МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС

«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»

НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №3

з курсу «Комп’ютерні мережі»

тема: «Протокол DNS»

Виконала: студентка 3 курсу

групи КА-77

Шахворостова Влада

Прийняв: Кухарєв С.О.

Київ – 2020р.

**Пакети для відповідей 1-6**

No. Time Source Destination Protocol Length Info

2 0.502308 192.168.0.103 192.168.0.1 DNS 84 Standard query 0xa5e3 PTR 1.0.168.192.in-addr.arpa

Frame 2: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

Ethernet II, Src: HonHaiPr\_29:7e:23 (38:b1:db:29:7e:23), Dst: Tp-LinkT\_3f:b7:0a (64:70:02:3f:b7:0a)

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

User Datagram Protocol, Src Port: 51144 (51144), Dst Port: domain (53)

Domain Name System (query)

Transaction ID: 0xa5e3

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

1.0.168.192.in-addr.arpa: type PTR, class IN

Name: 1.0.168.192.in-addr.arpa

[Name Length: 24]

[Label Count: 6]

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

[Response In: 6]

No. Time Source Destination Protocol Length Info

6 0.505784 192.168.0.1 192.168.0.103 DNS 307 Standard query response 0xa5e3 No such name PTR 1.0.168.192.in-addr.arpa SOA nobody.invalid TXT

Frame 6: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_3f:b7:0a (64:70:02:3f:b7:0a), Dst: HonHaiPr\_29:7e:23 (38:b1:db:29:7e:23)

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

User Datagram Protocol, Src Port: domain (53), Dst Port: 51144 (51144)

Domain Name System (response)

Transaction ID: 0xa5e3

Flags: 0x8583 Standard query response, No such name

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

.... .... .... 0011 = Reply code: No such name (3)

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 1

Queries

1.0.168.192.in-addr.arpa: type PTR, class IN

Name: 1.0.168.192.in-addr.arpa

[Name Length: 24]

[Label Count: 6]

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

Authoritative nameservers

1.0.168.192.in-addr.arpa: type SOA, class IN, mname nobody.invalid

Name: 1.0.168.192.in-addr.arpa

Type: SOA (Start Of a zone of Authority) (6)

Class: IN (0x0001)

Time to live: 10800 (3 hours)

Data length: 38

Primary name server: nobody.invalid

Responsible authority's mailbox: nobody.invalid

Serial Number: 1

Refresh Interval: 3600 (1 hour)

Retry Interval: 1200 (20 minutes)

Expire limit: 604800 (7 days)

Minimum TTL: 10800 (3 hours)

Additional records

explanation.invalid: type TXT, class IN

Name: explanation.invalid

Type: TXT (Text strings) (16)

Class: IN (0x0001)

Time to live: 10800 (3 hours)

Data length: 142

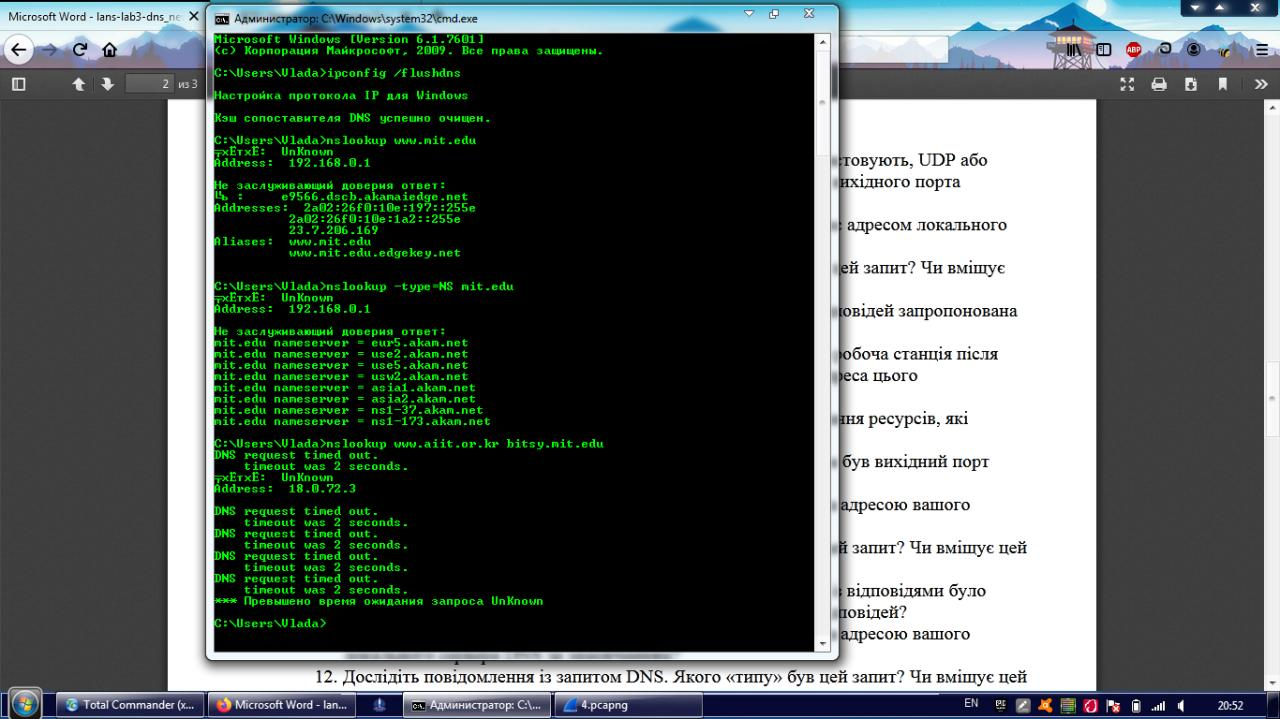
TXT Length: 141

TXT: Blocking is mandated by standards, see references on https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xhtml

[Request In: 2]

[Time: 0.003476000 seconds]

**Пакети для відповідей 7-10**

****

No. Time Source Destination Protocol Length Info

11 2.073357 192.168.0.103 192.168.0.1 DNS 84 Standard query 0xe01f PTR 1.0.168.192.in-addr.arpa

Frame 11: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

Ethernet II, Src: HonHaiPr\_29:7e:23 (38:b1:db:29:7e:23), Dst: Tp-LinkT\_3f:b7:0a (64:70:02:3f:b7:0a)

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

User Datagram Protocol, Src Port: 52643 (52643), Dst Port: domain (53)

Domain Name System (query)

Transaction ID: 0xe01f

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

1.0.168.192.in-addr.arpa: type PTR, class IN

Name: 1.0.168.192.in-addr.arpa

[Name Length: 24]

[Label Count: 6]

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

[Response In: 13]

No. Time Source Destination Protocol Length Info

13 2.078613 192.168.0.1 192.168.0.103 DNS 307 Standard query response 0xe01f No such name PTR 1.0.168.192.in-addr.arpa SOA nobody.invalid TXT

Frame 13: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_3f:b7:0a (64:70:02:3f:b7:0a), Dst: HonHaiPr\_29:7e:23 (38:b1:db:29:7e:23)

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

User Datagram Protocol, Src Port: domain (53), Dst Port: 52643 (52643)

Domain Name System (response)

Transaction ID: 0xe01f

Flags: 0x8583 Standard query response, No such name

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

.... .... .... 0011 = Reply code: No such name (3)

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 1

Queries

1.0.168.192.in-addr.arpa: type PTR, class IN

Name: 1.0.168.192.in-addr.arpa

[Name Length: 24]

[Label Count: 6]

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

Authoritative nameservers

1.0.168.192.in-addr.arpa: type SOA, class IN, mname nobody.invalid

Name: 1.0.168.192.in-addr.arpa

Type: SOA (Start Of a zone of Authority) (6)

Class: IN (0x0001)

Time to live: 10800 (3 hours)

Data length: 38

Primary name server: nobody.invalid

Responsible authority's mailbox: nobody.invalid

Serial Number: 1

Refresh Interval: 3600 (1 hour)

Retry Interval: 1200 (20 minutes)

Expire limit: 604800 (7 days)

Minimum TTL: 10800 (3 hours)

Additional records

explanation.invalid: type TXT, class IN

Name: explanation.invalid

Type: TXT (Text strings) (16)

Class: IN (0x0001)

Time to live: 10800 (3 hours)

Data length: 142

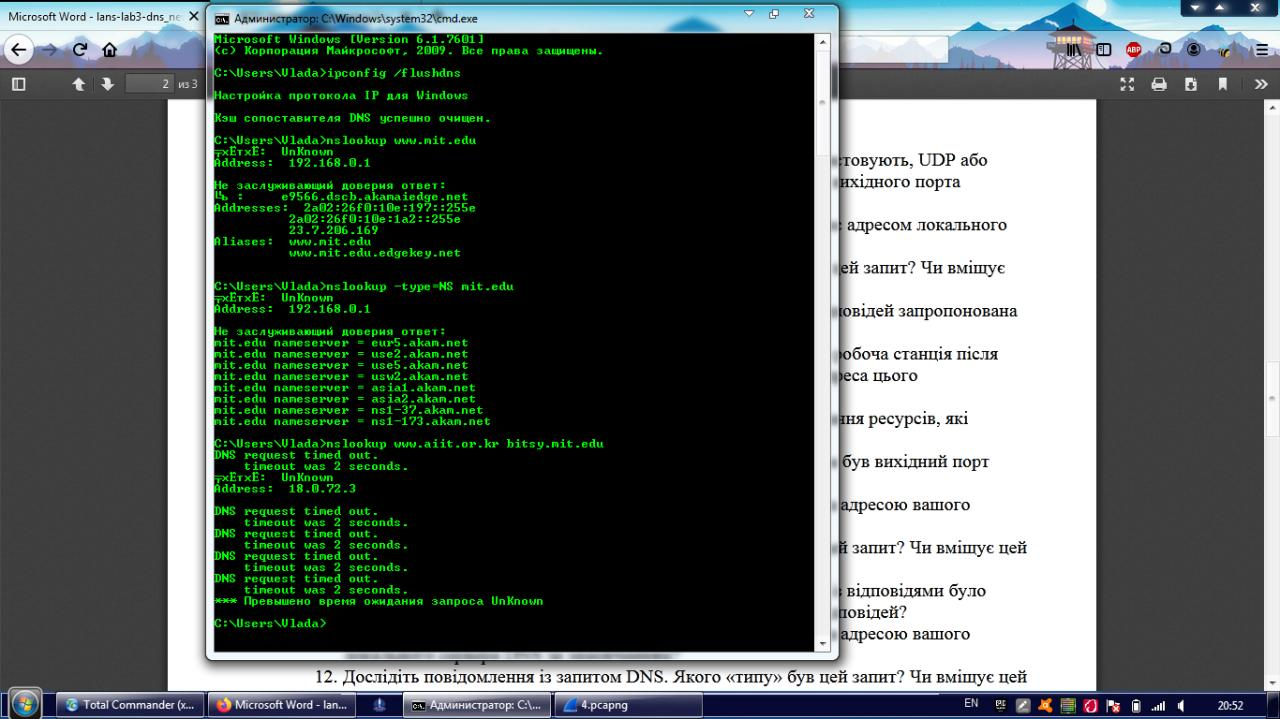
TXT Length: 141

TXT: Blocking is mandated by standards, see references on https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xhtml

[Request In: 11]

[Time: 0.005256000 seconds]

**Пакети для відповідей 11-13**

****

No. Time Source Destination Protocol Length Info

16 2.899391 192.168.0.103 192.168.0.1 DNS 87 Standard query 0xab6a A datarouter.ol.epicgames.com

Frame 16: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0

Ethernet II, Src: HonHaiPr\_29:7e:23 (38:b1:db:29:7e:23), Dst: Tp-LinkT\_3f:b7:0a (64:70:02:3f:b7:0a)

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

User Datagram Protocol, Src Port: 60821 (60821), Dst Port: domain (53)

Domain Name System (query)

Transaction ID: 0xab6a

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

datarouter.ol.epicgames.com: type A, class IN

Name: datarouter.ol.epicgames.com

[Name Length: 27]

[Label Count: 4]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 18]

No. Time Source Destination Protocol Length Info

18 2.902852 192.168.0.1 192.168.0.103 DNS 249 Standard query response 0xab6a A datarouter.ol.epicgames.com CNAME datarouter-weighted.ol.epicgames.com A 52.205.241.63 A 54.86.242.45 A 54.209.114.12 A 3.218.199.108 A 18.208.62.117 A 52.4.236.189 A 52.5.203.137 A 52.87.28.59

Frame 18: 249 bytes on wire (1992 bits), 249 bytes captured (1992 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_3f:b7:0a (64:70:02:3f:b7:0a), Dst: HonHaiPr\_29:7e:23 (38:b1:db:29:7e:23)

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

User Datagram Protocol, Src Port: domain (53), Dst Port: 60821 (60821)

Domain Name System (response)

Transaction ID: 0xab6a

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: 9

Authority RRs: 0

Additional RRs: 0

Queries

datarouter.ol.epicgames.com: type A, class IN

Name: datarouter.ol.epicgames.com

[Name Length: 27]

[Label Count: 4]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

datarouter.ol.epicgames.com: type CNAME, class IN, cname datarouter-weighted.ol.epicgames.com

Name: datarouter.ol.epicgames.com

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

Class: IN (0x0001)

Time to live: 205 (3 minutes, 25 seconds)

Data length: 22

CNAME: datarouter-weighted.ol.epicgames.com

datarouter-weighted.ol.epicgames.com: type A, class IN, addr 52.205.241.63

Name: datarouter-weighted.ol.epicgames.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 26 (26 seconds)

Data length: 4

Address: datarouter-weighted.ol.epicgames.com (52.205.241.63)

datarouter-weighted.ol.epicgames.com: type A, class IN, addr 54.86.242.45

Name: datarouter-weighted.ol.epicgames.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 26 (26 seconds)

Data length: 4

Address: datarouter-weighted.ol.epicgames.com (54.86.242.45)

datarouter-weighted.ol.epicgames.com: type A, class IN, addr 54.209.114.12

Name: datarouter-weighted.ol.epicgames.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 26 (26 seconds)

Data length: 4

Address: datarouter-weighted.ol.epicgames.com (54.209.114.12)

datarouter-weighted.ol.epicgames.com: type A, class IN, addr 3.218.199.108

Name: datarouter-weighted.ol.epicgames.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 26 (26 seconds)

Data length: 4

Address: datarouter-weighted.ol.epicgames.com (3.218.199.108)

datarouter-weighted.ol.epicgames.com: type A, class IN, addr 18.208.62.117

Name: datarouter-weighted.ol.epicgames.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 26 (26 seconds)

Data length: 4

Address: datarouter-weighted.ol.epicgames.com (18.208.62.117)

datarouter-weighted.ol.epicgames.com: type A, class IN, addr 52.4.236.189

Name: datarouter-weighted.ol.epicgames.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 26 (26 seconds)

Data length: 4

Address: datarouter-weighted.ol.epicgames.com (52.4.236.189)

datarouter-weighted.ol.epicgames.com: type A, class IN, addr 52.5.203.137

Name: datarouter-weighted.ol.epicgames.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 26 (26 seconds)

Data length: 4

Address: datarouter-weighted.ol.epicgames.com (52.5.203.137)

datarouter-weighted.ol.epicgames.com: type A, class IN, addr 52.87.28.59

Name: datarouter-weighted.ol.epicgames.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 26 (26 seconds)

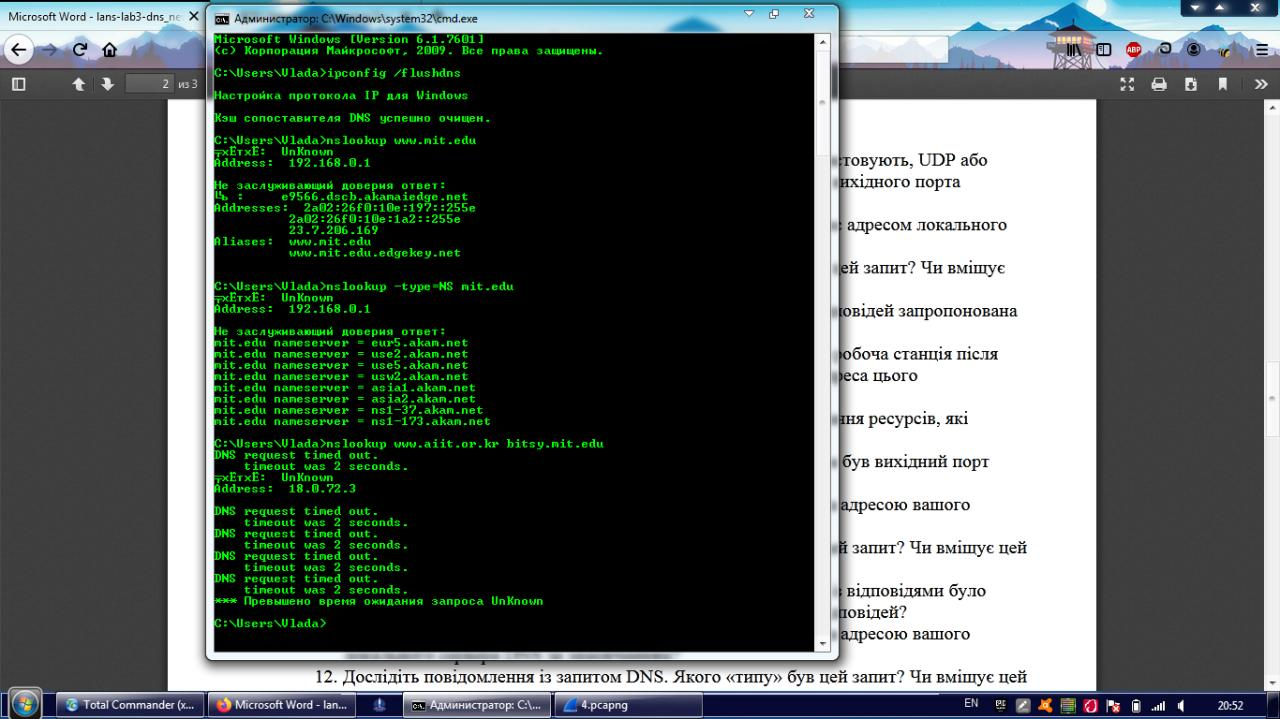
Data length: 4

Address: datarouter-weighted.ol.epicgames.com (52.87.28.59)

[Request In: 16]

[Time: 0.003461000 seconds]

**Пакети для відповідей 14-16**

****

No. Time Source Destination Protocol Length Info

11 1.694960 192.168.0.103 192.168.0.1 DNS 84 Standard query 0x6afa PTR 1.0.168.192.in-addr.arpa

Frame 11: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

Ethernet II, Src: HonHaiPr\_29:7e:23 (38:b1:db:29:7e:23), Dst: Tp-LinkT\_3f:b7:0a (64:70:02:3f:b7:0a)

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

User Datagram Protocol, Src Port: 61388 (61388), Dst Port: domain (53)

Domain Name System (query)

Transaction ID: 0x6afa

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

1.0.168.192.in-addr.arpa: type PTR, class IN

Name: 1.0.168.192.in-addr.arpa

[Name Length: 24]

[Label Count: 6]

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

[Response In: 13]

No. Time Source Destination Protocol Length Info

13 1.698247 192.168.0.1 192.168.0.103 DNS 307 Standard query response 0x6afa No such name PTR 1.0.168.192.in-addr.arpa SOA nobody.invalid TXT

Frame 13: 307 bytes on wire (2456 bits), 307 bytes captured (2456 bits) on interface 0

Ethernet II, Src: Tp-LinkT\_3f:b7:0a (64:70:02:3f:b7:0a), Dst: HonHaiPr\_29:7e:23 (38:b1:db:29:7e:23)

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

User Datagram Protocol, Src Port: domain (53), Dst Port: 61388 (61388)

Domain Name System (response)

Transaction ID: 0x6afa

Flags: 0x8583 Standard query response, No such name

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

.... .... .... 0011 = Reply code: No such name (3)

Questions: 1

Answer RRs: 0

Authority RRs: 1

Additional RRs: 1

Queries

1.0.168.192.in-addr.arpa: type PTR, class IN

Name: 1.0.168.192.in-addr.arpa

[Name Length: 24]

[Label Count: 6]

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

Authoritative nameservers

1.0.168.192.in-addr.arpa: type SOA, class IN, mname nobody.invalid

Name: 1.0.168.192.in-addr.arpa

Type: SOA (Start Of a zone of Authority) (6)

Class: IN (0x0001)

Time to live: 10800 (3 hours)

Data length: 38

Primary name server: nobody.invalid

Responsible authority's mailbox: nobody.invalid

Serial Number: 1

Refresh Interval: 3600 (1 hour)

Retry Interval: 1200 (20 minutes)

Expire limit: 604800 (7 days)

Minimum TTL: 10800 (3 hours)

Additional records

explanation.invalid: type TXT, class IN

Name: explanation.invalid

Type: TXT (Text strings) (16)

Class: IN (0x0001)

Time to live: 10800 (3 hours)

Data length: 142

TXT Length: 141

TXT: Blocking is mandated by standards, see references on https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xhtml

[Request In: 11]

[Time: 0.003287000 seconds]

**Контрольні питання**

**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?

UPD (17), номер цільового порту запиту DNS – domain (53), номер вихідного порту відповіді DNS – 51144 (51144).

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

На 192.168.0.1. Так, є.

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

Типу «А» (Host Address), ні.

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

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

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

Номер цільового порту запиту DNS – domain (53), номер вихідного порту відповіді DNS – 52643 (52643).

**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, є.

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

Типу «А» (Host address), ні.

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

3 записи із відповідями. Кожна відповідь складається з: Name, Type, Class, Time to live, Data length, CNAME/Adress.

**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 «А» (Host Address), 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 записів із відповідями: eur5.akam.net, use2.akam.net, use5.akam.net, usw2.akam.net, asia1.akam.net, asia2.akam.net, ns1-37.akam.net, ns1-173.akam.net. Сервери були запропоновані за домогою адреси IP.

**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?

192.168.0.1 – локальний сервер, 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»?

Типу PTR, ні.

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

Одна відповідь від першого сервера, жодної від другого. Відповідь складається з Name, Type, Class, Time to live, Data length, CNAME/Adress.

**Висновки**

Проаналізували деталі роботи протоколу DNS.