

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

**Комп'ютерні інформаційні мережі**

**ЛАБОРАТОРНА РОБОТА №3**

Виконав:

Ст. Лук'янчук Денис

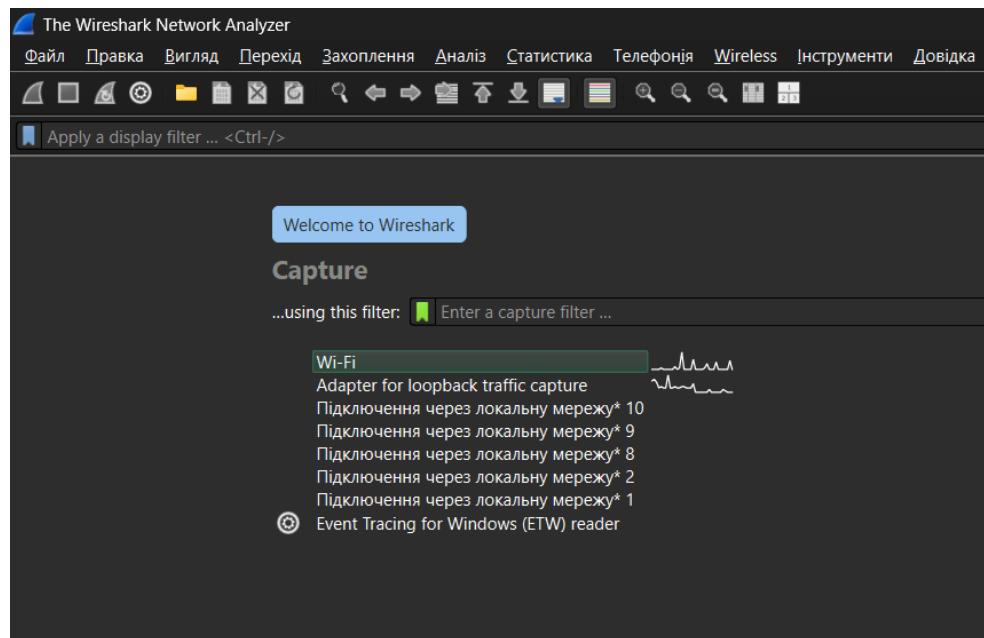
Група ПМі-33

## Тема: “Інтерфейс аналізатора мережевих пакетів Wireshark”

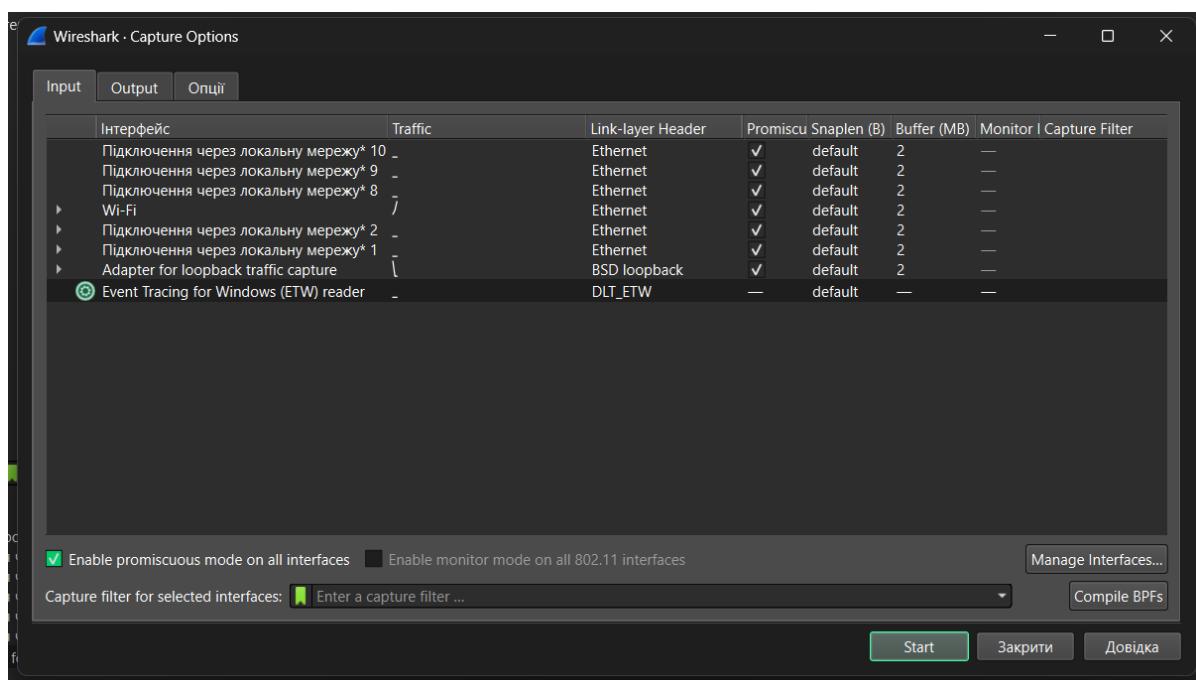
**Мета роботи:** Отримати загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark; ознайомитися з графічним інтерфейсом програми та основними параметрами конфігурації; навчитися захоплювати, сортувати та фільтрувати пакети.

### Хід роботи

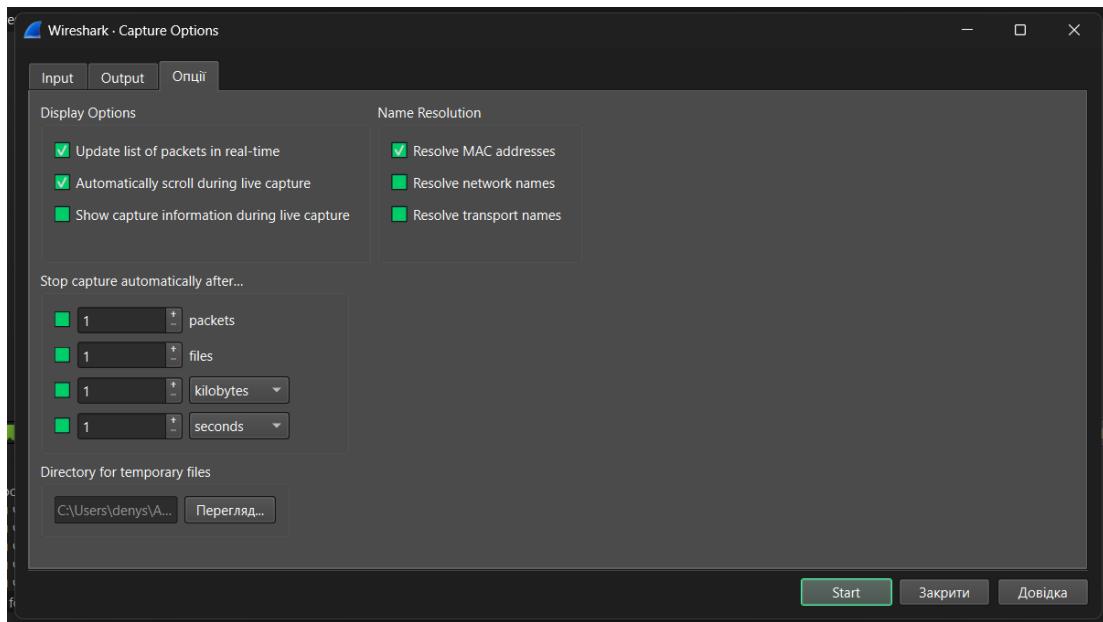
1. Запустив аналізатор мережевих пакетів Wireshark від імені адміністратора. Вибрав з переліку Wi-Fi та почав захоплення:



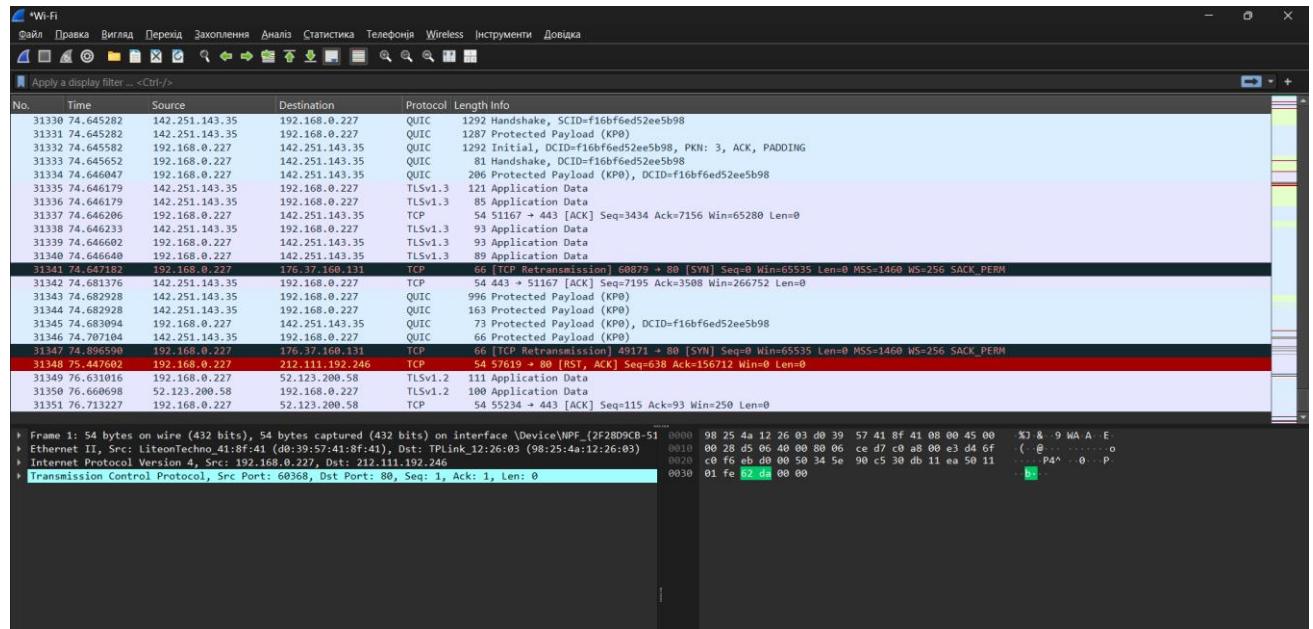
2. Виконав команду Захоплення → Опції, переконався, що мережеві карти (інтерфейси) налаштовані для роботи у нерозбірливому режимі (promiscuous mode):



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



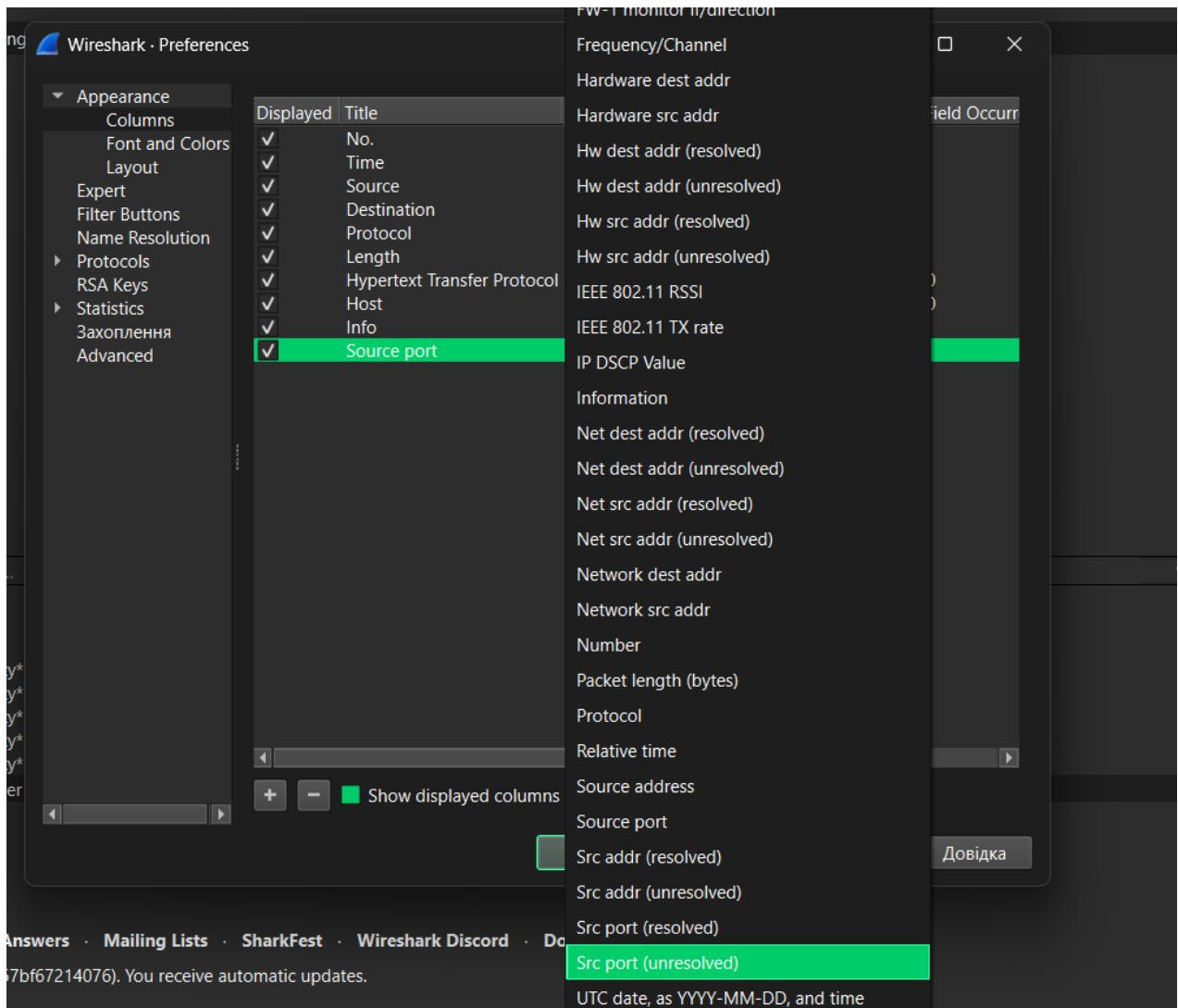
4. Вибрав з переліку Wi-Fi та почав захоплення пакетів. Упродовж 1 хвилини здійснив активність в браузері: перейшов на сайти <http://uac.gov.ua>, завантажив на комп’ютер зображення та різні файли. Зупинив процедуру захоплення пакетів. Ознайомився з трьома основними елементами головного вікна програми:



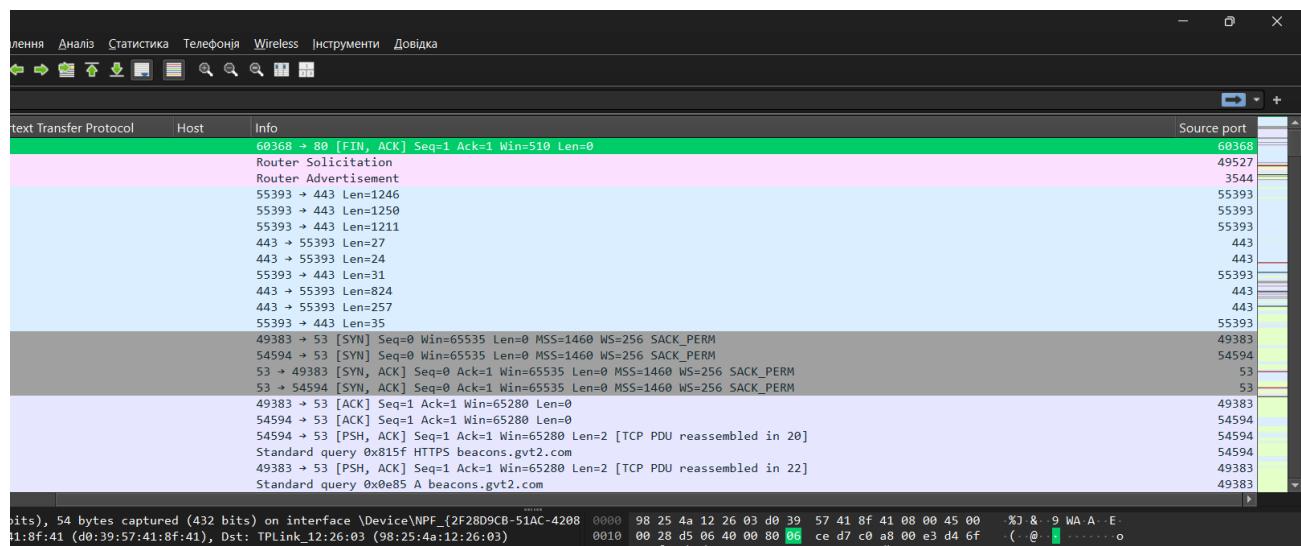
5. Зберіг захоплені пакети у файл для подальшого аналізу:



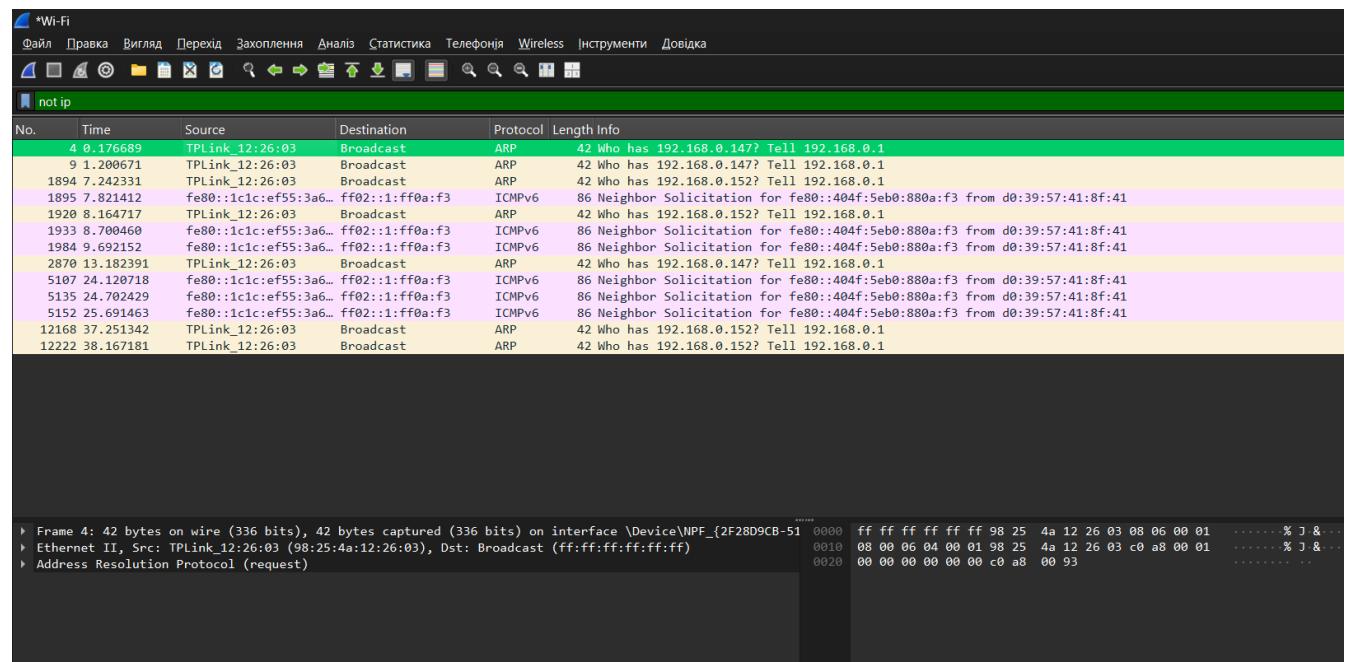
6. Відкрив вікно налаштувань, виконавши команду Правка → Налаштування. Добавив новий стовпчик Source port обравши пункт Columns, натиснув кнопку +, ввів назву стовпчика і тип даних у ньому:



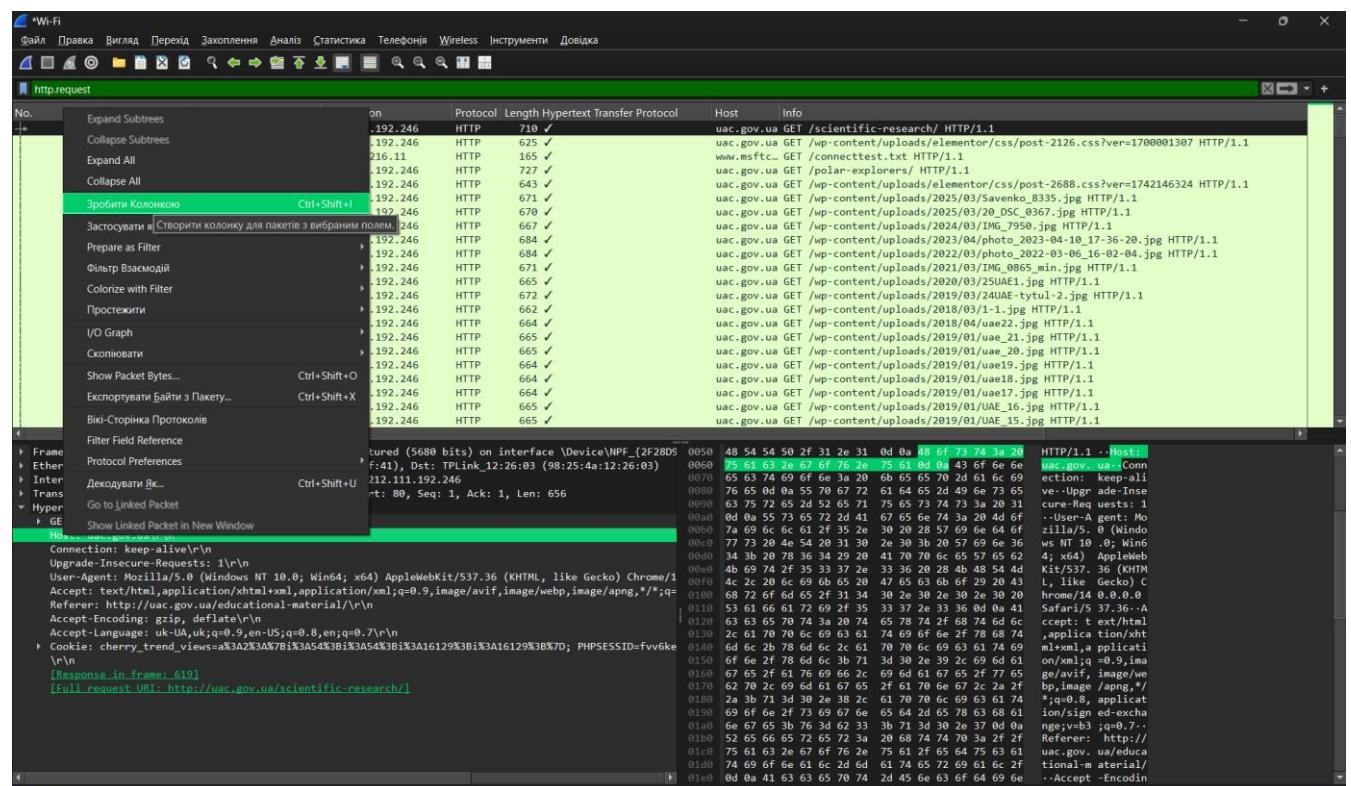
Переконався, що стовпчик з'явився в області “Список пакетів”:



## 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 “Ієархічний вміст пакета” та вибравши з контекстного меню рядка Host команду Зробити Колонкою:



9. Проекспериментував 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 моого локального IP або отримані ним:

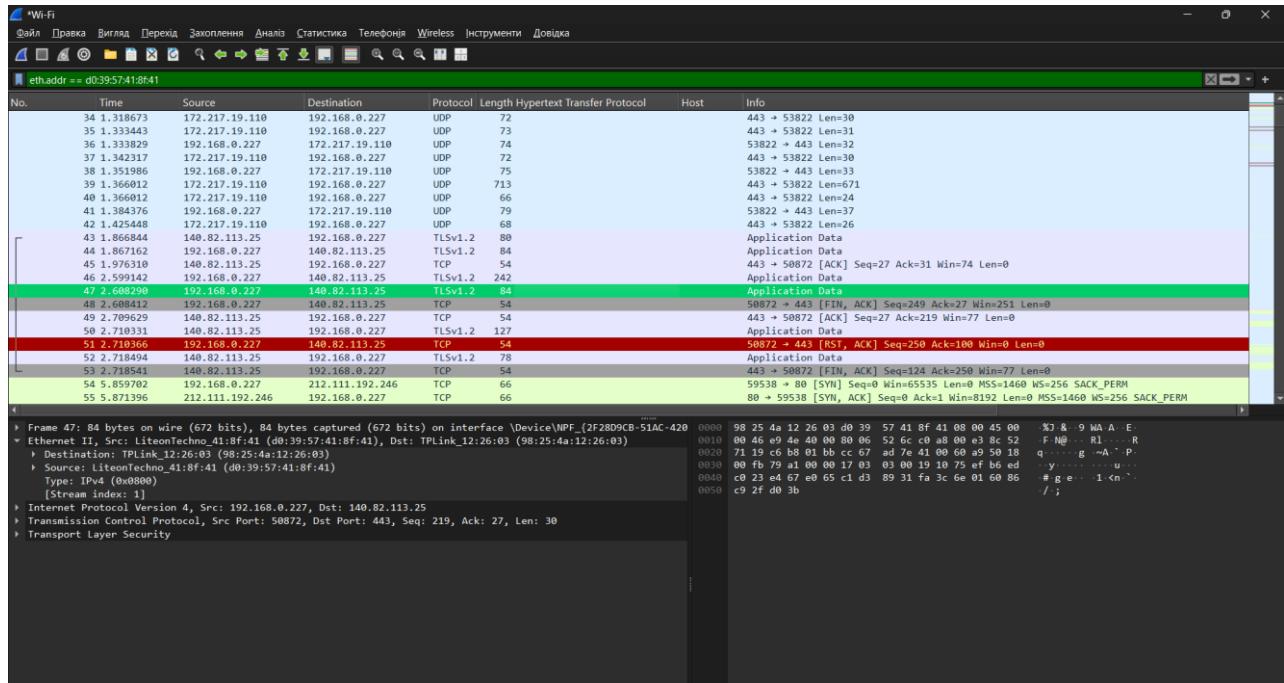
The figure shows a Wireshark capture window with the following details:

- Interface:** \*Wi-Fi
- Selected IP:** ip.addr == 192.168.0.227
- Columns:** No., Time, Source, Destination, Protocol, Length, Hypertext Transfer Protocol, Host, Info
- Packet List:** Shows approximately 250 packets. Many are QUIC (Protocol 995) or TCP (Protocol 6). Sources include 192.168.0.227, 142.250.180.238, 142.250.180.202, etc.
- Selected Packet (Frame 240):**
  - Details:** Src: TPLink\_12:26:03 (98:25:4a:12:26:03), Dst: liteonTechno\_41:8f:41 (d0:39:57:41:8f:41)
  - Hex:** Frame 240: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF\_{2F28D9CB-...}
  - ASCII:** 80 > 59538 [ACK] Seq=1 Ack=657 Win=131328 Len=0

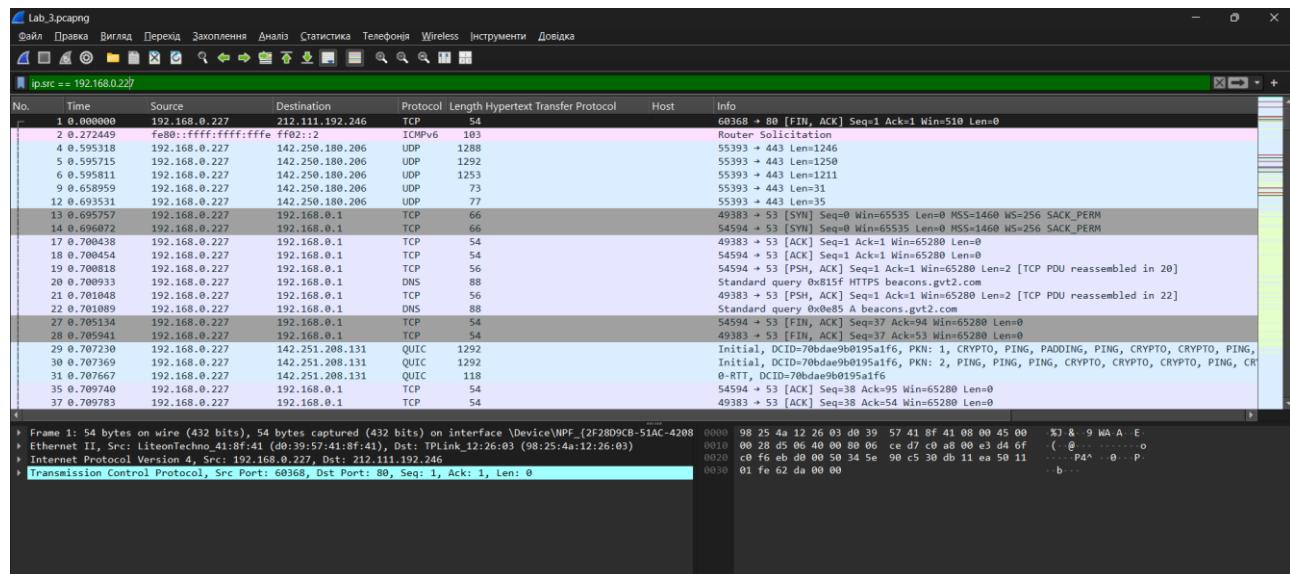
Пакети відправлені протоколом ARP або через UDP порт 53:

| 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.msftconnectte |
| 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 | 64.010899 | 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            |

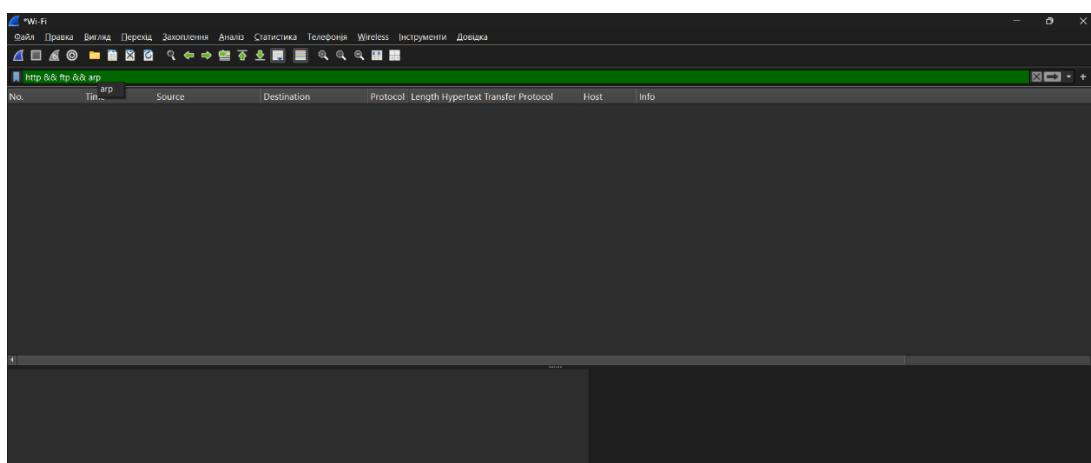
## Пакети відправлені або отримані фізичною адресою моого адаптеру:



## Пакети відправлені з моого локального IP:



## Пакети http, ftp та arp:



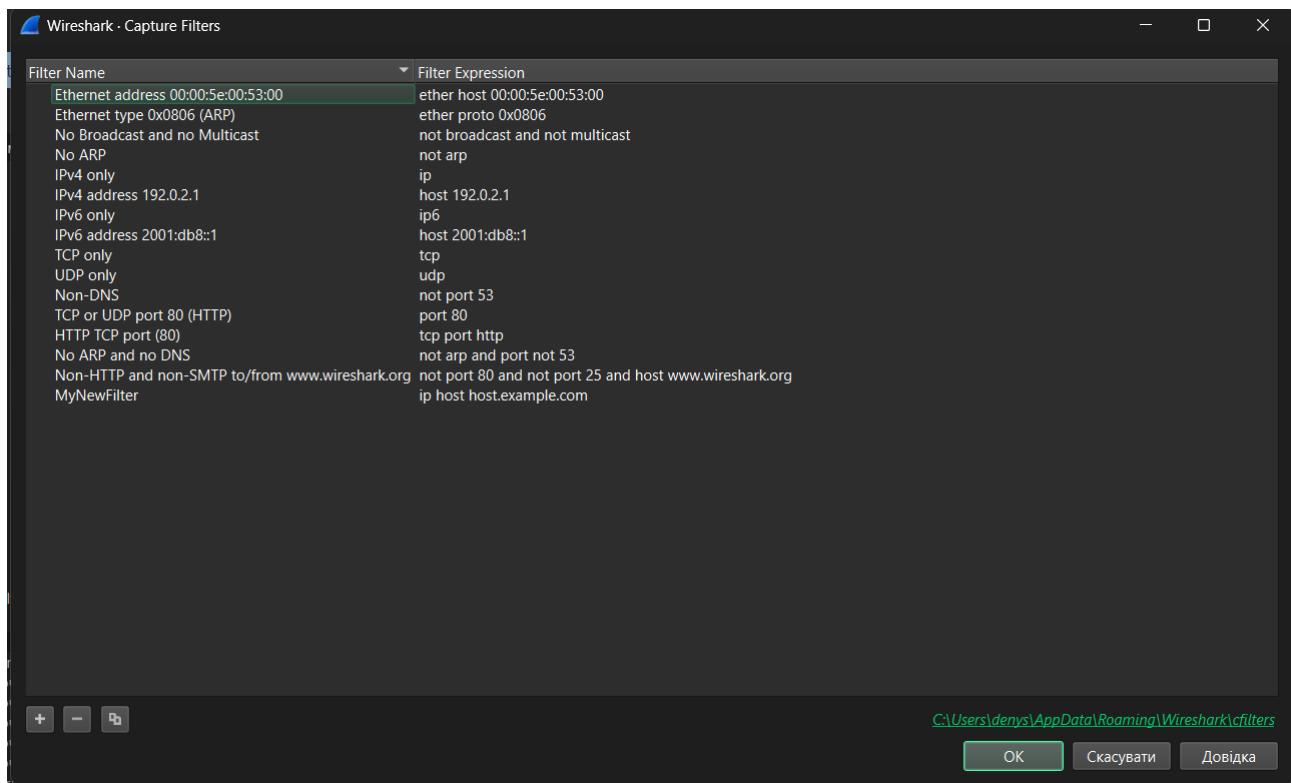
## Пакети отримані моїм локальним IP:

| 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 (KPO)   |
| 88  | 5.997336 | 142.251.208.110 | 192.168.0.227 | QUIC     | 986    |                             |      | Protected Payload (KPO)   |
| 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_PERF         |
| 90  | 5.997336 | 192.168.0.1     | 192.168.0.227 | TCP      | 66     |                             |      | 53 → 61380 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERF         |
| 103 | 5.998207 | 142.251.208.110 | 192.168.0.227 | QUIC     | 67     |                             |      | Protected Payload (KPO)   |
| 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_PERF          |
| 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 → 61380 [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 104.17.25.14 |
| 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 → 61380 [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 → 61380 [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=f920a909041596d, PKN: 1, ACK  |
| 176 | 6.028962 | 142.251.39.42   | 192.168.0.227 | QUIC     | 82     |                             |      | Initial, SCID=f920a909041596d, PKN: 2, ACK  |
| 177 | 6.028962 | 142.251.39.42   | 192.168.0.227 | QUIC     | 1292   |                             |      | Initial, SCID=f920a909041596d, PKN: 3, ACK, PADDING                                 |
| 178 | 6.028962 | 142.251.39.42   | 192.168.0.227 | QUIC     | 1292   |                             |      | Initial, SCID=f920a909041596d, PKN: 4, ACK, PADDING                                 |

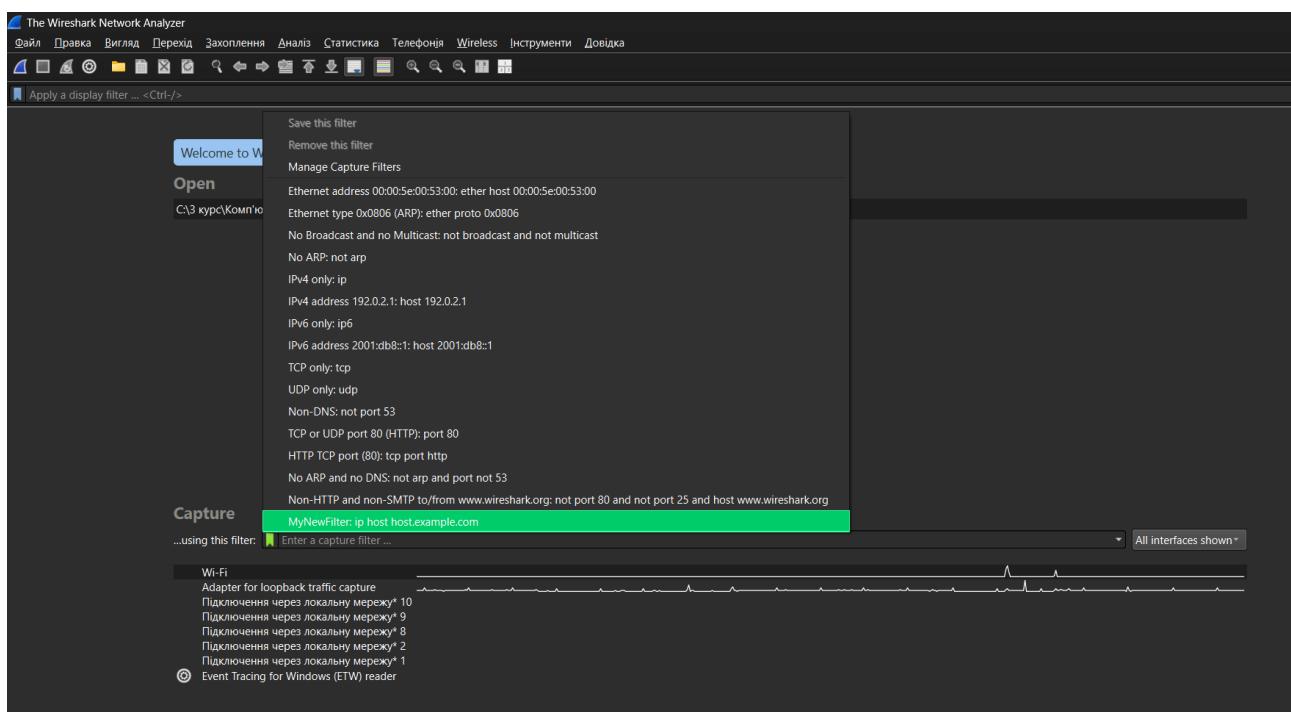
## Пакети отримані не моїм локальним IP:

| 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=1 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_Perf |
| 63  | 5.972816 | 142.251.208.110 | 192.168.0.227 | QUIC     | 82     |                             |      | Initial, SCID=e7d96572e30137d5, PKN: 1, ACK                                |
| 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                    |

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

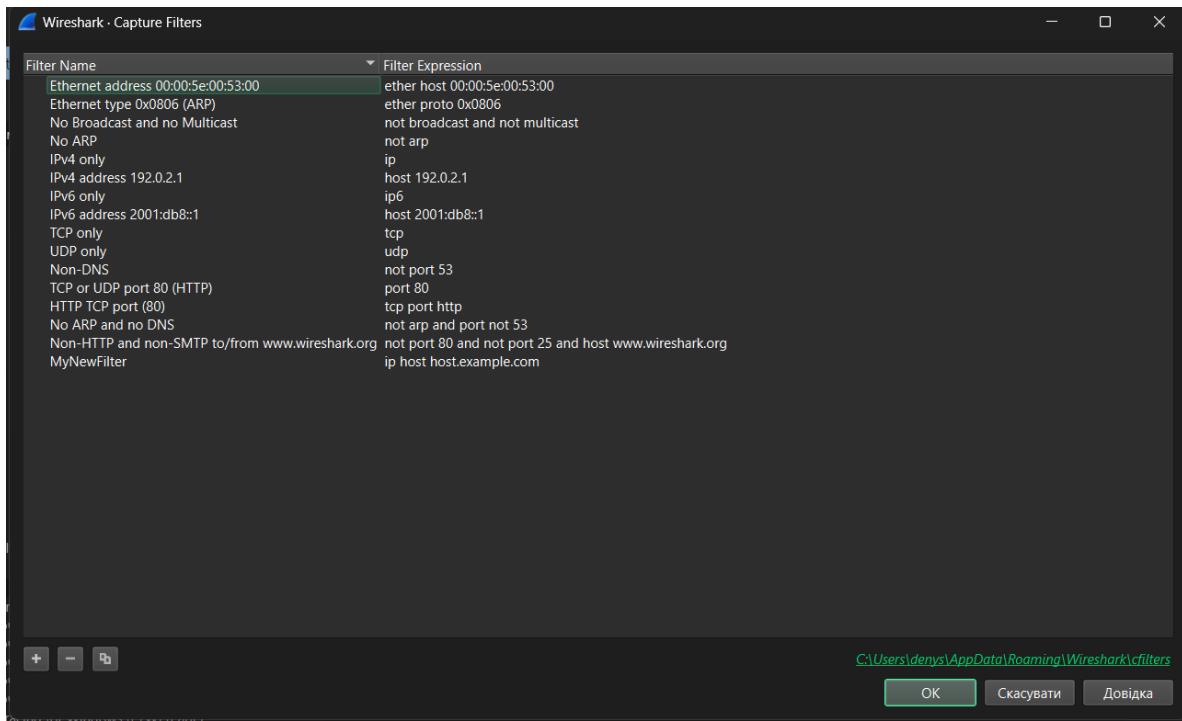


11. Створив власний фільтр і захопив пакети з його використанням. Для цього перед захопленням пакетів натиснув на зелену корогву у полі ...using this filter та обрав створений фільтр “MyNewFilter”:

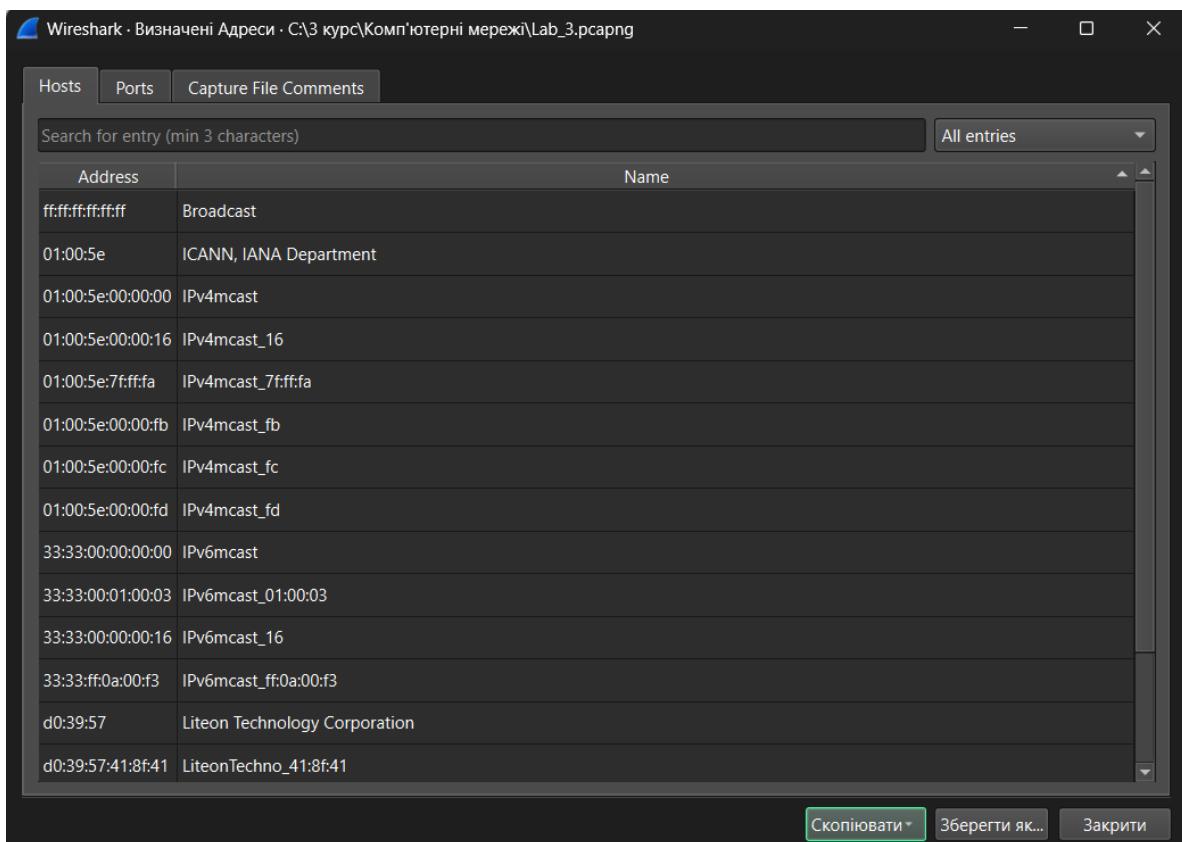


12. У меню Статистика вибрає по черзі пункти Властивості Файлу Захоплення, Визначені Адреси, Ієархія Протоколів, Conversations, I/O Graph, IPv4 Statistics та ознайомився з інформацією.

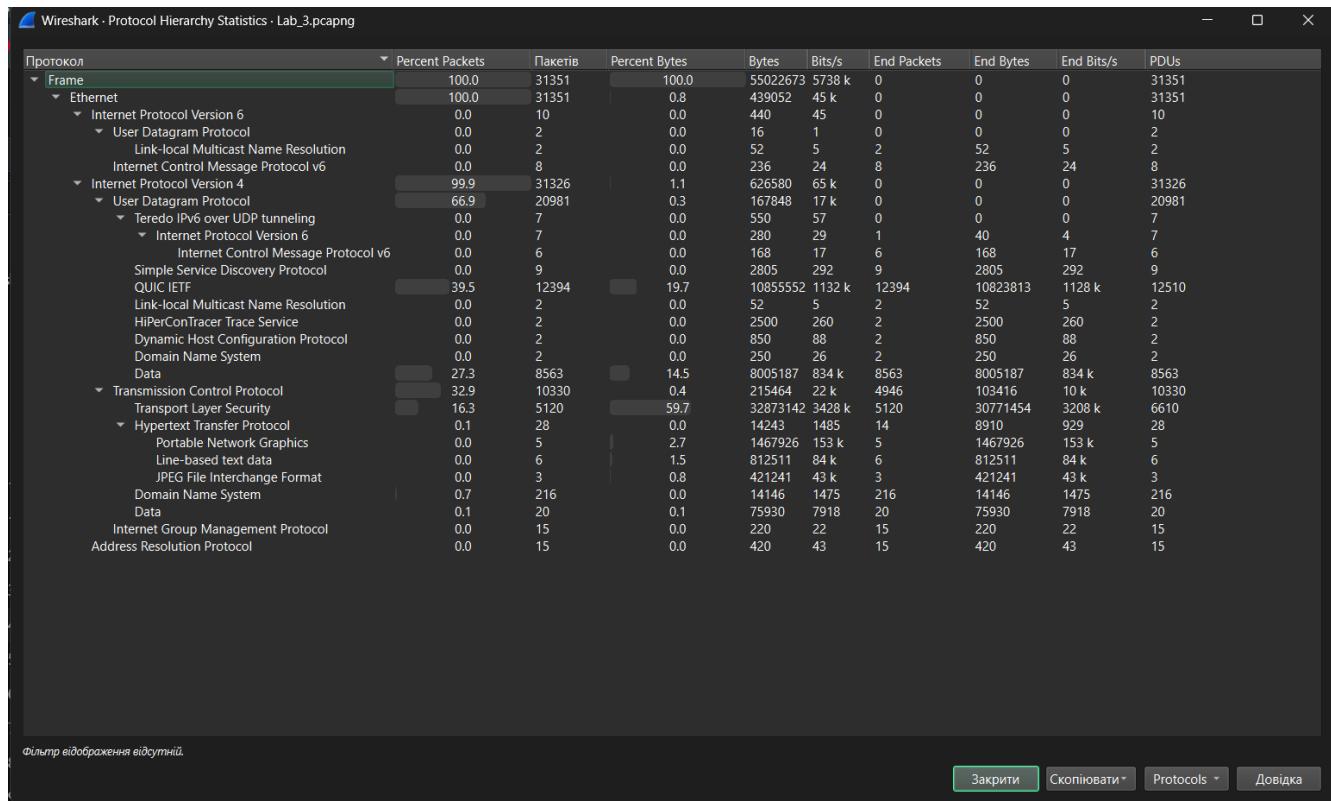
Властивості Файлу Захоплення – показує дані про пакети записані у файлі, час, та статистику пакетів:



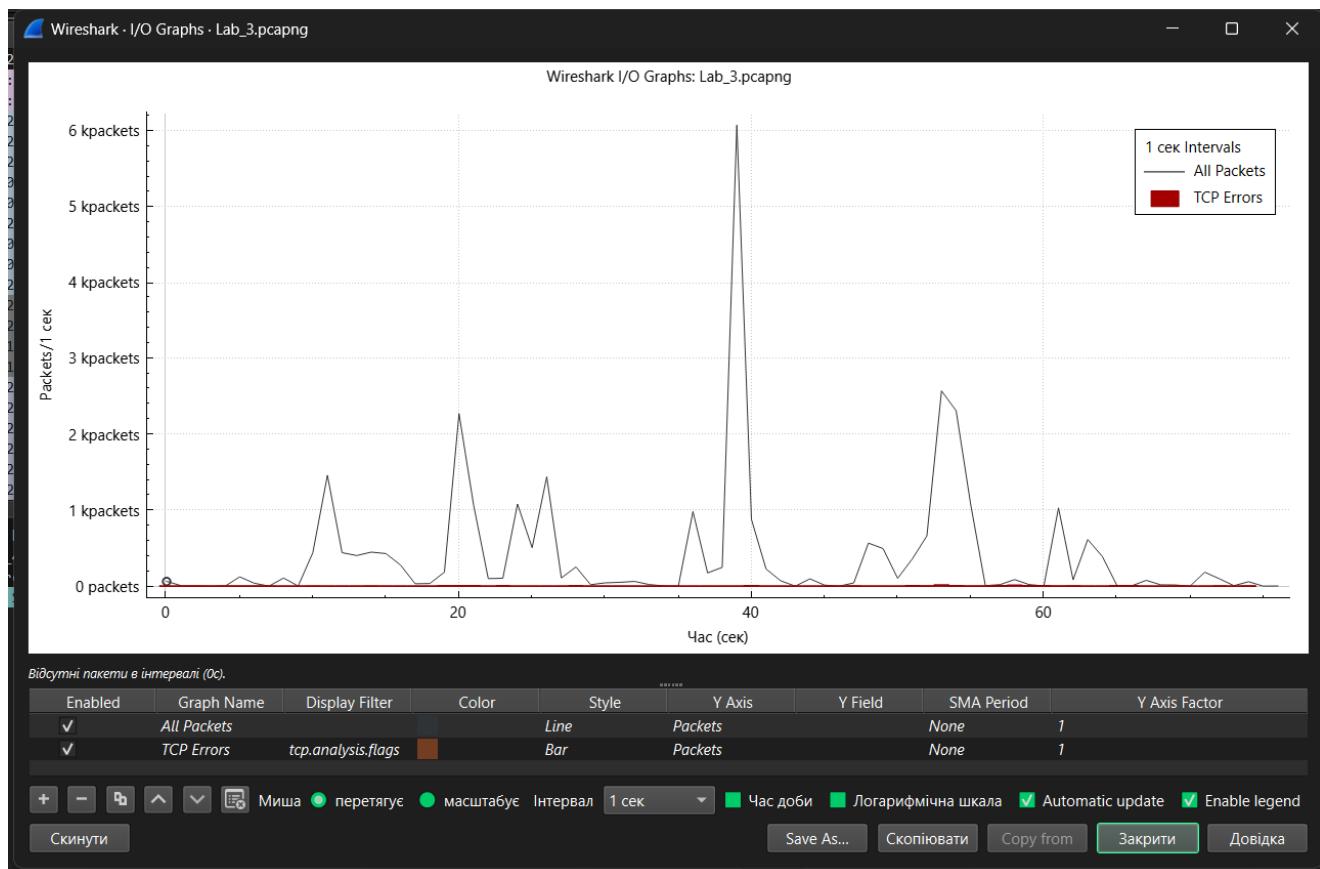
Визначені Адреси має фізичні адреси, які отримували пакети або відправляли, а також порт та протокол за яким відправлено в другій вкладці:



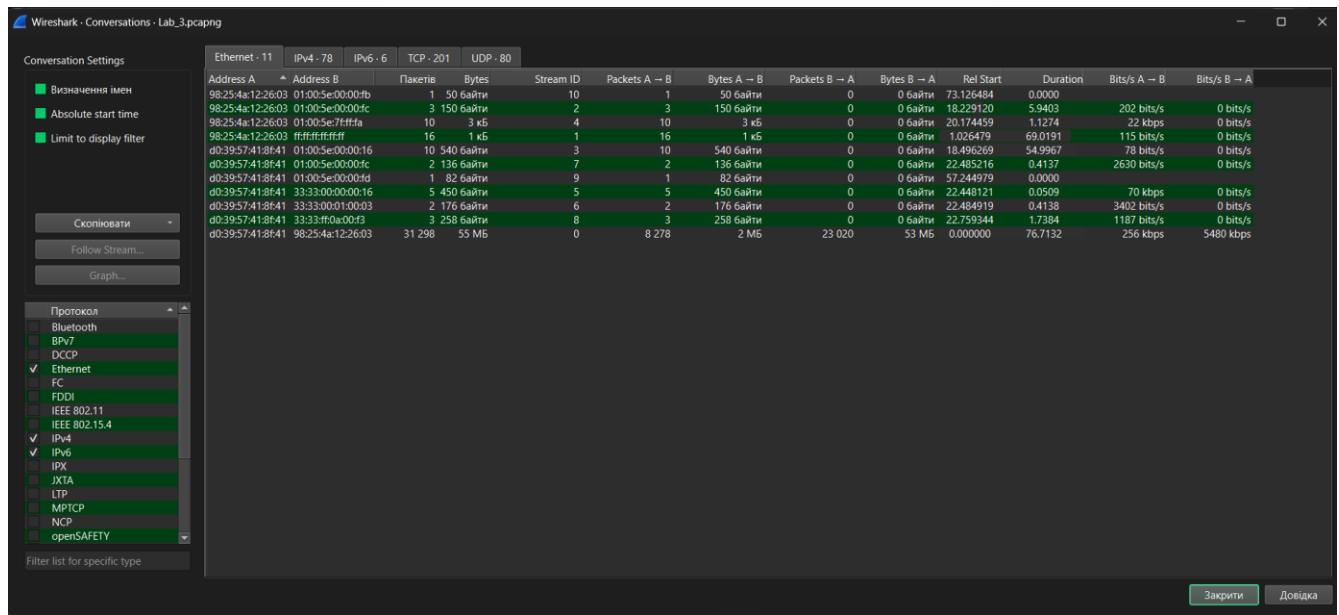
Ієархія Протоколів показує ієархію розподілення пакетів по протоколах:



I/O Graph - графік отриманих та відправлених пакетів:



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



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

| 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:ffe           | 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      |

**Висновок:** Під час виконання лабораторної 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.