Wireshark User's Guide

For Wireshark 2.1

Ulf Lamping <ulf.lamping[AT]web.de>
Richard Sharpe, NS Computer Software and Services P/L <rsharpe[AT]ns.aus.com>
Ed Warnicke <hagbard[AT]physics.rutgers.edu>

Wireshark User's Guide: For Wireshark 2.1

by Ulf Lamping, Richard Sharpe, and Ed Warnicke

Preface

1. Foreword

Wireshark is one of those programs that many network managers would love to be able to use, but they are often prevented from getting what they would like from Wireshark because of the lack of documentation.

This document is part of an effort by the Wireshark team to improve the usability of Wireshark.

We hope that you find it useful and look forward to your comments.

2. Who should read this document?

The intended audience of this book is anyone using Wireshark.

This book will explain all the basics and also some of the advanced features that Wireshark provides. As Wireshark has become a very complex program since the early days, not every feature of Wireshark may be explained in this book.

This book is not intended to explain network sniffing in general and it will not provide details about specific network protocols. A lot of useful information regarding these topics can be found at the Wireshark Wiki at https://wiki.wireshark.org/

By reading this book, you will learn how to install Wireshark, how to use the basic elements of the graphical user interface (such as the menu) and what's behind some of the advanced features that are not always obvious at first sight. It will hopefully guide you around some common problems that frequently appear for new (and sometimes even advanced) users of Wireshark.

3. Acknowledgements

The authors would like to thank the whole Wireshark team for their assistance. In particular, the authors would like to thank:

- Gerald Combs, for initiating the Wireshark project and funding to do this documentation.
- Guy Harris, for many helpful hints and a great deal of patience in reviewing this document.
- Gilbert Ramirez, for general encouragement and helpful hints along the way.

The authors would also like to thank the following people for their helpful feedback on this document:

- Pat Eyler, for his suggestions on improving the example on generating a backtrace.
- Martin Regner, for his various suggestions and corrections.
- Graeme Hewson, for a lot of grammatical corrections.

The authors would like to acknowledge those man page and README authors for the Wireshark project from who sections of this document borrow heavily:

- Scott Renfro from whose `mergecap` man page Section D.8, "*mergecap*: Merging multiple capture files into one" is derived.

- Ashok Narayanan from whose `text2pcap` man page Section D.9, *"text2pcap*: Converting ASCII hexdumps to network captures" is derived.

4. About this document

This book was originally developed by Richard Sharpe with funds provided from the Wireshark Fund. It was updated by Ed Warnicke and more recently redesigned and updated by Ulf Lamping.

It was originally written in DocBook/XML and converted to AsciiDoc by Gerald Combs.

You will find some specially marked parts in this book:

This is a warning

You should pay attention to a warning, otherwise data loss might occur.

This is a note

A note will point you to common mistakes and things that might not be obvious.

This is a tip

Tips are helpful for your everyday work using Wireshark.

5. Where to get the latest copy of this document?

The latest copy of this documentation can always be found at https://www.wireshark.org/docs/.

6. Providing feedback about this document

Should you have any feedback about this document, please send it to the authors through wireshark-dev[AT]wireshark.org.

Chapter 1. Introduction

1.1. What is Wireshark?

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed.

Wireshark is perhaps one of the best open source packet analyzers available today.

1.1.1. Some intended purposes

Here are some examples people use Wireshark for:

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals

Beside these examples Wireshark can be helpful in many other situations too.

1.1.2. Features

The following are some of the many features Wireshark provides:

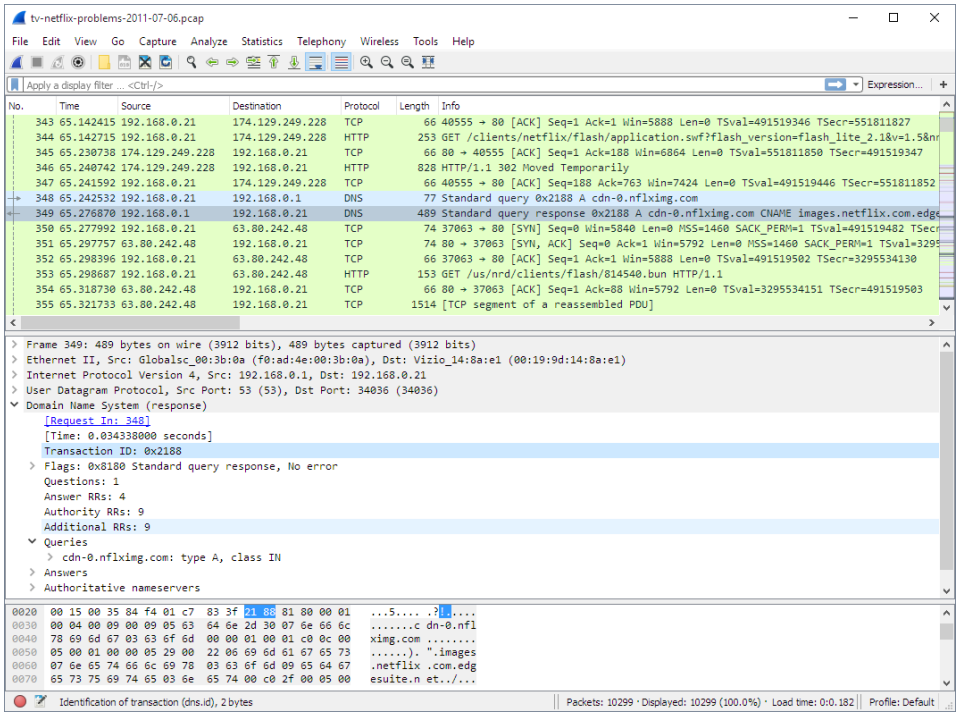
- Available for *UNIX* and *Windows*.
- *Capture* live packet data from a network interface.
- *Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- *Import* packets from text files containing hex dumps of packet data.
- Display packets with *very detailed protocol information*.
- *Save* packet data captured.
- *Export* some or all packets in a number of capture file formats.
- *Filter packets* on many criteria.
- *Search* for packets on many criteria.
- *Colorize* packet display based on filters.
- Create various *statistics*.

- …and *a lot more!*

However, to really appreciate its power you have to start using it.

Figure 1.1, “Wireshark captures packets and lets you examine their contents.” shows Wireshark having captured some packets and waiting for you to examine them.

Figure 1.1. Wireshark captures packets and lets you examine their contents.



1.1.3. Live capture from many different network media

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well. Which media types are supported, depends on many things like the operating system you are using. An overview of the supported media types can be found at https://wiki.wireshark.org/CaptureSetup/NetworkMedia.

1.1.4. Import files from many other capture programs

Wireshark can open packets captured from a large number of other capture programs. For a list of input formats see Section 5.2.2, “Input File Formats”.

1.1.5. Export files for many other capture programs

Wireshark can save packets captured in a large number of formats of other capture programs. For a list of output formats see Section 5.3.2, “Output File Formats”.

1.1.6. Many protocol dissectors

There are protocol dissectors (or decoders, as they are known in other products) for a great many protocols: see Appendix C, *Protocols and Protocol Fields*.

1.1.7. Open Source Software

Wireshark is an open source software project, and is released under the GNU General Public License (GPL). You can freely use Wireshark on any number of computers you like, without worrying about license keys or fees or such. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plugins, or built into the source, and they often do!

1.1.8. What Wireshark is not

Here are some things Wireshark does not provide:

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

1.2. System Requirements

The amount of resources Wireshark needs depends on your environment and on the size of the capture file you are analyzing. The values below should be fine for small to medium-sized capture files no more than a few hundred MB. Larger capture files will require more memory and disk space.

Busy networks mean large captures

Working with a busy network can easily produce huge capture files. Capturing on a gigabit or even 100 megabit network can produce hundreds of megabytes of capture data in a short time. A fast processor, lots of memory and disk space is always a good idea.

If Wireshark runs out of memory it will crash. See https://wiki.wireshark.org/KnownBugs/OutOfMemory for details and workarounds.

Although Wireshark captures packets using a separate process the main interface is single-threaded and won't benefit much from multi-core systems.

1.2.1. Microsoft Windows

- The current version of Wireshark should support any version of Windows that is still within its extended support lifetime. At the time of writing this includes Windows 10, 8, 7, Vista, Server 2016, Server 2012 R2, Server 2012, Server 2008 R2, and Server 2008.
- Any modern 64-bit AMD64/x86-64 or 32-bit x86 processor.
- 400 MB available RAM. Larger capture files require more RAM.
- 300 MB available disk space. Capture files require additional disk space.
- 1024×768 (1280×1024 or higher recommended) resolution with at least 16 bit color. 8 bit color should work but user experience will be degraded. Power users will find multiple monitors useful.
- A supported network card for capturing

- Ethernet. Any card supported by Windows should work. See the wiki pages on Ethernet capture and offloading for issues that may affect your environment.
- 802.11. See the Wireshark wiki page. Capturing raw 802.11 information may be difficult without special equipment.
- Other media. See https://wiki.wireshark.org/CaptureSetup/NetworkMedia

Older versions of Windows which are outside Microsoft's extended lifecycle support window are no longer supported. It is often difficult or impossible to support these systems due to circumstances beyond our control, such as third party libraries on which we depend or due to necessary features that are only present in newer versions of Windows (such as hardened security or memory management).

Wireshark 1.12 was the last release branch to support Windows Server 2003. Wireshark 1.10 was the last branch to officially support Windows XP. See the Wireshark release lifecycle page for more details.

1.2.2. UNIX / Linux

Wireshark runs on most UNIX and UNIX-like platforms including OS X and Linux. The system requirements should be comparable to the Windows values listed above.

Binary packages are available for most Unices and Linux distributions including the following platforms:

- Apple OS X
- Debian GNU/Linux
- FreeBSD
- Gentoo Linux
- HP-UX
- Mandriva Linux
- NetBSD
- OpenPKG
- Red Hat Enterprise/Fedora Linux
- Sun Solaris/i386
- Sun Solaris/SPARC
- Canonical Ubuntu

If a binary package is not available for your platform you can download the source and try to build it. Please report your experiences to wireshark-dev[AT]wireshark.org.

1.3. Where to get Wireshark

You can get the latest copy of the program from the Wireshark website at https://www.wireshark.org/download.html. The download page should automatically highlight the appropriate download for your

platform and direct you to the nearest mirror. Official Windows and OS X installers are signed by the **Wireshark Foundation**.

A new Wireshark version typically becomes available each month or two.

If you want to be notified about new Wireshark releases you should subscribe to the wireshark-announce mailing list. You will find more details in Section 1.6.5, “Mailing Lists”.

1.4. A brief history of Wireshark

In late 1997 Gerald Combs needed a tool for tracking down network problems and wanted to learn more about networking so he started writing Ethereal (the original name of the Wireshark project) as a way to solve both problems.

Ethereal was initially released after several pauses in development in July 1998 as version 0.2.0. Within days patches, bug reports, and words of encouragement started arriving and Ethereal was on its way to success.

Not long after that Gilbert Ramirez saw its potential and contributed a low-level dissector to it.

In October, 1998 Guy Harris was looking for something better than tcpview so he started applying patches and contributing dissectors to Ethereal.

In late 1998 Richard Sharpe, who was giving TCP/IP courses, saw its potential on such courses and started looking at it to see if it supported the protocols he needed. While it didn’t at that point new protocols could be easily added. So he started contributing dissectors and contributing patches.

The list of people who have contributed to the project has become very long since then, and almost all of them started with a protocol that they needed that Wireshark or did not already handle. So they copied an existing dissector and contributed the code back to the team.

In 2006 the project moved house and re-emerged under a new name: Wireshark.

In 2008, after ten years of development, Wireshark finally arrived at version 1.0. This release was the first deemed complete, with the minimum features implemented. Its release coincided with the first Wireshark Developer and User Conference, called Sharkfest.

In 2015 Wireshark 2.0 was released, which featured a new user interface.

1.5. Development and maintenance of Wireshark

Wireshark was initially developed by Gerald Combs. Ongoing development and maintenance of Wireshark is handled by the Wireshark team, a loose group of individuals who fix bugs and provide new functionality.

There have also been a large number of people who have contributed protocol dissectors to Wireshark, and it is expected that this will continue. You can find a list of the people who have contributed code to Wireshark by checking the about dialog box of Wireshark, or at the authors page on the Wireshark web site.

Wireshark is an open source software project, and is released under the GNU General Public License (GPL) version 2. All source code is freely available under the GPL. You are welcome to modify Wireshark to suit your own needs, and it would be appreciated if you contribute your improvements back to the Wireshark team.

You gain three benefits by contributing your improvements back to the community:

1. Other people who find your contributions useful will appreciate them, and you will know that you have helped people in the same way that the developers of Wireshark have helped people.

2. The developers of Wireshark might improve your changes even more, as there's always room for improvement. Or they may implement some advanced things on top of your code, which can be useful for yourself too.

3. The maintainers and developers of Wireshark will maintain your code as well, fixing it when API changes or other changes are made, and generally keeping it in tune with what is happening with Wireshark. So if Wireshark is updated (which is done often), you can get a new Wireshark version from the website and your changes will already be included without any effort for you.

The Wireshark source code and binary kits for some platforms are all available on the download page of the Wireshark website: https://www.wireshark.org/download.html.

1.6. Reporting problems and getting help

If you have problems or need help with Wireshark there are several places that may be of interest to you (well, besides this guide of course).

1.6.1. Website

You will find lots of useful information on the Wireshark homepage at https://www.wireshark.org/.

1.6.2. Wiki

The Wireshark Wiki at https://wiki.wireshark.org/ provides a wide range of information related to Wireshark and packet capture in general. You will find a lot of information not part of this user's guide. For example, there is an explanation how to capture on a switched network, an ongoing effort to build a protocol reference and a lot more.

And best of all, if you would like to contribute your knowledge on a specific topic (maybe a network protocol you know well) you can edit the wiki pages by simply using your web browser.

1.6.3. Q&A Site

The Wireshark Q&A site at https://ask.wireshark.org/ offers a resource where questions and answers come together. You have the option to search what questions were asked before and what answers were given by people who knew about the issue. Answers are graded, so you can pick out the best ones easily. If your question hasn't been discussed before you can post one yourself.

1.6.4. FAQ

The Frequently Asked Questions lists often asked questions and their corresponding answers.

Read the FAQ

Before sending any mail to the mailing lists below, be sure to read the FAQ. It will often answer any questions you might have. This will save yourself and others a lot of time. Keep in mind that a lot of people are subscribed to the mailing lists.

You will find the FAQ inside Wireshark by clicking the menu item Help/Contents and selecting the FAQ page in the dialog shown.

An online version is available at the Wireshark website: https://www.wireshark.org/faq.html. You might prefer this online version, as it's typically more up to date and the HTML format is easier to use.

1.6.5. Mailing Lists

There are several mailing lists of specific Wireshark topics available:

wireshark-announce
: This mailing list will inform you about new program releases, which usually appear about every 4-8 weeks.

wireshark-users
: This list is for users of Wireshark. People post questions about building and using Wireshark, others (hopefully) provide answers.

wireshark-dev
: This list is for Wireshark developers. If you want to start developing a protocol dissector, join this list.

You can subscribe to each of these lists from the Wireshark web site: https://www.wireshark.org/lists/. From there, you can choose which mailing list you want to subscribe to by clicking on the Subscribe/Unsubscribe/Options button under the title of the relevant list. The links to the archives are included on that page as well.

The lists are archived

You can search in the list archives to see if someone asked the same question some time before and maybe already got an answer. That way you don't have to wait until someone answers your question.

1.6.6. Reporting Problems

Note

Before reporting any problems, please make sure you have installed the latest version of Wireshark.

When reporting problems with Wireshark please supply the following information:

1. The version number of Wireshark and the dependent libraries linked with it, such as Qt or GLib. You can obtain this from Wireshark's about box or the command `wireshark -v`.
2. Information about the platform you run Wireshark on.
3. A detailed description of your problem.
4. If you get an error/warning message, copy the text of that message (and also a few lines before and after it, if there are some) so others may find the place where things go wrong. Please don't give something like: "I get a warning while doing x" as this won't give a good idea where to look.

Don't send large files

Do not send large files (> 1 MB) to the mailing lists. Just place a note that further data is available on request. Large files will only annoy a lot of people on the list who are not interested in your specific problem. If required you will be asked for further data by the persons who really can help you.

Don’t send confidential information!

If you send capture files to the mailing lists be sure they don’t contain any sensitive or confidential information like passwords or personally identifiable information (PII).

1.6.7. Reporting Crashes on UNIX/Linux platforms

When reporting crashes with Wireshark it is helpful if you supply the traceback information along with the information mentioned in "Reporting Problems".

You can obtain this traceback information with the following commands on UNIX or Linux (note the backticks):

```
$ gdb `whereis wireshark | cut -f2 -d: | cut -d' ' -f2` core >& backtrace.txt
backtrace
^D
```

If you do not have `gdb` available, you will have to check out your operating system’s debugger.

Mail `backtrace.txt` to wireshark-dev[AT]wireshark.org.

1.6.8. Reporting Crashes on Windows platforms

The Windows distributions don’t contain the symbol files (.pdb) because they are very large. You can download them separately at https://www.wireshark.org/download/win32/all-versions and https://www.wireshark.org/download/win64/all-versions

Chapter 2. Building and Installing Wireshark

2.1. Introduction

As with all things there must be a beginning and so it is with Wireshark. To use Wireshark you must first install it. If you are running Windows or OS X you can download an official release at https://www.wireshark.org/download.html, install it, and skip the rest of this chapter.

If you are running another operating system such as Linux or FreeBSD you might want to install from source. Several Linux distributions offer Wireshark packages but they commonly ship out-of-date versions. No other versions of UNIX ship Wireshark so far. For that reason, you will need to know where to get the latest version of Wireshark and how to install it.

This chapter shows you how to obtain source and binary packages and how to build Wireshark from source should you choose to do so.

The following are the general steps you would use:

1. Download the relevant package for your needs, e.g. source or binary distribution.
2. Compile the source into a binary if needed. This may involve building and/or installing other necessary packages.
3. Install the binaries into their final destinations.

2.2. Obtaining the source and binary distributions

You can obtain both source and binary distributions from the Wireshark web site: https://www.wireshark.org/. Select the download link and then select the desired binary or source package.

Download all required files

If you are building Wireshark from source you will In general, unless you have already downloaded Wireshark before, you will most likely need to download several source packages if you are building Wireshark from source. This is covered in more detail below.

Once you have downloaded the relevant files, you can go on to the next step.

2.3. Installing Wireshark under Windows

Windows installer names contain the platform and version. For example, Wireshark-win64-2.3.0.exe installs Wireshark 2.3.0 for 64-bit Windows. The Wireshark installer includes WinPcap which is required for packet capture.

Simply download the Wireshark installer from: https://www.wireshark.org/download.html and execute it. Official packages are signed by the **Wireshark Foundation**. You can choose to install several optional

components and select the location of the installed package. The default settings are recommended for most users.

2.3.1. Installation Components

On the *Choose Components* page of the installer you can select from the following:

- **Wireshark** - The network protocol analyzer that we all know and mostly love.
- **TShark** - A command-line network protocol analyzer. If you haven't tried it you should.
- **Wireshark 1 Legacy** - The old (GTK+) user interface in case you need it.
- **Plugins & Extensions** - Extras for the Wireshark and TShark dissection engines
  - **Dissector Plugins** - Plugins with some extended dissections.
  - **Tree Statistics Plugins** - Extended statistics.
  - **Mate - Meta Analysis and Tracing Engine** - User configurable extension(s) of the display filter engine, see https://wiki.wireshark.org/Mate for details.
  - **SNMP MIBs** - SNMP MIBs for a more detailed SNMP dissection.
- **Tools** - Additional command line tools to work with capture files
  - **Editcap** - Reads a capture file and writes some or all of the packets into another capture file.
  - **Text2Pcap** - Reads in an ASCII hex dump and writes the data into a pcap capture file.
  - **Reordercap** - Reorders a capture file by timestamp.
  - **Mergecap** - Combines multiple saved capture files into a single output file.
  - **Capinfos** - Provides information on capture files.
  - **Rawshark** - Raw packet filter.
- **User's Guide** - Local installation of the User's Guide. The Help buttons on most dialogs will require an internet connection to show help pages if the User's Guide is not installed locally.

2.3.2. Additional Tasks

- **Start Menu Shortcuts** - Add some start menu shortcuts.
- **Desktop Icon** - Add a Wireshark icon to the desktop.
- **Quick Launch Icon** - add a Wireshark icon to the Explorer quick launch toolbar.
- **Associate file extensions to Wireshark** - Associate standard network trace files to Wireshark.

2.3.3. Install Location

By default Wireshark installs into `%ProgramFiles%\Wireshark` on 32-bit Windows and `%ProgramFiles64%\Wireshark` on 64-bit Windows. This expands to `C:\Program Files\Wireshark` on most systems.

2.3.4. Installing WinPcap

The Wireshark installer contains the latest WinPcap installer.

If you don't have WinPcap installed you won't be able to capture live network traffic but you will still be able to open saved capture files. By default the latest version of WinPcap will be installed. If you don't wish to do this or if you wish to reinstall WinPcap you can check the *Install WinPcap* box as needed.

For more information about WinPcap see https://www.winpcap.org/ and https://wiki.wireshark.org/WinPcap.

2.3.5. Windows installer command line options

For special cases, there are some command line parameters available:

- `/S` runs the installer or uninstaller silently with default values. The silent installer **will not** install WinPCap.
- `/desktopicon` installation of the desktop icon, `=yes` - force installation, `=no` - don't install, otherwise use default settings. This option can be useful for a silent installer.
- `/quicklaunchicon` installation of the quick launch icon, `=yes` - force installation, `=no` - don't install, otherwise use default settings.
- `/D` sets the default installation directory ($INSTDIR), overriding InstallDir and InstallDirRegKey. It must be the last parameter used in the command line and must not contain any quotes even if the path contains spaces.
- `/NCRC` disables the CRC check. We recommend against using this flag.

Example:

```
> Wireshark-win64-wireshark-2.0.5.exe /NCRC /S /desktopicon=yes /quicklaunchicon=no /
D=C:\Program Files\Foo
```

Running the installer without any parameters shows the normal interactive installer.

2.3.6. Manual WinPcap Installation

As mentioned above, the Wireshark installer takes care of installing WinPcap. The following is only necessary if you want to use a different version than the one included in the Wireshark installer, e.g. because a new WinPcap version was released.

Additional WinPcap versions (including newer alpha or beta releases) can be downloaded from the main WinPcap site: https://www.winpcap.org/. The *Installer for Windows* supports modern Windows operating systems.

2.3.7. Update Wireshark

By default the offical Windows package will check for new versions and notify you when they are available. If you have the *Check for updates* preference disabled or if you run Wireshark in an isolated environment you should subcribe to the *wireshark-announce* mailing list. See Section 1.6.5, "Mailing Lists" for details on subscribing to this list.

New versions of Wireshark are usually released every four to six weeks. Updating Wireshark is done the same way as installing it. Simply download and start the installer exe. A reboot is usually not required and all your personal settings remain unchanged.

2.3.8. Update WinPcap

New versions of WinPcap are less frequently available. You will find WinPcap update instructions the WinPcap web site at https://www.winpcap.org/. You may have to reboot your machine after installing a new WinPcap version.

2.3.9. Uninstall Wireshark

You can uninstall Wireshark using the *Programs and Features* control panel. Select the "Wireshark" entry to start the uninstallation procedure.

The Wireshark uninstaller provides several options for removal. The default is to remove the core components but keep your personal settings and WinPcap. WinPcap is left installed by default in case other programs need it.

2.3.10. Uninstall WinPcap

You can uninstall WinPcap independently of Wireshark using the *WinPcap* entry in the *Programs and Features* control panel. Remember that if you uninstall WinPcap you won't be able to capture anything with Wireshark.

2.4. Installing Wireshark under OS X

The official OS X packages are distributed as disk images (.dmg) containing the application installer. To install Wireshark simply open the disk image and run the enclosed installer.

The installer package includes Wireshark, its related command line utilities, and a launch daemon that adjusts capture permissions at system startup. See the included *Read me first* file for more details.

2.5. Building Wireshark from source under UNIX

Building Wireshark requires the proper build environment including a compiler and many supporting libraries. See the Developer's Guide at https://www.wireshark.org/docs/ for more information.

Use the following general steps to build Wireshark from source under UNIX or Linux:

1. Unpack the source from its compressed `tar` file. If you are using Linux or your version of UNIX uses GNU `tar` you can use the following command:

   ```
   $ tar xaf wireshark-2.4.5.tar.xz
   ```

   In other cases you will have to use the following commands:

   ```
   $ xz -d wireshark-2.4.5.tar.xz
   $ tar xf wireshark-2.4.5.tar
   ```

2. Change directory to the Wireshark source directory.

```
$ cd wireshark-2.4.5
```

3. Configure your source so it will build correctly for your version of UNIX. You can do this with the following command:

   ```
   $ ./configure
   ```

   If this step fails you will have to rectify the problems and rerun `configure`. Troubleshooting hints are provided in Section 2.7, “Troubleshooting during the install on Unix”.

4. Build the sources.

   ```
   $ make
   ```

5. Install the software in its final destination.

   ```
   $ make install
   ```

Once you have installed Wireshark with *make install* above, you should be able to run it by entering `wireshark`.

2.6. Installing the binaries under UNIX

In general installing the binary under your version of UNIX will be specific to the installation methods used with your version of UNIX. For example, under AIX, you would use *smit* to install the Wireshark binary package, while under Tru64 UNIX (formerly Digital UNIX) you would use *setld*.

2.6.1. Installing from RPM’s under Red Hat and alike

Building RPMs from Wireshark’s source code results in several packages (most distributions follow the same system):

- The `wireshark` package contains the core Wireshark libraries and command-line tools.
- The `wireshark-qt` package contains the Qt-based GUI.
- The `wireshark-gtk` (formerly `wireshark-gnome`) package contains the legacy Gtk+ based GUI.

Many distributions use `yum` or a similar package management tool to make installation of software (including its dependencies) easier. If your distribution uses `yum`, use the following command to install Wireshark together with the Qt GUI:

```
yum install wireshark wireshark-qt
```

If you’ve built your own RPMs from the Wireshark sources you can install them by running, for example:

```
rpm -ivh wireshark-2.0.0-1.x86_64.rpm wireshark-qt-2.0.0-1.x86_64.rpm
```

If the above command fails because of missing dependencies, install the dependencies first, and then retry the step above.

2.6.2. Installing from deb’s under Debian, Ubuntu and other Debian derivatives

If you can just install from the repository then use

```
$ aptitude install wireshark
```

Aptitude should take care of all of the dependency issues for you.

Use the following command to install downloaded Wireshark deb's under Debian:

```
$ dpkg -i wireshark-common_2.0.5.0-1_i386.deb wireshark_wireshark-2.0.5.0-1_i386.deb
```

dpkg doesn't take care of all dependencies, but reports what's missing.

Capturing requires privileges

By installing Wireshark packages non-root users won't gain rights automatically to capture packets. To allow non-root users to capture packets follow the procedure described in /usr/share/doc/wireshark-common/README.Debian

2.6.3. Installing from portage under Gentoo Linux

Use the following command to install Wireshark under Gentoo Linux with all of the extra features:

```
$ USE="c-ares gtk ipv6 portaudio snmp ssl kerberos threads selinux" emerge wireshark
```

2.6.4. Installing from packages under FreeBSD

Use the following command to install Wireshark under FreeBSD:

```
$ pkg_add -r wireshark
```

pkg_add should take care of all of the dependency issues for you.

2.7. Troubleshooting during the install on Unix

A number of errors can occur during the installation process. Some hints on solving these are provided here.

If the `configure` stage fails you will need to find out why. You can check the file `config.log` in the source directory to find out what failed. The last few lines of this file should help in determining the problem.

The standard problems are that you do not have a required development package on your system or that the development package isn't new enough. Note that installing a library package isn't enough. You need to install its development package as well. `configure` will also fail if you do not have libpcap (at least the required include files) on your system.

If you cannot determine what the problems are, send an email to the *wireshark-dev* mailing list explaining your problem. Include the output from `config.log` and anything else you think is relevant such as a trace of the `make` stage.

2.8. Building from source under Windows

We strongly recommended that you use the binary installer for Windows unless you want to start developing Wireshark on the Windows platform.

For further information how to build Wireshark for Windows from the sources see the Developer's Guide at https://www.wireshark.org/docs/

You may also want to have a look at the Development Wiki (https://wiki.wireshark.org/Development) for the latest available development documentation.

Chapter 3. User Interface

3.1. Introduction

By now you have installed Wireshark and are most likely keen to get started capturing your first packets. In the next chapters we will explore:

- How the Wireshark user interface works
- How to capture packets in Wireshark
- How to view packets in Wireshark
- How to filter packets in Wireshark
- … and many other things!

3.2. Start Wireshark

You can start Wireshark from your shell or window manager.

Power user tip

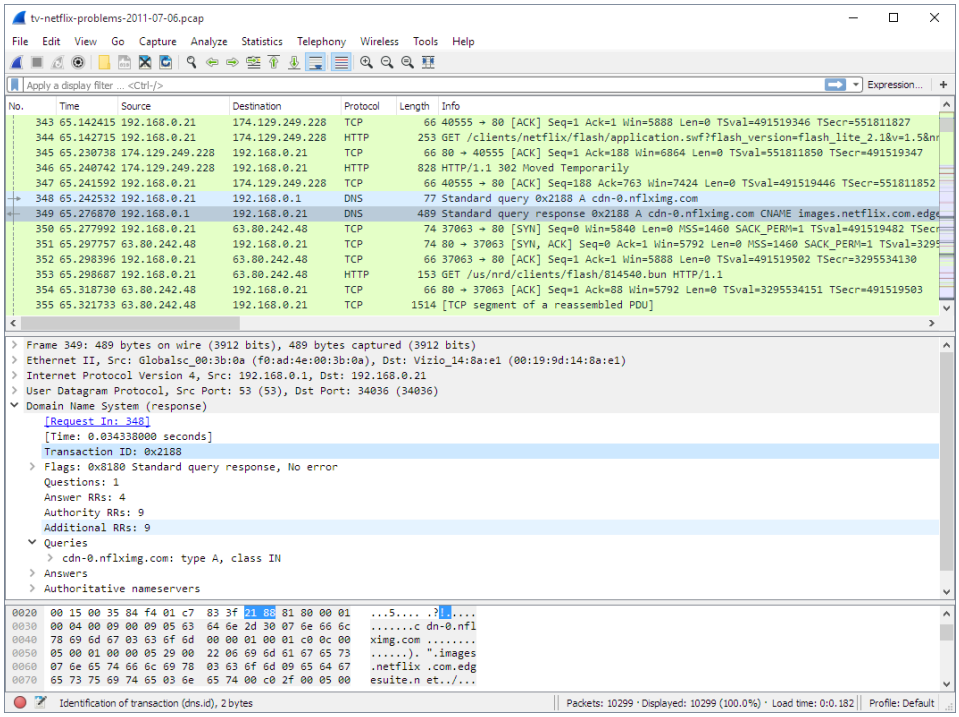
When starting Wireshark it's possible to specify optional settings using the command line. See Section 10.2, "Start Wireshark from the command line" for details.

In the following chapters a lot of screenshots from Wireshark will be shown. As Wireshark runs on many different platforms with many different window managers, different styles applied and there are different versions of the underlying GUI toolkit used, your screen might look different from the provided screenshots. But as there are no real differences in functionality these screenshots should still be well understandable.

3.3. The Main window

Let's look at Wireshark's user interface. Figure 3.1, "The Main window" shows Wireshark as you would usually see it after some packets are captured or loaded (how to do this will be described later).

Figure 3.1. The Main window



Wireshark's main window consists of parts that are commonly known from many other GUI programs.

1. The *menu* (see Section 3.4, "The Menu") is used to start actions.

2. The *main toolbar* (see Section 3.16, "The "Main" toolbar") provides quick access to frequently used items from the menu.

3. The *filter toolbar* (see Section 3.17, "The "Filter" toolbar") provides a way to directly manipulate the currently used display filter (see Section 6.3, "Filtering packets while viewing").

4. The *packet list pane* (see Section 3.18, "The "Packet List" pane") displays a summary of each packet captured. By clicking on packets in this pane you control what is displayed in the other two panes.

5. The *packet details pane* (see Section 3.19, "The "Packet Details" pane") displays the packet selected in the packet list pane in more detail.

6. The *packet bytes pane* (see Section 3.20, "The "Packet Bytes" pane") displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.

7. The *statusbar* (see Section 3.21, "The Statusbar") shows some detailed information about the current program state and the captured data.

Tip

The layout of the main window can be customized by changing preference settings. See Section 10.5, "Preferences" for details!

3.3.1. Main Window Navigation

Packet list and detail navigation can be done entirely from the keyboard. Table 3.1, “Keyboard Navigation” shows a list of keystrokes that will let you quickly move around a capture file. See Table 3.5, “Go menu items” for additional navigation keystrokes.

Table 3.1. Keyboard Navigation

Accelerator	Description
Tab, **Shift**+**Tab**	Move between screen elements, e.g. from the toolbars to the packet list to the packet detail.
Down	Move to the next packet or detail item.
Up	Move to the previous packet or detail item.
Ctrl+**Down**, **F8**	Move to the next packet, even if the packet list isn’t focused.
Ctrl+**Up**, **F7**	Move to the previous packet, even if the packet list isn’t focused.
Ctrl+**.**	Move to the next packet of the conversation (TCP, UDP or IP)
Ctrl+**,**	Move to the previous packet of the conversation (TCP, UDP or IP)
Left	In the packet detail, closes the selected tree item. If it’s already closed, jumps to the parent node.
Right	In the packet detail, opens the selected tree item.
Shift+**Right**	In the packet detail, opens the selected tree item and all of its subtrees.
Ctrl+**Right**	In the packet detail, opens all tree items.
Ctrl+**Left**	In the packet detail, closes all tree items.
Backspace	In the packet detail, jumps to the parent node.
Return, **Enter**	In the packet detail, toggles the selected tree item.

Help → About Wireshark → Keyboard Shortcuts will show a list of all shortcuts in the main window. Additionally, typing anywhere in the main window will start filling in a display filter.

3.4. The Menu

Wireshark’s main menu is located either at the top of the main window (Windows, Linux) or at the top of your main screen (OS X). An example is shown in Figure 3.2, “The Menu”.

Note

Some menu items will be disabled (greyed out(if the corresponding feature isn’t available. For example, you cannot save a capture file if you haven’t captured or loaded any packets.

Figure 3.2. The Menu

The main menu contains the following items:

File
: This menu contains items to open and merge capture files, save, print, or export capture files in whole or in part, and to quit the Wireshark application. See Section 3.5, “The “File” menu”.

Edit
: This menu contains items to find a packet, time reference or mark one or more packets, handle configuration profiles, and set your preferences; (cut, copy, and paste are not presently implemented). See Section 3.6, “The “Edit” menu”.

View
: This menu controls the display of the captured data, including colorization of packets, zooming the font, showing a packet in a separate window, expanding and collapsing trees in packet details, …. See Section 3.7, “The “View” menu”.

Go
: This menu contains items to go to a specific packet. See Section 3.8, “The “Go” menu”.

Capture
: This menu allows you to start and stop captures and to edit capture filters. See Section 3.9, “The “Capture” menu”.

Analyze
: This menu contains items to manipulate display filters, enable or disable the dissection of protocols, configure user specified decodes and follow a TCP stream. See Section 3.10, “The “Analyze” menu”.

Statistics
: This menu contains items to display various statistic windows, including a summary of the packets that have been captured, display protocol hierarchy statistics and much more. See Section 3.11, “The “Statistics” menu”.

Telephony
: This menu contains items to display various telephony related statistic windows, including a media analysis, flow diagrams, display protocol hierarchy statistics and much more. See Section 3.12, “The “Telephony” menu”.

Wireless
: The items in this menu show Bluetooth and IEEE 802.11 wireless statistics.

Tools
: This menu contains various tools available in Wireshark, such as creating Firewall ACL Rules. See Section 3.13, “The “Tools” menu”.

Help
: This menu contains items to help the user, e.g. access to some basic help, manual pages of the various command line tools, online access to some of the webpages, and the usual about dialog. See Section 3.15, “The “Help” menu”.

Each of these menu items is described in more detail in the sections that follow.

Shortcuts make life easier

Most common menu items have keyboard shortcuts. For example, you can press the Control (or Strg in German) and the K keys together to open the “Capture Options” dialog.

3.5. The “File” menu

The Wireshark file menu contains the fields shown in Table 3.2, “File menu items”.

Figure 3.3. The “File” Menu

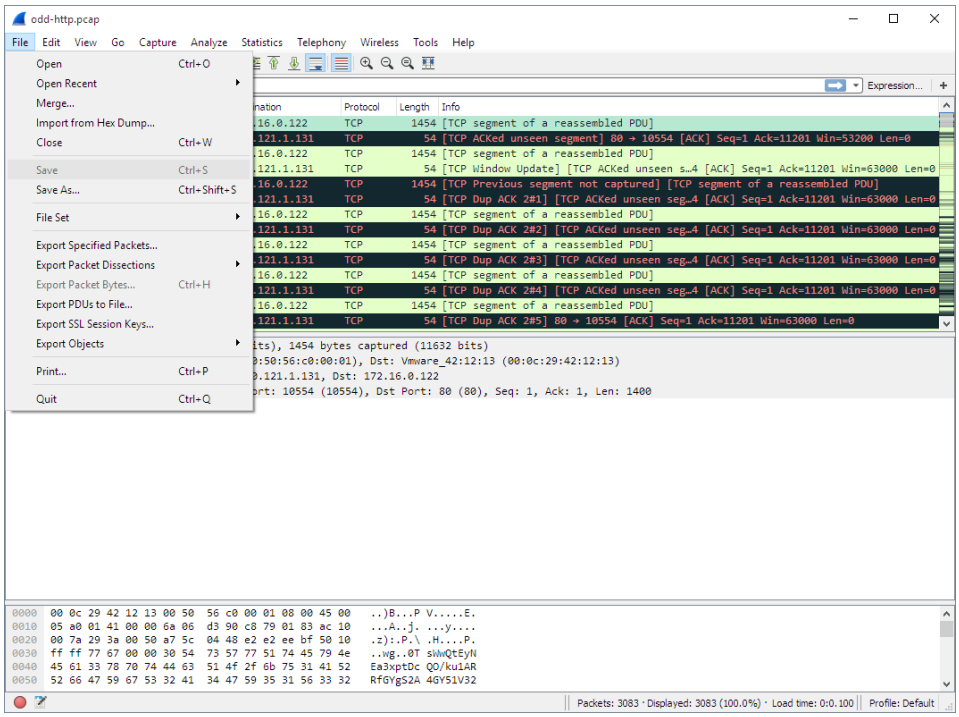


Table 3.2. File menu items

Menu Item	Accelerator	Description
Open…	**Ctrl**+**O**	This shows the file open dialog box that allows you to load a capture file for viewing. It is discussed in more detail in Section 5.2.1, “The “Open Capture File” dialog box”.
Open Recent		This lets you open recently opened capture files. Clicking on one of the submenu items will open the corresponding capture file directly.
Merge…		This menu item lets you merge a capture file into the currently loaded one. It is discussed in more detail in Section 5.4, “Merging capture files”.
Import from Hex Dump…		This menu item brings up the import file dialog box that allows you to import a text file containing a hex dump into a new temporary capture. It is discussed in more detail in Section 5.5, “Import hex dump”.
Close	**Ctrl**+**W**	This menu item closes the current capture. If you haven’t saved the capture, you will be asked to do so first (this can be disabled by a preference setting).
Save	**Ctrl**+**S**	This menu item saves the current capture. If you have not set a default capture file name (perhaps with the -w <capfile> option), Wireshark pops up the Save Capture File As dialog box (which

Menu Item	Accelerator	Description
		is discussed further in Section 5.3.1, “The “Save Capture File As” dialog box”). If you have already saved the current capture, this menu item will be greyed out. You cannot save a live capture while the capture is in progress. You must stop the capture in order to save.
Save As…	**Shift**+**Ctrl**+**S**	This menu item allows you to save the current capture file to whatever file you would like. It pops up the Save Capture File As dialog box (which is discussed further in Section 5.3.1, “The “Save Capture File As” dialog box”).
File Set → List Files		This menu item allows you to show a list of files in a file set. It pops up the Wireshark List File Set dialog box (which is discussed further in Section 5.6, “File Sets”).
File Set → Next File		If the currently loaded file is part of a file set, jump to the next file in the set. If it isn’t part of a file set or just the last file in that set, this item is greyed out.
File Set → Previous File		If the currently loaded file is part of a file set, jump to the previous file in the set. If it isn’t part of a file set or just the first file in that set, this item is greyed out.
Export Specified Packets…		This menu item allows you to export all (or some) of the packets in the capture file to file. It pops up the Wireshark Export dialog box (which is discussed further in Section 5.7, “Exporting data”).
Export Packet Dissections…	**Ctrl**+**H**	These menu items allow you to export the currently selected bytes in the packet bytes pane to a text file file in a number of formats including plain, CSV, and XML. It is discussed further in Section 5.7.7, “The "Export selected packet bytes" dialog box”.
Export Objects		These menu items allow you to export captured DICOM, HTTP, SMB, or TFTP objects into local files. It pops up a corresponding object list (which is discussed further in Section 5.7.8, “The "Export Objects" dialog box”)
Print…	**Ctrl**+**P**	This menu item allows you to print all (or some) of the packets in the capture file. It pops up the Wireshark Print dialog box (which is discussed further in Section 5.8, “Printing packets”).
Quit	**Ctrl**+**Q**	This menu item allows you to quit from Wireshark. Wireshark will ask to save your capture file if you haven’t previously saved it (this can be disabled by a preference setting).

3.6. The “Edit” menu

The Wireshark Edit menu contains the fields shown in Table 3.3, “Edit menu items”.

Figure 3.4. The “Edit” Menu

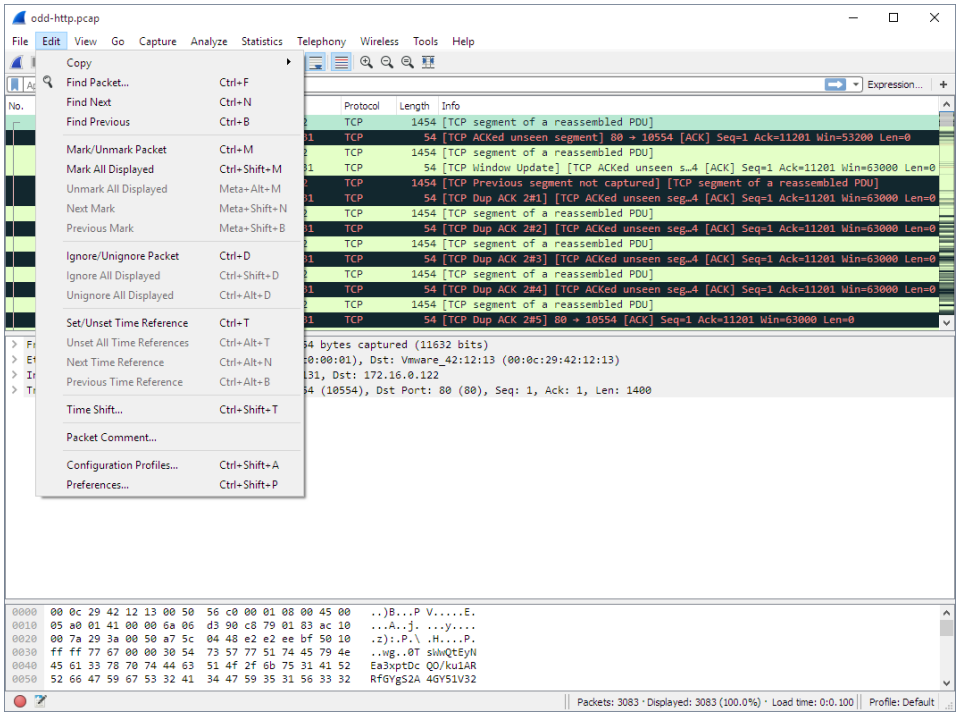


Table 3.3. Edit menu items

Menu Item	Accelerator	Description
Copy		These menu items will copy the packet list, packet detail, or properties of the currently selected packet to the clipboard.
Find Packet…	**Ctrl**+**F**	This menu item brings up a toolbar that allows you to find a packet by many criteria. There is further information on finding packets in Section 6.8, “Finding packets”.
Find Next	**Ctrl**+**N**	This menu item tries to find the next packet matching the settings from “Find Packet…”.
Find Previous	**Ctrl**+**B**	This menu item tries to find the previous packet matching the settings from “Find Packet…”.
Mark/Unmark Packet	**Ctrl**+**M**	This menu item marks the currently selected packet. See Section 6.10, “Marking packets” for details.
Mark All Displayed Packets	**Shift**+**Ctrl**+**M**	This menu item marks all displayed packets.
Unmark All Displayed Packets	**Ctrl**+**Alt**+**M**	This menu item unmarks all displayed packets.

Menu Item	Accelerator	Description
Next Mark	**Shift**+**Alt**+**N**	Find the next marked packet.
Previous Mark	**Shift**+**Alt**+**B**	Find the previous marked packet.
Ignore/Unignore Packet	**Ctrl**+**D**	This menu item marks the currently selected packet as ignored. See Section 6.11, “Ignoring packets” for details.
Ignore All Displayed	**Shift**+**Ctrl**+**D**	This menu item marks all displayed packets as ignored.
Unignore All Displayed	**Ctrl**+**Alt**+**D**	This menu item unmarks all ignored packets.
Set/Unset Time Reference	**Ctrl**+**T**	This menu item set a time reference on the currently selected packet. See Section 6.12.1, “Packet time referencing” for more information about the time referenced packets.
Unset All Time References	**Ctrl**+**Alt**+**T**	This menu item removes all time references on the packets.
Next Time Reference	**Ctrl**+**Alt**+**N**	This menu item tries to find the next time referenced packet.
Previous Time Reference	**Ctrl**+**Alt**+**B**	This menu item tries to find the previous time referenced packet.
Time Shift	**Ctrl**+**Shift**+**T**	This will show the Time Shift dialog, which allows you to adjust the timestamps of some or all packets.
Packet Comment…		This will let you add a comment to a single packet. Note that the ability to save packet comments depends on your file format. E.g. pcapng supports comments, pcap does not.
Capture Comment…		This will let you add a capture comment. Note that the ability to save capture comments depends on your file format. E.g. pcapng supports comments, pcap does not.
Configuration Profiles…	**Shift**+**Ctrl**+**A**	This menu item brings up a dialog box for handling configuration profiles. More detail is provided in Section 10.6, “Configuration Profiles”.
Preferences…	**Shift**+**Ctrl**+**P** or **Cmd**+ (OS X)	This menu item brings up a dialog box that allows you to set preferences for many parameters that control Wireshark. You can also save your preferences so Wireshark will use them the next time you start it. More detail is provided in Section 10.5, “Preferences”.

3.7. The “View” menu

The Wireshark View menu contains the fields shown in Table 3.4, “View menu items”.

Figure 3.5. The “View” Menu

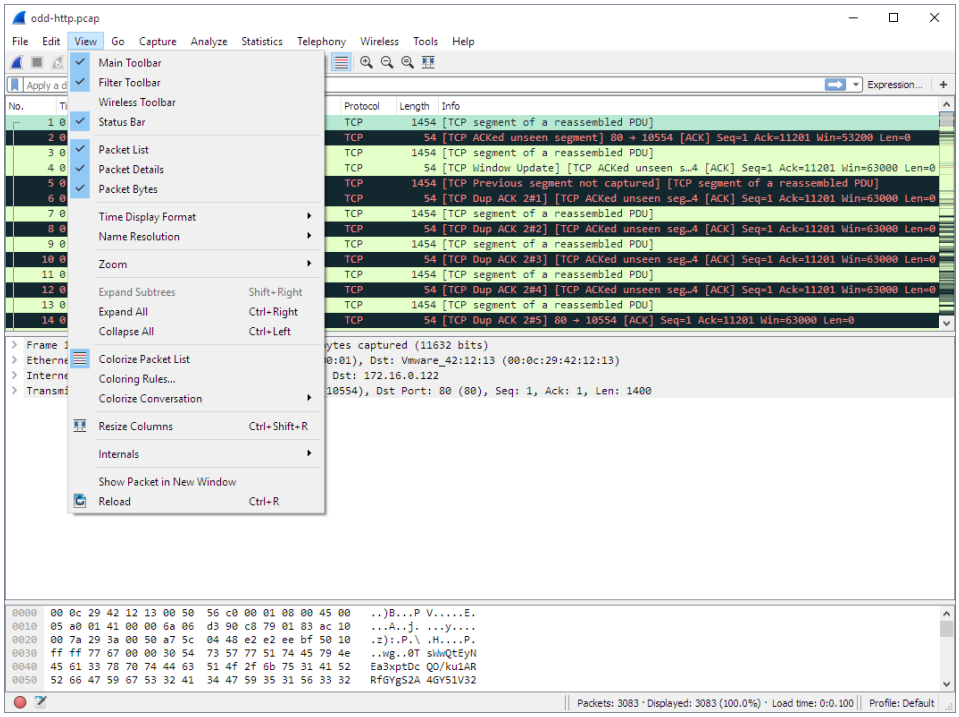


Table 3.4. View menu items

Menu Item	Accelerator	Description
Main Toolbar		This menu item hides or shows the main toolbar, see Section 3.16, “The “Main” toolbar”.
Filter Toolbar		This menu item hides or shows the filter toolbar, see Section 3.17, “The “Filter” toolbar”.
Wireless Toolbar		This menu item hides or shows the wireless toolbar. May not be present on some platforms.
Statusbar		This menu item hides or shows the statusbar, see Section 3.21, “The Statusbar”.
Packet List		This menu item hides or shows the packet list pane, see Section 3.18, “The “Packet List” pane”.
Packet Details		This menu item hides or shows the packet details pane, see Section 3.19, “The “Packet Details” pane”.
Packet Bytes		This menu item hides or shows the packet bytes pane, see Section 3.20, “The “Packet Bytes” pane”.
Time Display Format → Date and Time of Day: 1970-01-01 01:02:03.123456		Selecting this tells Wireshark to display the time stamps in date and time of day format, see Section 6.12, “Time display formats and time references”. The fields "Time of Day", "Date and Time of Day", "Seconds Since Beginning of Capture",

Menu Item	Accelerator	Description
		"Seconds Since Previous Captured Packet" and "Seconds Since Previous Displayed Packet" are mutually exclusive.
Time Display Format → Time of Day: 01:02:03.123456		Selecting this tells Wireshark to display time stamps in time of day format, see Section 6.12, "Time display formats and time references".
Time Display Format → Seconds Since Epoch (1970-01-01): 1234567890.123456		Selecting this tells Wireshark to display time stamps in seconds since 1970-01-01 00:00:00, see Section 6.12, "Time display formats and time references".
Time Display Format → Seconds Since Beginning of Capture: 123.123456		Selecting this tells Wireshark to display time stamps in seconds since beginning of capture format, see Section 6.12, "Time display formats and time references".
Time Display Format → Seconds Since Previous Captured Packet: 1.123456		Selecting this tells Wireshark to display time stamps in seconds since previous captured packet format, see Section 6.12, "Time display formats and time references".
Time Display Format → Seconds Since Previous Displayed Packet: 1.123456		Selecting this tells Wireshark to display time stamps in seconds since previous displayed packet format, see Section 6.12, "Time display formats and time references".
Time Display Format → Automatic (File Format Precision)		Selecting this tells Wireshark to display time stamps with the precision given by the capture file format used, see Section 6.12, "Time display formats and time references". The fields "Automatic", "Seconds" and "… seconds" are mutually exclusive.
Time Display Format → Seconds: 0		Selecting this tells Wireshark to display time stamps with a precision of one second, see Section 6.12, "Time display formats and time references".
Time Display Format → … seconds: 0….		Selecting this tells Wireshark to display time stamps with a precision of one second, decisecond, centisecond, millisecond, microsecond or nanosecond, see Section 6.12, "Time display formats and time references".
Time Display Format → Display Seconds with hours and minutes		Selecting this tells Wireshark to display time stamps in seconds, with hours and minutes.
Name Resolution → Resolve Name		This item allows you to trigger a name resolve of the current packet only, see Section 7.8, "Name Resolution".
Name Resolution → Enable for MAC Layer		This item allows you to control whether or not Wireshark translates MAC addresses into names, see Section 7.8, "Name Resolution".

Menu Item	Accelerator	Description
Name Resolution → Enable for Network Layer		This item allows you to control whether or not Wireshark translates network addresses into names, see Section 7.8, “Name Resolution”.
Name Resolution → Enable for Transport Layer		This item allows you to control whether or not Wireshark translates transport addresses into names, see Section 7.8, “Name Resolution”.
Colorize Packet List		This item allows you to control whether or not Wireshark should colorize the packet list. Enabling colorization will slow down the display of new packets while capturing / loading capture files.
Auto Scroll in Live Capture		This item allows you to specify that Wireshark should scroll the packet list pane as new packets come in, so you are always looking at the last packet. If you do not specify this, Wireshark simply adds new packets onto the end of the list, but does not scroll the packet list pane.
Zoom In	**Ctrl**++	Zoom into the packet data (increase the font size).
Zoom Out	**Ctrl**+-	Zoom out of the packet data (decrease the font size).
Normal Size	**Ctrl**+=	Set zoom level back to 100% (set font size back to normal).
Resize All Columns	**Shift**+**Ctrl**+**R**	Resize all column widths so the content will fit into it. Resizing may take a significant amount of time, especially if a large capture file is loaded.
Displayed Columns		This menu items folds out with a list of all configured columns. These columns can now be shown or hidden in the packet list.
Expand Subtrees	**Shift**+→	This menu item expands the currently selected subtree in the packet details tree.
Collapse Subtrees	**Shift**+←	This menu item collapses the currently selected subtree in the packet details tree.
Expand All	**Ctrl**+→	Wireshark keeps a list of all the protocol subtrees that are expanded, and uses it to ensure that the correct subtrees are expanded when you display a packet. This menu item expands all subtrees in all packets in the capture.
Collapse All	**Ctrl**+←	This menu item collapses the tree view of all packets in the capture list.
Colorize Conversation		This menu item brings up a submenu that allows you to color packets in the packet list pane based on the addresses of the currently selected packet. This makes it easy to distinguish packets

Menu Item	Accelerator	Description
		belonging to different conversations. Section 10.3, “Packet colorization”.
Colorize Conversation → Color 1-10		These menu items enable one of the ten temporary color filters based on the currently selected conversation.
Colorize Conversation → Reset coloring		This menu item clears all temporary coloring rules.
Colorize Conversation → New Coloring Rule…		This menu item opens a dialog window in which a new permanent coloring rule can be created based on the currently selected conversation.
Coloring Rules…		This menu item brings up a dialog box that allows you to color packets in the packet list pane according to filter expressions you choose. It can be very useful for spotting certain types of packets, see Section 10.3, “Packet colorization”.
Show Packet in New Window		This menu item brings up the selected packet in a separate window. The separate window shows only the tree view and byte view panes.
Reload	**Ctrl+R**	This menu item allows you to reload the current capture file.

3.8. The “Go” menu

The Wireshark Go menu contains the fields shown in Table 3.5, “Go menu items”.

Figure 3.6. The “Go” Menu

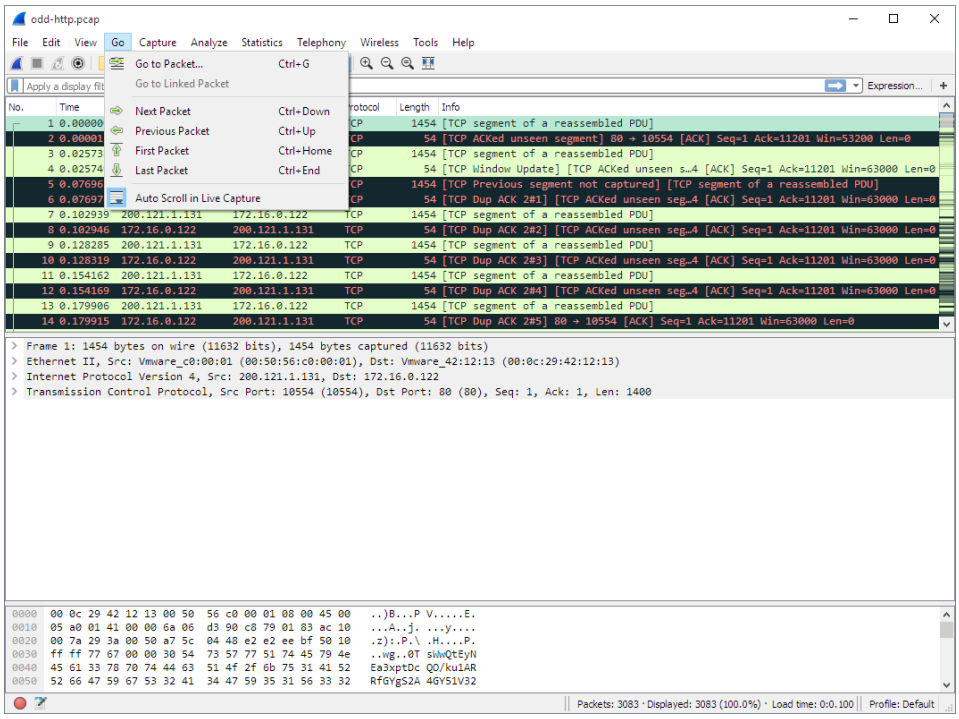


Table 3.5. Go menu items

Menu Item	Accelerator	Description
Back	**Alt**+←	Jump to the recently visited packet in the packet history, much like the page history in a web browser.
Forward	**Alt**+→	Jump to the next visited packet in the packet history, much like the page history in a web browser.
Go to Packet…	**Ctrl**+**G**	Bring up a window frame that allows you to specify a packet number, and then goes to that packet. See Section 6.9, “Go to a specific packet” for details.
Go to Corresponding Packet		Go to the corresponding packet of the currently selected protocol field. If the selected field doesn’t correspond to a packet, this item is greyed out.
Previous Packet	**Ctrl**+↑	Move to the previous packet in the list. This can be used to move to the previous packet even if the packet list doesn’t have keyboard focus.
Next Packet	**Ctrl**+↓	Move to the next packet in the list. This can be used to move to the previous packet even if the packet list doesn’t have keyboard focus.
First Packet	**Ctrl**+**Home**	Jump to the first packet of the capture file.
Last Packet	**Ctrl**+**End**	Jump to the last packet of the capture file.
Previous Packet In Conversation	**Ctrl**+**,**	Move to the previous packet in the current conversation. This can be used to move to the previous packet even if the packet list doesn’t have keyboard focus.
Next Packet In Conversation	**Ctrl**+**.**	Move to the next packet in the current conversation. This can be used to move to the previous packet even if the packet list doesn’t have keyboard focus.

3.9. The “Capture” menu

The Wireshark Capture menu contains the fields shown in Table 3.6, “Capture menu items”.

Figure 3.7. The “Capture” Menu

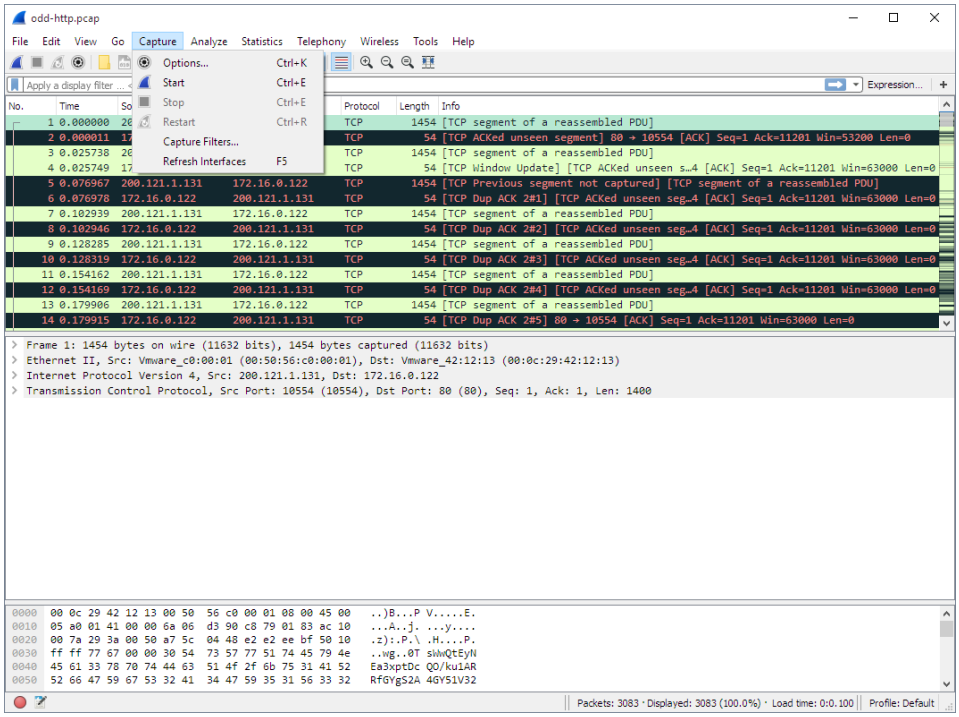


Table 3.6. Capture menu items

Menu Item	Accelerator	Description
Interfaces…	**Ctrl**+**I**	This menu item brings up a dialog box that shows what’s going on at the network interfaces Wireshark knows of, see Section 4.4, “The “Capture Interfaces” dialog box”) .
Options…	**Ctrl**+**K**	This menu item brings up the Capture Options dialog box (discussed further in Section 4.5, “The “Capture Options” dialog box”) and allows you to start capturing packets.
Start	**Ctrl**+**E**	Immediately start capturing packets with the same settings than the last time.
Stop	**Ctrl**+**E**	This menu item stops the currently running capture, see Section 4.13.2, “Stop the running capture”) .
Restart	**Ctrl**+**R**	This menu item stops the currently running capture and starts again with the same options, this is just for convenience.
Capture Filters…		This menu item brings up a dialog box that allows you to create and edit capture filters. You can name filters, and you can save them for future use. More detail on this subject is provided in Section 6.6, “Defining and saving filters”

3.10. The “Analyze” menu

The Wireshark Analyze menu contains the fields shown in Table 3.7, “Analyze menu items”.

Figure 3.8. The “Analyze” Menu

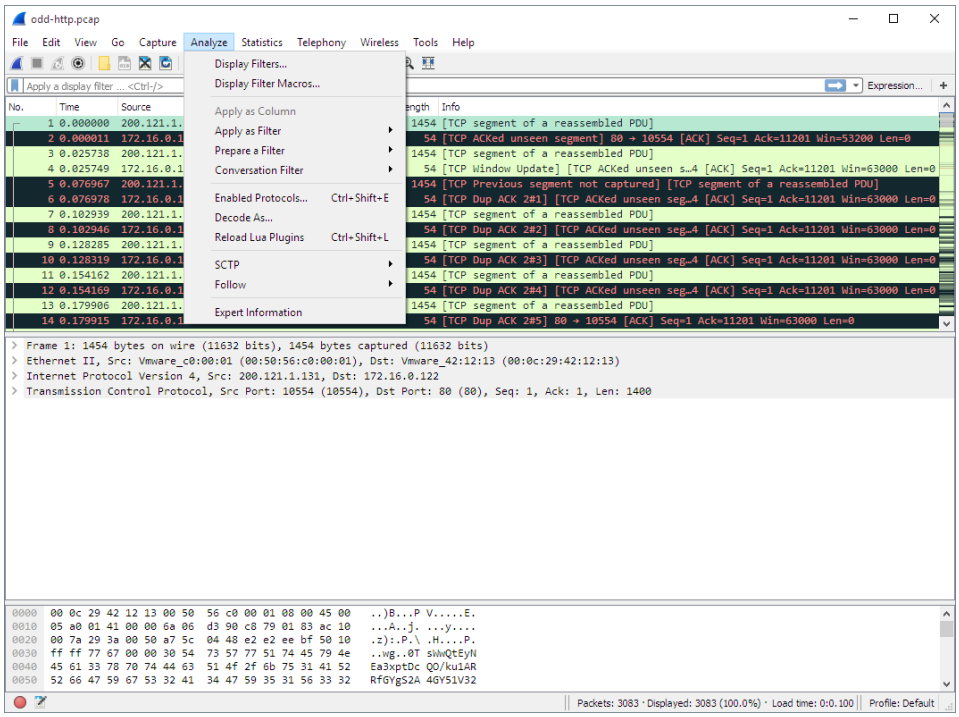


Table 3.7. Analyze menu items

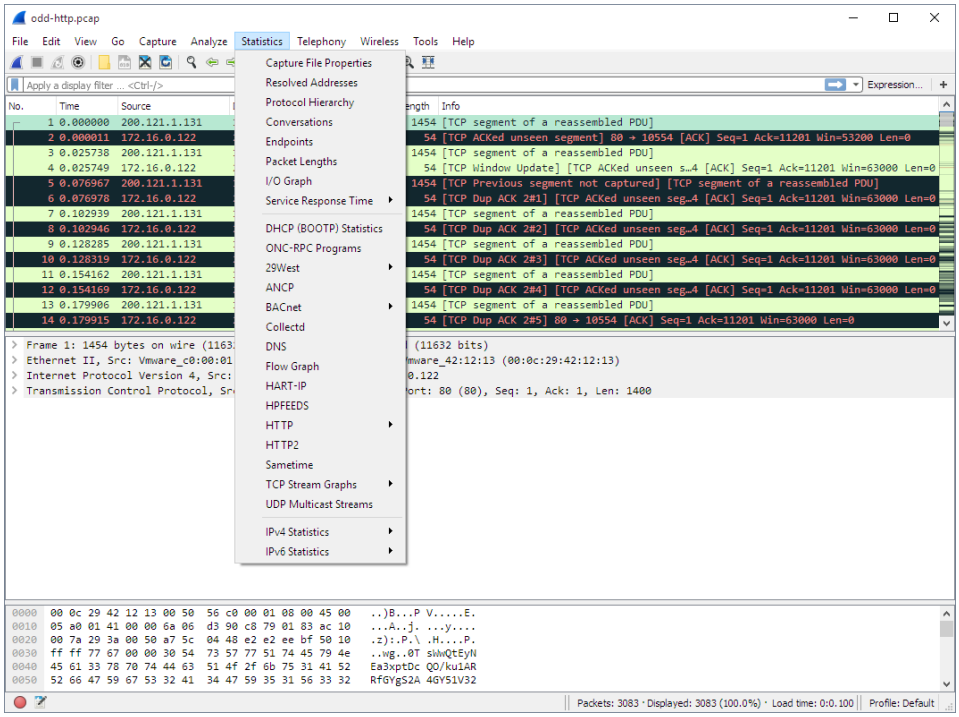
Menu Item	Accelerator	Description
Display Filters…		This menu item brings up a dialog box that allows you to create and edit display filters. You can name filters, and you can save them for future use. More detail on this subject is provided in Section 6.6, “Defining and saving filters”
Display Filter Macros…		This menu item brings up a dialog box that allows you to create and edit display filter macros. You can name filter macros, and you can save them for future use. More detail on this subject is provided in Section 6.7, “Defining and saving filter macros”
Apply as Column		This menu item adds the selected protocol item in the packet details pane as a column to the packet list.
Apply as Filter → …		These menu items will change the current display filter and apply the changed filter immediately. Depending on the chosen menu item, the current display filter string will be replaced or appended to by the selected protocol field in the packet details pane.

Menu Item	Accelerator	Description
Prepare a Filter → …		These menu items will change the current display filter but won't apply the changed filter. Depending on the chosen menu item, the current display filter string will be replaced or appended to by the selected protocol field in the packet details pane.
Enabled Protocols…	**Shift+Ctrl+E**	This menu item allows the user to enable/disable protocol dissectors, see Section 10.4.1, "The "Enabled Protocols" dialog box"
Decode As…		This menu item allows the user to force Wireshark to decode certain packets as a particular protocol, see Section 10.4.2, "User Specified Decodes"
User Specified Decodes…		This menu item allows the user to force Wireshark to decode certain packets as a particular protocol, see Section 10.4.3, "Show User Specified Decodes"
Follow TCP Stream		This menu item brings up a separate window and displays all the TCP segments captured that are on the same TCP connection as a selected packet, see Section 7.2, "Following TCP streams"
Follow UDP Stream		Same functionality as "Follow TCP Stream" but for UDP streams.
Follow SSL Stream		Same functionality as "Follow TCP Stream" but for SSL streams. See the wiki page on SSL for instructions on providing SSL keys.
Expert Info		Open a dialog showing some expert information about the captured packets. The amount of information will depend on the protocol and varies from very detailed to non-existent. XXX - add a new section about this and link from here
Conversation Filter → …		In this menu you will find conversation filter for various protocols.

3.11. The "Statistics" menu

The Wireshark Statistics menu contains the fields shown in Table 3.8, "Statistics menu items".

Figure 3.9. The “Statistics” Menu



All menu items will bring up a new window showing specific statistical information.

Table 3.8. Statistics menu items

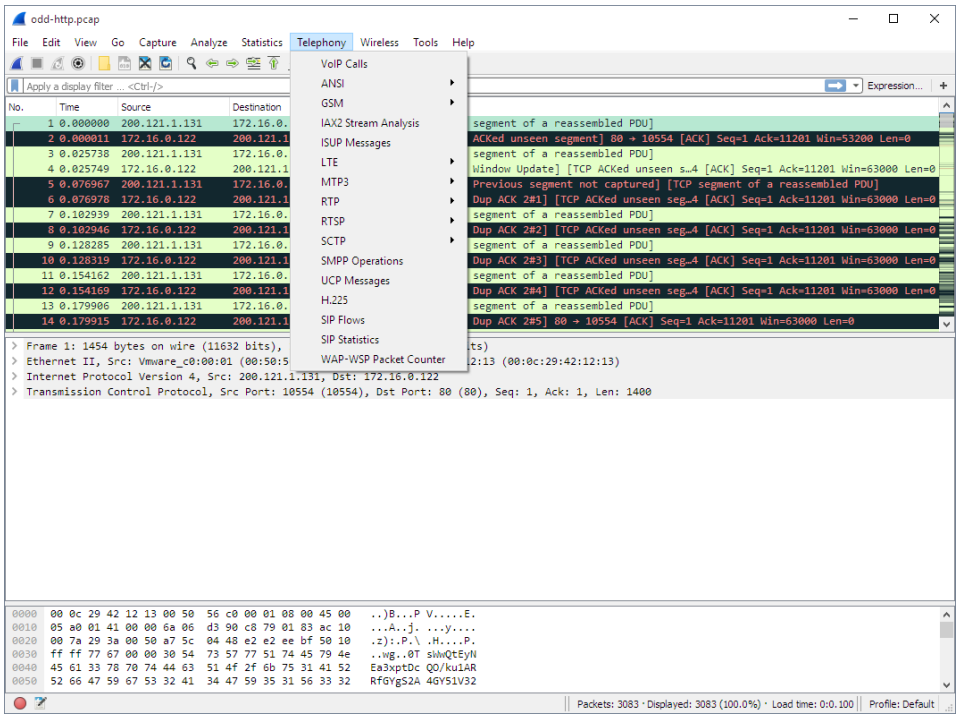
Menu Item	Accelerator	Description
Summary		Show information about the data captured, see Section 8.2, “The “Summary” window”.
Protocol Hierarchy		Display a hierarchical tree of protocol statistics, see Section 8.3, “The “Protocol Hierarchy” window”.
Conversations		Display a list of conversations (traffic between two endpoints), see Section 8.4.1, “The “Conversations” window”.
Endpoints		Display a list of endpoints (traffic to/from an address), see Section 8.5.1, “The “Endpoints” window”.
Packet Lengths…		See Section 8.10, “The protocol specific statistics windows”
IO Graphs		Display user specified graphs (e.g. the number of packets in the course of time), see Section 8.6, “The “IO Graphs” window”.
Service Response Time		Display the time between a request and the corresponding response, see Section 8.7, “Service Response Time”.
ANCP		See Section 8.10, “The protocol specific statistics windows”

Menu Item	Accelerator	Description
Colledtd…		See Section 8.10, “The protocol specific statistics windows”
Compare…		See Section 8.10, “The protocol specific statistics windows”
Flow Graph…		See Section 8.10, “The protocol specific statistics windows”
HTTP		HTTP request/response statistics, see Section 8.10, “The protocol specific statistics windows”
IP Addresses…		See Section 8.10, “The protocol specific statistics windows”
IP Destinations…		See Section 8.10, “The protocol specific statistics windows”
IP Protocol Types…		See Section 8.10, “The protocol specific statistics windows”
ONC-RPC Programs		See Section 8.10, “The protocol specific statistics windows”
Sametime		See Section 8.10, “The protocol specific statistics windows”
TCP Stream Graph		See Section 8.10, “The protocol specific statistics windows”
UDP Multicast Streams		See Section 8.10, “The protocol specific statistics windows”
WLAN Traffic		See Section 8.9, “WLAN Traffic Statistics”
BOOTP-DHCP		See Section 8.10, “The protocol specific statistics windows”

3.12. The “Telephony” menu

The Wireshark Telephony menu contains the fields shown in Table 3.9, “Telephony menu items”.

Figure 3.10. The “Telephony” Menu



All menu items will bring up a new window showing specific telephony related statistical information.

Table 3.9. Telephony menu items

Menu Item	Accelerator	Description
IAX2		See Section 9.7, “The protocol specific statistics windows”
SMPP Operations…		See Section 9.7, “The protocol specific statistics windows”
SCTP		See Section 9.7, “The protocol specific statistics windows”
ANSI		See Section 9.7, “The protocol specific statistics windows”
GSM		See Section 9.7, “The protocol specific statistics windows”
H.225…		See Section 9.7, “The protocol specific statistics windows”
ISUP Messages…		See Section 9.7, “The protocol specific statistics windows”
LTE		See Section 9.5, “LTE MAC Traffic Statistics”
MTP3		See Section 9.7, “The protocol specific statistics windows”
RTP		See Section 9.2, “RTP Analysis”
SIP…		See Section 9.7, “The protocol specific statistics windows”

Menu Item	Accelerator	Description
UCP Messages…		See Section 9.7, “The protocol specific statistics windows”
VoIP Calls…		See Section 9.4, “VoIP Calls”
WAP-WSP…		See Section 9.7, “The protocol specific statistics windows”

3.13. The “Tools” menu

The Wireshark Tools menu contains the fields shown in Table 3.10, “Tools menu items”.

Figure 3.11. The “Tools” Menu

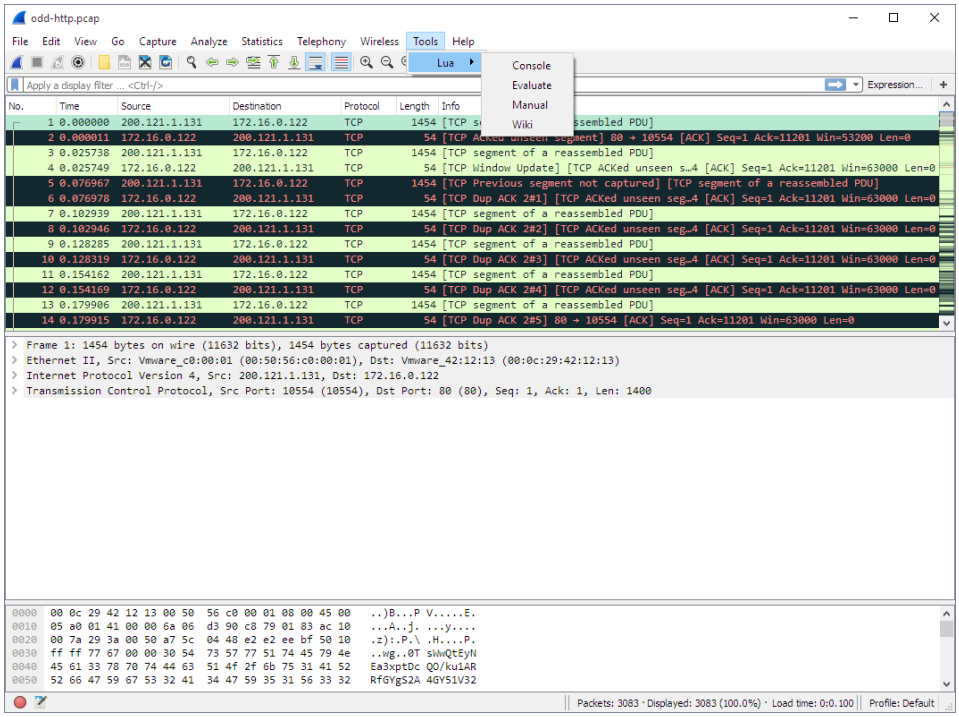


Table 3.10. Tools menu items

Menu Item	Accelerator	Description
Firewall ACL Rules		This allows you to create command-line ACL rules for many different firewall products, including Cisco IOS, Linux Netfilter (iptables), OpenBSD pf and Windows Firewall (via netsh). Rules for MAC addresses, IPv4 addresses, TCP and UDP ports, and IPv4+port combinations are supported. It is assumed that the rules will be applied to an outside interface.
Lua		These options allow you to work with the Lua interpreter optionally build into Wireshark. See

Menu Item	Accelerator	Description
		the “Lua Support in Wireshark” in the Wireshark Developer’s Guide.

3.14. The “Internals” menu

The Wireshark Internals menu contains the fields shown in Table 3.11, “Internals menu items”.

Figure 3.12. The “Internals” Menu

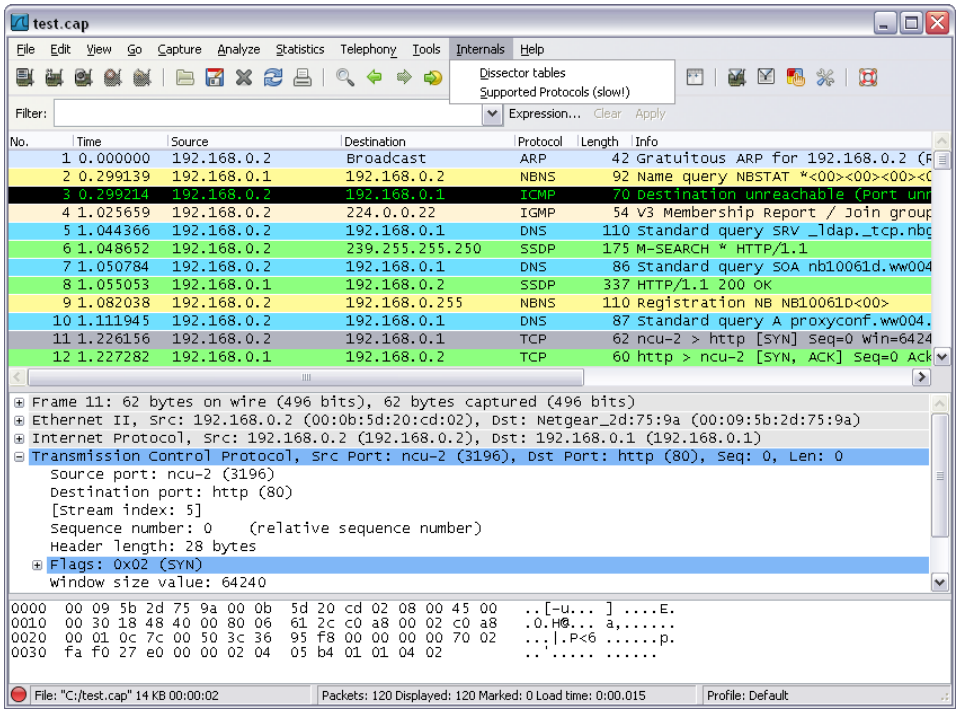


Table 3.11. Internals menu items

Menu Item	Accelerator	Description
Dissector tables		This menu item brings up a dialog box showing the tables with subdissector relationships.
Supported Protocols (slow!)		This menu item brings up a dialog box showing the supported protocols and protocol fields.

3.15. The “Help” menu

The Wireshark Help menu contains the fields shown in Table 3.12, “Help menu items”.

Figure 3.13. The “Help” Menu

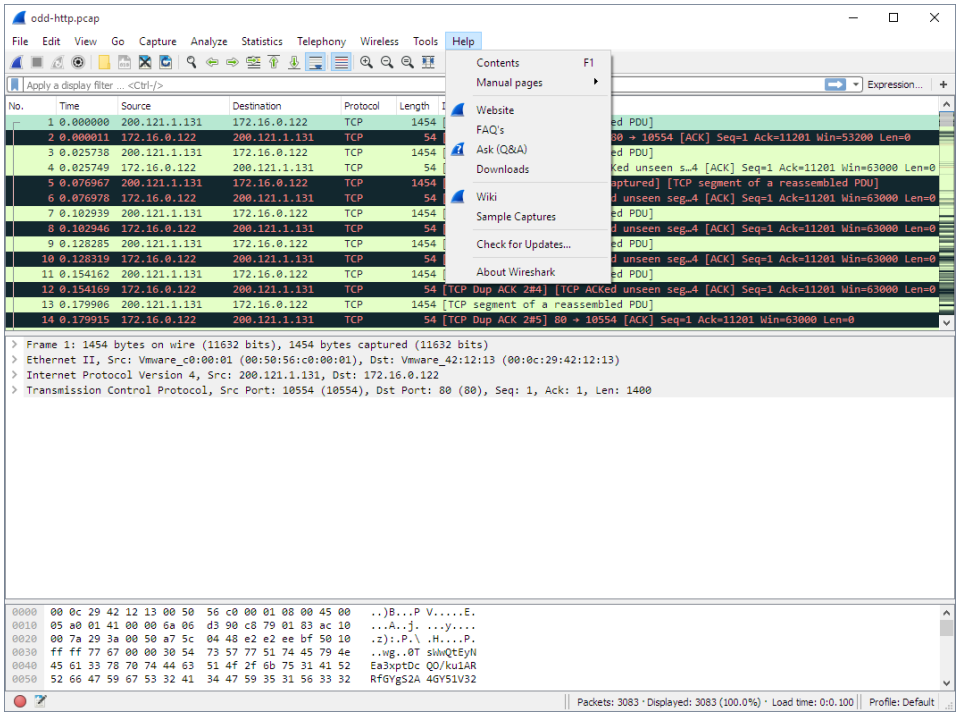


Table 3.12. Help menu items

Menu Item	Accelerator	Description
Contents	F1	This menu item brings up a basic help system.
Manual Pages → …		This menu item starts a Web browser showing one of the locally installed html manual pages.
Website		This menu item starts a Web browser showing the webpage from: https://www.wireshark.org/.
FAQ’s		This menu item starts a Web browser showing various FAQ’s.
Downloads		This menu item starts a Web browser showing the downloads from: https://www.wireshark.org/.
Wiki		This menu item starts a Web browser showing the front page from: https://wiki.wireshark.org/.
Sample Captures		This menu item starts a Web browser showing the sample captures from: https://wiki.wireshark.org/.
About Wireshark		This menu item brings up an information window that provides various detailed information items on Wireshark, such as how it’s build, the plugins loaded, the used folders, …

Note

Opening a Web browser might be unsupported in your version of Wireshark. If this is the case the corresponding menu items will be hidden.

If calling a Web browser fails on your machine, nothing happens, or the browser starts but no page is shown, have a look at the web browser setting in the preferences dialog.

3.16. The “Main” toolbar

The main toolbar provides quick access to frequently used items from the menu. This toolbar cannot be customized by the user, but it can be hidden using the View menu, if the space on the screen is needed to show even more packet data.

As in the menu, only the items useful in the current program state will be available. The others will be greyed out (e.g. you cannot save a capture file if you haven’t loaded one).

Figure 3.14. The “Main” toolbar

Table 3.13. Main toolbar items

Toolbar Icon	Toolbar Item	Menu Item	Description
	Interfaces…	Capture → Interfaces…	This item brings up the Capture Interfaces List dialog box (discussed further in Section 4.3, “Start Capturing”).
	Options…	Capture → Options…	This item brings up the Capture Options dialog box (discussed further in Section 4.3, “Start Capturing”) and allows you to start capturing packets.
	Start	Capture → Start	This item starts capturing packets with the options form the last time.
	Stop	Capture → Stop	This item stops the currently running live capture process Section 4.3, “Start Capturing”).
	Restart	Capture → Restart	This item stops the currently running live capture process and restarts it again, for convenience.
	Open…	File → Open…	This item brings up the file open dialog box that allows you to load a capture file for viewing. It is discussed in more detail in Section 5.2.1, “The “Open Capture File” dialog box”.
	Save As…	File → Save As…	This item allows you to save the current capture file to whatever file you would like. It pops up the Save Capture File As dialog box (which is discussed further in Section 5.3.1, “The “Save Capture File As” dialog box”). If you currently have a temporary capture file, the Save icon will be shown instead.

Toolbar Icon	Toolbar Item	Menu Item	Description
	Close	File → Close	This item closes the current capture. If you have not saved the capture, you will be asked to save it first.
	Reload	View → Reload	This item allows you to reload the current capture file.
	Print…	File → Print…	This item allows you to print all (or some of) the packets in the capture file. It pops up the Wireshark Print dialog box (which is discussed further in Section 5.8, “Printing packets”).
	Find Packet…	Edit → Find Packet…	This item brings up a dialog box that allows you to find a packet. There is further information on finding packets in Section 6.8, “Finding packets”.
	Go Back	Go → Go Back	This item jumps back in the packet history.
	Go Forward	Go → Go Forward	This item jumps forward in the packet history.
	Go to Packet…	Go → Go to Packet…	This item brings up a dialog box that allows you to specify a packet number to go to that packet.
	Go To First Packet	Go → First Packet	This item jumps to the first packet of the capture file.
	Go To Last Packet	Go → Last Packet	This item jumps to the last packet of the capture file.
	Colorize	View → Colorize	Colorize the packet list (or not).
	Auto Scroll in Live Capture	View → Auto Scroll in Live Capture	Auto scroll packet list while doing a live capture (or not).
	Zoom In	View → Zoom In	Zoom into the packet data (increase the font size).
	Zoom Out	View → Zoom Out	Zoom out of the packet data (decrease the font size).
	Normal Size	View → Normal Size	Set zoom level back to 100%.
	Resize Columns	View → Resize Columns	Resize columns, so the content fits into them.
	Capture Filters…	Capture → Capture Filters…	This item brings up a dialog box that allows you to create and edit capture filters. You can name filters, and you can save them for future use. More detail on this subject

Toolbar Icon	Toolbar Item	Menu Item	Description
			is provided in Section 6.6, “Defining and saving filters”.
	Display Filters…	Analyze → Display Filters…	This item brings up a dialog box that allows you to create and edit display filters. You can name filters, and you can save them for future use. More detail on this subject is provided in Section 6.6, “Defining and saving filters”.
	Coloring Rules…	View → Coloring Rules…	This item brings up a dialog box that allows you to color packets in the packet list pane according to filter expressions you choose. It can be very useful for spotting certain types of packets. More detail on this subject is provided in Section 10.3, “Packet colorization”.
	Preferences…	Edit → Preferences	This item brings up a dialog box that allows you to set preferences for many parameters that control Wireshark. You can also save your preferences so Wireshark will use them the next time you start it. More detail is provided in Section 10.5, “Preferences”
	Help	Help → Contents	This item brings up help dialog box.

3.17. The “Filter” toolbar

The filter toolbar lets you quickly edit and apply display filters. More information on display filters is available in Section 6.3, “Filtering packets while viewing”.

Figure 3.15. The “Filter” toolbar

Table 3.14. Filter toolbar items

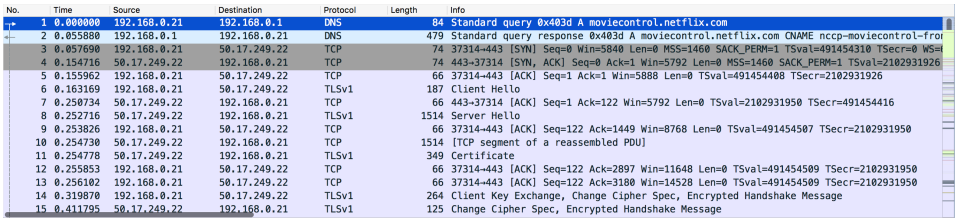
Toolbar Icon	Toolbar Item	Description
	Filter:	Brings up the filter construction dialog, described in Figure 6.8, “The “Capture Filters” and “Display Filters” dialog boxes”.
	Filter input	The area to enter or edit a display filter string, see Section 6.4, “Building display filter expressions”. A syntax check of your filter string is done while you are typing. The background will turn red if you enter an incomplete or invalid string, and will become green when you enter a valid string. You can click on the pull down arrow to select a previously-entered filter string from a list. The entries

Toolbar Icon	Toolbar Item	Description
		in the pull down list will remain available even after a program restart. After you've changed something in this field, don't forget to press the Apply button (or the Enter/Return key), to apply this filter string to the display. This field is also where the current filter in effect is displayed.
	Expression…	The middle button labeled "Add Expression…" opens a dialog box that lets you edit a display filter from a list of protocol fields, described in Section 6.5, "The "Filter Expression" dialog box"
	Clear	Reset the current display filter and clears the edit area.
	Apply	Apply the current value in the edit area as the new display filter. Applying a display filter on large capture files might take quite a long time.

3.18. The "Packet List" pane

The packet list pane displays all the packets in the current capture file.

Figure 3.16. The "Packet List" pane



Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes.

While dissecting a packet, Wireshark will place information from the protocol dissectors into the columns. As higher level protocols might overwrite information from lower levels, you will typically see the information from the highest possible level only.

For example, let's look at a packet containing TCP inside IP inside an Ethernet packet. The Ethernet dissector will write its data (such as the Ethernet addresses), the IP dissector will overwrite this by its own (such as the IP addresses), the TCP dissector will overwrite the IP information, and so on.

There are a lot of different columns available. Which columns are displayed can be selected by preference settings, see Section 10.5, "Preferences".

The default columns will show:

- No. The number of the packet in the capture file. This number won't change, even if a display filter is used.
- Time The timestamp of the packet. The presentation format of this timestamp can be changed, see Section 6.12, "Time display formats and time references".
- Source The address where this packet is coming from.
- Destination The address where this packet is going to.
- Protocol The protocol name in a short (perhaps abbreviated) version.
- Length The length of each packet.
- Info Additional information about the packet content.

The first column shows how each packet is related to the selected packet. For example, in the image above the first packet is selected, which is a DNS request. Wireshark shows a rightward arrow for the request itself, followed by a leftward arrow for the response in packet 2. Why is there a dashed line? There are more DNS packets further down that use the same port numbers. Wireshark treats them as belonging to the same conversation and draws a line connecting them.

Table 3.15. Related packet symbols

	First packet in a conversation.
	Part of the selected conversation.
	Not part of the selected conversation.
	Last packet in a conversation.
	Request.
	Response.
	The selected packet acknowledges this packet.
	The selected packet is a duplicate acknowledgement of this packet.
	The selected packet is related to this packet in some other way, e.g. as part of reassembly.

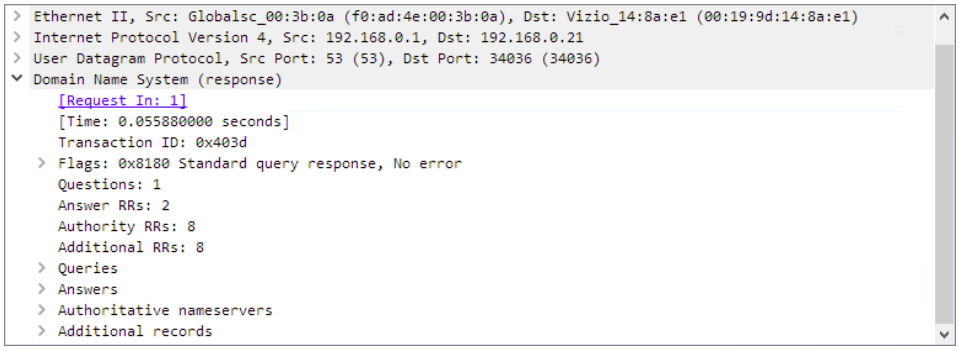
The packet list has an *Intelligent Scrollbar* which shows a miniature map of nearby packets. Each raster line of the scrollbar corresponds to a single packet, so the number of packets shown in the map depends on your physical display and the height of the packet list. A tall packet list on a high-resolution ("Retina") display will show you quite a few packets. In the image above the scrollbar shows the status of more than 500 packets along with the 15 shown in the packet list itself.

Right clicking will show a context menu, described in Figure 6.4, "Pop-up menu of the "Packet List" pane".

3.19. The “Packet Details” pane

The packet details pane shows the current packet (selected in the “Packet List” pane) in a more detailed form.

Figure 3.17. The “Packet Details” pane



This pane shows the protocols and protocol fields of the packet selected in the “Packet List” pane. The protocols and fields of the packet shown in a tree which can be expanded and collapsed.

There is a context menu (right mouse click) available. See details in Figure 6.5, “Pop-up menu of the “Packet Details” pane”.

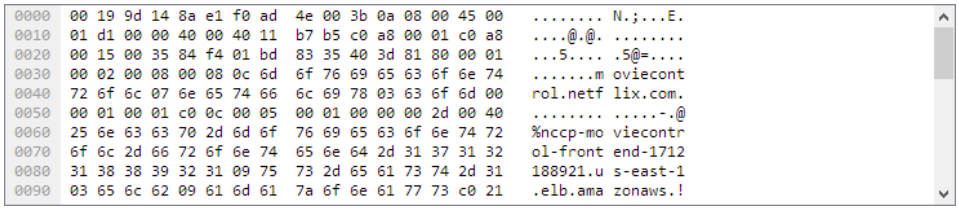
Some protocol fields have special meanings.

- **Generated fields.** Wireshark itself will generate additional protocol information which isn’t present in the captured data. This information is enclosed in square brackets (‘[’ and ‘]’). Generated information includes response times, TCP analysis, GeoIP information, and checksum validation.
- **Links.** If Wireshark detects a relationship to another packet in the capture file it will generate a link to that packet. Links are underlined and displayed in blue. If you double-clicked on a link Wireshark will jump to the corresponding packet.

3.20. The “Packet Bytes” pane

The packet bytes pane shows the data of the current packet (selected in the “Packet List” pane) in a hexdump style.

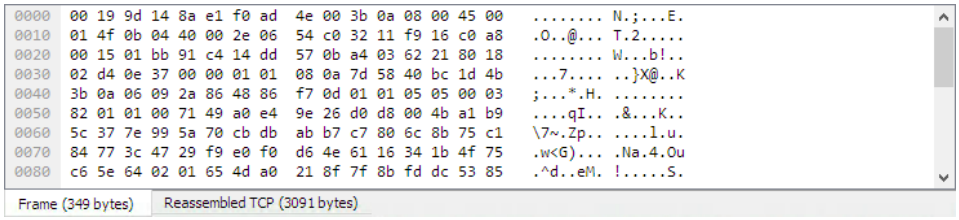
Figure 3.18. The “Packet Bytes” pane



The “Packet Bytes” pane shows a canonical hex dump of the packet data. Each line contains the data offset, sixteen hexadecimal bytes, and sixteen ASCII bytes. Non-printalbe bytes are replaced with a period (‘.’).

Depending on the packet data, sometimes more than one page is available, e.g. when Wireshark has reassembled some packets into a single chunk of data. (See Section 7.7, “Packet Reassembly” for details). In this case you can see each data source by clicking its corresponding tab at the bottom of the pane.

Figure 3.19. The “Packet Bytes” pane with tabs



Additional pages typically contain data reassembled from multiple packets or decrypted data.

The context menu (right mouse click) of the tab labels will show a list of all available pages. This can be helpful if the size in the pane is too small for all the tab labels.

3.21. The Statusbar

The statusbar displays informational messages.

In general, the left side will show context related information, the middle part will show information about the current capture file, and the right side will show the selected configuration profile. Drag the handles between the text areas to change the size.

Figure 3.20. The initial Statusbar

This statusbar is shown while no capture file is loaded, e.g. when Wireshark is started.

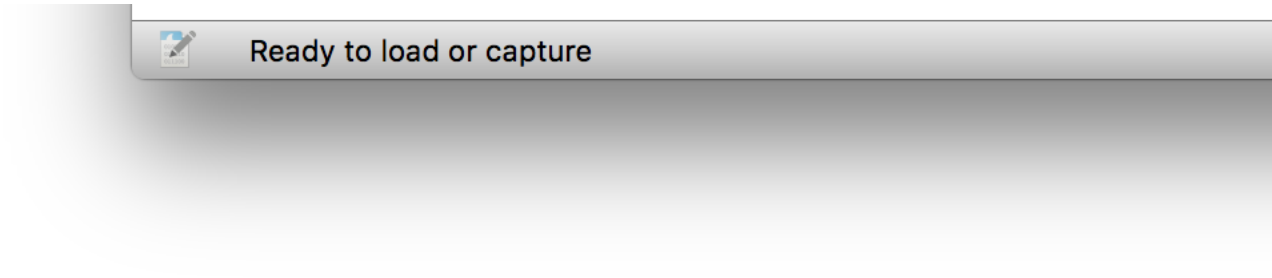
Figure 3.21. The Statusbar with a loaded capture file

- **The colorized bullet** on the left shows the highest expert info level found in the currently loaded capture file. Hovering the mouse over this icon will show a textual description of the expert info level, and clicking the icon will bring up the Expert Infos dialog box. For a detailed description of expert info, see Section 7.4, “Expert Information”.
- **The left side** shows information about the capture file, its name, its size and the elapsed time while it was being captured. Hovering over a file name will show its full path and size.
- **The middle part** shows the current number of packets in the capture file. The following values are displayed:
  - *Packets:* The number of captured packets.
  - *Displayed:* The number of packets currently being displayed.
  - *Marked:* The number of marked packets (only displayed if packets are marked).
  - *Dropped:* The number of dropped packets (only displayed if Wireshark was unable to capture all packets).
  - *Ignored:* The number of ignored packets (only displayed if packets are ignored).

- *Load time:* The time it took to load the capture (wall clock time).

- **The right side** shows the selected configuration profile. Clicking in this part of the statusbar will bring up a menu with all available configuration profiles, and selecting from this list will change the configuration profile.

Figure 3.22. The Statusbar with a configuration profile menu



For a detailed description of configuration profiles, see Section 10.6, “Configuration Profiles”.

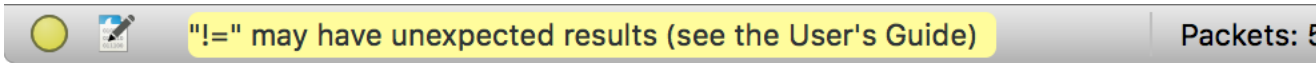
Figure 3.23. The Statusbar with a selected protocol field

This is displayed if you have selected a protocol field from the “Packet Details” pane.

Tip

The value between the parentheses (in this example ‘ipv6.src’) can be used as a display filter, representing the selected protocol field.

Figure 3.24. The Statusbar with a display filter message



This is displayed if you are trying to use a display filter which may have unexpected results. For a detailed description, see Section 6.4.6, “A Common Mistake”.

Chapter 4. Capturing Live Network Data

4.1. Introduction

Capturing live network data is one of the major features of Wireshark.

The Wireshark capture engine provides the following features:

- Capture from different kinds of network hardware such as Ethernet or 802.11.
- Stop the capture on different triggers such as the amount of captured data, elapsed time, or the number of packets.
- Simultaneously show decoded packets while Wireshark is capturing.
- Filter packets, reducing the amount of data to be captured. See Section 4.13, “Filtering while capturing”.
- Save packets in multiple files while doing a long term capture, optionally rotating through a fixed number of files (a “ringbuffer”). See Section 4.11, “Capture files and file modes”.
- Simultaneously capture from multiple network interfaces.

The capture engine still lacks the following features:

- Stop capturing (or perform some other action) depending on the captured data.

4.2. Prerequisites

Setting up Wireshark to capture packets for the first time can be tricky. A comprehensive guide “How To setup a Capture” is available at https://wiki.wireshark.org/CaptureSetup.

Here are some common pitfalls:

- You may need special privileges to start a live capture.
- You need to choose the right network interface to capture packet data from.
- You need to capture at the right place in the network to see the traffic you want to see.

If you have any problems setting up your capture environment you should have a look at the guide mentioned above.

4.3. Start Capturing

The following methods can be used to start capturing packets with Wireshark:

- You can double-click on an interface in the main window.
- You can get an overview of the available interfaces using the “Capture Interfaces” dialog box (Capture → Options…). See Figure 4.1, “The “Capture Interfaces” dialog box on Microsoft Windows” or

Figure 4.2, “The “Capture Interfaces” dialog box on Unix/Linux” for more information. You can start a capture from this dialog box using the Start button.

- You can immediately start a capture using your current settings by selecting Capture → Start or by cliking the first toolbar button.
- If you already know the name of the capture interface you can start Wireshark from the command line:

```
$ wireshark -i eth0 -k
```

This will start Wireshark capturing on interface eth0. More details can be found at Section 10.2, “Start Wireshark from the command line”.

4.4. The “Capture Interfaces” dialog box

When you select Capture → Options… from the main menu Wireshark pops up the “Capture Interfaces” dialog box as shown in Figure 4.1, “The “Capture Interfaces” dialog box on Microsoft Windows” or Figure 4.2, “The “Capture Interfaces” dialog box on Unix/Linux”.

Both you and your OS can hide interfaces

This dialog box will only show the local interfaces Wireshark can access. It will also hide interfaces marked as hidden in Section 10.5.1, “Interface Options”. As Wireshark might not be able to detect all local interfaces and it cannot detect the remote interfaces available there could be more capture interfaces available than listed.

It is possible to select more than one interface and capture from them simultaneously.

Figure 4.1. The “Capture Interfaces” dialog box on Microsoft Windows

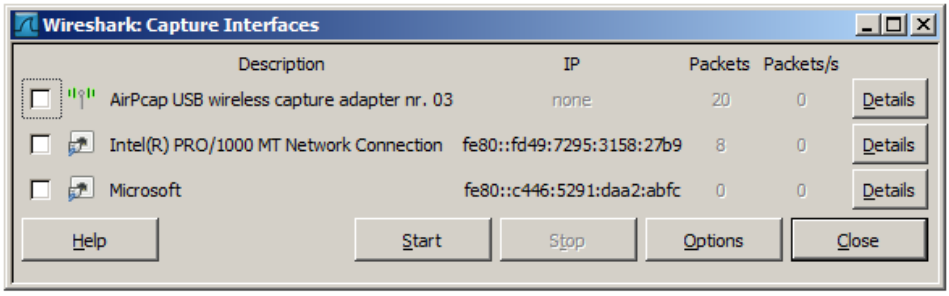
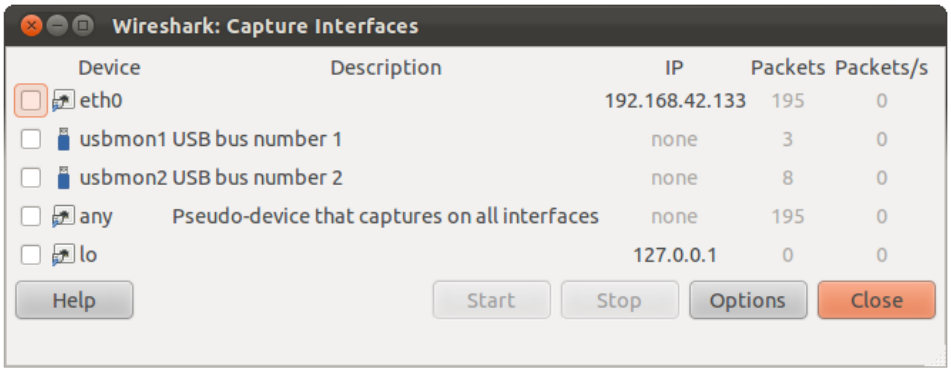


Figure 4.2. The “Capture Interfaces” dialog box on Unix/Linux



Device (Unix/Linux only)
The interface device name.

Description
The interface description provided by the operating system, or the user defined comment added in Section 10.5.1, “Interface Options”.

IP
The first IP address Wireshark could find for this interface. You can click on the address to cycle through other addresses assigned to it, if available. If no address could be found “none” will be displayed.

Packets
The number of packets captured from this interface, since this dialog was opened. Will be greyed out, if no packet was captured in the last second.

Packets/s
Number of packets captured in the last second. Will be greyed out, if no packet was captured in the last second.

Stop
Stop a currently running capture.

Start
Start a capture on all selected interfaces immediately, using the settings from the last capture or the default settings, if no options have been set.

Options
Open the Capture Options dialog with the marked interfaces selected. See Section 4.5, “The “Capture Options” dialog box”.

Details (Microsoft Windows only)
Open a dialog with detailed information about the interface. See Section 4.10, “The “Interface Details” dialog box”.

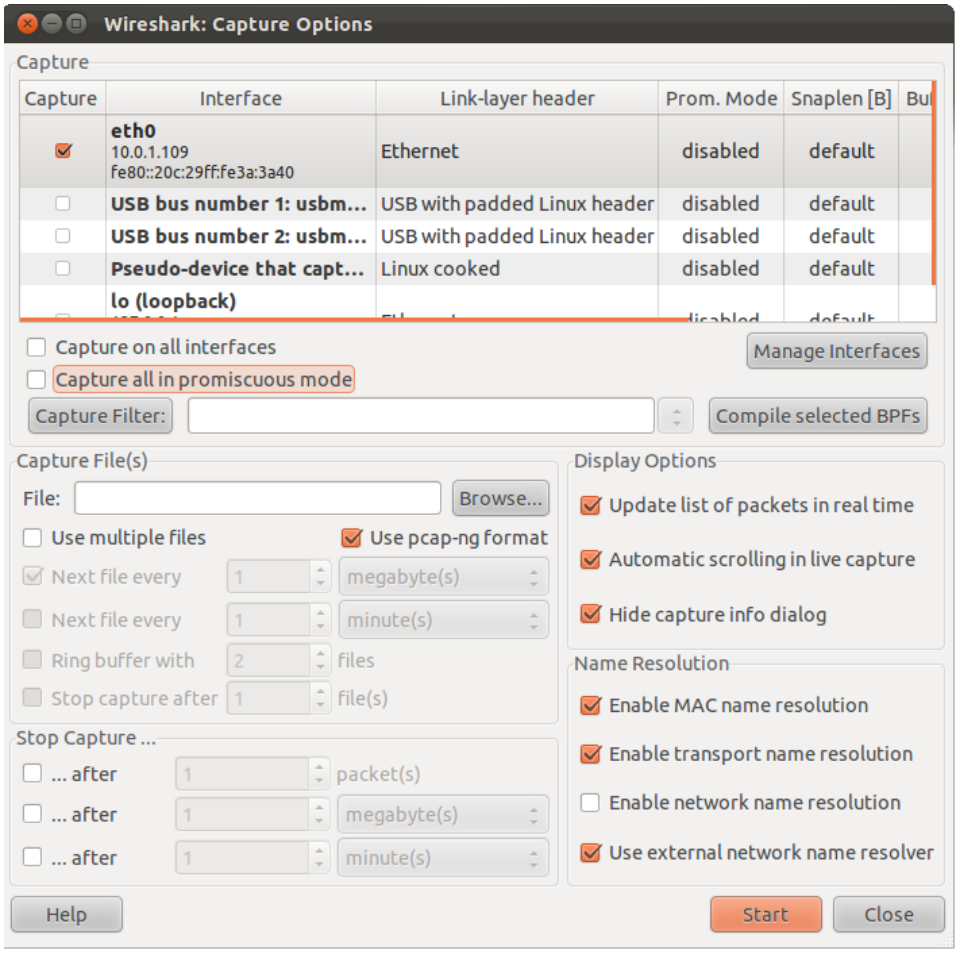
Help
Show this help page.

Close
Close this dialog box.

4.5. The “Capture Options” dialog box

When you select Capture → Options… (or use the corresponding item in the main toolbar), Wireshark pops up the “Capture Options” dialog box as shown in Figure 4.3, “The “Capture Options” dialog box”.

Figure 4.3. The “Capture Options” dialog box



Tip

If you are unsure which options to choose in this dialog box just try keeping the defaults as this should work well in many cases.

4.5.1. Capture frame

The table shows the settings for all available interfaces:

- The name of the interface and its IP addresses. If no address could be resolved from the system, “none” will be shown.

Note

Loopback interfaces are not available on Windows platforms.

- The link-layer header type.
- The information whether promicuous mode is enabled or disabled.
- The maximum amount of data that will be captured for each packet. The default value is set to the 65535 bytes.

- The size of the kernel buffer that is reserved to keep the captured packets.
- The information whether packets will be captured in monitor mode (Unix/Linux only).
- The chosen capture filter.

By marking the checkboxes in the first column the interfaces are selected to be captured from. By double-clicking on an interface the "Edit Interface Settings" dialog box as shown in Figure 4.4, "The "Edit Interface Settings" dialog box" will be opened.

Capture on all interfaces
As Wireshark can capture on multiple interfaces it is possible to choose to capture on all available interfaces.

Capture all packets in promiscuous mode
This checkbox allows you to specify that Wireshark should put all interfaces in promiscuous mode when capturing.

Capture Filter
This field allows you to specify a capture filter for all interfaces that are currently selected. Once a filter has been entered in this field, the newly selected interfaces will inherit the filter. Capture filters are discussed in more details in Section 4.13, "Filtering while capturing". It defaults to empty, or no filter.

You can also click on the Capture Filter button and Wireshark will bring up the Capture Filters dialog box and allow you to create and/or select a filter. Please see Section 6.6, "Defining and saving filters"

Compile selected BPFs
This button allows you to compile the capture filter into BPF code and pop up a window showing you the resulting pseudo code. This can help in understanding the working of the capture filter you created. The Compile Selected BPFs button leads you to Figure 4.5, "The "Compile Results" dialog box".

Tip

Linux power user tip

The execution of BPFs can be sped up on Linux by turning on BPF JIT by executing

```
$ echo 1 >/proc/sys/net/core/bpf_jit_enable
```

if it is not enabled already. To make the change persistent you can use sysfsutils.

Manage Interfaces
The Manage Interfaces button opens the Figure 4.6, "The "Add New Interfaces" dialog box" where pipes can be defined, local interfaces scanned or hidden, or remote interfaces added (Windows only).

4.5.2. Capture File(s) frame

An explanation about capture file usage can be found in Section 4.11, "Capture files and file modes".

File
This field allows you to specify the file name that will be used for the capture file. This field is left blank by default. If the field is left blank, the capture data will be stored in a temporary file. See Section 4.11, "Capture files and file modes" for details.

You can also click on the button to the right of this field to browse through the filesystem.

Use multiple files
Instead of using a single file Wireshark will automatically switch to a new one if a specific trigger condition is reached.

Use pcap-ng format
: This checkbox allows you to specify that Wireshark saves the captured packets in pcap-ng format. This next generation capture file format is currently in development. If more than one interface is chosen for capturing, this checkbox is set by default. See https://wiki.wireshark.org/Development/PcapNg for more details on pcap-ng.

Next file every n megabyte(s)
: Multiple files only. Switch to the next file after the given number of byte(s)/kilobyte(s)/megabyte(s)/gigabyte(s) have been captured.

Next file every n minute(s)
: Multiple files only: Switch to the next file after the given number of second(s)/minutes(s)/hours(s)/days(s) have elapsed.

Ring buffer with n files
: Multiple files only: Form a ring buffer of the capture files with the given number of files.

Stop capture after n file(s)
: Multiple files only: Stop capturing after switching to the next file the given number of times.

4.5.3. Stop Capture… frame

… after n packet(s)
: Stop capturing after the given number of packets have been captured.

… after n megabytes(s)
: Stop capturing after the given number of byte(s)/kilobyte(s)/megabyte(s)/gigabyte(s) have been captured. This option is greyed out if “Use multiple files” is selected.

… after n minute(s)
: Stop capturing after the given number of second(s)/minutes(s)/hours(s)/days(s) have elapsed.

4.5.4. Display Options frame

Update list of packets in real time
: This option allows you to specify that Wireshark should update the packet list pane in real time. If you do not specify this, Wireshark does not display any packets until you stop the capture. When you check this, Wireshark captures in a separate process and feeds the captures to the display process.

Automatic scrolling in live capture
: This option allows you to specify that Wireshark should scroll the packet list pane as new packets come in, so you are always looking at the last packet. If you do not specify this Wireshark simply adds new packets onto the end of the list but does not scroll the packet list pane. This option is greyed out if “Update list of packets in real time” is disabled.

4.5.5. Name Resolution frame

Enable MAC name resolution
: This option allows you to control whether or not Wireshark translates MAC addresses into names. See Section 7.8, “Name Resolution”.

Enable network name resolution
: This option allows you to control whether or not Wireshark translates network addresses into names. See Section 7.8, “Name Resolution”.

Enable transport name resolution
This option allows you to control whether or not Wireshark translates transport addresses into protocols. See Section 7.8, “Name Resolution”.

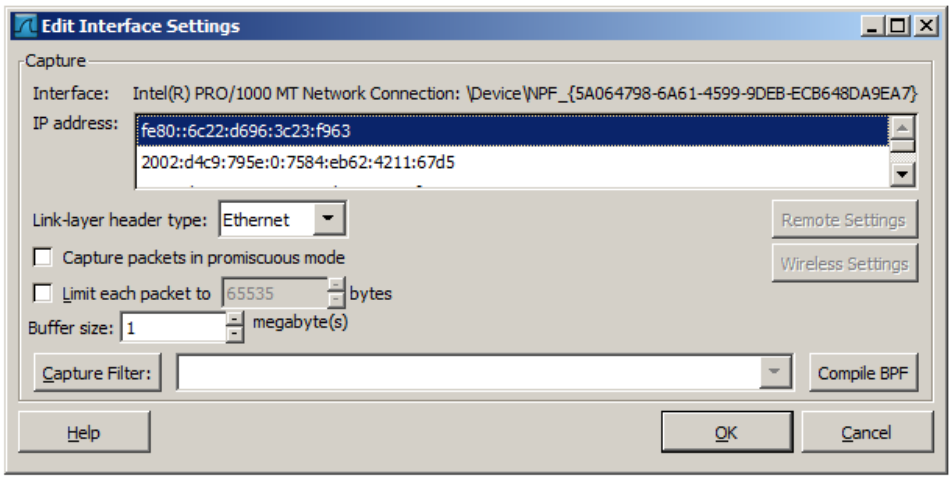
4.5.6. Buttons

Once you have set the values you desire and have selected the options you need, simply click on Start to commence the capture or Cancel to cancel the capture.

4.6. The “Edit Interface Settings” dialog box

If you double-click on an interface in Figure 4.3, “The “Capture Options” dialog box” the following dialog box pops up.

Figure 4.4. The “Edit Interface Settings” dialog box



You can set the following fields in this dialog box:

IP address
The IP address(es) of the selected interface. If no address could be resolved from the system “none” will be shown.

Link-layer header type
Unless you are in the rare situation that requires this keep the default setting. For a detailed description. See Section 4.12, “Link-layer header type”

Wireless settings (Windows only)
Here you can set the settings for wireless capture using the AirPCap adapter. For a detailed description see the AirPCap Users Guide.

Remote settings (Windows only)
Here you can set the settings for remote capture. For a detailed description see Section 4.9, “The “Remote Capture Interfaces” dialog box”

Capture packets in promiscuous mode
This checkbox allows you to specify that Wireshark should put the interface in promiscuous mode when capturing. If you do not specify this Wireshark will only capture the packets going to or from your computer (not all packets on your LAN segment).

Note

If some other process has put the interface in promiscuous mode you may be capturing in promiscuous mode even if you turn off this option.

Even in promiscuous mode you still won't necessarily see all packets on your LAN segment. See the Wireshark FAQ for more information.

Limit each packet to n bytes
This field allows you to specify the maximum amount of data that will be captured for each packet, and is sometimes referred to as the *snaplen*. If disabled the value is set to the maximum 65535 which will be sufficient for most protocols. Some rules of thumb:

- If you are unsure just keep the default value.
- If you don't need or don't want all of the data in a packet - for example, if you only need the link-layer, IP, and TCP headers - you might want to choose a small snapshot length, as less CPU time is required for copying packets, less buffer space is required for packets, and thus perhaps fewer packets will be dropped if traffic is very heavy.
- If you don't capture all of the data in a packet you might find that the packet data you want is in the part that's dropped or that reassembly isn't possible as the data required for reassembly is missing.

Buffer size: n megabyte(s)
Enter the buffer size to be used while capturing. This is the size of the kernel buffer which will keep the captured packets, until they are written to disk. If you encounter packet drops, try increasing this value.

Capture packets in monitor mode (Unix/Linux only)
This checkbox allows you to setup the Wireless interface to capture all traffic it can receive, not just the traffic on the BSS to which it is associated, which can happen even when you set promiscuous mode. Also it might be necessary to turn this option on in order to see IEEE 802.11 headers and/or radio information from the captured frames.

Note

In monitor mode the adapter might disassociate itself from the network it was associated to.

Capture Filter
This field allows you to specify a capture filter. Capture filters are discussed in more details in Section 4.13, "Filtering while capturing". It defaults to empty, or no filter.

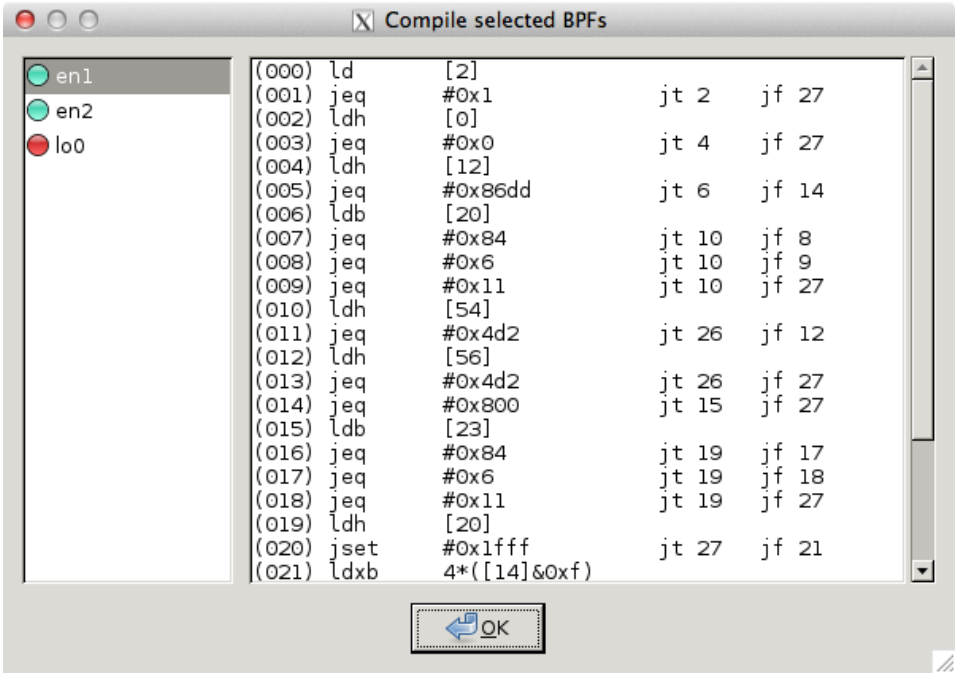
You can also click on the Capture Filter button and Wireshark will bring up the "Capture Filters" dialog box and allow you to create and/or select a filter. Please see Section 6.6, "Defining and saving filters"

Compile BPF
This button allows you to compile the capture filter into BPF code and pop up a window showing you the resulting pseudo code. This can help in understanding the working of the capture filter you created.

4.7. The "Compile Results" dialog box

This figure shows the compile results of the selected interfaces.

Figure 4.5. The “Compile Results” dialog box

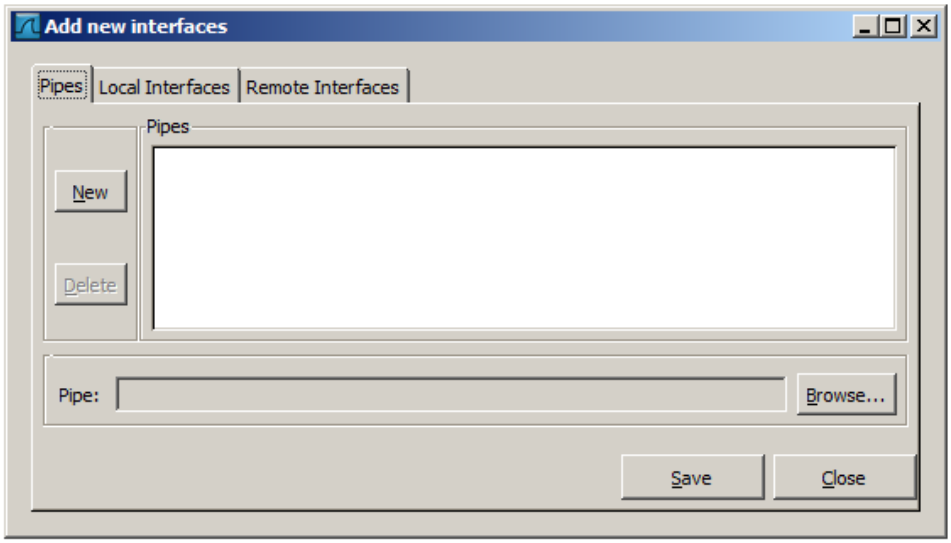


In the left window the interface names are listed. The results of an individual interface are shown in the right window when it is selected.

4.8. The “Add New Interfaces” dialog box

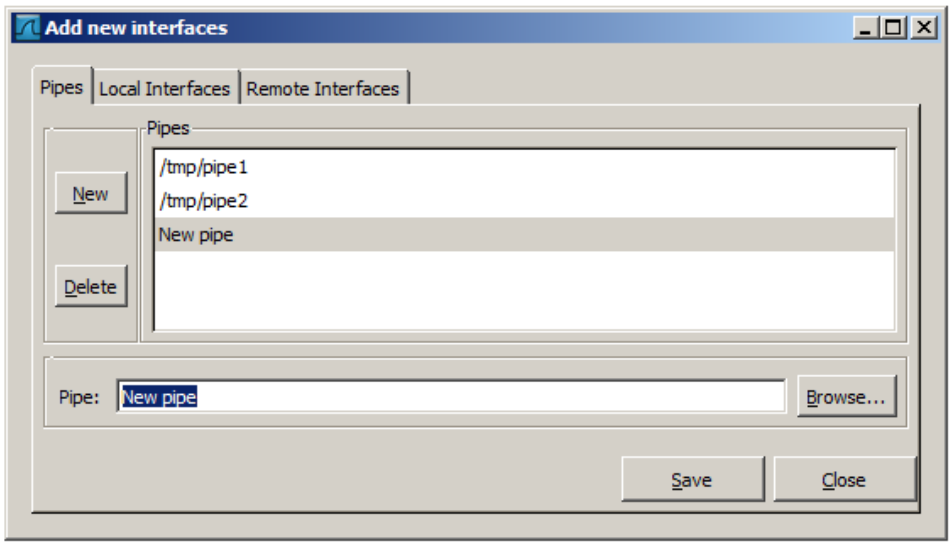
As a central point to manage interfaces this dialog box consists of three tabs to add or remove interfaces.

Figure 4.6. The “Add New Interfaces” dialog box



4.8.1. Add or remove pipes

Figure 4.7. The “Add New Interfaces - Pipes” dialog box

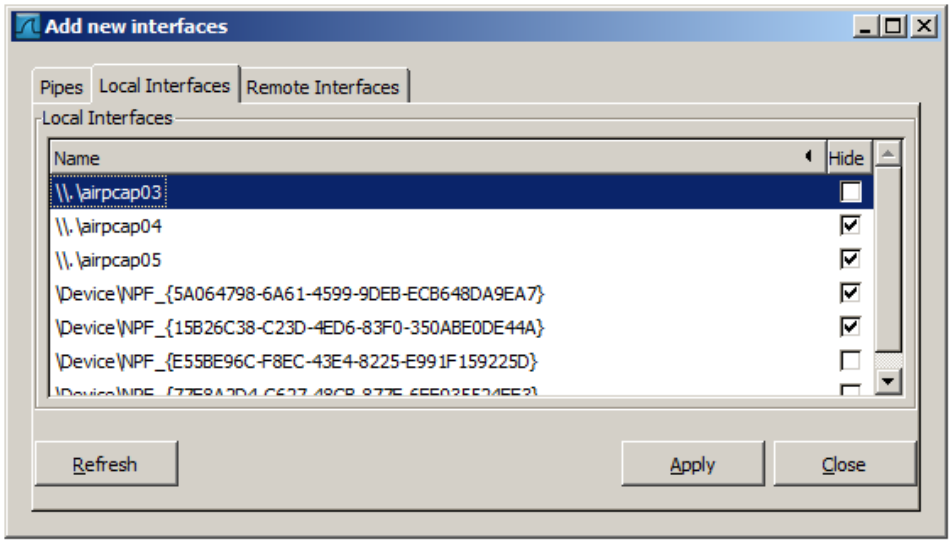


To successfully add a pipe, this pipe must have already been created. Click the New button and type the name of the pipe including its path. Alternatively, the Browse button can be used to locate the pipe. With the Save button the pipe is added to the list of available interfaces. Afterwards, other pipes can be added.

To remove a pipe from the list of interfaces it first has to be selected. Then click the Delete button.

4.8.2. Add or hide local interfaces

Figure 4.8. The “Add New Interfaces - Local Interfaces” dialog box



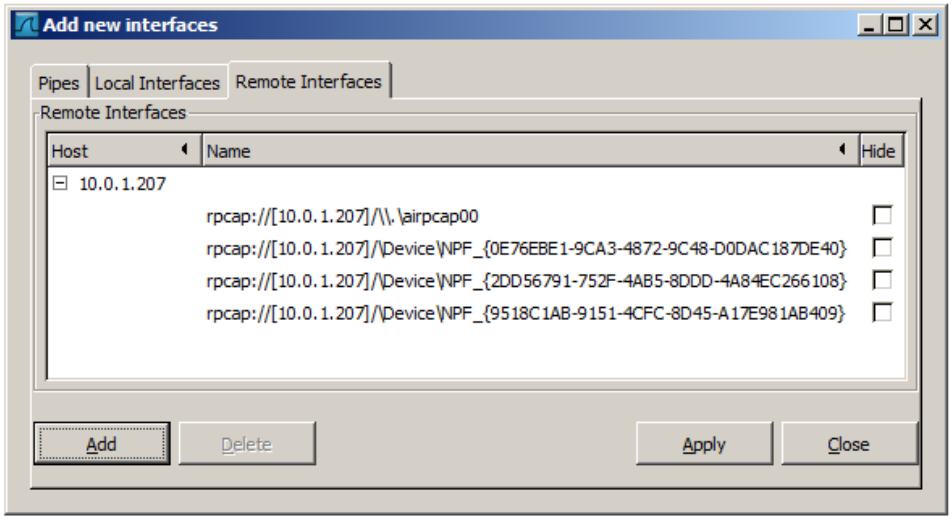
The tab “Local Interfaces” contains a list of available local interfaces, including the hidden ones, which are not shown in the other lists.

If a new local interface is added, for example, a wireless interface has been activated, it is not automatically added to the list to prevent the constant scanning for a change in the list of available interfaces. To renew the list a rescan can be done.

One way to hide an interface is to change the preferences. If the “Hide” checkbox is activated and the Apply button clicked, the interface will not be seen in the lists of the “Capture Interfaces” dialog box any more. The changes are also saved in the `preferences` file.

4.8.3. Add or hide remote interfaces

Figure 4.9. The “Add New Interfaces - Remote Interfaces” dialog box



In this tab interfaces on remote hosts can be added. One or more of these interfaces can be hidden. In contrast to the local interfaces they are not saved in the `preferences` file.

To remove a host including all its interfaces from the list, it has to be selected. Then click the Delete button.

For a detailed description see Section 4.9, “The “Remote Capture Interfaces” dialog box”

4.9. The “Remote Capture Interfaces” dialog box

Besides doing capture on local interfaces Wireshark is capable of reaching out across the network to a so called capture daemon or service processes to receive captured data from.

Microsoft Windows only

This dialog and capability is only available on Microsoft Windows. On Linux/Unix you can achieve the same effect (securely) through an SSH tunnel.

The Remote Packet Capture Protocol service must first be running on the target platform before Wireshark can connect to it. The easiest way is to install WinPcap from https://www.winpcap.org/install/ on the target. Once installation is completed go to the Services control panel, find the Remote Packet Capture Protocol service and start it.

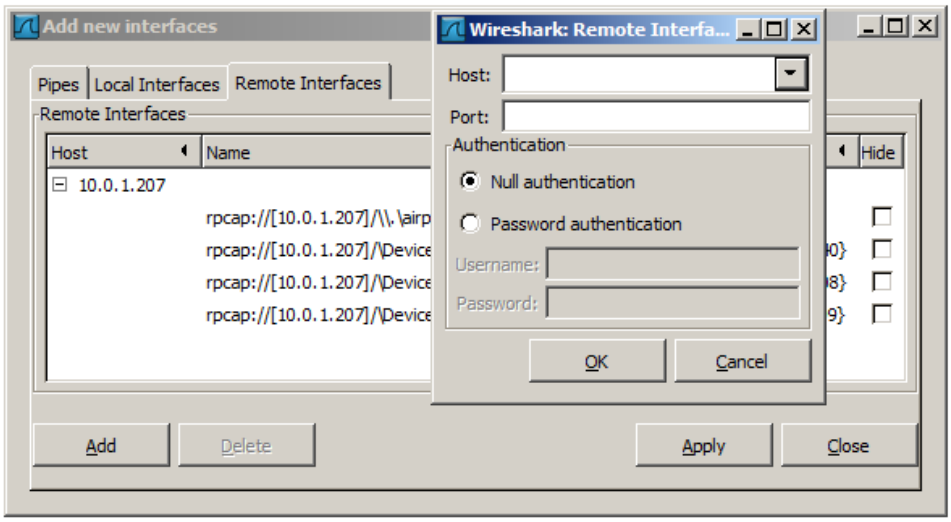
Note

Make sure you have outside access to port 2002 on the target platform. This is the port where the Remote Packet Capture Protocol service can be reached by default.

To access the Remote Capture Interfaces dialog use the “Add New Interfaces - Remote” dialog. See Figure 4.9, “The “Add New Interfaces - Remote Interfaces” dialog box” and select Add.

4.9.1. Remote Capture Interfaces

Figure 4.10. The “Remote Capture Interfaces” dialog box



You have to set the following parameters in this dialog:

Host
: Enter the IP address or host name of the target platform where the Remote Packet Capture Protocol service is listening. The drop down list contains the hosts that have previously been successfully contacted. The list can be emptied by choosing “Clear list” from the drop down list.

Port
: Set the port number where the Remote Packet Capture Protocol service is listening on. Leave open to use the default port (2002).

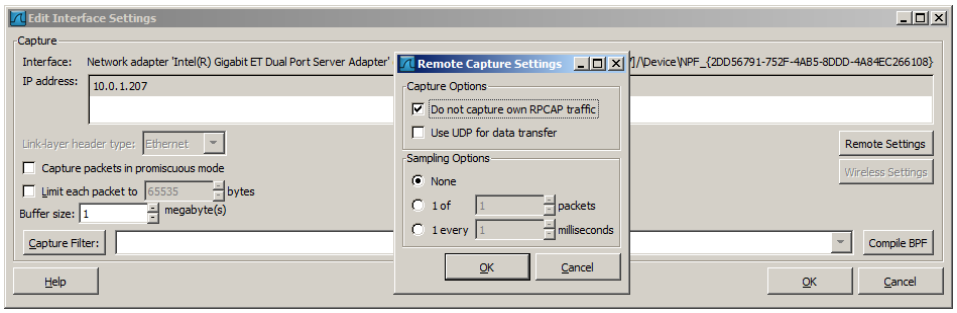
Null authentication
: Select this if you don’t need authentication to take place for a remote capture to be started. This depends on the target platform. Configuring the target platform like this makes it insecure.

Password authentication
: This is the normal way of connecting to a target platform. Set the credentials needed to connect to the Remote Packet Capture Protocol service.

4.9.2. Remote Capture Settings

The remote capture can be further fine tuned to match your situation. The Remote Settings button in Figure 4.4, “The “Edit Interface Settings” dialog box” gives you this option. It pops up the dialog shown in Figure 4.11, “The “Remote Capture Settings” dialog box”.

Figure 4.11. The “Remote Capture Settings” dialog box



You can set the following parameters in this dialog:

Do not capture own RPCAP traffic
: This option sets a capture filter so that the traffic flowing back from the Remote Packet Capture Protocol service to Wireshark isn’t captured as well and also send back. The recursion in this saturates the link with duplicate traffic.

  You only should switch this off when capturing on an interface other than the interface connecting back to Wireshark.

Use UDP for data transfer
: Remote capture control and data flows over a TCP connection. This option allows you to choose an UDP stream for data transfer.

Sampling option None
: This option instructs the Remote Packet Capture Protocol service to send back all captured packets which have passed the capture filter. This is usually not a problem on a remote capture session with sufficient bandwidth.

Sampling option 1 of x packets
: This option limits the Remote Packet Capture Protocol service to send only a sub sampling of the captured data, in terms of number of packets. This allows capture over a narrow band remote capture session of a higher bandwidth interface.

Sampling option 1 every x milliseconds
: This option limits the Remote Packet Capture Protocol service to send only a sub sampling of the captured data in terms of time. This allows capture over a narrow band capture session of a higher bandwidth interface.

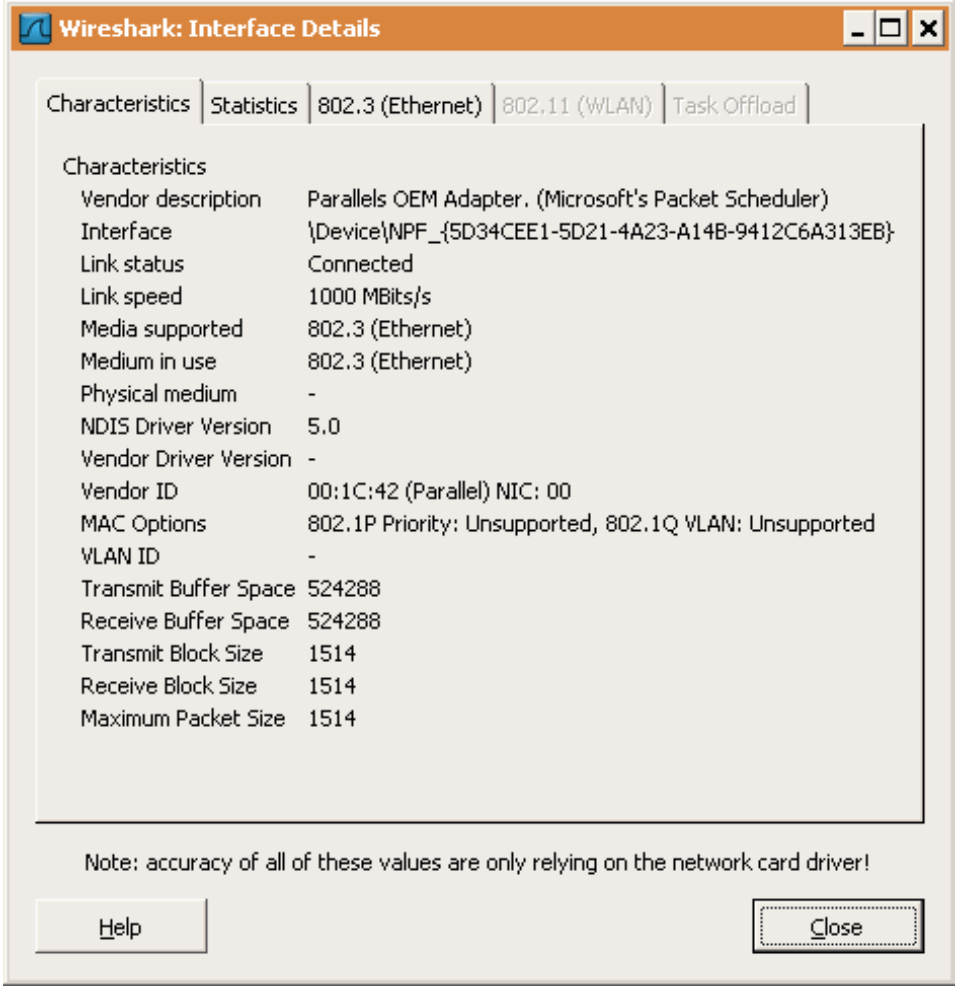
4.10. The “Interface Details” dialog box

When you select Details from the Capture Interface menu, Wireshark pops up the “Interface Details” dialog box as shown in Figure 4.12, “The “Interface Details” dialog box”. This dialog shows various characteristics and statistics for the selected interface.

Microsoft Windows only

This dialog is only available on Microsoft Windows

Figure 4.12. The “Interface Details” dialog box

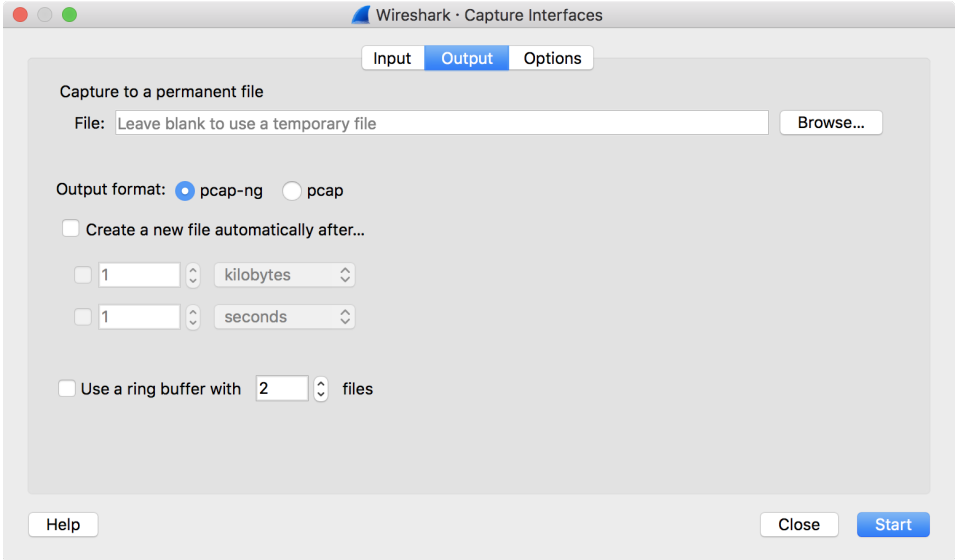


4.11. Capture files and file modes

While capturing the underlying libpcap capturing engine will grab the packets from the network card and keep the packet data in a (relatively) small kernel buffer. This data is read by Wireshark and saved into a capture file.

By default Wireshark saves packets to a temporary file. You can also tell Wireshark to save to a specific (“permanent”) file and switch to a different file after a given time has elapsed or a given number of packets have been captured. These options are controlled in the “Output” tab in the “Capture Options” dialog.

Figure 4.13. Capture output options



Tip

Working with large files (several hundred MB) can be quite slow. If you plan to do a long term capture or capturing from a high traffic network, think about using one of the "Multiple files" options. This will spread the captured packets over several smaller files which can be much more pleasant to work with.

Using Multiple files may cut context related information. Wireshark keeps context information of the loaded packet data, so it can report context related problems (like a stream error) and keeps information about context related protocols (e.g. where data is exchanged at the establishing phase and only referred to in later packets). As it keeps this information only for the loaded file, using one of the multiple file modes may cut these contexts. If the establishing phase is saved in one file and the things you would like to see is in another, you might not see some of the valuable context related information.

Information about the folders used for capture files can be found in Appendix B, *Files and Folders*.

Table 4.1. Capture file mode selected by capture options

File Name	"Create a new file…"	"Use a ring buffer…"	Mode	Resulting filename(s) used
-	-	-	*Single temporary file*	wiresharkXXXXXX (where XXXXXX is a unique number)
foo.cap	-	-	*Single named file*	foo.cap
foo.cap	x	-	*Multiple files, continuous*	foo_00001_20100205110102.cap, foo_00002_20100205110318.cap, …
foo.cap	x	x	*Multiple files, ring buffer*	foo_00001_20100205110102.cap, foo_00002_20100205110318.cap, …

Single temporary file
: A temporary file will be created and used (this is the default). After capturing is stopped this file can be saved later under a user specified name.

Single named file
: A single capture file will be used. If you want to place the new capture file in a specific folder choose this mode.

Multiple files, continuous
: Like the “Single named file” mode, but a new file is created and used after reaching one of the multiple file switch conditions (one of the “Next file every …” values).

Multiple files, ring buffer
: Much like “Multiple files continuous”, reaching one of the multiple files switch conditions (one of the “Next file every …” values) will switch to the next file. This will be a newly created file if value of “Ring buffer with n files” is not reached, otherwise it will replace the oldest of the formerly used files (thus forming a “ring”). This mode will limit the maximum disk usage, even for an unlimited amount of capture input data, only keeping the latest captured data.

4.12. Link-layer header type

In most cases you won’t have to modify link-layer header type. Some exceaptions are as follows:

If you are capturing on an Ethernet device you might be offered a choice of “Ethernet” or “DOCSIS”. If you are capturing traffic from a Cisco Cable Modem Termination System that is putting DOCSIS traffic onto the Ethernet to be captured, select “DOCSIS”, otherwise select “Ethernet”.

If you are capturing on an 802.11 device on some versions of BSD you might be offered a choice of “Ethernet” or “802.11”. “Ethernet” will cause the captured packets to have fake (“cooked”) Ethernet headers. “802.11” will cause them to have full IEEE 802.11 headers. Unless the capture needs to be read by an application that doesn’t support 802.11 headers you should select “802.11”.

If you are capturing on an Endace DAG card connected to a synchronous serial line you might be offered a choice of “PPP over serial” or “Cisco HDLC”. If the protocol on the serial line is PPP, select “PPP over serial” and if the protocol on the serial line is Cisco HDLC, select “Cisco HDLC”.

If you are capturing on an Endace DAG card connected to an ATM network you might be offered a choice of “RFC 1483 IP-over-ATM” or “Sun raw ATM”. If the only traffic being captured is RFC 1483 LLC-encapsulated IP, or if the capture needs to be read by an application that doesn’t support SunATM headers, select “RFC 1483 IP-over-ATM”, otherwise select “Sun raw ATM”.

4.13. Filtering while capturing

Wireshark uses the libpcap filter language for capture filters. A brief overview of the syntax follows. Complete documentation can be found in the pcap-filter man page. You can find a lot of Capture Filter examples at https://wiki.wireshark.org/CaptureFilters.

You enter the capture filter into the “Filter” field of the Wireshark “Capture Options” dialog box, as shown in Figure 4.3, “The “Capture Options” dialog box”.

A capture filter takes the form of a series of primitive expressions connected by conjunctions (*and/or*) and optionally preceded by *not*:

```
[not] primitive [and|or [not] primitive ...]
```

An example is shown in Example 4.1, “A capture filter for telnet that captures traffic to and from a particular host”.

Example 4.1. A capture filter for telnet that captures traffic to and from a particular host

A capture filter for telnet that captures traffic to and from a particular host

```
tcp port 23 and host 10.0.0.5
```

This example captures telnet traffic to and from the host 10.0.0.5, and shows how to use two primitives and the *and* conjunction. Another example is shown in Example 4.2, “Capturing all telnet traffic not from 10.0.0.5”, and shows how to capture all telnet traffic except that from 10.0.0.5.

Example 4.2. Capturing all telnet traffic not from 10.0.0.5

Capturing all telnet traffic not from 10.0.0.5

```
tcp port 23 and not src host 10.0.0.5
```

A primitive is simply one of the following: *[src|dst] host <host>*

This primitive allows you to filter on a host IP address or name. You can optionally precede the primitive with the keyword *src|dst* to specify that you are only interested in source or destination addresses. If these are not present, packets where the specified address appears as either the source or the destination address will be selected.

ether [src|dst] host <ehost>

This primitive allows you to filter on Ethernet host addresses. You can optionally include the keyword *src|dst* between the keywords *ether* and *host* to specify that you are only interested in source or destination addresses. If these are not present, packets where the specified address appears in either the source or destination address will be selected.

gateway host <host>

This primitive allows you to filter on packets that used *host* as a gateway. That is, where the Ethernet source or destination was *host* but neither the source nor destination IP address was *host*.

[src|dst] net <net> [{mask <mask>}|{len <len>}]

This primitive allows you to filter on network numbers. You can optionally precede this primitive with the keyword *src|dst* to specify that you are only interested in a source or destination network. If neither of these are present, packets will be selected that have the specified network in either the source or destination address. In addition, you can specify either the netmask or the CIDR prefix for the network if they are different from your own.

[tcp|udp] [src|dst] port <port>

This primitive allows you to filter on TCP and UDP port numbers. You can optionally precede this primitive with the keywords *src|dst* and *tcp|udp* which allow you to specify that you are only interested in source or destination ports and TCP or UDP packets respectively. The keywords *tcp|udp* must appear before *src|dst*.

If these are not specified, packets will be selected for both the TCP and UDP protocols and when the specified address appears in either the source or destination port field.

less|greater <length>

This primitive allows you to filter on packets whose length was less than or equal to the specified length, or greater than or equal to the specified length, respectively.

ip|ether proto <protocol>

This primitive allows you to filter on the specified protocol at either the Ethernet layer or the IP layer.

ether|ip broadcast|multicast
This primitive allows you to filter on either Ethernet or IP broadcasts or multicasts.

<expr> relop <expr>
This primitive allows you to create complex filter expressions that select bytes or ranges of bytes in packets. Please see the pcap-filter man page at http://www.tcpdump.org/manpages/pcap-filter.7.html for more details.

4.13.1. Automatic Remote Traffic Filtering

If Wireshark is running remotely (using e.g. SSH, an exported X11 window, a terminal server, …), the remote content has to be transported over the network, adding a lot of (usually unimportant) packets to the actually interesting traffic.

To avoid this, Wireshark tries to figure out if it's remotely connected (by looking at some specific environment variables) and automatically creates a capture filter that matches aspects of the connection.

The following environment variables are analyzed:

SSH_CONNECTION (ssh)
<remote IP> <remote port> <local IP> <local port>

SSH_CLIENT (ssh)
<remote IP> <remote port> <local port>

REMOTEHOST (tcsh, others?)
<remote name>

DISPLAY (x11)
[remote name]:<display num>

SESSIONNAME (terminal server)
<remote name>

On Windows it asks the operating system if it's running in a Remote Desktop Services environment.

4.13.2. Stop the running capture

A running capture session will be stopped in one of the following ways:

1. Using the button:[Stop[button from the "Capture Info" dialog box.

Note

The "Capture Info" dialog box might be hidden if the "Hide capture info dialog" option is used.

1. Using the Capture → Stop menu item.
2. Using the Stop toolbar button.
3. Pressing **Ctrl**+**E**.
4. The capture will be automatically stopped if one of the *Stop Conditions* is met, e.g. the maximum amount of data was captured.

4.13.3. Restart a running capture

A running capture session can be restarted with the same capture options as the last time, this will remove all packets previously captured. This can be useful, if some uninteresting packets are captured and there's no need to keep them.

Restart is a convenience function and equivalent to a capture stop following by an immediate capture start. A restart can be triggered in one of the following ways:

1. Using the Capture → Restart menu item.

2. Using the Restart toolbar button.

Chapter 5. File Input, Output, and Printing

5.1. Introduction

This chapter will describe input and output of capture data.

- Open capture files in various capture file formats
- Save/Export capture files in various capture file formats
- Merge capture files together
- Import text files containing hex dumps of packets
- Print packets

5.2. Open capture files

Wireshark can read in previously saved capture files. To read them, simply select the File → Open menu or toolbar item. Wireshark will then pop up the "File Open" dialog box, which is discussed in more detail in Section 5.2.1, "The "Open Capture File" dialog box".

It's convenient to use drag-and-drop

You can open a file by simply dragging it in your file manager and dropping it onto Wireshark's main window. However, drag-and-drop may not be available in all desktop environments.

If you haven't previously saved the current capture file you will be asked to do so to prevent data loss. This warning can be disabled in the preferences.

In addition to its native file format (pcapng), Wireshark can read and write capture files from a large number of other packet capture programs as well. See Section 5.2.2, "Input File Formats" for the list of capture formats Wireshark understands.

5.2.1. The "Open Capture File" dialog box

The "Open Capture File" dialog box allows you to search for a capture file containing previously captured packets for display in Wireshark. The following sections show some examples of the Wireshark "Open File" dialog box. The appearance of this dialog depends on the system. However, the functionality should be the same across systems.

Common dialog behaviour on all systems:

- Select files and directories.
- Click the Open or OK button to accept your selected file and open it.
- Click the Cancel button to go back to Wireshark and not load a capture file.

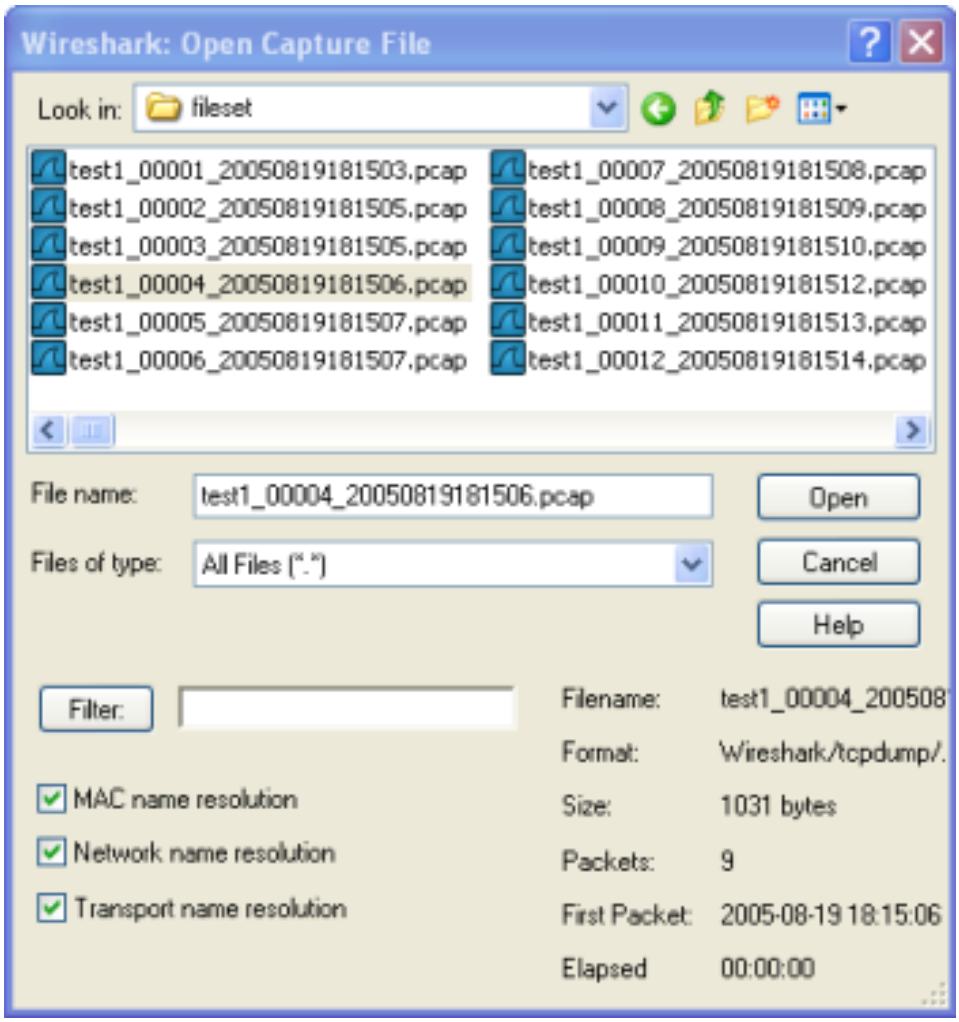
Wireshark extensions to the standard behaviour of these dialogs:

- View file preview information such as the filesize and the number of packets in a selected a capture file.
- Specify a display filter with the Filter button and filter field. This filter will be used when opening the new file. The text field background becomes green for a valid filter string and red for an invalid one. Clicking on the Filter button causes Wireshark to pop up the “Filters” dialog box (which is discussed further in Section 6.3, “Filtering packets while viewing”).
- Specify which type of name resolution is to be performed for all packets by clicking on one of the “… name resolution” check buttons. Details about name resolution can be found in Section 7.8, “Name Resolution”.

Save a lot of time loading huge capture files

You can change the display filter and name resolution settings later while viewing the packets. However, loading huge capture files can take a significant amount of extra time if these settings are changed later, so in such situations it can be a good idea to set at least the filter in advance here.

Figure 5.1. “Open” on Microsoft Windows

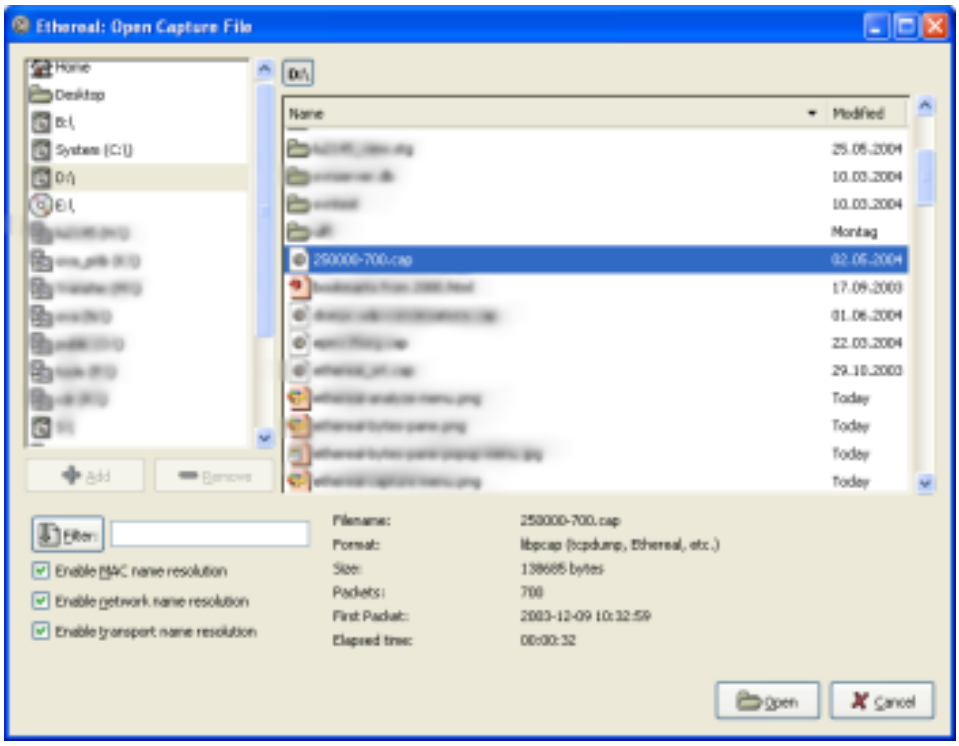


This is the common Windows file open dialog - plus some Wireshark extensions.

Specific for this dialog:

- The Help button will lead you to this section of this “User’s Guide”.

Figure 5.2. “Open” - Linux and UNIX



This is the common Gimp/GNOME file open dialog plus some Wireshark extensions.

Specific for this dialog:

- The + button allows you to add a directory selected in the right-hand pane to the favorites list on the left. These changes are persistent.
- The - button allows you to remove a selected directory from the list. Some items (such as “Desktop”) cannot be removed from the favorites list.
- If Wireshark doesn’t recognize the selected file as a capture file it will grey out the Open button.

5.2.2. Input File Formats

The following file formats from other capture tools can be opened by Wireshark:

- pcapng. A flexible, etensible successor to the libpcap format. Wireshark 1.8 and later save files as pcapng by default. Versions prior to 1.8 used libpcap.
- libpcap. The default format used by the *libpcap* packet capture library. Used by *tcpdump*, *_Snort*, *Nmap*, *Ntop*, and many other tools.
- Oracle (previously Sun) *snoop* and *atmsnoop*
- Finisar (previously Shomiti) *Surveyor* captures

- Microsoft *Network Monitor* captures
- Novell *LANalyzer* captures
- AIX *iptrace* captures
- Cinco Networks NetXray captures
- Network Associates Windows-based Sniffer and Sniffer Pro captures
- Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures
- AG Group/WildPackets/Savvius EtherPeek/TokenPeek/AiroPeek/EtherHelp/PacketGrabber captures
- RADCOM’s WAN/LAN Analyzer captures
- Network Instruments Observer version 9 captures
- Lucent/Ascend router debug output
- HP-UX’s nettl
- Toshiba’s ISDN routers dump output
- ISDN4BSD *i4btrace* utility
- traces from the EyeSDN USB S0
- IPLog format from the Cisco Secure Intrusion Detection System
- pppd logs (pppdump format)
- the output from VMS’s TCPIPtrace/TCPtrace/UCX$TRACE utilities
- the text output from the DBS Etherwatch VMS utility
- Visual Networks' Visual UpTime traffic capture
- the output from CoSine L2 debug
- the output from Accellent’s 5Views LAN agents
- Endace Measurement Systems' ERF format captures
- Linux Bluez Bluetooth stack hcidump -w traces
- Catapult DCT2000 .out files
- Gammu generated text output from Nokia DCT3 phones in Netmonitor mode
- IBM Series (OS/400) Comm traces (ASCII & UNICODE)
- Juniper Netscreen snoop captures
- Symbian OS btsnoop captures
- Tamosoft CommView captures
- Textronix K12xx 32bit .rf5 format captures
- Textronix K12 text file format captures

- Apple PacketLogger captures
- Captures from Aethra Telecommunications' PC108 software for their test instruments

New file formats are added from time to time.

It may not be possible to read some formats dependent on the packet types captured. Ethernet captures are usually supported for most file formats but it may not be possible to read other packet types such as PPP or IEEE 802.11 from all file formats.

5.3. Saving captured packets

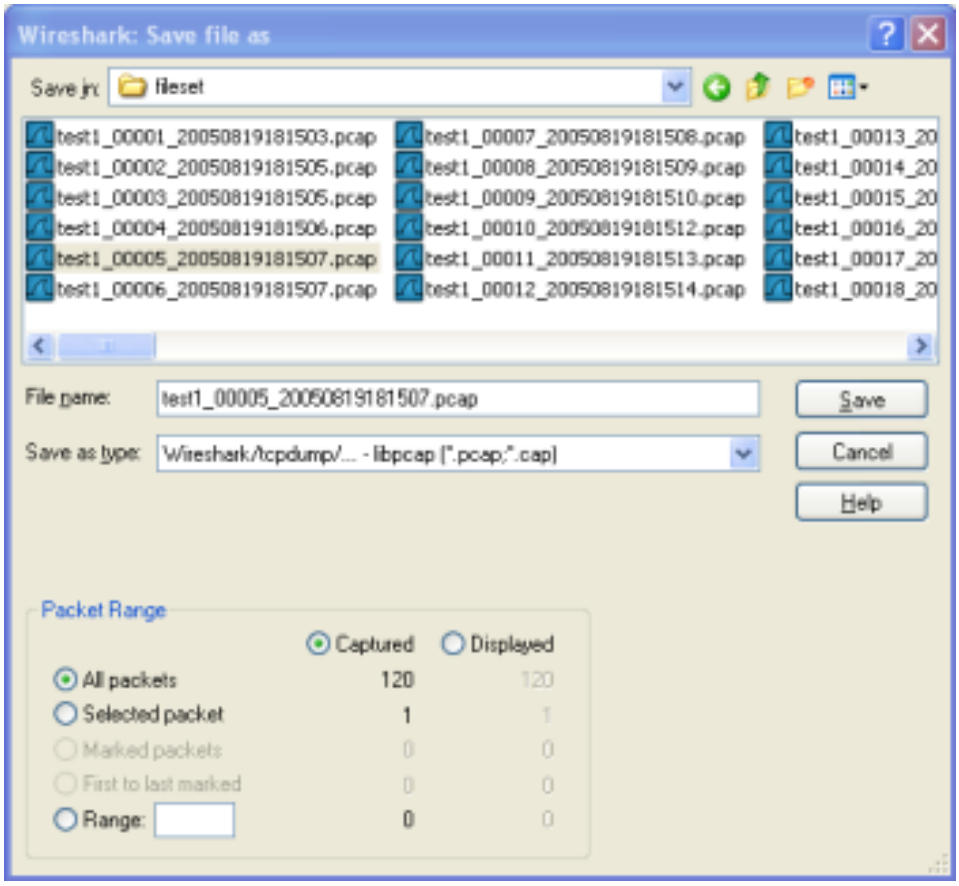
You can save captured packets simply by using the File → Save As… menu item. You can choose which packets to save and which file format to be used.

Not all information will be saved in a capture file. For example, most file formats don't record the number of dropped packets. See Section B.1, "Capture Files" for details.

5.3.1. The "Save Capture File As" dialog box

The "Save Capture File As" dialog box allows you to save the current capture to a file. The following sections show some examples of this dialog box. The appearance of this dialog depends on the system. However, the functionality should be the same across systems.

Figure 5.3. "Save" on Microsoft Windows

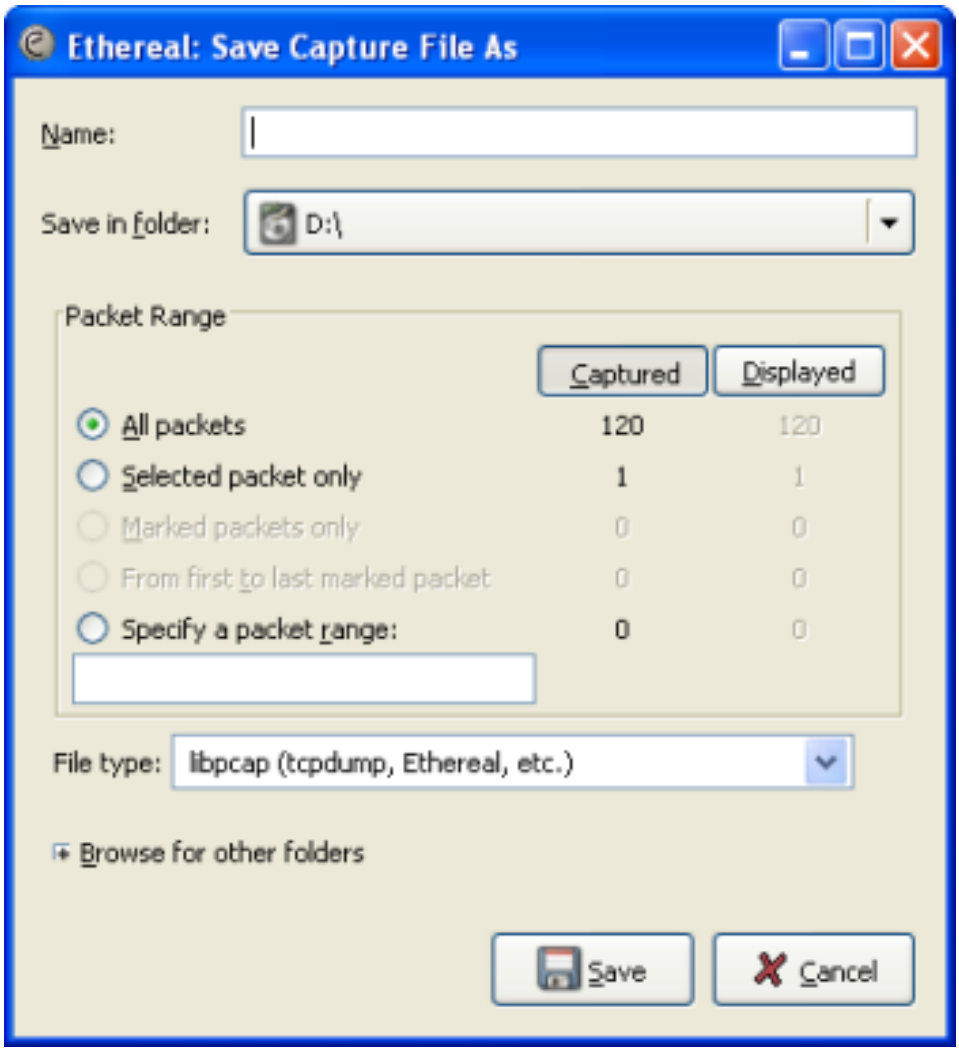


This is the common Windows file save dialog with some additional Wireshark extensions.

Specific behavior for this dialog:

- If available, the “Help” button will lead you to this section of this "User’s Guide".
- If you don’t provide a file extension to the filename (e.g. `.pcap`) Wireshark will append the standard file extension for that file format.

Figure 5.4. “Save” on Linux and UNIX



This is the common Gimp/GNOME file save dialog with additional Wireshark extensions.

Specific for this dialog:

- Clicking on the + at "Browse for other folders" will allow you to browse files and folders in your file system.

With this dialog box, you can perform the following actions:

1. Type in the name of the file you wish to save the captured packets in, as a standard file name in your file system.

2. Select the directory to save the file into.

3. Select the range of the packets to be saved. See Section 5.9, “The “Packet Range” frame”.

4. Specify the format of the saved capture file by clicking on the File type drop down box. You can choose from the types described in Section 5.3.2, “Output File Formats”.

Some capture formats may not be available depending on the packet types captured.

Wireshark can convert file formats

You can convert capture files from one format to another by reading in a capture file and writing it out using a different format.

1. Click the Save or OK button to accept your selected file and save to it. If Wireshark has a problem saving the captured packets to the file you specified it will display an error dialog box. After clicking OK on that error dialog box you can try again.

2. Click on the Cancel button to go back to Wireshark without saving any packets.

5.3.2. Output File Formats

Wireshark can save the packet data in its native file format (pcapng) and in the file formats of other protocol analyzers so other tools can read the capture data.

Different file formats have different time stamp accuracies

Saving from the currently used file format to a different format may reduce the time stamp accuracy; see the Section 7.5, “Time Stamps” for details.

The following file formats can be saved by Wireshark (with the known file extensions):

- pcapng (*.pcapng). A flexible, etensible successor to the libpcap format. Wireshark 1.8 and later save files as pcapng by default. Versions prior to 1.8 used libpcap.
- libpcap, tcpdump and various other tools using tcpdump’s capture format (*.pcap,*.cap,*.dmp)
- Accellent 5Views (*.5vw)
- HP-UX’s nettl (*.TRC0,*.TRC1)
- Microsoft Network Monitor - NetMon (*.cap)
- Network Associates Sniffer - DOS (*.cap,*.enc,*.trc,*fdc,*.syc)
- Network Associates Sniffer - Windows (*.cap)
- Network Instruments Observer version 9 (*.bfr)
- Novell LANalyzer (*.tr1)
- Oracle (previously Sun) snoop (*.snoop,*.cap)
- Visual Networks Visual UpTime traffic (*.*)

New file formats are added from time to time.

Whether or not the above tools will be more helpful than Wireshark is a different question ;-)

Third party protocol analyzers may require specific file extensions

Wireshark examines a file's contents to determine its type. Some other protocol analyzers only look at a filename extensions. For example, you might need to use the `.cap` extension in order to open a file using *Sniffer*.

5.4. Merging capture files

Sometimes you need to merge several capture files into one. For example, this can be useful if you have captured simultaneously from multiple interfaces at once (e.g. using multiple instances of Wireshark).

There are three ways to merge capture files using Wireshark:

- Use the File → Merge menu to open the "Merge" dialog. See Section 5.4.1, "The "Merge with Capture File" dialog box". This menu item will be disabled unless you have loaded a capture file.
- Use *drag-and-drop* to drop multiple files on the main window. Wireshark will try to merge the packets in chronological order from the dropped files into a newly created temporary file. If you drop only a single file it will simply replace the existing capture.
- Use the `mergecap` tool, a command line tool to merge capture files. This tool provides the most options to merge capture files. See Section D.8, "*mergecap*: Merging multiple capture files into one" for details.

5.4.1. The "Merge with Capture File" dialog box

This dialog box let you select a file to be merged into the currently loaded file. If your current data has not been saved you will be asked to save it first.

Most controls of this dialog will work the same way as described in the "Open Capture File" dialog box, see Section 5.2.1, "The "Open Capture File" dialog box".

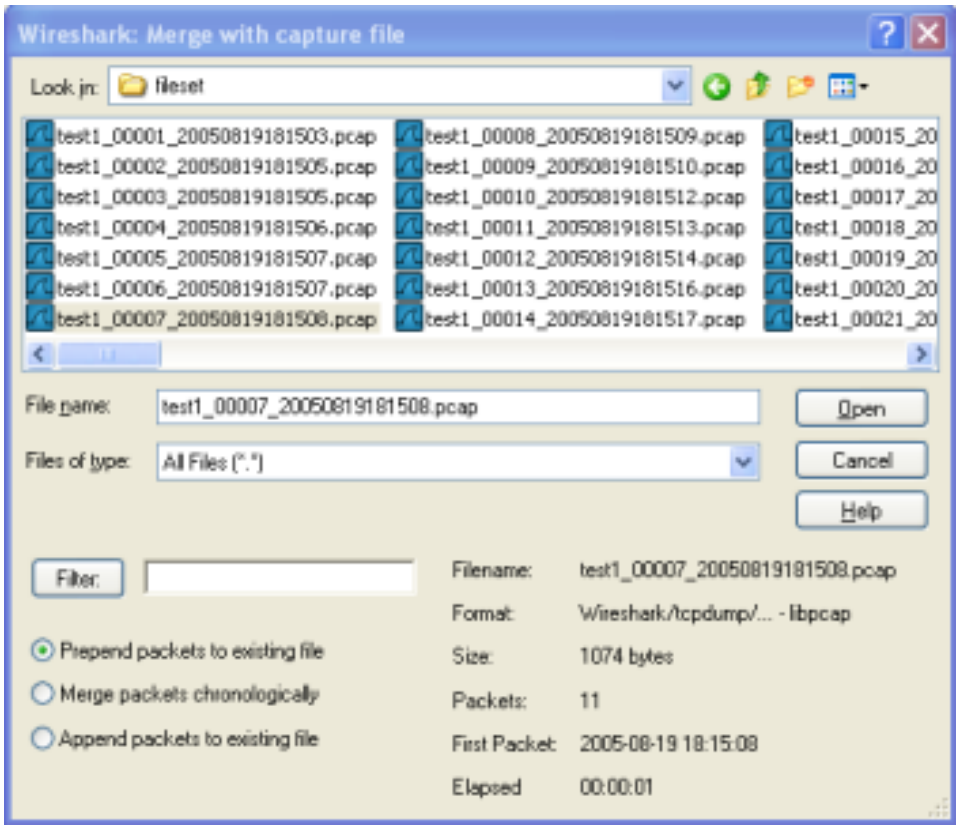
Specific controls of this merge dialog are:

Prepend packets to existing file
: Prepend the packets from the selected file before the currently loaded packets.

Merge packets chronologically
: Merge both the packets from the selected and currently loaded file in chronological order.

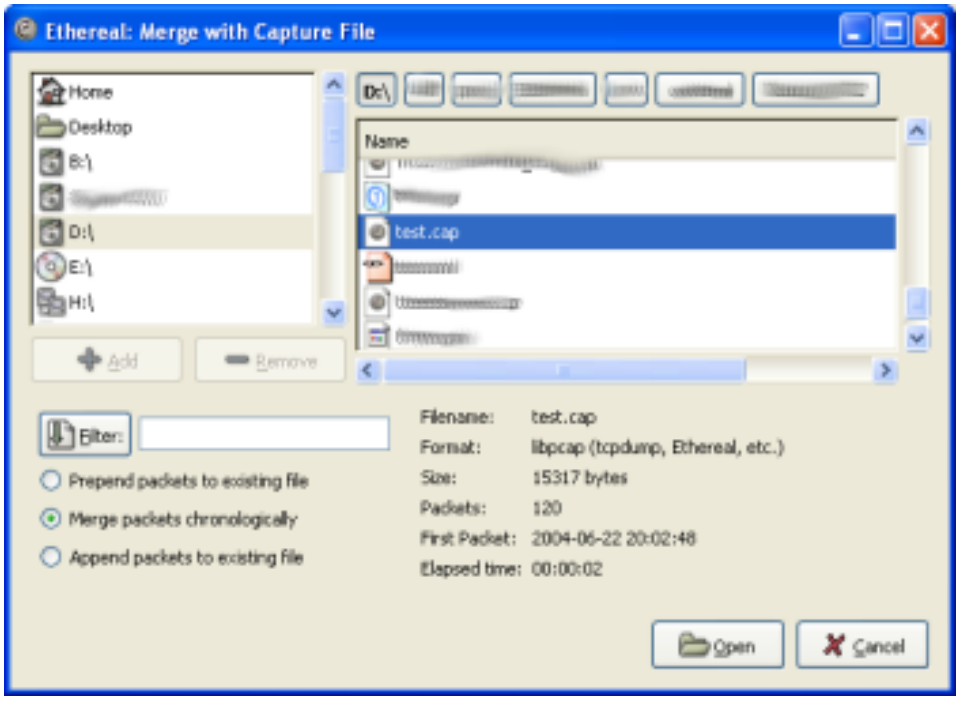
Append packets to existing file
: Append the packets from the selected file after the currently loaded packets.

Figure 5.5. “Merge” on Microsoft Windows



This is the common Windows file open dialog with additional Wireshark extensions.

Figure 5.6. “Merge” on Linux and UNIX



This is the common Gimp/GNOME file open dialog with additional Wireshark extensions.

5.5. Import hex dump

Wireshark can read in an ASCII hex dump and write the data described into a temporary libpcap capture file. It can read hex dumps with multiple packets in them, and build a capture file of multiple packets. It is also capable of generating dummy Ethernet, IP and UDP, TCP, or SCTP headers, in order to build fully processable packet dumps from hexdumps of application-level data only.

Wireshark understands a hexdump of the form generated by `od -Ax -tx1 -v`. In other words, each byte is individually displayed and surrounded with a space. Each line begins with an offset describing the position in the file. The offset is a hex number (can also be octal or decimal), of more than two hex digits. Here is a sample dump that can be imported:

```
000000 00 e0 1e a7 05 6f 00 10 ........
000008 5a a0 b9 12 08 00 46 00 ........
000010 03 68 00 00 00 00 0a 2e ........
000018 ee 33 0f 19 08 7f 0f 19 ........
000020 03 80 94 04 00 00 10 01 ........
000028 16 a2 0a 00 03 50 00 0c ........
000030 01 01 0f 19 03 80 11 01 ........
```

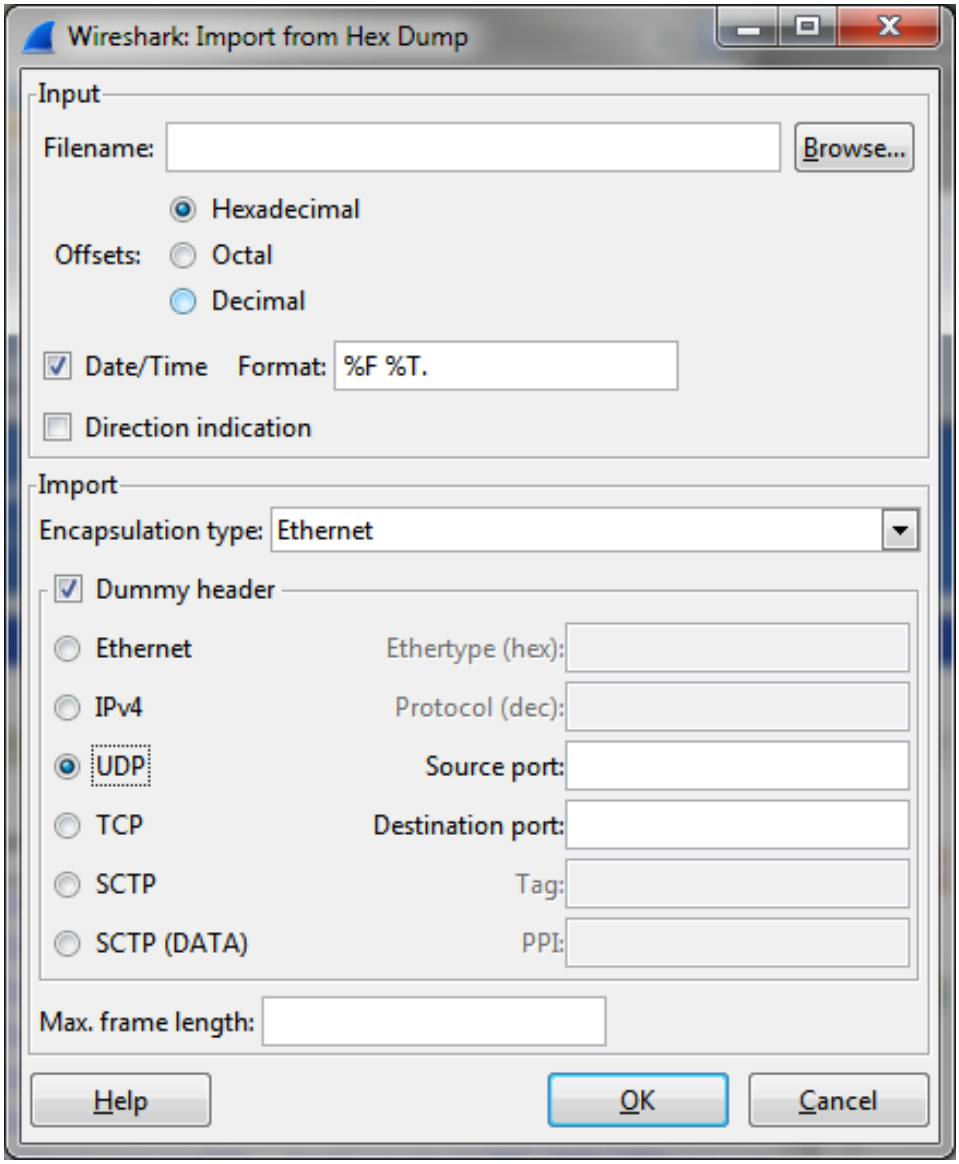
There is no limit on the width or number of bytes per line. Also the text dump at the end of the line is ignored. Byte and hex numbers can be uppercase or lowercase. Any text before the offset is ignored, including email forwarding characters >. Any lines of text between the bytestring lines are ignored. The offsets are used to track the bytes, so offsets must be correct. Any line which has only bytes without a leading offset is ignored. An offset is recognized as being a hex number longer than two characters. Any text after the bytes is ignored (e.g. the character dump). Any hex numbers in this text are also ignored. An offset of zero is indicative of starting a new packet, so a single text file with a series of hexdumps can be converted into a packet capture with multiple packets. Packets may be preceded by a timestamp. These are interpreted according to the format given. If not the first packet is timestamped with the current time the import takes place. Multiple packets are read in with timestamps differing by one microsecond each. In general, short of these restrictions, Wireshark is pretty liberal about reading in hexdumps and has been tested with a variety of mangled outputs (including being forwarded through email multiple times, with limited line wrap etc.)

There are a couple of other special features to note. Any line where the first non-whitespace character is # will be ignored as a comment. Any line beginning with `#TEXT2PCAP` is a directive and options can be inserted after this command to be processed by Wireshark. Currently there are no directives implemented. In the future these may be used to give more fine grained control on the dump and the way it should be processed e.g. timestamps, encapsulation type etc. Wireshark also allows the user to read in dumps of application-level data, by inserting dummy L2, L3 and L4 headers before each packet. The user can elect to insert Ethernet headers, Ethernet and IP, or Ethernet, IP and UDP/TCP/SCTP headers before each packet. This allows Wireshark or any other full-packet decoder to handle these dumps.

5.5.1. The “Import from Hex Dump” dialog box

This dialog box lets you select a text file, containing a hex dump of packet data, to be imported and set import parameters.

Figure 5.7. The “Import from Hex Dump” dialog



Specific controls of this import dialog are split in two sections:

Input
: Determine which input file has to be imported and how it is to be interpreted.

Import
: Determine how the data is to be imported.

The input parameters are as follows:

Filename / Browse
: Enter the name of the text file to import. You can use *Browse* to browse for a file.

Offsets
: Select the radix of the offsets given in the text file to import. This is usually hexadecimal, but decimal and octal are also supported.

Date/Time
Tick this checkbox if there are timestamps associated with the frames in the text file to import you would like to use. Otherwise the current time is used for timestamping the frames.

Format
This is the format specifier used to parse the timestamps in the text file to import. It uses a simple syntax to describe the format of the timestamps, using %H for hours, %M for minutes, %S for seconds, etc. The straightforward HH:MM:SS format is covered by %T. For a full definition of the syntax look for `strptime(3)`.

The import parameters are as follows:

Encapsulation type
Here you can select which type of frames you are importing. This all depends on from what type of medium the dump to import was taken. It lists all types that Wireshark understands, so as to pass the capture file contents to the right dissector.

Dummy header
When Ethernet encapsulation is selected you have to option to prepend dummy headers to the frames to import. These headers can provide artificial Ethernet, IP, UDP or TCP or SCTP headers and SCTP data chunks. When selecting a type of dummy header the applicable entries are enabled, others are grayed out and default values are used.

Maximum frame length
You may not be interested in the full frames from the text file, just the first part. Here you can define how much data from the start of the frame you want to import. If you leave this open the maximum is set to 65535 bytes.

Once all input and import parameters are setup click OK to start the import. If your current data wasn't saved before you will be asked to save it first.

When completed there will be a new capture file loaded with the frames imported from the text file.

5.6. File Sets

When using the "Multiple Files" option while doing a capture (see: Section 4.11, "Capture files and file modes"), the capture data is spread over several capture files, called a file set.

As it can become tedious to work with a file set by hand, Wireshark provides some features to handle these file sets in a convenient way.

How does Wireshark detect the files of a file set?

A filename in a file set uses the format Prefix_Number_DateTimeSuffix which might look something like `test_00001_20060420183910.pcap`. All files of a file set share the same prefix (e.g. "test") and suffix (e.g. ".pcap") and a varying middle part.

To find the files of a file set, Wireshark scans the directory where the currently loaded file resides and checks for files matching the filename pattern (prefix and suffix) of the currently loaded file.

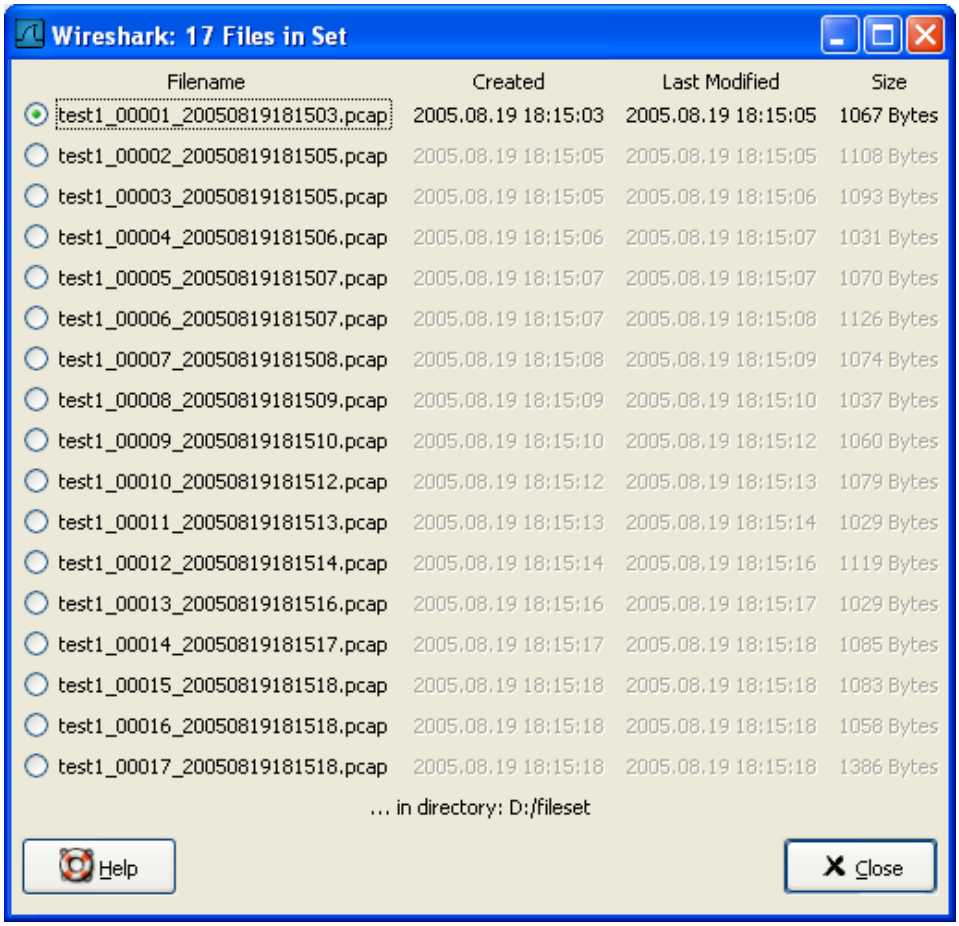
This simple mechanism usually works well but has its drawbacks. If several file sets were captured with the same prefix and suffix, Wireshark will detect them as a single file set. If files were renamed or spread over several directories the mechanism will fail to find all files of a set.

The following features in the File → File Set submenu are available to work with file sets in a convenient way:

- The “List Files” dialog box will list the files Wireshark has recognized as being part of the current file set.
- Next File closes the current and opens the next file in the file set.
- Previous File closes the current and opens the previous file in the file set.

5.6.1. The “List Files” dialog box

Figure 5.8. The "List Files" dialog box



Each line contains information about a file of the file set:

- *Filename* the name of the file. If you click on the filename (or the radio button left to it), the current file will be closed and the corresponding capture file will be opened.
- *Created* the creation time of the file
- *Last Modified* the last time the file was modified
- *Size* the size of the file

The last line will contain info about the currently used directory where all of the files in the file set can be found.

The content of this dialog box is updated each time a capture file is opened/closed.

The Close button will, well, close the dialog box.

5.7. Exporting data

Wireshark provides several ways and formats to export packet data. This section describes general ways to export data from the main Wireshark application. There are more specialized functions to export specific data which are described elsewhere.

5.7.1. The “Export as Plain Text File” dialog box

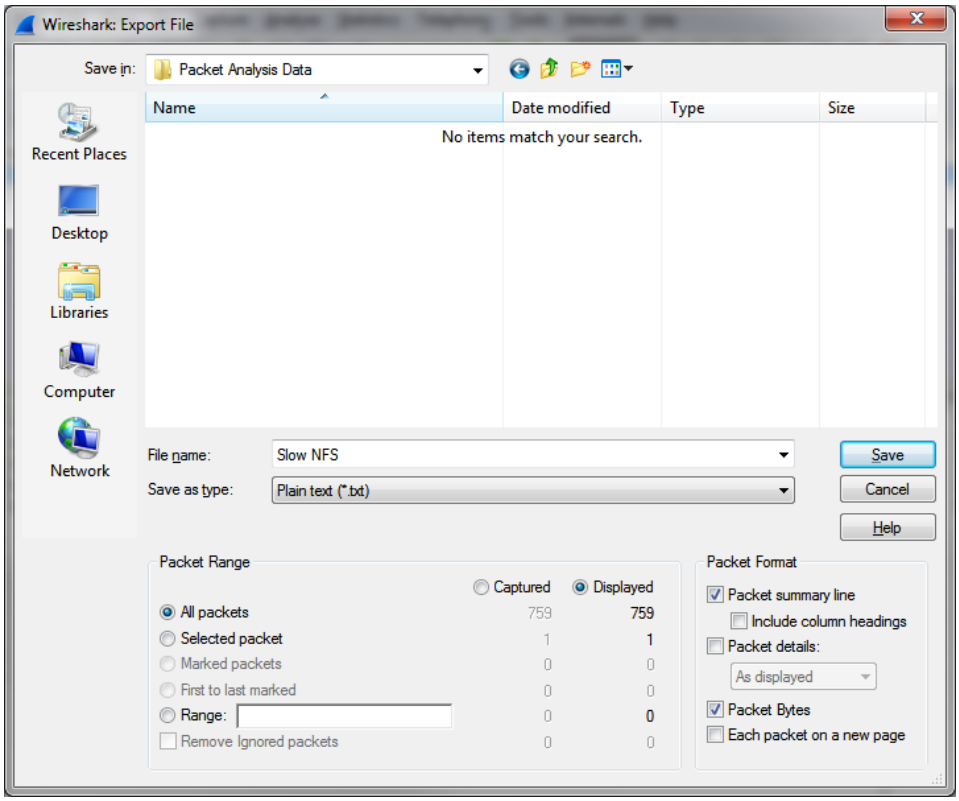
Export packet data into a plain ASCII text file, much like the format used to print packets.

Tip

If you would like to be able to import any previously exported packets from a plain text file it is recommended that you:

- Add the “Absolute date and time” column.
- Temporarily hide all other columns.
- Disable the Edit → Preferences → Protocols → Data “Show not dissected data on new Packet Bytes pane” preference. More details are provided in Section 10.5, “Preferences”
- Include the packet summary line.
- Exclude column headings.
- Exclude packet details.
- Include the packet bytes.

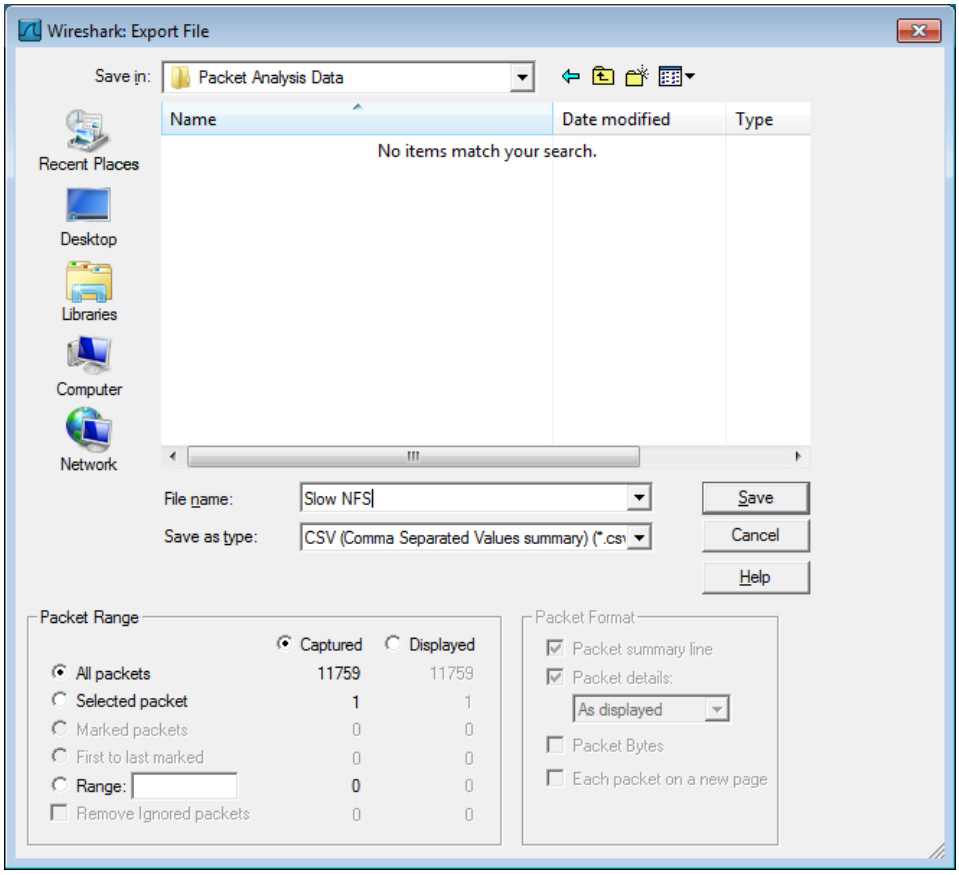
Figure 5.9. The “Export as Plain Text File” dialog box



- The “Export to file:” frame chooses the file to export the packet data to.
- The “Packet Range” frame is described in Section 5.9, “The “Packet Range” frame”.
- The “Packet Details” frame is described in Section 5.10, “The Packet Format frame”.

5.7.2. The “Export as PostScript File” dialog box

Figure 5.10. The "Export as PostScript File" dialog box



- *Export to file:* frame chooses the file to export the packet data to.
- The *Packet Range* frame is described in Section 5.9, “The “Packet Range” frame”.
- The *Packet Details* frame is described in Section 5.10, “The Packet Format frame”.

5.7.3. The "Export as CSV (Comma Separated Values) File" dialog box

Export packet summary into CSV, used e.g. by spreadsheet programs to im-/export data.

- *Export to file:* frame chooses the file to export the packet data to.
- The *Packet Range* frame is described in Section 5.9, “The “Packet Range” frame”.

5.7.4. The "Export as C Arrays (packet bytes) file" dialog box

Export packet bytes into C arrays so you can import the stream data into your own C program.

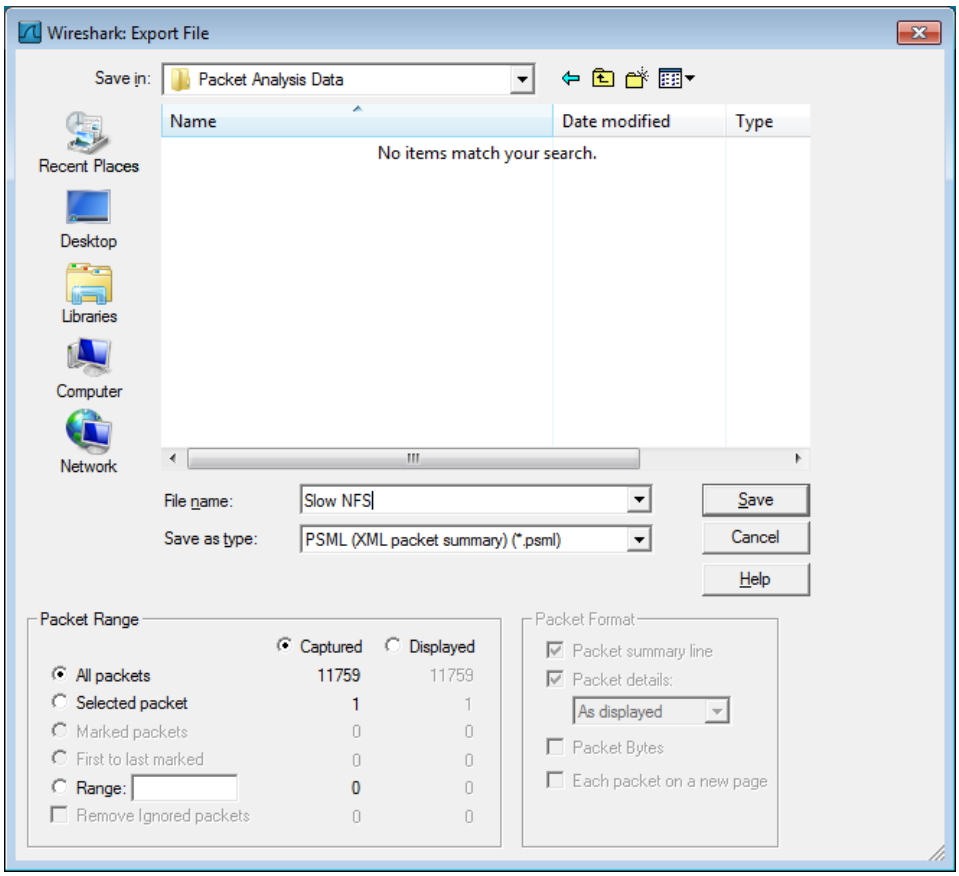
- *Export to file:* frame chooses the file to export the packet data to.

- The *Packet Range* frame is described in Section 5.9, “The “Packet Range” frame”.

5.7.5. The "Export as PSML File" dialog box

Export packet data into PSML. This is an XML based format including only the packet summary. The PSML file specification is available at: http://www.nbee.org/doku.php?id=netpdl:psml_specification.

Figure 5.11. The "Export as PSML File" dialog box



- *Export to file:* frame chooses the file to export the packet data to.

- The *Packet Range* frame is described in Section 5.9, “The “Packet Range” frame”.

There’s no such thing as a packet details frame for PSML export, as the packet format is defined by the PSML specification.

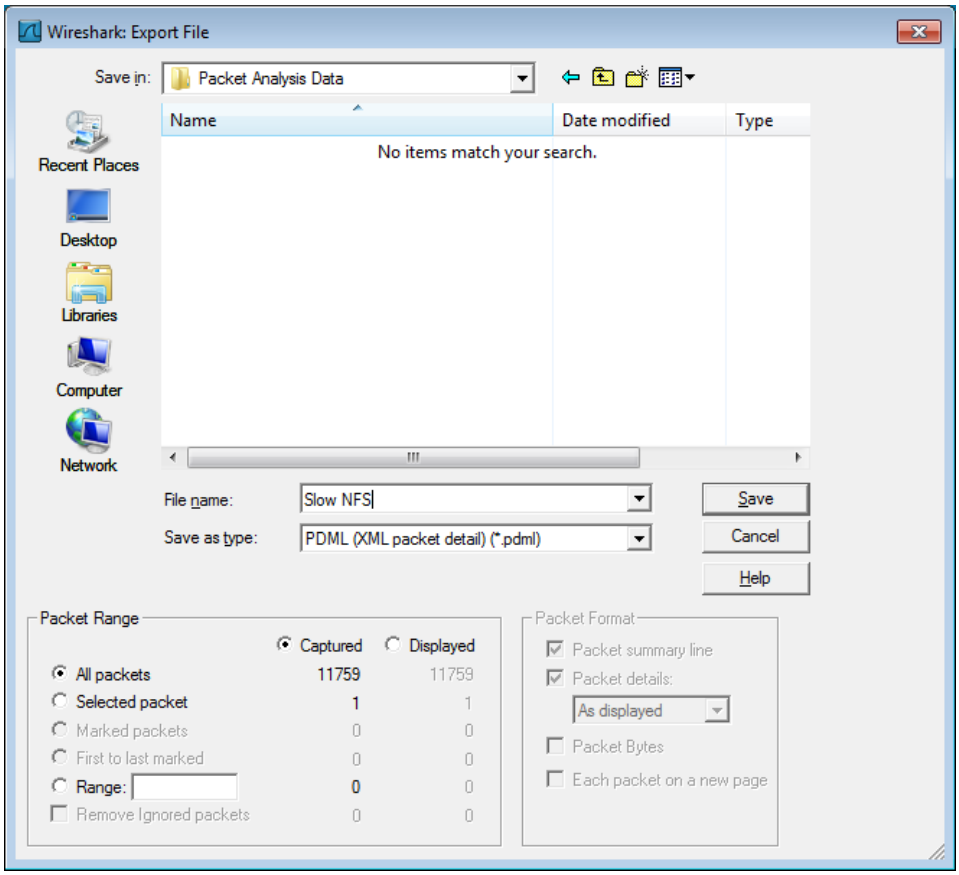
5.7.6. The "Export as PDML File" dialog box

Export packet data into PDML. This is an XML based format including the packet details. The PDML file specification is available at: http://www.nbee.org/doku.php?id=netpdl:pdml_specification.

Note

The PDML specification is not officially released and Wireshark’s implementation of it is still in an early beta state, so please expect changes in future Wireshark versions.

Figure 5.12. The "Export as PDML File" dialog box



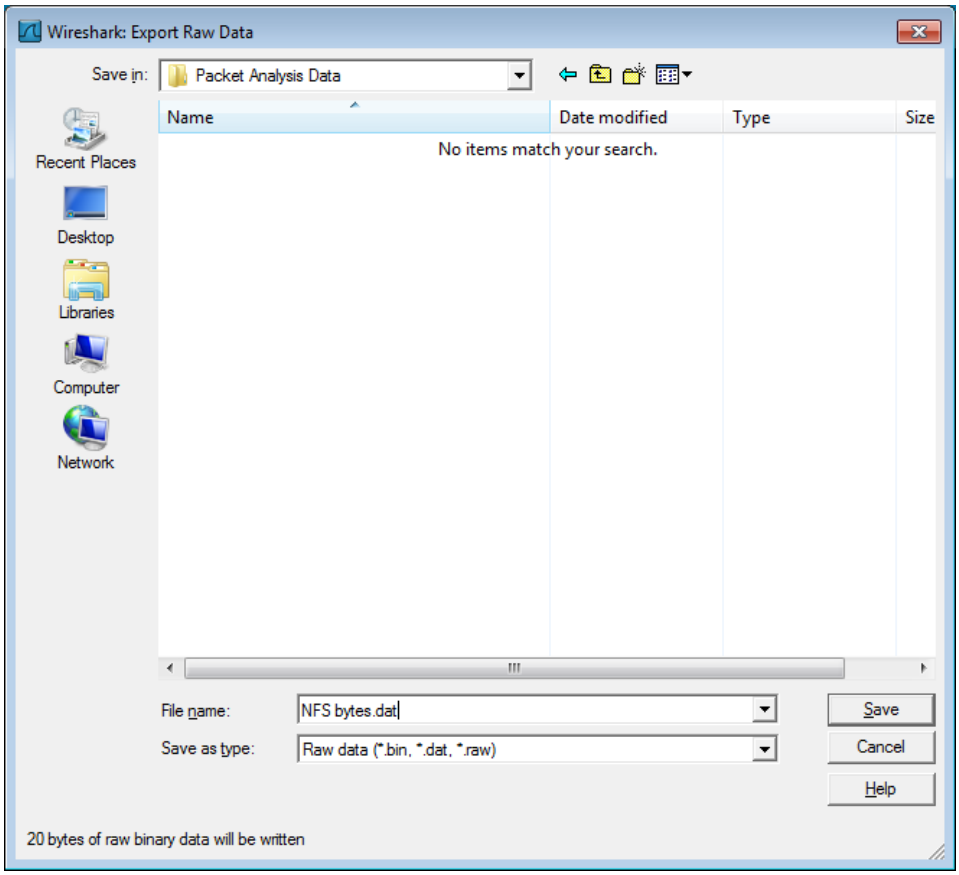
- *Export to file:* frame chooses the file to export the packet data to.
- The *Packet Range* frame is described in Section 5.9, “The “Packet Range” frame”.

There’s no such thing as a packet details frame for PDML export, as the packet format is defined by the PDML specification.

5.7.7. The "Export selected packet bytes" dialog box

Export the bytes selected in the "Packet Bytes" pane into a raw binary file.

Figure 5.13. The "Export Selected Packet Bytes" dialog box

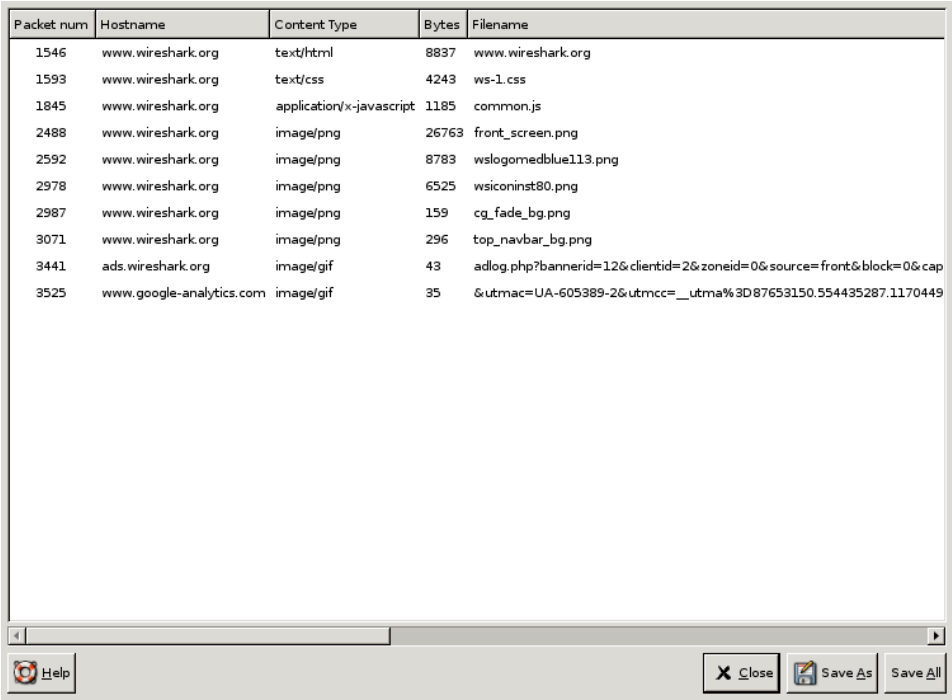


- *Name:* the filename to export the packet data to.
- The *Save in folder:* field lets you select the folder to save to (from some predefined folders).
- *Browse for other folders* provides a flexible way to choose a folder.

5.7.8. The "Export Objects" dialog box

This feature scans through HTTP streams in the currently open capture file or running capture and takes reassembled objects such as HTML documents, image files, executables and anything else that can be transferred over HTTP and lets you save them to disk. If you have a capture running, this list is automatically updated every few seconds with any new objects seen. The saved objects can then be opened with the proper viewer or executed in the case of executables (if it is for the same platform you are running Wireshark on) without any further work on your part. This feature is not available when using GTK2 versions below 2.4.

Figure 5.14. The "Export Objects" dialog box



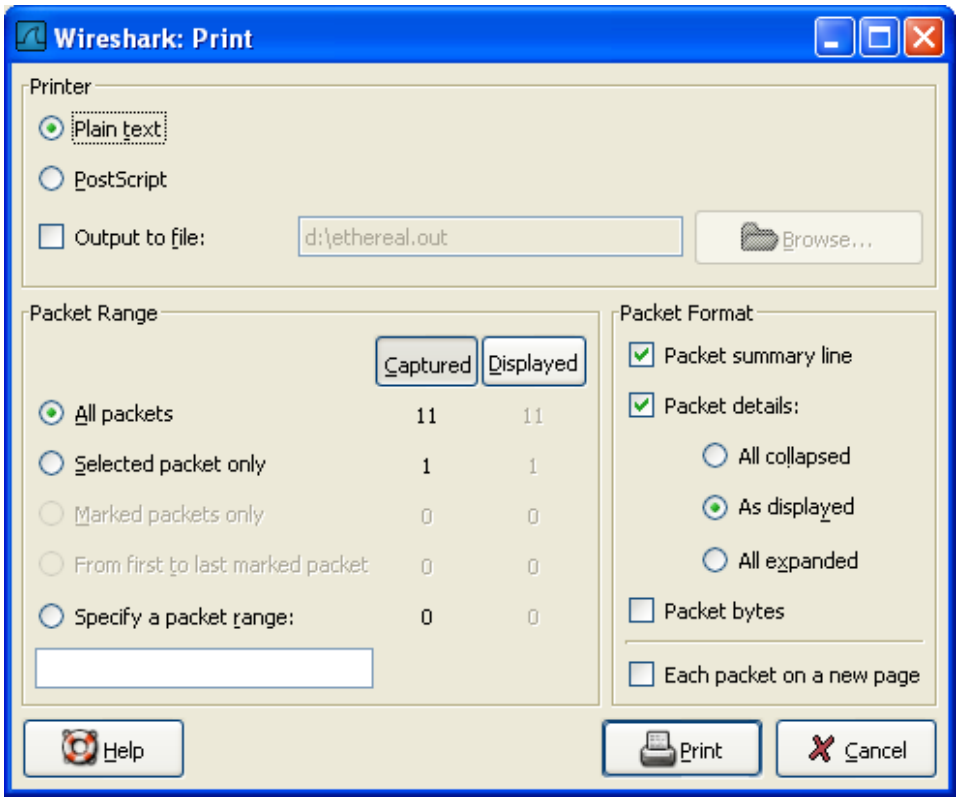
- *Packet num:* The packet number in which this object was found. In some cases, there can be multiple objects in the same packet.
- *Hostname:* The hostname of the server that sent the object as a response to an HTTP request.
- *Content Type:* The HTTP content type of this object.
- *Bytes:* The size of this object in bytes.
- *Filename:* The final part of the URI (after the last slash). This is typically a filename, but may be a long complex looking string, which typically indicates that the file was received in response to a HTTP POST request.
- *Help:* Opens this section in the user's guide.
- *Close:* Closes this dialog.
- *Save As:* Saves the currently selected object as a filename you specify. The default filename to save as is taken from the filename column of the objects list.
- *Save All:* Saves all objects in the list using the filename from the filename column. You will be asked what directory / folder to save them in. If the filename is invalid for the operating system / file system you are running Wireshark on, then an error will appear and that object will not be saved (but all of the others will be).

5.8. Printing packets

To print packets, select the File → Print… menu item. When you do this Wireshark pops up the "Print" dialog box as shown in Figure 5.15, "The "Print" dialog box".

5.8.1. The “Print” dialog box

Figure 5.15. The “Print” dialog box



The following fields are available in the Print dialog box: *Printer*
This field contains a pair of mutually exclusive radio buttons:

- *Plain Text* specifies that the packet print should be in plain text.
- *PostScript* specifies that the packet print process should use PostScript to generate a better print output on PostScript aware printers.
- *Output to file:* specifies that printing be done to a file, using the filename entered in the field or selected with the browse button.

  This field is where you enter the *file* to print to if you have selected Print to a file, or you can click the button to browse the filesystem. It is greyed out if Print to a file is not selected.
- *Print command* specifies that a command be used for printing.

  Note!

  These *Print command* fields are not available on windows platforms.

  This field specifies the command to use for printing. It is typically `lpr`. You would change it to specify a particular queue if you need to print to a queue other than the default. An example might be:

  ```
  $ lpr -Pmypostscript
  ```

This field is greyed out if *Output to file:* is checked above.

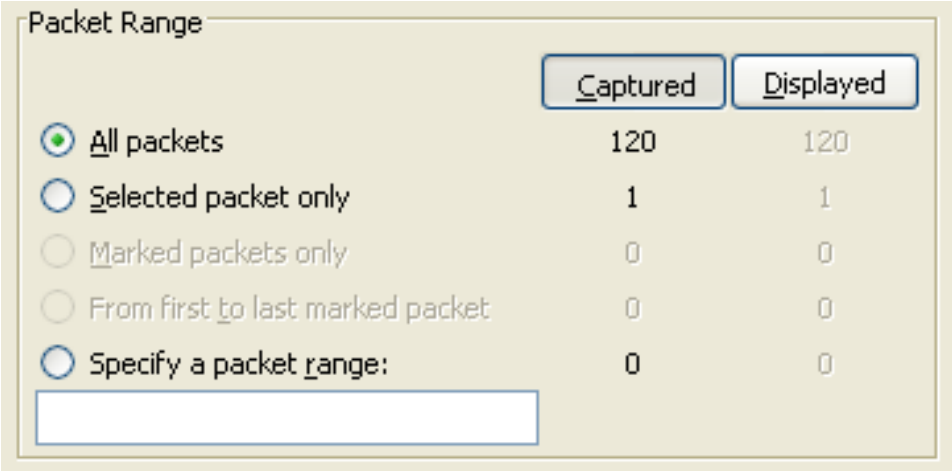
Packet Range
Select the packets to be printed, see Section 5.9, “The “Packet Range” frame”

Packet Format
Select the output format of the packets to be printed. You can choose, how each packet is printed, see Figure 5.17, “The “Packet Format” frame”

5.9. The “Packet Range” frame

The packet range frame is a part of various output related dialog boxes. It provides options to select which packets should be processed by the output function.

Figure 5.16. The “Packet Range” frame



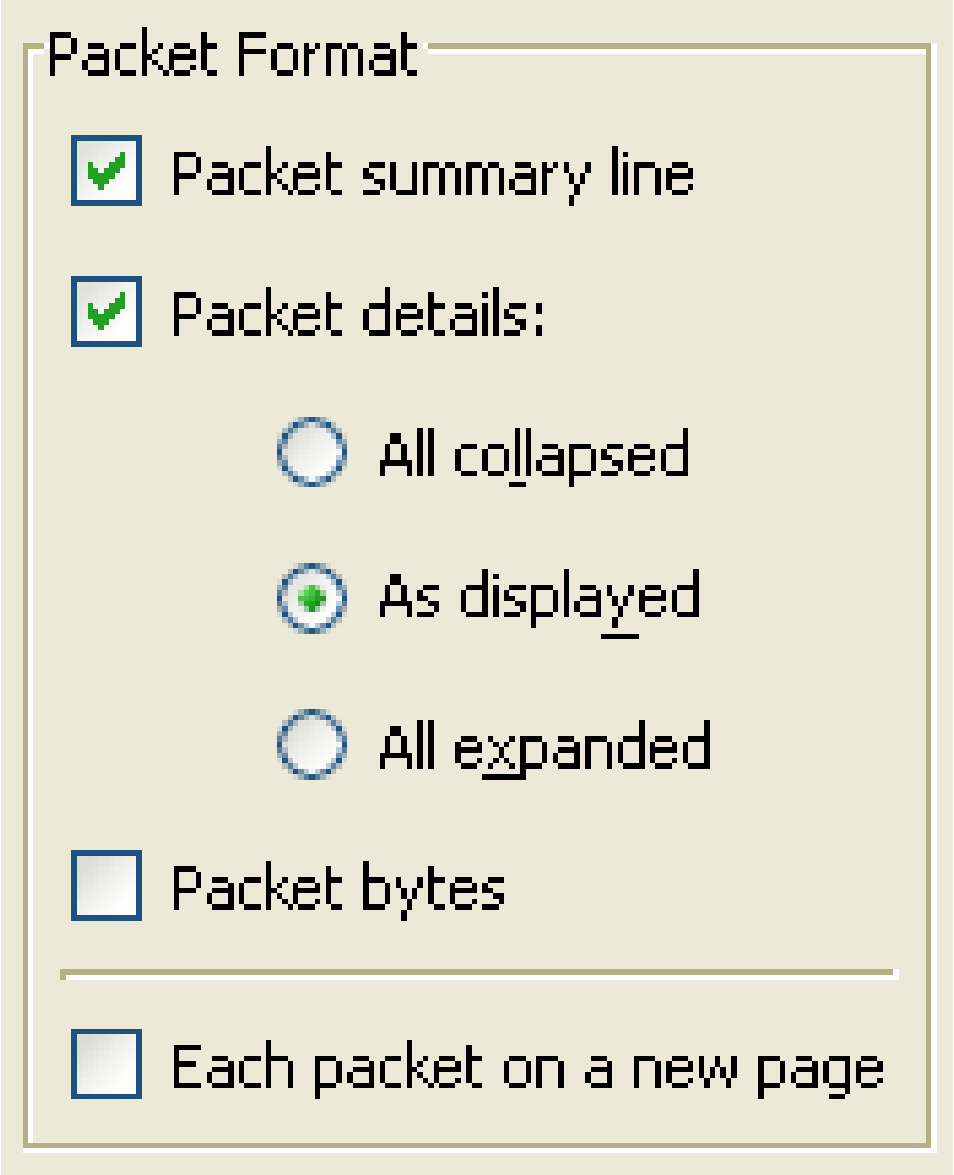
If the Captured button is set (default), all packets from the selected rule will be processed. If the Displayed button is set, only the currently displayed packets are taken into account to the selected rule.

- *All packets* will process all packets.
- *Selected packet only* process only the selected packet.
- *Marked packets only* process only the marked packets.
- *From first to last marked packet* process the packets from the first to the last marked one.
- *Specify a packet range* process a user specified range of packets, e.g. specifying *5,10-15,20-* will process the packet number five, the packets from packet number ten to fifteen (inclusive) and every packet from number twenty to the end of the capture.

5.10. The Packet Format frame

The packet format frame is a part of various output related dialog boxes. It provides options to select which parts of a packet should be used for the output function.

Figure 5.17. The “Packet Format” frame



- *Packet summary line* enable the output of the summary line, just as in the “Packet List” pane.
- *Packet details* enable the output of the packet details tree.
- *All collapsed* the info from the “Packet Details” pane in “all collapsed” state.
- *As displayed* the info from the “Packet Details” pane in the current state.
- *All expanded* the info from the “Packet Details” pane in “all expanded” state.
- *Packet bytes* enable the output of the packet bytes, just as in the “Packet Bytes” pane.
- *Each packet on a new page* put each packet on a separate page (e.g. when saving/printing to a text file, this will put a form feed character between the packets).

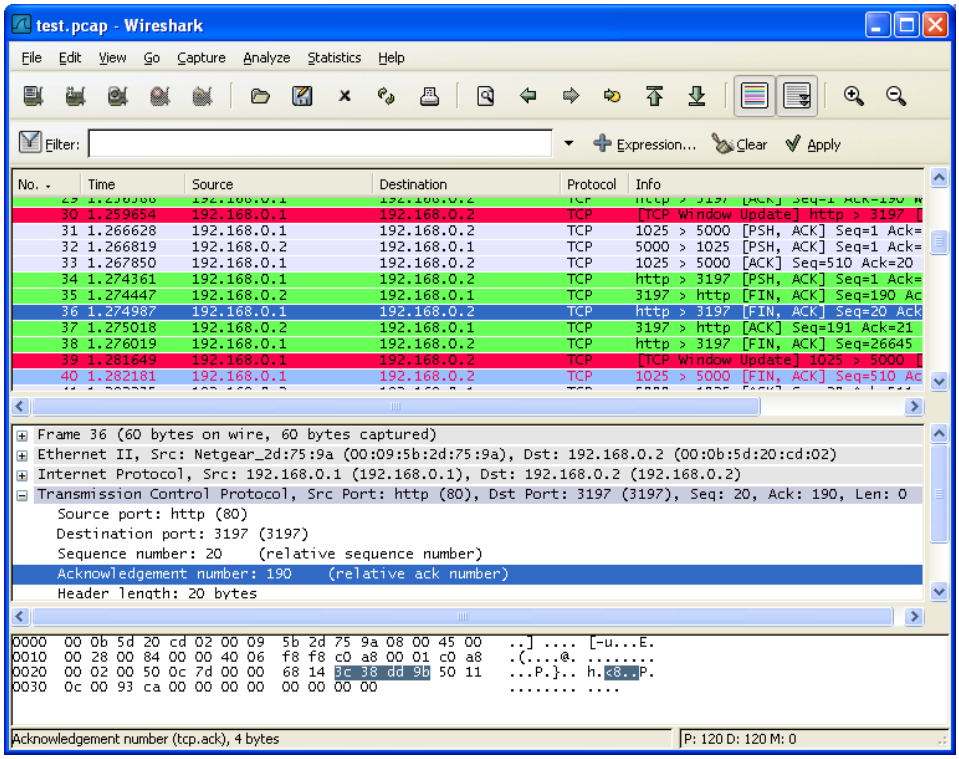
Chapter 6. Working with captured packets

6.1. Viewing packets you have captured

Once you have captured some packets or you have opened a previously saved capture file, you can view the packets that are displayed in the packet list pane by simply clicking on a packet in the packet list pane, which will bring up the selected packet in the tree view and byte view panes.

You can then expand any part of the tree to view detailed information about each protocol in each packet. Clicking on an item in the tree will highlight the corresponding bytes in the byte view. An example with a TCP packet selected is shown in Figure 6.1, “Wireshark with a TCP packet selected for viewing”. It also has the Acknowledgment number in the TCP header selected, which shows up in the byte view as the selected bytes.

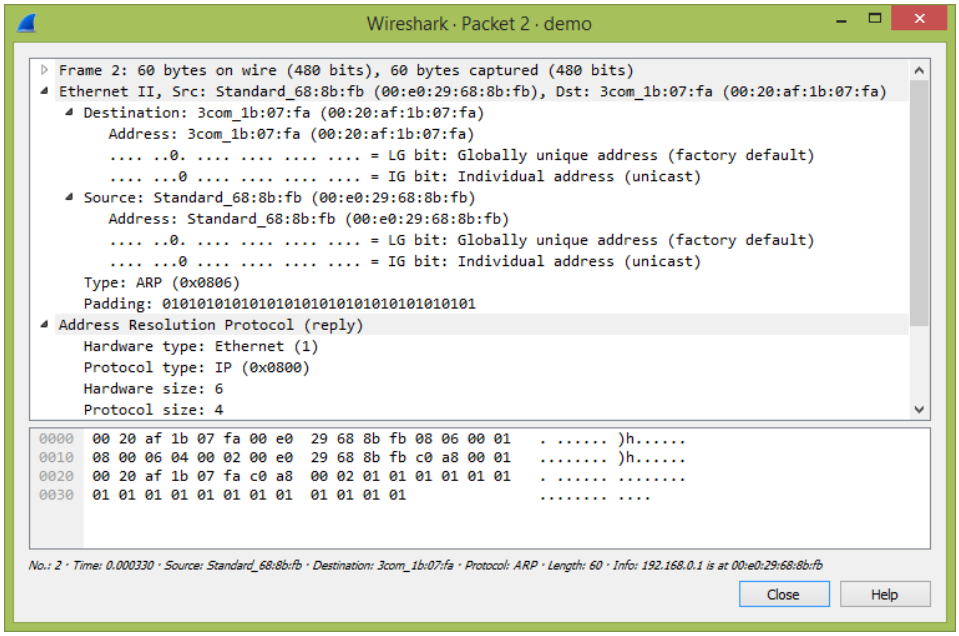
Figure 6.1. Wireshark with a TCP packet selected for viewing



You can also select and view packets the same way while Wireshark is capturing if you selected “Update list of packets in real time” in the “Capture Preferences” dialog box.

In addition you can view individual packets in a separate window as shown in Figure 6.2, “Viewing a packet in a separate window”. You can do this by double-clicking on an item in the packet list or by selecting the packet in which you are interested in the packet list pane and selecting View → Show Packet in New Window. This allows you to easily compare two or more packets, even across multiple files.

Figure 6.2. Viewing a packet in a separate window



Along with double-clicking the packet list and using the main menu there are a number of other ways to open a new packet window:

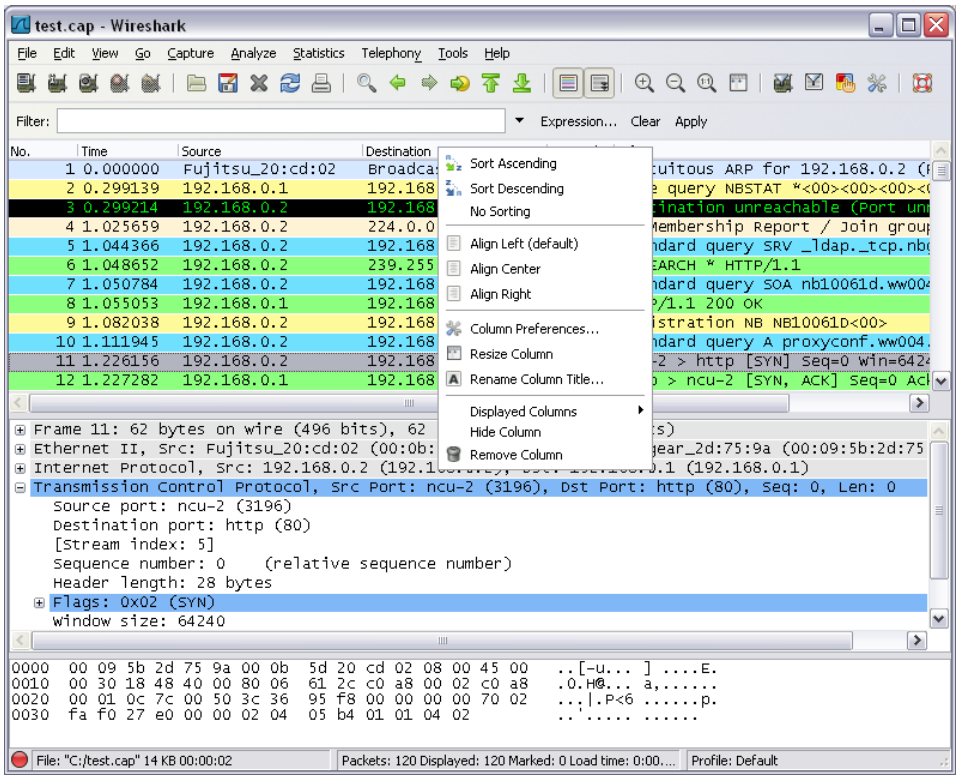
- Hold down the shift key and double-click on a frame link in the packet details.
- From Table 6.2, “The menu items of the “Packet List” pop-up menu”.
- From Table 6.3, “The menu items of the “Packet Details” pop-up menu”.

6.2. Pop-up menus

You can bring up a pop-up menu over either the “Packet List”, its column header, or “Packet Details” pane by clicking your right mouse button at the corresponding pane.

6.2.1. Pop-up menu of the “Packet List” column header

Figure 6.3. Pop-up menu of the “Packet List” column header



The following table gives an overview of which functions are available in this header, where to find the corresponding function in the main menu, and a short description of each item.

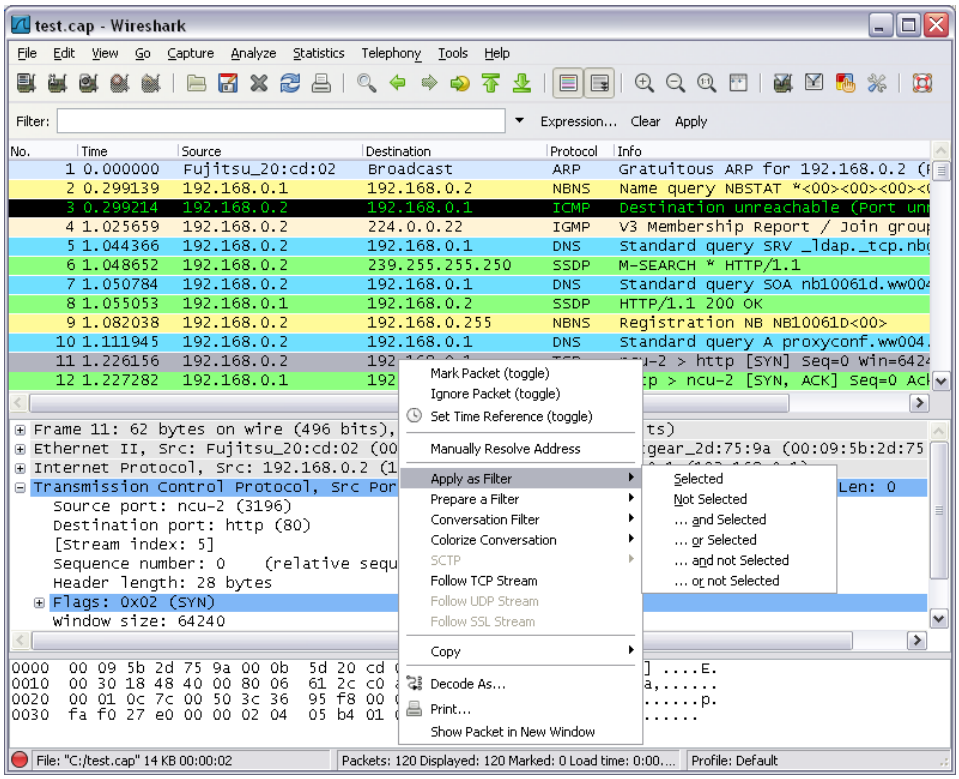
Table 6.1. The menu items of the “Packet List” column header pop-up menu

Item	Identical to main menu’s item:	Description
Sort Ascending		Sort the packet list in ascending order based on this column.
Sort Descending		Sort the packet list in descending order based on this column.
No Sort		Remove sorting order based on this column.
Align Left		Set left alignment of the values in this column.
Align Center		Set center alignment of the values in this column.
Align Right		Set right alignment of the values in this column.
Column Preferences…		Open the Preferences dialog box on the column tab.
Resize Column		Resize the column to fit the values.
Rename Column Title		Allows you to change the title of the column header.

Item	Identical to main menu's item:	Description
Displayed Column	View	This menu items folds out with a list of all configured columns. These columns can now be shown or hidden in the packet list.
Hide Column		Allows you to hide the column from the packet list.
Remove Column		Allows you to remove the column from the packet list.

6.2.2. Pop-up menu of the "Packet List" pane

Figure 6.4. Pop-up menu of the "Packet List" pane



The following table gives an overview of which functions are available in this pane, where to find the corresponding function in the main menu, and a short description of each item.

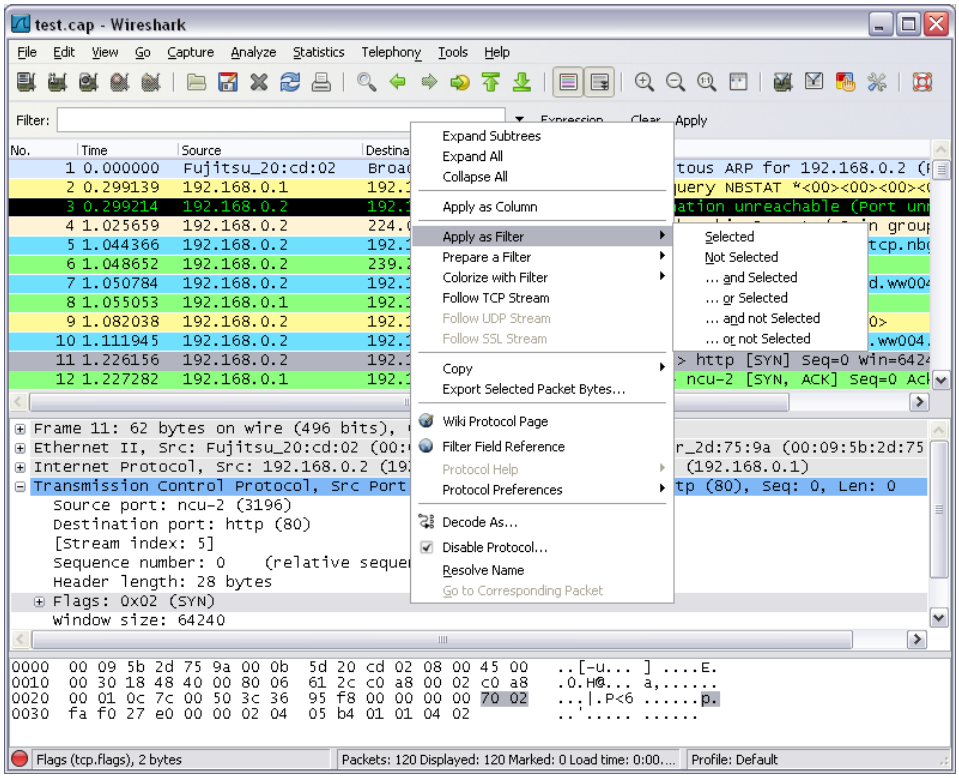
Table 6.2. The menu items of the "Packet List" pop-up menu

Item	Identical to main menu's item:	Description
Mark Packet (toggle)	Edit	Mark/unmark a packet.
Ignore Packet (toggle)	Edit	Ignore or inspect this packet while dissecting the capture file.
Set Time Reference (toggle)	Edit	Set/reset a time reference.

Item	Identical to main menu's item:	Description
Manually Resolve Address		Allows you to enter a name to resolve for the selected address.
Apply as Filter	Analyze	Prepare and apply a display filter based on the currently selected item.
Prepare a Filter	Analyze	Prepare a display filter based on the currently selected item.
Conversation Filter		This menu item applies a display filter with the address information from the selected packet. E.g. the IP menu entry will set a filter to show the traffic between the two IP addresses of the current packet. XXX - add a new section describing this better.
Colorize Conversation		This menu item uses a display filter with the address information from the selected packet to build a new colorizing rule.
SCTP		Allows you to analyze and prepare a filter for this SCTP association.
Follow TCP Stream	Analyze	Allows you to view all the data on a TCP stream between a pair of nodes.
Follow UDP Stream	Analyze	Allows you to view all the data on a UDP datagram stream between a pair of nodes.
Follow SSL Stream	Analyze	Same as "Follow TCP Stream" but for SSL. XXX - add a new section describing this better.
Copy/ Summary (Text)		Copy the summary fields as displayed to the clipboard, as tab-separated text.
Copy/ Summary (CSV)		Copy the summary fields as displayed to the clipboard, as comma-separated text.
Copy/ As Filter		Prepare a display filter based on the currently selected item and copy that filter to the clipboard.
Copy/ Bytes (Offset Hex Text)		Copy the packet bytes to the clipboard in hexdump-like format.
Copy/ Bytes (Offset Hex)		Copy the packet bytes to the clipboard in hexdump-like format, but without the text portion.
Copy/ Bytes (Printable Text Only)		Copy the packet bytes to the clipboard as ASCII text, excluding non-printable characters.
Copy/ Bytes (Hex Stream)		Copy the packet bytes to the clipboard as an unpunctuated list of hex digits.
Copy/ Bytes (Binary Stream)		Copy the packet bytes to the clipboard as raw binary. The data is stored in the clipboard as MIME-type "application/octet-stream".
Decode As…	Analyze	Change or apply a new relation between two dissectors.
Print…	File	Print packets.
Show Packet in New Window	View	Display the selected packet in a new window.

6.2.3. Pop-up menu of the “Packet Details” pane

Figure 6.5. Pop-up menu of the “Packet Details” pane



The following table gives an overview of which functions are available in this pane, where to find the corresponding function in the main menu, and a short description of each item.

Table 6.3. The menu items of the “Packet Details” pop-up menu

Item	Identical to main menu’s item:	Description
Expand Subtrees	View	Expand the currently selected subtree.
Collapse Subtrees	View	Collapse the currently selected subtree.
Expand All	View	Expand all subtrees in all packets in the capture.
Collapse All	View	Wireshark keeps a list of all the protocol subtrees that are expanded, and uses it to ensure that the correct subtrees are expanded when you display a packet. This menu item collapses the tree view of all packets in the capture list.
Apply as Column		Use the selected protocol item to create a new column in the packet list.
Apply as Filter	Analyze	Prepare and apply a display filter based on the currently selected item.
Prepare a Filter	Analyze	Prepare a display filter based on the currently selected item.

Item	Identical to main menu's item:	Description
Colorize with Filter		This menu item uses a display filter with the information from the selected protocol item to build a new colorizing rule.
Follow TCP Stream	Analyze	Allows you to view all the data on a TCP stream between a pair of nodes.
Follow UDP Stream	Analyze	Allows you to view all the data on a UDP datagram stream between a pair of nodes.
Follow SSL Stream	Analyze	Same as "Follow TCP Stream" but for SSL. XXX - add a new section describing this better.
Copy/ Description	Edit	Copy the displayed text of the selected field to the system clipboard.
Copy/ Fieldname	Edit	Copy the name of the selected field to the system clipboard.
Copy/ Value	Edit	Copy the value of the selected field to the system clipboard.
Copy/ As Filter	Edit	Prepare a display filter based on the currently selected item and copy it to the clipboard.
Copy/ Bytes (Offset Hex Text)		Copy the packet bytes to the clipboard in hexdump-like format; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane).
Copy/ Bytes (Offset Hex)		Copy the packet bytes to the clipboard in hexdump-like format, but without the text portion; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane).
Copy/ Bytes (Printable Text Only)		Copy the packet bytes to the clipboard as ASCII text, excluding non-printable characters; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane).
Copy/ Bytes (Hex Stream)		Copy the packet bytes to the clipboard as an unpunctuated list of hex digits; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane).
Copy/ Bytes (Binary Stream)		Copy the packet bytes to the clipboard as raw binary; similar to the Packet List Pane command, but copies only the bytes relevant to the selected part of the tree (the bytes selected in the Packet Bytes Pane). The data is stored in the clipboard as MIME-type "application/octet-stream".

Item	Identical to main menu's item:	Description
Export Selected Packet Bytes…	File	This menu item is the same as the File menu item of the same name. It allows you to export raw packet bytes to a binary file.
Wiki Protocol Page		Show the wiki page corresponding to the currently selected protocol in your web browser.
Filter Field Reference		Show the filter field reference web page corresponding to the currently selected protocol in your web browser.
Protocol Preferences…		The menu item takes you to the properties dialog and selects the page corresponding to the protocol if there are properties associated with the highlighted field. More information on preferences can be found in Figure 10.7, "The preferences dialog box".
Decode As…	Analyze	Change or apply a new relation between two dissectors.
Disable Protocol		Allows you to temporarily disable a protocol dissector, which may be blocking the legitimate dissector.
Resolve Name	View	Causes a name resolution to be performed for the selected packet, but NOT every packet in the capture.
Go to Corresponding Packet	Go	If the selected field has a corresponding packet, go to it. Corresponding packets will usually be a request/response packet pair or such.

6.3. Filtering packets while viewing

Wireshark has two filtering languages: One used when capturing packets, and one used when displaying packets. In this section we explore that second type of filter: Display filters. The first one has already been dealt with in Section 4.13, "Filtering while capturing".

Display filters allow you to concentrate on the packets you are interested in while hiding the currently uninteresting ones. They allow you to select packets by:

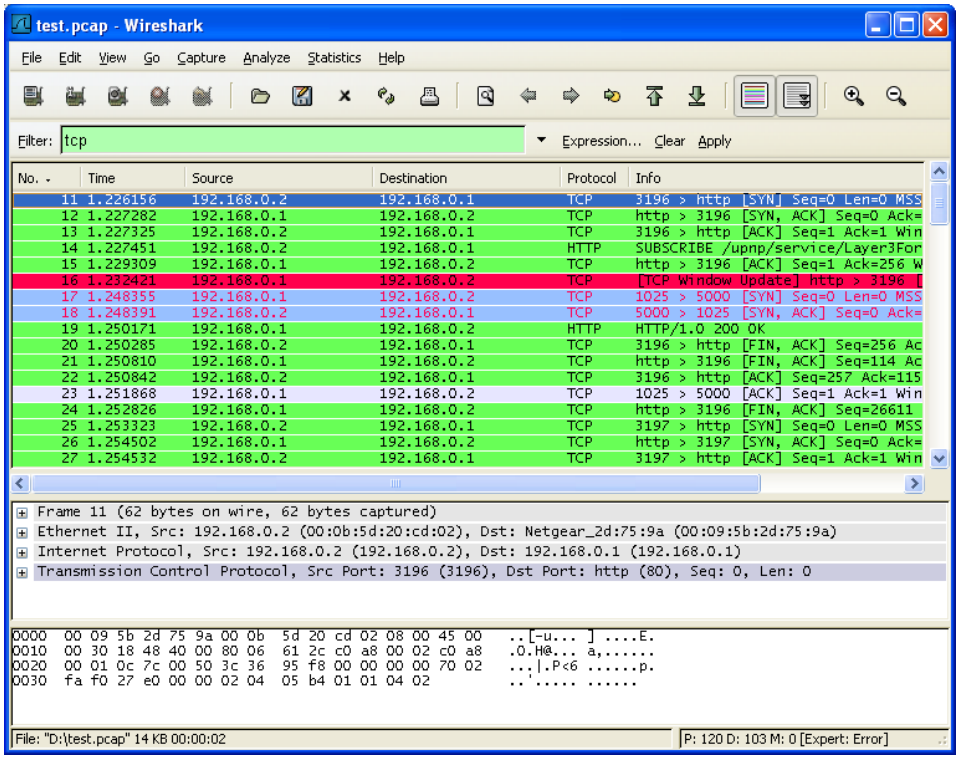
- Protocol
- The presence of a field
- The values of fields
- A comparison between fields
- … and a lot more!

To select packets based on protocol type, simply type the protocol in which you are interested in the *Filter:* field in the filter toolbar of the Wireshark window and press enter to initiate the filter. Figure 6.6, "Filtering on the TCP protocol" shows an example of what happens when you type *tcp* in the filter field.

Note

All protocol and field names are entered in lowercase. Also, don't forget to press enter after entering the filter expression.

Figure 6.6. Filtering on the TCP protocol



As you might have noticed, only packets of the TCP protocol are displayed now (e.g. packets 1-10 are hidden). The packet numbering will remain as before, so the first packet shown is now packet number 11.

Note

When using a display filter, all packets remain in the capture file. The display filter only changes the display of the capture file but not its content!

You can filter on any protocol that Wireshark understands. You can also filter on any field that a dissector adds to the tree view, but only if the dissector has added an abbreviation for the field. A list of such fields is available in Wireshark in the *Add Expression…* dialog box. You can find more information on the *Add Expression…* dialog box in Section 6.5, "The "Filter Expression" dialog box".

For example, to narrow the packet list pane down to only those packets to or from the IP address 192.168.0.1, use `ip.addr==192.168.0.1`.

Note

To remove the filter, click on the Clear button to the right of the filter field.

6.4. Building display filter expressions

Wireshark provides a simple but powerful display filter language that allows you to build quite complex filter expressions. You can compare values in packets as well as combine expressions into more specific expressions. The following sections provide more information on doing this.

Tip

You will find a lot of Display Filter examples at the *Wireshark Wiki Display Filter page* at: https://wiki.wireshark.org/DisplayFilters.

6.4.1. Display filter fields

Every field in the packet details pane can be used as a filter string, this will result in showing only the packets where this field exists. For example: the filter string: *tcp* will show all packets containing the tcp protocol.

There is a complete list of all filter fields available through the menu item Help → Supported Protocols in the page “Display Filter Fields” of the “Supported Protocols” dialog.

6.4.2. Comparing values

You can build display filters that compare values using a number of different comparison operators. They are shown in Table 6.4, “Display Filter comparison operators”.

Tip

You can use English and C-like terms in the same way, they can even be mixed in a filter string.

Table 6.4. Display Filter comparison operators

English	C-like	Description and example
eq	==	Equal. `ip.src==10.0.0.5`
ne	!=	Not equal. `ip.src!=10.0.0.5`
gt	>	Greater than. `frame.len > 10`
lt	<	Less than. `frame.len < 128`
ge	>=	Greater than or equal to. `frame.len ge 0x100`
le	<=	Less than or equal to. `frame.len <= 0x20`

In addition, all protocol fields have a type. Display Filter Field Types provides a list of the types and example of how to express them.

Display Filter Field Types

Unsigned integer

Can be 8, 16, 24, 32, or 64 bits. You can express integers in decimal, octal, or hexadecimal. The following display filters are equivalent:

```
ip.len le 1500
```

```
ip.len le 02734

ip.len le 0x436
```

Signed integer
: Can be 8, 16, 24, 32, or 64 bits. As with unsigned integers you can use decimal, octal, or hexadecimal.

Boolean
: A boolean field is present in the protocol decode only if its value is true. For example, `tcp.flags.syn` is present, and thus true, only if the SYN flag is present in a TCP segment header.

```
The filter expression  +tcp.flags.syn+ will select only  those packets for which
this flag exists, that is,  TCP segments where the segment header contains the
SYN flag. Similarly, to find source-routed token ring packets, use a filter
expression of  +tr.sr+.
```

Ethernet address
: 6 bytes separated by a colon (:), dot (.) or dash (-) with one or two bytes between separators:

```
eth.dst == ff:ff:ff:ff:ff:ff

eth.dst == ff-ff-ff-ff-ff-ff

eth.dst == ffff.ffff.ffff
```

IPv4 address
: ip.addr == 192.168.0.1

```
Classless InterDomain Routing (CIDR) notation can be used to test if
an IPv4 address is in a certain subnet. For example, this display
filter will find all packets in the 129.111 Class-B network:

ip.addr == 129.111.0.0/16
```

IPv6 address
: `ipv6.addr == ::1`

```
As with IPv4 addresses, IPv6 addresses can match a subnet.
```

Text string
: `http.request.uri == "https://www.wireshark.org/"`

6.4.3. Combining expressions

You can combine filter expressions in Wireshark using the logical operators shown in Table 6.5, “Display Filter Logical Operations”

Table 6.5. Display Filter Logical Operations

English	C-like	Description and example
and	&&	Logical AND. `ip.src==10.0.0.5 and tcp.flags.fin`
or	||	Logical OR. `ip.scr==10.0.0.5 or ip.src==192.1.1.1`
xor	^^	Logical XOR. `tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29`
not	!	Logical NOT. `not llc`
[…]		See “Substring Operator” below.

English	C-like	Description and example
in		See “Membership Operator” below.

6.4.4. Substring Operator

Wireshark allows you to select subsequences of a sequence in rather elaborate ways. After a label you can place a pair of brackets [] containing a comma separated list of range specifiers.

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

The example above uses the n:m format to specify a single range. In this case n is the beginning offset and m is the length of the range being specified.

```
eth.src[1-2] == 00:83
```

The example above uses the n-m format to specify a single range. In this case n is the beginning offset and m is the ending offset.

```
eth.src[:4] == 00:00:83:00
```

The example above uses the :m format, which takes everything from the beginning of a sequence to offset m. It is equivalent to 0:m

```
eth.src[4:] == 20:20
```

The example above uses the n: format, which takes everything from offset n to the end of the sequence.

```
eth.src[2] == 83
```

The example above uses the n format to specify a single range. In this case the element in the sequence at offset n is selected. This is equivalent to n:1.

```
eth.src[0:3,1-2,:4,4:,2] ==
00:00:83:00:83:00:00:83:00:20:20:83
```

Wireshark allows you to string together single ranges in a comma separated list to form compound ranges as shown above.

6.4.5. Membership Operator.

Wireshark allows you to test a field for membership in a set of values or fields. After the field name, use the in operator followed by the set items surrounded by braces {}.

```
tcp.port in {80 443 8080}
```

This can be considered a shortcut operator, as the previous expression could have been expressed as:

```
tcp.port == 80 || tcp.port == 443 || tcp.port == 8080
```

6.4.6. A Common Mistake

Using the != operator on combined expressions like eth.addr, ip.addr, tcp.port, and udp.port will probably not work as expected.

Often people use a filter string to display something like `ip.addr == 1.2.3.4` which will display all packets containing the IP address 1.2.3.4.

Then they use `ip.addr != 1.2.3.4` to see all packets not containing the IP address 1.2.3.4 in it. Unfortunately, this does *not* do the expected.

Instead, that expression will even be true for packets where either source or destination IP address equals 1.2.3.4. The reason for this, is that the expression `ip.addr != 1.2.3.4` must be read as “the packet contains a field named ip.addr with a value different from 1.2.3.4”. As an IP datagram contains both a source and a destination address, the expression will evaluate to true whenever at least one of the two addresses differs from 1.2.3.4.

If you want to filter out all packets containing IP datagrams to or from IP address 1.2.3.4, then the correct filter is `!(ip.addr == 1.2.3.4)` as it reads “show me all the packets for which it is not true that a field named ip.addr exists with a value of 1.2.3.4”, or in other words, “filter out all packets for which there are no occurrences of a field named ip.addr with the value 1.2.3.4”.

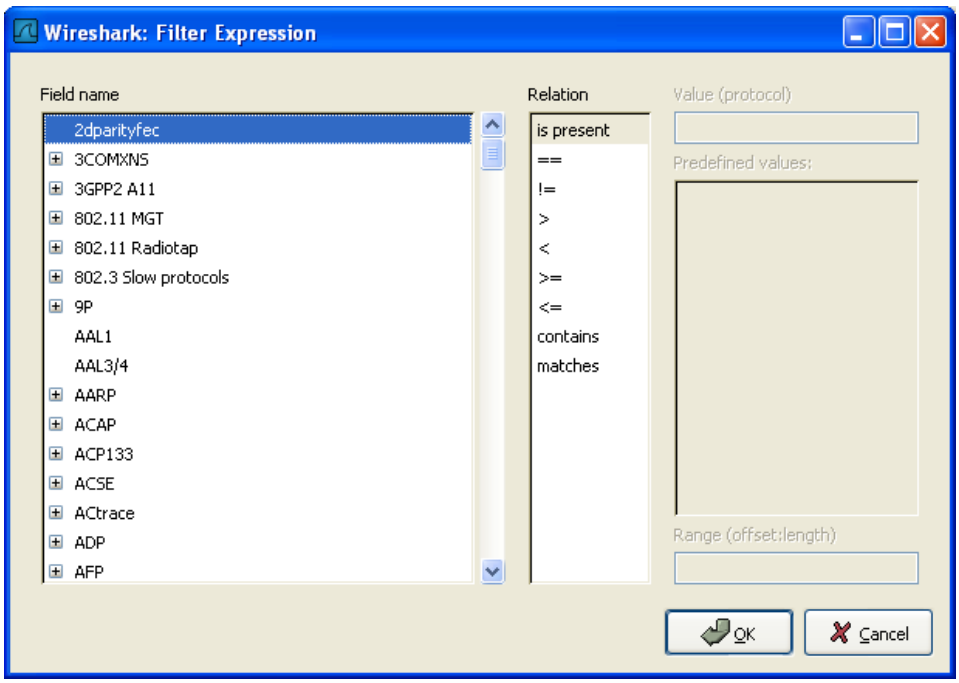
6.5. The “Filter Expression” dialog box

When you are accustomed to Wireshark’s filtering system and know what labels you wish to use in your filters it can be very quick to simply type a filter string. However if you are new to Wireshark or are working with a slightly unfamiliar protocol it can be very confusing to try to figure out what to type. The “Filter Expression” dialog box helps with this.

Tip

The “Filter Expression” dialog box is an excellent way to learn how to write Wireshark display filter strings.

Figure 6.7. The “Filter Expression” dialog box



When you first bring up the Filter Expression dialog box you are shown a tree of field names, organized by protocol, and a box for selecting a relation.

Field Name

Select a protocol field from the protocol field tree. Every protocol with filterable fields is listed at the top level. (You can search for a particular protocol entry by entering the first few letters of the

protocol name). By expanding a protocol name you can get a list of the field names available for filtering for that protocol.

Relation
Select a relation from the list of available relation. The *is present* is a unary relation which is true if the selected field is present in a packet. All other listed relations are binary relations which require additional data (e.g. a *Value* to match) to complete.

When you select a field from the field name list and select a binary relation (such as the equality relation ==) you will be given the opportunity to enter a value, and possibly some range information.

Value
You may enter an appropriate value in the *Value* text box. The *Value* will also indicate the type of value for the *field name* you have selected (like character string).

Predefined values
Some of the protocol fields have predefined values available, much like enum's in C. If the selected protocol field has such values defined, you can choose one of them here.

Range
A range of integers or a group of ranges, such as `1-12` or `39-42,98-2000`.

OK
When you have built a satisfactory expression click OK and a filter string will be built for you.

Cancel
You can leave the "Add Expression…" dialog box without any effect by clicking the Cancel button.

6.6. Defining and saving filters

You can define filters with Wireshark and give them labels for later use. This can save time in remembering and retyping some of the more complex filters you use.

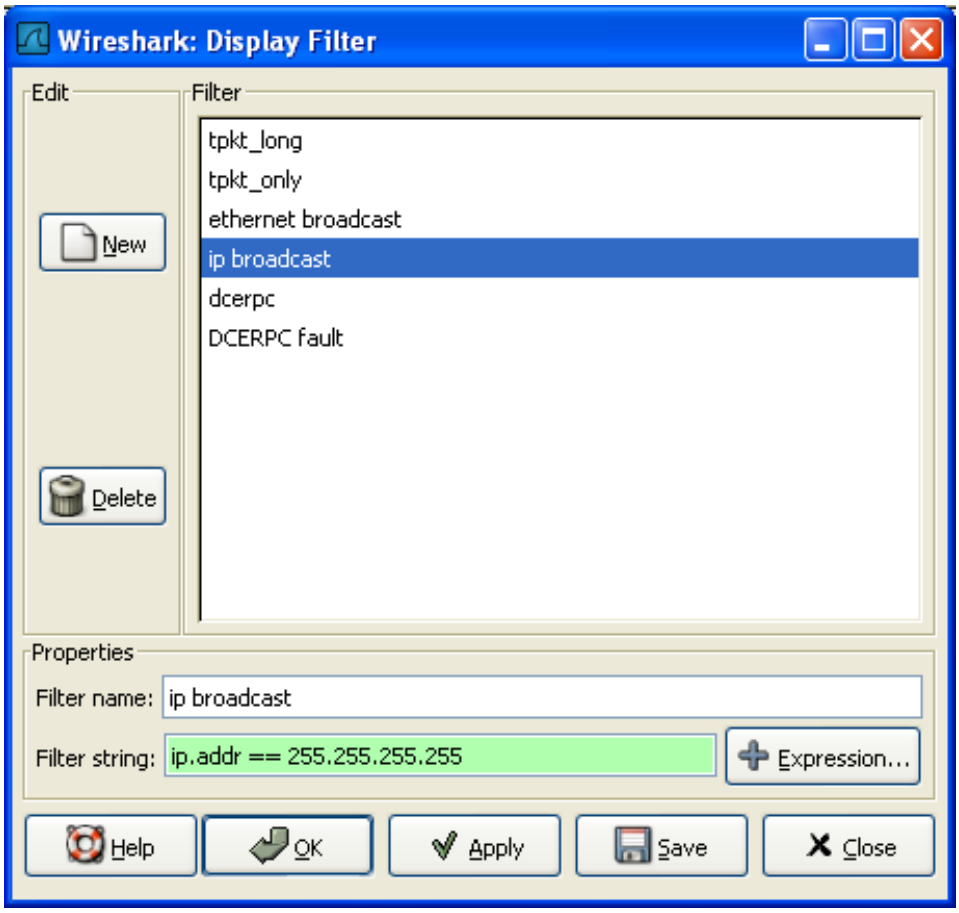
To define a new filter or edit an existing one, select Capture → Capture Filters… or Analyze → Display Filters…. Wireshark will then pop up the Filters dialog as shown in Figure 6.8, "The "Capture Filters" and "Display Filters" dialog boxes".

The mechanisms for defining and saving capture filters and display filters are almost identical. Both will be described here but the differences between these two will be marked as such.

Warning

You must use Save to save your filters permanently. OK or Apply will not save the filters and they will be lost when you close Wireshark.

Figure 6.8. The “Capture Filters” and “Display Filters” dialog boxes



New
: This button adds a new filter to the list of filters. The currently entered values from Filter name and Filter string will be used. If any of these fields are empty, it will be set to “new”.

Delete
: This button deletes the selected filter. It will be greyed out, if no filter is selected.

Filter
: You can select a filter from this list (which will fill in the filter name and filter string in the fields down at the bottom of the dialog box).

Filter name:
: You can change the name of the currently selected filter here.

  The filter name will only be used in this dialog to identify the filter for your convenience, it will not be used elsewhere. You can add multiple filters with the same name, but this is not very useful.

Filter string:
: You can change the filter string of the currently selected filter here. Display Filter only: the string will be syntax checked while you are typing.

Add Expression…
: Display Filter only: This button brings up the Add Expression dialog box which assists in building filter strings. You can find more information about the Add Expression dialog in Section 6.5, “The “Filter Expression” dialog box”

OK
Display Filter only: This button applies the selected filter to the current display and closes the dialog.

Apply
Display Filter only: This button applies the selected filter to the current display, and keeps the dialog open.

Save
Save the current settings in this dialog. The file location and format is explained in Appendix B, *Files and Folders*.

Close
Close this dialog. This will discard unsaved settings.

6.7. Defining and saving filter macros

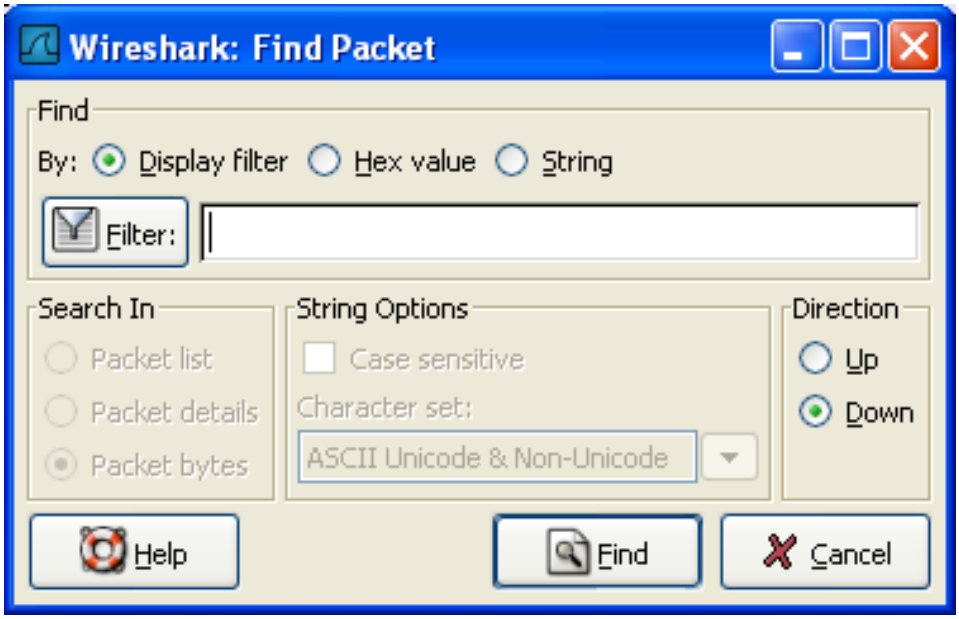
You can define filter macros with Wireshark and give them labels for later use. This can save time in remembering and retyping some of the more complex filters you use.

6.8. Finding packets

You can easily find packets once you have captured some packets or have read in a previously saved capture file. Simply select the *Find Packet…* menu item from the *Edit* menu. Wireshark will pop up the dialog box shown in Figure 6.9, “The “Find Packet” dialog box”.

6.8.1. The “Find Packet” dialog box

Figure 6.9. The “Find Packet” dialog box



You might first select the kind of thing to search for:

- *Display filter*

Simply enter a display filter string into the *Filter:* field, select a direction, and click on OK.

For example, to find the three way handshake for a connection from host 192.168.0.1, use the following filter string:

```
ip.src==192.168.0.1 and tcp.flags.syn==1
```

For more details on display filters, see Section 6.3, “Filtering packets while viewing”

- *Hex Value*

  Search for a specific byte sequence in the packet data.

  For example, use “00:00” to find the next packet including two null bytes in the packet data.

- *String*

  Find a string in the packet data, with various options.

  The value to be found will be syntax checked while you type it in. If the syntax check of your value succeeds, the background of the entry field will turn green, if it fails, it will turn red.

You can choose the search direction:

- *Up*

  Search upwards in the packet list (decreasing packet numbers).

- *Down*

  Search downwards in the packet list (increasing packet numbers).

6.8.2. The “Find Next” command

“Find Next” will continue searching with the same options used in the last “Find Packet”.

6.8.3. The “Find Previous” command

“Find Previous” will do the same thing as “Find Next”, but in the reverse direction.

6.9. Go to a specific packet

You can easily jump to specific packets with one of the menu items in the Go menu.

6.9.1. The “Go Back” command

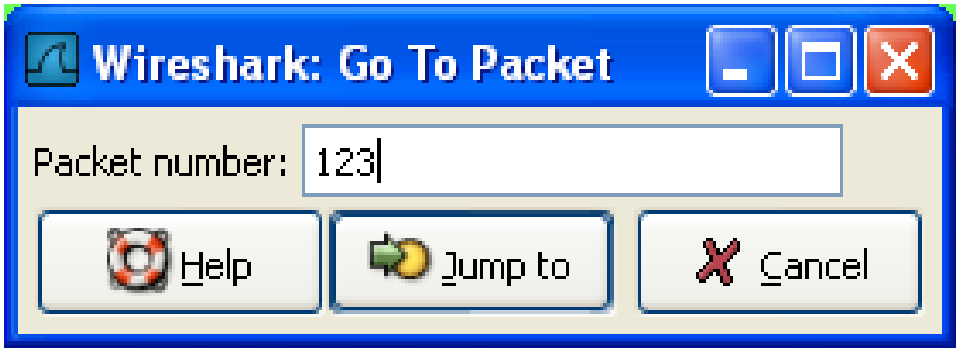
Go back in the packet history, works much like the page history in current web browsers.

6.9.2. The “Go Forward” command

Go forward in the packet history, works much like the page history in current web browsers.

6.9.3. The “Go to Packet” dialog box

Figure 6.10. The “Go To Packet” dialog box



This dialog box will let you enter a packet number. When you press OK, Wireshark will jump to that packet.

6.9.4. The “Go to Corresponding Packet” command

If a protocol field is selected which points to another packet in the capture file, this command will jump to that packet.

As these protocol fields now work like links (just as in your Web browser), it’s easier to simply double-click on the field to jump to the corresponding field.

6.9.5. The “Go to First Packet” command

This command will simply jump to the first packet displayed.

6.9.6. The “Go to Last Packet” command

This command will simply jump to the last packet displayed.

6.10. Marking packets

You can mark packets in the “Packet List” pane. A marked packet will be shown with black background, regardless of the coloring rules set. Marking a packet can be useful to find it later while analyzing in a large capture file.

The packet marks are not stored in the capture file or anywhere else. All packet marks will be lost when you close the capture file.

You can use packet marking to control the output of packets when saving, exporting, or printing. To do so, an option in the packet range is available, see Section 5.9, “The “Packet Range” frame”.

There are three functions to manipulate the marked state of a packet:

- *Mark packet (toggle)* toggles the marked state of a single packet.
- *Mark all displayed packets* set the mark state of all displayed packets.
- *Unmark all packets* reset the mark state of all packets.

These mark functions are available from the “Edit” menu, and the “Mark packet (toggle)” function is also available from the pop-up menu of the “Packet List” pane.

6.11. Ignoring packets

You can ignore packets in the “Packet List” pane. Wireshark will then pretend that this packets does not exist in the capture file. An ignored packet will be shown with white background and gray foreground, regardless of the coloring rules set.

The packet ignored marks are not stored in the capture file or anywhere else. All “packet ignored” marks will be lost when you close the capture file.

There are three functions to manipulate the ignored state of a packet:

- *Ignore packet (toggle)* toggles the ignored state of a single packet.
- *Ignore all displayed packets* set the ignored state of all displayed packets.
- *Un-Ignore all packets* reset the ignored state of all packets.

These ignore functions are available from the “Edit” menu, and the “Ignore packet (toggle)” function is also available from the pop-up menu of the “Packet List” pane.

6.12. Time display formats and time references

While packets are captured, each packet is timestamped. These timestamps will be saved to the capture file, so they will be available for later analysis.

A detailed description of timestamps, timezones and alike can be found at: Section 7.5, “Time Stamps”.

The timestamp presentation format and the precision in the packet list can be chosen using the View menu, see Figure 3.5, “The “View” Menu”.

The available presentation formats are:

- *Date and Time of Day: 1970-01-01 01:02:03.123456* The absolute date and time of the day when the packet was captured.
- *Time of Day: 01:02:03.123456* The absolute time of the day when the packet was captured.
- *Seconds Since Beginning of Capture: 123.123456* The time relative to the start of the capture file or the first “Time Reference” before this packet (see Section 6.12.1, “Packet time referencing”).
- *Seconds Since Previous Captured Packet: 1.123456* The time relative to the previous captured packet.
- *Seconds Since Previous Displayed Packet: 1.123456* The time relative to the previous displayed packet.
- *Seconds Since Epoch (1970-01-01): 1234567890.123456* The time relative to epoch (midnight UTC of January 1, 1970).

The available precisions (aka. the number of displayed decimal places) are:

- *Automatic* The timestamp precision of the loaded capture file format will be used (the default).
- *Seconds, Deciseconds, Centiseconds, Milliseconds, Microseconds or Nanoseconds* The timestamp precision will be forced to the given setting. If the actually available precision is smaller, zeros will be appended. If the precision is larger, the remaining decimal places will be cut off.

Precision example: If you have a timestamp and it's displayed using, "Seconds Since Previous Packet", : the value might be 1.123456. This will be displayed using the "Automatic" setting for libpcap files (which is microseconds). If you use Seconds it would show simply 1 and if you use Nanoseconds it shows 1.123456000.

6.12.1. Packet time referencing

The user can set time references to packets. A time reference is the starting point for all subsequent packet time calculations. It will be useful, if you want to see the time values relative to a special packet, e.g. the start of a new request. It's possible to set multiple time references in the capture file.

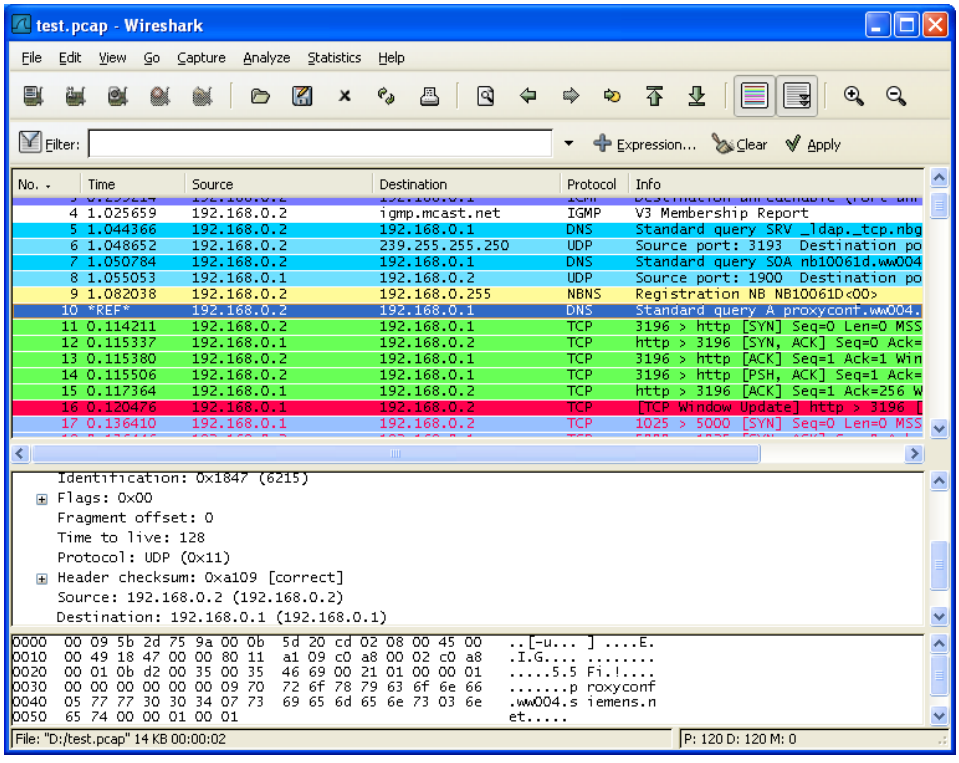
The time references will not be saved permanently and will be lost when you close the capture file.

Time referencing will only be useful if the time display format is set to "Seconds Since Beginning of Capture". If one of the other time display formats are used, time referencing will have no effect (and will make no sense either).

To work with time references, choose one of the Time Reference items in the Edit menu or from the pop-up menu of the "Packet List" pane. See Section 3.6, "The "Edit" menu".

- *Set Time Reference (toggle)* Toggles the time reference state of the currently selected packet to on or off.
- *Find Next* Find the next time referenced packet in the "Packet List" pane.
- *Find Previous* Find the previous time referenced packet in the "Packet List" pane.

Figure 6.11. Wireshark showing a time referenced packet



A time referenced packet will be marked with the string *REF* in the Time column (see packet number 10). All subsequent packets will show the time since the last time reference.

Chapter 7. Advanced Topics

7.1. Introduction

This chapter some of Wireshark's advanced features.

7.2. Following TCP streams

If you are working with TCP based protocols it can be very helpful to see the data from a TCP stream in the way that the application layer sees it. Perhaps you are looking for passwords in a Telnet stream, or you are trying to make sense of a data stream. Maybe you just need a display filter to show only the packets of that TCP stream. If so, Wireshark's ability to follow a TCP stream will be useful to you.

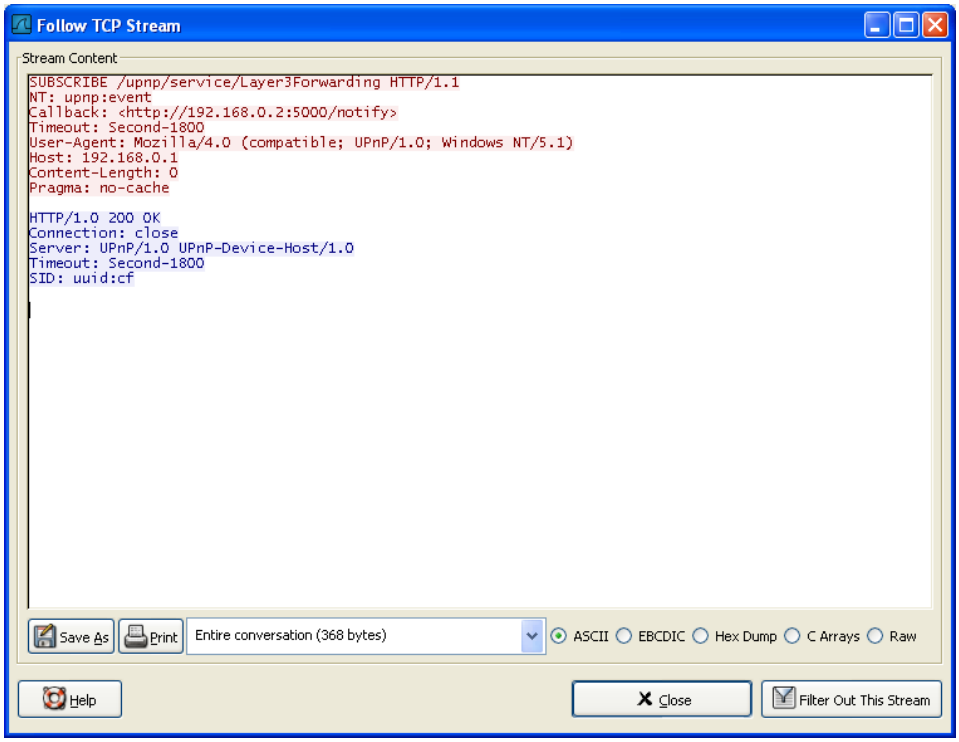
Simply select a TCP packet in the packet list of the stream/connection you are interested in and then select the Follow TCP Stream menu item from the Wireshark Tools menu (or use the context menu in the packet list). Wireshark will set an appropriate display filter and pop up a dialog box with all the data from the TCP stream laid out in order, as shown in Figure 7.1, "The "Follow TCP Stream" dialog box".

Note

Opening the "Follow TCP Stream" installs a display filter to select all the packets in the TCP stream you have selected.

7.2.1. The "Follow TCP Stream" dialog box

Figure 7.1. The "Follow TCP Stream" dialog box



The stream content is displayed in the same sequence as it appeared on the network. Traffic from A to B is marked in red, while traffic from B to A is marked in blue. If you like, you can change these colors in the “Colors” page if the “Preferences” dialog.

Non-printable characters will be replaced by dots.

The stream content won’t be updated while doing a live capture. To get the latest content you’ll have to reopen the dialog.

You can choose from the following actions:

1. *Save As*: Save the stream data in the currently selected format.

2. *Print*: Print the stream data in the currently selected format.

3. *Direction*: Choose the stream direction to be displayed (“Entire conversation”, “data from A to B only” or “data from B to A only”).

4. *Filter out this stream*: Apply a display filter removing the current TCP stream data from the display.

5. *Close*: Close this dialog box, leaving the current display filter in effect.

You can choose to view the data in one of the following formats:

1. *ASCII*: In this view you see the data from each direction in ASCII. Obviously best for ASCII based protocols, e.g. HTTP.

2. *EBCDIC*: For the big-iron freaks out there.

3. *HEX Dump*: This allows you to see all the data. This will require a lot of screen space and is best used with binary protocols.

4. *C Arrays*: This allows you to import the stream data into your own C program.

5. *Raw*: This allows you to load the unaltered stream data into a different program for further examination. The display will look the same as the ASCII setting, but “Save As” will result in a binary file.

7.3. Show Packet Bytes

If a selected packet field does not show all the bytes (i.e. they are truncated when displayed) or if they are shown as bytes rather than string or if they require more formatting because they contain an image or HTML then this dialog can be used.

This dialog can also be used to decode field bytes from base64, zlib compressed or quoted-printable and show the decoded bytes as configurable output. It’s also possible to select a subset of bytes setting the start byte and end byte.

You can choose from the following actions:

1. *Find*: Search for the given text. Matching text will be highlighted, and the “Find Next” will search for more. In the context menu for the find text it’s possible to configure to use regular expression find.

2. *Print*: Print the bytes in the currently selected format.

3. *Copy*: Copy the bytes to the clipboard in the currently selected format.

4. *Save As*: Save the bytes in the currently selected format.

5. *Close*: Close this dialog box.

7.3.1. Decode as

You can choose to decode the data from one of the following formats:

1. *None*: This is the default which does not decode anything.

2. *Base64*: This will decode from Base64.

3. *Compressed*: This will decompress the buffer using zlib.

4. *Quoted-Printable*: This will decode from a Quoted-Printable string.

7.3.2. Show as

You can choose to view the data in one of the following formats:

ASCII	In this view you see the bytes as ASCII. All control characters and non-ASCII bytes are replaced by dot.
ASCII & Control	In this view all control characters are shown using a UTF-8 symbol and all non-ASCII bytes are replaced by dot.
C Array	This allows you to import the field data into your own C program.
EBCDIC	For the big-iron freaks out there.
HEX Dump	This allows you to see all the data. This will require a lot of screen space and is best used with binary protocols.
HTML	This allows you to see all the data formatted as a HTML document. The HTML supported is what's supported by the Qt QTextEdit class.
Image	This will try to convert the bytes into an image. Images supported are what's supported by the Qt QImage class.
ISO 8859-1	In this view you see the bytes as ISO 8859-1.
Raw	This allows you to load the unaltered stream data into a different program for further examination. The display will show HEX data, but "Save As" will result in a binary file.
UTF8	In this view you see the bytes as UTF-8.
YAML	This will show the bytes as a YAML binary dump.

7.4. Expert Information

The expert infos is a kind of log of the anomalies found by Wireshark in a capture file.

The general idea behind the following "Expert Info" is to have a better display of "uncommon" or just notable network behaviour. This way, both novice and expert users will hopefully find probable network problems a lot faster, compared to scanning the packet list "manually" .

Expert infos are only a hint

Take expert infos as a hint what's worth looking at, but not more. For example, the absence of expert infos doesn't necessarily mean everything is OK.

The amount of expert infos largely depends on the protocol being used. While some common protocols like TCP/IP will show detailed expert infos, most other protocols currently won't show any expert infos at all.

The following will first describe the components of a single expert info, then the User Interface.

7.4.1. Expert Info Entries

Each expert info will contain the following things which will be described in detail below.

Table 7.1. Some example expert infos

Packet #	Severity	Group	Protocol	Summary
1	Note	Sequence	TCP	Duplicate ACK (#1)
2	Chat	Sequence	TCP	Connection reset (RST)
8	Note	Sequence	TCP	Keep-Alive
9	Warn	Sequence	TCP	Fast retransmission (suspected)

7.4.1.1. Severity

Every expert info has a specific severity level. The following severity levels are used, in parentheses are the colors in which the items will be marked in the GUI:

- *Chat (grey)*: information about usual workflow, e.g. a TCP packet with the SYN flag set
- *Note (cyan)*: notable things, e.g. an application returned an "usual" error code like HTTP 404
- *Warn (yellow)*: warning, e.g. application returned an "unusual" error code like a connection problem
- *Error (red)*: serious problem, e.g. [Malformed Packet]

7.4.1.2. Group

There are some common groups of expert infos. The following are currently implemented:

- *Checksum*: a checksum was invalid
- *Sequence*: protocol sequence suspicious, e.g. sequence wasn't continuous or a retransmission was detected or …
- *Response Code*: problem with application response code, e.g. HTTP 404 page not found
- *Request Code*: an application request (e.g. File Handle == x), usually Chat level
- *Undecoded*: dissector incomplete or data can't be decoded for other reasons
- *Reassemble*: problems while reassembling, e.g. not all fragments were available or an exception happened while reassembling
- *Protocol*: violation of protocol specs (e.g. invalid field values or illegal lengths), dissection of this packet is probably continued

- *Malformed*: malformed packet or dissector has a bug, dissection of this packet aborted
- *Debug*: debugging (should not occur in release versions)

It's possible that more groups will be added in the future.

7.4.1.3. Protocol

The protocol in which the expert info was caused.

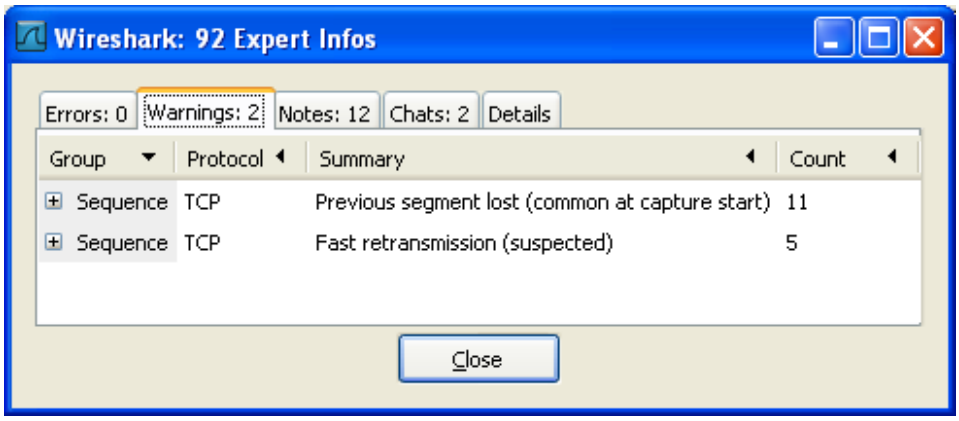
7.4.1.4. Summary

Each expert info will also have a short additional text with some further explanation.

7.4.2. "Expert Info" dialog

You can open the expert info dialog by selecting Analyze → Expert Info.

Figure 7.2. The "Expert Info" dialog box



7.4.2.1. Errors / Warnings / Notes / Chats tabs

An easy and quick way to find the most interesting infos (rather than using the Details tab), is to have a look at the separate tabs for each severity level. As the tab label also contains the number of existing entries, it's easy to find the tab with the most important entries.

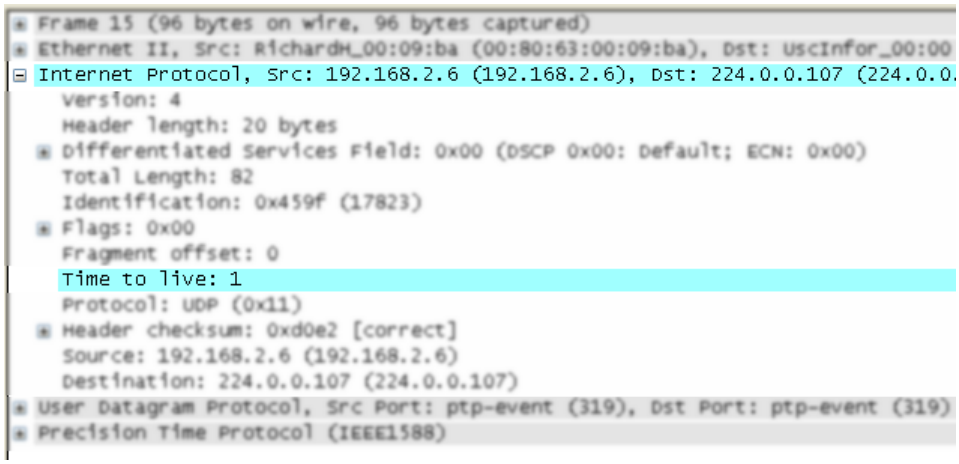
There are usually a lot of identical expert infos only differing in the packet number. These identical infos will be combined into a single line - with a count column showing how often they appeared in the capture file. Clicking on the plus sign shows the individual packet numbers in a tree view.

7.4.2.2. Details tab

The Details tab provides the expert infos in a "log like" view, each entry on its own line (much like the packet list). As the amount of expert infos for a capture file can easily become very large, getting an idea of the interesting infos with this view can take quite a while. The advantage of this tab is to have all entries in the sequence as they appeared, this is sometimes a help to pinpoint problems.

7.4.3. “Colorized” Protocol Details Tree

Figure 7.3. The “Colorized” protocol details tree

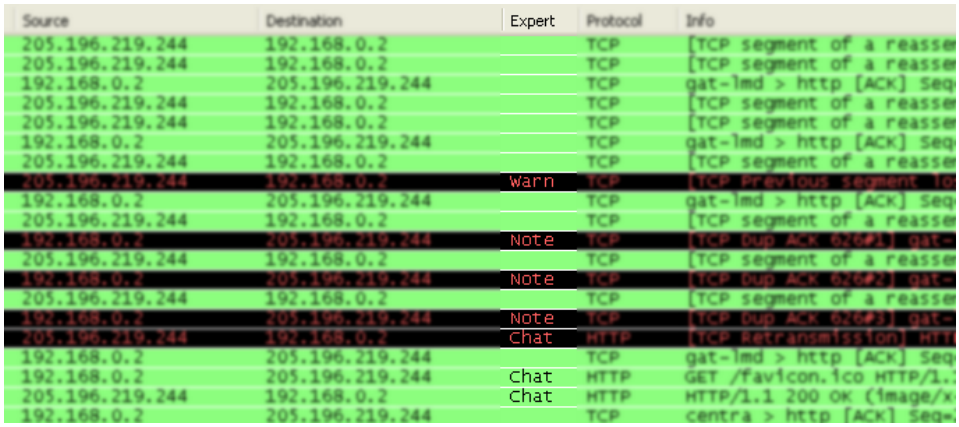


The protocol field causing an expert info is colorized, e.g. uses a cyan background for a note severity level. This color is propagated to the toplevel protocol item in the tree, so it’s easy to find the field that caused the expert info.

For the example screenshot above, the IP “Time to live” value is very low (only 1), so the corresponding protocol field is marked with a cyan background. To easier find that item in the packet tree, the IP protocol toplevel item is marked cyan as well.

7.4.4. “Expert” Packet List Column (optional)

Figure 7.4. The “Expert” packet list column



An optional “Expert Info Severity” packet list column is available that displays the most significant severity of a packet or stays empty if everything seems OK. This column is not displayed by default but can be easily added using the Preferences Columns page described in Section 10.5, “Preferences”.

7.5. Time Stamps

Time stamps, their precisions and all that can be quite confusing. This section will provide you with information about what’s going on while Wireshark processes time stamps.

While packets are captured, each packet is time stamped as it comes in. These time stamps will be saved to the capture file, so they also will be available for (later) analysis.

So where do these time stamps come from? While capturing, Wireshark gets the time stamps from the libpcap (WinPcap) library, which in turn gets them from the operating system kernel. If the capture data is loaded from a capture file, Wireshark obviously gets the data from that file.

7.5.1. Wireshark internals

The internal format that Wireshark uses to keep a packet time stamp consists of the date (in days since 1.1.1970) and the time of day (in nanoseconds since midnight). You can adjust the way Wireshark displays the time stamp data in the packet list, see the “Time Display Format” item in the Section 3.7, “The “View” menu” for details.

While reading or writing capture files, Wireshark converts the time stamp data between the capture file format and the internal format as required.

While capturing, Wireshark uses the libpcap (WinPcap) capture library which supports microsecond resolution. Unless you are working with specialized capturing hardware, this resolution should be adequate.

7.5.2. Capture file formats

Every capture file format that Wireshark knows supports time stamps. The time stamp precision supported by a specific capture file format differs widely and varies from one second “0” to one nanosecond “0.123456789”. Most file formats store the time stamps with a fixed precision (e.g. microseconds), while some file formats are even capable of storing the time stamp precision itself (whatever the benefit may be).

The common libpcap capture file format that is used by Wireshark (and a lot of other tools) supports a fixed microsecond resolution “0.123456” only.

Writing data into a capture file format that doesn’t provide the capability to store the actual precision will lead to loss of information. For example, if you load a capture file with nanosecond resolution and store the capture data in a libpcap file (with microsecond resolution) Wireshark obviously must reduce the precision from nanosecond to microsecond.

7.5.3. Accuracy

People often ask “Which time stamp accuracy is provided by Wireshark?”. Well, Wireshark doesn’t create any time stamps itself but simply gets them from “somewhere else” and displays them. So accuracy will depend on the capture system (operating system, performance, etc) that you use. Because of this, the above question is difficult to answer in a general way.

Note

USB connected network adapters often provide a very bad time stamp accuracy. The incoming packets have to take “a long and winding road” to travel through the USB cable until they actually reach the kernel. As the incoming packets are time stamped when they are processed by the kernel, this time stamping mechanism becomes very inaccurate.

Don’t use USB connected NICs when you need precise time stamp accuracy.

7.6. Time Zones

If you travel across the planet, time zones can be confusing. If you get a capture file from somewhere around the world time zones can even be a lot more confusing ;-)

First of all, there are two reasons why you may not need to think about time zones at all:

- You are only interested in the time differences between the packet time stamps and don't need to know the exact date and time of the captured packets (which is often the case).
- You don't get capture files from different time zones than your own, so there are simply no time zone problems. For example, everyone in your team is working in the same time zone as yourself.

What are time zones?

People expect that the time reflects the sunset. Dawn should be in the morning maybe around 06:00 and dusk in the evening maybe at 20:00. These times will obviously vary depending on the season. It would be very confusing if everyone on earth would use the same global time as this would correspond to the sunset only at a small part of the world.

For that reason, the earth is split into several different time zones, each zone with a local time that corresponds to the local sunset.

The time zone's base time is UTC (Coordinated Universal Time) or Zulu Time (military and aviation). The older term GMT (Greenwich Mean Time) shouldn't be used as it is slightly incorrect (up to 0.9 seconds difference to UTC). The UTC base time equals to 0 (based at Greenwich, England) and all time zones have an offset to UTC between -12 to +14 hours!

For example: If you live in Berlin you are in a time zone one hour earlier than UTC, so you are in time zone "+1" (time difference in hours compared to UTC). If it's 3 o'clock in Berlin it's 2 o'clock in UTC "at the same moment".

Be aware that at a few places on earth don't use time zones with even hour offsets (e.g. New Delhi uses UTC+05:30)!

Further information can be found at: https://en.wikipedia.org/wiki/Time_zone and https://en.wikipedia.org/wiki/Coordinated_Universal_Time.

What is daylight saving time (DST)?

Daylight Saving Time (DST), also known as Summer Time is intended to "save" some daylight during the summer months. To do this, a lot of countries (but not all!) add a DST hour to the already existing UTC offset. So you may need to take another hour (or in very rare cases even two hours!) difference into your "time zone calculations".

Unfortunately, the date at which DST actually takes effect is different throughout the world. You may also note, that the northern and southern hemispheres have opposite DST's (e.g. while it's summer in Europe it's winter in Australia).

Keep in mind: UTC remains the same all year around, regardless of DST!

Further information can be found at https://en.wikipedia.org/wiki/Daylight_saving.

Further time zone and DST information can be found at http://wwp.greenwichmeantime.com/ and http://www.timeanddate.com/worldclock/.

7.6.1. Set your computer's time correctly!

If you work with people around the world it's very helpful to set your computer's time and time zone right.

You should set your computers time and time zone in the correct sequence:

1. Set your time zone to your current location
2. Set your computer's clock to the local time

This way you will tell your computer both the local time and also the time offset to UTC. Many organizations simply set the time zone on their servers and networking gear to UTC in order to make coordination and troubleshooting easier.

Tip

If you travel around the world, it's an often made mistake to adjust the hours of your computer clock to the local time. Don't adjust the hours but your time zone setting instead! For your computer, the time is essentially the same as before, you are simply in a different time zone with a different local time.

You can use the Network Time Protocol (NTP) to automatically adjust your computer to the correct time, by synchronizing it to Internet NTP clock servers. NTP clients are available for all operating systems that Wireshark supports (and for a lot more), for examples see: http://www.ntp.org/.

7.6.2. Wireshark and Time Zones

So what's the relationship between Wireshark and time zones anyway?

Wireshark's native capture file format (libpcap format), and some other capture file formats, such as the Windows Sniffer, EtherPeek, AiroPeek, and Sun snoop formats, save the arrival time of packets as UTC values. UN*X systems, and "Windows NT based" systems represent time internally as UTC. When Wireshark is capturing, no conversion is necessary. However, if the system time zone is not set correctly, the system's UTC time might not be correctly set even if the system clock appears to display correct local time. When capturing, WinPcap has to convert the time to UTC before supplying it to Wireshark. If the system's time zone is not set correctly, that conversion will not be done correctly.

Other capture file formats, such as the Microsoft Network Monitor, DOS-based Sniffer, and Network Instruments Observer formats, save the arrival time of packets as local time values.

Internally to Wireshark, time stamps are represented in UTC. This means that when reading capture files that save the arrival time of packets as local time values, Wireshark must convert those local time values to UTC values.

Wireshark in turn will display the time stamps always in local time. The displaying computer will convert them from UTC to local time and displays this (local) time. For capture files saving the arrival time of packets as UTC values, this means that the arrival time will be displayed as the local time in your time zone, which might not be the same as the arrival time in the time zone in which the packet was captured. For capture files saving the arrival time of packets as local time values, the conversion to UTC will be done using your time zone's offset from UTC and DST rules, which means the conversion will not be

done correctly; the conversion back to local time for display might undo this correctly, in which case the arrival time will be displayed as the arrival time in which the packet was captured.

Table 7.2. Time zone examples for UTC arrival times (without DST)

	Los Angeles	New York	Madrid	London	Berlin	Tokyo
Capture File (UTC)	10:00	10:00	10:00	10:00	10:00	10:00
Local Offset to UTC	-8	-5	-1	0	+1	+9
Displayed Time (Local Time)	02:00	05:00	09:00	10:00	11:00	19:00

For example let's assume that someone in Los Angeles captured a packet with Wireshark at exactly 2 o'clock local time and sends you this capture file. The capture file's time stamp will be represented in UTC as 10 o'clock. You are located in Berlin and will see 11 o'clock on your Wireshark display.

Now you have a phone call, video conference or Internet meeting with that one to talk about that capture file. As you are both looking at the displayed time on your local computers, the one in Los Angeles still sees 2 o'clock but you in Berlin will see 11 o'clock. The time displays are different as both Wireshark displays will show the (different) local times at the same point in time.

Conclusion: You may not bother about the date/time of the time stamp you currently look at unless you must make sure that the date/time is as expected. So, if you get a capture file from a different time zone and/or DST, you'll have to find out the time zone/DST difference between the two local times and "mentally adjust" the time stamps accordingly. In any case, make sure that every computer in question has the correct time and time zone setting.

7.7. Packet Reassembly

7.7.1. What is it?

Network protocols often need to transport large chunks of data which are complete in themselves, e.g. when transferring a file. The underlying protocol might not be able to handle that chunk size (e.g. limitation of the network packet size), or is stream-based like TCP, which doesn't know data chunks at all.

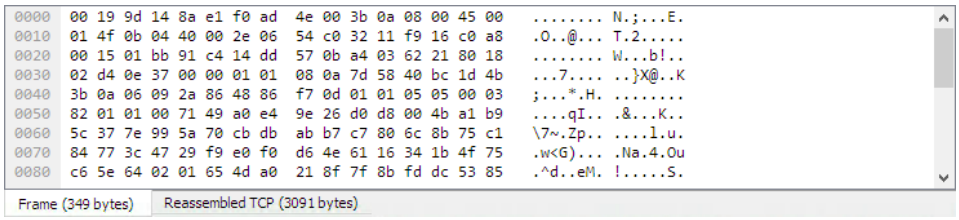
In that case the network protocol has to handle the chunk boundaries itself and (if required) spread the data over multiple packets. It obviously also needs a mechanism to determine the chunk boundaries on the receiving side.

Wireshark calls this mechanism reassembly, although a specific protocol specification might use a different term for this (e.g. desegmentation, defragmentation, etc).

7.7.2. How Wireshark handles it

For some of the network protocols Wireshark knows of, a mechanism is implemented to find, decode and display these chunks of data. Wireshark will try to find the corresponding packets of this chunk, and will show the combined data as additional pages in the "Packet Bytes" pane (for information about this pane. See Section 3.20, "The "Packet Bytes" pane").

Figure 7.5. The “Packet Bytes” pane with a reassembled tab



Reassembly might take place at several protocol layers, so it’s possible that multiple tabs in the “Packet Bytes” pane appear.

Note

You will find the reassembled data in the last packet of the chunk.

For example, in a *HTTP* GET response, the requested data (e.g. an HTML page) is returned. Wireshark will show the hex dump of the data in a new tab “Uncompressed entity body” in the “Packet Bytes” pane.

Reassembly is enabled in the preferences by default but can be disabled in the preferences for the protocol in question. Enabling or disabling reassembly settings for a protocol typically requires two things:

1. The lower level protocol (e.g., TCP) must support reassembly. Often this reassembly can be enabled or disabled via the protocol preferences.

2. The higher level protocol (e.g., HTTP) must use the reassembly mechanism to reassemble fragmented protocol data. This too can often be enabled or disabled via the protocol preferences.

The tooltip of the higher level protocol setting will notify you if and which lower level protocol setting also has to be considered.

7.8. Name Resolution

Name resolution tries to convert some of the numerical address values into a human readable format. There are two possible ways to do these conversions, depending on the resolution to be done: calling system/network services (like the gethostname() function) and/or resolve from Wireshark specific configuration files. For details about the configuration files Wireshark uses for name resolution and alike, see Appendix B, *Files and Folders*.

The name resolution feature can be enabled individually for the protocol layers listed in the following sections.

7.8.1. Name Resolution drawbacks

Name resolution can be invaluable while working with Wireshark and may even save you hours of work. Unfortunately, it also has its drawbacks.

- *Name resolution will often fail.* The name to be resolved might simply be unknown by the name servers asked, or the servers are just not available and the name is also not found in Wireshark’s configuration files.

- *The resolved names are not stored in the capture file or somewhere else.* So the resolved names might not be available if you open the capture file later or on a different machine. Each time you open a capture

file it may look “slightly different” simply because you can’t connect to the name server (which you could connect to before).

- *DNS may add additional packets to your capture file.* You may see packets to/from your machine in your capture file, which are caused by name resolution network services of the machine Wireshark captures from.
- *Resolved DNS names are cached by Wireshark.* This is required for acceptable performance. However, if the name resolution information should change while Wireshark is running, Wireshark won’t notice a change in the name resolution information once it gets cached. If this information changes while Wireshark is running, e.g. a new DHCP lease takes effect, Wireshark won’t notice it.

Name resolution in the packet list is done while the list is filled. If a name can be resolved after a packet is added to the list, its former entry won’t be changed. As the name resolution results are cached, you can use View → Reload to rebuild the packet list with the correctly resolved names. However, this isn’t possible while a capture is in progress.

7.8.2. Ethernet name resolution (MAC layer)

Try to resolve an Ethernet MAC address (e.g. 00:09:5b:01:02:03) to something more “human readable”.

ARP name resolution (system service): Wireshark will ask the operating system to convert an Ethernet address to the corresponding IP address (e.g. 00:09:5b:01:02:03 → 192.168.0.1).

Ethernet codes (ethers file): If the ARP name resolution failed, Wireshark tries to convert the Ethernet address to a known device name, which has been assigned by the user using an *ethers* file (e.g. 00:09:5b:01:02:03 → homerouter).

Ethernet manufacturer codes (manuf file): If neither ARP or ethers returns a result, Wireshark tries to convert the first 3 bytes of an ethernet address to an abbreviated manufacturer name, which has been assigned by the IEEE (e.g. 00:09:5b:01:02:03 → Netgear_01:02:03).

7.8.3. IP name resolution (network layer)

Try to resolve an IP address (e.g. 216.239.37.99) to something more “human readable”.

DNS name resolution (system/library service): Wireshark will use a name resolver to convert an IP address to the hostname associated with it (e.g. 216.239.37.99 → www.1.google.com).

DNS name resolution can generally be performed synchronously or asynchronously. Both mechanisms can be used to convert an IP address to some human readable (domain) name. A system call like gethostname() will try to convert the address to a name. To do this, it will first ask the systems hosts file (e.g. */etc/hosts*) if it finds a matching entry. If that fails, it will ask the configured DNS server(s) about the name.

So the real difference between synchronous DNS and asynchronous DNS comes when the system has to wait for the DNS server about a name resolution. The system call gethostname() will wait until a name is resolved or an error occurs. If the DNS server is unavailable, this might take quite a while (several seconds).

Warning

To provide acceptable performance Wireshark depends on an asynchronous DNS library to do name resolution. If one isn’t available during compilation the feature will be unavailable.

The asynchronous DNS service works a bit differently. It will also ask the DNS server, but it won’t wait for the answer. It will just return to Wireshark in a very short amount of time. The actual (and the following)

address fields won't show the resolved name until the DNS server returns an answer. As mentioned above, the values get cached, so you can use View → Reload to "update" these fields to show the resolved values.

hosts name resolution (hosts file): If DNS name resolution failed, Wireshark will try to convert an IP address to the hostname associated with it, using a hosts file provided by the user (e.g. 216.239.37.99 → www.google.com).

7.8.4. TCP/UDP port name resolution (transport layer)

Try to resolve a TCP/UDP port (e.g. 80) to something more "human readable".

TCP/UDP port conversion (system service): Wireshark will ask the operating system to convert a TCP or UDP port to its well known name (e.g. 80 → http).

7.8.5. VLAN ID resolution

To get a descriptive name for a VLAN tag ID a vlans file can be used.

7.9. Checksums

Several network protocols use checksums to ensure data integrity. Applying checksums as described here is also known as *redundancy checking*.

What are checksums for?

Checksums are used to ensure the integrity of data portions for data transmission or storage. A checksum is basically a calculated summary of such a data portion.

Network data transmissions often produce errors, such as toggled, missing or duplicated bits. As a result, the data received might not be identical to the data transmitted, which is obviously a bad thing.

Because of these transmission errors, network protocols very often use checksums to detect such errors. The transmitter will calculate a checksum of the data and transmits the data together with the checksum. The receiver will calculate the checksum of the received data with the same algorithm as the transmitter. If the received and calculated checksums don't match a transmission error has occurred.

Some checksum algorithms are able to recover (simple) errors by calculating where the expected error must be and repairing it.

If there are errors that cannot be recovered, the receiving side throws away the packet. Depending on the network protocol, this data loss is simply ignored or the sending side needs to detect this loss somehow and retransmits the required packet(s).

Using a checksum drastically reduces the number of undetected transmission errors. However, the usual checksum algorithms cannot guarantee an error detection of 100%, so a very small number of transmission errors may remain undetected.

There are several different kinds of checksum algorithms; an example of an often used checksum algorithm is CRC32. The checksum algorithm actually chosen for a specific network protocol will depend on the expected error rate of the network medium, the importance of error detection, the processor load to perform the calculation, the performance needed and many other things.

Further information about checksums can be found at: https://en.wikipedia.org/wiki/Checksum.

7.9.1. Wireshark checksum validation

Wireshark will validate the checksums of many protocols, e.g. IP, TCP, UDP, etc.

It will do the same calculation as a “normal receiver” would do, and shows the checksum fields in the packet details with a comment, e.g. [correct] or [invalid, must be 0x12345678].

Checksum validation can be switched off for various protocols in the Wireshark protocol preferences, e.g. to (very slightly) increase performance.

If the checksum validation is enabled and it detected an invalid checksum, features like packet reassembly won’t be processed. This is avoided as incorrect connection data could “confuse” the internal database.

7.9.2. Checksum offloading

The checksum calculation might be done by the network driver, protocol driver or even in hardware.

For example: The Ethernet transmitting hardware calculates the Ethernet CRC32 checksum and the receiving hardware validates this checksum. If the received checksum is wrong Wireshark won’t even see the packet, as the Ethernet hardware internally throws away the packet.

Higher level checksums are “traditionally” calculated by the protocol implementation and the completed packet is then handed over to the hardware.

Recent network hardware can perform advanced features such as IP checksum calculation, also known as checksum offloading. The network driver won’t calculate the checksum itself but will simply hand over an empty (zero or garbage filled) checksum field to the hardware.

Note

Checksum offloading often causes confusion as the network packets to be transmitted are handed over to Wireshark before the checksums are actually calculated. Wireshark gets these “empty” checksums and displays them as invalid, even though the packets will contain valid checksums when they leave the network hardware later.

Checksum offloading can be confusing and having a lot of [invalid] messages on the screen can be quite annoying. As mentioned above, invalid checksums may lead to unreassembled packets, making the analysis of the packet data much harder.

You can do two things to avoid this checksum offloading problem:

- Turn off the checksum offloading in the network driver, if this option is available.
- Turn off checksum validation of the specific protocol in the Wireshark preferences. Recent releases of Wireshark disable checksum validation by default due to the prevalance of offloading in modern hardware and operating systems.

Chapter 8. Statistics

8.1. Introduction

Wireshark provides a wide range of network statistics which can be accessed via the Statistics menu.

These statistics range from general information about the loaded capture file (like the number of captured packets), to statistics about specific protocols (e.g. statistics about the number of HTTP requests and responses captured).

- General statistics:
  - **Summary** about the capture file.
  - **Protocol Hierarchy** of the captured packets.
  - **Conversations** e.g. traffic between specific IP addresses.
  - **Endpoints** e.g. traffic to and from an IP addresses.
  - **IO Graphs** visualizing the number of packets (or similar) in time.
- Protocol specific statistics:
  - **Service Response Time** between request and response of some protocols.
  - Various other protocol specific statistics.

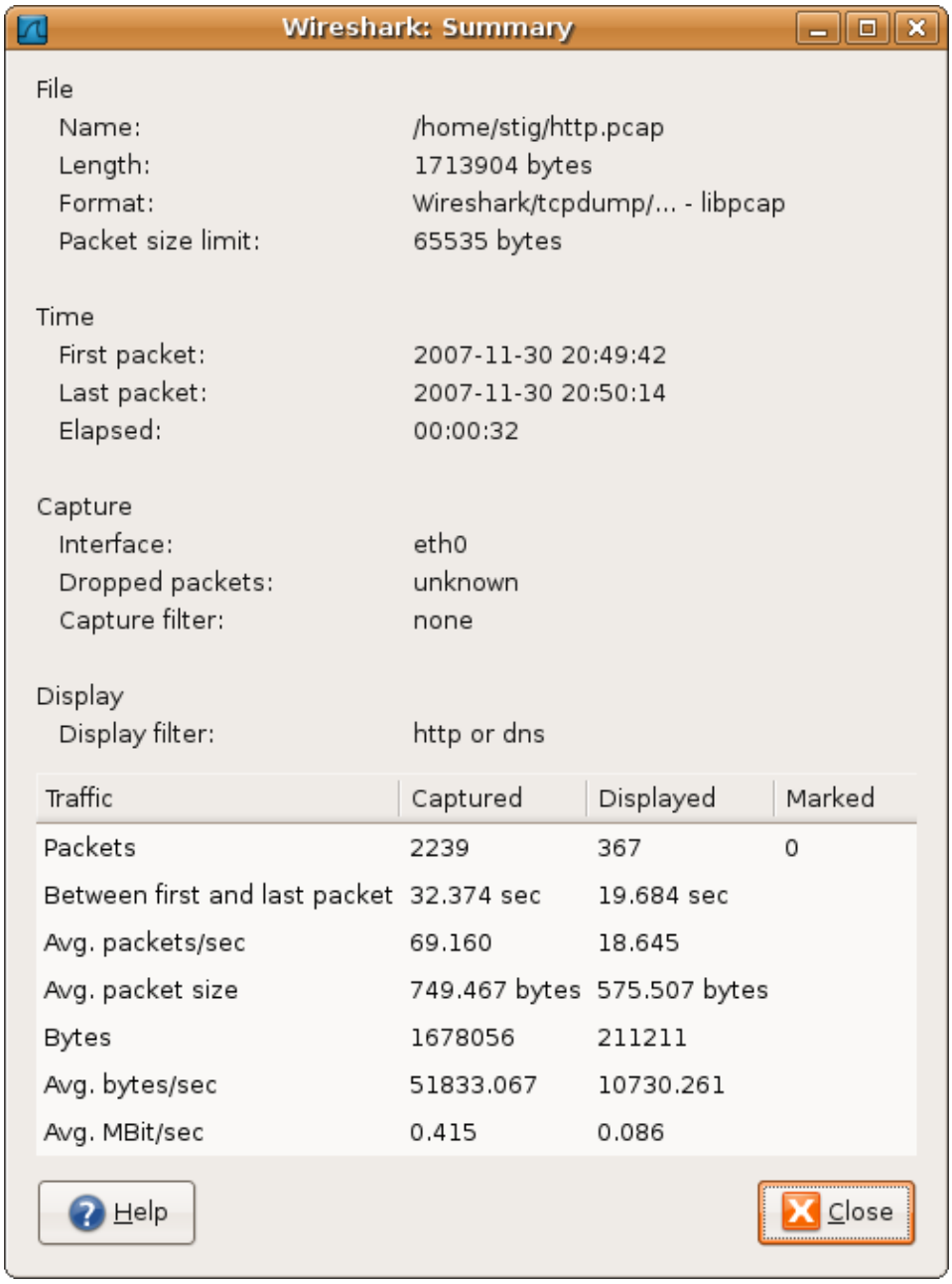
Note

The protocol specific statistics require detailed knowledge about the specific protocol. Unless you are familiar with that protocol, statistics about it will be pretty hard to understand.

8.2. The “Summary” window

General statistics about the current capture file.

Figure 8.1. The “Summary” window



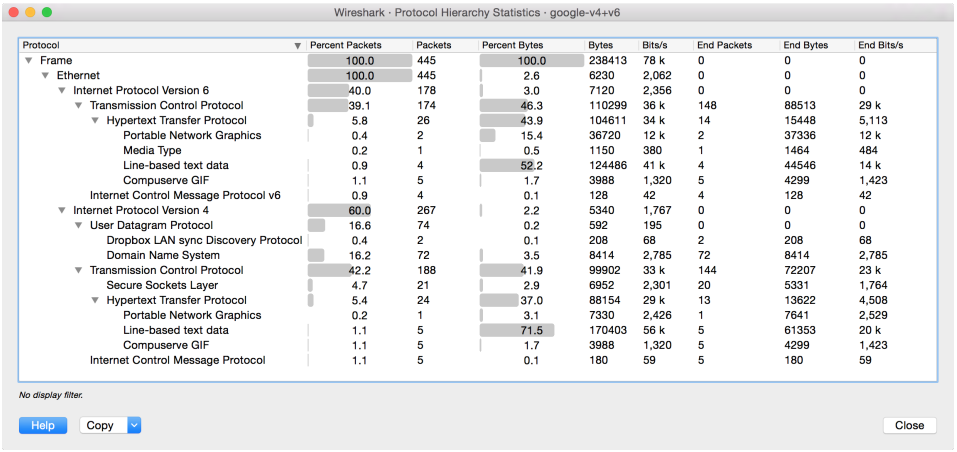
- *File*: general information about the capture file.
- *Time*: the timestamps when the first and the last packet were captured (and the time between them).
- *Capture*: information from the time when the capture was done (only available if the packet data was captured from the network and not loaded from a file).
- *Display*: some display related information.
- *Traffic*: some statistics of the network traffic seen. If a display filter is set, you will see values in the Captured column, and if any packages are marked, you will see values in the Marked column. The values

in the *Captured* column will remain the same as before, while the values in the *Displayed* column will reflect the values corresponding to the packets shown in the display. The values in the *Marked* column will reflect the values corresponding to the marked packages.

8.3. The “Protocol Hierarchy” window

The protocol hierarchy of the captured packets.

Figure 8.2. The “Protocol Hierarchy” window



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	445	100.0	238413	78 k	0	0	0
Ethernet	100.0	445	2.6	6230	2,062	0	0	0
Internet Protocol Version 6	40.0	178	3.0	7120	2,356	0	0	0
Transmission Control Protocol	39.1	174	46.3	110299	36 k	148	88513	29 k
Hypertext Transfer Protocol	5.8	26	43.9	104611	34 k	14	15448	5,113
Portable Network Graphics	0.4	2	15.4	36720	12 k	2	37336	12 k
Media Type	0.2	1	0.5	1150	380	1	1464	484
Line-based text data	0.9	4	52.2	124486	41 k	4	44546	14 k
Compuserve GIF	1.1	5	1.7	3988	1,320	5	4299	1,423
Internet Control Message Protocol v6	0.9	4	0.1	128	42	4	128	42
Internet Protocol Version 4	60.0	267	2.2	5340	1,767	0	0	0
User Datagram Protocol	16.6	74	0.2	592	195	0	0	0
Dropbox LAN sync Discovery Protocol	0.4	2	0.1	208	68	2	208	68
Domain Name System	16.2	72	3.5	8414	2,785	72	8414	2,785
Transmission Control Protocol	42.2	188	41.9	99902	33 k	144	72207	23 k
Secure Sockets Layer	4.7	21	2.9	6952	2,301	20	5331	1,764
Hypertext Transfer Protocol	5.4	24	37.0	88154	29 k	13	13622	4,508
Portable Network Graphics	0.2	1	3.1	7330	2,426	1	7641	2,529
Line-based text data	1.1	5	71.5	170403	56 k	5	61353	20 k
Compuserve GIF	1.1	5	1.7	3988	1,320	5	4299	1,423
Internet Control Message Protocol	1.1	5	0.1	180	59	5	180	59

This is a tree of all the protocols in the capture. Each row contains the statistical values of one protocol. Two of the columns (*Percent Packets* and *Percent Bytes*) serve double duty as bar graphs. If a display filter is set it will be shown at the bottom.

The Copy button will let you copy the window contents as CSV or YAML.

Protocol hierarchy columns

Protocol
: This protocol’s name

Percent Packets
: The percentage of protocol packets relative to all packets in the capture

Packets
: The total number of packets of this protocol

Percent Bytes
: The percentage of protocol bytes relative to the total bytes in the capture

Bytes
: The total number of bytes of this protocol

Bits/s
: The bandwidth of this protocol relative to the capture time

End Packets
: The absolute number of packets of this protocol where it was the highest protocol in the stack (last dissected)

End Bytes
: The absolute number of bytes of this protocol where it was the highest protocol in the stack (last dissected)

End Bits/s
: The bandwidth of this protocol relative to the capture time where was the highest protocol in the stack (last dissected)

Packets usually contain multiple protocols. As a result more than one protocol will be counted for each packet. Example: In the screenshot IP has 99.9% and TCP 98.5% (which is together much more than 100%).

Protocol layers can consist of packets that won't contain any higher layer protocol, so the sum of all higher layer packets may not sum up to the protocols packet count. Example: In the screenshot TCP has 98.5% but the sum of the subprotocols (SSL, HTTP, etc) is much less. This can be caused by continuation frames, TCP protocol overhead, and other undissected data.

A single packet can contain the same protocol more than once. In this case, the protocol is counted more than once. For example ICMP replies and many tunneling protocols will carry more than one IP header.

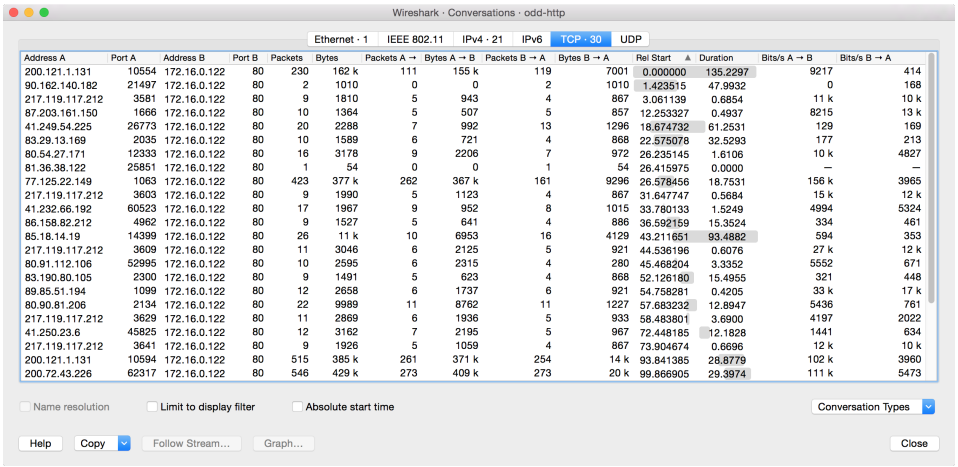
8.4. Conversations

A network conversation is the traffic between two specific endpoints. For example, an IP conversation is all the traffic between two IP addresses. The description of the known endpoint types can be found in Section 8.5, "Endpoints".

8.4.1. The "Conversations" window

The conversations window is similar to the endpoint Window. See Section 8.5.1, "The "Endpoints" window" for a description of their common features. Along with addresses, packet counters, and byte counters the conversation window adds four columns: the start time of the conversation ("Rel Start") or ("Abs Start"), the duration of the conversation in seconds, and the average bits (not bytes) per second in each direction. A timeline graph is also drawn across the "Rel Start" / "Abs Start" and "Duration" columns.

Figure 8.3. The "Conversations" window



Each row in the list shows the statistical values for exactly one conversation.

Name resolution will be done if selected in the window and if it is active for the specific protocol layer (MAC layer for the selected Ethernet endpoints page). *Limit to display filter* will only show conversations matching the current display filter. *Absolute start time* switches the start time column between relative ("Rel Start") and absolute ("Abs Start") times. Relative start times match the "Seconds Since Beginning of Capture" time display format in the packet list and absolute start times match the "Time of Day" display format.

The Copy button will copy the list values to the clipboard in CSV (Comma Separated Values) or YAML format. The Follow Stream… button will show the stream contents as described in Figure 7.1, "The "Follow TCP Stream" dialog box" dialog. The Graph… button will show a graph as described in Section 8.6, "The "IO Graphs" window".

Conversation Types lets you choose which traffic type tabs are shown. See Section 8.5, "Endpoints" for a list of endpoint types. The enabled types are saved in your profile settings.

Tip

This window will be updated frequently so it will be useful even if you open it before (or while) you are doing a live capture.

8.5. Endpoints

A network endpoint is the logical endpoint of separate protocol traffic of a specific protocol layer. The endpoint statistics of Wireshark will take the following endpoints into account:

Tip

If you are looking for a feature other network tools call a *hostlist*, here is the right place to look. The list of Ethernet or IP endpoints is usually what you're looking for.

Endpoint and Conversation types

Bluetooth
: A MAC-48 address similar to Ethernet.

Ethernet
: Identical to the Ethernet device's MAC-48 identifier.

Fibre Channel
: A MAC-48 address similar to Ethernet.

IEEE 802.11
: A MAC-48 address similar to Ethernet.

FDDI
: Identical to the FDDI MAC-48 address.

IPv4
: Identical to the 32-bit IPv4 address.

IPv6
: Identical to the 128-bit IPv6 address.

IPX
: A concatenation of a 32 bit network number and 48 bit node address, by default the Ethernet interface's MAC-48 address.

JXTA
A 160 bit SHA-1 URN.

NCP
Similar to IPX.

RSVP
A combination of varios RSVP session attributes and IPv4 addresses.

SCTP
A combination of the host IP addresses (plural) and the SCTP port used. So different SCTP ports on the same IP address are different SCTP endpoints, but the same SCTP port on different IP addresses of the same host are still the same endpoint.

TCP
A combination of the IP address and the TCP port used. Different TCP ports on the same IP address are different TCP endpoints.

Token Ring
Identical to the Token Ring MAC-48 address.

UDP
A combination of the IP address and the UDP port used, so different UDP ports on the same IP address are different UDP endpoints.

USB
Identical to the 7-bit USB address.

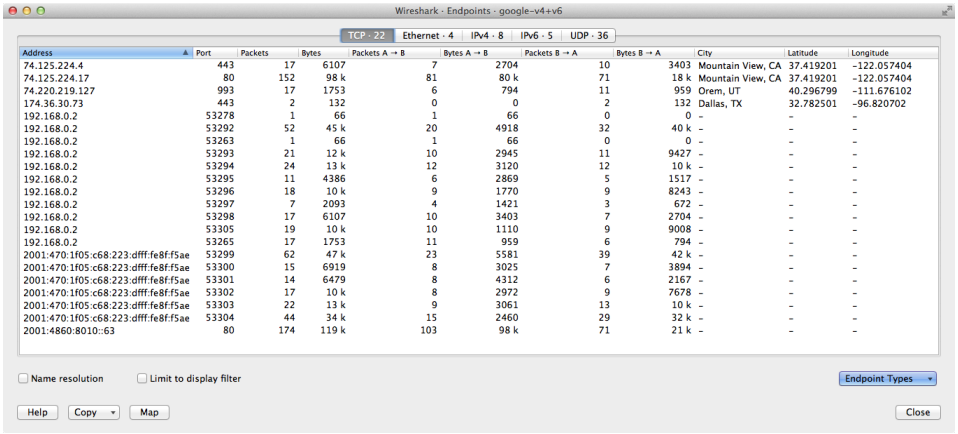
Broadcast and multicast endpoints

Broadcast and multicast traffic will be shown separately as additional endpoints. Of course, as these aren't physical endpoints the real traffic will be received by some or all of the listed unicast endpoints.

8.5.1. The "Endpoints" window

This window shows statistics about the endpoints captured.

Figure 8.4. The "Endpoints" window



For each supported protocol, a tab is shown in this window. Each tab label shows the number of endpoints captured (e.g. the tab label "Ethernet · 4" tells you that four ethernet endpoints have been captured). If

no endpoints of a specific protocol were captured, the tab label will be greyed out (although the related page can still be selected).

Each row in the list shows the statistical values for exactly one endpoint.

Name resolution will be done if selected in the window and if it is active for the specific protocol layer (MAC layer for the selected Ethernet endpoints page). *Limit to display filter* will only show conversations matching the current display filter. Note that in this example we have GeoIP configured which gives us extra geographic columns. See Section 10.10, “GeoIP Database Paths” for more information.

The Copy button will copy the list values to the clipboard in CSV (Comma Separated Values) or YAML format. The Map button will show the endpoints mapped in your web browser.

Endpoint Types lets you choose which traffic type tabs are shown. See Section 8.5, “Endpoints” above for a list of endpoint types. The enabled types are saved in your profile settings.

Tip

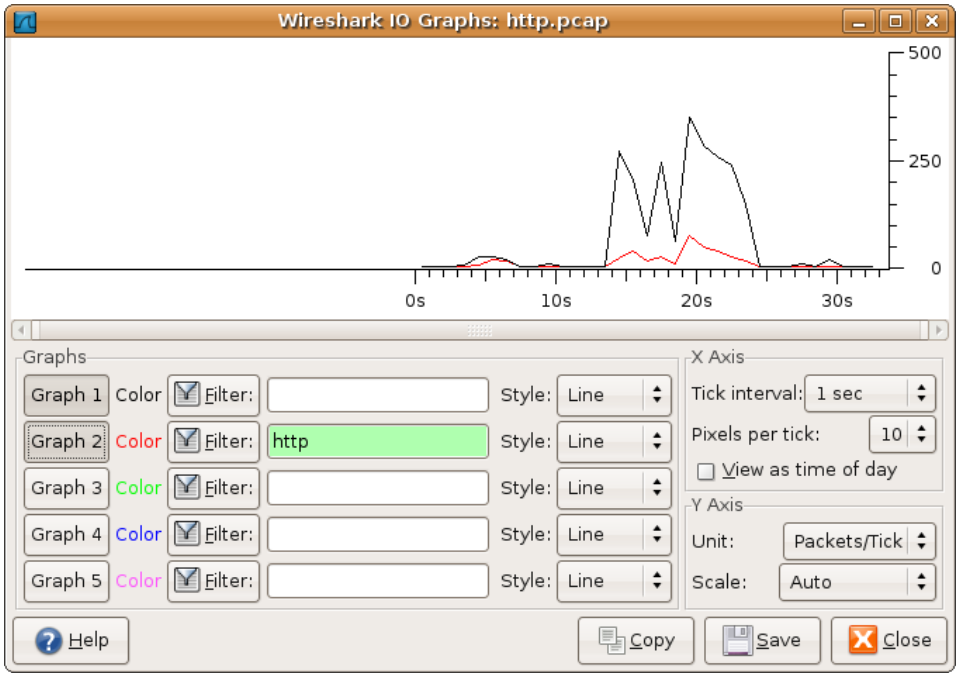
This window will be updated frequently, so it will be useful even if you open it before (or while) you are doing a live capture.

8.6. The “IO Graphs” window

User configurable graph of the captured network packets.

You can define up to five differently colored graphs.

Figure 8.5. The “IO Graphs” window



The user can configure the following things:

- *Graphs*
  - *Graph 1-5*: enable the specific graph 1-5 (only graph 1 is enabled by default)

- *Color*: the color of the graph (cannot be changed)
- *Filter*: a display filter for this graph (only the packets that pass this filter will be taken into account for this graph)
- *Style*: the style of the graph (Line/Impulse/FBar/Dot)

- *X Axis*
  - *Tick interval*: an interval in x direction lasts (10/1 minutes or 10/1/0.1/0.01/0.001 seconds)
  - *Pixels per tick*: use 10/5/2/1 pixels per tick interval
  - *View as time of day*: option to view x direction labels as time of day instead of seconds or minutes since beginning of capture
- *Y Axis*
  - *Unit*: the unit for the y direction (Packets/Tick, Bytes/Tick, Bits/Tick, Advanced…) [XXX - describe the Advanced feature.]
  - *Scale*: the scale for the y unit (Logarithmic,Auto,10,20,50,100,200,500,…)

The Save button will save the currently displayed portion of the graph as one of various file formats.

The Copy button will copy values from selected graphs to the clipboard in CSV (Comma Separated Values) format.

Tip

Click in the graph to select the first package in the selected interval.

8.7. Service Response Time

The service response time is the time between a request and the corresponding response. This information is available for many protocols.

Service response time statistics are currently available for the following protocols:

- *DCE-RPC*
- *Fibre Channel*
- *H.225 RAS*
- *LDAP*
- *LTE MAC*
- *MGCP*
- *ONC-RPC*
- *SMB*

As an example, the DCE-RPC service response time is described in more detail.

Note

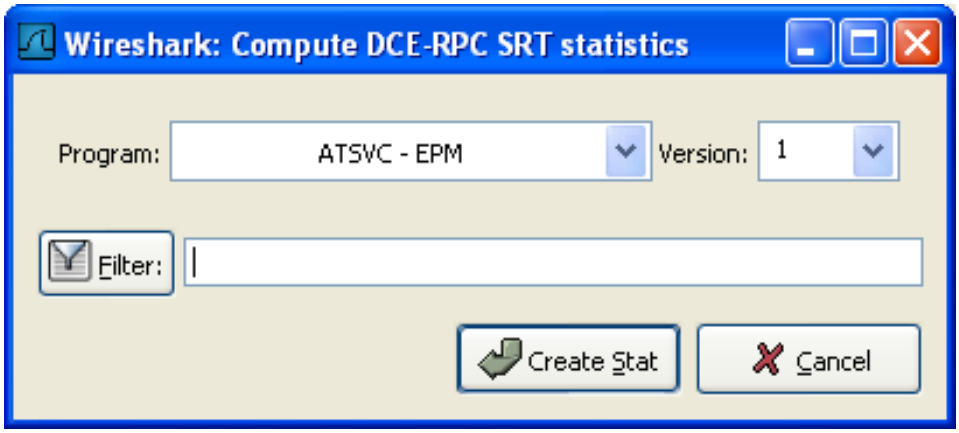
The other Service Response Time windows will work the same way (or only slightly different) compared to the following description.

8.7.1. The "Service Response Time DCE-RPC" window

The service response time of DCE-RPC is the time between the request and the corresponding response.

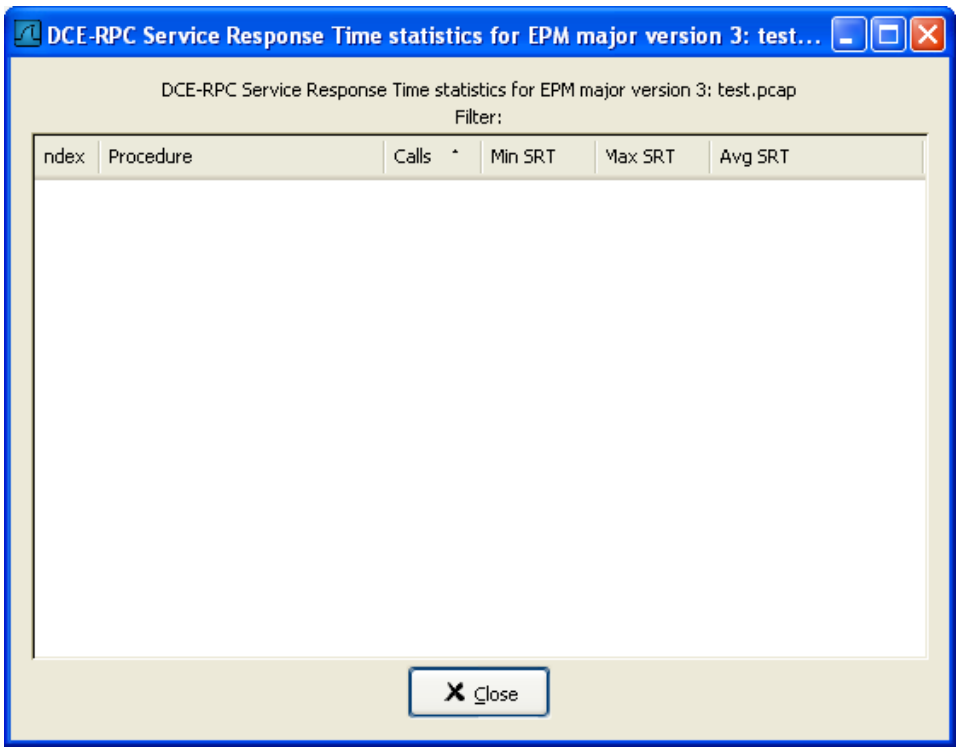
First of all, you have to select the DCE-RPC interface:

Figure 8.6. The "Compute DCE-RPC statistics" window



You can optionally set a display filter, to reduce the amount of packets.

Figure 8.7. The "DCE-RPC Statistic for …" window



Each row corresponds to a method of the interface selected (so the EPM interface in version 3 has 7 methods). For each method the number of calls, and the statistics of the SRT time is calculated.

8.8. Compare two capture files

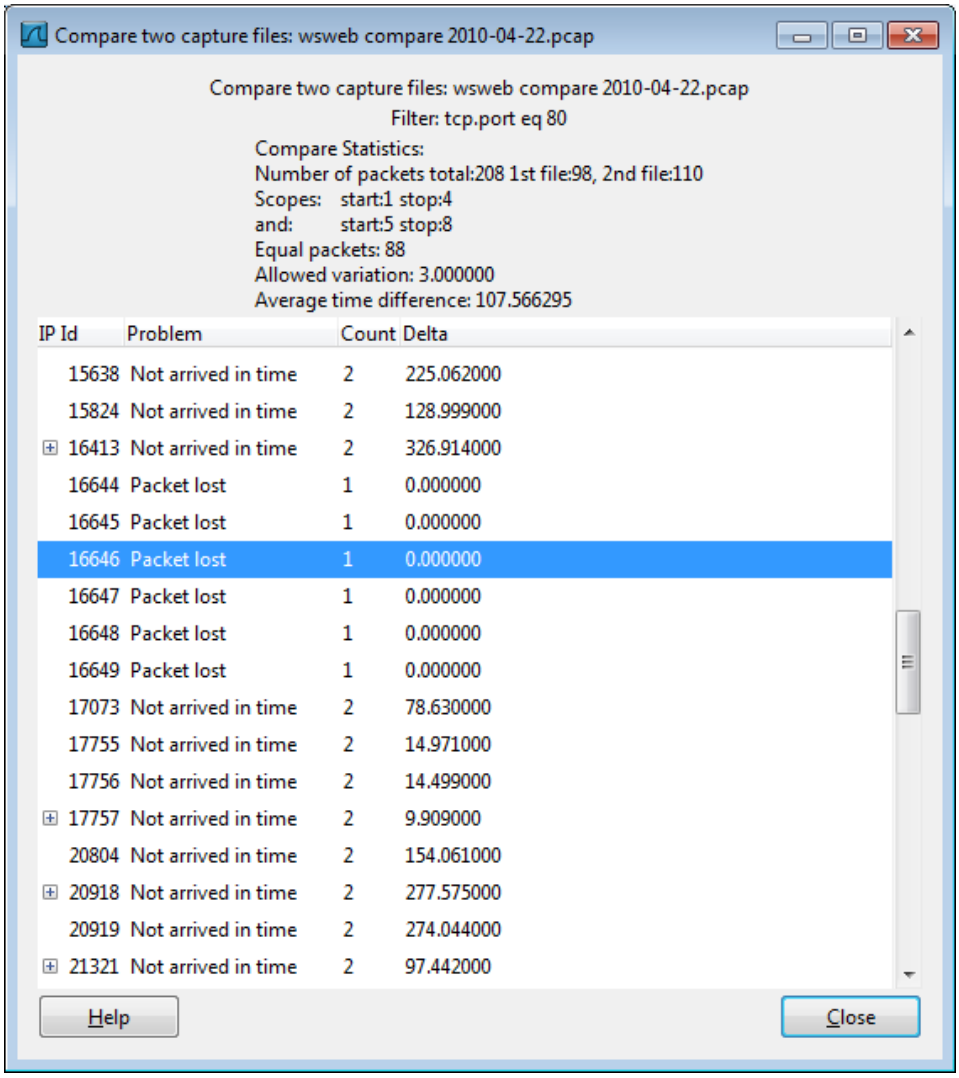
Compare two capture files.

This feature works best when you have merged two capture files chronologically, one from each side of a client/server connection.

The merged capture data is checked for missing packets. If a matching connection is found it is checked for:

- IP header checksums
- Excessive delay (defined by the "Time variance" setting)
- Packet order

Figure 8.8. The "Compare" window



You can configure the following:

- *Start compare:* Start comparing when this many IP IDs are matched. A zero value starts comparing immediately.
- *Stop compare:* Stop comparing when we can no longer match this many IP IDs. Zero always compares.
- *Endpoint distinction:* Use MAC addresses or IP time-to-live values to determine connection endpoints.
- *Check order:* Check for the same IP ID in the previous packet at each end.
- *Time variance:* Trigger an error if the packet arrives this many milliseconds after the average delay.
- *Filter:* Limit comparison to packets that match this display filter.

The info column contains new numbering so the same packets are parallel.

The color filtering differentiate the two files from each other. A “zebra” effect is create if the Info column is sorted.

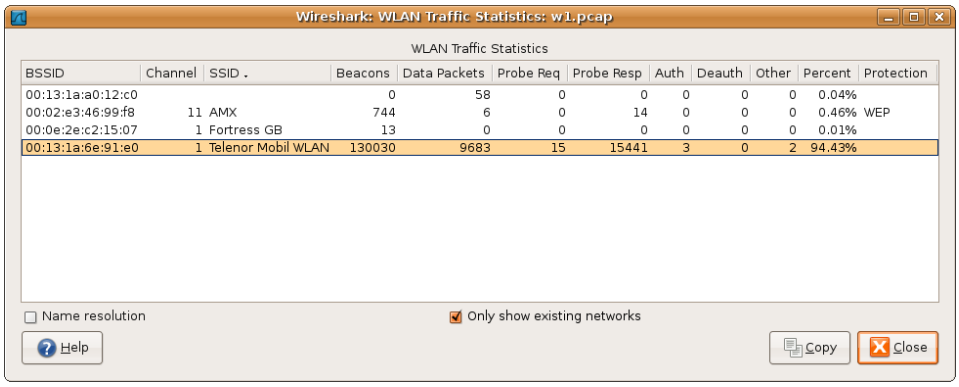
Tip

If you click on an item in the error list its corresponding packet will be selected in the main window.

8.9. WLAN Traffic Statistics

Statistics of the captured WLAN traffic. This window will summarize the wireless network traffic found in the capture. Probe requests will be merged into an existing network if the SSID matches.

Figure 8.9. The "WLAN Traffic Statistics" window



Each row in the list shows the statistical values for exactly one wireless network.

Name resolution will be done if selected in the window and if it is active for the MAC layer.

Only show existing networks will exclude probe requests with a SSID not matching any network from the list.

The Copy button will copy the list values to the clipboard in CSV (Comma Separated Values) format.

Tip

This window will be updated frequently, so it will be useful, even if you open it before (or while) you are doing a live capture.

8.10. The protocol specific statistics windows

The protocol specific statistics windows display detailed information of specific protocols and might be described in a later version of this document.

Some of these statistics are described at https://wiki.wireshark.org/Statistics.

Chapter 9. Telephony

9.1. Introduction

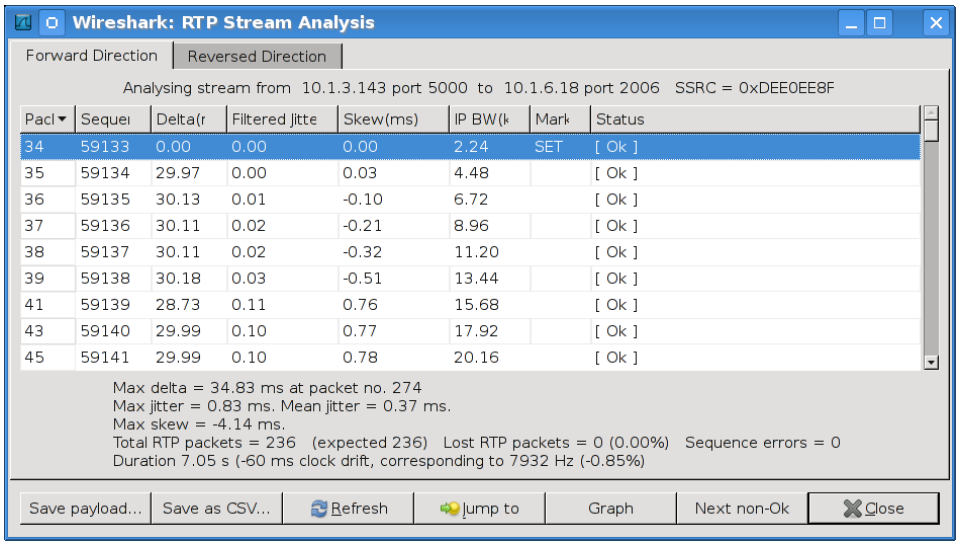
Wireshark provides a wide range of telephony related network statistics which can be accessed via the Telephony menu.

These statistics range from specific signaling protocols, to analysis of signaling and media flows. If encoded in a compatible encoding the media flow can even be played.

9.2. RTP Analysis

The RTP analysis function takes the selected RTP stream (and the reverse stream, if possible) and generates a list of statistics on it.

Figure 9.1. The “RTP Stream Analysis” window



Starting with basic data as packet number and sequence number, further statistics are created based on arrival time, delay, jitter, packet size, etc.

Besides the per packet statistics, the lower pane shows the overall statistics, with minimums and maximums for delta, jitter and clock skew. Also an indication of lost packets is included.

The RTP Stream Analysis window further provides the option to save the RTP payload (as raw data or, if in a PCM encoding, in an Audio file). Other options a to export and plot various statistics on the RTP streams.

9.3. IAX2 Analysis

The “IAX2 Analysis” dialog shows statistics for the forward and reverse streams of a selected IAX2 call along with a graph.

9.4. VoIP Calls

The VoIP Calls window shows a list of all detected VoIP calls in the captured traffic. It finds calls by their signaling.

More details can be found on the https://wiki.wireshark.org/VoIP_calls page.

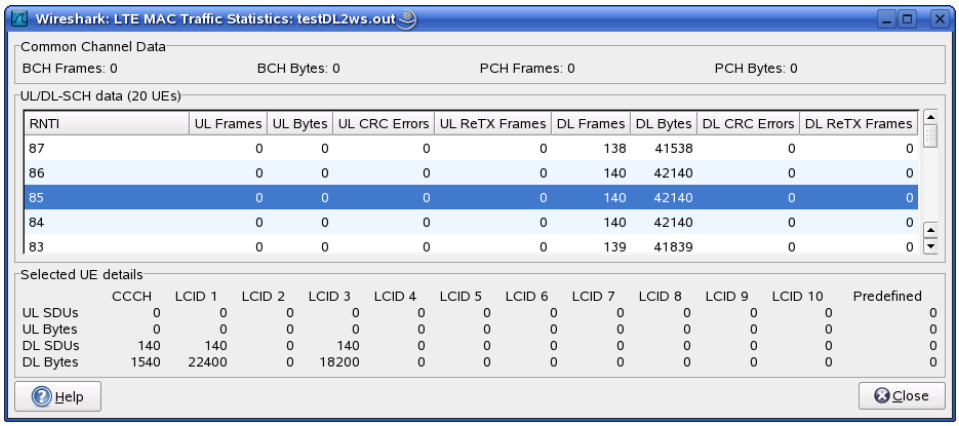
The RTP Player window lets you play back RTP audio data. In order to use this feature your version of Wireshark must support audio and the codecs used by each RTP stream.

More details can be found on the https://wiki.wireshark.org/VoIP_calls page.

9.5. LTE MAC Traffic Statistics

Statistics of the captured LTE MAC traffic. This window will summarize the LTE MAC traffic found in the capture.

Figure 9.2. The “LTE MAC Traffic Statistics” window

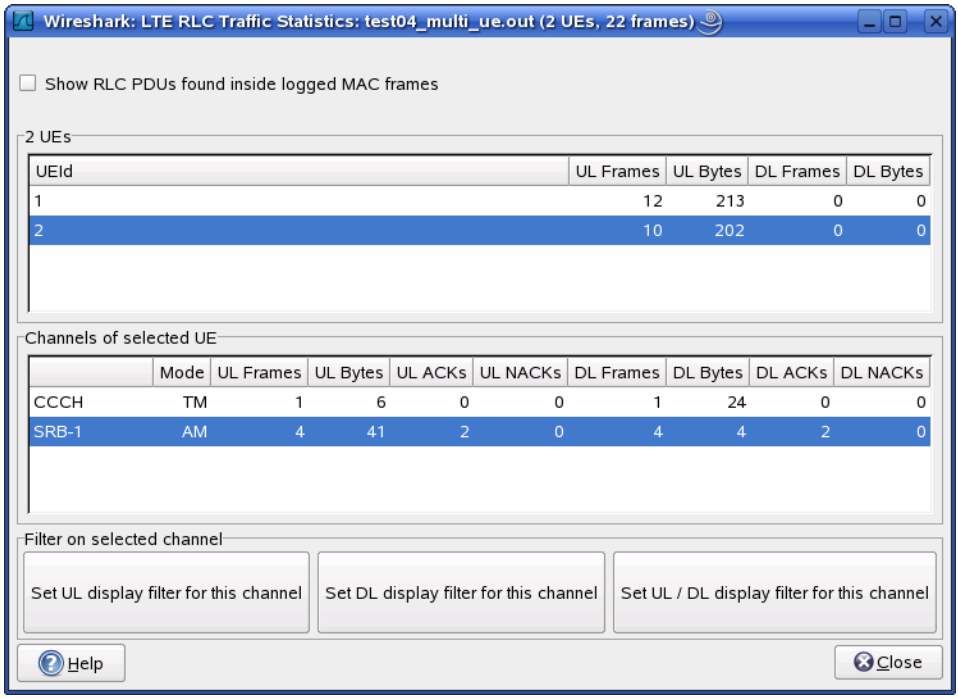


The top pane shows statistics for common channels. Each row in the middle pane shows statistical highlights for exactly one UE/C-RNTI. In the lower pane, you can see the for the currently selected UE/C-RNTI the traffic broken down by individual channel.

9.6. LTE RLC Traffic Statistics

Statistics of the captured LTE RLC traffic. This window will summarize the LTE RLC traffic found in the capture.

Figure 9.3. The “LTE RLC Traffic Statistics” window



At the top, the check-box allows this window to include RLC PDUs found within MAC PDUs or not. This will affect both the PDUs counted as well as the display filters generated (see below).

The upper list shows summaries of each active UE. Each row in the lower list shows statistical highlights for individual channels within the selected UE.

The lower part of the windows allows display filters to be generated and set for the selected channel. Note that in the case of Acknowledged Mode channels, if a single direction is chosen, the generated filter will show data in that direction and control PDUs in the opposite direction.

9.7. The protocol specific statistics windows

The protocol specific statistics windows display detailed information of specific protocols and might be described in a later version of this document.

Some of these statistics are described at the https://wiki.wireshark.org/Statistics pages.

Chapter 10. Customizing Wireshark

10.1. Introduction

Wireshark's default behaviour will usually suit your needs pretty well. However, as you become more familiar with Wireshark, it can be customized in various ways to suit your needs even better. In this chapter we explore:

- How to start Wireshark with command line parameters
- How to colorize the packet list
- How to control protocol dissection
- How to use the various preference settings

10.2. Start Wireshark from the command line

You can start Wireshark from the command line, but it can also be started from most Window managers as well. In this section we will look at starting it from the command line.

Wireshark supports a large number of command line parameters. To see what they are, simply enter the command *wireshark -h* and the help information shown in Example 10.1, "Help information available from Wireshark" (or something similar) should be printed.

Example 10.1. Help information available from Wireshark

```
Wireshark 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Interactively dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: wireshark [options] ... [ <infile> ]

Capture interface:
  -i <interface>           name or idx of interface (def: first non-loopback)
  -f <capfilter|predef:>   packet filter in libpcap filter syntax or
                           predef:filtername - predefined filtername from GUI
  -s <snaplen>             packet snapshot length (def: 65535)
  -p                       don't capture in promiscuous mode
  -k                       start capturing immediately (def: do nothing)
  -S                       update packet display when new packets are captured
  -l                       turn on automatic scrolling while -S is in use
  -I                       capture in monitor mode, if available
  -B <buffer size>         size of kernel buffer (def: 2MB)
  -y <link type>           link layer type (def: first appropriate)
  -D                       print list of interfaces and exit
  -L                       print list of link-layer types of iface and exit

Capture stop conditions:
  -c <packet count>        stop after n packets (def: infinite)
  -a <autostop cond.> ...  duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                              files:NUM - stop after NUM files
Capture output:
  -b <ringbuffer opt.> ... duration:NUM - switch to next file after NUM secs
                           filesize:NUM - switch to next file after NUM KB
                              files:NUM - ringbuffer: replace after NUM files
```

```
RPCAP options:
  -A <user>:<password>     use RPCAP password authentication
Input file:
  -r <infile>              set the filename to read from (no pipes or stdin!)

Processing:
  -R <read filter>         packet filter in Wireshark display filter syntax
  -n                       disable all name resolutions (def: all enabled)
  -N <name resolve flags>  enable specific name resolution(s): "mnNtCd"
  -d <layer_type>==<selector>,<decode_as_protocol> ...
                           "Decode As", see the man page for details
                           Example: tcp.port==8888,http
  --disable-protocol <proto_name>
                           disable dissection of proto_name
  --enable-heuristic <short_name>
                           enable dissection of heuristic protocol
  --disable-heuristic <short_name>
                           disable dissection of heuristic protocol

User interface:
  -C <config profile>      start with specified configuration profile
  -Y <display filter>      start with the given display filter
  -g <packet number>       go to specified packet number after "-r"
  -J <jump filter>         jump to the first packet matching the (display)
                           filter
  -j                       search backwards for a matching packet after "-J"
  -m <font>                set the font name used for most text
  -t a|ad|d|dd|e|r|u|ud    output format of time stamps (def: r: rel. to first)
  -u s|hms                 output format of seconds (def: s: seconds)
  -X <key>:<value>         eXtension options, see man page for details
  -z <statistics>          show various statistics, see man page for details

Output:
  -w <outfile|->           set the output filename (or '-' for stdout)

Miscellaneous:
  -h                       display this help and exit
  -v                       display version info and exit
  -P <key>:<path>          persconf:path - personal configuration files
                           persdata:path - personal data files
  -o <name>:<value> ...    override preference or recent setting
  -K <keytab>              keytab file to use for kerberos decryption
```

We will examine each of the command line options in turn.

The first thing to notice is that issuing the command `wireshark` by itself will bring up Wireshark. However, you can include as many of the command line parameters as you like. Their meanings are as follows (in alphabetical order):

-a <capture autostop condition>

Specify a criterion that specifies when Wireshark is to stop writing to a capture file. The criterion is of the form test:value, where test is one of:

duration:value

Stop writing to a capture file after value of seconds have elapsed.

filesize:value

Stop writing to a capture file after it reaches a size of value kilobytes (where a kilobyte is 1000 bytes, not 1024 bytes). If this option is used together with the -b option, Wireshark will stop writing to the current capture file and switch to the next one if filesize is reached.

files:value

Stop writing to capture files after value number of files were written.

-b <capture ring buffer option>

If a maximum capture file size was specified, this option causes Wireshark to run in “ring buffer” mode, with the specified number of files. In “ring buffer” mode, Wireshark will write to several capture files. Their name is based on the number of the file and on the creation date and time.

When the first capture file fills up Wireshark will switch to writing to the next file, and so on. With the <command>files</command> option it’s also possible to form a “ring buffer.” This will fill up new files until the number of files specified, at which point the data in the first file will be discarded so a new file can be written.

If the optional <command>duration</command> is specified, Wireshark will also switch to the next file when the specified number of seconds has elapsed even if the current file is not completely fills up.

duration</command>:value

Switch to the next file after value seconds have elapsed, even if the current file is not completely filled up.

filesize</command>:value

Switch to the next file after it reaches a size of value kilobytes (where a kilobyte is 1000 bytes, not 1024 bytes).

files</command>:value

Begin again with the first file after value number of files were written (form a ring buffer).

-B <capture buffer size>

Set capture buffer size (in MB, default is 1MB). This is used by the capture driver to buffer packet data until that data can be written to disk. If you encounter packet drops while capturing, try to increase this size. Not supported on some platforms.

-c <capture packet count>

This option specifies the maximum number of packets to capture when capturing live data. It would be used in conjunction with the `-k` option.

-D

Print a list of the interfaces on which Wireshark can capture, then exit. For each network interface, a number and an interface name, possibly followed by a text description of the interface, is printed. The interface name or the number can be supplied to the `-i` flag to specify an interface on which to capture.

This can be useful on systems that don’t have a command to list them (e.g., Windows systems, or UNIX systems lacking `ifconfig -a`). The number can be especially useful on Windows, where the interface name is a GUID.

Note that “can capture” means that Wireshark was able to open that device to do a live capture. If, on your system, a program doing a network capture must be run from an account with special privileges (for example, as root), then, if Wireshark is run with the `-D` flag and is not run from such an account, it will not list any interfaces.

-f <capture filter>

This option sets the initial capture filter expression to be used when capturing packets.

-g <packet number>

After reading in a capture file using the -r flag, go to the given packet number.

-h

The `-h` option requests Wireshark to print its version and usage instructions (as shown above) and exit.

-i <capture interface>

Set the name of the network interface or pipe to use for live packet capture.

Network interface names should match one of the names listed in `wireshark -D` (described above). A number, as reported by `wireshark -D`, can also be used. If you're using UNIX, `netstat -i` or `ifconfig -a` might also work to list interface names, although not all versions of UNIX support the `-a` flag to `ifconfig`.

If no interface is specified, Wireshark searches the list of interfaces, choosing the first non-loopback interface if there are any non-loopback interfaces, and choosing the first loopback interface if there are no non-loopback interfaces; if there are no interfaces, Wireshark reports an error and doesn't start the capture.

Pipe names should be either the name of a FIFO (named pipe) or "-" to read data from the standard input. Data read from pipes must be in standard libpcap format.

-J <jump filter>
After reading in a capture file using the `-r` flag, jump to the first packet which matches the filter expression. The filter expression is in display filter format. If an exact match cannot be found the first packet afterwards is selected.

-I
Capture wireless packets in monitor mode if available.

-j
Use this option after the `-J` option to search backwards for a first packet to go to.

-k
The `-k` option specifies that Wireshark should start capturing packets immediately. This option requires the use of the `-i` parameter to specify the interface that packet capture will occur from.

-K <keytab file>
Use the specified file for Kerberos decryption.

-l
This option turns on automatic scrolling if the packet list pane is being updated automatically as packets arrive during a capture (as specified by the `-S` flag).

-L
List the data link types supported by the interface and exit.

-m <font>
This option sets the name of the font used for most text displayed by Wireshark.

-n
Disable network object name resolution (such as hostname, TCP and UDP port names).

-N <name resolving flags>
Turns on name resolving for particular types of addresses and port numbers. The argument is a string that may contain the letters `m` to enable MAC address resolution, `n` to enable network address resolution, and `t` to enable transport-layer port number resolution. This overrides `-n` if both `-N` and `-n` are present. The letter `d` enables resolution from captured DNS packets.

-o <preference or recent settings>
Sets a preference or recent value, overriding the default value and any value read from a preference or recent file. The argument to the flag is a string of the form *prefname:value*, where *prefname* is the name of the preference (which is the same name that would appear in the `preferences` or `recent` file), and *value* is the value to which it should be set. Multiple instances of `-o <preference settings> ` can be given on a single command line.

An example of setting a single preference would be:

```
wireshark -o mgcp.display_dissect_tree:TRUE
```

An example of setting multiple preferences would be:

```
wireshark -o mgcp.display_dissect_tree:TRUE -o mgcp.udp.callagent_port:2627
```

You can get a list of all available preference strings from the preferences file. See Appendix B, *Files and Folders* for details.

User access tables can be overridden using "uat," followed by the UAT file name and a valid record for the file:

```
wireshark -o "uat:user_dlts:\"User 0 (DLT=147)\",\"http\",\"0\",\"\",\"0\",\"\""
```

The example above would dissect packets with a libpcap data link type 147 as HTTP, just as if you had configured it in the DLT_USER protocol preferences.

-p
: Don't put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason. Hence, `-p` cannot be used to ensure that the only traffic that is captured is traffic sent to or from the machine on which Wireshark is running, broadcast traffic, and multicast traffic to addresses received by that machine.

-P <path setting>
: Special path settings usually detected automatically. This is used for special cases, e.g. starting Wireshark from a known location on an USB stick.

  The criterion is of the form key:path, where key is one of:

  persconf:path
  : Path of personal configuration files, like the preferences files.

  persdata:path
  : Path of personal data files, it's the folder initially opened. After the initialization, the recent file will keep the folder last used.

-Q
: This option forces Wireshark to exit when capturing is complete. It can be used with the `-c` option. It must be used in conjunction with the `-i` and `-w` options.

-r <infile>
: This option provides the name of a capture file for Wireshark to read and display. This capture file can be in one of the formats Wireshark understands.

-R <read (display) filter>
: This option specifies a display filter to be applied when reading packets from a capture file. The syntax of this filter is that of the display filters discussed in Section 6.3, "Filtering packets while viewing". Packets not matching the filter are discarded.

-s <capture snapshot length>
: This option specifies the snapshot length to use when capturing packets. Wireshark will only capture *snaplen* bytes of data for each packet.

-S
: This option specifies that Wireshark will display packets as it captures them. This is done by capturing in one process and displaying them in a separate process. This is the same as "Update list of packets in real time" in the "Capture Options" dialog box.

-t <time stamp format>
This option sets the format of packet timestamps that are displayed in the packet list window. The format can be one of:

r
Relative, which specifies timestamps are displayed relative to the first packet captured.

a
Absolute, which specifies that actual times be displayed for all packets.

ad
Absolute with date, which specifies that actual dates and times be displayed for all packets.

d
Delta, which specifies that timestamps are relative to the previous packet.

e
Epoch, which specifies that timestamps are seconds since epoch (Jan 1, 1970 00:00:00)

-u <s | hms>
Show timesamps as seconds (*s*, the default) or hours, minutes, and seconts (*hms*)

-v
The `-v` option requests Wireshark to print out its version information and exit.

-w <savefile>
This option sets the name of the file to be used to save captured packets.

-y <capture link type>
If a capture is started from the command line with -k, set the data link type to use while capturing packets. The values reported by -L are the values that can be used.

-X <eXtension option>
Specify an option to be passed to a TShark module. The eXtension option is in the form extension_key:value, where extension_key can be:

lua_script:lua_script_filename
Tells Wireshark to load the given script in addition to the default Lua scripts.

lua_script[num]:argument
Tells Wireshark to pass the given argument to the lua script identified by *num*, which is the number indexed order of the *lua_script* command. For example, if only one script was loaded with `-X lua_script:my.lua`, then `-X lua_script1:foo` will pass the string *foo* to the *my.lua* script. If two scripts were loaded, such as `-X lua_script:my.lua` and `-X lua_script:other.lua` in that order, then a `-X lua_script2:bar` would pass the string *bar* to the second lua script, namely *other.lua*.

-z <statistics-string>
Get Wireshark to collect various types of statistics and display the result in a window that updates in semi-real time.

10.3. Packet colorization

A very useful mechanism available in Wireshark is packet colorization. You can set up Wireshark so that it will colorize packets according to a display filter. This allows you to emphasize the packets you might be interested in.

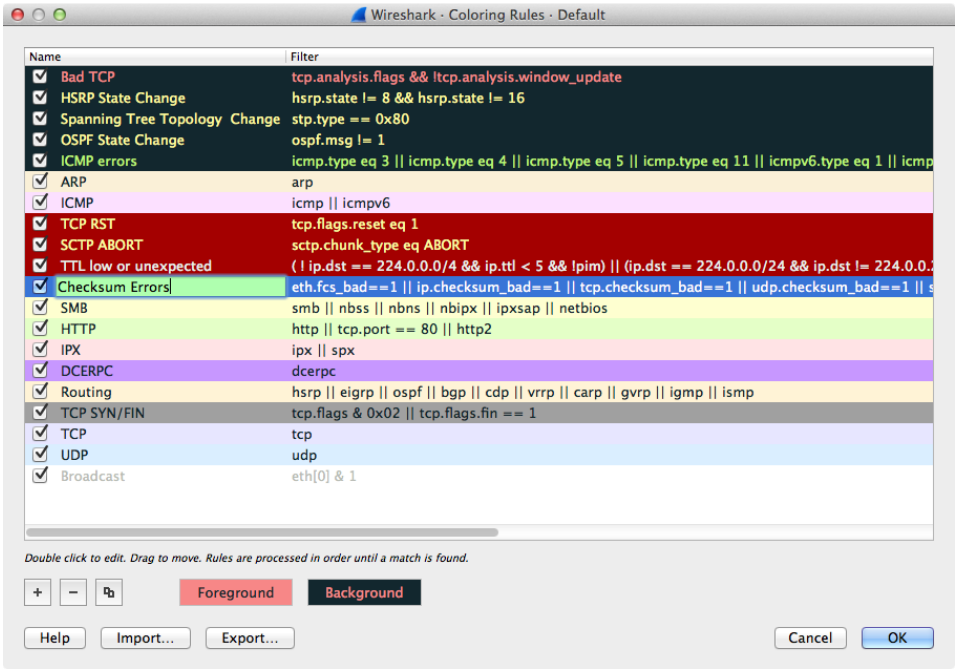
You can find a lot of coloring rule examples at the *Wireshark Wiki Coloring Rules page* at https://wiki.wireshark.org/ColoringRules.

There are two types of coloring rules in Wireshark: temporary rules that are only in effect until you quit the program, and permanent rules that are saved in a preference file so that they are available the next time you run Wireshark.

Temporary rules can be added by selecting a packet and pressing the **Ctrl** key together with one of the number keys. This will create a coloring rule based on the currently selected conversation. It will try to create a conversation filter based on TCP first, then UDP, then IP and at last Ethernet. Temporary filters can also be created by selecting the Colorize with Filter → Color X menu items when right-clicking in the packet detail pane.

To permanently colorize packets, select View → Coloring Rules…. Wireshark will display the "Coloring Rules" dialog box as shown in Figure 10.1, "The "Coloring Rules" dialog box".

Figure 10.1. The "Coloring Rules" dialog box



If this is the first time using the Coloring Rules dialog and you're using the default configuration profile you should see the default rules, shown above.

The first match wins

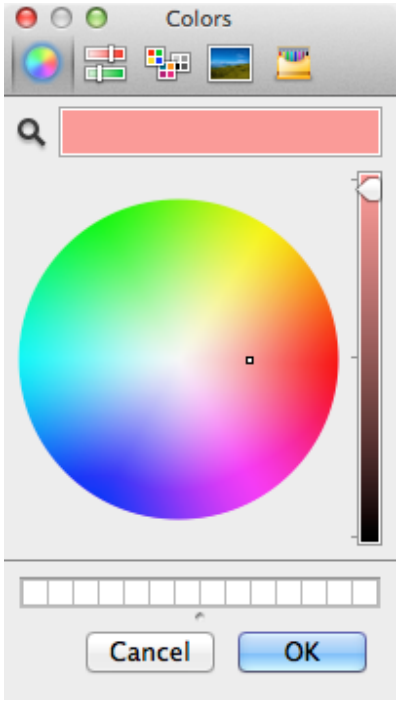
More specific rules should usually be listed before more general rules. For example, if you have a coloring rule for UDP before the one for DNS, the rule for DNS may not be applied (DNS is typically carried over UDP and the UDP rule will match first).

You can create a new rule by clicking on the + button. You can delete one or more rules by clicking the - button. The "copy" button will duplicate a rule.

You can edit a rule by double-clicking on its name or filter. In Figure 10.1, "The "Coloring Rules" dialog box" the name of the rule "Checksum Errors" is being edited. Clicking on the Foreground and Background

buttons will open a color chooser (Figure 10.2, “A color chooser”) for the foreground (text) and background colors respectively.

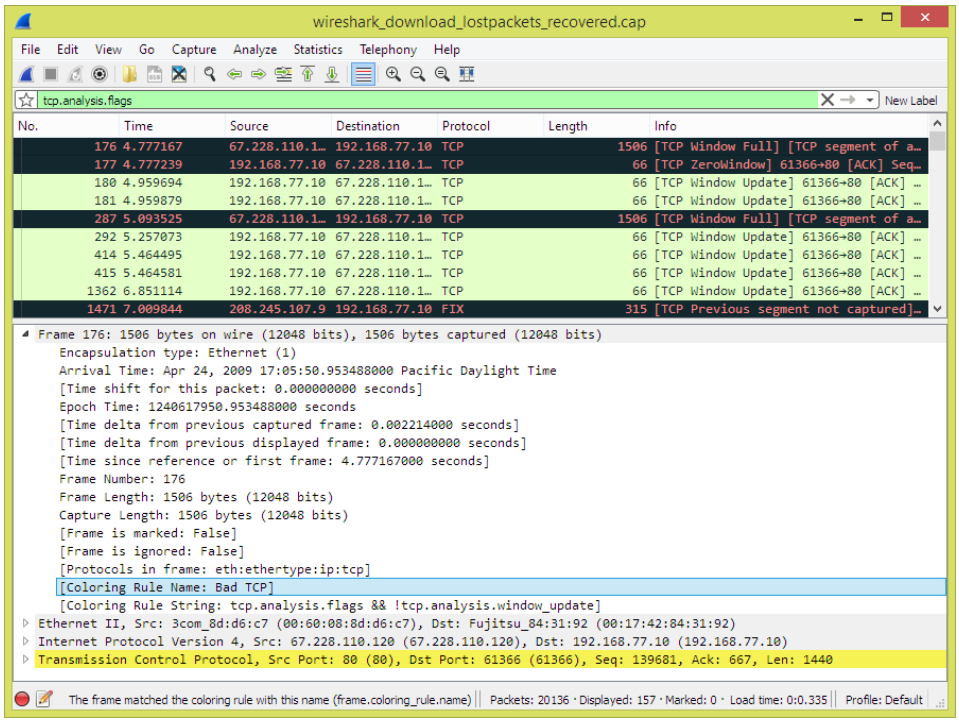
Figure 10.2. A color chooser



The color chooser appearance depends on your operating system. The OS X color picker is shown. Select the color you desire for the selected packets and click OK.

Figure 10.3, “Using color filters with Wireshark” shows an example of several color filters being used in Wireshark. Note that the frame detail shows that the “Bad TCP” rule rule was applied, along with the matching filter.

Figure 10.3. Using color filters with Wireshark



10.4. Control Protocol dissection

The user can control how protocols are dissected.

Each protocol has its own dissector, so dissecting a complete packet will typically involve several dissectors. As Wireshark tries to find the right dissector for each packet (using static “routes” and heuristics ``guessing"), it might choose the wrong dissector in your specific case. For example, Wireshark won’t know if you use a common protocol on an uncommon TCP port, e.g. using HTTP on TCP port 800 instead of the standard port 80.

There are two ways to control the relations between protocol dissectors: disable a protocol dissector completely or temporarily divert the way Wireshark calls the dissectors.

10.4.1. The “Enabled Protocols” dialog box

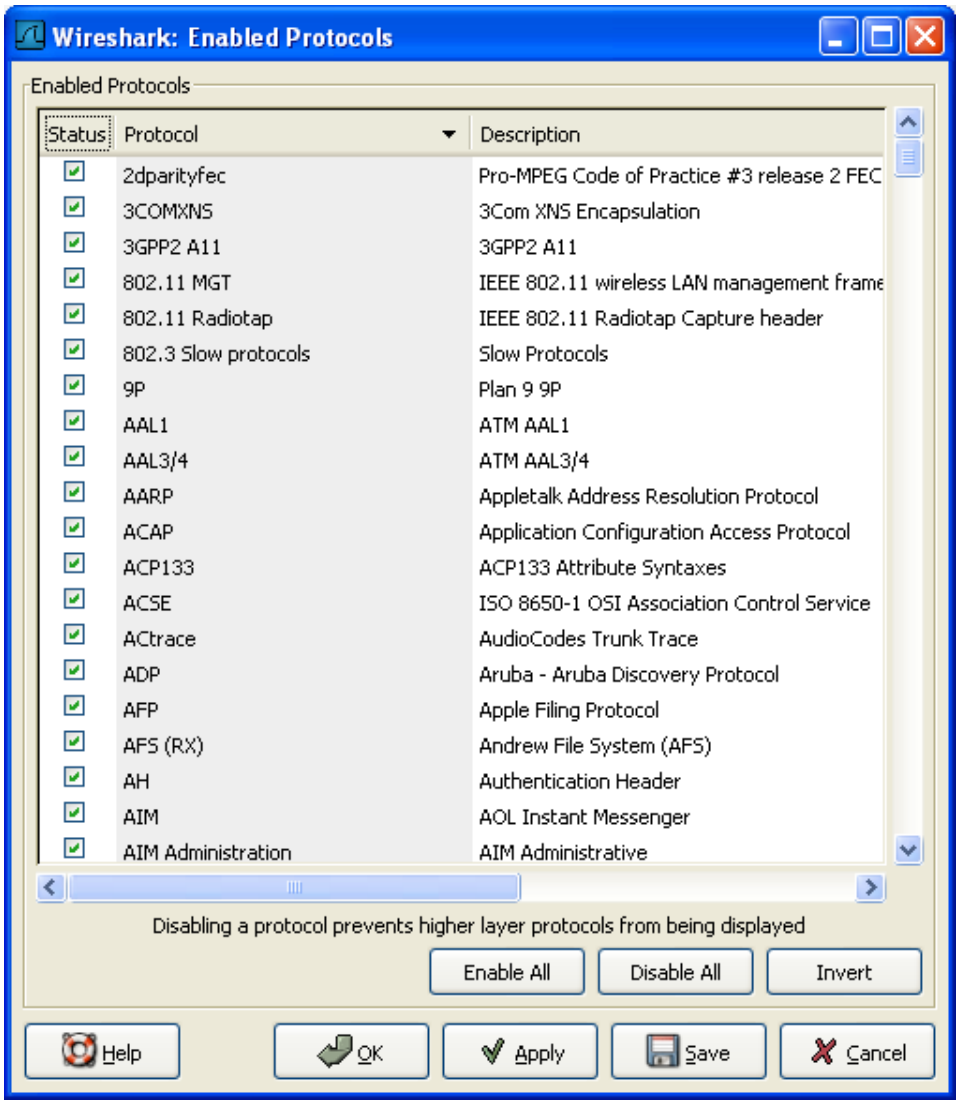
The Enabled Protocols dialog box lets you enable or disable specific protocols. All protocols are enabled by default. When a protocol is disabled, Wireshark stops processing a packet whenever that protocol is encountered.

Note

Disabling a protocol will prevent information about higher-layer protocols from being displayed. For example, suppose you disabled the IP protocol and selected a packet containing Ethernet, IP, TCP, and HTTP information. The Ethernet information would be displayed, but the IP, TCP and HTTP information would not - disabling IP would prevent it and the other protocols from being displayed.

To enable or disable protocols select Analyze → Enabled Protocols…. Wireshark will pop up the “Enabled Protocols” dialog box as shown in Figure 10.4, “The “Enabled Protocols” dialog box”.

Figure 10.4. The “Enabled Protocols” dialog box



To disable or enable a protocol, simply click on it using the mouse or press the space bar when the protocol is highlighted. Note that typing the first few letters of the protocol name when the Enabled Protocols dialog box is active will temporarily open a search text box and automatically select the first matching protocol name (if it exists).

You must use the Save button to save your settings. The OK or Apply buttons will not save your changes permanently and they will be lost when Wireshark is closed.

You can choose from the following actions:

1. Enable All: Enable all protocols in the list.
2. Disable All: Disable all protocols in the list.
3. Invert: Toggle the state of all protocols in the list.
4. OK: Apply the changes and close the dialog box.
5. Apply: Apply the changes and keep the dialog box open.

6. Save: Save the settings to the disabled_protos, see Appendix B, *Files and Folders* for details.

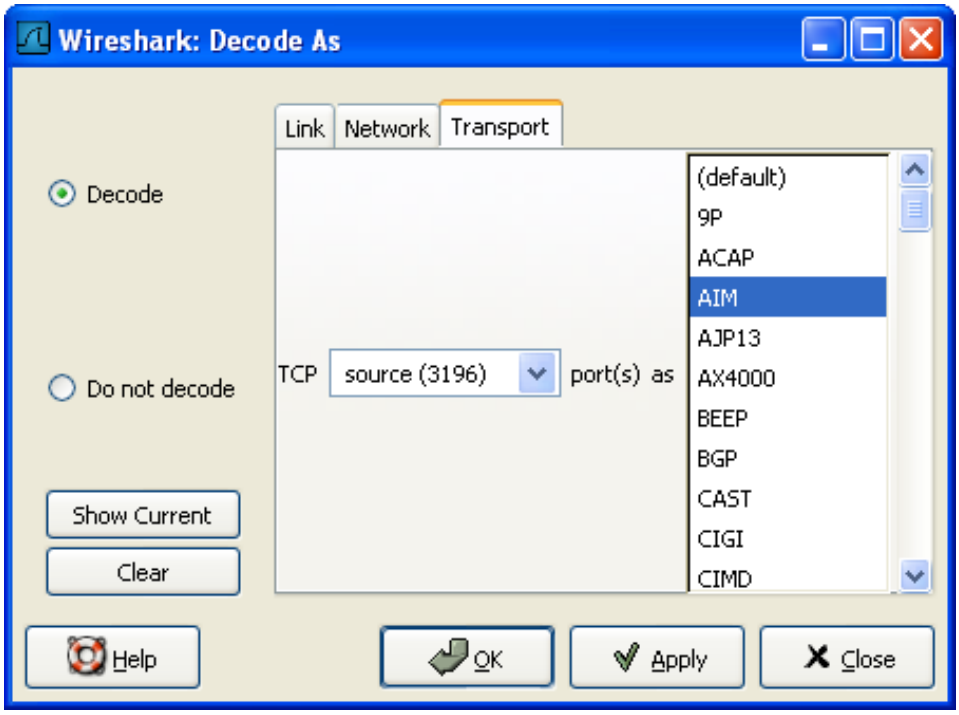
7. Cancel: Cancel the changes and close the dialog box.

10.4.2. User Specified Decodes

The “Decode As” functionality lets you temporarily divert specific protocol dissections. This might be useful for example, if you do some uncommon experiments on your network.

Decode As is accessed by selecting the Analyze → Decode As…. Wireshark will pop up the “Decode As” dialog box as shown in Figure 10.5, “The “Decode As” dialog box”.

Figure 10.5. The “Decode As” dialog box



The content of this dialog box depends on the selected packet when it was opened.

These settings will be lost if you quit Wireshark or change profile unless you save the entries in the *Show User Specified Decodes…* windows (Section 10.4.3, “Show User Specified Decodes”).

1. Decode: Decode packets the selected way.

2. Do not decode: Do not decode packets the selected way.

3. Link/Network/Transport: Specify the network layer at which “Decode As” should take place. Which of these pages are available depends on the content of the selected packet when this dialog box is opened.

4. Show Current: Open a dialog box showing the current list of user specified decodes.

5. OK: Apply the currently selected decode and close the dialog box.

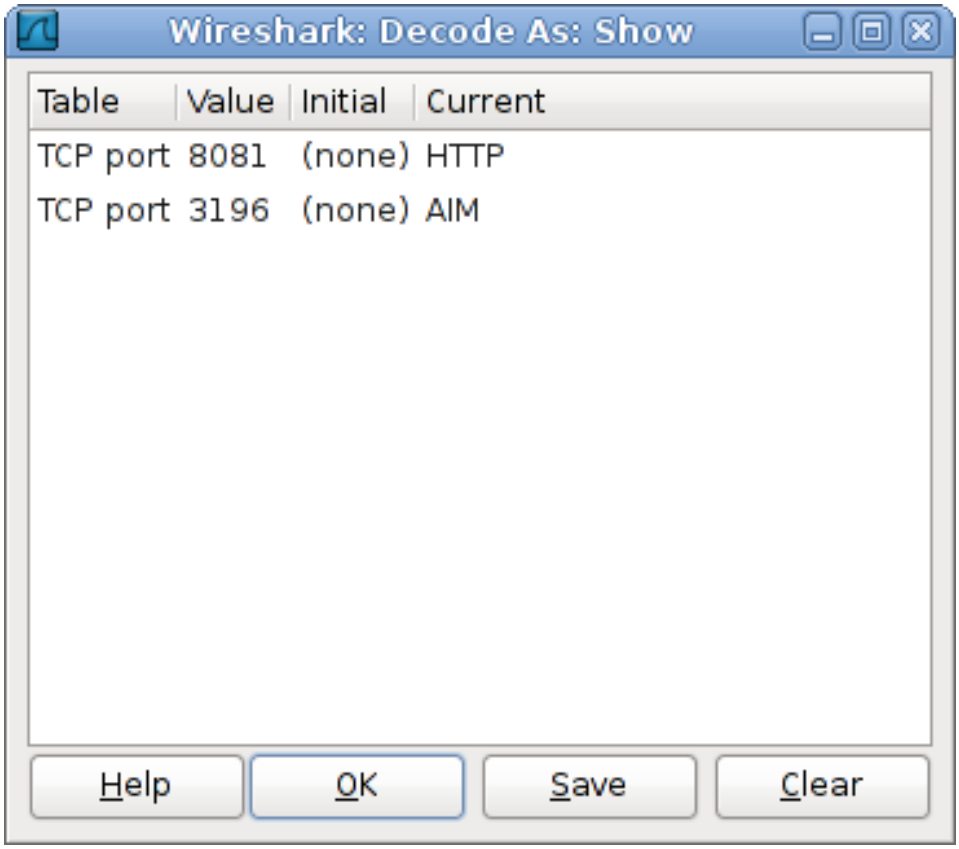
6. Apply: Apply the currently selected decode and keep the dialog box open.

7. Cancel: Cancel the changes and close the dialog box.

10.4.3. Show User Specified Decodes

This dialog box shows the currently active user specified decodes. These entries can be saved into current profile for later session.

Figure 10.6. The “Decode As: Show” dialog box



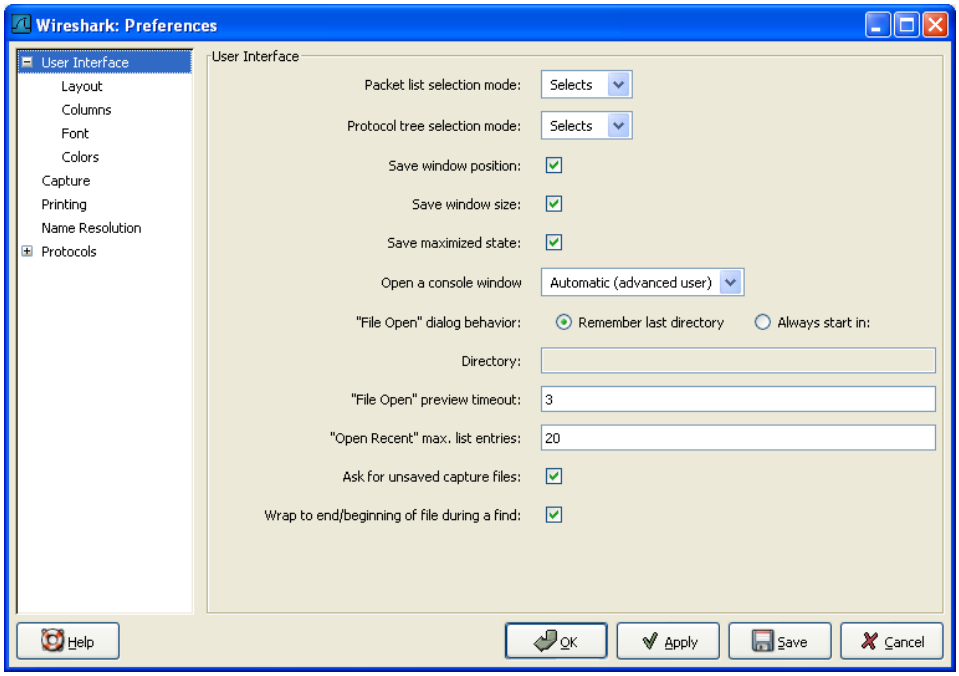
1. OK: Close this dialog box.
2. Save: Save the entries in the table into current profile.
3. Clear: Removes all user specified decodes without updating the profile.

10.5. Preferences

There are a number of preferences you can set. Simply select the Edit → Preferences… (Wireshark → Preferences… on OS X) and Wireshark will pop up the Preferences dialog box as shown in Figure 10.7, “The preferences dialog box”, with the “User Interface” page as default. On the left side is a tree where you can select the page to be shown.

- The OK button will apply the preferences settings and close the dialog.
- The Apply button will apply the preferences settings and keep the dialog open.
- The Cancel button will restore all preferences settings to the last saved state.

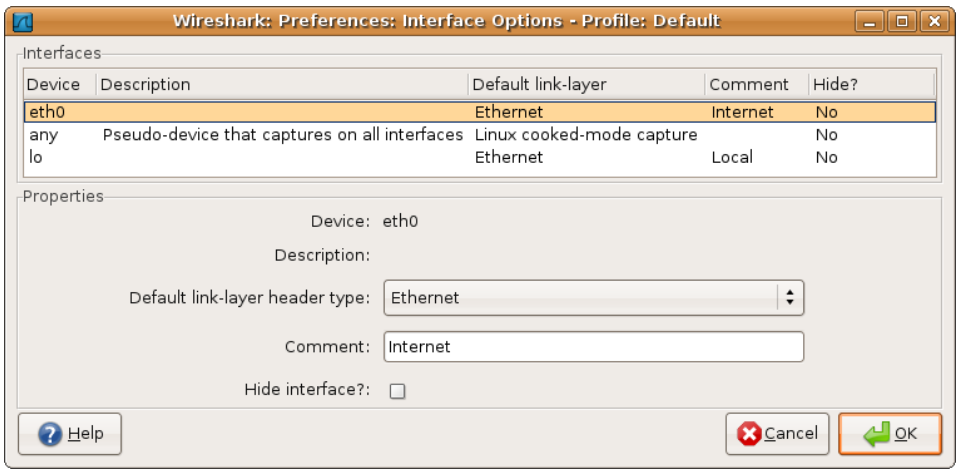
Figure 10.7. The preferences dialog box



10.5.1. Interface Options

In the “Capture” preferences it is possible to configure several options for the interfaces available on your computer. Select the “Capture” pane and press the Edit button. In this window it is possible to change the default link-layer header type for the interface, add a comment or choose to hide a interface from other parts of the program.

Figure 10.8. The interface options dialog box



Each row contains options for each interface available on your computer.

- Device: the device name provided by the operating system.
- Description: provided by the operating system.

- Default link-layer: each interface may provide several link-layer header types. The default link-layer chosen here is the one used when you first start Wireshark. It is also possible to change this value in Section 4.5, “The “Capture Options” dialog box” when you start a capture. For a detailed description, see Section 4.12, “Link-layer header type”.
- Comment: a user provided description of the interface. This comment will be used as a description instead of the operating system description.
- Hide?: enable this option to hide the interface from other parts of the program.

10.6. Configuration Profiles

Configuration Profiles can be used to configure and use more than one set of preferences and configurations. Select the *Configuration Profiles…* menu item from the *Edit* menu, or simply press Shift-Ctrl-A; and Wireshark will pop up the Configuration Profiles dialog box as shown in Figure 10.9, “The configuration profiles dialog box”. It is also possible to click in the “Profile” part of the statusbar to popup a menu with available Configuration Profiles (Figure 3.22, “The Statusbar with a configuration profile menu”).

Configuration files stored in the Profiles:

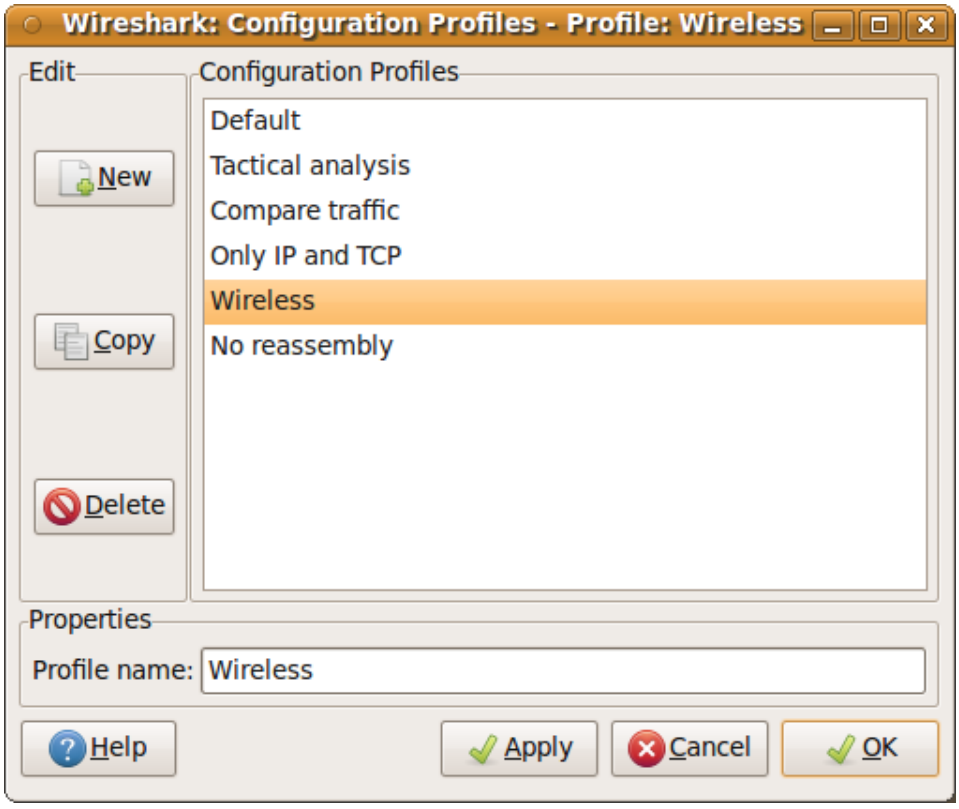
- Preferences (preferences) (Section 10.5, “Preferences”)
- Capture Filters (cfilters) (Section 6.6, “Defining and saving filters”)
- Display Filters (dfilters) (Section 6.6, “Defining and saving filters”)
- Coloring Rules (colorfilters) (Section 10.3, “Packet colorization”)
- Disabled Protocols (disabled_protos) (Section 10.4.1, “The “Enabled Protocols” dialog box”)
- User Accessible Tables:
  - Custom HTTP headers (custom_http_header_fields)
  - Custom IMF headers (imf_header_fields)
  - Custom LDAP AttributeValue types (custom_ldap_attribute_types)
  - Display Filter Macros (dfilter_macros) (Section 10.8, “Display Filter Macros”)
  - ESS Category Attributes (ess_category_attributes) (Section 10.9, “ESS Category Attributes”)
  - GeoIP Database Paths (geoip_db_paths) (Section 10.10, “GeoIP Database Paths”)
  - K12 Protocols (k12_protos) (Section 10.19, “Tektronix K12xx/15 RF5 protocols Table”)
  - Object Identifier Names and Associated Syntaxes (Section 10.12, “Object Identifiers”)
  - PRES Users Context List (pres_context_list) (Section 10.13, “PRES Users Context List”)
  - SCCP Users Table (sccp_users) (Section 10.14, “SCCP users Table”)
  - SNMP Enterprise Specific Trap Types (snmp_specific_traps) (Section 10.17, “SNMP Enterprise Specific Trap Types”)
  - SNMP Users (snmp_users) (Section 10.18, “SNMP users Table”)

- User DLTs Table (user_dlts) (Section 10.20, “User DLTs protocol table”)
- IKEv2 decryption table (ikev2_decryption_table) (Section 10.11, “IKEv2 decryption table”)

- Changed dissector assignments (decode_as_entries), which can be set in *Decode As…* dialog box (Section 10.4.2, “User Specified Decodes”), and further saved in the *User Specified Decodes…* window (Section 10.4.3, “Show User Specified Decodes”).
- Some recent settings (recent), such as pane sizes in the Main window (Section 3.3, “The Main window”), column widths in the packet list (Section 3.18, “The “Packet List” pane”), all selections in the “View” menu (Section 3.7, “The “View” menu”) and the last directory navigated to in the File Open dialog.

All other configurations are stored in the personal configuration folder, and are common to all profiles.

Figure 10.9. The configuration profiles dialog box



New
: This button adds a new profile to the profiles list. The name of the created profile is “New profile” and can be changed in the Properties field.

Copy
: This button adds a new profile to the profiles list, copying all configuration from the profile currently selected in the list. The name of the created profile is the same as the copied profile, with the text “(copy)” applied. The name can be changed in the Properties field.

Delete
: This button deletes the selected profile, including all configuration files used in this profile. It is not possible to delete the “Default” profile.

Configuration Profiles
: You can select a configuration profile from this list (which will fill in the profile name in the fields down at the bottom of the dialog box).

Profile name
: You can change the name of the currently selected profile here.

  The profile name will be used as a folder name in the configured “Personal configurations” folder. If adding multiple profiles with the same name, only one profile will be created.

  On Windows the profile name cannot start or end with a period (.), and cannot contain any of the following characters: ‘\’, ‘/’, ‘:’, ‘*’, ‘?’, ‘`’, ‘<’, ‘>’, ‘|’, or ‘+’. On Unix the profile name cannot contain the ‘/’ character.

OK
: This button saves all changes, applies the selected profile and closes the dialog.

Apply
: This button saves all changes, applies the selected profile and keeps the dialog open.

Cancel
: Close this dialog. This will discard unsaved settings, new profiles will not be added and deleted profiles will not be deleted.

Help
: Show this help page.

10.7. User Table

The User Table editor is used for managing various tables in wireshark. Its main dialog works very similarly to that of Section 10.3, “Packet colorization”.

10.8. Display Filter Macros

Display Filter Macros are a mechanism to create shortcuts for complex filters. For example defining a display filter macro named *tcp_conv* whose text is *((ip.src == $1 and ip.dst == $2 and tcp.srcport == $3 and tcp.dstport == $4) or (ip.src == $2 and ip.dst == $1 and tcp.srcport == $4 and tcp.dstport == $3))* would allow to use a display filter like *${tcp_conv:10.1.1.2;10.1.1.3;1200;1400}* instead of typing the whole filter.

Display Filter Macros can be managed with a Section 10.7, “User Table” by selecting Analyze → Display Filter Macros from the menu. The User Table has the following fields

Name
: The name of the macro.

Text
: The replacement text for the macro it uses $1, $2, $3, … as the input arguments.

10.9. ESS Category Attributes

Wireshark uses this table to map ESS Security Category attributes to textual representations. The values to put in this table are usually found in a XML SPIF, which is used for defining security labels.

This table is handled by an Section 10.7, “User Table” with the following fields.

Tag Set
: An Object Identifier representing the Category Tag Set.

Value
: The value (Label And Cert Value) representing the Category.

Name
: The textual representation for the value.

10.10. GeoIP Database Paths

If your copy of Wireshark supports MaxMind’s GeoIP library, you can use their databases to match IP addresses to countries, cites, autonomous system numbers, ISPs, and other bits of information. Some databases are available at no cost, while others require a licensing fee. See the MaxMind web site for more information.

This table is handled by an Section 10.7, “User Table” with the following fields.

Database pathname
: This specifies a directory containing GeoIP data files. Any files beginning with *Geo* and ending with *.dat* will be automatically loaded. A total of 8 files can be loaded.

  The locations for your data files are up to you, but `/usr/share/GeoIP` (Linux), `C:\GeoIP` (Windows), `C:\Program Files\Wireshark\GeoIP` (Windows) might be good choices.

10.11. IKEv2 decryption table

Wireshark can decrypt Encrypted Payloads of IKEv2 (Internet Key Exchange version 2) packets if necessary information is provided. Note that you can decrypt only IKEv2 packets with this feature. If you want to decrypt IKEv1 packets or ESP packets, use Log Filename setting under ISAKMP protocol preference or settings under ESP protocol preference respectively.

This table is handled by an Section 10.7, “User Table” with the following fields.

Initiator’s SPI
: Initiator’s SPI of the IKE_SA. This field takes hexadecimal string without “0x” prefix and the length must be 16 hex chars (represents 8 octets).

Responder’s SPI
: Responder’s SPI of the IKE_SA. This field takes hexadecimal string without “0x” prefix and the length must be 16 hex chars (represents 8 octets).

SK_ei
: Key used to encrypt/decrypt IKEv2 packets from initiator to responder. This field takes hexadecimal string without “0x” prefix and its length must meet the requirement of the encryption algorithm selected.

SK_er
: Key used to encrypt/decrypt IKEv2 packets from responder to initiator. This field takes hexadecimal string without “0x” prefix and its length must meet the requirement of the encryption algorithm selected.

Encryption Algorithm
: Encryption algorithm of the IKE_SA.

SK_ai
: Key used to calculate Integrity Checksum Data for IKEv2 packets from responder to initiator. This field takes hexadecimal string without “0x” prefix and its length must meet the requirement of the integrity algorithm selected.

SK_ar
: Key used to calculate Integrity Checksum Data for IKEv2 packets from initiator to responder. This field takes hexadecimal string without “0x” prefix and its length must meet the requirement of the integrity algorithm selected.

Integrity Algorithm
: Integrity algorithm of the IKE_SA.

10.12. Object Identifiers

Many protocols that use ASN.1 use Object Identifiers (OIDs) to uniquely identify certain pieces of information. In many cases, they are used in an extension mechanism so that new object identifiers (and associated values) may be defined without needing to change the base standard.

Whilst Wireshark has knowledge about many of the OIDs and the syntax of their associated values, the extensibility means that other values may be encountered.

Wireshark uses this table to allow the user to define the name and syntax of Object Identifiers that Wireshark does not know about (for example, a privately defined X.400 extension). It also allows the user to override the name and syntax of Object Identifiers that Wireshark does know about (e.g. changing the name “id-at-countryName” to just “c”).

This table is handled by an Section 10.7, “User Table” with the following fields.

OID
: The string representation of the Object Identifier e.g. “2.5.4.6”.

Name
: The name that should be displayed by Wireshark when the Object Identifier is dissected e.g. (*c*);

Syntax
: The syntax of the value associated with the Object Identifier. This must be one of the syntaxes that Wireshark already knows about (e.g. “PrintableString”).

10.13. PRES Users Context List

Wireshark uses this table to map a presentation context identifier to a given object identifier when the capture does not contain a PRES package with a presentation context definition list for the conversation.

This table is handled by an Section 10.7, “User Table” with the following fields.

Context Id
: An Integer representing the presentation context identifier for which this association is valid.

Syntax Name OID
: The object identifier representing the abstract syntax name, which defines the protocol that is carried over this association.

10.14. SCCP users Table

Wireshark uses this table to map specific protocols to a certain DPC/SSN combination for SCCP.

This table is handled by an Section 10.7, “User Table” with the following fields.

Network Indicator
: An Integer representing the network indicator for which this association is valid.

Called DPCs
: An range of integers representing the dpcs for which this association is valid.

Called SSNs
: An range of integers representing the ssns for which this association is valid.

User protocol
: The protocol that is carried over this association

10.15. SMI (MIB and PIB) Modules

If your copy of Wireshark supports libSMI, you can specify a list of MIB and PIB modules here. The COPS and SNMP dissectors can use them to resolve OIDs.

Module name
: The name of the module, e.g. IF-MIB.

10.16. SMI (MIB and PIB) Paths

If your copy of Wireshark supports libSMI, you can specify one or more paths to MIB and PIB modules here.

Directory name
: A module directory, e.g. `/usr/local/snmp/mibs`. Wireshark automatically uses the standard SMI path for your system, so you usually don’t have to add anything here.

10.17. SNMP Enterprise Specific Trap Types

Wireshark uses this table to map specific-trap values to user defined descriptions in a Trap PDU. The description is shown in the packet details specific-trap element.

This table is handled by an Section 10.7, “User Table” with the following fields.

Enterprise OID
: The object identifier representing the object generating the trap.

Trap Id
: An Integer representing the specific-trap code.

Description
: The description to show in the packet details.

10.18. SNMP users Table

Wireshark uses this table to verify authentication and to decrypt encrypted SNMPv3 packets.

This table is handled by an Section 10.7, “User Table” with the following fields.

Engine ID
: If given this entry will be used only for packets whose engine id is this. This field takes an hexadecimal string in the form 0102030405.

Username
: This is the userName. When a single user has more than one password for different SNMP-engines the first entry to match both is taken, if you need a catch all engine-id (empty) that entry should be the last one.

Authentication model
: Which auth model to use (either “MD5” or “SHA1”).

Password
: The authentication password. Use *\xDD* for unprintable characters. An hexadecimal password must be entered as a sequence of *\xDD* characters. For example the hex password 010203040506 must be entered as *\x01\x02\x03\x04\x05\x06*. The \ character must be treated as an unprintable character, i.e. it must be entered as *\x5C* or *\x5c*.

Privacy protocol
: Which encryption algorithm to use (either “DES” or ``AES").

Privacy password
: The privacy password. Use *\xDD* for unprintable characters. An hexadecimal password must be entered as a sequence of *\xDD* characters. For example the hex password 010203040506 must be entered as *\x01\x02\x03\x04\x05\x06*. The \ character must be treated as an unprintable character, i.e. it must be entered as *\x5C* or *\x5c*.

10.19. Tektronix K12xx/15 RF5 protocols Table

The Tektronix K12xx/15 rf5 file format uses helper files (*.stk) to identify the various protocols that are used by a certain interface. Wireshark doesn’t read these stk files, it uses a table that helps it identify which lowest layer protocol to use.

Stk file to protocol matching is handled by an Section 10.7, “User Table” with the following fields.

Match string
: A partial match for an stk filename, the first match wins, so if you have a specific case and a general one the specific one must appear first in the list.

Protocol
: This is the name of the encapsulating protocol (the lowest layer in the packet data) it can be either just the name of the protocol (e.g. mtp2, eth_witoutfcs, sscf-nni) or the name of the encapsulation protocol and the “application” protocol over it separated by a colon (e.g sscop:sscf-nni, sscop:alcap, sscop:nbap, …)

10.20. User DLTs protocol table

When a pcap file uses one of the user DLTs (147 to 162) wireshark uses this table to know which protocol(s) to use for each user DLT.

This table is handled by an Section 10.7, “User Table” with the following fields.

DLT
: One of the user dlts.

Payload protocol
: This is the name of the payload protocol (the lowest layer in the packet data). (e.g. “eth” for ethernet, “ip” for IPv4)

Header size
: If there is a header protocol (before the payload protocol) this tells which size this header is. A value of 0 disables the header protocol.

Header protocol
: The name of the header protocol to be used (uses “data” as default).

Trailer size
: If there is a trailer protocol (after the payload protocol) this tells which size this trailer is. A value of 0 disables the trailer protocol.

Trailer protocol
: The name of the trailer protocol to be used (uses “data” as default).

Appendix A. Wireshark Messages

Wireshark provides you with additional information generated out of the plain packet data or it may need to indicate dissection problems. Messages generated by Wireshark are usually placed in square brackets ("[]").

A.1. Packet List Messages

These messages might appear in the packet list.

A.1.1. [Malformed Packet]

Malformed packet means that the protocol dissector can't dissect the contents of the packet any further. There can be various reasons:

- *Wrong dissector*: Wireshark erroneously has chosen the wrong protocol dissector for this packet. This will happen e.g. if you are using a protocol not on its well known TCP or UDP port. You may try Analyze|Decode As to circumvent this problem.
- *Packet not reassembled*: The packet is longer than a single frame and it is not reassembled, see Section 7.7, "Packet Reassembly" for further details.
- *Packet is malformed*: The packet is actually wrong (malformed), meaning that a part of the packet is just not as expected (not following the protocol specifications).
- *Dissector is buggy*: The corresponding protocol dissector is simply buggy or still incomplete.

Any of the above is possible. You'll have to look into the specific situation to determine the reason. You could disable the dissector by disabling the protocol on the Analyze menu and check how Wireshark displays the packet then. You could (if it's TCP) enable reassembly for TCP and the specific dissector (if possible) in the Edit|Preferences menu. You could check the packet contents yourself by reading the packet bytes and comparing it to the protocol specification. This could reveal a dissector bug. Or you could find out that the packet is indeed wrong.

A.1.2. [Packet size limited during capture]

The packet size was limited during capture, see "Limit each packet to n bytes" at the Section 4.5, "The "Capture Options" dialog box". While dissecting, the current protocol dissector was simply running out of packet bytes and had to give up. There's nothing else you can do now, except to repeat the whole capture process again with a higher (or no) packet size limitation.

A.2. Packet Details Messages

These messages might appear in the packet details.

A.2.1. [Response in frame: 123]

The current packet is the request of a detected request/response pair. You can directly jump to the corresponding response packet just by double clicking on this message.

A.2.2. [Request in frame: 123]

Same as “Response in frame: 123” above, but the other way round.

A.2.3. [Time from request: 0.123 seconds]

The time between the request and the response packets.

A.2.4. [Stream setup by PROTOCOL (frame 123)]

The session control protocol (SDP, H225, etc) message which signaled the creation of this session. You can directly jump to the corresponding packet just by double clicking on this message.

Appendix B. Files and Folders

B.1. Capture Files

To understand which information will remain available after the captured packets are saved to a capture file, it's helpful to know a bit about the capture file contents.

Wireshark uses the pcapng file format as the default format to save captured packets. It is very flexible but other tools may not support it.

Wireshark also supports the libpcap file format. This is a much simpler format and is well established. However, it has some drawbacks: it's not extensible and lacks some information that would be really helpful (e.g. being able to add a comment to a packet such as "the problems start here" would be really nice).

In addition to the libpcap format, Wireshark supports several different capture file formats. However, the problems described above also applies for these formats.

B.1.1. Libpcap File Contents

At the start of each libpcap capture file some basic information is stored like a magic number to identify the libpcap file format. The most interesting information of this file start is the link layer type (Ethernet, 802.11, MPLS, etc).

The following data is saved for each packet:

- The timestamp with millisecond resolution
- The packet length as it was "on the wire"
- The packet length as it's saved in the file
- The packet's raw bytes

A detailed description of the libpcap file format can be found at: https://wiki.wireshark.org/Development/LibpcapFileFormat

B.1.2. Not Saved in the Capture File

You should also know the things that are *not saved* in capture files:

- Current selections (selected packet, …)
- Name resolution information. See Section 7.8, "Name Resolution" for details

  Pcapng files can optionally save name resolution information. Libpcap files can't. Other file formats have varying levels of support.
- The number of packets dropped while capturing
- Packet marks set with "Edit/Mark Packet"
- Time references set with "Edit/Time Reference"
- The current display filter

B.2. Configuration Files and Folders

Wireshark uses a number of files and folders while it is running. Some of these reside in the personal configuration folder and are used to maintain information between runs of Wireshark, while some of them are maintained in system areas.

Tip

A list of the folders Wireshark actually uses can be found under the *Folders* tab in the dialog box shown when you select *About Wireshark* from the *Help* menu.

The content format of the configuration files is the same on all platforms. However, to match the different policies for Unix and Windows platforms, different folders are used for these files.

Table B.1. Configuration files and folders overview

File/Folder	Description	Unix/Linux folders	Windows folders
preferences	Settings from the Preferences dialog box.	/etc/wireshark.conf, $HOME/.wireshark/ preferences	%WIRESHARK %\wireshark.conf, %APPDATA% \Wireshark\preferences
recent	Recent GUI settings (e.g. recent files lists).	$HOME/.wireshark/ recent	%APPDATA% \Wireshark\recent
cfilters	Capture filters.	$HOME/.wireshark/ cfilters	%WIRESHARK% \cfilters, %APPDATA% \Wireshark\cfilters
dfilters	Display filters.	$HOME/.wireshark/ dfilters	%WIRESHARK% \dfilters, %APPDATA% \Wireshark\dfilters
colorfilters	Coloring rules.	$HOME/.wireshark/ colorfilters	%WIRESHARK %\colorfilters, %APPDATA% \Wireshark\colorfilters
disabled_protos	Disabled protocols.	$HOME/.wireshark/ disabled_protos	%WIRESHARK% \disabled_protos, %APPDATA %\Wireshark \disabled_protos
ethers	Ethernet name resolution.	/etc/ethers, $HOME/.wireshark/ ethers	%WIRESHARK% \ethers, %APPDATA% \Wireshark\ethers
manuf	Ethernet name resolution.	/etc/manuf, $HOME/.wireshark/ manuf	%WIRESHARK% \manuf, %APPDATA% \Wireshark\manuf
hosts	IPv4 and IPv6 name resolution.	/etc/hosts, $HOME/.wireshark/ hosts	%WIRESHARK% \hosts, %APPDATA% \Wireshark\hosts
services	Network services.	/etc/services, $HOME/.wireshark/ services	%WIRESHARK% \services, %APPDATA %\Wireshark\services

File/Folder	Description	Unix/Linux folders	Windows folders
subnets	IPv4 subnet name resolution.	/etc/subnets, $HOME/.wireshark/subnets	%WIRESHARK%\subnets, %APPDATA%\Wireshark\subnets
ipxnets	IPX name resolution.	/etc/ipxnets, $HOME/.wireshark/ipxnets	%WIRESHARK%\ipxnets, %APPDATA%\Wireshark\ipxnets
vlans	VLAN ID name resolution.	$HOME/.wireshark/vlans	%APPDATA%\Wireshark\vlans
plugins	Plugin directories.	/usr/share/wireshark/plugins, /usr/local/share/wireshark/plugins, $HOME/.wireshark/plugins	%WIRESHARK%\plugins\<version>, %APPDATA%\Wireshark\plugins
temp	Temporary files.	Environment: TMPDIR	Environment: TMPDIR or TEMP

Windows folders

%APPDATA% points to the personal configuration folder, e.g.: *C:\Documents and Settings\<username>\Application Data* (details can be found at: Section B.3.1, “Windows profiles”),

%WIRESHARK% points to the Wireshark program folder, e.g.: *C:\Program Files\Wireshark*

Unix/Linux folders

The */etc* folder is the global Wireshark configuration folder. The folder actually used on your system may vary, maybe something like: */usr/local/etc*.

$HOME is usually something like: */home/<username>*

File contents

preferences/wireshark.conf

This file contains your Wireshark preferences, including defaults for capturing and displaying packets. It is a simple text file containing statements of the form:

```
variable: value
```

The settings from this file are read in at program start and written to disk when you press the Save button in the “Preferences” dialog box.

recent

This file contains various GUI related settings like the main window position and size, the recent files list and such. It is a simple text file containing statements of the form:

```
variable: value
```

It is read at program start and written at program exit.

cfilters

This file contains all the capture filters that you have defined and saved. It consists of one or more lines, where each line has the following format:

```
"<filter name>" <filter string>
```

The settings from this file are read in at program start and written to disk when you press the Save button in the “Capture Filters” dialog box.

dfilters

This file contains all the display filters that you have defined and saved. It consists of one or more lines, where each line has the following format:

```
"<filter name>" <filter string>
```

The settings from this file are read in at program start and written to disk when you press the Save button in the “Display Filters” dialog box.

colorfilters

This file contains all the color filters that you have defined and saved. It consists of one or more lines, where each line has the following format:

```
@<filter name>@<filter string>@[<bg RGB(16-bit)>][<fg RGB(16-bit)>]
```

The settings from this file are read in at program start and written to disk when you press the Save button in the “Coloring Rules” dialog box.

disabled_protos

Each line in this file specifies a disabled protocol name. The following are some examples:

```
tcp
udp
```

The settings from this file are read in at program start and written to disk when you press the Save button in the “Enabled Protocols” dialog box.

ethers

When Wireshark is trying to translate Ethernet hardware addresses to names, it consults the files listed in Table B.1, “Configuration files and folders overview”. If an address is not found in /etc/ethers, Wireshark looks in $HOME/.wireshark/ethers

Each line in these files consists of one hardware address and name separated by whitespace. The digits of hardware addresses are separated by colons (:), dashes (-) or periods(.). The following are some examples:

```
ff-ff-ff-ff-ff-ff    Broadcast
c0-00-ff-ff-ff-ff    TR_broadcast
00.2b.08.93.4b.a1    Freds_machine
```

The settings from this file are read in at program start and never written by Wireshark.

manuf

Wireshark uses the files listed in Table B.1, “Configuration files and folders overview” to translate the first three bytes of an Ethernet address into a manufacturers name. This file has the same format as the ethers file, except addresses are three bytes long.

An example is:

```
00:00:01    Xerox                   # XEROX CORPORATION
```

The settings from this file are read in at program start and never written by Wireshark.

hosts

Wireshark uses the files listed in Table B.1, “Configuration files and folders overview” to translate IPv4 and IPv6 addresses into names.

This file has the same format as the usual /etc/hosts file on Unix systems.

An example is:

```
# Comments must be prepended by the # sign!
192.168.0.1 homeserver
```

The settings from this file are read in at program start and never written by Wireshark.

services

Wireshark uses the files listed in Table B.1, “Configuration files and folders overview” to translate port numbers into names.

An example is:

```
mydns       5045/udp     # My own Domain Name Server
mydns       5045/tcp     # My own Domain Name Server
```

The settings from this file are read in at program start and never written by Wireshark.

subnets

Wireshark uses the files listed in Table B.1, “Configuration files and folders overview” to translate an IPv4 address into a subnet name. If no exact match from the hosts file or from DNS is found, Wireshark will attempt a partial match for the subnet of the address.

Each line of this file consists of an IPv4 address, a subnet mask length separated only by a / and a name separated by whitespace. While the address must be a full IPv4 address, any values beyond the mask length are subsequently ignored.

An example is:

```
# Comments must be prepended by the # sign!
192.168.0.0/24 ws_test_network
```

A partially matched name will be printed as “subnet-name.remaining-address”. For example, “192.168.0.1” under the subnet above would be printed as “ws_test_network.1"; if the mask length above had been 16 rather than 24, the printed address would be ``ws_test_network.0.1”.

The settings from this file are read in at program start and never written by Wireshark.

ipxnets

Wireshark uses the files listed in Table B.1, “Configuration files and folders overview” to translate IPX network numbers into names.

An example is:

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

The settings from this file are read in at program start and never written by Wireshark.

vlans

Wireshark uses the files listed in Table B.1, “Configuration files and folders overview” to translate VLAN tag IDs into names.

Each line in this file consists of one VLAN tag ID and a describing name separated by whitespace or tab.

An example is:

```
123     Server-LAN
2049    HR-Client-LAN
```

The settings from this file are read in at program start and never written by Wireshark.

plugins folder
: Wireshark searches for plugins in the directories listed in Table B.1, “Configuration files and folders overview”. They are searched in the order listed.

temp folder
: If you start a new capture and don’t specify a filename for it, Wireshark uses this directory to store that file; see Section 4.11, “Capture files and file modes”.

B.2.1. Protocol help configuration

Wireshark can use configuration files to create context-sensitive menu items for protocol detail items which will load help URLs in your web browser.

To create a protocol help file, create a folder named “protocol_help” in either the personal or global configuration folders. Then create a text file with the extension “.ini” in the “protocol_help” folder. The file must contain key-value pairs with the following sections:

[database]
: Mandatory. This contains initialization information for the help file. The following keys must be defined:

  source
  : Source name, e.g. “HyperGlobalMegaMart”

  version
  : Must be “1”.

  location
  : General URL for help items. Variables can be substituted using the [location data] section below.

[location data]
: Optional. Contains keys that will be used for variable substitution in the “location” value. For example, if the database section contains

  ```
  location = http://www.example.com/proto?cookie=${cookie}&amp;path=${PATH}
  ```

  then setting

  ```
  cookie = anonymous-user-1138
  ```

  will result in the URL PATH is used for help path substitution, and shouldn’t be defined in this section.

[map]
: Maps Wireshark protocol names to section names below. Each key MUST match a valid protocol name such as “ip”. Each value MUST have a matching section defined in the configuration file.

Each protocol section must contain an “_OVERVIEW” key which will be used as the first menu item for the help source. Subsequent keys must match descriptions will be appended to the location.

Suppose the file *C:\Users\sam.clemens\AppData\Roaming\Wireshark\protocol_help\wikipedia.ini* contains the following:

```
# Wikipedia (en) protocol help file.
```

```
# Help file initialization
# source: The source of the help information, e.g. ``Inacon'' or ``Wikipedia"
# version: Currently unused. Must be ``1''.
# url_template: Template for generated URLs. See ``URL Data'' below.
[database]
source=Wikipedia
version=1
url_template=https://${language}.wikipedia.org/wiki/${PATH}

# Substitution data for the location template.
# Each occurrence of the keys below in the location template will be
# substituted with their corresponding values. For example, ``${license}"
# in the URL template above will be replaced with the value of ``license"
# below.
#
# PATH is reserved for the help paths below; do not specify it here.
[location data]
language = en

# Maps Wireshark protocol names to section names below. Each key MUST match
# a valid protocol name. Each value MUST have a matching section below.
[map]
tcp=TCP

# Mapped protocol sections.
# Keys must match protocol detail items descriptions.
[TCP]
_OVERVIEW=Transmission_Control_Protocol
Destination port=Transmission_Control_Protocol#TCP_ports
Source port=Transmission_Control_Protocol#TCP_ports
```

Right-clicking on a TCP protocol detail item will display a help menu item that displays the Wikipedia page for TCP. Right-clicking on the TCP destination or source ports will display additional help menu items that take you to the “TCP ports” section of the page.

example, the following configuration is functionally equivalent to the previous configuration:

```
[database]
source=Wikipedia
version=1
location=https://en.wikipedia.org/wiki/

[map]
tcp=TCP

[TCP]
_OVERVIEW=Transmission_Control_Protocol
Destination port=Transmission_Control_Protocol#TCP_ports
Source port=Transmission_Control_Protocol#TCP_ports
```

B.3. Windows folders

Here you will find some details about the folders used in Wireshark on different Windows versions.

As already mentioned, you can find the currently used folders in the *About Wireshark* dialog.

B.3.1. Windows profiles

Windows uses some special directories to store user configuration files which define the “user profile”. This can be confusing, as the default directory location changed from Windows version to version and might also be different for English and internationalized versions of Windows.

Note

If you've upgraded to a new Windows version, your profile might be kept in the former location. The defaults mentioned here might not apply.

The following guides you to the right place where to look for Wireshark's profile data.

Windows 8, Windows 7, Windows Vista, and associated server editions
C:\Users\<username>\AppData\Roaming\Wireshark

Windows XP and Windows Server 2003 [1]
C:\Documents and Settings\<username>\Application Data. "Documents and Settings" and "Application Data" might be internationalized.

Windows 2000 [1]
C:\Documents and Settings\<username>\Application Data. "Documents and Settings" and "Application Data" might be internationalized.

Windows NT 4 [1]
C:\WINNT\Profiles\<username>\Application Data\Wireshark

Windows ME, Windows 98 with user profiles [1]
In Windows ME and 98 you could enable separate user profiles. In that case, something like *C:\windows\Profiles\<username>\Application Data\Wireshark* is used.

Windows ME, Windows 98 without user profiles [1]
Without user profiles enabled the default location for all users was *C:\windows\Application Data\Wireshark*

B.3.2. Windows roaming profiles

Some larger Windows environments use roaming profiles. If this is the case the configurations of all programs you use won't be saved on your local hard drive. They will be stored on the domain server instead.

Your settings will travel with you from computer to computer with one exception. The "Local Settings" folder in your profile data (typically something like: *C:\Documents and Settings\<username>\Local Settings*) will not be transferred to the domain server. This is the default for temporary capture files.

B.3.3. Windows temporary folder

Wireshark uses the folder which is set by the TMPDIR or TEMP environment variable. This variable will be set by the Windows installer.

Windows 8, Windows 7, Windows Vista, and associated server editions
C:\Users\<username>\AppData\Local\Temp

Windows XP, Windows Server 2003, Windows 2000 [1]
C:\Documents and Settings\<username>\Local Settings\Temp

Windows NT [1]
C:\TEMP

[1] No longer supported by Wireshark. For historical reference only.

Appendix C. Protocols and Protocol Fields

Wireshark distinguishes between protocols (e.g. tcp) and protocol fields (e.g. tcp.port).

A comprehensive list of all protocols and protocol fields can be found in the “Display Filter Reference” at https://www.wireshark.org/docs/dfref/

Appendix D. Related command line tools

D.1. Introduction

Along with the main application, Wireshark comes with an array of command line tools which can be helpful for specialized tasks. These tools will be described in this chapter. You can find more information about each command in the Manual Pages.

D.2. *tshark*: Terminal-based Wireshark

TShark is a terminal oriented version of Wireshark designed for capturing and displaying packets when an interactive user interface isn't necessary or available. It supports the same options as `wireshark`. For more information on `tshark` see the manual pages (`man tshark`).

Help information available from `tshark`.

```
TShark (Wireshark) 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...

Capture interface:
  -i <interface>           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>             packet snapshot length (def: 65535)
  -p                       don't capture in promiscuous mode
  -I                       capture in monitor mode, if available
  -B <buffer size>         size of kernel buffer (def: 2MB)
  -y <link type>           link layer type (def: first appropriate)
  -D                       print list of interfaces and exit
  -L                       print list of link-layer types of iface and exit

Capture stop conditions:
  -c <packet count>        stop after n packets (def: infinite)
  -a <autostop cond.> ...  duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                              files:NUM - stop after NUM files
Capture output:
  -b <ringbuffer opt.> ... duration:NUM - switch to next file after NUM secs
                           filesize:NUM - switch to next file after NUM KB
                              files:NUM - ringbuffer: replace after NUM files
RPCAP options:
  -A <user>:<password>     use RPCAP password authentication
Input file:
  -r <infile>              set the filename to read from (- to read from stdin)

Processing:
  -2                       perform a two-pass analysis
  -R <read filter>         packet Read filter in Wireshark display filter syntax
  -Y <display filter>      packet displaY filter in Wireshark display filter
                           syntax
  -n                       disable all name resolutions (def: all enabled)
  -N <name resolve flags>  enable specific name resolution(s): "mnNtCd"
  -d <layer_type>==<selector>,<decode_as_protocol> ...
                           "Decode As", see the man page for details
                           Example: tcp.port==8888,http
  -H <hosts file>          read a list of entries from a hosts file, which will
```

```
                           then be written to a capture file. (Implies -W n)
  --disable-protocol <proto_name>
                           disable dissection of proto_name
  --enable-heuristic <short_name>
                           enable dissection of heuristic protocol
  --disable-heuristic <short_name>
                           disable dissection of heuristic protocol
Output:
  -w <outfile|->           write packets to a pcap-format file named "outfile"
                           (or to the standard output for "-")
  -C <config profile>      start with specified configuration profile
  -F <output file type>    set the output file type, default is pcapng
                           an empty "-F" option will list the file types
  -V                       add output of packet tree        (Packet Details)
  -O <protocols>           Only show packet details of these protocols, comma
                           separated
  -P                       print packet summary even when writing to a file
  -S <separator>           the line separator to print between packets
  -x                       add output of hex and ASCII dump (Packet Bytes)
  -T pdml|ps|psml|text|fields
                           format of text output (def: text)
  -e <field>               field to print if -Tfields selected (e.g. tcp.port,
                           _ws.col.Info)
                           this option can be repeated to print multiple fields
  -E<fieldsoption>=<value> set options for output when -Tfields selected:
     header=y|n            switch headers on and off
     separator=/t|/s|<char> select tab, space, printable character as separator
     occurrence=f|l|a      print first, last or all occurrences of each field
     aggregator=,|/s|<char> select comma, space, printable character as
                           aggregator
     quote=d|s|n           select double, single, no quotes for values
  -t a|ad|d|dd|e|r|u|ud    output format of time stamps (def: r: rel. to first)
  -u s|hms                 output format of seconds (def: s: seconds)
  -l                       flush standard output after each packet
  -q                       be more quiet on stdout (e.g. when using statistics)
  -Q                       only log true errors to stderr (quieter than -q)
  -g                       enable group read access on the output file(s)
  -W n                     Save extra information in the file, if supported.
                           n = write network address resolution information
  -X <key>:<value>         eXtension options, see the man page for details
  -z <statistics>          various statistics, see the man page for details
  --capture-comment <comment>
                           add a capture comment to the newly created
                           output file (only for pcapng)

Miscellaneous:
  -h                       display this help and exit
  -v                       display version info and exit
  -o <name>:<value> ...    override preference setting
  -K <keytab>              keytab file to use for kerberos decryption
  -G [report]              dump one of several available reports and exit
                           default report="fields"
                           use "-G ?" for more help

WARNING: dumpcap will enable kernel BPF JIT compiler if available.
You might want to reset it
By doing "echo 0 > /proc/sys/net/core/bpf_jit_enable"
```

D.3. *tcpdump*: Capturing with `tcpdump` for viewing with Wireshark

It's often more useful to capture packets using `tcpdump` rather than `wireshark`. For example, you might want to do a remote capture and either don't have GUI access or don't have Wireshark installed on the remote machine.

Older versions of `tcpdump` truncate packets to 68 or 96 bytes. If this is the case, use `-s` to capture full-sized packets:

```
$ tcpdump -i <interface> -s 65535 -w <some-file>
```

You will have to specify the correct *interface* and the name of a *file* to save into. In addition, you will have to terminate the capture with ^C when you believe you have captured enough packets.

`tcpdump` is not part of the Wireshark distribution. You can get it from http://www.tcpdump.org or as a standard package in most Linux distributions.

D.4. *dumpcap*: Capturing with `dumpcap` for viewing with Wireshark

Dumpcap is a network traffic dump tool. It captures packet data from a live network and writes the packets to a file. Dumpcap's native capture file format is pcapng, which is also the format used by Wireshark.

Without any options set it will use the pcap library to capture traffic from the first available network interface and write the received raw packet data, along with the packets' time stamps into a pcapng file. The capture filter syntax follows the rules of the pcap library.

Help information available from dumpcap.

```
Dumpcap (Wireshark) 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Capture network packets and dump them into a pcapng or pcap file.
See https://www.wireshark.org for more information.

Usage: dumpcap [options] ...

Capture interface:
  -i <interface>           name or idx of interface (def: first non-loopback),
                           or for remote capturing, use one of these formats:
                               rpcap://<host>/<interface>
                               TCP@<host>:<port>
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>             packet snapshot length (def: 65535)
  -p                       don't capture in promiscuous mode
  -I                       capture in monitor mode, if available
  -B <buffer size>         size of kernel buffer in MiB (def: 2MiB)
  -y <link type>           link layer type (def: first appropriate)
  -D                       print list of interfaces and exit
  -L                       print list of link-layer types of iface and exit
  -d                       print generated BPF code for capture filter
  -k                       set channel on wifi interface <freq>,[<type>]
  -S                       print statistics for each interface once per second
  -M                       for -D, -L, and -S, produce machine-readable output

RPCAP options:
  -r                       don't ignore own RPCAP traffic in capture
  -u                       use UDP for RPCAP data transfer
  -A <user>:<password>     use RPCAP password authentication
  -m <sampling type>       use packet sampling
```

```
                           count:NUM - capture one packet of every NUM
                           timer:NUM - capture no more than 1 packet in NUM ms
Stop conditions:
  -c <packet count>        stop after n packets (def: infinite)
  -a <autostop cond.> ...  duration:NUM - stop after NUM seconds
                           filesize:NUM - stop this file after NUM KB
                              files:NUM - stop after NUM files
Output (files):
  -w <filename>            name of file to save (def: tempfile)
  -g                       enable group read access on the output file(s)
  -b <ringbuffer opt.> ... duration:NUM - switch to next file after NUM secs
                           filesize:NUM - switch to next file after NUM KB
                              files:NUM - ringbuffer: replace after NUM files
  -n                       use pcapng format instead of pcap (default)
  -P                       use libpcap format instead of pcapng
  --capture-comment <comment>
                           add a capture comment to the output file
                           (only for pcapng)

Miscellaneous:
  -N <packet_limit>        maximum number of packets buffered within dumpcap
  -C <byte_limit>          maximum number of bytes used for buffering packets
                           within dumpcap
  -t                       use a separate thread per interface
  -q                       don't report packet capture counts
  -v                       print version information and exit
  -h                       display this help and exit

WARNING: dumpcap will enable kernel BPF JIT compiler if available.
You might want to reset it
By doing "echo 0 > /proc/sys/net/core/bpf_jit_enable"

Example: dumpcap -i eth0 -a duration:60 -w output.pcapng
"Capture packets from interface eth0 until 60s passed into output.pcapng"

Use Ctrl-C to stop capturing at any time.
```

D.5. *capinfos*: Print information about capture files

`capinfos` can print information about binary capture files.

Help information available from capinfos.

```
Capinfos (Wireshark) 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Print various information (infos) about capture files.
See https://www.wireshark.org for more information.

Usage: capinfos [options] <infile> ...

General infos:
  -t display the capture file type
  -E display the capture file encapsulation
  -I display the capture file interface information
  -F display additional capture file information
  -H display the SHA1, RMD160, and MD5 hashes of the file
  -k display the capture comment

Size infos:
  -c display the number of packets
  -s display the size of the file (in bytes)
  -d display the total length of all packets (in bytes)
  -l display the packet size limit (snapshot length)
```

```
Time infos:
  -u display the capture duration (in seconds)
  -a display the capture start time
  -e display the capture end time
  -o display the capture file chronological status (True/False)
  -S display start and end times as seconds

Statistic infos:
  -y display average data rate (in bytes/sec)
  -i display average data rate (in bits/sec)
  -z display average packet size (in bytes)
  -x display average packet rate (in packets/sec)

Output format:
  -L generate long report (default)
  -T generate table report
  -M display machine-readable values in long reports

Table report options:
  -R generate header record (default)
  -r do not generate header record

  -B separate infos with TAB character (default)
  -m separate infos with comma (,) character
  -b separate infos with SPACE character

  -N do not quote infos (default)
  -q quote infos with single quotes (')
  -Q quote infos with double quotes (")

Miscellaneous:
  -h display this help and exit
  -C cancel processing if file open fails (default is to continue)
  -A generate all infos (default)

Options are processed from left to right order with later options superceding
or adding to earlier options.

If no options are given the default is to display all infos in long report
output format.
```

D.6. *rawshark*: Dump and analyze network traffic.

Rawshark reads a stream of packets from a file or pipe, and prints a line describing its output, followed by a set of matching fields for each packet on stdout.

Help information available from rawshark.

```
Rawshark (Wireshark) 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: rawshark [options] ...

Input file:
  -r <infile>              set the pipe or file name to read from

Processing:
  -d <encap:linktype>|<proto:protoname>
                           packet encapsulation or protocol
  -F <field>               field to display
  -n                       disable all name resolution (def: all enabled)
  -N <name resolve flags>  enable specific name resolution(s): "mnNtCd"
```

```
  -p                       use the system's packet header format
                           (which may have 64-bit timestamps)
  -R <read filter>         packet filter in Wireshark display filter syntax
  -s                       skip PCAP header on input

Output:
  -l                       flush output after each packet
  -S                       format string for fields
                           (%D - name, %S - stringval, %N numval)
  -t ad|a|r|d|dd|e         output format of time stamps (def: r: rel. to first)

Miscellaneous:
  -h                       display this help and exit
  -o <name>:<value> ...    override preference setting
  -v                       display version info and exit
```

D.7. *editcap*: Edit capture files

`editcap` is a general-purpose utility for modifying capture files. Its main function is to remove packets from capture files, but it can also be used to convert capture files from one format to another, as well as to print information about capture files.

Help information available from editcap.

```
Editcap (Wireshark) 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Edit and/or translate the format of capture files.
See https://www.wireshark.org for more information.

Usage: editcap [options] ... <infile> <outfile> [ <packet#>[-<packet#>] ... ]

<infile> and <outfile> must both be present.
A single packet or a range of packets can be selected.

Packet selection:
  -r                       keep the selected packets; default is to delete them.
  -A <start time>          only output packets whose timestamp is after (or equal
                           to) the given time (format as YYYY-MM-DD hh:mm:ss).
  -B <stop time>           only output packets whose timestamp is before the
                           given time (format as YYYY-MM-DD hh:mm:ss).

Duplicate packet removal:
  -d                       remove packet if duplicate (window == 5).
  -D <dup window>          remove packet if duplicate; configurable <dup window>
                           Valid <dup window> values are 0 to 1000000.
                           NOTE: A <dup window> of 0 with -v (verbose option) is
                           useful to print MD5 hashes.
  -w <dup time window>     remove packet if duplicate packet is found EQUAL TO OR
                           LESS THAN <dup time window> prior to current packet.
                           A <dup time window> is specified in relative seconds
                           (e.g. 0.000001).
  -a <framenum>:<comment>  Add or replace comment for given frame number

  -I <bytes to ignore>     ignore the specified bytes at the beginning of
                           the frame during MD5 hash calculation
                           Useful to remove duplicated packets taken on
                           several routers(differents mac addresses for
                           example)
                           e.g. -I 26 in case of Ether/IP/ will ignore
                           ether(14) and IP header(20 - 4(src ip) - 4(dst ip)).

          NOTE: The use of the 'Duplicate packet removal' options with
          other editcap options except -v may not always work as expected.
          Specifically the -r, -t or -S options will very likely NOT have the
          desired effect if combined with the -d, -D or -w.
```

```
Packet manipulation:
  -s <snaplen>            truncate each packet to max. <snaplen> bytes of data.
  -C [offset:]<choplen>   chop each packet by <choplen> bytes. Positive values
                          chop at the packet beginning, negative values at the
                          packet end. If an optional offset precedes the length,
                          then the bytes chopped will be offset from that value.
                          Positive offsets are from the packet beginning,
                          negative offsets are from the packet end. You can use
                          this option more than once, allowing up to 2 chopping
                          regions within a packet provided that at least 1
                          choplen is positive and at least 1 is negative.
  -L                      adjust the frame (i.e. reported) length when chopping
                          and/or snapping
  -t <time adjustment>    adjust the timestamp of each packet;
                          <time adjustment> is in relative seconds (e.g. -0.5).
  -S <strict adjustment> adjust timestamp of packets if necessary to insure
                          strict chronological increasing order. The <strict
                          adjustment> is specified in relative seconds with
                          values of 0 or 0.000001 being the most reasonable.
                          A negative adjustment value will modify timestamps so
                          that each packet's delta time is the absolute value
                          of the adjustment specified. A value of -0 will set
                          all packets to the timestamp of the first packet.
  -E <error probability> set the probability (between 0.0 and 1.0 incl.) that
                          a particular packet byte will be randomly changed.
  -o <change offset>      When used in conjuction with -E, skip some bytes from the
                          beginning of the packet. This allows to preserve some
                          bytes, in order to have some headers untouched.

Output File(s):
  -c <packets per file>   split the packet output to different files based on
                          uniform packet counts with a maximum of
                          <packets per file> each.
  -i <seconds per file>   split the packet output to different files based on
                          uniform time intervals with a maximum of
                          <seconds per file> each.
  -F <capture type>       set the output file type; default is pcapng. An empty
                          "-F" option will list the file types.
  -T <encap type>         set the output file encapsulation type; default is the
                          same as the input file. An empty "-T" option will
                          list the encapsulation types.

Miscellaneous:
  -h                      display this help and exit.
  -v                      verbose output.
                          If -v is used with any of the 'Duplicate Packet
                          Removal' options (-d, -D or -w) then Packet lengths
                          and MD5 hashes are printed to standard-error.
```

Capture file types available from `editcap -F`.

```
$ editcap -F
editcap: option requires an argument -- 'F'
editcap: The available capture file types for the "-F" flag are:
    5views - InfoVista 5View capture
    btsnoop - Symbian OS btsnoop
    commview - TamoSoft CommView
    dct2000 - Catapult DCT2000 trace (.out format)
    erf - Endace ERF capture
    eyesdn - EyeSDN USB S0/E1 ISDN trace format
    k12text - K12 text file
    lanalyzer - Novell LANalyzer
    logcat - Android Logcat Binary format
    logcat-brief - Android Logcat Brief text format
    logcat-long - Android Logcat Long text format
    logcat-process - Android Logcat Process text format
    logcat-tag - Android Logcat Tag text format
```

```
    logcat-thread - Android Logcat Thread text format
    logcat-threadtime - Android Logcat Threadtime text format
    logcat-time - Android Logcat Time text format
    modlibpcap - Modified tcpdump - libpcap
    netmon1 - Microsoft NetMon 1.x
    netmon2 - Microsoft NetMon 2.x
    nettl - HP-UX nettl trace
    ngsniffer - Sniffer (DOS)
    ngwsniffer_1_1 - NetXray, Sniffer (Windows) 1.1
    ngwsniffer_2_0 - Sniffer (Windows) 2.00x
    niobserver - Network Instruments Observer
    nokialibpcap - Nokia tcpdump - libpcap
    nseclibpcap - Wireshark - nanosecond libpcap
    nstrace10 - NetScaler Trace (Version 1.0)
    nstrace20 - NetScaler Trace (Version 2.0)
    nstrace30 - NetScaler Trace (Version 3.0)
    nstrace35 - NetScaler Trace (Version 3.5)
    pcap - Wireshark/tcpdump/... - pcap
    pcapng - Wireshark/... - pcapng
    rf5 - Tektronix K12xx 32-bit .rf5 format
    rh6_1libpcap - RedHat 6.1 tcpdump - libpcap
    snoop - Sun snoop
    suse6_3libpcap - SuSE 6.3 tcpdump - libpcap
    visual - Visual Networks traffic capture
```

Encapsulation types available from editcap.

```
$ editcap -T
editcap: option requires an argument -- 'T'
editcap: The available encapsulation types for the "-T" flag are:
    ap1394 - Apple IP-over-IEEE 1394
    arcnet - ARCNET
    arcnet_linux - Linux ARCNET
    ascend - Lucent/Ascend access equipment
    atm-pdus - ATM PDUs
    atm-pdus-untruncated - ATM PDUs - untruncated
    atm-rfc1483 - RFC 1483 ATM
    ax25 - Amateur Radio AX.25
    ax25-kiss - AX.25 with KISS header
    bacnet-ms-tp - BACnet MS/TP
    bacnet-ms-tp-with-direction - BACnet MS/TP with Directional Info
    ber - ASN.1 Basic Encoding Rules
    bluetooth-bredr-bb-rf - Bluetooth BR/EDR Baseband RF
    bluetooth-h4 - Bluetooth H4
    bluetooth-h4-linux - Bluetooth H4 with linux header
    bluetooth-hci - Bluetooth without transport layer
    bluetooth-le-ll - Bluetooth Low Energy Link Layer
    bluetooth-le-ll-rf - Bluetooth Low Energy Link Layer RF
    bluetooth-linux-monitor - Bluetooth Linux Monitor
    can20b - Controller Area Network 2.0B
    chdlc - Cisco HDLC
    chdlc-with-direction - Cisco HDLC with Directional Info
    cosine - CoSine L2 debug log
    dbus - D-Bus
    dct2000 - Catapult DCT2000
    docsis - Data Over Cable Service Interface Specification
    dpnss_link - Digital Private Signalling System No 1 Link Layer
    dvbci - DVB-CI (Common Interface)
    enc - OpenBSD enc(4) encapsulating interface
    epon - Ethernet Passive Optical Network
    erf - Extensible Record Format
    ether - Ethernet
    ether-nettl - Ethernet with nettl headers
    fc2 - Fibre Channel FC-2
    fc2sof - Fibre Channel FC-2 With Frame Delimiter
    fddi - FDDI
    fddi-nettl - FDDI with nettl headers
```

```
fddi-swapped - FDDI with bit-swapped MAC addresses
flexray - FlexRay
frelay - Frame Relay
frelay-with-direction - Frame Relay with Directional Info
gcom-serial - GCOM Serial
gcom-tie1 - GCOM TIE1
gprs-llc - GPRS LLC
gsm_um - GSM Um Interface
hhdlc - HiPath HDLC
i2c - I2C
ieee-802-11 - IEEE 802.11 Wireless LAN
ieee-802-11-airopeek - IEEE 802.11 plus AiroPeek radio header
ieee-802-11-avs - IEEE 802.11 plus AVS radio header
ieee-802-11-netmon - IEEE 802.11 plus Network Monitor radio header
ieee-802-11-prism - IEEE 802.11 plus Prism II monitor mode radio header
ieee-802-11-radio - IEEE 802.11 Wireless LAN with radio information
ieee-802-11-radiotap - IEEE 802.11 plus radiotap radio header
ieee-802-16-mac-cps - IEEE 802.16 MAC Common Part Sublayer
infiniband - InfiniBand
ios - Cisco IOS internal
ip-over-fc - RFC 2625 IP-over-Fibre Channel
ip-over-ib - IP over Infiniband
ipfix - IPFIX
ipmb - Intelligent Platform Management Bus
ipmi-trace - IPMI Trace Data Collection
ipnet - Solaris IPNET
irda - IrDA
isdn - ISDN
ixveriwave - IxVeriWave header and stats block
jfif - JPEG/JFIF
json - JavaScript Object Notation
juniper-atm1 - Juniper ATM1
juniper-atm2 - Juniper ATM2
juniper-chdlc - Juniper C-HDLC
juniper-ether - Juniper Ethernet
juniper-frelay - Juniper Frame-Relay
juniper-ggsn - Juniper GGSN
juniper-mlfr - Juniper MLFR
juniper-mlppp - Juniper MLPPP
juniper-ppp - Juniper PPP
juniper-pppoe - Juniper PPPoE
juniper-svcs - Juniper Services
juniper-vp - Juniper Voice PIC
k12 - K12 protocol analyzer
lapb - LAPB
lapd - LAPD
layer1-event - EyeSDN Layer 1 event
lin - Local Interconnect Network
linux-atm-clip - Linux ATM CLIP
linux-lapd - LAPD with Linux pseudo-header
linux-sll - Linux cooked-mode capture
logcat - Android Logcat Binary format
logcat_brief - Android Logcat Brief text format
logcat_long - Android Logcat Long text format
logcat_process - Android Logcat Process text format
logcat_tag - Android Logcat Tag text format
logcat_thread - Android Logcat Thread text format
logcat_threadtime - Android Logcat Threadtime text format
logcat_time - Android Logcat Time text format
loop - OpenBSD loopback
ltalk - Localtalk
mime - MIME
most - Media Oriented Systems Transport
mp2ts - ISO/IEC 13818-1 MPEG2-TS
mpeg - MPEG
mtp2 - SS7 MTP2
mtp2-with-phdr - MTP2 with pseudoheader
```

```
mtp3 - SS7 MTP3
mux27010 - MUX27010
netanalyzer - netANALYZER
netanalyzer-transparent - netANALYZER-Transparent
netlink - Linux Netlink
nfc-llcp - NFC LLCP
nflog - NFLOG
nstrace10 - NetScaler Encapsulation 1.0 of Ethernet
nstrace20 - NetScaler Encapsulation 2.0 of Ethernet
nstrace30 - NetScaler Encapsulation 3.0 of Ethernet
nstrace35 - NetScaler Encapsulation 3.5 of Ethernet
null - NULL/Loopback
packetlogger - PacketLogger
pflog - OpenBSD PF Firewall logs
pflog-old - OpenBSD PF Firewall logs, pre-3.4
pktap - Apple PKTAP
ppi - Per-Packet Information header
ppp - PPP
ppp-with-direction - PPP with Directional Info
pppoes - PPP-over-Ethernet session
raw-icmp-nettl - Raw ICMP with nettl headers
raw-icmpv6-nettl - Raw ICMPv6 with nettl headers
raw-telnet-nettl - Raw telnet with nettl headers
rawip - Raw IP
rawip-nettl - Raw IP with nettl headers
rawip4 - Raw IPv4
rawip6 - Raw IPv6
redback - Redback SmartEdge
rtac-serial - RTAC serial-line
s4607 - STANAG 4607
s5066-dpdu - STANAG 5066 Data Transfer Sublayer PDUs(D_PDU)
sccp - SS7 SCCP
sctp - SCTP
sdh - SDH
sdlc - SDLC
sita-wan - SITA WAN packets
slip - SLIP
socketcan - SocketCAN
symantec - Symantec Enterprise Firewall
tnef - Transport-Neutral Encapsulation Format
tr - Token Ring
tr-nettl - Token Ring with nettl headers
tzsp - Tazmen sniffer protocol
unknown - Unknown
unknown-nettl - Unknown link-layer type with nettl headers
usb - Raw USB packets
usb-linux - USB packets with Linux header
usb-linux-mmap - USB packets with Linux header and padding
usb-usbpcap - USB packets with USBPcap header
user0 - USER 0
user1 - USER 1
user2 - USER 2
user3 - USER 3
user4 - USER 4
user5 - USER 5
user6 - USER 6
user7 - USER 7
user8 - USER 8
user9 - USER 9
user10 - USER 10
user11 - USER 11
user12 - USER 12
user13 - USER 13
user14 - USER 14
user15 - USER 15
v5-ef - V5 Envelope Function
whdlc - Wellfleet HDLC
```

```
wireshark-upper-pdu - Wireshark Upper PDU export
wpan - IEEE 802.15.4 Wireless PAN
wpan-nofcs - IEEE 802.15.4 Wireless PAN with FCS not present
wpan-nonask-phy - IEEE 802.15.4 Wireless PAN non-ASK PHY
x2e-serial - X2E serial line capture
x2e-xoraya - X2E Xoraya
x25-nettl - X.25 with nettl headers
```

D.8. *mergecap*: Merging multiple capture files into one

Mergecap is a program that combines multiple saved capture files into a single output file specified by the `-w` argument. Mergecap knows how to read libpcap capture files, including those of tcpdump. In addition, Mergecap can read capture files from snoop (including Shomiti) and atmsnoop, LanAlyzer, Sniffer (compressed or uncompressed), Microsoft Network Monitor, AIX's iptrace, NetXray, Sniffer Pro, RADCOM's WAN/LAN analyzer, Lucent/Ascend router debug output, HP-UX's nettl, and the dump output from Toshiba's ISDN routers. There is no need to tell Mergecap what type of file you are reading; it will determine the file type by itself. Mergecap is also capable of reading any of these file formats if they are compressed using `gzip`. Mergecap recognizes this directly from the file; the ".gz" extension is not required for this purpose.

By default, it writes the capture file in pcapng format, and writes all of the packets in the input capture files to the output file. The `-F` flag can be used to specify the format in which to write the capture file; it can write the file in libpcap format (standard libpcap format, a modified format used by some patched versions of libpcap, the format used by Red Hat Linux 6.1, or the format used by SuSE Linux 6.3), snoop format, uncompressed Sniffer format, Microsoft Network Monitor 1.x format, and the format used by Windows-based versions of the Sniffer software.

Packets from the input files are merged in chronological order based on each frame's timestamp, unless the `-a` flag is specified. Mergecap assumes that frames within a single capture file are already stored in chronological order. When the `-a` flag is specified, packets are copied directly from each input file to the output file, independent of each frame's timestamp.

If the `-s` flag is used to specify a snapshot length, frames in the input file with more captured data than the specified snapshot length will have only the amount of data specified by the snapshot length written to the output file. This may be useful if the program that is to read the output file cannot handle packets larger than a certain size (for example, the versions of snoop in Solaris 2.5.1 and Solaris 2.6 appear to reject Ethernet frames larger than the standard Ethernet MTU, making them incapable of handling gigabit Ethernet captures if jumbo frames were used).

If the `-T` flag is used to specify an encapsulation type, the encapsulation type of the output capture file will be forced to the specified type, rather than being the type appropriate to the encapsulation type of the input capture file. Note that this merely forces the encapsulation type of the output file to be the specified type; the packet headers of the packets will not be translated from the encapsulation type of the input capture file to the specified encapsulation type (for example, it will not translate an Ethernet capture to an FDDI capture if an Ethernet capture is read and `-T fddi` is specified).

Help information available from mergecap.

```
Mergecap (Wireshark) 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Merge two or more capture files into one.
See https://www.wireshark.org for more information.

Usage: mergecap [options] -w <outfile>|- <infile> [<infile> ...]

Output:
  -a                concatenate rather than merge files.
```

```
                    default is to merge based on frame timestamps.
  -s <snaplen>      truncate packets to <snaplen> bytes of data.
  -w <outfile>|-    set the output filename to <outfile> or '-' for stdout.
  -F <capture type> set the output file type; default is pcapng.
                    an empty "-F" option will list the file types.
  -I <IDB merge mode> set the merge mode for Interface Description Blocks; default is
 'all'.
                    an empty "-I" option will list the merge modes.

Miscellaneous:
  -h                display this help and exit.
  -v                verbose output.
```

A simple example merging `dhcp-capture.pcapng` and `imap-1.pcapng` into `outfile.pcapng` is shown below.

Simple example of using mergecap.

```
$ mergecap -w outfile.pcapng dhcp-capture.pcapng imap-1.pcapng
```

D.9. *text2pcap*: Converting ASCII hexdumps to network captures

There may be some occasions when you wish to convert a hex dump of some network traffic into a libpcap file.

`text2pcap` is a program that reads in an ASCII hex dump and writes the data described into a libpcap-style capture file. text2pcap can read hexdumps with multiple packets in them, and build a capture file of multiple packets. `text2pcap` is also capable of generating dummy Ethernet, IP and UDP headers, in order to build fully processable packet dumps from hexdumps of application-level data only.

`text2pcap` understands a hexdump of the form generated by `od -A x -t x1`. In other words, each byte is individually displayed and surrounded with a space. Each line begins with an offset describing the position in the file. The offset is a hex number (can also be octal - see `-o`), of more than two hex digits. Here is a sample dump that `text2pcap` can recognize:

```
000000 00 e0 1e a7 05 6f 00 10 ........
000008 5a a0 b9 12 08 00 46 00 ........
000010 03 68 00 00 00 00 0a 2e ........
000018 ee 33 0f 19 08 7f 0f 19 ........
000020 03 80 94 04 00 00 10 01 ........
000028 16 a2 0a 00 03 50 00 0c ........
000030 01 01 0f 19 03 80 11 01 ........
```

There is no limit on the width or number of bytes per line. Also the text dump at the end of the line is ignored. Bytes/hex numbers can be uppercase or lowercase. Any text before the offset is ignored, including email forwarding characters '>'. Any lines of text between the bytestring lines is ignored. The offsets are used to track the bytes, so offsets must be correct. Any line which has only bytes without a leading offset is ignored. An offset is recognized as being a hex number longer than two characters. Any text after the bytes is ignored (e.g. the character dump). Any hex numbers in this text are also ignored. An offset of zero is indicative of starting a new packet, so a single text file with a series of hexdumps can be converted into a packet capture with multiple packets. Multiple packets are read in with timestamps differing by one second each. In general, short of these restrictions, text2pcap is pretty liberal about reading in hexdumps and has been tested with a variety of mangled outputs (including being forwarded through email multiple times, with limited line wrap etc.)

There are a couple of other special features to note. Any line where the first non-whitespace character is # will be ignored as a comment. Any line beginning with #TEXT2PCAP is a directive and options can be inserted after this command to be processed by `text2pcap`. Currently there are no directives

implemented; in the future, these may be used to give more fine grained control on the dump and the way it should be processed e.g. timestamps, encapsulation type etc.

`text2pcap` also allows the user to read in dumps of application-level data, by inserting dummy L2, L3 and L4 headers before each packet. Possibilities include inserting headers such as Ethernet, Ethernet + IP, Ethernet + IP + UDP, or Ethernet + Ip + TCP before each packet. This allows Wireshark or any other full-packet decoder to handle these dumps.

Help information available from text2pcap.

```
Text2pcap (Wireshark) 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Generate a capture file from an ASCII hexdump of packets.
See https://www.wireshark.org for more information.

Usage: text2pcap [options] <infile> <outfile>

where  <infile> specifies input  filename (use - for standard input)
      <outfile> specifies output filename (use - for standard output)

Input:
  -o hex|oct|dec         parse offsets as (h)ex, (o)ctal or (d)ecimal;
                         default is hex.
  -t <timefmt>           treat the text before the packet as a date/time code;
                         the specified argument is a format string of the sort
                         supported by strptime.
                         Example: The time "10:15:14.5476" has the format code
                         "%H:%M:%S."
                         NOTE: The subsecond component delimiter, '.', must be
                         given, but no pattern is required; the remaining
                         number is assumed to be fractions of a second.
                         NOTE: Date/time fields from the current date/time are
                         used as the default for unspecified fields.
  -D                     the text before the packet starts with an I or an O,
                         indicating that the packet is inbound or outbound.
                         This is only stored if the output format is PCAP-NG.
  -a                     enable ASCII text dump identification.
                         The start of the ASCII text dump can be identified
                         and excluded from the packet data, even if it looks
                         like a HEX dump.
                         NOTE: Do not enable it if the input file does not
                         contain the ASCII text dump.

Output:
  -l <typenum>           link-layer type number; default is 1 (Ethernet).  See
                         http://www.tcpdump.org/linktypes.html for a list of
                         numbers.  Use this option if your dump is a complete
                         hex dump of an encapsulated packet and you wish to
                         specify the exact type of encapsulation.
                         Example: -l 7 for ARCNet packets.
  -m <max-packet>        max packet length in output; default is 65535

Prepend dummy header:
  -e <l3pid>             prepend dummy Ethernet II header with specified L3PID
                         (in HEX).
                         Example: -e 0x806 to specify an ARP packet.
  -i <proto>             prepend dummy IP header with specified IP protocol
                         (in DECIMAL).
                         Automatically prepends Ethernet header as well.
                         Example: -i 46
  -4 <srcip>,<destip>    prepend dummy IPv4 header with specified
                         dest and source address.
                         Example: -4 10.0.0.1,10.0.0.2
  -6 <srcip>,<destip>    replace IPv6 header with specified
                         dest and source address.
                         Example: -6
 fe80:0:0:0:202:b3ff:fe1e:8329,2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

```
  -u <srcp>,<destp>      prepend dummy UDP header with specified
                         source and destination ports (in DECIMAL).
                         Automatically prepends Ethernet & IP headers as well.
                         Example: -u 1000,69 to make the packets look like
                         TFTP/UDP packets.
  -T <srcp>,<destp>      prepend dummy TCP header with specified
                         source and destination ports (in DECIMAL).
                         Automatically prepends Ethernet & IP headers as well.
                         Example: -T 50,60
  -s <srcp>,<dstp>,<tag> prepend dummy SCTP header with specified
                         source/dest ports and verification tag (in DECIMAL).
                         Automatically prepends Ethernet & IP headers as well.
                         Example: -s 30,40,34
  -S <srcp>,<dstp>,<ppi> prepend dummy SCTP header with specified
                         source/dest ports and verification tag 0.
                         Automatically prepends a dummy SCTP DATA
                         chunk header with payload protocol identifier ppi.
                         Example: -S 30,40,34

Miscellaneous:
  -h                     display this help and exit.
  -d                     show detailed debug of parser states.
  -q                     generate no output at all (automatically disables -d).
  -n                     use PCAP-NG instead of PCAP as output format.
```

D.10. *reordercap*: Reorder a capture file

`reordercap` lets you reorder a capture file according to the packets timestamp.

Help information available from reordercap.

```
Reordercap (Wireshark) 2.1.0 (v2.1.0rc0-502-g328fbc0 from master)
Reorder timestamps of input file frames into output file.
See https://www.wireshark.org for more information.

Usage: reordercap [options] <infile> <outfile>

Options:
  -n        don't write to output file if the input file is ordered.
  -h        display this help and exit.
```

Chapter 11. This Document’s License (GPL)

As with the original license and documentation distributed with Wireshark, this document is covered by the GNU General Public License (GNU GPL).

If you haven’t read the GPL before, please do so. It explains all the things that you are allowed to do with this code and documentation.

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
     51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.)  You can apply it to
your programs, too.

  When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

  To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

  For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have.  You must make sure that they, too, receive or can get the
source code.  And you must show them these terms so they know their
rights.

  We protect your rights with two steps: (1) copyright the software, and
(2) offer you this license which gives you legal permission to copy,
distribute and/or modify the software.

  Also, for each author's protection and ours, we want to make certain
that everyone understands that there is no warranty for this free
software.  If the software is modified by someone else and passed on, we
want its recipients to know that what they have is not the original, so
that any problems introduced by others will not reflect on the original
authors' reputations.

  Finally, any free program is threatened constantly by software
patents.  We wish to avoid the danger that redistributors of a free
program will individually obtain patent licenses, in effect making the
program proprietary.  To prevent this, we have made it clear that any
```

patent must be licensed for everyone's free use or not licensed at all.

  The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

  0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

  1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

  2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

    a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

    b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

    c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of

this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals

of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year> <name of author>

    This program is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 2 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program; if not, write to the Free Software
    Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate

parts of the General Public License. Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary. Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the program
  `Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs. If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library. If this is what you want to do, use the GNU Library General
Public License instead of this License.