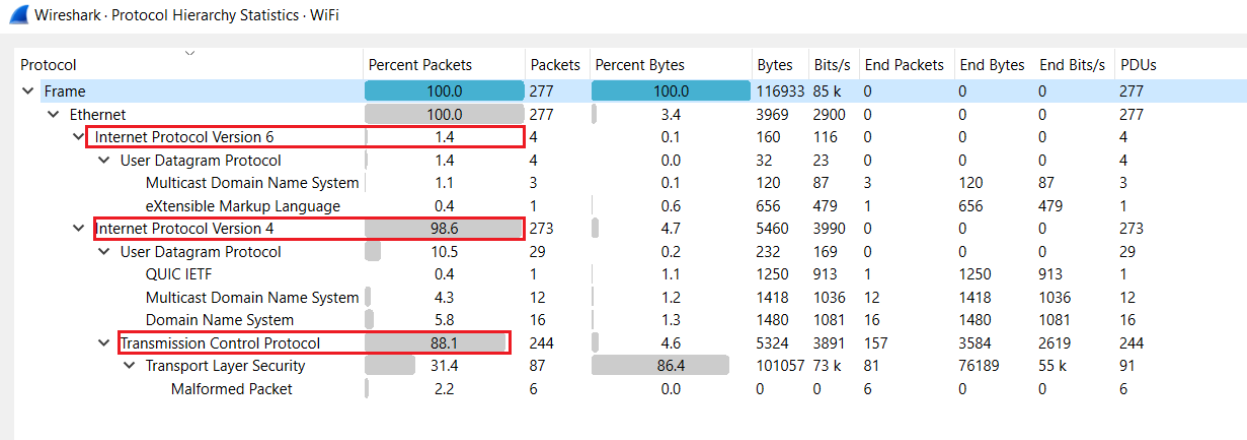
1. Utilizând utilitarul Protocol Hierarchy din cadrul wireshark stabiliți ce protocol este folosit mai mult. Dați răspunsul în valori procentuale.


Wireshark · Protocol Hierarchy Statistics · WiFi

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	277	100.0	116933	85 k	0	0	0	277
Ethernet	100.0	277	3.4	3969	2900	0	0	0	277
Internet Protocol Version 6	1.4	4	0.1	160	116	0	0	0	4
User Datagram Protocol	1.4	4	0.0	32	23	0	0	0	4
Multicast Domain Name System	1.1	3	0.1	120	87	3	120	87	3
eXtensible Markup Language	0.4	1	0.6	656	479	1	656	479	1
Internet Protocol Version 4	98.6	273	4.7	5460	3990	0	0	0	273
User Datagram Protocol	10.5	29	0.2	232	169	0	0	0	29
QUIC IETF	0.4	1	1.1	1250	913	1	1250	913	1
Multicast Domain Name System	4.3	12	1.2	1418	1036	12	1418	1036	12
Domain Name System	5.8	16	1.3	1480	1081	16	1480	1081	16
Transmission Control Protocol	88.1	244	4.6	5324	3891	157	3584	2619	244
Transport Layer Security	31.4	87	86.4	101057	73 k	81	76189	55 k	91
Malformed Packet	2.2	6	0.0	0	0	6	0	0	6

IPv6: 1.4% din pachete

IPv4: 98.6% din pachete

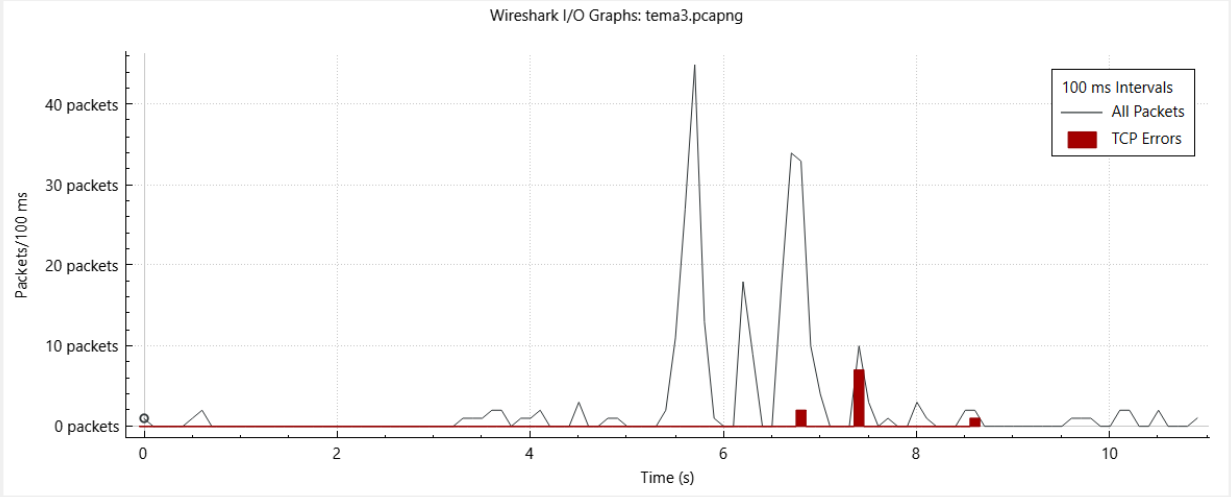
TCP: 88.1% din pachete

Astfel, protocolul IPv4 a fost utilizat mai mult în această trasă.

2. Utilizând utilitarul I/O Graph schimbați baza de timp la 1/10 dintr-o secundă și răspundeți la următoarele intrebări:

    a. Care este volumul maxim de pachete/s şi când îl găsiți?

Wireshark · I/O Graphs · tema3.pcapng



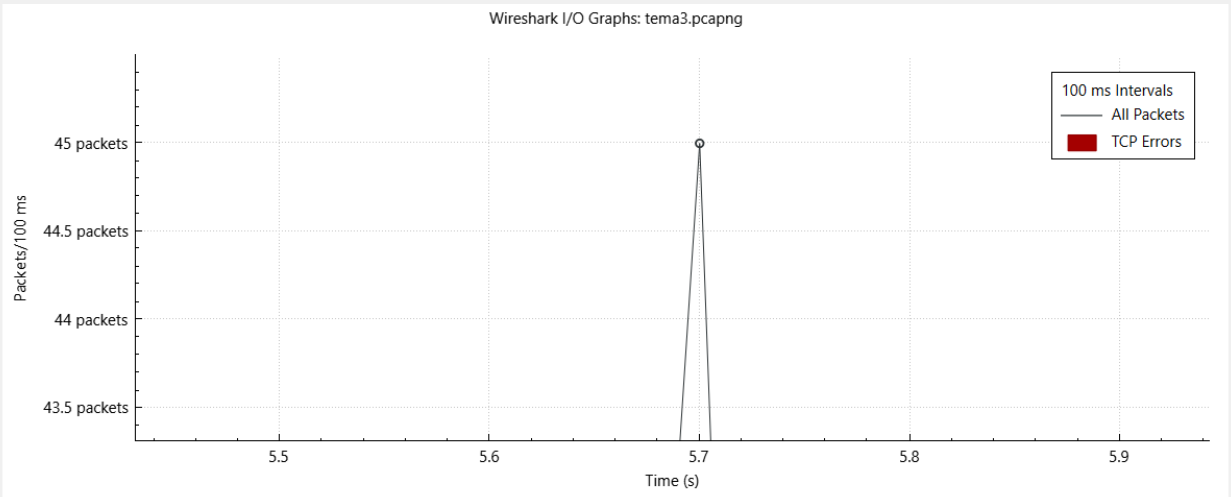
Click to select packet 1 (0.0s = 1).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	*All Packets*			*Line*	*Packets*		*None*	*1*
☑	*TCP Errors*	*tcp.analysis.flags*		*Bar*	*Packets*		*None*	*1*

Mouse ◉ drags ○ zooms Interval 100 ms ☐ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend

Reset Save As... Copy Copy from Close Help

Wireshark · I/O Graphs · tema3.pcapng



Click to select packet 105 (5.7s = 45).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	*All Packets*			*Line*	*Packets*		*None*	*1*
☑	*TCP Errors*	*tcp.analysis.flags*		*Bar*	*Packets*		*None*	*1*

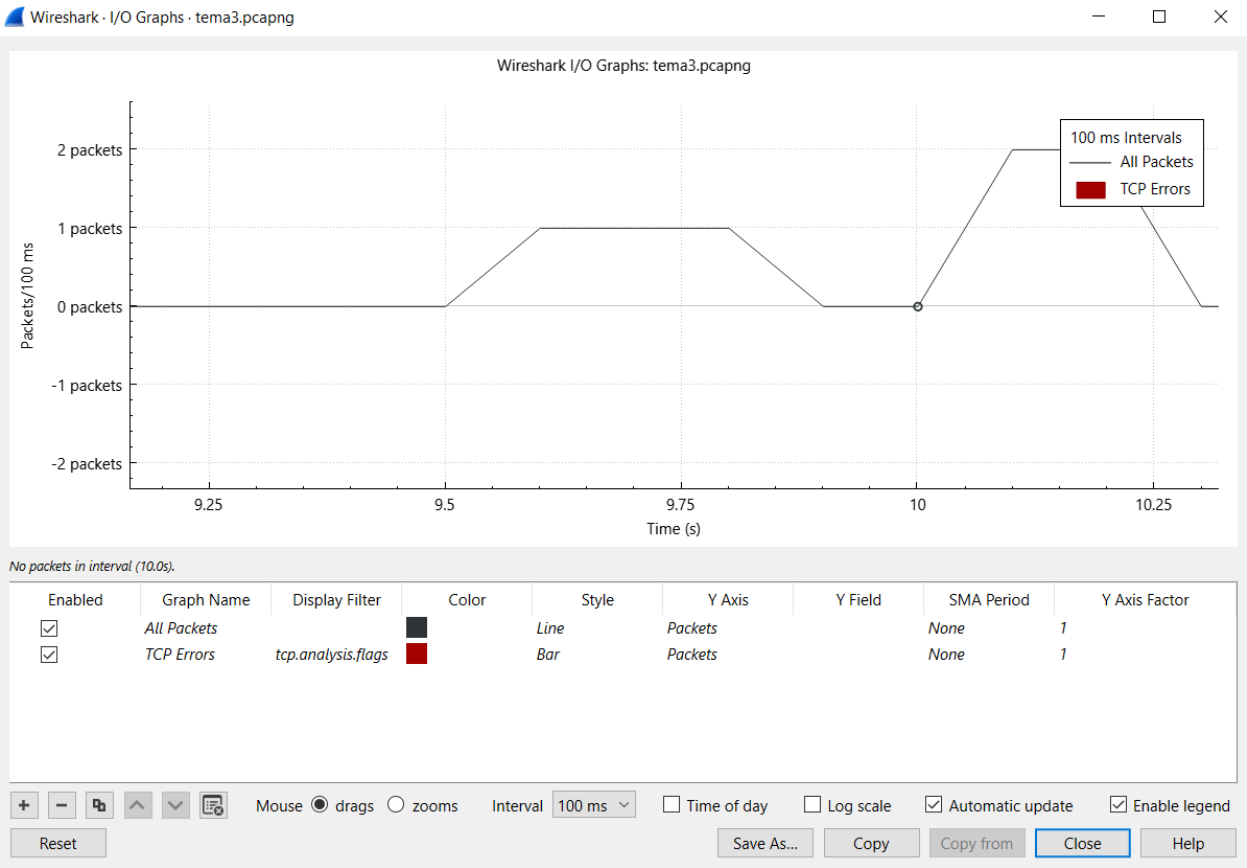
Mouse ◉ drags ○ zooms Interval 100 ms ☐ Time of day ☐ Log scale ☑ Automatic update ☑ Enable legend

Reset Save As... Copy Copy from Close Help

Volumul maxim de date este la secunda 5.7 și este de 45 pachete.

b. care este volumul de date la secundă=nr_litere_nume+nr_litere_prenume

Număr litere nume (Plesa) = 5
Număr litere prenume (Diana) = 5
Secunda = 5 + 5 = 10
Volumul de date la secunda 10 = 0 pachete



3. Utilizând o trasă de wireshark, care este dimensiunea antetului UDP, dacă luăm în considerare mai multe pachete.

No.	Time	Source	Destination	Protocol	Length	Info
16	4.501637	192.168.4.104	172.217.18.17	TCP	55	59545 → 44
17	4.572306	10.11.2.46	224.0.0.251	MDNS	100	Standard c
18	4.572827	172.217.18.17	192.168.4.104	TCP	68	443 → 5954
19	4.890174	192.168.4.104	142.250.185.238	TCP	55	59547 → 44
20	4.941910	142.250.185.238	192.168.4.104	TCP	68	443 → 5954
21	5.480757	192.168.4.104	192.168.4.1	DNS	94	Standard c
22	5.481072	192.168.4.104	192.168.4.1	DNS	94	Standard c
23	5.527171	192.168.4.1	192.168.4.104	DNS	138	Standard c
24	5.531906	192.168.4.1	192.168.4.104	DNS	177	Standard c
25	5.532617	192.168.4.104	52.236.29.249	TCP	66	59902 → 44
26	5.587792	192.168.4.104	192.168.4.1	DNS	128	Standard c

Wireshark · Packet 17 · tema3.pcapng

```
> Frame 17: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interfac
> Ethernet II, Src: TpLinkTechno_63:ce:e8 (14:cc:20:63:ce:e8), Dst: IPv4mcast_fb (0
> Internet Protocol Version 4, Src: 10.11.2.46, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)
```

```
0000  01 00 5e 00 00 fb 14 cc  20 63 ce e8 08 00 45 00   ··^····· c····E·
0010  00 56 6b 50 00 00 ff 11  63 12 0a 0b 02 2e e0 00   ·VkP···· c·······
0020  00 fb 14 e9 14 e9 00 42  ba e2 00 00 00 00 00 02   ·······B ········
0030  00 00 00 00 00 00 07 5f  72 64 6c 69 6e 6b 04 5f   ·······_ rdlink·_
0040  74 63 70 05 6c 6f 63 61  6c 00 00 0c 00 01 0f 5f   tcp·loca l·····_
0050  63 6f 6d 70 61 6e 69 6f  6e 2d 6c 69 6e 6b c0 14   companio n-link··
0060  00 0c 00 01                                       ····
```

User Datagram Protocol (udp), 8 bytes

Wireshark · Packet 22 · tema3.pcapng

```
> Frame 22: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device
> Ethernet II, Src: Intel_60:e1:7c (5c:80:b6:60:e1:7c), Dst: TpLinkTechno_63:ce:e8 (14:cc:
> Internet Protocol Version 4, Src: 192.168.4.104, Dst: 192.168.4.1
> User Datagram Protocol, Src Port: 57248, Dst Port: 53
> Domain Name System (query)
```

```
0000  14 cc 20 63 ce e8 5c 80  b6 60 e1 7c 08 00 45 00   ·· c··\· ·`·|··E·
0010  00 50 ce eb 00 00 80 11  e1 f7 c0 a8 04 68 c0 a8   ·P····· ·····h··
0020  04 01 df a0 00 35 00 3c  8c 9d ac 0e 01 00 00 01   ·····5·< ·· ·····
0030  00 00 00 00 00 00 04 70  72 6f 64 0f 72 65 77 61   ·······p rod·rewa
0040  72 64 73 70 6c 61 74 66  6f 72 6d 09 6d 69 63 72   rdsplatf orm·micr
0050  6f 73 6f 66 74 03 63 6f  6d 00 00 41 00 01         osoft·co m··A··
```

User Datagram Protocol (udp), 8 bytes

Wireshark · Packet 24 · tema3.pcapng

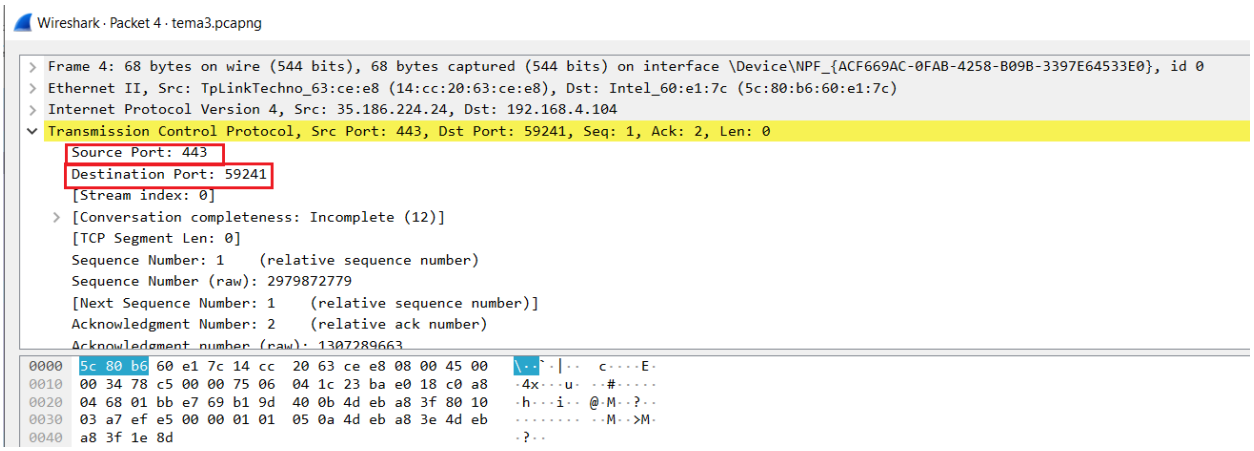
```
> Frame 24: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits) on int
> Ethernet II, Src: TpLinkTechno_63:ce:e8 (14:cc:20:63:ce:e8), Dst: Intel_60:e1:
> Internet Protocol Version 4, Src: 192.168.4.1, Dst: 192.168.4.104
> User Datagram Protocol, Src Port: 53, Dst Port: 58039
> Domain Name System (response)
```

```
0000  5c 80 b6 60 e1 7c 14 cc  20 63 ce e8 08 00 45 00   \··`·|·· c····E·
0010  00 a3 07 dd 00 00 3f 11  e9 b3 c0 a8 04 01 c0 a8   ·····?· ·····
0020  04 68 00 35 e2 b7 00 8f  07 f1 cc 9f 81 80 00 01   ·h·5···· ·· ·····
0030  00 03 00 00 00 00 04 70  72 6f 64 0f 72 65 77 61   ·····p rod·rewa
0040  72 64 73 70 6c 61 74 66  6f 72 6d 09 6d 69 63 72   rdsplatf orm·micr
0050  6f 73 6f 66 74 03 63 6f  6d 00 00 01 00 01 c0 0c   osoft·co m·····
0060  00 05 00 01 00 00 00 3f  00 20 0b 72 65 77 61 72   ·····? · ·rewar
0070  64 73 70 72 6f 64 0e 74  72 61 66 66 69 63 6d 61   dsprod·t rafficma
0080  6e 61 67 65 72 03 6e 65  74 00 c0 40 00 05 00 01   nager·ne t··@····
0090  00 00 00 3c 00 0b 08 70  72 6f 64 2d 34 63 31 c0   ···<···p rod-4c1·
00a0  11 c0 6c 00 01 00 01 00  00 00 b2 00 04 34 ec 1d   ··l····· ·····4··
00b0  f9                                                 ·
```

User Datagram Protocol (udp), 8 bytes

Dimensiunea antetului UDP este de 8 bytes.

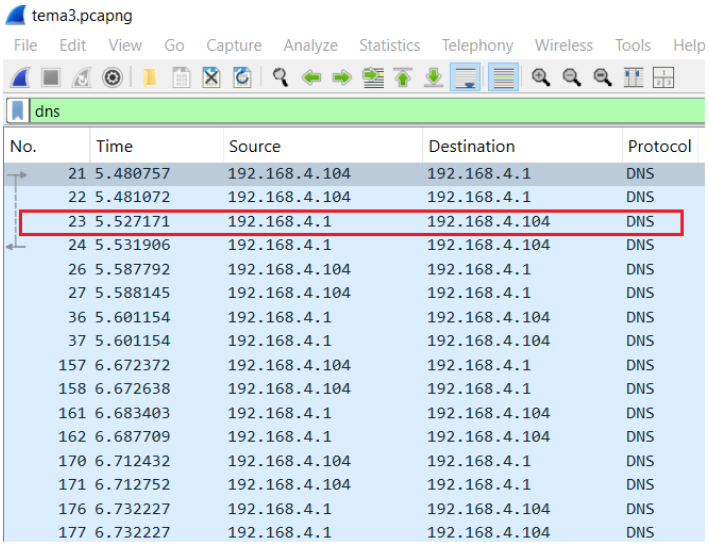
4. Utilizând al 4-lea cadru (frame), care este portul sursă şi portul destinație al cadrului?



Port sursă: 443

Port destinație: 59241

5. Pentru cel de-al 3-lea cadru DNS, care este suma, în octeți, a tuturor anetelor cadrului?



Wireshark · Packet 23 · tema3.pcapng

```
> Frame 23: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface \Device\NPF_{ACF669AC-0FAB-4258-B09B-3397E64533E0}, id 0
> Ethernet II, Src: TpLinkTechno_63:ce:e8 (14:cc:20:63:ce:e8), Dst: Intel_60:e1:7c (5c:80:b6:60:e1:7c)
> Internet Protocol Version 4, Src: 192.168.4.1, Dst: 192.168.4.104
> User Datagram Protocol, Src Port: 53, Dst Port: 57248
> Domain Name System (response)
```

```
0000  5c 80 b6 60 e1 7c 14 cc  20 63 ce e8 08 00 45 00   \··`·|··  c····E·
0010  00 7c 07 d0 00 00 3f 11  e9 e7 c0 a8 04 01 c0 a8   ·|····?· ········
0020  04 68 00 35 df a0 00 68  4c 7b ac 0e 81 80 00 01   ·h·5···h L{······
0030  00 01 00 00 00 00 04 70  72 6f 64 0f 72 65 77 61   ·······p rod·rewa
0040  72 64 73 70 6c 61 74 66  6f 72 6d 09 6d 69 63 72   rdsplatf orm·micr
0050  6f 73 6f 66 74 03 63 6f  6d 00 00 41 00 01 c0 0c   osoft·co m··A····
0060  00 05 00 01 00 00 00 3f  00 20 0b 72 65 77 61 72   ·······? · ·rewar
0070  64 73 70 72 6f 64 0e 74  72 61 66 66 69 63 6d 61   dsprod·t rafficma
0080  6e 61 67 65 72 03 6e 65  74 00                    nager·ne t·
```

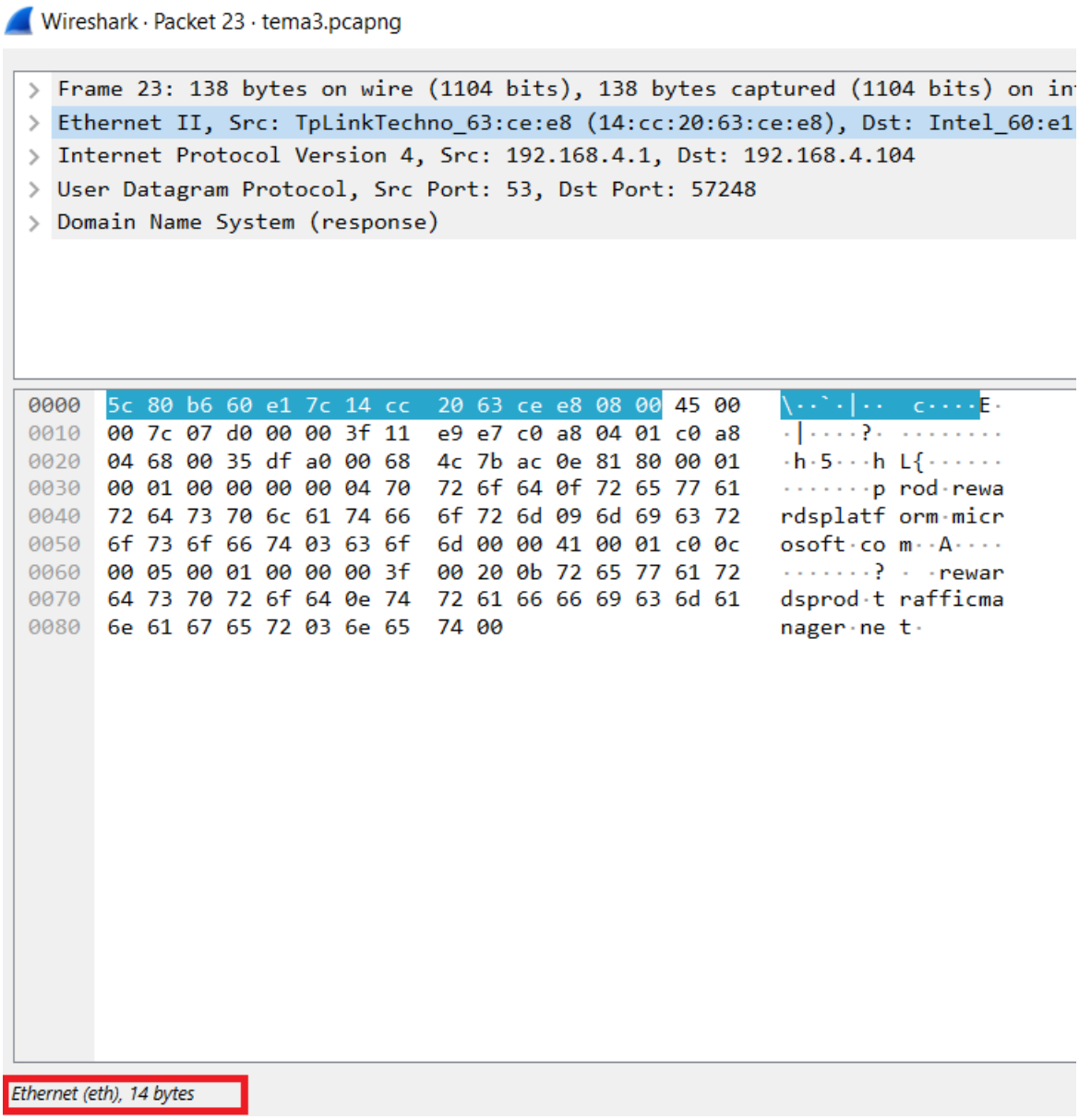
Internet Protocol Version 4 (ip), 20 bytes

Wireshark · Packet 23 · tema3.pcapng

```
> Frame 23: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface \Device\NPF_{ACF669AC-0FAB-4258-B09B-3397E64533E0}, id 0
> Ethernet II, Src: TpLinkTechno_63:ce:e8 (14:cc:20:63:ce:e8), Dst: Intel_60:e1:7c (5c:80:b6:60:e1:7c)
> Internet Protocol Version 4, Src: 192.168.4.1, Dst: 192.168.4.104
> User Datagram Protocol, Src Port: 53, Dst Port: 57248
> Domain Name System (response)
```

```
0000  5c 80 b6 60 e1 7c 14 cc  20 63 ce e8 08 00 45 00   \··`·|··  c····E·
0010  00 7c 07 d0 00 00 3f 11  e9 e7 c0 a8 04 01 c0 a8   ·|····?· ········
0020  04 68 00 35 df a0 00 68  4c 7b ac 0e 81 80 00 01   ·h·5···h L{······
0030  00 01 00 00 00 00 04 70  72 6f 64 0f 72 65 77 61   ·······p rod·rewa
0040  72 64 73 70 6c 61 74 66  6f 72 6d 09 6d 69 63 72   rdsplatf orm·micr
0050  6f 73 6f 66 74 03 63 6f  6d 00 00 41 00 01 c0 0c   osoft·co m··A····
0060  00 05 00 01 00 00 00 3f  00 20 0b 72 65 77 61 72   ·······? · ·rewar
0070  64 73 70 72 6f 64 0e 74  72 61 66 66 69 63 6d 61   dsprod·t rafficma
0080  6e 61 67 65 72 03 6e 65  74 00                    nager·ne t·
```

User Datagram Protocol (udp), 8 bytes



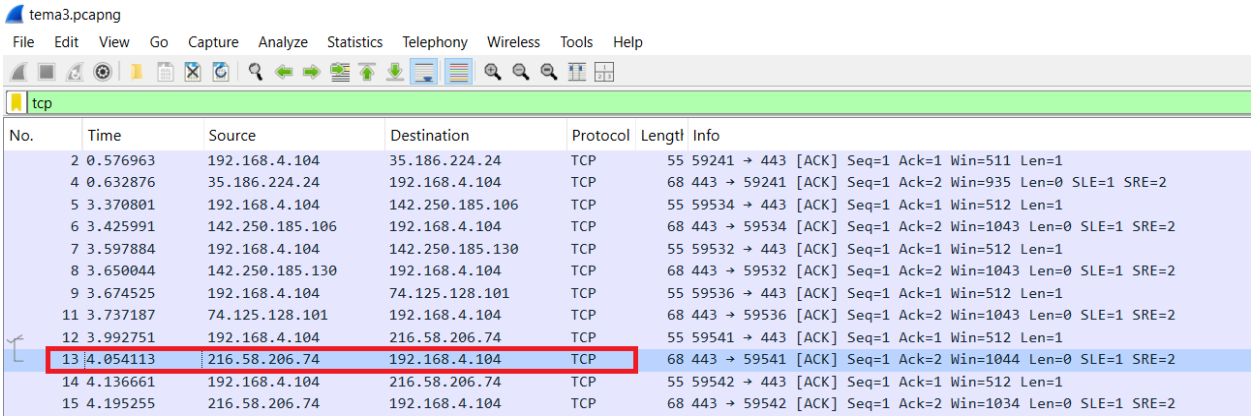
Antet IPv4 = 20 bytes

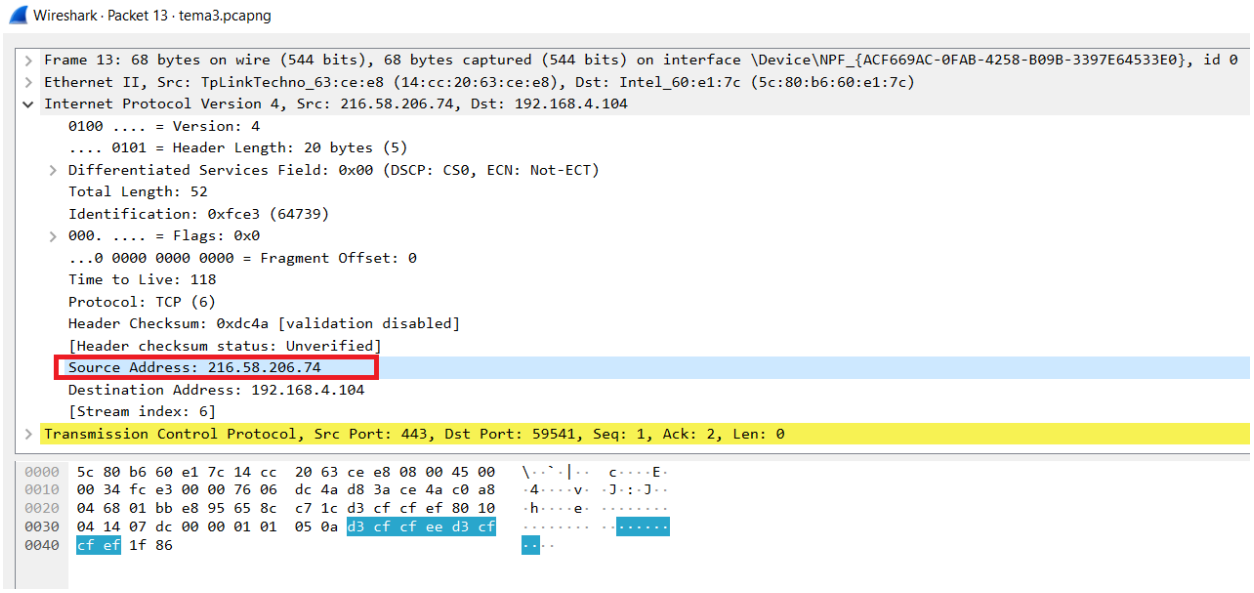
Antet UDP = 8 bytes

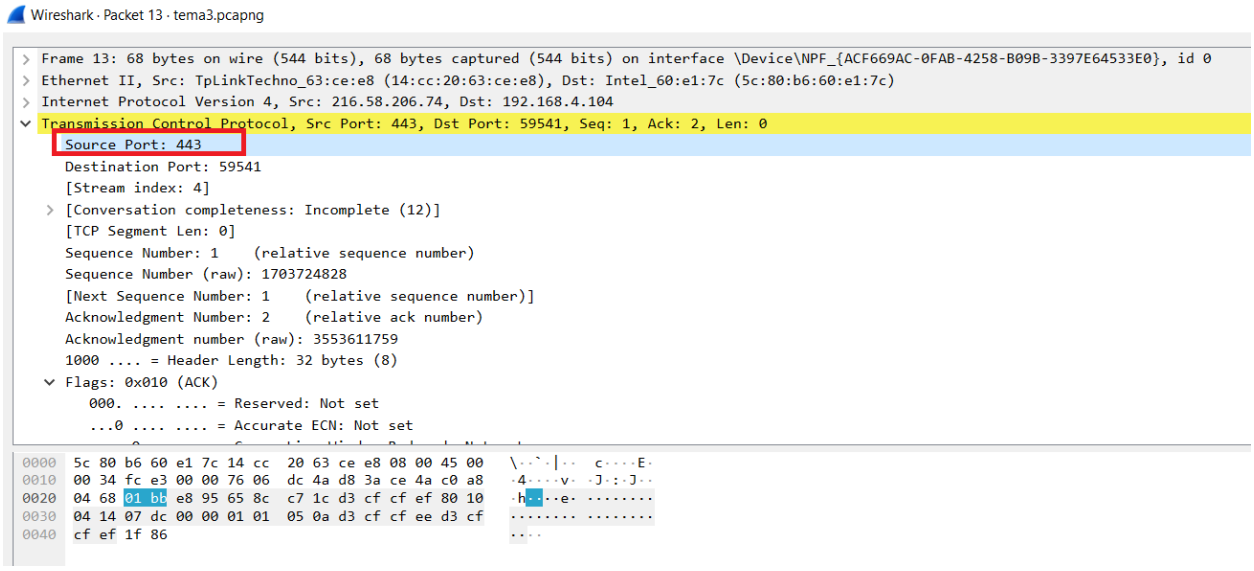
Antet Ethernet = 14 bytes

20 + 8 + 14 = 42 bytes

6. Care este socket-ul pentru sursă celui de-al 10-lea cadru TCP?







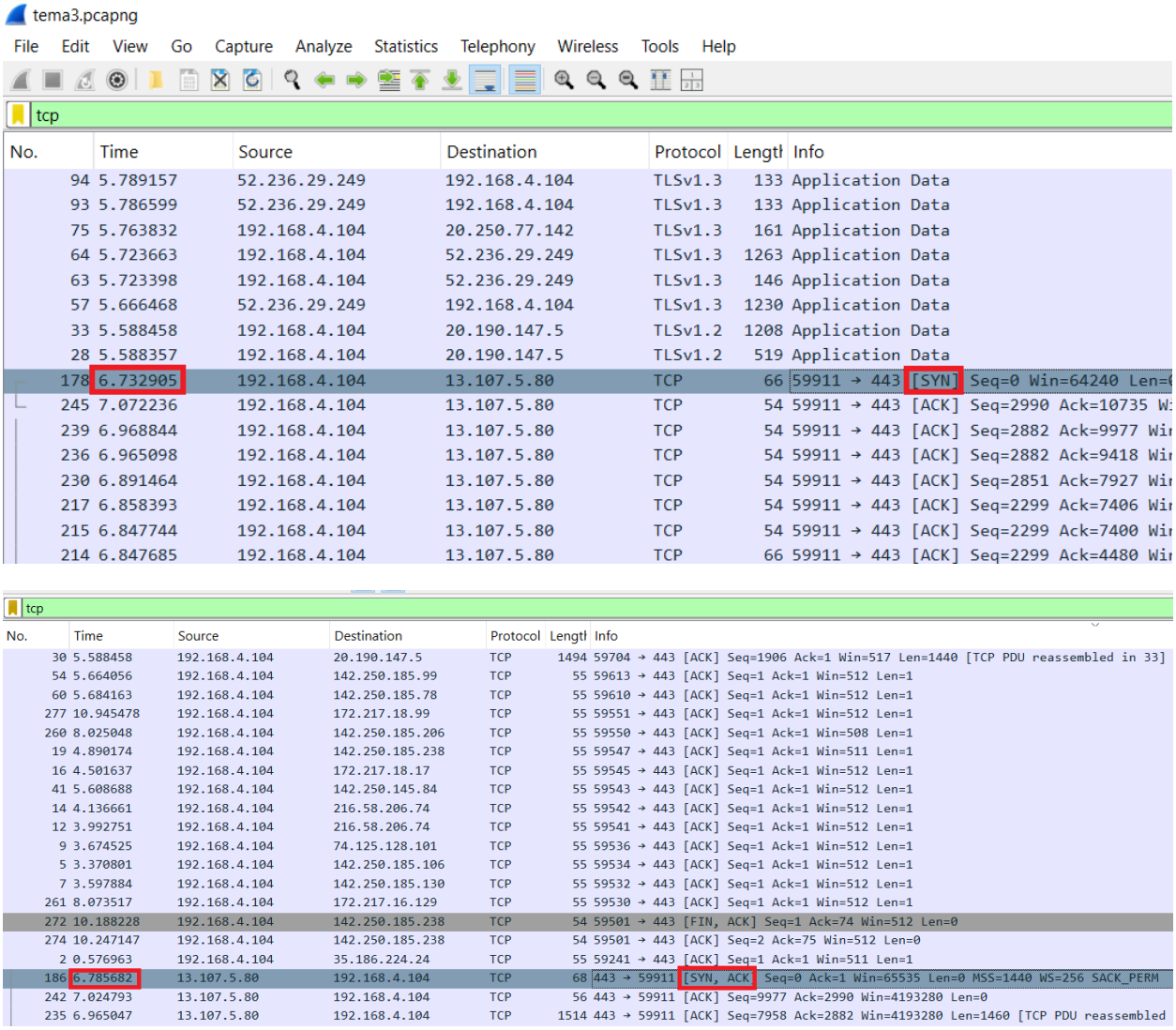
Source IPv4 Address: 216.58.206.74

Source TCP Port: 443

Socket = IPv4 Source Address:TCP Source Port

Socket = 216.58.206.74:443

7. Care este diferența de timp între mesajele SYN şi SYN-ACK ale unui singur transfer. Vă rugăm adresațivă câmpului „Info” din fereastra wireshark pentru a identifica mesajele.

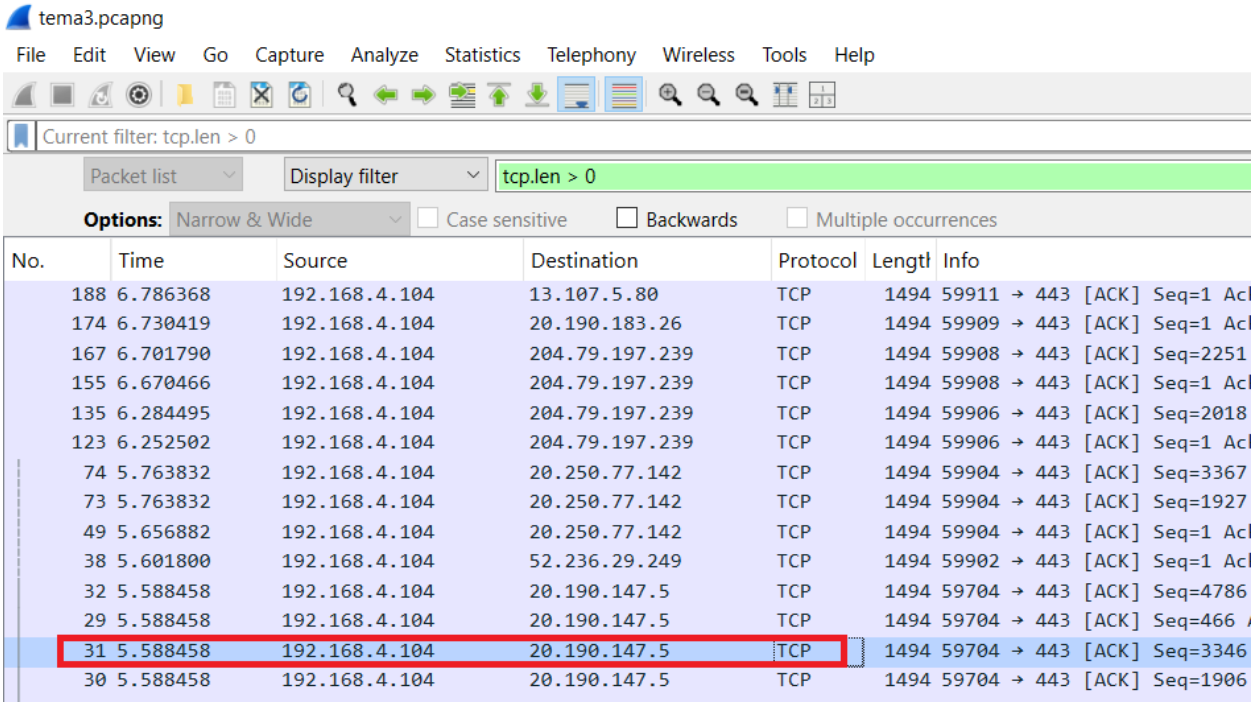


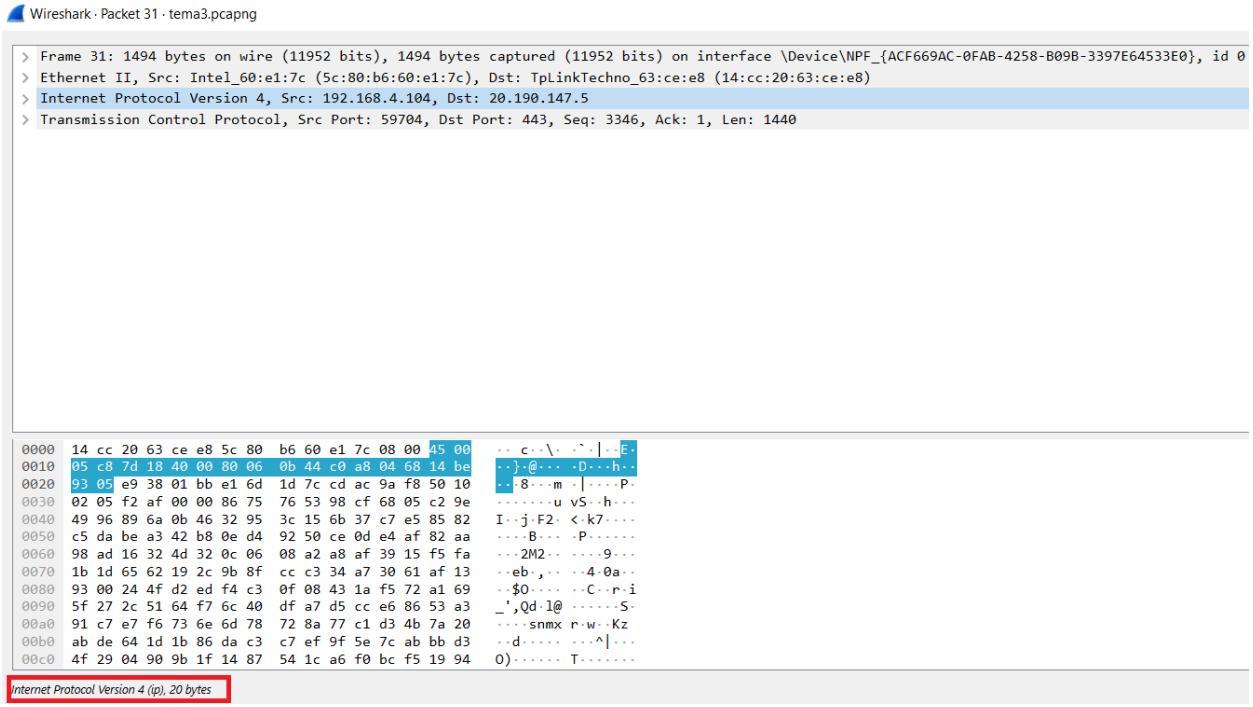
Timp SYN = 6.732905

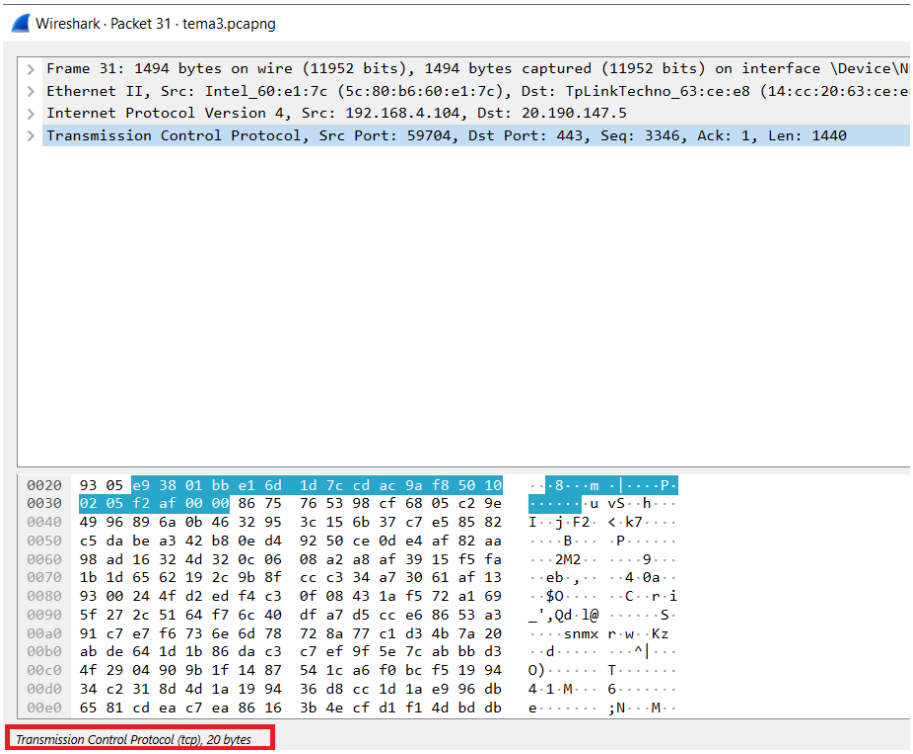
Timp SYN-ACK = 6.785682

6.732905 – 6.785682 = -0.052777

8. Vă rugăm calculați suma tuturor antetelor unui cadru TCP, având date utile (payload). Pentru o parcurgere mai facilă utilizați filtre de display(Display filter).







Antet ethernet + antet IPv4 + antet TCP = 14 + 20 + 20 = 54 bytes