Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Кафедра математичних методів системного аналізу

ЗВІТ

Про виконання лабораторних робіт

з дисципліни «Комп'ютерні мережі»

Виконав: ст. гр. ІС-зп92

Щербак Р.В.

Прийняв: Кухарєв С.О.

Київ – 2020

**Лабораторна робота 3**

**Протокол DNS**

**1. Хід роботи**

1. Очистіть кеш DNS-записів: ipconfig /flushdns (windows)

2. Запустіть веб-браузер, очистіть кеш браузера

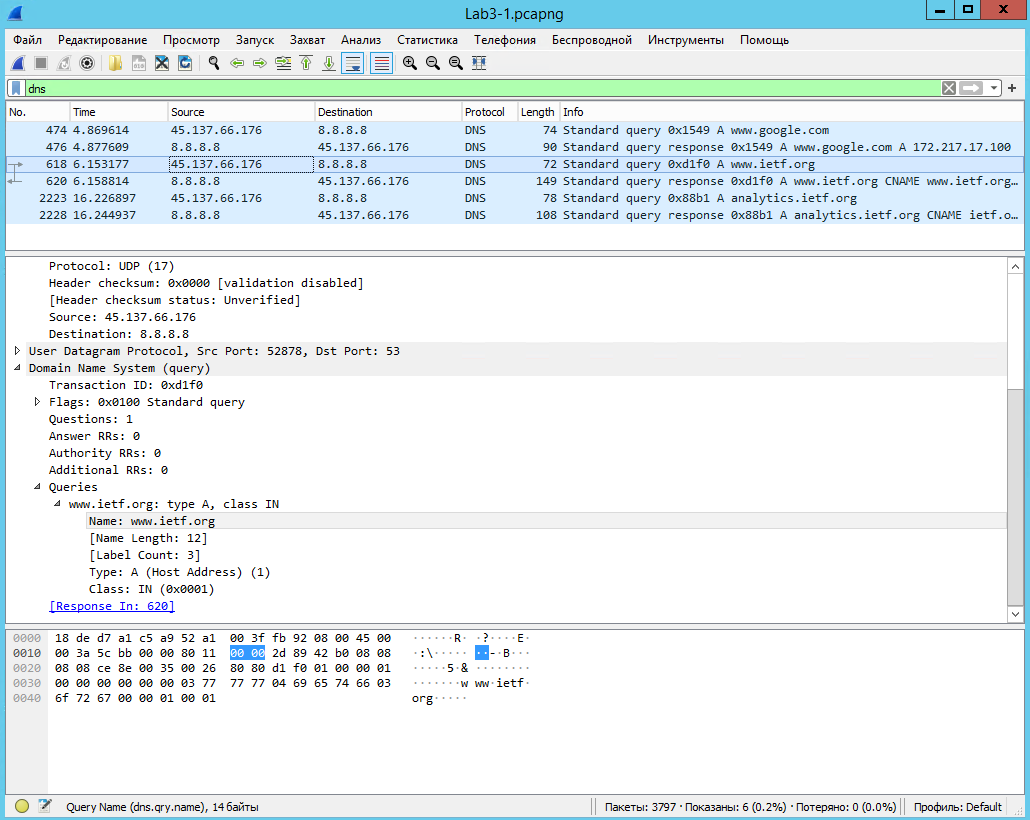
3. Запустіть Wireshark, почніть захоплення пакетів.

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 –Результати запиту

8. Почніть захоплення пакетів

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

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. Почніть захоплення пакетів

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

nslookup –type=NS mit.edu

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

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

18. Зупиніть захоплення пакетів.

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

захоплені пакети

20. Закрийте Wireshark

**2. 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?

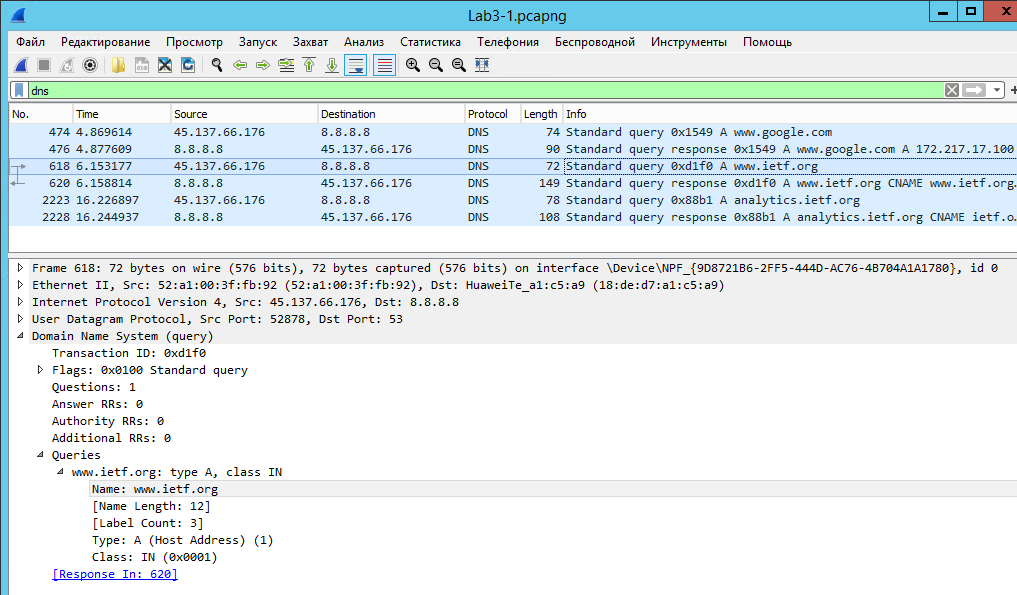
* Використовує протокол UDP. Source: 45.137.66.176, Dest.: 8.8.8.8

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

* Destination: 8.8.8.8 – це зовнішній DNS сервер

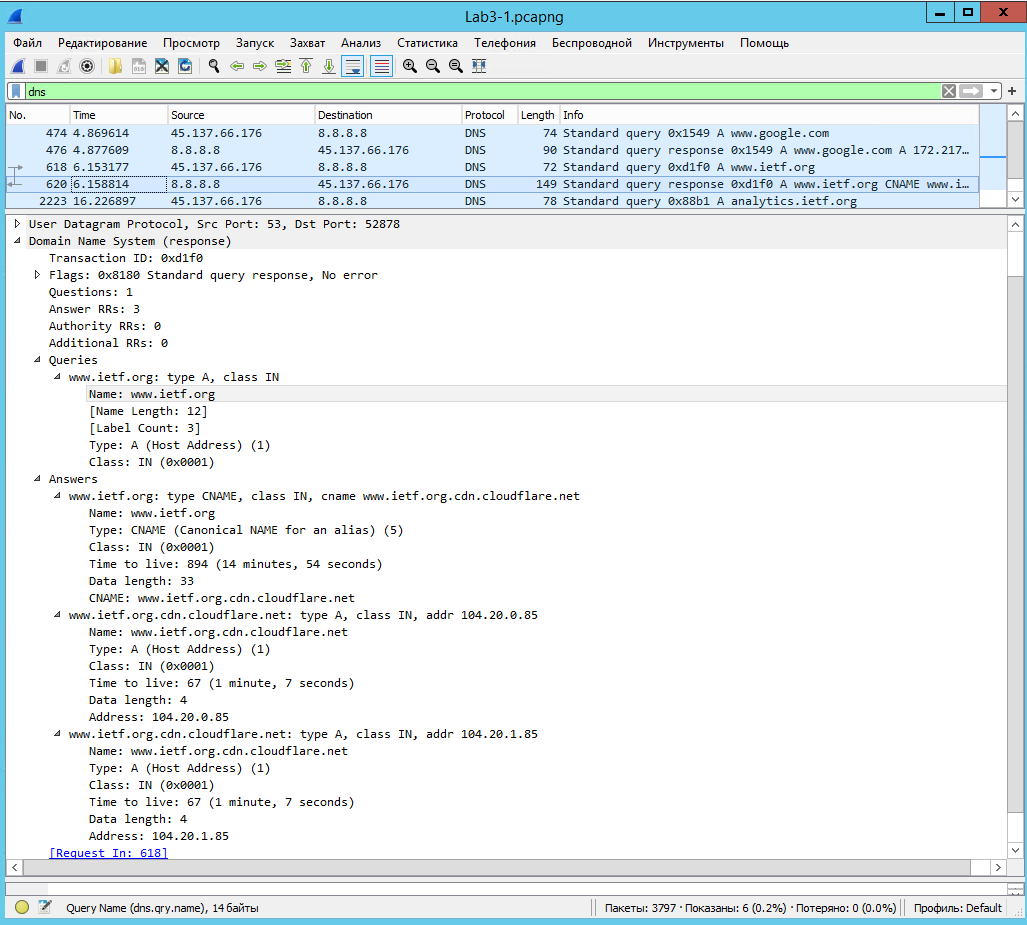
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи Вміщує цей запит деякі можливі компоненти «відповіді»?

* Запит має зону Queries, яка містить DNS-ім’я сайту IP-адресу якого потрібно отримати.
* Тип «A» (Адресний запис, відповідність між ім'ям і IP-адресою)
* В запиті є поле Answer RRs (dns.count.answers), але воно містить значення 0



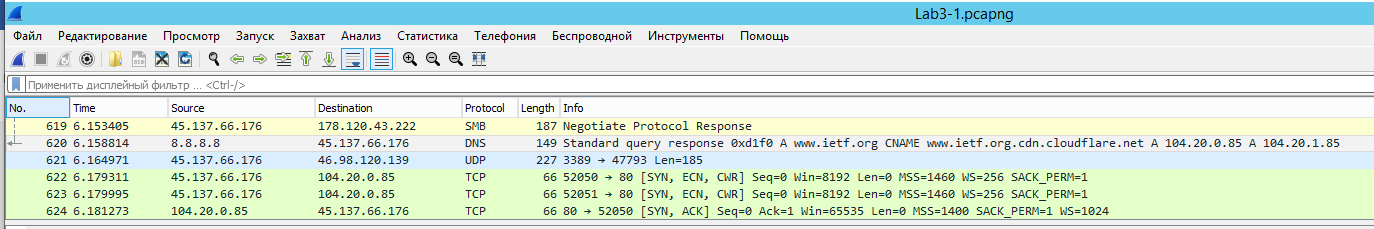
4. Дослідить повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

* 3 відповіді
* 1 відповідь типу CNAME (Канонічне ім'я для псевдоніма (однорівнева переадресація)
* 2 відповіді мають тип A (але повертають різні IP-адреси)
* Кожна відповідь має такі поля: Name, Type, Class, Time to live, Data length, Address;



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, співпадає



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

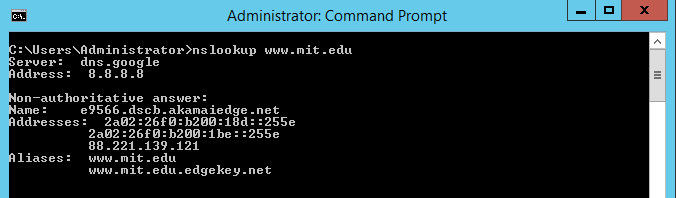
* Так, був виконан ще один запит

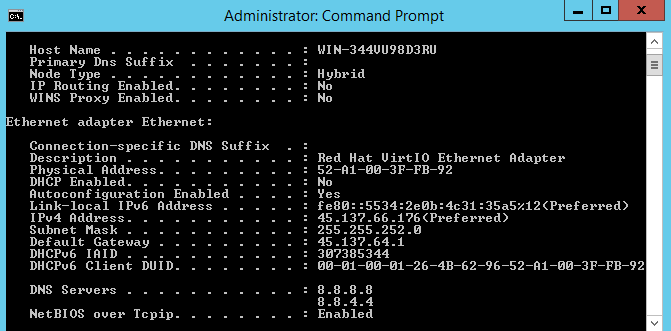
7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

* Запит: Source Port: 60666 Destination Port: 53
* Відповідь: Source Port: 53 Destination Port: 60666

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

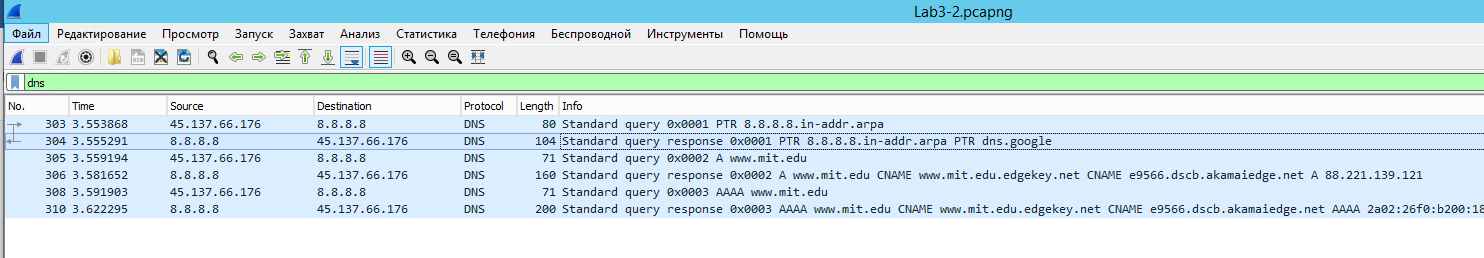
* Dst: 8.8.8.8 – адреса зовнішнього DNS-сервера, який вказано в налаштуваннях мережі





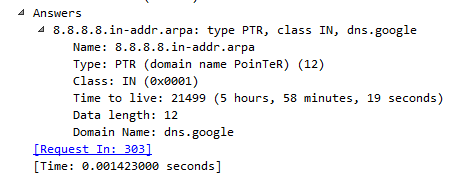
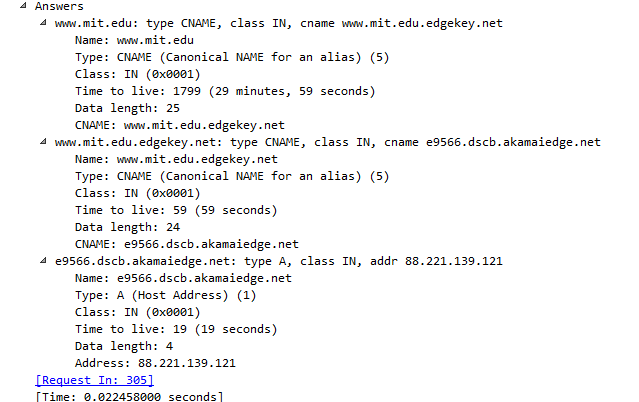
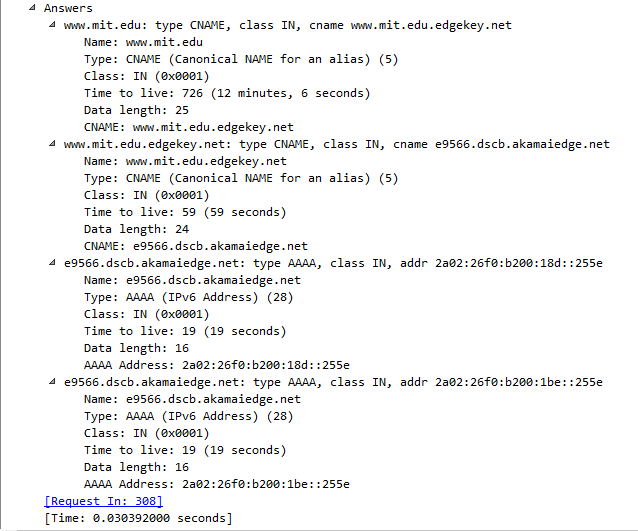
9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

* 1-й запит з типом PTR
* 2-й запит з типом A (Відповідність адреси імені — зворотня відповідність для A і AAAA)
* 3-й запит з типом AAAA (Адреса у форматі IPv6)

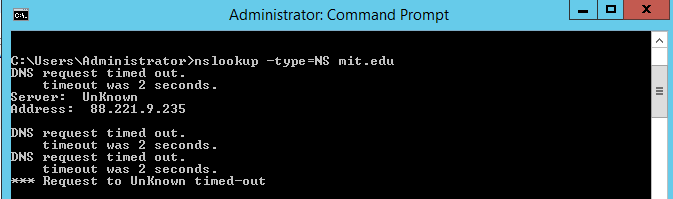


* В запиті є поле Answer RRs (dns.count.answers), але воно містить значення 0

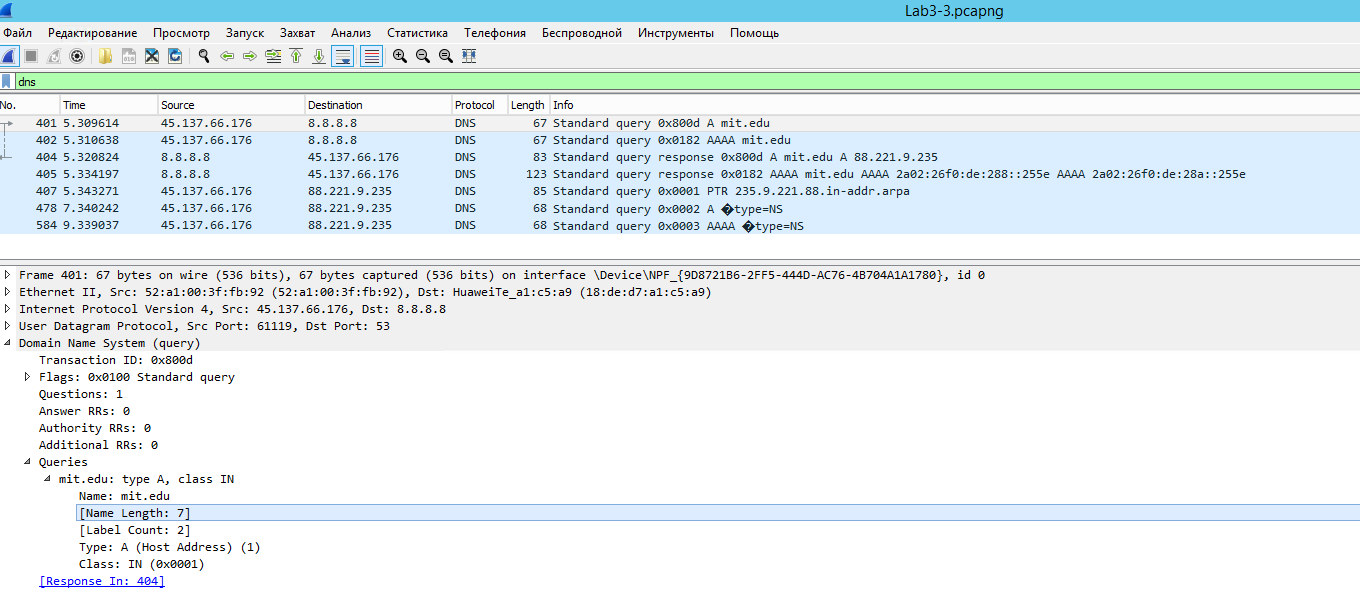
10. Дослідить повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей

* Відповідь (response) на 1-й запит містить 1 відповідь (answer)
* Відповідь (response) на 2-й запит містить 3 відповіді (answer)
* Відповідь (response) на 3-й запит містить 4 відповіді (answer)
* Склад записів відповідей:
  + 
  + 
  + 

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



* Відповідь: Destination: 88.221.9.235 – не є адреса локального сервера DNS за замовчанням



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

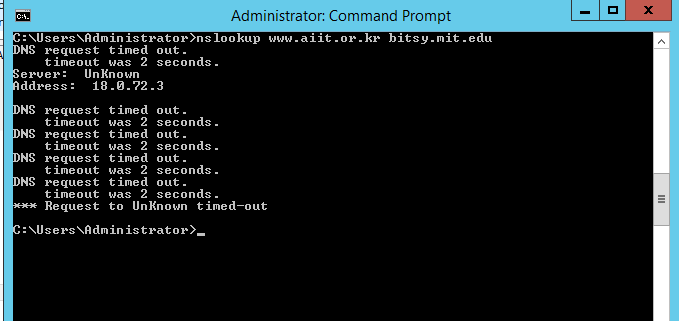
* Було п’ять запитів (request) та 2 відповіді (answer) (див. Малюнок п.11)
* Запити типу A, AAAA, PTR, NS
* Відповіді для типу NS не не отримано

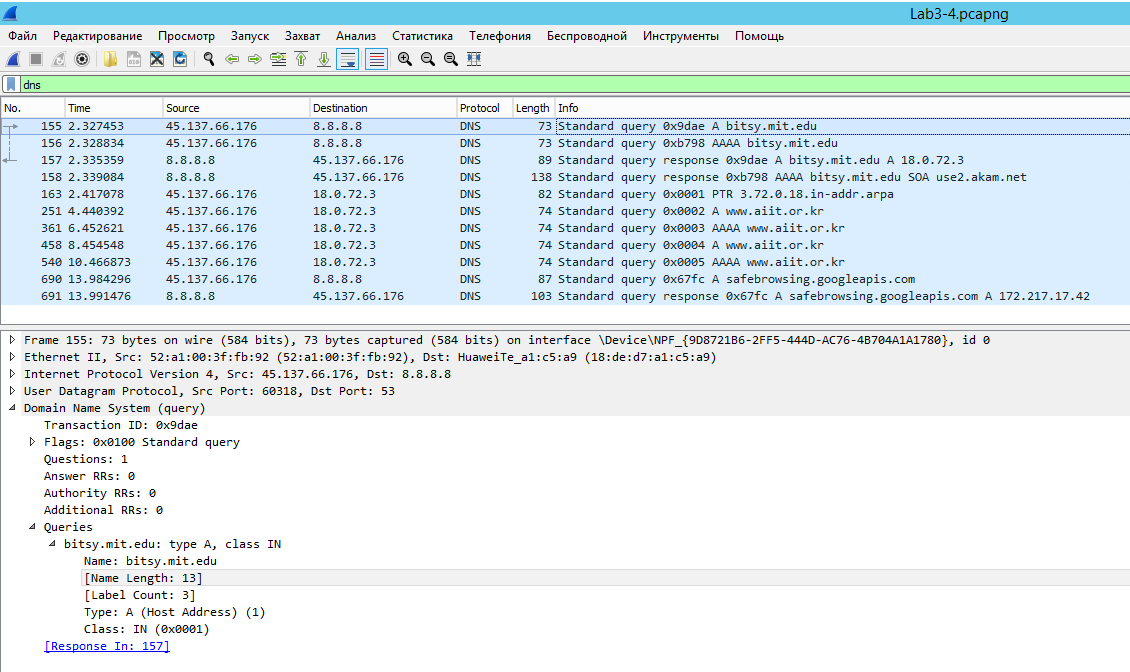
13. Дослідить повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

* 2 записи з відповідями
* Відповідей з типом NS не отримано

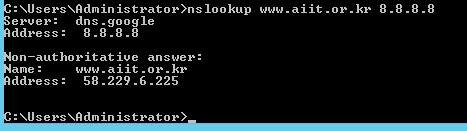
14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

* Запити були відправлені на 8.8.8.8 та 18.0.72.3 що не є адресами локального серверу за замовченням.





Якщо використати DNS-сервер 8.8.8.8, то буде наступний результат



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

Тип запиту А, AAAA, PTR

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

* Було отримано 3 відповіді на 8 запитів
* 