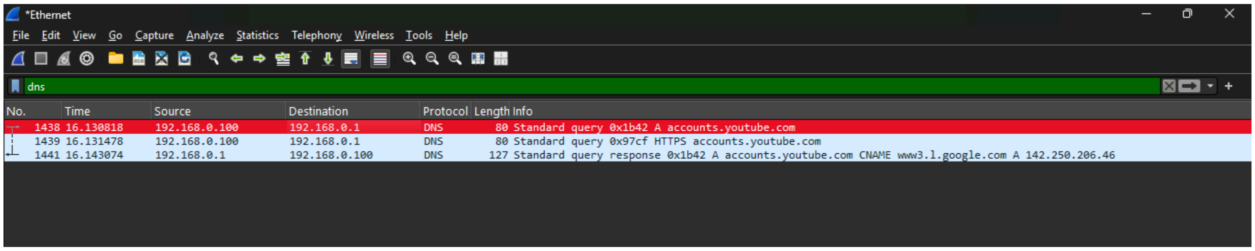
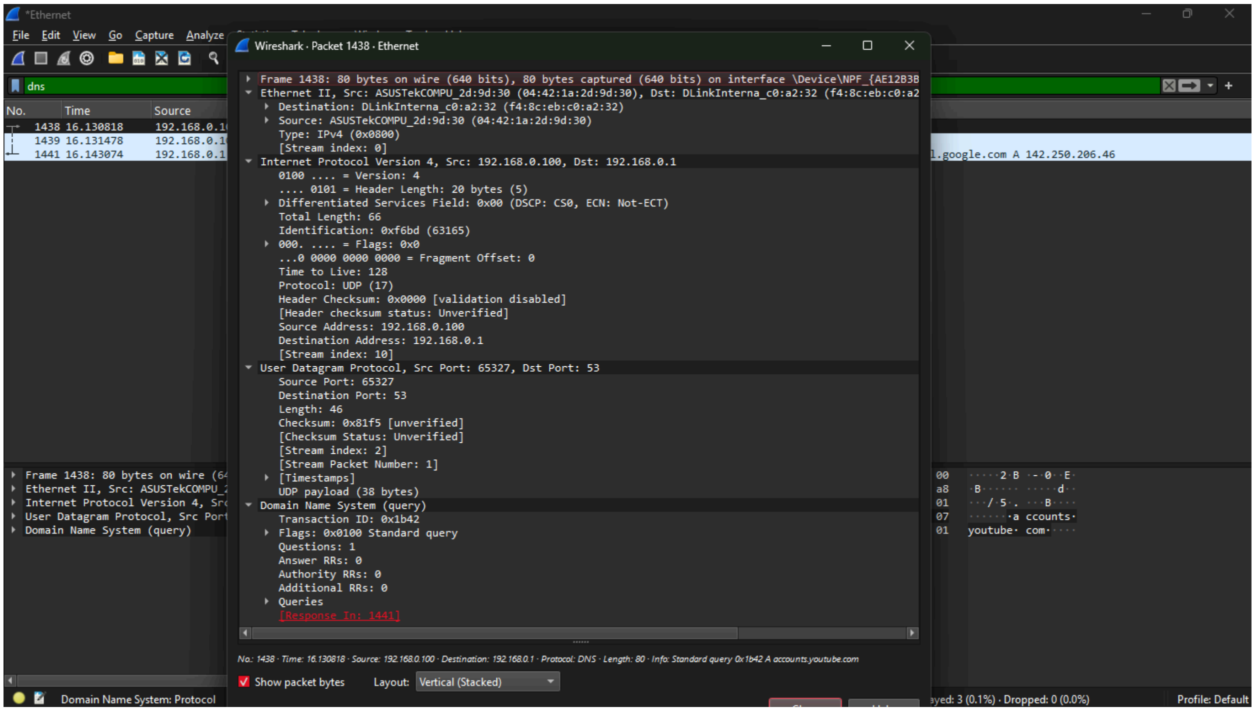
Wireshark Usage

Captured DNS packets :



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

```
dns
No.   Time       Source          Destination     Protocol Length Info
1438  16.130818  192.168.0.100   192.168.0.1     DNS        80 Standard query 0x1b42 A accounts.youtube.com
1439  16.131478  192.168.0.100   192.168.0.1     DNS        80 Standard query 0x97cf HTTPS accounts.youtube.com
1441  16.143074  192.168.0.1     192.168.0.100   DNS       127 Standard query response 0x1b42 A accounts.youtube.com CNAME www3.l.google.com A 142.250.206.46
```



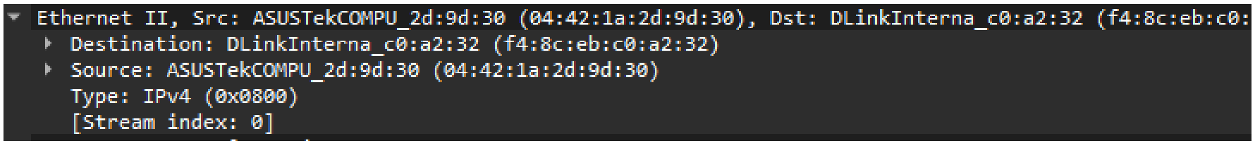
```
Frame 1438: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{AE12B3B
Ethernet II, Src: ASUSTekCOMPU_2d:9d:30 (04:42:1a:2d:9d:30), Dst: DLinkInterna_c0:a2:32 (f4:8c:eb:c0:a2
    Destination: DLinkInterna_c0:a2:32 (f4:8c:eb:c0:a2:32)
    Source: ASUSTekCOMPU_2d:9d:30 (04:42:1a:2d:9d:30)
    Type: IPv4 (0x0800)
    [Stream index: 0]
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0xf6bd (63165)
    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: 192.168.0.100
    Destination Address: 192.168.0.1
    [Stream index: 10]
User Datagram Protocol, Src Port: 65327, Dst Port: 53
    Source Port: 65327
    Destination Port: 53
    Length: 46
    Checksum: 0x81f5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 1]
    [Timestamps]
    UDP payload (38 bytes)
Domain Name System (query)
    Transaction ID: 0x1b42
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 1441]
```

No.: 1438 · Time: 16.130818 · Source: 192.168.0.100 · Destination: 192.168.0.1 · Protocol: DNS · Length: 80 · Info: Standard query 0x1b42 A accounts.youtube.com

☑ Show packet bytes Layout: Vertical (Stacked)

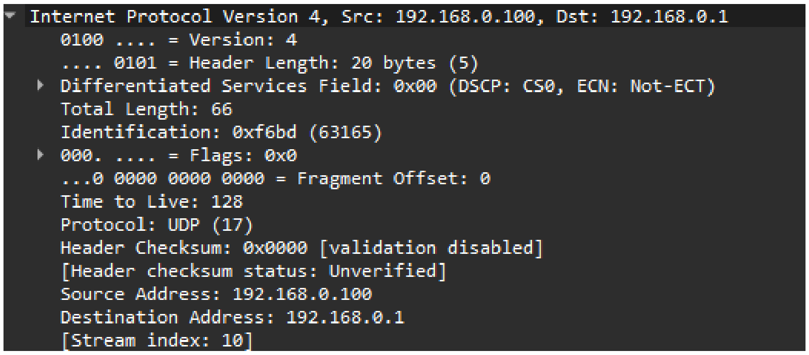
Analysis :

Source and Target MAC address :



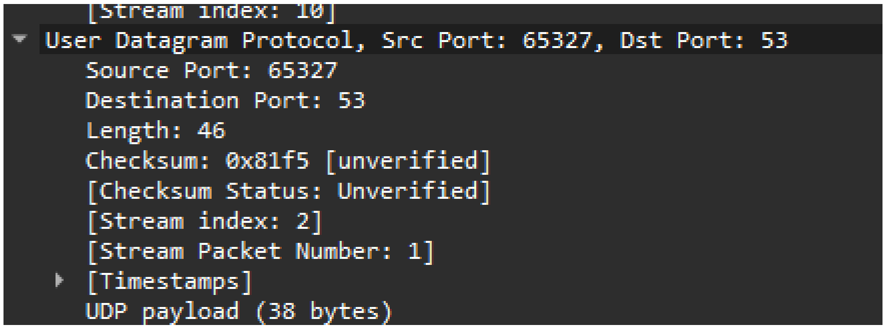
```
Ethernet II, Src: ASUSTekCOMPU_2d:9d:30 (04:42:1a:2d:9d:30), Dst: DLinkInterna_c0:a2:32 (f4:8c:eb:c0:
    Destination: DLinkInterna_c0:a2:32 (f4:8c:eb:c0:a2:32)
    Source: ASUSTekCOMPU_2d:9d:30 (04:42:1a:2d:9d:30)
    Type: IPv4 (0x0800)
    [Stream index: 0]
```

IP address :



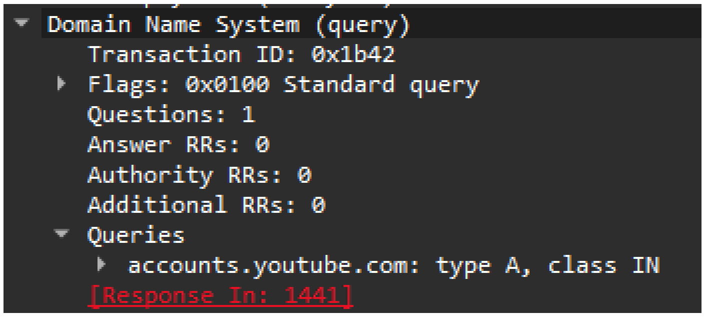
```
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0xf6bd (63165)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.100
    Destination Address: 192.168.0.1
    [Stream index: 10]
```

UDP protocol used here



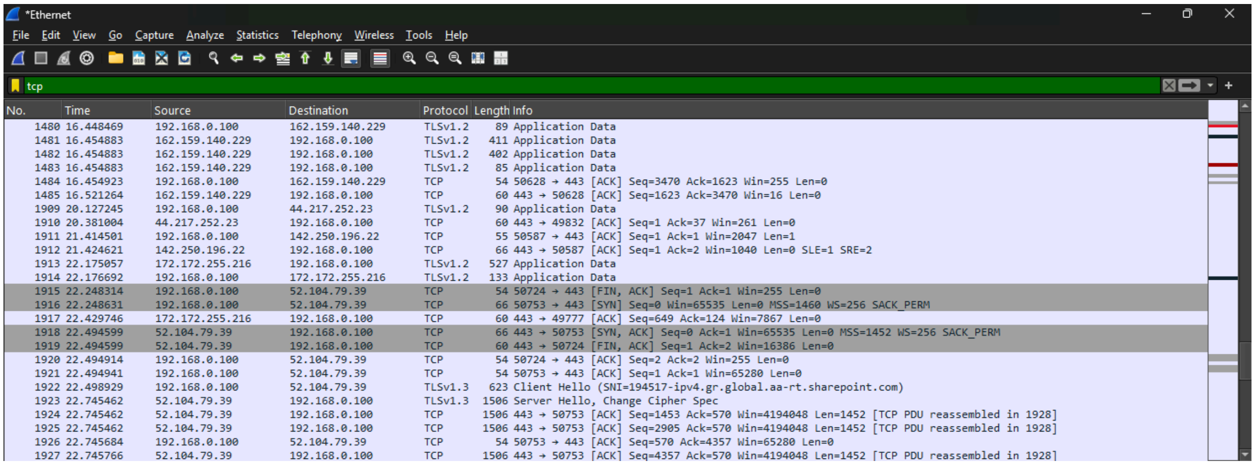
```
    [Stream index: 10]
▾ User Datagram Protocol, Src Port: 65327, Dst Port: 53
    Source Port: 65327
    Destination Port: 53
    Length: 46
    Checksum: 0x81f5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Stream Packet Number: 1]
  ▸ [Timestamps]
    UDP payload (38 bytes)
```

DNS Query :



```
▾ Domain Name System (query)
    Transaction ID: 0x1b42
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ accounts.youtube.com: type A, class IN
    [Response In: 1441]
```

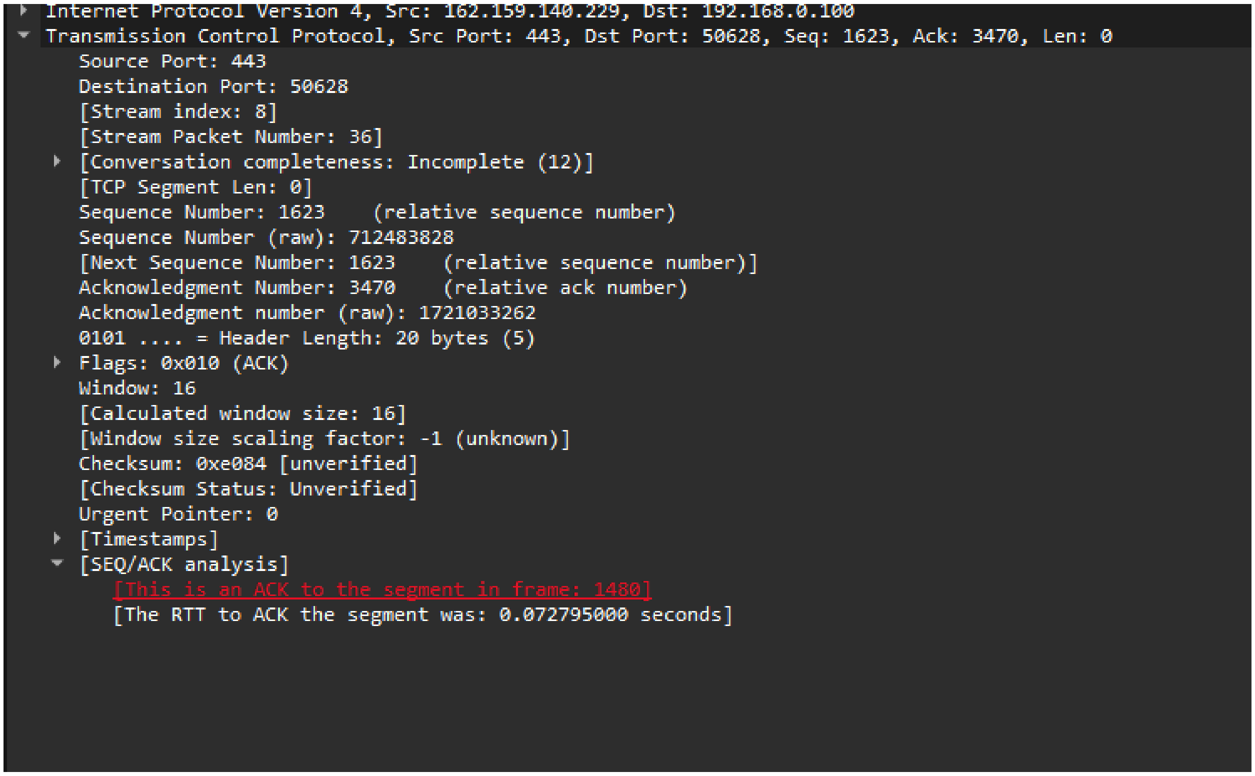
TCP packets are checked by filtering


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time      Source          Destination     Protocol Length Info
1480 16.448469 192.168.0.100   162.159.140.229 TLSv1.2    89 Application Data
1481 16.454883 162.159.140.229 192.168.0.100   TLSv1.2   411 Application Data
1482 16.454883 162.159.140.229 192.168.0.100   TLSv1.2   402 Application Data
1483 16.454883 162.159.140.229 192.168.0.100   TLSv1.2    85 Application Data
1484 16.454923 192.168.0.100   162.159.140.229 TCP        54 50628 → 443 [ACK] Seq=3470 Ack=1623 Win=255 Len=0
1485 16.521264 162.159.140.229 192.168.0.100   TCP        60 443 → 50628 [ACK] Seq=1623 Ack=3470 Win=16 Len=0
1909 20.127245 192.168.0.100   44.217.252.23   TLSv1.2    90 Application Data
1910 20.381004 44.217.252.23   192.168.0.100   TCP        60 443 → 49832 [ACK] Seq=1 Ack=37 Win=261 Len=0
1911 21.414501 192.168.0.100   142.250.196.22  TCP        55 50587 → 443 [ACK] Seq=1 Ack=1 Win=2047 Len=1
1912 21.424621 142.250.196.22  192.168.0.100   TCP        66 443 → 50587 [ACK] Seq=1 Ack=2 Win=1040 Len=0 SLE=1 SRE=2
1913 22.175057 172.172.255.216 192.168.0.100   TLSv1.2   527 Application Data
1914 22.176692 192.168.0.100   172.172.255.216 TLSv1.2   133 Application Data
1915 22.248314 192.168.0.100   52.104.79.39    TCP        54 50724 → 443 [FIN, ACK] Seq=1 Ack=1 Win=255 Len=0
1916 22.248631 192.168.0.100   52.104.79.39    TCP        66 50753 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1917 22.429746 172.172.255.216 192.168.0.100   TCP        60 443 → 49777 [ACK] Seq=649 Ack=124 Win=7867 Len=0
1918 22.494599 52.104.79.39    192.168.0.100   TCP        66 443 → 50753 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=256 SACK_PERM
1919 22.494599 52.104.79.39    192.168.0.100   TCP        60 443 → 50724 [FIN, ACK] Seq=1 Ack=2 Win=16386 Len=0
1920 22.494914 192.168.0.100   52.104.79.39    TCP        54 50724 → 443 [ACK] Seq=2 Ack=2 Win=255 Len=0
1921 22.494941 192.168.0.100   52.104.79.39    TCP        54 50753 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1922 22.498929 192.168.0.100   52.104.79.39    TLSv1.3   623 Client Hello (SNI=194517-ipv4.gr.global.aa-rt.sharepoint.com)
1923 22.745462 52.104.79.39    192.168.0.100   TLSv1.3  1506 Server Hello, Change Cipher Spec
1924 22.745462 52.104.79.39    192.168.0.100   TCP      1506 443 → 50753 [ACK] Seq=1453 Ack=570 Win=4194048 Len=1452 [TCP PDU reassembled in 1928]
1925 22.745462 52.104.79.39    192.168.0.100   TCP      1506 443 → 50753 [ACK] Seq=2905 Ack=570 Win=4194048 Len=1452 [TCP PDU reassembled in 1928]
1926 22.745684 192.168.0.100   52.104.79.39    TCP        54 50753 → 443 [ACK] Seq=570 Ack=4357 Win=65280 Len=0
1927 22.745766 52.104.79.39    192.168.0.100   TCP      1506 443 → 50753 [ACK] Seq=4357 Ack=570 Win=4194048 Len=1452 [TCP PDU reassembled in 1928]
```

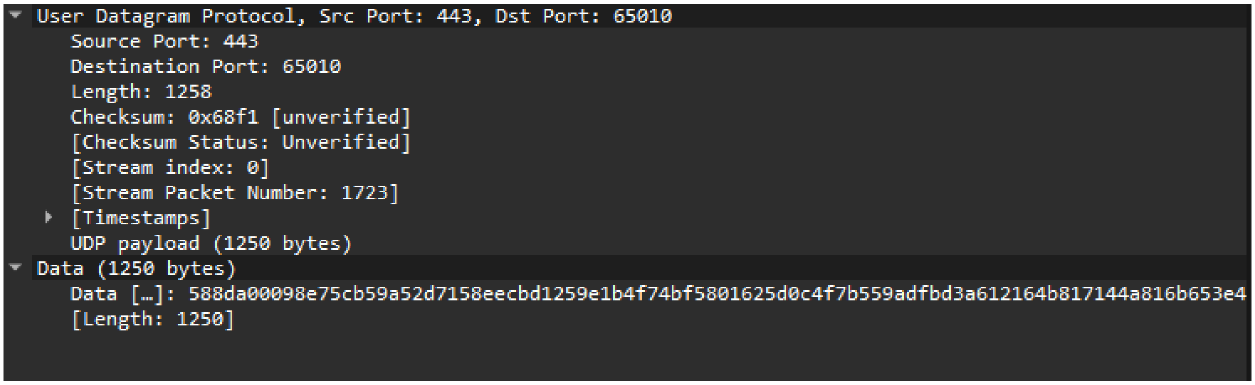
Here , In the TCP header,flags can be checked for :

SYN: Initiates a connection.
ACK: Acknowledges received data.
FIN: Closes a connection.
RST: Resets a connection.



```
▸ Internet Protocol Version 4, Src: 162.159.140.229, Dst: 192.168.0.100
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 50628, Seq: 1623, Ack: 3470, Len: 0
     Source Port: 443
     Destination Port: 50628
     [Stream index: 8]
     [Stream Packet Number: 36]
   ▸ [Conversation completeness: Incomplete (12)]
     [TCP Segment Len: 0]
     Sequence Number: 1623    (relative sequence number)
     Sequence Number (raw): 712483828
     [Next Sequence Number: 1623    (relative sequence number)]
     Acknowledgment Number: 3470    (relative ack number)
     Acknowledgment number (raw): 1721033262
     0101 .... = Header Length: 20 bytes (5)
   ▸ Flags: 0x010 (ACK)
     Window: 16
     [Calculated window size: 16]
     [Window size scaling factor: -1 (unknown)]
     Checksum: 0xe084 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   ▸ [Timestamps]
   ▾ [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 1480]
        [The RTT to ACK the segment was: 0.072795000 seconds]
```

Comparatively UDP has lesser options to view like length and checksum fields.



```
▾ User Datagram Protocol, Src Port: 443, Dst Port: 65010
     Source Port: 443
     Destination Port: 65010
     Length: 1258
     Checksum: 0x68f1 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
     [Stream Packet Number: 1723]
   ▸ [Timestamps]
     UDP payload (1250 bytes)
▾ Data (1250 bytes)
     Data […]: 588da00098e75cb59a52d7158eecbd1259e1b4f74bf5801625d0c4f7b559adfbd3a612164b817144a816b653e4
     [Length: 1250]
```