Львівський національний університет імені Івана Франка

Факультет прикладної математики та інформатики

Кафедра дискретного аналізу

**Комп’ютерні інформаційні мережі**

**Лабораторна робота №3**

Виконав:

Студент групи ПМі-33

Тимчишин Ярема

Прийняв:

Ас. Жировецький В.В.

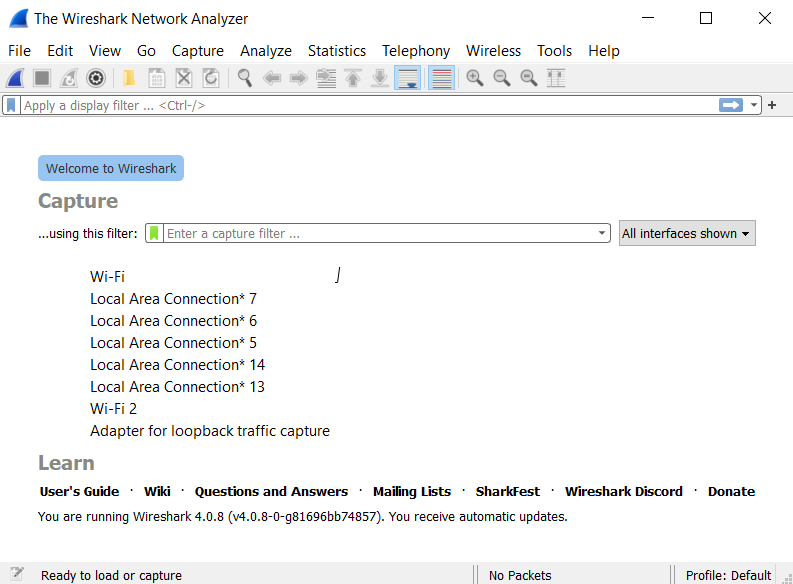
Львів 2023

**Тема:** Інтерфейс аналізатора пакетів Wireshark.

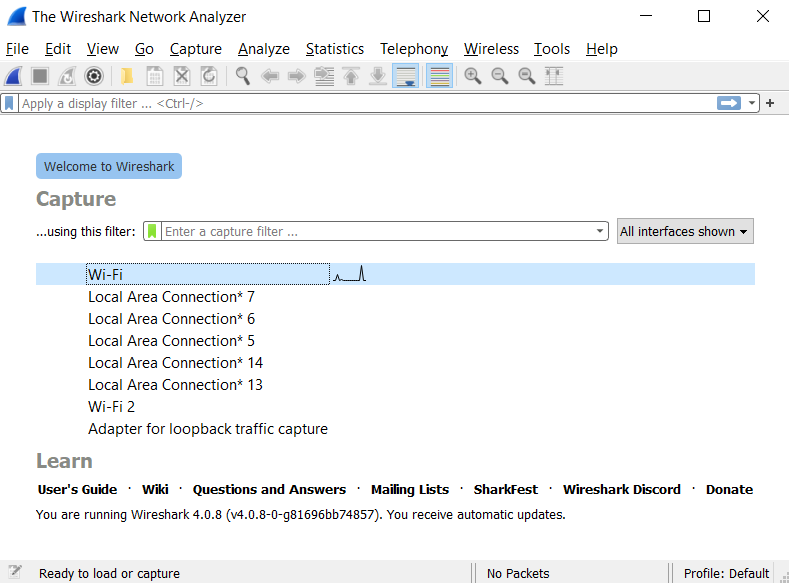
**Мета роботи:** Отримати загальні уявлення про функціональні можливості аналізатора мережевих пакетів Wireshark, ознайомитися з графічним інтерфейсом програми, навчитися захоплювати, сортувати та фільтрувати пакети.

**Хід роботи**

Запустив аналізатор мережевих пакетів Wireshark від імені адміністратора.



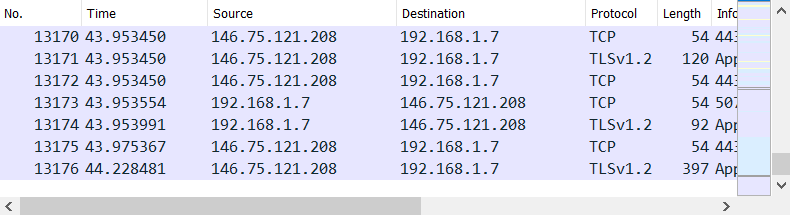
Вибрав з переліку Wi-Fi та почав захоплення пакетів.

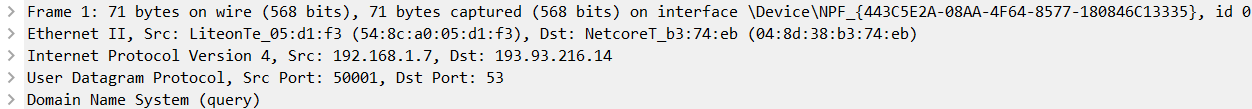


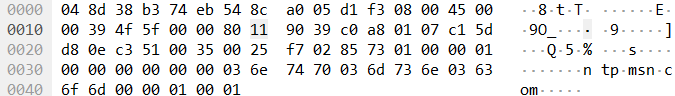
3. Упродовж 48 секунд здійснив різну активність у браузері: перейшов на сайти, залогінився, завантажив на комп’ютер зображення.

4. Зупинив процедуру захоплення пакетів.

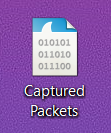
5. Ознайомився з трьома основними елементами головного вікна програми.



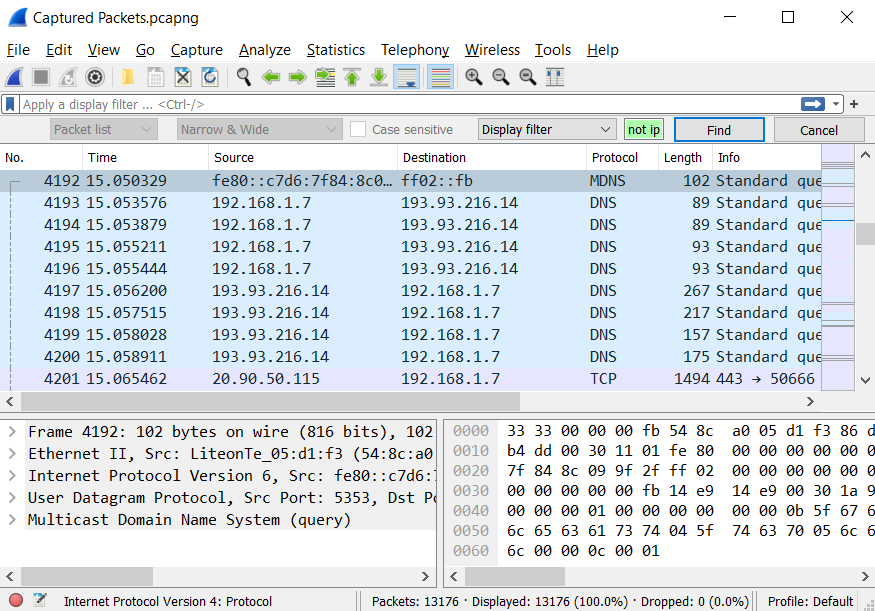




6. Зберіг захоплені пакети у файл для подальшого аналізу.



7. Знайшов пакети, які не стосуються протоколу IP, натиснувши кнопку пошуку а використавши спеціальний вираз “not ip”.



8-9. Проекспериментував з наступними виразами:

ip.addr == 192.168.0.107

arp || udp.port == 53

ipv6.addr == 2001:db8::1

eth.addr == 00:00:5e:00:53:00

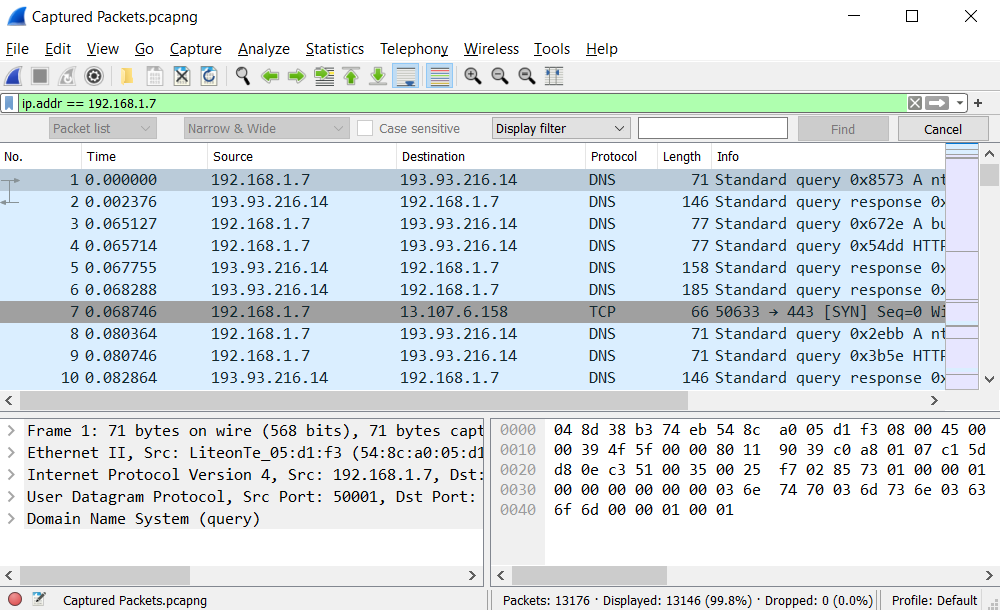
ip.src != 192.168.0.107

http && ftp && arp

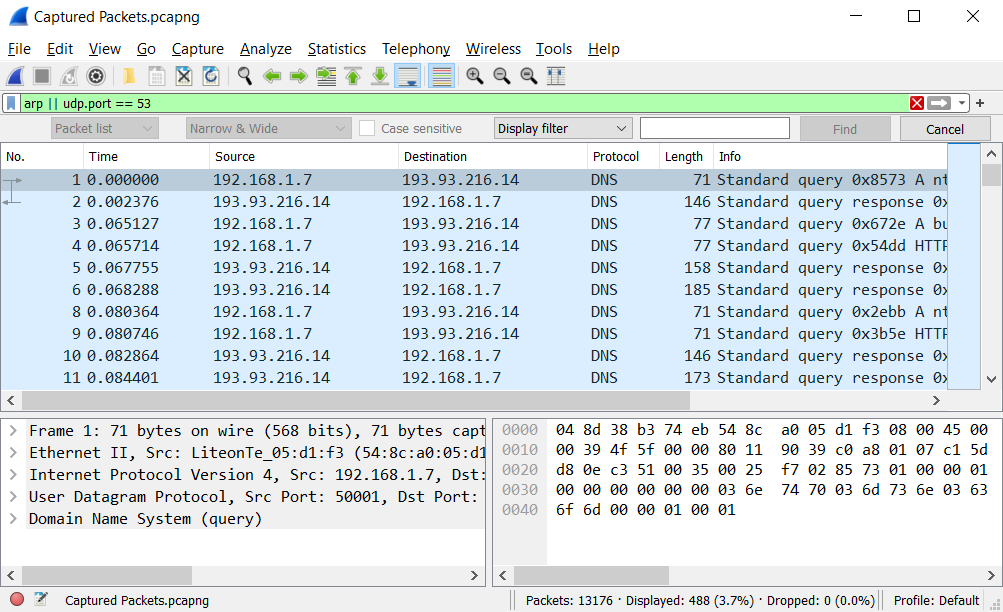
ip.dst == 216.58.215.78

та описав, які критерії пошуку вони задають:

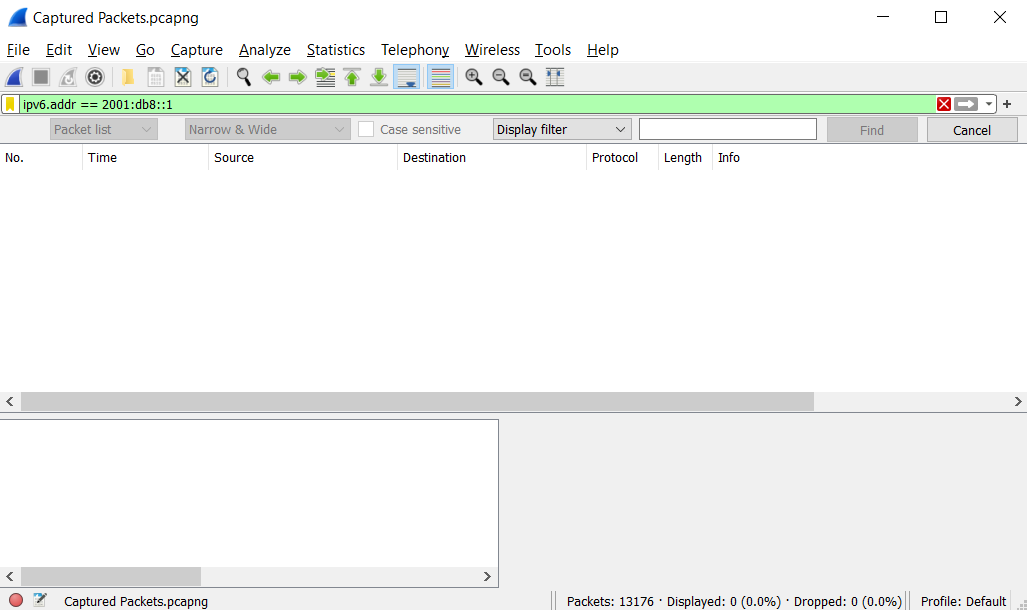
Пакети відправлені з мого локального IP або отримані ним.



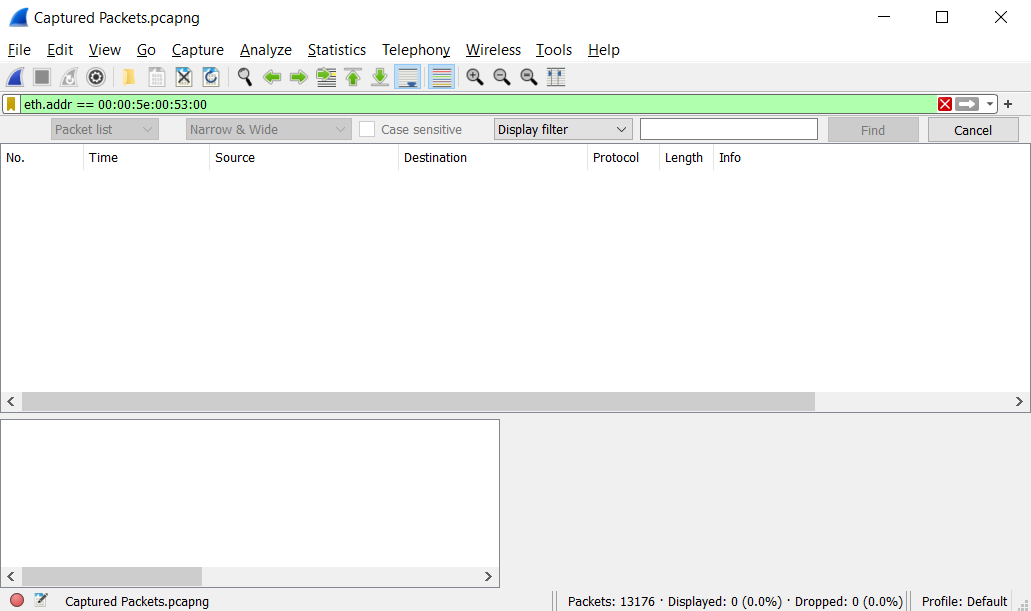
Пакети відправлені протоколом ARP або через UDP порт 53.



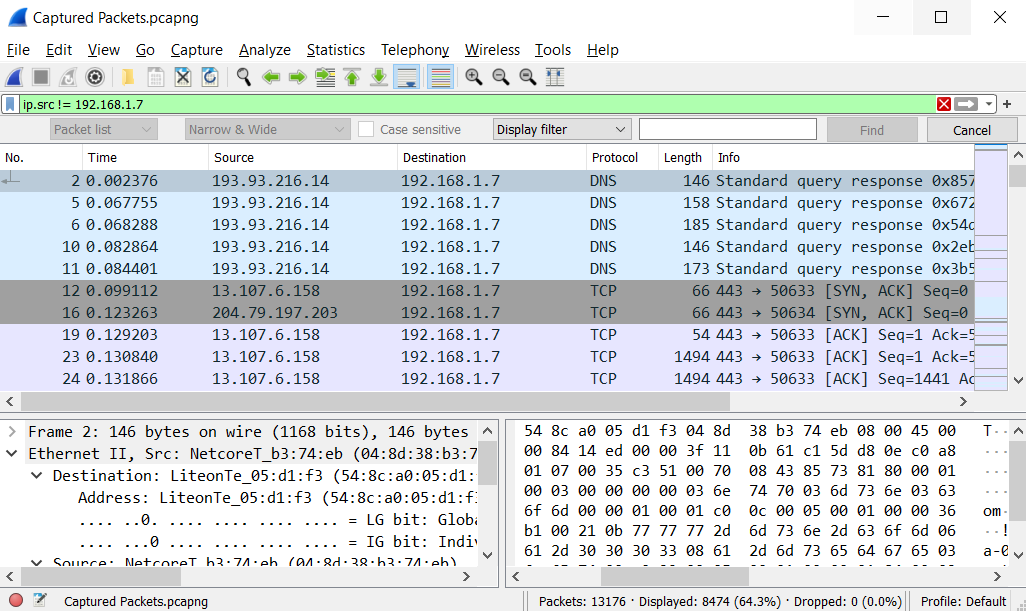
Пакети відправлені з мого IPv6 або отримані ним.



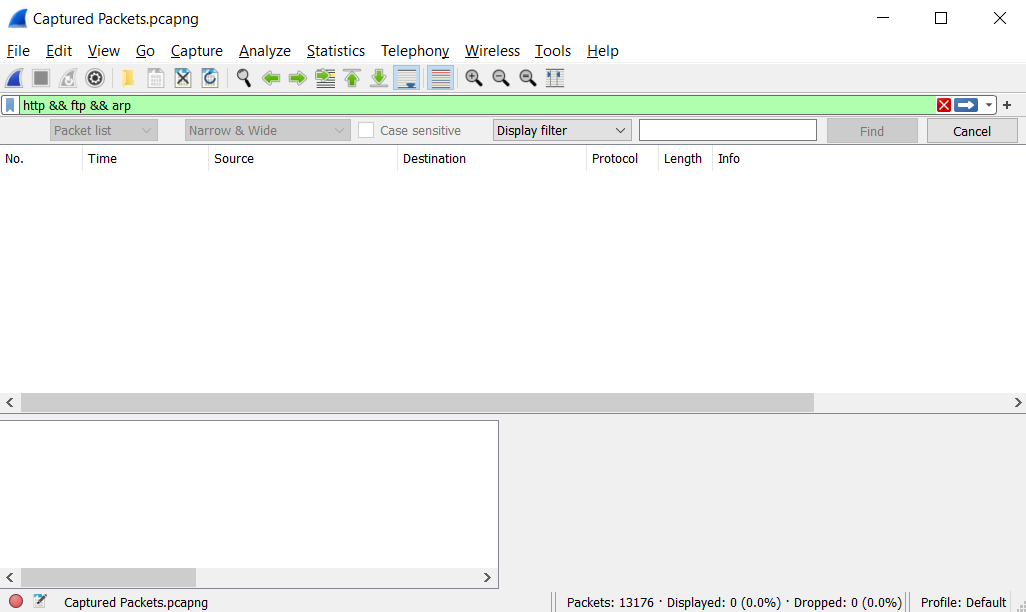
Пакети відправлені або отримані фізичною адресою мого адаптеру.



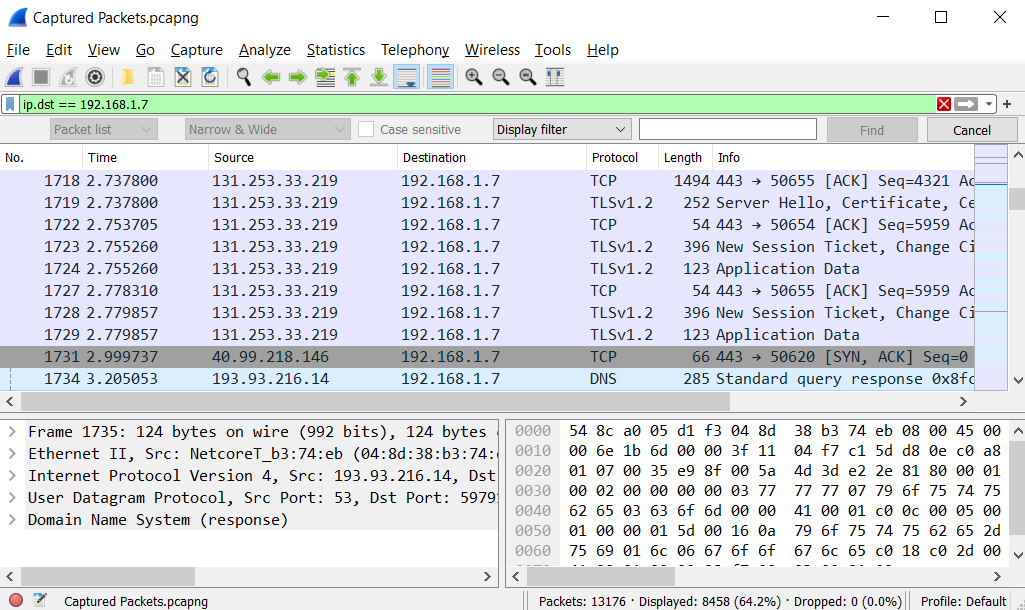
Пакети відправлені **не** з мого локального IP.



Пакети http, ftp та arp.



Пакети отримані моїм локальним IP.



10. У меню Statistics вибрав по черзі пункти:

Capture File Properties

Resolved Adresses

Protocol Hierarchy

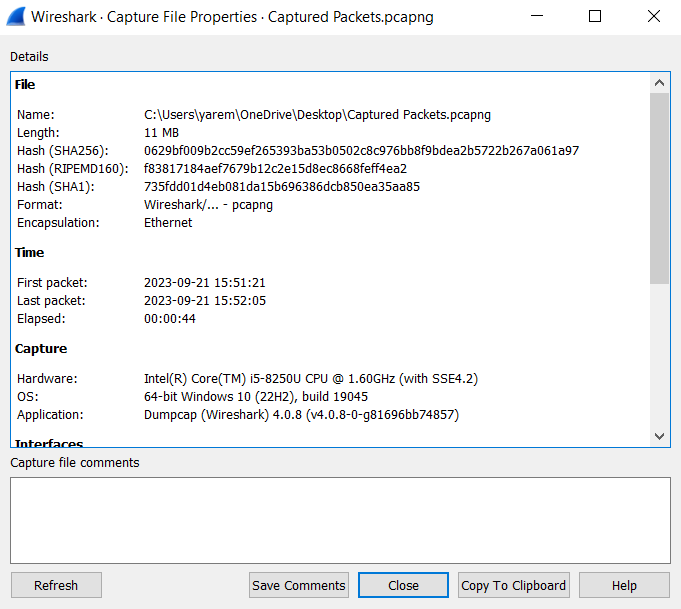
Conversations

I/O Graphs

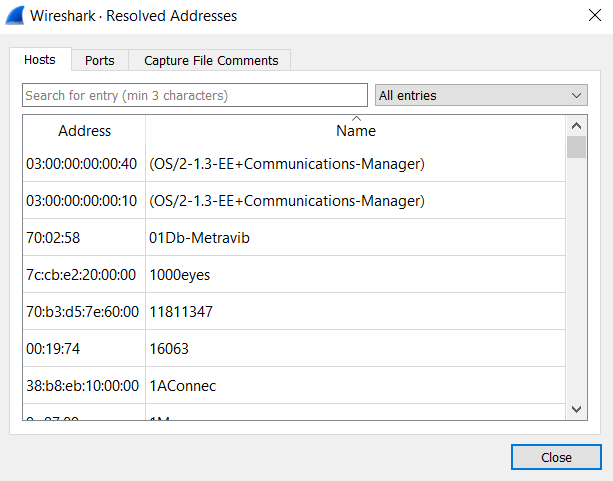
IPv4 Statistics

та ознайомився з інформацією.

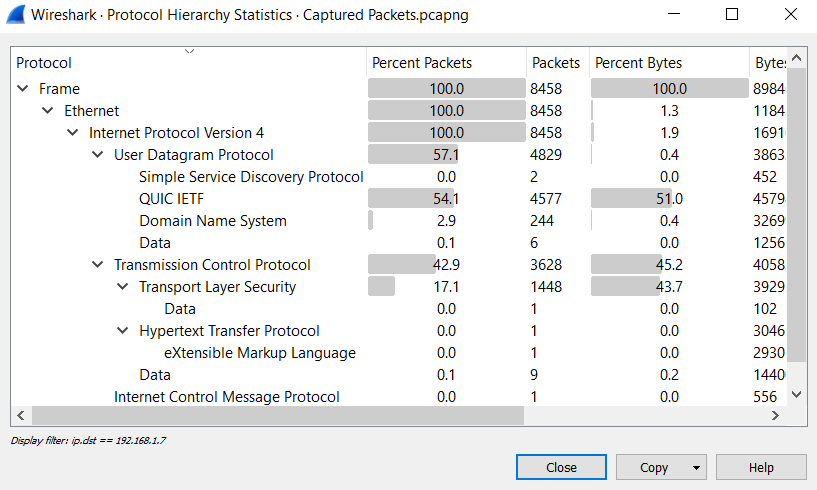
Capture File Properties – показує дані про пакети записані у файлі, час, і статистику пакетів.



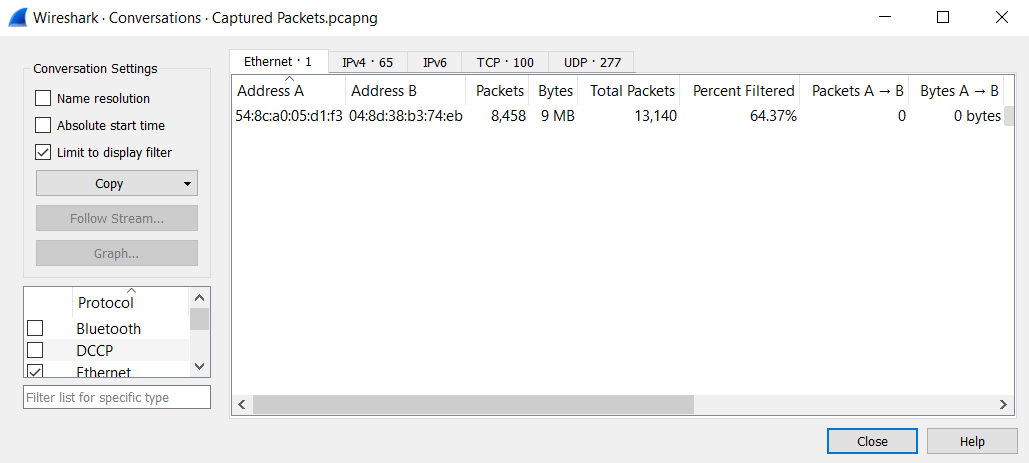
Resolved Adresses має фізичні адреси, які отримували пакети або відправляли, а також порт та протокол за яким відправлено в інших вкладках.



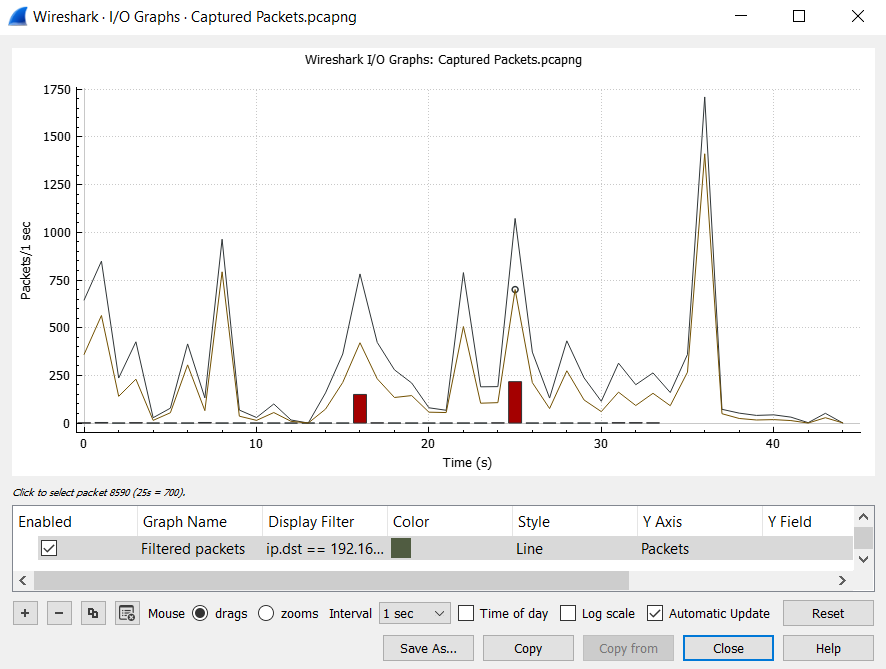
Protocol Hierarchy показує ієрархію розподілення пакетів по протоколах.



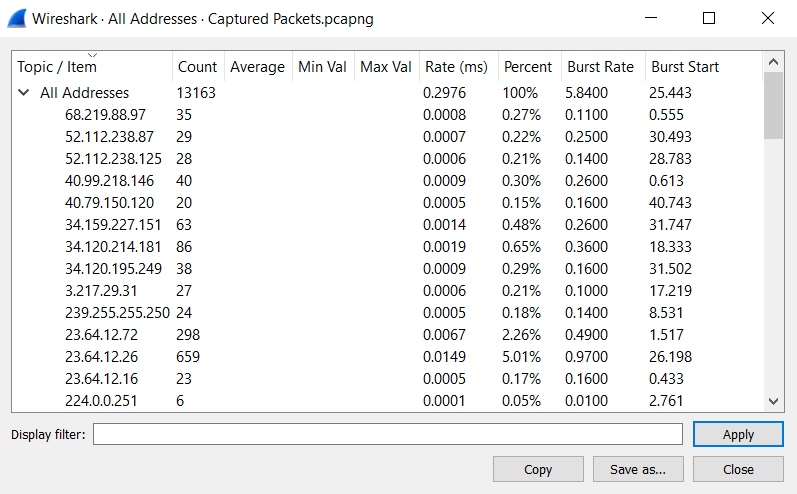
Conversations показує сумарні дані передачі даних між фізичними адресами, IP, тощо.



I/O Graph – графік отриманих та відправлених пакетів.



IPv4 Statistics показує усі адреси ipv4, які є у файлі та статистичні дані про них.



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