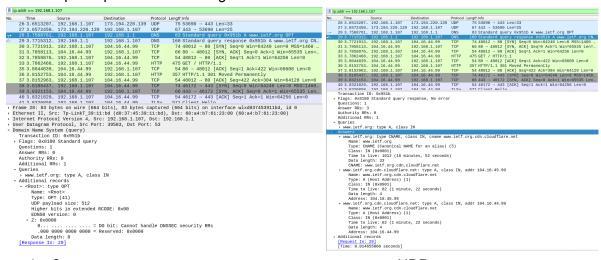
2. Wireshark. Работа с DNS

А. Утилита nslookup

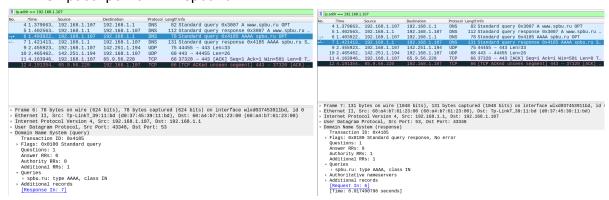
```
artser@eartser:~$ nslookup www.osaka-u.ac.jp
                               127.0.0.53
127.0.0.53#53
 Server:
Address:
 Non-authoritative answ
 Name: www.osaka-u.ac.jp
Address: 133.1.138.1
  cartser@eartser:-$ nslookup -type=ns ethz.ch
derver: 127.0.0.53
dddress: 127.0.0.53#53
Address:
  Non-authoritative answer:
 ethz.ch nameserver = ns1.ethz.ch.
ethz.ch nameserver = ns2.ethz.ch.
 Authoritative answers can be found from:
   artser@eartser:~$ nslookup www.thetimes.co.uk
erver: 127.0.0.53
ddress: 127.0.0.53#53
 Server:
Address:
Non-authoritative answer:
Name: www.thetimes.co.uk
Address: 143.204.98.117
Name: www.thetimes.co.uk
Address: 143.204.98.80
Name: www.thetimes.co.uk
Address: 143.204.98.78
Name: www.thetimes.co.uk
Address: 143.204.98.78
  artser@eartser:~$ nslookup spbu.ru
erver: 127.0.0.53
ddress: 127.0.0.53#53
 Non-authoritative answer:
 Name: spbu.ru
Address: 82.202.190.112
```

Б. DNS-трассировка www.ietf.org



- 1. Запрос и ответ отправлены с помощью протокола UDP.
- 2. Порт назначения запроса 53.
- 3. Запрос отправлен на IP-адрес 192.168.1.1, он совпадает с IP-адресом локального DNS сервера.
- 4. Запрашивается запись типа А, в запросе не содержатся ответы.
- 5. В ответном сообщении 3 ответа, в них содержатся CNAME и два IP-адреса.
- 6. IP-адрес назначения пакета с SYN соответствует второму полученному IP-адресу.
- 7. Хост не выполняет новых DNS-запросов перед загрузкой изображений.

B. DNS-трассировка www.spbu.ru

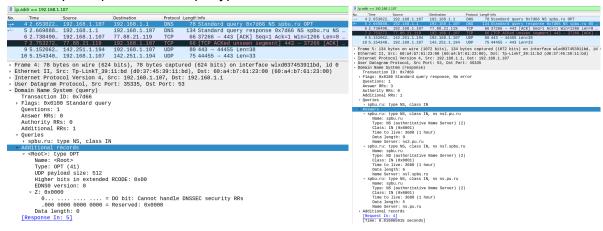


- 1. Порт назначения в DNS-запросе и порт источника в DNS-ответе 53.
- 2. Запрос отправлен на IP-адрес 192.168.1.1, он совпадает с IP-адресом локального DNS сервера.
- 3. Запрашивается запись типа АААА, в запросе не содержатся ответы.
- 4. В ответном сообщении нет ответов, но есть Authoritative nameservers, в котором содержится следующая информация:

```
Authoritative nameservers

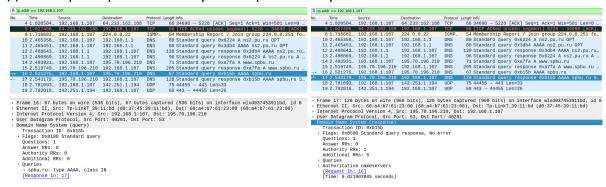
- spbu.ru: type SOA, class IN, mname ns.pu.ru
Name: spbu.ru
Type: SOA (Start Of a zone of Authority) (6)
class: IN (0x0001)
Time to live: 1416 (23 minutes, 36 seconds)
Data length: 41
Primary name server: ns.pu.ru
Responsible authority's mailbox: hostmaster.pu.ru
Serial Number: 2022012028
Refresh Interval: 7200 (2 hours)
Retry Interval: 3600 (1 hour)
Expire limit: 604800 (7 days)
Minimum TTL: 3600 (1 hour)
```

Г. DNS-трассировка nslookup –type=NS



- 1. Запрос отправлен на IP-адрес 192.168.1.1, он совпадает с IP-адресом локального DNS сервера.
- 2. Запрашивается запись типа NS, в запросе не содержатся ответы.
- 3. В ответах содержатся имена следующих DNS-серверов: ns2.pu.ru, ns7.spbu.ru, ns.pu.ru. Их адреса в ответе не содержатся.

Д. DNS-трассировка nslookup www.spbu.ru ns2.pu.ru



- 1. Запрос отправлен на IP-адрес 195.70.196.210, он не совпадает с IP-адресом локального DNS сервера, он принадлежит ns2.pu.ru.
- 2. Запрашивается запись типа АААА, в запросе не содержатся ответы.
- 3. В ответном сообщении нет ответов, но есть Authoritative nameservers, в котором содержится аналогичная заданию В информация.

E. Сервисы whois

whois – это база данных, в которой хранятся сведения о доменах. В ней можно найти следующую информацию:

- контактные данные регистранта, администратора и технических специалистов;
- сведения о спонсирующем регистраторе;
- дату создания и обновления домена, а также срок его регистрации;
- DNS-серверы и статус домена.

Для получения имен DNS-серверов я использовала whois сервис NS Lookup на dnschecker.org.

