Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Кафедра математичних методів системного аналізу

ЗВІТ

про виконання лабораторних робіт

з дисципліни “Комп’ютерні мережі”

Лабораторна робота №3 Протокол DNS

Виконав: студент групи ІС-зп91

Бабаркін Владислав Олексійович

Прийняв: Кухарєв С.О.

Київ 2020

**Лабораторна робота 3 : Протокол DNS**

|  |
| --- |
|  |
|  |
|  |

**Контрольні запитання:**

|  |
| --- |
| **Запитання 1-6** |
| **No. Time Source Destination Protocol Length Info**  **309 3.101196 fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7 fd21:e55c:63c0::1 DNS 92 Standard query 0xca31 A www.ietf.org**  Frame 309: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 6, Src: fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7, Dst: fd21:e55c:63c0::1  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000  Payload Length: 38  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7  Destination: fd21:e55c:63c0::1  User Datagram Protocol, Src Port: 60340, Dst Port: 53  Source Port: 60340  Destination Port: 53  Length: 38  Checksum: 0xd005 [unverified]  [Checksum Status: Unverified]  [Stream index: 11]  [Timestamps]  Domain Name System (query)  Transaction ID: 0xca31  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: 388]**  **No. Time Source Destination Protocol Length Info**  **310 3.101427 fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7 fd21:e55c:63c0::1 DNS 92 Standard query 0x8559 AAAA www.ietf.org**  Frame 310: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 6, Src: fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7, Dst: fd21:e55c:63c0::1  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000  Payload Length: 38  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7  Destination: fd21:e55c:63c0::1  User Datagram Protocol, Src Port: 54818, Dst Port: 53  Source Port: 54818  Destination Port: 53  Length: 38  Checksum: 0x2a55 [unverified]  [Checksum Status: Unverified]  [Stream index: 12]  [Timestamps]  Domain Name System (query)  Transaction ID: 0x8559  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 AAAA, class IN**  **Name: www.ietf.org**  **[Name Length: 12]**  **[Label Count: 3]**  **Type: AAAA (IPv6 Address) (28)**  **Class: IN (0x0001)**  [Response In: 387]  **No. Time Source Destination Protocol Length Info**  **387 3.402182 fd21:e55c:63c0::1 fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7 DNS 193 Standard query response 0x8559 AAAA www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net AAAA 2606:4700:10::6814:55 AAAA 2606:4700:10::6814:155**  Frame 387: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 6, Src: fd21:e55c:63c0::1, Dst: fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 0101 1001 1100 1001 1101 = Flow Label: 0x59c9d  Payload Length: 139  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0::1  Destination: fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7  User Datagram Protocol, Src Port: 53, Dst Port: 54818  Source Port: 53  Destination Port: 54818  Length: 139  Checksum: 0x5cd5 [unverified]  [Checksum Status: Unverified]  [Stream index: 12]  [Timestamps]  Domain Name System (response)  Transaction ID: 0x8559  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 AAAA, class IN  Name: www.ietf.org  [Name Length: 12]  [Label Count: 3]  Type: AAAA (IPv6 Address) (28)  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 (5 minutes)**  **Data length: 33**  **CNAME: www.ietf.org.cdn.cloudflare.net**  **www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:55**  **Name: www.ietf.org.cdn.cloudflare.net**  **Type: AAAA (IPv6 Address) (28)**  **Class: IN (0x0001)**  **Time to live: 53 (53 seconds)**  **Data length: 16**  **AAAA Address: 2606:4700:10::6814:55**  **www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700:10::6814:155**  **Name: www.ietf.org.cdn.cloudflare.net**  **Type: AAAA (IPv6 Address) (28)**  **Class: IN (0x0001)**  **Time to live: 53 (53 seconds)**  **Data length: 16**  **AAAA Address: 2606:4700:10::6814:155**  [Request In: 310]  [Time: 0.300755000 seconds]  **No. Time Source Destination Protocol Length Info**  **388 3.402182 fd21:e55c:63c0::1 fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7 DNS 169 Standard query response 0xca31 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85**  Frame 388: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 6, Src: fd21:e55c:63c0::1, Dst: fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 1110 1001 1010 1011 1101 = Flow Label: 0xe9abd  Payload Length: 115  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0::1  Destination: fd21:e55c:63c0:0:d0fd:f48c:343a:d0f7  User Datagram Protocol, Src Port: 53, Dst Port: 60340  Source Port: 53  Destination Port: 60340  Length: 115  Checksum: 0x8f8e [unverified]  [Checksum Status: Unverified]  [Stream index: 11]  [Timestamps]  Domain Name System (response)  Transaction ID: 0xca31  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 (5 minutes)**  **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 (5 minutes)**  **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 (5 minutes)**  **Data length: 4**  **Address: 104.20.1.85**  [Request In: 309]  [Time: 0.300986000 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?**

Протокол UDP.

Номер цільового порта запиту DNS : Destination Port = 53

Номер вихідного порта відповіді DNS: Source Port = 53

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

IP Destination: fd21:e55c:63c0::1

Локальний

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

Message is a Query – повідомлення є запросом.

Recursion Desired : do query recursively – зробити рекурсивний запит

Пакет 309: Тип запиту : А, тобто отримання адресу IPv4, класс class IN (internet)

Пакет 310: Тип запиту : АAAA, тобто отримання адресу IPv6, класс class IN (internet)

У відповідь включається сам запрос:

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)

Queries

www.ietf.org: type AAAA, class IN

Name: www.ietf.org

[Name Length: 12]

[Label Count: 3]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

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

**Answer RRs: 3** . Кількість відповідей 3

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 (5 minutes)

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 (5 minutes)

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 (5 minutes)

Data length: 4

Address: 104.20.1.85

Тип CNAME (канонічне ім’я)– означає використання псевдоніму [www.ietf.org](http://www.ietf.org) для імені [www.ietf.org.cdn.cloudflare.net](http://www.ietf.org.cdn.cloudflare.net), який далі має IP адреси 104.20.0.85 та 104.20.1.85.

Дві адреси [www.ietf.org.cdn.cloudflare.net](http://www.ietf.org.cdn.cloudflare.net): addr 104.20.0.85 та addr 104.20.1.85 – означають, що аналогічний запити сайту можуть проводитися за двома IP адресами. Зазвичай використовується для розподілення навантаження, або на випадок, якщо один із серверів вийшов з ладу.

1. **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 (рис. 3.1): 104.20.0.85

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\2.png |
| Рис. 3.1. Повідомлення TCP SYN |

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

Виконуються додаткові запроси з запитом DNS analytics.ietf.org ( рис. 3.2.)

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\1.png |

Рис. 3.2. Нові запити DNS для отримання ресурсів

|  |
| --- |
| **Запитання 7-10** |
| **No. Time Source Destination Protocol Length Info**  **10 2.865585 fd21:e55c:63c0:0:9cca:1103:ae42:3083 fd21:e55c:63c0::1 DNS 91 Standard query 0x0004 A www.mit.edu**  Frame 10: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 6, Src: fd21:e55c:63c0:0:9cca:1103:ae42:3083, Dst: fd21:e55c:63c0::1  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000  Payload Length: 37  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0:0:9cca:1103:ae42:3083  Destination: fd21:e55c:63c0::1  User Datagram Protocol, Src Port: 51464, Dst Port: 53  Source Port: 51464  Destination Port: 53  Length: 37  Checksum: 0xcaa4 [unverified]  [Checksum Status: Unverified]  [Stream index: 3]  [Timestamps]  Domain Name System (query)  Transaction ID: 0x0004  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: 11]  **No. Time Source Destination Protocol Length Info**  **11 2.884511 fd21:e55c:63c0::1 fd21:e55c:63c0:0:9cca:1103:ae42:3083 DNS 180 Standard query response 0x0004 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.96.143.80**  Frame 11: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 6, Src: fd21:e55c:63c0::1, Dst: fd21:e55c:63c0:0:9cca:1103:ae42:3083  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 1111 1100 0101 0110 1010 = Flow Label: 0xfc56a  Payload Length: 126  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0::1  Destination: fd21:e55c:63c0:0:9cca:1103:ae42:3083  User Datagram Protocol, Src Port: 53, Dst Port: 51464  Source Port: 53  Destination Port: 51464  Length: 126  Checksum: 0x3b70 [unverified]  [Checksum Status: Unverified]  [Stream index: 3]  [Timestamps]  Domain Name System (response)  Transaction ID: 0x0004  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: 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: 1 (1 second)**  **Data length: 24**  **CNAME: e9566.dscb.akamaiedge.net**  **e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.143.80**  **Name: e9566.dscb.akamaiedge.net**  **Type: A (Host Address) (1)**  **Class: IN (0x0001)**  **Time to live: 20 (20 seconds)**  **Data length: 4**  **Address: 104.96.143.80**  [Request In: 10]  [Time: 0.018926000 seconds]  **No. Time Source Destination Protocol Length Info**  **12 2.902830 fd21:e55c:63c0:0:9cca:1103:ae42:3083 fd21:e55c:63c0::1 DNS 91 Standard query 0x0005 AAAA www.mit.edu**  Frame 12: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 6, Src: fd21:e55c:63c0:0:9cca:1103:ae42:3083, Dst: fd21:e55c:63c0::1  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000  Payload Length: 37  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0:0:9cca:1103:ae42:3083  Destination: fd21:e55c:63c0::1  User Datagram Protocol, Src Port: 51465, Dst Port: 53  Source Port: 51465  Destination Port: 53  Length: 37  Checksum: 0xafa2 [unverified]  [Checksum Status: Unverified]  [Stream index: 4]  [Timestamps]  Domain Name System (query)  Transaction ID: 0x0005  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]  **No. Time Source Destination Protocol Length Info**  **13 2.922155 fd21:e55c:63c0::1 fd21:e55c:63c0:0:9cca:1103:ae42:3083 DNS 220 Standard query response 0x0005 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 13: 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 6, Src: fd21:e55c:63c0::1, Dst: fd21:e55c:63c0:0:9cca:1103:ae42:3083  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 0011 1000 1010 0111 1001 = Flow Label: 0x38a79  Payload Length: 166  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0::1  Destination: fd21:e55c:63c0:0:9cca:1103:ae42:3083  User Datagram Protocol, Src Port: 53, Dst Port: 51465  Source Port: 53  Destination Port: 51465  Length: 166  Checksum: 0xc345 [unverified]  [Checksum Status: Unverified]  [Stream index: 4]  [Timestamps]  Domain Name System (response)  Transaction ID: 0x0005  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: 1 (1 second)**  **Data length: 24**  **CNAME: e9566.dscb.akamaiedge.net**  **e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:19e::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:d200:19e::255e**  **e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:d200:191::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:d200:191::255e**  [Request In: 12]  [Time: 0.019325000 seconds] |
| **C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\3.png** |
| Рис. 3.3. Відповідь на запит “nslookup www.mit.edu” |

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

Номер цільового порта запиту DNS : Destination Port = 53

Номер вихідного порта відповіді DNS: Source Port = 53

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

IP Destination: fd21:e55c:63c0::1

Локальний

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

Message is a Query – повідомлення є запросом.

Recursion Desired : do query recursively – зробити рекурсивний запит

Пакет 10: Тип запиту : А, тобто отримання адресу IPv4, класс class IN (internet)

Пакет 12: Тип запиту : АAAA, тобто отримання адресу IPv6, класс class IN (internet)

У відповідь включається сам запрос:

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)

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)

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

Тип CNAME (канонічне ім’я)– означає використання псевдоніму www.mit.edu [www.mit.edu](http://www.mit.edu) для [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net), що в свою чергу є псевдонімом для e9566.dscb.akamaiedge.net, який має кінцеву IPv4 адресу 104.96.143.80 та IPv6 адреси 2a02:26f0:d200:19e::255e , 2a02:26f0:d200:191::255e

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: 1 (1 second)

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.143.80

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20 (20 seconds)

Data length: 4

Address: 104.96.143.80

|  |
| --- |
| **Запитання 11-13** |
| **No. Time Source Destination Protocol Length Info**  **27 2.296068 fd21:e55c:63c0:0:9cca:1103:ae42:3083 fd21:e55c:63c0::1 DNS 87 Standard query 0x0003 NS mit.edu**  Frame 27: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 6, Src: fd21:e55c:63c0:0:9cca:1103:ae42:3083, Dst: fd21:e55c:63c0::1  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000  Payload Length: 33  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0:0:9cca:1103:ae42:3083  Destination: fd21:e55c:63c0::1  User Datagram Protocol, Src Port: 56750, Dst Port: 53  Source Port: 56750  Destination Port: 53  Length: 33  Checksum: 0x2ff6 [unverified]  [Checksum Status: Unverified]  [Stream index: 6]  [Timestamps]  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**  **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: 28]  **No. Time Source Destination Protocol Length Info**  **28 2.300235 fd21:e55c:63c0::1 fd21:e55c:63c0:0:9cca:1103:ae42:3083 DNS 254 Standard query response 0x0003 NS mit.edu NS eur5.akam.net NS use5.akam.net NS usw2.akam.net NS asia1.akam.net NS ns1-173.akam.net NS ns1-37.akam.net NS use2.akam.net NS asia2.akam.net**  Frame 28: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 6, Src: fd21:e55c:63c0::1, Dst: fd21:e55c:63c0:0:9cca:1103:ae42:3083  0110 .... = Version: 6  .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)  .... 0000 00.. .... .... .... .... .... = Differentiated Services Codepoint: Default (0)  .... .... ..00 .... .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)  .... .... .... 1010 0100 0010 1000 0001 = Flow Label: 0xa4281  Payload Length: 200  Next Header: UDP (17)  Hop Limit: 64  Source: fd21:e55c:63c0::1  Destination: fd21:e55c:63c0:0:9cca:1103:ae42:3083  User Datagram Protocol, Src Port: 53, Dst Port: 56750  Source Port: 53  Destination Port: 56750  Length: 200  Checksum: 0x8558 [unverified]  [Checksum Status: Unverified]  [Stream index: 6]  [Timestamps]  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: 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: 300 (5 minutes)**  **Data length: 15**  **Name Server: eur5.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: 300 (5 minutes)**  **Data length: 7**  **Name Server: use5.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**  **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 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 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 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 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**  [Request In: 27]  [Time: 0.004167000 seconds] |

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\5.png |
| Рис. 3.4. Відповідь на запит “nslookup –ty=NS mit.edu” |

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

IP Destination: fd21:e55c:63c0::1

Локальний

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

Message is a Query – повідомлення є запросом.

Recursion Desired : do query recursively – зробити рекурсивний запит

Тип запиту : NS (Authoritative name server адреси вузлів, що відповідають за домену зону)

У відповідь включається сам запрос:

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)

**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 відповідей (Answer RRs: 8)

eur5.akam.net

use5.akam.net

usw2.akam.net

asia1.akam.net

ns1-173.akam.net

ns1-37.akam.net

use2.akam.net

ns asia2.akam.net

Сервери були запропоновані за допомогою доменного імені.

|  |
| --- |
| **Запитання 14-16** |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\7.png |

Рис. 3.5. Пакети отримані під час запиту nslookup www.aiit.or.kr bitsy.mit.edu

|  |
| --- |
| **Запитання 14-16** |
| **No. Time Source Destination Protocol Length Info**  **1 0.000000 fd21:e55c:63c0:0:8c2a:2988:982f:38fb fd21:e55c:63c0::1 DNS 93 Standard query 0x2de3 A bitsy.mit.edu**  Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 6, Src: fd21:e55c:63c0:0:8c2a:2988:982f:38fb, Dst: fd21:e55c:63c0::1  User Datagram Protocol, Src Port: 52907, Dst Port: 53  Domain Name System (query)  Transaction ID: 0x2de3  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: 3]  **No. Time Source Destination Protocol Length Info**  **2 0.000200 fd21:e55c:63c0:0:8c2a:2988:982f:38fb fd21:e55c:63c0::1 DNS 93 Standard query 0x49a5 AAAA bitsy.mit.edu**  Frame 2: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 6, Src: fd21:e55c:63c0:0:8c2a:2988:982f:38fb, Dst: fd21:e55c:63c0::1  User Datagram Protocol, Src Port: 65470, Dst Port: 53  Domain Name System (query)  Transaction ID: 0x49a5  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 AAAA, class IN  Name: bitsy.mit.edu  [Name Length: 13]  [Label Count: 3]  Type: AAAA (IPv6 Address) (28)  Class: IN (0x0001)  [Response In: 4]  **No. Time Source Destination Protocol Length Info**  **3 0.035913 fd21:e55c:63c0::1 fd21:e55c:63c0:0:8c2a:2988:982f:38fb DNS 109 Standard query response 0x2de3 A bitsy.mit.edu A 18.0.72.3**  Frame 3: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 6, Src: fd21:e55c:63c0::1, Dst: fd21:e55c:63c0:0:8c2a:2988:982f:38fb  User Datagram Protocol, Src Port: 53, Dst Port: 52907  Domain Name System (response)  Transaction ID: 0x2de3  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: 1]  [Time: 0.035913000 seconds]  **No. Time Source Destination Protocol Length Info**  **4 0.035914 fd21:e55c:63c0::1 fd21:e55c:63c0:0:8c2a:2988:982f:38fb DNS 158 Standard query response 0x49a5 AAAA bitsy.mit.edu SOA use2.akam.net**  Frame 4: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 6, Src: fd21:e55c:63c0::1, Dst: fd21:e55c:63c0:0:8c2a:2988:982f:38fb  User Datagram Protocol, Src Port: 53, Dst Port: 65470  Domain Name System (response)  Transaction ID: 0x49a5  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: 0  Authority RRs: 1  Additional RRs: 0  Queries  bitsy.mit.edu: type AAAA, class IN  Name: bitsy.mit.edu  [Name Length: 13]  [Label Count: 3]  Type: AAAA (IPv6 Address) (28)  Class: IN (0x0001)  Authoritative nameservers  mit.edu: type SOA, class IN, mname use2.akam.net  Name: mit.edu  Type: SOA (Start Of a zone of Authority) (6)  Class: IN (0x0001)  Time to live: 1 (1 second)  Data length: 53  Primary name server: use2.akam.net  Responsible authority's mailbox: network-request.mit.edu  Serial Number: 13377  Refresh Interval: 900 (15 minutes)  Retry Interval: 900 (15 minutes)  Expire limit: 3600000 (41 days, 16 hours)  Minimum TTL: 3600 (1 hour)  [Request In: 2]  [Time: 0.035714000 seconds]  **No. Time Source Destination Protocol Length Info**  **5 0.038616 192.168.1.108 18.0.72.3 DNS 82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa**  Frame 5: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 4, Src: 192.168.1.108, Dst: 18.0.72.3  User Datagram Protocol, Src Port: 65471, 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  3.72.0.18.in-addr.arpa: type PTR, class IN  Name: 3.72.0.18.in-addr.arpa  [Name Length: 22]  [Label Count: 6]  Type: PTR (domain name PoinTeR) (12)  Class: IN (0x0001)  [Response In: 6]  **No. Time Source Destination Protocol Length Info**  **6 0.042014 18.0.72.3 192.168.1.108 DNS 150 Standard query response 0x0001 PTR 3.72.0.18.in-addr.arpa SOA ns.lanet.ua**  Frame 6: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 4, Src: 18.0.72.3, Dst: 192.168.1.108  User Datagram Protocol, Src Port: 53, Dst Port: 65471  Domain Name System (response)  Transaction ID: 0x0001  Flags: 0x8580 Standard query response, No error  1... .... .... .... = Response: Message is a response  .000 0... .... .... = Opcode: Standard query (0)  .... .1.. .... .... = Authoritative: Server is 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: 0  Authority RRs: 1  Additional RRs: 0  Queries  3.72.0.18.in-addr.arpa: type PTR, class IN  Name: 3.72.0.18.in-addr.arpa  [Name Length: 22]  [Label Count: 6]  Type: PTR (domain name PoinTeR) (12)  Class: IN (0x0001)  Authoritative nameservers  <Root>: type SOA, class IN, mname ns.lanet.ua  Name: <Root>  Type: SOA (Start Of a zone of Authority) (6)  Class: IN (0x0001)  Time to live: 60 (1 minute)  Data length: 57  Primary name server: ns.lanet.ua  Responsible authority's mailbox: hostmaster.lanet.kiev.ua  Serial Number: 2013053101  Refresh Interval: 21600 (6 hours)  Retry Interval: 3600 (1 hour)  Expire limit: 604800 (7 days)  Minimum TTL: 60 (1 minute)  [Request In: 5]  [Time: 0.003398000 seconds]  **No. Time Source Destination Protocol Length Info**  **7 0.044427 192.168.1.108 18.0.72.3 DNS 80 Standard query 0x0002 A www.aiit.or.kr.local**  Frame 7: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 4, Src: 192.168.1.108, Dst: 18.0.72.3  User Datagram Protocol, Src Port: 65472, 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.aiit.or.kr.local: type A, class IN  Name: www.aiit.or.kr.local  [Name Length: 20]  [Label Count: 5]  Type: A (Host Address) (1)  Class: IN (0x0001)  [Response In: 8]  **No. Time Source Destination Protocol Length Info**  **8 0.047004 18.0.72.3 192.168.1.108 DNS 136 Standard query response 0x0002 A www.aiit.or.kr.local A 194.50.85.176 NS ns.lanet.ua A 194.50.85.1**  Frame 8: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 4, Src: 18.0.72.3, Dst: 192.168.1.108  User Datagram Protocol, Src Port: 53, Dst Port: 65472  Domain Name System (response)  Transaction ID: 0x0002  Flags: 0x8580 Standard query response, No error  1... .... .... .... = Response: Message is a response  .000 0... .... .... = Opcode: Standard query (0)  .... .1.. .... .... = Authoritative: Server is 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: 1  Additional RRs: 1  Queries  www.aiit.or.kr.local: type A, class IN  Name: www.aiit.or.kr.local  [Name Length: 20]  [Label Count: 5]  Type: A (Host Address) (1)  Class: IN (0x0001)  Answers  www.aiit.or.kr.local: type A, class IN, addr 194.50.85.176  Name: www.aiit.or.kr.local  Type: A (Host Address) (1)  Class: IN (0x0001)  Time to live: 60 (1 minute)  Data length: 4  Address: 194.50.85.176  Authoritative nameservers  <Root>: type NS, class IN, ns ns.lanet.ua  Name: <Root>  Type: NS (authoritative Name Server) (2)  Class: IN (0x0001)  Time to live: 60 (1 minute)  Data length: 13  Name Server: ns.lanet.ua  Additional records  ns.lanet.ua: type A, class IN, addr 194.50.85.1  Name: ns.lanet.ua  Type: A (Host Address) (1)  Class: IN (0x0001)  Time to live: 10800 (3 hours)  Data length: 4  Address: 194.50.85.1  [Request In: 7]  [Time: 0.002577000 seconds]  **No. Time Source Destination Protocol Length Info**  **9 0.047616 192.168.1.108 18.0.72.3 DNS 80 Standard query 0x0003 AAAA www.aiit.or.kr.local**  Frame 9: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: IntelCor\_4f:90:fc (60:57:18:4f:90:fc), Dst: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30)  Internet Protocol Version 4, Src: 192.168.1.108, Dst: 18.0.72.3  User Datagram Protocol, Src Port: 65473, 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.aiit.or.kr.local: type AAAA, class IN  Name: www.aiit.or.kr.local  [Name Length: 20]  [Label Count: 5]  Type: AAAA (IPv6 Address) (28)  Class: IN (0x0001)  [Response In: 10]  **No. Time Source Destination Protocol Length Info**  **10 0.050073 18.0.72.3 192.168.1.108 DNS 148 Standard query response 0x0003 AAAA www.aiit.or.kr.local SOA ns.lanet.ua**  Frame 10: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface \Device\NPF\_{515AB600-9DD9-44FB-9043-185B381F60A2}, id 0  Ethernet II, Src: BelkinIn\_c9:a4:30 (60:38:e0:c9:a4:30), Dst: IntelCor\_4f:90:fc (60:57:18:4f:90:fc)  Internet Protocol Version 4, Src: 18.0.72.3, Dst: 192.168.1.108  User Datagram Protocol, Src Port: 53, Dst Port: 65473  Domain Name System (response)  Transaction ID: 0x0003  Flags: 0x8580 Standard query response, No error  1... .... .... .... = Response: Message is a response  .000 0... .... .... = Opcode: Standard query (0)  .... .1.. .... .... = Authoritative: Server is 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: 0  Authority RRs: 1  Additional RRs: 0  Queries  www.aiit.or.kr.local: type AAAA, class IN  Name: www.aiit.or.kr.local  [Name Length: 20]  [Label Count: 5]  Type: AAAA (IPv6 Address) (28)  Class: IN (0x0001)  Authoritative nameservers  <Root>: type SOA, class IN, mname ns.lanet.ua  Name: <Root>  Type: SOA (Start Of a zone of Authority) (6)  Class: IN (0x0001)  Time to live: 60 (1 minute)  Data length: 57  Primary name server: ns.lanet.ua  Responsible authority's mailbox: hostmaster.lanet.kiev.ua  Serial Number: 2013053101  Refresh Interval: 21600 (6 hours)  Retry Interval: 3600 (1 hour)  Expire limit: 604800 (7 days)  Minimum TTL: 60 (1 minute)  [Request In: 9]  [Time: 0.002457000 seconds] |

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\6.png |
| Рис. 3.6. Відповідь на запит “nslookup www.aiit.or.kr bitsy.mit.edu” |

**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?**

Запит DNS був відправлений на адресу 18.0.72.3. Не є локальною. Ім’я домену bitsy.mit.edu

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

Message is a Query – повідомлення є запросом.

Recursion Desired : do query recursively – зробити рекурсивний запит

Пакет 7: Тип запиту : А, тобто отримання адресу IPv4, класс class IN (internet)

Пакет 9: Тип запиту : АAAA, тобто отримання адресу IPv6, класс class IN (internet)

Запит іде адреси www.aiit.or.kr.local

У відповідь включається сам запрос:

Queries

www.aiit.or.kr.local: type A, class IN

Name: www.aiit.or.kr.local

[Name Length: 20]

[Label Count: 5]

Type: A (Host Address) (1)

Class: IN (0x0001)

Queries

www.aiit.or.kr.local: type AAAA, class IN

Name: www.aiit.or.kr.local

[Name Length: 20]

[Label Count: 5]

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

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

Для IPv6 жодної відповіді . Лише ім’я довіреного серверу.

Для IPv4 одна відповідь (Answers) + Ім’я довіреного серверу (Authoritative nameservers

) + Записи з додатковою інформацією (Additional records)

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 1

Answers

www.aiit.or.kr.local: type A, class IN, addr 194.50.85.176

Name: www.aiit.or.kr.local

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 60 (1 minute)

Data length: 4

Address: 194.50.85.176

Authoritative nameservers

<Root>: type NS, class IN, ns ns.lanet.ua

Name: <Root>

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 60 (1 minute)

Data length: 13

Name Server: ns.lanet.ua

Additional records

ns.lanet.ua: type A, class IN, addr 194.50.85.1

Name: ns.lanet.ua

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 10800 (3 hours)

Data length: 4

Address: 194.50.85.1

[Request In: 7]

[Time: 0.002577000 seconds]

Фактично IP адресу [www.aiit.or.kr](http://www.aiit.or.kr) ми не отримуємо, а отримуємо адресу 194.50.85.176, що, згідно, запиту “nslookup 194.50.85.176” являє собою ім’я beryllium-carbon.la.net.ua

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\8.png |
| Рис. 3.7. Результат запиту «nslookup 194.50.85.176» |

Та за допомогою запиту використовуючи ім’я довіреного серверу Authoritative nameservers ns.lanet.ua, яке ми отримали у відповіді “nslookup www.aiit.or.kr ns.lanet.ua” отримуємо IP адресу для [www.aiit.or.kr](http://www.aiit.or.kr) = 58.229.6.225

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\9.png |
| Рис. 3.8. Результат запиту “nslookup www.aiit.or.kr ns.lanet.ua” |

Спроба відкрити дану адресу веде на сайт <https://www.cuenet.co.kr/main/index.php>

Перевірка даної адреси [www.cuenet.co.kr](http://www.cuenet.co.kr) через запит «nslookup [www.cuenet.co.kr»](http://www.cuenet.co.kr) дає ту саму IP адресу

|  |
| --- |
| C:\Разное\My\КПИ\Семестр 2\16.04.2020\206 Комп'ютерні мережі-20200416T175924Z-001\206 Комп_ютерні мережі\ВЫПОЛНЕНИЕ\Л3\10.png |
| Рис. 3.9 Результат запиту «nslookup [www.cuenet.co.kr»](http://www.cuenet.co.kr) |

Тобто згідно nslookup два ім’я [www.cuenet.co.kr](http://www.cuenet.co.kr) та [www.aiit.or.kr](http://www.aiit.or.kr), що ведуть на два різні сайти знаходяться за однією і тією самою IP адресою.