

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

**Практична робота №3
з курсу «Комп'ютерні мережі»**

Протокол DNS

**Виконав: студент 3 курсу
групи КА-74
Коваленко М.Д.
Прийняв: Кухарєв С.О.**

Київ – 2020р.

1. Очищено кеш DNS-записів

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.720]
(c) Корпорація Майкрософт (Microsoft Corporation), 2019. Усі права захищено.

C:\Users\Maria>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Maria>
```

Пакети

запит:

```
No.      Time          Source          Destination      Protocol Length Info
 2 0.030998      192.168.0.101    192.168.0.1      DNS              81      Standard query 0x50bb A developer.mozilla.org
Frame 2: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{2A724C26-154F-4708-A6B9-B9786A7A462A}, id 0
Ethernet II, Src: IntelCor_e3:95:22 (a0:c5:89:e3:95:22), Dst: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 63601, Dst Port: 53
  Source Port: 63601
  Destination Port: 53
  Length: 47
  Checksum: 0xc5c0 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
Domain Name System (query)
  Transaction ID: 0x50bb
  Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    ....0. .... = Truncated: Message is not truncated
    ....1. .... = Recursion desired: Do query recursively
    ....0. .... = Z: reserved (0)
    ....0. .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
  [Retransmitted request. Original request in: 1]
  [Retransmission: True]
```

ВІДПОВІДЬ:

```
No.      Time          Source          Destination      Protocol Length Info
 3 0.034507      192.168.0.1      192.168.0.101    DNS             188      Standard query response 0x50bb A
developer.mozilla.org CNAME d1avawhigh9uo1.cloudfront.net A 13.33.18.245 A 13.33.18.24 A 13.33.18.36 A 13.33.18.120
Frame 3: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits) on interface \Device\NPF_{2A724C26-154F-4708-A6B9-B9786A7A462A}, id 0
Ethernet II, Src: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0), Dst: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
User Datagram Protocol, Src Port: 53, Dst Port: 63601
  Source Port: 53
  Destination Port: 63601
  Length: 154
  Checksum: 0xa27d [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
Domain Name System (response)
  Transaction ID: 0x50bb
  Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    ....0. .... = Authoritative: Server is not an authority for domain
    ....0. .... = 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
    ....0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 5
  Authority RRs: 0
  Additional RRs: 0
  Queries
  Answers
  [Request In: 1]
  [Time: 0.034507000 seconds]
```

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?

Використовують протокол UDP, номер цільового порта - 53, вихідного - 63601

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

Відправлено на адресу 192.168.0.1, що є адресою локального сервера DNS

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

```
▼ Queries
  > developer.mozilla.org: type A, class IN
  [Retransmitted request. Original request in: 1]
```

Тип A. Вміщує деякі можливі компоненти «відповіді»

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

Було отримано такі відповіді:

```
▼ Answers
  > developer.mozilla.org: type CNAME, class IN, cname d1avawhiqh9uo1.cloudfront.net
  > d1avawhiqh9uo1.cloudfront.net: type A, class IN, addr 13.33.18.245
  > d1avawhiqh9uo1.cloudfront.net: type A, class IN, addr 13.33.18.24
  > d1avawhiqh9uo1.cloudfront.net: type A, class IN, addr 13.33.18.36
  > d1avawhiqh9uo1.cloudfront.net: type A, class IN, addr 13.33.18.120
```

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?

Ні, не співпадає:

tcp syn: 13.33.18.245 dns: 192.168.0.101

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

Так, виконує:

Protocol	Length	Info
DNS	81	Standard query 0x50bb A developer.mozilla.org
DNS	81	Standard query 0x50bb A developer.mozilla.org
DNS	188	Standard query response 0x50bb A developer.mozilla.org CNAME d1avawhiqh9uo1.cloudfront.net A ...
DNS	89	Standard query 0xfa71 A d1avawhiqh9uo1.cloudfront.net
DNS	188	Standard query response 0x50bb A developer.mozilla.org CNAME d1avawhiqh9uo1.cloudfront.net A ...
DNS	89	Standard query 0xfa71 A d1avawhiqh9uo1.cloudfront.net
DNS	153	Standard query response 0xfa71 A d1avawhiqh9uo1.cloudfront.net A 13.33.18.36 A 13.33.18.120 A...
DNS	153	Standard query response 0xfa71 A d1avawhiqh9uo1.cloudfront.net A 13.33.18.120 A 13.33.18.24 A...
DNS	75	Standard query 0x331f A www.mozilla.org
DNS	155	Standard query response 0x331f A www.mozilla.org CNAME www.mozilla.org.cdn.cloudflare.net A 1...
DNS	94	Standard query 0x5490 A www.mozilla.org.cdn.cloudflare.net
DNS	94	Standard query 0x5490 A www.mozilla.org.cdn.cloudflare.net
DNS	126	Standard query response 0x5490 A www.mozilla.org.cdn.cloudflare.net A 104.16.142.228 A 104.16...
DNS	126	Standard query response 0x5490 A www.mozilla.org.cdn.cloudflare.net A 104.16.142.228 A 104.16...

2. Виконання команди nslookup www.mit.edu

```
C:\Users\Maria>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
           23.61.218.91
Aliases: www.mit.edu
         www.mit.edu.edgekey.net
```

Пакети

Запит:

```
No.      Time          Source          Destination      Protocol Length Info
 109 23.093949    192.168.0.101   192.168.0.1      DNS              71      Standard query 0x0003 AAAA www.mit.edu
Frame 109: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{2A724C26-154F-4708-A6B9-B9786A7A462A},
id 0
Ethernet II, Src: IntelCor_e3:95:22 (a0:c5:89:e3:95:22), Dst: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
  Destination: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
  Address: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
  .... 0. .... = LG bit: Globally unique address (factory default)
  .... 0. .... = IG bit: Individual address (unicast)
Source: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
  Address: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
  .... 0. .... = LG bit: Globally unique address (factory default)
  .... 0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 57
  Identification: 0x6a87 (27271)
  Flags: 0x0000
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0x4e76 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.101
  Destination: 192.168.0.1
User Datagram Protocol, Src Port: 62432, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x0003
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.mit.edu: type AAAA, class IN
[Response In: 112]
```


ВІДПОВІДЬ:

```
No.    Time          Source           Destination      Protocol Length Info
112 23.145087      192.168.0.1      192.168.0.101    DNS             200      Standard query response 0x0003 AAAA www.mit.edu
CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:d200:19e::255e AAAA 2a02:26f0:d200:191::255e
Frame 112: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{2A724C26-154F-4708-A6B9-B9786A7A462A}, id 0
Ethernet II, Src: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0), Dst: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
  Destination: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
    Address: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
      .... 0. .... = LG bit: Globally unique address (factory default)
      .... 0. .... = IG bit: Individual address (unicast)
  Source: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
    Address: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
      .... 0. .... = LG bit: Globally unique address (factory default)
      .... 0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 186
  Identification: 0xe48b (58507)
  Flags: 0x0000
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 121
  Protocol: UDP (17)
  Header checksum: 0xdaf0 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.1
  Destination: 192.168.0.101
User Datagram Protocol, Src Port: 53, Dst Port: 62432
Domain Name System (response)
  Transaction ID: 0x0003
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.mit.edu: type AAAA, class IN
  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 AAAA, class IN, addr 2a02:26f0:d200:19e::255e
    e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:191::255e
[Request In: 109]
[Time: 0.051138000 seconds]
```

Контрольні запитання

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

цільовий порт із запитом: 53, вихідний порт із відповіддю: 53

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

на адресу 192.168.0.1 Так, є

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

▼ Queries

➤ www.mit.edu: type AAAA, class IN

[\[Response In: 112\]](#)

Тип AAAA . Так, вміщує

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

Отримано такі відповіді з наступним складом:

```
▼ 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 AAAA, class IN, addr 2a02:26f0:d200:19e::255e
> e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:191::255e
```

3. Виконання команди nslookup -type=NS mit.edu

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

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

Пакети

запиту:

```
No.      Time           Source           Destination      Protocol Length Info
 75 22.801425    192.168.0.101    192.168.0.1      DNS              67      Standard query 0x0002 NS mit.edu
Frame 75: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{2A724C26-154F-4708-A6B9-B9786A7A462A}, id 0
Ethernet II, Src: IntelCor_e3:95:22 (a0:c5:89:e3:95:22), Dst: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
  Destination: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
  Address: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Source: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
  Address: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 53
  Identification: 0x6afe (27390)
  Flags: 0x0000
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0x4e03 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.101
  Destination: 192.168.0.1
User Datagram Protocol, Src Port: 55923, 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
    mit.edu: type NS, class IN
  [Response In: 76]
```

ВІДПОВІДІ:

```
(Response: 76)
No.    Time           Source            Destination      Protocol Length Info
 76 22.833303      192.168.0.1      192.168.0.101   DNS             234    Standard query response 0x0002 NS mit.edu NS
asia2.akam.net NS use5.akam.net NS asia1.akam.net NS ns1-37.akam.net NS ns1-173.akam.net NS eur5.akam.net NS usw2.akam.net NS
use2.akam.net
Frame 76: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{2A724C26-154F-4708-A6B9-
B9786A7A462A}, id 0
Ethernet II, Src: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0), Dst: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
  Destination: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
    Address: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
    Address: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 220
  Identification: 0x2a1b (10779)
  Flags: 0x0000
  ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 121
  Protocol: UDP (17)
  Header checksum: 0x953f [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.0.1
  Destination: 192.168.0.101
User Datagram Protocol, Src Port: 53, Dst Port: 55923
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 asia2.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 ns1-37.akam.net
    mit.edu: type NS, class IN, ns ns1-173.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 use2.akam.net
[Request In: 75]
[Time: 0.031878000 seconds]
```

Контрольні запитання

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

На адресу 192.168.0.1 Так,є

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

▼ Queries

> mit.edu: type NS, class IN

[\[Response In: 76\]](#)

Тип NS. Так, вміщує

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?

Були запропоновані за допомогою доменного імені наступні сервери:

▼ Answers

```
> mit.edu: type NS, class IN, ns asia2.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 ns1-37.akam.net
> mit.edu: type NS, class IN, ns ns1-173.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 use2.akam.net
```

4. Виконуємо команду nslookup www.aiit.or.kr bitsy.mit.edu

```
C:\Users\Maria>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:\Users\Maria>
```

Пакети

запиту:

No.	Time	Source	Destination	Protocol	Length	Info
158	43.287851	192.168.0.101	192.168.0.1	DNS	73	Standard query 0x82a7 A bitsy.mit.edu

Frame 158: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{2A724C26-154F-4708-A6B9-B9786A7A462A}, id 0

Ethernet II, Src: IntelCor_e3:95:22 (a0:c5:89:e3:95:22), Dst: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)

Destination: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)

Address: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0. = IG bit: Individual address (unicast)

Source: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)

Address: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 59

Identification: 0x6b24 (27428)

Flags: 0x0000

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 128

Protocol: UDP (17)

Header checksum: 0x4dd7 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.101

Destination: 192.168.0.1

User Datagram Protocol, Src Port: 55471, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x82a7

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

bitsy.mit.edu: type A, class IN

[Response In: 160]

ВІДПОВІДІ:

No.	Time	Source	Destination	Protocol	Length	Info
160	43.320975	192.168.0.1	192.168.0.101	DNS	89	Standard query response 0x82a7 A bitsy.mit.edu A 18.0.72.3

Frame 160: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{2A724C26-154F-4708-A6B9-B9786A7A462A}, id 0

Ethernet II, Src: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0), Dst: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)

Destination: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)

Address: IntelCor_e3:95:22 (a0:c5:89:e3:95:22)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0. = IG bit: Individual address (unicast)

Source: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)

Address: Tp-LinkT_92:78:a0 (10:fe:ed:92:78:a0)

.... ..0. = LG bit: Globally unique address (factory default)

.... ..0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 75

Identification: 0xe6a6 (59046)

Flags: 0x0000

...0 0000 0000 0000 = Fragment offset: 0

Time to live: 121

Protocol: UDP (17)

Header checksum: 0xd944 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.0.1

Destination: 192.168.0.101

User Datagram Protocol, Src Port: 53, Dst Port: 55471

Domain Name System (response)

Transaction ID: 0x82a7

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

bitsy.mit.edu: type A, class IN

Answers

bitsy.mit.edu: type A, class IN, addr 18.0.72.3

[Request In: 158]

[Time: 0.033124000 seconds]

Контрольні запитання

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?

На адресу 192.168.0.1 Так, є

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

```
▼ Queries
  > bitsy.mit.edu: type A, class IN
    [Response In: 160]
```

Тип A. Так, вміщує

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

Отримана наступна відповідь:

```
▼ 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: 1381 (23 minutes, 1 second)
    Data length: 4
    Address: 18.0.72.3
```

Висновки: Під час виконання лабораторної роботи було розглянуто та проаналізовано деталі роботи протоколу DNS та покращено навички роботи у програмі Wireshark для захоплення пакетів.