

1. В приложенном файле "The Ultimate PCAP.pcapng" (из раздаточного материала) найти e-mail. Что внутри письма и для кого оно?

Дополнительный источник информации:

<https://wiki.wireshark.org/SMTP>

и

<https://wiki.wireshark.org/IMF.md>

Нужны фильтры SMTP и IMF

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a packet capture of an SMTP message. The packet list on the left shows packet 2064 selected, with filters 'smtp & IMF' and 'SMTP/IMF' applied. The packet details pane on the right shows the 'Internet Message Format' section expanded, revealing the 'To' field with the email address 'johannes@webertest.net'. The packet bytes pane at the bottom shows the raw data of the message body, which is a long string of base64-encoded text.

Wireshark - Пакет 2064 - The Ultimate PCAP v20221220.pcapng

Frame 2064: 3131 bytes on wire (25048 bits), 3131 bytes captured (25048 bits) on interface unknown, id 82

- Ethernet II, Src: Dell\_0a:8a:96 (00:12:3f:0a:8a:96), Dst: JuniperN\_a1:f9:89 (00:19:e2:a1:f9:89)
- Internet Protocol Version 4, Src: 192.168.110.9, Dst: 80.154.108.237
- Transmission Control Protocol, Src Port: 45271, Dst Port: 25, Seq: 7325, Ack: 130, Len: 3065
- Simple Mail Transfer Protocol
- Internet Message Format
  - Subject: SMTP Ping
  - Content-Type: text/plain
  - From: <>, 1 item
    - Item: <>\r\n
  - To: <johannes@webertest.net>, 1 item
    - Item: <johannes@webertest.net>\r\n
  - Message-Text
    - AABBCCDDEEFFGGHHIIJJKLLMNNOPPQQRRSSTTUUVVWXXYYZZ00112233445566778899
    - AABBCCDDEEFFGGHHIIJJKLLMNNOPPQQRRSSTTUUVVWXXYYZZ00112233445566778899
    - AABBCCDDEEFFGGHHIIJJKLLMNNOPPQQRRSSTTUUVVWXXYYZZ00112233445566778899
    - AABBCCDDEEFFGGHHIIJJKLLMNNOPPQQRRSSTTUUVVWXXYYZZ00112233445566778899
    - AABBCCDDEEFFGGHHIIJJKLLMNNOPPQQRRSSTTUUVVWXXYYZZ00112233445566778899
    - AABBCCDDEEFFGGHHIIJJKLLMNNOPPQQRRSSTTUUVVWXXYYZZ00112233445566778899
    - AABBCCDDEEFFGGHHIIJJKLLMNNOPPQQRRSSTTUUVVWXXYYZZ00112233445566778899

Frame (3131 bytes) Reassembled SMTP (10300 bytes)

Show packet bytes

Destination Address: 80.154.108.237

Transmission Control Protocol

Пакеты: 38642 · Показаны: 1 (0.0%)

Профиль: Default

2. Закрепите навыки фильтрации. Запустите трейс до 8.8.8.8. И перехватите его в Wireshark. Проанализируйте.

Дополнительный источник информации:

<https://www.youtube.com/watch?v=TbsBhyylth4>

```
Командная строка
Трассировка завершена.
C:\Users\fedor>tracert -d 8.8.8.8

Трассировка маршрута к 8.8.8.8 с максимальным числом прыжков 30

 1      3 ms      1 ms      1 ms  192.168.1.1
 2      5 ms      12 ms     6 ms  188.235.125.252
 3      2 ms      21 ms     4 ms  109.194.40.57
 4     55 ms     54 ms    55 ms  188.234.131.158
 5     50 ms     50 ms    50 ms  188.234.131.159
 6     51 ms     51 ms    55 ms  74.125.244.129
 7     50 ms     47 ms    50 ms  74.125.244.132
 8     57 ms     55 ms    58 ms  72.14.232.85
 9     59 ms     55 ms    55 ms  142.251.61.221
10     56 ms     54 ms    54 ms  172.253.79.237
11      *        *        *    Превышен интервал ожидания для запроса.
12      *        *        *    Превышен интервал ожидания для запроса.
13      *        *        *    Превышен интервал ожидания для запроса.
14      *        *        *    Превышен интервал ожидания для запроса.
15      *        *        *    Превышен интервал ожидания для запроса.
16      *        *        *    Превышен интервал ожидания для запроса.
17      *        *        *    Превышен интервал ожидания для запроса.
18      *        *        *    Превышен интервал ожидания для запроса.
19      *        *        *    Превышен интервал ожидания для запроса.
20     59 ms     56 ms    54 ms  8.8.8.8

Трассировка завершена.
C:\Users\fedor>
```

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

No.	Time	Source	Destination	Protocol	Length	Info
12039	292.359715	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=148/37888, ttl=1 (no response found!)
12040	292.362886	192.168.1.1	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12041	292.363510	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=149/38144, ttl=1 (no response found!)
12042	292.364936	192.168.1.1	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12043	292.365302	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=150/38400, ttl=1 (no response found!)
12044	292.366507	192.168.1.1	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12068	293.372548	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=151/38656, ttl=2 (no response found!)
12071	293.377512	188.235.125.252	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12072	293.378360	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=152/38912, ttl=2 (no response found!)
12073	293.391168	188.235.125.252	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12074	293.391963	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=153/39168, ttl=2 (no response found!)
12075	293.398381	188.235.125.252	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12088	294.400759	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=154/39424, ttl=3 (no response found!)
12089	294.403517	109.194.40.57	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12090	294.404255	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=155/39680, ttl=3 (no response found!)
12091	294.426099	109.194.40.57	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12092	294.426831	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=156/39936, ttl=3 (no response found!)
12093	294.431364	109.194.40.57	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12115	295.443263	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=157/40192, ttl=4 (no response found!)
12118	295.499078	188.234.131.158	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12119	295.499986	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=158/40448, ttl=4 (no response found!)
12122	295.554787	188.234.131.158	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12123	295.555634	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=159/40704, ttl=4 (no response found!)
12126	295.610661	188.234.131.158	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12138	296.564118	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=160/40960, ttl=5 (no response found!)
12139	296.614740	188.234.131.159	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12140	296.615721	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=161/41216, ttl=5 (no response found!)
12142	296.666243	188.234.131.159	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12143	296.667262	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=162/41472, ttl=5 (no response found!)

Первый маршрутизатор

Второй маршрутизатор

icmp

Время жизни пакета

> Frame 12039: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF\_{13395989-6719-4547-9EA9-EE5AB85557}

> Ethernet II, Src: CyberTAN\_b9:3e:6f (00:45:e2:b9:3e:6f), Dst: Tp-LinkT\_bb:a4:06 (f8:d1:11:bb:a4:06)

> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 8.8.8.8

> Internet Control Message Protocol

Ethernet

0 15 16 31

Destination  
f8:d1:11:bb:a4:06

Source  
00:45:e2:b9:3e:6f

Type  
IPv4

Internet Protocol Version 4

0 15 16 31

Version 4	Header Length 20	Differentiated Services Field 0x00	Total Length 92
Identification 0x68a6 (26790)		Flags 0x0	Fragment Offset 0

Internet Control Message Protocol: Protocol

Пакеты: 13892 · Показаны: 93 (0.7%) · Потери: 0 (0.0%)

Профиль: Default

\*Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

icmp

No.	Time	Source	Destination	Protocol	Length	Info
12039	292.359715	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=148/37888, ttl=1 (no response found!)
12040	292.362886	192.168.1.1	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12041	292.363510	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=149/38144, ttl=1 (no response found!)
12042	292.364936	192.168.1.1	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12043	292.365302	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=150/38400, ttl=1 (no response found!)
12044	292.366507	192.168.1.1	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12068	293.372548	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=151/38656, ttl=2 (no response found!)
12071	293.377512	188.235.125.252	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12072	293.378360	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=152/38912, ttl=2 (no response found!)
12073	293.391168	188.235.125.252	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12074	293.391963	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=153/39168, ttl=2 (no response found!)
12075	293.398381	188.235.125.252	192.168.1.101	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12088	294.400759	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=154/39424, ttl=3 (no response found!)
12089	294.403517	109.194.40.57	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12090	294.404255	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=155/39680, ttl=3 (no response found!)
12091	294.426099	109.194.40.57	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12092	294.426831	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=156/39936, ttl=3 (no response found!)
12093	294.431364	109.194.40.57	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12115	295.443263	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=157/40192, ttl=4 (no response found!)
12118	295.499078	188.234.131.158	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12119	295.499986	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=158/40448, ttl=4 (no response found!)
12122	295.554787	188.234.131.158	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
12123	295.555634	192.168.1.101	8.8.8.8	ICMP	106	Echo (ping) request id=0x0001, seq=159/40704, ttl=4 (no response found!)
12126	295.610661	188.234.131.158	192.168.1.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Total Length: 92  
Identification: 0x68a6 (26790)  
> 000. .... = Flags: 0x0  
0 0000 0000 0000 = Fragment Offset: 0  
> Time to Live: 1  
Protocol: ICMP (1)  
Header Checksum: 0x7ede [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.1.101  
Destination Address: 8.8.8.8

Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0xf76a [correct]  
[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 148 (0x0094)

Ethernet  
Destination  
f8:d1:11:bb:a4:06  
Source  
00:45:e2:b9:3e:6f  
Type  
IPv4

Internet Protocol Version 4  
Version  
4  
Header Length  
20  
Differentiated Services Code Point  
0x00  
Total Length  
92

Source Address (ip.src), 4 byte(s)

Пакеты: 13892 · Показаны: 93 (0.7%) · Потеряно: 0 (0.0%)

Профиль: Default

### 3. Закрепите навыки фильтрации.

Найдите еще один сайт без шифрования с возможностью ввода логина/пароля. (можно в гугл настроить соответствующую выдачу по запросу с ключом “-inurl:https” в конце). Перехватите их в Wiresharke, построив фильтр.

проф-обр.рф/register

My bookmarks Jupyter Обучение | GeekBrain... Тест по Итоговая атте... Полный курс по Djan... Тесты | GeekBrains - о... Byffer

Назад

## Регистрация

Через социальную сеть

и/или через форму на сайте

uCoz uID Google Одноклассники Яндекс

Email

Email@gamil.com ✓

Пароль

..... ✓

Имя

Имя ✓

Фамилия

Фамилия ✓

Никнейм

Никнейм ✓

Дата рождения

1 Январь 2023 ✓

Пол

☒ Мужчина ☐ Женщина ✓

ПРОДОЛЖИТЬ

```
C:\Users\fedor>ping проф-обр.рф
```

```
Обмен пакетами с xn----btb1bbcge2a.xn--p1ai [193.109.246.49] с 32 байтами данных:
```

```
Ответ от 193.109.246.49: число байт=32 время=48мс TTL=57
```

```
Ответ от 193.109.246.49: число байт=32 время=50мс TTL=57
```

```
Ответ от 193.109.246.49: число байт=32 время=51мс TTL=57
```

```
Ответ от 193.109.246.49: число байт=32 время=49мс TTL=57
```

```
Статистика Ping для 193.109.246.49:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0  
(0% потерь)
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 48мсек, Максимальное = 51 мсек, Среднее = 49 мсек
```

```
C:\Users\fedor>
```



Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

(ip.addr == 193.109.246.49) && http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
1191	128.530097	192.168.1.101	193.109.246.49	HTTP	673	POST /index/sub/ HTTP/1.1 (application/x-www-form-urlencoded)
1258	138.831675	192.168.1.101	193.109.246.49	HTTP	673	POST /index/sub/ HTTP/1.1 (application/x-www-form-urlencoded)
1851	179.468817	192.168.1.101	193.109.246.49	HTTP	855	POST /register HTTP/1.1 (application/x-www-form-urlencoded)

Request URI: /register  
Request Version: HTTP/1.1  
Host: xn---btb1bbcge2a.xn--plai\r\n  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0\r\n  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8\r\n  
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n  
Accept-Encoding: gzip, deflate\r\n  
Referer: http://xn---btb1bbcge2a.xn--plai/register\r\n  
Content-Type: application/x-www-form-urlencoded\r\n  
Content-Length: 196\r\n  
[Content length: 196]  
Origin: http://xn---btb1bbcge2a.xn--plai\r\n  
DNT: 1\r\n  
Connection: keep-alive\r\n  
Cookie: 2profobrazovanieuzl1=1687442569\r\n  
Cookie pair: 2profobrazovanieuzl1=1687442569  
Upgrade-Insecure-Requests: 1\r\n  
Full request URI: http://xn---btb1bbcge2a.xn--plai/register  
[HTTP request 1/2]  
[Response in frame: 1901]  
[Next request in frame: 1973]  
File Data: 196 bytes  
HTML Form URL Encoded: application/x-www-form-urlencoded  
> Form item: "email" = "Email@gamil.com"  
> Form item: "password" = "superpassword"  
> Form item: "name" = "Имя"  
> Form item: "surname" = "Фамилия"  
> Form item: "nick" = "Никнейм"  
> Form item: "bd" = "1"  
> Form item: "bm" = "1"  
> Form item: "by" = "2023"  
> Form item: "gender" = "1"

Ethernet

0		15		16		31	
Destination				f8:d1:11:bb:a4:06			
Source				00:45:e2:b9:3e:6f			
Type				IPv4			

Internet Protocol Version 4

0		15		16		31			
Version	4	Header L...	20	Differentiated Services ...	0x00	Total Length	841		
Identification				0x384c (14412)	Flags	0x2	Fragment Offset	0	
Time to Live		128		Protocol		TCP		Header Checksum	0x45b6
Source Address								192.168.1.101	
Destination Address								193.109.246.49	

Transmission Control Protocol

0		15		16		31	
Source Port				51666			
Destination Port				80			

Пакеты: 2525 · Показаны: 3 (0.1%) · Потери: 0 (0.0%)

Профиль: Default

Wireshark · Следовать HTTP Поток (tcp.stream eq 103) · Беспроводная сеть

```
POST /register HTTP/1.1
Host: xn----btb1bbcge2a.xn--plai
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://xn----btb1bbcge2a.xn--plai/register
Content-Type: application/x-www-form-urlencoded
Content-Length: 196
Origin: http://xn----btb1bbcge2a.xn--plai
DNT: 1
Connection: keep-alive
Cookie: 2profobrazovanieuzll=1687442569
Upgrade-Insecure-Requests: 1

email=Email%40gamil.com&password=superpassword&name=%D0%98%D0%BC%D1%8F&surname=%D0%A4%D0%B0%D0%BC%D0%B8%D0%B8%D0%B8%D1%8F&nick=%D0%9D%D0%B8%D0%BA%D0%BD%D0%B5%D0%B9%D0%BC&bd=1&bm=1&by=2023&gender=1HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Thu, 22 Jun 2023 14:07:08 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=15
Set-Cookie: 2profobrazovanieuCoz=; path=/; expires=Tue, 22-Jun-2021 14:07:08 GMT; HttpOnly; domain=.xn----btb1bbcge2a.xn--plai
Set-Cookie: 2profobrazovanieuUSR=aXZrZnVwbm54a2dla3hXV3ptZl53eFdycmloaVM0bnFCaUIxNiFiaFh4RW8%3D%0A; path=/; expires=Fri, 23-Jun-2023 14:07:08 GMT
Set-Cookie: 2profobrazovanieuSES=WjQ0bmNMN3p0aztjaF1TNmdDZkg5aHNuN1RGVk1aXk1QWmdXNTBncFdBcWdPSVRXNjFieFhpNhpj%0AaVcyN1RuNEXabmdwT0RDMdJ4OGVBvZXOEJLXnFIVFuzSkt0SG07Y2o1TTdITlUMVRPN1QwM15C%0AWFR5RnZ5QzNaavlnZ1h6ZU1ubDgyUDNEMud2ZE1sSzBBWmZ2IXJCWkRFdmZFZUteS1pLbVNYRm1t%0AVGloUmpZbWVWS2ZsXmFSVdc0aTbtbEZDQ2s1Z0FTOHRkSV50bk1EV1RpUTizM3ZFbXFNZVFgdVA4%0AXnpYYWh5NGswQmchV3pDSGhpcSE7YWNRuTFRSHF4RVNXUEk3O1JQNk43U0N4TjRFRjdCeWRMO0RF%0AMk03VGk5Nk96YTLNR1dudmhJbDBReG4%3D%0A; path=/; expires=Fri, 23-Jun-2023 14:07:08 GMT
Location: /register2
Cache-Control: private

GET /.s/img/ma/refresh.gif HTTP/1.1
Host: xn----btb1bbcge2a.xn--plai
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
Accept: image/avif,image/webp,*/*
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://xn----btb1bbcge2a.xn--plai/register2
```

2 client pkt(s), 2 server pkt(s), 3 turn(s).

Весь диалог (3213 bytes)

Показать данные как ASCII

Найти: pass

Отфильтровать Этот Поток Печатаь Сохранить как... Назад Закрыть Справка



Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
423	41.171684	192.168.1.101	91.105.192.100	HTTP	122	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
742	77.458061	192.168.1.101	91.105.192.100	HTTP	326	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
745	77.482333	192.168.1.101	91.105.192.100	HTTP	246	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
1191	128.530097	192.168.1.101	193.109.246.49	HTTP	673	POST /index/sub/ HTTP/1.1 (application/x-www-form-urlencoded)
1258	138.831675	192.168.1.101	193.109.246.49	HTTP	673	POST /index/sub/ HTTP/1.1 (application/x-www-form-urlencoded)
1584	163.438655	192.168.1.101	91.105.192.100	HTTP	142	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
1851	179.468817	192.168.1.101	193.109.246.49	HTTP	855	POST /register HTTP/1.1 (application/x-www-form-urlencoded)

Wireshark · Экспорт · HTTP список объектов

Текстовый Фильтр: Тип Содержимого: Все Типы Содержимого

Пакет	Имя хоста	Тип Содержимого	Размер	Имя файла
1553			239 bytes	
423	91.105.192.100:80	application/x-www-form-urlencoded	68 bytes	api
742	91.105.192.100:80	application/x-www-form-urlencoded	272 bytes	api
745	91.105.192.100:80	application/x-www-form-urlencoded	192 bytes	api
1584	91.105.192.100:80	application/x-www-form-urlencoded	88 bytes	api
150	s49.ucoz.net	application/javascript	0 bytes	uutils.fcgi?a=uSD&ca=2&ug=999&isp=1&r=0.900360154194983
1960	s49.ucoz.net	application/javascript	0 bytes	uutils.fcgi?a=uSD&ca=2&ug=999&isp=1&r=0.848956423118999
1901	xn---btb1bbcge2a.xn--p1ai	application/octet-stream	0 bytes	register
1191	xn---btb1bbcge2a.xn--p1ai	application/x-www-form-urlencoded	41 bytes	sub
1258	xn---btb1bbcge2a.xn--p1ai	application/x-www-form-urlencoded	41 bytes	sub
1851	xn---btb1bbcge2a.xn--p1ai	application/x-www-form-urlencoded	196 bytes	register
1204	xn---btb1bbcge2a.xn--p1ai	image/gif	1737 bytes	ajsmi.gif
1990	xn---btb1bbcge2a.xn--p1ai	image/gif	63 bytes	refresh.gif
1994	xn---btb1bbcge2a.xn--p1ai	image/gif	622 bytes	?k=2527380212883257084&m=usreg49119321&tm=1687442828
642	xn---btb1bbcge2a.xn--p1ai	image/png	1683 bytes	rocket.png
817	xn---btb1bbcge2a.xn--p1ai	image/svg+xml	715 bytes	pass.svg
133	xn---btb1bbcge2a.xn--p1ai	text/html	53 kB	register
1928	xn---btb1bbcge2a.xn--p1ai	text/html	42 kB	register2
1206	xn---btb1bbcge2a.xn--p1ai	text/xml	166 bytes	sub
1271	xn---btb1bbcge2a.xn--p1ai	text/xml	166 bytes	sub

Сохранить Сохранить все Превью Закрыть Справка

Cookie: 2profobrazovanieuz11=1687442569  
Cookie pair: 2profobrazovanieuz11=1687442569  
Upgrade-Insecure-Requests: 1\r\n\r\n  
[Full request URI: http://xn---btb1bbcge2a.xn--p1ai/register]  
[HTTP request 1/2]  
[Response in frame: 1901]  
[Next request in frame: 1973]  
File Data: 196 bytes

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

- > Form item: "email" = "Email@gamil.com"
- > Form item: "password" = "superpassword"

Строка 1, столбец 1

Identification	Flags	Fragment Offset
0x384c (14412)	0x2	0

Time to Live 128 Protocol TCP Header Checksum 0x45b6

Source Address 192.168.1.101

Пакеты: 2525 · Показаны: 7 (0.3%) · Потеряно: 0 (0.0%) Профиль: Default

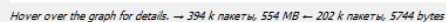
4\*. На сайте <https://launchpad.net/ubuntu/+archivemirrors> представлены зеркала с образами Убунту по странам. Скачайте файл `ls-IR.gz` из Чили и с Яндекса. Снимите два дампа для каждого скачивания. Проанализируйте скорость скачивания и посмотрите `tcptrace`. Прикиньте средний RTT и поищите максимальный RWND для скачивающего.

Предоставить скриншоты графиков скорости и `tcptrace`. Есть ли разница? В чем она?

### Загрузка на яндекс диск:

The screenshot displays the Yandex 360 web interface. At the top, there's a navigation bar with the Yandex 360 logo, a search bar labeled 'Поиск в моём Диске', and icons for various services: Почта, Диск, Документы, Календарь, Премиум, and Ещё. Below this, the left sidebar contains navigation options: Загрузить, Создать, Последние, Файлы, Фото, Альбомы, Общий доступ, Семья, История, Загрузки, and Корзина. A yellow box in the sidebar indicates 'Свободно 9,48 ГБ из 10 ГБ' and offers '+1 ТБ за 399 ₽'. The main content area is titled 'Последние файлы' and shows a file named 'webinar\_92978421970\_0.MP4' with a thumbnail. A blue notification banner at the bottom right states 'Все файлы загружены' and includes a 'Поделиться' button. The footer contains links for 'Справка и поддержка', 'Блог', 'Разработчикам', 'Вакансии', 'Условия использования', and 'Участие в исследованиях'.

```
> Frame 1600: 66 bytes on wire (5
> Ethernet II, Src: CyberTAN_b9:3
> Internet Protocol Version 4, Sr
0100 .... = Version: 4
.... 0101 = Header Length: 20
> Differentiated Services Field
Total Length: 52
Identification: 0x75b5 (3013)
> 010. .... = Flags: 0x2, Don't
...0 0000 0000 0000 = Fragment
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x99eb [val
[Header checksum status: Unve
Source Address: 192.168.1.101
Destination Address: 141.8.156
```



Тип Пропускная способность

Мышь ☒ перетягивание ☐ масштаб

☒ Длина Сегмента ☒ Пропускная способность ☐ Полезная пропускная способность

Окно МА (с) 1,000000

Поток 87  Переключить Направление

Сброс

Сохранить Как...    Закрыть    Справка

Internet Protocol Version 4			
0	15	16	3
Version 4	Header Length 20	Differentiated Services 0x00	Total Length 52
Identification 0x75b5 (30133)		Flags 0x2	Fragment Offset 0

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

ip.addr==192.168.1.101&&ip.addr==141.8.156.13

No.	Time	Source	Destination	Protocol	Length	Info
349572	108.756616	192.168.1.101	141.8.156.13	TCP	1464	56346 → 443 [ACK] Seq=316292668 Ack=5146 Win=130304 Len=1410 [TCP segment of a reassembled PDU]
349573	108.767805	141.8.156.13	192.168.1.101	TCP	54	443 → 56346 [ACK] Seq=5146 Ack=316109907 Win=9662464 Len=0
349574	108.767843	192.1				Номера Последовательностей (tcptrace) для 192.168.1.101:56346 → 141.8.156.13:443
349575	108.767843	192.1				
349576	108.768226	141.8				
349577	108.768242	192.1				
349578	108.768242	192.1				
349579	108.768880	141.8				
349580	108.768923	192.1				
349581	108.768923	192.1				
349582	108.769070	141.8				
349583	108.769087	192.1				
349584	108.769087	192.1				
349585	108.769805	141.8				
349586	108.769805	141.8				
349587	108.769862	192.1				
349588	108.769862	192.1				
349589	108.769862	192.1				
349590	108.769862	192.1				
349591	108.769998	141.8				
349592	108.770793	141.8				
349593	108.770793	141.8				
349594	108.770793	141.8				

> Frame 349572: 1464 bytes on wire (Ethernet II, Src: CyberTAN\_b9:3...)

> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 141.8.156.13

> 0100 .... = Version: 4

> .... 0101 = Header Length: 20 bytes

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

> Total Length: 1450

> Identification: 0xf2f3 (62195)

> 010. .... = Flags: 0x2, Don't Fragment

> ...0 0000 0000 0000 = Fragment Offset: 0

> Time to Live: 128

> Protocol: TCP (6)

> Header Checksum: 0x1737 [valid]

> [Header checksum status: Unverified]

> Source Address: 192.168.1.101

> Destination Address: 141.8.156.13

> Transmission Control Protocol, Src Port: 56346, Dst Port: 443, Seq: 316292668, Ack: 5146, Len: 1410

Номера Последовательностей (tcptrace) для 192.168.1.101:56346 → 141.8.156.13:443

Беспроводная сеть

Hover over the graph for details: → 394 k пакеты, 554 MB → 202 k пакеты, 5744 bytes

Тип Времени / Последовательность (tcptrace)

Мышь ☒ перетягивание ☐ масштаб

☐ Выбрать SACKs

Поток 87 Переключить Направление

Сброс

Сохранить Как... Заккрыть Справка

Internet Protocol Version 4

Version 4	Header Length 20	Differentiated Services Field 0x00	Total Length 1450
Identification 0xf2f3 (62195)			Flags 0x2
			Fragment Offset 0

Пакеты: 600524 · Показаны: 596866 (99.4%) · Потеряно: 0 (0.0%)

Профиль: Default

← → ↺

https://disk.yandex.ru/client/recent

130% ☆

🔍 яндекс диск

→ 📁 ⬇️ 📌 12 📄 ☰

Импорт закладок... Шаг 1 · Работа с моде... My bookmarks Jupyter Обучение | GeekBrain... Обучение | GeekBrain... Тест по Итоговая атте... Полный курс по Djan... Тесты | GeekBrains - о... Byffer GitHub vergeev/django-mode... М Руководство часть 9: ... >>

Я 360

Поиск в моём Диске 🔍

Почта Диск Документы Календарь Премиум Ещё ⚙️ 🌐

📤 Загрузить

✚ Создать

🕒 Последние

📁 Файлы

📷 Фото

📁 Альбомы

👥 Общий доступ

👤 Семья

🕒 История

⬇️ Загрузки

🗑 Корзина

📶 Свободно 9,48 ГБ из 10 ГБ

+1 ТБ за 399 ₽

📱 Установить приложение

Последние файлы

Сегодня

webinar\_421970\_1

📤 Поделиться

📁 Добавить в альбом

⬇️ Скачать

A| Переименовать

📁 Переместить

📄 Копировать

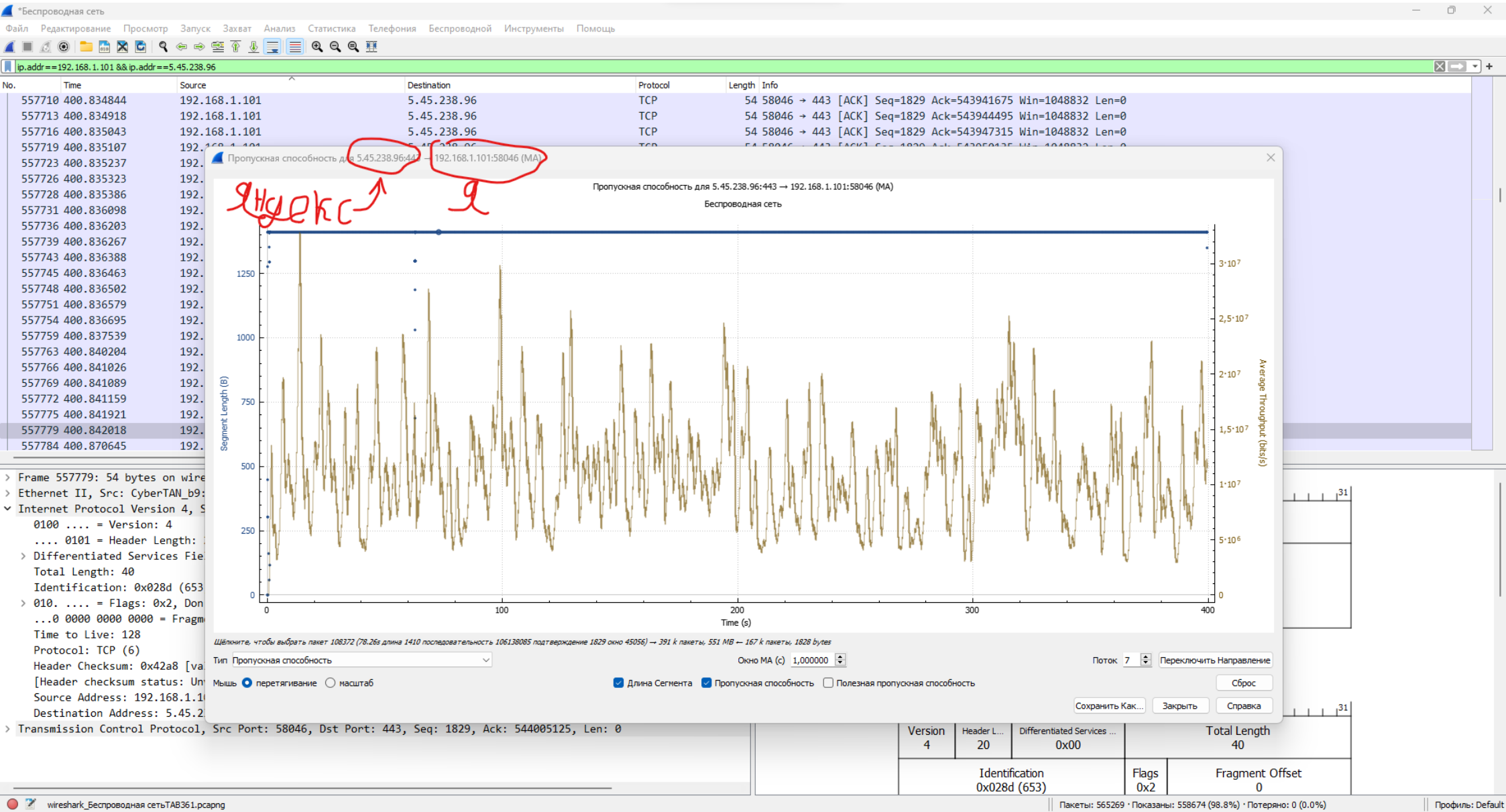
📄 Перейти к файлу

🕒 История изменений

🗑 Удалить

Справка и поддержка Блог Разработчикам Вакансии Условия использования Участие в исследованиях

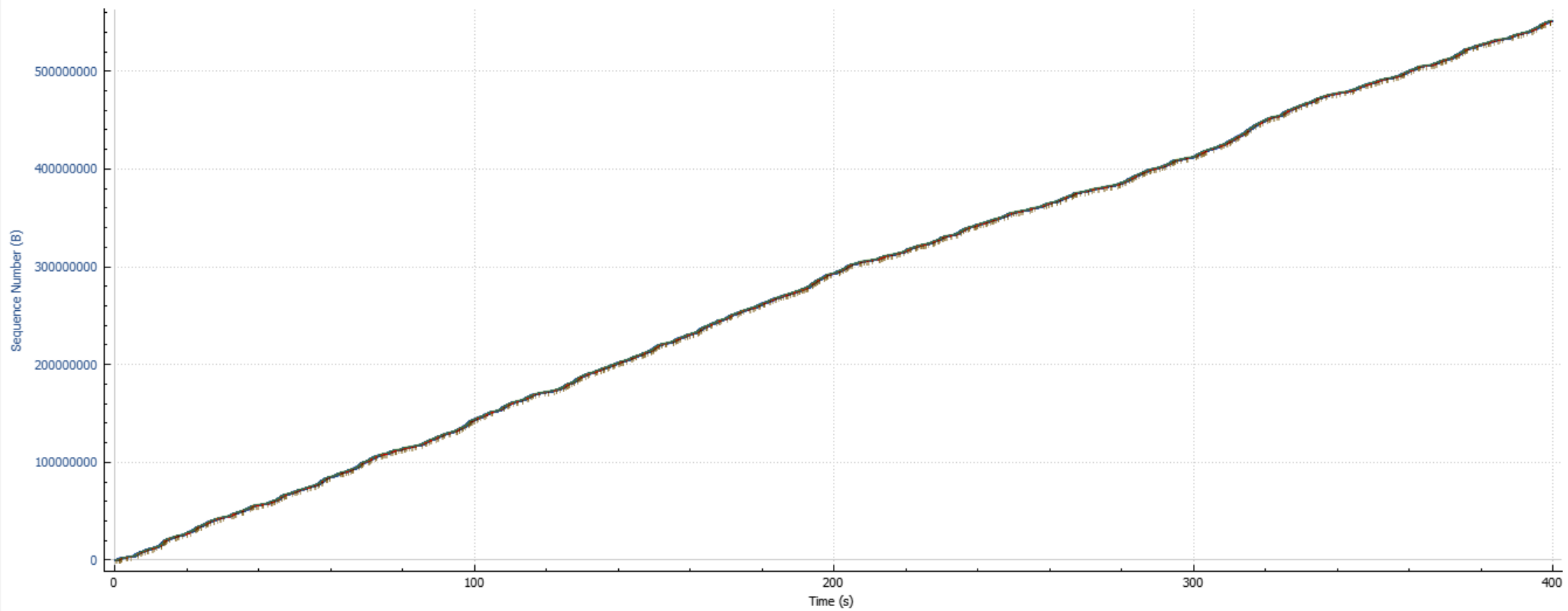
© 2012—2023 «Яндекс» 🇷🇺 RU





Номера Последовательностей (tcptrace) для 5.45.238.96:443 → 192.168.1.101:58046

Беспроводная сеть



Hover over the graph for details. → 391 k пакеты, 551 MB ← 167 k пакеты, 1828 bytes

Тип Время / Последовательность (tcptrace)

☐ Выбрать SACKи

Поток 7

Переключить Направление

Мышь ☒ перетягивание ☐ масштаб

Сброс

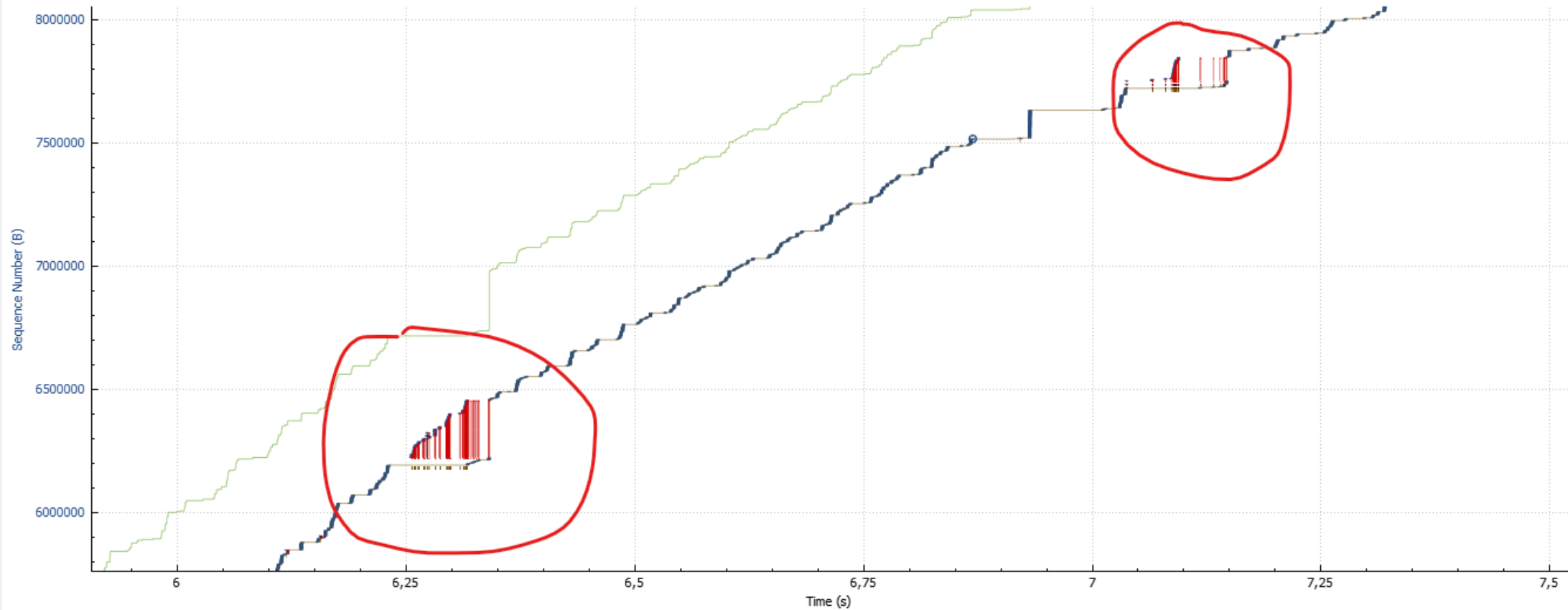
Сохранить Как...

Закрыть

Справка

Номера Последовательностей (tcptrace) для 5.45.238.96:443 → 192.168.1.101:58046

Беспроводная сеть



Щёлкните, чтобы выбрать пакет 7889 (12.23s длина 1410 последовательность 7514972 подтверждение 1829 окно 45056) → 391 k пакеты, 551 MB ← 167 k пакеты, 1828 bytes

Тип

☐ Выбрать SACKи

Поток

Мышь ☒ перетягивание ☐ масштаб