

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

Вдовенко А.М.

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.

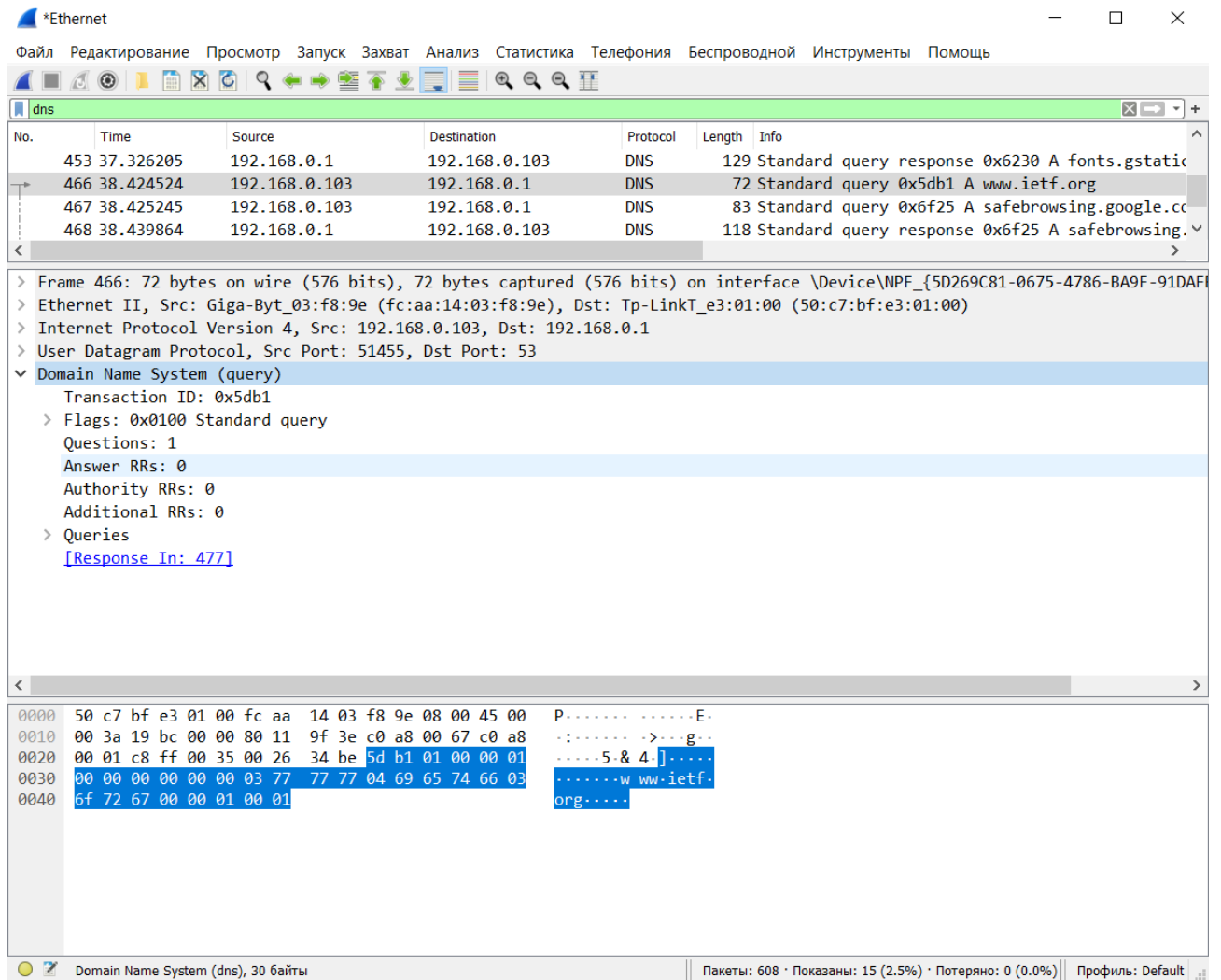


Рис. 1 – Результати запиту

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. 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. Src:192.168.1.248, Dst:192.168.1.1

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

- Dst:192.168.1.1 – це локальний DNS сервер

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

- Має ссилку на відповідь. [Response In: 15]

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;

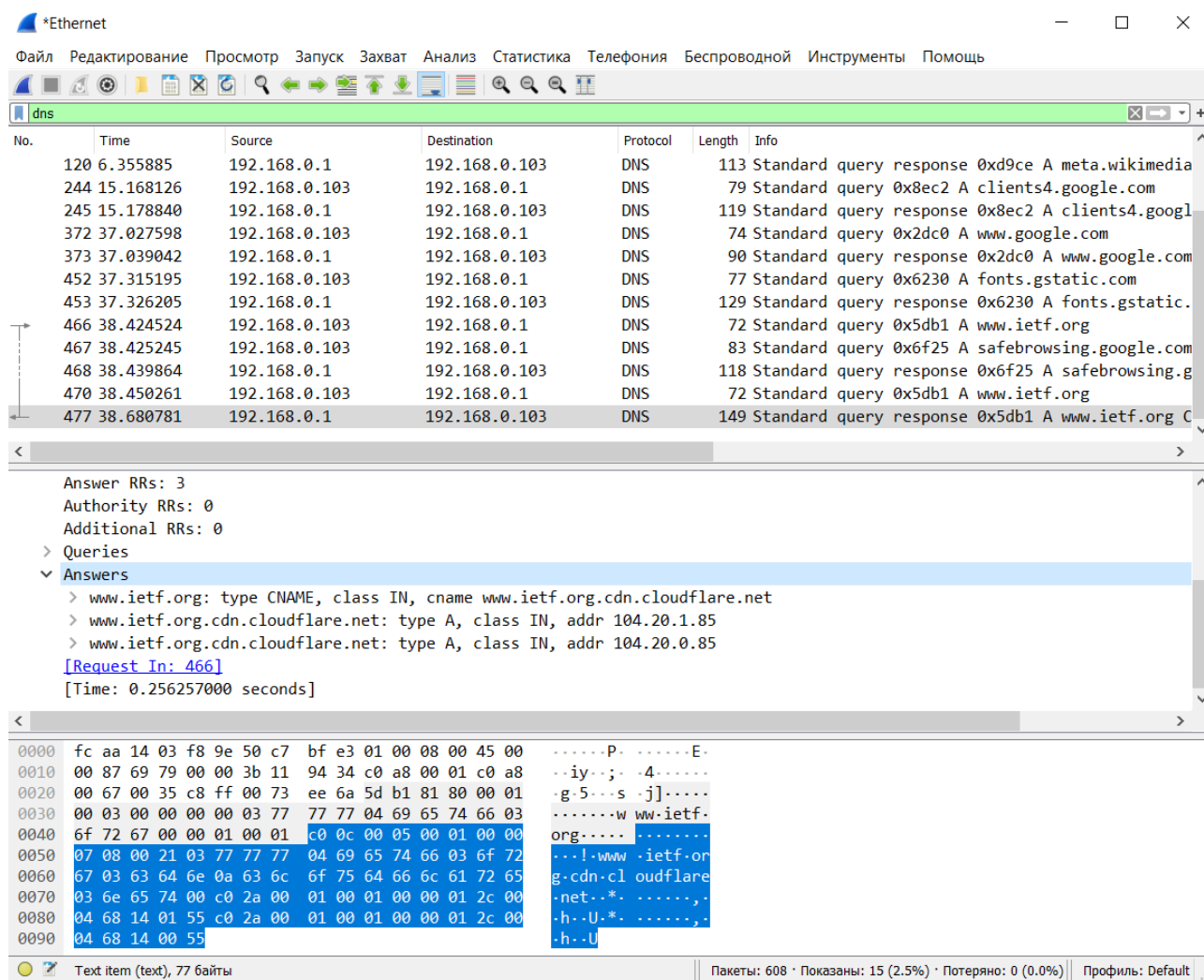


Рис. 2 – DNS Answers

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. В другій відповіді від DNS бачимо Address: 104.20.1.85 і в наступному запиті (рис 3) бачимо саме цю адресу.

477	38.680781	192.168.0.1	192.168.0.103	DNS	149 Standard query response 0x5db1 A www.ietf.org C
478	38.681275	192.168.0.103	104.20.1.85	TCP	66 55121 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146
479	38.710042	104.20.1.85	192.168.0.103	TCP	66 443 → 55121 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
480	38.710093	192.168.0.103	104.20.1.85	TCP	54 55121 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0

> Frame 477: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{5D269C81-0675-4786-BA9F-91D}

> Ethernet II, Src: Tp-LinkT_e3:01:00 (50:c7:bf:e3:01:00), Dst: Giga-Byt_03:f8:9e (fc:aa:14:03:f8:9e)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

> User Datagram Protocol, Src Port: 53, Dst Port: 51455

✓ Domain Name System (response)

Transaction ID: 0x5db1

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

> Queries

✓ Answers

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

✓ 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: 300 (5 minutes)

Data length: 4

Address: 104.20.1.85

Рис. 3 – TCP source address

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

- Так, був виконаний ще один запит

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

- Запит: Source Port: 61748 Destination Port: 53
- Відповідь: Source Port: 53 Destination Port: 61748

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

- Dst: 192.168.1.1 – адреса локального сервера за замовчанням

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

- Запит по UDP протоколу з посиланням на відповідь

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

- 4 записи з відповідями, кожна складається з таких значень:
 - Name: www.mit.edu
 - Type: CNAME (Canonical NAME for an alias) (5)
 - Class: IN (0x0001)
 - Time to live: 1264 (21 minutes, 4 seconds)
 - Data length: 25
 - CNAME: www.mit.edu.edgekey.net

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

- Відповідь: Destination: 192.168.1.1 – це 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»?

- Відповідь: Це був запит по UDP протоколу. Так, цей запит вміщує посилку 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?

- 8 записів з відповідями, сервери запропоновані за допомогою доменного імені

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.1550]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

C:\Users\Eva01>nslookup -type=NS mit.edu
тхЁтхЁ: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-37.akam.net

C:\Users\Eva01>
```

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?

- Запит було відправлено на 18.0.72.3 що не є адресою локального серверу за замовчанням, адреса відповідає доменному імені
 - Name: www.aiit.or.kr

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

Тип запиту А, вміщує посилання на відповідь

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: 1025 (17 minutes, 5 seconds)
 - Data length: 4

○ Address: 18.0.72.3

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
5	2.069370	192.168.1.248	192.168.1.1	DNS	73	Standard query 0xdb02 A bitsy.mit.edu
6	2.073283	192.168.1.1	192.168.1.248	DNS	408	Standard query response 0xdb02 A bitsy.mit.edu A 18.0.72.3 NS f...
7	2.075928	192.168.1.248	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
26	4.081766	192.168.1.248	18.0.72.3	DNS	90	Standard query 0x0002 A www.aiit.or.kr.infopulse.local
29	6.084541	192.168.1.248	18.0.72.3	DNS	90	Standard query 0x0003 AAAA www.aiit.or.kr.infopulse.local
32	8.091568	192.168.1.248	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
33	9.398920	192.168.1.248	192.168.1.1	DNS	110	Standard query 0x7f60 SRV _ldap._tcp.KVSite._sites.dc._msdcs.in...
34	9.401154	192.168.1.1	192.168.1.248	DNS	110	Standard query response 0x7f60 No such name SRV _ldap._tcp.kvsi...
35	9.401806	192.168.1.248	192.168.1.1	DNS	96	Standard query 0xaa6f SRV _ldap._tcp.dc._msdcs.infopulse.local
36	9.403785	192.168.1.1	192.168.1.248	DNS	96	Standard query response 0xaa6f No such name SRV _ldap._tcp.dc._...
37	9.404370	192.168.1.248	192.168.1.1	DNS	138	Standard query 0xde2e SRV _ldap._tcp.396d0204-9d7a-4a06-8b79-b1...
38	9.409840	192.168.1.1	192.168.1.248	DNS	138	Standard query response 0xde2e No such name SRV _ldap._tcp.396d...
39	9.420523	192.168.1.248	192.168.1.1	DNS	83	Standard query 0x1da2 A scm-vn.infopulse.local

Answer RRs: 1
Authority RRs: 13
Additional RRs: 6

Queries

- bitsy.mit.edu: type A, class IN
 - Name: bitsy.mit.edu
 - [Name Length: 13]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

Answers

- 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: 1025 (17 minutes, 5 seconds)
 - Data length: 4
 - Address: 18.0.72.3

Authoritative nameservers

```
0030 00 01 00 0d 00 06 05 62 69 74 73 79 03 6d 69 74 .....b itsy.mit
0040 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 .edu....
0050 00 04 01 00 04 12 00 48 03 c0 16 00 02 00 01 00 .....H .....
0060 02 0f e3 00 13 01 66 0b 65 64 75 2d 73 65 72 76 .....f. edu-serv
0070 65 72 73 03 6e 65 74 00 c0 16 00 02 00 01 00 02 ers.net. ....
0080 0f e3 00 04 01 6c c0 3d c0 16 00 02 00 01 00 02 .....l.= .....
0090 0f e3 00 04 01 62 c0 3d c0 16 00 02 00 01 00 02 .....b.= .....
00a0 0f e3 00 04 01 67 c0 3d c0 16 00 02 00 01 00 02 .....g.= .....
```

Number of additional records in packet (does not add up): 7 bytes

Drop rate: 100% | Discards: 15 (15.0%) | Drops: 0 (0.0%) | Profile: Default