

Indexing Capture Files

Joke Snelders reporting from the field



October 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

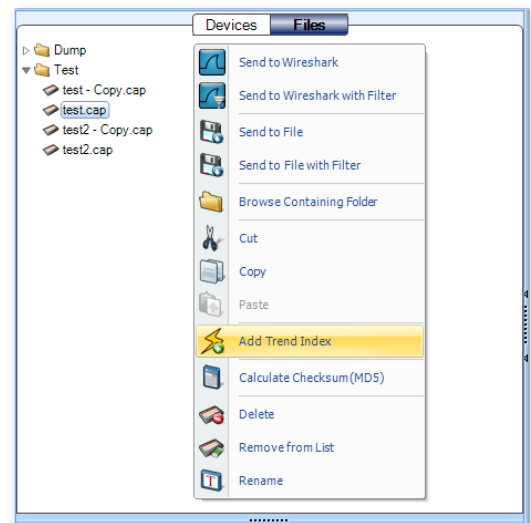
CACE Pilot® is a visually rich and powerful analyzer for wired and wireless networks that revolutionizes the use of Wireshark by providing capabilities not found in the world's most popular packet and network analysis tool. Fully integrated with Wireshark, CACE Pilot capitalizes on user's existing expertise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



CACE Pilot, the network visualization and analysis tool from **CACE Technologies**, has a great feature: Add Trend Index to capture files. Loading Views on multi-gigabyte capture files can take minutes. The time it takes to load a View on a capture file depends on a couple of things:

- the kind of View: some Views take longer to load than others
- the size of the capture file
- the hardware

After adding a Trend Index to an existing capture file Views load in seconds in stead of minutes.



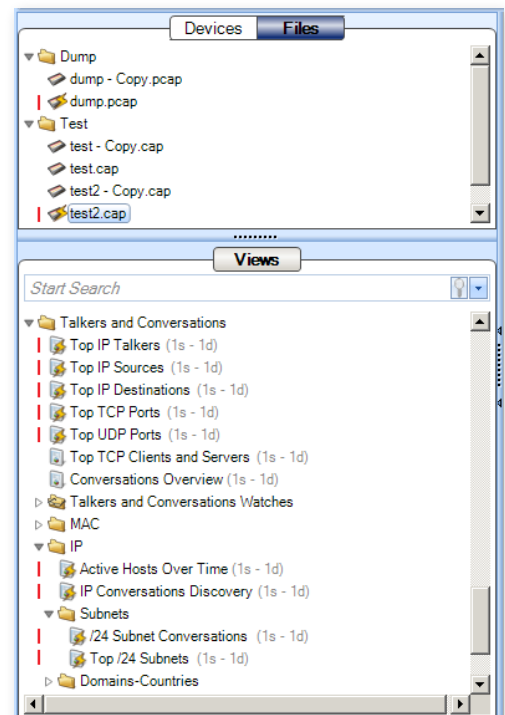
Adding a Trend Index

All you have to do is just right-click a capture file and select Add Trend Index from the context menu. On my machine it took about 80 seconds on a 4.5GB file and 160 seconds on a 9,5GB file.

Note: You cannot add a Trend Index to wireless capture files.

Lightning Icon

The lightning icon is the symbol of indexing. At a glance you can see which files are indexed. They all have the lightning icon on top. Select an indexed file and all Views, that support indexing, show the icon on top of them.



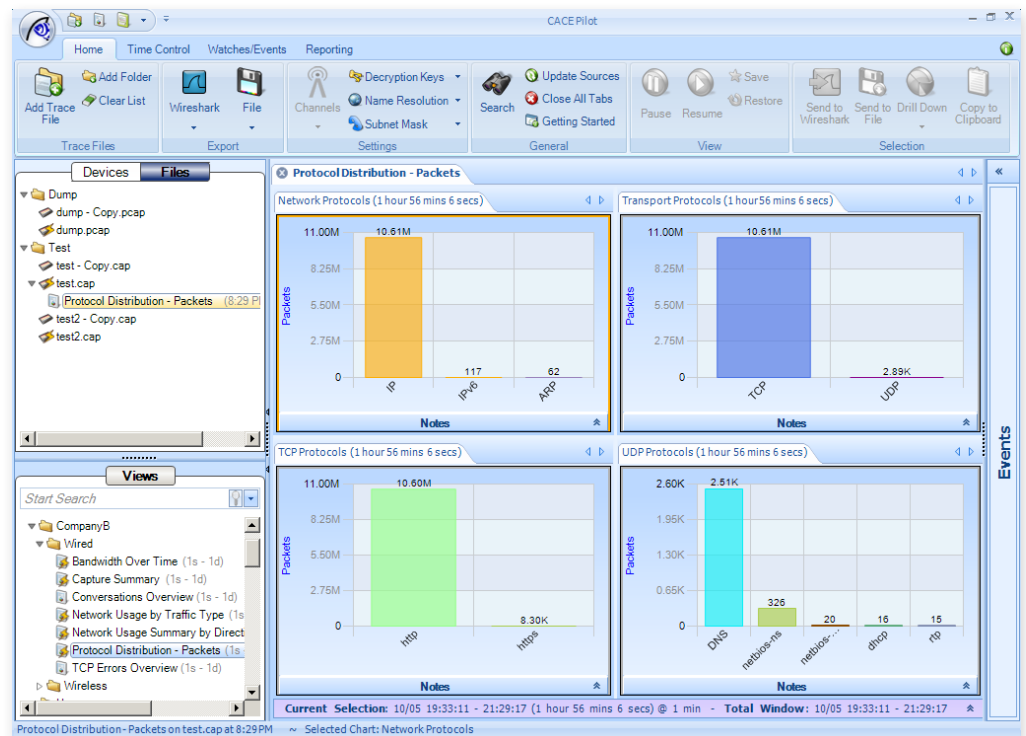
Applying Views

Applying Views to indexed files works the same way as applying them to non-indexed files:

- select a View
- drag and drop it on a capture file

The big difference is the time it takes to load supported Views on indexed files:

- loading a View on a indexed 4.5GB file takes about 2 seconds in stead of 80 seconds on the non-indexed file
- loading a View on a indexed 9.5GB file takes about 3 seconds in stead of 180 seconds on the non-indexed file



Removing a Trend Index

Yes, you can right-click an indexed file and select Remove Trend Index.

But... why should you?

In Short

Loading a View on a non-indexed 9,5GB capture file takes about 180 seconds. Adding a Trend Index takes about 160 seconds. Next loading a View takes about 3 seconds.

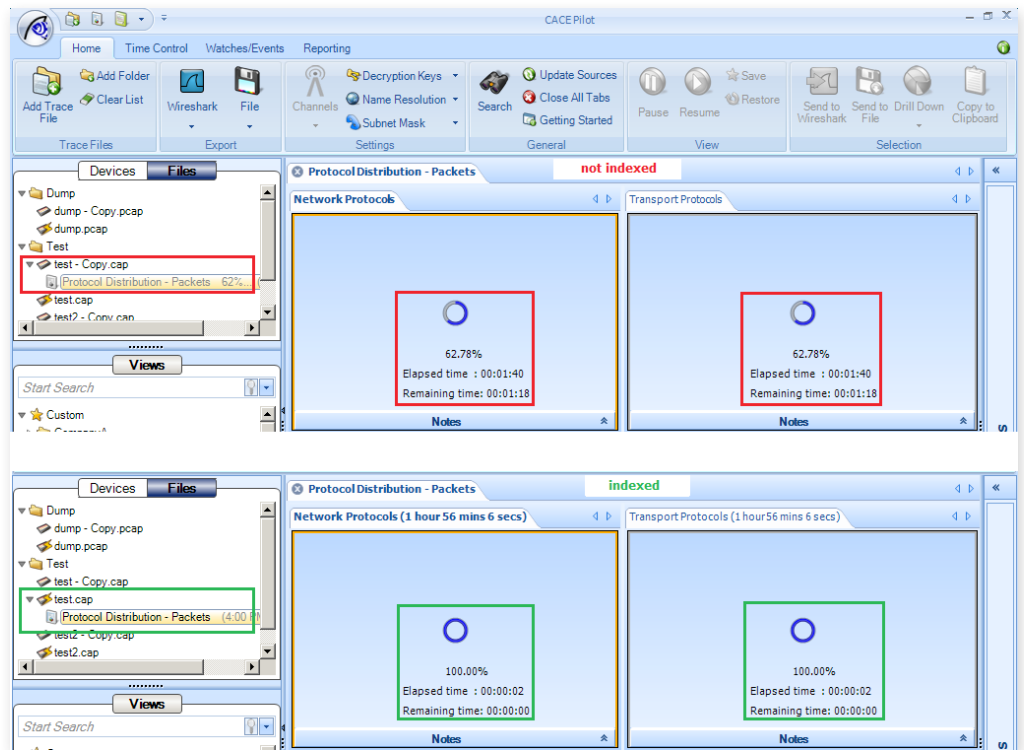
Adding a Trend Index takes about the same amount of time as loading one View to a file, that is not indexed. Once you have taken the time to index the file, supported Views load in seconds.

Note: These numbers count for this capture file on my machine. Different files or different hardware means different numbers. Take advantage of Indexing and just wait once for a couple of minutes.



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.



CACE Technologies

1949 5th Street, Suite 103
 Davis, CA 95616
 tel: 530.758.2790
 fax: 530.758.2781
www.cacetechnology.com