

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

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

**КАФЕДРА ММСА**

**Лабораторна робота № 3**

**З дисципліни: Комп’ютерні мережі**

***Протокол DNS***

**Виконала:**

**Студентка ІII курсу**

**Групи КА-74**

**Клименко І. О.**

**Перевірив: Кухарєв С. О.**

**Київ 2020**

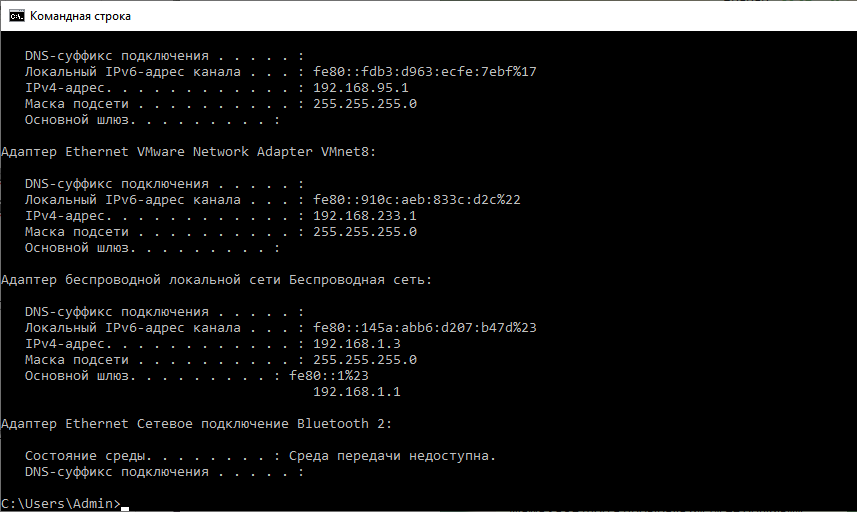
**Мета роботи:** аналіз деталей роботи протоколу DNS.

Wireshark, необхідними для дослідження мережевих протоколів.Начало формы

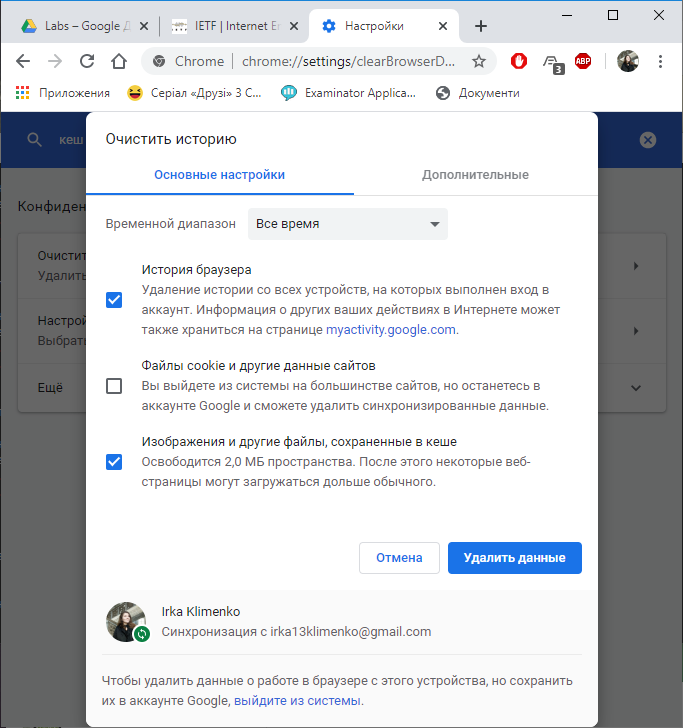
**Хід роботи**

Необхідно виконати наступні дії:

* Очистіть кеш DNS-записів
  + для windows-систем виконайте в терміналі ipconfig /flushdns
  + для linux-систем (можливо) спрацює перезапуск операційної системи;

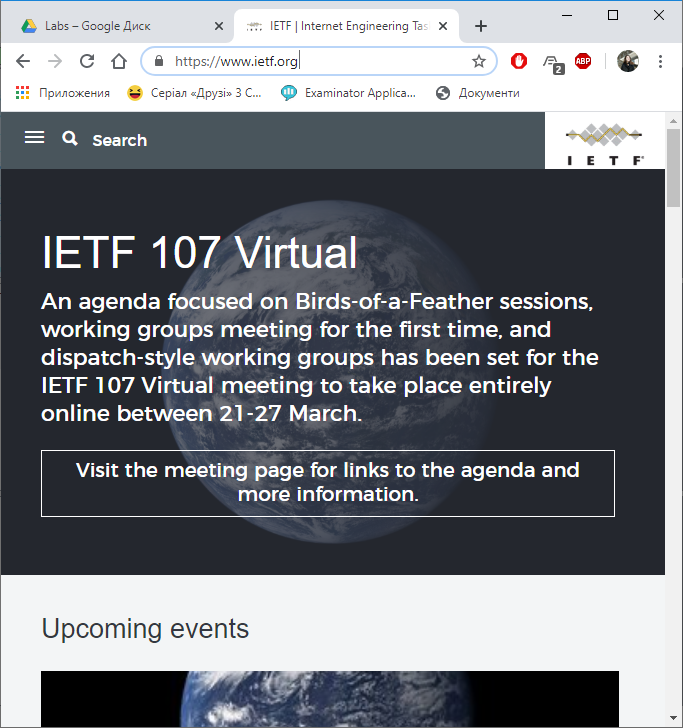


* Запустіть веб-браузер, очистіть кеш браузера:
  + для Firefox виконайте Tools >> Clear Private Data (або Ctrl + Shift + Del)
  + для MS IE виконайте Tools >> Internet Options >> Delete File
* Запустіть Wireshark, почніть захоплення пакетів.

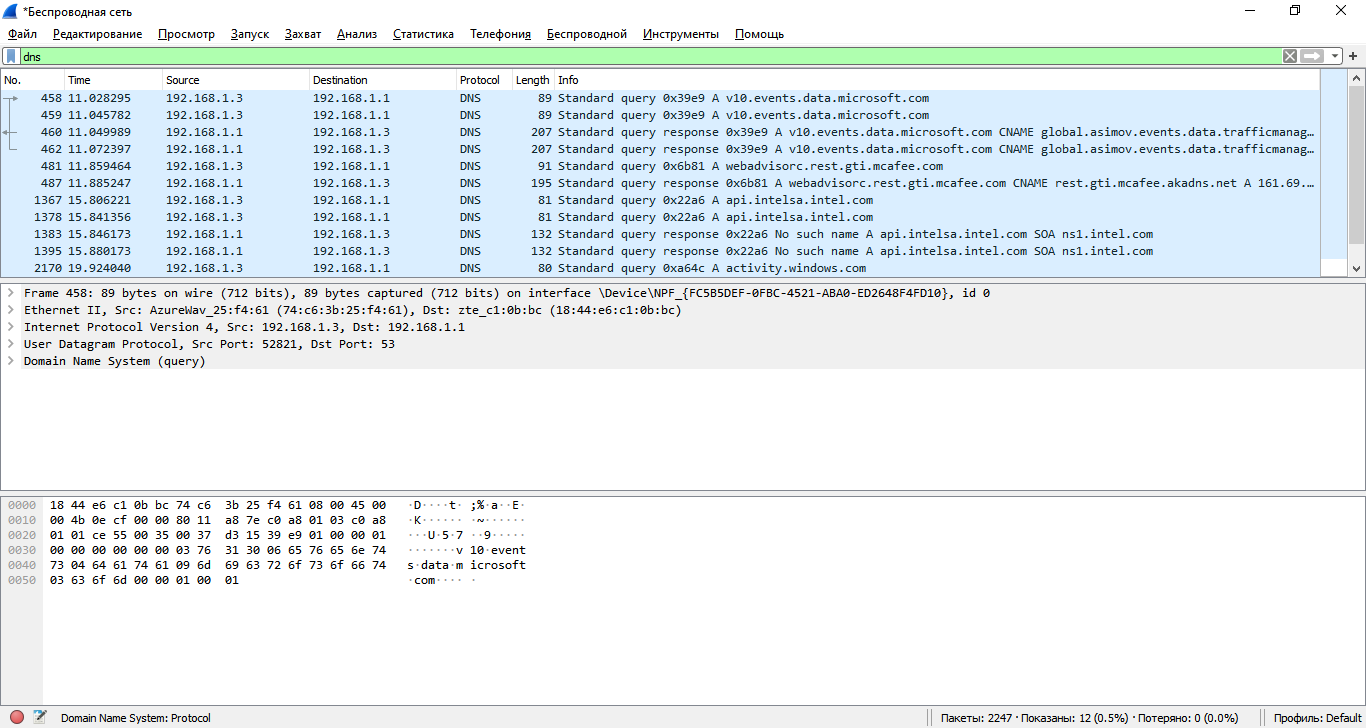


* Відкрийте за допомогою браузера одну із зазначених нижче адрес:

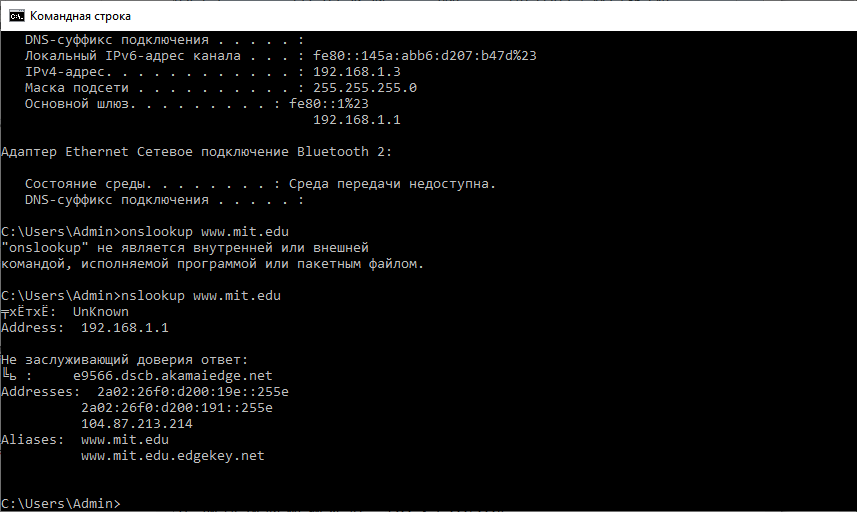
<http://www.ietf.org>



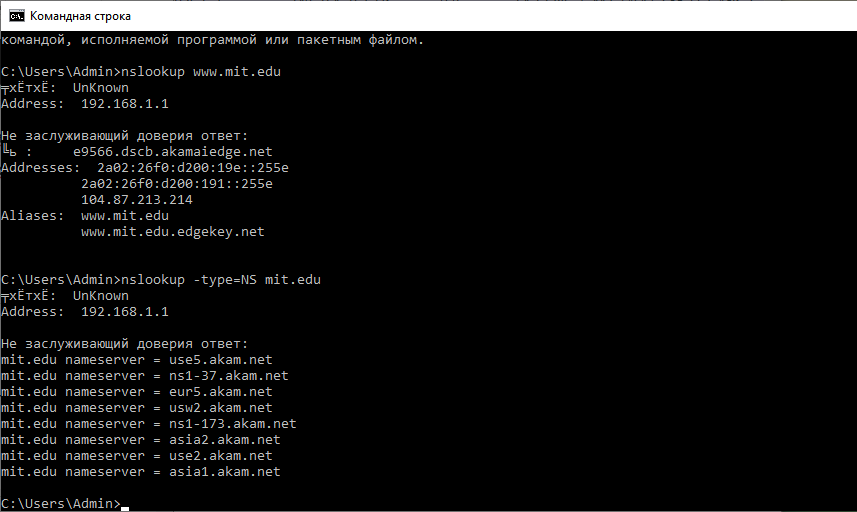
* Зупиніть захоплення пакетів.
* Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).



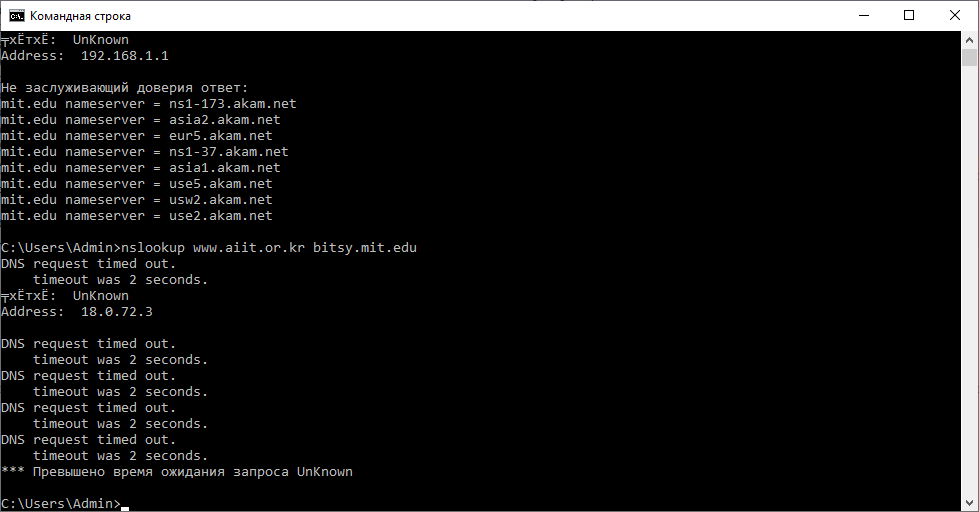
* Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.
* Почніть захоплення пакетів.
* Виконайте nslookup для домену www.mit.edu за допомогою команди
  + nslookup [www.mit.edu](http://www.mit.edu)



* Зупиніть захоплення пакетів.
* 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.
* Почніть захоплення пакетів.
* Виконайте nslookup для домену www.mit.edu за допомогою команди
  + nslookup –type=NS mit.edu



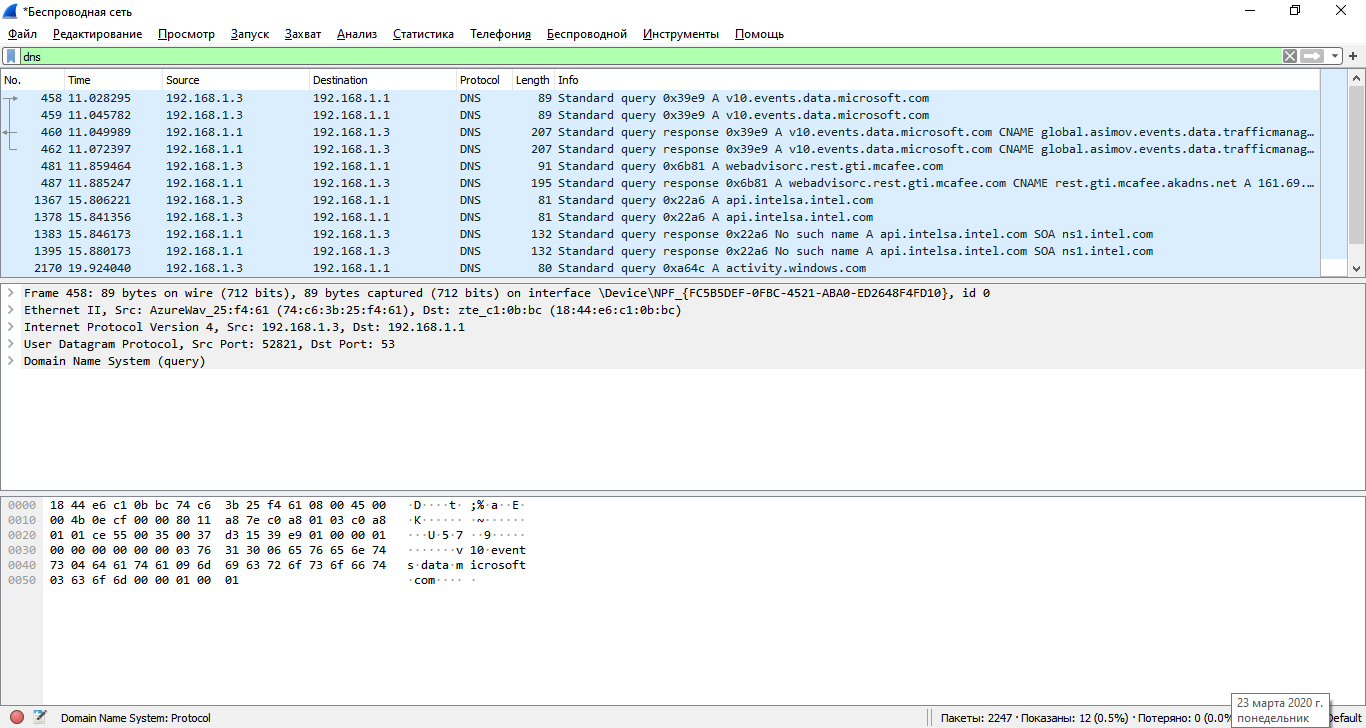
* Зупиніть захоплення пакетів.
* Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети.
* Почніть захоплення пакетів.
* Виконайте nslookup для домену www.mit.edu за допомогою команди
  + nslookup www.aiit.or.kr bitsy.mit.edu



* Зупиніть захоплення пакетів.
* Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.
* Закрийте Wireshark.

**Контрольні питання**

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?



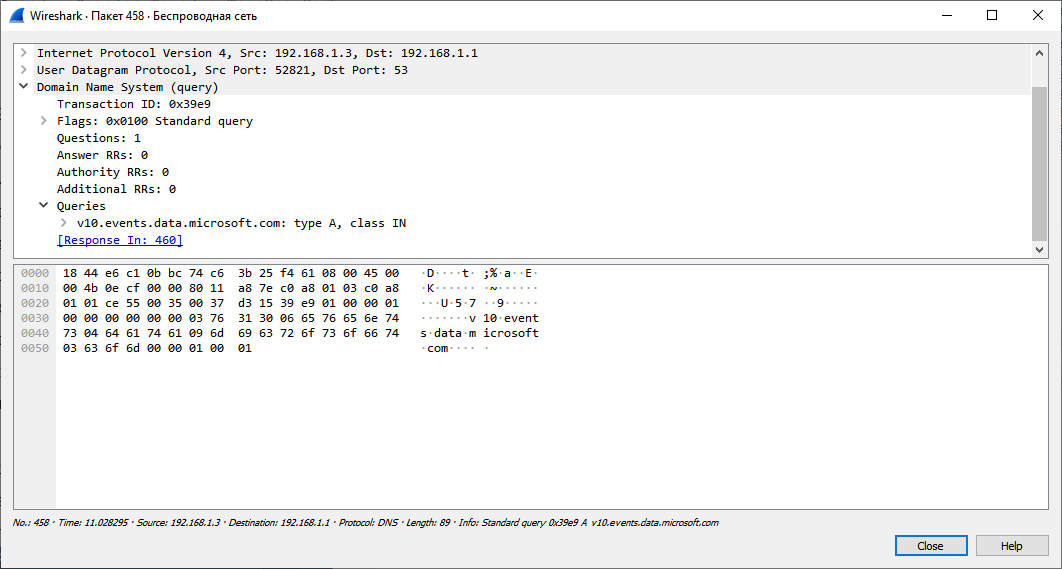
Цільовий: 53

Вихідний: 52821

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

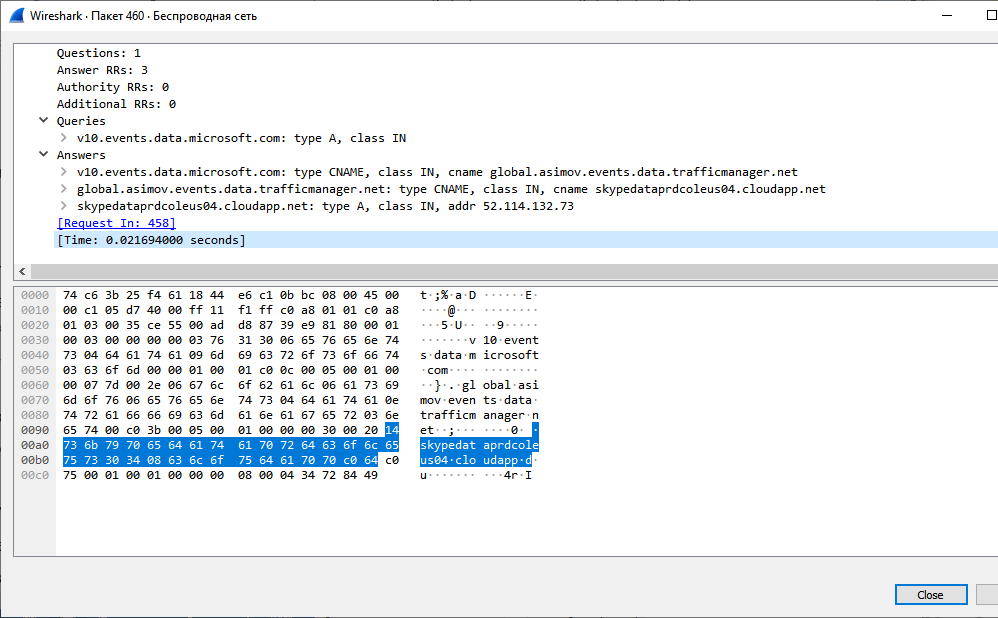
192.168.1.1. Так, є.

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



Вміщує.

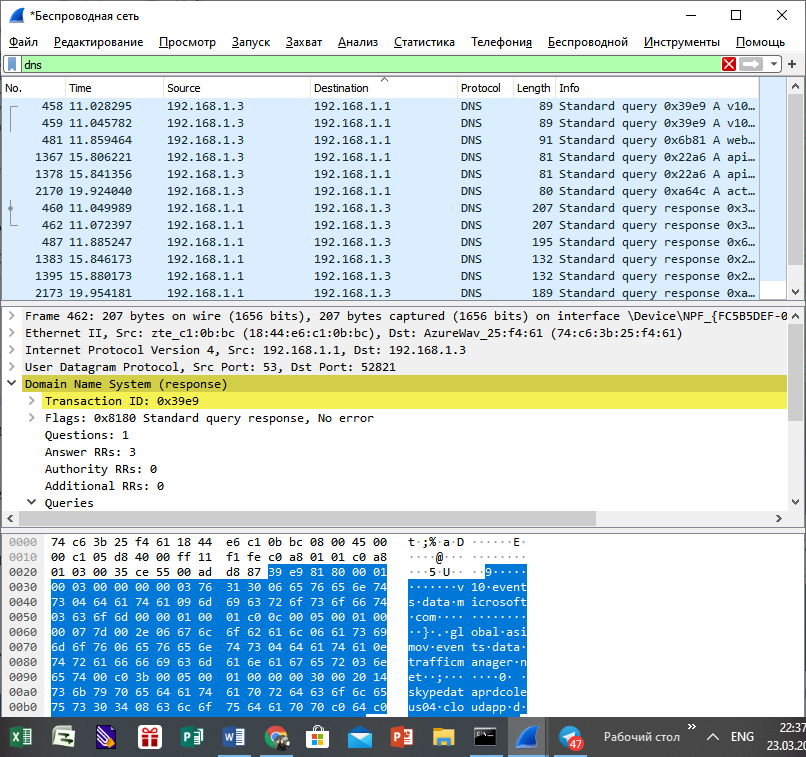
4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?



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?

Ні, не співпадає.

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

Так, виконує.

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

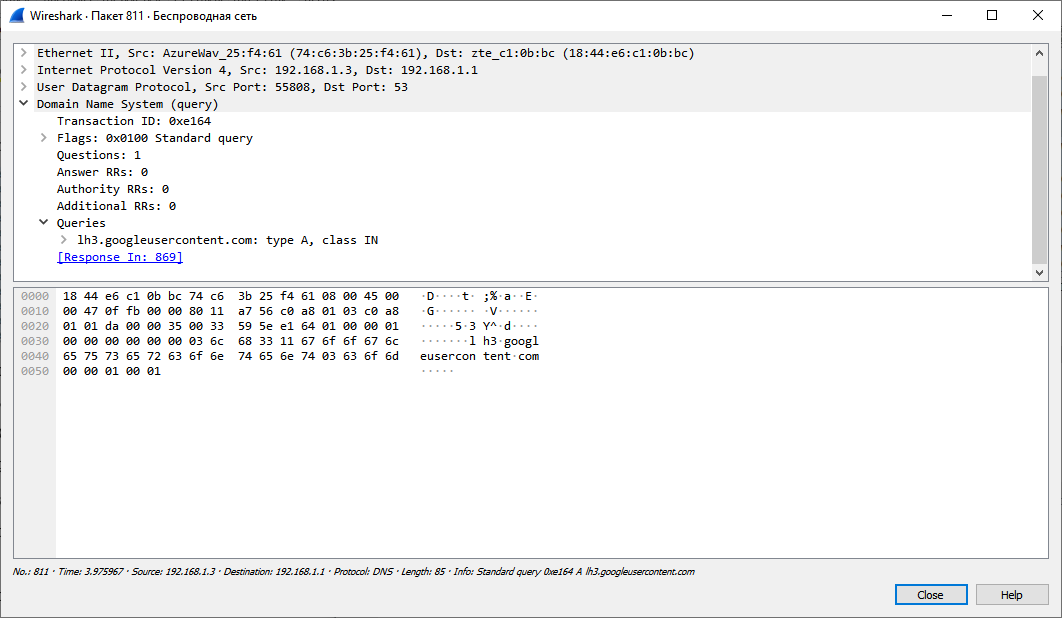
Цільовий: 192.168.1.3

Вихідний: 192.168.1.3

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

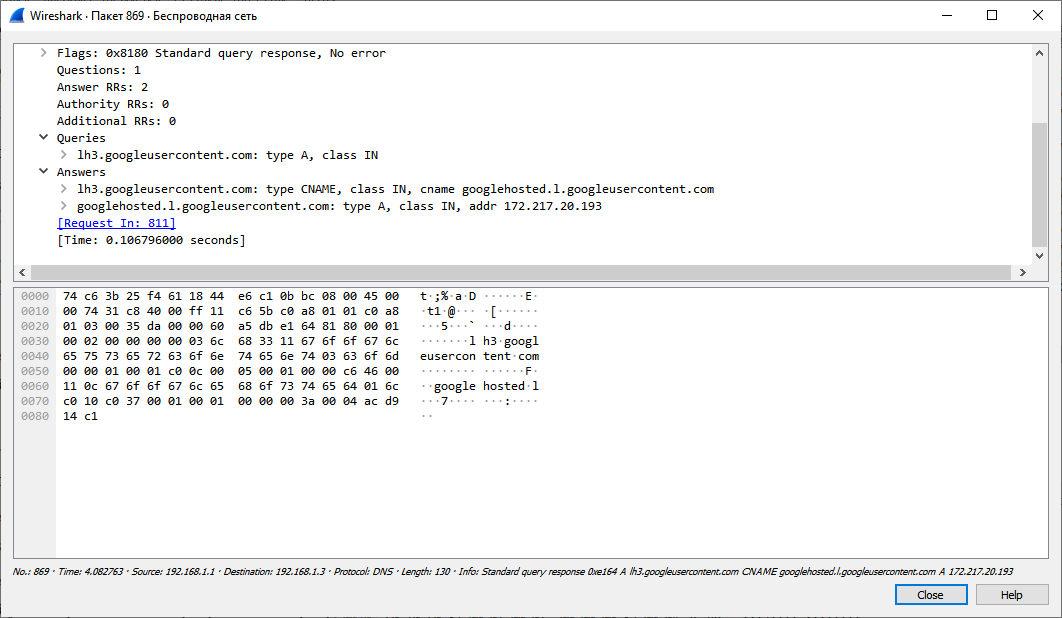
192.168.1.3 . Так, є.

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



Так, вміщує.

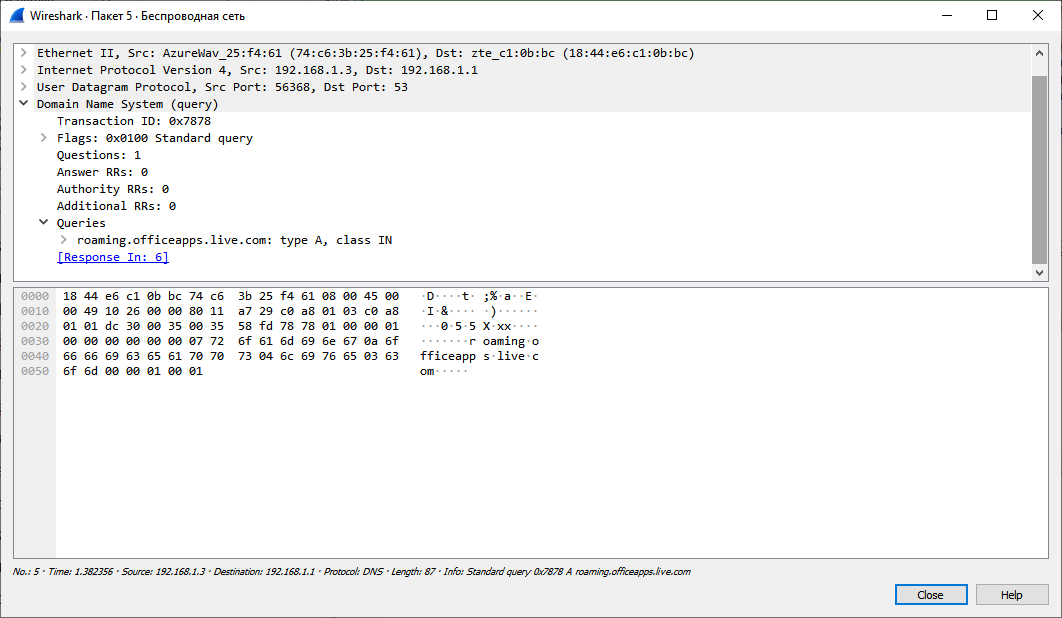
10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?



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

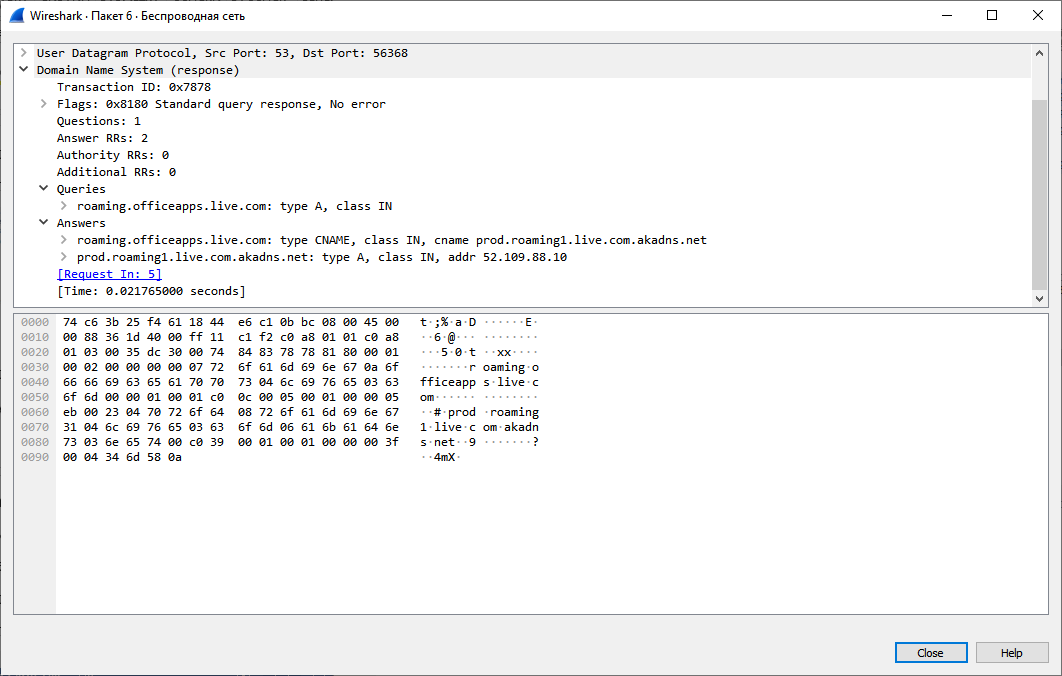
192.168.1.3 , Так, є.

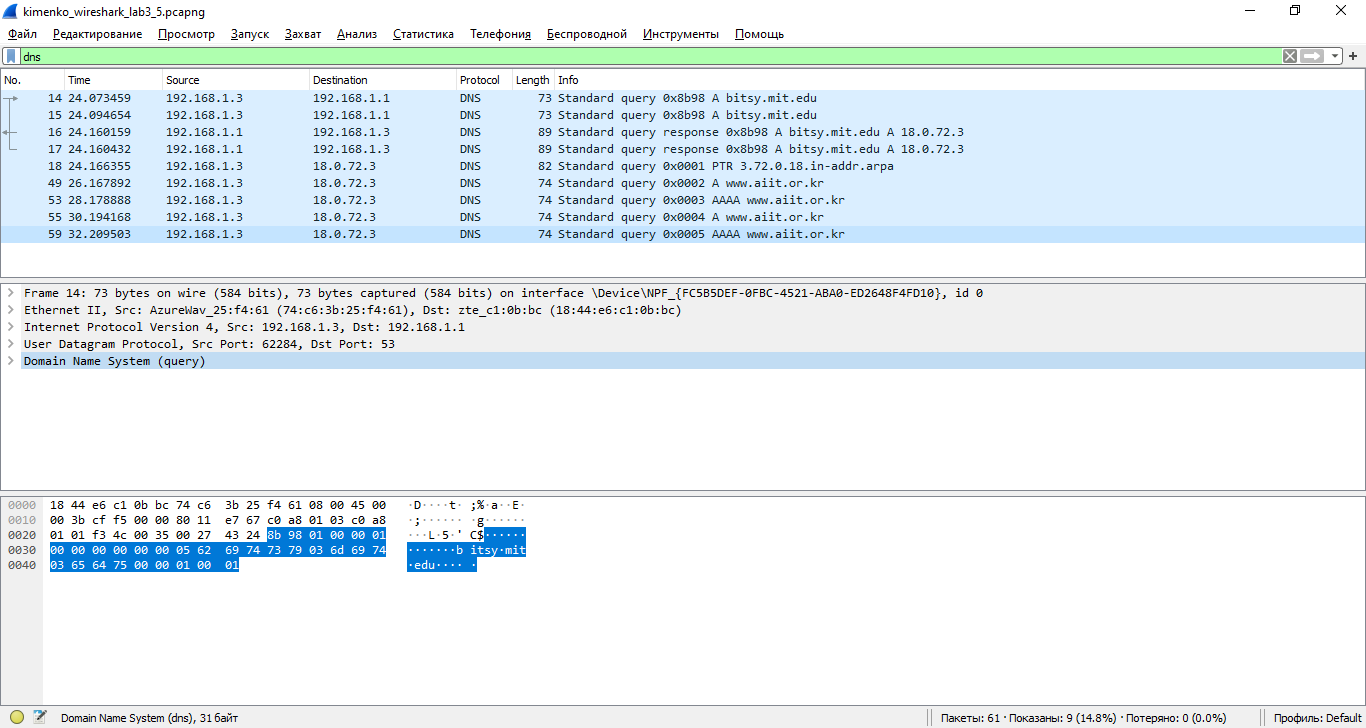
12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?



Так, вміщує.

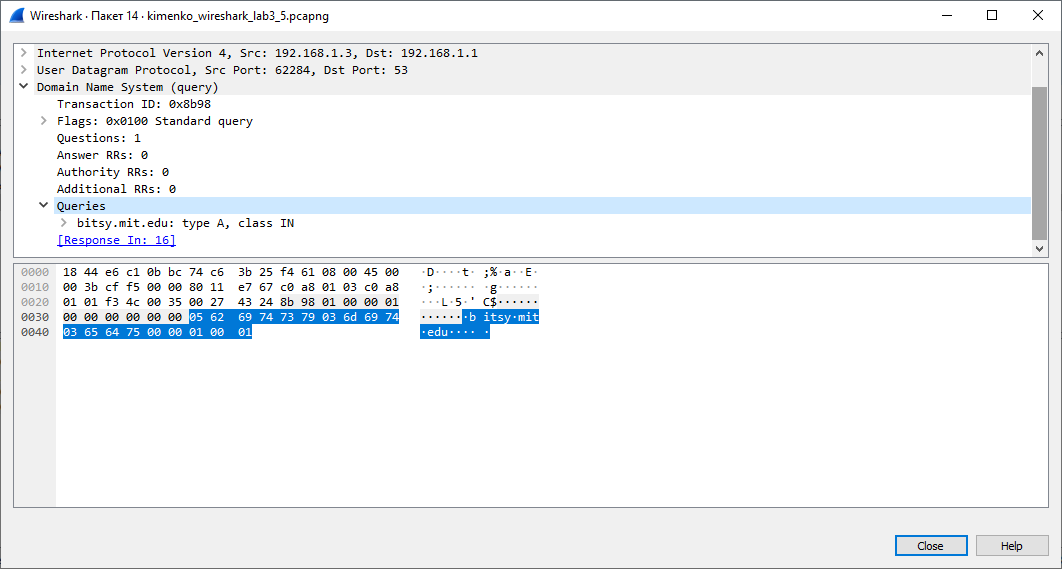
13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?



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

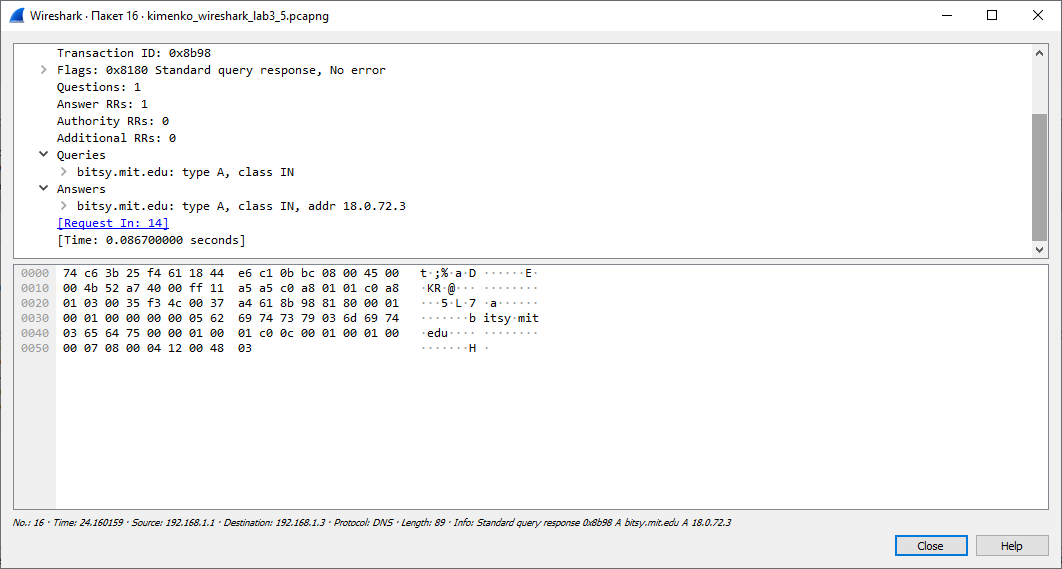
192.168.1.3 , Так, є

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



Так, вміщує.

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 деталей роботи даних протоколів.