

## TCP COMMUNICATION ANALYSIS

### Part 1:

#### 1. The messages:

The screenshot shows two terminal windows in VS Code. The top terminal window displays the execution of the server code and its interaction with a client. The bottom terminal window displays the execution of the client code and its interaction with the server.

**Top Terminal (Server Side):**

```
tcp_server.py > ...
1  import socket
2  server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
3  server.bind(('', 12345))
4  server.listen(5)
5
6  while True:
7      client_socket, client_address = server.accept()
8      print('Connection from: ', client_address)
9      data = client_socket.recv(100)
10     print('Received: ', data)
11     client_socket.send(data.upper())
12     data = client_socket.recv(100)
13     print('Received: ', data)
14     client_socket.send(data.upper())
15     client_socket.close()
16     print('Client disconnected')
```

Output:

```
PS C:\net2> c;; cd 'c:\net2'; & 'c:\Users\User\AppData\Local\Python\pythoncore-3.14-64\python.exe' 'c:\Users\User\.vscode\extensions\ms-python.debugpy-2025.18.0-win32-x64\bundled\libs\debugpy\launcher' '59957' '--' 'c:\net2\tcp_server.py'
Connection from: ('192.168.1.224', 54962)
Received: b'Noya Shindler and Oscar Stilogalo'
Received: b'2152162849 327613030'
Client disconnected
```

**Bottom Terminal (Client Side):**

```
tcp_client.py > ...
1  import socket
2  s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
3  s.connect(('192.168.1.221', 12345))
4  s.send(b'Noya Shindler and Oscar Stilogalo')
5  data = s.recv(100)
6  print("Server sent: ", data)
7  s.send(b'2152162849 327613030')
8  data = s.recv(100)
9  print("Server sent: ", data)
10 s.close()
```

Output:

```
PS O:\net2> o;; cd 'o:\net2'; & 'c:\Users\oscar\AppData\Local\Programs\Python\Python313\python.exe' 'c:\Users\oscar\.vscode\extensions\ms-python.debugpy-2025.18.0-win32-x64\bundled\libs\debugpy\launcher' '54958' '--' 'o:\net2\tcp_client.py'
Server sent: b'NOYA SHINDLER AND OSCAR STILOGALO'1ff1-dice-4149-afe8-149b3dbc09a
Server sent: b'2152162849 327613030'
PS O:\net2>
```

## 2. Wireshark

First message- client to server (224->221) only syn flag asks to make a connection

Sequence Number (raw): 1928250445 – where the stack starts

No.	Time	Source	Destination	Protocol	Length	Info
25	3.763688	192.168.1.224	192.168.1.221	TCP	66	54962 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

```

> Frame 25: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: ASRock_Incorp_a9:3f:73 (9c:6b:00:a9:3f:73), Dst: Intel Pro/100 MT Desktop (08:00:27:00:00:00)
> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.221
> Transmission Control Protocol, Src Port: 54962, Dst Port: 12345, Seq: 0
    Source Port: 54962
    Destination Port: 12345
    [Stream index: 7]
    [Stream Packet Number: 1]
    > Conversation completeness: Complete, WITH_DATA (31)
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Sequence Number (raw): 1928250445
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x002 (SYN)
        000. .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0.... .... = Congestion Window Reduced: Not set
        .... .0.... .... = ECN-Echo: Not set
        .... .0.... .... = Urgent: Not set
        .... 0.... .... = Acknowledgment: Not set
        .... 0.... .... = Push: Not set
        .... .0.... .... = Reset: Not set
        > .... .... .1. = Syn: Set
        .... .... 0 = Fin: Not set
    [TCP Flags: -----S-]

```

Second message- server to client (221->224), 2rd part of 3 part handshake,  
 Acknowledgment number (raw): 1928250446 for one bit after the seq in the client  
 for syn the client sent.

Sequence Number (raw): 2757540237: which is where the stack starts for the server

No.	Time	Source	Destination	Protocol	Length	Info
123	2.982234	192.168.1.224	192.168.1.221	TCP	66	54962 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
124	2.982344	192.168.1.224	192.168.1.221	TCP	66	12345 → 54962 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

< Internet Protocol Version 4, Src: 192.168.1.221, Dst: 192.168.1.224  
 Transmission Control Protocol, Src Port: 12345, Dst Port: 54962, Seq: 1  
 Source Port: 12345  
 Destination Port: 54962  
 [Stream index: 5]  
 [Stream Packet Number: 2]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 2757540237  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 1 (relative ack number)  
 Acknowledgment number (raw): 1928250446  
 1000 .... = Header Length: 32 bytes (8)  
 Flags: 0x012 (SYN, ACK)  
 000.... .... = Reserved: Not set  
 ...0.... .... = Accurate ECN: Not set  
 ...8.... .... = Congestion Window Reduced: Not set  
 ....0.... .... = ECN-Echo: Not set  
 ....0.... .... = Urgent: Not set  
 ....1.... .... = Acknowledgment: Set  
 ....0.... .... = Push: Not set  
 ....0.... .... = Reset: Not set  
 > ....1.... = Syn: Set  
 ....0.... = Fin: Not set  
 [TCP Flags: A-S]  
 Window: 65535  
 [Calculated window size: 65535]

This shows the raw value of the sequence number (tcp.seq.raw), 4 bytes

Packets: 177 - Displayed: 11 (6.2%)

Profile: Default

Third message- client to server (224->221),3rd part of 3part handshake only ack flag sets both server and Acknowledgment number (raw): 2757540238 for the 1 bit of syn

No.	Time	Source	Destination	Protocol	Length	Info
123	2.982234	192.168.1.224	192.168.1.221	TCP	66	54962 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
124	2.982344	192.168.1.221	192.168.1.224	TCP	66	12345 → 54962 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
125	2.985258	192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [ACK] Seq=1 Ack=1 Win=262656 Len=0

< Internet Protocol Version 4, Src: 192.168.1.221, Dst: 192.168.1.224  
 Transmission Control Protocol, Src Port: 12345, Dst Port: 54962, Seq: 1  
 Source Port: 12345  
 Destination Port: 54962  
 [Stream index: 5]  
 [Stream Packet Number: 3]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 Acknowledgment Number: 1 (relative ack number)  
 Acknowledgment number (raw): 2757540238  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x010 (ACK)  
 000.... .... = Reserved: Not set  
 ...0.... .... = Accurate ECN: Not set  
 ...0.... .... = Congestion Window Reduced: Not set  
 ....0.... .... = ECN-Echo: Not set  
 ....0.... .... = Urgent: Not set  
 ....1.... .... = Acknowledgment: Set  
 ....0.... .... = Push: Not set  
 ....0.... .... = Reset: Not set  
 ....0.... .... = Syn: Not set  
 ....0.... .... = Fin: Not set  
 [TCP Flags: A]  
 Window: 1024  
 [Calculated window size: 262656]  
 [Window size scaling factor: 256]  
 Checksum: 0xBab0 [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 > [Timestamps]  
 > [SEQ/ACK analysis]  
 > [Client Contiguous Streams: 1]  
 > [Server Contiguous Streams: 1]

Acknowledgment (tcp.flags.ack), 1 bit

Packets: 177 - Displayed: 11 (6.2%)

Profile: Default

Forth message- client to server (224->221), sent the names with ack and psh flag Ack is at 1(dynamically) because that's where we start the ack list, note that msg len is 33

No.	Time	Source	Destination	Protocol	Length	Info
123 2.982234		192.168.1.224	192.168.1.221	TCP	66	54962 → 12345 [SYN] Seq=0 Win=64400 MSS=1460 WS=256 SACK_PERM
124 2.982344		192.168.1.221	192.168.1.224	TCP	66	12345 → 54962 [SYN, ACK] Seq=0 Ack=1 Win=65535 MSS=1460 WS=256 SACK_PERM
125 2.985258		192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [ACK] Seq=1 Ack=1 Win=262656 Len=0
126 2.987040		192.168.1.224	192.168.1.221	TCP	87	54962 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=33

[Next Sequence Number: 34 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 2757540238  
0101 .... = Header Length: 28 bytes (5)  
Flags: 0x018 (PSH, ACK)  
000 ..... = Reserved: Not set  
...0 ..... = Accurate ECN: Not set  
....0.... = Congestion Window Reduced: Not set  
....0.... = ECN-Echo: Not set  
....0.... = Urgent: Not set  
....1.... = Acknowledgment: Set  
.....1.. = Push: Set  
.....0.. = Reset: Not set  
.....0.. = Syn: Not set  
.....0.. = Fin: Not set  
[TCP Flags: .....AP...]  
Window: 1026  
[Calculated window size: 262656]  
[Window size scaling factor: 256]  
Checksum: 0x85d7 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
[Client Contiguous Streams: 1]  
[Server Contiguous Streams: 1]

Acknowledgment (tcp.flags.ack).1 bit

Packets: 177 - Displayed: 11 (6.2%)

Profile: Default

Fifth message- server to client (221->224), sent Acknowledgment number (raw): 1928250479 (meaning took all the 79-46 = 33 len of the msg) and sent together its response which as well has len 33

Sequence Number (raw): 2757540238 is still at the start

No.	Time	Source	Destination	Protocol	Length	Info
123 2.982234		192.168.1.224	192.168.1.221	TCP	66	54962 → 12345 [SYN] Seq=0 Win=64400 MSS=1460 WS=256 SACK_PERM
124 2.982344		192.168.1.221	192.168.1.224	TCP	66	12345 → 54962 [SYN, ACK] Seq=0 Ack=1 Win=65535 MSS=1460 WS=256 SACK_PERM
125 2.985258		192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [ACK] Seq=1 Ack=1 Win=262656 Len=0
126 2.987040		192.168.1.224	192.168.1.221	TCP	87	54962 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=33
127 2.987690		192.168.1.221	192.168.1.224	TCP	87	12345 → 54962 [PSH, ACK] Seq=1 Ack=34 Win=1049600 Len=33

[Next Sequence Number: 34 (relative sequence number)]  
Acknowledgment Number: 34 (relative ack number)  
Acknowledgment number (raw): 1928250479  
0101 .... = Header Length: 28 bytes (5)  
Flags: 0x018 (PSH, ACK)  
000 ..... = Reserved: Not set  
...0 ..... = Accurate ECN: Not set  
....0.... = Congestion Window Reduced: Not set  
....0.... = ECN-Echo: Not set  
....0.... = Urgent: Not set  
....1.... = Acknowledgment: Set  
.....1.. = Push: Set  
.....0.. = Reset: Not set  
.....0.. = Syn: Not set  
.....0.. = Fin: Not set  
[TCP Flags: .....AP...]  
Window: 4100  
[Calculated window size: 1049600]  
[Window size scaling factor: 256]  
Checksum: 0x8549 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
[Client Contiguous Streams: 1]

Acknowledgment (tcp.flags.ack).1 bit

Display: 177 - Filtered: 11 (6.2%)

Profile: Default

Sixth message- client to server (224->221), sent Acknowledgment number (raw): 2757540271  
 (meaning took all the 71 -38 = 33 len of the msg) and sent the ids which have len 20

Acknowledgment number (raw): 2757540271 still after the 33 + 1 bits

No.	Time	Source	Destination	Protocol	Length	Info
123	2.902234	192.168.1.224	192.168.1.221	TCP	66	54962 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 WS=256 SACK_PERM
124	2.902344	192.168.1.221	192.168.1.224	TCP	66	12345 → 54962 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1468 WS=256 SACK_PERM
125	2.905258	192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [ACK] Seq=1 Ack=1 Win=262656 Len=0
126	2.907840	192.168.1.224	192.168.1.221	TCP	87	54962 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=33
127	2.907690	192.168.1.221	192.168.1.224	TCP	87	12345 → 54962 [PSH, ACK] Seq=1 Ack=34 Win=1049600 Len=33
130	2.981978	192.168.1.224	192.168.1.221	TCP	74	54962 → 12345 [PSH, ACK] Seq=34 Ack=34 Win=262656 Len=20

[Next Sequence Number: 54 (relative sequence number)]  
 Acknowledgment Number: 34 (relative ack number)  
 Acknowledgment number (raw): 2757540271  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x018 (PSH, ACK)  
 ...0.... .... = Reserved: Not set  
 ...B.... .... = Accurate ECN: Not set  
 ...0.... .... = Congestion Window Reduced: Not set  
 ...0.... .... = ECN-Echo: Not set  
 ...0.... .... = Urgent: Not set  
 ....1.... = Acknowledgment: Set  
 ....1.... = Push: Set  
 ....0.... = Reset: Not set  
 ....0.... = Syn: Not set  
 ....0.... = Fin: Not set  
 [TCP Flags: .....AP...]  
 Window: 1026  
 [Calculated window size: 262656]  
 [Window size scaling factor: 256]  
 Checksum: 0x9c4b [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 [Timestamps]  
 [SEO/ACK analysis]

Packets: 177 - Displayed: 11 (6.2%) Profile: Default

Seventh message- server to client (221->224), sent Acknowledgment number (raw): 1928250499  
 (1928250445+1+33+20) and sent the message back

No.	Time	Source	Destination	Protocol	Length	Info
123	2.902234	192.168.1.224	192.168.1.221	TCP	66	54962 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 WS=256 SACK_PERM
124	2.902344	192.168.1.221	192.168.1.224	TCP	66	12345 → 54962 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1468 WS=256 SACK_PERM
125	2.905258	192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [ACK] Seq=1 Ack=1 Win=262656 Len=0
126	2.907840	192.168.1.224	192.168.1.221	TCP	87	54962 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=33
127	2.907690	192.168.1.221	192.168.1.224	TCP	87	12345 → 54962 [PSH, ACK] Seq=1 Ack=34 Win=1049600 Len=33
130	2.981978	192.168.1.224	192.168.1.221	TCP	74	54962 → 12345 [PSH, ACK] Seq=34 Ack=34 Win=262656 Len=20
131	2.982750	192.168.1.221	192.168.1.224	TCP	74	12345 → 54962 [PSH, ACK] Seq=34 Ack=54 Win=1049600 Len=20

[TCP Segment Len: 28]  
 Sequence Number: 34 (relative sequence number)  
 Sequence Number (raw): 2757540271  
 [Next Sequence Number: 54 (relative sequence number)]  
 Acknowledgment Number: 54 (relative ack number)  
 Acknowledgment number (raw): 1928250499  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x018 (PSH, ACK)  
 ...0.... .... = Reserved: Not set  
 ...0.... .... = Accurate ECN: Not set  
 ...0.... .... = Congestion Window Reduced: Not set  
 ...0.... .... = ECN-Echo: Not set  
 ...0.... .... = Urgent: Not set  
 ....1.... = Acknowledgment: Set  
 ....1.... = Push: Set  
 ....0.... = Reset: Not set  
 ....0.... = Syn: Not set  
 ....0.... = Fin: Not set  
 [TCP Flags: .....AP...]  
 Window: 4108  
 [Calculated window size: 1049600]  
 [Window size scaling factor: 256]  
 Checksum: 0x853c [unverified]

This shows the raw value of the acknowledgment number (tcp.ack\_raw). 4 bytes

Packets: 177 - Displayed: 11 (6.2%) Profile: Default

Eight message- server to client (221->224), asking to close connection Fin flag up part 1 of 4 part handshake, this happened before client could give ack for the server msg

Sequence Number (raw): 2757540291 – even though we didn't get ack till here because client didn't send ack yet

No.	Time	Source	Destination	Protocol	Length	Info
123	2.902234	192.168.1.224	192.168.1.221	TCP	66	54962 + 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
124	2.902344	192.168.1.221	192.168.1.224	TCP	66	12345 + 54962 [SYN, ACK] Seq=8 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
125	2.905258	192.168.1.224	192.168.1.221	TCP	54	54962 + 12345 [ACK] Seq=1 Ack=1 Win=262656 Len=0
126	2.907040	192.168.1.224	192.168.1.221	TCP	87	54962 + 12345 [PSH, ACK] Seq=1 Ack=34 Win=262656 Len=33
127	2.907690	192.168.1.221	192.168.1.224	TCP	87	12345 + 54962 [PSH, ACK] Seq=1 Ack=34 Win=1049600 Len=33
130	2.981978	192.168.1.224	192.168.1.221	TCP	74	54962 + 12345 [PSH, ACK] Seq=34 Ack=34 Win=262656 Len=20
131	2.982750	192.168.1.221	192.168.1.224	TCP	74	12345 + 54962 [PSH, ACK] Seq=34 Ack=54 Win=1049600 Len=20
132	2.982881	192.168.1.223	192.168.1.224	TCP	54	12345 + 54962 [FIN, ACK] Seq=54 Ack=54 Win=1049600 Len=0

[Stream Packet Number: 8]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 0]  
 Sequence Number: 54 (relative sequence number)  
 Sequence Number (raw): 2757540291  
 [Next Sequence Number: 55 (relative sequence number)]  
 Acknowledgment Number: 54 (relative ack number)  
 Acknowledgment number (raw): 1928250499  
 0x01 .... = Header Length: 20 bytes (5)  
 Flags: 0x011 (FIN, ACK)  
 000.... = Reserved: Not set  
 ...0.... = Accurate ECN: Not set  
 ...0.... = Congestion Window Reduced: Not set  
 ...0.... = ECN-Echo: Not set  
 ...0.... = Urgent: Not set  
 ....1.... = Acknowledgment: Set  
 ....0.... = Push: Not set  
 ....0.... = Reset: Not set  
 ....0.... = Syn: Not set  
 > .....1 = Fin: Set  
 > [TCP Flags: .....A---F]  
 Window: 4100

Ninth message- client to server (224->221), part 3 of 4 part handshake client didn't receive fin yet but it started to close the connection itself with Acknowledgment number (raw): 2757540291 (meaning it got the last 20)

No.	Time	Source	Destination	Protocol	Length	Info
130	2.981978	192.168.1.224	192.168.1.221	TCP	74	54962 + 12345 [PSH, ACK] Seq=34 Ack=34 Win=262656 Len=20
131	2.982750	192.168.1.221	192.168.1.224	TCP	74	12345 + 54962 [PSH, ACK] Seq=34 Ack=54 Win=1049600 Len=20
132	2.982881	192.168.1.221	192.168.1.224	TCP	54	12345 + 54962 [FIN, ACK] Seq=54 Ack=54 Win=1049600 Len=0
133	1.998526	192.168.1.224	192.168.1.221	TCP	68	54962 + 12345 [FIN, ACK] Seq=54 Ack=54 Win=262656 Len=0

[Stream Packet Number: 9]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 0]  
 Sequence Number: 54 (relative sequence number)  
 Sequence Number (raw): 1928250499  
 [Next Sequence Number: 55 (relative sequence number)]  
 Acknowledgment Number: 54 (relative ack number)  
 Acknowledgment number (raw): 2757540291  
 0x01 .... = Header Length: 20 bytes (5)  
 Flags: 0x011 (FIN, ACK)  
 000.... = Reserved: Not set  
 ...0.... = Accurate ECN: Not set  
 ...0.... = Congestion Window Reduced: Not set  
 ...0.... = ECN-Echo: Not set  
 ...0.... = Urgent: Not set  
 ....1.... = Acknowledgment: Set  
 ....0.... = Push: Not set  
 ....0.... = Reset: Not set  
 ....0.... = Syn: Not set  
 > .....1 = Fin: Set  
 > [TCP Flags: .....A---F]  
 Window: 1826  
 [Calculated window size: 262656]  
 [Window size scaling factor: 256]  
 Checksum: 0x8d45 [unverified]  
 [Checksum Status: Unverified]

Tenth message- server to client (221->224 ), part 4 of 4 part handshake client received server ack to close connection so it can close the connection now

No.	Time	Source	Destination	Protocol	Length	Info
130	2.981978	192.168.1.224	192.168.1.221	TCP	74	54962 → 12345 [PSH, ACK] Seq=34 Ack=34 Win=262656 Len=20
131	2.982750	192.168.1.221	192.168.1.224	TCP	74	12345 → 54962 [PSH, ACK] Seq=34 Ack=34 Win=1049600 Len=20
132	2.982881	192.168.1.221	192.168.1.224	TCP	54	12345 → 54962 [FIN, ACK] Seq=54 Ack=54 Win=1049600 Len=0
133	2.998526	192.168.1.224	192.168.1.221	TCP	60	54962 → 12345 [FIN, ACK] Seq=54 Ack=54 Win=262656 Len=0
134	2.998601	192.168.1.221	192.168.1.224	TCP	54	12345 → 54962 [ACK] Seq=55 Ack=55 Win=1049600 Len=0

[Stream Packer Number: 10]  
> [Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 55 (relative sequence number)  
Sequence Number (raw): 2757540292  
[Next Sequence Number: 55 (relative sequence number)]  
Acknowledgment Number: 55 (relative ack number)  
Acknowledgment number (raw): 1928250500  
0101 .... = Header Length: 20 bytes (5)  
▼ Flags: 0x010 (ACK)  
  000.... = Reserved: Not set  
  ...0.... = Accurate ECN: Not set  
  ....0.... = Congestion Window Reduced: Not set  
  ....0.... = ECN-Echo: Not set  
  ....0.... = Urgent: Not set  
  ....1.... = Acknowledgment: Set  
  ....0.... = Push: Not set  
  ....0.... = Reset: Not set  
  ....0.... = Syn: Not set  
  ....0.... = Fin: Not set  
[TCP Flags: .....A....]  
Window: 4108  
[Calculated window size: 1049600]  
[Window size scaling factor: 256]  
Checksum: 0x8528 [unverified]

Packets: 177 - Displayed: 11 (6.2%) | Profile: Default

Final message- client to server (224->221),part 2 of 4 part handshake server received ack for fin and now can close connection

No.	Time	Source	Destination	Protocol	Length	Info
123	2.982234	192.168.1.224	192.168.1.221	TCP	68	54962 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1468 WS=256 SACK_PERM
124	2.982344	192.168.1.221	192.168.1.224	TCP	68	12345 → 54962 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1468 WS=256 SACK_PERM
125	2.982528	192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [ACK] Seq=1 Ack=1 Win=262656 Len=0
126	2.987040	192.168.1.224	192.168.1.221	TCP	87	54962 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=33
127	2.987698	192.168.1.221	192.168.1.224	TCP	87	12345 → 54962 [PSH, ACK] Seq=1 Ack=34 Win=1049600 Len=33
130	2.981978	192.168.1.224	192.168.1.221	TCP	74	54962 → 12345 [PSH, ACK] Seq=34 Ack=34 Win=262656 Len=20
131	2.982750	192.168.1.221	192.168.1.224	TCP	74	12345 → 54962 [PSH, ACK] Seq=34 Ack=34 Win=1049600 Len=20
132	2.982881	192.168.1.221	192.168.1.224	TCP	54	12345 → 54962 [FIN, ACK] Seq=54 Ack=54 Win=1049600 Len=0
133	2.998526	192.168.1.224	192.168.1.221	TCP	60	54962 → 12345 [FIN, ACK] Seq=54 Ack=54 Win=262656 Len=0
134	2.998601	192.168.1.221	192.168.1.224	TCP	54	12345 → 54962 [ACK] Seq=55 Ack=55 Win=1049600 Len=0
135	3.003159	192.168.1.224	192.168.1.221	TCP	68	54962 → 12345 [ACK] Seq=55 Ack=55 Win=262656 Len=0

> [Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 55 (relative sequence number)  
Sequence Number (raw): 1928250500  
[Next Sequence Number: 55 (relative sequence number)]  
Acknowledgment Number: 55 (relative ack number)  
Acknowledgment number (raw): 2757540292  
0101 .... = Header Length: 20 bytes (5)  
▼ Flags: 0x010 (ACK)  
  000.... = Reserved: Not set  
  ...0.... = Accurate ECN: Not set  
  ....0.... = Congestion Window Reduced: Not set  
  ....0.... = ECN-Echo: Not set  
  ....0.... = Urgent: Not set  
  ....1.... = Acknowledgment: Set  
  ....0.... = Push: Not set  
  ....0.... = Reset: Not set  
  ....0.... = Syn: Not set  
  ....0.... = Fin: Not set  
[TCP Flags: .....A....]  
Packets: 177 - Displayed: 11 (6.2%) | Profile: Default

## Part 2:

1. We will demonstrate the **keep alive** functionality using single\_fin and double\_fin files

**Single\_fin-** here I opened the default linkage of index.html and quickly refreshed as to demonstrate the keep alive (in practice chrome opens 2 ports for every request so I actually had to make python client to do this with the same port)

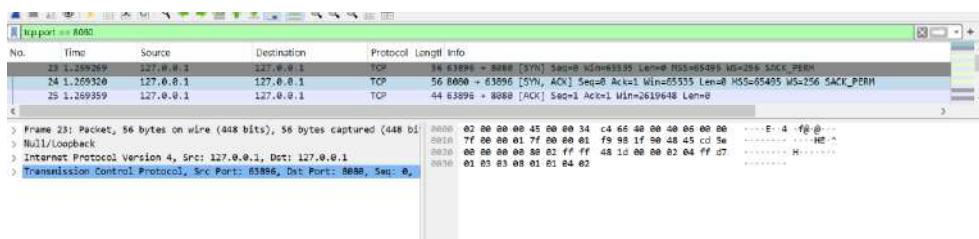


### Hello World

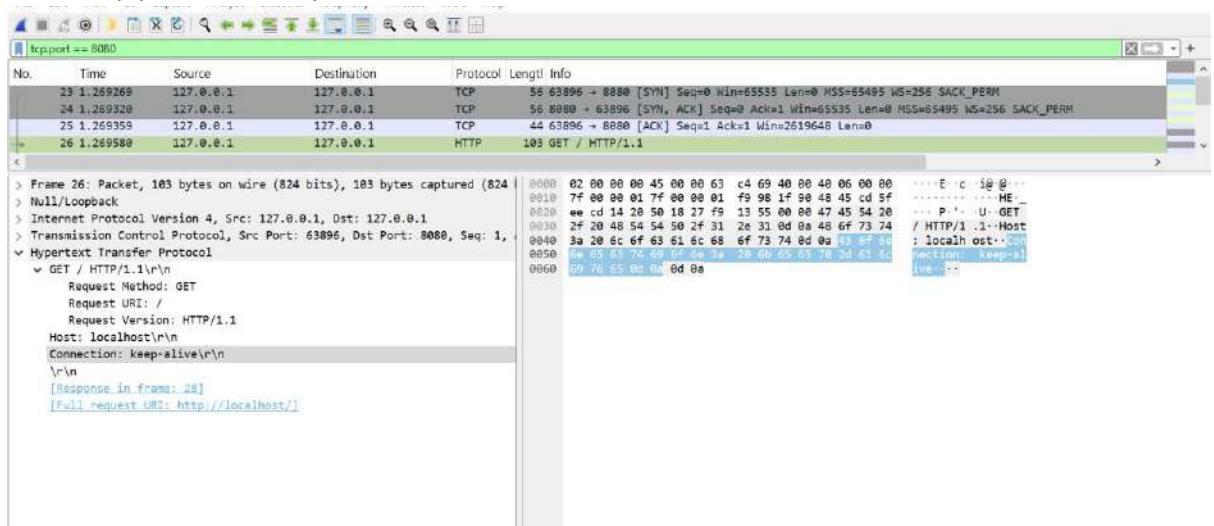


#### lets analyze single\_fin.pcapng:

First 3 packets are syn handshake as explained in part 1



Next message is the get / HTTP/1.1 request for the page- do notice that the connection type in the http protocol is keep-alive



The next 3 messages go as follows: 1: server send ack on the get / request 2:server sent HTTP/1.1 message with code 200 meaning success and sent the data which contains the header hello word for example , notice connection type is still keep-alive 3: client sent ack on all the bits (274 presumably)

```

[1] Wireshark - 00000000000000000000.pcap
No. Time Source Destination Protocol Length Info
23 1.269269 127.0.0.1 127.0.0.1 TCP 56 63896 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
24 1.269320 127.0.0.1 127.0.0.1 TCP 56 8080 → 63896 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
25 1.269359 127.0.0.1 127.0.0.1 TCP 44 63896 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
+ 26 1.269588 127.0.0.1 127.0.0.1 HTTP 103 GET / HTTP/1.1
27 1.269599 127.0.0.1 127.0.0.1 TCP 44 8080 → 63896 [ACK] Seq=1 Ack=60 Win=2619648 Len=0
- 28 1.270184 127.0.0.1 127.0.0.1 HTTP 318 HTTP/1.1 200 OK
+ 29 1.270281 127.0.0.1 127.0.0.1 TCP 44 63896 → 8080 [ACK] Seq=60 Ack=275 Win=2619392 Len=0

< Frame 28: Packet, 318 bytes on wire (2544 bits), 318 bytes captured (2544 bits) at 1.269588 (0x0000000000000000) on interface "VirtualBox Host Adapter", link-layer type 1000 (Ethernet), source 00:0c:29:7f:00:01, destination 00:0c:29:7f:00:01
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8080, Dst Port: 63896, Seq: 1, Ack: 60, Len: 254
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Connection: keep-alive\r\n
      Content-Length: 210\r\n
      \r\n
      [Request in frame: 26]
      [Time since request: 604.000 microseconds]
      [Request URI: /]
      [Full request URI: http://localhost/]
    File Data: 210 bytes
    Data [210 bytes]:
      Data [...] : 3c21444f43545950452068745d6c3e0a3c68746d6c206c616e673d226
      [Length: 210]
0000  02 00 00 00 45 00 01 3a c4 6b 40 00 48 06 00 00 ... E : k@ ...
0010  7f 00 00 01 7f 00 00 01 1f 90 f9 98 1f ee cd 14 20 ... -----
0020  48 45 cd 9a 58 18 27 f9 01 91 00 00 48 54 54 50 HE: P '-----HTTP
0030  2f 31 2e 31 2b 32 30 38 28 4f 4b 8d 0a 43 6f 6e /1.1 200 OK-Con
0040  66 65 63 74 69 6f 6e 3a 28 6b 65 65 78 2d 61 6c nection: keep-al
0050  69 76 65 0d 0a 43 6f 6e 74 65 66 74 2d 4c 65 6f ive-Conn-stant-Len
0060  67 74 68 3a 2b 32 31 30 0d 0d 0d 0a 3c 21 44 41 gth: 210 -----100
0070  43 54 59 50 05 00 00 00 74 60 62 74 9a 3c 68 74 60 HTTP/1.1 m32->int
0080  6c 24 6c 61 66 67 3d 22 65 66 22 34 99 3c 68 65 i Lange" en><he
0090  61 64 5e 07 70 20 10 30 3c 6d 65 74 61 20 03 68 d><meta ch
00a0  61 72 73 63 74 3d 22 53 54 6b 7d 38 22 36 0e 20 arset="UTF-8">
00b0  29 20 28 3c 75 40 74 6c 63 39 46 69 74 77 6f 72 <cell e>Networ
00c0  6b 20 41 73 75 69 67 6a 60 65 6e 74 3c 2f 74 69 k Assign name=</t>
00d0  74 6c 65 71 68 3c 2f 6b 65 61 64 3a 9a 3c 62 69 tyle><h head><bo
00e0  64 79 3e 05 26 29 28 3c 68 31 3e 48 65 6c 6d dy><h1>Hello
00f0  67 20 57 6f 72 6c 64 3c 2f 6b 91 3e 0a 20 26 26 o World</h1>
0100  20 3c 21 20 28 26 34 69 60 67 28 73 72 63 3d 22 <!--<-->
0130  2f 62 6f 54 29 3e 0a 3c 2f 68 74 6d 6c 3a /body></html>

< Frame 29: Packet, 103 bytes on wire (824 bits), 103 bytes captured (824 bits) at 1.270281 (0x0000000000000000) on interface "VirtualBox Host Adapter", link-layer type 1000 (Ethernet), source 00:0c:29:7f:00:01, destination 00:0c:29:7f:00:01
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 63896, Dst Port: 8080, Seq: 60, Ack: 275, Len: 103
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: localhost\r\n
      Connection: keep-alive\r\n
      \r\n
      [Response in frame: 28]
      [Full request URI: http://localhost/]

Data (data.data): 210 bytes
Packets: 333 - Displayed: 15 (4.5%) - Dropped: 0 (0.0%) | Profile: Default

```

**The second message:** immediately after we receive and sent ack (this at 1.27) at time 1.37 we sent another http get/ request

```

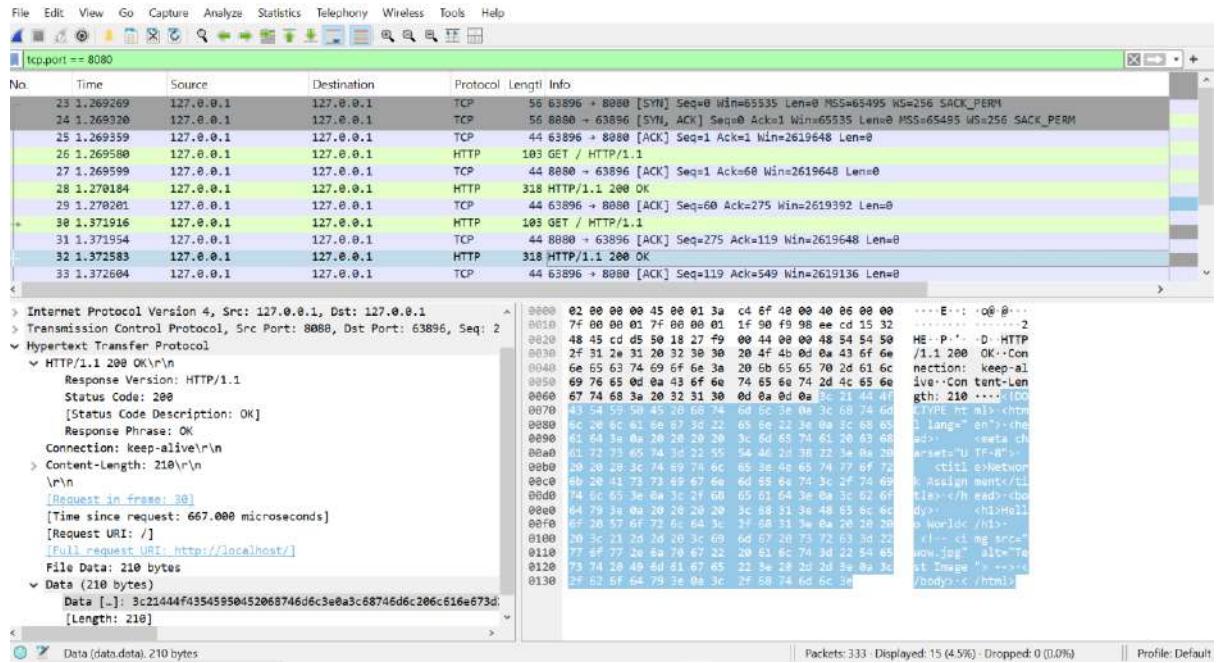
[1] Wireshark - 00000000000000000000.pcap
No. Time Source Destination Protocol Length Info
23 1.269269 127.0.0.1 127.0.0.1 TCP 56 63896 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
24 1.269320 127.0.0.1 127.0.0.1 TCP 56 8080 → 63896 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
25 1.269359 127.0.0.1 127.0.0.1 TCP 44 63896 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
+ 26 1.269588 127.0.0.1 127.0.0.1 HTTP 103 GET / HTTP/1.1
27 1.269599 127.0.0.1 127.0.0.1 TCP 44 8080 → 63896 [ACK] Seq=1 Ack=60 Win=2619648 Len=0
- 28 1.270184 127.0.0.1 127.0.0.1 HTTP 318 HTTP/1.1 200 OK
+ 29 1.270281 127.0.0.1 127.0.0.1 TCP 44 63896 → 8080 [ACK] Seq=60 Ack=275 Win=2619392 Len=0
+ 30 1.271916 127.0.0.1 127.0.0.1 HTTP 103 GET / HTTP/1.1

< Frame 30: Packet, 103 bytes on wire (824 bits), 103 bytes captured (824 bits) at 1.271916 (0x0000000000000000) on interface "VirtualBox Host Adapter", link-layer type 1000 (Ethernet), source 00:0c:29:7f:00:01, destination 00:0c:29:7f:00:01
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 63896, Dst Port: 8080, Seq: 60, Ack: 275, Len: 103
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: localhost\r\n
      Connection: keep-alive\r\n
      \r\n
      [Response in frame: 28]
      [Full request URI: http://localhost/]

Data (data.data): 210 bytes
Packets: 333 - Displayed: 15 (4.5%) - Dropped: 0 (0.0%) | Profile: Default

```

As the connection is kept alive we don't need to connect to the server again (no syn and we didn't even get fin yet) we get immediately the ack and response as it was in the first message:



The last ack was sent at 1.37 and after a second at 2.38 we received the first fin to sever the connection and do the 4 stage handshake

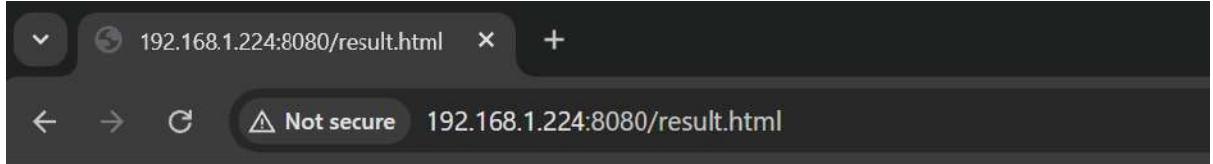
No.	Time	Source	Destination	Protocol	Length	Info
23	1.269269	127.0.0.1	127.0.0.1	TCP	56	63896 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
24	1.269320	127.0.0.1	127.0.0.1	TCP	56	8080 → 63896 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
25	1.269359	127.0.0.1	127.0.0.1	TCP	44	63896 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
26	1.269580	127.0.0.1	127.0.0.1	HTTP	103	GET / HTTP/1.1
27	1.269599	127.0.0.1	127.0.0.1	TCP	44	63896 → 8080 [ACK] Seq=1 Ack=60 Win=2619648 Len=0
28	1.270184	127.0.0.1	127.0.0.1	HTTP	318	HTTP/1.1 200 OK
29	1.270201	127.0.0.1	127.0.0.1	TCP	44	63896 → 8080 [ACK] Seq=60 Ack=275 Win=2619392 Len=0
30	1.371916	127.0.0.1	127.0.0.1	HTTP	103	GET / HTTP/1.1
31	1.371954	127.0.0.1	127.0.0.1	TCP	44	8080 → 63896 [ACK] Seq=275 Ack=119 Win=2619648 Len=0
32	1.372583	127.0.0.1	127.0.0.1	HTTP	318	HTTP/1.1 200 OK
33	1.372604	127.0.0.1	127.0.0.1	TCP	44	63896 → 8080 [ACK] Seq=119 Ack=549 Win=2619136 Len=0

All this shows that the server sent fin only after waiting a while for as the client sent the connection type as keep-alive

Now in file **double\_fin** you can see where we waited to send the second message it sent the fin before we could send the second message and so we got syn again and 2 disconnects meaning 4 fins

No.	Time	Source	Destination	Protocol	Length	Info
33	1.153947	127.0.0.1	127.0.0.1	TCP	56	64393 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
34	1.154832	127.0.0.1	127.0.0.1	TCP	56	8080 → 64393 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
35	1.154877	127.0.0.1	127.0.0.1	TCP	44	64393 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
36	1.154836	127.0.0.1	127.0.0.1	HTTP	103	GET / HTTP/1.1
37	1.154487	127.0.0.1	127.0.0.1	TCP	44	8080 → 64393 [ACK] Seq=1 Ack=60 Win=2619648 Len=0
38	1.155389	127.0.0.1	127.0.0.1	HTTP	318	HTTP/1.1 200 OK
39	1.155416	127.0.0.1	127.0.0.1	TCP	44	64393 → 8080 [ACK] Seq=60 Ack=275 Win=2619392 Len=0
40	2.165744	127.0.0.1	127.0.0.1	TCP	44	8080 → 64393 [FIN, ACK] Seq=275 Ack=60 Win=2619648 Len=0
41	2.165767	127.0.0.1	127.0.0.1	TCP	44	64393 → 8080 [ACK] Seq=60 Ack=276 Win=2619392 Len=0
56	3.159318	127.0.0.1	127.0.0.1	TCP	44	64393 → 8080 [FIN, ACK] Seq=60 Ack=276 Win=2619392 Len=0
57	3.159340	127.0.0.1	127.0.0.1	TCP	44	8080 → 64393 [ACK] Seq=276 Ack=61 Win=2619648 Len=0
58	3.159524	127.0.0.1	127.0.0.1	TCP	56	64394 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
59	3.159569	127.0.0.1	127.0.0.1	TCP	56	8080 → 64394 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
60	3.159595	127.0.0.1	127.0.0.1	TCP	44	64394 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
61	3.159785	127.0.0.1	127.0.0.1	HTTP	103	GET / HTTP/1.1
62	3.159811	127.0.0.1	127.0.0.1	TCP	44	8080 → 64394 [ACK] Seq=1 Ack=60 Win=2619648 Len=0
63	3.168674	127.0.0.1	127.0.0.1	HTTP	318	HTTP/1.1 200 OK
64	3.160697	127.0.0.1	127.0.0.1	TCP	44	64394 → 8080 [ACK] Seq=60 Ack=275 Win=2619392 Len=0
65	3.162168	127.0.0.1	127.0.0.1	TCP	44	64394 → 8080 [FIN, ACK] Seq=60 Ack=275 Win=2619392 Len=0
66	3.162184	127.0.0.1	127.0.0.1	TCP	44	8080 → 64394 [ACK] Seq=275 Ack=61 Win=2619648 Len=0
67	3.162399	127.0.0.1	127.0.0.1	TCP	44	64394 → 8080 [FIN, ACK] Seq=275 Ack=61 Win=2619648 Len=0
68	3.162420	127.0.0.1	127.0.0.1	TCP	44	64394 → 8080 [ACK] Seq=61 Ack=276 Win=2619392 Len=0

## 2. Let analyze redirect.pcapng:



**Success!**

You have been redirected to result.html

We as usual get the 3 part handshake for connection:

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.1.224	192.168.1.224	TCP	56	51489 + 8088 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM	
2 0.000065	192.168.1.224	192.168.1.224	TCP	56	8088 - 51489 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM	
3 0.000105	192.168.1.224	192.168.1.224	TCP	44	51489 + 8088 [ACK] Seq=1 Ack=1 Win=2619648 Len=0	

Now we send a http message get/redirect

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.1.224	192.168.1.224	TCP	56	51489 + 8088 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM	
2 0.000065	192.168.1.224	192.168.1.224	TCP	56	8088 - 51489 [SYN, ACK] Seq=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM	
3 0.000105	192.168.1.224	192.168.1.224	TCP	44	51489 + 8088 [ACK] Seq=1 Ack=1 Win=2619648 Len=0	
4 0.001505	192.168.1.224	192.168.1.224	HTTP	493	GET /redirect HTTP/1.1	

```

> Frame 4: Packet, 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits), 493 bytes selected
  Null/Loopback
  Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.224
  Transmission Control Protocol, Src Port: 51489, Dst Port: 8088, Seq: 1, Ack: 1, Len: 493
    Hypertext Transfer Protocol
      GET /redirect HTTP/1.1\r\n
        Request Method: GET
        Request URI: /redirect
        Request Version: HTTP/1.1
        Host: 192.168.1.224:8088\r\n
        Connection: keep-alive\r\n
        DNT: 1\r\n
        Upgrade-Insecure-Requests: 1\r\n
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
        Accept-Encoding: gzip, deflate\r\n
        Accept-Language: en-US,en;q=0.9\r\n
      [Response in frame 8]
      [Full request URI: http://192.168.1.224:8088/redirect]
```

We receive an ack from the server and then the message to redirect us to /result and to close the connection, which we send ack as a response

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.224	192.168.1.224	TCP	56	51489 + 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000066	192.168.1.224	192.168.1.224	TCP	56	8080 + 51489 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000185	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
4	0.001505	192.168.1.224	192.168.1.224	HTTP	493	GET /redirect HTTP/1.1
5	0.001524	192.168.1.224	192.168.1.224	TCP	44	8080 + 51489 [ACK] Seq=1 Ack=450 Win=2619648 Len=0
6	0.002810	192.168.1.224	192.168.1.224	TCP	121	8080 + 51489 [PSH, ACK] Seq=1 Ack=450 Win=2619648 Len=77 [TCP PDU reassembled in 8]
7	0.002828	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [ACK] Seq=450 Ack=78 Win=2619648 Len=0

```

> [Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 77]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1201178588
[Next Sequence Number: 78 (relative sequence number)]
Acknowledgment Number: 450 (relative ack number)
Acknowledgment number (raw): 3910103977
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 10233
[Calculated window size: 2619648]
[Window size scaling factor: 25]
Checksum: 0xaf6e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
TCP payload (77 bytes)
[Reassembled PDU in frame: 8]
TCP segment data (77 bytes)

```

Now we send a message that we moved permanently 301 close the connection from the client side (server side already knows to close the connection) then we open a new connection

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.224	192.168.1.224	TCP	56	51489 + 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000066	192.168.1.224	192.168.1.224	TCP	56	8080 + 51489 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000185	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
4	0.001505	192.168.1.224	192.168.1.224	HTTP	493	GET /redirect HTTP/1.1
5	0.001524	192.168.1.224	192.168.1.224	TCP	44	8080 + 51489 [ACK] Seq=1 Ack=450 Win=2619648 Len=0
6	0.002810	192.168.1.224	192.168.1.224	TCP	121	8080 + 51489 [PSH, ACK] Seq=1 Ack=450 Win=2619648 Len=77 [TCP PDU reassembled in 8]
7	0.002828	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [ACK] Seq=450 Ack=78 Win=2619648 Len=0
8	0.002854	192.168.1.224	192.168.1.224	HTTP	44	HTTP/1.1 301 Moved Permanently
9	0.002866	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [ACK] Seq=450 Ack=79 Win=2619648 Len=0
10	0.004396	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [FIN, ACK] Seq=450 Ack=79 Win=2619648 Len=0
11	0.004425	192.168.1.224	192.168.1.224	TCP	44	8080 + 51489 [ACK] Seq=79 Ack=451 Win=2619648 Len=0
12	0.006418	192.168.1.224	192.168.1.224	TCP	56	51490 + 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
13	0.006493	192.168.1.224	192.168.1.224	TCP	56	8080 + 51490 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
14	0.006534	192.168.1.224	192.168.1.224	TCP	44	51490 + 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

```

[Coloring Rule String: http || tcp.port == 80 || http2]
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.224
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x40fa (16634)
> 010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.224
Destination Address: 192.168.1.224

```

Packet (44 bytes) Reassembled TCP (77 bytes) || Packets: 22 || Profile: Default

From the new connection we send a new http get for /result we receive it from the server and after a second we close the connection

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.224	192.168.1.224	TCP	56	51489 + 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000056	192.168.1.224	192.168.1.224	TCP	56	8080 + 51489 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000105	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
4	0.000155	192.168.1.224	192.168.1.224	HTTP	493	GET /redirect HTTP/1.1
5	0.0001524	192.168.1.224	192.168.1.224	TCP	44	8080 + 51489 [ACK] Seq=1 Ack=450 Win=2619648 Len=0
6	0.000210	192.168.1.224	192.168.1.224	TCP	121	8080 + 51489 [PSH, ACK] Seq=1 Ack=450 Win=2619648 Len=77 [TCP PDU reassembled in 8]
7	0.0002828	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [ACK] Seq=450 Ack=78 Win=2619648 Len=0
8	0.0002854	192.168.1.224	192.168.1.224	HTTP	44	HTTP/1.1 301 Moved Permanently
9	0.0002866	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [ACK] Seq=450 Ack=79 Win=2619648 Len=0
10	0.0003596	192.168.1.224	192.168.1.224	TCP	44	51489 + 8080 [FIN, ACK] Seq=450 Ack=79 Win=2619648 Len=0
11	0.0004425	192.168.1.224	192.168.1.224	TCP	44	8080 + 51489 [ACK] Seq=79 Ack=451 Win=2619648 Len=0
12	0.0004418	192.168.1.224	192.168.1.224	TCP	56	51498 + 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
13	0.0004933	192.168.1.224	192.168.1.224	TCP	56	8080 + 51499 [ACK] Seq=0 Ack=1 Win=2619648 Len=0 MSS=65495 WS=256 SACK_PERM
14	0.000534	192.168.1.224	192.168.1.224	TCP	44	51498 + 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
15	0.000746	192.168.1.224	192.168.1.224	HTTP	496	GET /result.html HTTP/1.1
16	0.000772	192.168.1.224	192.168.1.224	TCP	44	8080 + 51499 [ACK] Seq=1 Ack=453 Win=2619648 Len=0
17	0.011276	192.168.1.224	192.168.1.224	HTTP	171	HTTP/1.1 200 OK
18	0.011302	192.168.1.224	192.168.1.224	TCP	44	51498 + 8080 [ACK] Seq=453 Ack=128 Win=2619648 Len=0
19	1.019537	192.168.1.224	192.168.1.224	TCP	44	8080 + 51499 [FIN, ACK] Seq=128 Ack=453 Win=2619648 Len=0
20	1.019562	192.168.1.224	192.168.1.224	TCP	44	51498 + 8080 [ACK] Seq=453 Ack=129 Win=2619648 Len=0
21	1.019566	192.168.1.224	192.168.1.224	TCP	44	51498 + 8080 [FIN, ACK] Seq=453 Ack=129 Win=2619648 Len=0
22	1.019607	192.168.1.224	192.168.1.224	TCP	44	8080 + 51499 [ACK] Seq=129 Ack=454 Win=2619648 Len=0

This shows the 301 redirect

### 3. Now we will analyze notfound.pcapng where we executed get/nope which doesn't exist

We can see that we sent the get /nope and received a 404 http code meaning the page was not found, everything else is similar to previous analysis.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.224	192.168.1.224	TCP	56	51856 + 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2	0.000072	192.168.1.224	192.168.1.224	TCP	56	8080 + 51856 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
3	0.000113	192.168.1.224	192.168.1.224	TCP	44	51856 + 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
4	0.000572	192.168.1.224	192.168.1.224	HTTP	522	GET /nope HTTP/1.1
5	0.000591	192.168.1.224	192.168.1.224	TCP	44	8080 + 51856 [ACK] Seq=1 Ack=479 Win=2619648 Len=0
6	0.001791	192.168.1.224	192.168.1.224	TCP	89	8080 + 51856 [PSH, ACK] Seq=1 Ack=479 Win=2619648 Len=45 [TCP PDU reassembled in 8]
7	0.001812	192.168.1.224	192.168.1.224	TCP	44	8080 + 51856 [ACK] Seq=479 Ack=46 Win=2619648 Len=0
8	0.001830	192.168.1.224	192.168.1.224	HTTP	44	HTTP/1.1 404 Not Found
9	0.001838	192.168.1.224	192.168.1.224	TCP	44	51856 + 8080 [ACK] Seq=479 Ack=47 Win=2619648 Len=0
10	0.004184	192.168.1.224	192.168.1.224	TCP	56	51857 + 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
11	0.004255	192.168.1.224	192.168.1.224	TCP	56	8080 + 51857 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
12	0.004426	192.168.1.224	192.168.1.224	TCP	44	51857 + 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
13	0.004573	192.168.1.224	192.168.1.224	TCP	44	51856 + 8080 [FIN, ACK] Seq=1 Ack=479 Ack=47 Win=2619648 Len=0
14	0.004685	192.168.1.224	192.168.1.224	TCP	44	8080 + 51856 [ACK] Seq=47 Ack=48 Win=2619648 Len=0
15	1.000897	192.168.1.224	192.168.1.224	TCP	44	8080 + 51857 [FIN, ACK] Seq=1 Ack=1 Win=2619648 Len=0
16	1.0008936	192.168.1.224	192.168.1.224	TCP	44	51857 + 8080 [ACK] Seq=1 Ack=2 Win=2619648 Len=0
17	2.619577	192.168.1.224	192.168.1.224	TCP	44	51857 + 8080 [FIN, ACK] Seq=1 Ack=2 Win=2619648 Len=0
18	2.619663	192.168.1.224	192.168.1.224	TCP	44	8080 + 51857 [ACK] Seq=2 Ack=2 Win=2619648 Len=0