

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
Орел Євгеній
Прийняв Кухарєв С.О.

Київ – 2020 р.

Контрольні запитання:

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP?
UDP і запит і відповідь
Який номер цільового порта запиту DNS?
53
Який номер вихідного порта відповіді DNS?
53
2. На який адрес IP був відправлений запит DNS?
192.168.0.1
Чи є цей адрес адресом локального сервера DNS?
Так
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит?
Type: A
Чи вміщує цей запит деякі можливі компоненти «відповіді»?
У відповіді - 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 – 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
12	1.828130	192.168.0.105	192.168.0.1	DNS	72	Standard query 0x1d3e A www.ietf.org

Frame 12: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
Ethernet II, Src: Apple_d6:45:86 (a4:d1:8c:d6:45:86), Dst: Tp-LinkT_55:94:64 (14:cc:20:55:94:64)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 39054, Dst Port: 53

Source Port: 39054
Destination Port: 53
Length: 38
Checksum: 0xa5a0 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]

Domain Name System (query)
Transaction ID: 0x1d3e
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 13]

]

No.	Time	Source	Destination	Protocol	Length	Info
113	1.839643	192.168.0.1	192.168.0.105	DNS	149	Standard query response 0x1d3e A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85

Frame 13: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface en0, id 0
 Ethernet II, Src: Tp-LinkT_55:94:64 (14:cc:20:55:94:64), Dst: Apple_d6:45:86 (a4:d1:8c:d6:45:86)
 Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105

User Datagram Protocol, Src Port: 53, Dst Port: 39054

Source Port: 53

Destination Port: 39054

Length: 115

Checksum: 0xb43d [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

Domain Name System (response)

Transaction ID: 0x1d3e

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

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: 3582 (59 minutes, 42 seconds)

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: 3582 (59 minutes, 42 seconds)

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: 3582 (59 minutes, 42 seconds)

Data length: 4

Address: 104.20.1.85

[Request In: 12]

[Time: 0.011513000 seconds]

7. Яким був цільовий порт повідомлення із запитом DNS?

53

Яким був вихідний порт повідомлення із відповіддю DNS?

54685

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

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 А

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 з чого складається кожна із цих відповідей?

2 відповіді типу CNAME і 1 відповідь типу А

No.	Time	Source	Destination	Protocol	Length	Info
8	2.389546	192.168.0.105	192.168.0.1	DNS	71	Standard query 0x436f A www.mit.edu

Frame 8: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0
Ethernet II, Src: Apple_d6:45:86 (a4:d1:8c:d6:45:86), Dst: Tp-LinkT_55:94:64
(14:cc:20:55:94:64)

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

User Datagram Protocol, Src Port: 54685, Dst Port: 53

Source Port: 54685

Destination Port: 53

Length: 37

Checksum: 0x11fc [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

[Timestamps]

Domain Name System (query)

Transaction ID: 0x436f

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: 9]

No.	Time	Source	Destination	Protocol	Length	Info
9	2.402239	192.168.0.1	192.168.0.105	DNS	160	Standard query response 0x436f A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 104.75.67.107

Frame 9: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface en0, id 0

Ethernet II, Src: Tp-LinkT_55:94:64 (14:cc:20:55:94:64), Dst: Apple_d6:45:86 (a4:d1:8c:d6:45:86)

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

User Datagram Protocol, Src Port: 53, Dst Port: 54685

Source Port: 53

Destination Port: 54685

Length: 126

Checksum: 0xdba4 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

[Timestamps]

Domain Name System (response)

Transaction ID: 0x436f

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: 3347 (55 minutes, 47 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: 1555 (25 minutes, 55 seconds)

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 104.75.67.107

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 1555 (25 minutes, 55 seconds)

Data length: 4

Address: 104.75.67.107

[Request In: 8]

[Time: 0.012693000 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	22.080433	192.168.0.105	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: 192.168.0.105, 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	22.126495	192.168.0.1	192.168.0.105	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: 192.168.0.105

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:

Під час виконання роботи я розглянув DNS, його базову роботу з боку клієнта. Також розглянув DNS протокол, структури запиту та відповіді. Також використано деякі можливості nslookup.