

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

Лабораторна робота № 3
З дисципліни: Комп'ютерні мережі

Протоколи DNS

Виконав:
Студент III курсу
Групи КА-77
Жук В.М.
Перевірив:
Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи

```
Last login: Sat Mar 28 22:18:56 on ttys000

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
MacBook-Pro-Roman:~ roman$ dscacheutil -flushcache
MacBook-Pro-Roman:~ roman$ sudo killall -HUP mDNSResponder
[Password:
MacBook-Pro-Roman:~ roman$ █
```

The image shows a Wireshark packet capture window titled "Wi-Fi: en0". The filter is set to "dns". The packet list shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
1078	6.315083	192.168.1.2	192.168.1.1	DNS	72	Standard query 0x7016 A www.ietf.org
1079	6.327053	192.168.1.1	192.168.1.2	DNS	149	Standard query response 0x7016 A www.ietf.o

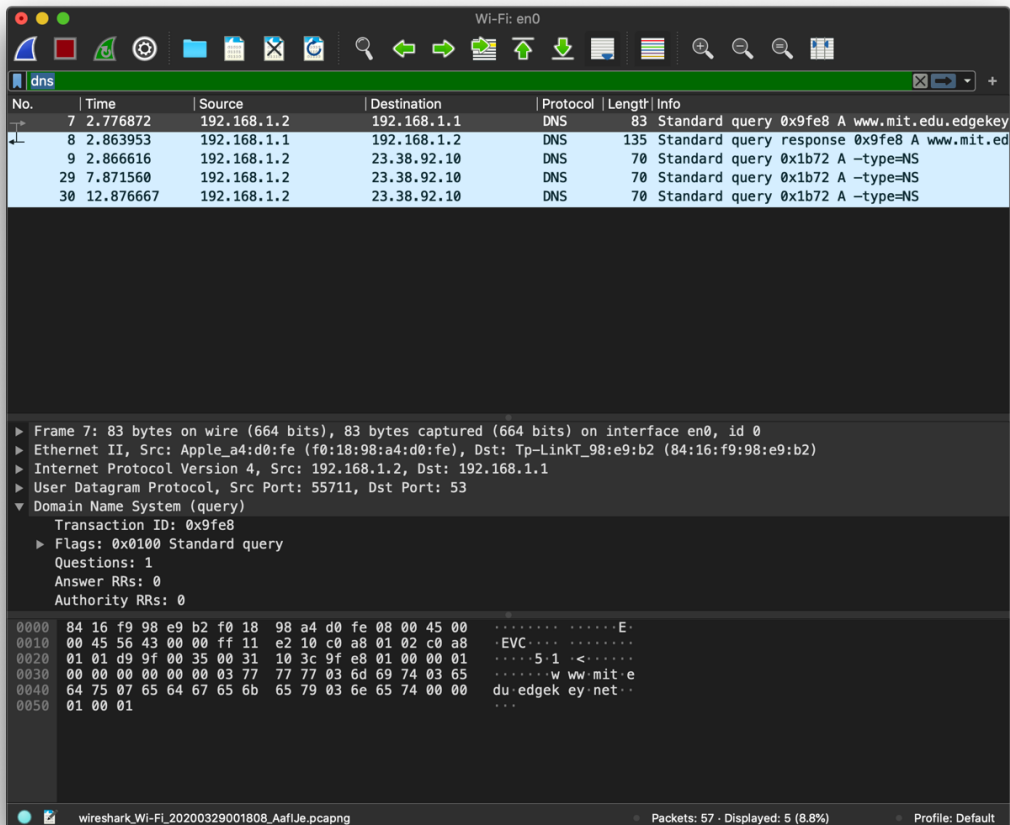
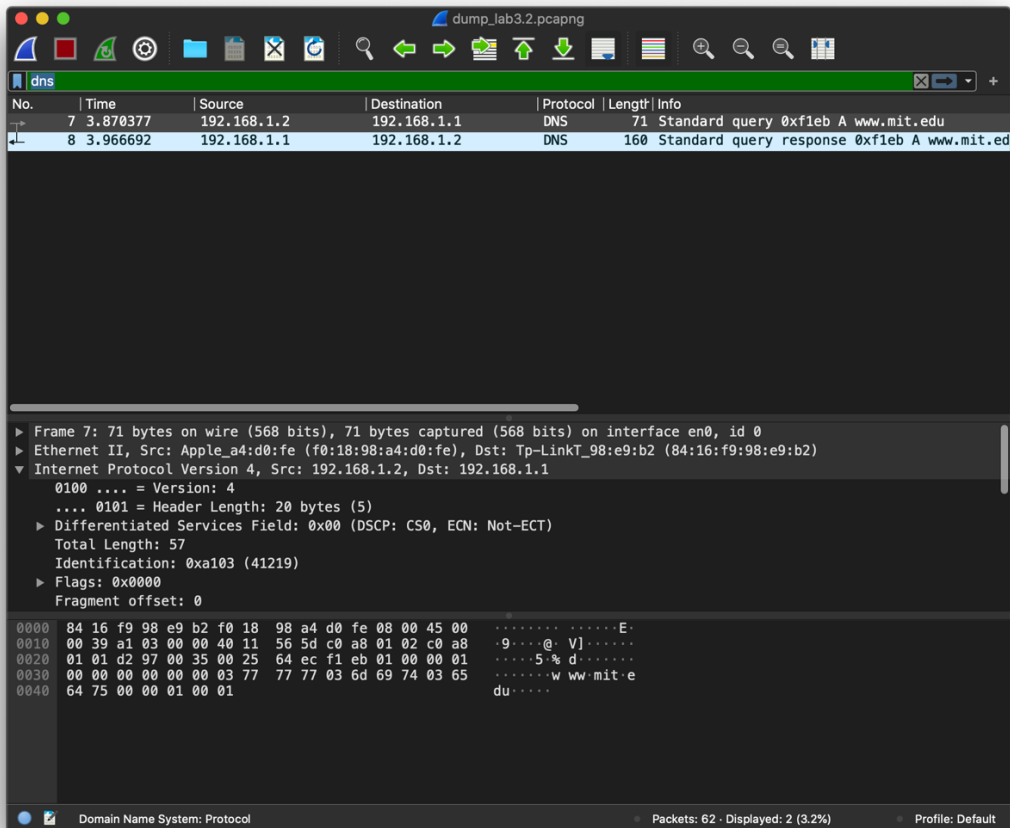
The packet details pane for packet 1078 (Standard query) shows:

- Transaction ID: 0x7016
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
 - [Response In: 1079]

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  84 16 f9 98 e9 b2 f0 18 98 a4 d0 fe 08 00 45 00  .....E.
0010  00 3a 01 23 00 00 ff 11 37 3c c0 a8 01 02 c0 a8  :.#....7<....
0020  01 01 df 4d 00 35 00 26 0a 70 70 16 01 00 00 01  ..M.5.&pp.....
```

The status bar at the bottom indicates: Domain Name System: Protocol, Packets: 2740 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) · Profile: Default



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.2	192.168.1.1	DNS	73	Standard query 0x27cb A bitsy.mit.edu
2	1.004016	192.168.1.2	192.168.1.1	DNS	73	Standard query 0x27cb A bitsy.mit.edu
3	1.632546	192.168.1.1	192.168.1.2	DNS	89	Standard query response 0x27cb A bitsy.mi...
4	1.635013	192.168.1.2	18.0.72.3	DNS	74	Standard query 0x062d A www.aiit.or.kr
5	2.866411	192.168.1.1	192.168.1.2	DNS	89	Standard query response 0x27cb A bitsy.mi...
7	6.639985	192.168.1.2	18.0.72.3	DNS	74	Standard query 0x062d A www.aiit.or.kr
8	11.644156	192.168.1.2	18.0.72.3	DNS	74	Standard query 0x062d A www.aiit.or.kr

▶ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface en0, id 0
 ▶ Ethernet II, Src: Apple_a4:d0:fe (f0:18:98:a4:d0:fe), Dst: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2)
 ▶ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
 ▶ User Datagram Protocol, Src Port: 53678, Dst Port: 53
 ▶ Domain Name System (query)

0000 84 16 f9 98 e9 b2 f0 18 98 a4 d0 fe 08 00 45 00E:
 Domain Name System: Protocol Packets: 18 · Displayed: 7 (38.9%) · Dropped: 0 (0.0%) · Profile: Default

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?

Цільовий порт: 53

Вихідний порт: 57165

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

IP: 192.168.1.2. 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.

dns.response_in 1079

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

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 104.20.0.85

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85

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.

No.	Time	Source	Destination	Protocol	Length	Info
1078	6.315083	192.168.1.2	192.168.1.1	DNS	72	Standard query 0x7016 A www.ietf.org

Frame 1078: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
Ethernet II, Src: Apple_a4:d0:fe (f0:18:98:a4:d0:fe), Dst: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1

0100= Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 58

Identification: 0x0123 (291)

Flags: 0x0000

Fragment offset: 0

Time to live: 255

Protocol: UDP (17)

Header checksum: 0x373c [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.2

Destination: 192.168.1.1

User Datagram Protocol, Src Port: 57165, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x7016

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

[Response In: 1079]

No.	Time	Source	Destination	Protocol	Length	Info
1079	6.327053	192.168.1.1	192.168.1.2	DNS	149	Standard query response 0x7016 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85

Frame 1079: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2), Dst: Apple_a4:d0:fe (f0:18:98:a4:d0:fe)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2

0100= Version: 4

.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 135
Identification: 0x5057 (20567)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 62
Protocol: UDP (17)
Header checksum: 0x68bb [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.1
Destination: 192.168.1.2
User Datagram Protocol, Src Port: 53, Dst Port: 57165
Domain Name System (response)
Transaction ID: 0x7016
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
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 104.20.0.85
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
[Request In: 1078]
[Time: 0.011970000 seconds]

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

Цільовий: 53

Вихідний: 53911

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»?

Type: A, Queries повернеться разом з відповіддю.

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

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: 1800 (30 minutes)

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: 60 (1 minute)

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

e9566.dscb.akamaiedge.net: type A, class IN, addr 104.96.143.80

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20 (20 seconds)

Data length: 4

Address: 104.96.143.80

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

IP: 23.38.92.10, Ні, не є.

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

Типу NS, Queries буде повернуте у відповіді

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?

No.	Time	Source	Destination	Protocol	Length	Info
7	2.776872	192.168.1.2	192.168.1.1	DNS	83	Standard query 0x9fe8 A www.mit.edu.edgekey.net

Frame 7: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface en0, id 0

Ethernet II, Src: Apple_a4:d0:fe (f0:18:98:a4:d0:fe), Dst: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 55711, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x9fe8
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 8]

No.	Time	Source	Destination	Protocol	Length	Info
8	2.863953	192.168.1.1	192.168.1.2	DNS	135	Standard query response
0x9fe8 A www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.38.92.10						

Frame 8: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface en0, id 0
Ethernet II, Src: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2), Dst: Apple_a4:d0:fe (f0:18:98:a4:d0:fe)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
User Datagram Protocol, Src Port: 53, Dst Port: 55711
Domain Name System (response)

Transaction ID: 0x9fe8
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
Answers
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: 60 (1 minute)
Data length: 24
CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type A, class IN, addr 23.38.92.10
Name: e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20 (20 seconds)

Data length: 4

Address: 23.38.92.10

[Request In: 7]

[Time: 0.087081000 seconds]

No.	Time	Source	Destination	Protocol	Length	Info
9	2.866616	192.168.1.2	23.38.92.10	DNS	70	Standard query 0x1b72 A – type=NS

Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0

Ethernet II, Src: Apple_a4:d0:fe (f0:18:98:a4:d0:fe), Dst: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 23.38.92.10

User Datagram Protocol, Src Port: 60874, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x1b72

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

No.	Time	Source	Destination	Protocol	Length	Info
29	7.871560	192.168.1.2	23.38.92.10	DNS	70	Standard query 0x1b72 A – type=NS

Frame 29: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0

Ethernet II, Src: Apple_a4:d0:fe (f0:18:98:a4:d0:fe), Dst: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 23.38.92.10

User Datagram Protocol, Src Port: 60874, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x1b72

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

No.	Time	Source	Destination	Protocol	Length	Info
30	12.876667	192.168.1.2	23.38.92.10	DNS	70	Standard query 0x1b72 A – type=NS

Frame 30: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface en0, id 0

Ethernet II, Src: Apple_a4:d0:fe (f0:18:98:a4:d0:fe), Dst: Tp-LinkT_98:e9:b2 (84:16:f9:98:e9:b2)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 23.38.92.10

User Datagram Protocol, Src Port: 60874, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x1b72

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

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»?
Типу NS, Queries буде повернуте у відповіді

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.

Висновок:

В ході виконання даної лабораторної роботи, були покращено навички використання програми Wireshark для захоплення пакетів. Було

проаналізовано протоколи DNS та було проведено аналіз деталей роботи даних протоколів.