

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:

студентка групи ІС-зп92

Оратовська А.С.

Прийняв: Кухарєв С.О.

Київ – 2020

Лабораторна робота №3

Хід роботи

1. Очистіть кеш DNS-записів

a. для windows-систем виконайте в терміналі

`ipconfig /flushdns`

b. для linux-систем (можливо) спрацює перезапуск операційної системи;

2. Запустіть веб-браузер, очистіть кеш браузера:

a. для Firefox виконайте

Tools >> Clear Private Data (або Ctrl + Shift + Del)

b. для MS IE виконайте

Tools >> Internet Options >> Delete File

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 а.
`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

a. 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 а.

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. Закрийте Wireshark.

Контрольні питання:

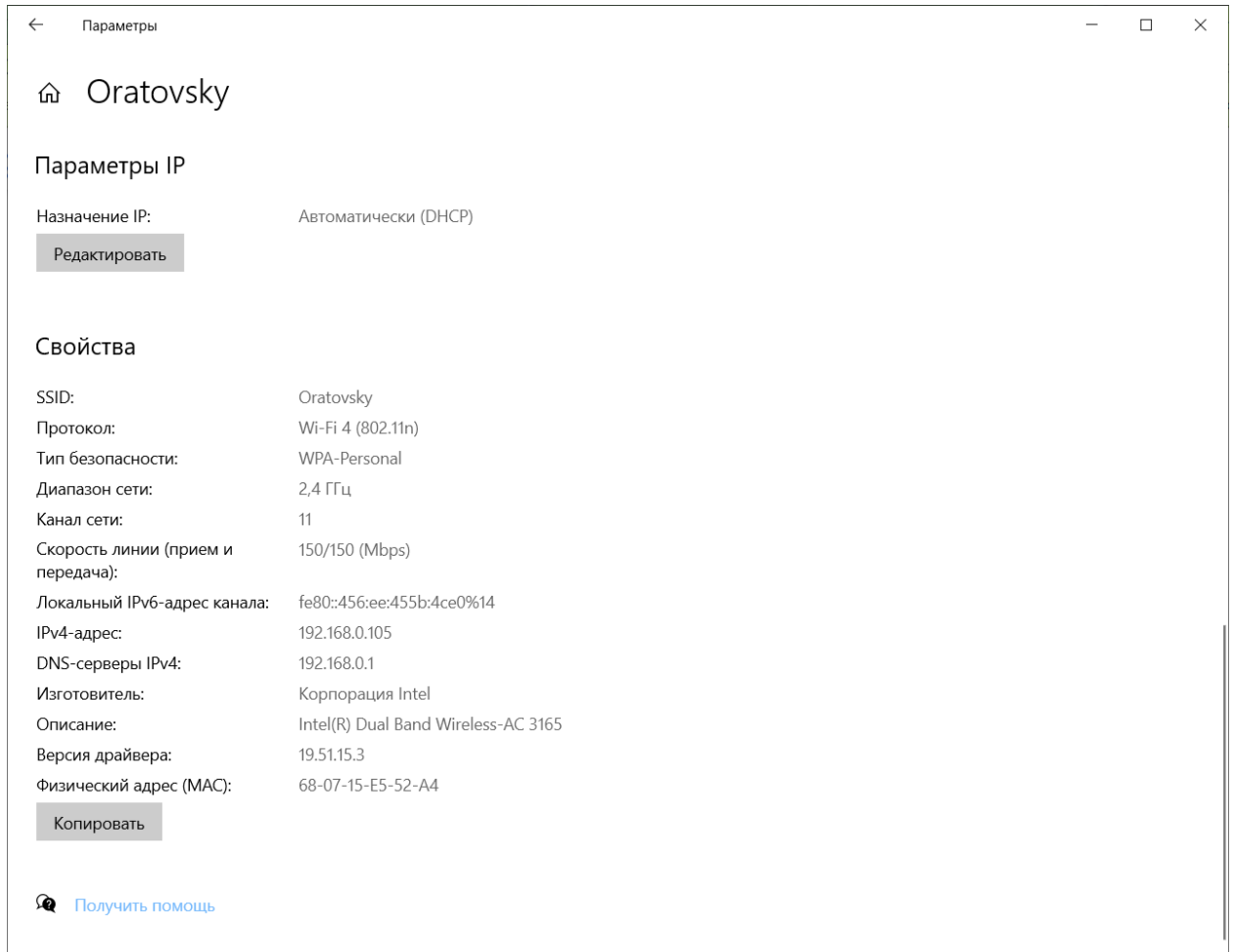
3.1 Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

Відповідь: DNS використовує протокол UDP

User Datagram Protocol, Src Port: 60584, Dst Port: 53

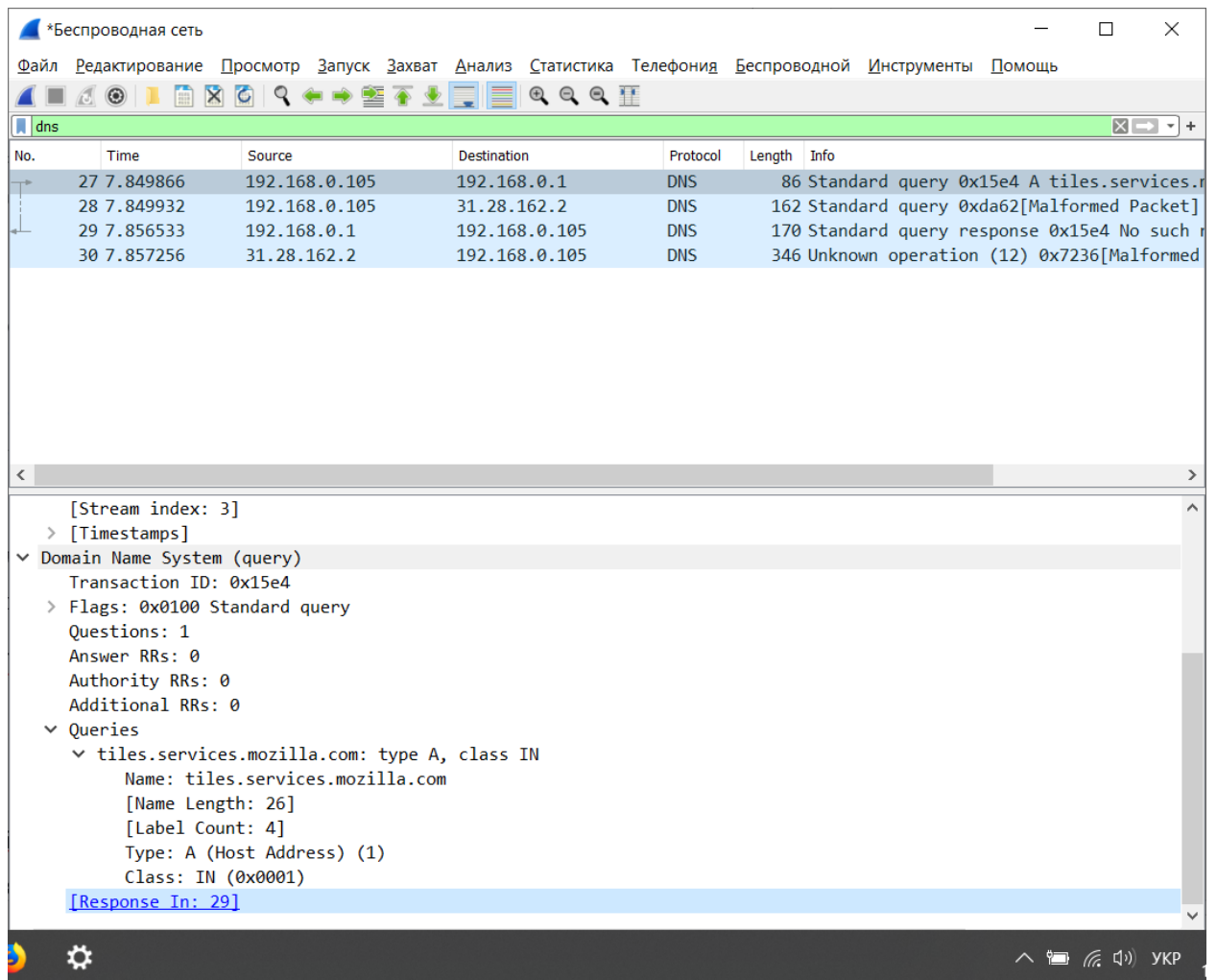
3.2 На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?

Відповідь: 192.168.0.1.Так



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

Відповідь: Type: A (Host Address) (1), містить відповідь [Response In: 39]



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

Відповідь: 3 відповіді:

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

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

Структура відповіді (www.ietf.org):

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

Name: www.ietf.org

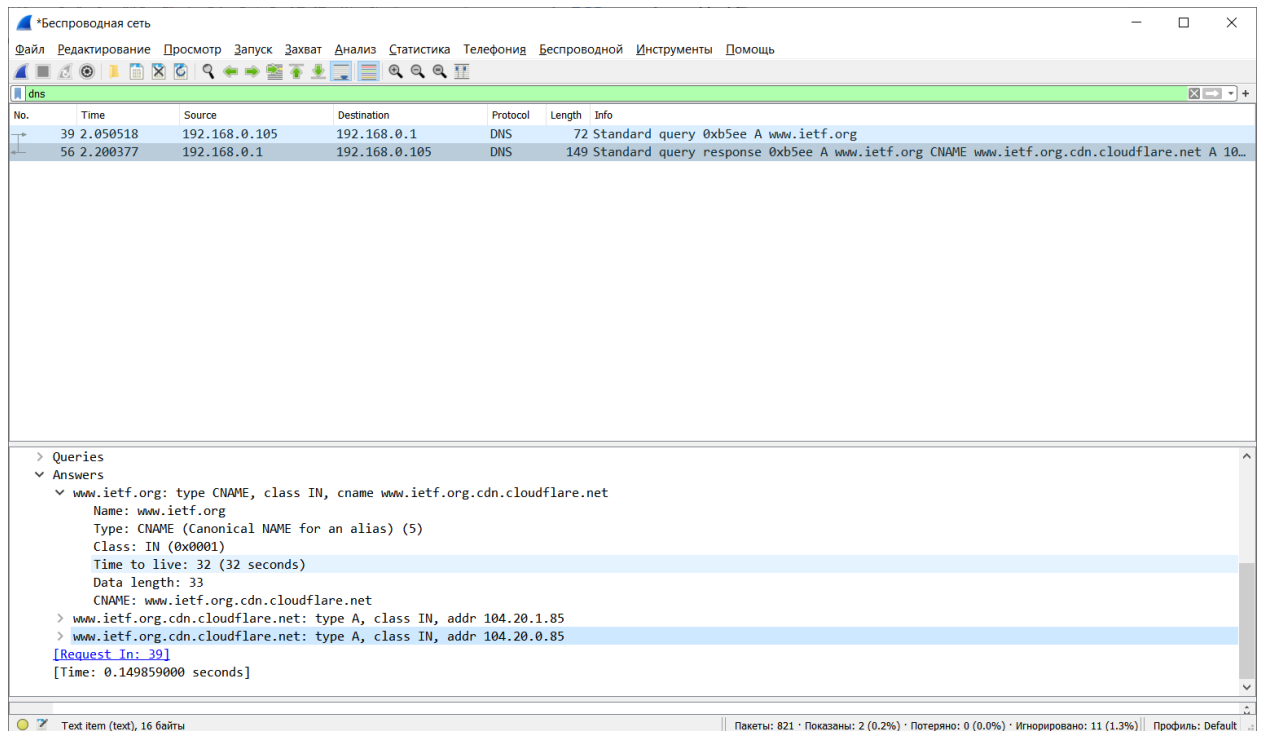
Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 32 (32 seconds)

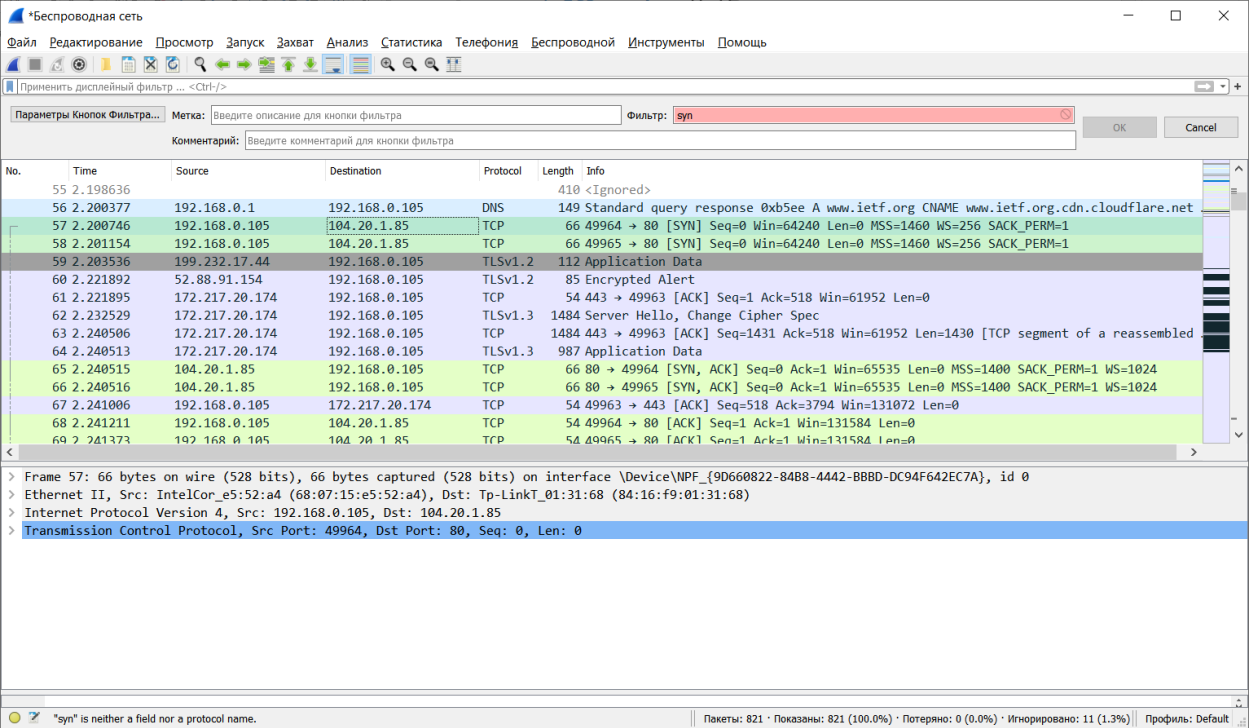
Data length: 33

CNAME: www.ietf.org.cdn.cloudflare.net



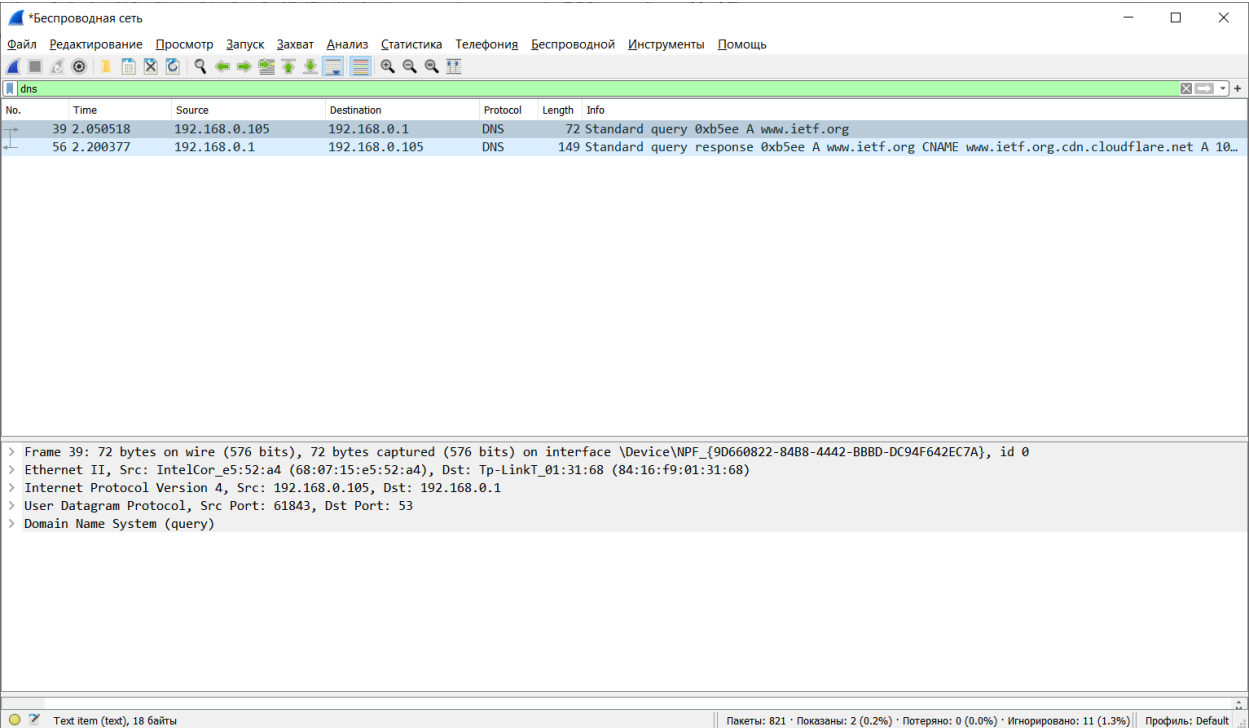
3.5 Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

Відповідь: Так



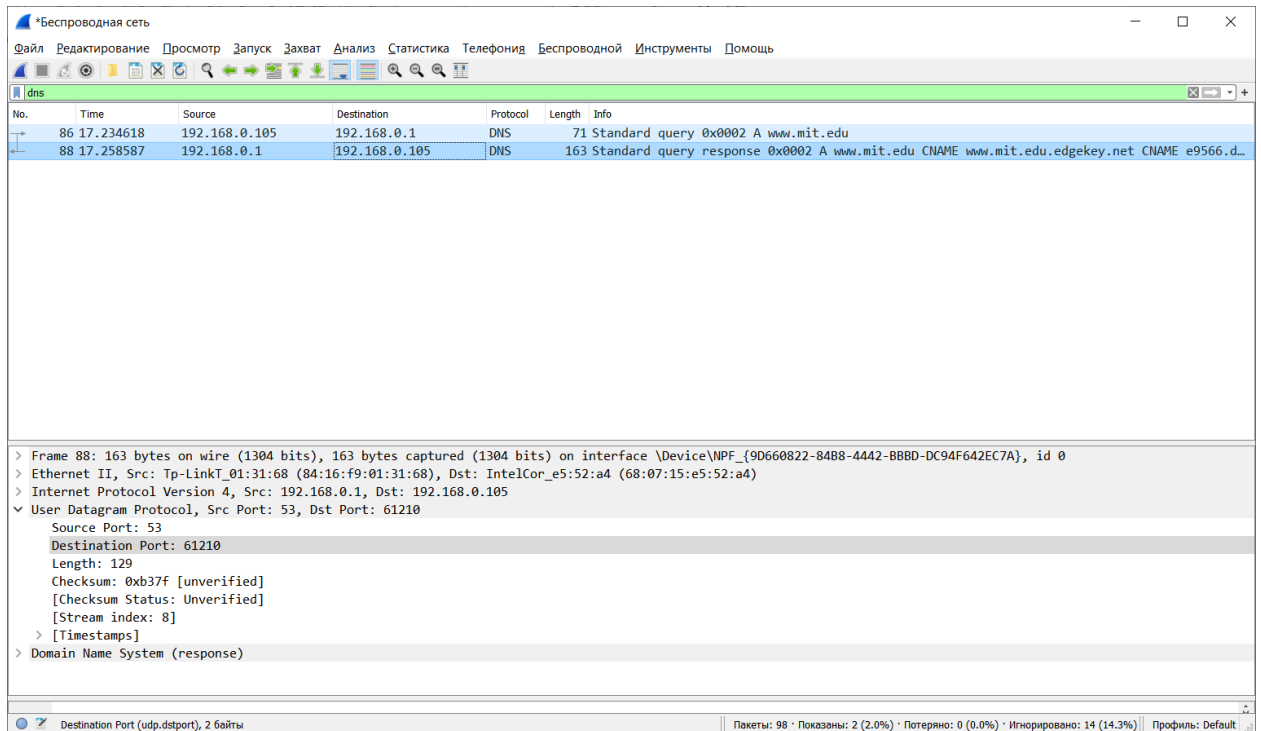
3.6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?

Відповідь: Ні



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

Відповідь: Source Port: 53, Destination Port: 61210



3.8. 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. Так, є.

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

Відповідь: Type: A (Host Address) (1), [Response In: 88]

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

Відповідь: 3

1. 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: 1711 (28 minutes, 31 seconds)
Data length: 25
CNAME: www.mit.edu.edgekey.net
2. 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: 60 (1 minute)
Data length: 27
CNAME: e9566.dscb.akamaiedge.net
3. e9566.dscb.akamaiedge.net: type A, class IN, addr 104.108.58.176
Name: e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 20 (20 seconds)
Data length: 4
Address: 104.108.58.176

3.11. 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. Так, є.

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

Відповідь: Type: NS (authoritative Name Server) (2). [Response In: 32]

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?

Відповідь: 8. Сервери були запропоновані за допомогою доменного імені:

mit.edu: type NS, class IN, ns asia2.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 eur5.akam.net

mit.edu: type NS, class IN, ns usw2.akam.net

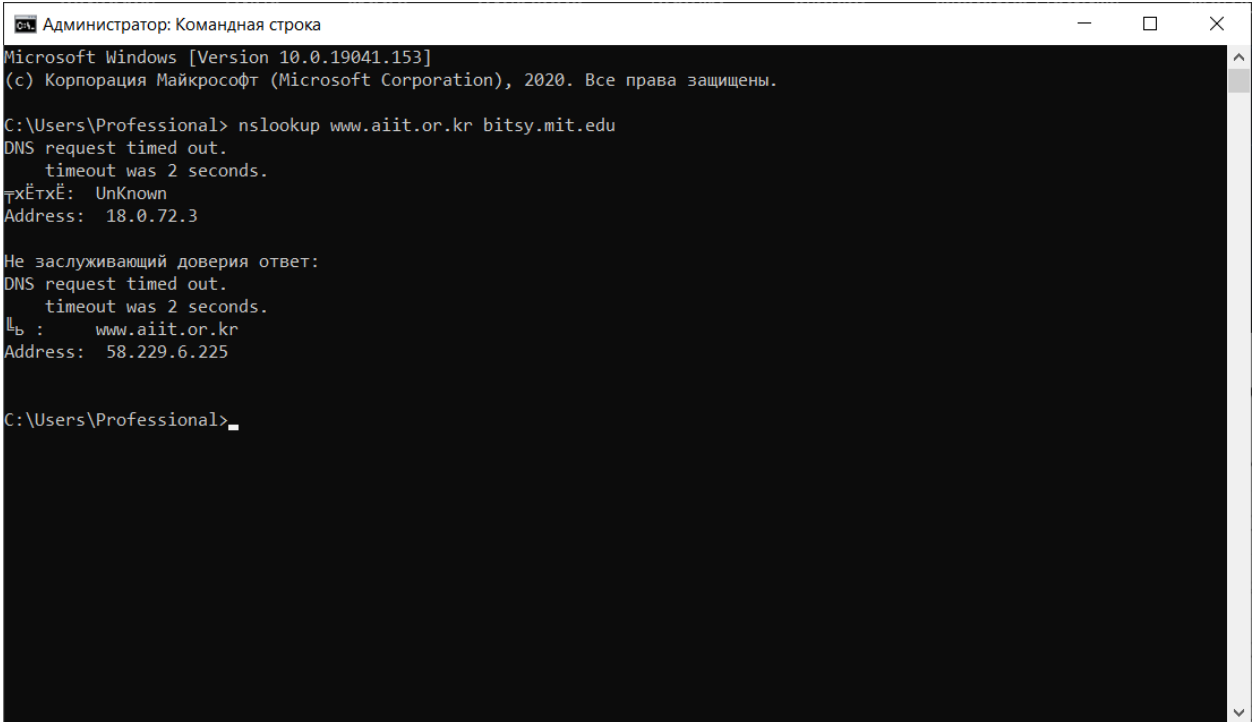
mit.edu: type NS, class IN, ns asia1.akam.net

mit.edu: type NS, class IN, ns use2.akam.net

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?

Відповідь: nslookup (англ. name server lookup пошук на сервері імен) — утиліта, що надає користувачеві інтерфейс командного рядка для звернення до системи DNS та дозволяє задавати різні типи запитів і запрошувати довільно вказані сервери. В запиті в запиті nslookup www.aiit.or.kr

bitsy.mit.edu ми вказуємо, що хочемо відправити запит не на локальний DNS-сервер, а на bitsy.mit.edu, який в свою чергу повинен нам надати IP-адресу www.aiit.or.kr. Проте bitsy.mit.edu наразі не відповідає, тому при зверненні видається помилка «DNS request timed out».



```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19041.153]
(c) Корпорация Майкрософт (Microsoft Corporation), 2020. Все права защищены.

C:\Users\Professional> nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:      UnKnown
Address:     18.0.72.3

Не заслуживающий доверия ответ:
DNS request timed out.
    timeout was 2 seconds.
Server:      www.aiit.or.kr
Address:     58.229.6.225

C:\Users\Professional>
```

Частковим вирішенням питання можна вважати запит через dns.google
nslookup www.aiit.or.kr 8.8.8.8

```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19041.153]
(c) Корпорация Майкрософт (Microsoft Corporation), 2020. Все права защищены.

C:\Users\Professional> nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 18.0.72.3

Не заслуживающий доверия ответ:
DNS request timed out.
    timeout was 2 seconds.
Server: www.aiit.or.kr
Address: 58.229.6.225

C:\Users\Professional> nslookup www.aiit.or.kr 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Не заслуживающий доверия ответ:
Server: www.aiit.or.kr
Address: 58.229.6.225

C:\Users\Professional>
```

Тож, запит був відправлений на IP-адресу 8.8.8.8, що відповідає доменному імені Google.

*Беспроводная сеть						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
dns						
No.	Time	Source	Destination	Protocol	Length	Info
7	4.189518	192.168.0.105	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
8	4.189575	192.168.0.105	31.28.162.2	DNS	156	Standard query 0xda62[Malformed Packet]
9	4.198497	31.28.162.2	192.168.0.105	DNS	282	Unknown operation (12) 0x7236[Malformed Packet]
10	4.205861	8.8.8.8	192.168.0.105	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa
11	4.208890	192.168.0.105	8.8.8.8	DNS	74	Standard query 0x0002 A www.aiit.or.kr
12	4.208953	192.168.0.105	31.28.162.2	DNS	150	Standard query 0xda62[Malformed Packet]
13	4.211277	31.28.162.2	192.168.0.105	DNS	410	Unknown operation (12) 0x7236[Malformed Packet]
14	4.215609	192.168.0.105	8.8.8.8	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
15	4.215674	192.168.0.105	31.28.162.2	DNS	150	Standard query 0xda62[Malformed Packet]
16	4.217825	31.28.162.2	192.168.0.105	DNS	282	Unknown operation (12) 0x7236[Malformed Packet]
17	4.509896	8.8.8.8	192.168.0.105	DNS	90	Standard query response 0x0002 A www.aiit.or.kr
18	4.817736	8.8.8.8	192.168.0.105	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr

Source Port: 59365
Destination Port: 53
Length: 46
Checksum: 0x2d28 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
> [Timestamps]

Domain Name System (query)
Transaction ID: 0x0001
> Flags: 0x0100 Standard query

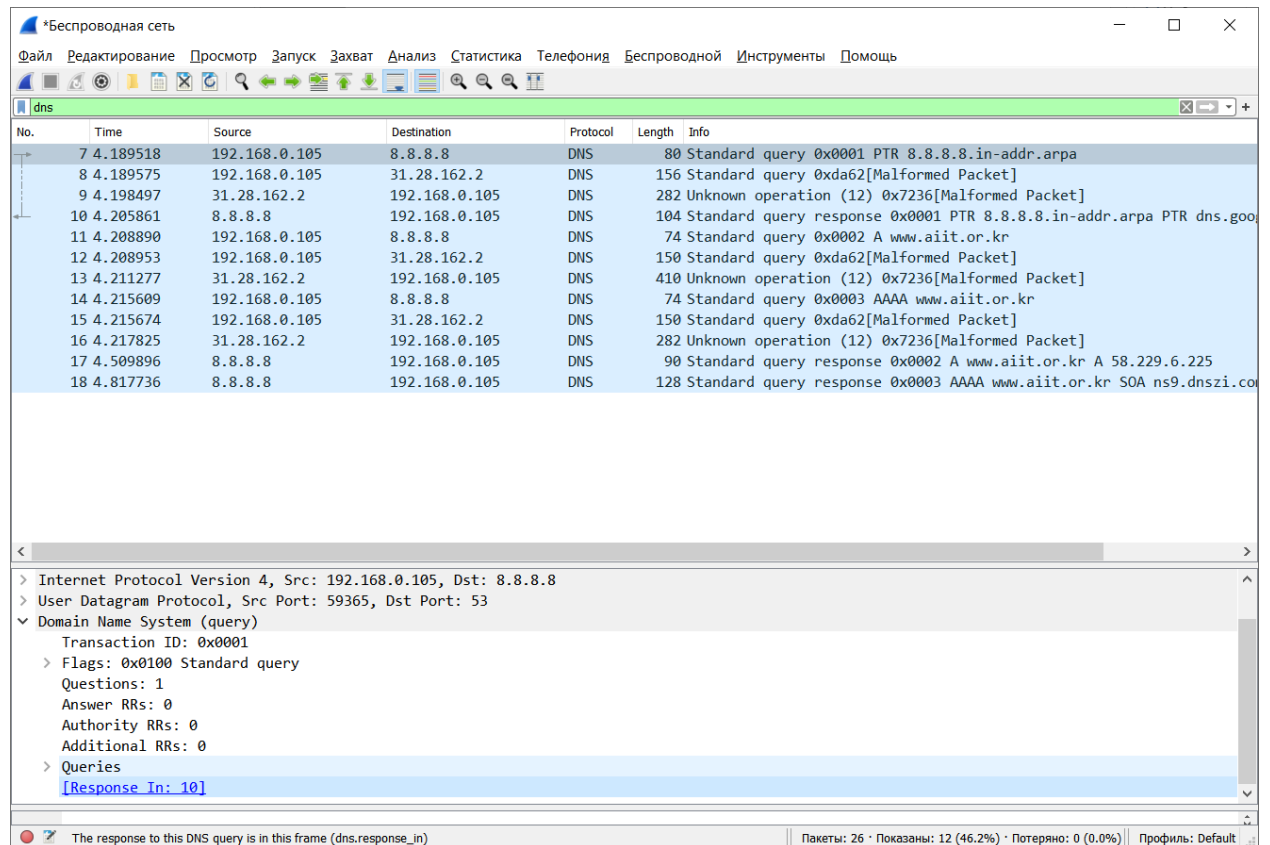
wireshark_Беспроводная сеть_20200612203317_a10096.pcapng | Пакеты: 26 · Показаны: 12 (46.2%) | Профиль: Default

3.15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит?

Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Відповідь: Type: PTR (domain name PoinTeR) (12)

[Response In: 10]



The screenshot shows the Wireshark interface with a packet list table and a detailed view of a DNS query.

No.	Time	Source	Destination	Protocol	Length	Info
7	4.189518	192.168.0.105	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
8	4.189575	192.168.0.105	31.28.162.2	DNS	156	Standard query 0xda62[Malformed Packet]
9	4.198497	31.28.162.2	192.168.0.105	DNS	282	Unknown operation (12) 0x7236[Malformed Packet]
10	4.205861	8.8.8.8	192.168.0.105	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
11	4.208890	192.168.0.105	8.8.8.8	DNS	74	Standard query 0x0002 A www.aiit.or.kr
12	4.208953	192.168.0.105	31.28.162.2	DNS	150	Standard query 0xda62[Malformed Packet]
13	4.211277	31.28.162.2	192.168.0.105	DNS	410	Unknown operation (12) 0x7236[Malformed Packet]
14	4.215609	192.168.0.105	8.8.8.8	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
15	4.215674	192.168.0.105	31.28.162.2	DNS	150	Standard query 0xda62[Malformed Packet]
16	4.217825	31.28.162.2	192.168.0.105	DNS	282	Unknown operation (12) 0x7236[Malformed Packet]
17	4.509896	8.8.8.8	192.168.0.105	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
18	4.817736	8.8.8.8	192.168.0.105	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.co

The detailed view shows the selected packet (No. 10) as a DNS query:

- Internet Protocol Version 4, Src: 192.168.0.105, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 59365, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0x0001
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - [Response In: 10]

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

Відповідь: 1. 8.8.8.8.in-addr.arpa: type PTR, class IN, dns.google, складається з:

Name: 8.8.8.8.in-addr.arpa

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

Time to live: 20925 (5 hours, 48 minutes, 45 seconds)

Data length: 12

Domain Name: dns.google

*Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
7	4.189518	192.168.0.105	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
8	4.189575	192.168.0.105	31.28.162.2	DNS	156	Standard query 0xda62[Malformed Packet]
9	4.198497	31.28.162.2	192.168.0.105	DNS	282	Unknown operation (12) 0x7236[Malformed Packet]
10	4.205861	8.8.8.8	192.168.0.105	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
11	4.208890	192.168.0.105	8.8.8.8	DNS	74	Standard query 0x0002 A www.aiit.or.kr
12	4.208953	192.168.0.105	31.28.162.2	DNS	150	Standard query 0xda62[Malformed Packet]
13	4.211277	31.28.162.2	192.168.0.105	DNS	410	Unknown operation (12) 0x7236[Malformed Packet]
14	4.215609	192.168.0.105	8.8.8.8	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
15	4.215674	192.168.0.105	31.28.162.2	DNS	150	Standard query 0xda62[Malformed Packet]
16	4.217825	31.28.162.2	192.168.0.105	DNS	282	Unknown operation (12) 0x7236[Malformed Packet]
17	4.509896	8.8.8.8	192.168.0.105	DNS	90	Standard query response 0x0002 A www.aiit.or.kr A 58.229.6.225
18	4.817736	8.8.8.8	192.168.0.105	DNS	128	Standard query response 0x0003 AAAA www.aiit.or.kr SOA ns9.dnszi.com

> Queries

▼ Answers

8.8.8.8.in-addr.arpa: type PTR, class IN, dns.google

Name: 8.8.8.8.in-addr.arpa

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

Time to live: 20925 (5 hours, 48 minutes, 45 seconds)

Data length: 12

Domain Name: dns.google

[Request In: 7]

[Time: 0.016343000 seconds]

Text item (text), 24 байты

Пакеты: 26 · Показаны: 12 (46.2%) · Потеряно: 0 (0.0%)

Профиль: Default