

**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**

**Гікал А.О.**

**Прийняв: Кухарєв С.О.**

**Київ 2020**

1.pcapng

Файл

Редактирование

Просмотр

Запуск

Захват

Анализ

Статистика

Телефония

Беспроводной

Инструменты

Помощь

dns

+

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.88.203	192.168.88.1	DNS	83	Standard query 0xa2c2 A safebrowsing.google.com
2	0.002983	192.168.88.203	192.168.88.1	DNS	72	Standard query 0x4d79 A www.ietf.org
3	0.005881	192.168.88.1	192.168.88.203	DNS	302	Standard query response 0xa2c2 A safebrowsing.google.com
5	0.017795	192.168.88.1	192.168.88.203	DNS	389	Standard query response 0x4d79 A www.ietf.org CNAME www.

> Internet Protocol Version 4, Src: 192.168.88.203, Dst: 192.168.88.1

> User Datagram Protocol, Src Port: 1025, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0xa2c2

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

> safebrowsing.google.com: type A, class IN

Name: safebrowsing.google.com

[Name Length: 23]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 3]

0020 58 01 04 01 00 35 00 31 df d4 a2 c2 01 00 00 01 X...5:1 .....

0030 00 00 00 00 00 00 0c 73 61 66 65 62 72 6f 77 73 .....s afebrows

0040 69 6e 67 06 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 ing-goog le.com..

The response to this DNS query is in this frame (dns.response\_in)

Пакеты: 1305 · Показаны: 4 (0.3%) · Потеряно: 0 (0.0%)

Профиль: Default

## ВІДПОВІДІ НА ПИТАННЯ 1-6

- 1) Використовується UDP. «Запрос и ответ передаются как UDP-пакеты». (Request) Dst Port: 53. (Response) Dst Port: 1025.
- 2) Destination IP: 192.168.88.1. Оскільки в нас очищений кеш, то браузер направляється до локального DNS-серверу, тому так, це і є його IP.
- 3) Запит Типу A
- 4) Усього було 2 запити-відповіді. Відповіді містять ім'я домену, час життя (в сек), тип запису, клас (IN якщо отримано через Інтернет), і саме значення адреси.
- 5) Так співпадає.
- 6) Так виконала ще один запит.

## ВІДПОВІДІ НА ПИТАННЯ 7-10

- 7) Цільовий порт запиту відповідав вихідному порту з відповіддю – Port: 53.
- 8) Мій локальний DNS сервер 192.168.88.1. Як бачимо запити відбувалися саме на цю адресу:

34	3.914997	192.168.88.203	192.168.88.1	DNS	85	Standard query 0x0001 PTR 1.88.168.192.in-addr.arpa
35	3.929968	192.168.88.1	192.168.88.203	DNS	364	Standard query response 0x0001 PTR 1.88.168.192.in-addr

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

- 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). Пояснення наявності кількох AAAA аналогічна п.4 для A.

#### Domain Name System (response 3)

##### Answers

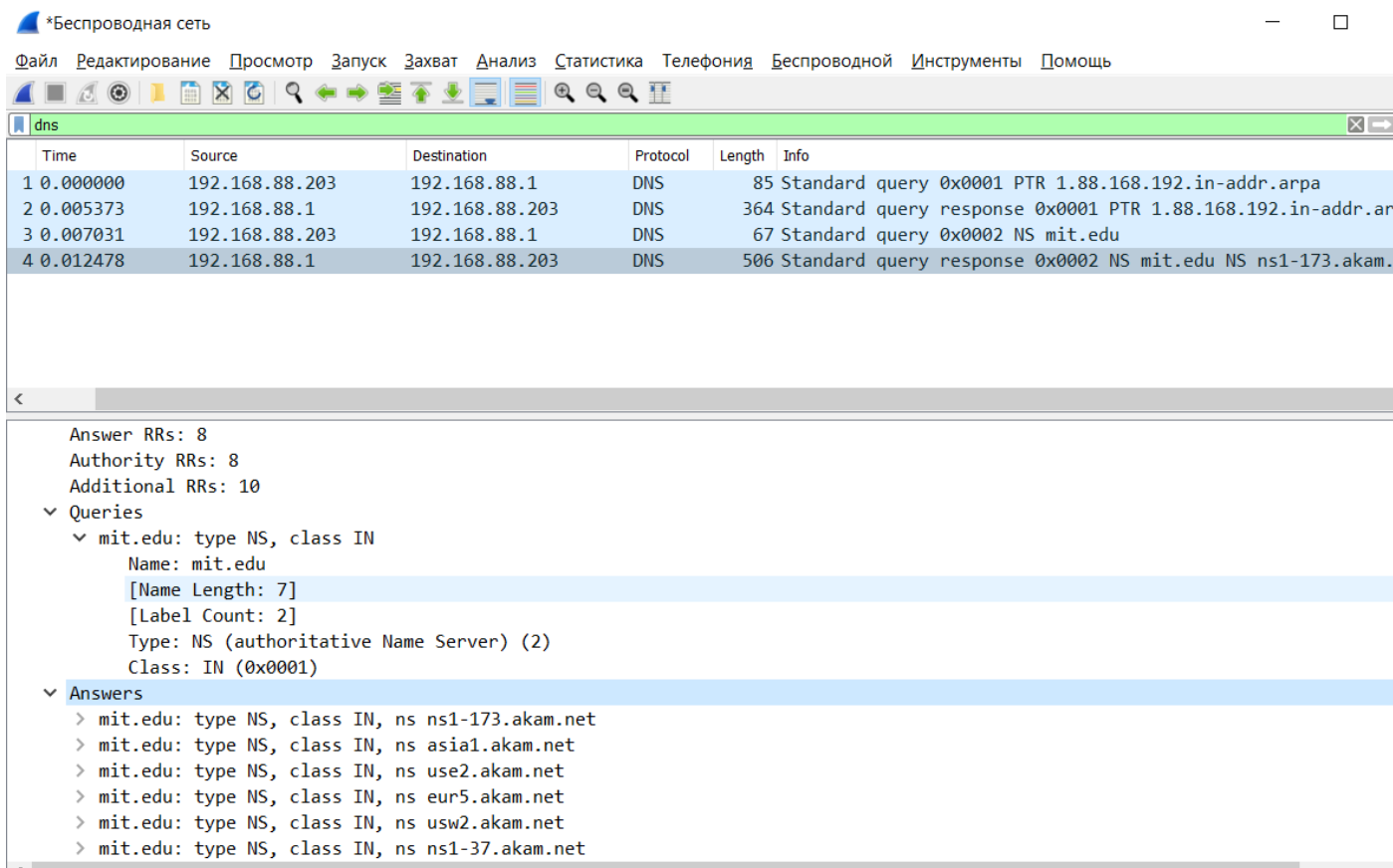
```
www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  Name: www.mit.edu
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 1741 (29 minutes, 1 second)
  Data length: 25
  CNAME: www.mit.edu.edgekey.net
www.mit.edu.edgekey.net: type CNAME, class IN, cname 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:d8:48f::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:d8:48f::255e
e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d8:490::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:d8:490::255e
```

## ВІДПОВІДІ НА ПИТАННЯ 11-13

Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.88.203	192.168.88.1	DNS	85	Standard query 0x0001 PTR 1.88.168.192.in-addr.arpa
2 0.005373	192.168.88.1	192.168.88.203	DNS	364	Standard query response 0x0001 PTR 1.88.168.192.in-addr.arpa ...
3 0.007031	192.168.88.203	192.168.88.1	DNS	67	Standard query 0x0002 NS mit.edu
4 0.012478	192.168.88.1	192.168.88.203	DNS	506	Standard query response 0x0002 NS mit.edu NS ns1-173.akam.net...

11) Мій локальний DNS сервер 192.168.88.1. 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.



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

### Domain Name System (response)

#### Answers

```

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: 1384 (23 minutes, 4 seconds)
Data length: 18
Name Server: ns1-173.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: 1384 (23 minutes, 4 seconds)
Data length: 8
Name Server: asia1.akam.net
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: 1384 (23 minutes, 4 seconds)  
Data length: 7  
Name Server: use2.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: 1384 (23 minutes, 4 seconds)  
Data length: 7  
Name Server: eur5.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: 1384 (23 minutes, 4 seconds)  
Data length: 7  
Name Server: usw2.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: 1384 (23 minutes, 4 seconds)  
Data length: 9  
Name Server: ns1-37.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: 1384 (23 minutes, 4 seconds)  
Data length: 8  
Name Server: asia2.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: 1384 (23 minutes, 4 seconds)  
Data length: 7  
Name Server: use5.akam.net

## ВІДПОВІДІ НА ПИТАННЯ 14-16

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.88.203	192.168.88.1	DNS	73	Standard query 0xaa6e A bitsy.mit.edu
2	0.009215	192.168.88.1	192.168.88.203	DNS	336	Standard query response 0xaa6e A bitsy.mit.edu A 18.0.72
3	0.011874	192.168.88.203	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
4	2.018726	192.168.88.203	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
5	4.019228	192.168.88.203	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
6	6.025042	192.168.88.203	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
7	8.024029	192.168.88.203	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

- 14) Спочатку на 192.168.88.1, а потім на 18.0.72.3
- 15) Типу А та типу PTR. Ні
- 16) Було отримано лише одну відповідь DNS з одним записом. Відповідь стандартна, містить ті ж дані, що і в розглянутих нами раніше запитах типу А.