Wireshark. Работа с DNS.

A. Утилита nslookup (1 балл).

1.

```
[dword@fedora ~]$ nslookup huawei.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   huawei.com
Address: 121.37.49.12
Name:   huawei.com
Address: 2407:c080:17ef:ffff::7274:d206
```

2.

```
[dword@fedora ~]$ nslookup -type=soa ox.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ox.ac.uk
        origin = raptor.dns.ox.ac.uk
        mail addr = hostmaster.ox.ac.uk
        serial = 2022031960
        refresh = 3600
        retry = 1800
        expire = 1209600
        minimum = 900

Authoritative answers can be found from:
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.
ns2.ja.net      internet address = 193.63.105.17
dns0.ox.ac.uk   internet address = 129.67.1.190
dns1.ox.ac.uk   internet address = 129.67.1.191
dns2.ox.ac.uk   internet address = 163.1.2.190
auth4.dns.ox.ac.uk      internet address = 45.33.127.156
auth5.dns.ox.ac.uk      internet address = 93.93.128.67
auth6.dns.ox.ac.uk      internet address = 185.24.221.32
ns2.ja.net      has AAAA address 2001:630:0:45::11
auth4.dns.ox.ac.uk      has AAAA address 2600:3c00::f03c:91ff:fe96:beac
auth5.dns.ox.ac.uk      has AAAA address 2a00:1098:0:80:1000::10
auth6.dns.ox.ac.uk      has AAAA address 2a02:2770:11:0:21a:4aff:febe:759b

[dword@fedora ~]$
```

Авторитетные DNS-серверы перечислены в записях вида nameserver =... после Authoritative answers can be found from.

3.

```
[dword@fedora ~]$ nslookup spbu.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   spbu.ru
Address: 195.70.219.101
```

Сайт СПбГУ имеет один IP-адрес.

Несколько IP-адресов имеет, например, сайт google.com:

```
[dword@fedora ~]$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 74.125.131.138
Name:   google.com
Address: 74.125.131.139
Name:   google.com
Address: 74.125.131.113
Name:   google.com
Address: 74.125.131.101
Name:   google.com
Address: 74.125.131.102
Name:   google.com
Address: 74.125.131.100
Name:   google.com
Address: 2a00:1450:4010:c0e::71
Name:   google.com
Address: 2a00:1450:4010:c0e::8b
Name:   google.com
Address: 2a00:1450:4010:c0e::65
Name:   google.com
Address: 2a00:1450:4010:c0e::64
```

Б. DNS-трассировка www.ietf.org (3 балла).

1. Используется UDP:

   ```
   User Datagram Protocol, Src Port: 43068, Dst Port: 53
   ```

2. Dst Port: 53
3.

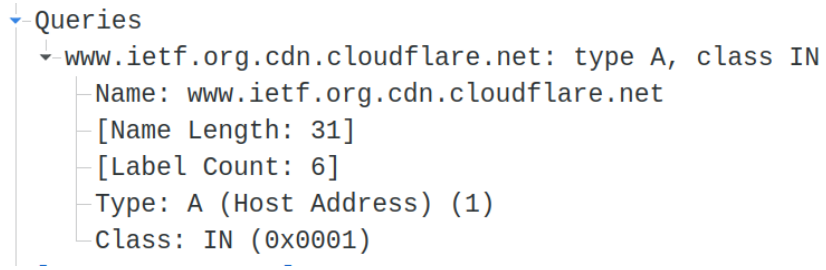
   ip.addr == 192.168.0.104 && dns

No.	Time	Source	Destination
12	2.166782459	192.168.0.104	192.168.0.1
13	2.175510817	192.168.0.1	192.168.0.104

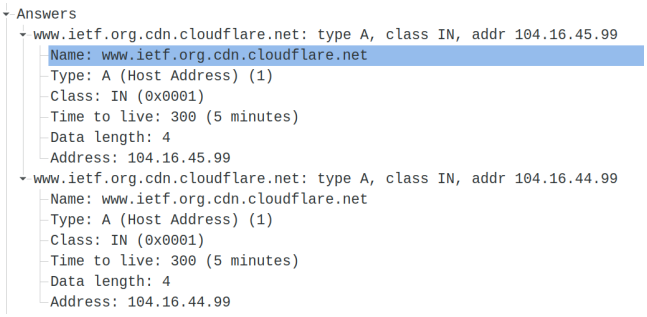
   DNS-запрос отправлен на адрес 192.168.0.1.
   IP-адрес локального DNS-сервера – 192.168.0.1:

   ```
   [dword@fedora ~]$ systemd-resolve --status
   Global
          Protocols: LLMNR=resolve -mDNS -DNSOverTLS DNSSEC=no/unsupported
   resolv.conf mode: stub

   Link 2 (wlp0s20f3)
       Current Scopes: DNS LLMNR/IPv4 LLMNR/IPv6
            Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
   Current DNS Server: 192.168.0.1
          DNS Servers: 192.168.0.1
           DNS Domain: www.tendawifi.com

   Link 3 (virbr0)
   Current Scopes: none
        Protocols: -DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
   ```

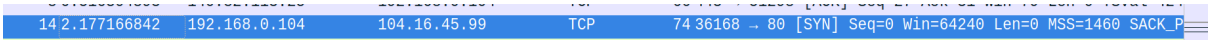
   Эти IP-адреса совпадают.
4. Запрашивается запись типа A:



Ответов в запросе не содержится.

5. 

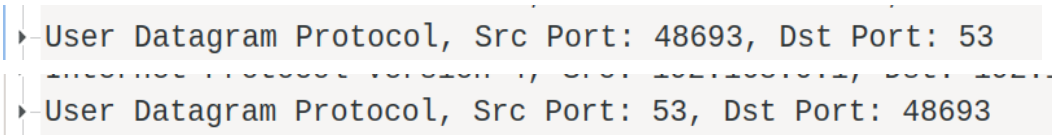
В ответном сообщении DNS два ответа, содержимое показано на скрине.

6. 

IP-адрес TCP-пакета с SYN соответствует адресу www.ietf.cdn.cloudflare.net.

7. Нет, такие запросы не выполняются

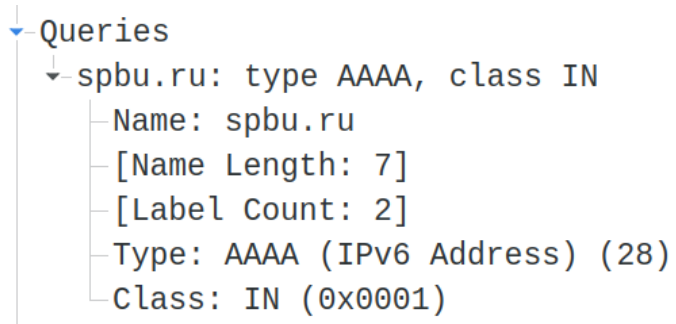
B. DNS-трассировка www.spbu.ru (2 балла).

1. 

Порт 53.

2. 

Запрос отправляется на адрес 192.168.0.1. Он совпадает с IP-адресом локального DNS-сервера.

3. 

Запрашивается запись типа AAAA, ответы не содержатся.

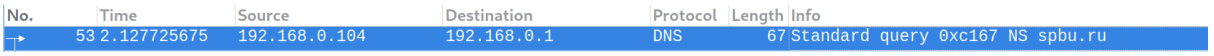
4.

```
Domain Name System (response)
    Transaction ID: 0xff6d
    Flags: 0x8580 Standard query response, No
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
    Queries
    Authoritative nameservers
```

Ответов нет.

Г. DNS-трассировка nslookup –type=NS (1 балл).

1.



Запрос отправлен на адрес 192.168.0.1, он совпадает с адресом локального DNS-сервера.

2.

```
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)
```

Запрашивается запись типа NS. Ответов в запросе не содержится.

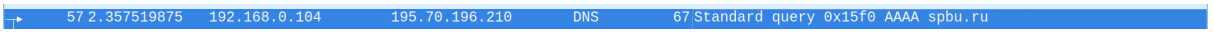
3.

```
Answers
    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: 8
        Name Server: ns.pu.ru
    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: 6
        Name Server: ns2.pu.ru
```

В ответах содержатся имена ns.pu.ru, ns2.pu.ru. Их IP-адресов в ответах нет.

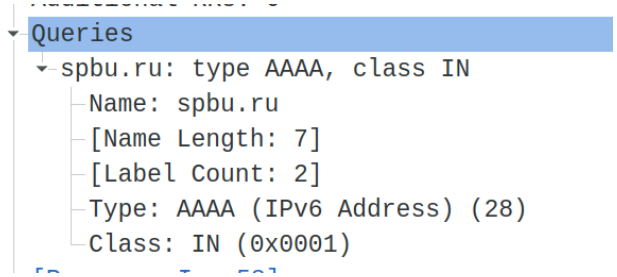
Д. DNS-трассировка nslookup www.spbu.ru ns2.pu.ru (1 балл).

1.

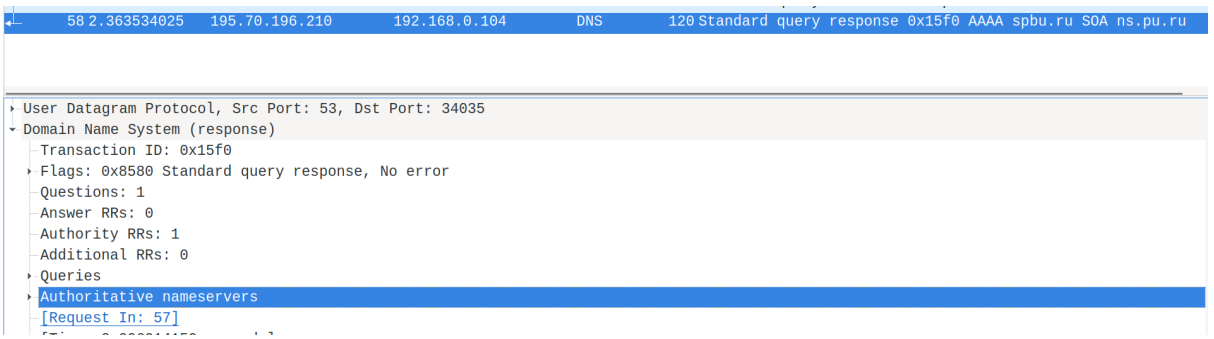


Запрос отправлен на адрес 195.70.196.210. Он не совпадает с адресом локального DNS-сервера, установленного по умолчанию.
Адрес принадлежит хосту ns2.pu.ru:

```
[dword@fedora ~]$ nslookup ns2.pu.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns2.pu.ru
Address: 195.70.196.210
```

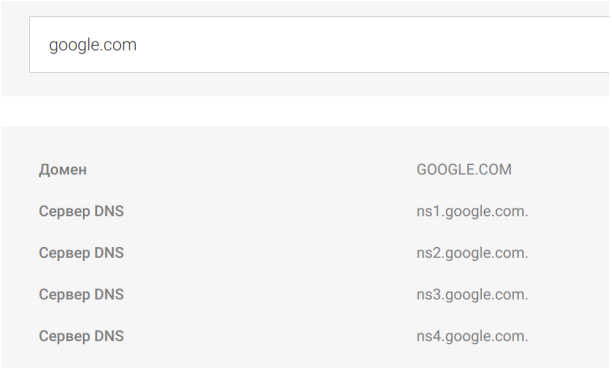
2. 
```
Queries
  spbu.ru: type AAAA, class IN
    Name: spbu.ru
    [Name Length: 7]
    [Label Count: 2]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
```

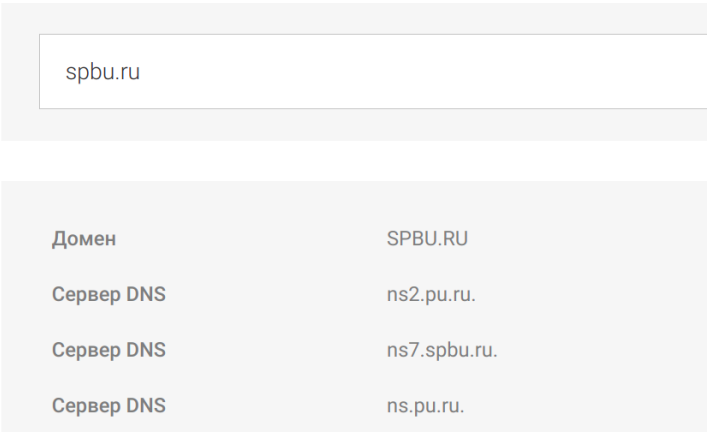
   Запрашивается запись типа AAAA. Ответов в запросе не содержится.

3. 
```
58 2.363534025   195.70.196.210   192.168.0.104   DNS   120 Standard query response 0x15f0 AAAA spbu.ru SOA ns.pu.ru

User Datagram Protocol, Src Port: 53, Dst Port: 34035
Domain Name System (response)
  Transaction ID: 0x15f0
  Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
  Queries
  Authoritative nameservers
  [Request In: 57]
```

   В ответном сообщении не содержится ни одного ответа.

E. Сервисы whois (2 балла).

1. WHOIS – это база данных, в которой хранятся сведения о доменах (контактные данные регистранта; дата создания и обновления домена, а также срок его регистрации; DNS-серверы и статус домена).
2. 



Использовался сервис https://2domains.ru/whois.

3.

```
[dword@fedora ~]$ nslookup 192.168.0.1
1.0.168.192.in-addr.arpa        name = _gateway.

[dword@fedora ~]$ nslookup ns1.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns1.google.com
Address: 216.239.32.10
Name:   ns1.google.com
Address: 2001:4860:4802:32::a

[dword@fedora ~]$ nslookup ns2.pu.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns2.pu.ru
Address: 195.70.196.210
```