**Міністерство освіти та науки України**

**Київський національний торговельно - економічний університет**

**Факультет інформаційних технологій**

**Кафедра інженерії програмного забезпечення та кібербезпеки**

**ПРАКТИЧНА РОБОТА № 8\_1**

**З ДИСЦИПЛІНИ**

**«Безпека інформаційних систем»**

**НА ТЕМУ:**

ПЕРЕГЛЯД МЕРЕЖЕВОГО ТРАФІКУ ЗА ДОПОМОГОЮ ПРОГРАМИ WIRESHARK

**Виконала:** студентка ФІТ

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Лахно Валерiй Анатолiйович

Київ 2023

**Практична робота №8\_1**

**Тема**: перегляд мережевого трафіку за допомогою програми Wireshark.

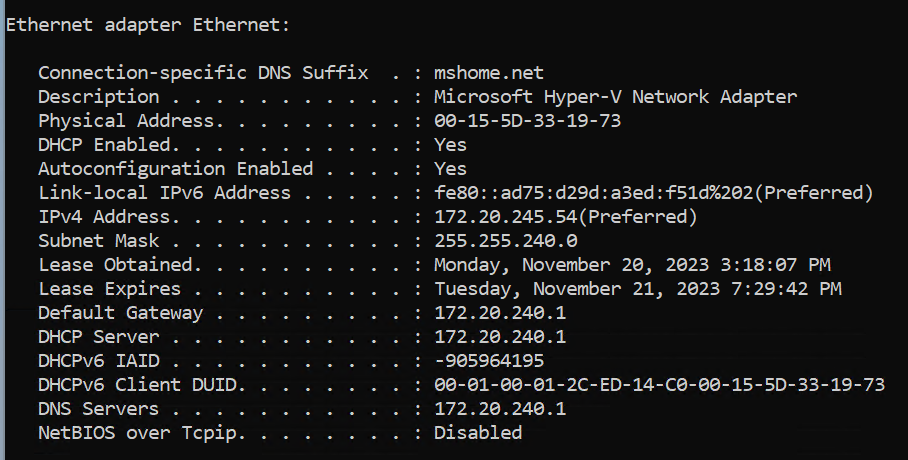
**Хід роботи:**

**Частина 1. Завантаження і установка програми Wireshark (необов'язково)**

Програма вже встановлена.

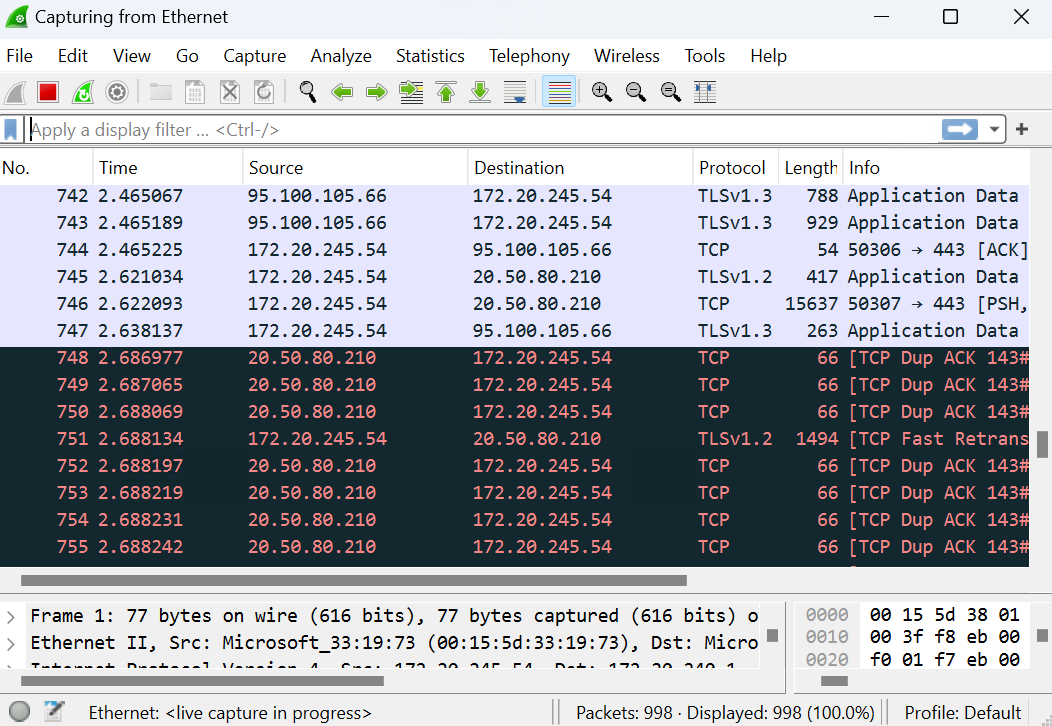
**Частина 2. Збір і аналіз даних протоколу ICMP по локальних вузлівв програмі Wireshark**

1. Визначаємо адреси інтерфейсів нашого ПК.
   1. Відкриваємо вікно командного рядка та вводимо команду ipconfig /all. Знаходимо IP-адресу інтерфейсу ПК – *172.20.245.54* і МАС-адресу (фізична адреса) – *00-15-5d-33-19-73*.

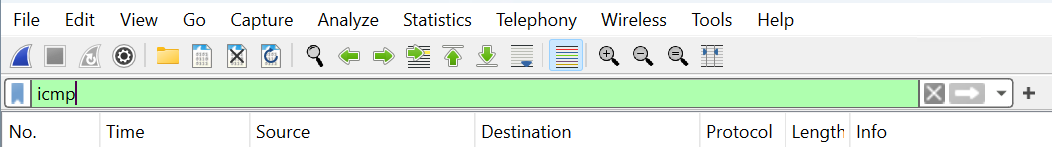


1. Запускаємо програму Wireshark і починаємо перехоплення даних.
   1. Обираємо потрібний інтерфейс та натискаємо Start.

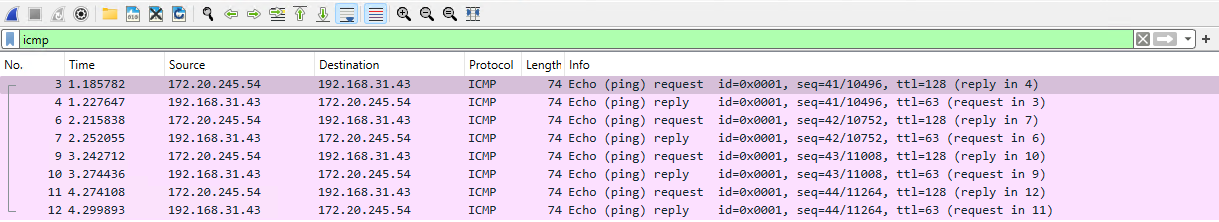
У верхній частині вікна програми Wireshark почне прокручуватися інформація. Рядки даних виділяються різними кольорами залежно від протоколу.



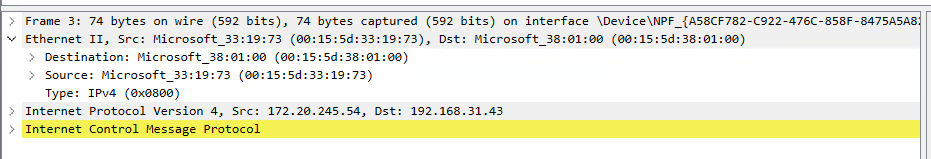
* 1. Для того, щоб вивести лише протокольні блоки даних (PDU) ICMP (ехо-запит за допомогою команди ping), нам потрібно в поле фільтра ввести icmp.



* 1. Відкриваємо вікно командного рядка і відправляємо ехо запит за допомогою команди ping на іншу IP-адресу.



1. Вивчаємо отримані дані
   1. Вибираємо PDU-кадри першого запиту ICMP в верхньому розділі вікна програми Wireshark. Не змінюючи вибір PDU-кадру в верхньому розділі програми, переходимо в середній розділ. Натискаємо на символ > зліва від рядка «Ethernet II», щоб побачити МАС-адреси джерела іпризначення.



Як ми можемо побачити, MAC-адреса джерела (Source) збігається з інтерфейсом нашого комп’ютера.

Для того, щоб дізнатися MAC-адресу ПК, на який був відправлений запит, комп’ютер робить наступне:

* Визначає IP-адресу цільового пристрою
* Перевіряє свій ARP-кеш, щоб побачити, чи вже відомий MAC-адресу для вказаної IP-адреси. Якщо він там є, використовується збережена інформація, і відправляється ехо-запит.
* Якщо в ARP-кеші відсутня інформація про відповідність IP- та MAC-адрес, то ваш комп'ютер відправляє ARP-запит на всю мережу, запитуючи про MAC-адрес пристрою з вказаною IP-адресою.
* Призначений пристрій відповідає на ARP-запит, надсилаючи свій MAC-адрес.
* Комп'ютер отримує відповідь і оновлює свій ARP-кеш, додаючи відомості про те, який MAC-адрес відповідає вказаній IP-адресі.

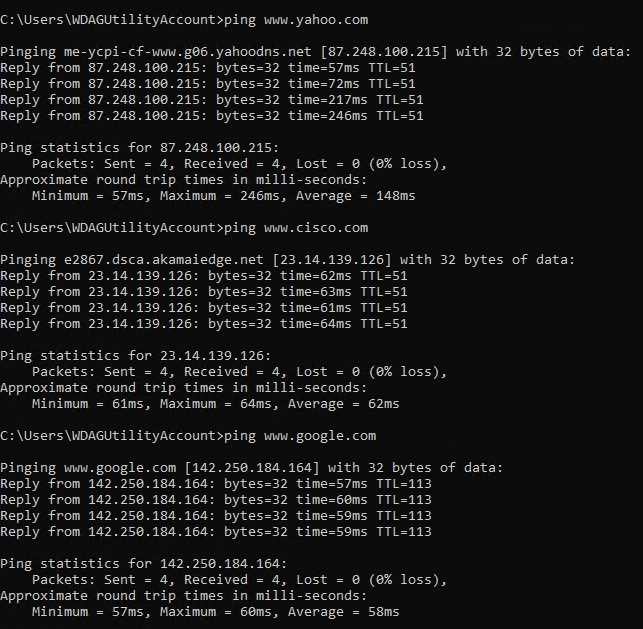
**Частина 3. Збір і аналіз даних протоколу ICMP по віддаленим вузламв програмі Wireshark**

1. Запускаємо перехоплення даних в інтерфейсі
   1. Запускаємо перехоплення даних для потрібного інтерфейсу.
   2. Активувавши перехоплення даних, відправляємо ехо-запит за допомогою команди ping на наступні три URL-адреси:

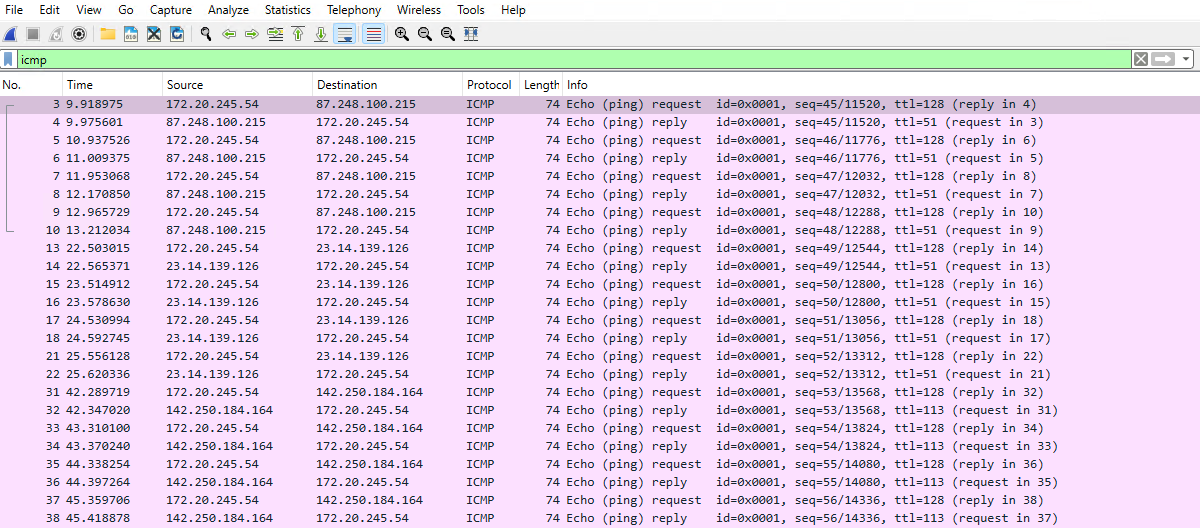
1)[www.yahoo.com](http://www.yahoo.com)

2)[www.cisco.com](http://www.cisco.com)

3)[www.google.com](http://www.google.com)



* 1. Зупиняємо перехоплення даних.



1. Вивчаємо і аналізуємо дані, отримані від віддалених вузлів.
   1. IP та MAC-адреси трьох запитаних веб-сайтів:
      * IP: 87.248.100.215   
        MAC: 00:15:5d:38:01:00
      * IP: 23.14.139.126  
        MAC: 00:15:5d:38:01:00
      * IP: 142.250.184.164  
        MAC: 00:15:5d:38:01:00
   2. Особливістю цих даних є те, що МАС-адреси запитаних веб-сайтів вийшли однаковими. Все через те, що використовується маршрутизатор, який виступає як точка виходу для всього трафіку.
   3. Отримана в цій частині інформація відрізняється від даних, отриманих в результаті ехо-запитів локальнихвузлів в частині 2, бо ехо-запити в локальній мережі дозволяють отримати реальні MAC-адреси конкретних пристроїв у вашій мережі, тоді як MAC-адреси, зазначені у попередньому запитанні, вказують на MAC-адреси проміжних мережевих пристроїв, які перебувають на шляху до веб-сайтів в Інтернеті.