Московский государственный технический университет им. Н.Э. Баумана

Факультет «Информатика и системы управления»

Кафедра «Автоматизированные системы обработки информации и управления»



**“Сети и сетевые технологии”**

**“Исследование протоколов транспортного уровня IP-сетей”**

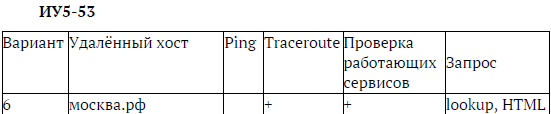
**Лабораторная работа № 9**

Студент группы ИУ5 -53 Бодунов А.Г.

Преподаватель \_\_\_\_\_\_\_\_\_\_\_\_ Аксенов.А.В.

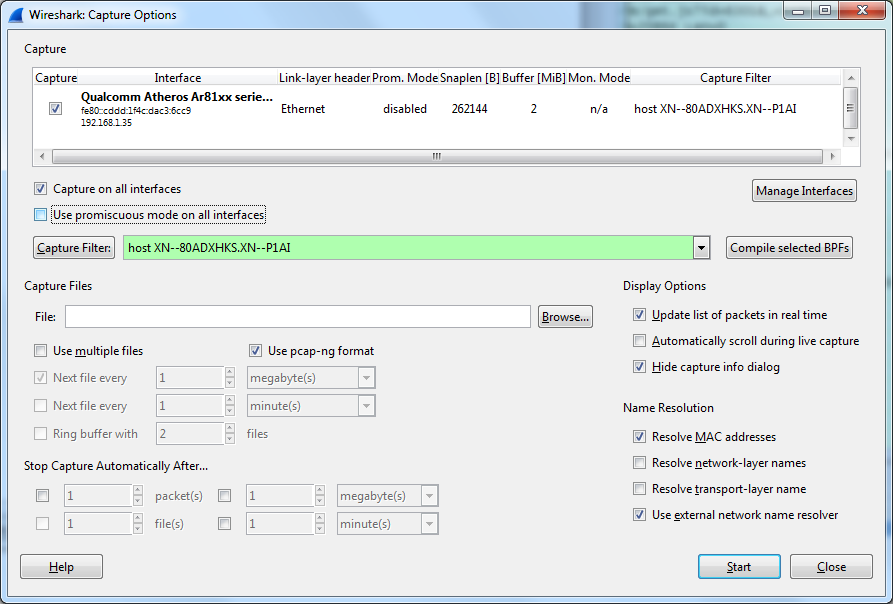
**Москва 2016**

Исходные данные для выполнения лабораторной работы:

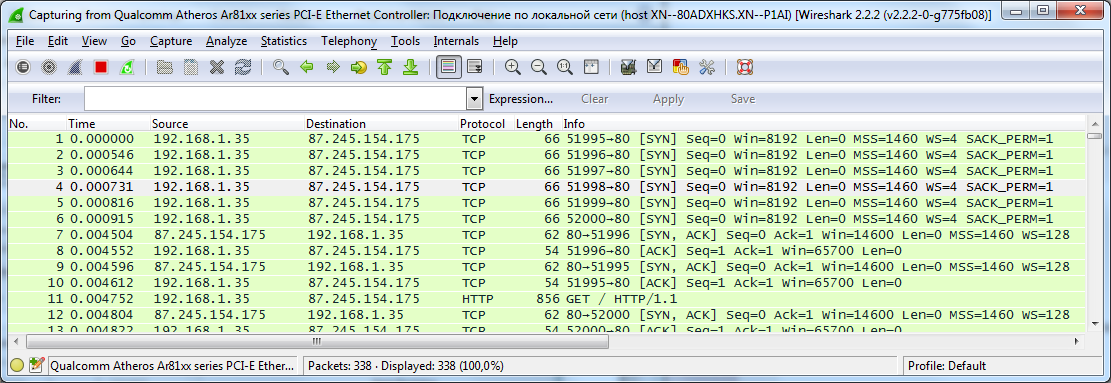


1)Инициируем TCP сеанс с хостом, указанным в нашем варианте(6 ,москва.рф).

2)Для этого настраиваем пакетный фильтр wireshark на хост москва.рф, заменяя его в строке фильтра wireshark на XN--80ADXHKS.XN--P1AI(описание замены было указано в ЛР №8)



Нажимаем на кнопку start и смотрим пакеты на интерфейсе Ethernet.Смотрим первые строчки:



Первые 5 строчек отражают попытки подключения к хосту москва.рф. Поскольку интернет-соединение было относительно медленным, успехом увенчалась только 6-я попытка. Здесь мы видим механизм троекратного рукопожатия.

6 0.000816 192.168.1.35 87.245.154.175 TCP 66 51999→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK\_PERM=1

Строка 6 показывает запрос от локального компьютера к серверу (87.245.154.175) с флагом SYN и ISN = 0.

Ответ сервера:

7 0.004504 87.245.154.175 192.168.1.35 TCP 62 80→51996 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=128

ISN сервера также = 0,флаги SYN и ASC = 1,подтверждаемый ISN клиента = 1(увеличен на 1)

Ответ клиента:

8 0.004552 192.168.1.35 87.245.154.175 TCP 54 51996→80 [ACK] Seq=1 Ack=1 Win=65700 Len=0

ISN сервера и клиента =1, установлен в 1 флаг подтверждения ACK.

Соединение установлено.

Далее компьютер периодически запрашивает от сервера информацию, посылая ему пакеты типа GET.

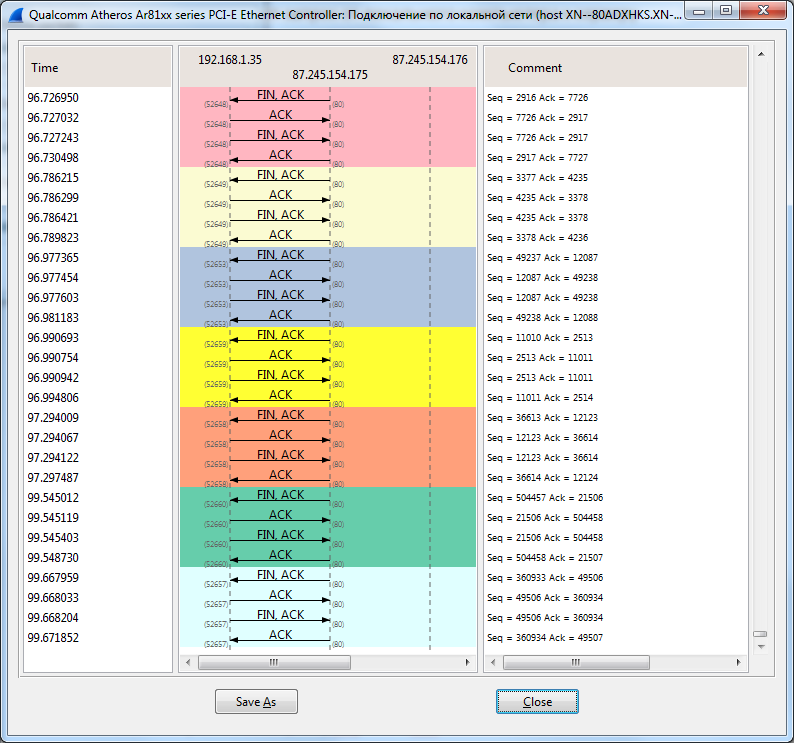
32 0.598994 192.168.1.35 87.245.154.175 HTTP 813 GET /api/catalog/v1/frontend/json/ru/catalog/pgu/popular HTTP/1.1

Чтобы сохранить соединение, не разрывая его, клиент и сервер обмениваются пакетами типа TCP KeepAlive, посылая их друг другу и отвечая на них:

330 156.343077 192.168.1.35 87.245.154.175 TCP 55 [TCP Keep-Alive] 51999→80 [ACK] Seq=698 Ack=1690 Win=65692 Len=1

331 156.346575 87.245.154.175 192.168.1.35 TCP 60 [TCP Keep-Alive ACK] 80→51999 [ACK] Seq=1690 Ack=699 Win=16000 Len=0

Далее при отсутствии обращения от клиента к серверу в течение долгого времени сервер закрывает соединения по всем открытым ранее портам:



Сервер отсылает пакет закрытия соединения FIN , закрывая поток данных со своей стороны:

1865 99.667959 87.245.154.175 192.168.1.35 TCP 60 80→52657 [FIN, ACK] Seq=360933 Ack=49506 Win=372 Len=0

В ответ на пришедший пакет локальный компьютер отсылает пакет подтверждения с ICN ,увеличенным на 1(360934):

1866 99.668033 192.168.1.35 87.245.154.175 TCP 54 52657→80 [ACK] Seq=49506 Ack=360934 Win=65247 Len=0

Клиент также закрывает свой поток данных:

1867 99.668204 192.168.1.35 87.245.154.175 TCP 54 52657→80 [FIN, ACK] Seq=49506 Ack=360934 Win=65247 Len=0

Сервер подтверждает закрытие соединения флагом ACK и ICN, увеличенным на 1(49507)

1868 99.671852 87.245.154.175 192.168.1.35 TCP 60 80→52657 [ACK] Seq=360934 Ack=49507 Win=372 Len=0

Соединение закрыто.