

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

Exemplu_TCP.pcapng

File Edit View Go Capture Analyze **Statistics** Telephony Wireless Tools Help

Capture File Properties Ctrl+Alt+Shift+C

Resolved Addresses

Protocol Hierarchy

Conversations

Endpoints

No.	Time	Source
510	8.791569	192.168.0.87

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
Frame	100.0	2128	100.0	1590179	114 k	0	0	0	2128
Ethernet	100.0	2128	1.9	29792	2148	0	0	0	2128
Internet Protocol Version 6	27.9	593	1.5	23728	1710	0	0	0	593
Internet Protocol Version 4	71.9	1529	1.9	30580	2204	0	0	0	1529
User Datagram Protocol	2.5	53	0.0	424	30	0	0	0	53
Simple Service Discovery Protocol	0.4	8	0.1	1060	76	8	1060	76	8
QUIC IETF	0.5	11	0.3	4792	345	11	2764	199	15
Multicast Domain Name System	0.6	12	0.1	1375	99	12	1375	99	12
Domain Name System	1.0	22	0.1	1434	103	22	1434	103	22
Transmission Control Protocol	69.4	1476	1.9	30624	2207	1183	24764	1785	1476
Transport Layer Security	13.7	291	86.7	1379243	99 k	291	1360099	98 k	299
Data	0.1	2	0.0	2	0	2	2	0	2
Address Resolution Protocol	0.3	6	0.0	168	12	6	168	12	6

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

Exemplu_TCP.pcapng

File Edit View Go Capture Analyze **Statistics** Telephony Wireless Tools Help

Capture File Properties Ctrl+Alt+Shift+C

Resolved Addresses

Protocol Hierarchy

Conversations

Endpoints

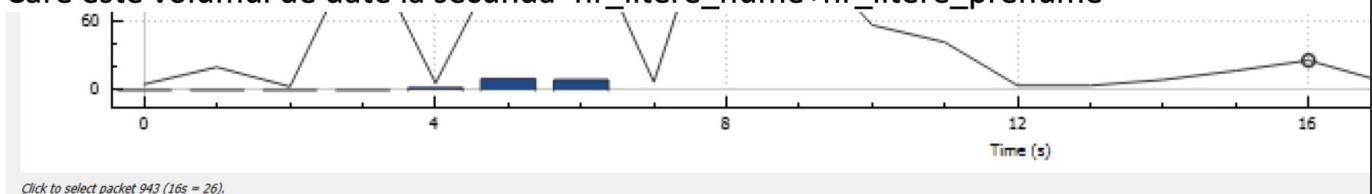
Packet Lengths

I/O Graph

Service Response Time

No.	Time	Source
510	8.791569	192.168.0.87
511	8.791703	51.116.131.41
512	8.792254	51.116.131.41
513	8.793236	78.96.7.88
514	8.794088	192.168.0.87
515	8.831530	116.202.179.166

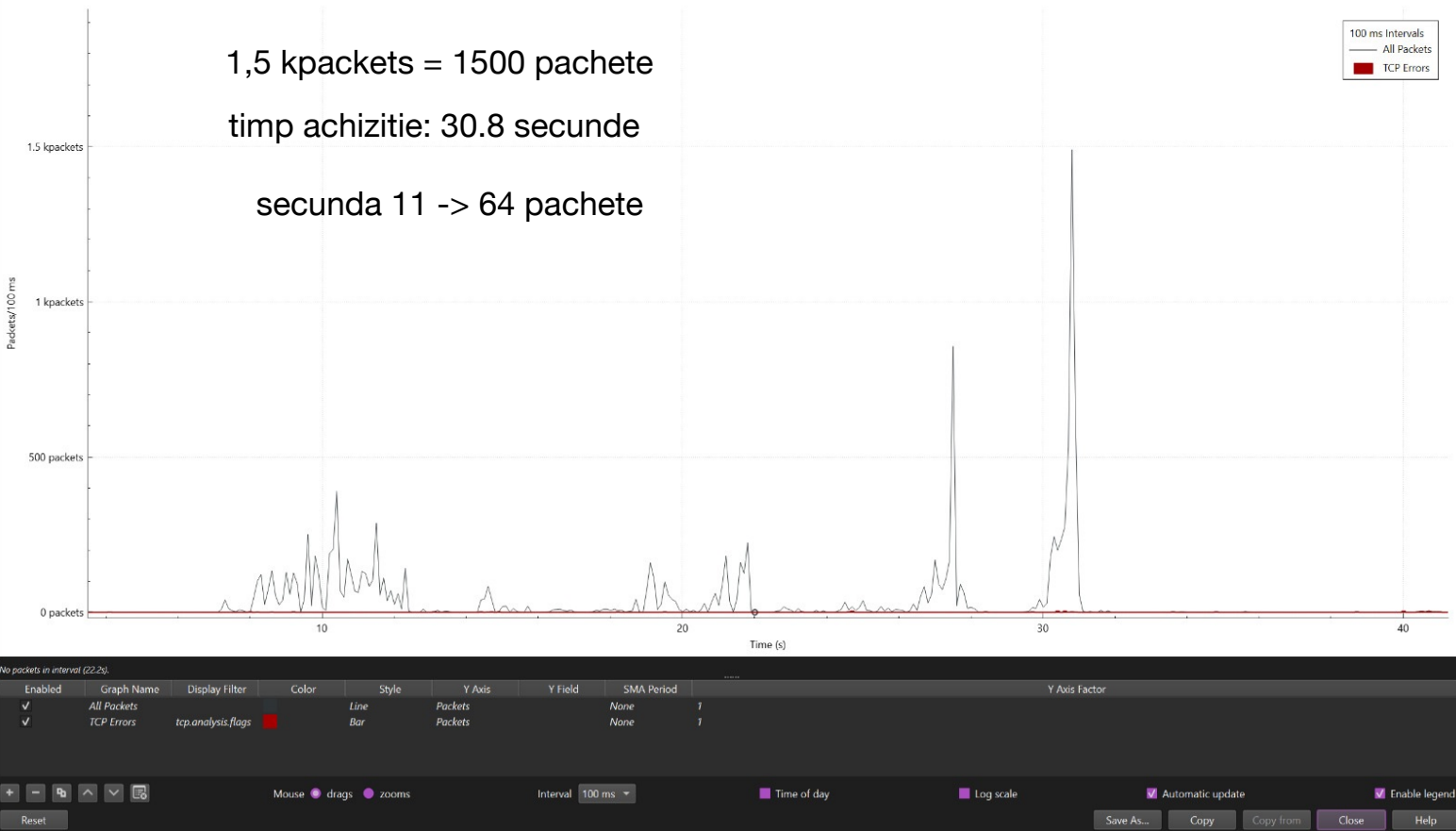
- a. Care este volumul maxim de pachete/s și când îl găsiți?
- b. Care este volumul de date la secundă= $\text{nr_litere_nume} + \text{nr_litere_prenume}$



1,5 kpackets = 1500 pachete

timp achizitie: 30.8 secunde

secunda 11 -> 64 pachete



II. UDP

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

User Datagram Protocol, Src Port: 56620, Dst Port: 53

Source Port: 56620
Destination Port: 53
Length: 45
Checksum: 0x1cd0 [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (37 bytes)

Domain Name System (query)

Transaction ID: 0x968d
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 718]

```

0000 b4 14 e6 e6 44 c7 14 ac 60 32 69 19 86 dd 60 0e ...D...2i...
0010 44 8c 00 2d 11 40 fe 80 00 00 00 00 00 00 f1 89 D...@.....
0020 a4 79 b4 ec c2 ef fe 80 00 00 00 00 00 00 00 00 y...@.....
0030 00 00 00 00 01 01 dd 2c 00 35 00 2d 1c d0 96 8d ...S...
0040 01 00 00 01 00 00 00 00 00 00 06 73 65 63 75 72 ...secu...
0050 65 08 67 72 61 76 61 74 61 72 03 63 6f 6d 00 00 e gravat ar com...
0060 1c 00 01
  
```

UDP Header -> 8 bytes

2 -> source port

2 -> destination port

2 -> message length

2 -> checksum

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

Time	Source	Destination	Protocol	Length	Info
3.0.026552	192.168.100.8	66.22.244.161	RTP	102	Sender Report
4.0.036236	66.22.244.161	192.168.100.8	UDP, H...	261	50027 -> 52142 Len=219 (SendTTL=85, Round=62)
5.0.057720	66.22.244.161	192.168.100.8	UDP, H...	265	50027 -> 52142 Len=223 (SendTTL=85, Round=62)

User Datagram Protocol, Src Port: 50027, Dst Port: 52142

Source Port: 50027
Destination Port: 52142
Length: 227

port sursa: 50027

port destinatie: 52142

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

```
> Frame 7: 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits) on interface en0, id 0
> Ethernet II, Src: HuaweiTechno_e6:44:c7 (b4:14:e6:e6:44:c7), Dst: Pauls-MacBook.local (a6:ce:07:
> Internet Protocol Version 6, Src: fe80::101 (fe80::101), Dst: Pauls-MacBook.local (fe80::c43:f7
< User Datagram Protocol, Src Port: domain (53), Dst Port: 61056 (61056)
  Source Port: domain (53)
  Destination Port: 61056 (61056)
  <Source or Destination Port: domain (53)>
  <Source or Destination Port: 61056 (61056)>
  Length: 119
  Checksum: 0x794a [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 3]
  > [Timestamps]
  UDP payload (111 bytes)
< Domain Name System (response)
  Transaction ID: 0xc547
  > Flags: 0x8583 Standard query response, No such name
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 1
  > Queries
  > Authoritative nameservers
  > Additional records
  [Request In: 6]
  [Time: 0.014160000 seconds]
```

173 bytes on wire
length: 119
length = 8 (antet udp) +
lungimea_datelor
lung_date = 119 - 8 = 111

lungimea cadrului = antet NA + antet
Internet + antet transport + lungimea
datelor

lung tuturor = lung cadru - lung date

lung tuturor = 173 - 111 = 62

bytes on wire - payload

III. TCP

Socket = IP:PORT -> 192.168.100.18:60422

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

```
> Frame 10: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface en0, id 0
> Ethernet II, Src: Pauls-MacBook.local (a6:ce:07:e9:51:30), Dst: HuaweiTechno_e6:44:c7 (b4:14:e6:e6:44:c7)
> Internet Protocol Version 4, Src: Pauls-MacBook.local (192.168.100.18), Dst: clientstream-ga.launchdarkly.com (76.223.31.44)
> Transmission Control Protocol, Src Port: 60422 (60422), Dst Port: https (443), Seq: 43, Ack: 1, Len: 46
> Transport Layer Security
```

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

398	2.398333	Pauls-MacBook.local	clientst...	TCP	78	60428 → https(443) [SYN] Seq=0
401	2.446819	clientstream-ga.laun...	Pauls-Ma...	TCP	74	https(443) → 60428 [SYN, ACK]

2.446819 - 2.398333 → 0,048486 secunde

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).

```
> Frame 844: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface en0, id 0
> Ethernet II, Src: HuaweiTechno_e6:44:c7 (b4:14:e6:e6:44:c7), Dst: a6:ce:07:e9:51:30 (a6:ce:07:e9:51:30)
> Internet Protocol Version 6, Src: mirrors.nxthost.com (2a02:13f0:8200::b064:c4fe), Dst: 2a02:2f0a:e302:1d00:c4b9
< Transmission Control Protocol, Src Port: https (443), Dst Port: 55872 (55872), Seq: 1106761, Ack: 1, Len: 1380
```

1466 - 1380 = 86 bytes