



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

Лабораторна робота № 3
З дисципліни: Комп'ютерні мережі

Протоколи DNS

Виконала:
Студентка III курсу
Групи КА-71
Кравченко А.А.
Перевірив: Кухарев С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи

Стандартний тип запиту. Так вміщує.

Microsoft Windows [Version 10.0.18363.778] (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>

*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

dns

No.	Time	Source	Destination	Protocol	Length	Info
140	0.289194	10.0.2.15	10.0.2.3	DNS	82	Standard query 0x2708 AAAA ieonline.microsoft.com
151	0.318879	10.0.2.3	10.0.2.15	DNS	175	Standard query response 0x2708 AAAA ieonline.microsoft...
607	1.118266	10.0.2.15	10.0.2.3	DNS	74	Standard query 0x2e83 A assets.msn.com
608	1.119339	10.0.2.15	10.0.2.3	DNS	74	Standard query 0xab8b AAAA assets.msn.com
609	1.134640	10.0.2.3	10.0.2.15	DNS	206	Standard query response 0xab8b AAAA assets.msn.com CNAME...
612	1.150078	10.0.2.15	10.0.2.3	DNS	74	Standard query 0x2e83 A assets.msn.com
619	1.163448	10.0.2.3	10.0.2.15	DNS	196	Standard query response 0x2e83 A assets.msn.com CNAME a...
620	1.164356	10.0.2.3	10.0.2.15	DNS	196	Standard query response 0x2e83 A assets.msn.com CNAME a...
635	1.250922	10.0.2.15	10.0.2.3	DNS	72	Standard query 0x15ae A srtb.msn.com
636	1.251704	10.0.2.15	10.0.2.3	DNS	72	Standard query 0xd1af AAAA srtb.msn.com
657	1.280071	10.0.2.3	10.0.2.15	DNS	206	Standard query response 0xd1af AAAA srtb.msn.com CNAME ...
658	1.280401	10.0.2.3	10.0.2.15	DNS	165	Standard query response 0x15ae A srtb.msn.com CNAME www...
1235	1.825111	10.0.2.15	10.0.2.3	DNS	78	Standard query 0xad5 A images.taboola.com

> Frame 140: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{59A8E6A6-5302-4C66-8D5D-71C92005B37A}, id 0

> Ethernet II, Src: RealtekU_be:b2:2e (52:54:00:be:b2:2e), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)

> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3

> User Datagram Protocol, Src Port: 63222, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x2708

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

[Response In: 151]

0000 52 55 0a 00 02 03 52 54 00 be b2 2e 08 00 45 00 RU...RT...E

0010 00 44 ef 63 00 00 40 11 73 34 0a 00 02 0f 0a 00 .D.c...@.s4....

0020 02 03 f6 f6 00 35 00 30 29 45 27 08 01 00 00 015.0)E'....

0030 00 00 00 00 00 00 08 69 65 6f 6e 6c 69 6e 65 09i eonline.

0040 6d 69 63 72 6f 73 6f 66 74 03 63 6f 6d 00 00 1c microsof t.com...

0050 00 01 ..

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

Domain Name System: Protocol | Пакеты: 5132 · Показаны: 59 (1.1%) · Потеряно: 0 (0.0%) | Профиль: Default

*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1261	1.903619	10.0.2.15	151.101.114.2	TLSv1.2	261	Client Hello
1262	1.903914	199.232.18.2	10.0.2.15	TCP	60	443 → 51975 [ACK] Seq=1 Ack=205 Win=8760 Len=0
1263	1.904080	199.232.18.2	10.0.2.15	TCP	60	443 → 51978 [ACK] Seq=1 Ack=205 Win=8760 Len=0
1264	1.904422	151.101.114.2	10.0.2.15	TCP	60	443 → 51977 [ACK] Seq=1 Ack=208 Win=8760 Len=0
1265	1.914877	10.0.2.15	204.79.197.203	TLSv1.2	344	Application Data
1266	1.915355	204.79.197.203	10.0.2.15	TCP	60	443 → 51946 [ACK] Seq=27025 Ack=5185 Win=8760 Len=0
1267	1.925137	10.0.2.15	10.0.2.3	DNS	74	Standard query 0xc567 A login.live.com
1268	1.925823	10.0.2.15	10.0.2.3	DNS	74	Standard query 0x7b69 AAAA login.live.com
1269	1.956683	10.0.2.15	10.0.2.3	DNS	74	Standard query 0xc567 A login.live.com
1270	1.957914	10.0.2.15	10.0.2.3	DNS	74	Standard query 0x7b69 AAAA login.live.com
1271	1.958360	10.0.2.15	199.232.18.2	TCP	74	51979 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=
1272	1.959751	10.0.2.15	204.79.197.203	TLSv1.2	178	Application Data
1273	1.960083	204.79.197.203	10.0.2.15	TCP	60	443 → 51946 [ACK] Seq=27025 Ack=5309 Win=8760 Len=0
1274	1.979070	151.101.114.2	10.0.2.15	TLSv1.2	1494	Server Hello
1275	1.979209	10.0.2.15	151.101.114.2	TCP	54	51977 → 443 [ACK] Seq=208 Ack=1441 Win=65535 Len=0
1276	1.979450	151.101.114.2	10.0.2.15	TCP	1494	443 → 51977 [ACK] Seq=1441 Ack=208 Win=8760 Len=1440 [TCP segment of a re
1277	1.979524	10.0.2.15	151.101.114.2	TCP	54	51977 → 443 [ACK] Seq=208 Ack=2881 Win=65535 Len=0
1278	1.979822	151.101.114.2	10.0.2.15	TCP	70	443 → 51977 [PSH, ACK] Seq=2881 Ack=208 Win=8760 Len=16 [TCP segment of a
1279	1.979884	10.0.2.15	151.101.114.2	TCP	54	51977 → 443 [ACK] Seq=208 Ack=2897 Win=65535 Len=0
1280	1.982211	151.101.114.2	10.0.2.15	TCP	1494	443 → 51977 [ACK] Seq=2897 Ack=208 Win=8760 Len=1440 [TCP segment of a re
1281	1.982356	10.0.2.15	151.101.114.2	TCP	54	51977 → 443 [ACK] Seq=208 Ack=4337 Win=65535 Len=0

> Frame 150: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{59A8E6A6-5302-4C66-8D5D-71C92005B37A}, id 0
 > Ethernet II, Src: RealtekU_be:b2:2e (52:54:00:be:b2:2e), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
 > Internet Protocol Version 4, Src: 10.0.2.15, Dst: 77.120.60.168
 > Transmission Control Protocol, Src Port: 51947, Dst Port: 443, Seq: 322, Ack: 87210, Len: 0

0000 52 55 0a 00 02 02 52 54 00 be b2 2e 08 00 45 00 RU...RT...E.
 0010 00 28 78 9c 40 00 40 06 2c 05 0a 00 02 0f 4d 78 .(x.@.@.,....Mx
 0020 3c a8 ca eb 01 bb fa ac b8 38 0b 27 d8 f0 50 10 <.....8.'...P
 0030 ff c4 b6 3c 00 00<..

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

wireshark_Ethernet_20200425143132_a09888.pcapng Microsoft Edge Пакеты: 5132 · Показаны: 5132 (100.0%) · Потеряно: 0 (0.0%) Профиль: 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?

> Ethernet II, Src: RealtekU_be:b2:2e (52:54:00:be:b2:2e), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
 > Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
 > User Datagram Protocol, Src Port: 63222, Dst Port: 53

Цільовий порт: 53

Вихідний порт: 57547

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

IP: 10.0.2.15 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: 151]

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


```

Transaction ID: 0x2708
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
> Queries
▼ Answers
  > ieonline.microsoft.com: type CNAME, class IN, cname any.edge.bing.com
> Authoritative nameservers
[Request In: 140]
[Time: 0.029685000 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.

No.	Time	Source	Destination	Protocol	Length	Info
47	0.188693	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=105 Ack=28035 Win=64095 Len=0
48	0.189192	77.120.60.168	10.0.2.15	TLSv1.2	886	Application Data, Application Data
49	0.189390	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=105 Ack=28867 Win=65535 Len=0
50	0.245433	10.0.2.15	77.120.60.168	TLSv1.2	157	Application Data
51	0.245733	77.120.60.168	10.0.2.15	TCP	60	443 → 51947 [ACK] Seq=28867 Ack=208 Win=8760 Len=0
52	0.257323	10.0.2.15	77.120.60.160	TCP	74	51963 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256...
53	0.257345	10.0.2.15	77.120.60.160	TCP	74	51964 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256...
54	0.261160	77.120.60.168	10.0.2.15	TLSv1.2	1107	Application Data
55	0.261288	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=208 Ack=29920 Win=64482 Len=0
56	0.266477	77.120.60.168	10.0.2.15	TLSv1.2	1107	Application Data
57	0.266587	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=208 Ack=30973 Win=65535 Len=0
58	0.266926	77.120.60.168	10.0.2.15	TLSv1.2	1494	Application Data
59	0.267082	10.0.2.15	77.120.60.168	TCP	54	51947 → 443 [ACK] Seq=208 Ack=32413 Win=64095 Len=0

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

Так виконує.

```

82 Standard query 0x2708 AAAA ieonline.microsoft.com
175 Standard query response 0x2708 AAAA ieonline.microsoft...
74 Standard query 0x2e83 A assets.msn.com
74 Standard query 0xab8b AAAA assets.msn.com
206 Standard query response 0xab8b AAAA assets.msn.com CNAM...
74 Standard query 0x2e83 A assets.msn.com
196 Standard query response 0x2e83 A assets.msn.com CNAME a...
196 Standard query response 0x2e83 A assets.msn.com CNAME a...
72 Standard query 0x15ae A srtb.msn.com
72 Standard query 0xd1af AAAA srtb.msn.com
206 Standard query response 0xd1af AAAA srtb.msn.com CNAME ...
165 Standard query response 0x15ae A srtb.msn.com CNAME www...
78 Standard query 0x6ad5 A images.taboola.com

```

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

Цільовий: 10.0.2.3

Вихідний: 10.0.2.15

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

10.0.2.15 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.

```
Transaction ID: 0x0003
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
[Response In: 5]
```

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

Packet 5 details:

```
User Datagram Protocol, Src Port: 53, Dst Port: 50613
Domain Name System (response)
Transaction ID: 0x0003
> Flags: 0x0100 Standard query response, No error
Questions: 1
Answer RRs: 4
Authority RRs: 0
Additional RRs: 0
> Queries
> Answers
  > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:2d8:3:9a2::255e
  > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:2d8:3:996::255e
[Request In: 4]
[Time: 0.245137000 seconds]
```

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

IP: 10.0.2.15 Так є.

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

```

▼ Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    [Response In: 3]

```

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?

```

> Frame 3: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) on interface \Device\NPF_{59A8E6A6-5302-4C66-8D5D-71C92005B37A}, id 0
> Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: RealtekU_be:b2:2e (52:54:00:be:b2:2e)
> Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
> User Datagram Protocol, Src Port: 53, Dst Port: 54013
▼ Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8100 Standard query response, No error
  Questions: 1
  Answer RRs: 8
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > Answers
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
  [Request In: 2]
  [Time: 0.046931000 seconds]

```

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: 10.0.2.15 є адресою локального сервера.

```

> Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{59A8E6A6-5302-4C66-8D5D-71C92005B37A}, id 0
> Ethernet II, Src: RealtekU_be:b2:2e (52:54:00:be:b2:2e), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
> User Datagram Protocol, Src Port: 50611, 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

```

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

Стандартний тип запиту. вміщує.

```
Transaction ID: 0x9043
► Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
► Queries
\[Response In: 4\]
```

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

```
Transaction ID: 0x9043
► Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
► Queries
▼ Answers
► bitsy.mit.edu: type A, class IN, addr 18.0.72.3
\[Request In: 3\]
[Time: 0.047087000 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.

