Computer Network

AmirReza Azari
99101087

ادامه تمرین دوم

وایرشارک

۱. پروتکل لایه‌ی 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 لایه‌ی انتقال بررسی کنیم. منظور از یک جریان *TCP* همه‌ی بسته‌هایی است که اولا حاوی قطعات *TCP* هستند و ثانیا 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 لایه‌ی کاربرد است؟

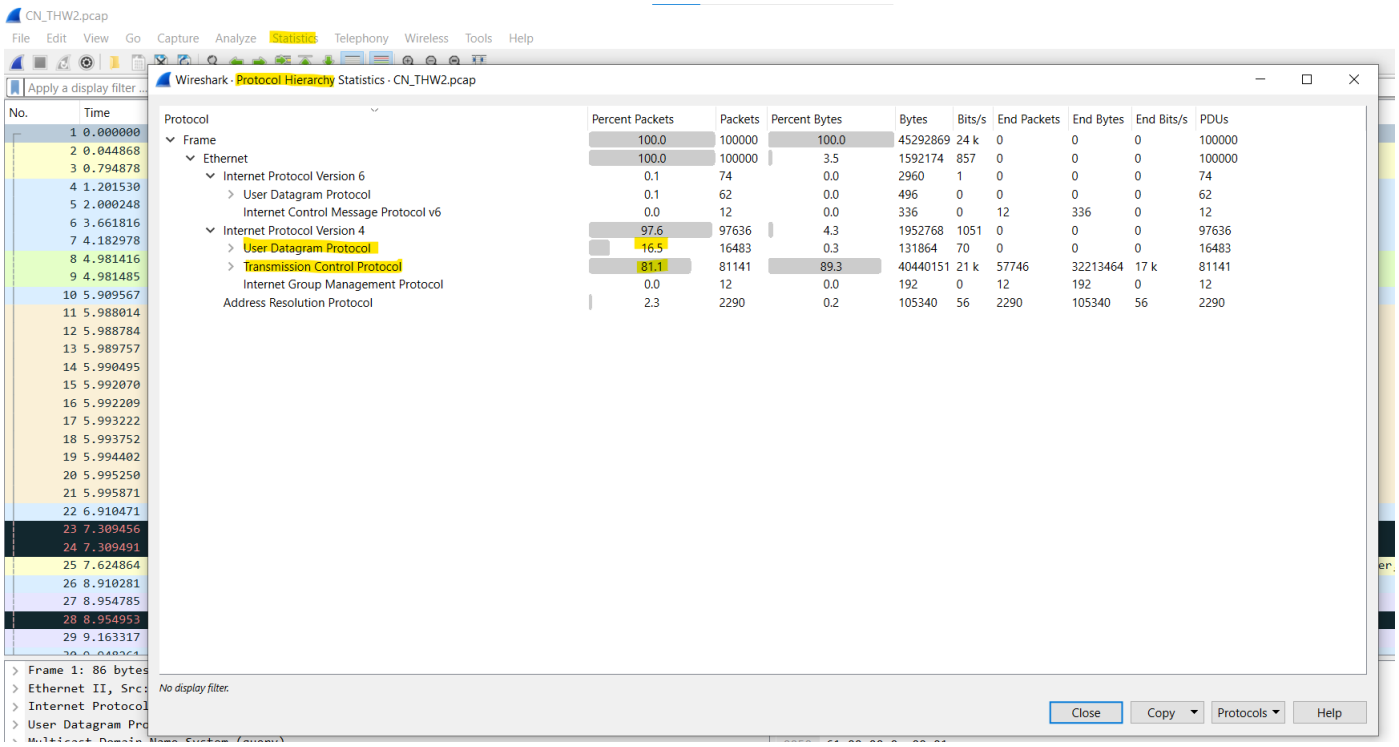
۱۰. آدرس *IP* و شماره‌ی پورت *client* و *server* را مشخص کنید.

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؟

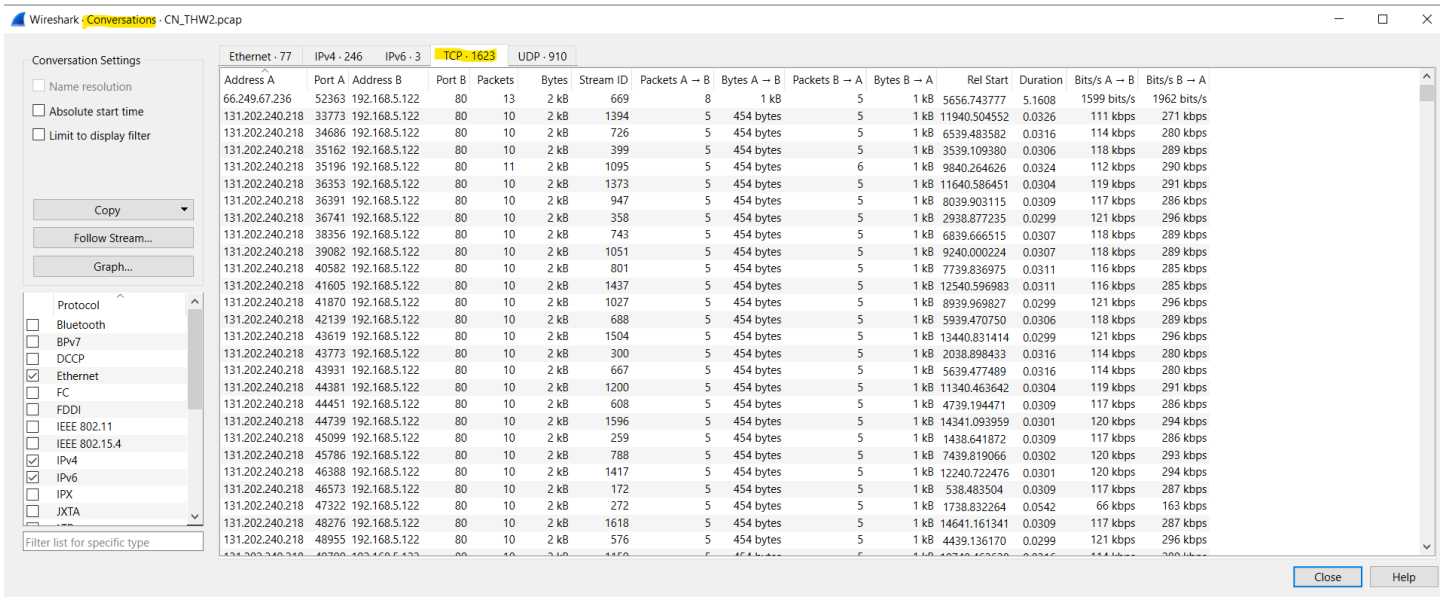
۱۳. این جریان چطور خاتمه یافته است؟ بسته‌هایی را که برای خاتمه‌ی جریان ارسال شده‌اند مشخص کنید.

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:

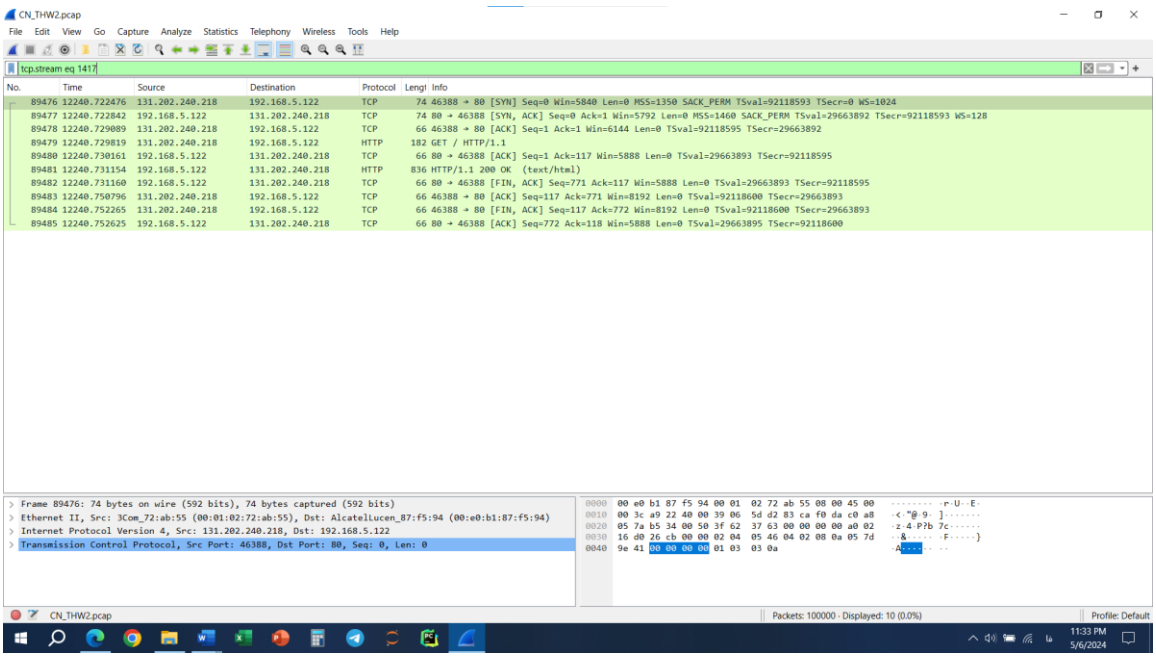
tcp.stream eq 399

No.	Time	Source	Destination	Protocol	Lengt	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

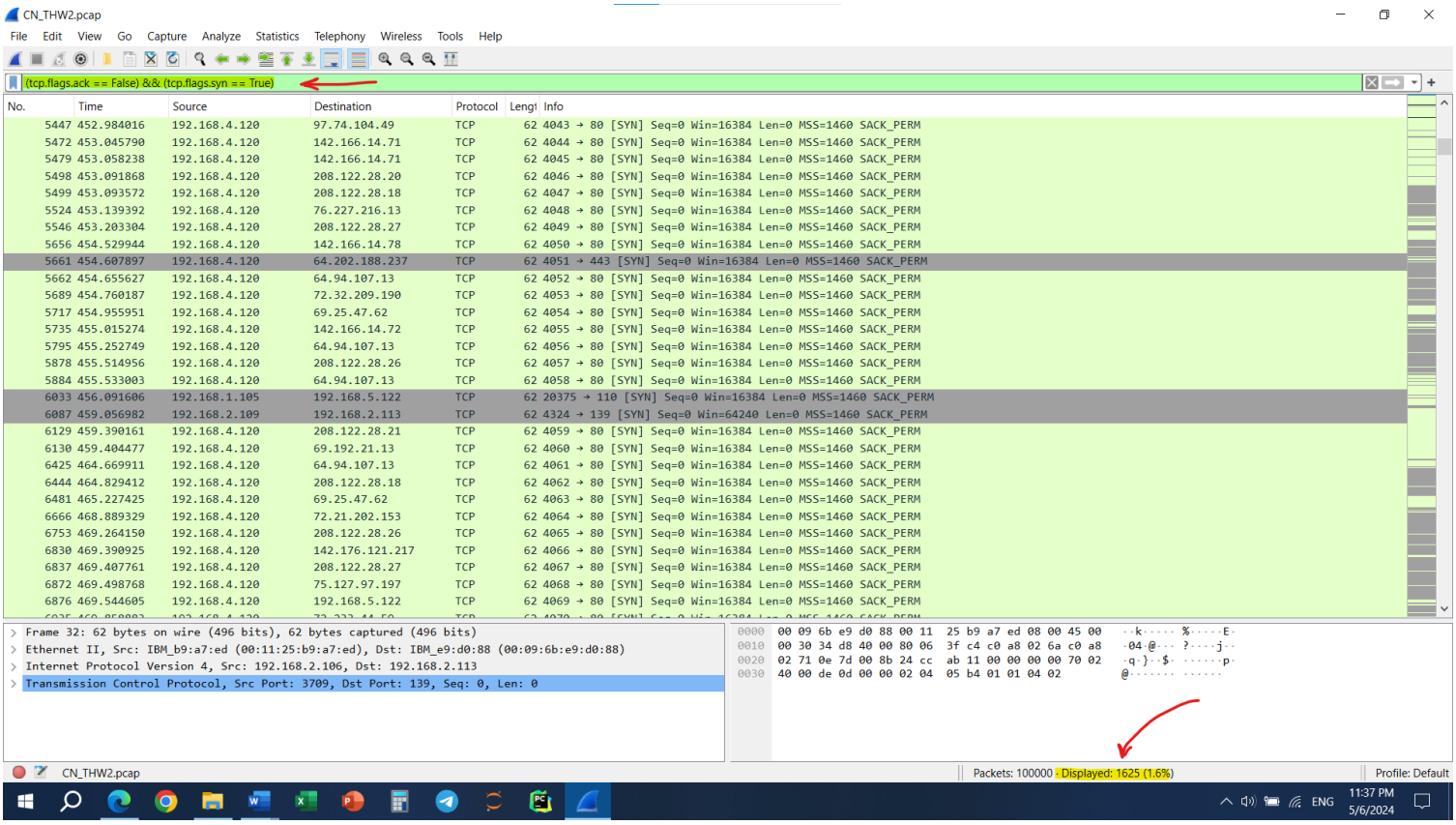
tcp.stream eq 1417

No.	Time	Source	Destination	Protocol	Lengt	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=
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

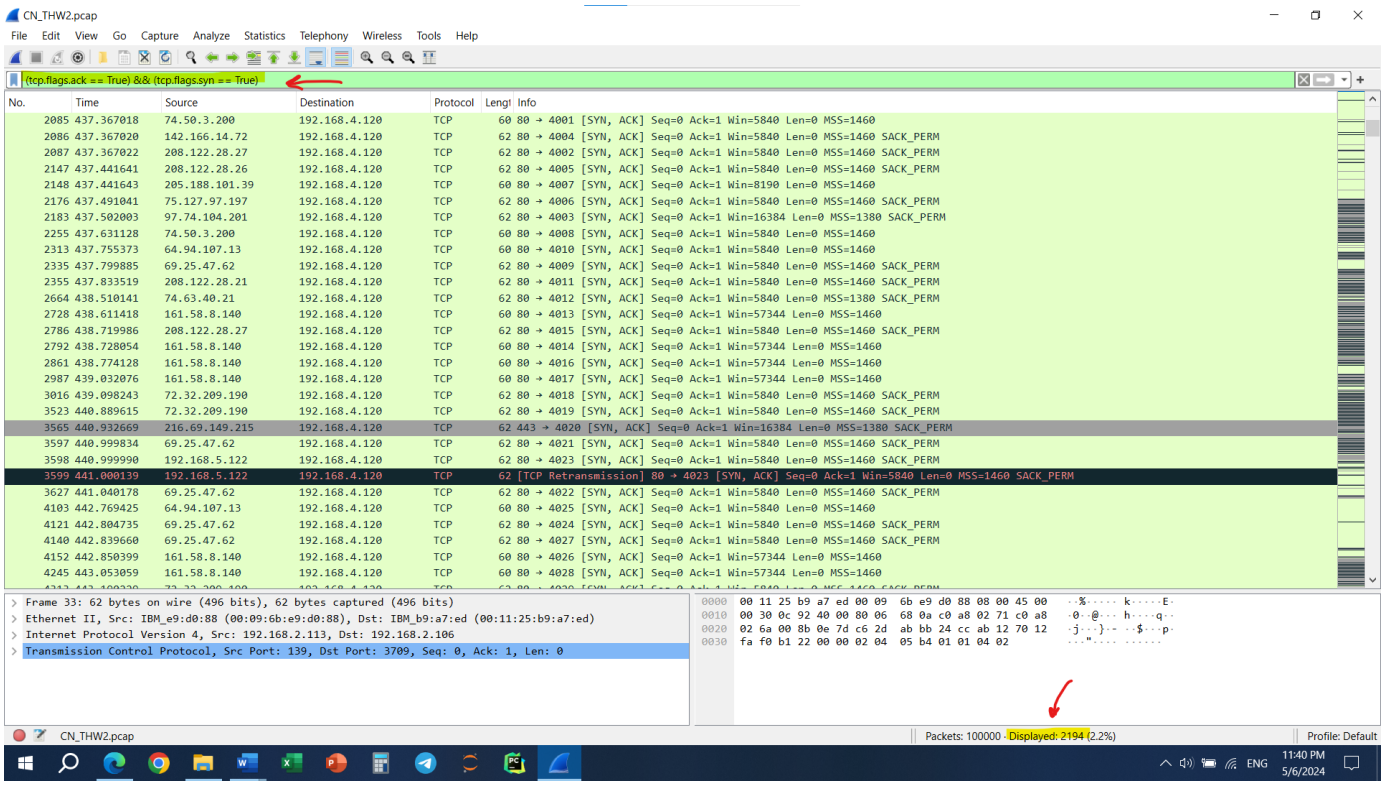
2تا از جریان‌ها را برای مثال مشاهده می‌کنید. این جریان ها با بسته هایی که بیتSYN شان 1 است و همچنین Acknowledge برای آن‌ها شروع شده و با بسته هایی که بیت FIN آن ها 1 است و همچنین Acknowledge برای آن‌ها به پایان می‌رسد. تصویر کل کامپیوتر:



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



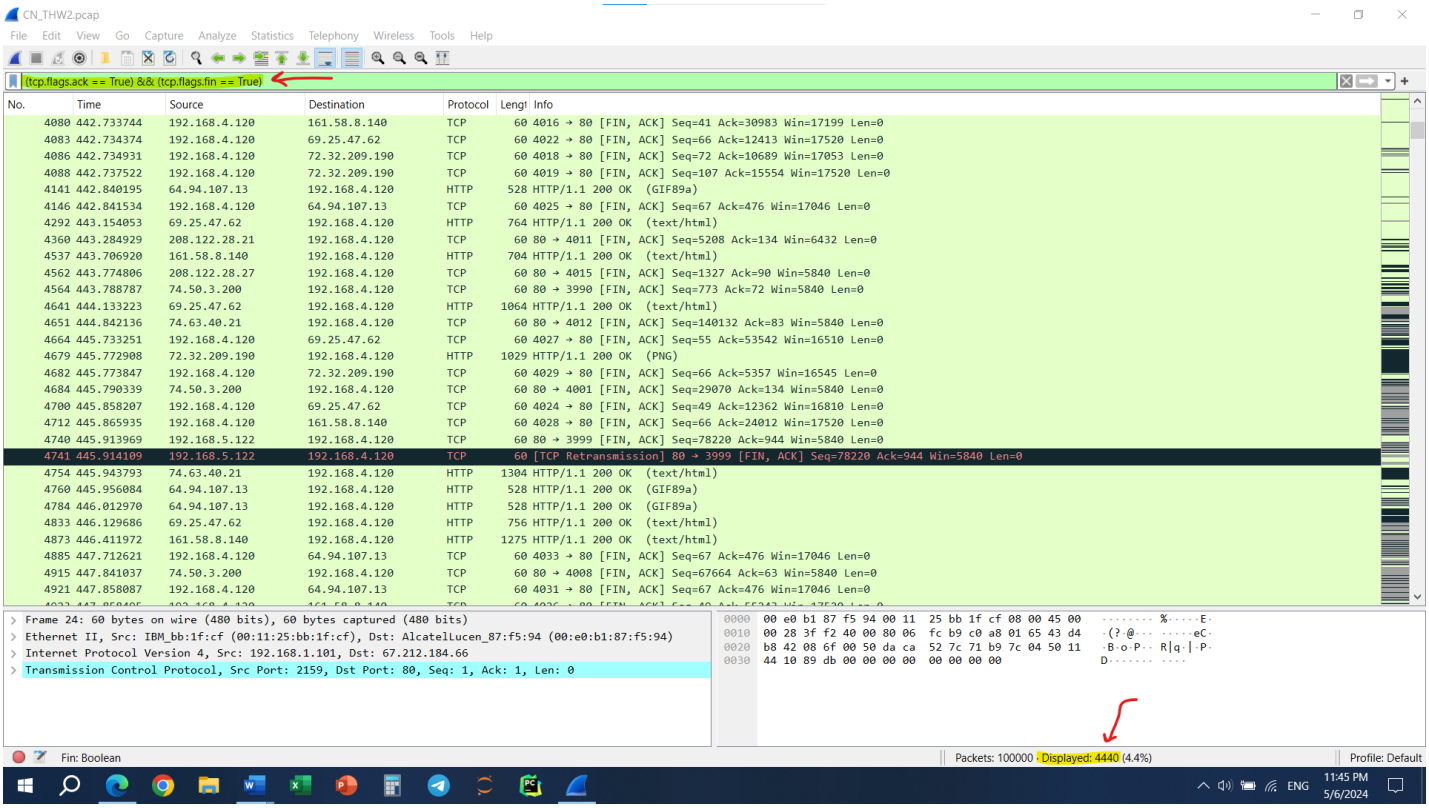
5. طبق تصویر زیر 2194 بسته داریم.



دلیل اختلاف مقادیر می‌تواند Unsuccessful handshakes و Retransmissions باشد.

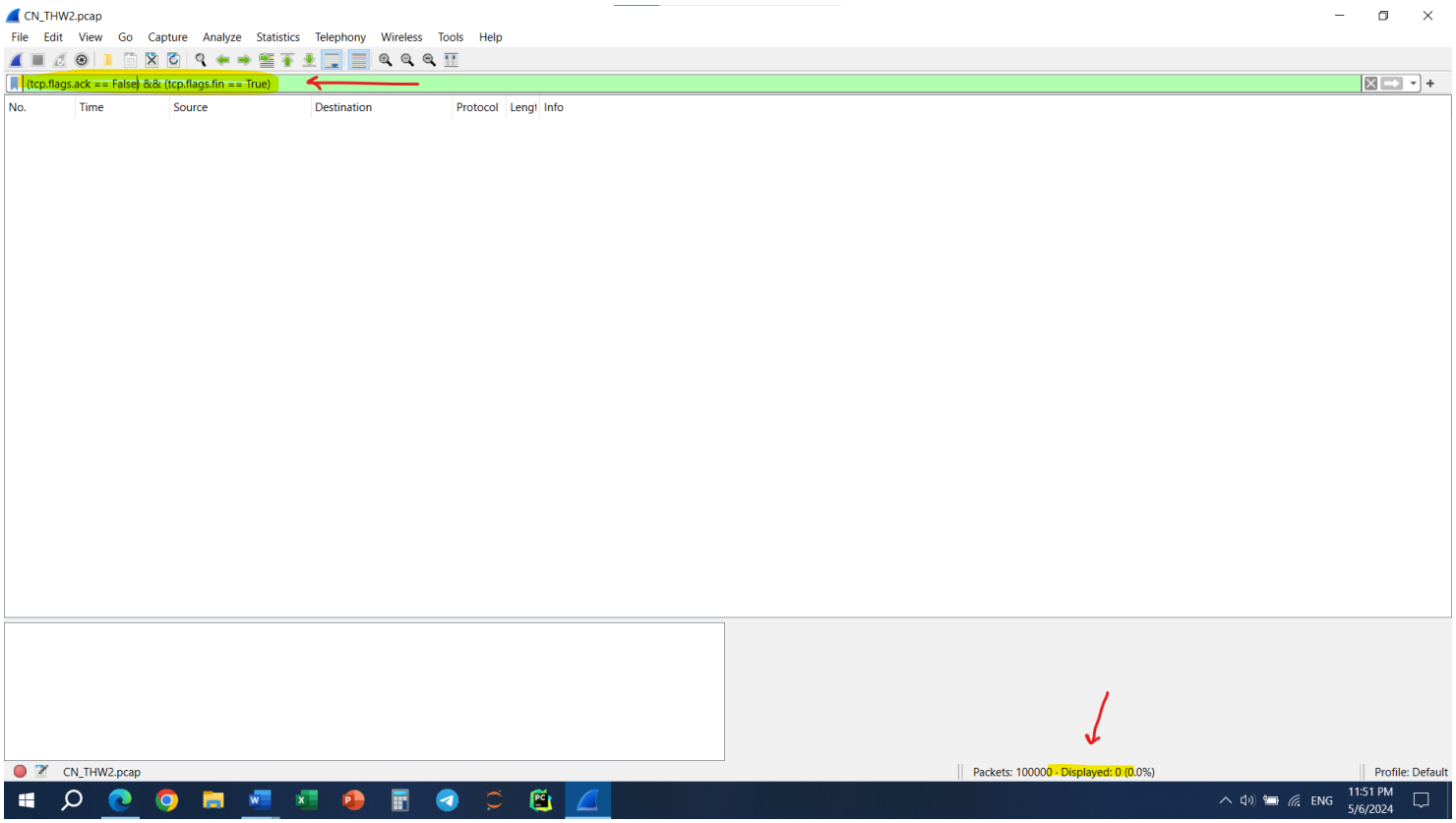
هنگامی که بسته‌ها گم بشود و یا به هر دلیلی مانند network error یا دلایل اشاره شده، مجبور شویم دوباره بسته را ارسال نماییم. به همین دلیل این 2 مقدار اختلاف دارند.

6. 4440 بسته داریم.



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.

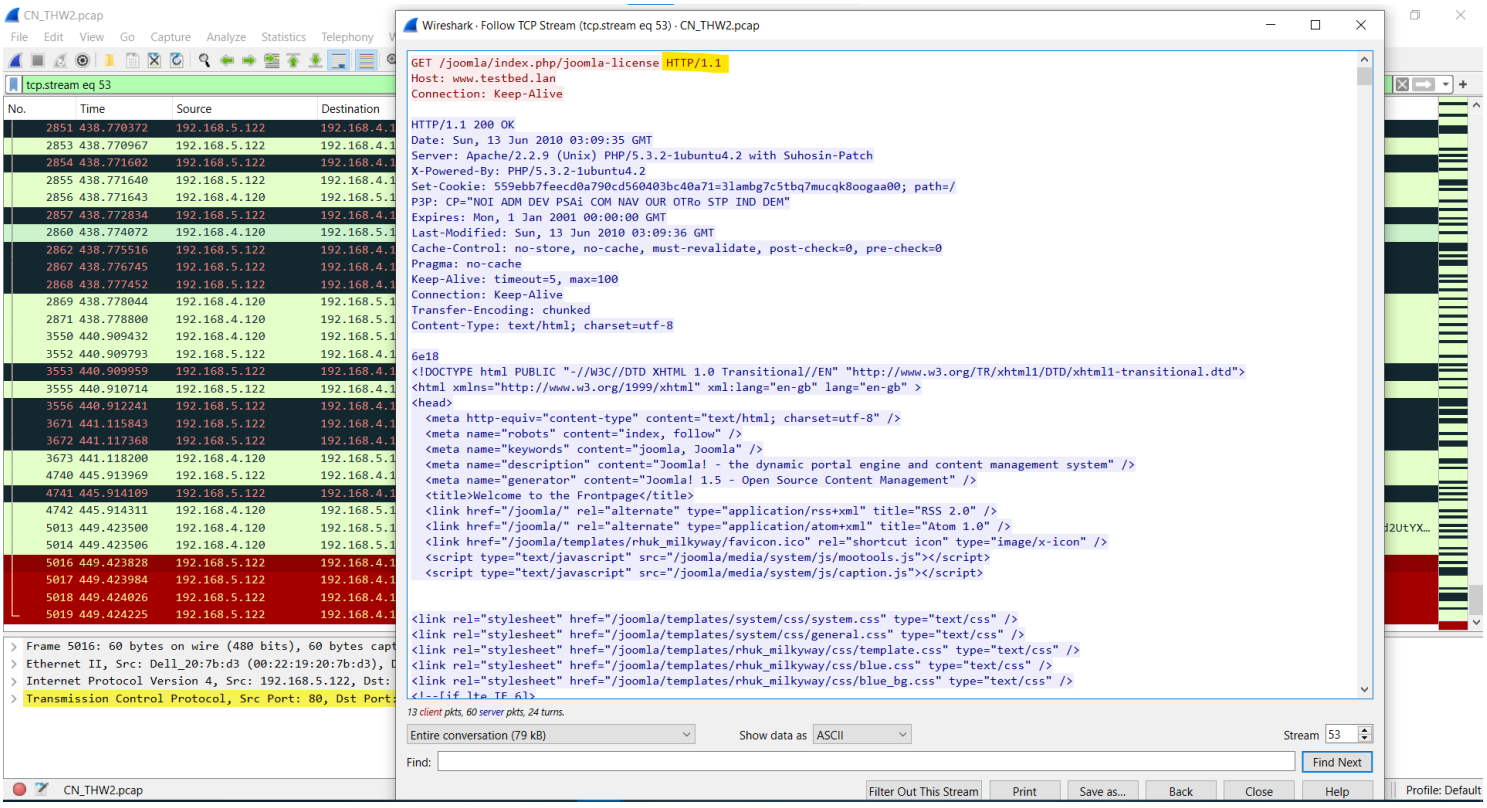
7. طبق تصویر 0 بسته داریم.

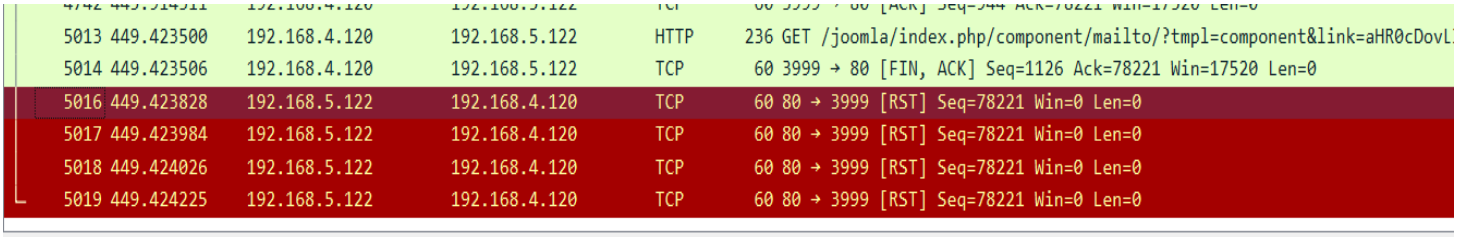


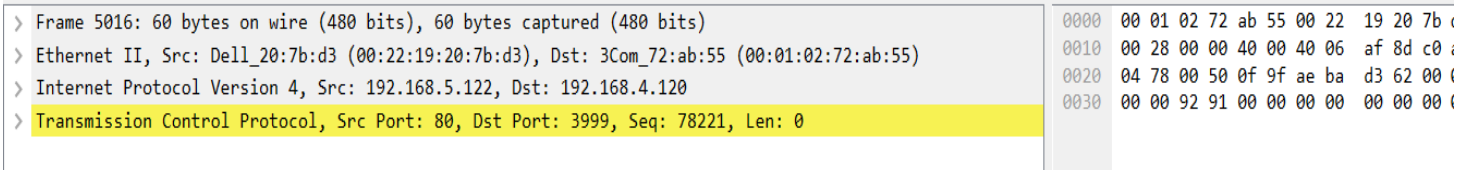
طبیعی است زیرا هر FIN اساساً بسته دریافتی قبلی خود را ACK می کند. بسته های FIN در انتهای ارتباط فرستاده می‌شوند و یک Host معمولا برای پایان ارتباط بسته قبلی را ACK کرده و سیگنال FIN را می‌فرستد و تمام موارد بسته های FIN در این فایل به این شکل هستند.

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

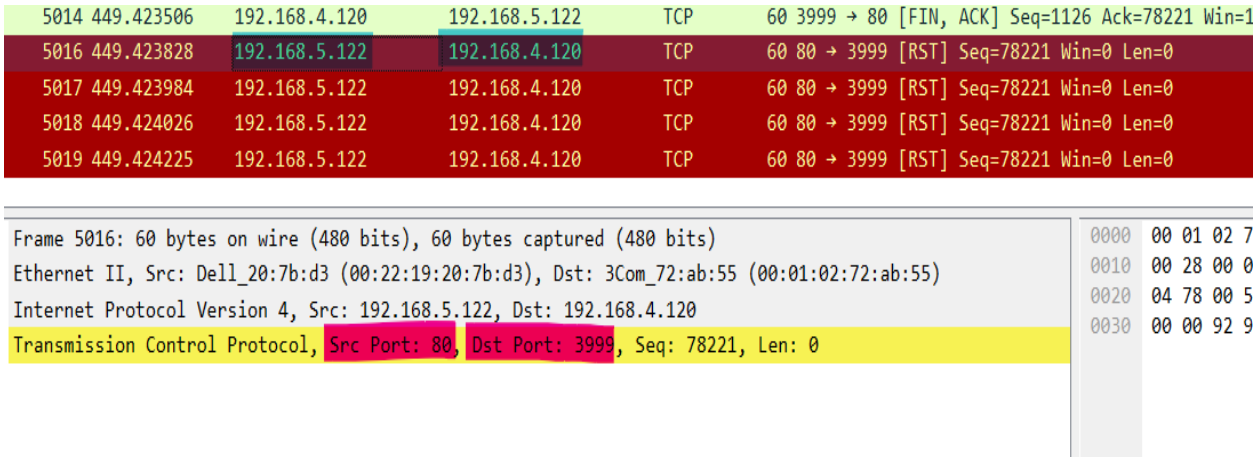
9. همانطور که در تصویر مشاهده می‌کنید، HTTP می‌باشد.







10. طبق تصویر زیر، شماره‌ها مشخص شده‌اند.



کلاینت:

192.168.4.120

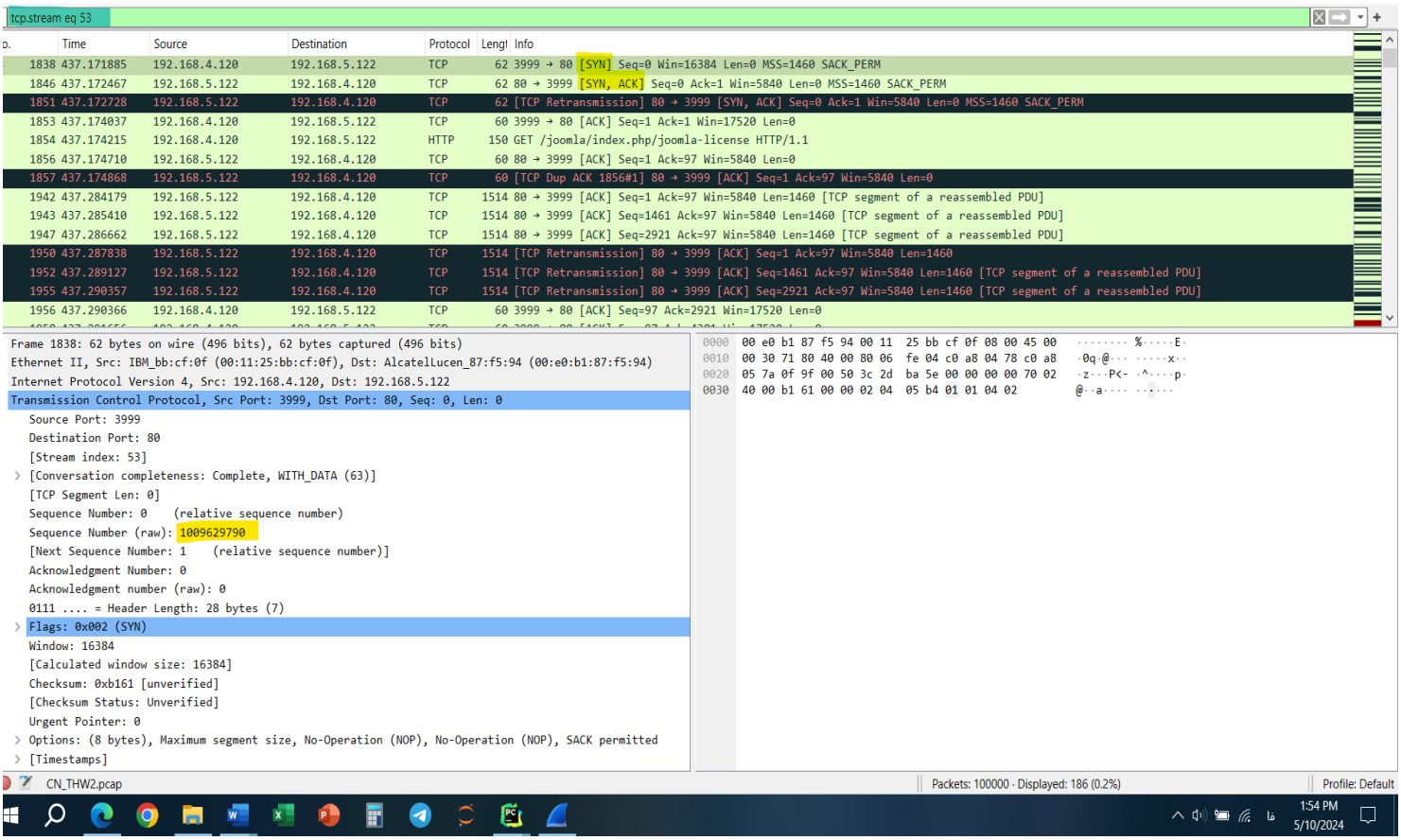
3999

سرور:

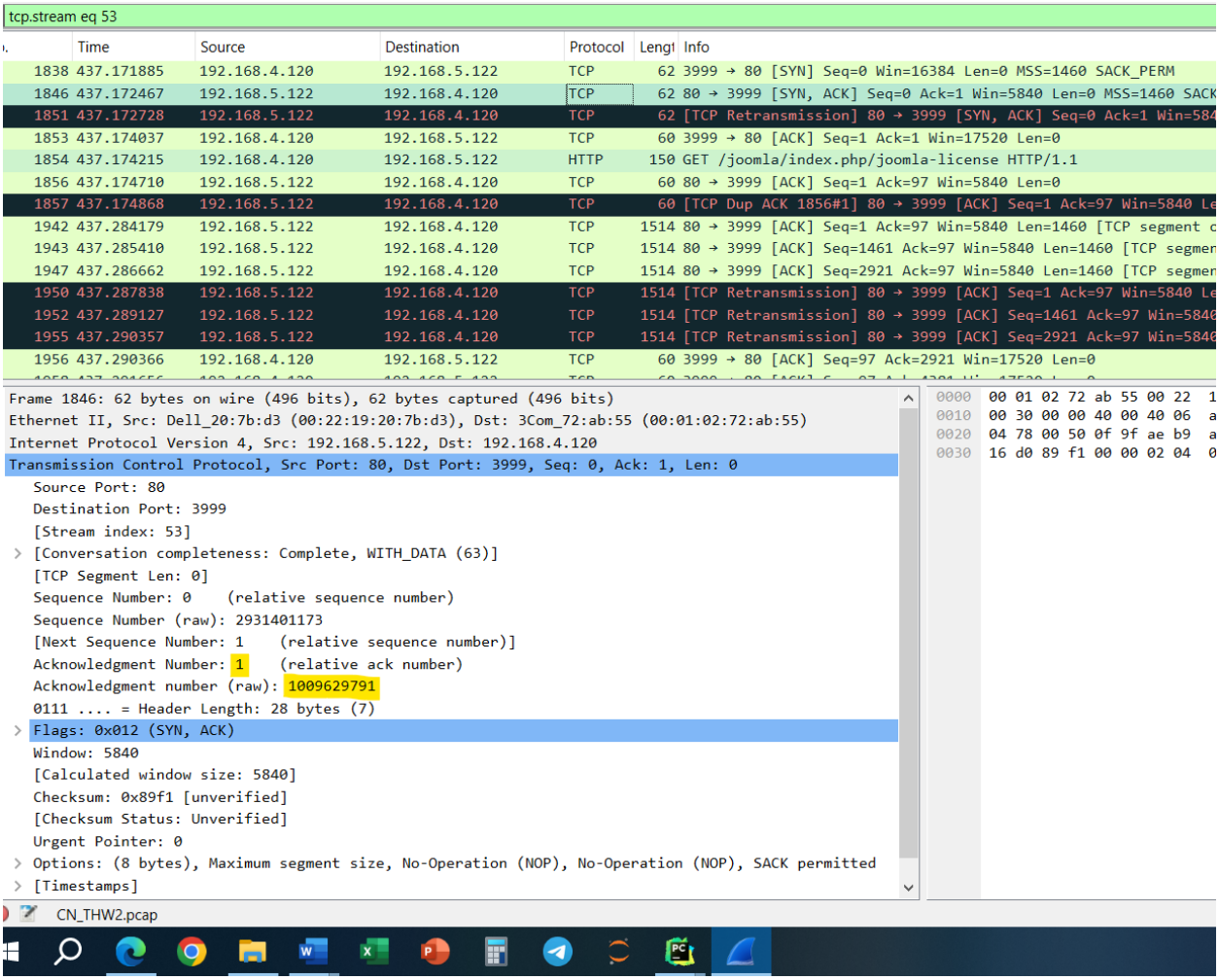
192.168.5.122

80

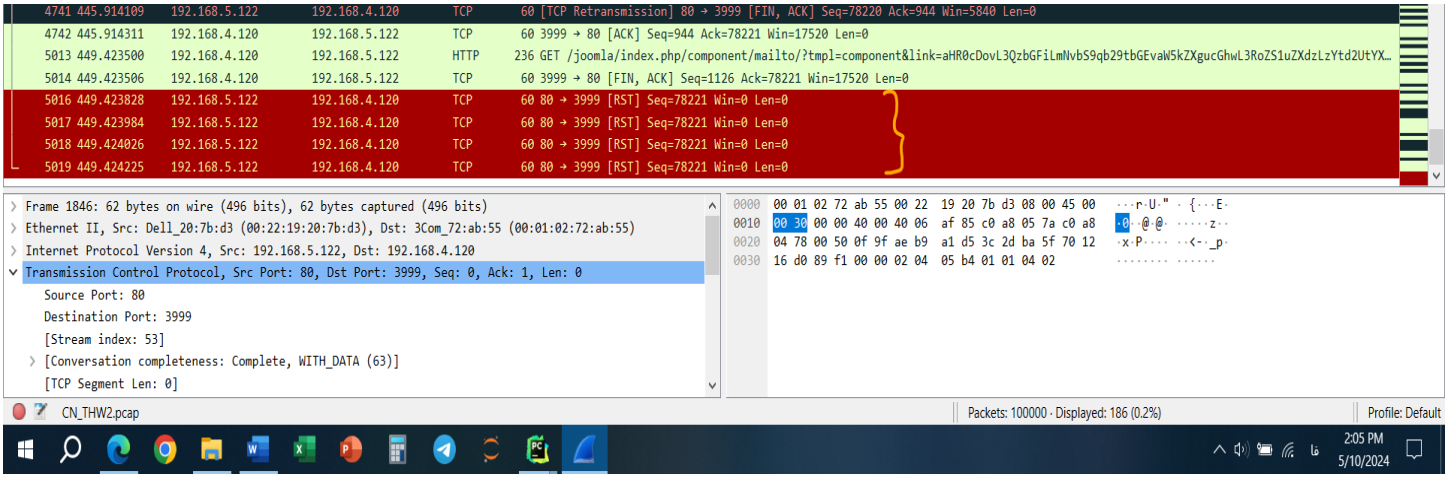
11. این مقدار برابر 1009629790 می‌باشد که از بسته SYN اول گرفتیم.

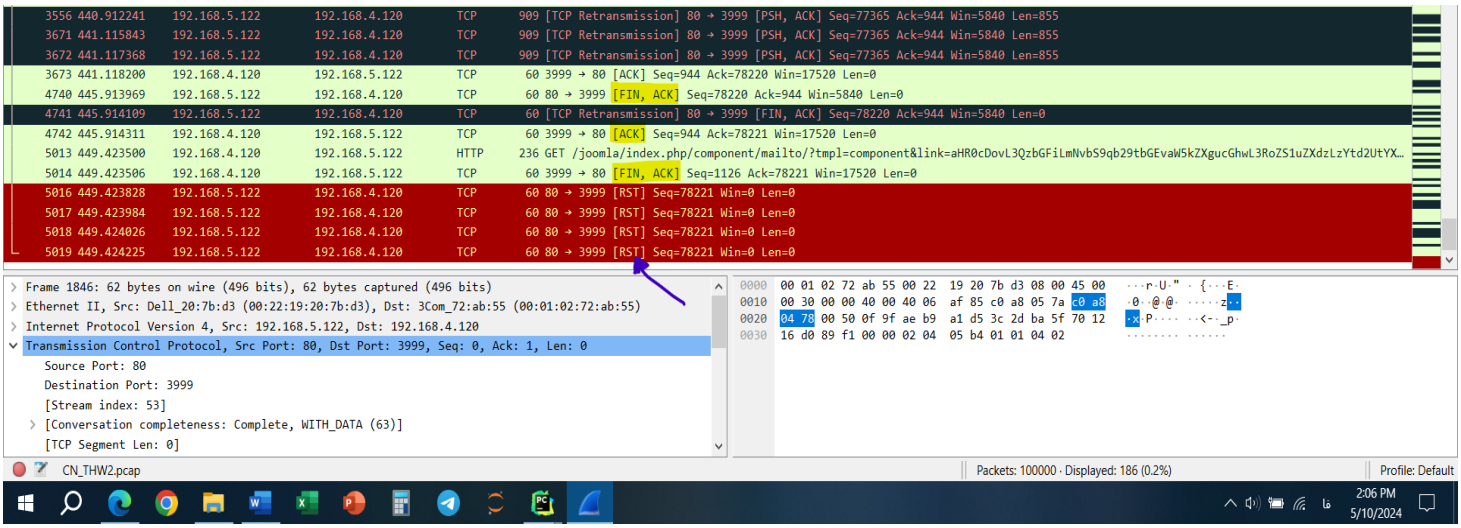


12. مطابق تصویر بالا در اولین بسته 0 است زیرا هنوز بسته‌ای نرسیده و در بسته پاسخ آن که از سرور ارسال می‌شود یکی اضافه شده و برابر با 1 و به صورت raw برابر با 1009629791 می‌شود.

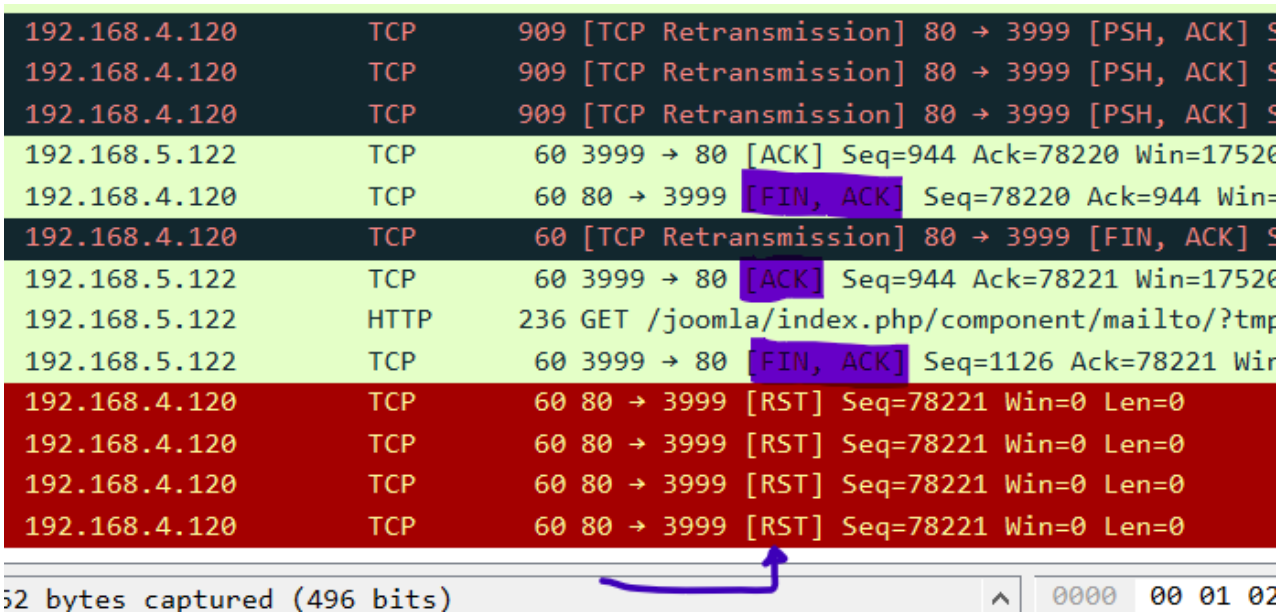

tcp.stream eq 53
No. Time Source Destination Protocol Length Info
1838 437.171885 192.168.4.120 192.168.5.122 TCP 62 3999 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1846 437.172467 192.168.5.122 192.168.4.120 TCP 62 80 → 3999 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK
1851 437.172728 192.168.5.122 192.168.4.120 TCP 62 [TCP Retransmission] 80 → 3999 [SYN, ACK] Seq=0 Ack=1 Win=584
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 Le
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 c
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 segmen
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 segmen
1950 437.287838 192.168.5.122 192.168.4.120 TCP 1514 [TCP Retransmission] 80 → 3999 [ACK] Seq=1 Ack=97 Win=5840 Le
1952 437.289127 192.168.5.122 192.168.4.120 TCP 1514 [TCP Retransmission] 80 → 3999 [ACK] Seq=1461 Ack=97 Win=5840
1955 437.290357 192.168.5.122 192.168.4.120 TCP 1514 [TCP Retransmission] 80 → 3999 [ACK] Seq=2921 Ack=97 Win=5840
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 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]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2931401173
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1009629791
0111 .... = Header Length: 28 bytes (7)
Flags: 0x012 (SYN, ACK)
Window: 5840
[Calculated window size: 5840]
Checksum: 0x89f1 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
[Timestamps]
0000 00 01 02 72 ab 55 00 22 1
0010 00 30 00 00 40 00 40 06 a
0020 04 78 00 50 0f 9f ae b9 a
0030 16 d0 89 f1 00 00 02 04 0
CN_THW2.pcap

13. داریم:





تصویر واضح‌تر:



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.