

# گزارش تحلیل ترافیک به وسیله وایرشارک

400130453

سهیل محمودی

تست سوکت

پروژه شماره ۵:

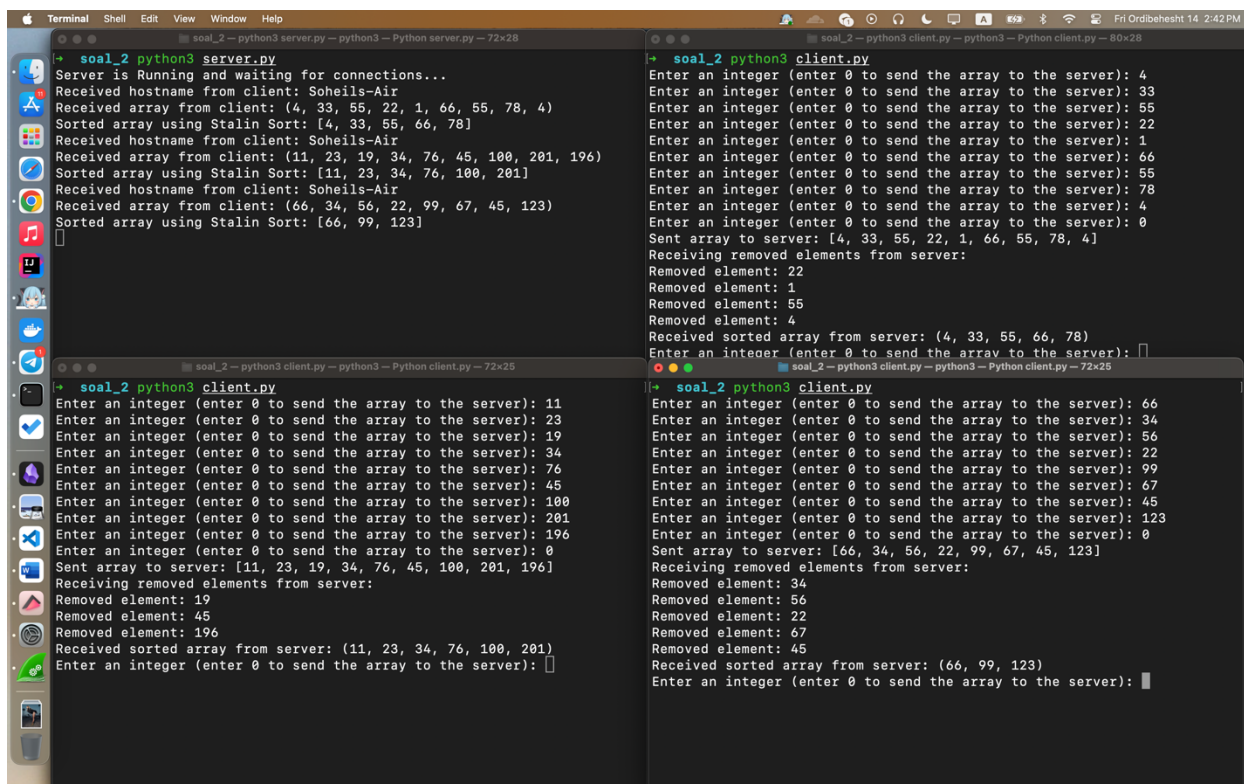
تحلیل ترافیک سوال دو:

استالین

## خروجی کد:

در تصویر زیر خروجی برنامه را مشاهده می کنیم که ابتدا زمانی که هر یک از کلاینت ها به سرور متصل می شوند hostname آن ها برای سرور ارسال می شود و هر کلاینت تعدادی عدد ورودی گرفته و آن را برای سرور می فرستد. سرور آن را گرفته و الگوریتم اسلاین سورت را بر روی آن اجرا می کند و هر زمان که عددی از آرایه بیرون ریخته می شود، آن را به کلاینت فرستاده گزارش می کند. در نهایت آرایه ی اعداد مرتب شده را برای کلاینت فرستاده و کلاینت آن را چاپ می کند.

(در این برنامه چون همه ی کلاینت ها بر روی IP یکسان هستند، hostname آن ها یکسان و برابر با hostname سیستم ، Soheils-Air ، می باشد.)



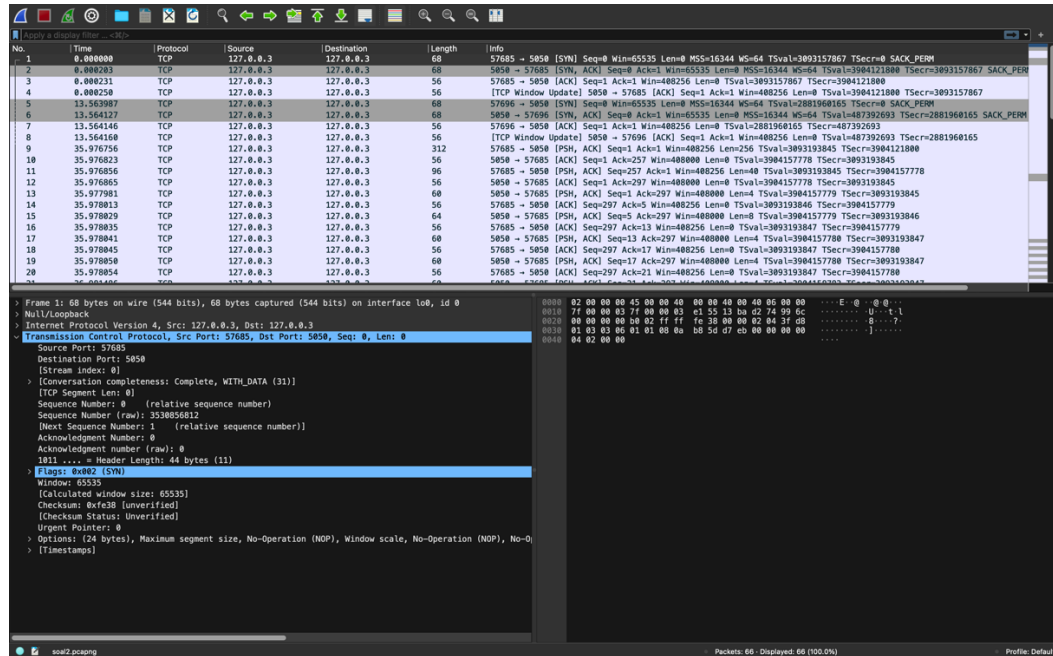
```
soal_2 python3 server.py
Server is Running and waiting for connections...
Received hostname from client: Soheils-Air
Received array from client: (4, 33, 55, 22, 1, 66, 55, 78, 4)
Sorted array using Stalin Sort: [4, 33, 55, 66, 78]
Received hostname from client: Soheils-Air
Received array from client: (11, 23, 19, 34, 76, 45, 100, 201, 196)
Sorted array using Stalin Sort: [11, 23, 34, 76, 100, 201]
Received hostname from client: Soheils-Air
Received array from client: (66, 34, 56, 22, 99, 67, 45, 123)
Sorted array using Stalin Sort: [66, 99, 123]

soal_2 python3 client.py
Enter an integer (enter 0 to send the array to the server): 4
Enter an integer (enter 0 to send the array to the server): 33
Enter an integer (enter 0 to send the array to the server): 55
Enter an integer (enter 0 to send the array to the server): 22
Enter an integer (enter 0 to send the array to the server): 1
Enter an integer (enter 0 to send the array to the server): 66
Enter an integer (enter 0 to send the array to the server): 55
Enter an integer (enter 0 to send the array to the server): 78
Enter an integer (enter 0 to send the array to the server): 4
Enter an integer (enter 0 to send the array to the server): 0
Sent array to server: [4, 33, 55, 22, 1, 66, 55, 78, 4]
Receiving removed elements from server:
Removed element: 22
Removed element: 1
Removed element: 55
Removed element: 4
Received sorted array from server: (4, 33, 55, 66, 78)
Enter an integer (enter 0 to send the array to the server):

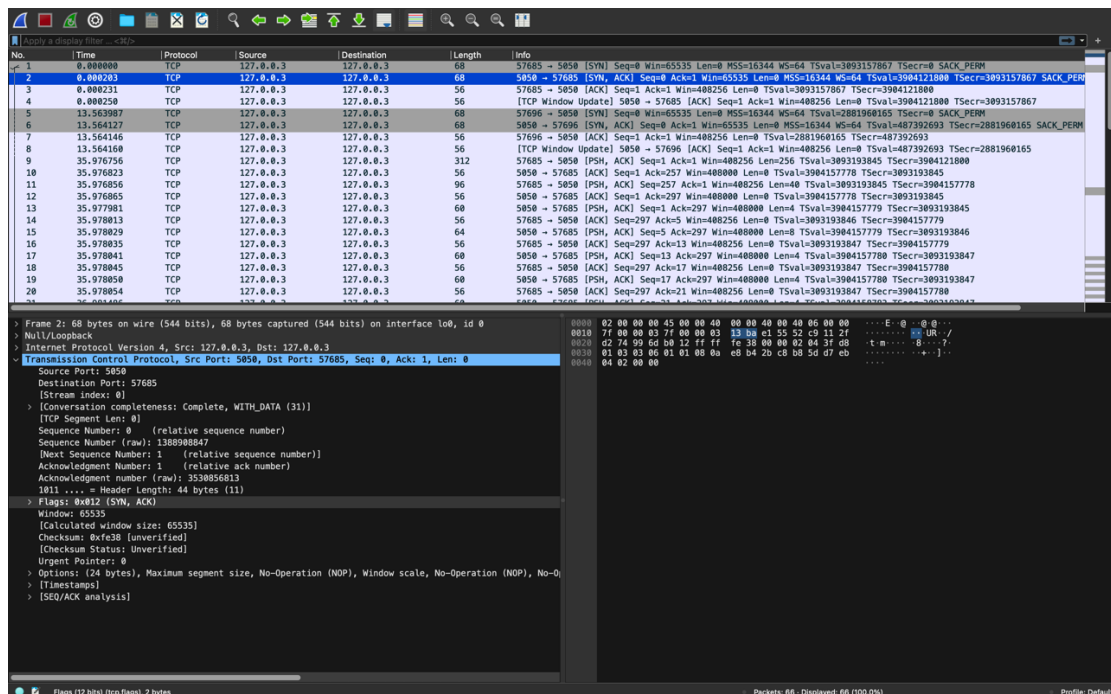
soal_2 python3 client.py
Enter an integer (enter 0 to send the array to the server): 66
Enter an integer (enter 0 to send the array to the server): 34
Enter an integer (enter 0 to send the array to the server): 56
Enter an integer (enter 0 to send the array to the server): 22
Enter an integer (enter 0 to send the array to the server): 99
Enter an integer (enter 0 to send the array to the server): 67
Enter an integer (enter 0 to send the array to the server): 45
Enter an integer (enter 0 to send the array to the server): 123
Enter an integer (enter 0 to send the array to the server): 0
Sent array to server: [66, 34, 56, 22, 99, 67, 45, 123]
Receiving removed elements from server:
Removed element: 34
Removed element: 56
Removed element: 22
Removed element: 67
Removed element: 45
Received sorted array from server: (66, 99, 123)
Enter an integer (enter 0 to send the array to the server):
```

# تحلیل ترافیک Wireshark:

در ابتدا هر کلاینت که می خواهد به سرور متصل شود یک پکت حاوی SYN flag به سرور ارسال می کند. همانطور که در تصویر زیر مشاهده می کنیم، کلاینت با پورت ۵۷۶۸۵ این پکت را به سرور ارسال کرده است.



سپس سرور با پورت ۵۰۵۰ یک پکت حاوی flag های SYN و ACK برای کلاینت ارسال کرده و کلاینت به سرور متصل شده است.



اینکه بسته تحویل گرفته شد از سوی سرور به کلاینت ارسال شده است.

[illegible]

برای سرور فرستاده و Acknowledgment آن را هم دریافت کرده است.

[illegible]

از پکت ۲۹ تا ۳۶ همانطور که مشاهده می کنیم یک در میان یک پکت از سرور با پورت ۵۰۵۰ برای کلاینت با پورت ۵۷۶۹۶ ارسال شده و پس از Acknowledgment آن را از همان کلاینت دریافت کرده است. این ۸ پکت برای ارسال index های دلالت شده از آرایه است و در نهایت آخرین پکتی که از سرور به این کلاینت ارسال شده حاوی آرایه ی مرتب شده توسط Stalin sort algorithm است:

No.	Time	Protocol	Source	Destination	Length	Info
21	36.981486	TCP	127.0.0.3	127.0.0.3	68	5850 → 57685 [PSH, ACK] Seq=21 Ack=297 Win=408000 Len=4 TSval=3904158783 TSecr=3093193847
22	36.981554	TCP	127.0.0.3	127.0.0.3	56	57685 → 5850 [ACK] Seq=297 Ack=25 Win=408256 Len=0 TSval=3093194850 TSecr=3904158783
23	36.981583	TCP	127.0.0.3	127.0.0.3	76	5850 → 57685 [PSH, ACK] Seq=25 Ack=297 Win=408000 Len=20 TSval=3904158783 TSecr=3093194850
24	36.981591	TCP	127.0.0.3	127.0.0.3	56	57685 → 5850 [ACK] Seq=297 Ack=45 Win=408256 Len=0 TSval=3093194850 TSecr=3904158783
25	69.984499	TCP	127.0.0.3	127.0.0.3	312	57696 → 5850 [PSH, ACK] Seq=1 Ack=1 Win=408256 Len=256 TSval=2882016587 TSecr=487392693
26	69.984558	TCP	127.0.0.3	127.0.0.3	56	5850 → 57696 [ACK] Seq=1 Ack=257 Win=408000 Len=0 TSval=487449115 TSecr=2882016587
27	69.984588	TCP	127.0.0.3	127.0.0.3	96	57696 → 5850 [PSH, ACK] Seq=257 Ack=1 Win=408256 Len=40 TSval=2882016587 TSecr=487449115
28	69.984596	TCP	127.0.0.3	127.0.0.3	56	5850 → 57696 [ACK] Seq=1 Ack=297 Win=408000 Len=0 TSval=487449115 TSecr=2882016587
29	69.985266	TCP	127.0.0.3	127.0.0.3	60	5850 → 57696 [PSH, ACK] Seq=1 Ack=297 Win=408000 Len=4 TSval=487449115 TSecr=2882016587
30	69.985296	TCP	127.0.0.3	127.0.0.3	56	57696 → 5850 [ACK] Seq=297 Ack=5 Win=408256 Len=0 TSval=2882016587 TSecr=487449115
31	69.985312	TCP	127.0.0.3	127.0.0.3	68	5850 → 57696 [PSH, ACK] Seq=5 Ack=297 Win=408000 Len=12 TSval=487449115 TSecr=2882016587
32	69.985317	TCP	127.0.0.3	127.0.0.3	56	57696 → 5850 [ACK] Seq=297 Ack=17 Win=408256 Len=0 TSval=2882016587 TSecr=487449115
33	70.998466	TCP	127.0.0.3	127.0.0.3	60	5850 → 57696 [PSH, ACK] Seq=17 Ack=297 Win=408000 Len=4 TSval=487450121 TSecr=2882016587
34	70.998530	TCP	127.0.0.3	127.0.0.3	56	57696 → 5850 [ACK] Seq=297 Ack=21 Win=408256 Len=0 TSval=2882017593 TSecr=487450121
35	70.998559	TCP	127.0.0.3	127.0.0.3	80	5850 → 57696 [PSH, ACK] Seq=21 Ack=297 Win=408000 Len=24 TSval=487450121 TSecr=2882017593
36	70.998566	TCP	127.0.0.3	127.0.0.3	56	57696 → 5850 [ACK] Seq=297 Ack=45 Win=408256 Len=0 TSval=2882017593 TSecr=487450121
37	85.871574	TCP	127.0.0.3	127.0.0.3	68	57749 → 5850 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=3019276528 TSecr=0 SACK_PERM
38	85.871708	TCP	127.0.0.3	127.0.0.3	68	5850 → 57749 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=64 TSval=1525021626 TSecr=3019276528 SACK_PERM
39	85.871726	TCP	127.0.0.3	127.0.0.3	56	57749 → 5850 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=3019276528 TSecr=1525021626
40	85.871738	TCP	127.0.0.3	127.0.0.3	56	[TCP Window Update] 5850 → 57749 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=1525021626 TSecr=3019276528
41	115.074649	TCP	127.0.0.3	127.0.0.3	312	57749 → 5850 [PSH, ACK] Seq=1 Ack=1 Win=408256 Len=256 TSval=3019305732 TSecr=1525021626

برای مثال پکت شماره ی ۳۱ حاوی ۱۲ بایت دیتا است و آرایه ی مرتب شده در پکت ۳۵ برای کلاینت ارسال شده است که اطلاعات هر دو پکت در زیر آورده شده است:

```
> Frame 31: 68 bytes on wire (544 bits), 68 bytes captured (544 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: 5850, Dst Port: 57696, Seq: 5, Ack: 297, Len: 12
  Source Port: 5850
  Destination Port: 57696
  [Stream index: 1]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 12]
  Sequence Number: 5 (relative sequence number)
  Sequence Number (raw): 2952282682
  [Next Sequence Number: 17 (relative sequence number)]
  Acknowledgment Number: 297 (relative ack number)
  Acknowledgment number (raw): 3590683239
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x018 (PSH, ACK)
  Window: 6375
  [Calculated window size: 408000]
  [Window size scaling factor: 64]
  Checksum: 0xfe38 (unverified)
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (12 bytes)
  Data (12 bytes)
    Data: 0000002d000000c400000000
    [Length: 12]
```

```
> Frame 35: 80 bytes on wire (640 bits), 80 bytes captured (640 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: 5850, Dst Port: 57696, Seq: 21, Ack: 297, Len: 24
  Source Port: 5850
  Destination Port: 57696
  [Stream index: 1]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 24]
  Sequence Number: 21 (relative sequence number)
  Sequence Number (raw): 2952282698
  [Next Sequence Number: 45 (relative sequence number)]
  Acknowledgment Number: 297 (relative ack number)
  Acknowledgment number (raw): 3590683239
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x018 (PSH, ACK)
  Window: 6375
  [Calculated window size: 408000]
  [Window size scaling factor: 64]
  Checksum: 0xfe44 (unverified)
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (24 bytes)
  Data (24 bytes)
    Data: 0000000b00000017000000220000004c00000064000000c9
    [Length: 24]
```