Практическая работа №2

БАСО-03-20

intitle:"qwerty" inurl:http after:20

google.com/search?rlz=1C1AVFC_enRU918RU918&ei=iuhoX5nFJeeFrwSJ5KmACw&q=intitle%3A"qwerty"+inurl%3Ahttp+after%3A2019

Google

intitle:"qwerty" inurl:http after:2019

Все Картинки Новости Видео Покупки Ещё Настройки Инструменты

Результатов: примерно 1 130 (0,71 сек.)

lurkmore.to › QWERTY

QWERTY — Lurkmore

22 июл. 2020 г. - qwerty — обозначение одной из латинских раскладок, используемой для английского языка. Сочетание клавиш, идущих друг за другом ...

qwerty.kg

QWERTY.KG — IT полезности

Made in KG · Интересное · О железе · Apple · Ноутбуки · Смартфоны · Полезное · О софте · Разное · СОФТ · Android · Apple · Windows · Unix / Linux.

qwerty.kg › Интересное › Разное

Смартфоны — QWERTY.KG

Недавно некоторые пользователи пожаловались на форумах Reddit и Google, что задняя панель их смартфона Pixel 4 XL отслоилась от корпуса без ...

vroom.uz › site › away › url=http: › qwerty

Qwerty.uz создание и продвижение сайтов, мобильных ...

Веб-студия QWERTY в Ташкенте, разработка сайтов Ташкент, мобильное приложение Ташкенте, smm продвижение в Ташкенте, разработка ...

www.роутердлядома.рф › QWERTY_prov

Wifi роутеры для QWERTY

LinkSys E900 подойдет людям, которые не стремятся за скоростью интернета, но и хотят что бы интер.. 4090.00P. На основе 8 отзывов. Zyxel Keenetic ...

www.vremyan.ru › news ›

«qwerty», «12345» и «йцукен»: названы пароли, которые ...

17 янв. 2020 г. - Главные новости. Политика, экономика, общество, культура, спорт, губерния, происшествия. Комментарии, интервью, персоны.

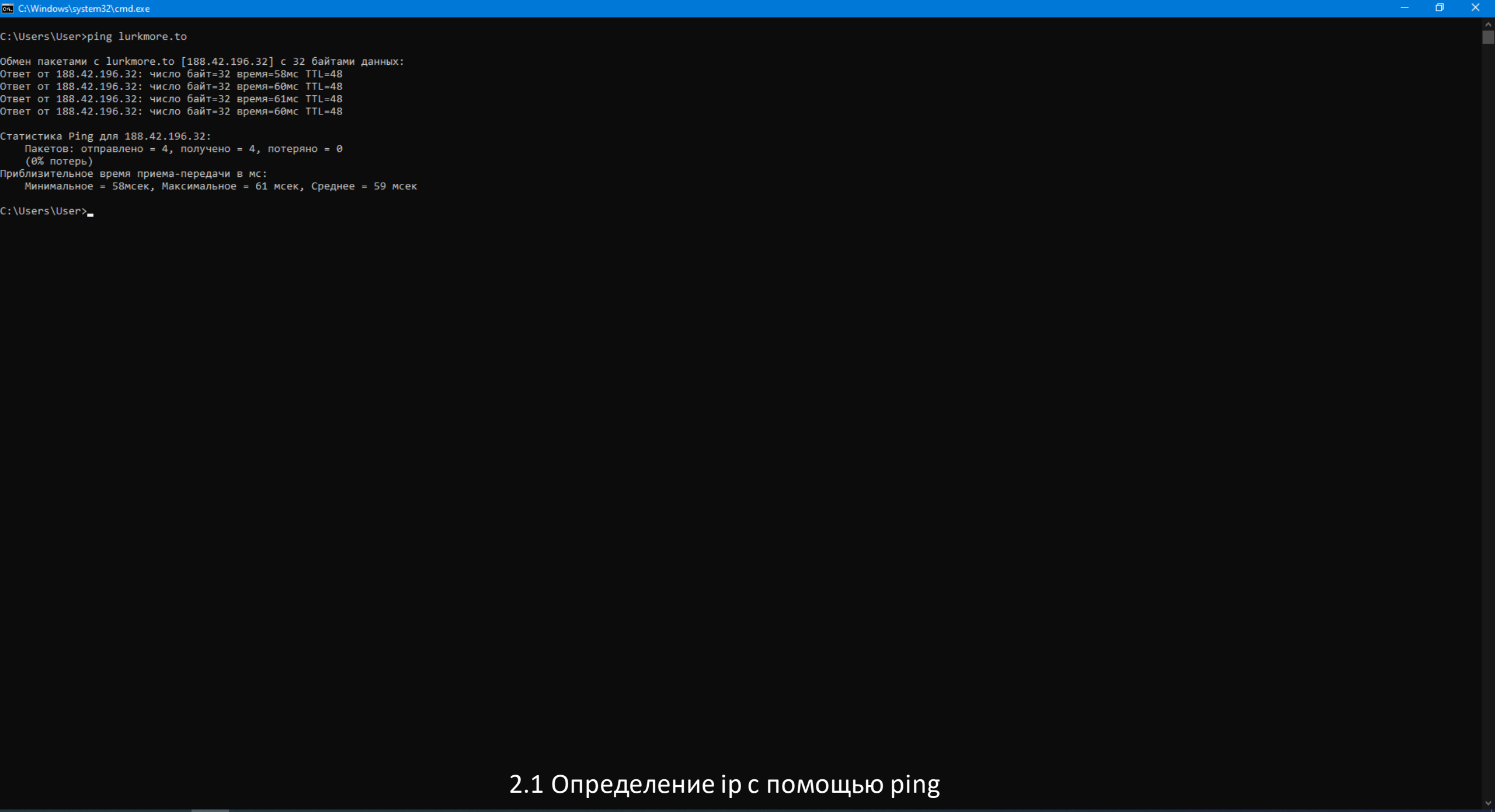
qe.se Перевести эту страницу

qwerty elektronik ab | Marine Navigation Interfaces

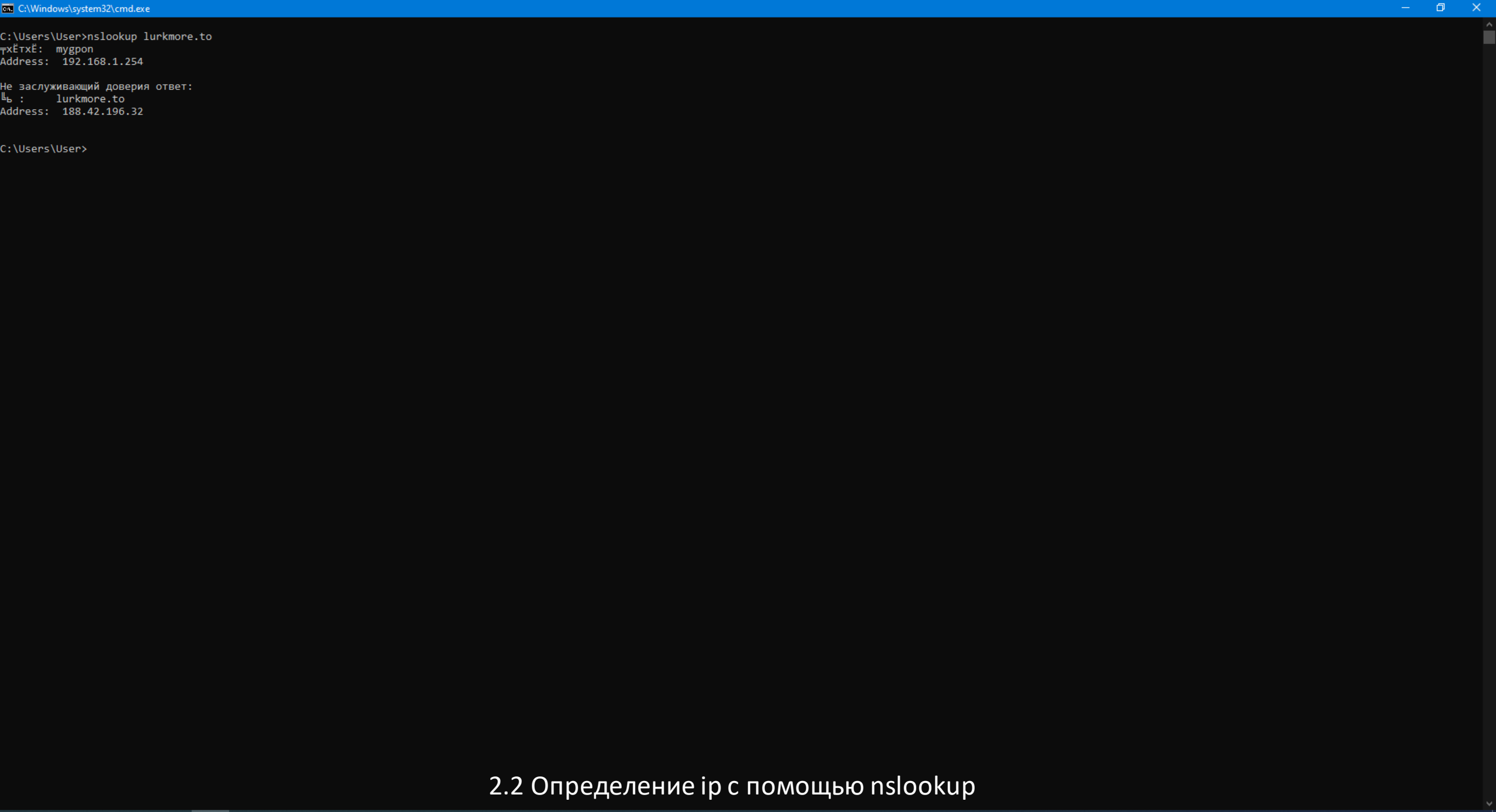
1. Обнаружен узел, работающий по http

lurkmore.to/QWERTY

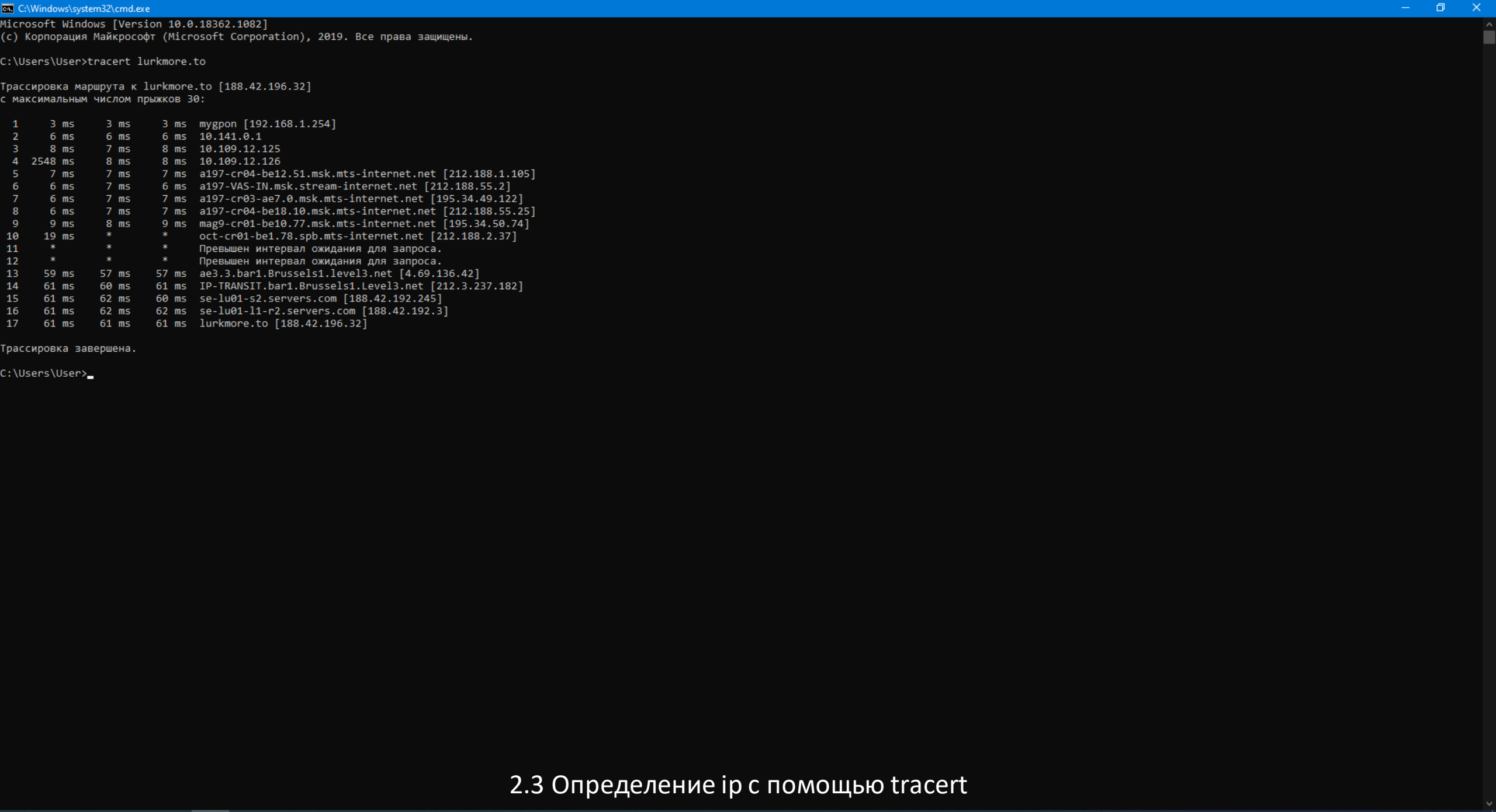
РУС 20:56 21.09.2020



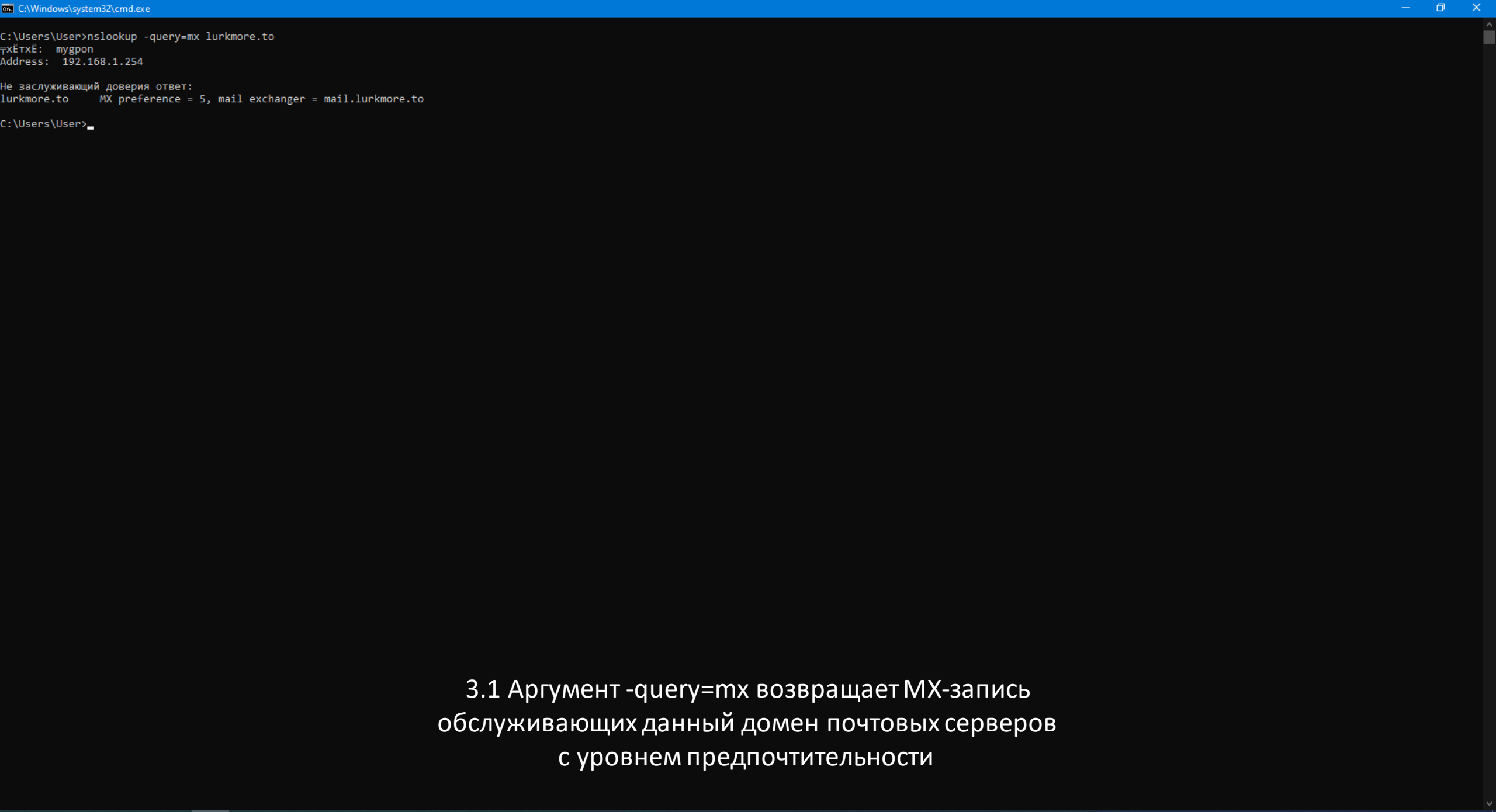
2.1 Определение ip с помощью ping



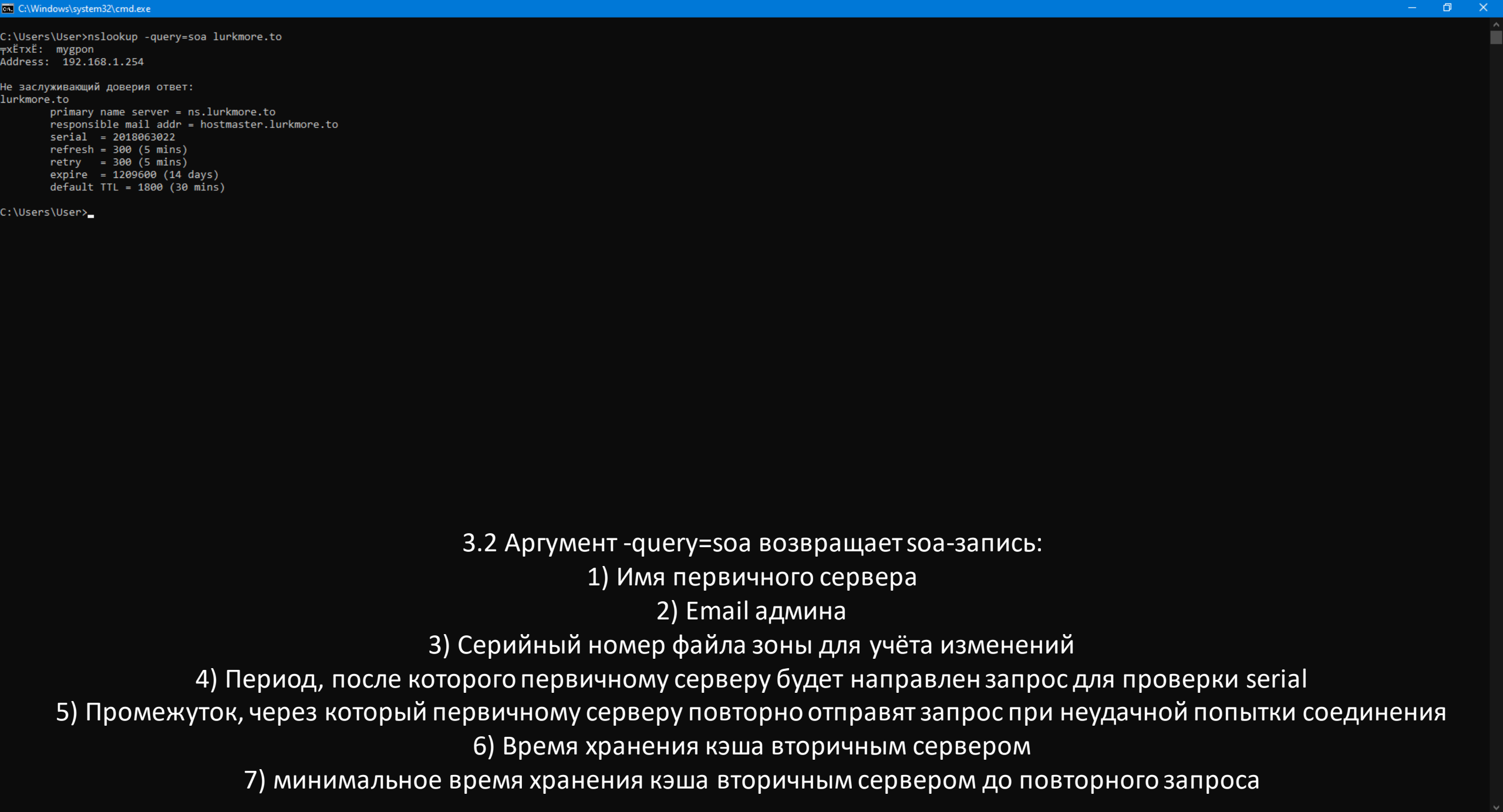
2.2 Определение ip с помощью nslookup



2.3 Определение ip с помощью tracert



3.1 Аргумент -query=mx возвращает MX-запись обслуживающих данный домен почтовых серверов с уровнем предпочтительности



3.2 Аргумент -query=soa возвращает soa-запись:

1) Имя первичного сервера

2) Email админа

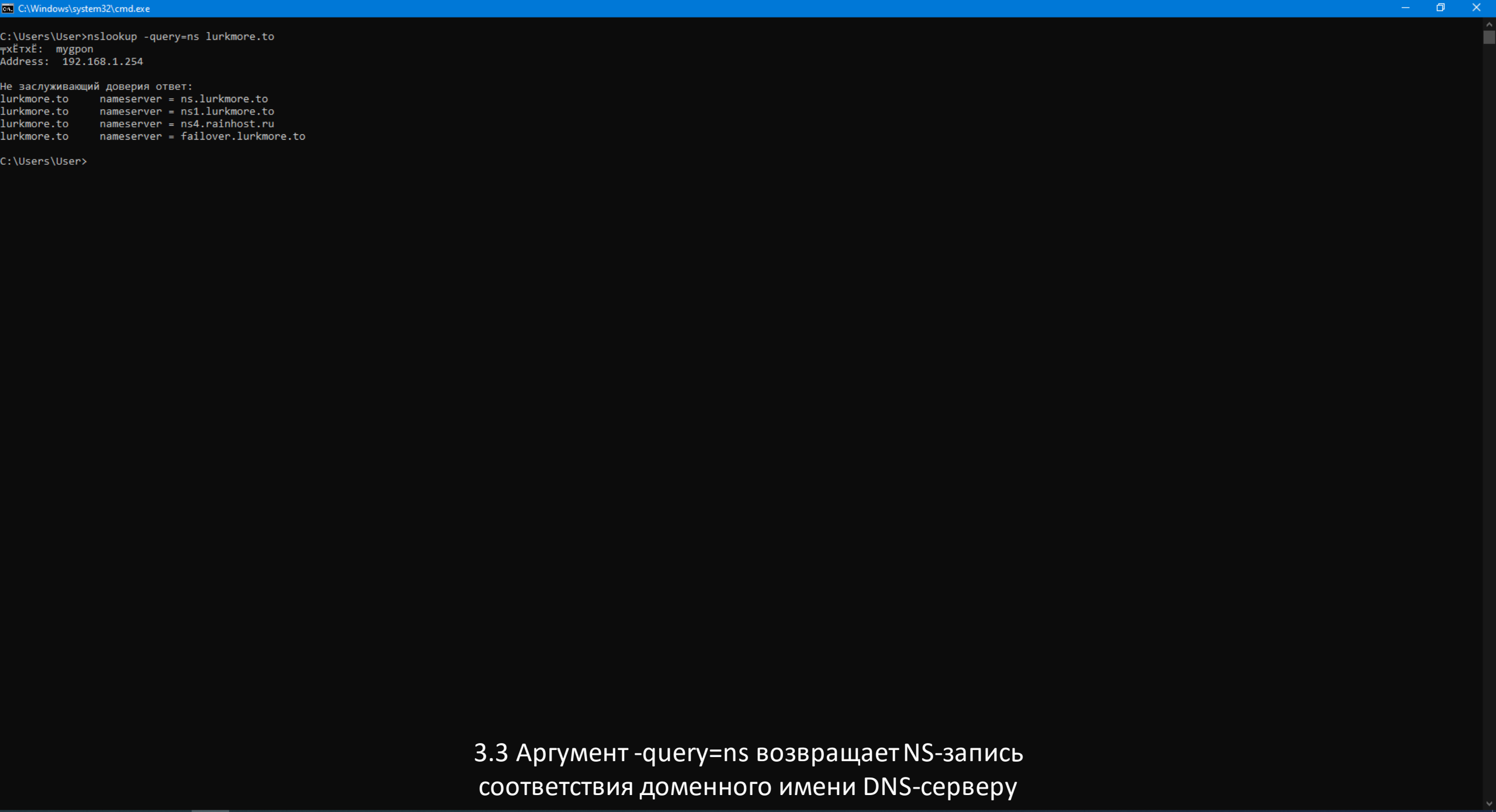
3) Серийный номер файла зоны для учёта изменений

4) Период, после которого первичному серверу будет направлен запрос для проверки serial

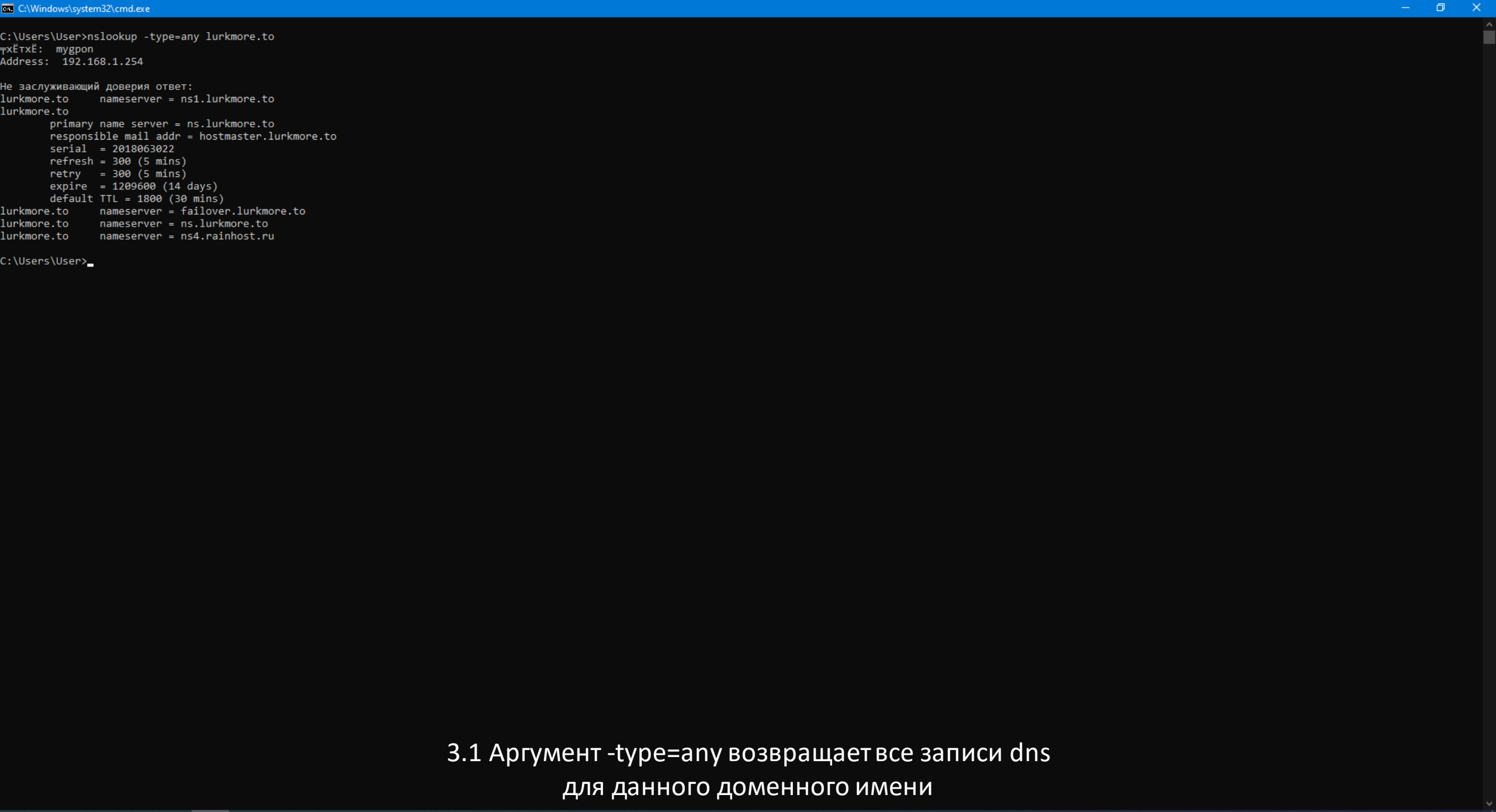
5) Промежуток, через который первичному серверу повторно отправят запрос при неудачной попытки соединения

6) Время хранения кэша вторичным сервером

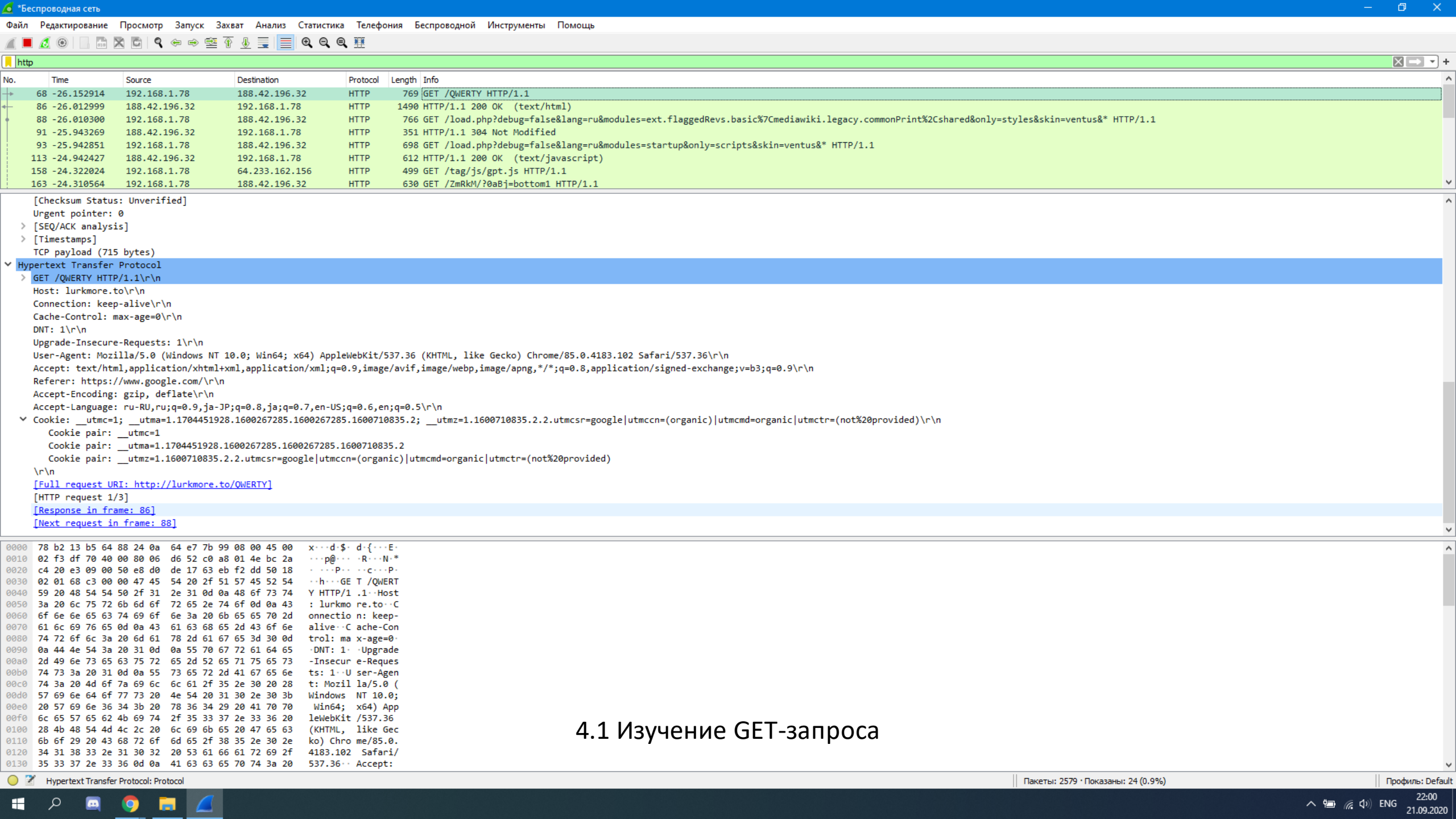
7) минимальное время хранения кэша вторичным сервером до повторного запроса

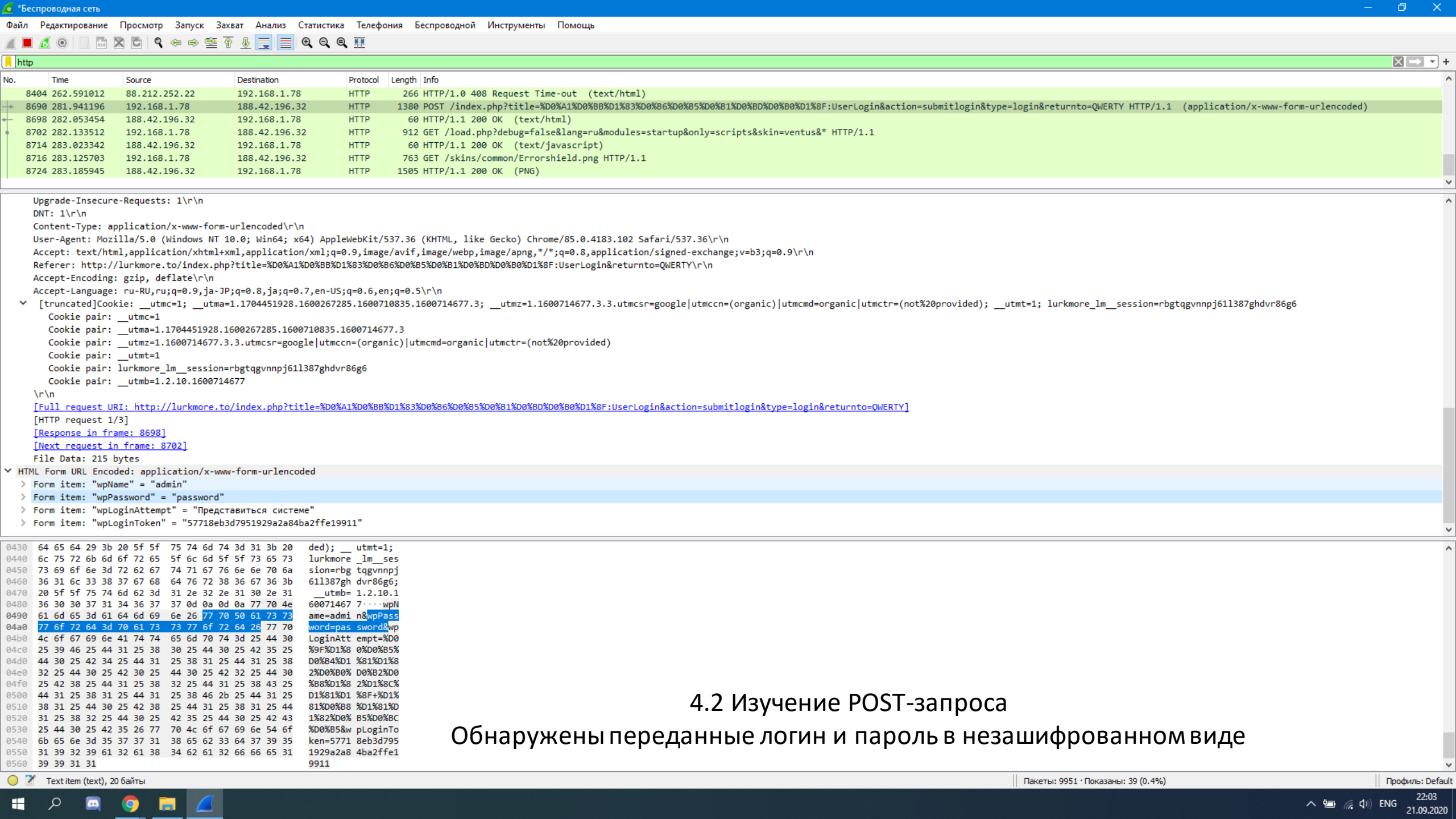


3.3 Аргумент -query=ns возвращает NS-запись соответствия доменного имени DNS-серверу



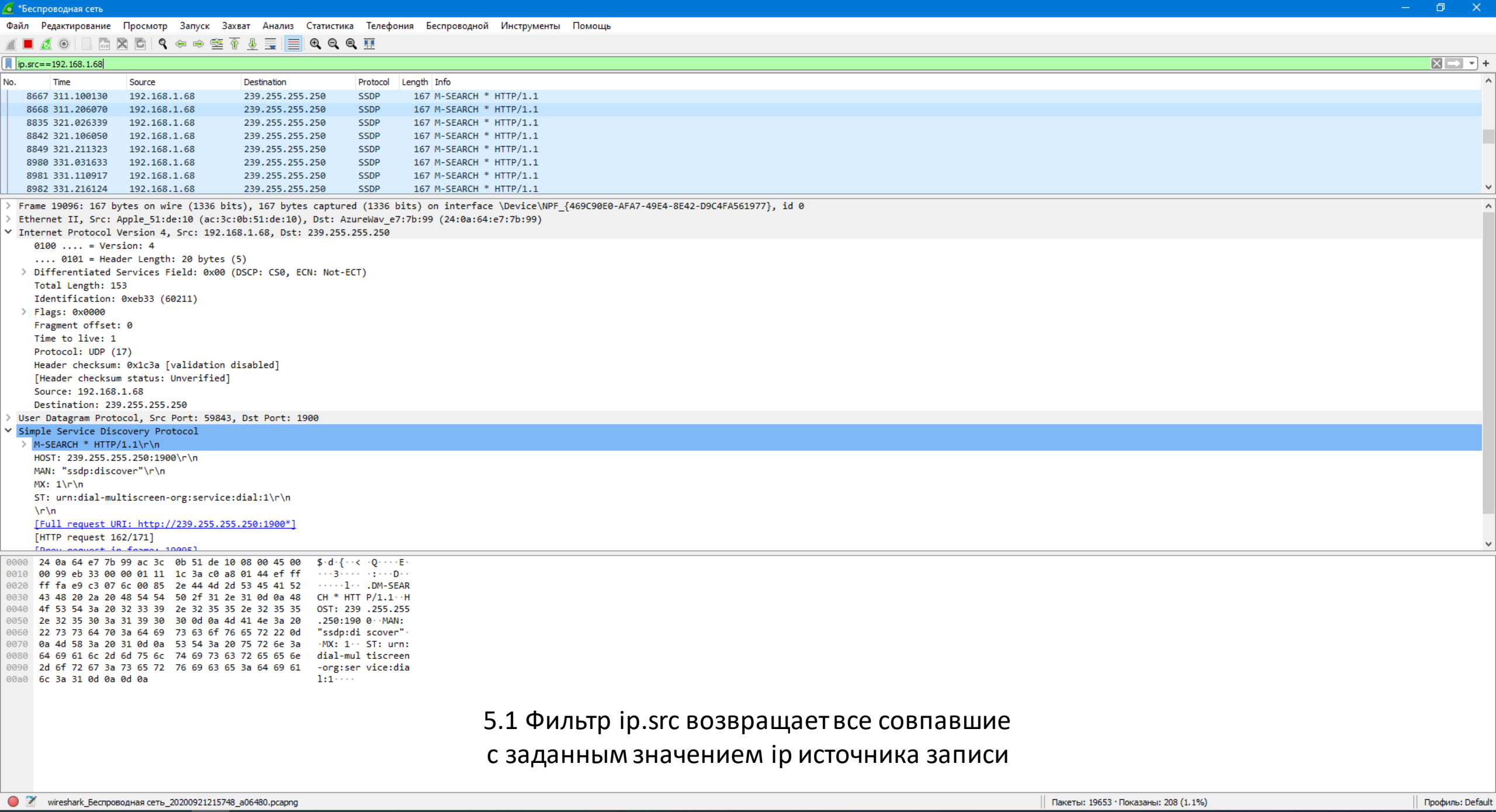
3.1 Аргумент -type=any возвращает все записи dns для данного доменного имени


*Беспроводная сеть
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
http
No. Time Source Destination Protocol Length Info
68 -26.152914 192.168.1.78 188.42.196.32 HTTP 769 GET /QWERTY HTTP/1.1
86 -26.012999 188.42.196.32 192.168.1.78 HTTP 1490 HTTP/1.1 200 OK (text/html)
88 -26.010300 192.168.1.78 188.42.196.32 HTTP 766 GET /load.php?debug=false&lang=ru&modules=ext.flaggedRevs.basic%7Cmediawiki.legacy.commonPrint%2Cshared&only=styles&skin=ventus&* HTTP/1.1
91 -25.943269 188.42.196.32 192.168.1.78 HTTP 351 HTTP/1.1 304 Not Modified
93 -25.942851 192.168.1.78 188.42.196.32 HTTP 698 GET /load.php?debug=false&lang=ru&modules=startup&only=scripts&skin=ventus&* HTTP/1.1
113 -24.942427 188.42.196.32 192.168.1.78 HTTP 612 HTTP/1.1 200 OK (text/javascript)
158 -24.322024 192.168.1.78 64.233.162.156 HTTP 499 GET /tag/js/gpt.js HTTP/1.1
163 -24.310564 192.168.1.78 188.42.196.32 HTTP 630 GET /ZmRkM/?0aBj=bottom1 HTTP/1.1
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (715 bytes)
Hypertext Transfer Protocol
GET /QWERTY HTTP/1.1\r\n
Host: lurkmore.to\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
DNT: 1\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Referer: https://www.google.com/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ru-RU,ru;q=0.9,ja-JP;q=0.8,ja;q=0.7,en-US;q=0.6,en;q=0.5\r\n
Cookie: __utmc=1; __utma=1.1704451928.1600267285.1600267285.1600710835.2; __utmz=1.1600710835.2.2.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)\r\n
Cookie pair: __utmc=1
Cookie pair: __utma=1.1704451928.1600267285.1600267285.1600710835.2
Cookie pair: __utmz=1.1600710835.2.2.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)
\r\n
[Full request URI: http://lurkmore.to/QWERTY]
[HTTP request 1/3]
[Response in frame: 86]
[Next request in frame: 88]
0000 78 b2 13 b5 64 88 24 0a 64 e7 7b 99 08 00 45 00 x···d·$· d·{···E·
0010 02 f3 df 70 40 00 80 06 d6 52 c0 a8 01 4e bc 2a ···p@··· ·R···N·*
0020 c4 20 e3 09 00 50 e8 d0 de 17 63 eb f2 dd 50 18 · ···P·· ··c···P·
0030 02 01 68 c3 00 00 47 45 54 20 2f 51 57 45 52 54 ··h···GE T /QWERT
0040 59 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 Y HTTP/1 .1··Host
0050 3a 20 6c 75 72 6b 6d 6f 72 65 2e 74 6f 0d 0a 43 : lurkmo re.to··C
0060 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnectio n: keep-
0070 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e alive··C ache-Con
0080 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d trol: ma x-age=0·
0090 0a 44 4e 54 3a 20 31 0d 0a 55 70 67 72 61 64 65 ·DNT: 1· ·Upgrade
00a0 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 -Insecur e-Reques
00b0 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e ts: 1··U ser-Agen
00c0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
00d0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
00e0 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70 Win64; x64) App
00f0 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 leWebKit /537.36
0100 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 (KHTML, like Gec
0110 6b 6f 29 20 43 68 72 6f 6d 65 2f 38 35 2e 30 2e ko) Chro me/85.0.
0120 34 31 38 33 2e 31 30 32 20 53 61 66 61 72 69 2f 4183.102 Safari/
0130 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 537.36·· Accept:
4.1 Изучение GET-запроса
Hypertext Transfer Protocol: Protocol
Пакеты: 2579 · Показаны: 24 (0.9%)
Профиль: Default
ENG
22:00
21.09.2020

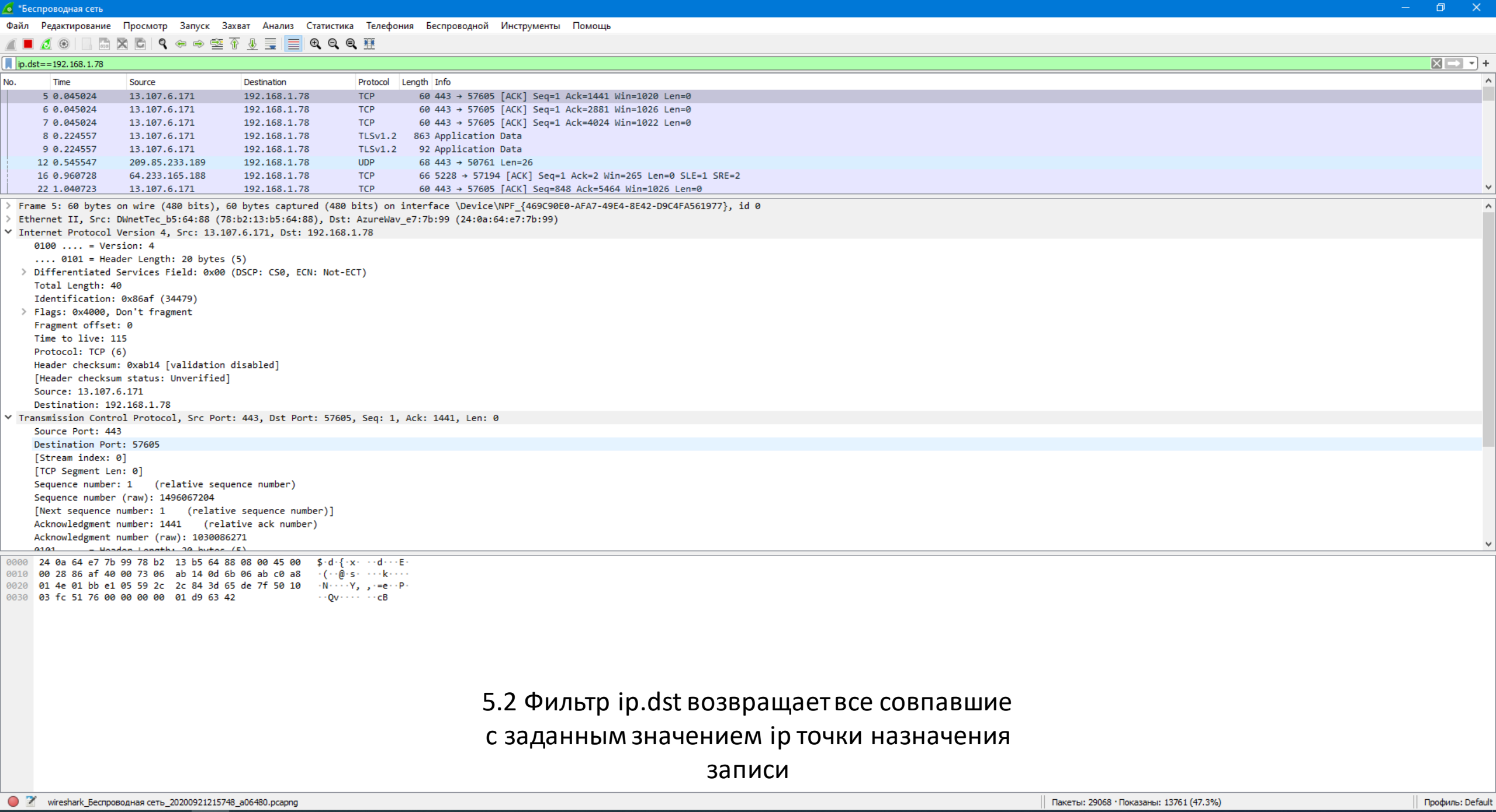


4.2 Изучение POST-запроса

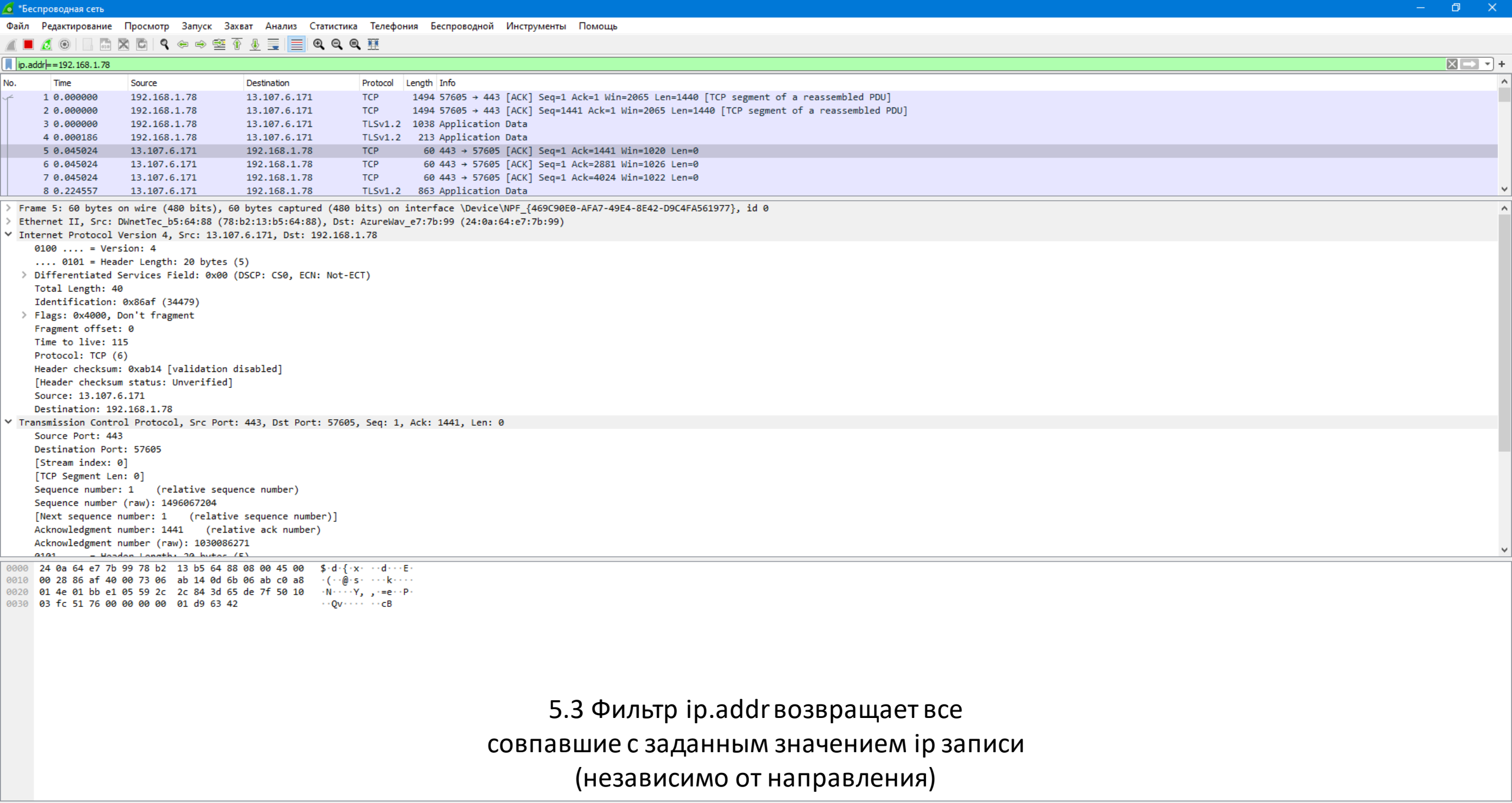
Обнаружены переданные логин и пароль в незашифрованном виде



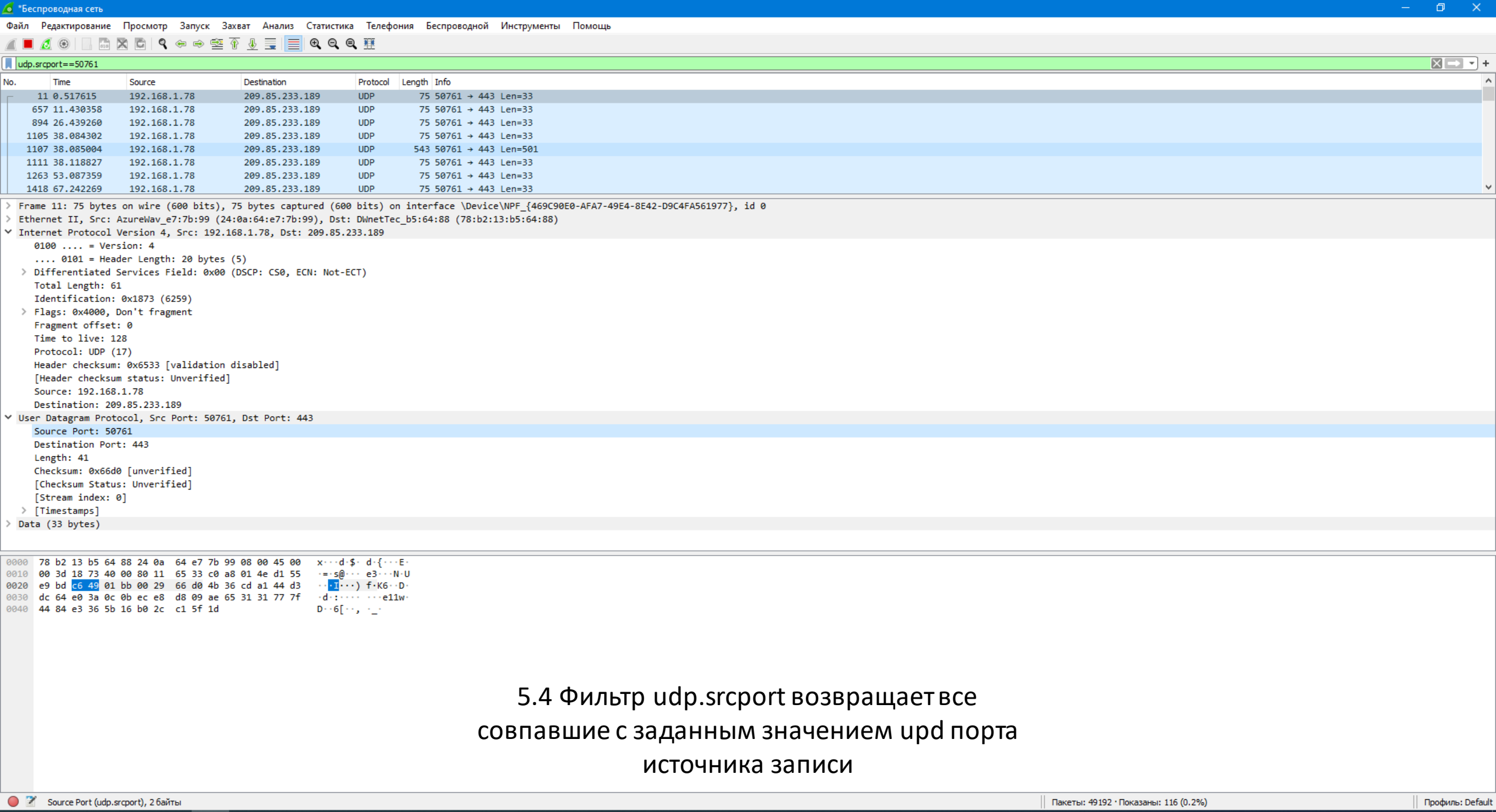
5.1 Фильтр ip.src возвращает все совпавшие с заданным значением ip источника записи



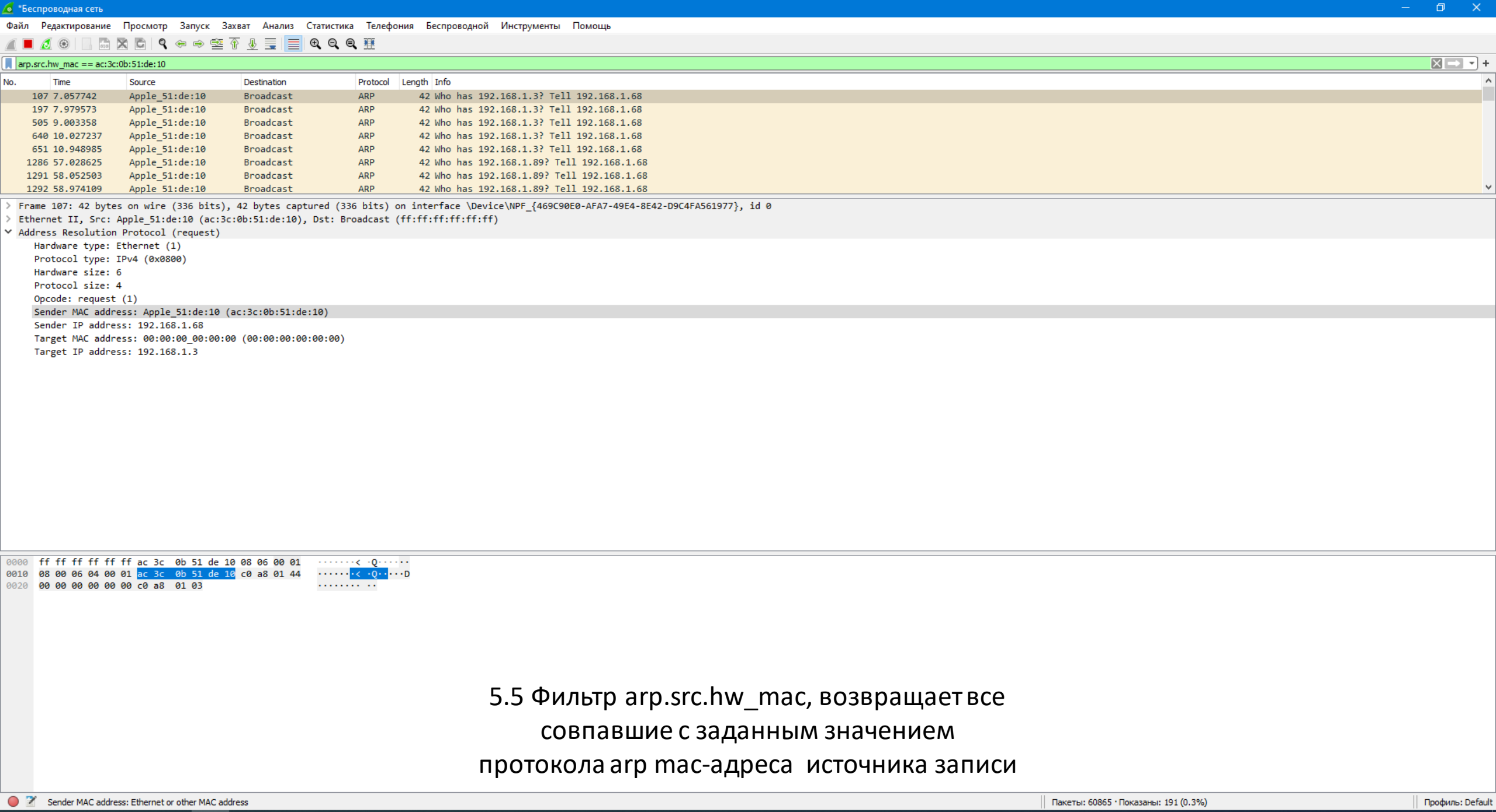
5.2 Фильтр ip.dst возвращает все совпавшие с заданным значением ip точки назначения записи



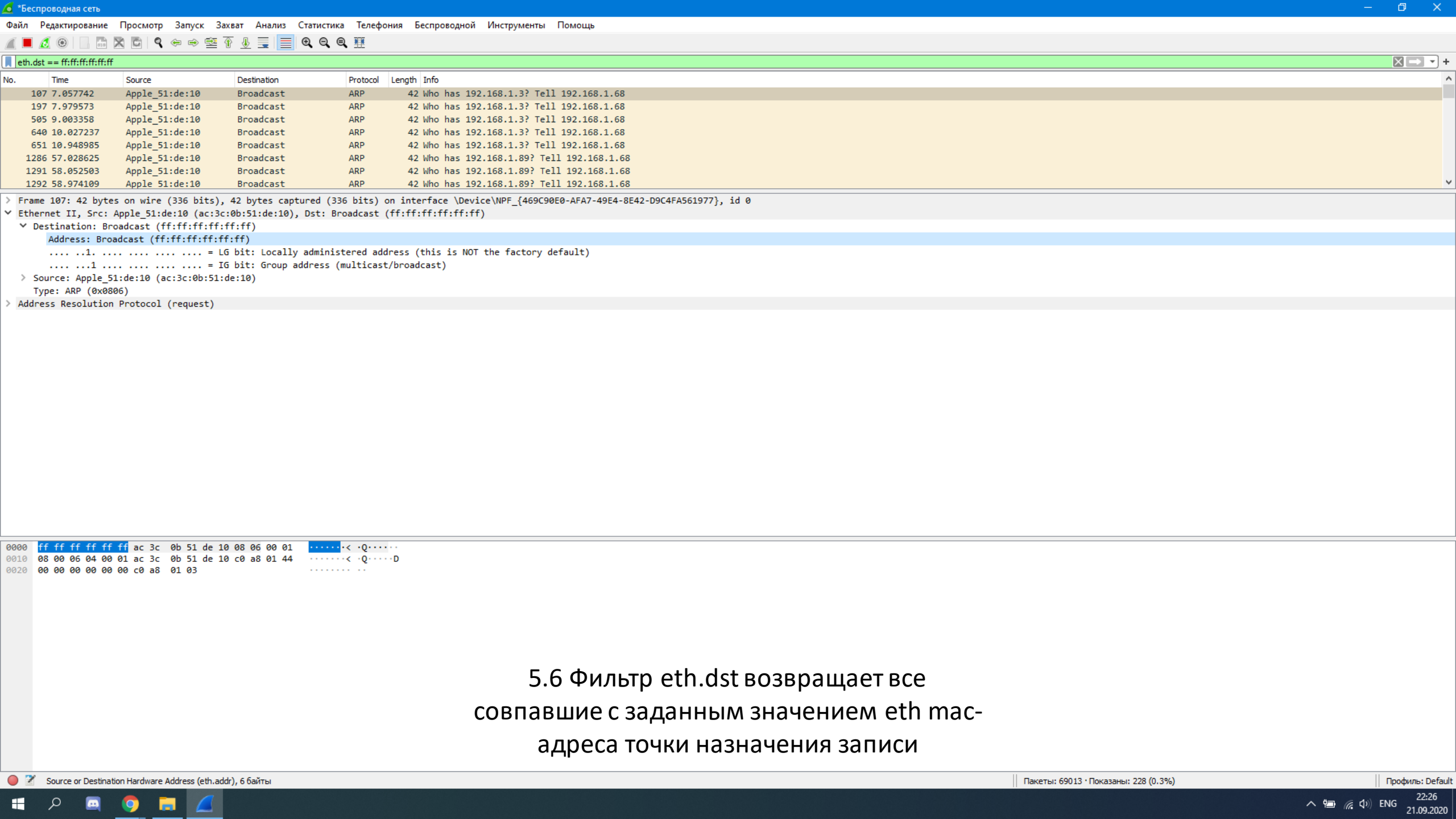
5.3 Фильтр ip.addr возвращает все совпавшие с заданным значением ip записи (независимо от направления)



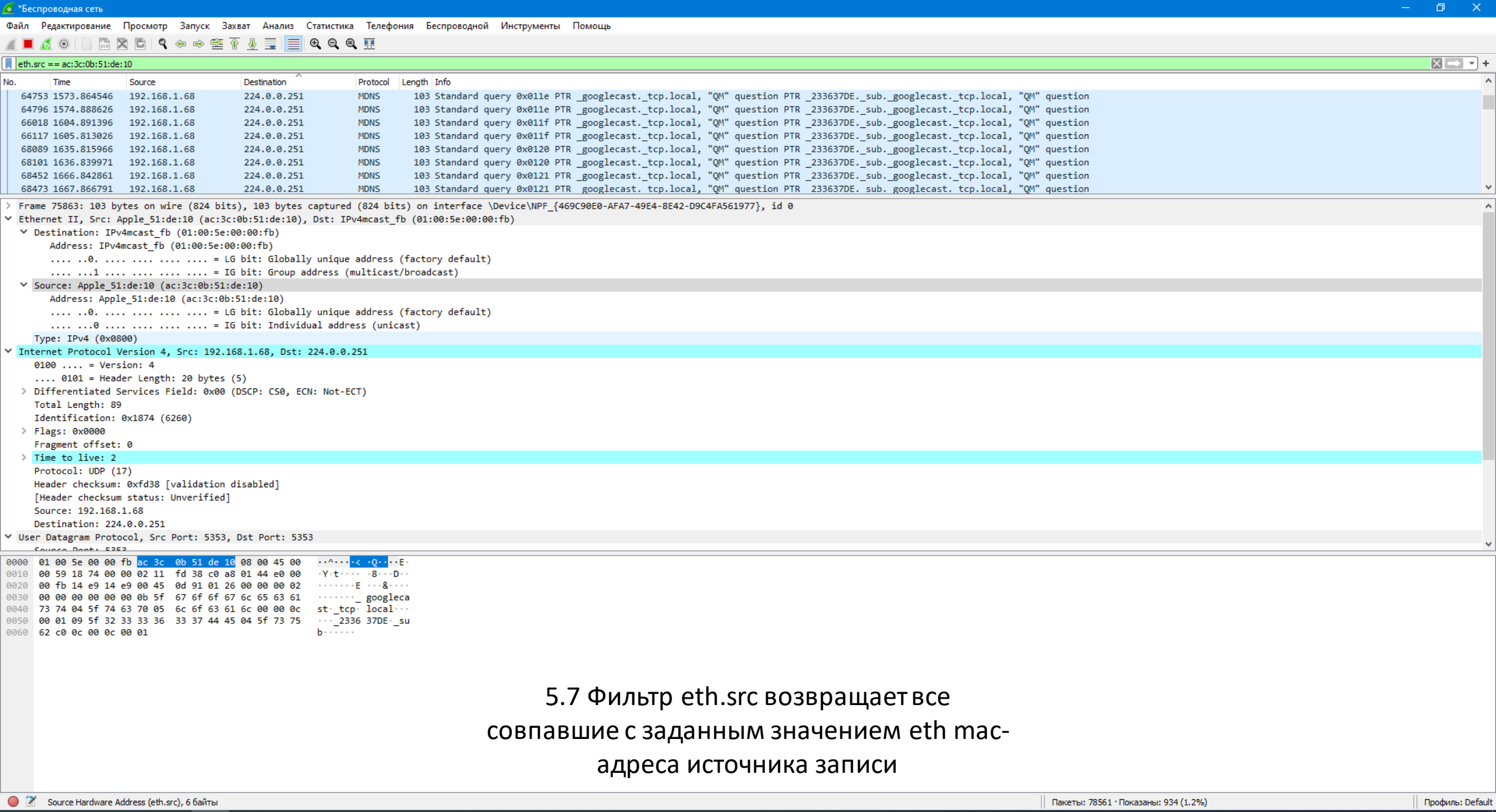
5.4 Фильтр udp.srcport возвращает все совпавшие с заданным значением upd порта источника записи



5.5 Фильтр arp.src.hw_mac, возвращает все совпавшие с заданным значением протокола arp mac-адреса источника записи



5.6 Фильтр eth.dst возвращает все совпавшие с заданным значением eth mac-адреса точки назначения записи



5.7 Фильтр eth.src возвращает все совпавшие с заданным значением eth mac-адреса источника записи