

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 3
З дисципліни: Комп'ютерні мережі

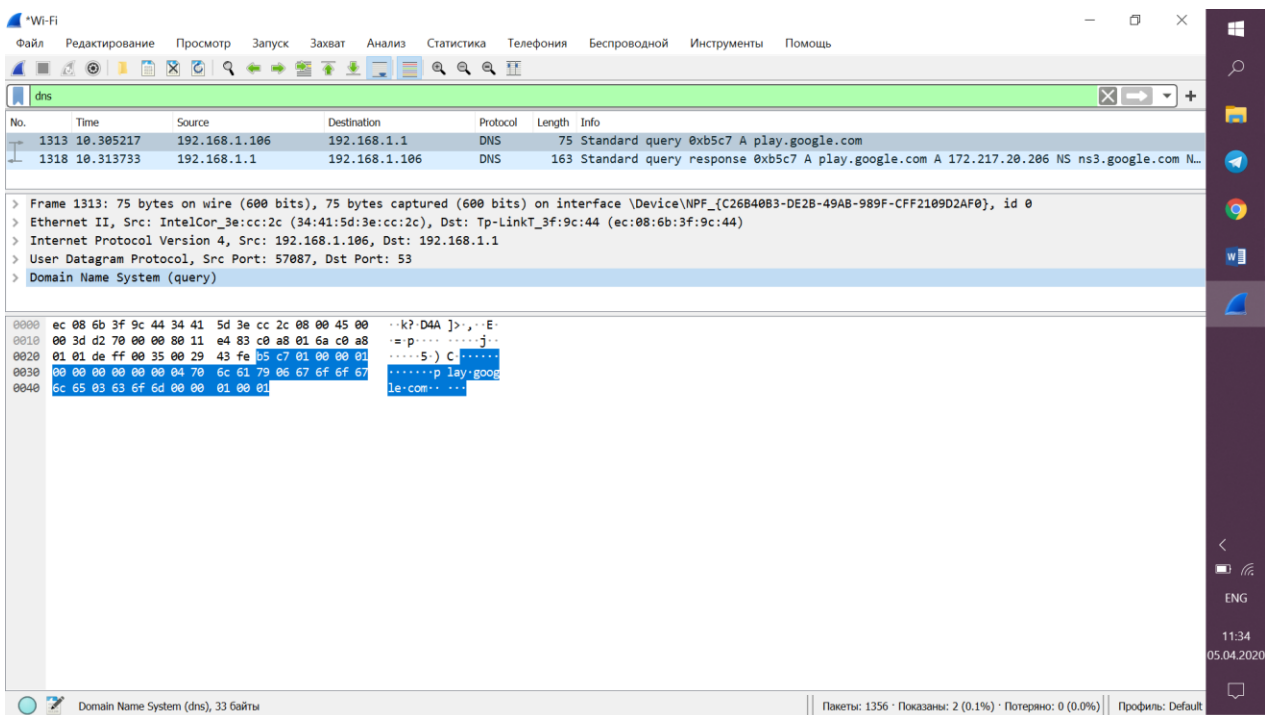
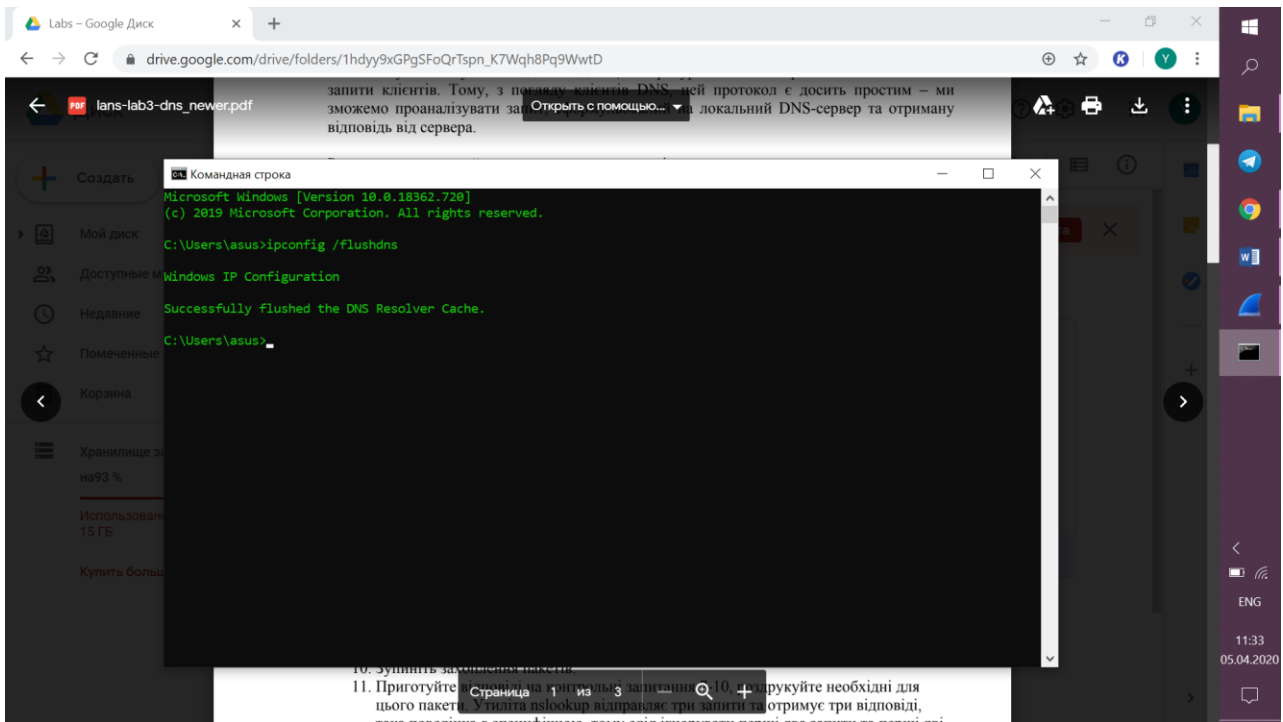
Протокол DNS

Виконала:
Студентка III курсу
Групи КА-77
Яцько Я. В.
Перевірів: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи



Non-authoritative answer:

Name: e9566.dscb.akamaiedge.net

Addresses: 2a02:26f0:d200:191::255e

2a02:26f0:d200:19e::255e

104.109.79.114

Aliases: www.mit.edu

www.mit.edu.edgekey.net

Wireshark packet capture showing DNS traffic. The packet list shows a standard query and response. The packet details pane shows the query for www.mit.edu. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
119	6.863570	192.168.1.106	192.168.1.1	DNS	78	Standard query 0x06ec A m.qualifiedring.com
120	6.868049	192.168.1.1	192.168.1.106	DNS	204	Standard query response 0x06ec A m.qualifiedring.com CNAME qualify-t-ring.azurefd.net
142	7.066109	192.168.1.106	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
143	7.068213	192.168.1.1	192.168.1.106	DNS	104	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-WRT
144	7.069705	192.168.1.106	192.168.1.1	DNS	67	Standard query 0x0002 NS mit.edu
146	7.104886	192.168.1.1	192.168.1.106	DNS	362	Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS use5.akam.net NS ns1-17...

Frame 119: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface...
Ethernet II, Src: IntelCor_3e:cc:2c (34:41:5d:3e:cc:2c), Dst: Tp-LinkT_3f:6d:00:00:01:00:01
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 57840, Dst Port: 53
Domain Name System (query)

0000 ec 08 6b 3f 9c 44 34 41 5d 3e cc 2c 08 00 45 00 ...k?D4A]>...E-
0010 00 40 d2 aa 00 00 80 11 e4 46 c0 a8 01 6a c0 a8 ...@.....F...j...
0020 01 01 e1 f0 00 35 00 2c 26 4f 06 ec 01 00 00 01 ...S., 80.....
0030 00 00 00 00 00 00 01 6d 0c 71 75 61 6c 69 66 79m qualify
0040 74 72 69 6e 67 03 63 6f 6d 00 00 01 00 01 ...tring co m.....

Command Prompt
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\asus>nslookup -type=NS mit.edu
Server: DD-WRT
Address: 192.168.1.1
Non-authoritative answer:
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net
eur5.akam.net internet address = 23.74.25.64
use2.akam.net internet address = 96.7.49.64
use5.akam.net internet address = 2.16.40.64
usw2.akam.net internet address = 184.26.161.64
asia1.akam.net internet address = 95.180.175.64
asia2.akam.net internet address = 95.181.36.64
ns1-37.akam.net internet address = 193.108.91.37
ns1-173.akam.net internet address = 193.108.91.173
C:\Users\asus>

Wireshark packet capture showing DNS traffic. The packet list shows a standard query and response. The packet details pane shows the query for www.mit.edu. The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
29	2.709102	192.168.1.106	192.168.1.1	DNS	73	Standard query 0x713d A bitsy.mit.edu
30	2.749275	192.168.1.1	192.168.1.106	DNS	384	Standard query response 0x713d A bitsy.mit.edu A 18.0.72.3 NS asia2.akam.net NS asia1...
31	2.756465	192.168.1.106	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
48	4.765842	192.168.1.106	18.0.72.3	DNS	74	Standard query 0x0002 A www.ait.or.kr
67	6.777883	192.168.1.106	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.ait.or.kr

Frame 29: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface...
Ethernet II, Src: IntelCor_3e:cc:2c (34:41:5d:3e:cc:2c), Dst: Tp-LinkT_3f:6d:00:00:01:00:01
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 60604, Dst Port: 53
Domain Name System (query)

0000 ec 08 6b 3f 9c 44 34 41 5d 3e cc 2c 08 00 45 00 ...k?D4A]>...E-
0010 00 3b d2 af 00 00 80 11 e4 46 c0 a8 01 6a c0 a8 ...@.....F...j...
0020 01 01 ec bc 35 00 27 63 a8 71 3d 01 00 00 01 ...S.' c;qe....
0030 00 00 00 00 00 00 05 62 69 74 73 79 03 6d 69 74b bitsy mit
0040 03 65 64 75 00 00 01 00 01 ...edu.....

Command Prompt
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\asus>nslookup www.ait.or.kr bitsy.mit.edu
DNS request timed out.
timeout was 2 seconds.
Server: Unknown
Address: 18.0.72.3
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Request to Unknown timed-out
C:\Users\asus>

Контрольні питання

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?

```
Frame 1313: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{C26B40B3-...}
Ethernet II, Src: IntelCor_3e:cc:2c (34:41:5d:3e:cc:2c), Dst: Tp-LinkT_3f:9c:44 (ec:08:6b:3f:9c:44)
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 57087, Dst Port: 53
Domain Name System (query)
```

Цільовий порт: 53

Вихідний порт: 57087

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

IP: 192.168.1.106. Так є.

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

Цей запит – є запитом стандартного типу. Вміщує.

Response in : 1318

4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

```
▼ Domain Name System (response)
  Transaction ID: 0xb5c7
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 4
  Additional RRs: 0
  > Queries
  > Answers
  > Authoritative nameservers
    [Request In: 1313]
    [Time: 0.008516000 seconds]
```

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 співпадає.

6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?

Так виконує.

7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

Цільовий: 192.168.1.106

Вихідний: 192.168.1.1

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 є адресою локального сервера.

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

Цей запит – є запитом стандартного типу. Вміщує

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

The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list on the left shows several DNS packets. The selected packet (No. 119) is a Standard query from 192.168.1.106 to 192.168.1.1. The packet details pane shows the structure of the DNS query, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and the Domain Name System (query) section. The packet bytes pane shows the raw data of the query, including the magic number, flags, and the query name 'm.qualifytring.com'.

No.	Time	Source	Destination	Protocol	Length	Info
119	6.863570	192.168.1.106	192.168.1.1	DNS	78	Standard query 0x06ec A m.qualifytring.com
120	6.868049	192.168.1.1	192.168.1.106	DNS	204	Standard query response 0x06ec A m.qualifytring.com CNAME qualify-t-ring.azurefd.net ..
142	7.066109	192.168.1.106	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
143	7.068213	192.168.1.1	192.168.1.106	DNS	104	Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-WRT
144	7.069705	192.168.1.106	192.168.1.1	DNS	67	Standard query 0x0002 NS mit.edu
146	7.104886	192.168.1.1	192.168.1.106	DNS	362	Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS use5.akam.net NS ns1-17..

Frame 119: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{C26B40B3-DE2B-49AB-989F-CFF2109D2AF0}, id 0
> Ethernet II, Src: IntelCor_3e:cc:2c (34:41:5d:3e:cc:2c), Dst: Tp-LinkT_3f:9c:44 (ec:08:6b:3f:9c:44)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 57840, Dst Port: 53
> Domain Name System (query)

0000 ec 08 6b 3f 9c 44 34 41 5d 3e cc 2c 08 00 45 00 ..k?.D4A]>...E-
0010 00 40 d2 aa 00 00 00 11 e4 46 c0 a8 01 6a c0 a8 @.....F...j..
0020 01 01 e1 f0 00 35 00 2c 26 4f 06 ec 01 00 00 015...80.....
0030 00 00 00 00 00 01 6d 0c 71 75 61 6c 69 66 79m..qualify
0040 74 72 69 6e 67 03 6f 6d 00 00 01 00 01 tring co m.....

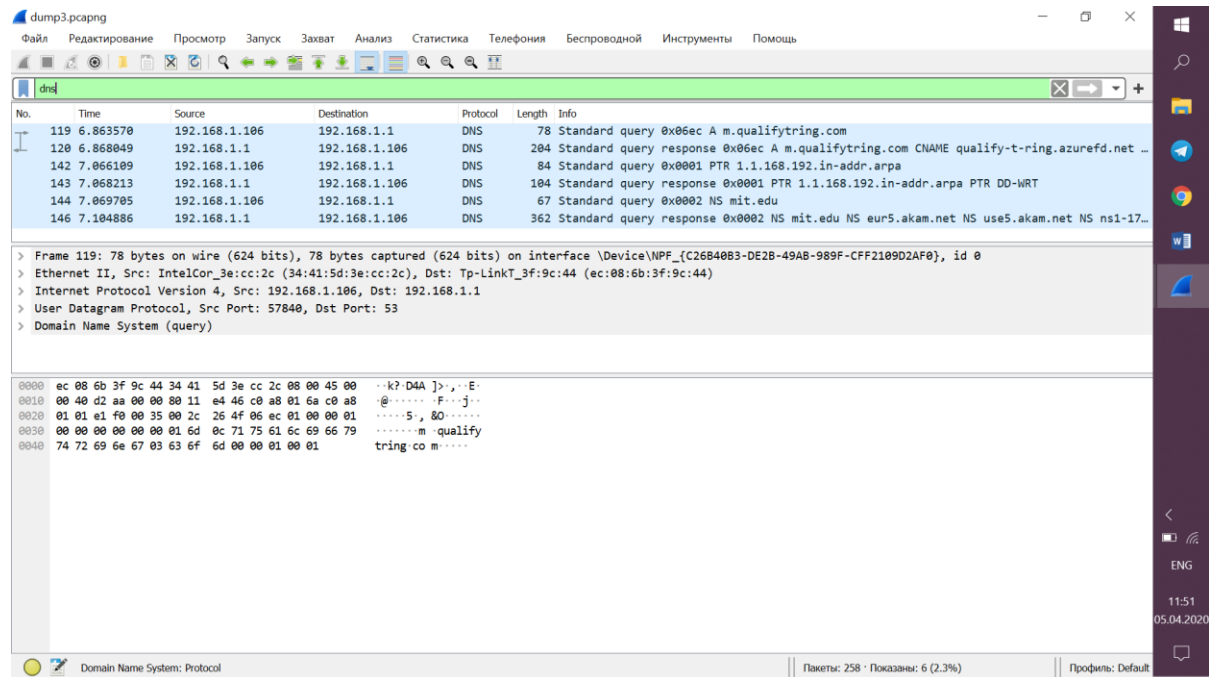
11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

IP: 192.168.1.1. Так є.

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

Стандартний тип запиту. Так вміщує.

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?



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?

IP: 18.0.72.3. Не є адресою локального сервера.

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

Стандартний тип запиту. Ні не вміщує.

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

Відповідь не була отримана.

Висновок

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було проаналізовано протоколи DNS та проведено аналіз деталей роботи даного протоколу.