

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

ЗВІТ

Про виконання лабораторної роботи №3
З дисципліни «Комп'ютерні мережі»

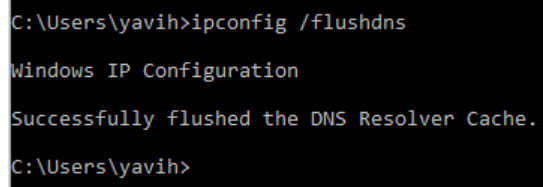
Виконав: ст. гр. ІС-ЗП91
Голуб Я.В.
Прийняв: Кухарев С.О.

Я включив відповіді на контрольні питання у опис ходу виконання роботи.

Хід виконання роботи

1. Очистіть кеш DNS-записів

- а. для windows-систем виконайте в терміналі `ipconfig /flushdns`
- б. для linux-систем (можливо) спрацює перезавпуск операційної системи;



```
C:\Users\yavih>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\yavih>
```

Рисунок 1

2. Запустіть веб-браузер, очистіть кеш браузера:

- а. для Firefox виконайте Tools >> Clear Private Data (або Ctrl + Shift + Del)
- б. для MS IE виконайте Tools >> Internet Options >> Delete File

3. Запустіть Wireshark, почніть захоплення пакетів.

4. Відкрийте за допомогою браузера одну із зазначених нижче адрес:

<http://www.ietf.org>

5. Зупиніть захоплення пакетів.

6. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).

7. Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.

7.1. 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 та відповідь DNS використовують протокол UDP

Номер цільового порта запиту DNS: 53

Який номер вихідного порта відповіді DNS: 53

Запит:

dns						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.118292	192.168.31.120	192.168.31.1	DNS	74	Standard query 0x75f7 A www.google.com
4	0.119722	192.168.31.1	192.168.31.120	DNS	90	Standard query response 0x75f7 A www.google.com A 172.21
38	1.066326	192.168.31.120	192.168.31.1	DNS	72	Standard query 0xf197 A www.ietf.org
39	1.069502	192.168.31.1	192.168.31.120	DNS	149	Standard query response 0xf197 A www.ietf.org CNAME ww.
293	1.299993	192.168.31.120	192.168.31.1	DNS	78	Standard query 0xb648 A analytics.ietf.org
294	1.301203	192.168.31.1	192.168.31.120	DNS	116	Standard query response 0xb648 A analytics.ietf.org CNAM

> Frame 38: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48},

> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIE1_5c:9d:79 (34:ce:00:5c:9d:79)

> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 192.168.31.1

> User Datagram Protocol, Src Port: 59786, Dst Port: 53

Source Port: 59786

Destination Port: 53

Length: 38

Checksum: 0xc001 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

> [Timestamps]

> Domain Name System (query)

Рисунок 2

Відповідь:

dns						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.118292	192.168.31.120	192.168.31.1	DNS	74	Standard query 0x75f7 A www.google.com
4	0.119722	192.168.31.1	192.168.31.120	DNS	90	Standard query response 0x75f7 A www.google
38	1.066326	192.168.31.120	192.168.31.1	DNS	72	Standard query 0xf197 A www.ietf.org
39	1.069502	192.168.31.1	192.168.31.120	DNS	149	Standard query response 0xf197 A www.ietf.o
293	1.299993	192.168.31.120	192.168.31.1	DNS	78	Standard query 0xb648 A analytics.ietf.org
294	1.301203	192.168.31.1	192.168.31.120	DNS	116	Standard query response 0xb648 A analytics.

> Frame 39: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48},

> Ethernet II, Src: XIAOMIE1_5c:9d:79 (34:ce:00:5c:9d:79), Dst: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf)

> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.120

> User Datagram Protocol, Src Port: 53, Dst Port: 59786

Source Port: 53

Destination Port: 59786

Length: 115

Checksum: 0x1ed4 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

> [Timestamps]

> Domain Name System (response)

Рисунок 3

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

запит DNS був відправлений на наступний адрес IP: 192.168.31.1

Цей адрес є адресом локального сервера DNS. Про це свідчить наступна інформація з системи Windows мого ноутбука:

Name:	Wi-Fi
Description:	Intel(R) Wi-Fi 6 AX201 160MHz
Physical address (MAC):	92:f9:6d:4a:60:bf
Status:	Operational
Maximum transmission unit:	1500
Link speed (Receive/Transmit):	780/866 (Mbps)
DHCP enabled:	Yes
DHCP servers:	192.168.31.1
DHCP lease obtained:	Friday, June 12, 2020 9:46:02 PM
DHCP lease expires:	Saturday, June 13, 2020 9:46:02 AM
IPv4 address:	192.168.31.120/24
IPv6 address:	fe80::e42c:b9f2:fe:f78e%5/64
Default gateway:	192.168.31.1
DNS servers:	192.168.31.1
DNS domain name:	
DNS connection suffix:	
DNS search suffix list:	
Network name:	boar1
Network category:	Private
Connectivity (IPv4/IPv6):	Connected to Internet / Connected to unknown network

Рисунок 4

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

Цей запит «Типу» А. посилання на рядок з відповіддю: [Response In: 39]

dns						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.118292	192.168.31.120	192.168.31.1	DNS	74	Standard query 0x75f7 A www.google.com
4	0.119722	192.168.31.1	192.168.31.120	DNS	90	Standard query response 0x75f7 A www.google.com A 172.217.1
38	1.066326	192.168.31.120	192.168.31.1	DNS	72	Standard query 0xf197 A www.ietf.org
39	1.069502	192.168.31.1	192.168.31.120	DNS	149	Standard query response 0xf197 A www.ietf.org CNAME www.ietf
293	1.299993	192.168.31.120	192.168.31.1	DNS	78	Standard query 0xb648 A analytics.ietf.org
294	1.301203	192.168.31.1	192.168.31.120	DNS	116	Standard query response 0xb648 A analytics.ietf.org CNAME :

>

Frame 38: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}, id

>

Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIEI_5c:9d:79 (34:ce:00:5c:9d:79)

>

Internet Protocol Version 4, Src: 192.168.31.120, Dst: 192.168.31.1

>

User Datagram Protocol, Src Port: 59786, Dst Port: 53

▼

Domain Name System (query)

Transaction ID: 0xf197

>

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: 39]

Рисунок 5

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

Відповідь: Запропоновано 3 відповіді, Кожна з відповідей містить наступні

поля: Name, Type, Class, Time to live, Data length, CNAME (або Address)

dns						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.118292	192.168.31.120	192.168.31.1	DNS	74	Standard query 0x75f7 A www.google.com
4	0.119722	192.168.31.1	192.168.31.120	DNS	90	Standard query response 0x75f7 A www.google.com A 172.217.2
38	1.066326	192.168.31.120	192.168.31.1	DNS	72	Standard query 0xf197 A www.ietf.org
39	1.069502	192.168.31.1	192.168.31.120	DNS	149	Standard query response 0xf197 A www.ietf.org CNAME www.iet
293	1.299993	192.168.31.120	192.168.31.1	DNS	78	Standard query 0xb648 A analytics.ietf.org
294	1.301203	192.168.31.1	192.168.31.120	DNS	116	Standard query response 0xb648 A analytics.ietf.org CNAME i

```

> Frame 39: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}
> Ethernet II, Src: XIAOMIEI_5c:9d:79 (34:ce:00:5c:9d:79), Dst: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf)
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.120
> User Datagram Protocol, Src Port: 53, Dst Port: 59786
▼ Domain Name System (response)
  Transaction ID: 0xf197
  > Flags: 0x8180 Standard query response, No error
  Questions: 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
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 30 (30 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: 30 (30 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: 30 (30 seconds)
      Data length: 4
      Address: 104.20.0.85
  [Request In: 38]
  [Time: 0.003176000 seconds]

```

Рисунок 6

7.5. 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?

Відповідь: в TCP SYN Destination: 104.20.1.85 співпадає з однією з запропонованих відповідей сервера DNS

No.	Time	Source	Destination	Protocol	Length	Info
39	1.069502	192.168.31.1	192.168.31.120	DNS	149	Standard query response 0xf197 A www.ietf.org CNAME www
40	1.070058	192.168.31.120	104.20.1.85	TCP	66	64222 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256


```

> Frame 40: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}.
> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIE1_5c:9d:79 (34:ce:00:5c:9d:79)
> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 104.20.1.85
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0xaf7 (2807)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.31.120
    Destination: 104.20.1.85
> Transmission Control Protocol, Src Port: 64222, Dst Port: 443, Seq: 0, Len: 0

```

Рисунок 7

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

Відповідь: так. Було виконано 3 DNS запити у порядку відсилки:

1. щодо www.google.com. Ймовірно не пов'язаний з адресою www.ietf.org
2. щодо www.ietf.org
3. щодо analytics.ietf.org. Ймовірно це новий DNS запит для отримання ресурсів, які використовує документ, що отримав браузер

No.	Time	Source	Destination	Protocol	Length	Info
3	0.118292	192.168.31.120	192.168.31.1	DNS	74	Standard query 0x75f7 A www.google.com
4	0.119722	192.168.31.1	192.168.31.120	DNS	90	Standard query response 0x75f7 A www.google.com A 172.217.20.164
38	1.066326	192.168.31.120	192.168.31.1	DNS	72	Standard query 0xf197 A www.ietf.org
39	1.069502	192.168.31.1	192.168.31.120	DNS	149	Standard query response 0xf197 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.n
293	1.299993	192.168.31.120	192.168.31.1	DNS	78	Standard query 0xb648 A analytics.ietf.org
294	1.301203	192.168.31.1	192.168.31.120	DNS	116	Standard query response 0xb648 A analytics.ietf.org CNAME ietf.org A 4.31.198.44

Рисунок 8

8. Почніть захоплення пакетів.

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

a. nslookup www.mit.edu

10. Зупинить захоплення пакетів.

11. Приготуйте відповіді на контрольні запитання 7-10, роздрукуйте 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?

Цільовим портом повідомлення із запитом DNS був порт 53

dns						
No.	Time	Source	Destination	Protocol	Length	Info
7	3.939645	192.168.31.120	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
8	3.941498	192.168.31.1	192.168.31.120	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa PTR XiaoQ
9	3.943271	192.168.31.120	192.168.31.1	DNS	71	Standard query 0x0002 A www.mit.edu
10	4.055779	192.168.31.1	192.168.31.120	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey
11	4.060891	192.168.31.120	192.168.31.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
12	4.093279	192.168.31.1	192.168.31.120	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey

> Frame 11: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}, id 0
> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIEI_5c:9d:79 (34:ce:00:5c:9d:79)
> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 192.168.31.1
> User Datagram Protocol, Src Port: 50881, Dst Port: 53
> Domain Name System (query)

Рисунок 9

вихідним портом повідомлення із відповіддю DNS був порт 53

dns						
No.	Time	Source	Destination	Protocol	Length	Info
7	3.939645	192.168.31.120	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
8	3.941498	192.168.31.1	192.168.31.120	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.
9	3.943271	192.168.31.120	192.168.31.1	DNS	71	Standard query 0x0002 A www.mit.edu
10	4.055779	192.168.31.1	192.168.31.120	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.m
11	4.060891	192.168.31.120	192.168.31.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
12	4.093279	192.168.31.1	192.168.31.120	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME ww

> Frame 12: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}
> Ethernet II, Src: XIAOMIEI_5c:9d:79 (34:ce:00:5c:9d:79), Dst: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf)
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.120
> User Datagram Protocol, Src Port: 53, Dst Port: 50881
> Domain Name System (response)

Рисунок 10

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

запит DNS був направлений на IP-адресу 192.168.31.1

Як було вказано у пункті 7.2 цього звіту, ця адреса є адресою мого локального сервера DNS за замовчанням.

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

Цей запит був типу AAAA. Він вміщує посилання на відповідь: [Response In: 12]

dns						
No.	Time	Source	Destination	Protocol	Length	Info
7	3.939645	192.168.31.120	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
8	3.941498	192.168.31.1	192.168.31.120	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.
9	3.943271	192.168.31.120	192.168.31.1	DNS	71	Standard query 0x0002 A www.mit.edu
10	4.055779	192.168.31.1	192.168.31.120	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.t
11	4.060891	192.168.31.120	192.168.31.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
12	4.093279	192.168.31.1	192.168.31.120	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME w


```

> Frame 11: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48},
> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIE1_5c:9d:79 (34:ce:00:5c:9d:79)
> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 192.168.31.1
> User Datagram Protocol, Src Port: 50881, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  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)
      [Response In: 12]

```

Рисунок 11

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

Сервером було запропоновано чотири відповіді. Кожна відповідь складається з полів Name, Type, Class, Time to live, Data length, CNAME (або AAAA Address)

dns						
No.	Time	Source	Destination	Protocol	Length	Info
7	3.939645	192.168.31.120	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
8	3.941498	192.168.31.1	192.168.31.120	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa P
9	3.943271	192.168.31.120	192.168.31.1	DNS	71	Standard query 0x0002 A www.mit.edu
10	4.055779	192.168.31.1	192.168.31.120	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu
11	4.060891	192.168.31.120	192.168.31.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
12	4.093279	192.168.31.1	192.168.31.120	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.

> Frame 12: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}, i

> Ethernet II, Src: XIAOMIEI_Sc:9d:79 (34:ce:00:5c:9d:79), Dst: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf)

> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.120

> User Datagram Protocol, Src Port: 53, Dst Port: 50881

▼ 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

▼ 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: 3600 (1 hour)

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: 3600 (1 hour)

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

▼ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d8:389::255e

Name: e9566.dscb.akamaiedge.net

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Time to live: 3600 (1 hour)

Data length: 16

AAAA Address: 2a02:26f0:d8:389::255e

▼ e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d8:3a2::255e

Name: e9566.dscb.akamaiedge.net

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Time to live: 3600 (1 hour)

Data length: 16

AAAA Address: 2a02:26f0:d8:3a2::255e

[Request In: 11]

[Time: 0.032388000 seconds]

Рисунок 12

12. Почніть захоплення пакетів.

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

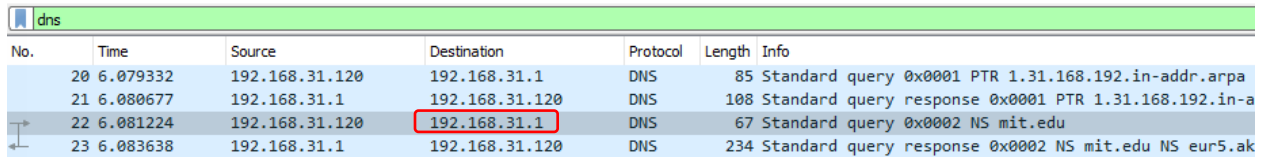
a. nslookup -type=NS mit.edu

14. Зупиніть захоплення пакетів.

15. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети.

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

запит DNS був направлений на IP-адресу 192.168.31.1. Як було показано у пункті 7.2, ця адреса є адресою мого локального сервера **DNS за замовчанням**



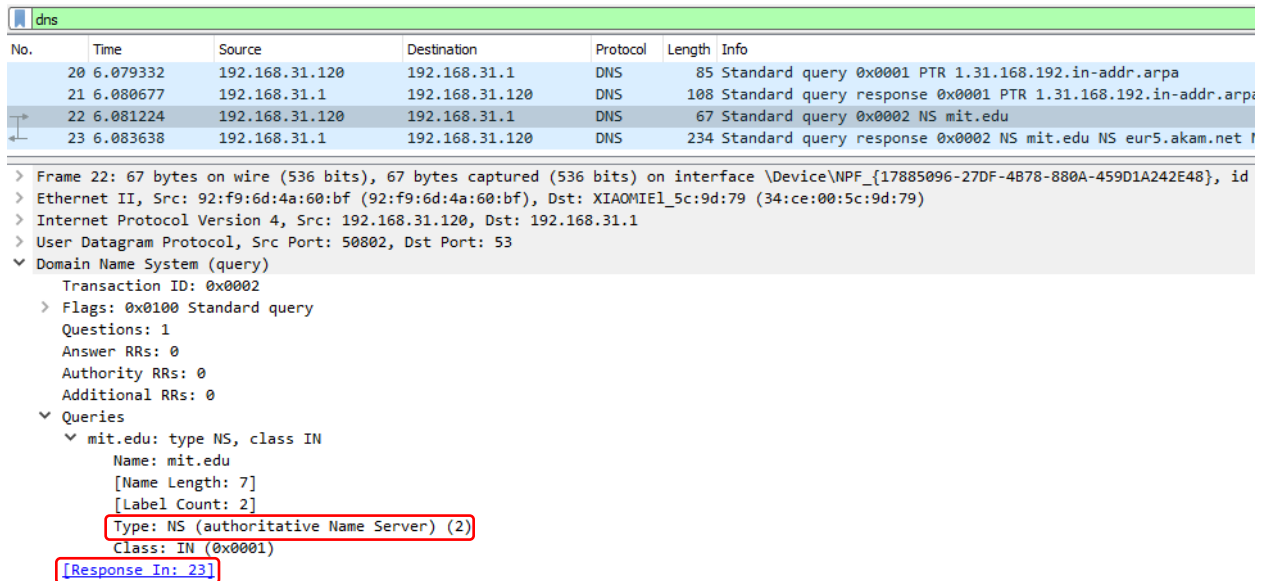
No.	Time	Source	Destination	Protocol	Length	Info
20	6.079332	192.168.31.120	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
21	6.080677	192.168.31.1	192.168.31.120	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa
22	6.081224	192.168.31.120	192.168.31.1	DNS	67	Standard query 0x0002 NS mit.edu
23	6.083638	192.168.31.1	192.168.31.120	DNS	234	Standard query response 0x0002 NS mit.edu NS eur5.akam.net

Рисунок 13

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

Цей запис був типу NS (authoritative Name Server) (2)

Він вміщує посилання на відповіді: [Response In: 23]



No.	Time	Source	Destination	Protocol	Length	Info
20	6.079332	192.168.31.120	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
21	6.080677	192.168.31.1	192.168.31.120	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa
22	6.081224	192.168.31.120	192.168.31.1	DNS	67	Standard query 0x0002 NS mit.edu
23	6.083638	192.168.31.1	192.168.31.120	DNS	234	Standard query response 0x0002 NS mit.edu NS eur5.akam.net

> Frame 22: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}, id 0x12345678

> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIEl_5c:9d:79 (34:ce:00:5c:9d:79)

> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 192.168.31.1

> User Datagram Protocol, Src Port: 50002, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

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)

[Response In: 23]

Рисунок 14

15.13. Дослідить 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?

сервером було запропоновано вісім записів із відповідями. Сервери були запропоновані за допомогою доменного імені. Див. рис. нижче для списку імен запропонованих серверів.

No.	Time	Source	Destination	Protocol	Length	Info
20	6.079332	192.168.31.120	192.168.31.1	DNS	85	Standard query 0x0001 PTR 1.31.168.192.in-addr.arpa
21	6.080677	192.168.31.1	192.168.31.120	DNS	108	Standard query response 0x0001 PTR 1.31.168.192.in-addr.arpa
22	6.081224	192.168.31.120	192.168.31.1	DNS	67	Standard query 0x0002 NS mit.edu
23	6.083638	192.168.31.1	192.168.31.120	DNS	234	Standard query response 0x0002 NS mit.edu NS eur5.akam.net N


```

> Frame 23: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48},
> Ethernet II, Src: XIAOMIEI_5c:9d:79 (34:ce:00:5c:9d:79), Dst: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf)
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.120
> User Datagram Protocol, Src Port: 53, Dst Port: 50802
▼ 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
  ▼ Answers
    ▼ 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: 969 (16 minutes, 9 seconds)
      Data length: 15
      Name Server: eur5.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
  [Request In: 22]
  [Time: 0.002414000 seconds]

```

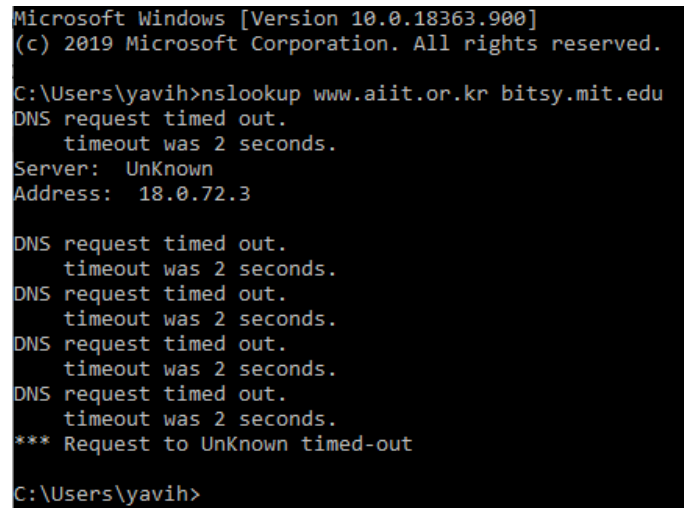
Рисунок 15

16. Почніть захоплення пакетів.

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

a. nslookup www.aiit.or.kr bitsy.mit.edu

виконання цієї команди видало наступний результат у командному вікні:



```
Microsoft Windows [Version 10.0.18363.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\yaviv>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:    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.
*** Request to UnKnown timed-out

C:\Users\yaviv>
```

Рисунок 16

Схоже під час відпрацювання запиту у серверу (-рів) виникли проблеми з отриманням відповідей

18. Зупиніть захоплення пакетів.

19. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.

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?

запит DNS був направлений на наступну IP-адресу:

Destination: 192.168.31.1

Згідно пункту 7.2 ця адреса є адресою мого локального сервера DNS за замовчанням

dns						
No.	Time	Source	Destination	Protocol	Length	Info
25	0.950021	192.168.31.120	192.168.31.1	DNS	73	Standard query 0x306e A bitsy.mit.edu
26	0.951286	192.168.31.1	192.168.31.120	DNS	89	Standard query response 0x306e A bitsy.mit.edu A 18.0
27	0.953236	192.168.31.120	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
32	2.956677	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
33	4.962244	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
34	6.963607	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
60	8.974970	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr


```

> Frame 25: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E44}
> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMI_E1_5c:9d:79 (34:ce:00:5c:9d:79)
> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 192.168.31.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 59
    Identification: 0xe5db (58843)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.31.120
    Destination: 192.168.31.1
  > User Datagram Protocol, Src Port: 56144, Dst Port: 53
  > Domain Name System (query)
  
```

Рисунок 17

Далі браузер послав п'ять запитів на IP адресу 18.0.72.3, яка не є адресою мого локального сервера DNS за замовчанням

dns						
No.	Time	Source	Destination	Protocol	Length	Info
25	0.950021	192.168.31.120	192.168.31.1	DNS	73	Standard query 0x306e A bitsy.mit.edu
26	0.951286	192.168.31.1	192.168.31.120	DNS	89	Standard query response 0x306e A bitsy.mit.ed
27	0.953236	192.168.31.120	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.a
32	2.956677	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
33	4.962244	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
34	6.963607	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
60	8.974970	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Рисунок 18

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

Перший запит був запитом «Типу» А (Host Address) (1) по UDP протоколу.

Посилання на рядок з відповіддю: [Response In: 26]

dns						
No.	Time	Source	Destination	Protocol	Length	Info
25	0.950021	192.168.31.120	192.168.31.1	DNS	73	Standard query 0x306e A bitsy.mit.edu
26	0.951286	192.168.31.1	192.168.31.120	DNS	89	Standard query response 0x306e A bitsy.mit.edu A 18.0
27	0.953236	192.168.31.120	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
32	2.956677	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
33	4.962244	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
34	6.963607	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
60	8.974970	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 25: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E4}

> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIEl_5c:9d:79 (34:ce:00:5c:9d:79)

> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 192.168.31.1

> User Datagram Protocol, Src Port: 56144, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x306e

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

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)

[Response In: 26]

Рисунок 19

Другий запит (№27) був запитом типу PTR (domain name PoinTeR) (12) по UDP протоколу

dns						
No.	Time	Source	Destination	Protocol	Length	Info
25	0.950021	192.168.31.120	192.168.31.1	DNS	73	Standard query 0x306e A bitsy.mit.edu
26	0.951286	192.168.31.1	192.168.31.120	DNS	89	Standard query response 0x306e A bitsy.mit.edu A 18.0.72.3
27	0.953236	192.168.31.120	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
32	2.956677	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
33	4.962244	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
34	6.963607	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
60	8.974970	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

```

> Frame 27: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}, id 0
> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIEI_5c:9d:79 (34:ce:00:5c:9d:79)
> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 56145, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0001
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ 3.72.0.18.in-addr.arpa: type PTR, class IN
      Name: 3.72.0.18.in-addr.arpa
      [Name Length: 22]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)

```

Рисунок 20

Третій (№) та п'ятий (№) запити були типу A (Host Address) (1) по UDP протоколу

dns						
No.	Time	Source	Destination	Protocol	Length	Info
25	0.950021	192.168.31.120	192.168.31.1	DNS	73	Standard query 0x306e A bitsy.mit.edu
26	0.951286	192.168.31.1	192.168.31.120	DNS	89	Standard query response 0x306e A bitsy.mit.edu A 18.0.72.3
27	0.953236	192.168.31.120	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
32	2.956677	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
33	4.962244	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
34	6.963607	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
60	8.974970	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

```

> Frame 32: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}, id 0
> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIEI_5c:9d:79 (34:ce:00:5c:9d:79)
> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 56146, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ 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)

```

Рисунок 21

Четвертий та шостий запити були типу AAAA (IPv6 Address) (28) по DNS протоколу

dns						
No.	Time	Source	Destination	Protocol	Length	Info
25	0.950021	192.168.31.120	192.168.31.1	DNS	73	Standard query 0x306e A bitsy.mit.edu
26	0.951286	192.168.31.1	192.168.31.120	DNS	89	Standard query response 0x306e A bitsy.mit.edu A 18.0.72.3
27	0.953236	192.168.31.120	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
32	2.956677	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
33	4.962244	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
34	6.963607	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
60	8.974970	192.168.31.120	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 33: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{17885096-27DF-4B78-880A-459D1A242E48}, id 0

> Ethernet II, Src: 92:f9:6d:4a:60:bf (92:f9:6d:4a:60:bf), Dst: XIAOMIEl_5c:9d:79 (34:ce:00:5c:9d:79)

> Internet Protocol Version 4, Src: 192.168.31.120, Dst: 18.0.72.3

> User Datagram Protocol, Src Port: 56147, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0003

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ www.aiit.or.kr: type AAAA, class IN

Name: www.aiit.or.kr

[Name Length: 14]

[Label Count: 4]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Рисунок 22

Сервером був запропонований лише один запис із відповіддю саме на перший запит. Відповідь складається з полів Name, Type, Class, Time to live, Data length, Address

Рисунок 23

20. Закрийте Wireshark.