Міністерство освіти і науки України

Національний університет “Львівська політехніка”

Інститут компютерних технологій, автоматики та метрології



**Комп`ютерні мережі**

**Лабораторна робота №6-b**

# Вивчення кадрів Ethernet за допомогою програми Wireshark

**Виконав:**

студ. групи ІР-21

Касараба В.В.

**Прийняла:**

Влах-Вигриновська Г. І.

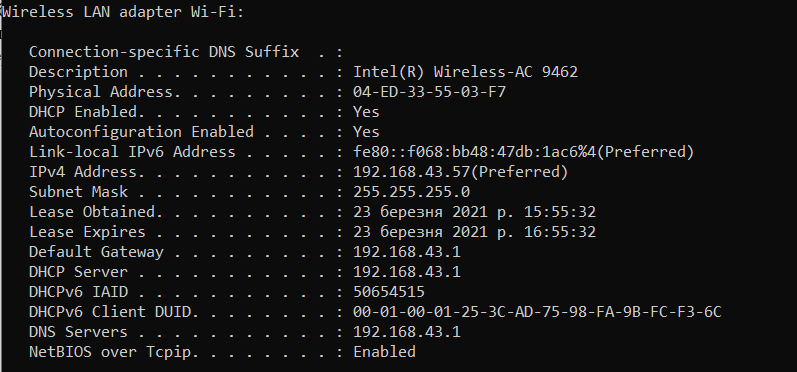
Львів — 2021

**Мета роботи:** Вивчення полів заголовків в кадрі Ethernet II. Захоплення і аналіз кадрів Ethernet за допомогою програми Wireshark.

**Частина 1**

1.Використавши навичкизлабораторної роботи №1 **«**Використання засобів командної оболонки для отримання відомостей про мережу» я виконав:

а) Використовуючи в командному рядку команду Ipconfig/all (відображення всіх поточних мережевих з’єднань) я визначив конфігурацію мережі у якій знаходиться ваш ПК.



б) Вказав власні:

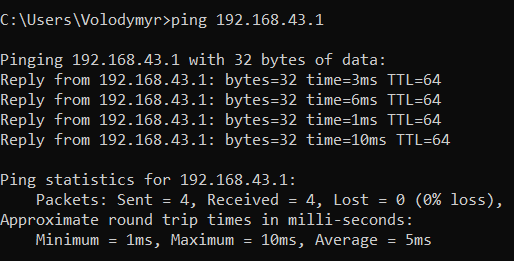
IP-адрес вузла ПК — 192.168.43.57

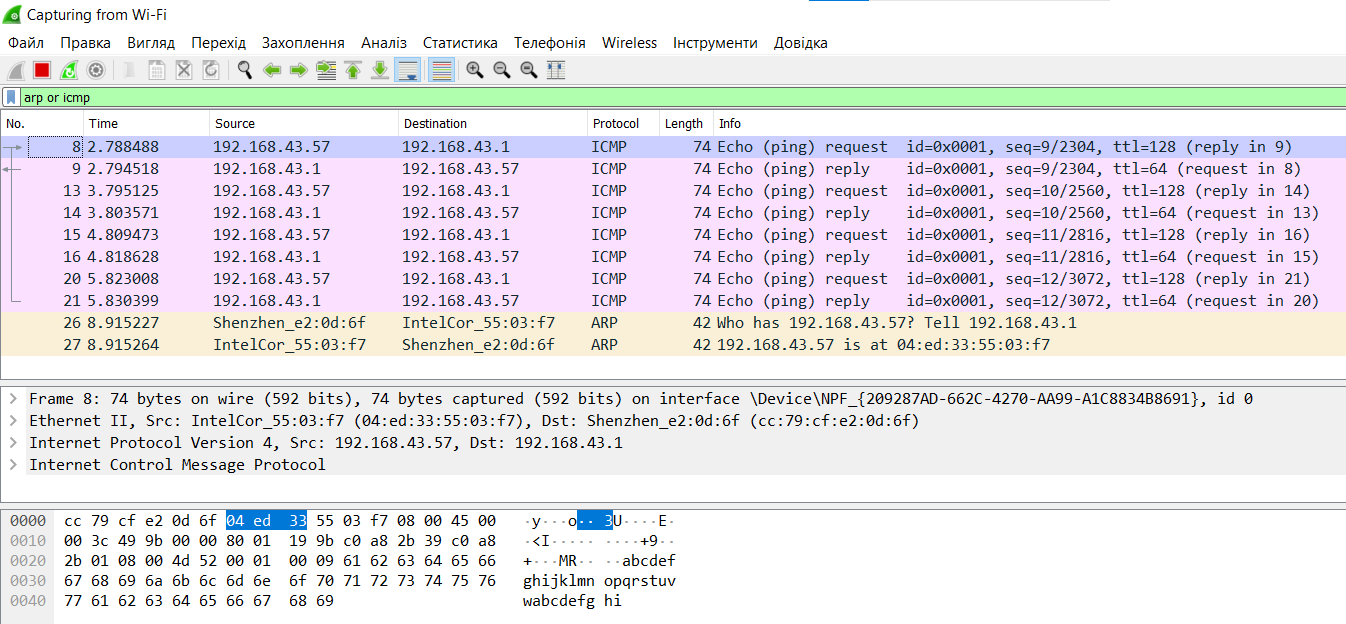
IP-адрес шлюзу по замовчуванню (основний шлюз) — 192.168.43.1

2: Вивчив кадри Ethernet в даних, захоплених програмою Wireshark.

а) запустив Wireshark та перейшов у режим захоплення пакетів.

б) використовуючи команду стрічку згенерував ехо-запит на визначений вище IP-адрес шлюзу по замовчуванню.



в) Нижченаведений результат захоплення даних в програмі Wireshark відображає пакети, які були згенеровані ехо-запитом вузлового ПК, відправленим на шлюз за замовчуванням. У програмі Wireshark включений фільтр для перегляду тільки ARP- і ICMP-протоколів. Сеанс починається з ARP запиту МАС-адреси маршрутизатора шлюзу, за яким слідують чотири ехо-запити за допомогою команди ping і відгуки. *(вставити власні результати дослідження).*

3. Вивчив зміст заголовків Ethernet II в ARP-запиті.

**Яка особливість змісту поля адреси призначення?**  
 У полі призначення ми вказуємо ІР-адресу отримувача. Для ARP протоколів, Broadcast запит означає широкомовний запит до всіх учасників локальної мережі, щоб довідатись потрібну МАС-адресу.

**Чому перед першим ехо-запитом за допомогою команди ping ПК відправляє широкомовну розсилку ARP?**

Щоб всі вузли в локальній мережі отримали пакети, і відповідний вузол із зазначенним ІР надіслав відповідь зі своєю МАС-адресою.

**Вкажіть MAC-адресу джерела в першому кадрі власного дослідження.**

cc:79:cf:e2:0d:6f

**Вкажіть ідентифікатор виробника (OUI) мережевого адаптера джерела.**

Перші 3 октети МАС-адреси: cc:79:cf

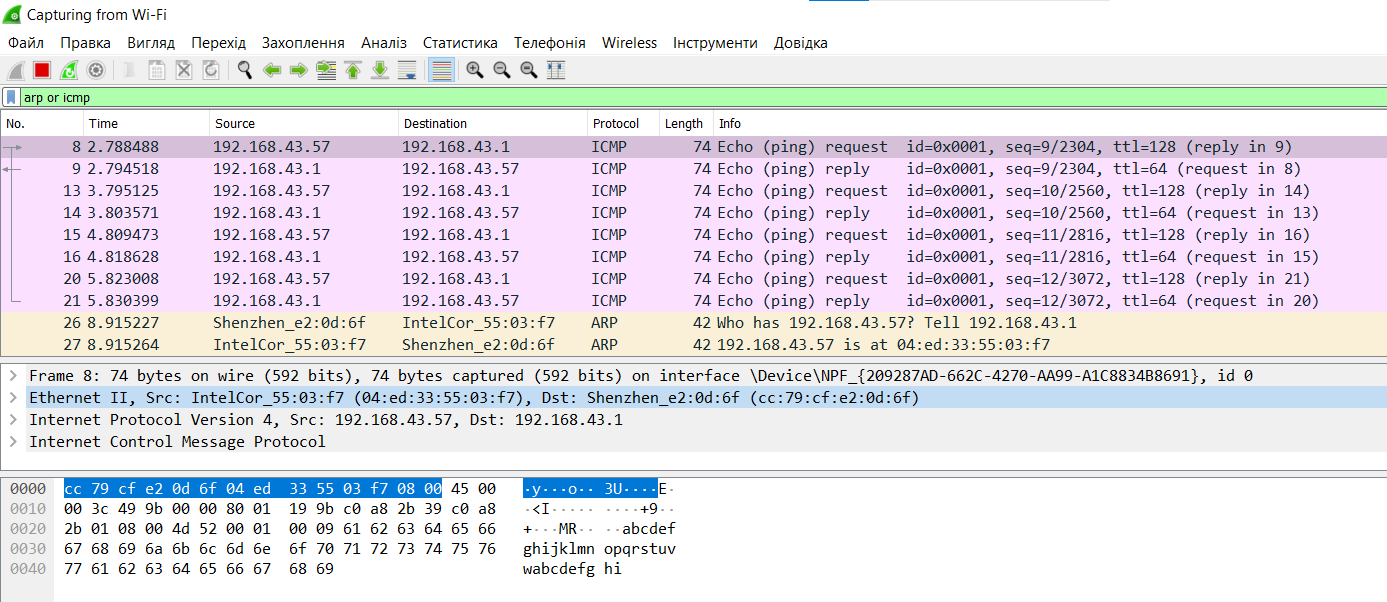
**Яка частина МАС-адреси відповідає OUI?**

Перші 3 октети

**Вкажіть серійний номер мережевого адаптера джерела.**

Останні 3 октети МАС-адреси: e2:0d:6f

4. Щоб виділити частину кадру (в шістнадцятковій системі і ASCII) в панелі відображення пакета у вигляді послідовності байтів (нижній розділ) натисніть на будь-який рядок в середньому розділі. Натисніть на рядок Ethernet II в середньому розділі і подивіться, що буде виділено в панелі відображення пакета у вигляді послідовності байтів.

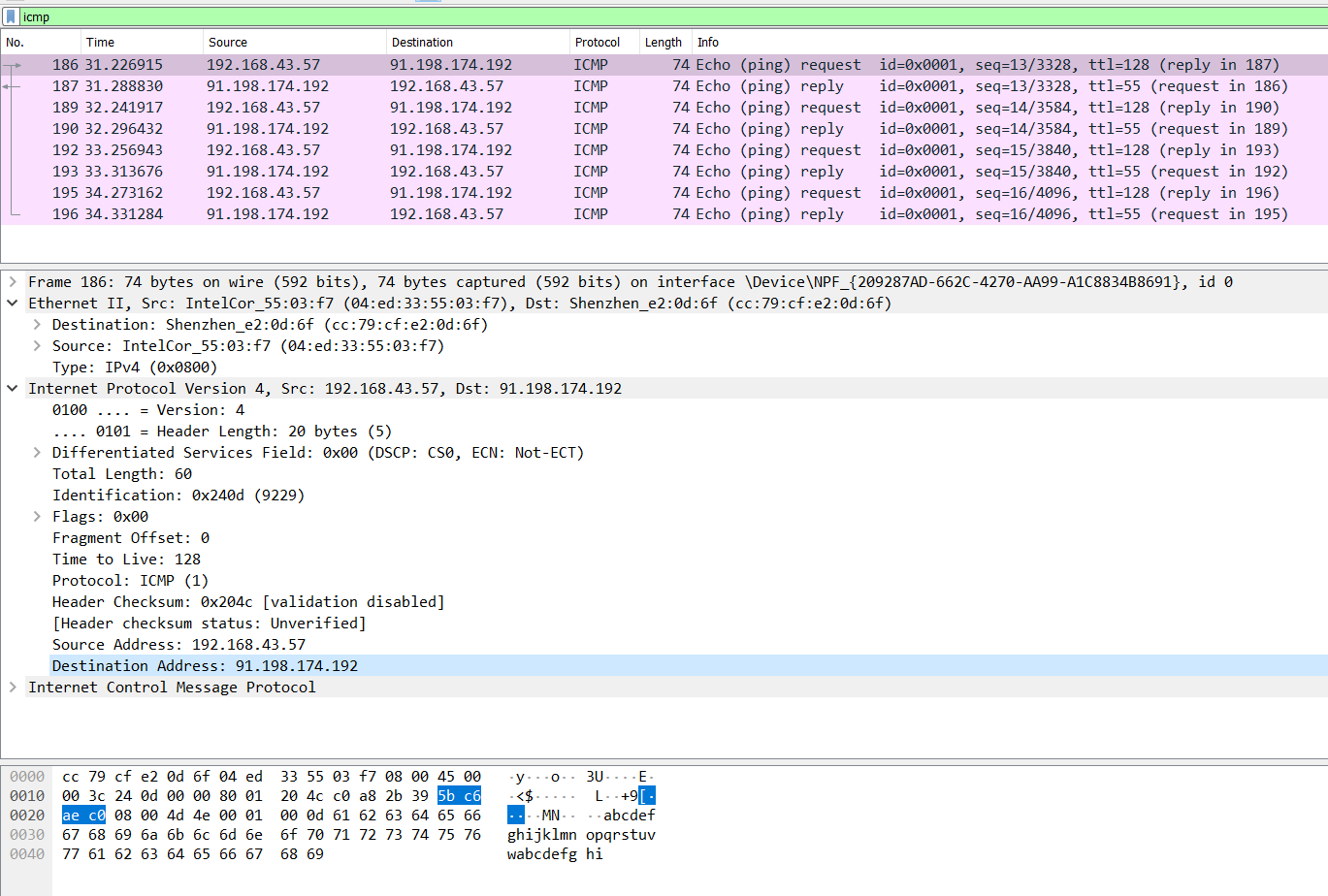


**Частина 2**

а) перезапустіть захоплення пакетів в програмі Wireshark. Через вікно командного рядка відправте ехо-запит за допомогою команди ping до одного віддаленого веб-сайту згідно варіанту в завданні 3.2 (ping www.wikipedia.org). Використавши фільтр програми Wireshark відобразіть на екрані тільки трафік ICMP.

Процедура виконання частини 2, згідно частини 1.

б) вивчіть кадри Ethernet в даних, захоплених програмою Wireshark.

 в) зупиніть захоплення пакетів та вивчіть нові дані на панелі списку пакетів в програмі Wireshark

Вкажіть МАС-адреси джерела і призначення в першому кадрі ехо-запиту за допомогою команди ping захоплених програмою Wireshark.

**Джерело**: 04:ed:33:55:03:f7

**Призначення**: cc:79:cf:e2:0d:6f

Назвіть IP-адреси джерела і призначення в поле даних кадру.

**Джерело**: 192.168.43.57

**Призначення**: 91.198.174.192

**Чому MAC-адреса призначення в частинах дослідження 1 і 2 однаковий?**

Тому, що встановлюється адреса власного МАС-шлюзу.

**Програма Wireshark не відображує поле преамбули заголовка кадру. Що містить преамбула?**

Преамбула (7 бітів) використовується для синхронізації відправляючих і одержуючих пристроїв. У цьому полі містяться синхронізовані біти, оброблені апаратним забезпеченням мережевого адаптера

**Висновок:**

На цій лабораторній роботі я вивчив поля заголовків в кадрі Ethernet II та випробував захоплення і аналіз кадрів Ethernet за допомогою програми Wireshark.

Для цього я спочатку я визначив конфігурацію мережі у якій знаходиться мій ПК з допомогою команди ipconfig /all. Встановивши програму Wireshark, я пропінгував основний шлюз (ping 192.168.43.1). У програмі я включив фільтр для перегляду тільки ARP- і ICMP-протоколів. Після цього я розглянув всі поля, та вивчив зміст заголовків Ethernet II в ARP-запиті.

Потім через вікно командного рядка відправте ехо-запит за допомогою команди ping до вебсайту [www.wikipedia.org](http://www.wikipedia.org). Зупинивши захоплення пакетів, я вивчив нові дані на панелі списку пакетів в програмі Wireshark