НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
“ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ”
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

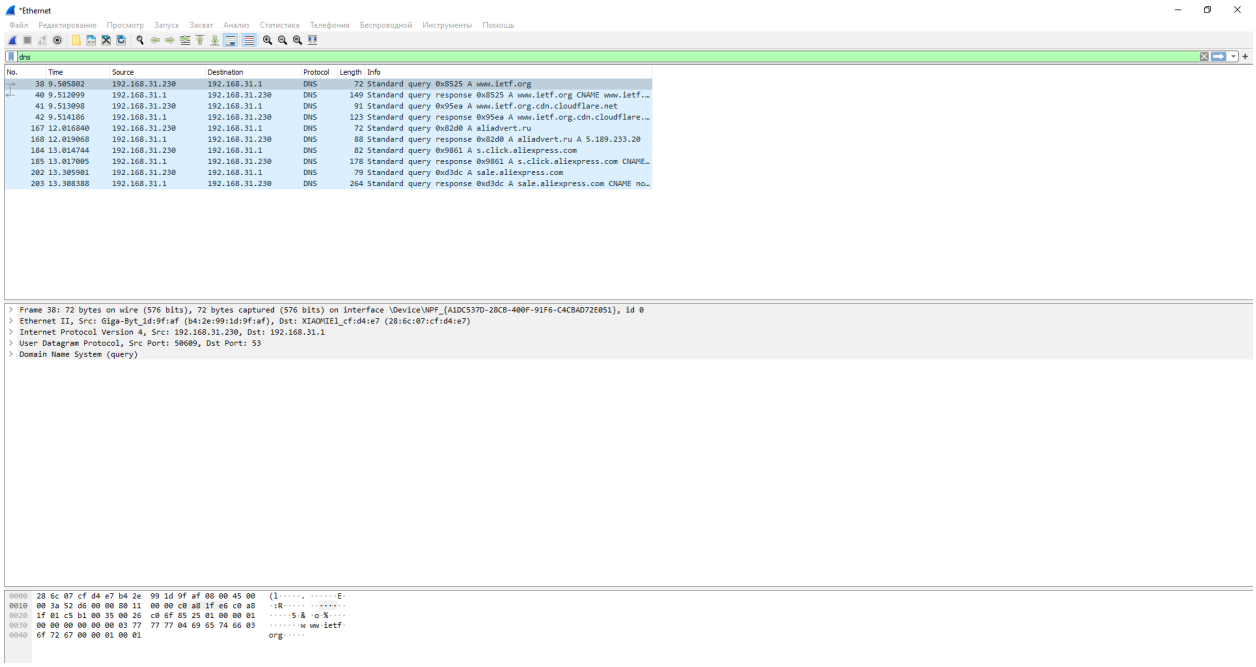
Лабораторна робота №3

з дисципліни “Комп'ютерні мережі”

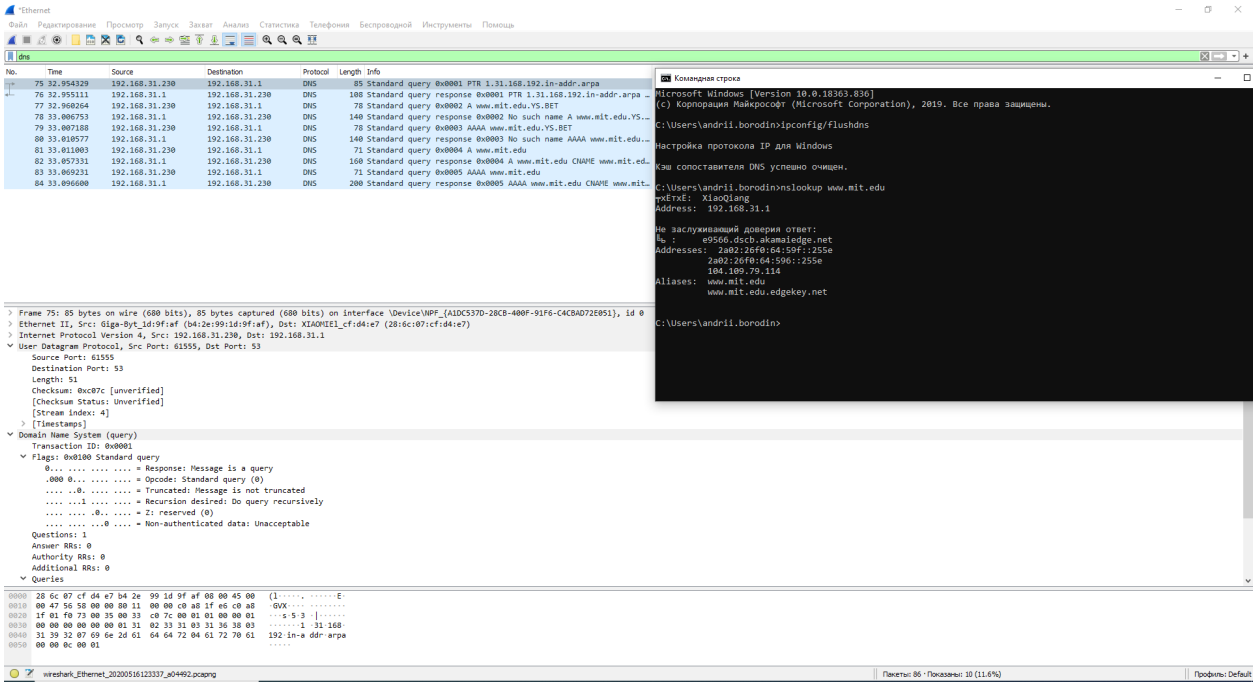
Виконав:
Студент групи ІС-зп92
Бородін А.А.
Перевірив:
Кухарєв С.О.

Київ – 2020

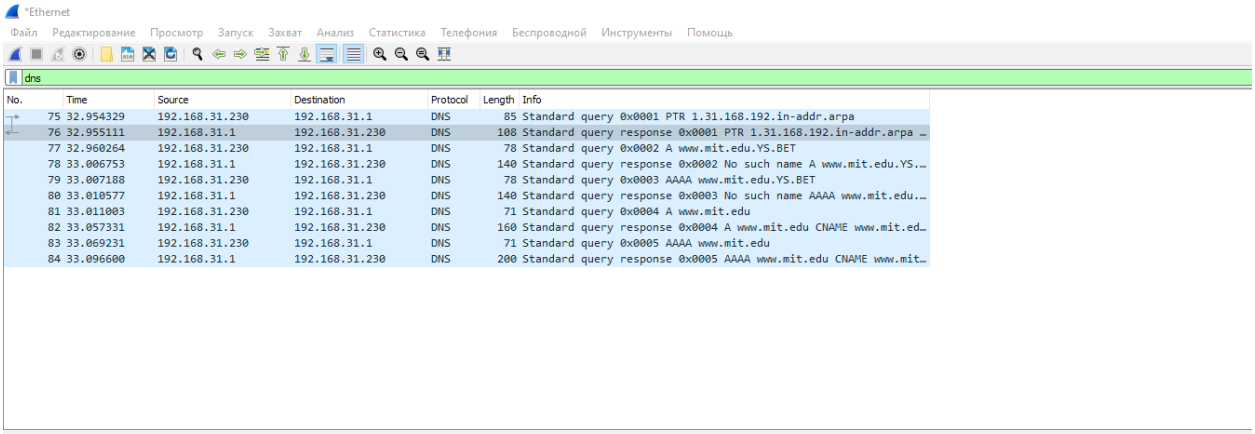
Перше захоплення пакетів



Друге захоплення пакетів

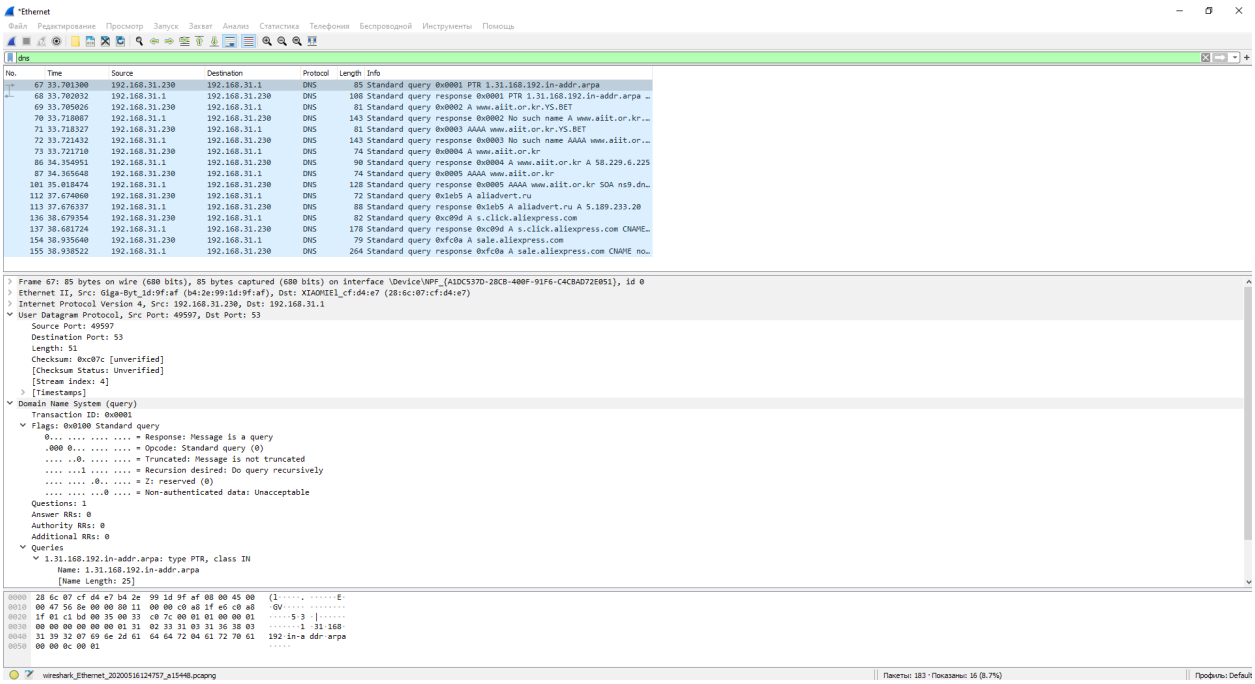


Третє захоплення пакетів




```
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    1.31.168.192.in-addr.arpa: type PTR, class IN
        Name: 1.31.168.192.in-addr.arpa
        [Name Length: 25]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
  Answers
    1.31.168.192.in-addr.arpa: type PTR, class IN, XiaoQiang
        Name: 1.31.168.192.in-addr.arpa
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
        Time to live: 0 (0 seconds)
        Data length: 11
        Domain Name: XiaoQiang
    [Request In: 75]
    [Time: 0.000782000 seconds]
```

Четверте захоплення пакетів




```
> Frame 67: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{A1DC537D-28CB-400F-91F6-C4CBAD72E051}, id 0
> Ethernet II, Src: Giga-Byt_1d:9f:af (b4:2e:99:1d:9f:af), Dst: XIAOMIEl_cf:d4:e7 (28:6c:07:cf:d4:e7)
> Internet Protocol Version 4, Src: 192.168.31.230, Dst: 192.168.31.1
v User Datagram Protocol, Src Port: 49597, Dst Port: 53
    Source Port: 49597
    Destination Port: 53
    Length: 51
    Checksum: 0xc07c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
v Domain Name System (query)
    Transaction ID: 0x0001
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 1.31.168.192.in-addr.arpa: type PTR, class IN
        Name: 1.31.168.192.in-addr.arpa
        [Name Length: 25]
```

```
0000  28 6c 07 cf d4 e7 b4 2e  99 1d 9f af 08 00 45 00   (l·····. ·····E·
0010  00 47 56 8e 00 00 80 11  00 00 c0 a8 1f e6 c0 a8   ·GV····· ········
0020  1f 01 c1 bd 00 35 00 33  c0 7c 00 01 01 00 00 01   ·····5·3 ·|······
0030  00 00 00 00 00 00 01 31  02 33 31 03 31 36 38 03   ·······1 ·31·168·
0040  31 39 32 07 69 6e 2d 61  64 64 72 04 61 72 70 61   192·in-a ddr·arpa
0050  00 00 0c 00 01                                     ·····
```

Контрольні запитання:

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

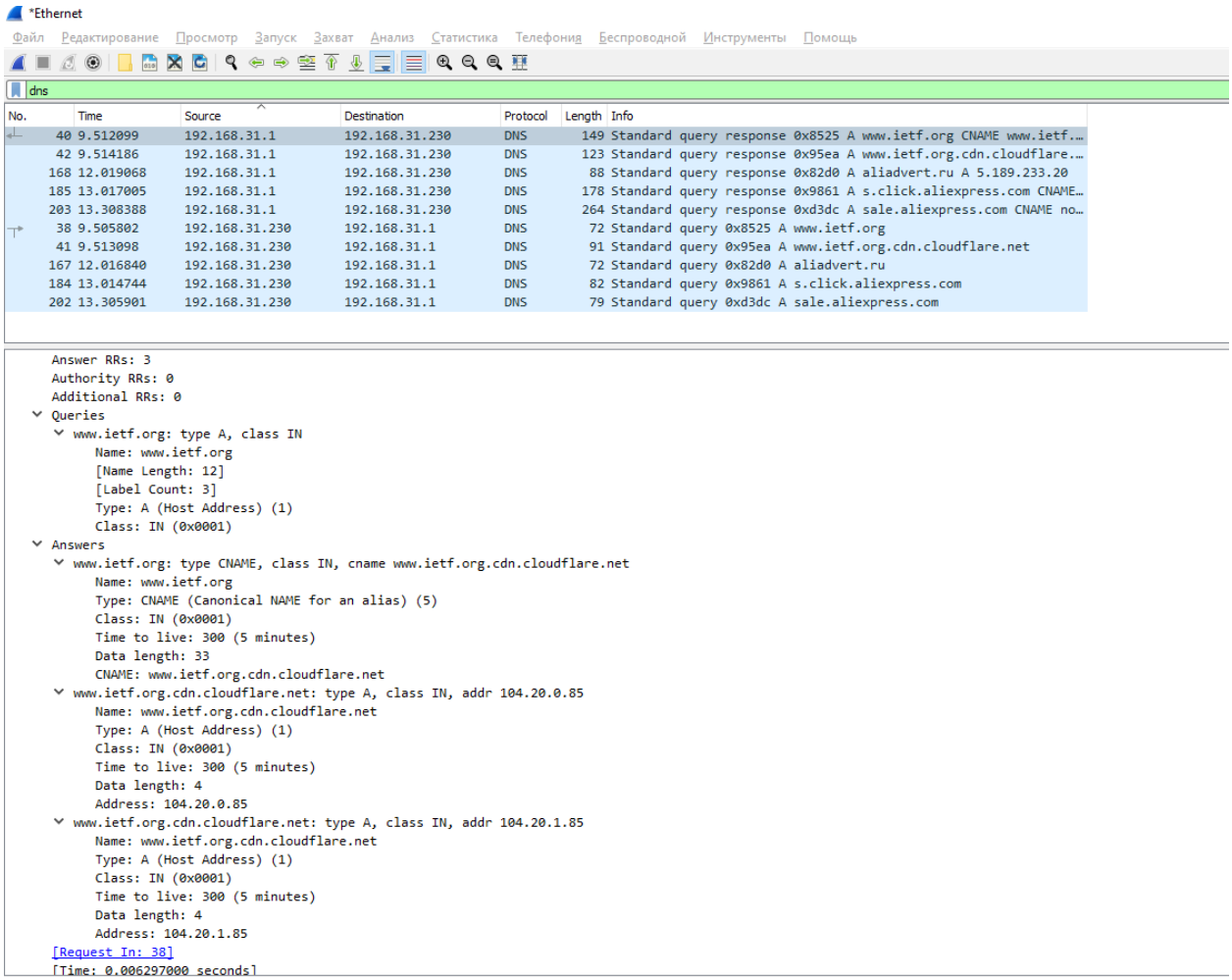
Запит UDP, відповідь UDP, номер вихідного порта відповіді DNS: 53

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?

192.168.31.1 Так, це адреса локального сервера DNS

3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Так вміщує



4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

Кількість відповідей — 3, відповіді вміщують: Name, Type, Class, Timi to live, Data Length, CNAME, Adress

5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

Так співпадає

6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?

Так виконує

7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

цільовий порт повідомлення — 53

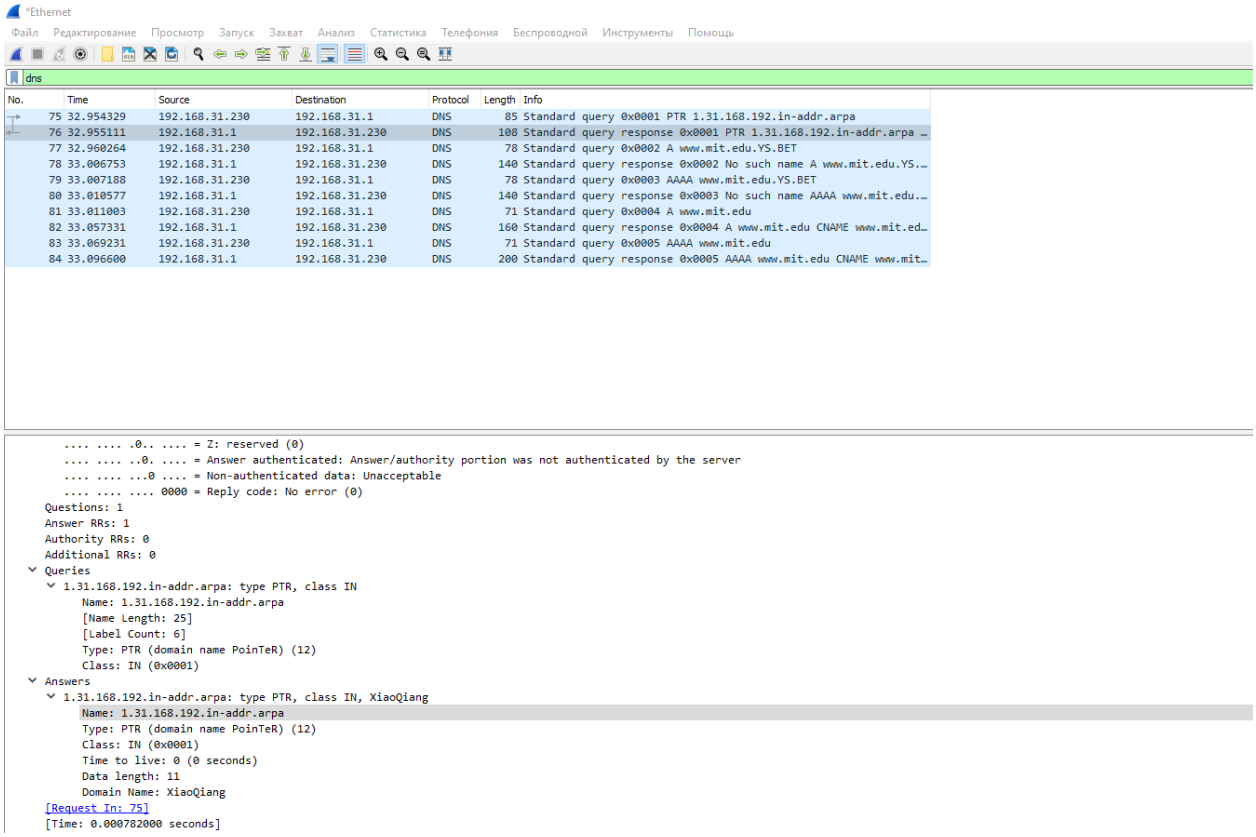
вихідний порт повідомлення — 61555

8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

192.168.31.1

9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Так вміщує



10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?

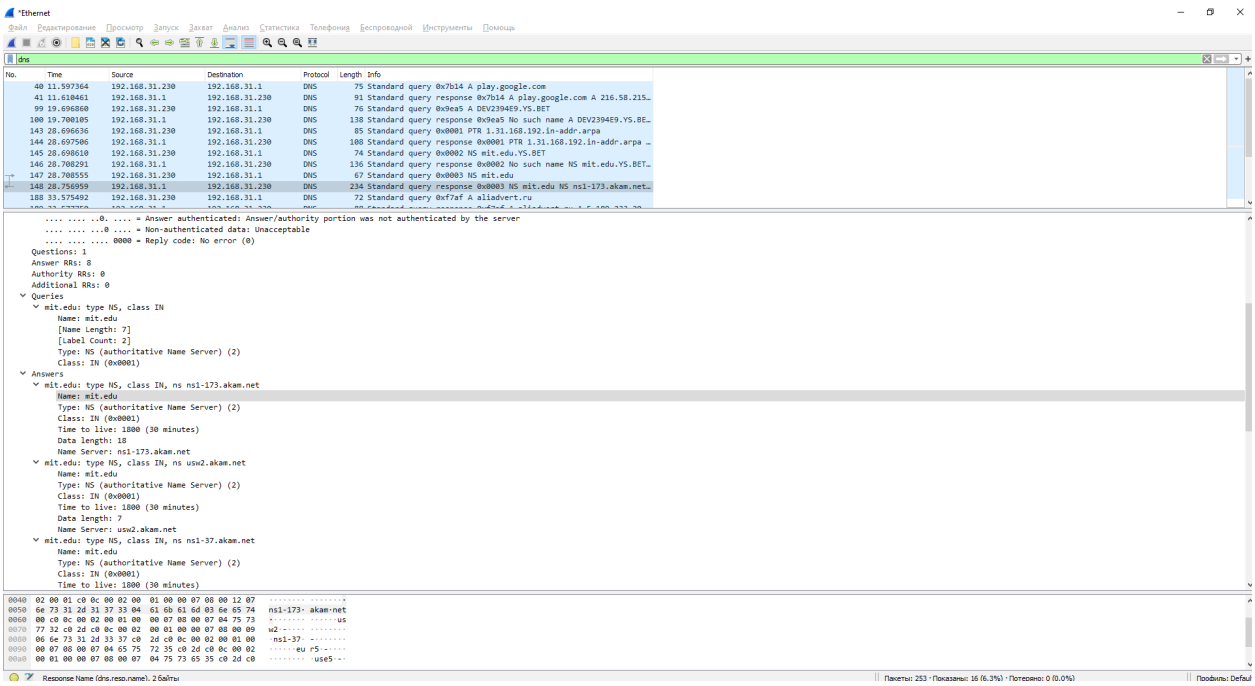
Один запис з відповіддю, складається з: Name, Type, Class, Time to live, Data length, Domain name

11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

192.168.31.1 Так ця адреса є адресою локального сервера DNS за замовчанням

12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Так вміщує



13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

Вісім записів з відповідями, сервери були запропоновані за допомогою доменного імені

14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

192.168.31.230, Ні, це одна з адрес локального середовища

15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Так вміщує, Name, Type, Class

16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?

8 відповідей складається з Name, Type, Class, Time to live, Data length, Domain name