

TCP COMMUNICATION ANALYSIS

Part 1:

1. The messages:

The screenshot shows a VS Code interface with two terminal panes. The top terminal pane displays the server code (`tcp_server.py`) and its execution output. The bottom terminal pane displays the client code (`tcp_client.py`) and its execution output.

Top Terminal (Server 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 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-d1ce-4149-afe8-149b3dbc09a
Server sent: b'2152162849 327613030'
```

2. Wireshark

The Wireshark interface displays two captures side-by-side:

- clientside.pcapng:** Shows traffic from client (192.168.1.224) to server (192.168.1.221). The first packet is a SYN (Seq=0, Ack=1) with a sequence number of 1928250445.
- serverside.pcapng:** Shows traffic from server (192.168.1.221) to client (192.168.1.224). The first packet is a SYN-ACK (Seq=1, Ack=2) with a sequence number of 1928250446.

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

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

Packet details for the first SYN packet (Frame 25):

- Source: 192.168.1.224
- Destination: 192.168.1.221
- Protocol: TCP
- Length: 66
- Info: 66 54962 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Raw bytes (hex dump):

```

> Frame 25: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: ASRockIncorp_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: 1928250445
  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: ....0....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	2.902234	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=0 Ack=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: 0
Source Port: 12345
Destination Port: 54962
[Stream index: 5]
[Stream Packer 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
...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
>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	2.902234	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=0 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

[Next Sequence Number: 1 (relative sequence number)]
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: 1026
[Calculated window size: 262656]
[Window size scaling factor: 256]
Checksum: 0x8ab0 [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	2.902234	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=0 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=1 Win=262656 Len=33

[Next Sequence Number: 34 (relative sequence number)]
Acknowledge Number: 1 (relative ack number)
Acknowledgment number (raw): 2757540238
0101 = Header Length: 20 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: 0x05d7 [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	2.902234	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=0 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=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

[Next Sequence Number: 34 (relative sequence number)]
Acknowledge Number: 34 (relative ack number)
Acknowledgment number (raw): 1928250479
0101 = Header Length: 20 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

Packets: 177 - Displayed: 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=1460 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=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=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)
 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: 0x9c4b [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 [Timestamps]
 ↳ TSO/ACK analysis1

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=1460 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=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=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: 20]
 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)
 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: 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=0 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=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
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

[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
 0101 = 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

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

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	2.998526	192.168.1.224	192.168.1.221	TCP	66	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
 0101 = 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: 1026
 [Calculated window size: 262656]
 [Window size scaling factor: 256]
 Checksum: 0x8a45 [unverified]
 'Checksum Status: Unverified'

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

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=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	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 Packet 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: 4100
[Calculated window size: 1049600]
[Window size scaling factor: 256]
Checksum: 0x8528 [unverified]

Fin (tcp.flags.fin), 1 bit

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	2.902234	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=0 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	2.907840	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
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	60	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....]

Fin (tcp.flags.fin), 1 bit

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

No.	Time	Source	Destination	Protocol	Length	Info
23	1.269269	127.0.0.1	127.0.0.1	TCP	56	63896 → 8880 [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	8880 → 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 → 8880 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

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

No.	Time	Source	Destination	Protocol	Length	Info
23	1.269269	127.0.0.1	127.0.0.1	TCP	56	63896 → 8880 [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	8880 → 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 → 8880 [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

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)

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

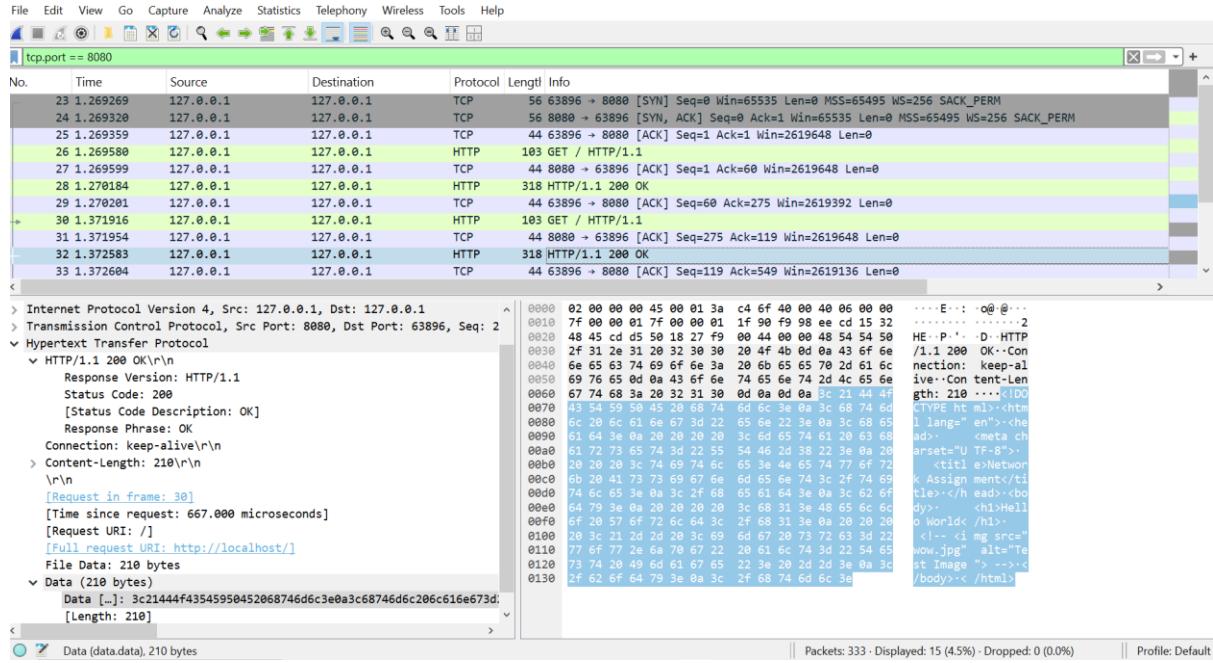
tcp.port == 8080

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	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	1.270201	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

> Frame 30: Packet, 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface null
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
> GET / HTTP/1.1\r\nRequest Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: localhost\r\nConnection: keep-alive\r\n\r\n[Response in frame: 32]
[Full request URI: http://localhost/]

0000 02 00 00 00 45 00 00 63 c4 6d 40 00 40 06 00 00 ... E c m@...
0010 7f 00 00 01 7f 00 00 01 f9 98 1f 90 48 45 cd 9aHE...
0020 ee cd 15 32 50 18 27 f8 12 09 00 00 47 45 54 20 ..P...'..GET
0030 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 / HTTP/1.1 Host:
0040 3a 20 6c 6f 63 61 6c 68 6f 73 74 0d 0a 43 6f 6e : localh ost: Con
0050 66 65 63 74 69 6f 6e 3a 20 6b 65 65 78 2d 61 6c nection: keep-al
0060 69 76 65 0d 0a 0d 0aive....

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

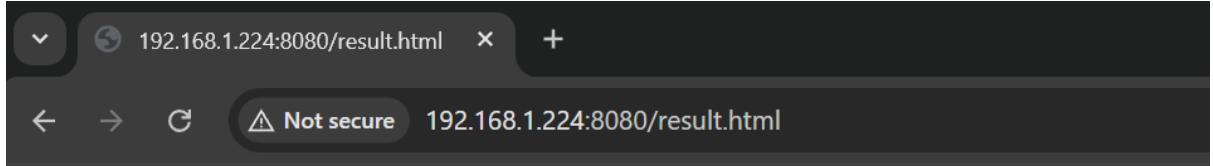
No.	Time	Source	Destination	Protocol	Length	Info
23	1.269269	127.0.0.1	127.0.0.1	TCP	56	63896 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
24	1.269320	127.0.0.1	127.0.0.1	TCP	56	8080 → 63896 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
25	1.269359	127.0.0.1	127.0.0.1	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	1.154032	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	1.154077	127.0.0.1	127.0.0.1	TCP	44	64393 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
36	1.154386	127.0.0.1	127.0.0.1	HTTP	103	GET / HTTP/1.1
37	1.154407	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
50	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	3.159348	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	3.160674	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 [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 → 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 0.000105	192.168.1.224	192.168.1.224	TCP	44	51489 → 8080 [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 → 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 0.000105	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	

```

> Frame 4: Packet, 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits), 493 bytes selected (3944 bits)
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.224
> Transmission Control Protocol, Src Port: 51489, Dst Port: 8080, Seq: 1, Ack: 1, Length: 493
  Hypertext Transfer Protocol
    GET /redirect HTTP/1.1\r\n
      Request Method: GET
      Request URI: /redirect
      Request Version: HTTP/1.1
      Host: 192.168.1.224:8080\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/57.0.2987.133 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://192.168.1.224:8080/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): 1201178508
[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: 256]
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	0.003596	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	0.008418	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	0.008493	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	0.008534	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

Header Checksum (ip.checksum), 2 bytes

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	0.000066	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=450 Win=2619648 Len=0
4	0.001585	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=2 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	0.008418	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	0.008493	192.168.1.224	192.168.1.224	TCP	56	8080 → 51490 [ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
14	0.008534	192.168.1.224	192.168.1.224	TCP	44	51490 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
15	0.008746	192.168.1.224	192.168.1.224	HTTP	496	GET /result.html HTTP/1.1
16	0.008772	192.168.1.224	192.168.1.224	TCP	44	8080 → 51490 [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	0.011382	192.168.1.224	192.168.1.224	TCP	44	51490 → 8080 [ACK] Seq=453 Ack=128 Win=2619648 Len=0
19	0.19527	192.168.1.224	192.168.1.224	TCP	44	8080 → 51490 [FIN, ACK] Seq=128 Ack=453 Win=2619648 Len=0
20	0.19562	192.168.1.224	192.168.1.224	TCP	44	51490 → 8080 [ACK] Seq=453 Ack=129 Win=2619648 Len=0
21	0.370566	192.168.1.224	192.168.1.224	TCP	44	51490 → 8080 [FIN, ACK] Seq=453 Ack=129 Win=2619648 Len=0
22	2.370607	192.168.1.224	192.168.1.224	TCP	44	8080 → 51490 [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	51856 → 8080 [ACK] Seq=479 Ack=46 Win=2619648 Len=0
8	0.001839	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	0.004296	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	8080 → 51857 [FIN, ACK] Seq=479 Ack=47 Win=2619648 Len=0
14	0.004605	192.168.1.224	192.168.1.224	TCP	44	8080 → 51856 [ACK] Seq=47 Ack=480 Win=2619648 Len=0
15	1.008997	192.168.1.224	192.168.1.224	TCP	44	8080 → 51857 [FIN, ACK] Seq=1 Ack=1 Win=2619648 Len=0
16	1.008936	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	2.619603	192.168.1.224	192.168.1.224	TCP	44	8080 → 51857 [ACK] Seq=2 Ack=2 Win=2619648 Len=0