

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 3
З дисципліни: Комп'ютерні мережі

Протоколи DNS

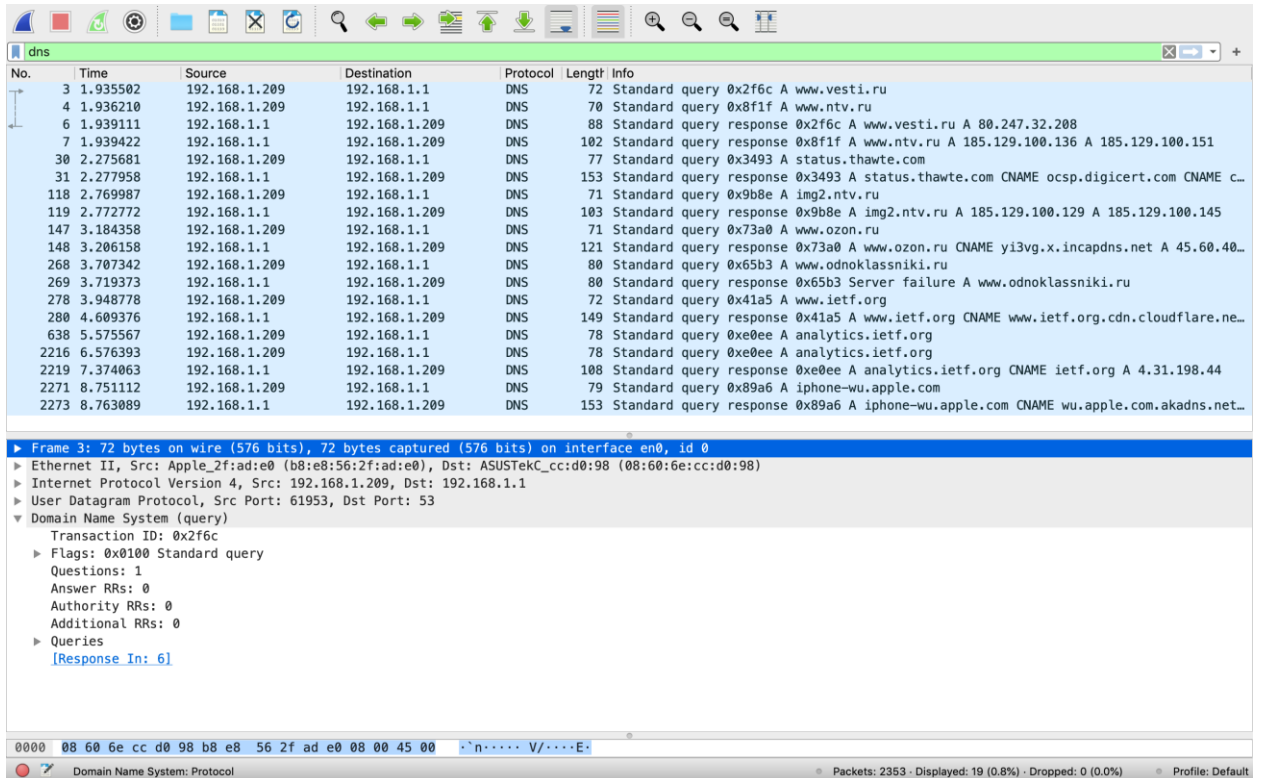
Виконав:
Студент III курсу
Групи КА-73
Яблуновський О. В.
Перевірів: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи

```
Sashka--PK:~ mac$ sudo killall -HUP mDNSResponder
Password:
Sorry, try again.
Password:
```



The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of 27 DNS packets (No. 3 to 27) with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are standard queries and responses for various domains like www.vesti.ru, www.ntv.ru, status.thawte.com, and others. The bottom pane shows the details of the selected packet (No. 72), which is a standard query response for www.vesti.ru. The details pane shows the transaction ID, flags, and the query type. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3	1.935502	192.168.1.209	192.168.1.1	DNS	72	Standard query 0x2f6c A www.vesti.ru
4	1.936210	192.168.1.209	192.168.1.1	DNS	70	Standard query 0x8f1f A www.ntv.ru
6	1.939111	192.168.1.1	192.168.1.209	DNS	88	Standard query response 0x2f6c A www.vesti.ru A 80.247.32.208
7	1.939422	192.168.1.1	192.168.1.209	DNS	102	Standard query response 0x8f1f A www.ntv.ru A 185.129.100.136 A 185.129.100.151
30	2.275681	192.168.1.209	192.168.1.1	DNS	77	Standard query 0x3493 A status.thawte.com
31	2.277958	192.168.1.1	192.168.1.209	DNS	153	Standard query response 0x3493 A status.thawte.com CNAME ocsp.digicert.com CNAME c...
118	2.769987	192.168.1.209	192.168.1.1	DNS	71	Standard query 0x9b8e A img2.ntv.ru
119	2.772772	192.168.1.1	192.168.1.209	DNS	103	Standard query response 0x9b8e A img2.ntv.ru A 185.129.100.129 A 185.129.100.145
147	3.184358	192.168.1.209	192.168.1.1	DNS	71	Standard query 0x73a0 A www.ozon.ru
148	3.206158	192.168.1.1	192.168.1.209	DNS	121	Standard query response 0x73a0 A www.ozon.ru CNAME yi3vg.x.incapdns.net A 45.60.40...
268	3.707342	192.168.1.209	192.168.1.1	DNS	80	Standard query 0x65b3 A www.odnoklassniki.ru
269	3.719373	192.168.1.1	192.168.1.209	DNS	80	Standard query response 0x65b3 Server failure A www.odnoklassniki.ru
278	3.948778	192.168.1.209	192.168.1.1	DNS	72	Standard query 0x41a5 A www.ietf.org
280	4.609376	192.168.1.1	192.168.1.209	DNS	149	Standard query response 0x41a5 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.ne...
638	5.575567	192.168.1.209	192.168.1.1	DNS	78	Standard query 0xe0ee A analytics.ietf.org
2216	6.576393	192.168.1.209	192.168.1.1	DNS	78	Standard query 0xe0ee A analytics.ietf.org
2219	7.374063	192.168.1.1	192.168.1.209	DNS	108	Standard query response 0xe0ee A analytics.ietf.org CNAME ietf.org A 4.31.198.44
2271	8.751112	192.168.1.209	192.168.1.1	DNS	79	Standard query 0x89a6 A iphone-wu.apple.com
2273	8.763089	192.168.1.1	192.168.1.209	DNS	153	Standard query response 0x89a6 A iphone-wu.apple.com CNAME wu.apple.com.akadns.net...

Frame 3: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0

Ethernet II, Src: Apple_2f:ad:e0 (b8:e8:56:2f:ad:e0), Dst: ASUSTekC_cc:d0:98 (08:60:6e:cc:d0:98)

Internet Protocol Version 4, Src: 192.168.1.209, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 61953, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x2f6c

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Response In: 6]

0000 08 60 6e cc d0 98 b8 e8 56 2f ad e0 08 00 45 00 ...n.....V/....E

Domain Name System: Protocol

Packets: 2353 · Displayed: 19 (0.8%) · Dropped: 0 (0.0%) · Profile: Default

SamsungE_6d:91:d5	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.210
192.168.1.209	192.168.1.1	DNS	72	Standard query 0x2f6c A www.vesti.ru
192.168.1.209	192.168.1.1	DNS	70	Standard query 0x8f1f A www.ntv.ru
ASUSTekC_cc:d0:9c	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/08:60:6e:cc:d0:98 Cost = 0 Port = 0x8003
192.168.1.1	192.168.1.209	DNS	88	Standard query response 0x2f6c A www.vesti.ru A 80.247.32.208
192.168.1.1	192.168.1.209	DNS	102	Standard query response 0x8f1f A www.ntv.ru A 185.129.100.136 A 185.129.100.151
192.168.1.209	80.247.32.208	TCP	78	64020 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=365304752 TSecr=0
192.168.1.209	185.129.100.136	TCP	78	64022 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=365304753 TSecr=0
185.129.100.136	192.168.1.209	TCP	74	80 → 64022 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=
192.168.1.209	185.129.100.136	TCP	66	64022 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=365304808 TSecr=3838441261
192.168.1.209	185.129.100.136	HTTP	390	GET / HTTP/1.1
185.129.100.136	192.168.1.209	TCP	66	80 → 64022 [ACK] Seq=1 Ack=325 Win=30080 Len=0 TSval=3838441316 TSecr=36530481
185.129.100.136	192.168.1.209	HTTP	459	HTTP/1.1 301 Moved Permanently (text/html)
192.168.1.209	185.129.100.136	TCP	66	64022 → 80 [ACK] Seq=325 Ack=394 Win=130880 Len=0 TSval=365304863 TSecr=383844

No.	Time	Source	Destination	Protocol	Length	Info
3	1.935502	192.168.1.209	192.168.1.1	DNS	72	Standard query 0x2f6c A www.vesti.ru
4	1.936210	192.168.1.209	192.168.1.1	DNS	70	Standard query 0x8f1f A www.ntv.ru
6	1.939111	192.168.1.1	192.168.1.209	DNS	88	Standard query response 0x2f6c A www.vesti.ru A 80.247.32.208
7	1.939422	192.168.1.1	192.168.1.209	DNS	102	Standard query response 0x8f1f A www.ntv.ru A 185.129.100.136 A 185.129.100.151
30	2.275681	192.168.1.209	192.168.1.1	DNS	77	Standard query 0x3493 A status.thawte.com
31	2.277958	192.168.1.1	192.168.1.209	DNS	153	Standard query response 0x3493 A status.thawte.com CNAME ocsp.digicert.com CNAME c...
118	2.769987	192.168.1.209	192.168.1.1	DNS	71	Standard query 0x9b8e A img2.ntv.ru
119	2.772772	192.168.1.1	192.168.1.209	DNS	103	Standard query response 0x9b8e A img2.ntv.ru A 185.129.100.129 A 185.129.100.145
147	3.184358	192.168.1.209	192.168.1.1	DNS	71	Standard query 0x73a0 A www.ozon.ru
148	3.206158	192.168.1.1	192.168.1.209	DNS	121	Standard query response 0x73a0 A www.ozon.ru CNAME y13vg.x.incapdns.net A 45.60.40...
268	3.707342	192.168.1.209	192.168.1.1	DNS	80	Standard query 0x65b3 A www.odnoklassniki.ru
269	3.719373	192.168.1.1	192.168.1.209	DNS	80	Standard query response 0x65b3 Server failure A www.odnoklassniki.ru
278	3.948778	192.168.1.209	192.168.1.1	DNS	72	Standard query 0x41a5 A www.ietf.org
280	4.609376	192.168.1.1	192.168.1.209	DNS	149	Standard query response 0x41a5 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.ne...
638	5.575567	192.168.1.209	192.168.1.1	DNS	78	Standard query 0xe0ee A analytics.ietf.org
2216	6.576393	192.168.1.209	192.168.1.1	DNS	78	Standard query 0xe0ee A analytics.ietf.org
2219	7.374063	192.168.1.1	192.168.1.209	DNS	108	Standard query response 0xe0ee A analytics.ietf.org CNAME ietf.org A 4.31.198.44
2271	8.751112	192.168.1.209	192.168.1.1	DNS	79	Standard query 0x89a6 A iphone-wu.apple.com
2273	8.763089	192.168.1.1	192.168.1.209	DNS	153	Standard query response 0x89a6 A iphone-wu.apple.com CNAME wu.apple.com.akadns.net...

Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0

- Ethernet II, Src: Apple_2f:ad:e0 (b8:e8:56:2f:ad:e0), Dst: ASUSTekC_cc:d0:98 (08:60:6e:cc:d0:98)
- Internet Protocol Version 4, Src: 192.168.1.209, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 57547, Dst Port: 53
- Domain Name System (query)

0000	08 60 6e cc d0 98 b8 e8 56 2f ad e0 08 00 45 00 V/....E.
0010	00 38 9d 52 00 00 ff 11 9a 3f c0 a8 01 d1 c0 a8	..8.R.....7.....
0020	01 01 e0 cb 00 35 00 24 a0 1a 8f 1f 01 00 00 015.\$.....
0030	00 00 00 00 00 00 03 77 77 77 03 6e 74 76 02 72w ww.ntv.r
0040	75 00 00 01 00 01	U.....

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?

Ethernet II, Src: Apple_2f:ad:e0 (b8:e8:56:2f:ad:e0), Dst: ASUSTekC_cc:d0:98 (08:60:6e:cc:d0:98)
 Internet Protocol Version 4, Src: 192.168.1.209, Dst: 192.168.1.1
 User Datagram Protocol, Src Port: 57547, Dst Port: 53
 Domain Name System (query)

Цільовий порт: 53

Вихідний порт: 57547

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

IP: 192.168.1.1. Так є.

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

Цей запит – є запитом стандартного типу. Вміщує.

[\[Response In: 7\]](#)

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

Transaction ID: 0x8f1f

- Flags: 0x8180 Standard query response, No error
- Questions: 1
- Answer RRs: 2
- Authority RRs: 0
- Additional RRs: 0
- Queries
- ▼ Answers
 - www.ntv.ru: type A, class IN, addr 185.129.100.136
 - www.ntv.ru: type A, class IN, addr 185.129.100.151

[\[Request In: 4\]](#)
[Time: 0.003212000 seconds]

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 співпадає.

SamsungE_6d:91:d5	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.210
192.168.1.209	192.168.1.1	DNS	72	Standard query 0x2f6c A www.vesti.ru
192.168.1.209	192.168.1.1	DNS	70	Standard query 0x8f1f A www.ntv.ru
ASUSTekC_cc:d0:9c	Spanning-tree-(for...	STP	52	Conf. Root = 32768/0/08:60:6e:cc:d0:98 Cost = 0 Port = 0x8003
192.168.1.1	192.168.1.209	DNS	88	Standard query response 0x2f6c A www.vesti.ru A 80.247.32.208
192.168.1.1	192.168.1.209	DNS	102	Standard query response 0x8f1f A www.ntv.ru A 185.129.100.136 A 185.129.100.151
192.168.1.209	80.247.32.208	TCP	78	64020 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=365304752 TSecr=0
192.168.1.209	185.129.100.136	TCP	78	64022 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=365304753 TSecr=0
185.129.100.136	192.168.1.209	TCP	74	80 → 64022 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1380 SACK_PERM=1 TSval=365304808 TSecr=3838441261
192.168.1.209	185.129.100.136	TCP	66	64022 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=365304808 TSecr=3838441261
192.168.1.209	185.129.100.136	HTTP	390	GET / HTTP/1.1
185.129.100.136	192.168.1.209	TCP	66	80 → 64022 [ACK] Seq=1 Ack=325 Win=30080 Len=0 TSval=3838441316 TSecr=365304808
185.129.100.136	192.168.1.209	HTTP	459	HTTP/1.1 301 Moved Permanently (text/html)
192.168.1.209	185.129.100.136	TCP	66	64022 → 80 [ACK] Seq=325 Ack=394 Win=130880 Len=0 TSval=365304863 TSecr=3838441316

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

Так виконує.

72	Standard query 0x2f6c A www.vesti.ru
70	Standard query 0x8f1f A www.ntv.ru
88	Standard query response 0x2f6c A www.vesti.ru A 80.247.32.208
102	Standard query response 0x8f1f A www.ntv.ru A 185.129.100.136 A 185.129.100.151
77	Standard query 0x3493 A status.thawte.com
153	Standard query response 0x3493 A status.thawte.com CNAME ocsdp.digicert.com CNAME c...
71	Standard query 0x9b8e A img2.ntv.ru
103	Standard query response 0x9b8e A img2.ntv.ru A 185.129.100.129 A 185.129.100.145
71	Standard query 0x73a0 A www.ozon.ru
121	Standard query response 0x73a0 A www.ozon.ru CNAME yi3vg.x.incapdns.net A 45.60.40...
80	Standard query 0x65b3 A www.odnoklassniki.ru
80	Standard query response 0x65b3 Server failure A www.odnoklassniki.ru
72	Standard query 0x41a5 A www.ietf.org
149	Standard query response 0x41a5 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.ne...
78	Standard query 0xe0ee A analytics.ietf.org
78	Standard query 0xe0ee A analytics.ietf.org
108	Standard query response 0xe0ee A analytics.ietf.org CNAME ietf.org A 4.31.198.44
79	Standard query 0x89a6 A iphone-wu.apple.com
153	Standard query response 0x89a6 A iphone-wu.apple.com CNAME wu.apple.com.akadns.net...

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

Цільовий: 192.168.1.1

Вихідний: 192.168.1.209

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

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

Цей запит – є запитом стандартного типу. Вміщує.

► **Flags:** 0x0100 Standard (Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0

► **Queries**
[Response In: 6]

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

```
Transaction ID: 0x90c3
► Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
► Queries
▼ 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 104.87.213.214
[Request In: 5]
[Time: 0.018340000 seconds]
```

```
0000 b8 e8 56 2f ad e0 08 60 6e cc d0 98 08 00 45 00 ..V/...`n.....E.
0010 00 92 00 00 40 00 40 11 b6 38 c0 a8 01 01 c0 a8 ...@...8.....
0020 01 d1 00 35 d9 b6 00 7e 95 35 90 c3 81 80 00 01 ...5...~.5.....
0030 00 03 00 00 00 00 03 77 77 77 03 6d 69 74 03 65 ...www.mit·e
0040 64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 05 du.....
0050 7f 00 19 03 77 77 77 03 6d 69 74 03 65 64 75 07 ...www·mit·edu·
0060 65 64 67 65 6b 65 79 03 6e 65 74 00 c0 29 00 05 edgekey·net·)·
0070 00 01 00 00 00 3c 00 18 05 65 39 35 36 36 04 64 .....<...e9566·d
0080 73 63 62 0a 61 6b 61 6d 61 69 65 64 67 65 c0 3d scb·akam aledge·=
0090 c0 4e 00 01 00 01 00 00 00 14 00 04 68 57 d5 d6 ·N..... ···hw·
```

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

IP: 192.168.1.1. Так є.

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

Стандартний тип запиту. Так вміщує.

- Transaction ID: 0x9d8e
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
- [\[Response In: 14\]](#)

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?

```

► Frame 14: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface en0, id 0
► Ethernet II, Src: ASUSTekC_cc:d0:98 (08:60:6e:cc:d0:98), Dst: Apple_2f:ad:e0 (b8:e8:56:2f:ad:e0)
► Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.209
► User Datagram Protocol, Src Port: 53, Dst Port: 52678
▼ Domain Name System (response)
  Transaction ID: 0x9d8e
  ► Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ► Queries
  ▼ Answers
    ► mit.edu: type A, class IN, addr 88.221.9.235
    \[Request In: 13\]
    [Time: 0.046954000 seconds]

```

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?

IP: 192.168.1.1. є адресою локального сервера.

```

► Frame 3: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface en0, id 0
► Ethernet II, Src: Apple_2f:ad:e0 (b8:e8:56:2f:ad:e0), Dst: ASUSTekC_cc:d0:98 (08:60:6e:cc:d0:98)
► Internet Protocol Version 4, Src: 192.168.1.209, Dst: 192.168.1.1
► User Datagram Protocol, Src Port: 58319, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x9043
  ► Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ► Queries
    \[Response In: 4\]

```

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

Стандартний тип запиту. вміщує.

Transaction ID: 0x9043
► Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
► Queries
[\[Response In: 4\]](#)

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

Transaction ID: 0x9043
► 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
[\[Request In: 3\]](#)
[Time: 0.047087000 seconds]

Висновок

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи DNS та було проведено аналіз деталей роботи даних протоколів.