ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №4

Виконав :

Ст *Гуменюк С. А.*

ПМІ -33

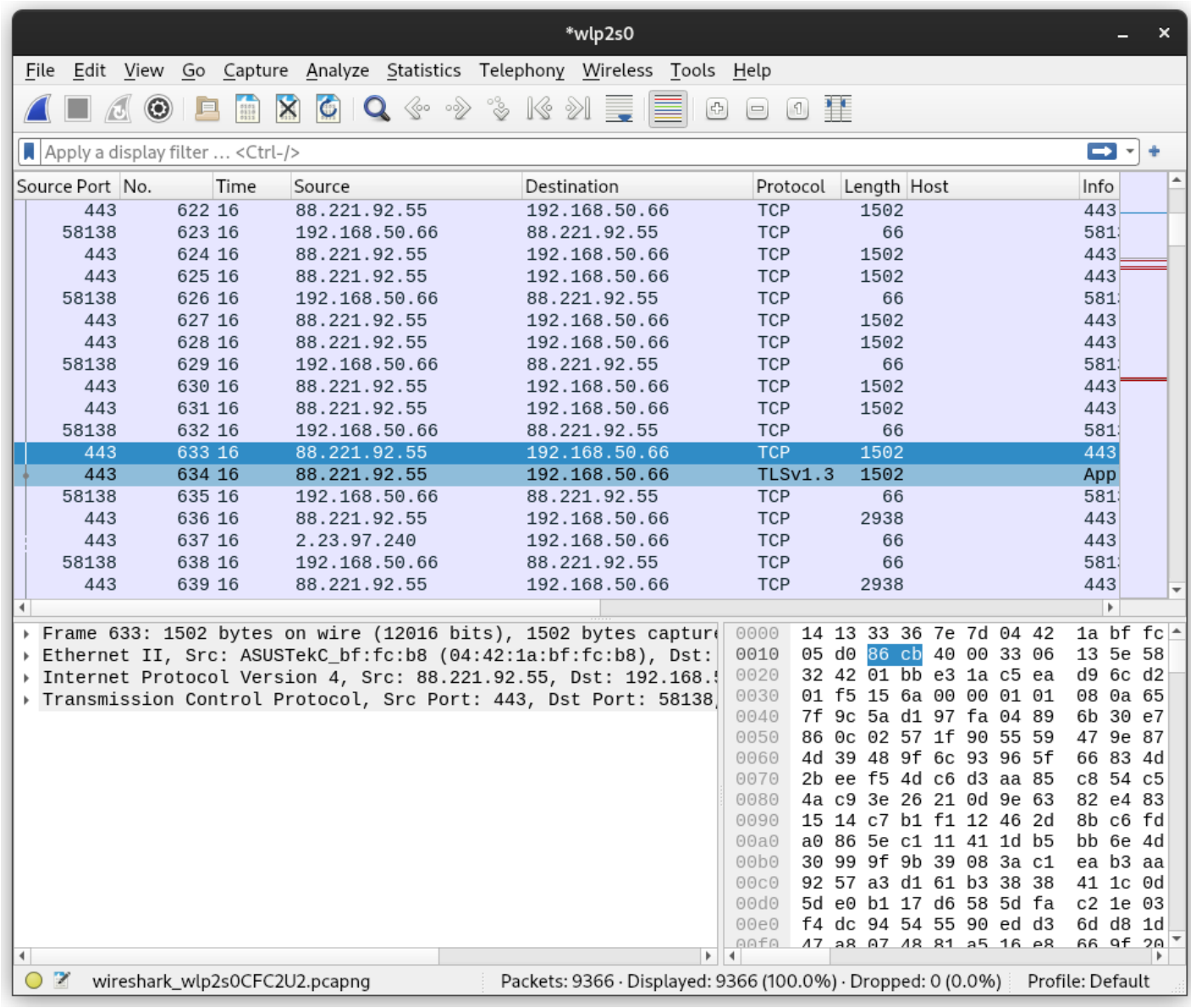
2024

Тема: Аналіз повідомлень канального рівня Ethernet засобами WireShark. Утиліти для діагностики мережі на канальному рівні

Мета роботи: Здобути практичні навички з інтерпретації Ethernet-кадрів та використання консольних утиліт для діагностики мережі на рівні мережевих інтерфейсів.

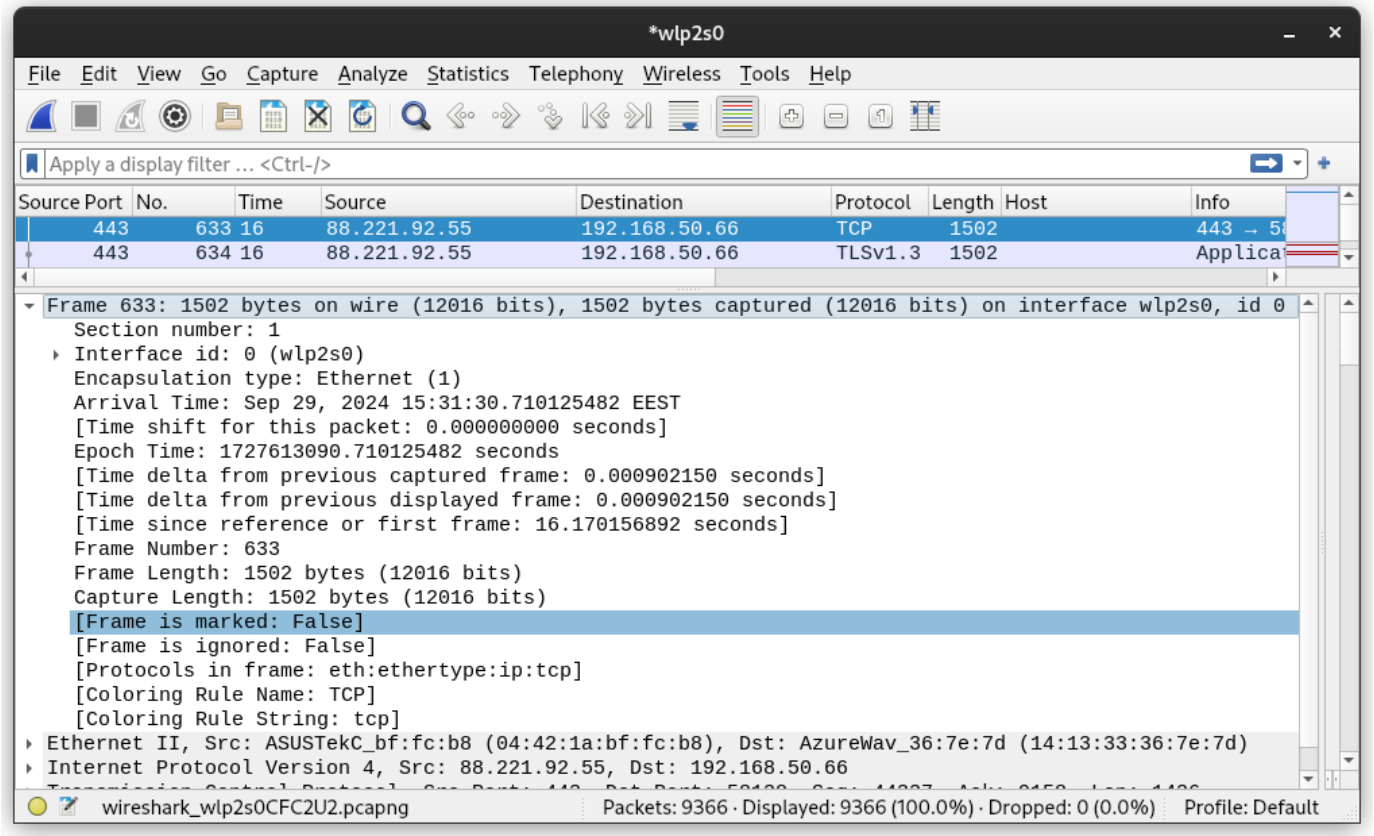
Хід роботи

1. Захопив кадр:



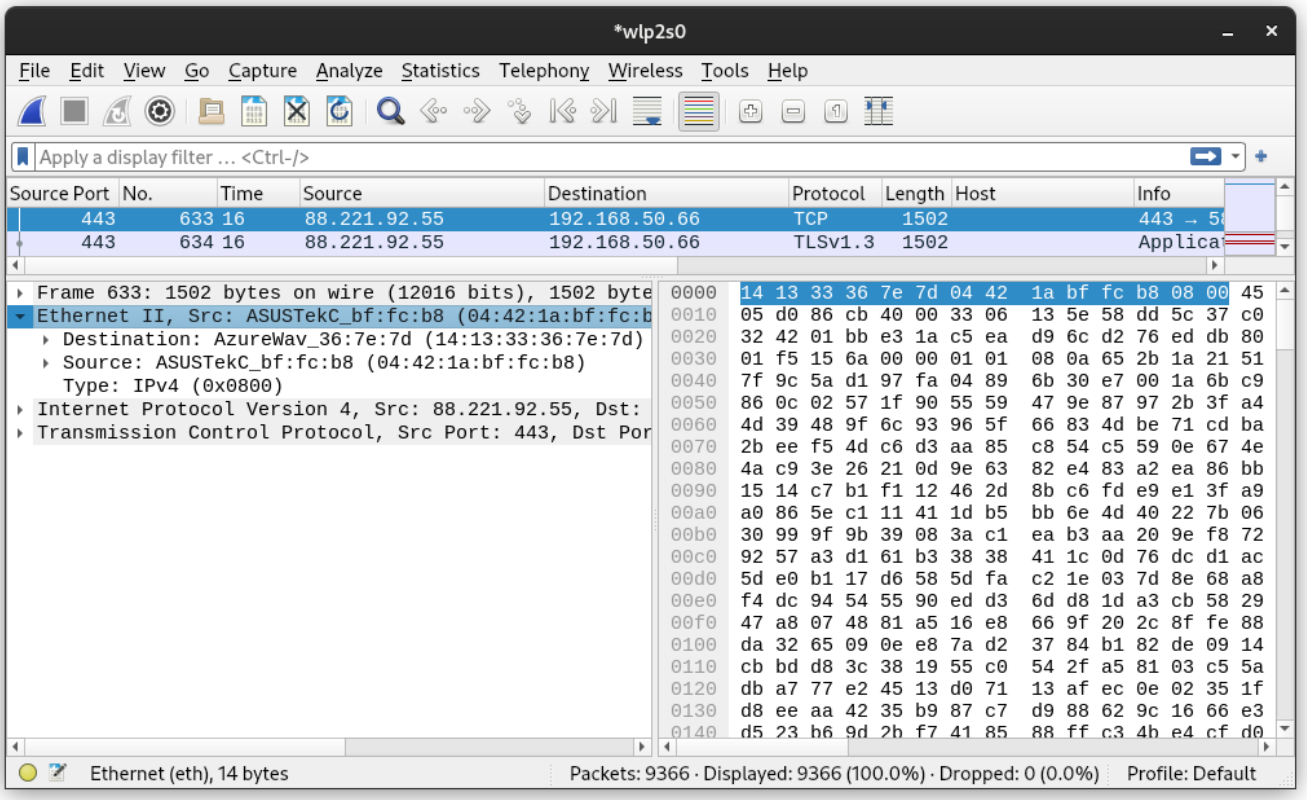
Кадр №633, розмір — 1502 байтів (12016 бітів).

2. Інформація про кадр:

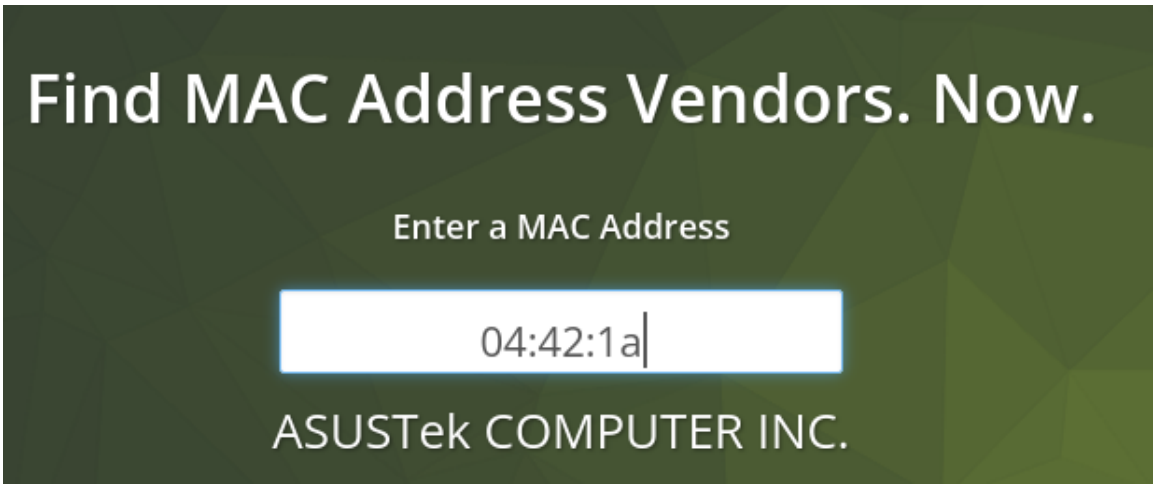


Arrival Time: Sep 29, 2024 15:31:30.710125482 EEST
[Protocols in frame: eth:ethertype:ip:tcp]

3. Дані про заголовок



Дані заголовка:
Розмір -14 байтів
Source: ASUSTek (04:42:1a:bf:fc:b8)
Destination: AzureWav_36:7e:7d (14:13:33:36:7e:7d)
Type: IPv4 (0x0800)



4. ARP-запит

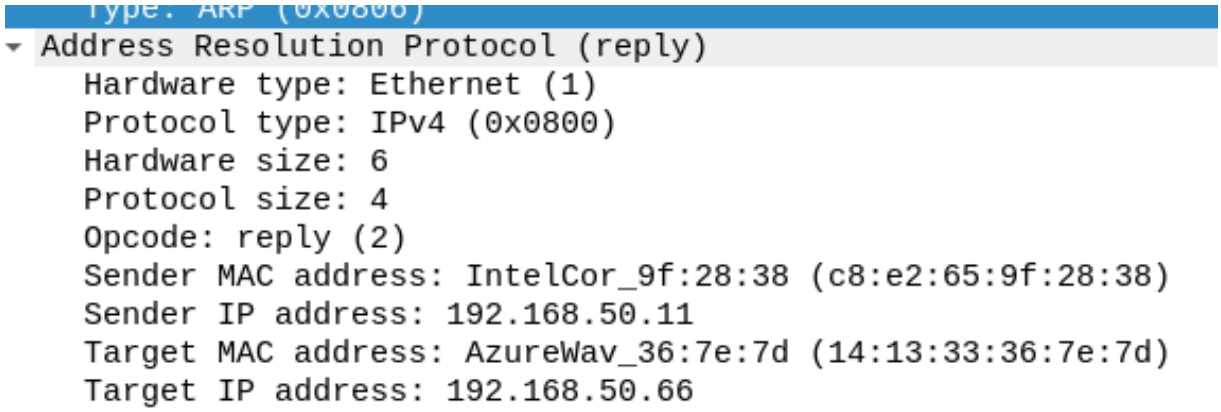
```
Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AzureWav_36:7e:7d (14:13:33:36:7e:7d)
    Sender IP address: 192.168.50.66
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.50.11
```

1. Що передається: Це ARP-запит (Address Resolution Protocol request), який використовується для визначення MAC-адреси пристрою за відомою IP-адресою.

2. Ким передається:
   Відправник має IP-адресу 192.168.50.66
   MAC-адреса відправника: 14:13:33:36:7e:7d (позначена як AzureWav_36:7e:7d)

3. Кому передається:
   Цільова IP-адреса: 192.168.50.11
   Цільова MAC-адреса: 00:00:00:00:00:00 (всі нулі, оскільки саме цю адресу і намагаються визначити)

5. ARP-відповідь



1. Що це: ARP-відповідь (видно з поля "Opcode: reply (2)")

2. Від кого:
   Відправник має IP-адресу 192.168.50.11
   MAC-адреса відправника: c8:e2:65:9f:28:38 (позначена як IntelCor_9f:28:38)

3. Кому:
   Цільова IP-адреса: 192.168.50.66
   Цільова MAC-адреса: 14:13:33:36:7e:7d (позначена як AzureWav_36:7e:7d)

По суті, це відповідь на попередній ARP-запит. Пристрій з IP-адресою 192.168.50.11 відповідає на запит, надаючи свою MAC-адресу (c8:e2:65:9f:28:38) пристрою, який зробив запит (з IP 192.168.50.66).

Поява поля Padding (доповнення) у кадрах, що переносять ARP-повідомлення, пов'язана з технічними вимогами мережевих протоколів та ефективністю передачі даних. Ось детальніше пояснення:

1. Мінімальний розмір кадру: В Ethernet існує вимога щодо мінімального розміру кадру - 64 байти (не враховуючи преамбулу та роздільник початку кадру). Це пов'язано з механізмом виявлення колізій.
2. Розмір ARP-повідомлення: Типове ARP-повідомлення має розмір 28 байтів.
3. Заголовок Ethernet: Заголовок Ethernet зазвичай займає 14 байтів.
4. Недостатній розмір: 28 (ARP) + 14 (Ethernet) = 42 байти, що менше за мінімальні 64 байти.
5. Доповнення (Padding): Щоб досягти мінімального розміру, додається поле Padding. У випадку ARP це зазвичай 18 байтів (64 - 42 - 4 = 18), де 4 байти - це контрольна сума кадру (FCS).

```
sonorma@hellcat:~$ sudo arp -a
? (192.168.50.82) at <incomplete> on wlp2s0
viktorpalych (192.168.50.11) at c8:e2:65:9f:28:38 [ether] on wlp2s0
RT-AX55-FCB8 (192.168.50.1) at 04:42:1a:bf:fc:b8 [ether] on wlp2s0
```

```
sonorma@hellcat:~$ sudo arp -a 192.168.50.11
viktorpalych (192.168.50.11) at c8:e2:65:9f:28:38 [ether] on wlp2s0
```

1. Структура Ethernet кадру:
Типовий Ethernet кадр складається з:
- Преамбули (7 байтів)
- Роздільника початку кадру (1 байт)
- Заголовка (зазвичай 14 байтів)
- Даних
- Контрольної суми кадру (FCS) або кінцевика (4 байти)

2. Причини відсутності кінцевика у захоплених кадрах:

a) Особливості захоплення на рівні мережевої карти:
- Більшість мережевих карт автоматично перевіряють FCS і відкидають його перед передачею даних операційній системі.
- Це робиться для ефективності та зменшення навантаження на процесор.

b) Налаштування програмного забезпечення для захоплення пакетів:
- Такі інструменти як Wireshark зазвичай налаштовані на роботу з даними, які вже пройшли перевірку на рівні мережевої карти.
- Вони часто не показують FCS, оскільки ця інформація вже була використана і відкинута.

c) Режими захоплення:
- Деякі мережеві карти та драйвери підтримують спеціальні режими захоплення, які можуть включати FCS.
- Однак це не є стандартною конфігурацією і вимагає спеціального налаштування.

d) Ефективність аналізу:
- Для більшості завдань аналізу трафіку FCS не є необхідним, оскільки цілісність пакету вже перевірена.

3. Можливості побачити FCS:
- Деякі спеціалізовані апаратні аналізатори можуть показувати повний кадр з FCS.
- Певні мережеві карти у поєднанні з спеціальними драйверами можуть бути налаштовані на захоплення повних кадрів.

4. Вплив на аналіз трафіку:
- Відсутність FCS у захоплених кадрах зазвичай не впливає на аналіз протоколів вищого рівня.
- Для більшості задач аналізу мережевого трафіку наявність FCS не є критичною.

5. Переваги відсутності FCS:
- Зменшення розміру захоплених даних.
- Спрощення аналізу для більшості користувачів.

Отже, відсутність кінцевика (FCS) у захоплених кадрах є результатом оптимізації процесу обробки мережевого трафіку на рівні апаратного та програмного забезпечення. Це дозволяє ефективніше працювати з даними, не втрачаючи важливої інформації для більшості завдань аналізу мережевого трафіку.