Федеральное агентство связи Российской Федерации
Государственное образовательное учреждение
высшего профессионального образования
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

А.Е. Костюкович

Методические указания

к лабораторной работе № 5

«Анализ протоколов службы Web»

Новосибирск – 2011

А.Е. Костюкович

Аннотация.

Методические указания к лабораторной работе для дисциплины «Информационные сервисы для СПС». Могут быть также использованы в процессе изучения дисциплин "Мультисервисные сети" и "Пакетная телефония".
В данной лабораторной работе студенту предоставляется возможность получить дополнительную информацию о работе службы и сервисов Web.

Кафедра АЭС
Ил. 15, список лит. - 13

Рецензент – Мелентьев О.Г.

По направлению – 210400 - Телекоммуникации

Утверждено редакционно-издательским советом СибГУТИ
в качестве методических указаний

Оглавление	
	Стр.
1. Цель работы	
2. Порядок выполнения работы	
3. Правила оформления отчета	
4. Контрольные вопросы	
5. Литература	

1. Цель работы:

1.1. На примере трассировки протоколов службы Web – изучить возможности анализатора протоколов Wireshark, приобрести навыки трассировки протоколов и глубже познакомиться с работой сервисов Web.

1.2. Выполнить анализ сделанных трассировок и отразить это в отчете

2. Порядок выполнения работы

Для понимания работы с анализатором, в данной лабораторной работе мы будем исследовать коммуникационные процессы, поддерживающие службу Web.

Порядок выполнения ЛР - 5 следующий:

2.1. Запускаем процесс перехвата пакетов анализатором Wireshark
2.2. Запускаем исследуемые процессы, для чего:
  2.2.1. Запускаем Ваш браузер (Internet Explorer, Mozilla Firefox или Opera)
  2.2.2. В адресной строке браузера набираем адрес сайта http://aek-54.ru
  2.2.3. Дожидаемся окончания загрузки начальной страницы сайта
2.3. Останавливаем процесс перехвата пакетов анализатором Wireshark
2.4. Копируем результаты выполнения процессов службы Web в отчет (файл в формате ЛР-5.doc)
2.5. Сохраняем результаты перехвата пакетов анализатором Wireshark в файле с именем web.pcap
2.6. Производим анализ результатов перехвата пакетов
2.7. Оформляем отчет по данной работе и отсылаем файл отчета ЛР-5.doc в адрес дистанционного деканата

2.1 Запускаем процесс перехвата пакетов анализатором Wireshark

2.1.1 В пункте меню **Capture** (фиксация, перехват) выберите **Options**.

2.1.2 Для того, чтобы следить за процессом перехвата всех пакетов (**без фильтрации**) – выберите режим «**Capture packets in promiscuous mode**» (Перехват всех пакетов без разбора) – для этого **уберите галочку** в соответствующем окне.

2.1.3 Чтобы начать перехват пакетов нажмите на значок  (**Start**) **главной панели**, либо кнопку «**Start**» в окне **Capture** – **Options.**

2.1.4 В появившемся списке сетевых интерфейсов выберите тот интерфейс, **для которого** параметр «**Packets**» постоянно увеличивается (это означает, что на данном интерфейсе **наблюдается активность**).

2.1.5 Для начала перехвата нажмите кнопку «**Start**» **для активного сетевого интерфейса**.

2.1.6 В рабочей области программы начнут сразу же появляться новые строчки. Каждая строчка – это сетевой пакет. Нажав на интересующую строчку, в нижнем окне появится расшифровка полей пакета в виде иерархического списка.

2.2 Запускаем исследуемые процессы службы Web

2.2.1 Запускаем Ваш браузер (Internet Explorer, Mozilla Firefox или Opera)
2.2.2 В адресной строке браузера набираем адрес сайта http://aek-54.ru
2.2.3 Дожидаемся окончания загрузки начальной страницы сайта

2.3 Останавливаем процесс перехвата пакетов анализатором Wireshark

Для остановки перехвата пакетов необходимо нажать на значок  (**Stop**) на панели управления.

2.4 Копируем результаты выполнения процессов службы Web в отчет (файл в формате ЛР-5.doc)

Используя функцию Print Screen – скопировать соответствующие экранные формы (см. пункты 2.6 данных методических указаний) и вставить их в файл отчета.

2.5 Сохраняем результаты перехвата пакетов анализатором Wireshark в файле с именем web.pcap

Для сохранения результатов перехвата пакетов выберите в пункте меню **File** главной панели пункт **Save as**:

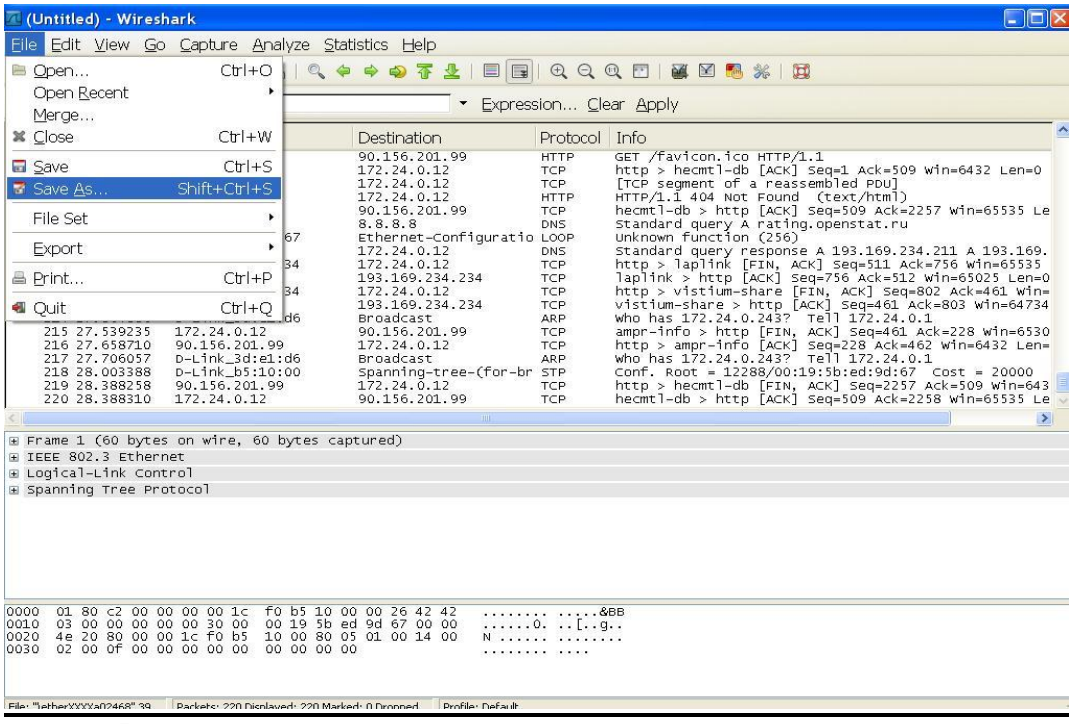


Рисунок 1 – сохранение результатов перехвата пакетов

Присвойте сохраняемому файлу имя и выберите расширение сохраняемого файла – **web-aek.pcap**, (вариант Wireshark/tcpdump…, который обычно предлагается по умолчанию).

Сохраненный файл с перехваченными Вами пакетами необходимо выслать как приложение к отчету по данной лабораторной работе.

Внимание:

Для правильного выполнения лабораторной работы необходимо соблюдать **следующие условия**:

1. Запускать приложение Wireshark (кнопка “START”) надо до запуска исследуемого процесса, а завершать приложение Wireshark (кнопка “STOP”) надо после остановки Вами исследуемого процесса. В этом случае в сохраняемом файле будут пакеты, соответствующие всему сеансу исследуемого процесса.
2. Следить, чтобы длительность работы Wireshark по перехвату пакетов не превышала 1 минуты. Для усвоения основных навыков работы этого достаточно! Превышение работы Wireshark приведет к тому, что размеры файла с перехваченными пакетами будут настолько большими, что это не позволит Вам не только передать Ваш файл в качестве приложения к отчету, но и забъет Ваш диск до полной остановки ОС. Например, для скорости Вашего интерфейса – 100 Мбит/с в каждую секунду будут перехватываться пакеты с общим объемом до 12 Мбайт, следовательно, за час работы Wireshark (3600 с) на Ваш диск набъется пакетов до 43-х Гбайт!!!

2.6 Анализ результатов перехвата пакетов

По умолчанию анализатор перехватывает все пакеты, от служб, которые работают на Вашем компьютере, поэтому вначале анализа, необходимо научиться работать с фильтрами, выбирая интересующие Вас протоколы.

В данном случае нас интересуют протоколы **TCP и HTTP**, используемые процессами службы Web.

Чтобы отфильтровать пакеты протоколов **TCP и HTTP**, введите в окне **Filter** маску **TCP** и нажмите «Enter». Когда маска введена правильно, поле ввода подсвечивается **зеленым** цветом, в противном случае – красным.

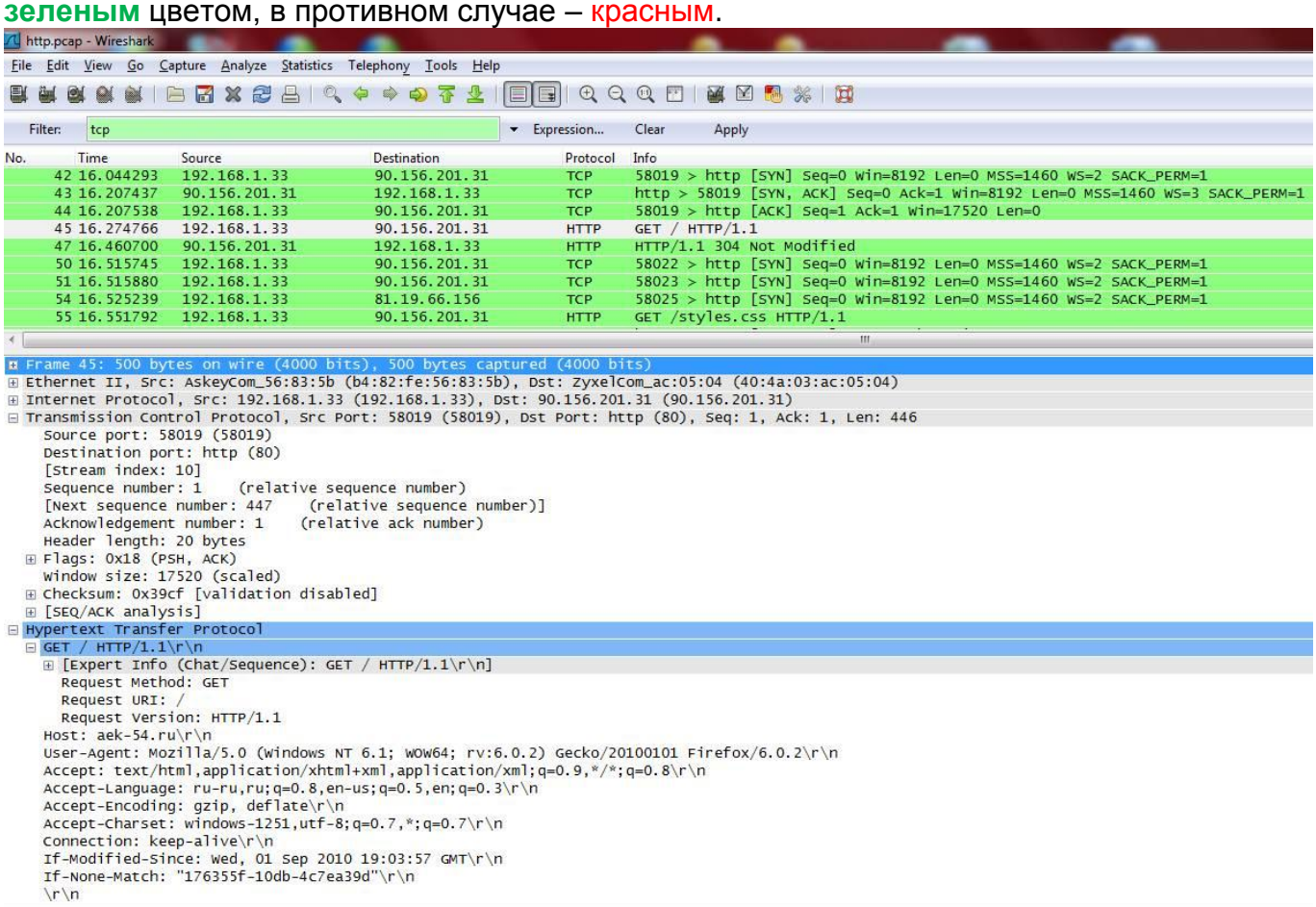


Рисунок 2 – Фильтрация пакетов TCP из общего потока перехваченных пакетов

Ваши комментарии по полям протоколов TCP и HTTP (по рис.2, но с данными Вашего перехвата): …….

Теперь необходимо привести результаты анализа пакетов TCP/HTTP:

2.6.1 В окне рисунка 2 мы видим детальную информацию о заголовках протоколов TCP и HTTP, а также тело запроса Get протокола HTTP. **Вам необходимо проанализировать и оставить на этом рисунке (или после него) комментарии по полям протокола TCP и HTTP, используя материалы лекций 10 и 15.**

2.6.2 Через пункт меню – **Statistics – IO-Graphs** покажите график скорости передачи пакетов TCP/HTTP (разними цветами) в бит/с – см. рис.3

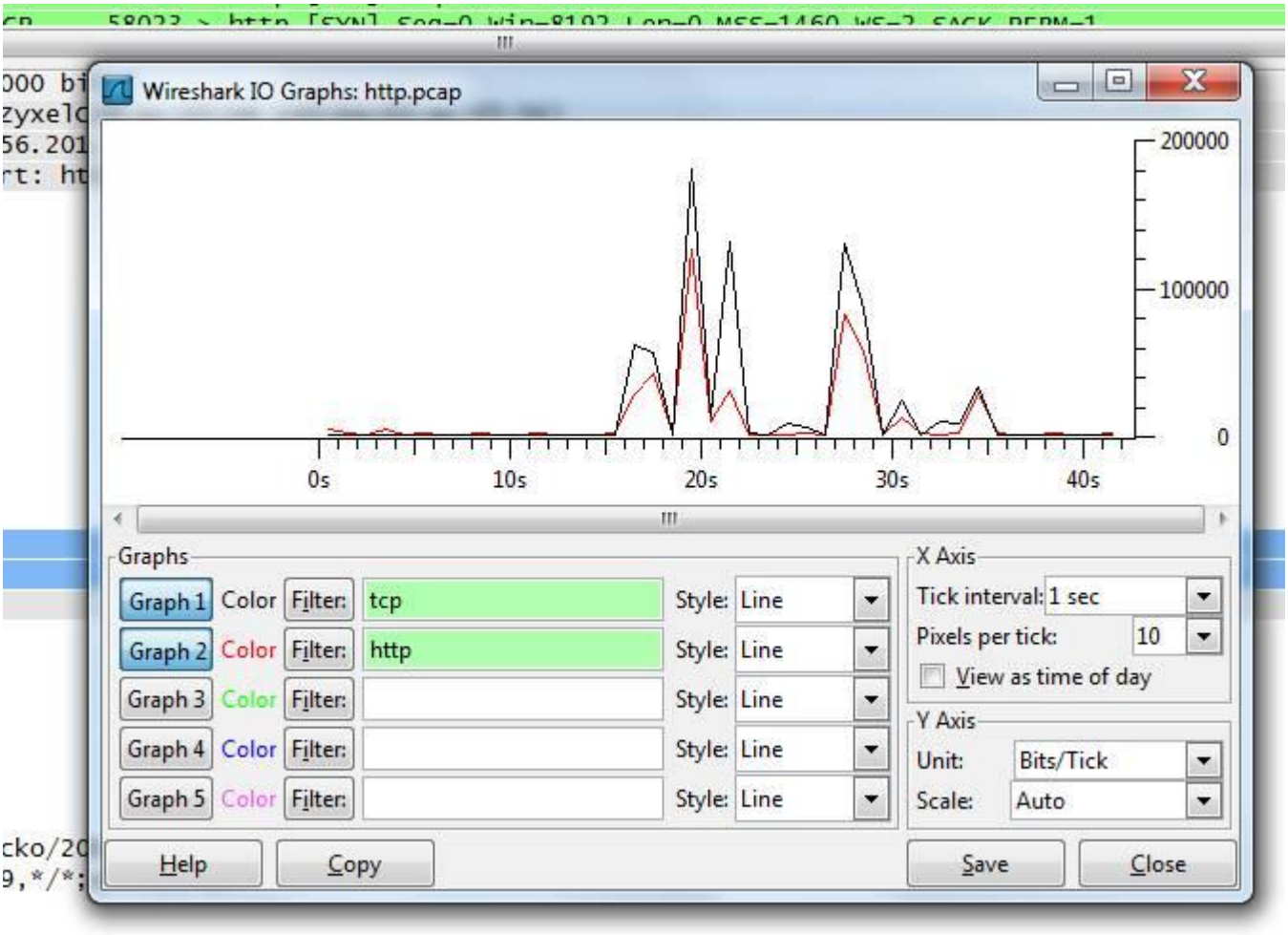


Рисунок 3 – скорость передачи пакетов TCP и HTTP

Для получения удобного отображения – настройте правильно параметры разрешения – Tick interval и Pixels per tick, а также единицы отображения пакетов (Unit) – Bits/Tick.

2.6.3 Через пункт меню – **Statistics – Flow-Graph** покажите процесс обмена пакетами TCP/HTTP для Вашего варианта перехвата:

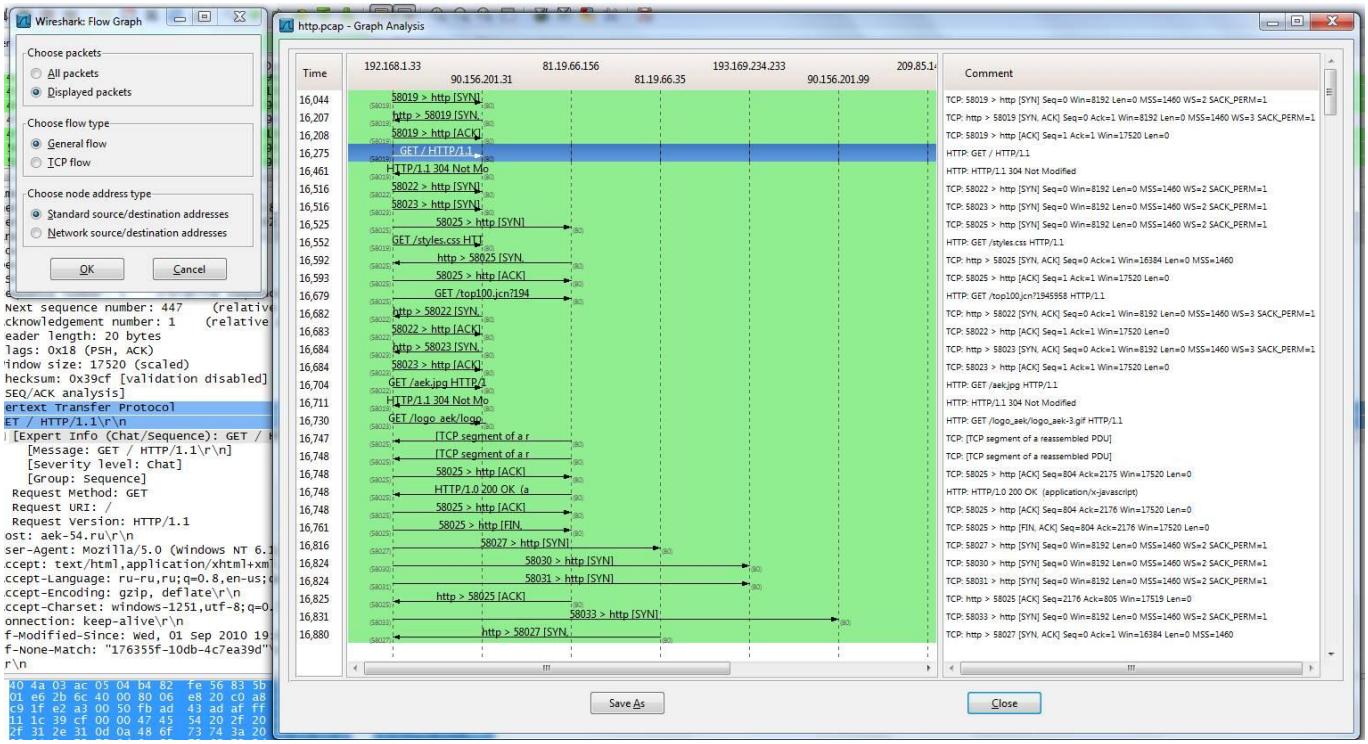
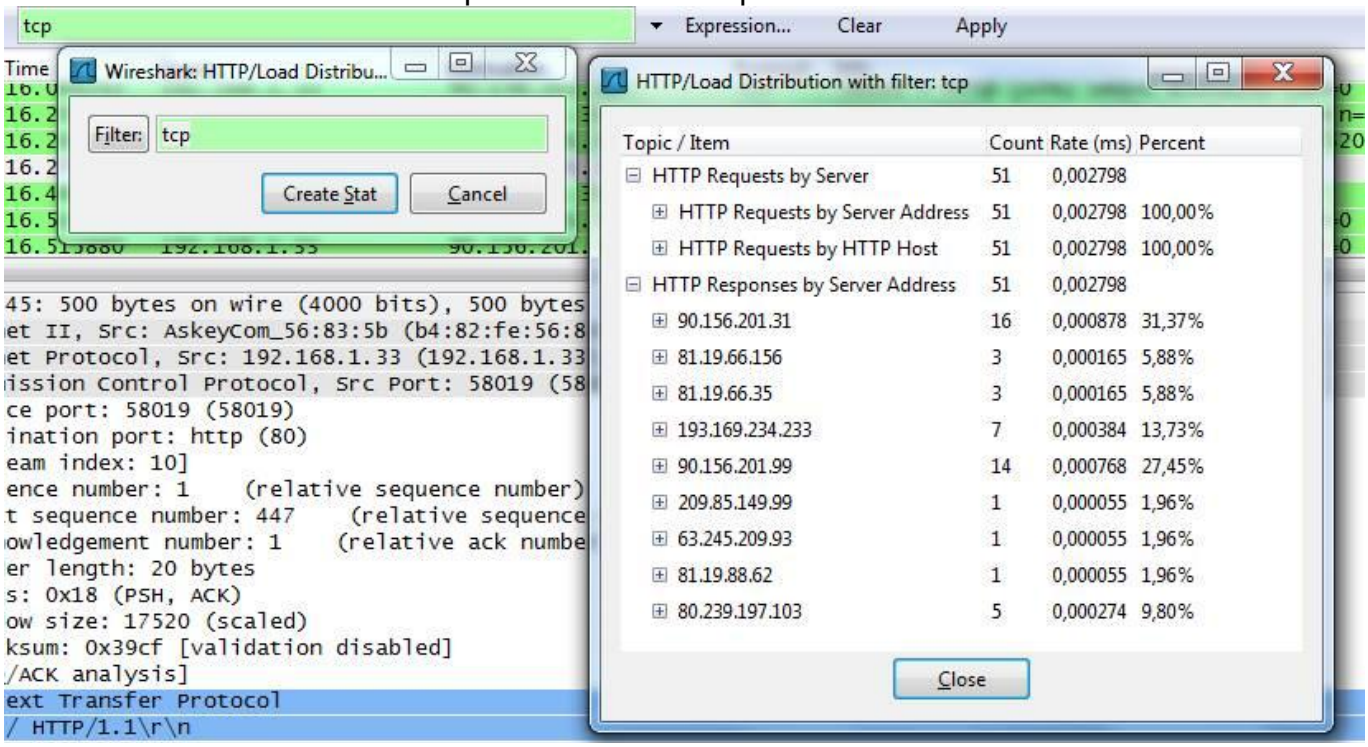
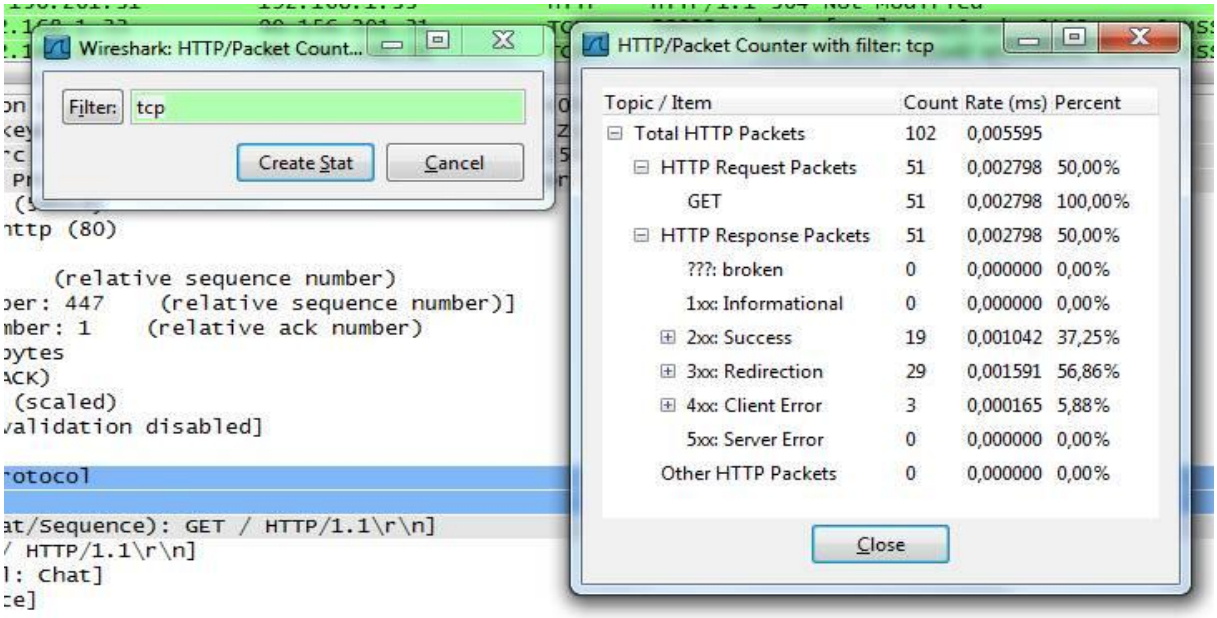


Рисунок 4 – Обмен пакетами TCP

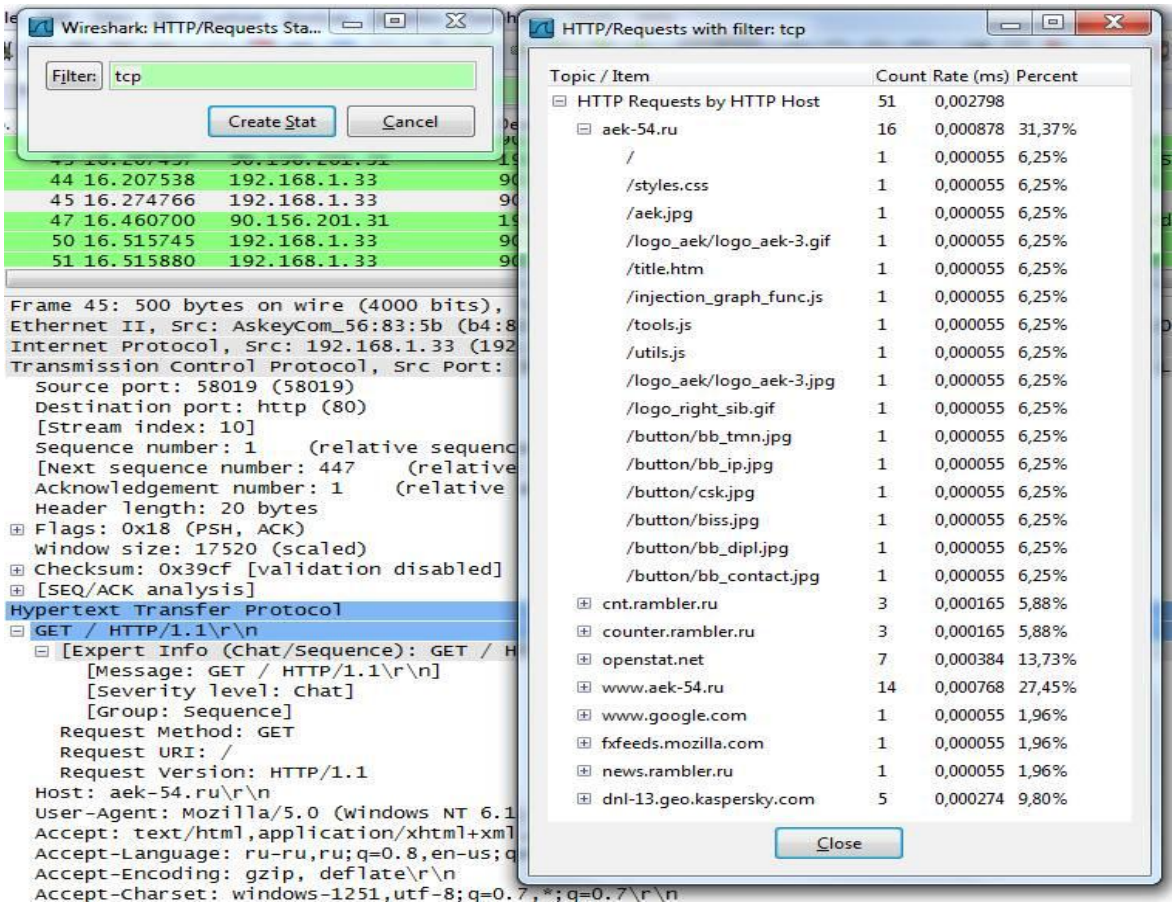
2.6.4 Статистика по запросам и ответам протокола HTTP:



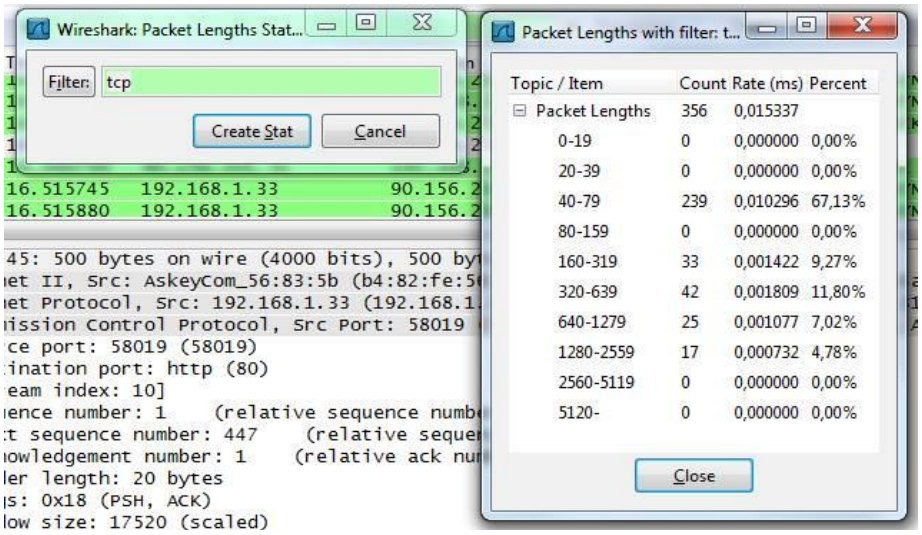
2.6.5 Статистика по типам запросов и ответов протокола HTTP:



2.6.6 Статистика по сайту aek-54.ru:



2.6.7 Статистика по распределению длины пакетов TCP/HTTP:



Для выполнения данной работы этого достаточно, но Вы не останавливайтесь на этом и глубже изучите все возможности перехвата и анализа пакетов от других протоколов службы Web.

3 Правила оформления отчета

Отчет по лабораторной работе должен содержать:

3.1 Титульный лист: ФИО, № группы, название лабораторной работы.
3.2 Цель работы.
3.3 Результаты перехвата и анализа пакетов TCP/HTTP – по всем пунктам раздела 2. Привести соответствующие экранные формы, **но с Вашими результатами**!
3.4 Комментарии и выводы по всем пунктам лабораторной работы.

Сохранить отчет в файле с именем ЛР-5.doc и выслать его в адрес дистанционного деканата.

В качестве подтверждения выполнения данной работы, необходимо вместе с файлом отчета выслать в одном архиве также файл с перехваченными пакетами (с расширением *.pcap).

4 Контрольные вопросы

4.1 Назначение полей протокола TCP
4.2 Назначение полей заголовка протокола HTTP
4.3 Сообщения протокола HTTP
4.3.1 Типы запросов протокола HTTP
4.3.2 Типы ответов протокола HTTP
4.4 Компоненты службы Web

5 Литература, рекомендуемая для выполнения лабораторной работы

5.1 Конспект лекций по дисциплине ИС СПС