

Завдання лабораторної роботи №3

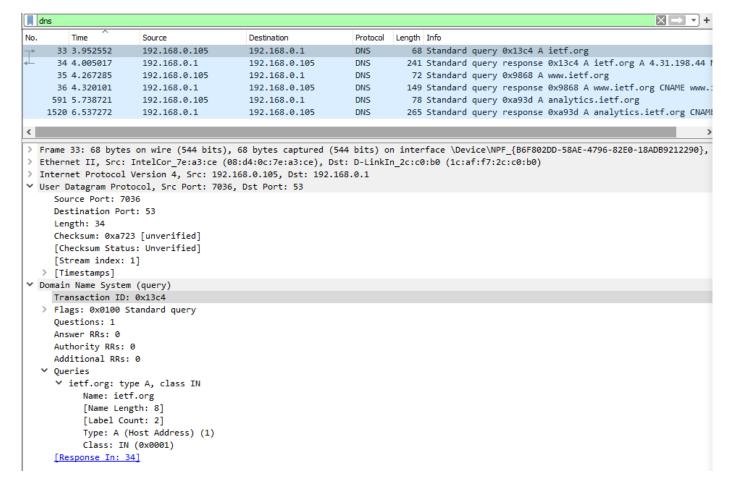
3 дисципліни «Комп'ютерні мережі»

Виконав: студент 3-го курсу

гр. КА-71

Островський З.Ю.

Прийняв: Кухарєв С.О.



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: 7036.
- 2) Destination IP: 192.168.0.1. 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 IPадресою). Під «компонентами відповіді» я розумію адресу сайту, який запитується - ietf.org, тобто який сайт ми хочемо отримати.
- 4) Усього було 3 запити-відповіді. Відповіді містять ім'я домену, час життя (в сек), тип запису, клас (IN якщо отримано через Інтернет), і саме значення адреси. Причому 3-ій запит іде на якийсь ресурс пов'язаний з аналітикою. Розглянемо перші два. Це власне запити на пошук нашого сайту www.ietf.org. Відповідно до моделі роботи DNS серверів, спочатку іде запит на по першому рівню доменів в .org шукаємо ietf.org. Сервер вертає посилання на інший сервер, в якому варто шукати наш www.ietf.org.

```
dns
                                                                                                                            × +
   Time
                 Source
                                      Destination
                                                           Protocol Length Info
 33 3.952552
                 192.168.0.105
                                      192.168.0.1
                                                           DNS
                                                                      68 Standard query 0x13c4 A ietf.org
 34 4.005017
               192.168.0.1
                                 192.168.0.105
                                                                     241 Standard query response 0x13c4 A ietf.org A 4.31.198.44 NS ns...
                                                           DNS
                                                                      72 Standard query 0x9868 A www.ietf.org
 35 4.267285
                 192.168.0.105
                                      192.168.0.1
                                                           DNS
                                                                     149 Standard query response 0x9868 A www.ietf.org CNAME www.ietf...
 36 4.320101
                 192.168.0.1
                                      192.168.0.105
                                                           DNS
591 5.738721
                 192.168.0.105
                                                                      78 Standard query 0xa93d A analytics.ietf.org
                                      192.168.0.1
                                                           DNS
520 6.537272
                 192.168.0.1
                                      192.168.0.105
                                                           DNS
                                                                     265 Standard query response 0xa93d A analytics.ietf.org CNAME iet...
> Frame 34: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{B6F802DD-58AE-4796-82E0-18ADB921229
> Ethernet II, Src: D-LinkIn_2c:c0:b0 (1c:af:f7:2c:c0:b0), Dst: IntelCor_7e:a3:ce (08:d4:0c:7e:a3:ce)
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105
 > User Datagram Protocol, Src Port: 53, Dst Port: 7036

✓ Domain Name System (response)

     Transaction ID: 0x13c4
   > Flags: 0x8180 Standard query response, No error
     Questions: 1
      Answer RRs: 1
      Authority RRs: 6
      Additional RRs: 0

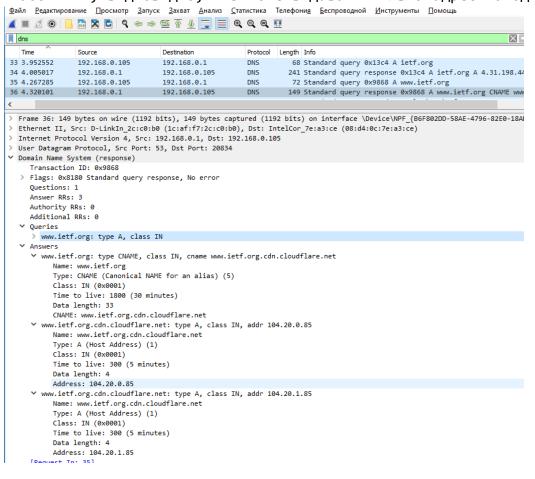
✓ Queries

       ietf.org: type A, class IN
   Answers

✓ ietf.org: type A, class IN, addr 4.31.198.44

           Name: ietf.org
           Type: A (Host Address) (1)
           Class: IN (0x0001)
           Time to live: 1800 (30 minutes)
           Data length: 4
           Address: 4.31.198.44
   > Authoritative nameservers
      [Request In: 33]
      [Time: 0.052465000 seconds]
```

Після цього іде наступний запит на новий сервер, де шукаємо вже www.ietf.org. У відповідь ми отримаємо поля у Answers: CNAME з канонічним іменем домену, а також двома ІР адресами. Пояснення цьому знаходимо у Таненбаума, «у деяких хостів може бути одночасно встановлено кілька мережевих з'єднань. В цьому випадку їм може бути потрібним 2+ записи типу А або АААА, відповідно, DNS може видавати кілька адрес на одне ім'я».



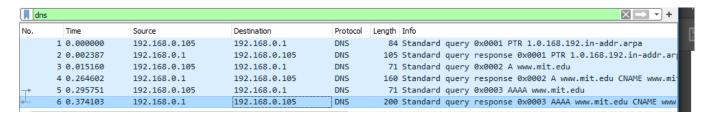
5) Так співпадає. На скріні наведено мишкою на цільову адресу і виділено її в деталях DNS запиту.

```
Time
                                         Destination
                                                               Protocol Length Info
   36 4.320101
                    192.168.0.1
                                          192.168.0.105
                                                                         149 Standard query response 0x9868 A www.ietf.org CN
   37 4.320908
                    192.168.0.105
                                         104.20.0.85
                                                               TCP
                                                                          74 21498 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 N
Frame 36: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{B6F802DD-58AE-4796-82E0-18A
Ethernet II, Src: D-LinkIn_2c:c0:b0 (1c:af:f7:2c:c0:b0), Dst: IntelCor_7e:a3:ce (08:d4:0c:7e:a3:ce)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105
User Datagram Protocol, Src Port: 53, Dst Port: 20834
Domain Name System (response)
  Transaction ID: 0x9868
> Flags: 0x8180 Standard query response, No error
  Ouestions: 1
  Answer RRs: 3
   Authority RRs: 0
  Additional RRs: 0
> Queries
Answers
   > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
   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: 300 (5 minutes)
        Data length: 4
        Address: 104.20.0.85
```

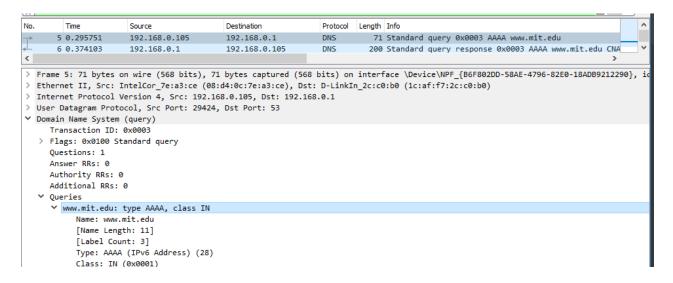
6) Так виконала ще один запит, як зазначалося в п.4 (отримує ресурс для аналітики сайту).

ВІДПОВІДІ НА ПИТАННЯ 7-10

- 7) Цільовий порт запиту відповідав вихідному порту з відповіддю Port: 53.
- 8) Мій локальний DNS сервер 192.168.0.1. Як бачимо запити відбувалися саме на цю адресу:



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



Всього містилося 3 відповіді (на 3 запити). Але оскільки вказано, що 10) потрібно розглядати лише 3-ю, то наведемо її опис. Цей респонс містив в собі 4 відповіді, 2 типу СПАМЕ, 2 - АААА. Як уже зазначалося СПАМЕ 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 АААА аналогічна п.4 для А.

```
Domain Name System (response 3)
    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: 1800 (30 minutes)
            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: 300 (5 minutes)
            Data length: 24
            CNAME: e9566.dscb.akamaiedge.net
        e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:191::255e
            Name: e9566.dscb.akamaiedge.net
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
            Time to live: 300 (5 minutes)
            Data length: 16
            AAAA Address: 2a02:26f0:d200:191::255e
        e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:19e::255e
            Name: e9566.dscb.akamaiedge.net
            Type: AAAA (IPv6 Address) (28)
            Class: IN (0x0001)
            Time to live: 300 (5 minutes)
            Data length: 16
            AAAA Address: 2a02:26f0:d200:19e::255e
    [Request In: 5]
    [Time: 0.078352000 seconds]
```

ВІДПОВІДІ НА ПИТАННЯ 11-13

dns								
No.	Time	Source	Destination	Protocol	Length	Info		
	6 1.211692	192.168.0.105	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa		
4	7 1.213455	192.168.0.1	192.168.0.105	DNS	105	Standard query response 0x0001 PTR 1.0.168.192.in-addr.arpa PTR dir-320		
	8 1.216752	192.168.0.105	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu		
	9 1.251431	192.168.0.1	192.168.0.105	DNS	234	Standard query response 0x0002 NS mit.edu NS use5.akam.net NS asia2.akam.net		
	10 1.848921	192.168.0.105	192.168.0.1	DNS	77	Standard query 0xfb01 A cdn2.ghostery.com		
	11 1.856666	192.168.0.1	192.168.0.105	DNS	277	Standard query response 0xfb01 A cdn2.ghostery.com A 13.227.198.21 A 13.227.		

- 11) Мій локальний DNS сервер 192.168.0.1. 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.

dn	S											
No.	Time	Source	Destination	Protocol	Length	Info						
	6 1.211692	192.168.0.105	192.168.0.1	DNS	84	Standard	query	0x0001 PTR 1.0.168.192.in-addr.arpa				
	7 1.213455	192.168.0.1	192.168.0.105	DNS	105	Standard	query	response 0x0001 PTR 1.0.168.192.in-				
→	8 1.216752	192.168.0.105	192.168.0.1	DNS	67	Standard	query	0x0002 NS mit.edu				
4	9 1.251431	192.168.0.1	192.168.0.105	DNS	234	Standard	query	response 0x0002 NS mit.edu NS use5.				
<												
> Fr	ame 8: 67 bytes	on wire (536 bits),	67 bytes captured (53	6 bits) on	interf	face \Devi	ce\NPF	F_{B6F802DD-58AE-4796-82E0-18ADB9212				
> Et	hernet II, Src:	IntelCor_7e:a3:ce (08:d4:0c:7e:a3:ce), Ds	t: D-LinkI	n_2c:c0):b0 (1c:a	f:f7:2	2c:c0:b0)				
> In	Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1											
> Us	User Datagram Protocol, Src Port: 1027, Dst Port: 53											
▼ Domain Name System (query)												
	Transaction ID: 0x0002											
> Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0												
	Authority RRs:											
	Additional RRs:	0										
~	Queries											
	∨ mit.edu: type NS, class IN											
	Name: mit											
	[Name Leng	•										
	[Label Cou	-	5) (5)									
	21	(authoritative Name	Server) (2)									
	Class: IN	Class: IN (0x0001)										

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

<u>Domain Name System (response)</u>

```
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 use5.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: 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 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 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 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 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
   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: 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: 1800 (30 minutes)
       Data length: 7
       Name Server: eur5.akam.net
[Request In: 8]
[Time: 0.034679000 seconds]
```

ВІДПОВІДІ НА ПИТАННЯ 14-16

dı	dns +								
No.	Time	Source	Destination	Protocol	Length	Info			
	1 0.000000	192.168.0.105	192.168.0.1	DNS	73	Standard query 0x5ab8 A bitsy.mit.edu			
	2 0.025408	192.168.0.105	192.168.0.1	DNS	73	Standard query 0x5ab8 A bitsy.mit.edu			
	3 0.109622	192.168.0.1	192.168.0.105	DNS	89	Standard query response 0x5ab8 A bitsy.mit.edu A 18.0.72.			
	4 0.123062	192.168.0.105	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa			
	7 2.142953	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr			
	11 4.149778	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr			
	21 6.154644	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr			
	35 8.162059	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr			

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

<u>Domain Name System (response)</u>

```
Transaction ID: 0x5ab8
Flags: 0x8180 Standard query response, No error
Ouestions: 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: 1]
[Time: 0.109622000 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 МІТ виконався запит А, для аііт — виконалося кілька запитів РТR, А, АААА. 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\rulit>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
   timeout was 2 seconds.

¬XËTXË: UnKnown
Address: 18.0.72.3

DNS request timed out.
   timeout was 2 seconds.

NS request timed out.
   timeout was 2 seconds.

The Bebiшено время ожидания запроса UnKnown
```

