ОБРАБОТКА ПЕРЕХВАЧЕННЫХ ПАКЕТОВ

Обработка файлов перехвата

Со временем вы обнаружите, что немалая доля анализа пакетов приходится на стадию, следующую после их перехвата. Как правило, несколько перехватов производится в разные моменты времени. При этом они сохраняются, а затем анализируются сообща. Таким образом, Wireshark позволяет сохранять файлы перехвата для последующего их анализа. Кроме того, несколько файлов перехвата можно объединить вместе.

Сохранение и экспорт файлов перехвата

Чтобы сохранить результат перехвата пакетов, выберите команду File⇨Save As (Файл⇨Сохранить как) из главного меню. В итоге появится диалоговое окно Save file as (Сохранение файла), приведенное на рис. 4.1, в котором вам будет предложено указать место для сохранения полученного перехвата

пакетов, а также выбрать для него подходящий формат файла. Если вы не укажете формат файла, Wireshark автоматически выберет задаваемый по умолчанию формат файла с расширением **.pcapng**.

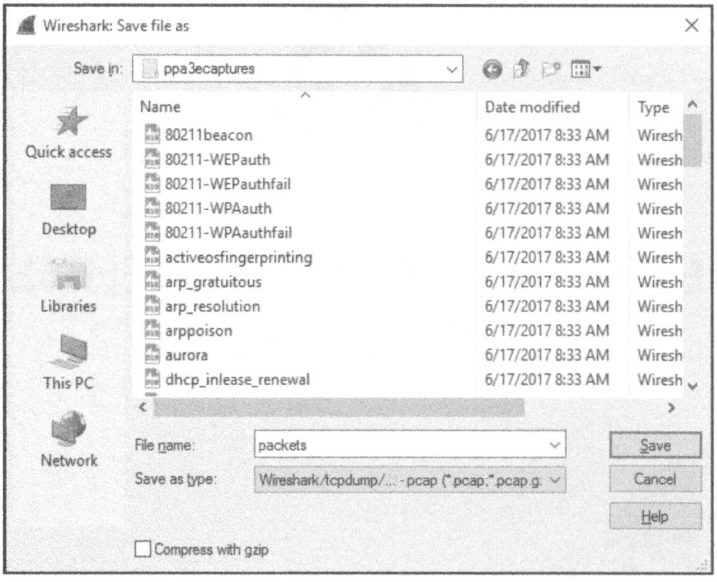


Рис. 4.1. В диалоговом окне Save file as можно сохранять полученные перехваты пакетов

Зачастую требуется сохранить лишь часть перехваченных пакетов. С этой целью выберите команду File⇨Export Specified Packets (Файл⇨Экспортировать указанные пакеты) из главного меню. В итоге появится диалоговое окно, приведенное на рис. 4.2. Это удобный случай сократить размеры чрезмерно раздутых файлов перехвата. В частности, можно выбрать сохранение пакетов лишь в конкретном диапазоне номеров, отмеченных пакетов или же тех пакетов, которые появляются на экране после применения фильтра отображения (отмеченные пакеты и фильтры рассматриваются далее в этой главе).

Объединение файлов перехвата

Для некоторых видов анализа требуется возможность объединять вместе несколько файлов перехвата. И это обычная норма практики, когда приходится сравнивать два потока данных или объединять потоки, относящиеся к одному сетевому трафику, но перехваченные отдельно.

Чтобы объединить файлы перехвата, откройте один из них и выберите команду File⇨Merge (Файл⇨Объединить) из главного меню. В итоге откроется диалоговое окно Merge with capture file (Объединение с файлом перехвата),

приведенное на рис. 4.3. Выберите сначала новый файл, с которым требуется объединить уже открытый файл, а затем способ их объединения. В частности, выбранный файл можно присоединить в начале или в конце открытого в настоящий момент файла или же объединить файлы в хронологическим порядке, исходя из отметок времени их создания или изменения.

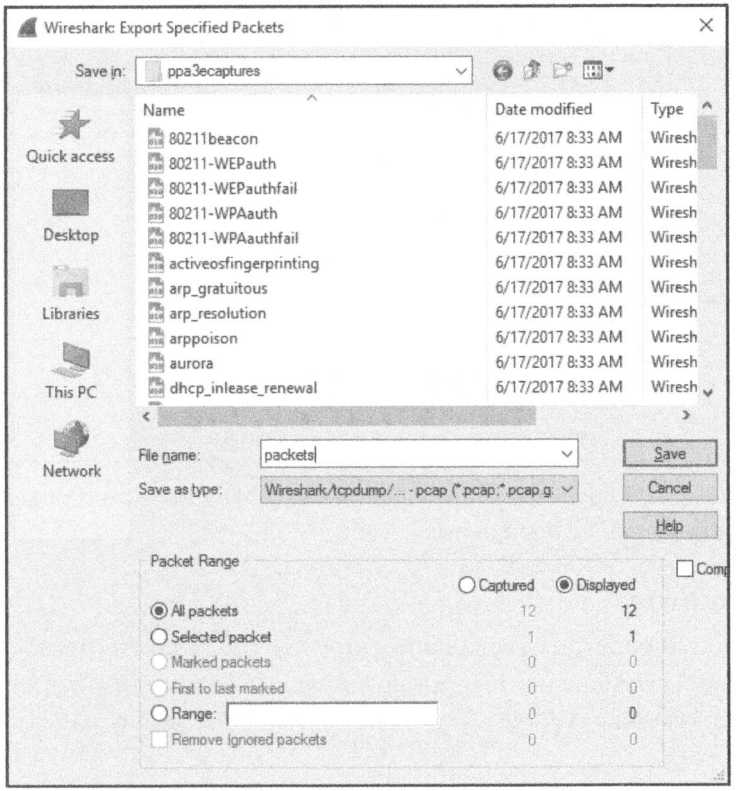


Рис. 4.2. В диалоговом окне Export Specified Packets можно более точно указать порядок сохранения перехваченных пакетов

Обработка пакетов

Дело в конечном итоге дойдет до того, что вам придется обрабатывать очень много пакетов. По мере увеличения количества пакетов до тысяч и даже миллионов у вас возникнет потребность эффективно перемещаться по этим пакетам. И для этой цели в Wireshark предусмотрен поиск и отметка пакетов, отвечающих определенным критериям. Чтобы упростить обращение к пакетам для получения быстрой справки, их можно распечатать.

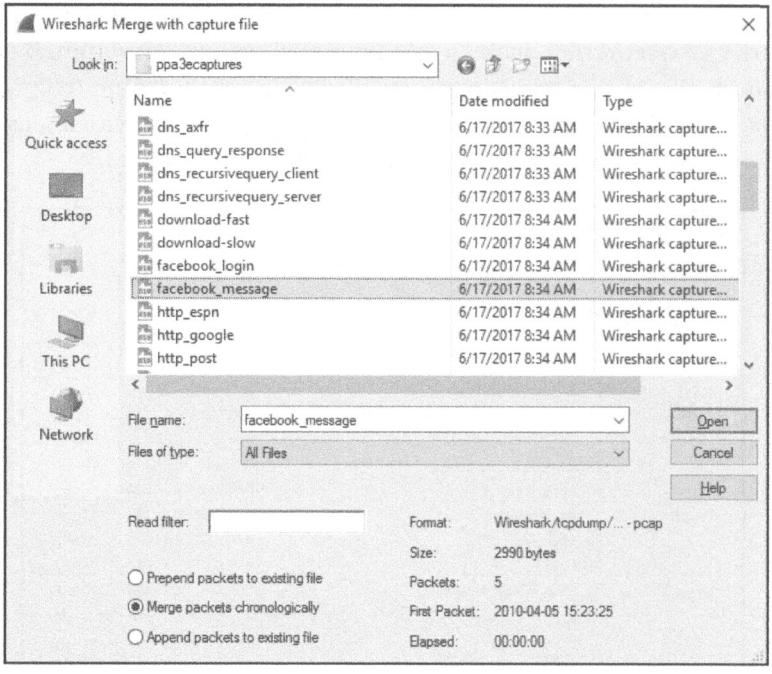


Рис. 4.3. В диалоговом окне Merge with capture file можно объединить два файла перехвата

Поиск пакетов

Чтобы найти пакеты, отвечающие определенным критериям, откройте панель Find Packet (Поиск пакета), приведенную в сжатом виде на рис. 4.4, нажав комбинацию клавиш <Ctrl+F>. Эта панель появится между панелью Filter и окном Packet List.

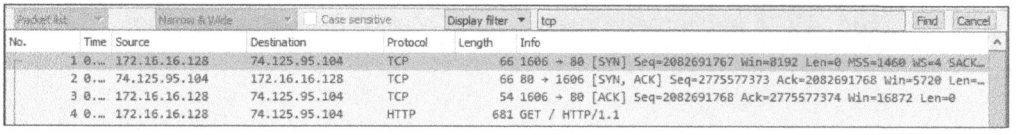


Рис. 4.4. Поиск пакетов в Wireshark по заданным критериям. В данном случае показаны пакеты, совпадающие с выражением **tcp**, *заданным в фильтре отображения*

На этой панели предоставляются три варианта поиска пакетов, как поясняется ниже.

- **Display filter (Фильтр отображения).** Этот вариант позволяет создать фильтр, чтобы найти только те пакеты, которые отвечают заданному в нем выражению. Именно этот вариант поиска пакетов использован для получения результатов, приведенных на рис. 4.4.

- **Hex value (Шестнадцатеричное значение).** Этот вариант предназначен для поиска пакетов по указанному шестнадцатеричному значению.
- **String (Символьная строка).** Этот вариант предназначен для поиска пакетов по указанной символьной строке. В частности, можно указать имя объекта для поиска пакетов или учитывать регистр букв в строке поиска.

Виды поиска пакетов сведены в табл. 4.1.

Таблица 4.1. Виды поиска пакетов

Вид поиска	Примеры
Фильтр отображения	`not ip`
	`ip.addr==192.168.0.1`
	`Arp`
Шестнадцатеричное значение	`00ff`
	`ffff`
	`00ABB1f0`
Символьная строка	`Workstation1`
	`UserB`
	`domain`

Выбрав вид поиска пакетов, введите критерий поиска в текстовом поле и щелкните на кнопке Find, чтобы найти первый пакет, отвечающий заданному критерию. Чтобы найти следующий пакет, щелкните на кнопке Find еще раз или нажмите комбинацию клавиш <Ctrl+N>, а для поиска предыдущего пакета, совпавшего с заданным критерием, – комбинацию клавиш <Ctrl+B>.

Отметка пакетов

Итак, найдя пакеты, отвечающие заданному критерию, можете отметить те из них, которые интересуют вас в первую очередь. Отметка пакетов, в частности, позволяет сохранить только эти пакеты. Кроме того, отмеченные пакеты можно быстро отыскать по их белому тексту на черном фоне, как показано на рис. 4.5.

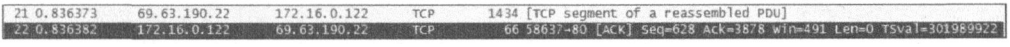


Рис. 4.5. Отмеченный пакет выделяется на экране. В данном примере второй пакет оказывается отмеченным и выглядит более темным на экране

Чтобы отметить пакет, щелкните на нем правой кнопкой мыши в панели Packet List и выберите команду Mark Packet (Отметить пакет) из контекстного

меню или нажмите комбинацию клавиш <Ctrl+M>, находясь в панели Packet List. Отметить можно столько перехваченных пакетов, сколько потребуется. А для перехода между отмеченными пакетами вперед или назад нажмите комбинацию клавиш <Shift+Ctrl+N> или <Shift+Ctrl+B> соответственно.

Вывод пакетов на печать

Несмотря на то что бо́льшая часть анализа проводится на экране компьютерного монитора, перехваченные данные иногда требуется распечатать. Время от времени я распечатываю перехваченные пакеты и приклеиваю липкой лентой полученные распечатки к своему рабочему столу, чтобы быстро обращаться за справкой к их содержимому по ходу анализа. Пакеты удобно также распечатать в формате PDF, особенно при подготовке отчетов.

Чтобы распечатать перехваченные пакеты, откройте диалоговое окно Print, выбрав команду File⇨Print (Файл⇨Печать) из главного меню (рис. 4.6).

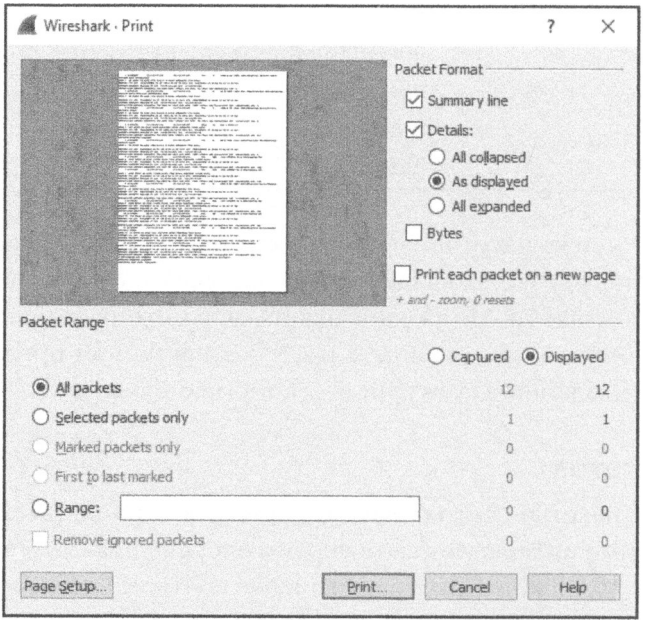


Рис. 4.6. В диалоговом окне Print можно распечатать указанные пакеты

Как и в диалоговом окне Export Specified Packets, в данном окне можно указать печать пакетов только в определенных пределах или же тех пакетов, которые отображаются после применения фильтра. Кроме того, можно указать требуемую степень детализации для печати каждого пакета. После того как выберете все параметры настройки печати, щелкните на кнопке Print.

Задание форматов отображения времени и привязок к нему

Время очень существенно, особенно для анализа пакетов. Все, что происходит в сети, зависит от времени, и поэтому в файлах перехвата приходится часто изучать тенденции и сетевые задержки. В приложении Wireshark предоставляется несколько настраиваемых параметров, имеющих отношение ко времени. В этом разделе будут рассмотрены форматы отображения времени и привязки к нему.

Форматы отображения времени

Каждый пакет, перехватываемый в Wireshark, снабжается отметкой времени, присваиваемой ему на уровне операционной системы. Приложение Wireshark способно отображать абсолютную отметку времени, обозначающую конкретный момент, когда пакет был перехвачен, время относительно последнего перехваченного пакета, а также начало и конец перехвата.

Параметры, имеющие отношение к отображению времени, находятся под заголовком View в главном меню. Пункт Time Display Format (Формат отображения времени) под этим заголовком главного меню позволяет настроить формат представления времени, а также точность его отображения, как показано на рис. 4.7.

Параметры настройки формата для представления времени позволяют выбрать разные варианты отображения времени. К их числу относится отображение даты и времени суток в стандартном формате или же в формате всеобщего скоординированного времени (UTC), количества секунд, прошедших с момента последнего перехвата, и прочее.

А параметры настройки точности позволяют задать точность отображения времени автоматически, т.е. в формате, взятом из файла перехвата, или вручную, например, в секундах, миллисекундах, микросекундах и т.д. Эти параметры будут настраиваться в примерах, приведенных далее в книге, поэтому вы должны ознакомиться с ними уже теперь.

ПРИМЕЧАНИЕ *Сравнивая данные из пакетов, поступающих из разных устройств, убедитесь, что эти устройства синхронизированы с одним и тем же источником времени, особенно если вы выполняете ретроспективный анализ или диагностику сети. Для синхронизации устройств в сети можно воспользоваться протоколом NTP (Network Time Protocol – протокол сетевого времени). Анализ пакетов, поступающих из устройств в разных часовых поясах, следует проводить в формате UTC, а не местного времени, чтобы избежать недоразумений при сообщении полученных результатов анализа.*

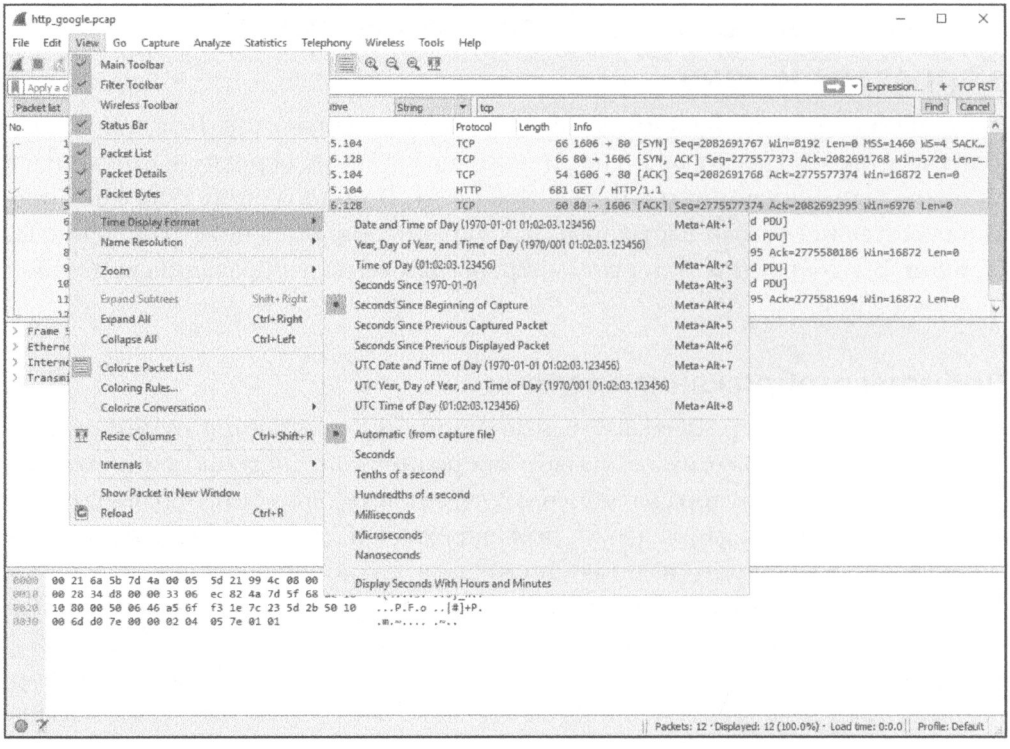


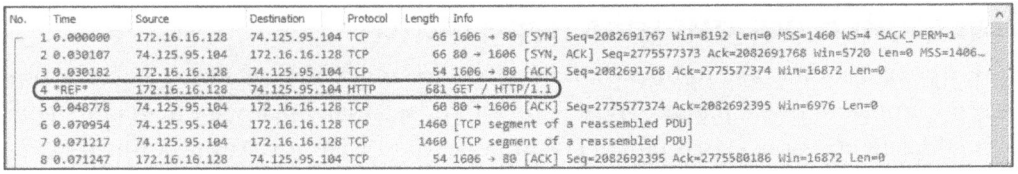
Рис. 4.7. По команде View⇨Time Display Format из главного меню можно выбрать один из нескольких форматов отображения времени

Временная привязка к пакетам

Временная привязка к пакетам позволяет настроить определенный пакет таким образом, чтобы последующие расчеты времени производились относительно данного пакета. Такая возможность особенно удобна при исследовании ряда последовательных событий, наступающих в какой-нибудь другой момент, а не в момент начала формирования файла перехвата.

Чтобы установить временную привязку к пакету, щелкните правой кнопкой мыши на избранном в качестве опорного пакете в панели Packet List и выберите команду Set/Unset Time Reference (Установить/Сбросить временную привязку) из контекстного меню. А для того чтобы сбросить временную привязку, повторите эту же операцию еще раз. Кроме того, устанавливать и сбрасывать временную привязку к пакету можно, выбрав опорный пакет в подокне Packet List и нажав комбинацию клавиш <Ctrl+T>.

Если временная привязка к пакету активизирована, в столбце **Time** (Время), отображаемом в панели Packet List, появится метка ***REF*** (рис. 4.8).



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.16.128	74.125.95.104	TCP	66	1606 → 80 [SYN] Seq=2082691767 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.030107	74.125.95.104	172.16.16.128	TCP	66	80 → 1606 [SYN, ACK] Seq=2775577373 Ack=2082691768 Win=5720 Len=0 MSS=1406…
3	0.030182	172.16.16.128	74.125.95.104	TCP	54	1606 → 80 [ACK] Seq=2082691768 Ack=2775577374 Win=16872 Len=0
4	*REF*	172.16.16.128	74.125.95.104	HTTP	681	GET / HTTP/1.1
5	0.048778	74.125.95.104	172.16.16.128	TCP	60	80 → 1606 [ACK] Seq=2775577374 Ack=2082692395 Win=6976 Len=0
6	0.070954	74.125.95.104	172.16.16.128	TCP	1460	[TCP segment of a reassembled PDU]
7	0.071217	74.125.95.104	172.16.16.128	TCP	1460	[TCP segment of a reassembled PDU]
8	0.071247	172.16.16.128	74.125.95.104	TCP	54	1606 → 80 [ACK] Seq=2082692395 Ack=2775580186 Win=16872 Len=0

Рис. 4.8. Пакет №4 с активизированной временной привязкой к нему

Устанавливать временную привязку к пакету удобно лишь в том случае, если формат отображения времени перехвата настроен на показ времени относительно начала перехвата. А в любом другом случае установка временной привязки к пакету ничего полезного не даст и на самом деле приведет к отображению моментов времени, в которых будет очень трудно разобраться.

Временной сдвиг

Иногда встречаются пакеты из разных источников, которые не синхронизированы с одним и тем же источником. Это особенно характерно для исследования файлов перехвата, взятых из двух мест, содержащих один и тот же поток данных. Большинство сетевых администраторов стремятся к тому, чтобы каждое устройство в их сети было синхронизировано. Но нередко между определенными типами устройств возникает временной сдвиг. В приложении Wireshark предоставляется возможность сдвигать отметку времени в пакетах, чтобы устранить данное затруднение в ходе анализа.

Чтобы сдвинуть отметку времени в одном или нескольких пакетах, выберите команду Edit⇨Time Shift (Правка⇨Временной сдвиг) из главного меню или нажмите комбинацию клавиш <Ctrl+Shift+T>. В открывшемся диалоговом окне Time Shift можно указать пределы для временного сдвига во всем файле перехвата в целом или же установить время для отдельных пакетов. В примере, приведенном на рис. 4.9, выбран сдвиг отметки времени в каждом пакете из файла перехвата на две минуты и пять секунд.

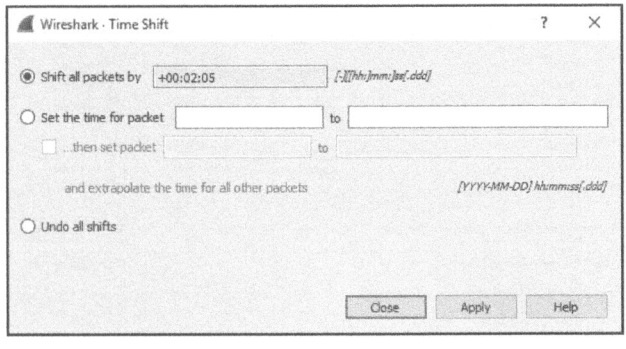


Рис. 4.9. Диалоговое окно Time Shift