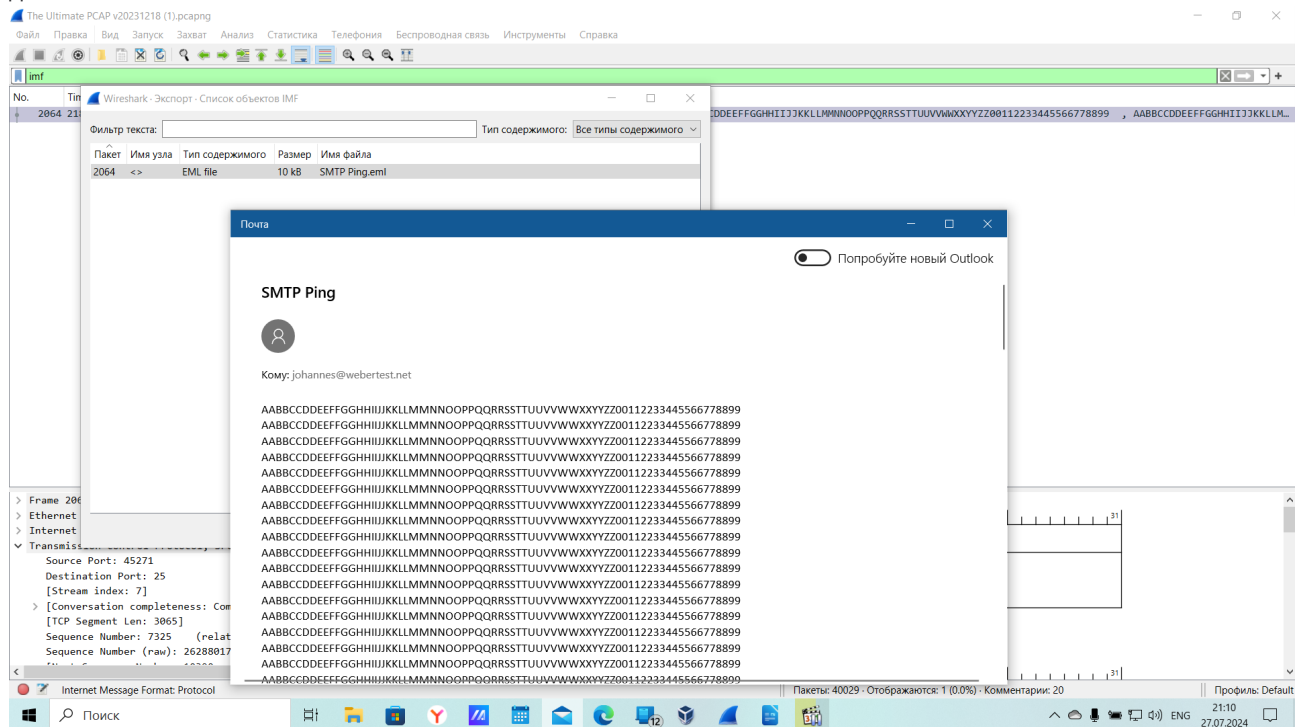


## Урок 5. Основы компьютерных сетей. Транспортный уровень. UDP и TCP.

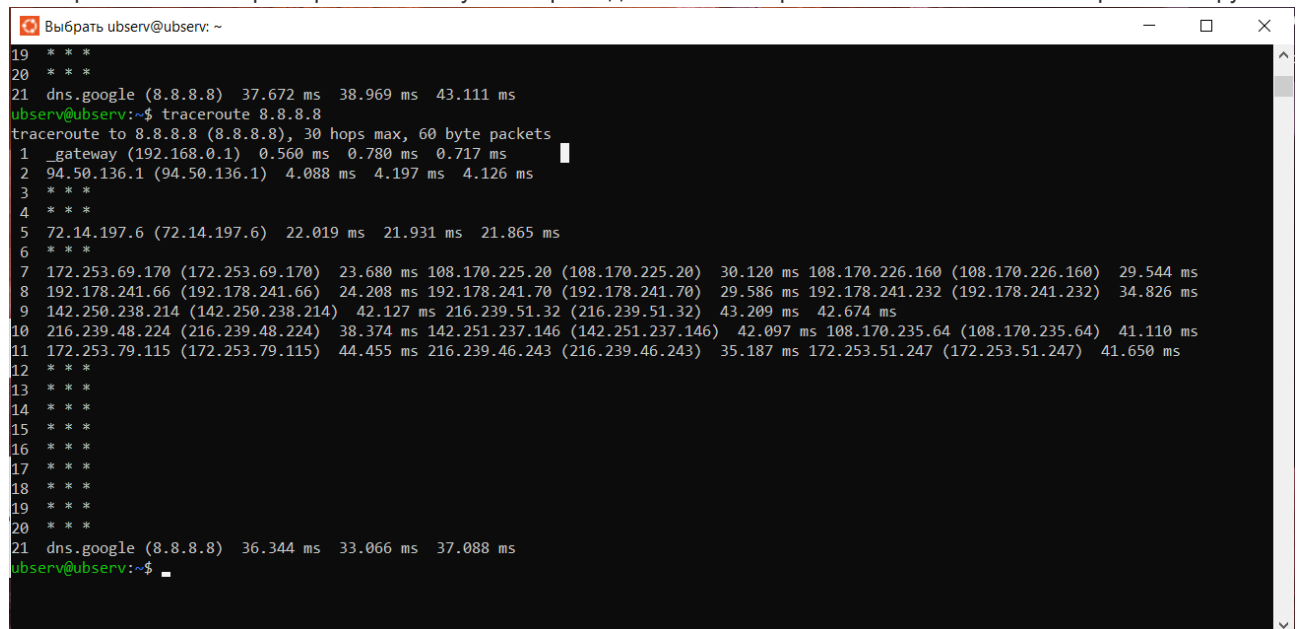
(29.07.24, потом перевели на курс devops)

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 перезагружаются 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 времени 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

\*Ethernet

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

ip.addr == 8.8.8.8 && icmp

Подпись: Введите описание кнопки фильтра Фильтр: Введите применяемое выражение фильтра

Комментарий: Введите комментарий для кнопки фильтра

No.	Time	Source	Destination	Protocol	Length	Info
7910	7.300209	192.168.0.1	192.168.0.167	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
7918	7.300768	192.168.0.1	192.168.0.167	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
7919	7.300768	192.168.0.1	192.168.0.167	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
7940	7.304327	94.50.136.1	192.168.0.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7941	7.304538	94.50.136.1	192.168.0.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7942	7.304538	94.50.136.1	192.168.0.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
7949	7.322915	72.14.197.6	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
7950	7.322915	72.14.197.6	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
7951	7.322915	72.14.197.6	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
8093	7.382570	172.253.69.170	192.168.0.167	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
8158	7.439701	192.178.241.66	192.168.0.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
8201	7.444838	108.170.226.160	192.168.0.167	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
8203	7.445187	192.178.241.70	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
8204	7.445393	108.170.225.20	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
8207	7.450496	192.178.241.232	192.168.0.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
8217	7.457918	142.250.238.214	192.168.0.167	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
8220	7.459160	216.239.51.32	192.168.0.167	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
8230	7.482514	216.239.51.32	192.168.0.167	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
8234	7.483404	216.239.48.224	192.168.0.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
8237	7.486527	108.170.235.64	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
8239	7.487405	142.251.237.146	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
8255	7.493135	216.239.46.243	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
8260	7.495109	172.253.79.115	192.168.0.167	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
8283	7.500931	172.253.51.247	192.168.0.167	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
69010	43.867668	8.8.8.8	192.168.0.167	ICMP	70	Destination unreachable (Port unreachable)
69014	43.870802	8.8.8.8	192.168.0.167	ICMP	70	Destination unreachable (Port unreachable)
69043	43.871739	8.8.8.8	192.168.0.167	ICMP	70	Destination unreachable (Port unreachable)

Frame 7910: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0  
 Ethernet II, Src: zte\_81:7e:6c (34:da:b7:81:7e:6c), Dst: 192.168.0.167  
 Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.167

Internet Control Message Protocol: Protocol

Пакеты: 75606 · Отображаются: 27 (0.0%) · Потеряно: 0 (0.0%) · Профиль: Default

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 фильтравания. 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.

Вход в личный кабинет

Небезопасно | www.fu.ru/Cabinet/\_layouts/15/FA/Cabinet/Login.aspx?Page=5&From=0

РУС ENG +7 (495) 249-5249 Контакт-центр academy@fu.ru

ВЕРСИЯ ДЛЯ СЛАБОВИДЯЩИХ Войти Поиск... ЛИЧНЫЙ КАБИНЕТ ЛК ПОСТУПАЮЩЕГО

МЫ НЕ СЛЕДУЕМ ПРИВЫЧНЫМ ТРЕНДАМ. МЫ ФОРМИРУЕМ НОВЫЕ!

105 ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Наш университет  
 Программа развития  
 Организационная структура  
 Сведения об образовательной организации  
 Ученый совет  
 Наука и инновации  
 Международная деятельность  
 Филиалы  
 Научные журналы  
 Пресс-служба  
 Контакты

ПОСТУПАЮЩИМ | СТУДЕНТАМ И АСПИРАНТАМ | ВЫПУСКНИКАМ | ПАРТНЕРАМ И РАБОТОДАТЕЛЯМ | РАБОТНИКАМ И СОИСКАТЕЛЯМ | ДОПОЛНИТЕЛЬНОЕ И БИЗНЕС-ОБРАЗОВАНИЕ | ЕСТЬ ВОПРОСЫ? ЗАДАВАЙТЕ!

Портал Финансового университета > Личный Кабинет участника мероприятий > Домашняя

## Вход в личный кабинет

E-mail:

Пароль:

Неверный логин или пароль

[Забыли пароль?](#) [Регистрация нового участника](#) [Вход](#)

shark

Беспроводная сеть

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
6617	79.497658	192.168.162.27	194.113.237.139	HTTP	1246	POST /Cabinet/_layouts/15/FA/Cabinet/Login.aspx?Page=5&From=0 HTTP/1.1 (application/x-www-form-urlencoded)

[Prev request in frame: 6367]  
[Response in frame: 6726]  
[Next request in frame: 6733]  
File Data: 12072 bytes

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

- Form item: "MSOWebPartPage\_PostbackSource" = ""
- Form item: "MSOT1Pn\_SelectedWpId" = ""
- Form item: "MSOT1Pn\_View" = "0"
- Form item: "MSOT1Pn\_ShowSettings" = "False"
- Form item: "MSOGallery\_SelectedLibrary" = ""
- Form item: "MSOGallery\_FilterString" = ""
- Form item: "MSOT1Pn\_Button" = "none"
- Form item: "MSOSPWebPartManager\_DisplayModeName" = "Browse"
- Form item: "MSOSPWebPartManager\_ExittingDesignMode" = "false"
- Form item: "\_\_EVENTTARGET" = "ctl00\$PlaceHolderMain\$BtnSend"
- Form item: "\_\_EVENTARGUMENT" = ""
- Form item: "MSOWebPartPage\_Shared" = ""
- Form item: "MSOLayout\_LayoutChanges" = ""
- Form item: "MSOLayout\_InDesignMode" = ""
- Form item: "MSOSPWebPartManager\_OldDisplayModeName" = "Browse"
- Form item: "MSOSPWebPartManager\_StartWebPartEditingName" = "false"
- Form item: "MSOSPWebPartManager\_EndWebPartEditing" = "false"
- Form item: "\_\_REQUESTDIGEST" = "0x3D079CFFC02849B1C1D830C1C5D3D0059A17E"
- [truncated] Form item: "\_\_VIEWSTATE" = "/wEPDwUJNjM2OTM2MjE3OD2QWAmYPZBv"
- Form item: "\_\_VIEWSTATEGENERATOR" = "EC0D7083"
- Form item: "\_\_EVENTVALIDATION" = "/wEdAAY0t7k7hI1rodXXNs+0BZT3AHgQ5JLQr"
- Form item: "ctl00\$PlaceHolderMain\$Email" = "111@mail.ru"
  - Key: ctl00\$PlaceHolderMain\$Email
  - Value: 111@mail.ru
- Form item: "ctl00\$PlaceHolderMain\$Password" = "111111111"
  - Key: ctl00\$PlaceHolderMain\$Password
  - Value: 111111111

Ethernet

Destination

Source

Type

Internet Protocol Version 4

Version Header Len... Differentiated Services Field Total Length

Identification Flags Fragment Offset

Time to Live Protocol Header Checksum

Source Address

Destination Address

Transmission Control Protocol

Source Port Destination Port

Sequence Number

Acknowledgment Number

Header Len... Flags Window

Checksum Urgent Pointer

wireshark\_Беспроводная сети\M6RR2.pcapng

Пакеты: 6974 · Отображаются: 1 (0.0%) · Потеряно: 0 (0.0%)

просматриваем почту и пароль

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?

(18.01.25, продолжаю после повторения предыдущих занятий)

Index of /ubuntu/

File Name	Size	Modified
<a href="#">dists/</a>		17-Oct-2024 10:07
<a href="#">indices/</a>		18-Jan-2025 08:55
<a href="#">pool/</a>		27-Feb-2010 06:30
<a href="#">project/</a>		24-Nov-2024 21:31
<a href="#">ubuntu/</a>		18-Jan-2025 10:00
<a href="#">ls-IR.gz</a>	31152337	18-Jan-2025 08:59

Чили

Index of /ubuntu/

File Name	Size	Modified
<a href="#">dists/</a>		17-Oct-2024 10:07
<a href="#">indices/</a>		18-Jan-2025 08:55
<a href="#">pool/</a>		27-Feb-2010 06:30
<a href="#">project/</a>		24-Nov-2024 21:31
<a href="#">ubuntu/</a>		18-Jan-2025 10:00
<a href="#">ls-IR.gz</a>	31152337	18-Jan-2025 08:59

Яндекс

дампы скачиваний выложены на [https://github.com/196-PetrT/base\\_cmp\\_net/tree/main/less\\_4\\_1](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)

Wireshark - Conversations - dump\_ya.pcapng

Conversation Settings

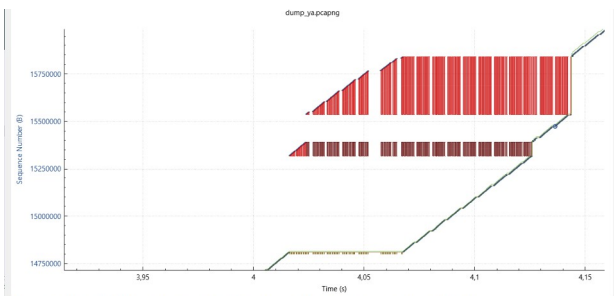
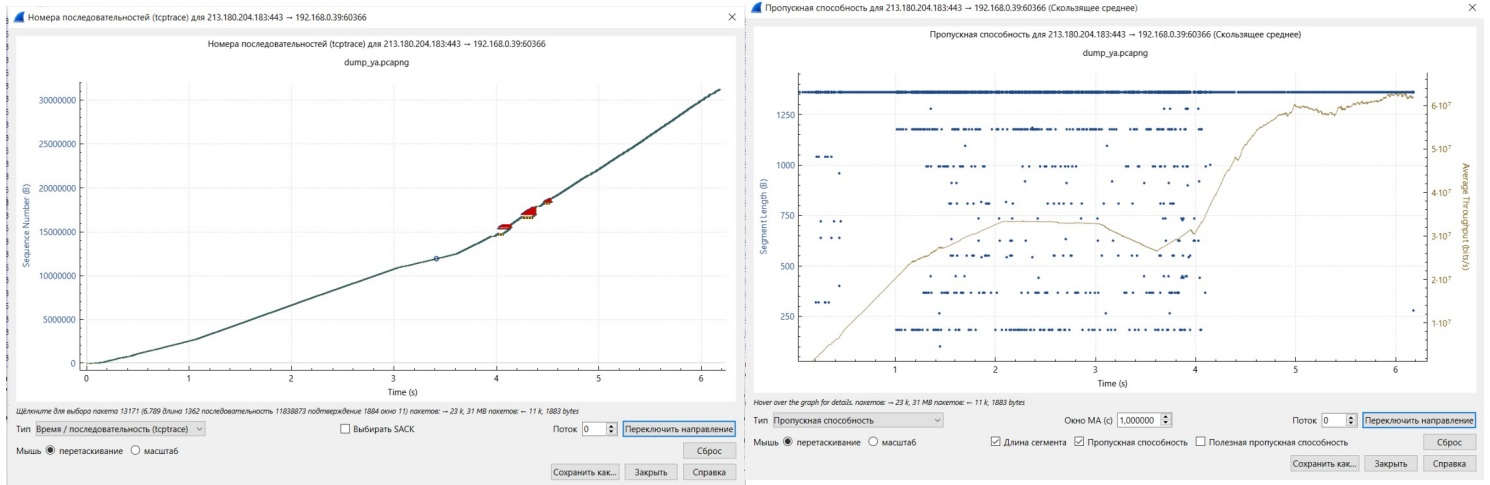
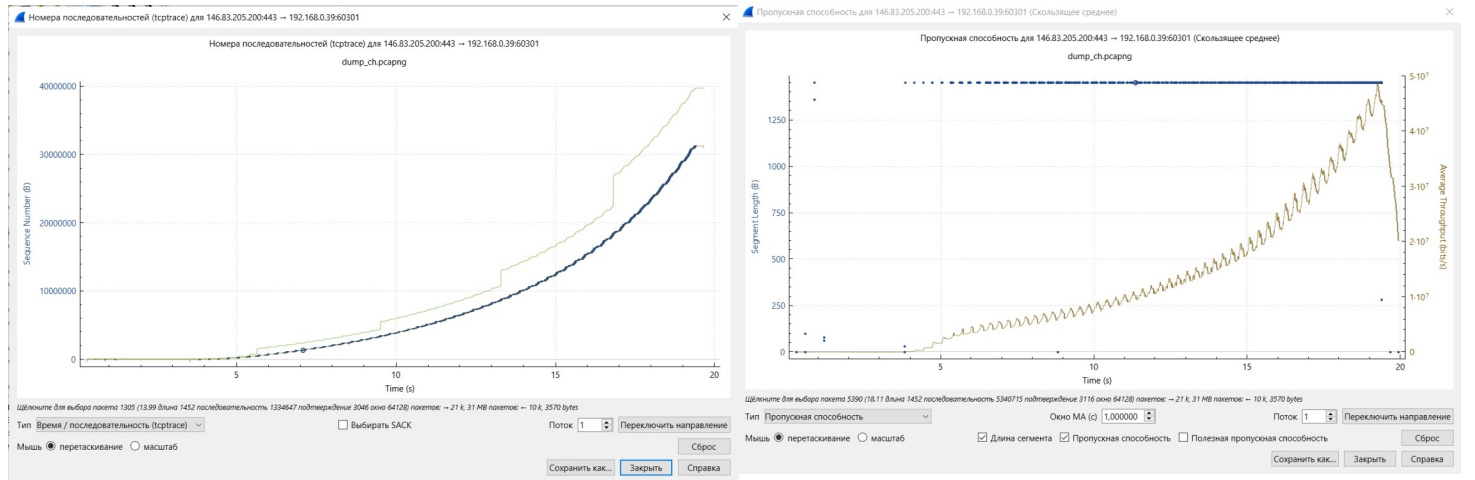
☐ Разрешение имен

☐ Абсолютное время запуска

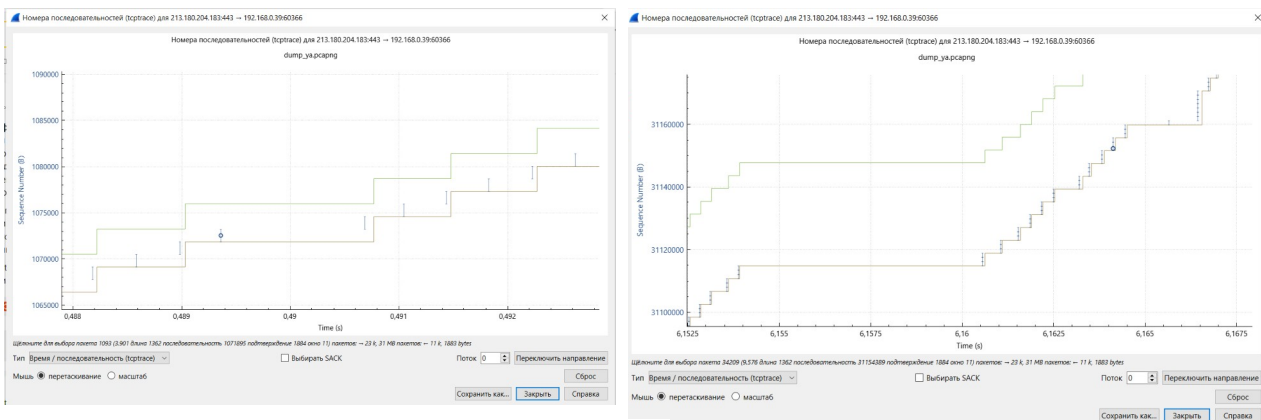
Ethernet · 8		IPv4 · 11		IPv6 · 2		TCP · 2		UDP · 8			
Адрес А	Адрес В	Пакеты	Байт	Пакеты А → В	Bytes А → В	Пакеты В → А	Bytes В → А	Отн. время начала	Продолжительность	Bits/s А → В	Bits/s В → А
192.168.0.39	213.180.204.183	34 266	33 МБ	11 115	630 кБ	23 151	32 МБ	3.41877	6.1728	816 kbps	42 Mbps
192.168.0.16	224.0.0.251	5	1 кБ	5	1 кБ	0	0 байт	9.830478	5.3250	1621 bits/s	0 bits/s

для каждого дампа сделал выборку в «диалогах» по В-->А ,

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)