іністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

[Кафедра математичних методів системного аналізу](http://e-u.in.ua/ukr/?page=35)

**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:

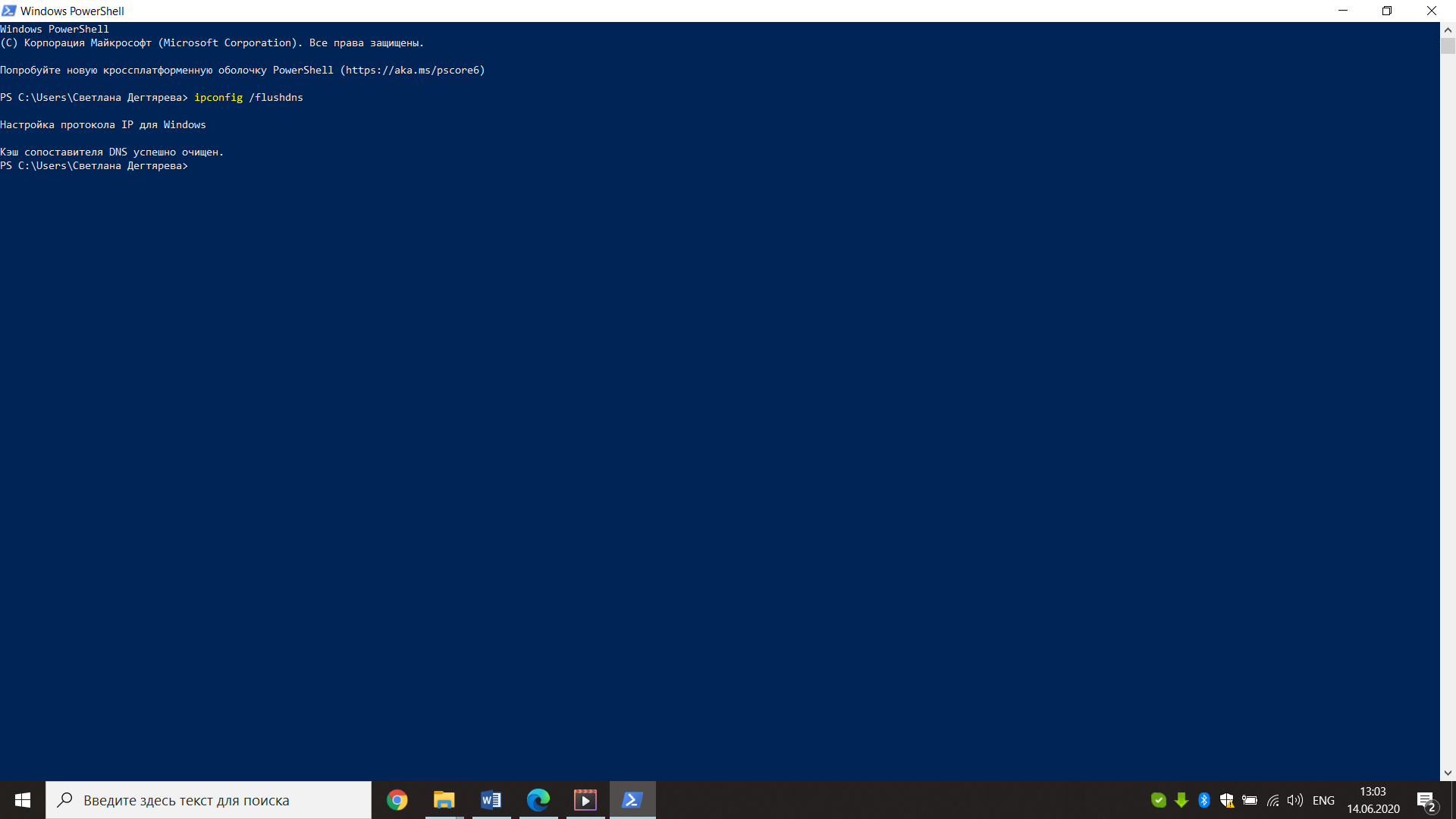


Рис. 1

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

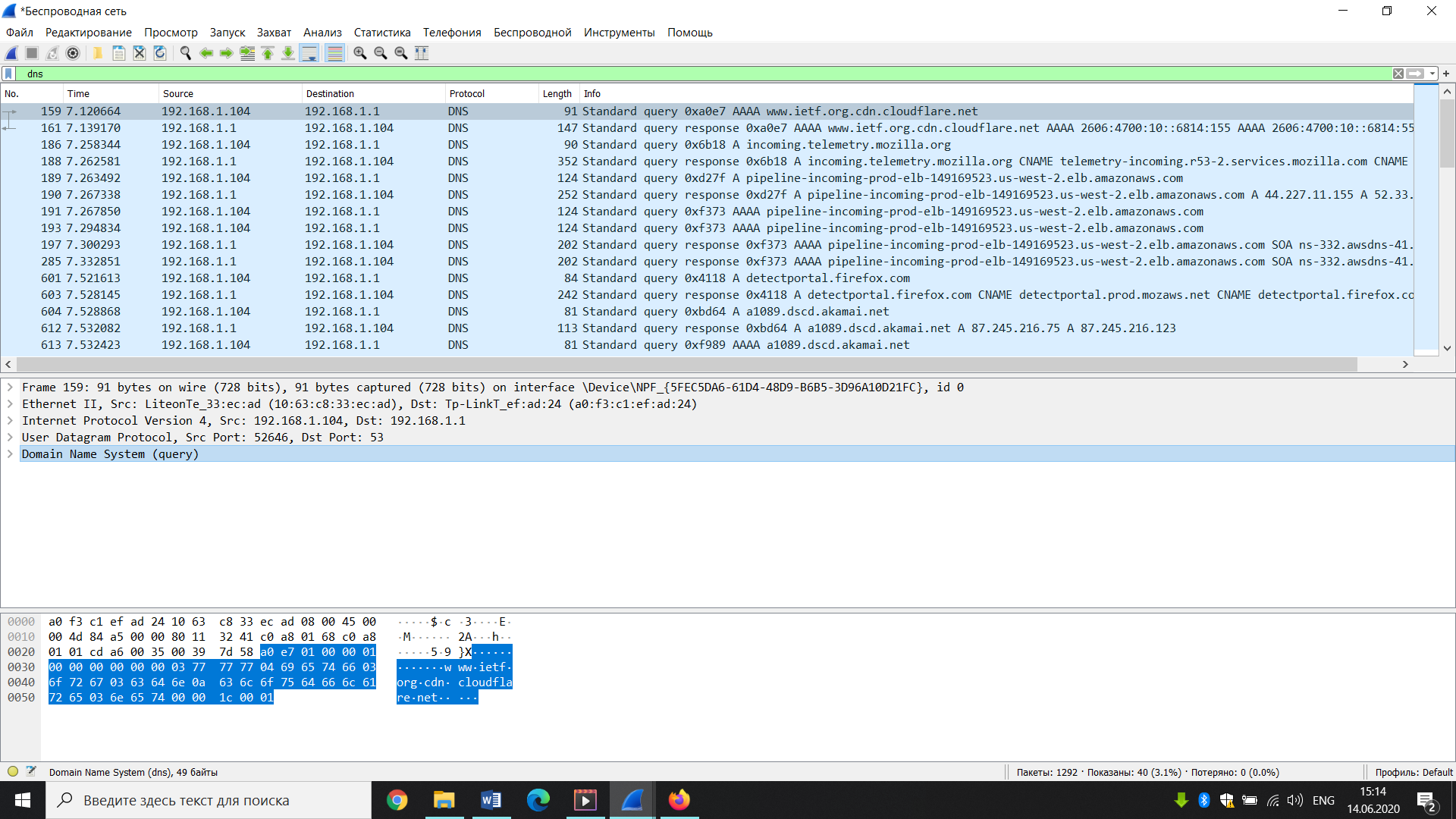
****

Рис. 2

1. Почнемо захоплення пакетів.
2. 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.
3. Зупиняємо захоплення пакетів.
4. 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

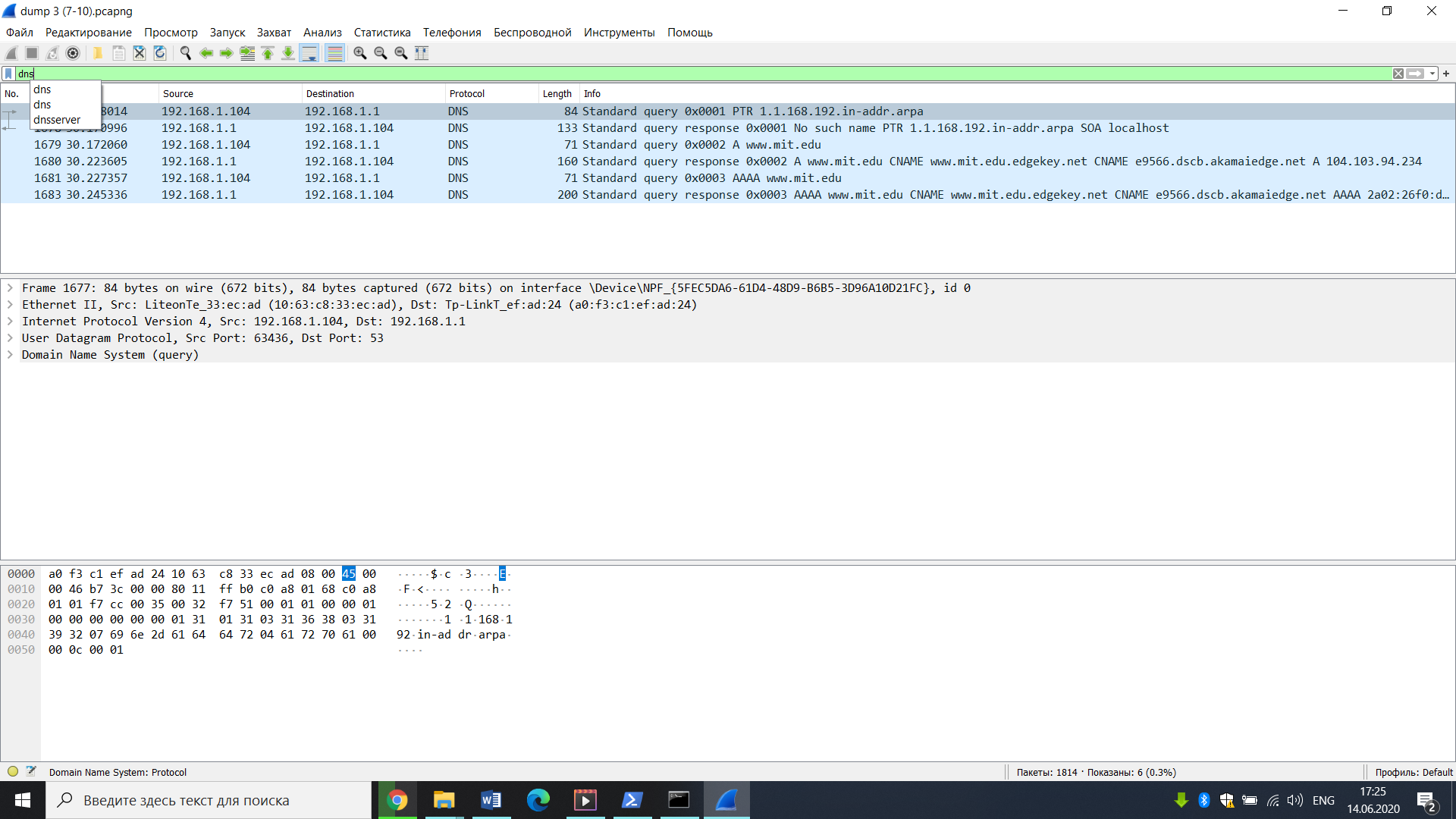
****

Рис. 3

1. Почнемо захоплення пакетів
2. Виконаємо nslookup для домену www.mit.edu за допомогою команди  
   a. nslookup –type=NS mit.edu
3. Зупиняємо захоплення пакетів
4. Готуємо відповіді на запитання 11-13. При необхідності, роздрукуємо деякі захоплені пакети
5. Почнемо захоплення пакетів
6. Виконуємо nslookup для домену www.mit.edu за допомогою команди  
   a. nslookup www.aiit.or.kr bitsy.mit.edu
7. Зупиняємо захоплення пакетів.
8. Готуємо відповіді на запитання 14-16. Друкуємо деякі  
   захоплені пакети
9. Готуємо відповіді на запитання 16, 17. Друкуємо необхідні для цього пакети.
10. 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

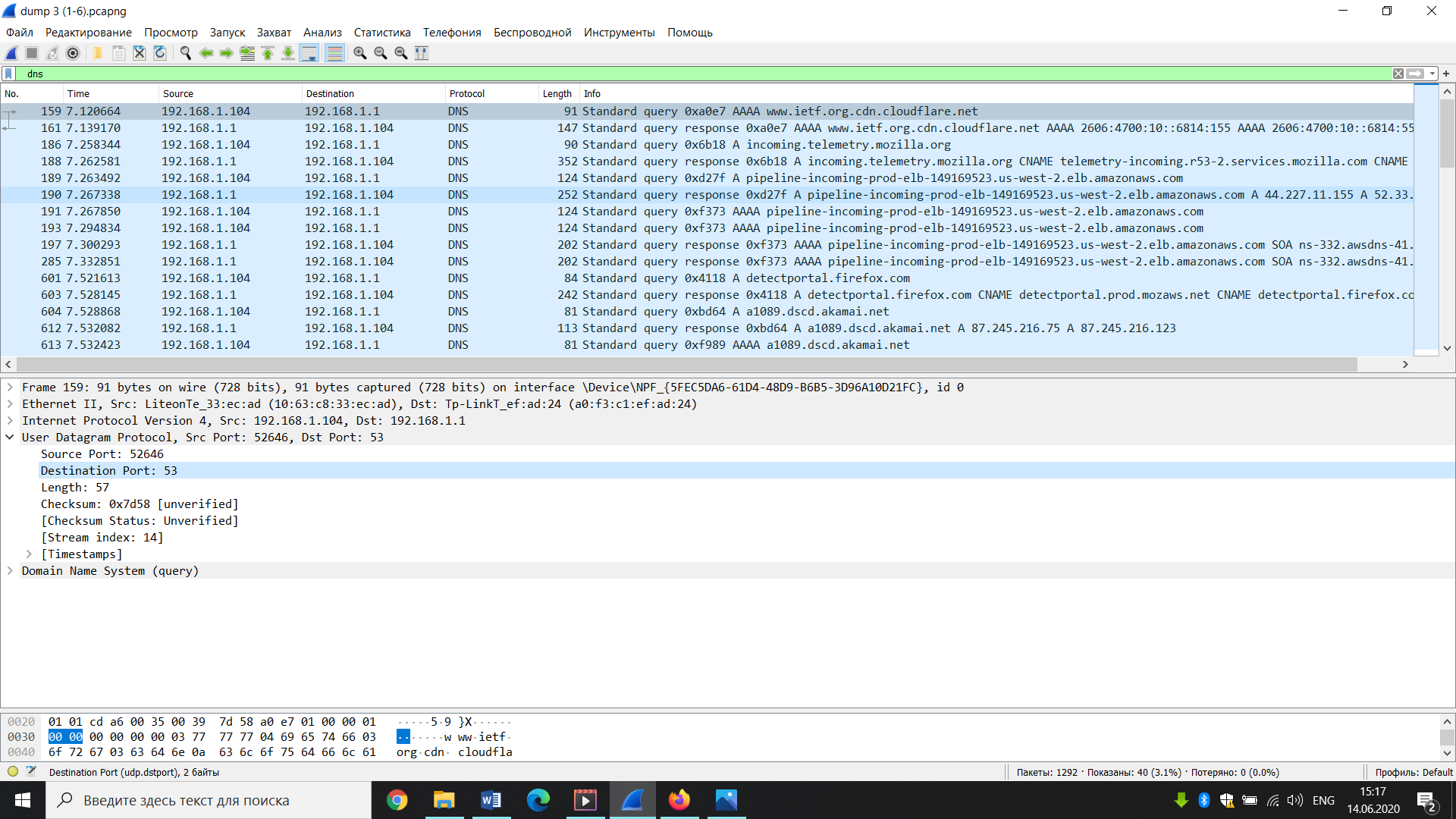


Рис.

1. 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

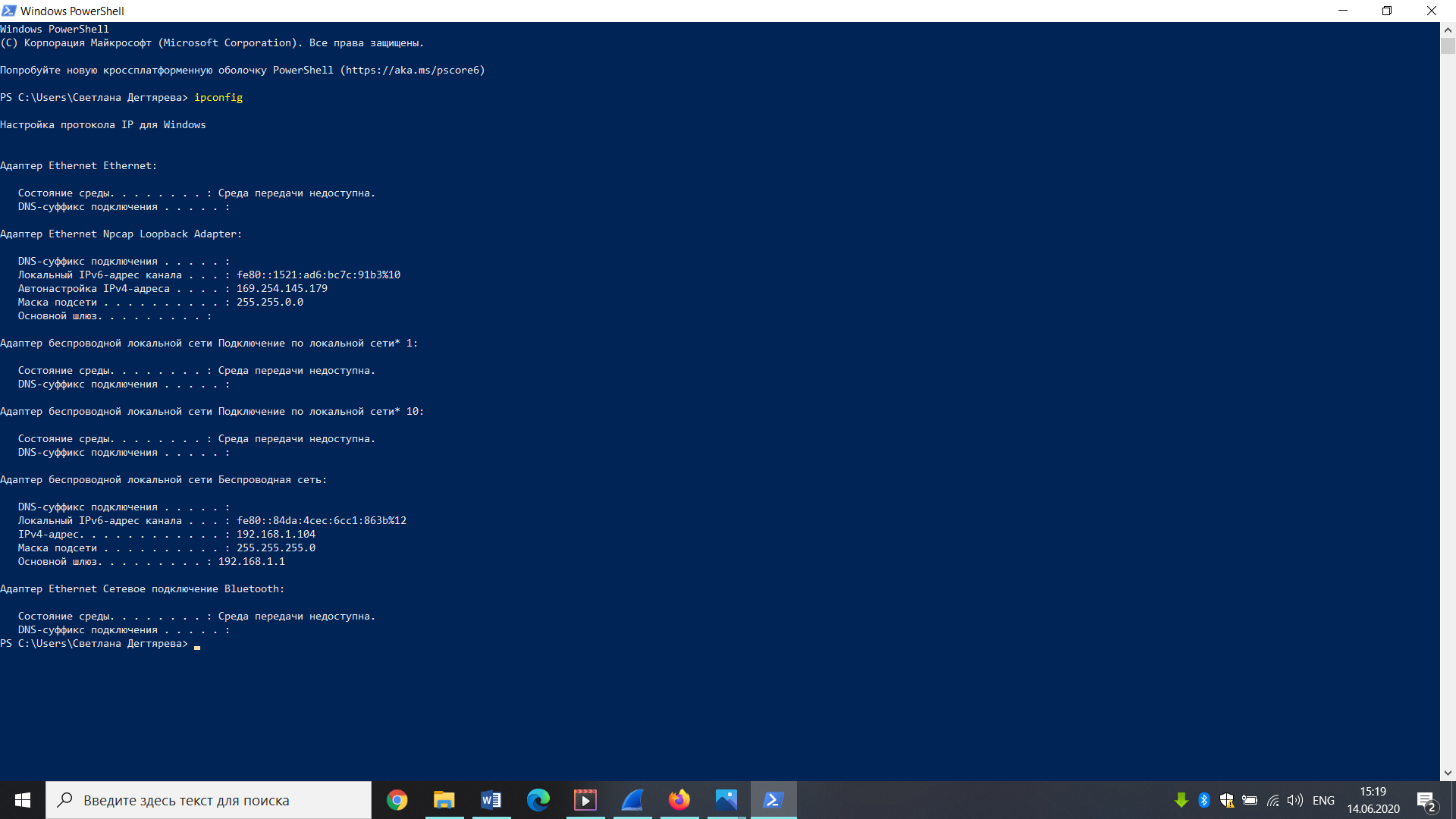


Рис.

1. 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.

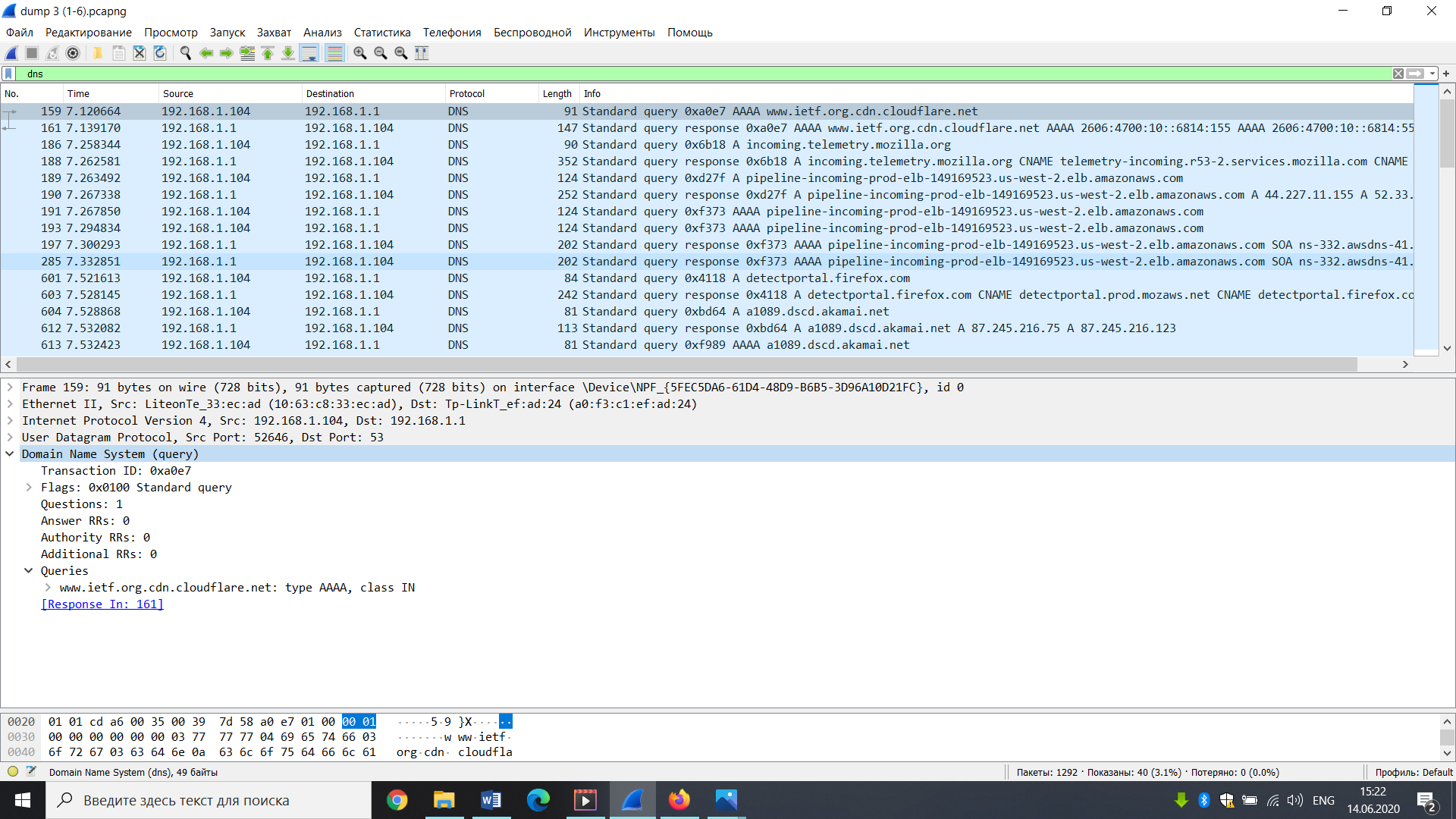


Рис.

1. 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

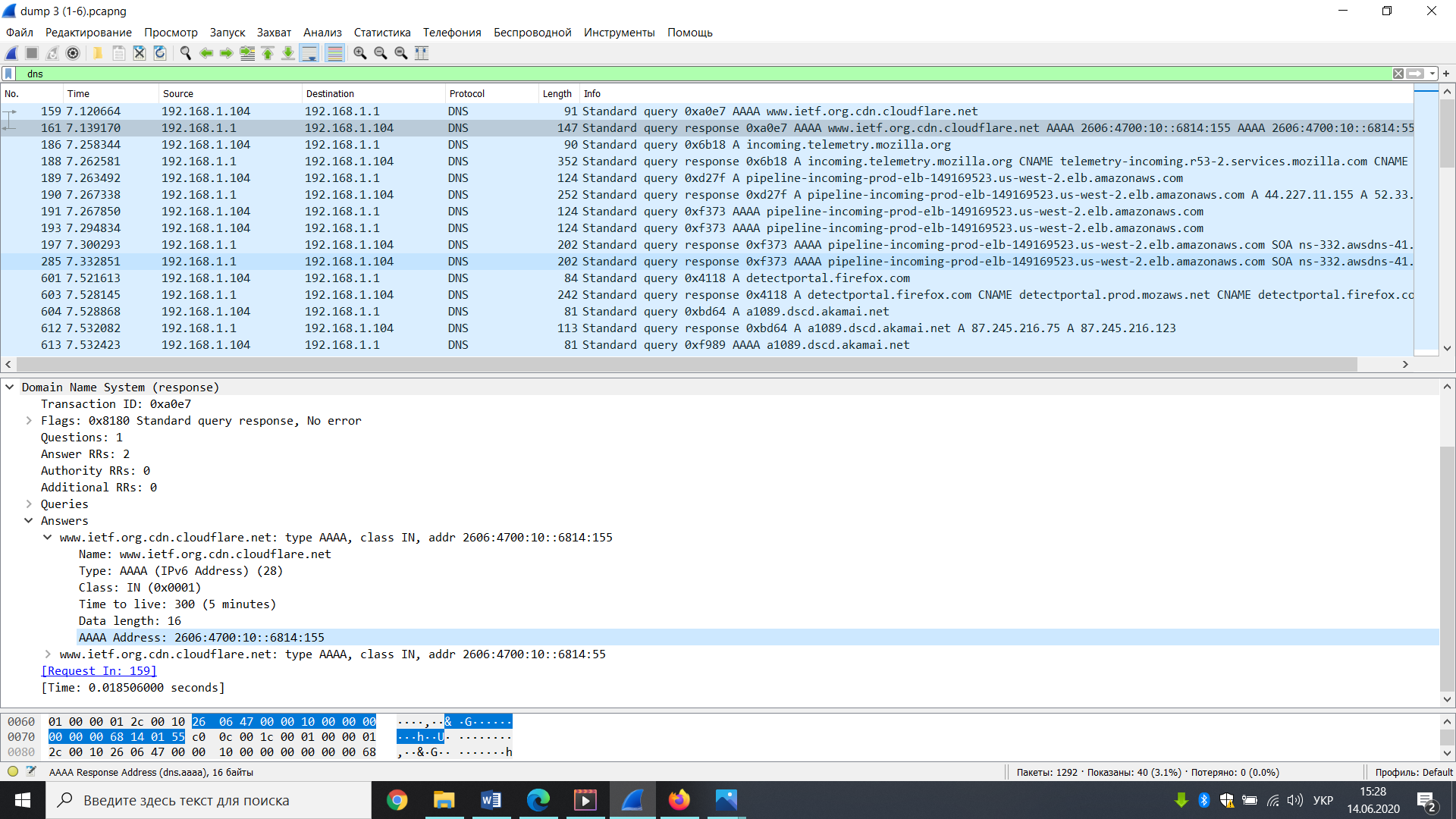
Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 16

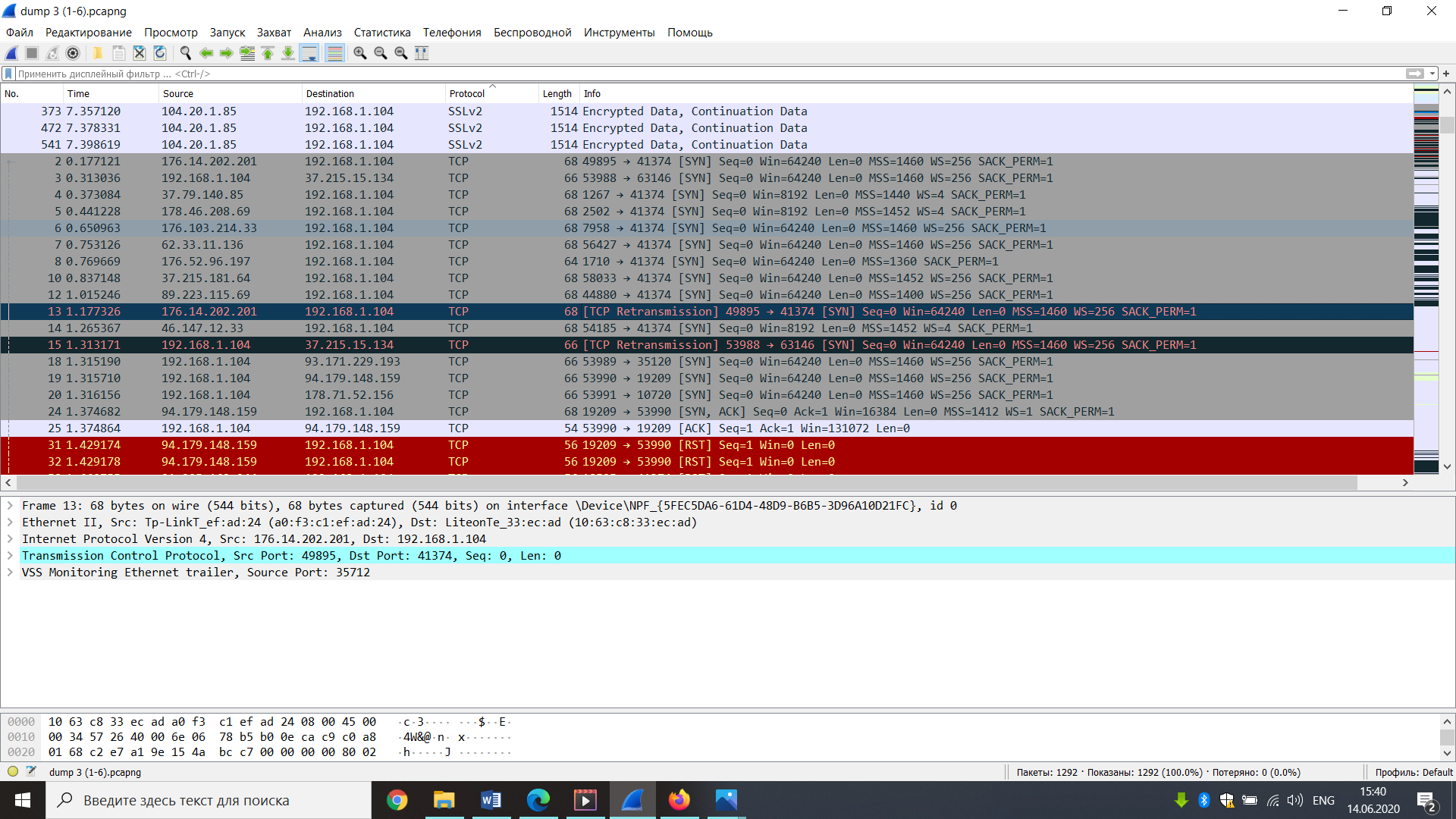
AAAA Address: 2606:4700:10::6814:155



Мал. 6

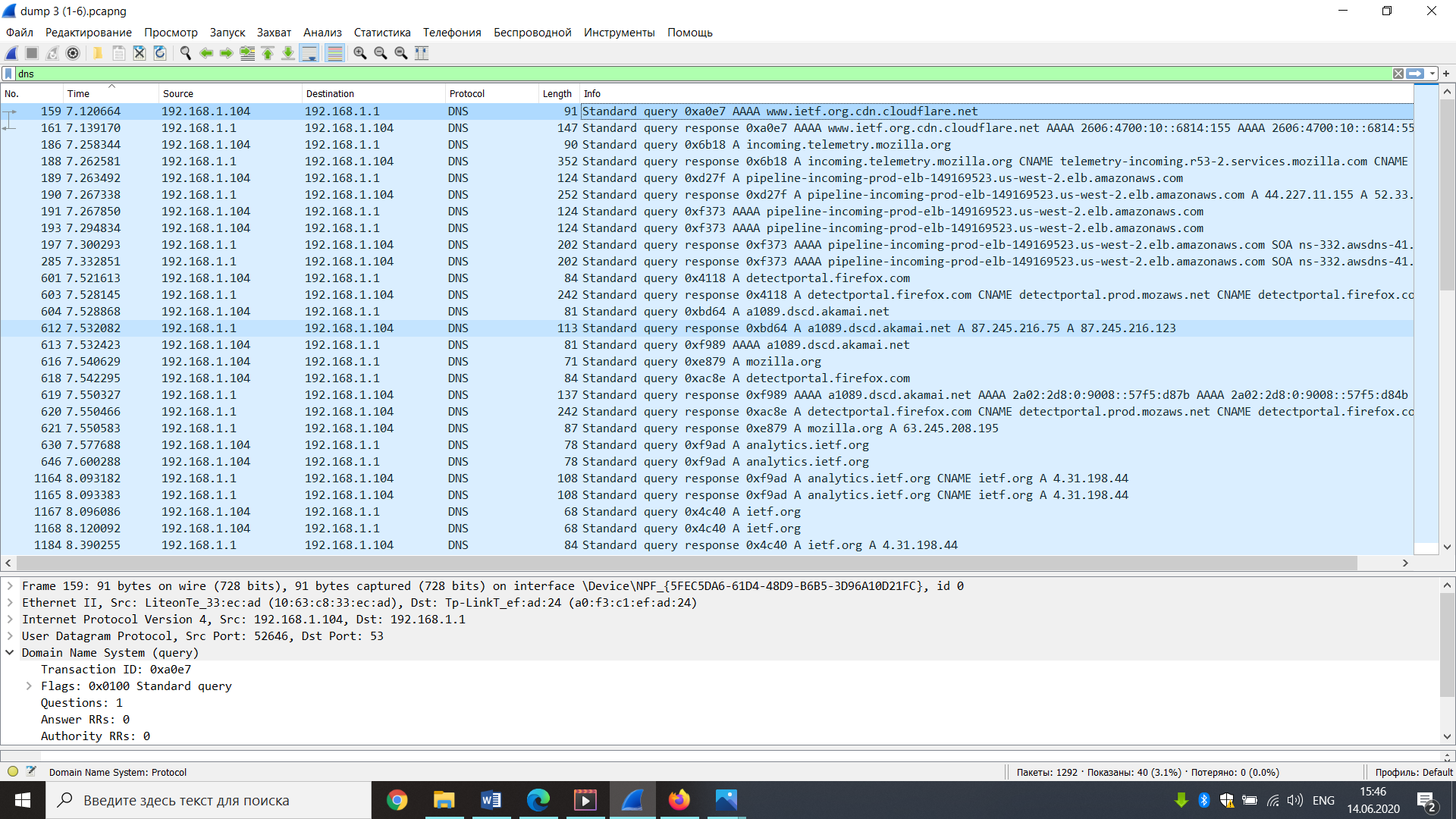
1. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього  
   повідомлення з одною із відповідей сервера DNS?

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



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

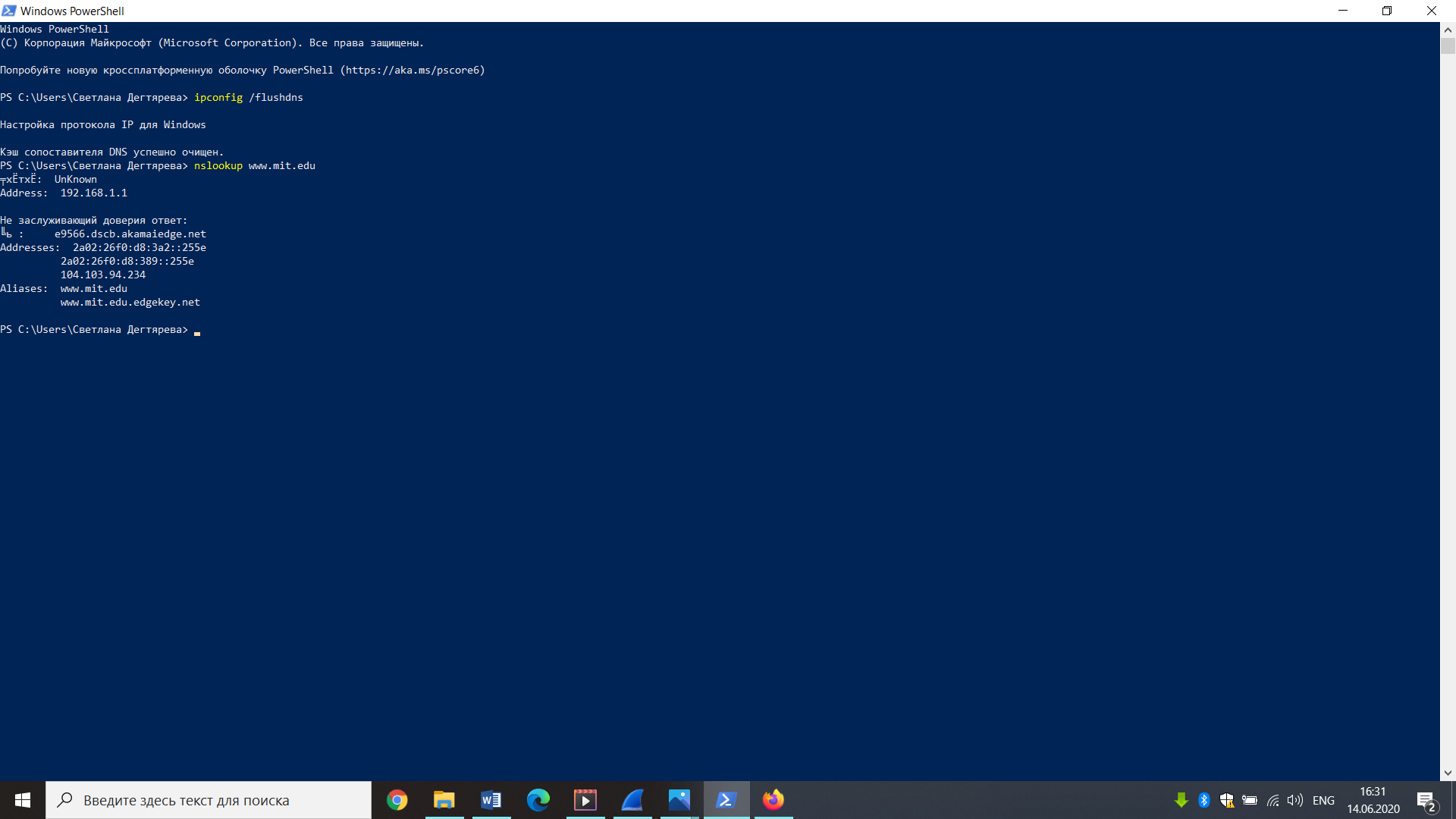
Відповідь: так.



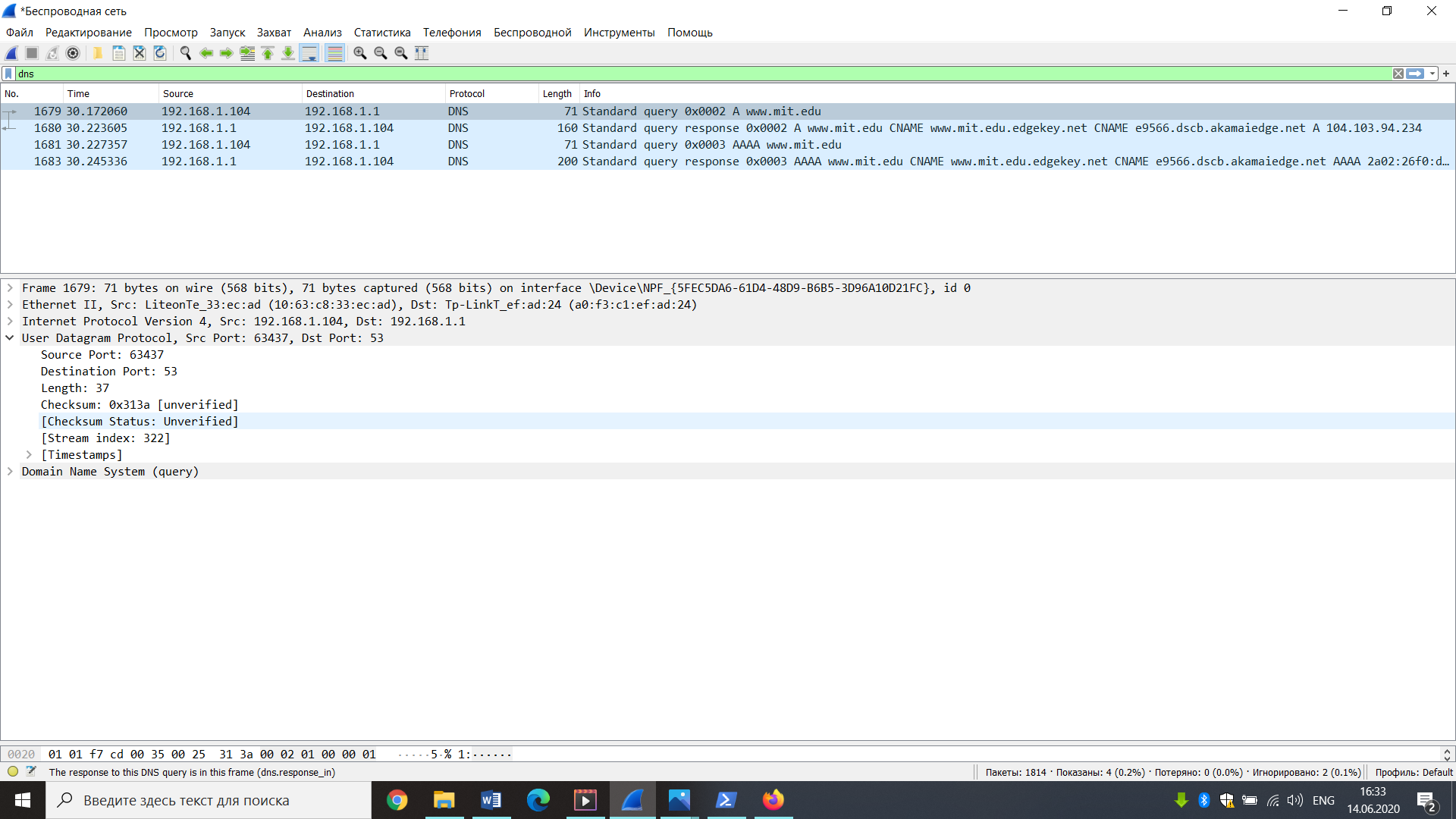
1. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

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

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



Мал. 8



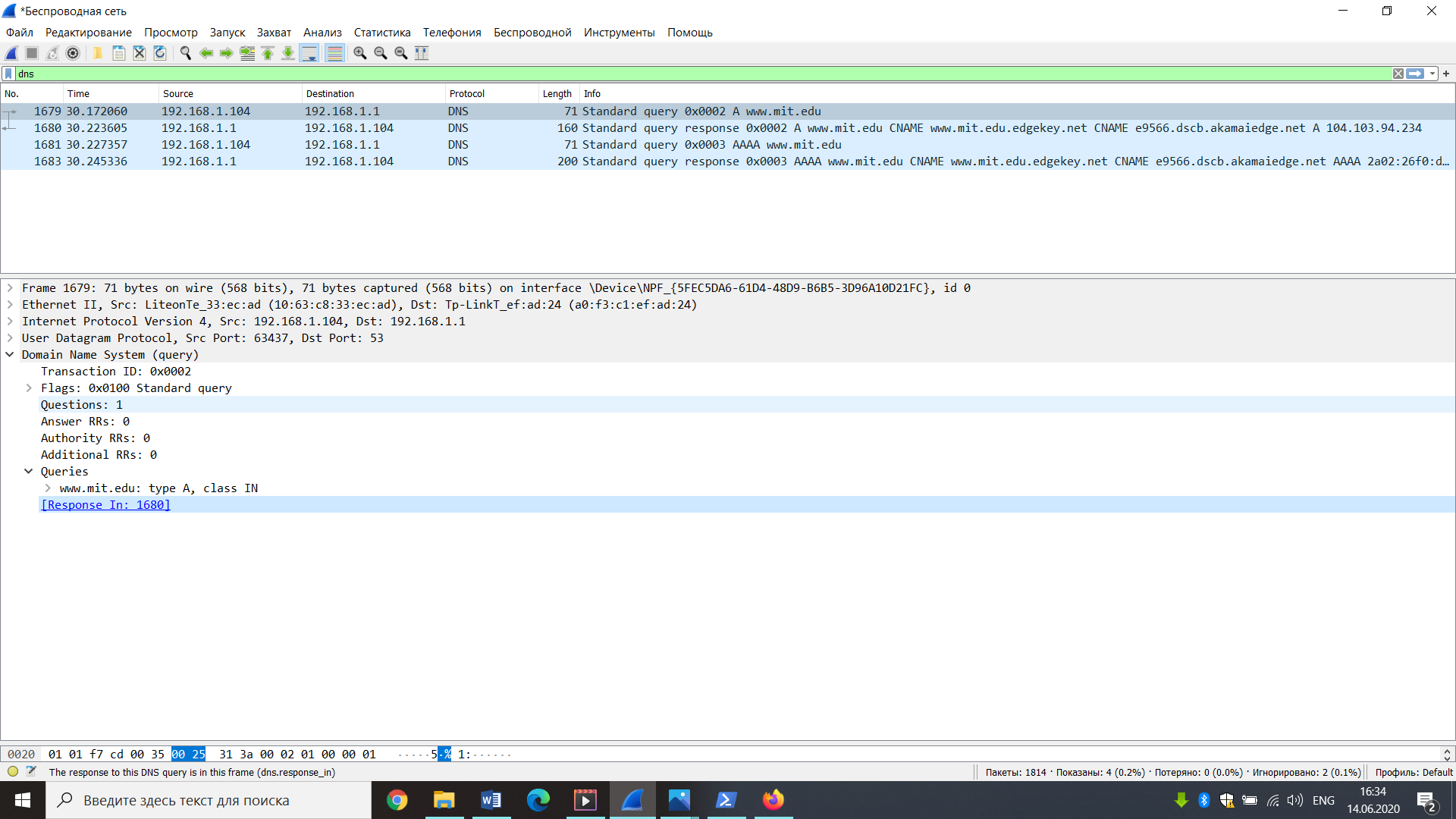
Мал. 9

1. 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.

1. 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



1. 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](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)

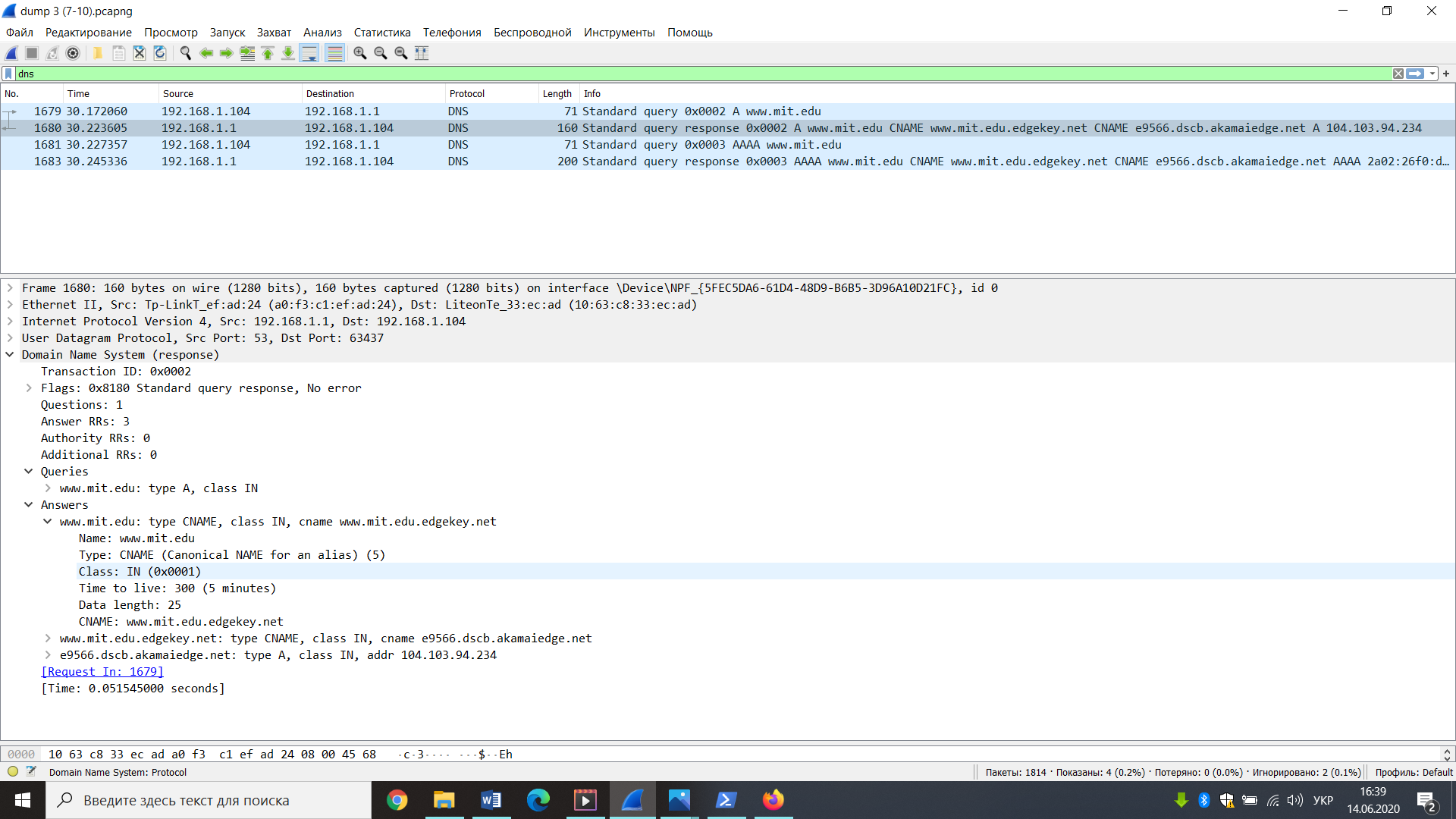
Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 25

CNAME: www.mit.edu.edgekey.net

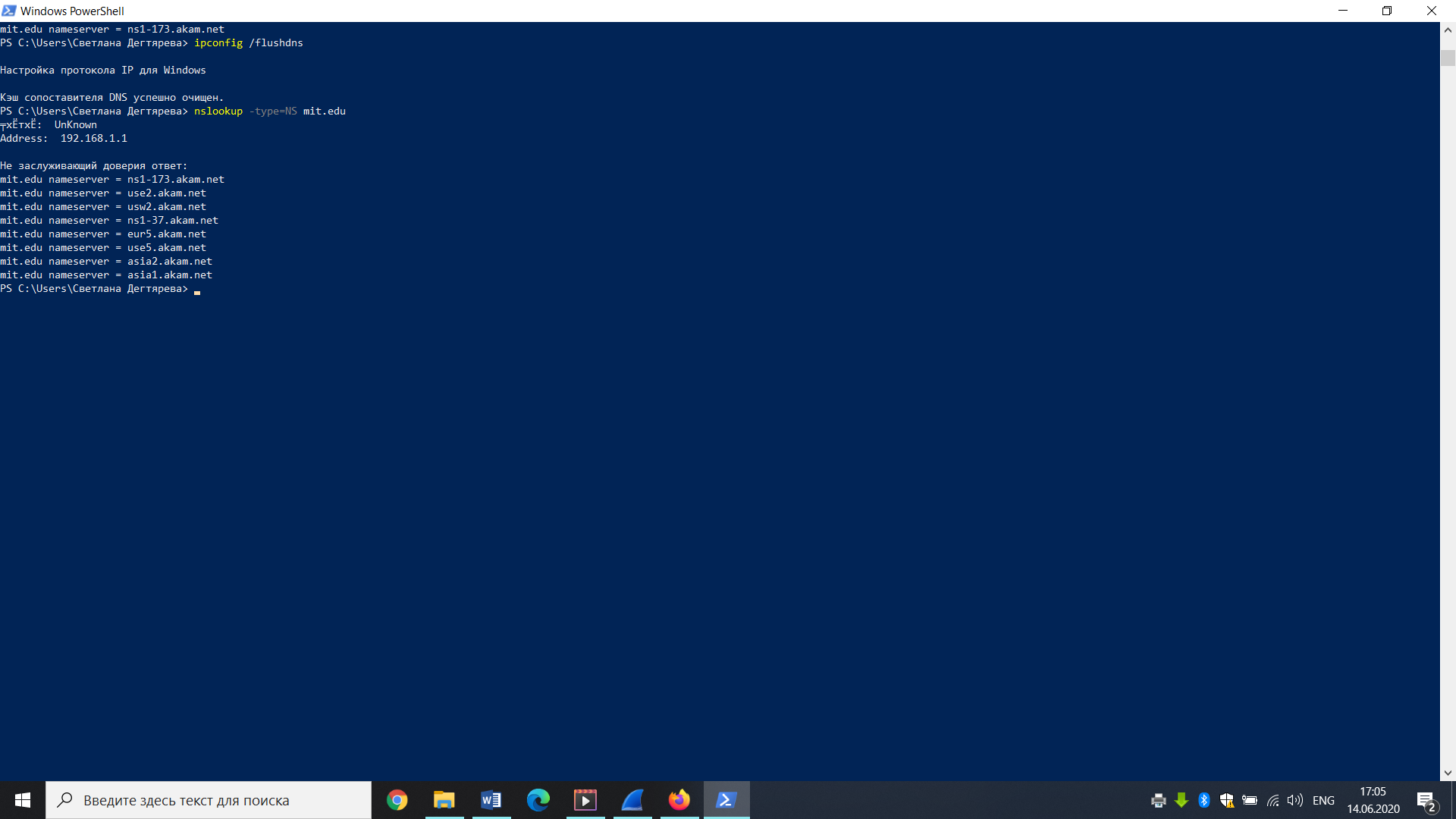
для типу AAAA – 4 відповіді;



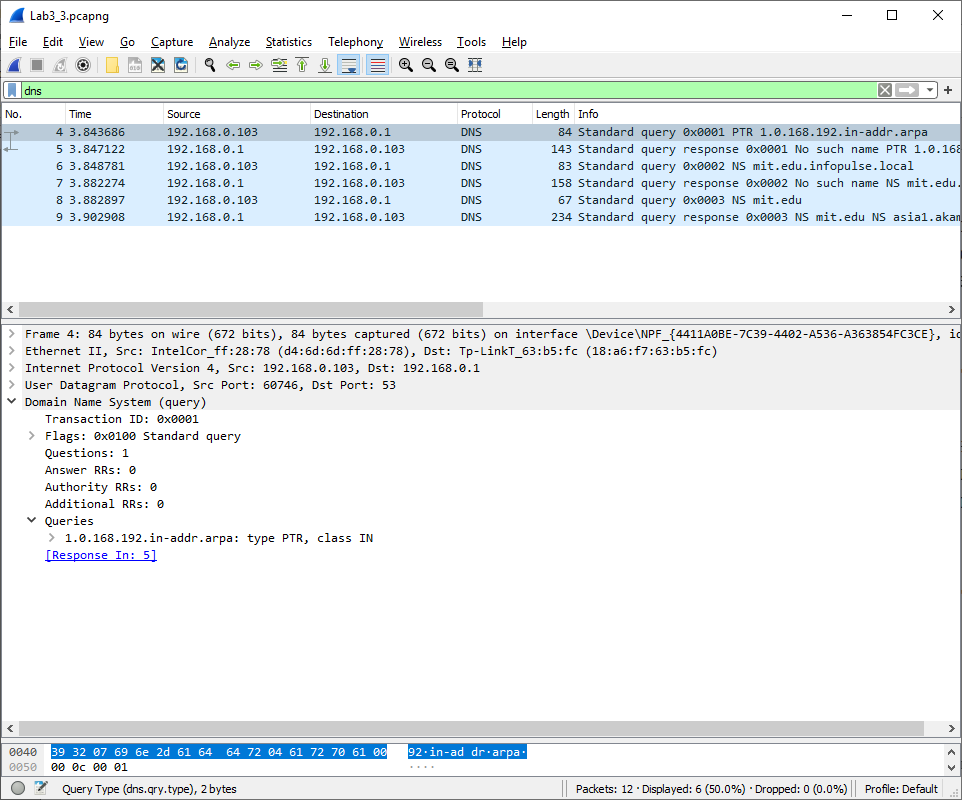
Мал. 10

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

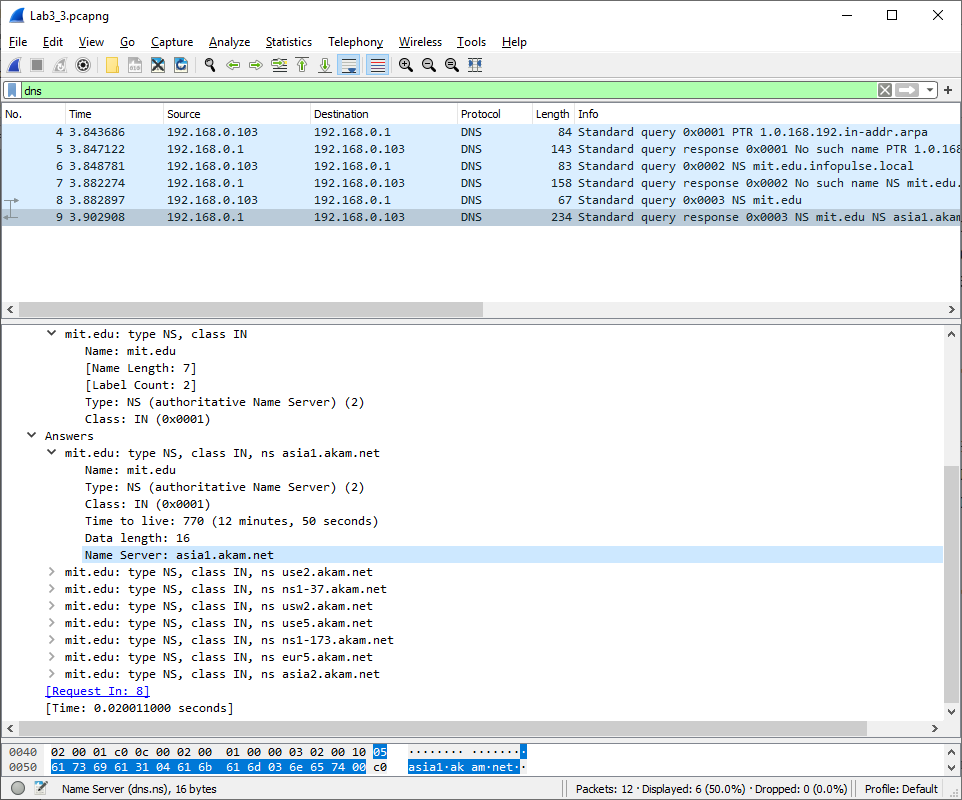
Відповідь: Destination: 192.168.0.1 – це є адреса локального сервера DNS за замовчанням



Мал. 11



Мал. 12



Мал. 13