

TCP COMMUNICATION ANALYSIS

Part 1:

- ## 1. The messages:

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

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS +

```
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
```

```
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()
```

PROBLEMS OUTPUT TERMINAL Python Debug Console +

```
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'
PS O:\net2> 
```

2. Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
25	3.763888	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
26	3.766102	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
27	3.766166	192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [ACK] Seq=1 Ack=1 Win=262656 Len=0
28	3.766194	192.168.1.224	192.168.1.221	TCP	87	54962 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=33
29	3.838753	192.168.1.221	192.168.1.224	TCP	87	12345 → 54962 [PSH, ACK] Seq=1 Ack=34 Win=1049600 Len=33
30	3.839111	192.168.1.224	192.168.1.221	TCP	74	54962 → 12345 [PSH, ACK] Seq=34 Ack=34 Win=262656 Len=20
31	3.859937	192.168.1.221	192.168.1.224	TCP	74	12345 → 54962 [PSH, ACK] Seq=34 Ack=54 Win=1049600 Len=20
32	3.860284	192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [FIN, ACK] Seq=54 Ack=54 Win=262656 Len=0
33	3.860479	192.168.1.221	192.168.1.224	TCP	60	12345 → 54962 [FIN, ACK] Seq=54 Ack=54 Win=262656 Len=0
34	3.860497	192.168.1.224	192.168.1.221	TCP	54	54962 → 12345 [ACK] Seq=55 Ack=55 Win=262656 Len=0
35	3.869725	192.168.1.221	192.168.1.224	TCP	60	12345 → 54962 [ACK] Seq=55 Ack=55 Win=1049600 Len=0

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	3.763888	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) on interface 0		0000 04 e8 b9 c5 89 06 9c 6b 00 a9 3f 73 08 00 45 00k--?s--E
> Ethernet II, Src: ASRockIncorp_a9:3f:73 (9c:6b:00:a9:3f:73), Dst: Intel_82:55:0a:00:00:00		0010 00 34 ff 91 40 00 40 06 00 00 c0 a8 01 e0 c0 a8 -4-@-@-.....
> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.221		0020 01 dd d6 b2 30 39 72 ee c4 d0 00 00 00 00 0209r-..M
> Transmission Control Protocol, Src Port: 54962, Dst Port: 12345, Seq: 0		0030 fa f0 85 34 00 00 02 04 05 b4 01 03 03 08 01 01 -4-----
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)		0040 0a 02
> Flags: 0x002 (SYN)		
0000 = Reserved: Not set ...0 = Accurate ECN: Not set0... = Congestion Window Reduced: Not set0... = ECN-Echo: Not set0... = Urgent: Not set0... = Acknowledgment: Not set0... = Push: Not set0... = Reset: Not set0... = Syn: Set0... = 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	2.902234	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	0000 9c 6b 00 a9 3f 73 04 e8 b9 c5 09 06 00 00 45 00 k 7s E
Transmission Control Protocol, Src Port: 12345, Dst Port: 54962, Seq: 0	0010 00 34 52 50 40 00 00 00 00 c0 a8 01 dd c0 a8 -4R[0
Source Port: 12345	0020 01 e0 30 39 d6 b2 72 ee c4 4e 00 12 -09- N
Destination Port: 54962	0030 ff ff 85 34 00 00 02 04 05 b4 01 03 00 01 01 -4
[Stream Index: 5]	0040 04 e2 ..
[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	
. . . . 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]	

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)]	0000 04 e8 b9 c5 09 06 9c 6b 00 a9 3f 73 08 00 45 00 k 7s E
Acknowledgment Number: 1 (relative ack number)	0010 00 28 ff 92 40 00 00 00 b6 2f c0 a8 01 e0 c0 a8 - @
Acknowledgment number (raw): 2757540238	0020 01 dd d6 b2 30 39 72 ee c4 4e a4 5c b9 8e 50 11 - 09- P
0101 = Header Length: 20 bytes (5)	0030 04 e2 8a b0 00 00
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]	

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

The image shows a Wireshark packet capture of a TCP acknowledgment packet. The packet list at the top shows five packets. The selected packet (No. 126) is a TCP acknowledgment from 192.168.1.224 to 192.168.1.221, with sequence number 54962 and acknowledgment number 12345. The packet details pane shows the following information:

- [Next Sequence Number: 34 (relative sequence number)]
- Acknowledgment 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: 0x85d7 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]
- [Client Contiguous Streams: 1]
- [Server Contiguous Streams: 1]

The packet bytes pane shows the raw data of the packet, including the header and the payload.

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

The image shows a Wireshark packet capture of a TCP acknowledgment packet. The packet list at the top shows five packets. The selected packet (No. 127) is a TCP acknowledgment from 192.168.1.221 to 192.168.1.224, with sequence number 12345 and acknowledgment number 54962. The packet details pane shows the following information:

- [Next Sequence Number: 34 (relative sequence number)]
- Acknowledgment 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]

The packet bytes pane shows the raw data of the packet, including the header and the payload.

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

The image shows a Wireshark packet capture of a TCP segment. The packet list on the left shows a sequence of packets from 123 to 130. Packet 126 is selected, showing details for a TCP segment from 192.168.1.224 to 192.168.1.221. The 'Info' pane shows the following details:

- [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: 0x804b [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- [SEQ/ACK analysis]

The packet bytes pane on the right shows the raw data of the packet, including the acknowledgment number 2757540271.

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

The image shows a Wireshark packet capture of a TCP segment. The packet list on the left shows a sequence of packets from 123 to 131. Packet 131 is selected, showing details for a TCP segment from 192.168.1.221 to 192.168.1.224. The 'Info' pane shows the following details:

- [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]

The packet bytes pane on the right shows the raw data of the packet, including the acknowledgment number 1928250499.

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

Wireshark packet capture showing the eighth message from server to client. The packet list shows a FIN segment from 192.168.1.221 to 192.168.1.224. The packet details show the TCP flags as FIN, ACK and the sequence number as 2757540291. The packet bytes show the raw data of the segment.

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 NS=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=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
0181 = 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: 4198

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)

Wireshark packet capture showing the ninth message from client to server. The packet list shows a FIN segment from 192.168.1.224 to 192.168.1.221. The packet details show the TCP flags as FIN, ACK and the acknowledgment number as 2757540291. The packet bytes show the raw data of the segment.

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	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
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]

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	2.982861	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	2.998681	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 set0... = ECN-Echo: Not set ...0. = Urgent: Not set1 = Acknowledgment: Set0... = Push: Not set0... = Reset: Not set0... = Syn: Not set0... = Fin: Not set [TCP Flags:A....] Window: 4100 [Calculated window size: 1049600] [Window size scaling factor: 256] Checksum: 0x8528 Unverified	0000 9c 6b 00 a9 3f 73 04 a8 b9 c5 89 06 08 00 45 00 k...Ps...E 0010 00 28 52 5f 40 00 00 06 00 00 c0 a8 01 dd c0 a8 ..(R_@...+..... 0020 01 e0 30 39 d6 b2 a4 5c b9 c4 72 ee c4 84 50 10 ...09...\\...P 0030 10 04 85 28 00 00 00 00 00 00 00 00 00 00 00 ...D.....
---	---

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	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=0 Ack=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
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
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	2.982861	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	2.998681	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 set0... = ECN-Echo: Not set ...0. = Urgent: Not set1 = Acknowledgment: Set0... = Push: Not set0... = Reset: Not set0... = Syn: Not set0... = Fin: Not set [TCP Flags:A....] Window: 4100 [Calculated window size: 1049600] [Window size scaling factor: 256] Checksum: 0x8528 Unverified	0000 04 e8 b9 c5 89 06 9c 6b 00 a9 3f 73 08 00 45 00k...Ps...E 0010 00 28 ff 96 40 00 00 06 b6 2b c0 a8 01 e0 c0 a8 ..(R_@...+..... 0020 01 dd d6 b2 30 39 72 ee c4 84 a4 5c b9 c4 50 10 ...09...\\...P 0030 04 02 8a 44 00 00 00 00 00 00 00 00 00 00 00 ...D.....
---	--

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)

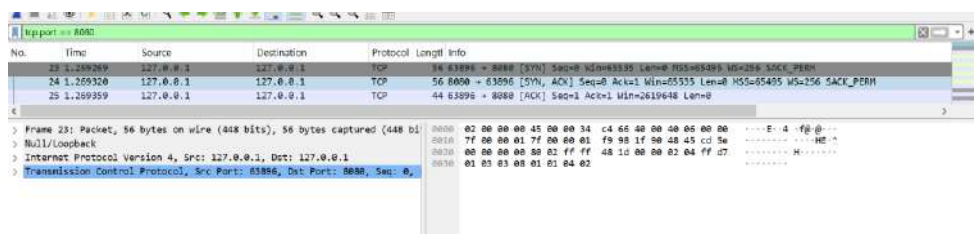


Hello World

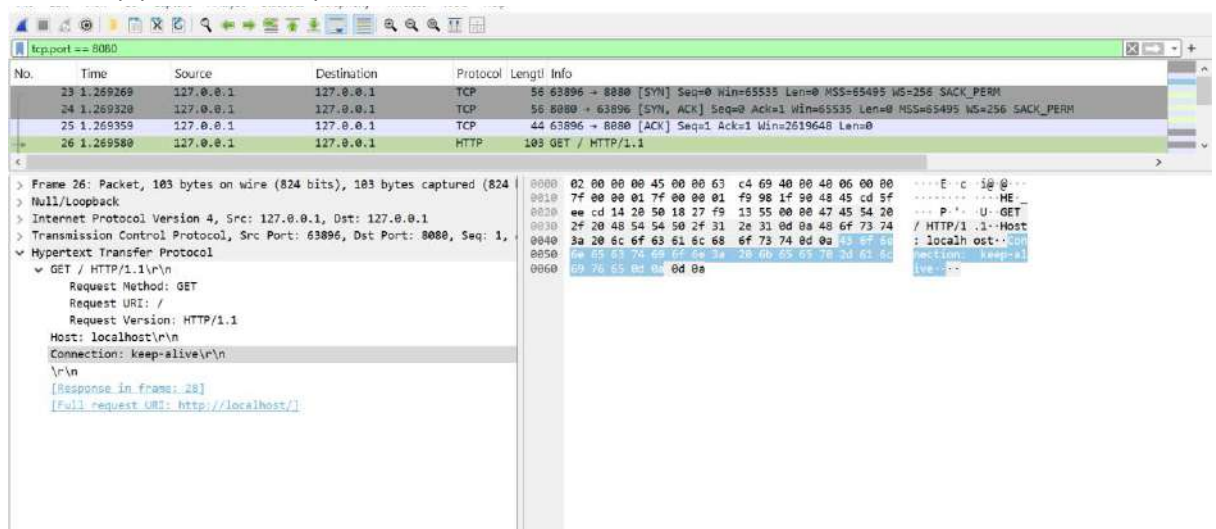


lets analyze single_fin.pcapng:

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)

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

Frame 28: Packet, 318 bytes on wire (2544 bits), 318 bytes captured (2544 bits) on interface 0

Ethernet II, Src: VirtualBox__enp000000000000, Dst: VirtualBox__enp000000000000

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, Len: 0

Hypertext Transfer Protocol

GET / HTTP/1.1

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Connection: keep-alive

Content-Length: 210

[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 [..]: 3c21444f43545950452068746d6c6e0a3c68746d6c206c616e673d226

[Length: 210]

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

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 0

Ethernet II, Src: VirtualBox__enp000000000000, Dst: VirtualBox__enp000000000000

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, Len: 0

Hypertext Transfer Protocol

GET / HTTP/1.1

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

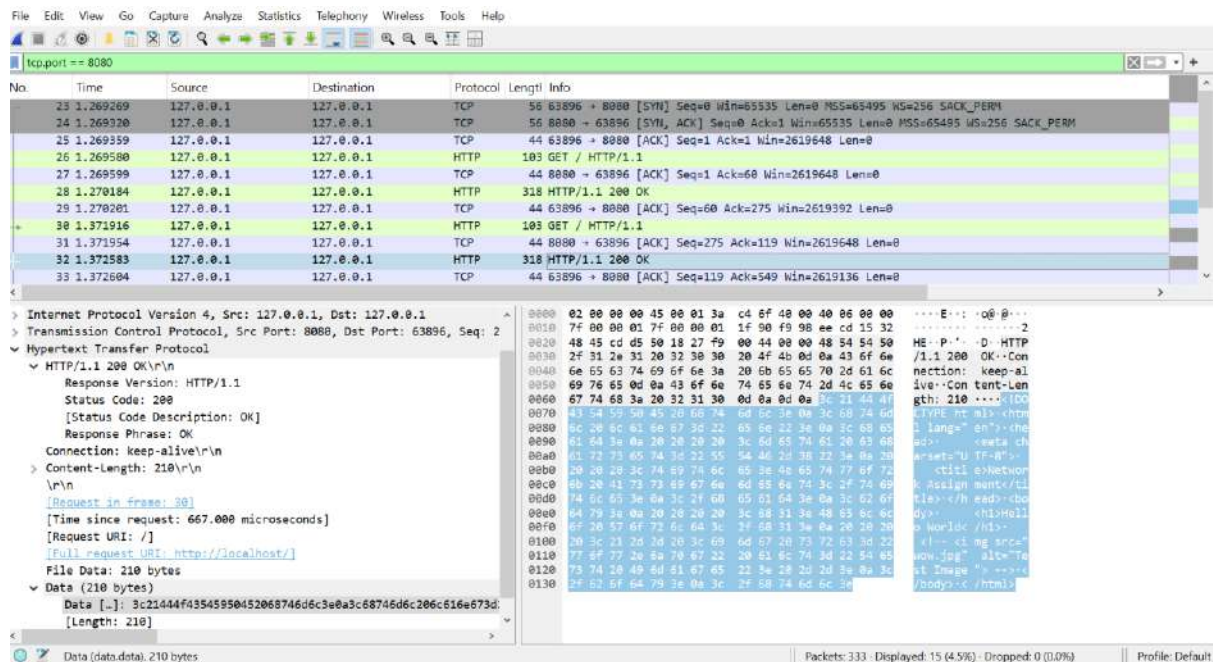
Host: localhost

Connection: keep-alive

[Response in frame: 32]

[Full request URI: http://localhost/]

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



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
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

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 8080, Dst Port: 63896, Seq: 2

Hypertext Transfer Protocol

- HTTP/1.1 200 OK
- Response Version: HTTP/1.1
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Connection: keep-alive
- Content-Length: 210
- [Request in frame: 30]
- [Time since request: 667.000 microseconds]
- [Request URI: /]
- [Full request URI: http://localhost/]
- File Data: 210 bytes
- Data (210 bytes)
- Data [..]: 3c21444f3545950452068746d6c3e0a3c68746d6c206c616e673d: [Length: 210]

Data (data.data), 210 bytes

Packets: 333 · Displayed: 15 (4.5%) · Dropped: 0 (0.0%) · Profile: Default

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

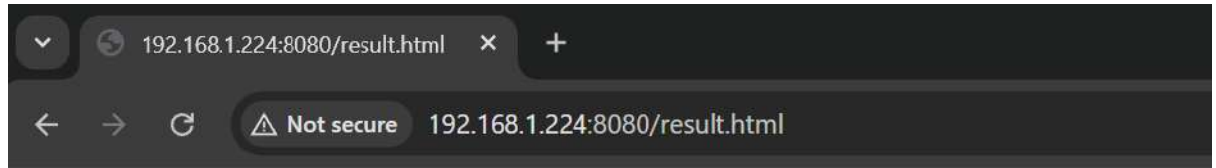
No.	Time	Source	Destination	Protocol	Length	Info
23	1.269269	127.0.0.1	127.0.0.1	TCP	56	63896 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
24	1.269320	127.0.0.1	127.0.0.1	TCP	56	8080 → 63896 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
25	1.269359	127.0.0.1	127.0.0.1	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	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
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
60	2.386178	127.0.0.1	127.0.0.1	TCP	44	8080 → 63896 [FIN, ACK] Seq=549 Ack=119 Win=2619648 Len=0
61	2.386208	127.0.0.1	127.0.0.1	TCP	44	63896 → 8080 [ACK] Seq=119 Ack=550 Win=2619136 Len=0
110	6.374259	127.0.0.1	127.0.0.1	TCP	44	63896 → 8080 [FIN, ACK] Seq=119 Ack=550 Win=2619136 Len=0
111	6.374288	127.0.0.1	127.0.0.1	TCP	44	8080 → 63896 [ACK] Seq=550 Ack=120 Win=2619648 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
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	3.159324	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	3.159369	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	8080 → 64394 [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 → 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	0000	02 00 00 00 45 00 01 e9	40 f6 40 00 40 05 00 00	... E... @ @ @...
> Null/Loopback	0010	c0 a8 01 e0 c0 a8 01 e0	c9 21 1f 90 e9 0f 71 e8 : [....]q
> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.224	0020	47 98 87 8c 50 18 27 f9	a9 4f 00 00 00 00 00 00	G...P... 0 [..]
> Transmission Control Protocol, Src Port: 51489, Dst Port: 8080, Seq: 1,	0030	2f 72 65 64 69 72 65 63	74 20 48 54 54 50 2f 31	/redirect HTTP/1
> Hypertext Transfer Protocol	0040	2e 31 8d 0a 48 6f 73 74	3a 20 31 39 32 2a 31 36	1-Host: 192.16
GET /redirect HTTP/1.1\r\n	0050	38 2e 31 2e 32 32 34 3a	38 30 38 30 8d 0a 43 6f	8.1.224: 8080- Co
Request Method: GET	0060	6e 6e 65 63 74 69 6f 6e	3a 20 6b 65 65 70 2d 61	nnnection: keep-a
Request URI: /redirect	0070	6c 69 76 65 6d 0a 44 4e	54 3a 20 31 8d 0a 55 70	live-NDN T: 1-..Up
Request Version: HTTP/1.1	0080	67 72 61 64 65 2d 49 6e	73 65 63 75 72 65 2d 52	grade-In secure-R
Host: 192.168.1.224:8080\r\n	0090	65 71 75 65 73 74 73 3a	20 31 0d 0a 55 73 65 72	requests: 1-User
Connection: keep-alive\r\n	00a0	2d 41 67 65 6e 74 3a 20	4d 6f 7a 69 6c 6c 61 2f	-Agent: Mozilla/
DNT: 1\r\n	00b0	35 2e 30 20 28 5f 69 6e	64 6f 77 73 20 4e 54 20	5.0 (Windows NT
Upgrade-Insecure-Requests: 1\r\n	00c0	31 30 2e 30 3b 20 2f 69	6e 36 34 3b 20 78 36 34	10.0; Win64; x64
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537	00d0	29 20 41 70 70 6c 65 57	65 62 4b 69 74 2f 35 33) AppleWebKit/53
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a	00e0	37 2e 33 36 20 28 4b 48	54 4d 4c 2c 20 6c 69 6b	7.36 (KHTML, lik
Accept-Encoding: gzip, deflate\r\n	00f0	65 20 47 65 63 6b 6f 29	20 43 68 72 6f 6d 65 2f	e Gecko) Chrome/
Accept-Language: en-US,en;q=0.9\r\n	0100	31 34 33 2e 30 2e 30 2e	30 20 53 61 66 61 72 69	143.0.0.0 Safari
\r\n	0110	2f 35 33 37 2e 33 36 0d	0a 41 63 63 65 70 74 3a	/537.36- -Accept:
[Response in frame 8]	0120	20 74 65 78 74 2f 68 74	6d 6c 2c 61 70 70 6c 69	text/html,appli
[Full request URI: http://192.168.1.224:8080/redirect]	0130	63 61 74 69 6f 6e 2f 78	68 74 6d 6c 2b 78 6d 6c	cation/xhtml+xml
	0140	2c 61 70 70 6c 69 63 61	74 69 6f 6e 2f 78 6d 6c	,application/xml
	0150	3b 71 3d 30 2e 39 2c 69	6d 61 67 65 2f 61 76 69	;q=0.9,image/svg
	0160	66 2c 69 6d 61 67 65 2f	77 65 62 70 2c 69 6d 61	f,image/webp,ima
	0170	67 65 2f 61 70 70 6e 67 2c	2a 2f 2a 3b 71 3d 30 2e	ge/apng, */*;q=0.
	0180	38 2c 61 70 70 6c 69 63	61 74 69 6f 6e 2f 73 69	8,application/si
	0190	67 6e 65 64 2d 65 78 63	68 61 6e 67 65 3b 76 3d	gned-encoding;v=
	01a0	62 33 3b 71 3d 30 2e 37	6d 0a 41 63 63 65 70 74	b3;q=0.7 -Accept
	01b0	2d 45 6e 63 6f 64 69 6e	67 3a 20 67 7a 69 70 2c	-Encoding: gzip,
	01c0	20 64 65 66 6c 61 74 65	6d 0a 41 63 63 65 70 74	deflate -Accept
	01d0	2d 4c 61 6e 67 75 61 67	65 3a 20 65 6e 2d 55 53	-Language: en-US
	01e0	2c 65 6e 3b 71 3d 30 2e	39 8d 0a 6d 6a	,en;q=0.9.....

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=65485 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
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)]	0000 02 00 00 00 45 00 00 75 40 f8 40 00 48 06 00 00	...E-u@.@...
[TCP Segment Len: 77]	0010 c0 a8 01 e0 c0 a8 01 e0 1f 90 c9 21 47 98 87 8c:IG...
Sequence Number: 1 (relative sequence number)	0020 e9 0f 73 a9 50 18 27 f9 af 6e 00 00 18 94 34 50	...sP...n...HTTP
Sequence Number (raw): 1201178508	0030 2f 31 2e 31 20 33 30 31 20 41 6f 76 65 64 20 50	/1.1 301 Moved P
[Next Sequence Number: 78 (relative sequence number)]	0040 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 43 6f 6e 68	ermanently+conn
Acknowledgment Number: 450 (relative ack number)	0050 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 00 0a 4c	ection: close+L
Acknowledgment number (raw): 3910103977	0060 6f 63 61 74 69 6f 6e 3a 20 2f 72 65 73 75 6c 74	ocation: /result
0101 = Header Length: 20 bytes (5)	0070 7e 68 74 6d 6c 0d 0d 0d 0a	.html...
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=65485 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
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	0.008534	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]	0000 02 00 00 00 45 00 00 28 40 f8 40 00 48 06 00 00	...E-(@.@...
> Null/Loopback	0010 c0 a8 01 e0 c0 a8 01 e0 1f 90 c9 21 47 98 87 8c:IG...
> Internet Protocol Version 4, Src: 192.168.1.224, Dst: 192.168.1.224	0020 e9 0f 73 a9 50 11 27 f9 ed ec 00 00	...sP... ..
0100 = Version: 4		
.... 0101 = Header Length: 20 bytes (5)		
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
Total Length: 40		
Identification: 0x40fa (16634)		
> 0101 = 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	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	0.000066	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	0.008418	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
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	0.011302	192.168.1.224	192.168.1.224	TCP	44	51490 → 8080 [ACK] Seq=453 Ack=128 Win=2619648 Len=0
19	1.019527	192.168.1.224	192.168.1.224	TCP	44	8080 → 51490 [FIN, ACK] Seq=128 Ack=453 Win=2619648 Len=0
20	1.019562	192.168.1.224	192.168.1.224	TCP	44	51490 → 8080 [ACK] Seq=453 Ack=129 Win=2619648 Len=0
21	2.370566	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

Request in frame 15:
[Time since request: 2.530000 milliseconds]
[Request URI: /result.html]
[Full request URI: http://192.168.1.224:8080/result.html]
File Data: 64 bytes
Data: 3c68313e53756363657373213c2f68313e0a3c703e596f7520686176657f1aneth: 641

0010 c0 a8 01 e0 c0 a8 01 e0 1f 90 c9 22 1c 0c 29 85P..... HTTP
0020 e1 45 c1 ae 50 18 27 f9 09 d1 00 00 48 54 54 50 E..P..... /1.1 200 OK..Con
0030 2f 31 2e 31 20 32 30 30 20 4f 4b 0d 0a 43 6f 6e/. 200 OK..Con
0040 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c ..e. 65 65 70 2d 61 6c
0050 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e ..ive..Content-Len
0060 67 74 68 3a 20 36 34 0d 0a 00 0a 3c 68 31 3e 13 ..gth: 64.../1.1S
0070 72 63 13 65 73 72 11 30 47 60 31 0a 0a 3e 70 3a ..nstruction: keep-al
0080 59 6f 75 20 80 61 70 65 20 62 65 65 6e 20 72 65 ..You have open re
0090 64 69 72 65 63 74 65 64 20 70 6f 20 72 65 73 75 ..directed to resu
00a0 6c 74 3a 88 74 6d 6c 3c 2f 70 3a ..it.html.js

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	0.001830	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	0.004296	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	51856 → 8080 [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	1.008987	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