Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут прикладного системного аналізу

Кафедра математичних методів системного аналізу

**ЗВІТ**

про виконання лабораторної роботи №2

з дисципліни: «Комп’ютерні мережі»

на тему: «Протокол DNS»

Виконала:

студент ІІI курсу, групи ІС-зп03

Єрмоленко В.О.

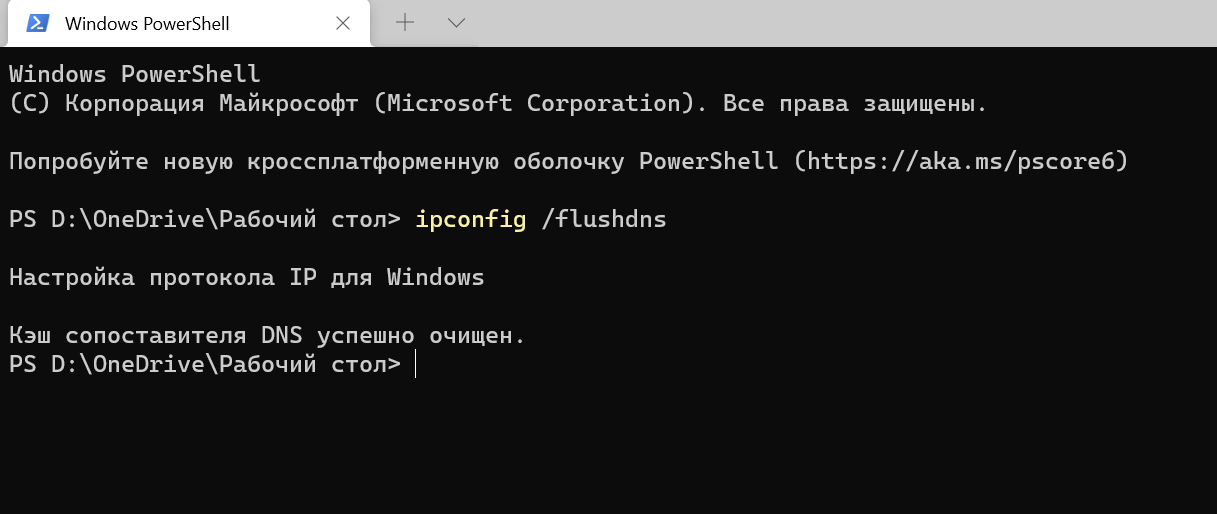
Прийняв:

Кухарєв С.О.

Київ 2021

***Хід роботи***

1. Очищуємо кеш DNS-записів

2. Запускаємо веб-браузер, очищуємо кеш браузера:

3. Запускаємо Wireshark, почнаємо захоплення пакетів.

4. Відкрийте за допомогою браузера одну із зазначених нижче адрес: http://www.ietf.org

5. Зупиняємо захоплення пакетів.

6. Переглядаємо деталі захоплених пакетів.

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

8. Почнаю захоплення пакетів.

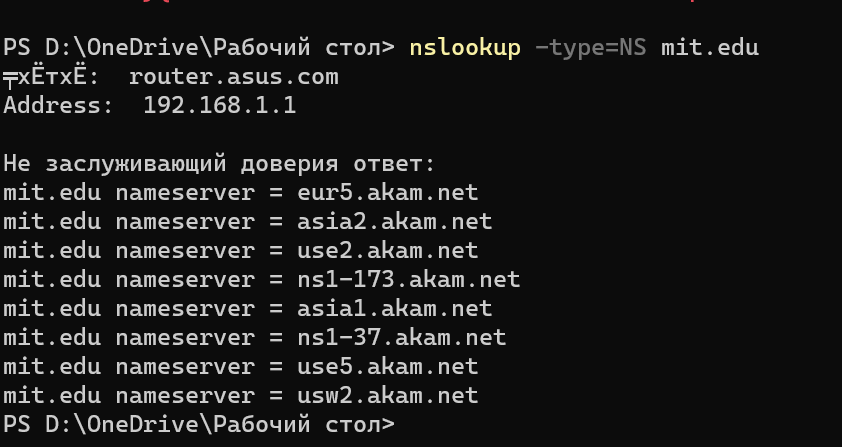
9. Виконайте nslookup для домену www.mit.edu за допомогою команди a. nslookup www.mit.edu

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. Почнаємо захоплення пакетів.

13. Виконуємо nslookup для домену www.mit.edu за допомогою команди a. nslookup –type=NS mit.edu

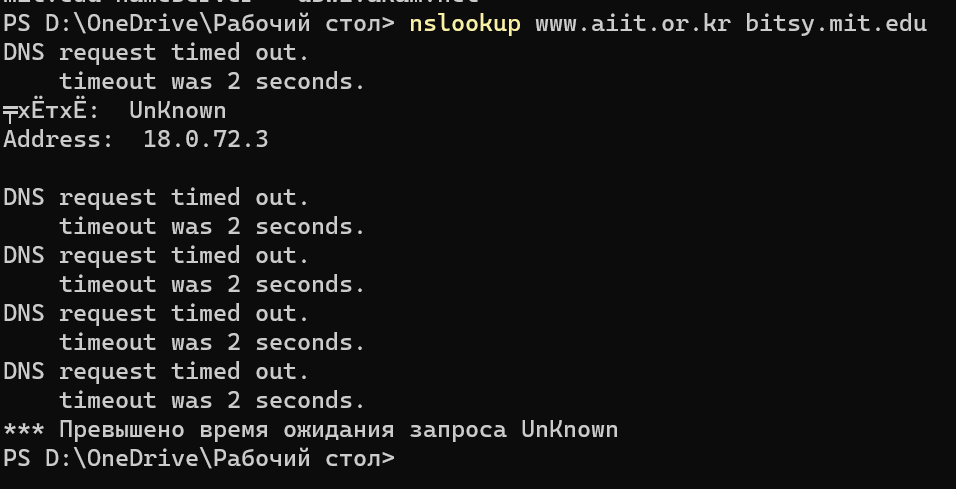


14. Зупиняємо захоплення пакетів.

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

16. Почнаємо захоплення пакетів.

17. Виконауємо 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. При необхідності роздрукуйте деякі захоплені пакети.

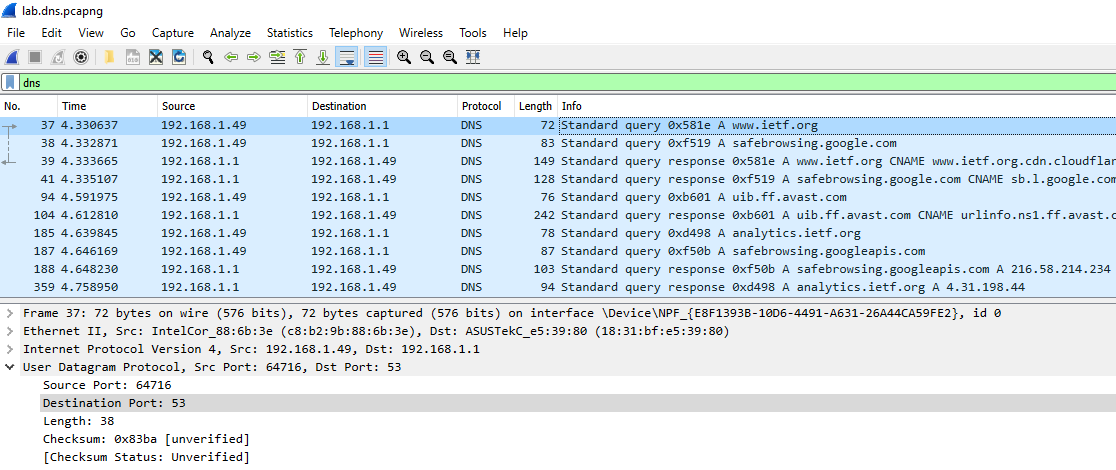
20. Закриваємо Wireshark.

***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?

**Sourse Port: 64716**

**Destination Port: 53**

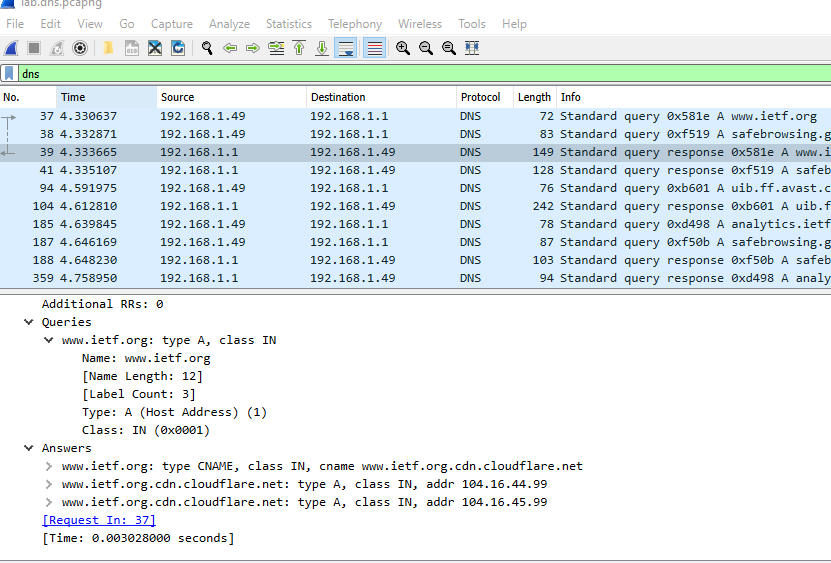
****

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

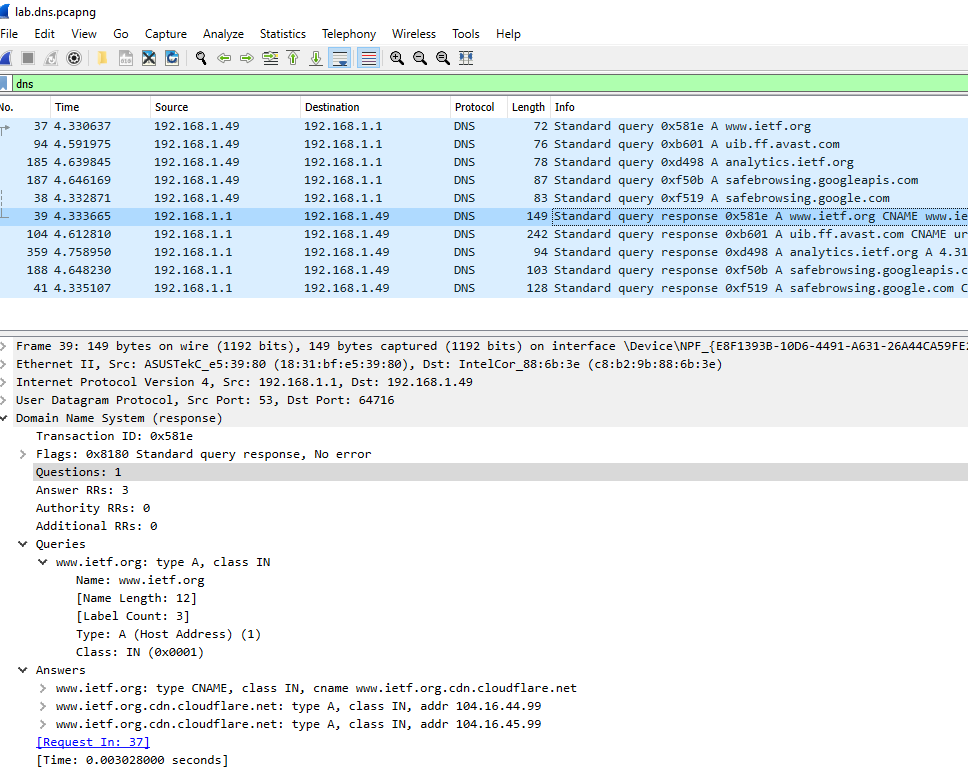
**Destination: 192.168.1.1**

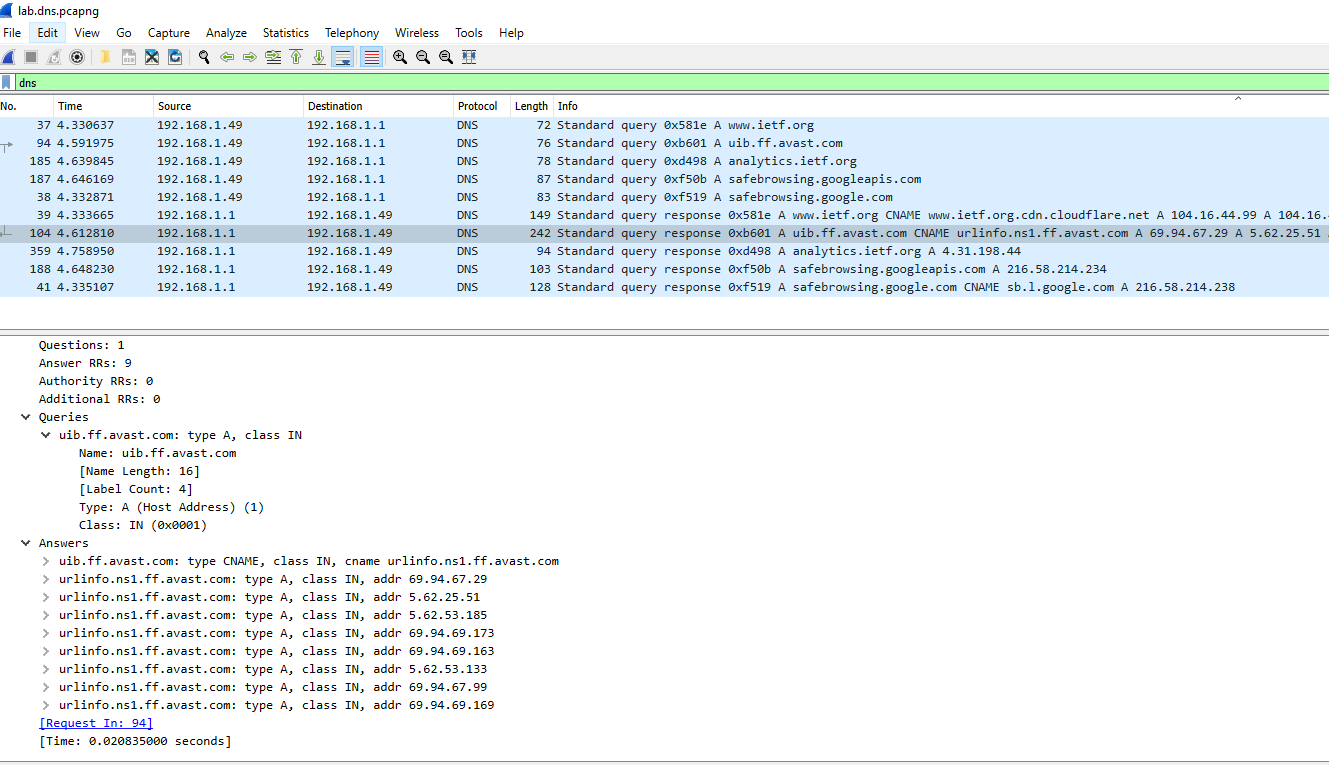
**Цей адрес є адресом локального сервера DNS?**

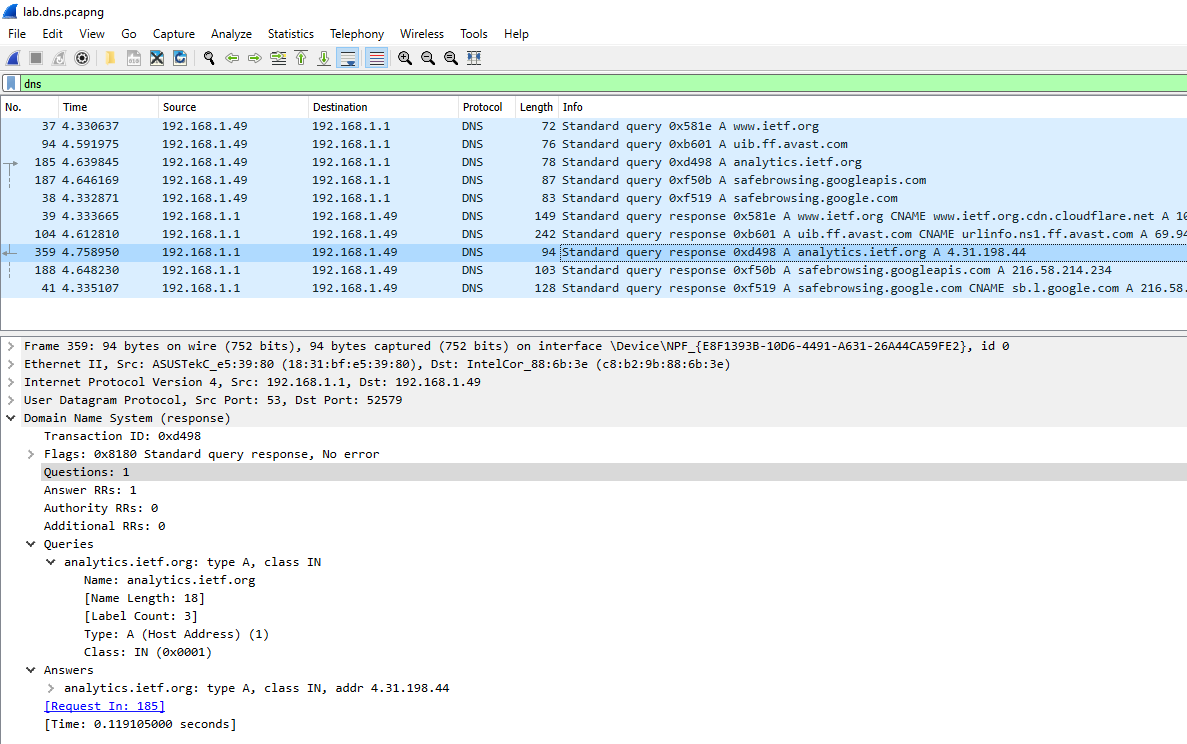
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

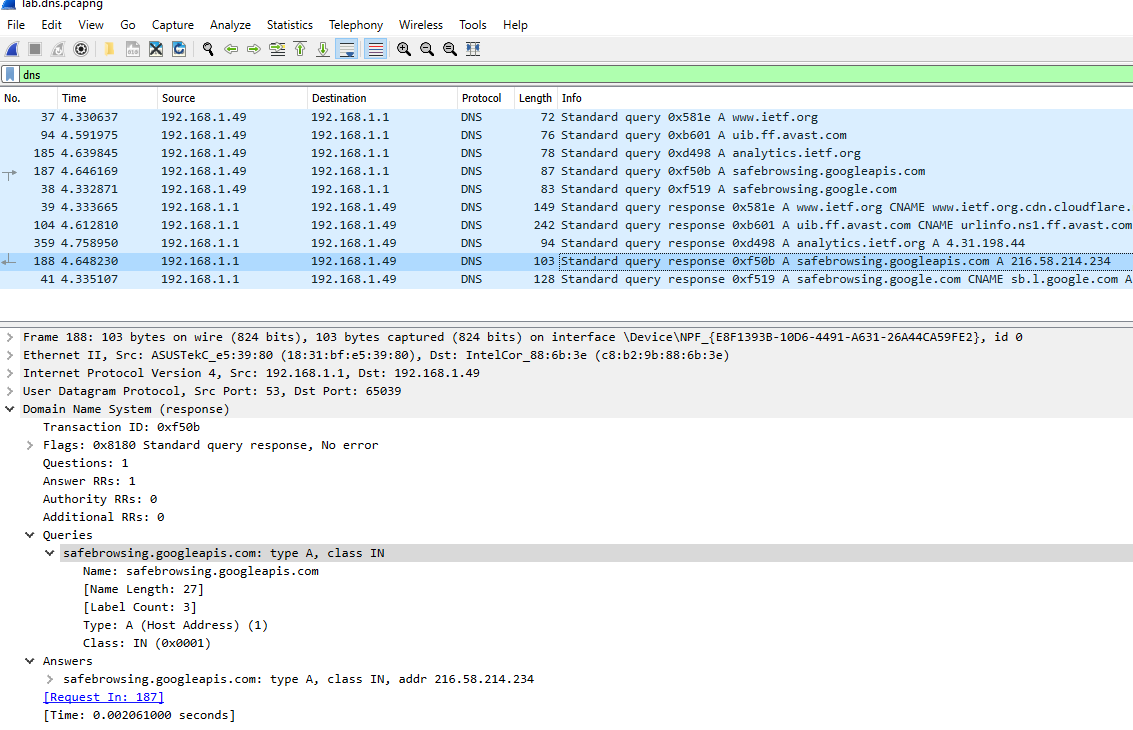


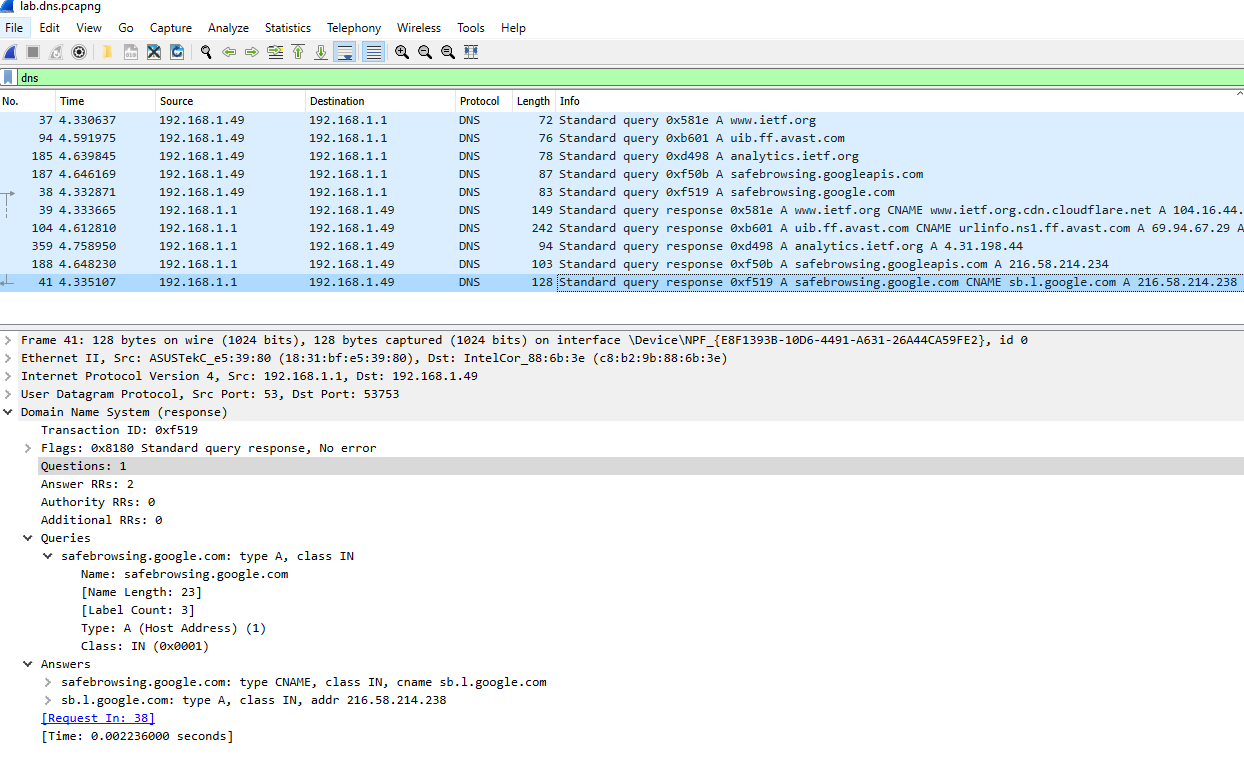
4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?



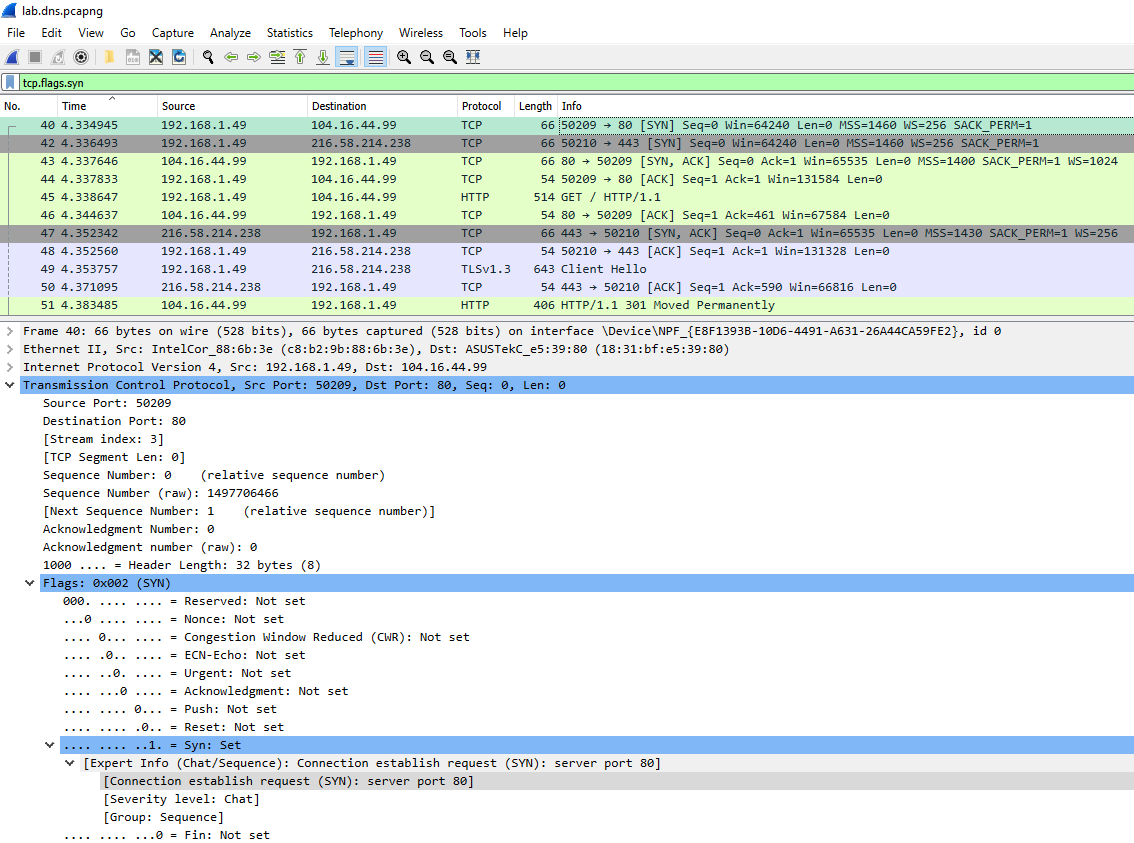




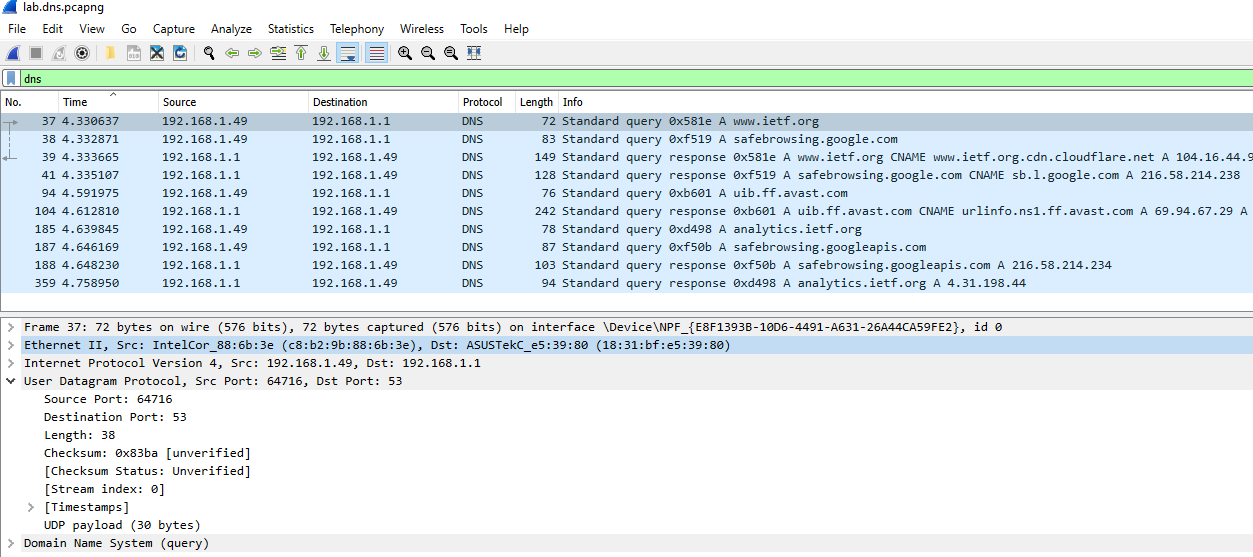




5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?



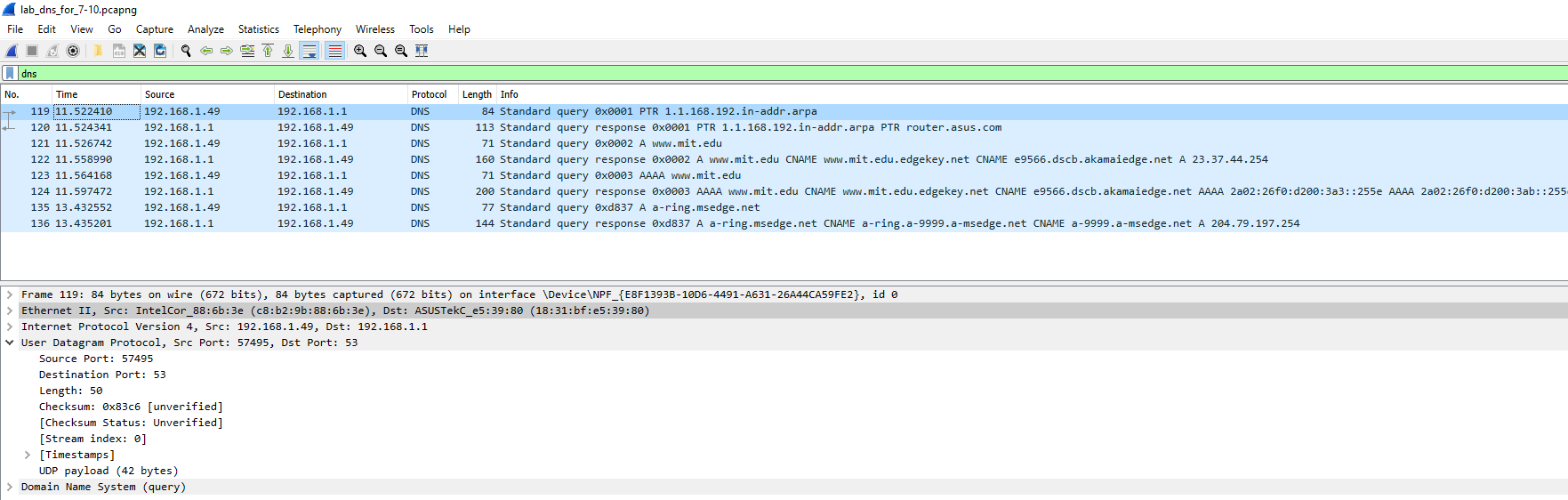
6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?



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

**Sourse Port: 57495**

**Destination Port: 53**

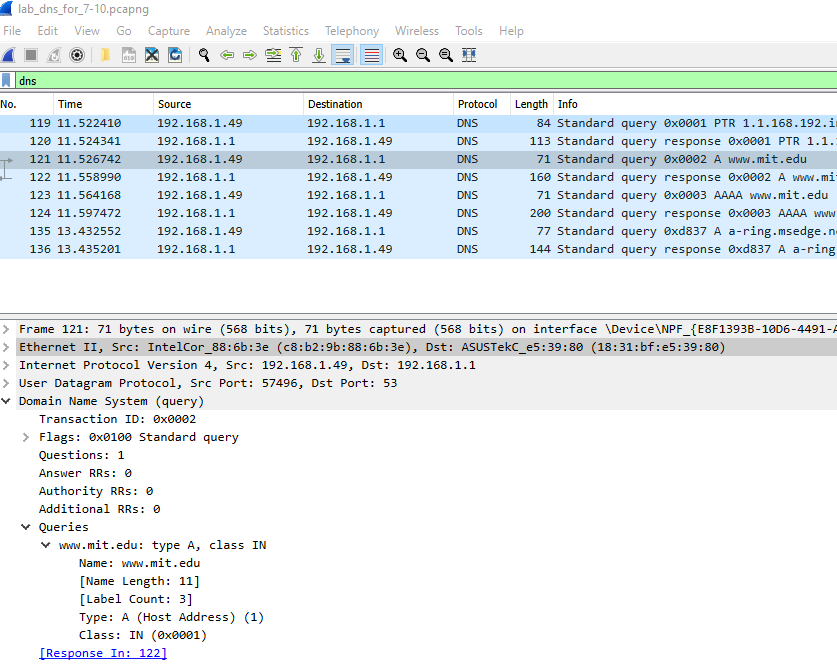
****

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

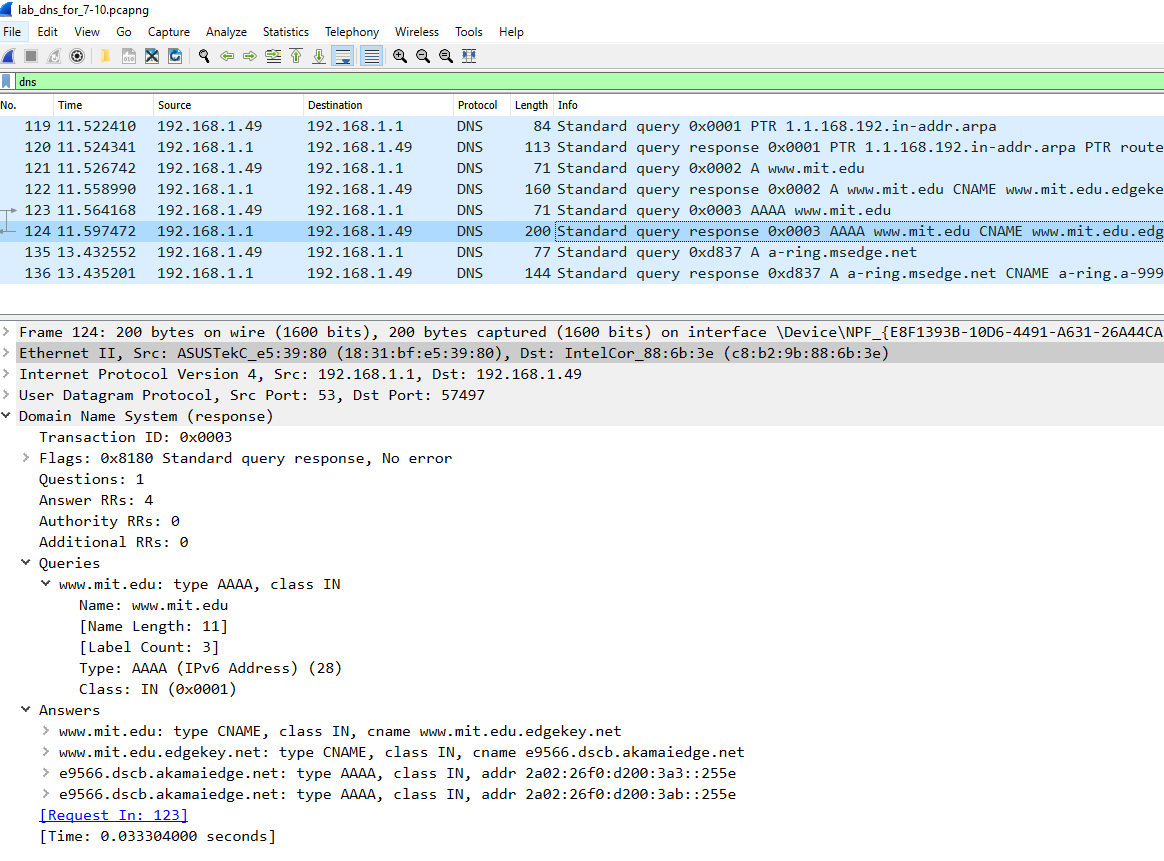
**Sourse: 192.168.1.49**

**Destination 192.168.1.1**

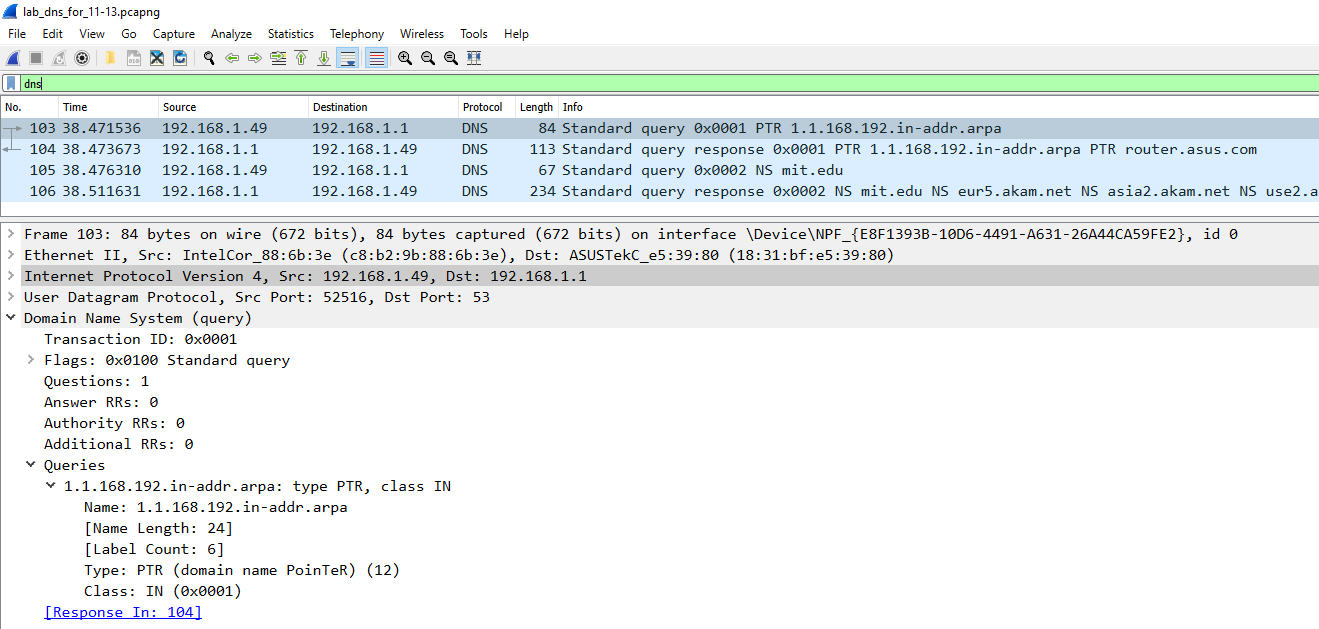
9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?



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

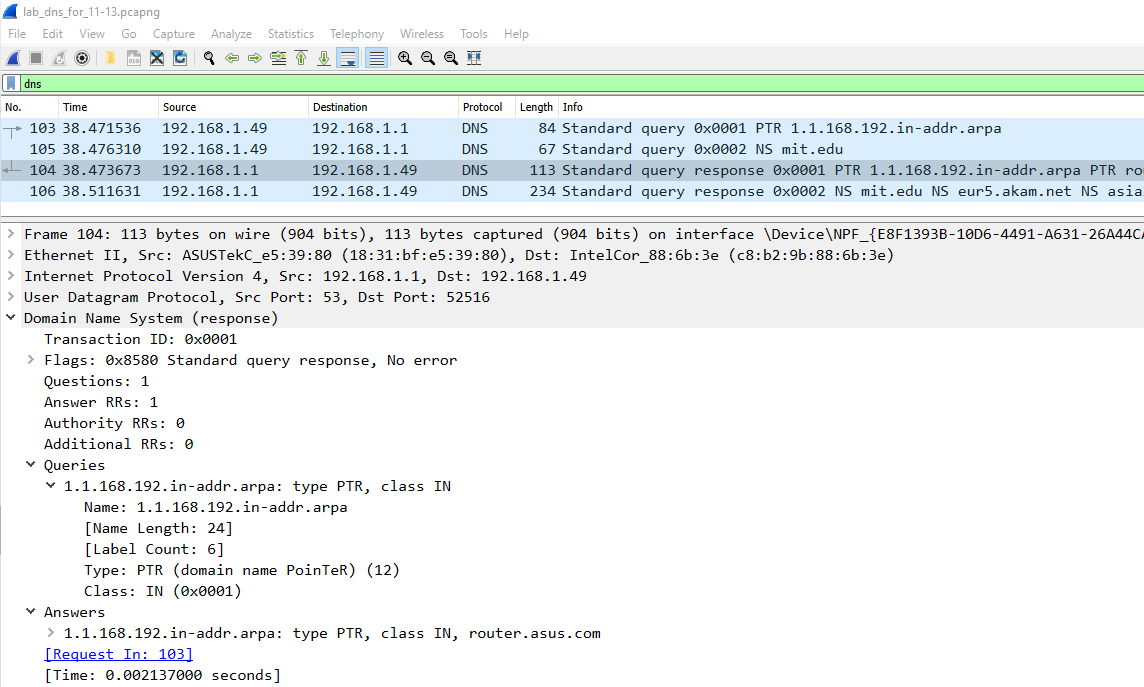


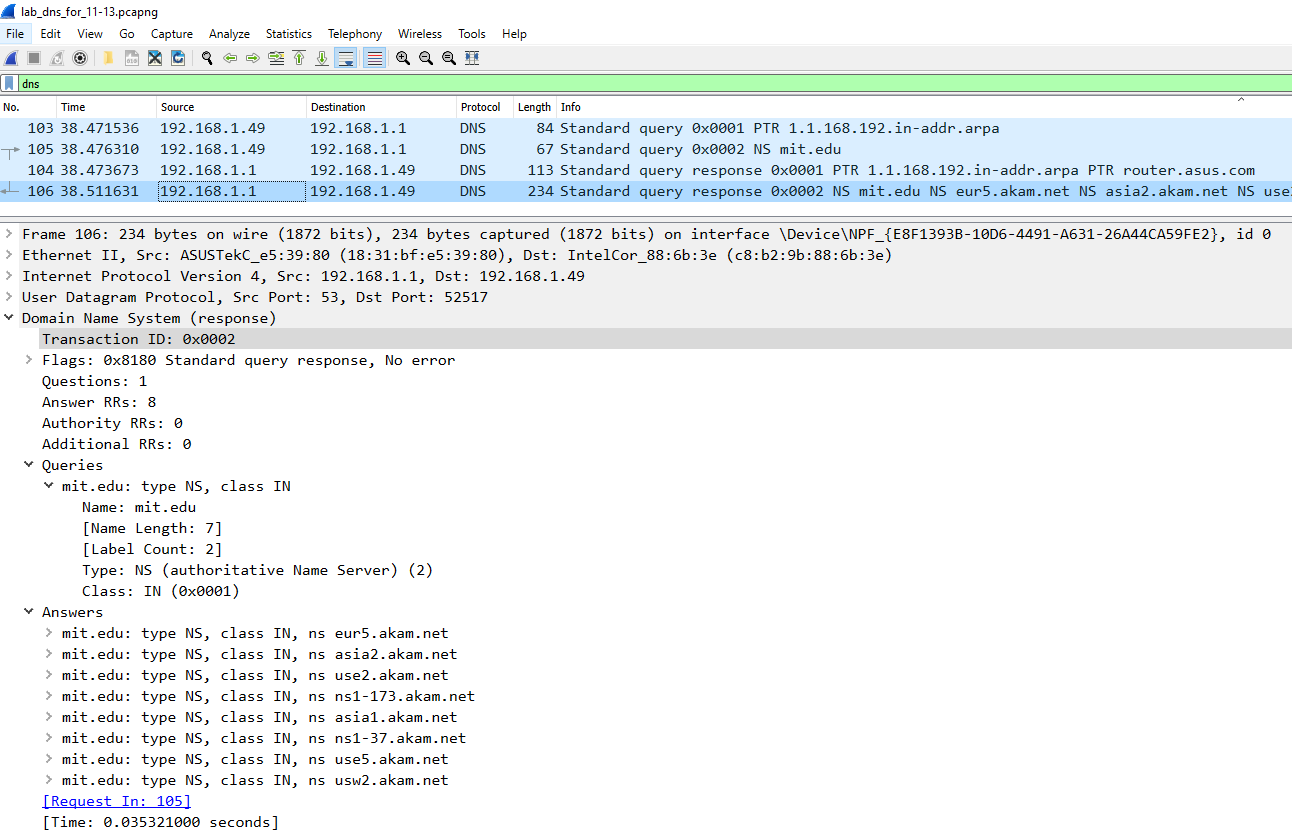
11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?



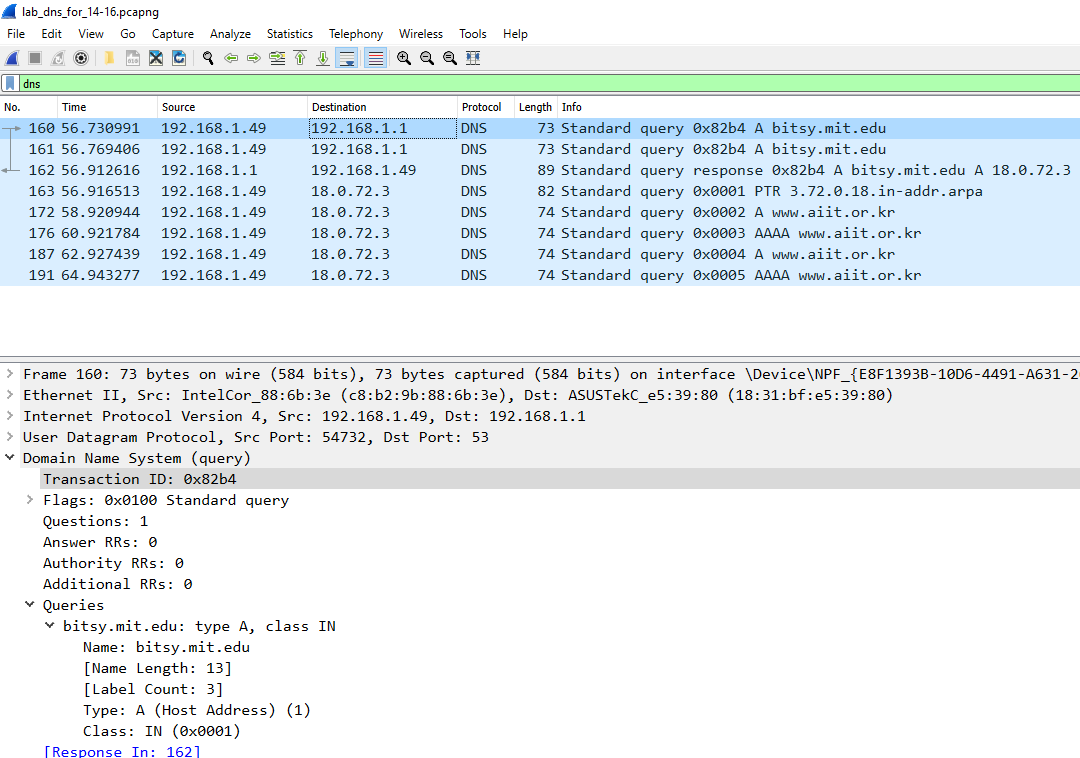
12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

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?

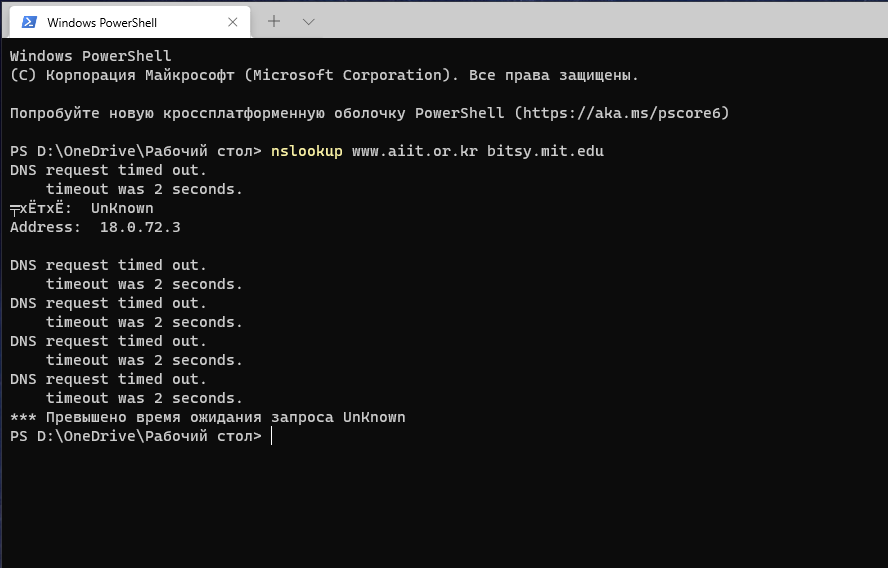




14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

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

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



**Висновок: у ході виконання лаборатоної роботи був проведений аналіз деталей роботи протоколу DNS.**