Міністерство 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

Мартиновська Т.В.

Прийняв: Кухарєв С.О.

Київ – 2020

**Лабораторна робота 3**

1. Хід роботи

1. Очистіть кеш DNS-записів

2. Запустіть веб-браузер, очистіть кеш браузера

3. Запустіть Wireshark, почніть захоплення пакетів.

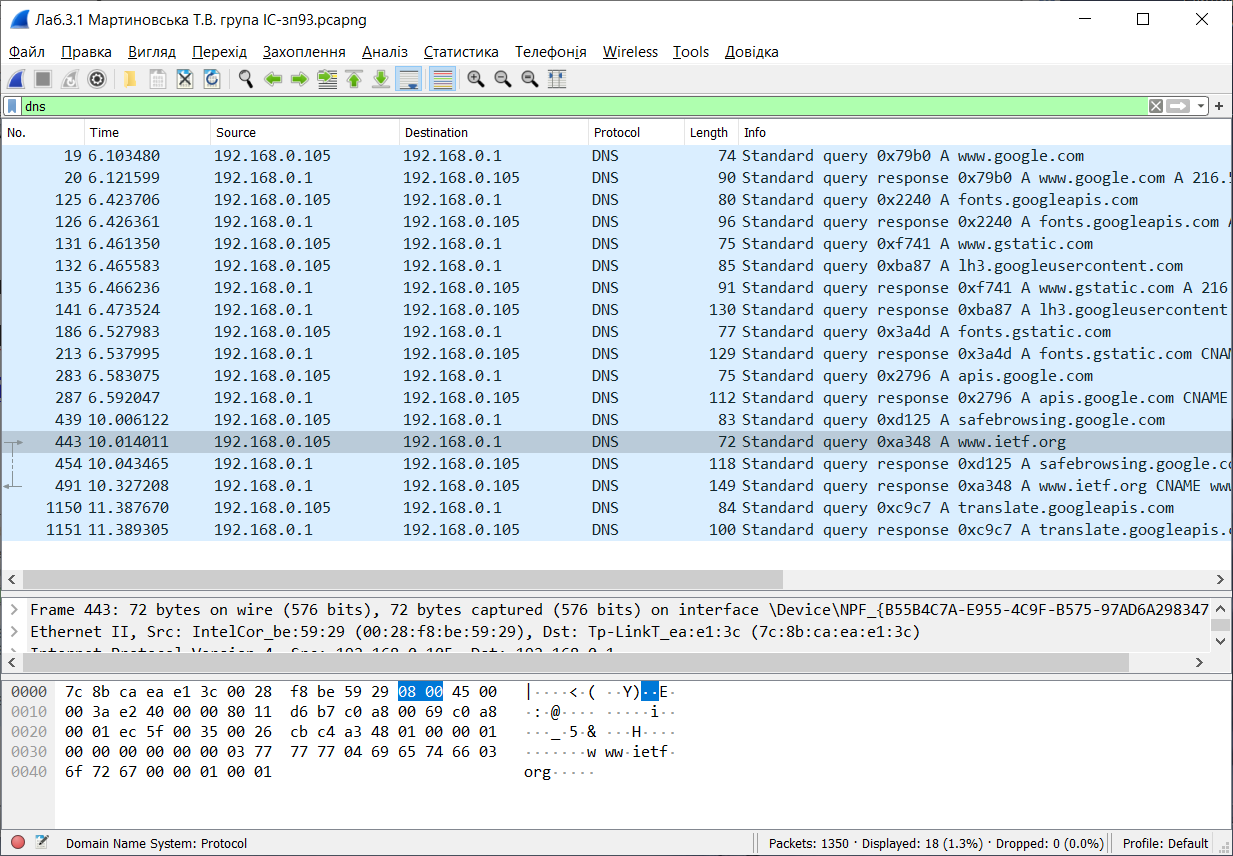
4. Відкрийте за допомогою браузера одну із зазначених нижче адрес:

<http://www.ietf.org>

5. Зупиніть захоплення пакетів.

6. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків+/-).

7. Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.

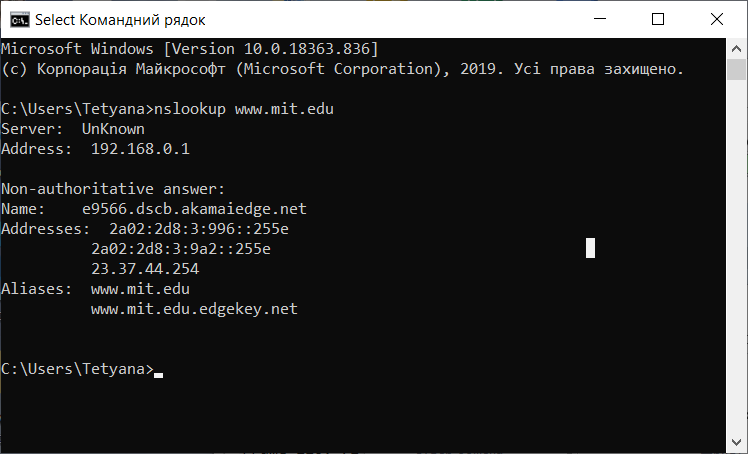


Мал.1

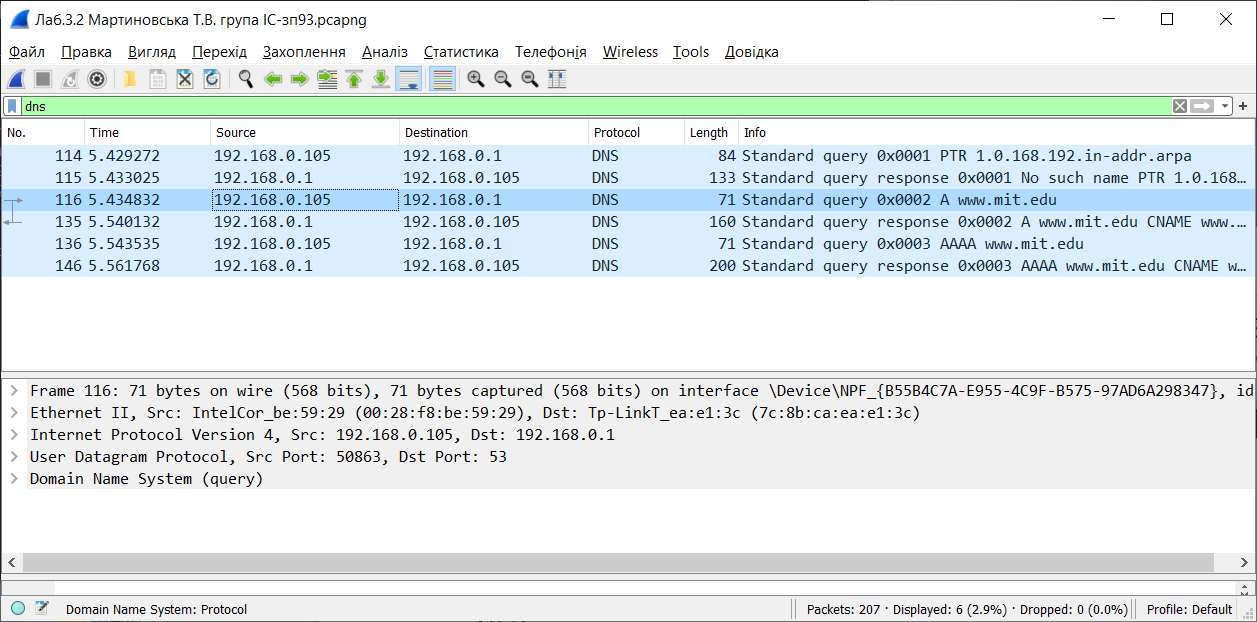
8. Почніть захоплення пакетів.

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

a. nslookup [www.mit.edu](http://www.mit.edu)



Мал.2



Мал.3

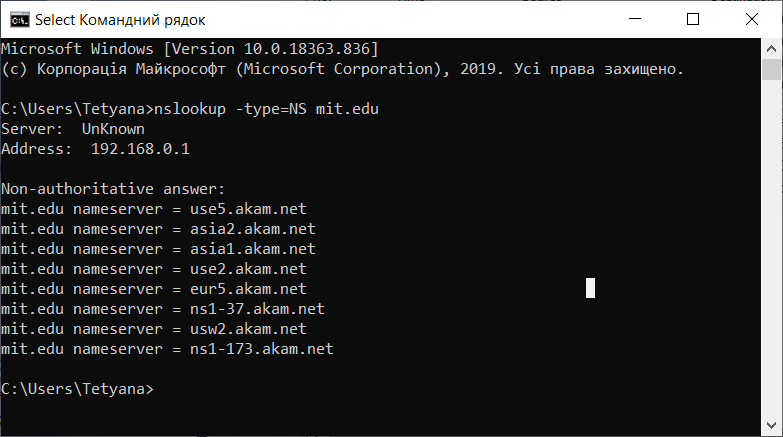
10.Зупиніть захоплення пакетів.

11.Приготуйте відповіді на контрольні запитання 7-10, роздрукуйте 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.

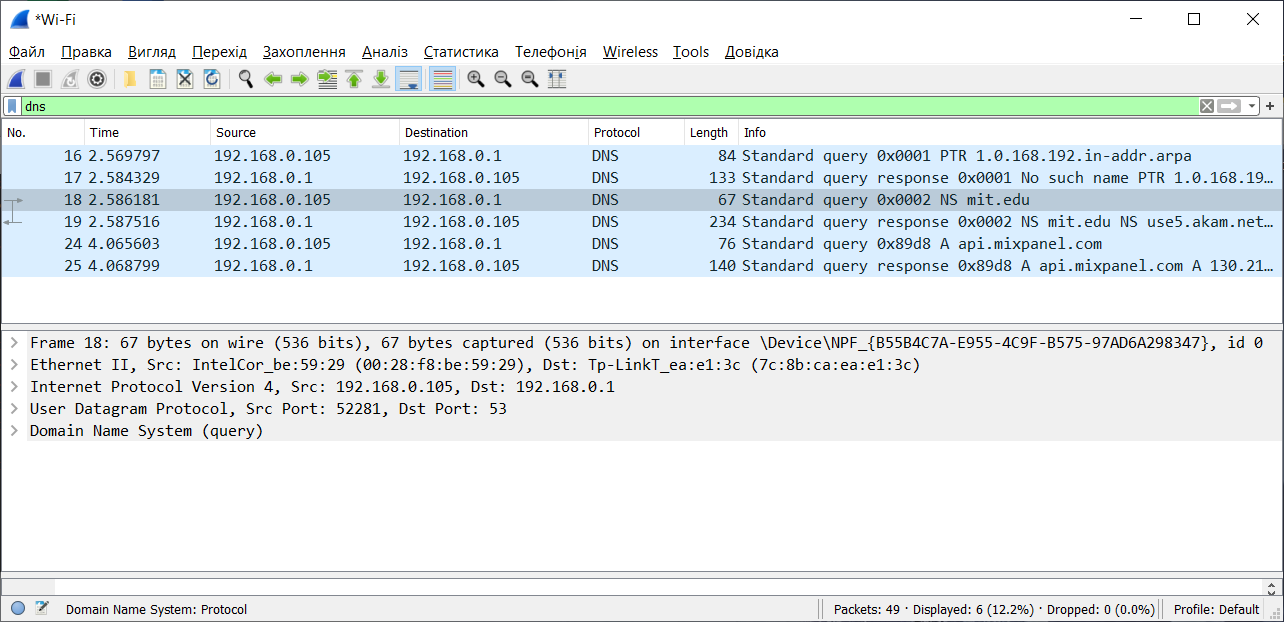
12.Почніть захоплення пакетів.

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

a. nslookup –type=NS mit.edu



Мал.4



Мал.5

14. Зупиніть захоплення пакетів.

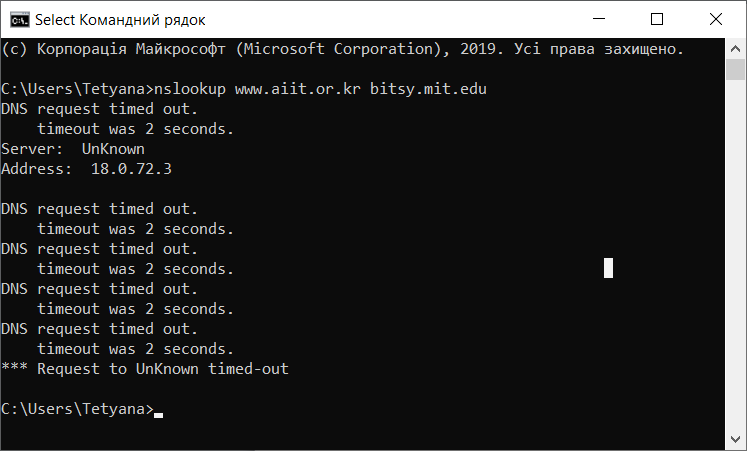
15.Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети.

16.Почніть захоплення пакетів.

17.Виконайте nslookup для домену www.mit.edu за допомогою команди

a. nslookup www.aiit.or.kr bitsy.mit.edu

18.Зупиніть захоплення пакетів.

Мал.6

19.Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякізахоплені пакети.

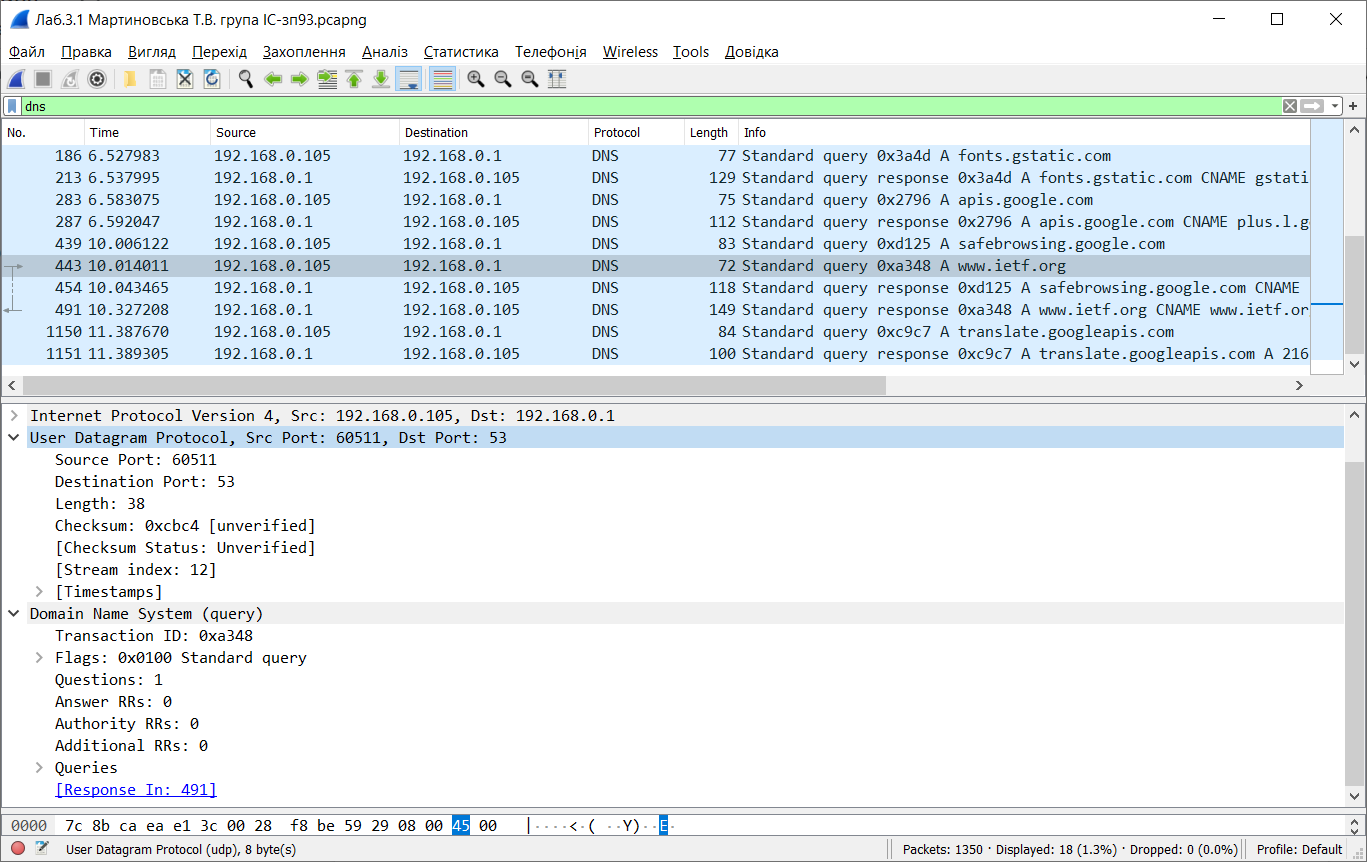
20.Закрийте Wireshark.

**Контрольні запитання:**

1.Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP абоTCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

Відповідь: DNS використовує прототокол UDP, Src Port:60511, Dst Port:53.

Інформація з Wireshark наведено на мал.7.



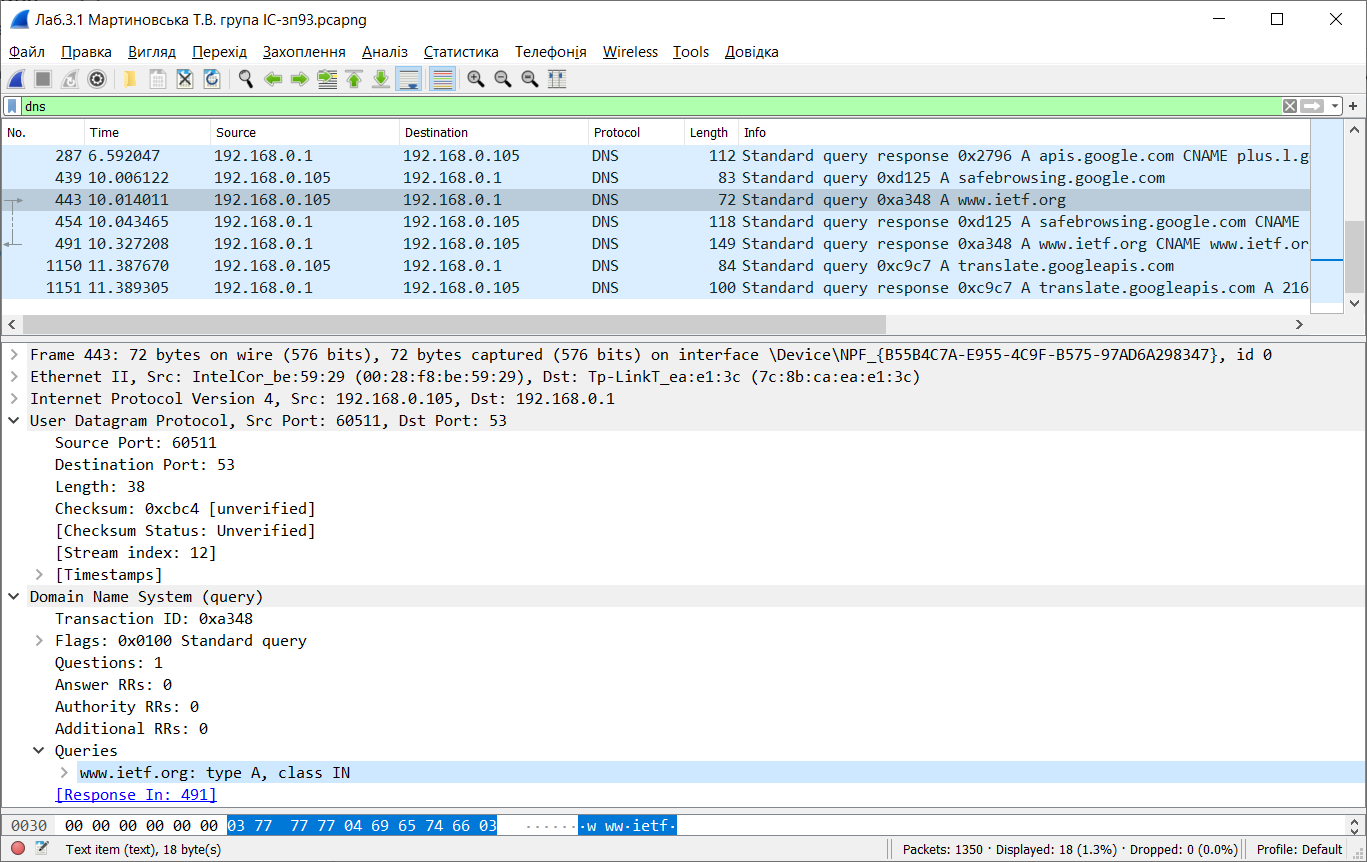
Мал.7

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

Відповідь: Destination: 192.168.0.1 – є адресою локального DNS сервера

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

Type A (Адресний запис, відповідність між ім'ям і IP-адресою). Вміщує посилання на рядок з відповіддю [Response In: 491]. Інформація з Wireshark про тип запиту та можливі компоненти відповідді наведено на мал.8.



Мал.8

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

Відповідь: Дсліджуємо [www.ietf.org](http://www.ietf.org): Отримано 3 відповіді:

-www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net

-www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

-www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

Адресні записи, відповідність між ім'ям і IP-адресою.

Структура кожної відповідь (на прикладі [www.ietf.org](http://www.ietf.org)):

-Name: [www.ietf.org](http://www.ietf.org)

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

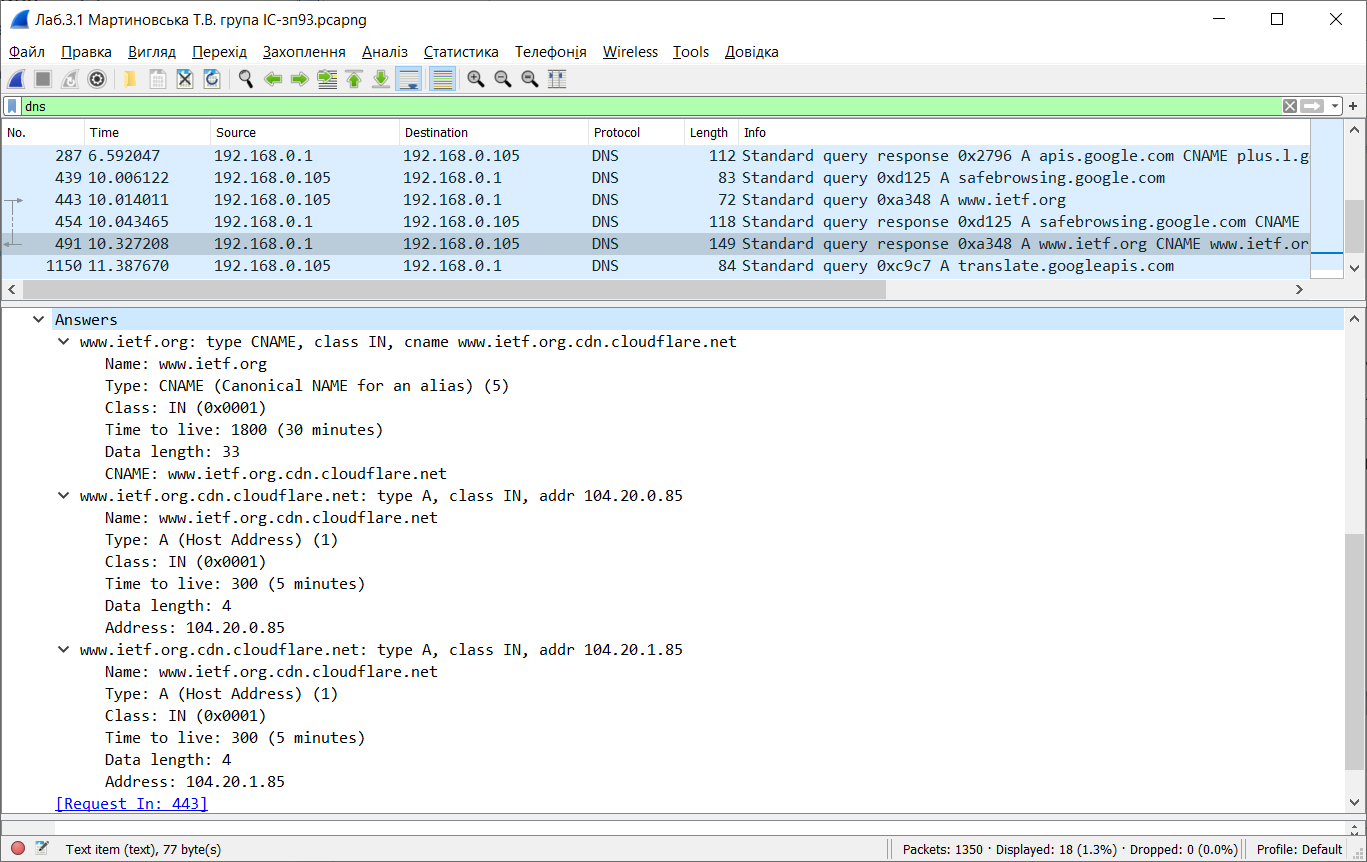
-Class: IN (0x0001)

-Time to live: 1800 (30 minutes)

-Data length: 33

-CNAME: www.ietf.org.cdn.cloudflare.net

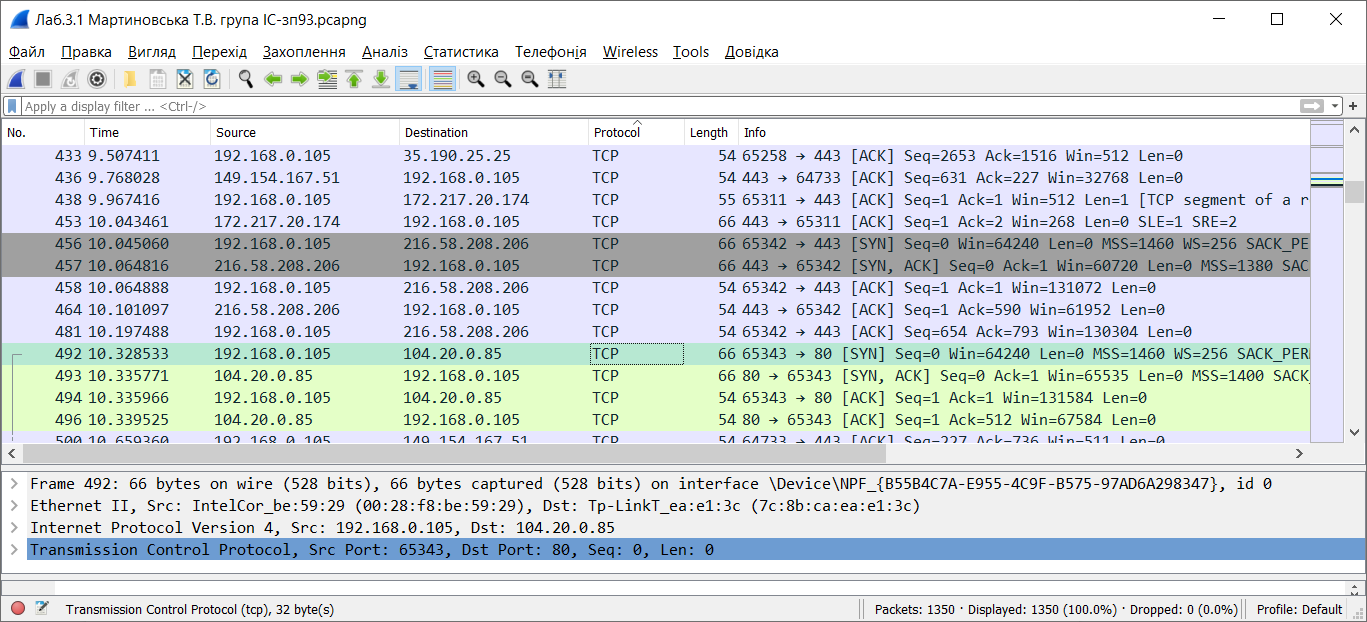
Інформація з Wireshark про відповідді запропоновані сервером наведено на мал.9



Мал.9

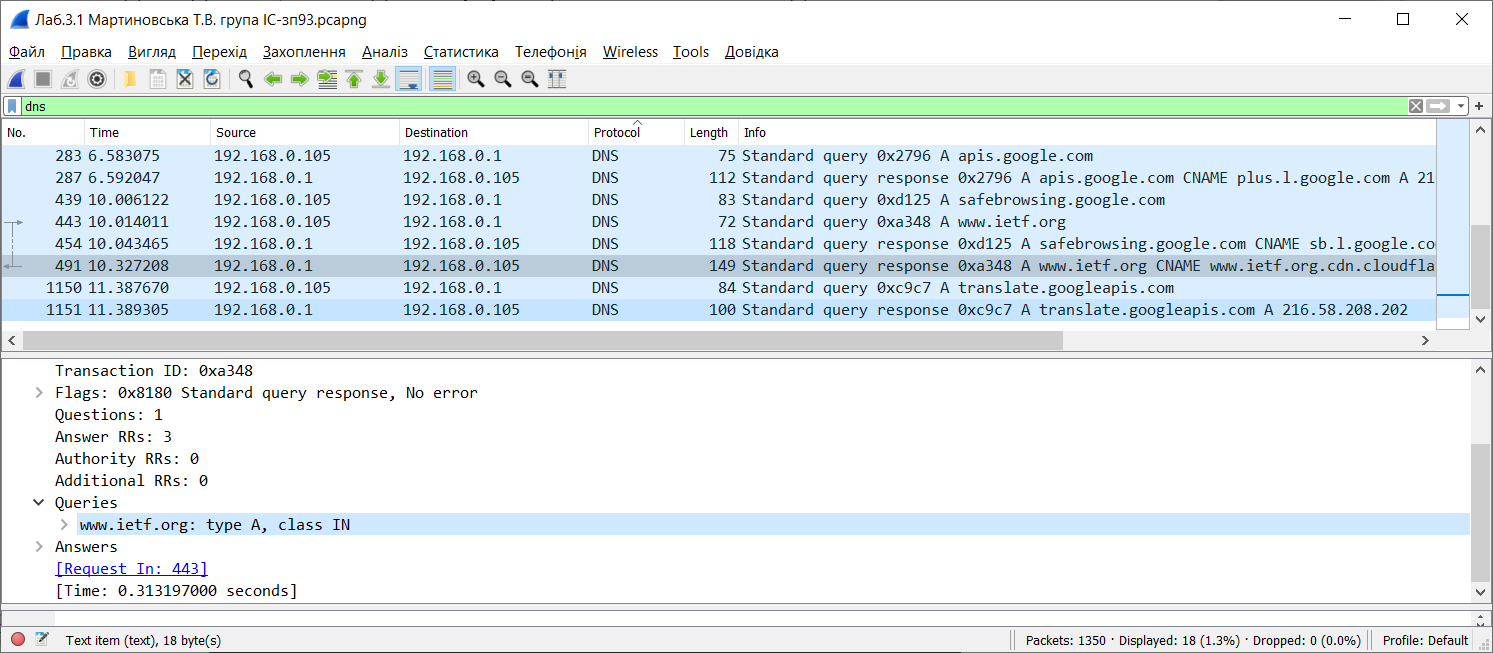
5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

Відповідь:Так, співпадає. Інформація з Wireshark наведено на мал.10.

Мал.10

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

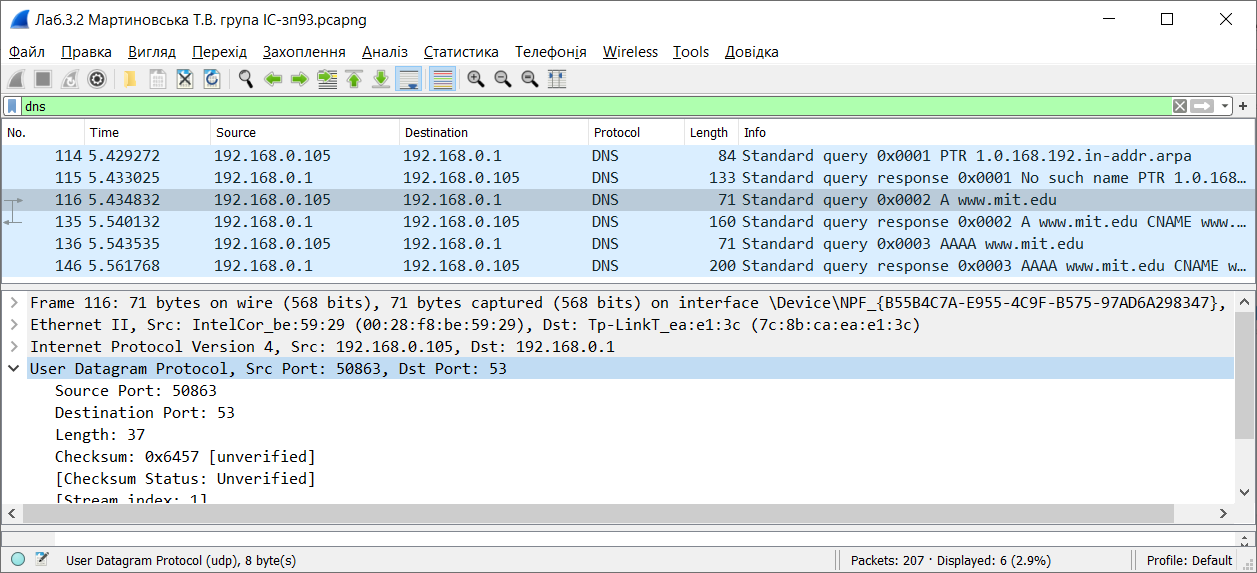
Відповідь: Так, було здійснено ще один DNS запит на отримання IP-адреси ресурсу www.ietf.org.



Мал.11

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

Відповідь: Src Port: 50863, Dst Port: 53



Мал.12

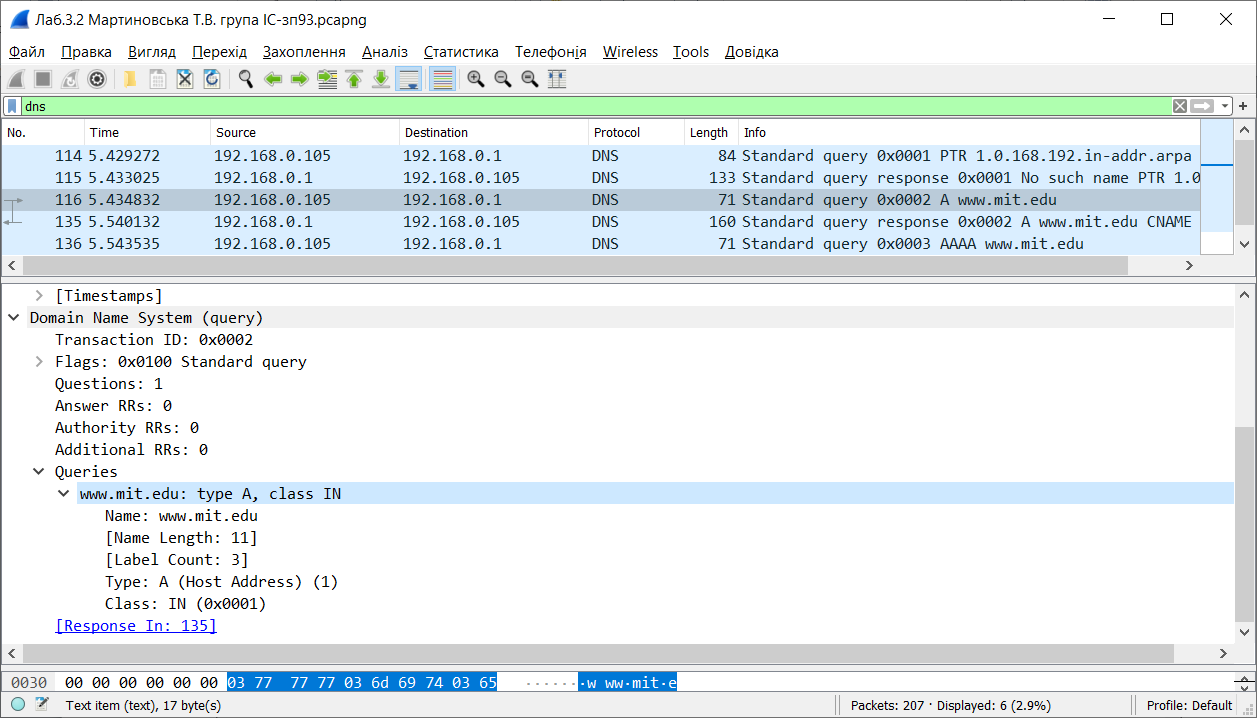
8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Відповідь: Destination: 192.168.0.1 – є адресою локального DNS сервера

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

Відповідь: Type A (Адресний запис, відповідність між ім'ям і IP-адресою),

вміщує посилання на рядок з відповіддю [Response In: 135]



Мал.13

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

Відповідь: Отримано 3 відповіді:

Структура відповіді на прикладі [www.mit.edu](http://www.mit.edu):

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

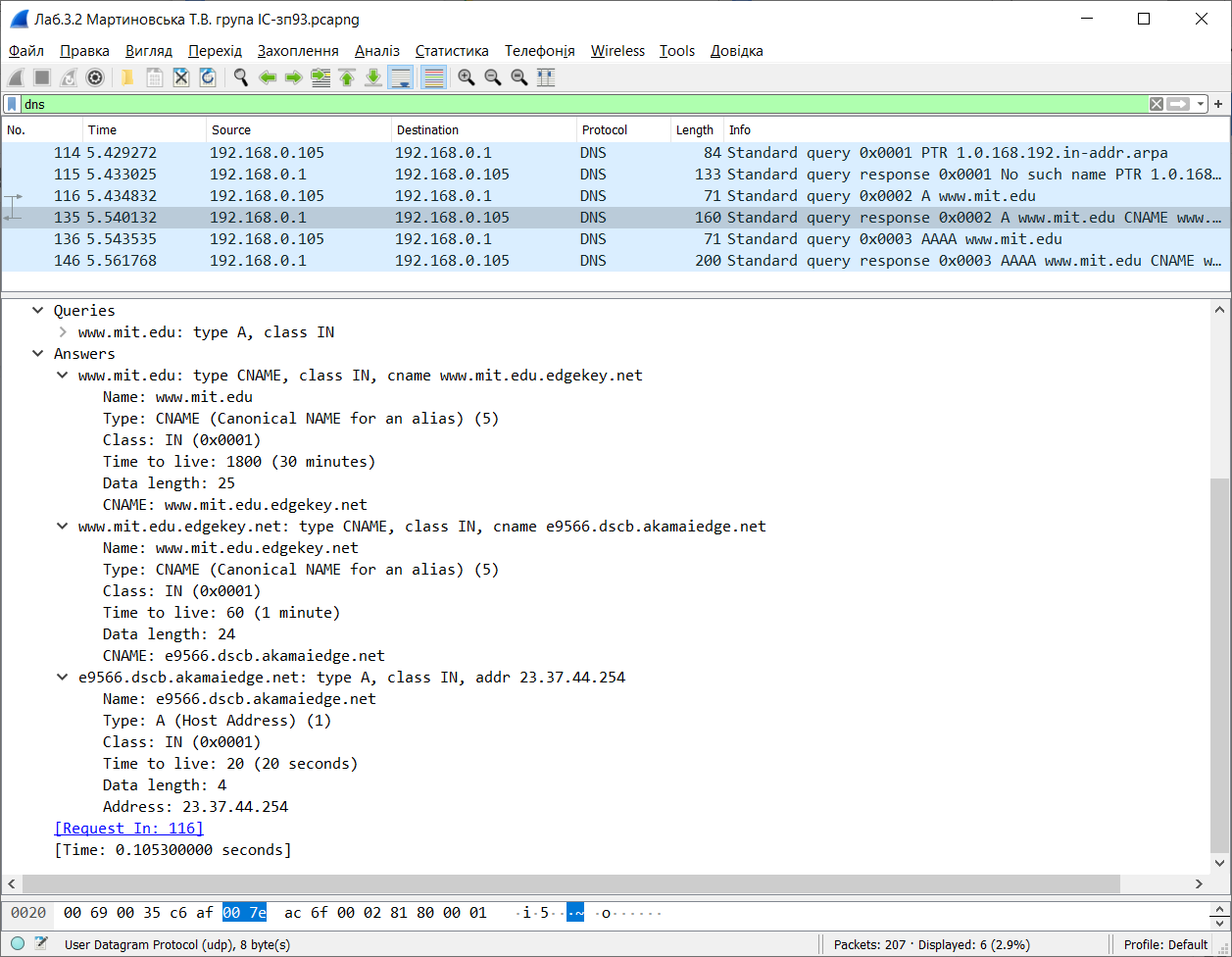
- Type: CNAME (Canonical NAME for an alias) (5)

-Class: IN (0x0001)

-Time to live: 1800 (30 minutes)

-Data length: 25

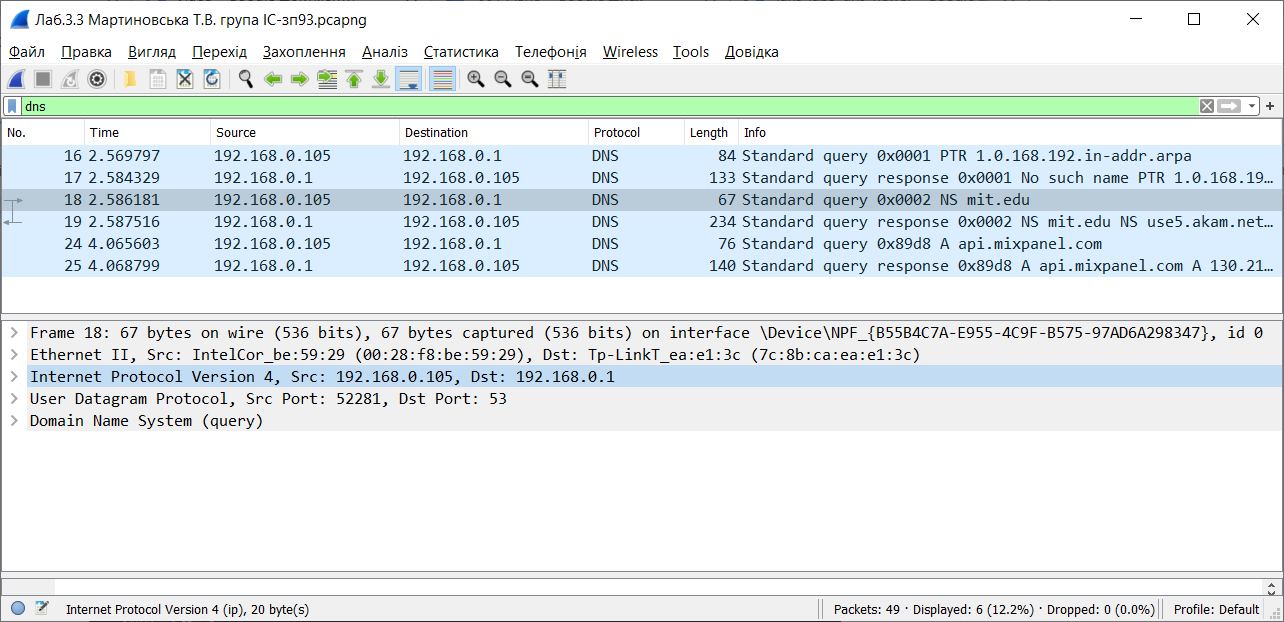
-CNAME: www.mit.edu.edgekey.net



Мал.14

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

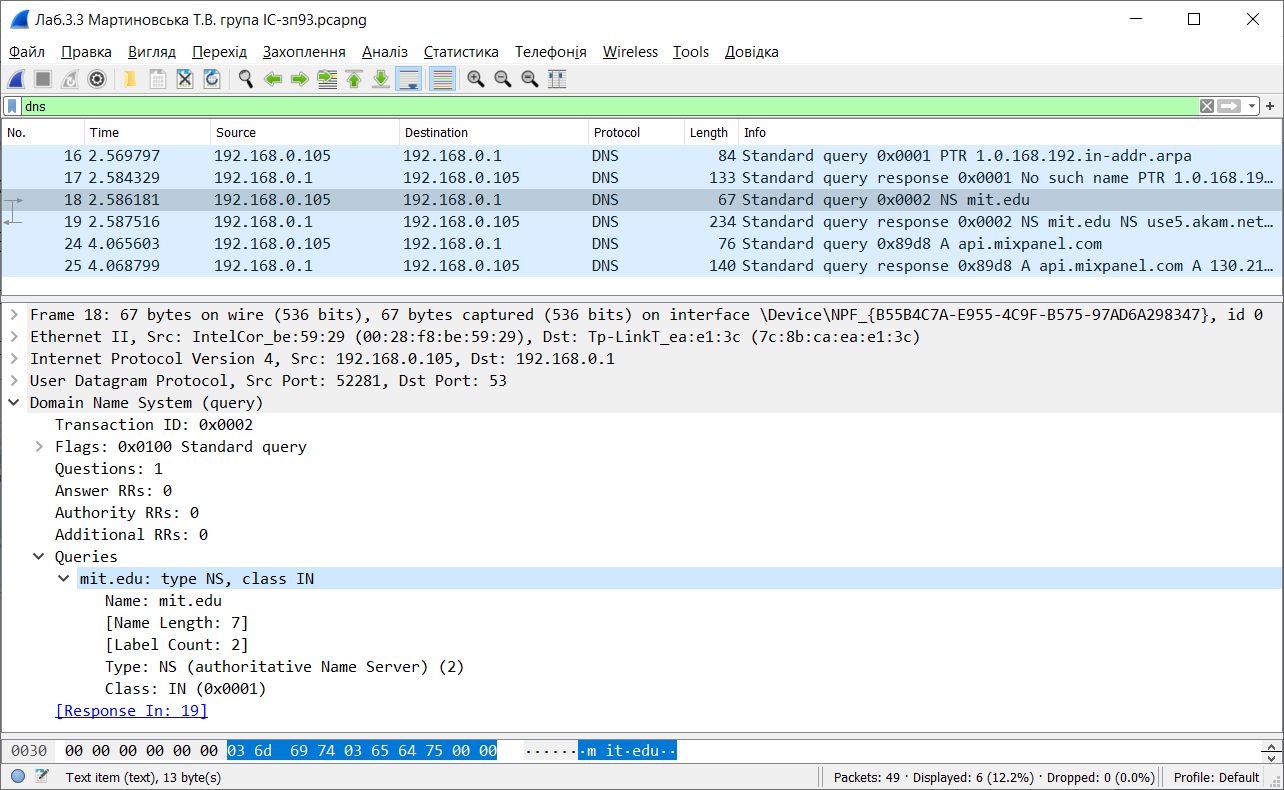
Відповідь: Destination: 192.168.0.1 – це є адреса локального сервера DNS за замовчанням



Мал.15

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

Відповідь: Type A (Адреса вузла, що відповідає за доменну зону), вміщує посилання на рядок з відповіддю [Response In: 19]. Це був запит по UDP протоколу.



Мал.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 запропоновано 8 записів:

- mit.edu: type NS, class IN, ns use5.akam.net

- mit.edu: type NS, class IN, ns asia2.akam.net

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

- mit.edu: type NS, class IN, ns use2.akam.net

- mit.edu: type NS, class IN, ns eur5.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 ns1-173.akam.net

Кожна з відповідей складаєеться з :

- Name: mit.edu

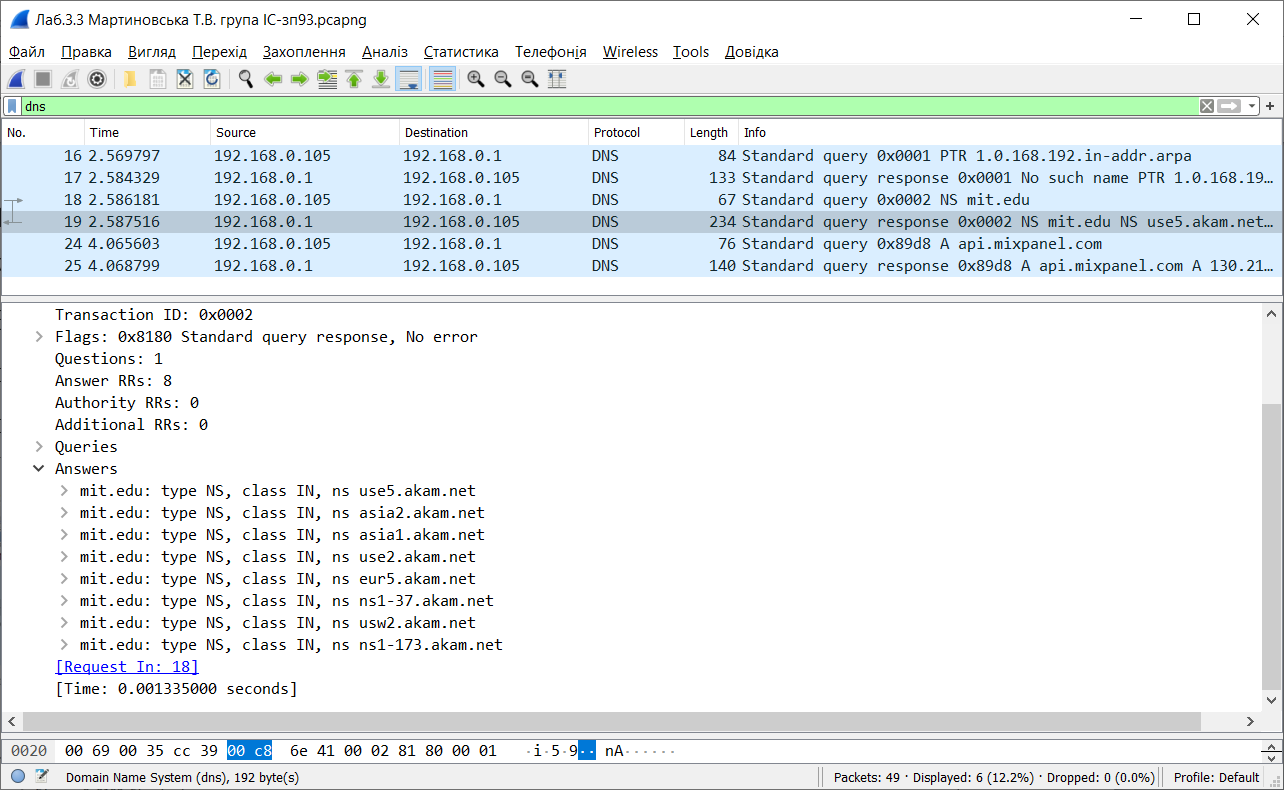
- Type: NS (authoritative Name Server) (2)

- Class: IN (0x0001)

- Time to live: 958 (15 minutes, 58 seconds)

- Data length: 15

- Name Server: use5.akam.net



Мал.17

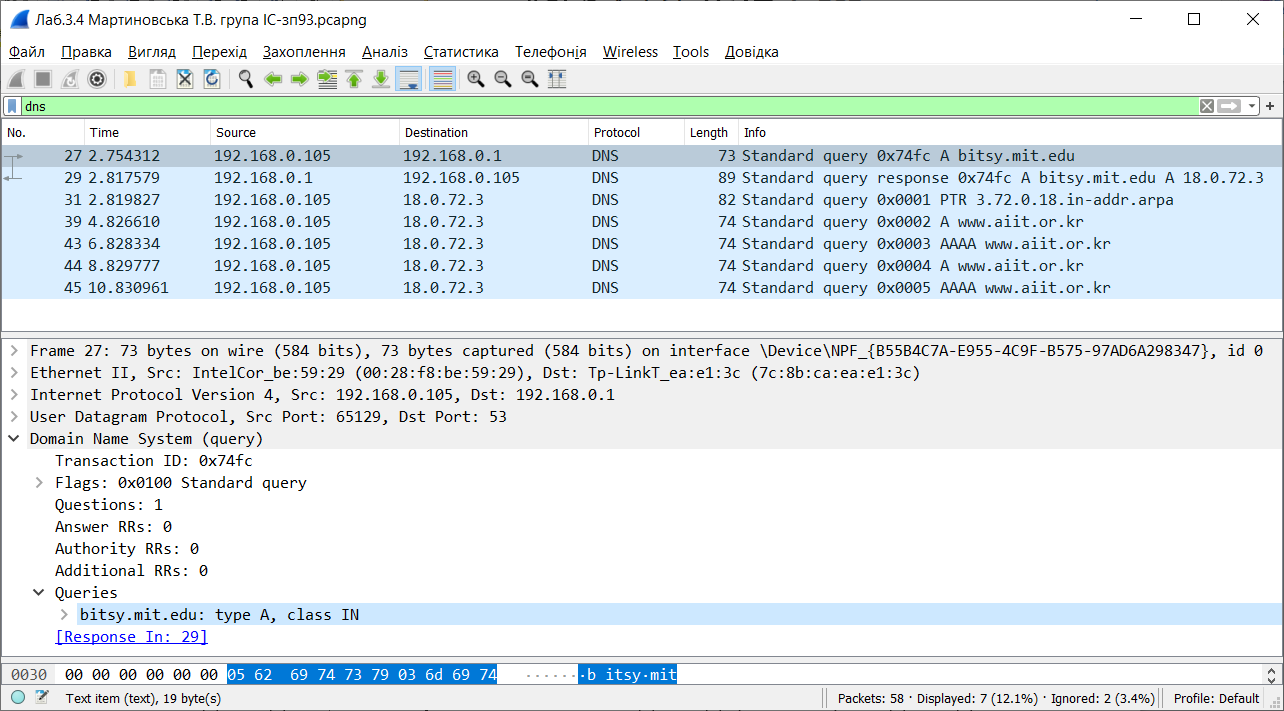
14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

Відповідь: Destination: 192.168.0.1 – це є адреса локального сервера DNS за замовчанням, також був запит на Destination: 18.0.72.3, що не є локальною адресою.

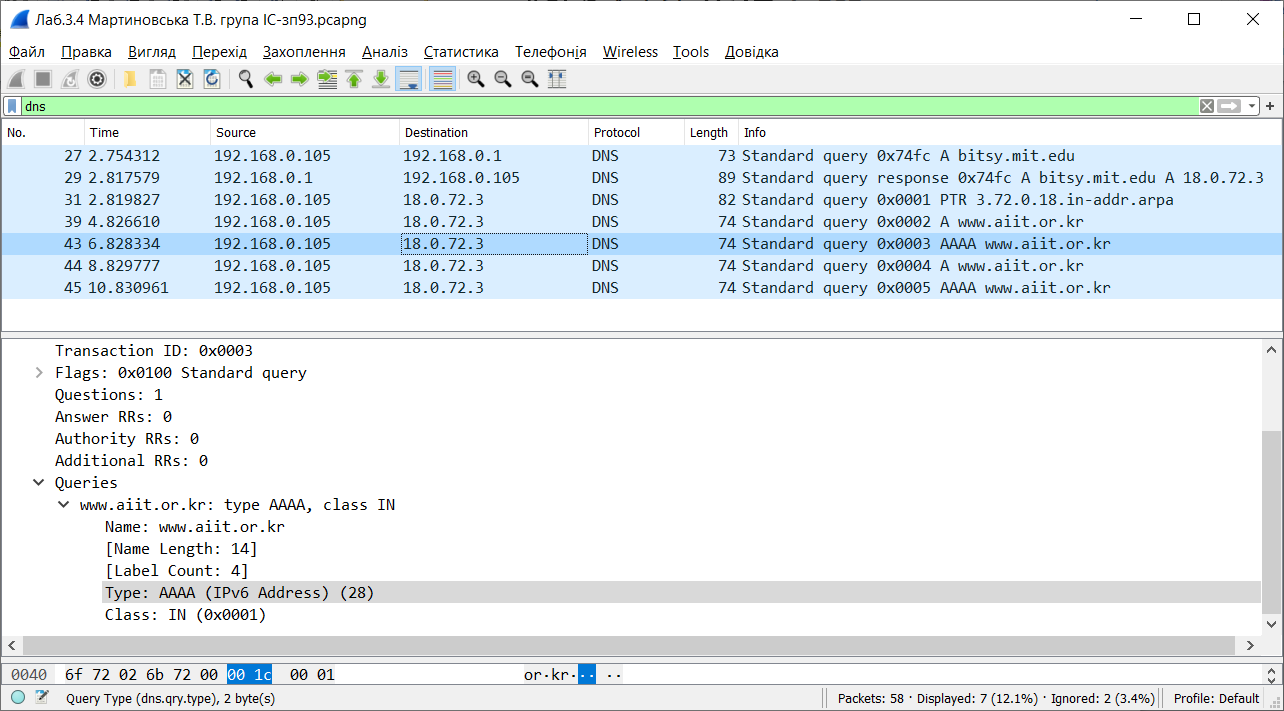
15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Це був запит по UDP протоколу. Так, цей запит вміщує відповідь:[Response In: 29]. Тип запиту A, class IN для запиту bitsy.mit.edu.

Для запиту www.aiit.or.kr тип запиту був А, PTR,АААА. Запит не вміщує посилання на відповідь.(Мал.19)



Мал.18



Мал.19

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

Відповідь: запит містив 1 відповідь- bitsy.mit.edu: type A, class IN, addr 18.0.72.3

Її структура:

- Name: bitsy.mit.edu

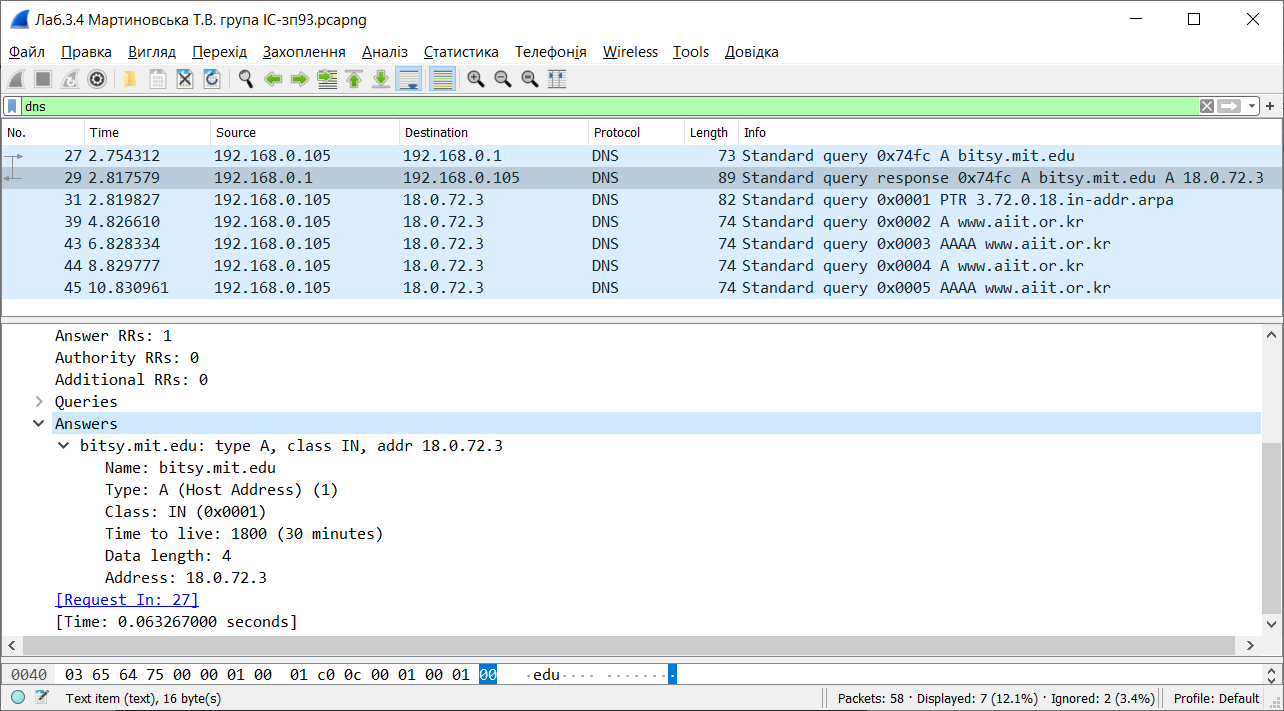
- Type: A (Host Address) (1)

- Class: IN (0x0001)

- Time to live: 1800 (30 minutes)

- Data length: 4

- Address: 18.0.72.3



Мал.20