Міністерство освіти і науки України

Львівський національний університет імені Івана Франка

Факультет прикладної математики та інформатики

Кафедра програмування

Звіт

до лабораторної роботи №7

з теми

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

Підготував:

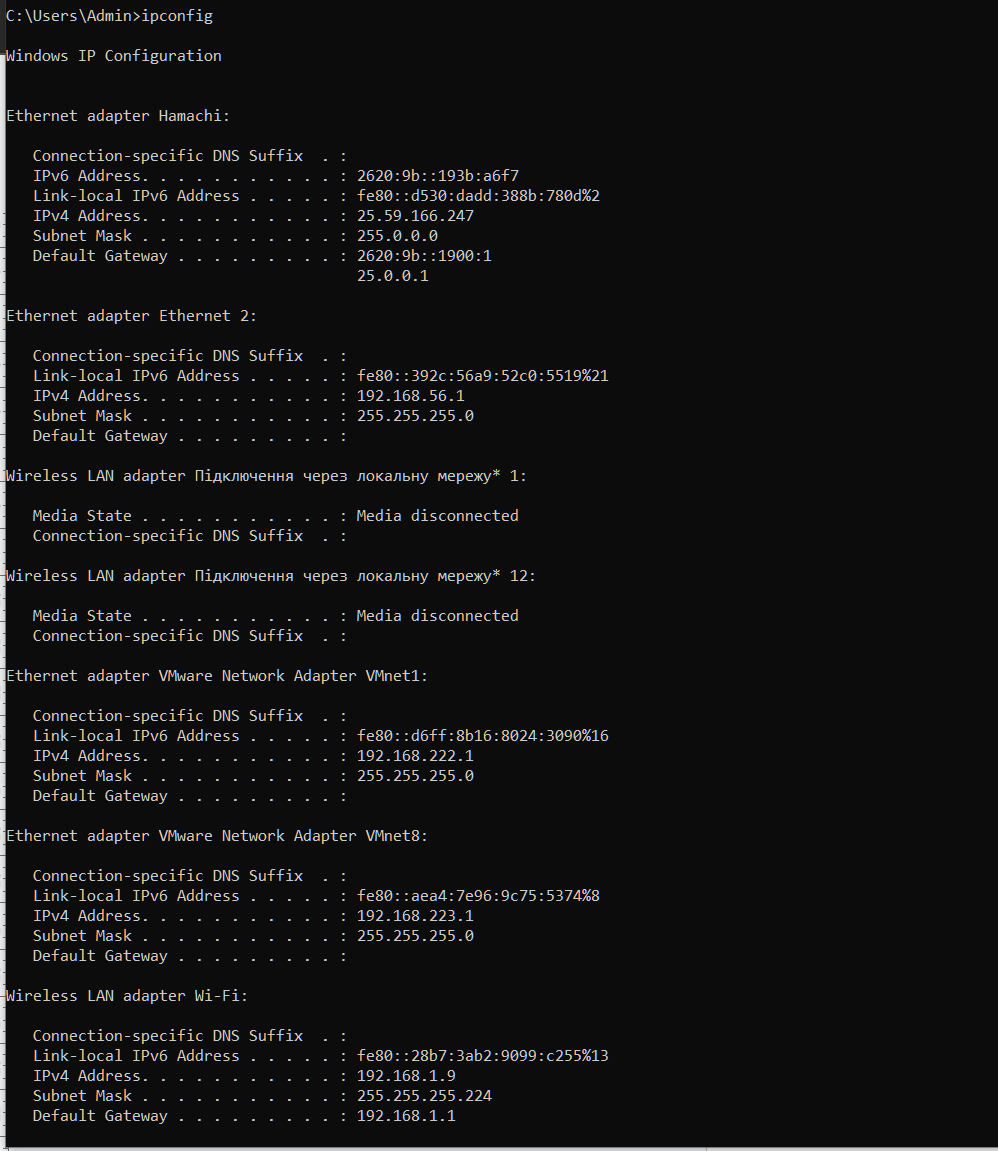
cтудент ПМІ-31

Процьків Назарій

Львів 2023

**Хід роботи**

1. Ознайомився з базовою мережевою конфігурацією свого комп’ютера, виконавши в консолі команду ipconfig та більше детальною конфігурацією за допомогою ipconfig/all:



1. Команда ipconfig/release використовується для вивільнення поточного IP-адреси комп'ютера у мережі. При виклику цієї команди комп'ютер надсилає повідомлення до DHCP-сервера, який відповідає за призначення IP-адресу.

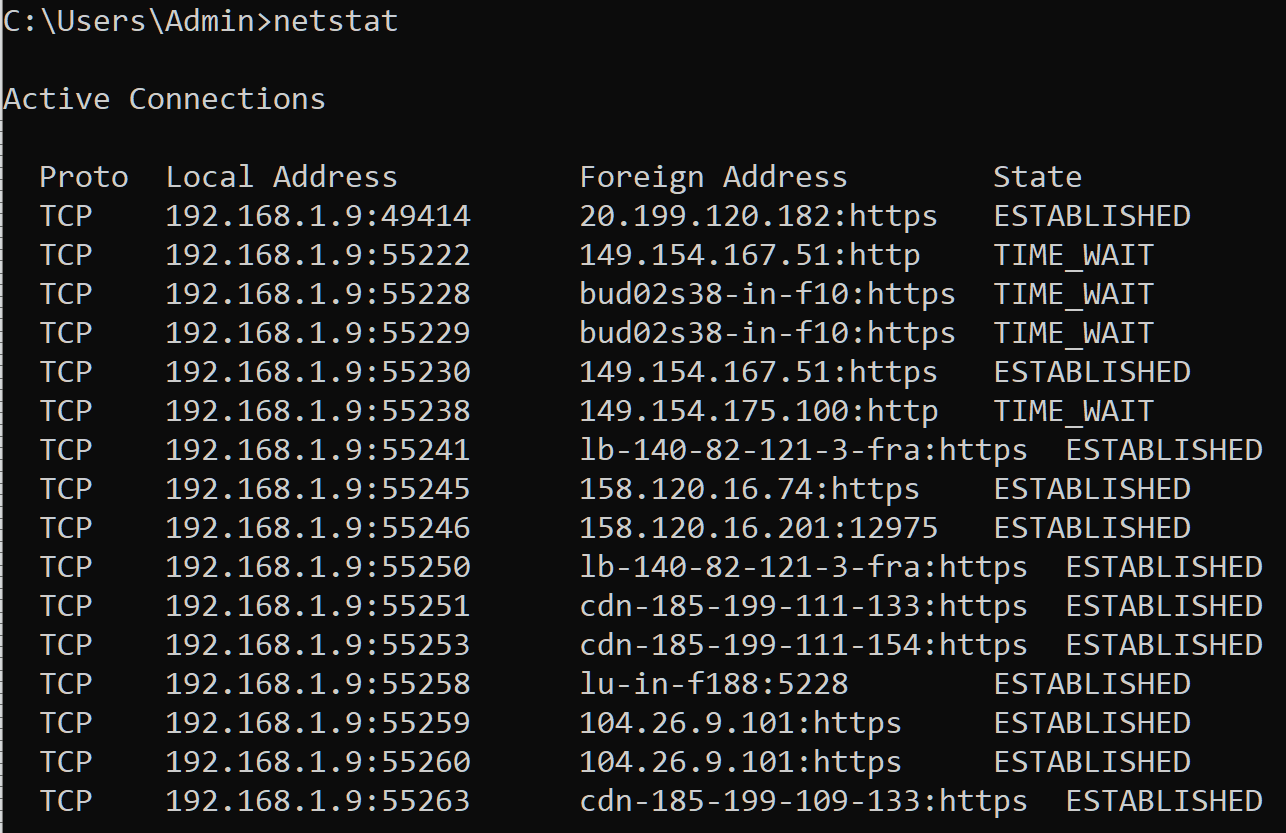
Після виклику команди /release комп'ютер втрачає свою поточну IP-адресу та будь-які інші налаштування мережі, пов'язані зі старою IP-адресою.

1. ipconfig/renew – команда, яка використовується для отримання нової IP-адреси від DHCP-сервера після того, як IP-адреса була вивільнена за допомогою команди /release.

Після виклику команди /renew комп'ютер надсилає запит до DHCP-сервера для отримання нової IP-адреси та інших налаштувань мережі.

Цією командою можна скористатись, коли потрібно змінити IP-адресу чи виправити проблеми з підключенням до мережі.

1. За допомогою команди netstat переглянув активні ТСР-з’єднання

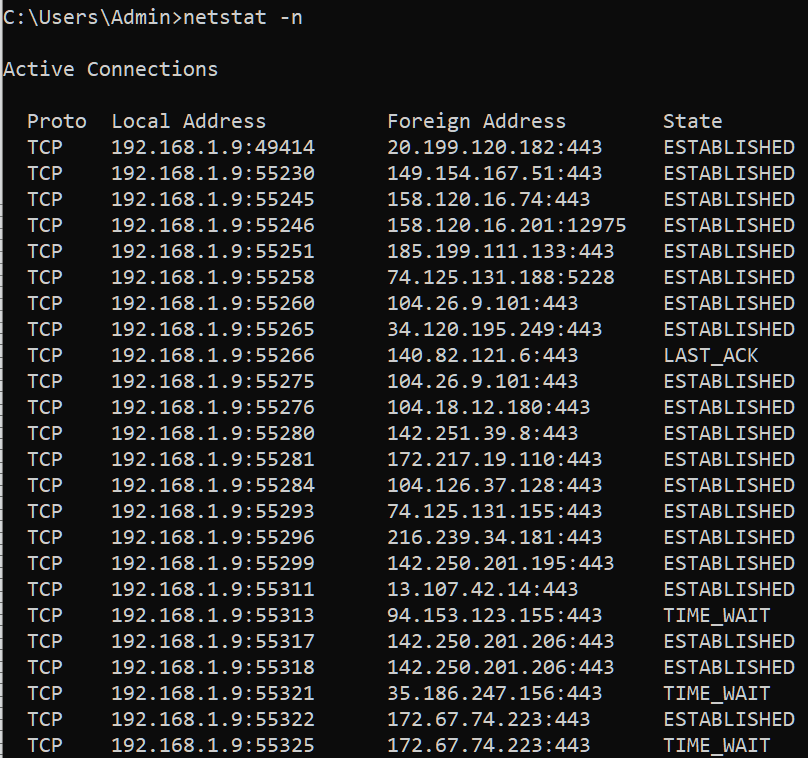
5. SYN\_SENT виникає, коли клієнт ініціює з'єднання, виславши сигнал SYN серверу.

ESTABLISHED позначає успішне встановлення з'єднання між клієнтом і сервером.

CLOSE\_WAIT вказує на те, що одна із сторін завершила передачу даних, але клієнт все ще може надсилати дані, чекаючи на сигнал від клієнта про готовність до закриття.

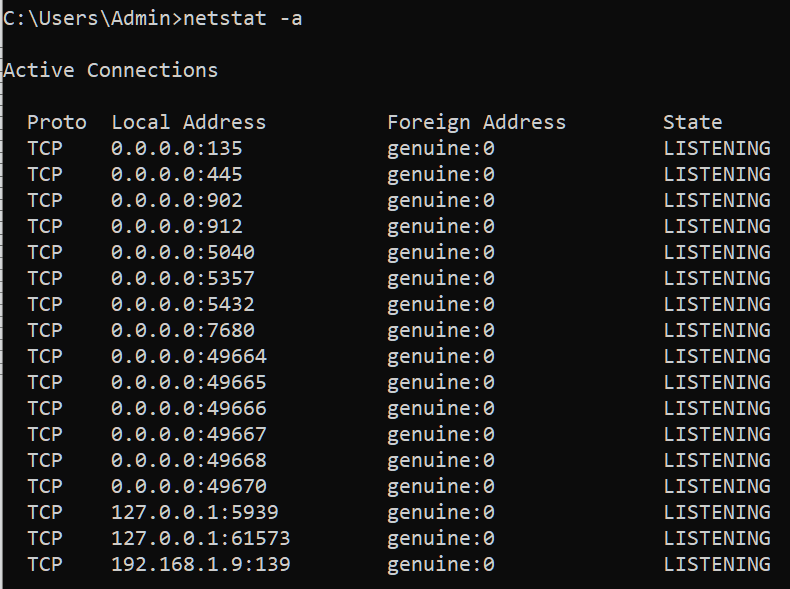
TIME\_WAIT виникає після закриття з'єднання.

1. При використанні netstat -n, відбувається вивід інформації, не виконуючи розгортання імен (hostname) та портів у числовому вигляді. Замість імен будуть показані числові представлення IP-адрес та номерів портів.

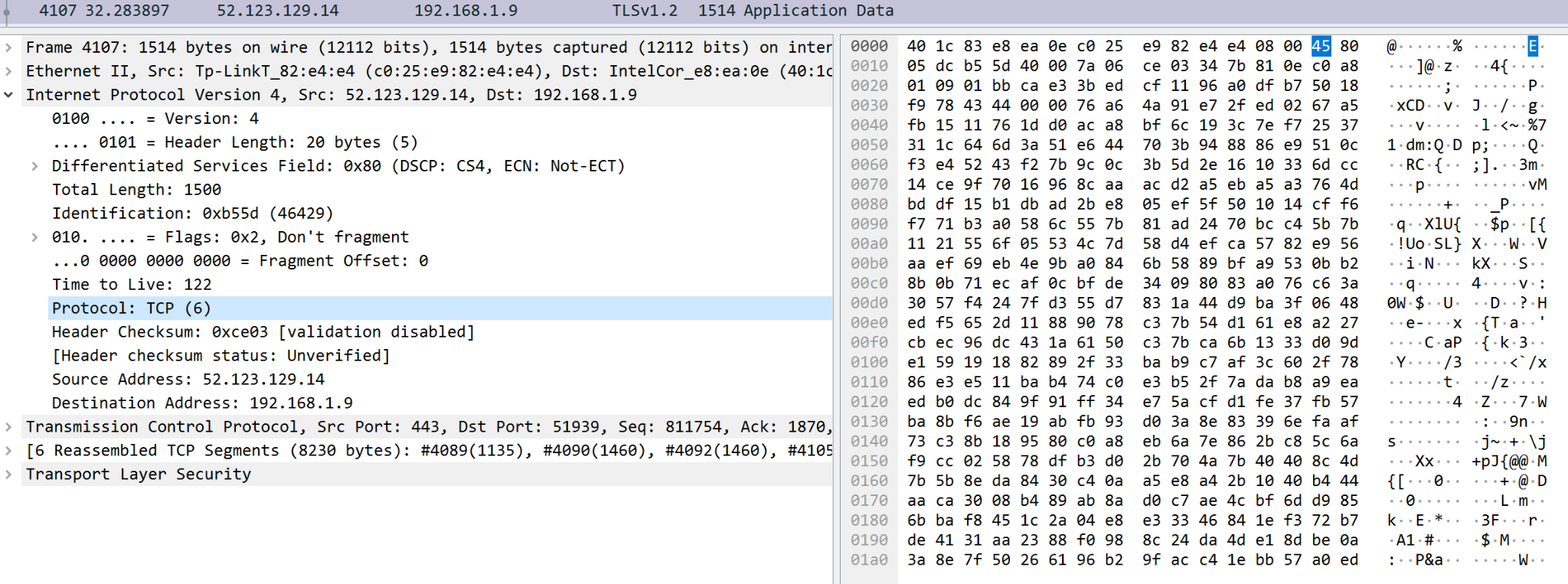


Параметр -a вказує netstat виводити інформацію про всі з'єднання та прослуховуючі порти, включаючи ті, які знаходяться в стані listening.

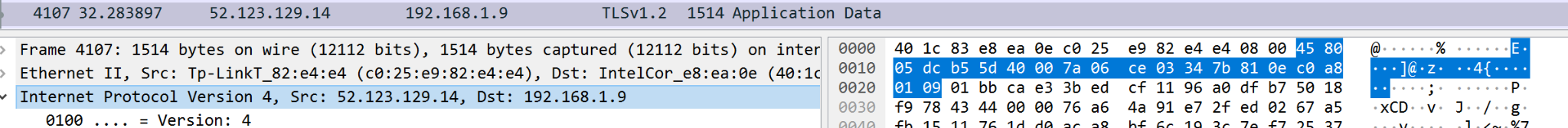
Використання цього параметра допомагає побачити всі активні мережеві з'єднання та порти на комп'ютері.



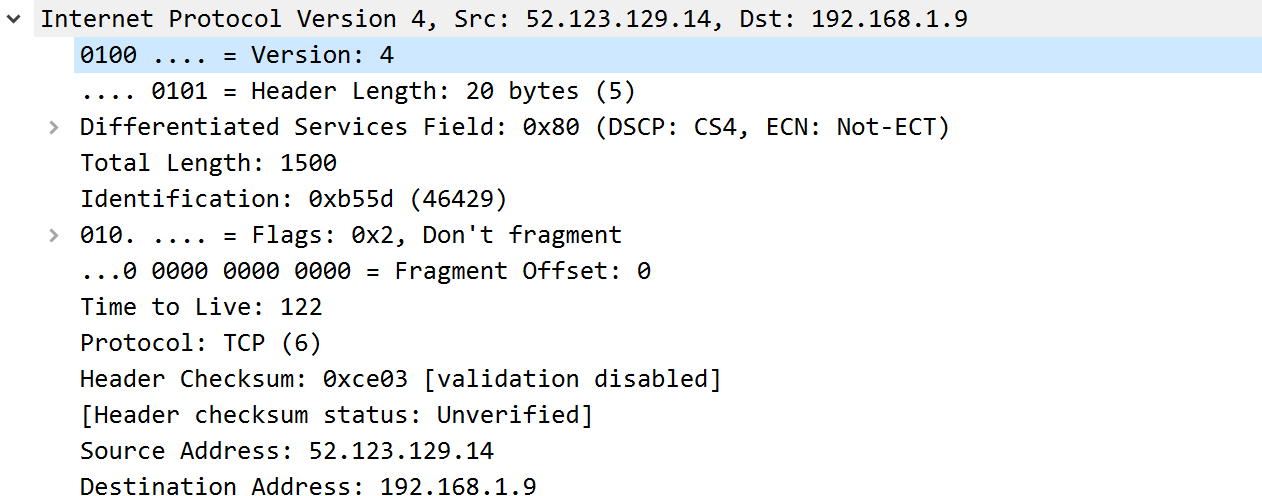
1. Запустив Wireshark, почав захоплення пакетів. Вибрав пакет для аналізу.



1. Клацнув на рядку Internet Protocol version 4 в області “Ієрархічний вміст пакета”. В області “Бітове подання” підсвітились біти, які відповідають заголовку ІР-пакета:



1. Довжина заголовка: це 4-бітне поле, що вказує на розмір IP-заголовка у 32-бітних блоках. Мінімальна довжина IP-заголовка складає 20 байтів, тому у цьому полі можна бачити значення 5, бо 20 байтів це 5 \* 32 біт. Максимальне можливе значення з 4 біт = 15, що відповідає довжині заголовка у 60 байтів, враховуючи 32-бітні інкременти. Це саме поле також називається IHL.



1. Для знаходження розміру корисних даних у пакеті IPv4, скористався полем Total Length у заголовку IPv4. Це 16-бітне поле, яке вказує на загальну довжину пакета.

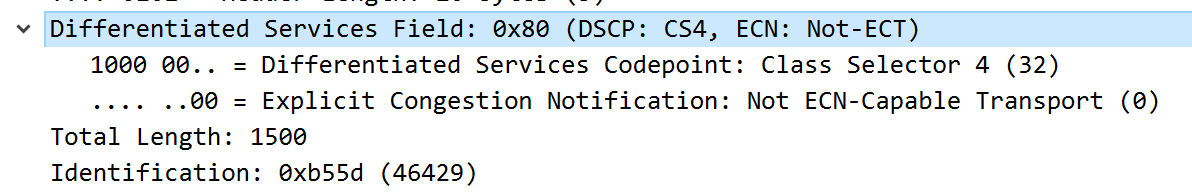
Загальний розмір пакета визначається як сума розміру заголовка та розміру корисних даних. Таким чином, розмір корисних даних можна знайти віднімаючи розмір заголовка від загальної довжини пакета.

* 1500 - 20 = 1480 байт

1. Адреса відправника(52.123.129.14) – глобальна адреса, яка може вказувати на зовнішній пристрій

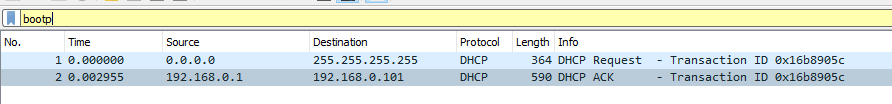
Адреса отримувача(192.168.1.9) - адреса мого Wifi-адаптера.

1. DSCP є розширенням ToS і використовує 6 бітів для кодування рівнів обслуговування. DSCP може включати як біти ToS, так і нові біти. Загалом, DSCP складається з шести бітів, які використовуються для визначення класу обслуговування.
   1. Class Selector: Перші три біти вказують на клас обслуговування і можуть імітувати значення старих бітів ToS.
   2. Drop Probability (Ймовірність втрат): Це два біти, які можуть вказувати ймовірність втрат для пакета.
   3. Explicit Congestion Notification (ECN): Останній біт використовується для реалізації ECN, що дозволяє обмінюватися інформацією про перенавантаження в мережі.



13. Цей пункт в мене не вийшло зробити, я пробував кілька разів, але зовсім не появлялись ніякі пакети протоколу DHCP. Тому я розглянув як цю секцію завдань (з цього по 17 пункт) зробив інший студент і пояснив це.

За допомогою фільтру bootp відобразив пакети протоколу DHCP.



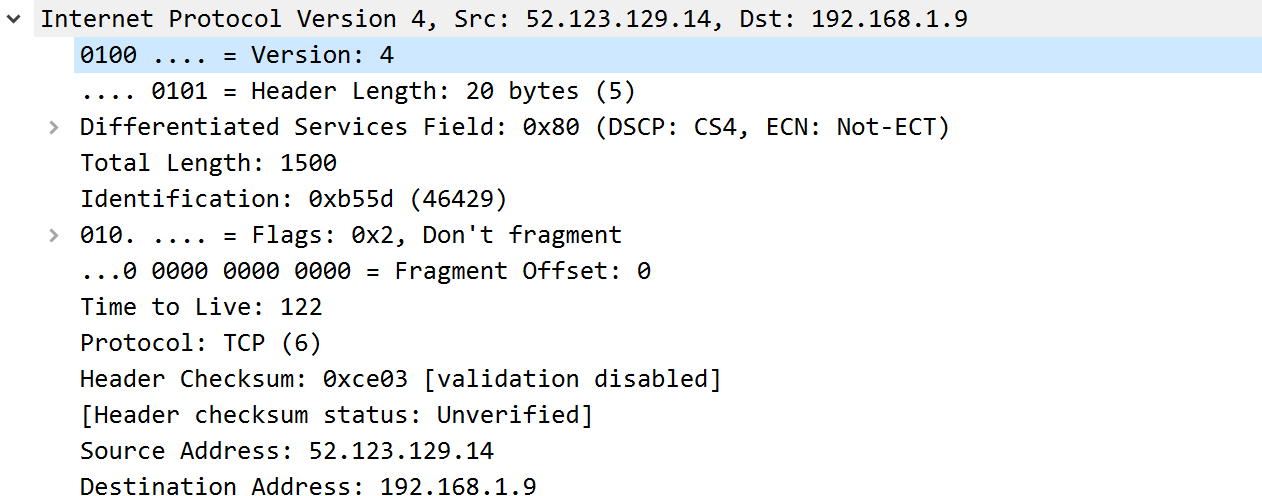
14. ІР-адреси відправника та отримувача у DHCP-запиті:

* 1. Source: Зазвичай вказується 0.0.0.0 або IP-адреса самого клієнта, оскільки DHCP-клієнт ще не отримав IP-адресу від DHCP-сервера.
  2. Destination: Зазвичай вказується 255.255.255.255, оскільки DHCP-клієнт спрямовує свій запит на весь локальний підмережевий діапазон і намагається звернутися до будь-якого доступного DHCP-сервера.



15. ІР-адреси відправника та отримувача у DHCP-відповіді:

* 1. Source: Це IP-адреса DHCP-сервера, який відправляє підтвердження клієнту.
  2. Destination: Це IP-адреса DHCP-клієнта, якому призначається IP-адреса та інші мережеві параметри.



16. Option 53: DHCP Message Type (Request)

Значення 3 вказує, що це DHCP-запит типу "Request". Клієнт просить підтвердження або оновлення своєї конфігурації IP.

Option 61: Client Identifier

Вказує ідентифікатор клієнта, включаючи тип апаратного забезпечення (Ethernet) та MAC-адресу клієнта.

Option 50: Requested IP Address

Вказує IP-адресу, яку клієнт запитує. У цьому випадку, 192.168.0.101.

Option 12: Host Name

Вказує ім'я хоста клієнта. У цьому випадку, "DESKTOP-21Q2D8Q".

Option 81: Client Fully Qualified Domain Name

Вказує повністю кваліфіковане доменне ім'я клієнта. У цьому випадку, "DESKTOP-21Q2D8Q".

Option 60: Vendor Class Identifier

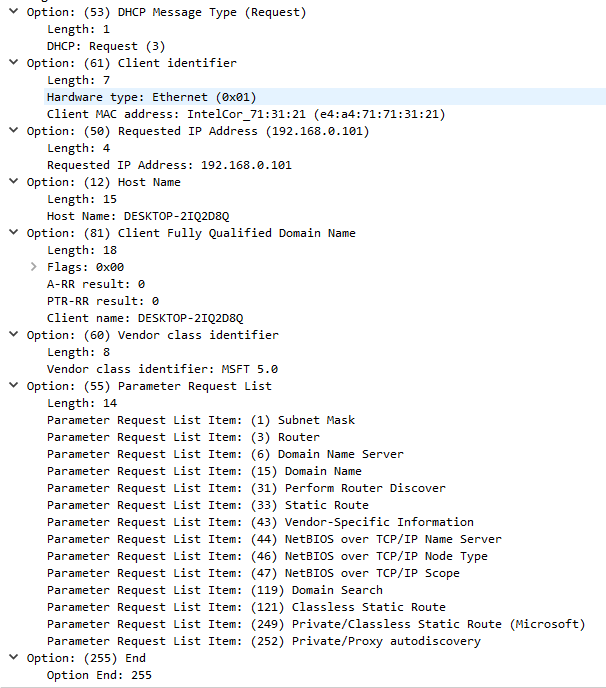
Вказує ідентифікатор вендора, у цьому випадку "MSFT 5.0".

Option 55: Parameter Request List

Вказує список запитуваних параметрів від DHCP-сервера.

Option 255: End

Вказує завершення списку опцій.



16. За допомогою команди hostname переконався, що ім’я мого комп’ютеру співпадає з іменем у DHCP-запиті.



17. Option 53: DHCP Message Type (ACK)

Значення 5 вказує, що це DHCP-підтвердження типу "ACK" (Acknowledgment). Це повідомлення підтверджує прийняття та надання IP-адреси клієнту.

Option 54: DHCP Server Identifier

Вказує IP-адресу DHCP-сервера, який надає підтвердження. У цьому випадку, 192.168.0.1.

Option 51: IP Address Lease Time

Вказує час, на який надається IP-адреса клієнту. У цьому випадку, 7200 секунд (2 години).

Option 1: Subnet Mask

Вказує маску підмережі для IP-адреси, яку клієнт отримав. У цьому випадку, 255.255.255.0.

Option 3: Router

Вказує IP-адресу маршрутизатора (шлюзу), який використовуватиметься клієнтом. У цьому випадку, 192.168.0.1.

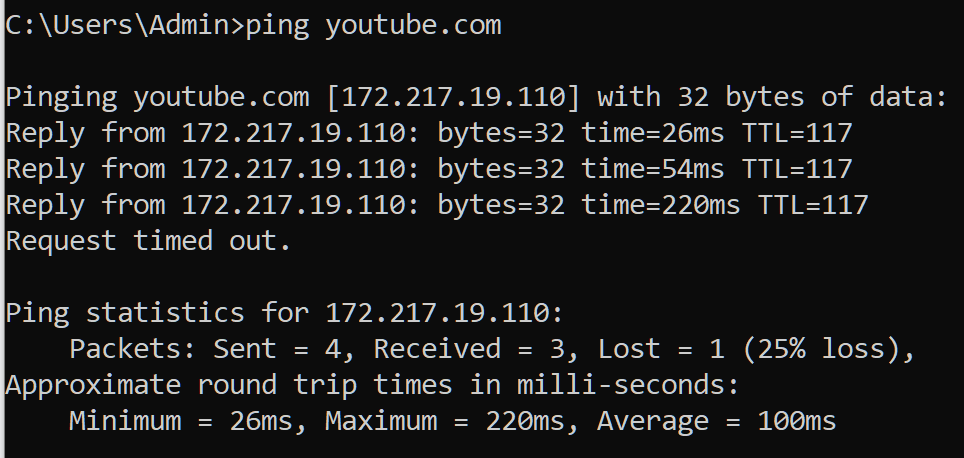
Option 6: Domain Name Server

Вказує IP-адреси серверів DNS, які клієнт повинен використовувати. У цьому випадку, 192.168.0.1 та 0.0.0.0 (вказує, що DNS-сервер не визначено).

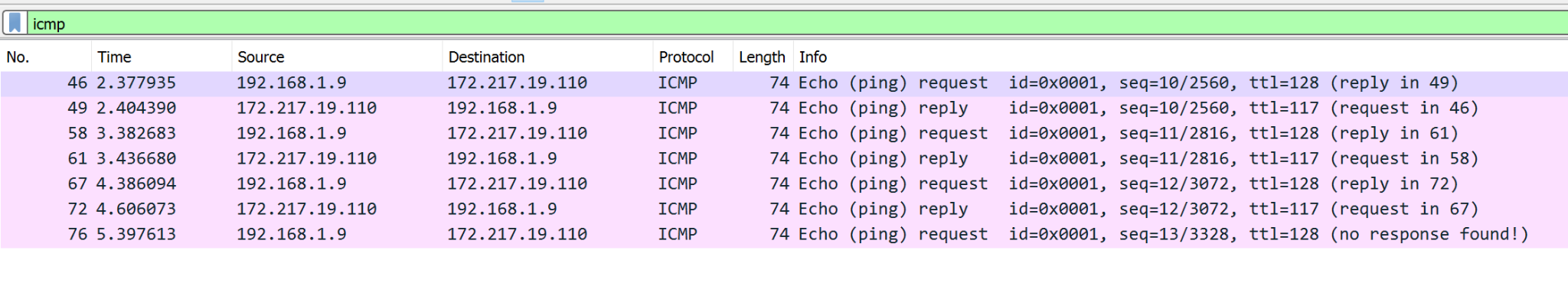
Option 255: End

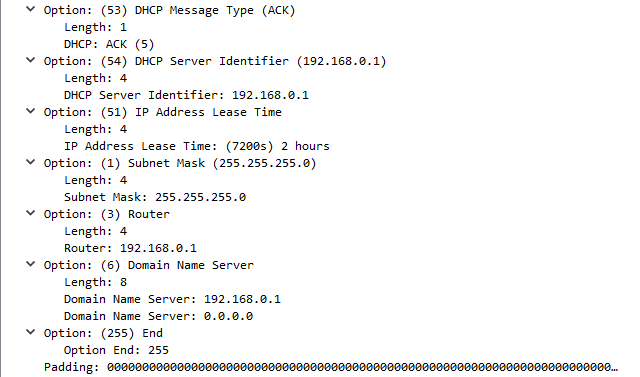
Вказує завершення блоку опцій в DHCP-повідомленні. Після цієї опції не слід вказувати інші опції. "Padding" використовується для забезпечення того, що загальна довжина DHCP-повідомлення буде кратної певному розміру.

18. Реалізував перехоплення ICMP-пакетів за допомогою консольної утиліти ping.



19. Бачу непорожній результат при фільтруванні:

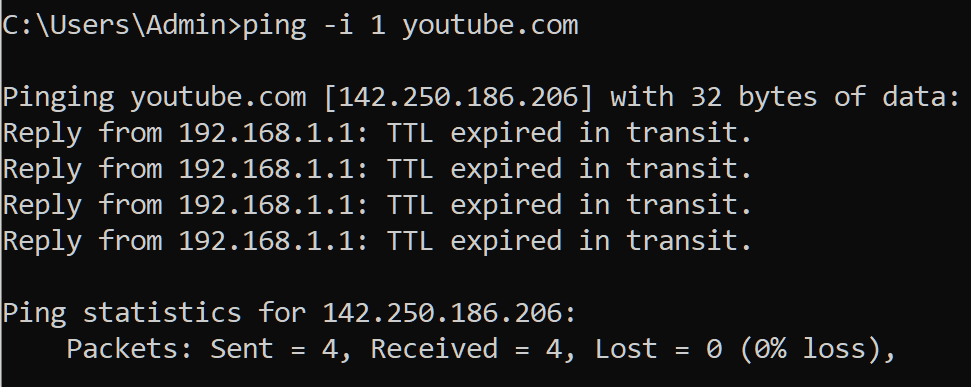




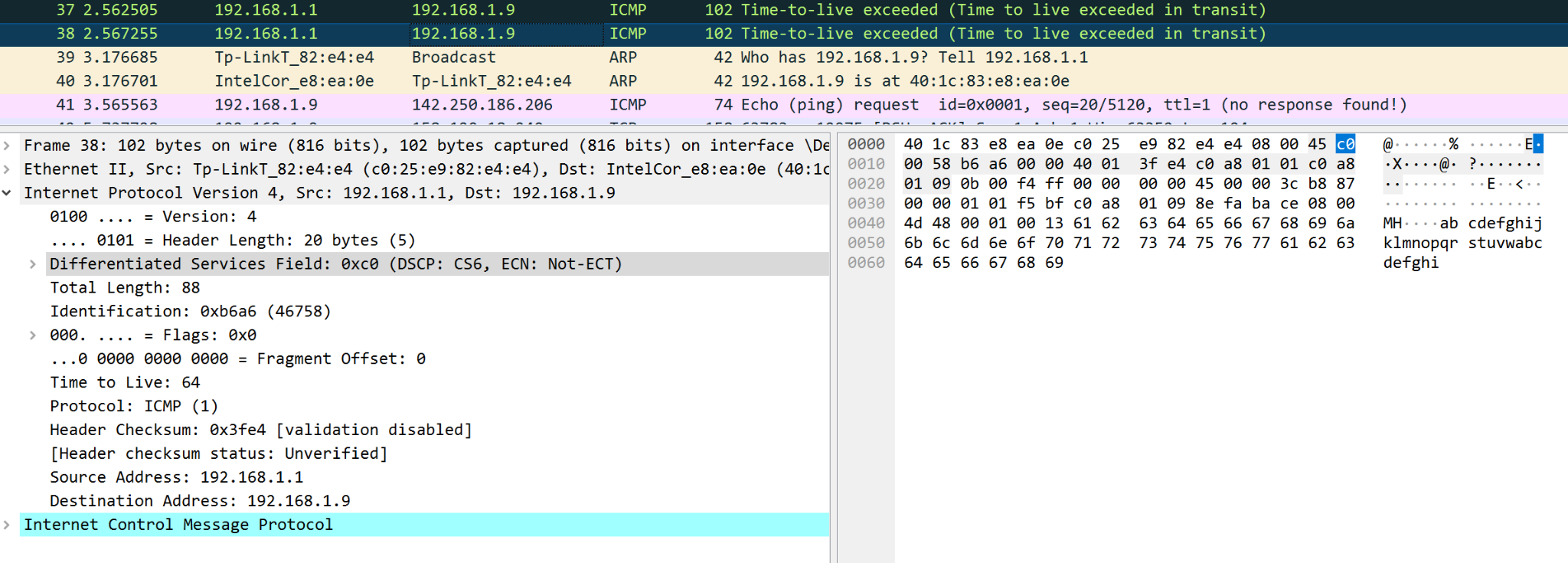
20. TTL в ICMP-запиті та відповіді може відрізнятися через різні шляхи, які вони пройшли в мережі та різні відстані до точки призначення та назад.

21. Аналіз отриманих пакетів показав, що ми отримали 2 типи ICMP-повідомлень:

* 1. 8-ехо-запит
  2. 0-ехо-відповідь

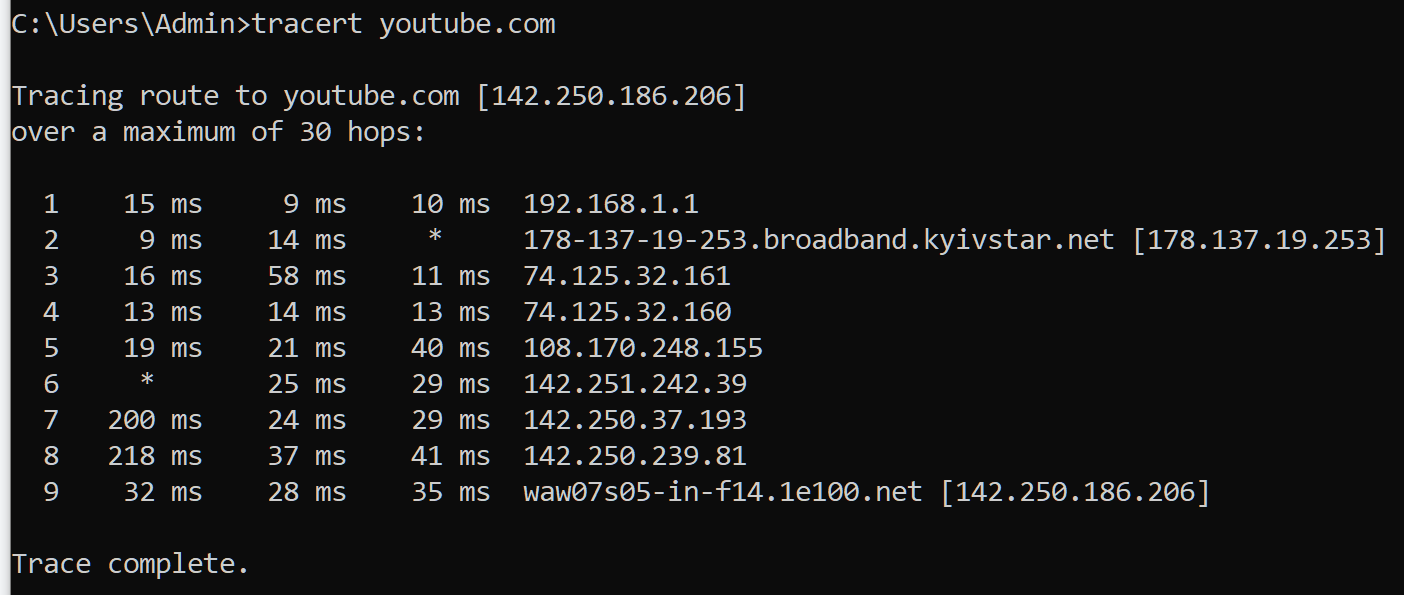
За допомогою задання TLL=1 я спробував отримати інший тип повідомлень

Отримав повідомлення типу 11

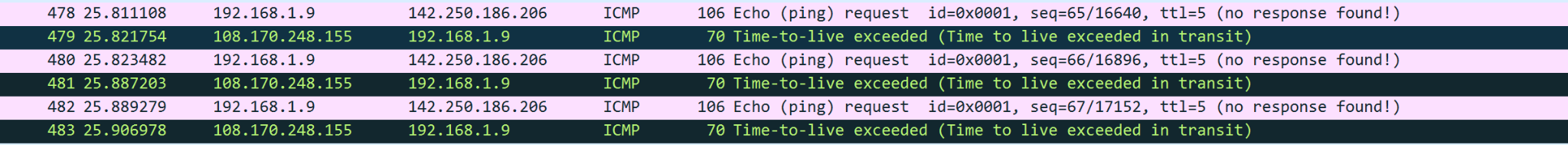


22. Коли TTL встановлено на 1, це означає, що пакет може пройти лише через один маршрутизатор. Якщо цей маршрутизатор відправляє пакет назовні мережі (наприклад, ретранслює його на іншу мережу), він може обрати новий IP-адресу для цього пакета.

23. Визначив маршрут, яким проходять пакети від мого ноутбука до отримувача. Проходять 9 додаткових маршрутизаторів.



24. 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.



25. Утиліта ping, зазвичай, не надає повний маршрут, який пакет проходить від джерела до призначення. Проте, існують параметри та інші інструменти, які дозволяють отримати додаткову інформацію про маршрут. Команда "ping -r 5 youtube.com" вказує, що пакет Ping буде містити інформацію про проміжні маршрутизатори для перших 5 етапів маршруту. Важливо врахувати, що якщо маршрут має більше 5 проміжних маршрутизаторів, інформація про них не буде включена в вивід.