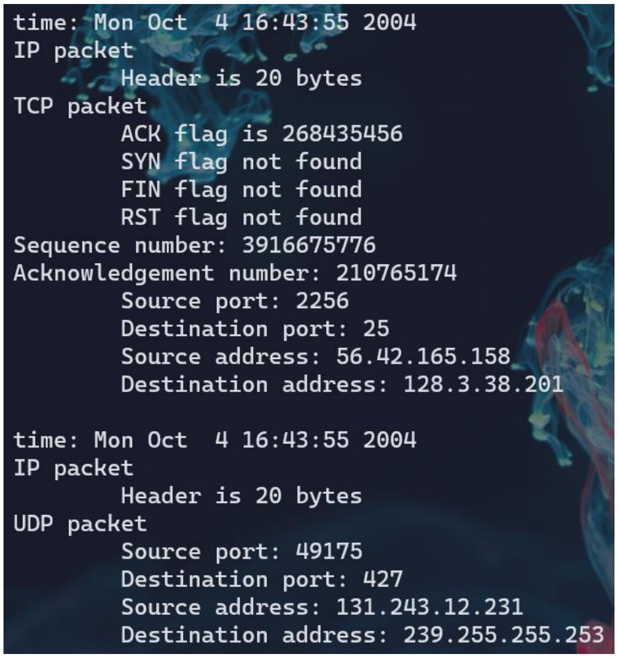
Assignment 3: Packet Sniffing

TCP & UDP Decode



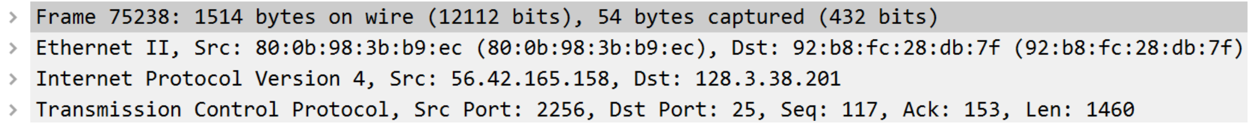
```
time: Mon Oct  4 16:43:55 2004
IP packet
        Header is 20 bytes
TCP packet
        ACK flag is 268435456
        SYN flag not found
        FIN flag not found
        RST flag not found
Sequence number: 3916675776
Acknowledgement number: 210765174
        Source port: 2256
        Destination port: 25
        Source address: 56.42.165.158
        Destination address: 128.3.38.201

time: Mon Oct  4 16:43:55 2004
IP packet
        Header is 20 bytes
UDP packet
        Source port: 49175
        Destination port: 427
        Source address: 131.243.12.231
        Destination address: 239.255.255.253
```

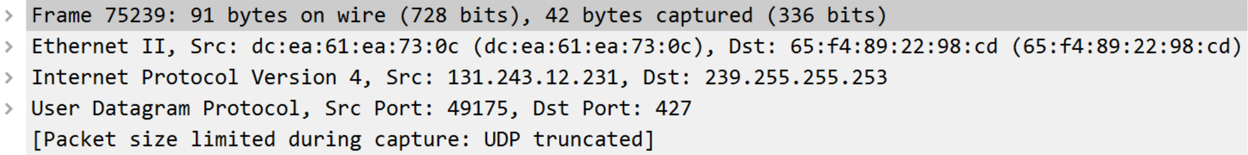
The TCP procedure is called on line 74 and the UDP procedure is called on line 104. Retrieve the TCP and UDP transactions from a payload. The payload consists of a packet and the size of the IP packet.

To decode TCP/UDP packets, retrieve the source and destination port numbers. For port numbers less than 1024, retrieve the service port via `getservbyport`. Afterwards, the source and destination addresses are displayed.

The rest of the code in `capture.c` is based on the code for lab 9. The only changes made in the code are in the `processIP` method. Similar to lab 9, the code would read from a file in order to decode packets. The Wireshark results, below, are as follows:



```
> Frame 75238: 1514 bytes on wire (12112 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: 80:0b:98:3b:b9:ec (80:0b:98:3b:b9:ec), Dst: 92:b8:fc:28:db:7f (92:b8:fc:28:db:7f)
> Internet Protocol Version 4, Src: 56.42.165.158, Dst: 128.3.38.201
> Transmission Control Protocol, Src Port: 2256, Dst Port: 25, Seq: 117, Ack: 153, Len: 1460
```



```
> Frame 75239: 91 bytes on wire (728 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: dc:ea:61:ea:73:0c (dc:ea:61:ea:73:0c), Dst: 65:f4:89:22:98:cd (65:f4:89:22:98:cd)
> Internet Protocol Version 4, Src: 131.243.12.231, Dst: 239.255.255.253
> User Datagram Protocol, Src Port: 49175, Dst Port: 427
  [Packet size limited during capture: UDP truncated]
```