

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

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

**Виконав студент 3 курсу
групи КА-72
Бойко Павло
Прийняв Кухарєв С.О.**

Київ – 2020 р.

Контрольні запитання:

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP?
Обидва UDP
Який номер цільового порта запиту DNS?
53
Який номер вихідного порта відповіді DNS?
53
2. На який адрес IP був відправлений запит DNS?
Destination: 192.168.0.1
Чи є цей адрес адресом локального сервера DNS?
Так, це адреса локального сервера
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит?
Type: A
Чи вміщує цей запит деякі можливі компоненти «відповіді»?
У відповіді повернеться весь блок Queries
4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером?
3 відповіді
Що вміщує кожна з цих відповідей?
Одна типу CNAME – канонічне ім'я
Два типу A, що повернули IP адреси
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

No.	Time	Source	Destination	Protocol	Length	Info
1902	8.555824	192.168.0.106	192.168.0.1	DNS	72	Standard query 0x62c6 A www.ietf.org

Frame 1902: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
Ethernet II, Src: Apple_12:88:12 (14:c2:13:12:88:12), Dst: Tp-LinkT_52:65:b6 (f4:f2:6d:52:65:b6)
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 59272, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x62c6
Flags: 0x0100 Standard query
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: 1944]

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

1944 8.613150 192.168.0.1 192.168.0.106 DNS 149 Standard query response 0x62c6 A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

Frame 1944: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_52:65:b6 (f4:f2:6d:52:65:b6), Dst: Apple_12:88:12 (14:c2:13:12:88:12)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106
User Datagram Protocol, Src Port: 53, Dst Port: 59272

Domain Name System (response)

Transaction ID: 0x62c6

Flags: 0x8180 Standard query response, No error

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: 743 (12 minutes, 23 seconds)

Data length: 33

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

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

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

[Request In: 1902]

[Time: 0.057326000 seconds]

7. Яким був цільовий порт повідомлення із запитом DNS?

Destination Port: 53

Яким був вихідний порт повідомлення із відповіддю DNS?

Source Port: 56041

8. На яку IP-адресу був направлений запит DNS?

Destination: 192.168.0.1

Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Так

9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит?
 Тип A
 Чи вміщує цей запит деякі можливі компоненти «відповіді»?
 Queries повернуться разом з відповіддю.
10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером?
 3 відповіді
 З чого складається кожна із цих відповідей?
 2 відповіді типу CNAME і 1 відповідь типу A

No.	Time	Source	Destination	Protocol	Length	Info
1912	2.518789	192.168.0.106	192.168.0.1	DNS	71	Standard query 0x5919 A www.mit.edu

Frame 1912: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0
 Ethernet II, Src: Apple_12:88:12 (14:c2:13:12:88:12), Dst: Tp-LinkT_52:65:b6 (f4:f2:6d:52:65:b6)

Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 60286, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x5919

Flags: 0x0100 Standard query

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: 1918]

No.	Time	Source	Destination	Protocol	Length	Info
1918	2.555782	192.168.0.1	192.168.0.106	DNS	160	Standard query response 0x5919 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.96.143.80

Frame 1918: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface en0, id 0

Ethernet II, Src: Tp-LinkT_52:65:b6 (f4:f2:6d:52:65:b6), Dst: Apple_12:88:12 (14:c2:13:12:88:12)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106

User Datagram Protocol, Src Port: 53, Dst Port: 60286

Domain Name System (response)

Transaction ID: 0x5919

Flags: 0x8180 Standard query response, No error

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: 1767 (29 minutes, 27 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: 27 (27 seconds)
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: 1912]
[Time: 0.036993000 seconds]

11. На яку IP-адресу був направлений запит DNS?

192.168.0.1

Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

Так

12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит?

Типу NS

Чи вміщує цей запит деякі можливі компоненти «відповіді»?

Queries буде повернуте у відповіді

13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером?

8 відповідей

Які сервери DNS були запропоновані у відповіді?

asia2.akam.net, asia1.akam.net, ns1-37.akam.net, use5.akam.net, eur5.akam.net,

usw2.akam.net, use2.akam.net, ns1-173.akam.net

Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

І того, й іншого. Answers містили доменні адреси, а Additional records – IP адреси

No.	Time	Source	Destination	Protocol	Length	Info
201	22.080444	192.168.0.106	192.168.0.1	DNS	67	Standard query
0x2794		NS mit.edu				

Frame 201: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface en0, id 0
Ethernet II, Src: Apple_12:88:12 (14:c2:13:12:88:12), Dst: Tp-LinkT_52:65:b6 (f4:f2:6d:52:65:b6)

Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 62385, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x2794

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: 202]

No.	Time	Source	Destination	Protocol	Length	Info
202	22.126995	192.168.0.1	192.168.0.106	DNS	234	Standard query response 0x2794 NS mit.edu NS asia2.akam.net NS asia1.akam.net NS ns1-37.akam.net NS use5.akam.net NS eur5.akam.net NS usw2.akam.net NS use2.akam.net NS ns1-173.akam.net

Frame 202: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface en0, id 0

Ethernet II, Src: Tp-LinkT_52:65:b6 (f4:f2:6d:52:65:b6), Dst: Apple_12:88:12 (14:c2:13:12:88:12)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.106

User Datagram Protocol, Src Port: 53, Dst Port: 62385

Domain Name System (response)

Transaction ID: 0x2794

Flags: 0x8180 Standard query response, No error

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 asia2.akam.net

Name: mit.edu

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

Time to live: 1800 (30 minutes)

Data length: 16
Name Server: asia2.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: 1800 (30 minutes)
Data length: 8
Name Server: asia1.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: 1800 (30 minutes)
Data length: 9
Name Server: ns1-37.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 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 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 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
[Request In: 201]
[Time: 0.046551000 seconds]

14. На яку IP-адресу був направлений запит DNS?
18.72.0.3
Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?
Ні
Якщо ні, то якому доменному імені відповідає ця IP-адреса?
bitsy.mit.edu
15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит?
Типу А
Чи вміщує цей запит деякі можливі компоненти «відповіді»?
Queries повернеться разом з відповіддю.
16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером?
З чого складається кожна з цих відповідей?
Відповіді не було. У DNS bitsy.mit.edu немає відповідних записів.

Висновки:

У ході роботи було розглянуто DNS, його базову роботу з боку клієнта. Було розглянуто DNS протокол, структури запиту та відповіді. Також використано базові можливості nslookup.