

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО
АНАЛІЗУ

Лабораторна робота №3
З дисципліни «Комп'ютерні мережі»

Виконав: студент 3-го курсу

гр. КА-74

Толстіков В.В.

Прийняв: Кухарев С.О.

Київ 2020р.

Пакети для відповідей 1-6:

Frame 538: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0

Ethernet II, Src: 42:9f:23:41:01:5a (42:9f:23:41:01:5a), Dst: Tp-LinkT_ae:15:aa (30:b5:c2:ae:15:aa)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1025, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x42f8

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

[Response In: 545]

Frame 545: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0

Ethernet II, Src: Tp-LinkT_ae:15:aa (30:b5:c2:ae:15:aa), Dst: 42:9f:23:41:01:5a (42:9f:23:41:01:5a)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101

User Datagram Protocol, Src Port: 53, Dst Port: 1025

Domain Name System (response)

Transaction ID: 0x42f8

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: 2

Authority RRs: 0

Additional RRs: 0

Queries

Answers

[Request In: 538]

[Time: 0.074450000 seconds]

Пакети для відповідей 7-10:

Не заслуживающий доверия ответ:

Л ь : e9566.dscb.akamaiedge.net

Addresses: 2a02:26f0:d8:4a5::255e

2a02:26f0:d8:490::255e

104.96.143.80

Aliases: www.mit.edu

www.mit.edu.edgekey.net

Frame 345: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{72CF045B-7343-40C7-B33B-B5654663C87B}, id 0

Ethernet II, Src: 42:9f:23:41:01:5a (42:9f:23:41:01:5a), Dst: Tp-LinkT_ae:15:aa (30:b5:c2:ae:15:aa)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 1025, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x6590

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Response In: 347]

Frame 347: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{72CF045B-7343-40C7-B33B-B5654663C87B}, id 0

Ethernet II, Src: Tp-LinkT_ae:15:aa (30:b5:c2:ae:15:aa), Dst: 42:9f:23:41:01:5a (42:9f:23:41:01:5a)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101

User Datagram Protocol, Src Port: 53, Dst Port: 1025

Domain Name System (response)

Transaction ID: 0x6590

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: 3

Authority RRs: 0

Additional RRs: 0

Queries

Answers

[Request In: 345]

[Time: 0.176675000 seconds]

Пакети для відповідей 11-13:

Не заслуживающий доверия ответ:

mit.edu nameserver = use5.akam.net

mit.edu nameserver = usw2.akam.net

mit.edu nameserver = ns1-37.akam.net

mit.edu nameserver = eur5.akam.net

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

mit.edu nameserver = use2.akam.net

mit.edu nameserver = asia1.akam.net

mit.edu nameserver = asia2.akam.net

522 38.207266 192.168.0.101 192.168.0.1 DNS 67 Standard query 0x0002 NS mit.edu

Frame 522: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{72CF045B-7343-40C7-B33B-B5654663C87B}, id 0

Ethernet II, Src: 42:9f:23:41:01:5a (42:9f:23:41:01:5a), Dst: Tp-LinkT_ae:15:aa (30:b5:c2:ae:15:aa)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 15757, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0002

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

[Response In: 523]

523 38.280048 192.168.0.1 192.168.0.101 DNS 234 Standard query response 0x0002 NS mit.edu NS use5.akam.net NS usw2.akam.net NS ns1-37.akam.net NS eur5.akam.net NS ns1-173.akam.net NS use2.akam.net NS asia1.akam.net NS asia2.akam.net

Frame 523: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{72CF045B-7343-40C7-B33B-B5654663C87B}, id 0

Ethernet II, Src: Tp-LinkT_ae:15:aa (30:b5:c2:ae:15:aa), Dst: 42:9f:23:41:01:5a (42:9f:23:41:01:5a)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101

User Datagram Protocol, Src Port: 53, Dst Port: 15757

Domain Name System (response)

Transaction ID: 0x0002

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: 8

Authority RRs: 0

Additional RRs: 0

Queries

Answers

[Request In: 522]

[Time: 0.072782000 seconds]

Пакети для відповідей 14-16:

Не заслуживающий доверия ответ:

Л ь : www.aiit.or.kr

Address: 58.229.6.225

C:\Users\user>nslookup www.aiit.or.kr bitsy.mit.edu

(root)

primary name server = ns.lanet.ua

responsible mail addr = hostmaster.lanet.kiev.ua

serial = 2013053101

refresh = 21600 (6 hours)

retry = 3600 (1 hour)

expire = 604800 (7 days)

default TTL = 60 (1 min)

⌘ x ð τ x ð : UnKnown

Address: 18.0.72.3

↳ : www.aiit.or.kr

Address: 194.50.85.176

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

242	80.498135	192.168.0.101	192.168.0.1	DNS	73	Standard query 0x9df7 A bitsy.mit.edu
-----	-----------	---------------	-------------	-----	----	---------------------------------------

Frame 242: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{72CF045B-7343-40C7-B33B-B5654663C87B}, id 0

Ethernet II, Src: 42:9f:23:41:01:5a (42:9f:23:41:01:5a), Dst: Tp-LinkT_ae:15:aa (30:b5:c2:ae:15:aa)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 24153, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x9df7

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

[Response In: 243]

243	80.507110	192.168.0.1	192.168.0.101	DNS	89	Standard query response 0x9df7 A bitsy.mit.edu A 18.0.72.3
-----	-----------	-------------	---------------	-----	----	--

Frame 243: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{72CF045B-7343-40C7-B33B-B5654663C87B}, id 0

Ethernet II, Src: Tp-LinkT_ae:15:aa (30:b5:c2:ae:15:aa), Dst: 42:9f:23:41:01:5a (42:9f:23:41:01:5a)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101

User Datagram Protocol, Src Port: 53, Dst Port: 24153

Domain Name System (response)

Transaction ID: 0x9df7

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: 1

Authority RRs: 0

Additional RRs: 0

Queries

Answers

[Request In: 242]

[Time: 0.008975000 seconds]

Контрольні запитання:

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, domain (53), 24153 (24153)

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

192.168.1.1 , Так, є.

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

Типу A (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, Primary name or Addr

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?

domain (53), 15757 (15757)

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

192.168.1.1, Так

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

Типу A (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, Name, Type, Class, Time to live, Data length, Primaryname

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

192.168.1.1, так

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

Типу NS, 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?

use5.akam.net usw2.akam.net ns1-37.akam.net eur5.akam.net ns1-173.akam.net use2.akam.net asia1.akam.net asia2.akam.net. Лише за допомогою доменного імені.

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?

192.168.1.1 - так, 18.72.0.3 - bitsy.mit.edu

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

Запита типу A та PTR. Ні.

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

Один запис, що складається з Name, Type, Class, Time to live, Data length, Addr.

Висновки: В процесі виконання даної лабораторної роботи я оволоділа знаннями про пакети DNS, що є необхідними для дослідження мережевих протоколів.