<u>Capture UDP packets and with the help of the captured UDP Packets.</u>

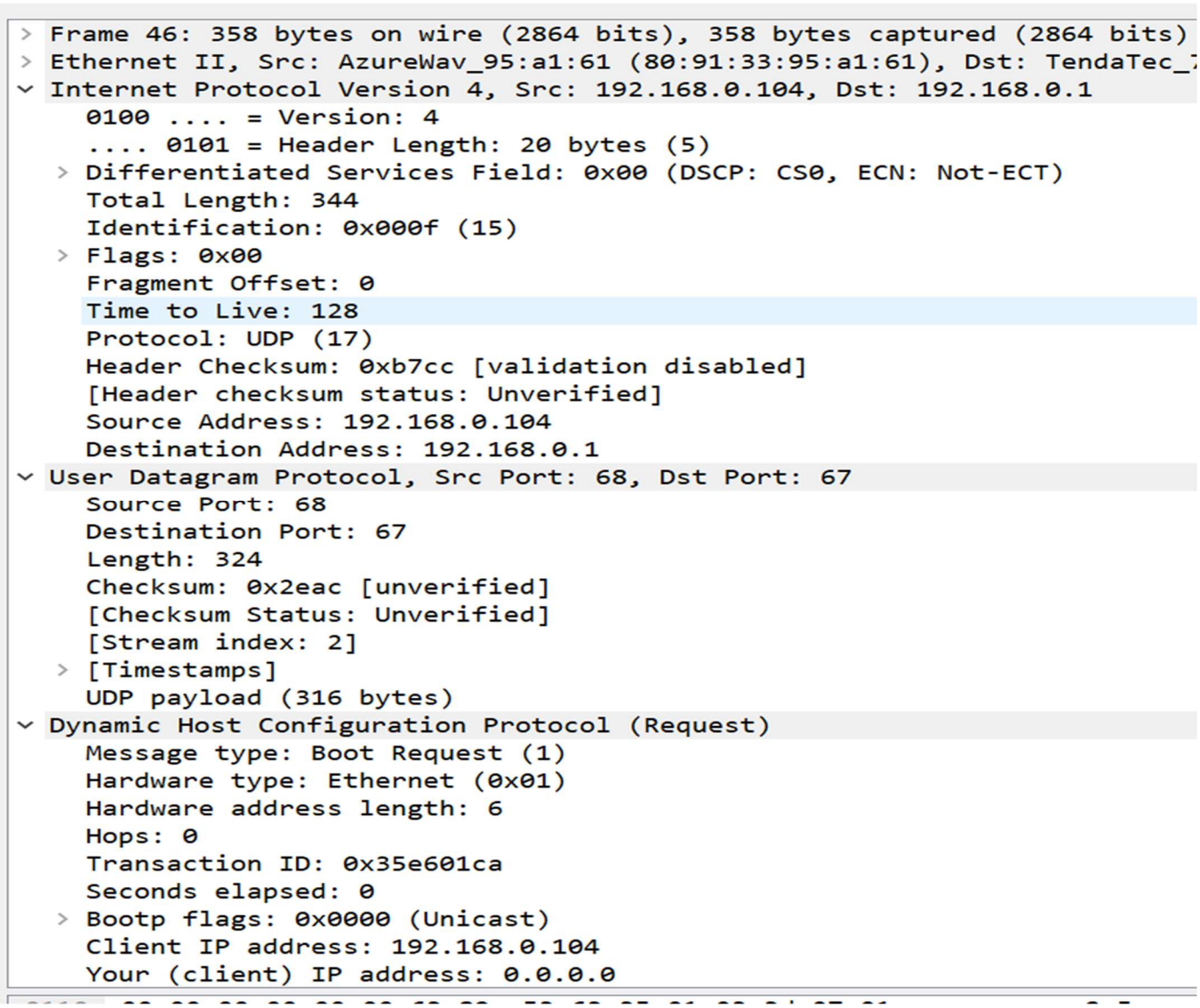
a. analyses UDP DHCP Packets

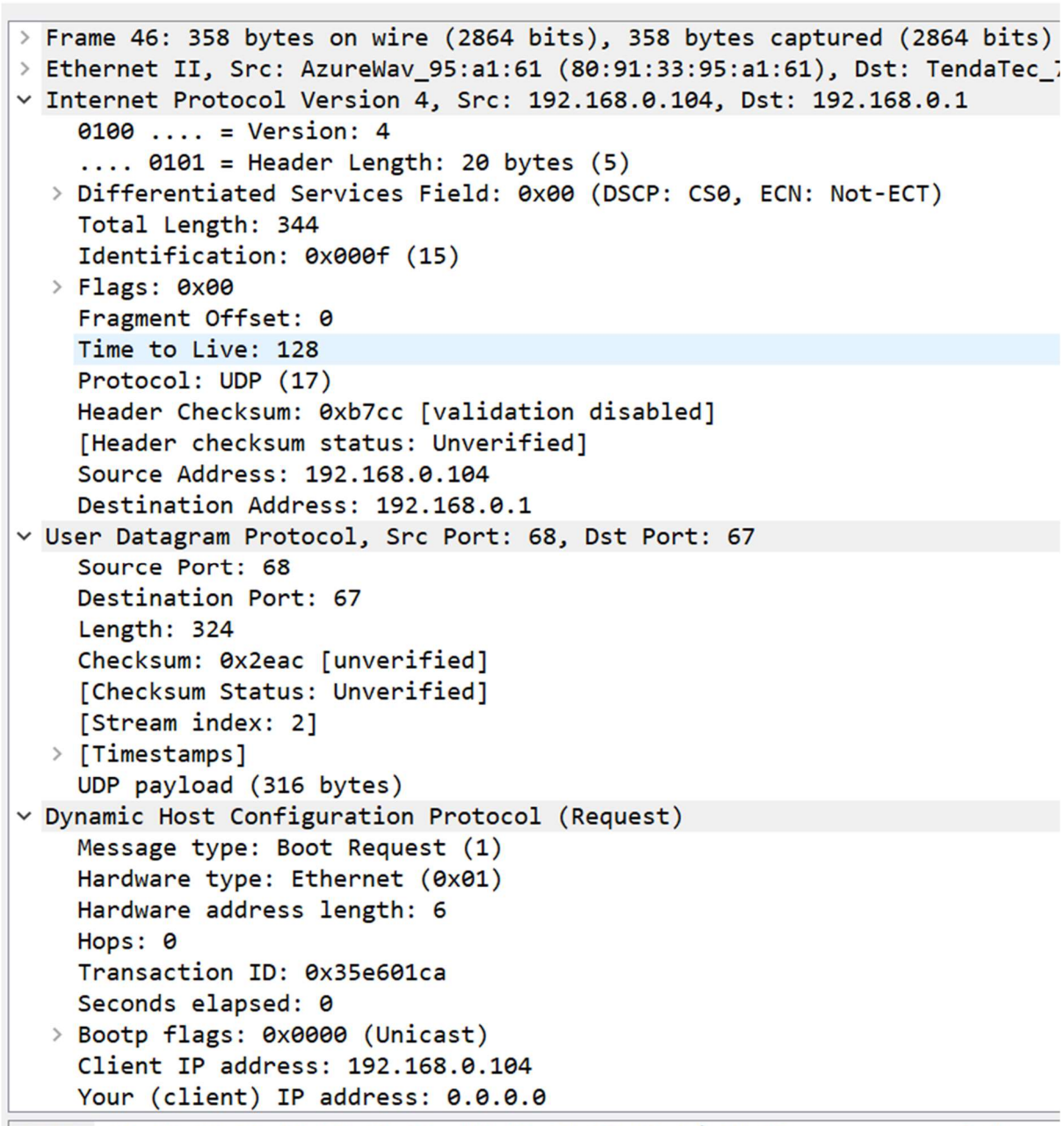
b. analyses UDP DNS Packets

Analysis of UDP DHCP Packets:

- DHCP is used for ip configuration

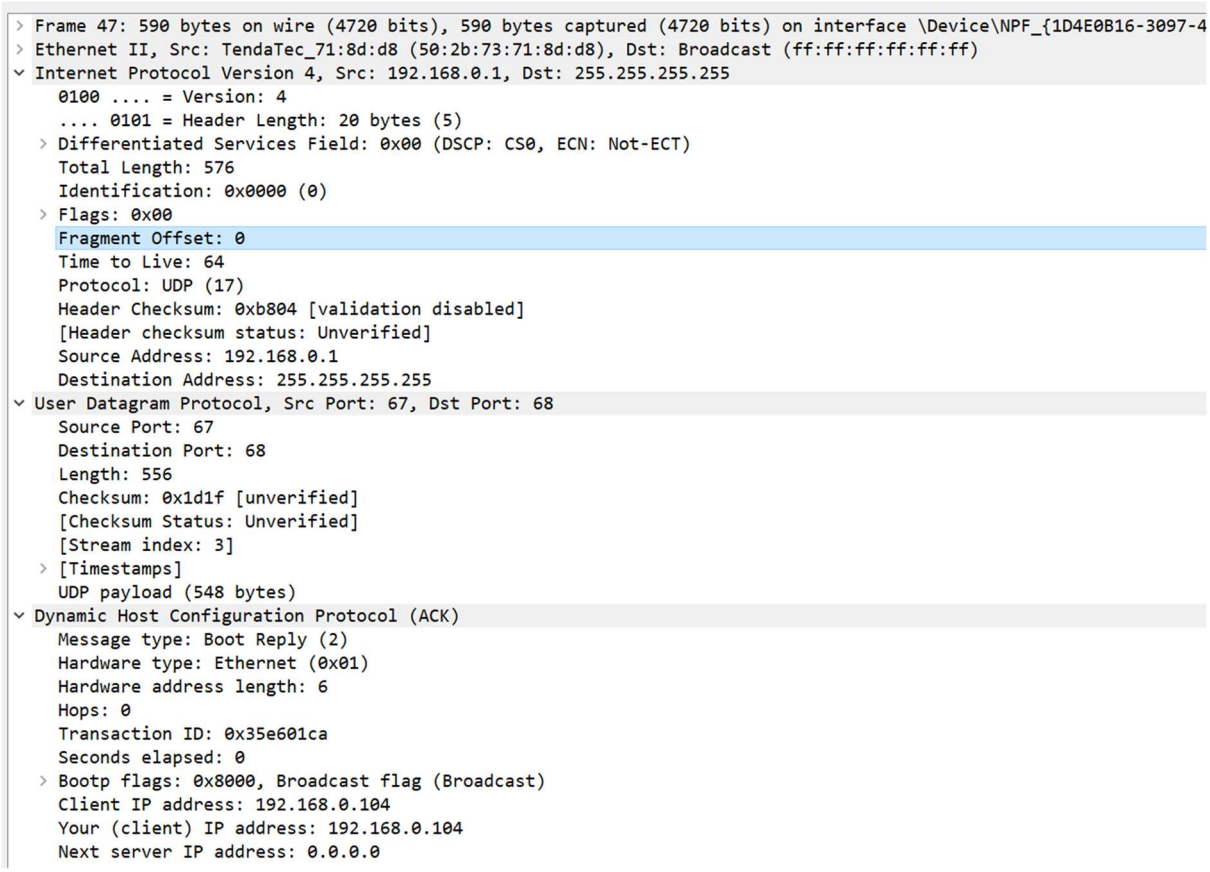
Dhcp Request





From the above pictures we can know the DHCP configuration. Source and Destination Ports and IP here source and destination has static port (67 ,68). And various other information regarding DHCP request.

DHCP ACK

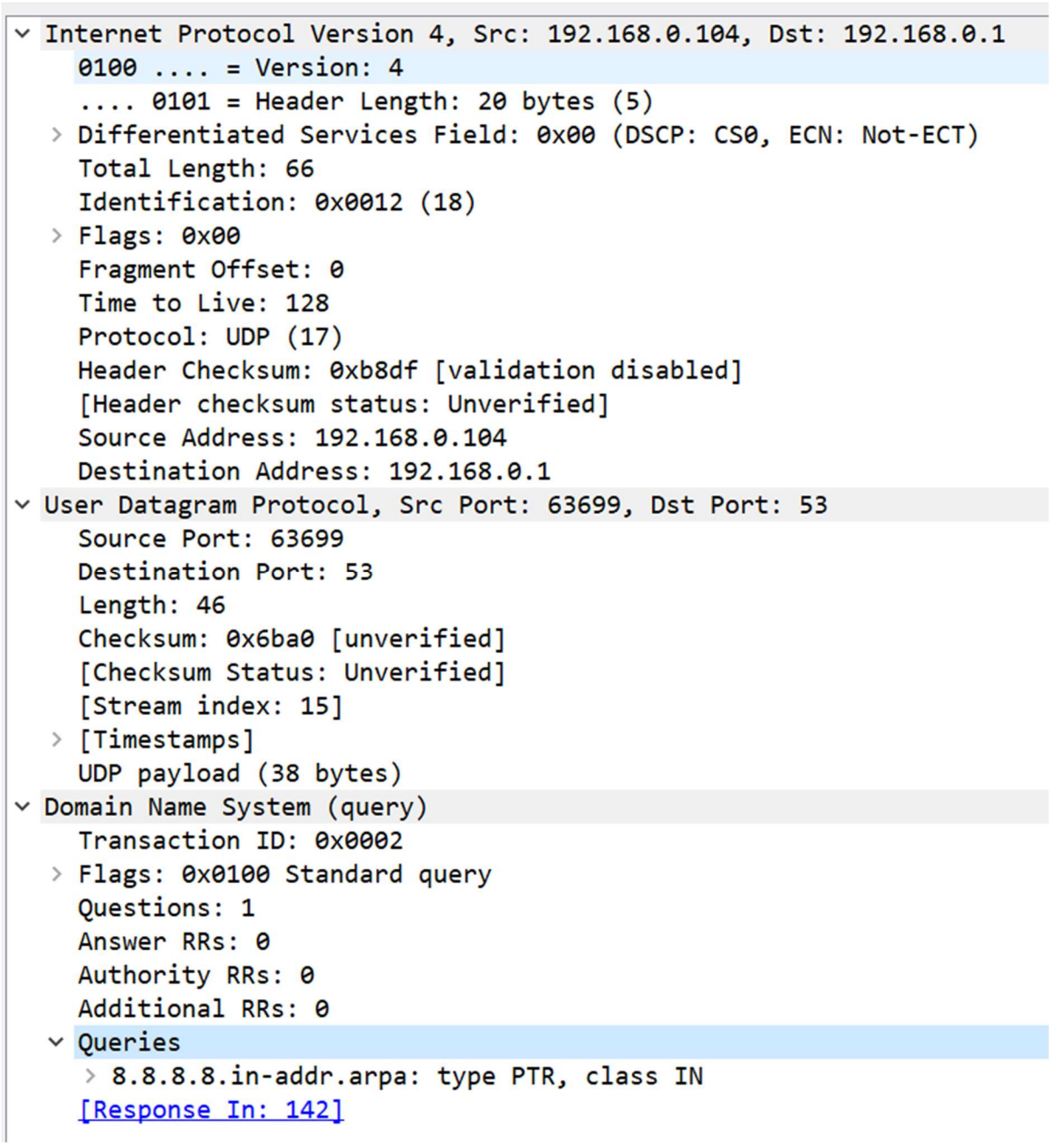

Frame 47: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{1D4E0B16-3097-4
Ethernet II, Src: TendaTec_71:8d:d8 (50:2b:73:71:8d:d8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 255.255.255.255
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 576
Identification: 0x0000 (0)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0xb804 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.1
Destination Address: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68
Source Port: 67
Destination Port: 68
Length: 556
Checksum: 0x1d1f [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Timestamps]
UDP payload (548 bytes)
Dynamic Host Configuration Protocol (ACK)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x35e601ca
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 192.168.0.104
Your (client) IP address: 192.168.0.104
Next server IP address: 0.0.0.0

```
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x35e601ca
  Seconds elapsed: 0
> Bootp flags: 0x8000, Broadcast flag (Broadcast)
  Client IP address: 192.168.0.104
  Your (client) IP address: 192.168.0.104
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: AzureWav_95:a1:61 (80:91:33:95:a1:61)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
v Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
v Option: (54) DHCP Server Identifier (192.168.0.1)
    Length: 4
    DHCP Server Identifier: 192.168.0.1
v Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
v Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
v Option: (3) Router
    Length: 4
    Router: 192.168.0.1
v Option: (6) Domain Name Server
    Length: 4
    Domain Name Server: 192.168.0.1
v Option: (0) Padding
    Padding: 000000000000000000000000000000000000000000000000000000000000000000000000…
v Option: (255) End
    Option End: 255
```

Basically, DHCP is used for providing an automatic IP address to Hosts which want to connect to a network

Analyses UDP DNS Packets

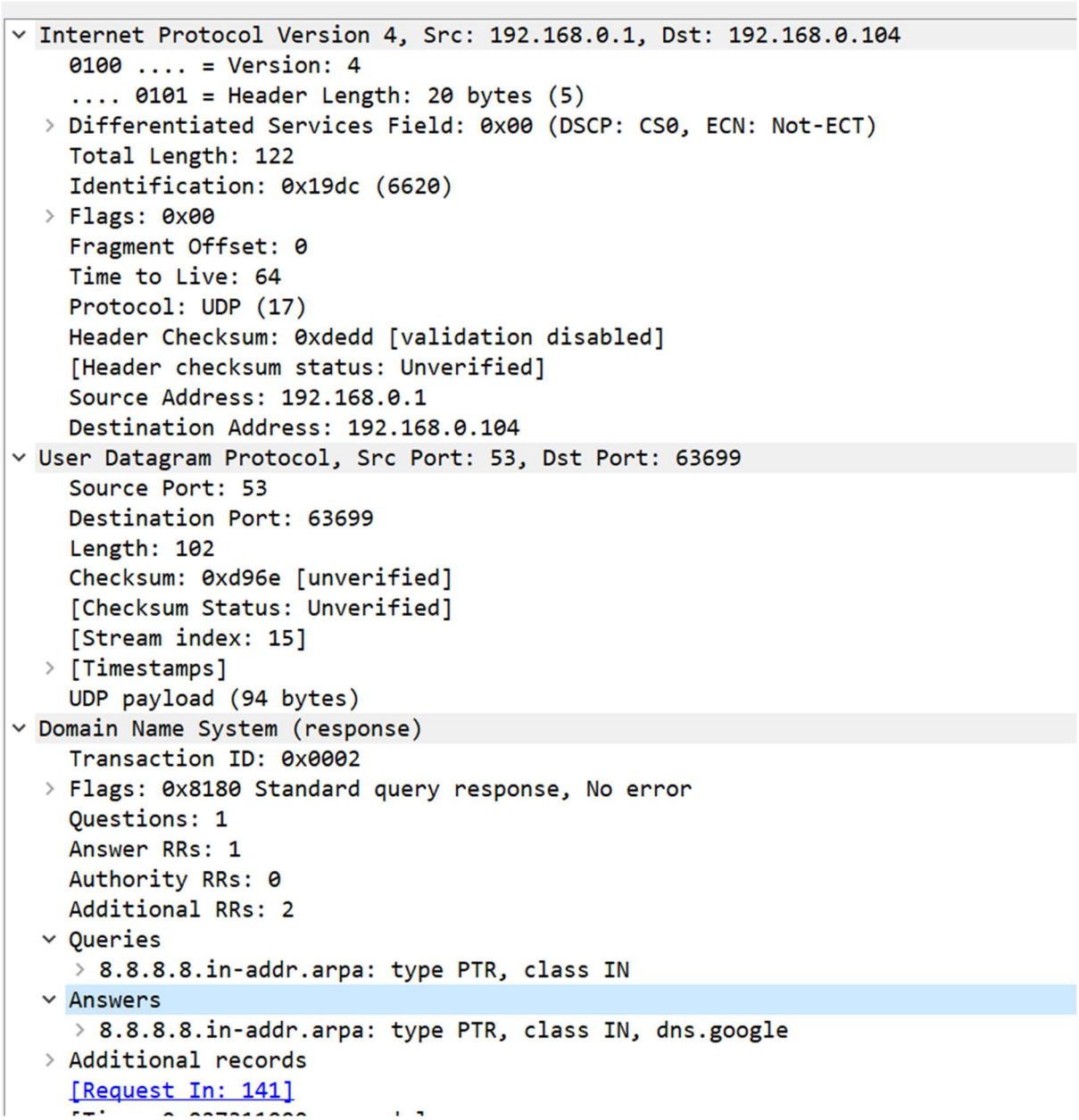
- *Dns server is used to resolve the domain name into IP*



In the above image we can find the source and Destination IP and ports

But here source Ip is dynamic. And we can also find the query..

And various other details regarding the DNS request



In the DNS Standard query response we can see the information regarding the request sent by my machine and Various other information regarding the request and response..