

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №5

Виконала:

Ст Кравець О. Б.

ПМО-31

Тема: Аналіз повідомлень канального рівня Ethernet засобами Wireshark.

Мета роботи: Здобути практичні навички з інтерпретації Ethernet-кадрів. Ознайомитися на основі опрацьованого теоретичного лекційного матеріалу з форматом кадру Ethernet II (порядок полів, їх розмір та призначення).

Хід роботи

1. Від'єдналася від мережі.
2. Запустила аналізатор мережевих пакетів Wireshark від імені адміністратора.
3. З'єдналася з мережею.
4. Захопила кадри впродовж приблизно 30 секунд, здійснюючи активність в браузері.
5. Вибрала пакет для аналізу.

The screenshot displays the Wireshark network protocol analyzer. The top pane shows a list of captured packets. Packet 3792 is highlighted, showing it is an Ethernet II frame from 192.168.1.5 to 185.199.109.133, protocol TCP, port 443, with a sequence number of 4236. The bottom pane provides a detailed view of this packet, showing the frame structure: Ethernet II (54 bytes), Internet Protocol Version 4 (20 bytes), and Transmission Control Protocol (54 bytes). The packet is captured on the interface \Device\NPF_{B61FBC2F-2A7E-4541-A05A-0931929D04EA}.

No.	Time	Source	Destination	Protocol	Length	Info
3785	30.156000	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=377698 Win=262656 Len=0
3786	30.164988	185.199.109.133	192.168.1.5	TLSv1.3	1514	Application Data [TCP segment of a reassembled PDU]
3787	30.165062	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=379158 Ack=4236 Win=151552 Len=1460...
3788	30.165087	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=380618 Win=262656 Len=0
3789	30.165136	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=380618 Ack=4236 Win=151552 Len=1460...
3790	30.165167	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=382078 Ack=4236 Win=151552 Len=1460...
3791	30.165184	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=383538 Win=262656 Len=0
3792	30.165223	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [PSH, ACK] Seq=383538 Ack=4236 Win=151552 Len=...
3793	30.165250	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=384998 Ack=4236 Win=151552 Len=1460...

Wireshark - Packet 3794 - Wi-Fi

> Frame 3794: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B61FBC2F-2A7E-4541-A05A-0931929D04EA}, id
> Ethernet II, Src: LiteonTe_67:fe:4b (80:30:49:67:fe:4b), Dst: Kaonmedi_ff:ff:05 (00:08:b9:ff:ff:05)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 185.199.109.133
> Transmission Control Protocol, Src Port: 53796, Dst Port: 443, Seq: 4236, Ack: 386458, Len: 0

```
0000  00 08 b9 ff ff 05 80 30 49 67 fe 4b 08 00 45 00  .....0 Ig·K·E·
0010  00 28 70 23 40 00 80 06 a1 b2 c0 a8 01 05 b9 c7  ·(p#@·····
0020  6d 85 d2 24 01 bb 69 4b c5 2b 6e 8e 31 59 50 10  m·$·iK ·+n·1YP·
0030  04 02 20 9a 00 00  .....
```

Кадр № 3792

Розмір – 54 байт (432 біт)

6. Вказала час захоплення кадру та ієрархію вкладених протоколів стеку ТСР/ІР, яка передається у кадрі.

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets. Packet 3794 is selected, and the bottom pane shows its details and raw data.

No.	Time	Source	Destination	Protocol	Length	Info
3785	30.156000	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=377698 Win=262656 Len=0
3786	30.164988	185.199.109.133	192.168.1.5	TLSv1.3	1514	Application Data [TCP segment of a reassembled PDU]
3787	30.165062	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=379158 Ack=4236 Win=151552 Len=1460...
3788	30.165087	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=380618 Win=262656 Len=0
3789	30.165136	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=380618 Ack=4236 Win=151552 Len=1460...
3790	30.165167	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=382078 Ack=4236 Win=151552 Len=1460...
3791	30.165184	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=383538 Win=262656 Len=0
3792	30.165223	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [PSH, ACK] Seq=383538 Ack=4236 Win=151552 Len=...

Wireshark - Packet 3794 - Wi-Fi

▼ Frame 3794: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B61FBC2F-2A7E-4541-A05A-0931929D04EA}, ...

- > Interface id: 0 (\Device\NPF_{B61FBC2F-2A7E-4541-A05A-0931929D04EA})
- Encapsulation type: Ethernet (1)
- Arrival Time: Oct 8, 2022 00:00:19.940277000 Фінляндія (літо)
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1665176419.940277000 seconds
- [Time delta from previous captured frame: 0.000015000 seconds]
- [Time delta from previous displayed frame: 0.000015000 seconds]
- [Time since reference or first frame: 30.165265000 seconds]
- Frame Number: 3794
- Frame Length: 54 bytes (432 bits)
- Capture Length: 54 bytes (432 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp]

0000 00 08 b9 ff ff 05 80 30 49 67 fe 4b 08 00 45 000 Ig K...E..
0010 00 28 70 23 40 00 00 06 a1 b2 c0 a8 01 05 b9 c7 ..(p#@.....

Закрити Довідка

Час захоплення:

08.10.2022, 00:00:19 EET

Ієрархія протоколів стеку ТСР/ІР:

- **Ethernet-кадр**
- **ІР-пакет**
 - **ТСР-пакет**

7. Вибрала заголовок кадру та описала його характеристики.

Заголовок кадру та його складові:

Розмір: 16 байт

Отримувач: мережевий адаптер (MAC 00 08 b9 ff ff 05)

Відправник: маршрутизатор (MAC 80 30 49 67 fe 4b)

Вкладений протокол, що передається: IPv4

The image shows a Wireshark packet capture analysis of a Wi-Fi frame. The top pane displays a list of captured packets. Packet 3794 is selected, and the bottom pane shows its detailed structure and raw data.

No.	Time	Source	Destination	Protocol	Length	Info
3785	30.156000	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=377698 Win=262656 Len=0
3786	30.164988	185.199.109.133	192.168.1.5	TLSv1.3	1514	Application Data [TCP segment of a reassembled PDU]
3787	30.165062	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=379158 Ack=4236 Win=151552 Len=1460...
3788	30.165087	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=380618 Win=262656 Len=0
3789	30.165136	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=380618 Ack=4236 Win=151552 Len=1460...
3790	30.165167	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [ACK] Seq=382078 Ack=4236 Win=151552 Len=1460...
3791	30.165184	192.168.1.5	185.199.109.133	TCP	54	53796 → 443 [ACK] Seq=4236 Ack=383538 Win=262656 Len=0
3792	30.165223	185.199.109.133	192.168.1.5	TCP	1514	443 → 53796 [PSH, ACK] Seq=383538 Ack=4236 Win=151552 Len=...

Wireshark · Packet 3794 · Wi-Fi

> Frame 3794: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B61FBC2F-2A7E-4541-A05A-0931929D04EA}, id
▼ Ethernet II, Src: LiteonTe_67:fe:4b (80:30:49:67:fe:4b), Dst: Kaonmedi_ff:ff:05 (00:08:b9:ff:ff:05)
 > Destination: Kaonmedi_ff:ff:05 (00:08:b9:ff:ff:05)
 > Source: LiteonTe_67:fe:4b (80:30:49:67:fe:4b)
 Type: IPv4 (0x0800)
 > Internet Protocol Version 4, Src: 192.168.1.5, Dst: 185.199.109.133
 > Transmission Control Protocol, Src Port: 53796, Dst Port: 443, Seq: 4236, Ack: 386458, Len: 0

0000 00 08 b9 ff ff 05 80 30 49 67 fe 4b 00 00 45 000 Ig·K··E·
0010 00 28 70 23 40 00 80 06 a1 b2 c0 a8 01 05 b9 c7 ·(p#@·...·
0020 6d 85 d2 24 01 bb 69 4b c5 2b 6e 8e 31 59 50 10 m·\$.·iK·+n·1YP·
0030 04 02 20 9a 00 00

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

- Для передавача:

Введіть mac-адресу для перевірки

00:08:b9:ff:ff:05

ПЕРЕВІРИТИ

Виробником пристрою з mac-адресою 00:08:b9:ff:ff:05 є компанія:

Ім'я компанії:	Kaonmedia CO., LTD.
Адреса компанії:	#113 Imae 1-Dong, Bundang-Gu Sungnam-City Kyungki-Do KR 463-829
Унікальний ідентифікатор організації:	0008B9
Розмір діапазону:	MA-L 




- Для отримувача:

Введіть mac-адресу для перевірки

80:30:49:67:fe:4b

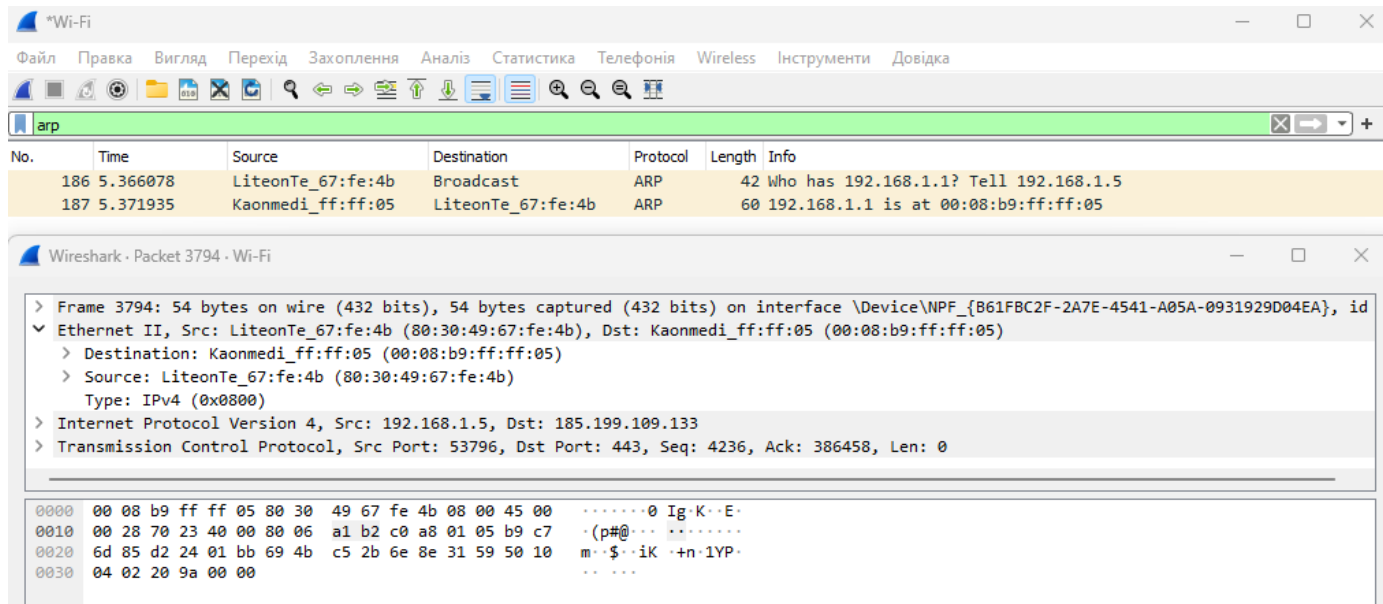
ПЕРЕВІРИТИ

Виробником пристрою з mac-адресою 80:30:49:67:fe:4b є компанія:

Ім'я компанії:	Liteon Technology Corporation
Адреса компанії:	4F, 90, Chien 1 Road New Taipei City Taiwan TW 23585
Унікальний ідентифікатор організації:	803049
Розмір діапазону:	MA-L 



9. Відшукала за допомогою фільтру кадри, які переносять повідомлення протоколу ARP.



10. Пояснила появу у кадрах поля “Padding” на прикладі рисунку зліва з ЛР.

Поле Padding потрібне для внесення додаткових нулів, щоб Ір-заголовок був кратним 32 бітам, якщо він кратний сам по собі, то падингу не буде.

11. Дала відповідь на запитання підвищеної складності:

Чому у захопленому кадрі немає кінцевика?

Кінцевик відсутній, бо він використовується для перевірки успішності передачі даних, так як перевірка була успішно пройдена, то він не потрібен, бо корисної інформації не несе.

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