

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ  
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Северо-Кавказский филиал  
ордена Трудового Красного Знамени федерального государственного  
бюджетного образовательного учреждения высшего образования  
«Московский технический университет связи и информатики»

Кафедра  
«Инфокоммуникационные технологии и системы связи»

Методические указания к лабораторной работе

## **Изучение способов анализа трафика в компьютерных сетях**

Дисциплина: Мультисервисные сети связи

Дисциплины: Сети связи,  
Мультисервисные сети связи

Направление подготовки 11.03.02  
«Инфокоммуникационные технологии и системы связи»,  
профиль Инфокоммуникационные системы и сети

Ростов-на-Дону  
2022

Составитель: доцент кафедры «ИТСС», к.т.н., доцент Решетникова И.В.

Данное методическое пособие предназначено для обеспечения проведения лабораторных работ со студентами направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи, профиль Инфокоммуникационные системы и сети, квалификации «бакалавр».

Пособие обеспечивает получение навыков по основополагающим вопросам изучаемой дисциплины.

Рецензент: Зав. кафедрой ИТСС, к.т.н., доцент Юхнов В.И.

Методическое пособие рассмотрено и утверждено на заседании кафедры ИТСС 19.12. 2022 г. Протокол №5

# Лабораторная работа

## Изучение способов анализа трафика в компьютерных сетях

### 1. Цель работы:

- ознакомить с принципами мониторинга сетей на примере возможностей сетевого анализатора CommView в ЛВС типа Ethernet;
- ознакомить студентов с механизмами ввода и контроля сетевых (IP), локальных (MAC) и символьных (DNS) адресов;
- освоить способы сбора статистики пакетов по различным параметрам (адреса, порты, протоколы и др.);
- освоить правила использования команд мониторинга связей в локальной и глобальной сетях (ping, tracert и др.);
- освоить механизмы создания тестовых потоков для определения пропускной способности ЛВС и ее элементов.

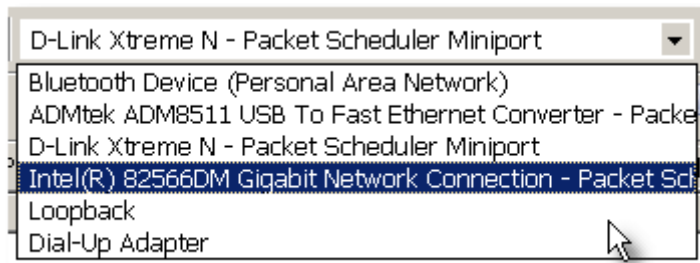
## 2 Руководство по работе с сетевым анализатором CommView

Анализатор пакетов - это программа (иногда - устройство), которая осуществляет мониторинг данных, проходящих между компьютерами в сети. Анализатор пакетов иногда еще называют *сетевым анализатором*, *декодером пакетов*, *сетевым монитором*, *декодером протоколов*, или, еще чаще, *снифером* (*сниффером*) *пакетов*. Слово "снифер" произошло от английского "sniffer", т.е. "нюхач".

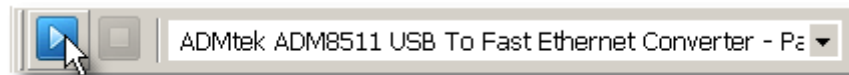
Сетевой анализатор переводит адаптер компьютера в так называемый режим "promiscuous", в котором он может перехватывать не только те пакеты, которые адресованы вашему компьютеру, но и другие пакеты, передаваемые или принимаемые в вашем сегменте сети.

### 2.1 Запуск перехвата пакетов в первый раз.

Итак, вы запустили CommView и видите перед собой главное окно. Все, что вам нужно для начала перехвата пакетов - это выбрать из выпадающего списка адаптер для мониторинга. У вас может быть один или несколько адаптеров. Если вы находитесь в корпоративной сети, у вас обычно будет лишь один адаптер, а если вы дома, то один из адаптеров может использоваться для подключения к кабельному модему, другой для подключения ко второму компьютеру, а адаптер Dial-up (это виртуальный адаптер) служит для подключения к Интернету посредством телефонной линии с использованием ADSL или аналогового модема.



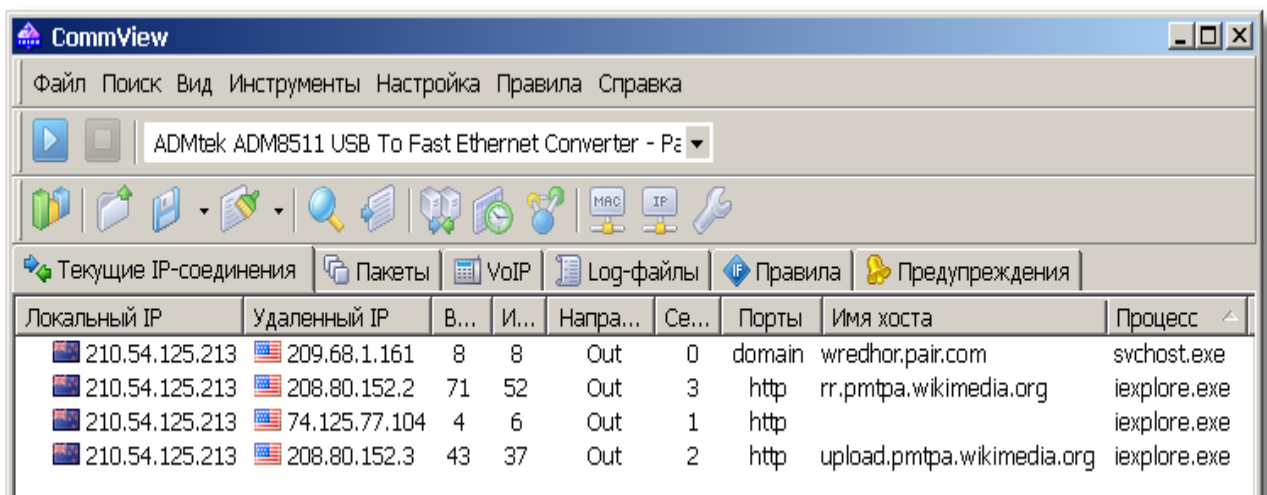
Сделали выбор? Хорошо, теперь нажмите **Начать захват**. Эту кнопку несложно найти на панели инструментов программы:



Ничего страшного, если вы случайно выбрали не тот адаптер. Вы быстро поймете, что сделали неверный выбор, потому что после нажатия кнопки **Начать захват** вы не увидите никаких пакетов.

## 2.2 Обзор последних IP-соединений

Давайте откроем браузер и посетим, например, веб-сайт [Wikipedia](http://Wikipedia). Затем вернемся к главному окну CommView и посмотрим, что записала программа:



Теперь вы можете нажать кнопку **Закончить захват** и осмыслить увиденное. Ваша картинка может немного отличаться от той, что показана, потому что ваш браузер может оказаться не единственной программой, принимающей и передающей пакеты, и еще по другим причинам, которые будут описаны ниже. Но суть в том, что вы наблюдаете сетевые подключения вашего компьютера!

Теперь давайте попробуем понять смысл того, что мы увидели. **Локальный IP** - это IP-адрес вашего компьютера, а **Удаленный IP** - это IP-адрес того компьютера, к которому вы подключаетесь. **Входящие** и **Исходящие** являются счетчиками пакетов, **Направление** показывает направление

соединения, в колонке **Порты** показаны номера или типы портов, участвующие в обмене данными, **Имя хоста** - это имя станции удаленного IP-адреса (если такое имя есть, что бывает не всегда), **Процесс**(детали) показывает имя исполняемого файла, ответственного за соединение (в некоторых случаях это имя недоступно).

Итак, что же происходит, когда мы посещаем веб-сайт, и почему мы видим все эти соединения? Когда вы ввели [www.wikipedia.org](http://www.wikipedia.org) в адресную строку браузера, ваш компьютер должен был преобразовать это имя хоста в IP-адрес. Несмотря на то, что имена хостов нужны людям (их легче запомнить), они совершенно бессмысленны с точки зрения компьютера, поскольку для создания подключения компьютеру требуется точный IP-адрес. Чтобы найти IP-адрес, соответствующий [www.wikipedia.org](http://www.wikipedia.org), ваш компьютер связался с сервером доменных имен (в нашем случае это [whedhor.pair.com](http://whedhor.pair.com), в вашем случае будет другой). Откуда мы это знаем? Поскольку в колонке **Порты** для данного соединения стоит строка *domain*, которая является именем порта для DNS-запросов.

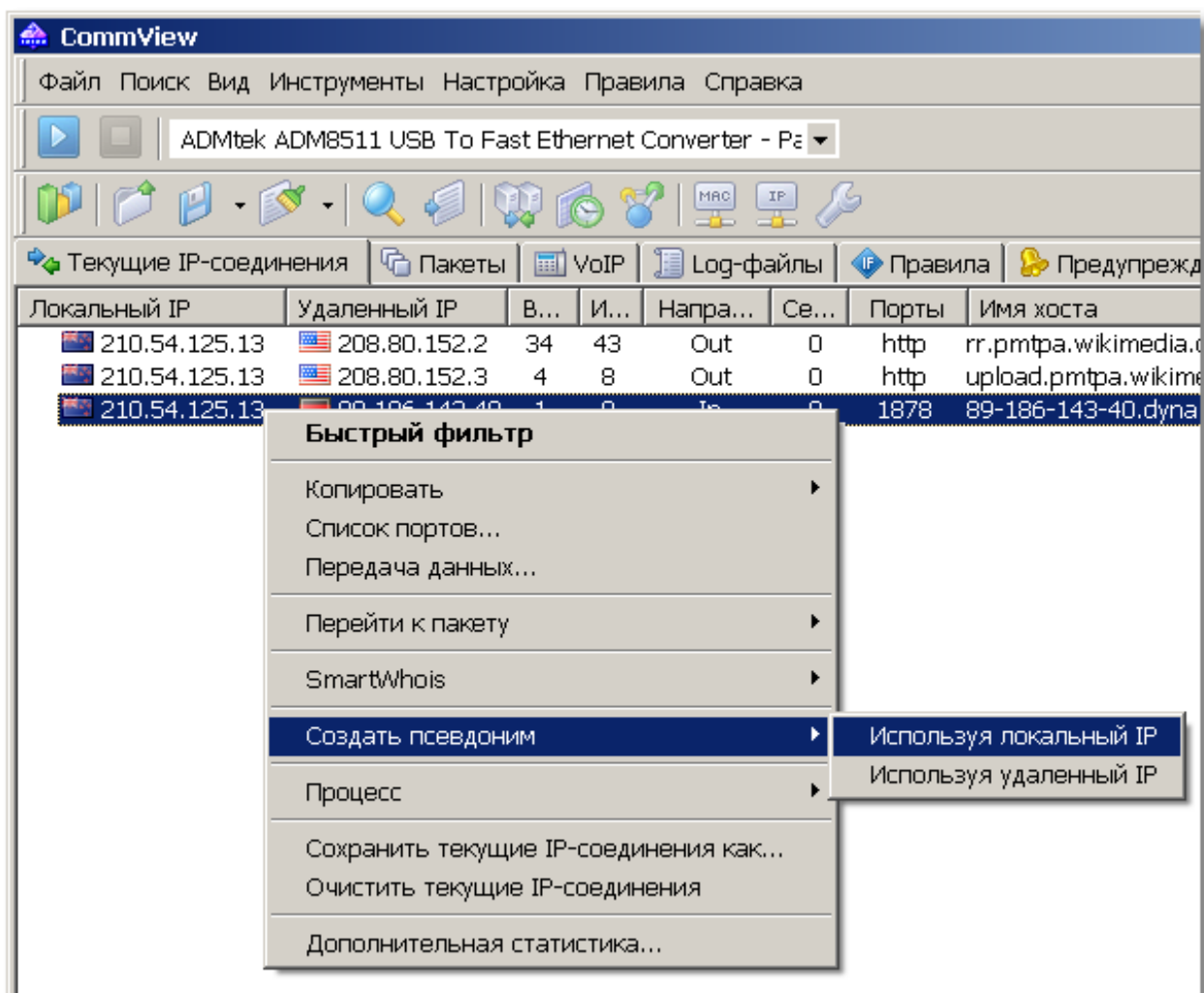
После того, как наш компьютер узнал от DNS-сервера IP-адрес сайта [www.wikipedia.org](http://www.wikipedia.org), он немедленно устанавливает соединение с этим веб-сервером и скачивает главную страницу, которую вы видите в своем браузере. Строка *http* в колонке **Порты** показывает, что это соединение происходит по гипертекстовому протоколу (HTTP).

После этого соединения могут идти другие, но мы поговорим об этом позже. Сейчас же мы выяснили, что в закладке **Текущие IP-соединения** показаны все текущие соединения.

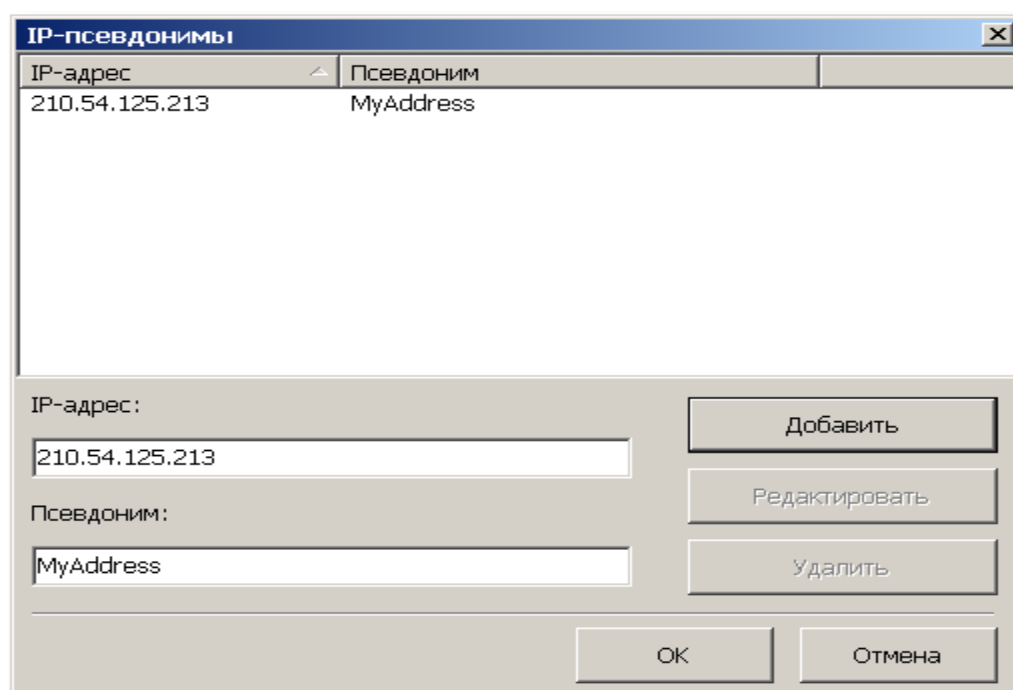
Заметим, что IP-адреса сопровождаются флагами стран. Эта функция называется "геолокация". С ее помощью вы можете определить географическое местоположение IP-адреса. В нашем случае, как показывают флаги, мы подключаемся к американскому серверу Wikipedia с новозеландского компьютера.

## 2.3 Использование псевдонимов

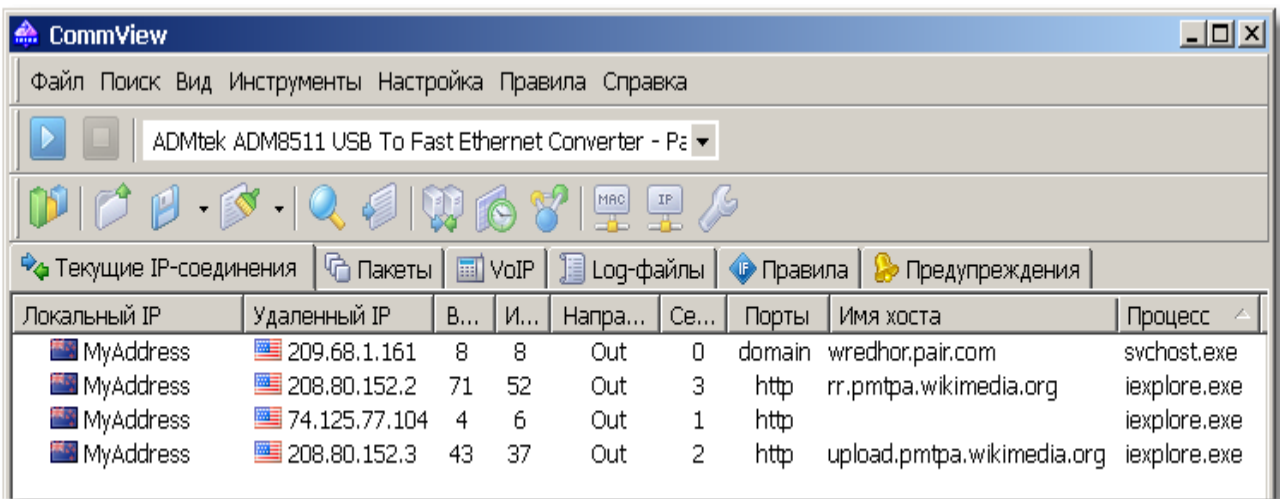
Посмотрим правде в глаза: числовые IP-адреса сложно запомнить. К счастью, вам не придется это делать. Кликните правой кнопкой мыши по любой строке в таблице Текущие IP-соединения и выберите Создать псевдоним, используя локальный или удалённый IP-адрес. Псевдоимя можно присвоить и для MAC-адреса, используя соответствующую кнопку главного меню.



Появится окно, в котором вы сможете назначить любому IP-адресу легко запоминаемое имя:



Введите любой псевдоним (мы выбрали *MyAddress*). Закройте это окно И...



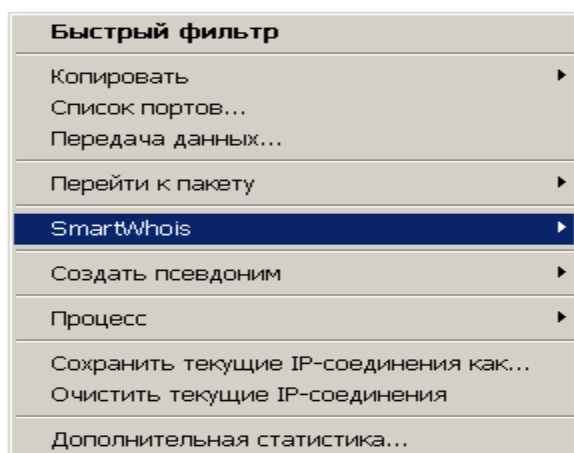
вы увидите, что данные теперь выглядят более понятно, особенно если вы наблюдаете сегмент локальной сети с десятками компьютеров. Мы видим, что первое соединение было DNS-запросом, а второе и четвертое - http-сессиями с Wikipedia. Это то, что мы ожидали увидеть? Не совсем... что это за подключение к 74.125.77.104? Почему мой компьютер его сделал? Давайте попробуем выяснить это.

## 2.4. Схема установления текущих соединений

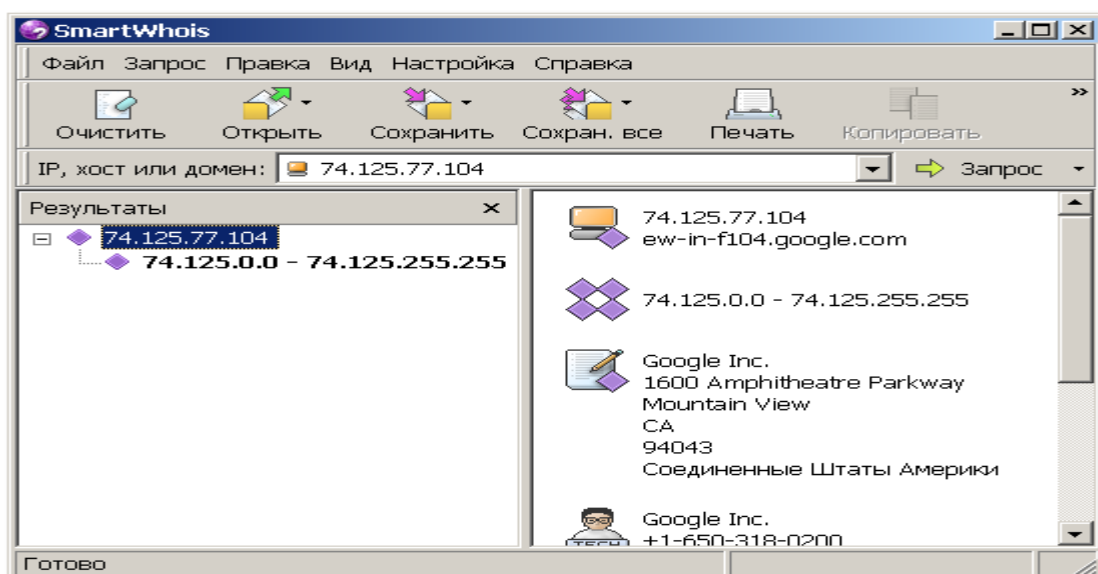
Реальность такова, что ваш компьютер создает больше соединений, чем вы ожидаете. Здравый смысл подсказывает вам, что загрузка веб-страницы влечет за собой только одну http-сессию, но это не всегда так. Во-первых, помните DNS-запросы? Вот вам, по крайней мере, еще одно соединение. Если ваш первый DNS-сервер отвечал слишком медленно или был недоступен, то последует другое соединение со вторым DNS-сервером. Во-вторых, многие веб-сайты часто хранят веб-страницы и графику на разных серверах, поэтому, если вы загружаете страницу с картинками, то происходит подключение к нескольким серверам. Существуют тысячи причин, по которым ваш компьютер может подключаться к другим. Большинство из этих причин вполне безобидны, но нередко можно увидеть программу, которая пересылает личные данные без вашего ведома. Это может быть spyware- или adware-программа, или даже коммерческая программа, у которой есть какие-то недокументированные функции. Это может быть даже программа-троян, с помощью которой кто-то сможет управлять вашим компьютером.

Прежде чем пугаться, давайте вспомним, что у нас на руках отличный инструмент. Ни один сетевой пакет не попадет в ваш компьютер и не покинет его не замеченным программой CommView. В нашем случае мы хотим выяснить, что скрывается за IP-адресом 74.125.77.104 и почему наш компьютер к нему подключился. Конечно, в закладке **Пакеты** мы можем посмот-

реть, что на самом деле передавалось, но мы сделаем это позже. Сейчас же кликнем правой кнопкой мыши по IP-адресу и выберем **SmartWhois**:



SmartWhois от TamoSoft - это полезная информационная сетевая утилита, которая позволяет вам получить всю доступную информацию об IP-адресе, имени хоста или домене, включая страну, штат/провинцию, город, название провайдера и контактную информацию технического персонала или администратора. Если вы еще не попробовали работать с этой утилитой, то запустите её на рабочем столе или скачайте ознакомительную версию. В SmartWhois много полезных функций, но в этой ситуации нам нужна лишь одна из них: установить, кто владеет этим IP-адресом. После выбора опции **SmartWhois** вы увидите окно программы со следующей информацией об интересующем нас IP-адресе:



Google? Но почему Google? Мы же посетили сайт Wikipedia. Все правильно. Давайте немного подумаем. Ваш браузер Internet Explorer может содержать небольшую встроенную утилиту, которая называется Google



Toolbar. А она, в свою очередь, подключается к серверу Google, чтобы выяснить рейтинг популярности данной страницы. Вот мы и нашли ответ.

Естественно, ваша картина соединений может быть другой. Может быть, вы используете другой браузер или посетили другой веб-сайт для нашего эксперимента, у вас может быть с десяток других сетевых программ, работающих в фоновом режиме, так что ваша закладка **Текущие IP-соединения** может выглядеть и по-другому. Но мы надеемся, что основной принцип стал понятен: с помощью CommView вы всегда можете увидеть всю картину ваших сетевых подключений в целом, и эта информация очень полезна.

## 2.5. Информация о пакетах

Теперь, после того, как мы изучили первую закладку главного окна CommView, давайте перейдем ко второй - **Пакеты**. В этой трех секционной закладке вы увидите каждый пакет, проходящий через ваш сетевой адаптер в любом направлении. В списке пакетов показаны общие сведения о пакетах. При выборе пакета в окне данных будет показано содержимое пакета, а дерево декодирования говорит само за себя - оно декодирует заголовки пакета и отображает каждую деталь.

Для придания компактности приведенной ниже иллюстрации мы не стали включать в нее дерево декодирования, но в своей копии CommView вы всегда видите декодер. Данные, пересылаемые по сети, разбиты на множество пакетов, пересылаемых по сети отдельно. Принимающая сторона собирает все эти пакеты воедино. В нашем примере при загрузке главной страницы Wikipedia был передан один пакет с нашего компьютера на веб-сервер (запрос нашего браузера на данную страницу) и принято несколько пакетов, содержащих запрошенную страницу. Поскольку запрошенная страница имеет размер примерно в 10000 байт, а средний размер пакета составляет 1500 байт, то принимаемая информация была разбита на 7 пакетов.

Теперь давайте выберем один из http-пакетов:

№	Проток...	IP источн.	IP назн.	Порт ис...	Порт на...	Время
58	IP/TCP	rr.pmtpa.wikimedia.org	MyAddress	http	2371	15:08:35.917118
59	IP/TCP	rr.pmtpa.wikimedia.org	MyAddress	http	2371	15:08:35.919068
60	IP/TCP	MyAddress	rr.pmtpa.wikimedia.org	2371	http	15:08:35.919105
61	IP/TCP	rr.pmtpa.wikimedia.org	MyAddress	http	2371	15:08:35.921022
62	IP/TCP	MyAddress	rr.pmtpa.wikimedia.org	2371	http	15:08:35.921086
63	IP/TCP	rr.pmtpa.wikimedia.org	MyAddress	http	2371	15:08:35.922975
64	IP/TCP	rr.pmtpa.wikimedia.org	MyAddress	http	2371	15:08:35.924934
65	IP/TCP	MyAddress	rr.pmtpa.wikimedia.org	2371	http	15:08:35.924987
0x0030	00 0C 2E 6B 00 00 2F 61-3E 0A 20 20 20 3C 61 20	...k../a>. <a				
0x0040	68 72 65 66 3D 22 23 45-6E 67 6C 69 73 68 22 20	href="#English"				
0x0050	63 6C 61 73 73 3D 22 42-6F 74 74 6F 6D 4C 69 6E	class="BottomLin				
0x0060	6B 73 22 20 69 64 3D 22-65 6E 5F 6C 69 6E 6B 22	ks" id="en_link"				
0x0070	20 6F 6E 63 6C 69 63 6B-3D 22 53 68 6F 77 4C 61	onclick="ShowLa				
0x0080	6E 67 75 61 67 65 28 27-65 6E 27 29 22 3E 45 6E	anguage('en') ">En				
0x0090	67 6C 69 73 68 3C 2F 61-3E 0A 20 20 20 3C 61 20	glish</a>. <a				
0x00A0	68 72 65 66 3D 22 23 53-70 61 6E 69 73 68 22 20	href="#Spanish"				
0x00B0	63 6C 61 73 73 3D 22 42-6F 74 74 6F 6D 4C 69 6E	class="BottomLin				

В зависимости от выбранного вами пакета вы увидите либо запрос на получение веб-страницы, либо ответ сервера, который содержит в себе со-

держимое страницы. Последнее показано на рисунке выше. Если вы знаете, что такое HTML, то вы легко узнаете HTML-код обычной веб-страницы!

Окно данных, которое вы видите - это стандартное шестнадцатеричное представление пакета. В первой колонке указано смещение каждой строки, во второй показано содержимое пакета в шестнадцатеричной форме, а в третьей - текстовый (ASCII) эквивалент. Зачем нам нужны и шестнадцатеричные, и ASCII-данные? Потому, что иногда одну форму легче прочесть, чем другую. Поздравляем, вы только что заглянули внутрь вашего первого сетевого пакета.

В дальнейшем мы обсудим, что делать с этой информацией, а сейчас попробуем кое-что интересное. Представьте... воскресный вечер, и вы только что скачали и поставили новую программу для e-mail. К вашему удивлению, она гораздо лучше той, которую вы сейчас используете! И вы решаете поработать с ней немедленно. Вы импортируете вашу базу данных и установки из старой программы, но... вы не можете импортировать ваш пароль к почте. И, что естественно, вы его не помните (а кто будет помнить строчку вроде *JKH667RtfS*, которую вы выбрали год назад и с тех пор ни разу не вводили, верно?). И служба технической поддержки вашего провайдера не работает по воскресеньям вечером.

Вот решение проблемы. Проверьте почту вашей старой программой и перехватите эту сессию с помощью CommView. После этого просмотрите пакеты POP3:

№	Протокол...	IP источн.	IP назн.	Порт ис...	Порт на...	Время
5	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.023926
6	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.024219
7	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.161584
8	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.161900
9	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.300261
10	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.300625
11	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.440890
12	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.441397

0x0000	4A E8 20 00 01 00 01 00-01 00 00 00 08 00 45 00	Жи .....	E.
0x0010	00 43 B3 9D 40 00 80 06-7E 65 D9 AC 11 D4 D1 44	.	Cik@.Ъ.~eЩ.фCD
0x0020	0B ED 09 63 00 6E 0E 0E-42 0E 17 E3 C8 72 80 18	.	н.с.н..В..rMrЪ.
0x0030	80 AA F8 E2 00 00 01 01-08 0A 00 01 CF 06 0A 5A	ЪEшв.....П..2	
0x0040	A7 48 55 53 45 52 20 67-65 6F 72 67 65 5F 61 0D	\$HUSER	george_a.
0x0050	0A	.	

Вот имя пользователя ...

№	Проток...	IP источн.	IP назн.	Порт ис...	Порт на...	Время
5	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.023926
6	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.024219
7	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.161584
8	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.161900
9	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.300261
10	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.300625
11	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.440890
12	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.441397

0x0000	01 00 01 00 00 00 4A E8-20 00 01 00 08 00 45 00	.....Жи.....Е.
0x0010	00 39 B4 A0 40 00 32 06-CB 6C D1 44 0B ED D9 AC	.9r @.2.LlCD.нЩ
0x0020	11 D4 00 6E 09 63 17 E3-C8 72 0E 0E 42 1D 80 18	.ф.n.c.rMr..B.Ъ.
0x0030	80 4C F1 CE 00 00 01 01-08 0A 0A 5A A7 D2 00 01	ЪLcO.....Z\$T..
0x0040	CF 06 2B 4F 4B 0D 0A	П.+OK..

... вот почтовый сервер запрашивает пароль ...

№	Проток...	IP источн.	IP назн.	Порт ис...	Порт на...	Время
5	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.023926
6	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.024219
7	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.161584
8	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.161900
9	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.300261
10	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.300625
11	IP/TCP	tamos.com	MyAddress	pop3	2403	15:20:41.440890
12	IP/TCP	MyAddress	tamos.com	2403	pop3	15:20:41.441397

0x0000	4A E8 20 00 01 00 01 00-01 00 00 00 08 00 45 00	Жи.....Е.
0x0010	00 45 B3 9E 40 00 80 06-7E 62 D9 AC 11 D4 D1 44	.Eih@.Ъ.~bЩ-.фCD
0x0020	0B ED 09 63 00 00 6E 0E 0E-42 1D 17 E3 C8 77 80 18	.н.c.n..B..rИwЪ.
0x0030	80 AA 23 98 00 00 01 01-08 0A 00 01 CF 07 0A 5A	ЪE#l.....П..Z
0x0040	A7 D2 50 41 53 53 20 4A-4B 48 36 36 37 52 74 66	\$TPASS JKH667Rtf
0x0050	53 0D 0A	S..

... а вот и сам пароль, который мы искали!

Кстати, если вы захотите просмотреть пакеты, имеющие отношение к конкретному соединению из закладки **Текущие IP-соединения**, просто кликните дважды по строке соединения.

## 2.6. Поток данных в сессии TCP

Мы видим данные, разбитые на множество пакетов. Но можно ли заново собрать TCP-сессии? Да, с помощью CommView это возможно. Выберите первый пакет в сессии (например, тот, где браузер запрашивает страницу с веб-сервера), кликните по нему правой кнопкой мыши и выберите Реконструкция TCP-сессии. Можете просто дважды кликнуть по выбранной строке:

№	Протокол	IP источн.	IP назн.	Порт ис...	Порт на...	Время
1	IP/TCP	MyAddress	rr.pmtpa.wikimedia.org	2410	http	15:25:28.265087
2	IP/TCP	rr.pmtpa.wikimed		2410		15:25:28.450324
3	IP/TCP	rr.pmtpa.wikimed		2410		15:25:28.450376
4	IP/TCP	MyAddress		10	http	15:25:28.450407
5	IP/TCP	rr.pmtpa.wikimed		2410		15:25:28.454398
6	IP/TCP	MyAddress		10	http	15:25:28.454472
7	IP/TCP	MyAddress		15	http	15:25:28.566995
8	IP/TCP	ew-in-f147.google		2415		15:25:28.622275

0x0000	4A E8 20 00 01 00 00	Копировать пакет	Жи .....
0x0010	02 24 B4 7B 40 00 80	Отправить пакет(ы)	.\$r{0.Б.р.Щ.ФPP
0x0020	98 02 09 6A 00 50 80	Сохранить пакет(ы) как...	0..j.РЪh."П ;«P.
0x0030	80 64 C2 56 00 00 40	SmartWhois	ТdBV..GET /wiki/
0x0040	57 69 6B 69 70 65 6A	Очистить буфер пакетов	Wikipedia:About
0x0050	48 54 54 50 2F 31 21	Декодировать как	HTTP/1.1..Accept
0x0060	3A 20 69 6D 61 67 6A	Шрифт	: image/gif, ima
0x0070	67 65 2F 78 2D 78 6A		ge/x-xbitmap, im
0x0080	61 67 65 2F 6A 70 6A		age/jpeg, image/
0x0090	70 6A 70 65 67 2C 20		pjpeg, applicati
0x00A0	6F 6E 2F 78 2D 73 6A		on/x-shockwave-f
0x00B0	66 61 73 69 2D 2D 6A		lash, applicatio

Пожалуйста, перед нами процесс обмена данными между нашим компьютером и веб-сервером Wikipedia. Текст запроса выведен синим, а ответ сервера - красным:

TCP-сессия

Файл Редактировать Установки

Содержимое

Анализ TCP-сессии

```

GET /wiki/Wikipedia:About HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, application/x-silverlight, */*
Referer: http://en.wikipedia.org/wiki/Main_Page
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727;
.NET CLR 1.1.4322)
Host: en.wikipedia.org
Connection: Keep-Alive

HTTP/1.0 200 OK
Date: Wed, 05 Mar 2008 14:13:35 GMT
Server: Apache
X-Powered-By: PHP/5.2.1
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Language: en
Vary: Accept-Encoding, Cookie
X-Vary-Options:
Accept-Encoding;list-contains=gzip, Cookie;string-contains=enwikiToken;string-contains=enwikiLoggedOut;string-contains=enwiki_session

```

☒ MyAddress:2410 => rr.pmtpa.wikimedia.org:80 \* 508 байт в 1 пакете(ах)
☒ rr.pmtpa.wikimedia.org:80 => MyAddress:2410 \* 33,988 байт в 24 пакете(ах)

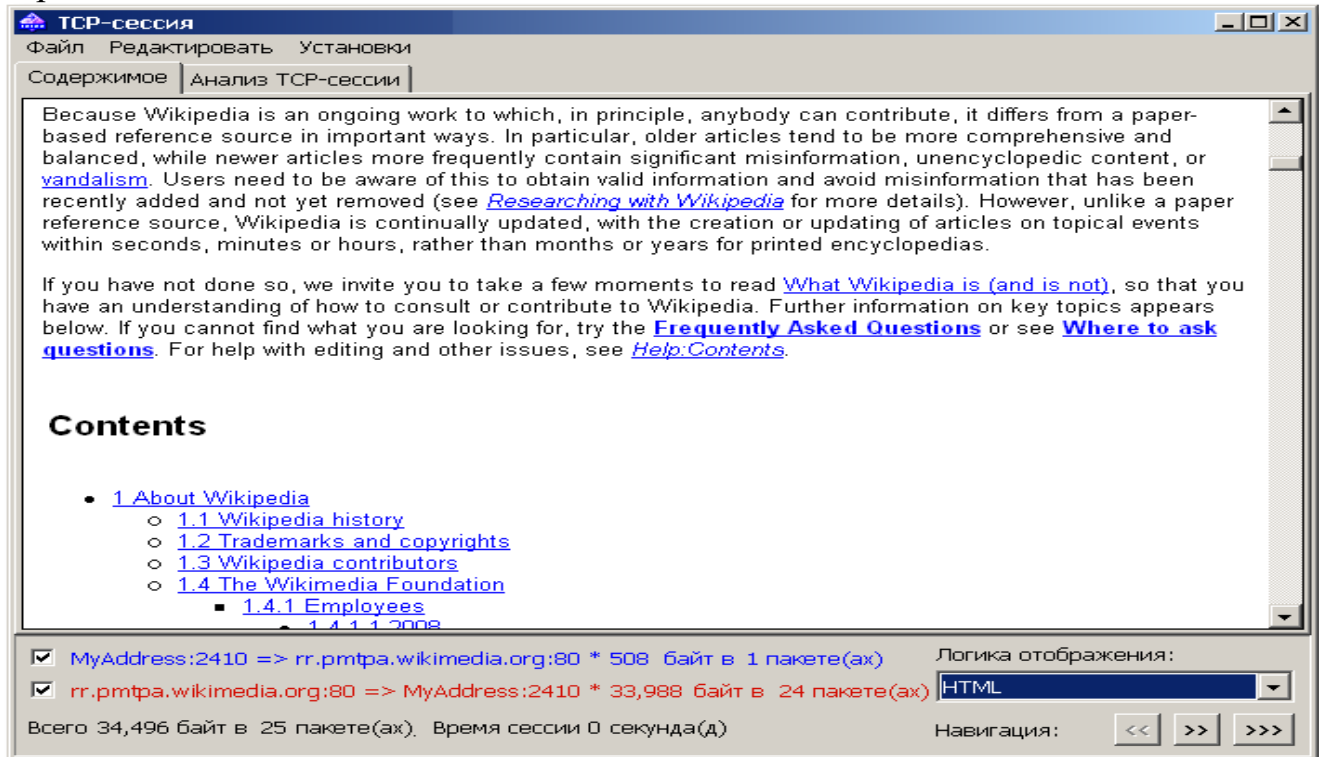
Логика отображения:

ASCII

Всего 34,496 байт в 25 пакете(ах). Время сессии 0 секунда(д)

Навигация: << >> >>>

Если вы прокрутите это окно пониже, то увидите полный HTML-код страницы, которая была загружена в браузер. Это и есть текстовое (ASCII) отображение этой сессии. Но браузер не показывает неформатированный текст: в нем мы видим красивые HTML-страницы, так ведь? То же самое мы можем сделать и с помощью CommView. Для этого в выпадающем списке **Логика отображения** выберите HTML и вы увидите данные в виде веб-страницы:

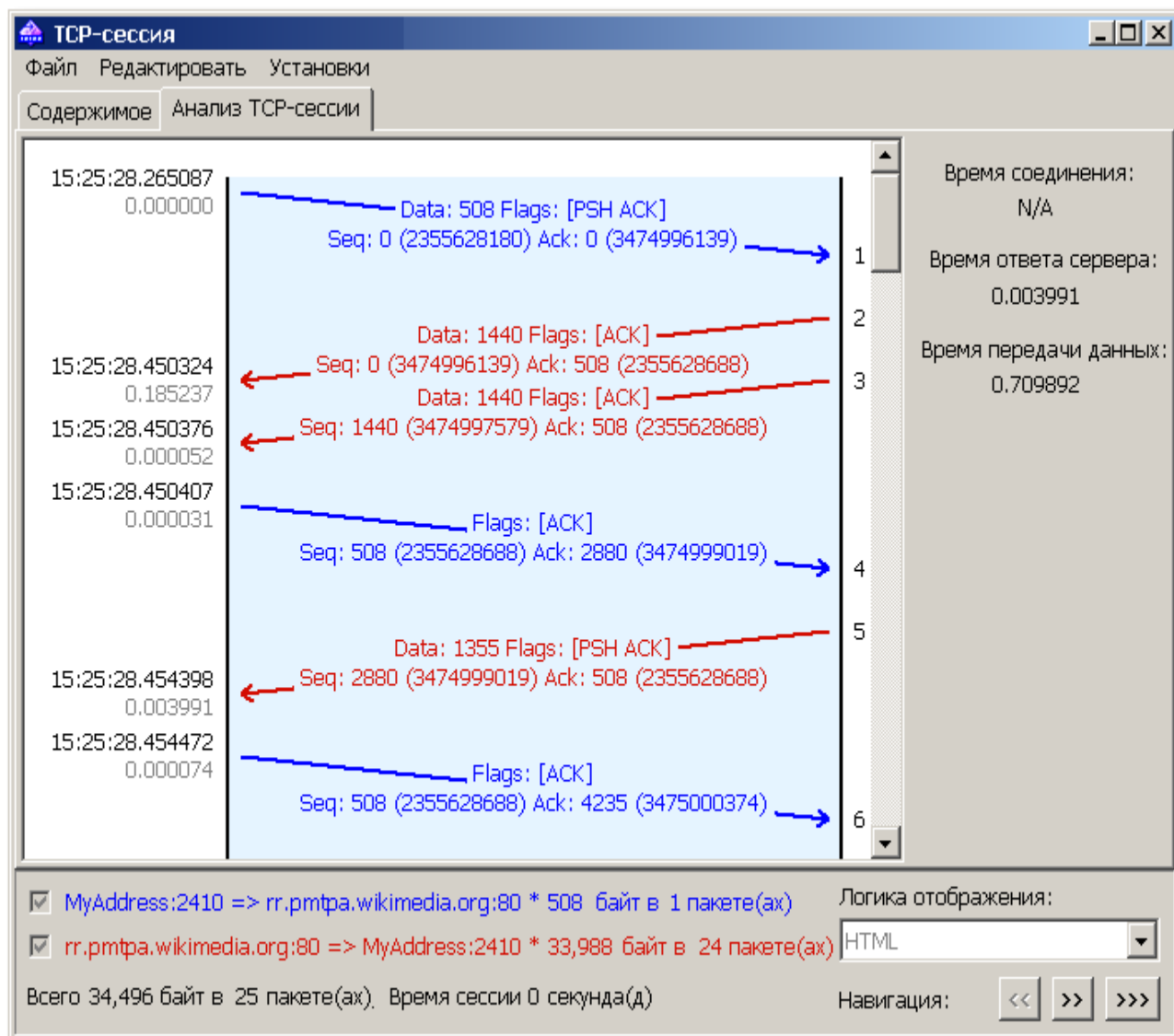


Все хорошо, но почему нет картинок? А потому, что графика обычно передается в другой TCP-сессии, и иногда с другого сервера. Нажав на кнопку >>>, вы перейдете к следующей TCP-сессии и найдете картинки (или совершенно другую TCP-сессию, ведь ваш компьютер к тому времени мог сделать несколько подключений):




В этом примере мы использовали CommView для реконструкции http-сессий, но вы также можете наблюдать TCP-потoki любого вида, будь то сессия POP3 между вашим почтовым клиентом и сервером, или загрузка файла по FTP.

Если в области сетей вы профессионал и хотите посмотреть потоки TCP-сессии в виде лестничной диаграммы, переключитесь в закладку **Анализ TCP-сессии**:





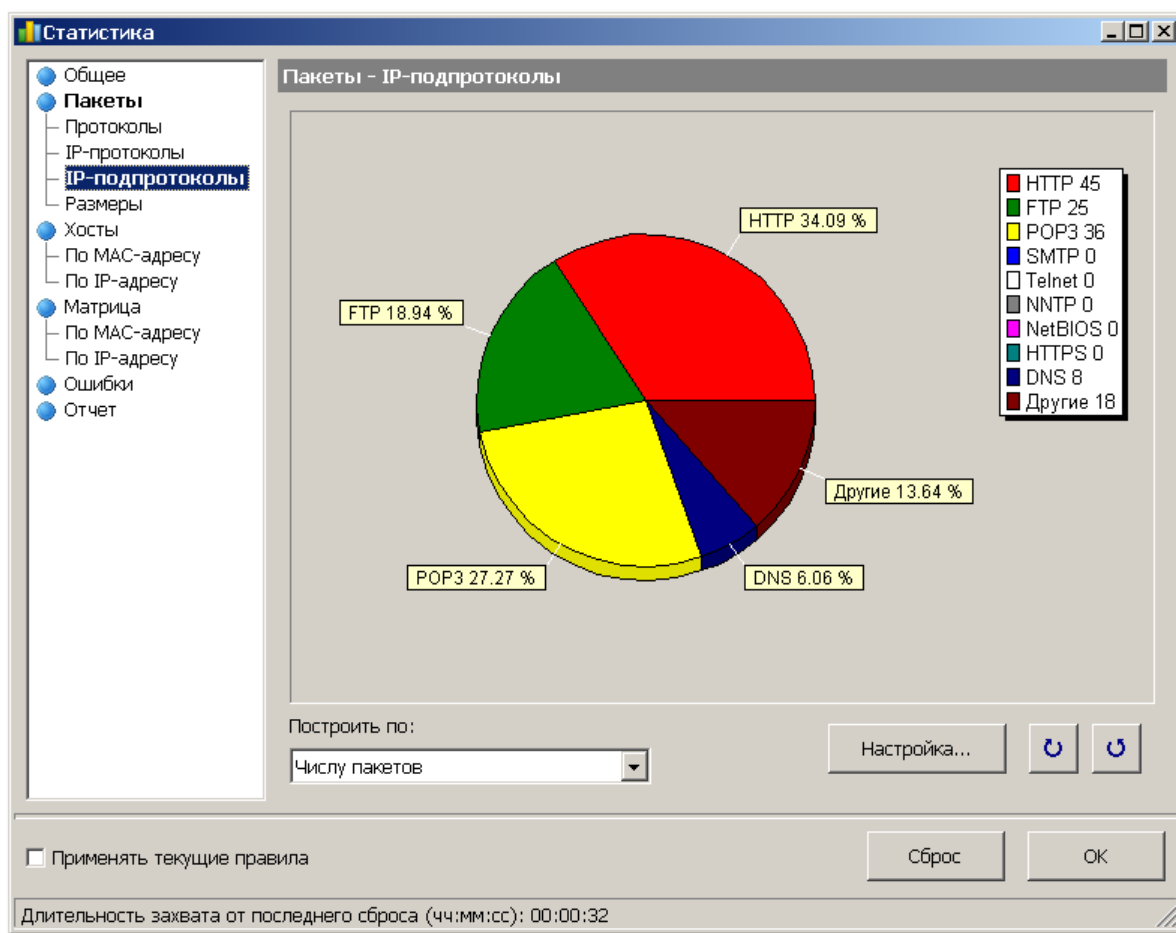
## 2.7. Обзор статистики

Пришло время взглянуть на окно **Статистика**, где представлено большое количество статистической информации о состоянии сети. Это окно можно вызывать, нажав на кнопку панели инструментов: . После этого выберите закладку **Общее** и посмотрите, что происходит с вашим сетевым подключением.

На этих графиках показана информация о передаваемых в вашей сети пакетах и байтах в реальном времени. Почему это так важно многим пользователям? Если вы находитесь в локальной сети, то это важные показатели качества работы вашего сегмента. Если загрузка вашего сегмента сети слишком велика, то есть повод разобраться в ситуации, найти источники перегрузок или обновить аппаратное обеспечение. Если у вас дома широкополосное соединение, то вы можете увидеть реальную скорость передачи данных и сравнить эту скорость с той, которую заявляет ваш провайдер. Вы также можете измерить скорость скачивания файла или наблюдать общий объем трафика. Если вам нужна программа, специально созданная для учета трафика, обратите внимание на [CommTraffic](#) от [TamoSoft](#).

## 2.8. Диаграммы протоколов

Вам интересно, какие программы загружают ваш сетевой канал? Перейдите к закладке IP-подпротоколы и посмотрите:



На этой секторной диаграмме вы сразу увидите, какие протоколы используются в вашей сети. Слишком большой SMTP-трафик? Ваш ПК или другие станции в вашем сегменте сети передают слишком много почты. Слишком большой FTP-трафик? Пожалуй, скачивается много программ. Хотя по умолчанию в диаграмме показаны наиболее популярные протоколы, вы всегда можете кликнуть по кнопке **Настройка** и ввести новый протокол и номер порта, например, для получения информации о популярном р2р-клиенте или chat-программе.

## 2.9. Работа с универсальными правилами

Изучение сетевого трафика может быть затруднено, если действительно нужная информация буквально похоронена под валом незначимых соединений и пакетов. Если вы интересуетесь, скажем, вопросами отладки сессии электронной почты, вероятно, вам совсем не нужно перехватывать и отображать несколько сотен пакетов, которые имеют отношение к постороннему процессу FTP-загрузки, который происходит параллельно. Возможно, даже не на вашем компьютере. Хорошие новости: в нормальном сетевом анализаторе всегда есть возможность применения правил перехвата (их часто называют фильтрами). Применяя правила, вы можете отфильтровывать незначимые для вас пакеты и сосредоточить свое внимание на важных пакетах. В закладке Правила вы можете управлять правилами перехвата, а в закладке Универсальные правила вы можете создавать чрезвычайно гибкие правила на базе формул:

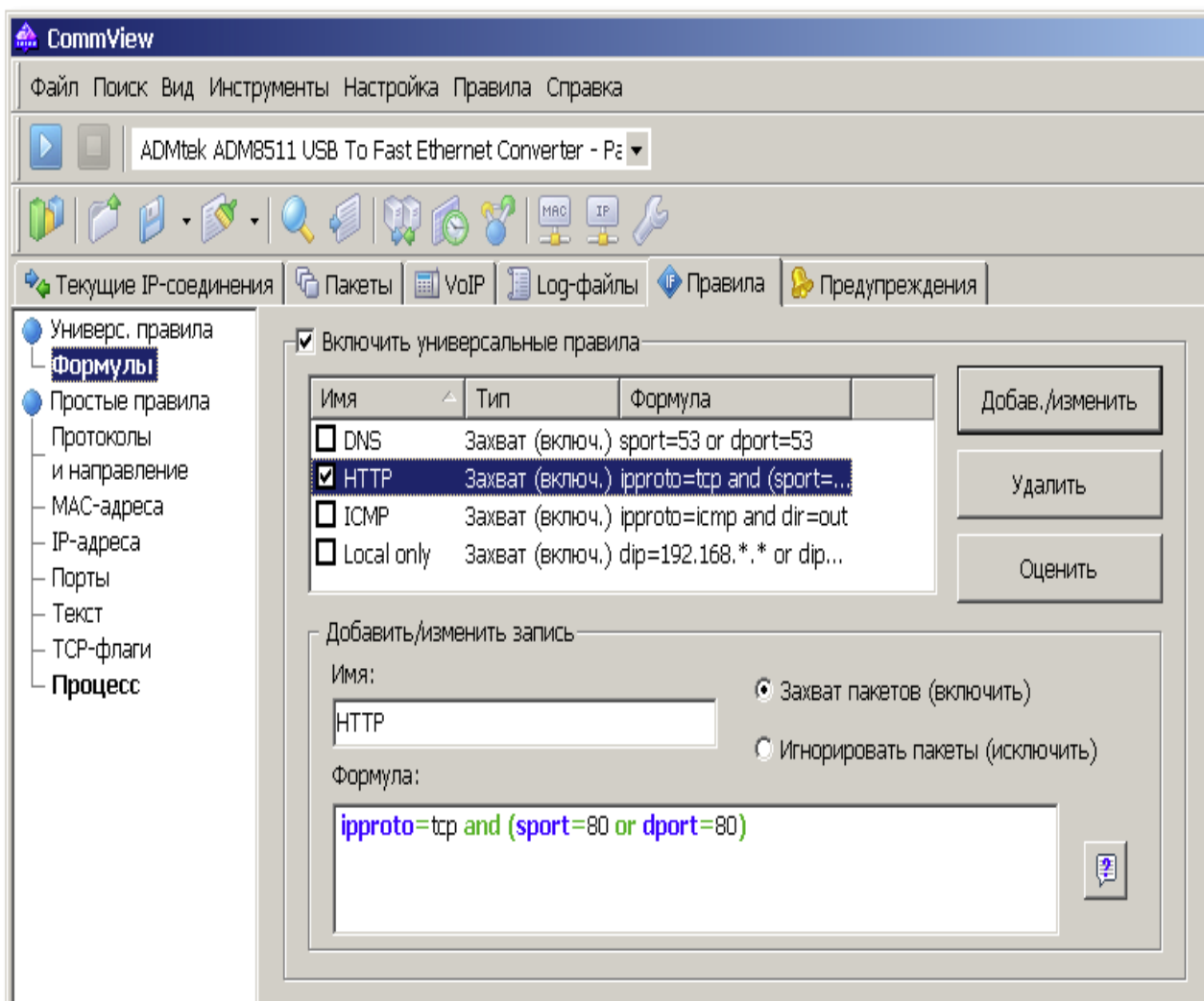
Вы также можете использовать и другие виды правил (Порты, Текст и т. п.), но универсальные правила дают гораздо больше гибкости, и мы покажем это на примере. Для создания нового правила введите произвольное имя в поле **Имя** и выберите одну из двух опций: **Захват пакетов** или **Игнорировать пакеты**. Первая опция даст вам возможность показывать только те пакеты, которые соответствуют вашей формуле, тогда как вторая опция позволит показать все пакеты, кроме тех, которые подпадают под ваш фильтр. И наконец, вам надо ввести формулу, описывающую ваш пакет. Предположим, мы хотим перехватывать только http-трафик.

В нашем примере с целью экономии времени мы используем интуитивно понятную формулу:

```
ipproto=tcp and(sport=80or dport=80)
```

В переводе на человеческий язык, это означает, что нас интересуют TCP-пакеты, входящие или исходящие из порта 80, т. е. порт, используемый для http-соединений. Теперь нажмите **Добав./Изменить**, и все готово! CommView будет отображать только http-пакеты, пока вы не отключите это правило. Как видите, все просто.





## Лабораторное задание

3.1. Рассмотреть (наружным осмотром) схему физических связей локального сегмента в учебном классе. Определить тип кабельной системы.

3.2. Загрузить анализатор CommView. Установить режим «Текущие IP-соединения» (см. пп. 2.1 и 2.2). В меню ФАЙЛ активизировать функцию «Начать захват» (Эквивалент – щелчок на треугольничке). После набора 10-15 сообщений о прошедших пакетах выбрать «Остановить захват». Зафиксировать в отчёте несколько сообщений о входящих и исходящих соединениях. Объяснить (устно) все параметры соединения. Зафиксировать IP-адрес своего персонального компьютера (PC).

Предупреждение. При выполнении этого пункта в меню закладки «Правила» галочки в квадратиках должны быть исключены.

3.3. Перейти в режим «Пакеты» (См. п. 2.3). Проанализировать содержимое нескольких строк в верхнем окне. Зафиксировать MAC и IP-адреса, а также номера портов для нескольких входящих и исходящих пакетов. Щелчком на одной из строк, соответствующей пакету в верхнем окне, получите

полный текст кадра с пакетом в нижнем окне (Учтите, что в версии CommView с ограниченной функциональностью эта операция выполняется не для всех пакетов). Обратите внимание на то, что в нижнем окне заголовок кадра окрашен красным цветом, заголовок пакета – синим, а номера портов – сиреневым. Кроме того, эти же адреса в явном виде присутствуют в левом окне. Снимите скриншот пакета для отчёта и отметьте на нём все адреса и номера портов. Зафиксируйте в отчёте длины адресов и номеров портов.

3.4. Перейти в режим «Просмотр статистики» (Левая закладка главного меню). Изучить и зафиксировать в отчёте основные результаты.

3.5. В закладке «Правила» поставьте фильтры для пропуска только определённой группы пакетов, а потом – для запрета каких-либо групп, как показано в п.2.9. Произведите небольшой прогон и зафиксируйте изменения статистики в круговых диаграммах.

3.6. Очистить таблицу (3-я кнопка слева на панели функций) и запустить генератор пакетов в непрерывном режиме. Генератор пакетов запускается кнопкой из Главного меню (3 шара). Произвести полный анализ статистики (первая кнопка меню) и зафиксировать её результаты в отчёте.

3.7. Перевести генератор пакетов в одиночный режим, очистить статистику и подготовить кадр для передачи на один из компьютеров сегмента вашей локальной сети. При этом нужно подготовить как MAC, так и IP-адреса (Использовать результаты скриншотов). Произвести передачу пакетов и удостовериться в их получении в таблицах «Пакеты» у PC-получателей.

3.8. Провести и зафиксировать в отчёте анализа TCP и UDP-сессий как показано в п. 2.6. Для этого в режиме «Пакеты», ориентируясь на тип протокола (TCP или UDP), щелкнуть правой кнопкой на выбранной строке и продолжить работу по выпадающему меню. Обратите внимание на то, что в анализе TCP-сессии времена указаны с точностью до микросекунд.

3.9. Произвести оценку максимальной производительности Вашего компьютера и сегмента локальной сети в целом. Продумать схему эксперимента с учётом того, что максимальная длина пакета в кадре составляет 1514 байт.

3.10. Через командную строку «Выполнить» ввести команду сбора сетевой статистики netstat. Вызвать адресную таблицу данного хоста (данной ЭВМ) командой netstat - r. Рассмотреть и объяснить её содержание.

Рассмотреть и зафиксировать в отчёте статистические сведения по остальным позициям команды netstat.

3.11. Через командную строку «Выполнить» ввести команду arp - отображения и изменения таблиц преобразования IP-адресов в физические (протокол преобразования адресов – ARP). Рассмотреть и зафиксировать в отчёте статистические сведения по всем позициям команды arp -.

3.12. Проверить связность Вашего компьютера с тремя компьютерами ЛВС СКФ (по выбору) с помощью команды ping. Например:

ping 192.168.0.4 или ping mtuci-ncb.donpac.ru

Сделайте 3 обращения по одному и тому же произвольному адресу глобальной сети и объясните результаты.

3.13. Определите маршруты в Internet к 3-м адресатам по e-mail адресам с помощью команды `tracert`. Например:

`tracert china.com`

Зафиксировать цепочку маршрутизаторов по пути к адресату и времена их прохождения зондирующими пакетами.

3.14. **Для продвинутых студентов.** Изучить самостоятельно дополнительные возможности анализатора CommView и зафиксировать результаты в отчёте.

*Примечание.* Последний пункт предназначен для особо одарённых студентов, успешно выполнивших все предыдущие задания.

#### **4. Содержание отчета.**

Представить схемы, таблицы, графики и диаграммы, полученные по результатам экспериментов лабораторного задания (Раздел 3).

#### **Список использованной литературы**

1. Олифер В.Г. Основы компьютерных сетей/ В.Г. Олифер, Н.А. Олифер. – М: Питер, 2009.

2. CommView – сетевой анализ и мониторинг - TamoSoft; Internet.