

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»**

**КАФЕДРА ММСА**

**Лабораторна робота № 3**

**З дисципліни: Комп’ютерні мережі**

***Основи захоплення та аналізу пакетів***

**Виконаd:**

**Студент ІII курсу**

**Групи КА-74**

**Таровський Б. Є.**

**Перевірив: Кухарєв С. О.**

**Київ 2020**

**Lab3\_Task1**

No. Time Source Destination Protocol Length Info

13 4.914603 192.168.0.102 192.168.0.1 DNS 72 Standard query 0xdb9c A www.ietf.org

Frame 13: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 61378, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xdb9c

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: 14]

No. Time Source Destination Protocol Length Info

14 5.035556 192.168.0.1 192.168.0.102 DNS 149 Standard query response 0xdb9c A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85

Frame 14: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a), Dst: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.102

User Datagram Protocol, Src Port: 53, Dst Port: 61378

Domain Name System (response)

Transaction ID: 0xdb9c

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: 300

Data length: 33

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

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: 300

Data length: 4

Address: 104.20.0.85

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: 300

Data length: 4

Address: 104.20.1.85

[Request In: 13]

[Time: 0.120953000 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, Цільовий порт запиту –53, вихідний порт - 61378.

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

192.168.0.102, 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?**

Три, Name, Type, Class, Time to live, Data length, Adress.

**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.

**6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які**

**використовує документ, що отримав браузер?**

Так.

**Lab3\_Task2**

**C:\Users\Roman>nslookup www.mit.edu**

**Server: UnKnown**

**Address: 192.168.0.1**

**Non-authoritative answer:**

**Name: e9566.dscb.akamaiedge.net**

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

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

**104.96.94.247**

**Aliases: www.mit.edu**

[**www.mit.edu.edgekey.net**](http://www.mit.edu.edgekey.net)

No. Time Source Destination Protocol Length Info

224 21.679629 192.168.0.102 192.168.0.1 DNS 71 Standard query 0x0002 A www.mit.edu

Frame 224: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 57578, 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

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 [Response In: 226]

No. Time Source Destination Protocol Length Info

226 21.735811 192.168.0.1 192.168.0.102 DNS 160 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.96.94.247

Frame 226: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a), Dst: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.102

User Datagram Protocol, Src Port: 53, Dst Port: 57578

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: 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: 261

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

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.94.247

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20

Data length: 4

Address: 104.96.94.247

[Request In: 224]

[Time: 0.056182000 seconds]

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

**повідомлення із відповіддю DNS?**

Цільовий порт запиту – 53, вихідний порт – 57578.

**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»?**

Типу A (Host address). Ні

**10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було**

**запропоновано сервером? З ч ого складається кожна із цих відповідей?**

3 відповіді, . Name, Type, Class, Time to live, Data length, CNAME/Adress.

**Lab3\_Task3**

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

Server: UnKnown

Address: 192.168.0.1

Non-authoritative answer:

mit.edu nameserver = ns1-37.akam.net

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

mit.edu nameserver = eur5.akam.net

mit.edu nameserver = asia2.akam.net

mit.edu nameserver = use2.akam.net

mit.edu nameserver = use5.akam.net

mit.edu nameserver = asia1.akam.net

mit.edu nameserver = usw2.akam.net

No. Time Source Destination Protocol Length Info

36 6.017053 192.168.0.102 192.168.0.1 DNS 67 Standard query 0x0002 NS mit.edu

Frame 36: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 59307, 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: 37]

No. Time Source Destination Protocol Length Info

37 6.020219 192.168.0.1 192.168.0.102 DNS 234 Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS ns1-173.akam.net NS eur5.akam.net NS asia2.akam.net NS use2.akam.net NS use5.akam.net NS asia1.akam.net NS usw2.akam.net

Frame 37: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a), Dst: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.102

User Datagram Protocol, Src Port: 53, Dst Port: 59307

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 ns1-37.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1740

Data length: 17

Name Server: ns1-37.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: 1740

Data length: 10

Name Server: ns1-173.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: 1740

Data length: 7

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: 1740

Data length: 8

Name Server: asia2.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: 1740

Data length: 7

Name Server: use2.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: 1740

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: 1740

Data length: 8

Name Server: asia1.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: 1740

Data length: 7

Name Server: usw2.akam.net

[Request In: 36]

[Time: 0.003166000 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»?**

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 і ншого?**

8 штук(ns1-37.akam.net ,ns1-173.akam.net, eur5.akam.net, asia2.akam.net, use2.akam.net, use5.akam.net, asia1.akam.net, usw2.akam.net). Лише за допомогою доменного імені.

**Lab3\_Task4**

No. Time Source Destination Protocol Length Info

5 2.258969 192.168.0.102 192.168.0.1 DNS 73 Standard query 0x8b32 A bitsy.mit.edu

Frame 5: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 61977, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x8b32

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

[Response In: 6]

No. Time Source Destination Protocol Length Info

6 2.263199 192.168.0.1 192.168.0.102 DNS 89 Standard query response 0x8b32 A bitsy.mit.edu A 18.72.0.3

Frame 6: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a), Dst: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.102

User Datagram Protocol, Src Port: 53, Dst Port: 61977

Domain Name System (response)

Transaction ID: 0x8b32

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: 1161

Data length: 4

Address: 18.72.0.3

[Request In: 5]

[Time: 0.004230000 seconds]

No. Time Source Destination Protocol Length Info

7 2.265973 192.168.0.102 18.72.0.3 DNS 82 Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa

Frame 7: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0

Ethernet II, Src: IntelCor\_08:d0:13 (ac:2b:6e:08:d0:13), Dst: Tp-LinkT\_5f:b5:0a (f4:f2:6d:5f:b5:0a)

Internet Protocol Version 4, Src: 192.168.0.102, Dst: 18.72.0.3

User Datagram Protocol, Src Port: 61978, 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)

**14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого**

**локального сервера DNS за замовчанням? Якщо ні, т о якому доменному імені**

**відповідає ця IP-адреса?**

Спочатку на 192.168.0.1, 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 ч ого складається кожна з цих відповідей?**

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