

Урок 5. Основы компьютерных сетей. Транспортный уровень. UDP и TCP.

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

The screenshot shows Wireshark capturing an SMTP message. The packet list shows a packet of 3131 bytes on the wire (25048 bits) captured on interface unknown, i. The packet details pane shows the SMTP message structure, including the subject 'SMTP Ping' and the message body. The packet bytes pane shows the raw data of the message body, which is a base64-encoded string.

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

The screenshot shows Wireshark capturing an ICMP echo request (ping) to 8.8.8.8. The packet list shows a packet of 106 bytes on the wire (848 bits) captured on interface \Device\NPF_{2091C...}. The packet details pane shows the ICMP message structure, including the type 'Echo (ping) request' and the sequence number 0. The packet bytes pane shows the raw data of the ICMP message.

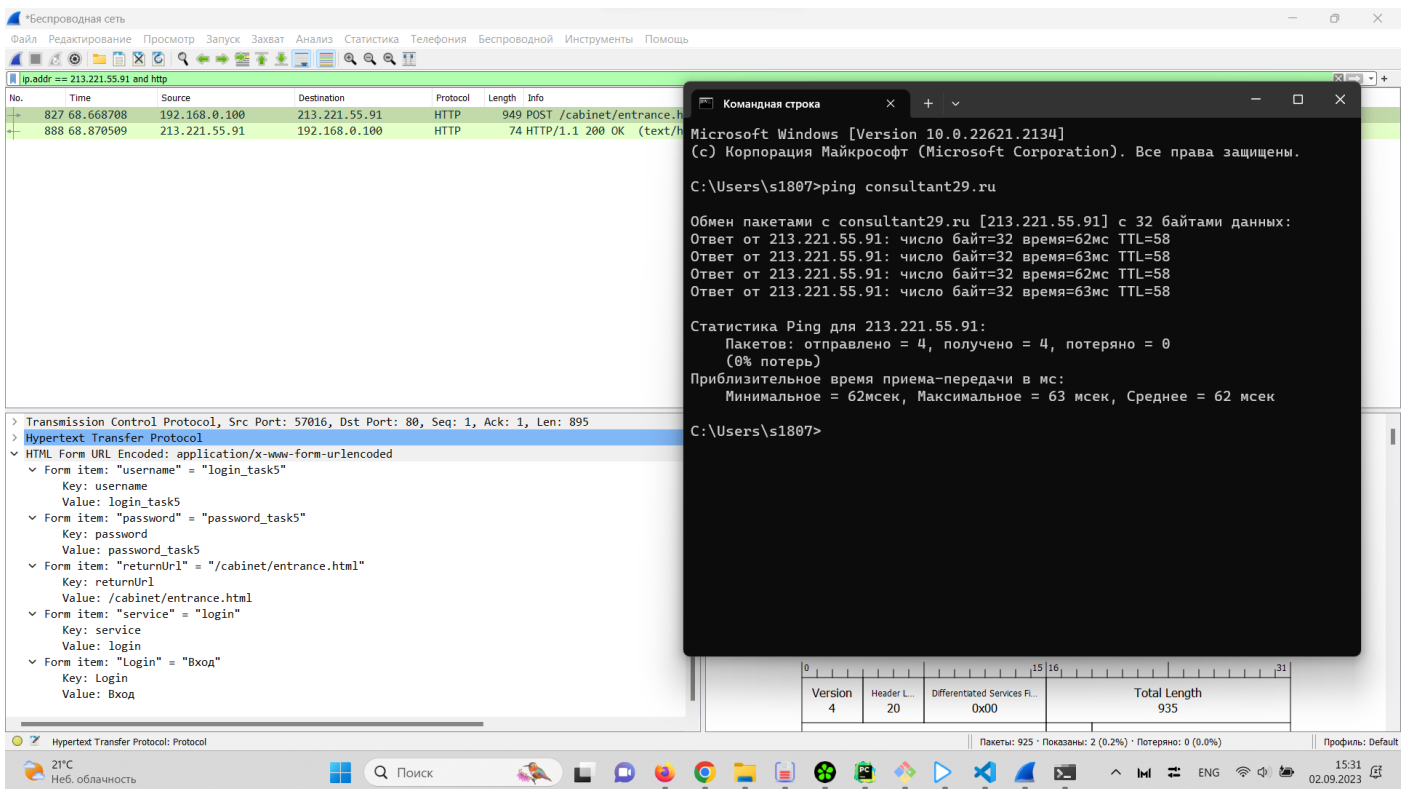
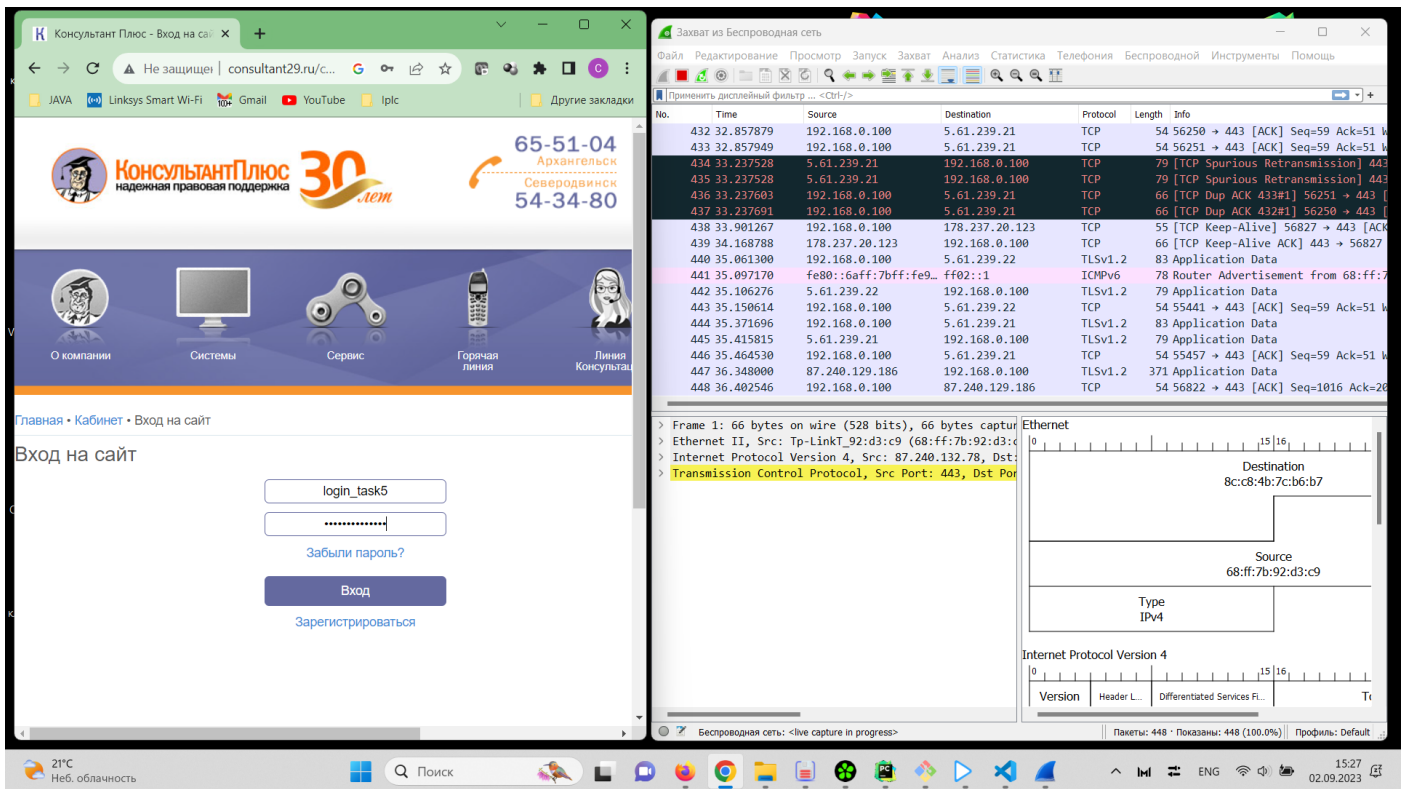
- Пакет №16 - первый из трех ICMP пакетов с ttl = 1 хоп, т.е. пакет дойдет до домашнего роутера и будет уничтожен.
- Пакет №17 - ответ от домашнего роутера
- Пакет №43 - первый из трех ICMP пакетов с ttl = 2 хоп, т.е. пакет дойдет через домашний роутер до роутера провайдера и будет уничтожен.
- Пакет №49 - ответ от роутера провайдера

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Файл', 'Редактирование', 'Просмотр', 'Запуск', 'Захват', 'Анализ', 'Статистика', 'Телефония', 'Беспроводной', 'Инструменты', and 'Помощь'. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. Packet 964 is selected, which is an ICMP Echo (ping) reply from 192.168.0.100 to 8.8.8.8.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, the Internet Protocol Version 4 header, and the ICMP Echo (ping) data.
- Packet Bytes:** Displays the raw packet data in hexadecimal and ASCII format.

The status bar at the bottom indicates that 970 packets have been captured, with 93 (9.6%) displayed and 0 (0.0%) lost. The system clock shows 15:17 on 02.09.2023.

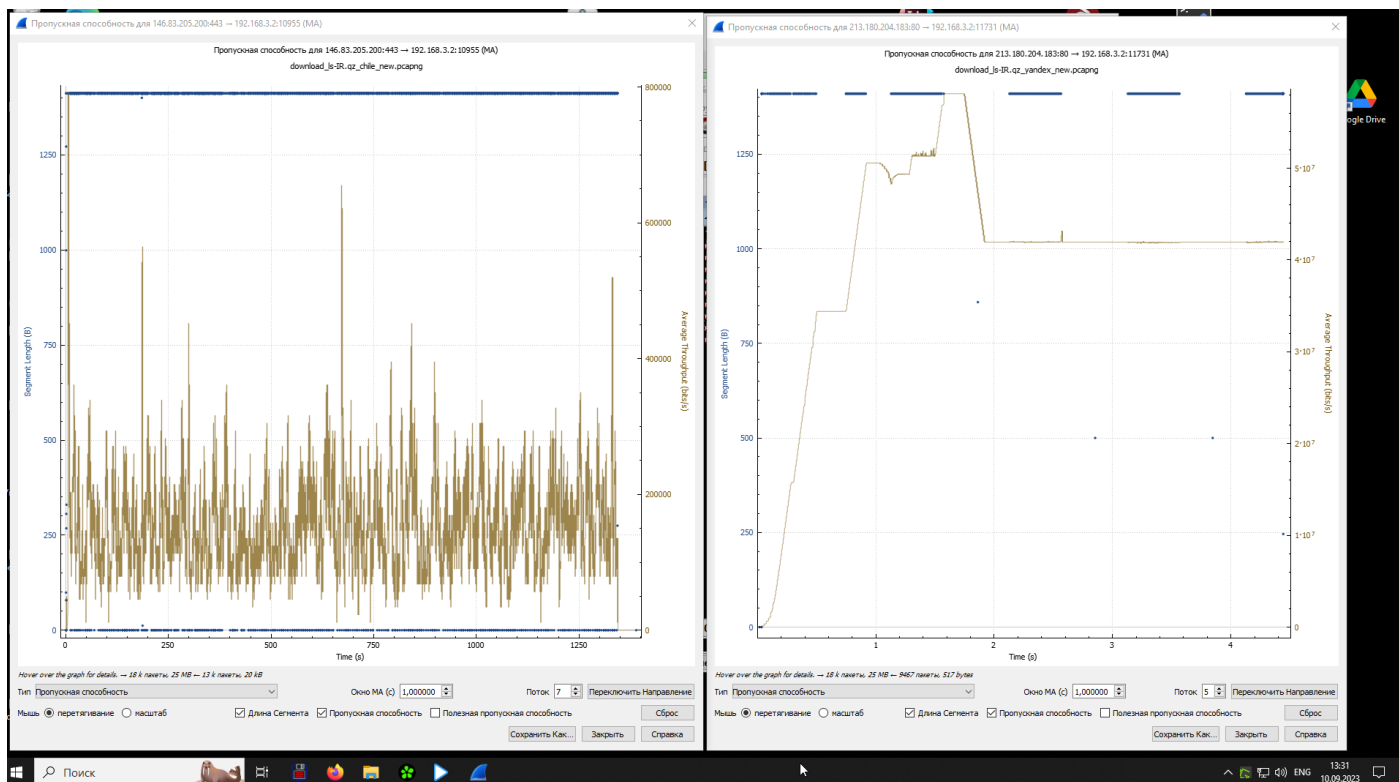
- Пакет №961 - первый из трех пингов с ttl = 20 хоп, т.е. пакет дойдет до роутера с IP 8.8.8.8 и будет уничтожен.
3. Закрепите навыки фильтрования. Найдите еще один сайт без шифрования с возможностью ввода логина/пароля. (можно в гугл настроить соответствующую выдачу по запросу с ключом “-inurl:https” в конце). Перехватите их в Wiresharke, построив фильтр.



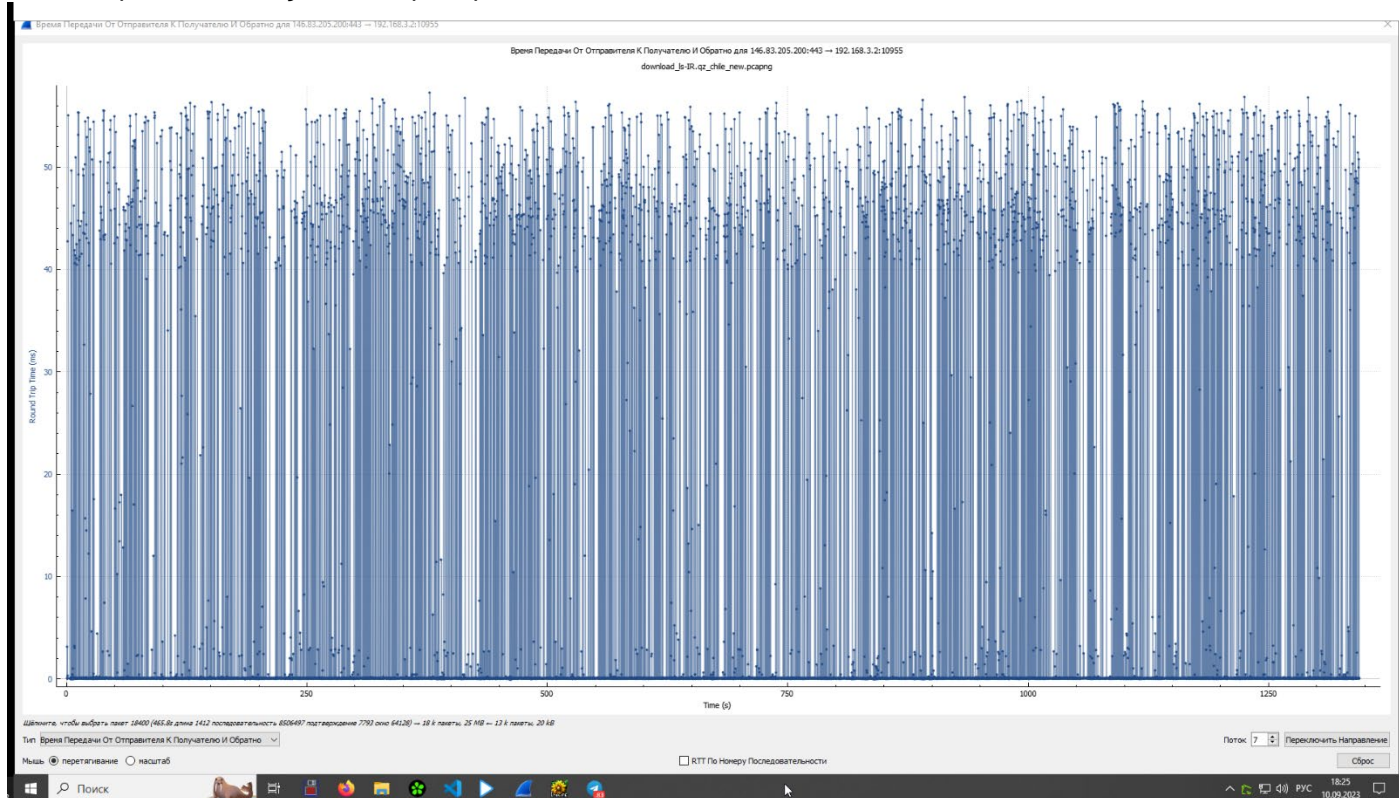
4*. На сайте <https://launchpad.net/ubuntu/+archivemirrors> представлены зеркала с образами Убунту по странам. Скачайте файл ls-IR.gz из Чили и с Яндекса. Снимите два дампа для каждого скачивания. Проанализируйте скорость скачивания и посмотрите tcptrace. Прикиньте средний RTT и поищите максимальный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

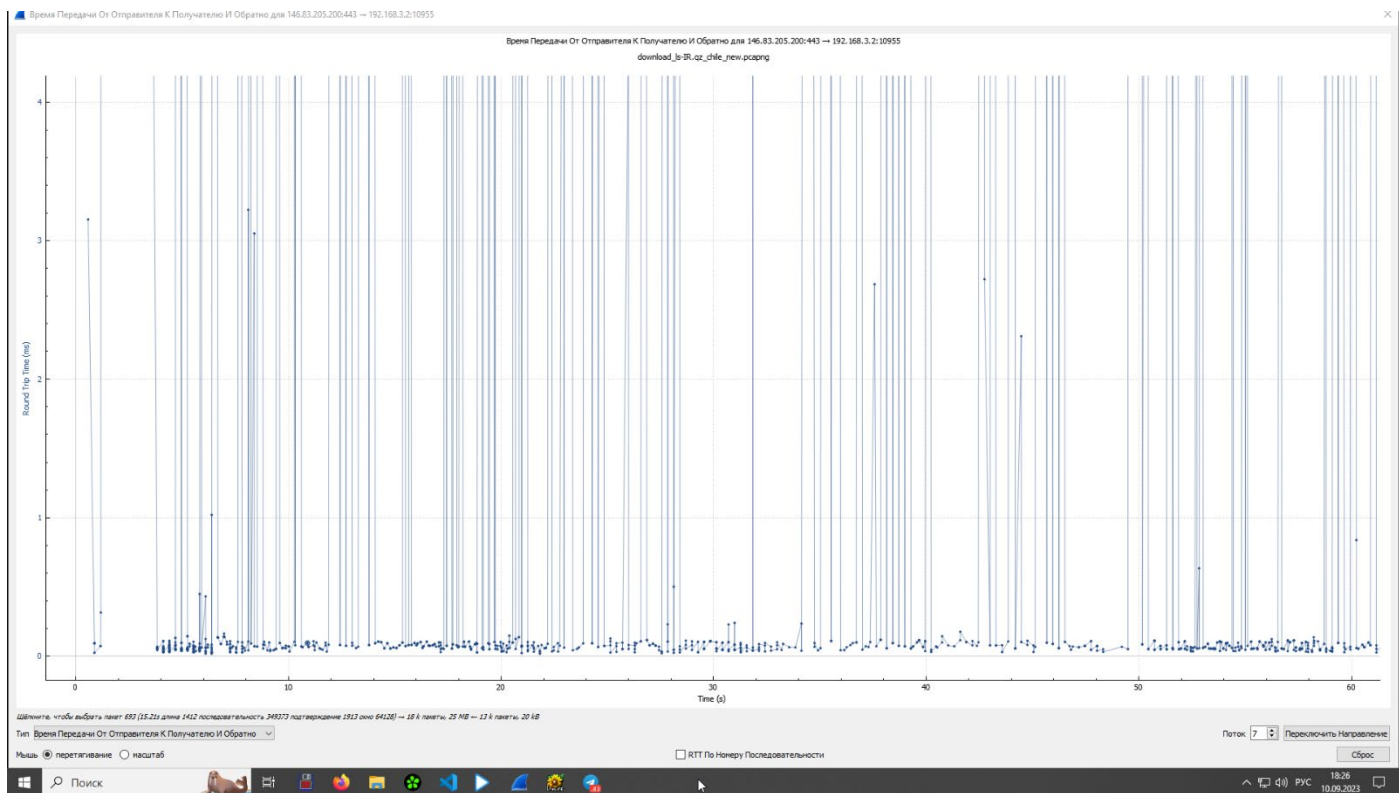
Предоставить скриншоты графиков скорости и tcptrace. Есть ли разница? В чем она?

- Скорость скачивания из Чили в среднем около 200 kbps, с яндекса в среднем около 42 Mbps, в пике до 60 Mbps. Разница скоростей из Чили и яндекса в 200 раз. Что обусловлено расстоянием, кол-вом и загруженностью промежуточного оборудования между конечными отправителем и получателем.

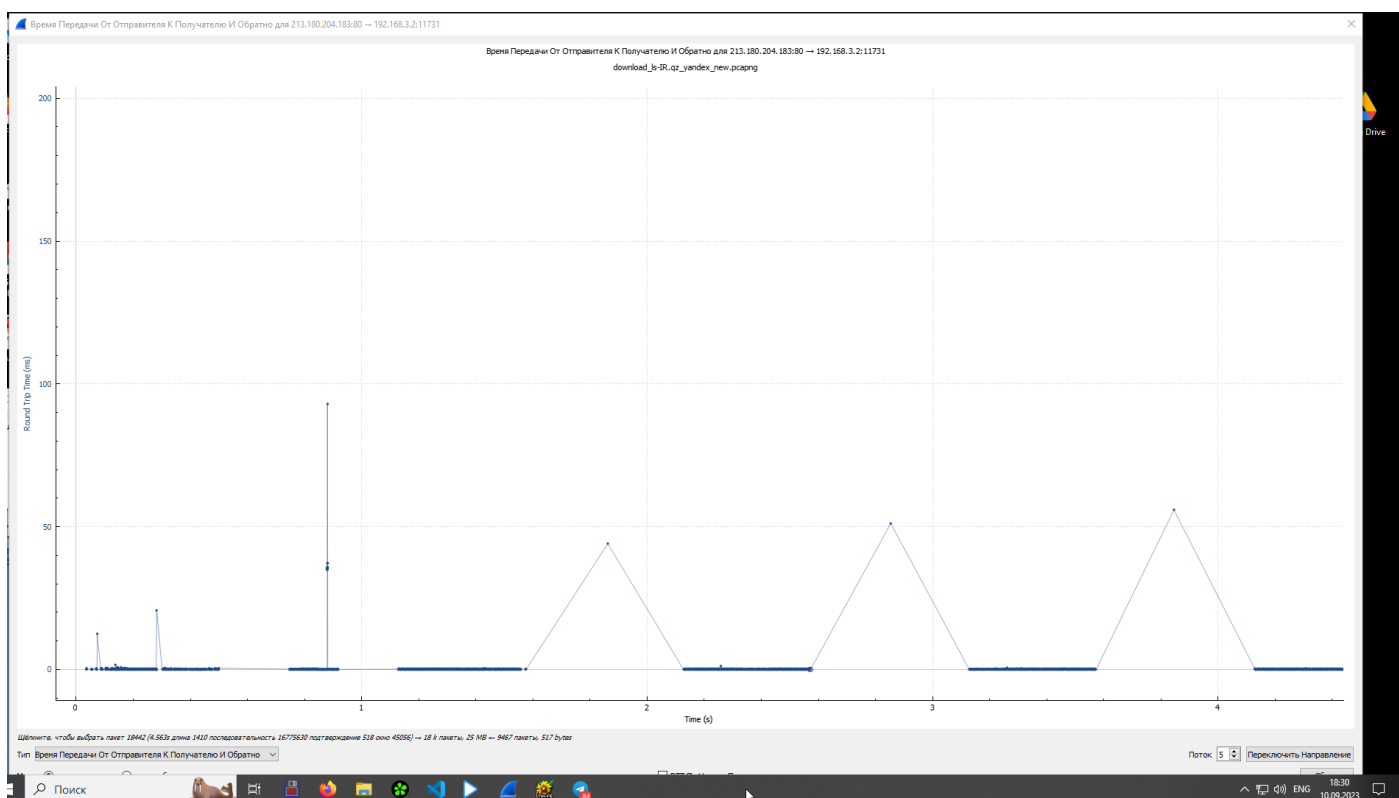


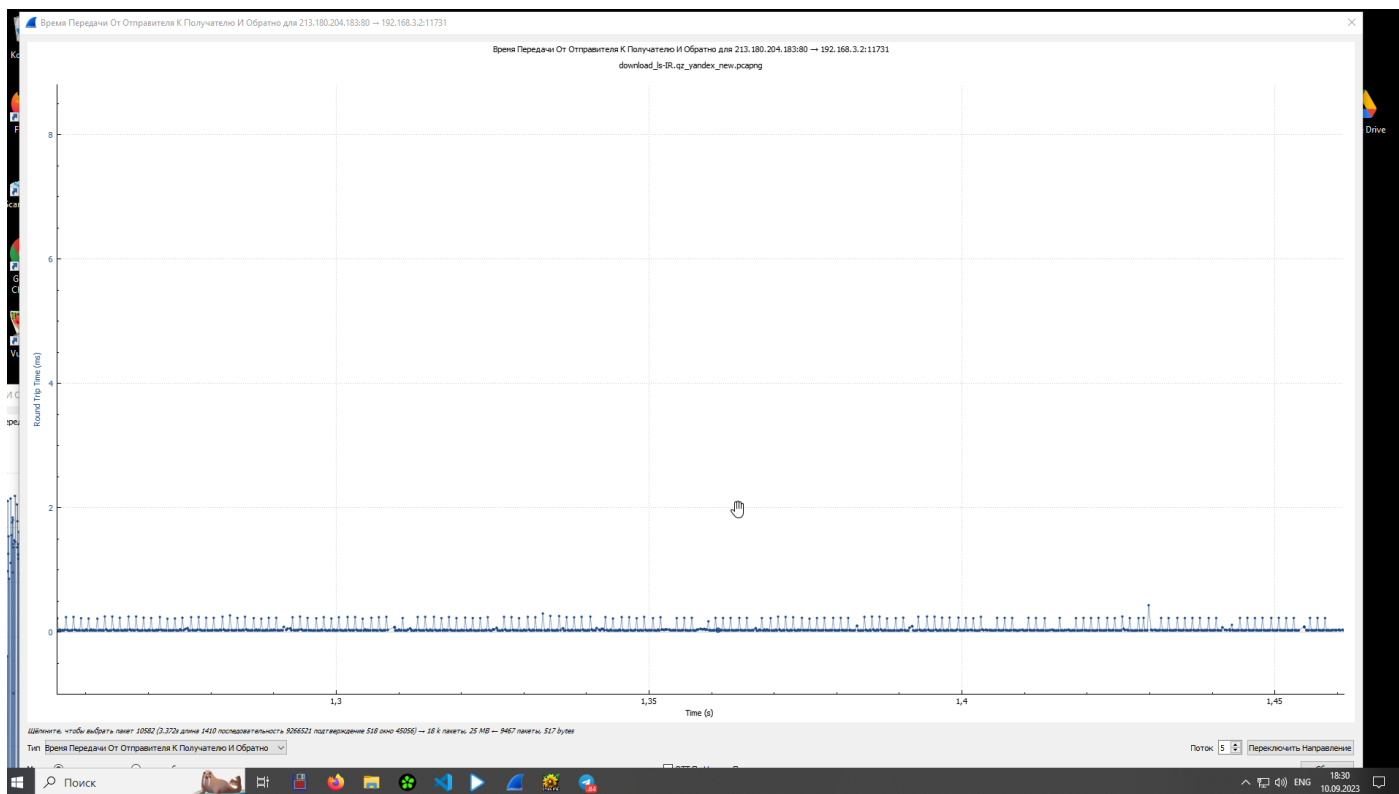
- Средний RTT у Чили примерно 20 ms



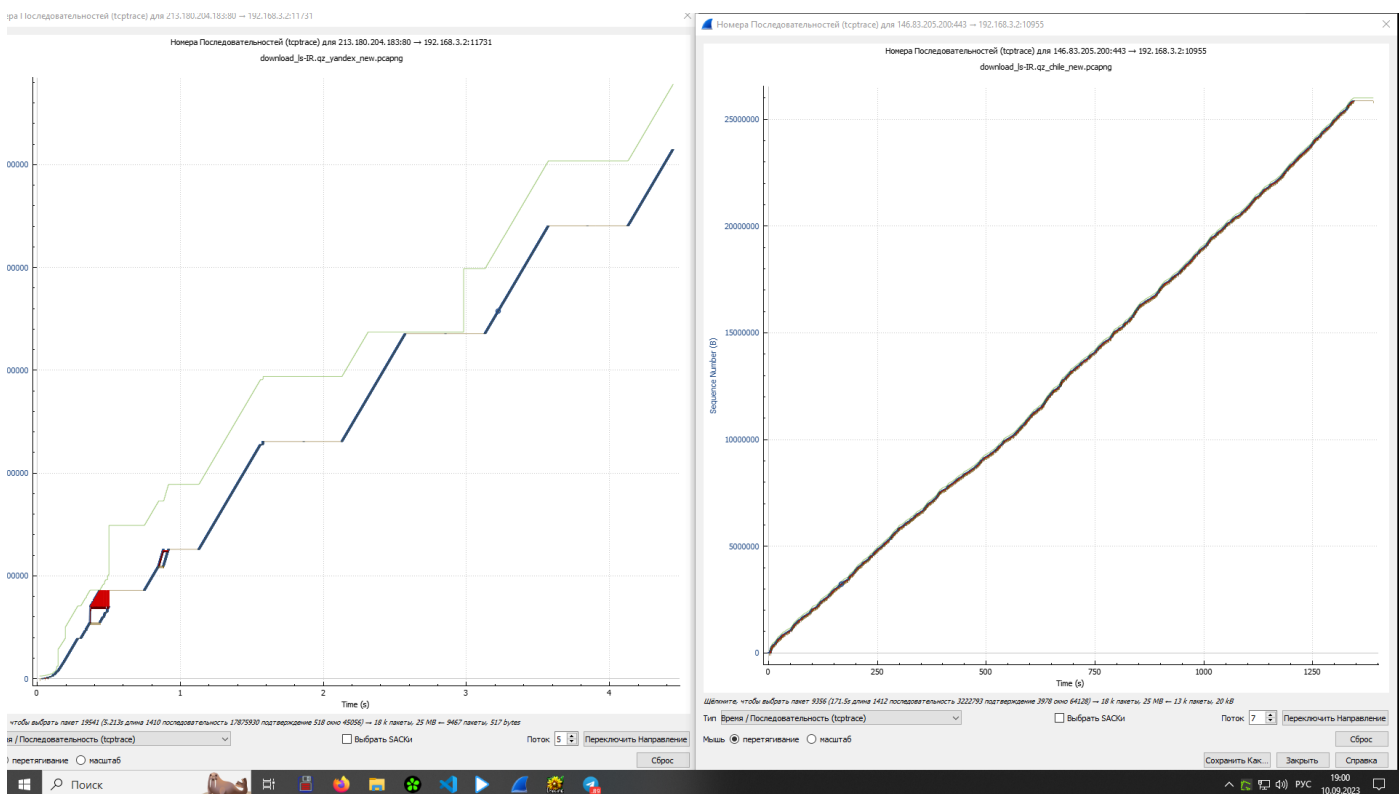


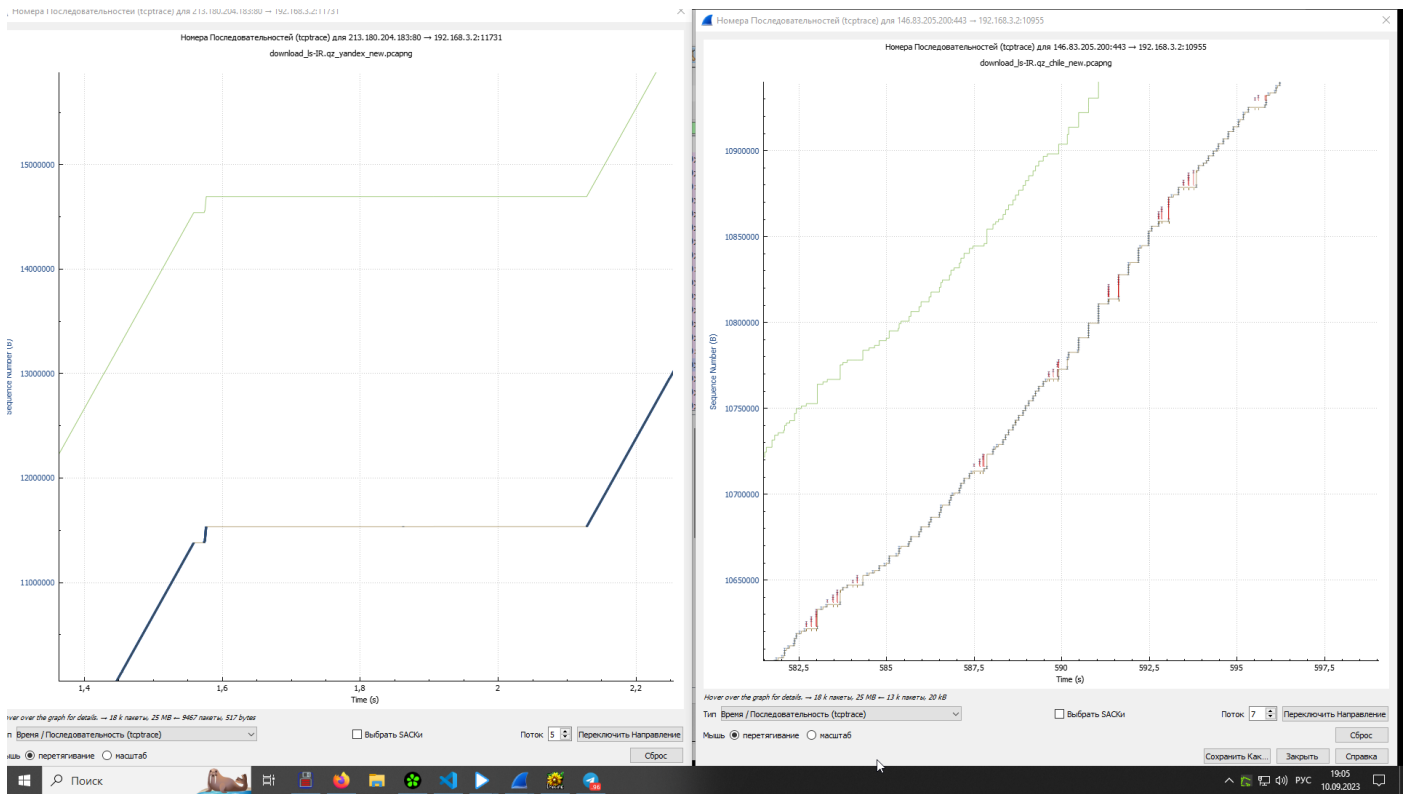
- Средний RTT у yandex примерно 0.4 ms, что примерно в 50 раз меньше чем у Чили



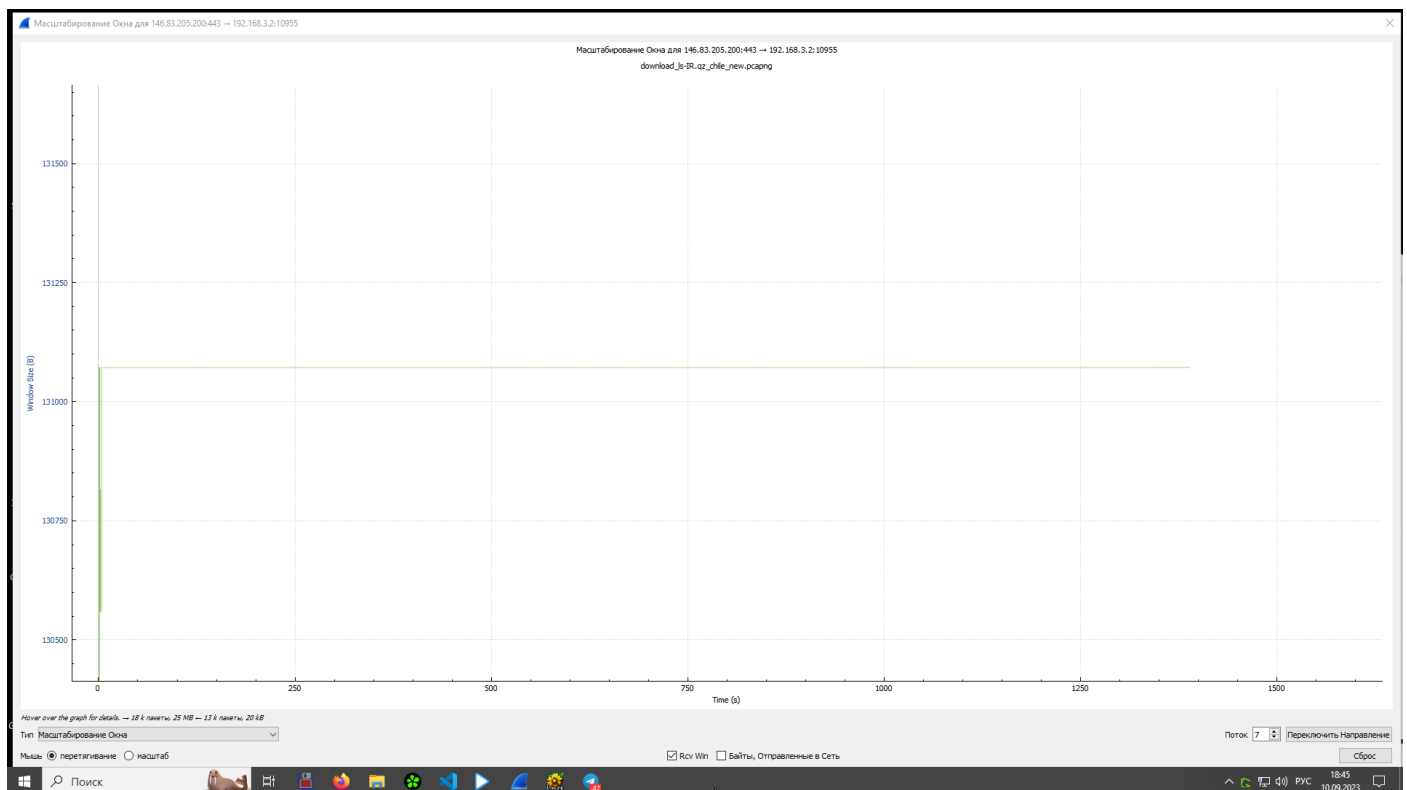


- tcptrace - из графиков видно, что ширина окна у Чили мизирная, почти сливается, что говорит о малой пропускной способности канала и невозможности нарастить объем передаваемых данных.





- RWND у Чили росло только на старте до значения 131070 на 4 секунды и далее оставалось на одном уровне, что говорит о загрузенности канала на стороне отправителя (или промежуточного оборудования) и невозможности увеличить ширину канала



- RWND у yandex максимальный рост окна пришелся на 0,5 секунду до значения 3300000, что примерно в 30 раз больше чем у Чили

