

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

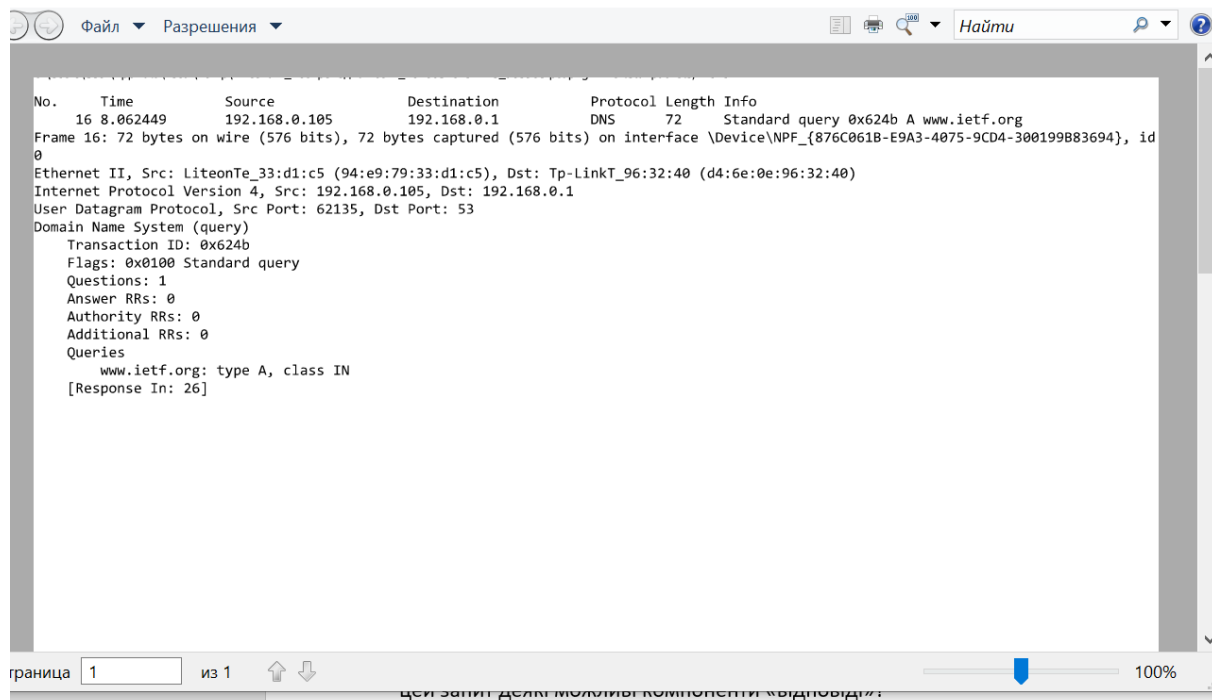
**Практична робота №3
з курсу «Комп'ютерні мережі»**

**Виконала: студентка 3 курсу
групи КА-72
Зінченко С. О.
Прийняв: Кухарєв С.О.**

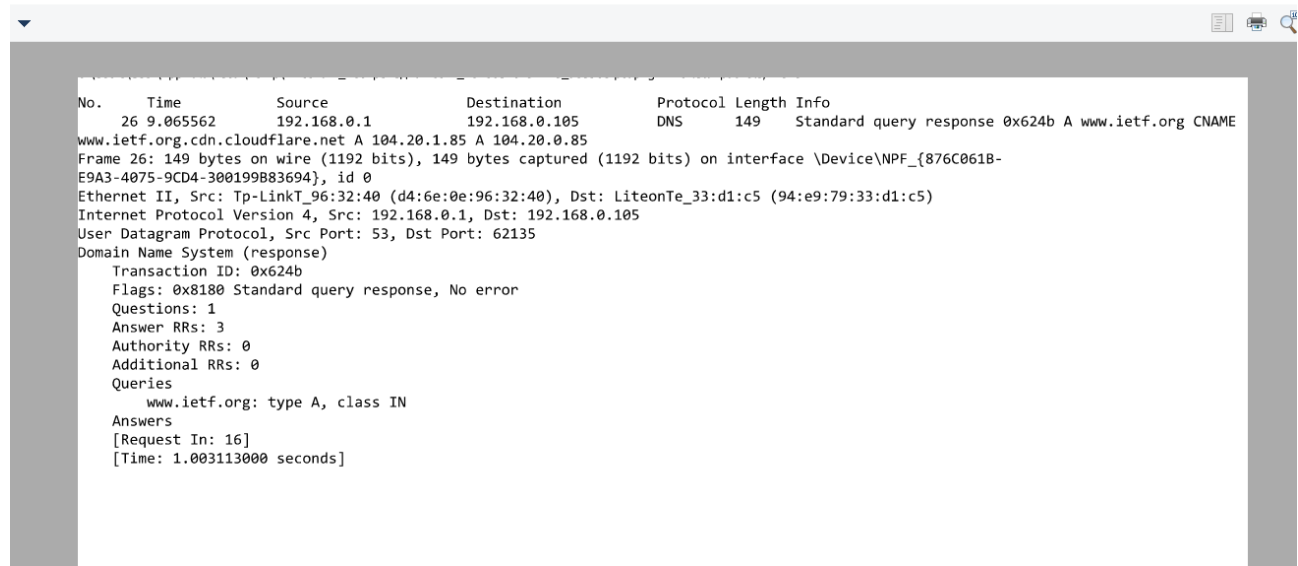
Київ – 2020 р.

Контрольні запитання:

dns_query.oxps - Средство просмотра XPS



просмотра XPS



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 запиту:53
Вихідний відповіді:53
2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?

Dst: 192.168.0.1

Так

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

Типу «А». Всі компоненти блоку Queries.

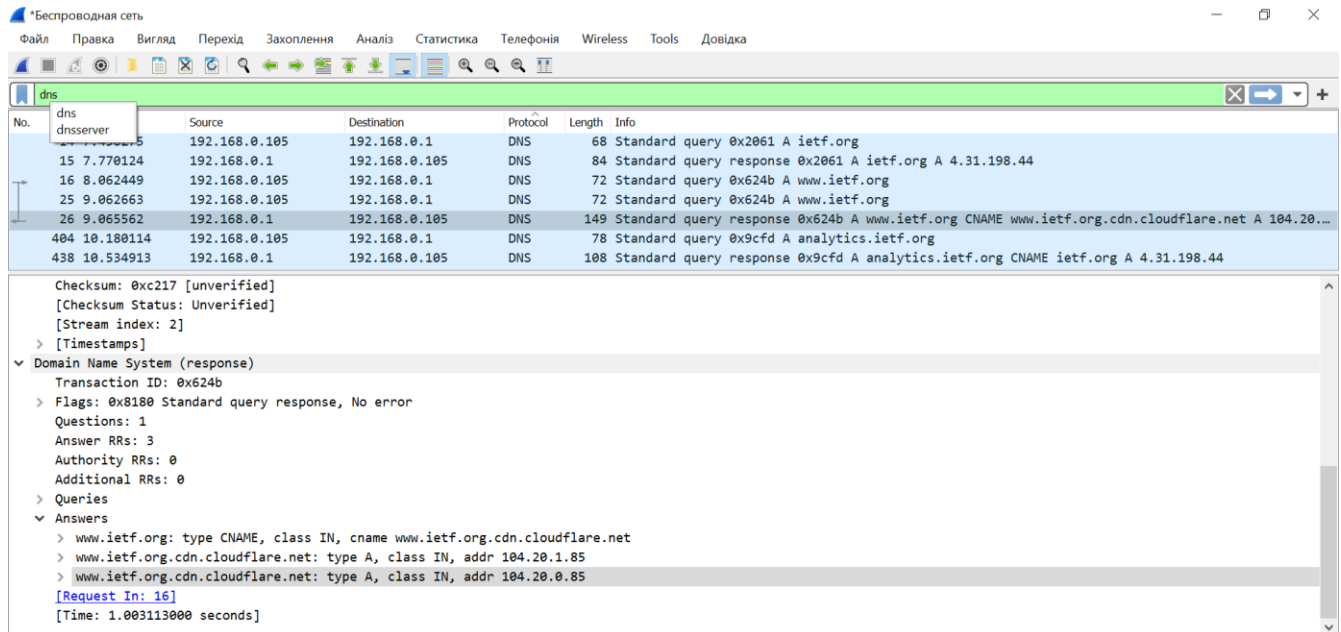
4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

3 відповіді.

www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85

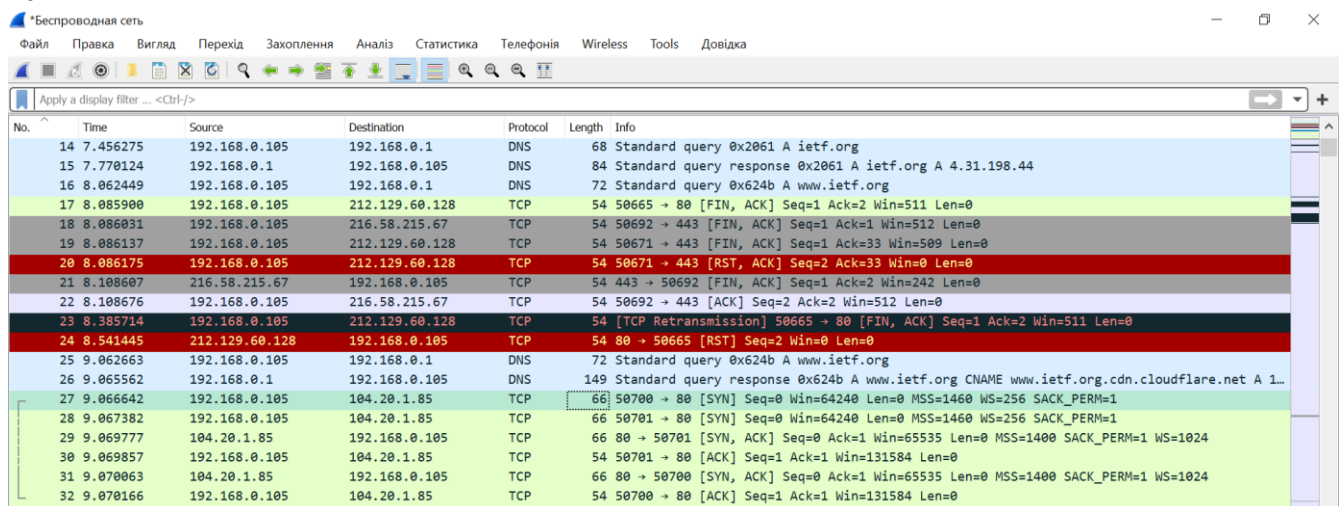


No.	Time	Source	Destination	Protocol	Length	Info
15	7.770124	192.168.0.105	192.168.0.1	DNS	68	Standard query 0x2061 A ietf.org
16	8.062449	192.168.0.105	192.168.0.1	DNS	84	Standard query response 0x2061 A ietf.org A 4.31.198.44
25	9.062663	192.168.0.105	192.168.0.1	DNS	72	Standard query 0x624b A www.ietf.org
26	9.065562	192.168.0.1	192.168.0.105	DNS	72	Standard query response 0x624b A www.ietf.org
404	10.180114	192.168.0.105	192.168.0.1	DNS	149	Standard query response 0x624b A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85
438	10.534913	192.168.0.1	192.168.0.105	DNS	78	Standard query 0x9cfd A analytics.ietf.org
				DNS	108	Standard query response 0x9cfd A analytics.ietf.org CNAME ietf.org A 4.31.198.44

Checksum: 0xc217 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
> [Timestamps]
▼ Domain Name System (response)
Transaction ID: 0x624b
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
> Queries
▼ Answers
> www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
[Request in: 16]
[Time: 1.003113000 seconds]

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



No.	Time	Source	Destination	Protocol	Length	Info
14	7.456275	192.168.0.105	192.168.0.1	DNS	68	Standard query 0x2061 A ietf.org
15	7.770124	192.168.0.1	192.168.0.105	DNS	84	Standard query response 0x2061 A ietf.org A 4.31.198.44
16	8.062449	192.168.0.105	192.168.0.1	DNS	72	Standard query 0x624b A www.ietf.org
17	8.085900	192.168.0.105	212.129.60.128	TCP	54	50665 → 80 [FIN, ACK] Seq=1 Ack=2 Win=511 Len=0
18	8.086031	192.168.0.105	216.58.215.67	TCP	54	50692 → 443 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0
19	8.086137	192.168.0.105	212.129.60.128	TCP	54	50671 → 443 [FIN, ACK] Seq=1 Ack=33 Win=509 Len=0
20	8.086175	192.168.0.105	212.129.60.128	TCP	54	50671 → 443 [RST, ACK] Seq=2 Ack=33 Win=0 Len=0
21	8.108607	216.58.215.67	192.168.0.105	TCP	54	443 → 50692 [FIN, ACK] Seq=1 Ack=2 Win=242 Len=0
22	8.108676	192.168.0.105	216.58.215.67	TCP	54	50692 → 443 [ACK] Seq=2 Ack=2 Win=512 Len=0
23	8.385714	192.168.0.105	212.129.60.128	TCP	54	[TCP Retransmission] 50665 → 80 [FIN, ACK] Seq=1 Ack=2 Win=511 Len=0
24	8.541445	212.129.60.128	192.168.0.105	TCP	54	80 → 50665 [RST] Seq=2 Win=0 Len=0
25	9.062663	192.168.0.105	192.168.0.1	DNS	72	Standard query 0x624b A www.ietf.org
26	9.065562	192.168.0.1	192.168.0.105	DNS	149	Standard query response 0x624b A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85
27	9.066642	192.168.0.105	104.20.1.85	TCP	66	50700 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28	9.067382	192.168.0.105	104.20.1.85	TCP	66	50701 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
29	9.069777	104.20.1.85	192.168.0.105	TCP	66	80 → 50701 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
30	9.069857	192.168.0.105	104.20.1.85	TCP	54	50701 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
31	9.070063	104.20.1.85	192.168.0.105	TCP	66	80 → 50700 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
32	9.070166	192.168.0.105	104.20.1.85	TCP	54	50700 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0

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

Так

*Беспроводная сеть

Файл Правка Видяг Перехід Захоплення Аналіз Статистика Телефонія Wireless Tools Довідка

dns

No.	Time	Source	Destination	Protocol	Length	Info
9	5.136329	192.168.0.105	192.168.0.1	DNS	80	Standard query 0x61bd A activity.windows.com
10	5.140561	192.168.0.1	192.168.0.105	DNS	189	Standard query response 0x61bd A activity.windows.com CNAME global.activity.windows.com.akadn...
100	33.601900	192.168.0.105	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
101	33.605828	192.168.0.1	192.168.0.105	DNS	139	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA 168.192.IN-ADDR...
102	33.607609	192.168.0.105	192.168.0.1	DNS	71	Standard query 0x0002 A www.mit.edu
103	33.735724	192.168.0.1	192.168.0.105	DNS	163	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.a...
104	33.748882	192.168.0.105	192.168.0.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
105	33.768294	192.168.0.1	192.168.0.105	DNS	203	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dsc...

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: 906 (15 minutes, 6 seconds)
Data length: 25

0040 64 75 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 03 du.....
0050 8a 00 19 03 77 77 77 03 6d 69 74 03 65 64 75 07www.mit.edu.
0060 65 64 67 65 6b 65 79 03 6e 65 74 00 c0 29 00 05 edgekey.net...
0070 00 01 00 00 3b 00 1b 05 65 39 35 36 04 64e9566.d

Text item (text), 132 byte(s) | Packets: 128 · Displayed: 8 (6.3%) · Dropped: 0 (0.0%) | Profile: Default

днс2_запрос.охрс - Средство просмотра XPS

Файл Разрешения

Haïmu

No. Time Source Destination Protocol Length Info

104 33.748882 192.168.0.105 192.168.0.1 DNS 71 Standard query 0x0003 AAAA www.mit.edu

Frame 104: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{876C061B-E9A3-4075-9CD4-3001998B3694}, id 0

Ethernet II, Src: LiteonTe_33:d1:c5 (94:e9:79:33:d1:c5), Dst: Tp-LinkT_96:32:40 (d4:6e:0e:96:32:40)

Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 64700, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0003

Flags: 0x0100 Standard query

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: 105]

Страница 1 из 1 100%

```

No.    Time    Source          Destination      Protocol Length Info
105    33.768294 192.168.0.1     192.168.0.105   DNS          203      Standard query response 0x0003 AAAA www.mit.edu
CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:d200:191::255e AAAA 2a02:26f0:d200:19e::255e
Frame 105: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on interface \Device\NPF_{876C061B-
E9A3-4075-9CD4-300199B83694}, id 0
Ethernet II, Src: Tp-LinkT_96:32:40 (d4:6e:0e:96:32:40), Dst: LiteonTe_33:d1:c5 (94:e9:79:33:d1:c5)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105
User Datagram Protocol, Src Port: 53, Dst Port: 64700
Domain Name System (response)
  Transaction ID: 0x0003
  Flags: 0x8180 Standard query response, No error
  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: 906 (15 minutes, 6 seconds)
      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: 59 (59 seconds)
      Data length: 27
      CNAME: e9566.dscb.akamaiedge.net
    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
    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
[Request In: 104]
[Time: 0.019412000 seconds]

```

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

Цільовий запит: 53

Вихідний відповіді: 53

8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Так, 192.168.0.1

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

Тип «AAAA». Всі компоненти блоку Queries.

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

Чотири

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: 906 (15 minutes, 6 seconds)

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: 59 (59 seconds)

Data length: 27

CNAME: e9566.dscb.akamaiedge.net

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

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

Беспроводная сеть

Файл Правка Видял Перехід Захоплення Аналіз Статистика Телефонія Wireless Tools Довідка

dns

No.	Time	Source	Destination	Protocol	Length	Info
3	0.540985	192.168.0.105	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
4	0.543931	192.168.0.1	192.168.0.105	DNS	139	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA 168.192.IN-ADDR...
5	0.545713	192.168.0.105	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
6	0.670478	192.168.0.1	192.168.0.105	DNS	390	Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS asia1.akam.net NS use5.akam.n...

> Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{876C061B-E9A3-4075-9CD4-300199B83694}, id 0

> Ethernet II, Src: LiteonTe_33:d1:c5 (94:e9:79:33:d1:c5), Dst: Tp-LinkT_96:32:40 (d4:6e:0e:96:32:40)

> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1

> User Datagram Protocol, Src Port: 63615, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0001

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

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

0000 d4 6e 0e 96 32 40 94 e9 79 33 d1 c5 08 00 45 00 n...2@... y3... E-

0010 00 46 f1 7b 00 00 80 11 c7 70 c0 a8 00 69 c0 a8 F{... p...i...

0020 00 01 f8 7f 00 35 00 32 f8 9e 00 01 01 00 00 015.2

0030 00 00 00 00 00 00 01 31 01 30 03 31 36 38 03 311 0 168 1

wireshark_Беспроводная сеть_20200320220507_a09576.pcapng

Packets: 58 · Displayed: 4 (6.9%)

Profile: Default

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

Так, адресу видно у скріншоті вище.

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

Типу NS. Всі компоненти блоку Queries.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.545713	192.168.0.105	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu

Frame 5: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{876C061B-E9A3-4075-9CD4-3001998B3694}, id 0

Ethernet II, Src: LiteonTe_33:d1:c5 (94:e9:79:33:d1:c5), Dst: Tp-LinkT_96:32:40 (d4:6e:0e:96:32:40)

Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 63616, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

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: 6]

No.	Time	Source	Destination	Protocol	Length	Info
6	0.670478	192.168.0.1	192.168.0.105	DNS	390	Standard query response 0x0002 NS mit.edu NS

Frame 6: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on interface \Device\NPF_{876C061B-E9A3-4075-9CD4-3001998B3694}, id 0

Ethernet II, Src: Tp-LinkT_96:32:40 (d4:6e:0e:96:32:40), Dst: LiteonTe_33:d1:c5 (94:e9:79:33:d1:c5)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105

User Datagram Protocol, Src Port: 53, Dst Port: 63616

Domain Name System (response)

Transaction ID: 0x0002

Flags: 0x8100 Standard query response, No error

Questions: 1

Answer RRs: 8

Authority RRs: 0

Additional RRs: 9

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: 1800 (30 minutes)

Data length: 17

Name Server: ns1-37.akam.net

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

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 8

Name Server: asial.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: 1800 (30 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: 1800 (30 minutes)

Data length: 7

Name Server: usw2.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: 1800 (30 minutes)

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: 1800 (30 minutes)

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: 1800 (30 minutes)

Data length: 7

Name Server: use2.akam.net

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

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 10

Name Server: ns1-173.akam.net

Additional records

eur5.akam.net: type A, class IN, addr 23.74.25.64

Name: eur5.akam.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 60229 (16 hours, 43 minutes, 49 seconds)

Data length: 4

Address: 23.74.25.64

use2.akam.net: type A, class IN, addr 96.7.49.64

Name: use2.akam.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 62135 (17 hours, 15 minutes, 35 seconds)

Data length: 4

Address: 96.7.49.64

use5.akam.net: type A, class IN, addr 2.16.40.64

Name: use5.akam.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 80891 (1 day, 8 minutes, 11 seconds)

Data length: 4

Address: 2.16.40.64

usw2.akam.net: type A, class IN, addr 184.26.161.64

Name: usw2.akam.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 75354 (20 hours, 55 minutes, 54 seconds)

Data length: 4

Address: 184.26.161.64

asial.akam.net: type A, class IN, addr 95.100.175.64

Name: asial.akam.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 53034 (14 hours, 43 minutes, 54 seconds)

Data length: 4

Address: 95.100.175.64

asia2.akam.net: type A, class IN, addr 95.101.36.64

Name: asia2.akam.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 33885 (9 hours, 24 minutes, 45 seconds)

Data length: 4

Address: 95.101.36.64

ns1-37.akam.net: type A, class IN, addr 193.108.91.37

Name: ns1-37.akam.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 25426 (7 hours, 3 minutes, 46 seconds)

Data length: 4

Address: 193.108.91.37

ns1-173.akam.net: type A, class IN, addr 193.108.91.173

Name: ns1-173.akam.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20031 (5 hours, 33 minutes, 51 seconds)

Data length: 4

Address: 193.108.91.173

ns1-173.akam.net: type AAAA, class IN, addr 2600:1401:2::ad

Name: ns1-173.akam.net

Type: AAAA (IPv6 Address) (28)

Class: IN (0x0001)

Time to live: 154661 (1 day, 18 hours, 57 minutes, 41 seconds)

Data length: 16

AAAA Address: 2600:1401:2::ad

[Request In: 5]

[Time: 0.124765000 seconds]

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

Назви серверів видно на скріншоті вище. І те і інше, доменне ім'я у відповідях, а адреси IP у додаткових записах(видно вище).

The screenshot displays a Windows 10 desktop environment. In the background, a Microsoft Word document titled 'CN_lab2_Zinchenko' is open. Overlaid on the Word document is a black command prompt window. The command prompt shows the execution of the 'nslookup' command, which returns DNS information for various domains including 'bitsy.mit.edu' and 'www.aiit.or.kr'. Below the command prompt, the Wireshark network protocol analyzer is open, showing a packet capture on the 'dns' filter. The packet list pane shows several DNS packets, with packet 16 selected. The packet details pane shows the structure of a DNS query for 'www.aiit.or.kr'. The packet bytes pane shows the raw data of the selected packet.

```
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-173.akam.net

eur5.akam.net internet address = 23.74.25.64
use2.akam.net internet address = 96.7.49.64
use5.akam.net internet address = 2.16.40.64
usw2.akam.net internet address = 184.26.161.64
asia1.akam.net internet address = 95.100.175.64
asia2.akam.net internet address = 95.101.36.64
ns1-37.akam.net internet address = 193.108.91.37
ns1-173.akam.net internet address = 193.108.91.173
ns1-173.akam.net AAAA IPv6 address = 2600:1401:2::ad

C:\Users\User>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
        timeout was 2 seconds.
*Server: UnKnown
Address: 18.0.72.3

DNS request timed out.
        timeout was 2 seconds.
DNS request timed out.
        timeout was 2 seconds.
DNS request timed out.
        timeout was 2 seconds.
DNS request timed out.
        timeout was 2 seconds.
*** Превышено время ожидания запроса UnKnown

C:\Users\User>
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.105	192.168.0.1	DNS	73	Standard query 0xf005 A bitsy.mit.edu
2	0.031533	192.168.0.105	192.168.0.1	DNS	73	Standard query 0xf005 A bitsy.mit.edu
3	0.094519	192.168.0.1	192.168.0.105	DNS	89	Standard query response 0xf005 A bitsy.mit.edu A 18.0.72.3
4	0.094520	192.168.0.1	192.168.0.105	DNS	89	Standard query response 0xf005 A bitsy.mit.edu A 18.0.72.3
5	0.101277	192.168.0.105	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
16	2.118236	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
17	4.123111	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
22	6.127009	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
23	8.136944	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{876C061B-E9A3-4075-9CD4-300199883694}, id 0
> Ethernet II, Src: LiteonTe_33:d1:c5 (94:e9:79:33:d1:c5), Dst: Tp-Link_T_96:32:40 (d4:6e:0e:96:32:40)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 63197, Dst Port: 53
> Domain Name System (query)
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
www.aiit.or.kr: type A, class IN

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?

18.0.72.3. Ні, вона відповідає bitsy.mit.edu

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

Типу «А». Всі компоненти блоку Queries.

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

Склад видно у скріншоті нижче.

The screenshot shows the Wireshark interface with the 'dns' filter applied. The packet list pane displays a series of DNS packets. Packet 3 is highlighted, showing a standard query response for bitsy.mit.edu with IP address 18.0.72.3. The packet details pane shows the structure of the response, including the query ID, flags, and the answer section with the IP address. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.105	192.168.0.1	DNS	73	Standard query 0xf005 A bitsy.mit.edu
2	0.031533	192.168.0.105	192.168.0.1	DNS	73	Standard query 0xf005 A bitsy.mit.edu
3	0.094519	192.168.0.1	192.168.0.105	DNS	89	Standard query response 0xf005 A bitsy.mit.edu A 18.0.72.3
4	0.094520	192.168.0.1	192.168.0.105	DNS	89	Standard query response 0xf005 A bitsy.mit.edu A 18.0.72.3
5	0.101277	192.168.0.105	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
16	2.118236	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
17	4.123111	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
22	6.127009	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
23	8.136944	192.168.0.105	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

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: 1800 (30 minutes)
Data length: 4
Address: 18.0.72.3
[Request In: 1]
[Time: 0.094519000 seconds]

Висновки:

В даній роботі у ролі клієнта було розглянуто протокол DNS, а саме принципи і деталі його роботи. Був проведений аналіз запитів, їх типів і складу. Також більш детально були розглянуті відповіді, їх кількість, структуру, те чи присутні при цьому додаткові записи тощо. Крім того був отриманий досвід створення запитів за допомогою утиліти nslookup.