Исследование размера окна приема TCP в различных ОС

Дунайцев Р.А. (СПбГУТ)

roman.dunaytsev@spbgut.ru

Краткая теоретическая справка

- Одной из многочисленных функций, реализуемых TCP, является управление потоком данных для защиты принимающей стороны от перегрузки. Иными словами, управление потоком представляет собой регулирование количества посылаемых отправителем данных в соответствии со свободным местом в буфере получателя для предотвращения переполнения буфера. Получатель осуществляет управление потоком данных, анонсируя в поле Window в виде двоичного числа количество байт данных (т.н. «окно»), которые он готов принять от отправителя. Длина этого поля составляет 16 бит, что ограничивает максимальный объем передаваемых за один раунд данных 65535 байтами. Опция масштабирования окна (**TCP Window Scale Option**) позволяет повысить производительность TCP, увеличив размер окна путем умножения его на специальный коэффициент масштабирования, который указывается на этапе установления TCP-соединения в сегментах SYN и SYN/ACK.
- https://tools.ietf.org/html/rfc7323
- https://tools.ietf.org/html/rfc793

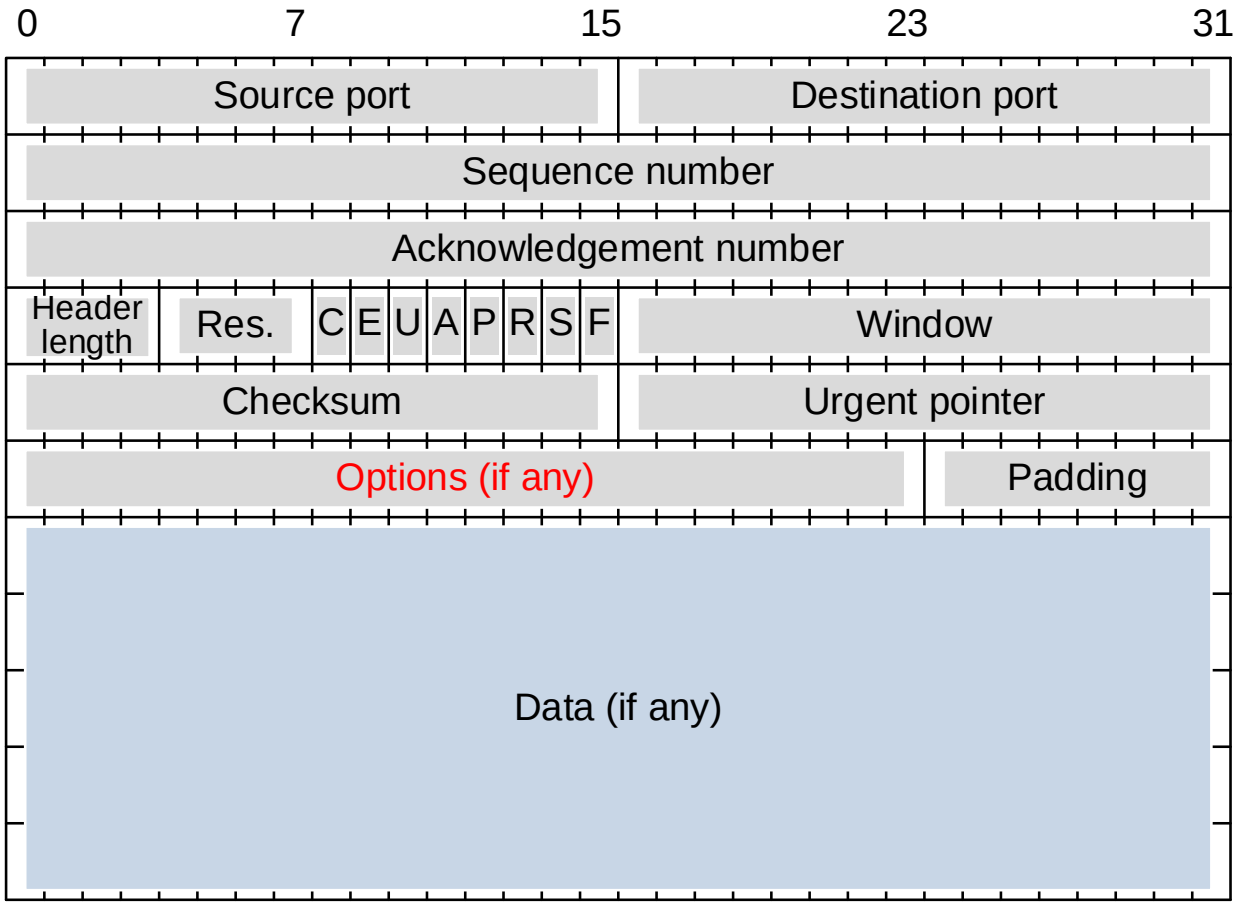
Задание на дом

1) Используя ПО для создания и запуска виртуальных машин (VirtualBox, VMware и т.п.), установить не менее 5 операционных систем (ОС) разных лет выпуска и/или разных типов. Например:
   - Windows XP/Vista/8.0/8.1/10
   - Ubuntu 9/11/13/15/17, см. http://old-releases.ubuntu.com/releases/
   - Любые ОС на ваш выбор из списка самых популярных https://distrowatch.com/dwres.php?resource=popularity
   - Если места на жестком диске мало, то ОС лучше устанавливать по очереди, удаляя предыдущую
2) С помощью Wireshark определить, какие опции TCP используют данные ОС, а также максимальный размер окна (с учетом масштабирования, если такая опция используется)
3) Ознакомиться с назначением обнаруженных опций TCP и дать их развернутое описание
4) **К отчету приложить собранные Wireshark пакеты!**

Оформление результатов

ОС	Год выпуска	Опции TCP	Макс. окно, байт

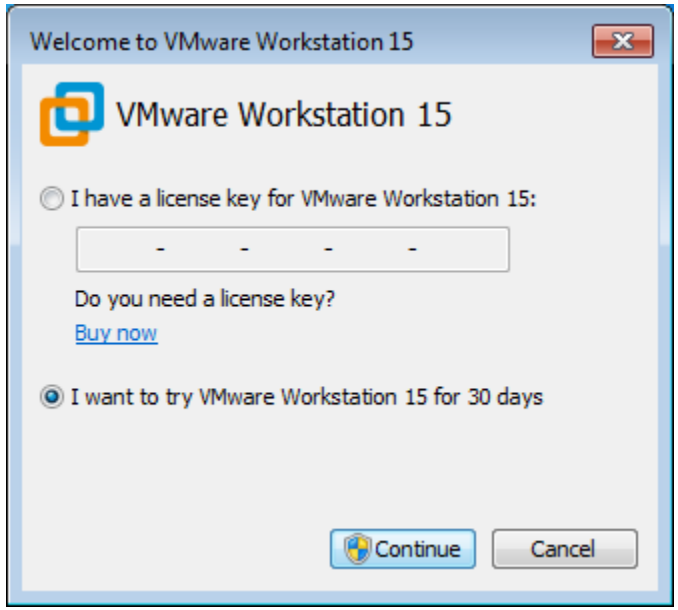
Структура TCP-сегмента



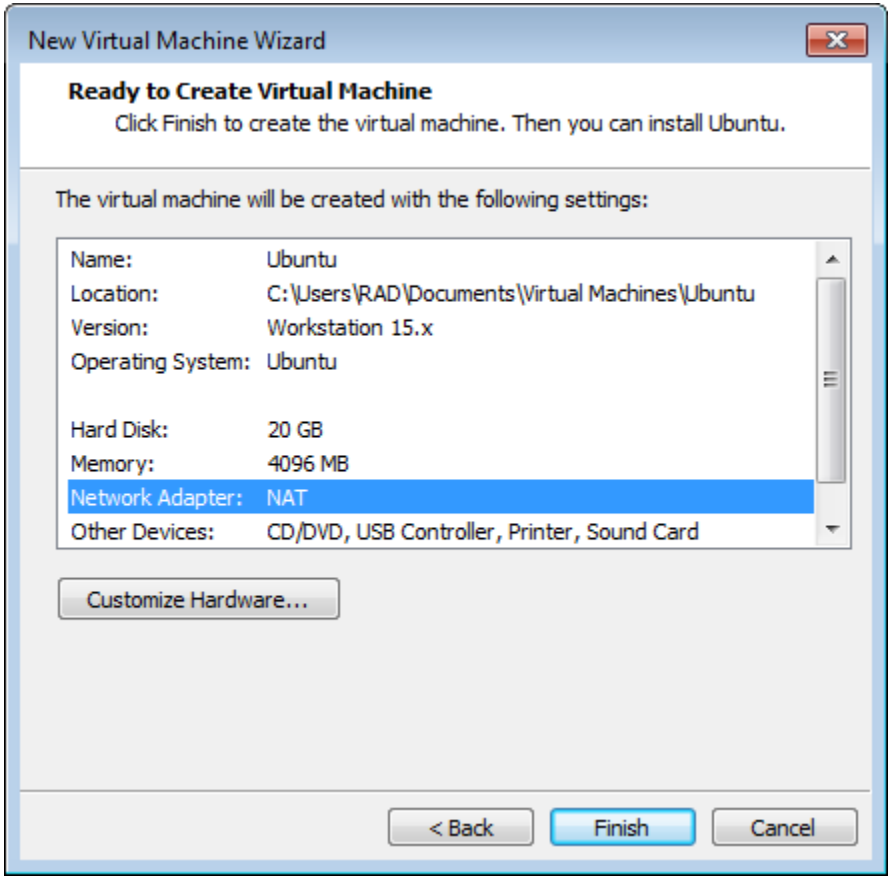
Пример исследования ОС

- Основная ОС: Windows 7 Enterprise 64-bit
- Тестируемая ОС: Linux Mint 19.3 Tricia Cinnamon 32-bit
  - https://www.linuxmint.com/edition.php?id=273
- Используемое ПО: VMware Workstation 15 Player
  - https://download3.vmware.com/software/player/file/VMware-player-15.5.2-15785246.exe
- Для Windows **32-bit** используйте VMware Player 6
  - https://download3.vmware.com/software/player/file/VMware-player-6.0.7-2844087.exe
- либо VMware Workstation 10
  - https://download3.vmware.com/software/wkst/file/VMware-workstation-full-10.0.7-2844087.exe

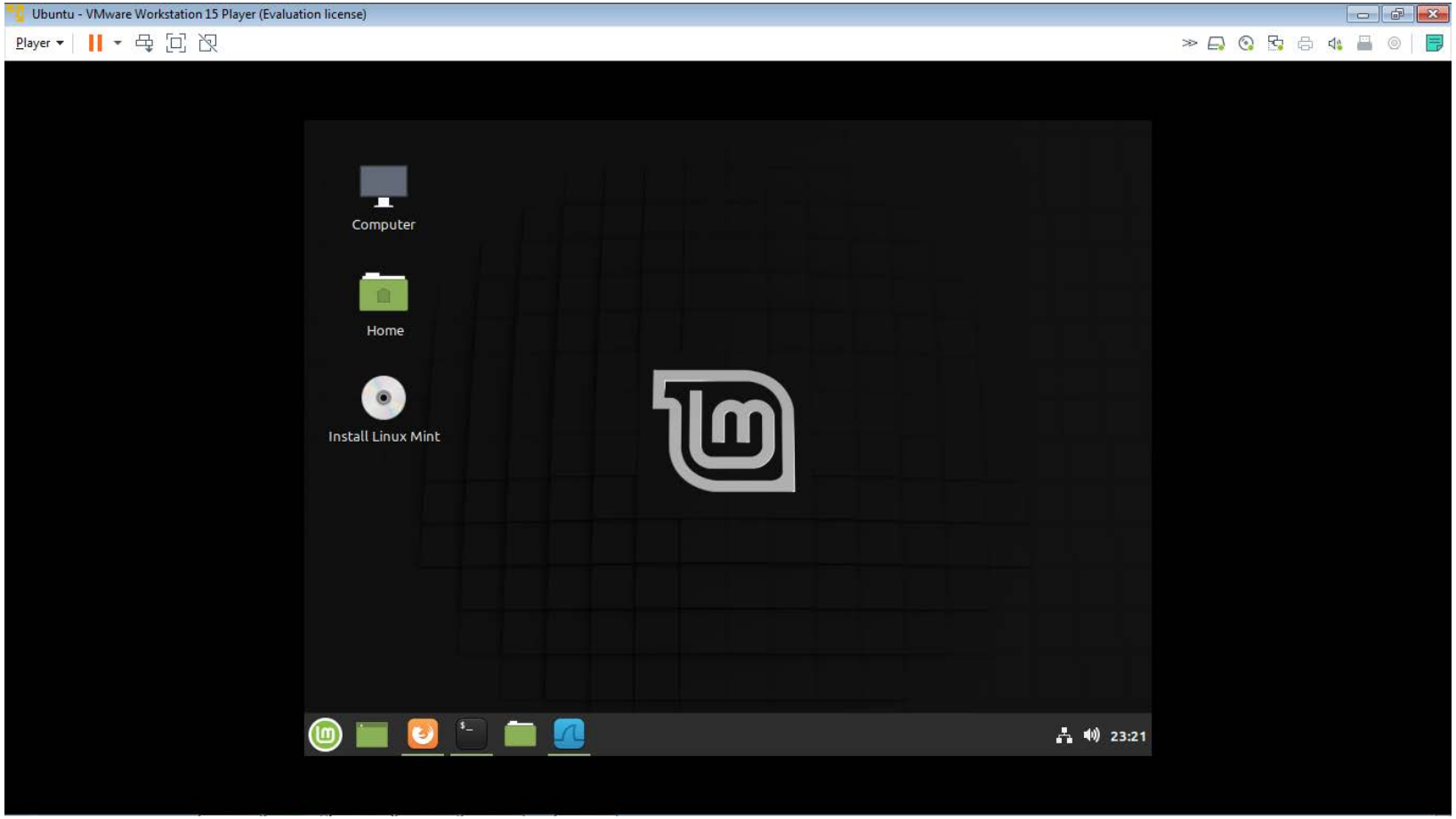
Player и Workstation бесплатны ☺



В VMware используется NAT!



Linux Mint 19.3 ‘Tricia’ Cinnamon

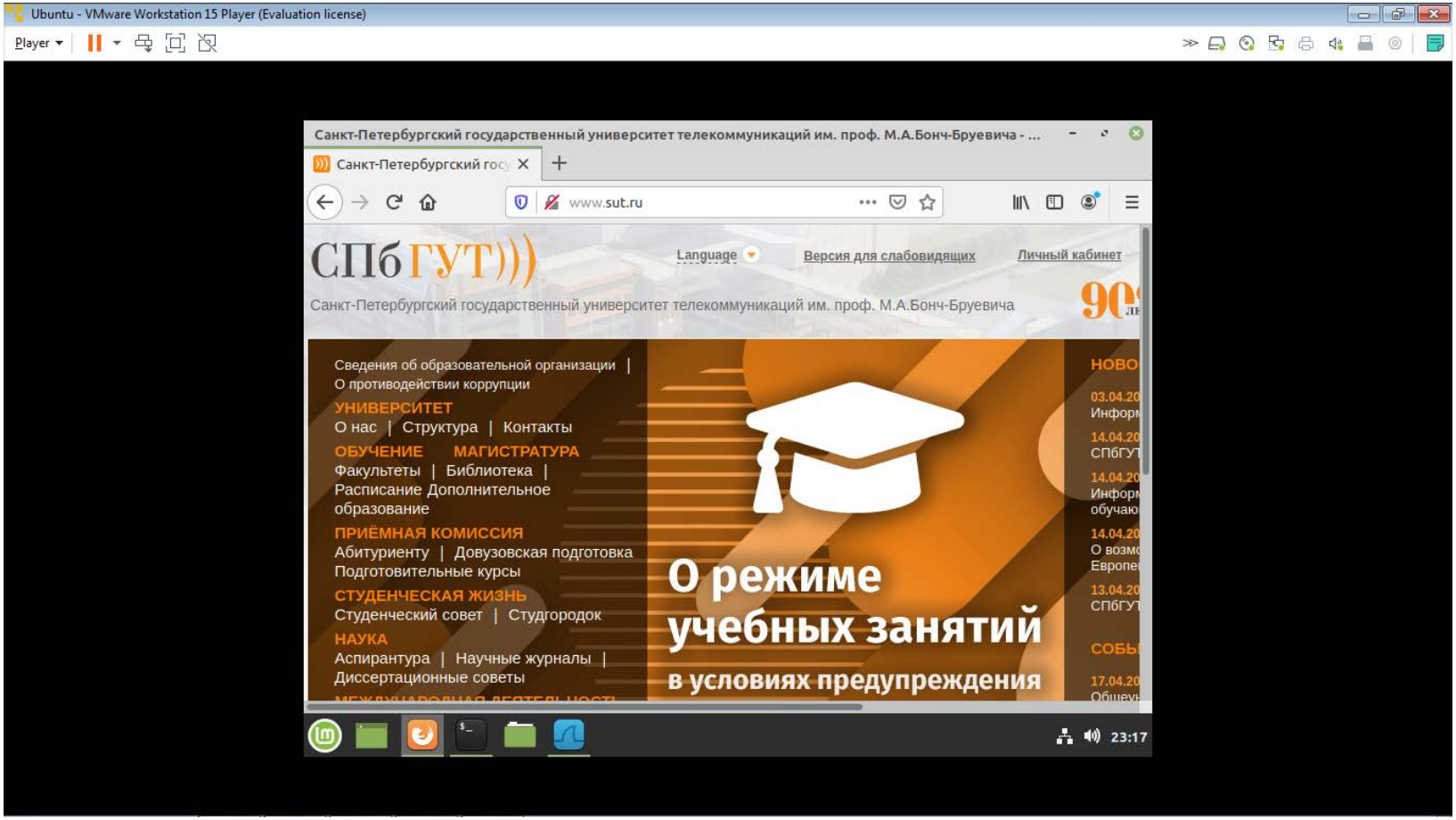


Установка Wireshark в Linux

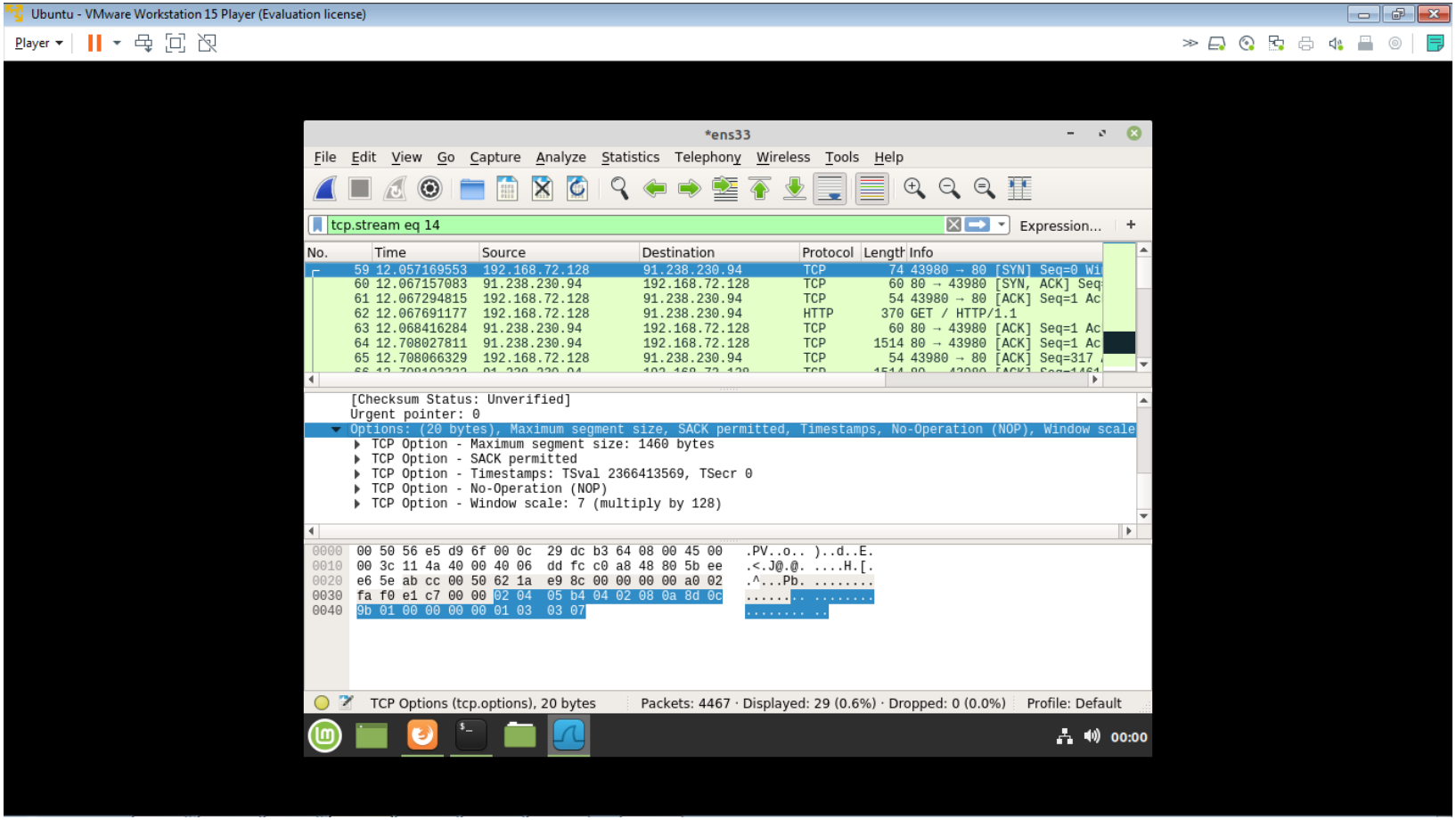
1) Запускаем Terminal:
   <Ctrl> + <Alt> + T
2) Обновляем пакеты:
   sudo apt-get update
3) Устанавливаем Wireshark:
   sudo apt-get install wireshark
4) Запускаем Wireshark для захвата трафика:
   sudo wireshark

- Кстати, в Ubuntu мне не удалось установить Wireshark. Может вам повезет больше… ☹

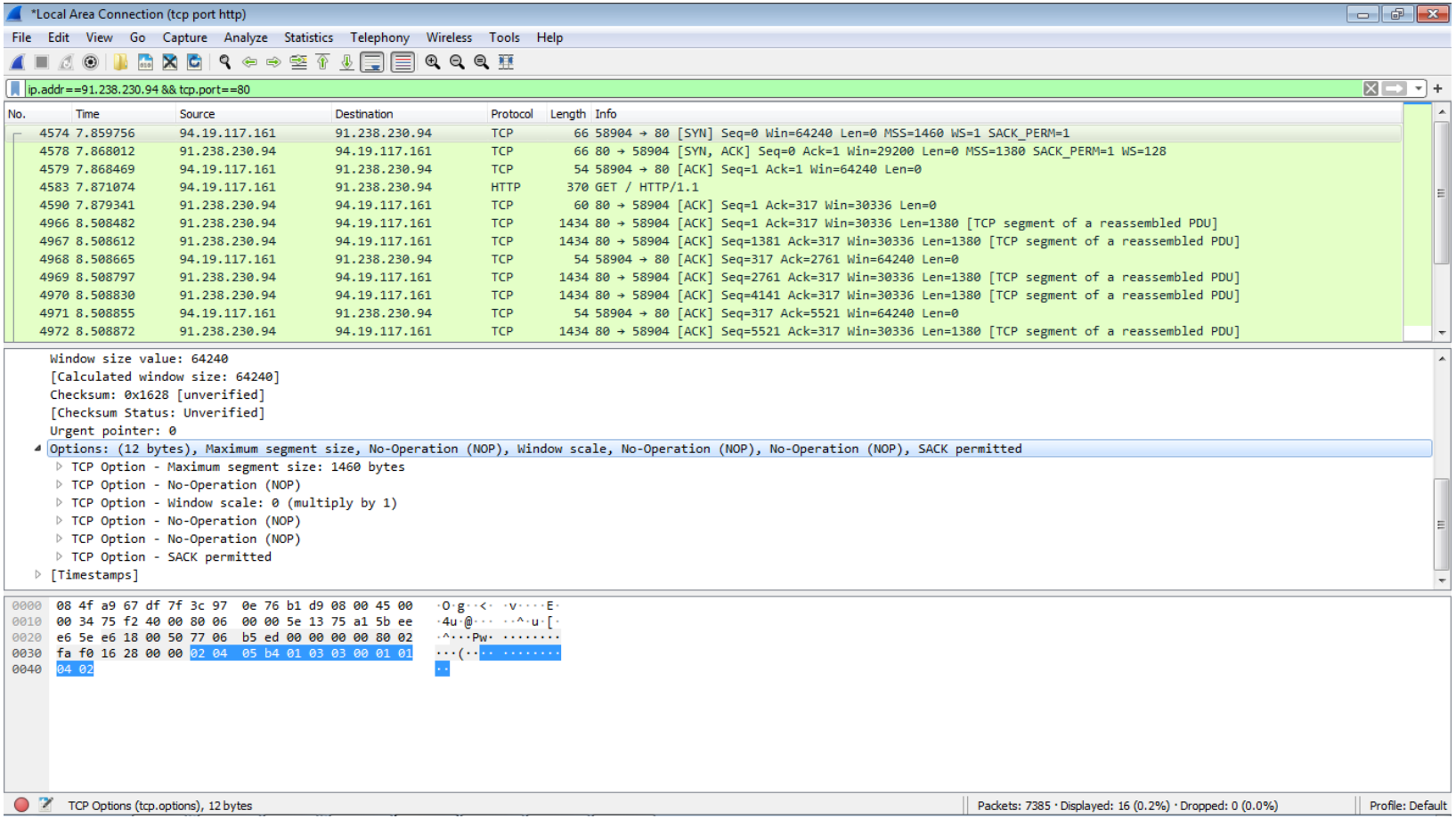
Открываем какой-нибудь сайт



Пакеты внутри VMware



Те же пакеты в основной ОС



После NAT опции TCP изменились

Внутри VMware Workstation 15 Player	В основной ОС после NAT
Maximum Segment Size: 1460 bytes	Maximum Segment Size: 1460 bytes
SACK permitted	No-Operation (NOP)
Timestamps	Window scale: 0 (multiply by 1)
No-Operation (NOP)	No-Operation (NOP)
Window scale: 7 (multiply by 128)	No-Operation (NOP)
	SACK permitted

Выводы

- При обращении из виртуальной машины к сайтам в сети Интернет используется **NAT (Network Address Translation)**
- Как показал проведенный эксперимент, использование NAT меняет состав и содержимое опций TCP
- В частности, отключилась опция масштабирования окна, так как вместо исходного коэффициента 128 умножение будет происходить на 1 и, следовательно, величина окна не изменится
- Также исчезла опция временной метки
- **Таким образом, для получения объективной информации захват пакетов с помощью Wireshark следует производить внутри виртуальной машины, а не снаружи!**

Итоговая таблица с одной ОС

ОС	Год выпуска	Опции TCP	Макс. окно, байт
linuxmint-19.3-cinnamon-32bit	December 18, 2019	MSS, SACK, Timestamps, NOP, Window scale	65535 x 128 = 8.388.480