**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»**



**Аналізатор мережевих пакетів Wireshark. Захват та аналіз мережевих кадрів**

**МЕТОДИЧНІ ВКАЗІВКИ**

**до лабораторної роботи №6**

**з дисципліни “Комп’ютерні мережі ” для студентів спеціальності 122 Комп’ютерні науки спеціалізації Системна інженерія (Інтернет речей)**

*Затверджено*

*на засіданні кафедри*

"Комп'ютеризовані системи автоматики"

Львів 2020

**Мета роботи**: За допомогою аналізатора вивчити структуру та типи кадрів у комп’ютерній мережі.

**Теоретична частина**

При взаємодії протоколів верхнього рівня дані проходять рівні взаємодії відкритих систем (OSI) і інкапсулюються в кадри рівня 2. Структура кадру залежить від типу доступу до середовища передачі даних. Наприклад, якщо в якості протоколів верхнього рівня використовуються TCP і IP, а тип доступу до середовища передачі - Ethernet, то інкапсуляція кадрів рівня 2 відбувається через формат кадру Ethernet II. Це типово для локального середовища. Загалом формат кадру Ethernet II є відносно простим і ефективним способом передачі даних через мережі Ethernet.

При вивченні концепцій рівня 2 корисно аналізувати дані заголовків кадрів. У першій частині цієї лабораторної роботи ви зможете ознайомитись з полями в кадрі Ethernet II. У другій частині вам потрібно захопити і проаналізувати поля заголовків кадру Ethernet II для локального і віддаленого трафіку за допомогою програми Wireshark.

**Wireshark**

Wireshark — популярний аналізатор мережевих протоколів із відкритим вихідним кодом, який дозволяє користувачам фіксувати та аналізувати мережевий трафік у реальному часі. Він широко використовується мережевими адміністраторами, спеціалістами з безпеки та розробниками програмного забезпечення для вирішення проблем мережі, виявлення загроз безпеці та налагодження мережевих протоколів.

Wireshark підтримує широкий спектр мережевих протоколів, включаючи TCP, UDP, HTTP, DNS та багато інших. Це дозволяє користувачам отримувати пакети та аналізувати деталі кожного пакета, включаючи використовуваний протокол, IP-адреси джерела та призначення та іншу інформацію.

Окрім захоплення та аналізу пакетів, Wireshark також містить розширені функції, такі як здатність фільтрувати та шукати певні пакети на основі різних критеріїв, здатність реконструювати та аналізувати мережеві потоки та можливість експортувати захоплені пакети в різні формати файлів для подальший аналіз.

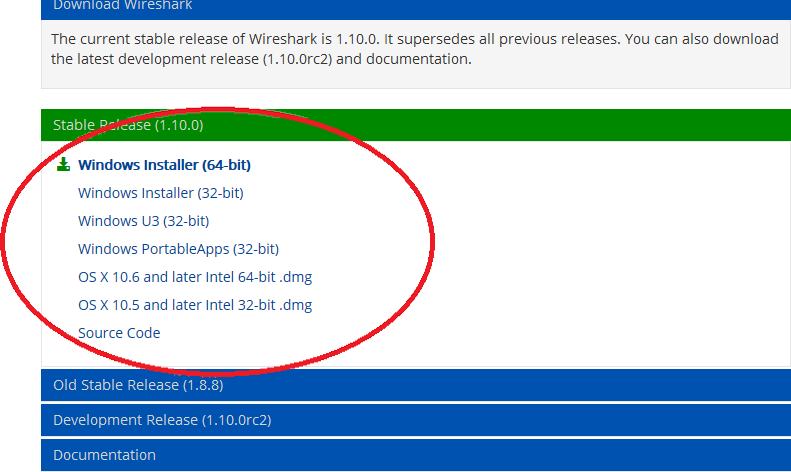
Wireshark можна використовувати в різних операційних системах, таких як Windows, Linux і macOS. Він має зручний графічний інтерфейс, що полегшує користувачам навігацію та використання різноманітних функцій. Він також дуже розширюваний, з багатьма плагінами та доповненнями, доступними для покращення його функціональності.

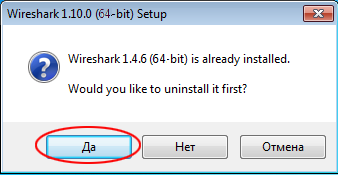
Загалом Wireshark є потужним інструментом для аналізу мережі та усунення несправностей, і він широко використовується в різних галузях, щоб допомогти забезпечити безперебійну та безпечну роботу мереж.

Завантажите програму Wireshark за адресою [**www.wireshark.org.**](http://www.wireshark.org/)

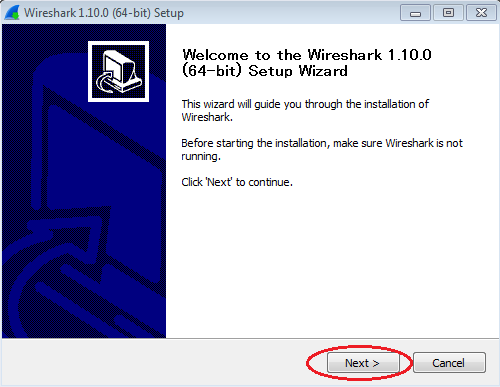


Виберіть версію програми відповідно до архітектури і операційної системи вашого ПК. Наприклад, якщо ваш ПК працює під управлінням 64-розрядною ОС Windows, виберіть Windows Installer (64 - bit).

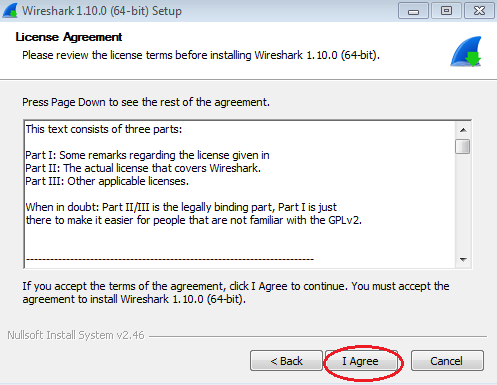


Відразу після цього почнеться завантаження. Місцезнаходження завантаженого файлу залежить від браузеру і операційної системи, якими ви користуєтеся. Завантажений файл називається **Wireshark - win64 - x.x.x.exe**, де "x" відповідає номеру версії. Двічі натисніть на файл, щоб почати установку. Дайте відповідь на усі повідомлення безпеки, які з'являться на екрані. Якщо на вашому ПК вже є копія Wireshark, перед установкою програми з'явиться запит на видалення старої версії. Рекомендується видалити стару версію програми перед установкою нової. Щоб видалити попередню версію програми Wireshark, натисніть кнопку **Так**.

Якщо програма Wireshark встановлюється уперше або попередня версія була видалена, відкриється майстер установки програми Wireshark. Натисніть кнопку **Next** (Далі).

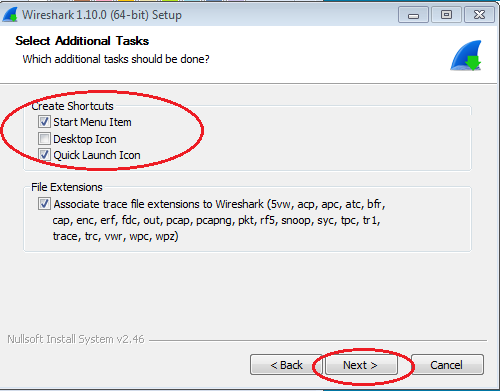
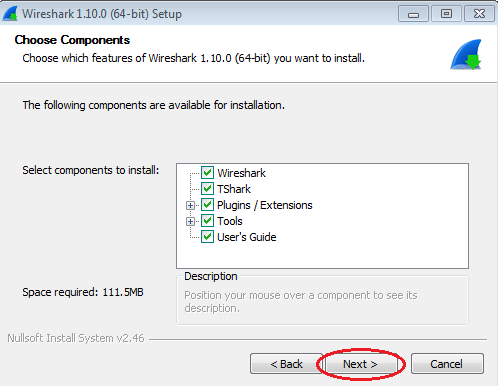


Виконайте інструкції по установці. Коли відкриється вікно "**License Agreement**" (Ліцензійна угода), натисніть кнопку **I accept** (Прийняти).

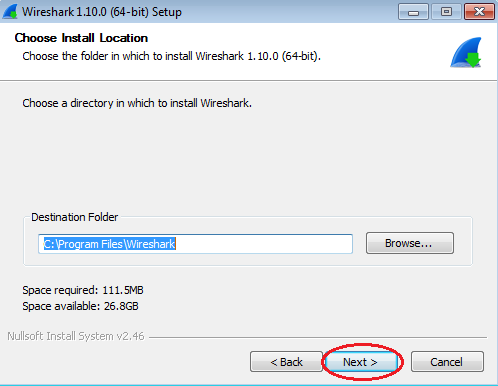


При виборі компонентів залиште налаштування за замовчуванням і натисніть кнопку

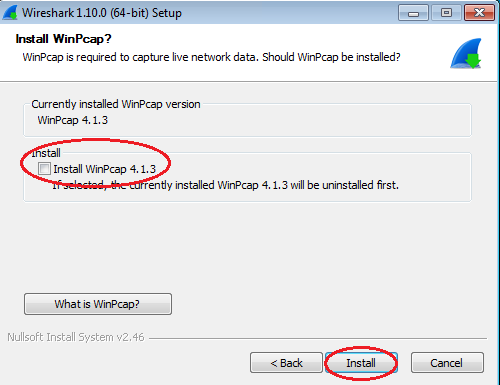
**Next** (Далі). Виберіть бажані ярлики і натисніть кнопку **Next** (Далі).



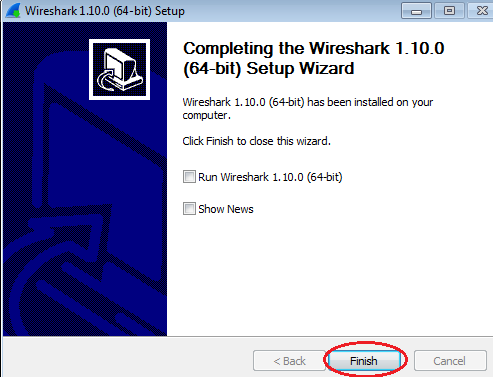
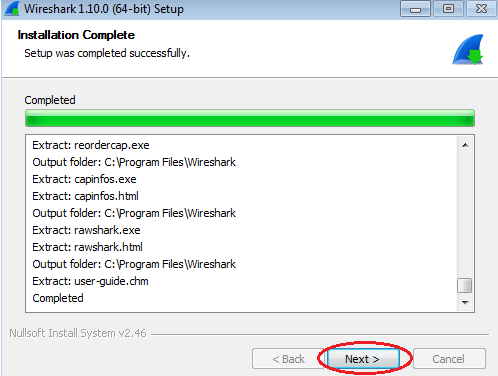
Якщо дисковий простір обмежений, директорію установки можна змінити, інакше, залиште адресу, вказану за замовчуванням.



Для збору мережевих даних на ваш ПК необхідно встановити програму **WinPcap**. Якщо встановлена версія WinPcap старша за версію, що додається до програми Wireshark, необхідно встановити новішу версію, натиснувши на прапорець поряд з варіантом **Install WinPcap x.x.x** (Встановити WinPcap x.x.x). Якщо установка пройшла успішно, закрийте майстер установки WinPcap.



Після цього почнеться установка програми Wireshark. Статус установки відображатиметься в окремому вікні. Після закінчення установки натисніть кнопку **Next**. Для завершення процесу установки програми Wireshark натисніть **Finish** (Готово).



Загалом, головне вікно Wireshark забезпечує всебічне уявлення про захоплені пакети, дозволяючи користувачам аналізувати та вирішувати проблеми з мережею в режимі реального часу. Різноманітні панелі та інструменти, які надає Wireshark, роблять його потужним і гнучким інструментом для аналізу мережі.

# Топологія



Необхідні ресурси:

• Один ПК з виходом в Інтернет і встановленою програмою Wireshark.

**Частина 1**: Вивчення полів заголовків в кадрі Ethernet II. Для цього буде використовуватися захоплення даних програмою Wireshark.

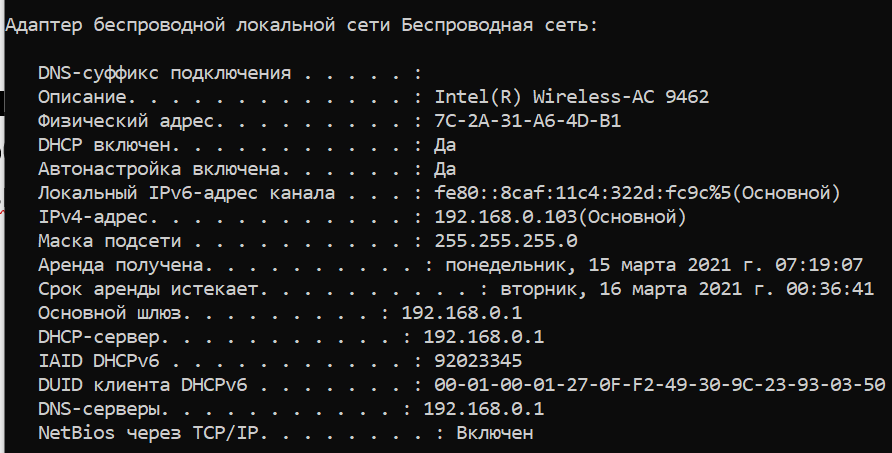
Перегляньте довжини і опису полів заголовків Ethernet II.

**Формат кадру Ethernet II**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Поле | Преамбула | MAC-адреса одержувача  (Destination Address) | MAC-адреса відправника  (Source Address) | Тип  кадра  (Туре) | Дані +заповнювач | Поле контрольної послідовності кадру  (FCS) |
| Кількість байт | 8 байтів | 6 байтів | 6 байтів | 2 байти | 46 – 1500 байтів | 4 байти |

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

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



б) Вкажіть власні:

IP-адрес вузла ПК — \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

IP-адрес шлюзу по замовчуванню (основний шлюз) — \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

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

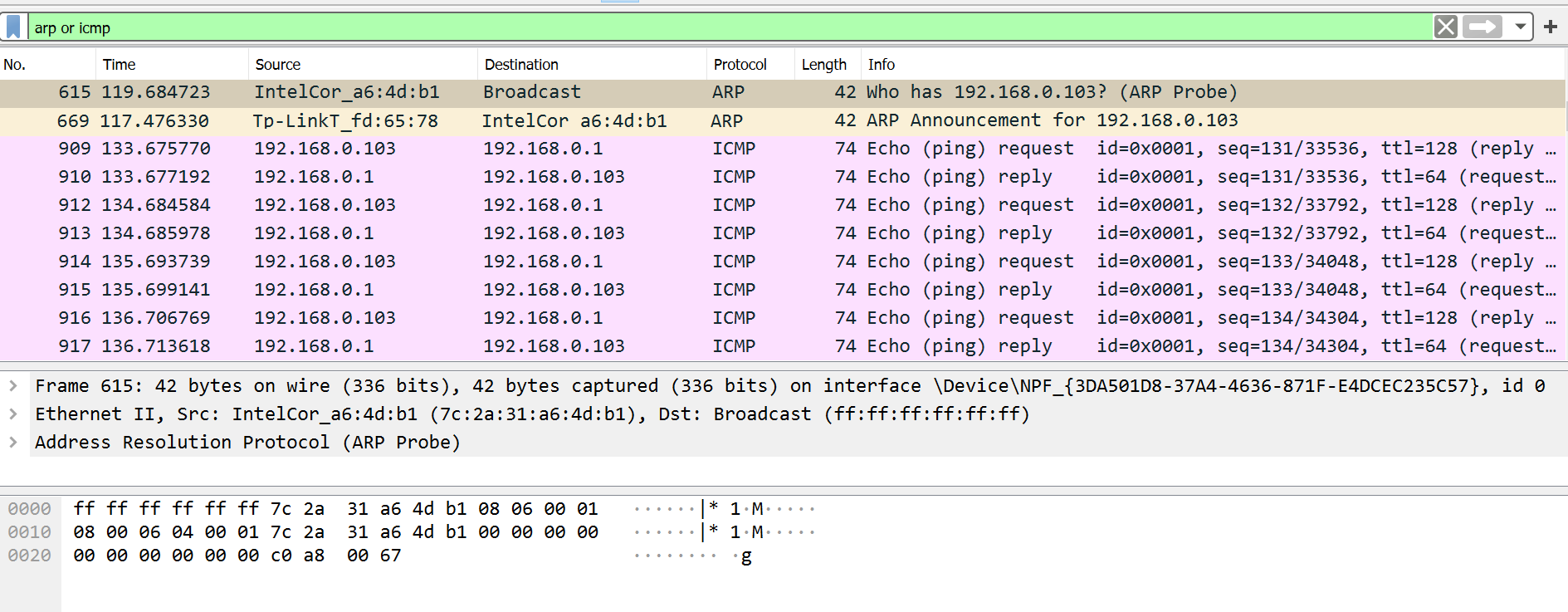
а) запустіть Wireshark та перейти у режим захоплення пакетів.

б) використовуючи команду стрічку згенеруйте ехо-запит на визначений вами 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 створені за допомогою команди ping і відгуки. *(вставити власні результати дослідження).*

*Примітка\*. Якщо при роботі* в програмі Wireshark *відсутні ARP пакети, то потрібно ввести в командному рядку команду ipconfig/release і оренда IP-адреси видана сервером DHCP буде завершена. Далі отримати нову IP-адресу від сервера DHCP виконавши команду ipconfig/renew і заново повторити пункт 2.*



Головне вікно програми Wireshark складається з наступних панелей, які відображають різні типи інформації про захоплені пакети: панель списку пакетів (вгорі-рожевий колір), панель відомостей про пакет (посередині) і панель відображення пакета у вигляді послідовності байтів (внизу).

* Область списку пакетів: на цій панелі відображається список усіх захоплених пакетів у хронологічному порядку, причому кожен пакет представлено одним рядком. Панель списку пакетів надає таку інформацію, як час захоплення, IP-адреси джерела та призначення, тип протоколу та розмір пакета.
* Панель відомостей про пакет: на цій панелі відображається детальна інформація про поточний вибраний пакет на панелі списку пакетів. Він надає ієрархічне подання пакета, показуючи різні рівні стеку протоколів та їхні відповідні поля та значення.
* Панель байтів пакетів: на цій панелі відображаються необроблені байти поточного вибраного пакета в шістнадцятковому форматі та форматі ASCII. Він забезпечує детальний перегляд вмісту пакета, включаючи будь-які корисні дані або заголовки.
* Панель інструментів фільтра: Ця панель інструментів дозволяє користувачам створювати та застосовувати фільтри до захоплених пакетів на основі конкретних критеріїв, таких як тип протоколу, IP-адреси джерела та призначення або номери портів. Це можна використовувати для виділення конкретних пакетів для подальшого аналізу.
* Рядок стану: цей рядок надає інформацію про поточний стан захоплення, включаючи кількість захоплених пакетів і тривалість захоплення. Він також відображає інформацію про будь-які помилки або попередження, які могли виникнути під час захоплення.

Завдання

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

У наведеній нижче таблиці обраний перший кадр з даних, захоплених програмою Wireshark, і відображені дані в полях заголовка Ethernet II.

ARP (Address Resolution Protocol) — це мережевий протокол, який використовується для зіставлення фізичної адреси (MAC-адреси) з IP-адресою в локальній мережі. Він в основному використовується в мережах Ethernet, де кожен пристрій у мережі має унікальну MAC-адресу, призначену йому, і спілкується за допомогою IP-адрес.

|  |  |  |
| --- | --- | --- |
| **Поле** | **Значення** | **Опис** |
| Преамбула | Чи не показано в захопленні даних | У цьому полі містяться синхронізовані біти, оброблені апаратним забезпеченням мережевого адаптера. |
| Адрес призначення | Широкомовна  розсилка  (ff:ff:ff:ff:ff:ff) | Адреси рівня 2 для кадру. Довжина кожної адреси становить 48 біт або 6 октетів, виражених 12 шістнадцятковими цифрами, 0-9,A-F. Загальний формат — 12:34:56:78:9А:BC.  Перші шість шістнадцяткових номерів позначають виробника мережевого адаптера, а останні - серійний номер пристрою.  Адреса призначення може бути широкомовною (що складається тільки з одиниць), або індивідуальна.  Адреса джерела завжди індивідуальна. |
| Адрес джерела | IntelCor\_a6:4d:b1 (7c:2a:31:a6:4d:b1) |
| Тип кадра | 0x0806 | У кадрах Ethernet II це поле містить шістнадцяткове значення, яке використовується для вказівки типу протоколу верхнього рівня в поле даних. Ethernet II підтримує безліч протоколів верхнього рівня. Найбільш поширені такі два типи кадрів:  Значення Опис  0x0800 Протокол IPv4  0x0806 Протокол дозволу адрес (ARP) |
| Дані | ARP | Містить інкапсульований протокол верхнього рівня. Поле даних в діапазоні від 46 до 1500 байт. |
| Контрольна послідовність кадру (Frame Check  Sequence-FCS) | Не показано в захопленні даних | Контрольна послідовність кадру, яка використовується мережним адаптером для виявлення помилок при передачі даних. Значення обчислюється комп'ютером відправника, включає адреси, тип і поле даних кадру та перевіряється одержувачем. |

Яка особливість змісту поля адреси призначення?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

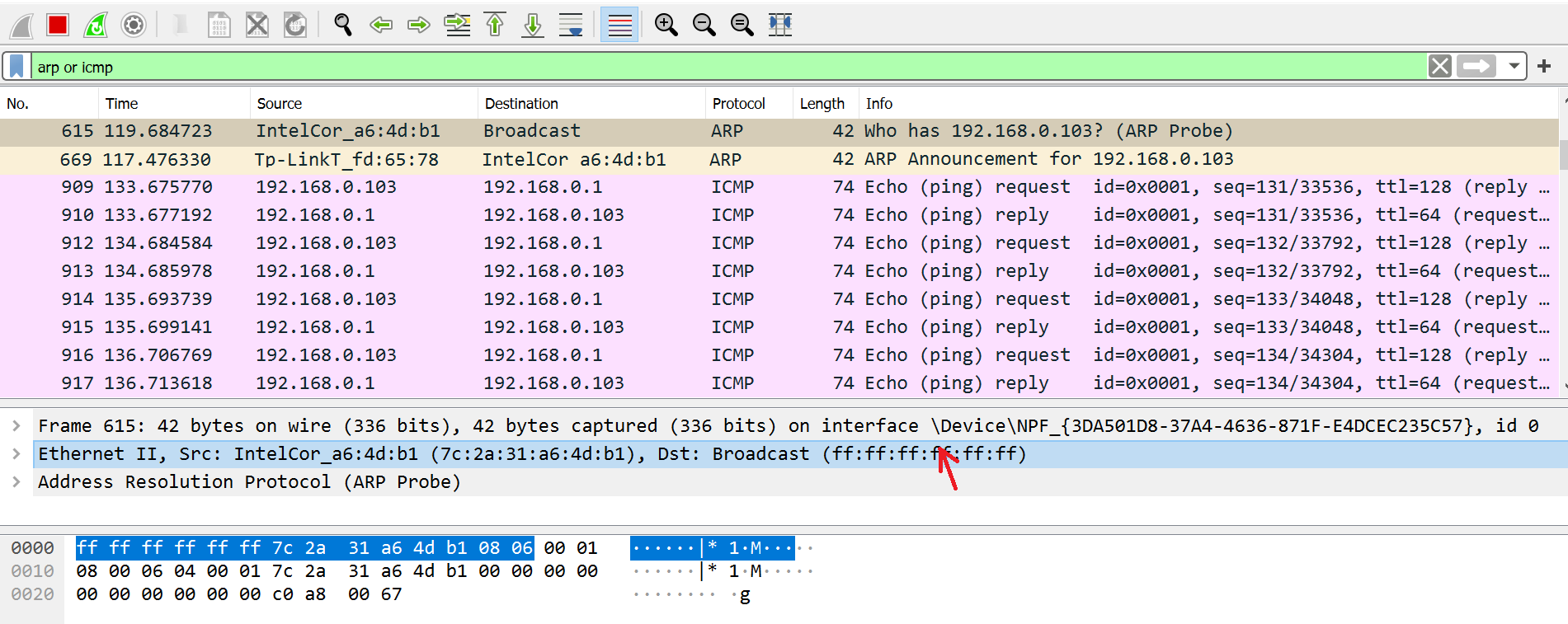
Вкажіть MAC-адресу джерела в першому кадрі власного дослідження.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Вкажіть ідентифікатор виробника (OUI) мережевого адаптера джерела. \_\_\_\_\_\_\_\_\_\_\_\_

Яка частина МАС-адреси відповідає OUI?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Вкажіть серійний номер мережевого адаптера джерела.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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.** Захоплення і аналіз **віддалених** кадрів Ethernet за допомогою програми Wireshark.

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 (лаб. робота1). 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Призначення: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Джерело: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Призначення: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Чому MAC-адрес призначення в частинах дослідження 1 і 2 однаковий?\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Наведіть висновки до роботи.