

Student name: Albert Nguyen

Email: anguy223@uwo.ca

Student number : 251098912

Below you can see a link to the UDP server test video as well as a screen shot of the wireshark analysis from the recorded video.

<https://youtu.be/pxTxKb8K3SA>

Wireshark · Packet 7 · Adapter for loopback traffic capture

```
▼ Frame 7: 51 bytes on wire (408 bits), 51 bytes captured (408 bits) on interface \Device\NPF_{Loopback}, id 0
  Section number: 1
  > Interface id: 0 (\Device\NPF_{Loopback})
  Encapsulation type: NULL/Loopback (15)
  Arrival Time: Oct 19, 2023 18:23:45.823690000 Eastern Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1697754225.823690000 seconds
  [Time delta from previous captured frame: 0.000628000 seconds]
  [Time delta from previous displayed frame: 0.000628000 seconds]
  [Time since reference or first frame: 21.984801000 seconds]
  Frame Number: 7
  Frame Length: 51 bytes (408 bits)
  Capture Length: 51 bytes (408 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: null:ip:udp:data]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
▼ Null/Loopback
  Family: IP (2)
▼ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 47
  Identification: 0x77e1 (30689)
  > 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: 127.0.0.1
  Destination Address: 127.0.0.1
▼ User Datagram Protocol, Src Port: 12345, Dst Port: 57525
  Source Port: 12345
  Destination Port: 57525
  Length: 27
  Checksum: 0xa57f [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  UDP payload (19 bytes)
▼ Data (19 bytes)
  Data: 616c626572743a2020686920616c6578697321
  [Length: 19]
```

```
0000  02 00 00 00 45 00 00 2f 77 e1 00 00 80 11 00 00  ....E../w.....
0010  7f 00 00 01 7f 00 00 01 30 39 e0 b5 00 1b a5 7f  ....09.....
0020  61 6c 62 65 72 74 3a 20 20 68 69 20 61 6c 65 78  albert: hi alex
0030  69 73 21                                     is!
```

☒ Show packet bytes

Below you can see a link to the TCP server test video as well as a screen shot of the wireshark analysis from the recorded video.

<https://youtu.be/uCsMirdR8dl>

Wireshark · Packet 17 · Adapter for loopback traffic capture

```
[Time since reference or first frame: 23.805771000 seconds]
Frame Number: 17
Frame Length: 52 bytes (416 bits)
Capture Length: 52 bytes (416 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: null:ip:tcp:data]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
▼ Null/Loopback
  Family: IP (2)
▼ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x78d4 (30932)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 127.0.0.1
    Destination Address: 127.0.0.1
▼ Transmission Control Protocol, Src Port: 57649, Dst Port: 12345, Seq: 10, Ack: 9, Len: 8
  Source Port: 57649
  Destination Port: 12345
  [Stream index: 0]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 8]
  Sequence Number: 10 (relative sequence number)
  Sequence Number (raw): 2287492134
  [Next Sequence Number: 18 (relative sequence number)]
  Acknowledgment Number: 9 (relative ack number)
  Acknowledgment number (raw): 87176312
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 10233
    [Calculated window size: 2619648]
    [Window size scaling factor: 256]
    Checksum: 0xece3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

0000	02 00 00 00 45 00 00 30	78 d4 40 00 80 06 00 00	....E..0 x.@..
0010	7f 00 00 01 7f 00 00 01	e1 31 30 39 88 58 5c 26	.....109.X\&
0020	05 32 34 78 50 18 27 f9	ec e3 00 00 68 69 20 61	·24xP·'·...hi a
0030	6c 65 78 21		lex!

☒ Show packet bytes

Analysis: Comparing the UDP parameters to the TCP parameters we can see many similarities. For example, both TCP and UDP use source and destination port numbers in their headers. Wireshark displays these port numbers for both protocols. Both TCP and UDP transport application data so you can see the actual data payload being transmitted for both protocols. The main difference you can see in TCP is that it has parameters like sequence number, relative sequence number, and next sequence number while UDP doesn't. This is because packets in a TCP stream are sequenced and numbered while UDP packets aren't. TCP also implements flow control which you wouldn't see in UDP.