

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

**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:

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list table shows the following data:

Source Port	No.	Time	Source	Destination	Protocol	Length	Host	Info
443	622	16	88.221.92.55	192.168.50.66	TCP	1502		443
58138	623	16	192.168.50.66	88.221.92.55	TCP	66		58138
443	624	16	88.221.92.55	192.168.50.66	TCP	1502		443
443	625	16	88.221.92.55	192.168.50.66	TCP	1502		443
58138	626	16	192.168.50.66	88.221.92.55	TCP	66		58138
443	627	16	88.221.92.55	192.168.50.66	TCP	1502		443
443	628	16	88.221.92.55	192.168.50.66	TCP	1502		443
58138	629	16	192.168.50.66	88.221.92.55	TCP	66		58138
443	630	16	88.221.92.55	192.168.50.66	TCP	1502		443
443	631	16	88.221.92.55	192.168.50.66	TCP	1502		443
58138	632	16	192.168.50.66	88.221.92.55	TCP	66		58138
443	633	16	88.221.92.55	192.168.50.66	TCP	1502		443
443	634	16	88.221.92.55	192.168.50.66	TLSv1.3	1502		App
58138	635	16	192.168.50.66	88.221.92.55	TCP	66		58138
443	636	16	88.221.92.55	192.168.50.66	TCP	2938		443
443	637	16	2.23.97.240	192.168.50.66	TCP	66		443
58138	638	16	192.168.50.66	88.221.92.55	TCP	66		58138
443	639	16	88.221.92.55	192.168.50.66	TCP	2938		443

The packet details pane for the selected packet (No. 633) shows the following structure:

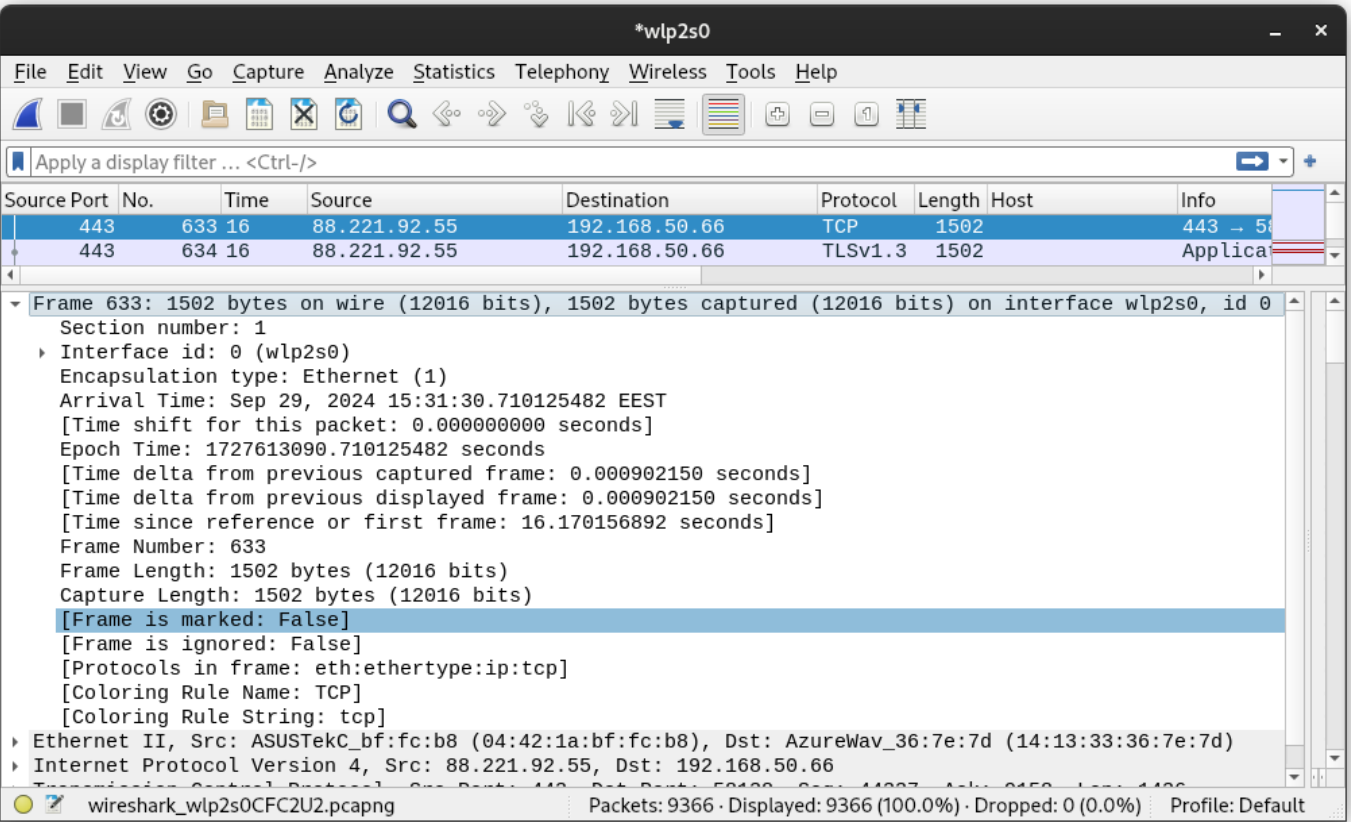
- Frame 633: 1502 bytes on wire (12016 bits), 1502 bytes captured
- Ethernet II, Src: ASUSTek\_bf:fc:b8 (04:42:1a:bf:fc:b8), Dst: 192.168.50.66
- Internet Protocol Version 4, Src: 88.221.92.55, Dst: 192.168.50.66
- Transmission Control Protocol, Src Port: 443, Dst Port: 58138

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 14 13 33 36 7e 7d 04 42 1a bf fc
0010 05 d0 86 cb 40 00 33 06 13 5e 58
0020 32 42 01 bb e3 1a c5 ea d9 6c d2
0030 01 f5 15 6a 00 00 01 01 08 0a 65
0040 7f 9c 5a d1 97 fa 04 89 6b 30 e7
0050 86 0c 02 57 1f 90 55 59 47 9e 87
0060 4d 39 48 9f 6c 93 96 5f 66 83 4d
0070 2b ee f5 4d c6 d3 aa 85 c8 54 c5
0080 4a c9 3e 26 21 0d 9e 63 82 e4 83
0090 15 14 c7 b1 f1 12 46 2d 8b c6 fd
00a0 a0 86 5e c1 11 41 1d b5 bb 6e 4d
00b0 30 99 9f 9b 39 08 3a c1 ea b3 aa
00c0 92 57 a3 d1 61 b3 38 38 41 1c 0d
00d0 5d e0 b1 17 d6 58 5d fa c2 1e 03
00e0 f4 dc 94 54 55 90 ed d3 6d d8 1d
00f0 47 a8 07 48 81 a5 16 e8 66 9f 20
```

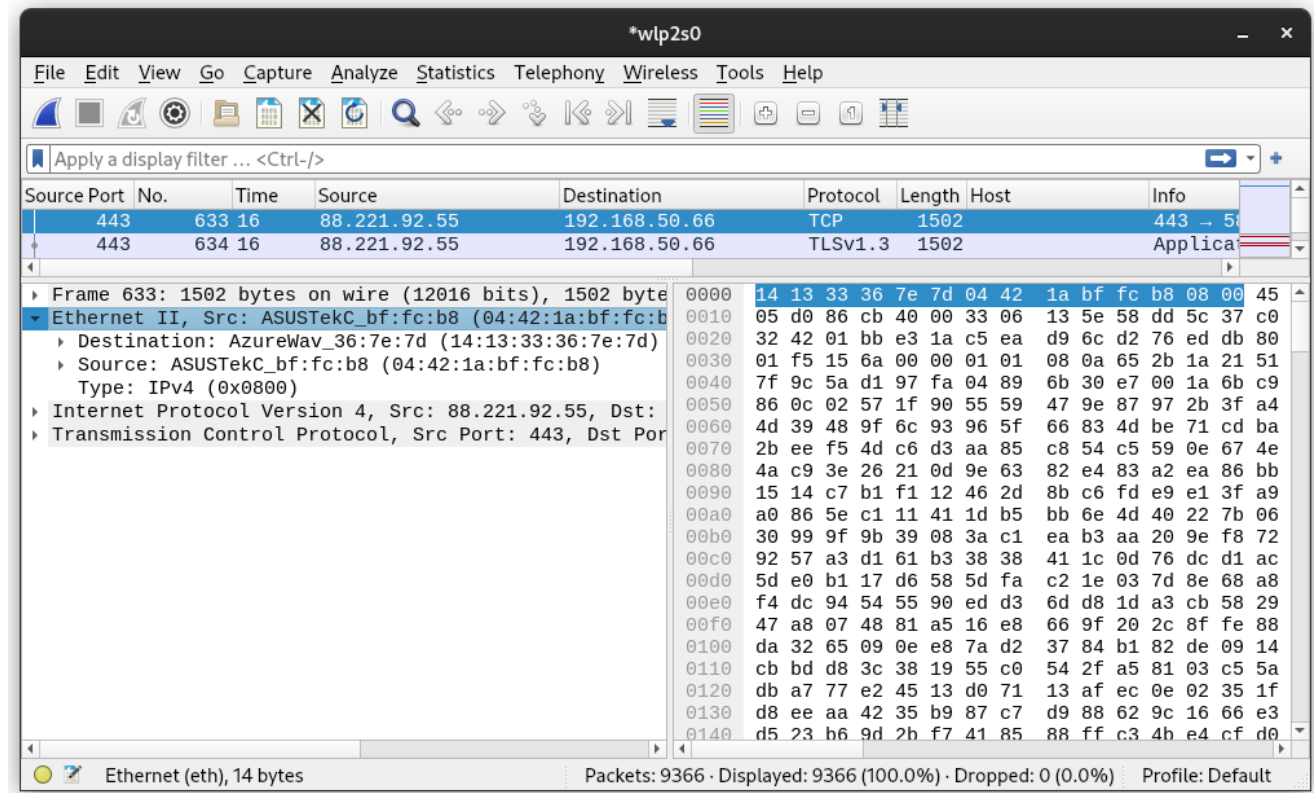
Кадр №633, розмір — 1502 байтів (12016 бітів).

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)

# Find MAC Address Vendors. Now.

Enter a MAC Address

04:42:1a|

ASUSTek COMPUTER INC.

# Find MAC Address Vendors. Now.

Enter a MAC Address

14:13:33|

AzureWave Technology Inc.

## 4. ARP-запит

```
Type: ARP (0x0800)
▼ 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

```
Type: ARP (0x0806)
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: IntelCor_9f:28:38 (c8:e2:65:9f:28:38)
  Sender IP address: 192.168.50.11
  Target MAC address: AzureWav_36:7e:7d (14:13:33:36:7e:7d)
  Target IP address: 192.168.50.66
```

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:  $28 \text{ (ARP)} + 14 \text{ (Ethernet)} = 42$  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:

а) 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.

б) 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.

с) 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.

д) 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.