

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»

Виконала: ст. гр. ІС-ЗП93

Ільїнська А.А.

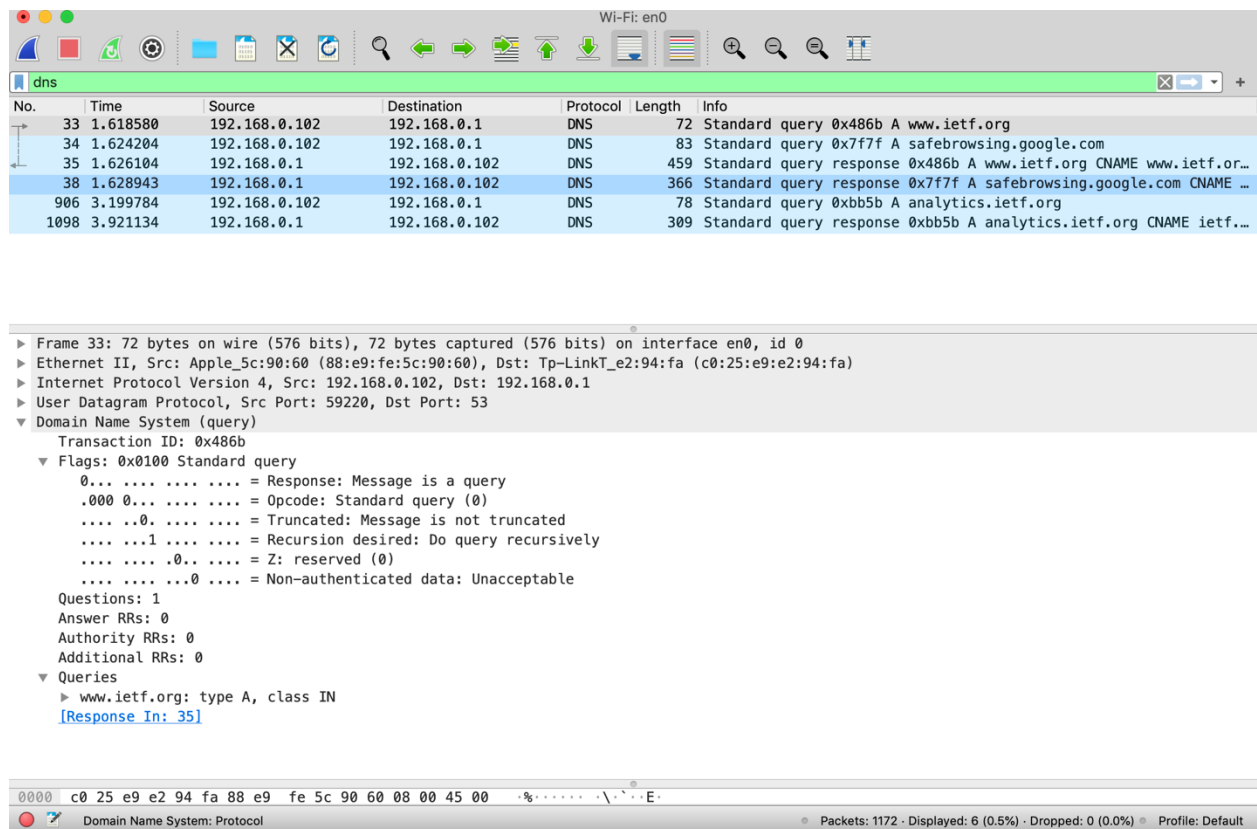
Прийняв: Кухарєв С.О.

Київ – 2020

Лабораторна робота 3

Хід роботи

1. Очистіть кеш DNS-записів:
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.



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

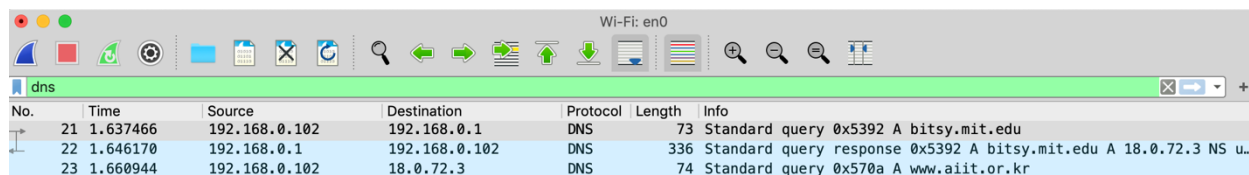
15. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети

16. Почніть захоплення пакетів

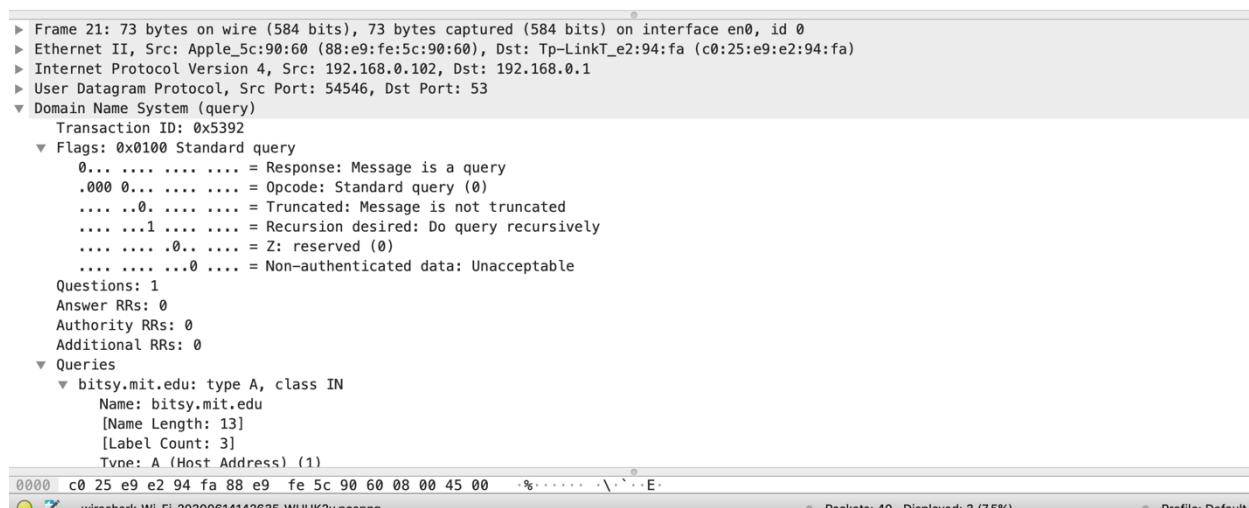
17. Виконайте nslookup для домену www.mit.edu за допомогою команди

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

18. Зупиніть захоплення пакетів.



No.	Time	Source	Destination	Protocol	Length	Info
21	1.637466	192.168.0.102	192.168.0.1	DNS	73	Standard query 0x5392 A bitsy.mit.edu
22	1.646170	192.168.0.1	192.168.0.102	DNS	336	Standard query response 0x5392 A bitsy.mit.edu A 18.0.72.3 NS u...
23	1.660944	192.168.0.102	18.0.72.3	DNS	74	Standard query 0x570a A www.aiit.or.kr



```
► Frame 21: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface en0, id 0
► Ethernet II, Src: Apple_5c:90:60 (88:e9:fe:5c:90:60), Dst: Tp-LinkT_e2:94:fa (c0:25:e9:e2:94:fa)
► Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1
► User Datagram Protocol, Src Port: 54546, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x5392
  ▼ Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    .... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    .... ..0... .. = Z: reserved (0)
    .... ..0... .. = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ bitsy.mit.edu: type A, class IN
      Name: bitsy.mit.edu
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
```

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

20. Приготуйте відповіді на запитання 16, 17. Роздрукуйте необхідні для цього пакети.

21. Закрийте Wireshark

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. 192.168.0.102, Dst:192.168.0.1

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

- Dst:192.168.0.1 – це локальний DNS сервер

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). Має посилання на відповідь. [Response In: 35]

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

- 3 відповіді, кожна 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 зроблений ще один запит

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

- Запит: Src Port: 64742, Dst Port: 53
- Відповідь: Src Port: 53, Dst Port: 64742

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

- Dst: 192.168.0.1 – адреса локального сервера за замовчанням

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: 113]

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

- 4 запита і 4 відповіді, кожна складається з таких значень: Name, Type, Class, Time to live, Data length, CNAME, address

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

- Відповідь: Destination: 192.168.0.1 – це є адреса локального сервера DNS за замовчанням

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

- Відповідь: Це був запит по UDP протоколу, typeA. Запит вміщує посилання на відповідь: [Response in: 7]

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 з відповідями було запропоновано сервером, сервери запропоновані за допомогою доменного імені

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?

- Destination: 192.168.0.1 – це є адреса локального сервера DNS за замовчанням, також був запит на Destination: 18.0.72.3, доменне ім'я www.aiit.or.kr

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

- type A, вміщує посилання на відповідь: [Response In: 22]

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

- 1 відповідь, що вміщує такі дані:
 - Name: bitsy.mit.edu
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 1800 (30 minutes)
 - Data length: 4
 - Address: 18.0.72.3