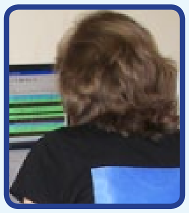
CACE Pilot: Views and Capture Filters

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.

Introduction

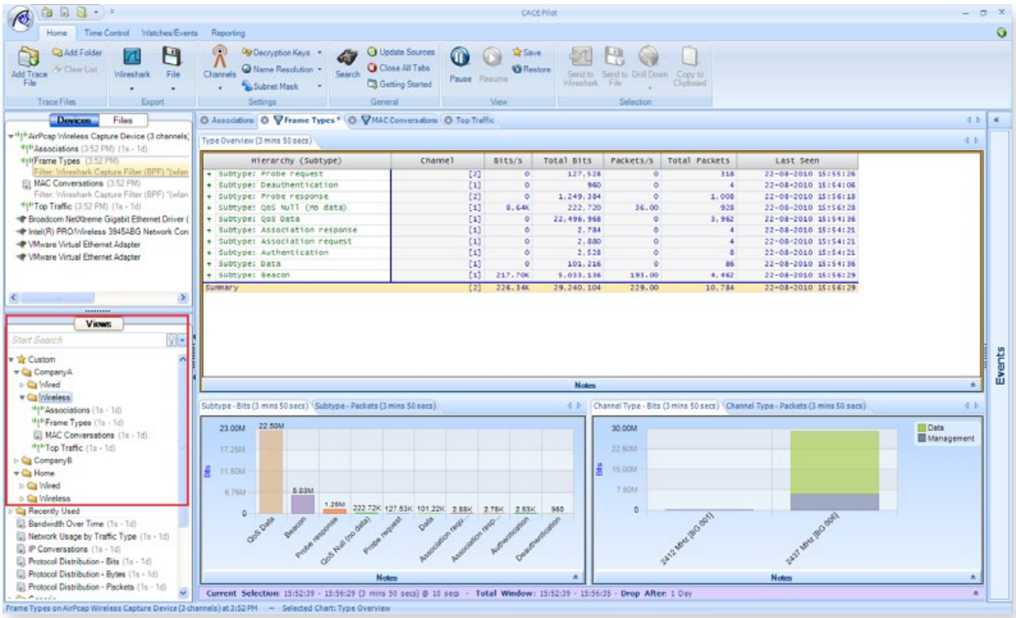
CACE Pilot, a network visualization and analysis tool from CACE Technologies, is fully integrated with Wireshark. Here you can read more about the latest release: version 2.3. In this article I will show how to organize Views and how to add capture filters to Views.

Views

CACE Pilot is shipped with approximately 200 Views. 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.

You can copy the Views, which you always want to use, to a custom folder. When you want to analyze a capture file, you just have to drag and drop the custom folder on the capture file and all the Views in the folder are applied at once.

It is even more handy to create several custom folders for different companies, locations, networks and so on. Copy the Views, you need to those folders. Next you can also set capture or display filters to those Views. These filters are saved in the Views. And again; you can apply them all at once by dragging and dropping the whole folder on a capture device or a capture file. It is also a good idea to create folders to monitor your wired and wireless home network.Want to see how this works? Continue reading to see how to manage the folders and how to add capture filters.



Type Overview (3 mins 50 secs)

Hierarchy (Subtype)	Channel	Bits/s	Total Bits	Packets/s	Total Packets	Last Seen
+ Subtype: Probe request	[2]	0	127,528	0	318	22-08-2010 15:55:26
+ Subtype: Deauthentication	[1]	0	960	0	4	22-08-2010 15:54:06
+ Subtype: Probe response	[2]	0	1,249,384	0	1,008	22-08-2010 15:56:18
+ Subtype: QoS Null (no data)	[1]	8.64K	222,720	36.00	928	22-08-2010 15:56:28
+ Subtype: QoS Data	[1]	0	22,496,968	0	3,962	22-08-2010 15:54:36
+ Subtype: Association response	[1]	0	2,784	0	4	22-08-2010 15:54:21
+ Subtype: Association request	[1]	0	2,880	0	4	22-08-2010 15:54:21
+ Subtype: Authentication	[1]	0	2,528	0	8	22-08-2010 15:54:21
+ Subtype: Data	[1]	0	101,216	0	86	22-08-2010 15:54:36
+ Subtype: Beacon	[1]	217.70K	5,033,136	193.00	4,462	22-08-2010 15:56:29
Summary	[2]	226.34K	29,240,104	229.00	10,784	22-08-2010 15:56:29

Current Selection: 15:52:39 - 15:56:29 (3 mins 50 secs) @ 10 secs - Total Window: 15:52:39 - 15:56:35 - Drop After: 1 Day

Frame Types on AirPcap Wireless Capture Device (3 channels) at 3:52 PM — Selected Chart: Type Overview

Create Custom Folders

1. Right-click on: Custom

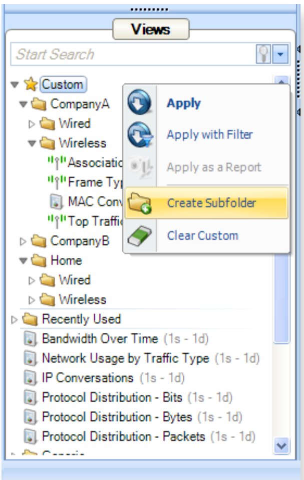
2. Select: Create Subfolder

3. Scroll down and look for the Views you want to copy to the folders you have just created.

4. Select the View.

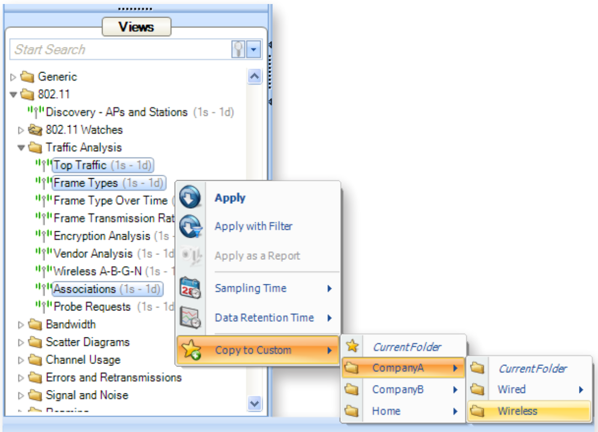
5. Use the CTRL-key to select multiple Views.

6. Right-click and select the appropriate folder.


Views
Start Search
Custom
CompanyA
Wired
Wireless
Associatio
Frame Ty
MAC Con
Top Traffi
CompanyB
Home
Wired
Wireless
Recently Used
Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)
IP Conversations (1s - 1d)
Protocol Distribution - Bits (1s - 1d)
Protocol Distribution - Bytes (1s - 1d)
Protocol Distribution - Packets (1s - 1d)
Apply
Apply with Filter
Apply as a Report
Create Subfolder
Clear Custom

Add a capture filter to a View

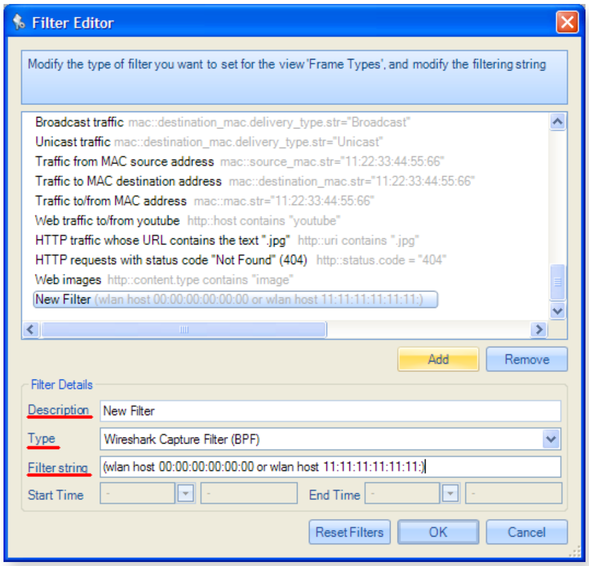
1. Right-click the View, you want to apply the filter to.
2. Select: User Filter
3. Select: Set



Choose one of the filters or create you own filter by hitting Add.

1. Choose a name
2. Select Wireshark Capture Filter (BPF)
3. Add filter string

You can find more nformation about capture filter in the Wireshark User's Guide, the Wireshark Wiki or my previous articles about capture filter samples.



Modify the type of filter you want to set for the view 'Frame Types', and modify the filtering string

Broadcast traffic mac::destination_mac.delivery_type.str="Broadcast"
Unicast traffic mac::destination_mac.delivery_type.str="Unicast"
Traffic from MAC source address mac::source_mac.str="11:22:33:44:55:66"
Traffic to MAC destination address mac::destination_mac.str="11:22:33:44:55:66"
Traffic to/from MAC address mac::mac.str="11:22:33:44:55:66"
Web traffic to/from youtube http::host contains "youtube"
HTTP traffic whose URL contains the text ".jpg" http::uri contains ".jpg"
HTTP requests with status code "Not Found" (404) http::status.code = "404"
Web images http::content.type contains "image"
New Filter (wlan host 00:00:00:00:00:00 or wlan host 11:11:11:11:11:11:)

Filter Details

Description: New Filter
Type: Wireshark Capture Filter (BPF)
Filter string: (wlan host 00:00:00:00:00:00 or wlan host 11:11:11:11:11:11:)
Start Time: - -
End Time: - -

When you are done, drag and drop the folder to the capture device or the capture file.

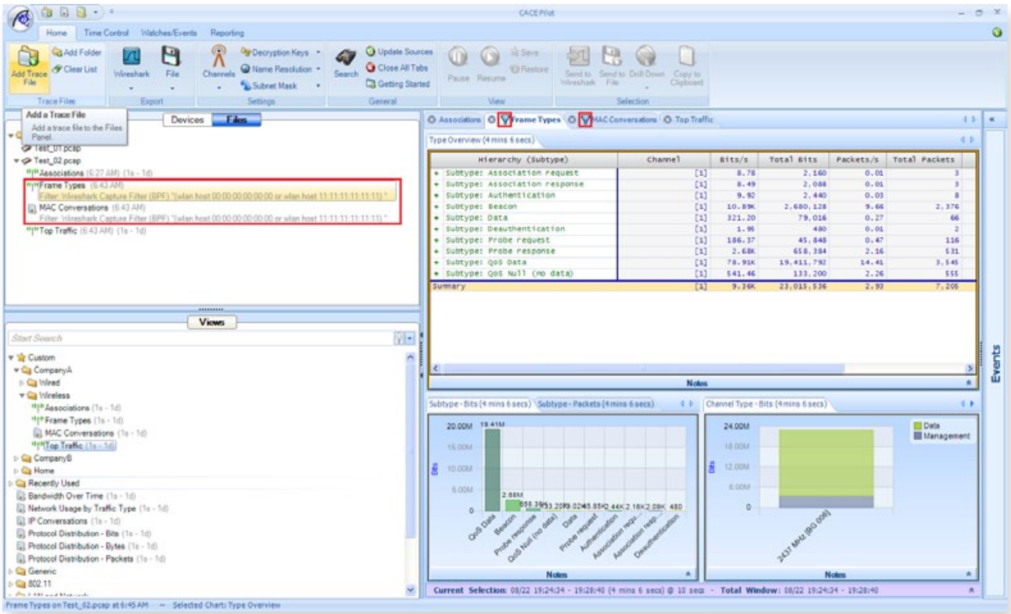
Note

The filters symbols show which Views contain filters. You can also see the filter syntax on the left side.

Get a full-featured 10-day free trial of CACE Pilot.

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.



Filter: Wireshark Capture Filter (BPF) "(wlan host 00:00:00:00:00:00 or wlan host 11:11:11:11:11:11)"

Filter: Wireshark Capture Filter (BPF) "(wlan host 00:00:00:00:00:00 or wlan host 11:11:11:11:11:11)"

Hierarchy (Subtype)	Channel	Bits/s	Total Bits	Packets/s	Total Packets
Subtype: Association request	[1]	8.78	2,160	0.01	3
Subtype: Association response	[1]	8.49	2,088	0.01	3
Subtype: Authentication	[1]	9.92	2,440	0.03	8
Subtype: Beacon	[1]	10.89K	2,680,128	9.66	2,376
Subtype: Data	[1]	321.20	79,016	0.27	66
Subtype: Deauthentication	[1]	1.95	480	0.01	2
Subtype: Probe request	[1]	186.37	45,848	0.47	116
Subtype: Probe response	[1]	2.68K	658,384	2.16	531
Subtype: QoS Data	[1]	78.91K	19,411,792	14.41	3,545
Subtype: QoS Null (no data)	[1]	541.46	133,200	2.26	555
Summary	[1]	9.36K	23,015,536	2.93	7,206

Current Selection: 08/22 19:24:34 - 19:28:40 (4 mins 6 secs) @ 10 secs - Total Window: 08/22 19:24:34 - 19:28:40

Frame Types on Test_02.pcap at 6:45 AM — Selected Chart: Type Overview

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