Санкт-Петербург, ул. Седова, 80, телефон (812) 449-0770, факс (812) 449-0771, E-mail: info@bilim.com

Анализатор протоколов Ethereal

Николай Малых
nmalykh@bilim.com

Предисловие

Приведенное здесь описание не является переводом пользовательской документации для программы Ethereal, хотя в нем используются фрагменты такого перевода. Документ описывает возможности программы на уровне версии 0.9.16. данный документ является частью курса "Системы безопасности на открытых платформах", подготовленного автором и читаемого в Network Training Center[1].

http://www.ethereal.com

Ethereal представляет собой анализатор сетевых протоколов с графическим интерфейсом (GUI). Программа позволяет просматривать и анализировать пакеты, полученные из сетевого интерфейса или ранее собранного файла. В Ethereal по умолчанию используется для файлов захвата формат libpcap, используемый программой tcpdump и другими анализаторами. Кроме того, Ethereal может читать файлы в форматах snoop и atmsnoop, Shomiti/Finisar Surveyor, Novell LANalyzer, Network General/Network Associates Sniffer[2] (DOS-версии), Microsoft Network Monitor, AIX iptrace, Cinco Networks NetXRay, Network Associates Sniffer (Windows-версии), AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek, RADCOM WAN/LAN, Lucent/Ascend router debug, HP-UX nettl, Toshiba ISDN router dump, ISDN4BSD, Cisco Secure IDS IPLog, pppd (формат pppdump), VMS TCPIPtrace/TCPtrace/UCX$TRACE, DBS Etherwatch VMS (текстовый формат, Visual Networks Visual UpTime, CoSine L2, Accellent 5Views LAN agent, Endace Measurement Systems ERF, Linux Bluez Bluetooth, Network Instruments Observer v9. Программе даже не нужно указывать тип исходного файла, она распознает форматы автоматически. Ethereal может также читать файлы перечисленных выше форматов, сжатые с использованием gzip. Получить более подробную информацию о поддерживаемых программой форматах и других возможностях Ethereal можно из руководства пользователя, доступного на сайте.

Подобно другим анализаторам протоколов окно Ethereal включает 3 области просмотра с разными уровнями детализации (см. рисунок 1). Верхнее окно содержит список собранных пакетов с кратким описанием, в среднем окне показывается дерево протоколов, инкапсулированных в кадр. Ветви дерево могут быть раскрыты для повышения уровня детализации выбранного протокола. Последнее окно содержит дамп пакета в шестнадцатеричном и текстовом представлении.

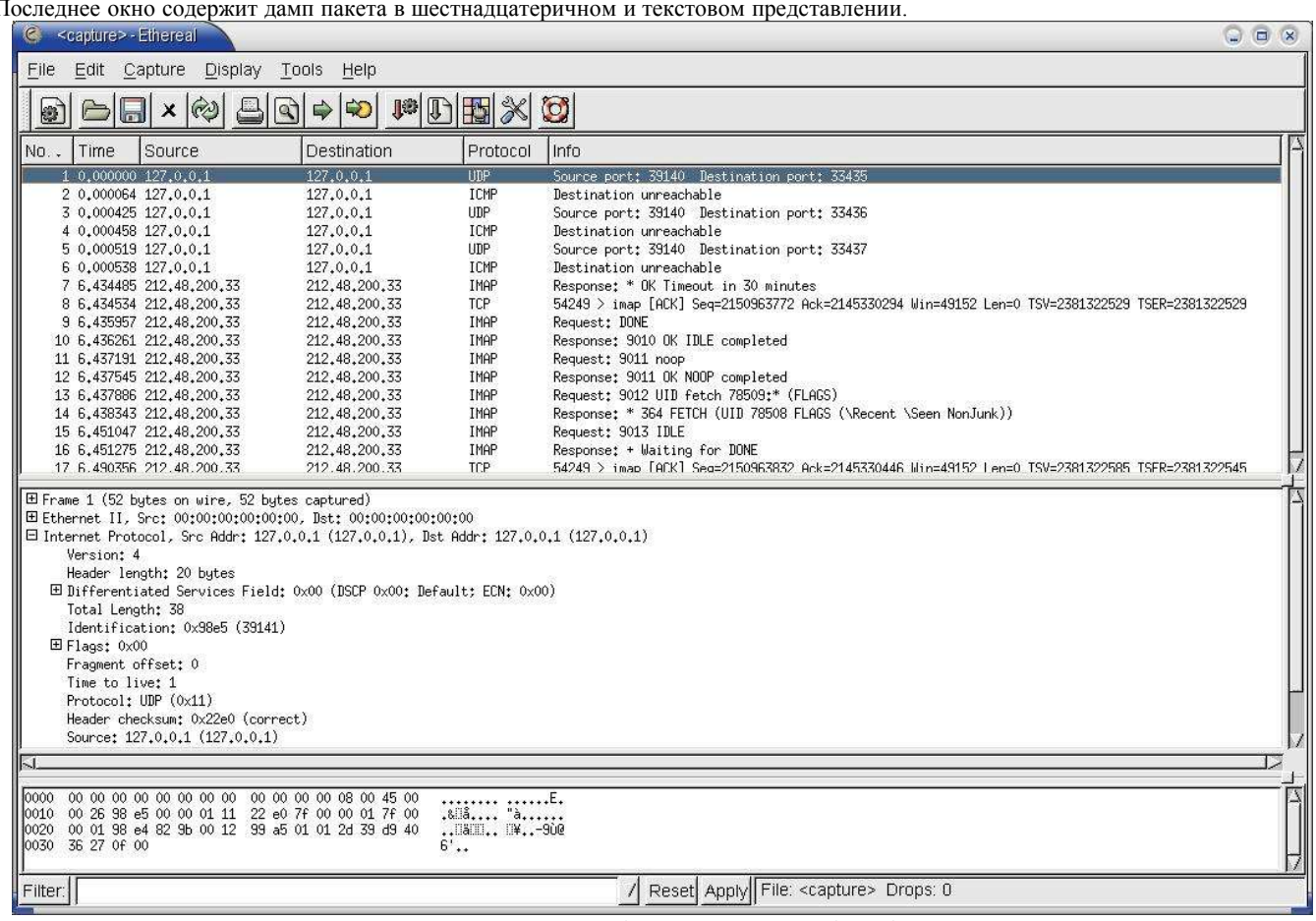

Рисунок 1 Интерфейс программы Ethereal

Программа Ethereal предоставляет пользователю ряд уникальных возможностей, не поддерживаемых другими анализаторами протоколов. Программа обеспечивает возможность сбора всех пакетов заданного соединения TCP и представления данных в удобном для просмотра формате (ASCII, EBCDIC или шестнадцатеричный). При выводе пакетов можно использовать мощную систему фильтрации Ethereal, отбирающую пакеты по большему, нежели в других анализаторах, числу полей.

[1] Информацию о данном курсе вы найдете на сайте http://www2.bilim.com/products/courses/OSSS-course.shtml.
[2] В сжатом и несжатом формате

Сбор пакетов осуществляется с использованием библиотеки pcap, входящей во все дистрибутивы UNIX[3]. Синтаксис фильтров сбора пакетов соответствует правилам, используемым библиотекой pcap[4] и программой tcpdump.

Для поддержки анализа данных из сжатых файлов требуется библиотека zlib. Отсутствие этой библиотеки не мешает компиляции Ethereal, но в этом случае работа со сжатыми файлами не поддерживается.

Опции Ethereal

Большинство пользователей запускает графический интерфейс Ethereal без каких-либо опций, однако приведенная в этом параграфе информация позволяет более эффективно использовать возможности программы за счет выбора режима работы с помощью опций командной строки.

`-a`

задает для программы Ethereal критерий прекращения записи в файл захвата. Критерий может иметь формат **test:value**, где параметр **test** может принимать значения:

`duration`

задает продолжительность сбора пакетов в секундах.

`filesize`

задает максимальный размер файла в тысячах байтов (не килобайтах = 1024 байт).

`-b`

если задан максимальный размер файла захвата, эта опция заставляет Ethereal работать в режиме кольцевого буфера **(ring buffer)** с указанным числом файлов. В режиме кольцевого буфера Ethereal будет записывать собранные данные в несколько файлов, давая им имена по дате и времени создания файла.

После заполнения первого файла Ethereal перейдет к записи во второй и так далее, пока не будет создано указанное число файлов. При достижении максимального числа файлов первый файл (самый старый) будет уничтожен перед созданием нового файла. Если для максимального числа файлов указано значение 0, сбор данных будет продолжаться неограниченно долго.

Если задана продолжительность сбора пакетов, Ethereal будет создавать новый файл по истечении заданного времени даже в тех случаях когда текущий файл не достиг максимального размера.

`-B <высота>`

задает начальную высоту (в пикселях) панели дампа пакетов (нижняя часть окна программы, показанного на рисунке 1).

`-c <число пакетов>`

задает используемое по умолчанию число пакетов для чтения при сборе “живых” данных.

`-f <фильтр>`

задает выражение для фильтра захвата пакетов.

`-h`

выводит информацию о номере версии и опциях программы, после чего завершает работу.

`-i <интерфейс>`

задает имя сетевого интерфейса или канала (pipe), используемого для сбора пакетов.

Имена сетевых интерфейсов должны соответствовать именам из списка поддерживаемых системой, которым можно получить по команде **tethereal -D**. Для Unix-систем список присутствующих в системе интерфейсов можно получить также по команде **netstat -i** или **ifconfig -a** (последняя команда может не работать в старых версиях Unix).

В качестве имен каналов могут использоваться имена буферов FIFO (named pipe – именованные каналы) или символ “**-**” для сбора пакетов со стандартного устройства ввода. Получаемые из канала данные должны использовать стандартный формат libpcap.

`-k`

инициирует начало сбора пакетов. Если задан флаг **-i**, пакеты собираются только с указанного этим параметром интерфейса. Если интерфейс не задан, Ethereal находит список интерфейсов системы и выбирает из него первый интерфейс, пропуская loopback. Если в системе присутствует только интерфейс loopback, Ethereal выводит сообщение об ошибке, не начиная сбор пакетов.

`-l`

включает автоматическую прокрутку списка пакетов, если включен режим автоматического обновления списка по мере захвата пакетов (опция **-S**).

`-L`

выводит список поддерживаемых типов кадров канального уровня, после чего работа программы завершается.

`-m <имя шрифта>`

задает имя растрового шрифта, используемого программой Ethereal в большинстве случаев. Для вывода в панели дампа данных, соответствующих выбранному в панели дерева протоколов полю, жирным шрифтом (bold) Ethereal будет создавать имя шрифта на основе имени, заданного этой опцией.

`-n`

отключает функцию определения имен сетевых объектов (например, названий портов TCP и UDP, имен хостов).

`-N <тип>`

включает функцию определения имен для отдельных типов адресов и номеров портов; прочие типы адресов и номера портов выводятся в цифровом представлении. Поле **<тип>** содержать значение **m** для преобразования MAC-адресов, **n** для преобразования адресов сетевого уровня (IP) или **t** для преобразования номеров портов. Данная опция отменяет действие флага **-n** при одновременном использовании. Значение **C** добавляет поддержку асинхронных запросов DNS.

`-o <имя:значение> [<имя:значение> ...]`

[3]Windows-версия Ethereal работает с библиотекой winpcap, доступной на сайте http://winpcap.polito.it.
[4]Для фильтров отображения пакетов используется другой синтаксис.

задает предпочтительное значение указанного параметра. Это значение отменяет принятое по умолчанию и указанное в файле предпочтений значение параметра. Имена параметров должны совпадать с именами в файле предпочтений.

`-p`

указывает программе, что интерфейс не нужно переводить в режим захвата[5].

`-P <число пикселей>`

задает начальную высоту панели со списком пакетов (верхняя панель программы, см. рис. 1).

`-Q`

задает завершение работы программы Ethereal после окончания сеанса сбора пакетов. Эта опция полезна при работе в пакетом режиме, задаваемом флагом **-c**. Для использования данной опции в командной строке должны присутствовать также флаги **-i** и **-w**.

`-r <имя файла>`

задает чтение пакетов из файла.

`-R <фильтр>`

при использовании совместно с флагом чтения данных из файла (**-r**) эта опция активизирует указанный фильтр[6] для всех читаемых из файла пакетов. Не соответствующие фильтру пакеты просто отбрасываются.

`-S`

задает выполнение операций по захвату пакетов в форме отдельного процесса с автоматическим обновлением отображаемого списка собранных пакетов.

`-s <размер захвата>`

задает принятый по умолчанию размер захвата (snapshot length) для использования при “живом” сборе данных. Для каждого пакета в память или на диск записывается не более заданного этим параметром числа байтов.

`-T <число пикселей>`

задает начальную высоту панели дерева протоколов (средняя панель на рисунке 1).

`-t <формат>`

задает формат временных меток для списка пакетов - **r** (relative – относительно времени старта), **a** (absolute – абсолютное время), **ad** (absolute with date - абсолютное время с указанием даты) или **d** (delta – интервал после захвата предыдущего пакета). По умолчанию временные метки выводятся относительно начала захвата (**r**).

`-v`

задает вывод номера версии программы и завершение работы.

`-w <имя файла>`

задает используемое по умолчанию имя файла захвата.

`-y <тип>`

при захвате пакетов, инициированном флагом **-k**, эта опция задает тип канального уровня для сеанса сбора. В качестве значения параметра могут использоваться значения, идентификаторы типов, выводимые при использовании команды с флагом **-L**.

`-z <параметры>`

задает программе Ethereal необходимость сбора статистики и вывода результатов в окне с периодическим обновлением содержимого. В настоящее время поддерживается несколько параметров сбора статистики:

`-z dcerpc,srt,uuid,major.minor[,filter]`

Программа собирает данные **SRT**[7] для вызовов/откликов интерфейса **DCERPC** с идентификатором **uuid**, версии **major.minor**. К собираемым данным относятся число вызовов каждой процедуры, MinSRT, MaxSRT и AvgSRT[8]. Например опция **-z dcerpc,srt,12345778-1234-abcd-ef00-0123456789ac,1.0** будет обеспечивать сбор информации для интерфейса CIFS SAMR. Такие опции можно использовать в командной строке неоднократно.

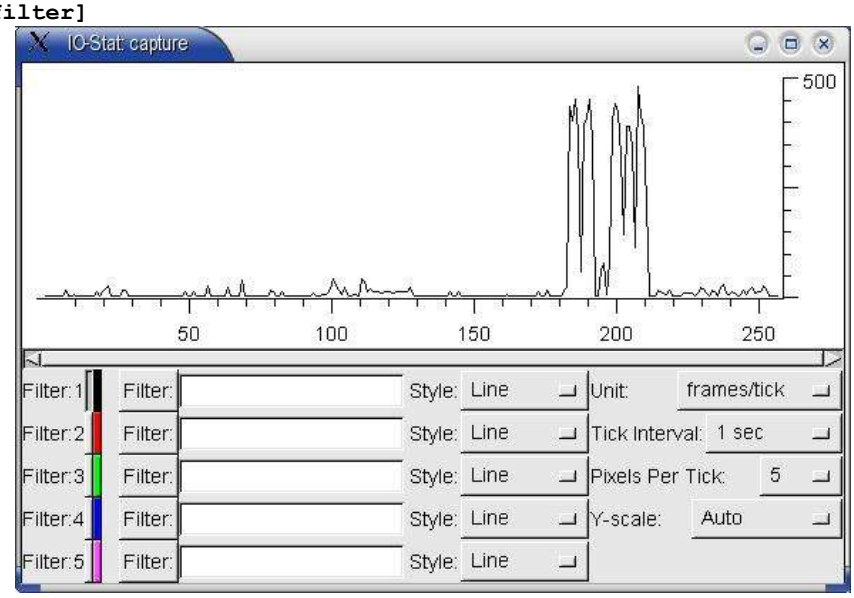

Рисунок 2 Окно IO-Stat

При использовании необязательного фильтра в результатах будут учитываться только соответствующие фильтру статистические данные. Например, опция **-z dcerpc,srt,12345778-1234-abcd-ef00-0123456789ac,1.0,ip.addr==1.2.3.4** будет обеспечивать сбор статистики **SAMR SRT** только для хоста с IP-адресом 1.2.3.4. Опция

`-z io,stat`

будет обеспечивать статистику по захвату кадров и байтов в течение каждой секунды. При использовании такой опции будет открываться диалоговое окно **IO-Stat** (см. рисунок 2), содержащее статистическую информацию с отдельным графиком для каждого фильтра. Такие опции можно использовать в командной строке неоднократно.

[5]Интерфейс может быть переведен в режим захвата другими программами, поэтому использование флага **-p** отнюдь не гарантирует работу интерфейса в обычном режиме – программа просто не будет переводить этот интерфейс в режим захвата. Кроме того, даже в обычном режиме захватываться будут не только пакеты, адресованные этому интерфейсу, поскольку в сети всегда присутствуют широковещательные пакеты и могут использоваться пакеты с групповыми адресами (multicast).

[6]Для этого фильтра используется синтаксис фильтров отображения, а не фильтров захвата.

[7]Service Response Time – время отклика службы.

[8]Минимальное, максимальное и среднее время отклика, соответственно.

Окно статистики, показанное на рисунке 2, можно открыть также с использованием меню **Tools|Statistics|Traffic|IO-Stat** (стр 18).

`-z rpc,srt,program,version[,<filter>]`

обеспечивает сбор статистики вызовов/откликов SRT для указанной программы и версии. Данные включают число вызовов для каждой процедуры, MinSRT, MaxSRT и AvgSRT. Например, опция **-z rpc,srt,100003,3** позволит собрать статистику вызовов для NFS v3. Допускается неоднократное использование опции в командной строке.

При указании в строке необязательного фильтра статистика будет выводиться только для соответствующих этому фильтру пакетов. Например, опция **-z rpc,srt,100003,3,nfs.fh.hash==0x12345678** задает сбор статистики NFS v3 SRT только для указанного файла.

`-z rpc,programs`

задает сбор статистики вызовов/откликов RTT для всех известных программ и версий **ONC-RPC**. Данные включают число вызовов, MinRTT, MaxRTT и AvgRTT.

`-z smb,srt[,filter]`

задает сбор статистики SRT для протокола SMB. Данные включают число вызовов каждой команды SMB, MinSRT, MaxSRT и AvgSRT.

Данные представляются в отдельных таблицах для всех нормальных команд каждой SMB, а также команд Transaction2 и всех команд NT. Отображается статистика только для тех команд, которые встретились в собранных пакетах. В цепочке команд **xAndX** для расчета используется только первая команда. Так, для распространенных цепочек **SessionSetupAndX** + **TreeConnectAndX** в статистике будут учитываться только вызовы **SessionSetupAndX**. Это ограничение планируется снять в будущих версиях программы. Допускается неоднократное использование опции в командной строке.

При использовании в командной строке необязательного фильтра статистика рассчитывается только с учетом пакетов, соответствующих заданному фильтру. Например, опция **-z "smb,srt,ip.addr==1.2.3.4"** будет выводить статистику только для пакетов SMB, обмен которыми происходит с сайтом, имеющим IP-адрес 1.2.3.4 .

`-z fc,srt[,filter]`

собирает статистику SRT для FC[9]. Данные включают число вызовов каждой команды Fibre Channel, MinSRT, MaxSRT и AvgSRT. Значение времени отклика SRT рассчитывается как временной интервал от первого до последнего кадра в сеансе обмена данными. Данные представляются в виде отдельной таблицы для каждой нормальной команды FC. Выводятся, данные только для тех команд, которые встречались в собранных пакетах. Допускается неоднократное использование опции в командной строке.

При использовании фильтра статистика рассчитывается с использованием только тех данных, которые соответствуют заданному фильтру. Например, опция **-z "fc,srt,fc.id==01.02.03"** задает сбор статистики только для обмена данными с хостом, имеющим FC-адрес 01.02.03 .

`-z mgcp,srt[,filter]`

задает сбор статистики SRT для MGCP. Выводятся данные по вызовам для каждого известного типа MGCP Type, Minimum SRT, Maximum SRT и Average SRT. Допускается неоднократное использование опции в командной строке.

При указании в командной строке фильтра, расчет статистики проводится только с учетом тех данных, которые соответствуют условиям фильтрации. Например, опция **-z "mgcp,srt,ip.addr==1.2.3.4"** задает сбор статистики MGCP только для пакетов, обмен которыми осуществляется с IP-хостом 1.2.3.4 .

`-z conv,type[,filter]`

создает таблицу, в которой указываются список всех сеансов обмена данными (conversation - “разговор”) в собранных пакетах. Параметр **type** задает тип соединений, для которых нужно генерировать статистику. Поддерживаются типы

eth – Ethernet;

fc – адреса Fibre Channel;

fddi – адреса FDDI;

ip – IP-адреса;

ipx – адреса IPX;

tcp – пары сокетов TCP/IP (поддерживаются протоколы IPv4 и IPv6);

tr – Token Ring;

udp – пары сокетов UDP/IP (поддерживаются протоколы IPv4 и IPv6).

Если командная строка включает фильтр, статистика генерируется только для тех соединений, которые соответствуют заданному фильтру.

Выводимая таблица содержит по одной строке для каждого соединения и показывает число пакетов/байтов, переданных в каждом направлении, а также общее число пакетов/кадров. Строки таблицы сортируются в в соответствии с общим числом кадров для соединения.

Для просмотра таблицы можно также воспользоваться во время сбора пакетов опцией меню **Tools|Statistics|Conversation List** (стр. 18).

`-z h225,counter[,filter]`

собирает сообщения ITU-T H.225 и сведения о причинах (reason) их генерации. В первой колонке создаваемой этой опцией таблицы указывается список сообщений H.225 и их причин для собранных программой пакетов. Вторая колонка таблицы указывает количество для каждого сообщения и причины. Допускается неоднократное использование опции в командной строке.

При указании в командной строке фильтра статистика будет рассчитываться только с учетом соответствующих этому фильтру пакетов. Например, опция **-z "h225,counter,ip.addr==1.2.3.4"** задает расчет статистики H.225 только для пакетов, обмен которыми ведется с IP-хостом 1.2.3.4 .

[9] Fibre Channel

Графический интерфейс Ethereal

Работа с программой Ethereal построена на базе графического интерфейса (GUI), показанного на рисунке 3. Режим захвата и отображения пакетов задается с помощью опций командной строки и описанных в последующих параграфах команд меню и диалоговых окон.

Главное окно программы

Главное окно Ethereal разделено на три панели. Размеры каждой из панелей можно менять, используя маркер в нижней правой части соответствующей панели.

Верхняя панель

Верхняя панель окна Ethereal содержит список пакетов. По умолчанию в списке выводится 6 колонок – номер пакета в списке собранных, временная метка, адреса и номера портов отправителя и получателя, протокол и краткое описание пакета. Вы можете изменить набор отображаемых колонок с помощью страницы **Columns** (стр. 21) диалогового окна **Preferences** (стр. 21). Для активизации диалогового окна можно использовать команду меню **Edit:Preferences** (стр. 8) или кнопку на панели инструментов окна Ethereal.

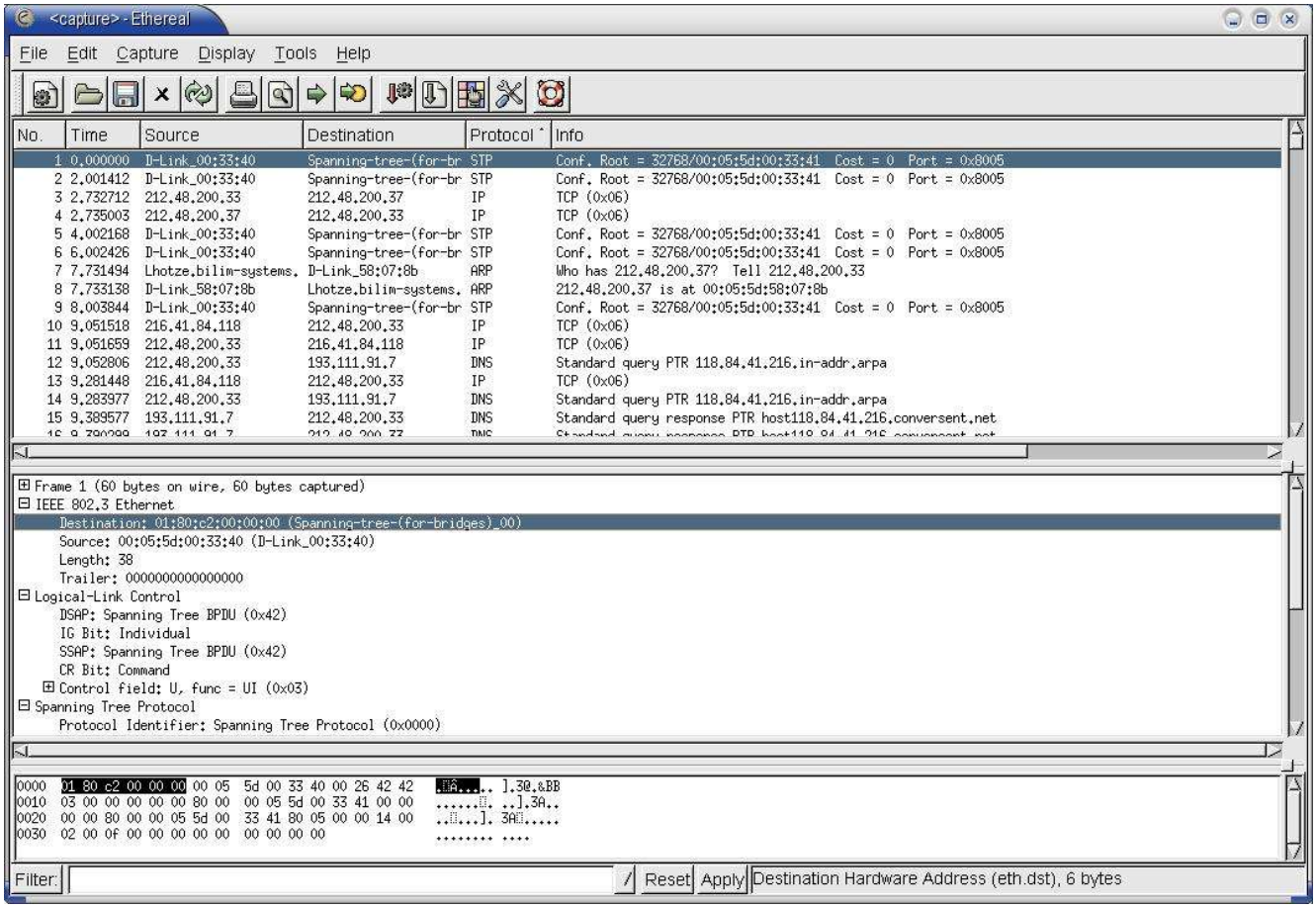

Рисунок 3 Панели главного окна Ethereal

Щелкнув кнопкой мыши на поле с именем колонки в верхней строке списка пакетов, вы можете задать сортировку пакетов по содержимому данной колонки. Повторный щелчок на этом поле изменит порядок сортировки.

В полях адресов выводится информация максимально доступного уровня. Например, для кадров Ethernet, содержащих пакеты IP будут указываться адреса IP, но если тип передаваемого в кадрах протокола неизвестен, поле будет содержать MAC-адрес.

Правая кнопка мыши активизирует всплывающее меню для списка пакетов.

Средняя кнопка мыши может использоваться для маркировки пакетов в списке.

Средняя панель

Средняя панель окна Ethereal содержит дерево протоколов для выбранного из списка верхней панели пакета. Дерево отображает каждое поле и его значение для заголовков всех протоколов стека. Структуру каждой ветви дерева можно раскрыть или свернуть, нажимая кнопку мыши на квадратике в начале строки соответствующего протокола.

Правая кнопка мыши активизирует всплывающее меню для панели дерева протоколов.

Нижняя панель

Нижняя панель окна содержит дамп указанного в списке пакета в шестнадцатеричном и ASCII-формате. Выбранное в панели дерева протоколов поле выделяется цветом соответствующей области дампа, как показано на рисунке 3.

Правая кнопка мыши активизирует всплывающее меню для панели дампа.

Панель Filter

Размещенная в строке состояния окна Ethereal панель управления фильтрами отображения позволяет выбирать фильтр из числа сохраненных или задавать условия фильтрации непосредственно в строке ввода. Кнопка **Apply** служит для активизации фильтра, кнопка **Reset** отключает текущий фильтр отображения. Для создания и редактирования фильтров отображения используется диа-

логовое окно (стр. 8), активизируемое с помощью команды меню **Edit:Display Filters** (стр. 8) или кнопки на панели инструментов Ethereal (стр. 20).

Фильтр для отображения только трафика HTTP, HTTPS и DNS может иметь форму:

```
tcp.port == 80 || tcp.port == 443 || tcp.port == 53
```

Кнопка **Filter** позволяет выбрать фильтр из числа созданных ранее. После выбора фильтра или его ввода в строке набора нажмите кнопку **Apply** или клавишу **Enter** для активизации указанного фильтра. Кнопка **Reset** сбрасывает фильтр и отключает фильтрацию, обеспечивая вывод всех собранных программой пакетов.

Меню File

Функции меню **File** служат для выбора файлов при анализе собранных ранее данных, сохранения собранных программой пакетов, печати информации о пакетах, а также для завершения работы программы.

Open, Close, Reload

Команды чтения (**Open**), закрытия (**Close**) и повторной загрузки (**Reload**) файла собранных пакетов. Диалоговое окно **File:Open** (см. рисунок 4) позволяет использовать указать фильтр, который будет использоваться по отношению к загружаемым из файла пакетам (фильтр захвата). Вы можете выбрать существующий фильтр или создать новый фильтр для обработки данного файла.

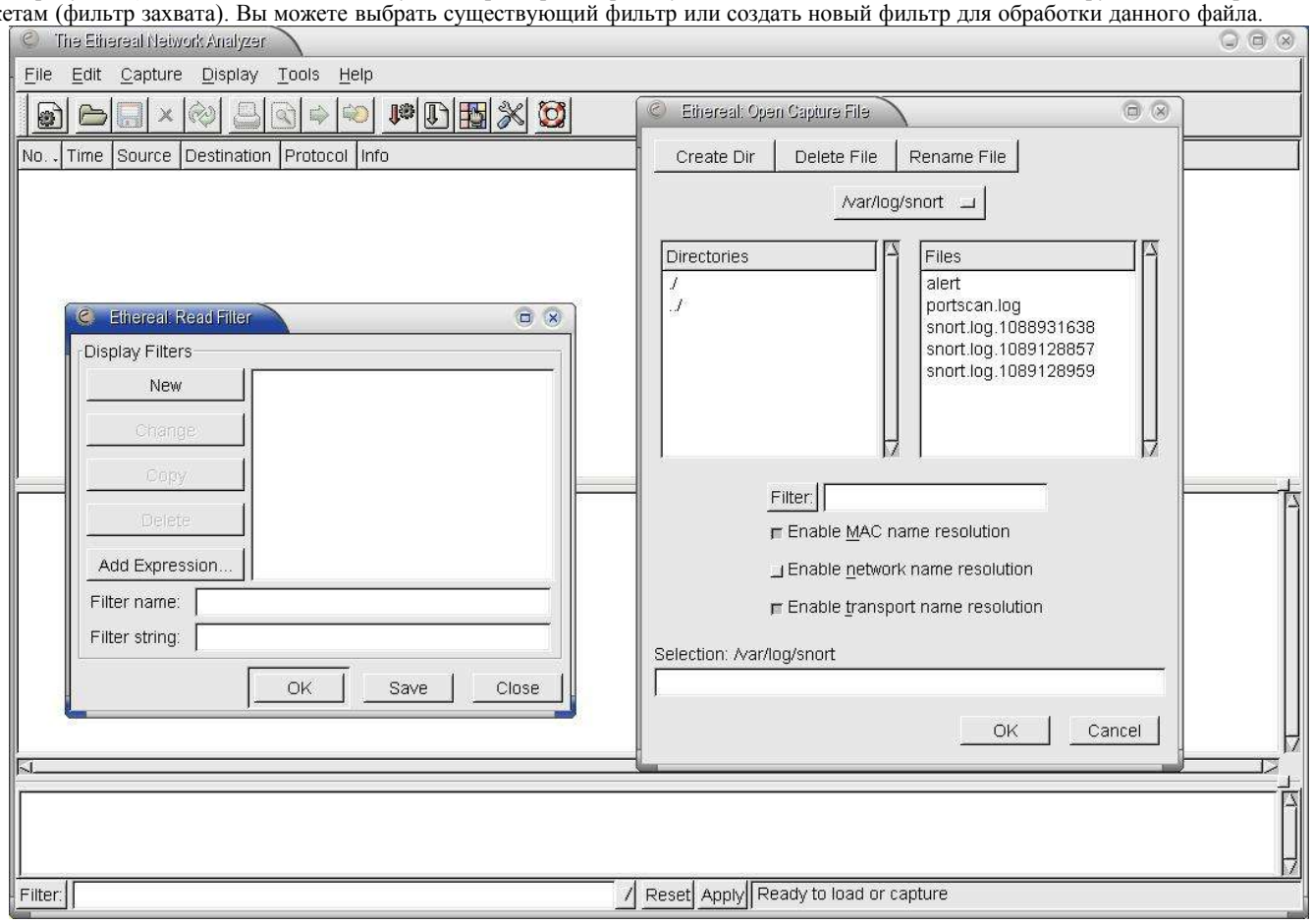

Рисунок 4 Диалоговые окна выбора файлов (справа) и фильтров

Перечисленные здесь команды работы с файлами захвата доступны также с помощью кнопок, выведенных на панель инструментов Ethereal (стр. 20), или комбинаций клавиш **Ctrl+O** (Open), **Ctrl+W** (Close), **Ctrl+R** (Reload).

Save, Save As

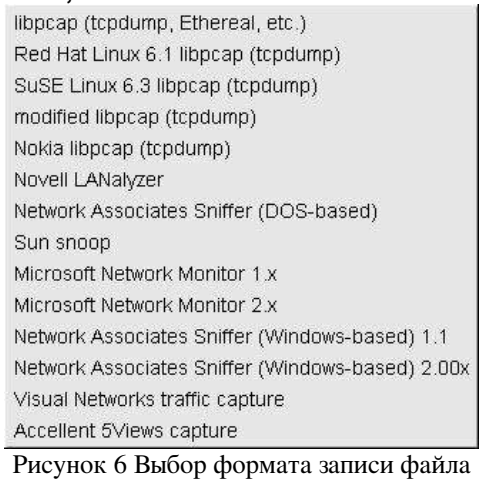

Рисунок 6 Выбор формата записи файла

Команды сохранения и записи с новым именем для файлов захвата. Поле выбора **Save only packets currently being displayed** (см. рисунок 5) позволяет записать в файл только пакеты, удовлетворяющие условиям фильтрации при отображении (стр. 8), а поле **Save only marked packets** – только отмеченные пакеты. Вы можете также выбрать из списка (см. рисунок 6) один из поддерживаемых программой форматов записи файлов захвата.

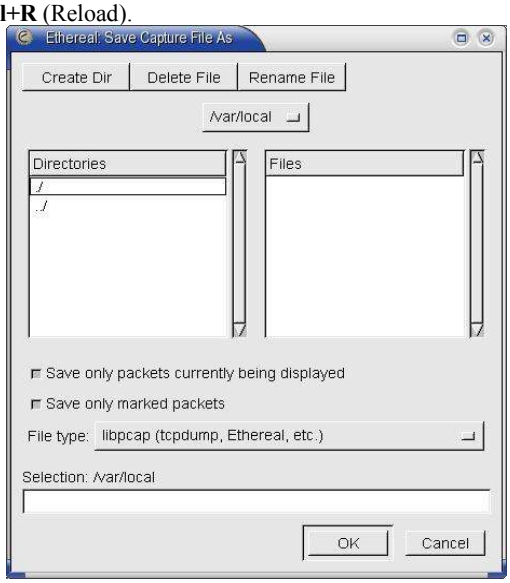

Рисунок 5 Диалоговое окно записи файла

Для записи собранных программой пакетов на диск можно также использовать кнопку на панели инструментов программы Ethereal (стр. 20) или комбинацию клавиш **Ctrl+S**.

Print

Эта команда служит для вывода на печать информации для всех собранных пакетов или отмеченных пакетов из списка. Для каждого пакета выводится строка из списка пакетов (**Print summary**) или содержимое окна дерева каталогов (**Print detail**). В режиме детального вывода может также печататься шестнадцатеричный дамп каждого пакета (опция **Print hex data**). Кроме того, для этого режима можно выбрать вывод всего дерева протоколов (**Expand all levels**) или только раскрытых ветвей дерева (**Print as displayed**).

Операцию печати можно активизировать также с помощью кнопки на панели инструментов программы Ethereal (стр. 20).

Опции печати общего назначения (принтер, формат и т. п.) можно указать в диалоговом окне **Print** (рисунок 7) или на странице **Printing** (стр. 21) диалогового окна **Preferences**.

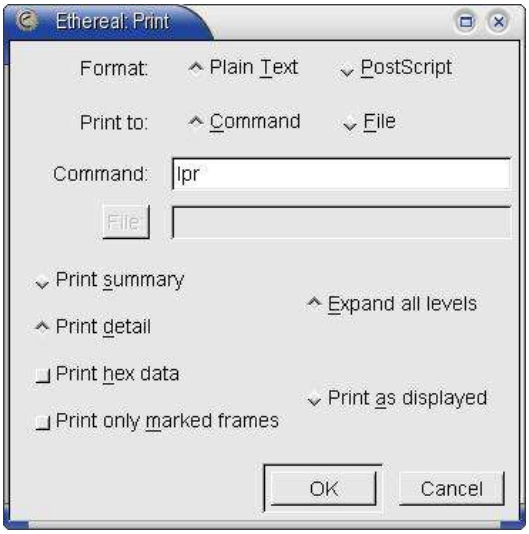

Рисунок 7 Диалоговое окно Print

Print Packet

Эта команда выводит на печать полностью раскрытое дерево протоколов для пакета, выбранного в списке. При печати используются опции, заданные на странице **Printing** (стр. 21) диалогового окна **Preferences**.

Команду печати пакета можно также активизировать с помощью комбинации клавиш **Ctrl+P**.

Рисунок 8 Диалоговое окно Find Frame

Quit

Завершает работу программы. Для завершения работы программы можно также использовать комбинацию клавиш **Ctrl+Q**.

Меню Edit

Find Frame

Эта команда (**Ctrl+F**) позволяет просматривать в прямом и обратном направлении список собранных пакетов на предмет поиска кадра, соответствующего заданному шаблону поиска. При активизации команды на экран выводится диалоговое окно **Find Frame** (см. рисунок 8), позволяющее задать направления, критерий поиска и дополнительные опции для выбранного критерия.

Для поиска кадров можно использовать указанный фильтр отображения (стр. 24) или контекст, заданный в шестнадцатеричном или символьном виде. При задании шаблона поиска в шестнадцатеричном формате разделителями шестнадцатеричных цифр могут служить пробел, двоеточие или дефис. При текстовом поиске вы можете задать кодировку (ASCII, Unicode или обе кодировки сразу) и опцию учета регистра символов.

Во всех режимах поиск начинается с выбранного в списке пакета. Если в данный момент указатель не установлен ни на один пакет в списке, в качестве начальной точки используется тот пакет, который был выбран последним.

Find Next

Продолжает поиск в направлении роста порядковых номеров (forward) в соответствии с заданными ранее критериями поиска. Для поиска следующего пакета можно также воспользоваться комбинацией клавиш **Ctrl+N** или кнопкой на панели инструментов программы Ethereal (стр. 20).

Find Previous

Продолжает поиск в направлении уменьшения порядковых номеров (backward) в соответствии с заданными ранее критериями поиска. Найти предыдущий пакет можно также с помощью комбинации клавиш **Ctrl+B**.

Go To Frame

Обеспечивает переход к кадра, указанному номером в списке. Для перехода к интересующему кадру вы можете также использовать комбинацию клавиш **Ctrl+G** или кнопки на панели инструментов программы Ethereal (стр. 20).

Субменю Time Reference

Команда (**Ctrl+T**) позволяет установить для указанного в списке пакета метку ***REF** или снять ранее установленную метку. Пакеты с такой меткой используются в качестве стартовых точек для отсчета временных интервалов, указываемых в списке пакетов. При наличии в списке нескольких пакетов с такой меткой для первого из них (минимальный номер в списке) отсчет от данного пакета происходит в обоих направлениях. Каждая последующая метка задает стартовую точку для отсчета временных интервалов только в направлении роста порядковых номеров.

Отметим, что пакеты с установленной меткой сохраняются в списке, независимо от заданных фильтров отображения (стр. 24).

При наличии в списке пакетов нескольких меток для перемещения от одной метки к другой могут использоваться команды этого субменю **Find Next** и **Find Previous**.

Mark Frame

Команда (**Ctrl+M**) служит для выбора указанного в списке пакета или снятия ранее установленной метки выбора. При установке метки выбора в поле **frame.marked** помещается флаг выбора, который может впоследствии использоваться фильтрами отображения или командами поиска кадров.

Mark All Frames
Эта команда служит для выделения всех имеющихся в списке кадров.

Unmark All Frames
Эта команда позволяет снять разом все установленные ранее метки выделения кадров.

Preferences
Эта команда позволяет пользователю настроить параметры программы (печать, содержимое колонок списка пакетов, цветовое представление потоков TCP и другие опции). Диалоговое окно Preferences (см. рисунок 9) содержит множество страниц для настройки отдельных аспектов работы программы, подробно описанных ниже (стр. 8).

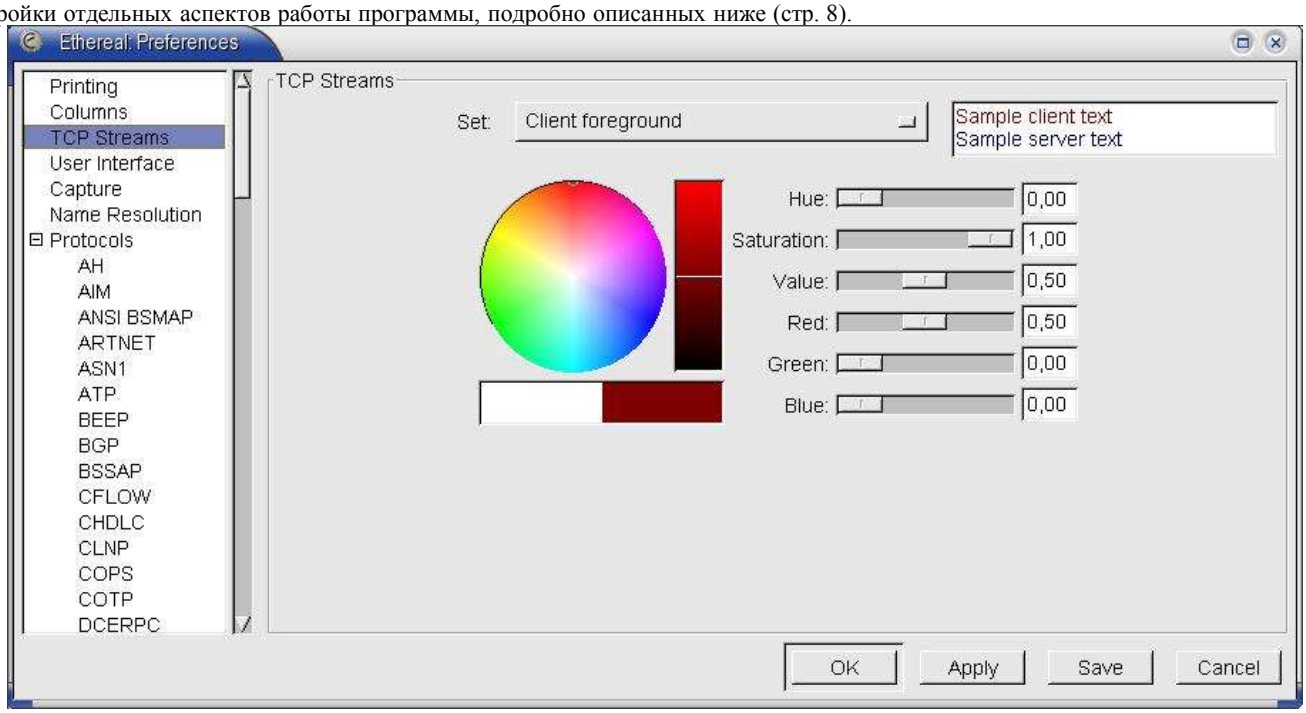

Рисунок 9 Диалоговое окно Preferences

Capture Filters
Эта команда позволяет создавать, редактировать и удалять фильтры захвата пакетов, используемые программой Ethereal. Синтаксис фильтров захвата полностью соответствует фильтрам программы tcpdump.

При активизации команды на экран выводится диалоговое окно **Edit Capture Filter List** (см. рисунок 10) со списком существующих фильтров. Для создания нового фильтра укажите имя (поле **Filter name:**) и выражение (поле **Filter string:**) после чего нажмите кнопку **New**. При создании сложных фильтров большую помощью окажет функция копирования фильтров.

Для редактирования и выбора фильтров захвата вы можете также воспользоваться кнопкой на панели инструментов Ethereal (стр. 20).

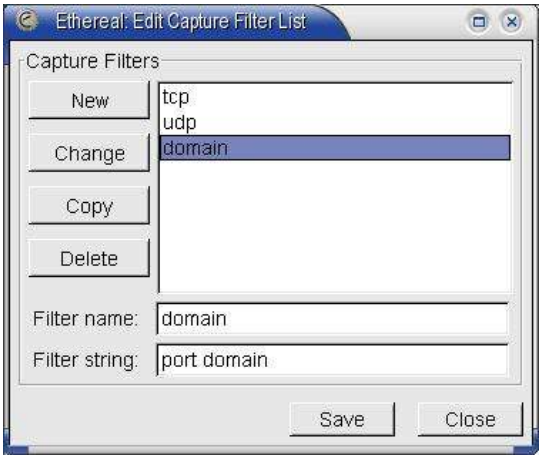

Рисунок 10 Диалоговое окно Edit Capture Filter List

Display Filters
Данная команда позволяет управлять фильтрами Ethereal, используемыми программой для отбора пакетов, отображаемых в списке. Фильтры отображения применяются после фильтров захвата и позволяют выбрать из собранных программой пакетов только те, которые в данный момент представляют интерес. При сборе большого числа пакетов возможность выбора отображаемых пакетов существенно упрощает работу администратора по анализу трафика. Синтаксис фильтров отображения рассматривается на стр. 24.

Для задания фильтра отображения служит также поле выбора в нижней части главного окна Ethereal (см. рисунок 3).

Активизировать диалоговое окно можно также с помощью кнопки на панели инструментов Ethereal (стр. 20).

Диалоговое окно Edit ... Filter List

Диалоговое окно **Edit ... Filter List** (см. рисунок 42) позволяет создавать, редактировать и удалять фильтры отображения, поиска и статистики. Синтаксис фильтров описан на стр. 24.

Окно содержит список существующих фильтров, поля для ввода имени фильтра и выражения, обеспечивающего фильтрацию, а также ряд кнопок, описанных в таблице 1.

Таблица 1 Кнопки диалогового окна выбора фильтров

Кнопка	*Выполняемые действия*
New	При заполненных полях **Filter name** и **Filter string** эта кнопка создает для нового фильтра соответствующую запись в списке.
Change	Эта кнопка служит для изменения указанного в фильтре списка в соответствии с новыми значениями полей ввода **Filter name** и **Filter string**.
Copy	Создает копию выбранного в списке фильтра.
Delete	Удаляет указанный фильтр из списка.
Add Expression...	Кнопка открывает диалоговое окно **Filter Expression** (стр. 9), позволяющее включать в фильтры логические выражения с использованием поддерживаемых синтаксисом языка описания фильтров примитивов и операций. Созданное в диалоговом окне **Filter Expression** выражение добавляется в поле **Filter string**.
OK	В диалоговых окнах **Display Filter**, **Read Filter** и **Search Filter** эта кнопка закрывает диалог, активизируя фильтр.
Apply	Вносит изменения в текущий фильтр отображения и применяет этот фильтр для списка пакетов.
Save	Сохраняет текущий список фильтров.
Close	Закрывает диалоговое окно без изменения фильтров.

Диалоговое окно Filter Expression

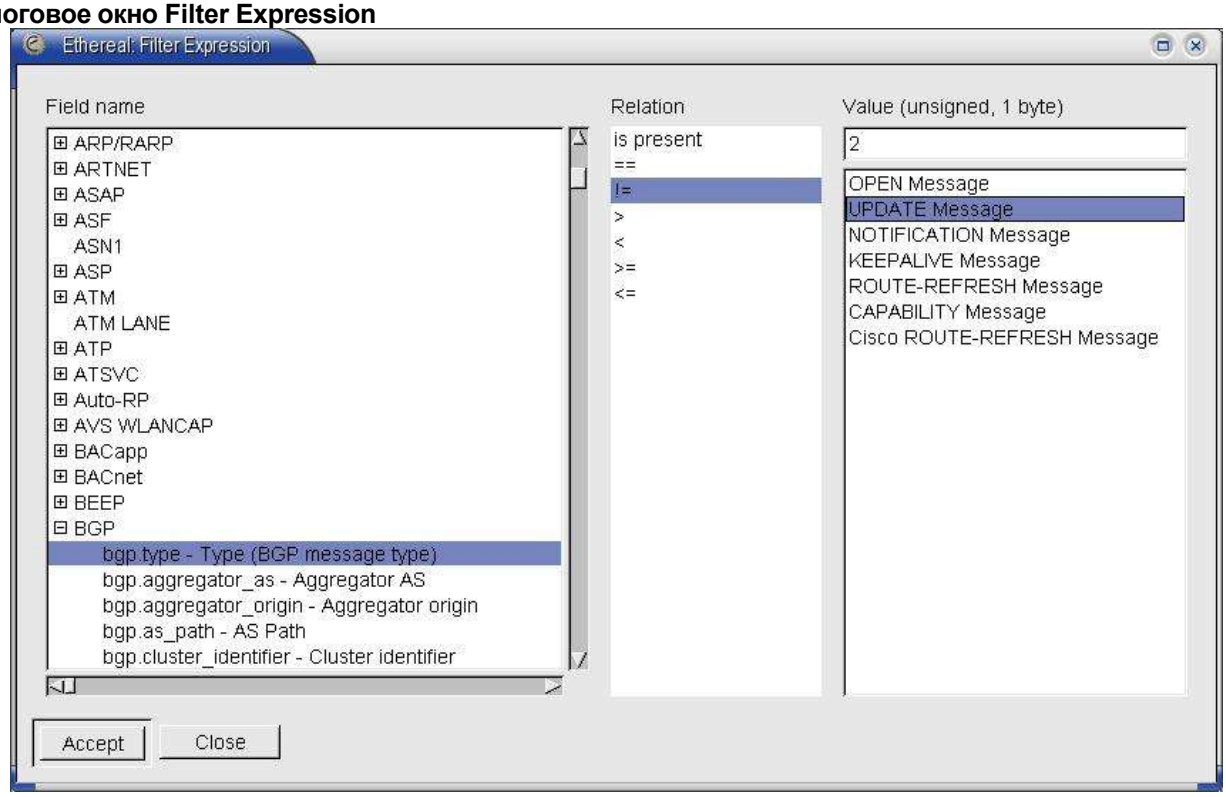

Рисунок 11 Диалоговое окно Filter Expression

Диалоговое окно служит для добавления выражений в строку описания фильтра с использованием поддерживаемых программой примитивов фильтрации и логических операций. При нажатии кнопки **Accept** созданное выражение добавляется в спецификацию фильтра. Кнопка **Close** закрывает окно без сохранения созданного выражения.

Protocols

Эта команда используется для выбора протоколов, которые принимаются во внимание при сборе пакетов. Диалоговое окно **Enabled Protocols** (рисунок 12) позволяет указать протоколы, которые будут учитываться при анализе собранных пакетов. Кнопки **Enable All** и **Disable All** позволяют включить и отключить все протоколы. Кнопка **Invert** изменяет для каждого протокола в списке состояние на обратное (разрешенные протоколы запрещаются, ранее запрещенные - разрешаются).

Если тот или иной протокол указан в числе запрещенных, обнаружив этот протокол в принятом пакете, программа Ethereal переходит к следующему пакету. Все протоколы вышележащих уровней для пакетов запрещенного к анализу протокола также не будут анализироваться и отображаться в списке. Например, при запрете протокола TCP не будет отображаться информация для протоколов TCP, HTTP, SMTP, Telnet и любых других протоколов, передаваемых с помощью пакетов TCP.

Список выбранных протоколов можно сохранить и программа Ethereal при следующем запуске будет учитывать этот список.

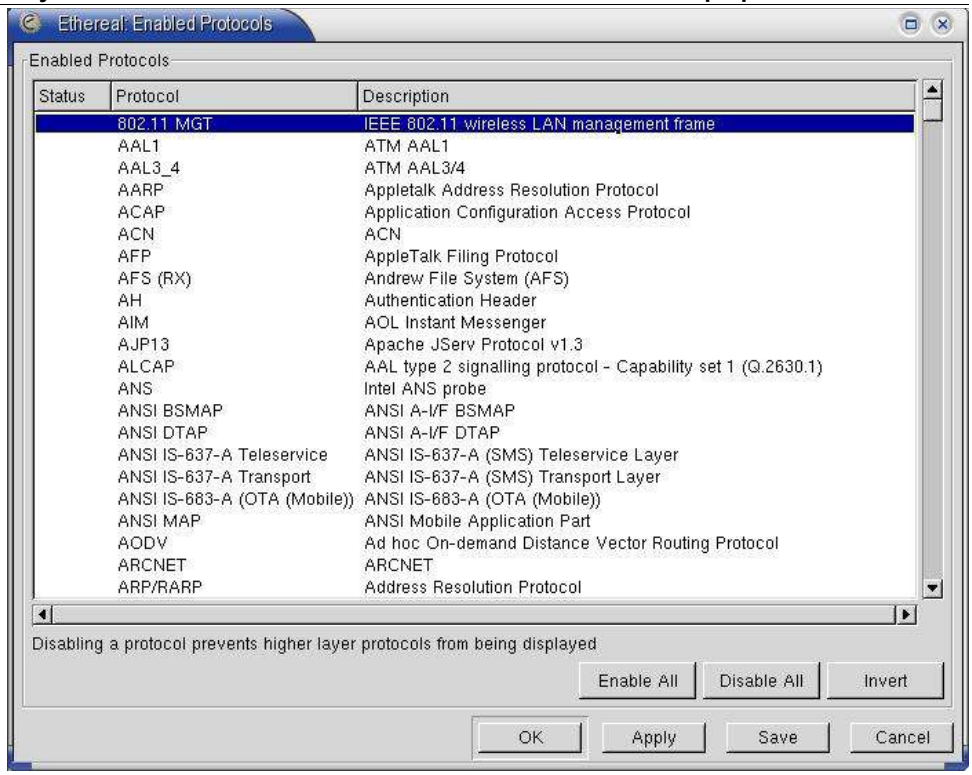

Рисунок 12 Диалоговое окно Protocols

Меню Capture

Меню Capture включает команды управления сбором пакетов.

Start

Команда **Start** выводит на экран диалоговое окно **Capture Options**, показанное на рисунке 13.

В процессе сбора все захваченные пакеты записываются во временный файл (местоположение этого файла указывает переменная окружения TMPDIR).

Для активизации процесса сбора пакетов можно также использовать комбинацию клавиш **Ctrl+K** или кнопку на панели инструментов Ethereal (стр. 20).

Диалоговое окно Capture Options

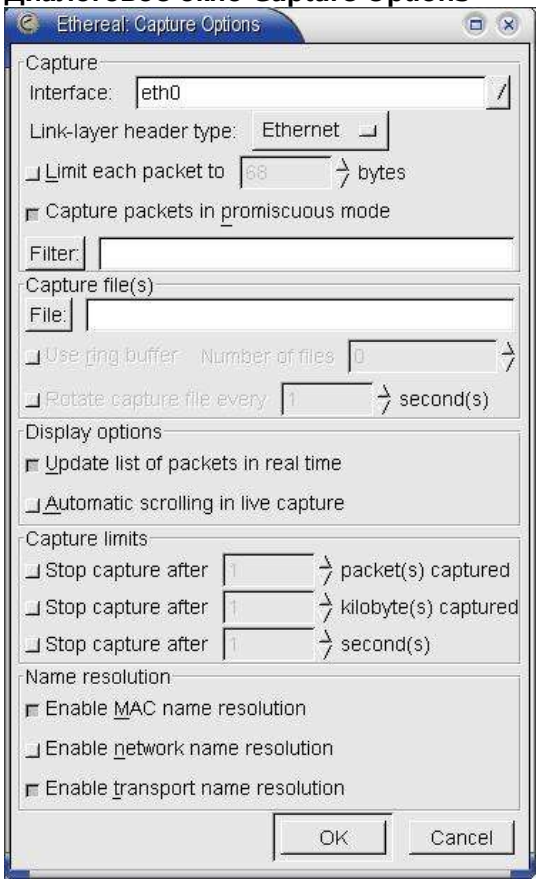

Рисунок 13 Диалоговое окно Capture Options

Диалог **Capture Options** позволяет задать опции сбора пакетов. При активизации окна в нем указаны принятые по умолчанию параметры, которые задаются на странице **Capture** (стр. 23) диалогового окна **Preferences**.

Поле **Interface** служит для выбора интерфейса, с которого будут собираться пакеты. Отметим, что для систем Linux поддерживается фиктивных интерфейс **any** позволяющий собирать пакеты со всех активных интерфейсов системы.

Поле Link-layer header type для некоторых типов интерфейсов позволяет выбрать тип заголовков канального уровня при захвате пакетов. Например, некоторые ОС и версии libpcap позволяют для интерфейсов 802.11 выбирать тип заголовка канального уровня Ethernet или 802.11.

Поле выбора **Limit each packet to ... bytes** позволяет задать размер кадра захвата, используемый при сборе пакетов. Выбрав это поле следует задать размер кадра захвата в поле ввода текста. Если опция не выбрана, размер кадра захвата составляет 65535 байтов, что позволяет собирать все пакеты целиком.

Поле выбора **Capture packets in promiscuous mode** позволяет использовать при сборе пакетов режим захвата, при котором интерфейс прослушивает все передаваемые через среду пакеты, а не только кадры, адресованные данному интерфейсу.

Поле **Filter** позволяет указать фильтр, который будет применяться при сборе пакетов (стр. 8).

Поле **File** служит для задания имени файла, в который будут записываться собранные программой пакеты. Если файл не указан, программа будет записывать пакеты во временный файл. По завершении сбора пакетов вы можете сохранить информацию в желаемом файле с помощью команды меню **File| Save As** (стр. 6).

Поле выбора **Use ring buffer** позволяет собирать пакеты в режиме “кольцевого буфера”. Поле **Number of files** позволяет указать число файлов захвата в кольцевом буфере. Для создания неограниченного числа файлов захвата используйте значение 0.

Поле выбора **Rotate capture file every ... second(s)** позволяет переходить к записи пакетов в новый файл кольцевого буфера по истечении заданного числа секунд, если ранее не был достигнут заданный размер файла захвата.

Поле **Update list of packets in real time** позволяет задать режим обновления списка пакетов непосредственно в процессе их сбора. Выбор этой опции активизирует поле выбора **Automatic scrolling in live**, которое позволяет включить автоматическую прокрутку списка собранных пакетов при которой в окне списка всегда выводится последний захваченный пакет.

Опция **Stop capture after ... packet(s)** позволяет ограничить процесс сбора захватом указанного числа пакетов.

Опция **Stop capture after ... kilobyte(s)** задает максимальный размер файла захвата. В режиме кольцевого буфера эта опция автоматически заменяется полем **Rotate capture file every ... kilobyte(s) -** после сбора заданного объема данных будет автоматически создаваться новый файл захвата. Отметим, что размер файла захвата задается в тысячах байтов, а не к килобайтах (1 кбайт = 1024 байт).

Поле выбора **Stop capture after ... second(s)** позволяет задать продолжительность сбора пакетов в секундах.

Опции **Enable MAC name resolution**, **Enable network name resolution** и **Enable transport name resolution** позволяют задать преобразование MAC-адресов, адресов IP, и номеров портов транспортного уровня в соответствующие имена.

Stop

Эта команда служит для остановки процесса сбора пакетов. Прервать процесс сбора пакетов можно также с помощью комбинации клавиш **Ctrl+E** или кнопки на панели инструментов Ethereal (стр. 20).

Меню Display

Options

Команда **Options** активизирует диалоговое окно **Display Options**, позволяющее установить опции отображения собранных программой пакетов.

Диалоговое окно Display Options

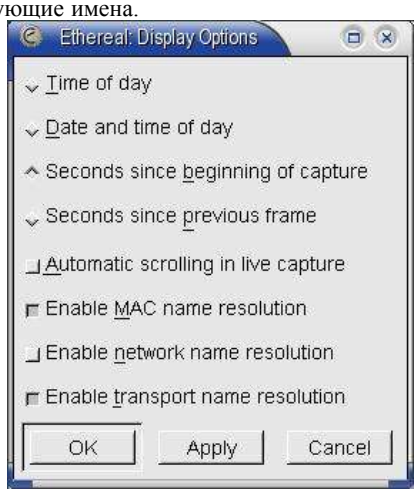

Рисунок 14 Диалоговое окно Display Options

В верхней части диалогового окна находятся 4 кнопки выбора режима отображения временных меток для собранных пакетов.

- **Time of day –** задает вывод временных меток как текущего времени суток.
- **Date and time of day** – временные метки выводятся в виде полной даты (год, число месяца и время суток).
- **Seconds since beginning of capture** – временные метки отсчитываются по числу секунд с момента начала сбора пакетов.
- **Seconds since previous frame** – временные метки задаются в виде интервала с момента прибытия предыдущего пакета.

Опция **Automatic scrolling in the live capture** позволяет задать режим автоматической прокрутки списка собранных пакетов. В этом режиме вы всегда будете видеть в списке последний захваченный пакет.

Кроме того, вы можете выбрать преобразования MAC-адресов, адресов IP и номеров портов транспортного уровня в соответствующие имена.

Match

Команда **Match** позволяет создать фильтр отображения или добавить к фильтру, указанному в нижней части окна программы, выражение на основе выбранной в дереве протоколов информации и применить этот фильтр для текущего отображения пакетов. Для создания фильтра отображения достаточно выбрать интересующее вас поле заголовке в дереве протоколов и указать операцию, которая будет служить для выбора отображаемых пакетов. Допускается последовательный выбор нескольких полей в одном или разных пакетах для создания сложных фильтров.

Selected – в списке остаются только те пакеты, которые имеют в указанном поле соответствующее выбранному пакету значение. Эта опция позволяет легко выделить из числа собранных все пакеты, идентичные указанному.

Not selected – в списке остаются только те пакеты, которые имеют в указанном поле не соответствующее выбранному пакету значение. Эта опция позволяет легко исключить из списка все пакеты, идентичные указанному.

And Selected – в списке остаются только пакеты, соответствующие условиям первого **и** второго выбора полей.

Or Selected – в списке остаются только пакеты, соответствующие условиям первого **или** второго выбора полей.

And Not Selected – в списке остаются только пакеты, соответствующие условиям первого **и** не соответствующие условиям второго выбора полей.

Or Not Selected в списке остаются только пакеты, соответствующие условиям первого **или** не соответствующие условиям второго выбора полей.

Две первые опции используются для задания первого выражения в фильтре отображения, остальные команды служат для добавления выражений в сложный фильтр.

Отметим, что для фильтров отображения используется абсолютное значение смещения полей, поэтому при наличии в заголовках полей переменной длины[10] фильтрация может не соответствовать вашим ожиданиям. Будьте аккуратны при создании фильтров отображения.

Prepare

Эта команда позволяет создать фильтр отображения, как описано в предыдущем параграфе, но не активизирует этот фильтр. Команда может быть весьма удобным инструментом для создания библиотеки фильтров изображения, поскольку при нажатии кнопки **Filter** активизируется диалоговое окно **Edit Display Filter List** (стр. 8), позволяющее отредактировать и сохранить созданные фильтры.

[10]Например, при работе с кадрами Token Ring, содержащими поля source-routed.

Colorize Display – цветовая маркировка пакетов в списке

Команда служит для выделения пакетов в списке в соответствии с фильтрами отображения. Список выбранных фильтров отображения применяется последовательно к каждому из пакетов пока не будет обнаружено соответствие какому-либо из фильтров (на этом процесс проверки прекращается). Следовательно, сначала разумно проверять протоколы более высоких уровней, постепенно спускаясь к канальному уровню.

Механизм цветового выделения

Строки списка выводятся с использованием различных цветов, определяемых списком фильтров цветовой маркировки. Цвет вывода для пакета определяется первым фильтром, которому этот пакет соответствует. Выражения для цветовых фильтров используют такой же синтаксис, какой применяется в фильтрах отображения (стр. 24).

Программа Ethereal при запуске будет загружать фильтры цветовой маркировки из пользовательского файла (если он существует) или глобального файла фильтров маркировки. Если программа не найдет ни одного из этих файлов, цветовая маркировка пакетов не будет использоваться.

Диалоговое окно Apply Color Filters

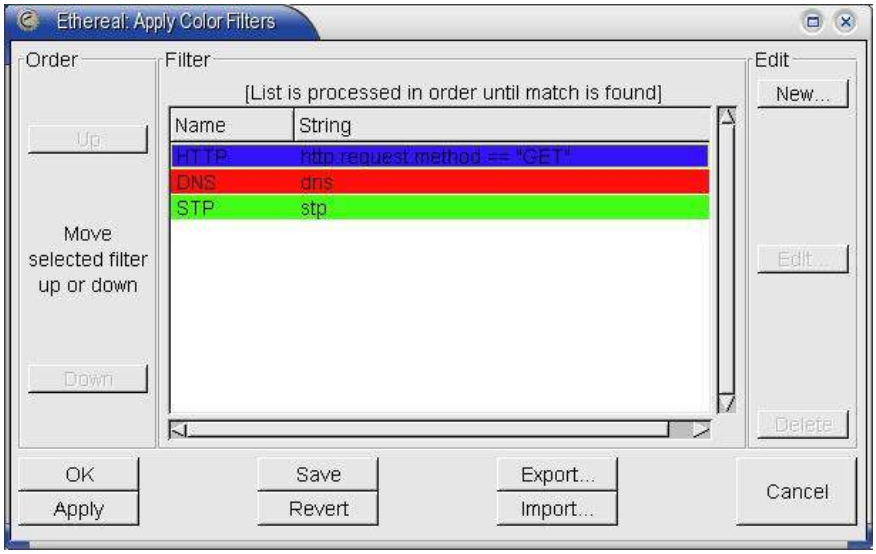

Рисунок 15 Диалоговое окно Apply Color Filters

Это диалоговое окно содержит список существующих фильтров цветовой маркировки и позволяет добавлять и удалять правила из списка, а также редактировать существующие правила и менять порядок их расположения в списке. Кроме списка фильтров, окно содержит ряд кнопок (таблица 2), служащих для выполнения операций над выделенными в списке фильтрами или всем набором фильтров. Внешний вид окна **Apply Color Filters** показан на рисунке 15, а отдельные элементы окна описаны ниже.

Список фильтров

Центральная часть диалогового окна содержит список существующих фильтров цветовой маркировки пакетов. Для выбора строки в списке фильтров достаточно щелкнуть на этой строке кнопкой мыши. Для выделения нескольких строк из списка используйте кнопку мыши при нажатой клавише **Ctrl** или **Shift**.

Кнопки управления фильтрами цветовой маркировки

Таблица 2 Кнопки диалогового окна Apply Color Filters

Кнопка	*Действия*
Up	Перемещает выбранные строки списка фильтров на одну позицию вверх[11].
Down	Перемещает выбранные строки списка фильтров на одну позицию вниз.
New	Добавляет новый фильтр в начало списка и активизирует диалоговое окно **Edit Color Filter** (стр. 13). После создания фильтра вы можете переместить его в нужное место списка.
Edit	Кнопка редактирования фильтра открывает диалоговое окно **Edit Color Filter** (стр. 13), позволяющее изменить указанный в списке фильтр. Если в списке выделено несколько фильтров, кнопка блокируется.
Delete	Удаляет из списка выделенные фильтры.
OK	Закрывает диалоговое окно, оставляя фильтры цветовой маркировки в текущем состоянии.
Apply	Активизирует фильтры из текущего списка, используя заданную этими фильтрами цветовую маркировку для существующего списка пакетов. Диалоговое окно при нажатии кнопки не закрывается.
Save	Сохраняет текущий список фильтров цветовой маркировки в персональном файле. Сохраненный список фильтров будет автоматически активизирован при следующем запуске программы Ethereal.
Revert	Удаляет файл с персональным списком фильтров, загружает глобальный фильтр цветовой маркировки (если такой фильтр имеется) и закрывает диалоговое окно.
Export	Позволяет сохранить текущий список фильтров цветовой маркировки в указанном файле. Вы можете сохранить весь список фильтров или только отмеченные в нем строки. Основным назначением этой кнопки является создание глобального списка фильтров цветовой маркировки (у вас должны быть для этого соответствующие полномочия).
Import	Позволяет включить фильтры из выбранного файла в начало текущего списка фильтров цветовой маркировки. После добавления фильтров из файла они находятся в состоянии выделенных, поэтому вы можете переместить весь набор добавленных из файла фильтров в нужную позицию списка.
Cancel	Закрывает диалоговое окно без изменения цветовой маркировки пакетов.

[11]Напомним, что цвет вывода для пакетов определяется первым фильтром, которому соответствует этот пакет. Поэтому порядок следования фильтров в списке имеет важное значение.

Диалоговое окно Edit Color Filter

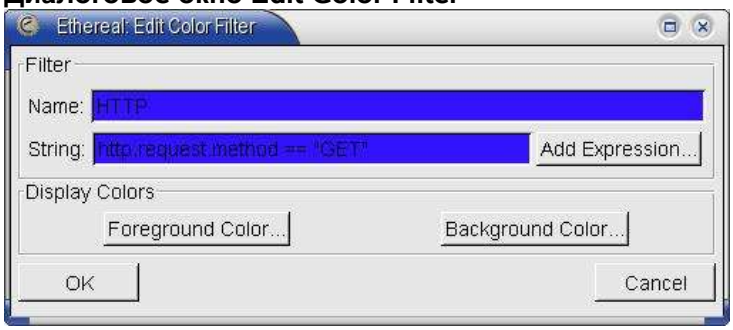

Рисунок 16 Диалоговое окно Edit Color Filter

Диалоговое окно редактирования фильтров цветовой маркировки позволяет изменить параметры фильтра, указанного в списке диалогового окна **Apply Color Filters**. Окно редактирования содержит строку с именем фильтра и выражение, используемое для фильтрации. Вы можете задать условия фильтрации вручную или создать фильтр с помощью диалога Filter Expression (стр. 9). Для выбора цветов фона и переднего плана при выводе пакетов, соответствующих фильтру, служат кнопки **Backgroung Color ...** и **Foregroung Color ...**. При нажатии на эти кнопки на экран выводится диалоговое окно выбора цвета, показанное на рисунке 17.

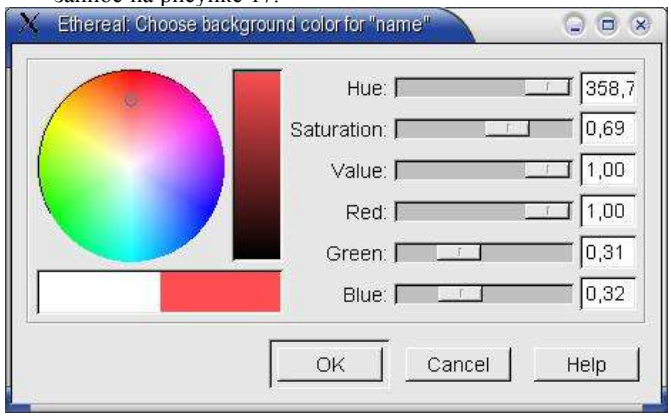

Рисунок 17 Диалоговое окно выбора цвета

Collapse All

Сворачивает все развернутые ветви дерева протоколов.

Expand All

Разворачивает все свернутые ветви дерева протоколов.

Show Packet In New Window

Эта команда создает новое окно, содержащее панели дерева протоколов и дампа для выбранного в списке пакета (рисунок 18). Это окно будет сохраняться на экране в неизменном виде даже при выборе списке другого пакета. Таким образом вы можете просматривать содержимое нескольких пакетов одновременно.

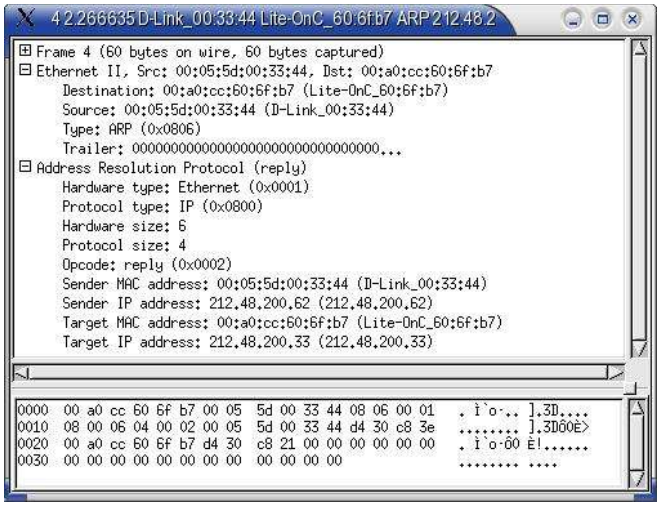

Рисунок 18 Вывод дерева протоколов и дампа пакета в новом окне

User Specified Decodes

Эта команда выводит на экран диалоговое окно **Decode As Show** со списком заданных пользователем изменений схемы декодирования (стр. 14). Кроме списка заданных пользователем изменений окно содержит кнопку **OK** для закрытия окна и кнопку **Reset Changes** для отказа от всех внесенных ранее изменений схемы декодирования. Вид диалогового окна показан на рисунке 19.

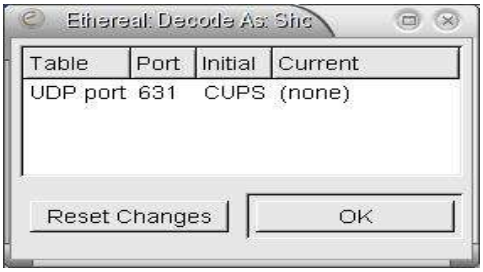

Рисунок 19 Диалоговое окно Decode As Show

Меню Tools

Plugins

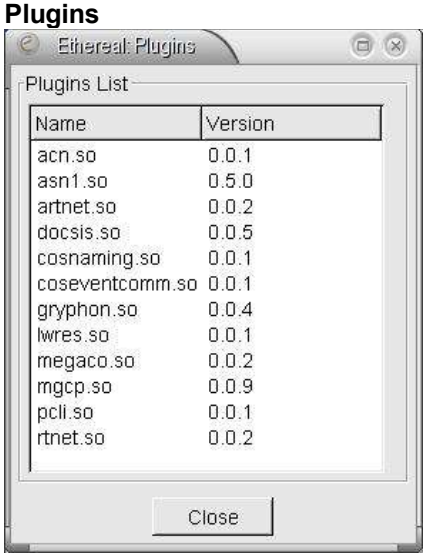

Рисунок 20 Диалоговое окно Plugins

Команда **Plugins** выводит на экран одноименное диалоговое окно (рисунок 20) со списком доступных plugin-модулей.

Список модулей показывает имя и номер версии всех найденных в системе подключаемых модулей Ethereal. Поиск модулей выполняется в каталоге **lib/ethereal/plugins/$VERSION** в основном каталоге программы ($VERSION – номер версии программы). Отметим, что каждый модуль может поддерживать не один протокол, поэтому не пытайтесь найти модель для каждого протокола. Анализ поддерживаемых подключаемыми модулями протоколов можно включать и отключать с помощью команды меню **Edit:Protocols** (стр. 9).

Follow TCP Stream

При выборе в списке пакета TCP или использующего этот протокол пакета вышележащего уровня, команда **Follow TCP Stream** открывает новое окно (см. рисунок 21), содержащее информацию из потока данных соединения TCP, к которому относится указанный в списке пакет. При этом в списке пакетов основного окна Ethereal автоматически активизируется фильтр отображения, показывающий только пакеты, относящиеся к данному соединению TCP. Для отключения этого фильтра можно использовать кнопку **Reset** в нижней части окна программы (справа от поля **Filter**).

Диалоговое окно **Follow TCP stream** позволяет просматривать весь поток данных для выбранного соединения TCP или потоки в отдельных направлениях и обеспечивает вывод информации в формате ASCII, EBCDIC, Hex Dump (дамп отдельных пакетов в текстовом и шестнадцатеричном формате) или C Arrays (массив шестнадцатеричных значений в формате языка C).

Содержимое окна можно напечатать с использованием опций команды меню **File:Print Packet** (стр. 7) или сохранить в текстовом файле. Цвета вывода в окне можно изменить с помощью страницы **TCP Streams** (стр. 22) диалогового окна **Preferences**.

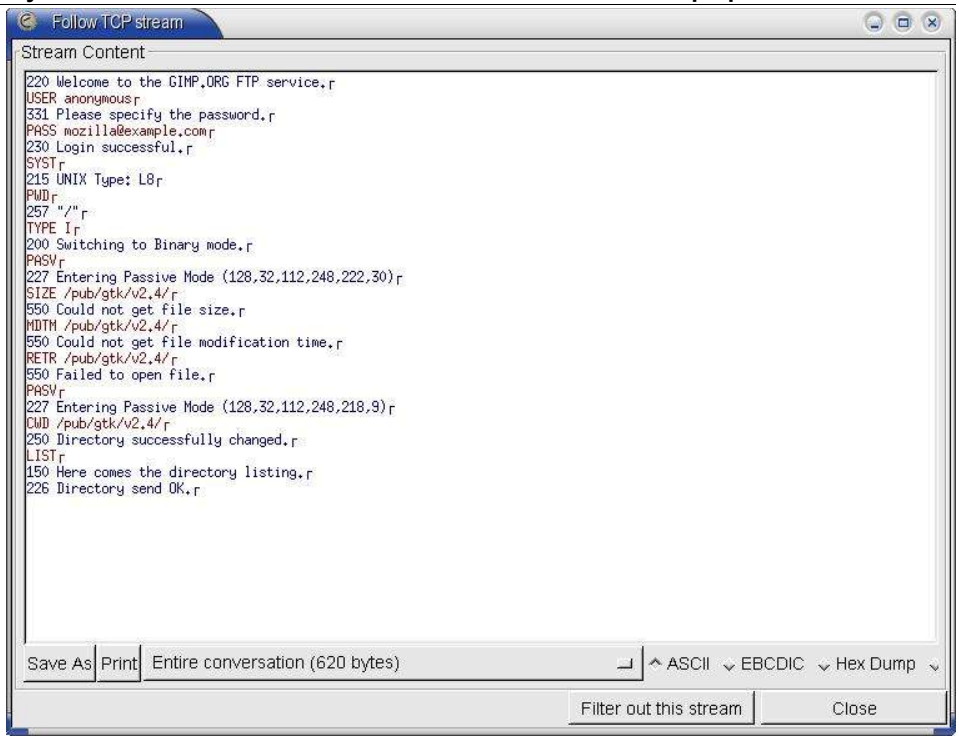

Рисунок 21 Окно вывода данных для выбранного соединения TCP

Decode As

Команда **Decode As** позволяет для выбранного в списке пакета задать тип декодирования, отличный от принятого по умолчанию. Например, вы можете попытаться декодировать пакеты пакеты TCP, адресованные в порт 10000, который используется программой Webmin, как пакеты HTTP[12] и видеть дерево протоколов в соответствии с выбранной трактовкой пакетов. Можно с помощью этой команды выполнить и обратную операцию – отказаться от принятого по умолчанию декодирования для указанного в списке кадра.

Активизируемое по этой диалоговое окно команде Decode As включает панель выбора для каждого из уровней, которые поддерживаются для выбранного в списке кадра (канальный, сетевой и транспортный), позволяя задать отображение при декодировании независимо для каждого уровня. Поля выбора **Decode**/**Do not decode** задают режим смены типа декодирования или отказа от принятого типа декодирования, соответственно.

Кнопка **OK** закрывает диалоговое окно и выполняет заданные в нем операции, **Apply** выполняет заданные операции, не закрывая окна, а **Cancel** закрывает окно без изменения существующей схемы декодирования. Кнопка **Show Current** выводит на экран список заданных пользователем изменений схемы декодирования протоколов (стр. 13).

Go To Corresponding Frame

Если выбранное поле в панели дерева протоколов содержит номер кадра, данная команда обеспечивает переход к соответствующему кадру в списке. Такая возможность обеспечивается только в тех случаях, когда модуль анализа (dissector), который поместил запись в дерево протоколов, включил туда эту запись как фильтруемое поле, а не просто текст.

Обеспечиваемая этой командой возможность перехода может быть полезна для переходов между запросами и откликами, если номер кадра помещается в дерево протоколов.

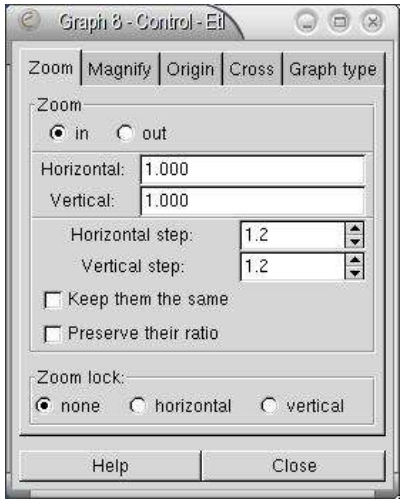

Рисунок 23 Диалоговое окно Graph Control

TCP Stream Analysis

Это субменю обеспечивает группу команд анализа потоков TCP. Управление выводом информации обеспечивается с помощью диалогового окна **Graph Control** (рисунок 23), выводимого при активизации любой из перечисленных здесь команд. Диалоговое окно позволяет задавать параметры отображения информации и выбирать тип отображения.

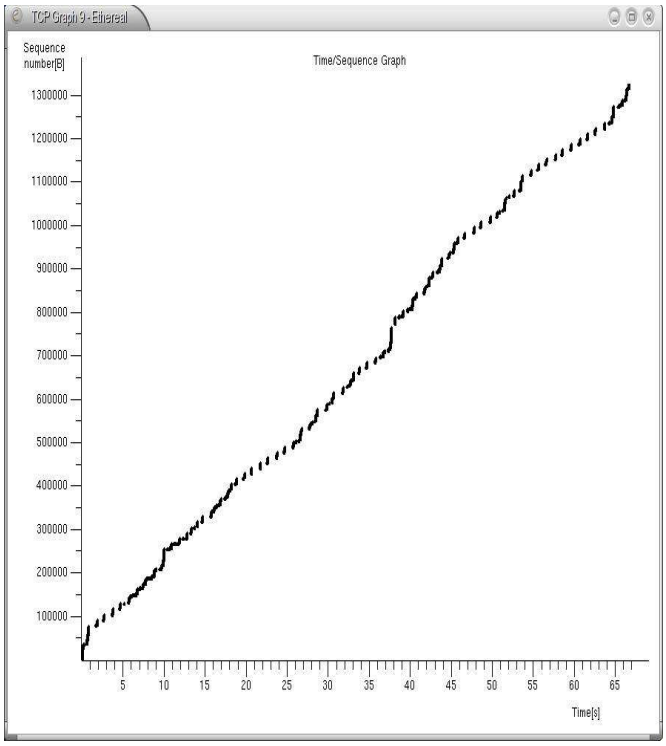

Рисунок 24 График роста порядковых номеров TCP (формат Stevens)

Time-sequence Graph (Stevens)

Эта команда позволяет увидеть на графике зависимость роста порядковых номеров пакетов TCP от времени, как показано на рисунке 24. Для перехода к просмотру другого типа графика можно использовать страницу **Graph Type** диалогового окна **Graph Control** или соответствующую команду субменю **TCP Stream Analysis**.

[12]Каковыми они обычно и являются.

Time-sequence Graph (tcptrace)

Эта команда позволяет увидеть на графике зависимость роста порядковых номеров пакетов TCP от времени в формате **tcptrace**, как показано на рисунке 25. Для перехода к просмотру другого типа графика можно использовать страницу **Graph Type** диалогового окна **Graph Control** или соответствующую команду субменю **TCP Stream Analysis**.

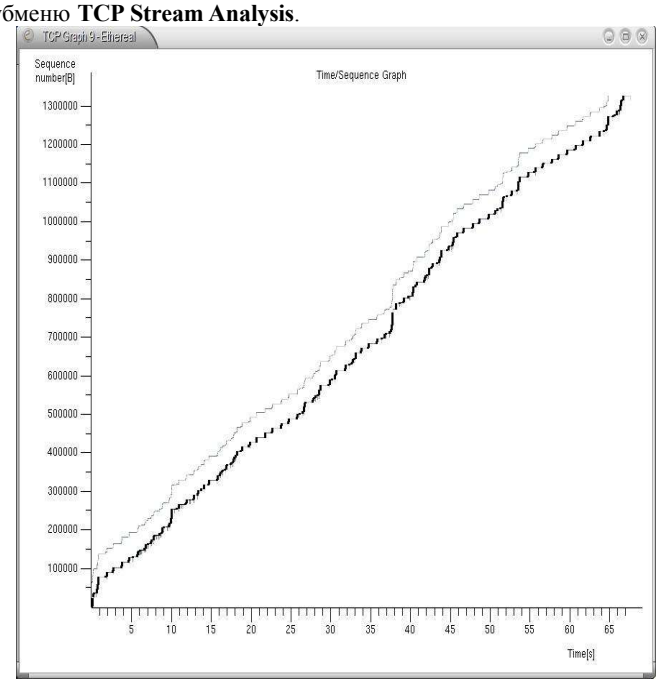

Рисунок 25 График роста порядковых номеров TCP (формат tcptrace)

Throughput Graph

Эта команда позволяет увидеть на графике зависимость потока данных через соединение TCP от времени, как показано на рисунке 26. Для перехода к просмотру другого типа графика можно использовать страницу **Graph Type** диалогового окна **Graph Control** или соответствующую команду субменю **TCP Stream Analysis**.

RTT Graph

Эта команда позволяет увидеть на графике временную зависимость RTT (время кругового обхода) для соединения TCP, как показано на рисунке 27. Для перехода к просмотру другого типа графика можно использовать страницу **Graph Type** диалогового окна **Graph Control** или соответствующую команду субменю **TCP Stream Analysis**.

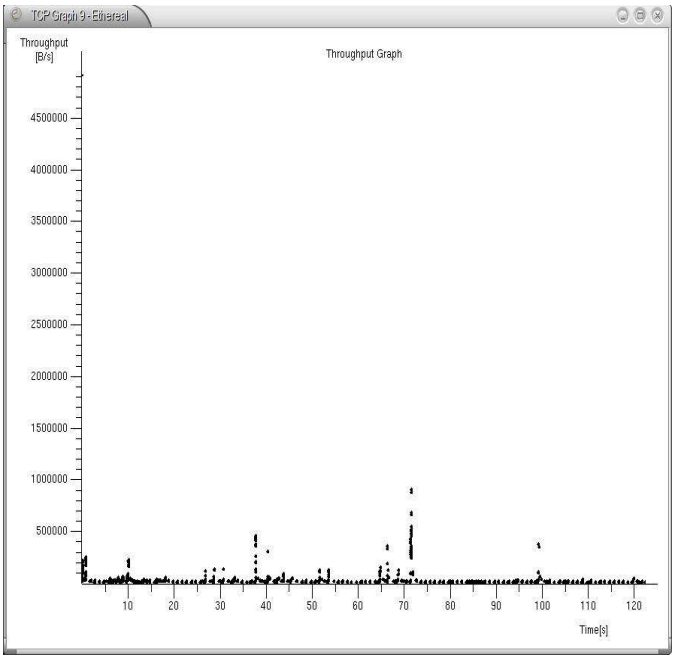

Рисунок 26 График зависимости потока данных через соединение TCP

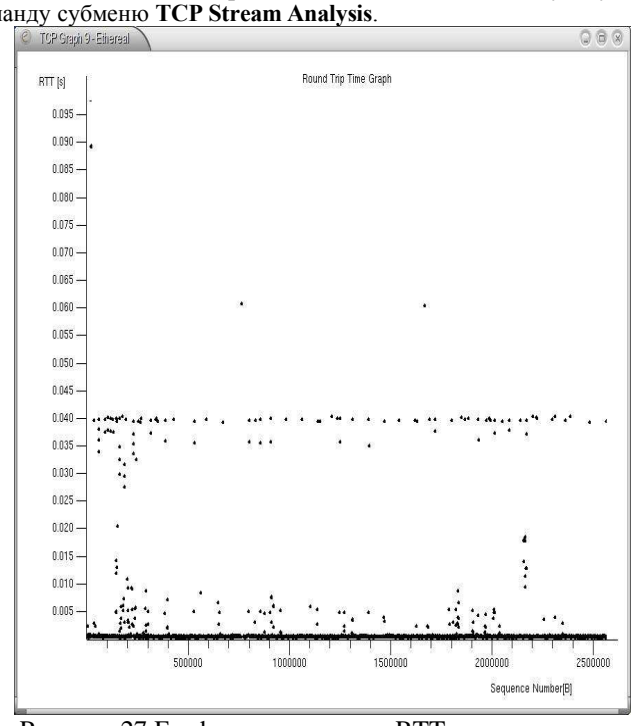

Рисунок 27 График зависимости RTT от времени для соединения TCP

Summary

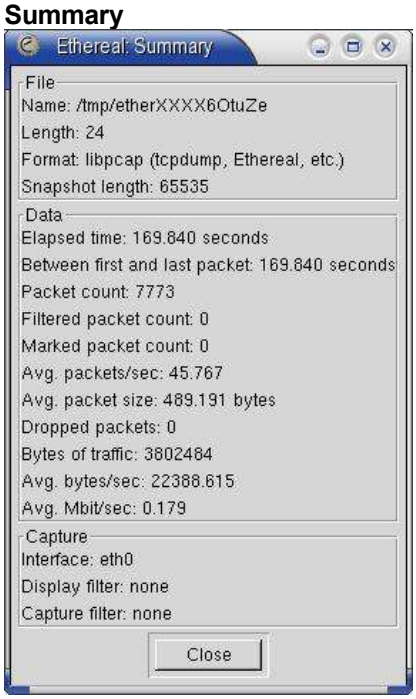

Рисунок 28 Диалоговое окно Summary

Эта команда обеспечивает вывод на экран одноименного диалогового окна (рисунок 28), содержащего сведения общего характера о текущем или последнем завершенном сеансе сбора пакетов (имя файла захвата и его формат, размер кадра захвата, продолжительность сбора пакетов, их число, статистика использования фильтров и т. п.).

Protocol Hierarchy Statistics

Эта команда активизирует одноименное диалоговое окно (рисунок 29), содержащее статистические сведения о распределении пакетов по протоколам за время сбора кадров. Для каждого протокола в иерархии указывается число пакетов и байтов, а также процент от общего трафика. Кроме того, в отдельной колонке учитываются количество и суммарный размер пакетов, для которых соответствующий протокол явился последним в стеке (т. е., не содержал в себе пакетов других протоколов). Эти счетчики выводятся в колонках **End Packets** и **End Bytes**.

Statistics

Субменю Statistics включает команды просмотра статистической информации, описанные ниже.

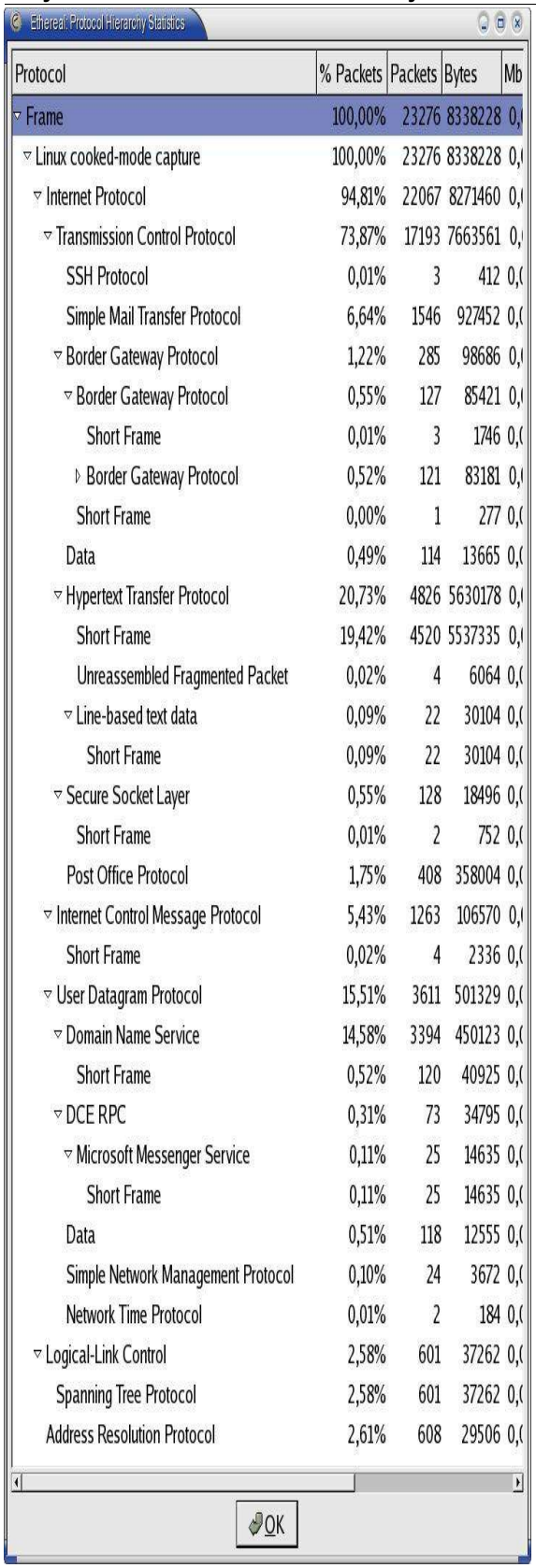

Рисунок 29 Диалоговое окно Protocol Hierarchy Statistics

Watch protocol

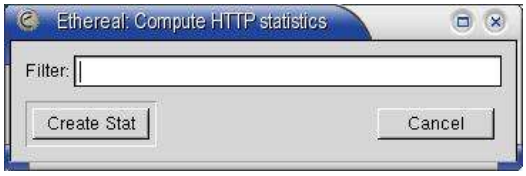

Рисунок 30 Диалоговое окно генерации статистики

Субменю Watch protocol позволяет просматривать статистику для протоколов BOOTP-DHCP, ITU-T H.225, HTTP и WAP-WSP. При активизации любой из команд этого субменю на экране появится диалоговое окно выбора фильтра и генерации статистики, показанное на рисунке 30. Вы можете использовать фильтр для учета соответствующего ему трафика или проста нажать кнопку **Create Stat** для генерации статистики по всем собранным пакетам интересующего протокола. Кнопка **Filter** позволяет выбрать из числа готовых или создать заново фильтр (стр. 8), который будет использоваться для отбора пакетов, принимаемых во внимание при расчете статистики. Выражение для фильтрации пакетов можно задать непосредственно в поле ввода справа от кнопки **Filter**.

BOOTP-DHCP

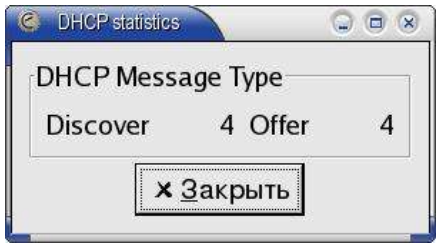

Рисунок 31 Статистика DHCP

Диалоговое окно BOOTP-DHCP содержит статистику использования протоколов удаленной конфигурации хостов, включающую сведения о полученных запросах и откликах серверов DHCP-BOOTP, как показано на рисунке 31.

ITU-T H.225

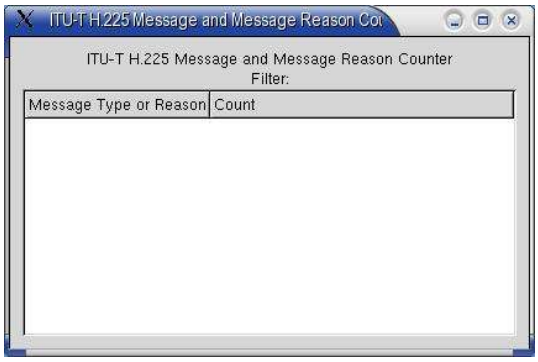

Рисунок 32 Статистика H.225

Диалоговое окно **ITU-T H.225 Message and Message Reason Counter** содержит статистику обмена сообщениями H.225. Форма диалогового окна показана на рисунке 32. Первая колонка списка содержит список сообщений H.225 и вызвавших их причин, а во второй указано количество сообщений в текущем файле захвата. Содержимое окна динамически обновляется в процессе сбора пакетов или загрузки новых файлов данных в программу Ethereal.

Вы можете использовать фильтр для отбора интересующих вас сообщений, указав его в диалоговом окне генерации статистики (см. рисунок 30).

HTTP

Рисунок 33 Статистика HTTP

Диалоговое окно статистики HTTP содержит сведения о количестве запросов и откликов HTTP в собранных программой пакетах. Содержимое окна статистики динамически обновляется при добавлении новых пакетов или загрузке новых файлов захвата. Форма окна статистики HTTP показана на рисунке 33.

Вы можете использовать фильтр для отбора интересующих вас сообщений, указав его в диалоговом окне генерации статистики (см. рисунок 30).

WAP-WSP

Окно статистики WAP-WSP (рисунок 34) включает сведения о количестве пакетов различных типов и данные о состоянии.

При подготовке статистического отчета можно задать фильтр, который позволит просматривать сведения только для интересующего вас трафика. Фильтр указывается в диалоговом окне генерации статистики (см. рисунок 30).

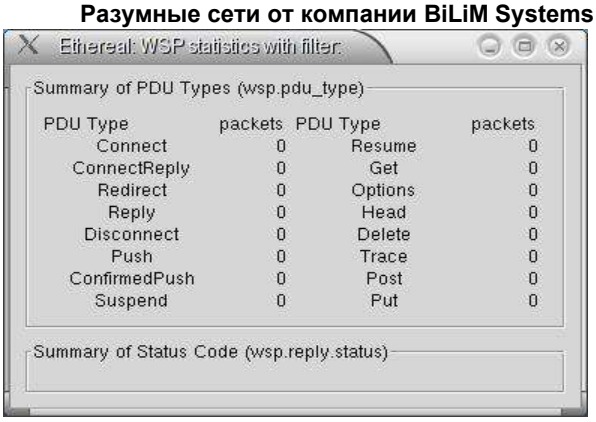

Рисунок 34 Статистика WAP-WSP

Service Response Time

Это субменю позволяет получить статистические сведения о времени отклика различных сетевых приложений и служб. Для выбора программы и номера версии, а также задания фильтра служит диалоговое окно **Compute ... SRT Statistics**, показанное на рисунке 35. Окно включает кнопки выбора программы, для которой генерируется статистика и номера версии. Кнопка **Filter** позволяет выбрать из числа готовых или создать заново фильтр (стр. 8), который будет использоваться для отбора пакетов, принимаемых во внимание при расчете статистики. Выражение для фильтрации пакетов можно задать непосредственно в поле ввода справа от кнопки **Filter**.

DCE-RPC

Рисунок 35 Диалоговое окно генерации статистики SRT

Команда открывает диалоговое окно **Compute DCE-RPC SRT Statistics** (рисунок 35) для выбора программы и номера версии, а также задания фильтра (если вы хотите собрать статистику для части трафика). После выбора опций генерации отчета нажмите кнопку **Create Stat** для генерации статистического отчета. Диалоговое окно статистики DCE-RCP[13] (рисунок 36) включает информацию о количестве вызовов процедур выбранной программы и времени отклика для каждой процедуры (минимальное, максимальное и среднее). Содержимое окна будет автоматически обновляться, если процесс сбора пакетов продолжается.

Fibre Channel

Команда открывает диалоговое окно **Compute Fibre Channel SRT Statistics** (рисунок 35) для задания фильтра (если вы хотите собрать статистику для части трафика). После нажатия кнопки **Create Stat** создается статистический отчет (см. рисунок 37), содержащий в каждой строке тип FC, число вызовов, минимальное, максимальное и среднее время отклика для всех типов FC. Информация в окне автоматически обновляется по мере получения новых пакетов.

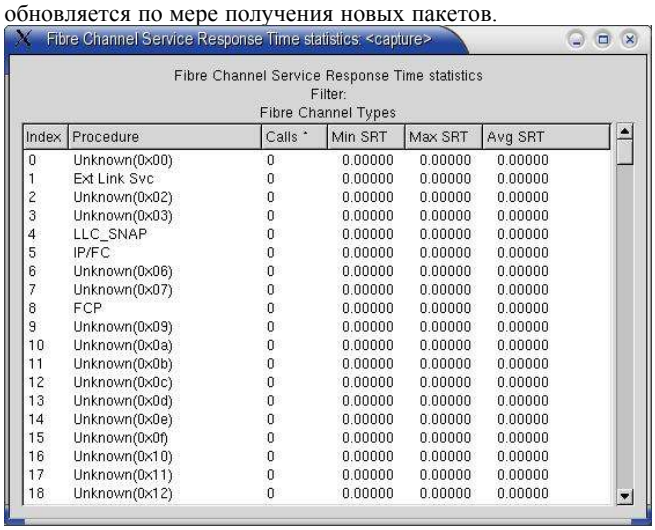

Рисунок 37 Статистика SRT для Fibre Channel

Эта команда служит для генерации и просмотра статистики MGCP[14]. Диалоговое окно **Compute MGCP Statistics** (рисунок 35) позволяет задать фильтр, используемый для генерации статистики. После нажатия кнопки **Create Stat** создается статистический отчет (см. рисунок 38), содержащий в каждой строке тип, сообщение, количество вызовов и время отклика сервиса (минимальное, максимальное и среднее). Статистика выводится для всех известных типов MGCP. Выводимые в отчете значения автоматически обновляются по мере получения новых пакетов MGCP.

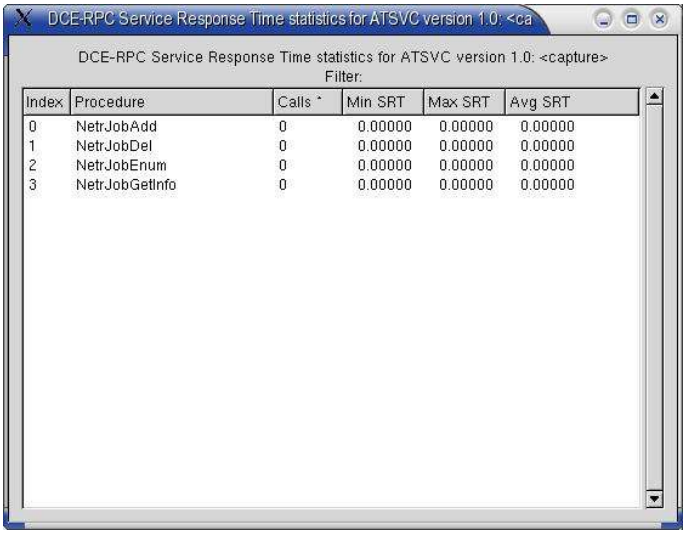

Рисунок 36 Статистика SRT для программ DCE-RPC

Время отклика рассчитывается как интервал между первым и последним кадром сеанса обмена данными.

Если при расчете статистики фильтр не был задан, принимаются во внимание все пары запрос-отклик.

MGCP

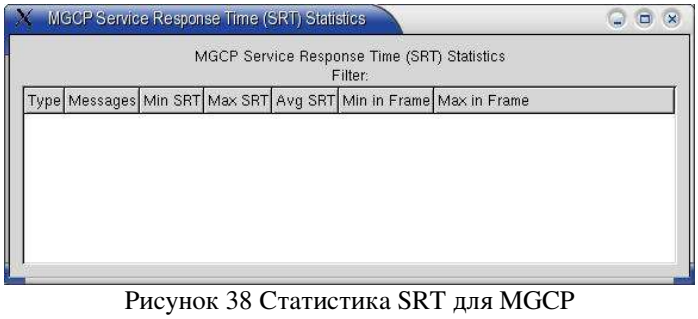

Рисунок 38 Статистика SRT для MGCP

[13]Distributed Computing Environment – среда распределенных вычислений, Remote Procedure Call – удаленный вызов процедур.

[14]Media Gateway Control Protocol – протокол управления шлюзом сред

ONC-RPC

Команда обеспечивает генерацию статистики вызовов ONC-RPC[15] для выбранной в диалоговом окне **Compute ONC-RPC Statistics** (рисунок 35) программы и номера версии. Если вы хотите получить статистику для части трафика, можно использовать фильтр. После нажатия кнопки **Create Stat** создается статистический отчет и на экран выводится диалоговое окно (рисунок 3939), содержащее имена процедур, количество вызовов, минимальное, максимальное и среднее время отклика для всех процедур выбранной версии программы. Если процесс сбора пакетов продолжается, статистические данные в диалоговом окне будут автоматически обновляться.

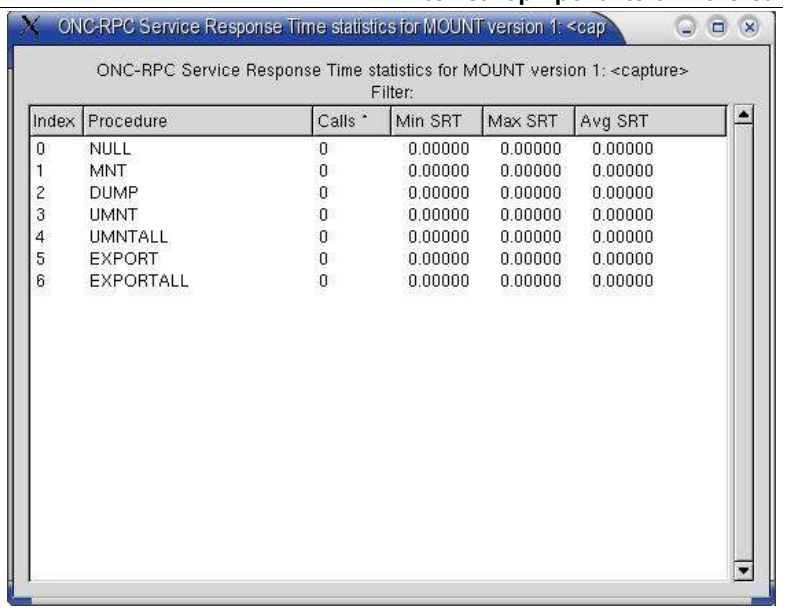

Рисунок 39 Статистика SRT для ONC-RPC

SMB

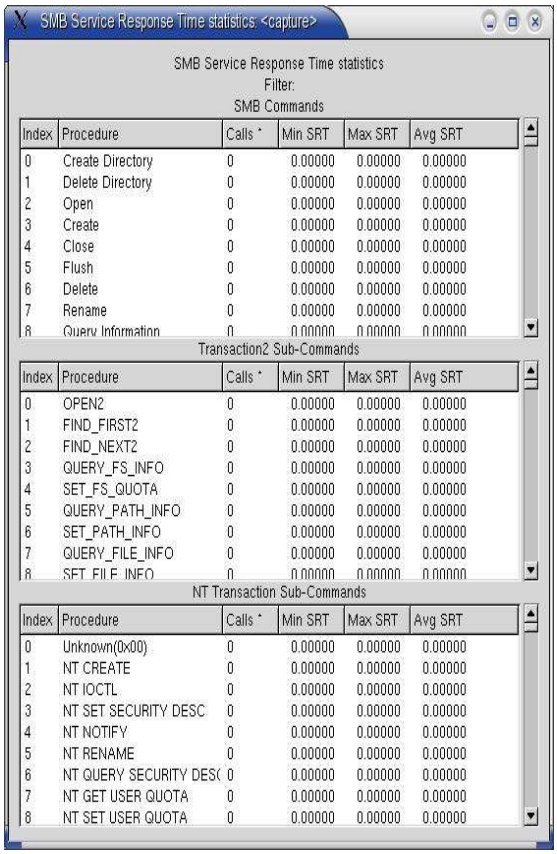

Рисунок 40 Статистика SRT для SMB

Эта команда обеспечивает генерацию и просмотр статистики SRT для трафика SMB. При вызове команды на экране появляется диалоговое окно **Compute ONC-RPC Statistics** (рисунок 35), позволяющее задать фильтр при генерации статистического отчета. После нажатия на кнопку **Create Stat** создается отчет и выводится диалоговое окно (см. рисунок 40), содержащее список всех команд SMB с числом вызовов и временем отклика (минимальное, максимальное и среднее) для каждой команды.

Отчет представляется в форме трех списков, содержащих обычные команды SMB, команды Transaction2 и команды NT Transaction. При расчете статистики используется только первая команда цепочек **xAndX** (т.е., для цепочки **SessionSetupAndX + TreeConnectAndX**)при подготовке статистики будет учитываться только команда **SessionSetupAndX**).

Conversation List

Это субменю позволяет просматривать обмен кадрами между парами конечных точек. Список содержит одну строку для каждого уникального “разговора” - в этой строке указываются адреса узлов, общее количество байтов и пакетов для этого “разговора”, а также количества пакетов и байтов, переданные в каждом направлении. На рисунке 41 показан пример такого списка для протокола IPv4.

По умолчанию строки списка сортируются в порядке убывания числа кадров, но вы можете поменять порядок сортировки, щелкнув кнопкой мыши на заголовке соответствующей колонки. Повторный щелчок по тому же заголовку изменит порядок сортировки на обратный.

Статистика обеспечивается для протоколов:

- Ethernet
- Fibre Channel
- FDDI
- IPv4
- IPX
- TCP (IPv4/v6)
- Token Ring
- UDP (Ipv4/v6)

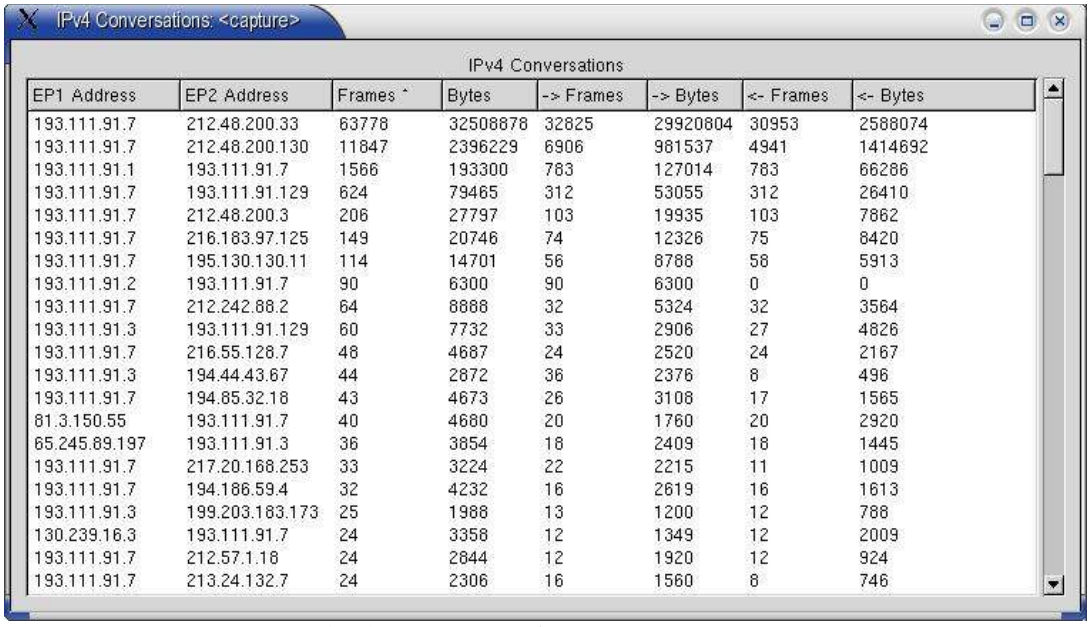

Рисунок 41 Статистика трафика между парами хостов IP

IO

Команда IO-Stat открывает одноименное диалоговое окно (рисунок 42), содержащее до 5 графиков, выведенных

[15]Open Network Computing Remote Procedure Call

различными цветами и показывающих число пакетов или байтов в секунду для кадров, соответствующих каждому из пяти поддерживаемых фильтров. По умолчанию выводится один график, показывающий количество кадров, собранных программой в секунду.

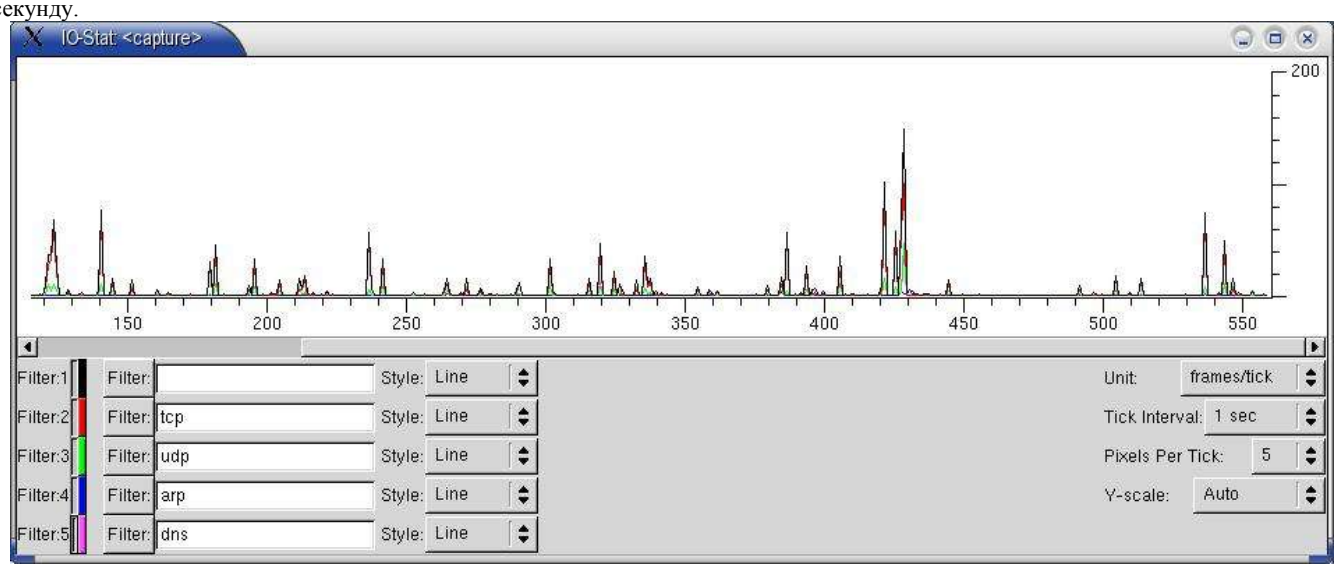

Рисунок 42 Статистика сбора кадров

Верхняя часть окна содержит графики сбора пакетов. При продолжительном сборе данных график перестает помещаться в окне и для возможности его просмотра по частям выводится горизонтальное поле прокрутки. По горизонтальной оси графика откладывается время, а по вертикальной – количественная характеристика скорости сбора пакетов, соответствующих фильтру.

Под графиком размещены элементы управления сбором и выводом статистики. В левой части окна расположены 5 строк, каждая из которых содержит однотипный набор полей:

Элемент	*Описание*
Номер фильтра	Filter1, Filter2, Filter3, Filter4, Filter5
Кнопка активизации	Нажатие кнопки мыши на небольшое поле между номером фильтра и цветовым маркером включает или отключает вывод графика для пакетов, соответствующих данному фильтру.
Цвет графика	Показывает предопределенный цвет[16] вывода графика для данного фильтра.
Кнопка выбора фильтра	Активизирует окно выбора фильтров (стр. 8).
Фильтр	Выражение, используемое для фильтрации при сборе статистики.
Стиль графика	Задает линейный, импульсный или столбчатый график для данного фильтра.

Если поле имени фильтра пусто, соответствующий график будет строиться с учетом всех собранных пакетов (без фильтрации), в противном случае будут приниматься во внимание только пакеты, соответствующие выбранному фильтру.

В правой части окна находятся общие для всех графиков элементы управления выводом.

Элемент	*Описание*
`Unit`	Задает единицы измерения по вертикальной оси (пакеты или байты). Вы можете также выбрать для этого поля значение **advanced...** (см. ниже)
`Tick Interval`	Задает гранулярность отсчета времени для построения графиков (10 мсек, 100 мсек, 1 сек или 10 сек).
`Pixels per Tick`	Задает размер временного интервала на графике в пикселях (1, 2, 5 или 10).
`Y-scale`	Задает масштаб вертикальной оси. Вы можете выбрать одно из приведенных в списке значений или задать режим Auto для автоматического масштабирования.

В режиме **advanced...** каждая строка слева будет включать два дополнительных элемента. Один элемент (текстовое поле) задает имя одного поля используемого для этого графика фильтра отображения, а второй – способ расчета значения – SUM (сумма), COUNT (текущее значение счетчика), MAX (максимум), MIN (минимум), AVG (среднее) или LOAD (загрузка). Значение SUM может использоваться для любых целочисленных полей, COUNT – для всех полей, MAX, MIN и AVG – для численных и временных[17] полей, LOAD – только для временных полей.

Указанное в строке ввода имя поля должно быть частью фильтра, используемого для данного графика, в противном случае вычисление станет невозможным.

Например, для просмотра изменений времени отклика NFS (MAX/MIN/AVG) можно установить для первого графика

```
filter:nfs&&rpc.time Calc:MAX rpc.time
```

для второго

```
filter:nfs&&rpc.time Calc:AVG rpc.time
```

и для третьего

```
filter:nfs&&rpc.time Calc:MIN rpc.time
```

Для просмотра среднего количества размера от хоста **a.b.c.d** можно установить для графика

```
filter:ip.addr==a.b.c.d&&frame.pkt_len Calc:AVG frame.pkt_len
```

[16]Изменение цвета графика возможно только при включенной поддержке GTK+ версии 2.x
[17]время отклика

ONC-RPC

Programs

Эта команда активизирует диалоговое окно, содержащее статистические данные RTT[18] для всех программ ONC-RPC, с которыми связаны пакеты из файла захвата. Выводимые сведения включают имя и номер версии программ, типы вызовов RPC, а также минимальное, максимальное и среднее время кругового обхода.

Рисунок 43 Статистика RTT для программ ONC-RPC

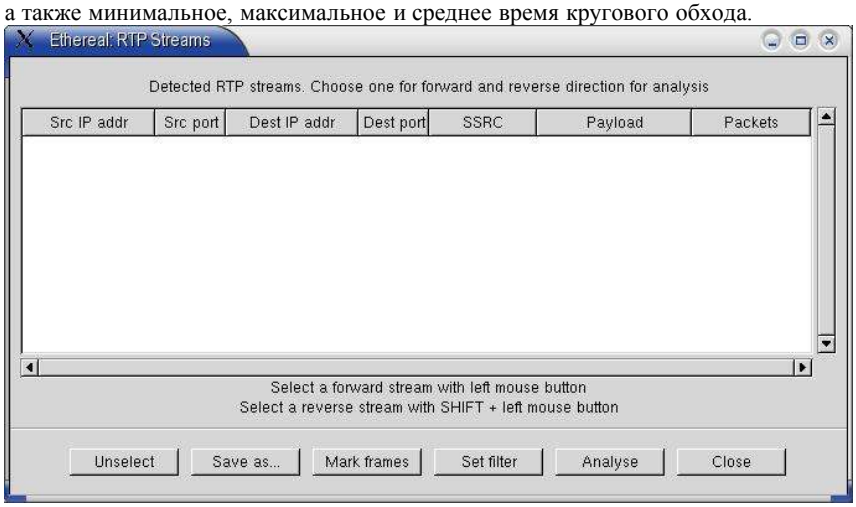

Рисунок 44 Диалоговое окно RTP Streams

RTP Streams

Это субменю позволяет генерировать и просматривать статистику трафика для приложений, работающих в реальном масштабе времени на базе протокола RTP[19].

Show All

Это диалоговое окно выводит информацию обо всех потоках RTP, для которых были собраны пакеты, включая адреса и номера портов, источник синхронизации, тип данных, число пакетов. Формат окна показан на рисунке 44.

Выбрав в списке интересующий вас поток RTP, вы можете проанализировать этот поток (кнопка Analyse).

Для списка доступных потоков обеспечивается возможность записи на диск, маркировки кадров, фильтрации и анализа.

Analyse

Результаты анализа выбранных потоков RTP выводятся в диалоговом окне **RTP Stream Analysis** (см. рисунок 45). В окне выводится список пакетов проанализированного потока с указанием порядковых номеров, задержки и ее флуктуаций, маркеров и состояния.

Кроме того, в нижней части диалогового окна выводятся сведения для всего потока в целом (число пакетов, число потерянных пакетов, количество пакетов с нарушением порядка доставки). Обеспечивается возможность просмотра списка пакетов для обоих направлений потока RTP.

Вы можете сохранить результаты анализа данных из потока в файле.

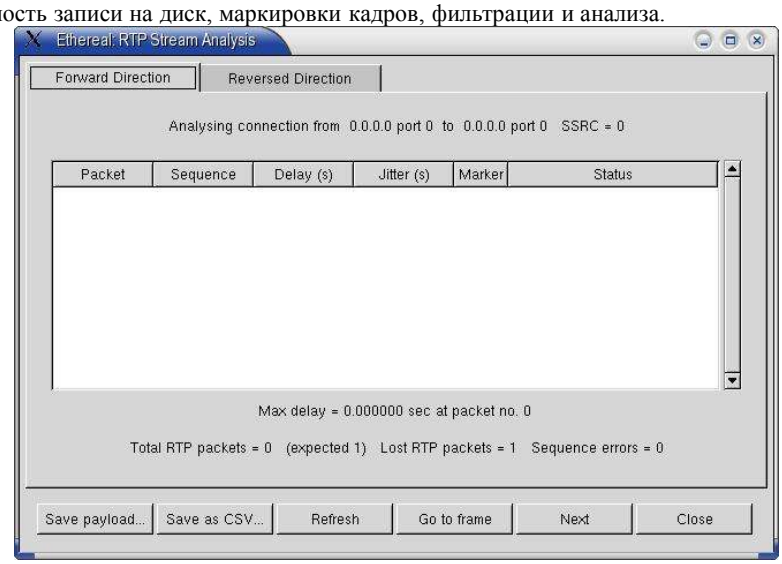

Рисунок 45 Диалоговое окно RTP Stream Analysis

Меню Help

Это меню обеспечивает доступ к справочной системе программы Ethereal. При активизации команды на экране появляется диалоговое окно **Help** (рисунок 46), обеспечивающее доступ к справочной информации. Окно включает 5 страниц:

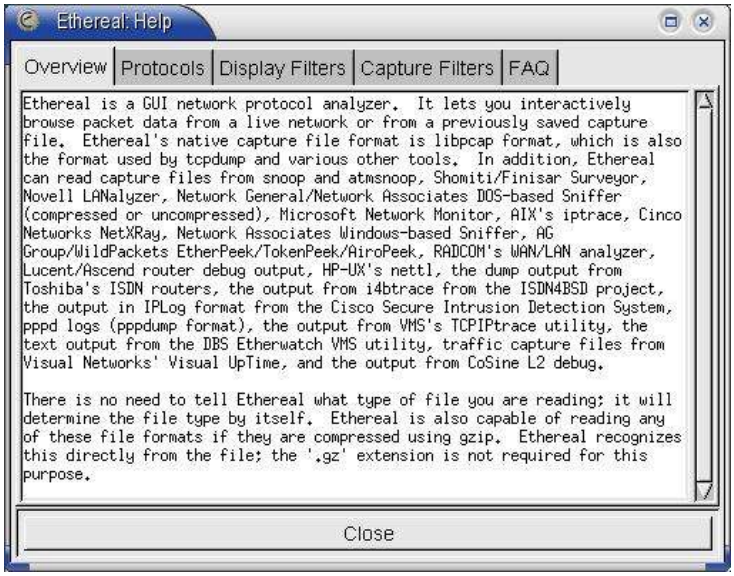

Рисунок 46 Диалоговое окно справочной системы Ethereal

Overview – обзорные сведения о программе.

Protocols – список поддерживаемых протоколов с краткой информацией о них.

Display Filters – информация о возможностях фильтрации выводимых в окне программы пакетов.

Capture Filters - информация о возможностях фильтрации пакетов в процессе их сбора.

FAQ – ответы на часто задаваемые вопросы.

About

Команда About выводит на экран окно с информацией о программе, включающей опции компиляции и версию используемой библиотеки libpcap.

Панель инструментов Ethereal

[18]Round-trip Time – время кругового обхода.
[19]Real Time Protocol

Кнопка	*Действие*
	Инициирует или прерывает процесс сбора пакетов
	Прерывает или прерывает процесс сбора пакетов
	Загружает собранные ранее пакеты из файла (стр. 6)
	Сохраняет собранные программой пакеты в файле (стр. 6)
	Закрывает файл захвата (стр. 6)
	Повторно загружает собранные пакеты из файла (стр. 6)
	Выводит на печать информацию о пакетах (стр. 7)
	Находит пакет, соответствующий заданным условиям (стр. 7)
	Находит следующий пакет (стр. 7)
	Находит в списке пакет по указанному номеру (стр. 7)
	Выводит диалоговое окно **Edit Capture Filters** (стр. 8)
	Выводит диалоговое окно **Edit Display Filters** (стр. 8)
	Выводит диалоговое окно **Ethereal Coloring Rules**
	Выводит диалоговое окно **Prefernces** (стр. 21)
	Выводит на экран диалоговое окно справочной системы (стр. 20)

Диалоговое окно Preferences

Диалоговое окно **Preferences**, активизируемое с помощью команды меню **Edit:Preferences** или кнопки на панели инструментов, позволяет пользователю задать предпочтительные режимы поведения программы Ethereal. Диалоговое окно содержит несколько страниц, переключение между которыми обеспечивается выбором соответствующего элемента из списка в левой части диалогового окна.

Страница Printing

Страница **Printing** служит для управления параметрами печати для команды меню **File:Print Packet** (стр. 7). В двух верхней строках расположены переключатели **Format** и **Print to,** определяющие режим печати. Пакеты могут выводиться в текстовом виде или в формате PostScript на принтер или в файл.

Поле **Command:** позволяет ввести команду, используемую для печати[20], а поле **File:** - имя файла для записи в режиме **File**. Кнопка **File:** открывает диалоговое окно просмотра каталогов и выбора файлов для записи.

Страница Columns

Страница **Columns** позволяет управлять столбцами списка пакетов, выводимого в главном окне программы.

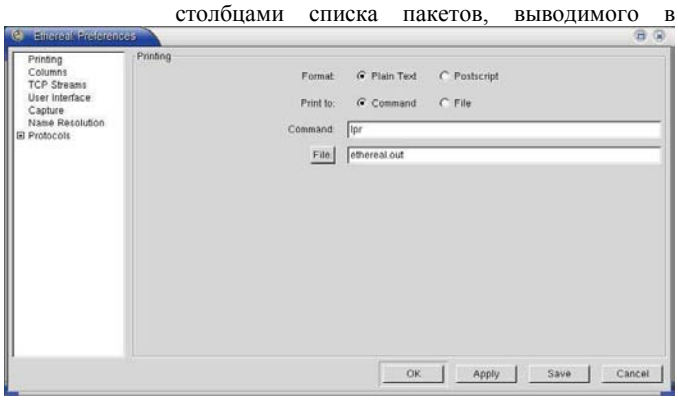

Рисунок 47 Страница Printing

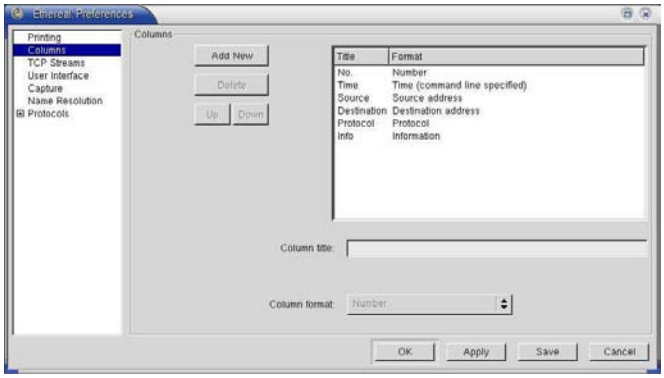

Рисунок 48 Страница Columns

Поле **Title** задает имя столбца, выводимое в заголовке списка пакетов. Для ввода имени новой колонки или изменения существующего имени служит поле ввода **Column title**. Тип данных в столбце определяется выбором одного из элементов списка **Column format**.

Группа кнопок слева от списка столбцов служит для управления отдельными элементами списка. Действия кнопок описаны в таблице 3.

Таблица 3 Кнопки управления колонками списка пакетов Ethereal

Кнопка	*Действие*
Add New	Добавляет в список новую колонку.
Delete	Удаляет из списка указанную колонку.
Up	Перемещает указанную колонку на одну позицию вверх по списку[21].
Down	Перемещает указанную колонку на одну позицию вниз по списку

В нижней части окна расположены кнопки управления списком в целом.

Таблица 4 Кнопки страницы Columns диалогового окна Preferences

Кнопка	*Действие*
OK	Закрывает окно с сохранением внесенных изменений до конца текущего сеанса работы программы. При завершении работы изменения будут потеряны, если вы не воспользуетесь кнопкой Save.
Apply	Эта кнопка не выполняет никаких действий в данном окне.
Save	Сохраняет список столбцов для использования по умолчанию при следующем запуске программы.
Cancel	Закрывает окно без сохранения изменений.

[20]В системах UNIX это поле обычно содержит команду lpr.
[21]В списке пакетов эта колонка будет перемещаться влево.

Отметим, что изменения в структуре списка пакетов реально произойдут только при следующем запуске программы.

Страница TCP Streams

Страница **TCP Streams** позволяет управлять цветами вывода текста в окне **TCP stream** (стр. 13). Для изменения цвета достаточно выбрать атрибут в раскрывающемся списке **Set:** и указать желаемый цвет в поле выбора оттенков. Можно выбрать цвет и с помощью явного задания цветовых компонент. Выбранный текст будет показан в тестовом поле (справа вверху диалогового окна).

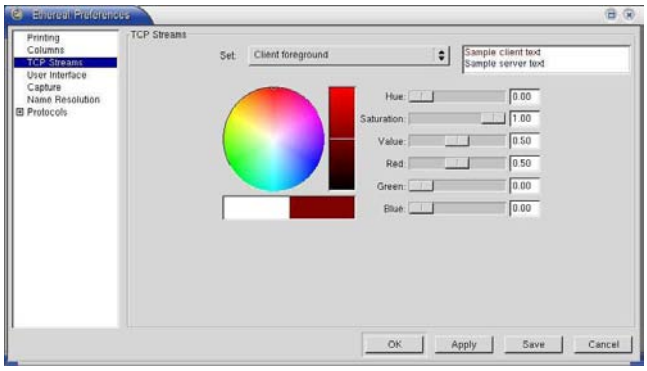

Рисунок 49 Страница TCP Streams

Страница User Interface

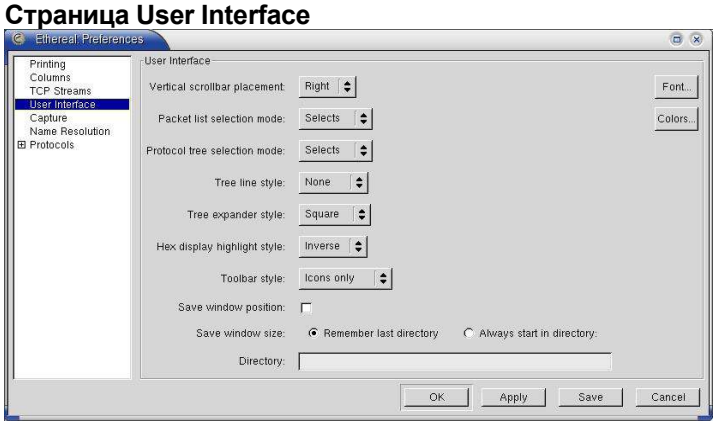

Рисунок 50 Страница User Interface

Страница **User Interface** позволяет задать поведение отдельных элементов графического интерфейса программы:

Элемент	*Назначение*
Vertical scrollbar placement	Позволяет разместить поля прокрутки в панелях главного окна программы справа или слева.
Packet list selection mode	В режиме **Selects** перемещение указателя по списку пакетов приводит к смене содержимого панели дерева протоколов и дампа в соответствии с пакетом, на который установлена строка указателя. В режиме **Browses** перемещение указателя не приводит к изменению содержимого панели дерева протоколов и дампа, пока пакет в списке не будет указан явно (щелчок кнопкой мыши или нажатие клавиши пробела).
Protocol tree selection mode	В режиме **Selects** перемещение указателя по дереву протоколов приводит к смене содержимого панели дампа в соответствии с полем, на которое установлена строка указателя. В режиме **Browses** перемещение указателя не приводит к изменению содержимого панели дампа, пока поле не будет указано явно (щелчок кнопкой мыши или нажатие клавиши пробела).
Tree line style	Задает стиль линий, используемых для вывода дерева протоколов. Дерево может выводиться без соединительных линий (**none**), со сплошными (**solid**) или прерывистыми (**dotted**) линиями, а также в форме закладок (**tabbed**)
Tree expander style	Задает стиль вывода элементов раскрытия/закрытия ветвей дерева протоколов – без значков (**none**), треугольники (**triangle**), квадраты (**square**) и кружки (**circle**). В первом случае для раскрытия или закрытия ветви требуется двойной щелчок кнопкой мыши на соответствующей строке дерева, в остальных случаях достаточно однократного щелчка на соответствующем элементе.
Hex display highlight style	Задает стиль выделения в панели дампа – инверсия цвета (**inverse**) или жирный шрифт (**bold**).
Toolbar style	Задает стиль панели инструментов – пиктограммы (**icons only**), текст (**text only**) или то и другое (**icons & text**)

Поле выбора **Save Window Position** задает сохранение положения окна, а поле **Save Window Size** обеспечивает сохранение размеров окна при следующем запуске программы.

Кнопки **Fonts** и **Colors** в правом верхнем углу окна позволяют выбрать шрифт, используемый в программе и цвет используемый для маркированных кадров.

Страница Capture

Страница **Capture** позволяет управлять параметрами захвата кадров, устанавливаемыми по умолчанию для стартового диалога **Capture Options** (стр. 10).

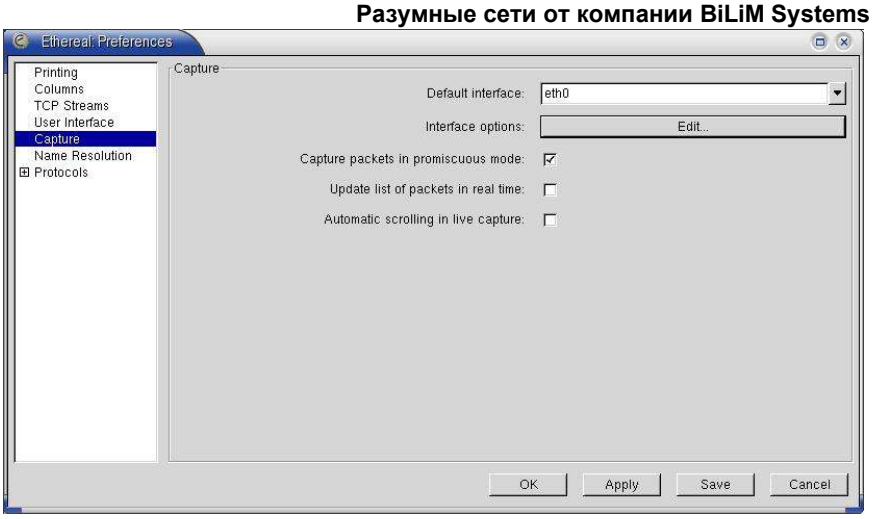

Рисунок 51 Страница Capture

Поле **Default Interface**: (см. рисунок 51) служит для выбора интерфейса или буфера FIFO, который будет служить для сбора пакетов. Фиктивный интерфейс **all** в Linux-системах служит для сбора пакетов со всех интерфейсов системы.

Кнопка **Edit** активизирует диалоговое окно **Inreface Options** (рисунок 52), позволяющее выбрать некоторые опции интерфейса.

Поле выбора **Capture packets in promiscuous mode** определяет режим в котором должен находиться интерфейс, собирающий пакеты. В обычном режиме интерфейс будет принимать из среды только те кадры, в которых указан адрес канального уровня данного интерфейса. Режим захвата позволяет интерфейсу принимать из среды все передаваемые через нее кадры.

Поле выбора **Update list of packets in real time** позволяет задать режим обновления списка пакетов при “живом” захвате. Если вы поставите отметку в этом поле, пакеты будут появляться в списке на панели Ethereal по мере их захвата. В противном случае список пакетов появится только после завершения процедуры сбора пакетов.

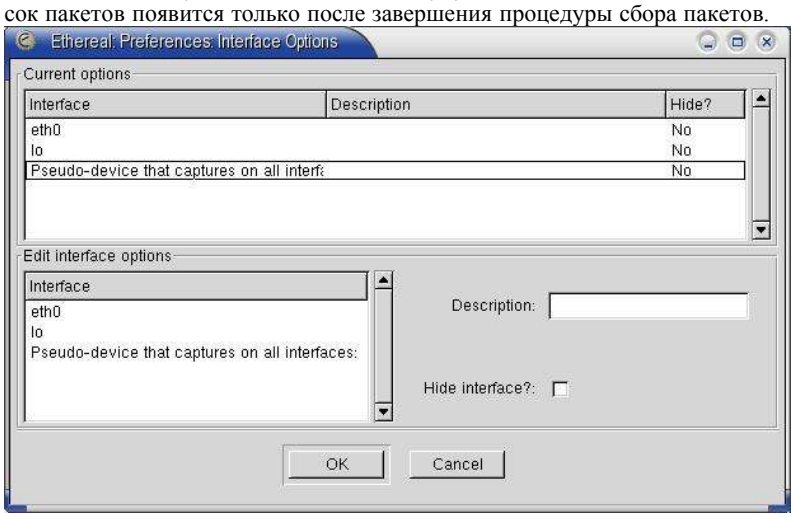

Рисунок 52 Диалоговое окно Inreface Options

Поле выбора **Automatic scrolling in live capture** обеспечивает управление режимом прокрутки списка пакетов при включенной опции обновления списка в реальном масштабе времени. Если вы отметите это поле, список собранных программой пакетов будет автоматически прокручиваться вверх так, чтобы последний пакет всегда находился в видимой части списка.

Диалоговое окно Inreface Options

Этот диалог служит для управления списком доступных интерфейсов, появляющимся на странице **Capture** диалогового окна **Preferences** и в окне выбора опций захвата кадров **Capture Options** (стр. 10). Вы можете изменить описание появляющихся в списке интерфейсов (поле **Description**)или спрятать (поле **Hide**) некоторые интерфейсы, чтобы они не включались в список доступных.

Кнопка **OK** служит для сохранения внесенных изменений, а кнопка **Cancel** закрывает диалоговое окно без сохранения результатов.

Страница Name Resolutions

Страница **Name Resolutions** (рисунок 53) управляет преобразованием адресов канального, сетевого и транспортного уровней в символьные имена.

Поле	*Назначение*
Enable MAC name resolutions	Включает или выключает преобразование MAC-адресов в символьные имена. Преобразование адресов осуществляется с использованием файлов **/etc/ethers** и **$HOME/.ethereal/ethers**, а при отсутствии такой записи адреса преобразуются в соответствии с записями из файла **manuf** программы Ethereal
Enable network name resolutions	Включает или выключает преобразование адресов сетевого уровня в имена хостов.
Enable transport name resolutions	Включает или выключает преобразование номеров портов транспортного уровня в символьные имена связанных с портами служб.

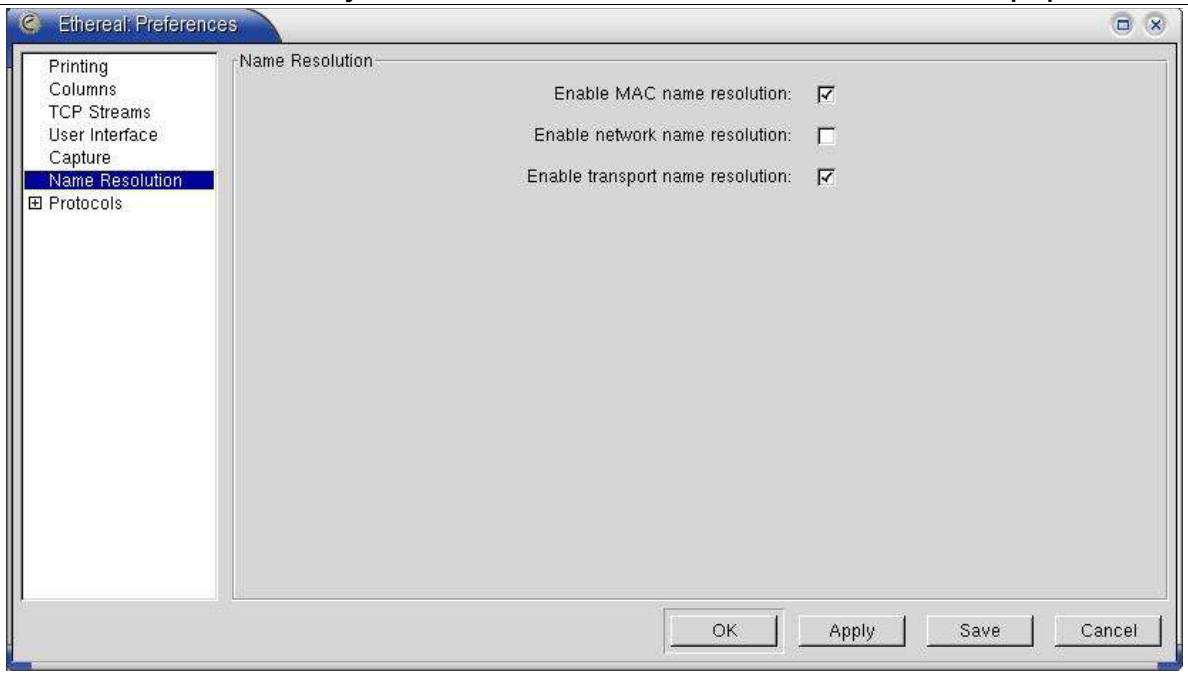

Рисунок 53 Страница Name Resolutions

Страница Protocols

Эта страница (см. рисунок 54) служит для управления опциями трактовки полей отдельных протоколов, обрабатываемых программой Ethereal. Набор доступных опций зависит от выбранного протокола

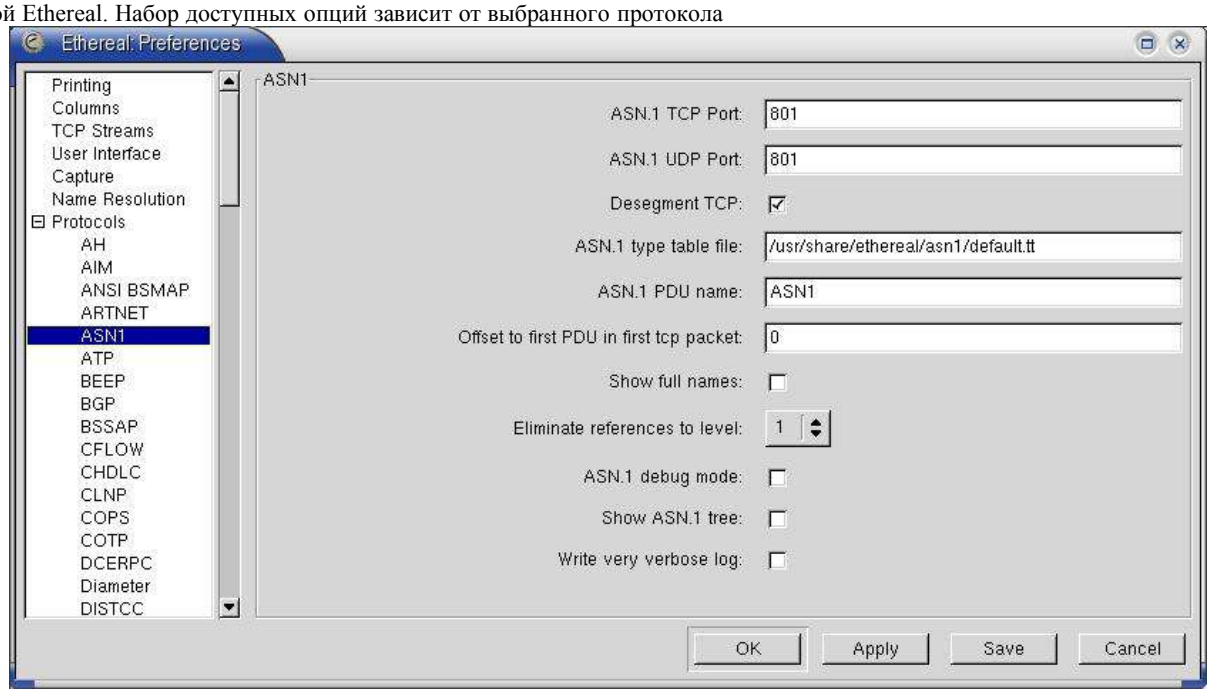

Рисунок 54 Страница Protocols

Фильтры сбора пакетов

Фильтры, используемые при сборе пакетов, работают точно так же, как фильтры tcpdump и используют аналогичный синтаксис.

Фильтры отображения

Программы **Ethereal** и **Tethereal** (стр. 27) поддерживают мощный язык фильтров отображения, позволяющий выводить для просмотра и анализа только интересующие пакеты из числа собранных этой или другой программой захвата. Полное описание системы фильтров отображения можно получить по команде **man ethereal-filter**.

Фильтры отображения позволяют выбирать пакеты на основе сравнения полей с заданными значениями, одного поля с другим или проверки существования указанных полей или протоколов.

Фильтры могут также использоваться для подготовки статистических отчетов (стр. 16 и стр. 17) или цветовой маркировки пакетов в списке пакетов Ethereal (стр. 12). В последующих параграфах описывается синтаксис фильтров отображения.

Синтаксис фильтров

Простейший фильтр позволяет проверить для кадра присутствие протокола или поля. Если вы хотите получить в списке все кадры, содержащие пакеты IPX, фильтр будет состоять лишь из идентификатора этого протокола - **ipx**. Для просмотра кадров Token Ring, содержащих поле RIF можно использовать выражение **tr.rif**.

Фильтры могут также использовать операции сравнения, перечисленные в таблице 5. Для записи операторов сравнения может использоваться синтаксис, подобный принятому в языке C, или сокращенная запись соответствующих терминов английского языка.

Таблица 5 Операции в фильтрах отображения

C	*Английский термин*	*Операция*
==	**eq**	равно
!=	**ne**	Не равно
>	**gt**	больше
<	**lt**	меньше
>=	**ge**	больше или равно
<=	**le**	меньше или равно
	contains	содержит протокол, строку или последовательность байтов

Каждое поле протокола, используемое в фильтрах отображения, имеет определенных тип. Поддерживаемый набор типов полей перечислен в таблице .

Таблица 6 Типы полей в фильтрах отображения

Обозначение	*Тип поля*
Unsigned integer	Беззнаковое целое число размером 6, 16, 24 или 32 бита.
Signed integer	Целое число со знаком размером 6, 16, 24 или 32 бита.
Boolean	Логическое значение.
Ethernet	MAC-адрес Ethernet (6 байтов).
Byte string	Строка байтов.
IPv4	Адрес IPv4 (4 байта).
IPv6	Адрес IPv6 (16 байтов).
IPX	Номер сети IPX.
String	Строка символов.
Double-precision floating point	Действительное число с плавающей запятой.

Целые числа могут задаваться в десятичном, восьмеричном или шестнадцатеричном формате. Например, три приведенных ниже выражения эквивалентны одно другому:

```
frame.pkt_len > 10
frame.pkt_len > 012
frame.pkt_len > 0xa
```

Логические поля могут принимать значения **true** (1) или **false** (0). В фильтрах отображения применяются только числовые эквиваленты логических значений. Например, для выбора кадров Token Ring с установленным полем source-routed может использоваться выражение:

```
tr.sr == 1
```

Адреса Ethernet и строки байтов представляются в шестнадцатеричной записи с разделением байтов двоеточием, точкой или дефисом:

```
fddi.dst eq ff:ff:ff:ff:ff:ff
ipx.srcnode == 0.0.0.0.0.1
eth.src == aa-aa-aa-aa-aa-aa
```

Если строка байтов содержит единственный байт, он представляется как целое число без знака. Т.е., если вы хотите проверить наличие в однобайтовом поле значения **ff**, вы должны сравнивать поле с **0xff** (а не с **ff**).

Адреса IPv4 представляются в десятичном формате с разделением байтов точками или задаются именами хостов:

```
ip.dst eq www.mit.edu
ip.src == 192.168.1.1
```

Адреса IPv4 можно сравнивать как числовые значения с использованием операций **eq**, **ne**, **gt**, **ge**, **lt** и **le**. При проверке адресов IPv4 может использоваться CIDR-нотация[22], если проверяемые адреса относятся к одной подсети. Например, для вывода списка всех адресов из сети класса B 129.111 можно воспользоваться выражением:

```
ip.addr == 129.111.0.0/16
```

Помните, что число справа от дробной черты указывает количество битов, используемых для представления номера сети. Нотацию CIDR можно использовать даже с именами хостов. Например, для выбора всех пакетов из сети класса C, к которой относится хост **sneezy** можно использовать выражение:

```
ip.addr eq sneezy/24
```

Нотацию CIDR можно использовать только с константами (адресами IP или именами хостов), но не с переменными. В частности, выражения типа

```
ip.src/24 == ip.dst/24
```

являются некорректными.

Сети IPX указываются 32-битовыми целыми числами без знака. Обычно для задания этих номеров используют шестнадцатиричное представление:

[22]Classless InterDomain Routing – бесклассовая междоменная маршрутизация. Спецификации CIDR приведены в RFC 1518 и RFC 1519, которые можно загрузить с сайта http://rfc-editor.org/rfc/ или найти в каталоге Documents/ приложенного к книге компакт-диска.

```
ipx.srcnet == 0xc0a82c00
```

текстовые строки указываются в двойных кавычках:

```
http.request.method == "POST"
```

Если строка содержит двойные кавычки, следует использовать символ обратной дробной черты перед знаком кавычек внутри строки или указывать взамен символа кавычек его шестнадцатеричный или восьмеричный код. Ниже приведены примеры использования этих вариантов:

```
browser.comment == "An embedded \" double-quote"
browser.comment == "An embedded \0x22 double-quote"
browser.comment == "An embedded \042 double-quote"
```

Если внутри строки используется символ \ его следует задавать последовательностью \\. Например, для вывода пакетов, содержащих строку **\\SERVER\SHARE** в поле **smb.path** следует задавать выражение:

```
smb.path contains "\\\\SERVER\\SHARE"
```

Существует возможность проверки наличия подстроки в поле любого протокола. Например, для проверки принадлежности адреса Ethernet определенному производителю (три старших байта MAC-адреса) можно воспользоваться выражением:

```
eth.src[0:3] == 00:00:83
```

Если для проверки используется только один байт поля, можно задавать для проверки шетнадцатеричное значение байта без префикса **0x**:

```
llc[3] == aa
```

Проверку подстроки можно использовать не только для полей, но и для любой последовательности байтов в кадре. Помните, что кадр канального уровня содержит пакет целиком и любое поле этого пакета можно задать в формате **смещение:размер**. и для имен протоколов. Например, выражение

```
eth[0x1a:3] == d4:30:c8
```

позволяет показать пакеты, отправленные всеми станциями нашей локальной сети 212.48.200.0/24[23]. Для выборки полей по смещению можно использовать несколько вариантов синтаксиса:

[i:j] – i задает стартовое смещение, j – размер;

[i-j] – i задает первый байт, j – последний (включительно);

[i] – i задает смещение для единственного сравниваемого байта;

[:j] – стартовое смещение равно 0, j задает размер;

[i:] – i задает стартовое смещение и данные считываются до конца поля.

Для смещения и размера можно использовать отрицательные значения. В этом случае отсчет ведется от конца поля. Например, для проверки последних 4 байтов кадра можно использовать выражение :

```
frame[-4:4] == 0.1.2.3
```

или

```
frame[-4:] == 0.1.2.3
```

Можно задать сложную выборку байтов, задавая смещения и диапазоны с использованием запятых и дефисов:

```
field[1,3-5,9:] == 01:03:04:05:09:0a:0b
```

Все описанные выше проверки можно комбинировать с использованием логических выражений, задаваемых в стиле языка C или сокращениями английских терминов:

and (**&&**) - логическая операция AND (И);

or (||) - логическая операция OR (ИЛИ);

not (**!**) - логическая операция NOT (отрицание).

Для группировки выражений можно использовать скобки. Ниже приведены примеры корректных выражений с использованием скобок и логических операций:

```
tcp.port == 80 and ip.src == 192.168.2.1
not llc
(ipx.srcnet == 0xbad && ipx.srnode == 0.0.0.0.0.1) || ip
tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29
```

Особенно аккуратно следует относиться к полям, которые могут встречаться в пакетах неоднократно. Например, поле **ip.addr** встречается в каждом пакете IP дважды – как адрес получателя и как адрес отправителя пакета. Другим примером может служить поле **tr.rif.ring**, которое также неоднократно появляется в пакете. С учетом сказанного очевидно, что выражения:

```
    ip.addr ne 192.168.4.1
not ip.addr eq 192.168.4.1
```

не являются эквивалентными. Первой строка задает поиск пакетов, в которых существует поле **ip.addr**, значение которого не совпадает с **192.168.4.1**. Очевидно, что этому условию соответствуют пакеты, в которых хотя бы один из адресов отправителя и получателя не равен **192.168.44.1**. Второму правилу соответствуют все пакеты, кроме тех, где хотя бы одно значение **ip.addr** совпадает с **192.168.4.1**. Значит пакеты, в которых адрес отправителя или получателя имеет значение **192.168.4.1**, не будут соответствовать данному фильтру.

Следует также очень аккуратно задавать фильтры при необходимости избавиться от “шума”. Например, если вы хотите исключить из списка все широковещательные пакеты, адресованные хосту **224.1.2.3**, правило:

```
ip.dst ne 224.1.2.3
```

[23]Существует и более естественный способ задания такого фильтра, и приведенное выражение лишь иллюстрирует возможности проверки полей по смещению

будет слишком жестким, поскольку оно будет отбирать только те кадры, в которых существует поле **ip.dst** и значение этого поля не равно указанному. В результате из списка будут удалены все кадры, не содержащие пакетов IP. Лучше будет воспользоваться одним из фильтров:

```
not ip or ip.dst ne 224.1.2.3
not ip.dst eq 224.1.2.3
```

Первое правило обеспечит включение в список кадров, не относящихся к протоколу IP (**not ip**) и пакетов IP, адресованных другим хостам (**ip.dst ne 224.1.2.3**). Второе правило обеспечит включение в список всех кадров, кроме тех, которые содержат указанный адрес IP в поле получателя.

Файлы Ethereal

Файлы **/etc/ethereal.conf** и **$HOME/.ethereal/preferences** содержат глобальные и персональные параметры настройки **Ethereal**, соответственно. Параметры задаются в формате **prefname:value**, где **prefname** совпадает с именем параметра в соответствующем диалоговом окне программы, а поле **value** содержит значение параметра. Между двоеточием после имени параметра и значением допускается использование пробелов и символов табуляции. Часть строки справа от символа # является комментарием.

При загрузке программы сначала просматриваются глобальные параметры, а потом файл персональных настроек.

Протоколы, для которых анализ полей запрещен, указываются в файле **$HOME/.ethereal/disabled_protos**, содержащем список имен протоколов, для которых анализ полей не производится. Каждая строка должна содержать не более одного имени протокола. Текст справа от символа # является комментарием.

Файл **/etc/ethers** служит для преобразования MAC-адресов в символьные имена. Если адрес не найден в этом файле, программа просматривает файл **$HOME/.ethereal/ethers**. Каждая строка такого файла содержит пару адрес-имя. В качестве разделителя между именем и адресом могут использоваться пробелы или символы табуляции, а для разделения байтов адреса могут использоваться двоеточие (:), дефис (-) или точка (.). Ниже приведен пример записей:

```
ff:ff:ff:ff:ff:ff          Broadcast
c0-00-ff-ff-ff-ff          TR_broadcast
00.00.00.00.00.00          Zero_broadcast
```

Файл **/usr/local/etc/manuf**[24] содержит список 3-байтовых идентификаторов, выделенных производителям оборудования. Эти идентификаторы используются для указания в списке пакетов в тех случаях, когда файлы **ethers** отсутствуют или не содержат искомого адреса. Записи в файле имеют формат

```
00:00:0C       Cisco
```

Кроме того, в этом файле перечислены специальные значения MAC-адресов, используемые для тех или иных целей. Например, запись

```
00-00-0C-07-AC/40     All-HSRP-routers
```

будет приводить к появлению в списке адресов поля **All-HSRP-routers** для всех MAC в диапазоне от **00-00-0C-07-AC-00** до **00-00-0C-07-AC-FF**. Размер значимой части специального адреса указывает маска, приведенная справа от дробной черты в строке адреса.

Файл **/etc/ipxnets** связывает 4-байтовые номера сетей IPX с символьными именами. Если искомая сеть не указана в этом файле, программа просматривает файл **$HOME/.ethereal/ipxnets**. Формат этих файлов аналогичен формату файлов **ethers**, но адреса указываются 4-байтовыми значениями вместо 6-байтовых MAC-адресов. Кроме того, номера сетей могут записываться без разделения отдельных байтов.

```
C0.A8.2C.00              HR
c0-a8-1c-00              CEO
00:00:BE:EF              IT_Server1
110f                     FileServer3
```

Файлы **/usr/local/etc/colorfilters** и **$HOME/.ethereal/colorfilters** содержат глобальные и персональные настройки цветовых фильтров, соответственно.

Tethereal

Программа tethereal является текстовым вариантом анализатора Ethereal и поддерживает такие же функции и опции, за исключением тех, которые не применимы к текстовому интерфейсу. Пример вывода программы tethereal показан на рисунке 55.

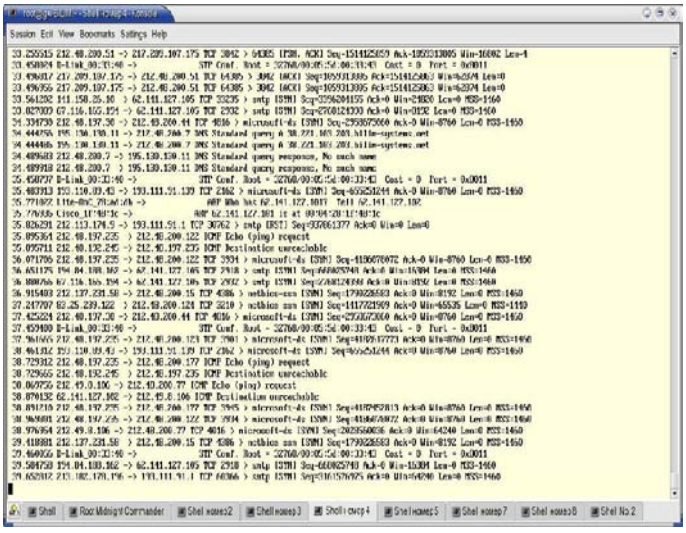

Рисунок 55 Вывод программы Tethereal

Утилиты Ethereal

Пакет Ethereal, кроме анализаторов протоколов с текстовым и графическим интерфейсом, включает утилиты для работы с файлами захвата, собранными Ethereal или другими программами.

Утилиты Ethereal могут читать и сохранять файлы захвата с использованием различных форматов, включая **libpcap** (**tcpdump**, **Ethereal** и др.), **snoop** и **atmsnoop**, **Shomiti/Finisar Surveyor**, **Novell LANalyzer**, **Network General/Network Associates Sniffer** (DOS, сжатые и несжатые/Windows), **Microsoft Network Monitor**, **iptrace** (AIX), Cinco Networks NetXRay, **AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek**, **RADCOM WAN/LAN**, **Lucent/Ascend** (router debug), **nettl** (HP-UX), **дампы ISDN-маршрутизаторов Toshiba**, **i4btrace**, **IPLog** (Cisco Secure IDS), **pppd** (формат pppdump), **VMS TCPIPtrace/TCPtrace/UCX$TRACE**, **DBS Etherwatch VMS** (текстовый формат), **Visual Networks Visual UpTime**, **CoSine L2** (debug), **Accellent's 5Views LAN**, **Endace Measurement Systems ERF**, **Linux Bluez Bluetooth**

[24] В зависимости от параметров компиляции программы Ethereal каталог, где хранится этот файл, может изменяться

(hcidump -w), **Network Instruments Observer** (v9). Утилитам не нужно указывать формат входного файла, он определяется автоматически. Утилиты Ethereal способны также работать со всеми перечисленными форматами файлов, сжатыми с использованием формата gzip, который распознается автоматически.

По умолчанию утилиты сохраняют файлы в формате **libpcap**, записывая в выходной файл все пакеты. Флаг **-F** позволяет задать формат выходного файла (стандартный и модифицированный формат **libpcap**, **snoop**, **Sniffer** (без компрессии), **Microsoft Network Monitor 1.x**, **Visual Networks**).

editcap

Программа **editcap** позволяет удалять пакеты из файлов захвата и обеспечивает преобразование файлов из одного формата в другой.

Синтаксис

```
editcap [-F <формат>] [-T <тип>] [-r] [-v] [-s snaplen] [-t time adjustment] [-h] infile
outfile [record# ...]
```

Опции

Таблица 7 Опции команды editcap

Опция	*Значение*
-F <формат>	Задает формат выходного файла.
-T <тип>	Задает тип инкапсуляции для выходного файла.
-r	Управляет записью в выходной файл пакетов с номерами из списка, указанного в командной строке.
-v	Заставляет **editcap** выводить номер версии при работе программы.
-s <размер>	Задает размер пакетов при записи в выходной файл.
-t <значение>	Задает корректировку временных меток при записи пакетов в выходной файл.
-h	Выводит справочную информацию и завершает работу программы.

В командной строке **editcap** можно указать список номеров пакетов, которые не будут записаны в выходной файл, если не задана опция **-r**, при использовании которой будут записываться только пакеты из указанного списка. Диапазоны номеров пакетов задаются в формате начало-конец.

При использовании в командной строке опции **-s** пакеты из входного файла, имеющие больший размер, усекаются при записи до заданного значения. Это может быть полезно в тех случаях, когда программа анализа не умеет работать с большими пакетами[25].

При использовании флага **-t** корректировка времени осуществляется для всех пакетов выходного файла. Величина корректировки задается числом секунд и знаком. Например, **-t 3600** увеличит на один час значение временных меток для всех пакетов, **-t -0.5** уменьшит значение временных меток на полсекунды. Корректировка временных меток полезна для синхронизации данных, собранных в различных точках сети, если разницу в показаниях локальных часов можно определить или хотя бы оценить.

Задаваемый флагом **-T** тип инкапсуляции для выходного файла является лишь “рекомендательным” - если в заголовке входного пакета явно указан тип инкапсуляции, отличный от заданного опцией и несовместимый с ним, тип инкапсуляции в выходном файле не будет изменен.

Параметр **record# ...** задает список номеров пакетов, записываемых в выходной файл.

mergecap

Утилита **mergecap** позволяет объединить два файла данных (записанные пакеты) в один.

Синтаксис

```
mergecap [-hva] [-s snaplen] [-F <формат>] [-T encapsulation type] -w outfile infile ...
```

Опции

Таблица 8 Опции команды mergecap

Опция	*Значение*
-w	Задает имя выходного файла.
-F <формат>	Задает формат выходного файла.
-T <тип>	Задает тип инкапсуляции для выходного файла.
-a	Заставляет программу игнорировать временные метки и записывать в выходной файл сначала все пакеты из первого входного файла, затем из второго и т. д. По умолчанию пакеты из входных файлов при записи выходного файла упорядочиваются в соответствии с имеющимися в файлах временными метками для каждого пакета[26].
-v	Заставляет editcap выводить номер версии при работе программы.
-s <размер>	Задает размер пакетов при записи в выходной файл.
-h	Выводит справочную информацию и завершает работу программы.

Программа собирает в хронологическом порядке (если не задан флаг **-a**) пакеты из заданных входных файлов и записывает их в выходной файл.

[25]Например программа **snoop** под управление Solaris 2.5.1 и Solaris 2.6 будет отбрасывать кадры Ethernet, размер которых превышает стандартное значение Ethernet MTU, что делает невозможным анализ кадров Gigabit Ethernet с использованием **jumbo**.
[26]Программа предполагает, что пакеты в каждом из входных файлов упорядочены по времени.

При использовании в командной строке опции **-s** пакеты из входного файла, имеющие больший размер, усекаются при записи до заданного значения. Это может быть полезно в тех случаях, когда программа анализа не умеет работать с большими пакетами (см. примечание 26).

Для выходного файла используется такой же тип инкапсуляции, как во входных файлах (если тип инкапсуляции для них совпадает). Если входные файлы используют разные типы инкапсуляции, тип инкапсуляции выходного файла будет помещаться в поля **WTAP_ENCAP_PER_PACKET**[27]. Если поле **WTAP_ENCAP_PER_PACKET** не поддерживается выбранным форматом выходного файла, объединения данных в один выходной файл не происходит.

Задаваемый флагом **-T** тип инкапсуляции для выходного файла является лишь “рекомендательным” - если в заголовке входного пакета явно указан тип инкапсуляции, отличный от заданного опцией и несовместимый с ним, тип инкапсуляции в выходном файле не будет изменен.

[27]Поле WTAP_ENCAP_PER_PACKET поддерживается не всеми форматами файлов захвата. В частности, формат libpcap его не поддерживает.