

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №4

Виконав:

Ст. Лук'янчук Денис

Група 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. Від'єднався від мережі.
2. Запустив аналізатор мережевих пакетів Wireshark від імені адміністратора.
3. З'єднався назад з мережею.
4. Почав захоплення кадрів впродовж приблизно 30 секунд, здійснюючи активність в браузері.
5. Вибрав пакет для аналізу згідно порядковому номеру у списку групи.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Instruments, and Help. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

Packet List: Shows a list of captured packets. Packet 1433 is highlighted, showing it is a TLSv1.3 packet of 1514 bytes.

Packet Details: Provides a hierarchical view of the selected packet's structure. For packet 1433, it shows:

- Frame 1433: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{2F28D9C...}
- Ethernet II, Src: TPLink 12:26:03 (08:25:4a:12:26:03), Dst: LiteonTechno_41:8f:41 (d0:39:57:41:8f:41)
- Internet Protocol Version 4, Src: 13.107.136.10, Dst: 192.168.0.227
- Transmission Control Protocol, Src Port: 443, Dst Port: 61945, Seq: 72129, Ack: 6707, Len: 1460
- [6 Reassembled TCP Segments (8223 bytes): #1427(1225), #1428(1460), #1430(1460), #1431(1460), #1432(1460), #1433(1460)]
- Transport Layer Security

Packet Bytes: Displays the raw hexadecimal and ASCII data of the selected packet. The data starts with 0000 40 39 57 41 8f 41 98 25 4a 12 26 03 08 00 45 00, which corresponds to the Ethernet II header.

Кадр 1433, розмір — 1514 байтів (12112 бітів).

6. Вказав час захоплення кадру та ієрархію вкладених протоколів стеку TCP/IP, яка передається у кадрі.

```
▼ Frame 1433: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{2F28D9CB-51AC-4208-8E93-753BFC1644FB}, id 0
  Section number: 1
  ▶ Interface id: 0 (\Device\NPF_{2F28D9CB-51AC-4208-8E93-753BFC1644FB})
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct  2, 2025 15:51:38.144354000 Фінляндія (літо)
  UTC Arrival Time: Oct  2, 2025 12:51:38.144354000 UTC
  Epoch Arrival Time: 1759409498.144354000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 7.694207000 seconds]
  Frame Number: 1433
  Frame Length: 1514 bytes (12112 bits)
  Capture Length: 1514 bytes (12112 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:tls]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  ▶ Ethernet II, Src: TPLink_12:26:03 (98:25:4a:12:26:03), Dst: LiteonTechno_41:8f:41 (d0:39:57:41:8f:41)
  ▶ Internet Protocol Version 4, Src: 13.107.136.10, Dst: 192.168.0.227
  ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 61945, Seq: 72129, Ack: 6707, Len: 1460
  ▶ [6 Reassembled TCP Segments (8223 bytes): #1427(1225), #1428(1460), #1430(1460), #1431(1460), #1432(1460), #1433(1158)]
  ▶ Transport Layer Security
```

Час захоплення — 02.10.2025 15:51:38

Ієрархія протоколів стеку TCP/IP — Ethernet-кадр

IP-пакет — TCP пакет

7. Вибрав заголовок кадру та описав його характеристики.

```
▼ Frame 1433: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{2F28D9CB-51AC-4208-8E93-753BFC1644FB}, id 0
  Section number: 1
  ▶ Interface id: 0 (\Device\NPF_{2F28D9CB-51AC-4208-8E93-753BFC1644FB})
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct  2, 2025 15:51:38.144354000 Фінляндія (літо)
  UTC Arrival Time: Oct  2, 2025 12:51:38.144354000 UTC
  Epoch Arrival Time: 1759409498.144354000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 7.694207000 seconds]
  Frame Number: 1433
  Frame Length: 1514 bytes (12112 bits)
  Capture Length: 1514 bytes (12112 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:tls]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  ▶ Ethernet II, Src: TPLink_12:26:03 (98:25:4a:12:26:03), Dst: LiteonTechno_41:8f:41 (d0:39:57:41:8f:41)
  ▶ Destination: LiteonTechno_41:8f:41 (d0:39:57:41:8f:41)
  ▶ Source: TPLink_12:26:03 (98:25:4a:12:26:03)
  Type: IPv4 (0x0800)
  [Stream index: 1]
  ▶ Internet Protocol Version 4, Src: 13.107.136.10, Dst: 192.168.0.227
  ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 61945, Seq: 72129, Ack: 6707, Len: 1460
  ▶ [6 Reassembled TCP Segments (8223 bytes): #1427(1225), #1428(1460), #1430(1460), #1431(1460), #1432(1460), #1433(1158)]
  ▶ Transport Layer Security
```

0000	d0 39 57 41 8f 41 98 25 4a 12 26 03 08 00 45 00
0010	05 dc e1 e7 40 00 73 06 c9 33 0d 6b 88 8a c0 a8
0020	00 e3 01 bb f1 f9 5f 4e b2 b9 55 6d 4e a3 50 18
0030	40 01 b3 be 00 00 08 bb a5 d7 3e 84 6a a8 61 c0
0040	37 0c 9a 9a 71 8a a9 c2 cf e2 1b 72 48 ec e7 92
0050	5b ff 50 21 3d 9e ab 7b e8 b5 e0 79 36 f0 a0 27
0060	3d fa fa 61 8a 32 ce 28 bd 85 0d 89 bc 51 f7 9a
0070	e3 fa 81 6e 72 86 26 c6 9e 67 1f 43 91 ff ac 28
0080	0b 22 b7 76 4e 88 d7 22 cd d7 95 3a f9 cd b6 7d
0090	d1 26 ef ed cb d3 ff 6a 1f e2 8a b8 35 bc ce b0
00a0	f0 94 01 96 64 d5 83 8b 03 44 dc f3 01 23 9d a7
00b0	e2 55 1a d2 8f ee ca 5d 45 c0 97 c1 04 9e b9 b2
00c0	57 0d 4c 1a 22 fb c5 32 7a 4c a6 a3 06 93 c4 b2
00d0	c8 21 c2 8b 14 8e b2 bf 4b 21 95 78 bc 44 27 e3
00e0	b5 97 ad be fb 98 39 21 7f c0 18 9b d2 fc 7d b6
00f0	10 d7 ea 23 a2 ba dc fa aa 3b 74 e4 85 c7 34 dd
0100	d4 50 46 76 68 d5 4e a9 92 15 a7 93 2d 9f 17 f4
0110	c6 58 1d ba b1 ad be b7 d0 18 b5 e9 75 64 ed 5b
0120	ab 7c 5a 96 14 87 36 af 02 59 3b f7 c9 66 e1 35
0130	06 7b 7a ab f3 f0 d6 16 63 f0 09 7d 6e 47 32 a8
0140	23 d1 38 3e 73 2c 56 51 d1 f5 00 5d 78 a5 9c e6
0150	a9 56 45 8e b1 f1 61 42 ae 66 72 e3 b1 98 31 87
0160	36 4c 57 bb f0 2c 89 58 5f 0c 24 81 97 ce 59 65

Дані заголовка:

Розмір — 16 байтів


Відправник — мережевий адаптер (MAC 98:25:4a:12:26:03)

Отримувач — маршрутизатор (MAC d0:39:57:41:8f:41)

Вкладений протокол — IPv4

8. За першими половинами MAC-адрес отримав інформацію про виробників пристроїв передавача та отримувача:


Для отримувача:

 Визначення виробника по MAC-адресі


Введіть mac-адресу для перевірки
98:25:4a


ПЕРЕВІРИТИ

Виробником пристрою з mac-адресою 98:25:4a є компанія:

Ім'я компанії:	TP-Link Systems Inc
Адреса компанії:	5 Peters Canyon Rd Suit 300 Irvine CA SG 92606
Унікальний ідентифікатор організації:	98254A
Розмір діапазону:	MA-L 


MA-S






Up to
4,096 devices


MA-M






Up to
1 million devices


MA-L





Up to
16 million devices


Для передавача:

 Визначення виробника по MAC-адресі


Введіть mac-адресу для перевірки
d0:39:57


ПЕРЕВІРИТИ

Виробником пристрою з mac-адресою d0:39:57 є компанія:

Ім'я компанії:	Liteon Technology Corporation
Адреса компанії:	4F, 90, Chien 1 Road New Taipei City Taiwan TW 23585
Унікальний ідентифікатор організації:	D03957
Розмір діапазону:	MA-L 


MA-S






Up to
4,096 devices


MA-M






Up to
1 million devices

MA-L





Up to
16 million devices

9. Дослідив протокол ARP. Для відображення пакетів цього протоколу скористався однойменним фільтром arp:

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Capture, Analyze, Statistics, Telephony, Wireless, Instruments, and Help. Below the menu is a toolbar with icons for common actions like opening files, saving, and zooming. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is #621, an ARP request from 192.168.0.227 to 192.168.0.1. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, and the ARP (Request) payload.
- Packet Bytes:** Displays the raw packet data in hexadecimal and ASCII. The ARP payload is highlighted in green, showing the sender and target MAC and IP addresses.

The selected packet (621) is an ARP request from 192.168.0.227 to 192.168.0.1. The details pane shows the Ethernet II header (Type: ARP), the Internet Protocol Version 4 header (Source: 192.168.0.227, Destination: 192.168.0.1), and the ARP (Request) payload (Sender: 08:00:27:00:00:00, Target: 08:00:27:00:00:00).

10. Вибрав довільний ARP-запит:

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: TPLink_12:26:03 (98:25:4a:12:26:03)
  Sender IP address: 192.168.0.1
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.0.226
```

У запиті пристрій з IP-адресою і MAC-адресою розсилає по всій мережі широкомовне повідомлення. Він питає: «Хто має таку IP адресу? Скажіть мені свою MAC-адресу». У полі призначеного MAC-адреса ще невідома, тому там стоять нулі.

11. Вибрав ARP-відповідь на ARP-запит з попереднього пункту і пояснив:

У відповіді вже сам власник IP 192.168.0.1 (наприклад, роутер з MAC 98:25:4a:12:26:03) надсилає повідомлення напряму відправнику: «Я маю IP 192.168.0.1, моя MAC-адреса — 98:25:4a:12:26:03». Це повідомлення йде не всім, а конкретно тому, хто питає.

12. Поясніть появу у кадрах, які переносять ARP-повідомлення, поля Padding:

Поле Padding з'являється тому, що Ethernet-кадр має мінімальний розмір — 64 байти. Якщо передані дані менші, то кадр добивають нулями, щоб він був потрібної довжини. Тому у невеликих повідомленнях у кадрі додаються байти-заповнювачі.

13. Ознайомився з повною ARP-таблицею, виконавши у консолі команду `arp -a`:

```
PS C:\Users\denys> arp -a

Interface: 192.168.0.227 --- 0x8
    Internet Address      Physical Address      Type
    192.168.0.1           98-25-4a-12-26-03    dynamic
    192.168.0.109         cc-b1-1a-0d-ea-f1     dynamic
    192.168.0.255         ff-ff-ff-ff-ff-ff     static
    224.0.0.22            01-00-5e-00-00-16     static
    224.0.0.251           01-00-5e-00-00-fb     static
    224.0.0.252           01-00-5e-00-00-fc     static
    224.0.0.253           01-00-5e-00-00-fd     static
    239.255.255.246       01-00-5e-7f-ff-f6     static
    239.255.255.250       01-00-5e-7f-ff-fa     static
    255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.21.128.1 --- 0x2b
    Internet Address      Physical Address      Type
    172.21.136.221        00-15-5d-2e-4c-5c     dynamic
    172.21.143.255        ff-ff-ff-ff-ff-ff     static
    224.0.0.22            01-00-5e-00-00-16     static
    224.0.0.251           01-00-5e-00-00-fb     static
    239.255.255.246       01-00-5e-7f-ff-f6     static
    239.255.255.250       01-00-5e-7f-ff-fa     static
PS C:\Users\denys> |
```

14. Отримав запис ARP-таблиці для конкретної IP-адреси:

```
PS C:\Users\denys> arp -a 192.168.0.1

Interface: 192.168.0.227 --- 0x8
    Internet Address      Physical Address      Type
    192.168.0.1           98-25-4a-12-26-03    dynamic
PS C:\Users\denys> |
```

15. Дав відповідь на питання “Чому у захоплених кадрах немає кінцевика?”:

У захоплених кадрах немає кінцевика (FCS), тому що він використовується тільки для перевірки цілісності на рівні мережевої карти. Після успішної перевірки він відкидається і не передається в Wireshark, бо більше не несе корисної інформації.

Висновок: Під час виконання лабораторно роботи я отримав знання і практичні навички про інтерпретації Ethernet-кадрів. Ознайомився на основі опрацьованого теоретичного лекційного матеріалу з форматом кадру Ethernet II (порядок полів, їх розмір та призначення).