МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Мегафакультет трансляционных информационных технологий

Факультет информационных технологий и программирования

**Лабораторная работа №3**

**По дисциплине «Телекоммуникационные системы и технологии»**

Мониторинг сетевого трафика на хосте и работа с утилитами диагностики и мониторинга сетевых соединений в Linux

**Выполнили студенты группы М33081**

**Аль Даббагх Харит Хуссейн**

**Мазумдер Шоувик**

**Миах Такбир**

**Проверила**

**Шараева Кристина Витальевна**

САНКТ-ПЕТЕРБУРГ

2022

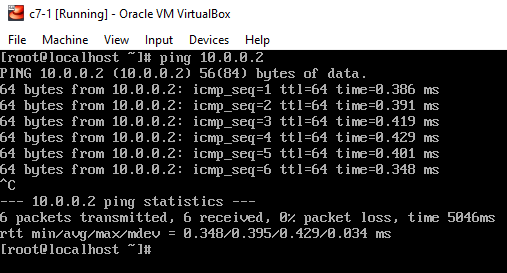
Содержание

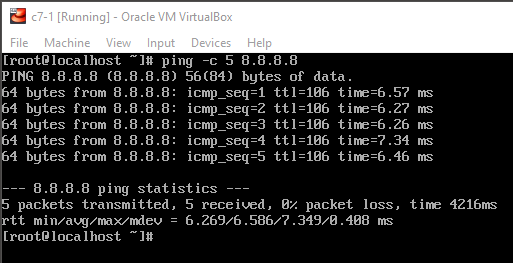
[Артефакты 2](#_Toc98858654)

[Вопросы и задания 15](#_Toc98858655)

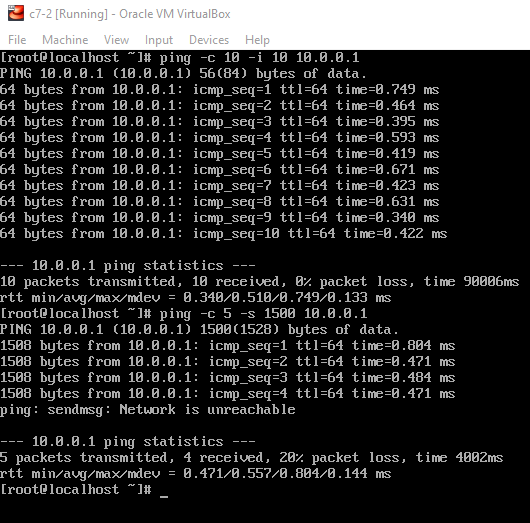
# Артефакты

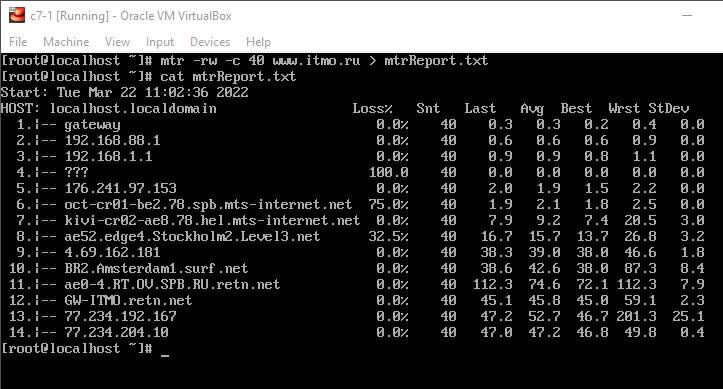
1. **Тексты команд и консольный вывод из Части 1. п. 8**

****

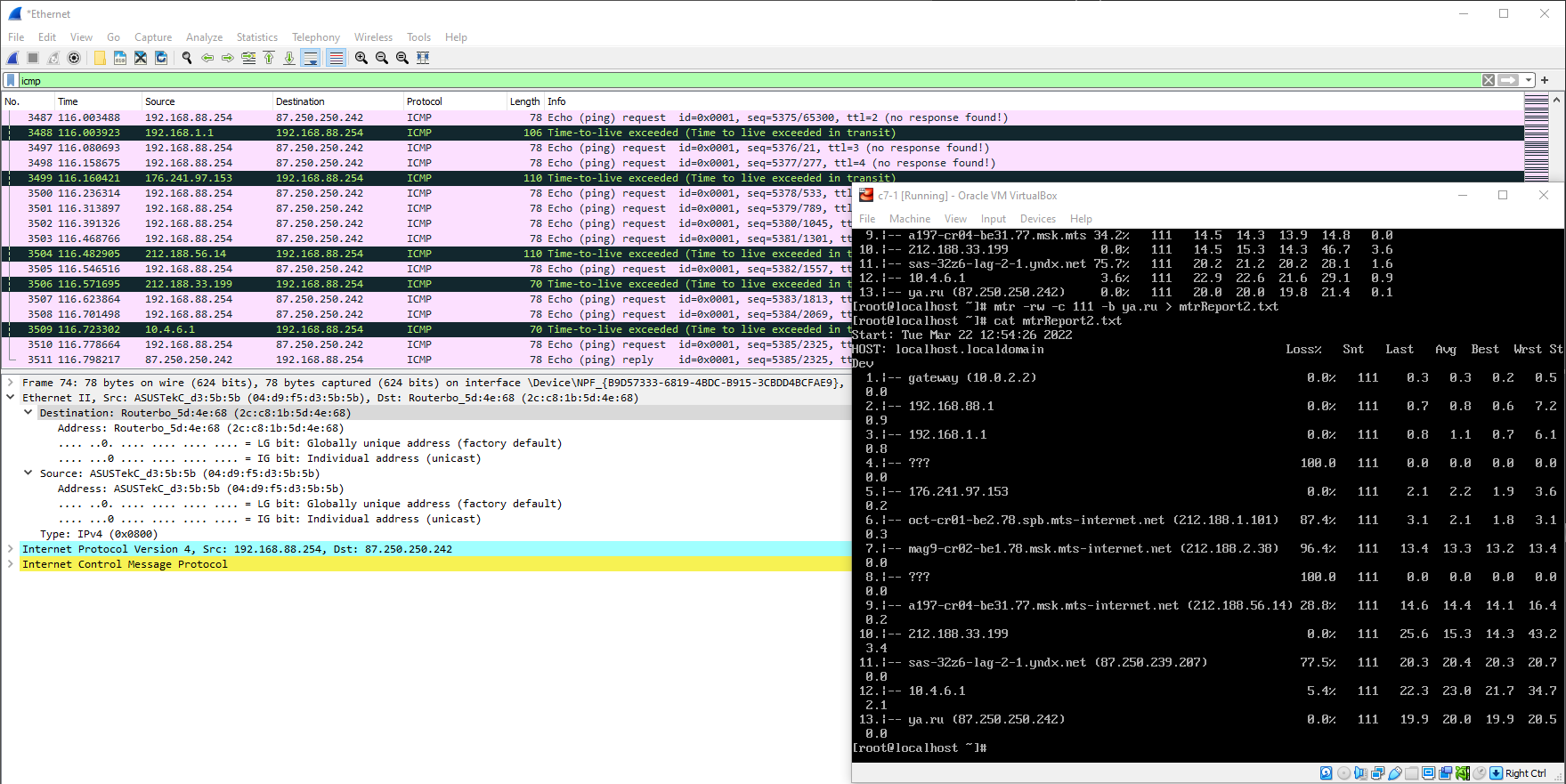
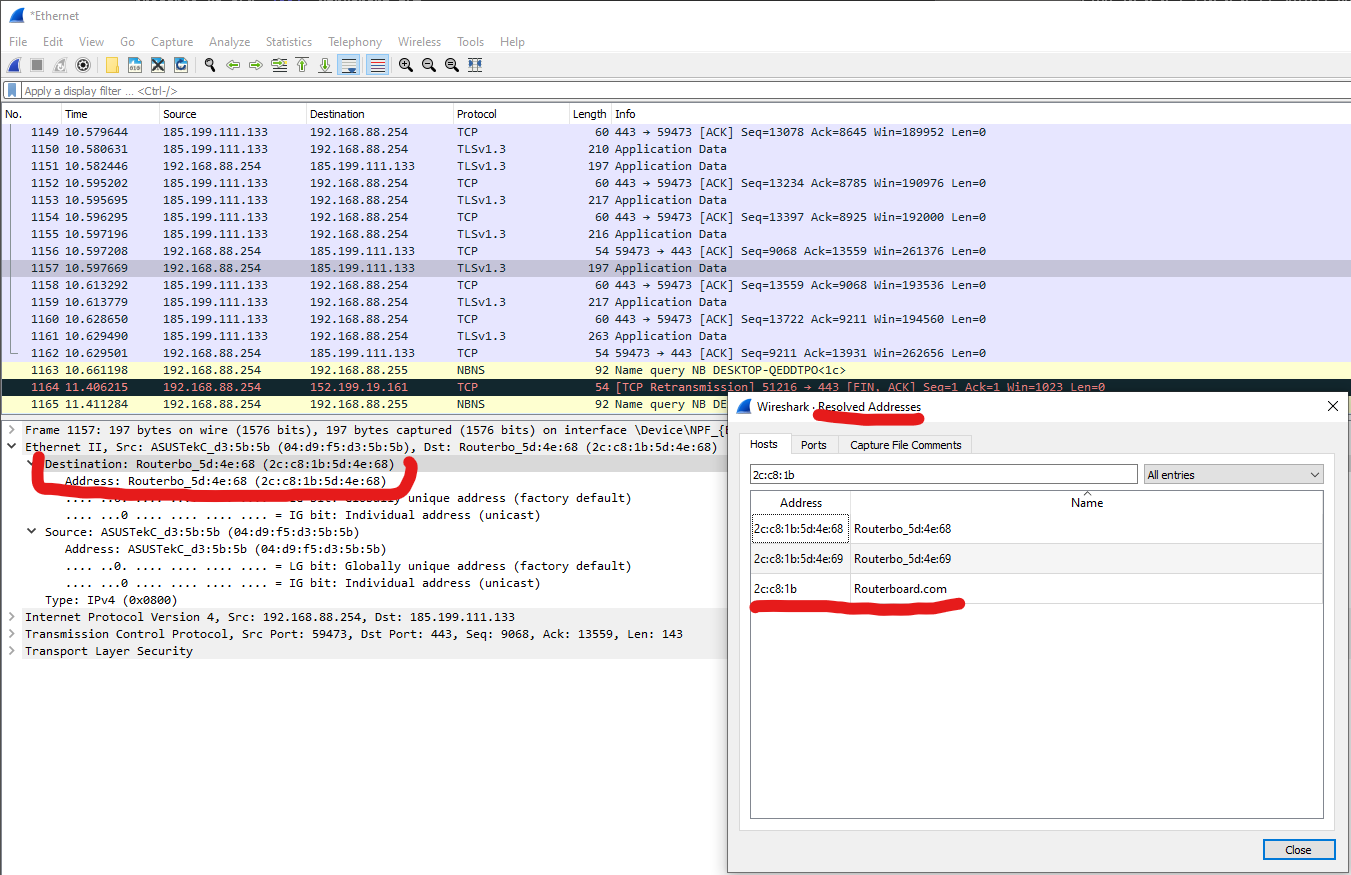
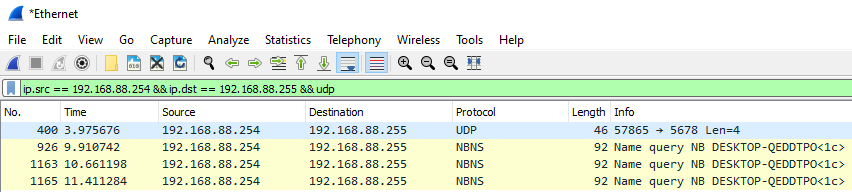
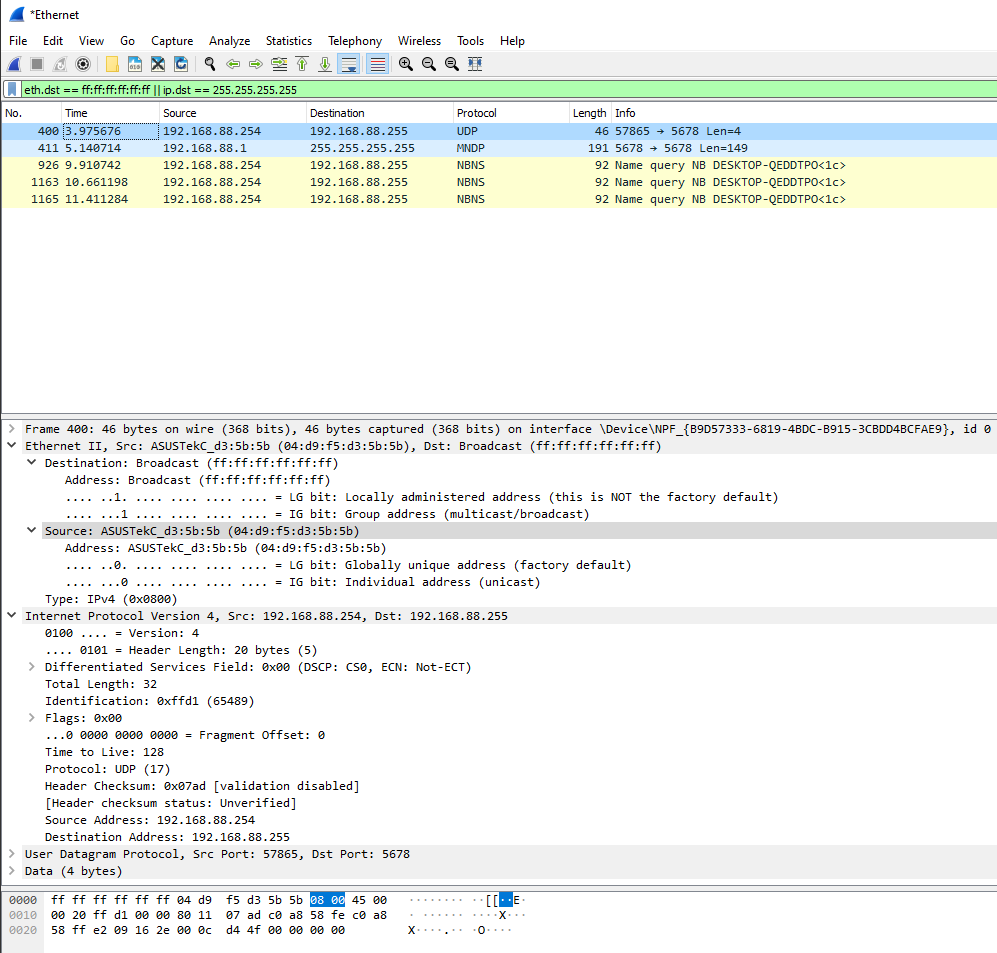
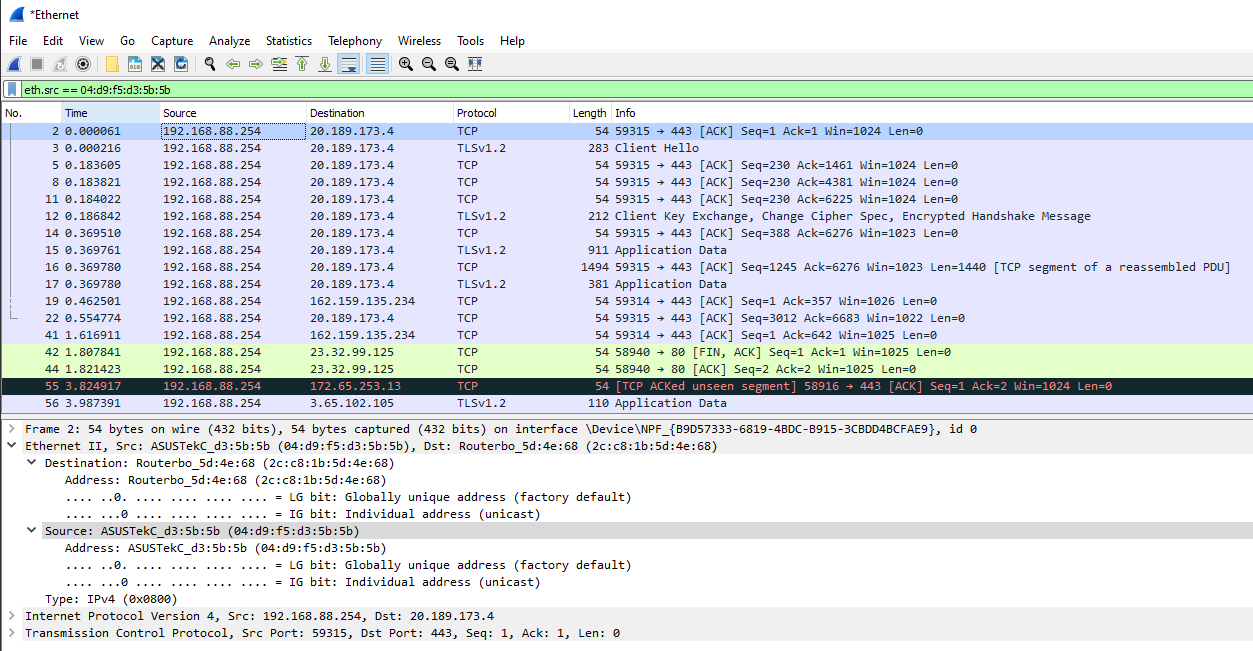
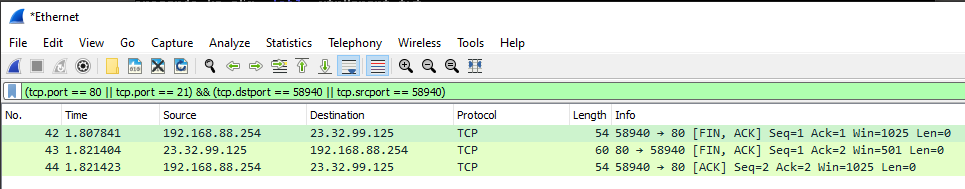
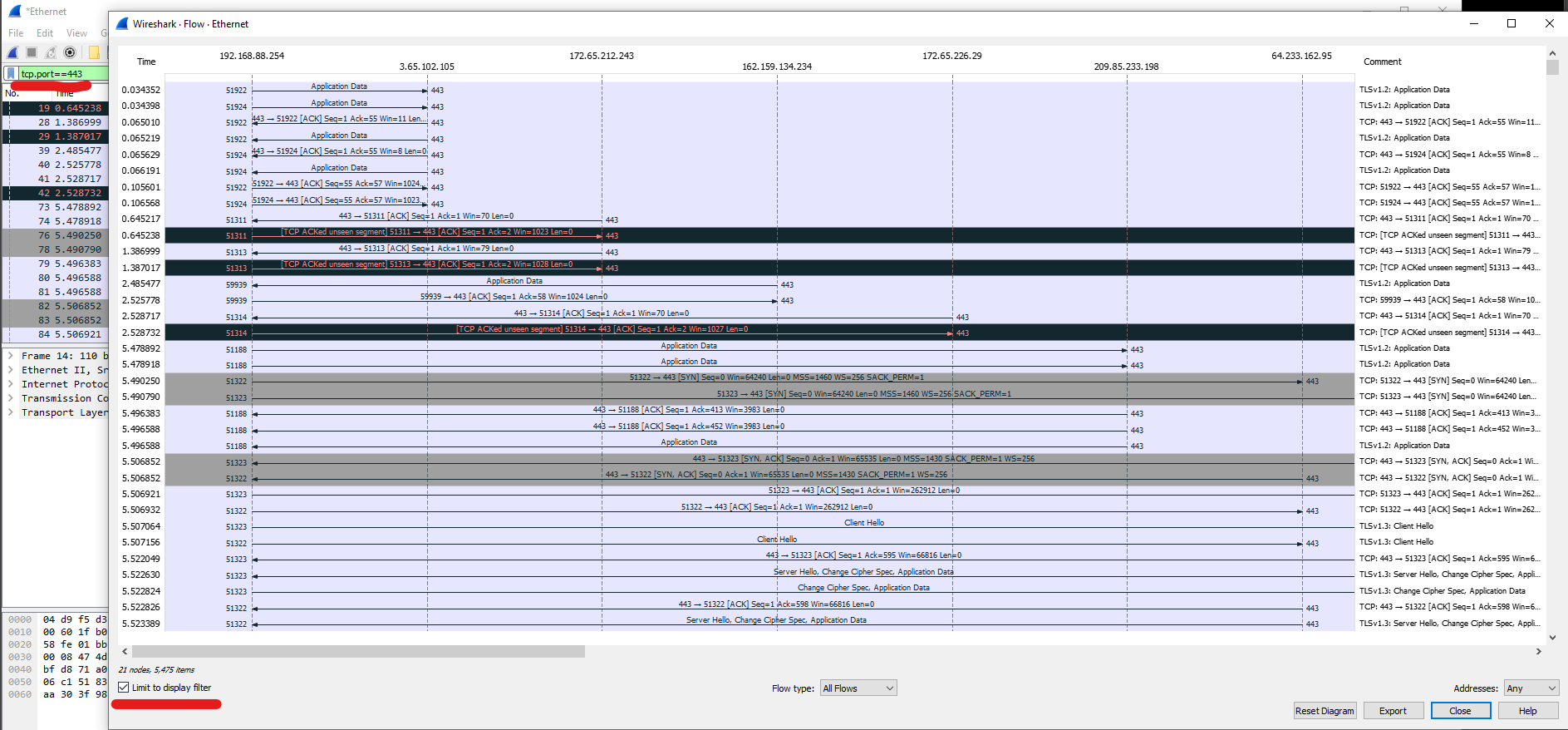
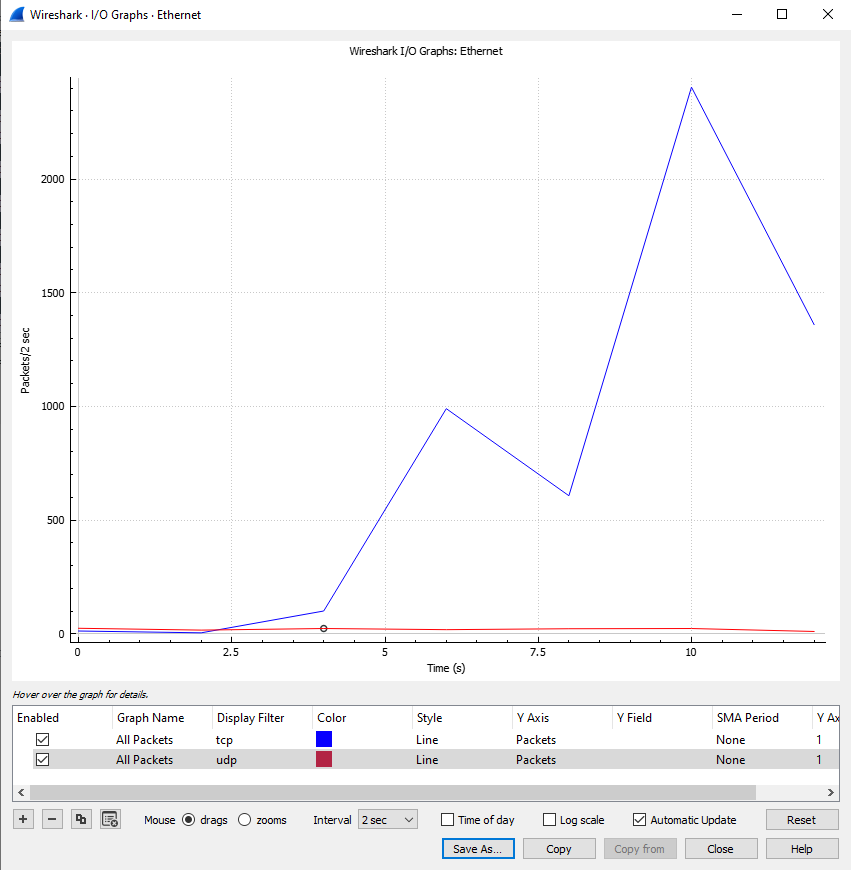
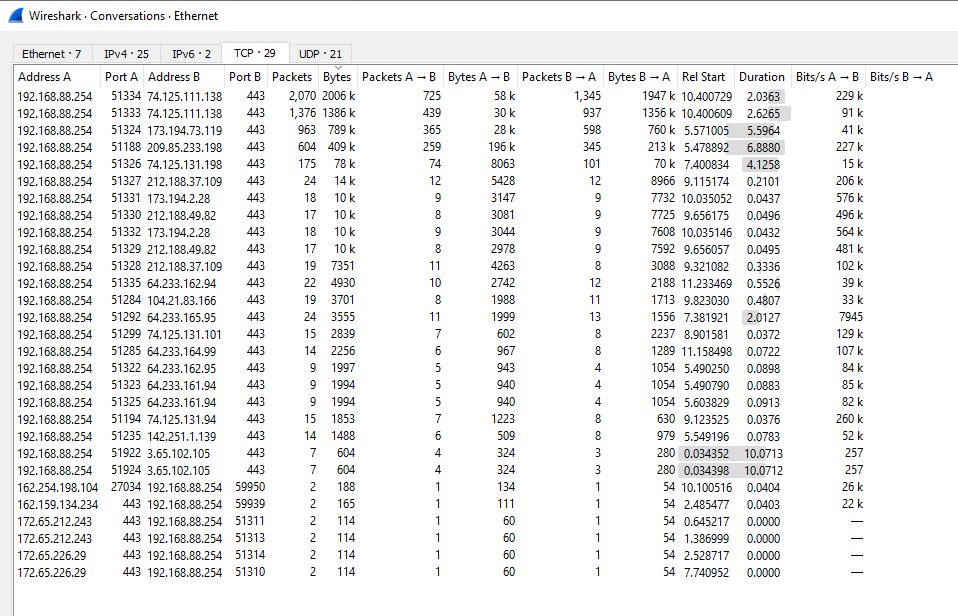
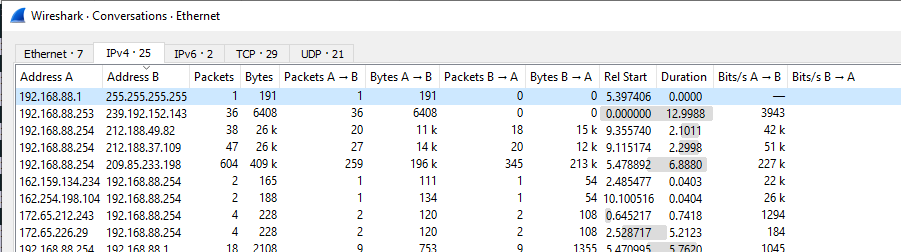
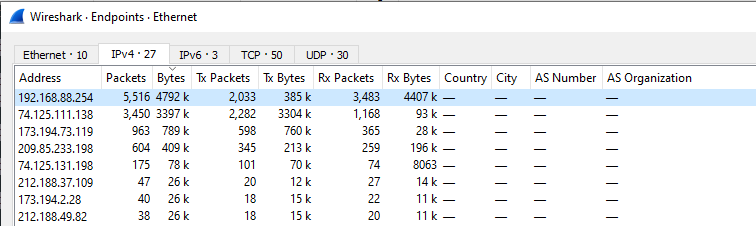
****

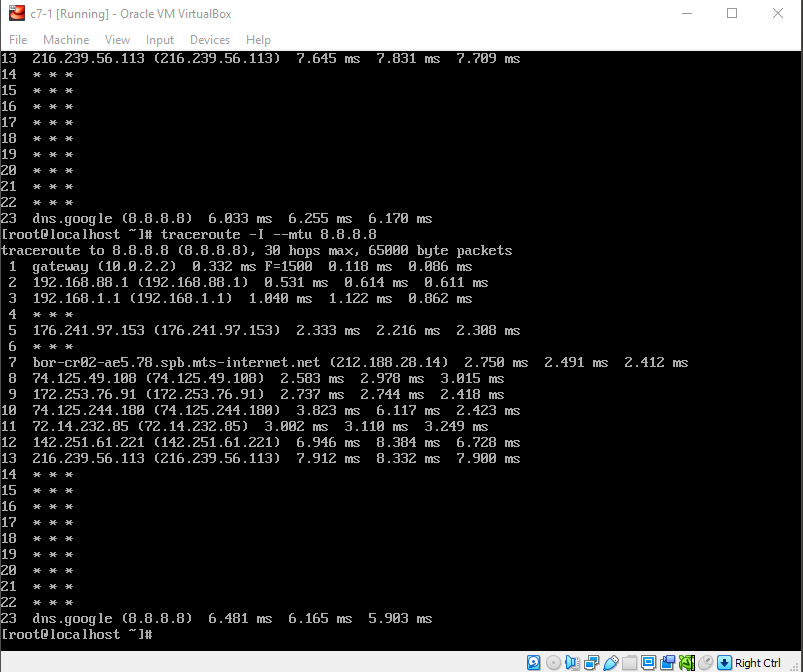
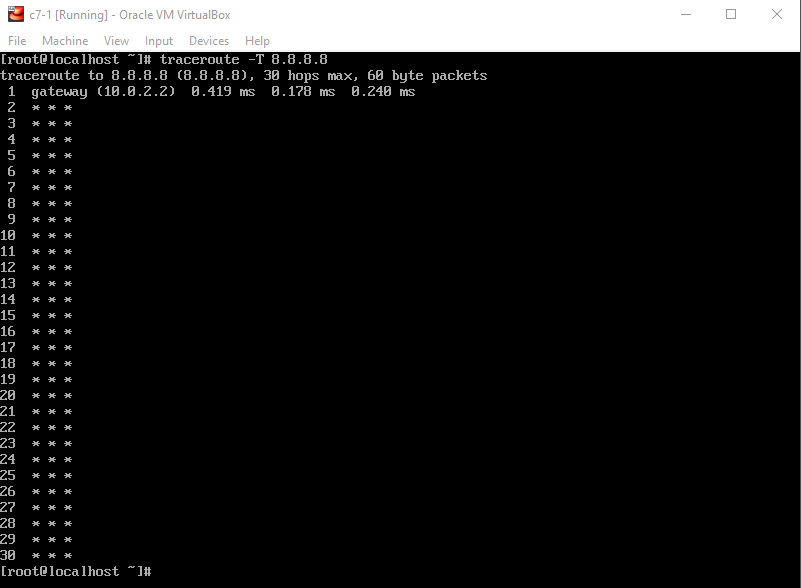
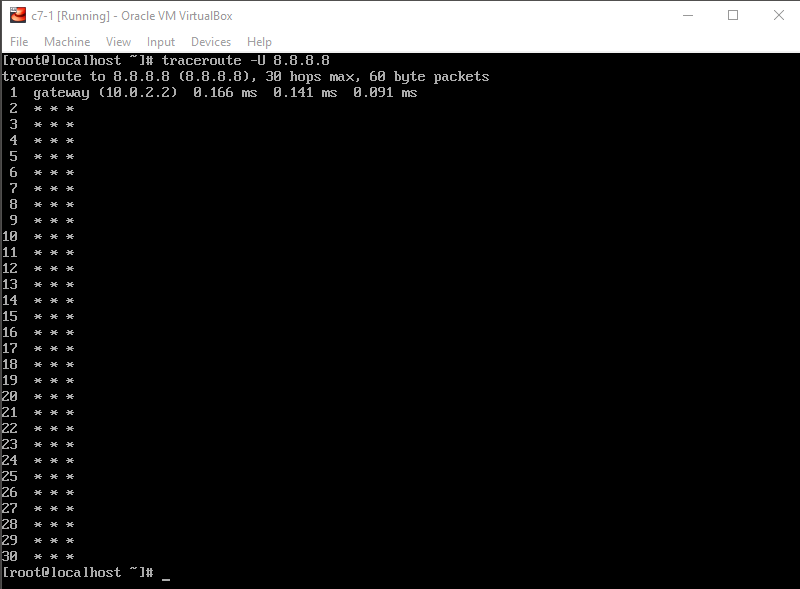
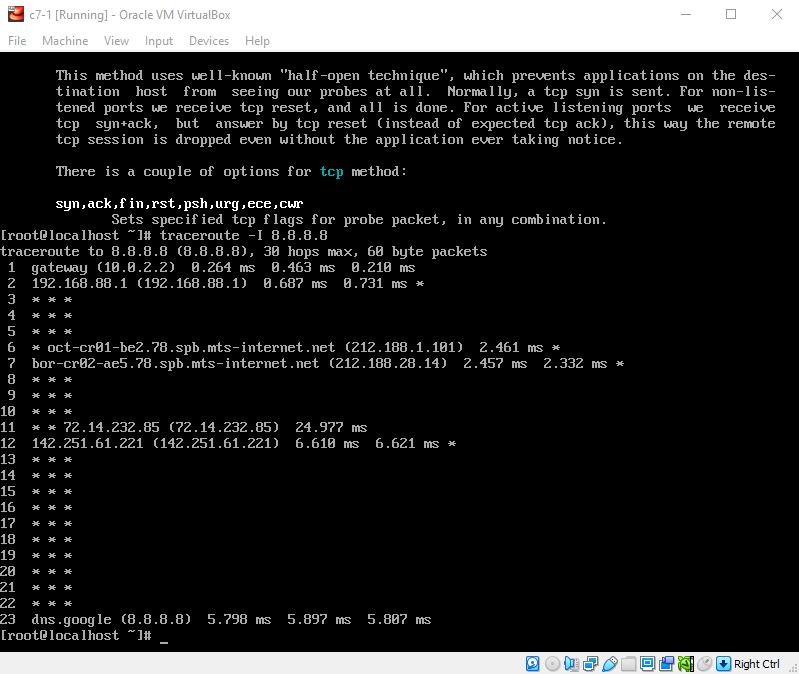
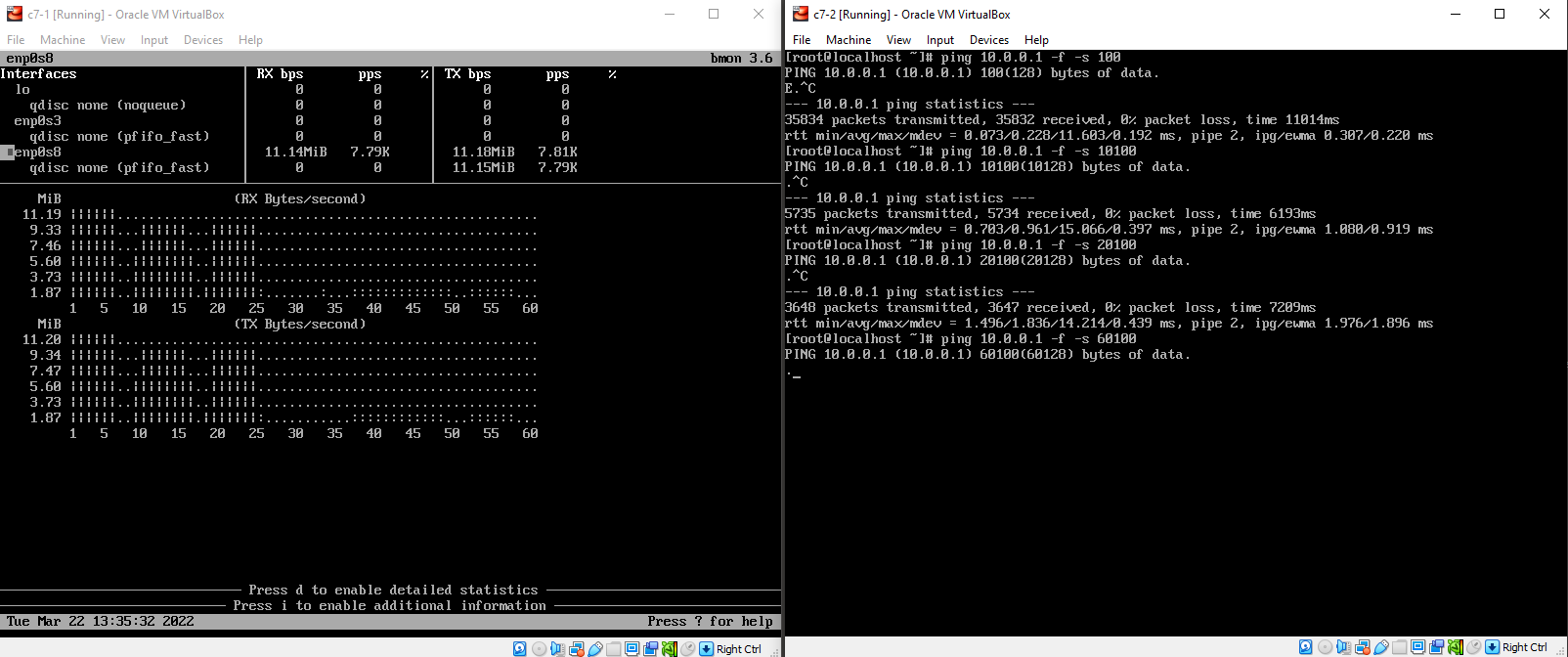
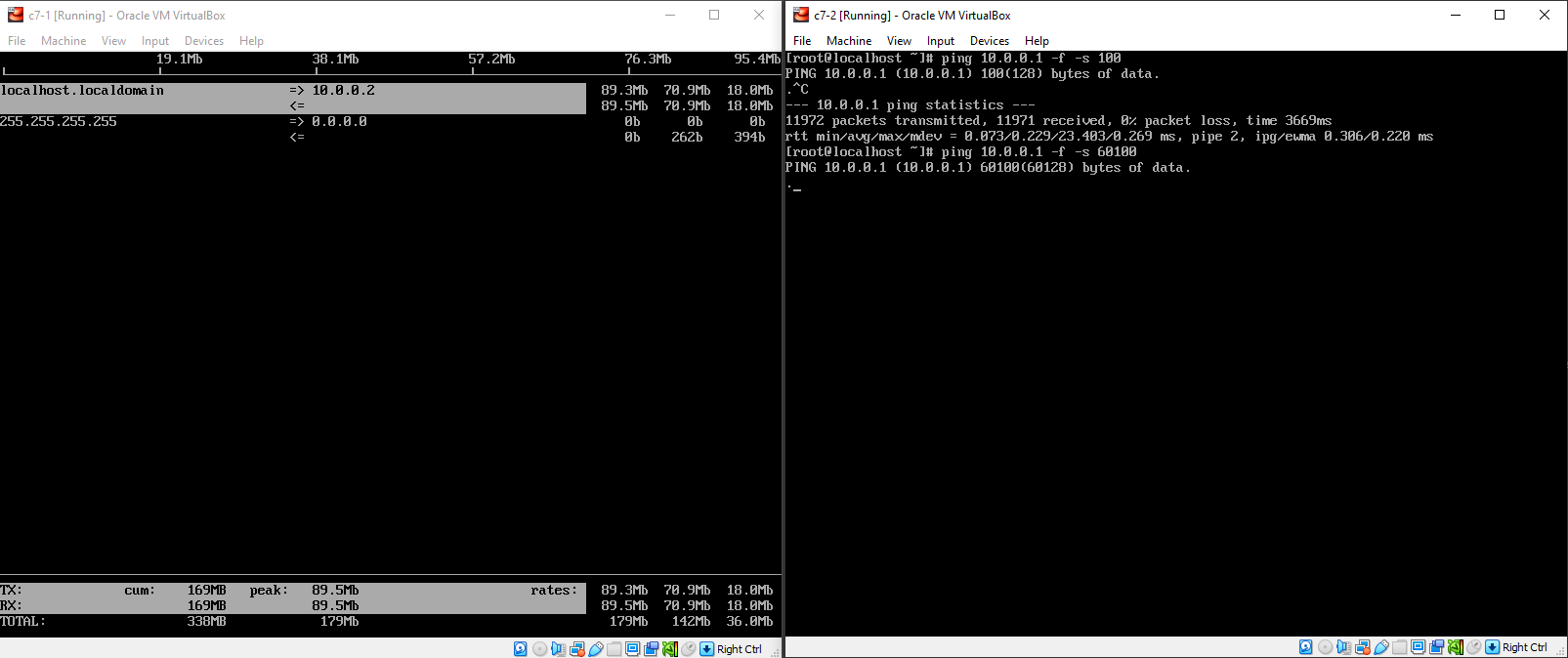
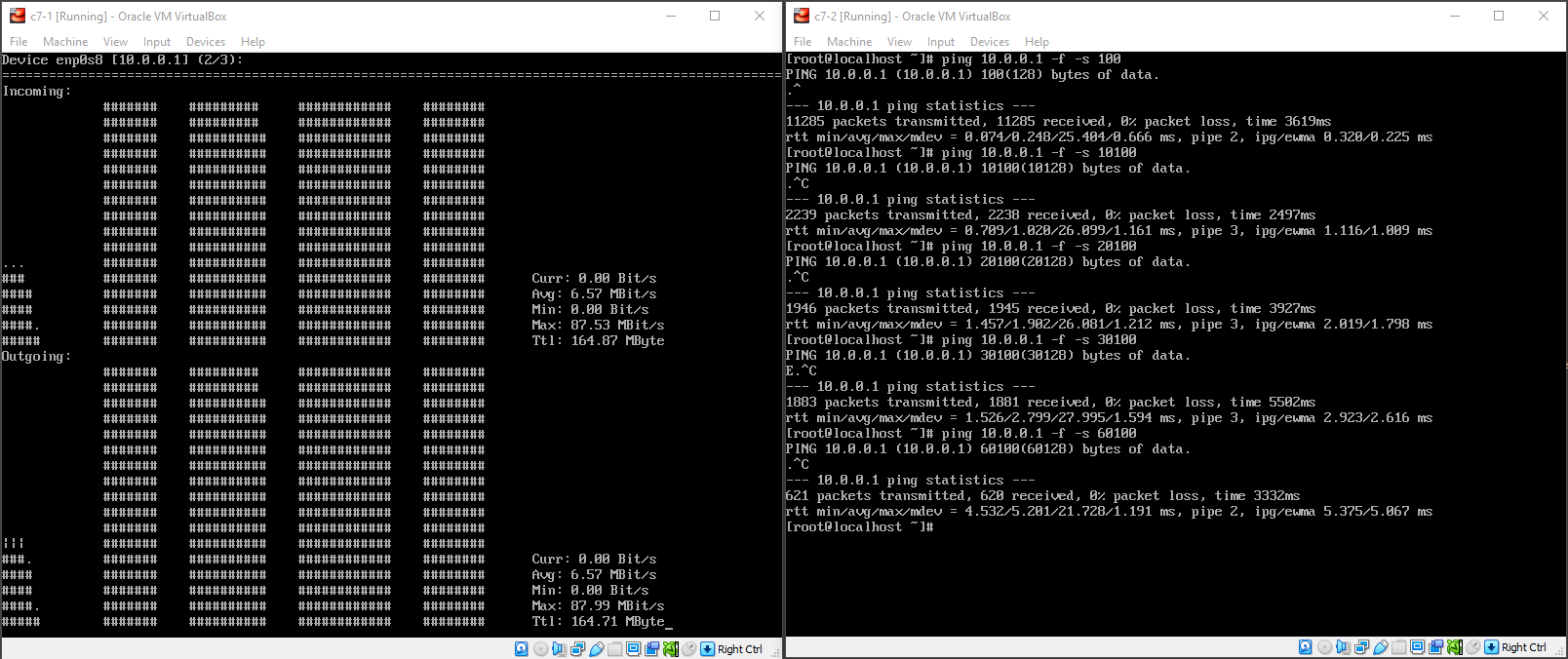
1. **Тексты команд, консольный вывод и полученный файл из Части 2. п. 2,7**

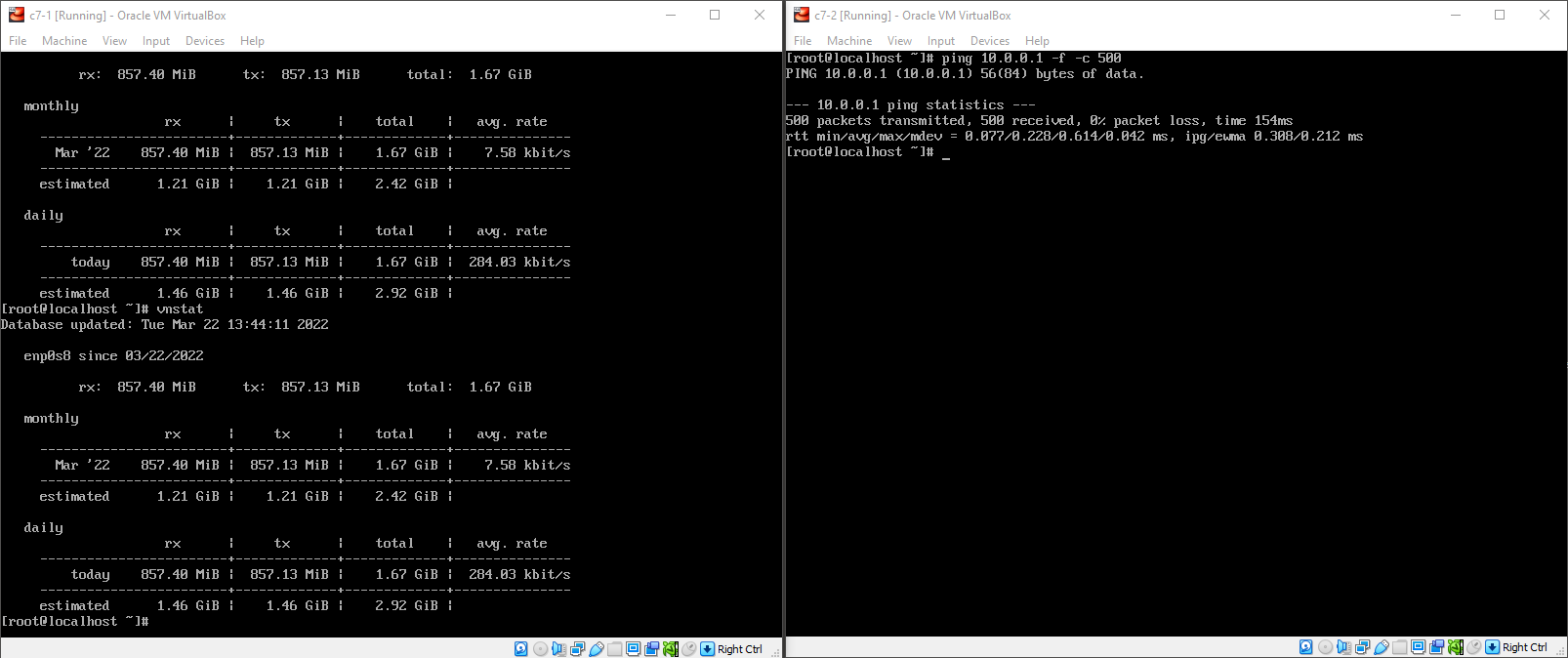
****

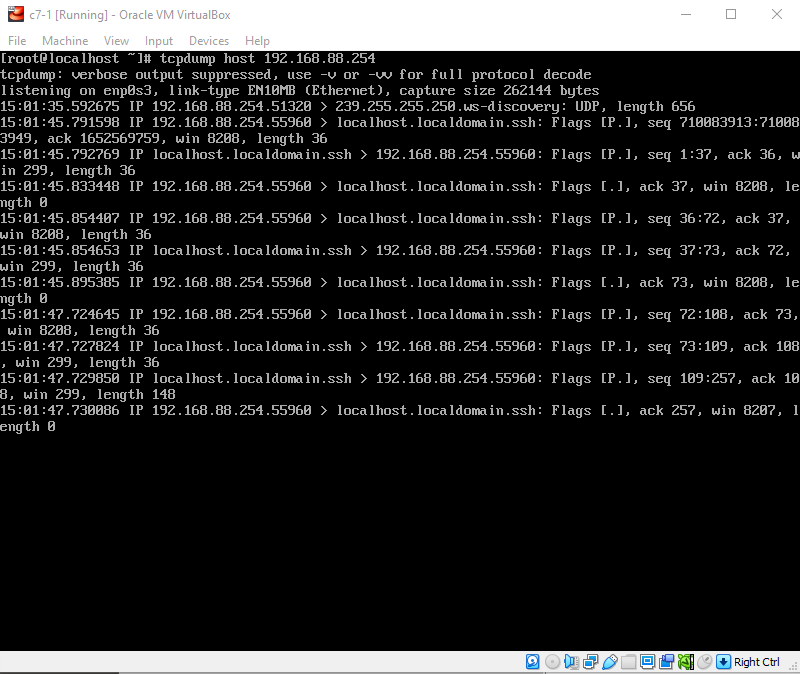
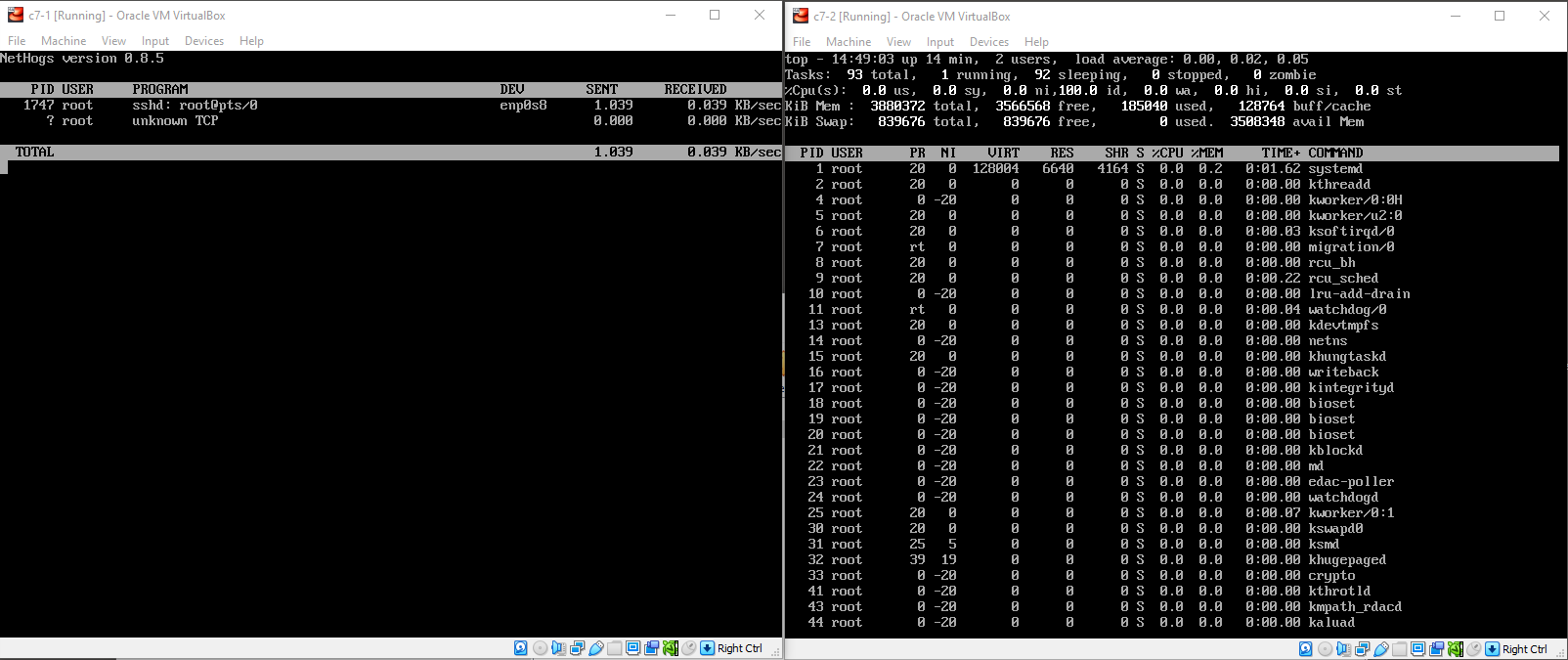
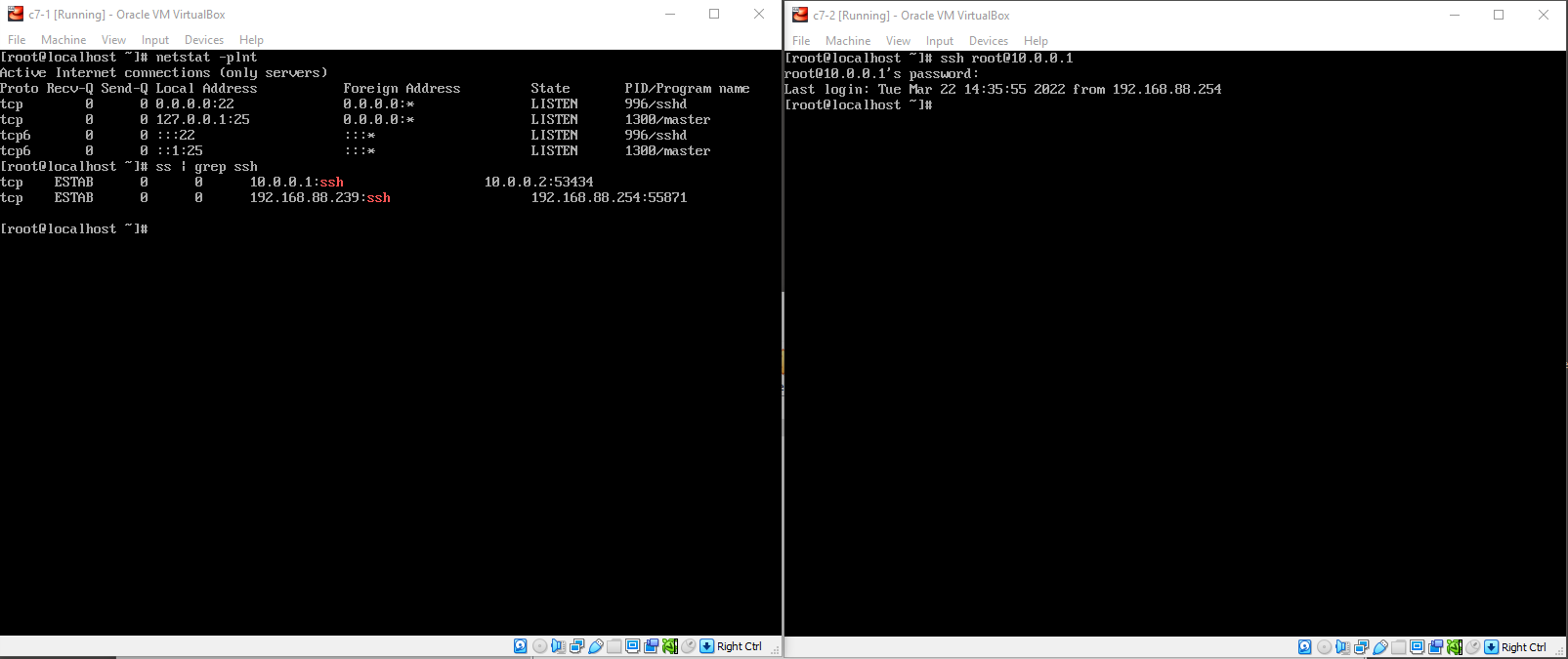
****

1. **Графики, тексты фильтров и ответы на вопросы из Части 3. п. 2-5.**

****

1. **Тексты команд и консольный вывод из Части 4, п.2. **
2. **Тексты команд и консольный вывод из Части 5, п.2. **
3. **Тексты команд и консольный вывод из Части 6, п.4.**

****

1. **Тексты команд и консольный вывод (или его часть) из Части 7, п.2-4, 8,9. **

# Вопросы и задания

1. **По какому протоколу работает утилита mtr? Как вы это определили?**

mtr работает с ICMP, ICMP - это вспомогательный протокол, который используется в основном для диагностики сети.

1. **Опишите значения столбцов статистики, выводимой утилитой mtr.**

Loss% = процент пакетов, на которые не был получен ответ ICMP.

Snt = Количество пакетов, отправленных в каждый хоп.

Last = Время обхода последнего зонда traceroute, в миллисекундах.

Avg = Среднее время обхода всех зондов traceroute, в миллисекундах.

Best = Наименьшее время обхода всех зондов traceroute, в миллисекундах.

Wrst = Наибольшее время прохождения в обе стороны среди всех зондов traceroute, в миллисекундах.

StDev = Стандартное отклонение результатов зондирования до каждого хопа.

1. **Какие типы кадров Ethernet бывают, в чем их отличия?**

Классический Ethernet - в природе в настоящее время не встречается

Ethernet II - он же Arpa, в нём есть поле EtherType - определяющее тип вложения

Ethernet 802.3 - от Novell, он же RAW. В нём поле другое - Length - длинна вложения. Заточенный он только под IPX.

Ethernet 802.2 - он же LLC. Имеет поле Length и LLC - позволяя внутри кадра держать несколько независимых потоков данных

Ethernet SNAP - к тому что выше добавляется поле SNAP - позволяя ещё боле гибко разруливать потоки данных внутри кадра. Часто встречается в сложных сетях, в которых есть ether channel или прочие кастомные протоколы.

1. **Какой тип кадров Ethernet используется в анализируемой сети? Почему именно он?**

Ethernet II - он же Arpa, в нём есть поле EtherType - определяющее тип вложения

1. **Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику? Какой тип коммутационного оборудования использовался в сети?**

Судя по физическому адресу устройства (Включен в отслеживаемый кадр), первая половина его называется OUI (Organizational Unique Identifier), и они распространяются производителям организацией IEEE.

1. **На какие адреса сетевого уровня осуществляются широковещательные рассылки?**

Для уровня-2: Адрес ff:ff:ff:ff:ff:ff:ff:ff является широковещательным адресом.

Для уровня-3: Это последний адрес подсети. Например, для сети 192.168.1.0/24 широковещательный адрес 192.168.1.255

1. **На какой канальный адрес осуществляются широковещательные рассылки?**

Адрес ff:ff:ff:ff:ff:ff:ff:ff является широковещательным адресом для канального уровня.

1. **Для чего применяются перехваченные широковещательные рассылки в Части 3 п. 3-e?**

Большинство перехваченных передач предназначались для обнаружения устройств. В нашем случае MNDP (Mikrotik Network Discovery Protocol) использовался winbox для обнаружения сетевых устройств (Проверено специально).

1. **В Части 4 при разном использовании утилиты traceroute вы получили разные данные. Почему?**

Поскольку большинство этих узлов находятся за фаерволами, защищающими от ненужного трафика и обеспечивающими безопасность, поэтому отображаются звезды. Лучшие результаты были получены при использовании ICMP вместо UDP или TCP, поскольку он предназначен для диагностики сети и разрешен большинством фаерволов.

1. **Какая из утилит из Части 5 вам больше понравилась? Почему?**

По нашему мнению, bmon был лучшим, поскольку он отображает информацию в более организованном виде, в остальном все они служат одной цели.

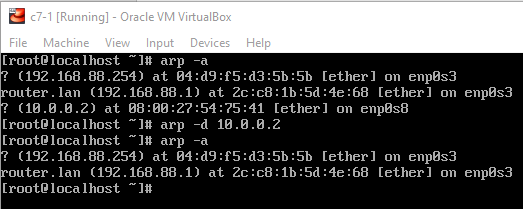
1. **Как изменяется загрузка интерфейса в Части 5. п. 3? Почему?**

Скорость не превышает 11,2 MiB, так как это максимальная скорость для данного интерфейса (100mbps).

1. **На каком уровне модели OSI работает vnstat?**

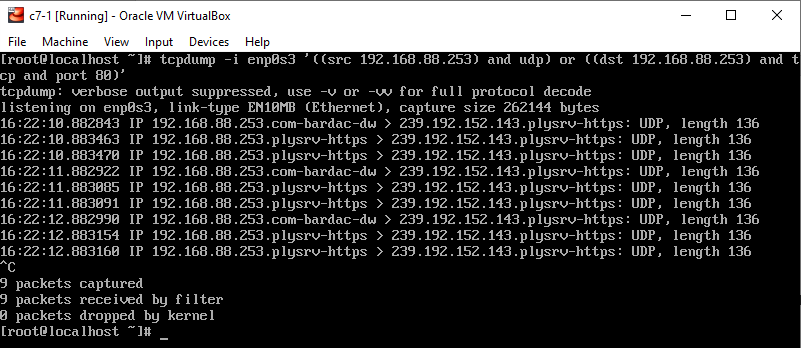
vnstat не является обычным монитором трафика, он использует статистику, предоставляемую кернелом в качестве источника информации, поэтому если мы действительно должны поместить его в модель OSI, то он будет находиться на уровне приложений (уровень 7).

1. **Как с помощью утилиты ip просмотреть arp-кэш и как его очистить. В каких случаях может понадобиться последняя операция?**

****

1. **Напишите команду tcpdump, выводящую все пакеты с хоста 192.168.0.254 и содержащего udp или идущего на tcp порт 80.**

Просто заменить 192.168.88.253 на 192.168.0.254 (скриншот для собственного тестирования)

****