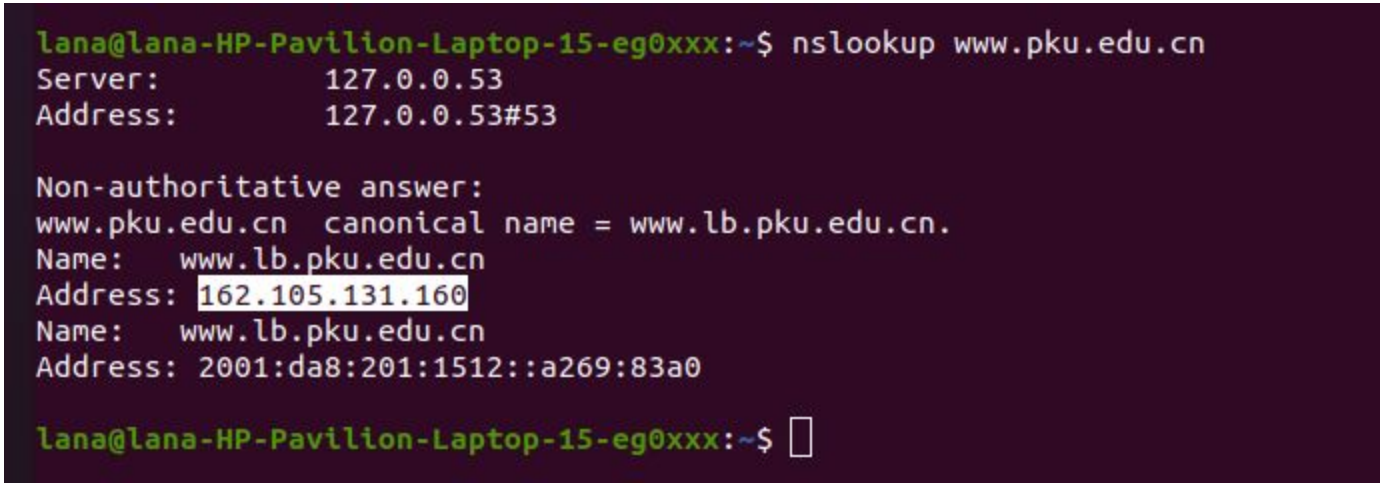
Лабораторная работа №4

Компьютерные сети

Утилита nslookup



IP адрес веб-сервера Пекинского университета: 162.105.131.160

```
lana@lana-HP-Pavilion-Laptop-15-eg0xxx:~$ nslookup -type=ns tum.de
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
tum.de  nameserver = dns1.lrz.de.
tum.de  nameserver = dns3.lrz.eu.
tum.de  nameserver = dns2.lrz.bayern.
```

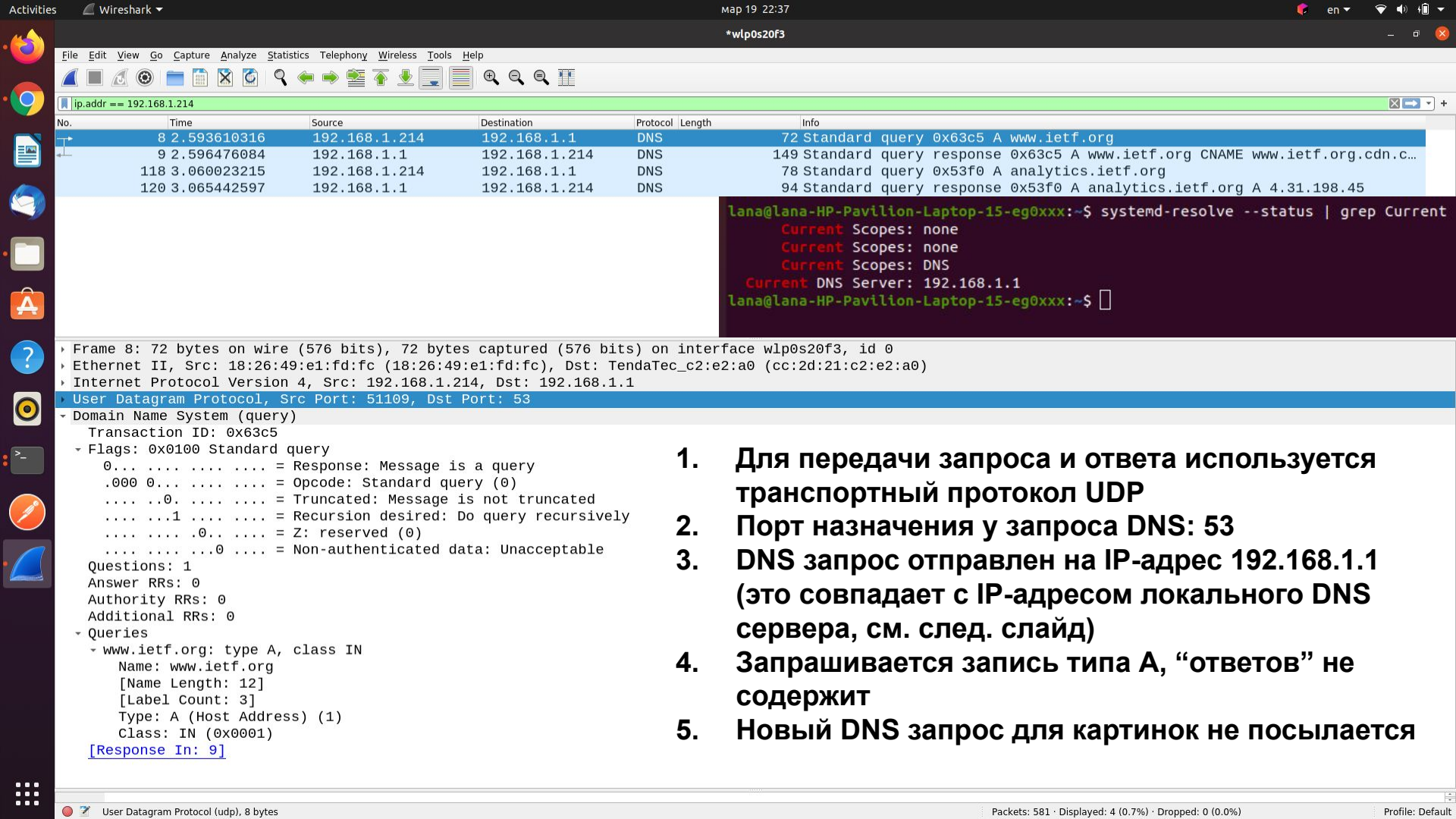
Для веб-сервера Мюнхенского технического университета были найдены 3 авторитетных DNS-сервера: dns1.lrz.de, dns3.lrz.eu, dns2.lrz.bayern

```
lana@lana-HP-Pavilion-Laptop-15-eg0xxx:~$ nslookup www.ox.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.ox.ac.uk
Address: 151.101.2.216
Name:   www.ox.ac.uk
Address: 151.101.194.216
Name:   www.ox.ac.uk
Address: 151.101.66.216
Name:   www.ox.ac.uk
Address: 151.101.130.216

lana@lana-HP-Pavilion-Laptop-15-eg0xxx:~$ nslookup www.spbu.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.spbu.ru     canonical name = spbu.ru.
Name:   spbu.ru
Address: 82.202.190.112

lana@lana-HP-Pavilion-Laptop-15-eg0xxx:~$
```

Веб-сервер Оксфордского университета имеет 4 IP-адреса.

Веб сервер СПбГУ имеет 1 IP-адрес

DNS-трассировка www.ietf.org



1. **Для передачи запроса и ответа используется транспортный протокол UDP**
2. **Порт назначения у запроса DNS: 53**
3. **DNS запрос отправлен на IP-адрес 192.168.1.1 (это совпадает с IP-адресом локального DNS сервера, см. след. слайд)**
4. **Запрашивается запись типа A, “ответов” не содержит**
5. **Новый DNS запрос для картинок не посылается**

ip.addr == 192.168.1.214

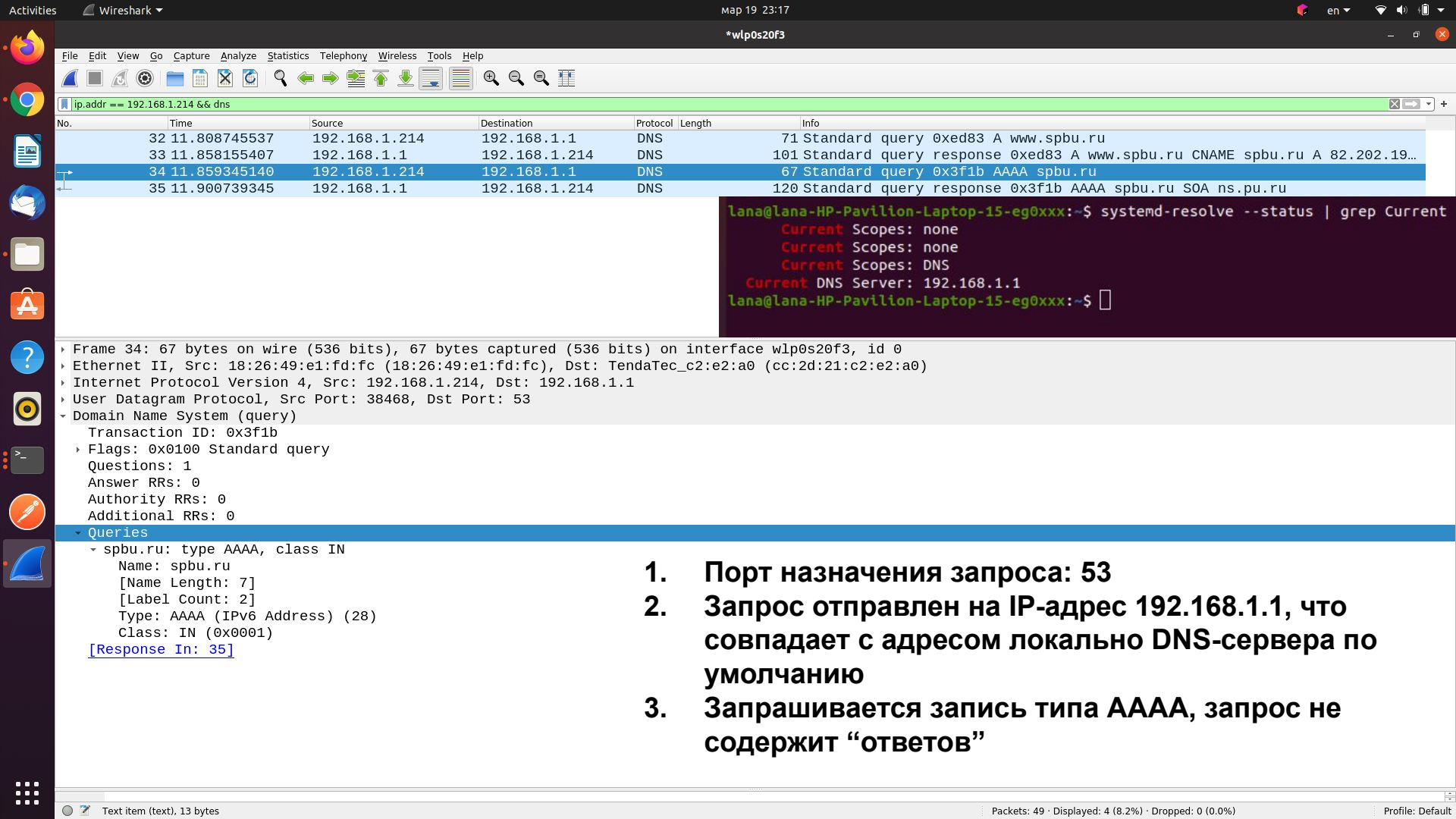
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.214	34.104.35.123	TCP	66	36822 → 80 [FIN, ACK] Seq=1 Ack=1 Win=12302 Len=0 TSval=4165591768 TSe…
2	0.064076869	192.168.1.214	64.233.165.94	TCP	66	40420 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=4127285529 TSecr=426…
3	0.110354698	64.233.165.94	192.168.1.214	TCP	66	[TCP ACKed unseen segment] 443 → 40420 [ACK] Seq=1 Ack=2 Win=265 Len=0…
7	2.584474855	192.168.1.214	64.233.165.103	UDP	1292	54062 → 443 Len=1250
8	2.593610316	192.168.1.214	192.168.1.1	DNS	72	Standard query 0x63c5 A www.ietf.org
9	2.596476084	192.168.1.1	192.168.1.214	DNS	149	Standard query response 0x63c5 A www.ietf.org CNAME www.ietf.org.cdn.c…
10	2.597152076	192.168.1.214	104.16.44.99	TCP	74	40620 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=390…
11	2.597202716	192.168.1.214	104.16.44.99	TCP	74	40624 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=390…
12	2.622021780	104.16.44.99	192.168.1.214	TCP	66	443 → 40620 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=…
13	2.622072050	192.168.1.214	104.16.44.99	TCP	54	40620 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
14	2.622022057	104.16.44.99	192.168.1.214	TCP	66	443 → 40624 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=…
15	2.622092321	192.168.1.214	104.16.44.99	TCP	54	40624 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0

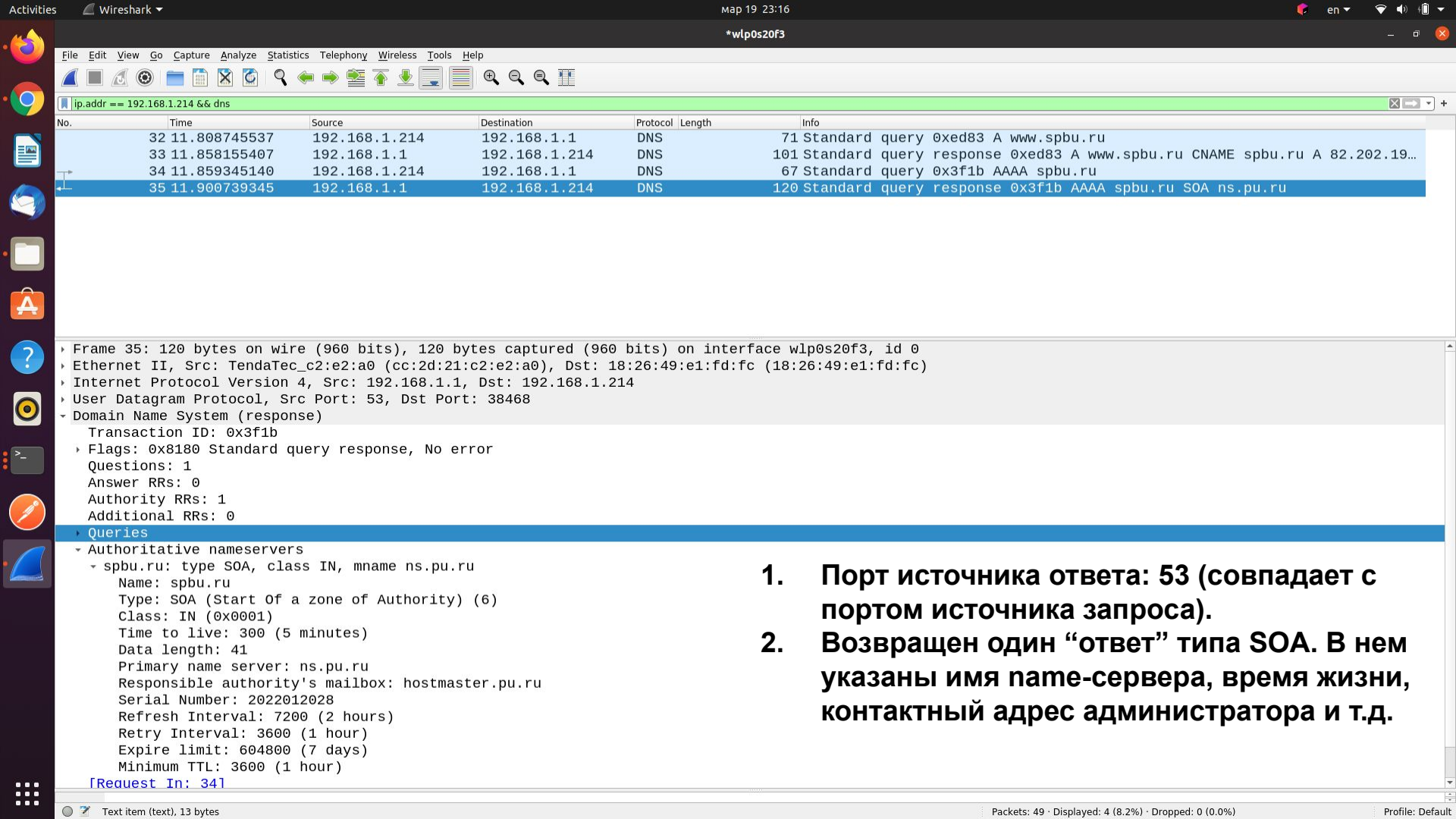
```
Additional RRs: 0
▸ Queries
▾ Answers
  ▾ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1430 (23 minutes, 50 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.44.99
  [Request In: 8]
  [Time: 0.002865768 seconds]
```

Вернулось 3 “ответа”.
Первый типа CNAME – каноническое имя www.ietf.org.cdn.cloudflare.name
Второй и третий типа A – два IP-адреса этого веб-сервера: 104.16.45.99 и 104.16.44.99

IP-адрес назначения следующего TCP-запроса с флагом SYN соответствует второму адресу, который вернул DNS-сервер.

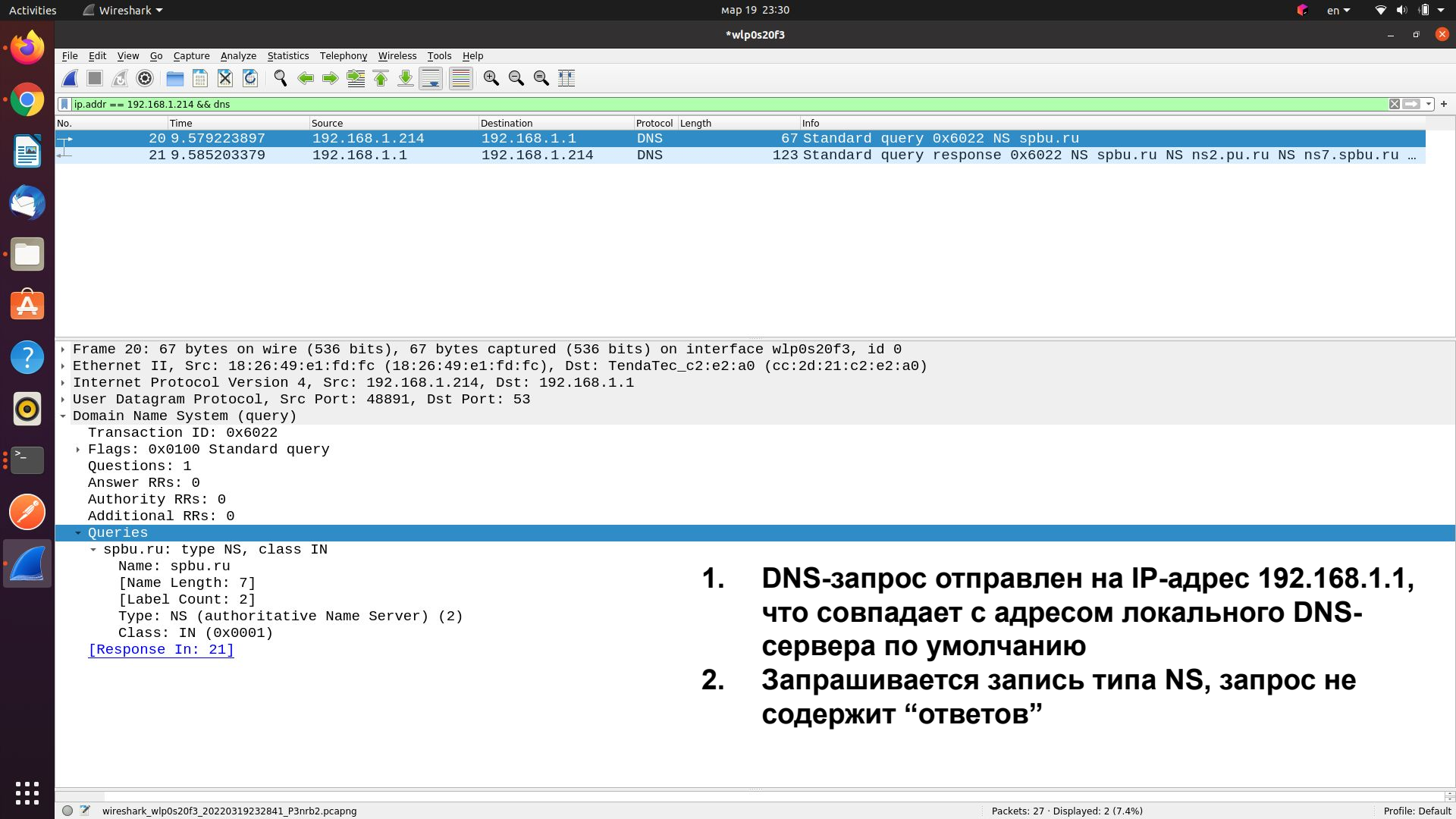
DNS-трассировка nslookup www.spbu.ru

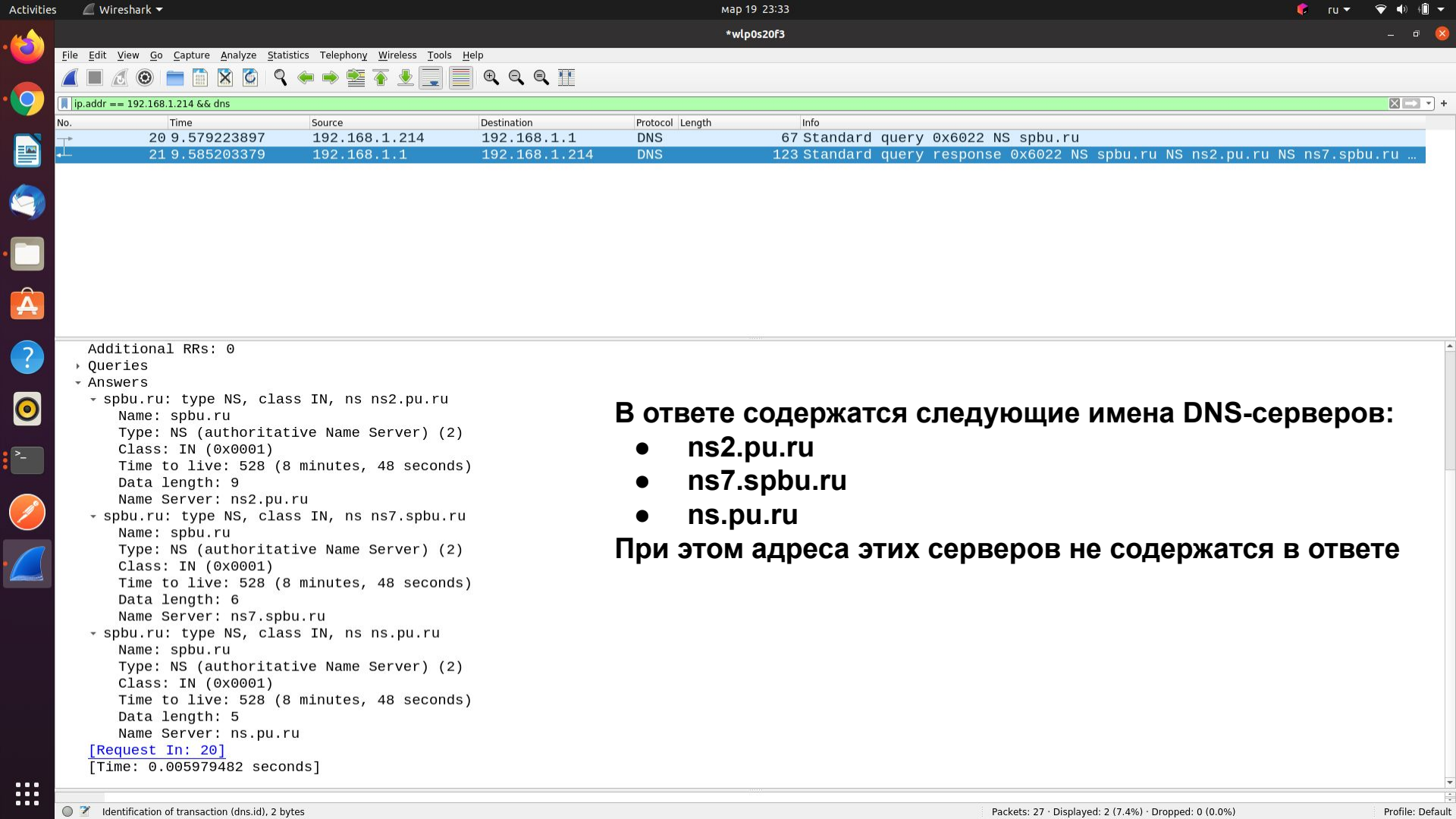

Activities
Wireshark
мар 19 23:17
en
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.214 && dns
No. Time Source Destination Protocol Length Info
32 11.808745537 192.168.1.214 192.168.1.1 DNS 71 Standard query 0xed83 A www.spbu.ru
33 11.858155407 192.168.1.1 192.168.1.214 DNS 101 Standard query response 0xed83 A www.spbu.ru CNAME spbu.ru A 82.202.19…
34 11.859345140 192.168.1.214 192.168.1.1 DNS 67 Standard query 0x3f1b AAAA spbu.ru
35 11.900739345 192.168.1.1 192.168.1.214 DNS 120 Standard query response 0x3f1b AAAA spbu.ru SOA ns.pu.ru
lana@lana-HP-Pavilion-Laptop-15-eg0xxx:~$ systemd-resolve --status | grep Current
Current Scopes: none
Current Scopes: none
Current Scopes: DNS
Current DNS Server: 192.168.1.1
lana@lana-HP-Pavilion-Laptop-15-eg0xxx:~$
Frame 34: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: 18:26:49:e1:fd:fc (18:26:49:e1:fd:fc), Dst: TendaTec_c2:e2:a0 (cc:2d:21:c2:e2:a0)
Internet Protocol Version 4, Src: 192.168.1.214, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 38468, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x3f1b
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
spbu.ru: type AAAA, class IN
Name: spbu.ru
[Name Length: 7]
[Label Count: 2]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 35]
1. Порт назначения запроса: 53
2. Запрос отправлен на IP-адрес 192.168.1.1, что совпадает с адресом локально DNS-сервера по умолчанию
3. Запрашивается запись типа AAAA, запрос не содержит “ответов”
Text item (text), 13 bytes
Packets: 49 · Displayed: 4 (8.2%) · Dropped: 0 (0.0%)
Profile: Default



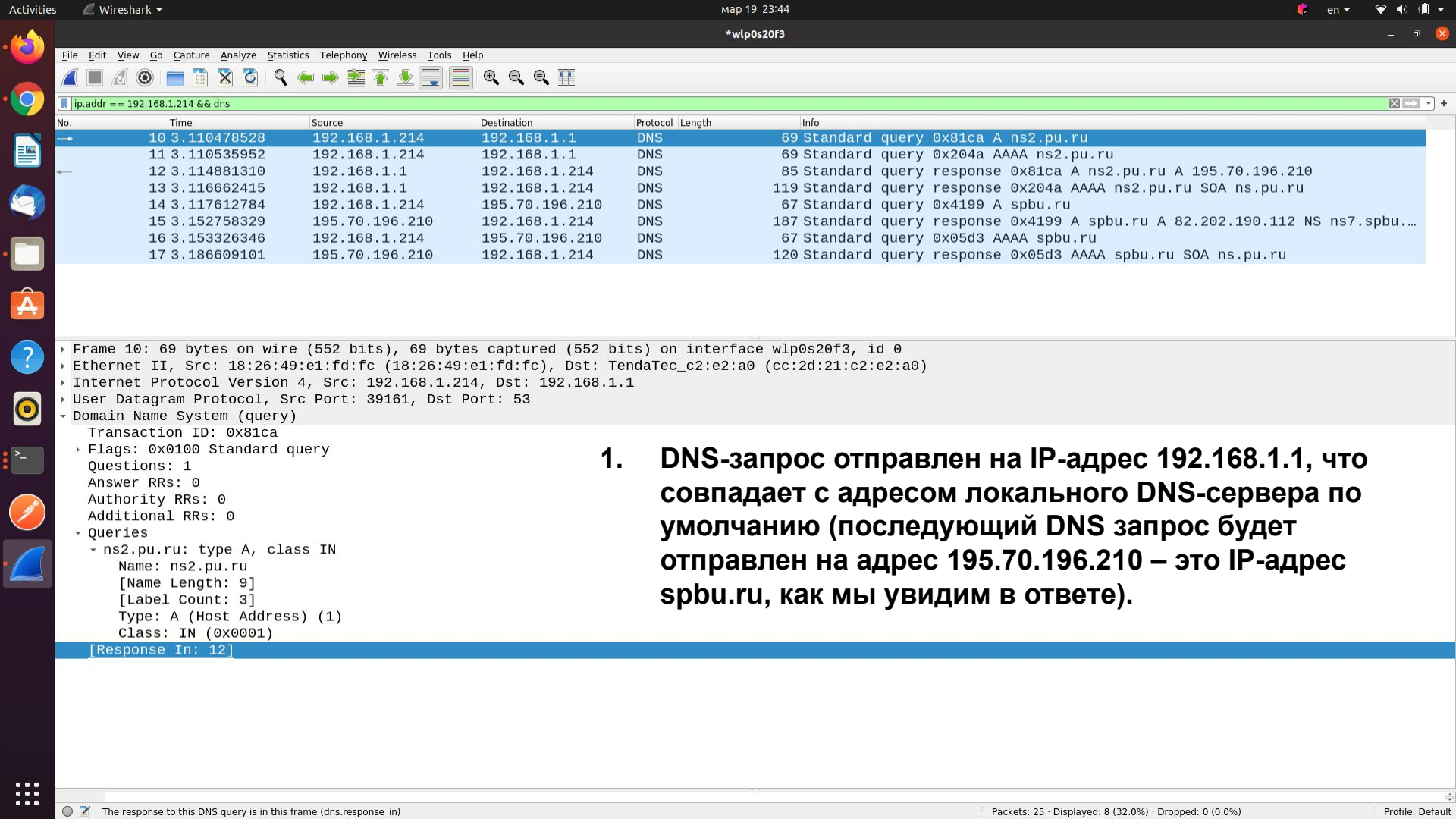
1. **Порт источника ответа: 53 (совпадает с портом источника запроса).**
2. **Возвращен один “ответ” типа SOA. В нем указаны имя name-сервера, время жизни, контактный адрес администратора и т.д.**

DNS-трассировка nslookup –type=NS spbu.ru

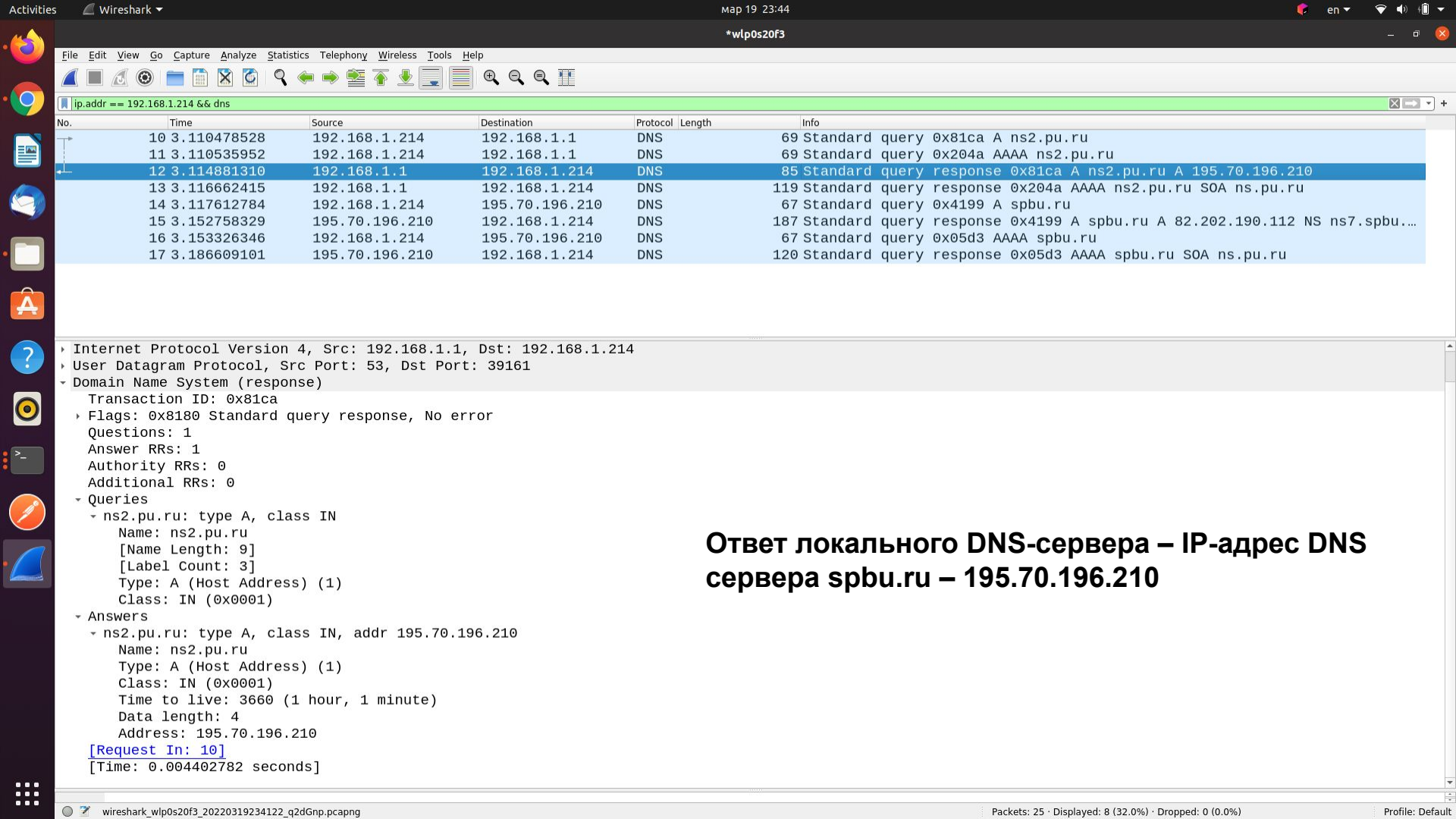

Activities
Wireshark
мар 19 23:30
en
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.214 && dns
No. Time Source Destination Protocol Length Info
20 9.579223897 192.168.1.214 192.168.1.1 DNS 67 Standard query 0x6022 NS spbu.ru
21 9.585203379 192.168.1.1 192.168.1.214 DNS 123 Standard query response 0x6022 NS spbu.ru NS ns2.pu.ru NS ns7.spbu.ru …
Frame 20: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: 18:26:49:e1:fd:fc (18:26:49:e1:fd:fc), Dst: TendaTec_c2:e2:a0 (cc:2d:21:c2:e2:a0)
Internet Protocol Version 4, Src: 192.168.1.214, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 48891, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x6022
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: 21]
1. DNS-запрос отправлен на IP-адрес 192.168.1.1, что совпадает с адресом локального DNS-сервера по умолчанию
2. Запрашивается запись типа NS, запрос не содержит “ответов”
wireshark_wlp0s20f3_20220319232841_P3nrb2.pcapng
Packets: 27 · Displayed: 2 (7.4%)
Profile: Default

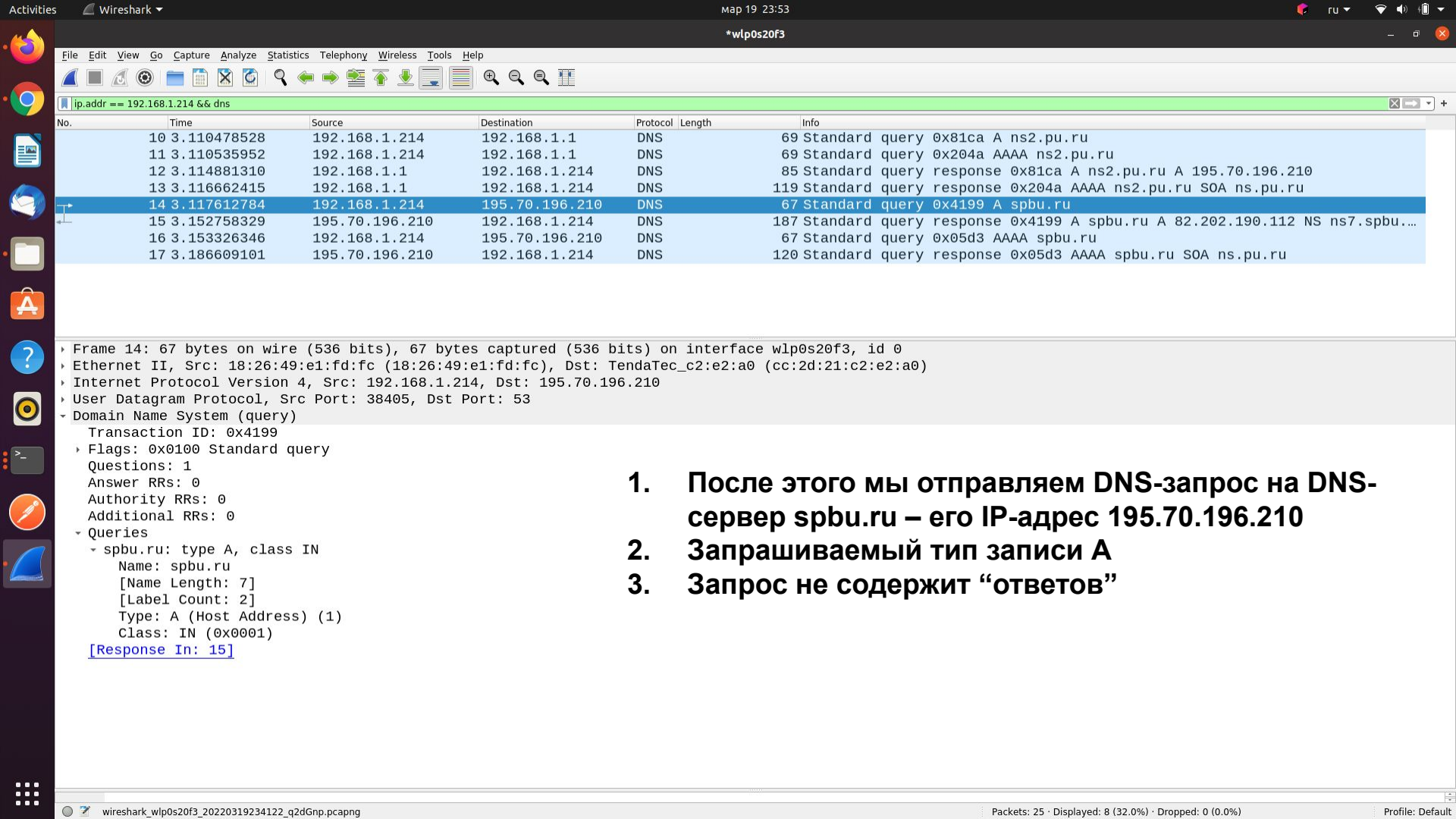

Activities
Wireshark
мар 19 23:33
ru
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.214 && dns
No. Time Source Destination Protocol Length Info
20 9.579223897 192.168.1.214 192.168.1.1 DNS 67 Standard query 0x6022 NS spbu.ru
21 9.585203379 192.168.1.1 192.168.1.214 DNS 123 Standard query response 0x6022 NS spbu.ru NS ns2.pu.ru NS ns7.spbu.ru …
Additional RRs: 0
Queries
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: 528 (8 minutes, 48 seconds)
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: 528 (8 minutes, 48 seconds)
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: 528 (8 minutes, 48 seconds)
Data length: 5
Name Server: ns.pu.ru
[Request In: 20]
[Time: 0.005979482 seconds]
В ответе содержатся следующие имена DNS-серверов:
ns2.pu.ru
ns7.spbu.ru
ns.pu.ru
При этом адреса этих серверов не содержатся в ответе
Identification of transaction (dns.id), 2 bytes
Packets: 27 · Displayed: 2 (7.4%) · Dropped: 0 (0.0%)
Profile: Default

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



1. **DNS-запрос отправлен на IP-адрес 192.168.1.1, что совпадает с адресом локального DNS-сервера по умолчанию (последующий DNS запрос будет отправлен на адрес 195.70.196.210 – это IP-адрес spbu.ru, как мы увидим в ответе).**


Activities
Wireshark
мар 19 23:44
en
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.214 && dns
No. Time Source Destination Protocol Length Info
10 3.110478528 192.168.1.214 192.168.1.1 DNS 69 Standard query 0x81ca A ns2.pu.ru
11 3.110535952 192.168.1.214 192.168.1.1 DNS 69 Standard query 0x204a AAAA ns2.pu.ru
12 3.114881310 192.168.1.1 192.168.1.214 DNS 85 Standard query response 0x81ca A ns2.pu.ru A 195.70.196.210
13 3.116662415 192.168.1.1 192.168.1.214 DNS 119 Standard query response 0x204a AAAA ns2.pu.ru SOA ns.pu.ru
14 3.117612784 192.168.1.214 195.70.196.210 DNS 67 Standard query 0x4199 A spbu.ru
15 3.152758329 195.70.196.210 192.168.1.214 DNS 187 Standard query response 0x4199 A spbu.ru A 82.202.190.112 NS ns7.spbu.…
16 3.153326346 192.168.1.214 195.70.196.210 DNS 67 Standard query 0x05d3 AAAA spbu.ru
17 3.186609101 195.70.196.210 192.168.1.214 DNS 120 Standard query response 0x05d3 AAAA spbu.ru SOA ns.pu.ru
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.214
User Datagram Protocol, Src Port: 53, Dst Port: 39161
Domain Name System (response)
Transaction ID: 0x81ca
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
ns2.pu.ru: type A, class IN
Name: ns2.pu.ru
[Name Length: 9]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
ns2.pu.ru: type A, class IN, addr 195.70.196.210
Name: ns2.pu.ru
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 3660 (1 hour, 1 minute)
Data length: 4
Address: 195.70.196.210
[Request In: 10]
[Time: 0.004402782 seconds]
Ответ локального DNS-сервера – IP-адрес DNS сервера spbu.ru – 195.70.196.210
wireshark_wlp0s20f3_20220319234122_q2dGnp.pcapng
Packets: 25 · Displayed: 8 (32.0%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Wireshark
мар 19 23:53
ru
*wlp0s20f3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.214 && dns
No. Time Source Destination Protocol Length Info
10 3.110478528 192.168.1.214 192.168.1.1 DNS 69 Standard query 0x81ca A ns2.pu.ru
11 3.110535952 192.168.1.214 192.168.1.1 DNS 69 Standard query 0x204a AAAA ns2.pu.ru
12 3.114881310 192.168.1.1 192.168.1.214 DNS 85 Standard query response 0x81ca A ns2.pu.ru A 195.70.196.210
13 3.116662415 192.168.1.1 192.168.1.214 DNS 119 Standard query response 0x204a AAAA ns2.pu.ru SOA ns.pu.ru
14 3.117612784 192.168.1.214 195.70.196.210 DNS 67 Standard query 0x4199 A spbu.ru
15 3.152758329 195.70.196.210 192.168.1.214 DNS 187 Standard query response 0x4199 A spbu.ru A 82.202.190.112 NS ns7.spbu.…
16 3.153326346 192.168.1.214 195.70.196.210 DNS 67 Standard query 0x05d3 AAAA spbu.ru
17 3.186609101 195.70.196.210 192.168.1.214 DNS 120 Standard query response 0x05d3 AAAA spbu.ru SOA ns.pu.ru
Frame 14: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: 18:26:49:e1:fd:fc (18:26:49:e1:fd:fc), Dst: TendaTec_c2:e2:a0 (cc:2d:21:c2:e2:a0)
Internet Protocol Version 4, Src: 192.168.1.214, Dst: 195.70.196.210
User Datagram Protocol, Src Port: 38405, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x4199
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
spbu.ru: type A, class IN
Name: spbu.ru
[Name Length: 7]
[Label Count: 2]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 15]
1. После этого мы отправляем DNS-запрос на DNS-сервер spbu.ru – его IP-адрес 195.70.196.210
2. Запрашиваемый тип записи A
3. Запрос не содержит “ответов”
wireshark_wlp0s20f3_20220319234122_q2dGnp.pcapng
Packets: 25 · Displayed: 8 (32.0%) · Dropped: 0 (0.0%)
Profile: Default

ip.addr == 192.168.1.214 && dns

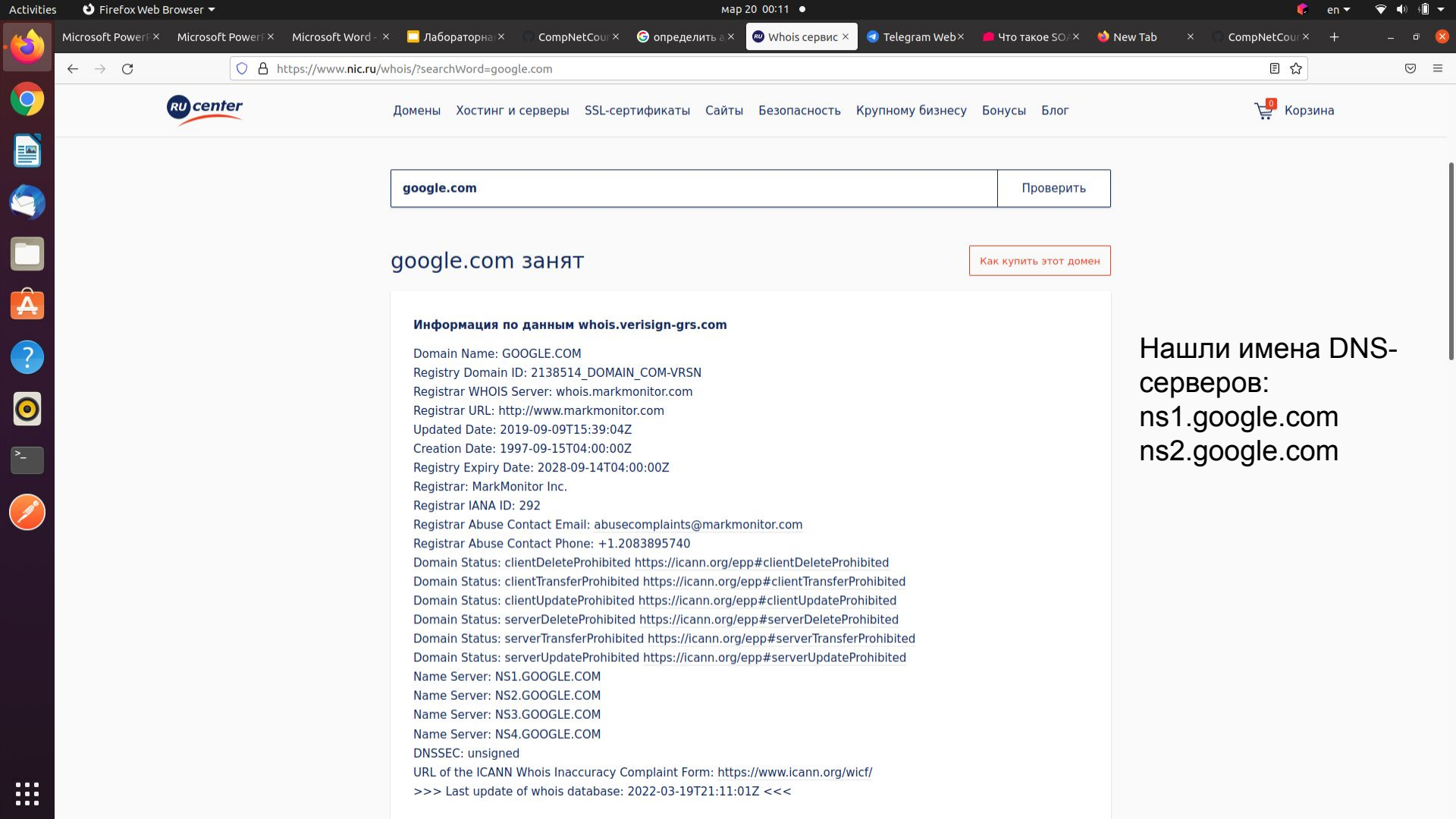
```
Answers
  spbu.ru: type A, class IN, addr 82.202.190.112
      Name: spbu.ru
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 3600 (1 hour)
      Data length: 4
      Address: 82.202.190.112
Authoritative nameservers
  spbu.ru: type NS, class IN, ns ns7.spbu.ru
      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: 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
Additional records
  ns.pu.ru: type A, class IN, addr 195.70.196.219
      Name: ns.pu.ru
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 3660 (1 hour, 1 minute)
      Data length: 4
      Address: 195.70.196.219
  ns2.pu.ru: type A, class IN, addr 195.70.196.210
      Name: ns2.pu.ru
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 3660 (1 hour, 1 minute)
      Data length: 4
      Address: 195.70.196.210
  ns7.spbu.ru: type A, class IN, addr 185.44.15.195
      Name: ns7.spbu.ru
      Type: A (Host Address) (1)
```

Ответное сообщение DNS-сервера содержит IP-адрес spbu.ru

Также вернулась дополнительная информация, а именно: все авторитетные DNS-серверы для spbu.ru с IP-адресами

WHOIS

WHOIS — сетевой протокол прикладного уровня, основным применением которого является получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем.


Activities
Firefox Web Browser
мар 20 00:11
en
Microsoft Power
Microsoft Power
Microsoft Word -
Лабораторна
CompNetCour
определить а
Whois сервис
Telegram Web
Что такое SO
New Tab
CompNetCour
https://www.nic.ru/whois/?searchWord=google.com
RU center
Домены
Хостинг и серверы
SSL-сертификаты
Сайты
Безопасность
Крупному бизнесу
Бонусы
Блог
Корзина
google.com
Проверить
google.com занят
Как купить этот домен
Информация по данным whois.verisign-grs.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-03-19T21:11:01Z <<<
Нашли имена DNS-серверов:
ns1.google.com
ns2.google.com

```
lana@lana-HP-Pavilion-Laptop-15-eg0xxx:~$ nslookup google.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   google.com
Address: 173.194.222.100
Name:   google.com
Address: 173.194.222.113
Name:   google.com
Address: 173.194.222.102
Name:   google.com
Address: 173.194.222.139
Name:   google.com
Address: 173.194.222.138
Name:   google.com
Address: 173.194.222.101
Name:   google.com
Address: 2a00:1450:4010:c0b::8a
Name:   google.com
Address: 2a00:1450:4010:c0b::64
Name:   google.com
Address: 2a00:1450:4010:c0b::66
Name:   google.com
Address: 2a00:1450:4010:c0b::71

lana@lana-HP-Pavilion-Laptop-15-eg0xxx:~$ nslookup google.com ns2.google.com
Server:         ns2.google.com
Address:        216.239.34.10#53

Name:   google.com
Address: 173.194.222.102
Name:   google.com
Address: 173.194.222.113
Name:   google.com
Address: 173.194.222.139
Name:   google.com
Address: 173.194.222.101
Name:   google.com
Address: 173.194.222.100
Name:   google.com
Address: 173.194.222.138
Name:   google.com
Address: 2a00:1450:4010:c0b::65
Name:   google.com
Address: 2a00:1450:4010:c0b::66
Name:   google.com
Address: 2a00:1450:4010:c0b::8a
Name:   google.com
Address: 2a00:1450:4010:c0b::71
```