**Міністерство освіти та науки України**

**Київський національний торговельно - економічний університет**

**Факультет інформаційних технологій**

**Кафедра інженерії програмного забезпечення та кібербезпеки**

**ПРАКТИЧНА РОБОТА № 8\_01**

**З ДИСЦИПЛІНИ**

**«Безпека інформаційних систем»**

**НА ТЕМУ:**

ВИВЧЕННЯ ЗАСОБІВ МОНІТОРИНГУ ТА АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ. СНІФФЕР WIRESHARK

**Виконала:** студентка ФІТ

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Лахно Валерiй Анатолiйович

Київ 2023

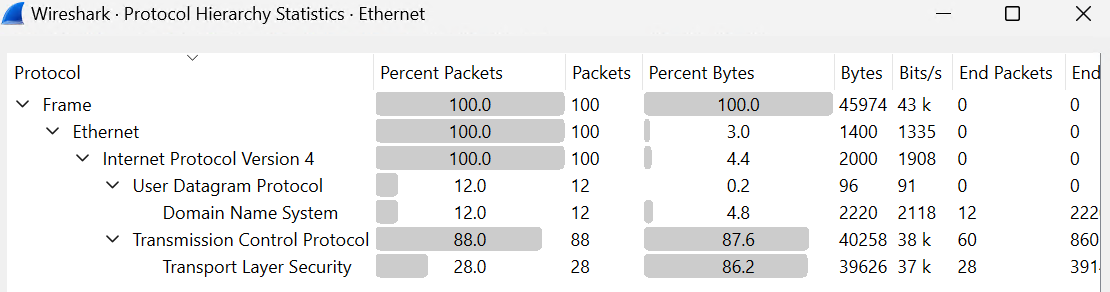
**Практична робота №8\_02**

**Тема**: Вивчення засобів моніторингу та аналізу мережевого трафіку. Сніффер Wireshark

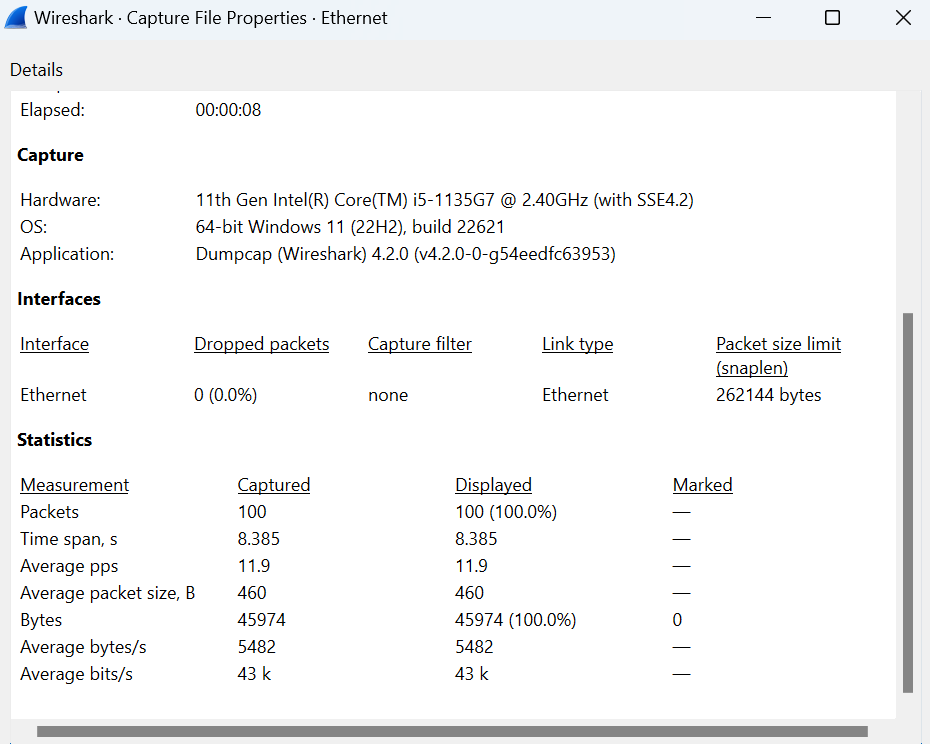
Мета: дізнатися принципи аналізу мережевого трафіку, навчитися використовувати мережевий аналізатор (сніффер Wireshark), навчитися аналізувати мережевий трафік на прикладі протоколів ARP, IP іICMP.

**Хід роботи:**

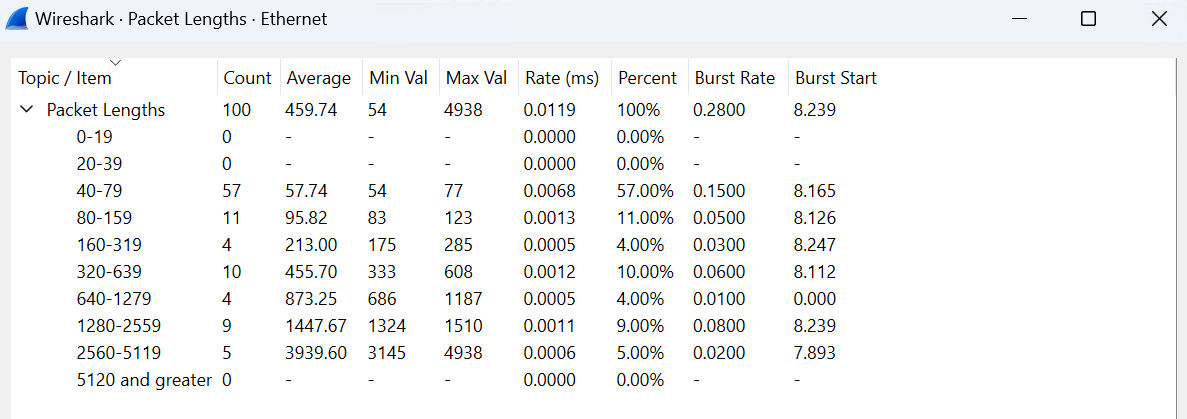
1. Вивчивши інтерфейс програми, приступаємо до захоплення пакетів.
2. Захопивши 100 пакетів, визначаємо статистичні дані:
   1. Відсоткове співвідношення трафіку різних протоколів в мережі:
      * DNS – 12%
      * TCP – 88%



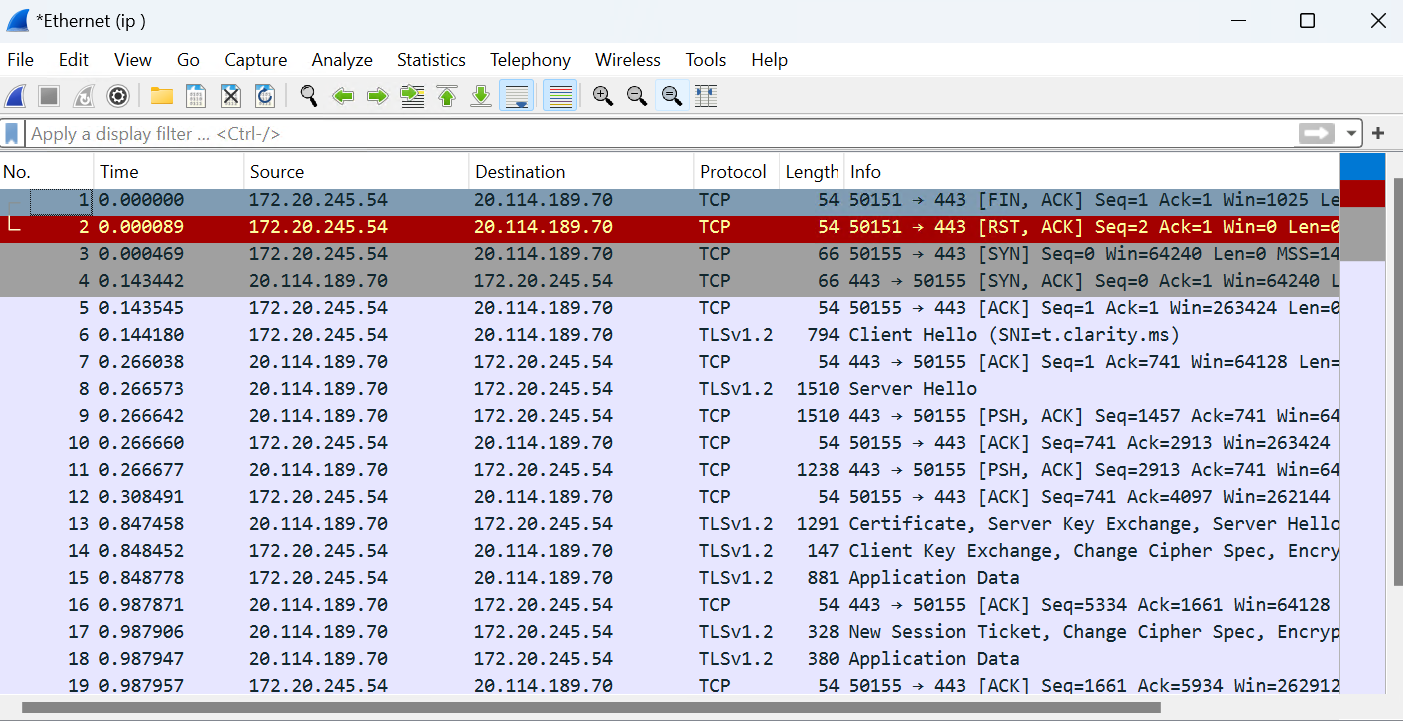
* 1. Середня швидкість кадрів/сек: 11,9
  2. Середня швидкість байт / сек: 5482



* 1. Мінімальний, максимальний та середній розміри пакету:
     + Min value: 54
     + Max value: 4938
     + Average: 458,74
  2. Ступінь використання смуги пропускання каналу (завантаження мережі): 8,239

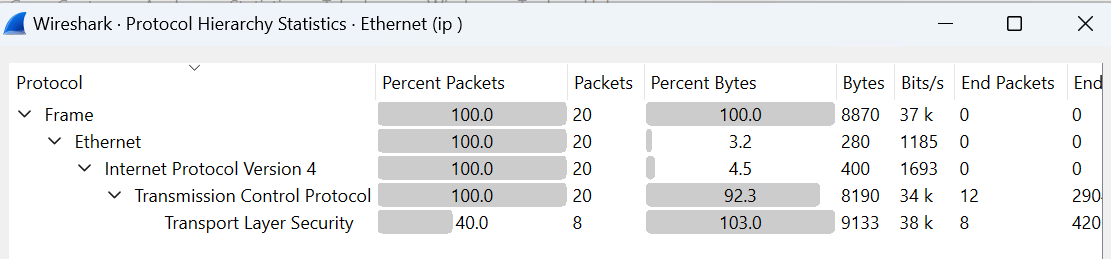


1. Зафіксуємо 20 ІР-пакетів.

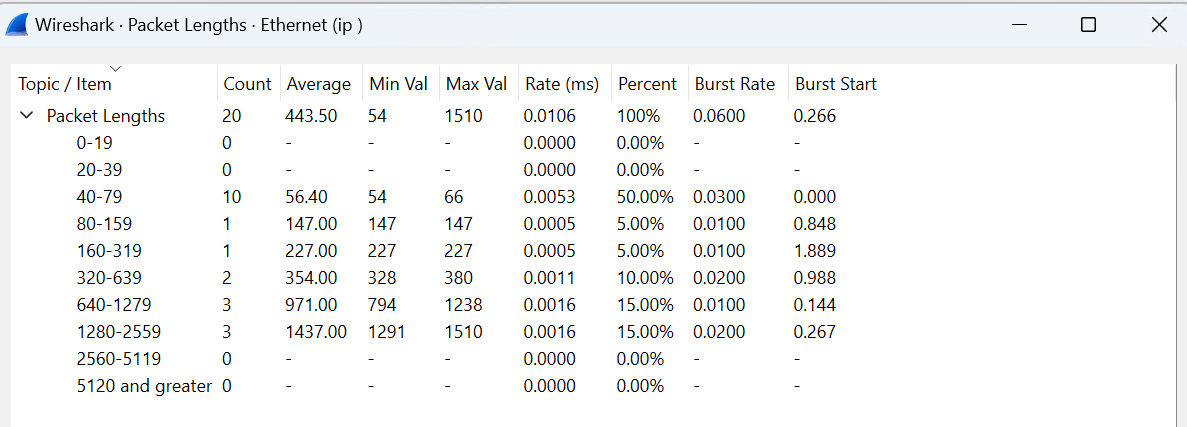


Визначимо статистичні дані:

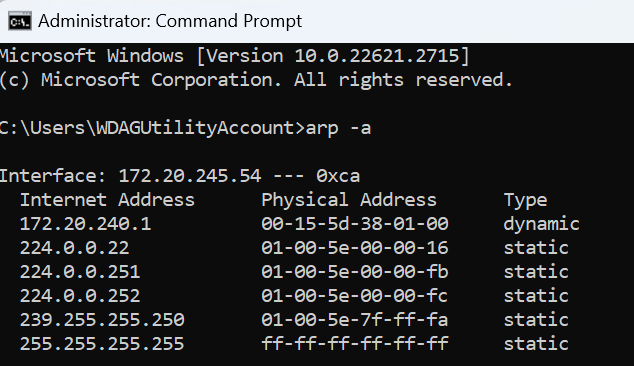
* 1. відсоткове співвідношення трафіку різних протоколів стека tcp / ip в мережі:



* 1. середній, мінімальний, максимальний розміри пакету:
     + Min value: 54
     + Max value: 1510
     + Average: 443.50

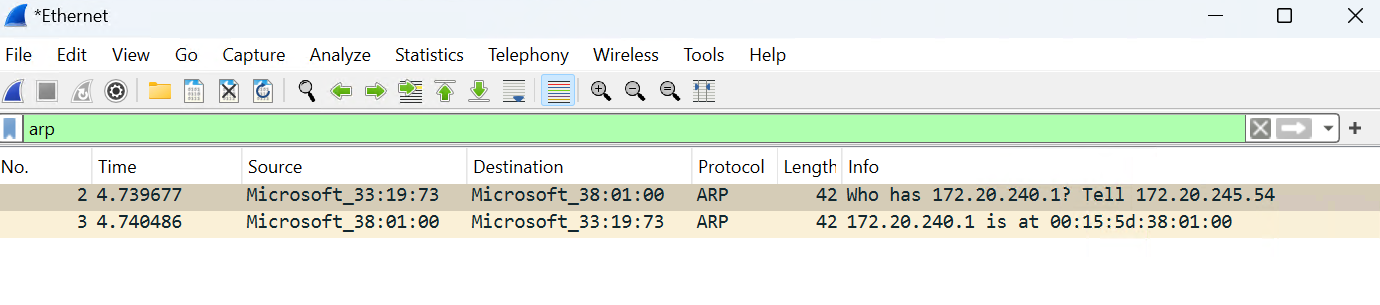


1. Виконаємо аналіз ARP-протоколу за прикладом з методичних вказівок:
   1. Для перегляду ARP-кеша можна використовувати однойменну утиліту arp з параметром «-a».



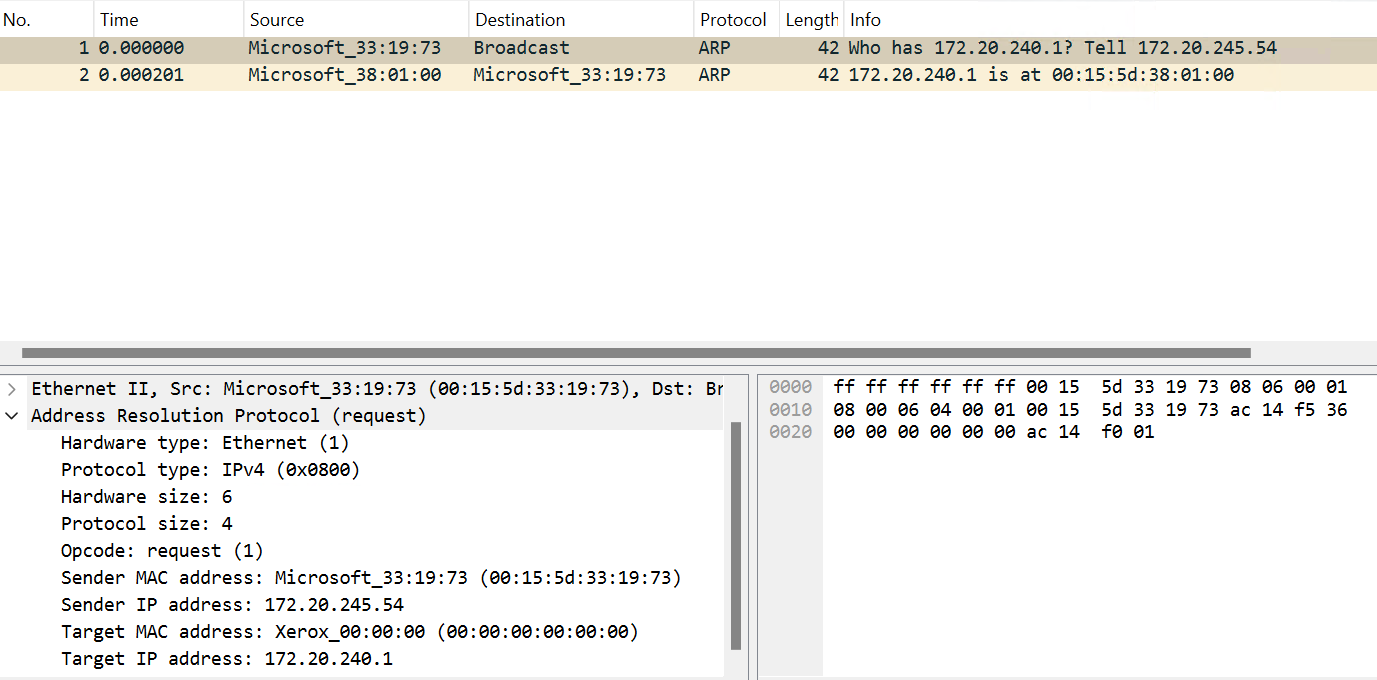
З даного результату команди arp видно, що в кеші на даний момент знаходиться 6 записів і видно відповідно ip-адреси машин і MAC-адреси їх мережевих адаптерів.

* 1. Очистимо arp-кеш командою arp -d. Далі запустимо захоплення трафіку і пропінгуємо задану машину командою ping 192.168.1.5.



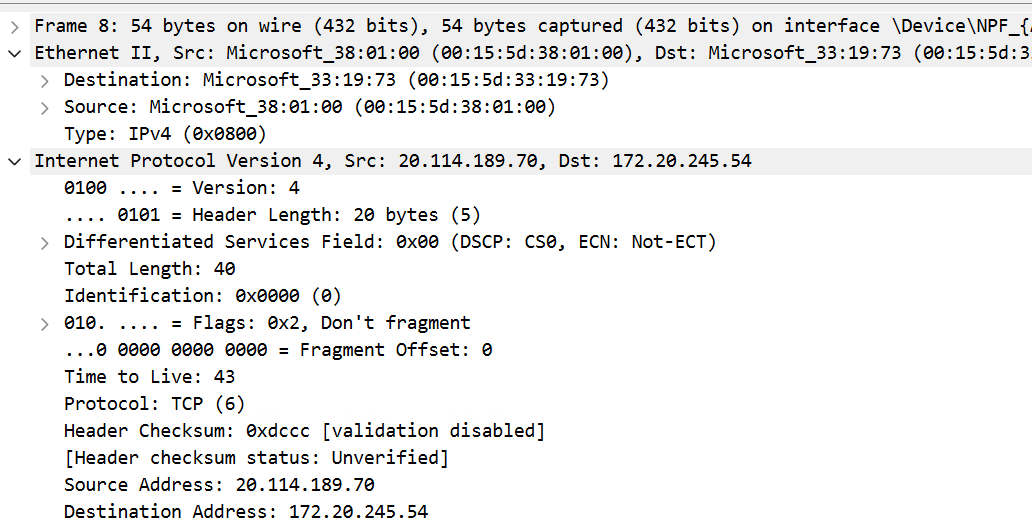
Ми бачимо 2 захоплених пакету: ARP-запит і ARP-відповідь.

* 1. Проаналізуємо отримані пакети. Спочатку розглянемо ARP-запит.



Ми можемо бачити, що в пакеті вказані MAC- і IP-адреси відправника («Sender MAC address» і «Sender IP address» відповідно). Це параметри машини, з якої виконується запит. В даному випадку запит направлений на отримання («Opcode: request» - запит) MAC-адреси машини, у якій IP-адреса («Protocol type: IP») 192.168.1.5 («Target IP address»). При цьому поле «Target MAC address» обнулене. Так як одержувач ARP-запиту на момент запиту не відомий, Ethernet-пакет відправляється всім машинам в даному локальному сегменті, про що сигналізує MAC адреса Ethernet-пакета «ff: ff: ff: ff: ff: ff».

1. На прикладі довільного IP-пакета вказуємо структури протоколів Ethernet і IP, відзначаємо поля заголовків і описуємо їх.
   1. Ethernet
      * Destination MAC Address: 00:15:5d:33:19:73 (Призначення МАС-адреси)
      * Sourse: 00:14:5d:38:01:00 (Джерело МАС-адреси)
      * Type: IPv4 (Тип Ethernet)
   2. IP
      * Version: 4
      * Header Length: 20 bytes (Довжина заголовка)
      * Total Length: 40 (Загальна довжина)
      * Identification: 0x0000 (0) (Ідентифікація)
      * Time to Live: 43 (Час життя)
      * Protocol: TCP (Протокол)
      * Source IP Address: 20.114.189.70
      * Destination IP Address: 172.20.245.54



1. Проаналізуємо принцип роботи утиліти ping.

Утиліта ping використовуєся для вимірювання часу відправлення та отримання повідомлень (пакетів) в мережі. Основна ідея полягає в тому, щоб визначити, чи можна успішно встановити з'єднання з вказаною мережевою адресою, а також визначити час, який необхідний для проходження цього з'єднання.

Ping базується на протоколі ICMP для відправлення і отримання пакетів. ICMP є частиною стеку протоколів TCP/IP і використовується для передачі повідомлень про помилки, відладки та управління мережею.

Поля протоколу ICMP:

* Type (Тип): Вказує на тип повідомлення (наприклад, Echo Request або Echo Reply).
* Code (Код): Доповнює тип і вказує на конкретний варіант повідомлення.
* Checksum (Контрольна сума): Використовується для перевірки цілісності пакету.
* Identifier та Sequence Number (Ідентифікатор і номер послідовності): Використовуються для відслідковування пар Echo Request/Echo Reply.

Давайте розглянемо основні етапи взаємодії при використанні утиліти Ping:

* Відправка Echo Request:
  + Ping Client: Генерує ICMP Echo Request пакет і відправляє його до вказаної мережевої адреси.
  + Ping Server (Destination): Отримує Echo Request пакет.
* Обробка Echo Request:
  + Ping Server: Приймає Echo Request, визначає, що це Echo Request, і готує Echo Reply.
* Відправка Echo Reply:
  + Ping Server: Відправляє відповідь (Echo Reply) до вказаної мережевої адреси.
  + Ping Client: Отримує Echo Reply.
* Вимірювання часу:
  + Ping Client: Вимірює час між відправленням Echo Request і отриманням Echo Reply.
* Виведення результатів:
  + Ping Client: Виводить результати, такі як час відповіді, втрати пакетів тощо.

**Контрольні питання:**

1. Основні цілі моніторингу мережевого трафіку:
   1. Виявлення проблем: Моніторинг дозволяє виявляти проблеми в мережі, такі як перевантаження, втрати пакетів, затримки тощо.
   2. Безпека: Виявлення аномального або небажаного трафіку, що може свідчити про атаки або інші загрози безпеці мережі.
   3. Видимість мережі: Отримання інформації про типові трафікові шаблони, джерела, призначення та обсяги, що допомагає управлінцям мережі в прийнятті рішень.
2. Відмінність моніторингу трафіку від фільтрації:

Моніторинг трафіку: Спостереження та аналіз всього мережевого трафіку для виявлення проблем і отримання загальної картини мережі.

Фільтрація трафіку: Вибіркове блокування або приймання певних типів трафіку на основі заданих умов.

1. Призначення класу програм-сніфферів:

Сніффери призначені для аналізу та перехоплення мережевого трафіку, дозволяючи вивчати передачу даних між пристроями в реальному часі.

1. Основні функції сніфферів:
   1. Захоплення пакетів: Перехоплення та запис мережевого трафіку.
   2. Аналіз пакетів: Декодування та вивчення вмісту пакетів для з'ясування інформації про комунікацію між пристроями.
   3. Статистика мережі: Надання інформації про використання мережі, пропускну здатність, затримки тощо.
2. Фільтри відображення і фільтри захоплення у сніффері Wireshark:
   1. Фільтри захоплення: Визначають, які пакети повинні бути захоплені при роботі з сніффером.
   2. Фільтри відображення: Визначають, які пакети відображаються на екрані після захоплення.
3. Основні функції статистичної обробки захоплених пакетів у сніффері Wireshark:
   1. Статистика мережевого трафіку: Виведення інформації про пропускну здатність, кількість пакетів, розподіл протоколів тощо.
   2. Статистика протоколів: Розгортання статистики для окремих мережевих протоколів.
4. Завдання протоколу ARP:

Визначення MAC-адреси по IP-адресі: ARP (Address Resolution Protocol) використовується для визначення фізичної (MAC) адреси мережевого пристрою, знаючи його IP-адресу.