**Лабораторна робота № 13**

**Використання Wireshark для перегляду**

**мережного трафіку**

Цілі та задачі

Частина 1: Перехоплення та аналіз локальних ICMP-даних за допомогою Wireshark

**Частина 2: Перехоплення та аналіз віддалених ICMP-даних за допомогою Wireshark**

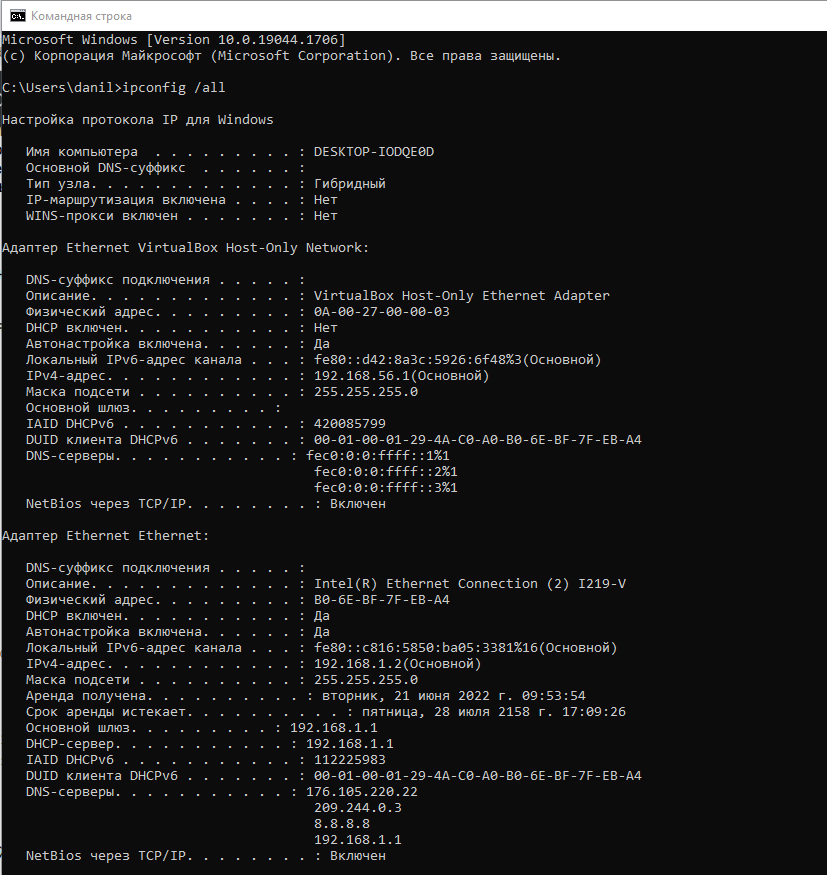
**Хід роботи:**

**Частина 1: Перехоплення та аналіз локальних ICMP-даних за допомогою Wireshark**

**Завдання на лабораторну роботу**

1. Визначення адрес мережної плати Вашого ПК

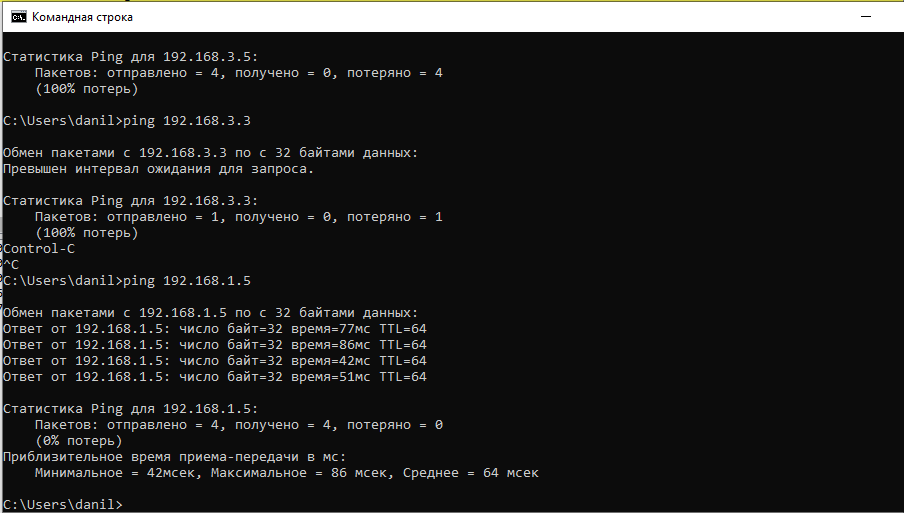
a. У командному рядку введіть команду ipconfig /all, щоб переглянути IP-адресу, MAC-адресу, опис мережної плати Вашого ПК.

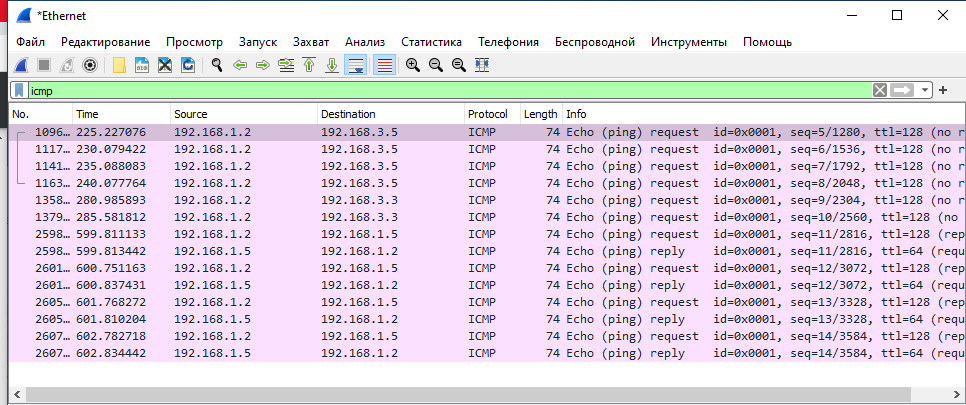


b. Запитайте члена або членів команди про IP-адресу їх ПК та надайтe їм IP-адресу свого ПК. На цьому етапі не повідомляйте їм свою MAC-адресу IP-адреса телефону підключеного до локальної мережі: 192.168.3.3

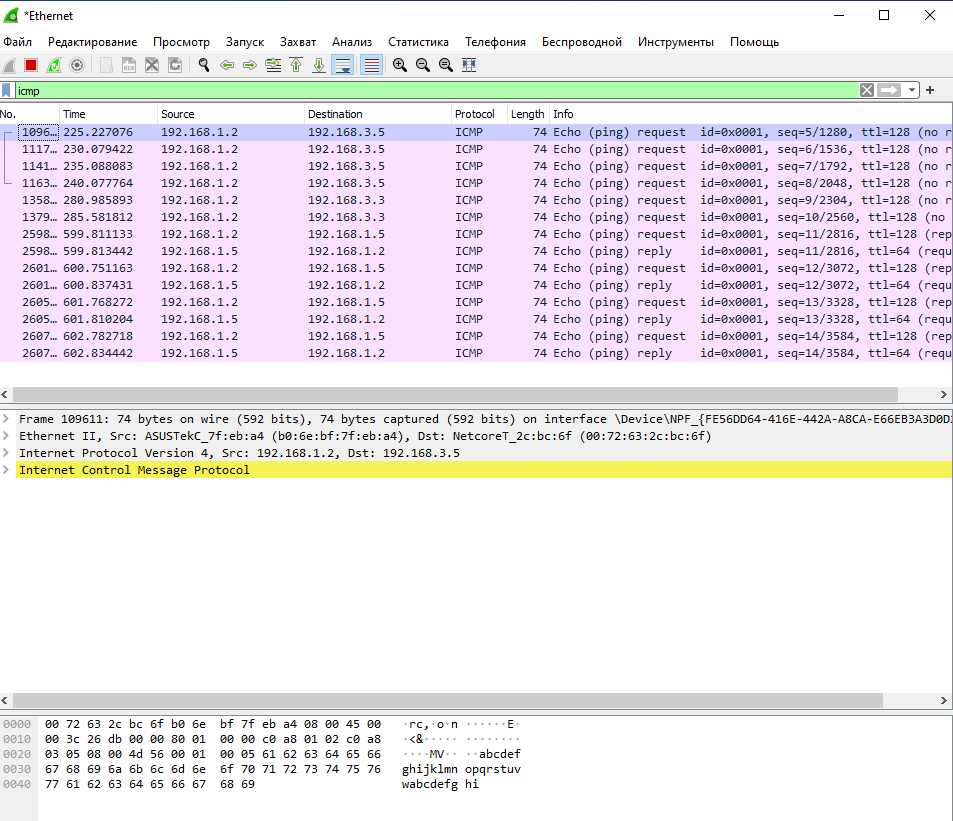
1. Запуск Wireshark і початок перехоплення даних

a. Перейдіть до Wireshark. Двічі натисніть на потрібному інтерфейсі, щоб розпочати перехоплення повідомлень. Переконайтеся, що на потрібний інтерфейс надходить трафік.





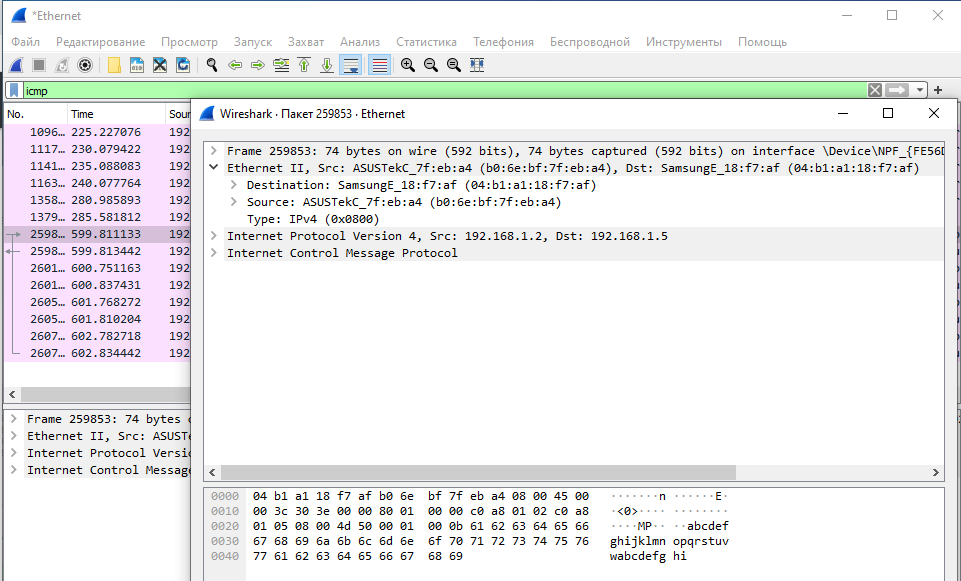
b. У верхній частині вікна Wireshark рядки даних почнуть прокручуватися донизу. Рядки даних, залежно від протоколу, матимуть різне забарвлення. Вони можуть прокручуватися дуже швидко. Швидкість залежатиме від інтенсивності спілкування, яке зараз відбувається між Вашим ПК та іншими вузлами локальної мережі. Для полегшення перегляду даних, які перехоплює Wireshark, та подальшого їх опрацювання можна застосувати фільтри. У цій лабораторній роботі нас цікавить відображення лише повідомлень протоколу ICMP (ping). Наберіть icmp у полі Filter у верхній частині вікна Wireshark і натисніть або Enter, або кнопку Apply (значок стрілочки), щоб переглядати тільки ICMP-повідомлення.



d. Зупиніть перехоплення даних, натиснувши значок Stop Capture

3. Дослідження перехоплених даних

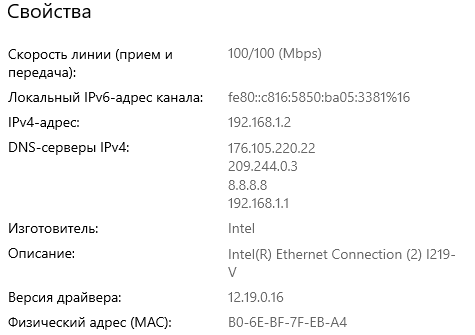
a. У верхній частині вікна Wireshark натисніть на кадр, що містить перший ICMP-запит. Зауважте, що стовпчик Source містить IP-адресу Вашого ПК, а стовпчик Destination містить IP-адресу ПК Вашого колеги по команді (саме того ПК, який Ви пінгували).



Чи співпадає MAC-адреса відправника з MAC-адресою мережної плати/інтерфейсу Вашого ПК?

Чи відповідає у Wireshark MAC-адреса отримувача MAC-адресі ПК Вашого колеги по команді?

Так – співпадає.

Як Ваш ПК отримав MAC-адресу пропінгованого ПК?

Спочатку була введена команда ping у cmd, а далі з перехопленого ICMP-запиту, дані протоколу ICMP інкапсулюються в IPv4-пакет (додається заголовок IPv4), який потім інкапсулюється у кадр Ethernet II (додаються заголовок та трейлер - контрольна сума Ethernet II) для передачі через локальну мережу.

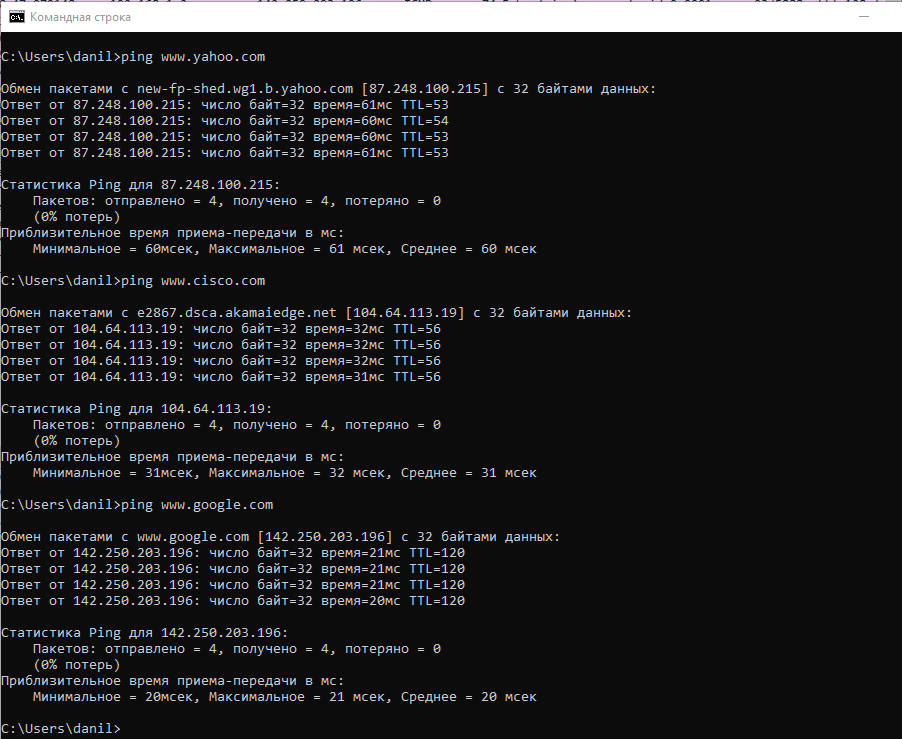
**Частина 2: Перехоплення та аналіз віддалених ICMP-даних за допомогою Wireshark**

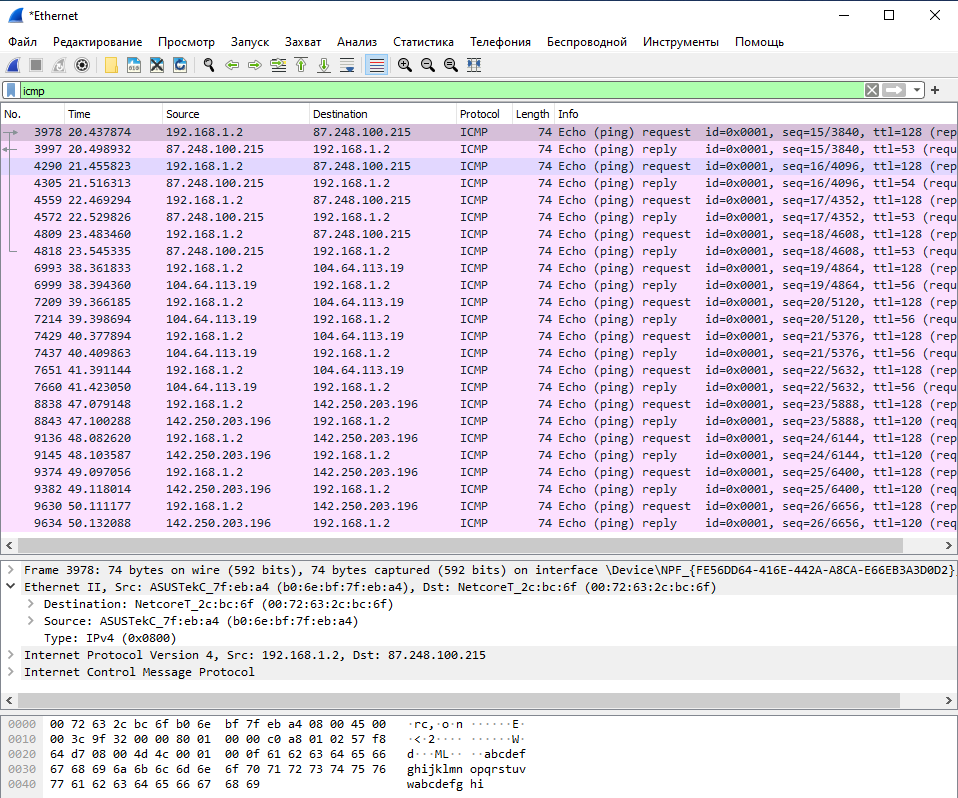
1. Початок перехоплення даних на мережній платі/інтерфейсі.

a. Розпочніть перехоплення даних знову.

b. Wireshark запропонує Вам зберегти раніше перехоплені дані перед початком іншого перехоплення. Зберігати ці дані не обов’язково. Натисніть Continue without Saving.

c. Після активізації перехоплення у командному рядку Windows виконайте команду ping для таких трьох URL-адрес веб-сайтів:





2. Дослідіть та проаналізуйте дані з віддалених вузлів.

IP-адреса для [www.yahoo.com](http://www.yahoo.com): 87.248.100.216

MAC-адреса для [www.yahoo.com](http://www.yahoo.com): NetcoreT\_2c:bc:6f (00:72:63:2c:bc:6f)

IP-адреса для [www.cisco.com](http://www.cisco.com): 104.64.113.19

MAC-адреса для [www.cisco.com](http://www.cisco.com): NetcoreT\_2c:bc:6f (00:72:63:2c:bc:6f)

IP-адреса для [www.google.com](http://www.google.com): 142.250.203.196

MAC-адреса для [www.google.com](http://www.google.com): NetcoreT\_2c:bc:6f (00:72:63:2c:bc:6f)

У цій інформації важливо те, що Wireshark показує ip адреси відправника та отримувача. Також не показує реальні МАС-адреси вузлів віддалених мереж.

Ця інформація відрізняється від першого завдання тим, що ми за допомогою команди ping перевіряли зв’язок з віддаленими вузлами, які не належать нашій локальні мережі. МАС-адреса віддалених вузлів відрізняється від МАС-адреси у локальній мережі, а інші дані залишаються тими ж самими. Не показується МАС- адреса для віддалених вузлів з ціллю приватностні.

***Висновок:*** ознайомився з використання Wireshark для перегляду мережного трафіку