

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: студент групи ІС-ЗП93
Гавриленко Олександр

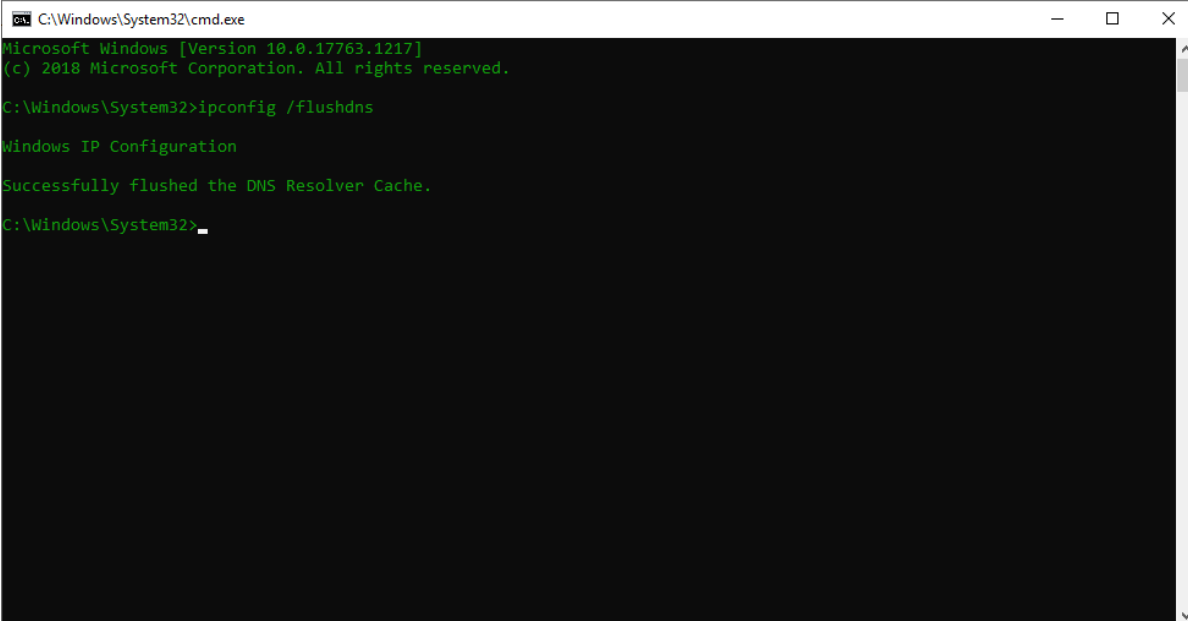
Прийняв: Кухарєв С.О.

Київ – 2020

Лабораторна робота 3

1. Хід роботи

1. Очистіть кеш DNS-записів:



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.1217]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\System32>ipconfig /flushdns

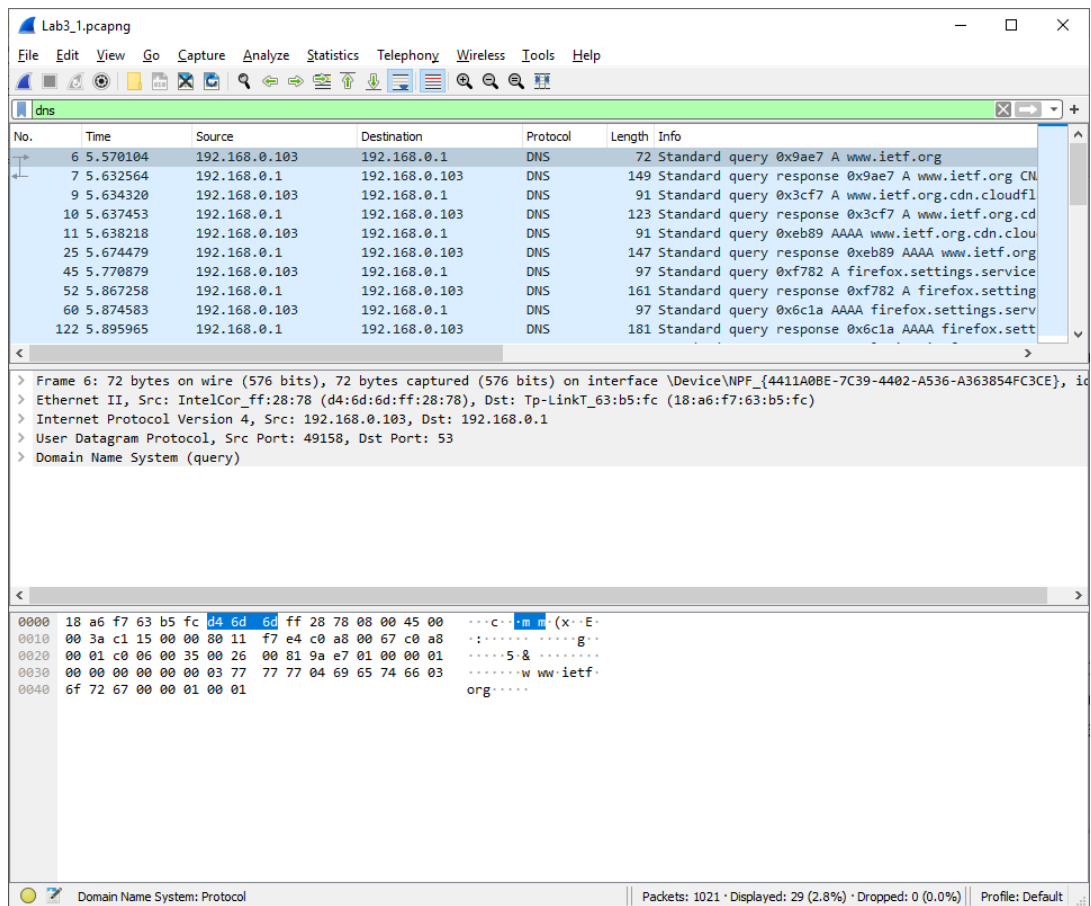
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\System32>_
```

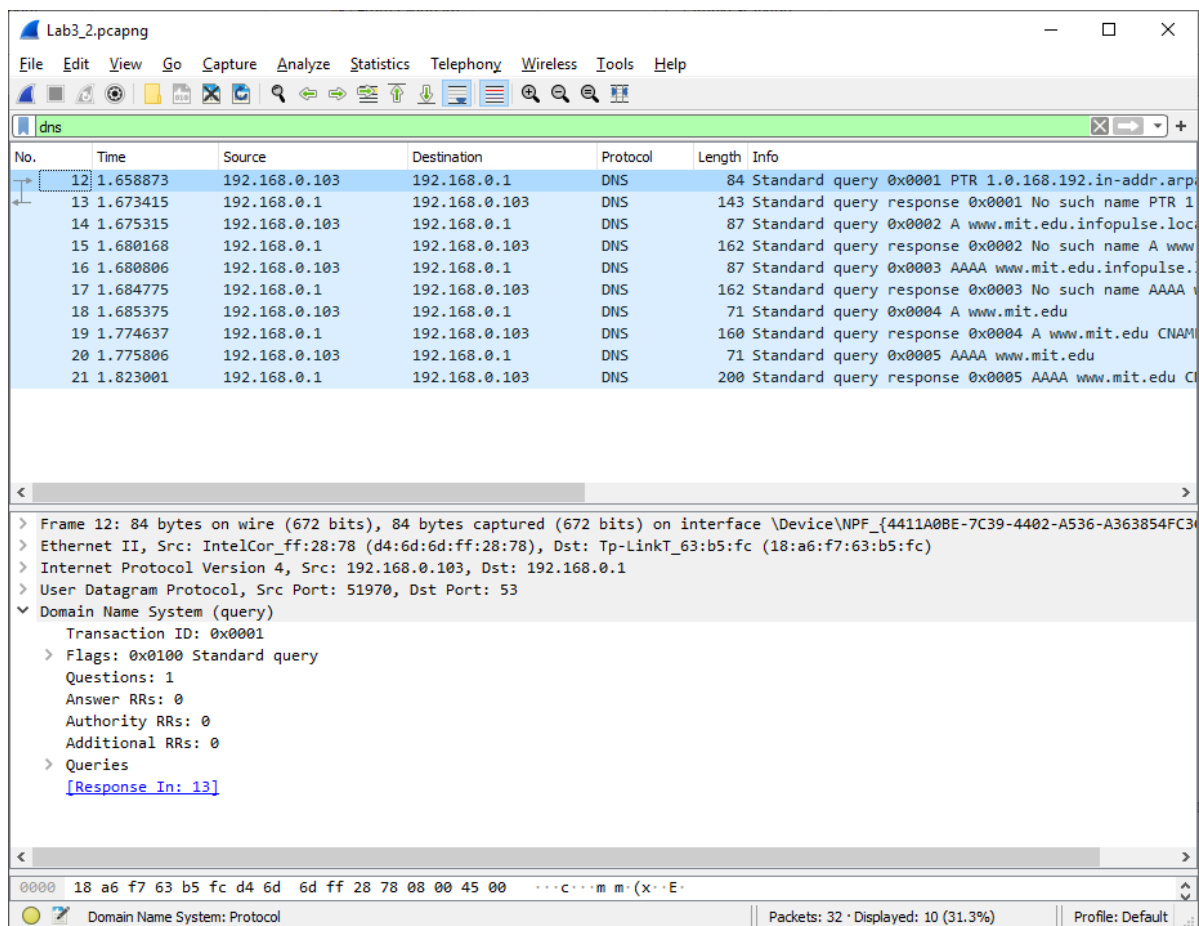
Мал. 1

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. 2

8. Почніть захоплення пакетів
9. Виконайте nslookup для домену `www.mit.edu` за допомогою команди `a. nslookup www.mit.edu` кожну хвилину) – почніть спочатку та виконайте кроки 1,2,3 та 8.
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



Мал. 2

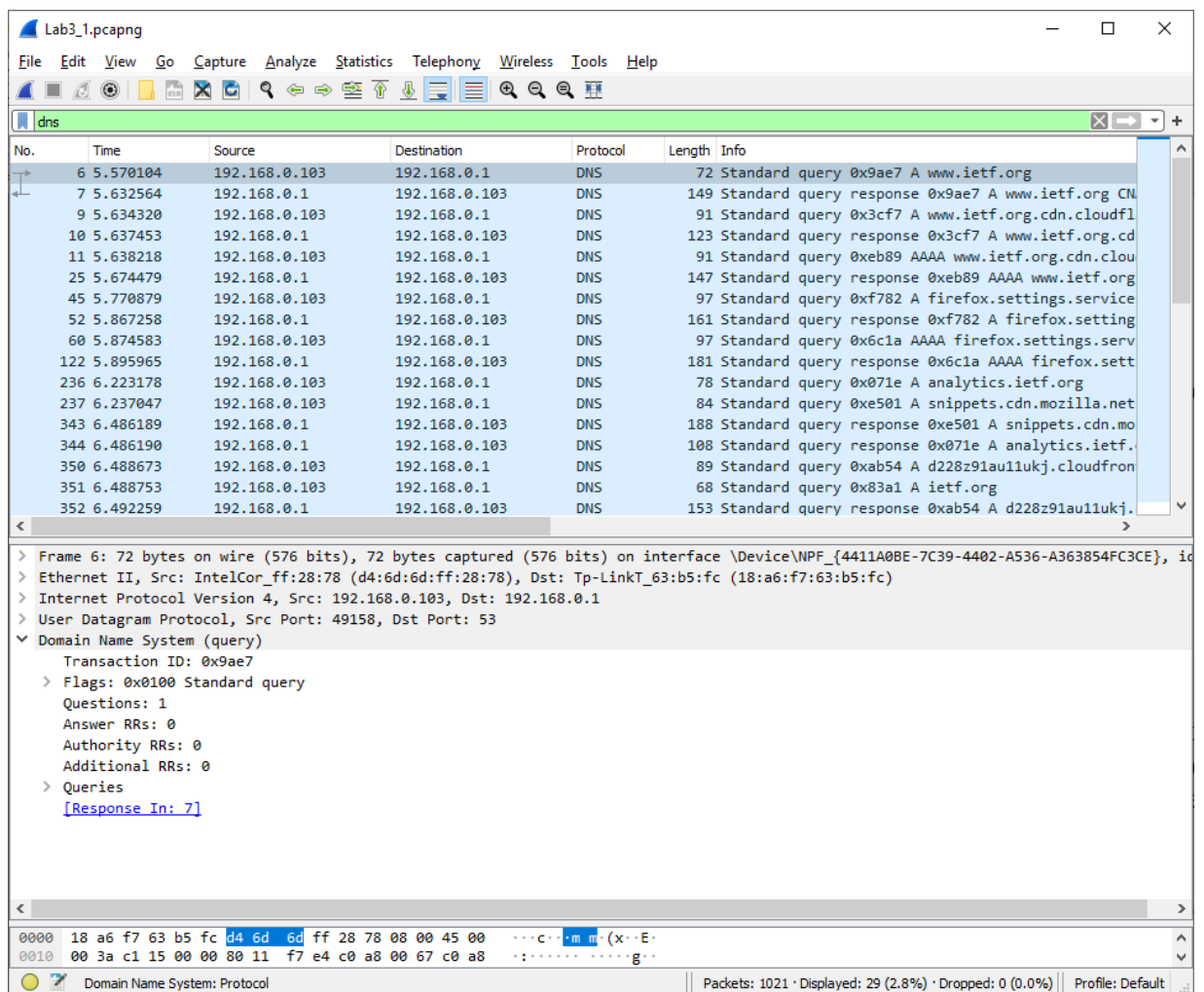
12. Почніть захоплення пакетів
13. Виконайте nslookup для домену www.mit.edu за допомогою команди
 - a. nslookup -type=NS mit.edu
14. Зупиніть захоплення пакетів
15. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети
16. Почніть захоплення пакетів
17. Виконайте nslookup для домену www.mit.edu за допомогою команди
 - a. 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

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: DNS використовує протокол UDP: Source: 192.168.0.103; Destination: 192.168.0.1



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

Відповідь: Destination: 192.168.0.1 – є адресою локального DNS сервера

```

Select C:\Windows\System32\cmd.exe

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : evry.com

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::6855:f175:a3c1:32a6%7
IPv4 Address. . . . . : 192.168.0.103
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected

```

Мал. 4

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

Відповідь: Запит типу A; Має ссилку на відповідь. [Response In: 7]

Lab3_1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
6	5.570104	192.168.0.103	192.168.0.1	DNS	72	Standard query 0x9ae7 A www.ietf.org
7	5.632564	192.168.0.1	192.168.0.103	DNS	149	Standard query response 0x9ae7 A www.ietf.org CN
9	5.634320	192.168.0.103	192.168.0.1	DNS	91	Standard query 0x3cf7 A www.ietf.org.cdn.cloudfl
10	5.637453	192.168.0.1	192.168.0.103	DNS	123	Standard query response 0x3cf7 A www.ietf.org.cd
11	5.638218	192.168.0.103	192.168.0.1	DNS	91	Standard query 0xeb89 AAAA www.ietf.org.cdn.clou
25	5.674479	192.168.0.1	192.168.0.103	DNS	147	Standard query response 0xeb89 AAAA www.ietf.org
45	5.770879	192.168.0.103	192.168.0.1	DNS	97	Standard query 0xf782 A firefox.settings.service
52	5.867258	192.168.0.1	192.168.0.103	DNS	161	Standard query response 0xf782 A firefox.setting
60	5.874583	192.168.0.103	192.168.0.1	DNS	97	Standard query 0x6c1a AAAA firefox.settings.serv
122	5.895965	192.168.0.1	192.168.0.103	DNS	181	Standard query response 0x6c1a AAAA firefox.sett
236	6.223178	192.168.0.103	192.168.0.1	DNS	78	Standard query 0x071e A analytics.ietf.org
237	6.237047	192.168.0.103	192.168.0.1	DNS	84	Standard query 0xe501 A snippets.cdn.mozilla.net
343	6.486189	192.168.0.1	192.168.0.103	DNS	188	Standard query response 0xe501 A snippets.cdn.mo
344	6.486190	192.168.0.1	192.168.0.103	DNS	108	Standard query response 0x071e A analytics.ietf.
350	6.488673	192.168.0.103	192.168.0.1	DNS	89	Standard query 0xab54 A d228z91au1lukj.cloudfron
351	6.488753	192.168.0.103	192.168.0.1	DNS	68	Standard query 0x83a1 A ietf.org
352	6.492259	192.168.0.1	192.168.0.103	DNS	153	Standard query response 0xab54 A d228z91au1lukj.

< >

> User Datagram Protocol, Src Port: 49158, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x9ae7

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ www.ietf.org: type A, class IN

Name: www.ietf.org

[Name Length: 12]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 7]

< >

0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03w ww.ietf.

0040 0f 72 67 00 00 01 00 01 org.....

Text item (text), 18 bytes

Packets: 1021 · Displayed: 29 (2.8%) · Dropped: 0 (0.0%) Profile: Default

Мал. 5

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

Відповідь: Запропоновано 3 відповіді, Кожна з відповідей містить наступні поля: Name, Type, Class, TTL, Data length, CNAME;

Приклад відповіді:

Name: www.ietf.org

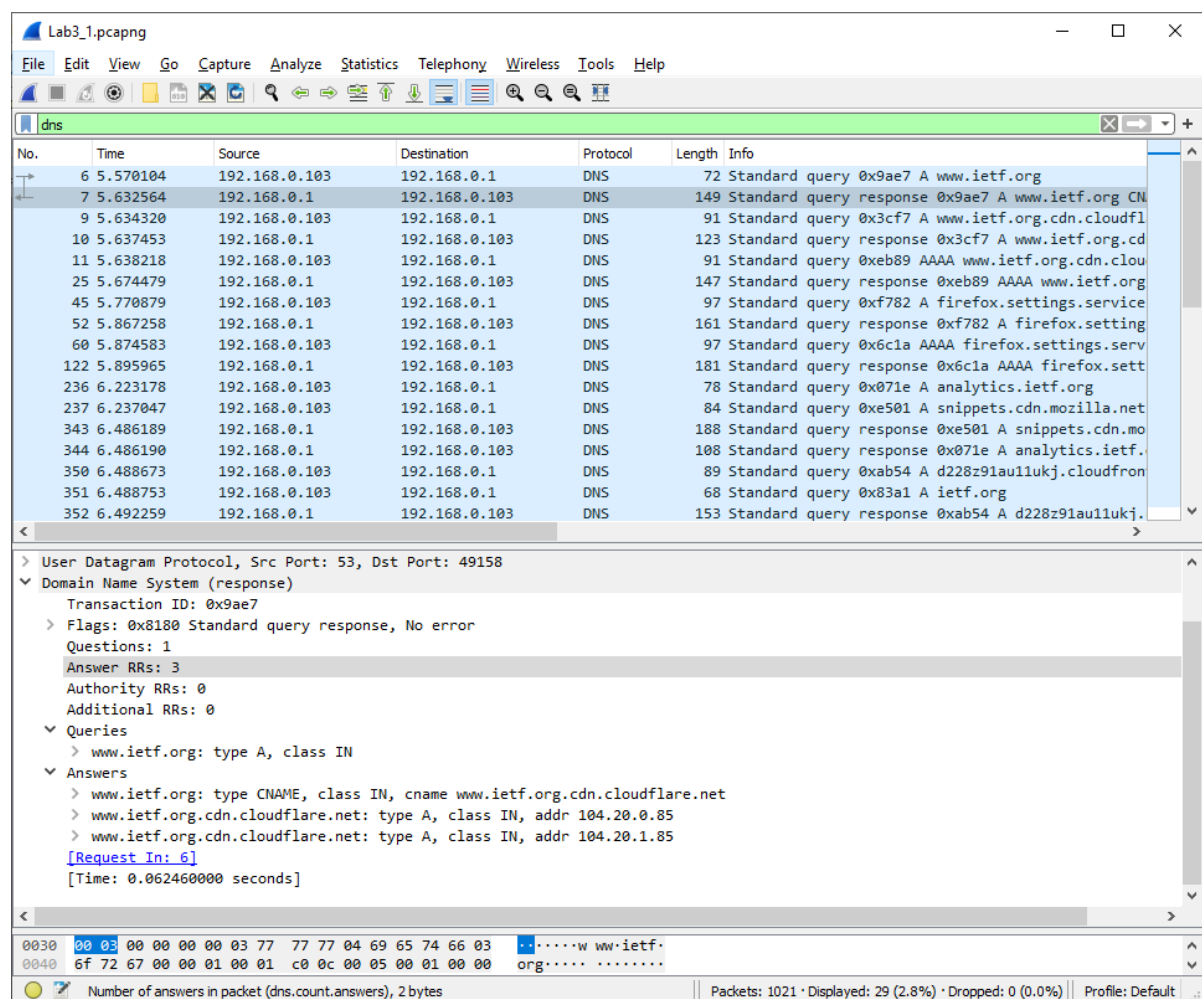
Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 1483 (24 minutes, 43 seconds)

Data length: 33

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



Мал. 6

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: в TCP SYN Destination: 104.20.0.85 співпадає з однією з

запропонованих відповідей сервера DNS.

The image shows a Wireshark packet capture analysis of a DNS query and response. The top pane displays a list of 17 packets. The bottom pane shows the details of the selected packet (No. 17), which is a DNS response from 104.20.0.85 to 192.168.0.103.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.103	172.18.57.65	TCP	66	3127 → 4369 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.976153	192.168.0.1	255.255.255.255	UDP	215	38259 → 7437 Len=173
3	4.048536	192.168.0.1	255.255.255.255	UDP	215	38259 → 7437 Len=173
4	4.793777	IntelCor_ff:28:78	Tp-LinkT_63:b5:fc	ARP	42	Who has 192.168.0.1? Tell 192.168.0.103
5	4.795724	Tp-LinkT_63:b5:fc	IntelCor_ff:28:78	ARP	42	192.168.0.1 is at 18:a6:f7:63:b5:fc
6	5.570104	192.168.0.103	192.168.0.1	DNS	72	Standard query 0x9ae7 A www.ietf.org
7	5.632564	192.168.0.1	192.168.0.103	DNS	149	Standard query response 0x9ae7 A www.ietf.org CN
8	5.633938	192.168.0.103	104.20.0.85	TCP	66	3128 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
9	5.634320	192.168.0.103	192.168.0.1	DNS	91	Standard query 0x3cf7 A www.ietf.org.cdn.cloudflare
10	5.637453	192.168.0.1	192.168.0.103	DNS	123	Standard query response 0x3cf7 A www.ietf.org.cdn
11	5.638218	192.168.0.103	192.168.0.1	DNS	91	Standard query 0xeb89 AAAA www.ietf.org.cdn.clou
12	5.651217	104.20.0.85	192.168.0.103	TCP	68	443 → 3128 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
13	5.651296	192.168.0.103	104.20.0.85	TCP	54	3128 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
14	5.651458	192.168.0.103	104.20.0.85	TLShv1.2	249	Client Hello
15	5.665058	104.20.0.85	192.168.0.103	TCP	56	443 → 3128 [ACK] Seq=1 Ack=196 Win=67584 Len=0
16	5.665722	104.20.0.85	192.168.0.103	TLShv1.2	1494	Server Hello
17	5.665727	104.20.0.85	192.168.0.103	TLShv1.2	1315	Certificate, Certificate Status, Server Key Exch

Packet Details (No. 17):

- User Datagram Protocol, Src Port: 53, Dst Port: 49158
- Domain Name System (response)
 - Transaction ID: 0x9ae7
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - www.ietf.org: type A, class IN
- 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 104.20.0.85
 - www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
- [Request in: 6]
- [Time: 0.062460000 seconds]

Packet Bytes:

```

0070  03 6e 65 74 00 c0 2a 00 01 00 01 00 00 00 2a 00  .net.*.*.....*
0080  04 68 14 00 55 c0 2a 00 01 00 01 00 00 00 2a 00  .h..l.*.*.....
  
```

Text item (text), 16 bytes

Packets: 1021 · Displayed: 1021 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

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

Відповідь: так. Було виконано ще 13 нових DNS запитів. Взагалі було 14 DNS запитів разом із першим.

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

Відповідь: Порти у запиті: Source Port: 60631; Destination Port: 53;

Порти у відповіді: Source Port: 53; Destination Port: 60631.


```

C:\Windows\System32>nslookup www.mit.edu
Server:      Unknown
Address:     192.168.0.1

Non-authoritative answer:
Name:       e9566.dscb.akamaiedge.net
Addresses:  2a02:26f0:d200:19e::255e
            2a02:26f0:d200:191::255e
            104.121.176.214
Aliases:    www.mit.edu
            www.mit.edu.edgekey.net

C:\Windows\System32>

```

Мал. 8

Lab3_2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
13	19.579094	192.168.0.103	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
14	19.584217	192.168.0.1	192.168.0.103	DNS	143	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
15	19.586315	192.168.0.103	192.168.0.1	DNS	87	Standard query 0x0002 A www.mit.edu.infopulse.local
16	19.618600	192.168.0.1	192.168.0.103	DNS	162	Standard query response 0x0002 No such name A www.mit.edu.infopulse.local
17	19.619417	192.168.0.103	192.168.0.1	DNS	87	Standard query 0x0003 AAAA www.mit.edu.infopulse.local
18	19.652117	192.168.0.1	192.168.0.103	DNS	162	Standard query response 0x0003 No such name AAAA www.mit.edu.infopulse.local
19	19.652649	192.168.0.103	192.168.0.1	DNS	71	Standard query 0x0004 A www.mit.edu
20	19.769346	192.168.0.1	192.168.0.103	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu
21	19.772554	192.168.0.103	192.168.0.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
22	19.806074	192.168.0.1	192.168.0.103	DNS	200	Standard query response 0x0005 AAAA www.mit.edu CNAME www.mit.edu

< Frame 13: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{4411A0BE-7C39-4402-A536-A363854FC3CE}, 1
 > Ethernet II, Src: IntelCor_ff:28:78 (d4:6d:6d:ff:28:78), Dst: Tp-LinkT_63:b5:fc (18:a6:f7:63:b5:fc)
 > Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1
 > User Datagram Protocol, Src Port: 60631, Dst Port: 53
 > Source Port: 60631
 > Destination Port: 53
 > Length: 50
 > Checksum: 0x0449 [unverified]
 > [Checksum Status: Unverified]
 > [Stream index: 1]
 > [Timestamps]
 > Domain Name System (query)

0020 00 01 ec d7 00 35 00 32 04 49 00 01 01 00 00 01S.2 .I.....
 0030 00 00 00 00 00 00 01 31 01 30 03 31 36 38 03 311 .0.168.1

Destination Port (udp.dstport), 2 bytes | Packets: 23 · Displayed: 10 (43.5%) · Dropped: 0 (0.0%) | Profile: Default

Мал. 9

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 – це є адреса локального сервера DNS за замовчанням.

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

Відповідь: Це був запит типу PTR. Також був запит типу A для IPv4 – для AAAA – для IPv6, SOA, CNAME.

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

Відповідь: Було взагалі 5 запитів і 5 відповідей. У останній відповіді було запропоновано 4 запису. Кожна з відповідей складається з :

для PTR – була 1 відповідь;

для типу A – 3 відповіді;

для типу AAAA – 4 відповіді;

The screenshot shows the Wireshark interface with the following details:

- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
13	19.579094	192.168.0.103	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
14	19.584217	192.168.0.1	192.168.0.103	DNS	143	Standard query response 0x0001 No such name PTR 1.0.168
15	19.586315	192.168.0.103	192.168.0.1	DNS	87	Standard query 0x0002 A www.mit.edu.infopulse.local
16	19.618600	192.168.0.1	192.168.0.103	DNS	162	Standard query response 0x0002 No such name A www.mit.e
17	19.619417	192.168.0.103	192.168.0.1	DNS	87	Standard query 0x0003 AAAA www.mit.edu.infopulse.local
18	19.652117	192.168.0.1	192.168.0.103	DNS	162	Standard query response 0x0003 No such name AAAA www.mi
19	19.652649	192.168.0.103	192.168.0.1	DNS	71	Standard query 0x0004 A www.mit.edu
20	19.769346	192.168.0.1	192.168.0.103	DNS	160	Standard query response 0x0004 A www.mit.edu CNAME ww
21	19.772554	192.168.0.103	192.168.0.1	DNS	71	Standard query 0x0005 AAAA www.mit.edu
22	19.806074	192.168.0.1	192.168.0.103	DNS	200	Standard query response 0x0005 AAAA www.mit.edu CNAME v
- Packet Details:**
 - Ethernet II, Src: Tp-LinkT_63:b5:fc (18:a6:f7:63:b5:fc), Dst: IntelCor_ff:28:78 (d4:6d:6d:ff:28:78)
 - Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103
 - User Datagram Protocol, Src Port: 53, Dst Port: 60634
 - Domain Name System (response)
 - Transaction ID: 0x0004
 - Flags: 0x8180 Standard query response, No error
 - Questions: 1
 - Answer RRs: 3
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.mit.edu: type A, class IN
 - Name: www.mit.edu
 - [Name Length: 11]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Answers
 - www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
 - www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
 - e9566.dscb.akamaiedge.net: type A, class IN, addr 104.121.176.214
- Packet Bytes:**

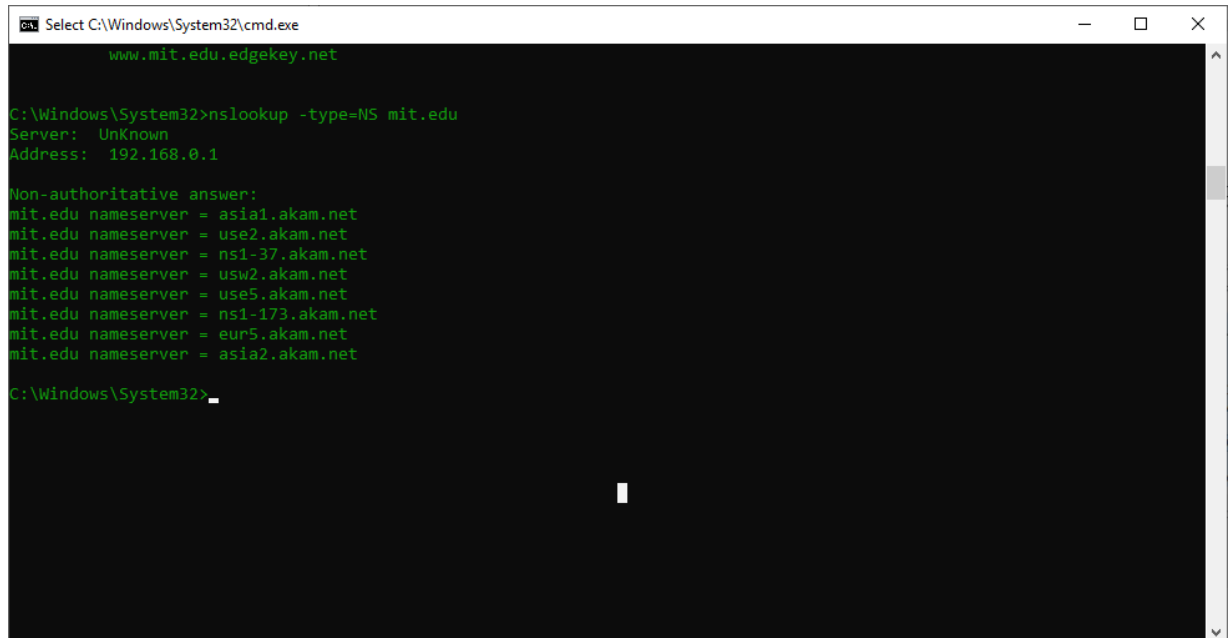
```

0040  64 75 00 00 01 c0 0c 00 05 00 01 00 00 05  du...
0050  ab 00 19 03 77 77 03 6d 69 74 03 65 64 75 07  ....www.mit.edu

```

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



```
Select C:\Windows\System32\cmd.exe
www.mit.edu.edgekey.net

C:\Windows\System32>nslookup -type=NS mit.edu
Server:  UnKnown
Address:  192.168.0.1

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

C:\Windows\System32>
```

Мал. 11

Lab3_3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
4	3.843686	192.168.0.103	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
5	3.847122	192.168.0.1	192.168.0.103	DNS	143	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
6	3.848781	192.168.0.103	192.168.0.1	DNS	83	Standard query 0x0002 NS mit.edu.infopulse.local
7	3.882274	192.168.0.1	192.168.0.103	DNS	158	Standard query response 0x0002 No such name NS mit.edu.infopulse.local
8	3.882897	192.168.0.103	192.168.0.1	DNS	67	Standard query 0x0003 NS mit.edu
9	3.902908	192.168.0.1	192.168.0.103	DNS	234	Standard query response 0x0003 NS mit.edu NS asia1.akan

< >

> Frame 4: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{4411A0BE-7C39-4402-A536-A363854FC3CE}, id 0040
 > Ethernet II, Src: IntelCor_ff:28:78 (d4:6d:6d:ff:28:78), Dst: Tp-LinkT_63:b5:fc (18:a6:f7:63:b5:fc)
 > Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1
 > User Datagram Protocol, Src Port: 60746, 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
 > 1.0.168.192.in-addr.arpa: type PTR, class IN
 [Response In: 5]

< >

0040 39 32 07 69 6e 2d 61 64 64 72 04 61 72 70 61 00 92-in-ad dr-arpa-
 0050 00 0c 00 01

Query Type (dns.qry.type), 2 bytes | Packets: 12 · Displayed: 6 (50.0%) · Dropped: 0 (0.0%) | Profile: Default

Мал. 12

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

Відповідь: було 3 запита. Один з них був типу PTR, два інших типу NS. Так, цей запит вміщує посилку на відповіді: [Response In: 5]

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 взагалі 3 запита і 3 відповіді. У останній відповіді було запропоновано 8 записів. Кожна з відповідей складається з таких полів: Name, Type, Class, TTL, Data length, Name Server;

Приклад відповіді:

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

Name: mit.edu

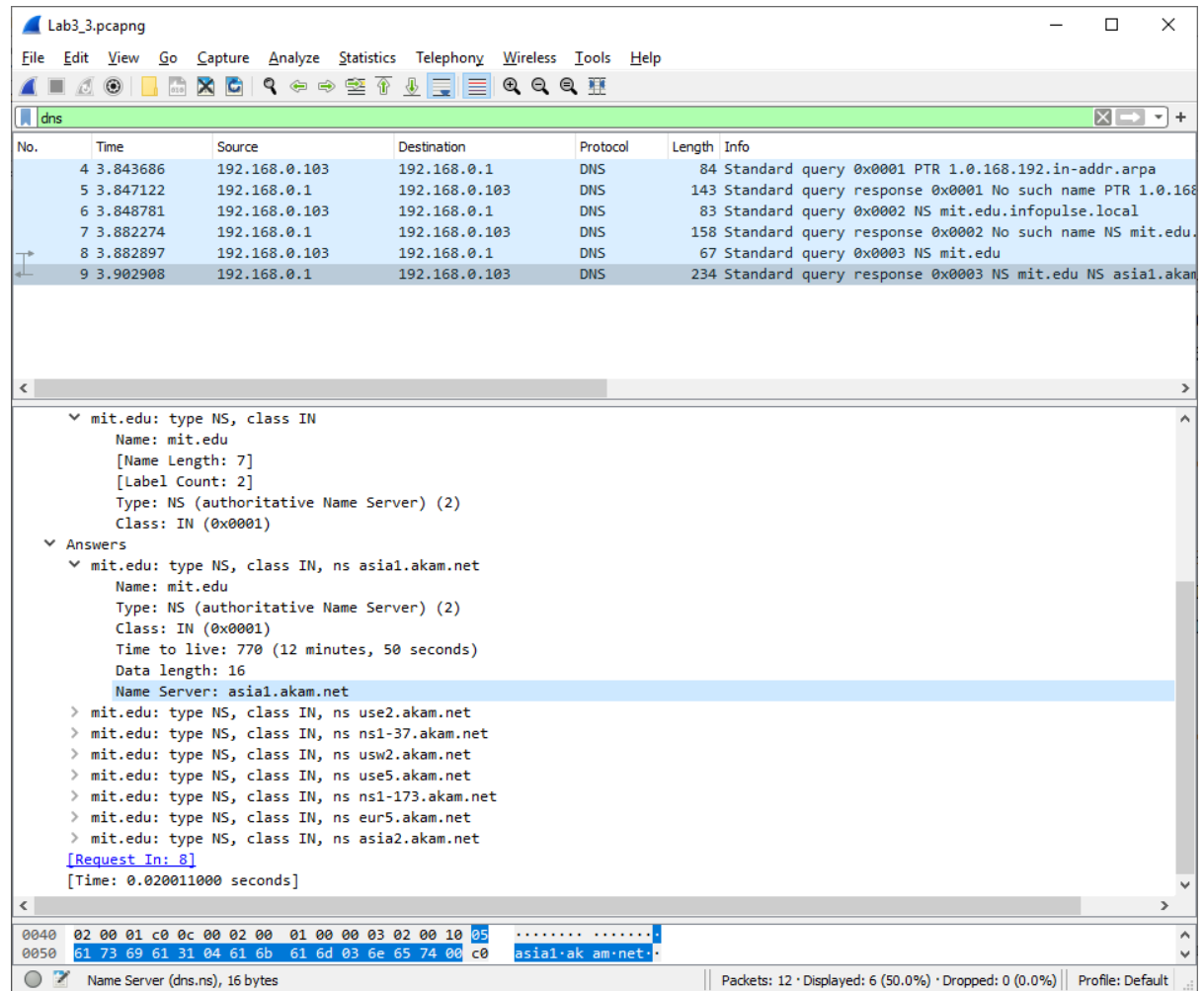
Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 770 (12 minutes, 50 seconds)

Data length: 16

Name Server: asia1.akam.net



Мал. 13

- 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: Destination: 192.168.0.1 – це є адреса локального сервера DNS за замовчанням, також був запит на Destination: 18.0.72.3

```

Select C:\Windows\System32\cmd.exe

mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia2.akam.net

C:\Windows\System32>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Windows\System32>

```

Мал. 14

*Wi-Fi						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
dns						
No.	Time	Source	Destination	Protocol	Length	Info
7	12.361819	192.168.0.103	192.168.0.1	DNS	73	Standard query 0xa11d A bitsy.mit.edu
8	12.386823	192.168.0.103	192.168.0.1	DNS	73	Standard query 0xa11d A bitsy.mit.edu
9	12.395772	192.168.0.1	192.168.0.103	DNS	89	Standard query response 0xa11d A bitsy.mit.edu A
10	12.395772	192.168.0.1	192.168.0.103	DNS	89	Standard query response 0xa11d A bitsy.mit.edu A
11	12.398865	192.168.0.103	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
12	14.405557	192.168.0.103	18.0.72.3	DNS	90	Standard query 0x0002 A www.aiit.or.kr.infopulse
14	16.407199	192.168.0.103	18.0.72.3	DNS	90	Standard query 0x0003 AAAA www.aiit.or.kr.infopu
16	18.410656	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
17	20.414130	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
19	23.768954	192.168.0.103	192.168.0.1	DNS	76	Standard query 0x12ab A dns.msftncsi.com
20	23.773382	192.168.0.1	192.168.0.103	DNS	92	Standard query response 0x12ab A dns.msftncsi.co
25	27.972055	192.168.0.103	192.168.0.1	DNS	110	Standard query 0xc936 SRV _ldap._tcp.CRSite._sit
26	27.997503	192.168.0.103	192.168.0.1	DNS	110	Standard query 0xc936 SRV _ldap._tcp.CRSite._sit
27	28.083661	192.168.0.1	192.168.0.103	DNS	185	Standard query response 0xc936 No such name SRV
28	28.083662	192.168.0.1	192.168.0.103	DNS	185	Standard query response 0xc936 No such name SRV
29	28.086195	192.168.0.103	192.168.0.1	DNS	96	Standard query 0xe8a8 SRV _ldap._tcp.dc._msdcs.i
30	28.090311	192.168.0.1	192.168.0.103	DNS	171	Standard query response 0xe8a8 No such name SRV

> Frame 12: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{4411A0BE-7C39-4402-A536-A363854FC3CE}, 3
 > Ethernet II, Src: IntelCor_ff:28:78 (d4:6d:6d:ff:28:78), Dst: Tp-LinkT_63:b5:fc (18:a6:f7:63:b5:fc)
 > Internet Protocol Version 4, Src: 192.168.0.103, Dst: 18.0.72.3
 > User Datagram Protocol, Src Port: 63797, Dst Port: 53
 > Domain Name System (query)
 Transaction ID: 0x0002
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > www.aiit.or.kr.infopulse.local: type A, class IN

0000 18 a6 f7 63 b5 fc d4 6d 6d ff 28 78 08 00 45 00 ...c...m m(x...E...
 0010 00 4c 83 c6 00 00 80 11 9b c8 c0 a8 00 67 12 00 ...L.....g...

wireshark_Wi-Fi_20200610195400_a13812.pcapng Packets: 78 · Displayed: 25 (32.1%) · Dropped: 0 (0.0%) Profile: Default

Мал. 15

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

Відповідь: Взагалі було виконано 18 запитів та 7 відповідей DNS. Були запити

типу A, PTR, SRV, AAAA.

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

Відповідь: Було взагалі 18 запитів але тільки 7 відповідей. У відповіді для bitsy.mit.edu було 1 відповідь, яка складається з таких полів:

Name, Type, Class, TTL, Data length, Address;

Приклад відповіді:

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: 1531 (25 minutes, 31 seconds)

Data length: 4

Address: 18.0.72.3

The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list pane displays a list of packets, including a query for bitsy.mit.edu and its response. The packet details pane shows the response structure with fields: Name, Type, Class, TTL, Data length, and Address. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
7	12.361819	192.168.0.103	192.168.0.1	DNS	73	Standard query 0xa11d A bitsy.mit.edu
8	12.386823	192.168.0.103	192.168.0.1	DNS	73	Standard query 0xa11d A bitsy.mit.edu
9	12.395772	192.168.0.1	192.168.0.103	DNS	89	Standard query response 0xa11d A bitsy.mit.edu A
10	12.395772	192.168.0.1	192.168.0.103	DNS	89	Standard query response 0xa11d A bitsy.mit.edu A
11	12.398865	192.168.0.103	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
12	14.405557	192.168.0.103	18.0.72.3	DNS	90	Standard query 0x0002 A www.aiit.or.kr.infopulse
14	16.407199	192.168.0.103	18.0.72.3	DNS	90	Standard query 0x0003 AAAA www.aiit.or.kr.infopulse
16	18.410656	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
17	20.414130	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
19	23.768954	192.168.0.103	192.168.0.1	DNS	76	Standard query 0x12ab A dns.msftncsi.com
20	23.773382	192.168.0.1	192.168.0.103	DNS	92	Standard query response 0x12ab A dns.msftncsi.com
25	27.972055	192.168.0.103	192.168.0.1	DNS	110	Standard query 0xc936 SRV _ldap._tcp.CRSite._sit
26	27.997503	192.168.0.103	192.168.0.1	DNS	110	Standard query 0xc936 SRV _ldap._tcp.CRSite._sit
27	28.083661	192.168.0.1	192.168.0.103	DNS	185	Standard query response 0xc936 No such name SRV
28	28.083662	192.168.0.1	192.168.0.103	DNS	185	Standard query response 0xc936 No such name SRV
29	28.086195	192.168.0.103	192.168.0.1	DNS	96	Standard query 0xe8a8 SRV _ldap._tcp.dc._msdcs.i
30	28.090311	192.168.0.1	192.168.0.103	DNS	171	Standard query response 0xe8a8 No such name SRV

Transaction ID: 0xa11d

- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 0
- Additional RRs: 0
- Queries
- 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: 1531 (25 minutes, 31 seconds)
 - Data length: 4
 - Address: 18.0.72.3

[Request In: 7]
[Time: 0.033953000 seconds]

0040 03 65 64 75 00 00 01 00 01 c0 0c 00 01 00 01 00 .edu....
0050 00 05 fb 00 04 12 00 48 03H.

Response Address (dns.a), 4 bytes

Packets: 78 · Displayed: 25 (32.1%) · Dropped: 0 (0.0%) · Profile: Default

Мал. 16