іністерство 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:

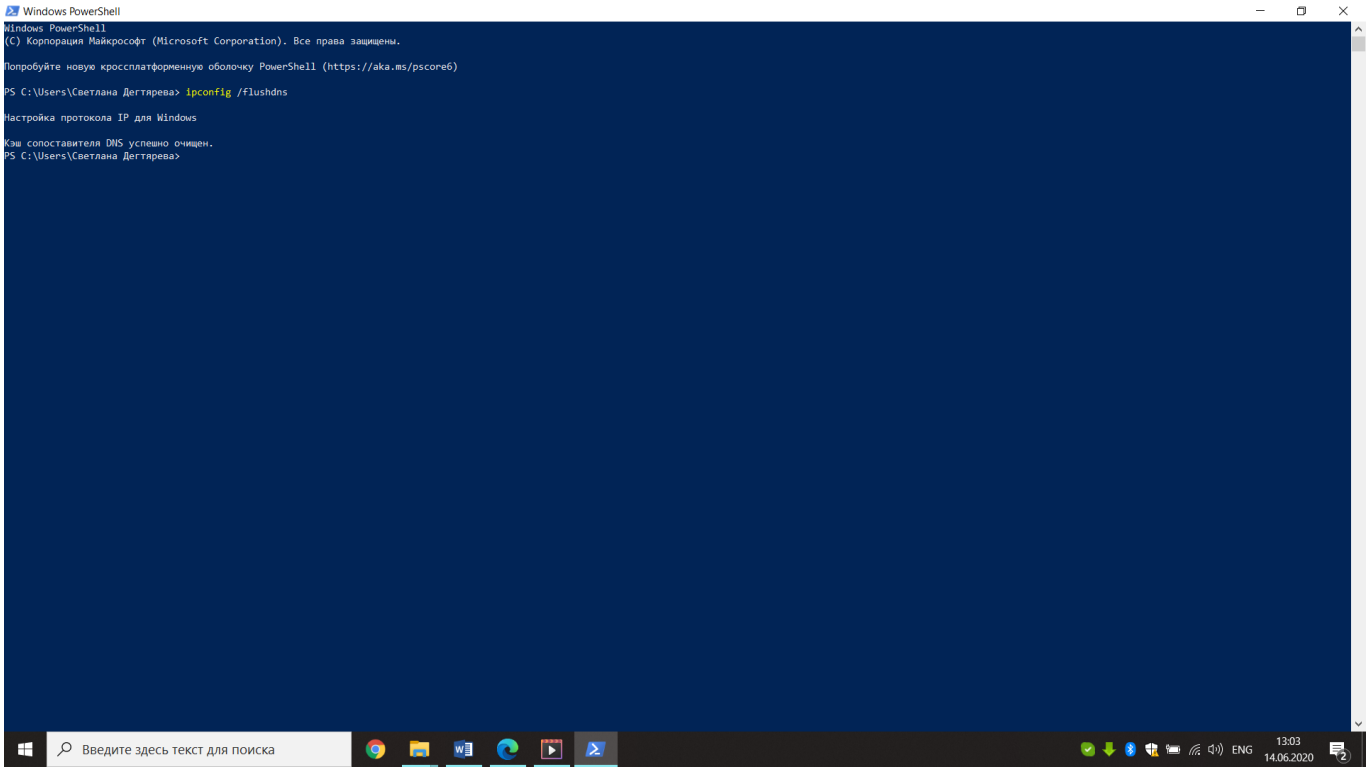


Рис. 1

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.

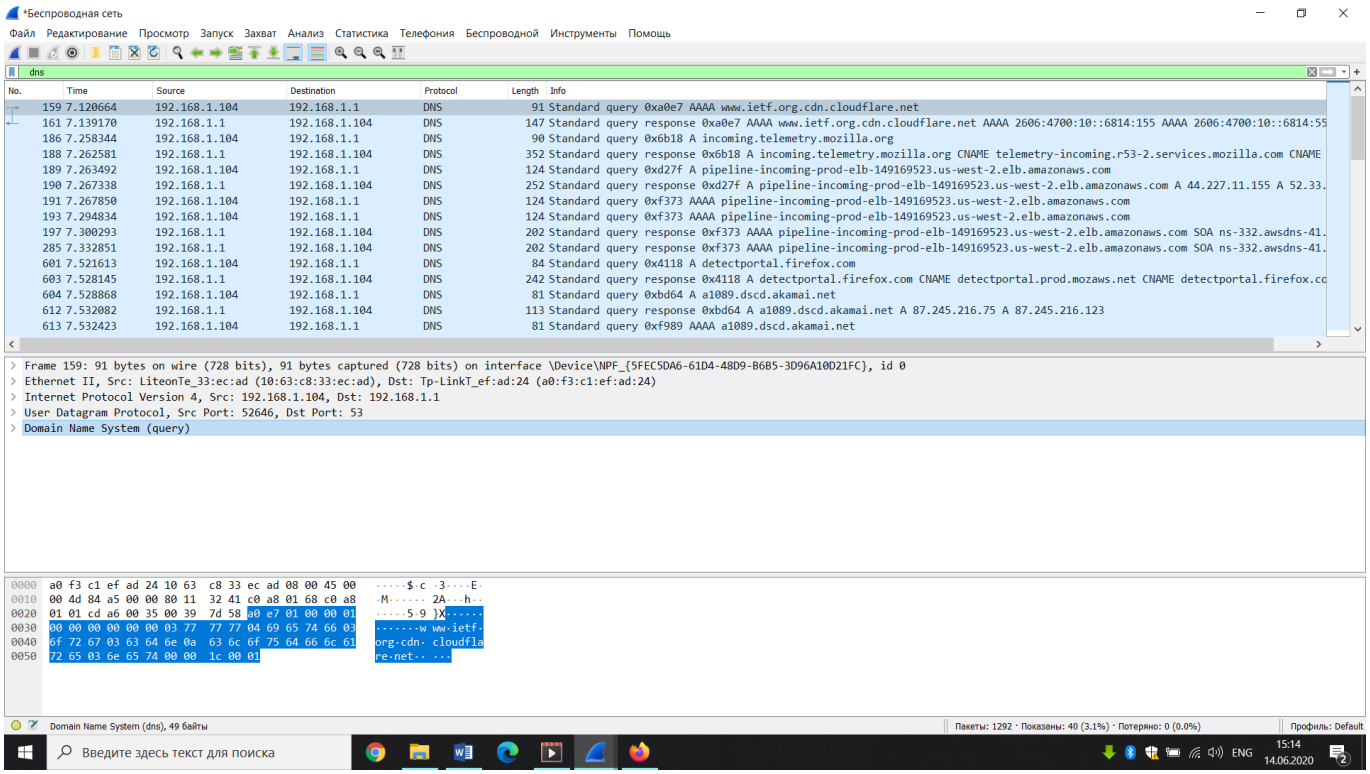


Рис. 2

8. Почнемо захоплення пакетів.

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

a. 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

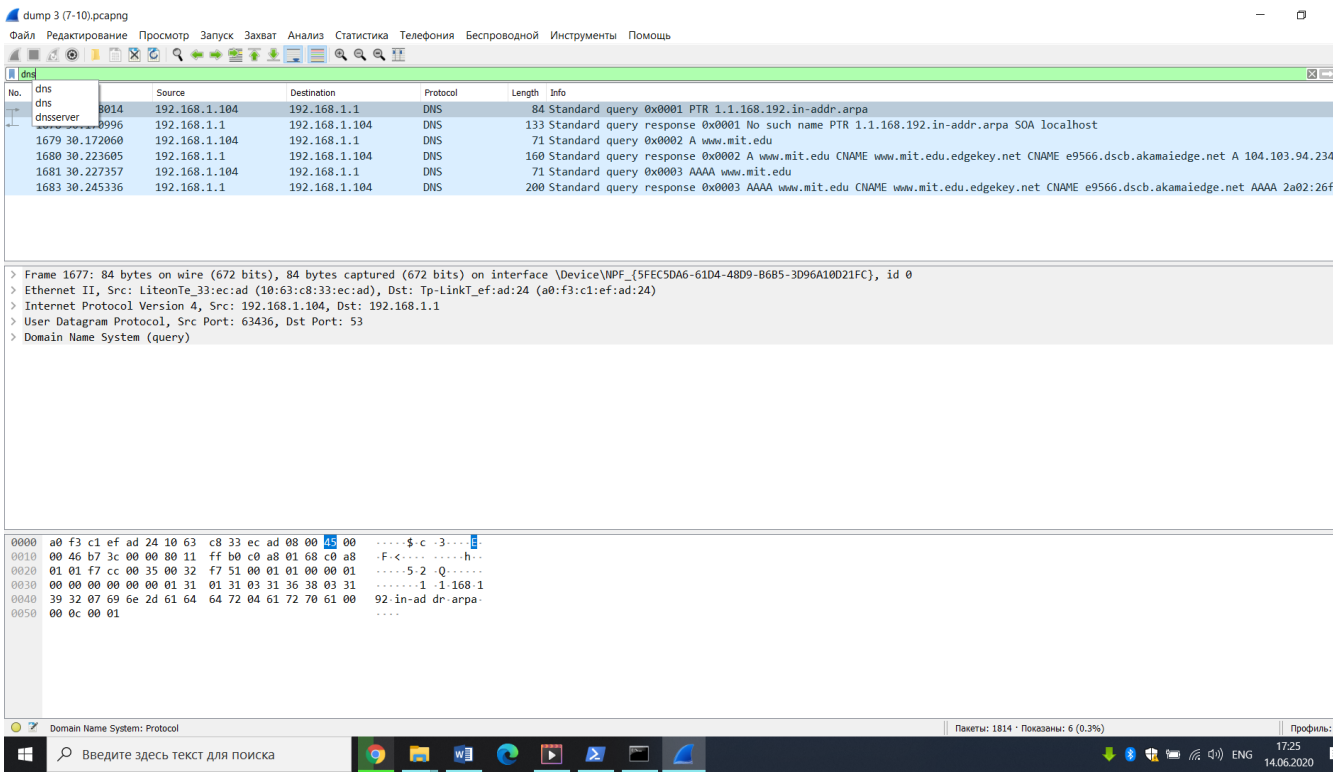


Рис. 3

12. Почнемо захоплення пакетів

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

a. 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

a. 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

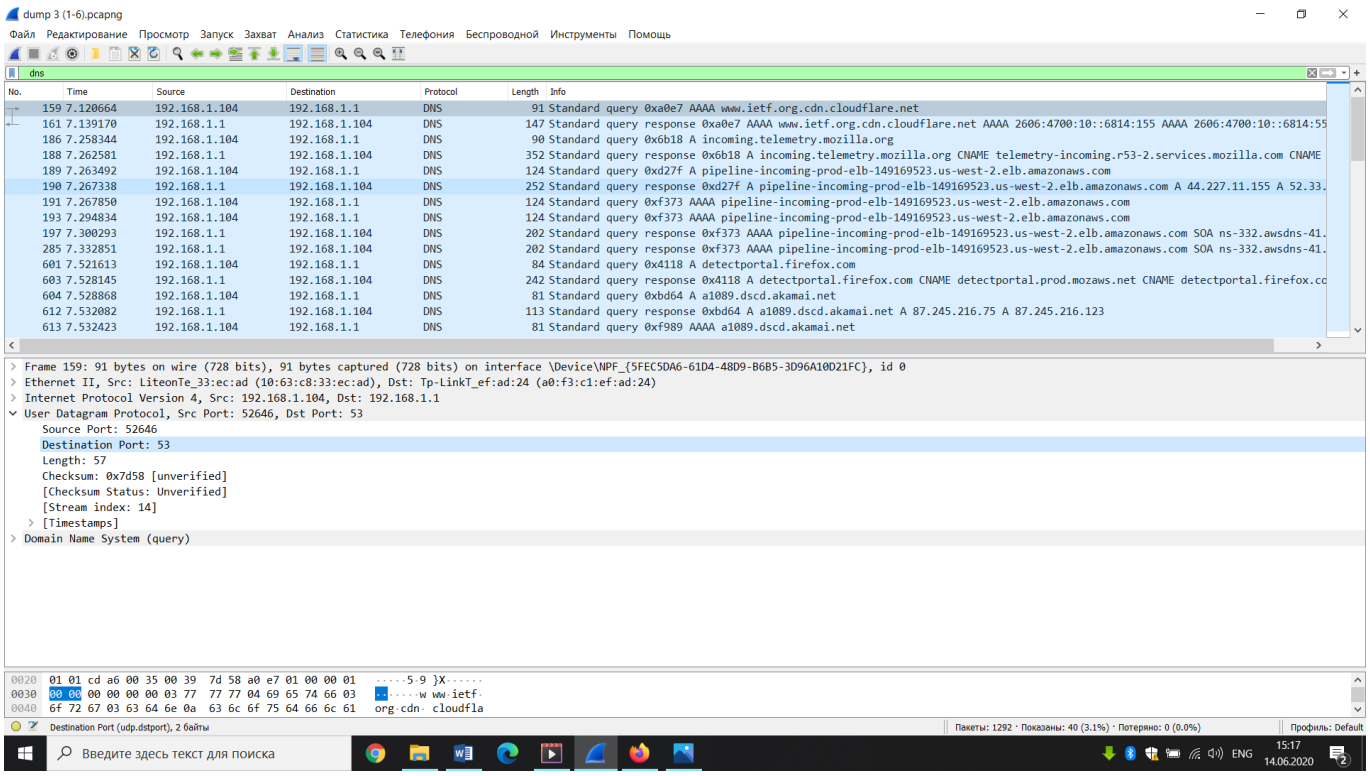


Рис.

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

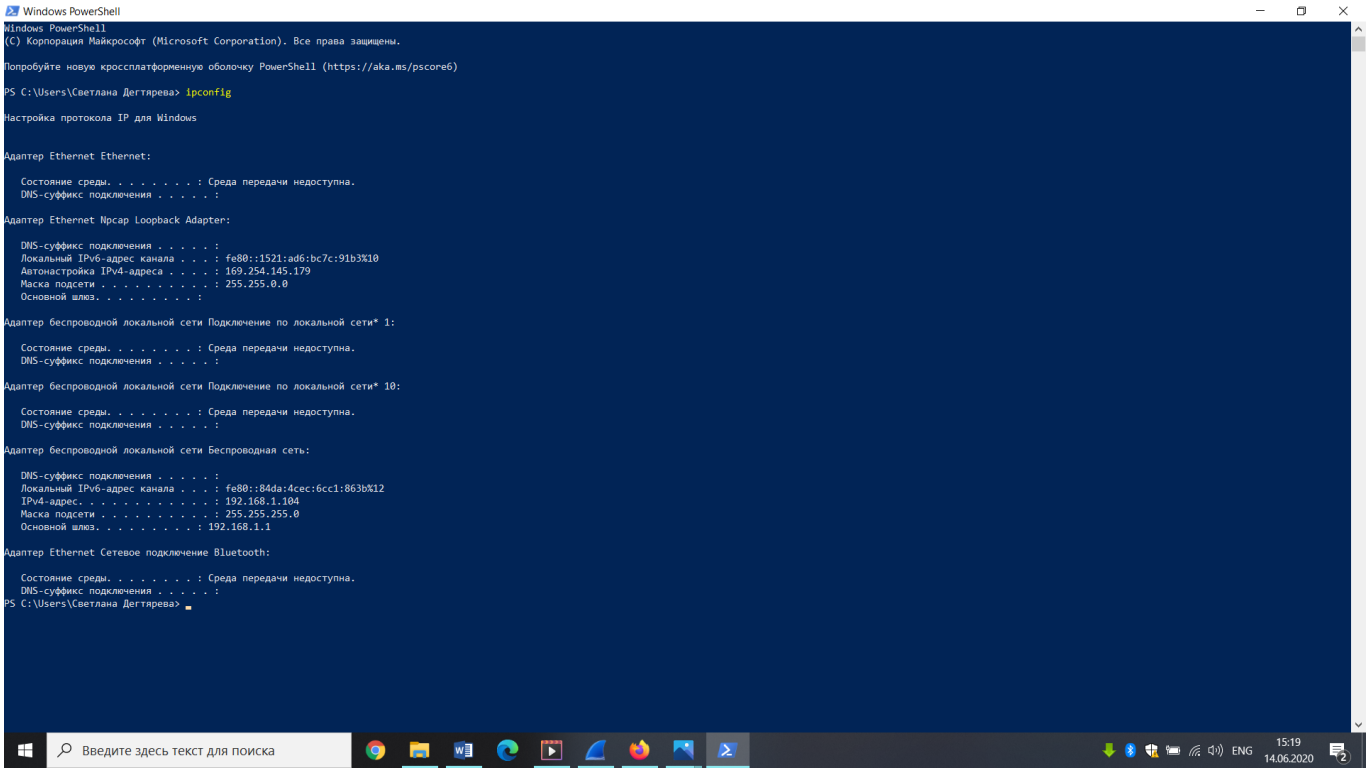


Рис.

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.

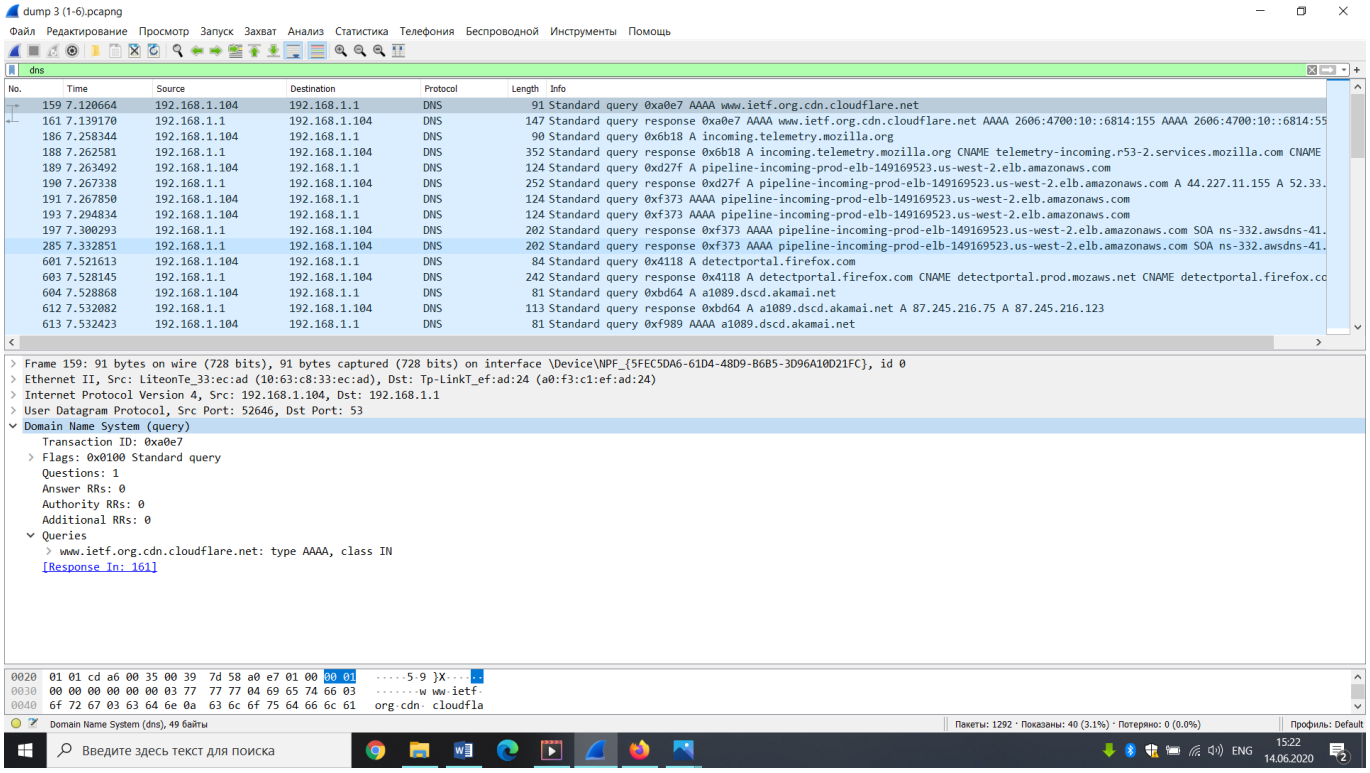


Рис.

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

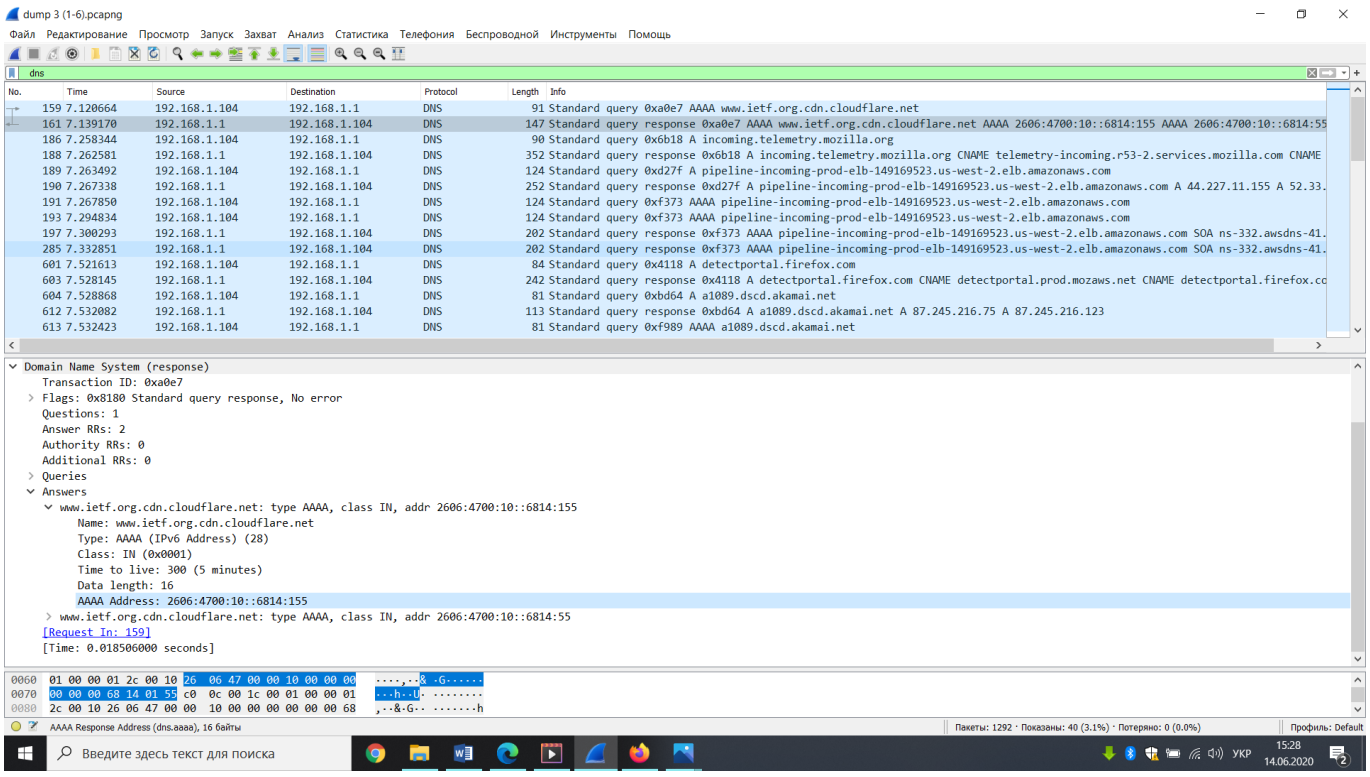
Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 16

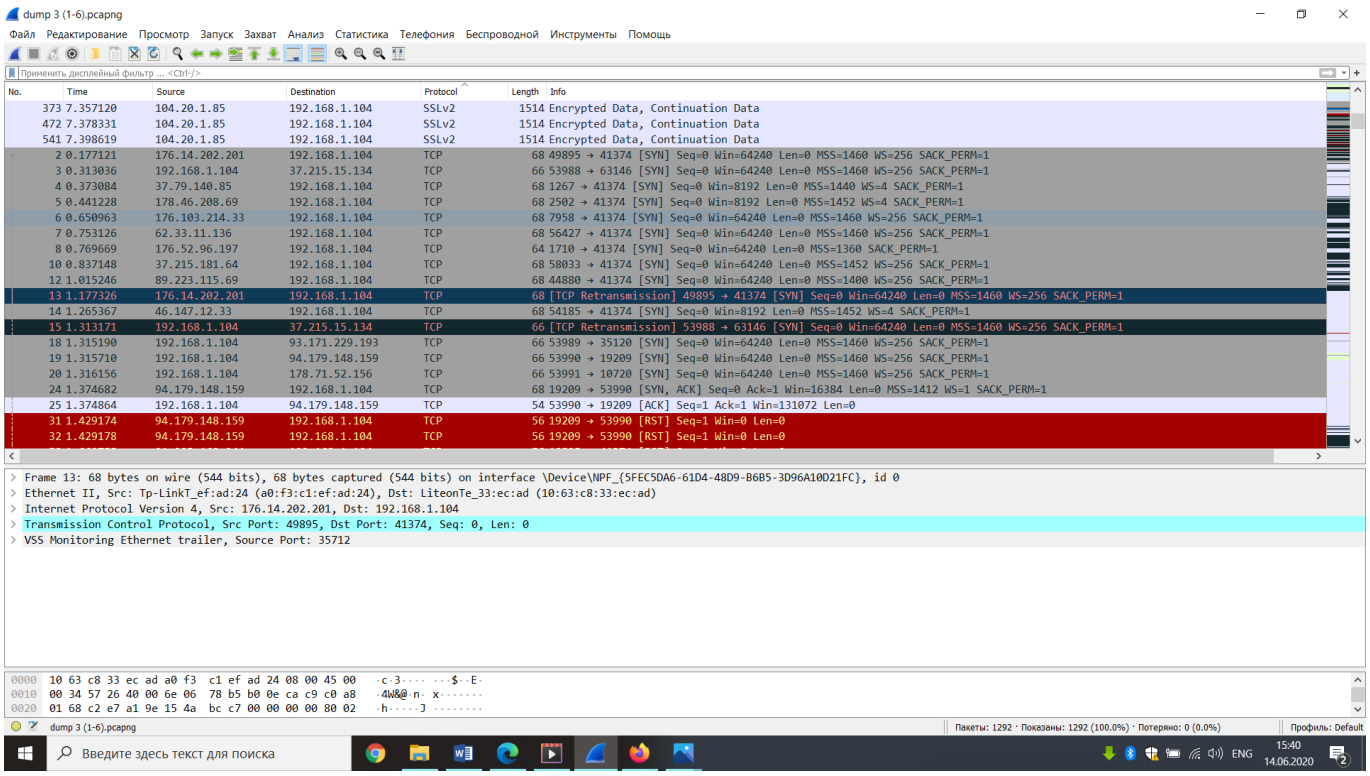
AAAA Address: 2606:4700:10::6814:155



Мал. 6

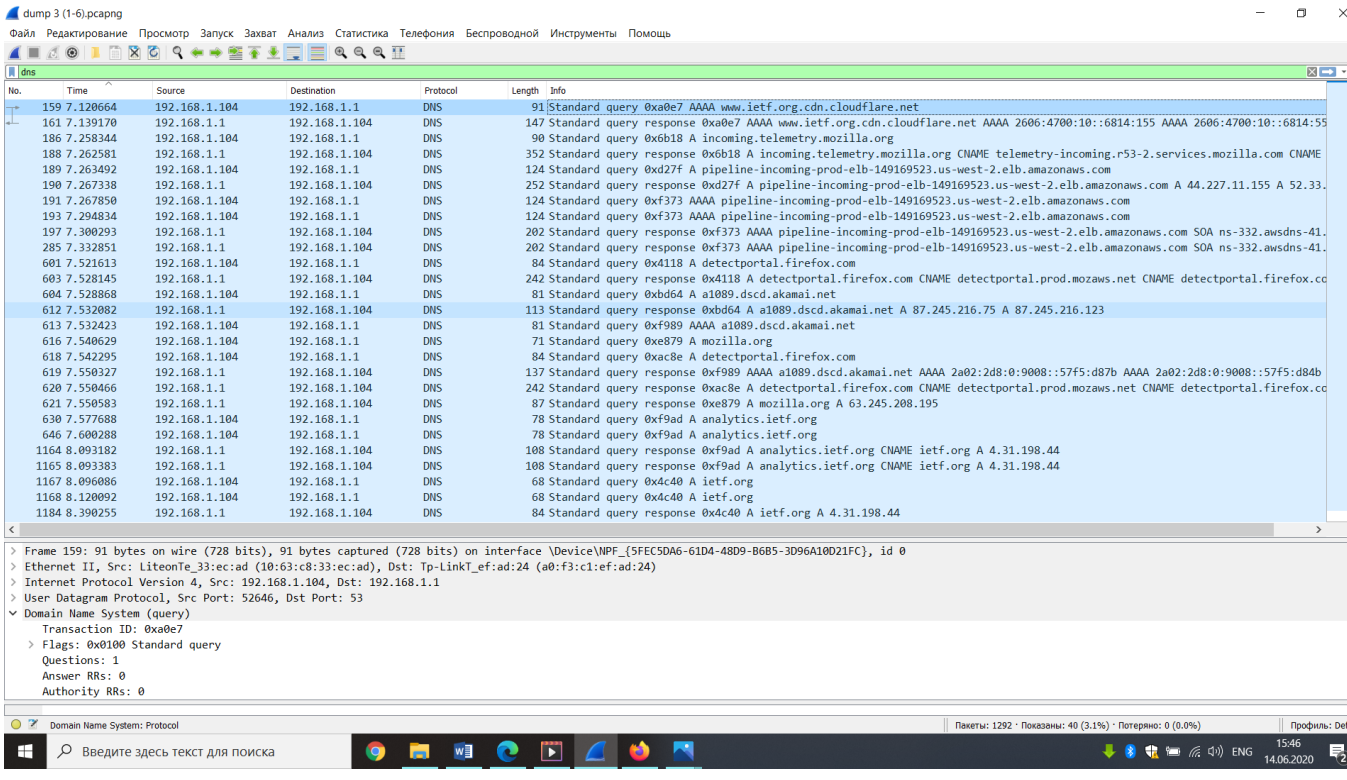
5) Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

Відповідь: в TCP SYN Destination: 192.168.1.104 співпадає з однією з запропонованих віповідей сервера DNS.



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

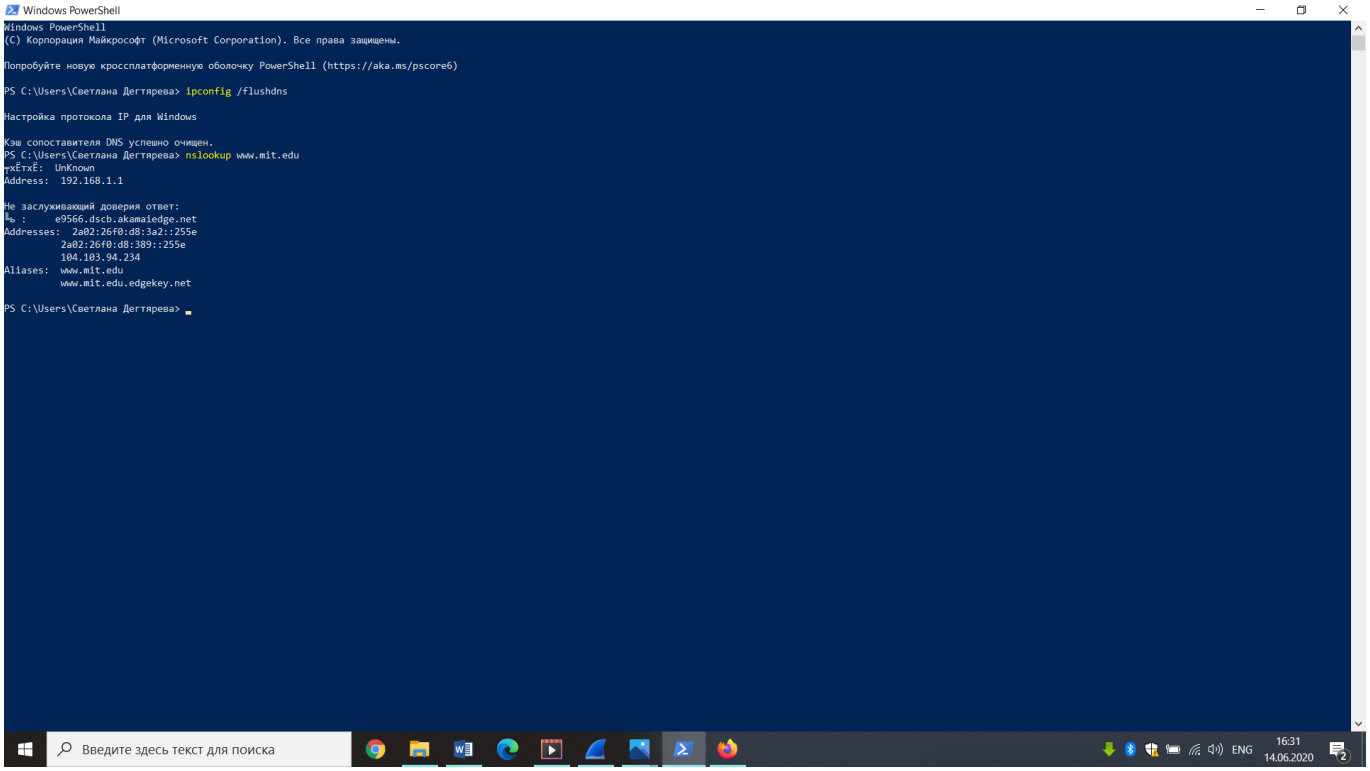
Відповідь: так.



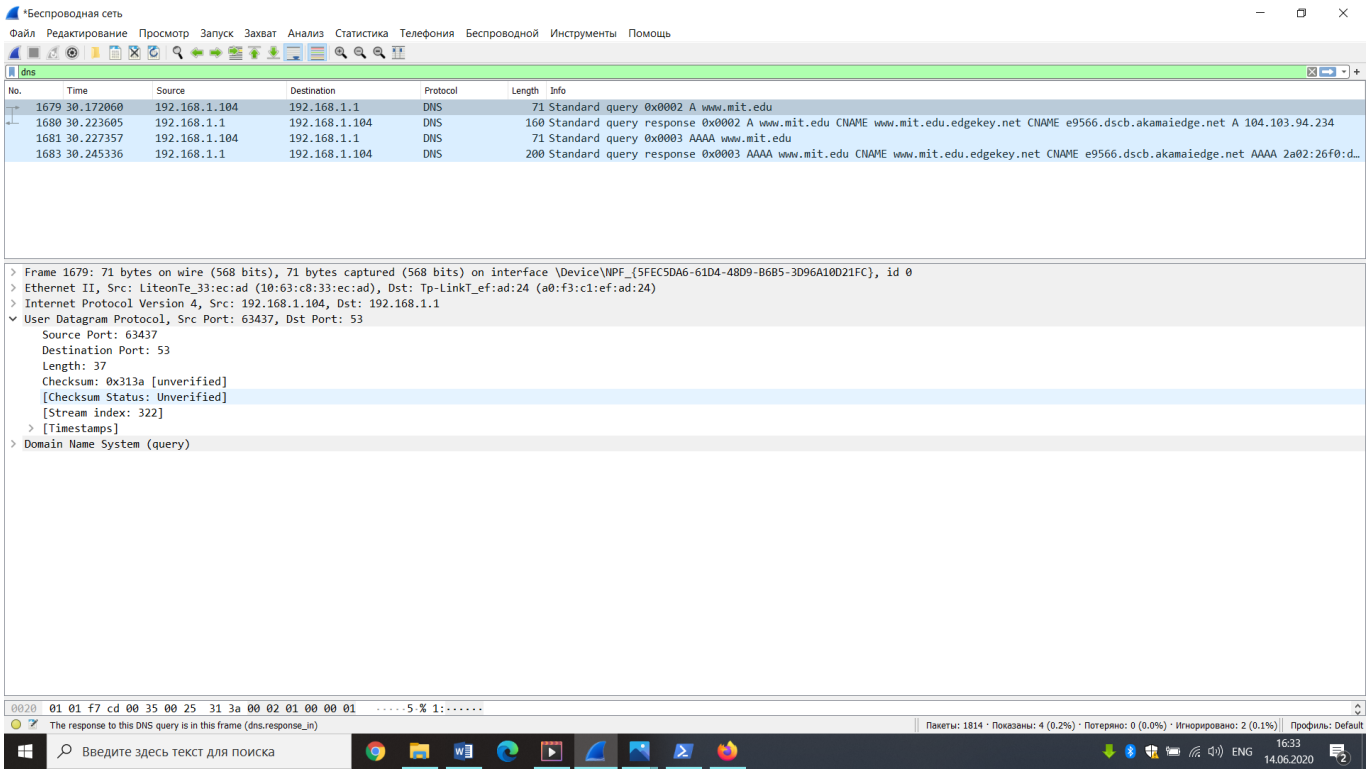
7) Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

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

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



Мал. 8



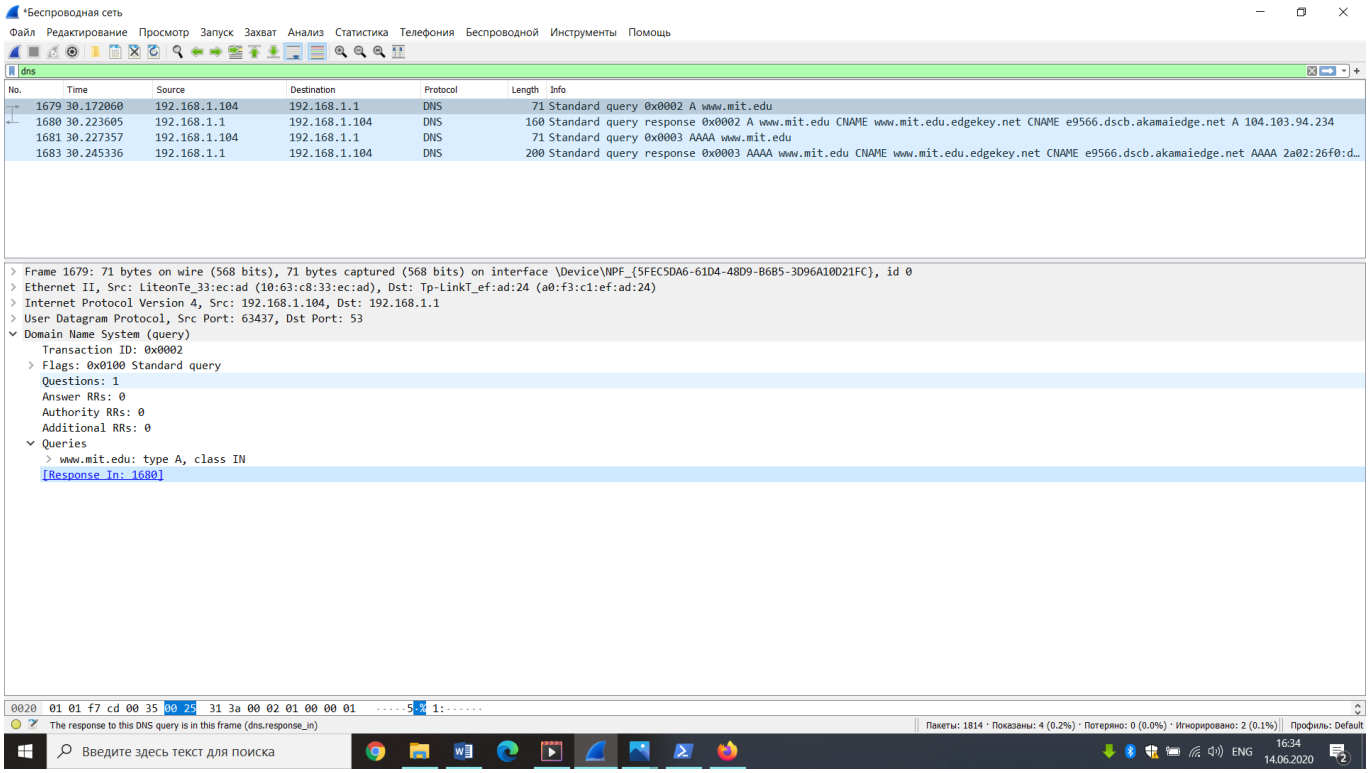
Мал. 9

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 складаєеться з :

для А– було 3 відповіді:

www.mit.edu: type CNAME, class IN, cname 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 складається з:

Name: www.mit.edu

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

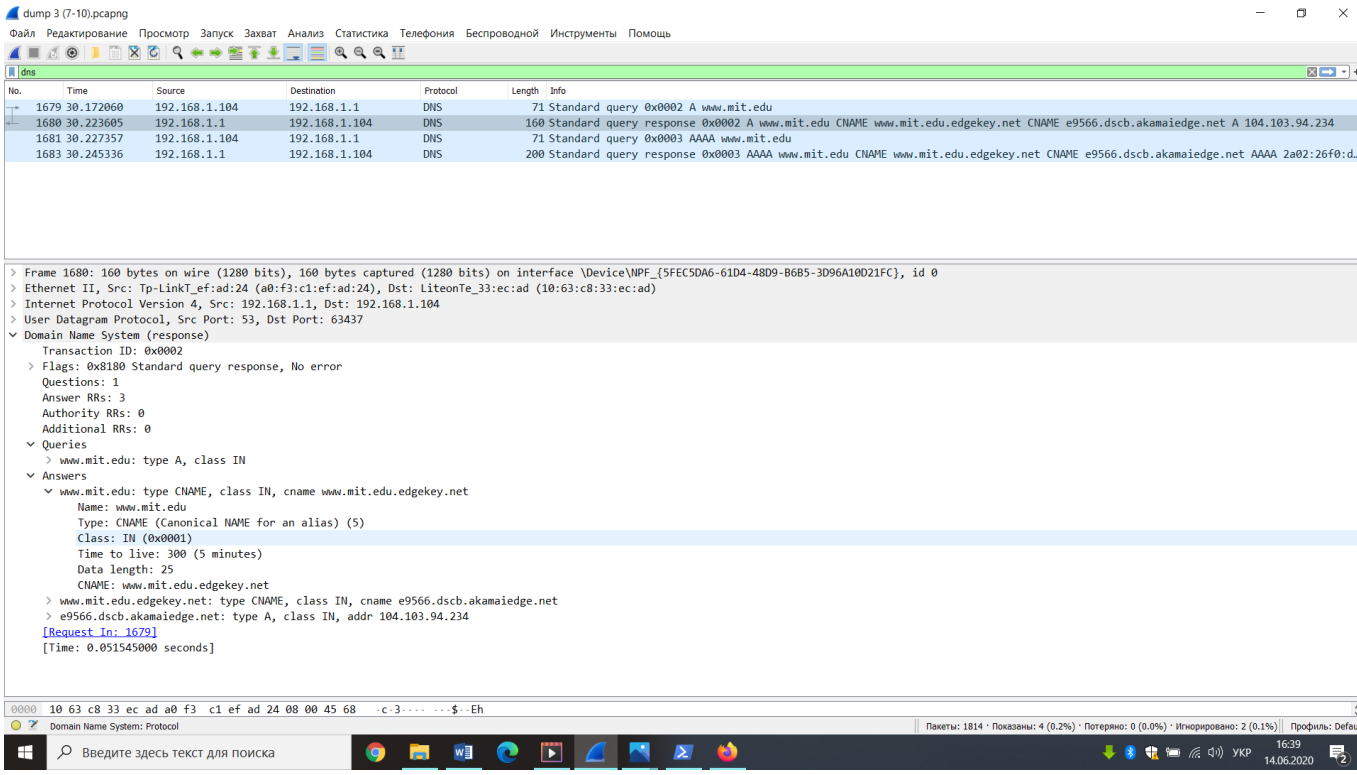
Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 25

CNAME: www.mit.edu.edgekey.net

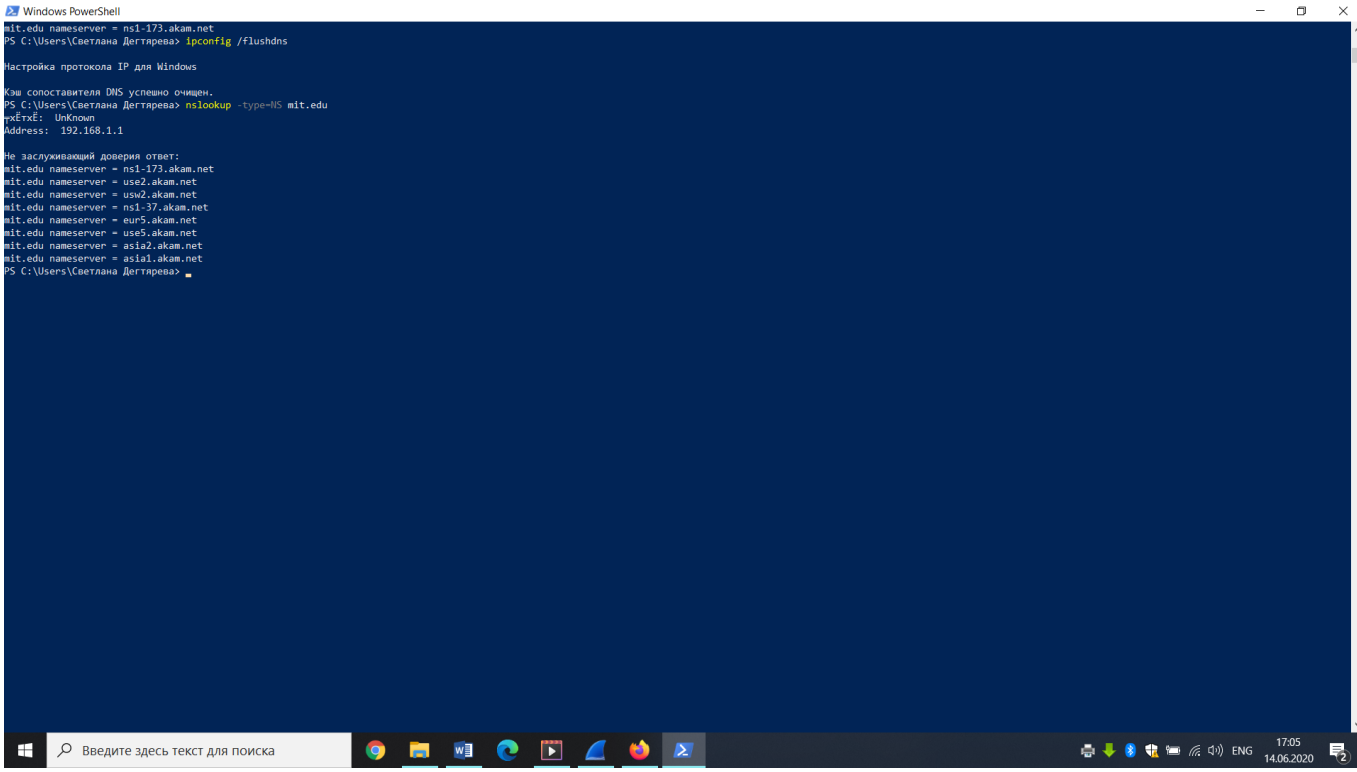
для типу AAAA – 4 відповіді;



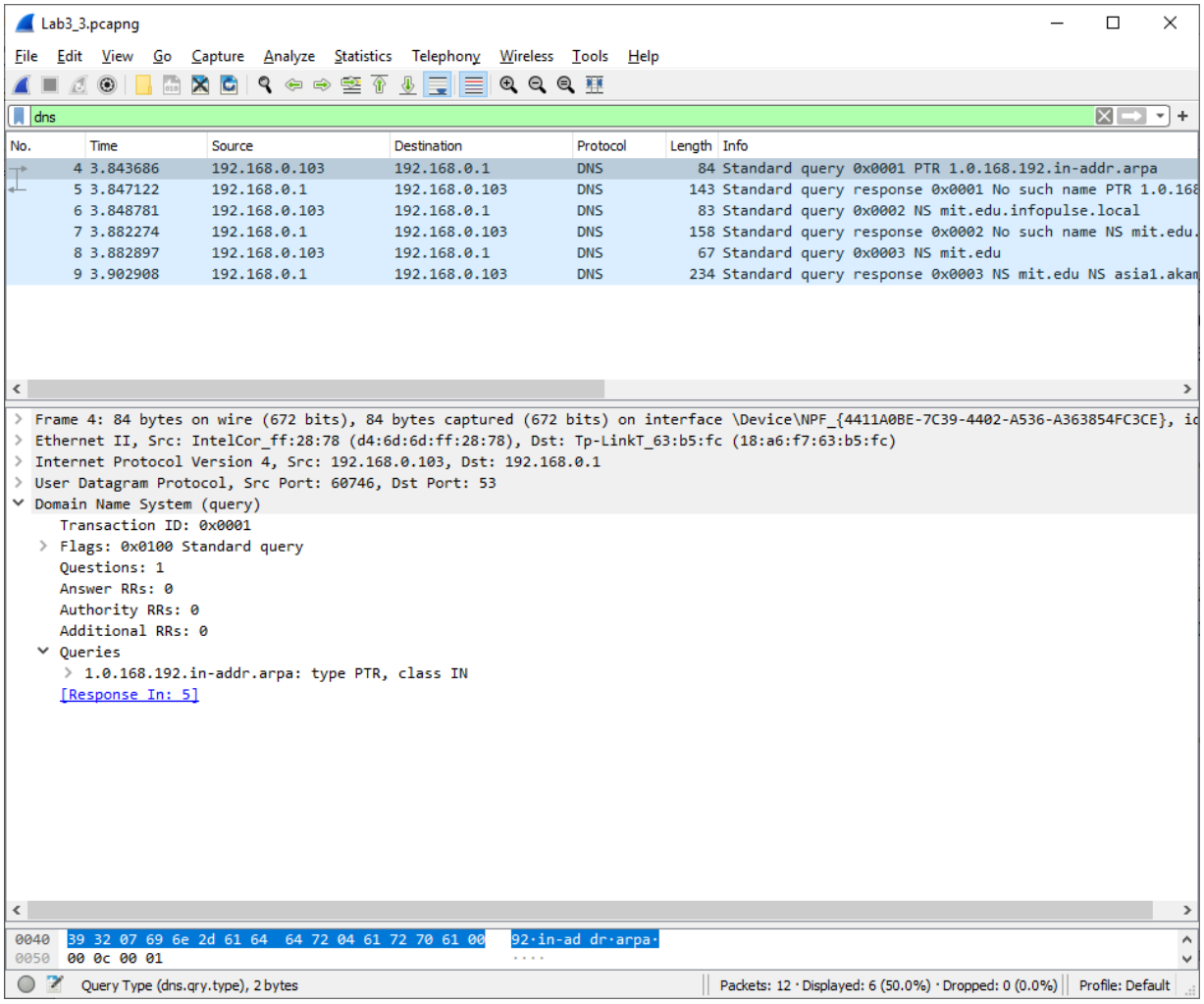
Мал. 10

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

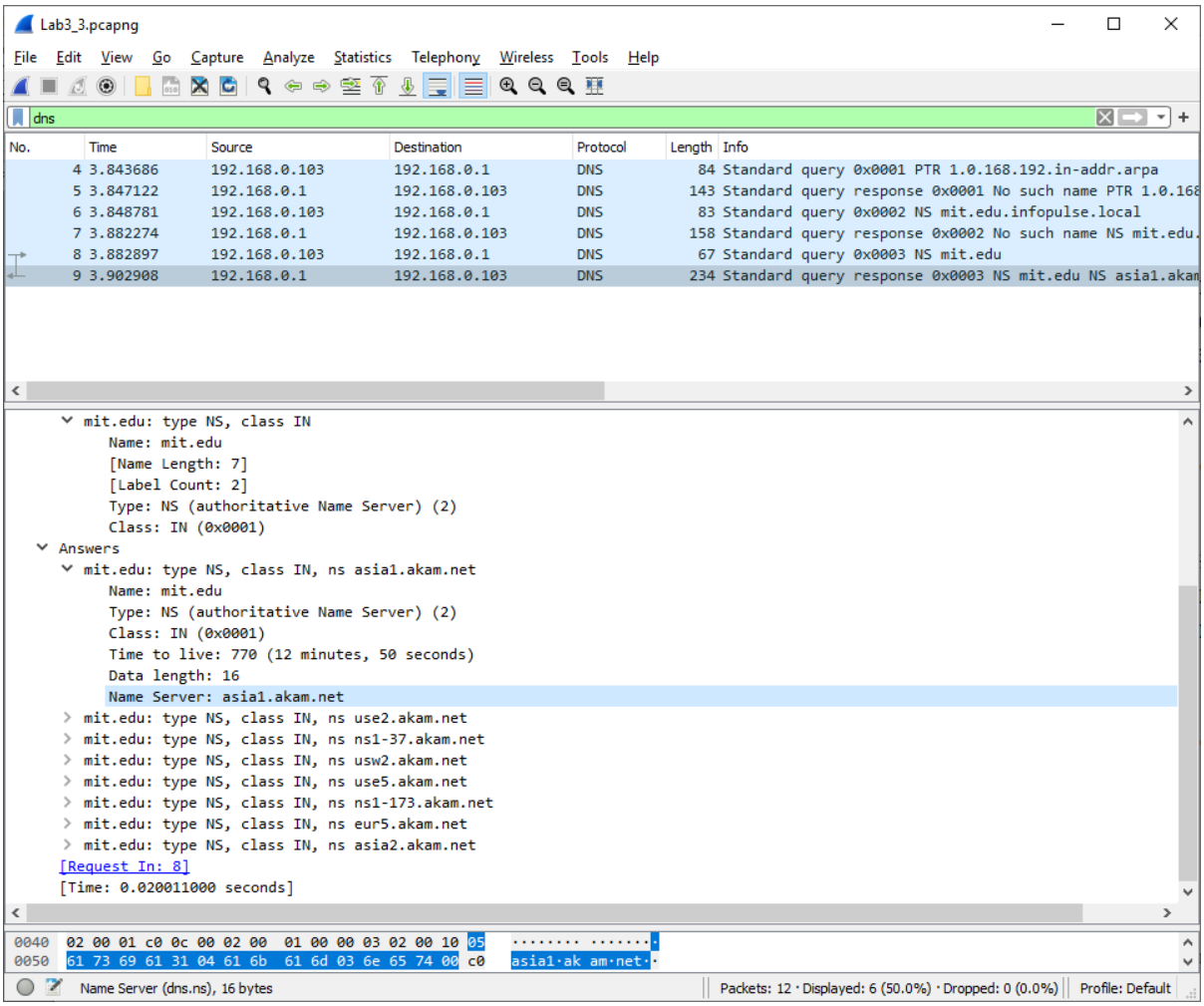
Відповідь: Destination: 192.168.0.1 – це є адреса локального сервера DNS за замовчанням


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
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 = usw2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = asia1.akam.net
PS C:\Users\Светлана Дегтярева>
Введите здесь текст для поиска
ENG
17:05
14.06.2020

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
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
Frame 4: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{4411A0BE-7C39-4402-A536-A363854FC3CE}, id
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
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
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
Name Server (dns.ns), 16 bytes
Packets: 12 · Displayed: 6 (50.0%) · Dropped: 0 (0.0%)
Profile: Default

Мал. 13