МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

**Комп’ютерні інформаційні мережі**

**Лабораторна робота №7**

Виконала:

студентка групи ПМі-31

Харитонова Анастасія

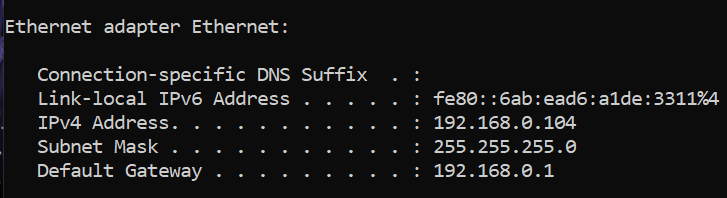
Львів 2024

**Тема:** Аналіз ІР-пакетів і повідомлень керуючих протоколів. Утиліти для діагностики мережі на мережевому рівні

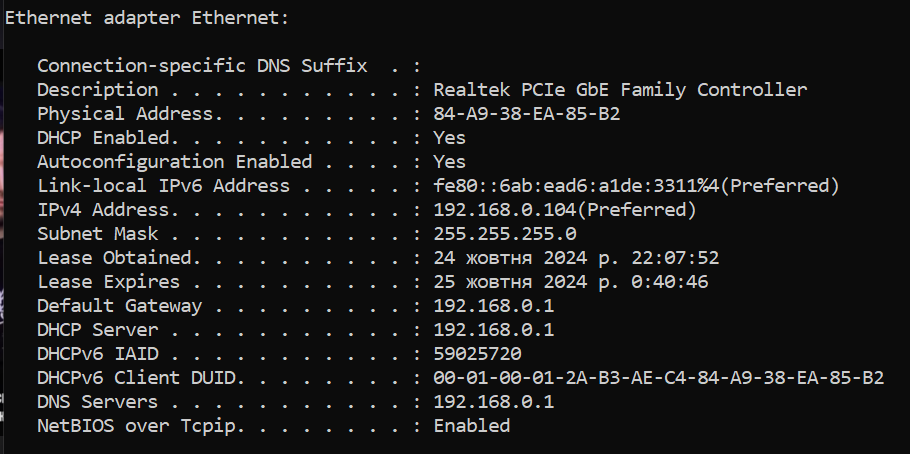
**Мета:** Здобути практичні навички з інтерпретації ІР-пакетів і повідомлень керуючих протоколів, а також використання консольних утиліт для діагностики мережі на мережевому рівні.

**Хід роботи:**

**1.**



**2.**



**3.** ipconfig /release – відправляє команду DHCPRELEASE на DHCP‑сервер, щоб повідомити серверу про скидання ІР адреси на ПК.

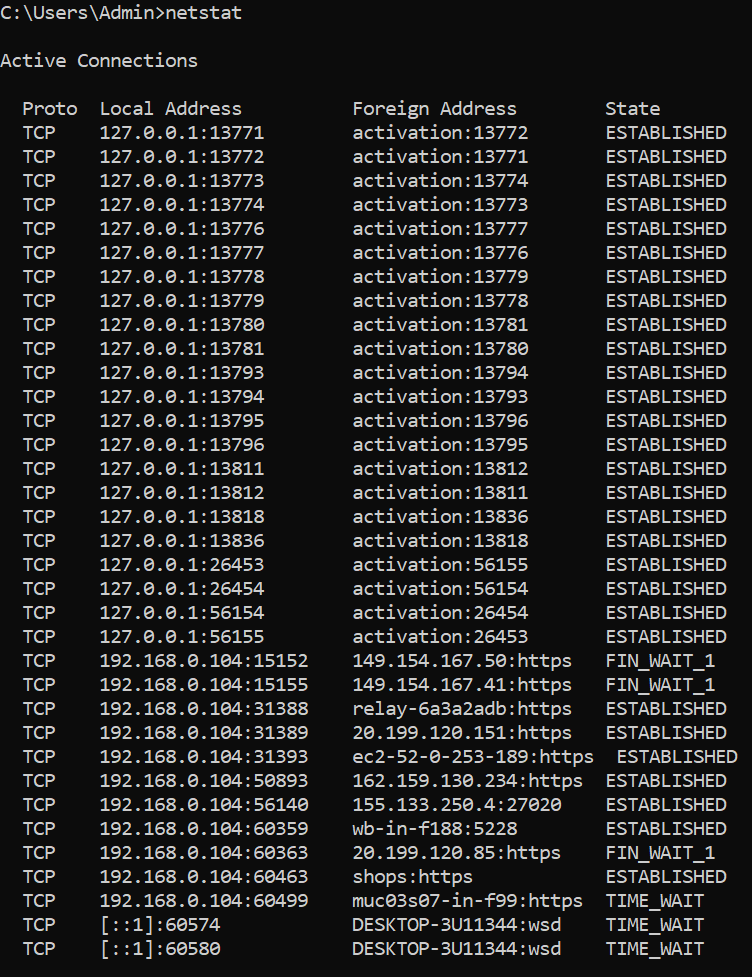
ipconfig /renew - використовується для запиту нової адреси у DHCP‑сервера.

**4.**

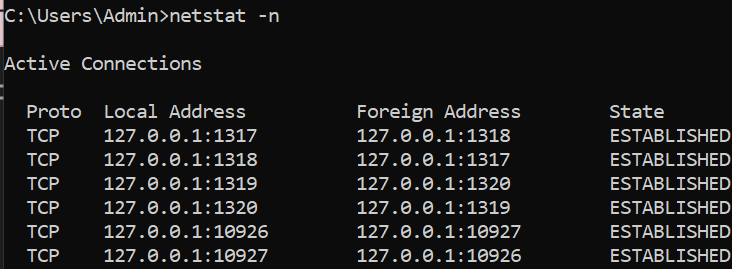
**ESTABLISHED** – з’єднання встановлено, йде передача даних.

**FIN\_WAIT\_1** – одна з сторін (вузол 1), завершує з’єднання, відправляючи сегмент з прапорцем FIN

**TIME\_WAIT** – Вузол 1 отримав сегмент з прапорцем FIN, відправив сегмент з прапорцем ACK і чекає 2 \* MSL (Maximum Segment Lifetime) секунд, перед остаточним завершенням з’єднання.

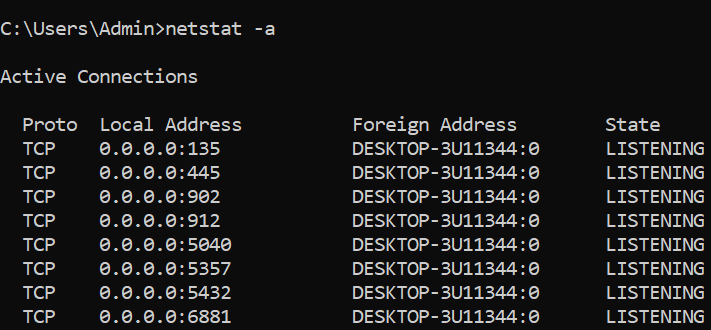


**netstat -n** - виводить інформацію про підключення в числовому вигляді, без перетворення IP-адрес і портів у їхні символьні назви. Це дозволяє швидше отримати дані, оскільки система не витрачає час на виконання DNS-запитів для перетворення IP-адрес.

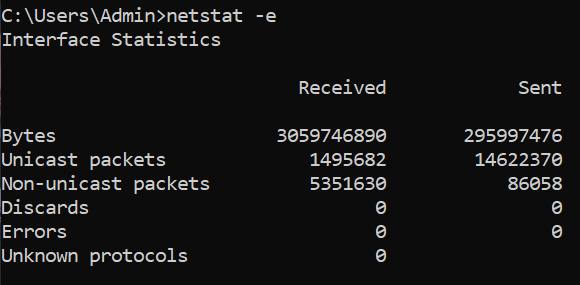
CLOSE\_WAIT – з’єднання закрите.

**netstat -a** - виводить інформацію про всі активні з'єднання та порти, які перебувають у режимі прослуховування. Крім активних з'єднань, цей параметр покаже ті порти, які відкриті та чекають на підключення.

LISTENING – очікує з’єднання.



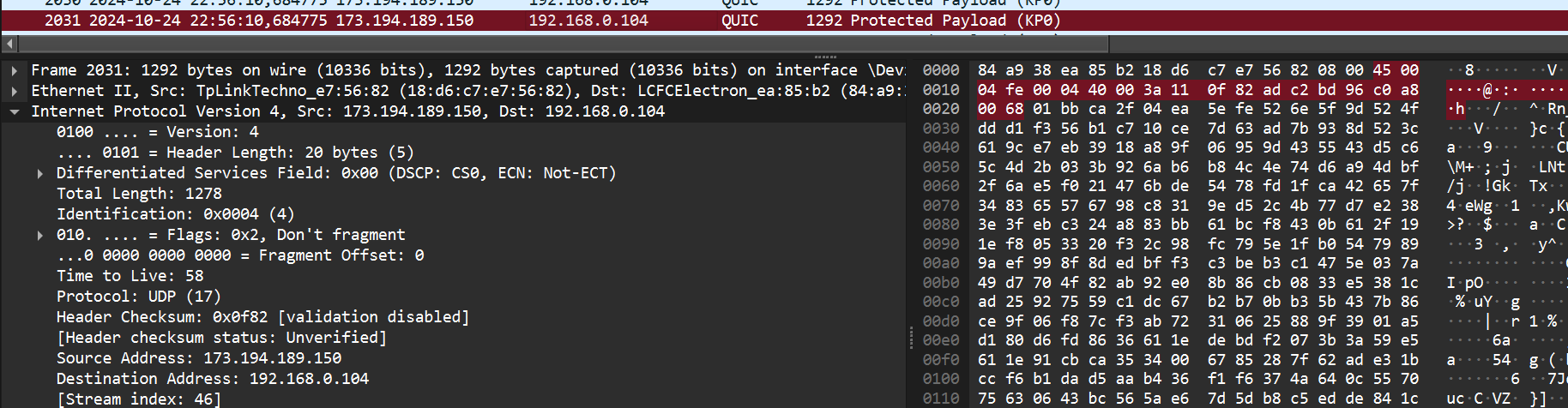
**5.**



Видно, що з мережею нема фізичних проблем.

**netstat -s** - показує статистику мережевих протоколів на вашому комп'ютері, надаючи детальну інформацію про кожен мережевий протокол (TCP, UDP, IP, ICMP та ін.)

**6-11.** Запустила Wireshark в режимі адміністратора, від’єдналась від мережі, почала захоплення пакетів, знову під’єдналась, здійснила деяку активність в браузері та закінчила захоплення пакетів.

**12. Пакет №2031** 

**13. Version** - версія протоколу (4).

**Header length –** довжина заголовка.

**Total length –** загальна довжина пакета, включаючи заголовок і дані (в байтах).

**Identification –** ідентифікатор пакета, який використовується для складання фрагментів. (якщо пакет фрагментований, то кожен фрагмент буде використовувати той самий ідентифікаційний номер, щоб ідентифікувати до якого пакета він належить).

**Flags:**

-Reserved bit – завжди 0

**- Don’t fragment –** заборона фрагментації

- More fragments – означає, що пакет є частиною фрагментованого пакета і не є останнім.

**Fragment offset –**для визначення послідовності фрагментів у кадрі.

**Time to live –** час життя пекета в мережі, зменшується при кожному проходженні маршрутизатора. Якщо TTL досягає 0 то пакет відкидається.

**Protocol –** вказує, який протокол транспортного рівня використовується.

**Header checksum –** контрольна сума заголовка, для перевірки цілісності.

**Source Ip address –** ІР-адреса відправника.

**Destination address –** ІР-адреса одержувача.

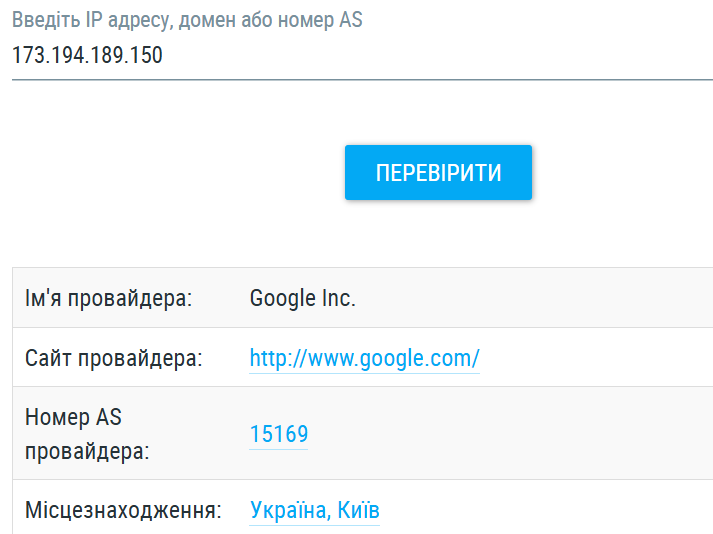
**14. Header length** – це поле довжиною 4 біти в заголовку, яке позначає загальну довжину заголовка пакета в одиницях, кратних 32 бітам (4 байтам). Значення, вказане в цьому полі треба множити на 4 для отримання довжини заголовка. Мінімальна довжина заголовка – 20 байт. (5 \*4=20-мінімальна довжина, включає лише стандартні поля без додаткових параметрів. 15\*4=60-максимаьна довжина). Це масштабування, що дозволяє представити довжину заголовка від 20 до 60 байт лише за допомогою 4 бітів.

**15.** Розміркориснихданих: Total length-Header length = 1278-20=1258 байт

**16.**

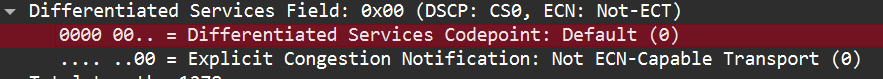
****

Адреса відправника – звідки відправляються дані.



Адреса одержувача – кому відправляються (моя ІР адреса).

**17.** **Differential services field: розмір 8 біт**

****

* **Differentiated services code point (DHCP)- 6 біт.** (як пакети повинні оброблятись в залежності від пріоритету) Визначає клас обслуговування для пакету. DSCP дозволяє мережевим пристроям (маршрутизаторам, комутаторам) обробляти пакети відповідно до заданих політик якості обслуговування (QoS). Значення може варіюватись від 0 до 63, різні комбінації – різні значення.

**000000 (CS0)**: Нормальний трафік без особливого пріоритету.

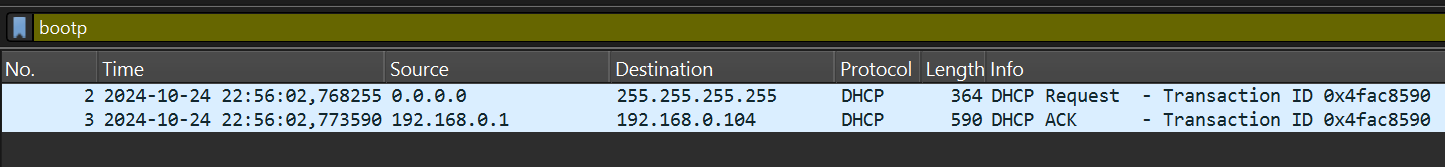
**CS7 (56) – найвищий пріоритет.  
EF –** для голосового трафіку.

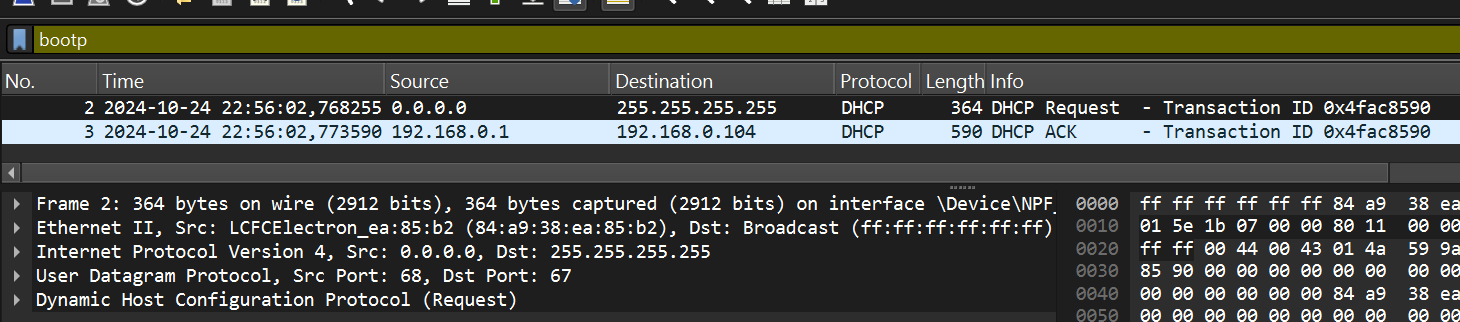
**А F** – різні класи, які забезпечують певний рівень QoS

* **Explicit congestion notification (ECN)- 2 біта.** для інформування про перевантаження мережі.

**00 (Not-ECT)** – немає перевантаження.

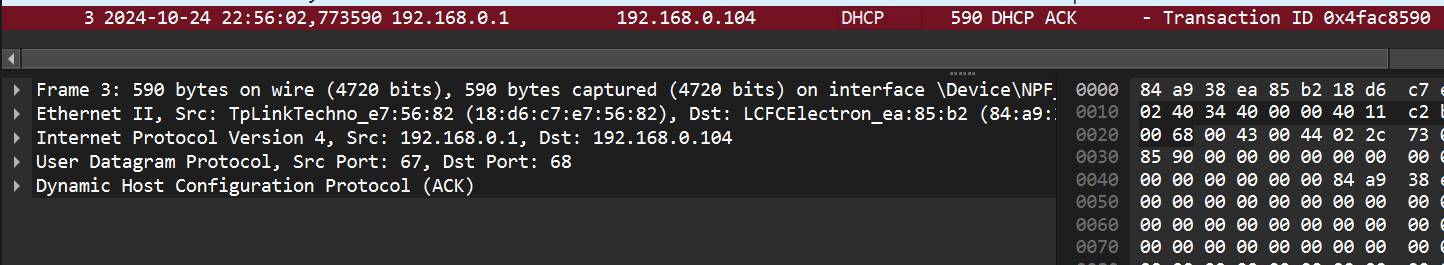
**11 (CE) –** підтверджене перевантаження.

**18.** 

**19.** 

Source address 0.0.0.0 – поки у клієнта немає адреси.

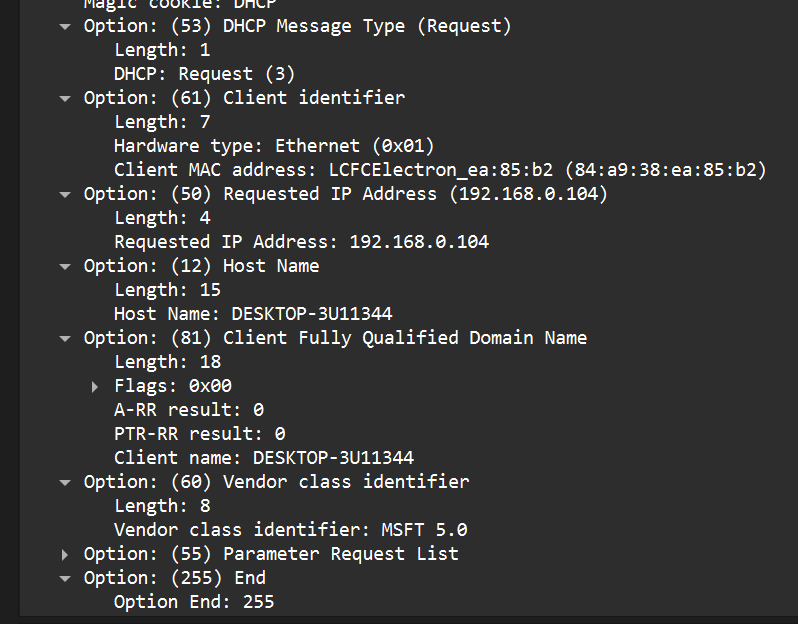
Destination address 255.255.255.255 – широкомовна адреса, оскільки невідомо де сервер запит надсилається до всіх пристроїв в локальній мережі.

**20.** 

Source address 192.168.0.1 – ІР адреса DHCP сервера.

Destination address 192.168.0.104 – нова адреса, видана клієнту (мені).

**21.**

****

**DHCP message type –** тип повідомлення (Request – запит)

**Client identifier –** унікальний іддентифікатор клієнта, на основі МАС – адреси.

**Requested IP – address –** ІР адреса, яку запитує клієнт.

**Host name –** ім’я хоста клієнта.

**Client fully qualified domain name –** повне ім’я клієнта, яке містить ім’я хоста та домен, використовується для точного іменування клієнта в мережі.

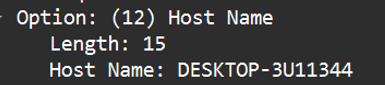
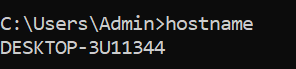
* A-RR result = 0 – ІР – адреса, на яку вказує доменне ім’я. (0 бо поки клієнт немає ІР).
* PTR-RR = 0 – доменне ім’я, яке асоційоване з ІР – адресою.

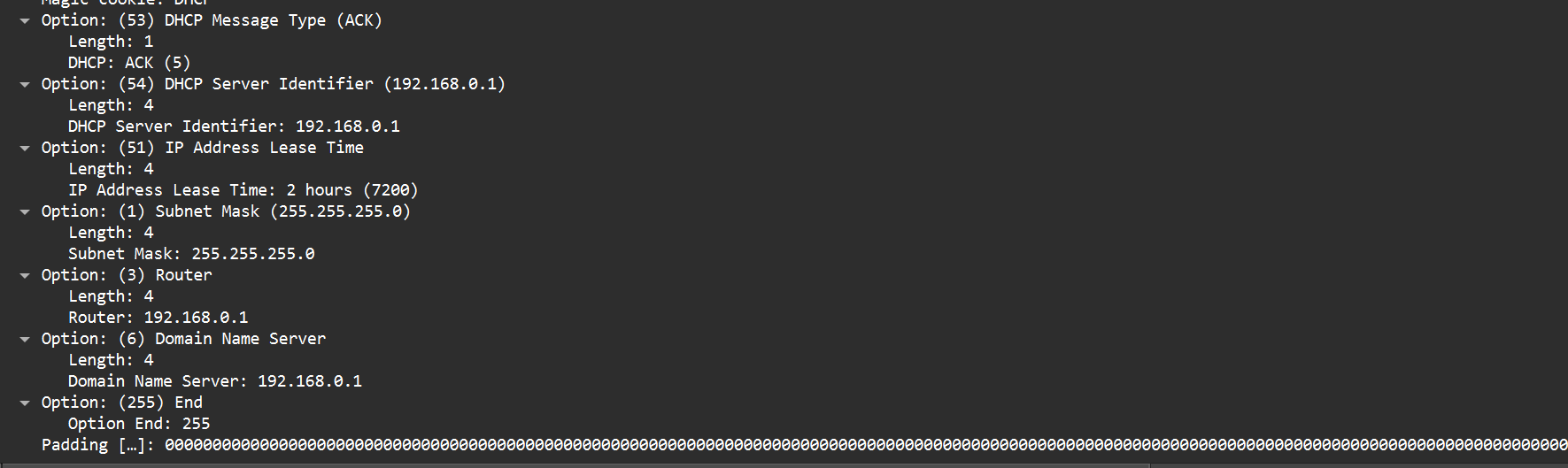
**Vendor class identifier –** ідентифікатор виробника або тип пристрою, який надсилає запит.

**Parameter request list –** список параметрів, які клієнт запитує від DHCP сервера

**End –**закінчення повідомлення DHCP

**22.** Порівняла назви хостів, усе зійшлось.

**23.** 

**DHCP message type –** тип повідомлення (АСК – надсилається DHCP сервером клієнту після успішного виконяння запиту на отримання ІР адреси).

**DHCP server identifier –** ІР адреса DHCP сервера, який надав адрусу.

**IP address lease time –** час оренди ІР адреси вказаний в секундах.

**Subnet mask –** маска підмережі, яку повинен використовувати клієнт.

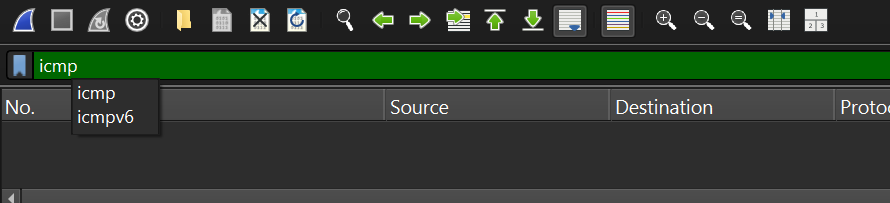
**Router –** список ІР адрес шлюзів (маршрутизаторів), в моєму випадку один, який клієнт може використовувати для доступу до зовнішніх мереж.

**Domain name server –** список ІР адрес DHCP серверів, які клієнтт повинен використовувати для перетворення доменних імен в ІР адреси.

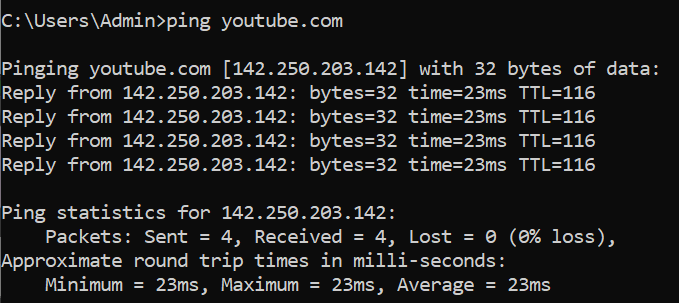
**End** – позначає кінець списку опцій в повідомленні.

**Padding** – додакові байти для зберігання довжини повіомлення

**24.** Поки немає пакетів ICMP

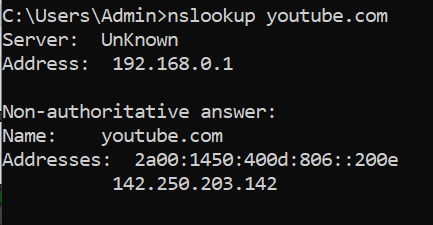


**25.** Почала захоплювати пакети і скористувалась утилітою ping

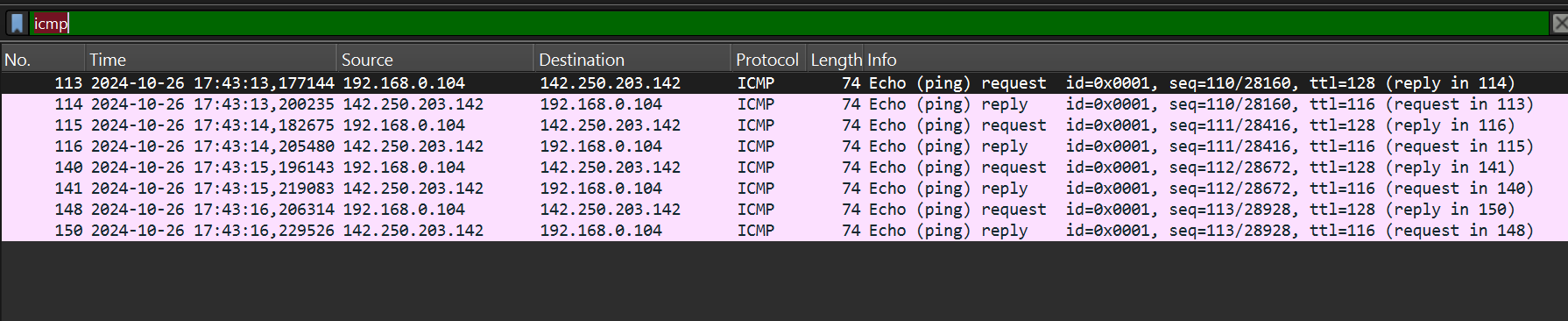


Сервер youtube.com з ІР – адресою 142.250.203.142 доступний і середній час відклику – 23мс.

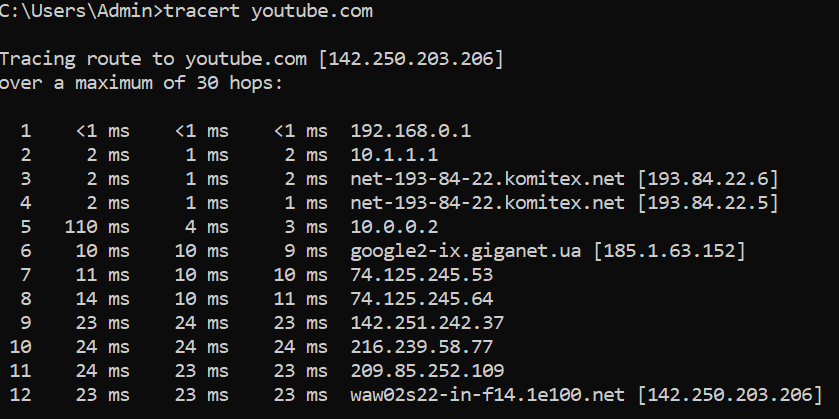
**26.** Використала nslookup щоб знайти ІР за доменним ім’ям.



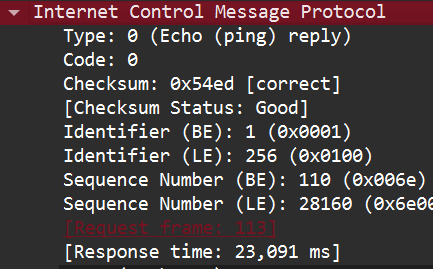
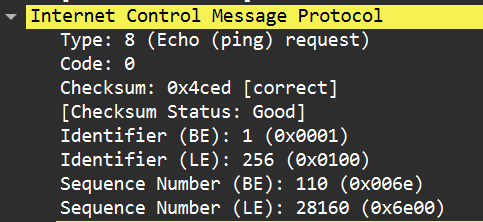
**27.** Зупинила захопленням пакетів, і відфільтрувала щоб знайти ІСМР пакети.



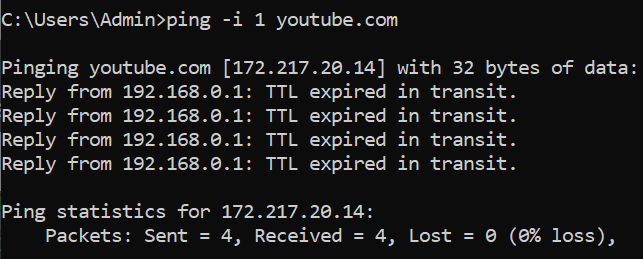
**28.** TTL (time to live) мають різні значення тому, що ttl request – для Windows максимальне значення 128. В процесі проходження через кожен маршрутизатор, це значення зменшується на 1. ttl reply- показує значення, яке було зменшене під час проходжень. (128-116=12 маршрутизаторів, можна перевірити утилітою tracert

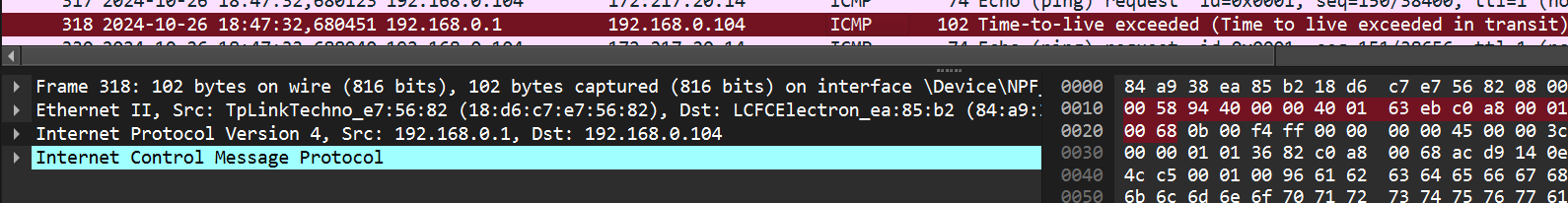


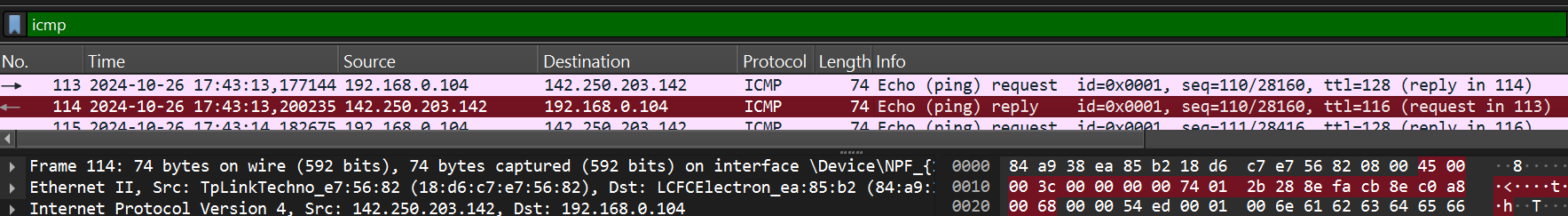
**29.** Отримала 2 типи ІСМР повідомлень.

****

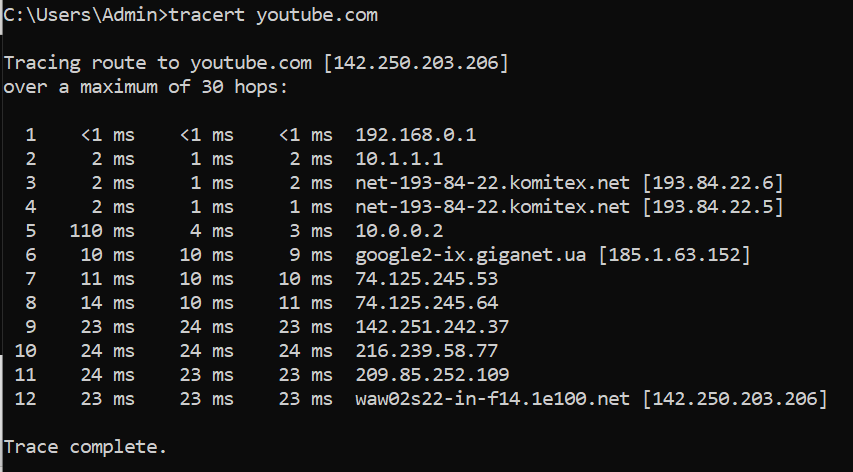
**30.**



****

(Попередні пакети)

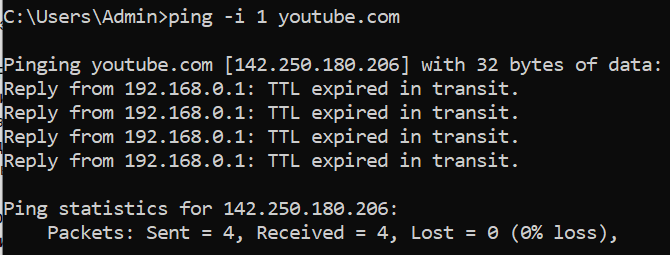
Source адреси відрізняються тому, що обмеження на відправку лише 1 пакета, тому ping досягає лише першого маршрутизатора і він відправляє повідомлення time-to-live exceeded.

**31.** Пакет пройшов 11 маршрутизаторів

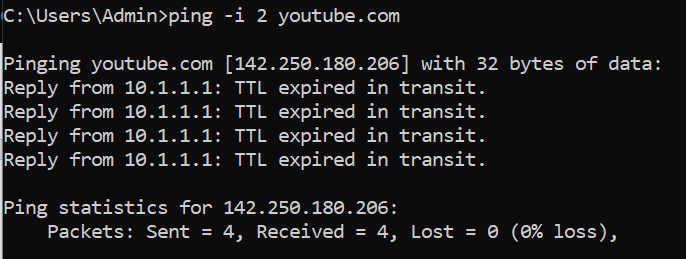
**32.** Захопила ІСМР пакети утиліти tracert. Ця утиліта відправляє пакет, де ttl=1, перший маршрутизатор змінює на 0, блокує передачу пакета і відправляє назад повідомлення time-to-live exceeded. Це повідомлення містить адресу маршрутизатора і tracert реєструє це як перший перехід. Наступний пакет буде мати значення ttl=2 (далі 3, 4…) і кожен наступний маршрутизатор буде зменшувати це значення до 0 і відправляти відповіді назад. Коли пакет досяг кінцевого призначення приходить reply.

**33.** За допомогою ping можна дізнатись маршрут:

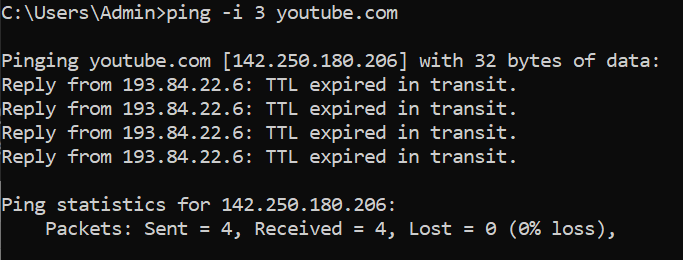
Вказати ttl =1 і отримати відповідь з маршрутизатора



Далі ttl=2



Далі 3

і так поки не отримаю повідомлення від кінцевого пункту призначення.

**Висновок:** здобула практичні навички з інтерпретації ІР-пакетів і повідомлень керуючих протоколів, а також використання консольних утиліт для діагностики мережі на мережевому рівні.