

Міністерство освіти і науки України
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра програмування

Звіт
до лабораторної роботи №4
з теми
**“Аналіз повідомлень канального рівня Ethernet
засобами Wireshark”**

Підготував:
студент ПМІ-33
Процьків Назарій

Львів 2023

Хід роботи

1. Від'єднавшись від мережі, запустив аналізатор мережевих пакетів Wireshark від імені адміністратора.
2. Після під'єднання до мережі реалізував захоплення кадрів та обрав кадр для аналізу. Кадр №1731, розмір 1242 байт (9936 біт).

1731	16.766973	104.16.224.149	192.168.1.11	QUIC	1242	Protected Payload (KP0)
<						
>						
> Frame 1731: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF_{8B57350D-B6BD-4305-8E40-6D0F4C2B595C}, id 0						
> Ethernet II, Src: Tp-LinkT_82:e4:e4 (c0:25:e9:82:e4:e4), Dst: IntelCor_e8:ea:0e (40:1c:83:e8:ea:0e)						
> Internet Protocol Version 4, Src: 104.16.224.149, Dst: 192.168.1.11						
> User Datagram Protocol, Src Port: 443, Dst Port: 54529						
> QUIC IETF						

3. Час захоплення – 07.10.2023 23:58:14

Ієрархія протоколів стеку TCP/IP:

- Ethernet-кадр
- IP-пакет
- UDP-сегмент
- DNS-повідомлення

▼ Frame 1731: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF_{8B57350D-B6BD-4305-8E40-6D0F4C2B595C}, id 0	
Section number: 1	
> Interface id: 0 (\Device\NPF_{8B57350D-B6BD-4305-8E40-6D0F4C2B595C})	
Encapsulation type: Ethernet (1)	
Arrival Time: Oct 7, 2023 23:58:14.490247000 Фінляндія (літо)	
[Time shift for this packet: 0.000000000 seconds]	
Epoch Time: 1696712294.490247000 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: 16.766973000 seconds]	
Frame Number: 1731	
Frame Length: 1242 bytes (9936 bits)	
Capture Length: 1242 bytes (9936 bits)	
[Frame is marked: False]	
[Frame is ignored: False]	
[Protocols in frame: eth:ethertype:ip:udp:quic]	
[Coloring Rule Name: UDP]	
[Coloring Rule String: udp]	
> Ethernet II, Src: Tp-LinkT_82:e4:e4 (c0:25:e9:82:e4:e4), Dst: IntelCor_e8:ea:0e (40:1c:83:e8:ea:0e)	
> Internet Protocol Version 4, Src: 104.16.224.149, Dst: 192.168.1.11	
> User Datagram Protocol, Src Port: 443, Dst Port: 54529	
> QUIC IETF	

4. Заголовок кадру та його складові:

Отримувач: мережевий адаптер (MAC 40:1c:83:e8:ea:0e)


Відправник: маршрутизатор (MAC c0:25:e9:82:e4:e4)

Вкладений протокол, що передається: IPv4

> Frame 1731: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF_{8B57350D-B6BD-4305-8E40-6D0F4C2B595C}, id 0	
▼ Ethernet II, Src: Tp-LinkT_82:e4:e4 (c0:25:e9:82:e4:e4), Dst: IntelCor_e8:ea:0e (40:1c:83:e8:ea:0e)	
> Destination: IntelCor_e8:ea:0e (40:1c:83:e8:ea:0e)	
> Source: Tp-LinkT_82:e4:e4 (c0:25:e9:82:e4:e4)	
Type: IPv4 (0x0800)	

5. За першою половиною MAC адреси отримав інформацію про виробника пристроїв отримувача та передавача:

Виробником пристрою з mac-адресою 40:1c:83 є компанія:

Ім'я компанії:	Intel Corporate
Адреса компанії:	Lot 8, Jalan Hi-Tech 2/3 Kulim Kedah MY 09000
Унікальний ідентифікатор організації:	401C83
Розмір діапазону:	MA-L 

Виробником пристрою з mac-адресою c0:25:e9 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:	C025E9
Розмір діапазону:	MA-L 

6. За допомогою фільтра знайшов кадри, які переносять повідомлення протоколу ARP

arp						
No.	Time	Source	Destination	Protocol	Length	Info
19	0.370071	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
25	1.394158	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
28	2.421753	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
29	2.597047	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.1
32	3.339470	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
40	4.363972	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
77	5.387886	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
636	8.462325	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
713	9.485590	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
790	10.508072	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
794	11.531401	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
953	12.555582	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
1059	13.477302	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
1179	14.506386	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
1305	15.524835	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
1577	16.550098	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
1954	17.575262	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
2435	18.597104	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1
3104	19.620789	Tp-LinkT_82:e4:e4	Broadcast	ARP	42	Who has 192.168.1.13? Tell 192.168.1.1

7. Поле Padding потрібне для внесення додаткових нулів, щоб ір-заголовок був кратним 32 бітам, у захоплених мною кадрів він і так є кратним тож це поле відсутнє.
8. Кінцевик відсутній, бо він використовується для перевірки успішності передачі даних, оскільки перевірка була успішно пройдена, то він не потрібен, бо корисної інформації не несе.