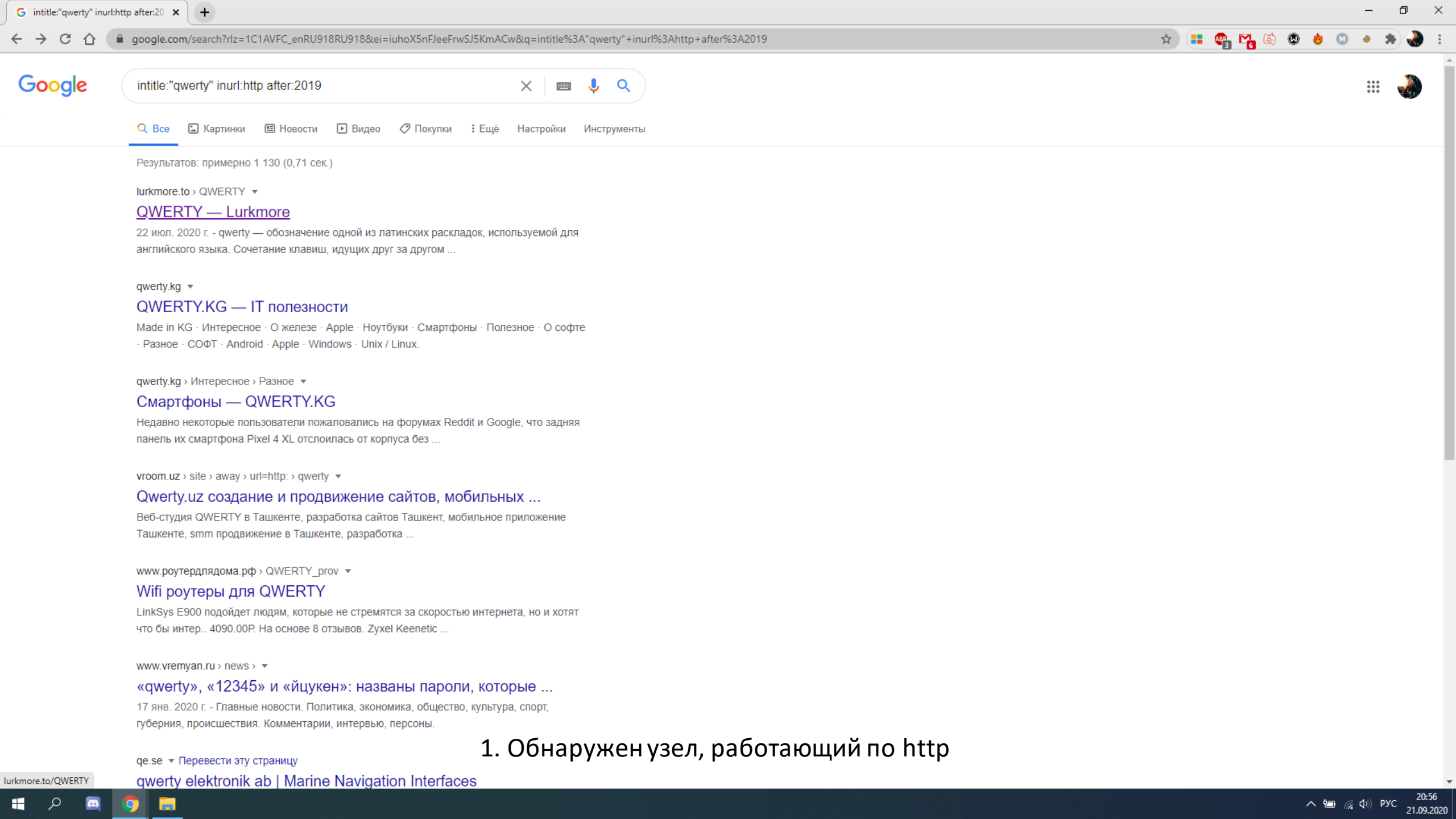
A large, dark blue ink splatter or blotch serves as the background for the text. The splatter has irregular, organic edges with some lighter blue and white areas visible within and around it, suggesting a liquid or paint-like texture. The overall shape is roughly circular but with many protrusions and indentations.

Практическая работа №2

БАСО-03-20



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.. 4090.00Р. 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

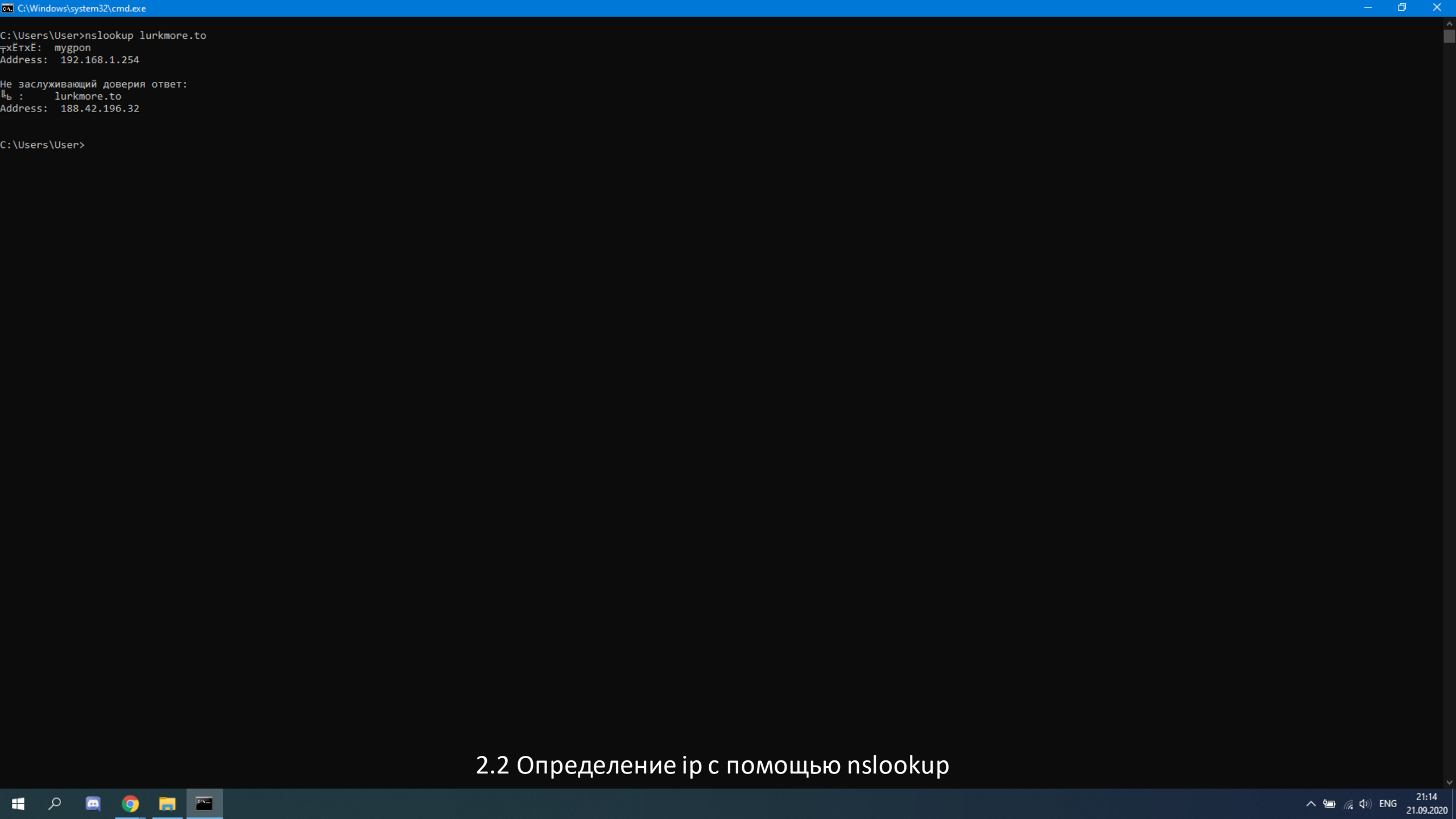
```
C:\Windows\system32\cmd.exe
C:\Users\User>ping lurkmore.to

Обмен пакетами с lurkmore.to [188.42.196.32] с 32 байтами данных:
Ответ от 188.42.196.32: число байт=32 время=58мс TTL=48
Ответ от 188.42.196.32: число байт=32 время=60мс TTL=48
Ответ от 188.42.196.32: число байт=32 время=61мс TTL=48
Ответ от 188.42.196.32: число байт=32 время=60мс TTL=48

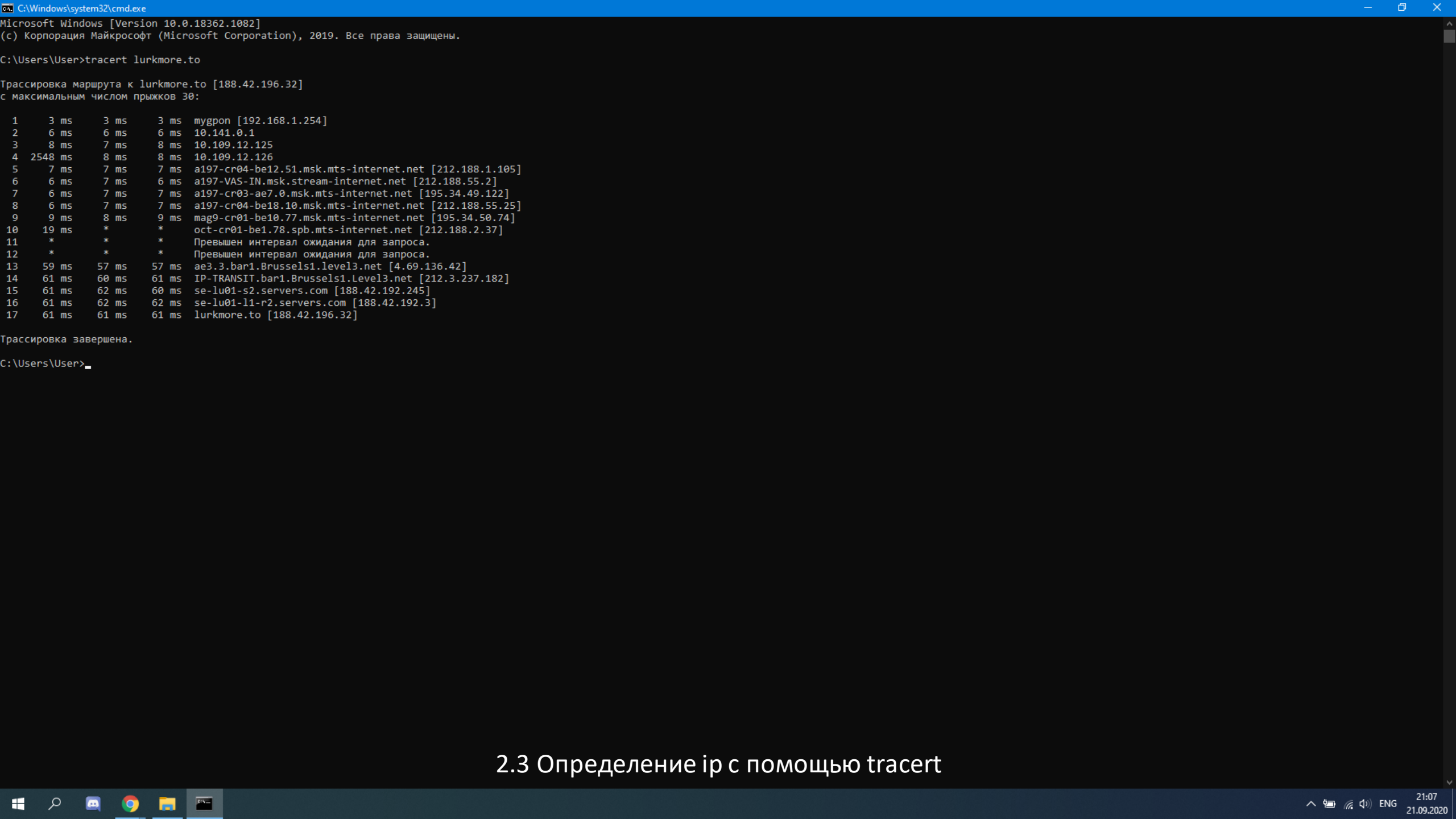
Статистика Ping для 188.42.196.32:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 58мсек, Максимальное = 61 мсек, Среднее = 59 мсек

C:\Users\User>
```

2.1 Определение ip с помощью ping



2.2 Определение ip с помощью nslookup



2.3 Определение ip с помощью tracert

```
C:\Windows\system32\cmd.exe
C:\Users\User>nslookup -query=mx lurkmore.to
тхЕтхЕ:  mygpon
Address:  192.168.1.254

Не заслуживающий доверия ответ:
lurkmore.to      MX preference = 5, mail exchanger = mail.lurkmore.to

C:\Users\User>
```

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

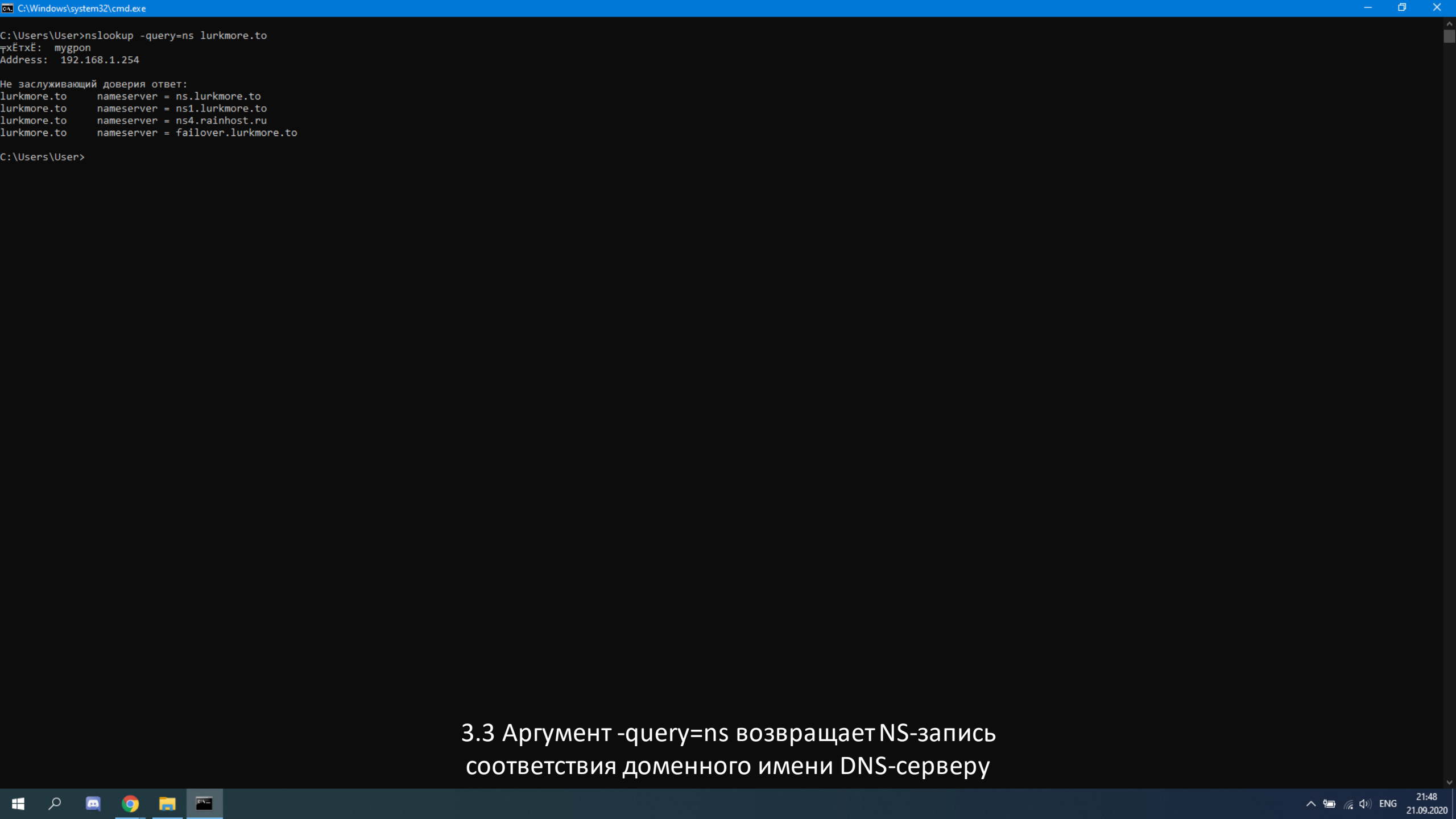
```
C:\Windows\system32\cmd.exe
C:\Users\User>nslookup -query=soa lurkmore.to
тхЕтхЕ: mygpon
Address: 192.168.1.254

Не заслуживающий доверия ответ:
lurkmore.to
    primary name server = ns.lurkmore.to
    responsible mail addr = hostmaster.lurkmore.to
    serial = 2018063022
    refresh = 300 (5 mins)
    retry = 300 (5 mins)
    expire = 1209600 (14 days)
    default TTL = 1800 (30 mins)

C:\Users\User>
```

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 попытке 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


```
C:\Windows\system32\cmd.exe
C:\Users\User>nslookup -type=any lurkmore.to
тхЕтхЕ: mygpon
Address: 192.168.1.254

Не заслуживающий доверия ответ:
lurkmore.to      nameserver = ns1.lurkmore.to
lurkmore.to
    primary name server = ns.lurkmore.to
    responsible mail addr = hostmaster.lurkmore.to
    serial = 2018063022
    refresh = 300 (5 mins)
    retry = 300 (5 mins)
    expire = 1209600 (14 days)
    default TTL = 1800 (30 mins)
lurkmore.to      nameserver = failover.lurkmore.to
lurkmore.to      nameserver = ns.lurkmore.to
lurkmore.to      nameserver = ns4.rainhost.ru

C:\Users\User>
```

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

22:00

21.09.2020

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http

No.	Time	Source	Destination	Protocol	Length	Info
8404	262.591012	88.212.252.22	192.168.1.78	HTTP	266	HTTP/1.0 408 Request Time-out (text/html)
8690	281.941196	192.168.1.78	188.42.196.32	HTTP	1380	POST /index.php?title=%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:UserLogin&action=submitlogin&type=login&returnto=QWERTY HTTP/1.1 (application/x-www-form-urlencoded)
8698	282.053454	188.42.196.32	192.168.1.78	HTTP	60	HTTP/1.1 200 OK (text/html)
8702	282.133512	192.168.1.78	188.42.196.32	HTTP	912	GET /load.php?debug=false&lang=ru&modules=startup&only=scripts&skin=ventus&* HTTP/1.1
8714	283.023342	188.42.196.32	192.168.1.78	HTTP	60	HTTP/1.1 200 OK (text/javascript)
8716	283.125703	192.168.1.78	188.42.196.32	HTTP	763	GET /skins/common/Errorshield.png HTTP/1.1
8724	283.185945	188.42.196.32	192.168.1.78	HTTP	1505	HTTP/1.1 200 OK (PNG)

Upgrade-Insecure-Requests: 1\r\n

DNT: 1\r\n

Content-Type: application/x-www-form-urlencoded\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: http://lurkmore.to/index.php?title=%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:UserLogin&returnto=QWERTY\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

[truncated]Cookie: __utmc=1; __utma=1.1704451928.1600267285.1600710835.1600714677.3; __utms=1.1600714677.3.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); __utmt=1; lurkmore_lm_session=rbgtqgvnpj611387ghdvr86g6

Cookie pair: __utmc=1

Cookie pair: __utma=1.1704451928.1600267285.1600710835.1600714677.3

Cookie pair: __utms=1.1600714677.3.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)

Cookie pair: __utmt=1

Cookie pair: lurkmore_lm_session=rbgtqgvnpj611387ghdvr86g6

Cookie pair: __utmb=1.2.10.1600714677

\r\n

[Full request URI: http://lurkmore.to/index.php?title=%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:UserLogin&action=submitlogin&type=login&returnto=QWERTY]

[HTTP request 1/3]

[Response in frame: 8698]

[Next request in frame: 8702]

File Data: 215 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

> Form item: "wpName" = "admin"

> Form item: "wpPassword" = "password"

> Form item: "wpLoginAttempt" = "Представиться системе"

> Form item: "wpLoginToken" = "57718eb3d7951929a2a84ba2ffe19911"

0430 64 65 64 29 3b 20 5f 5f 75 74 6d 74 3d 31 3b 20 ded); __ utmt=1;

0440 6c 75 72 6b 6d 6f 72 65 5f 6c 6d 5f 5f 73 65 73 lurkmore_lm_ses

0450 73 69 6f 6e 3d 72 62 67 74 71 67 76 6e 6e 70 6a sion=rbg tqgvnpj

0460 36 31 6c 33 38 37 67 68 64 76 72 38 36 67 36 3b 611387gh dvr86g6;

0470 20 5f 5f 75 74 6d 62 3d 31 2e 32 2e 31 30 2e 31 __utmb= 1.2.10.1

0480 36 30 30 37 31 34 36 37 37 0d 0a 0d 0a 77 70 4e 60071467 7...wpN

0490 61 6d 65 3d 61 64 6d 69 6e 26 77 70 50 61 73 73 ame=admin&wpPass

04a0 77 6f 72 64 3d 70 61 73 73 77 6f 72 64 26 77 70 word=password&wp

04b0 4c 6f 67 69 6e 41 74 74 65 6d 70 74 3d 25 44 30 LoginAtt empt=%D0

04c0 25 39 46 25 44 31 25 38 30 25 44 30 25 42 35 25 %9F%D1%8 0%D0%B5%

04d0 44 30 25 42 34 25 44 31 25 38 31 25 44 31 25 38 D0%B4%D1 %81%D1%8

04e0 32 25 44 30 25 42 30 25 44 30 25 42 32 25 44 30 2%D0%B0% D0%B2%D0

04f0 25 42 38 25 44 31 25 38 32 25 44 31 25 38 43 25 %88%D1%8 2%D1%8c%

0500 44 31 25 38 31 25 44 31 25 38 46 2b 25 44 31 25 D1%81%D1 %8F+%D1%

0510 38 31 25 44 30 25 42 38 25 44 31 25 38 31 25 44 81%D0%B8 %D1%81%D

0520 31 25 38 32 25 44 30 25 42 35 25 44 30 25 42 43 1%82%D0% B5%D0%BC

0530 25 44 30 25 42 35 26 77 70 4c 6f 67 69 6e 54 6f %D0%B5&w pLoginTo

0540 6b 65 6e 3d 35 37 37 31 38 65 62 33 64 37 39 35 ken=5771 8eb3d795

0550 31 39 32 39 61 32 61 38 34 62 61 32 66 66 65 31 1929a2a8 4ba2ffe1

0560 39 39 31 31 9911

Text item (text), 20 bytes

Пакеты: 9951 · Показаны: 39 (0.4%)

Профиль: Default

4.2 Изучение POST-запроса

Обнаружены переданные логин и пароль в незашифрованном виде

22:03

21.09.2020

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.src==192.168.1.68

No.	Time	Source	Destination	Protocol	Length	Info
8667	311.100130	192.168.1.68	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8668	311.206070	192.168.1.68	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8835	321.026339	192.168.1.68	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8842	321.106050	192.168.1.68	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8849	321.211323	192.168.1.68	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8980	331.031633	192.168.1.68	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8981	331.110917	192.168.1.68	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8982	331.216124	192.168.1.68	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1

> Frame 19096: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{469C90E0-AFA7-49E4-8E42-D9C4FA561977}, id 0

> Ethernet II, Src: Apple_51:de:10 (ac:3c:0b:51:de:10), Dst: AzureWav_e7:7b:99 (24:0a:64:e7:7b:99)

> Internet Protocol Version 4, Src: 192.168.1.68, Dst: 239.255.255.250

0100 = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 153

Identification: 0xeb33 (60211)

> Flags: 0x0000

Fragment offset: 0

Time to live: 1

Protocol: UDP (17)

Header checksum: 0x1c3a [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.68

Destination: 239.255.255.250

> User Datagram Protocol, Src Port: 59843, Dst Port: 1900

> Simple Service Discovery Protocol

> M-SEARCH * HTTP/1.1\r\n

HOST: 239.255.255.250:1900\r\n

MAN: "ssdp:discover"\r\n

MX: 1\r\n

ST: urn:dial-multiscreen-org:service:dial:1\r\n

\r\n

[Full request URI: http://239.255.255.250:1900*]

[HTTP request 162/171]

[Decap request in frame 19095]

```
0000  24 0a 64 e7 7b 99 ac 3c 0b 51 de 10 08 00 45 00  $-d-{\<< Q....E-
0010  00 99 eb 33 00 00 01 11 1c 3a c0 a8 01 44 ef ff  ....3....:...D-
0020  ff fa e9 c3 07 6c 00 85 2e 44 4d 2d 53 45 41 52  ....1...DM-SEAR
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH *HTT P/1.1-H
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:190 0-MAN:
0060  22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:di scover"-
0070  0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  :MX: 1- ST: urn:
0080  64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  -org:ser vice:dia
00a0  6c 3a 31 0d 0a 0d 0a 1:1----
```

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

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.dst==192.168.1.78

No.	Time	Source	Destination	Protocol	Length	Info
5	0.045024	13.107.6.171	192.168.1.78	TCP	60	443 → 57605 [ACK] Seq=1 Ack=1441 Win=1020 Len=0
6	0.045024	13.107.6.171	192.168.1.78	TCP	60	443 → 57605 [ACK] Seq=1 Ack=2881 Win=1026 Len=0
7	0.045024	13.107.6.171	192.168.1.78	TCP	60	443 → 57605 [ACK] Seq=1 Ack=4024 Win=1022 Len=0
8	0.224557	13.107.6.171	192.168.1.78	TLSv1.2	863	Application Data
9	0.224557	13.107.6.171	192.168.1.78	TLSv1.2	92	Application Data
12	0.545547	209.85.233.189	192.168.1.78	UDP	68	443 → 50761 Len=26
16	0.960728	64.233.165.188	192.168.1.78	TCP	66	5228 → 57194 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
22	1.040723	13.107.6.171	192.168.1.78	TCP	60	443 → 57605 [ACK] Seq=848 Ack=5464 Win=1026 Len=0

> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{469C90E0-AFA7-49E4-8E42-D9C4FA561977}, id 0

> Ethernet II, Src: Dwnetec_b5:64:88 (78:b2:13:b5:64:88), Dst: AzureWav_e7:7b:99 (24:0a:64:e7:7b:99)

> Internet Protocol Version 4, Src: 13.107.6.171, Dst: 192.168.1.78

0100 = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 40

Identification: 0x86af (34479)

> Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 115

Protocol: TCP (6)

Header checksum: 0xab14 [validation disabled]

[Header checksum status: Unverified]

Source: 13.107.6.171

Destination: 192.168.1.78

> Transmission Control Protocol, Src Port: 443, Dst Port: 57605, Seq: 1, Ack: 1441, Len: 0

Source Port: 443

Destination Port: 57605

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 1496067204

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1441 (relative ack number)

Acknowledgment number (raw): 1030086271

0101 ... = Header Length: 20 bytes (5)

0000 24 0a 64 e7 7b 99 78 b2 13 b5 64 88 08 00 45 00 \$·d·{·x· ··d··E·

0010 00 28 86 af 40 00 73 06 ab 14 0d 6b 06 ab c0 a8 ·(·@·s· ··k···

0020 01 4e 01 bb e1 05 59 2c 2c 84 3d 65 de 7f 50 10 ·N···Y, ,·e··P·

0030 03 fc 51 76 00 00 00 00 01 d9 63 42 ··Qv······cB

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

wireshark_Беспроводная сеть_20200921215748_a06480.pcapng

Пакеты: 29068 · Показаны: 13761 (47.3%)

Профиль: Default

22:11 21.09.2020

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr==192.168.1.78

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.78	13.107.6.171	TCP	1494	57605 → 443 [ACK] Seq=1 Ack=1 Win=2065 Len=1440 [TCP segment of a reassembled PDU]
2	0.000000	192.168.1.78	13.107.6.171	TCP	1494	57605 → 443 [ACK] Seq=1441 Ack=1 Win=2065 Len=1440 [TCP segment of a reassembled PDU]
3	0.000000	192.168.1.78	13.107.6.171	TLSv1.2	1038	Application Data
4	0.000186	192.168.1.78	13.107.6.171	TLSv1.2	213	Application Data
5	0.045024	13.107.6.171	192.168.1.78	TCP	60	443 → 57605 [ACK] Seq=1 Ack=1441 Win=1020 Len=0
6	0.045024	13.107.6.171	192.168.1.78	TCP	60	443 → 57605 [ACK] Seq=1 Ack=2881 Win=1026 Len=0
7	0.045024	13.107.6.171	192.168.1.78	TCP	60	443 → 57605 [ACK] Seq=1 Ack=4024 Win=1022 Len=0
8	0.224557	13.107.6.171	192.168.1.78	TLSv1.2	863	Application Data

> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{469C90E0-AFA7-49E4-8E42-D9C4FA561977}, id 0

> Ethernet II, Src: DNetTec_b5:64:88 (78:b2:13:b5:64:88), Dst: AzureWav_e7:7b:99 (24:0a:64:e7:7b:99)

> Internet Protocol Version 4, Src: 13.107.6.171, Dst: 192.168.1.78

0100 = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 40

Identification: 0x86af (34479)

> Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 115

Protocol: TCP (6)

Header checksum: 0xab14 [validation disabled]

[Header checksum status: Unverified]

Source: 13.107.6.171

Destination: 192.168.1.78

> Transmission Control Protocol, Src Port: 443, Dst Port: 57605, Seq: 1, Ack: 1441, Len: 0

Source Port: 443

Destination Port: 57605

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 1496067204

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1441 (relative ack number)

Acknowledgment number (raw): 1030086271

0101 = Header Length: 20 bytes (5)

0000 24 0a 64 e7 7b 99 78 b2 13 b5 64 88 08 00 45 00 \$·d·{·x· ··d···E·

0010 00 28 86 af 40 00 73 06 ab 14 0d 6b 06 ab c0 a8 ·(·@·s· ··k····

0020 01 4e 01 bb e1 05 59 2c 2c 84 3d 65 de 7f 50 10 ·N···Y, ,·e··P·

0030 03 fc 51 76 00 00 00 00 01 d9 63 42 ··Qv······cB

Source or Destination Address: IPv4 address

Пакеты: 40004 · Показаны: 38984 (97.5%)

Профиль: Default

22:14
21.09.2020

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

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

udp.srcport==50761

No.	Time	Source	Destination	Protocol	Length	Info
11	0.517615	192.168.1.78	209.85.233.189	UDP	75	50761 → 443 Len=33
657	11.430358	192.168.1.78	209.85.233.189	UDP	75	50761 → 443 Len=33
894	26.439260	192.168.1.78	209.85.233.189	UDP	75	50761 → 443 Len=33
1105	38.084302	192.168.1.78	209.85.233.189	UDP	75	50761 → 443 Len=33
1107	38.085004	192.168.1.78	209.85.233.189	UDP	543	50761 → 443 Len=501
1111	38.118827	192.168.1.78	209.85.233.189	UDP	75	50761 → 443 Len=33
1263	53.087359	192.168.1.78	209.85.233.189	UDP	75	50761 → 443 Len=33
1418	67.242269	192.168.1.78	209.85.233.189	UDP	75	50761 → 443 Len=33

> Frame 11: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{469C90E0-AFA7-49E4-8E42-D9C4FA561977}, id 0

> Ethernet II, Src: AzureWav_e7:7b:99 (24:0a:64:e7:7b:99), Dst: DWNnetTec_b5:64:88 (78:b2:13:b5:64:88)

> Internet Protocol Version 4, Src: 192.168.1.78, Dst: 209.85.233.189

0100 = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 61

Identification: 0x1873 (6259)

> Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 128

Protocol: UDP (17)

Header checksum: 0x6533 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.78

Destination: 209.85.233.189

> User Datagram Protocol, Src Port: 50761, Dst Port: 443

Source Port: 50761

Destination Port: 443

Length: 41

Checksum: 0x66d0 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

> Data (33 bytes)

0000 78 b2 13 b5 64 88 24 0a 64 e7 7b 99 08 00 45 00 x...d\$.d.{...E.

0010 00 3d 18 73 40 00 80 11 65 33 c0 a8 01 4e d1 55 ..=s@...e3...N.U

0020 e9 bd c6 49 01 bb 00 29 66 d0 4b 36 cd a1 44 d3 ..[...])f.K6..D.

0030 dc 64 e0 3a 0c 0b ec e8 d8 09 ae 65 31 31 77 7f ..d:.....e1lw.

0040 44 84 e3 36 5b 16 b0 2c c1 5f 1d D..6[... , _.

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

Source Port (udp.srcport), 2 байты

Пакеты: 49192 · Показаны: 116 (0.2%)

Профиль: Default

22:18 21.09.2020

Беспроводная сеть

Файл Редактирование Просмотр Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp.src.hw_mac == ac:3c:0b:51:de:10

No.	Time	Source	Destination	Protocol	Length	Info
107	7.057742	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
197	7.979573	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
505	9.003358	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
640	10.027237	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
651	10.948985	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
1286	57.028625	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.89? Tell 192.168.1.68
1291	58.052503	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.89? Tell 192.168.1.68
1292	58.974109	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.89? Tell 192.168.1.68

> Frame 107: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{469C90E0-AFA7-49E4-8E42-D9C4FA561977}, id 0

> Ethernet II, Src: Apple_51:de:10 (ac:3c:0b:51:de:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Address Resolution Protocol (request)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Apple_51:de:10 (ac:3c:0b:51:de:10)
Sender IP address: 192.168.1.68
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.3

0000 ff ff ff ff ff ff ac 3c 0b 51 de 10 08 06 00 01<.Q.....
0010 08 00 06 04 00 01 ac 3c 0b 51 de 10 c0 a8 01 44<.Q.....D
0020 00 00 00 00 00 00 c0 a8 01 03<.Q.....

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

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

eth.dst == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Info
107	7.057742	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
197	7.979573	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
505	9.003358	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
640	10.027237	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
651	10.948985	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.68
1286	57.028625	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.89? Tell 192.168.1.68
1291	58.052503	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.89? Tell 192.168.1.68
1292	58.974109	Apple_51:de:10	Broadcast	ARP	42	Who has 192.168.1.89? Tell 192.168.1.68

> Frame 107: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{469C90E0-AFA7-49E4-8E42-D9C4FA561977}, id 0

> Ethernet II, Src: Apple_51:de:10 (ac:3c:0b:51:de:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

.... .. = LG bit: Locally administered address (this is NOT the factory default)

.... .. = IG bit: Group address (multicast/broadcast)

> Source: Apple_51:de:10 (ac:3c:0b:51:de:10)

Type: ARP (0x0806)

> Address Resolution Protocol (request)

0000 ff ff ff ff ff ff ac 3c 0b 51 de 10 08 06 00 01< .Q.....

0010 08 00 06 04 00 01 ac 3c 0b 51 de 10 c0 a8 01 44< .Q.....D

0020 00 00 00 00 00 00 c0 a8 01 03

Source or Destination Hardware Address (eth.addr), 6 байты

Пакеты: 69013 · Показаны: 228 (0.3%)

Профиль: Default

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

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

eth.src == ac:3c:0b:51:de:10

No. Time Source Destination Protocol Length Info

64753 1573.864546 192.168.1.68 224.0.0.251 MDNS 103 Standard query 0x011e PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question

64796 1574.888626 192.168.1.68 224.0.0.251 MDNS 103 Standard query 0x011e PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question

66018 1604.891396 192.168.1.68 224.0.0.251 MDNS 103 Standard query 0x011f PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question

66117 1605.813026 192.168.1.68 224.0.0.251 MDNS 103 Standard query 0x011f PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question

68089 1635.815966 192.168.1.68 224.0.0.251 MDNS 103 Standard query 0x0120 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question

68101 1636.839971 192.168.1.68 224.0.0.251 MDNS 103 Standard query 0x0120 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question

68452 1666.842861 192.168.1.68 224.0.0.251 MDNS 103 Standard query 0x0121 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question

68473 1667.866791 192.168.1.68 224.0.0.251 MDNS 103 Standard query 0x0121 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question

> Frame 75863: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{469C90E0-AFA7-49E4-8E42-D9C4FA561977}, id 0

> Ethernet II, Src: Apple_51:de:10 (ac:3c:0b:51:de:10), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)

> Destination: IPv4mcast_fb (01:00:5e:00:00:fb)

Address: IPv4mcast_fb (01:00:5e:00:00:fb)

.... .. = LG bit: Globally unique address (factory default)

.... ..1 = IG bit: Group address (multicast/broadcast)

> Source: Apple_51:de:10 (ac:3c:0b:51:de:10)

Address: Apple_51:de:10 (ac:3c:0b:51:de:10)

.... .. = LG bit: Globally unique address (factory default)

.... ..0 = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.1.68, Dst: 224.0.0.251

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 89

Identification: 0x1874 (6260)

> Flags: 0x0000

Fragment offset: 0

> Time to live: 2

Protocol: UDP (17)

Header checksum: 0xfd38 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.68

Destination: 224.0.0.251

> User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Source Port: 5353

0000 01 00 5e 00 00 fb ac 3c 0b 51 de 10 08 00 45 00 ..^...<..Q...E

0010 00 59 18 74 00 00 02 11 fd 38 c0 a8 01 44 e0 00 .Y.t...8...D

0020 00 fb 14 e9 14 e9 00 45 0d 91 01 26 00 00 00 02E...&...

0030 00 00 00 00 00 00 0b 5f 67 6f 6f 67 6c 65 63 61_googleca

0040 73 74 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c st_tcp local...

0050 00 01 09 5f 32 33 33 36 33 37 44 45 04 5f 73 75 ..._2336 37DE._su

0060 62 c0 0c 00 0c 00 01 b.....

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

Source Hardware Address (eth.src), 6 байты

Пакеты: 78561 · Показаны: 934 (1.2%)

Профиль: Default

22:29 21.09.2020