

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Кафедра математичних методів системного аналізу

ЗВІТ

Про виконання лабораторних робіт
З дисципліни «Комп'ютерні мережі»

Виконав: ст. гр. ІС-ЗП91

Коган Антон

Прийняв: Кухарєв С.О.

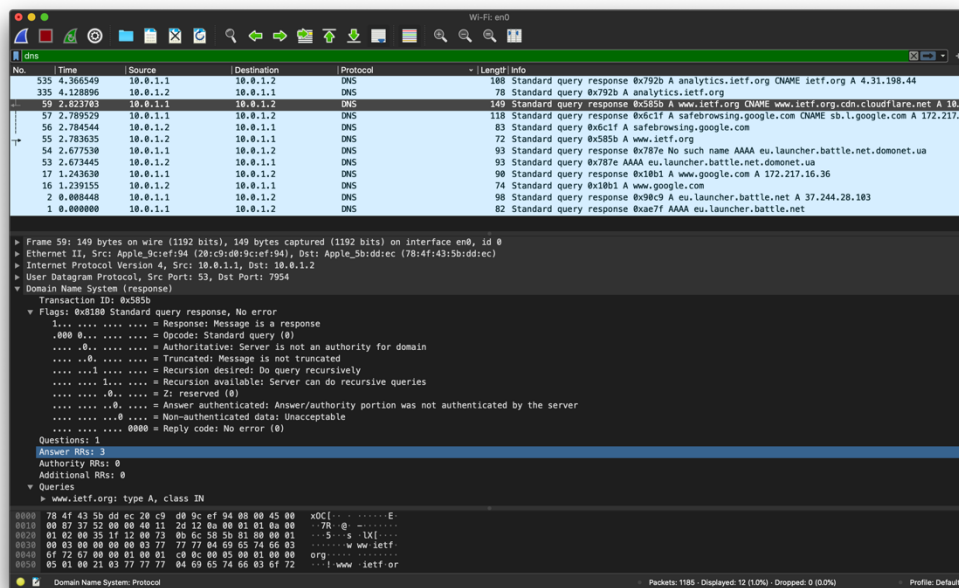
Лабораторна робота №3 3. Протокол DNS

Мета роботи: аналіз деталей роботи протоколу DNS NS.

3.2. Хід роботи

Виконаємо наступні дії:

1. Очистимо кеш DNS-записів
2. Запустимо веб-браузер, очистимо кеш браузера:
3. Запустимо Wireshark, почнемо захоплення пакетів.
4. Відкриємо за допомогою браузера одну із зазначених нижче адрес:
<http://www.ietf.org>
5. Зупинимо захоплення пакетів.
6. Переглянемо деталі захоплених пакетів.



7. Приготуємо відповіді на контрольні запитання 1-6, роздрукуємо необхідні для цього пакети.

7.1. Знайдемо запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер

вихідного порта відповіді DNS?

```
▼ User Datagram Protocol, Src Port: 53, Dst Port: 36655
  Source Port: 53
  Destination Port: 36655
  Length: 74
  Checksum: 0xe431 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 6]
  ► [Timestamps]
```

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

Internet Protocol Version 4, Src: 10.0.1.1, Dst: 10.0.1.2

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

```
▼ Queries
  ▼ analytics.ietf.org: type A, class IN
    Name: analytics.ietf.org
    [Name Length: 18]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
```

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

```
▼ Answers
  ▼ analytics.ietf.org: type CNAME, class IN, cname ietf.org
    Name: analytics.ietf.org
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 2
    CNAME: ietf.org
  ▼ 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
  [Request In: 335]
  [Time: 0.237653000 seconds]
```

7.5. Проаналізуємо 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

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

```

> Frame 59: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface en0, id 0
> Ethernet II, Src: Apple_9c:ef:94 (20:c9:d0:9c:ef:94), Dst: Apple_5b:dd:ec (78:4f:43:5b:dd:ec)
> Internet Protocol Version 4, Src: 10.0.1.1, Dst: 10.0.1.2
▼ User Datagram Protocol, Src Port: 53, Dst Port: 7954
  Source Port: 53
  Destination Port: 7954
  Length: 115
  Checksum: 0xb6c [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  ▼ [Timestamps]
    [Time since first frame: 0.040068000 seconds]
    [Time since previous frame: 0.040068000 seconds]
▼ Domain Name System (response)
  Transaction ID: 0x585b
  ▼ Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    ....0... .. = Authoritative: Server is not an authority for domain
    ....0... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    ....1... .. = Recursion available: Server can do recursive queries
    ....0... .. = Z: reserved (0)
```

8. Почнемо захоплення пакетів.

9. Виконаємо nslookup для домену www.mit.edu за допомогою команди

a. nslookup www.mit.edu

10. Зупинимо захоплення пакетів.

```

antonio@Antons-MacBook-Pro networks % nslookup www.mit.edu
Server:          10.0.1.1
Address:         10.0.1.1#53

Non-authoritative answer:
www.mit.edu      canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.96.141.207

antonio@Antons-MacBook-Pro networks % nslookup www.mit.edu
Server:          10.0.1.1
Address:         10.0.1.1#53

Non-authoritative answer:
www.mit.edu      canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.96.141.207
```

```

No. | Time | Source | Destination | Protocol | Length | Info
---+---+---+---+---+---+---
25 | 3.488591 | 10.0.1.2 | 10.0.1.1 | DNS | 71 | Standard query 0x6fe9 A www.mit.edu
26 | 3.411496 | 10.0.1.1 | 10.0.1.2 | DNS | 160 | Standard query response 0x6fe9 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.d...

> Frame 25: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0
> Ethernet II, Src: Apple_5b:dd:ec (78:4f:43:5b:dd:ec), Dst: Apple_9c:ef:94 (20:c9:d0:9c:ef:94)
> Internet Protocol Version 4, Src: 10.0.1.2, Dst: 10.0.1.1
> User Datagram Protocol, Src Port: 52860, Dst Port: 53
  Source Port: 52860
  Destination Port: 53
  Length: 37
  Checksum: 0x585b [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
    [Time since first frame: 0.00000000 seconds]
    [Time since previous frame: 0.00000000 seconds]
  Domain Name System (query)
    Transaction ID: 0x6fe9
    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
    0000 20 c9 d0 9c ef 94 78 4f 43 5b dd ec 00 00 45 00 .....x0 c[...E
    0010 00 39 f6 b0 00 00 00 11 00 01 00 00 01 02 0a 00 .....9xxx0000000000
    0020 01 01 ce 7c 00 35 00 25 58 5b 6f e9 01 00 00 01 ...].5%X[0.....
    0030 00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65 .....www.mit-e
    0040 64 75 00 00 01 00 01 .....du.....
  
```

11. Приготуємо відповіді на контрольні запитання 7-10, роздрукуємо необхідні для цього пакети. Утиліта nslookup відправляє три запити та отримує три відповіді, така поведінка є специфічною, тому слід ігнорувати перші два запити та перші дві відповіді.

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

```

User Datagram Protocol, Src Port: 52860, Dst Port: 53
Source Port: 52860
Destination Port: 53
  
```

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

```

Source: 10.0.1.2
Destination: 10.0.1.1
  
```

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

```

Queries
  www.mit.edu: type A, class IN
    Name: www.mit.edu
    [Name Length: 11]
    [Label Count: 3]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    [Response In: 26]
  
```

10. Дослідимо повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей? з 3х записів.

```
▼ 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: 1788 (29 minutes, 48 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: 48 (48 seconds)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.141.207
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 8 (8 seconds)
    Data length: 4
    Address: 104.96.141.207
  [Request In: 25]
  [Time: 0.002905000 seconds]
```

12. Почнімо захоплення пакетів.

13. Виконаємо nslookup для домену www.mit.edu за допомогою команди

a. nslookup -type=NS mit.edu

```
antonio@Antons-MacBook-Pro networks % nslookup www.mit.edu
Server:          10.0.1.1
Address:         10.0.1.1#53

Non-authoritative answer:
www.mit.edu      canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.96.141.207

antonio@Antons-MacBook-Pro networks % nslookup -type=NS mit.edu
;; connection timed out; no servers could be reached
```

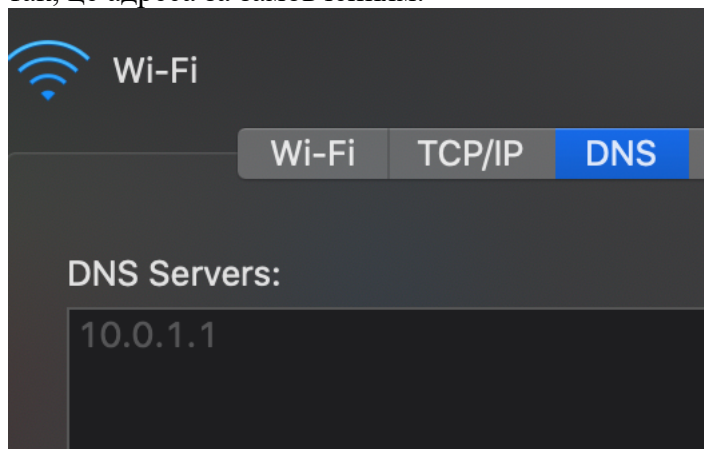
14. Зупинимо захоплення пакетів.

15. Приготуємо відповіді на запитання 11-13. При необхідності роздрукуємо деякі захоплені пакети.

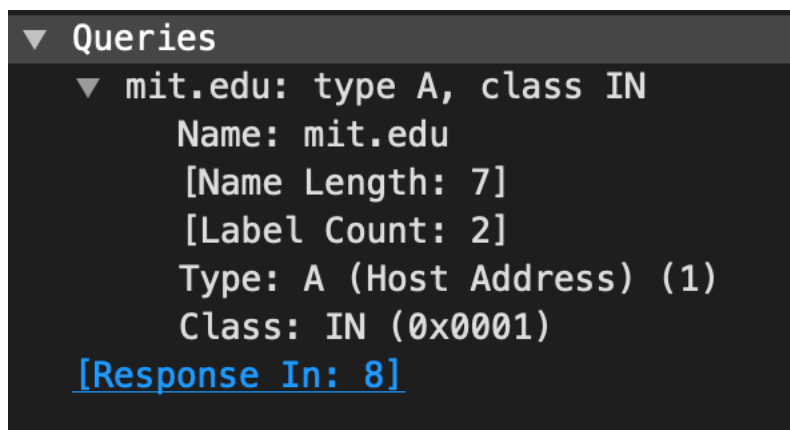
15.11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

10.0.1.1 DNS 67 Standard query 0x34a1 A mit.edu

так, це адреса за замовчанням.



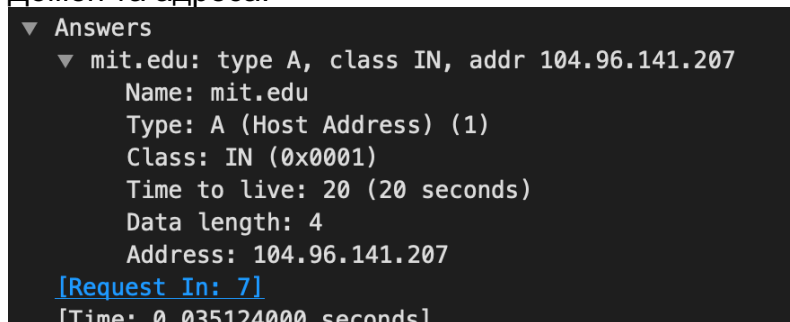
15.12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»? тип A, відповідь прийшла окремо.



15.13. Дослідимо 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?

1 відповідь mit.edu: type A, class IN, addr 104.96.141.207

Домен та адреса.



16. Почнемо захоплення пакетів.

17. Виконаємо nslookup для домену www.mit.edu за допомогою команди

a. nslookup www.aiit.or.kr

```
antonio@Antons-MacBook-Pro networks % nslookup www.aiit.or.kr
Server:          10.0.1.1
Address:         10.0.1.1#53

Non-authoritative answer:
Name:   www.aiit.or.kr
Address: 58.229.6.225
```

18. Зупинимо захоплення пакетів.

19. Приготуємо відповіді на запитання 14-16

19.14. 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?

60 3.400217 10.0.1.2 10.0.1.1 DNS 74 Standard query 0xc1a9
A www.aiit.or.kr

10.0.1.1 - моя адреса за замовчанням.

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

```
▼ Queries
  ▼ www.aiit.or.kr: type A, class IN
    Name: www.aiit.or.kr
    [Name Length: 14]
    [Label Count: 4]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    [Response In: 61]
```

19.16. Дослідимо повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей? 1 запис:

```
▼ Answers
  ▼ www.aiit.or.kr: type A, class IN, addr 58.229.6.225
    Name: www.aiit.or.kr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3561 (59 minutes, 21 seconds)
    Data length: 4
    Address: 58.229.6.225
    [Request In: 60]
    [Time: 0.002746000 seconds]
```