

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Компьютерные сети

Лабораторная работа № 4

«Работа с сетевым анализатором»

Выполнил студент

Стеберг Артём Алексеевич

Группа № Р33232

Преподаватель: Болдырева Елена Александровна

г. Санкт-Петербург

2024

Оглавление	
Программа работы:	2
Отчет:	2
Теперь - nslookup.	7
Теперь <i>nslookup - type = ns itmo.ru</i>	9
<i>nslookup address_what_you_want your_DNS</i>	10
Вывод:	11

Программа работы:

1. Используйте nslookup для анализа сообщений DNS.
2. Используйте ipconfig для анализа сообщений DNS.
3. Используйте Wireshark для анализа сообщений DNS.

Отчет:

Используйте nslookup для анализа сообщений DNS

Запустите nslookup, чтобы получить IP-адрес веб-сервера университета (любого) в России.
Какой IP-адрес у этого сервера?

Найдем веб-адрес Курганского Государственного университета:

```
PS C:\Users\Artem_Step> nslookup www.kgsu.ru
ТхЀтхЀ: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
Ѐ : www.kgsu.ru
Address: 85.143.32.32
```

Запустите nslookup, чтобы определить авторитетные DNS-серверы для университета в Европе.

Найдем авторитетный DNS сервер для университета Аалто:

```
PS C:\Users\Artem_Step> nslookup -type=ns aalto.fi
ТхЀтхЀ: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
aalto.fi      nameserver = ns02.aalto.fi
aalto.fi      nameserver = ns03.aalto.fi
aalto.fi      nameserver = ns01.aalto.fi
aalto.fi      nameserver = ns-secondary.funet.fi
```

Запустите nslookup, чтобы один из DNS-серверов, полученных в вопросе 2, запросил почтовые серверы для почты Яндекса. Какой у него IP-адрес?

```
PS C:\Users\Artem_Step> nslookup -type=mx yandex.ru ns-secondary.funet.fi
ТхЕтхЕ: ns-secondary.funet.fi
Address: 128.214.248.132

*** ns-secondary.funet.fi не удалось найти yandex.ru: Query refused
```

Используйте ipconfig для анализа сообщений DNS
Введите следующую команду: *ipconfig / displaydns*

```
PS C:\Users\Artem_Step> ipconfig /displaydns

Настройка протокола IP для Windows

www.tu-ilmenau.de
-----
Имя записи. . . . . : www.tu-ilmenau.de
Тип записи. . . . . : 5
Срок жизни. . . . . : 12122
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : wcms-proxy2.rz.tu-ilmenau.de

Имя записи. . . . . : wcms-proxy2.rz.tu-ilmenau.de
Тип записи. . . . . : 1
Срок жизни. . . . . : 12122
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 141.24.186.181

www.gstatic.com
-----
Имя записи. . . . . : www.gstatic.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 173
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 108.177.14.94
```

ipconfig / flushdns

```
PS C:\Users\Artem_Step> ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.
```

Используйте Wireshark для анализа сообщений DNS

Найдите сообщения DNS-запроса и ответа. Они отправляются по UDP или TCP?

The image displays two Wireshark packet capture windows. The top window shows a packet list with several entries, including a DNS query (packet 3837) and a DNS response (packet 3841). The packet details pane for packet 3837 shows a User Datagram Protocol (UDP) header with Source Port: 49318 and Destination Port: 53. The Domain Name System (query) section shows Transaction ID: 0x69de, Flags: 0x0100 Standard query, Questions: 1, Answer RRs: 0, and Authority RRs: 0. The packet bytes pane shows the raw data of the UDP packet.

The bottom window shows a similar packet capture, with a DNS query (packet 3836) and a DNS response (packet 3841). The packet details pane for packet 3836 shows a User Datagram Protocol (UDP) header with Source Port: 49318 and Destination Port: 53. The Domain Name System (query) section shows Transaction ID: 0x16d5, Flags: 0x0100 Standard query, Questions: 1, Answer RRs: 0, and Authority RRs: 0. The packet bytes pane shows the raw data of the UDP packet.

Они отправляются по UDP

Каков порт назначения для сообщения DNS-запроса? Каков порт источника ответа DNS?

3837	7.054031	192.168.0.101	192.168.0.1	DNS	74 Standard query 0x69de HTTPS clck.yandex.ru
3838	7.054140	192.168.0.101	87.250.247.184	TLSv1.3	162 Application Data
3839	7.055055	192.168.0.101	87.250.250.119	TLSv1.3	978 Application Data
3840	7.057898	192.168.0.1	192.168.0.101	DNS	170 Standard query response 0x16d5 A clck.yandex.ru A 87.250.251.14 A 213.184.201.119
3841	7.058358	192.168.0.1	192.168.0.101	DNS	135 Standard query response 0x69de HTTPS clck.yandex.ru SOA ns1.yandex.ru
3842	7.058794	192.168.0.101	87.250.251.14	TCP	66 62009 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3843	7.063019	192.168.0.101	64.233.165.155	TCP	662 [TCP Retransmission] 62008 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=0
3844	7.068672	87.250.247.184	192.168.0.101	TCP	1274 443 → 61982 [ACK] Seq=1997033 Ack=4266 Win=45056 Len=1220 [TCP segment of a stream already in the table]
User Datagram Protocol, Src Port: 49318, Dst Port: 53					0000 cc 32 e5 71 a3 7e 14 18 c3 68 84 a4 08 00 45 00 -- 2-q
Source Port: 49318					0010 00 3c 1a e1 00 00 80 11 00 00 c0 a8 00 65 c0 a8 -- <--
Destination Port: 53					0020 00 01 c0 a6 00 35 00 28 81 f0 69 de 01 00 00 01 -- --
Length: 40					0030 00 00 00 00 00 04 63 6c 63 6b 06 79 61 6e 64 -- --
Checksum: 0x81f0 [unverified]					0040 65 78 02 72 75 00 00 41 00 01 -- --
[Checksum Status: Unverified]					
[Stream index: 72]					
> [Timestamps]					
UDP payload (32 bytes)					
Domain Name System (query)					
Transaction ID: 0x69de					
> Flags: 0x0100 Standard query					
Questions: 1					
Answer RRs: 0					
Authority RRs: 0					
3837	7.054031	192.168.0.101	192.168.0.1	DNS	74 Standard query 0x69de HTTPS clck.yandex.ru
3838	7.054140	192.168.0.101	87.250.247.184	TLSv1.3	162 Application Data
3839	7.055055	192.168.0.101	87.250.250.119	TLSv1.3	978 Application Data
3840	7.057898	192.168.0.1	192.168.0.101	DNS	170 Standard query response 0x16d5 A clck.yandex.ru A 87.250.251.14 A 213.184.201.119
3841	7.058358	192.168.0.1	192.168.0.101	DNS	135 Standard query response 0x69de HTTPS clck.yandex.ru SOA ns1.yandex.ru
3842	7.058794	192.168.0.101	87.250.251.14	TCP	66 62009 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3843	7.063019	192.168.0.101	64.233.165.155	TCP	662 [TCP Retransmission] 62008 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=0
3844	7.068672	87.250.247.184	192.168.0.101	TCP	1274 443 → 61982 [ACK] Seq=1997033 Ack=4266 Win=45056 Len=1220 [TCP segment of a stream already in the table]
User Datagram Protocol, Src Port: 53, Dst Port: 49318					0000 14 18 c3 68 84 a4 cc 32 e5 71 a3 7e 08 00 45 00 -- --
Source Port: 53					0010 00 79 17 c2 00 00 3c 11 e4 fb c0 a8 00 01 c0 a8 -- y
Destination Port: 49318					0020 00 65 00 35 c0 a6 00 65 fe 67 69 de 81 80 00 01 -- e
Length: 101					0030 00 00 00 01 00 00 04 63 6c 63 6b 06 79 61 6e 64 -- --
Checksum: 0xfe67 [unverified]					0040 65 78 02 72 75 00 00 41 00 01 c0 11 00 06 00 01 -- ex
[Checksum Status: Unverified]					0050 00 00 00 64 00 31 03 6e 73 31 c0 11 08 73 79 73 -- --
[Stream index: 72]					0060 61 64 6d 69 6e 0b 79 61 6e 64 65 78 2d 74 65 61 -- adi
> [Timestamps]					0070 6d c0 18 78 95 09 51 00 00 02 58 00 00 01 2c 00 -- m-
UDP payload (93 bytes)					0080 27 8d 00 00 00 03 84 -- --
Domain Name System (response)					
Transaction ID: 0x69de					
> Flags: 0x8180 Standard query response, No error					
Questions: 1					
Answer RRs: 0					
Authority RRs: 1					

На какой IP-адрес отправляется сообщение с запросом DNS? Используйте `ipconfig`, чтобы определить IP-адрес вашего локального DNS-сервера. Эти два IP-адреса одинаковы?

```
DNS-суффикс подключения . . . . . :  
Описание. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz  
Физический адрес. . . . . : 14-18-C3-68-84-A4  
DHCP включен. . . . . : Да  
Автонастройка включена. . . . . : Да  
Локальный IPv6-адрес канала . . . : fe80::2d44:7685:19ff:202e%7(Основной)  
IPv4-адрес. . . . . : 192.168.0.101(Основной)  
Маска подсети . . . . . : 255.255.255.0  
Аренда получена. . . . . : 2 апреля 2024 г. 15:32:28  
Срок аренды истекает. . . . . : 3 апреля 2024 г. 20:33:28  
Основной шлюз. . . . . : 192.168.0.1  
DHCP-сервер. . . . . : 192.168.0.1  
IAID DHCPv6 . . . . . : 85203139  
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2D-64-CB-62-14-18-C3-68-84-A4  
DNS-серверы. . . . . : 192.168.0.1  
                        0.0.0.0  
NetBios через TCP/IP. . . . . : Включен  
  
адаптер Ethernet Сетевое подключение Bluetooth:  
  
Состояние среды. . . . . : Среда передачи недоступна.  
DNS-суффикс подключения . . . . . :  
Описание. . . . . : Bluetooth Device (Personal Area Network)  
Физический адрес. . . . . : 14-18-C3-68-84-A8  
DHCP включен. . . . . : Да  
Автонастройка включена. . . . . : Да
```

```
... .. = 192.168.0.101(Основной) (адаптер Ethernet Сетевое подключение Bluetooth)  
Type: IPv4 (0x0800)  
▼ Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1  
    0100 .... = Version: 4
```

Это два одинаковых IP адреса.

Изучите сообщение DNS-запроса. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»?

3836	7.053775	192.168.0.101	192.168.0.1	DNS	74 Standard query 0x16d5 A click.yandex.ru
3837	7.054031	192.168.0.101	192.168.0.1	DNS	74 Standard query 0x69de HTTPS click.yandex.ru

Два типа: А и HTTPS

Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов?

- ▼ Answers
 - > clck.yandex.ru: type A, class IN, addr 87.250.251.14
 - > clck.yandex.ru: type A, class IN, addr 213.180.193.14
 - > clck.yandex.ru: type A, class IN, addr 87.250.250.14
 - > clck.yandex.ru: type A, class IN, addr 213.180.204.14
 - > clck.yandex.ru: type A, class IN, addr 77.88.21.14
 - > clck.yandex.ru: type A, class IN, addr 93.158.134.14
- [\[Request In: 3836\]](#)
- ▼ Authoritative nameservers
 - ▼ yandex.ru: type SOA, class IN, mname ns1.yandex.ru
 - Name: yandex.ru
 - Type: SOA (6) (Start Of a zone of Authority)
 - Class: IN (0x0001)
 - Time to live: 100 (1 minute, 40 seconds)
 - Data length: 49
 - Primary name server: ns1.yandex.ru
 - Responsible authority's mailbox: sysadmin.yandex-team.ru
 - Serial Number: 2023033169
 - Refresh Interval: 600 (10 minutes)
 - Retry Interval: 300 (5 minutes)
 - Expire limit: 2592000 (30 days)

Есть ли на этой веб-странице изображения? Перед получением каждого изображения ваш хост выдает новые DNS-запросы?

Всего два запроса.

Теперь - nslookup.

nslookup www.hdu.edu.cn

Какой порт назначения для сообщения DNS-запроса? Каков порт источника ответного сообщения DNS?

| > User Datagram Protocol, Src Port: 63328, Dst Port: 53

На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию?

> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1

Да, это адрес моего DNS сервера.

Изучите сообщение DNS-запроса. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»?

```
84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
143 Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA localhost
74 Standard query 0x0002 A www.hdu.edu.cn
114 Standard query response 0x0002 A www.hdu.edu.cn CNAME www.split.hdu.edu.cn A 218.75.123.179
74 Standard query 0x0003 AAAA www.hdu.edu.cn
55 61997 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
66 443 → 61997 [ACK] Seq=1 Ack=2 Win=166 Len=0 SLE=1 SRE=2
126 Standard query response 0x0003 AAAA www.hdu.edu.cn CNAME www.split.hdu.edu.cn AAAA 2001:250:6402:1...
55 61532 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
66 5228 → 61532 [ACK] Seq=1 Ack=2 Win=254 Len=0 SLE=1 SRE=2
```

Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов?

▼ Answers

- ▼ www.hdu.edu.cn: type CNAME, class IN, cname www.split.hdu.edu.cn
 - Name: www.hdu.edu.cn
 - Type: CNAME (5) (Canonical NAME for an alias)
 - Class: IN (0x0001)
 - Time to live: 1797 (29 minutes, 57 seconds)
 - Data length: 12
 - CNAME: www.split.hdu.edu.cn
- ▼ www.split.hdu.edu.cn: type AAAA, class IN, addr 2001:250:6402:106::102:34
 - Name: www.split.hdu.edu.cn
 - Type: AAAA (28) (IP6 Address)
 - Class: IN (0x0001)
 - Time to live: 600 (10 minutes)
 - Data length: 16
 - AAAA Address: 2001:250:6402:106::102:34

▼ Answers

- ▼ www.hdu.edu.cn: type CNAME, class IN, cname www.split.hdu.edu.cn
 - Name: www.hdu.edu.cn
 - Type: CNAME (5) (Canonical NAME for an alias)
 - Class: IN (0x0001)
 - Time to live: 1800 (30 minutes)
 - Data length: 12
 - CNAME: www.split.hdu.edu.cn
- ▼ www.split.hdu.edu.cn: type A, class IN, addr 218.75.123.179
 - Name: www.split.hdu.edu.cn
 - Type: A (1) (Host Address)
 - Class: IN (0x0001)
 - Time to live: 600 (10 minutes)
 - Data length: 4
 - Address: 218.75.123.179


```
▼ Authoritative nameservers
  ▼ 168.192.in-addr.arpa: type SOA, class IN, mname localhost
    Name: 168.192.in-addr.arpa
    Type: SOA (6) (Start Of a zone of Authority)
    Class: IN (0x0001)
    Time to live: 10800 (3 hours)
    Data length: 47
    Primary name server: localhost
    Responsible authority's mailbox: nobody.invalid
    Serial Number: 1
    Refresh Interval: 3600 (1 hour)
    Retry Interval: 1200 (20 minutes)
    Expire limit: 604800 (7 days)
    Minimum TTL: 10800 (3 hours)
```

Теперь *nslookup* - *type* = ns itmo.ru

На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию?

```
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
```

Изучите сообщение с запросом DNS. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»?

```
84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
143 Standard query response 0x0001 No such name PTR 1.0.168.192.in-addr.arpa SOA localhost
67 Standard query 0x0002 NS itmo.ru
138 Standard query response 0x0002 NS itmo.ru NS ns3.itmo.ru NS ns2.itmo.ru NS ns5.itmo.ru NS n...
```

Изучите ответное сообщение DNS. Какие серверы имен предоставляет ответное сообщение?

```
Answers:  
> itmo.ru: type NS, class IN, ns ns3.itmo.ru  
> itmo.ru: type NS, class IN, ns ns2.itmo.ru  
> itmo.ru: type NS, class IN, ns ns5.itmo.ru  
> itmo.ru: type NS, class IN, ns ns.itmo.ru
```

nslookup address_what_you_want your_DNS

На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию? Если нет, то чему соответствует IP-адрес?

```
| > Internet Protocol Version 4, Src: 192.168.0.101, Dst: 77.234.194.2
```

Не соответствует так как, мы отправляем на определённые DNS сервер.

Изучите сообщение с запросом DNS. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»?

```
67 Standard query 0x0002 A itmo.ru  
218 Standard query response 0x0002 A itmo.ru A 51.250.120.146 NS ns3.itmo.ru NS ns2.itmo.ru NS ..  
67 Standard query 0x0003 AAAA itmo.ru  
117 Standard query response 0x0003 AAAA itmo.ru SOA ns.itmo.ru
```

Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов?

```
▼ Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8500 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 4
  Additional RRs: 4
  ▼ Queries
    > itmo.ru: type A, class IN
  ▼ Answers
    > itmo.ru: type A, class IN, addr 51.250.120.146
    > Authoritative nameservers
    > Additional records
    [Request In: 30]
    [Time: 0.042371000 seconds]
    [Label Count: 2]
    Type: AAAA (28) (IP6 Address)
    Class: IN (0x0001)
  ▼ Authoritative nameservers
    ▼ itmo.ru: type SOA, class IN, mname ns.itmo.ru
      Name: itmo.ru
      Type: SOA (6) (Start Of a zone of Authority)
      Class: IN (0x0001)
      Time to live: 3600 (1 hour)
      Data length: 38
      Primary name server: ns.itmo.ru
      Responsible authority's mailbox: hostmaster.itmo.ru
      Serial Number: 2024012259
      Refresh Interval: 3600 (1 hour)
      Retry Interval: 1800 (30 minutes)
```

Вывод:

Сетевые анализаторы – это комплексная программа, основанная на взаимодействии основных сетевых механизмов. Подобно наблюдателю, мы можем отслеживать хронологию формирования запросов и ответов порожденные собственной активностью. Такой функционал позволяет четко рассмотреть работу DNS служб, формирование датафреймов любого протокола и взаимодействие локальных и глобальных сетей.