Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Кафедра математичних методів системного аналізу

ЗВІТ

Про виконання лабораторної роботи №3

з дисципліни «Комп'ютерні мережі»

Виконала:

ст. гр. ІС-зп92

Іконнікова-Скуценя Л.Ю.

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.

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

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.
- Destination Port: 22769
- Source Port: 53

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

- Destination: 172.20.10.1 – адреса локального сервера за замовчуванням

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

- Type: A (Host Address) (1)
- Містить посилання на відповідь. [Response In: 20]

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

- 3 відповіді:

➢ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net

Name: www.ietf.org
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 2252 (37 minutes, 32 seconds)
Data length: 33
CNAME: www.ietf.org.cdn.cloudflare.net

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

Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 377 (6 minutes, 17 seconds)
Data length: 4
Address: 104.20.0.85

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

Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 377 (6 minutes, 17 seconds)
Data length: 4
Address: 104.20.1.85

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, було виконано ще один DNS запит на отримання IP-адреси ресурсу analytics.ietf.org.

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

- Source Port: 51716
- Destination Port: 53

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

- Destination: 172.20.10.1 – адреса локального сервера за замовчуванням

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

- Type: A (Host Address) (1)
- Містить посилання на відповідь: [Response In: 15]

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

- 3 записи з відповідями:

➢ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net

Name: www.mit.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1473 (24 minutes, 33 seconds)
Data length: 25
CNAME: www.mit.edu.edgekey.net

➢ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

Name: www.mit.edu.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 77 (1 minute, 17 seconds)
Data length: 24
CNAME: e9566.dscb.akamaiedge.net

➢ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.141.207

Name: e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 27 (27 seconds)
Data length: 4
Address: 104.96.141.207

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

- Destination: 172.20.10.1 – адреса локального сервера за замовчуванням

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

- Тип запиту: type NS.
- Містить посилання на відповідь: [Response In: 16]

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?

- Запропоновано 8 записів із відповідями.
- Сервери: asia1.akam.net, asia2.akam.net, ns1-173.akam.net, ns1-37.akam.net, usw2.akam.net, use2.akam.net, use5.akam.net, eur5.akam.net
- Сервери запропоновано за допомогою доменного імені.

У запиті **nslookup www.aiit.or.kr bitsy.mit.edu** ми зазначаємо, що запит повинен бути направлений на DNS сервер bitsy.mit.edu замість основного DNS серверу (dns-prime.poly.edu). Таким чином, запит і отримання відповіді відбувається безпосередньо між хостом, який направляє запит і bitsy.mit.edu. DNS сервер bitsy.mit.edu надає IP адресу хосту www.aiit.or.kr (веб-серверу Advanced Institute of Information Technology).[1]
Спроби запиту nslookup www.aiit.or.kr bitsy.mit.edu повертали відповідь, що вичерпано час з'єднання і жоден з серверів неможливо досягти.

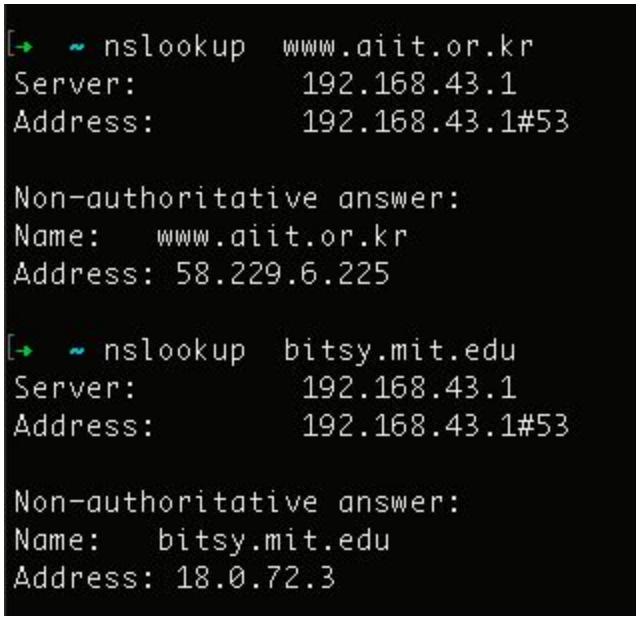
```
→  ~ nslookup  www.aiit.or.kr bitsy.mit.edu
;; connection timed out; no servers could be reached
```

Окремі запити nslookup на доменні імена www.aiit.or.kr та bitsy.mit.edu повертали інформацію про сервер, адресу, доменне ім'я і адресу.

[1] Wireshark Lab: DNS v6.01

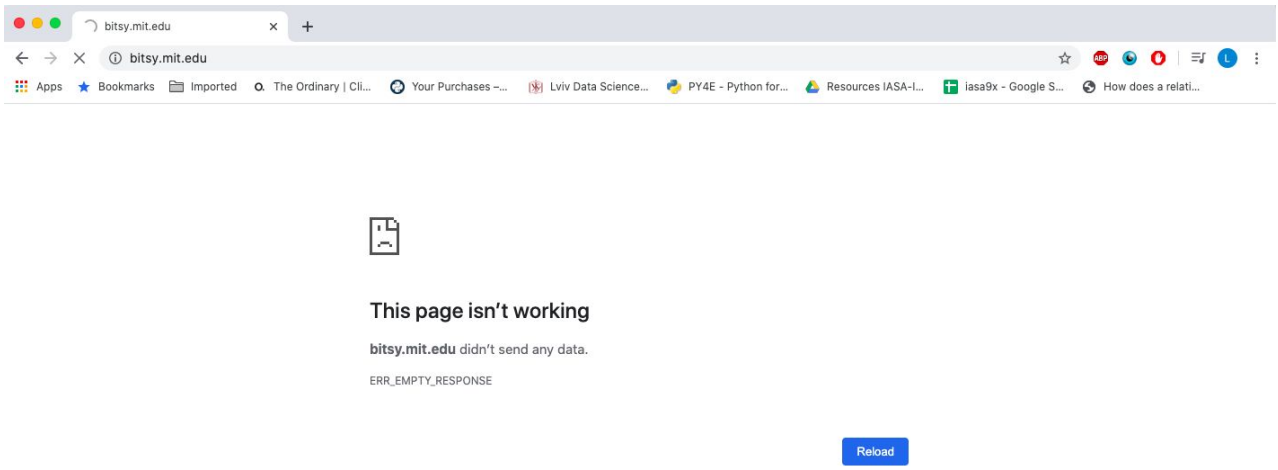
```
➜  ~ nslookup  www.aiit.or.kr
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
Name:   www.aiit.or.kr
Address: 58.229.6.225

➜  ~ nslookup  bitsy.mit.edu
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
Name:   bitsy.mit.edu
Address: 18.0.72.3
```

Окремі запити nslookup та host за отриманими на попередньому кроці адресами повертали відповідь ** server can't find (адреси отримані на попередньому кроці).in-addr.arpa: NXDOMAIN. DNS клієнт отримує тип повідомлення NXDOMAIN (Non-Existent Domain) коли запит на вирішення домену направляється до DNS, але не може бути вирішеним щодо IP адреси. Тобто NXDOMAIN помилка означає, що домен не існує.[2]

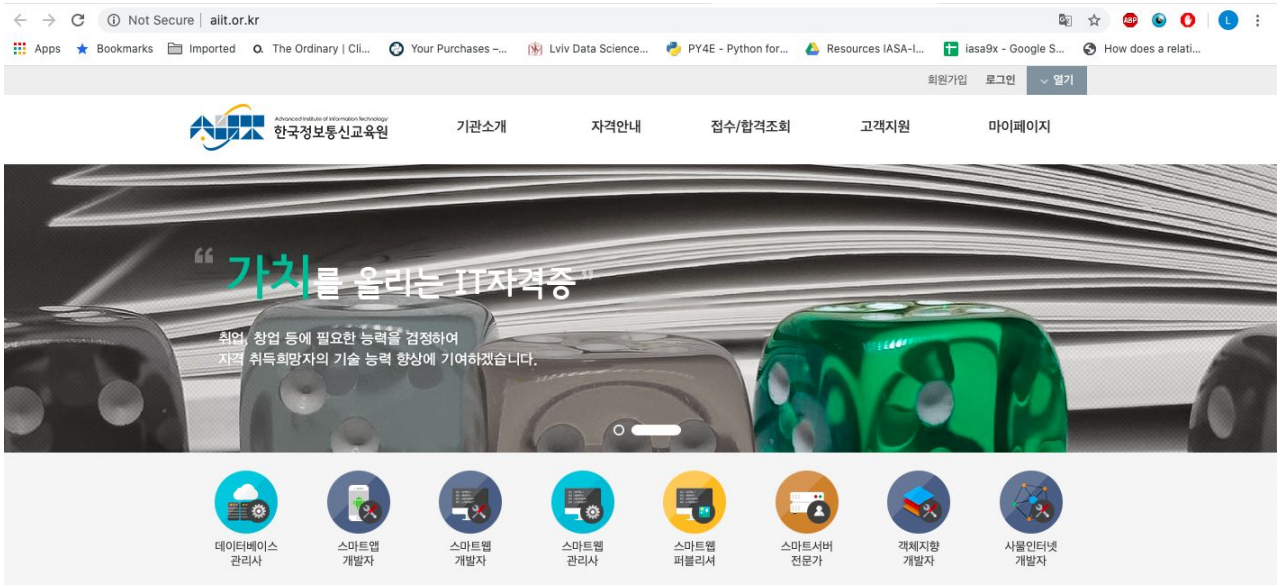


[2] What Is NXDOMAIN?

При переході за посиланням bitsy.mit.edu у браузері, було отримано відповідь bitsy.mit.edu didn’t send any data. ERR_EMPTY_RESPONSE.



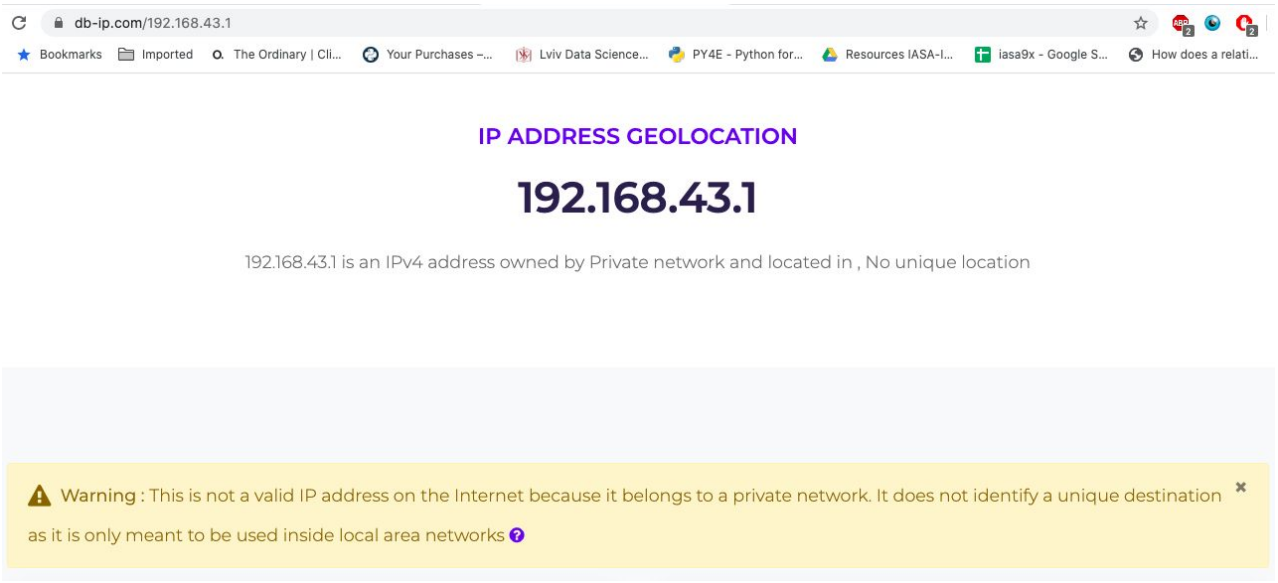
При переході за посиланням www.aiit.or.kr у браузері, сторінка була робочою.



Для отримання відповідей на питання 14-17 було розпочато захоплення пакетів та виконано команду **dig www.aiit.or.kr bitsy.mit.edu**, оскільки запити даної команди містять більше інформації для вирішення помилок пов’язаними з DNS.

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

- Було направлено 2 запити на IP-адресу: 192.168.43.1, ця адреса не є адресою локального сервера DNS за замовчуванням.



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

- Запити мали відповідні типи:
  - ➢ www.aiit.or.kr: type A, class IN, містить посилання на відповідь: [Response In: 4]
  - ➢ bitsy.mit.edu: type A, class IN, містить посилання на відповідь: [Response In: 6]

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

- 2 записи з відповідями:

  - ➢ www.aiit.or.kr: type A, class IN, addr 58.229.6.225
    Name: www.aiit.or.kr
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 2369 (39 minutes, 29 seconds)

Data length: 4
Address: 58.229.6.225

➢ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
Name: bitsy.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 1772 (29 minutes, 32 seconds)
Data length: 4
Address: 18.0.72.3