

**Комп'ютерні інформаційні мережі  
ЛАБОРАТОРНА РОБОТА №4**

**Тема: «Аналіз повідомлень канального рівня Ethernet засобами Wireshark. Утиліти для діагностики мережі на канальному рівні».**

Виконала:  
Ст. Пелещак Вероніка  
ПМІ-35с

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

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

### Хід роботи:

1. Спочатку я від'єдналась від мережі, запустила Wireshark від імені адміністратора і з'єдналась з мережею. Захопила кадри, здійснюючи активність у браузері.

No.	Time	Source	Destination	Protocol	Length	Info	Source Port	Host
1117	20	192.168.0.151	192.168.0.255	NBNS	92	Name query NB WORKGROUP<1d>		137
1118	20	fe80::147f:b5df:64...	fe80::1a:9b1a:78fc...	ICMPv6	86	Neighbor Advertisement fe80::147f:b5df:6440:4405 (sol, ...		
1119	21	192.168.0.151	192.168.0.255	NBNS	92	Name query NB WORKGROUP<1d>		137
1120	23	192.168.0.151	192.168.0.255	NBNS	92	Name query NB WORKGROUP<1d>		137
1121	23	192.168.0.151	17.248.213.65	TLSv1...	268	Application Data		65028
1122	23	192.168.0.151	17.248.213.65	TLSv1...	532	Application Data		65028
1123	23	192.168.0.151	17.248.213.65	TLSv1...	97	Application Data		65028
1124	23	17.248.213.65	192.168.0.151	TCP	66	443 → 65028 [ACK] Seq=3516 Ack=3717 Win=63 Len=0 TSval=...		443
1125	23	17.248.213.65	192.168.0.151	TCP	66	443 → 65028 [ACK] Seq=3516 Ack=3748 Win=63 Len=0 TSval=...		443
1126	23	17.248.213.65	192.168.0.151	TLSv1...	666	Application Data		443
1127	23	192.168.0.151	17.248.213.65	TCP	66	65028 → 443 [ACK] Seq=3748 Ack=4116 Win=2039 Len=0 TSva=...		65028
1128	23	192.168.0.151	17.248.213.65	TLSv1...	200	Application Data		65028
1129	23	192.168.0.151	17.248.213.65	TLSv1...	748	Application Data		65028
1130	23	192.168.0.151	17.248.213.65	TLSv1...	97	Application Data		65028
1131	23	17.248.213.65	192.168.0.151	TCP	66	443 → 65028 [ACK] Seq=4116 Ack=3882 Win=63 Len=0 TSval=...		443
1132	23	17.248.213.65	192.168.0.151	TCP	66	443 → 65028 [ACK] Seq=4116 Ack=4564 Win=63 Len=0 TSval=...		443
1133	23	17.248.213.65	192.168.0.151	TLSv1...	101	Application Data		443
1134	23	192.168.0.151	17.248.213.65	TCP	66	65028 → 443 [ACK] Seq=4595 Ack=4151 Win=2048 Len=0 TSva=...		65028
1135	23	17.248.213.65	192.168.0.151	TCP	66	443 → 65028 [ACK] Seq=4151 Ack=4595 Win=63 Len=0 TSval=...		443
1136	24	17.248.213.65	192.168.0.151	TLSv1...	837	Application Data		443
1137	24	17.248.213.65	192.168.0.151	TLSv1...	97	Application Data		443
1138	24	192.168.0.151	17.248.213.65	TCP	66	65028 → 443 [ACK] Seq=4595 Ack=4953 Win=2036 Len=0 TSva=...		65028

> Frame 1135: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on int...

> Ethernet II, Src: TplinkTechno\_5a:6d:f5 (b0:be:76:5a:6d:f5), Dst: 7a:53:94:6...

> Internet Protocol Version 4, Src: 17.248.213.65, Dst: 192.168.0.151

> Transmission Control Protocol, Src Port: 443, Dst Port: 65028, Seq: 4151, Ac...

*Кадр: №1135, Розмір: 66 байтів (528 бітів).*

2. Інформація про кадр:

```
▼ Frame 1135: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on int
  Section number: 1
  > Interface id: 0 (en0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 24, 2025 19:37:18.831815000 EEST
  UTC Arrival Time: Sep 24, 2025 16:37:18.831815000 UTC
  Epoch Arrival Time: 1758731838.831815000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.042017000 seconds]
  [Time delta from previous displayed frame: 0.042017000 seconds]
  [Time since reference or first frame: 23.979369000 seconds]
  Frame Number: 1135
  Frame Length: 66 bytes (528 bits)
  Capture Length: 66 bytes (528 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
  > Ethernet II, Src: TplinkTechno_5a:6d:f5 (b0:be:76:5a:6d:f5), Dst: 7a:53:94:6
  > Internet Protocol Version 4, Src: 17.248.213.65, Dst: 192.168.0.151
  > Transmission Control Protocol, Src Port: 443, Dst Port: 65028, Seq: 4151, Ac
```

Час захоплення: 24.09.2025 19:37:18.

Ієрархія протоколів: кадр Ethernet → IP-пакет → TCP-сегмент.

### 3. Основні складові заголовку кадра:

```
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
v Ethernet II, Src: TpLinkTechno_5a:6d:f5 (b0:be:76:5a:6d:f5), Dst: 7a:53:94:6a:1b:a3 (7a:53:94:6a:1b:a3)
  > Destination: 7a:53:94:6a:1b:a3 (7a:53:94:6a:1b:a3)
  > Source: TpLinkTechno_5a:6d:f5 (b0:be:76:5a:6d:f5)
  Type: IPv4 (0x0800)
  [Stream index: 2]
  > Internet Protocol Version 4, Src: 17.248.213.65, Dst: 192.168.0.151
  > Transmission Control Protocol, Src Port: 443, Dst Port: 65028, Seq: 4151, Ack: 4595, Len: 0

0000  7a 53 94 6a 1b a3 b0 be 76 5a 6d f5 08 00 45 80  zS j . . . . vZm . . E .
0010  00 34 73 ad 40 00 36 06 28 1e 11 f8 d5 41 c0 a8  4s @ 6 . ( . . . A . .
0020  00 97 01 bb fe 04 44 75 68 93 77 4f a8 7f 80 10  . . . . Du h w 0 . . .
0030  00 3f 85 69 00 00 01 01 08 0a 44 f2 7f 1e 63 79  . ? i . . . . D . . cy
0040  54 7a                                     Tz
```

Розмір: 14 байтів

Відправник: мережевий адаптер (MAC b0:be:76:5a:6d:f5)

Отримувач: маршрутизатор (MAC 7a:53:94:6a:1b:a3)

Вкладений протокол: IPv4

### 4. За допомогою MAC адреси дізналась інформацію про виробника відправника:

b0:be:76

[ПЕРЕВІРИТИ](#)

Виробником пристрою з mac-адресою b0:be:76 є компанія:

Ім'я компанії:	TP-LINK TECHNOLOGIES CO.,LTD.
Адреса компанії:	Building 24(floors 1,3,4,5)and 28(floors 1-4)Central Science and Technology Park,Shennan Road,Nanshan Shenzhen Guangdong CN 5180
Унікальний ідентифікатор організації:	B0BE76
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

Введіть mac-адресу для перевірки

7a:53:94

ПЕРЕВІРИТИ

Виробника пристрою не знайдено

5. Дослідила протокол ARP і скористалась однойменним фільтром arp:

arp									
No.	Time	Source	Destination	Protocol	Length	Info	Source Port	Host	
977	14	TpLinkTechno_5a:6d:f5	7a:53:94:6a:1b:a3	ARP	42	Who has 192.168.0.151? Tell 192.168.0.1			
978	14	7a:53:94:6a:1b:a3	TpLinkTechno_5a:6d:f5	ARP	42	192.168.0.151 is at 7a:53:94:6a:1b:a3			

6. ARP-запит:

```
> Frame 977: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
> Ethernet II, Src: TpLinkTechno_5a:6d:f5 (b0:be:76:5a:6d:f5), Dst: 7a:53:94:6a:1b:a3 (7a:53:94:6a:1b:a3)
v Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: TpLinkTechno_5a:6d:f5 (b0:be:76:5a:6d:f5)
  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: 192.168.0.151
```

**Hardware type: Ethernet (1)** — використовується Ethernet.

**Protocol type: IPv4 (0x0800)** — визначається IP-протокол версії 4.

**Hardware size: 6** — довжина MAC-адреси 6 байт.

**Protocol size: 4** — довжина IP-адреси 4 байти.

**Opcode: request (1)** — це ARP-запит.

**Sender MAC address: b0:be:76:5a:6d:f5** — MAC-адреса відправника.

***Sender IP address: 192.168.0.1*** — IP-адреса відправника.

***Target MAC address: 00:00:00:00:00:00*** — MAC-адреса цілі невідома.

***Target IP address: 192.168.0.151*** — IP-адреса, чию MAC-адресу шукають.

## 7. ARP-відповідь:

```
[Stream index: 2]
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: 7a:53:94:6a:1b:a3 (7a:53:94:6a:1b:a3)
  Sender IP address: 192.168.0.151
  Target MAC address: TpLinkTechno_5a:6d:f5 (b0:be:76:5a:6d:f5)
  Target IP address: 192.168.0.1
```

***Hardware type: Ethernet (1)*** — використовується Ethernet.

***Protocol type: IPv4 (0x0800)*** — протокол – IPv4.

***Hardware size: 6*** — MAC-адреса має 6 байт.

***Protocol size: 4*** — IP-адреса має 4 байти.

***Opcode: reply (2)*** — це ARP-відповідь.

***Sender MAC address: 7a:53:94:6a:1b:a3*** — MAC-адреса відправника.

***Sender IP address: 192.168.0.151*** — IP-адреса відправника.

***Target MAC address: b0:be:76:5a:6d:f5*** — MAC-адреса запитувача.

***Target IP address: 192.168.0.1*** — IP-адреса запитувача.

**8. Padding:** У Ethernet-кадрі мінімальна довжина повинна бути 64 байти. Якщо ARP-повідомлення менше, ніж ця довжина, то в кінець кадру додається Padding (заповнення нулями), щоб «добити» розмір. Якщо поле Padding відсутнє, то це означає, що загальна довжина кадру і так досягла мінімально необхідних 64 байт.

**9.** Виконала команду `arp -a` у Terminal:

```
veronikapelesak@Noutbuk-Veronika ~ % arp -a
? (192.168.0.1) at b0:be:76:5a:6d:f5 on en0 ifscope [ethernet]
? (192.168.0.123) at 8a:7f:25:72:15:6f on en0 ifscope [ethernet]
? (192.168.0.143) at cc:b5:d1:6c:34:2f on en0 ifscope [ethernet]
? (192.168.0.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
veronikapelesak@Noutbuk-Veronika ~ %
```

## **10. Чому у захоплених кадрах немає кінцевика?**

У захоплених кадрах Wireshark немає кінцевика, бо цей елемент кадру перевіряється апаратно мережею та не передається операційній системі. Мережеві карти відкидають його ще до того, як дані потрапляють у Wireshark. Тому програма показує тільки основну частину кадру, і це нормальна поведінка, яка не впливає на аналіз мережевого трафіку.

**Висновок:** Під час роботи проаналізовано Ethernet-кадри та протокол ARP за допомогою Wireshark і консольних утиліт. Визначено розмір кадру, MAC-адреси, вкладений протокол, обмін ARP-запитами та відповідями, пояснено призначення поля Padding і відсутність кінцевика (FCS). Робота закріпила практичні навички аналізу мережевих повідомлень.