

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: студентка групи ІС-ЗП93

Дударенко Олеся

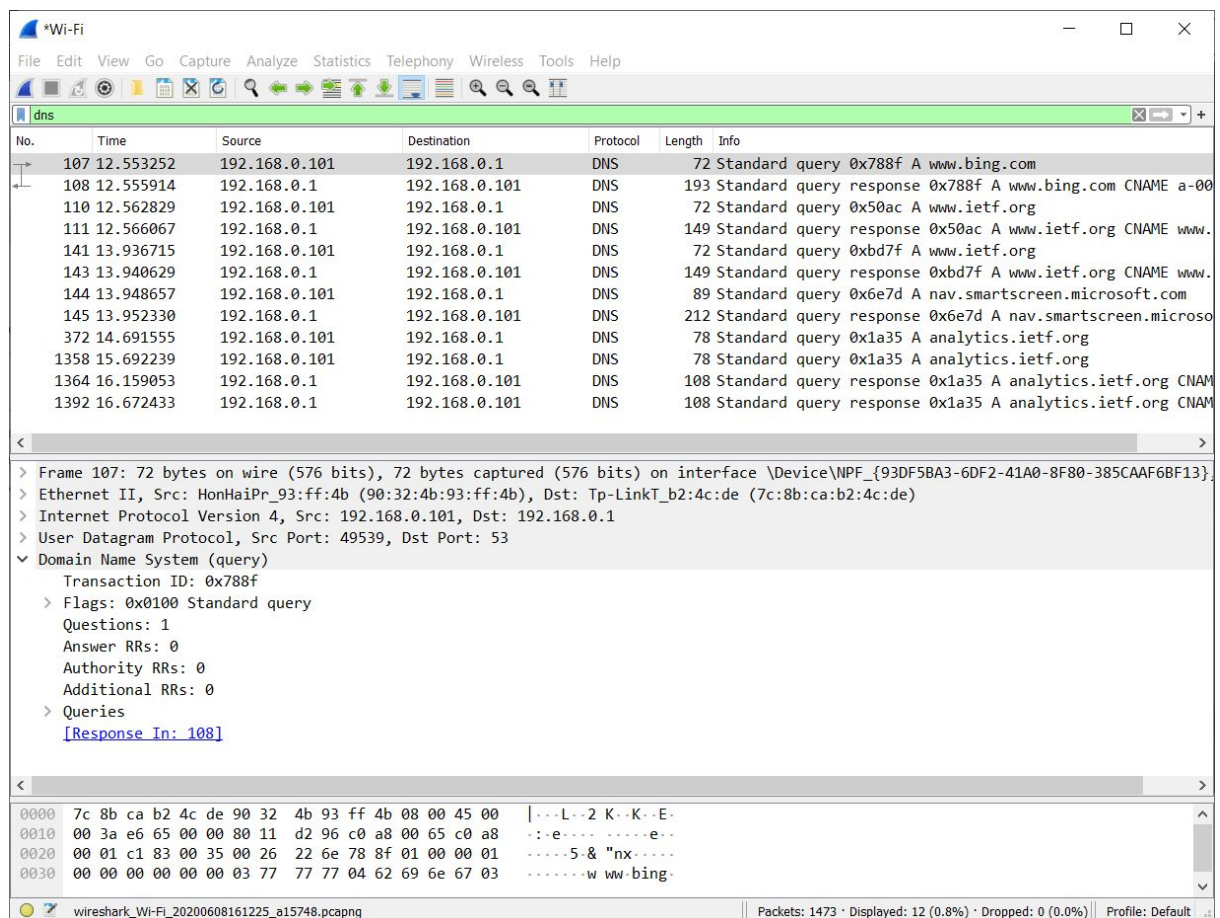
Прийняв: Кухарев С.О.

Київ – 2020

Лабораторна робота 3

1. 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.



Мал.1

8. Почніть захоплення пакетів
9. Виконайте nslookup для домену www.mit.edu за допомогою команди
a. nslookup www.mit.edu

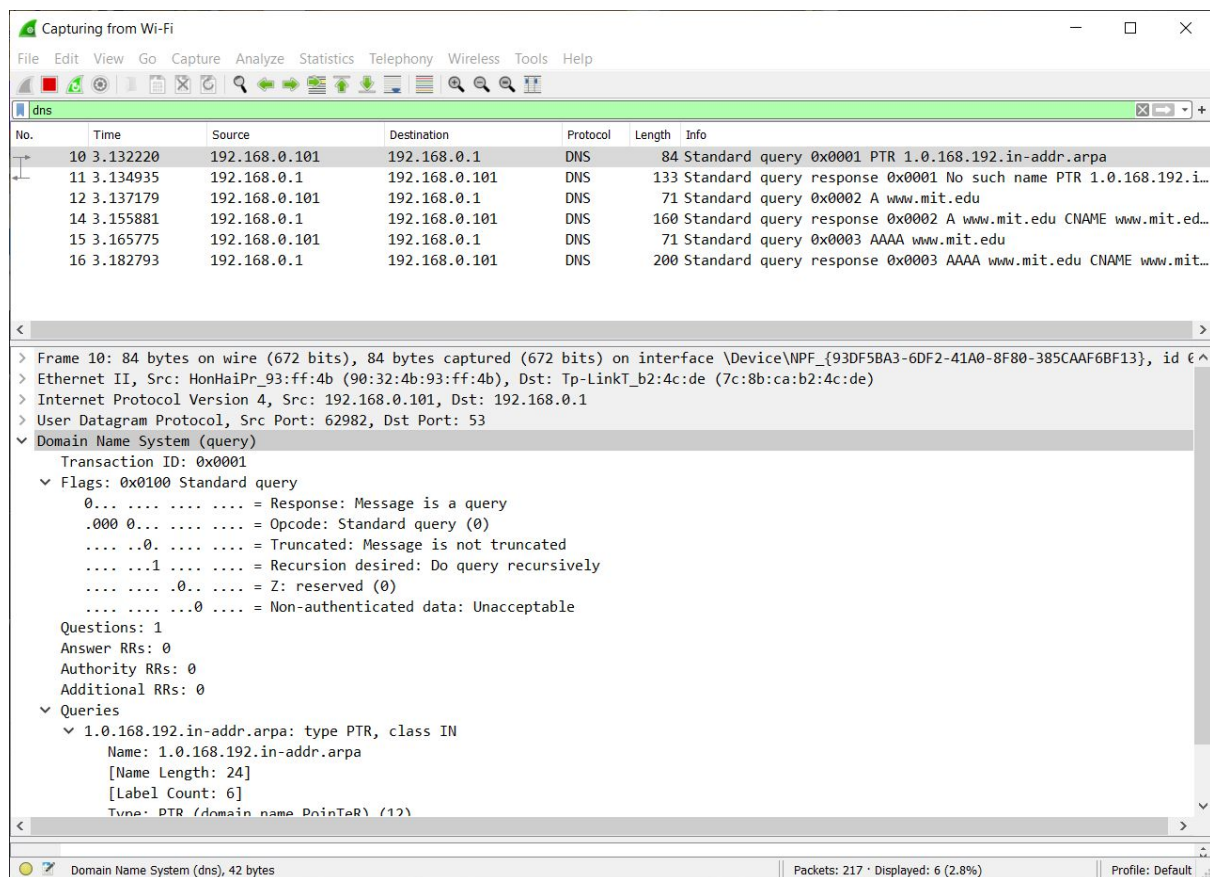
```

Non-authoritative answer:
Name:   e9566.dscb.akamaiedge.net
Addresses:  2a02:26f0:d8:3a2::255e
            2a02:26f0:d8:389::255e
            184.84.235.19
Aliases:  www.mit.edu
            www.mit.edu.edgekey.net

C:\Users\thegr>

```

Мал. 2



Мал. 3

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
 - а. nslookup -type=NS mit.edu

```
Command Prompt

C:\Users\thegr>nslookup www.mit.edu
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d8:3a2::255e
           2a02:26f0:d8:389::255e
           184.84.235.19
Aliases: www.mit.edu
         www.mit.edu.edgekey.net

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

Non-authoritative answer:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = usw2.akam.net

C:\Users\thegr>
```

Мал. 4

dump_after_nslookup -type=NS mit.edu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
44	6.014237	192.168.0.101	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
45	6.018574	192.168.0.1	192.168.0.101	DNS	133	Standard query response 0x0001 No such name PTR 1.0.168.192.i...
46	6.020581	192.168.0.101	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
47	6.055463	192.168.0.1	192.168.0.101	DNS	234	Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS...
49	6.608594	192.168.0.101	192.168.0.1	DNS	75	Standard query 0xbc8a A mail.google.com
50	6.611075	192.168.0.1	192.168.0.101	DNS	118	Standard query response 0xbc8a A mail.google.com CNAME google...

... .. = Authoritative: Server is not an authority for domain
... .. = Truncated: Message is not truncated
... ..1 ... = Recursion desired: Do query recursively
... ..1 ... = Recursion available: Server can do recursive queries
... .. .0.. = Z: reserved (0)
... .. .0. = Answer authenticated: Answer/authority portion was not authenticated by the server
... .. .0 = Non-authenticated data: Unacceptable
... .. .0011 = Reply code: No such name (3)

Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0

Queries

- 1.0.168.192.in-addr.arpa: type PTR, class IN
Name: 1.0.168.192.in-addr.arpa
[Name Length: 24]
[Label Count: 6]
Type: PTR (domain name PoinTeR) (12)
Class: IN (0x0001)

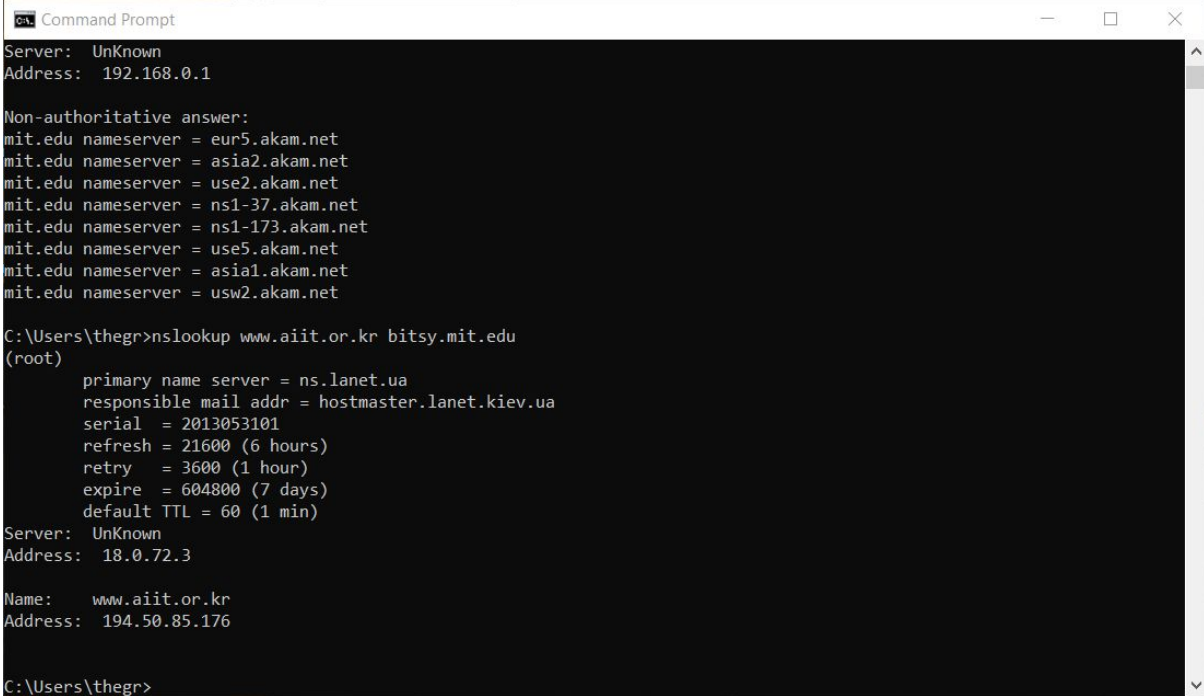
> Authoritative nameservers
[Request In: 44]
[Time: 0.004337000 seconds]

Query Name Len (dns.qry.name.len), 26 bytes

Packets: 112 · Displayed: 6 (5.4%) · Dropped: 0 (0.0%) Profile: Default

Мал. 5

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



```
Command Prompt
Server: UnKnown
Address: 192.168.0.1

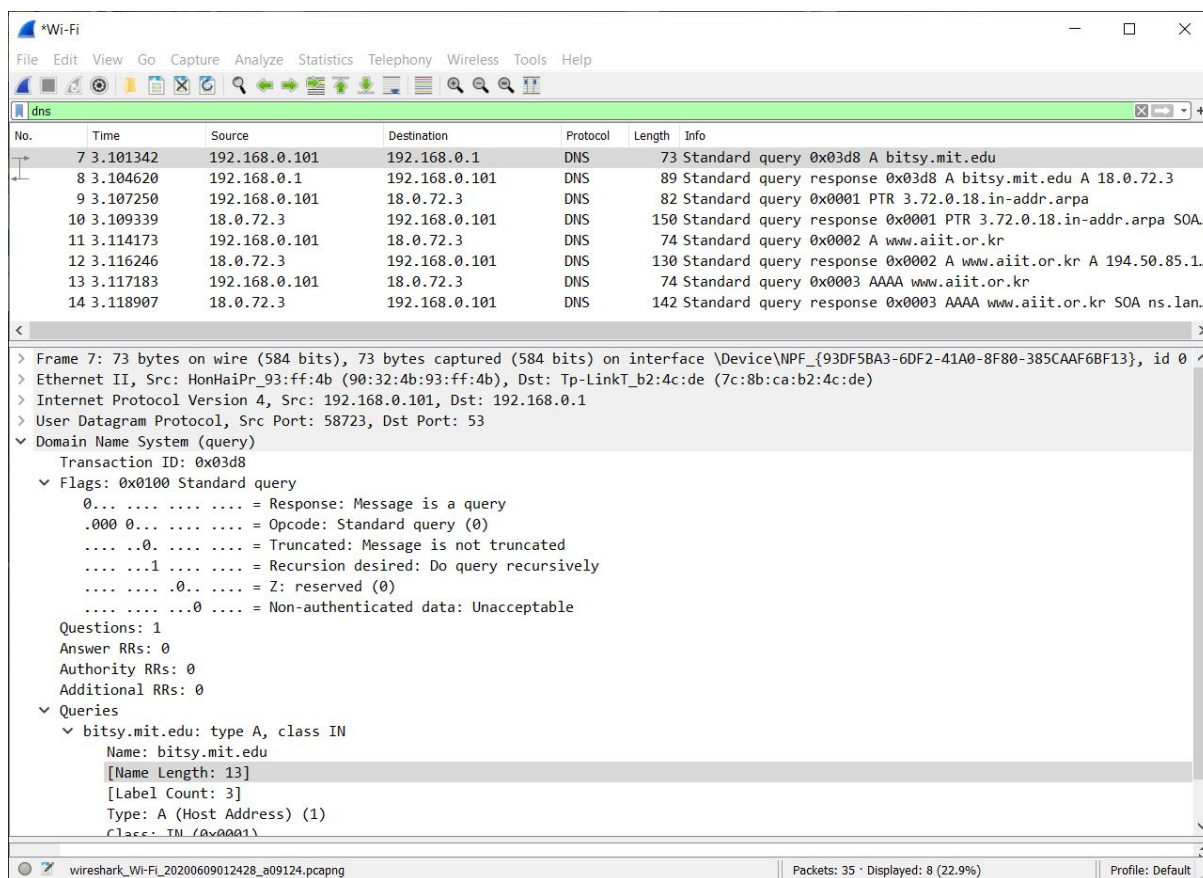
Non-authoritative answer:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = usw2.akam.net

C:\Users\thegr>nslookup www.aiit.or.kr bitsy.mit.edu
(root)
    primary name server = ns.lanet.ua
    responsible mail addr = hostmaster.lanet.kiev.ua
    serial = 2013053101
    refresh = 21600 (6 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 60 (1 min)
Server: UnKnown
Address: 18.0.72.3

Name:    www.aiit.or.kr
Address: 194.50.85.176

C:\Users\thegr>
```

Мал. 6



Мал. 7

18. Зупиніть захоплення пакетів.

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

20. Закрийте Wireshark.

2. 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?

Відповідь: UDP. User Datagram Protocol, Src Port: 49332, Dst Port: 53.

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

Відповідь: Destination: 192.168.0.1. Так.

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

Відповідь: Type A. Містить лінк на рядок з відповіддю [Response In: 1364].

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

Відповідь: Отримано 3 відповіді (Lab3_1clean.pdf)

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: 300 (5 minutes)

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: 148 (2 minutes, 28 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: 148 (2 minutes, 28 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 одною із відповідей сервера DNS?

Відповідь: Так, співпадає.

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

Відповідь: Так, було виконано ще один запит DNS, тобто загалом таких запитів було два.

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

Відповідь: *Src Port: 49626, Dst Port: 53*

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

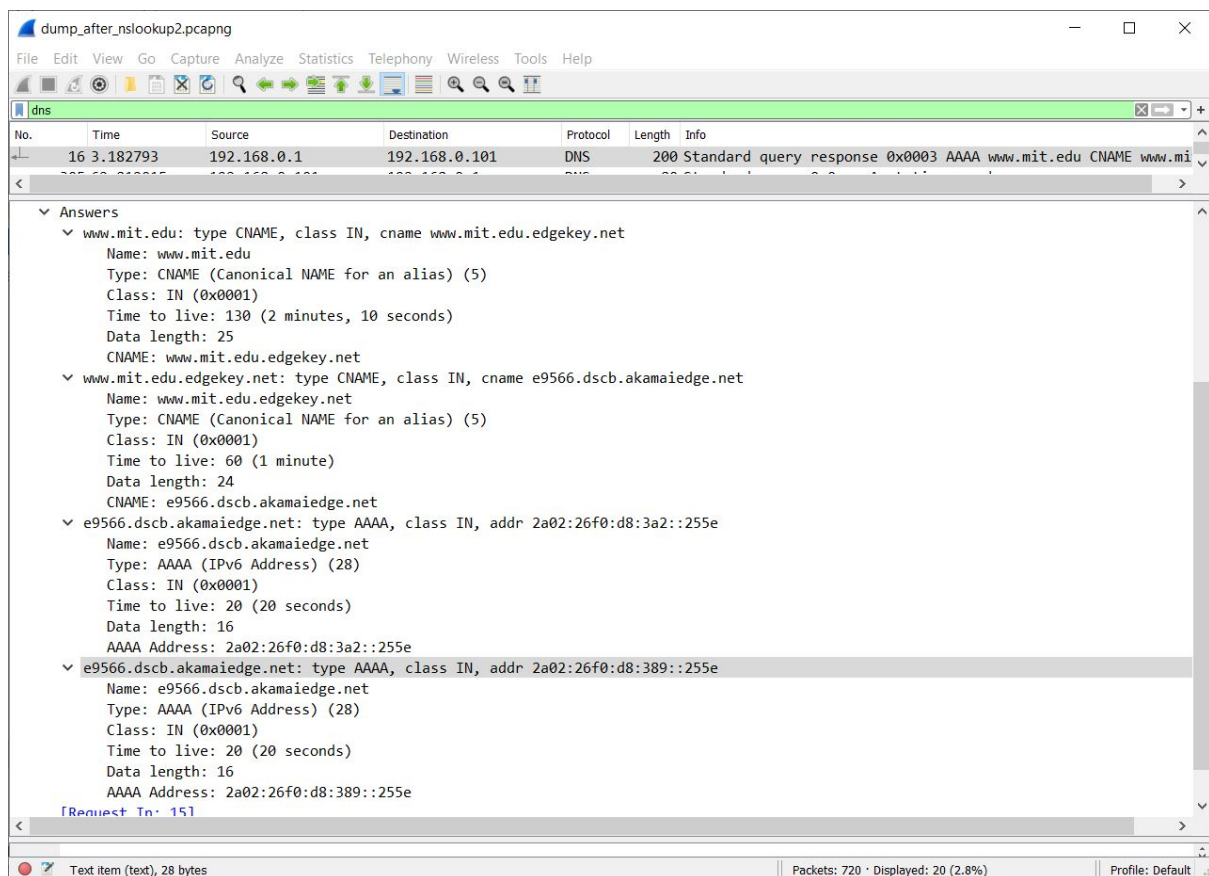
Відповідь: *Dst: 192.168.0.1. Це є адресою локального DNS-серверу.*

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

Відповідь: *Це був запит типу A. Він містить посилання на рядок з відповіддю: [Response In: 14].*

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

Відповідь:

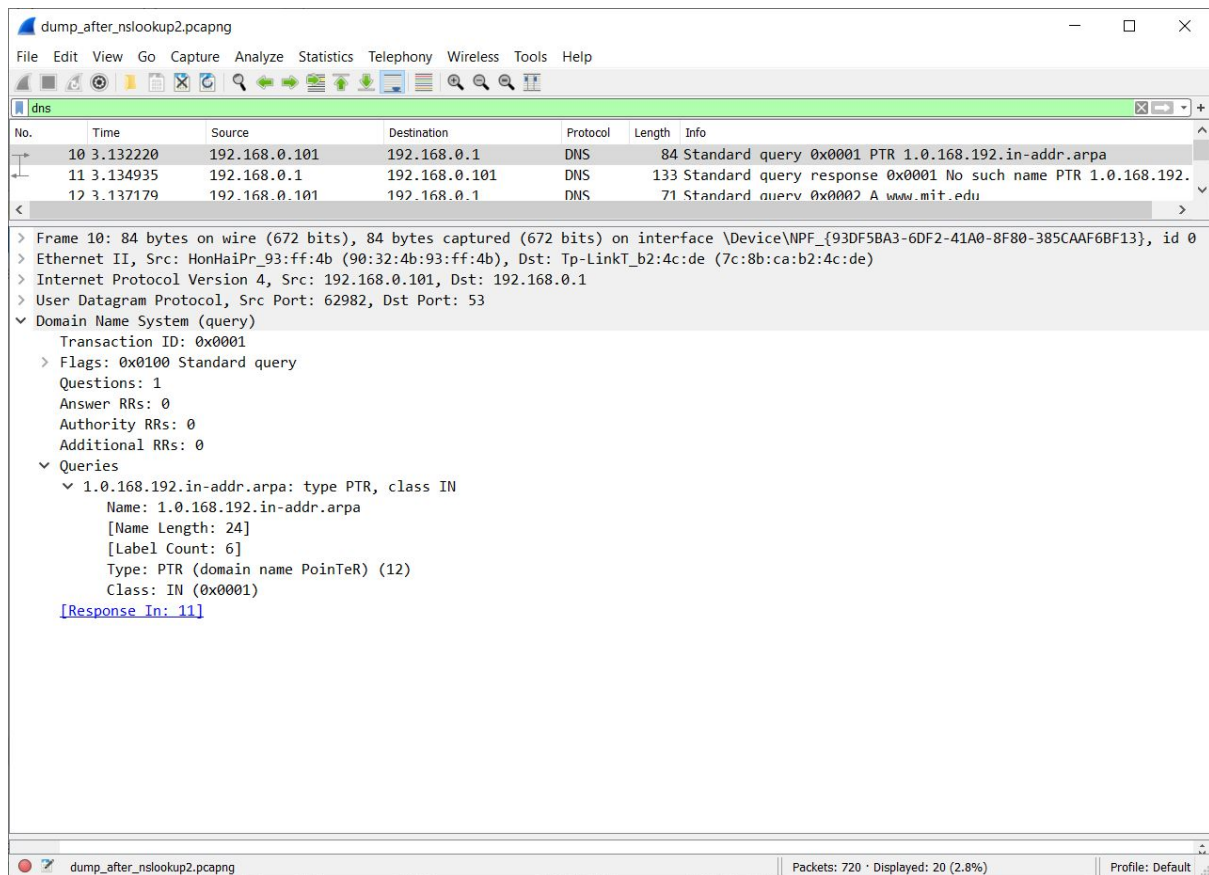


11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Відповідь: *Dst: 192.168.0.1. Це є адресою локального DNS-серверу.*

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

Відповідь:



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?

Відповідь: Було зроблено кілька DNS запитів. Спочатку був запит на *mit.edu*, який повернув 8 відповідей:

dump_after_nslookup -type=NS mit.edu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
44	6.014237	192.168.0.101	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
45	6.018574	192.168.0.1	192.168.0.101	DNS	133	Standard query response 0x0001 No such name PTR 1.0.168.192.i...
46	6.020581	192.168.0.101	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
47	6.055463	192.168.0.1	192.168.0.101	DNS	234	Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS...
49	6.608594	192.168.0.101	192.168.0.1	DNS	75	Standard query 0xbc8a A mail.google.com
50	6.611075	192.168.0.1	192.168.0.101	DNS	118	Standard query response 0xbc8a A mail.google.com CNAME google...

< >

> Frame 47: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{93DF5BA3-6DF2-41A0-8F80-385CAAF6BF13}, id
 > Ethernet II, Src: Tp-LinkT_b2:4c:de (7c:8b:ca:b2:4c:de), Dst: HonHaiPr_93:ff:4b (90:32:4b:93:ff:4b)
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
 > User Datagram Protocol, Src Port: 53, Dst Port: 49429
 > Domain Name System (response)
 Transaction ID: 0x0002
 > Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 8
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > mit.edu: type NS, class IN
 > Answers
 > mit.edu: type NS, class IN, ns eur5.akam.net
 > mit.edu: type NS, class IN, ns asia2.akam.net
 > mit.edu: type NS, class IN, ns use2.akam.net
 > mit.edu: type NS, class IN, ns ns1-37.akam.net
 > mit.edu: type NS, class IN, ns ns1-173.akam.net
 > mit.edu: type NS, class IN, ns use5.akam.net
 > mit.edu: type NS, class IN, ns asia1.akam.net
 > mit.edu: type NS, class IN, ns usw2.akam.net
[\[Request In: 46\]](#)
 [Time: 0.034882000 seconds]

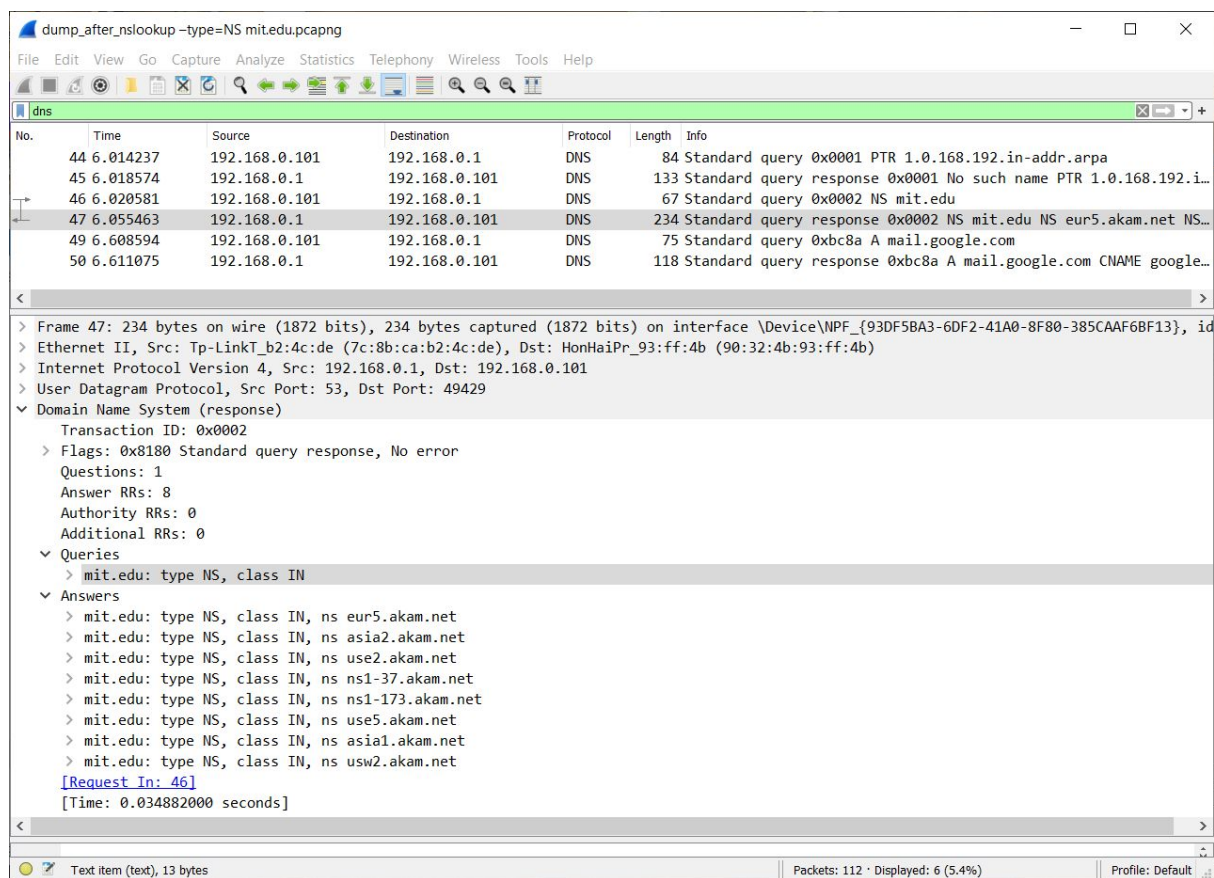
< >

Text item (text), 13 bytes

Packets: 112 · Displayed: 6 (5.4%)

Profile: Default

а потім запит на 1.0.168.192.in-addr.arpa, який повернув query



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?

Відповідь: Було зроблено 4 запиту. Один на 192.168.0.1. Це є адресою локального DNS-серверу. Та 3 запита на адресу 18.0.72.3, що не є локальною адресою. Цій IP-адресі відповідає доменне ім'я *bitsy.mit.edu*.

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

Відповідь: Два запита типу A, один запит типу AAA та один RTP
www.aiit.or.kr: type AAAA, class IN
www.aiit.or.kr: type A, class IN
3.72.0.18.in-addr.arpa: type PTR, class IN
bitsy.mit.edu: type A, class IN

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

Відповідь: Було отримано 4 response, але тільки 2 містять answer PR

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: 300 (5 minutes)
Data length: 4
Address: 18.0.72.3

(no answer)
3.72.0.18.in-addr.arpa: type PTR, class IN
Answer RRs: 0

www.aiit.or.kr: type A, class IN, addr 194.50.85.176
Name: www.aiit.or.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 4
Address: 194.50.85.176

(no answer)
www.aiit.or.kr: type AAAA, class IN
Answer RRs: 0