1. Мета роботи

Метою даної лабораторної роботи є аналіз деталей роботи протоколу DNS.

2. Хід роботи

Під час виконання лабораторної роботи виконано наступні дії:

1. Очищено кеш DNS-записів.

2. Запущено веб-браузер, очищено кеш браузера.

3. Запущено Wireshark, розпочато захоплення пакетів.

4. Відкрито за допомогою браузера адресу http://www.ietf.org.

5. Зупинено захоплення пакетів.

6. Переглянуто деталі захоплених пакетів.

7. Підготовлено відповіді на контрольні запитання 1-6, роздруковано необхідні для цього пакети. Відповіді на запитання 1 - 6 наведено у розділі 3.

8. Знов розпочато захоплення пакетів.

9. Виконано nslookup для домену www.mit.edu за допомогою команди nslookup www.mit.edu.

10. Зупинено захоплення пакетів.

11. Підготовлено відповіді на контрольні запитання 7-10, роздруковано необхідні для цього пакети.

12. Знов розпочато захоплення пакетів.

13. Виконано nslookup для домену www.mit.edu за допомогою команди nslookup -type=NS mit.edu.

14. Зупинено захоплення пакетів.

15. Підготовлено відповіді на запитання 11-13. Роздруковано необхідні для цього пакети.

16. Знов розпочато захоплення пакетів.

17. Виконано nslookup для домену www.mit.edu за допомогою команди nslookup www.aiit.or.kr bitsy.mit.edu.

18. Зупинено захоплення пакетів.

19. Підготовлено відповіді на запитання 14-16. Роздруковано необхідні для цього пакети.

20. Закрито Wireshark.

3. Відповіді на контрольні питання

3.1. 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 протокол UDP.

Destination Port: 53, Source Port: 6308.

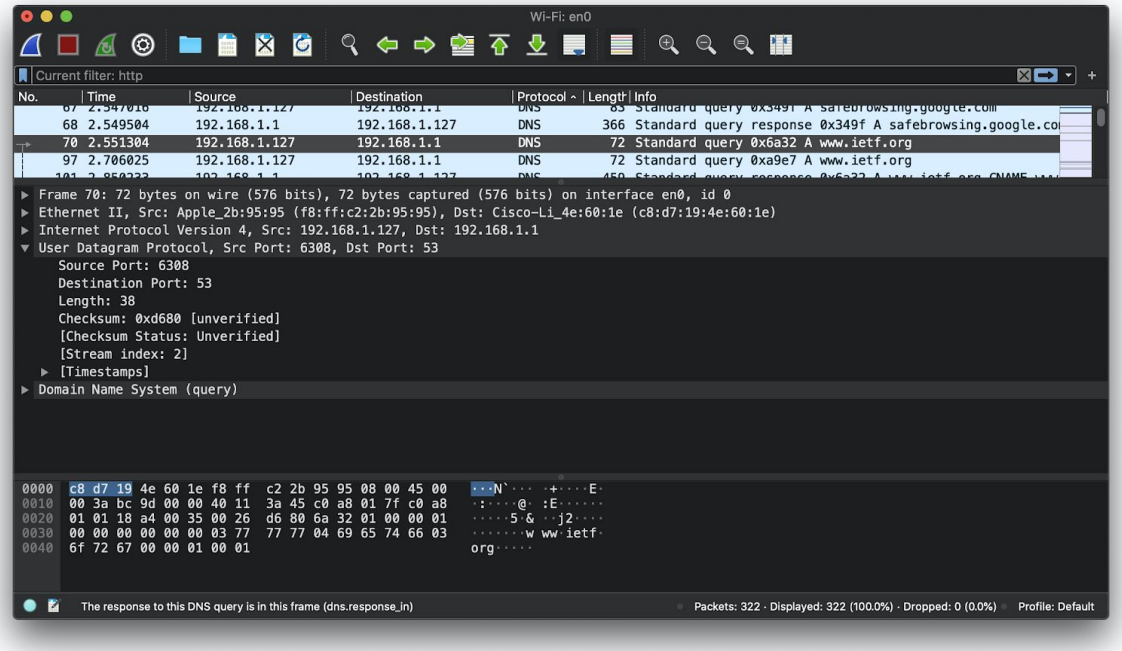

Рис 1. Використаний протокол та використані порти запиту

3.2. На який адрес IP був відправлений запит DNS? Чи є цей

адрес адресом локального сервера DNS?

Destination: 192.168.1.1 – є адресою локального DNS сервера

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

Type A (Адресний запис, відповідність між ім'ям і IP-адресою). Вміщує посилання на рядок з відповіддю [Response In: 168].

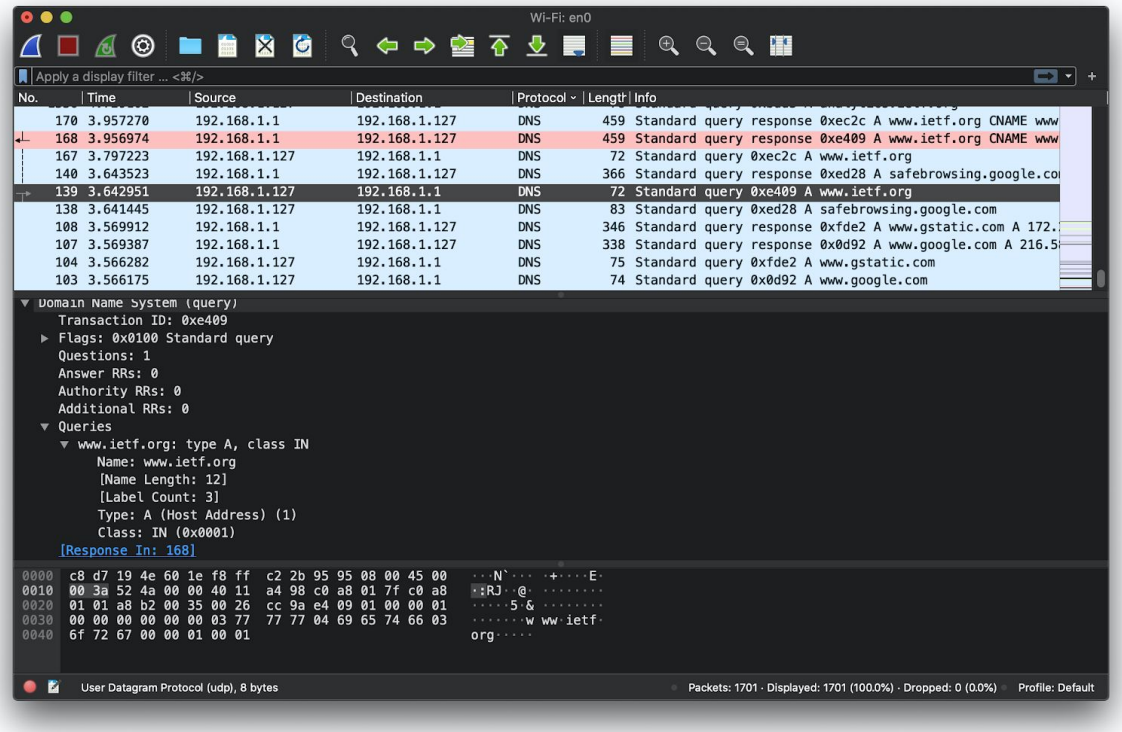

Рис 2. Тип запиту та можливі компоненти відповіді

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

Отримано 3 відповіді:

1. www.ietf.org: type CNAME, class IN,

cname www.ietf.org.cdn.cloudflare.net

Type CNAME - канонічне ім'я для псевдоніма.

2. www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

3. www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

- адресні записи, відповідність між ім'ям і IP-адресою.

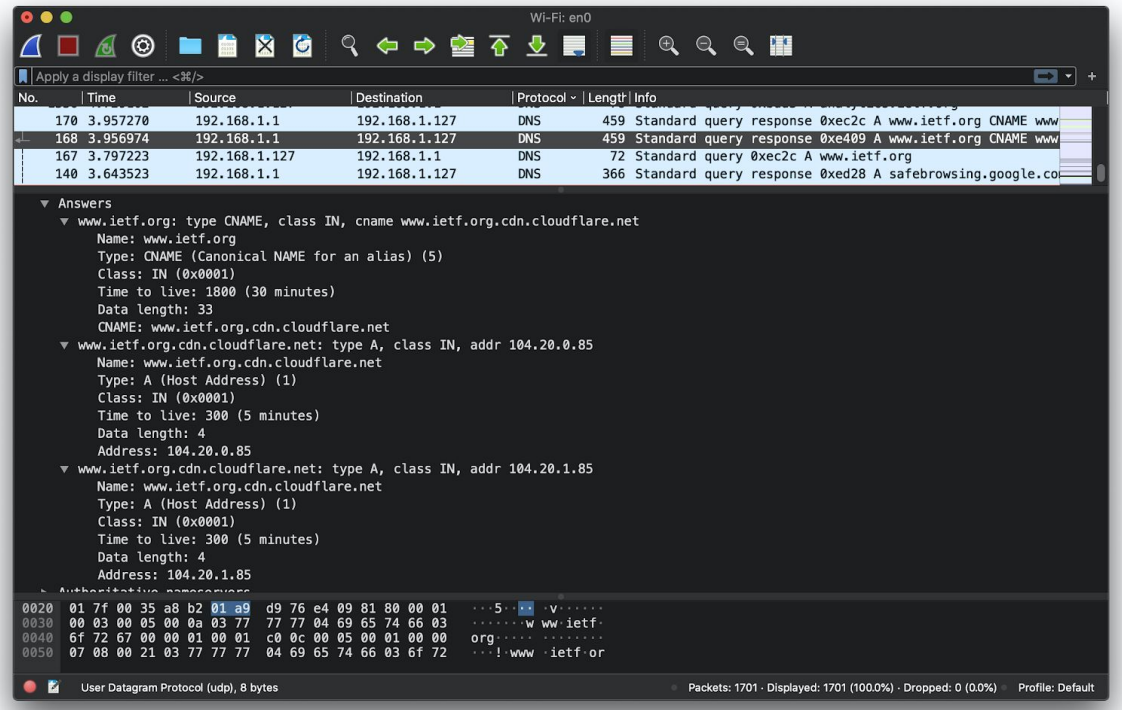

Рис 3. Відповіді запропоновані сервером

3.5. 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.

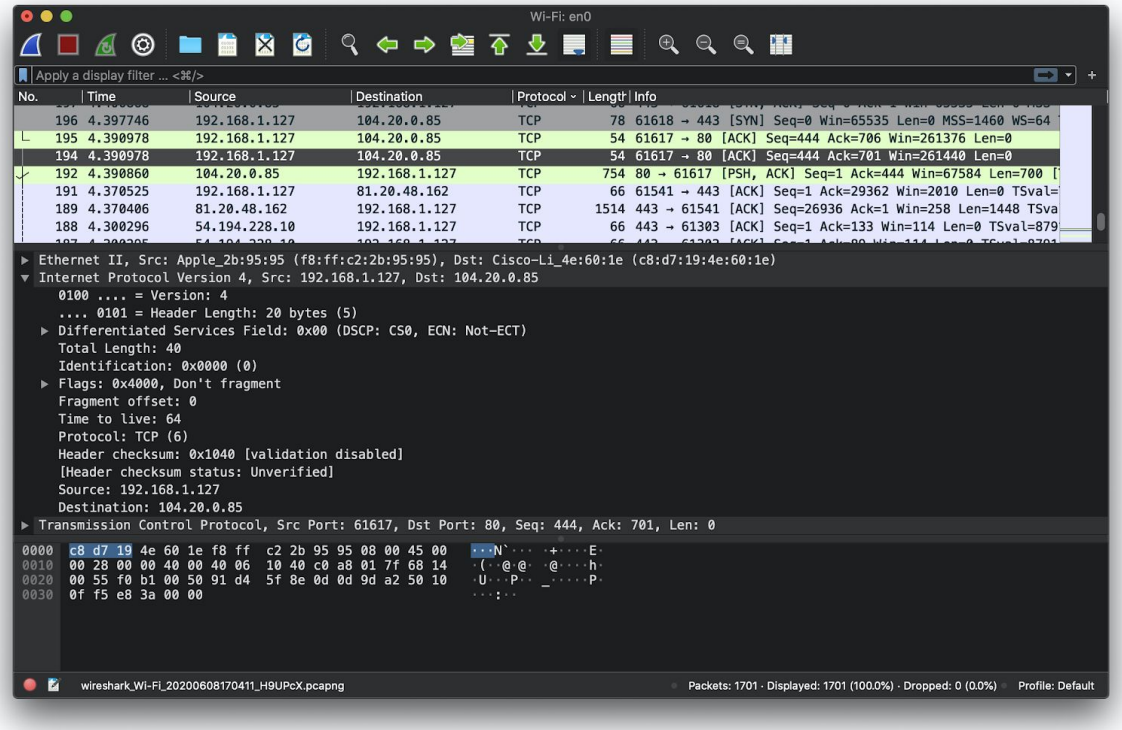

Рис 4. Цільова IP адреса TCP SYN повідомлення

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

Так. Було відправлено запити на отримання IP адреси до analytics.ietf.org

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

Destination Port: 53, Source Port: 58234

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

Destination: 192.168.1.1 – є адресою локального DNS сервера.

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

Type A (Адресний запис, відповідність між ім'ям і IP-адресою), вміщує посилання на рядок з відповіддю [Response In: 70]

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

3 записи із відповідями було запропоновано сервером. 2 запису типу CNAME, які прив’язують псевдонім к дійсному (канонічному) доменному імені, та 1 типу A, який повертає IP адресу цих імен.

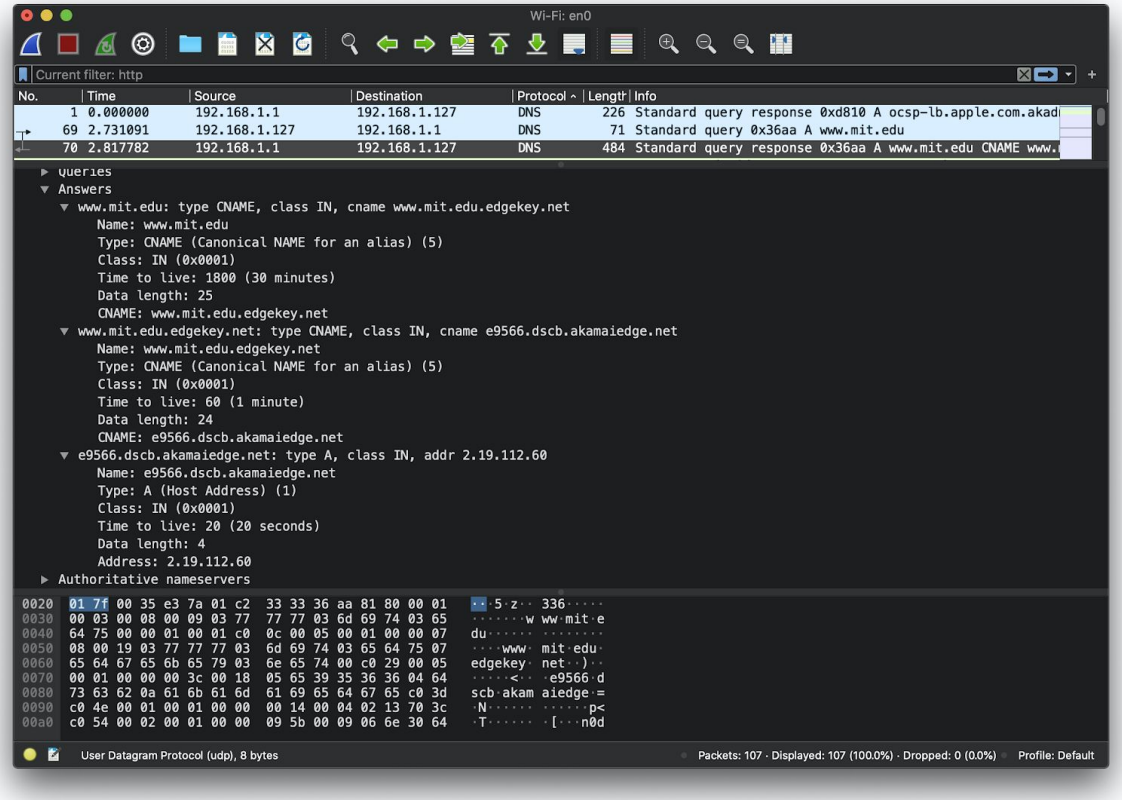

Рис 5. Записи, які були повернуті сервером

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

Destination: 192.168.1.1 – є адресою локального DNS сервера.

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

«відповіді»?

Type NS (Адреса вузла, що відповідає за доменну зону), вміщує посилання на рядок з відповіддю [Response In: 321]

3.13. 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?

Були запропоновані наступні сервери:

ns1-173.akam.net, asia2.akam.net, ns1-37.akam.net, usw2.akam.net, use5.akam.net, asia1.akam.net, use2.akam.net, eur5.akam.net.

Сервери були запропоновані за допомогою доменного імені.

3.14. 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?

Для доменного імені bitsy.mit.edu запит був відправлений на 192.168.1.1 - адресою локального DNS сервера.

Для доменного імені www.aiit.or.kr запит був відправлений на 18.0.72.3. Команда намагалася 3 рази відправити запит, але відповіді від сервера отримано не було.

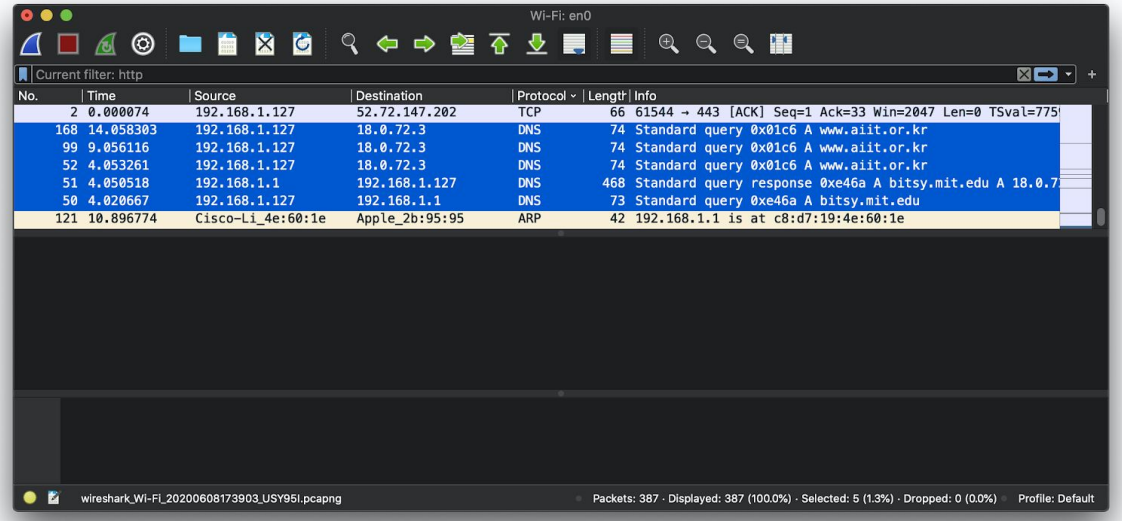

Рис 6. Запити nslookup www.aiit.or.kr та bitsy.mit.edu

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

Для запиту bitsy.mit.edu тип запиту був A (Адресний запис, відповідність між ім'ям і IP-адресою). Запит вміщує посилання на відповідь [Response In: 51]

Для запиту www.aiit.or.kr тип запиту був A (Адресний запис, відповідність між ім'ям і IP-адресою). Запит не вміщує посилання на відповідь.

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

Для запиту bitsy.mit.edu було повернуто один запис типу SOA (вказівка на авторитетність інформації, використовується для вказівки на нову зону) зі значенням mname use2.akam.net.

Для запиту www.aiit.or.kr відповіді отримано не було.