

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

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

**Виконала: студентка 3 курсу
групи КА-73
Федоренко А. П.
Прийняв: Кухарєв С.О.**

REQUEST

Frame 28: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface
\\Device\\NPF_{CC431E3D-E278-4CA9-8757-FF32C2AC82FE}, id 0
Ethernet II, Src: RivetNet_6b:7b:13 (9c:b6:d0:6b:7b:13), Dst: Tp-LinkT_50:ec:fe
(c4:71:54:50:ec:fe)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 58447, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xcfa5

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

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: 34]

ANSWER

Frame 34: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface
\\Device\\NPF_{CC431E3D-E278-4CA9-8757-FF32C2AC82FE}, id 0
Ethernet II, Src: Tp-LinkT_50:ec:fe (c4:71:54:50:ec:fe), Dst: RivetNet_6b:7b:13
(9c:b6:d0:6b:7b:13)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 58447

Domain Name System (response)

Transaction ID: 0xcfa5

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: 3

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)

Answers

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: 210 (3 minutes, 30 seconds)

Data length: 33

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

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: 209 (3 minutes, 29 seconds)

Data length: 4

Address: 104.20.1.85

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: 209 (3 minutes, 29 seconds)

Data length: 4

Address: 104.20.0.85

[Request In: 28]

[Time: 0.006986000 seconds]

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?

UDP

номер цільового порта запиту DNS - 53

номер вихідного порта відповіді DNS – 53

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

192.168.0.103

Так

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

Type: A (Host Address) (1)

Ні

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

Три

Name, Type, Class, Time to live, Data length, CNAME

Name, Type, Class, Time to live, Data length, Address

Name, Type, Class, Time to live, Data length, Address

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?

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 104.20.1.85

Так

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

Так

C:\Users\Роман>nslookup www.mit.edu

== x È т x È: UnKnown

Address: 192.168.0.1

Не заслуживающий доверия ответ:

↳ : e9566.dscb.akamaiedge.net

Addresses: 2a02:26f0:d8:389::255e

2a02:26f0:d8:3a2::255e

104.96.143.80

Aliases: www.mit.edu

www.mit.edu.edgekey.net

REQUEST

Frame 11: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface

\Device\NPF_{CC431E3D-E278-4CA9-8757-FF32C2AC82FE}, id 0

Ethernet II, Src: RivetNet_6b:7b:13 (9c:b6:d0:6b:7b:13), Dst: Tp-LinkT_50:ec:fe (c4:71:54:50:ec:fe)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 57974, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0003

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

www.mit.edu: type AAAA, class IN

Name: www.mit.edu

[Name Length: 11]

[Label Count: 3]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

[Response In: 13]

ANSWER

Frame 13: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface

\Device\NPF_{CC431E3D-E278-4CA9-8757-FF32C2AC82FE}, id 0

Ethernet II, Src: Tp-LinkT_50:ec:fe (c4:71:54:50:ec:fe), Dst: RivetNet_6b:7b:13 (9c:b6:d0:6b:7b:13)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 57974

Domain Name System (response)

Transaction ID: 0x0003

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: 4

Authority RRs: 0

Additional RRs: 0

Queries

www.mit.edu: type AAAA, class IN

Name: www.mit.edu

[Name Length: 11]

[Label Count: 3]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Answers

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: 300 (5 minutes)

Data length: 25

CNAME: www.mit.edu.edgekey.net

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: 24

CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d8:3a2::255e
Name: e9566.dscb.akamaiedge.net
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 20 (20 seconds)
Data length: 16
AAAA Address: 2a02:26f0:d8:3a2::255e
e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d8:389::255e
Name: e9566.dscb.akamaiedge.net
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 20 (20 seconds)
Data length: 16
AAAA Address: 2a02:26f0:d8:389::255e

[Request In: 11]

[Time: 0.162406000 seconds]

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

цільовий порт повідомлення із запитом DNS - 53

вихідний порт повідомлення із відповіддю DNS – 53

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

192.168.0.1

Так

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

Type: AAAA (IPv6 Address) (28)

Ні

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

4

Name, Type, Class, Time to live, Data length, CNAME

Name, Type, Class, Time to live, Data length, CNAME

Name, Type, Class, Time to live, Data length, AAAA Address

Name, Type, Class, Time to live, Data length, AAAA Address

```
C:\Users\Роман>nslookup -type=NS mit.edu
= x È т x È: UnKnown
Address: 192.168.0.1
```

Не заслуживающий доверия ответ:
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net

REQUEST

Frame 9: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface
\Device\NPF_{CC431E3D-E278-4CA9-8757-FF32C2AC82FE}, id 0
Ethernet II, Src: RivetNet_6b:7b:13 (9c:b6:d0:6b:7b:13), Dst: Tp-LinkT_50:ec:fe
(c4:71:54:50:ec:fe)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 57976, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0002

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

mit.edu: type NS, class IN

Name: mit.edu

[Name Length: 7]

[Label Count: 2]

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

[Response In: 10]

ANSWER

Frame 10: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface
\\Device\\NPF_{CC431E3D-E278-4CA9-8757-FF32C2AC82FE}, id 0

Ethernet II, Src: Tp-LinkT_50:ec:fe (c4:71:54:50:ec:fe), Dst: RivetNet_6b:7b:13
(9c:b6:d0:6b:7b:13)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 57976

Domain Name System (response)

Transaction ID: 0x0002

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: 8

Authority RRs: 0

Additional RRs: 0

Queries

mit.edu: type NS, class IN

Name: mit.edu

[Name Length: 7]

[Label Count: 2]

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Answers

mit.edu: type NS, class IN, ns use5.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 15

Name Server: use5.akam.net

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

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 7

Name Server: use2.akam.net

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

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 7

Name Server: eur5.akam.net

mit.edu: type NS, class IN, ns ns1-173.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 10

Name Server: ns1-173.akam.net

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: 300 (5 minutes)

Data length: 8

Name Server: asia1.akam.net

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

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 8

Name Server: asia2.akam.net

mit.edu: type NS, class IN, ns ns1-37.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 300 (5 minutes)

Data length: 9
Name Server: ns1-37.akam.net
mit.edu: type NS, class IN, ns usw2.akam.net
Name: mit.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 7
Name Server: usw2.akam.net
[Request In: 9]
[Time: 0.071277000 seconds]

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

192.168.0.1

Так

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

Type: NS (authoritative Name Server) (2)

Ні

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?

8

use5.akam.net

use2.akam.net

eur5.akam.net

ns1-173.akam.net

asia1.akam.net

asia2.akam.net

ns1-37.akam.net

usw2.akam.net

Лише за допомогою доменного імені

C:\Users\Роман>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)

⌘ x È T x È: UnKnown

Address: 18.0.72.3

ℒ Б : www.aiit.or.kr

Address: 194.50.85.176

REQUEST

Frame 10: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface
\\Device\\NPF_{CC431E3D-E278-4CA9-8757-FF32C2AC82FE}, id 0

Ethernet II, Src: RivetNet_6b:7b:13 (9c:b6:d0:6b:7b:13), Dst: Tp-LinkT_50:ec:fe
(c4:71:54:50:ec:fe)

Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 56660, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0900

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

bitsy.mit.edu: type A, class IN

Name: bitsy.mit.edu

[Name Length: 13]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 13]

ANSWER

Frame 13: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface
\\Device\\NPF_{CC431E3D-E278-4CA9-8757-FF32C2AC82FE}, id 0

Ethernet II, Src: Tp-LinkT_50:ec:fe (c4:71:54:50:ec:fe), Dst: RivetNet_6b:7b:13
(9c:b6:d0:6b:7b:13)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 56660

Domain Name System (response)

Transaction ID: 0x0900

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: 1

Authority RRs: 0

Additional RRs: 0

Queries

bitsy.mit.edu: type A, class IN

Name: bitsy.mit.edu

[Name Length: 13]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

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: 300 (5 minutes)

Data length: 4

Address: 18.0.72.3
[Request In: 10]
[Time: 0.035832000 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?

Спочатку на локальний сервер 192.168.0.1, а потім на 18.0.72.3 (bitsy.mit.edu)

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

Type: A (Host Address) (1)

Ні

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

1

Name, Type, Class, Time to live, Data length, Address

Висновок: після завершення 4 завдань, які склалися з виконання запитів, було проведено аналіз протоколу DNS