

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Компьютерные сети

Лабораторная работа № 4

«Работа с сетевым анализатором»

Выполнил студент

Неизвестная Екатерина Павловна

Группа № Р33701

Преподаватель: Болдырева Елена Александровна

г. Санкт-Петербург

2022

**Цель работы:** изучить принципы организации взаимодействия прикладных программ с помощью протоколов электронной почты SMTP и POP3 в режиме симуляции Cisco Packet Tracer.

Задача:

1. Установите Wireshark (лабораторная работа 1, часть 1) - у вас уже есть вся информация.
2. Используйте nslookup для анализа сообщений DNS.
3. Используйте ipconfig для анализа сообщений DNS.
4. Используйте Wireshark для анализа сообщений DNS.

**Вариант: 11**

ИСУ – 285625

$25 / 14 = 1$  (11 – остаток)

Отчет:

Введем команду: nslookup www.itmo.ru

```
PS C:\> nslookup www.itmo.ru
Server: ns.itmo.ru
Address: 77.234.194.2

www.itmo.ru
Address: 77.234.204.10

PS C:\> |
```

Введем команду: nslookup -type=NS www.itmo.ru

```
# поиск узла "host" с использованием сервера "ser
PS C:\> nslookup -type=NS www.itmo.ru
Server: ns.itmo.ru
Address: 77.234.194.2

itmo.ru
    primary name server = ns.itmo.ru
    responsible mail addr = hostmaster.itmo.ru
    serial = 2021011388
    refresh = 3600 (1 hour)
    retry = 1800 (30 mins)
    expire = 86400 (1 day)
    default TTL = 3600 (1 hour)
PS C:\> |
```

Введем команду: nslookup -type=NS itmo.ru

```
default TTL = 3600 (1 hour)
PS C:\> nslookup -type=NS itmo.ru
Получен ответ от ns.itmo.ru:
Address: 77.234.194.2

itmo.ru nameserver = ns2.itmo.ru
itmo.ru nameserver = ns3.itmo.ru
itmo.ru nameserver = ns.itmo.ru
ns.itmo.ru internet address = 77.234.194.2
ns2.itmo.ru internet address = 77.234.221.75
ns3.itmo.ru internet address = 77.234.216.2
PS C:\>
```

Введем команду: nslookup www.hdu.edu.cn router.asus.com

```
PS C:\> nslookup www.hdu.edu.cn router.asus.com
*** Не найден адрес сервера для "router.asus.com":
Получен ответ от ns.itmo.ru:
Address: 77.234.194.2

Не заслуживающий доверия ответ:
Ль : www.split.hdu.edu.cn
Addresses: 2001:250:6402:106::102:34
          218.75.123.181
Aliases: www.hdu.edu.cn
```

1. Запустите nslookup, чтобы получить IP-адрес веб-сервера в России. Какой IP-адрес у этого сервера?

**Томский Государственный Университет: 92.63.64.162**

```
PS C:\> nslookup www.tsu.ru
Получен ответ от ns.itmo.ru:
Address: 77.234.194.2

Не заслуживающий доверия ответ:
Ль : www.tsu.ru
Address: 92.63.64.162
```

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

**Таллинский университет: 193.40.239.40**

```
PS C:\> nslookup www.tlu.ee
Server: ns.itmo.ru
Address: 77.234.194.2

Не заслуживающий доверия ответ:
Ль : www7.tlu.ee
Address: 193.40.239.40
Aliases: www.tlu.ee
```

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

Сделала запрос через адрес таллинского университета на адрес gmail, получили в ответ IP-адрес: **64.233.164.18**.

```
PS C:\> nslookup www.tlu.ee mail.google.com
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: 64.233.164.18

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
PS C:\> |
```

## Ipconfig

1. Результат команды ipconfig

```

PS C:\> ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet 2:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 3:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::98fe:ac2f:4514:9044%6
    IPv4-адрес. . . . . : 172.28.22.67
    Маска подсети . . . . . : 255.255.240.0
    Основной шлюз. . . . . : 172.28.16.1
PS C:\>

```

## 2. Результат команды ipconfig /displaydns

```

PS C:\> ipconfig /displaydns

Настройка протокола IP для Windows

cloud-fes-ru2.acronis.com
-----
Нет записей типа AAAA

cloud-fes-ru2.acronis.com
-----
Имя записи. . . . . : cloud-fes-ru2.acronis.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 370174
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 0.0.0.0

ssau.ru
-----
Имя записи. . . . . : ssau.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 70610
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 91.222.128.63

Имя записи. . . . . : mb.SSAU.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 70610
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 91.222.128.18

```

```

Имя записи. . . . . : mb.SSAU.ru
Тип записи. . . . . : 28
Срок жизни. . . . . : 70610
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:678:ec:1::18

```

```

Имя записи. . . . . : stream.SSAU.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 70610
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 91.222.128.56

```

```

Имя записи. . . . . : stream.SSAU.ru
Тип записи. . . . . : 28
Срок жизни. . . . . : 70610
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:678:ec:1::56

```

```

drive-thirdparty.googleusercontent.com
-----
Имя записи. . . . . : drive-thirdparty.googleusercontent.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 59
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : googlehosted.l.googleusercontent.com

```

```
Имя записи. . . . . : googlehosted.l.googleusercontent.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 59
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 173.194.73.132
```

```
Имя записи. . . . . : ns1.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 59
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 216.239.32.10
```

```
Имя записи. . . . . : ns1.google.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 59
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:4860:4802:32::a
```

```
Имя записи. . . . . : ns2.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 59
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 216.239.34.10
```

```
Имя записи. . . . . : stream.SSAU.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 70609
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 91.222.128.56
```

```
Имя записи. . . . . : stream.SSAU.ru
Тип записи. . . . . : 28
Срок жизни. . . . . : 70609
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:678:ec:1::56
```

ocsp.digicert.com

```
-----
Имя записи. . . . . : ocsp.digicert.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 1624
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : cs9.wac.phicdn.net
```

```
Имя записи. . . . . : cs9.wac.phicdn.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 1624
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 93.184.220.29
```

```
Имя записи. . . . . : ns2.google.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 59
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:4860:4802:34::a
```

```
Имя записи. . . . . : ns3.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 59
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 216.239.36.10
```

```
Имя записи. . . . . : ns3.google.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 59
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:4860:4802:36::a
```

```
Имя записи. . . . . : ns4.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 59
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 216.239.38.10
```

```
Имя записи. . . . . : ns1.phicdn.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 1624
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 72.21.80.5
```

```
Имя записи. . . . . : ns1.phicdn.net
Тип записи. . . . . : 28
Срок жизни. . . . . : 1624
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2606:2800:1::5
```

```
Имя записи. . . . . : ns2.phicdn.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 1624
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 72.21.80.6
```

```
Имя записи. . . . . : ns2.phicdn.net
Тип записи. . . . . : 28
Срок жизни. . . . . : 1624
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2606:2800:1::6
```

```
Имя записи. . . . . : ns4.google.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 59
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:4860:4802:38::a
```

www.ssau.ru

```
-----
Имя записи. . . . . : www.ssau.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 70609
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 91.222.128.63
```

```
Имя записи. . . . . : mb.SSAU.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 70609
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 91.222.128.18
```

```
Имя записи. . . . . : mb.SSAU.ru
Тип записи. . . . . : 28
Срок жизни. . . . . : 70609
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:678:ec:1::18
```

```
Имя записи. . . . . : ns3.phicdn.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 1624
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 192.229.254.5
```

```
Имя записи. . . . . : ns3.phicdn.net
Тип записи. . . . . : 28
Срок жизни. . . . . : 1624
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2606:2800:e::5
```

```
Имя записи. . . . . : ns4.phicdn.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 1624
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 192.229.254.6
```

```
Имя записи. . . . . : ns4.phicdn.net
Тип записи. . . . . : 28
Срок жизни. . . . . : 1624
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2606:2800:e::6
```

```

signaler-pa.clients6.google.com
-----
Имя записи. . . . . : signaler-pa.clients6.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 78
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 74.125.131.95

Имя записи. . . . . : ns1.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 78
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 216.239.32.10

Имя записи. . . . . : ns1.google.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 78
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:4860:4802:32::a

Имя записи. . . . . : ns2.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 78
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 216.239.34.10

```

```

Имя записи. . . . . : ns2.google.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 78
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:4860:4802:34::a

Имя записи. . . . . : ns3.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 78
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 216.239.36.10

Имя записи. . . . . : ns3.google.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 78
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:4860:4802:36::a

Имя записи. . . . . : ns4.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 78
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 216.239.38.10

```

```

Имя записи. . . . . : ns4.google.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 78
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2001:4860:4802:38::a

cm-statin.megalabs.ru
-----
Имя записи. . . . . : cm-statin.MEGALABS.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 493
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 37.29.76.102

Имя записи. . . . . : ns1.MEGALABS.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 493
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 83.149.14.243

Имя записи. . . . . : ns2.MEGALABS.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 493
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 83.149.13.65

```

```

sun9-39.userapi.com
-----
Имя записи. . . . . : sun9-39.userapi.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 185
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 87.240.185.146

Имя записи. . . . . : ns1.VKONTAKTE.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 185
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 87.240.131.131

Имя записи. . . . . : ns1.VKONTAKTE.ru
Тип записи. . . . . : 28
Срок жизни. . . . . : 185
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2a00:bdc0:ff:1::2

Имя записи. . . . . : ns2.VKONTAKTE.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 185
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 95.213.21.21

```

```

Имя записи. . . . . : ns2.VKONTAKTE.ru
Тип записи. . . . . : 28
Срок жизни. . . . . : 185
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2a00:bdc0:ff:2::2

Имя записи. . . . . : ns3.VKONTAKTE.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 185
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 93.186.238.238

Имя записи. . . . . : ns3.VKONTAKTE.ru
Тип записи. . . . . : 28
Срок жизни. . . . . : 185
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2a00:bdc0:ff:3::2

Имя записи. . . . . : ns4.VKONTAKTE.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 185
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 87.240.136.136

```

```

edu.academiait.ru
-----
Имя записи. . . . . : edu.academiait.ru
Тип записи. . . . . : 1
Срок жизни. . . . . : 6863
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 78.140.185.180

Имя записи. . . . . : ns2.fozzy.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 6863
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
А-запись (узла) . . . : 88.85.81.2

Имя записи. . . . . : ns2.fozzy.com
Тип записи. . . . . : 28
Срок жизни. . . . . : 6863
Длина данных. . . . . : 16
Раздел. . . . . : Дополнительно
AAAA-запись . . . . . : 2a00:1178:1:66:6::2

```

Результат команды ipconfig /flushdns

```

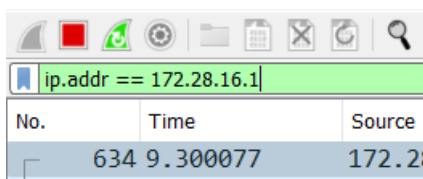
PS C:\> ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.
PS C:\>

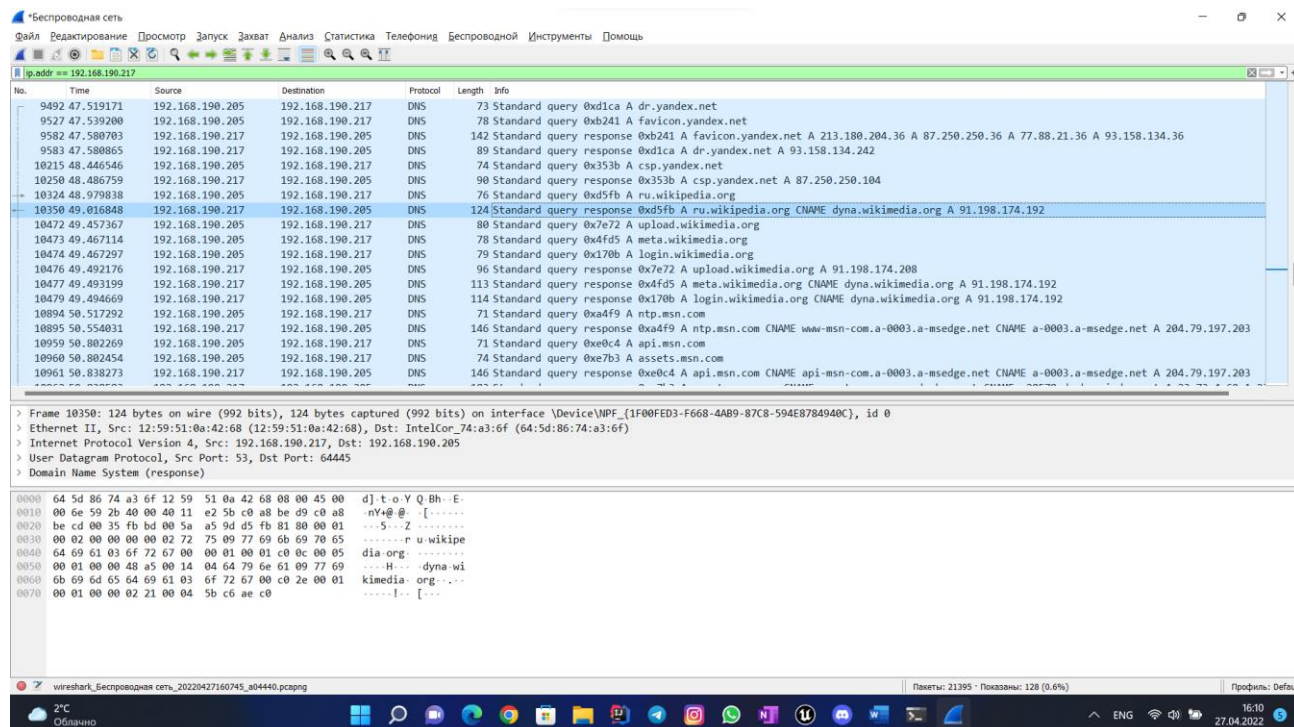
```

### 3. Отслеживание DNS с помощью Wireshark



No.	Time	Source
634	9.300077	172.28.16.1

## Запуск захвата пакетов с фильтром:



Вопросы (сделайте скриншот результатов):

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

DNS запрос и ответ:

10324 48.979838	192.168.190.205	192.168.190.217	DNS	76 Standard query 0xd5fb A ru.wikipedia.org
10350 49.016848	192.168.190.217	192.168.190.205	DNS	124 Standard query response 0xd5fb A ru.wikipedia.org CNAME dyna.wikimedia.org A 91.198.174.192

UDP:

> Flags: 0x4000, Don't fragment  
Fragment offset: 0  
Time to live: 64  
Protocol: (17)  
Header checksum: 0xe25b [validation disabled]  
[Header checksum status: Unverified]

> User Datagram Protocol, Src Port: 53, Dst Port: 64445  
Source Port: 53  
Destination Port: 64445  
Length: 90  
Checksum: 0xa59d [unverified]  
[Checksum Status: Unverified]  
[Stream index: 11]  
> [Timestamps]

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

Запрос:



Source Port: 64445  
Destination Port: 53

Порт источника запроса: 64445

Порт назначения запроса: 53

Ответ:

Порт назначения ответа: 64445

Порт источника ответа: 53

Source Port: 53  
Destination Port: 64445

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

Отправляется на адрес 192.168.190.217 – это мой!!!!, да одинаковые.

10250.48.486759	192.168.190.217	192.168.190.205	DNS	90 Standard query response 0x353b A csp.yandex.net A 87.250.250.104
10324.48.979838	192.168.190.205	192.168.190.217	DNS	76 Standard query 0xd5fb A ru.wikipedia.org
10350.49.016848	192.168.190.217	192.168.190.205	DNS	124 Standard query response 0xd5fb A ru.wikipedia.org CNAME dyna.wikimedia.org A 91.198.174.192
10472.49.457367	192.168.190.205	192.168.190.217	DNS	80 Standard query 0x7e72 A upload.wikimedia.org

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

Тип «A», «CNAME», «ответов» нет.

▼ Domain Name System (query)
Transaction ID: 0xd5fb
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
> ru.wikipedia.org: type A, class IN
<a href="#">[Response In: 10350]</a>

5. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов? «Ответов» 2, каждый содержит: имя, тип, класс, время жизни, длину данных.

```

Domain Name System (response)
  Transaction ID: 0xd5fb
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > ru.wikipedia.org: type A, class IN
  > Answers
    > ru.wikipedia.org: type CNAME, class IN, cname dyna.wikimedia.org
    > dyna.wikimedia.org: type A, class IN, addr 91.198.174.192
    [Request In: 10324]
    [Time: 0.037010000 seconds]
0000 64 5d 86 74 a3 6f 12 59 51 0a 42 68 08 00 45 00 d1-t-o-y 0-Rh--F-
```

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

У меня нет пикч))))))0)))0

На странице могут быть картинки, но для них DNS-запросы не будут выдаваться, ибо dns-запросы могут храниться в кэше браузера.

**Теперь - nslookup.**

- Начать захват пакета.
- Сделайте nslookup www.hdu.edu.cn
- Остановить захват пакетов. У вас должен получиться след, который выглядит примерно так (на последних фотографиях).

```

PS C:\Users\Екатерина\Desktop> nslookup www.hdu.edu.cn
тхЁтхЁ: UnKnown
Address: 192.168.190.217

Не заслуживающий доверия ответ:
ль : www.split.hdu.edu.cn
Addresses: 2001:250:6402:106::102:34
          218.75.123.181
Aliases: www.hdu.edu.cn
```

No.	Time	Source	Destination	Protocol	Length	Info
183	20.005172	192.168.190.205	192.168.190.217	DNS	88	Standard query 0x0001 PTR 217.190.168.192.in-addr.arpa
185	20.059233	192.168.190.217	192.168.190.205	DNS	143	Standard query response 0x0001 No such name PTR 217.190.168.192.in-addr.arpa SOA 168.192.IN-ADDR.ARPA
187	20.087829	192.168.190.205	192.168.190.217	DNS	74	Standard query 0x0002 A www.hdu.edu.cn
193	21.204535	192.168.190.217	192.168.190.205	DNS	124	Standard query response 0x0002 A www.hdu.edu.cn CNAME www.split.hdu.edu.cn A 218.75.123.181
195	21.217962	192.168.190.205	192.168.190.217	DNS	74	Standard query 0x0003 AAAA www.hdu.edu.cn
200	21.807952	192.168.190.217	192.168.190.205	DNS	136	Standard query response 0x0003 AAAA www.hdu.edu.cn CNAME www.split.hdu.edu.cn AAAA 2001:250:6402:106::102:34
299	29.685558	192.168.190.205	192.168.190.217	DNS	74	Standard query 0xa39e A www.google.com
300	29.749077	192.168.190.217	192.168.190.205	DNS	170	Standard query response 0xa39e A www.google.com A 173.194.73.99 A 173.194.73.105 A 173.194.73.106 A 173.194.73.103 A 173.194.73.104
328	30.219507	192.168.190.205	192.168.190.217	DNS	75	Standard query 0xc62b A play.google.com
329	30.276911	192.168.190.217	192.168.190.205	DNS	171	Standard query response 0xc62b A play.google.com A 209.85.233.113 A 209.85.233.102 A 209.85.233.100 A 209.85.233.101 A 209.85.233.13
537	36.027516	192.168.190.205	192.168.190.217	DNS	89	Standard query 0x518c A addons-pa.clients6.google.com
538	36.051487	192.168.190.217	192.168.190.205	DNS	105	Standard query response 0x518c A addons-pa.clients6.google.com A 64.233.161.95

Из приведенного выше снимка экрана видно, что nslookup действительно отправлял DNS-запросы и получал DNS-ответы.

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

Запрос: Порт назначения: 53, источника: 50416.

Destination: 192.168.190.217
▼ User Datagram Protocol, Src Port: 50416, Dst Port: 53
Source Port: 50416
Destination Port: 53
Length: 40
Checksum: 0xff31 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
> [Timestamps]

Ответ: Порт назначения - 50416, порт источника - 53.

Destination: 192.168.190.205
▼ User Datagram Protocol, Src Port: 53, Dst Port: 50416
Source Port: 53
Destination Port: 50416
Length: 90
Checksum: 0x8470 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
> [Timestamps]

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

[Header checksum status: Unverified]
Source: 192.168.190.205
Destination: 192.168.190.217
▼ User Datagram Protocol, Src Port: 50

Отправляется на адрес 192.168.190.217 – это мой!!!!!!!!!!!!1, да

3. Изучите сообщение DNS-запроса. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»? Тип «A», нет.

```

    Domain Name System (query)
      Transaction ID: 0x0002
      > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    > Queries

```

4. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов? Дается два ответа, разных типов: «CNAME» и «A». Содержат авторитетные имена серверов.

```

    > Answers
      > www.hdu.edu.cn: type CNAME, class IN, cname www.split.hdu.edu.cn
      > www.split.hdu.edu.cn: type A, class IN, addr 218.75.123.181
      [Request In: 187]
      [Time: 1.116706000 seconds]

```

Команда: nslookup -type=NS address\_what\_you\_want

```

PS C:\Users\Екатерина\Desktop> nslookup -type=NS www.itmo.ru
Server: 192.168.190.217
Address: 192.168.190.217

itmo.ru
primary name server = ns.itmo.ru
responsible mail addr = hostmaster.itmo.ru
serial = 2021011393
refresh = 3600 (1 hour)
retry = 1800 (30 mins)
expire = 86400 (1 day)
default TTL = 3600 (1 hour)

```

Ответьте на следующие вопросы:

1. На какой IP-адрес отправляется сообщение с запросом DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию? Отправляется на адрес 192.168.190.217 – это мой!!!!!!!, да.

```

[Header checksum status: Unverified]
Source: 192.168.190.205
Destination: 192.168.190.217
User Datagram Protocol Src Port: 55

```

2. Изучите сообщение с запросом DNS. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»? Тип «NS», ответов нет.

- Transaction ID: 0x0002
    - Flags: 0x0100 Standard query
    - Questions: 1
    - Answer RRs: 0
    - Authority RRs: 0
    - Additional RRs: 0
  - Queries
    - www.itmo.ru: type NS, class IN
      - Name: www.itmo.ru
      - [Name Length: 11]
      - [Label Count: 3]
      - Type: NS (authoritative Name Server) (2)
      - Class: IN (0x0001)

[\[Response In: 517\]](#)

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

Class: IN (0x0001)

- Authoritative nameservers
    - itmo.ru: type SOA, class IN, mname ns.itmo.ru
      - Name: itmo.ru
      - Type: SOA (Start Of a zone of Authority) (6)
      - Class: IN (0x0001)
      - Time to live: 1200 (20 minutes)
      - Data length: 38
      - Primary name server: ns.itmo.ru
      - Responsible authority's mailbox: hostmaster.itmo.ru
      - Serial Number: 2021011393
      - Refresh Interval: 3600 (1 hour)
      - Retry Interval: 1800 (30 minutes)
      - Expire limit: 86400 (1 day)
      - Minimum TTL: 3600 (1 hour)

[\[Request In: 516\]](#)  
[Time: 0.059529000 seconds]

Команда: nslookup address\_what\_you\_want your\_DNS

```
PS C:\Users\Екатерина\Desktop> nslookup www.itmo.ru 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Не заслуживающий доверия ответ:
_Л_ : www.itmo.ru
Address: 77.234.204.10
```

No.	Time	Source	Destination	Protocol	Length	Info
514	33.758418	192.168.190.205	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
515	33.806932	8.8.8.8	192.168.190.205	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
516	33.810440	192.168.190.205	8.8.8.8	DNS	71	Standard query 0x0002 A www.itmo.ru
517	33.853357	8.8.8.8	192.168.190.205	DNS	87	Standard query response 0x0002 A www.itmo.ru A 77.234.204.10
518	33.867423	192.168.190.205	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.itmo.ru
519	33.921066	8.8.8.8	192.168.190.205	DNS	121	Standard query response 0x0003 AAAA www.itmo.ru SOA ns.itmo.ru

Ответьте на следующие вопросы:

1. 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? IP-адрес локального DNS-сервера.

```

Header checksum: 0x0000 [Unverified]
[Header checksum status: Unverified]
Source: 192.168.190.205
Destination: 8.8.8.8
▼ User Datagram Protocol, Src Port: 59304, I

```

Нет, не мой!!!!!!!!!!!!!!!!!!!!!!1 Это тот, который я захотела и ввела (гугловский)

2. Изучите сообщение с запросом DNS. Что это за «тип» DNS-запроса? Содержит ли запросное сообщение какие-либо «ответы»? Тип «А» и «AAAA», нет ответов.

№	Time	Source	Destination	Protocol	Length	Info
514	33.758418	192.168.190.205	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
515	33.806932	8.8.8.8	192.168.190.205	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
516	33.810440	192.168.190.205	8.8.8.8	DNS	71	Standard query 0x0002 A www.itmo.ru
517	33.853357	8.8.8.8	192.168.190.205	DNS	87	Standard query response 0x0002 A www.itmo.ru A 77.234.204.10
518	33.867423	192.168.190.205	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.itmo.ru
519	33.921066	8.8.8.8	192.168.190.205	DNS	121	Standard query response 0x0003 AAAA www.itmo.ru SOA ns.itmo.ru

3. Изучите ответное сообщение DNS. Сколько «ответов» дается? Что содержит каждый из этих ответов? Дается два ответа, разных типов: «SOA» и «А» (в каждом из запросов по 1 ответу).

```

Class: IN (0x0001)
▼ Answers
  ▼ www.itmo.ru: type A, class IN, addr 77.234.204.10
    Name: www.itmo.ru
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 7200 (2 hours)
    Data length: 4
    Address: 77.234.204.10
    [Request In: 516]
    [Time: 0.042917000 seconds]

Class: IN (0x0001)
▼ Authoritative nameservers
  ▼ itmo.ru: type SOA, class IN, mname ns.itmo.ru
    Name: itmo.ru
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 38
    Primary name server: ns.itmo.ru
    Responsible authority's mailbox: hostmaster.itmo.ru
    Serial Number: 2021011393
    Refresh Interval: 3600 (1 hour)
    Retry Interval: 1800 (30 minutes)
    Expire limit: 86400 (1 day)
    Minimum TTL: 3600 (1 hour)
    [Request In: 518]
    [Time: 0.053643000 seconds]

```

**Вывод:**

В результате лабораторной работы я научилась работать в терминале с различными запросами, захватывать запросы с помощью программы Wireshark (работать с сетевым анализатором).