Санкт-Петербургский Политехнический Университет Петра Великого

Институт металлургии, машиностроения и транспорта

Кафедра «Мехатроника и роботостроение»

Отчет по лабораторной работе

Дисциплина «Сети ЭВМ»

Тема: «. Средства анализа пакетного трафика. Утилита Tcpdump (Windump)»

Выполнил:

Студент гр. 33328/1

Е. Э. Хомутов

Санкт-Петербург

2018

Цель работы

• Ознакомление с принципами работы программ анализа пакетного

трафика;

• Практическое освоение приемов сбора и анализа трафика с помощью

утилиты Tcpdump (Windump);

• Получение навыков расшифровки выходных результатов работы

утилиты Tcpdump.(Windump).

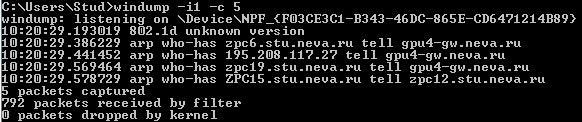
Программа работы.

**Номер рабочего места 15 и IP-адрес ПК – 195.208.117.14**

1. Запустить программу Tcpdump, ознакомиться с форматом вывода и

основными опциями (–c, –e, –q, –n, –x).

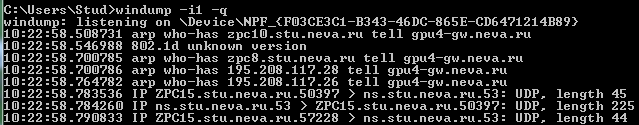
-c выход после обработки count пакетов



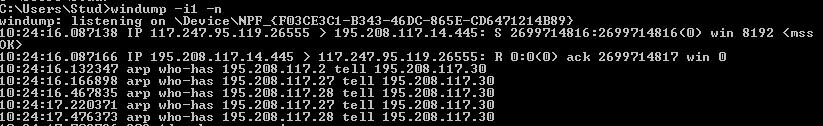
-e выводит заголовки канального уровня в каждой новой строке



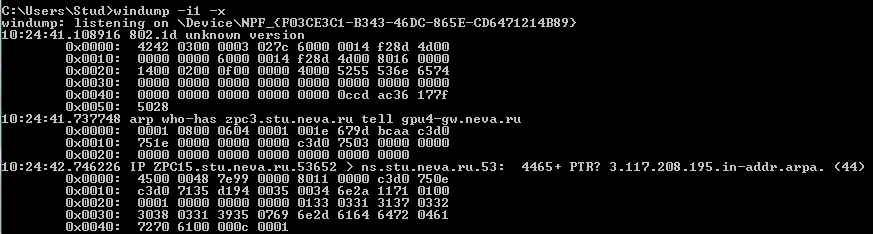
-q выводит информацию в сокращенном виде



-n не преобразовывать адреса (т.e. адрес хоста, номер порта и т.д.) в имена



-x выводит каждый пакет в шестнадцатеричном виде



Расшифровка заголовка IP пакета

 4500: 4 – версия IP протокола (IPv4), 5 – длина заголовка в словах (4байта), т.е 5\*4=20байт, 00 – тип сервиса (низкий приоритет пакет и т.п.)

0048: общая длина пакета – 16 \* 4 + 8 = 72 байта

7e99: идентификатор пакета

0000: три старших бита под флаги (DF-Don’t fragment and MF-More fragments), 13 бит – смещение в 8-байтных словах от начала общего поля данных исходного пакета

80: время жизни – 8 \* 16 = 120, после прохода маршрутизатора – уменьшается на 1

11: UDP Protocol – 8бит -протокол верхнего уровня

0000: контрольная сумма заголовка (если 0, то она не учитыавется)

c3d0 750e: IP адрес источника = 195.208.117.14

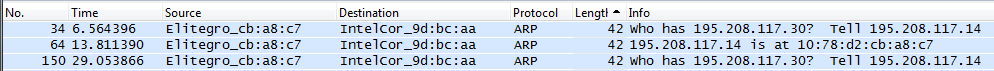
c3d0 7135: IP адрес назначения = 195.208.113.53

2. Средствами программыTcpdump определить минимальный и

максимальный размер пакетов в сети.

Воспользуемся программой Wireshark:

Остановив перехват пакетов и включив сортировку по возрастанию размера пакета, определим, что максимальный размер: 3863 байт, минимальный 42 байта.

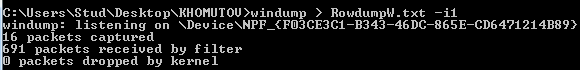


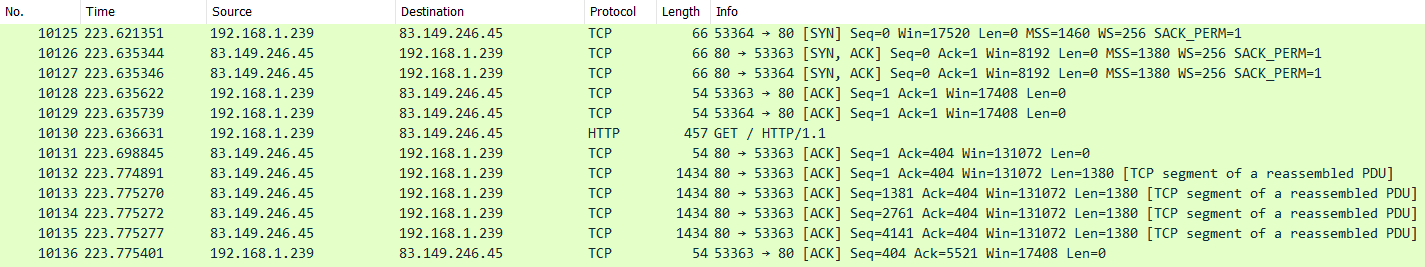
3.



a) Запустить программу Tcpdump с записью необработанных

результатов в файл RowdumpW. Обратиться к WEB-серверу.

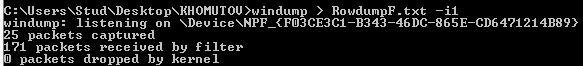


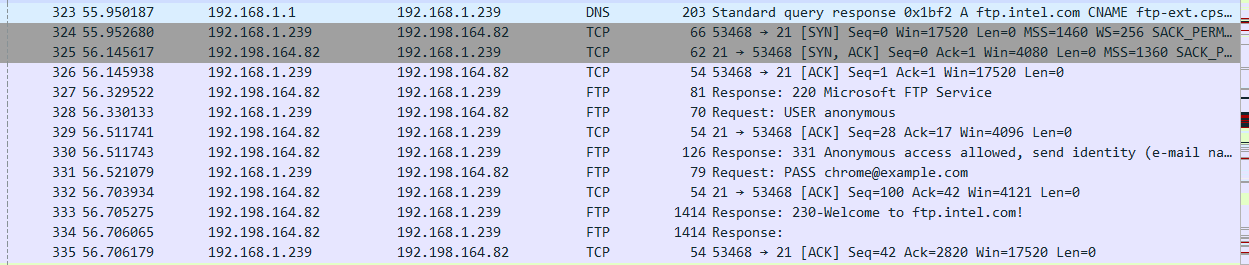


После ответа сервера остановить Tcpdump.

b) Запустить программу Tcpdump с записью необработанных

результатов в файл RowdumpF. Обратиться к FTP-серверу.

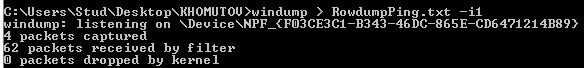


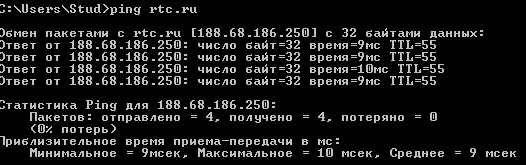


После ответа сервера остановить Tcpdump.

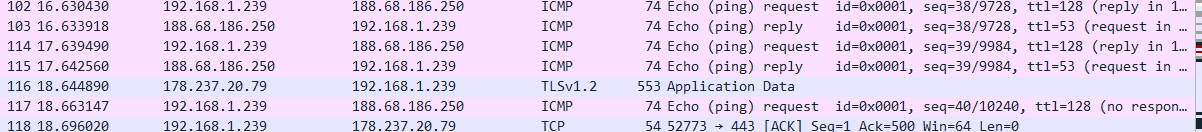
c) Запустить программу Tcpdump с записью необработанных

результатов в файл RowdumpPing. Выполнить команду Ping .





Сохранить результат (вывод команды Ping) в файле RowdumpPing.txt.

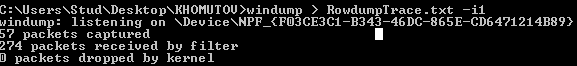


Эхо-отклик = 16.630430 – 16.633918 = 0.003488 c

Остановить Tcpdump.

d) Запустить программу Tcpdump с записью необработанных

результатов в файл RowdumpTrace. Выполнить команду tracert.

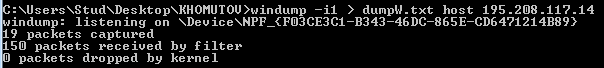


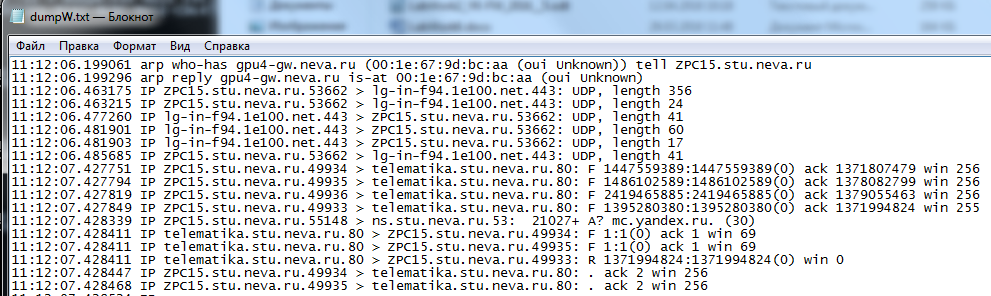


Сохранить результат в файле RowdumpTrace.txt. Остановить Tcpdump.

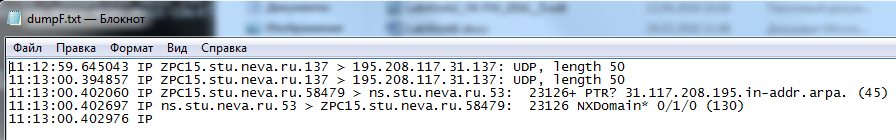


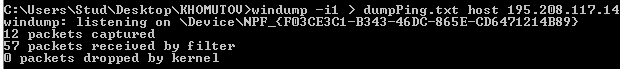
5. Обработать файл Rowdump (файлы RowdumpW, RowdumpF, RowdumpPing, RowdumpTrace) с целью вывода всех пакетов вашего компьютера. Сохранить результаты в файлах dumpW.txt, dumpF.txt, dumping.txt. dumptrace.txt соответственно.

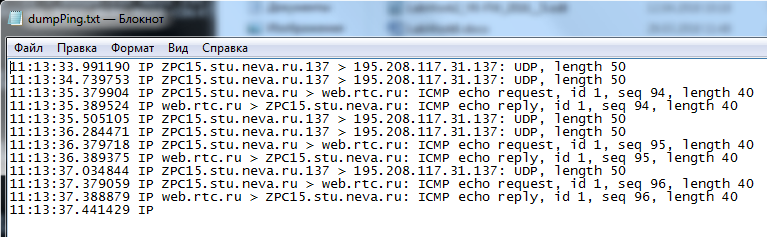












Эхо-отклик = 35.389524 – 35.379904 = 0.00962 c

