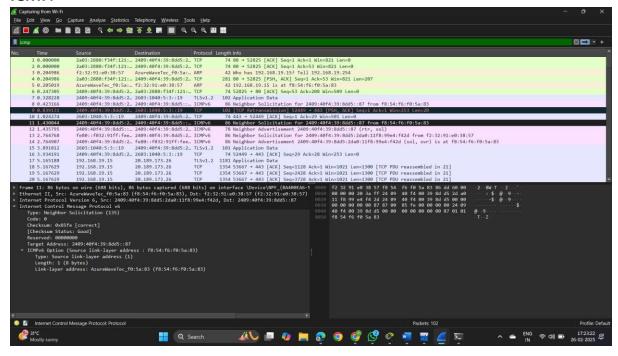
24.Network layer protocol header analysis using Wire shark – SMTP and ICMP.



SMTP

```
101 0.120645
                     192.168.186.197
                                          223.196.146.77
                                                               UDP
                                                                          81 62236 → 443 Len=39
   Source: AzureWaveTec_a4:43:01 (a8:41:f4:a4:43:01)
    Type: IPv4 (0x0800)
    [Stream index: 0]

    Internet Protocol Version 4, Src: 192.168.186.197, Dst: 216.239.38.223

    0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1195
    Identification: 0x19cd (6605)
   ▶ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 62
    Protocol: UDP (17)
    Header Checksum: 0xa338 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.186.197
    Destination Address: 216.239.38.223
    [Stream index: 0]
User Datagram Protocol, Src Port: 62604, Dst Port: 443
    Source Port: 62604
    Destination Port: 443
    Length: 1175
    Checksum: 0xe7dc [unverified]
    [Checksum Status: Unverified]
     [Stream index: 0]
    [Stream Packet Number: 3]
   [Timestamps]
    UDP payload (1167 bytes)
▼ Data (1167 bytes)
    Data [...]: 45f48b9ec6180490719e858ebad1ae4f96227fd4808946eecf178cb9b7c4d4b7d0f6a5a5b1a9e9c6af67ae7a7
     [Length: 1167]
```