Wireshark Lab: Getting Started

From my windows start menu, I selected the Run application and typed “cmd” to open the command prompt, then I typed in the command “ipconfig” to display the Windows IP configuration. The system I have been using uses IPv6 and IPv4.

Example 1: With IPv4 version.

Where The first captured frame is of the IPv4 version.

1. Capture the IP address in the command prompt and the Wireshark, application attach the screenshot of both.

Here we can observe that the IPv4 Address is 192.168.1.127

C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 10.0.22000.1574]
(c) Microsoft Corporation. All rights reserved.

C:\Users\badda>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   IPv6 Address. . . . . . . . . . . : 2600:6c56:7ff0:8c00::1764
   IPv6 Address. . . . . . . . . . . : 2600:6c56:7ff0:8c00:f029:d3c:86aa:35d7
   Temporary IPv6 Address. . . . . . : 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
   Link-local IPv6 Address . . . . . : fe80::184f:df62:7eb5:df65%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.127
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::46ad:b1ff:fe4a:c55a%10
                                       192.168.1.1

C:\Users\badda>
```

Now I have opened the Wireshark application that has been downloaded. Selected the Wi-Fi option to capture the packets. Below is the IP information from a packet that was captured. In the Internet Protocol Version 4 section, we can see the destination Address, which is the same as the IP in the command prompt.

Wireshark · Packet 1 · Wi-Fi

```
Frame 1: 1005 bytes on wire (8040 bits), 1005 bytes captured (8040 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 28, 2023 17:19:47.821136000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677626387.821136000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 1005 bytes (8040 bits)
    Capture Length: 1005 bytes (8040 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Destination: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Source: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 13.107.42.12, Dst: 192.168.1.127
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 991
    Identification: 0x0000 (0)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 116
    Protocol: TCP (6)
    Header Checksum: 0x097b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 13.107.42.12
    Destination Address: 192.168.1.127
Transmission Control Protocol, Src Port: 443, Dst Port: 57223, Seq: 1, Ack: 1, Len: 951
    Source Port: 443
    Destination Port: 57223
    [Stream index: 0]
    [Conversation completeness: Incomplete (60)]
    [TCP Segment Len: 951]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 788285000
    [Next Sequence Number: 952    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 372093651
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 16383
    [Calculated window size: 16383]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x9db3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (951 bytes)
Transport Layer Security
    TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
        Content Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 889
        Encrypted Application Data: 000000000000005f2ce58a96f8d19733b8e82fa2c200151434c8a2c49a182e6debcd179e…
        [Application Data Protocol: Hypertext Transfer Protocol]
    TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
        Content Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 52
        Encrypted Application Data: 0000000000000000607168b2095a6a7ac6a5bf9e327ceb1c6125925b952218cdeafe765d60…
        [Application Data Protocol: Hypertext Transfer Protocol]
```

No.: 1 · Time: 0.000000 · Source: 13.107.42.12 · Destination: 192.168.1.127 · Protocol: TLSv1.2 · Length: 1005 · Info: Application Data, Application Data

Show packet bytes

2. What is the source and destination address of the first request in the wire shark?

Below is the First Frame that was captured. The source and destination address can be found in the Internet Protocol Version 4 section.

Source Address: 13.107.42.12

Destination Address: 192.168.1.127

The source address is the IP address of the device that sent the packet, which is some other device that sent the packet, while the destination address is the address of my device that received the packet.

Wireshark · Packet 1 · Wi-Fi

```
> Frame 1: 1005 bytes on wire (8040 bits), 1005 bytes captured (8040 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
  > Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 28, 2023 17:19:47.821136000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677626387.821136000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 1005 bytes (8040 bits)
    Capture Length: 1005 bytes (8040 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> Ethernet II, Src: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
  > Destination: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
  > Source: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 13.107.42.12, Dst: 192.168.1.127
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 991
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 116
    Protocol: TCP (6)
    Header Checksum: 0x097b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 13.107.42.12
    Destination Address: 192.168.1.127
```

```
> Transmission Control Protocol, Src Port: 443, Dst Port: 57223, Seq: 1, Ack: 1, Len: 951
    Source Port: 443
    Destination Port: 57223
    [Stream index: 0]
    [Conversation completeness: Incomplete (60)]
    [TCP Segment Len: 951]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 788285000
    [Next Sequence Number: 952    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 372093651
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 16383
    [Calculated window size: 16383]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x9db3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (951 bytes)
> Transport Layer Security
  > TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 889
      Encrypted Application Data: 000000000000005f2ce58a96f8d19733b8e82fa2c200151434c8a2c49a182e6debcd179e…
      [Application Data Protocol: Hypertext Transfer Protocol]
  > TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 52
      Encrypted Application Data: 0000000000000607168b2095a6a7ac6a5bf9e327ceb1c6125925b952218cdeafe765d60…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

No.: 1 · Time: 0.000000 · Source: 13.107.42.12 · Destination: 192.168.1.127 · Protocol: TLSv1.2 · Length: 1005 · Info: Application Data, Application Data

☐ Show packet bytes

3. What internet protocol version is used?

In frame 1, the IP protocol version that is being used is IPv4, we can find the version field in the Internet Protocol Version 4 section.

Wireshark · Packet 1 · Wi-Fi

```
Frame 1: 1005 bytes on wire (8040 bits), 1005 bytes captured (8040 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 28, 2023 17:19:47.821136000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677626387.821136000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 1005 bytes (8040 bits)
    Capture Length: 1005 bytes (8040 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a), Dst: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Destination: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Source: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 13.107.42.12, Dst: 192.168.1.127
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 991
    Identification: 0x0000 (0)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 116
    Protocol: TCP (6)
    Header Checksum: 0x097b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 13.107.42.12
    Destination Address: 192.168.1.127
Transmission Control Protocol, Src Port: 443, Dst Port: 57223, Seq: 1, Ack: 1, Len: 951
    Source Port: 443
    Destination Port: 57223
    [Stream index: 0]
    [Conversation completeness: Incomplete (60)]
    [TCP Segment Len: 951]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 788285000
    [Next Sequence Number: 952    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 372093651
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 16383
    [Calculated window size: 16383]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x9db3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (951 bytes)
Transport Layer Security
    TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
        Content Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 889
        Encrypted Application Data: 0000000000000005f2ce58a96f8d19733b8e82fa2c200151434c8a2c49a182e6debcd179e…
        [Application Data Protocol: Hypertext Transfer Protocol]
    TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
        Content Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 52
        Encrypted Application Data: 0000000000000000607168b2095a6a7ac6a5bf9e327ceb1c6125925b952218cdeafe765d60…
        [Application Data Protocol: Hypertext Transfer Protocol]
```

No.: 1 · Time: 0.000000 · Source: 13.107.42.12 · Destination: 192.168.1.127 · Protocol: TLSv1.2 · Length: 1005 · Info: Application Data, Application Data

Show packet bytes

4. What is the source port in the UDP?

The source port is a port number that is chosen by the sending device to identify the specific application that is sending the data. The receiving device uses the source port to identify which application on the sending device is responsible for generating the data.

UDP Source Port: 55502

Wireshark · Packet 105 · ipv4 assignment 1.pcapng

```
> Frame 105: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
  > Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 28, 2023 17:20:13.146146000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677626413.146146000 seconds
    [Time delta from previous captured frame: 0.000926000 seconds]
    [Time delta from previous displayed frame: 0.000926000 seconds]
    [Time since reference or first frame: 25.325010000 seconds]
    Frame Number: 105
    Frame Length: 105 bytes (840 bits)
    Capture Length: 105 bytes (840 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
> Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 91
    Identification: 0xec24 (60452)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xca9c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.127
    Destination Address: 192.168.1.1
> User Datagram Protocol, Src Port: 55502, Dst Port: 53
    Source Port: 55502
    Destination Port: 53
    Length: 71
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (63 bytes)
> Domain Name System (query)
    Transaction ID: 0x7685
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 107]
```

No.: 105 · Time: 25.325010 · Source: 192.168.1.127 · Destination: 192.168.1.1 · Protocol: DNS · Length: 105 · Info: Standard query 0x7685 A onedriveclucproddm20007.blob.core.windows.net

☐ Show packet bytes

5. What is the destination port in the UDP?

The destination port is a number that identifies the specific application that the data is intended for on the receiving device. This allows the receiving device to deliver the data to the correct application.

UDP Destination Port: 53

Wireshark · Packet 105 · ipv4 assignment 1.pcapng

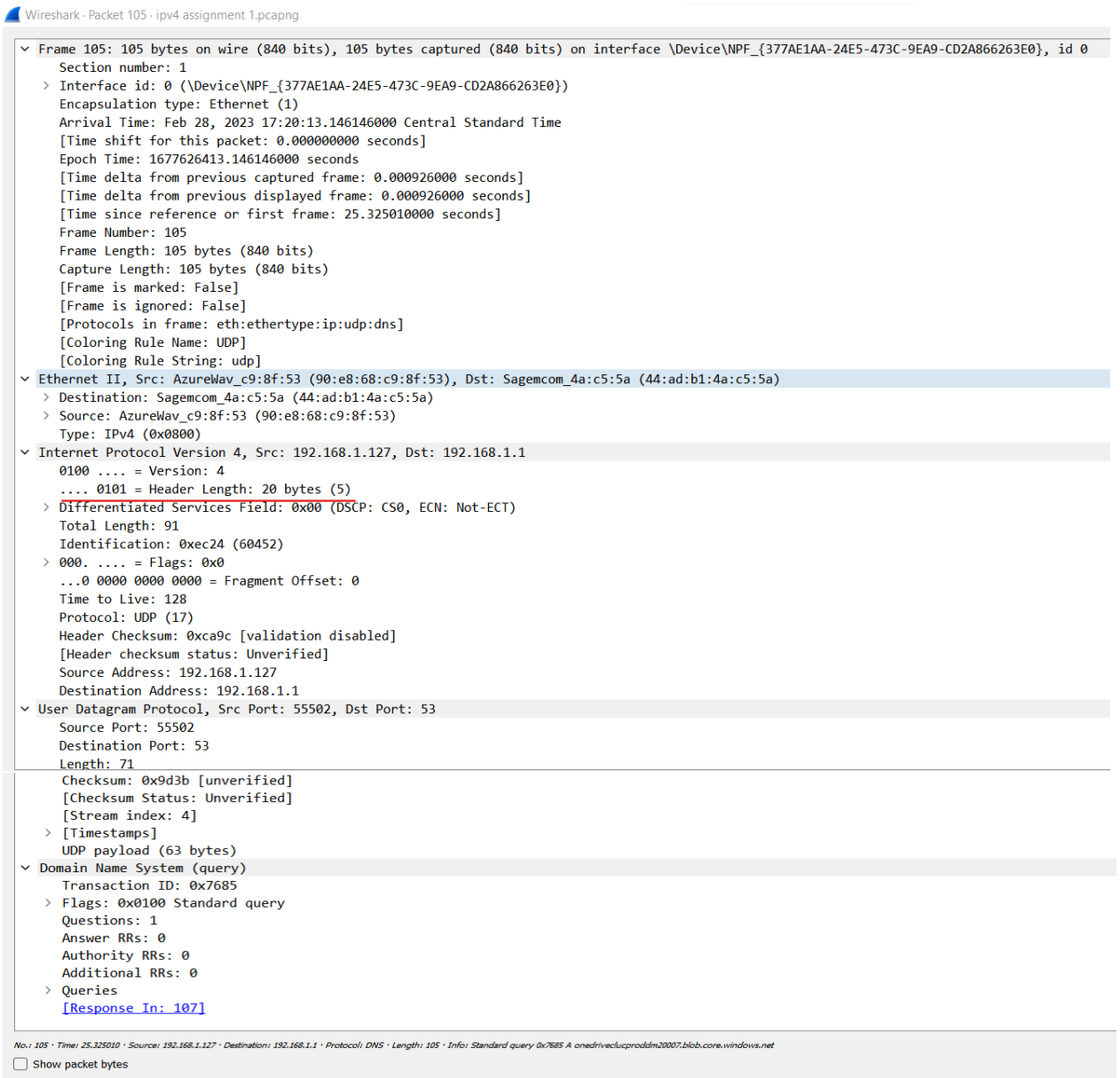
```
Frame 105: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
  > Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 28, 2023 17:20:13.146146000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677626413.146146000 seconds
    [Time delta from previous captured frame: 0.000926000 seconds]
    [Time delta from previous displayed frame: 0.000926000 seconds]
    [Time since reference or first frame: 25.325010000 seconds]
    Frame Number: 105
    Frame Length: 105 bytes (840 bits)
    Capture Length: 105 bytes (840 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 91
    Identification: 0xec24 (60452)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xca9c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.127
    Destination Address: 192.168.1.1
User Datagram Protocol, Src Port: 55502, Dst Port: 53
    Source Port: 55502
    Destination Port: 53
    Length: 71
    Checksum: 0x9d3b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (63 bytes)
Domain Name System (query)
    Transaction ID: 0x7685
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 107]
```

No.: 105 · Time: 25.325010 · Source: 192.168.1.127 · Destination: 192.168.1.1 · Protocol: DNS · Length: 105 · Info: Standard query 0x7685 A onedriveclucproddm20007.blob.core.windows.net

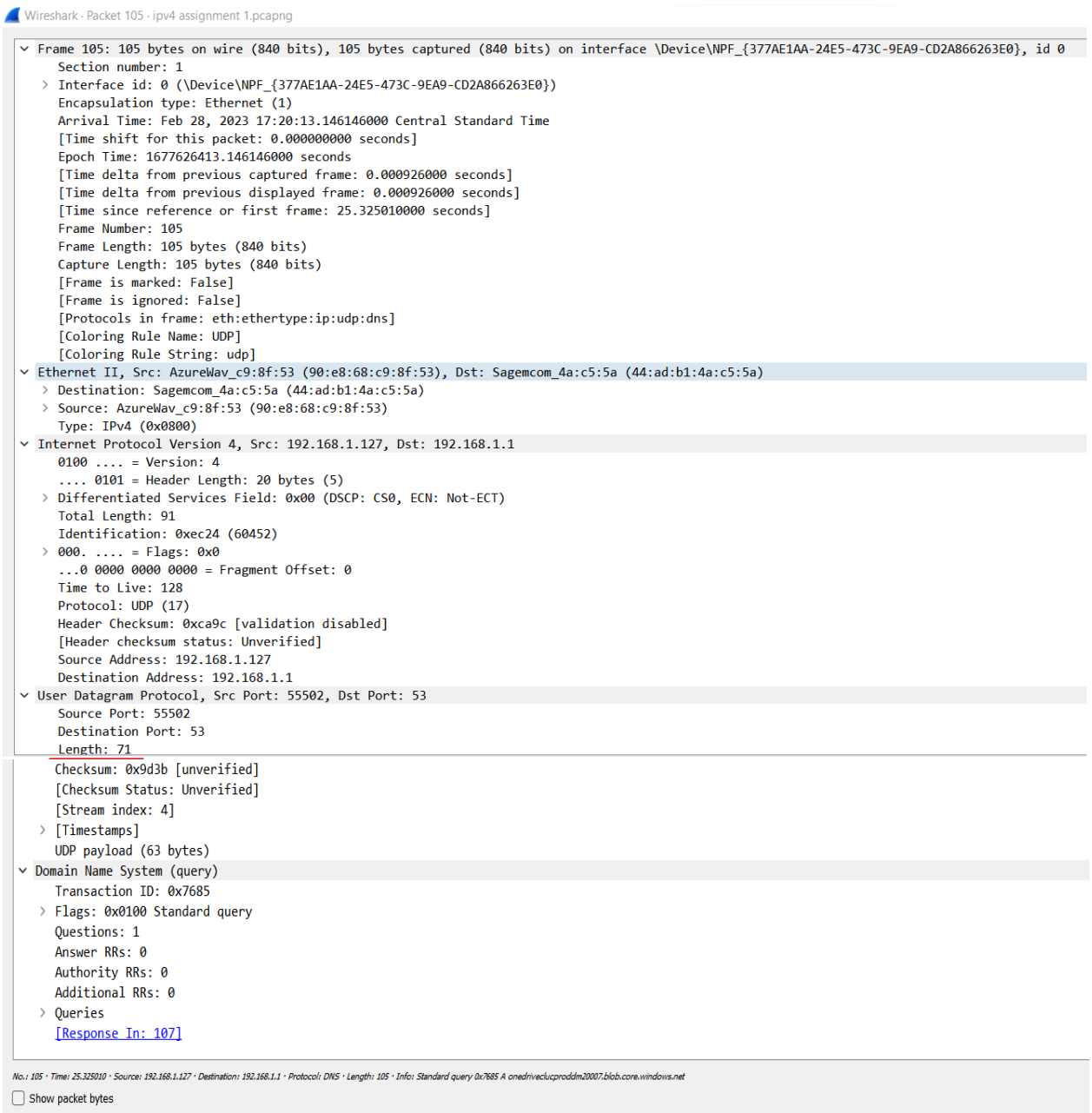
☐ Show packet bytes

6. What is the header length?

The header contains information that is required to route the packet through the network. In IPv4, the header length is variable and can range from 20 to 60 bytes in length, in the below frame the header length is 20 bytes.



UDP Header Length: 71



Example 2: With IPv6 version.

Where The first captured frame is of the IPv6 version.

1. Capture the IP address in the command prompt and the Wireshark, application attach the screenshot of both.

Here we can observe that the IPv6 has 3 different IP Addresses, the temporary IPv6 Address is 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b

C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 10.0.22000.1574]
(c) Microsoft Corporation. All rights reserved.

C:\Users\badda>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   IPv6 Address. . . . . . . . . . . : 2600:6c56:7ff0:8c00::1764
   IPv6 Address. . . . . . . . . . . : 2600:6c56:7ff0:8c00:f029:d3c:86aa:35d7
   Temporary IPv6 Address. . . . . . : 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
   Link-local IPv6 Address . . . . . : fe80::184f:df62:7eb5:df65%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.127
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::46ad:b1ff:fe4a:c55a%10
                                       192.168.1.1

C:\Users\badda>
```

Now I have opened the Wireshark application that has been downloaded. Selected the Wi-Fi option to capture the packets. Below is the IP information from a packet that was captured. In the Internet Protocol Version 6 section, we can see the source Address, which is the same as the IP in the command prompt.

Wireshark · Packet 2 · Wi-Fi

```
Frame 2: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 26, 2023 19:18:39.300511000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677460719.300511000 seconds
    [Time delta from previous captured frame: 0.003549000 seconds]
    [Time delta from previous displayed frame: 0.003549000 seconds]
    [Time since reference or first frame: 0.003549000 seconds]
    Frame Number: 2
    Frame Length: 1292 bytes (10336 bits)
    Capture Length: 1292 bytes (10336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:quic:tls:tls:tls]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b, Dst: 2607:f8b0:4009:81b::2004
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 1010 1100 1101 1011 = Flow Label: 0xaacdb
    Payload Length: 1238
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
    Destination Address: 2607:f8b0:4009:81b::2004
User Datagram Protocol, Src Port: 52238, Dst Port: 443
    Source Port: 52238
    Destination Port: 443
```

```
0000  44 ad b1 4a c5 5a 90 e8  68 c9 8f 53 86 dd 60 0a   D··J·Z·· h··S··`·
0010  ac db 04 d6 11 40 26 00  6c 56 7f f0 8c 00 04 59   ·····@&· lV·····Y
0020  76 1f 15 f3 5c 3b 26 07  f8 b0 40 09 08 1b 00 00   v···\;&· ··@·····
0030  00 00 00 00 20 04 cc 0e  01 bb 04 d6 a1 6b cb 00   ···· ··· ·····k··
```

Frame (1292 bytes) | Decrypted QUIC (1124 bytes) | Reassembled QUIC CRYPTO (82 bytes) | Reassembled TLS Handshake (780 bytes)

Wireshark · Packet 1 · Wi-Fi

```
    Frame Number: 1
    Frame Length: 117 bytes (936 bits)
    Capture Length: 117 bytes (936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b, Dst: 2600:6c56:7ff0:8c00::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 0011 0111 0100 0011 = Flow Label: 0xa3743
    Payload Length: 63
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
    Destination Address: 2600:6c56:7ff0:8c00::1
v User Datagram Protocol, Src Port: 53365, Dst Port: 53
    Source Port: 53365
    Destination Port: 53
    Length: 63
    Checksum: 0xf95e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (55 bytes)
v Domain Name System (query)
    Transaction ID: 0x47e6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 4]
```

2. What is the source and destination address of the first request in the wire shark?

Below is the First Frame that was captured. The source and destination address can be found in the Internet Protocol Version 6 section.

Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b

Destination Address: 2600:6c56:7ff0:8c00::1

The source address is the IP address of the device that sent the packet which is my device, while the destination address is the IP address of the device that received the packet.

Wireshark · Packet 1 · Wi-Fi

```
Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 26, 2023 19:18:39.296962000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677460719.296962000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 117 bytes (936 bits)
    Capture Length: 117 bytes (936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b, Dst: 2600:6c56:7ff0:8c00::1
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 0011 0111 0100 0011 = Flow Label: 0xa3743
    Payload Length: 63
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
    Destination Address: 2600:6c56:7ff0:8c00::1
User Datagram Protocol, Src Port: 53365, Dst Port: 53
    Source Port: 53365
    Destination Port: 53
    Length: 63
    Checksum: 0xf95e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
    UDP payload (55 bytes)
```

```
Domain Name System (query)
    Transaction ID: 0x47e6
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 4]
```

3. What internet protocol version is used?

In frame 1, the IP protocol version that is being used is IPv6, we can find the version field in the Internet Protocol Version 6 section.

Wireshark · Packet 1 · Wi-Fi

```
Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
  > Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 26, 2023 19:18:39.296962000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677460719.296962000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 117 bytes (936 bits)
    Capture Length: 117 bytes (936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b, Dst: 2600:6c56:7ff0:8c00::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 0011 0111 0100 0011 = Flow Label: 0xa3743
    Payload Length: 63
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
    Destination Address: 2600:6c56:7ff0:8c00::1
User Datagram Protocol, Src Port: 53365, Dst Port: 53
    Source Port: 53365
    Destination Port: 53
    Length: 63
    Checksum: 0xf95e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (55 bytes)
```

Show packet bytes

```
Domain Name System (query)
    Transaction ID: 0x47e6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 4]
```

4. What is the source port in the UDP?

The source port is a port number that is chosen by the sending device to identify the specific application that is sending the data. The receiving device uses the source port to identify which application on the sending device is responsible for generating the data.

UDP Source Port: 53365

Wireshark · Packet 1 · Wi-Fi

```
    Frame Number: 1
    Frame Length: 117 bytes (936 bits)
    Capture Length: 117 bytes (936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b, Dst: 2600:6c56:7ff0:8c00::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 0011 0111 0100 0011 = Flow Label: 0xa3743
    Payload Length: 63
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
    Destination Address: 2600:6c56:7ff0:8c00::1
v User Datagram Protocol, Src Port: 53365, Dst Port: 53
    Source Port: 53365
    Destination Port: 53
    Length: 63
    Checksum: 0xf95e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (55 bytes)
v Domain Name System (query)
    Transaction ID: 0x47e6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 4]
```

5. What is the destination port in the UDP?

The destination port is a number that identifies the specific application that the data is intended for on the receiving device. This allows the receiving device to deliver the data to the correct application.

UDP Destination Port: 53

Wireshark · Packet 1 · Wi-Fi

```
    Frame Number: 1
    Frame Length: 117 bytes (936 bits)
    Capture Length: 117 bytes (936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
  > Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b, Dst: 2600:6c56:7ff0:8c00::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 0011 0111 0100 0011 = Flow Label: 0xa3743
    Payload Length: 63
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
    Destination Address: 2600:6c56:7ff0:8c00::1
v User Datagram Protocol, Src Port: 53365, Dst Port: 53
    Source Port: 53365
    Destination Port: 53
    Length: 63
    Checksum: 0xf95e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (55 bytes)
v Domain Name System (query)
    Transaction ID: 0x47e6
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 4]
```

6. What is the header length?

The header contains information that is required to route the packet through the network. In IPv6, the header length is fixed at 40 bytes unlike in IPv4, where the header length can vary. However, within the IPv6 header, there is a "Payload Length" field that specifies the length of the payload, the payload length field value plus the fixed 40-byte header length will give the total length of the IPv6 packet.

Wireshark · Packet 1 · Assignment1.pcapng

```
Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 26, 2023 19:18:39.296962000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677460719.296962000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 117 bytes (936 bits)
    Capture Length: 117 bytes (936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b, Dst: 2600:6c56:7ff0:8c00::1
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 0011 0111 0100 0011 = Flow Label: 0xa3743
    Payload Length: 63
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
    Destination Address: 2600:6c56:7ff0:8c00::1
User Datagram Protocol, Src Port: 53365, Dst Port: 53
    Source Port: 53365
    Destination Port: 53
    Length: 63
    Checksum: 0xf95e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
    UDP payload (55 bytes)
```

No.: 1 · Time: 0.000000 · Source: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b · Destination: 2600:6c56:7ff0:8c00::1 · Protocol: DNS · Length: 117 · Info: Standard query 0x47e6 AAAA pus6-collabhubrtc.officeapps.live.com

Show packet bytes

UDP Header Length: 63

Wireshark · Packet 1 · Assignment1.pcapng

```
Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{377AE1AA-24E5-473C-9EA9-CD2A866263E0})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 26, 2023 19:18:39.296962000 Central Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677460719.296962000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 117 bytes (936 bits)
    Capture Length: 117 bytes (936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53), Dst: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Destination: Sagemcom_4a:c5:5a (44:ad:b1:4a:c5:5a)
    Source: AzureWav_c9:8f:53 (90:e8:68:c9:8f:53)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b, Dst: 2600:6c56:7ff0:8c00::1
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1010 0011 0111 0100 0011 = Flow Label: 0xa3743
    Payload Length: 63
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b
    Destination Address: 2600:6c56:7ff0:8c00::1
User Datagram Protocol, Src Port: 53365, Dst Port: 53
    Source Port: 53365
    Destination Port: 53
    Length: 63
    Checksum: 0xf95e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
    UDP payload (55 bytes)
```

No.: 1 · Time: 0.000000 · Source: 2600:6c56:7ff0:8c00:459:761f:15f3:5c3b · Destination: 2600:6c56:7ff0:8c00::1 · Protocol: DNS · Length: 117 · Info: Standard query 0x47e6 AAAA pus6-collabhubrtc.officeapps.live.com

Show packet bytes