МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС

«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»

НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Завдання лабораторної роботи №3

З дисципліни «Комп'ютерні мережі»

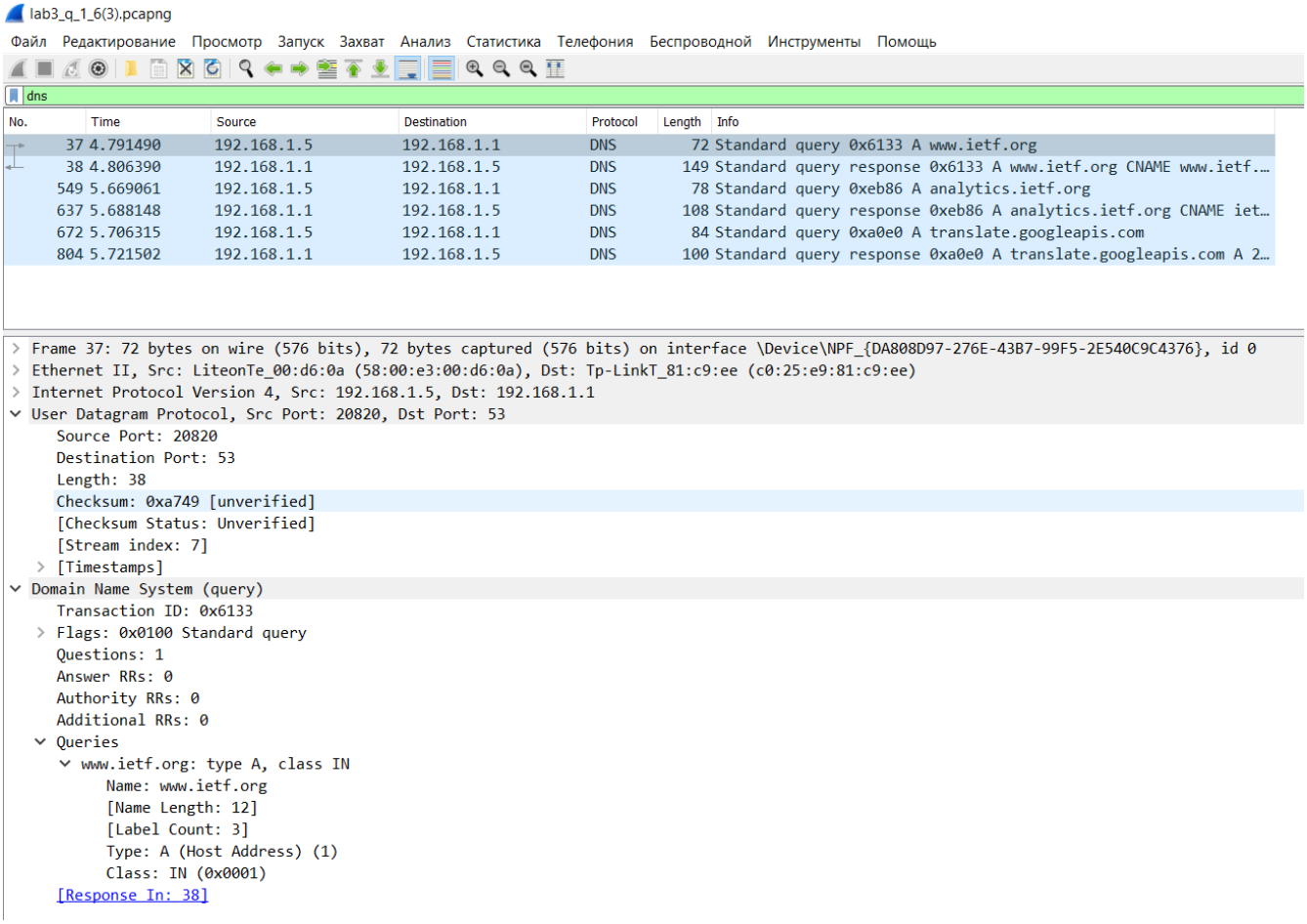
Виконав: студент 3-го курсу

гр. КА-71

Возняк В. З.

Прийняв: Кухарєв С.О.

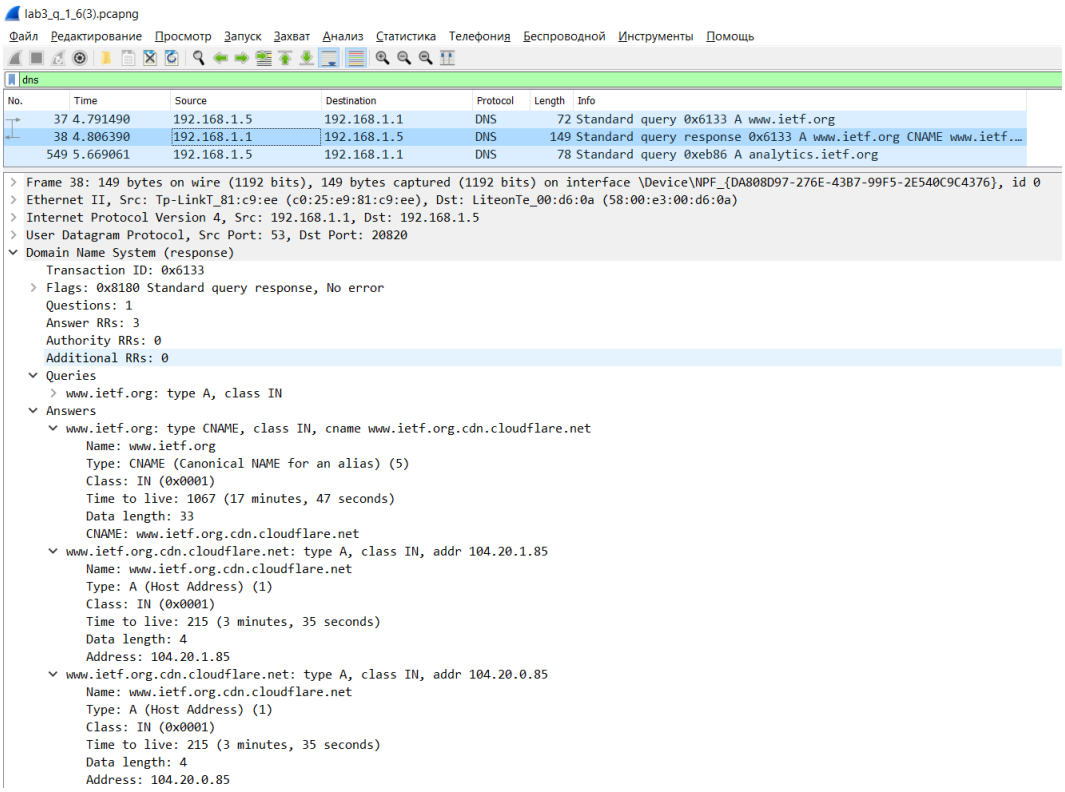
Київ 2020



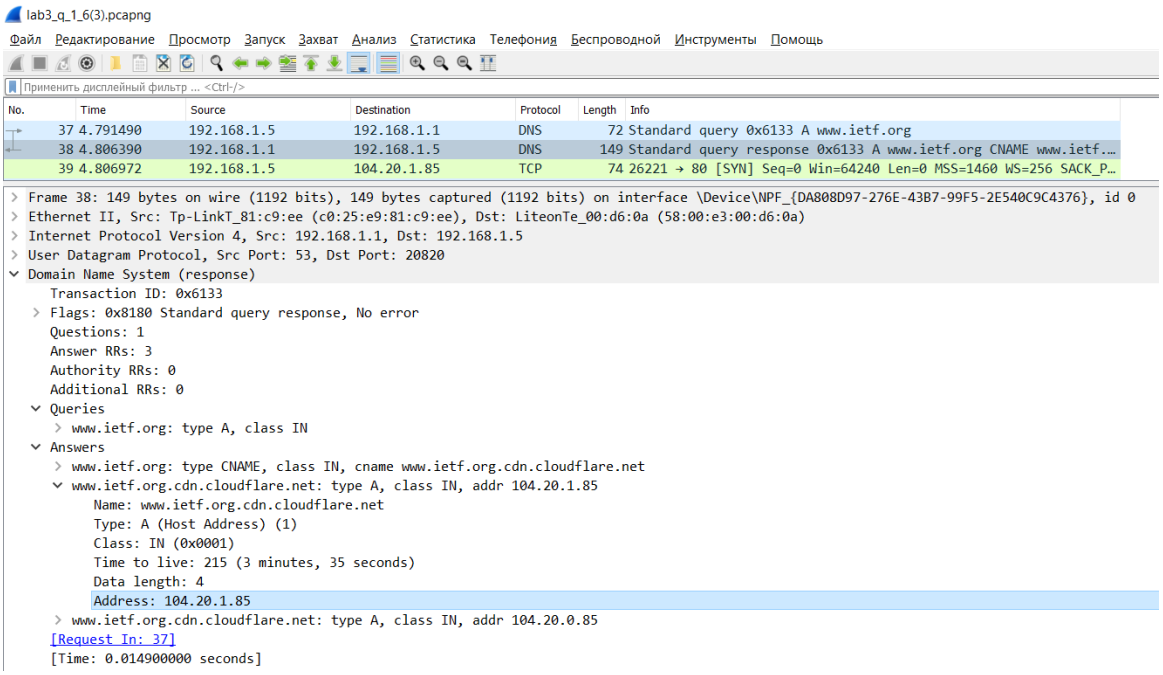
ВІДПОВІДІ НА ПИТАННЯ 1-6

1) Використовується UDP. Крім того, використання UDP прямо зазначалося в книжці Таненбаума, яка доступна на Гугл Диску: «Запрос и ответ передаются как UDP-пакеты». (Request) Dst Port: 53. (Response) Dst Port: 20820.
2) Destination IP: 192.168.1.1. Взагалі, спочатку браузер перевіряє локально на комп’ютері файл hosts.txt, і якщо там не знаходиться необхідної адреси, то направляється до локального DNS-серверу. Оскільки в нас очищений кеш, то браузер направляється до локального DNS-серверу, тому так, це і є його IP.
3) Запит Типу A (Адресний запис, встановлює відповідність між іменем і IP-адресою). Під «компонентами відповіді» я розумію адресу сайту, який запитується - ietf.org, тобто який сайт ми хочемо отримати.
4) Усього було 6 запитів-відповідей. Відповіді містять ім’я домену, час життя (в сек), тип запису, клас (IN якщо отримано через Інтернет), і саме значення

адреси. Причому 2-ий та 3-ій запити ідуть на якісь ресурси, пов’язані з аналітикою та перекладом відповідно. Розглянемо перший. Це власне запити на пошук нашого сайту www.ietf.org.



5) Так, співпадає. На скріні наведено мишкою на цільову адресу і виділено її в деталях DNS запиту:



6) Так, виконала ще два запити, як зазначалося в п.4 (отримує ресурси для аналітики та перекладу сайту).

Domain Name System (1st query)

```
    Transaction ID: 0x6133
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ietf.org: type A, class IN
            Name: www.ietf.org
            [Name Length: 12]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    [Response In: 38]
```

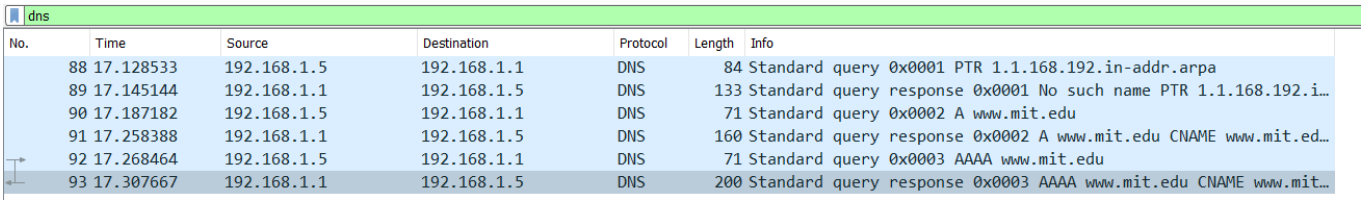
Domain Name System (1st response)

```
    Transaction ID: 0x6133
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ietf.org: type A, class IN
            Name: www.ietf.org
            [Name Length: 12]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    Answers
        www.ietf.org: type CNAME, class IN, cname
www.ietf.org.cdn.cloudflare.net
            Name: www.ietf.org
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 1067 (17 minutes, 47 seconds)
            Data length: 33
            CNAME: www.ietf.org.cdn.cloudflare.net
        www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
            Name: www.ietf.org.cdn.cloudflare.net
```

```
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 215 (3 minutes, 35 seconds)
        Data length: 4
        Address: 104.20.1.85
    www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
        Name: www.ietf.org.cdn.cloudflare.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 215 (3 minutes, 35 seconds)
        Data length: 4
        Address: 104.20.0.85
[Request In: 37]
[Time: 0.014900000 seconds]
```

ВІДПОВІДІ НА ПИТАННЯ 7-10

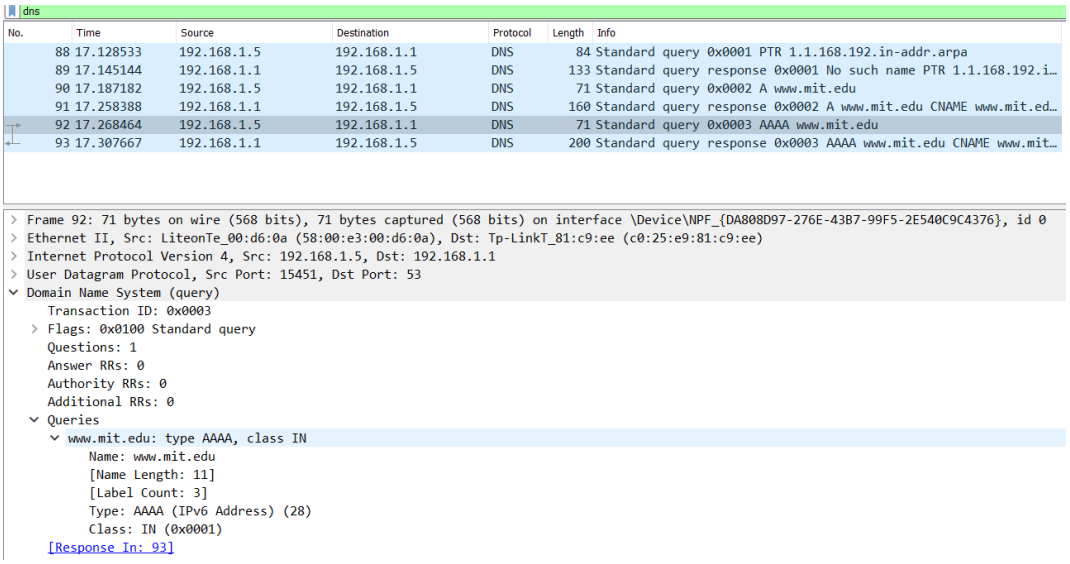
7) Цільовий порт запиту відповідав вихідному порту з відповіддю – Port: 53.
8) Мій локальний DNS сервер 192.168.1.1. Як бачимо запити відбувалися саме на цю адресу:



dns

No.	Time	Source	Destination	Protocol	Length	Info
88	17.128533	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
89	17.145144	192.168.1.1	192.168.1.5	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.i…
90	17.187182	192.168.1.5	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
91	17.258388	192.168.1.1	192.168.1.5	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.ed…
92	17.268464	192.168.1.5	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
93	17.307667	192.168.1.1	192.168.1.5	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit…

9) Цей запит мав тип AAAA (запис AAAA містить 128 розрядну IPv6-адресу).



dns

No.	Time	Source	Destination	Protocol	Length	Info
88	17.128533	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
89	17.145144	192.168.1.1	192.168.1.5	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.i…
90	17.187182	192.168.1.5	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
91	17.258388	192.168.1.1	192.168.1.5	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.ed…
92	17.268464	192.168.1.5	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
93	17.307667	192.168.1.1	192.168.1.5	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit…

```
> Frame 92: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{DA808D97-276E-43B7-99F5-2E540C9C4376}, id 0
> Ethernet II, Src: LiteonTe_00:d6:0a (58:00:e3:00:d6:0a), Dst: Tp-LinkT_81:c9:ee (c0:25:e9:81:c9:ee)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 15451, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type AAAA, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
    [Response In: 93]
```

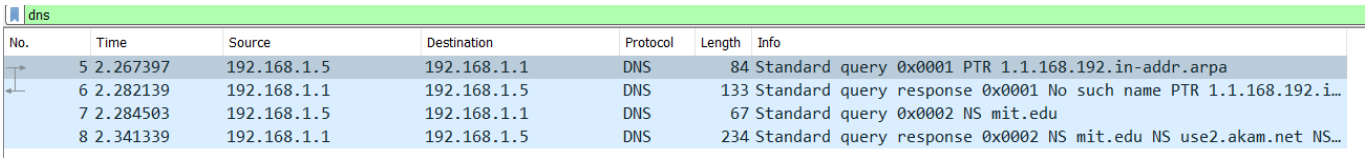
10) Всього містилося 3 відповіді (на 3 запити). Але оскільки вказано, що потрібно розглядати лише 3-ю, то наведемо її опис. Цей респонс містив в собі 4 відповіді, 2 типу CNAME, 2 – AAAA. Як уже зазначалося CNAME допомагає створити псевдоніми для адресу сторінки. Тоді, ввівши різні псевдоніми, ми все одно потрапляємо на одну і ту ж сторінку (це необхідно для зручності в деяких випадках).

Domain Name System (response)

```
    Transaction ID: 0x0003
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.mit.edu: type AAAA, class IN
            Name: www.mit.edu
            [Name Length: 11]
            [Label Count: 3]
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
    Answers
        www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
            Name: www.mit.edu
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 737 (12 minutes, 17 seconds)
            Data length: 25
            CNAME: www.mit.edu.edgekey.net
        www.mit.edu.edgekey.net: type CNAME, class IN, cname
e9566.dscb.akamaiedge.net
            Name: www.mit.edu.edgekey.net
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 60 (1 minute)
            Data length: 24
            CNAME: e9566.dscb.akamaiedge.net
        e9566.dscb.akamaiedge.net: type AAAA, class IN, addr
2a02:26f0:10e:1a2::255e
            Name: e9566.dscb.akamaiedge.net
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
            Time to live: 20 (20 seconds)
```

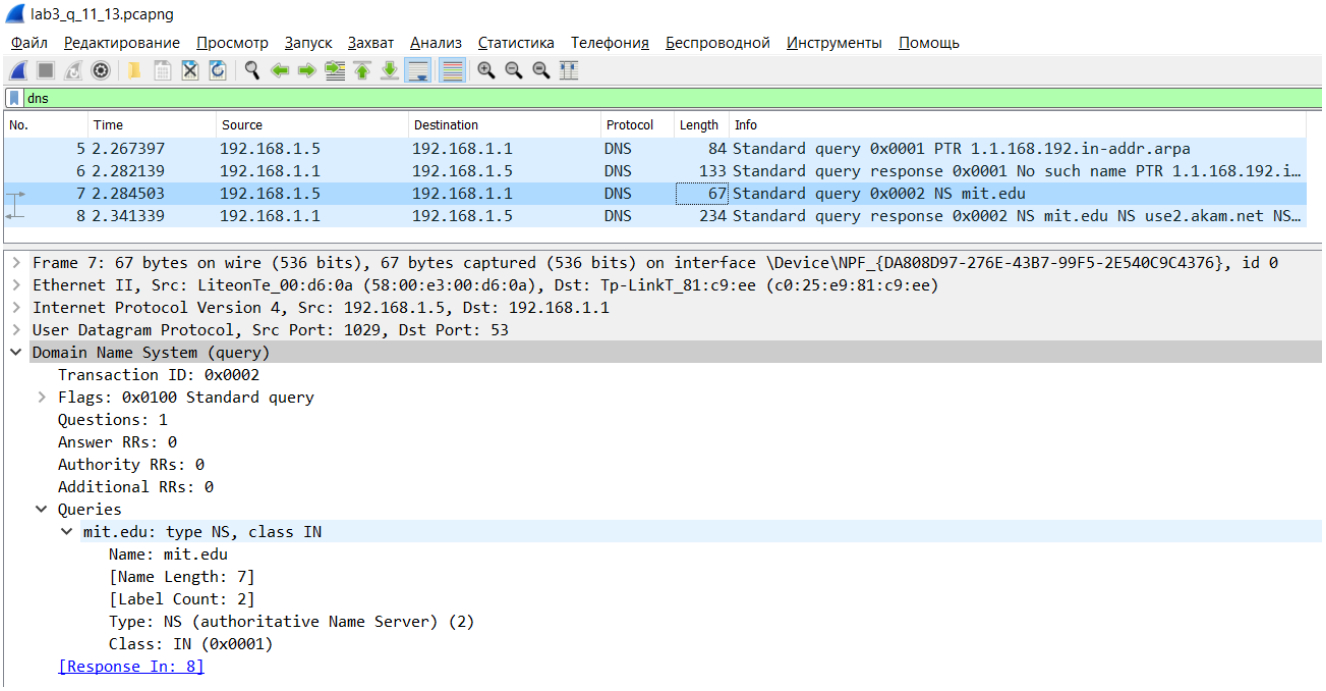
```
            Data length: 16
            AAAA Address: 2a02:26f0:10e:1a2::255e
        e9566.dscb.akamaiedge.net: type AAAA, class IN, addr
2a02:26f0:10e:197::255e
            Name: e9566.dscb.akamaiedge.net
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
            Time to live: 20 (20 seconds)
            Data length: 16
            AAAA Address: 2a02:26f0:10e:197::255e
    [Request In: 92]
    [Time: 0.039203000 seconds]
```

ВІДПОВІДІ НА ПИТАННЯ 11-13



No.	Time	Source	Destination	Protocol	Length	Info
5	2.267397	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
6	2.282139	192.168.1.1	192.168.1.5	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.i…
7	2.284503	192.168.1.5	192.168.1.1	DNS	67	Standard query 0x0002 NS mit.edu
8	2.341339	192.168.1.1	192.168.1.5	DNS	234	Standard query response 0x0002 NS mit.edu NS use2.akam.net NS…

11) Мій локальний DNS сервер 192.168.1.1. Як бачимо запити знову відбувалися саме на цю адресу.
12) Типу NS. Запис цього типу містить інформацію про сервер імені для нашого домену або субдомену.



lab3_q_11_13.pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

No.	Time	Source	Destination	Protocol	Length	Info
5	2.267397	192.168.1.5	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
6	2.282139	192.168.1.1	192.168.1.5	DNS	133	Standard query response 0x0001 No such name PTR 1.1.168.192.i…
7	2.284503	192.168.1.5	192.168.1.1	DNS	67	Standard query 0x0002 NS mit.edu
8	2.341339	192.168.1.1	192.168.1.5	DNS	234	Standard query response 0x0002 NS mit.edu NS use2.akam.net NS…

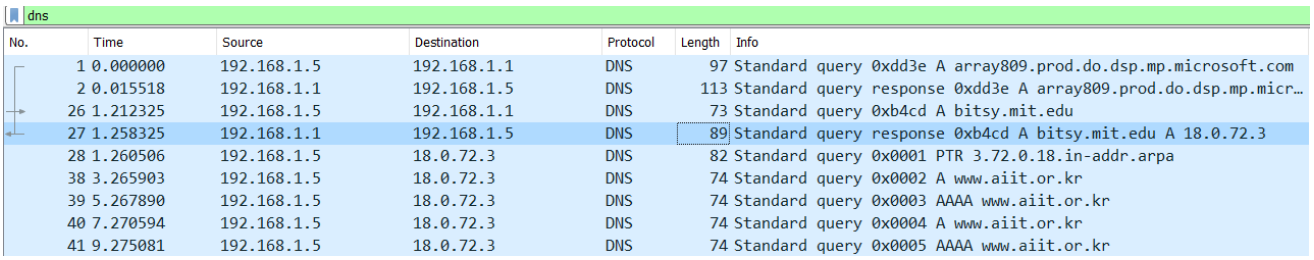
```
> Frame 7: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{DA808D97-276E-43B7-99F5-2E540C9C4376}, id 0
> Ethernet II, Src: LiteonTe_00:d6:0a (58:00:e3:00:d6:0a), Dst: Tp-LinkT_81:c9:ee (c0:25:e9:81:c9:ee)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 1029, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 8]
```

13) Містилося 8 відповідей і всі вони були запропоновані за допомогою доменного імені:

```
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
    Queries
        mit.edu: type NS, class IN
            Name: mit.edu
            [Name Length: 7]
            [Label Count: 2]
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
    Answers
        mit.edu: type NS, class IN, ns use2.akam.net
            Name: mit.edu
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 1800 (30 minutes)
            Data length: 15
            Name Server: use2.akam.net
        mit.edu: type NS, class IN, ns usw2.akam.net
            Name: mit.edu
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 1800 (30 minutes)
            Data length: 7
            Name Server: usw2.akam.net
        mit.edu: type NS, class IN, ns use5.akam.net
            Name: mit.edu
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 1800 (30 minutes)
            Data length: 7
            Name Server: use5.akam.net
        mit.edu: type NS, class IN, ns asia2.akam.net
            Name: mit.edu
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
            Time to live: 1800 (30 minutes)
```

```
        Data length: 8
        Name Server: asia2.akam.net
    mit.edu: type NS, class IN, ns eur5.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 7
        Name Server: eur5.akam.net
    mit.edu: type NS, class IN, ns ns1-173.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 10
        Name Server: ns1-173.akam.net
    mit.edu: type NS, class IN, ns ns1-37.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 9
        Name Server: ns1-37.akam.net
    mit.edu: type NS, class IN, ns asia1.akam.net
        Name: mit.edu
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 1800 (30 minutes)
        Data length: 8
        Name Server: asia1.akam.net
[Request In: 7]
[Time: 0.056836000 seconds]
```

ВІДПОВІДІ НА ПИТАННЯ 14-16



dns

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.5	192.168.1.1	DNS	97	Standard query 0xdd3e A array809.prod.do.dsp.mp.microsoft.com
2	0.015518	192.168.1.1	192.168.1.5	DNS	113	Standard query response 0xdd3e A array809.prod.do.dsp.mp.micr…
26	1.212325	192.168.1.5	192.168.1.1	DNS	73	Standard query 0xb4cd A bitsy.mit.edu
27	1.258325	192.168.1.1	192.168.1.5	DNS	89	Standard query response 0xb4cd A bitsy.mit.edu A 18.0.72.3
28	1.260506	192.168.1.5	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
38	3.265903	192.168.1.5	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
39	5.267890	192.168.1.5	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
40	7.270594	192.168.1.5	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
41	9.275081	192.168.1.5	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

14) Як бачимо для mit виконався запит на мій локальний сервер ДНС. Ось відповідь на цей запит:

```
Domain Name System (response)
    Transaction ID: 0xb4cd
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        bitsy.mit.edu: type A, class IN
            Name: bitsy.mit.edu
            [Name Length: 13]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    Answers
        bitsy.mit.edu: type A, class IN, addr 18.0.72.3
            Name: bitsy.mit.edu
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 1800 (30 minutes)
            Data length: 4
            Address: 18.0.72.3
    [Request In: 26]
    [Time: 0.046000000 seconds]
```

У відповідь отримали IP-адресу для bitsy.mit.edu. Тому наступні запити з IP 18.0.72.3 виконувалися саме на цей домен.

15) Для MIT виконався запит A, для aiit – виконалося кілька запитів PTR, A, AAAA. Але жоден запит не був успішним (я думаю саме із-за цього виконувалися запити різних типів, для того щоб спробувати отримати успішний запит).

```
C:\Users\admin>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
╥xËтxË:  UnKnown
Address:  18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Превышено время ожидания запроса UnKnown
```

16) Було отримано лише одну відповідь DNS з одним записом, яку наведено у пункті 14. Відповідь стандартна, містить ті ж дані, що і в розглянутих нами раніше запитах типу A.