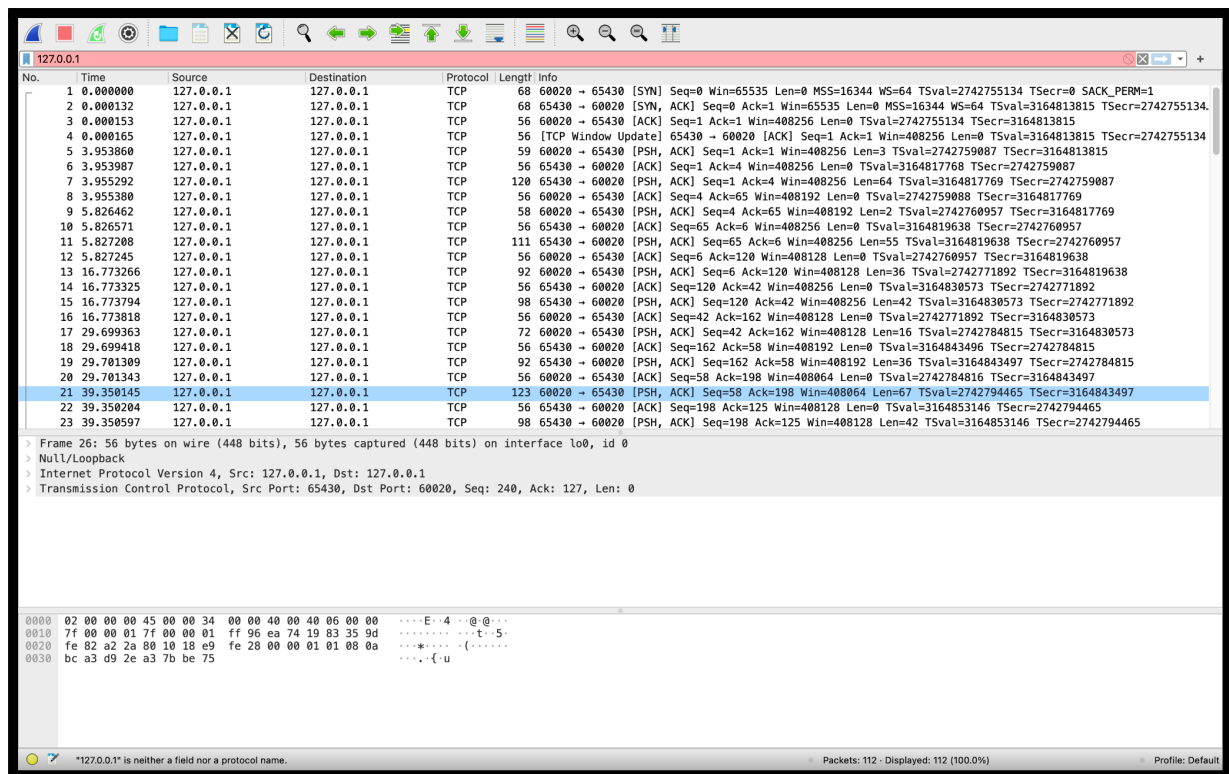We close all other processes running on the system and just run the client server interaction on the terminal. We capture this client server interaction on Wireshark.

Some noticeable points from the Wireshark dump are

1. Notice that first SYN and [SYN, ACK] appear which send the connection request followed by ACK which signifies the conformation of connection.
2. Host and the destination are same IP address since we were running in the standar loopback mode and connection to no external device was established.
3. Protocol for all the steps in the layers is TCP since this is the way we coded in the client and server.
4. SYN and ACK are seen more continuously and synchrously as compared to when we perform the dump analysis on the internet activities.
5. We can see the encrypted data. Which conforms that we were indeed using the functionalities of the crypt layer. See the marked-up 'dwc' and the reverse directory path in the bottom pane.

Wireshark capture — top window

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	68	60020 → 65430 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSval=2742755134 TSecr=0 SACK_PERM=1
2	0.000132	127.0.0.1	127.0.0.1	TCP	68	65430 → 60020 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=3164813815 TSecr=2742755134.
3	0.000153	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2742755134 TSecr=3164813815
4	0.000165	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 65430 → 60020 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=3164813815 TSecr=2742755134
5	3.953860	127.0.0.1	127.0.0.1	TCP	59	60020 → 65430 [PSH, ACK] Seq=1 Ack=1 Win=408256 Len=3 TSval=2742759087 TSecr=3164813815
6	3.953987	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=1 Ack=4 Win=408256 Len=0 TSval=3164817768 TSecr=2742759087
7	3.955292	127.0.0.1	127.0.0.1	TCP	120	65430 → 60020 [PSH, ACK] Seq=1 Ack=4 Win=408256 Len=64 TSval=3164817769 TSecr=2742759087
8	3.955380	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=4 Ack=65 Win=408192 Len=0 TSval=2742759088 TSecr=3164817769
9	5.826462	127.0.0.1	127.0.0.1	TCP	58	60020 → 65430 [PSH, ACK] Seq=4 Ack=65 Win=408192 Len=2 TSval=2742760957 TSecr=3164817769
10	5.826571	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=65 Ack=6 Win=408256 Len=0 TSval=3164819638 TSecr=2742760957
11	5.827208	127.0.0.1	127.0.0.1	TCP	111	65430 → 60020 [PSH, ACK] Seq=65 Ack=6 Win=408256 Len=55 TSval=3164819638 TSecr=2742760957
12	5.827245	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=6 Ack=120 Win=408128 Len=0 TSval=2742760957 TSecr=3164819638
13	16.773266	127.0.0.1	127.0.0.1	TCP	92	60020 → 65430 [PSH, ACK] Seq=6 Ack=120 Win=408128 Len=36 TSval=2742771892 TSecr=3164819638
14	16.773325	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=120 Ack=42 Win=408256 Len=0 TSval=3164830573 TSecr=2742771892
15	16.773794	127.0.0.1	127.0.0.1	TCP	98	65430 → 60020 [PSH, ACK] Seq=120 Ack=42 Win=408256 Len=42 TSval=3164830573 TSecr=2742771892
16	16.773818	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=42 Ack=162 Win=408128 Len=0 TSval=2742771892 TSecr=3164830573
17	29.699363	127.0.0.1	127.0.0.1	TCP	72	60020 → 65430 [PSH, ACK] Seq=42 Ack=162 Win=408128 Len=16 TSval=2742784815 TSecr=3164830573
18	29.699418	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=162 Ack=58 Win=408192 Len=0 TSval=3164843496 TSecr=2742784815
19	29.701309	127.0.0.1	127.0.0.1	TCP	92	65430 → 60020 [PSH, ACK] Seq=162 Ack=58 Win=408192 Len=36 TSval=3164843497 TSecr=2742784815
20	29.701343	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=58 Ack=198 Win=408064 Len=0 TSval=2742784816 TSecr=3164843497
21	39.350145	127.0.0.1	127.0.0.1	TCP	123	60020 → 65430 [PSH, ACK] Seq=58 Ack=198 Win=408064 Len=67 TSval=2742794465 TSecr=3164843497
22	39.350204	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=198 Ack=125 Win=408128 Len=0 TSval=3164853146 TSecr=2742794465
23	39.350597	127.0.0.1	127.0.0.1	TCP	98	65430 → 60020 [PSH, ACK] Seq=198 Ack=125 Win=408128 Len=42 TSval=3164853146 TSecr=2742794465

Frame 5: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface lo0, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 60020, Dst Port: 65430, Seq: 1, Ack: 1, Len: 3
Data (3 bytes)

```
0000  02 00 00 00 45 00 00 37  00 00 40 00 40 06 00 00   ····E··7 ··@·@··
0010  7f 00 00 01 7f 00 00 01  ea 74 ff 96 fe 82 a1 ac   ·········t······
0020  19 83 34 ae 80 18 18 eb  fe 2b 00 00 01 01 08 0a   ··4·····+·······
0030  a3 7b 2e af bc a3 39 f7  64 77 63                   ·{····9· dwc
```

wireshark_lo0KNESS1.pcapng — Packets: 112 · Displayed: 112 (100.0%) · Dropped: 0 (0.0%) — Profile: Default

Wireshark capture — bottom window

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000153	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=2742755134 TSecr=3164813815
4	0.000165	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 65430 → 60020 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=3164813815 TSecr=2742755134
5	3.953860	127.0.0.1	127.0.0.1	TCP	59	60020 → 65430 [PSH, ACK] Seq=1 Ack=1 Win=408256 Len=3 TSval=2742759087 TSecr=3164813815
6	3.953987	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=1 Ack=4 Win=408256 Len=0 TSval=3164817768 TSecr=2742759087
7	3.955292	127.0.0.1	127.0.0.1	TCP	120	65430 → 60020 [PSH, ACK] Seq=1 Ack=4 Win=408256 Len=64 TSval=3164817769 TSecr=2742759087
8	3.955380	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=4 Ack=65 Win=408192 Len=0 TSval=2742759088 TSecr=3164817769
9	5.826462	127.0.0.1	127.0.0.1	TCP	58	60020 → 65430 [PSH, ACK] Seq=4 Ack=65 Win=408192 Len=2 TSval=2742760957 TSecr=3164817769
10	5.826571	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=65 Ack=6 Win=408256 Len=0 TSval=3164819638 TSecr=2742760957
11	5.827208	127.0.0.1	127.0.0.1	TCP	111	65430 → 60020 [PSH, ACK] Seq=65 Ack=6 Win=408256 Len=55 TSval=3164819638 TSecr=2742760957
12	5.827245	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=6 Ack=120 Win=408128 Len=0 TSval=2742760957 TSecr=3164819638
13	16.773266	127.0.0.1	127.0.0.1	TCP	92	60020 → 65430 [PSH, ACK] Seq=6 Ack=120 Win=408128 Len=36 TSval=2742771892 TSecr=3164819638
14	16.773325	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=120 Ack=42 Win=408256 Len=0 TSval=3164830573 TSecr=2742771892
15	16.773794	127.0.0.1	127.0.0.1	TCP	98	65430 → 60020 [PSH, ACK] Seq=120 Ack=42 Win=408256 Len=42 TSval=3164830573 TSecr=2742771892
16	16.773818	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=42 Ack=162 Win=408128 Len=0 TSval=2742771892 TSecr=3164830573
17	29.699363	127.0.0.1	127.0.0.1	TCP	72	60020 → 65430 [PSH, ACK] Seq=42 Ack=162 Win=408128 Len=16 TSval=2742784815 TSecr=3164830573
18	29.699418	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=162 Ack=58 Win=408192 Len=0 TSval=3164843496 TSecr=2742784815
19	29.701309	127.0.0.1	127.0.0.1	TCP	92	65430 → 60020 [PSH, ACK] Seq=162 Ack=58 Win=408192 Len=36 TSval=3164843497 TSecr=2742784815
20	29.701343	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=58 Ack=198 Win=408064 Len=0 TSval=2742784816 TSecr=3164843497
21	39.350145	127.0.0.1	127.0.0.1	TCP	123	60020 → 65430 [PSH, ACK] Seq=58 Ack=198 Win=408064 Len=67 TSval=2742794465 TSecr=3164843497
22	39.350204	127.0.0.1	127.0.0.1	TCP	56	65430 → 60020 [ACK] Seq=198 Ack=125 Win=408128 Len=0 TSval=3164853146 TSecr=2742794465
23	39.350597	127.0.0.1	127.0.0.1	TCP	98	65430 → 60020 [PSH, ACK] Seq=198 Ack=125 Win=408128 Len=42 TSval=3164853146 TSecr=2742794465
24	39.350620	127.0.0.1	127.0.0.1	TCP	56	60020 → 65430 [ACK] Seq=125 Ack=240 Win=408000 Len=0 TSval=2742794465 TSecr=3164853146
25	40.779491	127.0.0.1	127.0.0.1	TCP	58	60020 → 65430 [PSH, ACK] Seq=125 Ack=240 Win=408000 Len=2 TSval=2742795893 TSecr=3164853146

Frame 7: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface lo0, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 65430, Dst Port: 60020, Seq: 1, Ack: 4, Len: 64
Data (64 bytes)

```
0000  02 00 00 00 45 00 00 74  00 00 40 00 40 06 00 00   ····E··t ··@·@··
0010  7f 00 00 01 7f 00 00 01  ff 96 ea 74 19 83 34 ae   ···········t··4·
0020  fe 82 a1 af 80 18 18 eb  fe 68 00 00 01 01 08 0a   ·········h······
0030  bc a3 49 69 a3 7b 2e af  65 64 6f 43 65 63 72 75   ··Ii·{.· edoCecru
0040  6f 53 2f 31 51 2f 31 41  5f 33 33 34 53 43 5f 36   oS/1Q/1A _334SC_6
0050  30 32 30 31 31 39 31 2f  70 6f 74 6b 73 65 44 2f   0201191/ potkseD/
0060  68 67 6e 69 73 70 61 74  61 72 70 68 73 65 6d 6f   hgnispat arphsemo
0070  73 2f 73 72 65 73 55 2f                            s/sresU/
```

wireshark_lo0KNESS1.pcapng — Packets: 112 · Displayed: 112 (100.0%) · Dropped: 0 (0.0%) — Profile: Default