

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»**

**КАФЕДРА ММСА**

**Лабораторна робота № 3**

**З дисципліни: Комп’ютерні мережі**

***Основи захоплення та аналізу пакетів***

**Виконав:**

**Студентка ІII курсу**

**Групи КА-71**

**Висоцька М. А.**

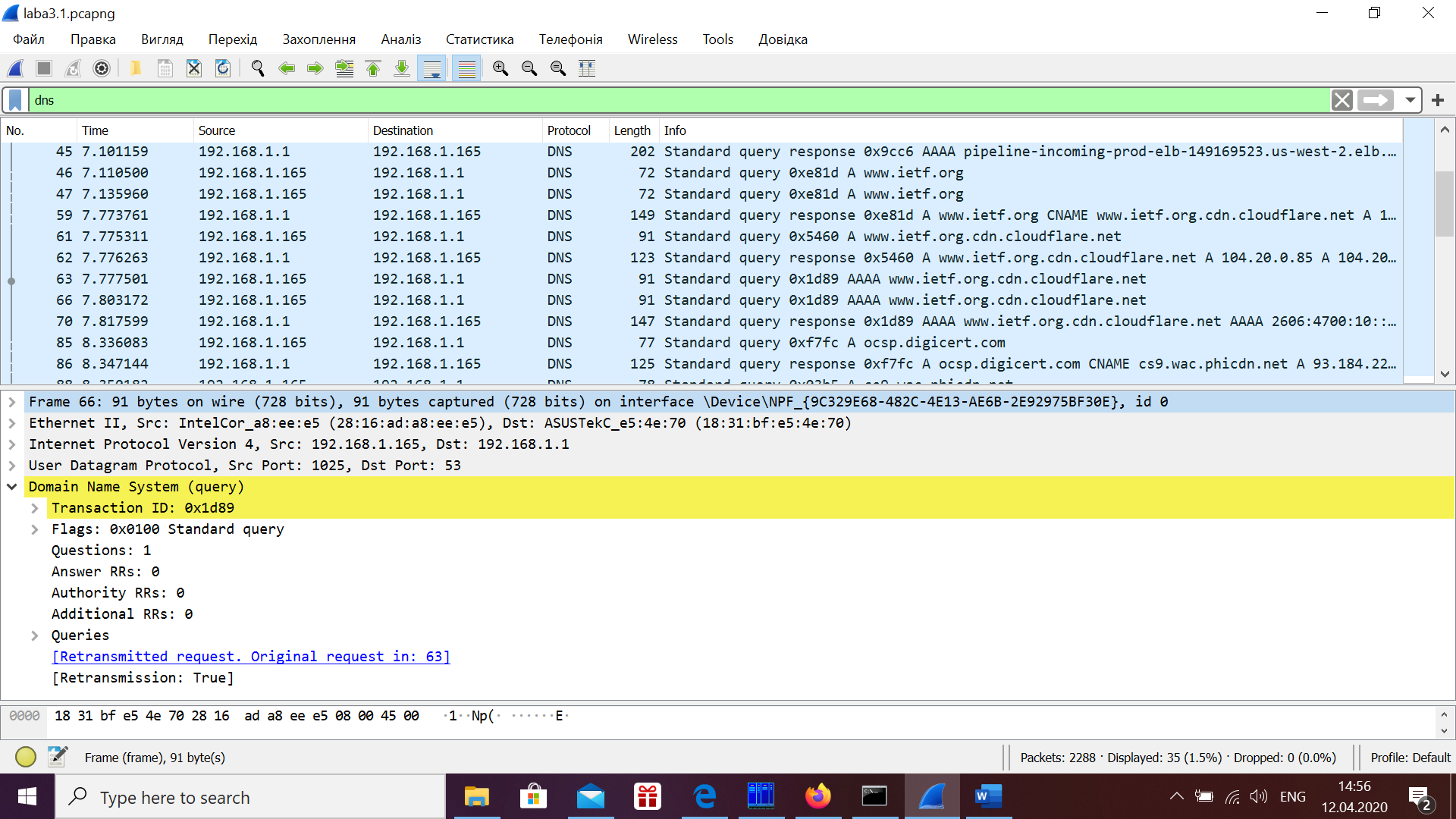
**Перевірив: Кухарєв С. О.**

**Київ 2020**

**Мета роботи:** оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

Wireshark, необхідними для дослідження мережевих протоколів.Начало формы

**Хід виконання роботи**



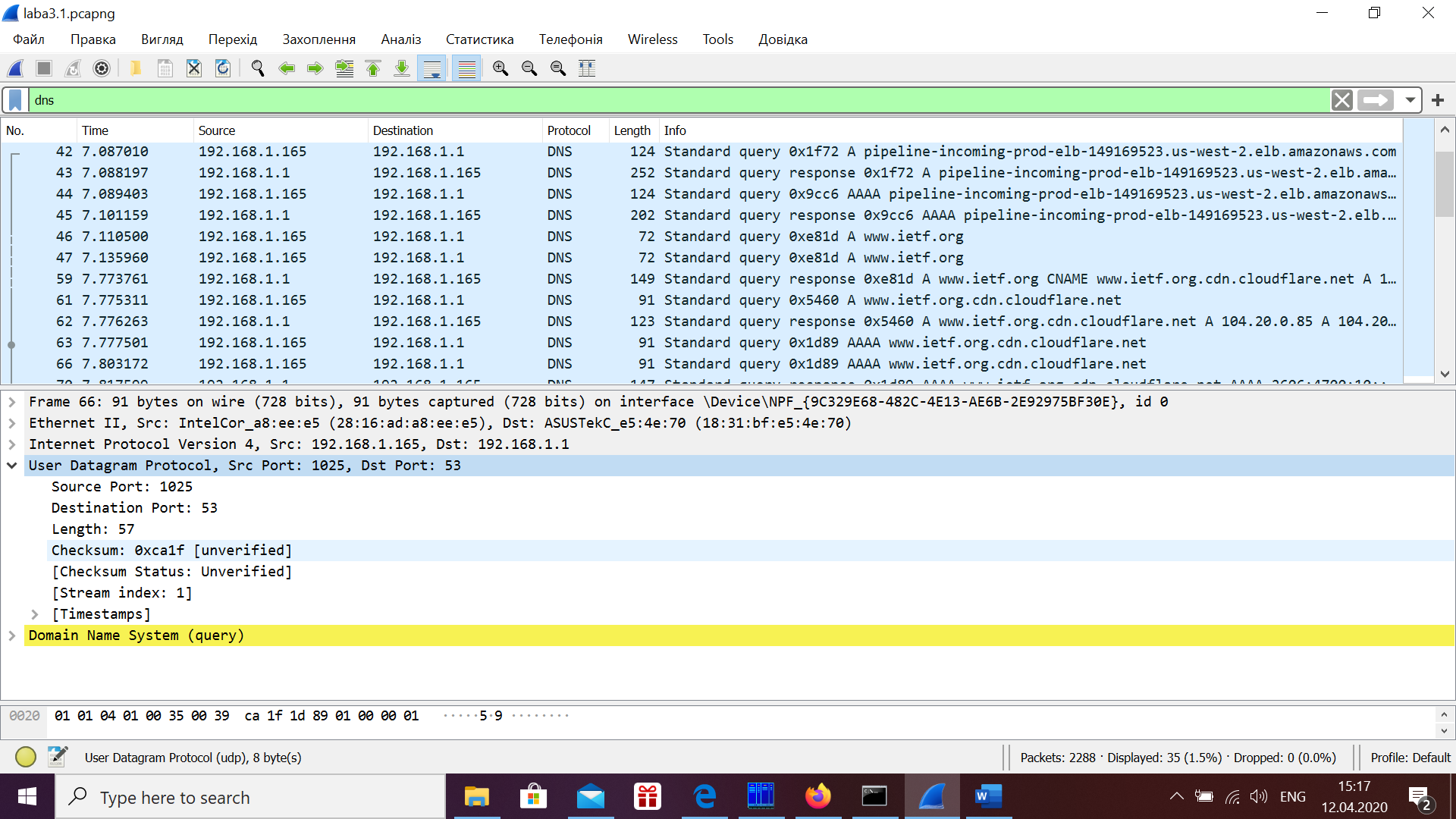
Контрольні запитання:

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?

UDP



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

сервера DNS?

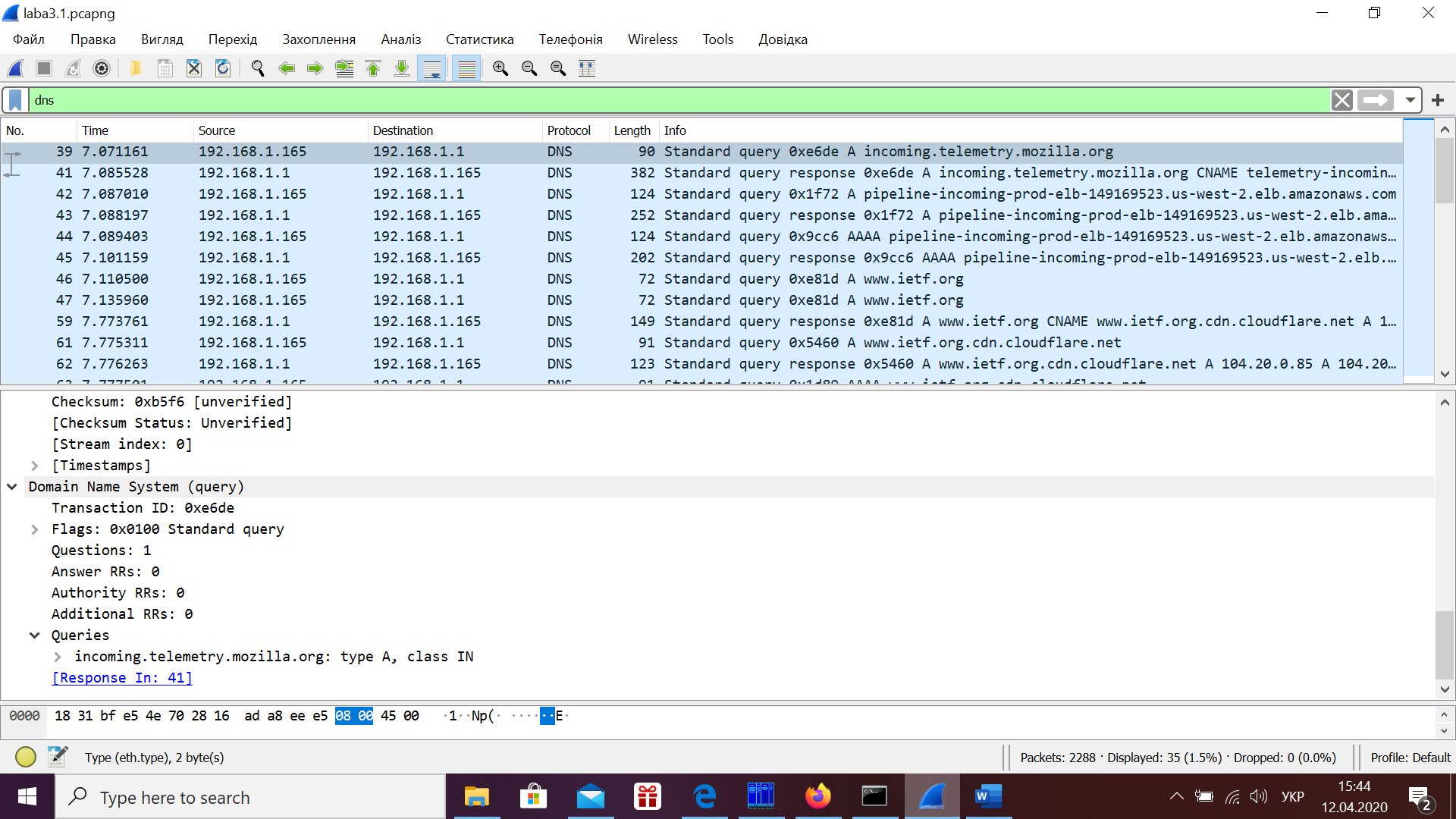
192.168.1.1

Так

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

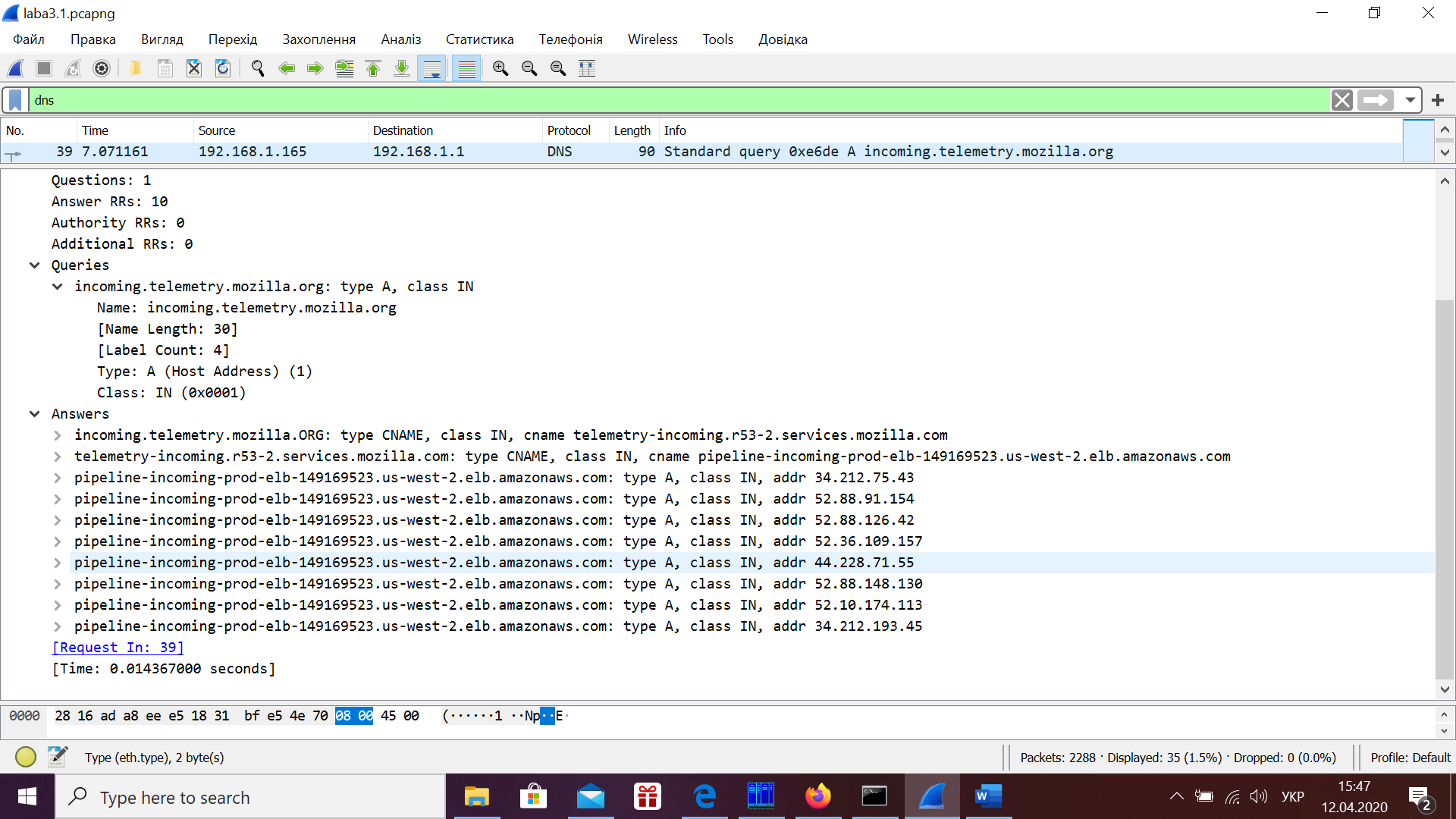
цей запит деякі можливі компоненти «відповіді»?

Тип Стандартний



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?

Так

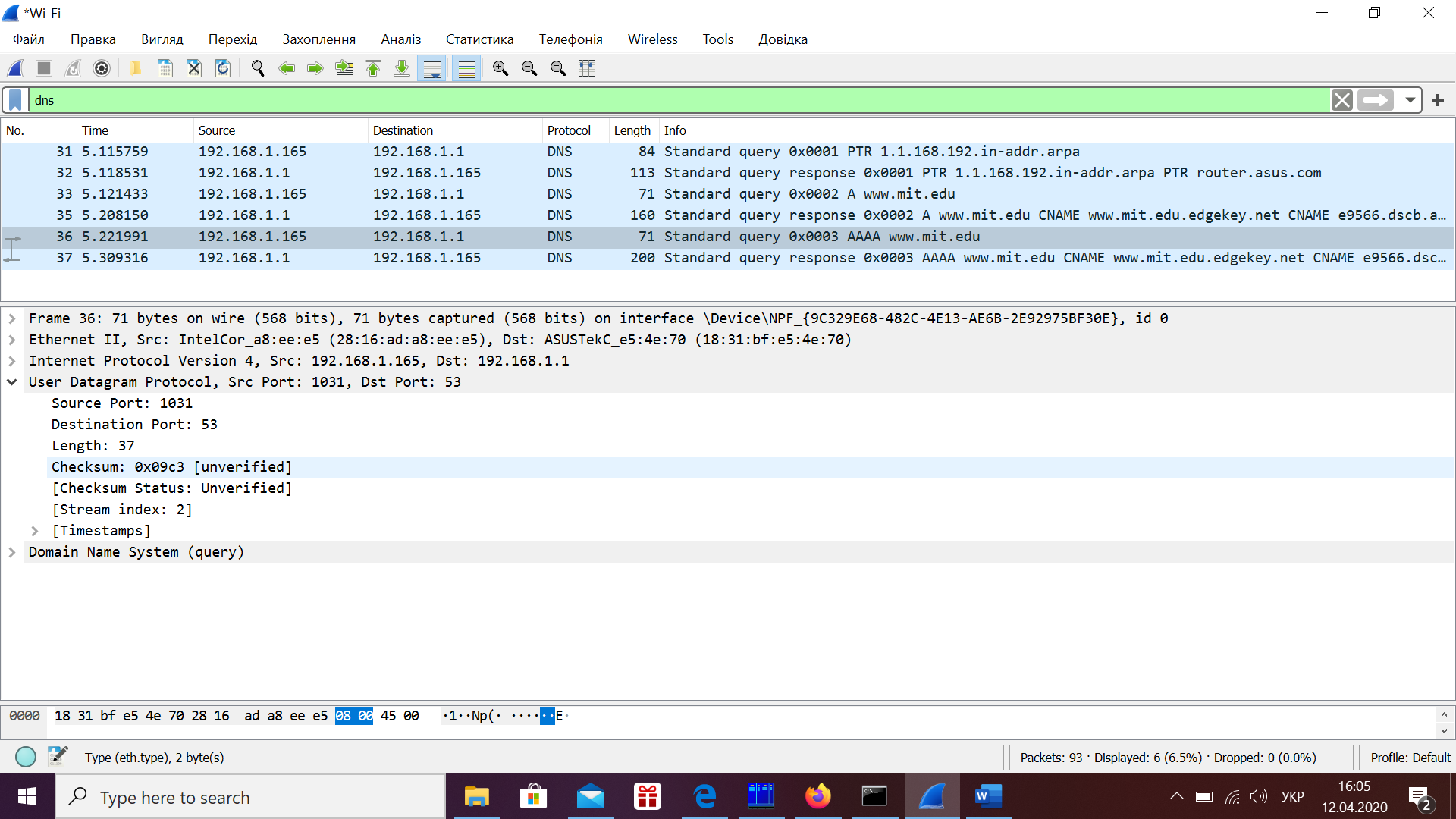
6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які

використовує документ, що отримав браузер?

Так

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

повідомлення із відповіддю DNS?



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

локального сервера DNS за замовчанням?

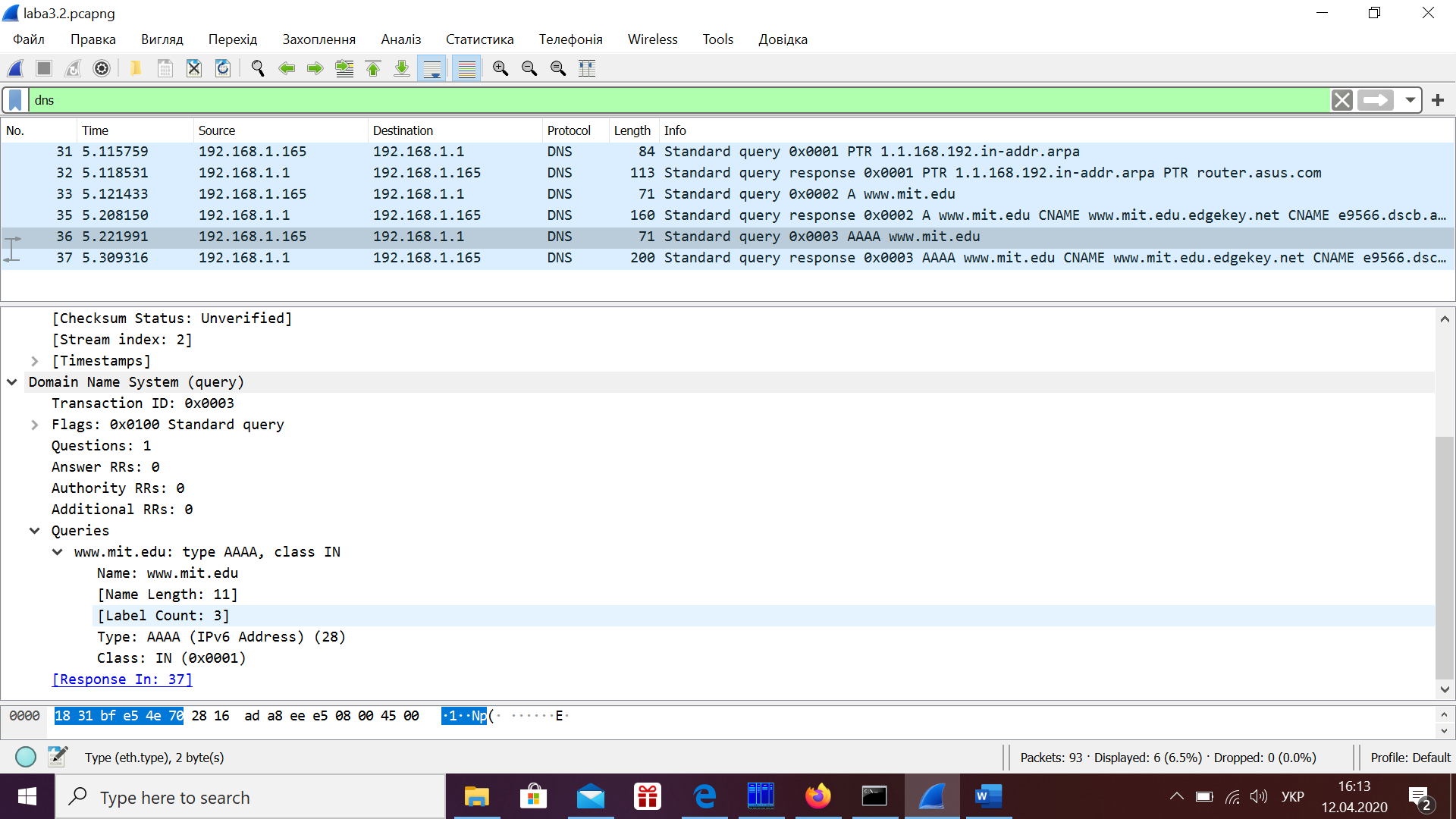
192.168.1.1

Так

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

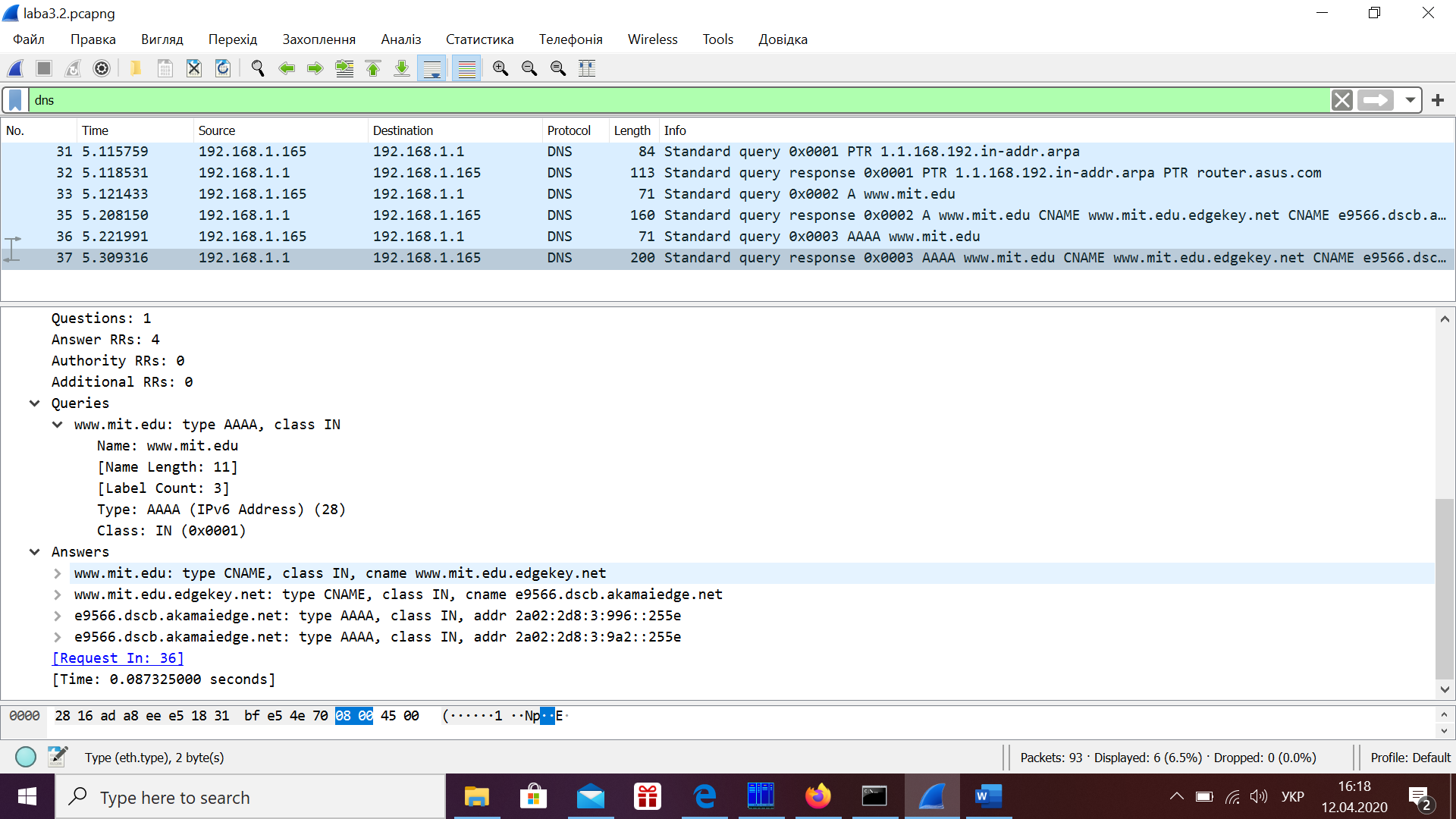
запит деякі можливі компоненти «відповіді»?

Тип Стандартний



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?

192.168.1.1

Так

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

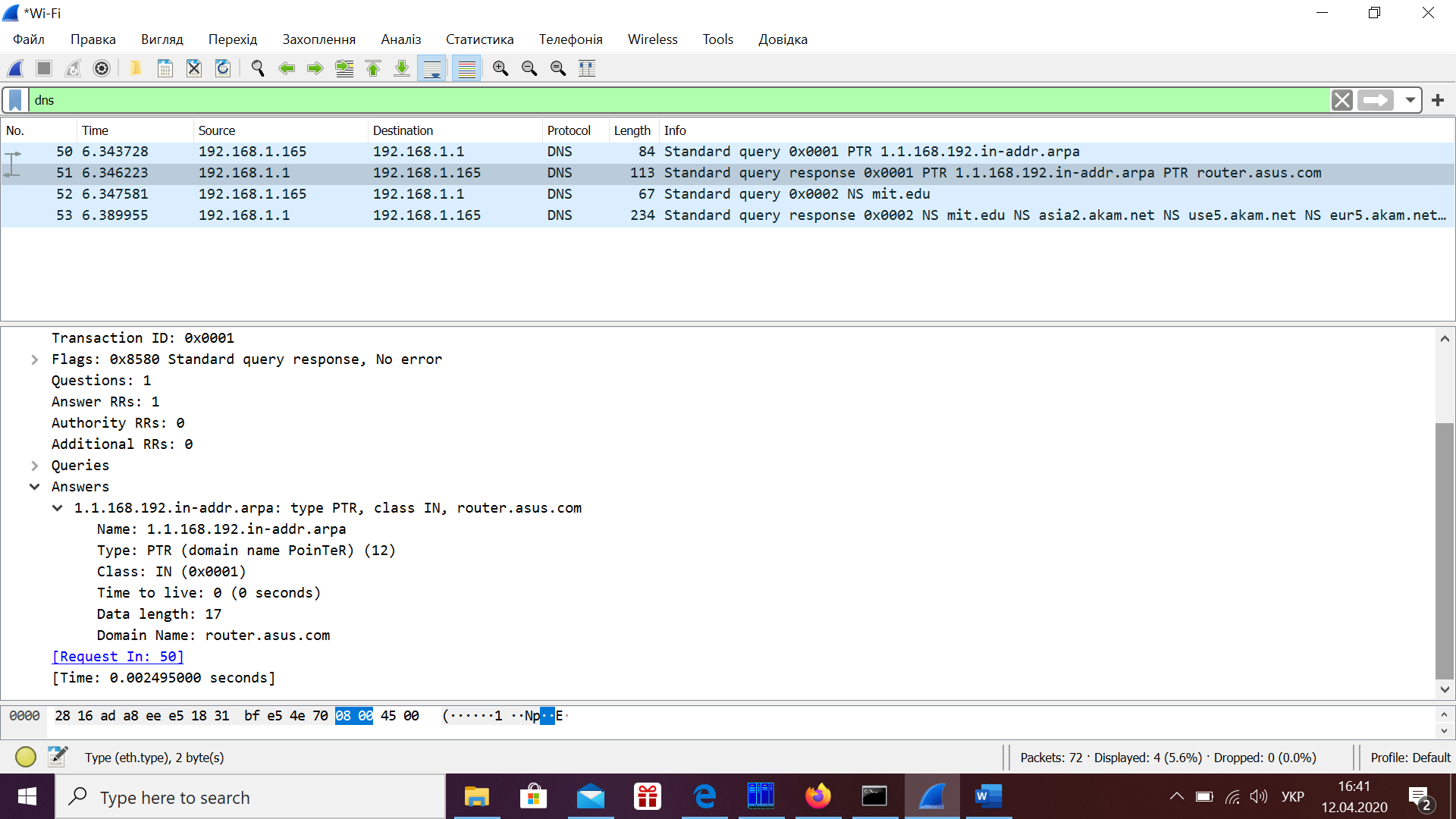
запит деякі можливі компоненти «відповіді»?

Стандартного типу. Так, вміщує

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

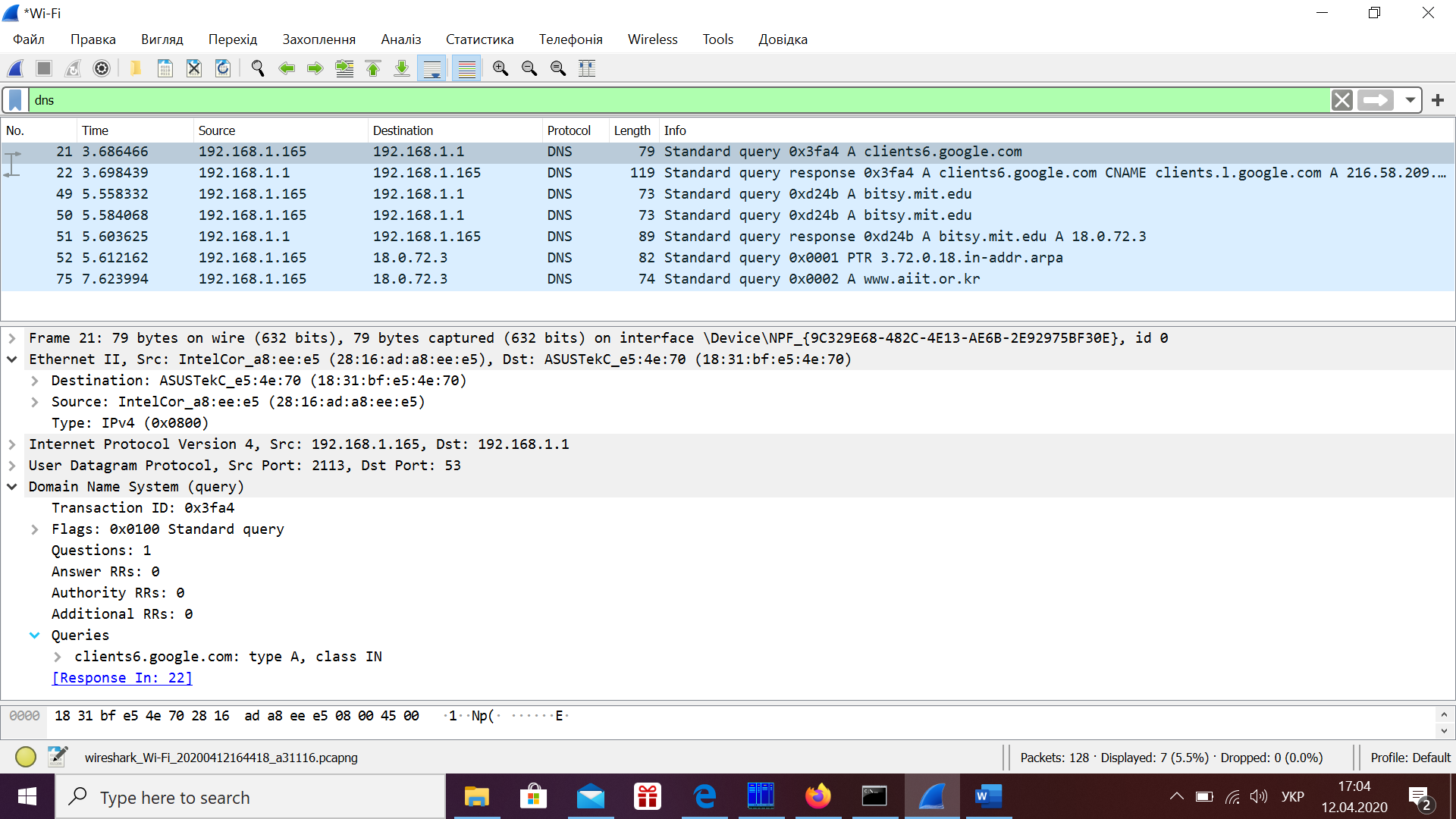
відповідає ця IP-адреса?

192.168.1.1

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

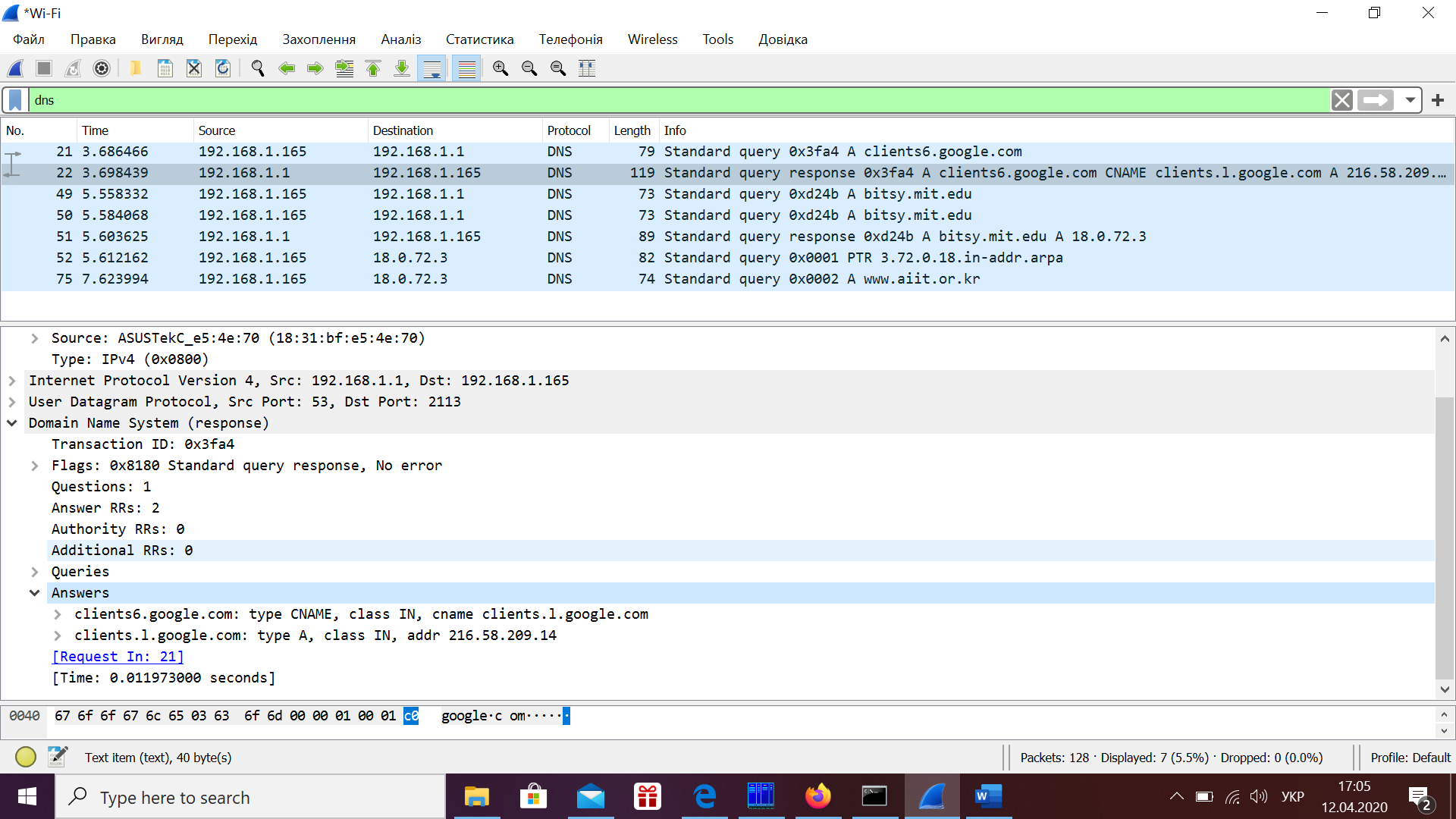
запит деякі можливі компоненти «відповіді»?

Стандартного типу



16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було

запропоновано сервером? З чого складається кожна з цих відповідей?



**Висновок**

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи DNS та було проведено аналіз роботи даних протоколів.