

گزارش تحلیل ترافیک به وسیله وایرشارک

400130453

سهیل محمودی

تست سوکت

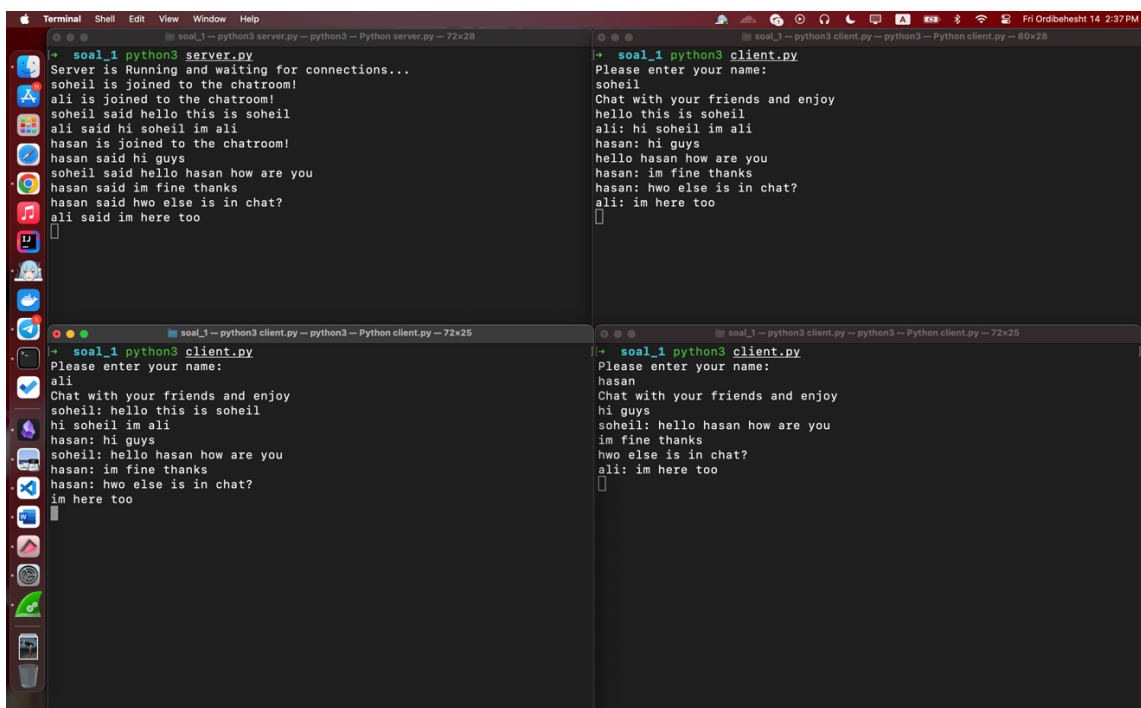
پروژه شماره ۵:

تحلیل ترافیک سوال یک :

چت همگانی

خروجی کد:

در تصویر زیر خروجی برنامه ی چت روم را مشاهده می کنیم که سه کلاینت با نام های سهیل، علی و حسن به سرور متصل شده و می توانند باهم چت کنند. در ابتدا برنامه نام کلاینت ها را گرفته و برای سرور ارسال می کند. سرور هم هر پیامی که ارسال می شود را با نام کلاینت نمایش می دهد.

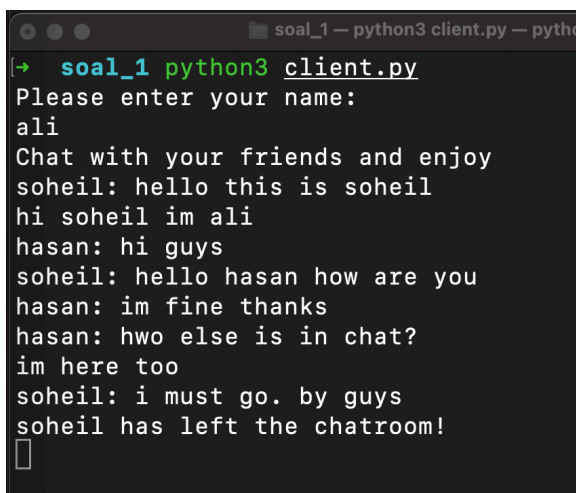


```
soal_1 python3 server.py
Server is Running and waiting for connections...
soheil is joined to the chatroom!
ali is joined to the chatroom!
soheil said hello this is soheil
ali said hi soheil im ali
hasan is joined to the chatroom!
hasan said hi guys
soheil said hello hasan how are you
hasan said im fine thanks
hasan said hwo else is in chat?
ali said im here too

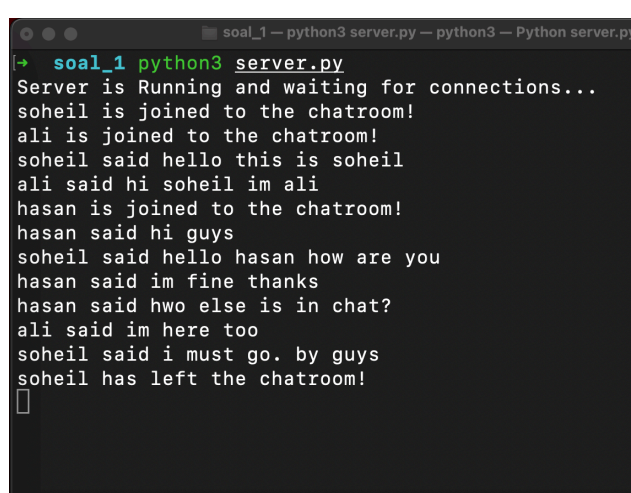
soal_1 python3 client.py
Please enter your name:
soheil
Chat with your friends and enjoy
soheil: hello this is soheil
hi soheil im ali
hasan: hi guys
soheil: hello hasan how are you
hasan: im fine thanks
hasan: hwo else is in chat?
ali: im here too

soal_1 python3 client.py
Please enter your name:
ali
Chat with your friends and enjoy
soheil: hello this is soheil
hi soheil im ali
hasan: hi guys
soheil: hello hasan how are you
im fine thanks
hwo else is in chat?
ali: im here too
```

در نهایت هم با خروج هر کلاینت از سرور، پیام خروج آن از چت روم گزارش می شود.



```
soal_1 python3 client.py
Please enter your name:
ali
Chat with your friends and enjoy
soheil: hello this is soheil
hi soheil im ali
hasan: hi guys
soheil: hello hasan how are you
hasan: im fine thanks
hasan: hwo else is in chat?
im here too
soheil: i must go. by guys
soheil has left the chatroom!
```



```
soal_1 python3 server.py
Server is Running and waiting for connections...
soheil is joined to the chatroom!
ali is joined to the chatroom!
soheil said hello this is soheil
ali said hi soheil im ali
hasan is joined to the chatroom!
hasan said hi guys
soheil said hello hasan how are you
hasan said im fine thanks
hasan said hwo else is in chat?
ali said im here too
soheil said i must go. by guys
soheil has left the chatroom!
```

تحلیل ترافیک Wiershark:

همانطور که می دانیم، برنامه از پروتکل TCP استفاده می کند و این پروتکل بر پایه ی Acknowledgment است. در ۳ پکت اول کلاینت با پورت ۵۷۳۹۶ به سرور با پورت ۵۰۵۰ متصل شده در خواست کانکشن داده و پس از متصل شدن هر دو پیامی مبنا بر Acknowledgment برای یکدیگر فرستاده اند.

Wireshark packet capture showing the initial TCP connection setup. The packet list shows packets 1, 2, and 3. Packet 1 is a SYN from 127.0.0.1 to 127.0.0.3. Packet 2 is a SYN-ACK from 127.0.0.3 to 127.0.0.1. Packet 3 is an ACK from 127.0.0.1 to 127.0.0.3. The packet details pane shows the TCP segment information for packet 3, including sequence number 1, acknowledgment number 1, and window size 65535.

همانطور که گفته شد مثال دیگری از نحوه ی ارتباط سرور و کلاینت ها در عکس های زیر آورده شده است. کلاینت باپورت ۵۷۳۹۶ پیامی با دیتای ”hello hsan how are you” برای سرور (۵۰۵۰) ارسال کرده و سرور هم برای آن Acknowledgment ارسال کرده است.

Wireshark packet capture showing the data transfer and acknowledgment. The packet list shows packets 4 through 6. Packet 4 is a data packet from 127.0.0.1 to 127.0.0.3. Packet 5 is an ACK from 127.0.0.3 to 127.0.0.1. Packet 6 is a data packet from 127.0.0.3 to 127.0.0.1. The packet details pane for packet 4 shows the data field containing "hello hsan how are you". The packet details pane for packet 5 shows the acknowledgment number 36. The packet details pane for packet 6 shows the data field containing "san how are you".

دیتای ارسال شده

در مرحله ی بعد سرور آن پیام را (به همراه اسم کلاینت ارسال کننده) برای دو کلاینت دیگر با پورت های ۵۷۴۲۶ و ۵۷۴۶۰ فرستاده و هر کدام از آن کلاینت ها یک پکت برای Acknowledgment به سرور ارسال کرده اند که این ۴ پکت در اسکرین شات زیر select شده اند:

No.	Time	Protocol	Source	Destination	Length	Info
26	118.881693	TCP	127.0.0.3	127.0.0.3	56	5050 → 57460 [ACK] Seq=1 Ack=6 Win=408256 Len=0 TSval=710317159 TSecr=2460217295
27	123.062316	TCP	127.0.0.3	127.0.0.3	63	57460 → 5050 [PSH, ACK] Seq=6 Ack=1 Win=408256 Len=7 TSval=2460221476 TSecr=710317159
28	123.062372	TCP	127.0.0.3	127.0.0.3	56	5050 → 57460 [ACK] Seq=1 Ack=13 Win=408256 Len=0 TSval=710321340 TSecr=2460221476
29	123.062697	TCP	127.0.0.3	127.0.0.3	70	5050 → 57396 [PSH, ACK] Seq=22 Ack=27 Win=408256 Len=14 TSval=599119515 TSecr=3751187732
30	123.062714	TCP	127.0.0.3	127.0.0.3	70	5050 → 57426 [PSH, ACK] Seq=29 Ack=20 Win=408256 Len=14 TSval=969199022 TSecr=2469751759
31	123.062723	TCP	127.0.0.3	127.0.0.3	56	57396 → 5050 [ACK] Seq=27 Ack=36 Win=408256 Len=0 TSval=3751202994 TSecr=599119515
32	123.062736	TCP	127.0.0.3	127.0.0.3	56	57426 → 5050 [ACK] Seq=20 Ack=43 Win=408256 Len=0 TSval=2469767021 TSecr=969199022
33	139.117796	TCP	127.0.0.3	127.0.0.3	79	57396 → 5050 [PSH, ACK] Seq=27 Ack=36 Win=408256 Len=23 TSval=3751219650 TSecr=599119515
34	139.117835	TCP	127.0.0.3	127.0.0.3	56	5050 → 57396 [ACK] Seq=36 Ack=50 Win=408192 Len=0 TSval=599135571 TSecr=3751219050
35	139.118954	TCP	127.0.0.3	127.0.0.3	87	5050 → 57426 [PSH, ACK] Seq=43 Ack=20 Win=408256 Len=31 TSval=969215979 TSecr=2469767021
36	139.118978	TCP	127.0.0.3	127.0.0.3	87	5050 → 57460 [PSH, ACK] Seq=1 Ack=13 Win=408256 Len=31 TSval=710337397 TSecr=2460221476
37	139.118987	TCP	127.0.0.3	127.0.0.3	56	57426 → 5050 [ACK] Seq=20 Ack=74 Win=408192 Len=0 TSval=2469783078 TSecr=969215079
38	139.119086	TCP	127.0.0.3	127.0.0.3	56	57460 → 5050 [ACK] Seq=13 Ack=32 Win=408256 Len=0 TSval=2460237533 TSecr=710337397
39	152.160839	TCP	127.0.0.3	127.0.0.3	71	57460 → 5050 [PSH, ACK] Seq=13 Ack=32 Win=408256 Len=15 TSval=2460250576 TSecr=710337397
40	152.160911	TCP	127.0.0.3	127.0.0.3	56	5050 → 57460 [ACK] Seq=32 Ack=28 Win=408256 Len=0 TSval=710339440 TSecr=2460250576
41	152.161231	TCP	127.0.0.3	127.0.0.3	78	5050 → 57396 [PSH, ACK] Seq=36 Ack=50 Win=408192 Len=22 TSval=599148615 TSecr=3751219050
42	152.161264	TCP	127.0.0.3	127.0.0.3	56	57396 → 5050 [ACK] Seq=50 Ack=58 Win=408192 Len=0 TSval=3751232094 TSecr=599148615
43	152.161299	TCP	127.0.0.3	127.0.0.3	78	5050 → 57426 [PSH, ACK] Seq=74 Ack=20 Win=408256 Len=22 TSval=969228122 TSecr=2469783078
44	152.161325	TCP	127.0.0.3	127.0.0.3	56	57426 → 5050 [ACK] Seq=20 Ack=96 Win=408192 Len=0 TSval=2469796121 TSecr=969228122
45	189.984794	TCP	127.0.0.3	127.0.0.3	76	57460 → 5050 [PSH, ACK] Seq=28 Ack=32 Win=408256 Len=20 TSval=2460288321 TSecr=710350440
46	189.984844	TCP	127.0.0.3	127.0.0.3	56	5050 → 57460 [ACK] Seq=32 Ack=40 Win=408192 Len=0 TSval=710308185 TSecr=2460288321

پکت هایی که سرور با پورت ۵۰۵۰ به کلاینت ها ارسال کرده حاوی دیتای زیر بوده اند:

<pre> > Frame 35: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface lo0, id 0 > Null/Loopback > Internet Protocol Version 4, Src: 127.0.0.3, Dst: 127.0.0.3 > Transmission Control Protocol, Src Port: 5050, Dst Port: 57426, Seq: 43, Ack: 20, Len: 31 Source Port: 5050 Destination Port: 57426 [Stream index: 1] [Conversation completeness: Complete, WITH_DATA (31)] [TCP Segment Len: 31] Sequence Number: 43 (relative sequence number) Sequence Number (raw): 3115644527 [Next Sequence Number: 74 (relative sequence number)] Acknowledgment Number: 20 (relative ack number) Acknowledgment number (raw): 715977238 1000 = Header Length: 32 bytes (8) > Flags: 0x010 (PSH, ACK) Window: 6379 [Calculated window size: 408256] [Window size scaling factor: 64] Checksum: 0xfe4b [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps > [Timestamps] > [SEQ/ACK analysis] TCP payload (31 bytes) > Data (31 bytes) Data: 726f6865696c3a2068656c6c6f20686173616e20686f772061726520796f75 [Length: 31] </pre>	<pre> 0000 02 00 00 00 45 00 00 53 00 00 40 00 40 06 00 00 E..S..@... 0010 7f 00 00 03 7f 00 00 03 13 ba e0 52 09 b4 16 0f R..... 0020 2a ac f2 16 08 18 18 eb fe 4b 00 00 01 01 08 0a *.....K..... 0030 39 c5 0c 67 93 35 a7 6d 73 6f 68 65 69 6c 3a 20 9:g:5 m \$hell 0040 68 65 6c 6c 6f 20 68 61 73 61 6e 20 68 6f 77 20 hello ha san how 0050 61 72 65 20 79 6f 75 are you </pre>
--	--

در نهایت کلاینت با پورت ۵۷۳۹۶ یک پکت به همراه flag های FIN و ACK به سرور ارسال کرده است که FIN نشان می‌دهد که فرستنده، ارسال داده‌ها را به پایان رسانده و می‌خواهد اتصال را ببندد. زمانی که بسته TCP دارای پرچم FIN باشد، به این معناست که این آخرین انتقال داده است و اتصال باید بسته شود:

The image shows a Wireshark packet capture interface. The top pane displays a list of network packets. Packet 63 is highlighted, showing a TCP segment from 127.0.0.1 to 127.0.0.1 on port 5050. The packet details pane on the right shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Protocol	Source	Destination	Length	Info
56	229.262700	TCP	127.0.0.3	127.0.0.3	56	57460 → 5050 [ACK] Seq=48 Ack=48 Win=408192 Len=0 TSval=246834713 TSecr=718427853
57	229.570734	TCP	127.0.0.3	127.0.0.3	74	57396 → 5050 [PSH, ACK] Seq=50 Ack=101 Win=408192 Len=18 TSval=3751309507 TSecr=599201718
58	229.570770	TCP	127.0.0.3	127.0.0.3	56	5050 → 57396 [ACK] Seq=101 Ack=68 Win=408192 Len=0 TSval=599226028 TSecr=3751309507
59	229.570959	TCP	127.0.0.3	127.0.0.3	82	5050 → 57426 [PSH, ACK] Seq=123 Ack=31 Win=408256 Len=26 TSval=969305535 TSecr=2469849224
60	229.570974	TCP	127.0.0.3	127.0.0.3	56	57426 → 5050 [ACK] Seq=31 Ack=149 Win=408128 Len=0 TSval=2469873534 TSecr=969305535
61	229.571001	TCP	127.0.0.3	127.0.0.3	82	5050 → 57460 [PSH, ACK] Seq=48 Ack=48 Win=408192 Len=26 TSval=718427853 TSecr=2468303679
62	229.571020	TCP	127.0.0.3	127.0.0.3	56	57460 → 5050 [ACK] Seq=48 Ack=74 Win=408192 Len=0 TSval=2468327989 TSecr=718427853
63	231.122111	TCP	127.0.0.3	127.0.0.3	56	57396 → 5050 [FIN, ACK] Seq=69 Ack=101 Win=408192 Len=0 TSval=3751311338 TSecr=599226028
64	231.402360	TCP	127.0.0.3	127.0.0.3	56	5050 → 57396 [ACK] Seq=101 Ack=69 Win=408192 Len=0 TSval=599227859 TSecr=3751311338
65	231.402639	TCP	127.0.0.3	127.0.0.3	56	5050 → 57396 [FIN, ACK] Seq=101 Ack=69 Win=408192 Len=0 TSval=599227859 TSecr=3751311338
66	231.402688	TCP	127.0.0.3	127.0.0.3	56	57396 → 5050 [ACK] Seq=69 Ack=102 Win=408192 Len=0 TSval=3751311338 TSecr=599227859
67	231.402744	TCP	127.0.0.3	127.0.0.3	85	5050 → 57426 [PSH, ACK] Seq=149 Ack=31 Win=408256 Len=29 TSval=969307366 TSecr=2469873534
68	231.402760	TCP	127.0.0.3	127.0.0.3	85	5050 → 57460 [PSH, ACK] Seq=74 Ack=48 Win=408192 Len=29 TSval=718429684 TSecr=2468327989
69	231.402783	TCP	127.0.0.3	127.0.0.3	56	57426 → 5050 [ACK] Seq=31 Ack=170 Win=408064 Len=0 TSval=2469875365 TSecr=969307366
70	231.402795	TCP	127.0.0.3	127.0.0.3	56	57460 → 5050 [ACK] Seq=48 Ack=103 Win=408192 Len=0 TSval=2468329820 TSecr=718429684
71	246.294400	TCP	127.0.0.3	127.0.0.3	56	57460 → 5050 [FIN, ACK] Seq=48 Ack=103 Win=408192 Len=0 TSval=2468344713 TSecr=718429684
72	246.294470	TCP	127.0.0.3	127.0.0.3	56	5050 → 57460 [ACK] Seq=103 Ack=49 Win=408192 Len=0 TSval=718444577 TSecr=2468344713
73	246.294956	TCP	127.0.0.3	127.0.0.3	56	5050 → 57460 [FIN, ACK] Seq=103 Ack=49 Win=408192 Len=0 TSval=718444577 TSecr=2468344713
74	246.295004	TCP	127.0.0.3	127.0.0.3	56	57460 → 5050 [ACK] Seq=49 Ack=104 Win=408192 Len=0 TSval=2468344713 TSecr=718444577
75	246.295237	TCP	127.0.0.3	127.0.0.3	84	5050 → 57426 [PSH, ACK] Seq=178 Ack=31 Win=408256 Len=28 TSval=969322259 TSecr=2469875365
76	246.295262	TCP	127.0.0.3	127.0.0.3	56	57426 → 5050 [ACK] Seq=31 Ack=206 Win=408064 Len=0 TSval=2469890250 TSecr=969322259

Frame 63: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface lo0, id 0

- Null/Loopback
- Internet Protocol Version 4, Src: 127.0.0.3, Dst: 127.0.0.3
- Transmission Control Protocol, Src Port: 57396, Dst Port: 5050, Seq: 68, Ack: 101, Len: 0**
 - Source Port: 57396
 - Destination Port: 5050
 - [Stream index: 0]
 - [Conversation completeness: Complete, WITH_DATA (31)]
 - [TCP Segment Len: 0]
 - Sequence Number: 68 (relative sequence number)
 - Sequence Number (raw): 2477615619
 - [Next Sequence Number: 69 (relative sequence number)]
 - Acknowledgment Number: 101 (relative ack number)
 - Acknowledgment number (raw): 408559756
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x011 (FIN, ACK)
 - Window: 6378
 - [Calculated window size: 408192]
 - [Window size scaling factor: 64]
 - Checksum: 0xfe2c [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - [Timestamps]

Flags: 0x011 (tcp.flags), 2 bytes

Packets: 80 - Displayed: 80 (100.0%)

Profile: Default