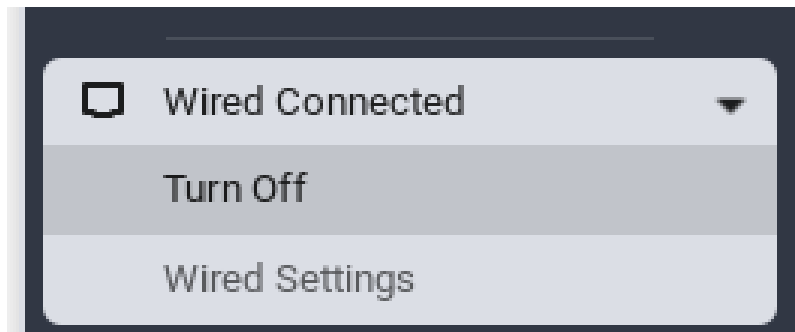


Хід роботи

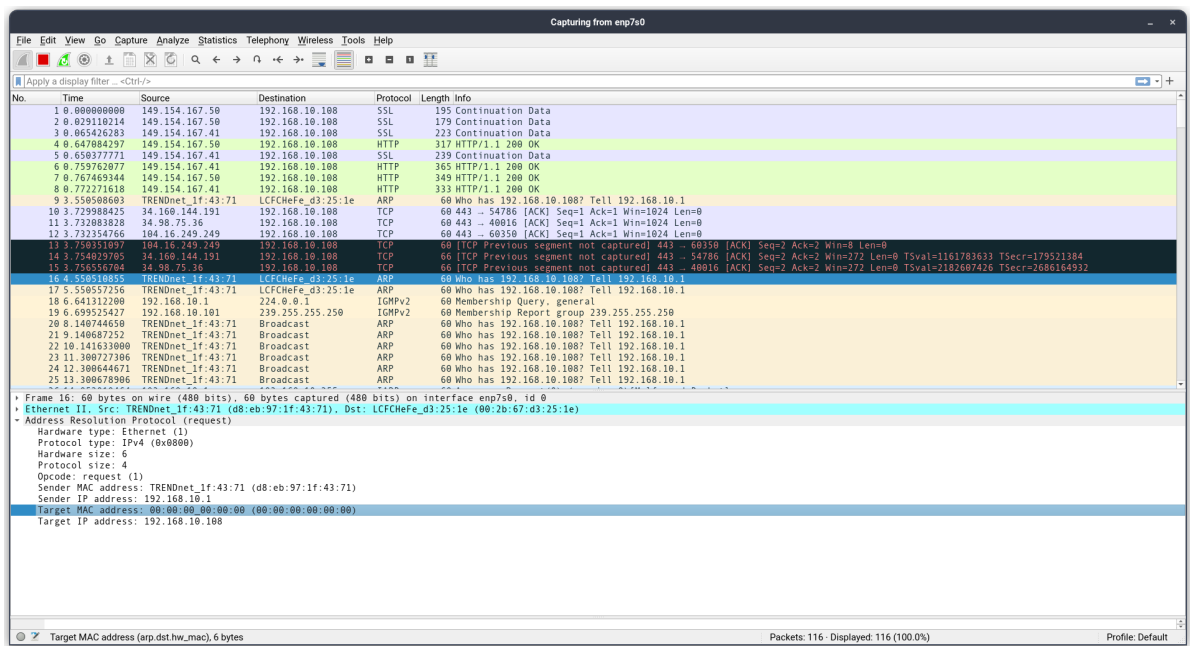
1. Від'єднання від мережі

Від мережі можна від'єднатись 2 способами - витягнути ethernet провід, або відключитись системно. Я використаю другий варіант



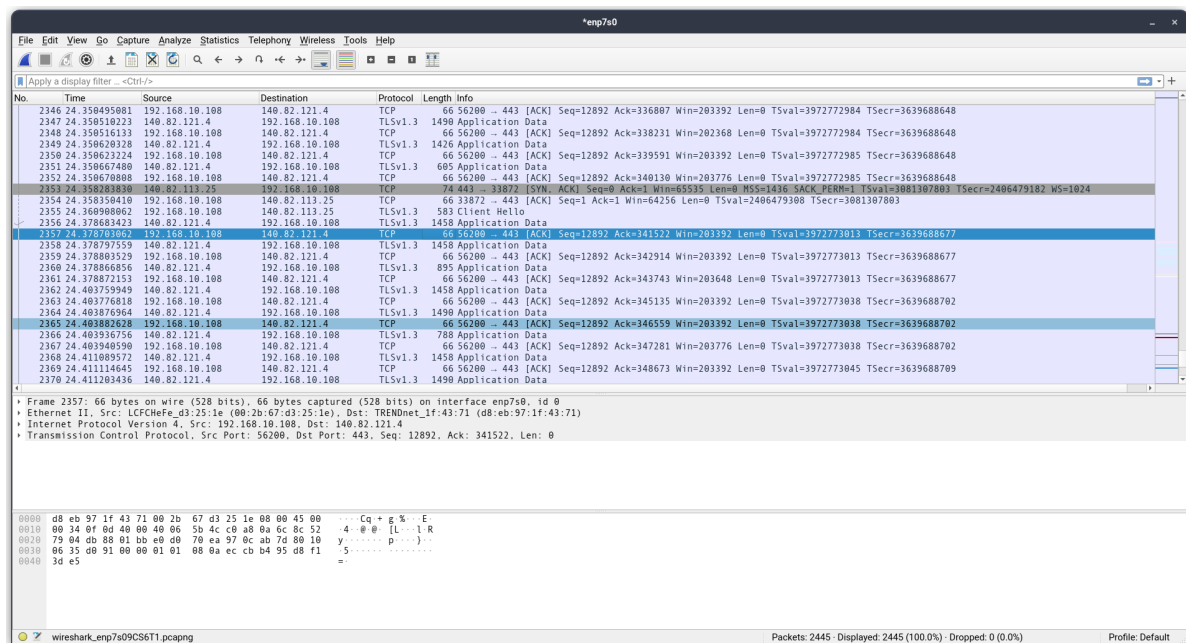
2. Запускаємо аналізатор з вимкнутим інтернетом

Такі пакети я перехоплював, коли мав відключений інтернет. Підозрюю, що це додатка "Teams" та "Telegram" перевіряли, чи є підключення



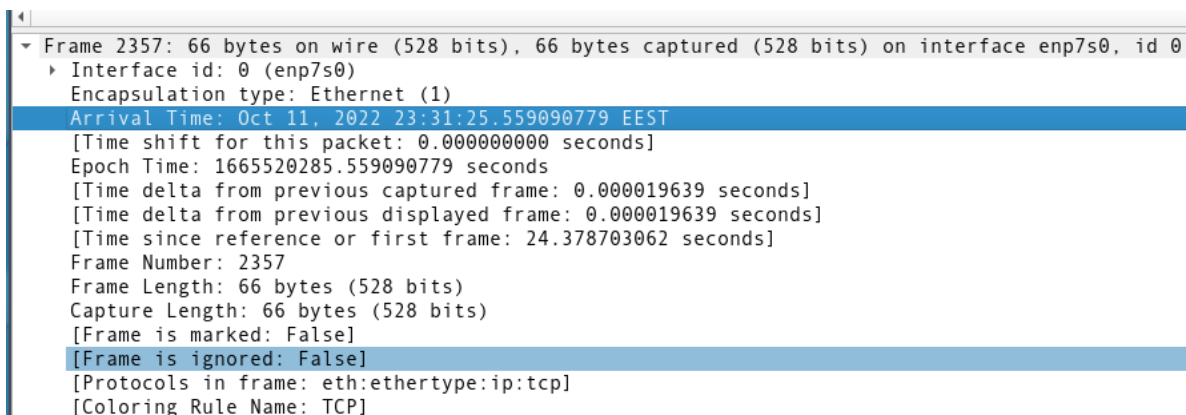
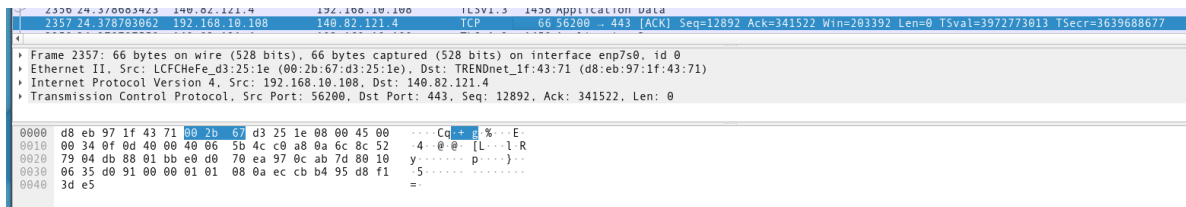
3. Підключаємось до інтернету

коли підключились до інтернету, перехоплено такі пакети:



4. Переглянемо інформацію про певний кадр

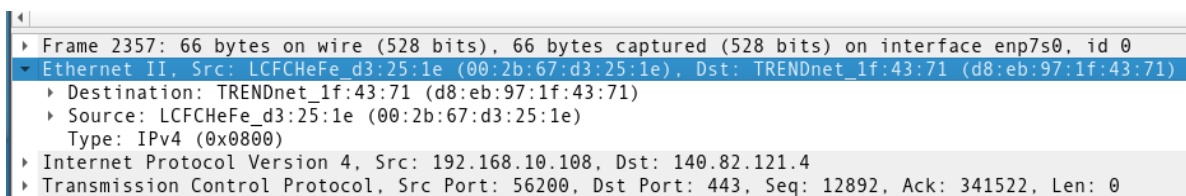
Оберемо певний кадр, та переглянемо інформацію про нього



Кадр №2357

- **розмір** - 66 байт(528 біт)
- **час захоплення** - 11.09.2022, 23:31:25 EEST
- **ієрархія протоколів**: Ethernet кадр -> ip пакет -> tcp

5. Переглянемо інформацію про заголовок кадру




- **розмір** - 14 байт

- Отримувач - маршрутизатор (MAC `d8:eb:97:1f:43:71`)
- Відправник - мережевий адаптер (MAC `00:2b:67:d3:25:1e`)
- Вкладений протокол - IPv4

6. Переглянемо інформацію про виробників

З допомогою сайту 2ip.ua (повне посилання до сервісу - <https://2ip.ua/ua/services/information-service/mac-find>), переглянемо інформацію про виробників

- дані про виробника мережевого адаптера:


 Визначення виробника по MAC-адресі

Введіть mac-адресу для перевірки


00:2b:67:d3:25:1e


ПЕРЕВІРИТИ

Виробником пристрою з mac-адресою 00:2b:67:d3:25:1e є компанія:

Ім'я компанії:	LCFC(HeFei) Electronics Technology co., ltd
Адреса компанії:	YunGu Road 3188-1 Hefei Anhui CN 230000
Унікальний ідентифікатор організації:	002B67
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

- дані про виробника маршрутизатора

Визначення виробника по MAC-адресі

Введіть тас-адресу для перевірки

d8:eb:97:1f:43:71

ПЕРЕВІРИТИ

Виробником пристрою з тас-адресою d8:eb:97:1f:43:71 є компанія:

Ім'я компанії:	TRENDnet, Inc.
Адреса компанії:	20675 Manhattan Place Torrance CA US 90501
Унікальний ідентифікатор організації:	D8EB97
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

7. ARP пакет

Зараз, пофільтруємо наші пакети за протоколом ARP, та переглянемо декілька з них.

The screenshot displays a Wireshark capture of network traffic on interface enp7s0. The packet list shows a series of ARP requests from source TRENDnet_1f:43:71 to destination Broadcast. The packet details pane shows the structure of an ARP request packet, including Ethernet II, Internet Protocol Version 4, and Address Resolution Protocol (request) fields. The packet bytes pane shows the raw data of the packet.

Packet 21: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp7s0, id 0

Ethernet II, Src: TRENDnet_1f:43:71 (d8:eb:97:1f:43:71), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

Source: TRENDnet_1f:43:71 (d8:eb:97:1f:43:71)

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: TRENDnet_1f:43:71 (d8:eb:97:1f:43:71)

Sender IP address: 192.168.10.1

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.10.107

В деяких є поля Padding, з 18 байтами нульової інформації. Все тому, що я використовую підключення через ethernet. padding - це додаткові байти(зазвичай нульові), які доповнюють пакет, щоб він досяг розміру 64 байти.

8. Чому у захопленому кадрі немає кінцевика

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows the ARP table for interface 'enp7s0', listing 30 entries with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 14), identifying it as an Ethernet II frame with source TRENDnet_1f:43:71 and destination Broadcast (ff:ff:ff:ff:ff:ff). The bottom pane shows the packet bytes (34) and the details of the Ethernet II frame, including the source and destination MAC addresses and the IP address 192.168.10.1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
1	0.000131337	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
1	1.200430453	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
2	1.110190888	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
2	2.270235819	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
3	3.110321769	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
3	3.270320411	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
10	4.110390156	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
11	5.220379149	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
12	6.060310091	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
13	6.220452499	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
14	7.060701494	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
15	7.220501861	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
16	8.060676831	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
17	8.330662870	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
18	9.331601030	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
21	10.330650577	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
23	10.881546590	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
24	11.440708081	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
26	11.880830192	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
27	12.440827473	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
28	13.080891835	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
29	13.440907156	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
31	14.550993875	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1
30	15.000000000	TRENDnet_1f:43:71	Broadcast	ARP	60	Who has 192.168.10.10? Tell 192.168.10.1

Frame 14: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp7s0, id 0

- Ethernet II, Src: TRENDnet_1f:43:71 (d8:eb:97:1f:43:71), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: TRENDnet_1f:43:71 (d8:eb:97:1f:43:71)
 - Type: ARP (0x0806)
 - Trailer: ffee00000000000040000005001400030000
- Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: request (1)
 - Sender MAC address: TRENDnet_1f:43:71 (d8:eb:97:1f:43:71)
 - Sender IP address: 192.168.10.1
 - Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
 - Target IP address: 192.168.10.100

Source or Destination Hardware Address (eth.addr), 6 bytes

Packets: 2445 · Displayed: 42 (1.7%) · Dropped: 0 (0.0%)

Profile: Default