

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-71
Кічангіна О.Є.
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?
56842
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
1018	6.592660	192.168.0.103	192.168.0.1	DNS	72	Standard query 0xe7f2 A www.ietf.org

Frame 1018: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1
User Datagram Protocol, Src Port: 56842, Dst Port: 53

Source Port: 56842
Destination Port: 53
Length: 38
Checksum: 0x9571 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]

Domain Name System (query)
Transaction ID: 0xe7f2
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
[Response In: 1023]

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

1023 6.609076 192.168.0.1 192.168.0.103 DNS 149 Standard query response 0xe7f2 A
www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

Frame 1023: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 56842

Source Port: 53

Destination Port: 56842

Length: 115

Checksum: 0xdccf [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

Domain Name System (response)

Transaction ID: 0xe7f2

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

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: 1018]

[Time: 0.016416000 seconds]

7. Яким був цільовий порт повідомлення із запитом DNS?

Destination Port: 53

Яким був вихідний порт повідомлення із відповіддю DNS?

Source Port: 63628

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
248	1.563094	192.168.0.103	192.168.0.1	DNS	91	Standard query 0x489e A signaler-pa.clients6.google.com

Frame 248: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0
Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0)

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

User Datagram Protocol, Src Port: 63628, Dst Port: 53

Source Port: 63628

Destination Port: 53

Length: 57

Checksum: 0xcc70 [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

Domain Name System (query)

Transaction ID: 0x489e

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

signaler-pa.clients6.google.com: type A, class IN

Name: signaler-pa.clients6.google.com

[Name Length: 31]

[Label Count: 4]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 258]

No.	Time	Source	Destination	Protocol	Length	Info
258	1.585200	192.168.0.1	192.168.0.103	DNS	107	Standard query response 0x489e A signaler-pa.clients6.google.com A 172.217.20.202

Frame 258: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)

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

User Datagram Protocol, Src Port: 53, Dst Port: 63628

Source Port: 53

Destination Port: 63628

Length: 73

Checksum: 0x7f4d [unverified]

[Checksum Status: Unverified]

[Stream index: 1]

[Timestamps]

Domain Name System (response)

Transaction ID: 0x489e

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

Queries

signaler-pa.clients6.google.com: type A, class IN

Name: signaler-pa.clients6.google.com

[Name Length: 31]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

Answers

signaler-pa.clients6.google.com: type A, class IN, addr 172.217.20.202
[Request In: 248]
[Time: 0.022106000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
4352	35.896730	192.168.0.103	192.168.0.1	DNS	71	Standard query 0xa4f4 A www.mit.edu

Frame 4352: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 0
Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0)

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

User Datagram Protocol, Src Port: 50830, Dst Port: 53

Source Port: 50830

Destination Port: 53

Length: 37

Checksum: 0xbf87 [unverified]

[Checksum Status: Unverified]

[Stream index: 4]

[Timestamps]

Domain Name System (query)

Transaction ID: 0xa4f4

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: 4363]

No.	Time	Source	Destination	Protocol	Length	Info
4363	36.016275	192.168.0.1	192.168.0.103	DNS	160	Standard query response 0xa4f4 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.38.92.10

Frame 4363: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface en0, id 0

Ethernet II, Src: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)

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

User Datagram Protocol, Src Port: 53, Dst Port: 50830

Source Port: 53

Destination Port: 50830

Length: 126

Checksum: 0xd892 [unverified]

[Checksum Status: Unverified]

[Stream index: 4]

[Timestamps]

Domain Name System (response)

Transaction ID: 0xa4f4

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

www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 23.38.92.10

[Request In: 4352]

[Time: 0.119545000 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
7262	28.669230	192.168.0.103	192.168.0.1	DNS	67	Standard query 0x547f NS mit.edu

Frame 7262: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface en0, id 0
 Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0)
 Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.1
 User Datagram Protocol, Src Port: 61091, Dst Port: 53
 Source Port: 61091
 Destination Port: 53
 Length: 33
 Checksum: 0x61de [unverified]
 [Checksum Status: Unverified]
 [Stream index: 3]
 [Timestamps]
 Domain Name System (query)
 Transaction ID: 0x547f
 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: 7267]

No.	Time	Source	Destination	Protocol	Length	Info
7267	28.713838	192.168.0.1	192.168.0.103	DNS	234	Standard query response
0x547f NS mit.edu NS ns1-37.akam.net NS ns1-173.akam.net NS use5.akam.net NS eur5.akam.net NS asia2.akam.net NS asia1.akam.net NS use2.akam.net NS usw2.akam.net						

Frame 7267: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface en0, id 0
 Ethernet II, Src: Tp-LinkT_66:4b:e0 (b0:be:76:66:4b:e0), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)
 Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103
 User Datagram Protocol, Src Port: 53, Dst Port: 61091
 Source Port: 53
 Destination Port: 61091
 Length: 200
 Checksum: 0x3b9f [unverified]
 [Checksum Status: Unverified]
 [Stream index: 3]
 [Timestamps]
 Domain Name System (response)
 Transaction ID: 0x547f
 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 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 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
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 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 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 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 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
[Request In: 7262]
[Time: 0.044608000 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.