ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

**Комп’ютерні інформаційні мережі**

**ЛАБОРАТОРНА РОБОТА №7**

# Аналіз ІР-пакетів і повідомлень керуючих протоколів.

# Утиліти для діагностики мережі на мережевому рівні

Виконав:

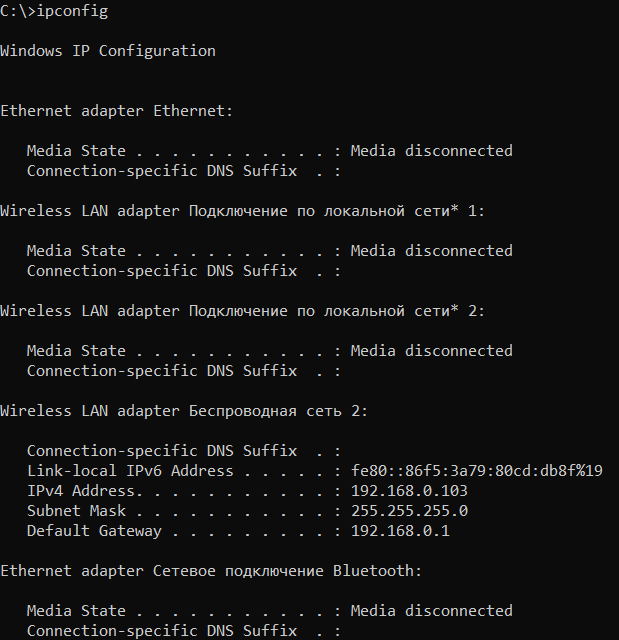
Студент групи ПМі-31Яцуляк Андрій

2023

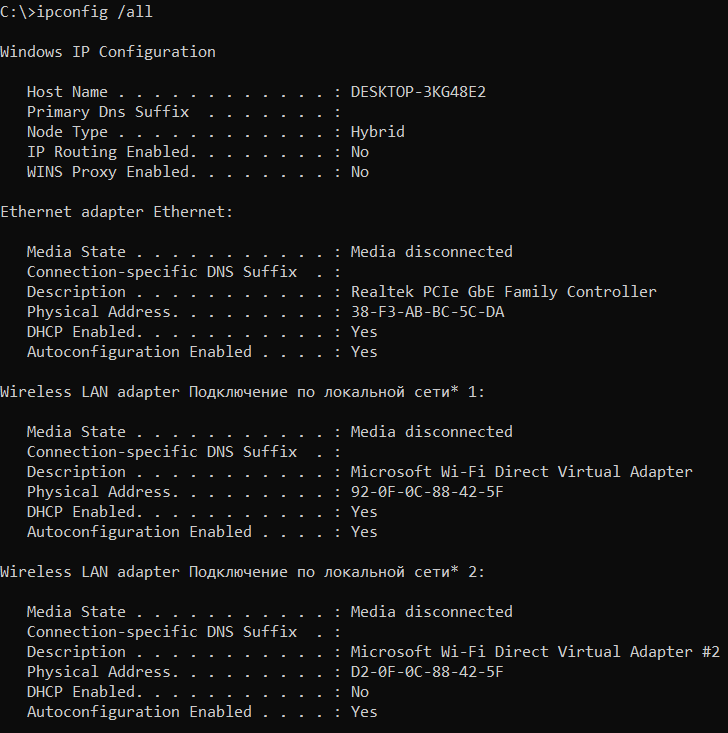
**Мета:** Здобути практичні навички з інтерпретації ІР-пакетів і повідомлень керуючих протоколів, а також використання консольних утиліт для діагностики мережі на мережевому рівні.

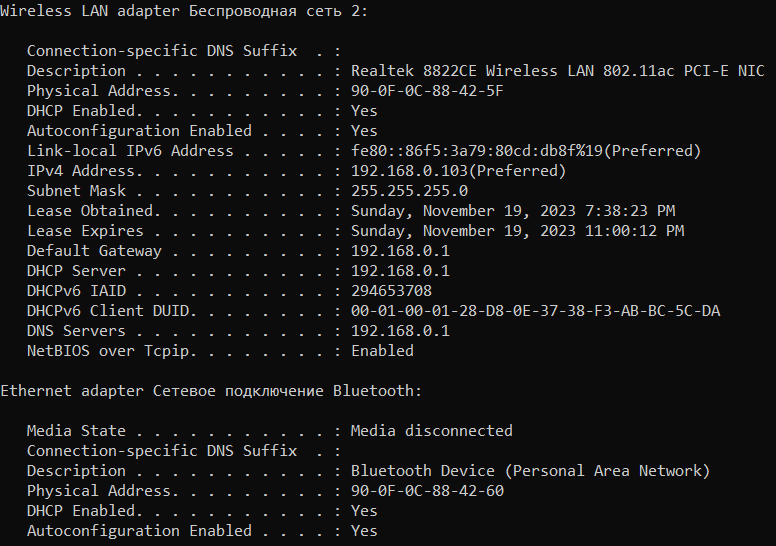
**Хід роботи**

1. Опрацював теоретичний матеріал.
2. Ознайомився з базовою мережевою конфігурацією свого ноутбука, виконавши в консолі команду ipconfig:



1. Отримав більш детальну інформацію командою ipconfig /all:

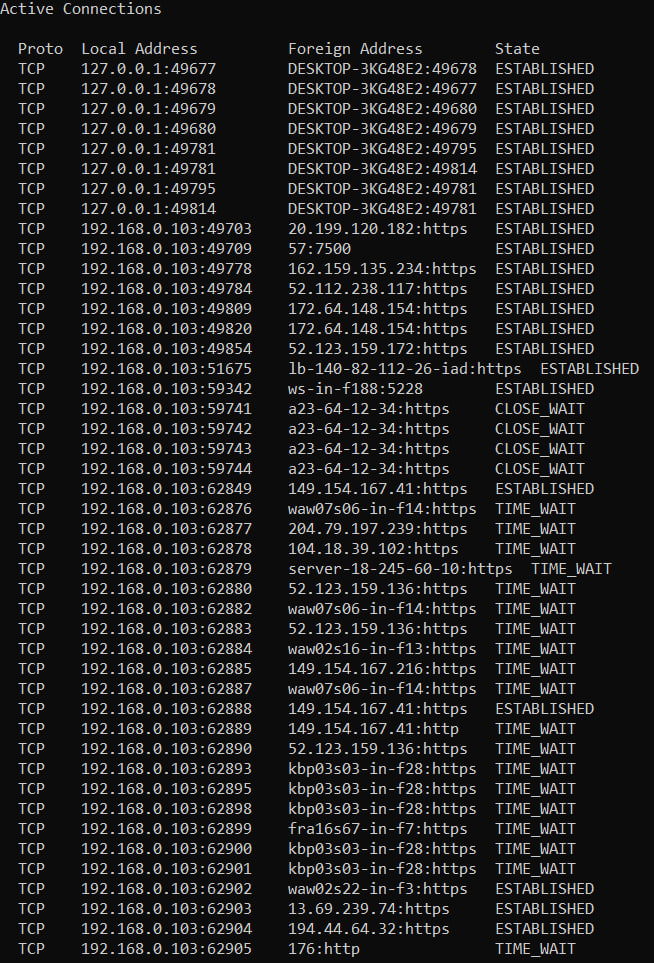




1. Команда ipconfig /renew оновлює конфігурацію DHCP для всіх адаптерів (якщо адаптер не вказано) або для певного адаптера, якщо включено параметр адаптера. Цей параметр доступний лише на комп’ютерах з адаптерами, налаштованими на автоматичне отримання IP-адреси.

Команда ipconfig /release надсилає повідомлення DHCPRELEASE серверу DHCP, щоб звільнити поточну конфігурацію DHCP і скасувати конфігурацію IP-адреси для всіх адаптерів (якщо адаптер не вказано) або для окремого адаптера, якщо включено параметр адаптера. Цей параметр вимикає TCP/IP для адаптерів, налаштованих на автоматичне отримання IP-адреси.

1. Переглянув активні ТСР-з’єднання за допомогою команди netstat:



Опис отриманих станів.

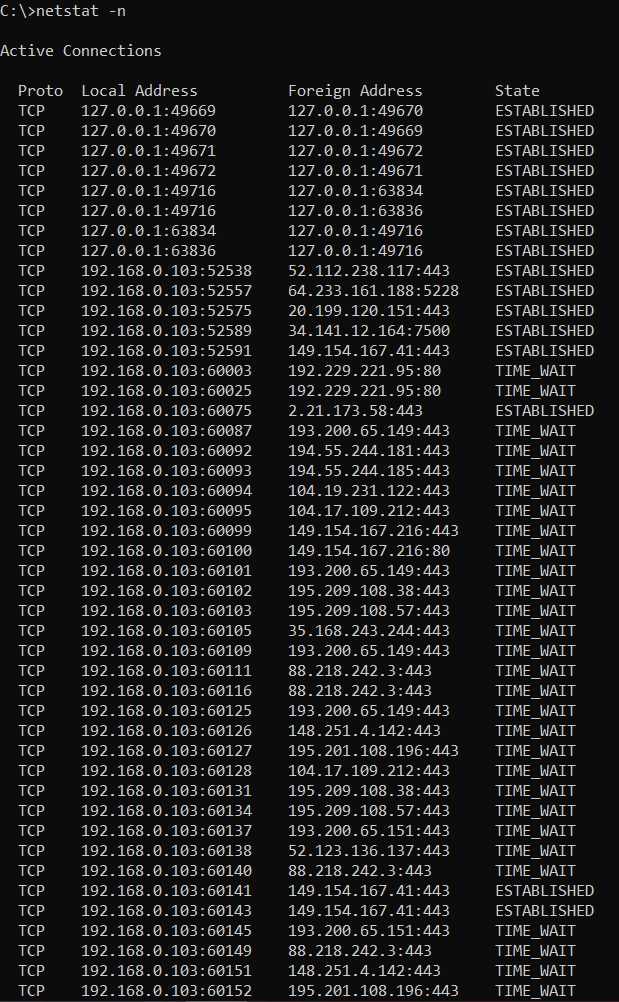
ESTABLISHED - цей стан вказує на те, що TCP-з'єднання активне і дані можна надсилати або отримувати. Це означає, що з’єднання між локальною та віддаленою системами успішно встановлено, і обидві готові до обміну даними.

SYN\_SENT – цей стан відображається, коли система надіслала запит на підключення TCP (SYN) до віддаленої системи, але ще не отримала підтвердження (SYN-ACK) від віддаленої системи.

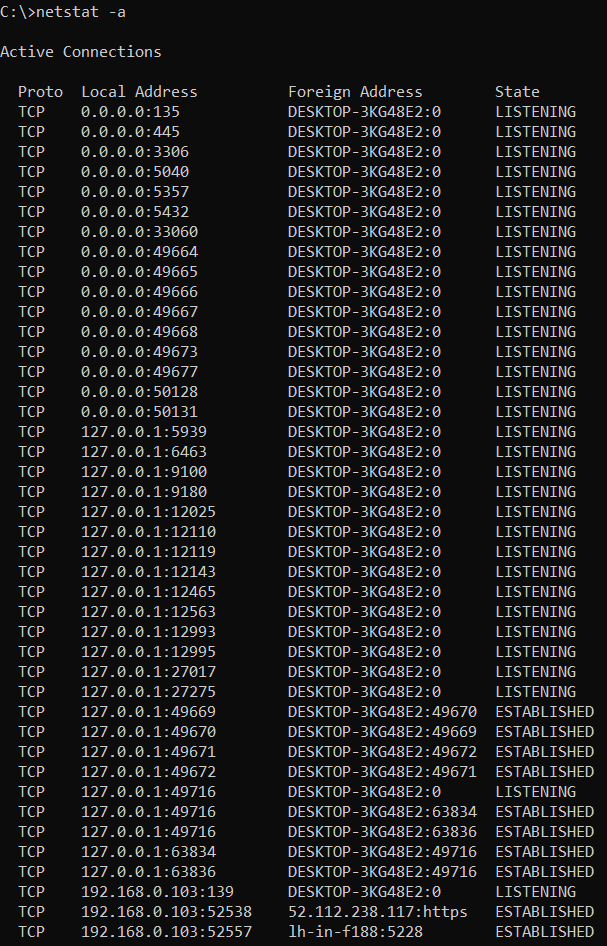
CLOSE\_WAIT – цей стан вказує на те, що віддалена система закрила з’єднання, а локальна система чекає, поки програма підтвердить запит на закриття. По суті, це означає, що з’єднання перебуває в процесі закриття, але локальна програма все ще має виконати операцію закриття.

TIME\_WAIT – цей стан виникає після того, як локальна система закрила з’єднання та очікує на будь-які затримані пакети, які ще можуть бути в дорозі. Стан TIME\_WAIT гарантує, що обидві сторони з’єднання мають достатньо часу для обробки будь-яких затриманих пакетів, і запобігає плутанині, якщо нові з’єднання встановлюються з однаковими номерами портів.

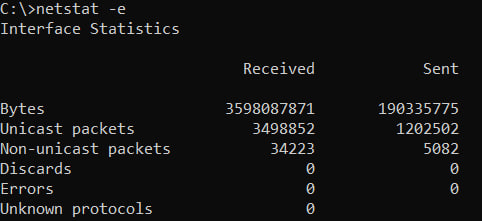
Параметр -n наказує netstat відображати числові адреси замість того, щоб перетворювати їх на імена хостів. Іншими словами, IP-адреси відображатимуться в цифровій формі, а не в доменні імена:



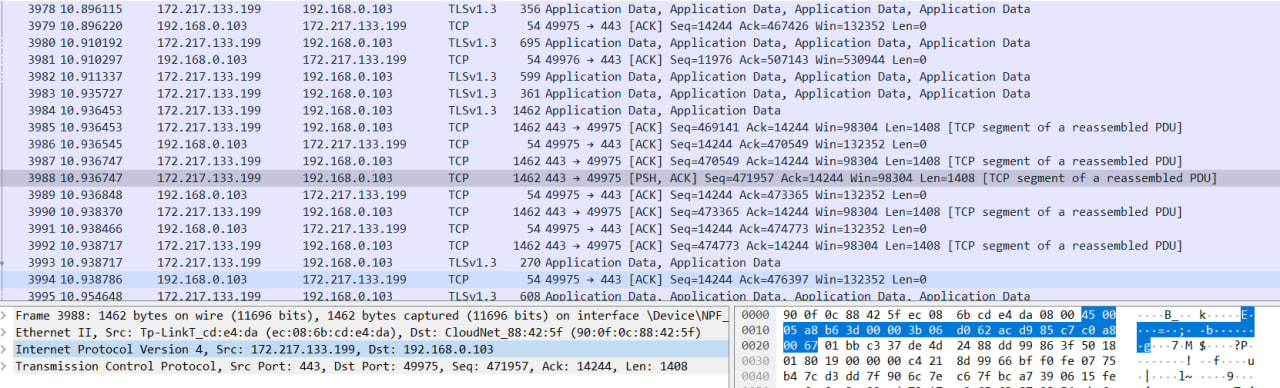
Параметр -a показує всі активні з’єднання та порти прослуховування, включаючи TCP і UDP. Він відображає стан кожного сокета в системі:



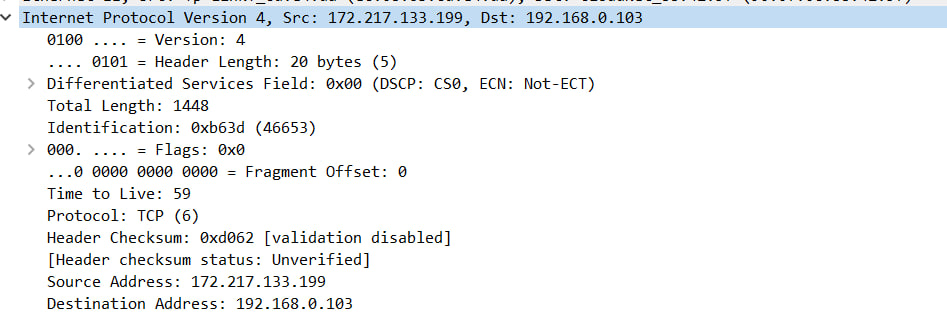
1. Для отримання статистики про отримані/відправлені пакети виконав команду netstat -е:



1. Запустив Wireshark від імені адміністратора.
2. Від’єднався від мережі.
3. Почав захоплення пакетів.
4. Підключився до мережі.
5. Здійснив активність в браузері.
6. Закінчив захоплення пакетів та зберіг результати у файл.
7. Обрав пакет для аналізу. Біти, які відповідають заголовку:



1. Розгорнув заголовок та отримав більш детальну інформацію:



Version (0100 …) - версія IP-протоколу. У цьому випадку це 4, що рівне 0100 у двійковому записі.

Header Length (.... 0101) - представляє довжину IP-заголовка в 32-розрядних словах. У даному випадку це 5, а оскільки кожне слово має 4 байти, загальна довжина заголовка становить 5 \* 4 = 20 байтів.

Differentiated Services Field (DSCP: CS0, ECN: Not-ECT) - використовуються для маркування якості обслуговування.

Total Length - вказується загальна довжина IP-пакета (header + data). У даному прикладі це 1448 байт.

Identification - 16-бітове поле, яке використовується для унікальної ідентифікації фрагмента. Фрагменти пакета матимуть однакове ідентифікаційне значення. У даному випадку це 46653 (0xb63d).

Flags (000. ....) - використовується для керування інформацією, пов’язаною з

фрагментацією.

Fragment Offset (...0 0000 0000 0000) - вказує позицію фрагмента у вихідному потоці даних. У даному випадку зміщення фрагмента дорівнює 0.

Time to Live (TTL) - позначає максимальний час, протягом якого пакет може жити в мережі. Він зменшується кожним маршрутизатором, через який проходить пакет. У даному випадку це 59.

Protocol - визначає протокол, який використовується в частині даних пакета. У даному випадку це TCP (6).

Header Checksum - контрольна сума для заголовка для забезпечення цілісності даних. Контрольна сума обчислюється по всьому заголовку. У даному випадку значення контрольної суми дорівнює 0x781d.

Source Address – IP-адреса відправника. У даному випадку це 172.217.133.199.

Destination Address - IP-адреса одержувача. У даному випадку це 192.168.0.103.

1. **“Біти 0100 поля Версія (Version) дають десяткове число 4, яке відповідає протоколу IPv4. Чому тоді біти 0101 (десяткове число 5) поля Довжина заголовку Комп’ютерні інформаційні мережі:**

**лабораторна робота “Аналіз ІР-пакетів і повідомлень керуючих …” — сторінка 4 (Header Length) відповідають значенню 20 байт, а не 5 байт?”.**

Header Length (.... 0101) - представляє довжину IP-заголовка в 32-розрядних словах. У даному випадку це 5, а оскільки кожне слово має 4 байти, загальна довжина заголовка становить 5 \* 4 = 20 байтів.

1. **“Який розмір корисних даних?”.**

Довжина хедера = 20 байт, загальна довжина = 1448 байт, отже розмір корисних даних – 1428 байт.

1. **“Що Ви можете сказати про одержувача та відправника за виглядом їхніх ІР-адрес?”.**

IP-адреса відправника 172.217.133.199 - глобальна адреса, яка може

вказувати на зовнішній пристрій

IP-адреса отримувача 192.168.0.103 є адресою мого Wifi-адаптера.

1. **Інформація про тип обслуговування**.

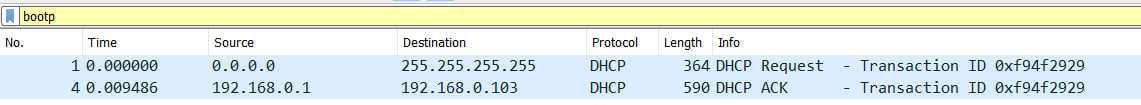
Поле DSCP складається з двох частин:

* DSCP (6 біт): Ця частина поля визначає значення DSCP і вказує на клас обслуговування. Ці 6 біт визначають 64 різних значення DSCP, які використовуються для призначення пакетам різного пріоритету обслуговування в мережі.

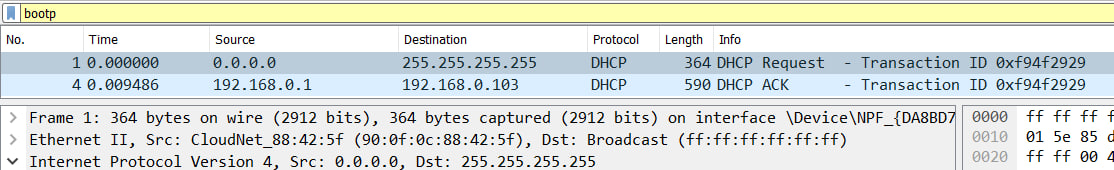
* ECN (Explicit Congestion Notification) (2 біти): Ця частина поля використовується для вказівки на стан перевантаження в мережі. Два біти ECN можуть приймати значення 00 (не використовується), 01 (ECT - ECT(0)), 10 (ECT(1)), або 11 (CE - Congestion Experienced).

Значення DSCP та ECN визначаються при визначенні якості обслуговування для пакета. Вони використовуються для вказівки на приоритет обслуговування і стан перевантаження в мережі. Наприклад, важливі пакети можуть мати більший пріоритет, або, якщо мережа перевантажена, може використовуватися управління затримкою для зменшення витрат пакетів в мережі.

1. Відфільтрував протоколи динамічної конфігурації хостів (DHCP) з усіх:



1. Обрав DHCP запит для аналізу:



* Source: Зазвичай вказується 0.0.0.0 або IP-адреса самого клієнта,

оскільки DHCP-клієнт ще не отримав IP-адресу від

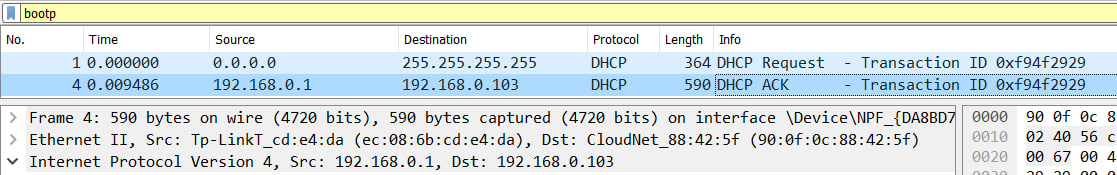
DHCP-сервера.

* Destination: Зазвичай вказується 255.255.255.255, оскільки

DHCP-клієнт спрямовує свій запит на весь локальний

підмережевий діапазон і намагається звернутися до будь-якого

1. доступного DHCP-сервера.Обрав DHCP відповідь для аналізу:



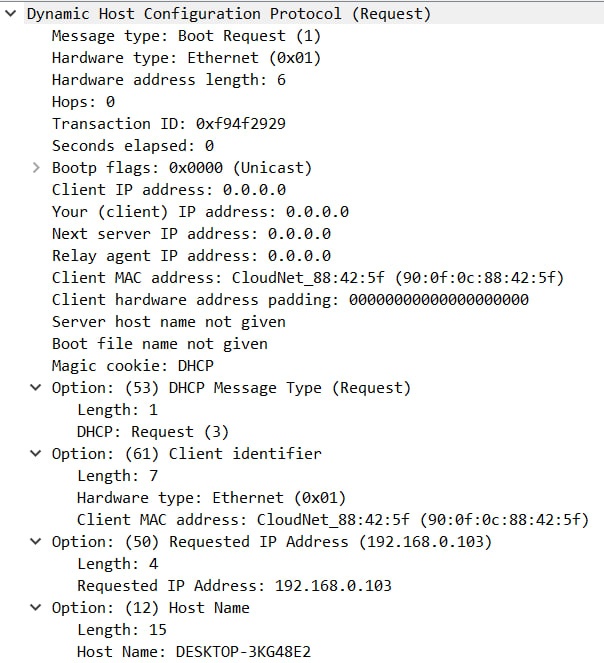
* Source: Це IP-адреса DHCP-сервера, який відправляє

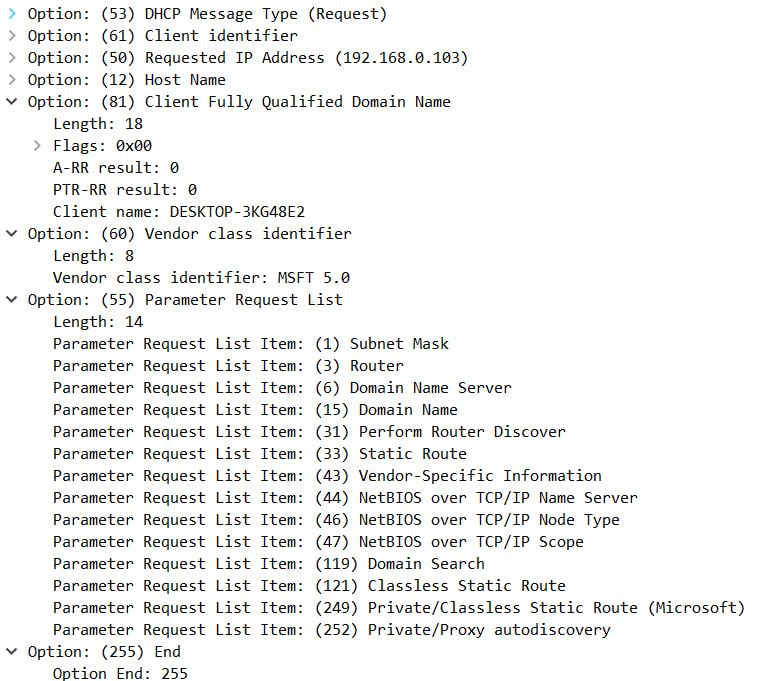
підтвердження клієнту.

* Destination: Це IP-адреса DHCP-клієнта, якому призначається

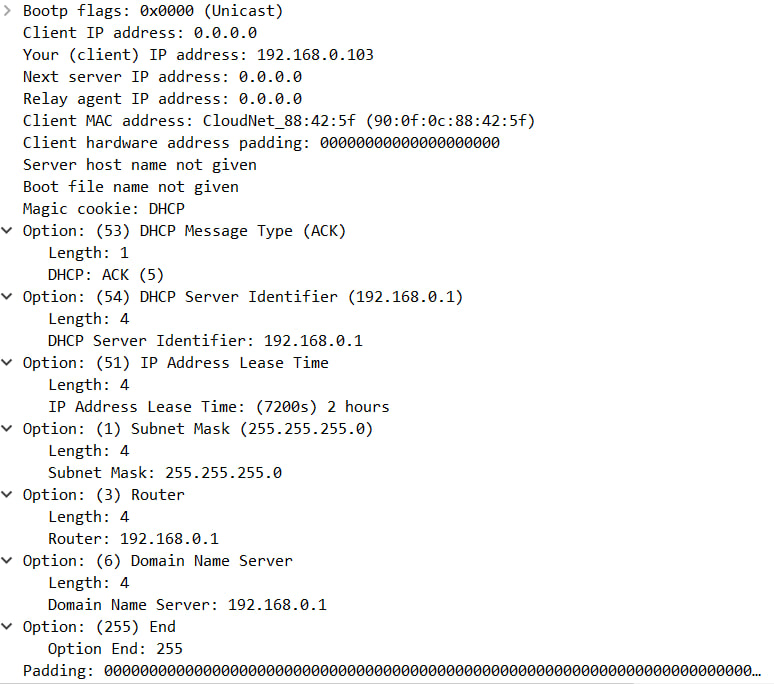
IP-адреса та інші мережеві параметри.

1. Інформація, що передається у DHCP запиті:

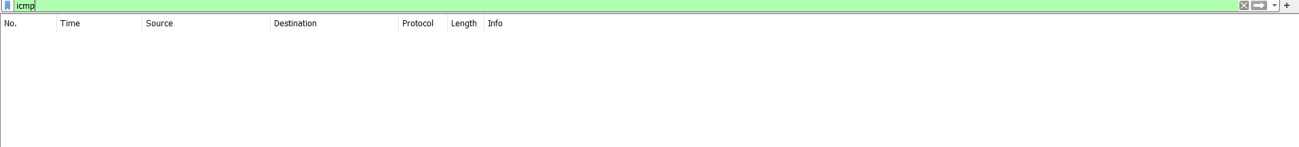




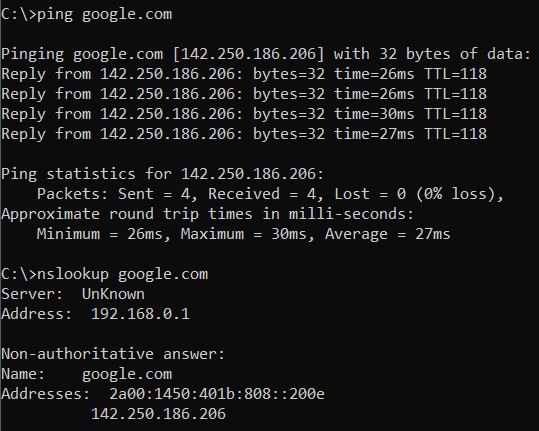
1. Ввів у консолі команду *hostname* та переконався, що ім’я комп’ютера збігається з іменем у DHCP-запиті та з іменем у пункті 3.
2. Інформація, що передається у DHCP відповіді:



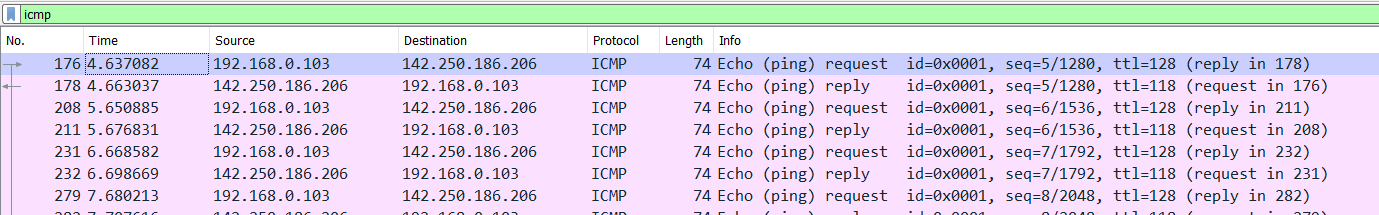
1. Застосувавши фільтр icmp, не знайшов жодного пакета:



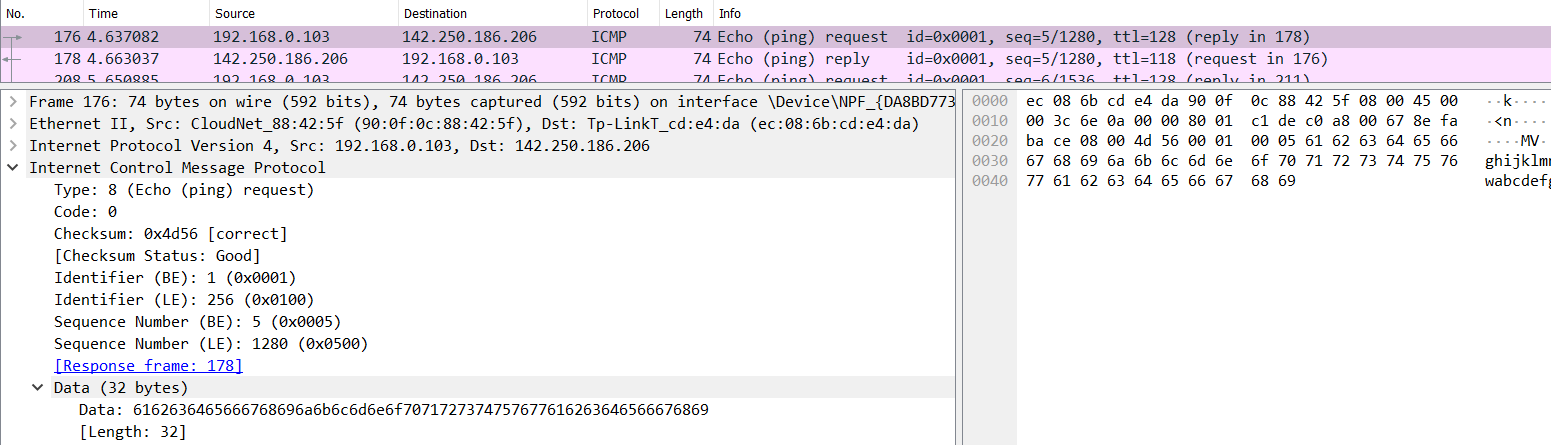
1. Запустив Wireshark заново та почав захоплення пакетів. Застосував команди *ping* та *nsloopup*:



1. Зупинив захоплення пакетів. Знову застосував фільтр icmp та переконався, що цього разу результат не порожній:

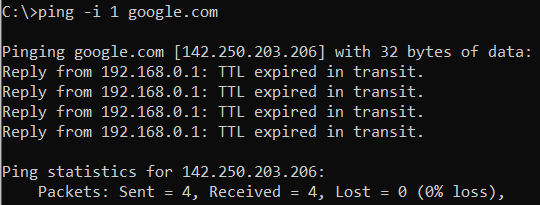


1. TTL в ICMP-запиті та відповіді може відрізнятися через різні шляхи, які вони пройшли в мережі та різні відстані до точки призначення та назад.
2. В попередньому захопленні я отримав 2 типи ICMP-повідомлень: 8 - ехо-запит та 0 – ехо відповідь:

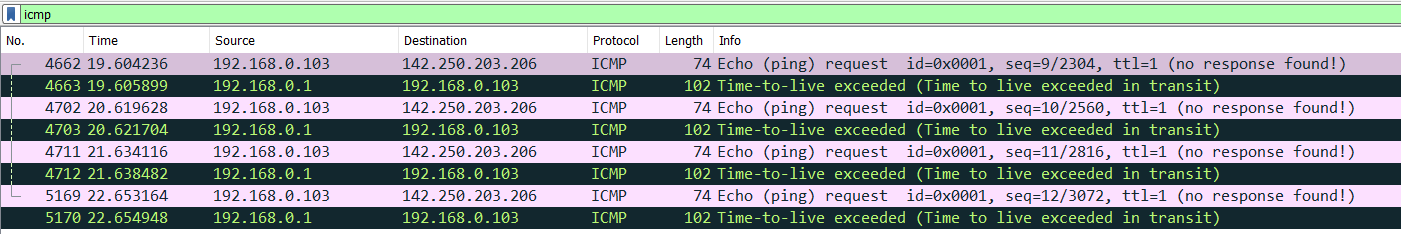




1. Почав заново захоплення пакетів. Після цього викорисав команду *ping -i 1 google.com* та припинив захоплення пакетів:



Переконався, що всі пакети були втрачені:

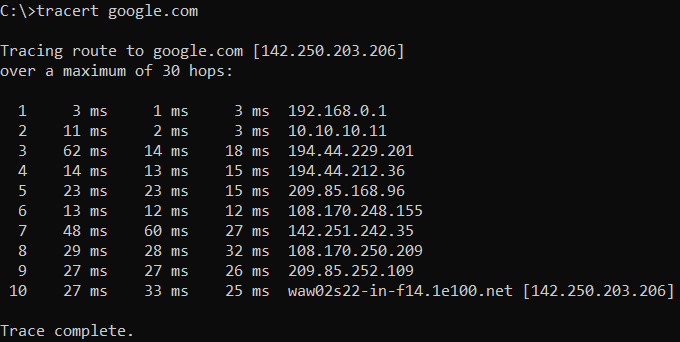


Різниця в адресах отримувачів для запитів між цими пакетами і попередніми полягає в тому, що для цих кожен пакет намагався отримати відповідь, але не зміг отримати через закінчення TTL. Попередні пакети отримали IP-адресу цільового пристрою або сервера в Інтернеті.

Різниця в адресах відправників для відповідей полягає в тому, що для цих пакетів - це IP-адреса маршрутизатора або шлюзу, який згенерував повідомлення ICMP Time Exceeded, в той час як попередні пакети отримали у відповідь IP цілі.

Різниця в адресах отримувачів для відповідей полягає в тому, що для цих пакетів це IP-адреса відправника початкового запиту ICMP, а для попередніх це IP-адреса відправника запиту.

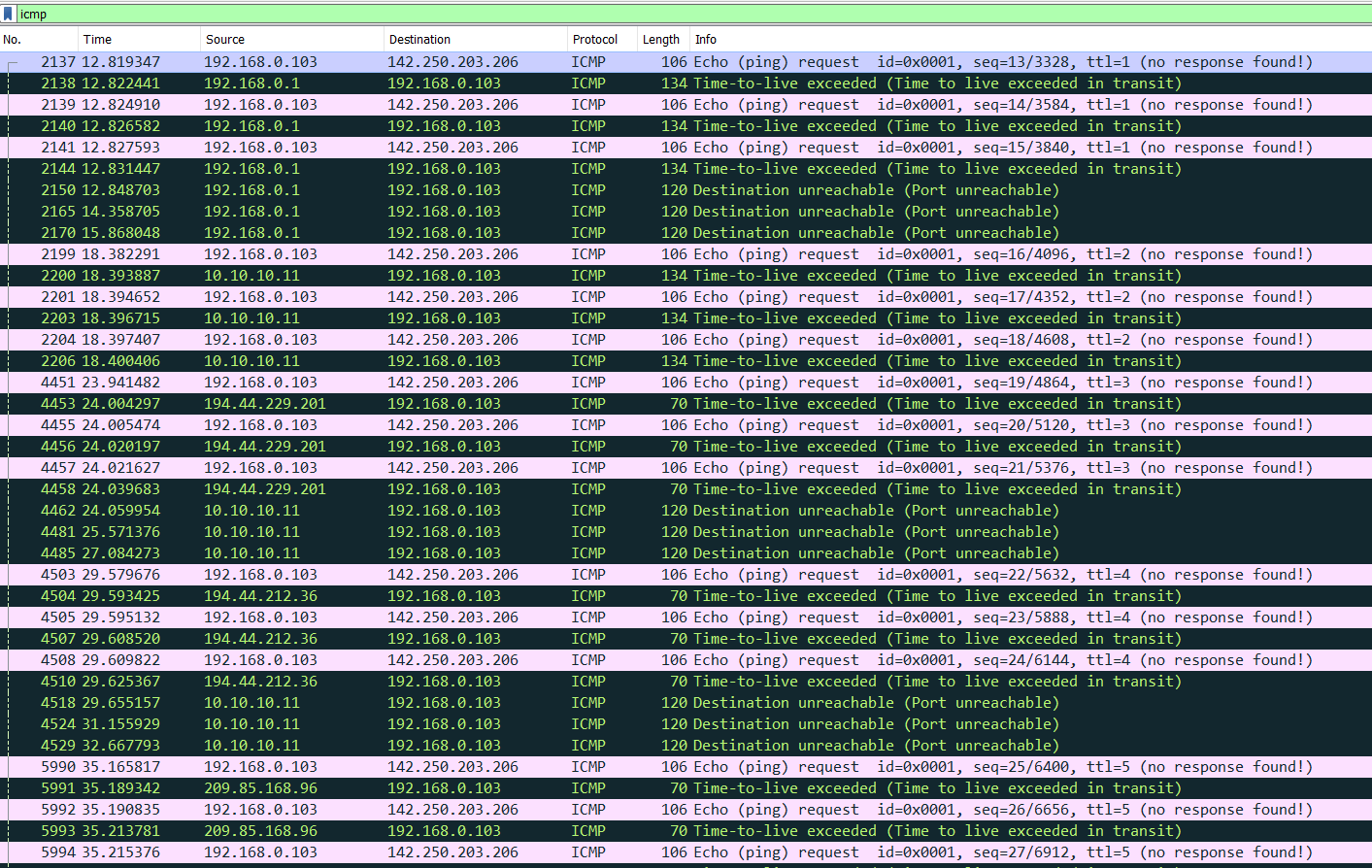
31. Скористався командою *tracert*, попередньо почавши знову захоплення пакетів:



Отже, щоб пакет потрапив до сервера google.com з ІР-адресою

142.250.203.206, йому потрібно пройти 9 проміжних маршрутизаторів

32. Зупинив захоплення пакетів. Помітивши певну послідовність полів TTL для пакетів:

 дійшов наступного висновку. Утиліта tracert використовує ICMP-пакети для відстеження маршруту до пункту призначення. Кожен пакет має поле TTL (Time to Live), яке визначає, скільки маршрутизаторів може пройти пакет перед викиданням. Починаючи з TTL = 1, кожен маршрутизатор, через який проходить пакет, зменшує TTL на одиницю, і якщо TTL стає рівним нулю, маршрутизатор відкидає пакет та надсилає повідомлення про помилку назад.

33. Стандартна утиліта ping сама по собі не надає детальної інформації про маршрут, яким пакети досягають місця призначення. ping в основному перевіряє доступність хоста, надсилаючи повідомлення ICMP Echo Request і очікуючи повідомлень ICMP Echo Reply.

**Висновок**: Під час виконання лабораторної роботи я здобув практичні навички з інтерпретації ІР-пакетів і повідомлень керуючих протоколів, а також використання консольних утиліт для діагностики мережі на мережевому рівні.