яМИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра вычислительные системы и технологии

ОТЧЕТ

По лабораторной работе №1

РУКОВОДИТЕЛЬ:

_____ Гай В.Е.
(подпись) (фамилия, и.,о.)

СТУДЕНТ:

_____ Расторопов Д.С.
(подпись) (фамилия, и.,о.)

19-В-2
(шифр группы)

Работа защищена «___» _____

С оценкой _____

Нижний Новгород 2022

Задание:

Работа с анализатором протоколов tcpdump

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.

4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

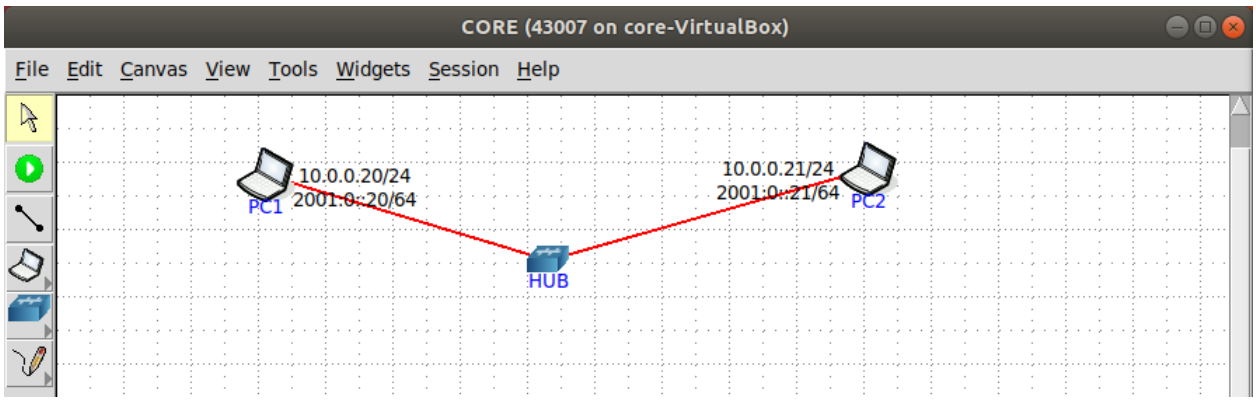
Работа с анализатором протоколов wireshark

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

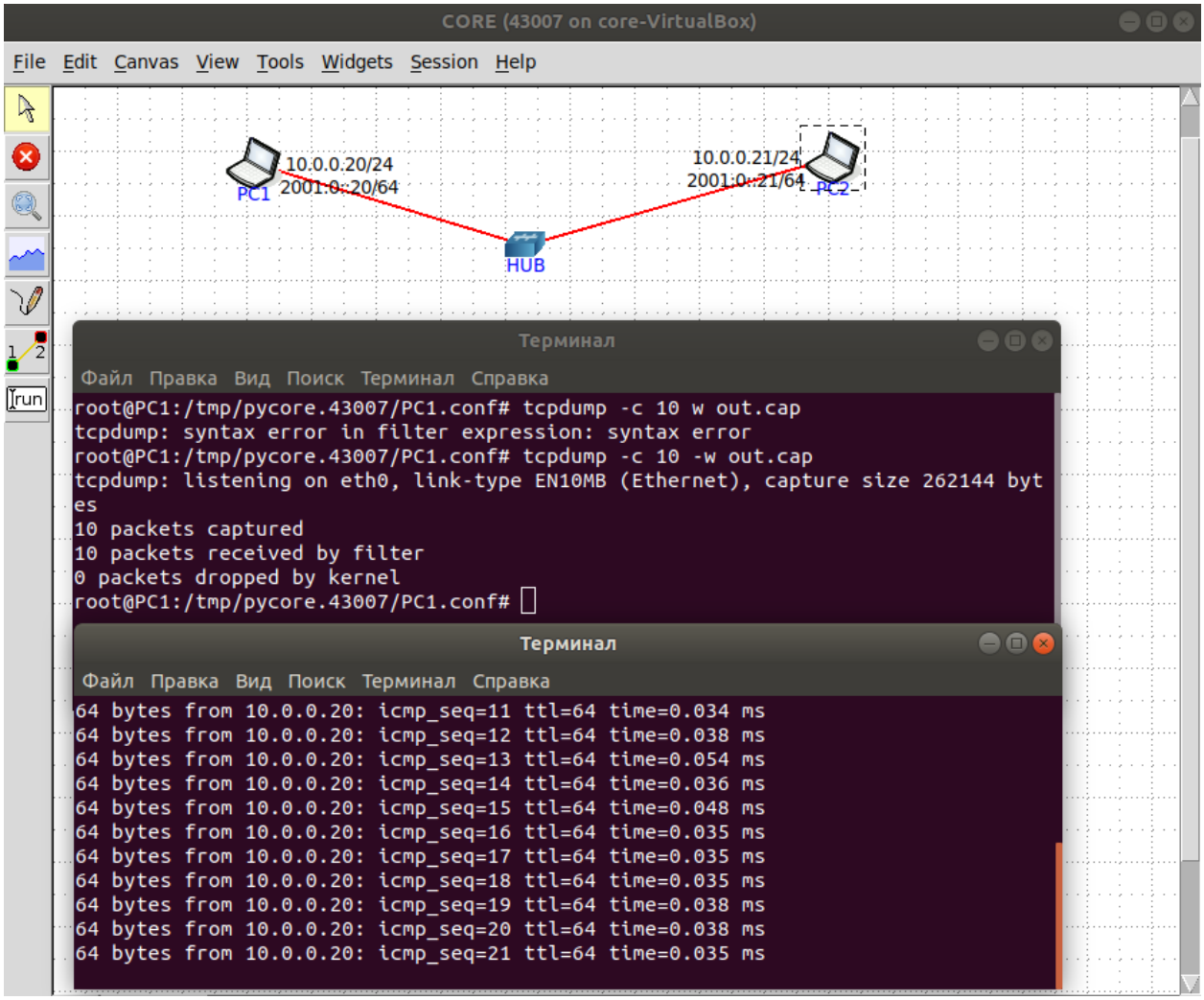
3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

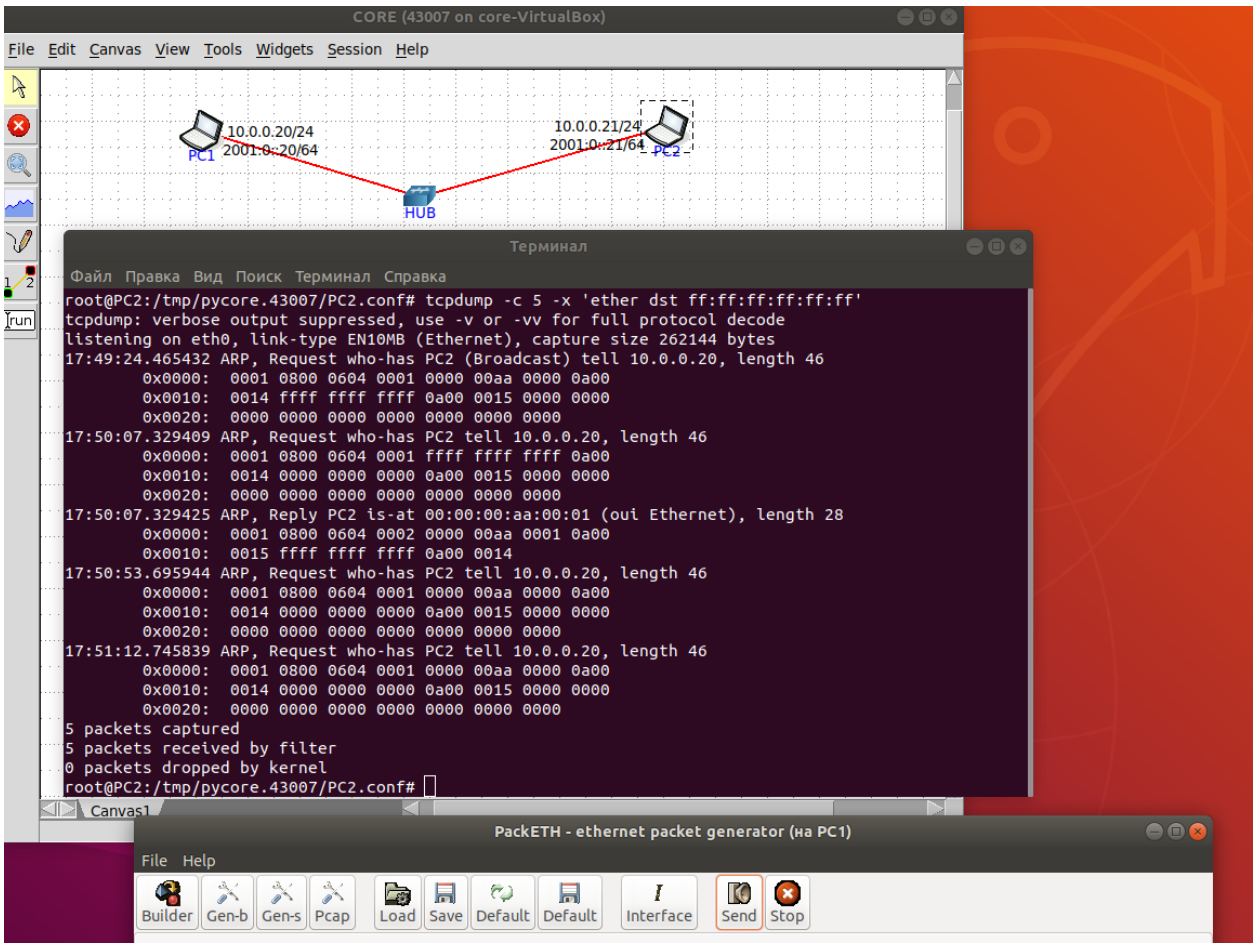


Работа с анализатором протоколов tcpdump

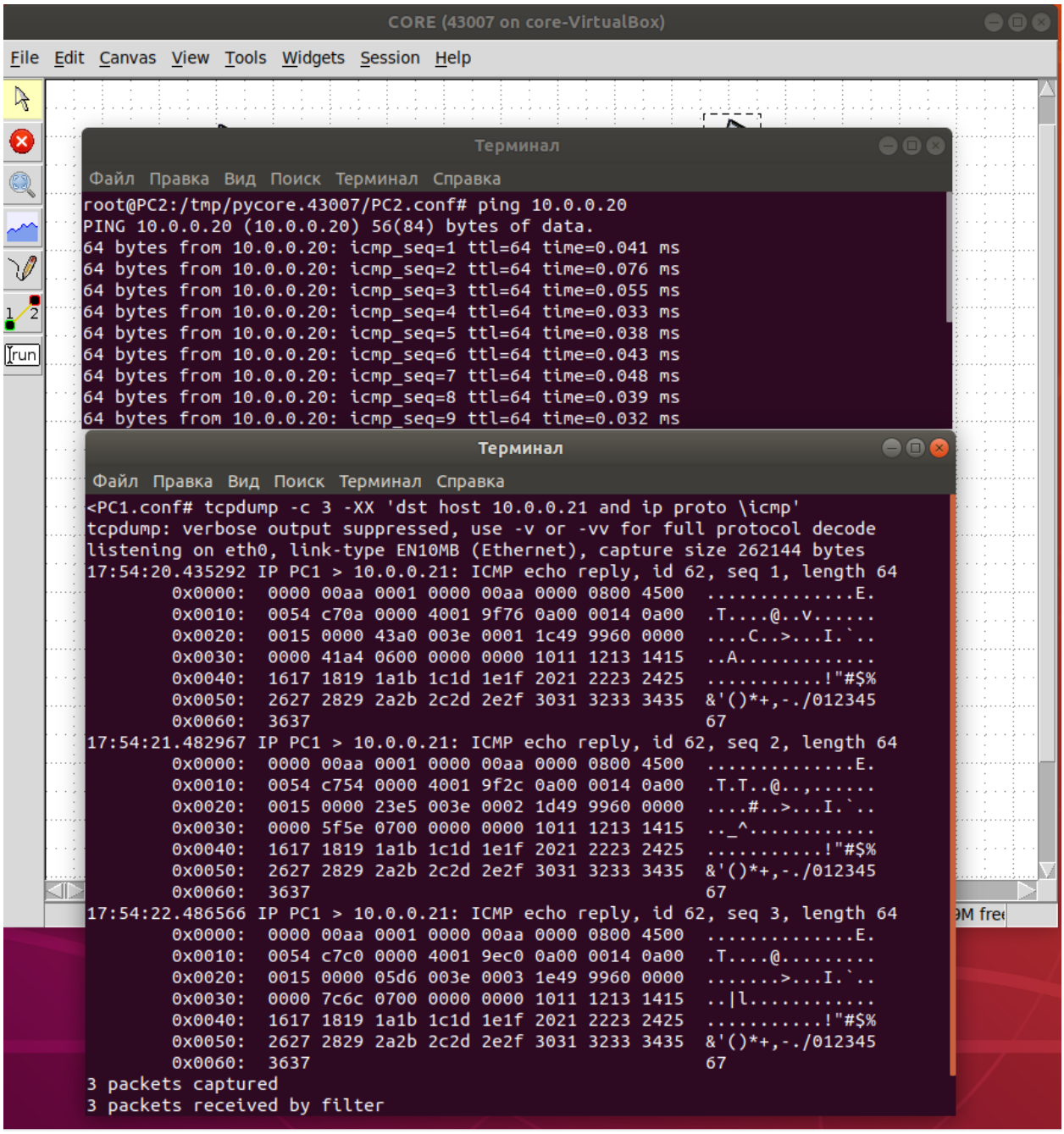
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.



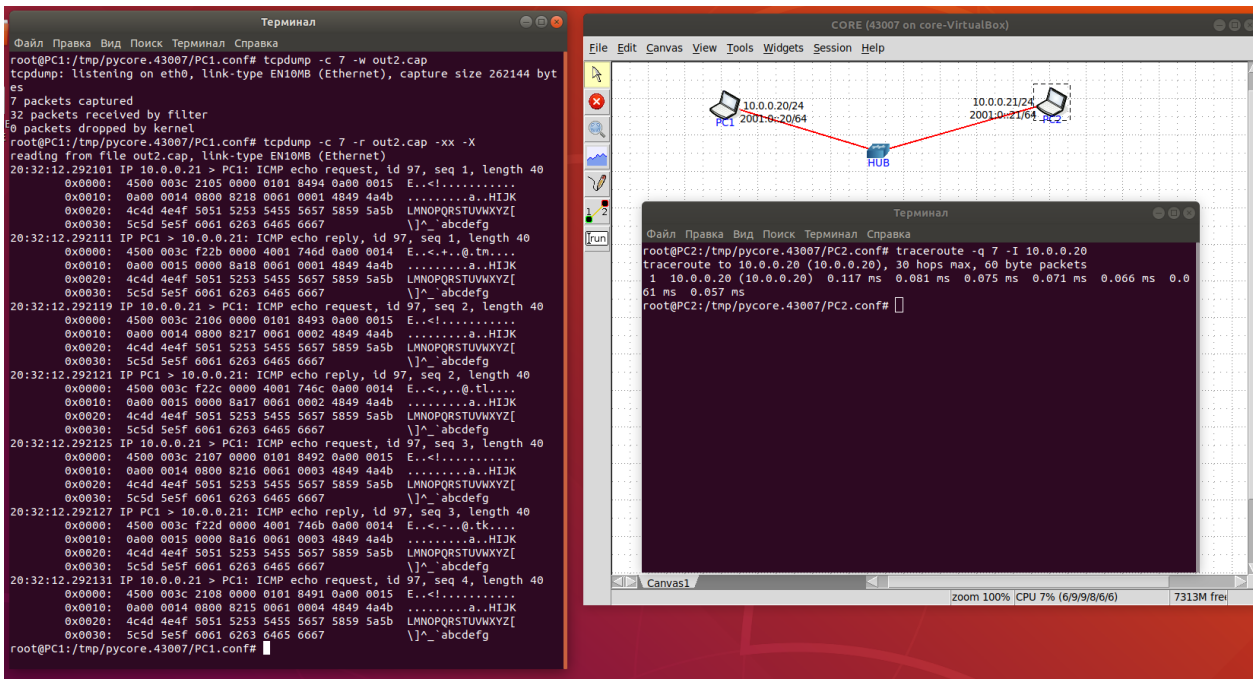
2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).


CORE (43007 on core-VirtualBox)
File Edit Canvas View Tools Widgets Session Help
10.0.0.20/24
2001:0::20/64
PC1
10.0.0.21/24
2001:0::21/64
PC2
HUB
Терминал
Файл Правка Вид Поиск Терминал Справка
root@PC2:/tmp/pycore.43007/PC2.conf# tcpdump -c 5 -x 'ether dst ff:ff:ff:ff:ff:ff'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:49:24.465432 ARP, Request who-has PC2 (Broadcast) tell 10.0.0.20, length 46
0x0000: 0001 0800 0604 0001 0000 00aa 0000 0a00
0x0010: 0014 ffff ffff ffff 0a00 0015 0000 0000
0x0020: 0000 0000 0000 0000 0000 0000 0000
17:50:07.329409 ARP, Request who-has PC2 tell 10.0.0.20, length 46
0x0000: 0001 0800 0604 0001 ffff ffff ffff 0a00
0x0010: 0014 0000 0000 0000 0a00 0015 0000 0000
0x0020: 0000 0000 0000 0000 0000 0000 0000
17:50:07.329425 ARP, Reply PC2 is-at 00:00:00:aa:00:01 (oui Ethernet), length 28
0x0000: 0001 0800 0604 0002 0000 00aa 0001 0a00
0x0010: 0015 ffff ffff ffff 0a00 0014
17:50:53.695944 ARP, Request who-has PC2 tell 10.0.0.20, length 46
0x0000: 0001 0800 0604 0001 0000 00aa 0000 0a00
0x0010: 0014 0000 0000 0000 0a00 0015 0000 0000
0x0020: 0000 0000 0000 0000 0000 0000 0000
17:51:12.745839 ARP, Request who-has PC2 tell 10.0.0.20, length 46
0x0000: 0001 0800 0604 0001 0000 00aa 0000 0a00
0x0010: 0014 0000 0000 0000 0a00 0015 0000 0000
0x0020: 0000 0000 0000 0000 0000 0000 0000
5 packets captured
5 packets received by filter
0 packets dropped by kernel
root@PC2:/tmp/pycore.43007/PC2.conf#
Canvas1
PackETH - ethernet packet generator (на PC1)
File Help
Builder
Gen-b
Gen-s
Pcap
Load
Save
Default
Default
Interface
Send
Stop

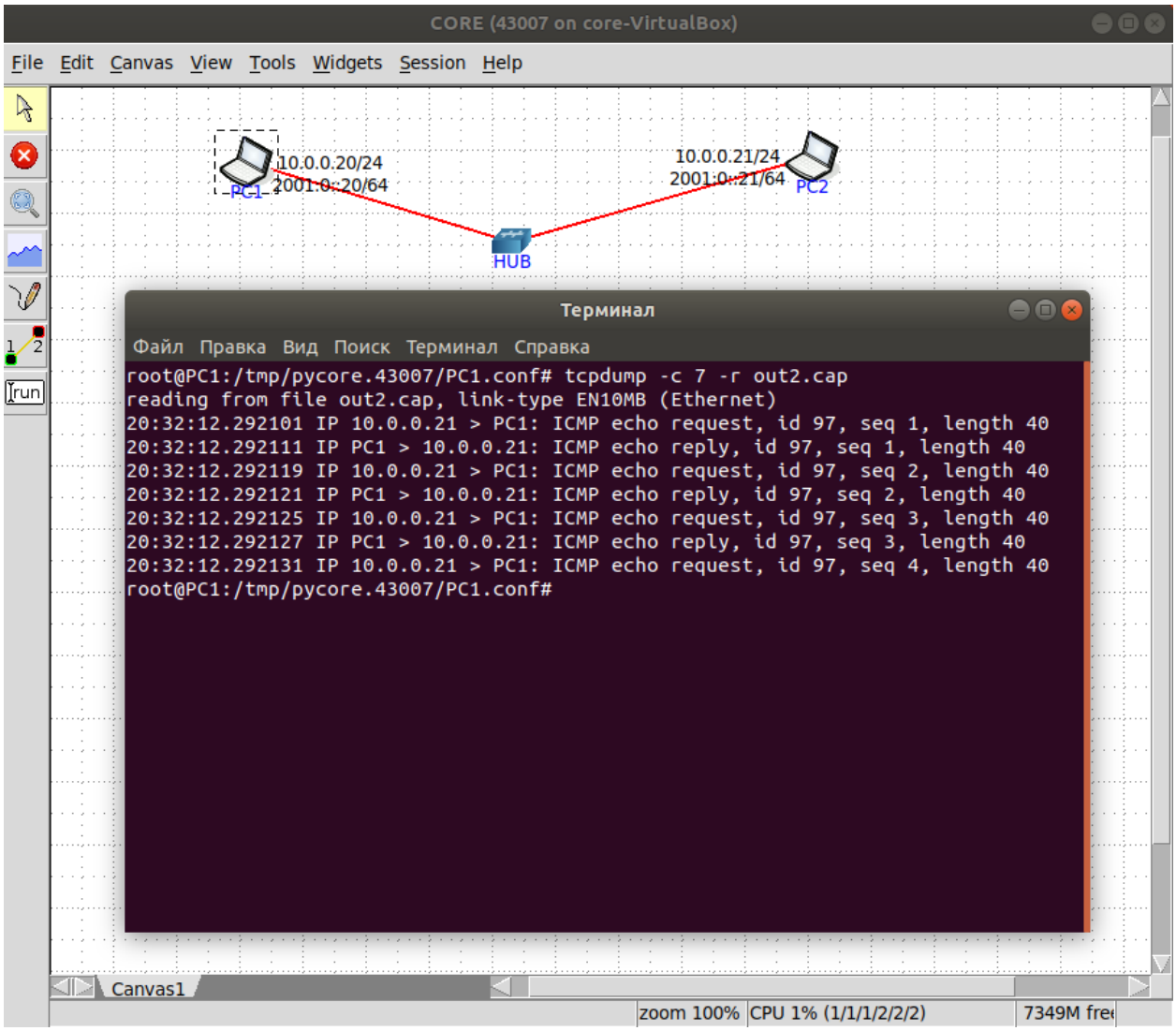
3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.



4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

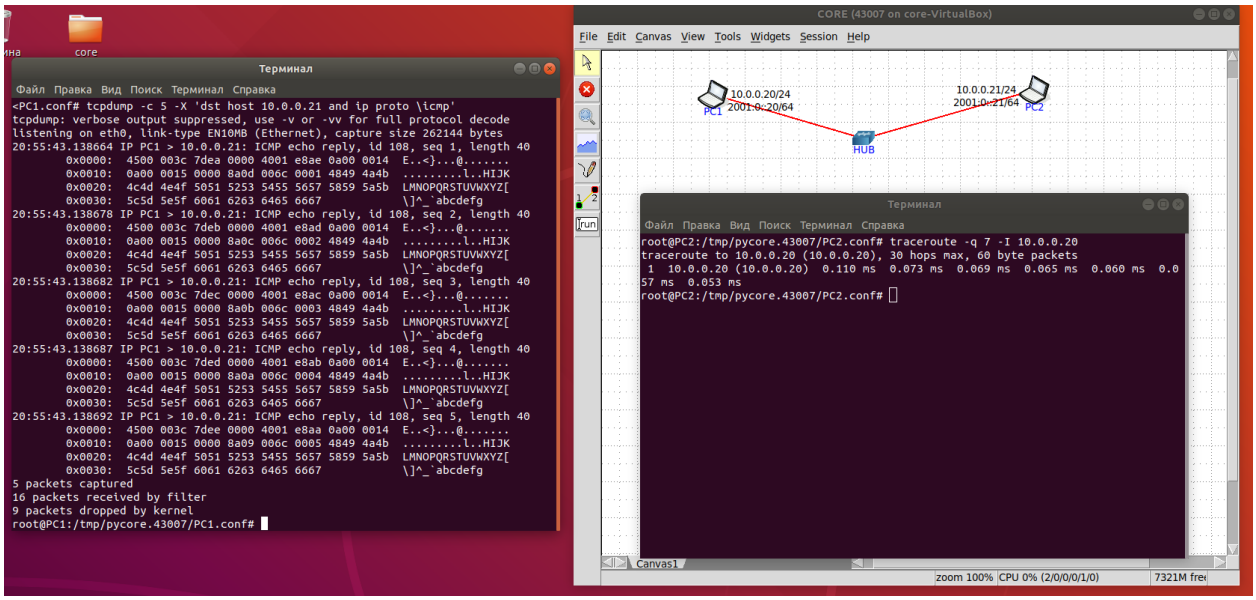


5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

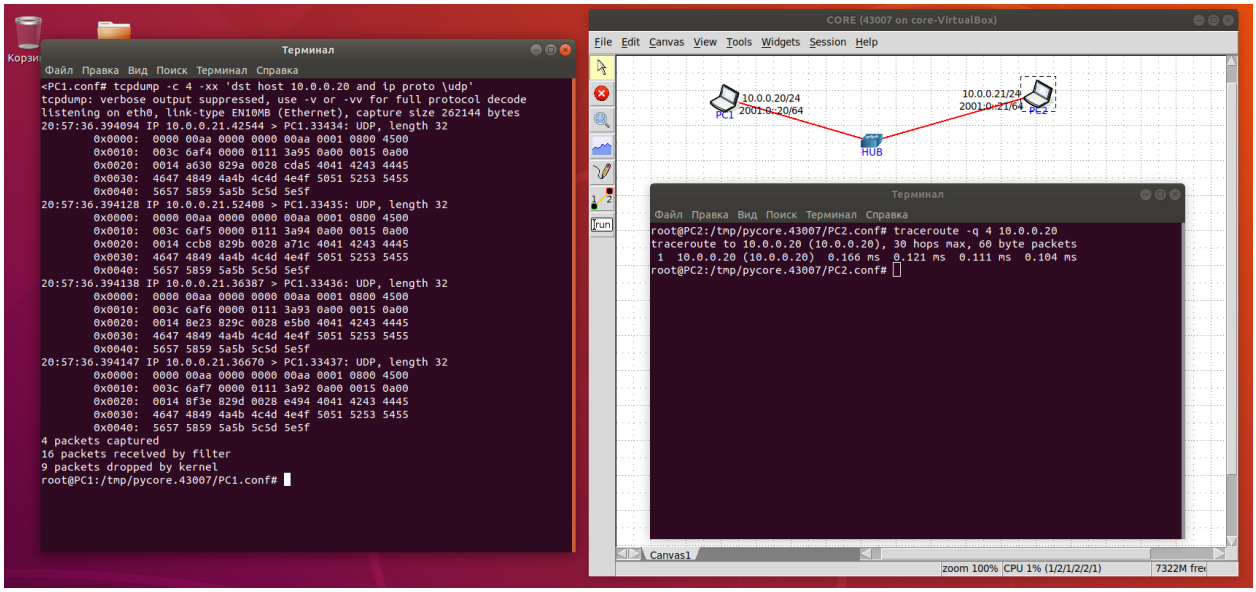


6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

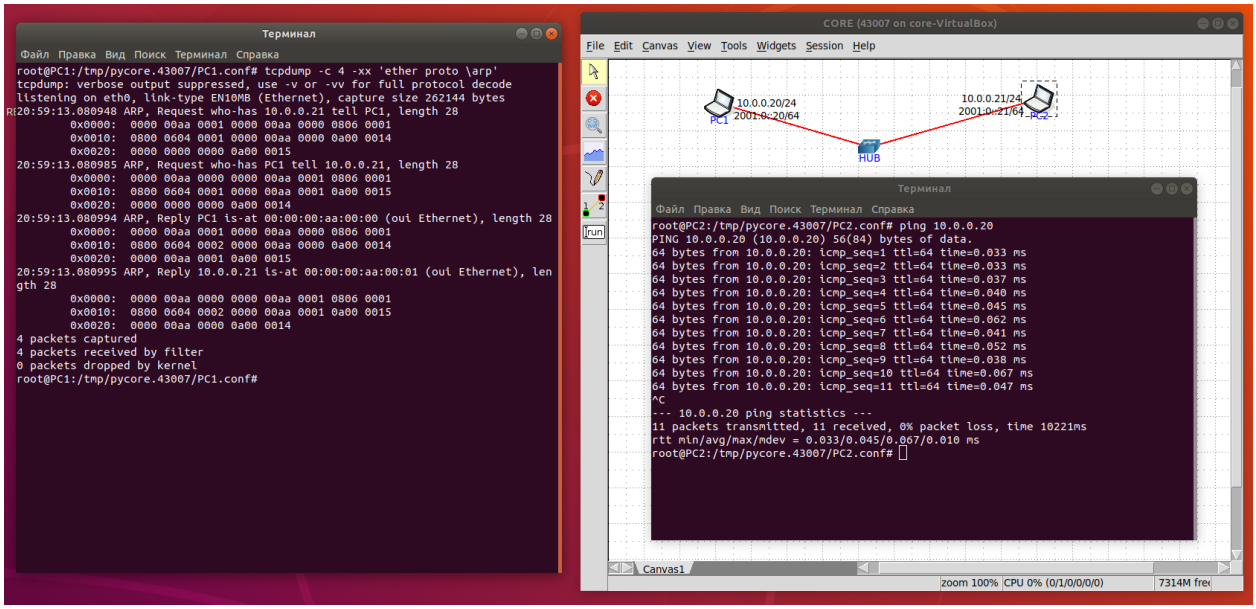
1) Запустить tcpdump так, чтобы он перехватывал только пакеты протоколов ICMP, отправленные на определенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой traceroute. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (не включая заголовок канального уровня). Количество захватываемых пакетов ограничить 5.



2) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола UDP, отправленные на определенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой traceroute. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 4.

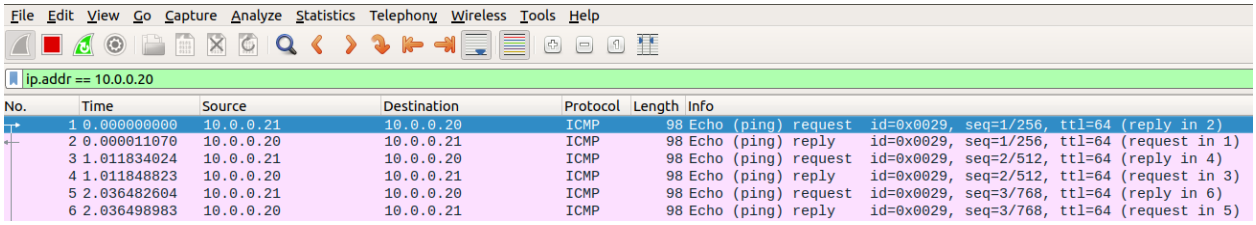


3) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ARP, отправленные на определенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой ping. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 4.

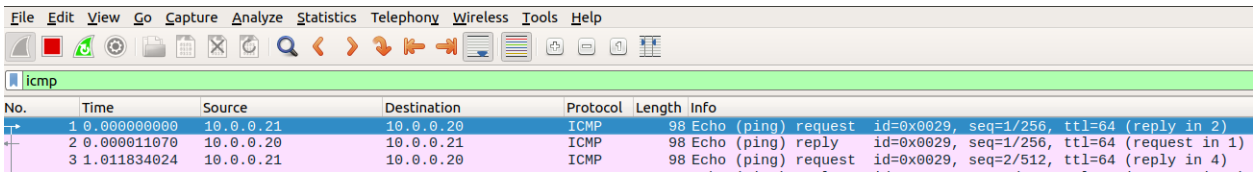


Работа с анализатором протоколов wireshark

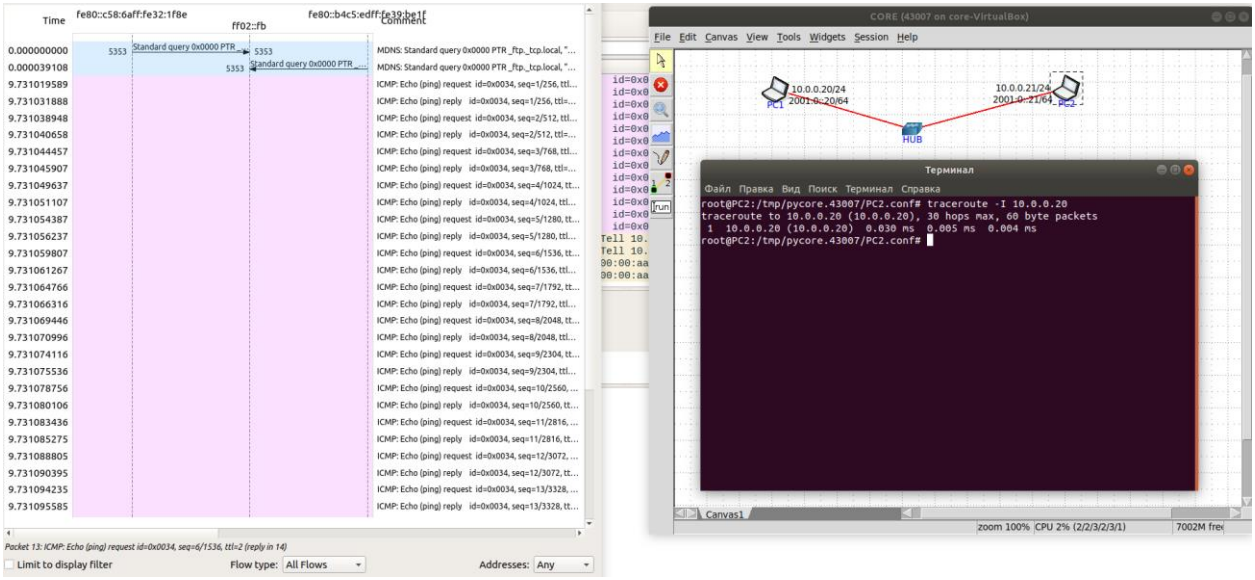
1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.



2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.



3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.



4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.