ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА
Факультет прикладної математики та інформатики

Комп’ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №3

Інтерфейс аналізатора пакетів Wireshark

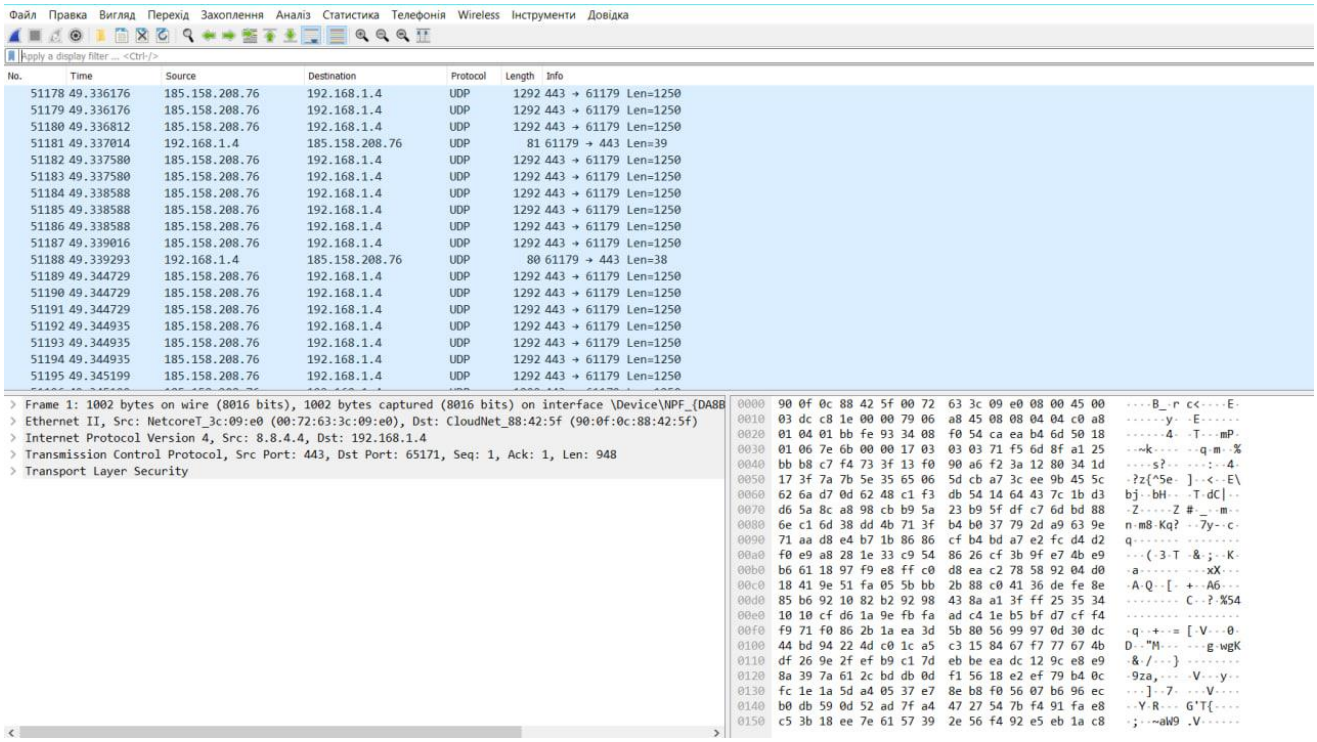
Виконав:
Студент групи ПМі-31
Яцуляк Андрій

2023

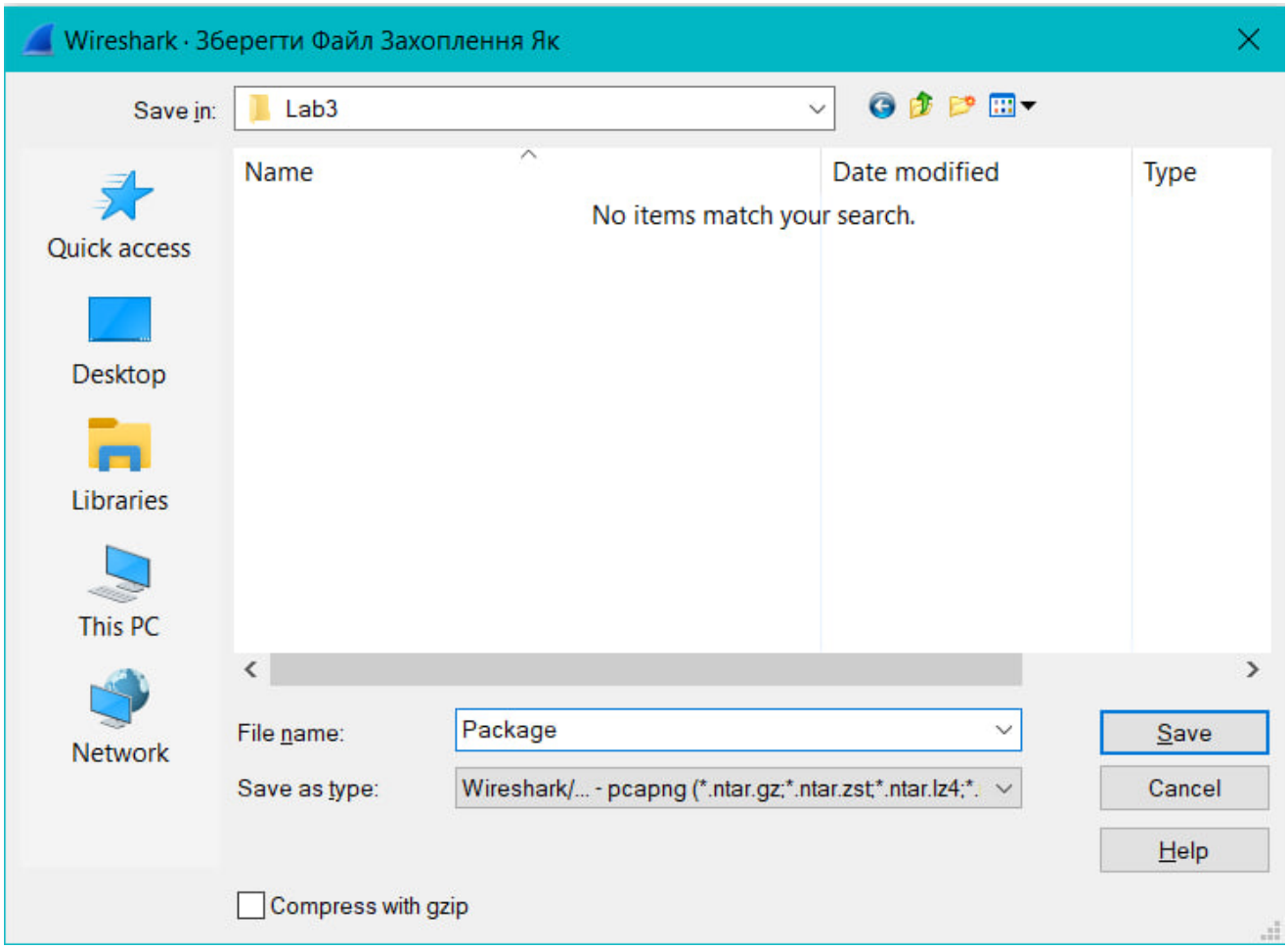
Мета: Отримати загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомитися з графічним інтерфейсом програми, навчитися захоплювати, сортувати та фільтрувати пакети.

Хід роботи

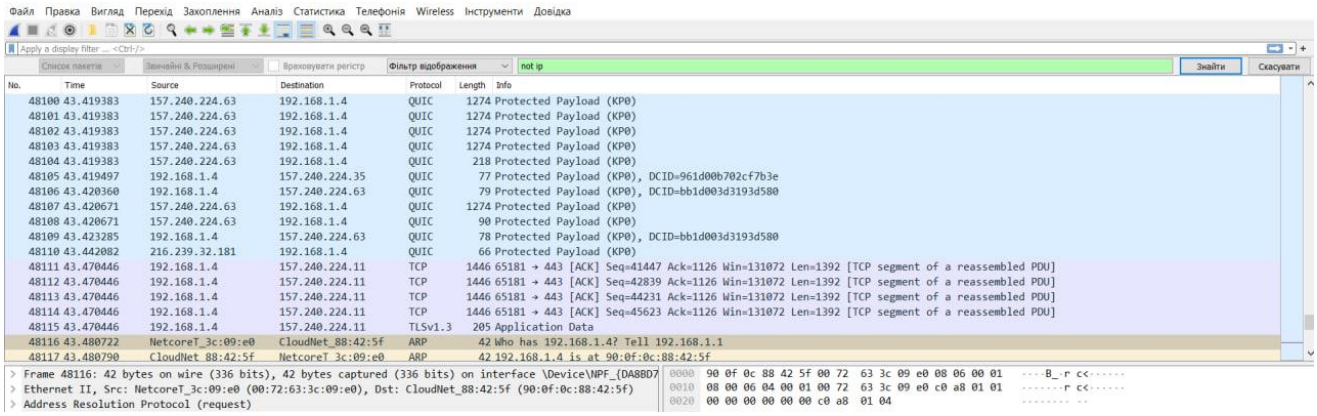
1. Опрацював теоретичний матеріал.
2. Запустив аналізатор мережевих пакетів Wireshark від імені адміністратора.
3. Вибрав з переліку потрібний мережевий інтерфейс та почав процедуру.
4. Упродовж 60 секунд здійснив активність в браузері (перейшов на сайт, залогінився, скачав файл).
5. Зупинив процедуру захоплення пакетів.
6. Ознайомився з трьома основними елементами головного вікна програми:



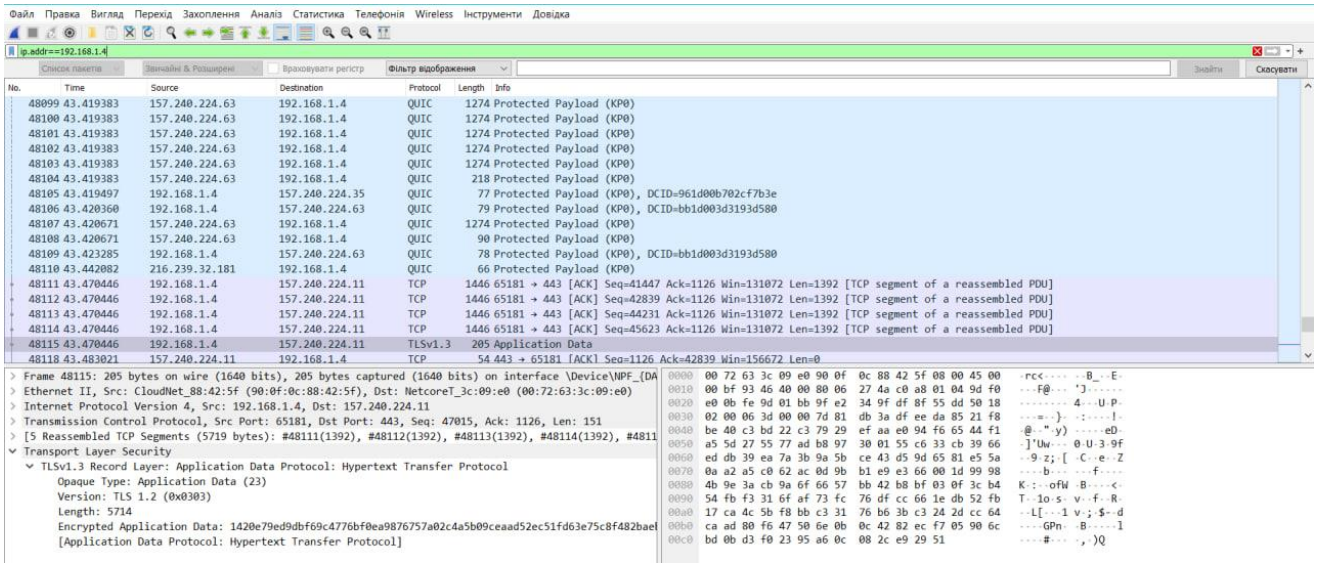
7. Зберіг захоплені пакети у файл для подальшого аналізу:



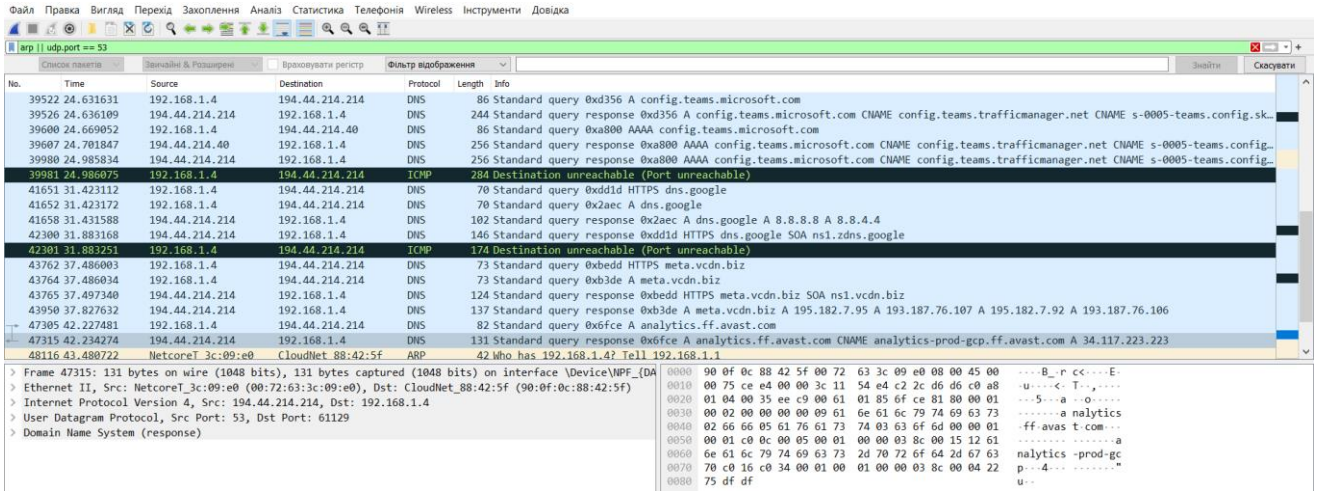
8. Знайшов пакети, які не стосуються протоколу IP, натиснувши кнопку пошуку та використавши спеціальний вираз **not ip**:



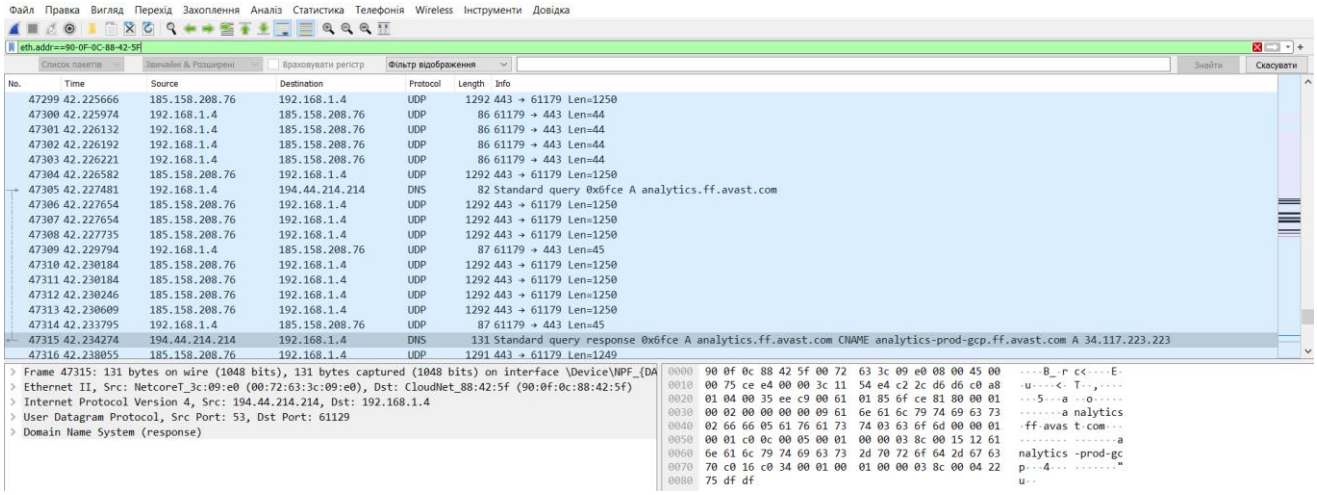
9. Поекспериментував з різними виразами:
   - ip.addr == 192.168.1.4 – пакети, які були відправлені з мого IPv4 або отримані ним:



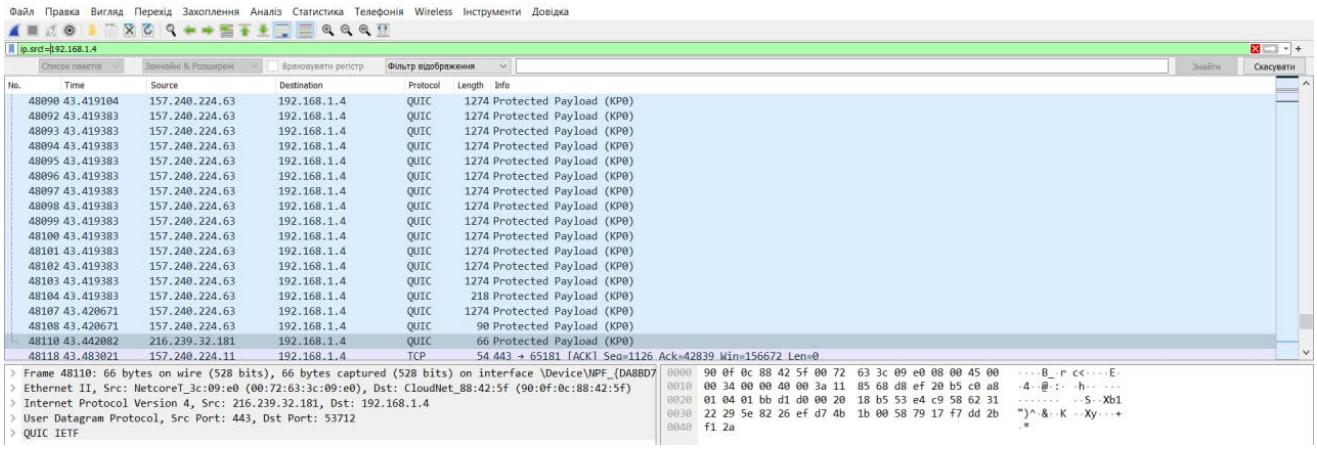
- arp || udp.port == 53 – пакети, які були відправлені протоколом ARP або через UDP порт 53:



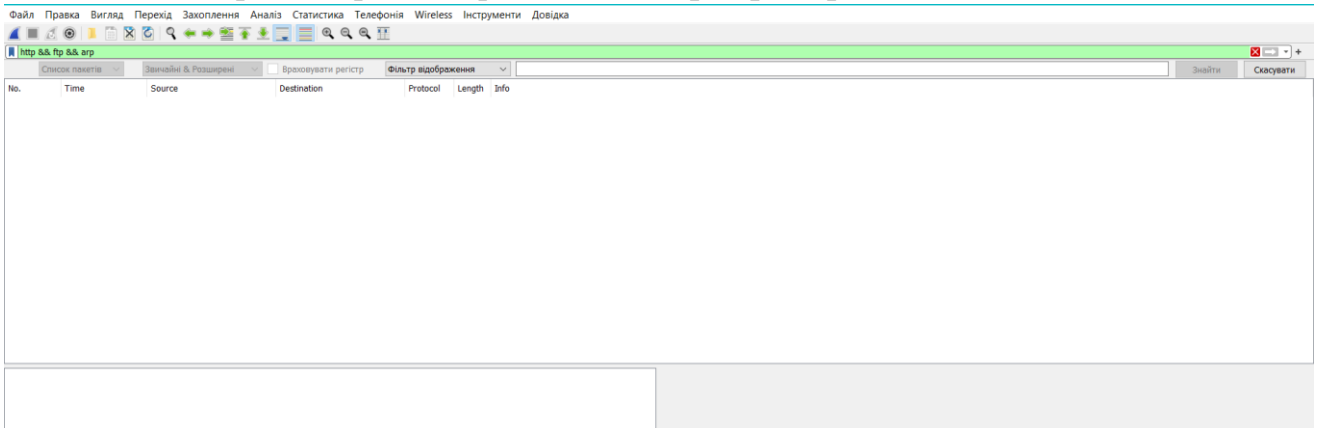
- eth.addr == 90-0F-0C-88-42-5F – пакети, які були відправлені або отримані фізичною адресою мого адаптеру:



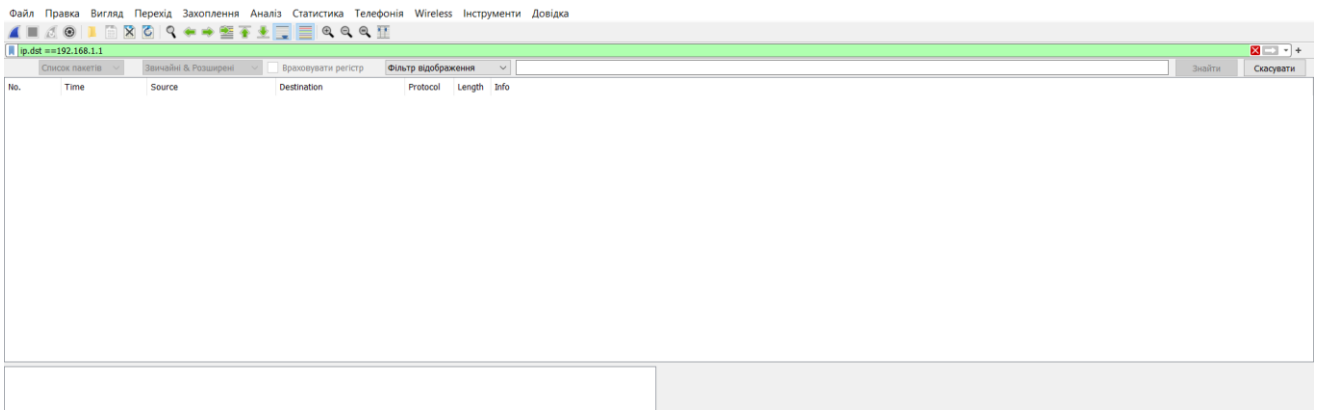
- ip.src!=192.168.1.4 – пакети, які були відправлені НЕ з мого IPv4:



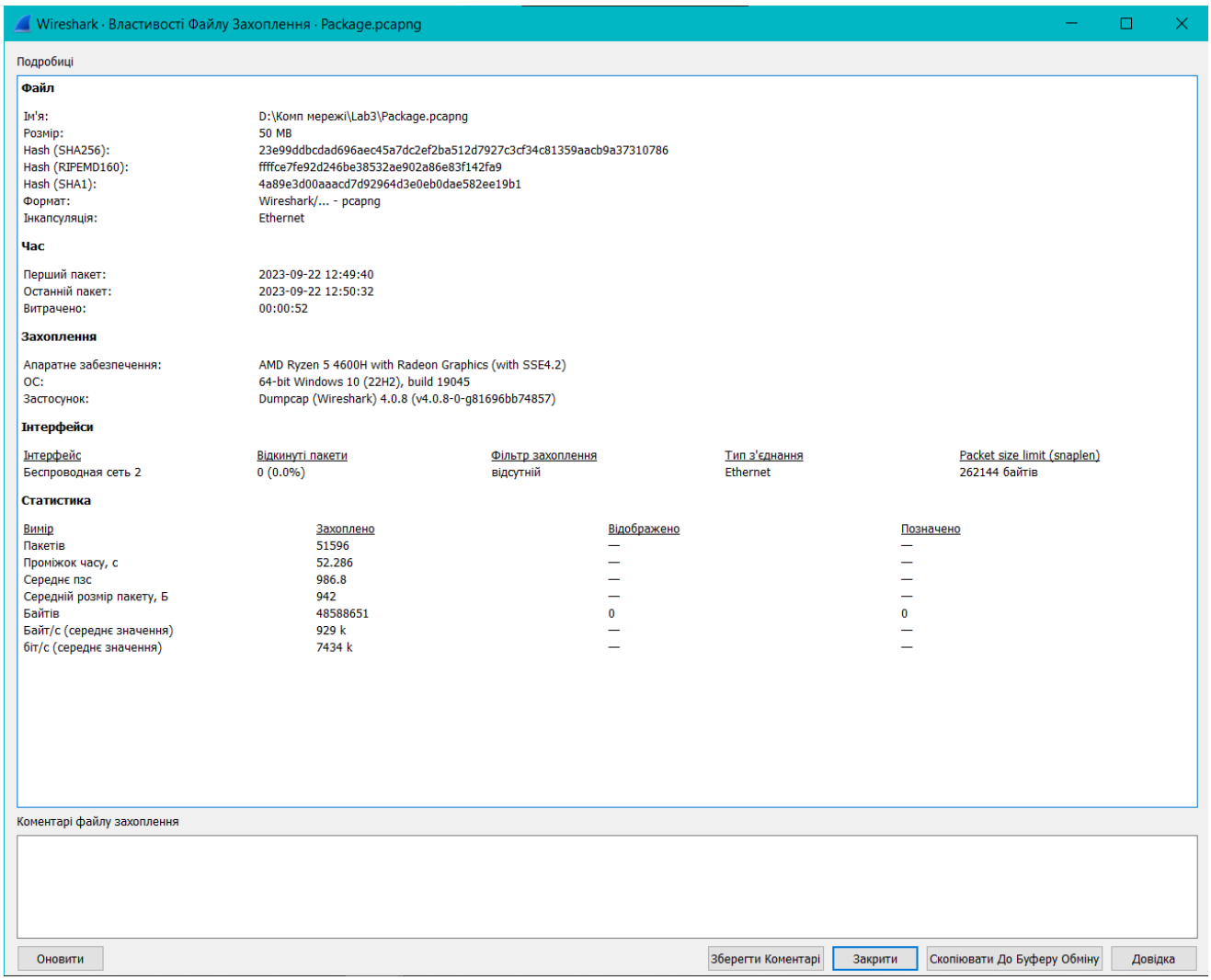
- http && ftp && arp – пакети http, ftp і arp:



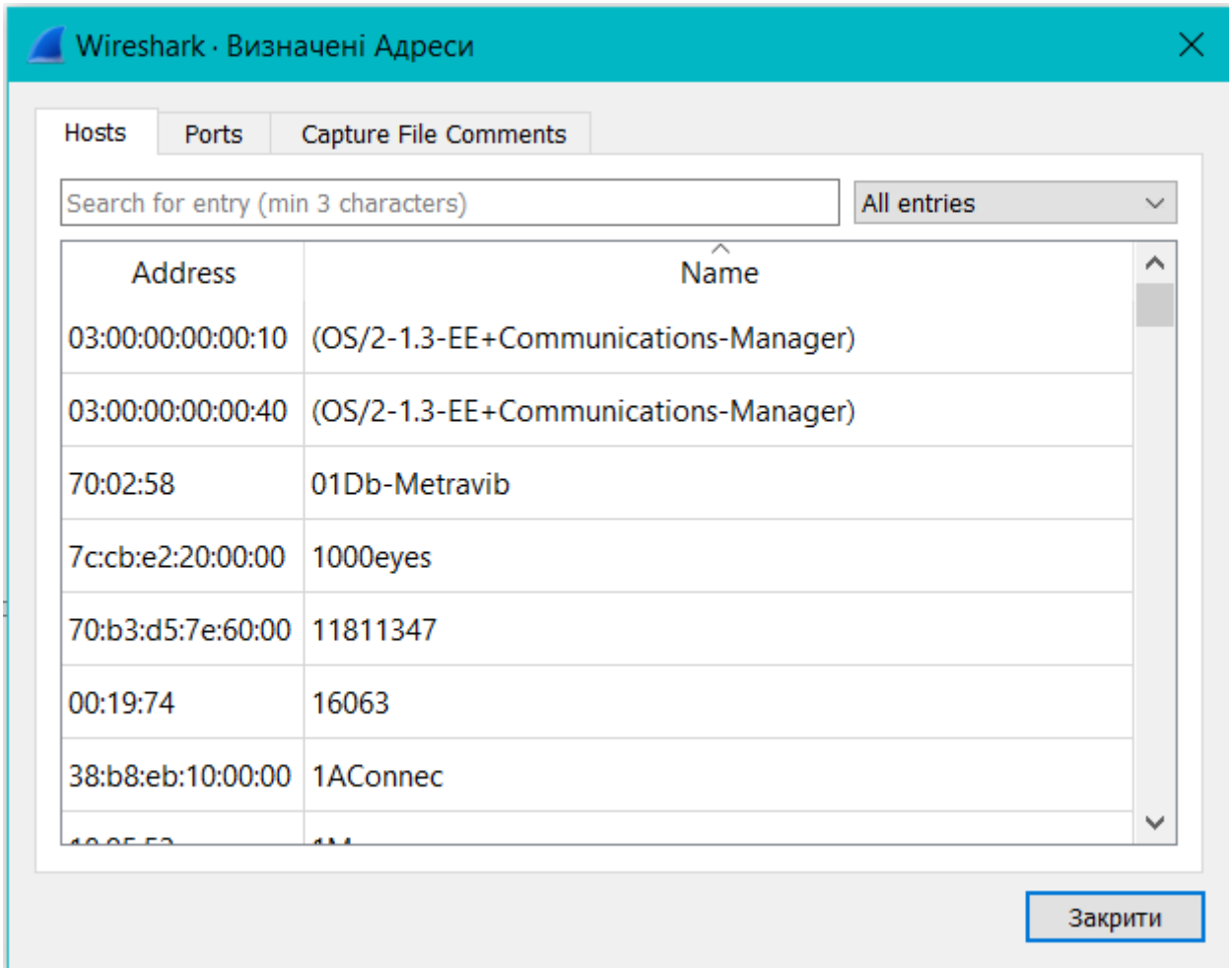
- ip.dst == 192.168.1.1 – пакети, отримані моїм локальним IP:



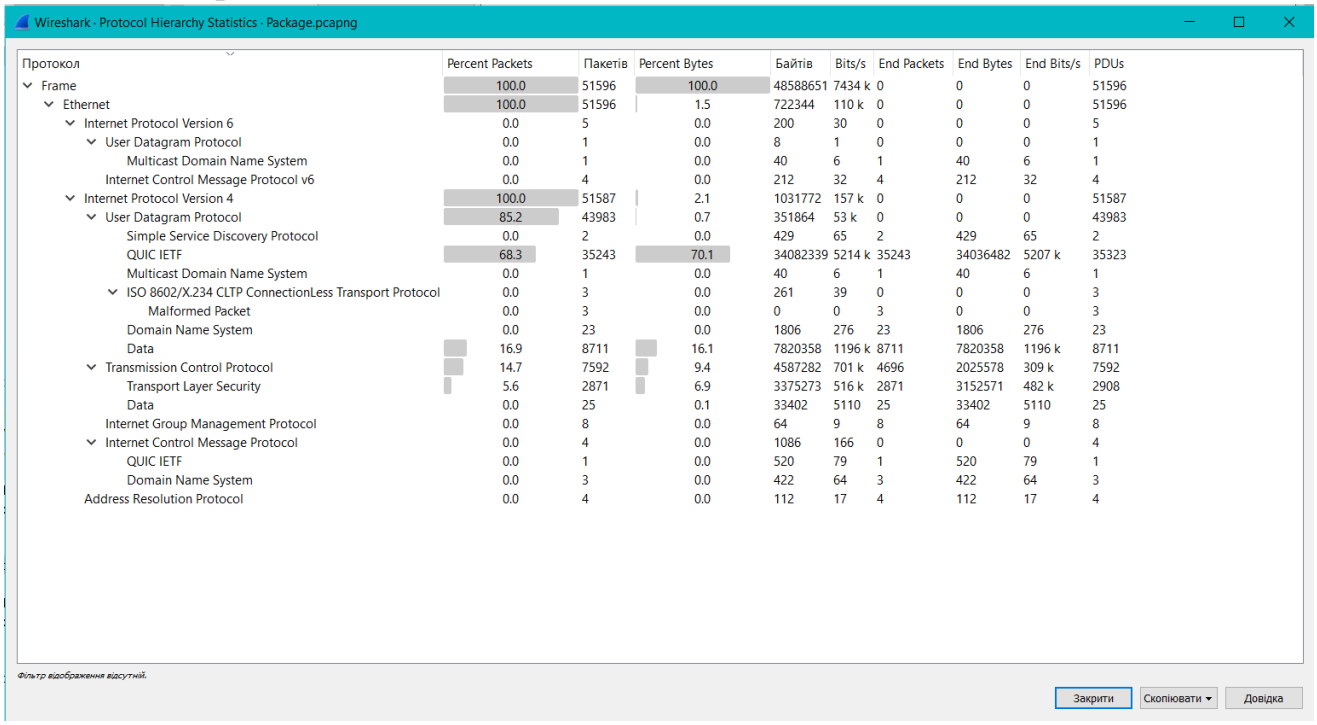
10. У меню Statistics вибрав по черзі пункти Capture File Properties, Resolved Adresses, Protocol Hierarchy, Conversations, I/O Graph, IPv4 Statistics та ознайомився з інформацією:
    - Capture file properties – показує дані про пакети записані у файлі, час, та статистику пакетів:



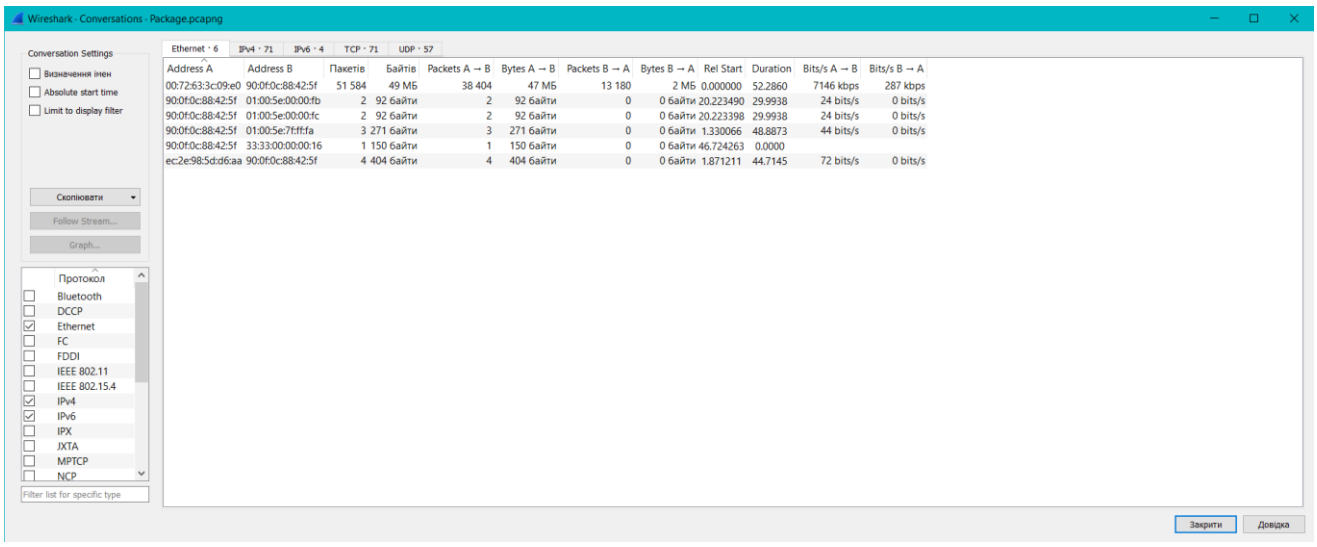
- Resolved addresses має фізичні адреси, які отримували пакети або відправляли, а також порт та протокол за яким відправлено в другій вкладці:



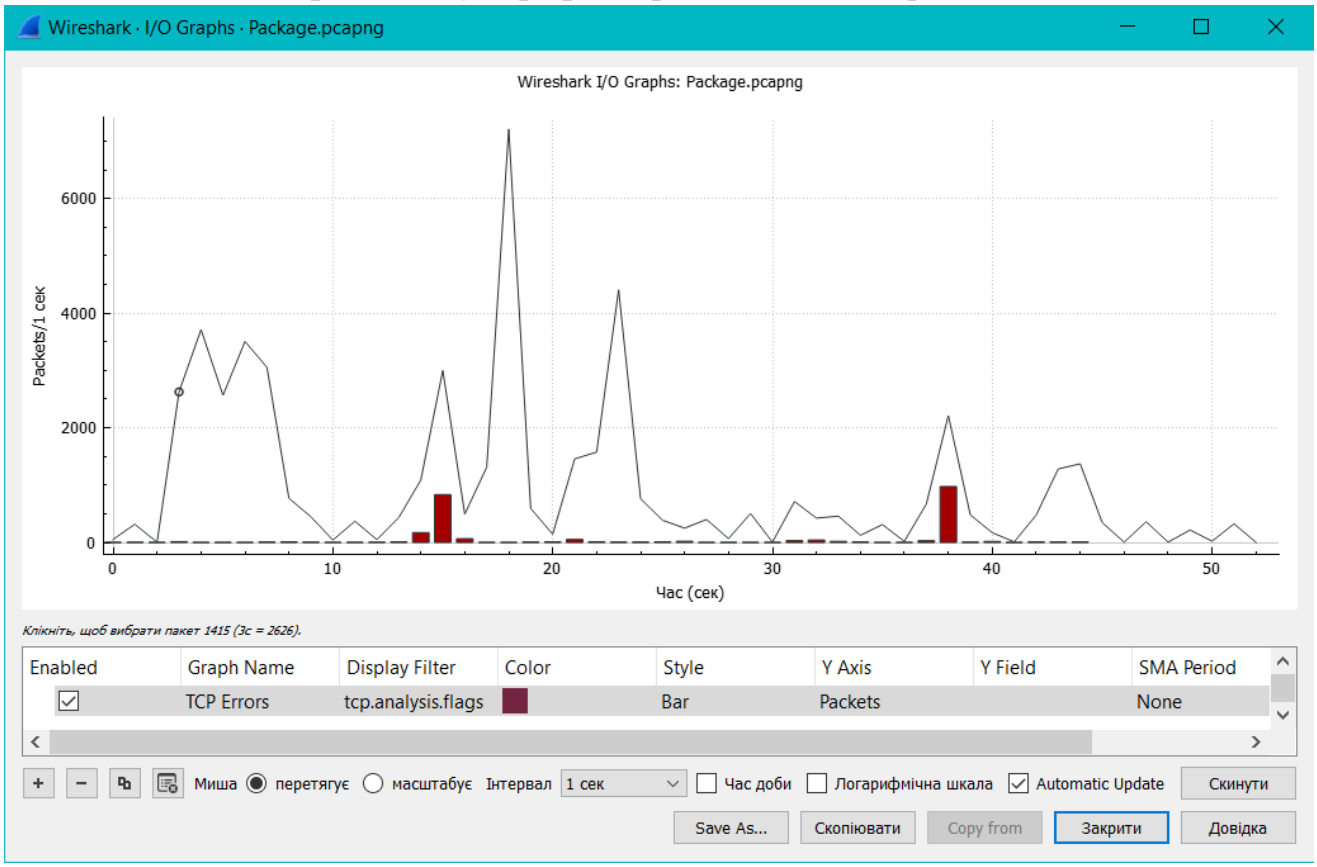
- Protocol hierarchy показує ієрархію розподілення пакетів по протоколах:



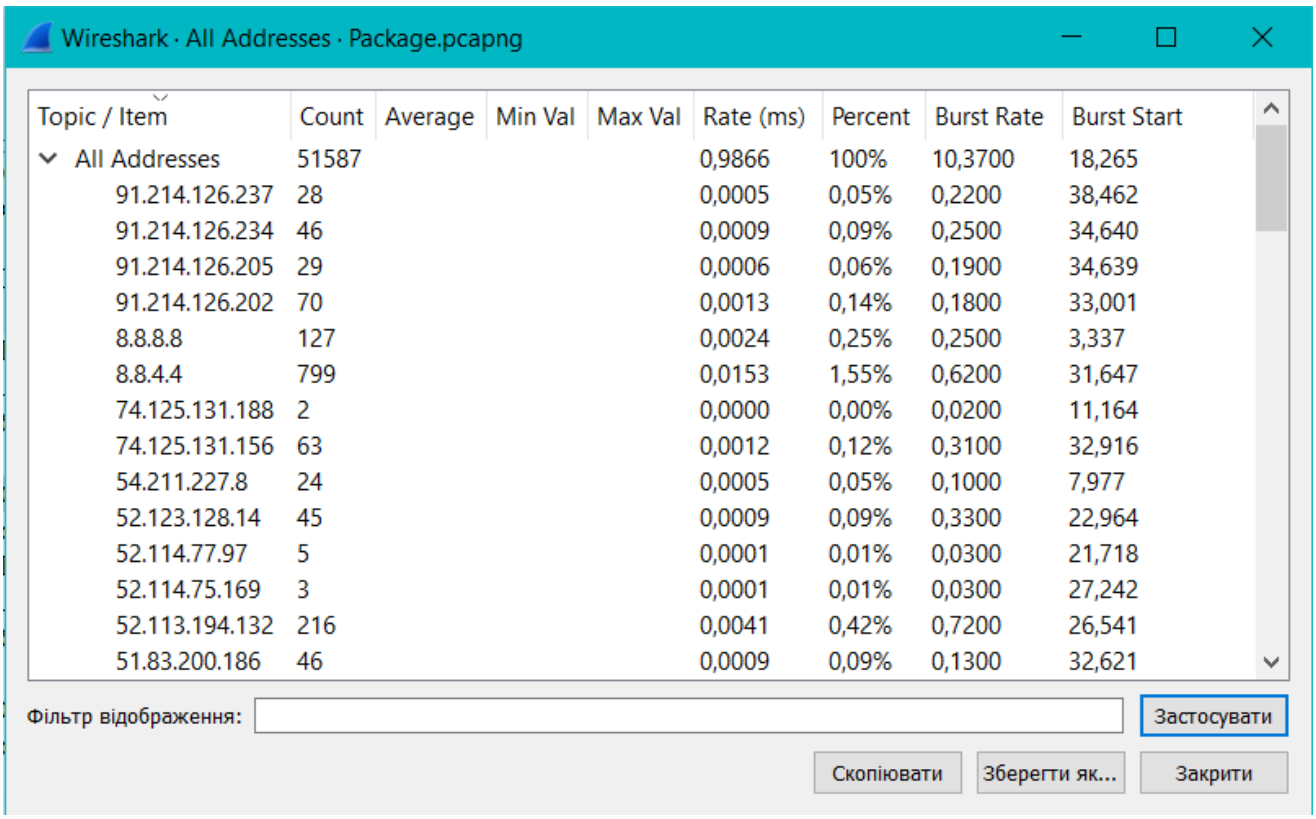
- Conversations показує сумарні дані передачі даних між фізичними адресами, IP, тощо:



- I/O Graphs показує графік отриманих та відправлених пакетів:



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



Висновок. Під час виконання лабораторної роботи я отримав загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомився з графічним інтерфейсом програми, навчився захоплювати, сортувати та фільтрувати пакети.