Міністерство освіти і науки України

Львівський національний університет імені Івана Франка

Факультет прикладної математики та інформатики

Кафедра програмування

Звіт

до лабораторної роботи №3

з теми

**“Інтерфейс аналізатора пакетів Wireshark”**

Підготував:

cтудент ПМІ-31

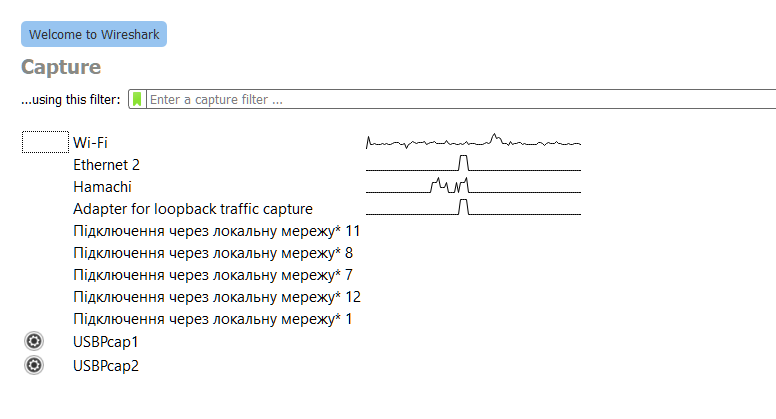
Процьків Назарій

Львів 2023

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

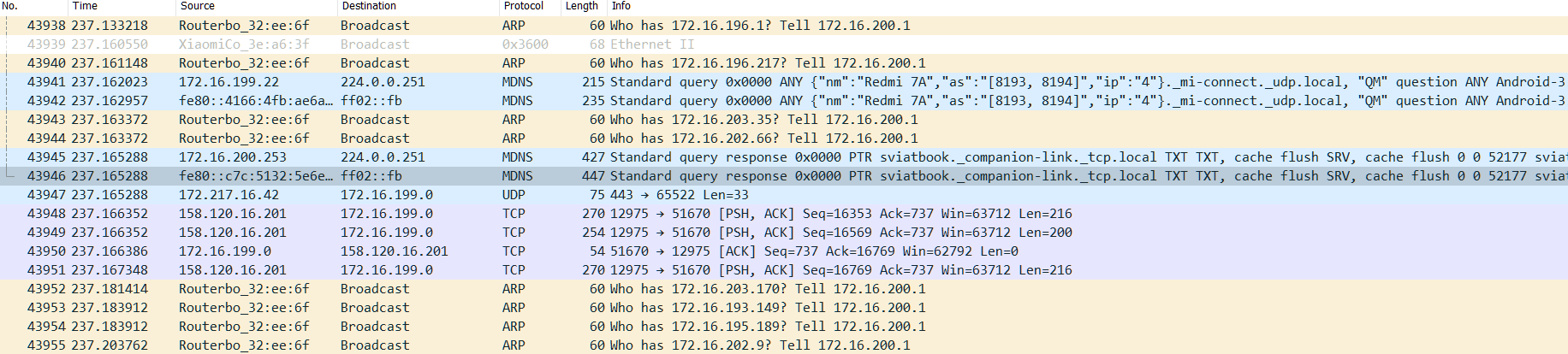
**Хід роботи**

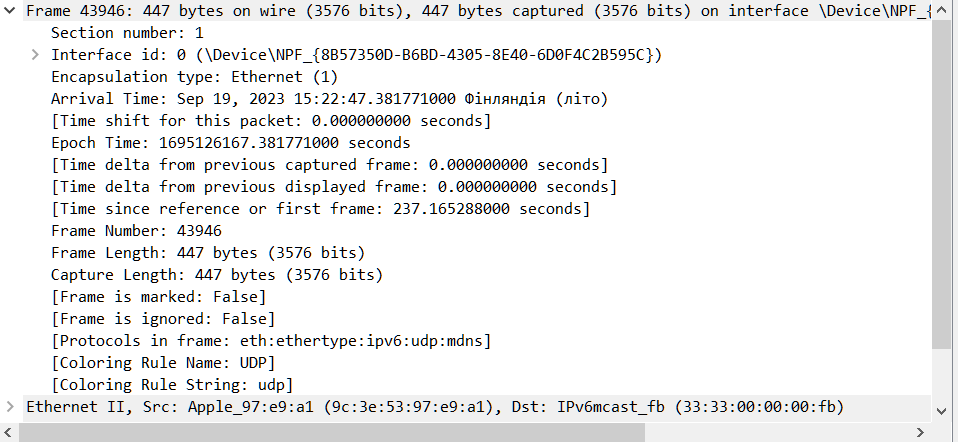
1. Для виконання цієї лабораторної інсталював аналізатор мережевих пакетів Wireshark та Npcap, драйвер для захоплення мережевого трафіку.
2. Відкрив його у режимі адміністратора:

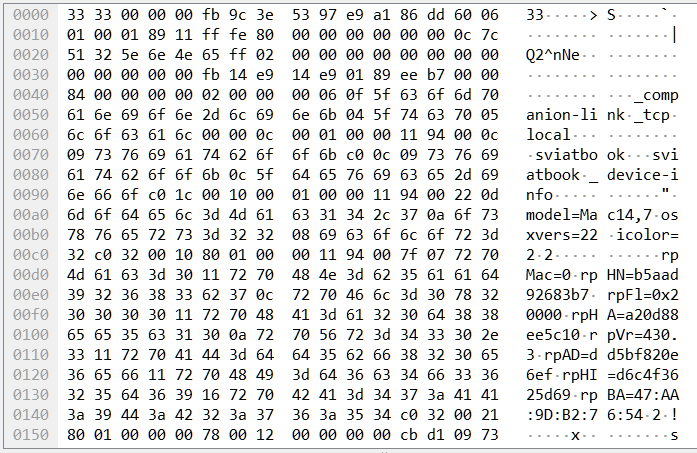


Обрав з переліку потрібний мережевий інтерфейс та почав процедуру захоплення пакетів.

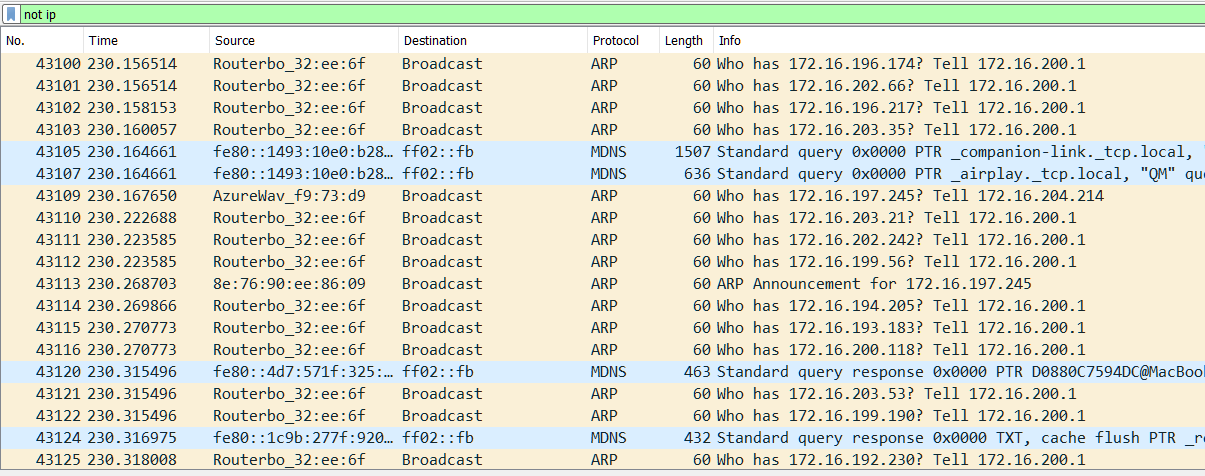
1. Здійснив перехід на сайт у браузері.
2. Ознайомився з трьома основними елементами головного вікна програми.



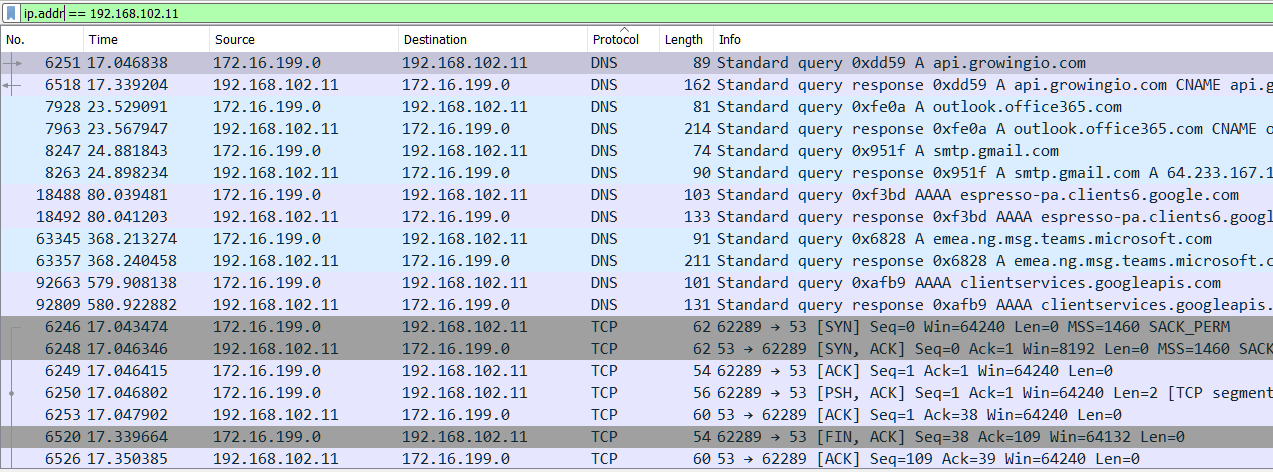




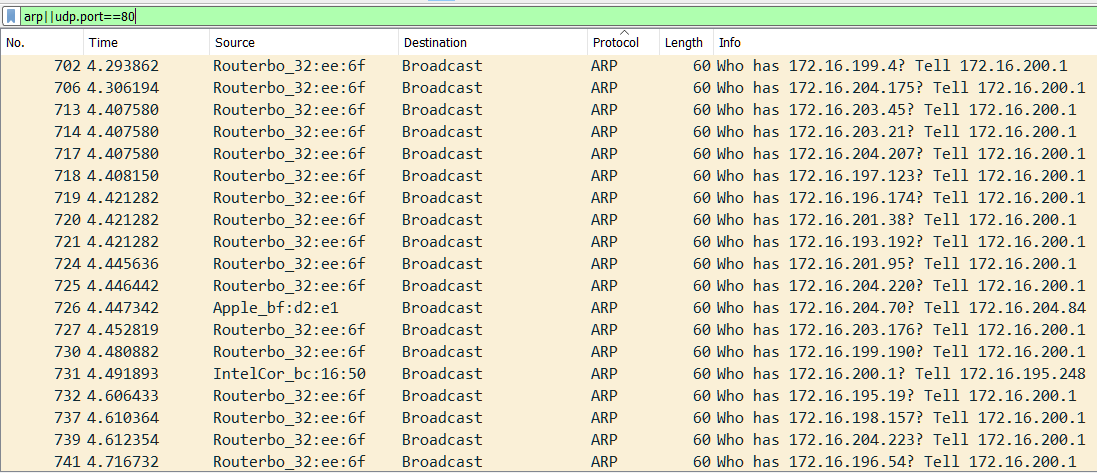
1. Зберіг файл для подальшого аналізу.
2. Натиснувши кнопку пошуку та використовуючи спеціальний вираз **not ip**, знайшов пакети, які не стосуються протоколу ІР:



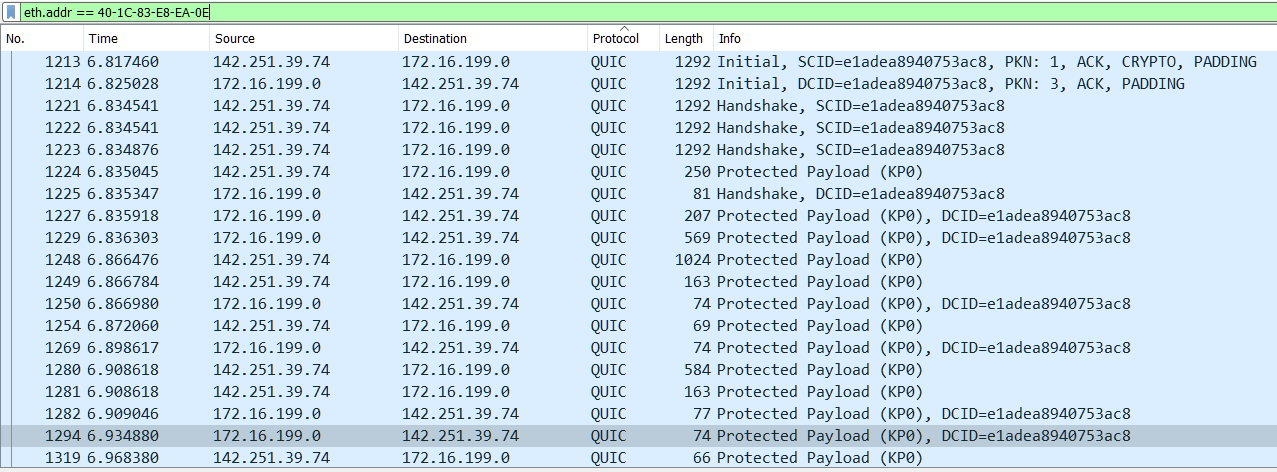
1. Знайшов пакети відправлені з мого локального IP або отримані ним:



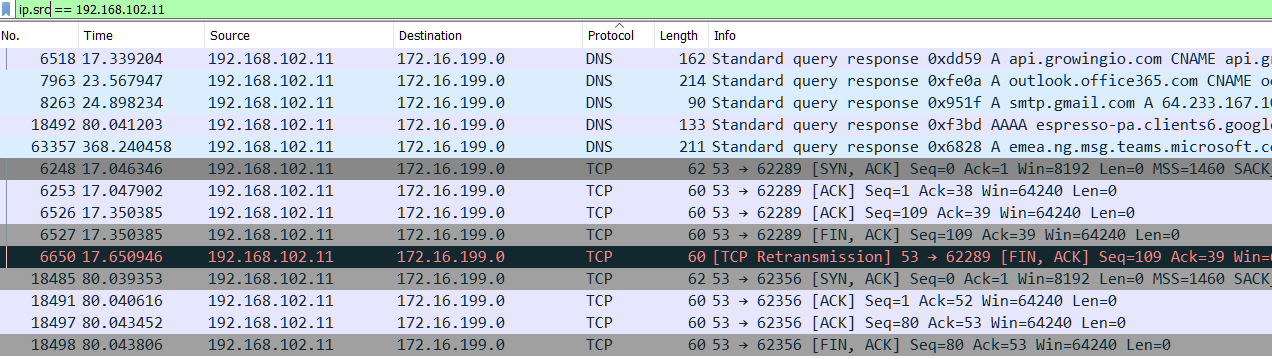
1. Також знайшов пакети відправлені протоколом ARP або через UPD порт 80:



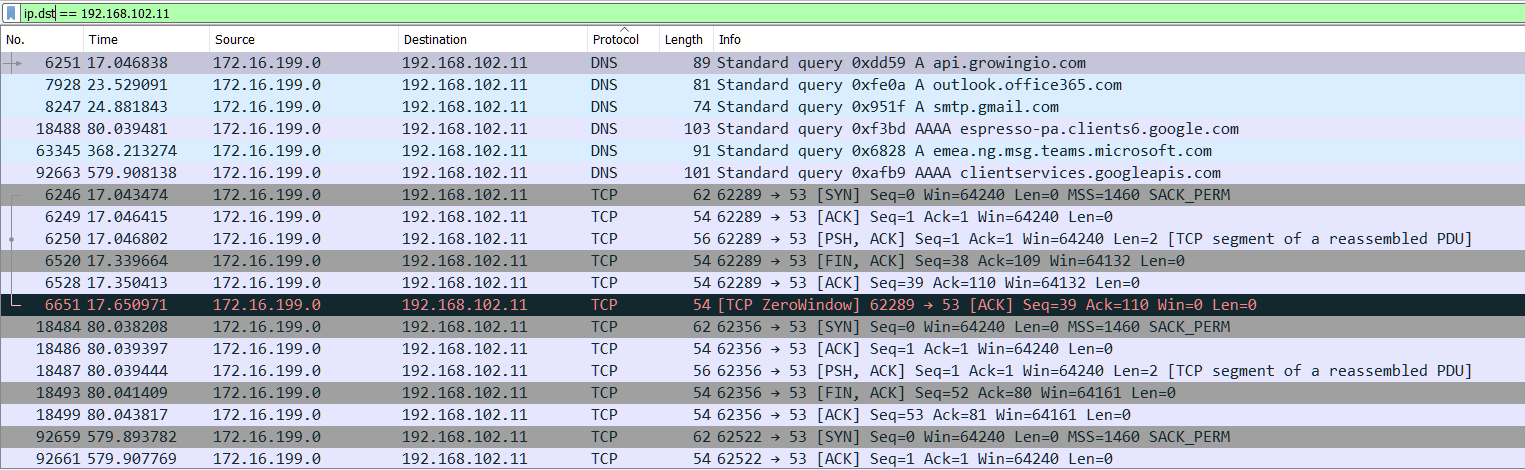
1. Пакети відправлені та отримані фізичною адресою мого адаптера:



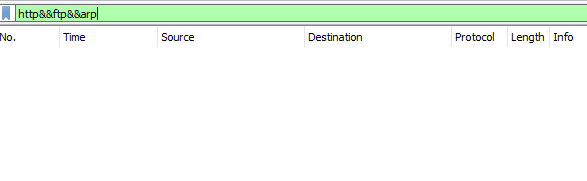
1. Пакети відправлені з мого локального IP:



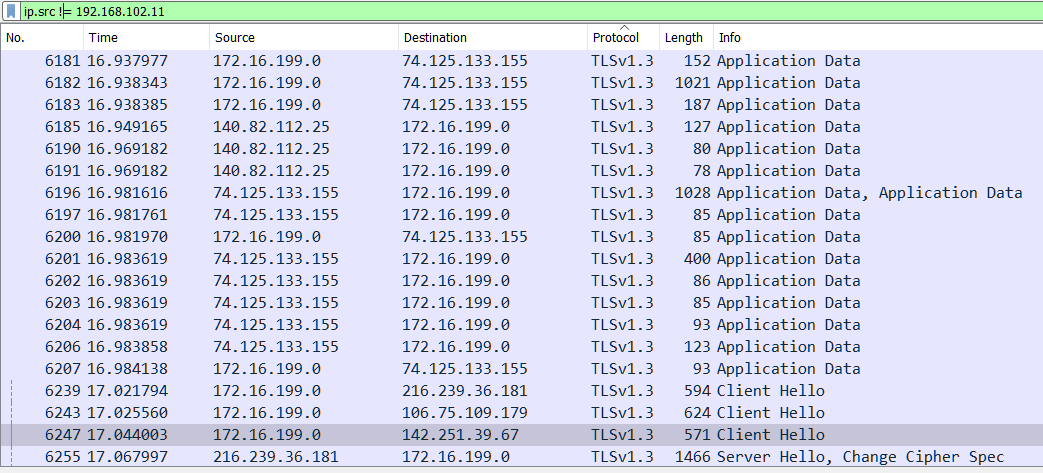
1. Пакети отримані моїм локальним IP:



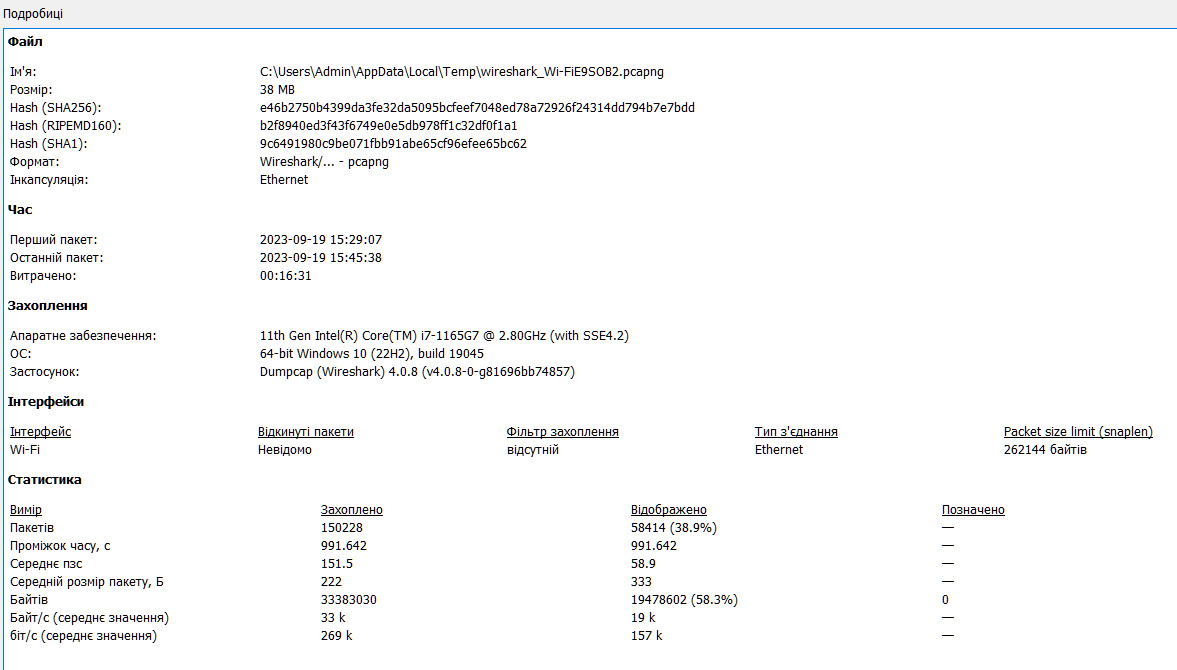
1. Пакети http && ftp && arp:



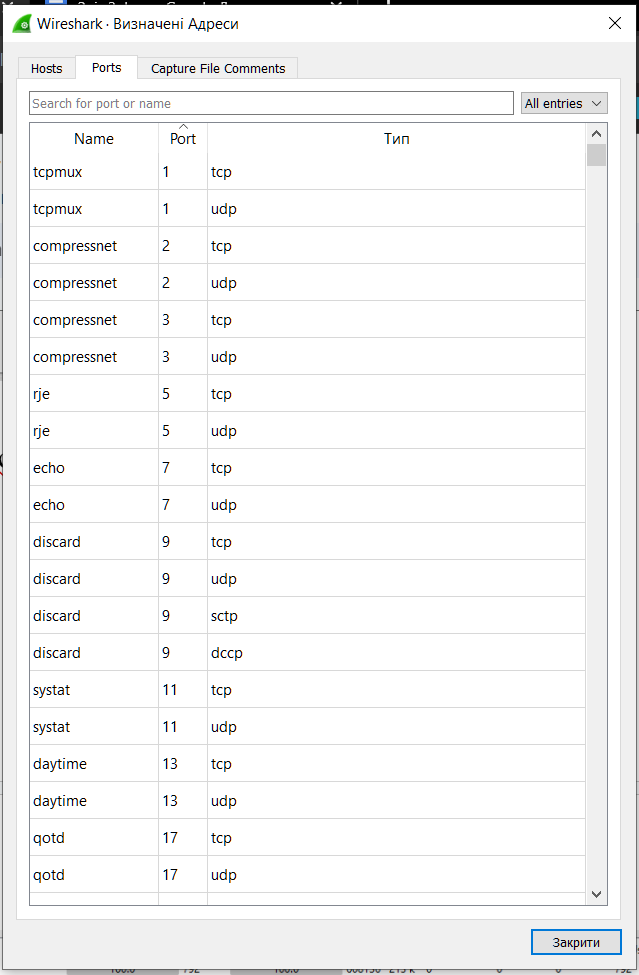
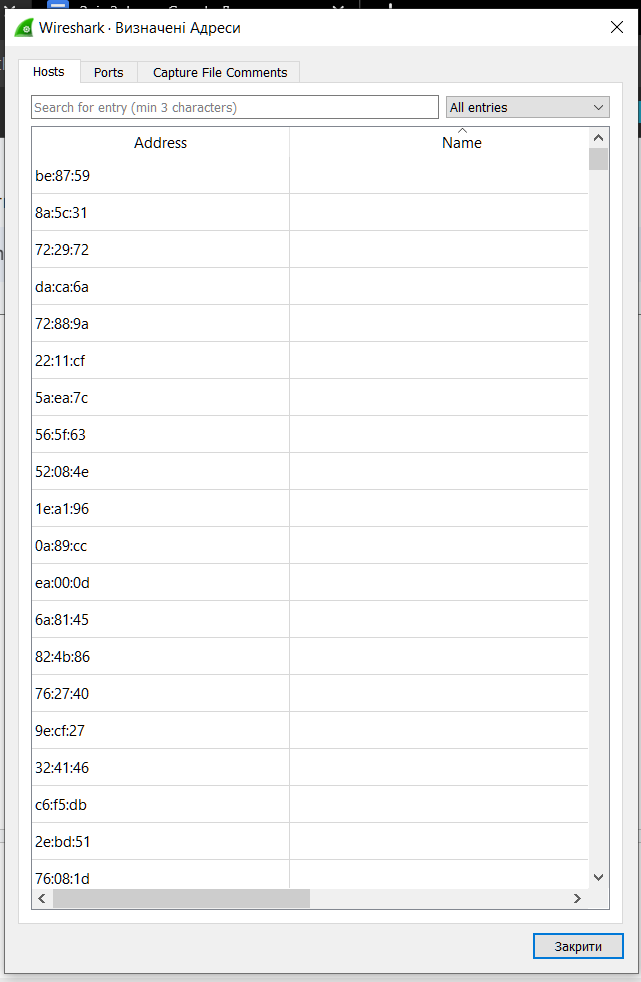
1. Пакети відправлені не з моєї локальної IP адреси:



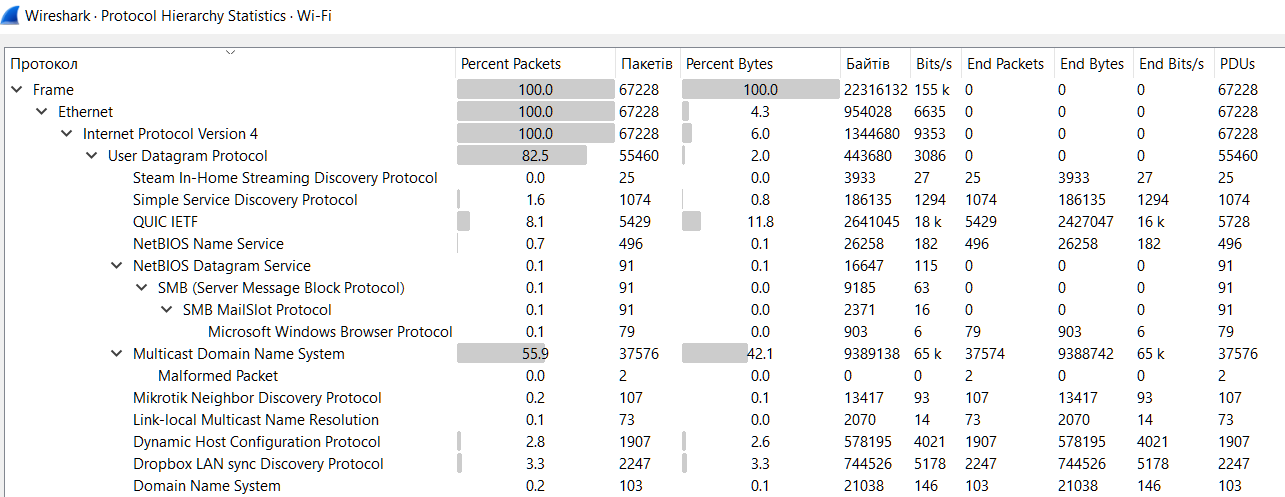
1. Ознайомився з пунктами у меню Statistics.
2. CaptureFileProperties – показує дані про пакети записані у файлі, час, та статистику пакетів.



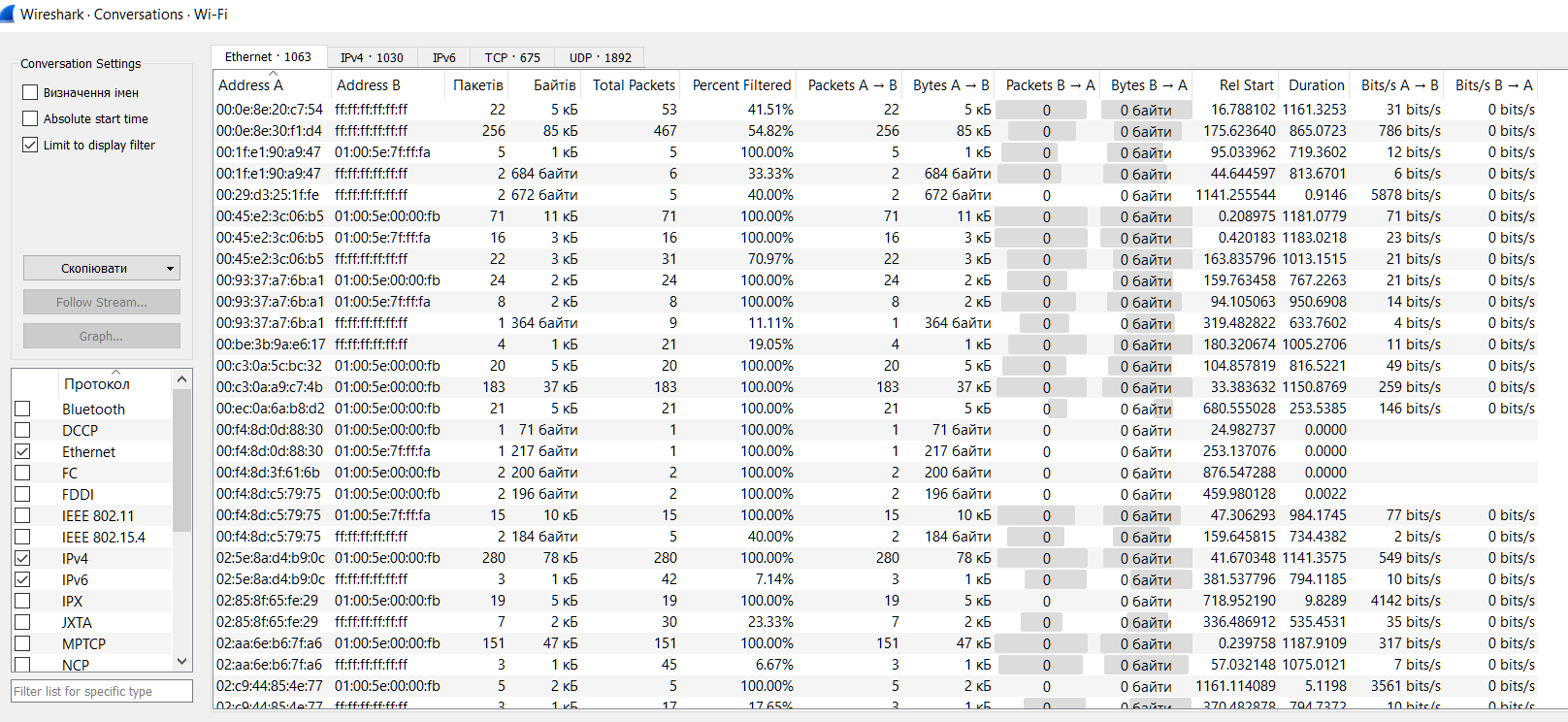
1. ResolvedAddresses – має фізичні адреси, які отримували пакети або відправляли, а також порт та протокол за яким відправлено в другій вкладці.



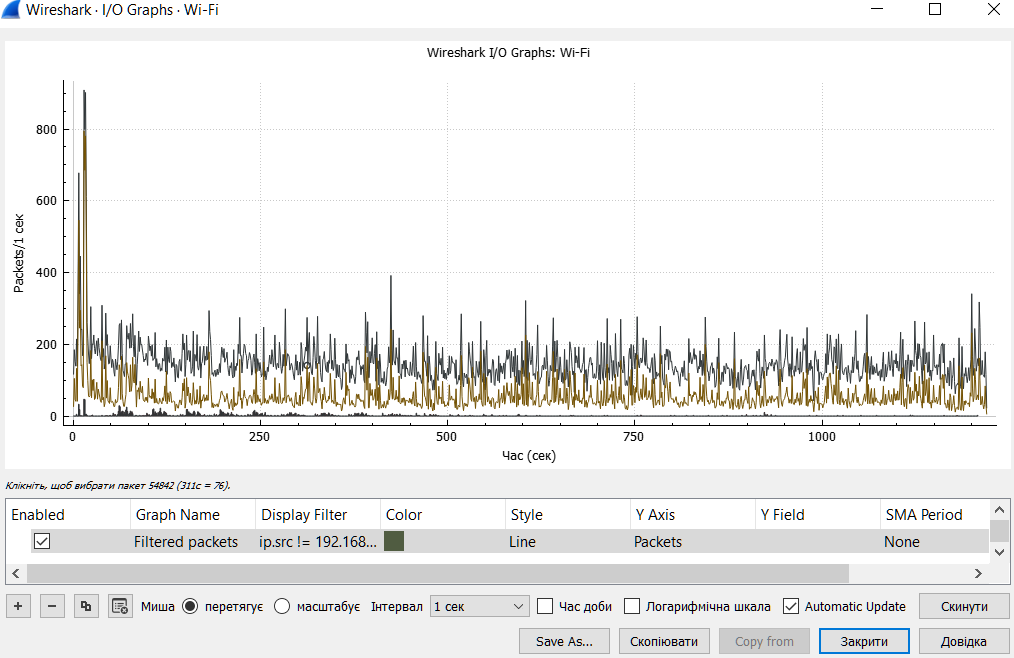
1. ProtocolHierarchy – показує ієрархію розподілення пакетів.



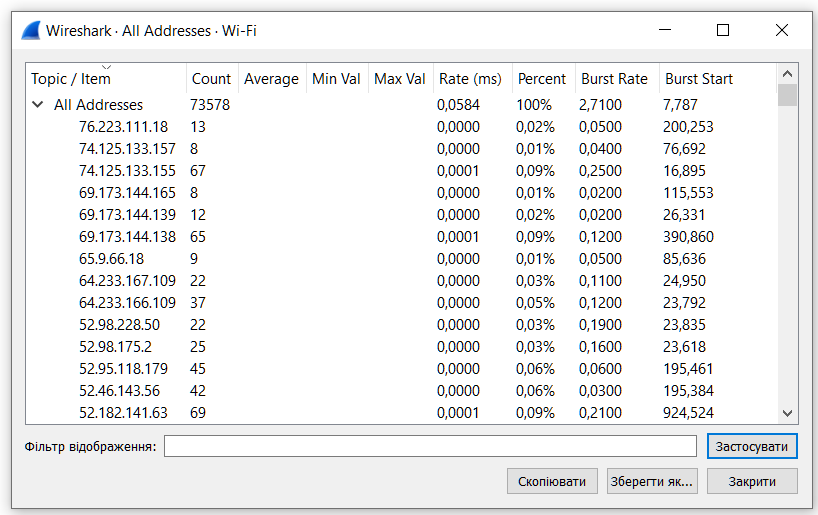
1. Conversations показує сумарні дані фізичними адресами, ip.



1. I/OGraph – графік отриманих та відправлених пакетів.



1. IPv4Statistics – показує всі адреси ipv4, які є у файлі та статистичні дані про них.



**Висновок**: отримав загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомився з графічним інтерфейсом програми, навчився захоплювати, сортувати та фільтрувати пакети.