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

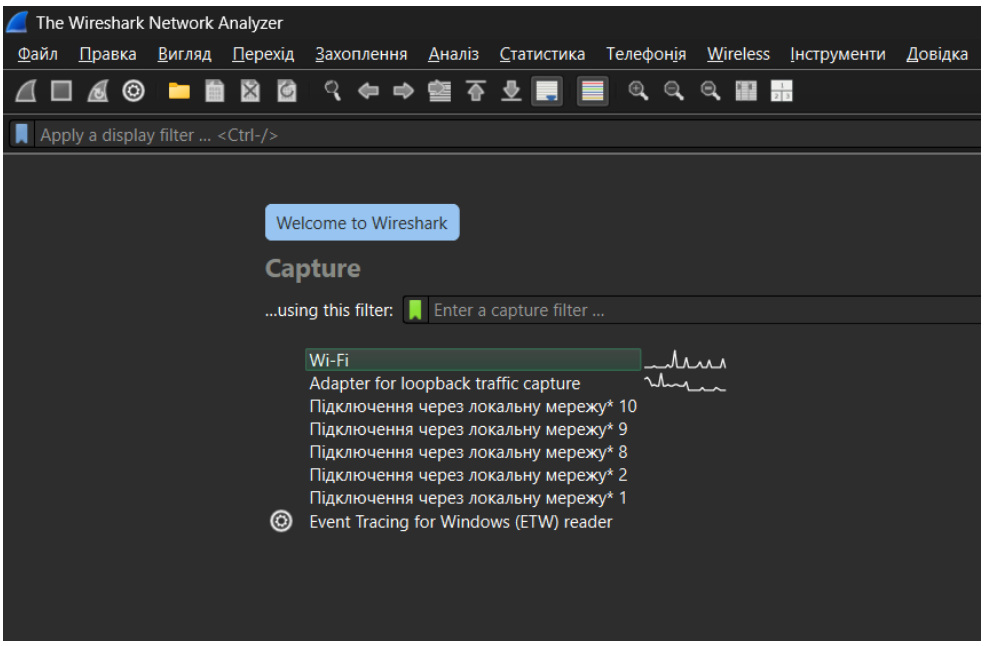
2025

Тема: “Інтерфейс аналізатора мережевих пакетів Wireshark”

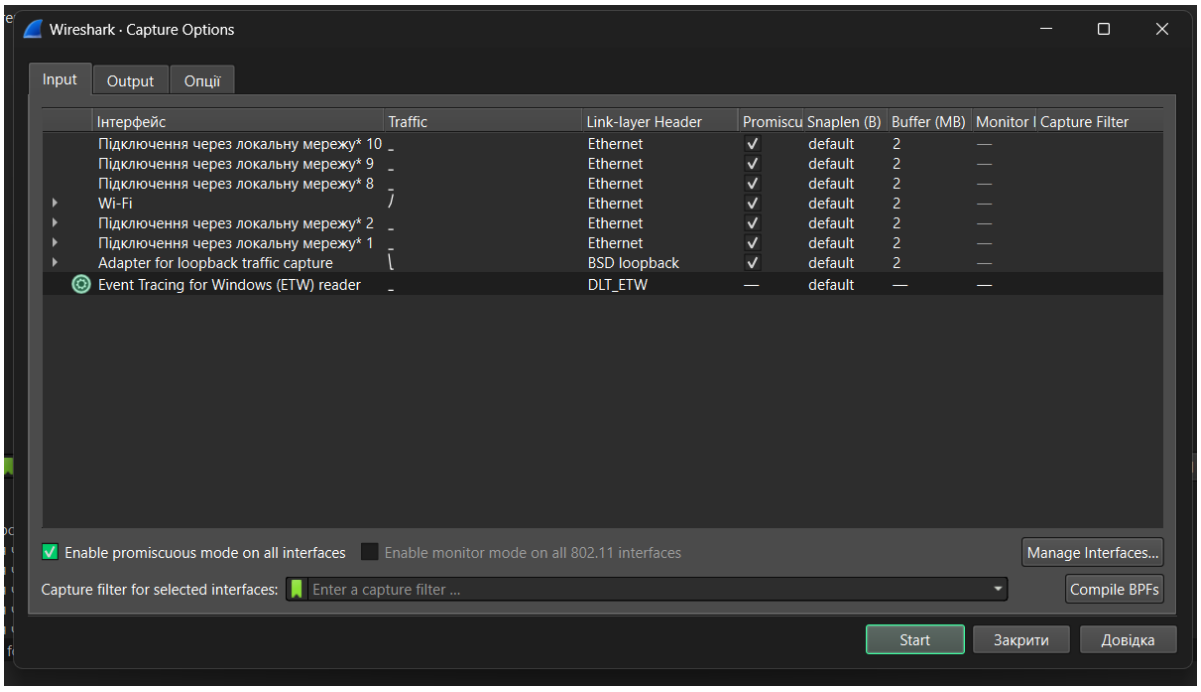
Мета роботи: Отримати загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark; ознайомитися з графічним інтерфейсом програми та основними параметрами конфігурації; навчитися захоплювати, сортувати та фільтрувати пакети.

Хід роботи

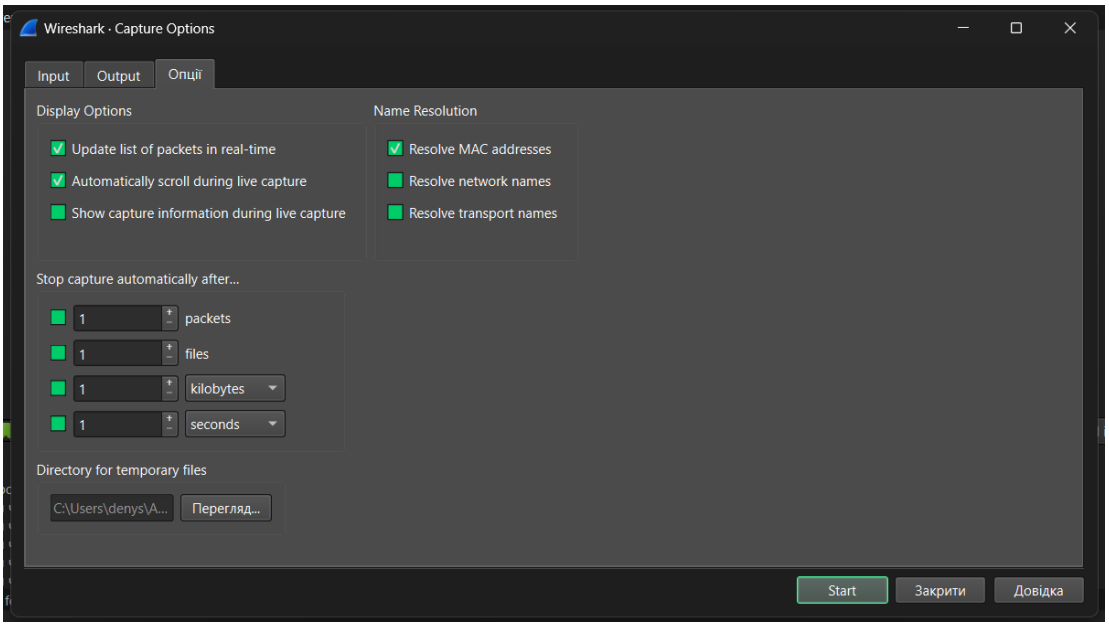
1. Запустив аналізатор мережевих пакетів Wireshark від імені адміністратора. Вибрав з переліку Wi-Fi та почав захоплення:



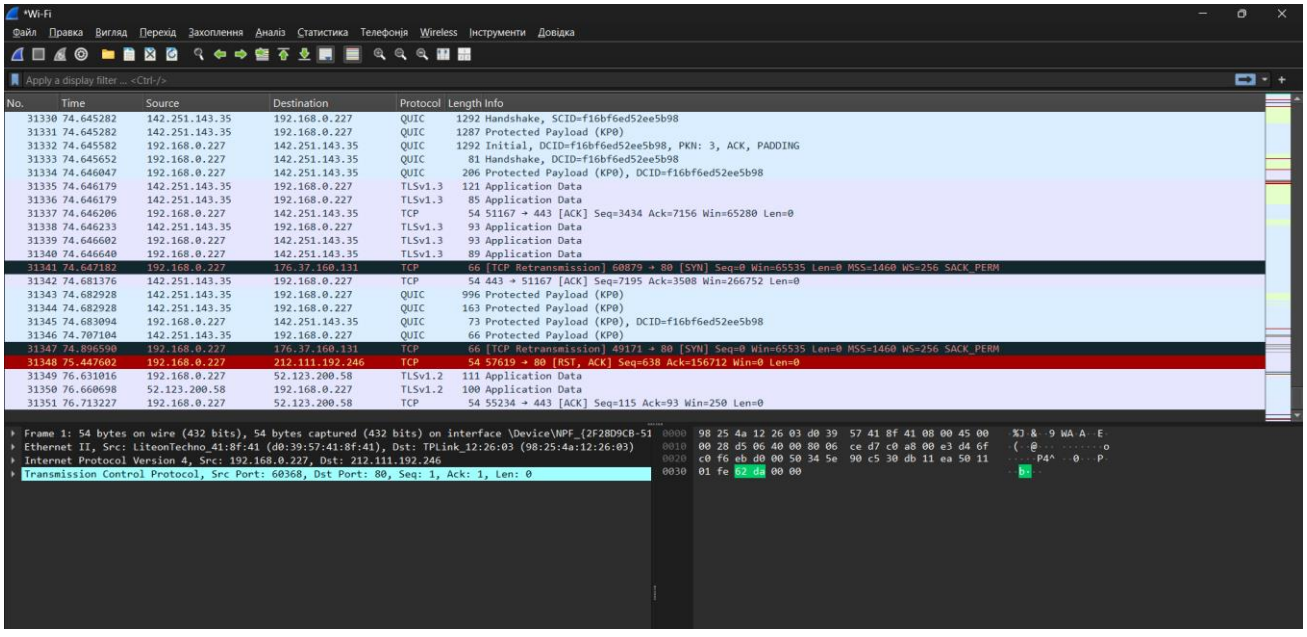
2. Виконав команду Захоплення → Опції, переконався, що мережеві карти (інтерфейси) налаштовані для роботи у нерозбірливому режимі (promiscuous mode):



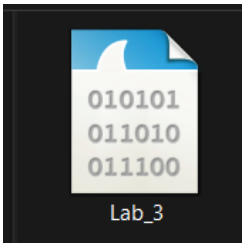
3. Перейшов на вкладку Опції та ознайомився з налаштуванням захоплення пакетів:



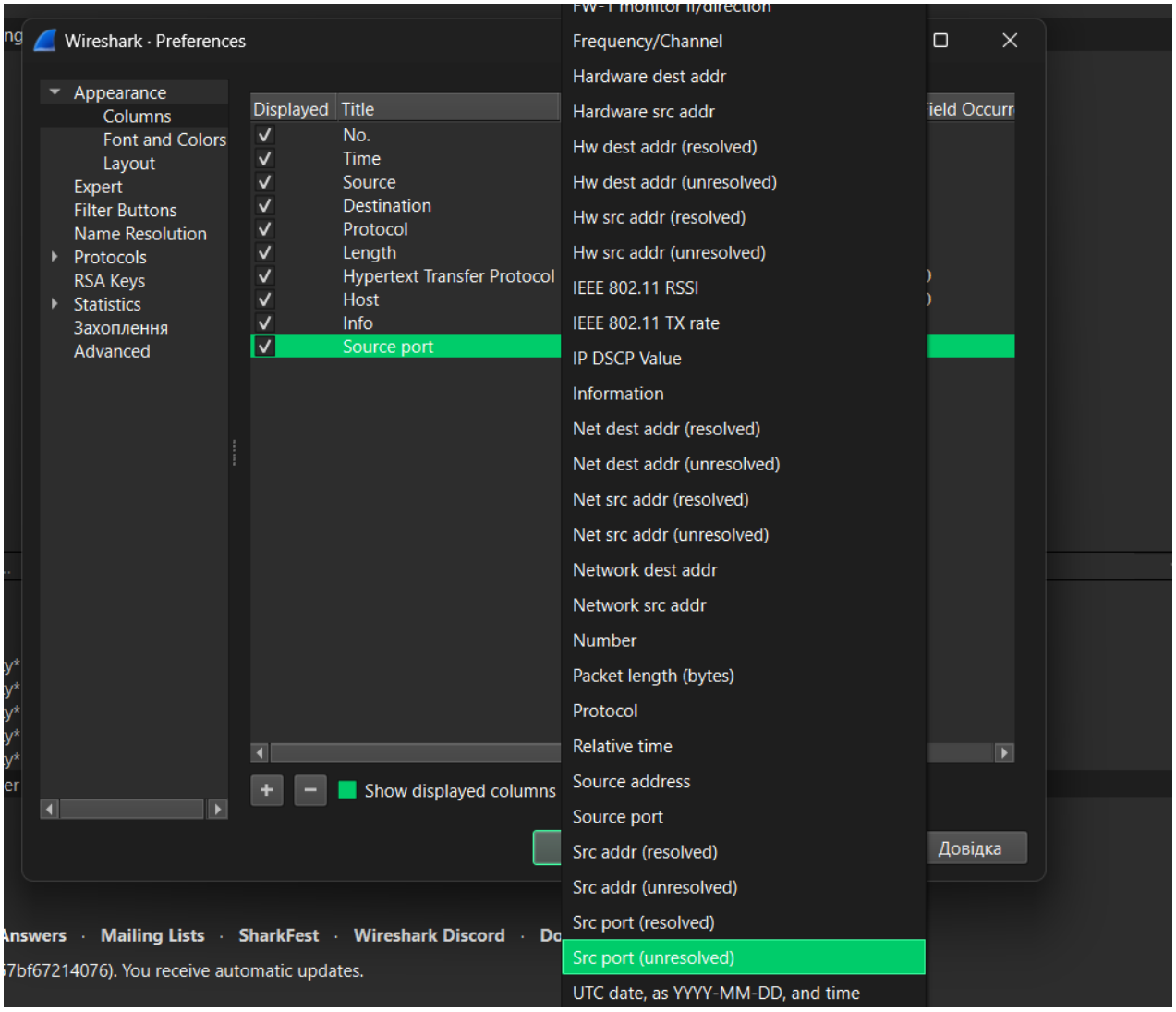
4. Вибрав з переліку Wi-Fi та почав захоплення пакетів. Упродовж 1 хвилини здійснив активність в браузері: перейшов на сайти http://uac.gov.ua, завантажив на комп'ютер зображення та різні файли. Зупинив процедуру захоплення пакетів. Ознайомився з трьома основними елементами головного вікна програми:



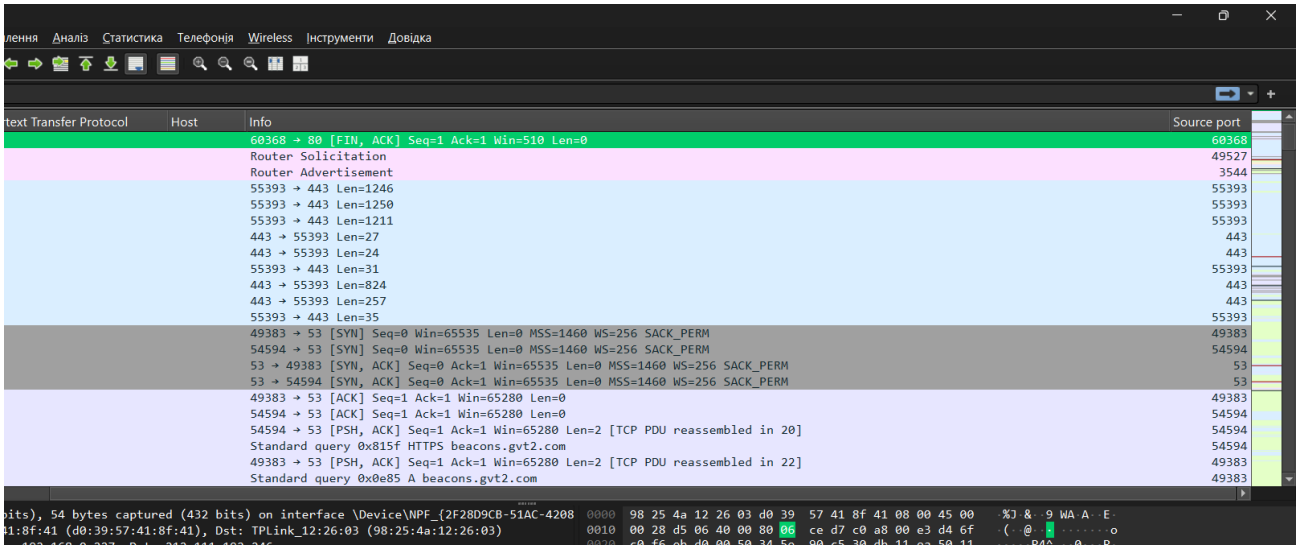
5. Зберіг захоплені пакети у файл для подальшого аналізу:



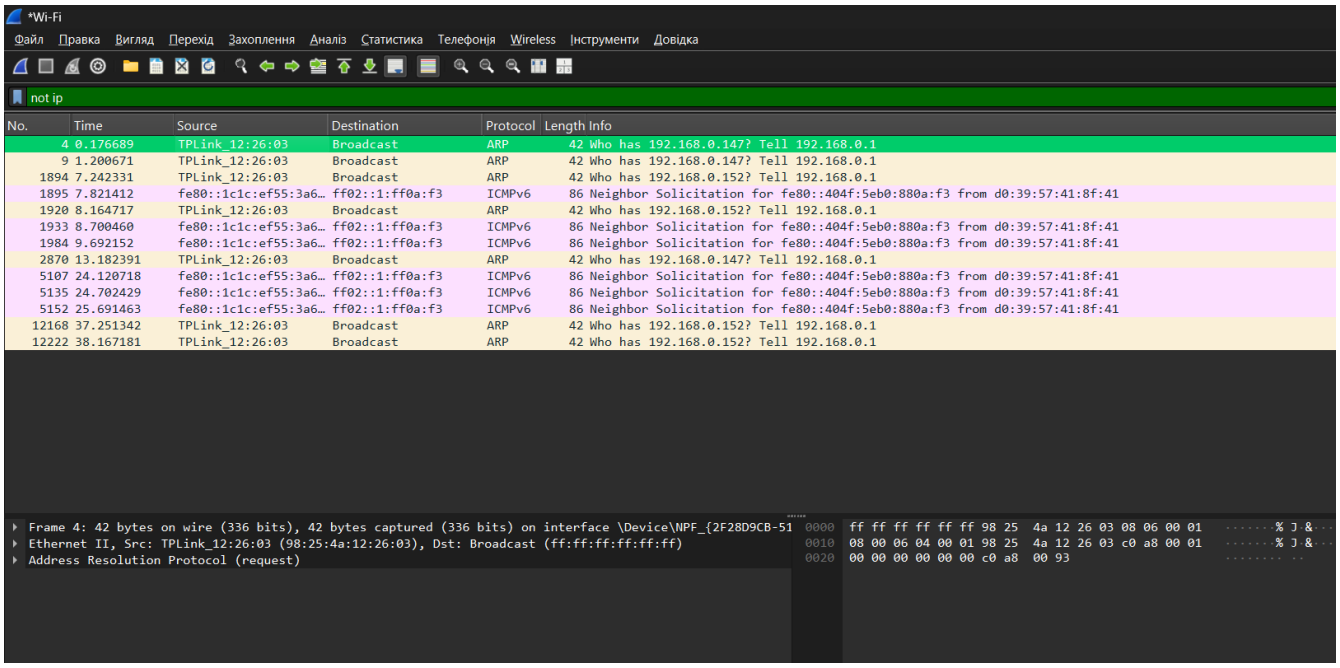
6. Відкрив вікно налаштувань, виконавши команду Правка → Налаштування. Додавав новий стовпчик Source port обравши пункт Columns, натиснув кнопку +, ввів назву стовпчика і тип даних у ньому:



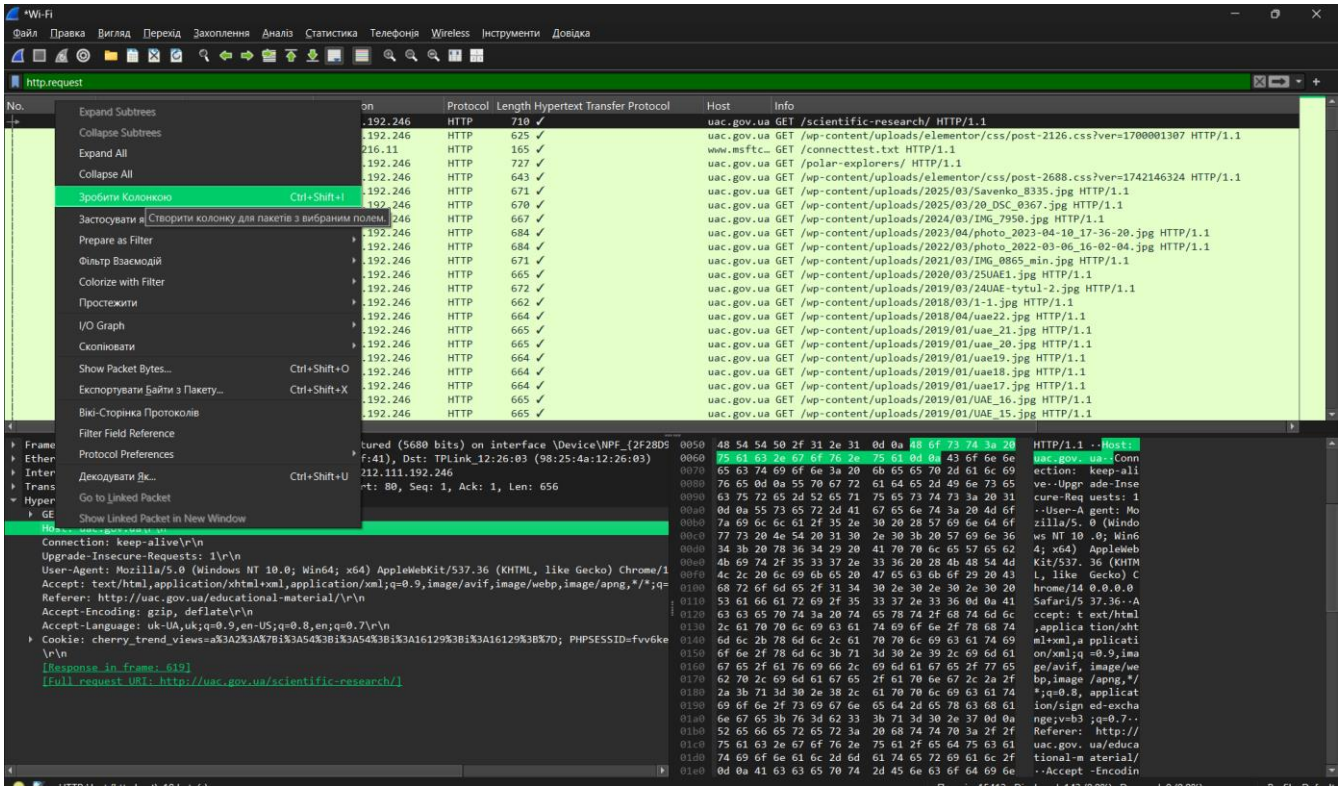
Переконався, що стовпчик з’явився в області “Список пакетів”:



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



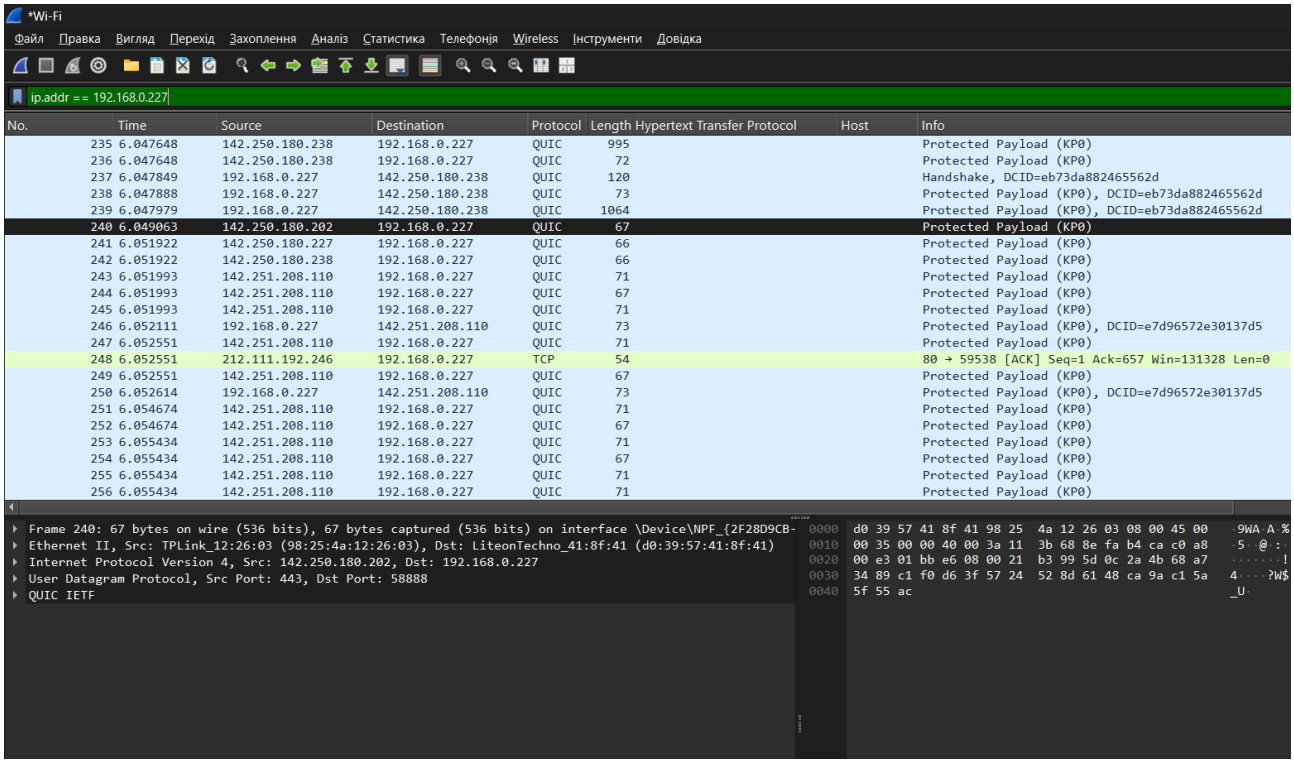
8. Додав стовпчик Host іншим способом. Для цього відфільтрував пакети, які відповідають HTTP-запитам, ввівши у поле фільтрування вираз http.request, розгорнувши інформацію Hypertext Transfer Protocol в області “Ієрархічний вміст пакета” та вибравши з контекстного меню рядка Host команду Зробити Колонкою:



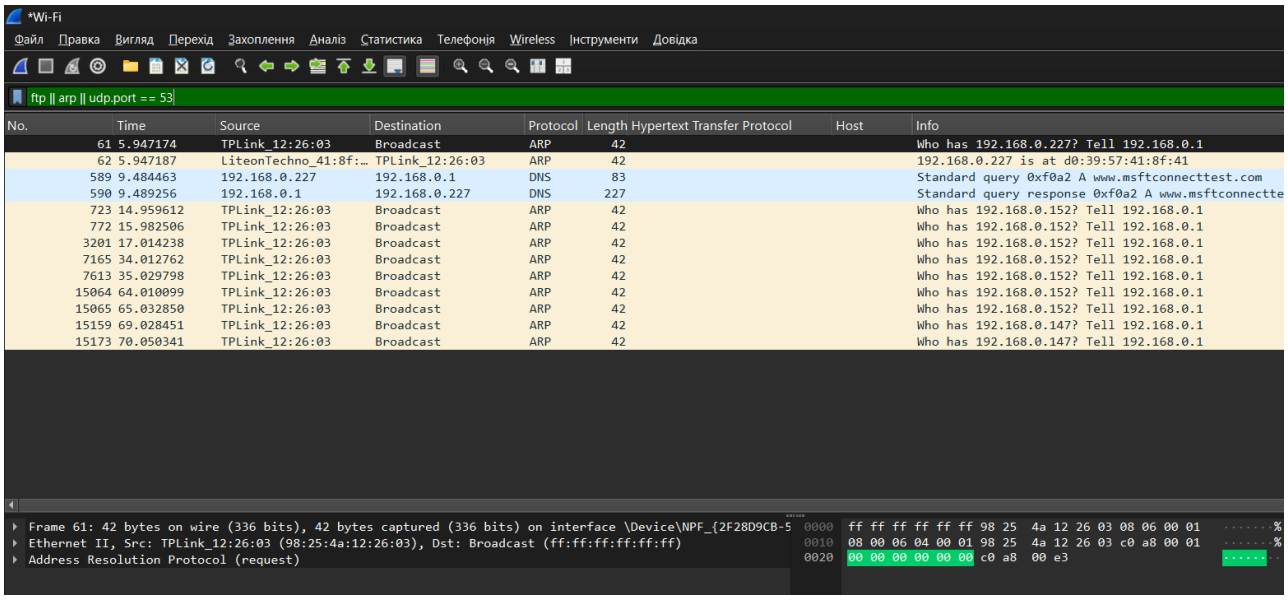
9. Проекспериментував з виразами та описав, які критерії пошуку вони задають:

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

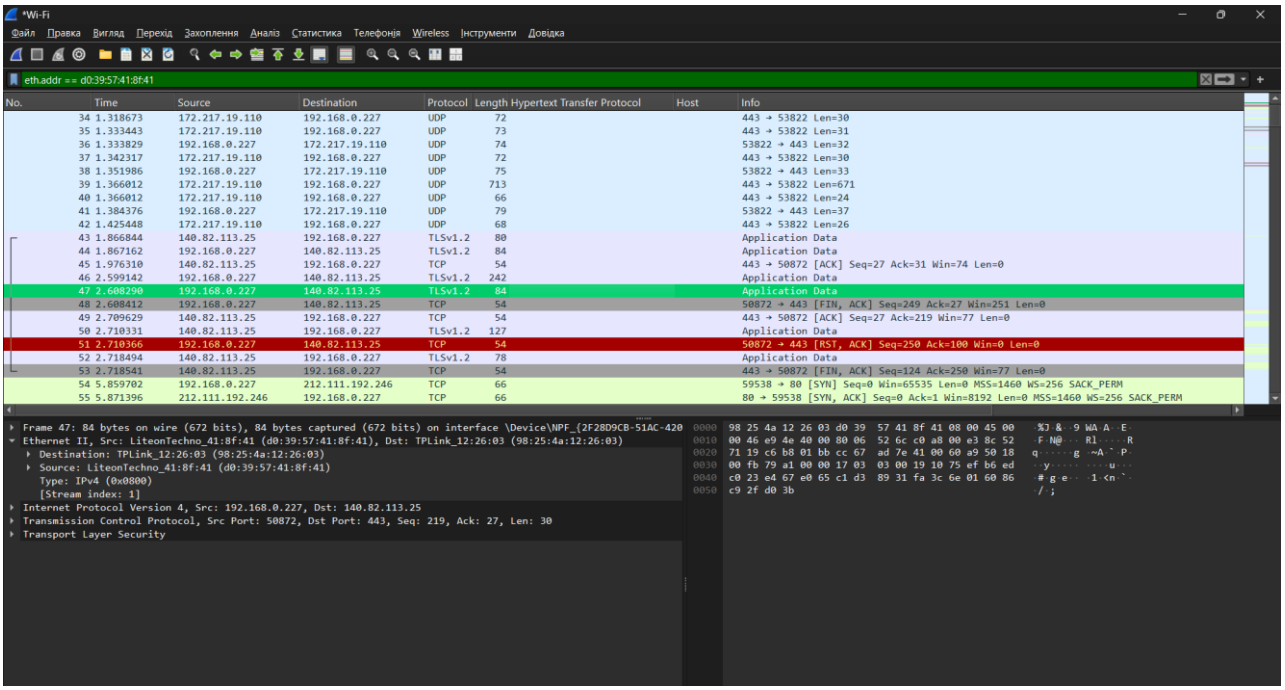
Пакети відправлені з мого локального IP або отримані ним:



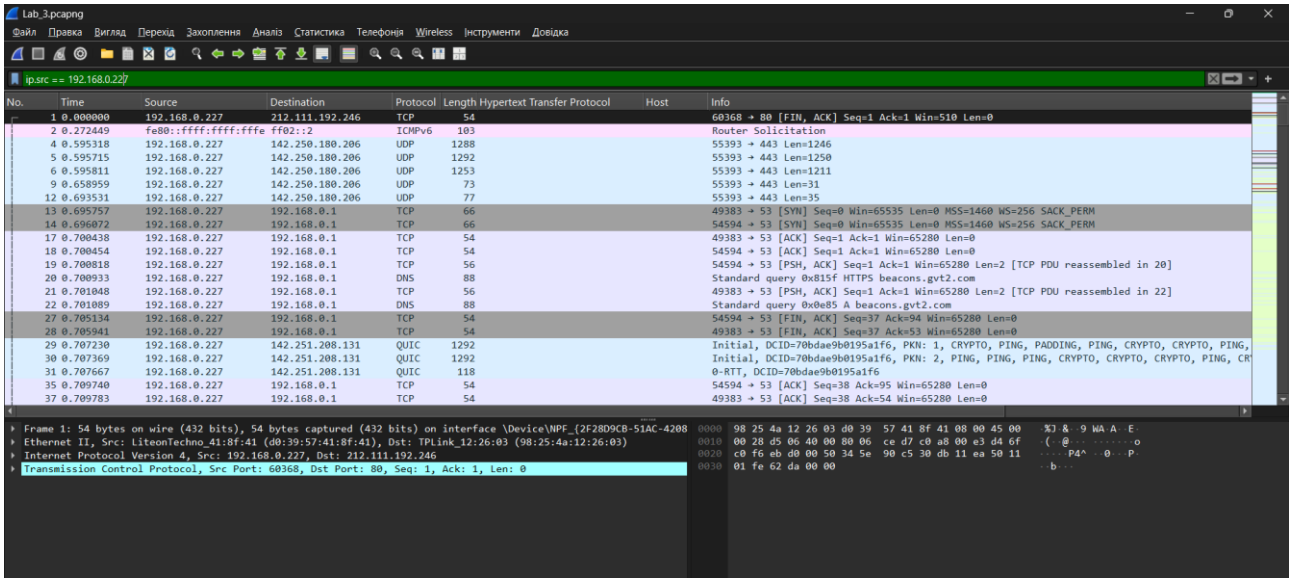
Пакети відправлені протоколом ARP або через UDP порт 53:



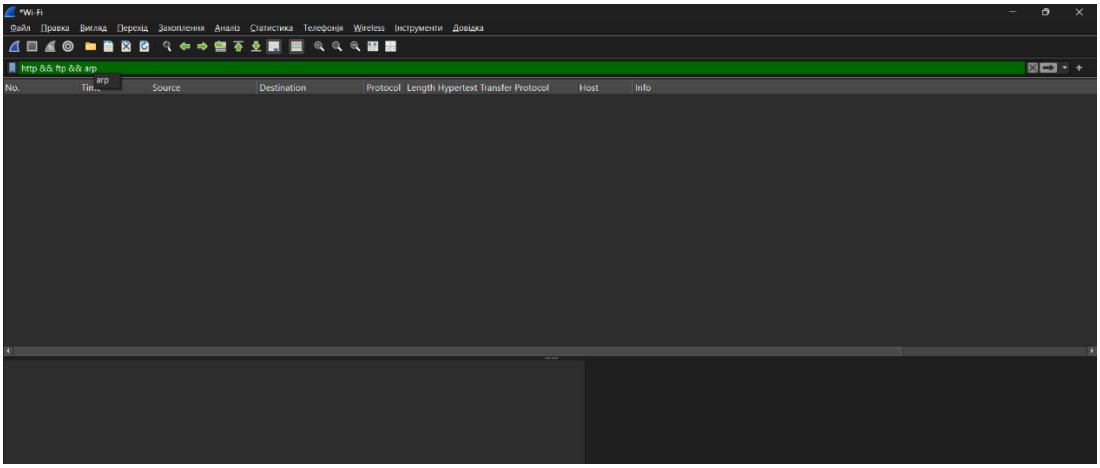
Пакети відправлені або отримані фізичною адресою мого адаптеру:



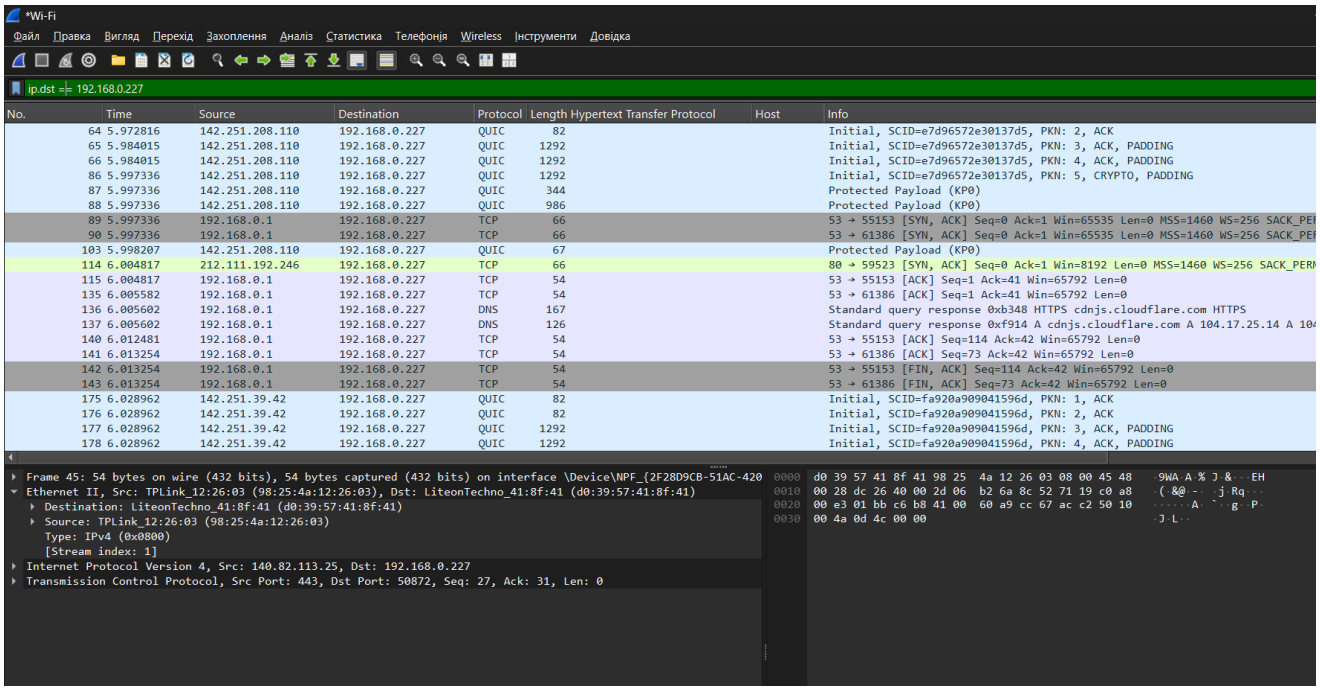
Пакети відправлені з мого локального IP:



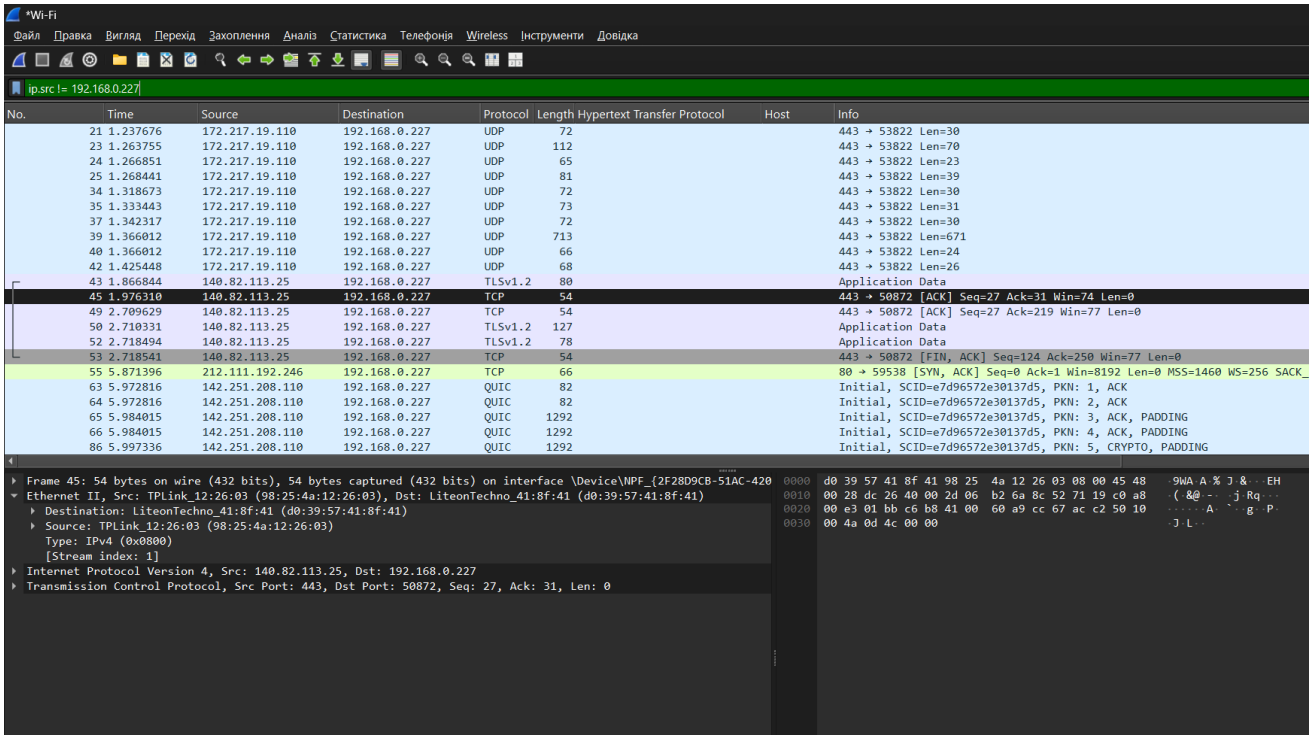
Пакети http, ftp та arp:



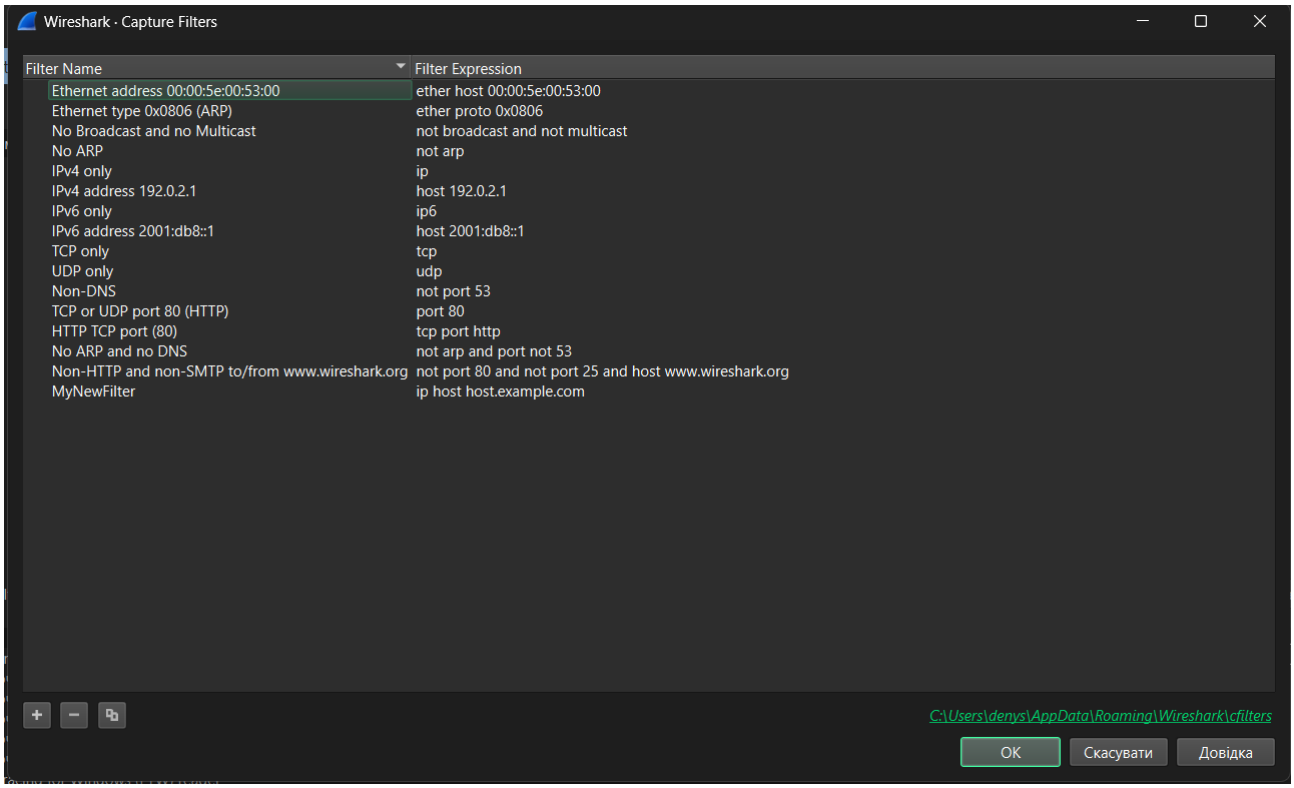
Пакети отримані моїм локальним IP:



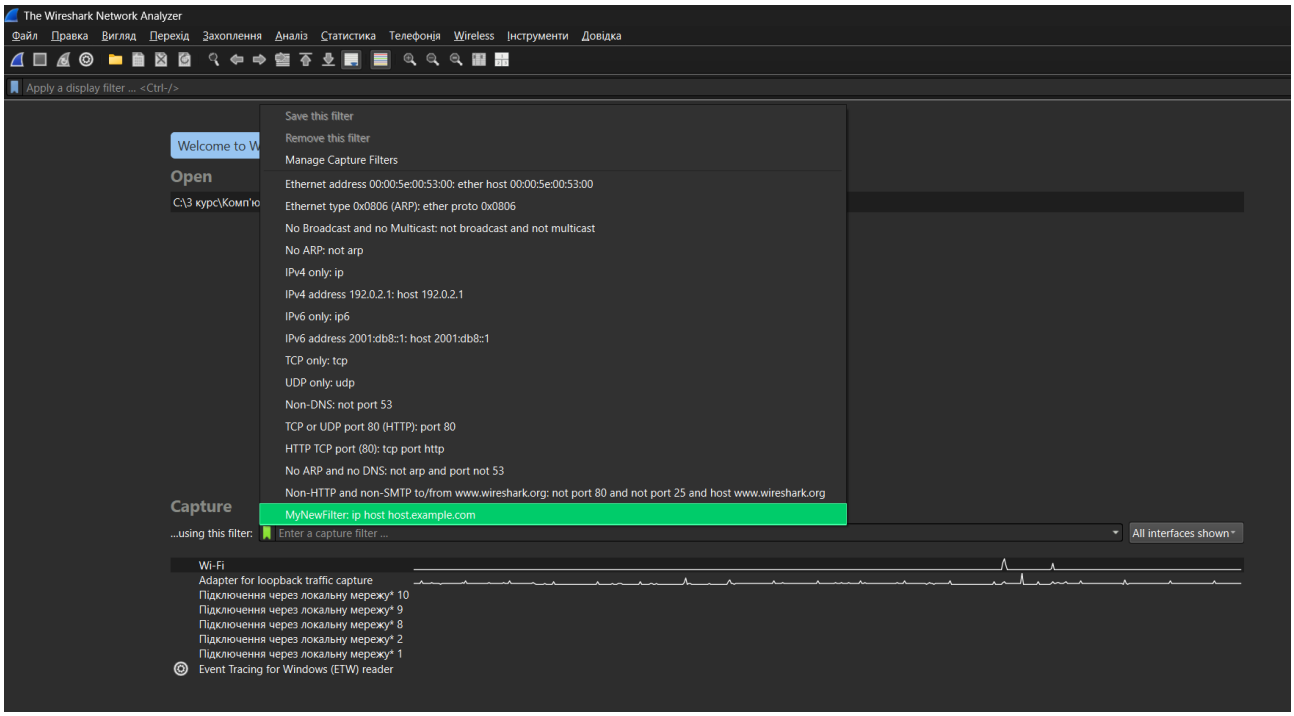
Пакети отримані не моїм локальним IP:



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

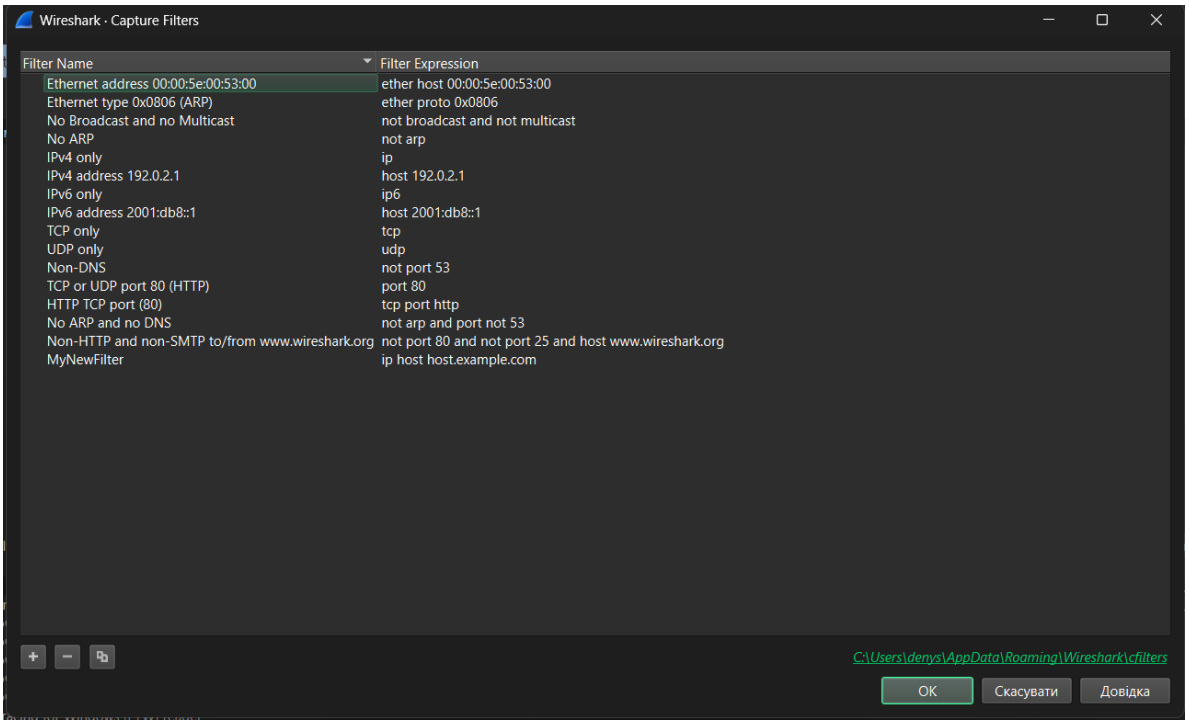


11. Створив власний фільтр і захопив пакети з його використанням. Для цього перед захопленням пакетів натиснув на зелену коругву у полі …using this filter та обрав створений фільтр “MyNewFilter”:

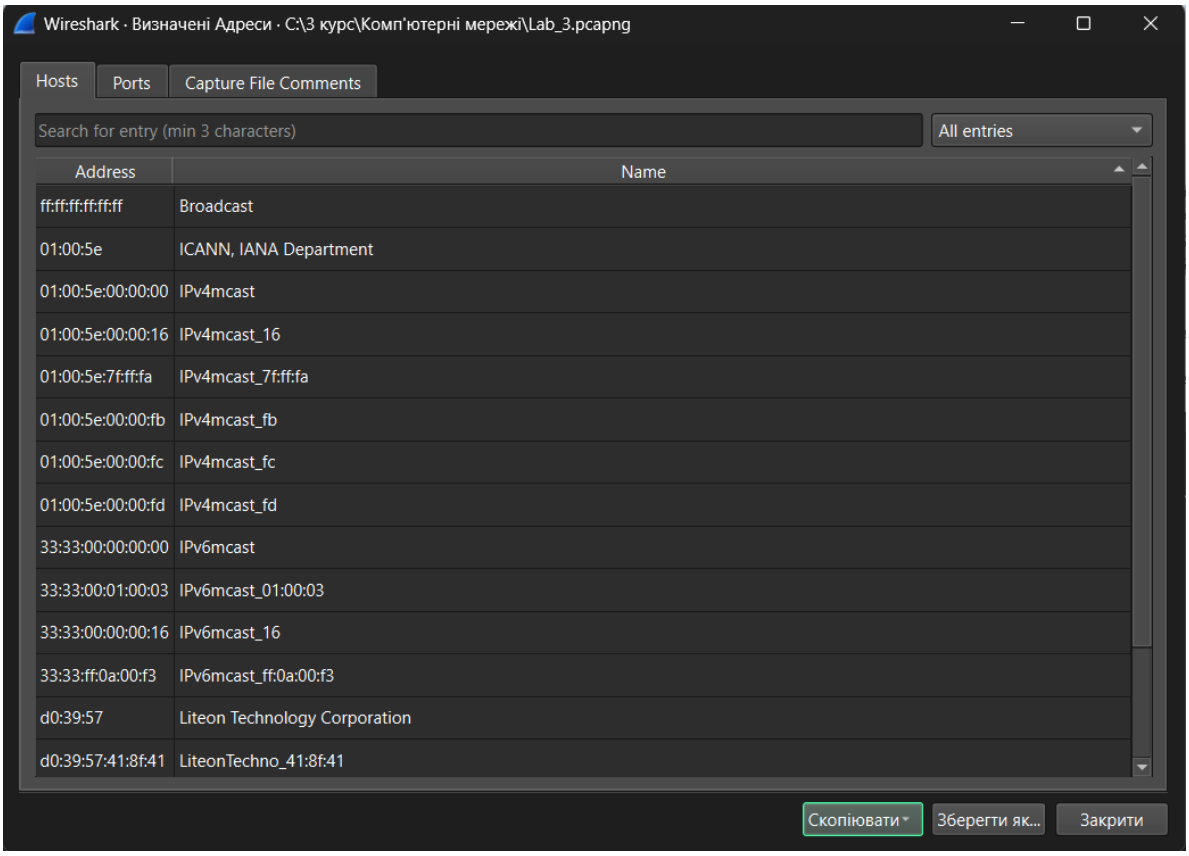


12. У меню Статистика вибрав по черзі пункти Властивості Файлу Захоплення, Визначені Адреси, Ієрархія Протоколів, Conversations, I/O Graph, IPv4 Statistics та ознайомився з інформацією.

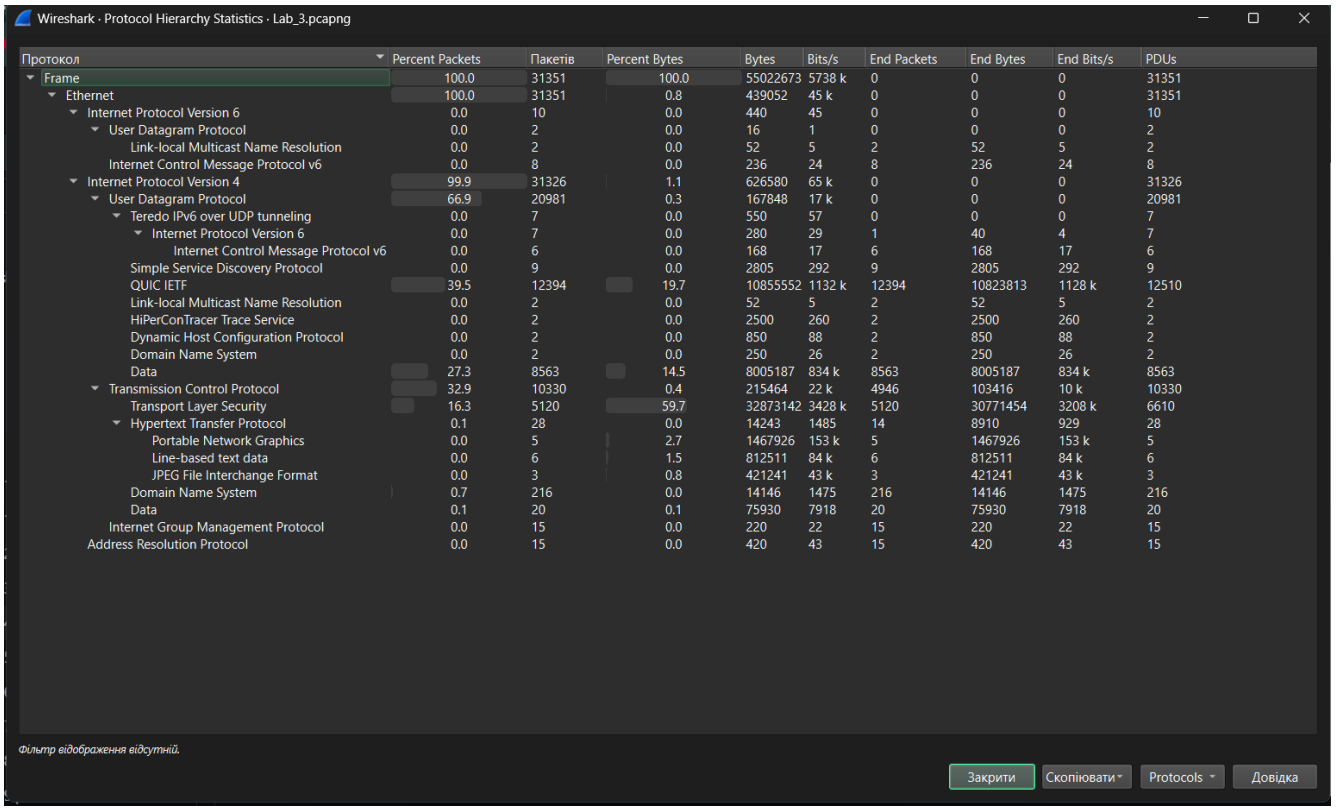
Властивості Файлу Захоплення – показує дані про пакети записані у файлі, час, та статистику пакетів:



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

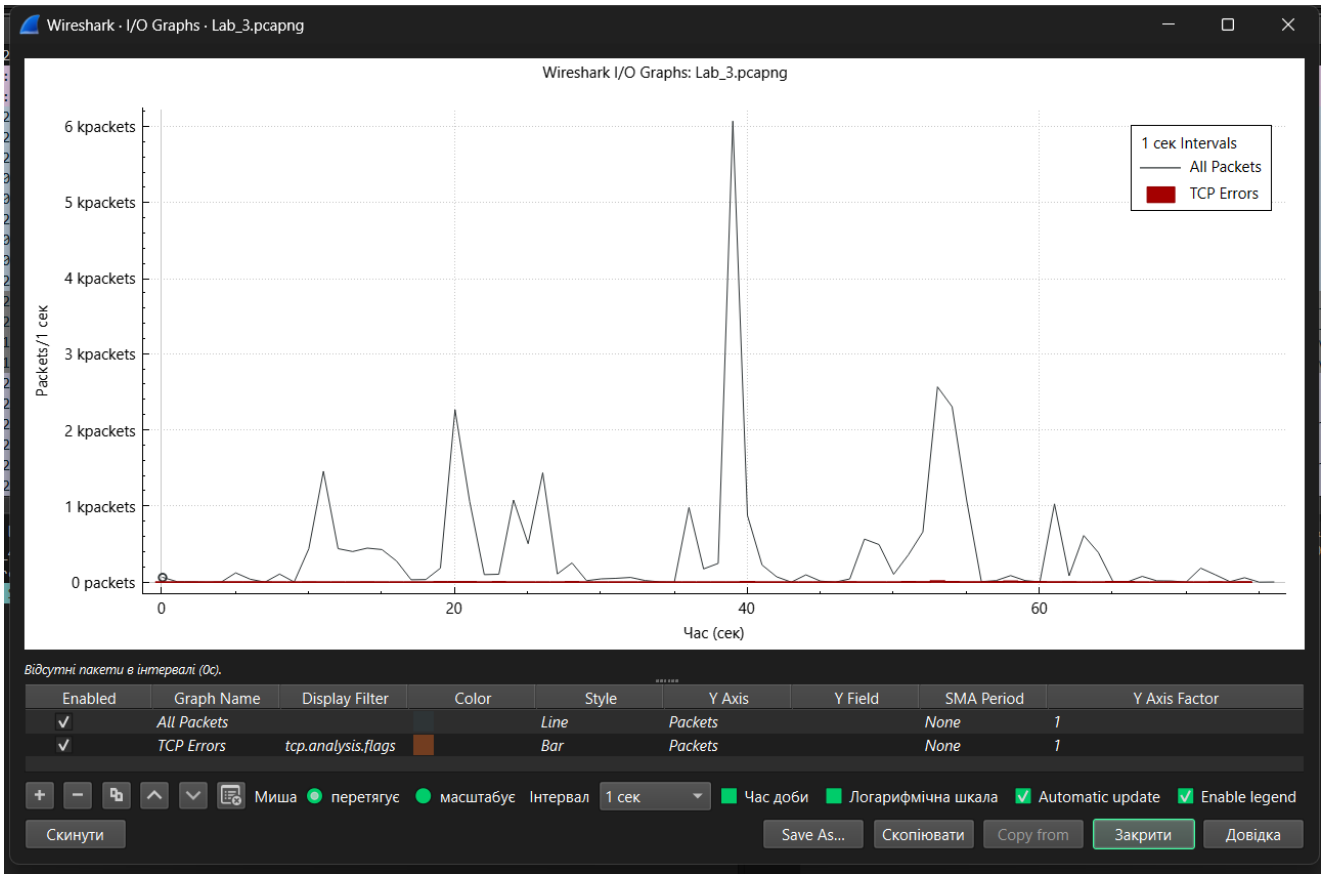


Ієрархія Протоколів показує ієрархію розподілення пакетів по протоколах:

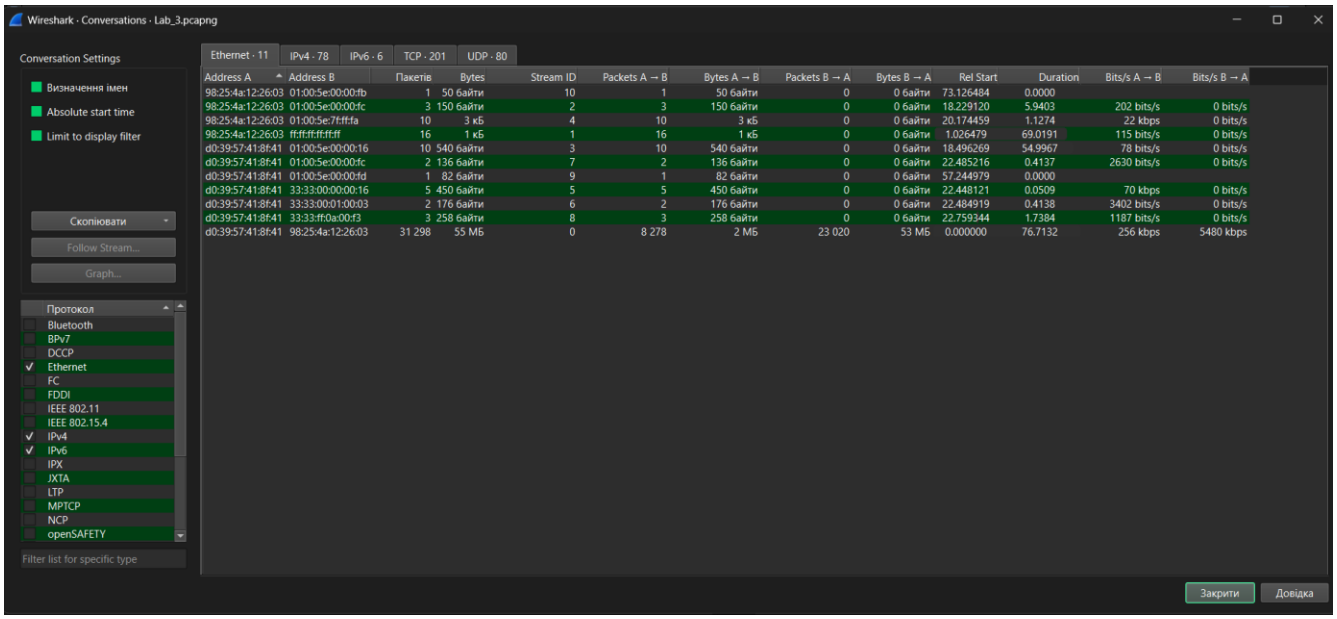


Протокол	Percent Packets	Пакетів	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	31351	100.0	55022673	5738 k	0	0	0	31351
Ethernet	100.0	31351	0.8	439052	45 k	0	0	0	31351
Internet Protocol Version 6	0.0	10	0.0	440	45	0	0	0	10
User Datagram Protocol	0.0	2	0.0	16	1	0	0	0	2
Link-local 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

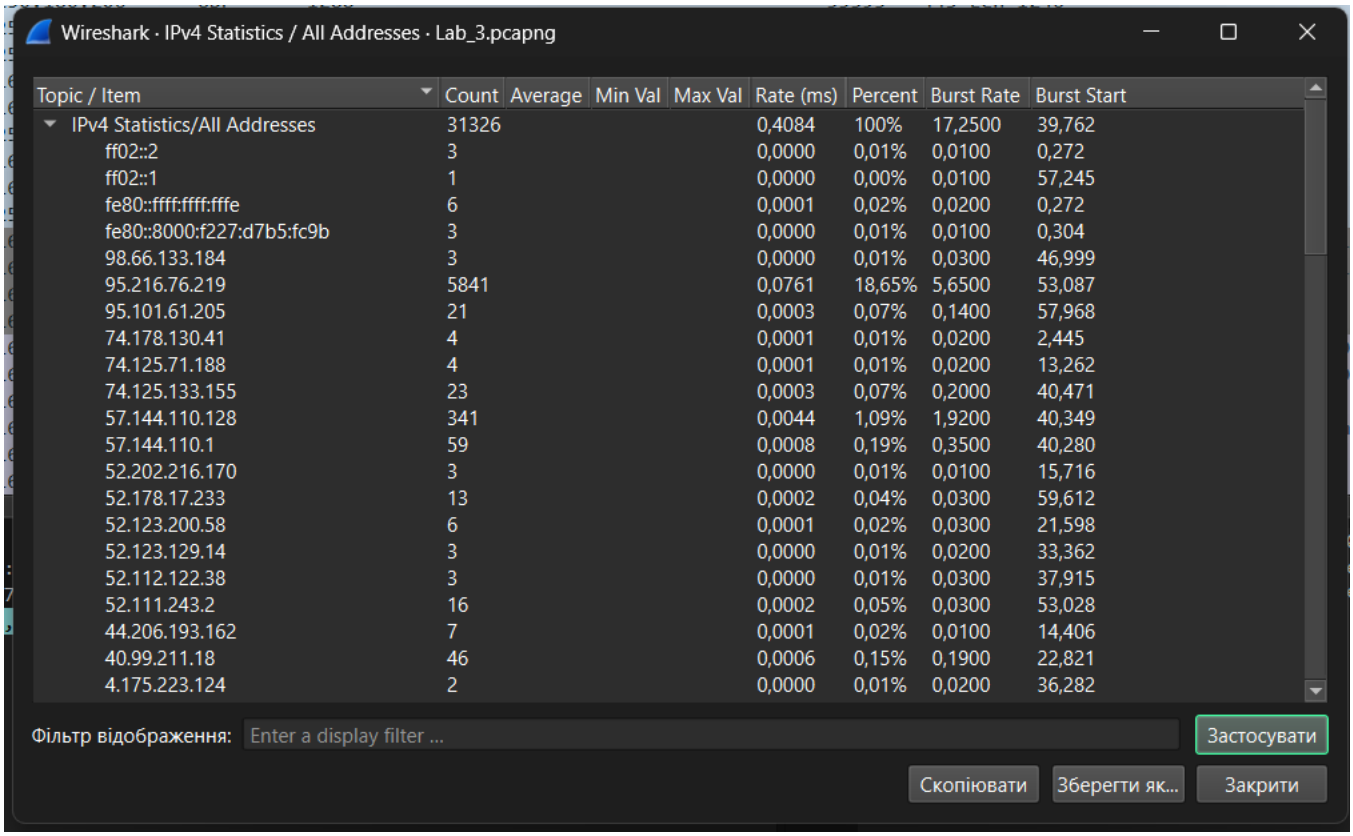
I/O Graph - графік отриманих та відправлених пакетів:



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:



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.