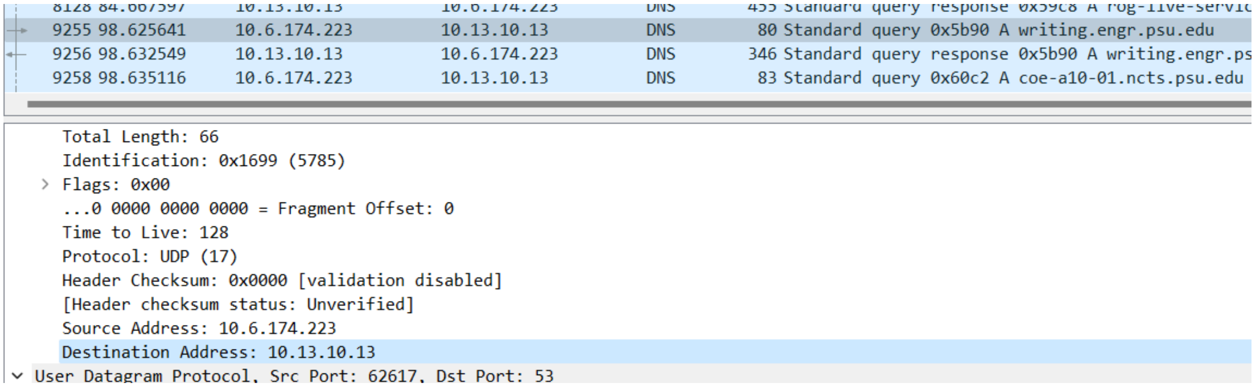
```
v User Datagram Protocol, Src Port: 62617, Dst Port: 53
    Source Port: 62617
    Destination Port: 53
```

Source Port of response message: 53



```
v User Datagram Protocol, Src Port: 53, Dst Port: 62617
    Source Port: 53
    Destination Port: 62617
```

8. To what IP address is the DNS query message sent?

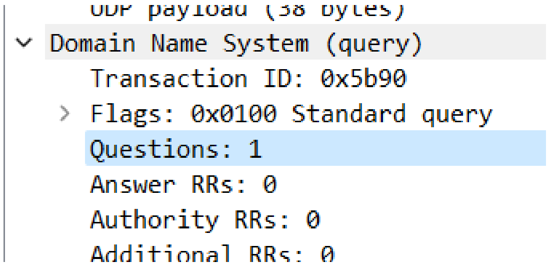


```
8128 84.667597   10.13.10.13    10.6.174.223   DNS   455 Standard query response 0x59c8 A rog-live-servic
9255 98.625641   10.6.174.223   10.13.10.13    DNS    80 Standard query 0x5b90 A writing.engr.psu.edu
9256 98.632549   10.13.10.13    10.6.174.223   DNS   346 Standard query response 0x5b90 A writing.engr.ps
9258 98.635116   10.6.174.223   10.13.10.13    DNS    83 Standard query 0x60c2 A coe-a10-01.ncts.psu.edu
```

```
    Total Length: 66
    Identification: 0x1699 (5785)
  > Flags: 0x00
    ...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: 10.6.174.223
    Destination Address: 10.13.10.13
v User Datagram Protocol, Src Port: 62617, Dst Port: 53
```

Destination IP Address: 10.13.10.13

9. Examine the DNS query message. How many "questions" does this DNS message contain? How many "answers" answers does it contain?

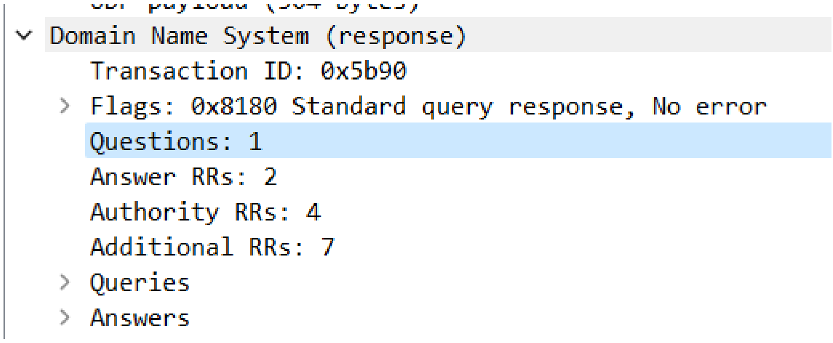


```
    UDP payload (38 bytes)
v Domain Name System (query)
    Transaction ID: 0x5b90
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

Question: 1

Answer: 0

10. Examine the DNS response message to the initial query message. How many "questions" does this DNS message contain? How many "answers" answers does it contain?



```
    UDP payload (304 bytes)
v Domain Name System (response)
    Transaction ID: 0x5b90
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 7
  > Queries
  > Answers
```

Question: 1

Answers: 2