ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА Факультет прикладної математики та інформатики

**Лабораторна робота №4**

**«Комп’ютерні інформаційні мережі»**

Оцінка                          ⠀

Виконала:

студентка групи ПМі-33

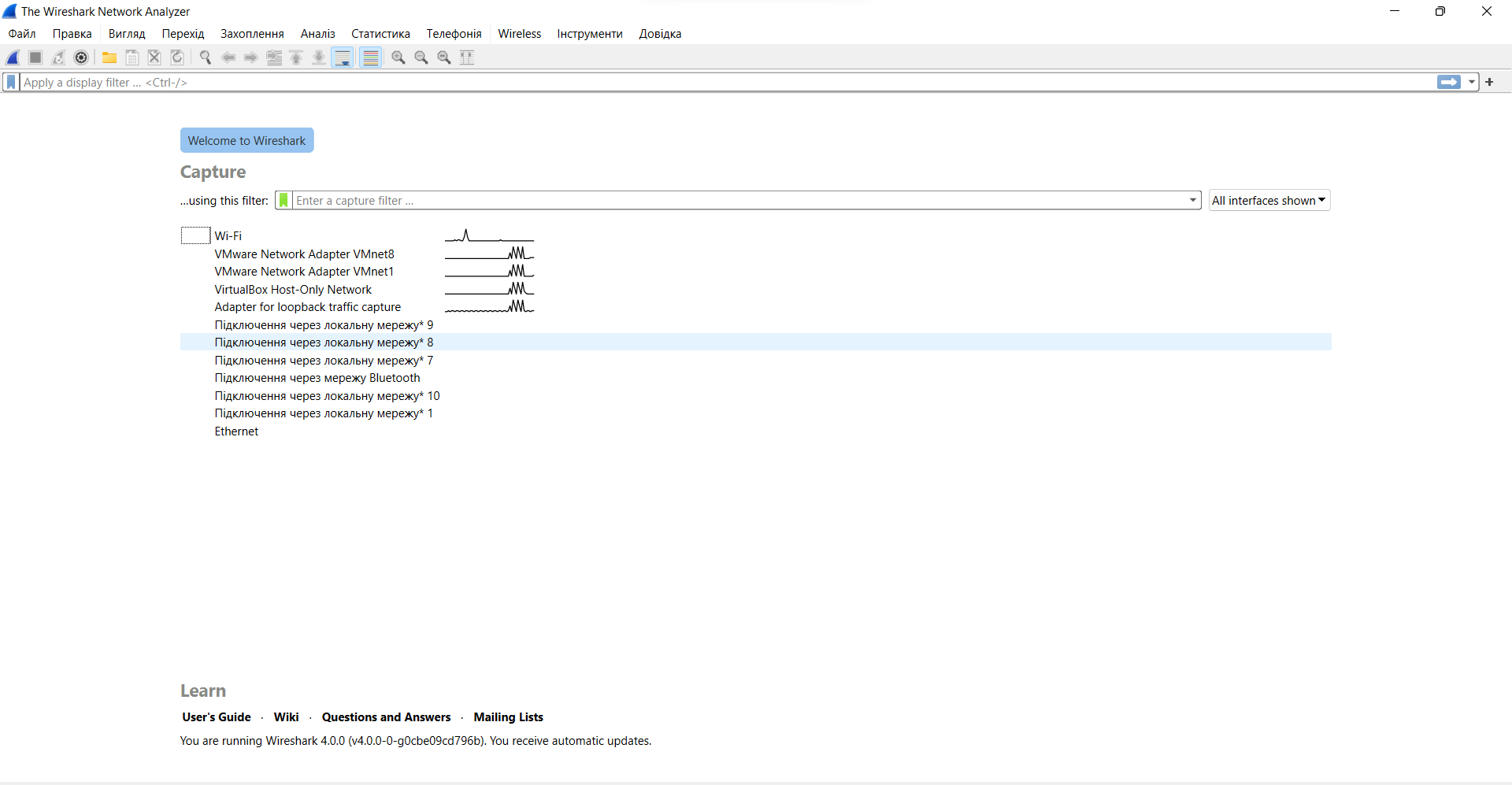
**Лиско Оксана**

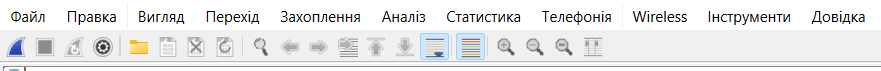
 Викладач:

**ас. Жировецький В.В.**

2022

1. Запускаю аналізатор мережевих пакетів Wireshark від імені адміністратора.



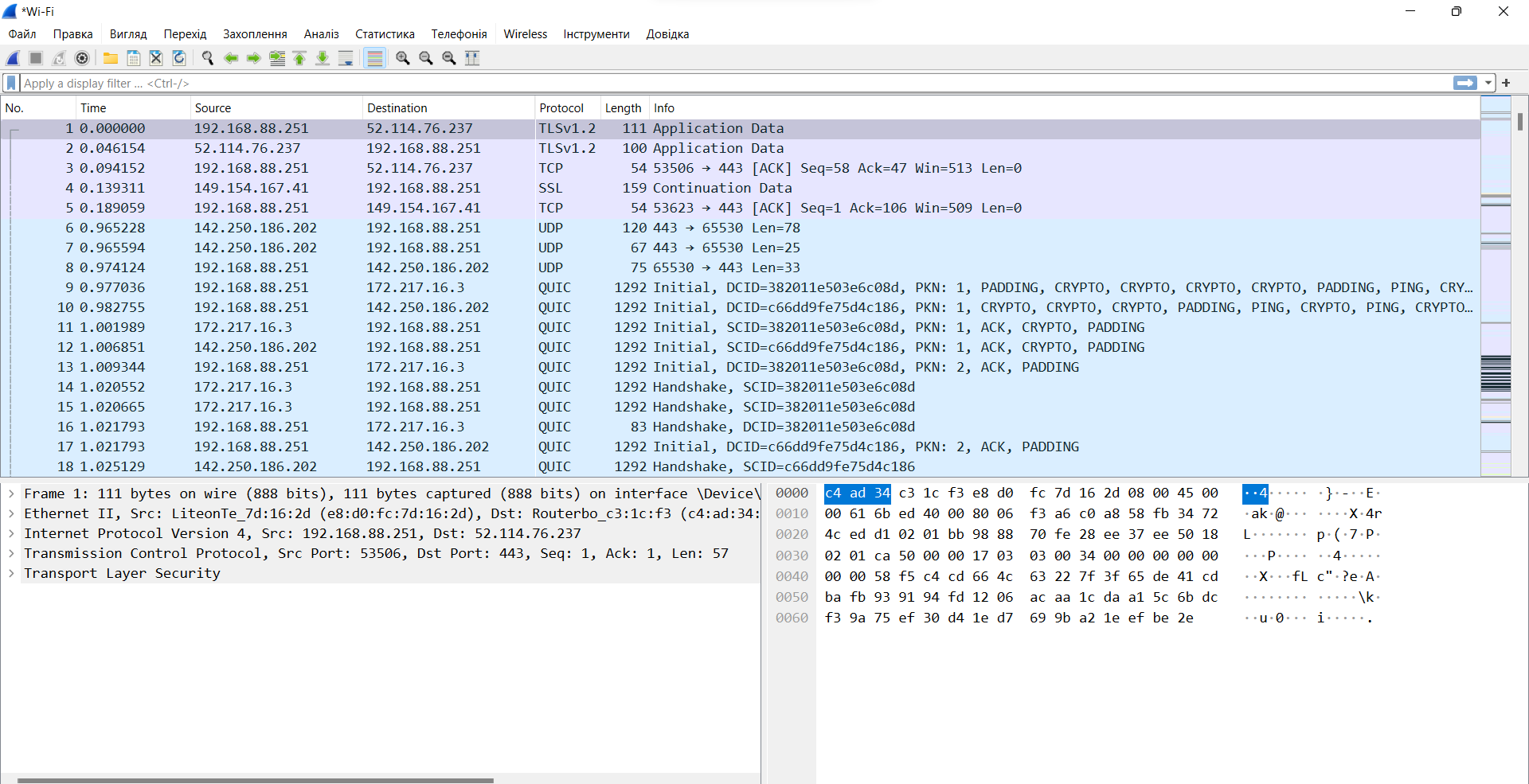


2. Вибираю з переліку необхідний мережевий інтерфейс та починаю процедуру захоплення пакетів.

3. Упродовж 30-60 секунд здійснюю деяку активність в браузері.

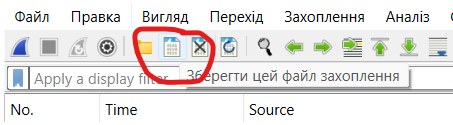
4. Зупиняю процедуру захоплення пакетів.

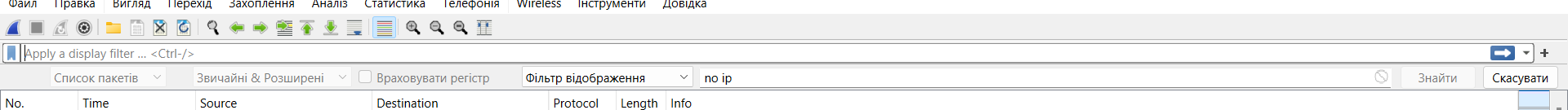
5. Ознайомлююсь з трьома основними елементами головного вікна програми:

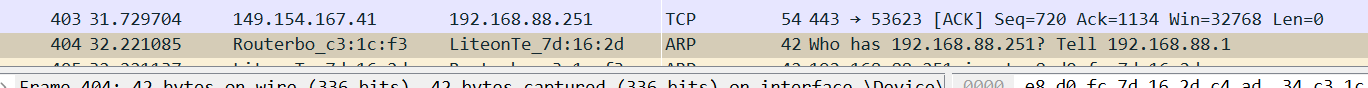


6. Зберігаю захоплені пакети у файл для подальшого аналізу.

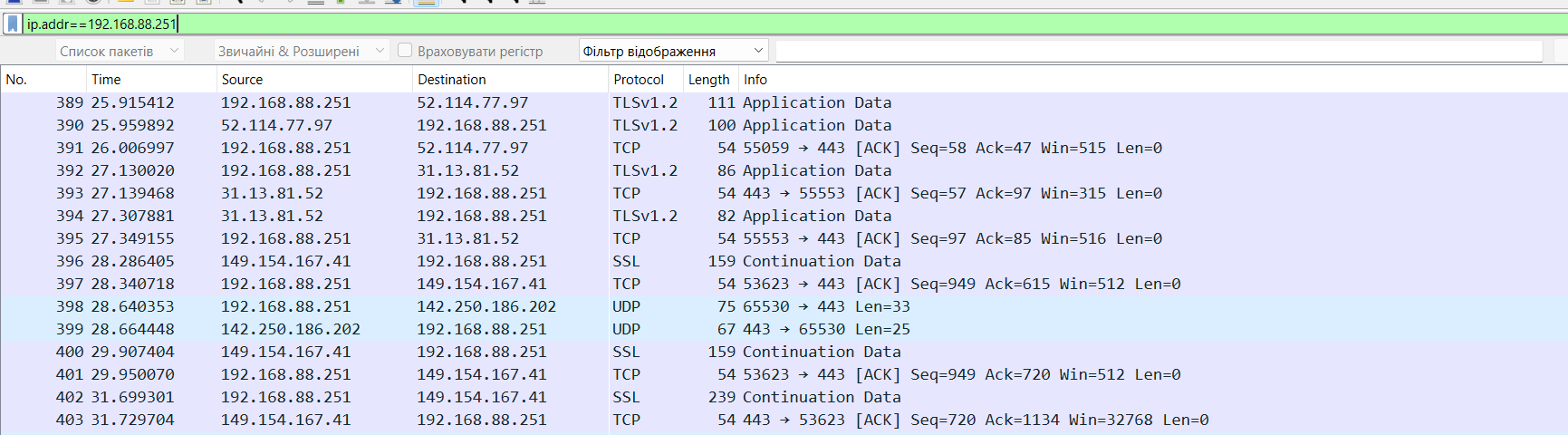
7. Знаходжу пакети, які не стосуються протоколу ІР, натиснувши кнопку пошуку та використавши спеціальний вираз not ip

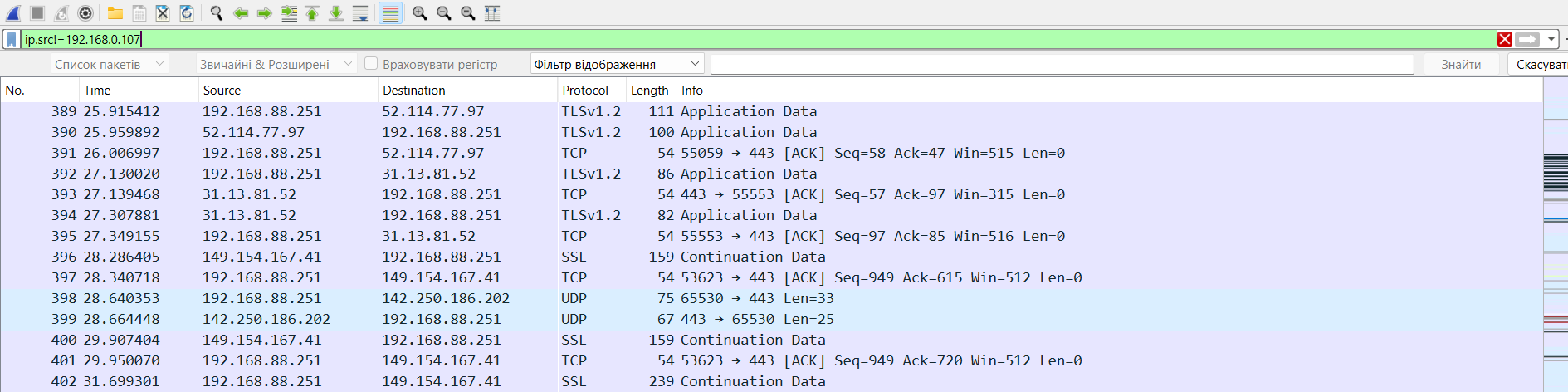


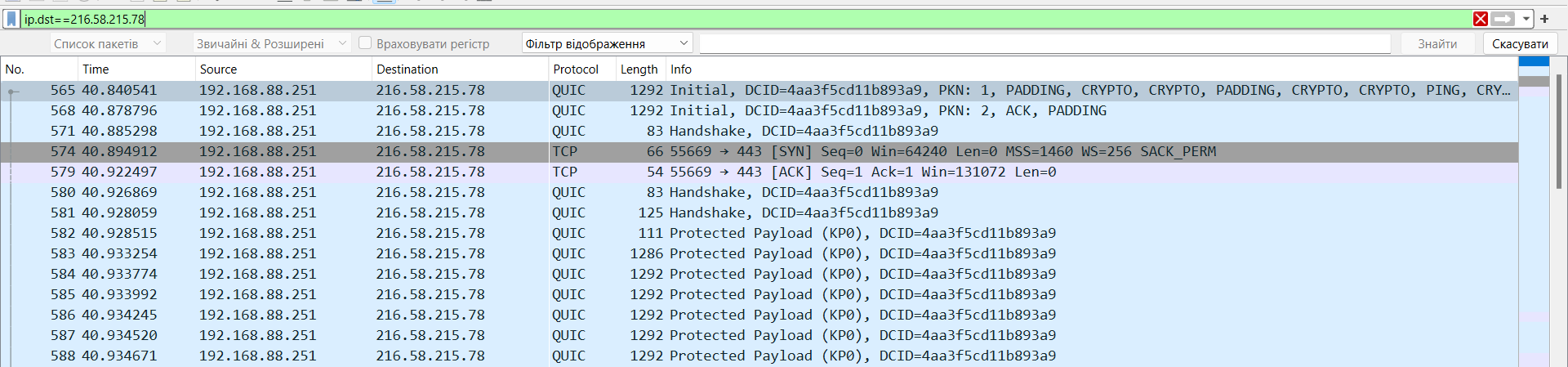




8. Експериментую з різними виразами:







ip.addr==192.168.0.107 – видає пакети із заданою ір адресою, які є джерелом даних або отримувачем.

arp||udp.port==53 – || використовується для логічного або. Виведе порт призначення або вихідний порт що відповідає 53.

ipv6.addr==2001:db8::1 – Фільтрує трафіки що відправлені на відповідний IPv6 адрес

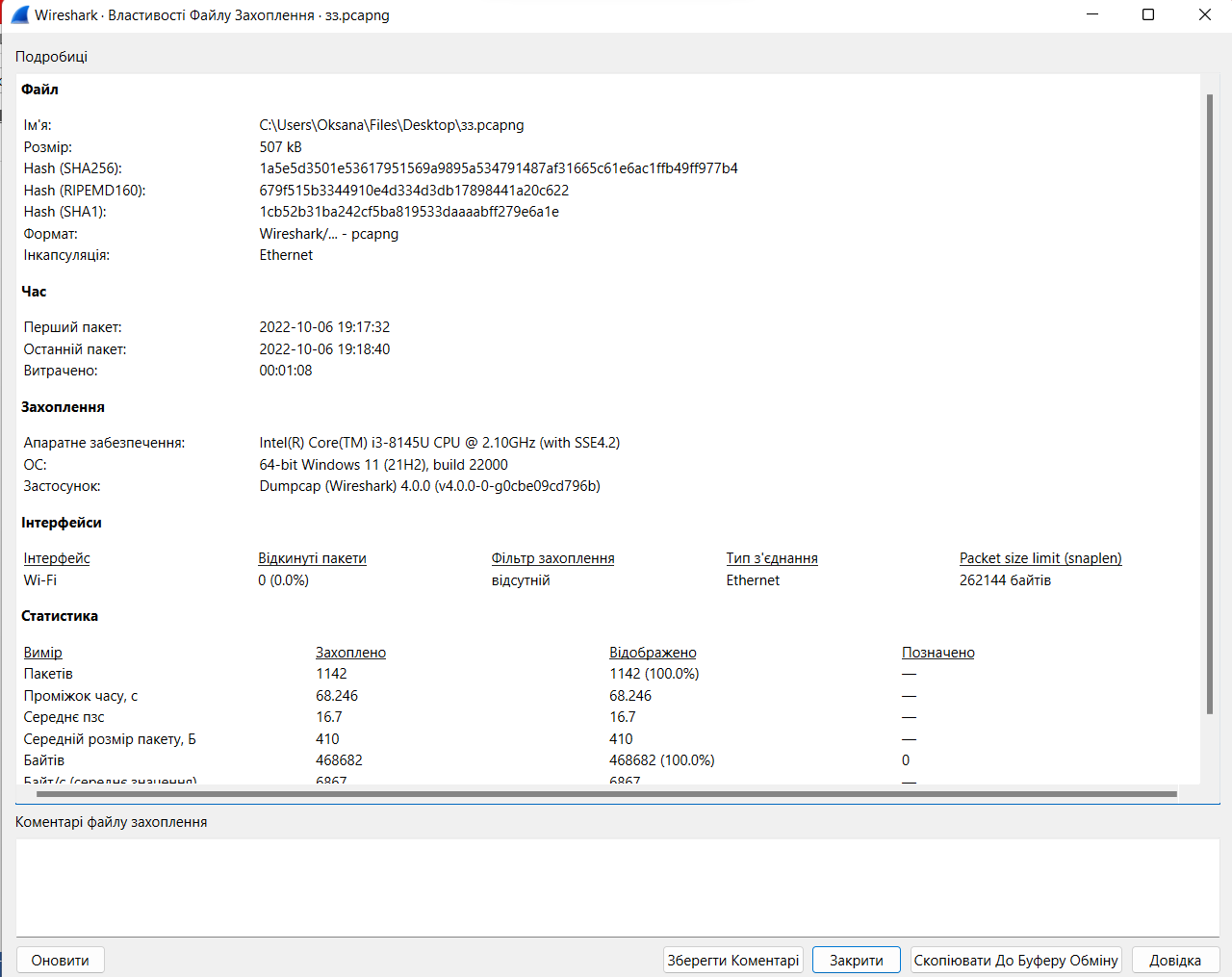
eth.addr==00:00:5e:00:53:00 – Фільтрує Ethernet адреси що відповідають 00:00:5e:00:53:00

ip.src!=192.168.0.107 - відображає трафік, джерелом якого не є хост з вказаною ІР адресою

ip.dst==216.58.215.78 - відображає трафік, джерелом якого є хост з вказаною ІР адресою

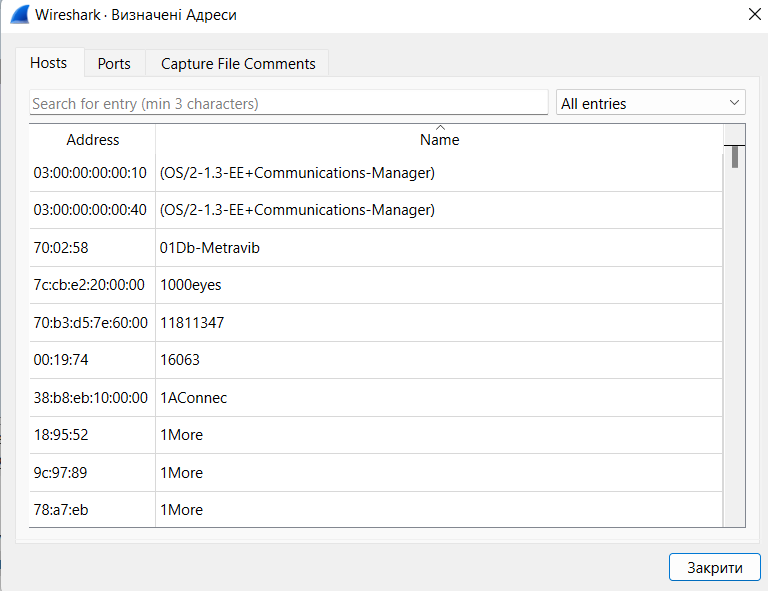
9. Оглянула вміст меню Statistics:

Capture File Properties – показує дані про пакети записані у файлі.



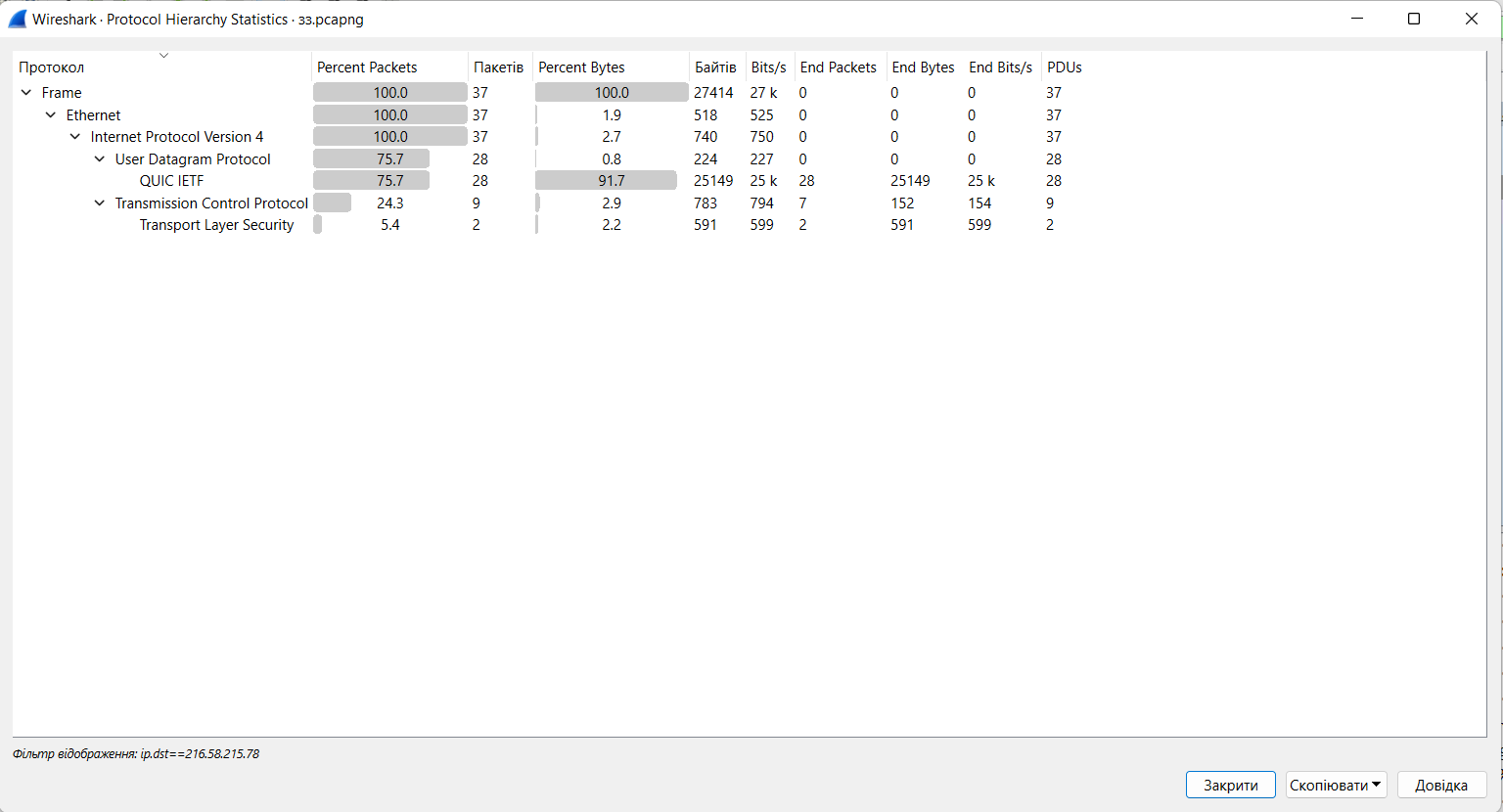
Визначені адреси:

надає список всіх IP-адрес і DNS-імен, які були розпізнані під час захоплення пакетів.

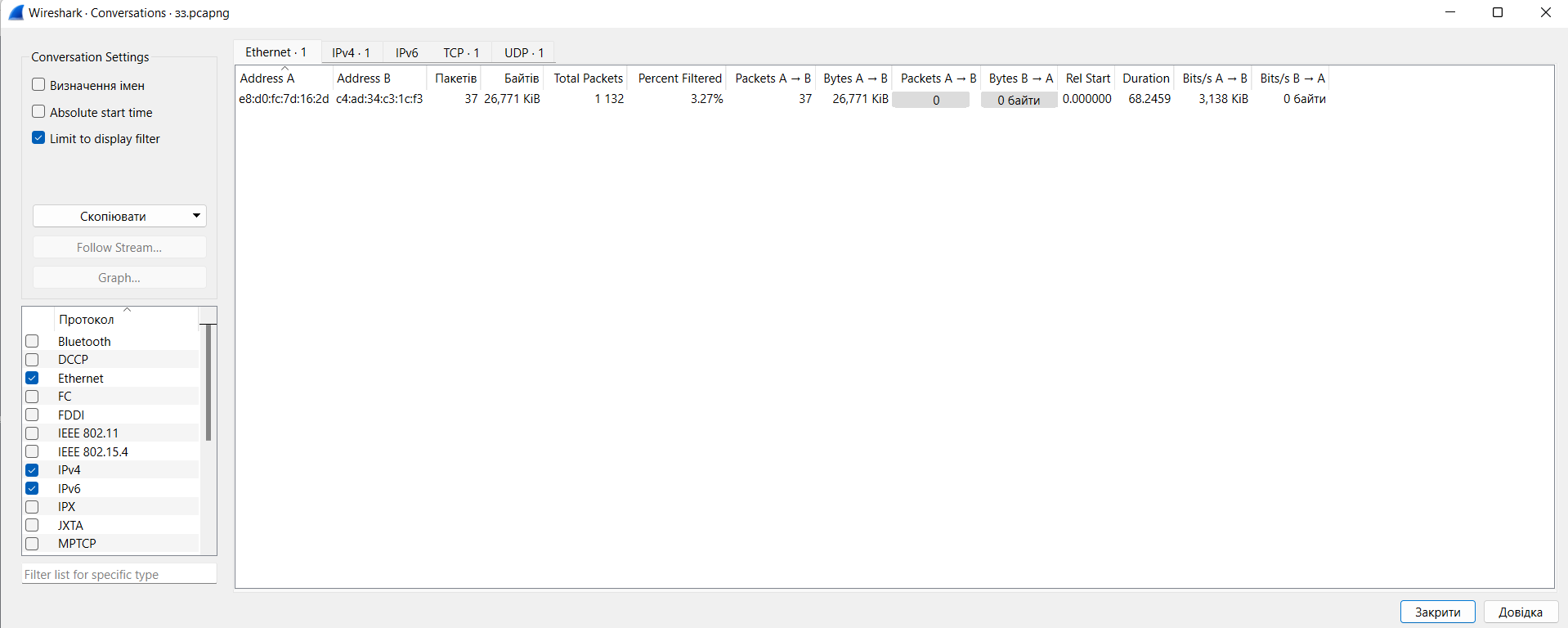


Ієрархія протоколів

Це дерево всіх протоколів захоплення. Кожен рядок містить статистичні значення одного протоколу.

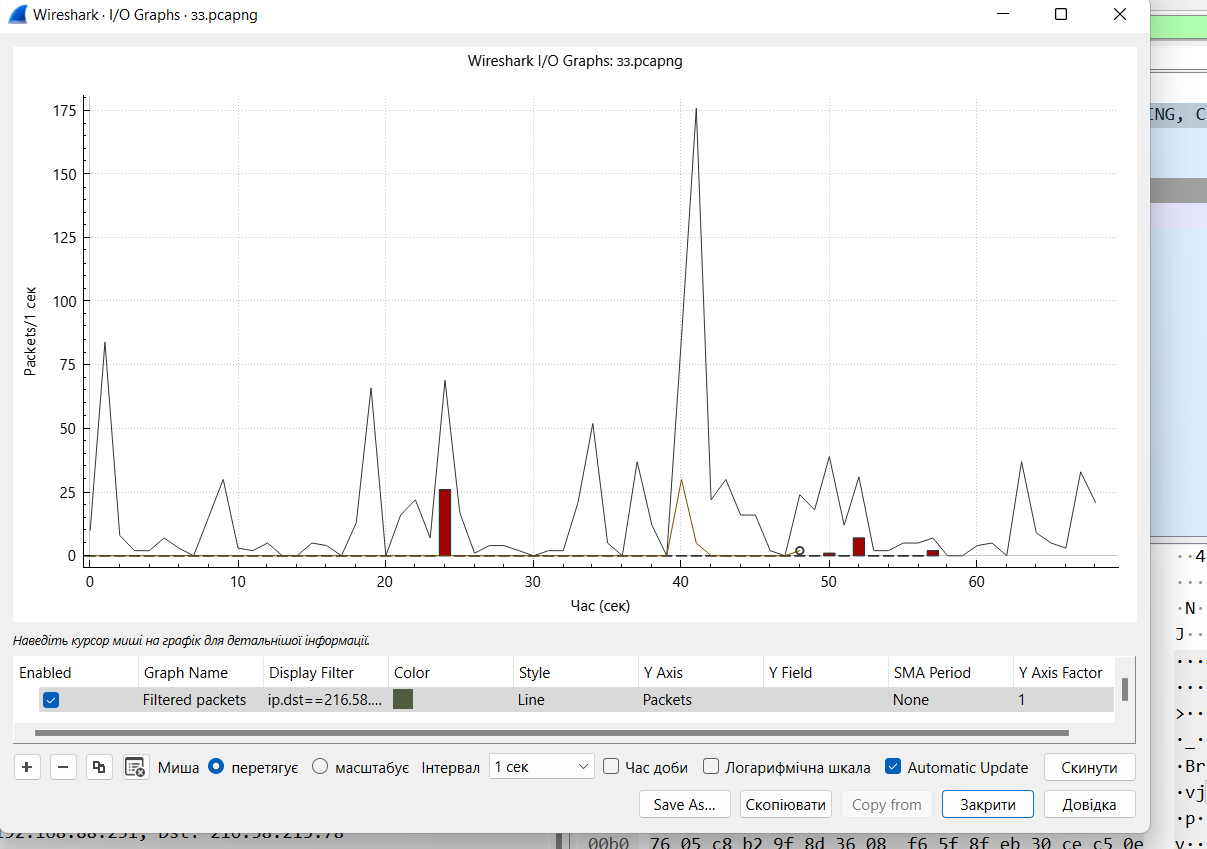


Conversations – інформація про передачу даних між двома конкретними кінцевими точками.



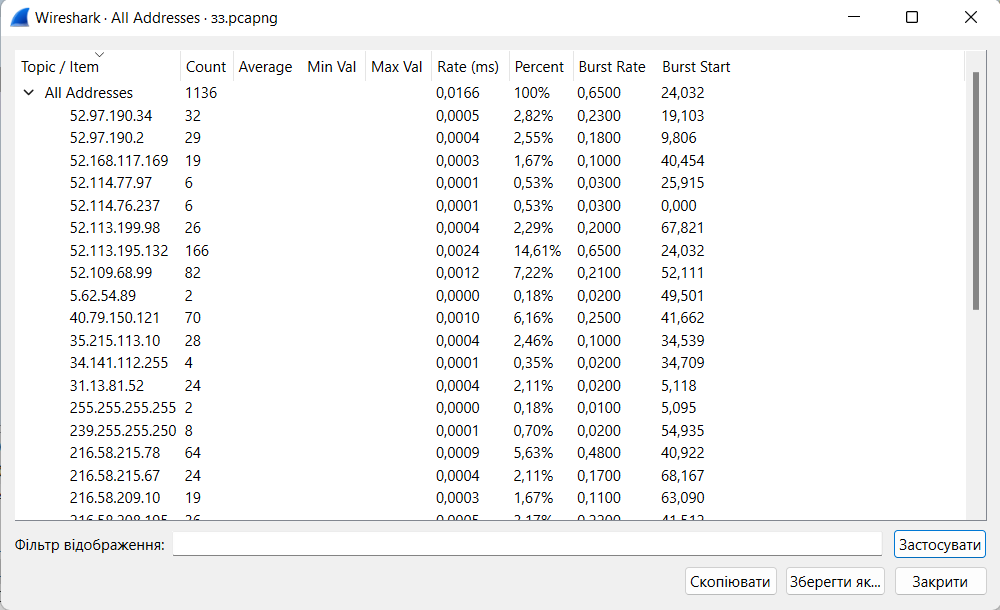
I/O Graph

показує загальний трафік у файлі захоплення, який зазвичай вимірюється у швидкості за секунду в байтах або пакетах



IPv4Statistics

основний протокол для Інтернет-рівня.



Висновок: Отримала загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомилася з графічним інтерфейсом програми та навчилася захоплювати, сортувати та фільтрувати пакети.