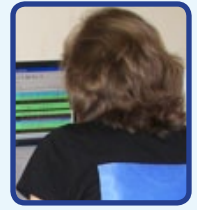


# Wireshark & CACE Pilot

Joke Snelders reporting from the field



August 2010

## About The Author

My name is Joke (pronounced \yo-kə or Joan for those who do not speak Dutch). During the day, I work as a secretary for a non-profit organization providing assisted living for mentally handicapped people in the south of The Netherlands. In my spare time I like to use Wireshark. I find it interesting and necessary to monitor my home network to see what is going on. As a user I like to answer questions at the Wireshark Mailing List.

What is in it for me? Well, I learn a great deal whenever I try to solve real-world problems. I am also a member of the NGN (the Dutch Network User's Group). I write articles about how to use Wireshark and the command line tools. And if there is still some spare time left, I like to go biking in the woods near my hometown with my husband and fellow geek.

## About CACE Pilot

CACE Pilot® is a visually rich and powerful analyzer for wired and wireless networks that revolutionizes the use of Wireshark by providing capabilities not found in the world's most popular packet and network analysis tool. Fully integrated with Wireshark, CACE Pilot capitalizes on user's existing expertise while dramatically increasing efficiency in identifying and diagnosing network problems.



## One Plus One Equals More Than Two

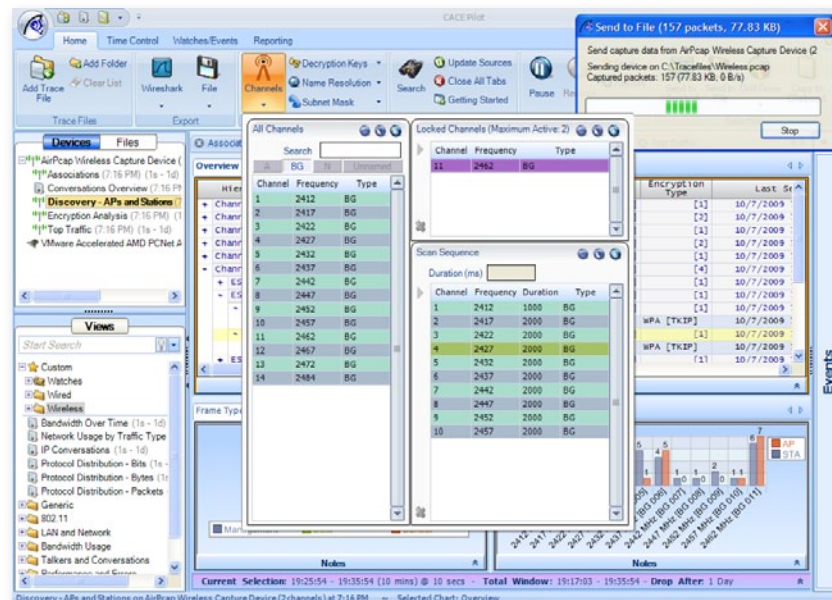
CACE Pilot is an analyzer for wired and wireless networks and is fully integrated with Wireshark. Version 2.3 is recently released by CACE Technologies.

## CACE Pilot = Visualization

It is shipped with a lot of Views, so you can start right away. The Views consist of a collection of interactive display components like bar charts, strip charts, conversation rings, grids and so on. After loading a capture file you can apply one or more Views. You can also use traffic from a live source: a wired ethernet adapter or a wireless adapter. In the strip chart Bandwith Over Time you see right away when the bandwidth usage drops down to zero. The bar chart TCP Errors shows for instance the number of Retransmissions, Duplicate ACK's, Zero Windows. CACE Pilot offers the flexibility to customize the Views by using display filters. This way you can create all the Views you need for your job.

## Capture files

It's amazing that CACE Pilot can handle gigabyte capture files without the need to split those files. Use views like Capture Summary, Conversations Overview, Protocol Distribution to start and use the powerful feature Drill-Down to zoom into the details. By selecting one or more bars in a bar chart or select a certain amount of time in a strip chart you focus in on parts of the trace file, where you suspect a problem. You can also send the selected traffic to Wireshark for further analyzing. CACE Pilot has a whole lot of options; continue reading while I dig into a few of them.

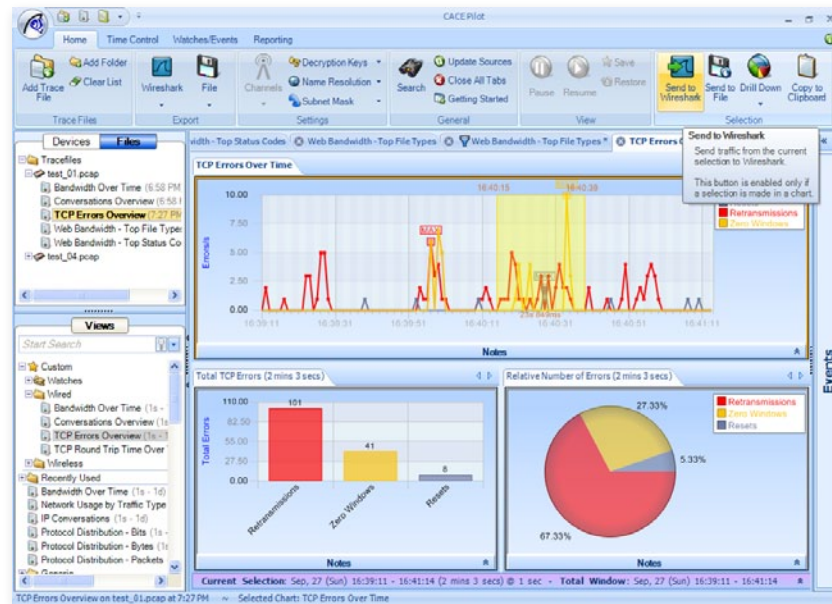


This screenshot shows how the traffic from two AirPcap adapters is monitored.

One AirPcap adapter is used to monitor the traffic on channel 11 (Locked Channels). The other adapter is used to monitor the traffic on channel 1 to 10 (Scan Sequence). The Duration (ms) box sets how long each selected channel will be locked before moving to the next channel. You can apply one or more Views by drag and drop Views on the "AirPcap Wireless Capture Device". If you want to save the traffic, hit the Export -> Wireshark or Export -> File button. When you choose Export -> Wireshark, Wireshark is launched and all the features like Follow TCP Stream, Decode as and Follow TCP Stream are available. Use Export ->File, if you just want to save the traffic to a trace file.

### Trace files

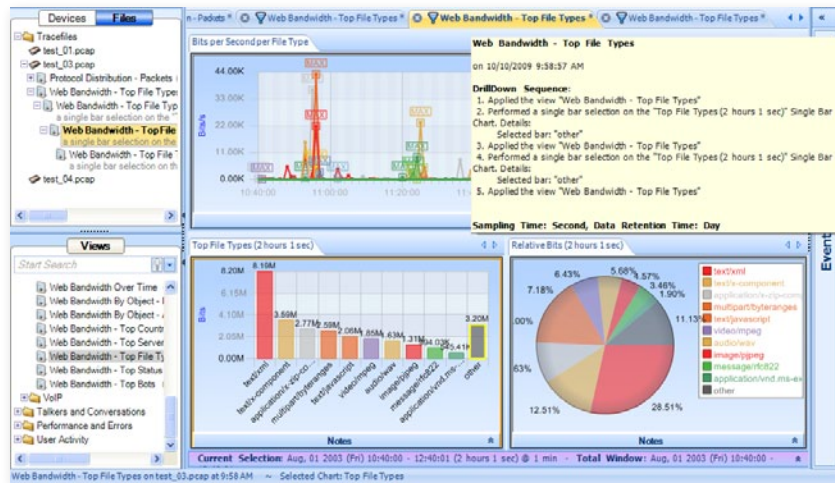
Select the Files -> Add Trace File to open previous captured files. You can load multiple files at the same time.



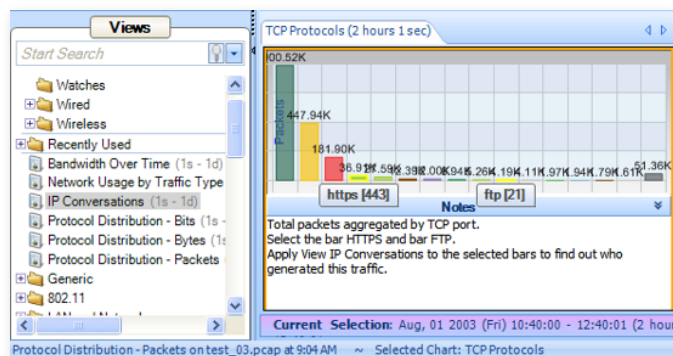
You apply Views by dragging and dropping them on the file name.

Select a specific period of time in a strip chart by clicking and dragging. The selection, from 16:40:15 til 16:40:39, is highlighted. This way you can use Time Control to Zoom In on the selected time interval or you can Drill-Down by drag and drop another View, for instance IP Conversations, straight to the selection. And, of course, you can send the selection to Wireshark. You will find all the available options in the context menu.

## Drill-Down

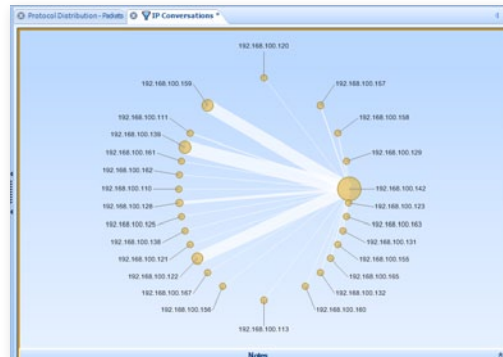


I started with applying the “Web Bandwidth - Top File Types” to the trace file test\_03.pcap. If there are more than 10 file types the View will show you the Top 10 and the “other” bar. Of course you like to know, what’s in the “other” bar. Now it is time to Drill-Down. Select the “other” bar. Drag and drop the View “Web Bandwidth - Top File Types” to this bar. You can repeat this action as long as the “other” bar pops up. Hover over the tab to review the Drill-Down sequence.



Here is another example of Drill-Down.

You have applied the View “Protocol Distribution – Packets” to a trace file. You are curious to know who generated the https and ftp traffic. Select the bars https and ftp. Select the View “IP Conversation” and drag and drop it on the selected bars.



The Conversation Ring gives an overview of the endpoints. The size of lines gives an indication for the amount of traffic.



### About CACE Technologies, Inc.

CACE Technologies Inc. is the sponsor and innovative force behind Wireshark and WinPcap, the world's most widely used Open Source network traffic capture and analysis tools. The company develops cutting-edge network analysis and troubleshooting products that complement Wireshark's prodigious packet inspection capabilities. The CACE Shark Distributed Monitoring System provides enterprise-class, end-to-end network monitoring and analytics capabilities and extends the Wireshark experience into distributed network environments. Known for its user-friendly modular products, the company offers the most cost-effective analysis solutions for modern enterprise networks.

## Reports

When all the work is done, you can generate reports in various formats, e.g. PDF Report, Excel Spreadsheet or HTML Page. Select the Views you want to include in the report. The personal notes you added to the charts will also be included. Select the report format(s). My favorite is the ZIP Package.

The result is a ZIP file with the following contents:

Name	Type	Packed Size	Size	Ratio	Date
analysis report.pdf	PDF-XChange Viewer Document	943 KB	1.463 KB	36%	09-10-2009 23:27
analysis report.txt	Text Document	1 KB	2 KB	71%	09-10-2009 23:27
test_01.pcap	Wireshark capture file	19.461 KB	20.933 KB	8%	27-09-2009 16:41
test_01.pcap.md5	MD5 File	1 KB	1 KB	0%	09-10-2009 23:27

## Teamwork

Take advantage of the interaction between Wireshark and CACE Pilot. Open large trace files in CACE Pilot and send the selected traffic back to Wireshark. Setup a Watch to start capturing and send the traffic to Wireshark. The Wireshark's capture and display filters are available in CACE Pilot.

## Learn more?

Go and ask for an Evaluation Copy; a full working version for 10 days. Additional information is available at [CACE Technologies](http://www.cacetech.com). Have an nice analyze time.

### CACE Technologies

1949 5th Street, Suite 103

Davis, CA 95616

tel: 530.758.2790

fax: 530.758.2781

[www.cacetech.com](http://www.cacetech.com)