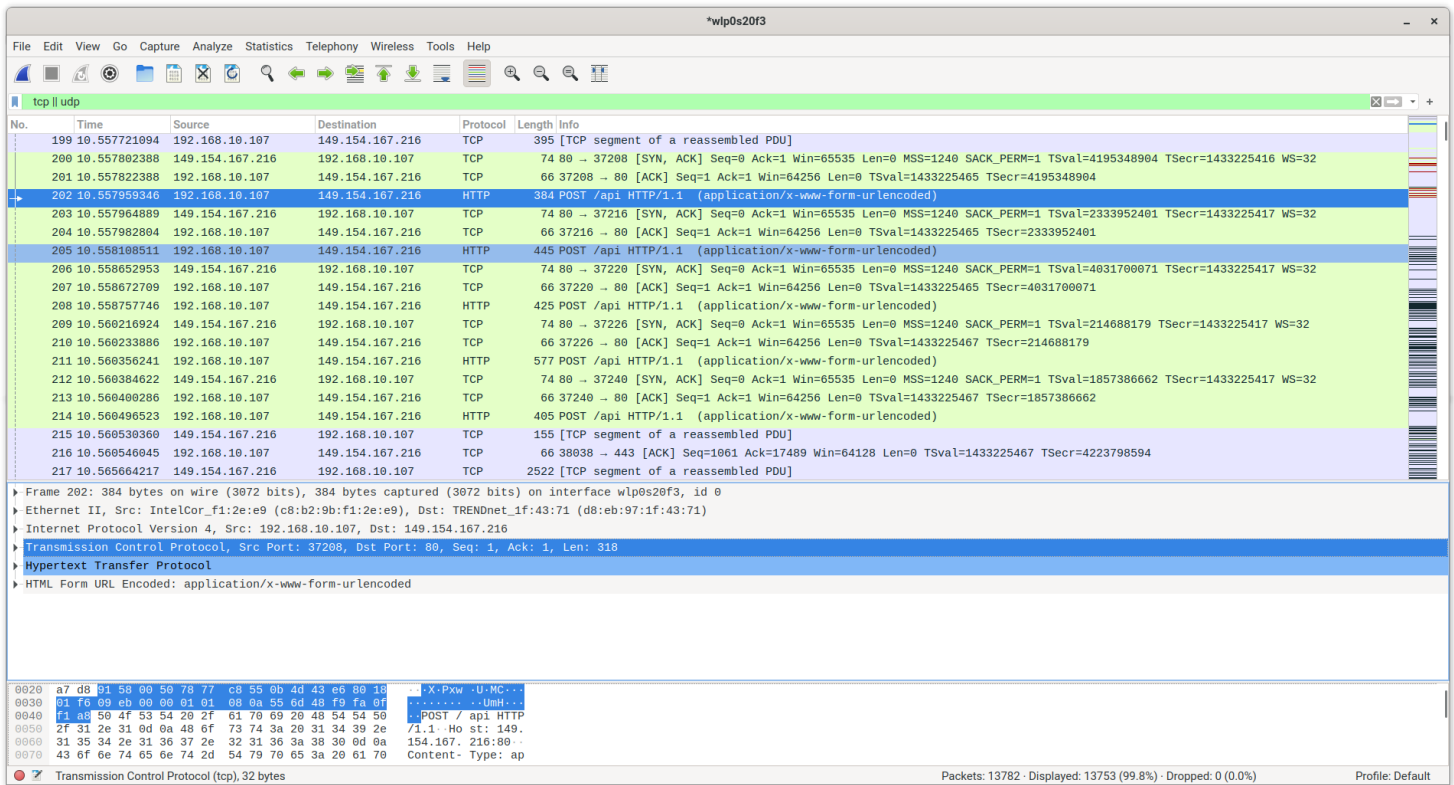


1. Порти

1. Захоплення проектів

Як http сайт брався: <http://example.com/>

2. Фільтрація по tcp || udp



На скріншоті вище, ми бачимо приклад того, що нам відображаються і інші протоколи окрім TCP і UDP - наприклад DNS, HTTP. Вони відображаються тому що, DNS використовує 53 порт UDP(або 53 порт TCP), HTTP - 80 порт TCP.

3. UDP

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp II udp

No.	Time	Source	Destination	Protocol	Length	Info
5669	19.041183579	192.168.10.107	192.168.10.1	DNS	74	Standard query 0xa300 AAAA whynohttps.com
5670	19.041169965	192.168.10.107	192.168.10.1	DNS	74	Standard query 0x2b79 A whynohttps.com
5671	19.094885437	192.168.10.1	192.168.10.107	DNS	445	Standard query response 0xa300 AAAA whynohttps.com AAAA 2606:4700:3033::6815:1c95 AAAA 2606:4700:3030::ac43:aae1 NS rob.ns.cloudflare.com
5672	19.100739584	192.168.10.1	192.168.10.107	DNS	421	Standard query response 0x2b79 A whynohttps.com A 104.21.28.149 A 172.67.170.225 NS rob.ns.cloudflare.com NS Leah.ns.cloudflare.com
5713	20.844326304	192.168.10.107	192.168.10.1	DNS	80	Standard query 0xb7c A fonts.googleapis.com
5714	20.844366725	192.168.10.107	192.168.10.1	DNS	80	Standard query 0x691a AAAA fonts.googleapis.com
5715	20.877844878	192.168.10.1	192.168.10.107	DNS	351	Standard query response 0xb7c A fonts.googleapis.com A 142.250.203.202 NS ns2.google.com NS ns4.google.com NS ns1.google.com NS ns3.google.com
5716	20.877859498	192.168.10.1	192.168.10.107	DNS	363	Standard query response 0x691a AAAA fonts.googleapis.com AAAA 2a00:1450:401b:810::200a NS ns2.google.com NS ns4.google.com NS ns1.google.com NS ns3.google.com
5737	20.947257385	192.168.10.107	192.168.10.1	DNS	87	Standard query 0x937c A safebrowsing.googleapis.com
5746	20.974295824	192.168.10.1	192.168.10.107	DNS	358	Standard query response 0x937c A safebrowsing.googleapis.com A 142.250.75.10 NS ns1.google.com NS ns2.google.com NS ns4.google.com NS ns3.google.com
5894	22.039997128	192.168.10.107	192.168.10.1	DNS	77	Standard query 0xda68 AAAA fonts.gstatic.com
5895	22.039942226	192.168.10.107	192.168.10.1	DNS	77	Standard query 0xfda3 A fonts.gstatic.com
5902	22.047692725	192.168.10.1	192.168.10.107	DNS	360	Standard query response 0xda68 AAAA fonts.gstatic.com AAAA 2a00:1450:401b:807::2003 NS ns2.google.com NS ns4.google.com NS ns1.google.com NS ns3.google.com
5903	22.048432172	192.168.10.1	192.168.10.107	DNS	348	Standard query response 0xfda3 A fonts.gstatic.com A 216.58.215.99 NS ns1.google.com NS ns3.google.com NS ns4.google.com NS ns2.google.com NS ns5.google.com
7137	26.851970111	192.168.10.107	192.168.10.1	DNS	71	Standard query 0x39ce A example.com
7138	26.852056111	192.168.10.107	192.168.10.1	DNS	71	Standard query 0x545b AAAA example.com
7139	26.856694179	192.168.10.1	192.168.10.107	DNS	223	Standard query response 0x39ce A example.com A 93.184.216.34 NS h.iana-servers.net NS a.iana-servers.net A 199.43.135.53 A 199.43.135.54

Frame 5672: 421 bytes on wire (3368 bits), 421 bytes captured (3368 bits) on interface wlp0s20f3, id 0
 Ethernet II, Src: TRENDnet_1f:43:71 (d8:eb:97:1f:43:71), Dst: IntelCor_f1:2e:e9 (c8:b2:9b:f1:2e:e9)
 Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.107
 User Datagram Protocol, Src Port: 53, Dst Port: 42930
 Source Port: 53
 Destination Port: 42930
 Length: 387
 Checksum: 0xe412 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 5]
 [Timestamps]
 UDP payload (379 bytes)
 Domain Name System (response)

0000 c8 b2 9b f1 2e e9 d8 eb 97 1f 43 71 08 00 45 00Cq...E
 0010 01 97 00 00 40 00 40 11 a3 99 c0 a8 0a 01 c0 a8@...k...

Packets: 13782 - Displayed: 122 (0.9%) Profile: Default

Порт відправника: **42930** (згенерований операційною системою)

Порт одержувача: **53** (закріплений за DNS)

4. HTTP

lab.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp II udp

No.	Time	Source	Destination	Protocol	Length	Info
200	10.557802388	149.154.167.2	192.168.10.107	TCP	74	80 → 37208 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1240 SACK_PERM=1 TSval=4195348904 TSecr=1433225416 WS=32
201	10.557822388	192.168.10.107	149.154.167.216	TCP	66	37208 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1433225465 TSecr=4195348904
202	10.557959346	192.168.10.107	149.154.167.216	HTTP	384	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
203	10.557964899	149.154.167.2	192.168.10.107	TCP	74	80 → 37210 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1240 SACK_PERM=1 TSval=4195348904 TSecr=1433225417 WS=32

Frame 202: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface wlp0s20f3, id 0
 Ethernet II, Src: IntelCor_f1:2e:e9 (c8:b2:9b:f1:2e:e9), Dst: TRENDnet_1f:43:71 (d8:eb:97:1f:43:71)
 Internet Protocol Version 4, Src: 192.168.10.107, Dst: 149.154.167.216
 Transmission Control Protocol, Src Port: 37208, Dst Port: 80, Seq: 1, Ack: 1, Len: 318
 Source Port: 37208
 Destination Port: 80
 [Stream index: 29]
 [Conversation completeness: Complete, WITH_DATA (63)]
 [TCP Segment Len: 318]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 2021115989
 [Next Sequence Number: 319 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 189613030
 1000 = Header Length: 32 bytes (8)
 Flags: 0x018 (PSH, ACK)
 Window: 502
 [Calculated window size: 64256]
 [Window size scaling factor: 128]
 Checksum: 0x99eb [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 [Timestamps]
 [SEQ/ACK analysis]
 TCP payload (318 bytes)
 Hypertext Transfer Protocol
 HTML Form URL Encoded: application/x-www-form-urlencoded

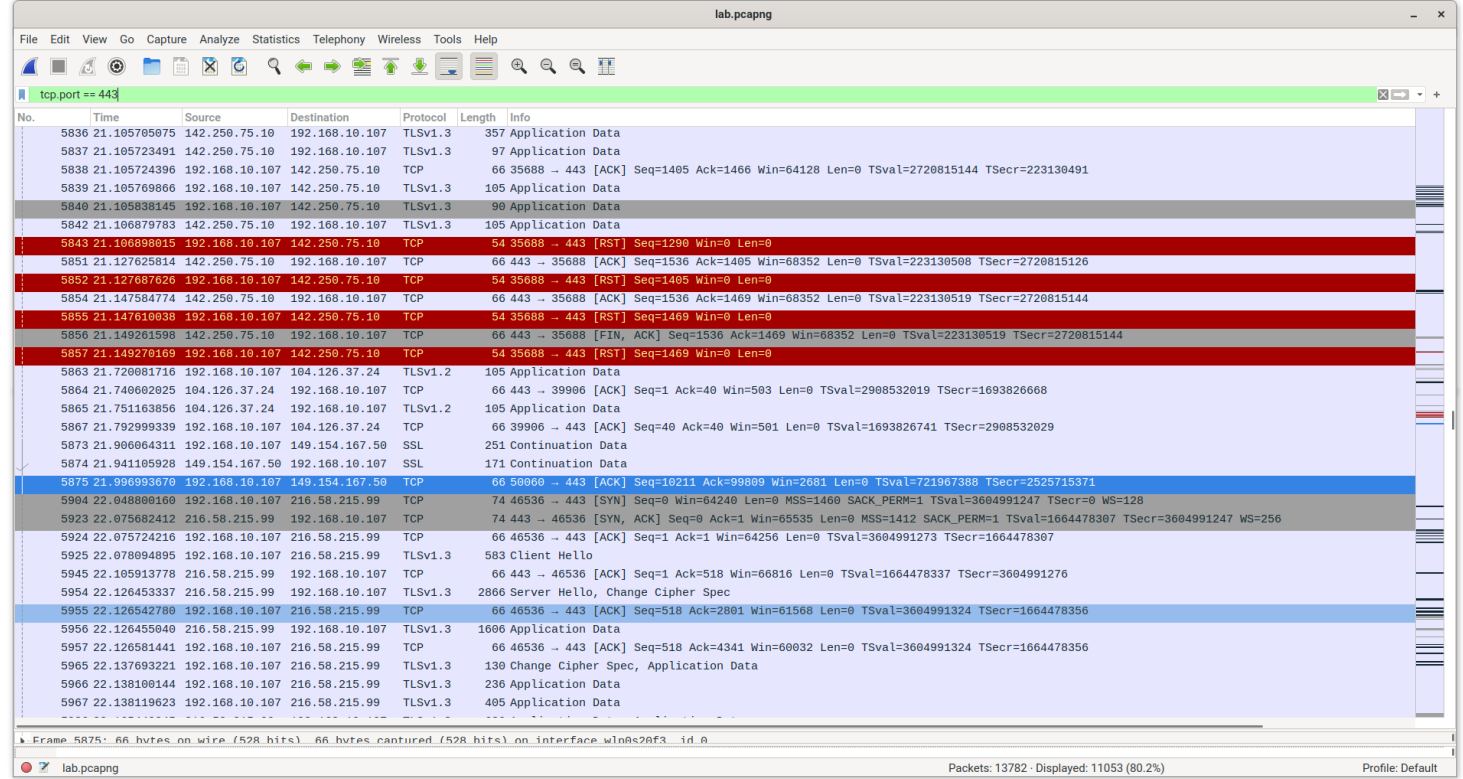
0000 d8 eb 97 1f 43 71 c8 b2 9b f1 2e e9 08 00 45 00Cq...E
 0010 01 72 8c 51 40 00 40 06 a4 ae c0 a8 0a 0b 95 9ar.Q@...k...

Packets: 13782 - Displayed: 13753 (99.8%) Profile: Default

Порт відправника: **37208** (згенерований операційною системою)

Порт одержувача: **80** (закріплений за HTTP)

5. HTTPS port



Пофільтруємо пакети за стандартним для HTTPS портом - 443. В стопці Protocol, замість HTTPS містяться такі протоколи, як TLSv1.3, TCP, SSL. Це тому, що HTTPS зашифрований у TCP, через SSL. І тому, що порт tcp == 443, ми підозрюємо, що цей пакет містить в собі HTTPS

2. TCP з'єднання

6. Потрійне рукостискання

1	0.000000000	192.168.10.108	93.184.216.34	TCP	74	39630 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2481362717 TSecr=0 WS=128
2	0.108194940	93.184.216.34	192.168.10.108	TCP	74	80 → 39630 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 SACK_PERM=1 TSval=188616514 TSecr=2481362717 WS=512
3	0.108259151	192.168.10.108	93.184.216.34	TCP	66	39630 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2481362825 TSecr=188616514

7. Опис полів

Порти:

- Порт відправника(ініціатора рукостикання): **39630** (згенерований системою)
- Порт одержувача: **80** (порт протоколу HTTP)

Прапорці:

- SYN(Synchronize): позначає ініціювання та встановлення з'єднання. Також допомагає синхронізувати порядкові номери між пристроями. Відправляється зі сторони клієнта

- ACK(Acknowledge): позначає підтвердження про надходження пакету, з прапорцем SYN. Відправляється зі сторони клієнта
- SYN, ACK: комбінація двох прапорців. Відправляється зі сторони сервера

Номери послідовностей

1 пакет

```
Transmission Control Protocol, Src Port: 39630, Dst Port: 80, Seq: 0, Len: 0
- Source Port: 39630
- Destination Port: 80
- [Stream index: 0]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 175515878
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1010 .... = Header Length: 40 bytes (10)
- Flags: 0x002 (SYN)
- Window: 64240
```

Номер послідовності - **175515878**. Це випадково згенероване число, що вказує на початок порядкових номерів для даних, які має передати

2 пакет

```
Transmission Control Protocol, Src Port: 80, Dst Port: 39630, Seq: 0, Ack: 1, Len: 0
- Source Port: 80
- Destination Port: 39630
- [Stream index: 0]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 1910895045
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 175515879
- 1010 .... = Header Length: 40 bytes (10)
- Flags: 0x012 (SYN, ACK)
```

Номер послідовності - **1910895045**. Окрім випадково згенерованого Sequence

number , також містить Acknowledgment number , що рівне Sequence number першого пакету + 1

3 пакет

Transmission Control Protocol, Src Port: 39630, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 39630

Destination Port: 80

[Stream index: 0]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 175515879

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1910895046

1000 = Header Length: 32 bytes (8)

Flags: 0x010 (ACK)

Window: 502

Номер послідовності - 175515879. Рівне Sequence number першого пакету + 1

8. HTTP пакети

lab.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
113	8.823642985	192.168.10.107	149.154.167.216	HTTP	348	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
120	8.948968183	149.154.167.2...	192.168.10.107	HTTP	413	HTTP/1.1 200 OK
202	10.557959346	192.168.10.107	149.154.167.216	HTTP	384	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
205	10.558108511	192.168.10.107	149.154.167.216	HTTP	445	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
208	10.558757746	192.168.10.107	149.154.167.216	HTTP	425	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
211	10.560356241	192.168.10.107	149.154.167.216	HTTP	577	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
214	10.560496523	192.168.10.107	149.154.167.216	HTTP	485	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
244	10.614713872	149.154.167.2...	192.168.10.107	HTTP	381	HTTP/1.1 200 OK
253	10.625399431	149.154.167.2...	192.168.10.107	HTTP	373	HTTP/1.1 200 OK
254	10.625423955	149.154.167.2...	192.168.10.107	HTTP	300	HTTP/1.1 200 OK
257	10.628018281	149.154.167.2...	192.168.10.107	HTTP	401	HTTP/1.1 200 OK
262	10.631046186	149.154.167.2...	192.168.10.107	HTTP	321	HTTP/1.1 200 OK
749	11.212936609	192.168.10.107	149.154.165.96	HTTP	504	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
869	11.349221554	149.154.165.96	192.168.10.107	HTTP	300	HTTP/1.1 200 OK
1012	11.453201016	192.168.10.107	149.154.165.96	HTTP	516	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
1161	11.582893303	149.154.165.96	192.168.10.107	HTTP	337	HTTP/1.1 200 OK
3849	14.516889546	192.168.10.107	149.154.167.216	HTTP	489	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
3914	14.560071539	149.154.167.2...	192.168.10.107	HTTP	389	HTTP/1.1 200 OK
7144	27.093107579	192.168.10.107	93.184.216.34	HTTP	401	GET / HTTP/1.1

Acknowledgment number (raw): 1129896895

1000 = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)

Window: 502

[Calculated window size: 64256]

[Window size scaling factor: 128]

Checksum: 0x09c7 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

0030 01 f6 09 c7 00 00 01 01 08 0a 55 6d 42 32 fa 4dUmB2-K
0040 03 8c 50 4f 53 54 20 2f 61 70 69 20 48 54 5a 50 POST / api HTTP
0050 2f 31 2e 31 9d 0a 49 6f 73 74 3a 20 31 34 39 2e /1.1-Host: 149.
0060 31 35 34 2e 31 36 37 2e 32 31 36 3a 38 30 0d 0a 154.167.216:80
0070 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 Content-Type: ap
0080 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d plicatio n/x-www-

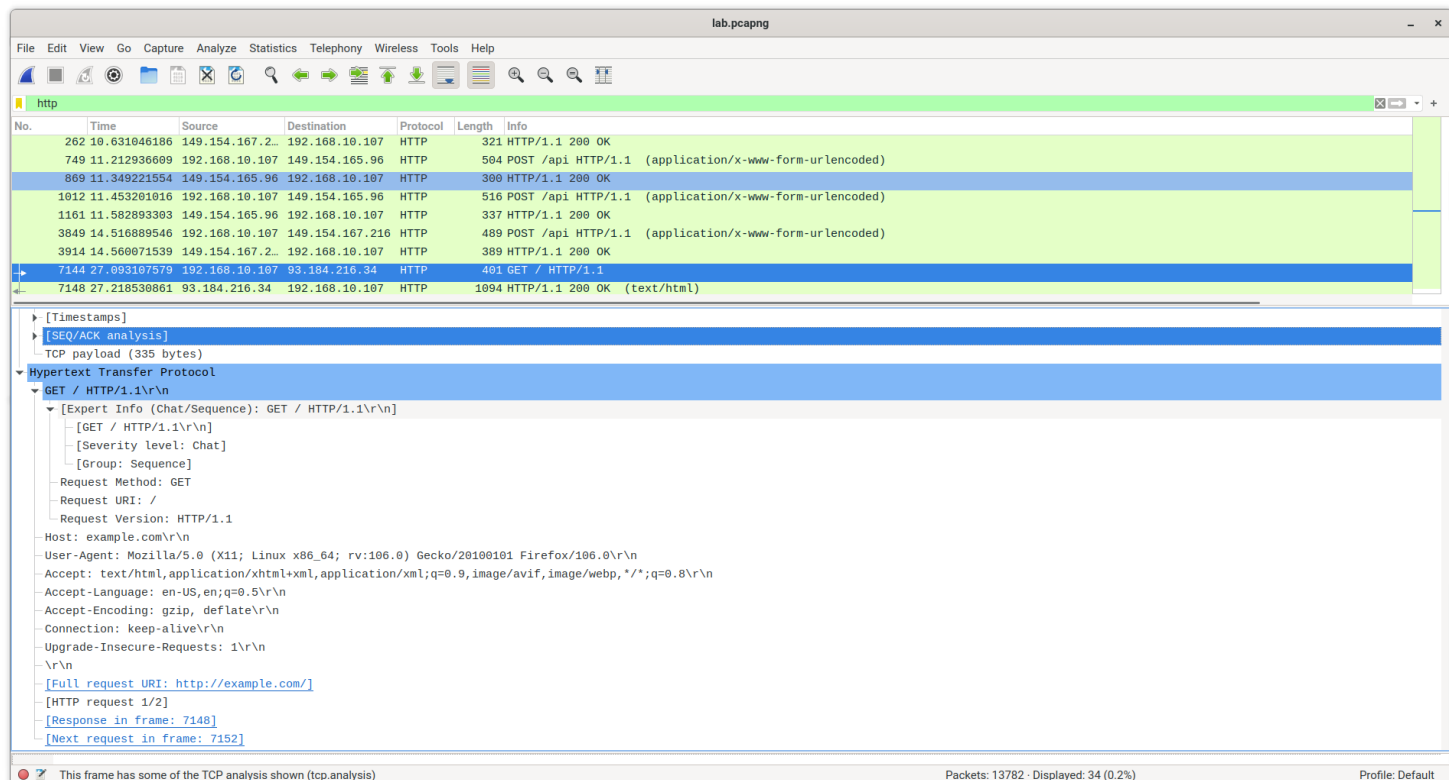
Hypertext Transfer Protocol: Protocol

Packets: 13782 - Displayed: 34 (0.2%)

Profile: Default

9. Текст запитів

Запит



GET /HTTP/1.1 - інформація про метод

Expert info

Severity level - рівень важливості (chat == звичайний пакет)

Group: Sequence - порядковий номер протоколу був підозрілим, наприклад, він не був безперервним або була виявлена повторна передача.

Request method - використовуваний HTTP метод

Uri - ідентифікатор ресурсу по сайту

Version - версія HTTP

Host - хост сайту, на який надіслано запит

User-Agent - інформація про програму, операційну система та версію запитуючого агента клієнта

Асерт - можливі формати, які можуть бути в тілі запиту

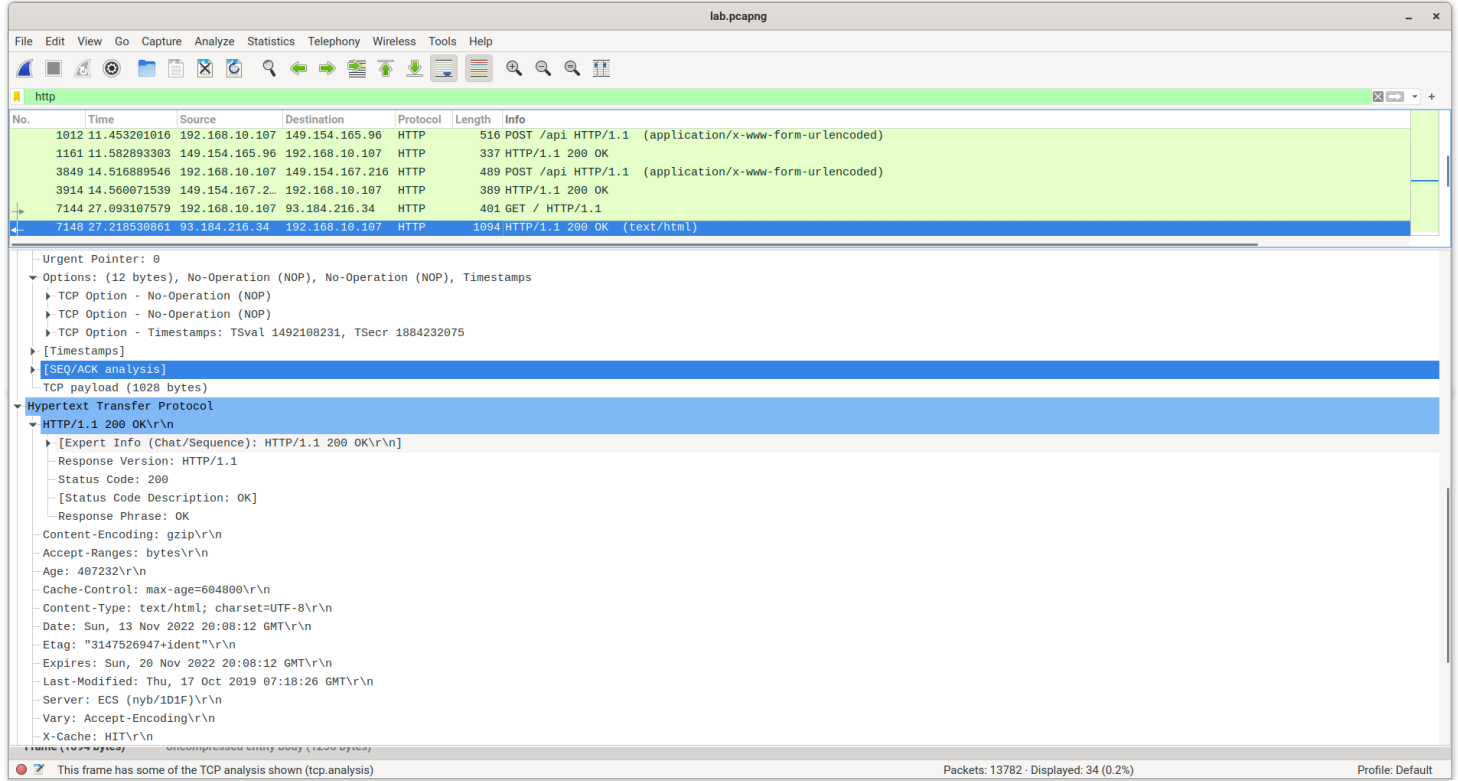
Асерт-Language - мова, якою клієнт хоче отримувати інформацію

Асерт-Encoding - кодування вмісту, зазвичай алгоритми стиснення

Connection - вказує, чи залишиться з'єднання дійсним після завершення транзакції

Upgrage-Insecure-Requests - містить інформацію про те, чи клієнт надає перевагу зашифрованій відповіді. Тобто - чи підвищувати рівень безпеки до HTTPS

Відповідь



HTTP/1.1 200 OK - інформація про метод

Expert info

Severity level - рівень важливості (chat == звичайний пакет)

Group: Sequence - порядковий номер протоколу був підозрілим, наприклад, він не був безперервним або була виявлена повторна передача.

Request method - використовуваний HTTP метод

Uri - ідентифікатор ресурсу по сайту

Version - версія HTTP

Status Code - статус відповіді запиту

Response phrase -

Content-Encoding - список всіх типів кодувань, що використовувались для вмісту

Age - час в секундах, коли відповідь була в кеші проксі

Cache-Control - містить інструкції, що керують кешуванням браузера

Content-Type - оригінальний тип ресурсу(до кодування вмісту)

Date - дата та час відповіді

Etag - ідентифікатором певної версії ресурсу

Expires - дата та час, після яких відповідь вважається простроченою.

Last-Modified - дата й час, коли вихідний сервер вважає, що ресурс було востаннє змінено

Server - сервер, який згенерував відповідь

Vary - частини повідомлення запиту(окрім методу та адреси) які вплинули на вміст відповіді

10 Типи запитів

Окрім GET методів був тільки POST (який ймовірно виник при пошуку повідомлення в програмі "телеграм"). Інших методів не було, бо я не робив відповідних дій - модифікування даних або їхнє видалення.