



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-74
Поліщук А.Б.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи

Администратор: Командная строка

Microsoft Windows [Version 10.0.18362.778]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\WINDOWS\system32>ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.

C:\WINDOWS\system32>

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
17	3.638891	192.168.0.106	192.168.0.1	DNS	74	Standard query 0x8d3d A www.google.com
18	3.654366	192.168.0.1	192.168.0.106	DNS	338	Standard query response 0x8d3d A www.google.com A 172.217.16.36 NS ns1.google.com NS ns2.google.com NS ns3.google.com
19	3.688361	192.168.0.106	192.168.0.1	DNS	72	Standard query 0xaa5b A www.ietf.org
23	3.978638	192.168.0.1	192.168.0.106	DNS	459	Standard query response 0xaa5b A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85 N...
86	7.897935	192.168.0.106	192.168.0.1	DNS	79	Standard query 0x984c A clients6.google.com
87	7.903941	192.168.0.1	192.168.0.106	DNS	367	Standard query response 0x984c A clients6.google.com CNAME clients1.google.com A 172.217.16.46 NS ns4.google.com...

> Frame 19: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{F69135E3-F800-4849-9B7E-D6BA2ECEC81A}, id 0
> Ethernet II, Src: 5a:00:b4:e5:9c:fb (5a:00:b4:e5:9c:fb), Dst: Tp-LinkT_fb:ed:d2 (78:4f:57:fb:ed:d2)
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 61495, Dst Port: 53
> Domain Name System (query)

0000 70 4f 57 fb ed d2 5a 00 b4 e5 9c fb 08 00 45 00 p0w...Z-E-
0010 00 3a 0c 61 00 00 80 11 ac 96 c0 a8 00 6a c0 a8 ..:a.....j..
0020 00 01 f0 37 00 35 00 26 c0 d8 aa 5b 01 00 00 01 ...7:5& ...[....
0030 00 00 00 00 00 00 03 77 77 04 69 65 74 66 03w ww-ietf-
0040 6f 72 67 00 00 01 00 01 org.....

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Encapsulation type (frame_encap_type) | Пакеты: 196 · Показаны: 6 (3.1%) · Потеряно: 0 (0.0%) | Профиль: Default

```
Администратор: Командная строка
Microsoft Windows [Version 10.0.18362.778]
(c) Корпорация Майкрософт (Microsoft Corporation), 2019. Все права защищены.

C:\WINDOWS\system32>ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.

C:\WINDOWS\system32>nslookup www.mit.edu
Server: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
Server: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d8:3a2::255e
           2a02:26f0:d8:389::255e
           92.123.2.59
Aliases:   www.mit.edu
           www.mit.edu.edgekey.net

C:\WINDOWS\system32>
```

```
Администратор: Командная строка

Addresses: 2a02:26f0:d8:3a2::255e
           2a02:26f0:d8:389::255e
           92.123.2.59
Aliases:   www.mit.edu
           www.mit.edu.edgekey.net

C:\WINDOWS\system32>nslookup -type=NS mit.edu
Server: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net

C:\WINDOWS\system32>
```

Администратор: Командная строка

pxEtXĖ: UnKnown

Address: 192.168.0.1

Не заслуживающий доверия ответ:

mit.edu nameserver = usw2.akam.net

mit.edu nameserver = asia2.akam.net

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

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

mit.edu nameserver = eur5.akam.net

mit.edu nameserver = asia1.akam.net

mit.edu nameserver = use5.akam.net

mit.edu nameserver = use2.akam.net

C:\WINDOWS\system32>nslookup www.aiit.or.kr bitsy.mit.edu

DNS request timed out.

timeout was 2 seconds.

pxEtXĖ: 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.

*** Превышено время ожидания запроса UnKnown

C:\WINDOWS\system32>

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?

DNS використовує UDP.

The screenshot shows the Wireshark interface with a packet capture of DNS traffic. The packet list pane shows three packets:

No.	Time	Source	Destination	Protocol	Length	Info
1684	10.551270	192.168.0.104	192.168.0.1	DNS	72	Standard query 0x23a4 A www.ietf.org
1696	10.671519	192.168.0.1	192.168.0.104	DNS	149	Standard query response 0x23a4 A www.ietf.org CNAME www.ietf.org.cdn.c...
1772	11.280310	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x03cf A analytics.ietf.org

The packet details pane for the first packet (No. 1684) is expanded, showing the following structure:

- > Frame 1684: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}, id 0
- > Ethernet II, Src: IntelCor_d6:66:72 (3c:f8:62:d6:66:72), Dst: Tp-LinkT_a1:df:10 (74:da:88:a1:df:10)
- > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
- ✓ User Datagram Protocol, Src Port: 10372, Dst Port: 53
 - Source Port: 10372
 - Destination Port: 53
 - Length: 38
 - Checksum: 0x0f46 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 172]
 - > [Timestamps]
- > Domain Name System (query)

Цільовий порт: 53

Вихідний порт: 10372

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?
IP: 192.168.0.1 Так є.
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

*Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
1684	10.551270	192.168.0.104	192.168.0.1	DNS	72	Standard query 0x23a4 A www.ietf.org
1696	10.671519	192.168.0.1	192.168.0.104	DNS	149	Standard query response 0x23a4 A www.ietf.org
1772	11.280310	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x03cf A analytics.ietf.org

> Frame 1684: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}, id 0

> Ethernet II, Src: IntelCor_d6:66:72 (3c:f8:62:d6:66:72), Dst: Tp-LinkT_a1:df:10 (74:da:88:a1:df:10)

> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1

> User Datagram Protocol, Src Port: 10372, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x23a4

> 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: 1696]

```

0000 74 da 88 a1 df 10 3c f8 62 d6 66 72 08 00 45 00  t.....< b-fr..E-
0010 00 3a 44 e4 00 00 80 11 74 15 c0 a8 00 68 c0 a8  .:D..... t...h..
0020 00 01 28 84 00 35 00 26 0f 46 23 a4 01 00 00 01  ..(..5.& .F#.....
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03  ....w ww.ietf.
0040 6f 72 67 00 00 01 00 01  org.....
  
```

Тип запиту – А . Вміщує.

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

*Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
1316	8.074875	192.168.0.1	192.168.0.104	DNS	129	Standard query response 0x2850 A fonts.gstatic.com CNAME.gstaticssl1.l.google.com A 172.16.0.104
1684	10.551270	192.168.0.104	192.168.0.1	DNS	72	Standard query 0x23a4 A www.ietf.org
1696	10.671519	192.168.0.1	192.168.0.104	DNS	149	Standard query response 0x23a4 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85
1772	11.280310	192.168.0.104	192.168.0.1	DNS	78	Standard query 0x03cf A analytics.ietf.org
1773	11.336583	192.168.0.104	192.168.0.1	DNS	83	Standard query 0xc9fc A response.cu-riety-ba.com

> Frame 1696: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}, id 0

> Ethernet II, Src: Tp-LinkT_a1:df:10 (74:da:88:a1:df:10), Dst: IntelCor_d6:66:72 (3c:f8:62:d6:66:72)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104

> User Datagram Protocol, Src Port: 53, Dst Port: 10372

> Domain Name System (response)

Transaction ID: 0x23a4

> 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: 1684]

[Time: 0.120249000 seconds]

3 відповіді.

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: 53

Вихідний: 1036

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

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

10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей? – 3 відповіді.

```
▼ 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: 1294 (21 minutes, 34 seconds)
    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: 11 (11 seconds)
    Data length: 24
    CNAME: e9566.dscb.akamaiedge.net
  ▼ e9566.dscb.akamaiedge.net: type A, class IN, addr 92.123.2.59
    Name: e9566.dscb.akamaiedge.net
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 19 (19 seconds)
    Data length: 4
    Address: 92.123.2.59
\[Request In: 1166\]
```

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

dns						
No.	Time	Source	Destination	Protocol	Length	Info
3482	15.218774	192.168.0.104	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
3484	15.238941	192.168.0.1	192.168.0.104	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
3485	15.240562	192.168.0.104	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
3501	15.292576	192.168.0.1	192.168.0.104	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS eur5.akam.net
3682	16.442192	192.168.0.104	192.168.0.1	DNS	75	Standard query 0x1aca A docs.google.com
3698	16.503421	192.168.0.1	192.168.0.104	DNS	91	Standard query response 0x1aca A docs.google.com A 172.217.16.14

> Frame 3482: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}, id 0
 > Ethernet II, Src: IntelCor_d6:66:72 (3c:f8:62:d6:66:72), Dst: Tp-LinkT_a1:df:10 (74:da:88:a1:df:10)
 > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
 > User Datagram Protocol, Src Port: 1038, Dst Port: 53
 > Domain Name System (query)
 Transaction ID: 0x0001
 > Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 [Response In: 3484]

0000	74	da	88	a1	df	10	3c	f8	62	d6	66	72	08	00	45	00	t-----<- b-fr--E-
0010	00	46	bb	ef	00	00	80	11	fc	fd	c0	a8	00	68	c0	a8	-F-----<-h--
0020	00	01	04	0e	00	35	00	32	ed	11	00	01	01	00	00	01	-----5-2-----
0030	00	00	00	00	00	01	31	01	30	03	31	36	38	03	311...0-168-1
0040	39	32	07	69	6e	2d	61	64	64	72	04	61	72	70	61	00	92-in-ad dr-arpa-
0050	00	0c	00	01													0x1a

IP: 192.168.0.1. Так є.

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

Тип запиту - PTR. 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?

dns						
No.	Time	Source	Destination	Protocol	Length	Info
3482	15.218774	192.168.0.104	192.168.0.1	DNS	84	Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
3484	15.238941	192.168.0.1	192.168.0.104	DNS	84	Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa
3485	15.240562	192.168.0.104	192.168.0.1	DNS	67	Standard query 0x0002 NS mit.edu
3501	15.292576	192.168.0.1	192.168.0.104	DNS	234	Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS eur5.akam.net
3682	16.442192	192.168.0.104	192.168.0.1	DNS	75	Standard query 0x1aca A docs.google.com
3698	16.503421	192.168.0.1	192.168.0.104	DNS	91	Standard query response 0x1aca A docs.google.com A 172.217.16.14

> Frame 3484: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{3CE8ED40-6CFE-47DB-8508-9072AD0B8C48}, id 0
 > Ethernet II, Src: Tp-LinkT_a1:df:10 (74:da:88:a1:df:10), Dst: IntelCor_d6:66:72 (3c:f8:62:d6:66:72)
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
 > User Datagram Protocol, Src Port: 53, Dst Port: 1038
 > Domain Name System (response)
 Transaction ID: 0x0001
 > Flags: 0x8183 Standard query response, No such name
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 > Queries
 > 1.0.168.192.in-addr.arpa: type PTR, class IN
 [Request In: 3482]
 [Time: 0.020167000 seconds]

0 записів із відповіддю. У відповідь було запропоновано сервер: *__*

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: 192.168.0.1. Є адресою локального сервера.

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
1559	11.445721	192.168.0.104	192.168.0.1	DNS	73	Standard query 0xff7d A bitsy.mit.edu
1560	11.480238	192.168.0.1	192.168.0.104	DNS	89	Standard query response 0xff7d A bitsy.mit.edu A 18.0.72.3
1561	11.485736	192.168.0.104	18.0.72.3	DNS	82	Standard query 0x001 PTR 3.72.0.18.in-addr.arpa
1833	13.504469	192.168.0.104	18.0.72.3	DNS	74	Standard query 0x002 A www.aiit.or.kr
2083	15.508794	192.168.0.104	18.0.72.3	DNS	74	Standard query 0x003 AAAA www.aiit.or.kr
2398	17.517658	192.168.0.104	18.0.72.3	DNS	74	Standard query 0x004 A www.aiit.or.kr
2695	19.522635	192.168.0.104	18.0.72.3	DNS	74	Standard query 0x005 AAAA www.aiit.or.kr

15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?/ Тип запиту - А. Вміщує.

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

Була отримана одна відповідь.

```
Transaction ID: 0xff7d
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
> Queries
v Answers
  v 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: 1677 (27 minutes, 57 seconds)
    Data length: 4
    Address: 18.0.72.3
    [Request In: 1559]
    [Time: 0.034517000 seconds]
```

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.