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:

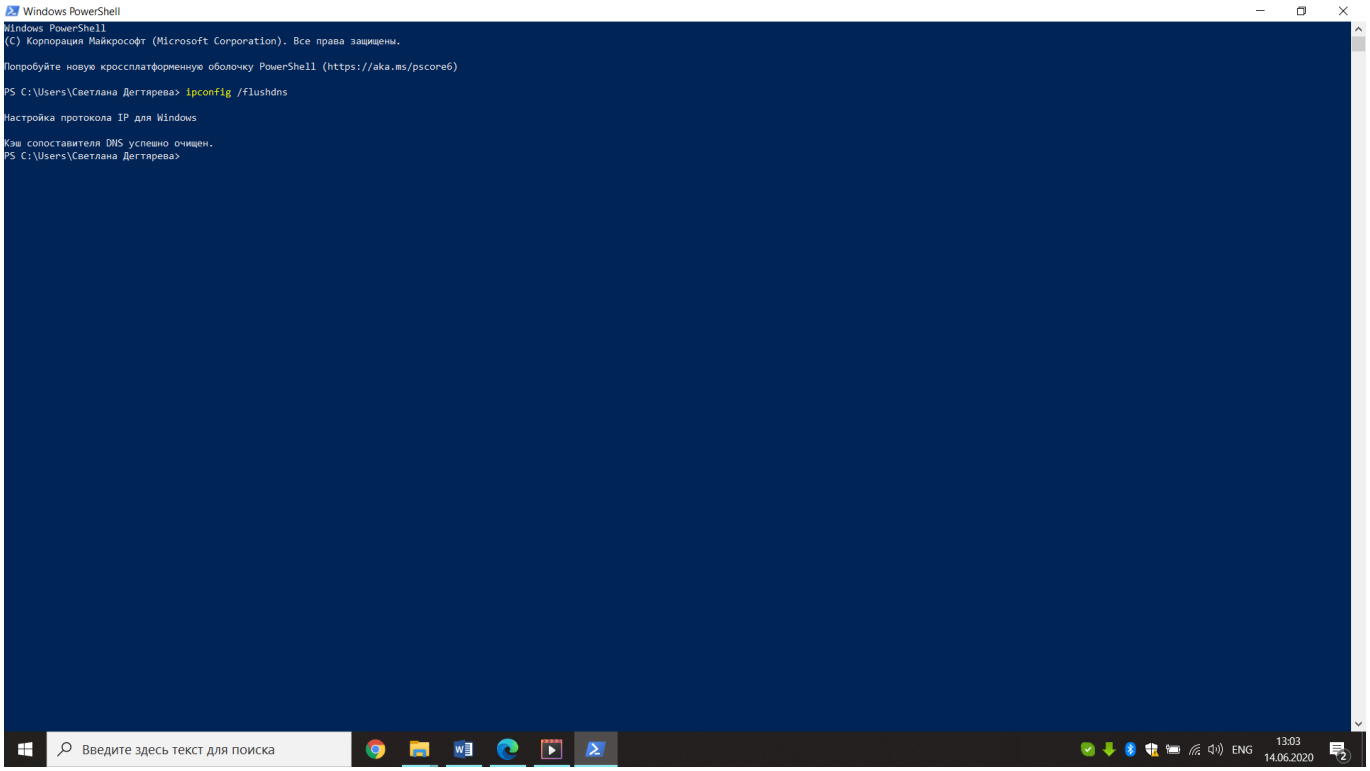

Рис. 1

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.

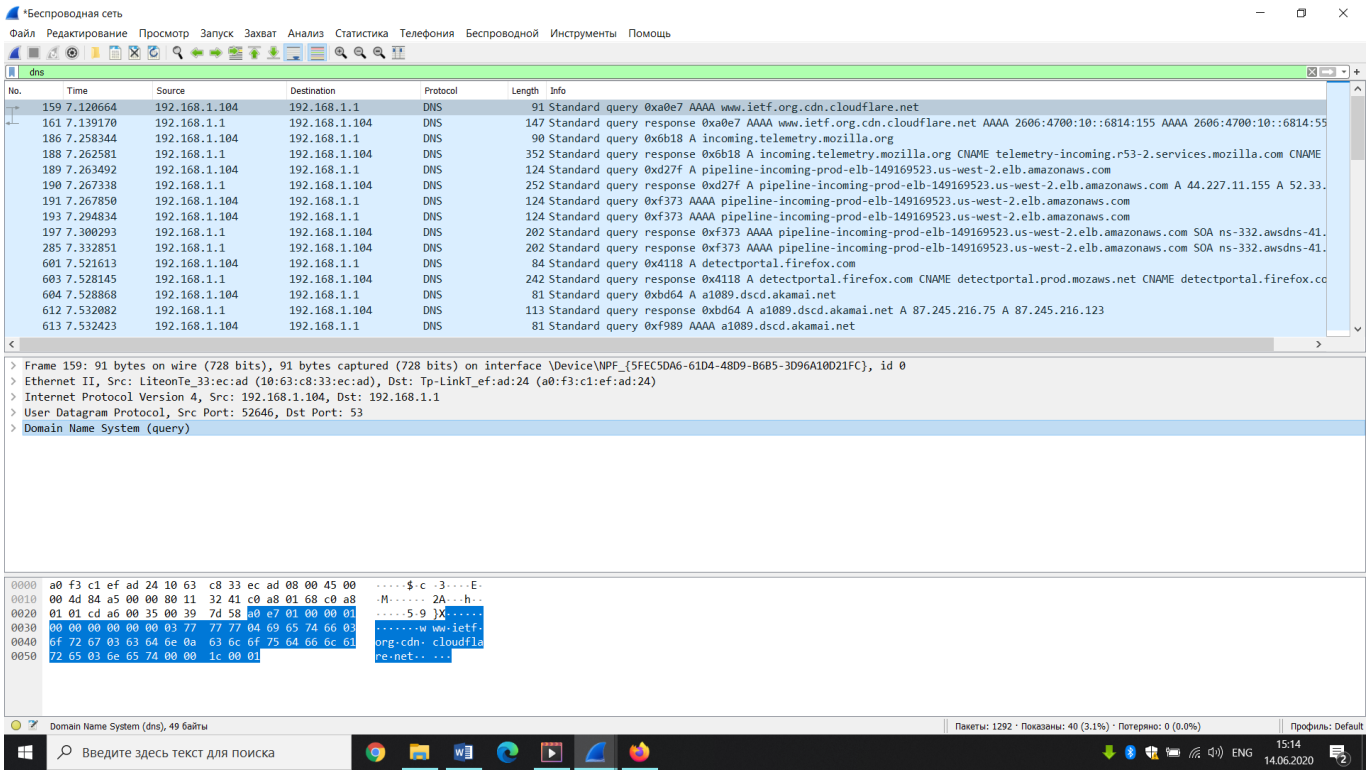

Рис. 2

8. Почнемо захоплення пакетів.

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

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

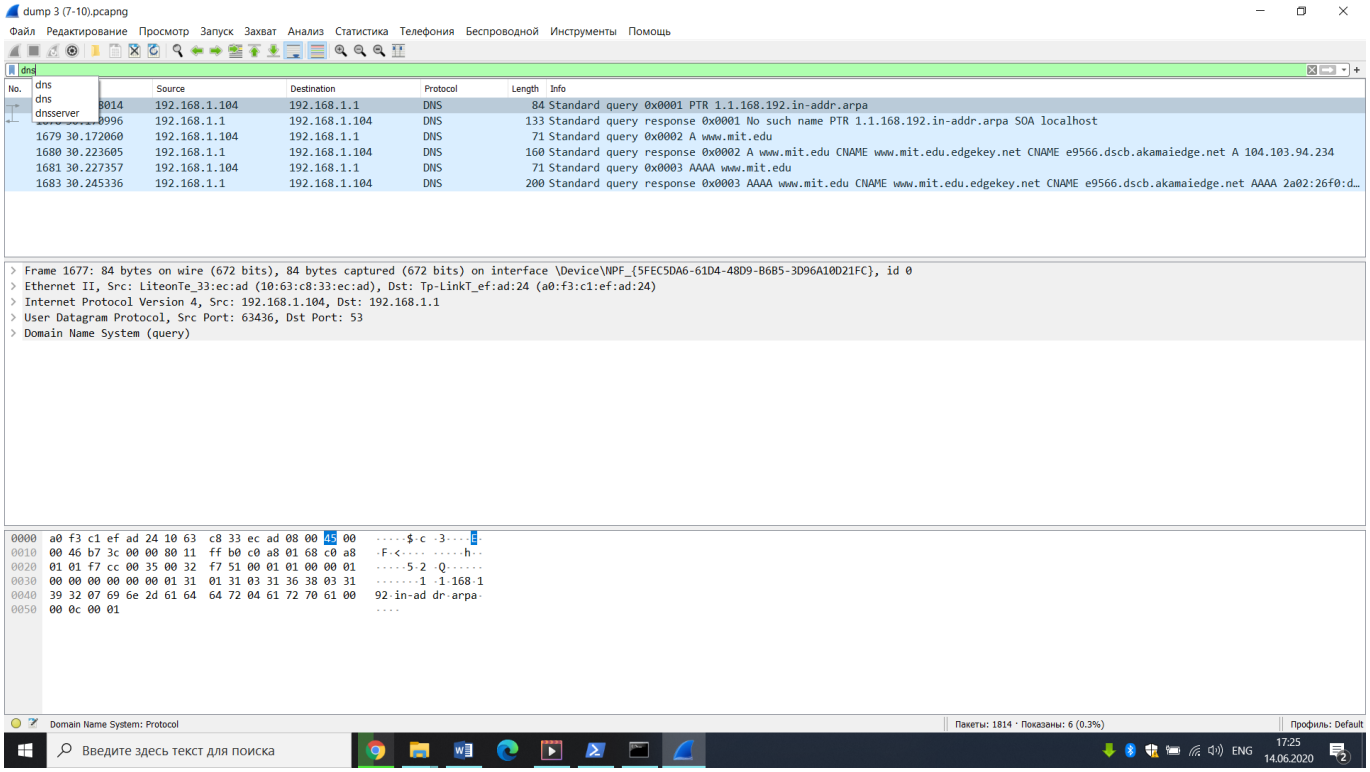

Рис. 3

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

Виконуємо nslookup для домену www.mit.edu за допомогою команди

a. nslookup www.aiit.or.kr bitsy.mit.edu або nslookup -type=ns mit.edu 8.8.8.8

17. Зупиняємо захоплення пакетів.

18. Готуємо відповіді на запитання 14-16. Друкуємо деякі захоплені пакети

19. 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

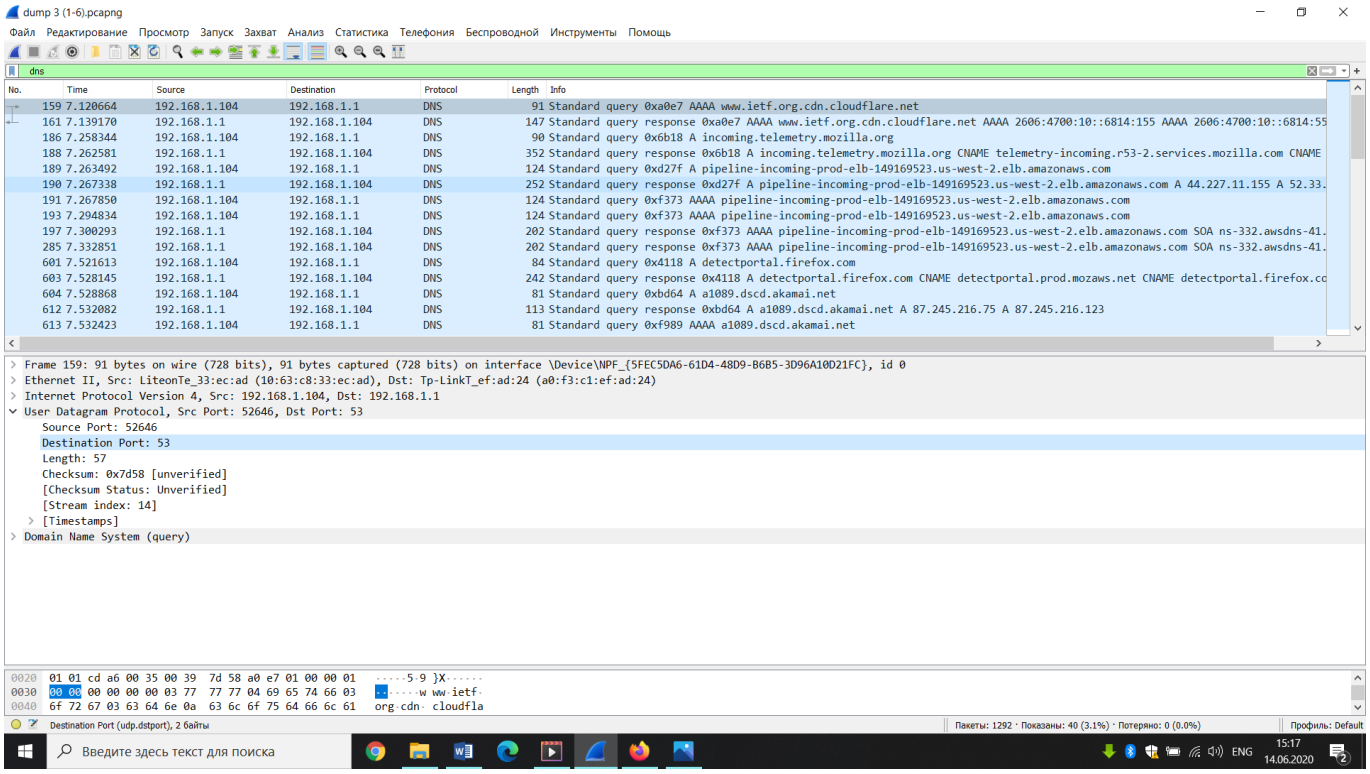

Рис.4

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

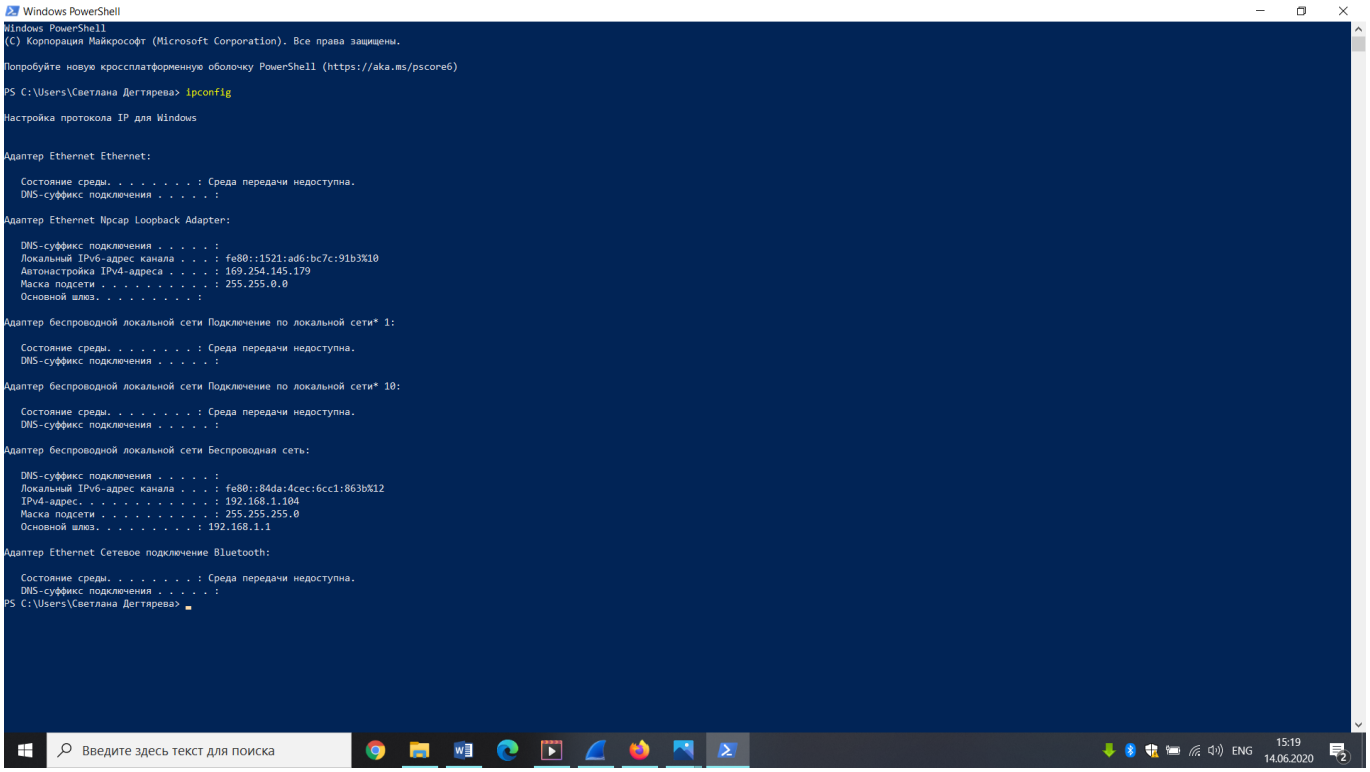

Рис.5

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.

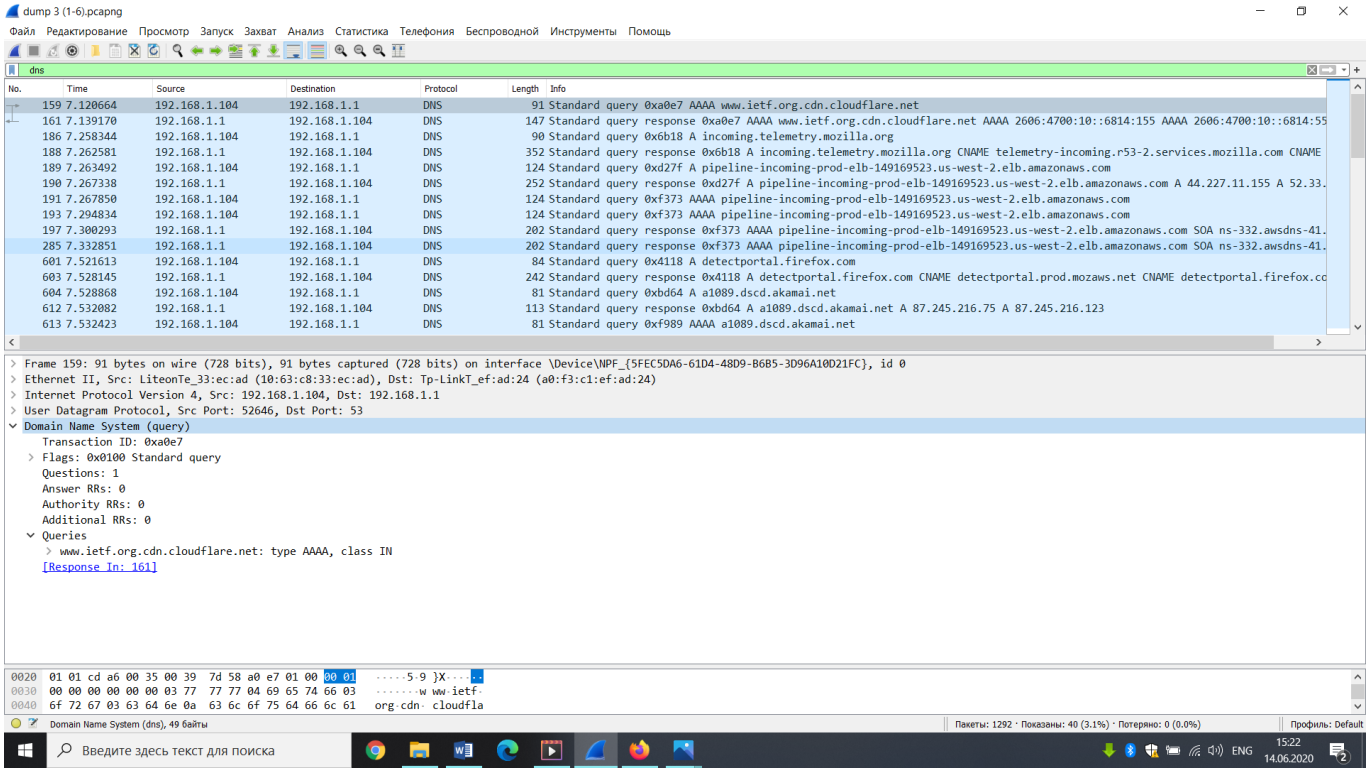

Рис.6

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

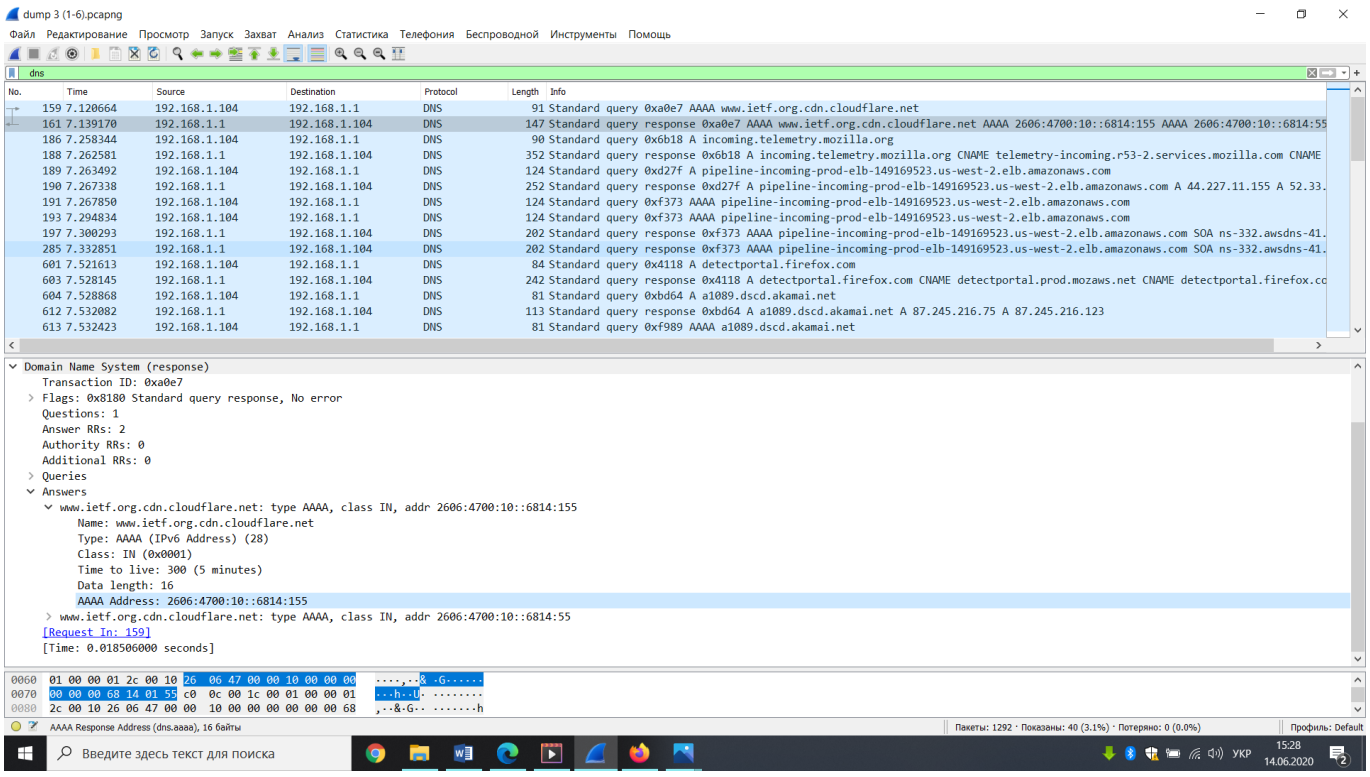

Рис.7

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: 192.168.1.104 співпадає з однією з запропонованих віповідей сервера DNS.

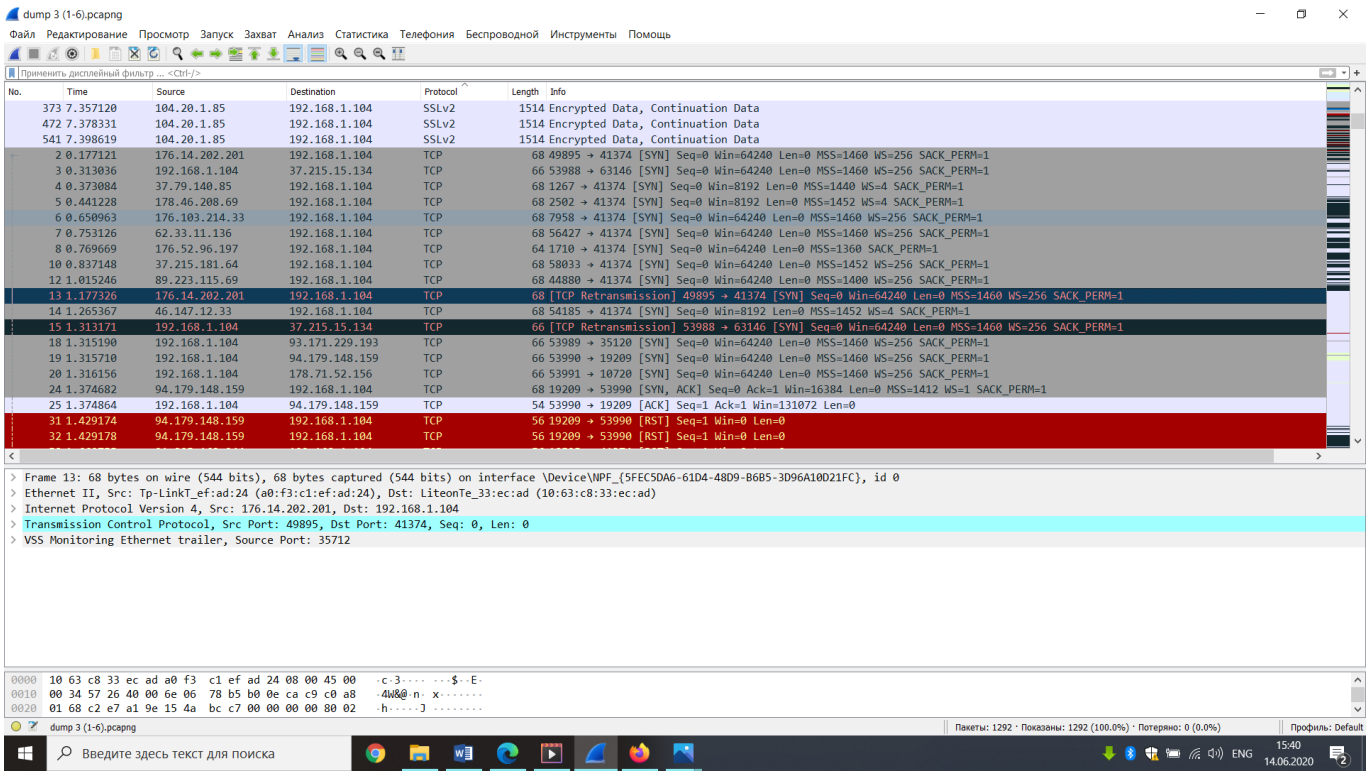

Рис.8

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

Відповідь: так.

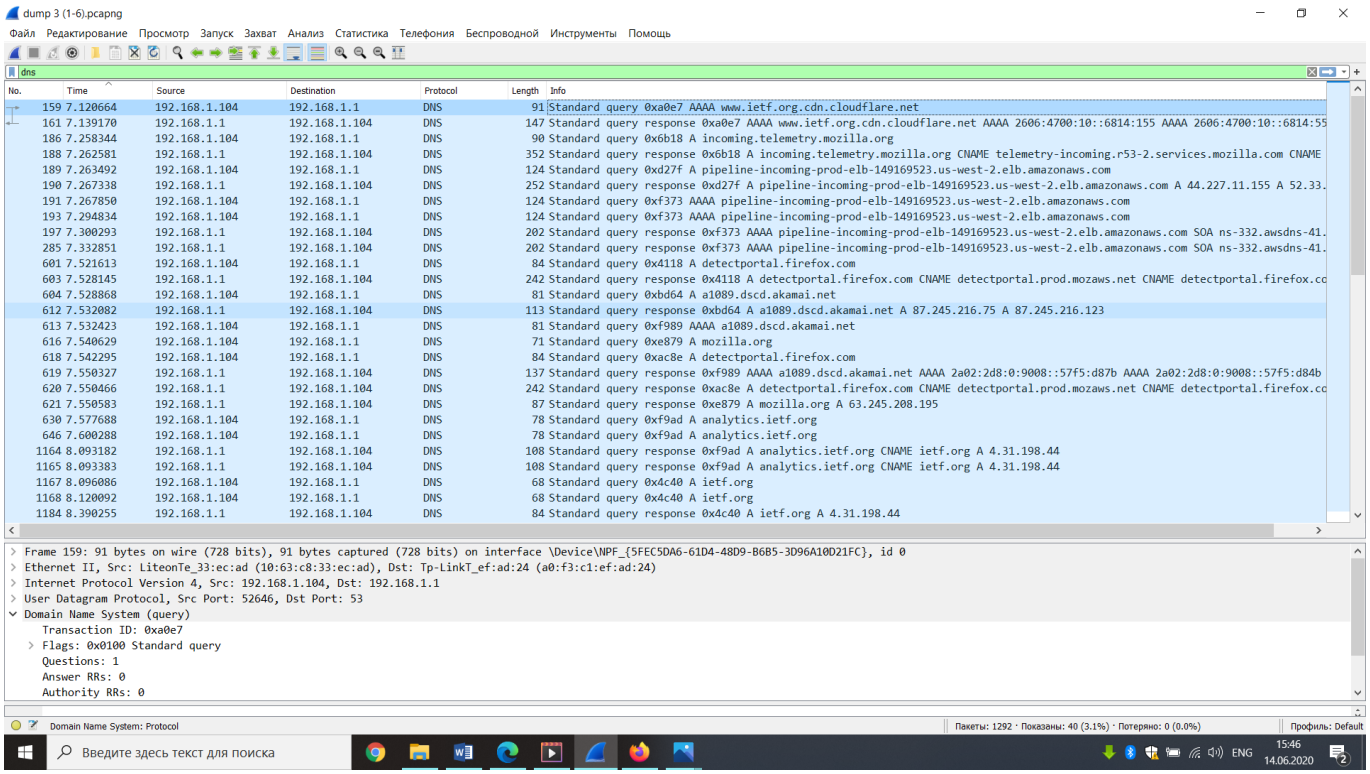

Рис.9

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.

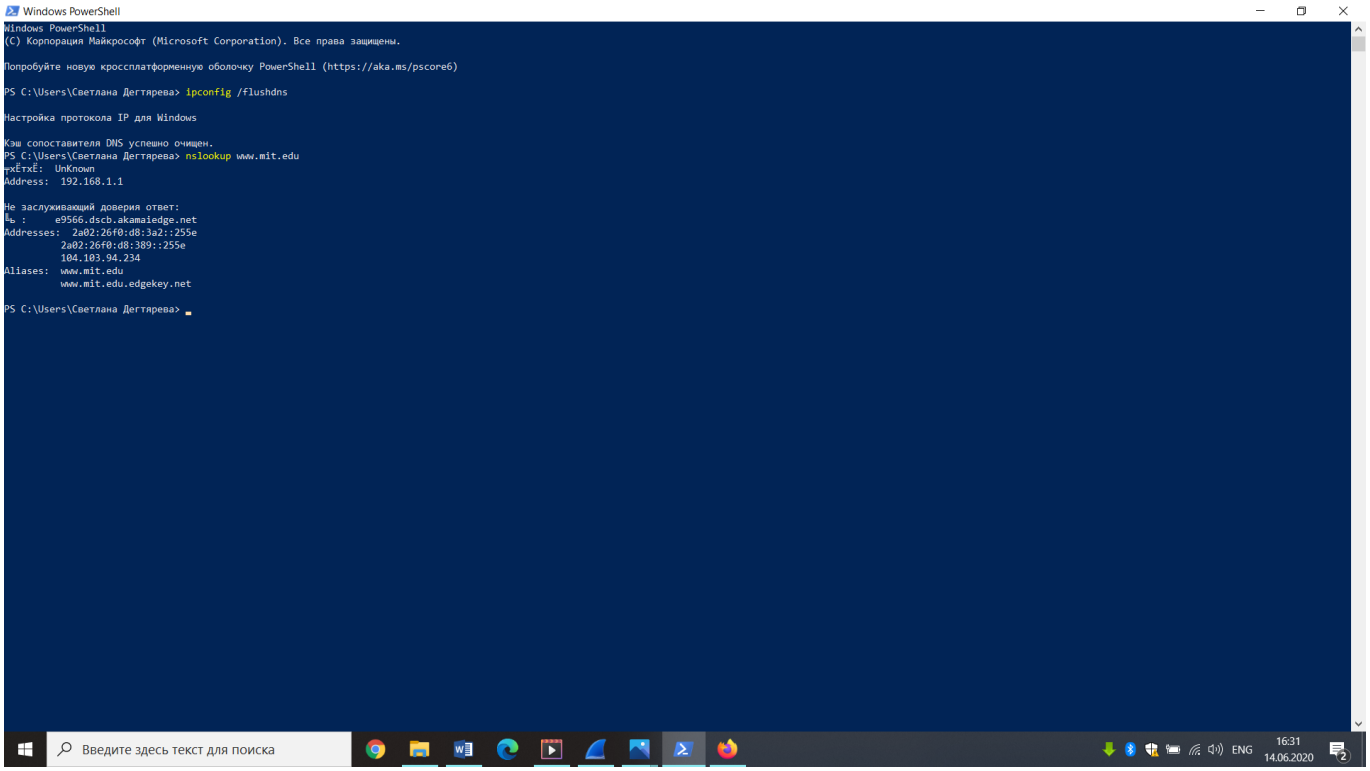

Рис.10

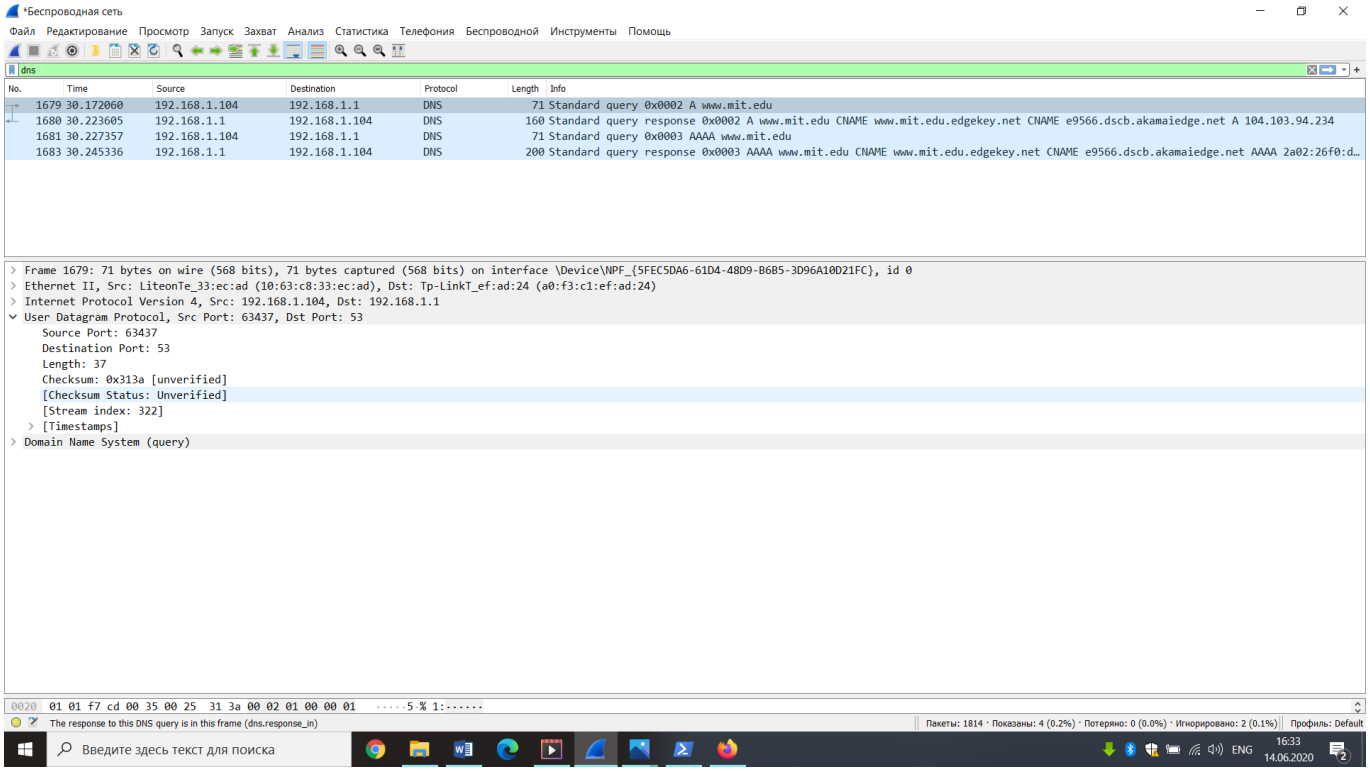

Рис.11

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

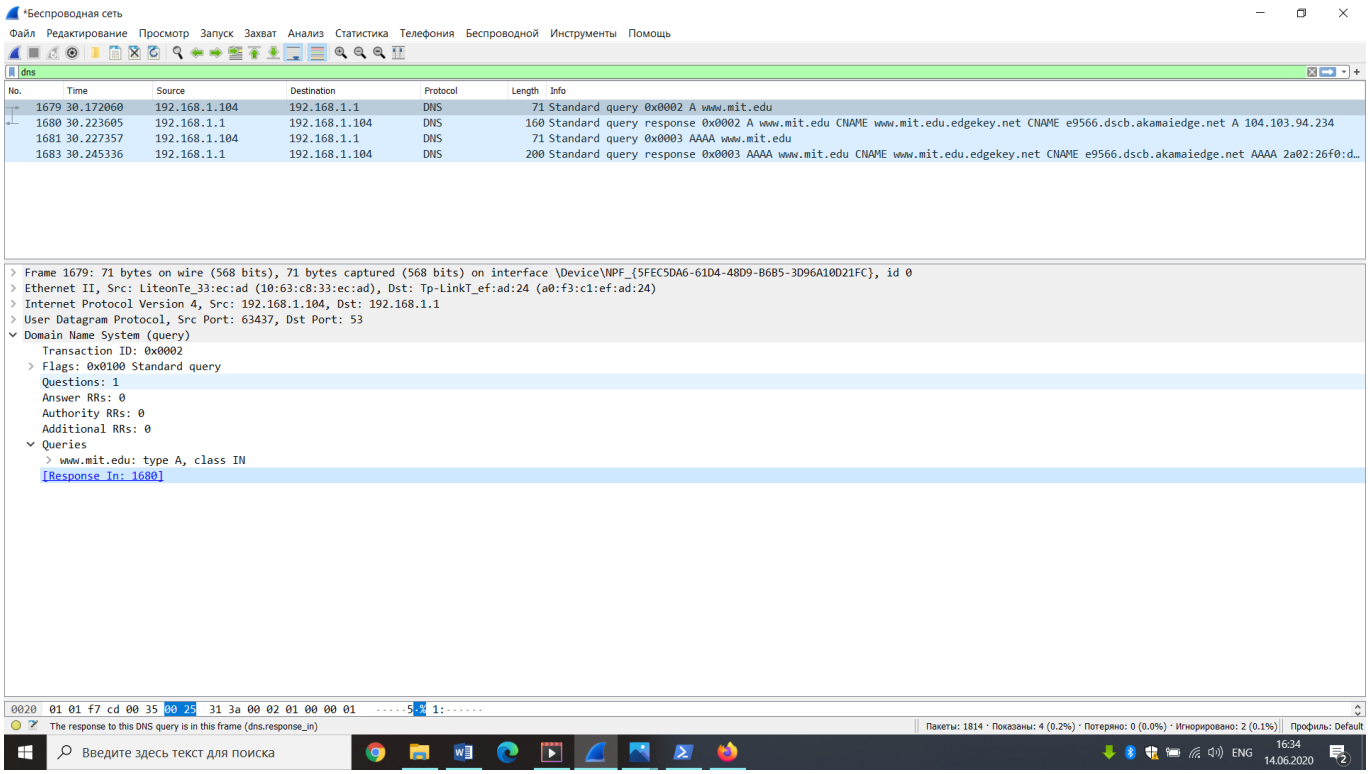

Рис.12

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;

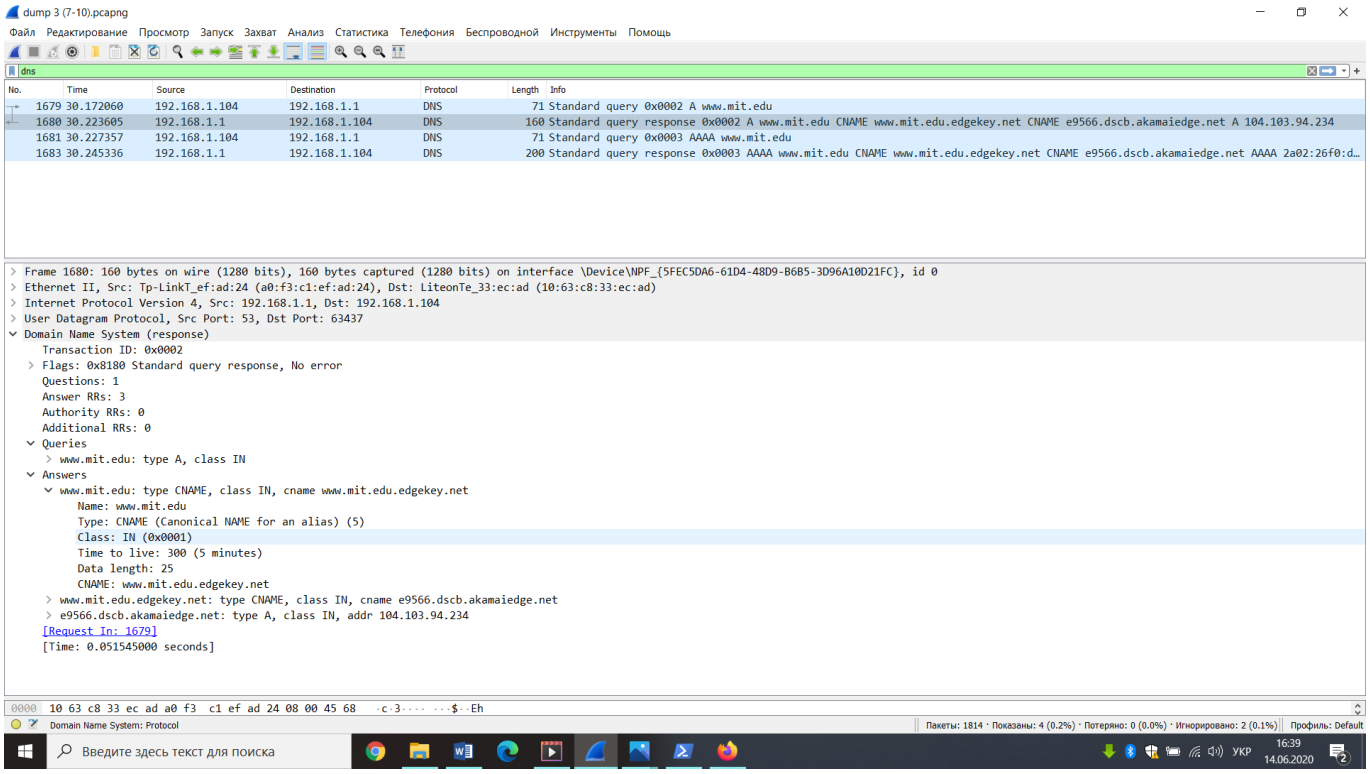

Рис.13

11) 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.

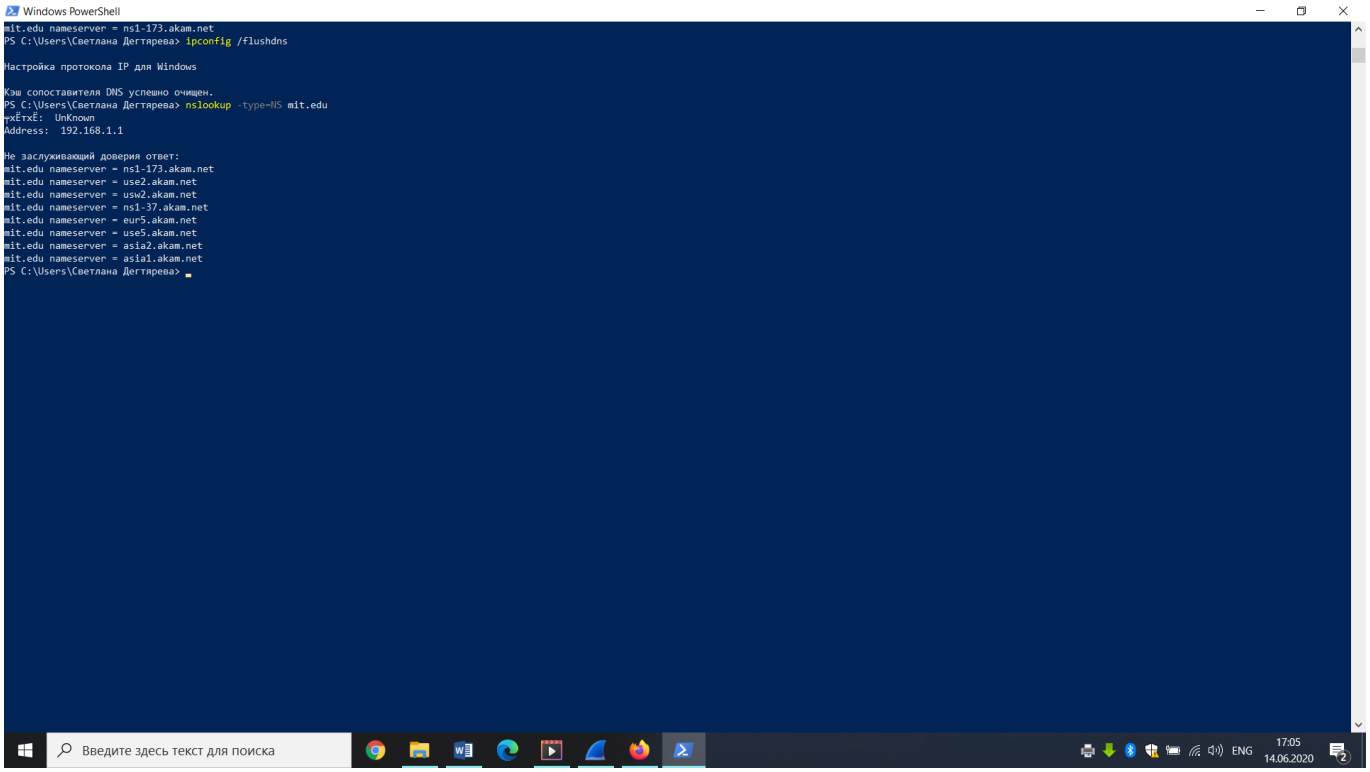

Рис.14

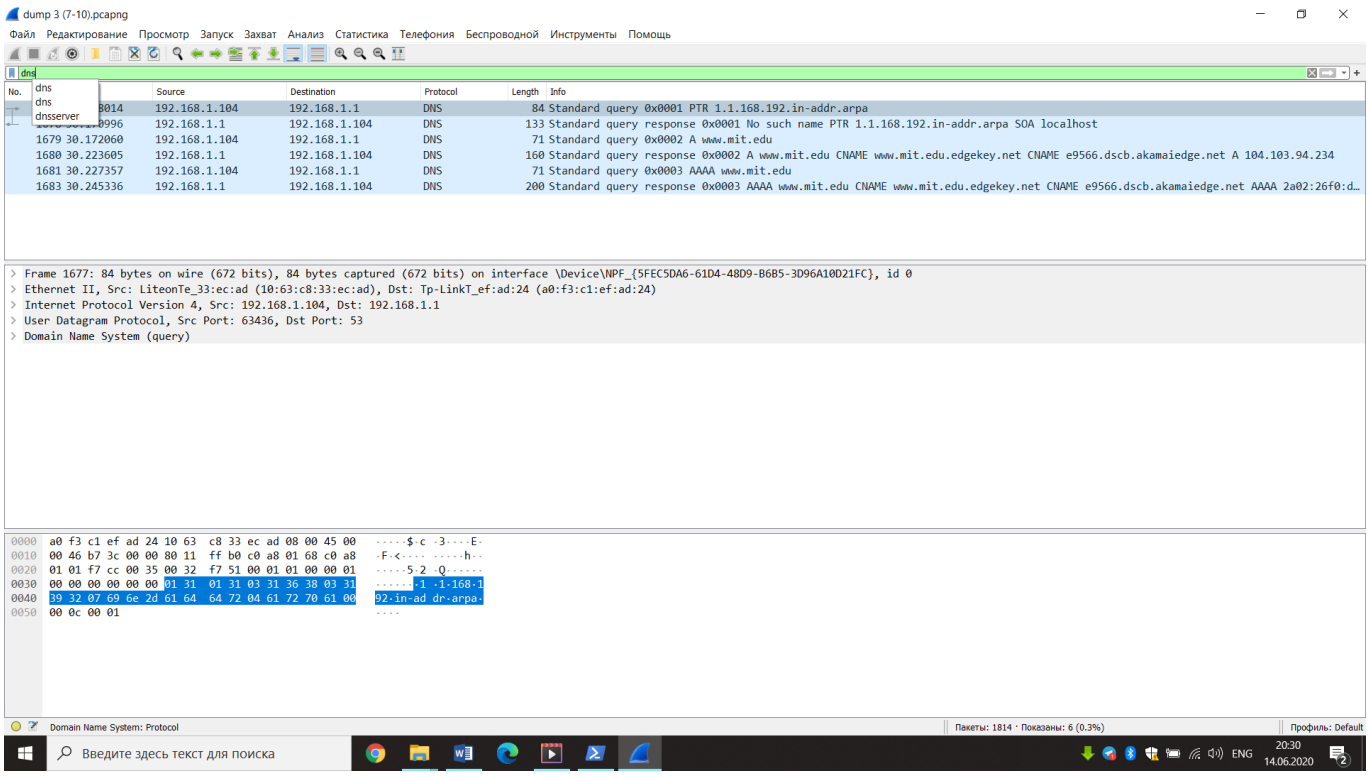

Рис.15

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

Відповідь: було 3 запита. Один з них був типу PTR, другий типу A, третій

типу AAA. Запит типу A вміщує ссилку на відповіді: [Response In: 1680].

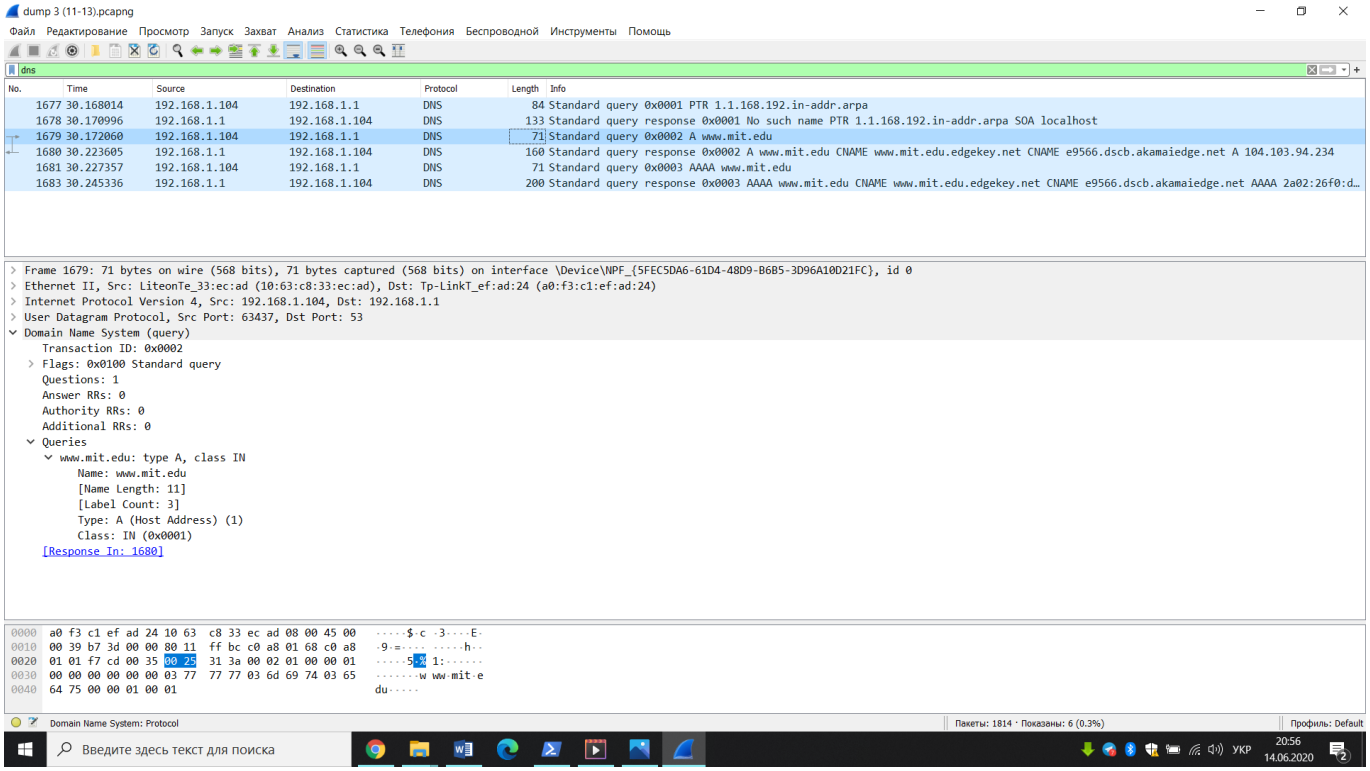

Рис.16

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?

Відповідь: Було взагалі 3 запита і 3 відповіді. У другій відповіді було запропоновано 3 записи:

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

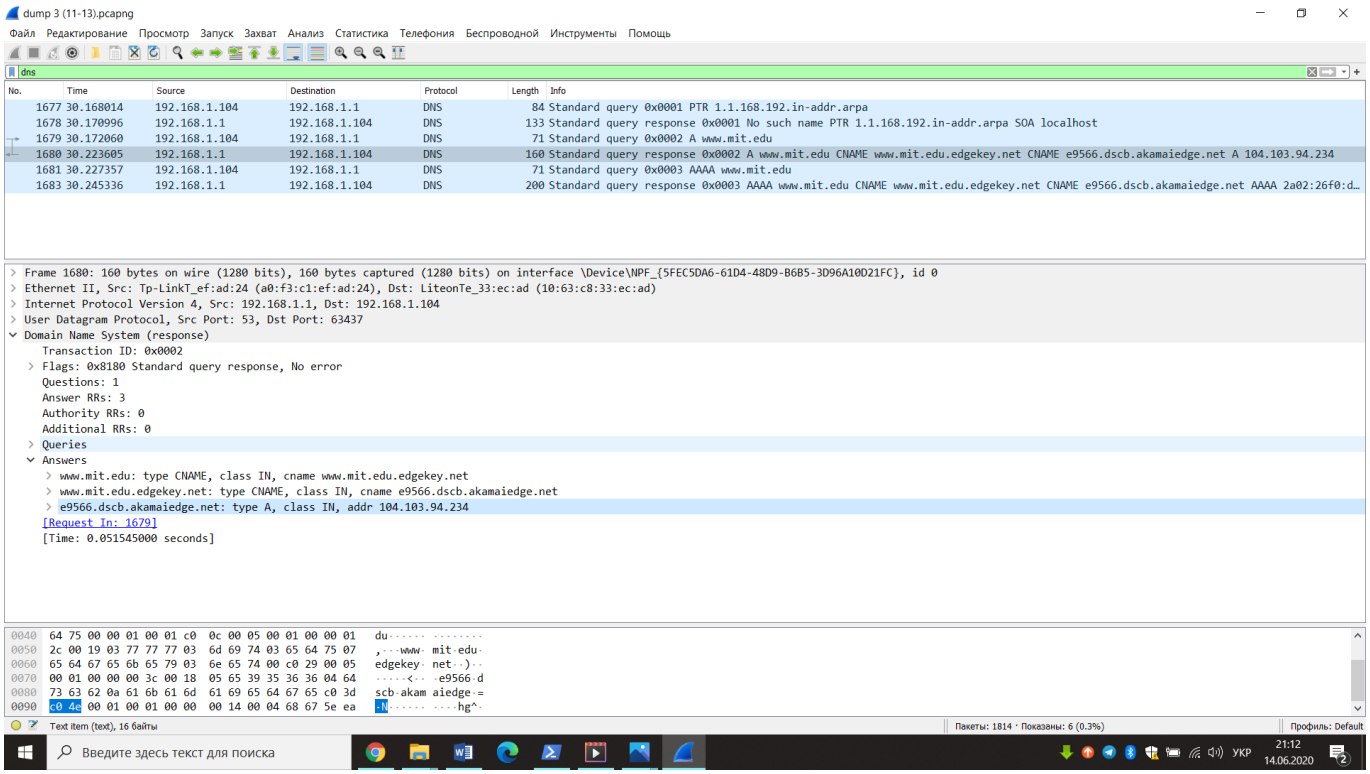

Рис.17

Кожна з відповідей складаєеться з таких полів:

Name, Type, Class, TTL, Data length, CNAME або IP Address;

Приклад відповіді:

mit.edu: type NS, class IN, ns asia1.akam.net

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

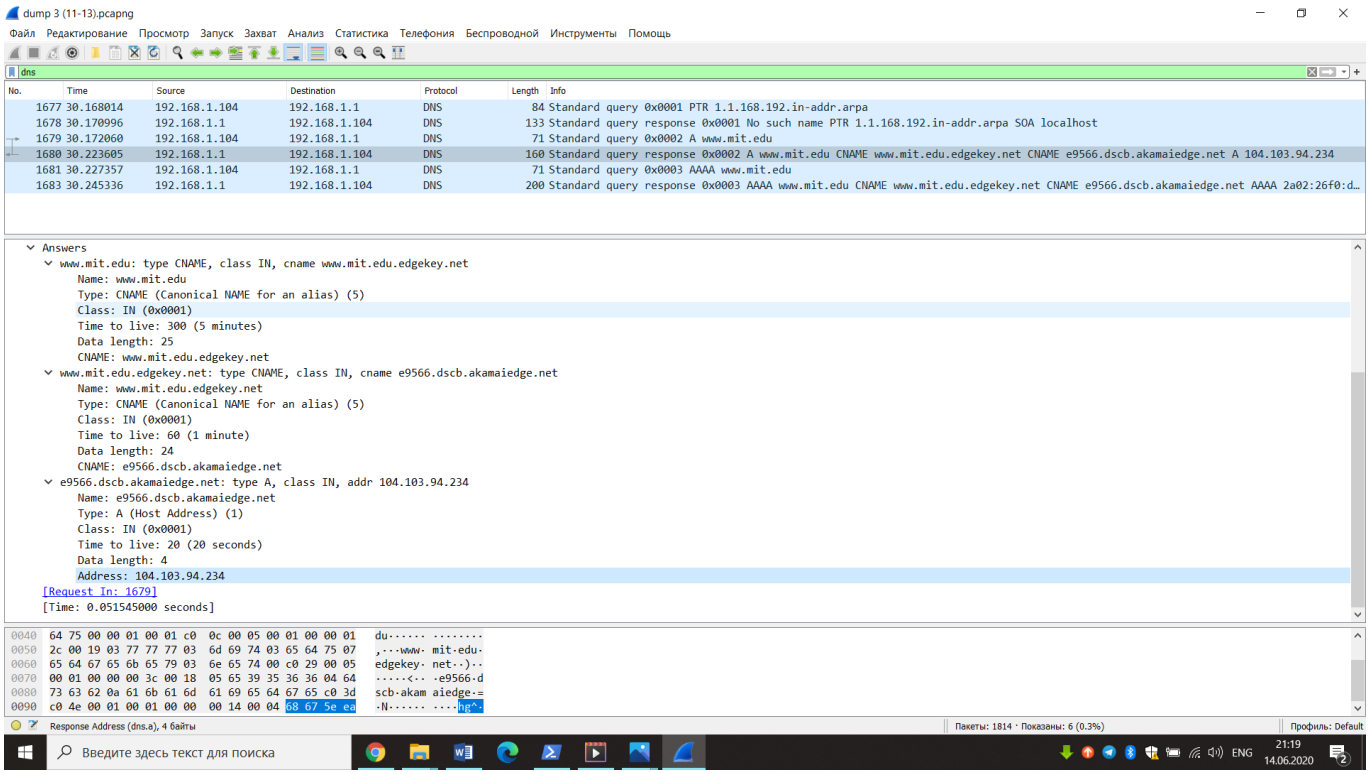

Рис.18

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?

Відповідь: Destination: 192.168.1.1 – це є адреса локального сервера DNS за замовчанням, також був запит на Destination: 18.0.72.3

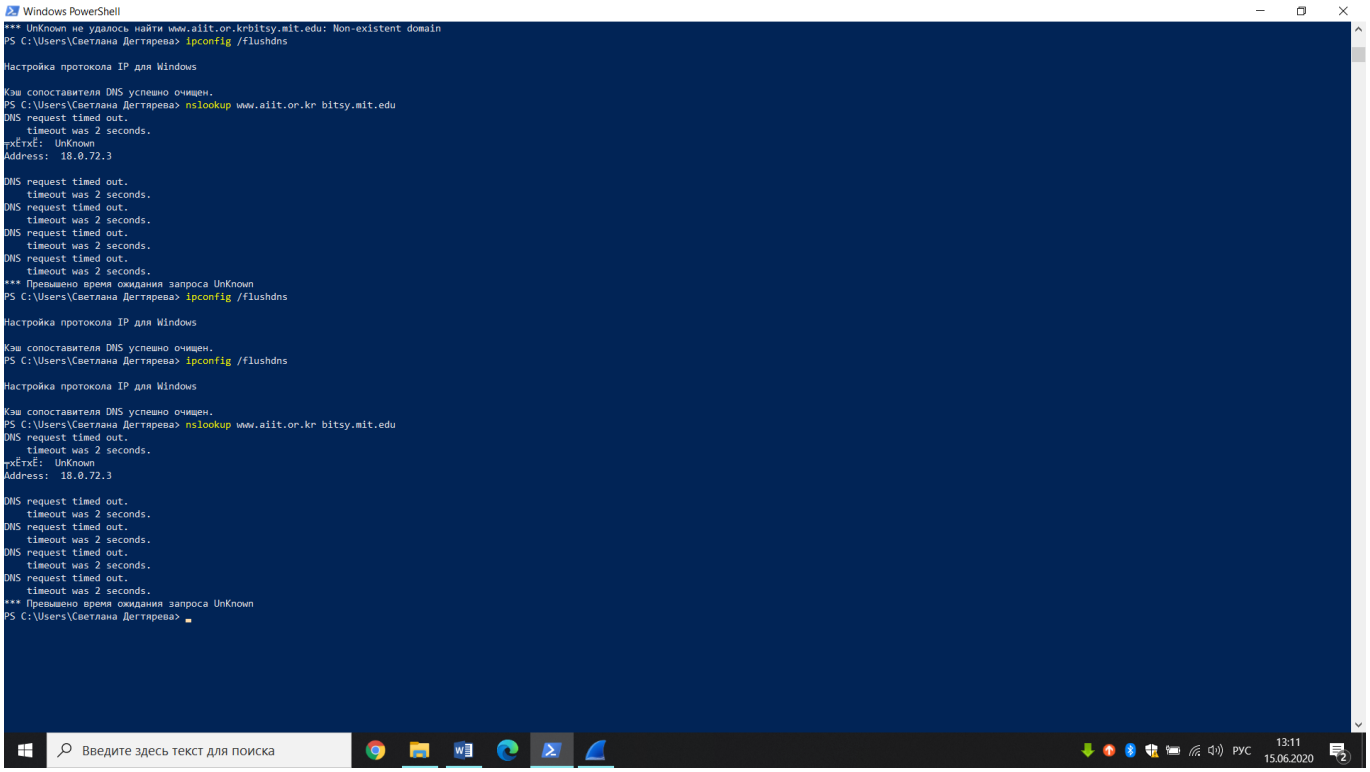

Рис.19

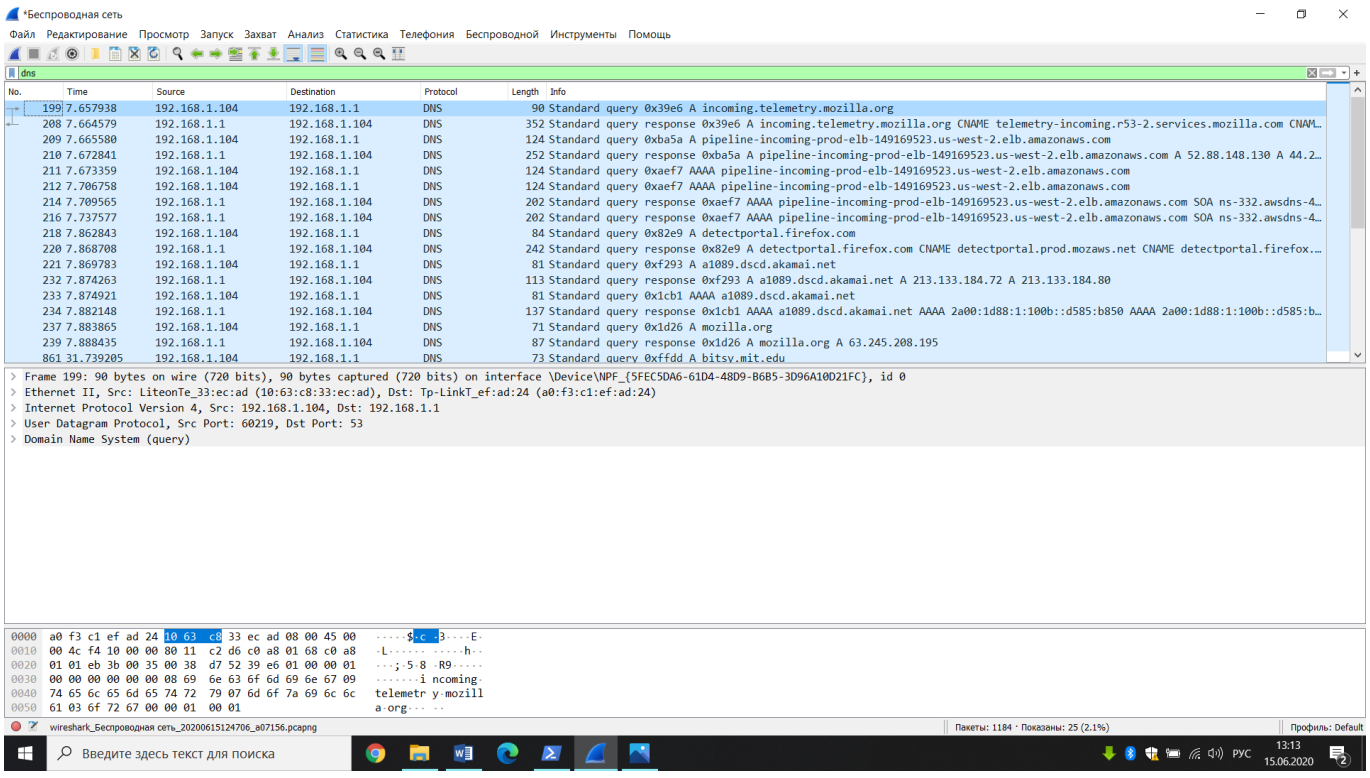

Рис.20

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

Відповідь: Були запити тупу A, AAAA та PTR. Запит типу A вміщує ссилку на

відповіді: Response In: 863.

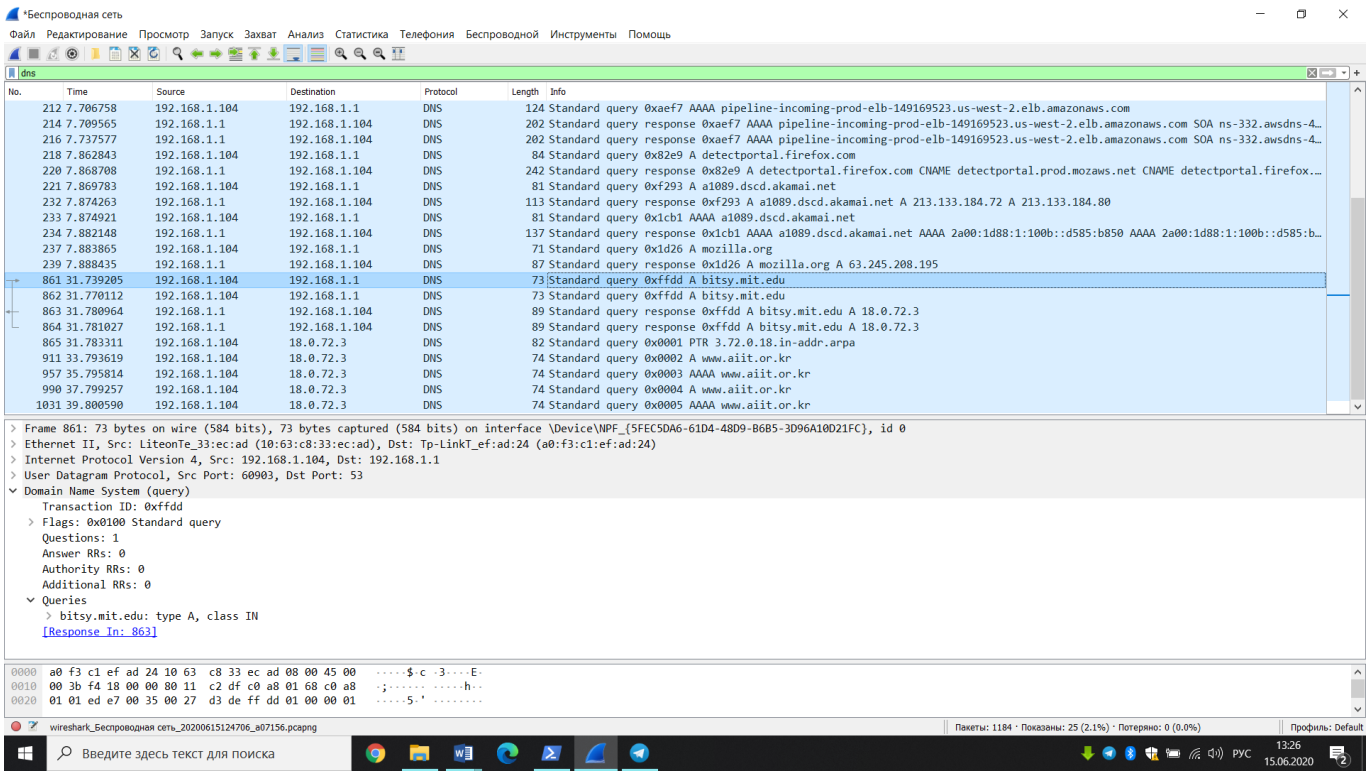

Рис.21

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

Відповідь: Взагалі було виконано 25 запитів та 10 відповідей DNS. У відповіді для bitsy.mit.edu було 1 відповідь, яка складається з таких полів:

Name, Type, Class, TTL, Data length, Address;

Приклад відповіді:

bitsy.mit.edu: type A, class IN, addr 18.0.72.3

Name: bitsy.mit.edu

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 4

Address: 18.0.72.3

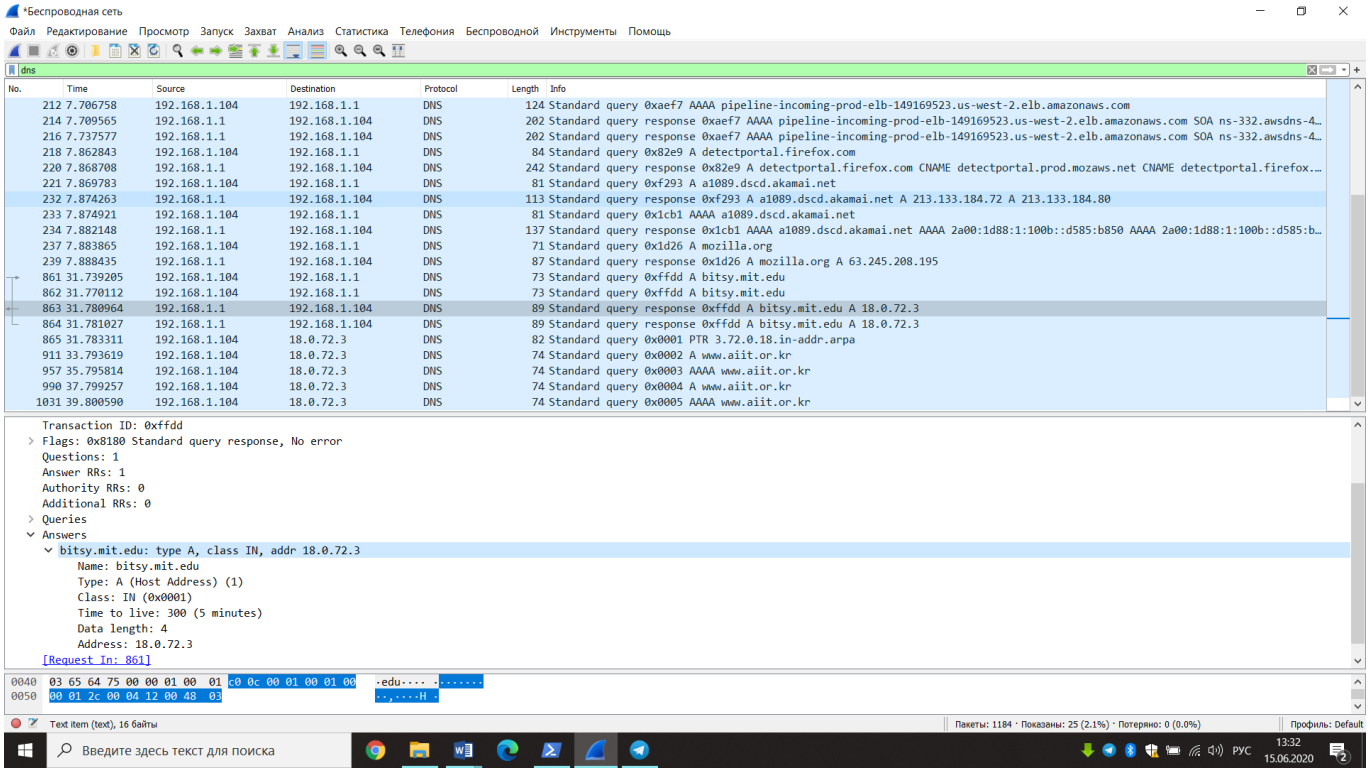
*Беспроводная сеть
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
dns
No. Time Source Destination Protocol Length Info
212 7.706758 192.168.1.104 192.168.1.1 DNS 124 Standard query 0xaef7 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com
214 7.709565 192.168.1.1 192.168.1.104 DNS 202 Standard query response 0xaef7 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com SOA ns-332.awsdns-4…
216 7.737577 192.168.1.1 192.168.1.104 DNS 202 Standard query response 0xaef7 AAAA pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com SOA ns-332.awsdns-4…
218 7.862843 192.168.1.104 192.168.1.1 DNS 84 Standard query 0x82e9 A detectportal.firefox.com
220 7.868708 192.168.1.1 192.168.1.104 DNS 242 Standard query response 0x82e9 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME detectportal.firefox.…
221 7.869783 192.168.1.104 192.168.1.1 DNS 81 Standard query 0xf293 A a1089.dscd.akamai.net
232 7.874263 192.168.1.1 192.168.1.104 DNS 113 Standard query response 0xf293 A a1089.dscd.akamai.net A 213.133.184.72 A 213.133.184.80
233 7.874921 192.168.1.104 192.168.1.1 DNS 81 Standard query 0x1cb1 AAAA a1089.dscd.akamai.net
234 7.882148 192.168.1.1 192.168.1.104 DNS 137 Standard query response 0x1cb1 AAAA a1089.dscd.akamai.net AAAA 2a00:1d88:1:100b::d585:b850 AAAA 2a00:1d88:1:100b::d585:b…
237 7.883865 192.168.1.104 192.168.1.1 DNS 71 Standard query 0x1d26 A mozilla.org
239 7.888435 192.168.1.1 192.168.1.104 DNS 87 Standard query response 0x1d26 A mozilla.org A 63.245.208.195
861 31.739205 192.168.1.104 192.168.1.1 DNS 73 Standard query 0xffdd A bitsy.mit.edu
862 31.770112 192.168.1.104 192.168.1.1 DNS 73 Standard query 0xffdd A bitsy.mit.edu
863 31.780964 192.168.1.1 192.168.1.104 DNS 89 Standard query response 0xffdd A bitsy.mit.edu A 18.0.72.3
864 31.781027 192.168.1.1 192.168.1.104 DNS 89 Standard query response 0xffdd A bitsy.mit.edu A 18.0.72.3
865 31.783311 192.168.1.104 18.0.72.3 DNS 82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
911 33.793619 192.168.1.104 18.0.72.3 DNS 74 Standard query 0x0002 A www.aiit.or.kr
957 35.795814 192.168.1.104 18.0.72.3 DNS 74 Standard query 0x0003 AAAA www.aiit.or.kr
990 37.799257 192.168.1.104 18.0.72.3 DNS 74 Standard query 0x0004 A www.aiit.or.kr
1031 39.800590 192.168.1.104 18.0.72.3 DNS 74 Standard query 0x0005 AAAA www.aiit.or.kr
Transaction ID: 0xffdd
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
bitsy.mit.edu: type A, class IN, addr 18.0.72.3
Name: bitsy.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 18.0.72.3
[Request In: 861]
0040 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 ·edu···· ·····
0050 00 01 2c 00 04 12 00 48 03 ··,····H ·
Text item (text), 16 байты
Пакеты: 1184 · Показаны: 25 (2.1%) · Потеряно: 0 (0.0%)
Профиль: Default
Введите здесь текст для поиска
РУС
13:32
15.06.2020

Рис.22