



# Computer Network



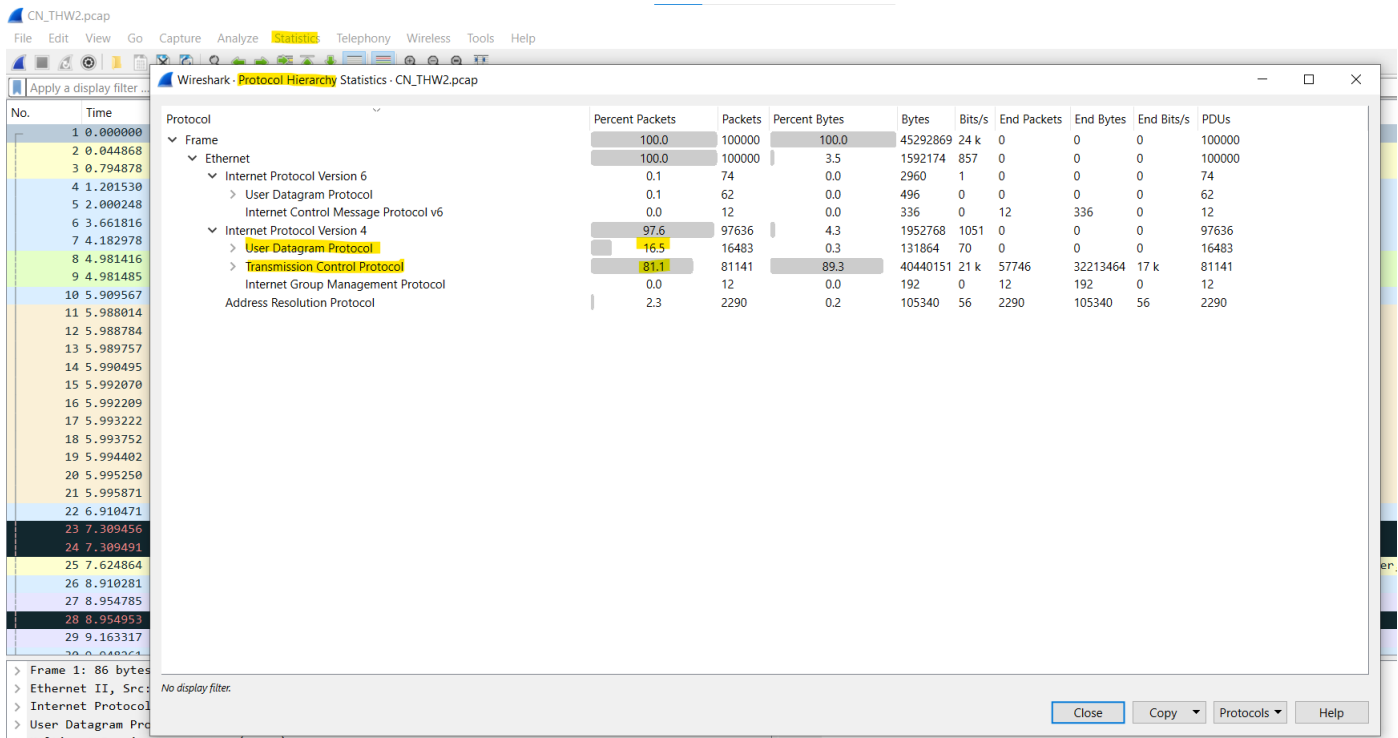
**AmirReza Azari**  
**99101087**

## ادامه تمرین دوم

### وایر شارک

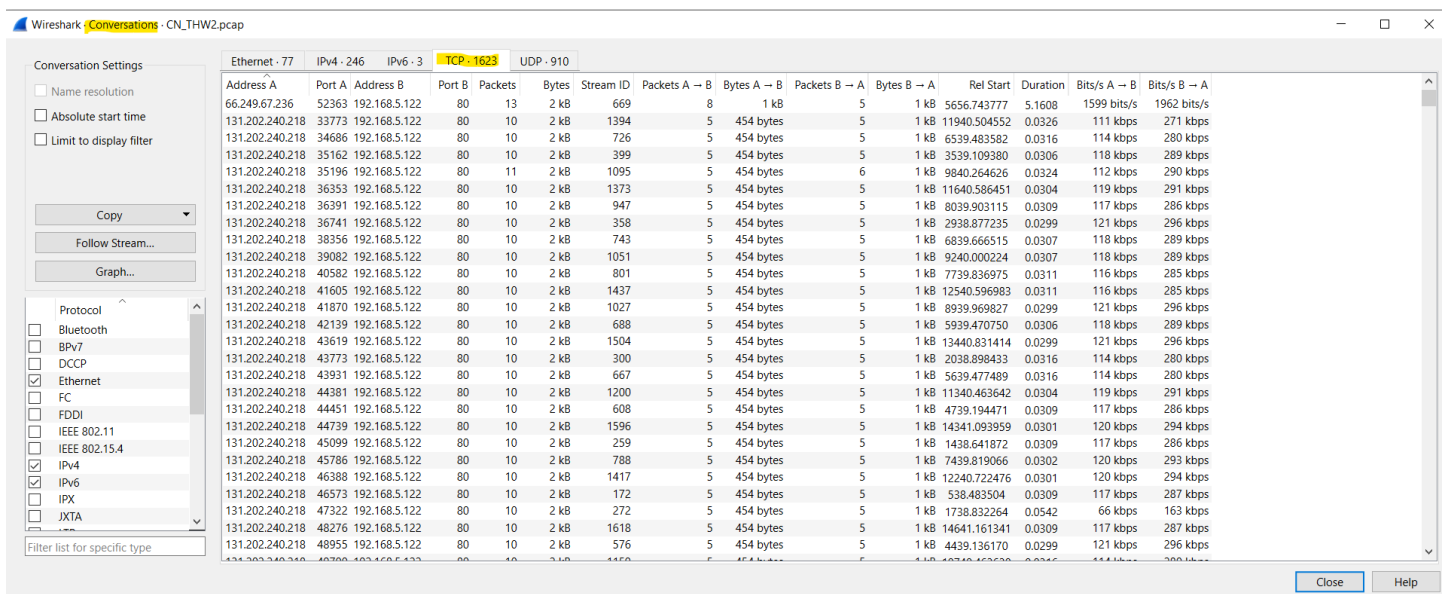
۱. پروتکل لایه انتقال در چند درصد از این بسته‌ها *TCP* و در چند درصد *UDP* است؟
۲. بسته‌های دیگر (غیر از *TCP*، *UDP*) مربوط به چه پروتکلی هستند؟  
گاهی لازم است برای تحلیل ترافیک شبکه، بسته‌ها را به شکل جریان (*flow*) های مجزایی در لایه انتقال بررسی کنیم. منظور از یک جریان *TCP* همه بسته‌هایی است که اولاً حاوی قطعات *TCP* هستند و ثانياً آدرس‌های *IP* و شماره‌های پورت مبدا و مقصدشان یکی است. گاهی برای تمایز جریان‌های *TCP*، زمان را هم در نظر می‌گیرند. به این معنا که اختلاف دو بسته در یک جریان *TCP* از حد خاصی بیش‌تر نباشد. هرچند ما در این تمرین زمان را در نظر نمی‌گیریم.
۳. به‌طور کلی هر جریان *TCP* با چه بسته (هایی) شروع می‌شود و با چه بسته (هایی) خاتمه می‌یابد؟
۴. چند بسته حاوی *SYN Segment* در این فایل می‌بینید؟ (بدون *ACK*)
۵. چند بسته حاوی *SYN-ACK Segment* در این فایل می‌بینید؟ به‌نظر شما چرا تعداد این بسته‌ها با تعداد بسته‌های حاوی *SYN Segment* متفاوت است؟
۶. چند بسته حاوی *FIN-ACK Segment* در این فایل می‌بینید؟ به‌نظر شما چرا تعداد این بسته‌ها با تعداد بسته‌های حاوی *SYN Segment* متفاوت است؟
۷. چند بسته حاوی *FIN Segment* در این فایل می‌بینید؟ (بدون *ACK*) به‌نظرتان چرا این‌طور است؟
۸. با توجه به پاسخ چند سوال قبل، یک راه تقریبی برای شمارش جریان‌های *TCP* در این فایل پیشنهاد دهید.  
بسته‌های شماره‌ی ۵۰۱۶ تا ۵۰۱۹ را در نظر گرفته و جریان مربوط به آن‌ها را جدا کنید. (برای جدا کردن بسته‌های مربوط به یک جریان *TCP*، روی یکی از بسته‌ها کلیک راست کرده و گزینه‌ی *follow* و سپس گزینه‌ی *TCP stream* را انتخاب کنید.)
۹. این جریان حاوی داده‌های کدام پروتکل لایه کاربرد است؟
۱۰. آدرس *IP* و شماره‌ی پورت *client* و *server* را مشخص کنید.
۱۱. شماره‌ی ترتیب (*seq number*) کلاینت از چه عددی شروع می‌شود؟ این اطلاعات را از کدام بسته گرفتید؟
۱۲. شماره‌ی تایید (*ack number*) در اولین بسته‌ی این جریان چند است؟ چرا؟
۱۳. این جریان چگونه خاتمه یافته است؟ بسته‌هایی را که برای خاتمه‌ی جریان ارسال شده‌اند مشخص کنید.

1. طبق تصویر پایین، 81.1 درصد برای TCP و 16.5 درصد برای UDP است.



2. طبق تصویر قبل، ICMP و IGMP و همچنین ARP در لایه دیتا لینک موجود هستند.

3. طبق بخش conversation داریم:



می‌توان جریان های TCP را مشاهده کرد و همانطور که مشخص است 1623 تا وجود دارد. حال برای جریان داریم:

tcp.stream eq 399						
No.	Time	Source	Destination	Protocol	Leng	Info
24935	3539.109380	131.202.240.218	192.168.5.122	TCP	74	35162 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1350 SACK_PERM TSval=89943061 TSecr=0 WS=1024
24936	3539.109728	192.168.5.122	131.202.240.218	TCP	74	80 → 35162 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=28793550 TSecr=89943061 WS=128
24937	3539.116230	131.202.240.218	192.168.5.122	TCP	66	35162 → 80 [ACK] Seq=1 Ack=1 Win=6144 Len=0 TSval=89943063 TSecr=28793550
24938	3539.116934	131.202.240.218	192.168.5.122	HTTP	182	GET / HTTP/1.1
24939	3539.117300	192.168.5.122	131.202.240.218	TCP	66	80 → 35162 [ACK] Seq=1 Ack=117 Win=5888 Len=0 TSval=28793551 TSecr=89943063
24940	3539.118288	192.168.5.122	131.202.240.218	HTTP	836	HTTP/1.1 200 OK (text/html)
24941	3539.118294	192.168.5.122	131.202.240.218	TCP	66	80 → 35162 [FIN, ACK] Seq=771 Ack=117 Win=5888 Len=0 TSval=28793551 TSecr=89943063
24942	3539.138667	131.202.240.218	192.168.5.122	TCP	66	35162 → 80 [ACK] Seq=117 Ack=771 Win=8192 Len=0 TSval=89943068 TSecr=28793551
24943	3539.139665	131.202.240.218	192.168.5.122	TCP	66	35162 → 80 [FIN, ACK] Seq=117 Ack=772 Win=8192 Len=0 TSval=89943068 TSecr=28793551
24944	3539.140006	192.168.5.122	131.202.240.218	TCP	66	80 → 35162 [ACK] Seq=772 Ack=118 Win=5888 Len=0 TSval=28793553 TSecr=89943068

tcp.stream eq 1417						
No.	Time	Source	Destination	Protocol	Leng	Info
89476	12240.722476	131.202.240.218	192.168.5.122	TCP	74	46388 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1350 SACK_PERM TSval=92118593 TSecr=0 WS=1024
89477	12240.722842	192.168.5.122	131.202.240.218	TCP	74	80 → 46388 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=29663892 TSecr=92118593 WS=128
89478	12240.729089	131.202.240.218	192.168.5.122	TCP	66	46388 → 80 [ACK] Seq=1 Ack=1 Win=6144 Len=0 TSval=92118595 TSecr=29663892
89479	12240.729819	131.202.240.218	192.168.5.122	HTTP	182	GET / HTTP/1.1
89480	12240.730161	192.168.5.122	131.202.240.218	TCP	66	80 → 46388 [ACK] Seq=1 Ack=117 Win=5888 Len=0 TSval=29663893 TSecr=92118595
89481	12240.731154	192.168.5.122	131.202.240.218	HTTP	836	HTTP/1.1 200 OK (text/html)
89482	12240.731160	192.168.5.122	131.202.240.218	TCP	66	80 → 46388 [FIN, ACK] Seq=771 Ack=117 Win=5888 Len=0 TSval=29663893 TSecr=92118595
89483	12240.750796	131.202.240.218	192.168.5.122	TCP	66	46388 → 80 [ACK] Seq=117 Ack=771 Win=8192 Len=0 TSval=92118600 TSecr=29663893
89484	12240.752265	131.202.240.218	192.168.5.122	TCP	66	46388 → 80 [FIN, ACK] Seq=117 Ack=772 Win=8192 Len=0 TSval=92118600 TSecr=29663893
89485	12240.752625	192.168.5.122	131.202.240.218	TCP	66	80 → 46388 [ACK] Seq=772 Ack=118 Win=5888 Len=0 TSval=29663895 TSecr=92118600

2 تا از جریان‌ها را برای مثال مشاهده می‌کنید. این جریان‌ها با بسته‌هایی که بیت SYN شان 1 است و همچنین Acknowledge برای آن‌ها شروع شده و با بسته‌هایی که بیت FIN آن‌ها 1 است و همچنین Acknowledge برای آن‌ها به پایان می‌رسد. تصویر کل کامپیوتر:

Frame 89476: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
Ethernet II, Src: 3Com\_72:ab:55 (00:01:02:72:ab:55), Dst: AlcatelLucen\_87:fd:94 (00:e0:b1:87:fd:94)  
Internet Protocol Version 4, Src: 131.202.240.218, Dst: 192.168.5.122  
Transmission Control Protocol, Src Port: 46388, Dst Port: 80, Seq: 0, Len: 0

4. همانطور که مشخص است با استفاده از فیلتر مشخص شده، 1625 بسته داریم.

Wireshark interface showing a packet capture for CN\_THW2.pcap. The filter bar displays the filter: `(tcp.flags.ack == False) && (tcp.flags.syn == True)`. The packet list shows multiple TCP SYN packets. The packet details pane shows the selected packet (Frame 32) with details: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Frame 32: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Ethernet II, Src: IBM\_b9:a7:ed (00:11:25:b9:a7:ed), Dst: IBM\_e9:d0:88 (00:09:6b:e9:d0:88)

Internet Protocol Version 4, Src: 192.168.2.106, Dst: 192.168.2.113

Transmission Control Protocol, Src Port: 3709, Dst Port: 139, Seq: 0, Len: 0

0000 00 09 6b e9 d0 88 00 11 25 b9 a7 ed 08 00 45 00 ..k.....%....E.  
0010 00 30 34 d8 40 00 00 06 3f c4 c0 a8 02 6a c0 a8 .04.@...?....j..  
0020 02 71 0e 7d 00 8b 24 cc ab 11 00 00 00 00 70 02 .q.)-\$. ....p..  
0030 40 00 de 0d 00 00 02 04 05 b4 01 01 04 02 @.....

## 5. طبق تصویر زیر 2194 بسته داریم.

Wireshark packet capture interface showing a list of network packets. The filter applied is `(tcp.flags.ack == True) && (tcp.flags.syn == True)`. The packet list shows various TCP connections, including a retransmission (packet 3599). The packet details pane for packet 3599 shows the Transmission Control Protocol fields: Src Port: 139, Dst Port: 3709, Seq: 0, Ack: 1, Len: 0. A red arrow points to the status bar indicating 2194 packets displayed (2.2% of 100000 total).

دلیل اختلاف مقادیر می‌تواند **Retransmissions** و **Unsuccessful handshakes** باشد. هنگامی که بسته‌ها گم بشود و یا به هر دلیلی مانند **network error** یا دلایل اشاره شده، مجبور شویم دوباره بسته را ارسال نماییم. به همین دلیل این 2 مقدار اختلاف دارند.

## 6. 4440 بسته داریم.

Wireshark packet capture analysis showing a TCP retransmission. The filter is `(tcp.flags.ack == True) && (tcp.flags.fin == True)`. Packet 4741 is highlighted, showing a TCP Retransmission of a FIN packet. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4080	442.733744	192.168.4.120	161.58.8.140	TCP	60	4016 → 80 [FIN, ACK] Seq=41 Ack=30983 Win=17199 Len=0
4083	442.734374	192.168.4.120	69.25.47.62	TCP	60	4022 → 80 [FIN, ACK] Seq=66 Ack=12413 Win=17520 Len=0
4086	442.734931	192.168.4.120	72.32.209.190	TCP	60	4018 → 80 [FIN, ACK] Seq=72 Ack=10689 Win=17053 Len=0
4088	442.737522	192.168.4.120	72.32.209.190	TCP	60	4019 → 80 [FIN, ACK] Seq=107 Ack=15554 Win=17520 Len=0
4141	442.840195	64.94.107.13	192.168.4.120	HTTP	528	HTTP/1.1 200 OK (GIF89a)
4146	442.841534	192.168.4.120	64.94.107.13	TCP	60	4025 → 80 [FIN, ACK] Seq=67 Ack=476 Win=17046 Len=0
4292	443.154053	69.25.47.62	192.168.4.120	HTTP	764	HTTP/1.1 200 OK (text/html)
4360	443.284929	208.122.28.21	192.168.4.120	TCP	60	80 → 4011 [FIN, ACK] Seq=5208 Ack=134 Win=6432 Len=0
4537	443.706920	161.58.8.140	192.168.4.120	HTTP	704	HTTP/1.1 200 OK (text/html)
4562	443.774806	208.122.28.27	192.168.4.120	TCP	60	80 → 4015 [FIN, ACK] Seq=1327 Ack=90 Win=5840 Len=0
4564	443.788787	74.50.3.200	192.168.4.120	TCP	60	80 → 3990 [FIN, ACK] Seq=773 Ack=72 Win=5840 Len=0
4641	444.133223	69.25.47.62	192.168.4.120	HTTP	1064	HTTP/1.1 200 OK (text/html)
4651	444.842136	74.63.40.21	192.168.4.120	TCP	60	80 → 4012 [FIN, ACK] Seq=140132 Ack=83 Win=5840 Len=0
4664	445.733251	192.168.4.120	69.25.47.62	TCP	60	4027 → 80 [FIN, ACK] Seq=55 Ack=53542 Win=16510 Len=0
4679	445.772908	72.32.209.190	192.168.4.120	HTTP	1029	HTTP/1.1 200 OK (PNG)
4682	445.773847	192.168.4.120	72.32.209.190	TCP	60	4029 → 80 [FIN, ACK] Seq=66 Ack=5357 Win=16545 Len=0
4684	445.790339	74.50.3.200	192.168.4.120	TCP	60	80 → 4001 [FIN, ACK] Seq=29070 Ack=134 Win=5840 Len=0
4700	445.858207	192.168.4.120	69.25.47.62	TCP	60	4024 → 80 [FIN, ACK] Seq=49 Ack=12362 Win=16810 Len=0
4712	445.865935	192.168.4.120	161.58.8.140	TCP	60	4028 → 80 [FIN, ACK] Seq=66 Ack=24012 Win=17520 Len=0
4740	445.913969	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [FIN, ACK] Seq=78220 Ack=944 Win=5840 Len=0
4741	445.914109	192.168.5.122	192.168.4.120	TCP	60	[TCP Retransmission] 80 → 3999 [FIN, ACK] Seq=78220 Ack=944 Win=5840 Len=0
4754	445.943793	74.63.40.21	192.168.4.120	HTTP	1304	HTTP/1.1 200 OK (text/html)
4760	445.956084	64.94.107.13	192.168.4.120	HTTP	528	HTTP/1.1 200 OK (GIF89a)
4784	446.012970	64.94.107.13	192.168.4.120	HTTP	528	HTTP/1.1 200 OK (GIF89a)
4833	446.129686	69.25.47.62	192.168.4.120	HTTP	756	HTTP/1.1 200 OK (text/html)
4873	446.411972	161.58.8.140	192.168.4.120	HTTP	1275	HTTP/1.1 200 OK (text/html)
4885	447.712621	192.168.4.120	64.94.107.13	TCP	60	4033 → 80 [FIN, ACK] Seq=67 Ack=476 Win=17046 Len=0
4915	447.841037	74.50.3.200	192.168.4.120	TCP	60	80 → 4008 [FIN, ACK] Seq=67664 Ack=63 Win=5840 Len=0
4921	447.858087	192.168.4.120	64.94.107.13	TCP	60	4031 → 80 [FIN, ACK] Seq=67 Ack=476 Win=17046 Len=0
4933	447.858405	192.168.4.120	64.94.107.13	TCP	60	4035 → 80 [FIN, ACK] Seq=67 Ack=476 Win=17046 Len=0

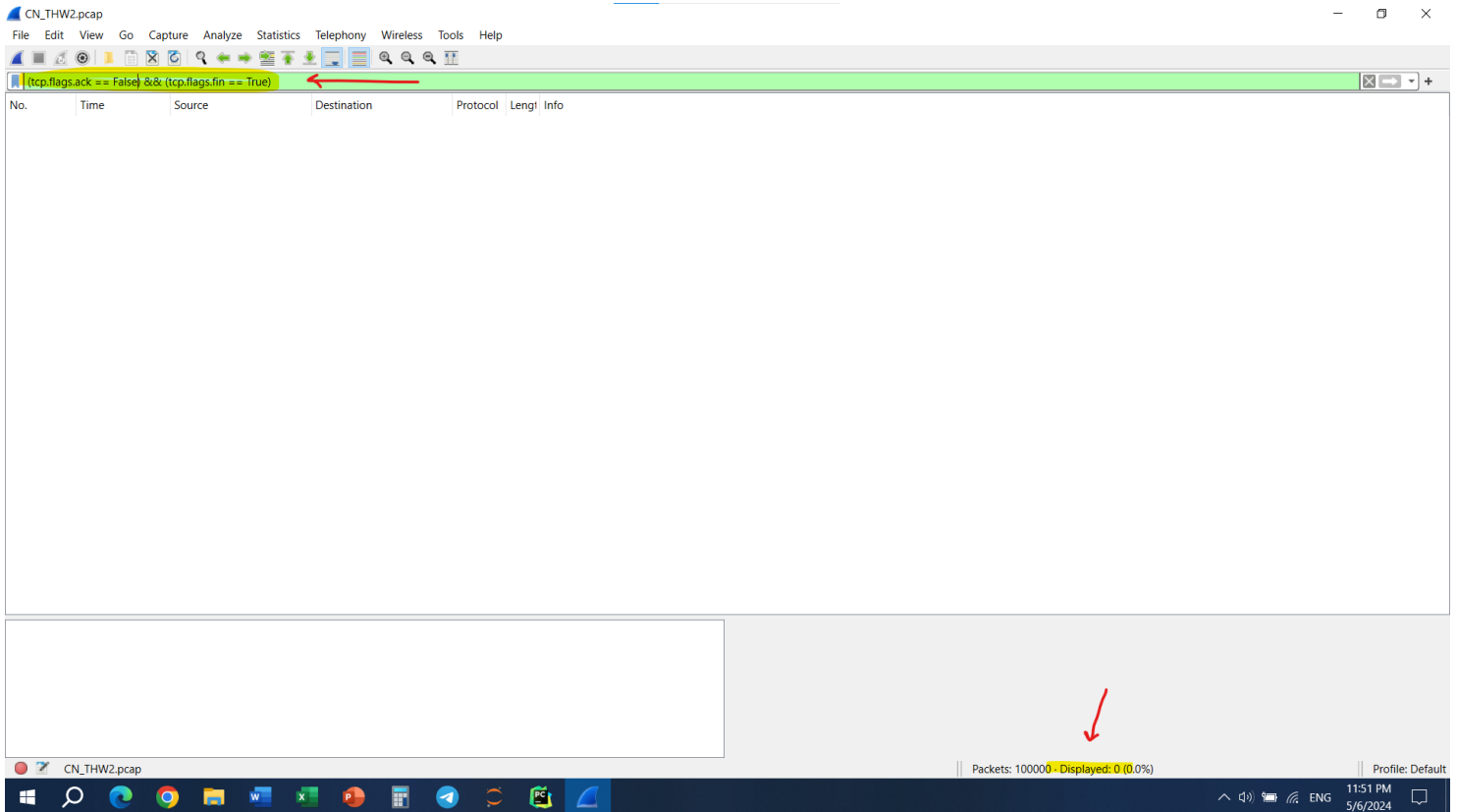
Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: IBM\_bbf1:cf (00:11:25:bb:1f:cf), Dst: AlcatellLucen\_87:f5:94 (00:e0:b1:87:f5:94)  
 Internet Protocol Version 4, Src: 192.168.1.101, Dst: 67.212.184.66  
 Transmission Control Protocol, Src Port: 2159, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Packet 4440 (4.4%) is displayed. Packets: 100000. Profile: Default.

دلیل این اختلاف این است که ممکن است خیلی از ارتباطات طبق روال معمول خاتمه نیابند. یا مانند بخش قبل Retransmissions داشته باشیم. همچنین ریست یا ریدایرکت شدن هم تاثیرگذار است. در ارتباطات موازی نیز می‌توانیم چند بسته FIN داشته باشیم.



## 7. طبق تصویر 0 بسته داریم.



طبیعی است زیرا هر FIN اساساً بسته دریافتی قبلی خود را ACK می کند. بسته های FIN در انتهای ارتباط فرستاده می شوند و یک Host معمولاً برای پایان ارتباط بسته قبلی را ACK کرده و سیگنال FIN را می فرستد و تمام موارد بسته های FIN در این فایل به این شکل هستند.

8. یک روش تقریبی مناسب، شمردن تعداد پکت‌های SYN است. به ازای هر کانکشن یک پکت با SYN فرستاده می‌شود و می‌توان با استفاده از آن‌ها به تعداد مورد نظر رسید. راه دیگر min گرفتن از پاسخ‌های بخش 4 تا 7 است که معمولاً به همان تعداد SYN خواهیم رسید.

9. همانطور که در تصویر مشاهده می‌کنید، HTTP می‌باشد.

The image shows a Wireshark packet capture analysis. The left pane displays a list of packets, with packet 53 selected. The middle pane shows the details of packet 53, which is an HTTP GET request. The right pane shows the raw data of the packet in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination
2851	438.770372	192.168.5.122	192.168.4.120
2853	438.770967	192.168.5.122	192.168.4.120
2854	438.771602	192.168.5.122	192.168.4.120
2855	438.771640	192.168.5.122	192.168.4.120
2856	438.771643	192.168.4.120	192.168.5.122
2857	438.772834	192.168.5.122	192.168.4.120
2860	438.774072	192.168.4.120	192.168.5.122
2862	438.775516	192.168.5.122	192.168.4.120
2867	438.776745	192.168.5.122	192.168.4.120
2868	438.777452	192.168.5.122	192.168.4.120
2869	438.778044	192.168.4.120	192.168.5.122
2871	438.778800	192.168.4.120	192.168.5.122
3550	440.909432	192.168.4.120	192.168.5.122
3552	440.909793	192.168.5.122	192.168.4.120
3553	440.909959	192.168.5.122	192.168.4.120
3555	440.910714	192.168.5.122	192.168.4.120
3556	440.912241	192.168.5.122	192.168.4.120
3671	441.115843	192.168.5.122	192.168.4.120
3672	441.117368	192.168.5.122	192.168.4.120
3673	441.118200	192.168.4.120	192.168.5.122
4740	445.913969	192.168.5.122	192.168.4.120
4741	445.914109	192.168.5.122	192.168.4.120
4742	445.914311	192.168.4.120	192.168.5.122
5013	449.423500	192.168.4.120	192.168.5.122
5014	449.423506	192.168.4.120	192.168.5.122
5016	449.423828	192.168.5.122	192.168.4.120
5017	449.423984	192.168.5.122	192.168.4.120
5018	449.424026	192.168.5.122	192.168.4.120
5019	449.424225	192.168.5.122	192.168.4.120

**Packet 53 Details:**

- Frame 5016:** 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II:** Src: Dell\_20:7b:d3 (00:22:19:20:7b:d3), Dst: 3Com\_72:ab:55 (00:01:02:72:ab:55)
- Internet Protocol Version 4:** Src: 192.168.5.122, Dst: 192.168.4.120
- Transmission Control Protocol:** Src Port: 80, Dst Port: 3999, Seq: 78221, Len: 0
- Hypertext Transfer Protocol:** GET /joomla/index.php/joomla-license HTTP/1.1

**Raw Data:**

```

0000  00 01 02 72 ab 55 00 22 19 20 7b d3 00 00 00 00
0010  00 28 00 00 40 00 40 06 af 8d c0 00 00 00 00
0020  04 78 00 50 0f 9f ae ba d3 62 00 00 00 00 00
0030  00 00 92 91 00 00 00 00 00 00 00 00 00 00 00
  
```

5013	449.423500	192.168.4.120	192.168.5.122	HTTP	236	GET /joomla/index.php/component/mailto/?tmpl=component&link=aHR0cDovL
5014	449.423506	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [FIN, ACK] Seq=1126 Ack=78221 Win=17520 Len=0
5016	449.423828	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5017	449.423984	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5018	449.424026	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5019	449.424225	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0

> Frame 5016: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
 > Ethernet II, Src: Dell\_20:7b:d3 (00:22:19:20:7b:d3), Dst: 3Com\_72:ab:55 (00:01:02:72:ab:55)  
 > Internet Protocol Version 4, Src: 192.168.5.122, Dst: 192.168.4.120  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 3999, Seq: 78221, Len: 0

```

0000  00 01 02 72 ab 55 00 22 19 20 7b d3 00 00 00 00
0010  00 28 00 00 40 00 40 06 af 8d c0 00 00 00 00
0020  04 78 00 50 0f 9f ae ba d3 62 00 00 00 00 00
0030  00 00 92 91 00 00 00 00 00 00 00 00 00 00 00
  
```

10. طبق تصویر زیر، شماره‌ها مشخص شده‌اند.

5014	449.423506	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [FIN, ACK] Seq=1126 Ack=78221 Win=1
5016	449.423828	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5017	449.423984	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5018	449.424026	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5019	449.424225	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0

Frame 5016: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Dell\_20:7b:d3 (00:22:19:20:7b:d3), Dst: 3Com\_72:ab:55 (00:01:02:72:ab:55)

Internet Protocol Version 4, Src: 192.168.5.122, Dst: 192.168.4.120

Transmission Control Protocol, Src Port: 80, Dst Port: 3999, Seq: 78221, Len: 0

0000 00 01 02 7  
0010 00 28 00 0  
0020 04 78 00 5  
0030 00 00 92 9

کلاینت:

192.168.4.120

3999

سرور:

192.168.5.122

80

11. این مقدار برابر 1009629790 می‌باشد که از بسته SYN اول گرفتیم.

tcpstream eq 53

Time	Source	Destination	Protocol	Length	Info
1838.437.171885	192.168.4.120	192.168.5.122	TCP	62	3999 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1846.437.172467	192.168.5.122	192.168.4.120	TCP	62	80 → 3999 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1851.437.172728	192.168.5.122	192.168.4.120	TCP	62	[TCP Retransmission] 80 → 3999 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1853.437.174037	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
1854.437.174215	192.168.4.120	192.168.5.122	HTTP	150	GET /joomla/index.php/joomla-license HTTP/1.1
1856.437.174710	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [ACK] Seq=1 Ack=97 Win=5840 Len=0
1857.437.174868	192.168.5.122	192.168.4.120	TCP	60	[TCP Dup ACK 1856#1] 80 → 3999 [ACK] Seq=1 Ack=97 Win=5840 Len=0
1942.437.284179	192.168.5.122	192.168.4.120	TCP	1514	80 → 3999 [ACK] Seq=1 Ack=97 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
1943.437.285410	192.168.5.122	192.168.4.120	TCP	1514	80 → 3999 [ACK] Seq=1461 Ack=97 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
1947.437.286662	192.168.5.122	192.168.4.120	TCP	1514	80 → 3999 [ACK] Seq=2921 Ack=97 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
1950.437.287838	192.168.5.122	192.168.4.120	TCP	1514	[TCP Retransmission] 80 → 3999 [ACK] Seq=1 Ack=97 Win=5840 Len=1460
1952.437.289127	192.168.5.122	192.168.4.120	TCP	1514	[TCP Retransmission] 80 → 3999 [ACK] Seq=1461 Ack=97 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
1955.437.290357	192.168.5.122	192.168.4.120	TCP	1514	[TCP Retransmission] 80 → 3999 [ACK] Seq=2921 Ack=97 Win=5840 Len=1460 [TCP segment of a reassembled PDU]
1956.437.290366	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [ACK] Seq=97 Ack=2921 Win=17520 Len=0

Frame 1838: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0  
 Ethernet II, Src: IBM\_bbcf:cf:0f (00:11:25:bb:cf:0f), Dst: Alcatellucen\_87:f5:94 (00:e0:b1:87:f5:94)  
 Internet Protocol Version 4, Src: 192.168.4.120, Dst: 192.168.5.122  
 Transmission Control Protocol, Src Port: 3999, Dst Port: 80, Seq: 0, Len: 0

Source Port: 3999  
 Destination Port: 80  
 [Stream index: 53]  
 [Conversation completeness: Complete, WITH\_DATA (63)]  
 [TCP Segment Len: 0]  
 Sequence Number: 0 (relative sequence number)  
 Sequence Number (raw): 1009629798  
 [Next Sequence Number: 1 (relative sequence number)]  
 Acknowledgment Number: 0  
 Acknowledgment number (raw): 0  
 0111 .... = Header Length: 28 bytes (7)  
 Flags: 0x002 (SYN)  
 Window: 16384  
 [Calculated window size: 16384]  
 Checksum: 0xb161 [Unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted  
 [Timestamps]

0000 00 e0 b1 87 f5 94 00 11 25 bb cf 0f 08 00 45 00 .....%.....E-  
 0010 00 30 71 80 40 00 80 06 fe 04 c0 a8 04 78 c0 a8 0q @.....x..  
 0020 05 7a 0f 9f 00 50 3c 2d ba 5e 00 00 00 70 02 -z...P<-.....p-  
 0030 40 00 b1 61 00 00 02 04 05 b4 01 01 04 02 @..a.....

CN\_THW2.pcap | Packets: 100000 - Displayed: 186 (0.2%) | Profiler: Default

1:54 PM 5/10/2024

12. مطابق تصویر بالا در اولین بسته 0 است زیرا هنوز بسته‌ای نرسیده و در بسته پاسخ آن که از سرور ارسال می‌شود یکی اضافه شده و برابر با 1 و به صورت raw برابر با 1009629791 می‌شود.



## 13. داریم:

Wireshark packet capture showing a TCP RST sequence. The packet list shows a series of RST packets from 192.168.5.122 to 192.168.4.120. The packet details pane shows the selected packet (Frame 1846) with source port 80 and destination port 3999. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
4741	445.914109	192.168.5.122	192.168.4.120	TCP	60	[TCP Retransmission] 80 → 3999 [FIN, ACK] Seq=78220 Ack=944 Win=5840 Len=0
4742	445.914311	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [ACK] Seq=944 Ack=78221 Win=17520 Len=0
5013	449.423500	192.168.4.120	192.168.5.122	HTTP	236	GET /joomla/index.php/component/mailto/?tmpl=component&link=aHR0cDovL3QzbGFiLmVbS9qb29tbGEvaW5kZXgucGhwL3RoZS1uZXZlZytd2UtYX...
5014	449.423506	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [FIN, ACK] Seq=1126 Ack=78221 Win=17520 Len=0
5016	449.423828	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5017	449.423984	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5018	449.424026	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5019	449.424225	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0

Frame 1846: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Ethernet II, Src: Dell\_20:7b:d3 (00:22:19:20:7b:d3), Dst: 3Com\_72:ab:55 (00:01:02:72:ab:55)

Internet Protocol Version 4, Src: 192.168.5.122, Dst: 192.168.4.120

Transmission Control Protocol, Src Port: 80, Dst Port: 3999, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 3999

[Stream index: 53]

[Conversation completeness: Complete, WITH\_DATA (63)]

[TCP Segment Len: 0]

Packets: 100000 · Displayed: 186 (0.2%)

Profile: Default

2:05 PM 5/10/2024

Wireshark packet capture showing a TCP RST sequence. The packet list shows a series of RST packets from 192.168.5.122 to 192.168.4.120. The packet details pane shows the selected packet (Frame 1846) with source port 80 and destination port 3999. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
3556	440.912241	192.168.5.122	192.168.4.120	TCP	909	[TCP Retransmission] 80 → 3999 [PSH, ACK] Seq=77365 Ack=944 Win=5840 Len=855
3671	441.115843	192.168.5.122	192.168.4.120	TCP	909	[TCP Retransmission] 80 → 3999 [PSH, ACK] Seq=77365 Ack=944 Win=5840 Len=855
3672	441.117368	192.168.5.122	192.168.4.120	TCP	909	[TCP Retransmission] 80 → 3999 [PSH, ACK] Seq=77365 Ack=944 Win=5840 Len=855
3673	441.118200	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [ACK] Seq=944 Ack=78220 Win=17520 Len=0
4740	445.913969	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [FIN, ACK] Seq=78220 Ack=944 Win=5840 Len=0
4741	445.914109	192.168.5.122	192.168.4.120	TCP	60	[TCP Retransmission] 80 → 3999 [FIN, ACK] Seq=78220 Ack=944 Win=5840 Len=0
4742	445.914311	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [ACK] Seq=944 Ack=78221 Win=17520 Len=0
5013	449.423500	192.168.4.120	192.168.5.122	HTTP	236	GET /joomla/index.php/component/mailto/?tmpl=component&link=aHR0cDovL3QzbGFiLmVbS9qb29tbGEvaW5kZXgucGhwL3RoZS1uZXZlZytd2UtYX...
5014	449.423506	192.168.4.120	192.168.5.122	TCP	60	3999 → 80 [FIN, ACK] Seq=1126 Ack=78221 Win=17520 Len=0
5016	449.423828	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5017	449.423984	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5018	449.424026	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0
5019	449.424225	192.168.5.122	192.168.4.120	TCP	60	80 → 3999 [RST] Seq=78221 Win=0 Len=0

Frame 1846: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)

Ethernet II, Src: Dell\_20:7b:d3 (00:22:19:20:7b:d3), Dst: 3Com\_72:ab:55 (00:01:02:72:ab:55)

Internet Protocol Version 4, Src: 192.168.5.122, Dst: 192.168.4.120

Transmission Control Protocol, Src Port: 80, Dst Port: 3999, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 3999

[Stream index: 53]

[Conversation completeness: Complete, WITH\_DATA (63)]

[TCP Segment Len: 0]

Packets: 100000 · Displayed: 186 (0.2%)

Profile: Default

2:06 PM 5/10/2024

تصویر واضح تر:

192.168.4.120	TCP	909 [TCP Retransmission] 80 → 3999 [PSH, ACK] S
192.168.4.120	TCP	909 [TCP Retransmission] 80 → 3999 [PSH, ACK] S
192.168.4.120	TCP	909 [TCP Retransmission] 80 → 3999 [PSH, ACK] S
192.168.5.122	TCP	60 3999 → 80 [ACK] Seq=944 Ack=78220 Win=17520
192.168.4.120	TCP	60 80 → 3999 [FIN, ACK] Seq=78220 Ack=944 Win=
192.168.4.120	TCP	60 [TCP Retransmission] 80 → 3999 [FIN, ACK] S
192.168.5.122	TCP	60 3999 → 80 [ACK] Seq=944 Ack=78221 Win=17520
192.168.5.122	HTTP	236 GET /joomla/index.php/component/mailto/?tmp
192.168.5.122	TCP	60 3999 → 80 [FIN, ACK] Seq=1126 Ack=78221 Win
192.168.4.120	TCP	60 80 → 3999 [RST] Seq=78221 Win=0 Len=0
192.168.4.120	TCP	60 80 → 3999 [RST] Seq=78221 Win=0 Len=0
192.168.4.120	TCP	60 80 → 3999 [RST] Seq=78221 Win=0 Len=0
192.168.4.120	TCP	60 80 → 3999 [RST] Seq=78221 Win=0 Len=0

52 bytes captured (496 bits)

0000 00 01 02

آخرین بسته‌ها مربوط به FIN ACK و RST یا همان ریست هستند. سرور ابتدا سیگنال خاتمه را داده و سپس کلاینت ack کرده و بسته و fin خود را فرستاده و به ارتباط پایان می‌دهد. سپس 4 بسته reset وجود دارد که هنگامی که خاتمه ارتباط با مشکل مواجه می‌شود ارسال می‌شوند.