

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

**Комп'ютерні інформаційні мережі**

**ЛАБОРАТОРНА РОБОТА №3**

Виконав:

*Ст. Лук'янчук Денис*

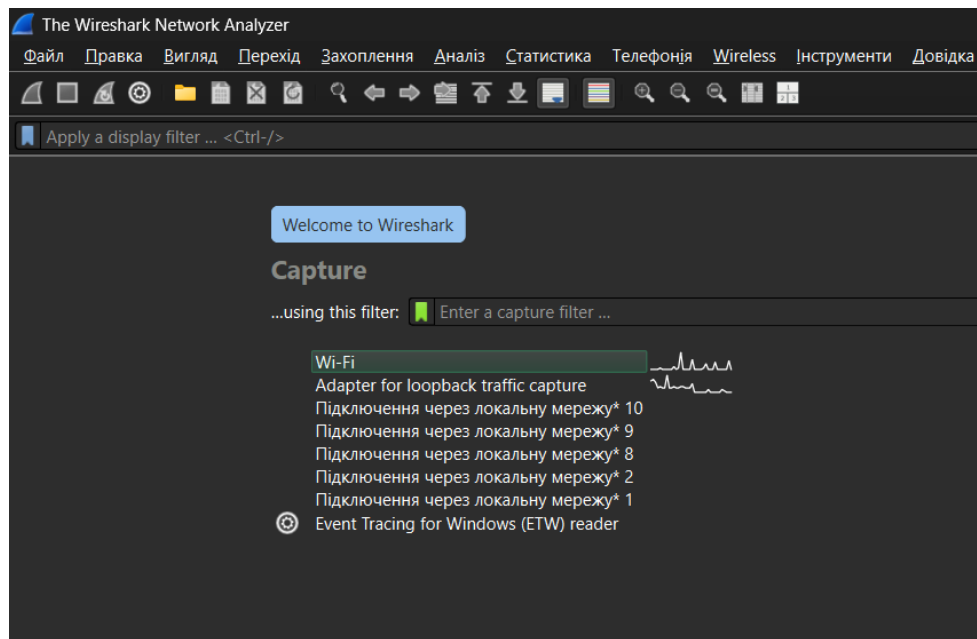
Група ПМі-33

## Тема: “Інтерфейс аналізатора мережевих пакетів Wireshark”

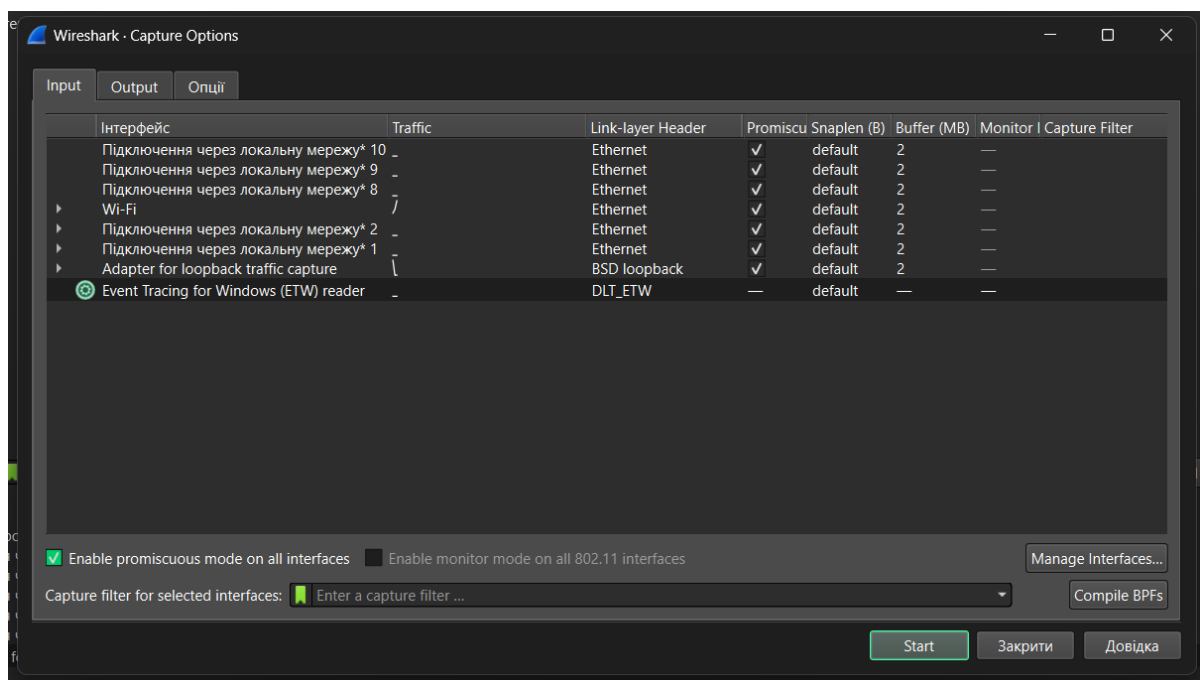
**Мета роботи:** Отримати загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark; ознайомитися з графічним інтерфейсом програми та основними параметрами конфігурації; навчитися захоплювати, сортувати та фільтрувати пакети.

### Хід роботи

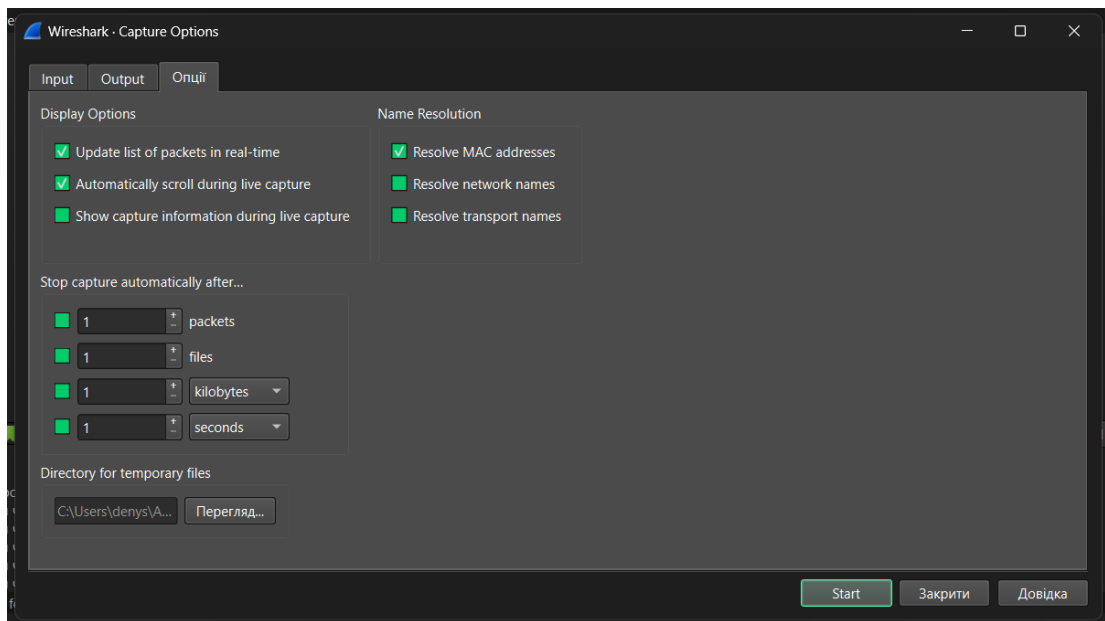
1. Запустив аналізатор мережевих пакетів Wireshark від імені адміністратора. Вибрав з переліку Wi-Fi та почав захоплення:



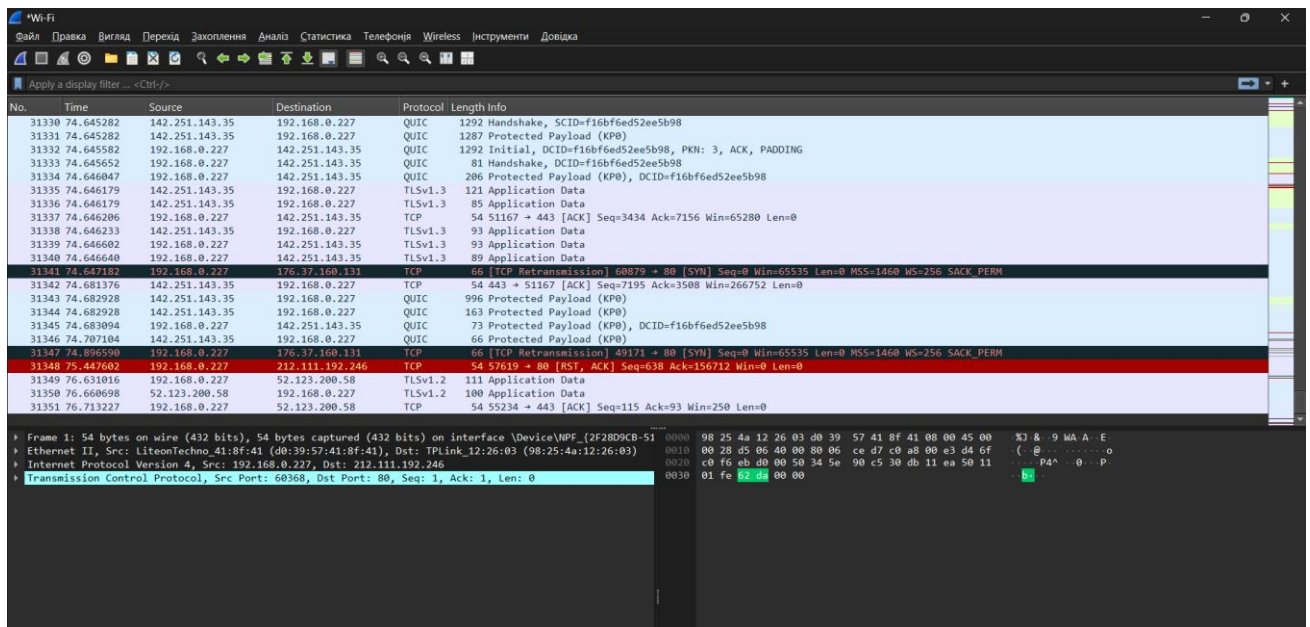
2. Виконав команду Захоплення → Опції, переконався, що мережеві карти (інтерфейси) налаштовані для роботи у нерозбірливому режимі (promiscuous mode):



3. Перейшов на вкладку Опції та ознайомився з налаштуванням захоплення пакетів:



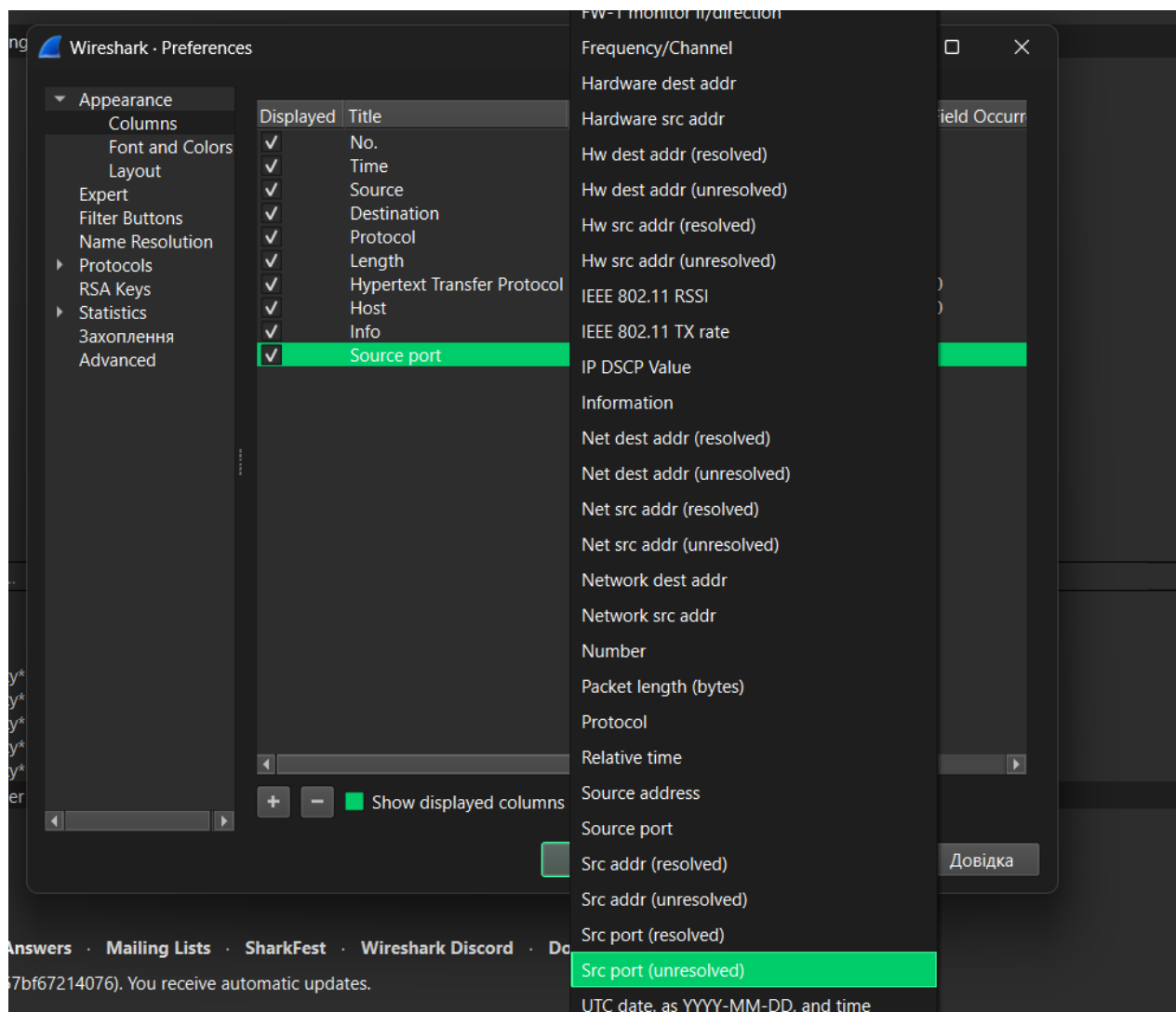
4. Вибрав з переліку Wi-Fi та почав захоплення пакетів. Упродовж 1 хвилини здійснив активність в браузері: перейшов на сайти <http://uac.gov.ua>, завантажив на комп'ютер зображення та різні файли. Зупинив процедуру захоплення пакетів. Ознайомився з трьома основними елементами головного вікна програми:



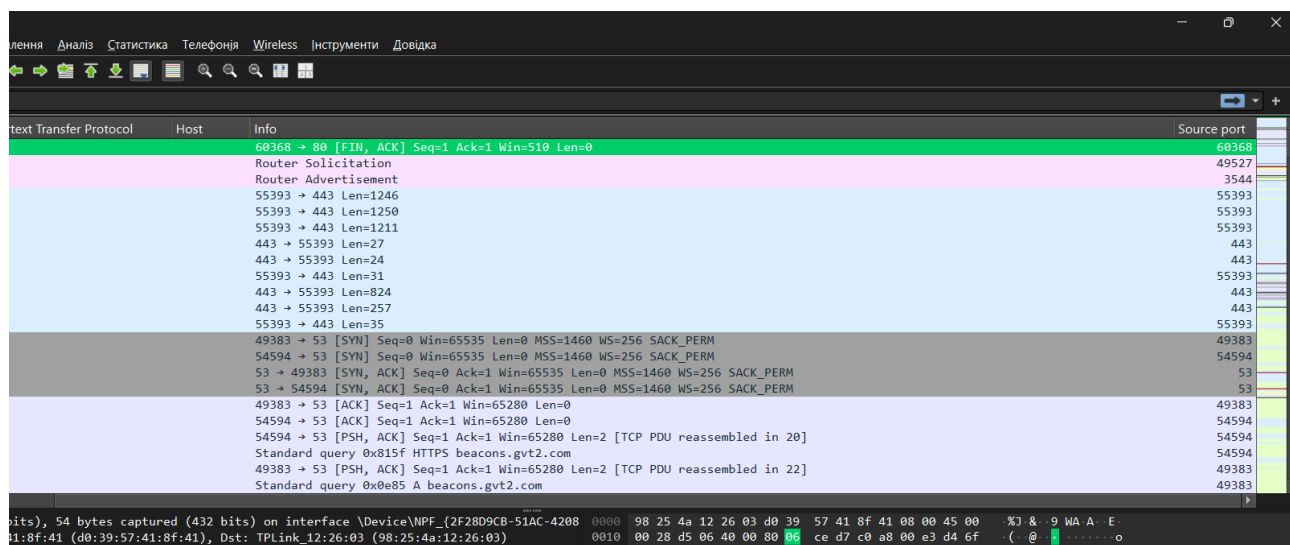
5. Зберіг захоплені пакети у файл для подальшого аналізу:



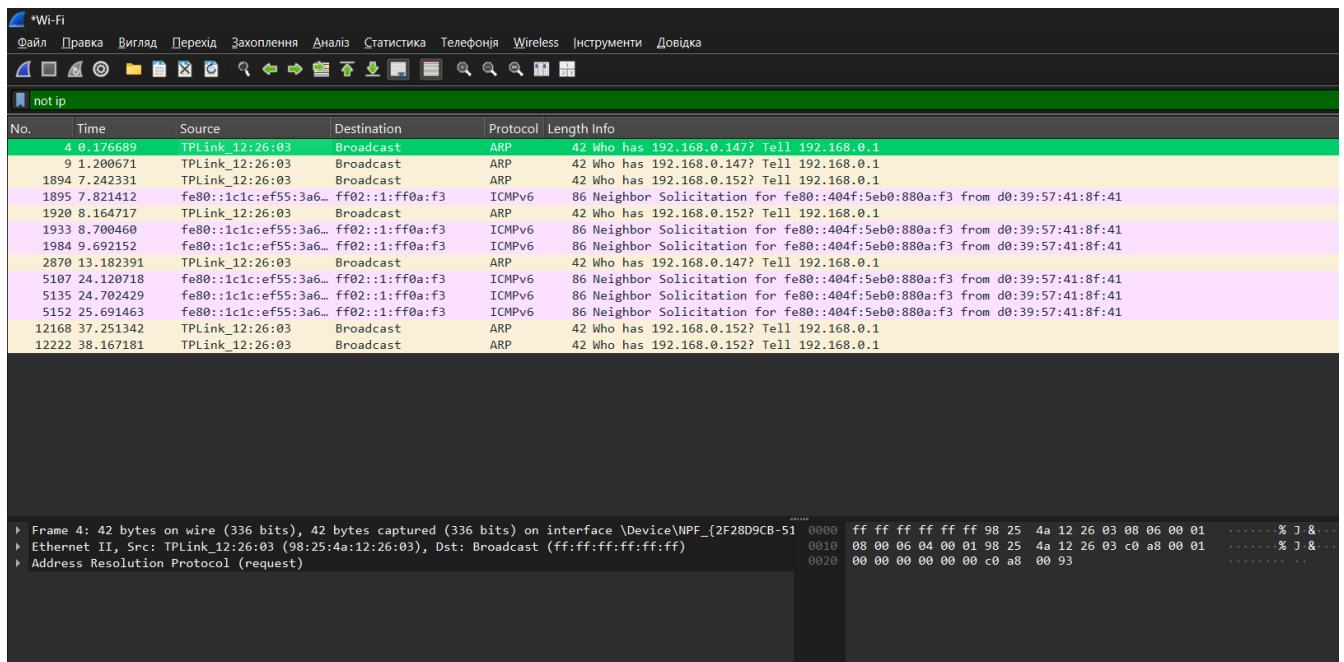
6. Відкрив вікно налаштувань, виконавши команду Правка → Налаштування. Додавав новий стовпчик Source port обравши пункт Columns, натиснув кнопку +, ввів назву стовпчика і тип даних у ньому:



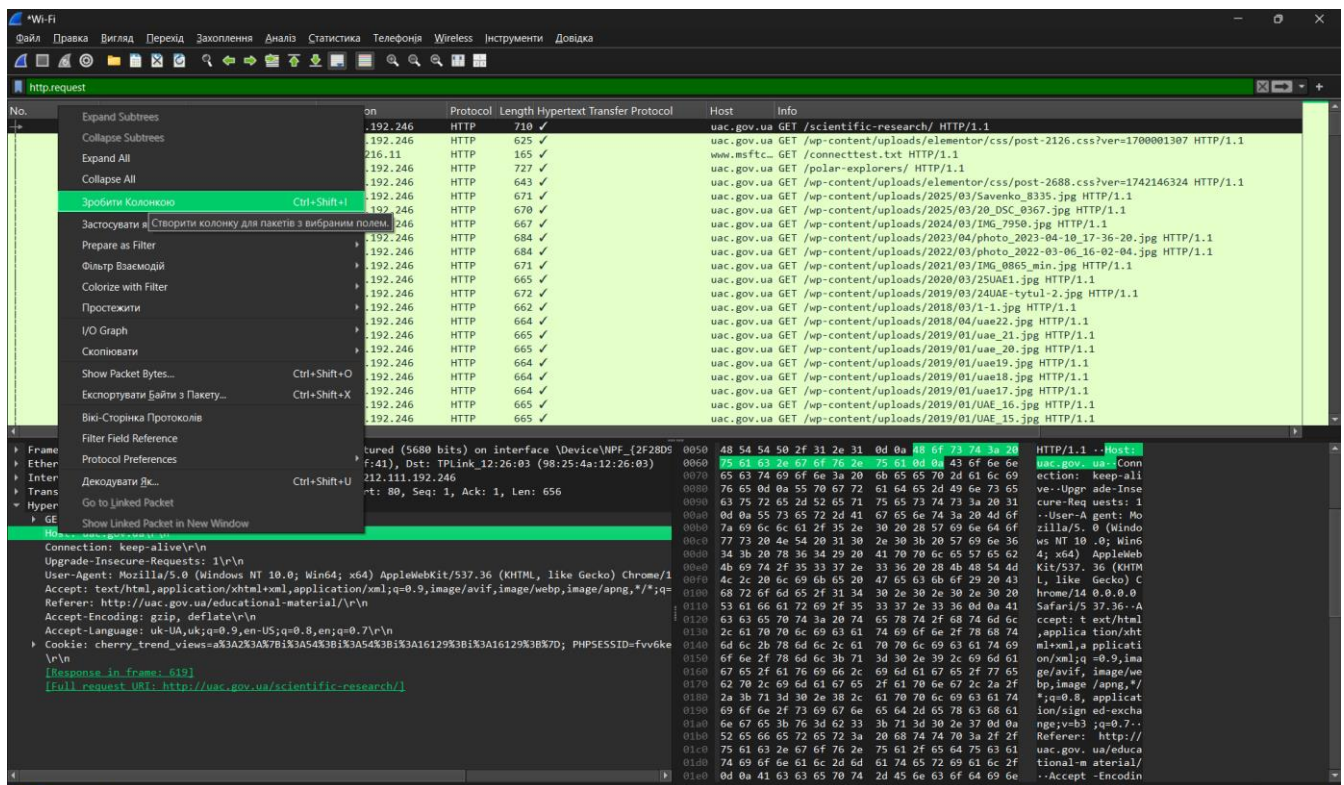
Переконався, що стовпчик з'явився в області “Список пакетів”:



7. Знайшов пакети, які не стосуються протоколу IP, натиснувши кнопку пошуку та використавши спеціальний вираз `not ip`:



8. Додав стовпчик Host іншим способом. Для цього відфільтрував пакети, які відповідають HTTP-запитам, ввівши у поле фільтрування вираз `http.request`, розгорнувши інформацію Hypertext Transfer Protocol в області “Ієрархічний вміст пакета” та вибравши з контекстного меню рядка Host команду Зробити Колонкою:



9. Проєкспериментував з виразами та описав, які критерії пошуку вони задають:

```
ip.addr == 192.168.0.227
```

```
ftp || arp || udp.port == 53
```

```
ipv6.addr == 2001:db8::1
```

```
eth.addr == 00:00:5e:00:53:00
```

```
ip.src != 192.168.0.107
```

```
tcp && ip.dst == 192.168.0.107
```

```
http && ftp && arp
```

Пакети відправлені з мого локального IP або отримані ним:

Wireshark capture showing traffic filtered by `ip.addr == 192.168.0.227`. The packet list shows multiple QUIC and TCP packets. Packet 240 is highlighted, showing a TCP Reset (RST) from 192.168.0.227 to 192.168.0.107.

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
235	6.047648	142.250.180.238	192.168.0.227	QUIC	995			Protected Payload (KP0)
236	6.047648	142.250.180.238	192.168.0.227	QUIC	72			Protected Payload (KP0)
237	6.047849	192.168.0.227	142.250.180.238	QUIC	120			Handshake, DCID=eb73da882465562d
238	6.047888	192.168.0.227	142.250.180.238	QUIC	73			Protected Payload (KP0), DCID=eb73da882465562d
239	6.047979	192.168.0.227	142.250.180.238	QUIC	1064			Protected Payload (KP0), DCID=eb73da882465562d
240	6.049063	142.250.180.202	192.168.0.227	QUIC	67			Protected Payload (KP0)
241	6.051922	142.250.180.227	192.168.0.227	QUIC	66			Protected Payload (KP0)
242	6.051922	142.250.180.238	192.168.0.227	QUIC	66			Protected Payload (KP0)
243	6.051993	142.251.208.110	192.168.0.227	QUIC	71			Protected Payload (KP0)
244	6.051993	142.251.208.110	192.168.0.227	QUIC	67			Protected Payload (KP0)
245	6.051993	142.251.208.110	192.168.0.227	QUIC	71			Protected Payload (KP0)
246	6.052111	192.168.0.227	142.251.208.110	QUIC	73			Protected Payload (KP0), DCID=e7d96572e30137d5
247	6.052551	142.251.208.110	192.168.0.227	QUIC	71			Protected Payload (KP0)
248	6.052551	212.111.192.246	192.168.0.227	TCP	54			80 → 59538 [ACK] Seq=1 Ack=657 Win=131328 Len=0
249	6.052551	142.251.208.110	192.168.0.227	QUIC	67			Protected Payload (KP0)
250	6.052614	192.168.0.227	142.251.208.110	QUIC	73			Protected Payload (KP0), DCID=e7d96572e30137d5
251	6.054674	142.251.208.110	192.168.0.227	QUIC	71			Protected Payload (KP0)
252	6.054674	142.251.208.110	192.168.0.227	QUIC	67			Protected Payload (KP0)
253	6.055434	142.251.208.110	192.168.0.227	QUIC	71			Protected Payload (KP0)
254	6.055434	142.251.208.110	192.168.0.227	QUIC	67			Protected Payload (KP0)
255	6.055434	142.251.208.110	192.168.0.227	QUIC	71			Protected Payload (KP0)
256	6.055434	142.251.208.110	192.168.0.227	QUIC	71			Protected Payload (KP0)

Frame 240: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF\_{2F28D9CB-5... Ethernet II, Src: TPLink\_12:26:03 (98:25:4a:12:26:03), Dst: LiteonTechno\_41:8f:41 (d0:39:57:41:8f:41) Internet Protocol Version 4, Src: 142.250.180.202, Dst: 192.168.0.227 User Datagram Protocol, Src Port: 443, Dst Port: 58888 QUIC IETF

Пакети відправлені протоколом ARP або через UDP порт 53:

Wireshark capture showing traffic filtered by `ftp || arp || udp.port == 53`. The packet list shows ARP and DNS packets. Packet 61 is highlighted, showing an ARP request from 192.168.0.227 to Broadcast.

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
61	5.947174	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.227? Tell 192.168.0.1
62	5.947187	LiteonTechno_41:8f:...	TPLink_12:26:03	ARP	42			192.168.0.227 is at d0:39:57:41:8f:41
589	9.484463	192.168.0.227	192.168.0.1	DNS	83			Standard query 0xf0a2 A www.msftconnecttest.com
590	9.489256	192.168.0.1	192.168.0.227	DNS	227			Standard query response 0xf0a2 A www.msftconnecttest.com
723	14.959612	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.152? Tell 192.168.0.1
772	15.982506	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.152? Tell 192.168.0.1
3201	17.014238	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.152? Tell 192.168.0.1
7165	34.012762	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.152? Tell 192.168.0.1
7613	35.029798	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.152? Tell 192.168.0.1
15064	64.010099	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.152? Tell 192.168.0.1
15065	65.032850	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.152? Tell 192.168.0.1
15159	69.028451	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.147? Tell 192.168.0.1
15173	70.050341	TPLink_12:26:03	Broadcast	ARP	42			Who has 192.168.0.147? Tell 192.168.0.1

Frame 61: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{2F28D9CB-5... Ethernet II, Src: TPLink\_12:26:03 (98:25:4a:12:26:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff) Address Resolution Protocol (request)



## Пакети відправлені або отримані фізичною адресою мого адаптеру:

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
34	1.318673	172.217.19.110	192.168.0.227	UDP	72			443 → 53822 Len=30
35	1.333443	172.217.19.110	192.168.0.227	UDP	73			443 → 53822 Len=31
36	1.333829	192.168.0.227	172.217.19.110	UDP	74			53822 → 443 Len=32
37	1.342317	172.217.19.110	192.168.0.227	UDP	72			443 → 53822 Len=30
38	1.351986	192.168.0.227	172.217.19.110	UDP	75			53822 → 443 Len=33
39	1.366012	172.217.19.110	192.168.0.227	UDP	713			443 → 53822 Len=671
40	1.366012	172.217.19.110	192.168.0.227	UDP	66			443 → 53822 Len=24
41	1.384376	192.168.0.227	172.217.19.110	UDP	79			53822 → 443 Len=37
42	1.425448	172.217.19.110	192.168.0.227	UDP	68			443 → 53822 Len=26
43	1.866844	140.82.113.25	192.168.0.227	TLSv1.2	80			Application Data
44	1.867162	192.168.0.227	140.82.113.25	TLSv1.2	84			Application Data
45	1.976310	140.82.113.25	192.168.0.227	TCP	54			443 → 50872 [ACK] Seq=27 Ack=31 Win=74 Len=0
46	2.599142	192.168.0.227	140.82.113.25	TLSv1.2	242			Application Data
47	2.688290	192.168.0.227	140.82.113.25	TLSv1.2	84			Application Data
48	2.688412	192.168.0.227	140.82.113.25	TCP	54			50872 → 443 [FIN, ACK] Seq=249 Ack=27 Win=251 Len=0
49	2.709629	140.82.113.25	192.168.0.227	TCP	54			443 → 50872 [ACK] Seq=27 Ack=219 Win=77 Len=0
50	2.710331	140.82.113.25	192.168.0.227	TLSv1.2	127			Application Data
51	2.710365	192.168.0.227	140.82.113.25	TCP	54			50872 → 443 [ACK] Seq=250 Ack=100 Win=0 Len=0
52	2.718494	140.82.113.25	192.168.0.227	TLSv1.2	78			Application Data
53	2.718541	140.82.113.25	192.168.0.227	TCP	54			443 → 50872 [FIN, ACK] Seq=124 Ack=250 Win=77 Len=0
54	5.859702	192.168.0.227	212.111.192.246	TCP	66			59538 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
55	5.871396	212.111.192.246	192.168.0.227	TCP	66			80 → 59538 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM

Frame 47: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF\_{2F28D9C8-51AC-420...}

Ethernet II, Src: LiteonTechno\_41:8f:41 (d0:39:57:41:8f:41), Dst: TPLink\_12:26:03 (98:25:4a:12:26:03)

Destination: TPLink\_12:26:03 (98:25:4a:12:26:03)

Source: LiteonTechno\_41:8f:41 (d0:39:57:41:8f:41)

Type: IPv4 (0x0800)

[Stream index: 1]

Internet Protocol Version 4, Src: 192.168.0.227, Dst: 140.82.113.25

Transmission Control Protocol, Src Port: 50872, Dst Port: 443, Seq: 219, Ack: 27, Len: 30

Transport Layer Security

## Пакети відправлені з мого локального IP:

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
1	0.000000	192.168.0.227	212.111.192.246	TCP	54			60368 → 80 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
2	0.272449	fe80::ffff:ffff:ffff:ff02::12		ICMPv6	103			Router Solicitation
4	0.595318	192.168.0.227	142.250.180.206	UDP	1288			55393 → 443 Len=1246
5	0.595715	192.168.0.227	142.250.180.206	UDP	1292			55393 → 443 Len=1250
6	0.595811	192.168.0.227	142.250.180.206	UDP	1253			55393 → 443 Len=1211
9	0.658959	192.168.0.227	142.250.180.206	UDP	73			55393 → 443 Len=31
12	0.693531	192.168.0.227	142.250.180.206	UDP	77			55393 → 443 Len=35
13	0.695757	192.168.0.227	192.168.0.1	TCP	66			49383 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
14	0.696072	192.168.0.227	192.168.0.1	TCP	66			54594 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
17	0.700438	192.168.0.227	192.168.0.1	TCP	54			49383 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
18	0.700454	192.168.0.227	192.168.0.1	TCP	54			54594 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
19	0.700818	192.168.0.227	192.168.0.1	TCP	56			54594 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 20]
20	0.700933	192.168.0.227	192.168.0.1	DNS	88			Standard query 0x815f HTTPS beacons.gvt2.com
21	0.701048	192.168.0.227	192.168.0.1	TCP	56			49383 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 22]
22	0.701089	192.168.0.227	192.168.0.1	DNS	88			Standard query 0x8e85 A beacons.gvt2.com
27	0.705134	192.168.0.227	192.168.0.1	TCP	54			54594 → 53 [FIN, ACK] Seq=37 Ack=94 Win=65280 Len=0
28	0.705941	192.168.0.227	192.168.0.1	TCP	54			49383 → 53 [FIN, ACK] Seq=37 Ack=53 Win=65280 Len=0
29	0.707230	192.168.0.227	142.251.208.131	QUIC	1292			Initial, DCID=70bd9b0195a1f6, PKN: 1, CRYPTO, PING, PADDING, PING, CRYPTO, CRYPTO, PING,
30	0.707369	192.168.0.227	142.251.208.131	QUIC	1292			Initial, DCID=70bd9b0195a1f6, PKN: 2, PING, PING, PING, CRYPTO, CRYPTO, PING, CR
31	0.707667	192.168.0.227	142.251.208.131	QUIC	118			0-RTT, DCID=70bd9b0195a1f6
35	0.709740	192.168.0.227	192.168.0.1	TCP	54			54594 → 53 [ACK] Seq=38 Ack=95 Win=65280 Len=0
37	0.709783	192.168.0.227	192.168.0.1	TCP	54			49383 → 53 [ACK] Seq=38 Ack=54 Win=65280 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{2F28D9C8-51AC-4208...}

Ethernet II, Src: LiteonTechno\_41:8f:41 (d0:39:57:41:8f:41), Dst: TPLink\_12:26:03 (98:25:4a:12:26:03)

Internet Protocol Version 4, Src: 192.168.0.227, Dst: 212.111.192.246

Transmission Control Protocol, Src Port: 60368, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

## Пакети http, ftp та arp:

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
1	0.000000	192.168.0.227	192.168.0.1	ARP	42			Request to resolve 192.168.0.1 to MAC address
2	0.000000	192.168.0.1	192.168.0.227	ARP	42			Reply to resolve 192.168.0.227 to MAC address
3	0.000000	192.168.0.227	192.168.0.1	HTTP	100			GET / HTTP/1.1
4	0.000000	192.168.0.1	192.168.0.227	FTP	100			220 Ready for new user

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{2F28D9C8-51AC-4208...}

Ethernet II, Src: LiteonTechno\_41:8f:41 (d0:39:57:41:8f:41), Dst: TPLink\_12:26:03 (98:25:4a:12:26:03)

Internet Protocol Version 4, Src: 192.168.0.227, Dst: 192.168.0.1

ARP, Operation: Request, Src MAC: d0:39:57:41:8f:41, Dst MAC: 00:00:00:00:00:00, Dst IP: 192.168.0.1

Wi-Fi
Файл Правка Видял Перехід Заволення Аналіз Статистика Телефонія Wireless Інструменти Довідка

ip.dst == 192.168.0.227

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
64	5.972816	142.251.208.110	192.168.0.227	QUIC	82			Initial, SCID=e7d96572e30137d5, PKN: 2, ACK
65	5.984015	142.251.208.110	192.168.0.227	QUIC	1292			Initial, SCID=e7d96572e30137d5, PKN: 3, ACK, PADDING
66	5.984015	142.251.208.110	192.168.0.227	QUIC	1292			Initial, SCID=e7d96572e30137d5, PKN: 4, ACK, PADDING
86	5.997336	142.251.208.110	192.168.0.227	QUIC	1292			Initial, SCID=e7d96572e30137d5, PKN: 5, CRYPTO, PADDING
87	5.997336	142.251.208.110	192.168.0.227	QUIC	344			Protected Payload (KP0)
88	5.997336	142.251.208.110	192.168.0.227	QUIC	986			Protected Payload (KP0)
89	5.997336	192.168.0.1	192.168.0.227	TCP	66			53 → 55153 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PER
90	5.997336	192.168.0.1	192.168.0.227	TCP	66			53 → 61386 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PER
103	5.998207	142.251.208.110	192.168.0.227	QUIC	67			Protected Payload (KP0)
114	6.004817	212.111.192.246	192.168.0.227	TCP	66			80 → 59523 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PER
115	6.004817	192.168.0.1	192.168.0.227	TCP	54			53 → 55153 [ACK] Seq=1 Ack=41 Win=65792 Len=0
135	6.005582	192.168.0.1	192.168.0.227	TCP	54			53 → 61386 [ACK] Seq=1 Ack=41 Win=65792 Len=0
136	6.005602	192.168.0.1	192.168.0.227	DNS	167			Standard query response 0xb348 HTTPS cdnjs.cloudflare.com HTTPS
137	6.005602	192.168.0.1	192.168.0.227	DNS	126			Standard query response 0xf914 A cdnjs.cloudflare.com A 104.17.25.14 A 10
140	6.012481	192.168.0.1	192.168.0.227	TCP	54			53 → 55153 [ACK] Seq=114 Ack=42 Win=65792 Len=0
141	6.013254	192.168.0.1	192.168.0.227	TCP	54			53 → 61386 [ACK] Seq=73 Ack=42 Win=65792 Len=0
142	6.013254	192.168.0.1	192.168.0.227	TCP	54			53 → 55153 [FIN, ACK] Seq=114 Ack=42 Win=65792 Len=0
143	6.013254	192.168.0.1	192.168.0.227	TCP	54			53 → 61386 [FIN, ACK] Seq=73 Ack=42 Win=65792 Len=0
175	6.028962	142.251.39.42	192.168.0.227	QUIC	82			Initial, SCID=fa920a909041596d, PKN: 1, ACK
176	6.028962	142.251.39.42	192.168.0.227	QUIC	82			Initial, SCID=fa920a909041596d, PKN: 2, ACK
177	6.028962	142.251.39.42	192.168.0.227	QUIC	1292			Initial, SCID=fa920a909041596d, PKN: 3, ACK, PADDING
178	6.028962	142.251.39.42	192.168.0.227	QUIC	1292			Initial, SCID=fa920a909041596d, PKN: 4, ACK, PADDING

Frame 45: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{2F2809CB-51AC-420} 0000 d0 38 57 41 8f 41 98 25 4a 12 26 03 08 00 45 48 9NA A % J & . - EH

Ethernet II, Src: TPLink 12:26:03 (98:25:4a:12:26:03), Dst: LiteonTechno 41:8f:41 (d0:39:57:41:8f:41) 0010 00 28 d0 26 40 00 24 06 b2 6a 8c 52 71 19 c0 80 (.) @ - - j Rq .

Destination: LiteonTechno 41:8f:41 (d0:39:57:41:8f:41) 0020 00 e3 01 bb c6 b8 41 00 60 a9 cc 67 ac c2 50 10 00 00 A . . . g P

Source: TPLink 12:26:03 (98:25:4a:12:26:03) 0030 00 4a d0 4c 00 00 00 00 00 00 00 00 00 00 00 J L .

Type: IPv4 (0x0800)

[Stream index: 1]

Internet Protocol Version 4, Src: 140.82.113.25, Dst: 192.168.0.227

Transmission Control Protocol, Src Port: 443, Dst Port: 50872, Seq: 27, Ack: 31, Len: 0

**\*Wi-Fi**

Файл Правка Видгал Перехід Заполнення Аналіз Статистика Телефонія Wireless Інструменти Довідка

ip.src != 192.168.0.227

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Host	Info
21	1.237676	172.217.19.110	192.168.0.227	UDP	72			443 → 53822 Len=30
23	1.263755	172.217.19.110	192.168.0.227	UDP	112			443 → 53822 Len=70
24	1.266851	172.217.19.110	192.168.0.227	UDP	65			443 → 53822 Len=23
25	1.268441	172.217.19.110	192.168.0.227	UDP	81			443 → 53822 Len=39
34	1.318673	172.217.19.110	192.168.0.227	UDP	72			443 → 53822 Len=30
35	1.333443	172.217.19.110	192.168.0.227	UDP	73			443 → 53822 Len=31
37	1.342317	172.217.19.110	192.168.0.227	UDP	72			443 → 53822 Len=30
39	1.366012	172.217.19.110	192.168.0.227	UDP	713			443 → 53822 Len=671
40	1.366012	172.217.19.110	192.168.0.227	UDP	66			443 → 53822 Len=24
42	1.425448	172.217.19.110	192.168.0.227	UDP	68			443 → 53822 Len=26
43	1.866844	140.82.113.25	192.168.0.227	TLSv1.2	80			Application Data
45	1.976310	140.82.113.25	192.168.0.227	TCP	54			443 → 50872 [ACK] Seq=27 Ack=31 Win=74 Len=0
49	2.709629	140.82.113.25	192.168.0.227	TCP	54			443 → 50872 [ACK] Seq=27 Ack=219 Win=77 Len=0
50	2.710331	140.82.113.25	192.168.0.227	TLSv1.2	127			Application Data
52	2.718494	140.82.113.25	192.168.0.227	TLSv1.2	78			Application Data
53	2.718541	140.82.113.25	192.168.0.227	TCP	54			443 → 50872 [FIN, ACK] Seq=124 Ack=250 Win=77 Len=0
55	5.871396	212.111.192.246	192.168.0.227	TCP	66			80 → 59538 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK Initial, SCID=e7d96572e30137d5, PKM: 1, ACK
63	5.972816	142.251.208.110	192.168.0.227	QUIC	82			Initial, SCID=e7d96572e30137d5, PKM: 2, ACK
64	5.972816	142.251.208.110	192.168.0.227	QUIC	1292			Initial, SCID=e7d96572e30137d5, PKM: 3, ACK, PADDING
65	5.984015	142.251.208.110	192.168.0.227	QUIC	1292			Initial, SCID=e7d96572e30137d5, PKM: 4, ACK, PADDING
86	5.997336	142.251.208.110	192.168.0.227	QUIC	1292			Initial, SCID=e7d96572e30137d5, PKM: 5, CRYPTO, PADDING

```

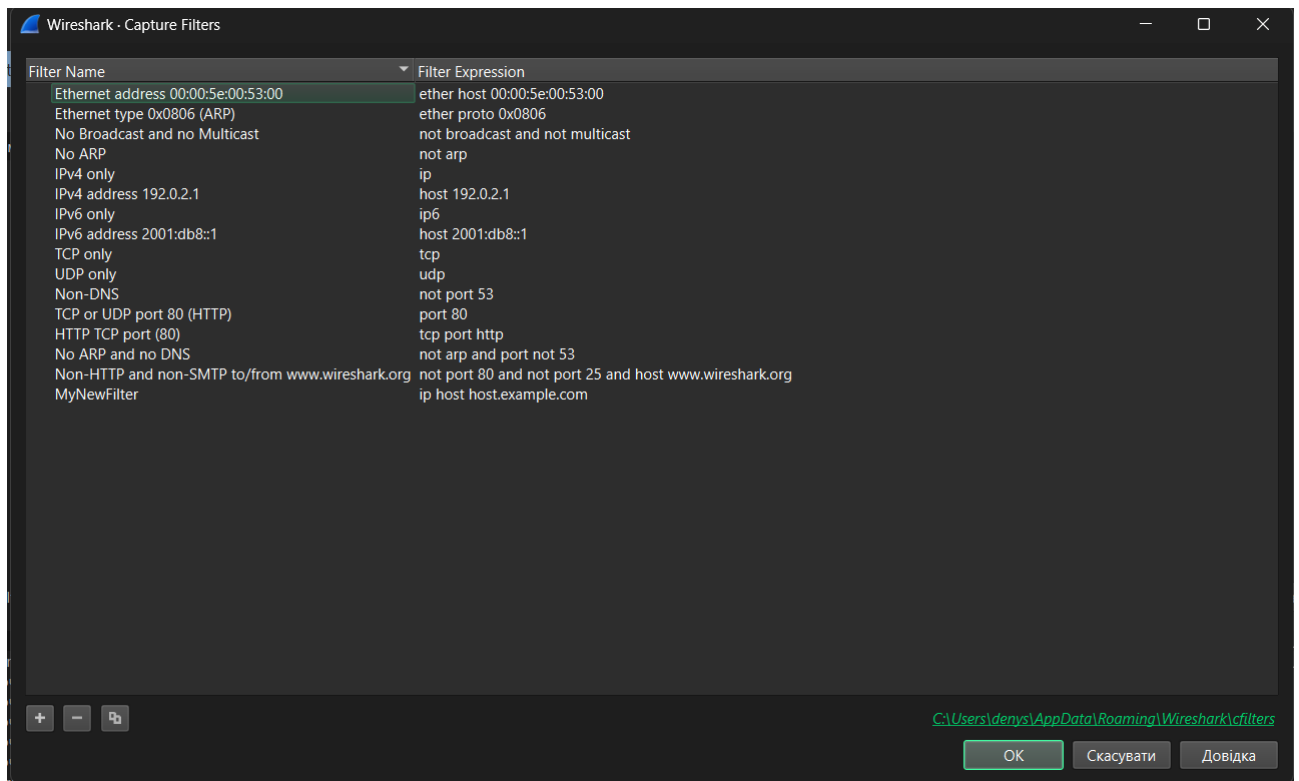
Frame 45: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device{NPF_{2F28D9CB-51AC-420}
Ethernet II, Src: TPLink_12:26:B3 (98:25:4a:12:26:b3), Dst: LiteonTechno_41:8f:41 (d0:39:57:41:8f:41)
    Destination: LiteonTechno_41:8f:41 (d0:39:57:41:8f:41)
    Source: TPLink_12:26:B3 (98:25:4a:12:26:b3)
    Type: IPv4 (0x0800)
        [Stream index: 1]
    Internet Protocol Version 4, Src: 140.82.113.25, Dst: 192.168.0.227
    Transmission Control Protocol, Src Port: 443, Dst Port: 50872, Seq: 27, Ack: 31, Len: 0
  
```

```

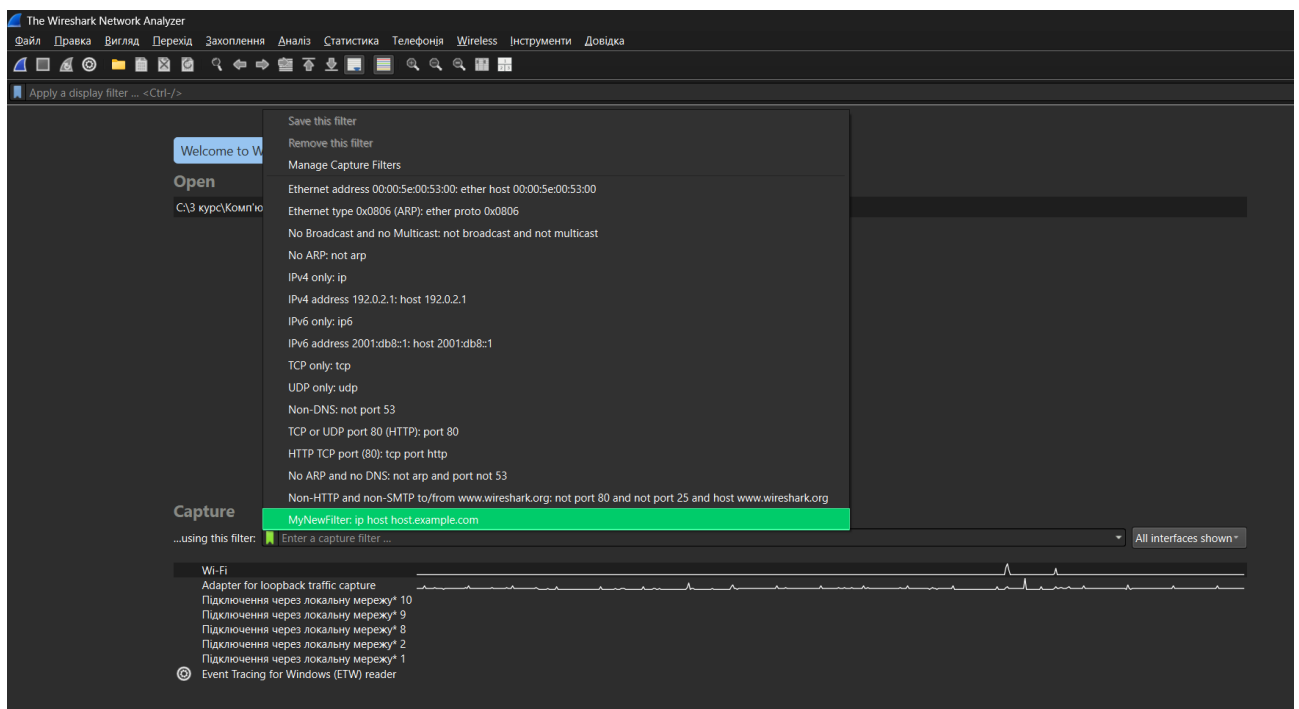
0000  d0 39 57 41 8f 41 98 25 4a 12 26 03 08 00 45 48   9NA A % j R . EH
0010  00 28 dc 26 40 00 2d 06 b2 6a 8c 52 71 f9 c0 a8   ( & - j Rq .
0020  00 e3 01 bb c6 8b 41 00 60 a9 cc 67 ac c2 50 10   ... A ` g P
0030  00 4a 0d 4c 00 00                                J L :
  
```



10. Ознайомився з переліком фільтрів за замовчуванням, виконавши команду Захоплення → Фільтри Захоплення...:

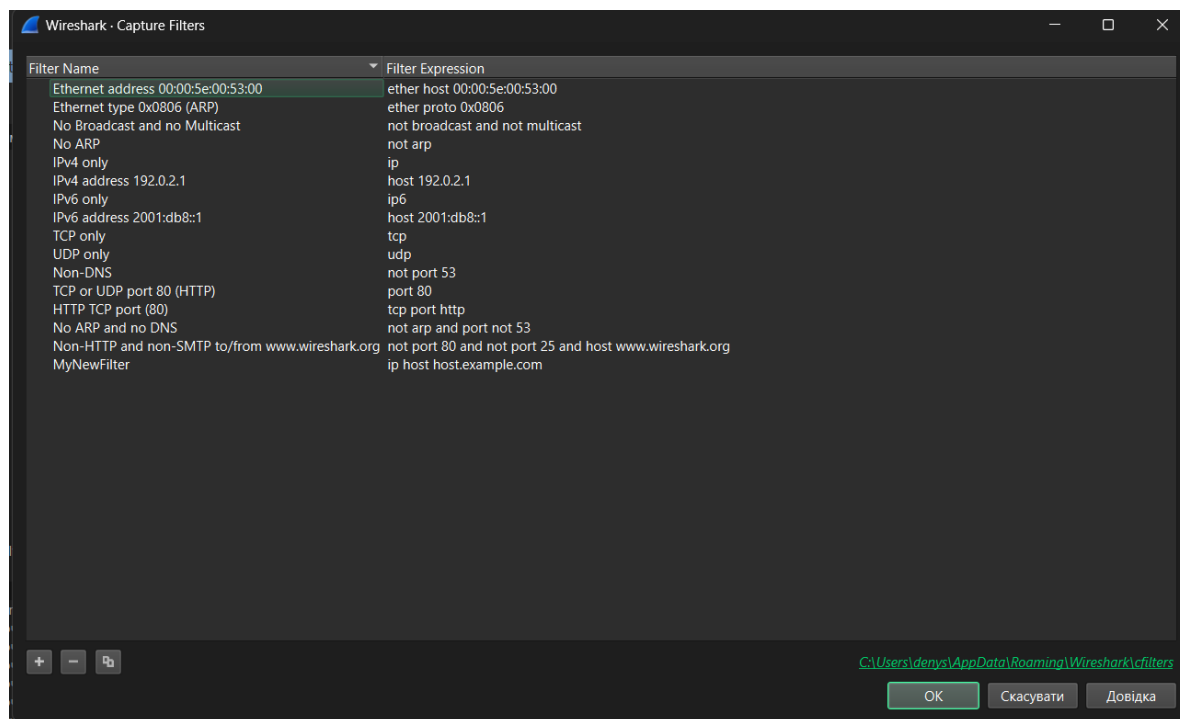


11. Створив власний фільтр і захопив пакети з його використанням. Для цього перед захопленням пакетів натиснув на зелену корогу у полі ...using this filter та обрав створений фільтр “MyNewFilter”:

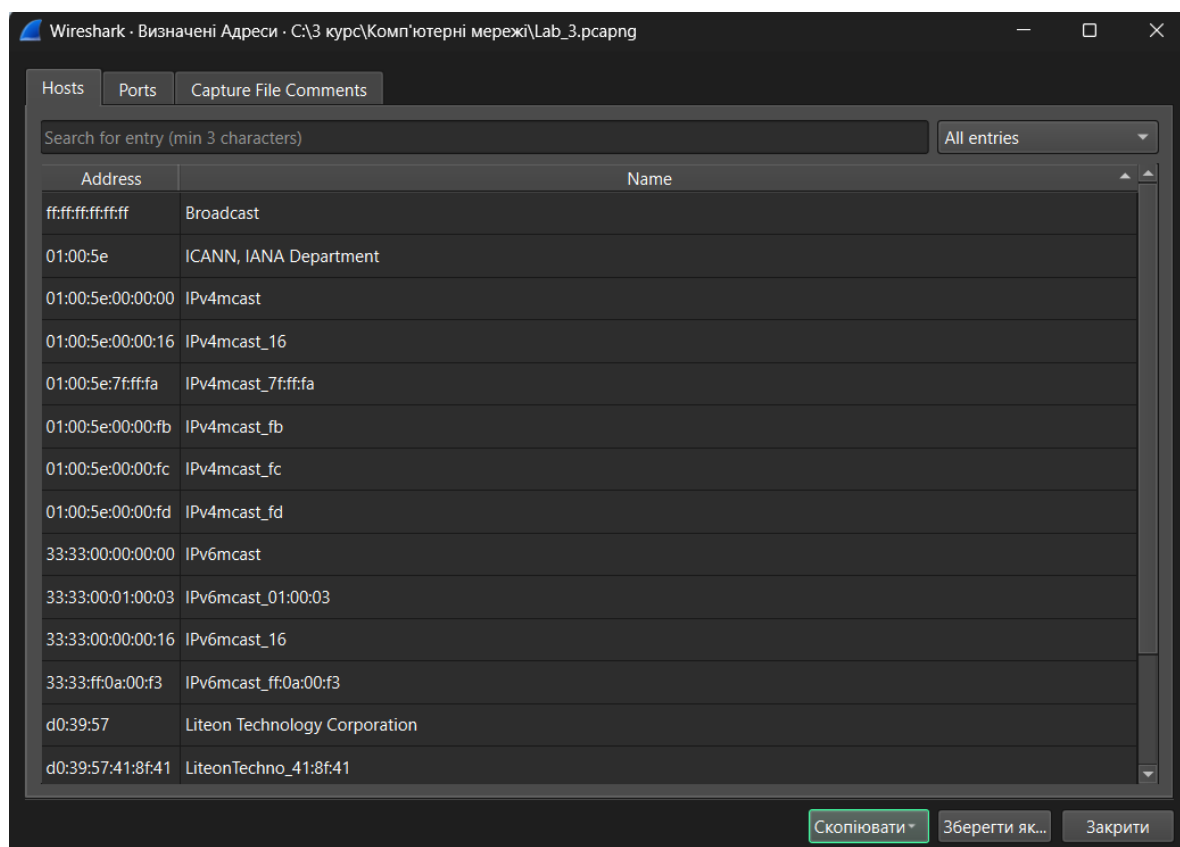


12. У меню Статистика вибрав по черзі пункти Властивості Файлу Захоплення, Визначені Адреси, Ієрархія Протоколів, Conversations, I/O Graph, IPv4 Statistics та ознайомився з інформацією.

Властивості Файлу Захоплення – показує дані про пакети записані у файлі, час, та статистику пакетів:



Визначені Адреси має фізичні адреси, які отримували пакети або відправляли, а також порт та протокол за яким відправлено в другій вкладці:



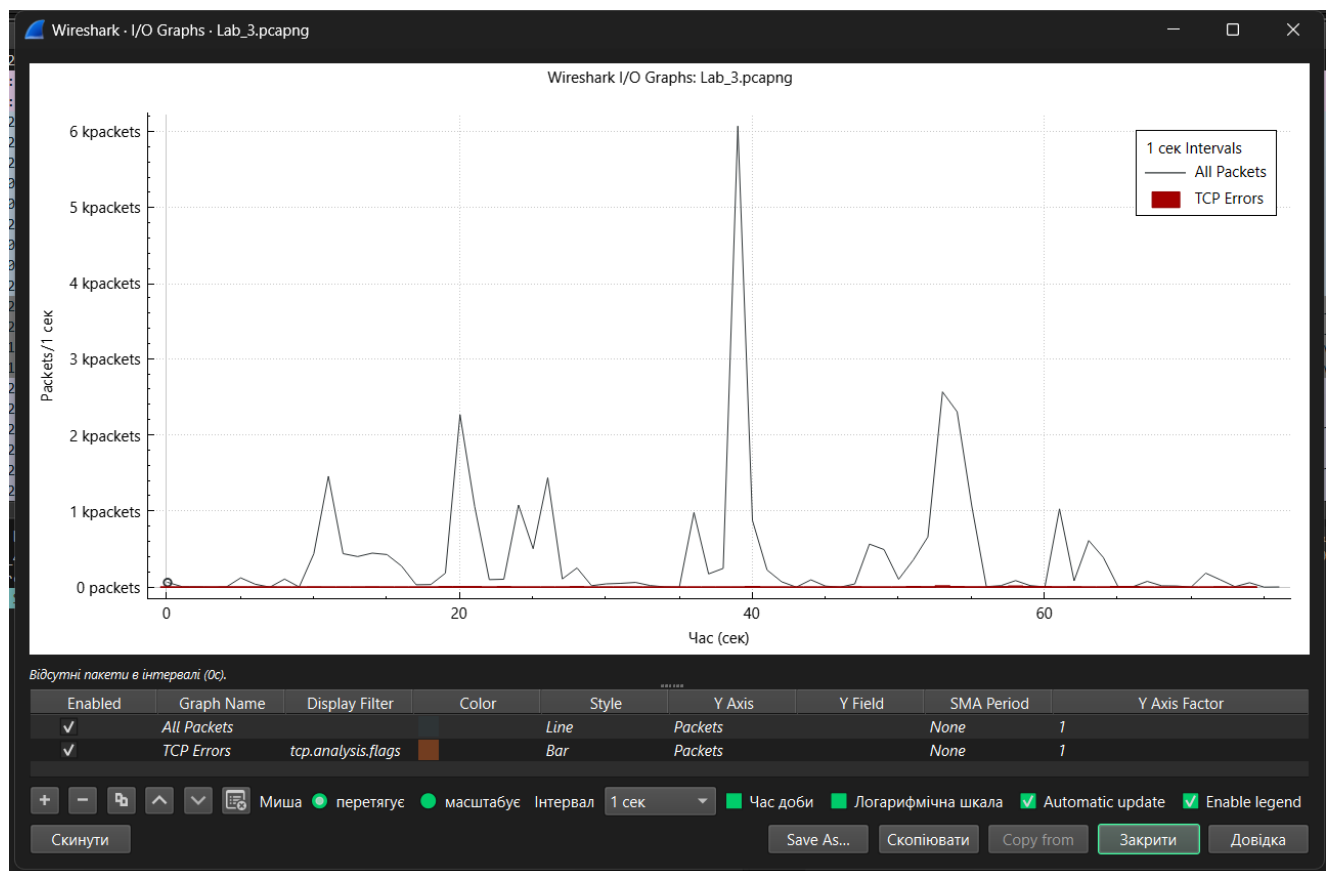
Ієрархія Протоколів показує ієрархію розподілення пакетів по протоколах:

Протокол	Percent Packets	Пакетів	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
Frame	100.0	31351	100.0	55022673	5738 k	0	0	0	31351
Ethernet	100.0	31351	0.8	439052	45 k	0	0	0	31351
Internet Protocol Version 6	0.0	10	0.0	440	45	0	0	0	10
User Datagram Protocol	0.0	2	0.0	16	1	0	0	0	2
Link-local Multicast Name Resolution	0.0	2	0.0	52	5	2	52	5	2
Internet Control Message Protocol v6	0.0	8	0.0	236	24	8	236	24	8
Internet Protocol Version 4	99.9	31326	1.1	626580	65 k	0	0	0	31326
User Datagram Protocol	66.9	20981	0.3	167848	17 k	0	0	0	20981
Teredo IPv6 over UDP tunneling	0.0	7	0.0	550	57	0	0	0	7
Internet Protocol Version 6	0.0	7	0.0	280	29	1	40	4	7
Internet Control Message Protocol v6	0.0	6	0.0	168	17	6	168	17	6
Simple Service Discovery Protocol	0.0	9	0.0	2805	292	9	2805	292	9
QUIC IETF	39.5	12394	19.7	10855552	1132 k	12394	10823813	1128 k	12510
Link-local Multicast Name Resolution	0.0	2	0.0	52	5	2	52	5	2
HiPerConTracer Trace Service	0.0	2	0.0	2500	260	2	2500	260	2
Dynamic Host Configuration Protocol	0.0	2	0.0	850	88	2	850	88	2
Domain Name System	0.0	2	0.0	250	26	2	250	26	2
Data	27.3	8563	14.5	8005187	834 k	8563	8005187	834 k	8563
Transmission Control Protocol	32.9	10330	0.4	215464	22 k	4946	103416	10 k	10330
Transport Layer Security	16.3	5120	59.7	32873142	3428 k	5120	30771454	3208 k	6610
Hypertext Transfer Protocol	0.1	28	0.0	14243	1485	14	8910	929	28
Portable Network Graphics	0.0	5	2.7	1467926	153 k	5	1467926	153 k	5
Line-based text data	0.0	6	1.5	812511	84 k	6	812511	84 k	6
JPEG File Interchange Format	0.0	3	0.8	421241	43 k	3	421241	43 k	3
Domain Name System	0.7	216	0.0	14146	1475	216	14146	1475	216
Data	0.1	20	0.1	75930	7918	20	75930	7918	20
Internet Group Management Protocol	0.0	15	0.0	220	22	15	220	22	15
Address Resolution Protocol	0.0	15	0.0	420	43	15	420	43	15

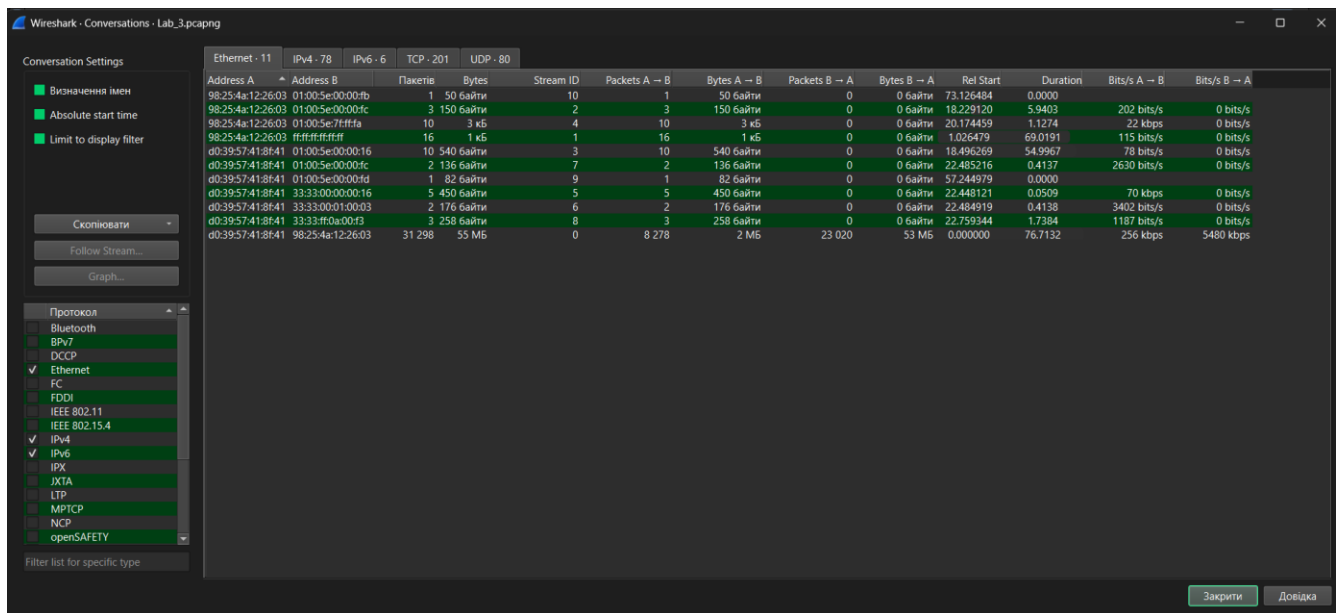
Фільтр відображення відсутній.

Закрити Скопіювати\* Protocols Довідка

I/O Graph - графік отриманих та відправлених пакетів:



Conversations показує сумарні дані передачі даних між фізичними адресами, IP, тощо:



Wireshark - Conversations - Lab\_3.pcapng

Conversation Settings

- ☒ Визначення імен
- ☒ Absolute start time
- ☒ Limit to display filter

Скопіювати

Follow Stream...

Graph...

Протокол

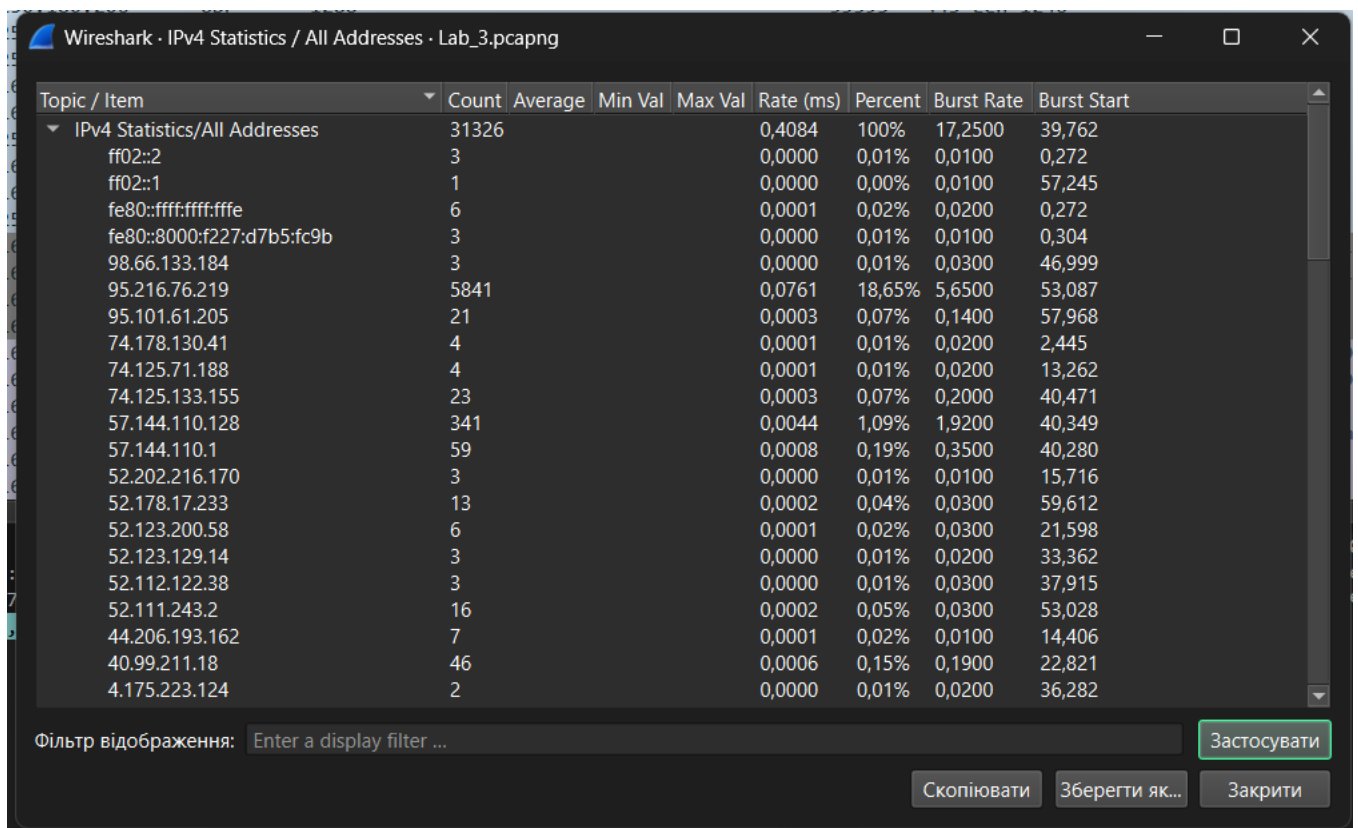
- ☐ Bluetooth
- ☐ BPv7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ JXTA
- ☐ LTP
- ☐ MPTCP
- ☐ NCP
- ☐ openSAFETY

Filter list for specific type

Address A	Address B	Пакети	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
98:25:4a:12:26:03	01:00:5e:00:00:fb	1	50 байти	10	1	50 байти	0	0 байти	73.126484	0.0000		
98:25:4a:12:26:03	01:00:5e:00:00:fc	3	150 байти	2	3	150 байти	0	0 байти	18.229120	5.9403	202 bits/s	0 bits/s
98:25:4a:12:26:03	01:00:5e:7b:ff:fa	10	3 кБ	4	10	3 кБ	0	0 байти	20.174459	1.1274	22 kbps	0 bits/s
98:25:4a:12:26:03	ff:ff:ff:ff:ff:ff	16	1 кБ	1	16	1 кБ	0	0 байти	1.026479	69.0191	115 bits/s	0 bits/s
d0:39:57:41:8f:41	01:00:5e:00:00:16	10	540 байти	3	10	540 байти	0	0 байти	18.496269	54.9967	78 bits/s	0 bits/s
d0:39:57:41:8f:41	01:00:5e:00:00:fc	2	136 байти	7	2	136 байти	0	0 байти	22.485216	0.4137	2630 bits/s	0 bits/s
d0:39:57:41:8f:41	01:00:5e:00:00:fd	1	82 байти	9	1	82 байти	0	0 байти	57.244979	0.0000		
d0:39:57:41:8f:41	33:33:00:00:00:16	5	450 байти	5	5	450 байти	0	0 байти	22.448121	0.0509	70 kbps	0 bits/s
d0:39:57:41:8f:41	33:33:00:01:00:03	2	176 байти	6	2	176 байти	0	0 байти	22.484919	0.4138	3402 bits/s	0 bits/s
d0:39:57:41:8f:41	33:33:fc:0a:00:f3	3	258 байти	8	3	258 байти	0	0 байти	22.759344	1.7384	1187 bits/s	0 bits/s
d0:39:57:41:8f:41	98:25:4a:12:26:03	31 298	53 МБ	0	8 278	2 МБ	23 020	53 МБ	0.000000	76.7132	256 kbps	5480 kbps

Закрити Довідка

IPv4 Statistics показує всі адреси ipv4, які є у файлі та статистичні дані про них:



Wireshark - IPv4 Statistics / All Addresses - Lab\_3.pcapng

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/All Addresses	31326				0,4084	100%	17,2500	39,762
ff02::2	3				0,0000	0,01%	0,0100	0,272
ff02::1	1				0,0000	0,00%	0,0100	57,245
fe80::ffff:ffff:ffff	6				0,0001	0,02%	0,0200	0,272
fe80::8000:f227:d7b5:fc9b	3				0,0000	0,01%	0,0100	0,304
98.66.133.184	3				0,0000	0,01%	0,0300	46,999
95.216.76.219	5841				0,0761	18,65%	5,6500	53,087
95.101.61.205	21				0,0003	0,07%	0,1400	57,968
74.178.130.41	4				0,0001	0,01%	0,0200	2,445
74.125.71.188	4				0,0001	0,01%	0,0200	13,262
74.125.133.155	23				0,0003	0,07%	0,2000	40,471
57.144.110.128	341				0,0044	1,09%	1,9200	40,349
57.144.110.1	59				0,0008	0,19%	0,3500	40,280
52.202.216.170	3				0,0000	0,01%	0,0100	15,716
52.178.17.233	13				0,0002	0,04%	0,0300	59,612
52.123.200.58	6				0,0001	0,02%	0,0300	21,598
52.123.129.14	3				0,0000	0,01%	0,0200	33,362
52.112.122.38	3				0,0000	0,01%	0,0300	37,915
52.111.243.2	16				0,0002	0,05%	0,0300	53,028
44.206.193.162	7				0,0001	0,02%	0,0100	14,406
40.99.211.18	46				0,0006	0,15%	0,1900	22,821
4.175.223.124	2				0,0000	0,01%	0,0200	36,282

Фільтр відображення: Enter a display filter ...

Застосувати

Скопіювати Зберегти як... Закрити

**Висновок:** Під час виконання лабораторно роботи я отримав знання і практичні навички про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомився з графічним інтерфейсом програми, навчився захоплювати, сортувати та фільтрувати пакети.