



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

Лабораторна робота № 3
З дисципліни: Комп'ютерні мережі

Протокол DNS

Виконав:
Студент III курсу
Групи КА-72
Жакулін Н. В.
Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід виконання роботи

Перша частина

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture, and analysis. The main display area is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is a DNS Standard query response (No. 149, Time 12.4.568603, Source 8.8.8.8, Destination 192.168.0.103, Protocol DNS, Length 149 bytes).
- Packet Details:** Shows the hierarchical structure of the selected packet. It includes Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The query is for the domain www.ietf.org.
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates that the Domain Name System: Protocol is selected, and the display filter is set to 'Packets: 1562 · Displayed: 6 (0.4%)'. The system clock shows 18:38 on 24.03.2020.

Request:

```

No.      Time      Source      Destination      Protocol Length Info
   9 4.530186    192.168.0.103    8.8.8.8          DNS      72      Standard query 0xaa70 A www.ietf.org
Frame 9: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{8A2CE6CD-F596-41A8-9F9F-6404B65AB4DF},
id 0
Ethernet II, Src: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac), Dst: Tp-LinkT_72:eb:50 (18:d6:c7:72:eb:50)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 41838, Dst Port: 53
    Source Port: 41838
    Destination Port: 53
    Length: 38
    Checksum: 0xbe29 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
    [Timestamps]
Domain Name System (query)
    Transaction ID: 0xaa70
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 12]

```

Response:

No.	Time	Source	Destination	Protocol	Length	Info
12	4.568603	8.8.8.8	192.168.0.103	DNS	149	Standard query response 0xaa70 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85

Frame 12: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{8A2CE6CD-F596-41A8-9F9F-6404B65AB4DF}, id 0

Ethernet II, Src: Tp-LinkT_72:eb:50 (18:d6:c7:72:eb:50), Dst: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac)

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.103

User Datagram Protocol, Src Port: 53, Dst Port: 41838

Source Port: 53

Destination Port: 41838

Length: 115

Checksum: 0xf6d2 [unverified]

[Checksum Status: Unverified]

[Stream index: 2]

[Timestamps]

Domain Name System (response)

Transaction ID: 0xaa70

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

Queries

Answers

[Request In: 9]

[Time: 0.038417000 seconds]

Друга частина

```
Командная строка
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Nikita>nslookup www.mit.edu
Server: dns.google
Address: 8.8.8.8

Не заслуживающий доверия ответ:
Server: e9566.dscb.akamaiedge.net
Addresses: 2a02:26f0:d8:490::255e
           2a02:26f0:d8:4a5::255e
           23.77.209.53
Aliases: www.mit.edu
         www.mit.edu.edgekey.net
```

2pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
5	2.339408	192.168.0.103	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
6	2.362009	8.8.8.8	192.168.0.103	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
7	2.364243	192.168.0.103	8.8.8.8	DNS	71	Standard query 0x0002 A www.mit.edu
8	2.411188	8.8.8.8	192.168.0.103	DNS	160	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.7...
9	2.412426	192.168.0.103	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.mit.edu
10	2.458996	8.8.8.8	192.168.0.103	DNS	200	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAA...

Domain Name System: Protocol

Packets: 13 · Displayed: 6 (46.2%)

Profile: Default

20:17 30.03.2020

Request:

```
No.      Time      Source      Destination      Protocol Length Info
  9 2.412426    192.168.0.103 8.8.8.8          DNS           71      Standard query 0x0003 AAAA www.mit.edu
Frame 9: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{8A2CE6CD-F596-41A8-9F9F-6404B65AB4DF}, id 0
Ethernet II, Src: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac), Dst: Tp-LinkT_72:eb:50 (18:d6:c7:72:eb:50)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 43321, Dst Port: 53
    Source Port: 43321
    Destination Port: 53
    Length: 37
    Checksum: 0x1768 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Timestamps]
Domain Name System (query)
    Transaction ID: 0x0003
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 10]
```

Response:

```
No.      Time      Source      Destination      Protocol Length Info
 10 2.458996     8.8.8.8      192.168.0.103    DNS           200     Standard query response 0x0003 AAAA www.mit.edu
CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net AAAA 2a02:26f0:d8:4a5::255e AAAA 2a02:26f0:d8:490::255e
Frame 10: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{8A2CE6CD-F596-41A8-9F9F-6404B65AB4DF}, id 0
Ethernet II, Src: Tp-LinkT_72:eb:50 (18:d6:c7:72:eb:50), Dst: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.0.103
User Datagram Protocol, Src Port: 53, Dst Port: 43321
    Source Port: 53
    Destination Port: 43321
    Length: 166
    Checksum: 0xa21c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Timestamps]
Domain Name System (response)
    Transaction ID: 0x0003
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
    [Request In: 9]
    [Time: 0.046570000 seconds]
```

Третья часть

```
C:\Users\Nikita>nslookup -type=NS mit.edu  
DNS request timed out.  
    timeout was 2 seconds.  
***  
Address: 23.79.89.21  
  
DNS request timed out.  
    timeout was 2 seconds.  
DNS request timed out.  
    timeout was 2 seconds.  
*** Превышено время ожидания запроса UnKnown
```

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, navigation, and analysis. The main display area is divided into three panes. The top pane, titled 'dns', shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the packet details for the selected packet (No. 32), and the bottom-most pane shows the packet bytes. The status bar at the bottom indicates 'Domain Name System: Protocol', 'Packets: 41 · Displayed: 5 (12.2%)', and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
14	3.017114	192.168.0.103	8.8.8.8	DNS	67	Standard query 0x304a A mit.edu
15	3.055363	8.8.8.8	192.168.0.103	DNS	83	Standard query response 0x304a A mit.edu A 104.74.143.40
16	3.058398	192.168.0.103	104.74.143.40	DNS	86	Standard query 0x0001 PTR 40.143.74.104.in-addr.arpa
17	5.060846	192.168.0.103	104.74.143.40	DNS	68	Standard query 0x0002 A *type=NS
32	7.061578	192.168.0.103	104.74.143.40	DNS	68	Standard query 0x0003 AAAA *type=NS

Четверта частина

```
C:\Users\Nikita>nslookup www.aiit.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.
*** Превышено время ожидания запроса UnKnown
```

The screenshot displays the Wireshark network protocol analyzer interface. The title bar indicates the capture file is "Беспроводное сетевое соединение". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis.

The packet list pane shows a series of DNS packets. Packet 17 is a Standard query from 192.168.0.103 to 8.8.8.8. The packet details pane for packet 17 shows the query structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
17	2.944016	192.168.0.103	8.8.8.8	DNS	73	Standard query 0x95a3 A bitsy.mit.edu
18	2.982697	8.8.8.8	192.168.0.103	DNS	89	Standard query response 0x95a3 A bitsy.mit.edu A 18.0.72.3
19	2.985144	192.168.0.103	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
22	4.988168	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
28	6.989100	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
31	8.990364	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
35	10.991606	192.168.0.103	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

Frame 17: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{8A2CE6CD-F596-41A8-9F9F-6404B65AB4DF}, id 0
 Ethernet II, Src: LiteonTe_e9:5f:ac (70:f1:a1:e9:5f:ac), Dst: Tp-LinkT_72:eb:50 (18:d6:c7:72:eb:50)
 Internet Protocol Version 4, Src: 192.168.0.103, Dst: 8.8.8.8
 User Datagram Protocol, Src Port: 28295, Dst Port: 53
 Domain Name System (query)

0000 18 d6 c7 72 eb 50 70 f1 a1 e9 5f ac 08 00 45 00 ...Pp.....E-
 0010 00 3b 7f 48 00 00 00 11 ea 4a c0 a8 00 67 08 08 ;H.....J...g..
 0020 08 08 6e 87 00 35 00 27 70 14 95 a3 01 00 00 01 ..n-5..p.....
 0030 00 00 00 00 00 00 05 62 69 74 73 79 03 6d 69 74b itsy.mit
 0040 03 65 64 75 00 00 01 00 01edu.....

Wireshark, Беспроводное сетевое соединение_20200324185749_a04568.pcapng | Packets: 45 · Displayed: 7 (15.6%) · Dropped: 0 (0.0%) · Ignored: 2 (4.4%) | Profile: Default

Відповіді на контрольні запитання:

1. Вони використовують протокол UDP. Порт 53.
2. 8.8.8.8, Google Public DNS, вказаний в параметрах адаптера.
3. Тип A.
4. Три відповіді. Містять name, type, class, ttl, data length, answer (cname або addr).
5. Так.

12	4.568603	8.8.8.8	192.168.0.103	DNS	149 Standard query response 0xa
13	4.569547	192.168.0.103	104.20.0.85	TCP	74 1996 → 80 [SYN] Seq=0 Win=8
▶ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85					

6. Так.
7. Порт 53.
8. 8.8.8.8. Так.
9. PTR, A, AAAA.
10. Чотири відповіді. Містять name, type, class, ttl, data length, answer (cname або addr).
11. 104.74.143.40. Ні.
12. PTR, A, AAAA.
13. Відповіді не було.
14. 18.0.72.3. Не є. bitsy.mit.edu.
15. PTR, A, AAAA.
16. Відповіді не було.

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення та аналізу пакетів. Було розглянуто інформацію, що містить в собі протокол DNS.