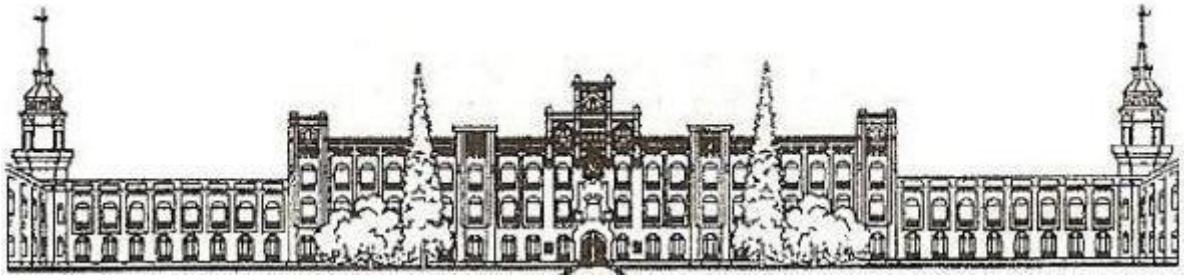


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Практична робота № 3

З курсу: «Комп'ютерні мережі»

Виконав:

Студент III курсу

Групи КА-73

Гаврюшин

П.А.

Прийняв: Кухарєв С.О.

Київ 2020

Запит 1

```
No.     Time           Source                Destination           Protocol Length Info
      1 0.000000       192.168.11.100        192.168.1.1           DNS      75     Standard query 0x4ed4 A ssl.gstatic.com
Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{98209E65-AD2B-4D55-AE9E-5CA9D244F892}, id 0
Ethernet II, Src: LiteonTe_e4:88:db (64:6e:69:e4:88:db), Dst: Tp-LinkT_a4:95:3c (94:0c:6d:a4:95:3c)
Internet Protocol Version 4, Src: 192.168.11.100, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 64038, Dst Port: 53
    Source Port: 64038
    Destination Port: 53
    Length: 41
    Checksum: 0xf651 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
Domain Name System (query)
    Transaction ID: 0x4ed4
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 3]
```

Відповідь 1

```
No.     Time           Source                Destination           Protocol Length Info
      3 0.025048       192.168.1.1           192.168.11.100        DNS      91     Standard query response 0x4ed4 A ssl.gstatic.com
A 216.58.215.67
Frame 3: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{98209E65-AD2B-4D55-AE9E-5CA9D244F892}, id 0
Ethernet II, Src: Tp-LinkT_a4:95:3c (94:0c:6d:a4:95:3c), Dst: LiteonTe_e4:88:db (64:6e:69:e4:88:db)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.11.100
User Datagram Protocol, Src Port: 53, Dst Port: 64038
    Source Port: 53
    Destination Port: 64038
    Length: 57
    Checksum: 0x9640 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
Domain Name System (response)
    Transaction ID: 0x4ed4
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
    [Request In: 1]
    [Time: 0.025048000 seconds]
```

Запит 2

```
No.     Time           Source                Destination           Protocol Length Info
      8 8.935947       192.168.11.100        192.168.1.1           DNS      71     Standard query 0x0002 A www.mit.edu
Frame 8: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{98209E65-AD2B-4D55-AE9E-5CA9D244F892}, id 0
Ethernet II, Src: LiteonTe_e4:88:db (64:6e:69:e4:88:db), Dst: Tp-LinkT_a4:95:3c (94:0c:6d:a4:95:3c)
Internet Protocol Version 4, Src: 192.168.11.100, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 51087, Dst Port: 53
    Source Port: 51087
    Destination Port: 53
    Length: 37
    Checksum: 0x577c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    [Timestamps]
Domain Name System (query)
    Transaction ID: 0x0002
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    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: 9]
```

Відповідь 2

```
No.     Time           Source                Destination           Protocol Length Info
      9 9.181771       192.168.1.1           192.168.11.100        DNS      160    Standard query response 0x0002 A www.mit.edu CNAME
www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.14.241.4
Frame 9: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{98209E65-AD2B-4D55-AE9E-5CA9D244F892}, id 0
Ethernet II, Src: Tp-LinkT_a4:95:3c (94:0c:6d:a4:95:3c), Dst: LiteonTe_e4:88:db (64:6e:69:e4:88:db)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.11.100
User Datagram Protocol, Src Port: 53, Dst Port: 51087
    Source Port: 53
    Destination Port: 51087
    Length: 126
    Checksum: 0xdba4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    [Timestamps]
Domain Name System (response)
    Transaction ID: 0x0002
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    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)
    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: 60 (1 minute)
            Data length: 24
            CNAME: e9566.dscb.akamaiedge.net
        e9566.dscb.akamaiedge.net: type A, class IN, addr 23.14.241.4
            Name: e9566.dscb.akamaiedge.net
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 20 (20 seconds)
            Data length: 4
            Address: 23.14.241.4
    [Request In: 8]
    [Time: 0.245824000 seconds]
```

Контрольні запитання

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?

```
> Frame 13: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{98209E65-AD2B-4D55-AE9E-5CA9D244F892}, id 0
> Ethernet II, Src: LiteonTe_e4:88:db (64:6e:69:e4:88:db), Dst: Tp-LinkT_a4:95:3c (94:0c:6d:a4:95:3c)
> Internet Protocol Version 4, Src: 192.168.11.102, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57684, Dst Port: 53
> Domain Name System (query)
```

UDP

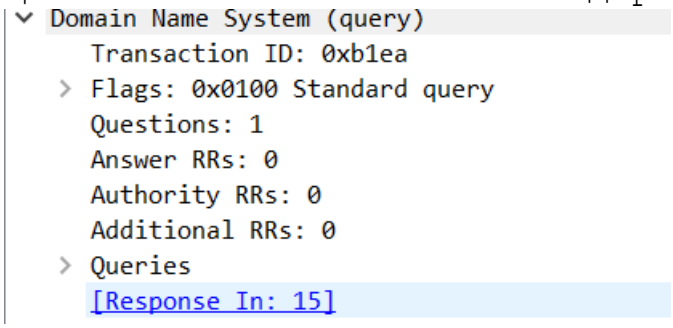
Цільовий порт: 53

Вихідний порт: 64038

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

IP:192.168.1.1, є адресом локального порта.
3.Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Цей запит – є запитом стандартного типу. Вміщує.



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

```
Transaction ID: 0xb1ea
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 4
Authority RRs: 0
Additional RRs: 0
> Queries
v Answers
  > sitecheck.opera.com: type CNAME, class IN, cname sitecheck.geo.opera.com
  > sitecheck.geo.opera.com: type CNAME, class IN, cname nl.sitecheck.opera.com
  > nl.sitecheck.opera.com: type A, class IN, addr 185.26.182.106
  > nl.sitecheck.opera.com: type A, class IN, addr 185.26.182.118
[Request In: 13]
```

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?

Ні, не співпадає

3	0.025048	192.168.1.1	192.168.11.100	DNS	91 Standard query response
4	0.025342	192.168.11.100	216.58.215.67	TCP	74 56792 → 443 [SYN] Seq=0

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

No.	Time	Source	Destination	Protocol	Length	Info
13	5.852872	192.168.11.102	192.168.1.1	DNS	79	Standard query 0xb1ea A sitecheck.opera.com
14	5.854139	192.168.11.102	192.168.1.1	DNS	74	Standard query 0xae34 A www.google.com
15	5.878266	192.168.1.1	192.168.11.102	DNS	156	Standard query response 0xb1ea A sitecheck.opera.com CNAME si…
16	5.878358	192.168.1.1	192.168.11.102	DNS	90	Standard query response 0xae34 A www.google.com A 216.58.215.…
59	6.050702	192.168.11.102	192.168.1.1	DNS	72	Standard query 0x7367 A www.ietf.org
70	6.169162	192.168.1.1	192.168.11.102	DNS	149	Standard query response 0x7367 A www.ietf.org CNAME www.ietf.…
120	6.824384	192.168.11.102	192.168.1.1	DNS	80	Standard query 0xf774 A speeddials.opera.com
121	6.855646	192.168.1.1	192.168.11.102	DNS	190	Standard query response 0xf774 A speeddials.opera.com CNAME s…
384	7.320302	192.168.11.102	192.168.1.1	DNS	78	Standard query 0xde54 A analytics.ietf.org
545	7.495855	192.168.11.102	192.168.11.1	DNS	78	Standard query 0xa4fa A analytics.ietf.org
595	7.667537	192.168.1.1	192.168.11.102	DNS	108	Standard query response 0xde54 A analytics.ietf.org CNAME iet…
886	8.049065	192.168.11.1	192.168.11.102	DNS	108	Standard query response 0xa4fa A analytics.ietf.org CNAME iet…

Так, використовує

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

Цільовий: 192.168.1.1
Вихідний: 192.168.1.1

No.	Time	Source	Destination	Protocol	Length	Info
6	8.904018	192.168.11.100	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
7	8.926404	192.168.1.1	192.168.11.100	DNS	133	Standard query response 0x0001 No such name PTR 1.1.16
8	8.935947	192.168.11.100	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
9	9.181771	192.168.1.1	192.168.11.100	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www
10	9.185616	192.168.11.100	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
11	9.222529	192.168.1.1	192.168.11.100	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME
15	13.286742	192.168.11.100	192.168.1.1	DNS	79	Standard query 0xf344 A clients6.google.com
16	13.309083	192.168.1.1	192.168.11.100	DNS	119	Standard query response 0xf344 A clients6.google.com C

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

192.168.1.1, є адресою локального сервера

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

Цей запит – є запитом стандартного типу. Вміщує.

```
▾ Domain Name System (query)
    Transaction ID: 0x0001
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 7]
```

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

```
▾ 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: 60 (1 minute)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▾ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.14.241.4
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
```

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

IP: 192.168.1.1. Так, є.

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

Стандартний тип запиту. Так вміщує.

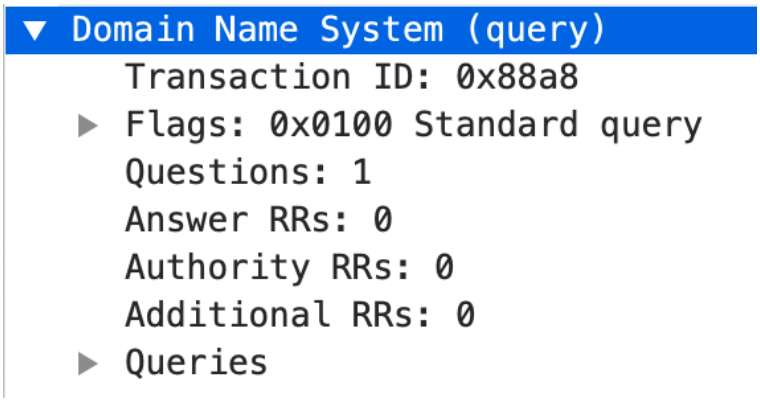
```
Domain Name System (query)
    Transaction ID: 0x93dd
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 2]
```

13. Дослідіть 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?

```
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v mit.edu: type A, class IN, addr 88.221.9.235
        Name: mit.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 20 (20 seconds)
        Data length: 4
        Address: 88.221.9.235
    [Request In: 1]
```

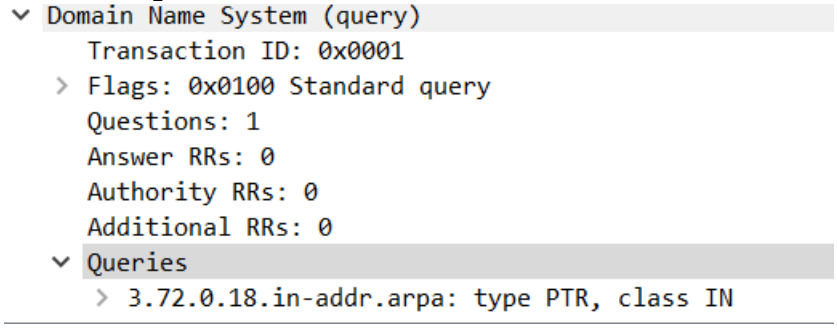
14.На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

IP: 18.0.72.3. Не є адресою локального сервера.


▼ Domain Name System (query)
Transaction ID: 0x88a8
▶ Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▶ Queries

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

Стандартний тип запиту. Ні не вміщує.



16.Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?

Відповідь не була отримана.

Висновок: В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи DNS та було проведено аналіз деталей роботи даних протоколів.