Длина пакетов

Файл перехвата **download-slow.pcapng**

Размер одного пакета или группы пакетов может сообщить немало интересного о сложившейся ситуации в сети. При обычных обстоятельствах максимальный размер фрейма в сети Ethernet составляет 1518 байт. Если вычесть из этой числовой величины заголовки протоколов Ethernet, IP и TCP, то останется 1460 байт, предназначенных для передачи заголовка протокола седьмого уровня или данных. Если известны минимальные требования к передаче пакетов, то можно начать с анализа распределения длин пакетов в перехваченном трафике, чтобы сделать обоснованное предположение о составе данного трафика. Это очень помогает при попытках понять состав крупных файлов перехвата. Для просмотра распределения пакетов по длине в Wireshark предоставляется диалоговое окно Packet Lengths (Длины пакетов).

Обратимся к конкретному примеру из файла перехвата `download-slow.pcapng`. Открыв его, выберите команду Statistics⇨Packet Lengths из главного меню. В итоге откроется диалоговое окно Packet Lengths, приведенное на рис. 5.16.

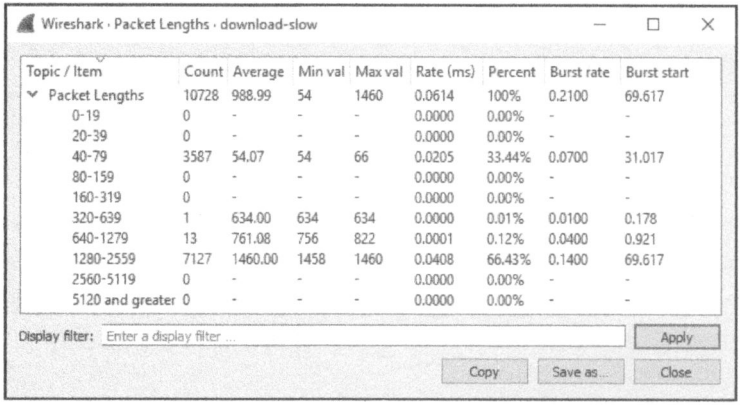

Рис. 5.16. Диалоговое окно Packet Lengths помогает сделать обоснованное предположение о сетевом трафике в файле перехвата

Обратите особое внимание на строку со статическими данными о пакетах длиной от 1280 до 2559 байт. Крупные пакеты вроде этих обычно свидетельствуют о передаче данных, тогда как более мелкие пакеты — о последовательностях управления протоколами. В данном случае наблюдается немалая доля крупных пакетов (66,43%). Даже не просматривая пакеты в файле перехвата, можно сделать вполне обоснованное предположение, что перехваченный трафик содержит одну или несколько передач данных, которые могут принимать форму загрузки по протоколу HTTP, выгрузки по протоколу FTP или любой другой операции в сети, где данные передаются между хостами.

Длина большинства оставшихся пакетов (33,44%) находится в пределах от 40 до 79 байт. К этой категории обычно относятся управляющие пакеты TCP, не несущие полезную информацию. Рассмотрим типичный размер заголовков протоколов. Так, заголовок протокола Ethernet занимает 14 байт (плюс 4 байта на циклический избыточный код CRC), заголовок протокола IP – как минимум 20 байт, а пакет TCP без данных или параметров – те же 20 байт. Это означает, что длина стандартных управляющих пакетов TCP (например, пакетов SYN, ACK, RST и FIN) составит около 54 байт и укладывается в рассматриваемые здесь пределы. Разумеется, эта длина увеличится, если добавить параметры протокола IP или TCP. Более подробно сетевые протоколы IP и TCP рассматриваются в главах 7, "Протоколы сетевого уровня", и 8, "Протоколы транспортного уровня", соответственно.

Анализ длин пакетов позволяет составить общее представление о крупном перехваченном трафике. Если в нем имеется много крупных пакетов, то можно с уверенностью предположить, что в сети передается большой объем данных. Если же длина большинства пакетов невелика, это означает, что передается немного данных, и можно предположить, что перехваченный трафик состоит из команд управления сетевыми протоколами. Но это не правила, которые следует считать непреложными, а всего лишь предположения, помогающие приступить к более углубленному анализу.

Составление графиков

Графики служат основой анализа пакетов и одним из лучших способов получения итогового представления о массиве данных. В состав Wireshark входит несколько средств для составления графиков, помогающих лучше понять перехваченные данные. И в первую очередь – это возможности графического представления ввода-вывода.

Просмотр графиков ввода-вывода

Файлы перехвата **download-fast.pcapng**, **download-slow.pcapng**, **http_espn.pcapng**

В окне IO Graph (График ввода-вывода) предоставляется возможность построить график передачи данных в сети. Такие графики позволяют быстро выявлять всплески и провалы в работе канала связи, обнаруживать задержки в производительности отдельных протоколов и сравнивать параллельные потоки данных.

В качестве примера построения графика ввода-вывода при загрузке файла на компьютер из Интернета обратимся к файлу перехвата `download-fast.pcapng`. Откройте этот файл, щелкните на любом пакете TCP, чтобы выбрать его, и выберите команду Statistics⇨IO Graph из главного меню.

В открывшемся окне IO Graph появится графическое представление потока данных во времени. Как следует из примера, приведенного на рис. 5.17, на данном графике загрузки файла передается около 500 пакетов в секунду. И этот показатель остается постоянным почти до конца графика, где он резко снижается.

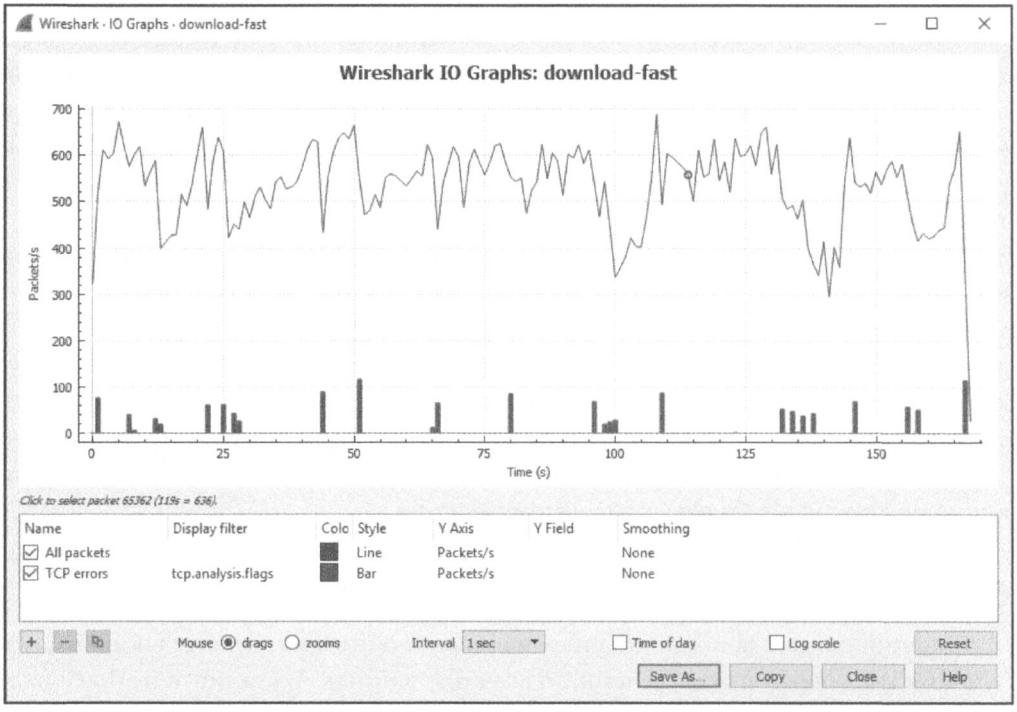

Рис. 5.17. Этот график ввода-вывода демонстрирует практически постоянную скорость передачи пакетов при быстрой загрузке файла

А теперь рассмотрим для сравнения пример более медленной загрузки файла. Оставив открытым текущий файл перехвата, откройте файл перехвата `download-slow.pcapng` в другом экземпляре Wireshark. Составив график ввода-вывода для данного примера загрузки файла описанным выше способом, вы увидите совсем другую картину, как показано на рис. 5.18.

Рассматриваемая здесь загрузка происходит со скоростью от 15 до 100 пакетов в секунду, и такая скорость далека от постоянной, а иногда даже падает до нуля пакетов в секунду. Подобное непостоянство можно лучше увидеть, если расположить рядом графики ввода-вывода обоих файлов, как показано на рис. 5.19. Сравнивая оба графика, обратите особое внимание на значения, откладываемые по осям X и Y, чтобы сравнивать сопоставимые величины. Масштаб в обоих случаях автоматически корректируется в зависимости от количества пакетов и/или объема переданных данных, что составляет главное

отличие сравниваемых графиков. Так, медленная загрузка файла демонстрируется в масштабе от 0 до 100 пакетов в секунду, тогда как быстрая загрузка – от 0 до 700 пакетов в секунду.

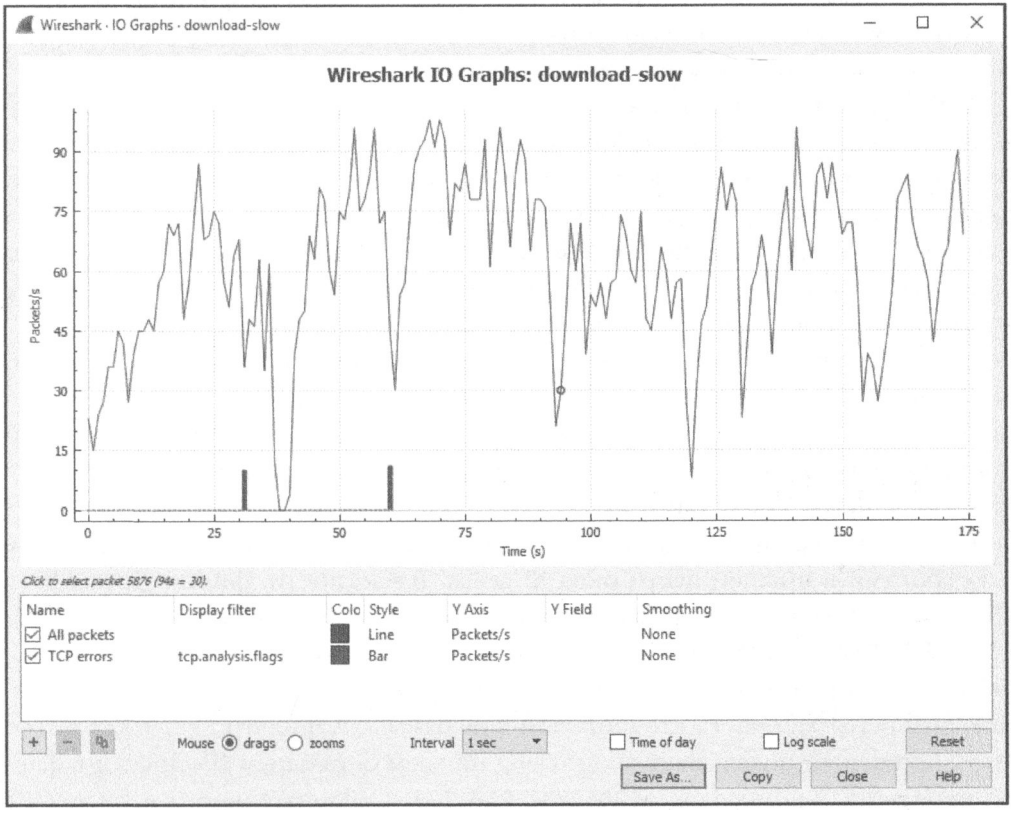

Рис. 5.18. Этот график ввода-вывода демонстрирует непостоянную скорость передачи пакетов при медленной загрузке файла

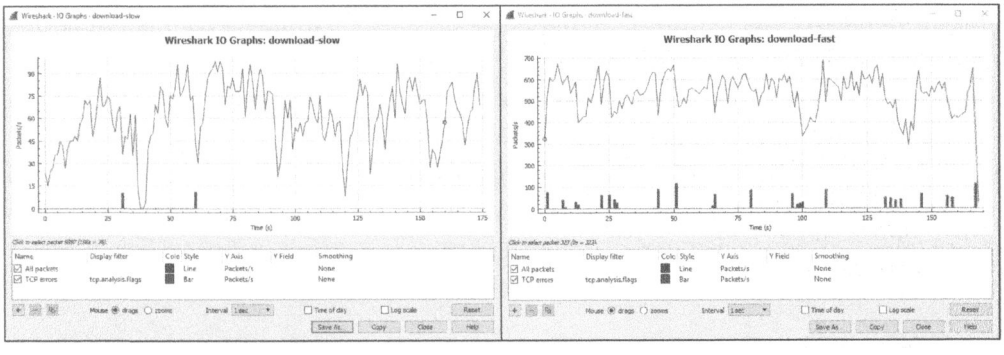

Рис. 5.19. Просмотр двух расположенных рядом графиков ввода-вывода может помочь в выявлении отклонений

Параметры, настраиваемые в нижней части окна IO Graph, позволяют применять ряд особых фильтров, составляемых с помощью того же самого синтаксиса, что и для фильтров отображения, а также выбирать цвета для отображения данных из этих фильтров. Например, можно создать фильтры конкретных IP-адресов и назначить для них особые цвета для просмотра отклонений в пропускной способности каждого устройства.

Опробуйте такую возможность, открыв файл перехвата `http_espn.pcapng`, который был получен при посещении начальной страницы американского кабельного спортивного телеканала ESPN из анализируемого устройства. В окне Conversations вы обнаружите, что наиболее активным оказывается сетевой узел с внешним IP-адресом **`205.234.218.129`**. Из этого можно сделать вывод, что данный сетевой узел, вероятнее всего, служит основным поставщиком содержимого, которое получается при посещении веб-страницы по адресу `espn.com`. Но в диалоге принимают участие и сетевые узлы по другим IP-адресам, вероятнее всего, потому, что дополнительное содержимое загружается из внешних его поставщиков и рекламодателей. Отличия в прямой и сторонней доставке содержимого можно продемонстрировать с помощью графика ввода-вывода, приведенного на рис. 5.20.

Оба фильтра, применяемых на этом графике, представлены отдельными строками в нижней части окна IO Graph. В частности, фильтр `Top Talker` (Наиболее активный сетевой узел) показывает ввод-вывод только по IP-адресу **`205.234.218.129`** основного в данном случае поставщика содержимого. Объем этого ввода-вывода отображается на графике черным цветом, заполняющим верхнюю часть столбиковой диаграммы. А фильтр `Everything Else` (Все остальные) показывает ввод-вывод по всем остальным IP-адресам в файле перехвата, кроме адреса **`205.234.218.129`**. Следовательно, он включает в себя всех сторонних поставщиков содержимого. Объем этого ввода-вывода отображается на графике красным цветом (светлым оттенком серого на рис. 5.20), заполняющим нижнюю часть столбиковой диаграммы. Обратите внимание на то, что единицы измерения по оси Y данного графика были изменены на байты в секунду. С учетом этих изменений очень легко увидеть отличия в объеме трафика основного и сторонних поставщиков содержимого, а также выяснить, сколько содержимого поступает из стороннего источника. Вам, вероятно, будет любопытно повторить это упражнение на часто посещаемых вами веб-сайтах и взять эту полезную стратегию на вооружение для сравнения объемов ввода-вывода в разных хостах.

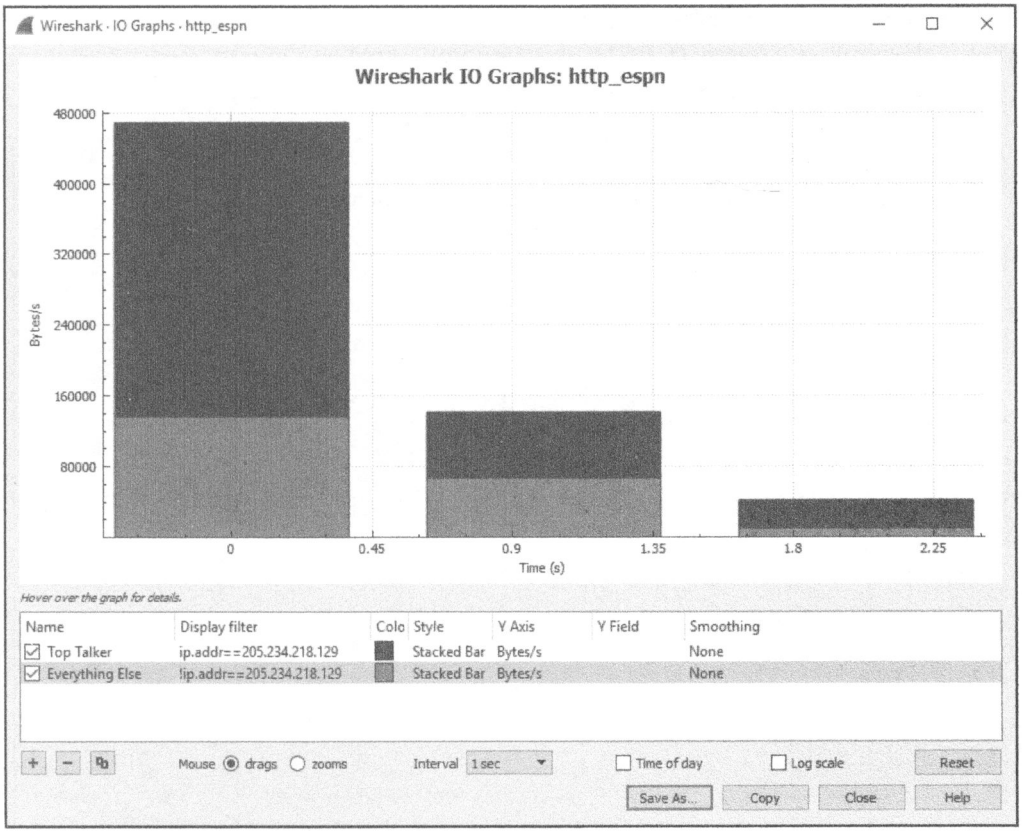

Рис. 5.20. График, демонстрирующий отличия ввода-вывода в двух отдельных устройствах

Составление графика времени круговой передачи пакетов

Файл перехвата **`download-fast.pcapng`**

В приложении Wireshark имеется также возможность составлять и просматривать график времени круговой (round-trip) передачи пакетов из заданного файла перехвата. *Время круговой передачи* (Round-Trip Time, RTT) — это время, которое требуется на получение подтверждения доставки пакета адресату. По существу, это время, которое требуется, чтобы пакет достиг получателя, а отправленное обратно подтверждение его получения — отправителя этого пакета. Анализ времени круговой передачи пакета зачастую выполняется с целью выявить места замедления или узкие места в передаче данных, а также любые задержки, возникающие в этой связи.

Чтобы опробовать такую возможность на конкретном примере, откройте файл перехвата `download-fast.pcapng`. Чтобы просмотреть график времени круговой передачи пакетов из этого файла, выберите сначала любой пакет

TCP, а затем команду Statistics⇨TCP Stream Graphs⇨Round Trip Time Graph (Статистика⇨Графики потоков TCP⇨График времени круговой передачи) из главного меню. В итоге появится график, приведенный на рис. 5.21.

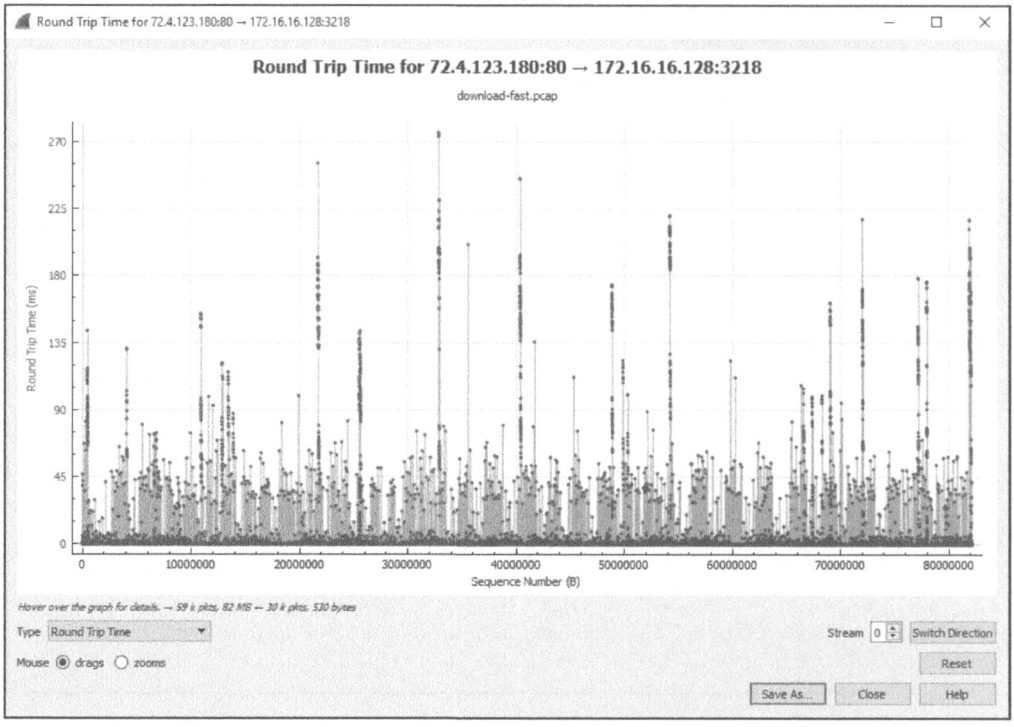

Рис. 5.21. График времени круговой передачи пакетов при быстрой загрузке файла демонстрирует практическое постоянство этой временной характеристики, за исключением нескольких случайных отклонений

Каждая точка на этом графике представляет время на передачу и подтверждение приема пакета. По умолчанию эти величины отсортированы по порядковым номерам пакетов. Чтобы перейти непосредственно к пакету на панели Packet List, достаточно щелкнуть на соответствующей точке графика.

ПРИМЕЧАНИЕ *График времени круговой передачи пакетов носит однонаправленный характер, поэтому очень важно выбрать для анализа нужное направление сетевого трафика. Если у вас этот график выглядит иначе, чем на рис. 5.21, попробуйте дважды щелкнуть на кнопке* Switch Direction *(Сменить направление).*

На этом графике, построенном для быстрой загрузки файла, величины времени круговой передачи пакетов в основном оказываются меньше 0,05 с,

и лишь в некоторых точках они находятся в пределах от 0,10 до 0,25 с. И несмотря на немалое количество больших величин, они в основном обозначают вполне допустимое для загрузки файла время на передачу и подтверждение приема. Анализируя график времени круговой передачи пакетов с точки зрения пропускной способности сети, следует выявлять большие величины времени задержки, обозначаемые множеством точек при больших значениях, откладываемых по оси Y.

Составление графиков потоков

Файл перехвата **dns_recursivequery_server.pcapng**

Возможность составлять графики потоков оказывается полезной для наглядного представления сетевых соединений и передачи потоков данных во времени. Подобные сведения облегчают понимание характера обмена данными между устройствами в сети. График потоков состоит из столбцов, обозначающих соединение между хостами, наглядно представляя сетевой трафик для удобства его интерпретации.

Чтобы создать график потоков, откройте файл перехвата `dns_recursivequery_server.pcapng` и выберите команду Statistics⇨Flow Graph (Статистика⇨График потоков) из главного меню. Полученный в итоге график приведен на рис. 5.22.

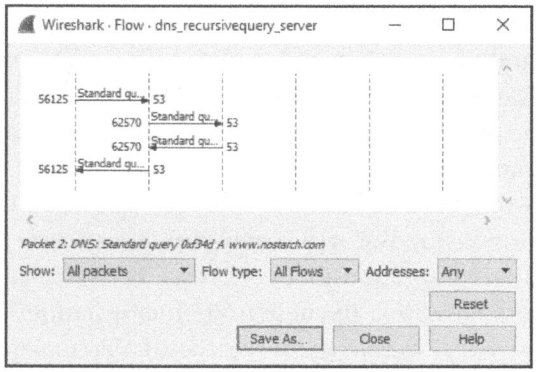

Рис. 5.22. График потоков TCP позволяет намного лучше представить наглядно сетевое соединение

На этом графике потоков наглядно представлен рекурсивный DNS-запрос, получаемый одним хостом и пересылаемый другому хосту (подробнее о протоколе DNS речь пойдет в главе 9, "Распространенные протоколы верхнего уровня"). Каждая вертикальная линия на этом графике обозначает отдельный хост. График потоков позволяет наглядно представить двухсторонний обмен данными между двумя устройствами в сети, а в данном примере — соотношение

обмена данными между несколькими устройствами. Такой график полезен и для понимания обычного потока данных, передаваемых по менее известным из вашего опыта сетевым протоколам.

Экспертная информация

Файл перехвата **download-slow.pcapng**

В дешифраторах каждого протокола в Wireshark определена *экспертная информация*, предупреждающая о конкретных состояниях в пакетах данного протокола. Эти состояния разделяются на следующие категории.

- **Chat (Текстовый диалог).** Основные сведения об обмене данными.
- **Note (Уведомление).** Необычные пакеты, которые могут быть частью обычного обмена данными.
- **Warning (Предупреждение).** Необычные пакеты, которые, вероятнее всего, не являются частью обычного обмена данными.
- **Error (Ошибка).** Ошибка в пакете или интерпретирующем его дешифраторе.

В качестве примера откройте файл перехвата `download-slow.pcapng` и выберите команду Analyze⇨Expert Information (Анализ⇨Экспертная информация) из главного меню, чтобы открыть окно Expert Information. Установите в этом окне флажок Group by summary (Группировать по сводке), чтобы организовать вывод экспертной информации по степени ее важности (рис. 5.23).

В этом окне имеются разделы по каждой категории экспертной информации. В данном случае ошибки отсутствуют, имеются 3 предупреждения, 19 уведомлений и 3 текстовых диалога.

Большинство сообщений из данного файла перехвата связаны с сетевым протоколом TCP просто потому, что к данному протоколу традиционно применялась экспертная информационная система. В то же время в данном окне отображается 29 сообщений с экспертной информацией, настроенных на протокол TCP, и они могут оказаться полезными для диагностики файлов перехвата. Эти сообщения помечают отдельные пакеты, когда они удовлетворяют определенным критериям, как перечислено ниже. (Это означает, что подобные сообщения станут более понятными при изучении сетевого протокола TCP в главе 8, "Протоколы транспортного уровня", и диагностики медленных сетей в главе 11, "Меры борьбы с медленной сетью".

- **Сообщения текстового диалога.**

  Сообщение `"Window Update"` (Изменение размера окна), посылаемое получателем, чтобы уведомить отправителя об изменении размера окна приема в протоколе TCP.

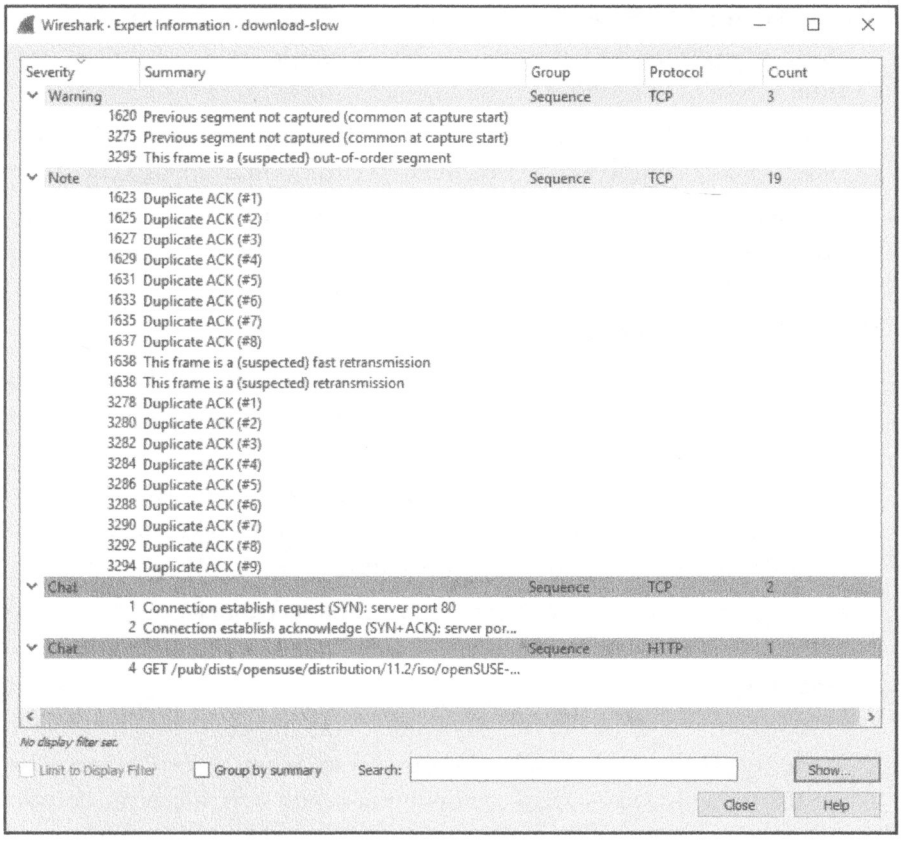

Рис. 5.23. В окне Expert Information отображаются сведения из экспертной системы, запрограммированной в дешифраторах сетевых протоколов

- **Сообщения с уведомлениями.**

  Сообщение "`TCP Retransmission`" (Повторная передача по протоколу TCP), посылаемое в результате потери пакетов. Оно появляется, когда получен дубликат подтверждения приема пакета или сработал таймер времени ожидания повторной передачи пакетов.

  Сообщение "`Duplicate ACK`" (Дубликат подтверждения), посылаемое в том случае, если хост не получает пакет с ожидаемым следующим порядковым номером и формирует дубликат подтверждения последних полученных данных.

  Сообщение "`Zero Window Probe`" (Проба нулевого окна), посылаемое в ходе текущего контроля состояния окна приема в протоколе TCP после передачи пакета с нулевым окном, как поясняется в главе 11, "Меры борьбы с медленной сетью".

Сообщение "Keep Alive ACK" (Подтверждение активности соединения), посылаемое в ответ на пакеты поддержания активным соединения.

Сообщение "Zero Window Probe ACK" (Подтверждение пробы нулевого окна), посылаемое в ответ на пакеты с пробой нулевого окна.

Сообщение "Window Is Full" (Окно заполнено), посылаемое для уведомления о заполнении на стороне получателя окна приема в протоколе TCP.

- **Предупреждающие сообщения.**

  Сообщение "Previous Segment Lost" (Предыдущий сегмент потерян), посылаемое в том случае, если пропущен пакет с ожидаемым порядковым номером в потоке данных.

  Сообщение "ACKed Lost Packet" (Подтверждение потери пакета), посылаемое в том случае, если обнаружен пакет подтверждения ACK, но не пакет, который он подтверждает.

  Сообщение "Keep Alive" (Поддержание активным соединения), посылаемое в том случае, если обнаружен пакет поддержания активным соединения.

  Сообщение "Zero Window" (Нулевое окно), посылаемое в том случае, если достигнут размер окна приема в протоколе TCP и послано уведомление о нулевом окне, запрашивающее отправителя остановить передачу данных.

  Сообщение "Out-of-Order" (Нарушение порядка следования), посылаемое в том случае, если на основании порядковых номеров обнаружено, что пакеты получаются не по порядку следования их номеров.

  Сообщение "Fast Retransmission" (Быстрая повторная передача), посылаемое в том случае, если повторная передача пакета происходит в течение 20 мс после получения дубликата подтверждения.

- **Сообщения об ошибках.**

  Сообщение "No Error Messages" (Сообщения об ошибках отсутствуют).

На первый взгляд может показаться, что некоторые возможности Wireshark, рассматриваемые в этой главе, пригодны лишь в особых, малоизвестных ситуациях, но на самом деле вам придется пользоваться ими чаще, чем вы могли бы предположить. Ознакомиться с рассмотренными здесь возможностями и окнами очень важно потому, что к ним придется еще не раз обращаться в ряде последующих глав.