

## HW4

1

```
C:\Users\mozha>nslookup www.huya.com
Server: UnKnown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Ль : 36d62c2e.tweb.sched.ovscdns.com
Addresses: 101.33.11.88
          101.33.11.29
          101.33.11.45
          101.33.10.114
          101.33.10.52
          101.33.11.48
          101.33.11.110
Aliases: www.huya.com
         www.huya.com.cdn.dnsv1.com
```

www.huya.com имеет несколько IP адресов

101.33.11.88  
101.33.11.29  
101.33.11.45  
101.33.10.114  
101.33.10.52  
101.33.11.48  
101.33.11.110

```
C:\Users\mozha>nslookup -type=NS www.ox.ac.uk
Server: UnKnown
Address: 192.168.1.1

ox.ac.uk
    primary name server = raptor.dns.ox.ac.uk
    responsible mail addr = hostmaster.ox.ac.uk
    serial = 2022050852
    refresh = 3600 (1 hour)
    retry = 1800 (30 mins)
    expire = 1209600 (14 days)
    default TTL = 900 (15 mins)
```

авторитетный DNS-сервер для Оксфорда raptor.dns.ox.ac.uk

```
C:\Users\mozha>nslookup www.spbu.ru
Server: UnKnown
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Ль : spbu.ru
Address: 195.70.219.101
Aliases: www.spbu.ru
```

spbu.ru имеет один IP адрес 195.70.219.101

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source         | Destination  | Protocol | Length | Info                                     |
|-----|----------|----------------|--------------|----------|--------|------------------------------------------|
| 49  | 1.045407 | 104.16.44.99   | 192.168.1.63 | TLSv1.3  | 1514   | Server Hello, Change Cipher Spec         |
| 691 | 1.627745 | 50.223.129.196 | 192.168.1.63 | TLSv1.3  | 1514   | Server Hello, Change Cipher Spec, Appli  |
| 9   | 0.978023 | 192.168.1.63   | 192.168.1.1  | DNS      | 72     | Standard query 0x0590 A www.ietf.org     |
| 10  | 0.980090 | 192.168.1.63   | 192.168.1.1  | DNS      | 83     | Standard query 0x264b A safebrowsing.go  |
| 18  | 0.999172 | 192.168.1.1    | 192.168.1.63 | DNS      | 149    | Standard query response 0x0590 A www.iet |
| 11  | 0.989224 | 192.168.1.1    | 192.168.1.63 | DNS      | 166    | Standard query response 0x264b A safebro |
| 79  | 1.115939 | 104.16.44.99   | 192.168.1.63 | TCP      | 1445   | [TCP Out-Of-Order] 443 → 56675 [PSH, ACK |
| 78  | 1.115939 | 104.16.44.99   | 192.168.1.63 | TLSv1.3  | 1445   | [TCP Previous segment not captured] , Ap |

...0 0000 0000 0000 = Fragment Offset: 0  
 Time to Live: 64  
 Protocol: UDP (17)  
 Header Checksum: 0x0000 [validation disabled]  
 [Header checksum status: Unverified]  
 Source Address: 192.168.1.63  
 Destination Address: 192.168.1.1  
 > User Datagram Protocol, Src Port: 52551, Dst Port: 53  
 > Domain Name System (query)

0010 00 3a d5 11 00 00 40 11 00 00 c0 a8 01 3f c0 a8 .:....@. ....?..

Protocol (ip.proto), 1 byte(s) || Пакеты: 806 · Показаны: 791 (98.1%) · Потеряно: 0 (0.0%) || Профиль: Default

Протокол UDP, порт назначения 53

```
C:\Users\mozha>ipconfig /all
```

#### Настройка протокола IP для Windows

```
Имя компьютера . . . . . : LAPTOP-F4SR9KIR
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
```

#### Адаптер Ethernet Ethernet:

```
DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek PCIe GbE Family Controller
Физический адрес. . . . . : 84-A9-3E-0E-F2-25
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::10d4:1733:b61a:8bed%8(Основной)
IPv4-адрес. . . . . : 192.168.1.63(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 8 мая 2022 г. 9:40:35
Срок аренды истекает. . . . . : 8 мая 2022 г. 22:23:11
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 109357374
DUID клиента DHCPv6 . . . . . : 00-01-00-01-23-73-BE-41-84-A9-3E-0E-F2-25
DNS-серверы. . . . . : 192.168.1.1
NetBios через TCP/IP. . . . . : Включен
```

Отправлен на адрес 192.168.1.1, совпадает с локальным

The image shows a Wireshark packet capture window titled "\*Ethernet". The filter bar at the top shows "ip.addr == 192.168.1.63". The packet list shows four packets:

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                                     |
|-----|----------|--------------|--------------|----------|--------|----------------------------------------------------------|
| 9   | 0.978023 | 192.168.1.63 | 192.168.1.1  | DNS      | 72     | Standard query 0x0590 A www.ietf.org                     |
| 10  | 0.980090 | 192.168.1.63 | 192.168.1.1  | DNS      | 83     | Standard query 0x264b A safebrowsing.google.com          |
| 18  | 0.999172 | 192.168.1.1  | 192.168.1.63 | DNS      | 149    | Standard query response 0x0590 A www.ietf.org            |
| 11  | 0.989224 | 192.168.1.1  | 192.168.1.63 | DNS      | 166    | Standard query response 0x264b A safebrowsing.google.com |

The packet details pane for packet 9 shows:

- Internet Protocol Version 4, Src: 192.168.1.63, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 52551, Dst Port: 53
- Domain Name System (query)
  - Transaction ID: 0x0590
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
- Queries
  - www.ietf.org: type A, class IN
    - Name: www.ietf.org
    - [Name Length: 12]
    - [Label Count: 3]
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)

The packet bytes pane shows the raw data for packet 9:

```
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.....
```

The status bar at the bottom indicates: "Text item (text), 18 byte(s) | Пакеты: 806 · Показаны: 791 (98.1%) · Потеряно: 0 (0.0%) | Профиль: Default"

www.ietf.org: type A, class IN, ответов нет

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                                     |
|-----|----------|--------------|--------------|----------|--------|----------------------------------------------------------|
| 9   | 0.978023 | 192.168.1.63 | 192.168.1.1  | DNS      | 72     | Standard query 0x0590 A www.ietf.org                     |
| 10  | 0.980090 | 192.168.1.63 | 192.168.1.1  | DNS      | 83     | Standard query 0x264b A safebrowsing.google.com          |
| 18  | 0.999172 | 192.168.1.1  | 192.168.1.63 | DNS      | 149    | Standard query response 0x0590 A www.ietf.org            |
| 11  | 0.989224 | 192.168.1.1  | 192.168.1.63 | DNS      | 166    | Standard query response 0x264b A safebrowsing.google.com |

Questions: 1  
 Answer RRs: 3  
 Authority RRs: 0  
 Additional RRs: 0

Queries

- www.ietf.org: type A, class IN
  - Name: www.ietf.org
  - [Name Length: 12]
  - [Label Count: 3]
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)

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 104.16.44.99
- > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99

[Request In: 9]  
 [Time: 0.021149000 seconds]

0040 6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00 org.....  
 0050 04 65 00 21 03 77 77 77 04 69 65 74 66 03 6f 72 .e!.www.ietf.or

Text item (text), 77 byte(s) | Пакеты: 806 · Показаны: 791 (98.1%) · Потеряно: 0 (0.0%) | Профиль: Default

3 ответа, содержащие тип, класс, домен и адрес

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 104.16.44.99

www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination    | Protocol | Length | Info                                                     |
|-----|----------|--------------|----------------|----------|--------|----------------------------------------------------------|
| 9   | 0.978023 | 192.168.1.63 | 192.168.1.1    | DNS      | 72     | Standard query 0x0590 A www.ietf.org                     |
| 10  | 0.980090 | 192.168.1.63 | 192.168.1.1    | DNS      | 83     | Standard query 0x264b A safebrowsing.google.com          |
| 18  | 0.999172 | 192.168.1.1  | 192.168.1.63   | DNS      | 149    | Standard query response 0x0590 A www.ietf.org            |
| 11  | 0.989224 | 192.168.1.1  | 192.168.1.63   | DNS      | 166    | Standard query response 0x264b A safebrowsing.google.com |
| 79  | 1.115939 | 104.16.44.99 | 192.168.1.63   | TCP      | 1445   | [TCP Out-Of-Order] 443 → 56675 [PSH, ACK]                |
| 78  | 1.115939 | 104.16.44.99 | 192.168.1.63   | TLSv1.3  | 1445   | [TCP Previous segment not captured] , Application Data   |
| 753 | 2.005338 | 192.168.1.63 | 50.223.129.196 | TCP      | 54     | 56679 → 443 [ACK] Seq=1199 Ack=38643 Win=0 Len=0         |

> Frame 79: 1445 bytes on wire (11560 bits), 1445 bytes captured (11560 bits) on interface \Device\NPF\_{45939136-950B-4A8E-8000-000000000000}

> Ethernet II, Src: Keenetic\_1e:95:c8 (50:ff:20:1e:95:c8), Dst: HewlettP\_0e:f2:25 (84:a9:3e:0e:f2:25)

> Internet Protocol Version 4, Src: 104.16.44.99, Dst: 192.168.1.63

✓ Transmission Control Protocol, Src Port: 443, Dst Port: 56675, Seq: 11422, Ack: 1446, Len: 1391

Source Port: 443

Destination Port: 56675

[Stream index: 3]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 1391]

Sequence Number: 11422 (relative sequence number)

Sequence Number (raw): 1065457127

[Next Sequence Number: 12813 (relative sequence number)]

Acknowledgment Number: 1446 (relative ack number)

Acknowledgment number (raw): 559115699

0000 84 a9 3e 0e f2 25 50 ff 20 1e 95 c8 08 00 45 00 ..>..%P. ....E.

0010 05 97 f8 0d 40 00 38 06 ee f8 68 10 2c 63 c0 a8 ....@.8. ..h.,c..

wireshark\_Ethernet9W2WL1.pcapng | Пакеты: 806 · Показаны: 791 (98.1%) · Потеряно: 0 (0.0%) | Профиль: Default

Адрес 104.16.44.99 совпадает, новых DNS запросов не видно

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                           |
|-----|----------|--------------|--------------|----------|--------|------------------------------------------------|
| 5   | 0.799093 | 192.168.1.63 | 192.168.1.1  | DNS      | 84     | Standard query 0x0001 PTR 1.1.168.192.in-addr. |
| 6   | 0.816268 | 192.168.1.1  | 192.168.1.63 | DNS      | 84     | Standard query response 0x0001 No such name PT |
| 7   | 0.818611 | 192.168.1.63 | 192.168.1.1  | DNS      | 71     | Standard query 0x0002 A www.spbu.ru            |
| 8   | 0.843526 | 192.168.1.1  | 192.168.1.63 | DNS      | 101    | Standard query response 0x0002 A www.spbu.ru C |
| 9   | 0.848897 | 192.168.1.63 | 192.168.1.1  | DNS      | 71     | Standard query 0x0003 AAAA www.spbu.ru         |
| 10  | 0.873034 | 192.168.1.1  | 192.168.1.63 | DNS      | 138    | Standard query response 0x0003 AAAA www.spbu.r |

> Frame 9: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{45939136-950B-4A86-B5D2-5B4}

> Ethernet II, Src: HewlettP\_0e:f2:25 (84:a9:3e:0e:f2:25), Dst: Keenetic\_1e:95:c8 (50:ff:20:1e:95:c8)

> Internet Protocol Version 4, Src: 192.168.1.63, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 59513, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0003

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ www.spbu.ru: type AAAA, class IN

Name: www.spbu.ru

0020 01 01 e8 79 00 35 00 25 83 c7 00 03 01 00 00 01 ..y.5.% ..

0030 00 00 00 00 00 00 00 03 77 77 77 04 73 70 62 75 02 .....w ww.spbu

User Datagram Protocol (udp), 8 byte(s) | Пакеты: 26 · Показаны: 6 (23.1%) · Потеряно: 0 (0.0%) | Профиль: Default

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                           |
|-----|----------|--------------|--------------|----------|--------|------------------------------------------------|
| 5   | 0.799093 | 192.168.1.63 | 192.168.1.1  | DNS      | 84     | Standard query 0x0001 PTR 1.1.168.192.in-addr. |
| 6   | 0.816268 | 192.168.1.1  | 192.168.1.63 | DNS      | 84     | Standard query response 0x0001 No such name PT |
| 7   | 0.818611 | 192.168.1.63 | 192.168.1.1  | DNS      | 71     | Standard query 0x0002 A www.spbu.ru            |
| 8   | 0.843526 | 192.168.1.1  | 192.168.1.63 | DNS      | 101    | Standard query response 0x0002 A www.spbu.ru C |
| 9   | 0.848897 | 192.168.1.63 | 192.168.1.1  | DNS      | 71     | Standard query 0x0003 AAAA www.spbu.ru         |
| 10  | 0.873034 | 192.168.1.1  | 192.168.1.63 | DNS      | 138    | Standard query response 0x0003 AAAA www.spbu.r |

> Frame 10: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface \Device\NPF\_{45939136-950B-4A86-B5C}

> Ethernet II, Src: Keenetic\_1e:95:c8 (50:ff:20:1e:95:c8), Dst: HewlettP\_0e:f2:25 (84:a9:3e:0e:f2:25)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.63

> User Datagram Protocol, Src Port: 53, Dst Port: 59513

▼ Domain Name System (response)

Transaction ID: 0x0003

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 0

▼ Queries

▼ www.spbu.ru: type AAAA, class IN

Name: www.spbu.ru

0020 01 3f 00 35 e8 79 00 68 ca 2c 00 03 81 80 00 01 .? .5 .y .h . , . . . . .

0030 00 01 00 01 00 00 03 77 77 77 04 73 70 62 75 02 . . . . . w ww .spbu .

User Datagram Protocol (udp), 8 byte(s) | Пакеты: 26 · Показаны: 6 (23.1%) · Потеряно: 0 (0.0%) | Профиль: Default

Порт 53

Отправлен на адрес 192.168.1.1, совпадает с локальным

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                           |
|-----|----------|--------------|--------------|----------|--------|------------------------------------------------|
| 5   | 0.799093 | 192.168.1.63 | 192.168.1.1  | DNS      | 84     | Standard query 0x0001 PTR 1.1.168.192.in-addr. |
| 6   | 0.816268 | 192.168.1.1  | 192.168.1.63 | DNS      | 84     | Standard query response 0x0001 No such name PT |
| 7   | 0.818611 | 192.168.1.63 | 192.168.1.1  | DNS      | 71     | Standard query 0x0002 A www.spbu.ru            |
| 8   | 0.843526 | 192.168.1.1  | 192.168.1.63 | DNS      | 101    | Standard query response 0x0002 A www.spbu.ru C |
| 9   | 0.848897 | 192.168.1.63 | 192.168.1.1  | DNS      | 71     | Standard query 0x0003 AAAA www.spbu.ru         |
| 10  | 0.873034 | 192.168.1.1  | 192.168.1.63 | DNS      | 138    | Standard query response 0x0003 AAAA www.spbu.r |

Transaction ID: 0x0003

- > Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
  - www.spbu.ru: type AAAA, class IN
    - Name: www.spbu.ru
    - [Name Length: 11]
    - [Label Count: 3]
    - Type: AAAA (IPv6 Address) (28)
    - Class: IN (0x0001)
    - [Response In: 10]

0030 00 00 00 00 00 03 77 77 77 04 73 70 62 75 02 ..w ww.spbu.  
 0040 72 75 00 00 1c 00 01 ru.....

Text item (text), 17 byte(s) | Пакеты: 26 · Показаны: 6 (23.1%) · Потеряно: 0 (0.0%) | Профиль: Default

www.spbu.ru: type AAAA, class IN, ответов нет



\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                           |
|-----|----------|--------------|--------------|----------|--------|------------------------------------------------|
| 5   | 0.799093 | 192.168.1.63 | 192.168.1.1  | DNS      | 84     | Standard query 0x0001 PTR 1.1.168.192.in-addr. |
| 6   | 0.816268 | 192.168.1.1  | 192.168.1.63 | DNS      | 84     | Standard query response 0x0001 No such name PT |
| 7   | 0.818611 | 192.168.1.63 | 192.168.1.1  | DNS      | 71     | Standard query 0x0002 A www.spbu.ru            |
| 8   | 0.843526 | 192.168.1.1  | 192.168.1.63 | DNS      | 101    | Standard query response 0x0002 A www.spbu.ru C |
| 9   | 0.848897 | 192.168.1.63 | 192.168.1.1  | DNS      | 71     | Standard query 0x0003 AAAA www.spbu.ru         |
| 10  | 0.873034 | 192.168.1.1  | 192.168.1.63 | DNS      | 138    | Standard query response 0x0003 AAAA www.spbu.r |

Type: AAAA (IPv6 Address) (28)  
Class: IN (0x0001)

Answers

www.spbu.ru: type CNAME, class IN, cname spbu.ru

Name: www.spbu.ru  
Type: CNAME (Canonical NAME for an alias) (5)  
Class: IN (0x0001)  
Time to live: 3600 (1 hour)  
Data length: 2  
CNAME: spbu.ru

Authoritative nameservers

> spbu.ru: type SOA, class IN, mname ns.pu.ru  
[\[Request In: 9\]](#)  
[Time: 0.024137000 seconds]

0040 72 75 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 0e ru .....  
0050 10 00 02 c0 10 c0 10 00 06 00 01 00 00 07 08 00 .....

Text item (text), 14 byte(s) | Пакеты: 26 · Показаны: 6 (23.1%) · Потеряно: 0 (0.0%) | Профиль: Default

Ответ один: www.spbu.ru: type CNAME, class IN, cname spbu.ru

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                     |
|-----|----------|--------------|--------------|----------|--------|------------------------------------------|
| 5   | 0.374086 | 192.168.1.63 | 192.168.1.1  | DNS      | 84     | Standard query 0x0001 PTR 1.1.168.192.in |
| 6   | 0.375845 | 192.168.1.1  | 192.168.1.63 | DNS      | 84     | Standard query response 0x0001 No such r |
| 7   | 0.377996 | 192.168.1.63 | 192.168.1.1  | DNS      | 67     | Standard query 0x0002 NS spbu.ru         |
| 8   | 0.379316 | 192.168.1.1  | 192.168.1.63 | DNS      | 123    | Standard query response 0x0002 NS spbu.r |

> Frame 7: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF\_{45939136-950B-4A86-B5D2-5B4}

> Ethernet II, Src: HewlettP\_0e:f2:25 (84:a9:3e:0e:f2:25), Dst: Keenetic\_1e:95:c8 (50:ff:20:1e:95:c8)

> Internet Protocol Version 4, Src: 192.168.1.63, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 62288, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ spbu.ru: type NS, class IN

Name: spbu.ru

[Name Length: 7]

[Label Count: 2]

Type: NS (authoritative Name Server) (2)

0000 50 ff 20 1e 95 c8 84 a9 3e 0e f2 25 08 00 45 00 p. .... >..%.E.

0010 00 35 d7 ff 00 00 40 11 00 00 c0 a8 01 3f c0 a8 .5...@. ....?..

wireshark\_EthernetC02NL1.pcapng | Пакеты: 32 · Показаны: 22 (68.8%) · Потеряно: 0 (0.0%) | Профиль: Default

Отправлен на адрес 192.168.1.1, совпадает с локальным

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                      |
|-----|----------|--------------|--------------|----------|--------|-------------------------------------------|
| 5   | 0.374086 | 192.168.1.63 | 192.168.1.1  | DNS      | 84     | Standard query 0x0001 PTR 1.1.168.192.in  |
| 6   | 0.375845 | 192.168.1.1  | 192.168.1.63 | DNS      | 84     | Standard query response 0x0001 No such    |
| 7   | 0.377996 | 192.168.1.63 | 192.168.1.1  | DNS      | 67     | Standard query 0x0002 NS spbu.ru          |
| 8   | 0.379316 | 192.168.1.1  | 192.168.1.63 | DNS      | 123    | Standard query response 0x0002 NS spbu.ru |

> User Datagram Protocol, Src Port: 62288, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0002

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

▼ spbu.ru: type NS, class IN

Name: spbu.ru

[Name Length: 7]

[Label Count: 2]

Type: NS (authoritative Name Server) (2)

Class: IN (0x0001)

[Response In: 8]

0030 00 00 00 00 00 00 04 73 70 62 75 02 72 75 00 00 .....s pbu.ru..

0040 02 00 01 ...

Text item (text), 13 byte(s) | Пакеты: 32 · Показаны: 22 (68.8%) · Потеряно: 0 (0.0%) | Профиль: Default

spbu.ru: type NS, class IN, ответов нет

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source       | Destination  | Protocol | Length | Info                                      |
|-----|----------|--------------|--------------|----------|--------|-------------------------------------------|
| 5   | 0.374086 | 192.168.1.63 | 192.168.1.1  | DNS      | 84     | Standard query 0x0001 PTR 1.1.168.192.in  |
| 6   | 0.375845 | 192.168.1.1  | 192.168.1.63 | DNS      | 84     | Standard query response 0x0001 No such    |
| 7   | 0.377996 | 192.168.1.63 | 192.168.1.1  | DNS      | 67     | Standard query 0x0002 NS spbu.ru          |
| 8   | 0.379316 | 192.168.1.1  | 192.168.1.63 | DNS      | 123    | Standard query response 0x0002 NS spbu.ru |

Queries

- spbu.ru: type NS, class IN

Answers

- spbu.ru: type NS, class IN, ns ns2.pu.ru
  - Name: spbu.ru
  - Type: NS (authoritative Name Server) (2)
  - Class: IN (0x0001)
  - Time to live: 3600 (1 hour)
  - Data length: 9
  - Name Server: ns2.pu.ru
- spbu.ru: type NS, class IN, ns ns7.spbu.ru
  - Name: spbu.ru
  - Type: NS (authoritative Name Server) (2)
  - Class: IN (0x0001)
  - Time to live: 3600 (1 hour)
  - Data length: 6
  - Name Server: ns7.spbu.ru
- spbu.ru: type NS, class IN, ns ns.pu.ru
  - Name: spbu.ru
  - Type: NS (authoritative Name Server) (2)
  - Class: IN (0x0001)
  - Time to live: 3600 (1 hour)
  - Data length: 5
  - Name Server: ns.pu.ru

[Request In: 7]

[Time: 0.001320000 seconds]

```

0030 00 03 00 00 00 00 04 73 70 62 75 02 72 75 00 00  ...s pbu.ru..
0040 02 00 01 c0 0c 00 02 00 01 00 00 0e 10 00 09 03  .....
0050 6e 73 32 02 70 75 c0 11 c0 0c 00 02 00 01 00 00  ns2.pu.....
  
```

Text item (text), 13 byte(s) | Пакеты: 32 · Показаны: 22 (68.8%) · Потеряно: 0 (0.0%) | Профиль: Default

3 ответа, содержат тип, класс и имена ns серверов

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source         | Destination    | Protocol | Length | Info                                           |
|-----|----------|----------------|----------------|----------|--------|------------------------------------------------|
| 6   | 0.541659 | 192.168.1.63   | 192.168.1.1    | DNS      | 69     | Standard query 0x4316 A ns2.pu.ru              |
| 7   | 0.558376 | 192.168.1.1    | 192.168.1.63   | DNS      | 85     | Standard query response 0x4316 A ns2.pu.ru A 1 |
| 8   | 0.575911 | 192.168.1.63   | 195.70.196.210 | DNS      | 87     | Standard query 0x0001 PTR 210.196.70.195.in-ad |
| 9   | 0.578176 | 195.70.196.210 | 192.168.1.63   | DNS      | 173    | Standard query response 0x0001 PTR 210.196.70. |
| 10  | 0.580044 | 192.168.1.63   | 195.70.196.210 | DNS      | 71     | Standard query 0x0002 A www.spbu.ru            |
| 11  | 0.582207 | 195.70.196.210 | 192.168.1.63   | DNS      | 205    | Standard query response 0x0002 A www.spbu.ru C |
| 12  | 0.582752 | 192.168.1.63   | 195.70.196.210 | DNS      | 71     | Standard query 0x0003 AAAA www.spbu.ru         |
| 13  | 0.598708 | 195.70.196.210 | 192.168.1.63   | DNS      | 138    | Standard query response 0x0003 AAAA www.spbu.r |
| 14  | 0.939506 | 141.8.179.63   | 192.168.1.63   | TCP      | 60     | 443 → 57764 [ACK] Seq=1 Ack=1 Win=11 Len=0     |
| 15  | 0.939580 | 192.168.1.63   | 141.8.179.63   | TCP      | 54     | [TCP ZeroWindow] [TCP ACKed unseen segment] 57 |

> Frame 12: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{45939136-950B-4A86-B5D2-5B48}

> Ethernet II, Src: HewlettP\_0e:f2:25 (84:a9:3e:0e:f2:25), Dst: Keenetic\_1e:95:c8 (50:ff:20:1e:95:c8)

> Internet Protocol Version 4, Src: 192.168.1.63, Dst: 195.70.196.210

> User Datagram Protocol, Src Port: 63930, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0003

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> www.spbu.ru: type AAAA, class IN

[\[Response In: 13\]](#)

```

0020  c4 d2 f9 ba 00 35 00 25 4a 37 00 03 01 00 00 01  .....5.% J7.....
0030  00 00 00 00 00 00 03 77 77 77 04 73 70 62 75 02  ....w ww.spbu.
0040  72 75 00 00 1c 00 01                          ru.....

```

Number of answers in packet (dns.count.answers), 2 byte(s) || Пакеты: 24 · Показаны: 10 (41.7%) · Потеряно: 0 (0.0%) || Профиль: Default

Адрес 195.70.196.210, это адрес ns2.pu.ru

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source         | Destination    | Protocol | Length | Info                                           |
|-----|----------|----------------|----------------|----------|--------|------------------------------------------------|
| 6   | 0.541659 | 192.168.1.63   | 192.168.1.1    | DNS      | 69     | Standard query 0x4316 A ns2.pu.ru              |
| 7   | 0.558376 | 192.168.1.1    | 192.168.1.63   | DNS      | 85     | Standard query response 0x4316 A ns2.pu.ru A 1 |
| 8   | 0.575911 | 192.168.1.63   | 195.70.196.210 | DNS      | 87     | Standard query 0x0001 PTR 210.196.70.195.in-ad |
| 9   | 0.578176 | 195.70.196.210 | 192.168.1.63   | DNS      | 173    | Standard query response 0x0001 PTR 210.196.70. |
| 10  | 0.580044 | 192.168.1.63   | 195.70.196.210 | DNS      | 71     | Standard query 0x0002 A www.spbu.ru            |
| 11  | 0.582207 | 195.70.196.210 | 192.168.1.63   | DNS      | 205    | Standard query response 0x0002 A www.spbu.ru C |
| 12  | 0.582752 | 192.168.1.63   | 195.70.196.210 | DNS      | 71     | Standard query 0x0003 AAAA www.spbu.ru         |
| 13  | 0.598708 | 195.70.196.210 | 192.168.1.63   | DNS      | 138    | Standard query response 0x0003 AAAA www.spbu.r |
| 14  | 0.939506 | 141.8.179.63   | 192.168.1.63   | TCP      | 60     | 443 → 57764 [ACK] Seq=1 Ack=1 Win=11 Len=0     |
| 15  | 0.939580 | 192.168.1.63   | 141.8.179.63   | TCP      | 54     | [TCP ZeroWindow] [TCP ACKed unseen segment] 57 |

> Frame 12: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{45939136-950B-4A86-B5D2-5B48}

> Ethernet II, Src: HewlettP\_0e:f2:25 (84:a9:3e:0e:f2:25), Dst: Keenetic\_1e:95:c8 (50:ff:20:1e:95:c8)

> Internet Protocol Version 4, Src: 192.168.1.63, Dst: 195.70.196.210

> User Datagram Protocol, Src Port: 63930, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x0003

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> www.spbu.ru: type AAAA, class IN

[\[Response In: 13\]](#)

```

0020  c4 d2 f9 ba 00 35 00 25 4a 37 00 03 01 00 00 01  ....5.% J7....
0030  00 00 00 00 00 00 03 77 77 77 04 73 70 62 75 02  ....w ww.spbu
0040  72 75 00 00 1c 00 01                               ru.....

```

Text item (text), 17 byte(s) || Пакеты: 24 · Показаны: 10 (41.7%) · Потеряно: 0 (0.0%) || Профиль: Default

www.spbu.ru: type AAAA, class IN, ответов нет

\*Ethernet

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr == 192.168.1.63

| No. | Time     | Source         | Destination    | Protocol | Length | Info                                           |
|-----|----------|----------------|----------------|----------|--------|------------------------------------------------|
| 6   | 0.541659 | 192.168.1.63   | 192.168.1.1    | DNS      | 69     | Standard query 0x4316 A ns2.pu.ru              |
| 7   | 0.558376 | 192.168.1.1    | 192.168.1.63   | DNS      | 85     | Standard query response 0x4316 A ns2.pu.ru A 1 |
| 8   | 0.575911 | 192.168.1.63   | 195.70.196.210 | DNS      | 87     | Standard query 0x0001 PTR 210.196.70.195.in-ad |
| 9   | 0.578176 | 195.70.196.210 | 192.168.1.63   | DNS      | 173    | Standard query response 0x0001 PTR 210.196.70. |
| 10  | 0.580044 | 192.168.1.63   | 195.70.196.210 | DNS      | 71     | Standard query 0x0002 A www.spbu.ru            |
| 11  | 0.582207 | 195.70.196.210 | 192.168.1.63   | DNS      | 205    | Standard query response 0x0002 A www.spbu.ru C |
| 12  | 0.582752 | 192.168.1.63   | 195.70.196.210 | DNS      | 71     | Standard query 0x0003 AAAA www.spbu.ru         |
| 13  | 0.598708 | 195.70.196.210 | 192.168.1.63   | DNS      | 138    | Standard query response 0x0003 AAAA www.spbu.r |
| 14  | 0.939506 | 141.8.179.63   | 192.168.1.63   | TCP      | 60     | 443 → 57764 [ACK] Seq=1 Ack=1 Win=11 Len=0     |
| 15  | 0.939580 | 192.168.1.63   | 141.8.179.63   | TCP      | 54     | [TCP ZeroWindow] [TCP ACKed unseen segment] 57 |

Transaction ID: 0x0003

- > Flags: 0x8500 Standard query response, No error
- Questions: 1
- Answer RRs: 1
- Authority RRs: 1
- Additional RRs: 0
- Queries
  - > www.spbu.ru: type AAAA, class IN
- Answers
  - www.spbu.ru: type CNAME, class IN, cname spbu.ru
    - Name: www.spbu.ru
    - Type: CNAME (Canonical NAME for an alias) (5)
    - Class: IN (0x0001)
    - Time to live: 3600 (1 hour)
    - Data length: 2
    - CNAME: spbu.ru
- Authoritative nameservers
  - > spbu.ru: type SOA, class IN, mname ns.pu.ru
  - [Request In: 12]
  - [Time: 0.015956000 seconds]

```

0040 72 75 00 00 1c 00 01 c0 0c 00 05 00 01 00 00 0e ru.....
0050 10 00 02 c0 10 c0 10 00 06 00 01 00 00 0e 10 00 .....
0060 29 02 6e 73 02 70 75 c0 15 0a 68 6f 73 74 6d 61 )ns.pu..hostma

```

Text item (text), 14 byte(s) | Пакеты: 24 · Показаны: 10 (41.7%) · Потеряно: 0 (0.0%) | Профиль: Default

Ответ www.spbu.ru: type CNAME, class IN, cname spbu.ru

6 whois - база данных со сведениями о доменах. Запись о домене обычно содержит имя и контактную информацию «регистранта» (владельца домена) и «регистратора» (организации, которая домен зарегистрировала), имена DNS серверов, дату регистрации и дату истечения срока ее действия.

<https://2domains.ru/whois>

|          |                                      |           |
|----------|--------------------------------------|-----------|
| habr.com | <a href="#">Punycode-конвертация</a> | Проверить |
|----------|--------------------------------------|-----------|

|            |                   |
|------------|-------------------|
| Домен      | HABR.COM          |
| Сервер DNS | ns1.habradns.net. |
| Сервер DNS | ns2.habradns.net. |
| Сервер DNS | ns3.habradns.net. |



```
C:\Users\mozha>nslookup 192.168.1.1
```

```
ᐃᐃᐃᐃᐃᐃ: UnKnown
```

```
Address: 192.168.1.1
```

```
*** UnKnown не удалось найти 192.168.1.1: Non-existent domain
```

```
C:\Users\mozha>nslookup ns1.habradns.net
```

```
ᐃᐃᐃᐃᐃᐃ: UnKnown
```

```
Address: 192.168.1.1
```

```
Не заслуживающий доверия ответ:
```

```
ᐃᐃᐃ : ns1.habradns.net
```

```
Addresses: 2604:240:1:3::16
```

```
2a03:f480:1:c::29
```

```
2a01:5a60:2::38
```

```
185.105.224.58
```

```
159.253.22.172
```

```
205.196.80.14
```

```
C:\Users\mozha>nslookup ns2.habradns.net
```

```
ᐃᐃᐃᐃᐃᐃ: UnKnown
```

```
Address: 192.168.1.1
```

```
Не заслуживающий доверия ответ:
```

```
ᐃᐃᐃ : ns2.habradns.net
```

```
Addresses: 2a03:b0c0:1:d0::1194:e001
```

```
2a03:b0c0:2:d0::135b:7001
```

```
2a03:b0c0:3:d0::de9:1
```

```
159.65.29.206
```

```
46.101.153.50
```

```
142.93.224.28
```