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-ЗП91

Коган Антон

Прийняв: Кухарєв С.О.

**Лабораторна робота No3 3. Протокол DNS**

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

***3.2. Хід роботи***

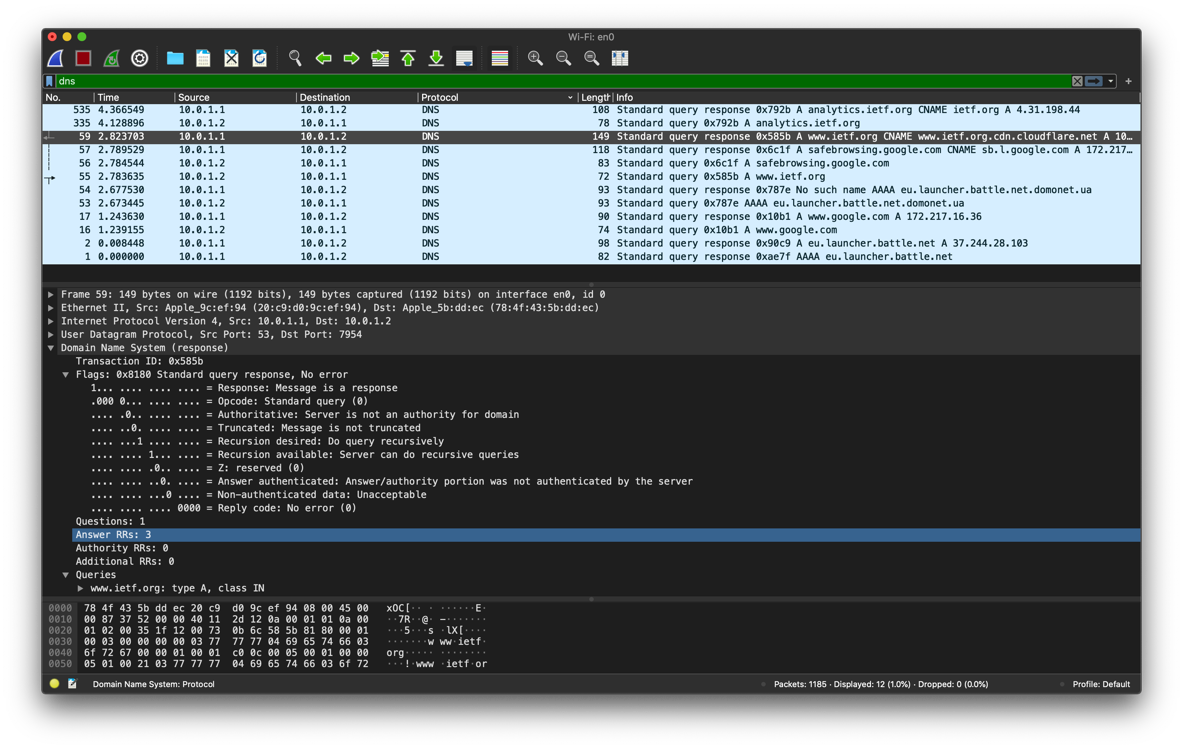
Виконаємо наступні дії:  
1. Очистимо кеш DNS-записів

2. Запустимо веб-браузер, очистимо кеш браузера:

3. Запустимо Wireshark, почнемо захоплення пакетів.  
4. Відкриємо за допомогою браузера одну із зазначених нижче адрес:

http://www.ietf.org

5. Зупинемо захоплення пакетів.  
6. Переглянемо деталі захоплених пакетів.



7. Приготуємо відповіді на контрольні запитання 1-6, роздрукуємо необхідні для цього пакети.

7.1. Знайдемо запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер

вихідного порта відповіді DNS?   
A screenshot of a cell phone

Description automatically generated

7.2.  На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?   
Internet Protocol Version 4, Src: 10.0.1.1, Dst: 10.0.1.2

7.3.  Проаналізуємо повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?   
A screenshot of a cell phone

Description automatically generated

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

A close up of text on a black background

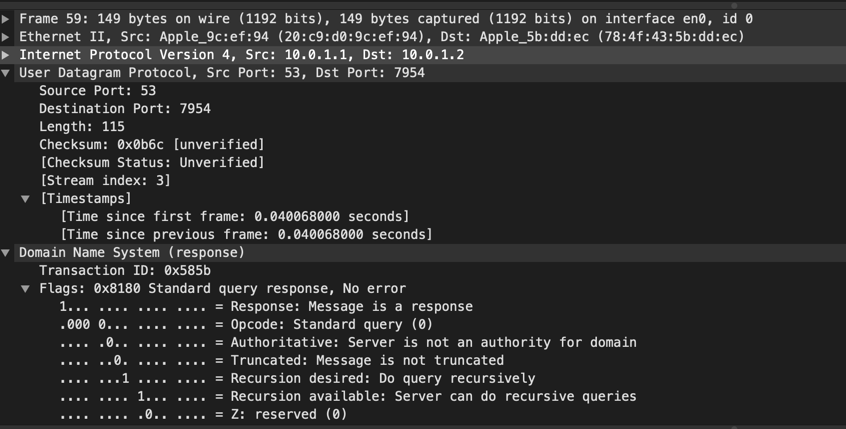
Description automatically generated

7.5.  Проаналізуємо 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

7.6.  Чи виконує ваша робоча станція нові запити DNS для отримання

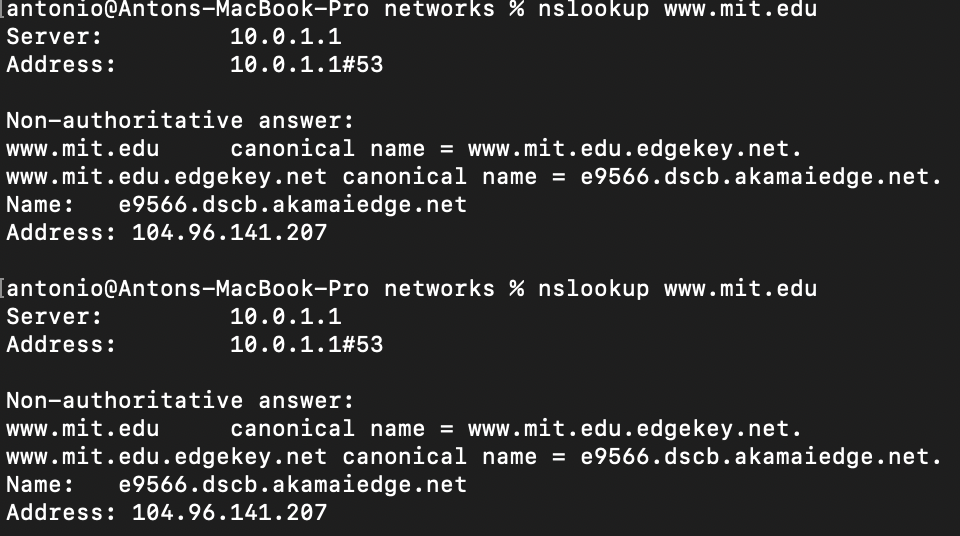
ресурсів, які використовує документ, що отримав браузер? так

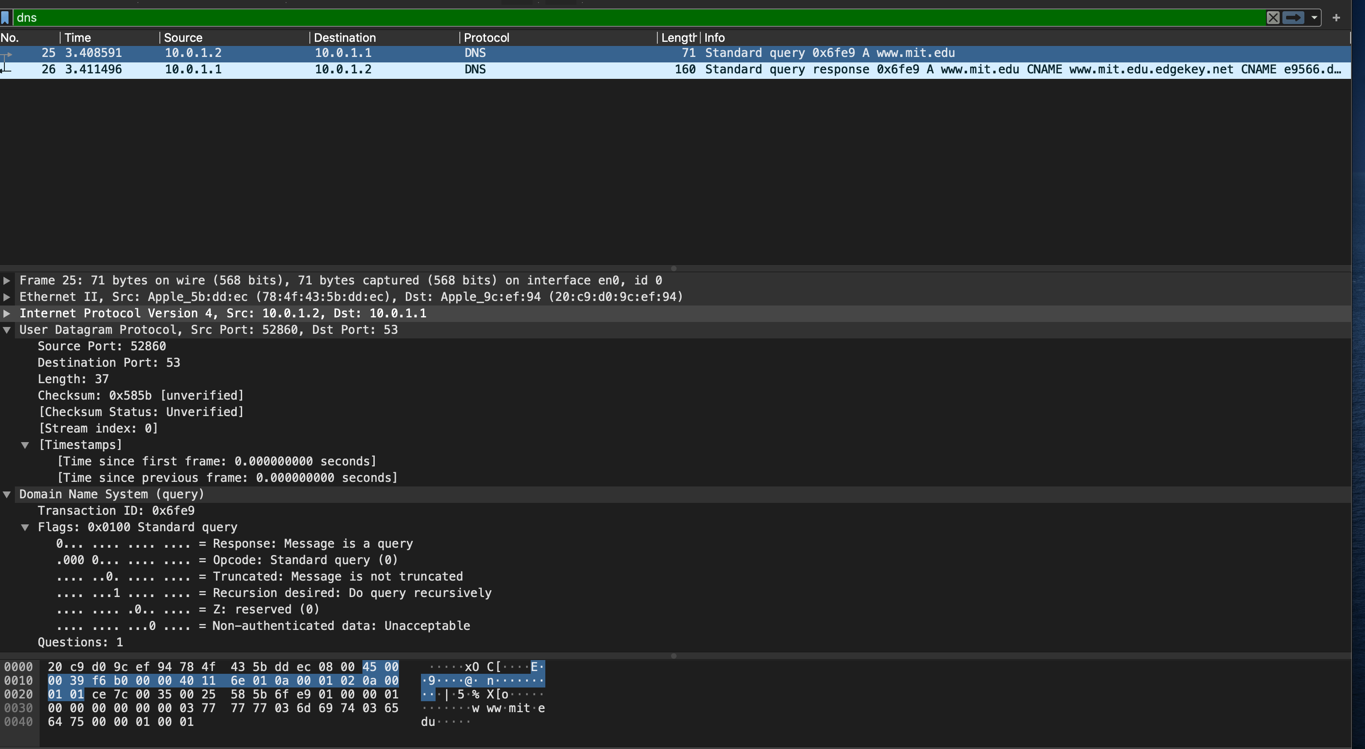


8. Почнимо захоплення пакетів.  
9. Виконаємо nslookup для домену www.mit.edu за допомогою команди

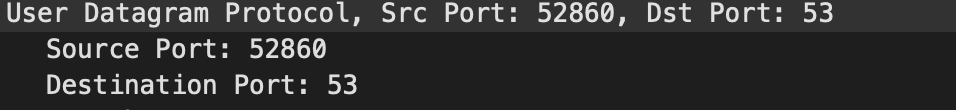
a. nslookup www.mit.edu

10. Зупинимо захоплення пакетів.





11. Приготуємо відповіді на контрольні запитання 7-10, роздрукуємо 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.

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

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

A picture containing drawing, meter

Description automatically generated

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

A screenshot of a cell phone

Description automatically generated

10. Дослідимо повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?   
з 3х записів.

A screenshot of a cell phone

Description automatically generated

12. Почнимо захоплення пакетів.  
13. Виконаємо nslookup для домену www.mit.edu за допомогою команди

a. nslookup –type=NS mit.edu   
A screenshot of a cell phone

Description automatically generated

14. Зупинимо захоплення пакетів.

15. Приготуємо відповіді на запитання 11-13. При необхідності роздрукуємо деякі захоплені пакети.

15.11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?   
 10.0.1.1 DNS 67 Standard query 0x34a1 A mit.edu  
так, це адреса за замовченням.   
A screen shot of a social media post

Description automatically generated

15.12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»? тип А, відповідь прийшла окремо.

A close up of a black background

Description automatically generated

15.13. Дослідимо 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?   
1 відповідь mit.edu: type A, class IN, addr 104.96.141.207   
Домен та адреса.  
A screenshot of a cell phone

Description automatically generated

16. Почнемо захоплення пакетів.  
17. Виконаємо nslookup для домену www.mit.edu за допомогою команди

a. nslookup www.aiit.or.kr

A screenshot of a cell phone

Description automatically generated

1. Зупинимо захоплення пакетів.
2. Приготуємо відповіді на запитання 14-16  
   19.14. 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?   
   60 3.400217 10.0.1.2 **10.0.1.1** DNS 74 Standard query 0xc1a9 A [www.aiit.or.kr](http://www.aiit.or.kr)

10.0.1.1 - моя адреса за замовченням.

19.15. Дослідимо повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?   
A screenshot of a cell phone

Description automatically generated

19.16. Дослідимо повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей? 1 запис:

A screenshot of a cell phone

Description automatically generated