

**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»**

Виконав: студентки 3 курсу

групи КА-63

Ярошенко В.О.

Прийняв: Кухарєв С.О.

Київ-2020

1281 17.620136 192.168.11 192.168.1.1 DNS 68 Standard query 0x73b3 A ietf.org

Frame 1281: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
 Ethernet II, Src: IntelCor_7f:48:fb(f8:16:54:7f:48:fb), Dst: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c)
 Internet Protocol Version 4, Src: 192.168.11, Dst: 192.168.1.1
 User Datagram Protocol, Src Port: 52751, Dst Port: 53
 Domain Name System (query)
 [Response In: 1282]
 Transaction ID: 0x73b3
 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
 ietf.org: type A, class IN

1282 17.622607 192.168.1.1 192.168.11 DNS 84 Standard query response 0x73b3 A ietf.org A 4.31.198.44

Frame 1282: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
 Ethernet II, Src: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c), Dst: IntelCor_7f:48:fb(f8:16:54:7f:48:fb)
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.11
 User Datagram Protocol, Src Port: 53, Dst Port: 52751
 Domain Name System (response)
 [Request In: 1281]
 [Time: 0.002471000 seconds]
 Transaction ID: 0x73b3
 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
 ietf.org: type A, class IN
 Name: ietf.org
 [Name Length: 8]
 [Label Count: 2]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Answers
 ietf.org: type A, class IN, addr 4.31.198.44
 Name: ietf.org
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 3600
 Data length: 4
 Address: 4.31.198.44

291 14.680285 192.168.11 77.222.148.105 TCP 66 49435 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

Frame 291: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Ethernet II, Src: IntelCor_7f:48:fb(f8:16:54:7f:48:fb), Dst: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c)
 Internet Protocol Version 4, Src: 192.168.11, Dst: 77.222.148.105
 Transmission Control Protocol, Src Port: 49435, Dst Port: 80, Seq: 0, Len: 0
 Source Port: 49435
 Destination Port: 80
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 0 (relative sequence number)
 Acknowledgment number: 0
 1000= Header Length: 32 bytes (8)
 Flags: 0x002 (SYN)
 Window size value: 8192
 [Calculated window size: 8192]
 Checksum: 0x543c [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

7-10

Не заслуживающий доверия ответ:

ℒ : e9566.dscb.akamaiedge.net

Addresses: 2a02:26f0:41:586::255e

2a02:26f0:41:593::255e

23.61.235.184

Aliases: www.mit.edu

www.mit.edu.edgekey.net

**65 3.447474 192.168.11 192.168.1.1 DNS 71 Standard query 0x0002 A
www.mit.edu**

Frame 65: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
 Ethernet II, Src: IntelCor_7f:48:fb(f8:16:54:7f:48:fb), Dst: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c)
 Internet Protocol Version 4, Src: 192.168.11, Dst: 192.168.1.1
 User Datagram Protocol, Src Port: 54848, Dst Port: 53
 Domain Name System (query)

[Response In: 66]
 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

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)

Frame 66: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
Ethernet II, Src: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c), Dst: IntelCor_7f:48:fb(f8:16:54:7f:48:fb)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.11
User Datagram Protocol, Src Port: 53, Dst Port: 54848
Domain Name System (response)

[Request In: 65]

[Time: 0.008994000 seconds]

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: 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

Name: www.mit.edu

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

Class: IN (0x0001)

Time to live: 3144

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: 2952

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 23.61.235.184

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 2952

Data length: 4

Address: 23.61.235.184

11-13

C:\Users\ASUS>nslookup -type=NS mit.edu

my.totolink.net

Address: 192.168.1.1

Не заслуживающий доверия ответ:

mit.edu nameserver = eur5.akam.net

mit.edu nameserver = asia2.akam.net

mit.edu nameserver = use5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = ns1-37.akam.net

6 1.958137 192.168.11 192.168.1.1 DNS 67 Standard query 0x0002 NS mit.edu

Frame 6: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: IntelCor_7f:48:fb(f8:16:54:7f:48:fb), Dst: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c)
Internet Protocol Version 4, Src: 192.168.11, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 49319, Dst Port: 53
Domain Name System (query)

[Response In: 7]
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)

7 1.960704 192.168.1.1 192.168.11 DNS 234 Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS asia2.akam.net NS use5.akam.net NS eur5.akam.net NS use2.akam.net NS ns1-173.akam.net NS asia1.akam.net NS ns1-37.akam.net

Frame 7: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0
Ethernet II, Src: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c), Dst: IntelCor_7f:48:fb(f8:16:54:7f:48:fb)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.11
User Datagram Protocol, Src Port: 53, Dst Port: 29592
Domain Name System (response)

[Request In: 5]

[Time: 0.019670000 seconds]

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: 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 eur5.akam.net
Name: mit.edu
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 262
Data length: 15
Name Server: eur5.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: 262
Data length: 8
Name Server: asia2.akam.net

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: 262
Data length: 7
Name Server: use5.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: 262
Data length: 8
Name Server: asia1.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: 262
Data length: 7
Name Server: use2.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: 262
Data length: 10
Name Server: ns1-173.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: 262
Data length: 7
Name Server: usw2.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: 262
Data length: 9
Name Server: ns1-37.akam.net

16-18

C:\Users\ASUS>nslookup www.aiit.or.kr bitsy.mit.edu

DNS request timed out.

timeout was 2 seconds.

⌘xËtxË: UnKnown

Address: 18.72.0.3

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.

*** Превышено время ожидания запроса UnKnown

43 3.168578 192.168.11 192.168.1.1 DNS 73 Standard query 0xc881 A bitsy.mit.edu

Frame 43: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

Ethernet II, Src: IntelCor_7f:48:fb(f8:16:54:7f:48:fb), Dst: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c)

Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 55707, Dst Port: 53

Domain Name System (query)

[Response In: 44]

Transaction ID: 0xc881

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)

44 3.170732 192.168.1.1 192.168.11 DNS 89 Standard query response 0xc881 A bitsy.mit.edu A 18.72.0.3

Frame 44: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0

Ethernet II, Src: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c), Dst: IntelCor_7f:48:fb(f8:16:54:7f:48:fb)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.11

User Datagram Protocol, Src Port: 53, Dst Port: 55707

Domain Name System (response)

[Request In: 43]

[Time: 0.002154000 seconds]

Transaction ID: 0xc881

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 18.72.0.3
    Name: bitsy.mit.edu
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 3441
    Data length: 4
    Address: 18.72.0.3

```

**45 3.172932 192.168.11 18.72.0.3 DNS 82 Standard query 0x0001 PTR
3.0.72.18.in-addr.arpa**

```

Frame 45: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Ethernet II, Src: IntelCor_7f:48:fb(f8:16:54:7f:48:fb), Dst: ZioncomE_f8:a0:3c (78:44:76:f8:a0:3c)
Internet Protocol Version 4, Src: 192.168.11, Dst: 18.72.0.3
User Datagram Protocol, Src Port: 55708, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x0001
  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
    3.0.72.18.in-addr.arpa: type PTR, class IN
      Name: 3.0.72.18.in-addr.arpa
      [Name Length: 22]
      [Label Count: 6]
      Type: PTR (domain name PoinTeR) (12)
      Class: IN (0x0001)

```

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?

UDP, Цільовий порт запиту –53, вихідний порт - 52751.

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

192.168.1.1 , так.

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

Типу A (Host address). Ні

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

Одна, 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?

Ні.

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

Так.

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

Цільовий порт запиту – 53, вихідний порт – 54848

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.

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

Типу A (Host address). Ні

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

Name, Type, Class, Time to live, Data length, CNAME/Address.

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

192.168.1.1 , так.

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

Типу NS (authoritative Name Server). 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 штук(asia1.akam.net, eur5.akam.net, usw2.akam.net, ns1-37.akam.net, asia2.akam.net, ns1-173.akam.net, use2.akam.net, use5.akam.net). Лише за допомогою доменного імені.

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 192.168.1.1, а потім на 18.72.0.3

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

Типу A (Host address) та типу PTR (domain name PoinTeR). Ні

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

1 відповідь. . Name, Type, Class, Time to live, Data length, Address

Висновки

Під час виконання цієї лабораторної роботи я навчилась аналізувати деталі роботи протоколу Системи Доменних імен(DNS), що переводить імена хостів в IP-адреси. Також я дізналась, що TLD «.tv» не відноситься до ТВ-індустрії, а є національним доменом верхнього рівня (ccTLD) для Тувалу.