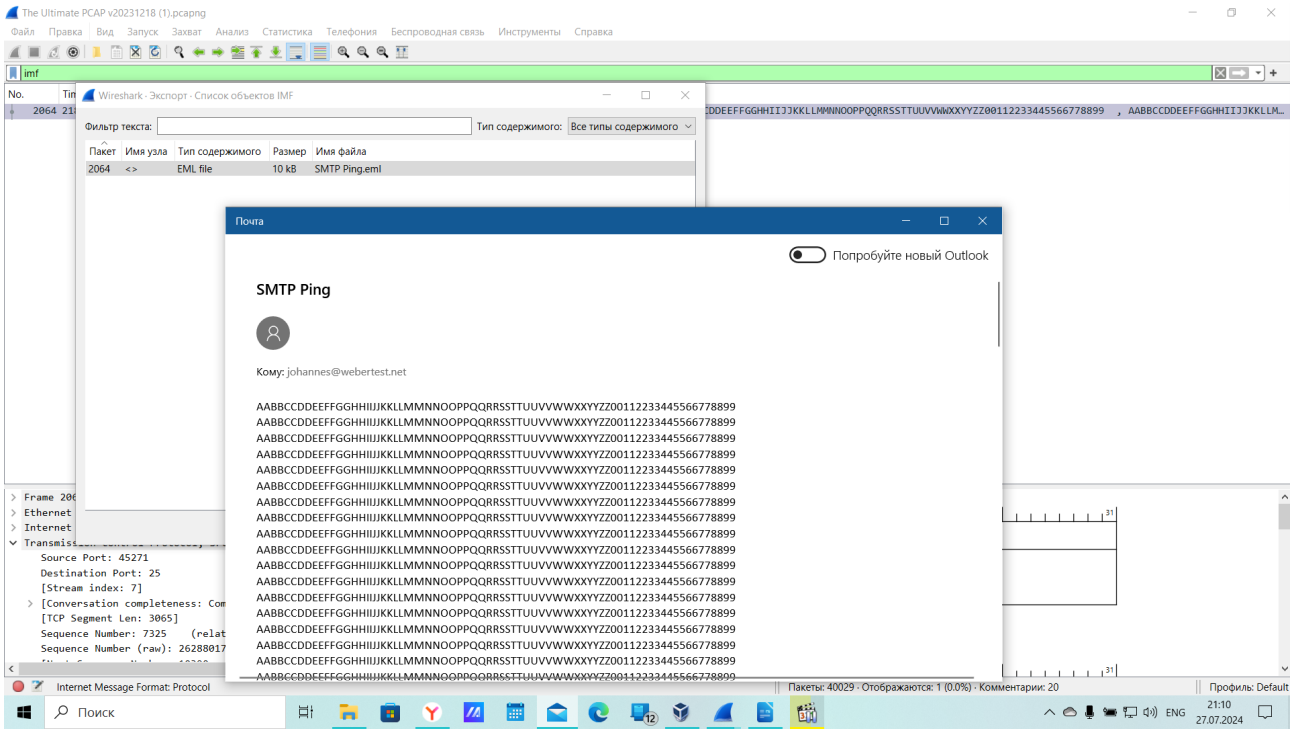
Урок 5. Основы компьютерных сетей. Транспортный уровень. UDP и TCP.

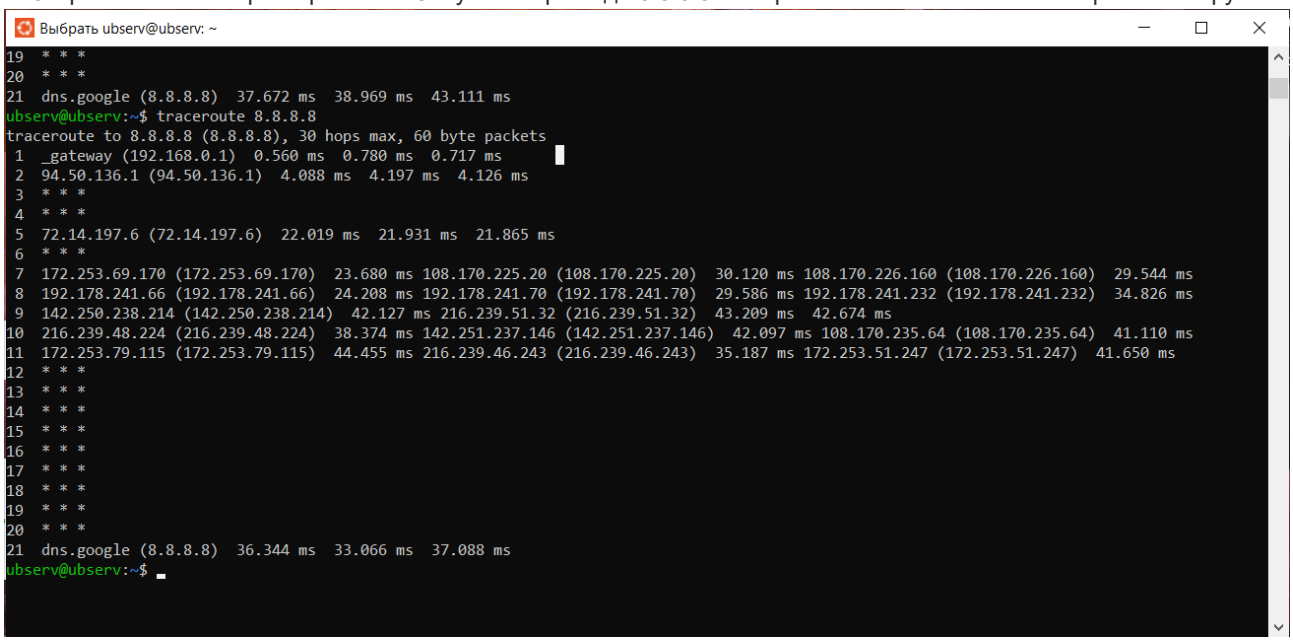
(29.07.24, потом перевели на курс devops)

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



Кому: johannes@webertest.net

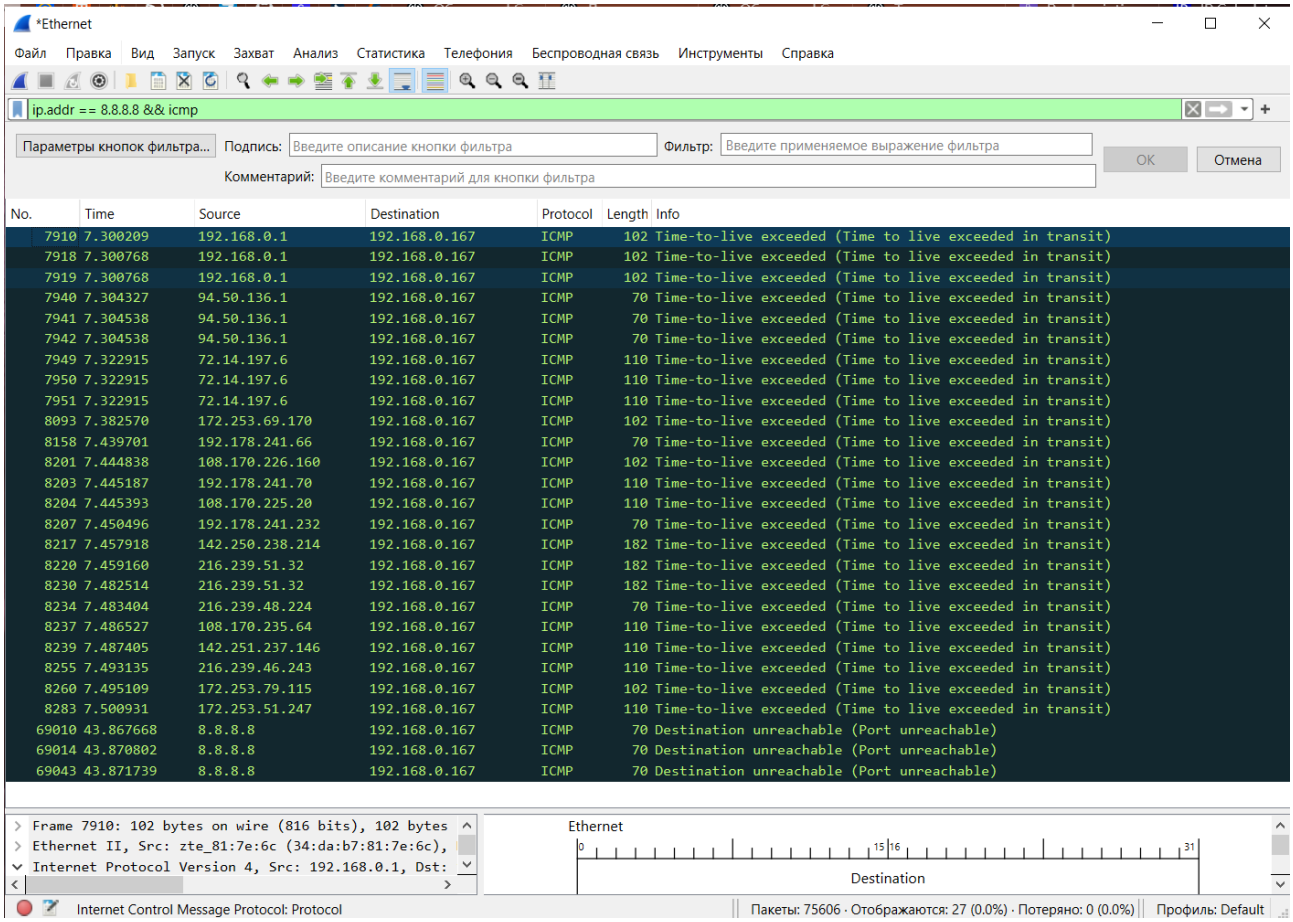
2. Закрепите навыки фильтрования. Запустите трейс до 8.8.8.8. И перехватите его в Wireshark. Проанализируйте.



tracert проходя через создает запросы на целевой адрес
на шаге 3,4, 6 устройства не хотят отвечать, скорее всего перезруз по запросу (предполагаю что это места «ветвлений» - домовые маршрутизаторы, которые не дают ответ по сетям)

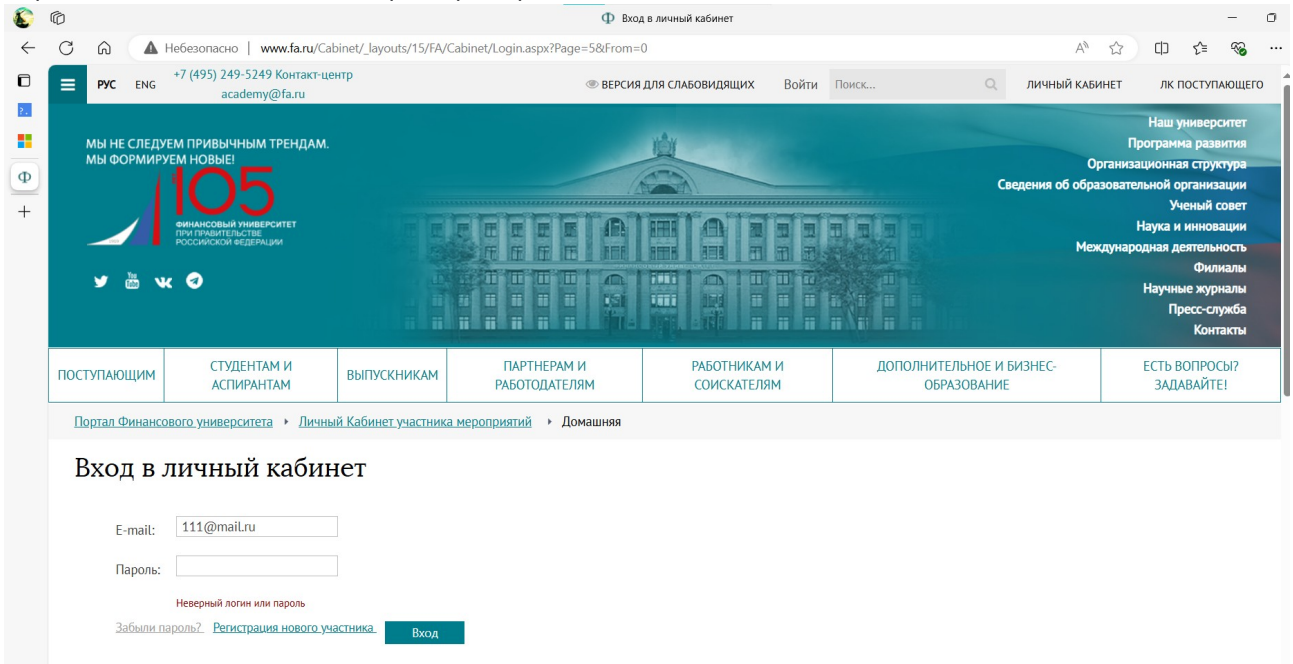
По другим шагам, можно видеть отклик до 45 мс, скорее всего временя ожидания не должно его превышать.

Каждый шаг идет по три запроса,но с 7 по 11 запросы на разные адреса — скорее всего сеть закольцована дважды, имеет как минимум два запасных маршрута

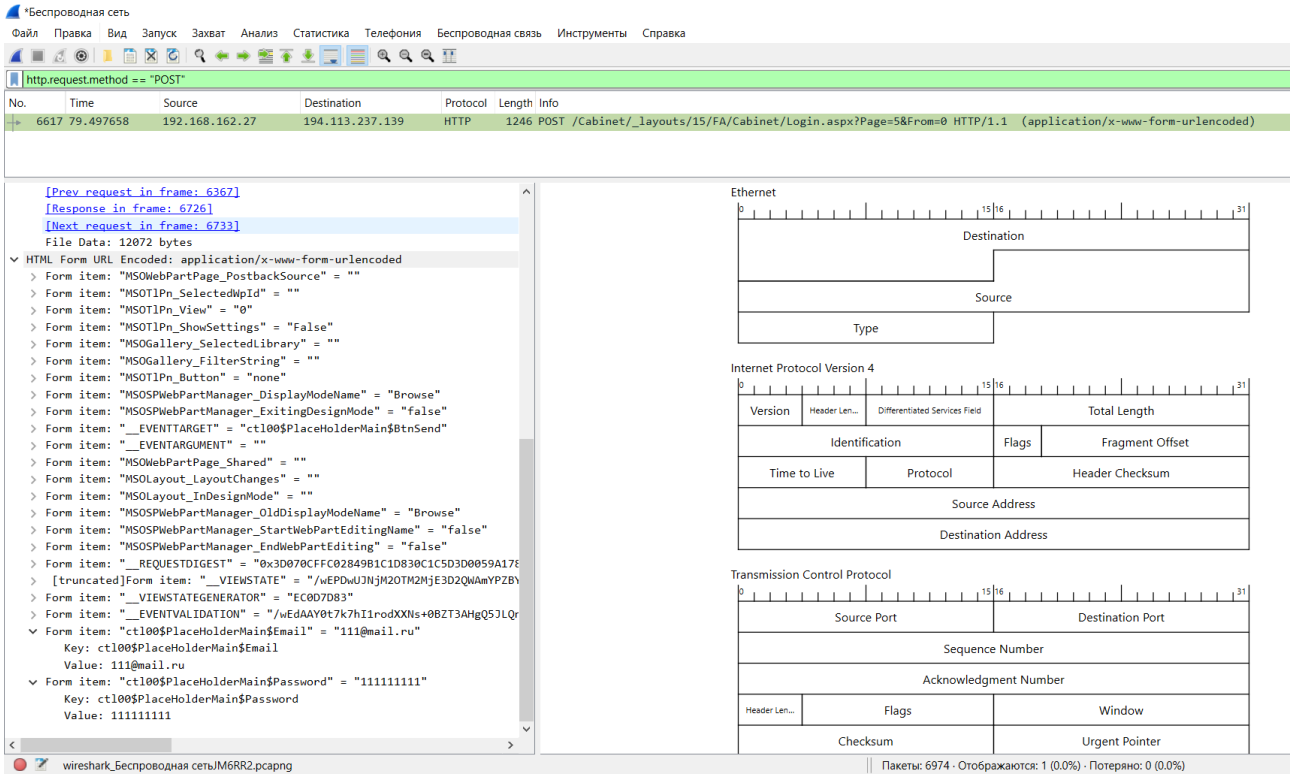


на 9 шаге целевой адрес определен, о чем говорит запись о недоступности порта. В других шагах — запись «первышено время жизни», из предыдущего скрина оно примерно 45 мс.

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.



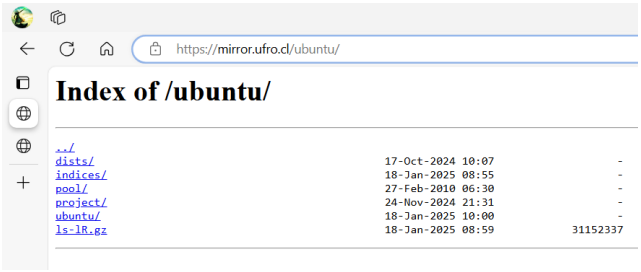
shark



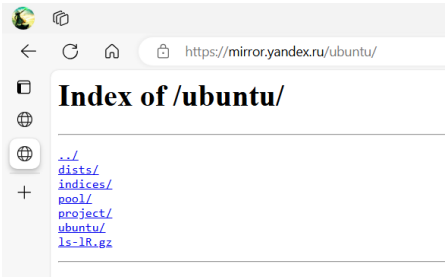
просматриваем почту и пароль

4*. На сайте https://launchpad.net/ubuntu/+archivemirrors представлены зеркала с образами Убунту по странам. Скачайте файл ls-lR.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?

(18.01.25, продолжаю после повторения предыдущих занятий)



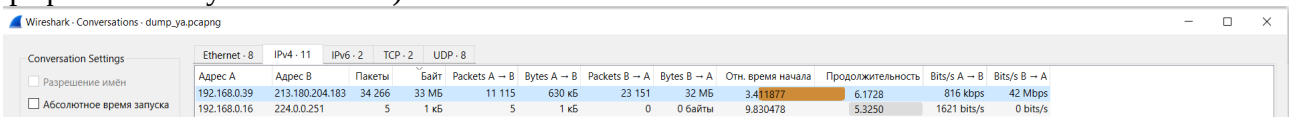
Чили



Яндекс

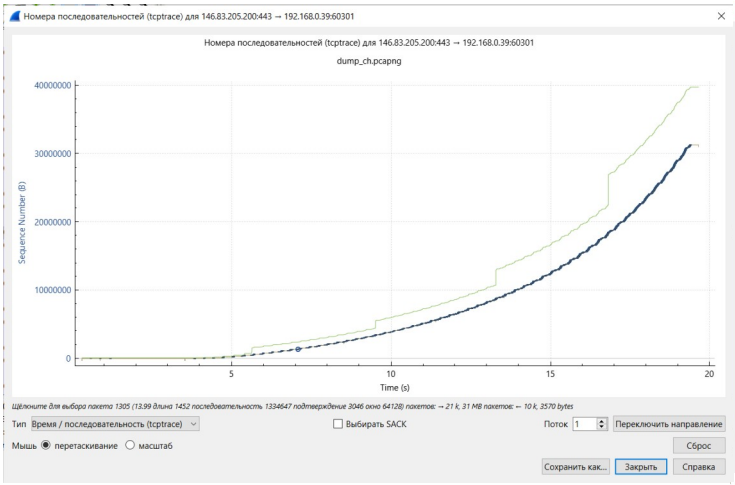
дампы скачиваний выложены на https://github.com/196-PetrT/base_cmp_net/tree/main/less_4_1

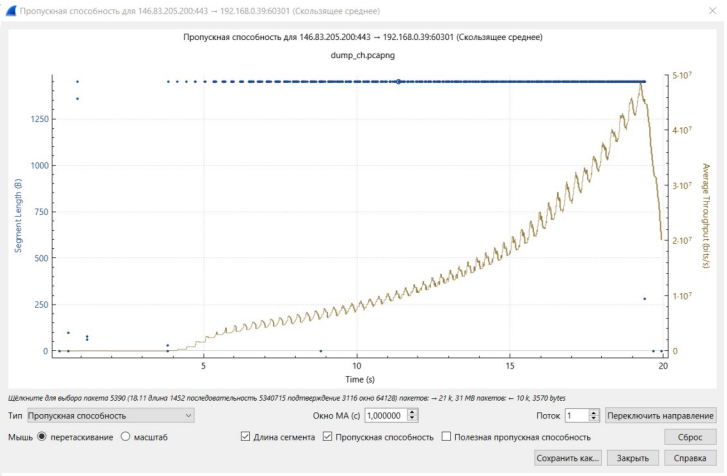
(не совсем понял для чего для каждого скачивания делать по два дампа, если tcptrace дает график по всему скачиванию)

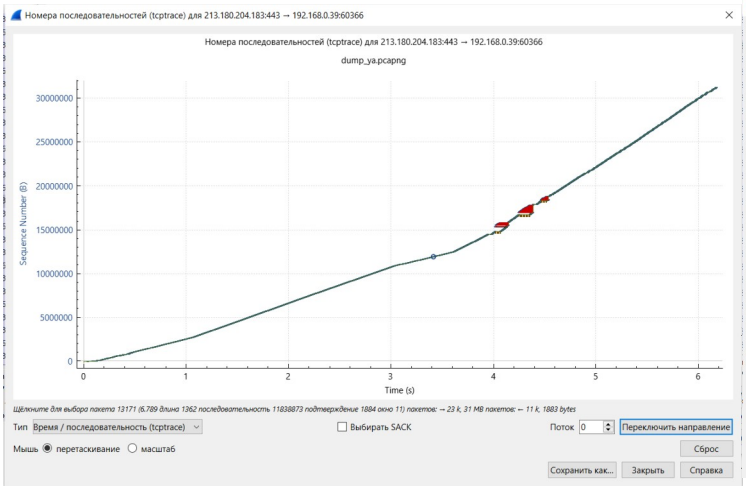


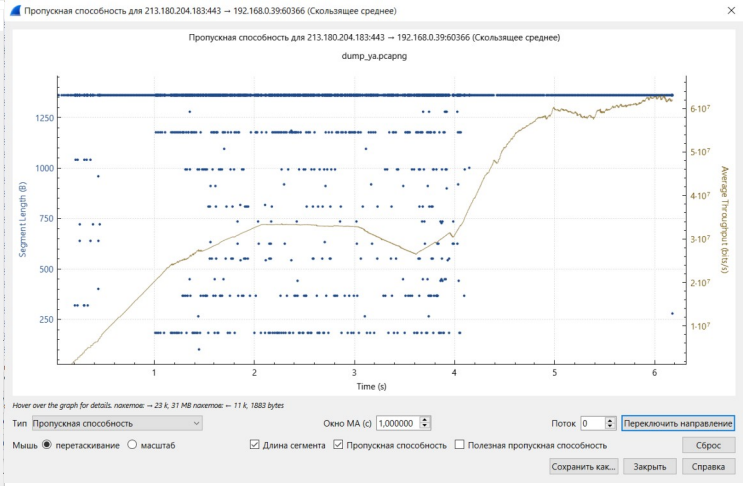
для каждого дампа сделал выборку в «диалогах» по B-->A ,

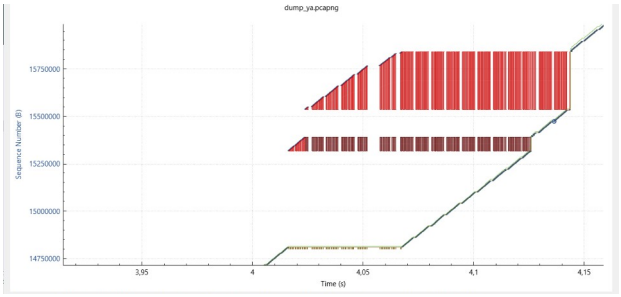
и просмотрел графики временных потоков (на графиках чили — все как по учебнику)), но медленнее). С сервера чили разгон загрузки, и соответственно время, дольше. Макс.скорость примерно одинаковая



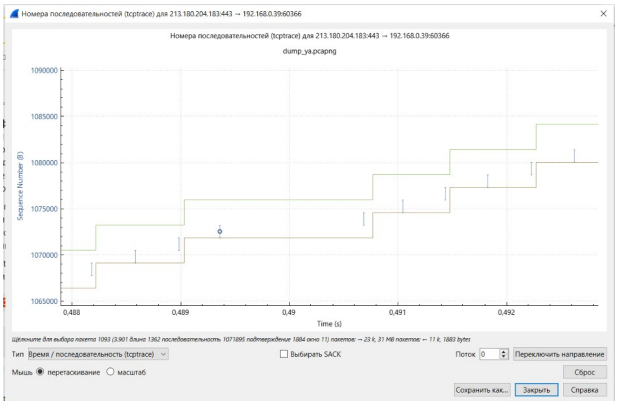


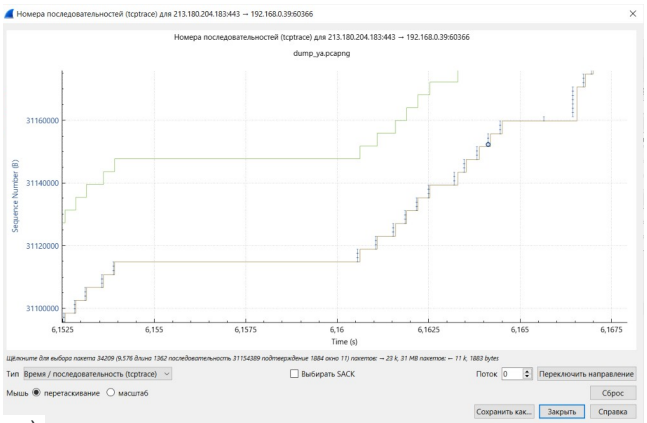






- какое то нарушение последовательности передачи пакетов данных





- RTT ~ 2-0,5 ms (с уменьшением к концу загрузки),
- максимальный RWND ~ 30 000 B. (с увеличением к концу загрузки)