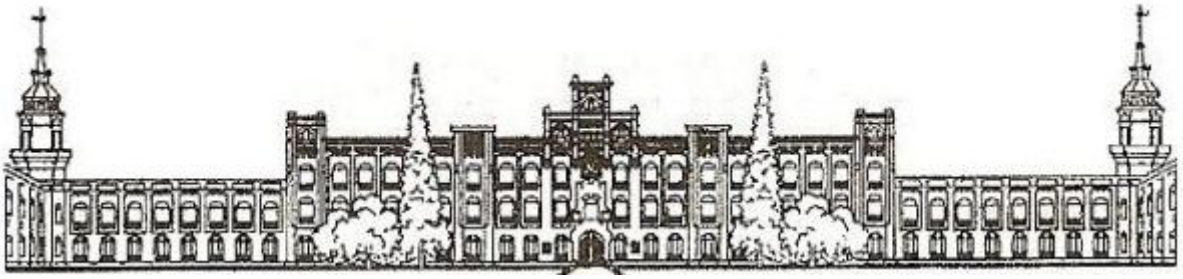


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

КАФЕДРА ММСА

Лабораторна робота № 3

З дисципліни: Комп'ютерні мережі

Протоколи DNS

Виконала:

Студентка III курсу

Групи КА-74

Семіконь Я. В.

Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Wireshark, необхідними для дослідження мережевих протоколів.Начало формы

Хід виконання роботи

```
Germes-Air:~ some321user_34$ nslookup www.mit.edu
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.96.143.80

Germes-Air:~ some321user_34$
```

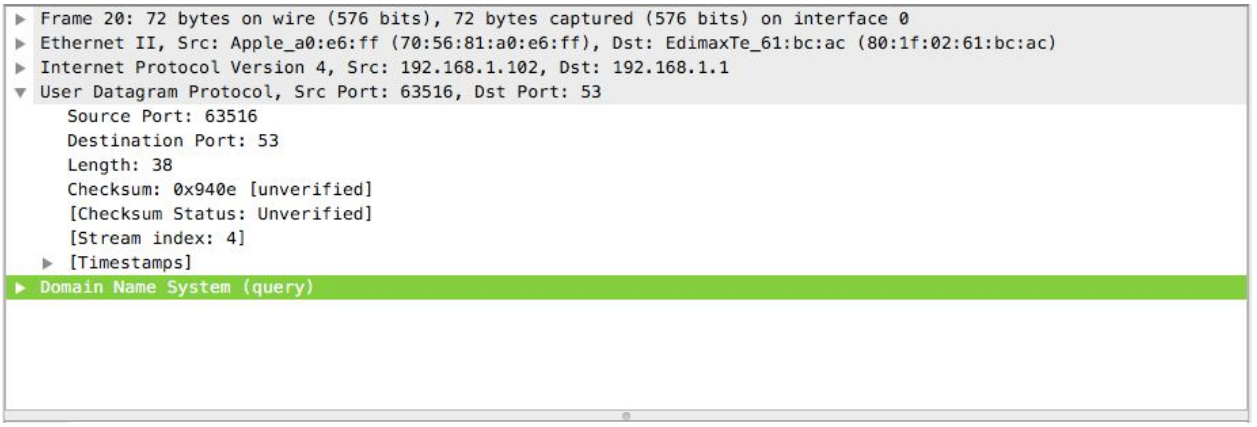
==========

```
Germes-Air:~ some321user_34$ nslookup -type=NS mit.edu
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = eur5.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = use2.akam.net.

Authoritative answers can be found from:

Germes-Air:~ some321user_34$
```

Контрольні запитання:

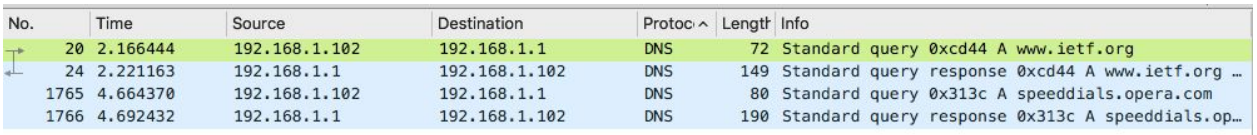
1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

DNS використовує UDP.



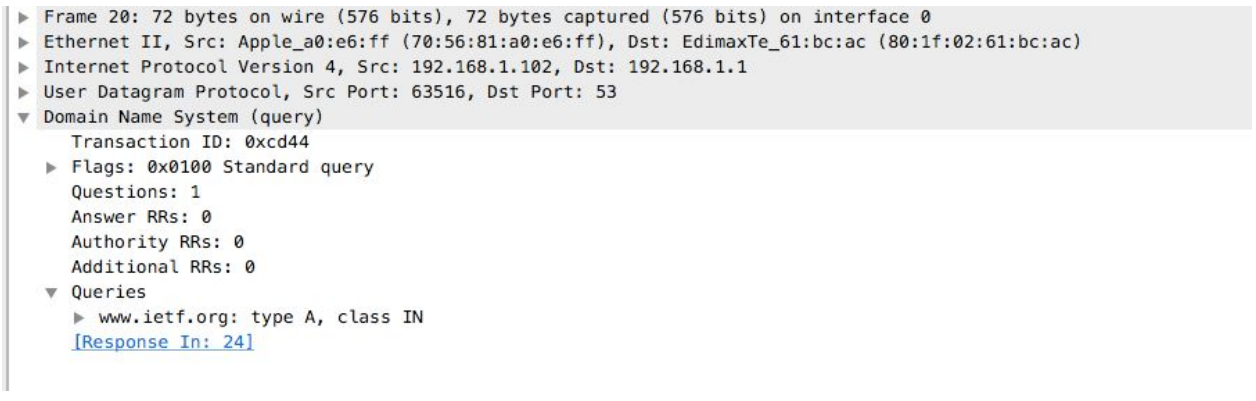
Цільовий порт: 53
Вихідний порт: 63516

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



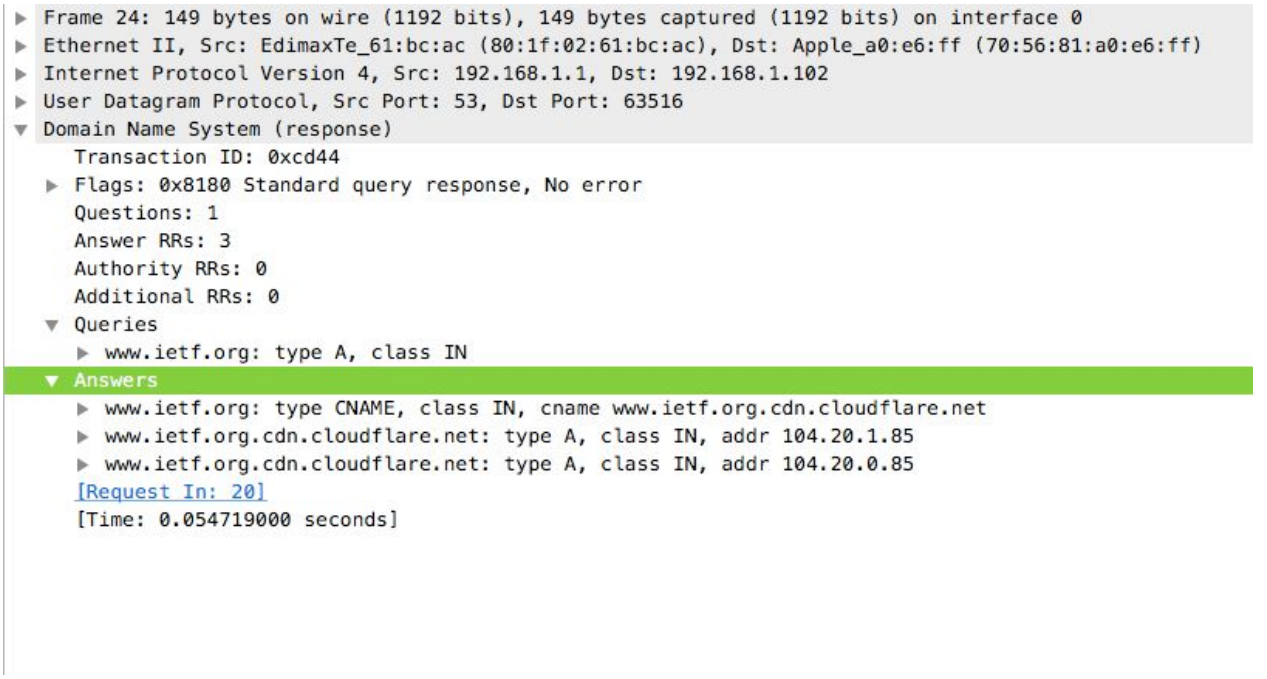
IP: 192.168.1.1 Так є.

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



Тип запиту – A . Вміщує.

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



3 відповіді.

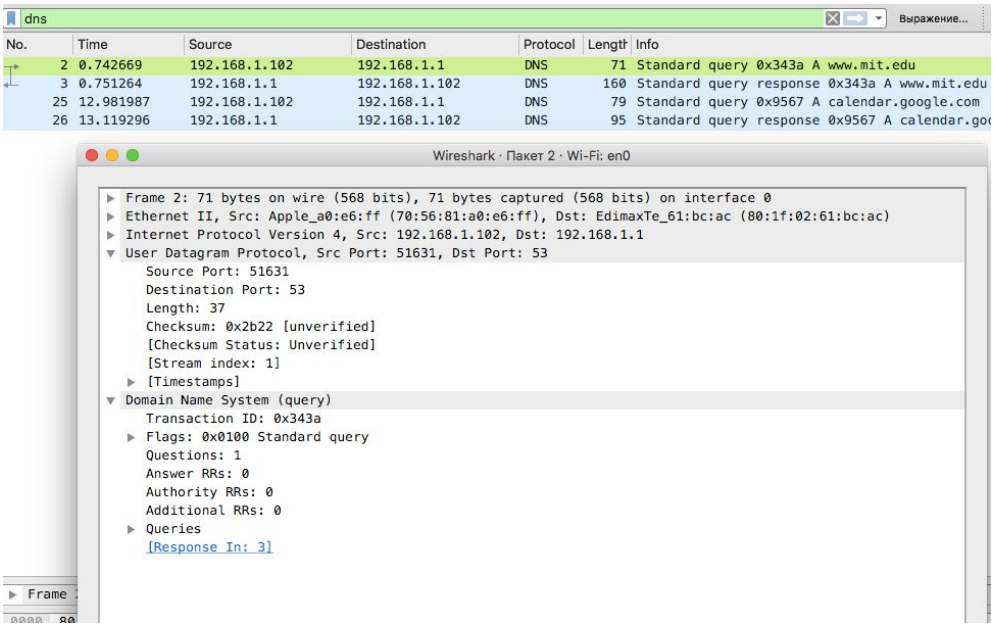
5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з однією із відповідей сервера DNS?

Так, співпадає.

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

Так виконує.

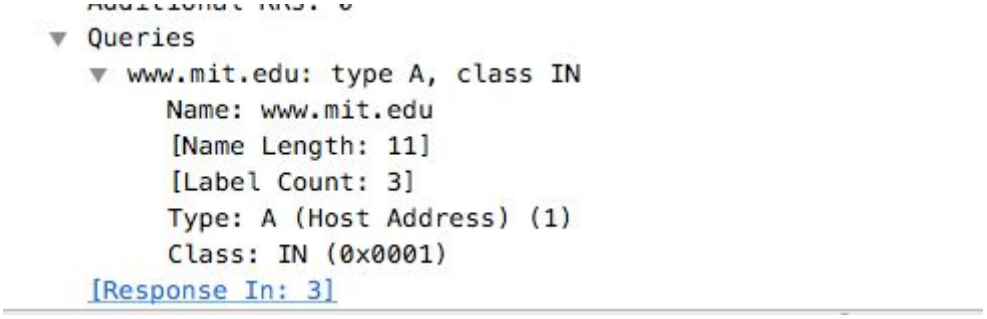
7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?



Цільовий: 53
Вихідний: 51631

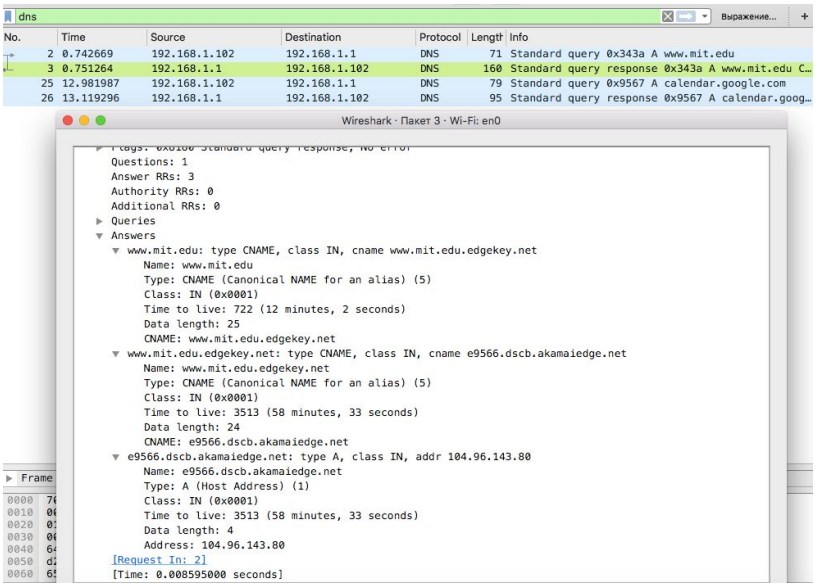
8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?
   192.168.1.1. Так, є адресою локального сервера.

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



Тип запиту - A. Вміщує.

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

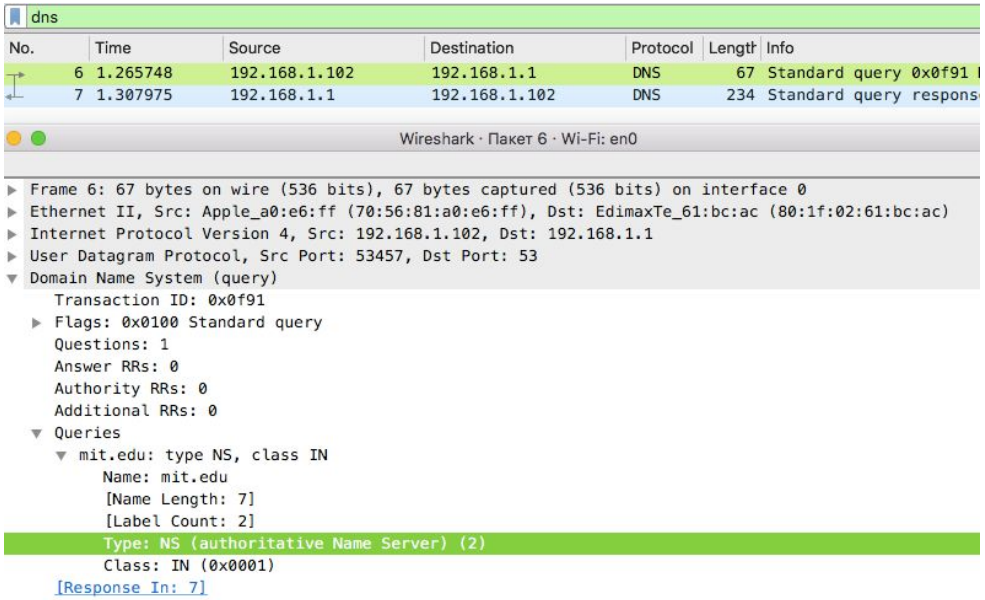


цих відповідей? – 3 відповіді.

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

IP: 192.168.1.1. Так є.

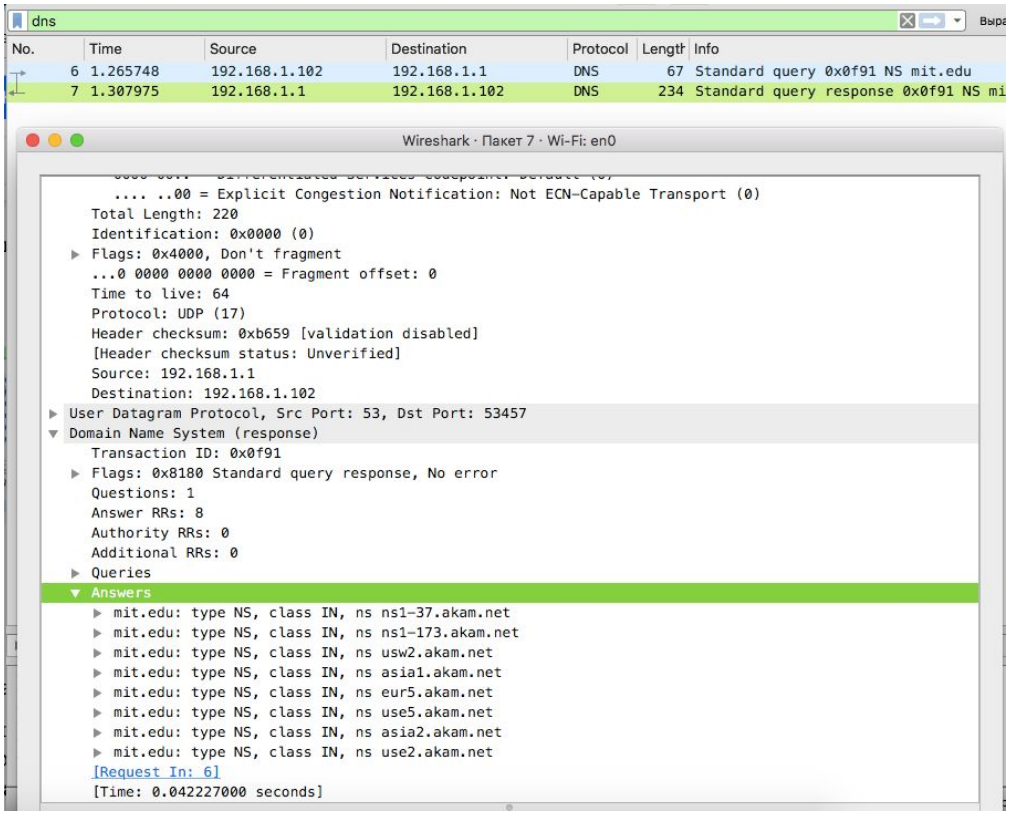
12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?



Тип запиту - NS. Так вміщує.

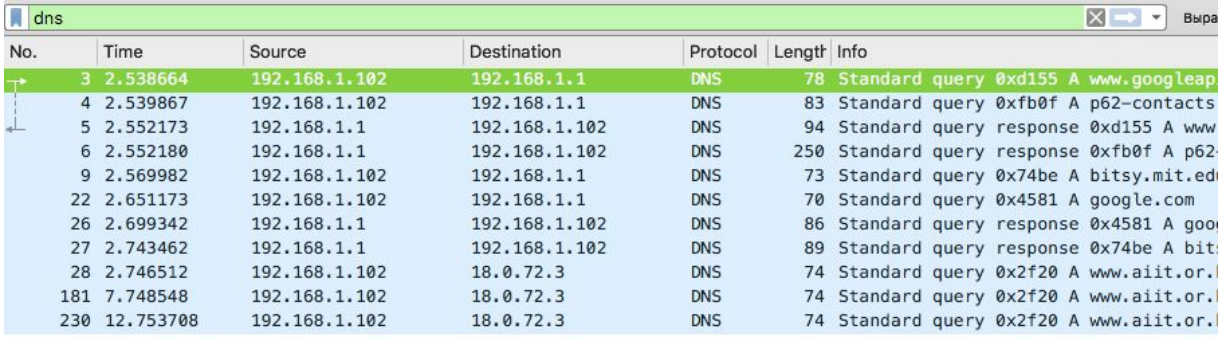
13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою

доменного імені, адреси IP або й того й іншого?



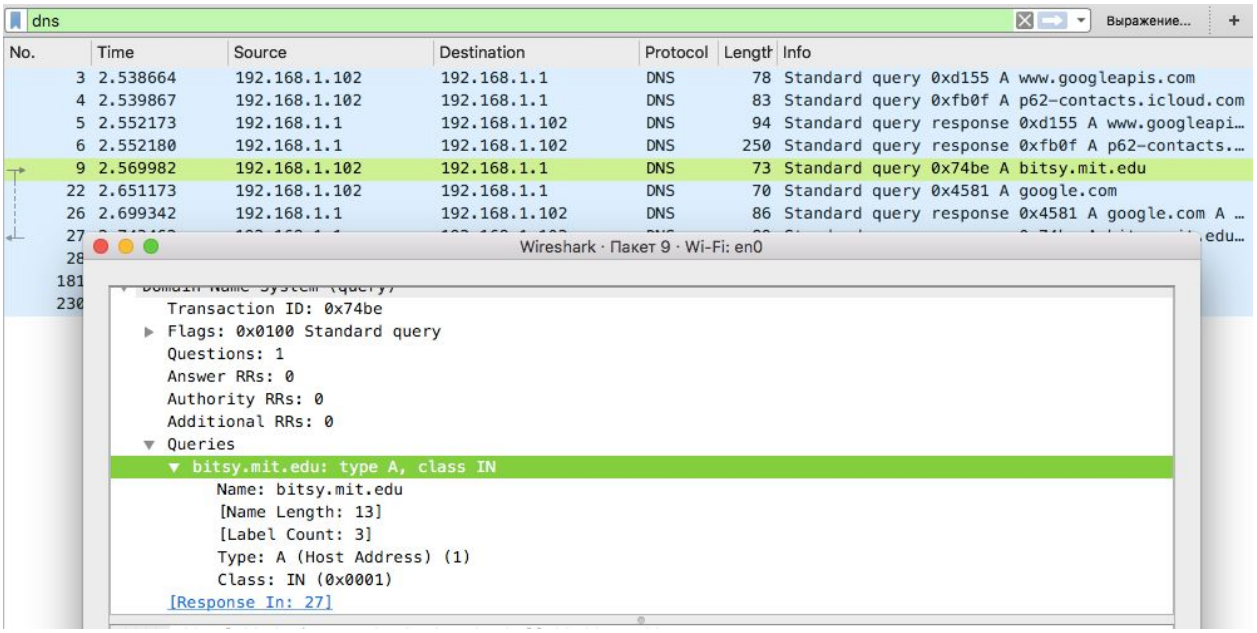
8 записів із відповіддю.

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?



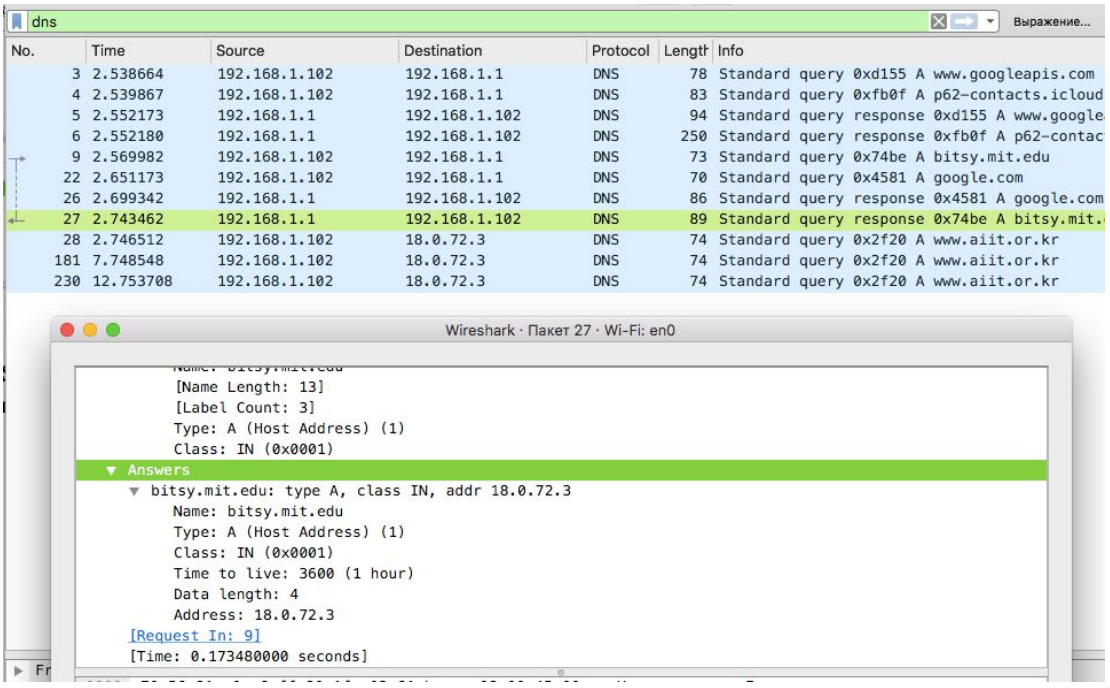
IP: 192.168.1.1. Є адресою локального сервера.

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



Тип запиту - A. Вміщує.

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



Була отримана одна відповідь.

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.