CommView®
Краткое руководство
Анализировать пакеты увлекательно!

Об этом руководстве

Это краткое неформальное руководство было создано специально для ответов на часто возникающие вопросы пользователей, которые либо мало знакомы со средствами сетевого анализа, либо являются профессионалами, но еще не пользовались анализатором пакетов, о котором пойдет речь: CommView от компании TamoSoft. Если вам требуется формальная, детализованная документация, то она включена в продукт: просто нажмите F1. Целью же этой статьи не является описание всех функциональных особенностей программы. Скорее, это лишь краткий обзор, который поможет вам познакомиться с CommView.

Несмотря на то, что CommView является, пожалуй, самым удобным для пользователя анализатором пакетов из существующих на рынке, процесс ознакомления все равно займет некоторое время. К счастью, этот процесс довольно краток, так что начнем!

Что же такое анализатор пакетов?

Это лишь звучит угрожающе

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".

Когда вы подключаете кабель к сетевому адаптеру вашего компьютера или подключаетесь к вашему провайдеру через ADSL или dial-up, вы входите в сеть, которая позволяет вашему компьютеру "общаться" со многими другими, будь то веб-сервер вашей любимой поисковой системы, компьютер вашего друга, на котором запущена программа ICQ, или почтовый сервер, хранящий вашу почту. Так же, как и людям, компьютеру надо "общаться" для получения информации. Это как раз то, чем ваш компьютер занят практически каждую секунду, пока вы в сети. Последний раз это случилось несколько секунд назад, когда вы скачали этот документ с нашего веб-сервера.

Опять-таки, так же, как люди для обмена информацией используют разные языки и диалекты, компьютеры используют протоколы – взаимно согласованные стандарты, которые позволяют компьютерам "понимать" друг друга. Проблема состоит в том, что внешне обмен между компьютерами обычно выглядит, как хаотичная последовательность двоичных данных. Именно поэтому вам и нужен анализатор пакетов: он декодирует трафик в сети, придает ему смысл и выполняет множество других интересных функций.

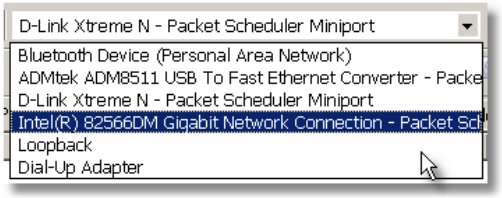
Теперь самое время взглянуть на CommView. Скачайте программу, если вы этого еще не сделали, установите ее на вашем компьютере под Windows 2000/XP/2003/Vista/2008 (32- или 64-бит), и начнем.

CommView: нажал и поехали!

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.



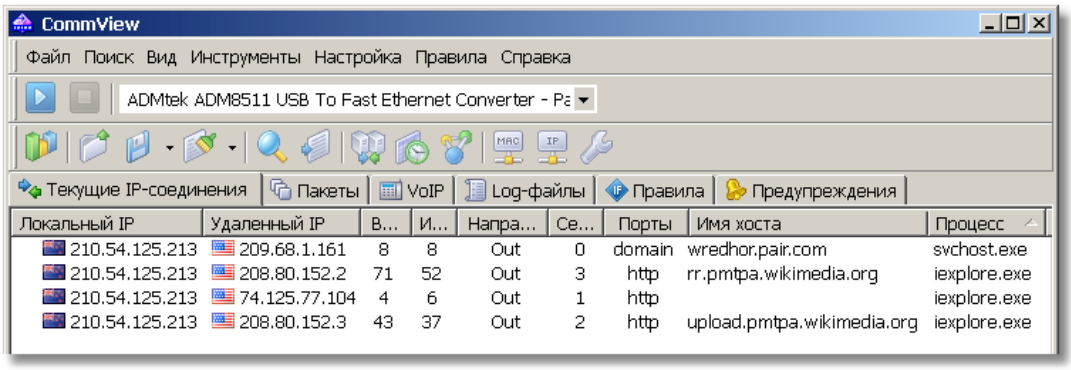
Сделали выбор? Хорошо, теперь нажмите **Начать захват**. Эту кнопку несложно найти на панели инструментов программы:

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.

Есть связь!

Обзор последних IP-соединений

Давайте откроем браузер и посетим веб-сайт Wikipedia, www.wikipedia.org. 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 TCP- или

UDP-порты, участвующие в обмене данными, **Имя хоста** – это имя станции удаленного IP-адреса (если такое имя есть, что бывает не всегда), **Процесс** 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 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, ваш компьютер связался с сервером доменных имен (в нашем случае это 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 IP-адрес сайта 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).

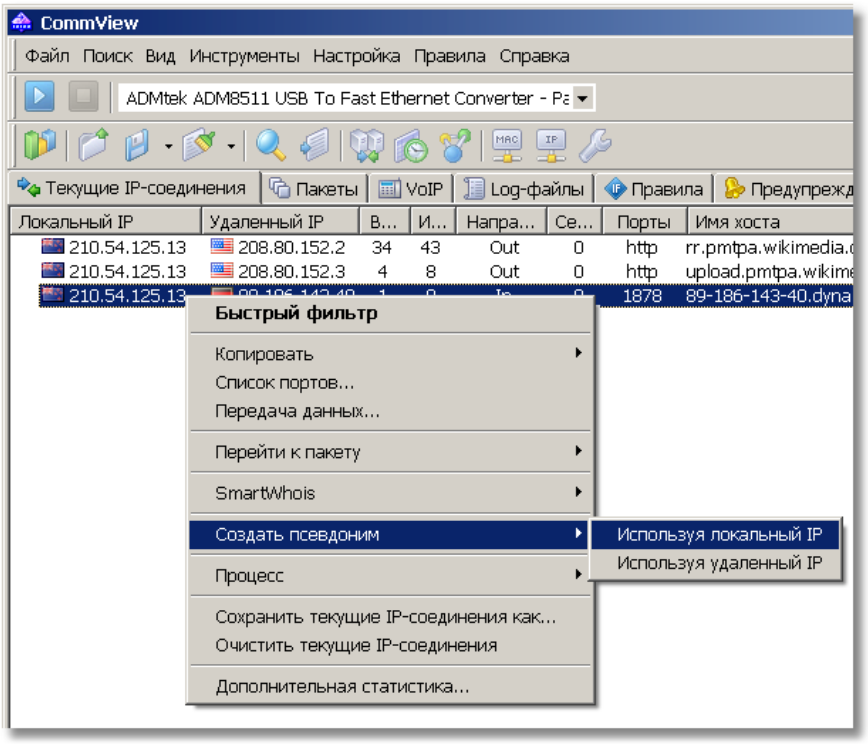
После этого соединения могут идти другие, но мы поговорим об этом позже. Сейчас же мы выяснили, что в закладке **Текущие IP-соединения** показаны все текущие соединения.

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. Если вы не очень хорошо знакомы с флагами, CommView может вместо них использовать названия стран и двухбуквенные коды стран. Для этого откройте окно **Установки** и настройте опции отображения так, как вам больше нравится.

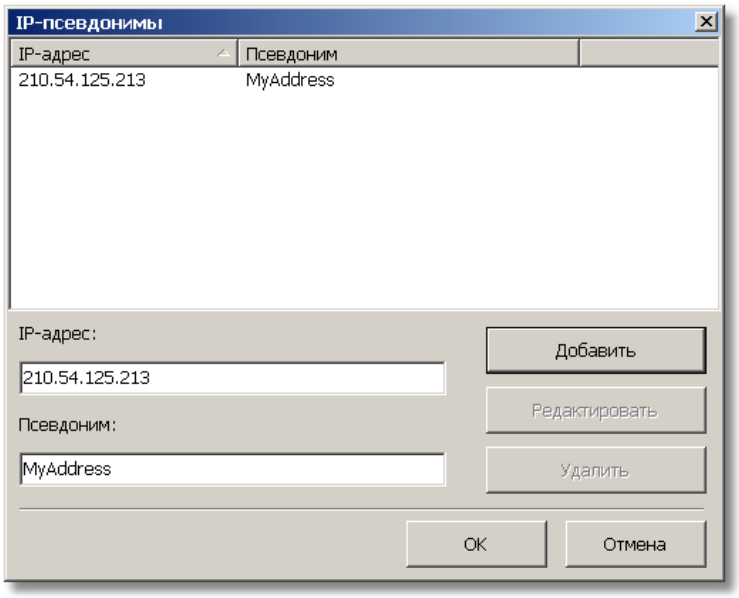
Упрощаем

Использование псевдонимов

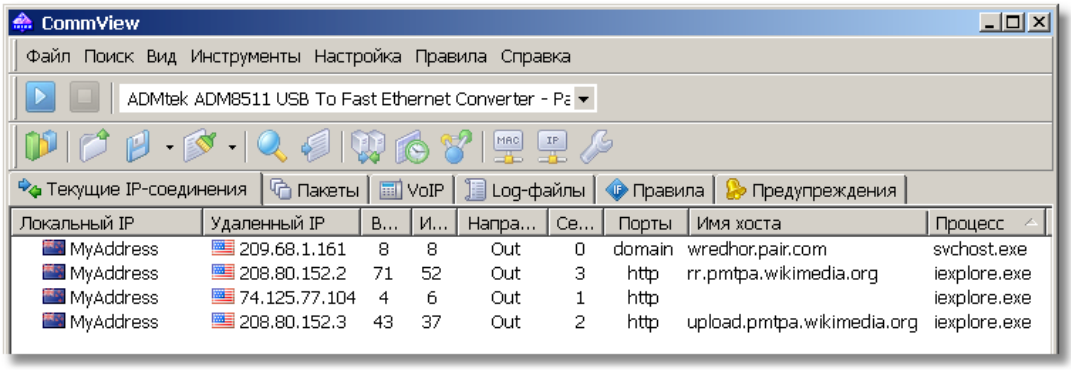
Посмотрим правде в глаза: числовые IP-адреса сложно запомнить. К счастью, вам не придется это делать. Кликните правой кнопкой мыши по любой строке в таблице **Текущие IP-соединения** и выберите **Создать псевдоним => Используя локальный IP**.



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



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



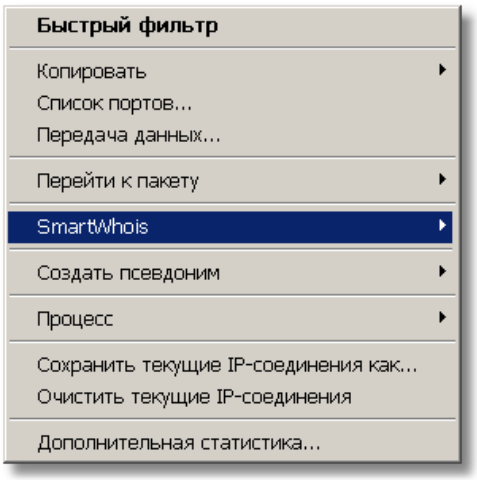
вы увидите, что данные теперь выглядят более понятно, особенно если вы наблюдаете сегмент локальной сети с десятками компьютеров. Мы видим, что первое соединение было DNS-запросом, а второе и четвертое – http-сессиями с Wikipedia. Это то, что мы ожидали увидеть? Не совсем… что это за подключение к 74.125.77.104?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

Небольшое расследование

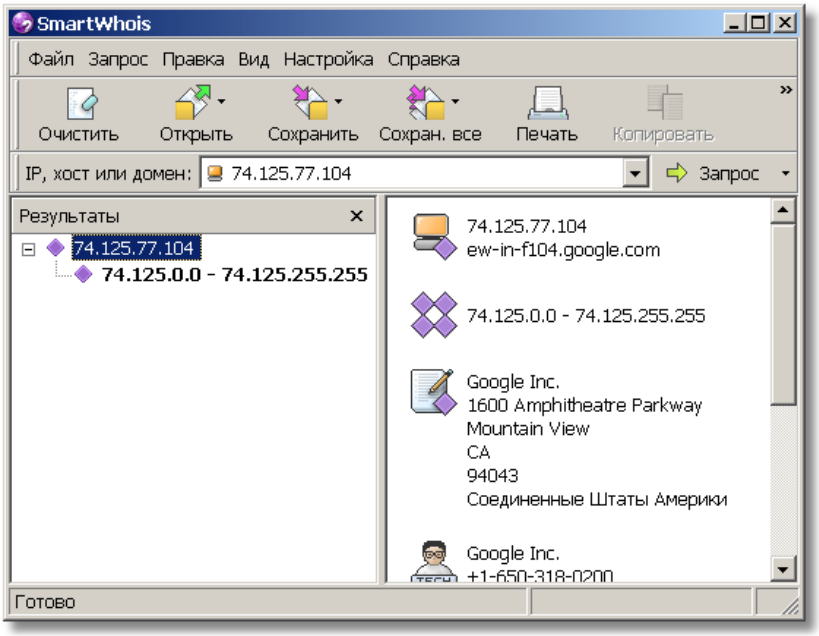
Пытаемся выяснить больше о текущих соединениях

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 незамеченным 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 посмотреть, 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 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 информаций 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.

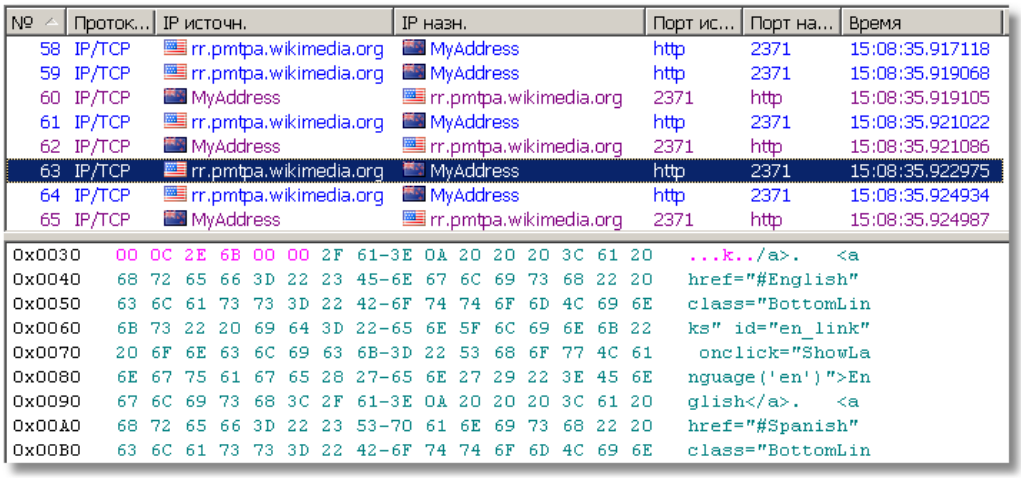
Пакеты, пакеты, пакеты...

Смотрим на перехваченные пакеты

Теперь, после того, как мы изучили первую закладку главного окна CommView, давайте перейдем ко второй – **Пакеты**. В этой трехсекционной 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. Эти панели можно расположить удобным для себя образом с помощью небольшой панели инструментов:

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   nguage('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
```

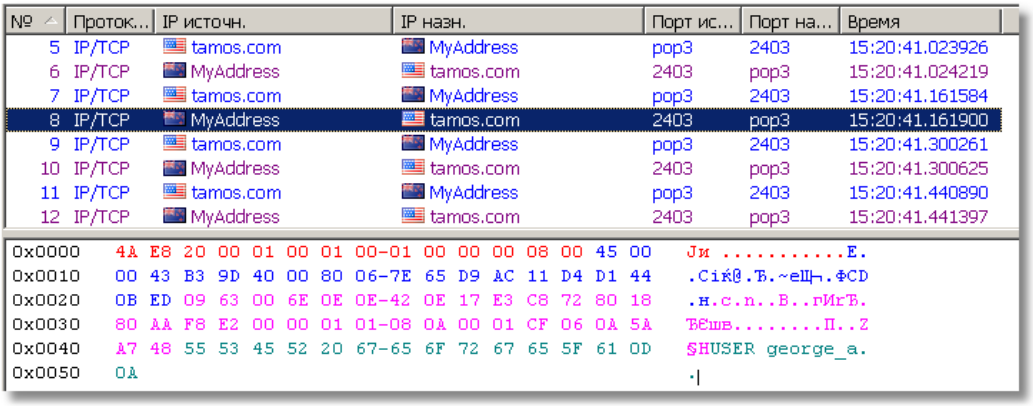
В зависимости от выбранного вами пакета вы увидите либо запрос на получение веб-страницы, либо ответ сервера, который содержит в себе содержимое страницы. Последнее

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 прочитать, 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.

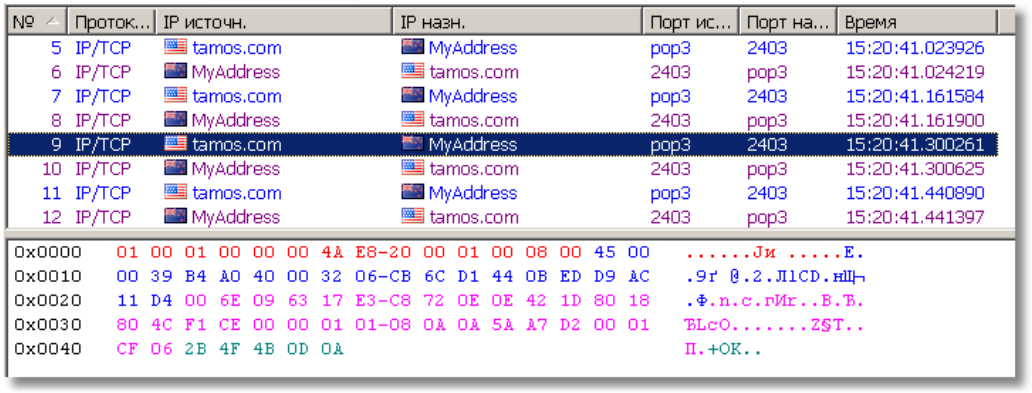
Вот решение проблемы. Проверьте почту вашей старой программой и перехватите эту сессию с помощью CommView. После этого просмотрите пакеты POP3:



№	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   Jи ..........E.
0x0010   00 43 B3 9D 40 00 80 06-7E 65 D9 AC 11 D4 D1 44   .Ciќ@.Ъ.~eЩ¬.ФСD
0x0020   0B ED 09 63 00 6E 0E 0E-42 0E 17 E3 C8 72 80 18   .н.c.n..B..rИrЪ.
0x0030   80 AA F8 E2 00 00 01 01-08 0A 00 01 CF 06 0A 5A   ЪЄшв........П..Z
0x0040   A7 48 55 53 45 52 20 67-65 6F 72 67 65 5F 61 0D   §HUSER george_a.
0x0050   0A                                               .|
```

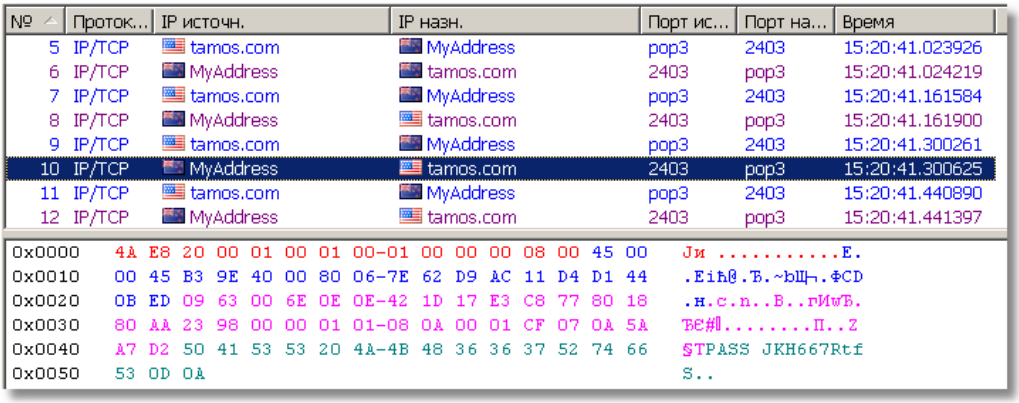
Вот имя пользователя …



№	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   ......Jи .....E.
0x0010   00 39 B4 A0 40 00 32 06-CB 6C D1 44 0B ED D9 AC   .9ґ @.2.ЛlCD.нЩ¬
0x0020   11 D4 00 6E 09 63 17 E3-C8 72 0E 0E 42 1D 80 18   .Ф.n.c.rИr..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 …



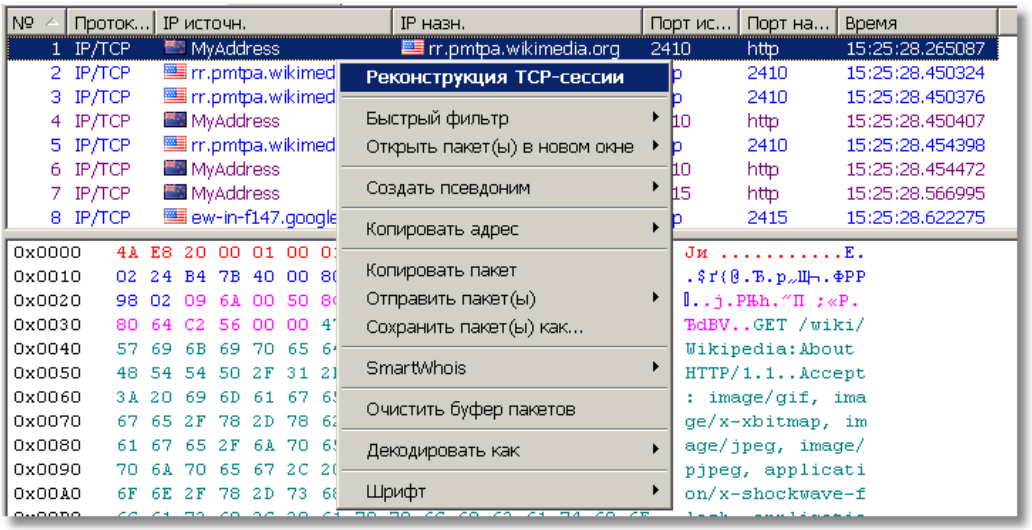
… а вот и сам пароль, который мы искали!

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

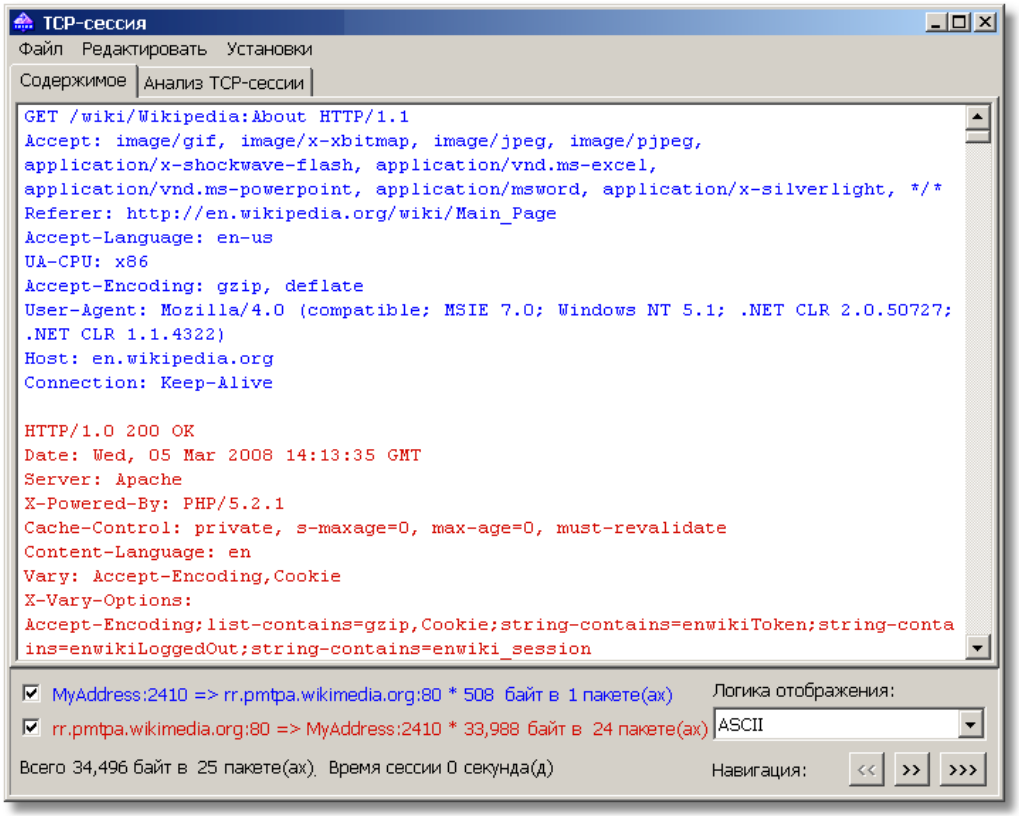
Посмотрим на эту сессию

Потоки данных TCP

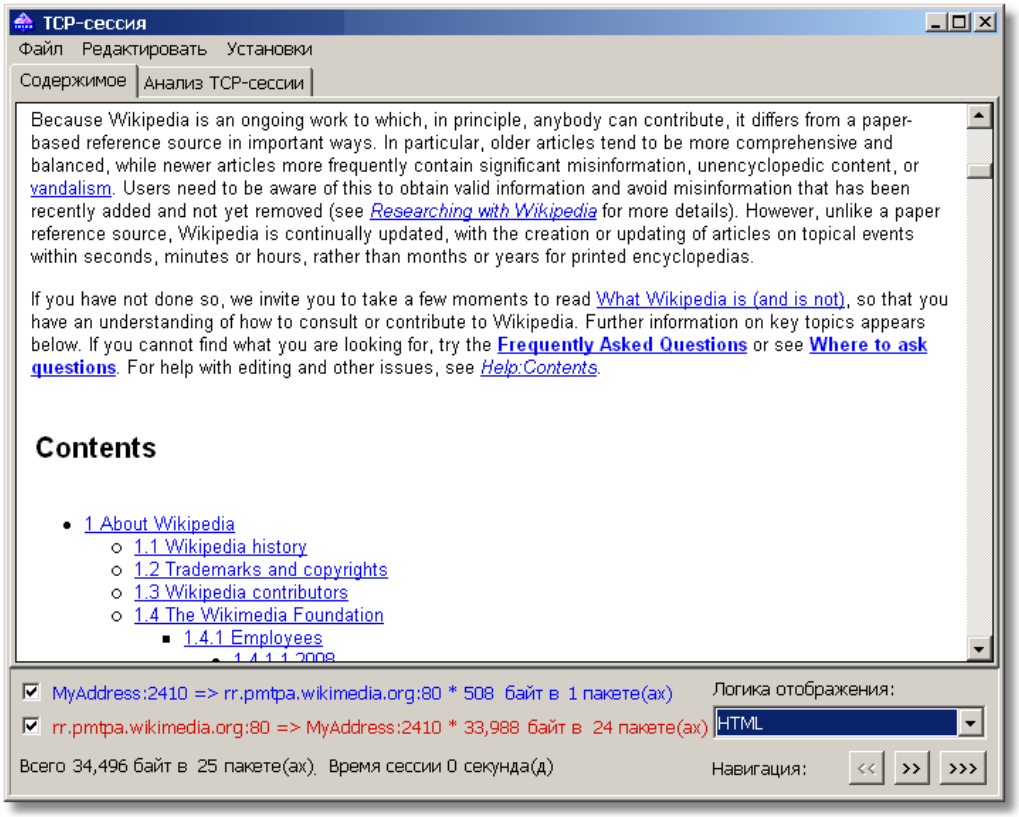
Мы видим данные, разбитые на множество пакетов. Но можно ли заново собрать TCP-сессии? Да, с помощью CommView это возможно. Выберите первый пакет в сессии (например, тот, где браузер запрашивает страницу с веб-сервера), кликните по нему правой кнопкой мыши и выберите **Реконструкция TCP-сессии**. Можете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



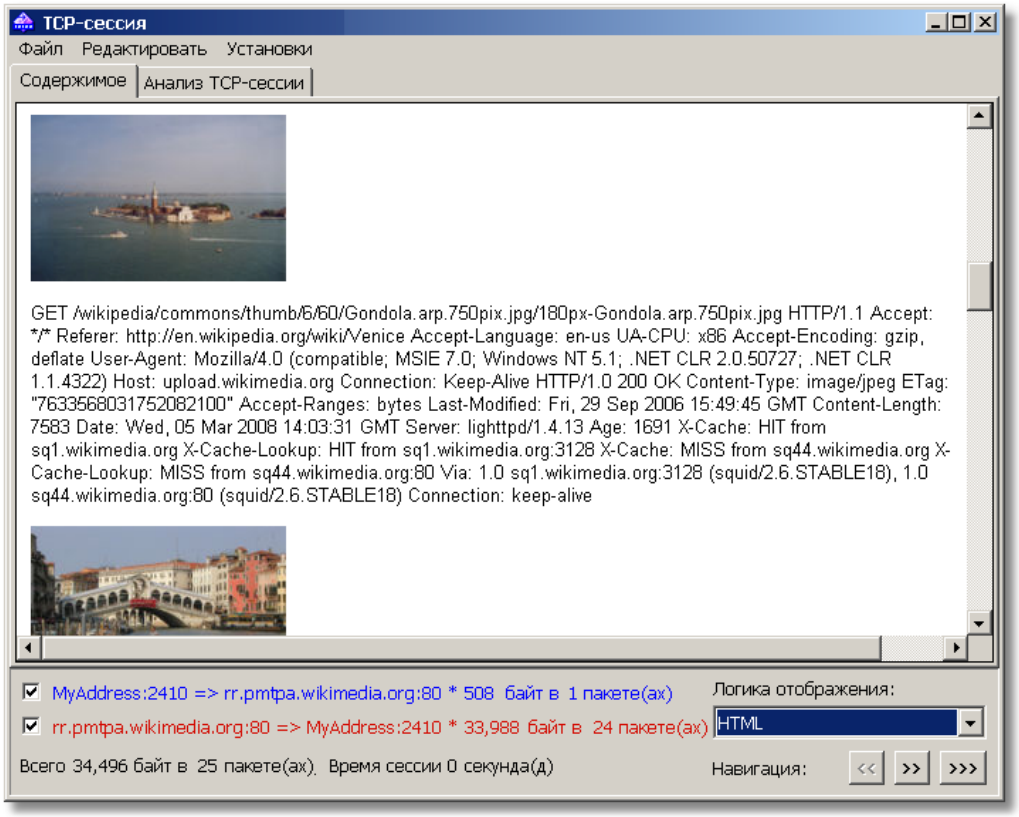
Пожалуйста, перед нами процесс обмена данными между нашим компьютером и веб-сервером Wikipedia. Текст запроса выведен синим, а ответ сервера – красным:



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:

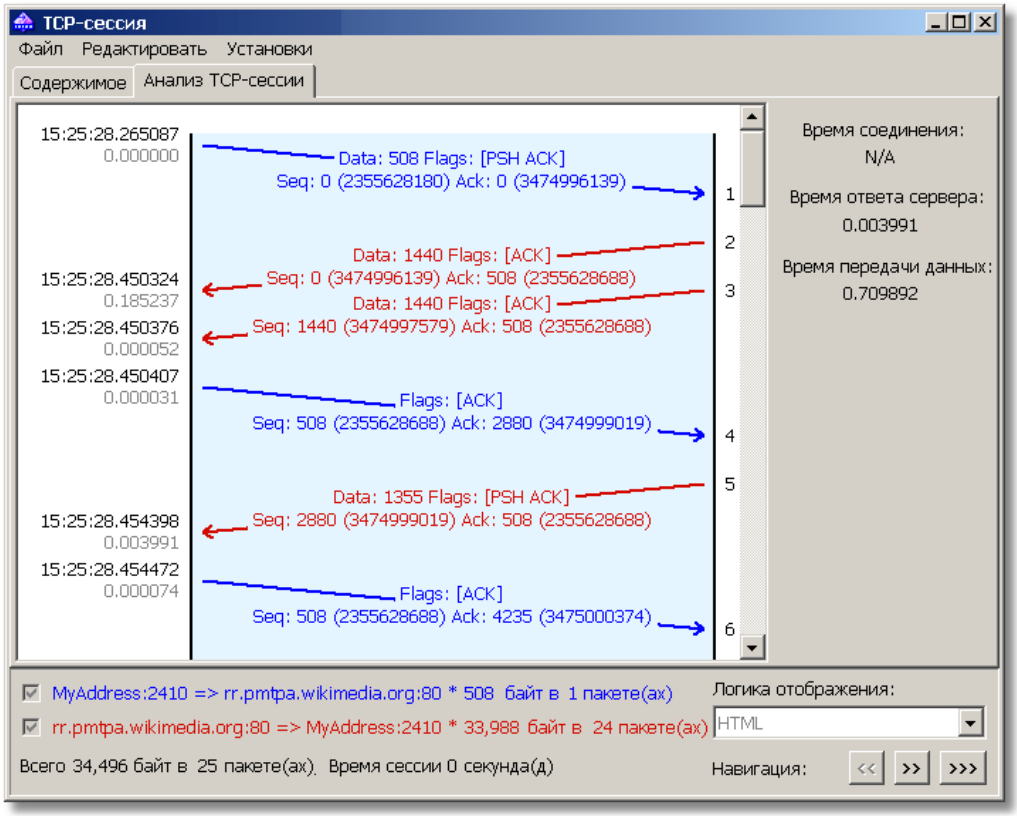


Все хорошо, но почему нет картинок? А потому, что графика обычно передается в другой TCP-сессии, и иногда с другого сервера. Нажав на кнопку **>>>** , вы перейдете к следующей TCP-сессии и найдете картинки (или совершенно другую TCP-сессию, ведь ваш компьютер к тому времени мог сделать несколько подключений):



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

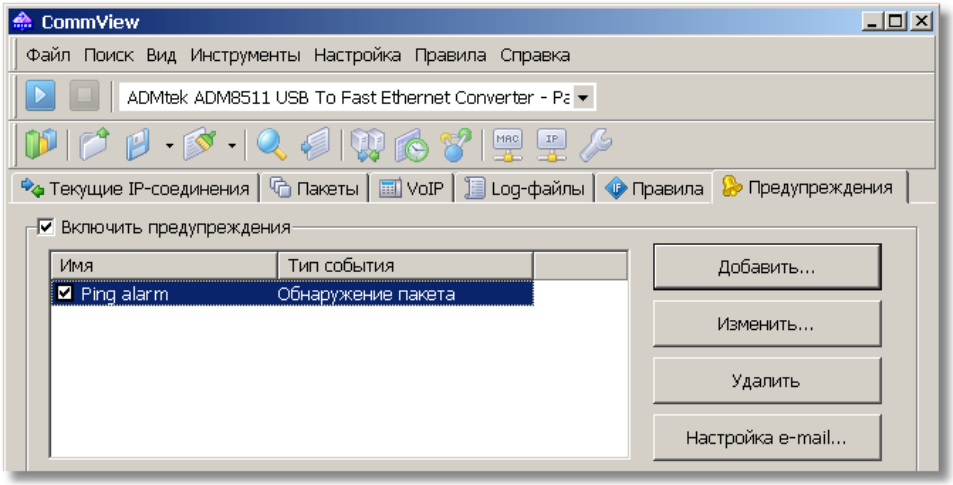
Если в области сетей вы профессионал и хотите посмотреть потоки TCP-сессии в виде лестничной диаграммы, переключитесь в закладку **Анализ TCP-сессии**:



Тревога!

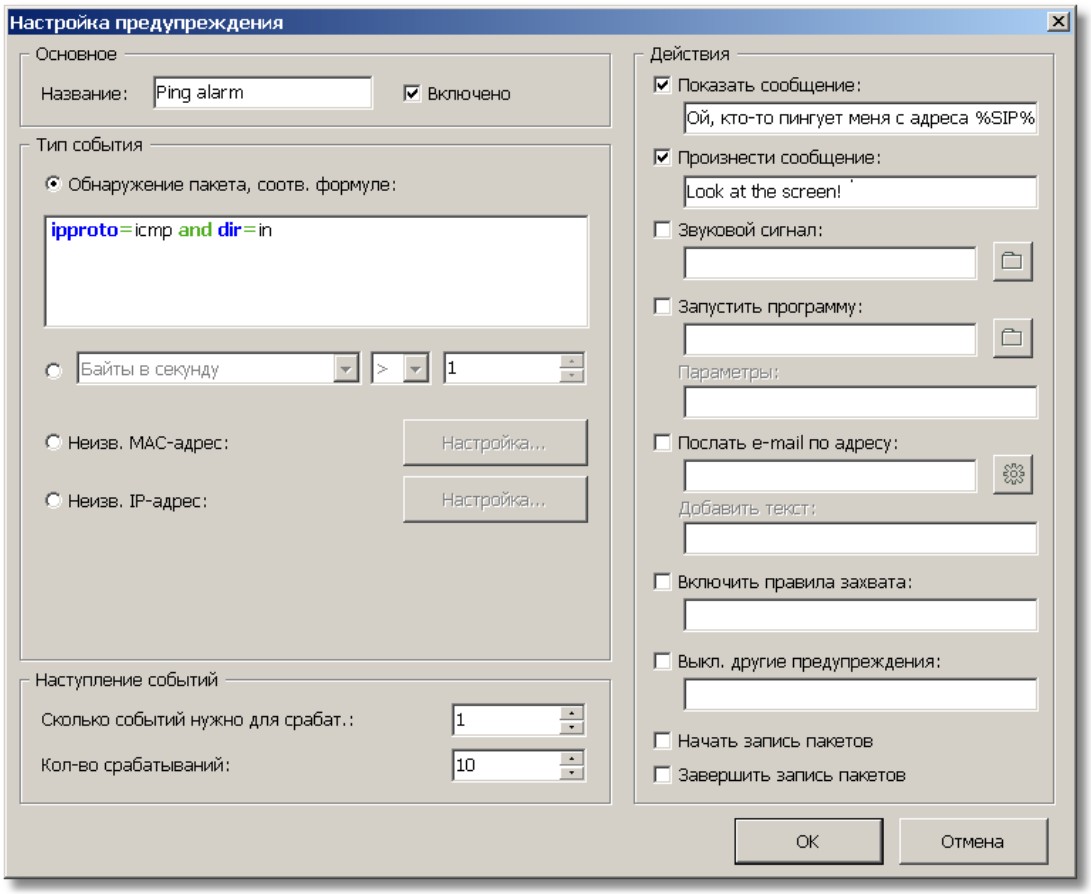
Как работают предупреждения

Помимо пассивного мониторинга, CommView может уведомлять вас о важных событиях в сети. Для этого и нужна закладка **Предупреждения**. Перейдите в эту закладку, активируйте опцию **Включить предупреждения** и нажмите **Добавить**.



Появится большое окно настройки предупреждений с множеством селекторов и кнопок, но не пугайтесь; для начала мы попробуем что-то очень простое. Предположим, мы хотим

получать уведомления каждый раз, когда кто-то пингует наш компьютер или мы пингуем чей-то компьютер. Для этого мы создадим новое предупреждение под названием *Ping Alarm*, которое будет срабатывать каждый раз при приеме пакета ICMP.



В CommView есть встроенный язык, с помощью которого можно задать формулу, включающую в себя событие для предупреждения или правило перехвата. Подробное объяснение принципов этого языка выходит за рамки данного обзора, но вы всегда можете обратиться к главе **Универсальные предупреждения** файла-справки программы. А сейчас просто воспользуемся готовой формулой:

```
ipproto=icmp and dir=in
```

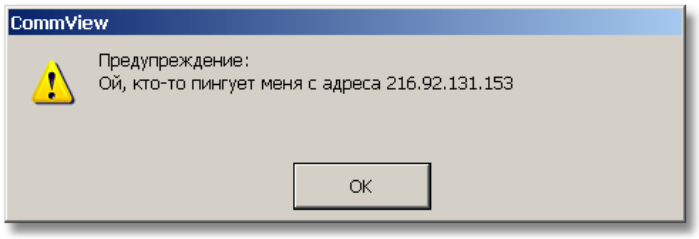
На человеческом языке это означает, что нас интересует каждый входящий ICMP-пакет (поскольку при Ping используется протокол ICMP). В области **Наступление событий** мы можем указать, сколько CommView должен выдать предупреждений перед тем, как отключить уведомления. Выбираем десять. В завершение нам предстоит выбрать, как именно CommView будет нас оповещать о событии. Как насчет всплывающего окна? Хорошо, выбираем **Показать сообщение** и вводим следующий текст:

Ой, кто-то пингует меня с адреса %SIP% !

Что такое "*%SIP%*"? Вместо этой переменной будет подставлен реальный IP-адрес компьютера, который вас пинговал (SIP = Source IP Address = IP-адрес источника). Вам необязательно использовать такую переменную, но все же интересно знать, кто вас

пинговал. В разделе **Предупреждения** файла-справки программы вы найдете более подробную информацию о синтаксисе и сообщениях. Мы также выберем опцию **Произнести сообщение,** чтобы услышать в динамиках голос компьютера.

Итак, мы закончили настройку. Нажмите **ОК** и закройте окно настройки предупреждения, мы готовы к тестированию. Не забудьте начать перехват и перейдите на веб-сайт, откуда можно пропинговать IP-адрес, например, сюда: http://www.all-nettools.com/toolbox. Введите ваш IP-адрес в поле модуля **Ping** и нажмите "Go!". Через несколько секунд CommView известит вас о входящем ping-пакете:

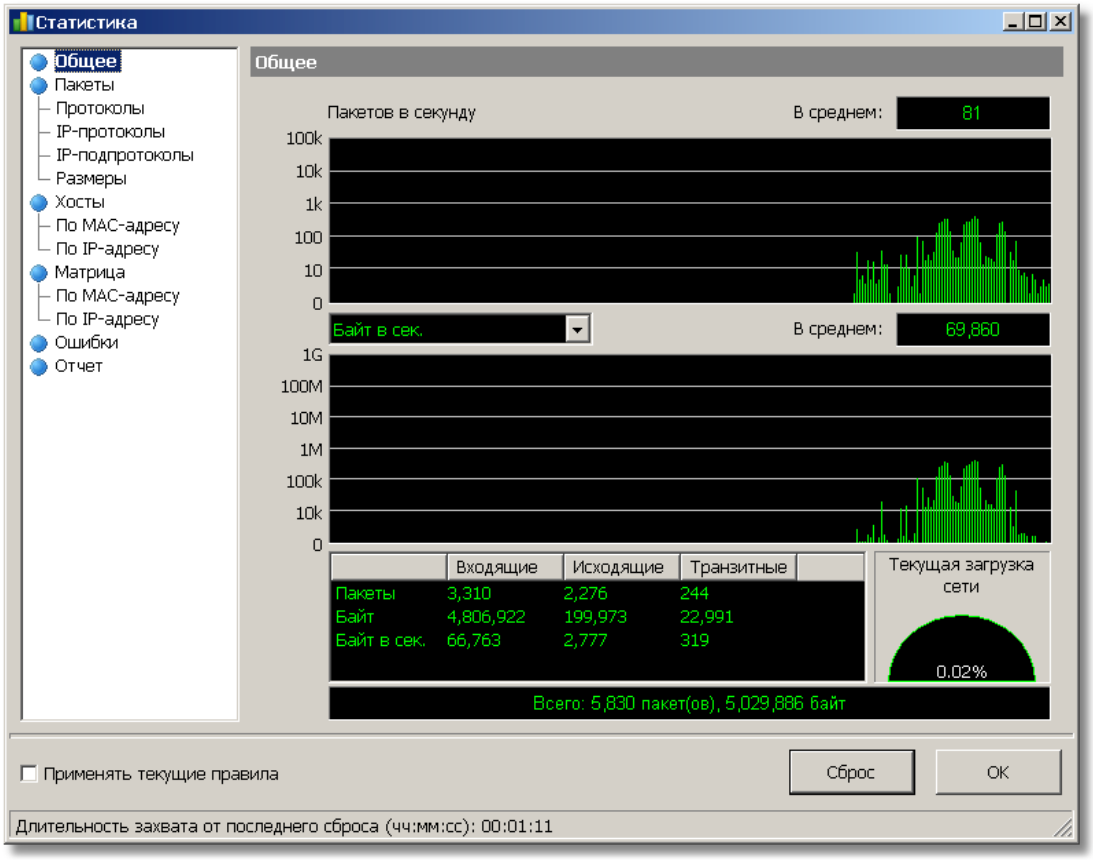


Кроме этого, система речевых сигналов вашего компьютера произнесет приятным (ну ладно уж, не совсем приятным) механическим голосом через наушники или динамик фразу "Look at the screen". Заметим, что Windows поставляется только с английскими "голосами", поэтому текст предупреждения мы ввели на английском языке. На русском это, увы, не сработает. Это лишь два из всех возможных способов оповещения. Можно получать сообщения электронной почты на ваш ящик, запускать программу, и т. д.

А как поживает мое соединение?

Наблюдаем загрузку сети

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

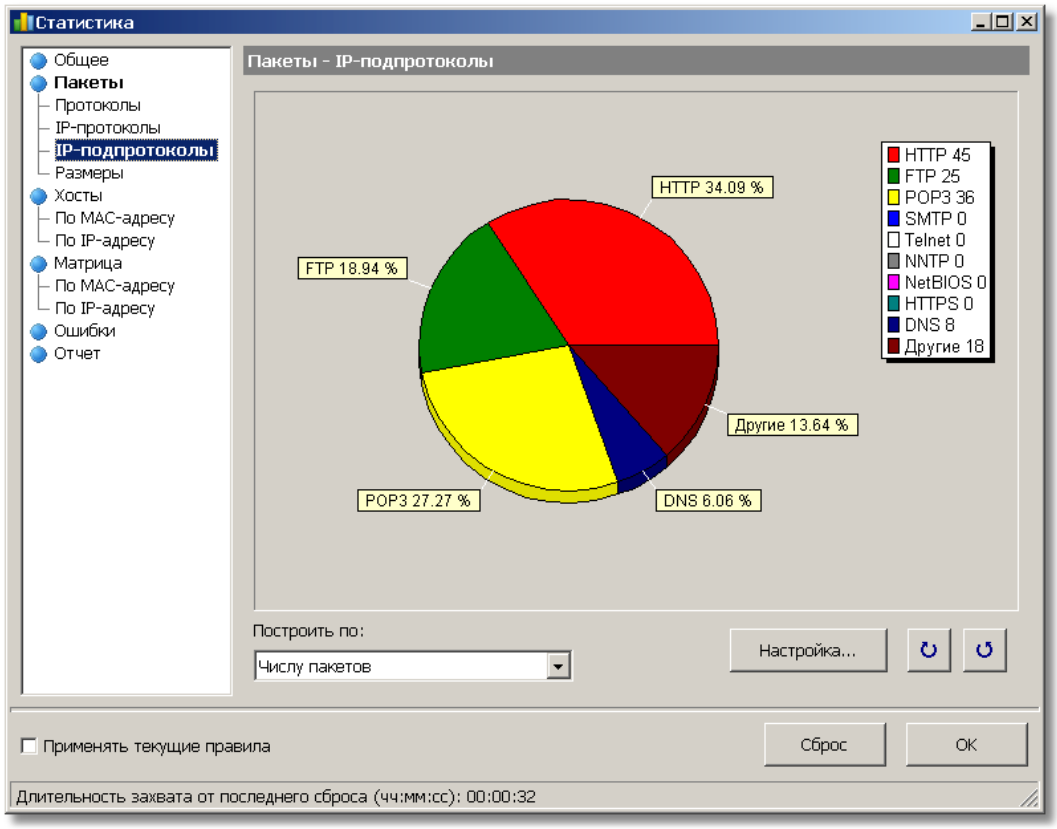


На этих графиках показана информация о передаваемых в вашей сети пакетах и байтах в реальном времени. Почему это так важно многим пользователям? Если вы находитесь в локальной сети, то это важные показатели качества работы вашего сегмента. Если загрузка вашего сегмента сети слишком велика, то есть повод 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.

Диалекты моей сети

Диаграммы протоколов

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

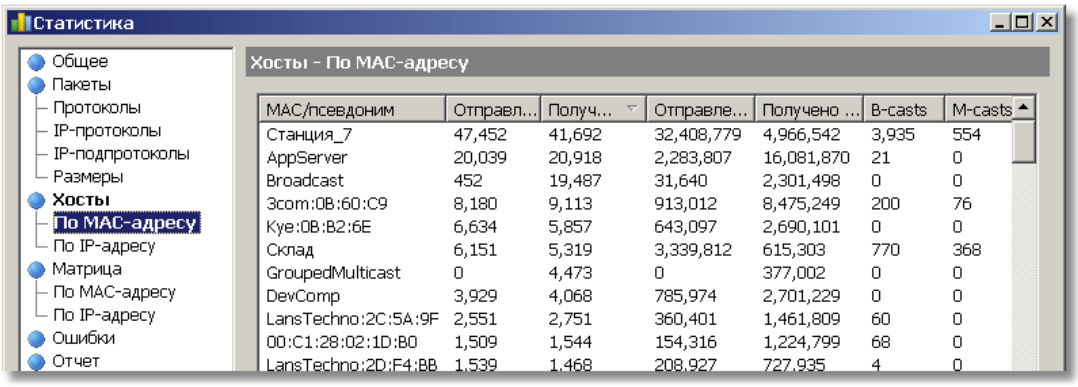


На этой секторной диаграмме вы сразу увидите, какие протоколы используются в вашей сети. Слишком большой SMTP-трафик? Ваш ПК или другие станции в вашем сегменте сети передают слишком много почты. Слишком большой FTP-трафик? Пожалуй, скачивается много программ. Хотя по умолчанию в диаграмме показаны наиболее популярные протоколы, вы всегда можете кликнуть по кнопке **Настройка** и ввести новый протокол и номер порта, например, для получения информации о популярном p2p-клиенте или chat-программе.

Кто перегружает мою сеть?

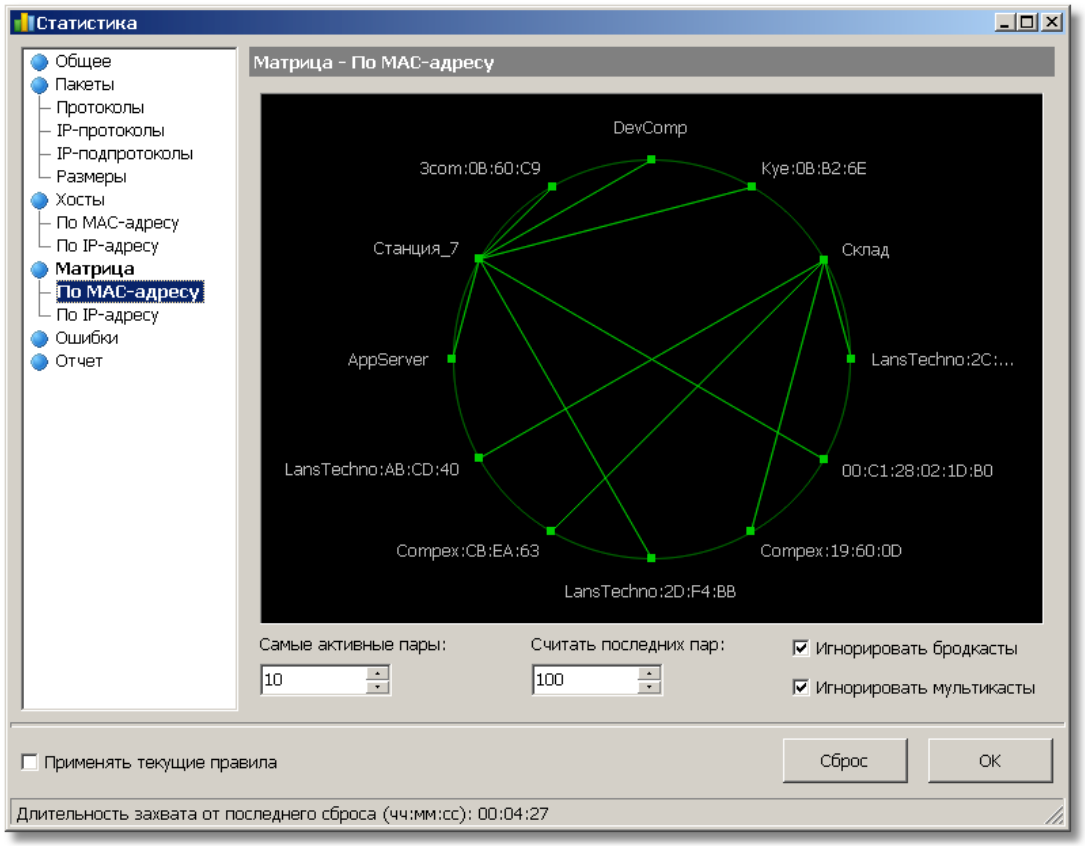
Ищем источники перегрузок

Теперь, когда мы разобрались с протоколами, мы, вероятно, захотим узнать, кто же больше всего общается в нашей сети. Для этого перейдем в закладку **Хосты (по MAC-адресу)**. Если ваш компьютер не является частью локальной сети, то в этой закладке вы не найдете ничего полезного, но если вы наблюдаете сегмент сети с компьютера, подключенного к порту мониторинга свича (или старого доброго хаба), вы легко вычислите источники наибольшей нагрузки или станции, ответственные за массовую рассылку бродкастов ("broadcast storms").



Как вы, возможно, знаете, сетевой анализатор переводит ваш адаптер в так называемый режим "promiscuous", в котором вы можете перехватывать не только пакеты, адресованные вашему компьютеру, но и другие пакеты, передаваемые или принимаемые в вашем сегменте сети. Обратите внимание, что некоторые записи в первой колонке – это MAC-адреса, в то время как другие являются читаемыми именами. Помните, как мы привязывали псевдонимы к IP-адресам в предыдущих главах? То же самое можно делать и с MAC-адресами, для этого кликните правой кнопкой мыши и выберите в меню пункт **Псевдонимы**.

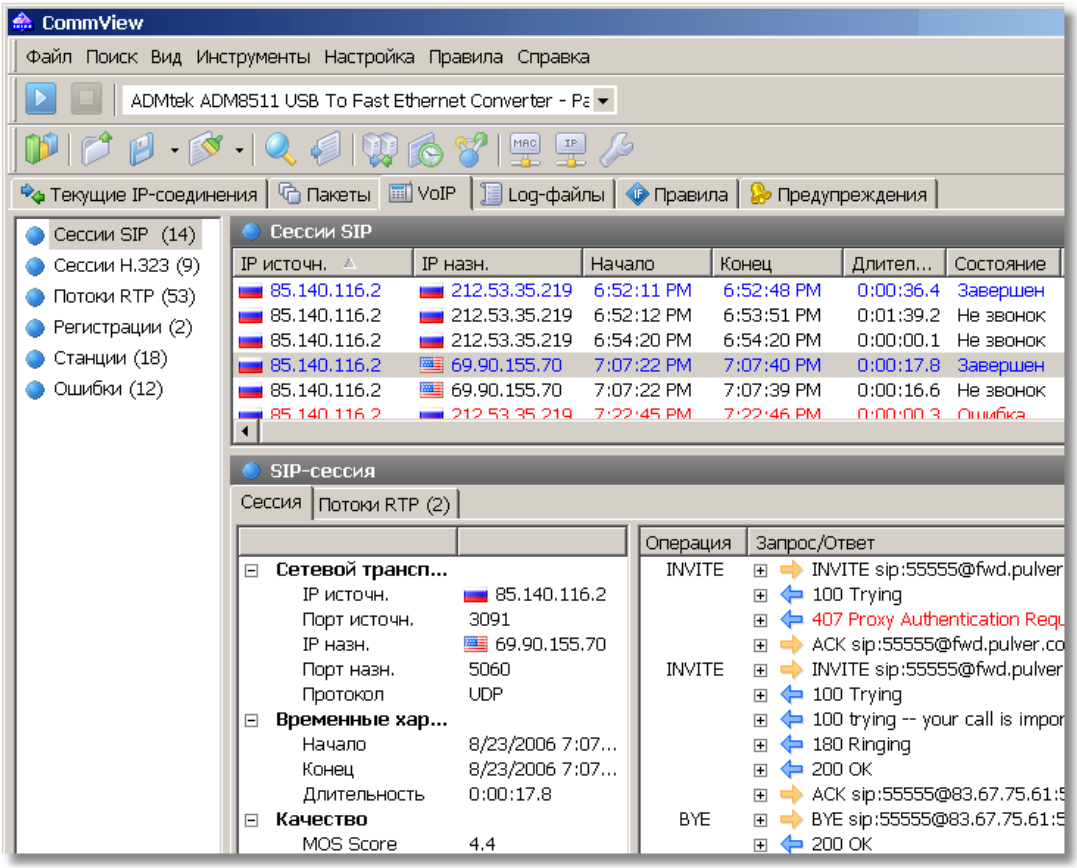
Еще один способ взглянуть на активные узлы вашего сетевого сегмента – закладка **Матрица**. В этой закладке показана карта клиентов, в которой обозначены потоки трафика между различными хостами. С помощью матрицы вы сразу увидите, кто с кем обменивается данными:



Отдайте свой голос!

Работа с модулем анализа VoIP

Те сетевые специалисты, которые имеют дело с внедрением и эксплуатацией сетей IP-телефонии, знают, насколько полезен может оказаться сетевой анализатор при отладке и мониторинге VoIP. Здесь на помощь приходит CommView с его модулем анализа протоколов SIP и H.323. Анализ VoIP выходит далеко за рамки данного обзора, но мы решили, что обозначить эту функцию просто необходимо.

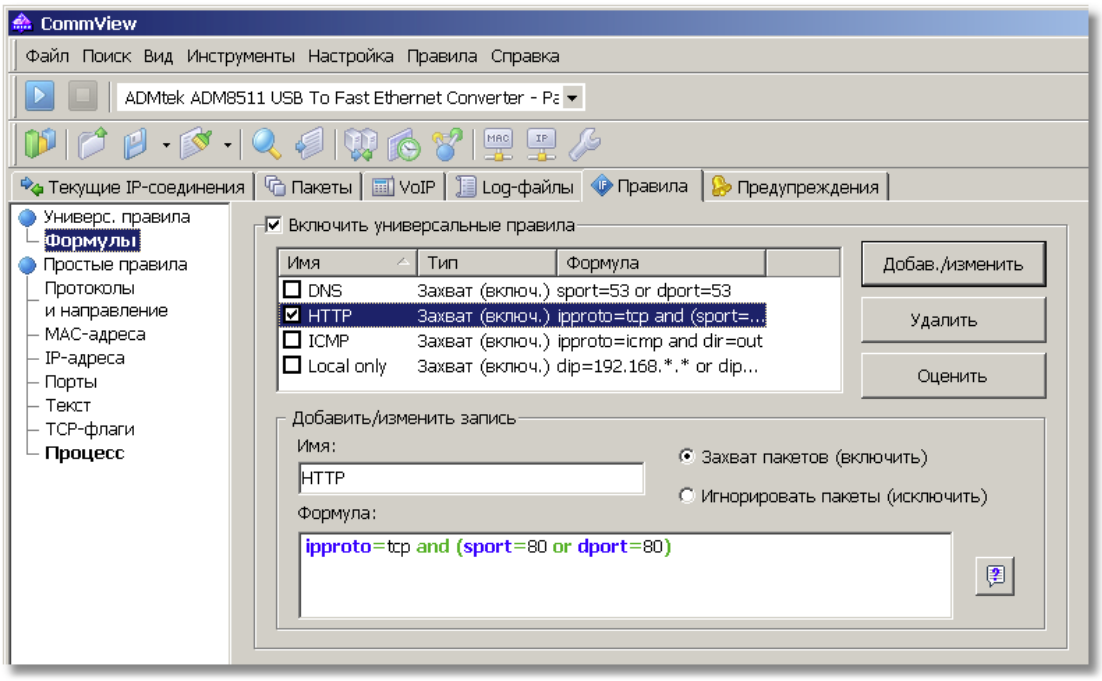


При работе с CommView вы можете анализировать сигнальные сессии и потоки RTP в реальном времени, выявлять возможные проблемы с качеством вашей VoIP-сети с помощью графиков и диаграмм (потери пакетов, джиттер или ошибки последовательности), наблюдать за показателями MOS и R-factor каждого звонка. И еще – CommView может записывать и воспроизводить звонки. О том, как это можно использовать в работе, подробно рассказано в статье Мониторинг и отладка VoIP-сетей с помощью сетевого анализатора.

Сосредоточимся на важном

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.

Как мы уже упоминали выше, в главе **Универсальные правила** файла-справки программы вы найдете подробное описание синтаксиса формул.

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

```
ipproto=tcp and (sport=80 or  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. Ах, да… вы можете сохранять правила в файл и загружать их из файла с помощью пункта меню **Правила** главного окна программы.

Идем дальше

Мы надеемся, что этот обзор помог вам лучше понять тот мощный инструмент, который вы купили или планируете купить. Этот обзор ни в коем случае не является полноценным руководством. Мы лишь хотели показать, что анализировать пакеты увлекательно, особенно с CommView!

По мере ознакомления с функциональными возможностями продукта, задачи сетевого анализа и декодирования протоколов будут для вас решаться все легче и легче. Если вы работаете в беспроводной сети, не пропустите специальную беспроводную версию этой программы - CommView for WiFi.

Посетив наш сайт, www.tamos.ru, вы найдете более подробную информацию, отменную техническую поддержку, возможности онлайн-заказа и многое другое!