

Computer Networks - UE23CS252B

4th Semester, Academic Year 2024-25

Lab 3

Exploring UDP with DNS and Sockets using Wireshark

Experiment 3.2: Exploring UDP with Sockets – Wireshark

Date: 10-03-2025

Name: Keerthan P.V	SRN: PES2UG23CS272	Section: 4E
---------------------------	---------------------------	--------------------

Steps to Execute:-

Step 1: Find the IP Addresses

1. Open Command Prompt on both laptops.

2. Run the following command:

ipconfig

```
Command Prompt
Microsoft Windows [Version 10.0.26100.3323]
(c) Microsoft Corporation. All rights reserved.

C:\Users\heert>ipconfig
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\heert>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::811:ed07:5c7f:8339%21
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . : localdomain
    Link-local IPv6 Address . . . . . : fe80::b88a:7957:51be:af7d%2
    IPv4 Address. . . . . : 192.168.70.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix . : localdomain
    Link-local IPv6 Address . . . . . : fe80::2fca:ad9f:7fa7:3b62%19
    IPv4 Address. . . . . : 192.168.208.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . : pdc.local
    Link-local IPv6 Address . . . . . : fe80::d37a:dabc:d6da:4bce%17
    IPv4 Address. . . . . : 10.1.1.217
    Subnet Mask . . . . . : 255.255.248.0
    Default Gateway . . . . . : 10.1.0.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\heert>
```

```
Command Prompt
Microsoft Windows [Version 10.0.26100.3323]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Mahesh Ajjer>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . : pdc.local
    Link-local IPv6 Address . . . . . : fe80::cc0e:450b:51a0:ba5d%14
    IPv4 Address. . . . . : 10.1.2.127
    Subnet Mask . . . . . : 255.255.248.0
    Default Gateway . . . . . : 10.1.0.1

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::6b0f:c65c:acc8:5ff1%7
    IPv4 Address. . . . . : 192.168.91.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

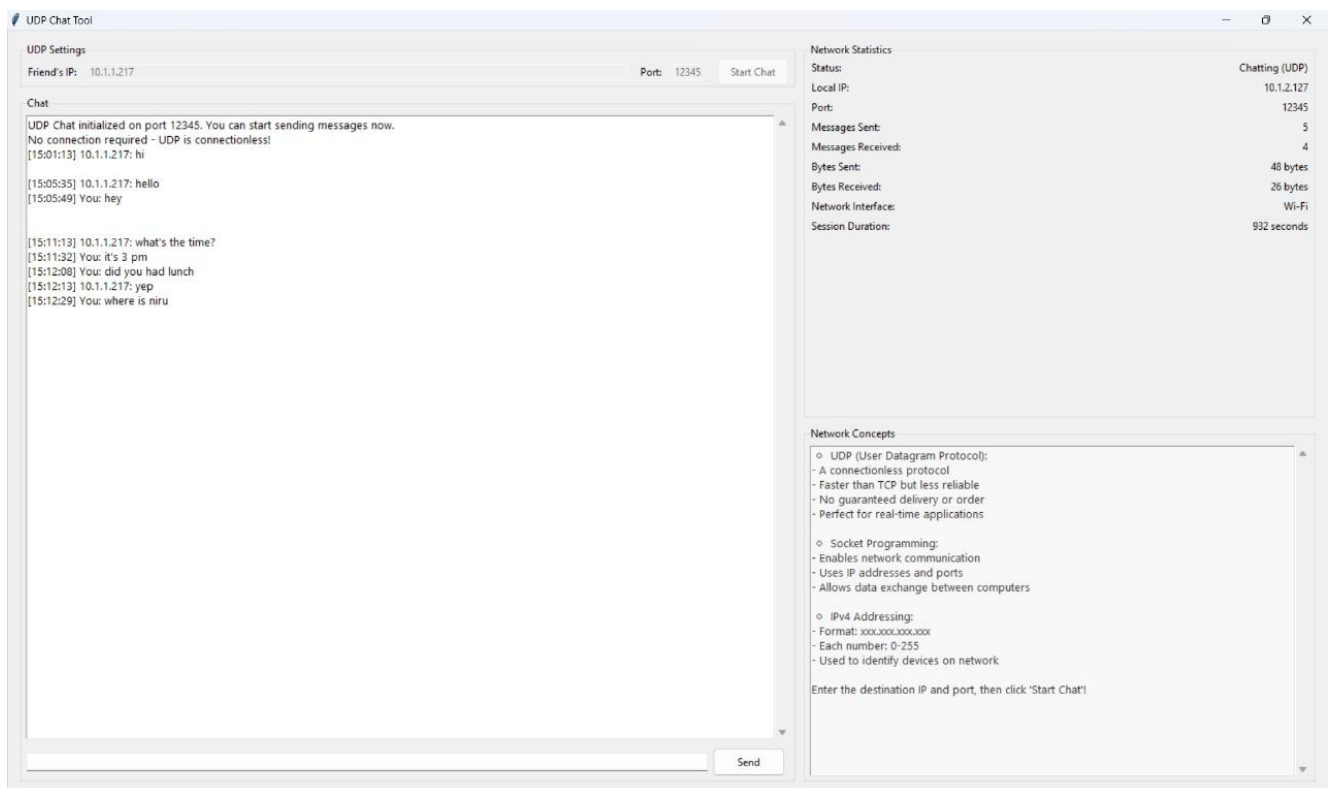
    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::a979:d5fc:66bc:acad%19
    IPv4 Address. . . . . : 192.168.253.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

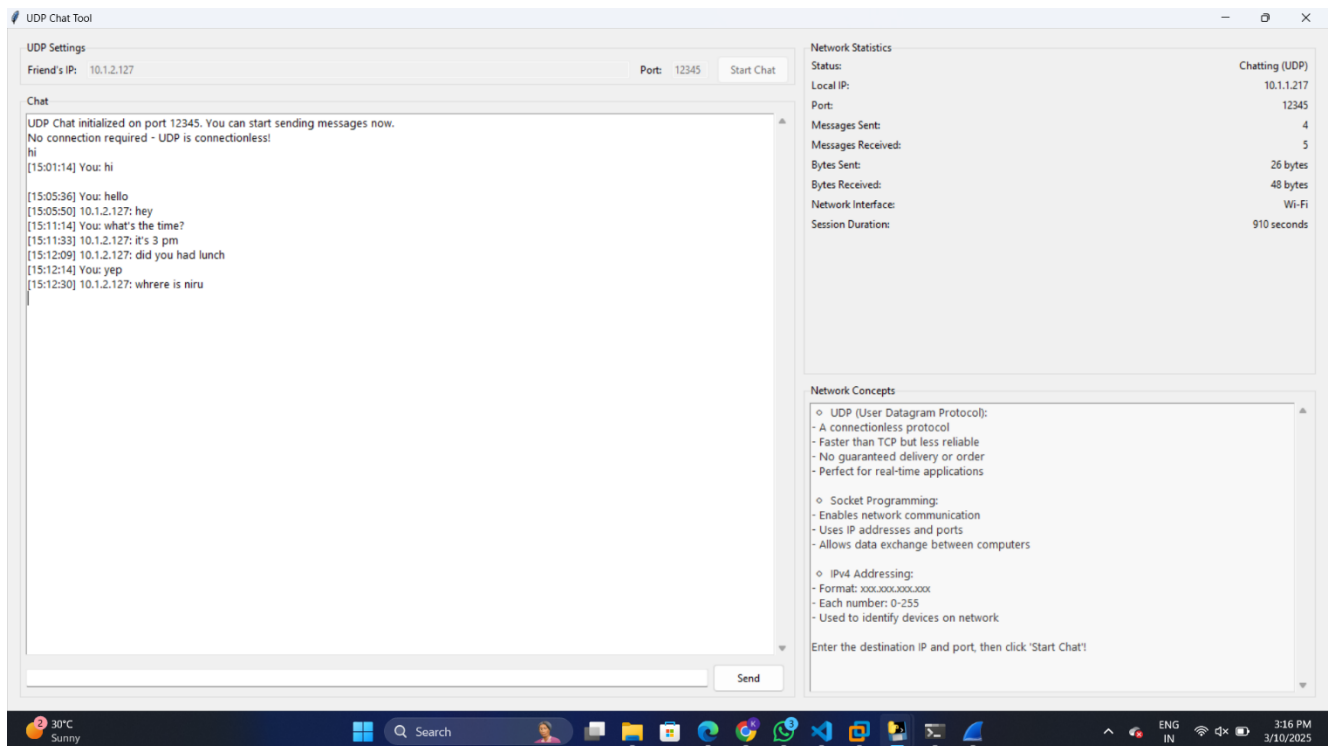
C:\Users\Mahesh Ajjer>
```

3. Note the IPv4 Address (e.g., 192.168.x.x) and share it with the other user.

Step 2: Launch the Chat Application (Make sure to run as Administrator)

1. Open Computer Networks Lab 3 Tool on both laptops.
2. Enter your friend's IPv4 Address in the provided field.
3. Enter the desired Port Number (for example = 12345), make sure both of you both the same port number.
4. Click on Start chat to begin the Chat. 5. Start sending and receiving messages in real-time.





Step 3: Capture UDP Packets in Wireshark

1. Open Wireshark on both laptops.
2. Select the active network adapter (Wi-Fi or Ethernet).
3. Apply the following filter to see only UDP packets related to the chat: `udp.port == (port number of your choice eg:12345)`
4. Start capturing packets and observe the data being transmitted.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 12345

No.	Time	Source	Destination	Protocol	Length	Info
7033	35.431557	10.1.1.217	10.1.2.127	UDP	60	12345 → 12345 Len=5
10063	49.527050	10.1.2.127	10.1.1.217	UDP	45	12345 → 12345 Len=3
68276	373.039492	10.1.1.217	10.1.2.127	UDP	60	12345 → 12345 Len=16
70339	391.996883	10.1.2.127	10.1.1.217	UDP	51	12345 → 12345 Len=9
74802	428.154194	10.1.2.127	10.1.1.217	UDP	59	12345 → 12345 Len=17
75476	433.206640	10.1.1.217	10.1.2.127	UDP	45	12345 → 12345 Len=3
77319	449.522747	10.1.2.127	10.1.1.217	UDP	56	12345 → 12345 Len=14

[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 35.431557000 seconds]
Frame Number: 7033
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocol in frame: ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

▼ Ethernet II, Src: AzureWaveTec_43:78:17 (c0:bf:be:43:78:17), Dst: Intel_e5:98:0e (e0:2e:0b:e5:98:0e)
► Destination: Intel_e5:98:0e (e0:2e:0b:e5:98:0e)
► Source: AzureWaveTec_43:78:17 (c0:bf:be:43:78:17)
Type: IPv4 (0x0800)
[Stream index: 682]
Padding: 00000000000000000000000000000000

▼ Internet Protocol Version 4, Src: 10.1.1.217, Dst: 10.1.2.127
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 33
Identification: 0x9998 (39320)
► 000. = Flags: 0x0
0.0000.0000.0000 = Fragment Offset: 0

0000 c0 2e 0b e5 98 0e c0 bf be 43 78 17 08 00 45 00 ...C...E
0010 00 21 99 98 00 00 80 11 88 da 0a 01 01 d9 0a 01 ...I...
0020 02 7f 30 39 30 39 00 0d 43 36 68 65 6c 6c 6f 00 ...0909...Cshello
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Data (data), 5 bytes

Packets: 95173 · Displayed: 7 (0.0%) Profile: Default

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 12345

No.	Time	Source	Destination	Protocol	Length	Info
7033	35.431557	10.1.1.217	10.1.2.127	UDP	60	12345 → 12345 Len=5
10063	49.527050	10.1.2.127	10.1.1.217	UDP	45	12345 → 12345 Len=3
68276	373.039492	10.1.1.217	10.1.2.127	UDP	60	12345 → 12345 Len=16
70339	391.996883	10.1.2.127	10.1.1.217	UDP	51	12345 → 12345 Len=9
74802	428.154194	10.1.2.127	10.1.1.217	UDP	59	12345 → 12345 Len=17
75476	433.206640	10.1.1.217	10.1.2.127	UDP	45	12345 → 12345 Len=3
77319	449.522747	10.1.2.127	10.1.1.217	UDP	56	12345 → 12345 Len=14

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 45
Identification: 0x0420 (1056)
► 000. = Flags: 0x0
0.0.0000.0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.2.127
Destination Address: 10.1.1.217
[Stream index: 390]

▼ User Datagram Protocol, Src Port: 12345, Dst Port: 12345
Source Port: 12345
Destination Port: 12345
Length: 25
Checksum: 0x1884 [unverified]
[Checksum Status: Unverified]
[Stream index: 891]
[Stream Packet Number: 5]
► [Timestamps]
UDP payload (17 bytes)

▼ Data (17 bytes)
Data: 66064708f7c70b8c16a706c756c6368

0000 c0 bf be 43 78 17 e0 2e 0b e5 98 0e 00 00 45 00 ...C...E
0010 00 2d 04 20 00 00 80 11 00 00 0a 01 02 7f 0a 01 ...I...
0020 01 d9 30 39 30 39 00 19 18 84 64 69 64 20 79 6f ...0909...did yo
0030 75 20 68 61 64 20 6c 75 6e 63 68 u had lu nch

wireshark-Wi-Fi\CD02.pcapng

Packets: 101013 · Displayed: 7 (0.0%) Profile: Default

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 12345

No.	Time	Source	Destination	Protocol	Length	Info
7833	35.431557	10.1.1.217	10.1.2.127	UDP	60	12345 → 12345 Len=5
10063	49.527050	10.1.2.127	10.1.1.217	UDP	45	12345 → 12345 Len=3

[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 35.431557000 seconds]
Frame Number: 7833
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

▼ Ethernet II, Src: AzureWaveTec_43:78:17 (c0:bf:be:43:78:17), Dst: Intel_e5:98:0e (e0:2e:0b:e5:98:0e)
► Destination: Intel_e5:98:0e (e0:2e:0b:e5:98:0e)
► Source: AzureWaveTec_43:78:17 (c0:bf:be:43:78:17)
Type: IPv4 (0x0800)
[Stream index: 682]
Padding: 00000000000000000000000000000000

▼ Internet Protocol Version 4, Src: 10.1.1.217, Dst: 10.1.2.127
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 33
Identification: 0x9998 (39320)
► 000 = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to live: 128
Protocol: UDP (17)
Header Checksum: 0x88da [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.1.217
Destination Address: 10.1.2.127
[Stream index: 358]

▼ User Datagram Protocol, Src Port: 12345, Dst Port: 12345
Source Port: 12345
Destination Port: 12345
Length: 13
Checksum: 0x4336 [unverified]
[Checksum Status: Unverified]
[Stream index: 891]
[Stream Packet Number: 1]
► [Timestamps]
UDP payload (5 bytes)

▼ Data (5 bytes)
Data: 68656c6c6f
[Length: 5]

Data (data), 5 bytes

Packets: 32528 - Displayed: 2 (0.0%) Profile: Default

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 12345

No.	Time	Source	Destination	Protocol	Length	Info
7937	38.929526	10.1.1.217	10.1.2.127	UDP	47	12345 → 12345 Len=5
10767	53.034740	10.1.1.217	10.1.1.217	UDP	60	12345 → 12345 Len=3
69801	376.517420	10.1.1.217	10.1.2.127	UDP	58	12345 → 12345 Len=16
71178	395.534284	10.1.1.217	10.1.1.217	UDP	60	12345 → 12345 Len=9
76010	431.671066	10.1.1.217	10.1.1.217	UDP	60	12345 → 12345 Len=17
76751	436.710605	10.1.1.217	10.1.2.127	UDP	45	12345 → 12345 Len=3
78668	453.035691	10.1.1.217	10.1.1.217	UDP	60	12345 → 12345 Len=14

[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]

▼ Ethernet II, Src: Intel_e5:98:0e (e0:2e:0b:e5:98:0e), Dst: AzureWaveTec_43:78:17 (c0:bf:be:43:78:17)
► Destination: AzureWaveTec_43:78:17 (c0:bf:be:43:78:17)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
► Source: Intel_e5:98:0e (e0:2e:0b:e5:98:0e)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 698]
Padding: 00

▼ Internet Protocol Version 4, Src: 10.1.2.127, Dst: 10.1.1.217
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 45
Identification: 0x0420 (1056)
► 000 = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to live: 128
Protocol: UDP (17)
Header Checksum: 0x1e47 [validation disabled]
[Header checksum status: Unverified]

wireshark-Wi-Fi-C8B22-pcapng

Packets: 106602 - Displayed: 7 (0.0%) Profile: Default

