МДК.01.01
Организация, принципы построения и функционирования компьютерных сетей
2-курс

Занятие 21, 22

Снифферы или Анализаторы сетевых пакетов

Снифферы или Анализаторы сетевых пакетов

Анализаторы сетевых пакетов, или **снифферы**, первоначально были разработаны как средство решения сетевых проблем.

Они умеют **перехватывать**, **интерпретировать** и **сохранять** для последующего анализа пакеты, передаваемые по сети.

С одной стороны, это **позволяет** системным администраторам и инженерам службы технической поддержки **наблюдать** за тем, как данные передаются по сети, диагностировать и устранять возникающие проблемы.

В этом смысле пакетные снифферы представляют собой мощный инструмент диагностики сетевых проблем.

Снифферы или Анализаторы сетевых пакетов

С другой стороны, подобно многим другим мощным средствам, изначально предназначавшимся для администрирования, с течением времени снифферы стали применяться абсолютно **для других целей**.

Действительно, сниффер в руках **злоумышленника** представляет собой довольно опасное средство и может использоваться для завладения паролями и другой конфиденциальной информацией.

Однако не стоит думать, что снифферы — это некий инструмент, посредством которого любой хакер сможет легко просматривать конфиденциальную информацию, передаваемую по сети.

Принципы работы пакетных снифферов

Принципы работы пакетных снифферов

Сниффер — это программа, которая работает на уровне сетевого адаптера NIC (Network Interface Card) (канальный уровень) и скрытым образом перехватывает весь трафик.

Поскольку снифферы работают на канальном уровне модели OSI, они не должны играть по правилам протоколов более высокого уровня.

Снифферы обходят механизмы фильтрации (адреса, порты и т. д.), которые драйверы Ethernet и стек TCP/IP используют для интерпретации данных.

Пакетные снифферы захватывают из кабеля все данные, которые по нему передаются.

Снифферы могут сохранять кадры в двоичном формате и позже расшифровывать их, чтобы раскрыть информацию более высокого уровня, спрятанную внутри (рис. 1).

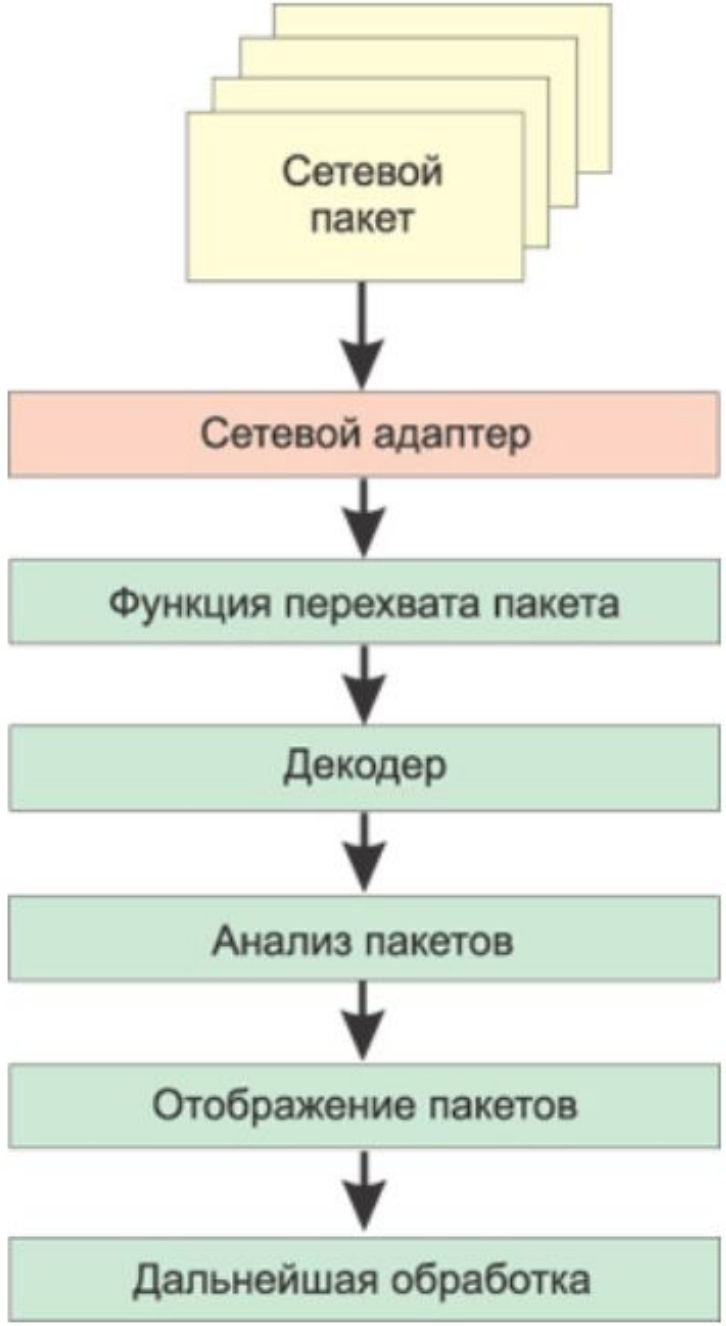

Рис. 1. Схема работы сниффера

Принципы работы пакетных снифферов

Для того чтобы сниффер мог перехватывать все пакеты, проходящие через сетевой адаптер, драйвер сетевого адаптера должен поддерживать режим функционирования promiscuous mode (**беспорядочный режим**).

Именно в этом режиме работы сетевого адаптера сниффер способен перехватывать все пакеты.

Данный режим работы сетевого адаптера **автоматически** активизируется при запуске сниффера или устанавливается вручную соответствующими настройками сниффера.

Принципы работы пакетных снифферов

Весь перехваченный трафик передается **декодеру** пакетов, который идентифицирует и **расщепляет** пакеты по соответствующим уровням иерархии.

В зависимости от возможностей конкретного сниффера представленная информация о пакетах может впоследствии дополнительно анализироваться и отфильтровываться.

Ограничения использования снифферов

Ограничения использования снифферов

Наибольшую опасность снифферы представляли в те времена, когда информация передавалась по сети в **открытом виде** (без шифрования), а локальные сети строились на основе **концентраторов** (хабов).

Однако эти времена безвозвратно ушли, т.к значительная часть информации **шифруется**, концентраторы постепенно вытесняются коммутаторами.

В настоящее время использование снифферов для получения доступа к конфиденциальной информации — задача отнюдь не из простых.

Ограничения использования снифферов

Дело в том, что при построении локальных сетей на основе **концентраторов** существует некая общая среда передачи данных (сетевой кабель).

Все узлы сети обмениваются пакетами, конкурируя за доступ к этой среде (рис. 2).

Причем пакет, посылаемый одним узлом сети, передается на **все порты** концентратора.

Этот пакет **прослушивают** все остальные узлы сети, но **принимает** его только тот узел, которому он адресован.

Ограничения использования снифферов

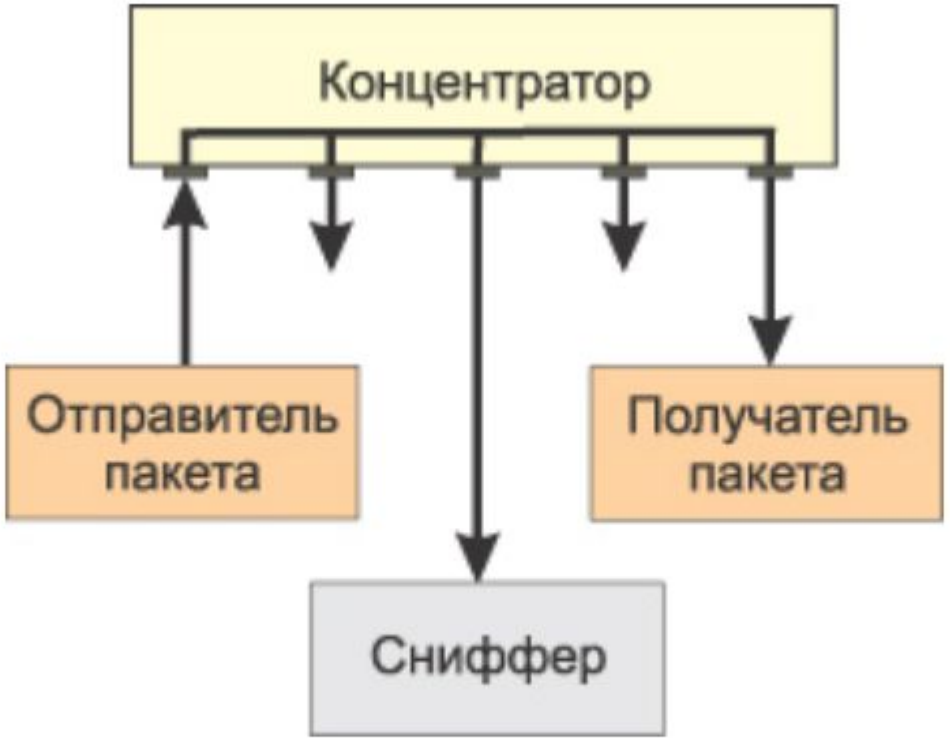

Рис. 2. При использовании концентраторов сниффер способен перехватывать все пакеты сетевого сегмента

Ограничения использования снифферов

При этом если на одном из узлов сети установлен пакетный **сниффер**, то он **может перехватывать** все сетевые пакеты, относящиеся к данному сегменту сети (участком сети, образованной концентратором).

Коммутаторы являются более **интеллектуальными** устройствами, чем широковещательные концентраторы

Коммутаторы **изолируют** сетевой трафик.

Ограничения использования снифферов

Коммутатор **знает адреса** устройств, подключенных к каждому порту, и передает пакеты только между нужными портами.

Это позволяет **разгрузить** другие порты, не передавая на них каждый пакет, как это делает концентратор.

Таким образом, посланный неким узлом сети пакет передается только на тот порт коммутатора, к которому подключен получатель пакета.

Все остальные узлы сети **не имеют** возможности обнаружить данный пакет (рис. 3).

Ограничения использования снифферов

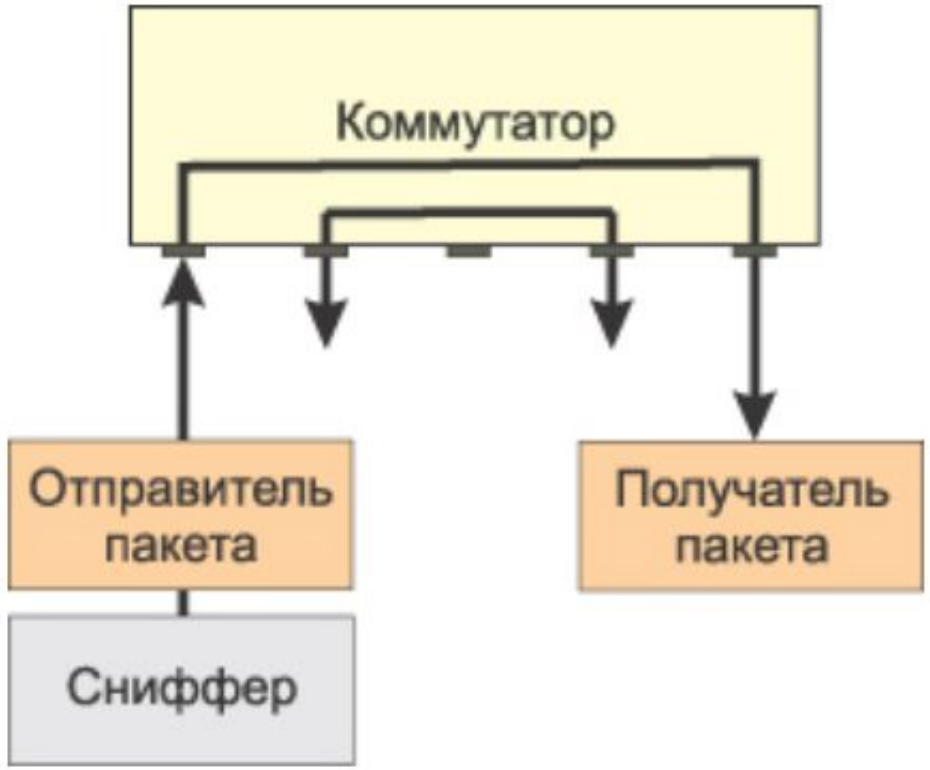

Рис. 3. При использовании коммутаторов сниффер способен перехватывать только входящие и исходящие пакеты одного узла сети

Ограничения использования снифферов

Поэтому если сеть построена на основе коммутатора, то сниффер, установленный на одном из компьютеров сети, **способен перехватывать** только те пакеты, которыми обменивается **данный компьютер** с другими узлами сети.

В результате, чтобы иметь возможность перехватывать пакеты, которыми интересующий злоумышленника компьютер или сервер обменивается с остальными узлами сети, **необходимо установить** сниффер именно **на этом компьютере** (сервере).

А это на самом деле не так-то просто.

Ограничения использования снифферов

Правда, следует иметь в виду, что некоторые пакетные снифферы запускаются **из командной строки** и могут не иметь графического интерфейса.

Такие снифферы, в принципе, можно устанавливать и запускать **удаленно** и **незаметно** для пользователя.

Кроме того, необходимо также иметь в виду следующее.

Хотя коммутаторы изолируют сетевой трафик, все управляемые коммутаторы имеют функцию **перенаправления** или **зеркалирования** портов.

То есть порт коммутатора можно настроить таким образом, чтобы на него **дублировались** все пакеты, приходящие на другие порты коммутатора.

Ограничения использования снифферов

Если в этом случае к такому порту подключен компьютер с пакетным снифферером, то он может **перехватывать** все пакеты, которыми обмениваются компьютеры в данном сетевом сегменте.

Однако, как правило, возможность конфигурирования коммутатора доступна только **сетевому администратору**.

Это, конечно, не означает, что он не может быть злоумышленником, но у сетевого администратора существует множество других способов контролировать всех пользователей локальной сети, и вряд ли он будет следить за вами столь изощренным способом.

Ограничения использования снифферов

Другая причина, по которой снифферы **перестали** быть настолько **опасными**, как раньше, заключается в том, что в настоящее время наиболее важные данные передаются в **зашифрованном** виде.

Открытые, **незашифрованные** службы быстро **исчезают** из Интернета.

К примеру, при посещении web-сайтов все чаще используется протокол SSL (Secure Sockets Layer); вместо открытого FTP используется SFTP (Secure FTP).

А для других служб, которые не применяют шифрование по умолчанию, все чаще используются виртуальные частные сети (VPN).

Ограничения использования снифферов

Итак, те, кто беспокоится о возможности злонамеренного применения пакетных снифферов, должны иметь в виду следующее.

- Во-первых, чтобы представлять серьезную **угрозу** для вашей сети, снифферы должны находиться **внутри** самой сети.
- Во-вторых, сегодняшние стандарты **шифрования** чрезвычайно **затрудняют** процесс перехвата конфиденциальной информации.

Ограничения использования снифферов

Поэтому в настоящее время пакетные снифферы постепенно **утрачивают** свою **актуальность** в качестве инструментов хакеров.

В то же время остаются действенным и мощным средством для **диагностирования** сетей.

Более того, снифферы могут с успехом использоваться не только для **диагностики** и **локализации** сетевых проблем, но и для **аудита** сетевой безопасности.

Ограничения использования снифферов

В частности, применение пакетных анализаторов позволяет:

- обнаружить **несанкционированный трафик**,
- обнаружить и идентифицировать **несанкционированное** программное обеспечение,
- идентифицировать **неиспользуемые протоколы** для удаления их из сети,
- осуществлять генерацию трафика для **испытания на вторжение** (penetration test) с целью проверки системы защиты,
- работать с системами **обнаружения вторжений** (Intrusion Detection System, IDS).

Обзор программных пакетных снифферов

Обзор программных пакетных снифферов

Все программные снифферы можно условно разделить на две категории:

- снифферы, поддерживающие запуск из командной строки,
- снифферы, имеющие графический интерфейс.

При этом отметим, что существуют снифферы, которые **объединяют** в себе **обе эти возможности**.

Обзор программных пакетных снифферов

Кроме того, снифферы **отличаются** друг от друга:

- **протоколами**, которые они поддерживают,
- **глубиной анализа** перехваченных пакетов,
- возможностями по **настройке фильтров**,
- а также возможностью **совместимости** с другими программами.

Обзор программных пакетных снифферов

Обычно окно любого сниффера с графическим интерфейсом состоит их трех областей.

В первой из них отображаются итоговые данные перехваченных пакетов.

Обычно в этой области отображается минимум полей, а именно:

- **время** перехвата пакета;
- **IP-адреса** отправителя и получателя пакета;
- **MAC-адреса** отправителя и получателя пакета, исходные и целевые адреса портов;
- тип **протокола** (сетевой, транспортный или прикладного уровня);
- некоторая **суммарная информация** о перехваченных

Обзор программных пакетных снифферов

Во второй области выводится статистическая информация об отдельном выбранном пакете.

В третьей области пакет представлен в шестнадцатеричном виде или в символьной форме — ASCII.

Практически все пакетные снифферы позволяют производить **анализ** декодированных пакетов.

Именно поэтому пакетные снифферы также называют пакетными **анализаторами**, или протокольными **анализаторами**.

Сниффер распределяет перехваченные пакеты по уровням и протоколам.

Обзор программных пакетных снифферов

Некоторые анализаторы пакетов способны **распознавать** протокол и **отображать** перехваченную информацию.

Этот тип информации обычно отображается во второй области окна сниффера.

К примеру, любой сниффер способен распознавать протокол TCP, а продвинутые снифферы умеют определять, каким приложением порожден данный трафик.

Большинство анализаторов протоколов **распознают свыше 500 (пятиста) различных протоколов** и умеют описывать и декодировать их по именам.

Обзор программных пакетных снифферов

Чем **больше** информации в состоянии декодировать и представить на экране сниффер, тем **меньше** придется декодировать вручную.

Одна из проблем, с которой могут сталкиваться анализаторы пакетов, — невозможность корректной идентификации протокола, использующего порт, отличный от порта по умолчанию.

К примеру, с целью повышения безопасности некоторые известные приложения могут настраиваться на применение портов, отличных от портов по умолчанию.

Обзор программных пакетных снифферов

Так, вместо традиционного порта 80, зарезервированного для web-сервера, данный сервер можно принудительно перенастроить на порт 8088 или на любой другой.

Некоторые анализаторы пакетов в подобной ситуации **не способны корректно определить протокол** и отображают лишь информацию о протоколе нижнего уровня (TCP или UDP).

Существуют программные снифферы, к которым в качестве плагинов или встроенных модулей **прилагаются программные аналитические модули**, позволяющие **создавать отчеты** с полезной аналитической информацией о перехваченном трафике.

Обзор программных пакетных снифферов

Другая характерная черта большинства программных анализаторов пакетов — **возможность настройки** фильтров до и после захвата трафика.

Фильтры **выделяют из общего трафика** определенные пакеты по заданному критерию, что позволяет при анализе трафика избавиться от лишней информации.

Далее мы рассмотрим возможности нескольких доступных для скачивания снифферов, которые ориентированы на использование с платформами Windows.

Ethereal 0.10.14

Ethereal 0.10.14

Пакетный сниффер Ethereal 0.10.14 (эфириал, www.ethereal.com) является, пожалуй, **одним из лучших** и поистине легендарных некоммерческих (а значит, бесплатных) пакетных анализаторов.

Этот сниффер изначально был создан под Linux-платформы и основывался на базе утилиты Libpcap.

Впоследствии появилась Windows-версия сниффера Ethereal.

Она основывалась на базе утилиты WinPcap (Windows-версия Libpcap).

Ethereal 0.10.14

Утилита WinPcap (www.winpcap.org) представляет собой стандартный инструмент, посредством которого Windows-приложения могут непосредственно получать доступ к сетевому адаптеру (NIC-уровню) и перехватывать сетевые пакеты.

Кроме того, драйвер WinPcap имеет дополнительные функциональные возможности, заключающиеся в фильтрации пакетов, сборе сетевой статистики и поддержке возможности удаленного перехвата пакетов.

В состав утилиты WinPcap входит драйвер, обеспечивающий взаимодействие с NIC-уровнем, и библиотека, отвечающая за взаимодействие с интерфейсом API.

Ethereal 0.10.14

Сниффер Ethereal 0.10.14 поставляется в комплекте с утилитой WinPcap 3.1, однако с сайта www.winpcap.org можно скачать версию WinPcap 3.2 alpha 1.

Несмотря на то что графический интерфейс утилиты Ethereal 0.10.14 достаточно понятен, к программе прилагается очень подробный учебник (более 200 страниц).

Ethereal 0.10.14 — один из немногих снифферов, который поддерживает как графический интерфейс, так и запуск из командной строки.

Это удобно при составлении сценариев или активизации функций перехвата пакетов в случае возникновения в сети определенных событий.

Ethereal 0.10.14

Функциональные возможности пакета Ethereal 0.10.14 очень обширны и выходят далеко за рамки обычных возможностей других пакетных снифферов.

В пакете Ethereal 0.10.14 встречаются практически все функции, которые только могут быть у анализатора пакетов.

Программа может декодировать 752 протокола и поддерживает работу в Wi-Fi-сетях.

Графический интерфейс пакета Ethereal 0.10.14 вполне традиционен.

Ethereal 0.10.14

Интерфейс содержит три области:

- отображения перехваченных пакетов,
- отображения статистической информации о конкретном выбранном пакете,
- содержимого конкретного пакета.

Главное окно программы Ethereal 0.10.14 представлено на **рисунке 4**.

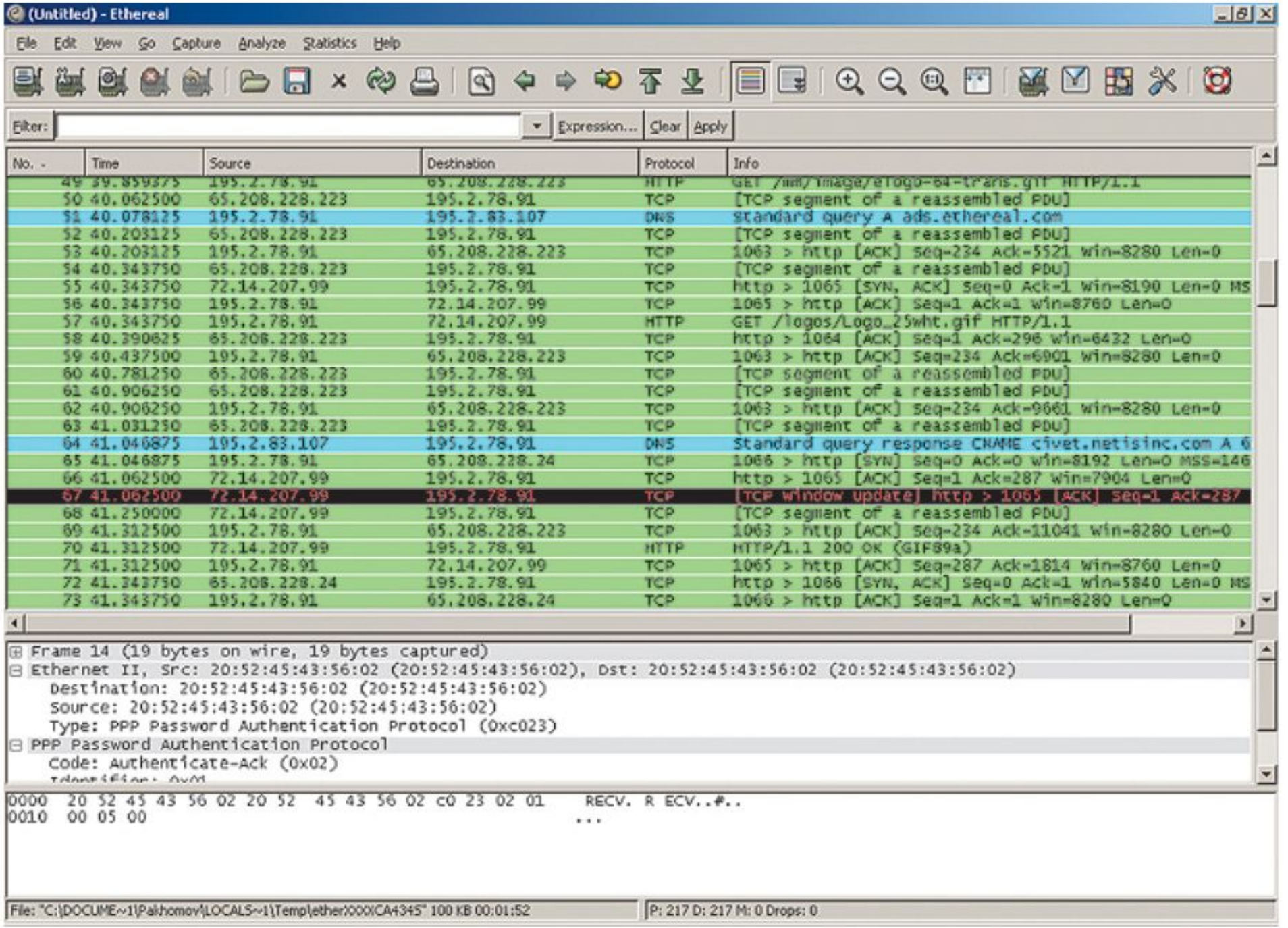

Рис. 4. Главное окно программы Ethereal 0.10.14

Ethereal 0.10.14

Графический интерфейс программы Ethereal облегчает создание пакетных фильтров как для файлов перехваченных пакетов (**фильтры отображения**), так и для «живого» перехвата (**фильтры перехвата**).

После изучения синтаксиса фильтров программы Ethereal можно создавать фильтры самостоятельно, присваивать им имена и сохранять их для последующего использования (рис. 5).

Программа Ethereal обладает довольно удобным интерфейсом для создания фильтров.

Достаточно нажать на кнопку **Add Expression**, чтобы создать фильтры в диалоговом окне **Filter Expression**.

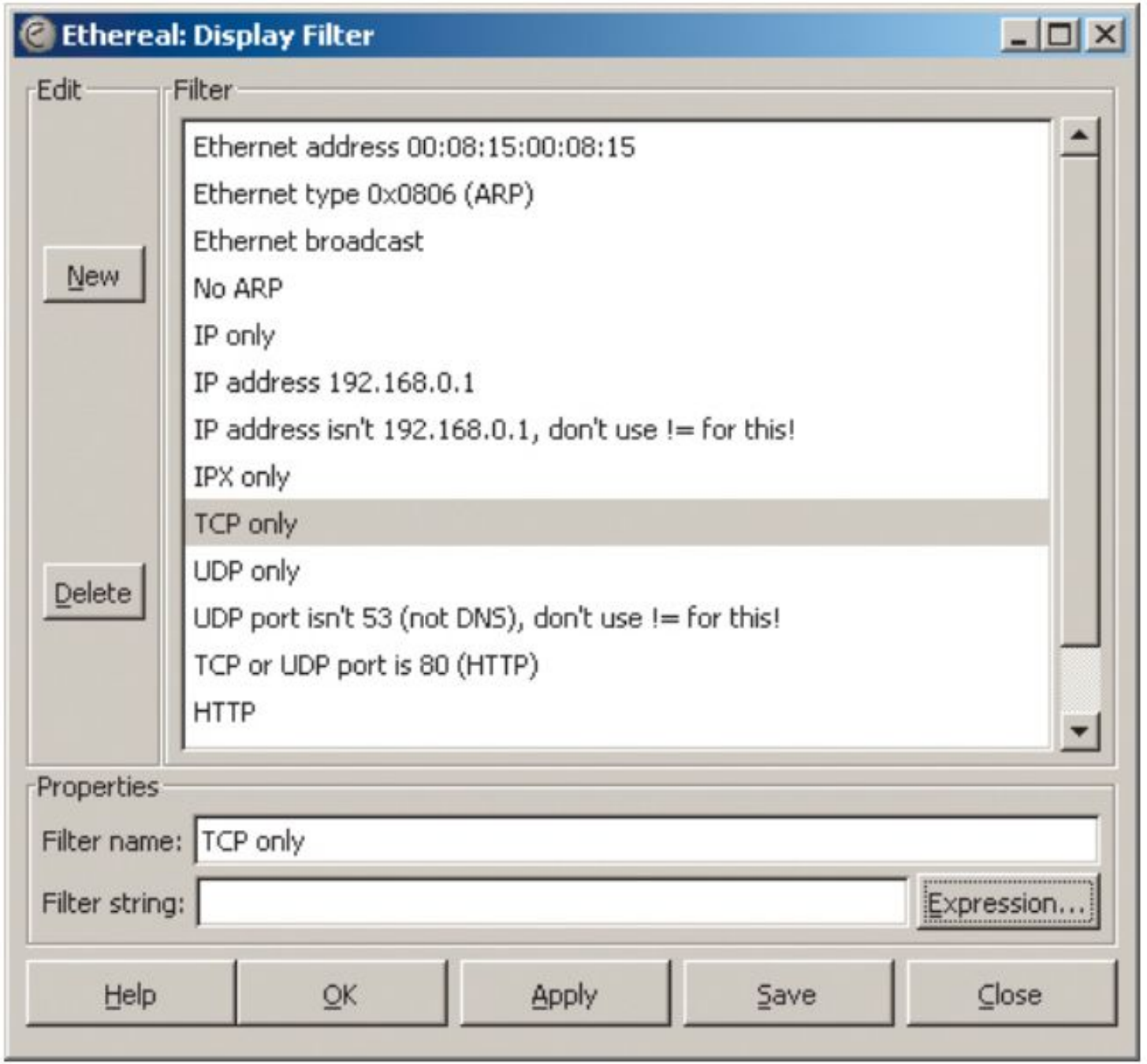

Рис. 5. Создание фильтра в программе Ethereal 0.10.14

Ethereal 0.10.14

Стоит отметить, что программа Ethereal **обладает** очень **гибкими возможностями** по созданию фильтров.

Программа способна осуществлять фильтрацию практически по любой характеристике пакета и по любому значению этой характеристики.

Кроме того, фильтры можно **комбинировать** друг с другом с использованием булевых операторов AND и OR.

Применение фильтров в анализаторе Ethereal позволяет легко выделить из общего потока перехваченной информации именно те или даже **тот единственный кадр**, который требуется.

Ethereal 0.10.14

Рассмотрим, к примеру, как найти при помощи фильтра **пакет с паролем** при подключении пользователя к Интернету через dial-up-соединение.

Прежде всего **запускаем** сниффер.

Это можно сделать из командной строки, причем удаленно и незаметно для пользователя.

Далее, **накапливаем** информацию до тех пор, пока пользователь не установит соединение с Интернетом.

Ethereal 0.10.14

Затем необходимо **настроить** фильтр, позволяющий найти нужный пакет.

Поскольку процесс аутентификации пользователя проходит по протоколу PPP PAP, необходимо **создать фильтр на выделение этого протокола**.

Для этого в строке выражения достаточно **указать** «pap» и **присвоить** имя новому фильтру (например, DialUp_Password) (рис. 6).

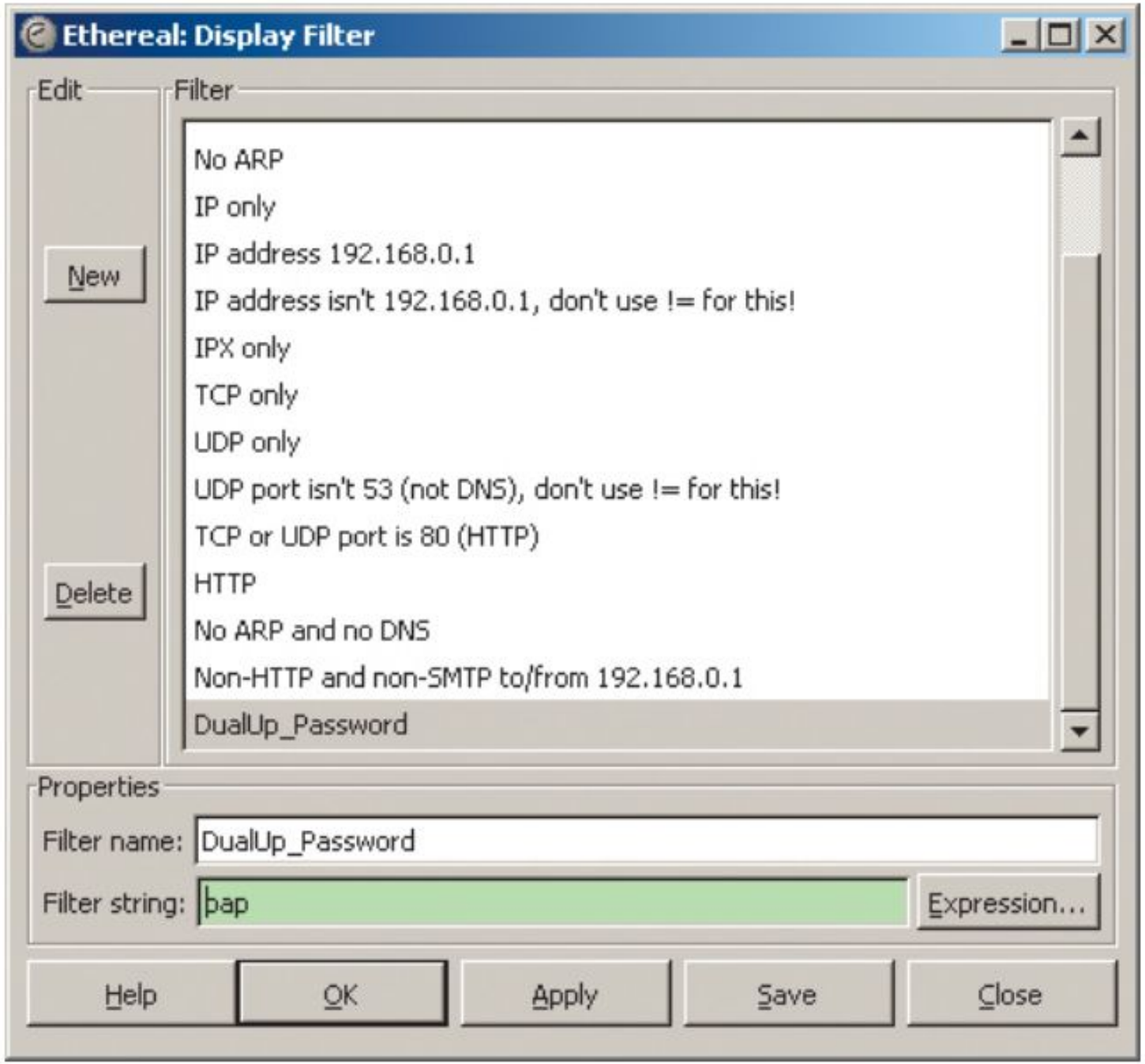

Рис. 6. Настройка фильтра для получения пакета с паролем

Ethereal 0.10.14

После применения фильтра из всей совокупности пакетов останутся **только два**:

пакет-запрос на аутентификацию (Authenticate-Request),

пакет подтверждения аутентификации (Authenticate-ACK).

Понятно, что **пароль содержится в первом пакете**, в чем несложно убедиться, просмотрев содержимое самого пакета (рис. 7).

Как правило, пароль передается провайдеру в **незашифрованном** виде.

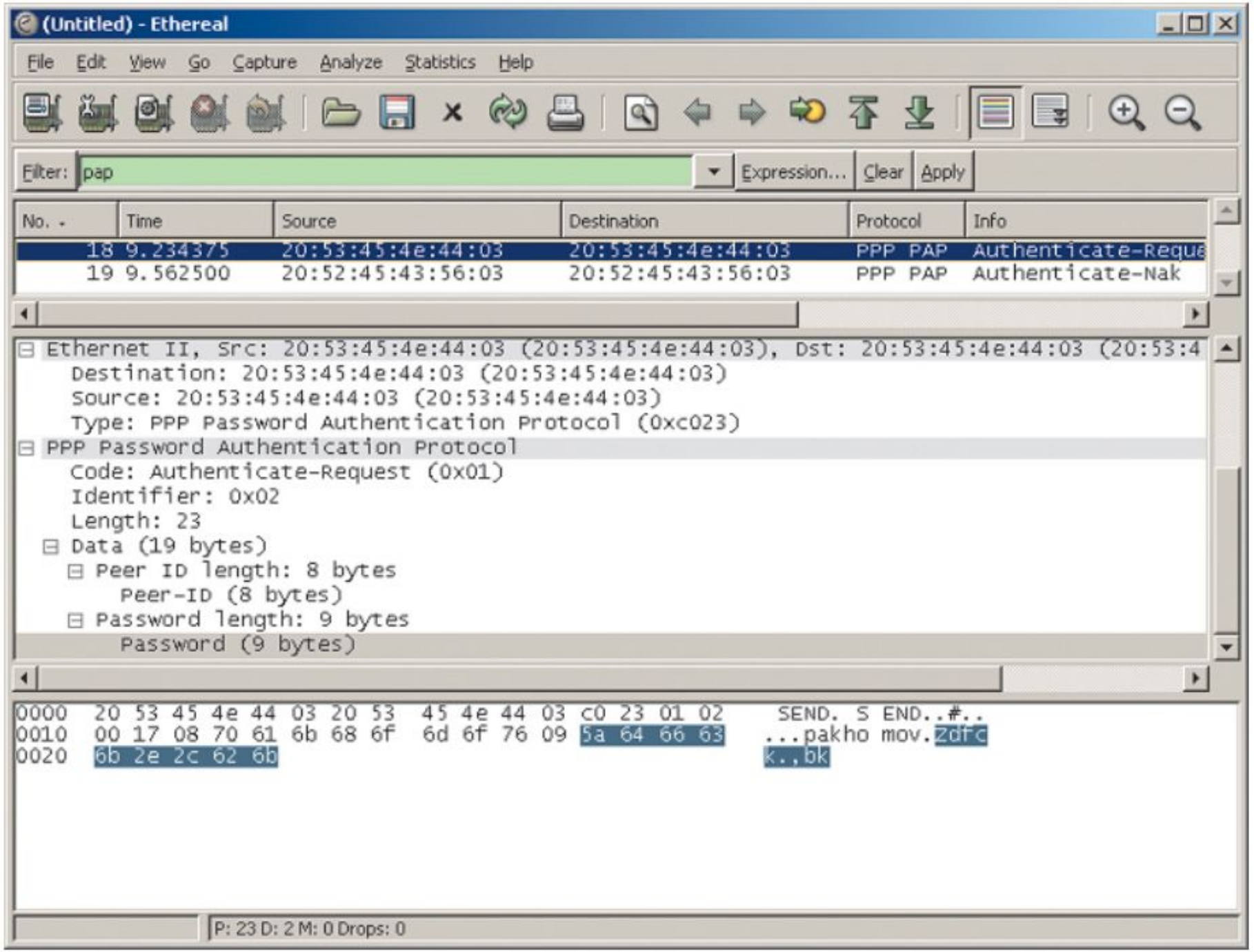

Рис. 7. Содержимое пакета

Ethereal 0.10.14

Еще один пример эффективного использования программы Ethereal 0.10.14 в мирных целях — это **точная настройка размера TCP-окна**.

Чтобы оптимальным образом **настроить** размер TCP-окна, необходимо запустить сниффер в процессе скачивания файла по сети и затем, настроив соответствующим образом фильтр, **просмотреть**:

- количество запросов на повторную передачу пакетов,
- количество пакетов-подтверждений,
- количество ошибочных пакетов.

Ethereal 0.10.14

Манипулируя с размером TCP-окна, можно добиться максимально возможной скорости передачи:

- снизив количество подтверждений при хорошем качестве связи,

- или уменьшив число запросов на повторную передачу, — при не очень хорошем качестве связи.

Ethereal 0.10.14

Помимо прекрасных возможностей по созданию разного рода фильтров, программа Ethereal позволяет выполнять всесторонний анализ трафика, представляя его:

- в графической форме,
- в форме статистического отчета.

К примеру, можно выполнить анализ TCP-трафика:

- по пропускной способности,
- по времени передачи туда и обратно,
- по номерам пакетов.

Ethereal 0.10.14

Результаты анализа представляются в виде графиков.

Так, анализ, использующий порядковые номера пакетов и время, **позволяет получить представление** о том, какой объем данных был послан в различные моменты времени, поскольку порядковые номера пакетов увеличиваются на размер пакета данных.

Ethereal 0.10.14

В целом можно сказать, что пакетный анализатор Ethereal 0.10.14 **является очень мощным** инструментальным средством диагностики сетей.

Конечно, для детального освоения пакета потребуется немало времени.

Однако если все-таки удастся преодолеть этот барьер и освоить пакет Ethereal, то необходимость освоения других аналогичных продуктов попросту отпадет.

Analyzer v.2.2

Analyzer v.2.2

Утилита Analyzer v.2.2 компании NetGroup — еще один небольшой по объему пакетный анализатор, распространяемый на бесплатной основе.

К достоинствам данной утилиты можно отнести то, что она не требует инсталляции на компьютер.

Единственное, что необходимо, — наличие установленной утилиты WinPcap, которая используется снифферером Analyzer v.2.2.

Кроме того, пакетный анализатор Analyzer v.2.2. очень прост в обращении и может быть рекомендован для начинающих пользователей.

Analyzer v.2.2

Недостатки этого анализатора вытекают из его достоинств — простота в обращении не позволяет производить глубокий анализ пакетов и создавать фильтры по любой характеристике пакета.

Утилита Analyzer v.2.2 поддерживает выбор интерфейса: сетевой адаптер или аналоговый модем.

Работа в беспроводных сетях не предусмотрена.

Графический интерфейс пакетного анализатора Analyzer v.2.2 содержит три традиционных окна (рис. 8).

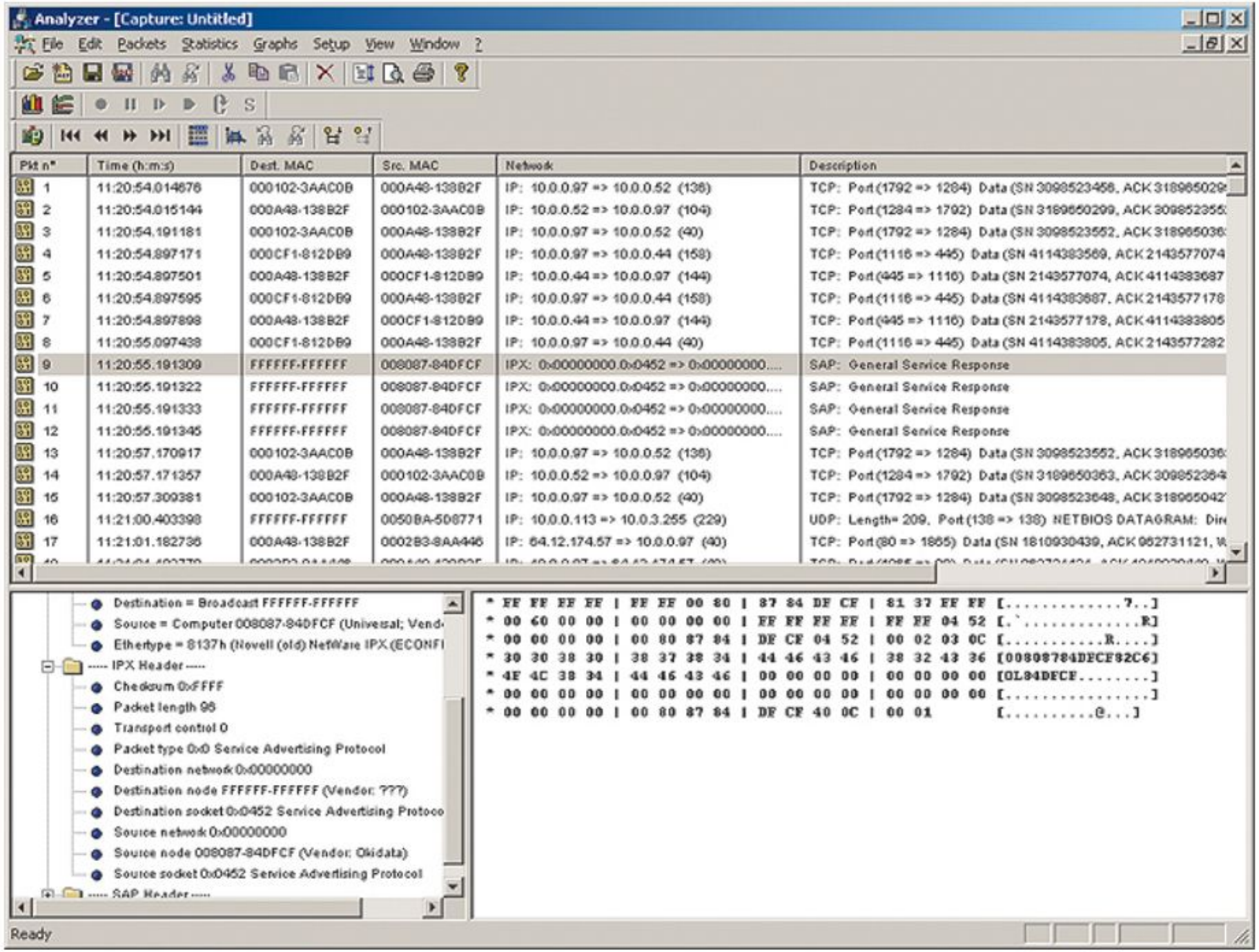

Рис. 8. Главное окно пакетного анализатора Analyzer v.2.2

Analyzer v.2.2

В первом окне отображаются перехваченные пакеты с информацией:

- о времени получения пакета,
- о MAC-адресах отправителя и получателя,
- о IP-адресах отправителя и получателя,
- о протоколе передачи,
- о портах источника и получателя пакетов,
- о размер TCP-окна,
- номер последовательности пакета,
- номер подтверждения этого пакета.

Analyzer v.2.2

Во втором окне выводится декодированная информация об отдельных полях пакета.

Третье окно отображает содержимое самого пакета.

Из недостатков данного пакета можно отметить невозможность использования фильтров после сбора информации.

Единственное, что можно сделать в данном случае, — это выделить по заданному фильтру пакеты.

Сами фильтры, как мы уже отмечали, не предоставляют гибкого механизма сбора требуемой информации (в сравнении с пакетом Ethereal).

Analyzer v.2.2

Для сравнения возможностей пакетов Analyzer v.2.2 и Ethereal 0.10.14 можно провести захват одного и того же трафика и проанализировали его сначала с помощью программы Ethereal 0.10.14, а затем — Analyzer v.2.2.

Как правило, информация, выдаваемая об отдельном пакете анализатором Ethereal 0.10.14, более подробная, чем та, что выдает анализатор Analyzer v.2.2.

Поэтому еще раз подчеркнем, что программа Analyzer v.2.2 представляет интерес только для начинающих пользователей и в качестве средства ознакомления с принципами функционирования сетей и структурами пакетов различных протоколов.

CommView 5.0

CommView 5.0

В отличие от всех рассмотренных выше анализаторов, программа CommView 5.0 (www.tamos.com) распространяется на коммерческой основе и для свободного скачивания доступна лишь ее демонстрационная версия с урезанной функциональностью.

Данный пакетный анализатор предназначен для мониторинга локальной сети и соединения с Интернетом.

Он способен:

- захватывать пакеты, проходящие через сетевой адаптер или модем,
- декодировать пакеты,
- представлять достаточно подробную информацию в удобном для восприятия виде.

CommView 5.0

В отличие от большинства снифферов, программа CommView 5.0 не требует предварительной установки на ПК WinPcap.

Сниффер CommView 5.0 поддерживает операционные системы Windows 98/Me/NT/2000/XP/2003 и Windows XP 64-bit Edition.

Перечень поддерживаемых протоколов довольно обширен.

В этом плане можно рассчитывать на предоставление достаточно подробной информации о перехваченных пакетах.

Пакетный анализатор CommView 5.0 поддерживает возможность создания гибко настраиваемых фильтров (правил).

CommView 5.0

Однако **недостатком** здесь является то, что эти фильтры нельзя применить к уже имеющимся собранным пакетам.

Создаваемые правила распространяются только на захват пакетов.

Графический интерфейс программы CommView 5.0 традиционен — три окна:

- в первом из которых отображаются захваченные пакеты,
- во втором — декодированная информация об отдельном пакете,
- а в третьем — содержимое самого пакета (рис. 9).

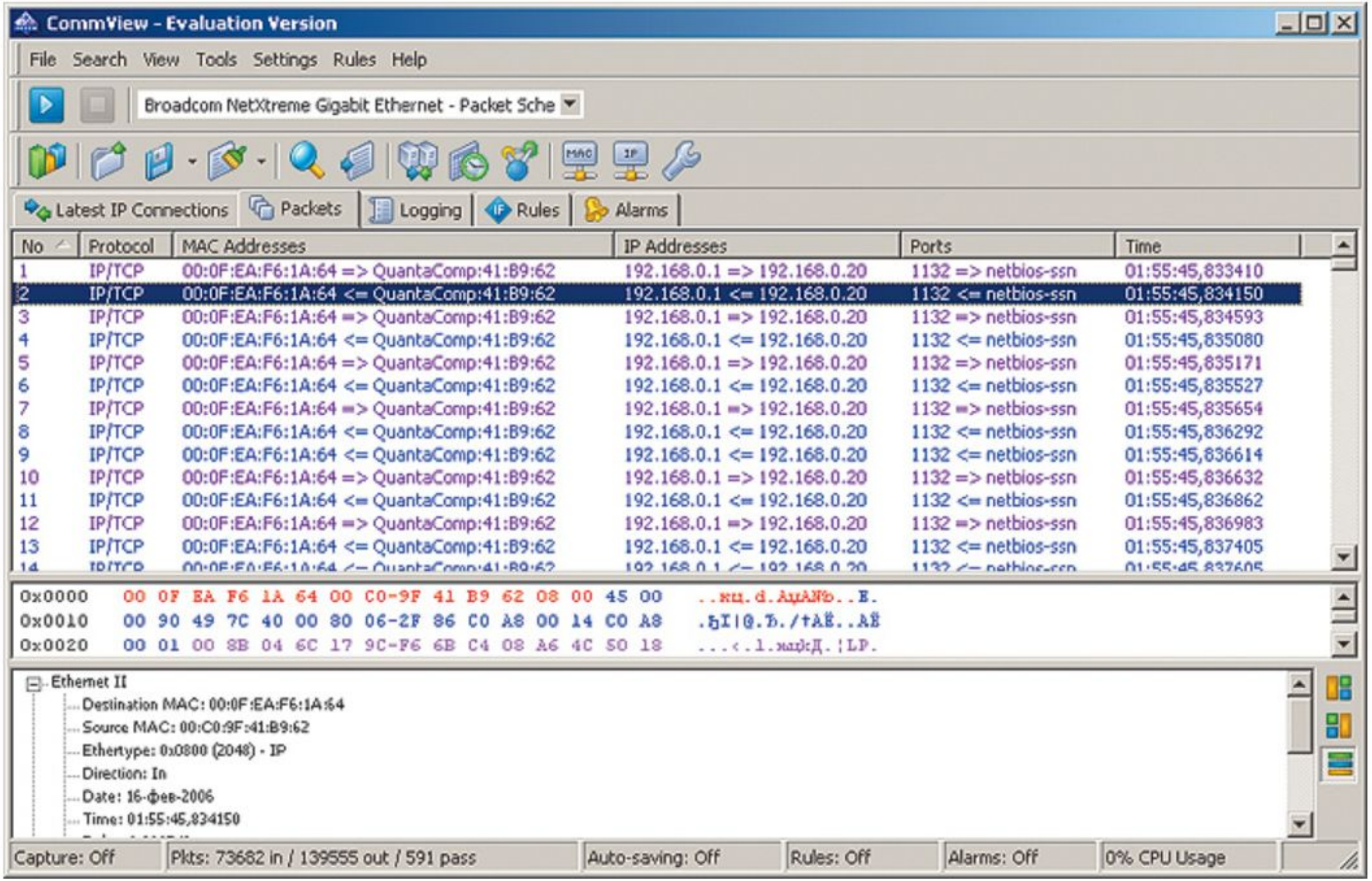

Рис. 9. Главное окно пакетного анализатора CommView 5.0

CommView 5.0

Информация в окне с захваченными пакетами довольно скудная.

Отображаются лишь:

- тип протокола,
- IP- и MAC-адреса источника и получателя пакета,
- время и порт назначения и отправления.

Окно с декодированной информацией об отдельном пакете значительно более информативно и по детализации предоставляемой информации не уступает анализатору Ethereal (во всяком случае это касается протокола TCP).

CommView 5.0

К **достоинствам** анализатора CommView 5.0 можно отнести:

- возможность просмотра подробной статистической информации о сеансе перехвата, которая представляется в отдельном окне в удобном графическом виде (рис. 10),
- а также составление отчета в отдельном файле.

Еще одним отличием анализатора CommView 5.0 является возможность настройки сигнала тревоги по предопределенным событиям.

В частности, можно задать правила, при выполнении которых будет послано оповещение по электронной почте.

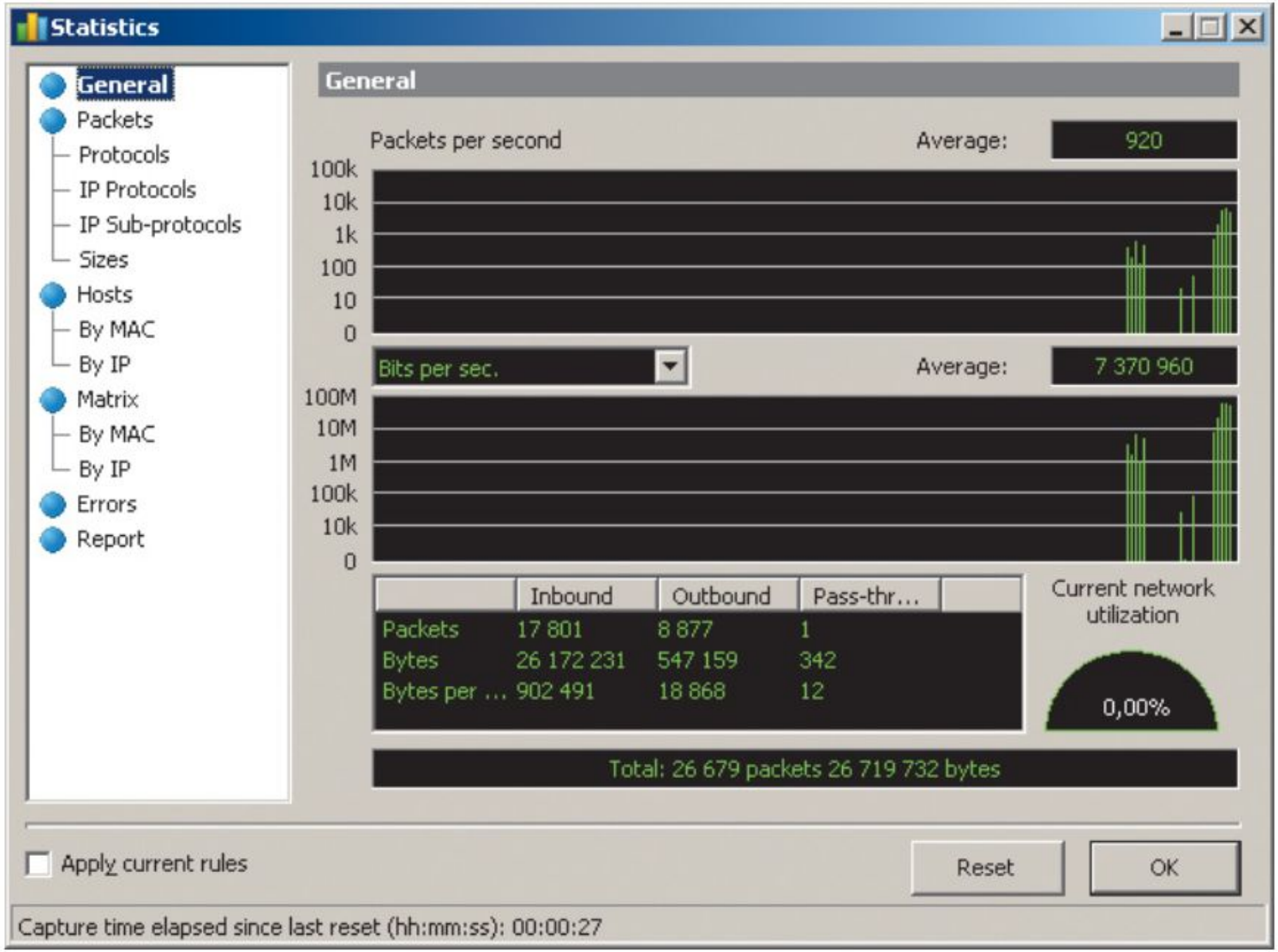

Рис. 10. Статистическая информация о сеансе перехвата в программе CommView 5.0

CommView 5.0

Кроме того, сниффер CommView 5.0 позволяет заменять IP- и MAC-адреса сетевого адаптера на имена пользователей.

Это значительно упрощает мониторинг сети.

С целью диагностики сети данный сниффер имеет встроенный генератор трафика с возможностью настройки размера передаваемого пакета и скорости генерации пакетов.

CommView 5.0

И наконец, последняя особенность снифферa CommView 5.0 — возможность создания удаленного агента, что позволяет производить удаленный мониторинг сети.

Для реализации данной функции на удаленном ПК необходимо инсталлировать программу Remote Agent.

А используя консоль CommView 5.0, можно устанавливать соединение с компьютером, на котором инсталлирована утилита Remote Agent.

Iris Network Traffic Analyzer4.07

Iris Network Traffic Analyzer4.07

Пакетный анализатор Iris 4.07 (www.eeye.com) от компании eEye digital Security представляет собой мощное инструментальное средство для диагностики локальных сетей и каналов связи с Интернетом.

Программа Iris 4.07 распространяется на коммерческой основе, однако на сайте производителя доступна ее ознакомительная версия.

Несмотря на заявленную в документации поддержку только операционных систем Windows 95/98/NT/2000, реально этот список можно расширить, и, скорее всего, данная программа способна работать с любой операционной системой семейства Windows.

Iris Network Traffic Analyzer4.07

Графический интерфейс программы (рис. 11) интуитивно понятен, прост и традиционен для пакетных снифферов.

Имеется три окна.

В первом из которых отображаются перехваченные пакеты с достаточно подробной информацией о каждом пакете, включающей:

- MAC- и IP-адреса источника и отправителя пакетов,
- тип пакета,
- протокол,
- порт отправления и назначения,
- размер пакета,
- а также порядковые номера SEQ и ACK.

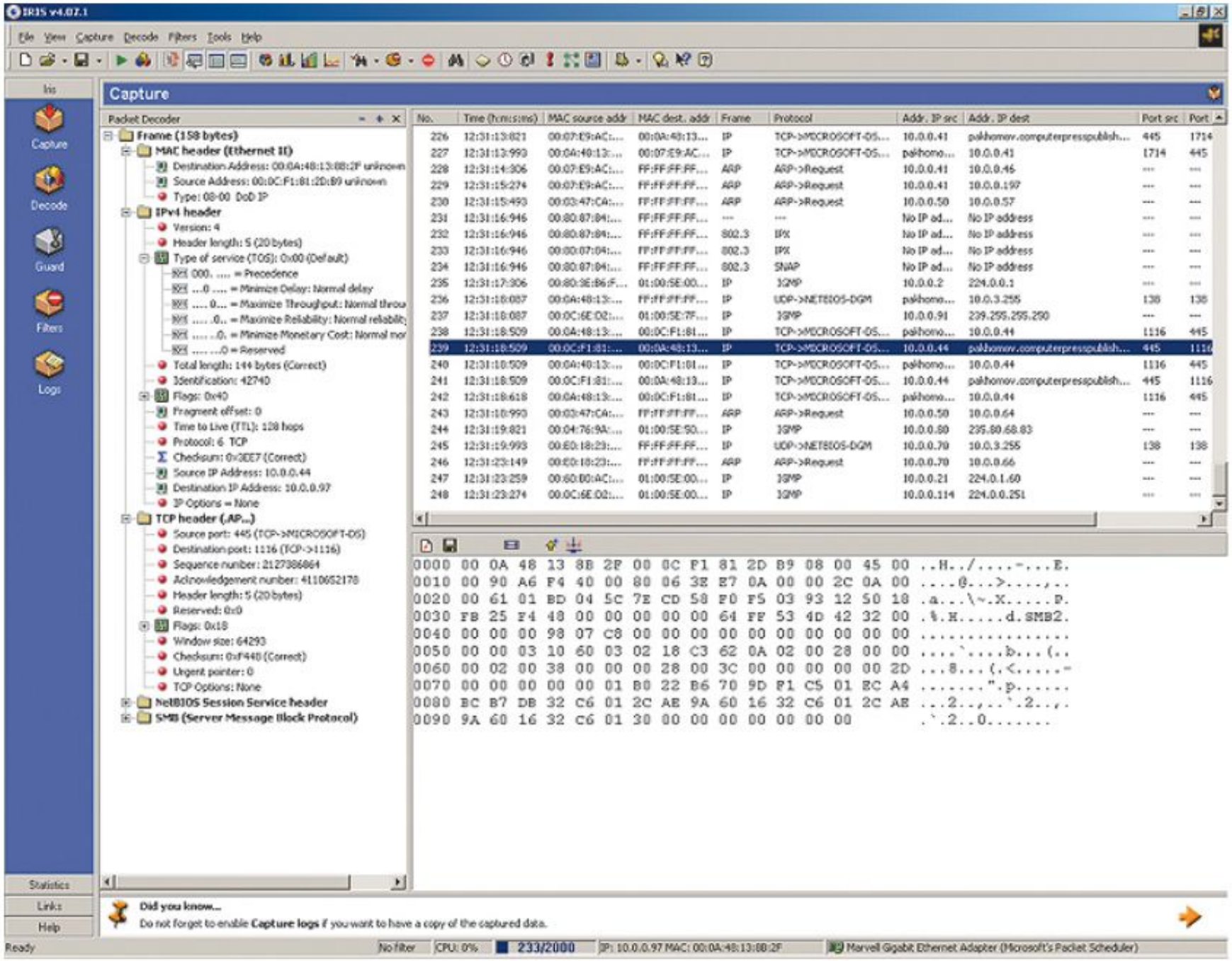

Рис. 11. Главное окно пакетного анализатора Iris 4.07

Iris Network Traffic Analyzer4.07

Подробная декодированная информация о каждом отдельном пакете доступна **во втором** окне.

Содержимое каждого пакета отображено **в третьем** окне.

Нужно отметить, что по степени детализации предоставляемой информации данный пакет не уступает анализатору Ethereal.

Пожалуй, единственный **недостаток** данного анализатора заключается в том, что отображаемые в первом окне пакеты **не маркируются цветом**, как это делается в других анализаторах.

Это создает определенное неудобство при визуальном восприятии информации.

Iris Network Traffic Analyzer4.07

Пакетный анализатор Iris 4.07 позволяет очень гибко и в то же время просто настраивать фильтры для захвата пакетов.

Так, используя диалоговое окно (рис. 12) Edit filter settings, можно создавать фильтры по MAC-адресам источника и получателя, по IP-адресам источника и получателя, по портам, протоколам, а также по вхождению в содержимое пакета определенного слова.

Кроме того, можно настраивать фильтры на размер пакета и на фрагмент пакета в HEX-формате.

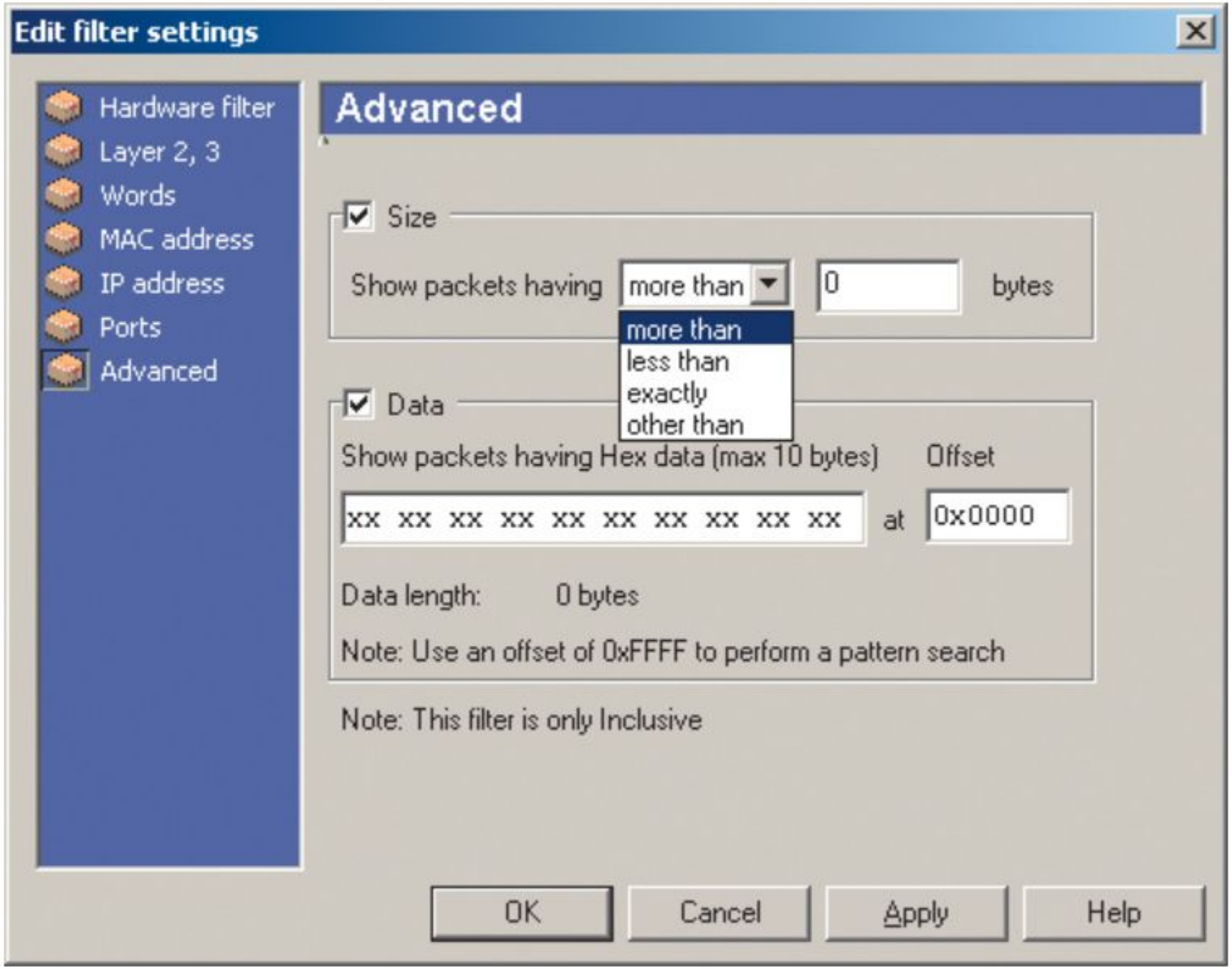

Рис. 12. Настройка пакетного фильтра в анализаторе Iris 4.07

Iris Network Traffic Analyzer4.07

Отметим, что **недостатком** программы Iris 4.07 является то, что фильтры можно создавать только для вновь принимаемых пакетов, а реализовать фильтрацию уже перехваченных пакетов не представляется возможным.

Вместо этого в программе предусмотрен поиск нужных пакетов по фильтру.

Другим отличием программы Iris 4.07 является возможность отображения в графической форме статистической информации во время запуска режима захвата пакетов.

Так, имеется возможность отображать график скорости передачи пакетов (рис. 13).

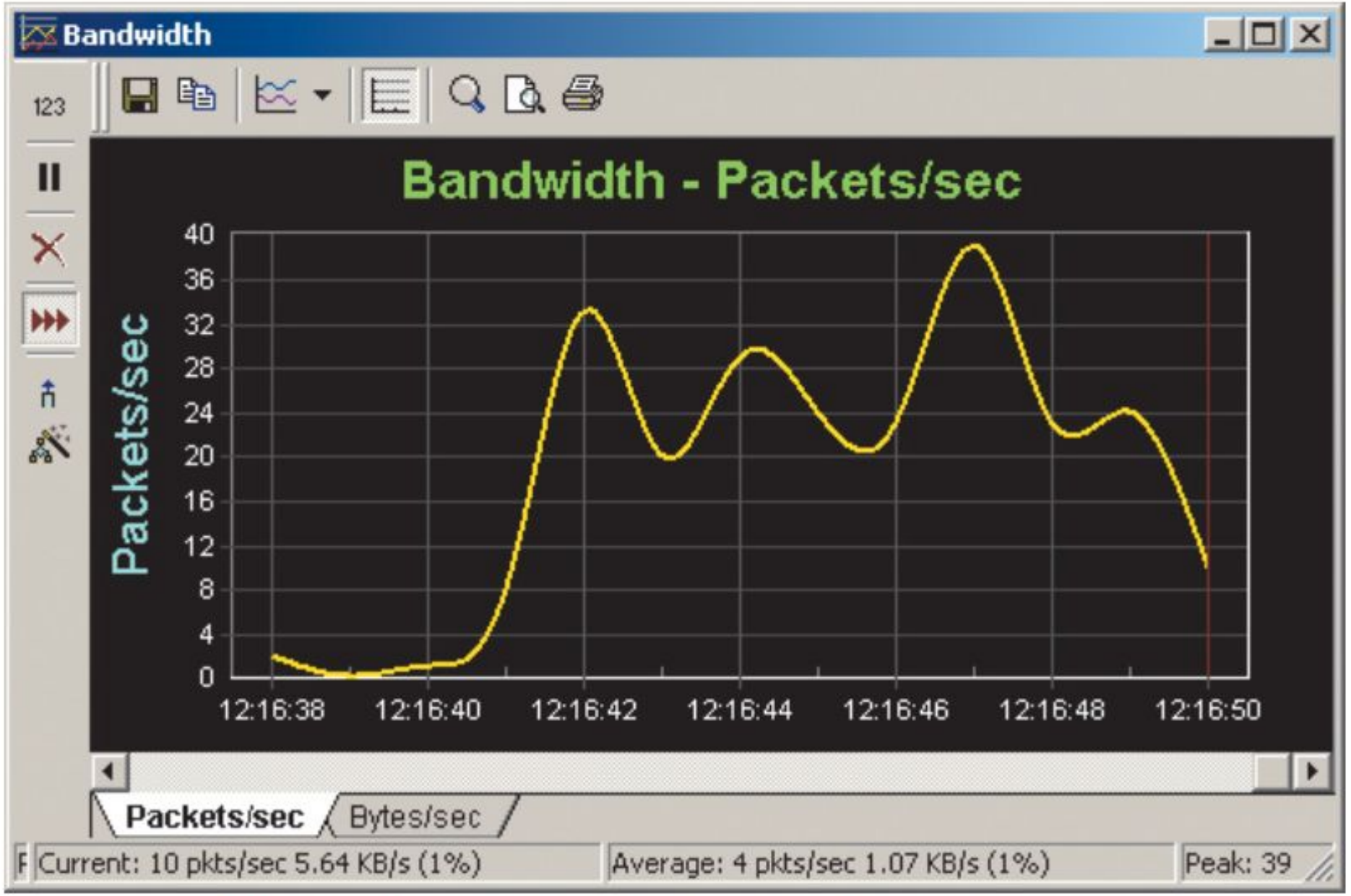

Рис. 13. График скорости передачи пакетов в анализаторе Iris 4.07

Iris Network Traffic Analyzer4.07

Также, имеется возможность отображать диаграмму распределения размеров пакетов (рис. 14) и многое другое.

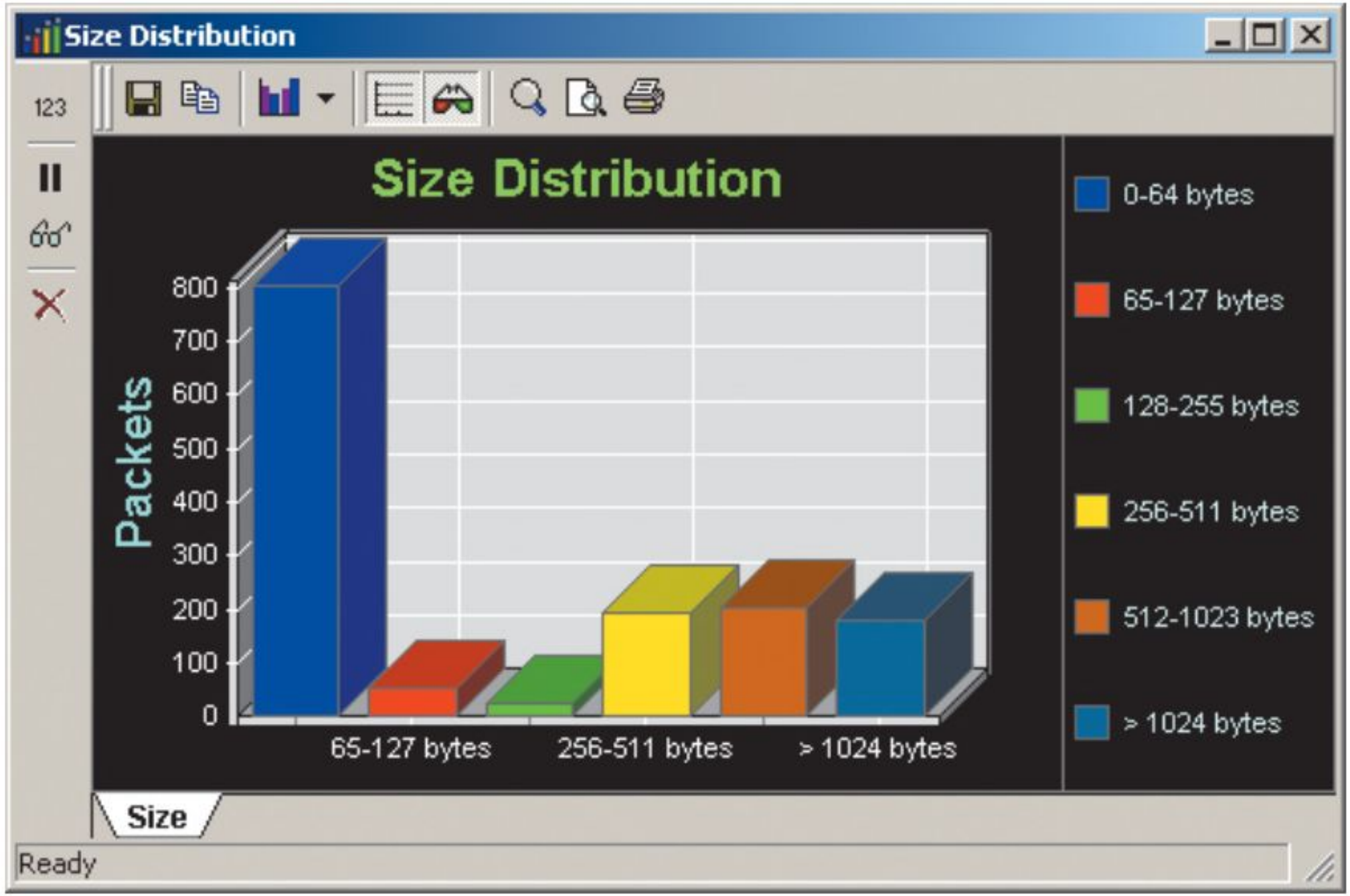

Рис. 14. Диаграмма распределения размеров пакетов в анализаторе Iris 4.07

Iris Network Traffic Analyzer4.07

Помимо перечисленных возможностей анализатор пакетов Iris 4.07 позволяет создавать HTML-отчеты о сеансе связи, куда включается наиболее важная информация, в том числе статистика о посещении сайтов, объеме переданного и принятого трафика и многое другое.

Также программа Iris 4.07 имеет встроенный генератор трафика, что удобно для диагностики узких мест в сети.

Еще одной особенностью программы Iris 4.07 является наличие встроенного модуля, позволяющего фиксировать все попытки соединения с компьютером, что обеспечивает отслеживание попыток несанкционированного проникновения в сеть.

Методы перехвата сетевого трафика

Методы перехвата сетевого трафика

Прослушивание сети с помощью программ сетевых анализаторов, является первым, самым простым способом перехвата данных.

Для защиты от прослушивания сети применяются специальные программы, например, AntiSniff (http://www.securitysoftwaretech.com/antisniff), которые способны выявлять в сети компьютеры, занятые прослушиванием сетевого трафика.

Программы-антисниферы для решения своих задач используют особый признак наличия в сети прослушивающих устройств - сетевая плата компьютера-снифера должна находиться в специальном режиме прослушивания.

Методы перехвата сетевого трафика

Находясь в режиме **прослушивания**, сетевые компьютеры особенным образом **реагируют** на IP-дейтаграммы, посылаемые в адрес тестируемого хоста.

Например, прослушивающие хосты, как правило, обрабатывают **весь поступающий трафик**.

Они не ограничиваются только посланными на адрес хоста дейтаграммами.

Имеются и другие признаки, указывающие на подозрительное поведение хоста, которые способна распознать программа AntiSniff.

Методы перехвата сетевого трафика

Прослушивание позволяет получить множество полезной информации:

- передаваемые по сети пароли,
- адреса компьютеров сети,
- конфиденциальные данные,
- письма,
- прочее.

Методы перехвата сетевого трафика

Несомненно, прослушивание по сети очень полезно с точки зрения злоумышленника.

Однако простое прослушивание не позволяет хакеру вмешиваться в сетевое взаимодействие между двумя хостами с целью модификации и искажения данных.

Для решения такой задачи требуется более сложная технология.

Ложные запросы arp

Ложные запросы arp

Чтобы **перехватить** и замкнуть на себя процесс сетевого взаимодействия между двумя хостами A и B злоумышленник может **подменить** IP-адреса взаимодействующих хостов своим IP-адресом.

При этом хостам A и B направляются фальсифицированные сообщения ARP.

(Address Resolution Protocol - Протокол разрешения адресов).

Посмотрим, как хакер может воспользоваться протоколом ARP для выполнения перехвата сетевого взаимодействия между хостами A и B.

Ложные запросы arp

Для перехвата сетевого трафика между хостами A и B хакер **навязывает** этим хостам свой IP-адрес.

Это нужно чтобы хосты A и B использовали этот фальсифицированный IP-адрес при обмене сообщениями.

Для навязывания своего IP-адреса хакер выполняет следующие операции.

- Злоумышленник определяет MAC-адреса хостов A и B.

Это можно сделать, например, с помощью команды **nbtstat** из пакета **W2RK**.

Ложные запросы arp

- Злоумышленник отправляет на выявленные MAC-адреса хостов A и B определённые сообщения.

Эти сообщения представляют собой фальсифицированные ARP-ответы на запросы разрешения IP-адресов хостов в MAC-адреса компьютеров.

Хосту A сообщается, что IP-адресу хоста B соответствует MAC-адрес компьютера злоумышленника.

Хосту B сообщается, что IP-адресу хоста A также соответствует MAC-адрес компьютера злоумышленника.

Ложные запросы arp

- Хосты A и B заносят полученные MAC-адреса в свои кэши ARP и далее используют их для отправки сообщений друг другу.

Поскольку IP-адресам A и B соответствует MAC-адрес компьютера злоумышленника, хосты A и B, ничего не подозревая, общаются через посредника.

Посредник, при этом, способен делать с их посланиями всё что угодно.

Для защиты от таких атак сетевые администраторы должны поддерживать базу данных с таблицей соответствия MAC-адресов и IP-адресов своих сетевых компьютеров.

Ложные запросы arp

В сетях UNIX такого рода атаку ложными запросами ARP можно реализовать с помощью системных утилит отслеживания и управления сетевым трафиком, например, **arpredirect**.

К сожалению, в сетях Windows 2000/XP такие надежные утилиты, по-видимому, не реализованы.

Например, на сайте NTsecurity (http://www.ntsecurity.nu) можно загрузить утилиту GrabitAll, представленную как средство для перенаправления трафика между сетевыми хостами.

Однако элементарная проверка работоспособности утилиты GrabitAll показывает, что до полного успеха в реализации ее функций еще далеко.

Ложная маршрутизация

Ложная маршрутизация

Чтобы перехватить сетевой трафик, злоумышленник может подменить реальный IP-адрес сетевого маршрутизатора своим IP-адресом.

Это можно сделать, например, с помощью фальсифицированных ICMP-сообщений **Redirect**.

Полученное сообщение Redirect хост А должен, согласно документу RFC-1122, воспринять как ответ на дейтаграмму, посланную другому хосту, например, В.

Свои действия на сообщение Redirect хост А определяет, исходя из содержимого полученного сообщения Redirect.

Ложная маршрутизация

Если в Redirect задать перенаправление дейтаграмм из A в B по новому маршруту, то именно это хост A и сделает.

Для выполнения ложной маршрутизации злоумышленник должен знать некоторые подробности об организации локальной сети, в которой находится хост A.

В частности, ему нужно знать IP-адрес маршрутизатора, через который отправляется трафик из хоста A в B.

Зная это, злоумышленник сформирует IP-дейтаграмму, в которой IP-адрес отправителя определен как IP-адрес маршрутизатора.

При этом получателем будет указан хост A.

Ложная маршрутизация

Также в дейтаграмму включается сообщение ICMP Redirect с полем адреса нового маршрутизатора, установленным как IP-адрес компьютера злоумышленника.

Получив такое сообщение, хост А будет отправлять все сообщения по IP-адресу компьютера злоумышленника.

Для защиты от такой атаки следует отключить на хосте А обработку сообщений ICMP Redirect.

Это можно сделать, например, с помощью брандмауэра.

А выявить IP-адрес компьютера злоумышленника может команда **tracert**.

В Unix это команда называется **tracerout**.

Ложная маршрутизация

Эти утилиты способны **найти** появившийся в локальной сети дополнительный, непредусмотренный при инсталляции, маршрут.

Конечно, это возможно, если администратор сети проявит соответствующую бдительность.

Приведенные выше примеры перехватов, которыми возможности злоумышленников далеко не ограничиваются, убеждают в необходимости защиты данных, передаваемых по сети.

Это особенно важно, если в данных содержится конфиденциальная информация.

Ложная маршрутизация

Единственным методом защиты от перехватов сетевого трафика является использование программ:

- реализующих криптографические алгоритмы,
- реализующих криптографические протоколы шифрования,
- позволяющих предотвратить раскрытие секретной информации,
- позволяющих предотвратить подмену секретной информации.

Ложная маршрутизация

Для решения таких задач криптография предоставляет средства для:

- шифрования,
- подписи,
- проверки подлинности передаваемых по защищенным протоколам сообщений.

Практическую реализацию всех криптографических методов защиты обмена информацией предоставляют сети VPN.

(Virtual Private Network - Виртуальные частные сети).

Перехват tcp-соединения

Перехват tcp-соединения

Наиболее изощренной атакой перехвата сетевого трафика следует считать захват TCP-соединения (TCP-hijacking, «хайджекин»).

Это происходит, когда хакер путем генерации и отсылки на атакуемых хост TCP-пакетов прерывает текущий сеанс связи с хостом.

Далее, пользуясь возможностями протокола TCP по восстановлению прерванного TCP-соединения, хакер перехватывает прерванный сеанс связи и продолжает его вместо отключенного клиента.

Перехват tcp-соединения

Для выполнения атак перехвата TCP-соединения создано несколько эффективных утилит.

Однако все они реализованы для платформы Unix.

На сайтах Web эти утилиты представлены только в виде исходных кодов.

Таким образом, от атак методом перехвата TCP-соединения проку не много.

Протокол TCP (Transmission Control Protocol - Протокол управления передачей) является одним из базовых протоколов транспортного уровня OSI.

Перехват tcp-соединения

Он позволяет устанавливать логические соединения по виртуальному каналу связи.

По этому каналу передаются и принимаются пакеты с регистрацией их последовательности, осуществляется управление потоком пакетов, организовывается повторная передача искаженных пакетов, а в конце сеанса канал связи разрывается.

Протокол TCP является единственным базовым протоколом из семейства TCP/IP, имеющим продвинутую систему идентификации сообщений и соединения.

Список литературы:

1. Компьютерные сети. Н.В. Максимов, И.И. Попов, 4-е издание, переработанное и дополненное, «Форум», Москва, 2015.
2. Компьютерные сети. Принципы, технологии, протоколы, В. Олифер, Н. Олифер (5-е издание), «Питер», Москва, Санк-Петербург, 2016.
3. Компьютерные сети. Э. Таненбаум, 4-е издание, «Питер», Москва, Санк-Петербург, 2003.
4. Построение сетей на базе коммутаторов и маршрутизаторов / Н.Н. Васин, Национальный Открытый Университет «ИНТУИТ», 2016.
5. Компьютерные сети : учебное пособие / А.В. Кузин, 3-е издание, издательство «Форум», Москва, 2017.
6. https://compress.ru/article.aspx?id=16244
7. https://studfile.net/preview/6449371/
8. https://www.sibsutis.ru/upload/8ea/%D0%A8%D0%B0%D0%BD%D1%8B%D0%B3%D0%B8%D0%BD%20%D0%95.%D0%90..pdf

Благодарю за внимание!

Преподаватель: Солодухин Андрей Геннадьевич

Электронная почта: asoloduhin@kait20.ru