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

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

Виконала: студентка 3 курсу
групи КА-77
Тарасевич А.А.
Прийняв: Кухарєв С.О.

Київ – 2020р.

1-6

Запит:

Frame 48: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9), Dst: 66:c2:de:fb:31:14 (66:c2:de:fb:31:14)

Internet Protocol Version 4, Src: 192.168.43.213, Dst: 192.168.43.1

User Datagram Protocol, Src Port: 61108, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xb916

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

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: 49]

Відповідь:

Frame 49: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: 66:c2:de:fb:31:14 (66:c2:de:fb:31:14), Dst: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9)

Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.213

User Datagram Protocol, Src Port: 53, Dst Port: 61108

Domain Name System (response)

Transaction ID: 0xb916

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

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: 57 (57 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: 54 (54 seconds)

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: 54 (54 seconds)

Data length: 4

Address: 104.20.0.85

[Request In: 48]

[Time: 0.092600000 seconds]

7-10

C:\Users\Dmkrol>nslookup www.mit.edu

Не заслуживающий доверия ответ:

Addresses: 2a02:26f0:10e:1a2::255e

2a02:26f0:10e:197::255e

104.96.143.80

Aliases: www.mit.edu

www.mit.edu.edgekey.net

Запит:

Відповідь:

т
х
ё
т

Не заслуживающий доверия ответ:

Запит:

Відповідь

Frame 76: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: ASUSTekC_bb:49:ec (0c:9d:92:bb:49:ec), Dst: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9)

Internet Protocol Version 4, Src: 31.43.120.254, Dst: 172.16.7.104

User Datagram Protocol, Src Port: 53, Dst Port: 1035

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

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: 1628 (27 minutes, 8 seconds)

Data length: 17

Name Server: ns1-37.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: 1628 (27 minutes, 8 seconds)

Data length: 8

Name Server: asia2.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: 1628 (27 minutes, 8 seconds)

Data length: 10

Name Server: ns1-173.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: 1628 (27 minutes, 8 seconds)

Data length: 8

Name Server: asia1.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: 1628 (27 minutes, 8 seconds)

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: 1628 (27 minutes, 8 seconds)

Data length: 7

Name Server: usw2.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: 1628 (27 minutes, 8 seconds)

Data length: 7

Name Server: use5.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: 1628 (27 minutes, 8 seconds)

Data length: 7

Name Server: use2.akam.net

[Request In: 75]

[Time: 0.107354000 seconds]

14-16

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

┬xЁтxЁ: bitsy.mit.edu

Address: 18.0.72.3

Не заслуживающий доверия ответ:

└

Address: 58.229.6.225

Запит:

Відповідь:

Frame 21: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: ASUSTekC_bb:49:ec (0c:9d:92:bb:49:ec), Dst: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9)

Internet Protocol Version 4, Src: 31.43.120.254, Dst: 172.16.7.104

User Datagram Protocol, Src Port: 53, Dst Port: 16011

Domain Name System (response)

Transaction ID: 0x5aa7

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

bitsy.mit.edu: type A, class IN

Name: bitsy.mit.edu

[Name Length: 13]

[Label Count: 3]

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: 1779 (29 minutes, 39 seconds)

Data length: 4

Address: 18.0.72.3

[Request In: 20]

[Time: 0.032112000 seconds]

Запит:

Frame 22: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9), Dst: Fortinet_dc:64:1d (00:09:0f:dc:64:1d)

Internet Protocol Version 4, Src: 172.16.7.104, Dst: 18.0.72.3

User Datagram Protocol, Src Port: 16012, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x0001

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

3.72.0.18.in-addr.arpa: type PTR, class IN

Name: 3.72.0.18.in-addr.arpa

[Name Length: 22]

[Label Count: 6]

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

[Response In: 23]

Відповідь:

Frame 23: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface

\Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0

Ethernet II, Src: ASUSTekC_bb:49:ec (0c:9d:92:bb:49:ec), Dst: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9)

Internet Protocol Version 4, Src: 18.0.72.3, Dst: 172.16.7.104

User Datagram Protocol, Src Port: 53, Dst Port: 16012

Domain Name System (response)

Transaction ID: 0x0001

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

3.72.0.18.in-addr.arpa: type PTR, class IN

Name: 3.72.0.18.in-addr.arpa

[Name Length: 22]

[Label Count: 6]

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

Answers

3.72.0.18.in-addr.arpa: type PTR, class IN, bitsy.mit.edu

Name: 3.72.0.18.in-addr.arpa

Type: PTR (domain name PoinTeR) (12)

Class: IN (0x0001)

Time to live: 1799 (29 minutes, 59 seconds)

Data length: 15

Domain Name: bitsy.mit.edu

[Request In: 22]

[Time: 0.041456000 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?

U
d
o
m
a

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?**

104.20.1.85 - так, співпадає з другою відповіддю.

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), 58894 (58894)

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?**

так.

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

Перший типу A, останній - AAAA. 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?

Тільки одна відповідь за допомогою адреси

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?**

- так, 31.43.120.254 - bitsy.mit.edu

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

2 запита типу A та один - AAAA. 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.

Висновок:

На цій роботі я навчився перехоплювати та аналізувати деталі протоколу DNS.