

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: студент групи ІС-ЗП93  
Дегтярьова С.М.

Прийняв: Кухарєв С.О.

Київ – 2020

## Лабораторна робота 3.

### Хід роботи

#### 1. Очистимо кеш DNS-записів:

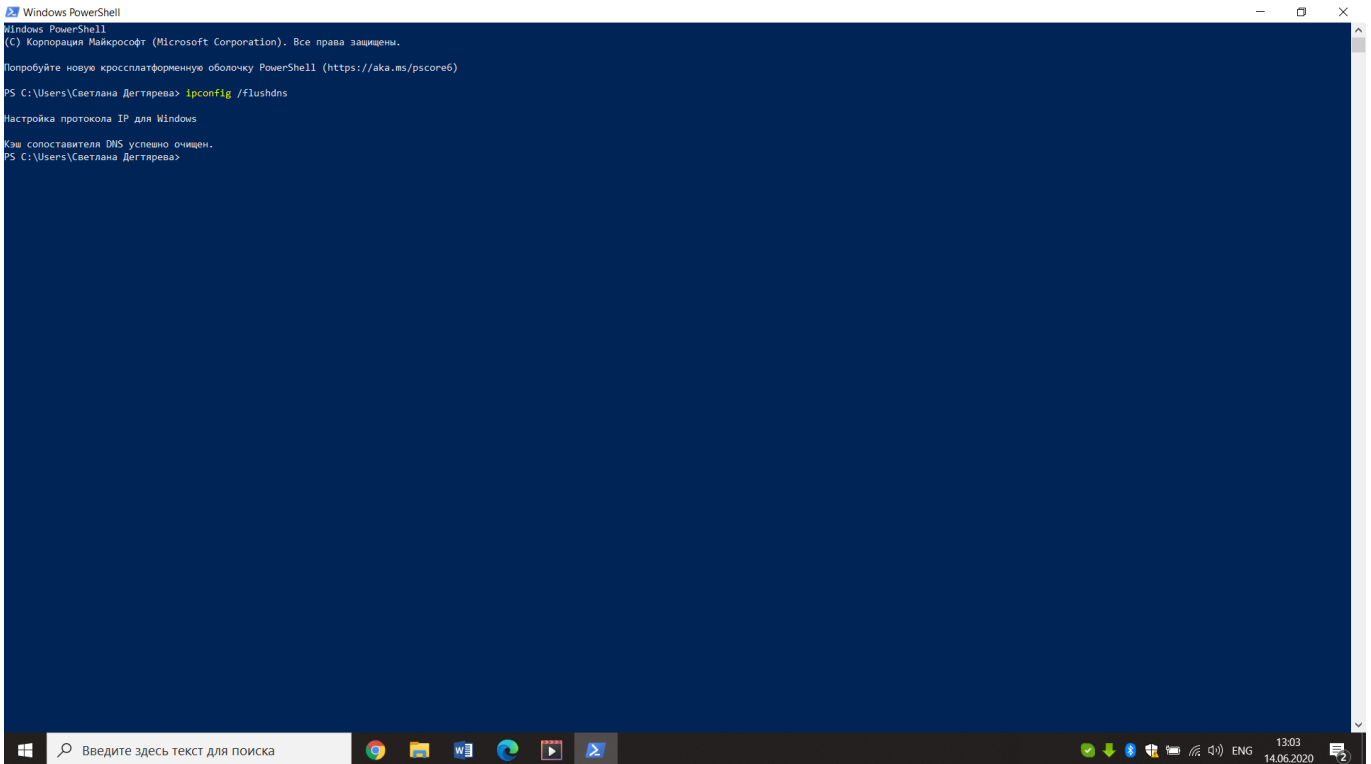


Рис. 1

2. Запустимо веб-браузер, очистимо кеш браузера.
3. Запустіть Wireshark, почніть захоплення пакетів.
4. Відкриємо за допомогою браузера одну із зазначених нижче адрес:  
<http://www.ietf.org>
5. Зупиняємо захоплення пакетів.
6. Переглядаємо деталі захоплених пакетів. Для цього налаштуємо вікно деталей пакету: згорнемо деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).
7. Готуємо відповіді на контрольні запитання 1-6, друкуємо необхідні для цього пакети.

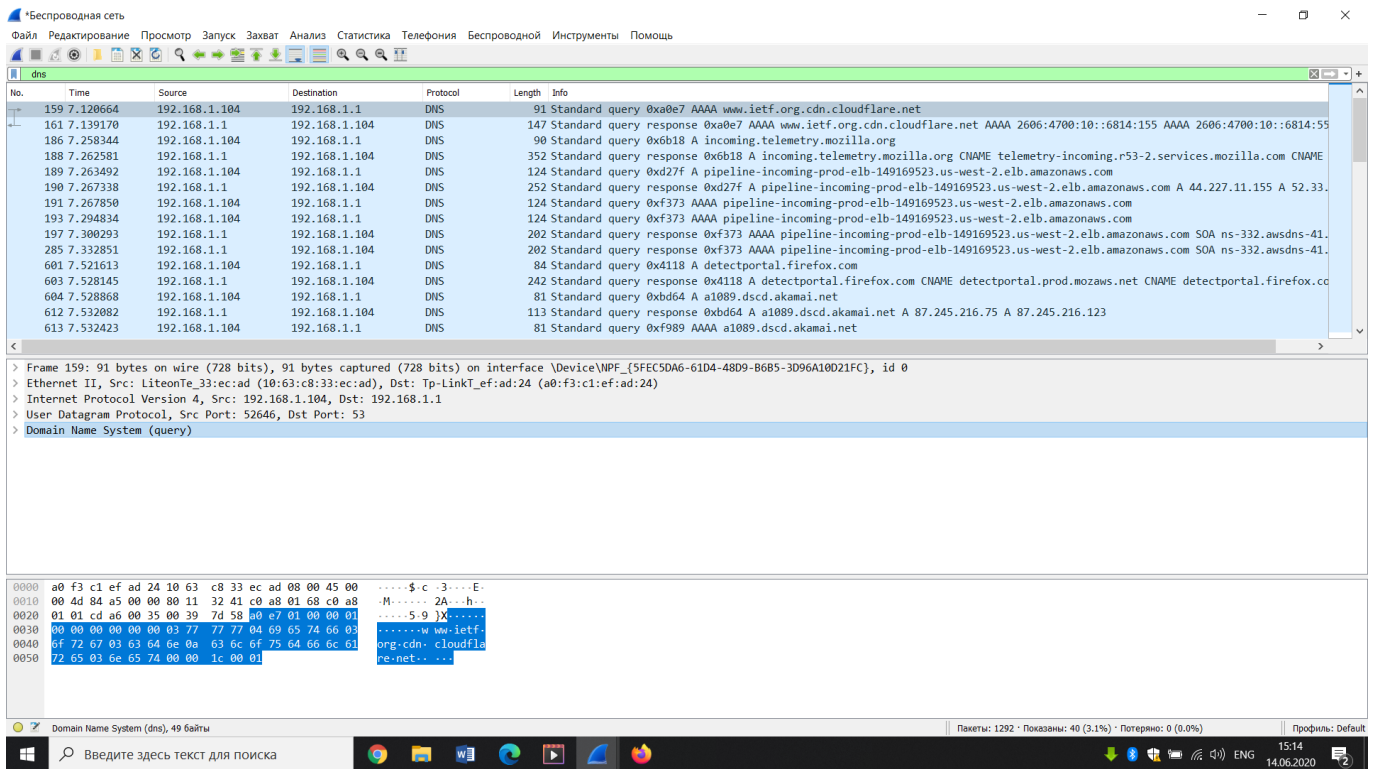


Рис. 2

8. Почнемо захоплення пакетів.

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

а. `Nslookup` `www.mit.edu`

кожну хвилину) – почніть спочатку та виконайте кроки 1,2,3 та 8.

10. Зупиняємо захоплення пакетів.

11. Готуйте відповіді на контрольні запитання 7-10, друкуємо 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

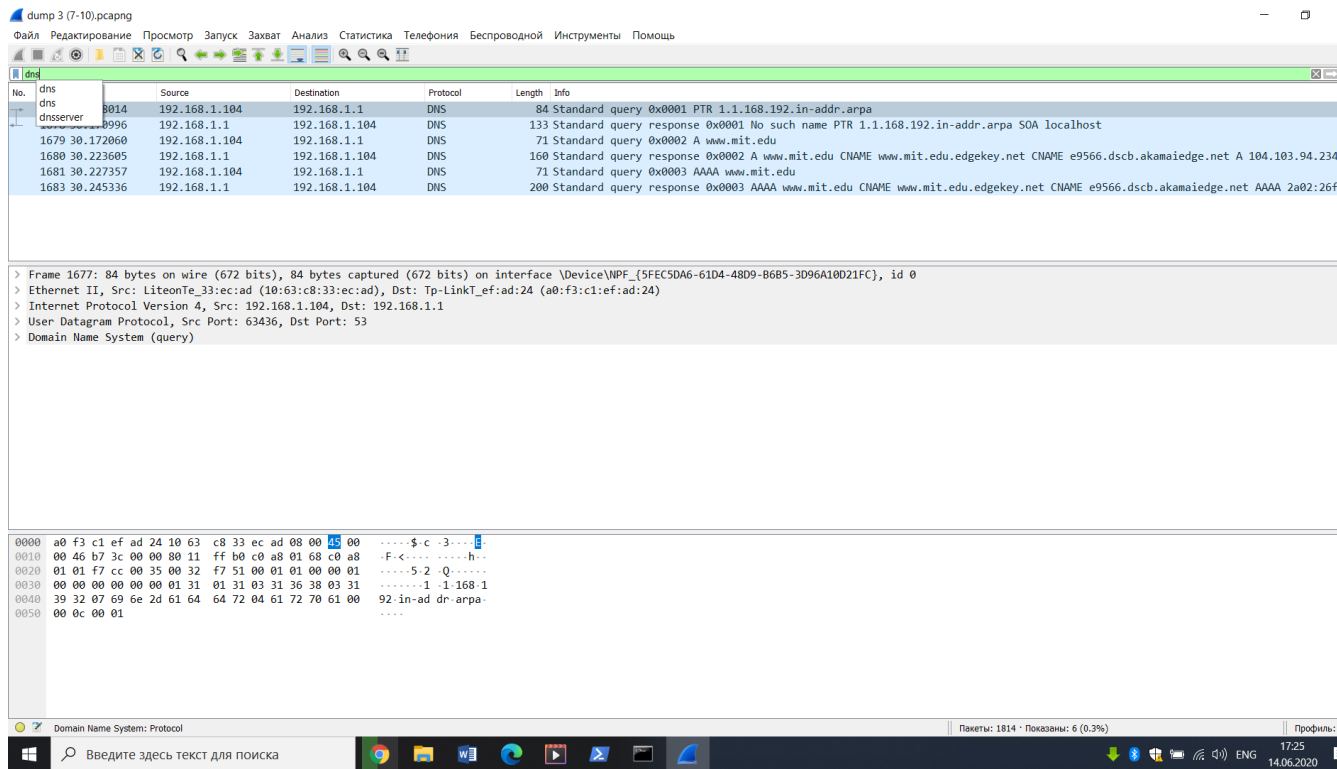


Рис. 3

12. Почнемо захоплення пакетів
13. Виконаємо nslookup для домену `www.mit.edu` за допомогою команди  
а. `nslookup -type=NS mit.edu`
14. Зупиняємо захоплення пакетів
15. Готуємо відповіді на запитання 11-13. При необхідності, роздрукуємо деякі захоплені пакети
16. Почнемо захоплення пакетів
17. Виконуємо nslookup для домену `www.mit.edu` за допомогою команди  
а. `nslookup www.aiit.or.kr bitsy.mit.edu`
18. Зупиняємо захоплення пакетів.
19. Готуємо відповіді на запитання 14-16. Друкуємо деякі захоплені пакети
20. Готуємо відповіді на запитання 16, 17. Друкуємо необхідні для цього пакети.
21. Закриваємо Wireshark.

### 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?

Відповідь: DNS використовує прототокол UDP: User Datagram Protocol,  
Source Port: 52646, Destination Port: 53

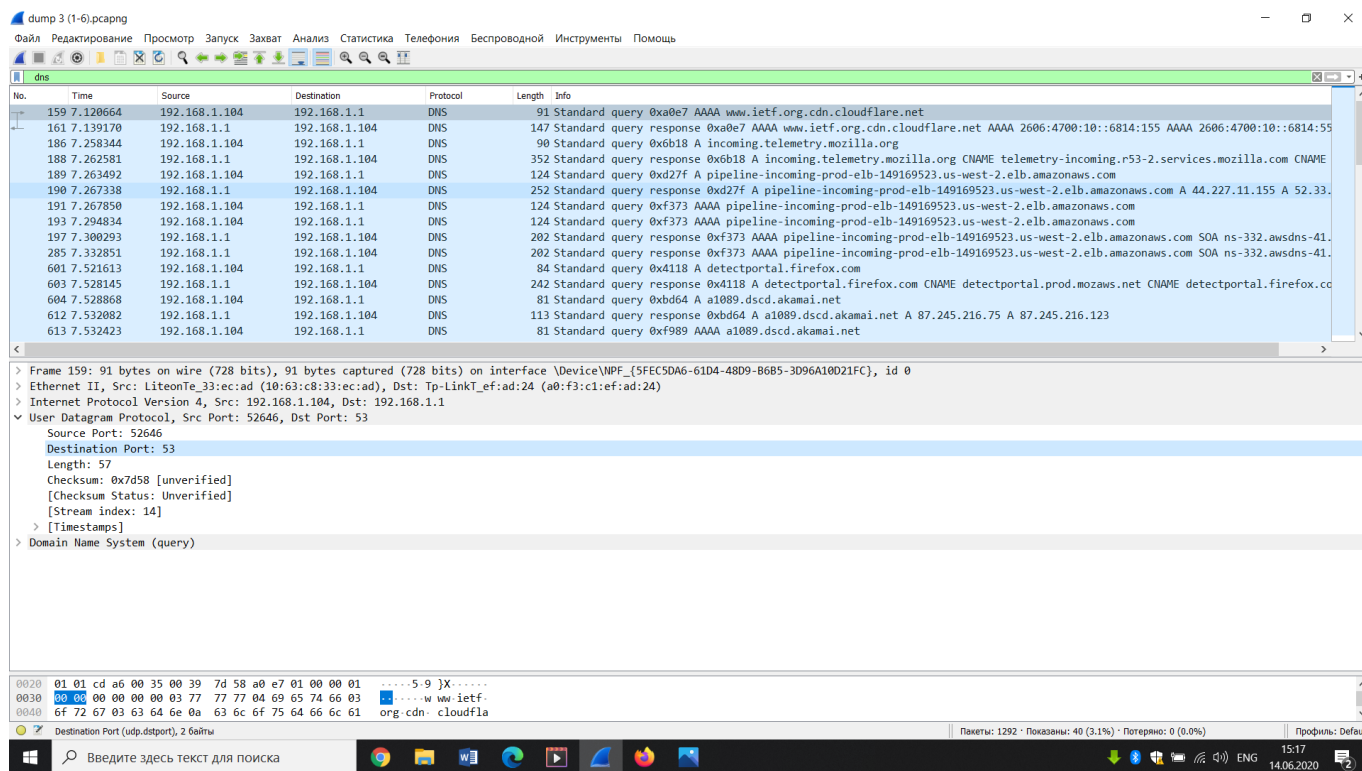


Рис.

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

Відповідь: Destination: 192.168.1.1 – є адресою локального DNS сервера

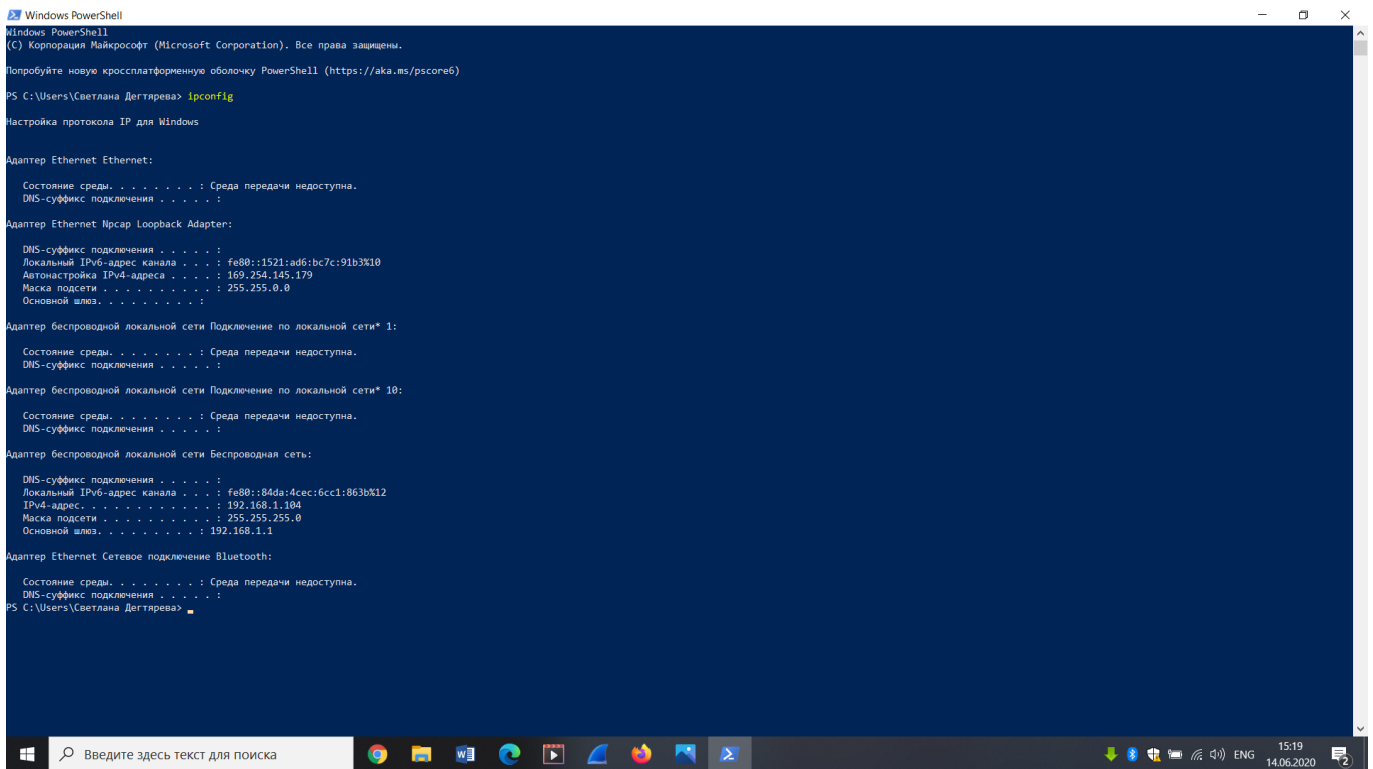


Рис.

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

Відповідь: Запит type AAAA; Має ссилку на відповідь: Response In: 161.

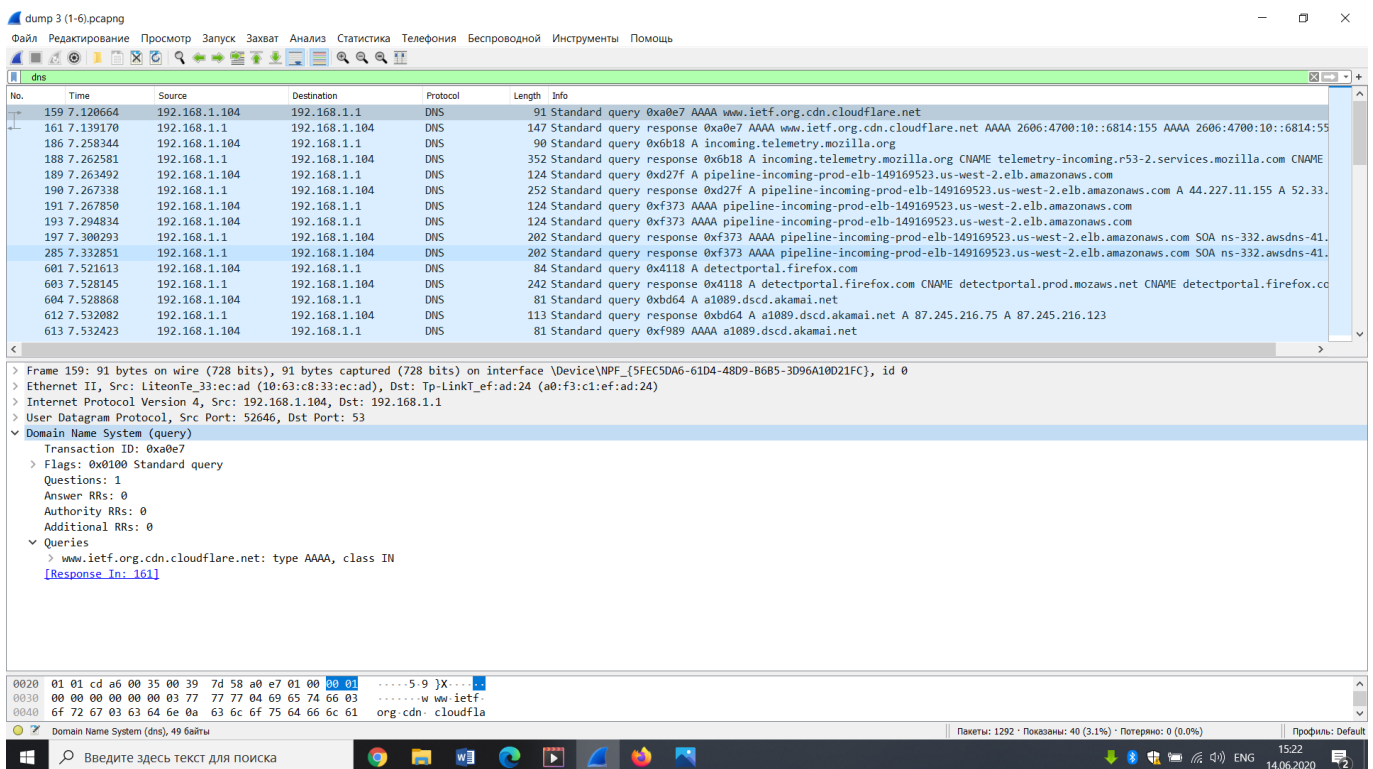


Рис.

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

Відповідь: Запропоновано 2 відповіді:

www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:155

www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:55

Кожна з відповідей містить наступні поля: Name, Type, Class, TTL, Data length AAAA Address;

Приклад відповіді:

Name: www.ietf.org.cdn.cloudflare.net

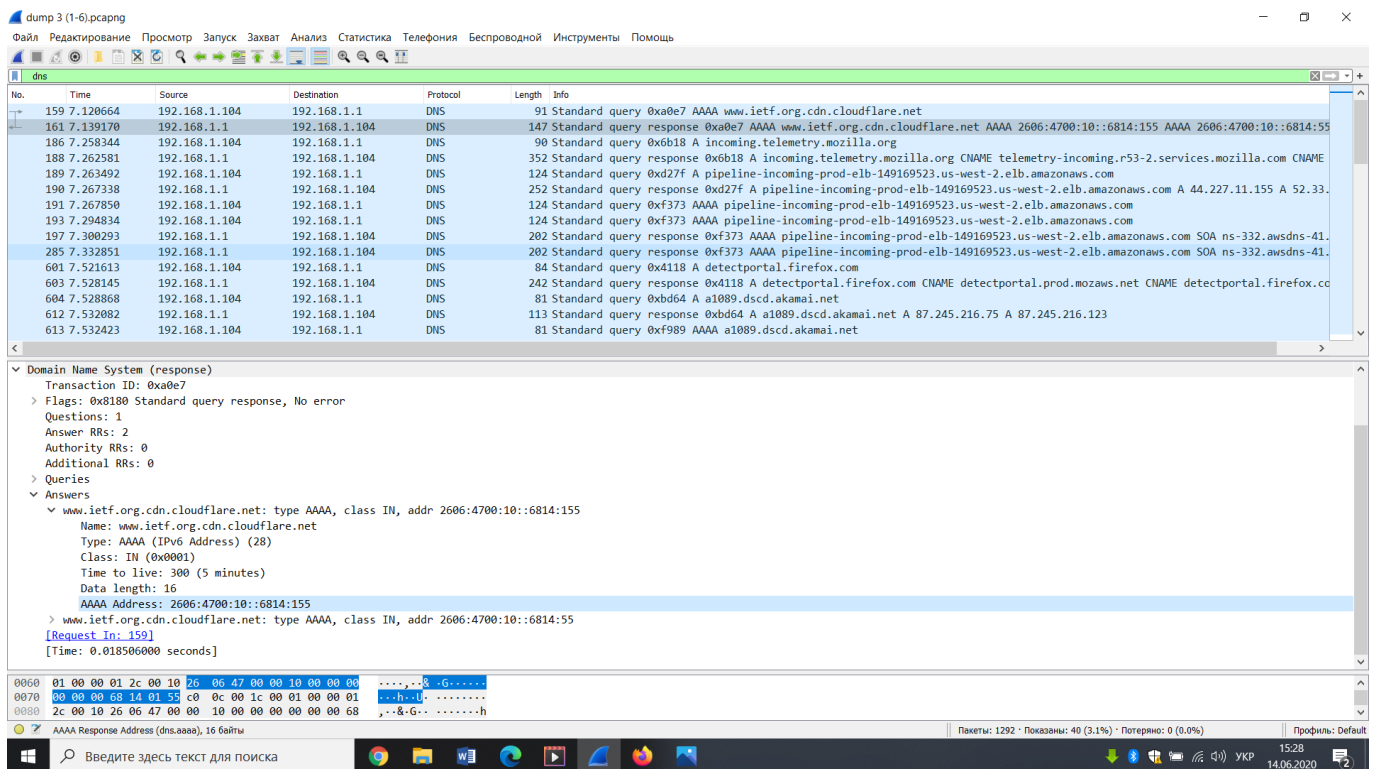
Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 16

AAAA Address: 2606:4700:10::6814:155



Мал. 6

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: 192.168.1.104 співпадає з однією з запропонованих відповідей сервера DNS.

dump 3 (1-6).pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-F>

| No. | Time     | Source         | Destination    | Protocol | Length | Info                                                                                       |
|-----|----------|----------------|----------------|----------|--------|--------------------------------------------------------------------------------------------|
| 373 | 7.357120 | 104.20.1.85    | 192.168.1.104  | SSLv2    | 1514   | Encrypted Data, Continuation Data                                                          |
| 472 | 7.378331 | 104.20.1.85    | 192.168.1.104  | SSLv2    | 1514   | Encrypted Data, Continuation Data                                                          |
| 541 | 7.398619 | 104.20.1.85    | 192.168.1.104  | SSLv2    | 1514   | Encrypted Data, Continuation Data                                                          |
| 2   | 0.177121 | 176.14.202.201 | 192.168.1.104  | TCP      | 68     | 49895 → 41374 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                      |
| 3   | 0.313036 | 192.168.1.104  | 37.215.15.134  | TCP      | 66     | 53988 → 63146 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                      |
| 4   | 0.373004 | 37.79.140.85   | 192.168.1.104  | TCP      | 68     | 1267 → 41374 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=4 SACK_PERM=1                          |
| 5   | 0.441228 | 176.46.208.69  | 192.168.1.104  | TCP      | 68     | 2502 → 41374 [SYN] Seq=0 Win=8192 Len=0 MSS=1452 WS=4 SACK_PERM=1                          |
| 6   | 0.659663 | 176.103.214.33 | 192.168.1.104  | TCP      | 68     | 7958 → 41374 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                       |
| 7   | 0.753126 | 62.33.11.136   | 192.168.1.104  | TCP      | 68     | 56427 → 41374 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                      |
| 8   | 0.766969 | 176.52.96.197  | 192.168.1.104  | TCP      | 64     | 1710 → 41374 [SYN] Seq=0 Win=64240 Len=0 MSS=1360 SACK_PERM=1                              |
| 10  | 0.837148 | 37.215.181.64  | 192.168.1.104  | TCP      | 68     | 50033 → 41374 [SYN] Seq=0 Win=64240 Len=0 MSS=1452 WS=256 SACK_PERM=1                      |
| 12  | 1.015246 | 89.223.115.69  | 192.168.1.104  | TCP      | 68     | 44880 → 41374 [SYN] Seq=0 Win=64240 Len=0 MSS=1400 WS=256 SACK_PERM=1                      |
| 13  | 1.173236 | 176.14.202.201 | 192.168.1.104  | TCP      | 68     | [TCP Retransmission] 49895 → 41374 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 14  | 1.265367 | 46.147.12.33   | 192.168.1.104  | TCP      | 68     | 54185 → 41374 [SYN] Seq=0 Win=8192 Len=0 MSS=1452 WS=4 SACK_PERM=1                         |
| 15  | 1.313171 | 192.168.1.104  | 37.215.15.134  | TCP      | 66     | [TCP Retransmission] 53988 → 63146 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 18  | 1.315190 | 192.168.1.104  | 93.171.229.193 | TCP      | 66     | 53989 → 35120 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                      |
| 19  | 1.315710 | 192.168.1.104  | 94.179.148.159 | TCP      | 66     | 53990 → 19209 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                      |
| 20  | 1.316156 | 192.168.1.104  | 178.71.52.156  | TCP      | 66     | 53991 → 10720 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                      |
| 24  | 1.374682 | 94.179.148.159 | 192.168.1.104  | TCP      | 68     | 19209 → 53990 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1412 WS=1 SACK_PERM=1             |
| 25  | 1.374864 | 192.168.1.104  | 94.179.148.159 | TCP      | 54     | 53990 → 19209 [ACK] Seq=1 Ack=1 Win=131072 Len=0                                           |
| 31  | 1.429174 | 94.179.148.159 | 192.168.1.104  | TCP      | 56     | 19209 → 53990 [RST] Seq=1 Win=0 Len=0                                                      |
| 32  | 1.429178 | 94.179.148.159 | 192.168.1.104  | TCP      | 56     | 19209 → 53990 [RST] Seq=1 Win=0 Len=0                                                      |

> Frame 13: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF\_{5FEC5DA6-61D4-48D9-B6B5-3D96A10021FC}, id 0  
 > Ethernet II, Src: Tp-LinkT\_ef:ad:24 (a0:f3:c1:ef:ad:24), Dst: LiteonTe\_33:ec:ad (10:63:c8:33:ec:ad)  
 > Internet Protocol Version 4, Src: 176.14.202.201, Dst: 192.168.1.104  
 > Transmission Control Protocol, Src Port: 49895, Dst Port: 41374, Seq: 0, Len: 0  
 > VSS Monitoring Ethernet trailer, Source Port: 35712

0000 10 63 c8 33 ec ad a0 f3 c1 ef ad 24 08 00 45 00 c:3...:..\$..E..  
 0010 00 34 57 26 40 00 6e 0e 78 b5 0e ca c9 c0 a8 4w&@.n.x.....  
 0020 01 68 c2 e7 a1 9e 15 4a bc c7 00 00 00 00 80 02 h.....J.....

dump 3 (1-6).pcapng

Пакеты: 1292 · Показаны: 1292 (100.0%) · Потеряно: 0 (0.0%) · Профиль: Default

Введите здесь текст для поиска

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

Відповідь: так.

dump 3 (1-6).pcapng

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

| No.  | Time     | Source        | Destination   | Protocol | Length | Info                                                                                                                       |
|------|----------|---------------|---------------|----------|--------|----------------------------------------------------------------------------------------------------------------------------|
| 159  | 7.120664 | 192.168.1.104 | 192.168.1.1   | DNS      | 91     | Standard query 0xa0e7 AAAA www.ietf.org.cdn.cloudflare.net                                                                 |
| 161  | 7.139170 | 192.168.1.1   | 192.168.1.104 | DNS      | 147    | Standard query response 0xa0e7 AAAA www.ietf.org.cdn.cloudflare.net AAAA 2606:4700:10::6814:155 AAAA 2606:4700:10::6814:55 |
| 186  | 7.258344 | 192.168.1.104 | 192.168.1.1   | DNS      | 90     | Standard query 0x6b18 A incoming.telemetry.mozilla.org                                                                     |
| 188  | 7.262581 | 192.168.1.1   | 192.168.1.104 | DNS      | 352    | Standard query response 0x6b18 A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.services.mozilla.com CNAME  |
| 189  | 7.263492 | 192.168.1.104 | 192.168.1.1   | DNS      | 124    | Standard query 0xd27f A pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com                                   |
| 190  | 7.267338 | 192.168.1.1   | 192.168.1.104 | DNS      | 252    | Standard query response 0xd27f A pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com A 44.227.11.155 A 52.33. |
| 191  | 7.267890 | 192.168.1.104 | 192.168.1.1   | DNS      | 124    | Standard query 0xf373 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com                                |
| 193  | 7.294834 | 192.168.1.104 | 192.168.1.1   | DNS      | 124    | Standard query 0xf373 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com                                |
| 197  | 7.300293 | 192.168.1.1   | 192.168.1.104 | DNS      | 202    | Standard query response 0xf373 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com SOA ns-332.awsdns-41. |
| 285  | 7.332851 | 192.168.1.1   | 192.168.1.104 | DNS      | 202    | Standard query response 0xf373 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com SOA ns-332.awsdns-41. |
| 601  | 7.521613 | 192.168.1.104 | 192.168.1.1   | DNS      | 84     | Standard query 0xd118 A detectportal.firefox.com                                                                           |
| 603  | 7.528145 | 192.168.1.1   | 192.168.1.104 | DNS      | 242    | Standard query response 0xd118 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.co |
| 604  | 7.528068 | 192.168.1.104 | 192.168.1.1   | DNS      | 81     | Standard query 0xbd64 A a1089.dscd.akamai.net                                                                              |
| 612  | 7.532082 | 192.168.1.1   | 192.168.1.104 | DNS      | 113    | Standard query response 0xbd64 A a1089.dscd.akamai.net A 87.245.216.75 A 87.245.216.123                                    |
| 613  | 7.532423 | 192.168.1.104 | 192.168.1.1   | DNS      | 81     | Standard query 0xf989 AAAA a1089.dscd.akamai.net                                                                           |
| 616  | 7.540629 | 192.168.1.104 | 192.168.1.1   | DNS      | 71     | Standard query 0xe879 A mozilla.org                                                                                        |
| 618  | 7.542295 | 192.168.1.104 | 192.168.1.1   | DNS      | 84     | Standard query 0xac8e A detectportal.firefox.com                                                                           |
| 619  | 7.550327 | 192.168.1.1   | 192.168.1.104 | DNS      | 137    | Standard query response 0xf989 AAAA a1089.dscd.akamai.net AAAA 2a02:2d8:0:9008::57f5:d87b AAAA 2a02:2d8:0:9008::57f5:d84b  |
| 620  | 7.550466 | 192.168.1.1   | 192.168.1.104 | DNS      | 242    | Standard query response 0xac8e A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.co |
| 621  | 7.550583 | 192.168.1.1   | 192.168.1.104 | DNS      | 87     | Standard query response 0xe879 A mozilla.org A 63.245.208.195                                                              |
| 630  | 7.577688 | 192.168.1.104 | 192.168.1.1   | DNS      | 78     | Standard query 0xf9ad A analytics.ietf.org                                                                                 |
| 646  | 7.600288 | 192.168.1.104 | 192.168.1.1   | DNS      | 78     | Standard query 0xf9ad A analytics.ietf.org                                                                                 |
| 1164 | 8.093182 | 192.168.1.1   | 192.168.1.104 | DNS      | 108    | Standard query response 0xf9ad A analytics.ietf.org CNAME ietf.org A 4.31.198.44                                           |
| 1165 | 8.093383 | 192.168.1.1   | 192.168.1.104 | DNS      | 108    | Standard query response 0xf9ad A analytics.ietf.org CNAME ietf.org A 4.31.198.44                                           |
| 1167 | 8.096086 | 192.168.1.104 | 192.168.1.1   | DNS      | 68     | Standard query 0x4c40 A ietf.org                                                                                           |
| 1168 | 8.120092 | 192.168.1.104 | 192.168.1.1   | DNS      | 68     | Standard query 0x4c40 A ietf.org                                                                                           |
| 1184 | 8.390255 | 192.168.1.1   | 192.168.1.104 | DNS      | 84     | Standard query response 0x4c40 A ietf.org A 4.31.198.44                                                                    |

> Frame 159: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF\_{5FEC5DA6-61D4-48D9-B6B5-3D96A10021FC}, id 0  
 > Ethernet II, Src: LiteonTe\_33:ec:ad (10:63:c8:33:ec:ad), Dst: Tp-LinkT\_ef:ad:24 (a0:f3:c1:ef:ad:24)  
 > Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.1  
 > User Datagram Protocol, Src Port: 52646, Dst Port: 53  
 > Domain Name System (query)  
 Transaction ID: 0xa0e7  
 > Flags: 0x0100 Standard query  
 Questions: 1  
 Answer RRs: 0  
 Authority RRs: 0

Domain Name System: Protocol

Пакеты: 1292 · Показаны: 40 (3.1%) · Потеряно: 0 (0.0%) · Профиль: Default

Введите здесь текст для поиска



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

Відповідь: Порти у запиті: Source Port: 63437; Destination Port: 53;

Порти у відповіді: Source Port: 53; Destination Port: 63437.

```

Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/powershell)

PS C:\Users\Светлана Дегтярева> ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.
PS C:\Users\Светлана Дегтярева> nslookup www.mit.edu
Server: UnKnown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Server: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d8:3a2::259e
           2a02:26f0:d8:3a3::235e
           104.103.94.234
Aliases: www.mit.edu
          www.mit.edu.edgekey.net

PS C:\Users\Светлана Дегтярева>
  
```

Мал. 8

Wireshark packet capture details for a DNS query and response. The packet list shows a query from 192.168.1.104 to 192.168.1.1 and a response from 192.168.1.1 to 192.168.1.104.

| No.  | Time      | Source        | Destination   | Protocol | Length | Info                                                                                                                                      |
|------|-----------|---------------|---------------|----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 1679 | 30.172060 | 192.168.1.104 | 192.168.1.1   | DNS      | 71     | Standard query 0x0002 A www.mit.edu                                                                                                       |
| 1680 | 30.223605 | 192.168.1.1   | 192.168.1.104 | DNS      | 160    | Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.103.94.234               |
| 1681 | 30.227357 | 192.168.1.104 | 192.168.1.1   | DNS      | 71     | Standard query 0x0003 AAAA www.mit.edu                                                                                                    |
| 1683 | 30.245336 | 192.168.1.1   | 192.168.1.104 | DNS      | 200    | Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:d8:3a2::259e |

Packet 1680 details:

- Frame 1679: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{5FEC5DA6-6104-4809-B685-3D96A10021FC}, id 0
- Ethernet II, Src: LiteonTe\_33:ec:ad (10:63:c8:33:ec:ad), Dst: Tp-LinkT\_ef:ad:24 (a0:f3:c1:ef:ad:24)
- Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 63437, Dst Port: 53
  - Source Port: 63437
  - Destination Port: 53
  - Length: 37
  - Checksum: 0x313a [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 322]
  - [Timestamps]
- Domain Name System (query)

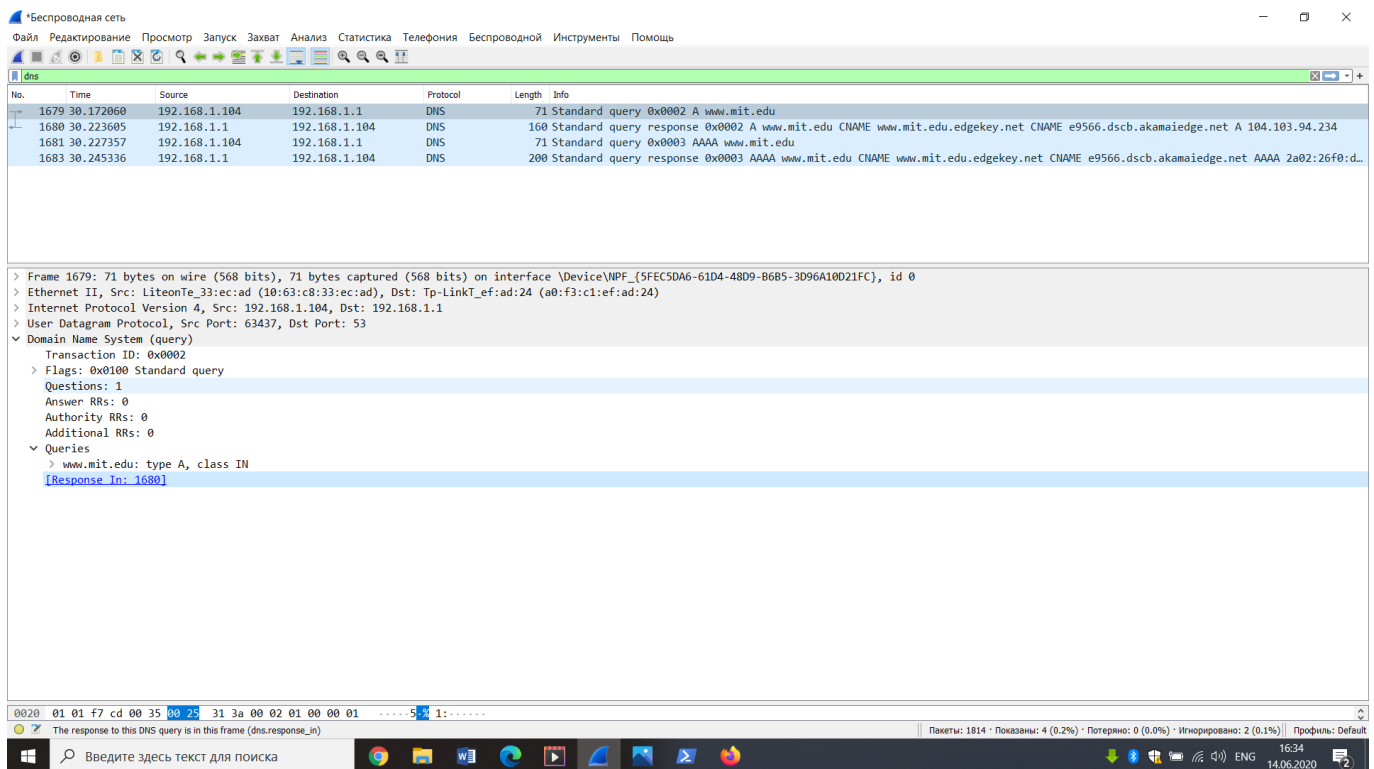
## Мал. 9

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

Відповідь: Destination: 192.168.1.1 – це є адреса локального сервера DNS за замовчанням.

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

Відповідь: Це був запит type A. Має ссилку на відповідь: Response In: 1680



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

Відповідь: Було взагалі 2 запита та 2 відповіді. У останній відповіді було запропоновано 4 запису. Кожна з відповідей складається з :

для А– було 3 відповіді:

www.mit.edu: type CNAME, class IN, cname [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net)

www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 104.103.94.234

Відповідь www.mit.edu: type CNAME, class IN, cname [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net)  
складається з:

Name: [www.mit.edu](http://www.mit.edu)

Type: CNAME (Canonical NAME for an alias) (5)

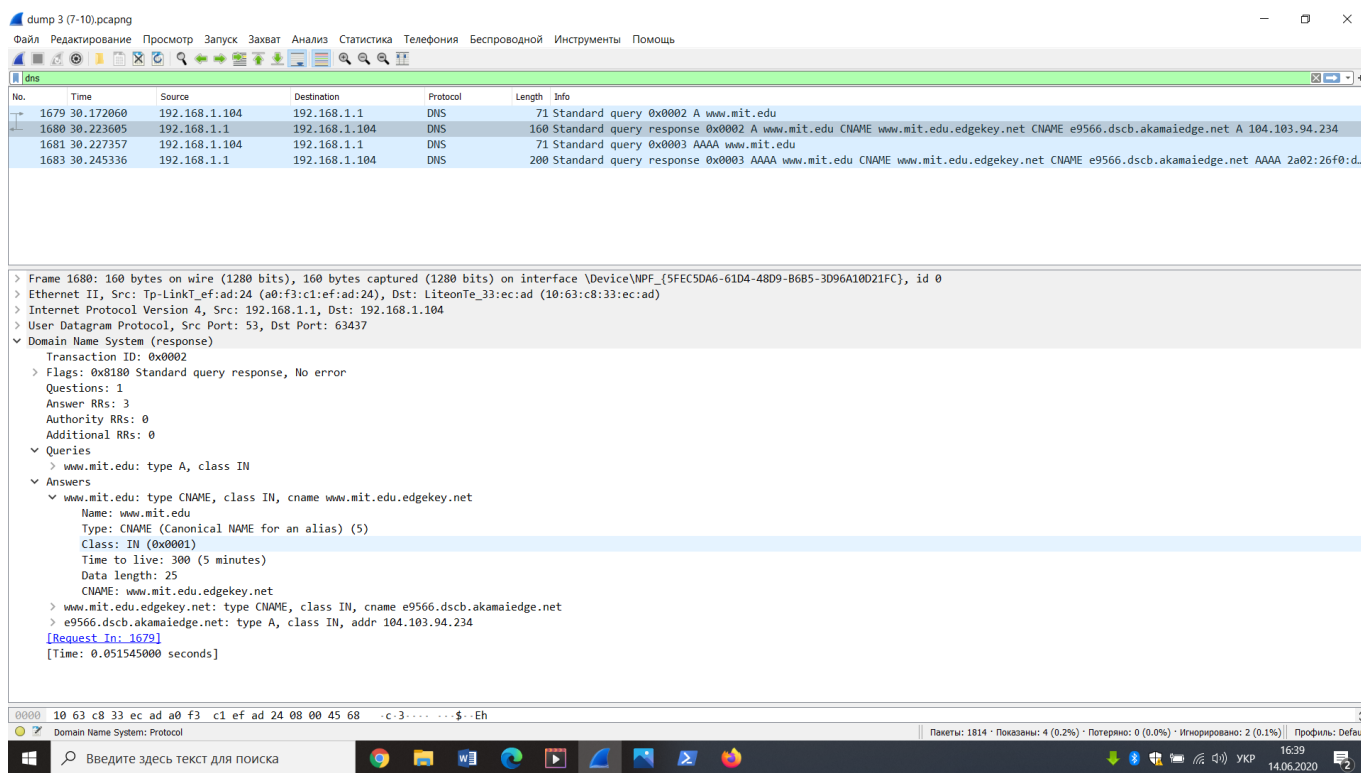
Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 25

CNAME: www.mit.edu.edgekey.net

для типу AAAA – 4 відповіді;



Мал. 10

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

Відповідь: Destination: 192.168.0.1 – це є адреса локального сервера DNS за замовчанням

```

Windows PowerShell
mit.edu nameserver = ns1-173.akam.net
PS C:\Users\Светлана Дегтярева> ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.
PS C:\Users\Светлана Дегтярева> nslookup -type=NS mit.edu
Server: 192.168.1.1
Address: 192.168.1.1

Не заслуживающий доверия ответ:
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = asia1.akam.net
PS C:\Users\Светлана Дегтярева>

```

Мал. 11

Lab3\_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

| No. | Time     | Source        | Destination   | Protocol | Length | Info                                                                     |
|-----|----------|---------------|---------------|----------|--------|--------------------------------------------------------------------------|
| 4   | 3.843686 | 192.168.0.103 | 192.168.0.1   | DNS      | 84     | Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa                       |
| 5   | 3.847122 | 192.168.0.1   | 192.168.0.103 | DNS      | 143    | Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa |
| 6   | 3.848781 | 192.168.0.103 | 192.168.0.1   | DNS      | 83     | Standard query 0x0002 NS mit.edu.infopulse.local                         |
| 7   | 3.882274 | 192.168.0.1   | 192.168.0.103 | DNS      | 158    | Standard query response 0x0002 No such name NS mit.edu                   |
| 8   | 3.882897 | 192.168.0.103 | 192.168.0.1   | DNS      | 67     | Standard query 0x0003 NS mit.edu                                         |
| 9   | 3.902908 | 192.168.0.1   | 192.168.0.103 | DNS      | 234    | Standard query response 0x0003 NS mit.edu NS asia1.akam.net              |

< >

> Frame 4: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF\_{4411A0BE-7C39-4402-A536-A363854FC3CE}, id 0

> Ethernet II, Src: IntelCor\_ff:28:78 (d4:6d:6d:ff:28:78), Dst: Tp-LinkT\_63:b5:fc (18:a6:f7:63:b5:fc)

> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

> User Datagram Protocol, Src Port: 60746, 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

> 1.0.168.192.in-addr.arpa: type PTR, class IN

[Response In: 5]

0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92.in-ad dr.arpa.

0050 00 0c 00 01 ....

Query Type (dns.qry.type), 2 bytes

Packets: 12 · Displayed: 6 (50.0%) · Dropped: 0 (0.0%) · Profile: Default

Мал. 12

Lab3\_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

| No. | Time     | Source        | Destination   | Protocol | Length | Info                                                                     |
|-----|----------|---------------|---------------|----------|--------|--------------------------------------------------------------------------|
| 4   | 3.843686 | 192.168.0.103 | 192.168.0.1   | DNS      | 84     | Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa                       |
| 5   | 3.847122 | 192.168.0.1   | 192.168.0.103 | DNS      | 143    | Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa |
| 6   | 3.848781 | 192.168.0.103 | 192.168.0.1   | DNS      | 83     | Standard query 0x0002 NS mit.edu.infopulse.local                         |
| 7   | 3.882274 | 192.168.0.1   | 192.168.0.103 | DNS      | 158    | Standard query response 0x0002 No such name NS mit.edu.infopulse.local   |
| 8   | 3.882897 | 192.168.0.103 | 192.168.0.1   | DNS      | 67     | Standard query 0x0003 NS mit.edu                                         |
| 9   | 3.902908 | 192.168.0.1   | 192.168.0.103 | DNS      | 234    | Standard query response 0x0003 NS mit.edu NS asia1.akam.net              |

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 asia1.akam.net  
 Name: mit.edu  
 Type: NS (authoritative Name Server) (2)  
 Class: IN (0x0001)  
 Time to live: 770 (12 minutes, 50 seconds)  
 Data length: 16  
 Name Server: 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 usw2.akam.net  
 > mit.edu: type NS, class IN, ns use5.akam.net  
 > mit.edu: type NS, class IN, ns ns1-173.akam.net  
 > mit.edu: type NS, class IN, ns eur5.akam.net  
 > mit.edu: type NS, class IN, ns asia2.akam.net

[Request In: 8]  
 [Time: 0.020011000 seconds]

0040 02 00 01 c0 0c 00 02 00 01 00 00 03 02 00 10 05 .....  
 0050 61 73 69 61 31 04 61 6b 61 6d 03 6e 65 74 00 c0 asia1.akam.net.

Name Server (dns.ns), 16 bytes

Packets: 12 · Displayed: 6 (50.0%) · Dropped: 0 (0.0%) Profile: Default

Мал. 13