WildPackets

EtherPeek NX™

real-time expert protocol analysis

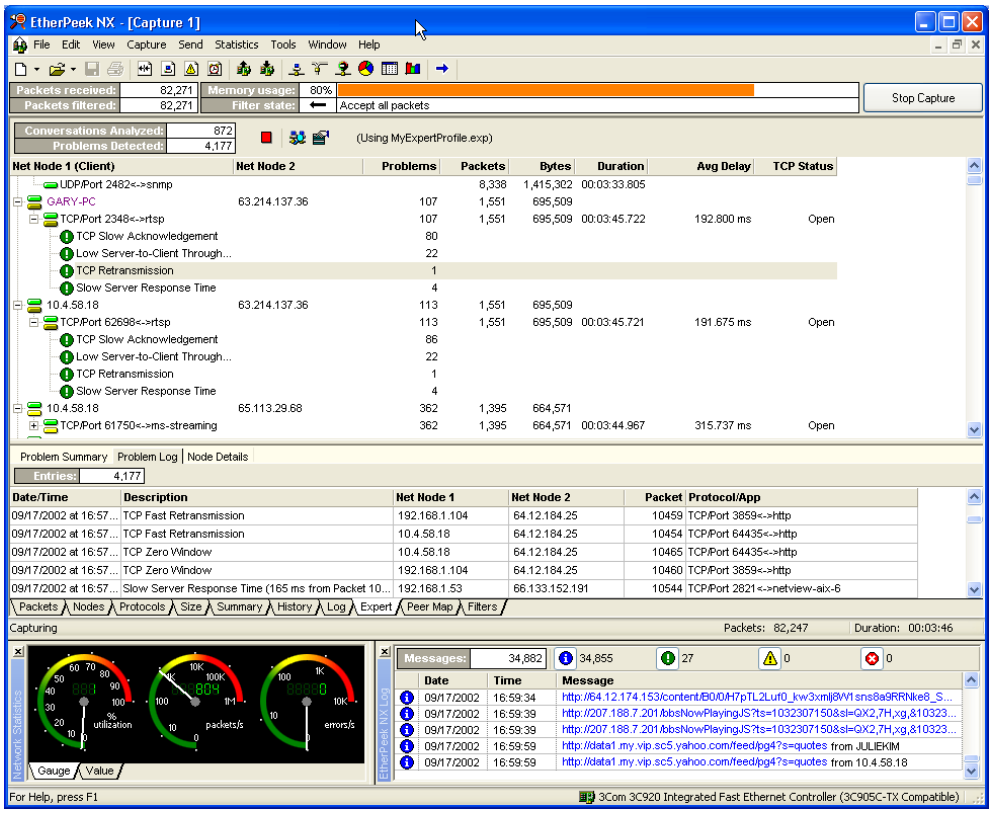
Ten Cool Things

Contents

10 Cool Things You Can Do With EtherPeek NX

EtherPeek NX is the first protocol analyzer to offer both expert diagnostics and frame decoding in real time, during capture. WildPackets' EtherPeek NX has been carefully designed to help IT Professionals analyze and diagnose increasingly diverse volumes of network data, providing precise, contemporary analysis of the problems facing today's networks.

Here are ten cool things you can do today with EtherPeek NX!

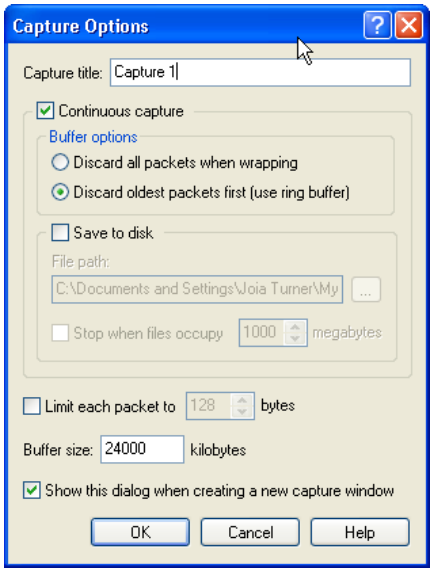


Main window of EtherPeek NX, showing the Expert view

1. Capture and view packets

Though you can see global network statistics without capturing packets, for most analysis sessions you'll want to capture packets. One of EtherPeek's many strengths is in its flexibility. This is immediately apparent in the packet list display, where you can easily customize the display.

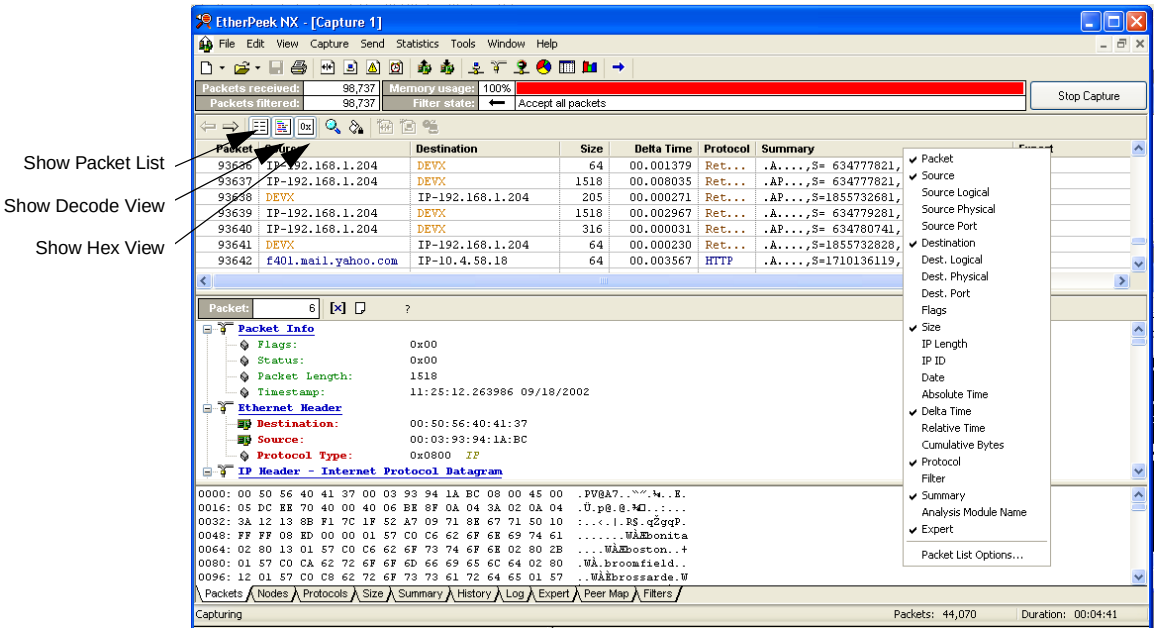
1. Click on the *New Capture* button on the **Start Page**, or pull down **File...New** from the menu bar. Click OK in the **Capture Options Dialog,** then click the Start Capture button.



2. EtherPeek provides several ways to customize your view of traffic with a single click.

a. The auto scroll option (Ctrl-K) allows you to see packets as they come in, which is useful if you're looking for particular information in the ***Summary*** or ***Expert*** columns.

b. The **Show Packet List**, **Show Decode View**, and **Show Hex View** buttons allow you to pick the content you want to see in real-time. Most other analyzers show all three (and not usually in real time) and do not allow you to toggle between the different views.

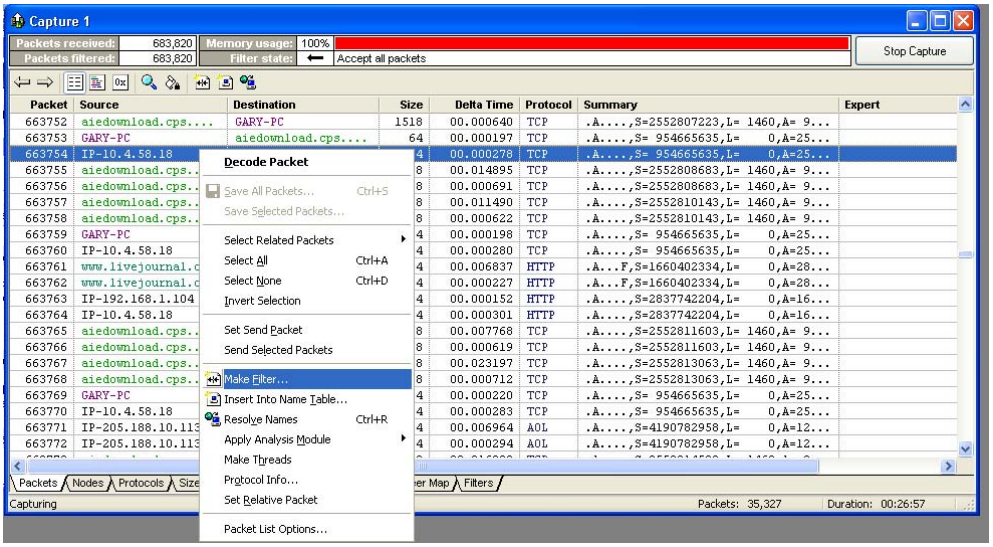


c. Right-click on one of the columns in the packet list to customize the column display.

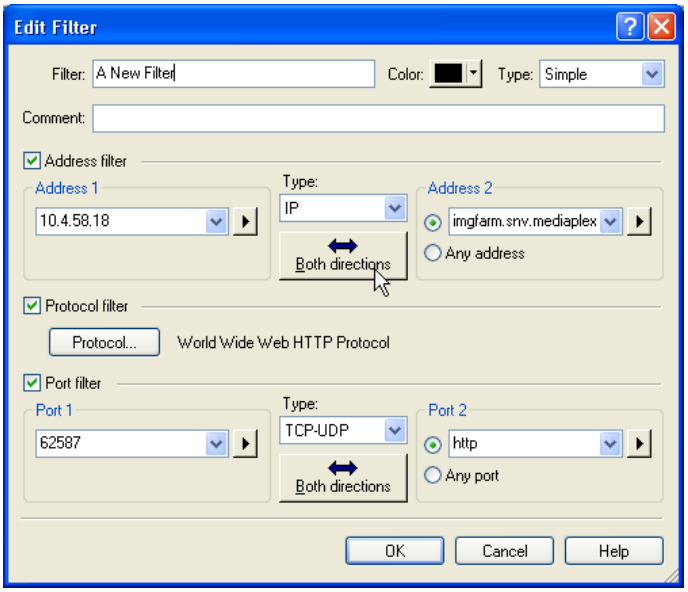
2. Capture filtering the easy way

EtherPeek ships with a set of common, pre-defined filters, but its real power is in the ease with which you can create your own filters.

1. As packets are coming in, choose something you might want to filter on, such as a protocol or source IP address. Right click on that packet (stop the scrolling, if necessary, by keying Ctrl-K).



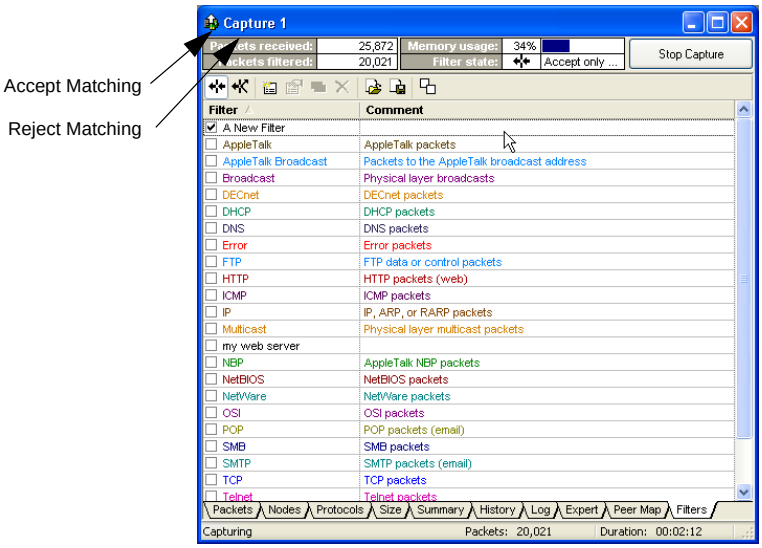
2. Click on *Make Filter* – notice that the information on the packet you chose is already set up in the **Edit Filter** dialog for you.



3. Name the filter and make modifications. You may wish to restrict the data to only one attribute, for example, source IP address or protocol.

4. Click OK to save the filter.

5. Click on the ***Filters*** tab and find your new filter in the list. Check the box next to the filter. You will now be capturing only packets that meet the criteria of that filter. (Alternatively, you can reject only those packets matching the filter criteria by clicking on the **Reject Matching** button.)

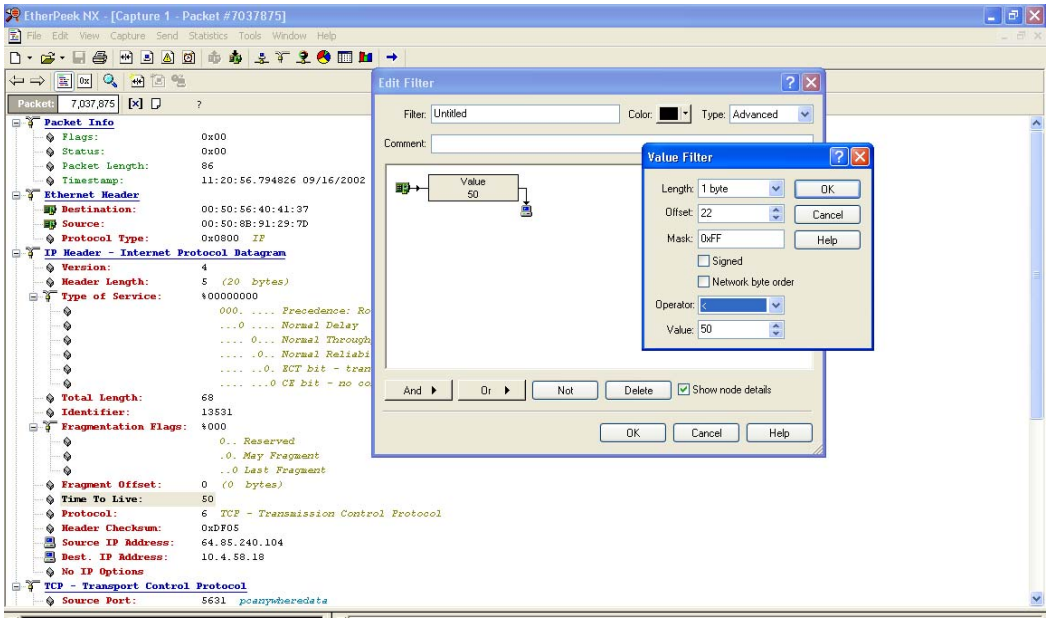


6. Go back to the packet list in the ***Packets*** view. You should only be seeing packets that meet your filter criteria. Notice the packet counts differ in the upper left corner (*Packets Received* vs. *Packets Filtered*).

3. Advanced filtering

EtherPeek's advanced filtering is easier to use than most analyzers' simple filtering. Filtering on specific protocol decode fields, for example, can be accomplished in just a couple of mouse clicks. Suppose you wanted to view all packets with a Time To Live (TTL) of under 128. A packet with a TTL of less than 128 indicates the packet has most likely traversed a router. When dealing with network slowdowns, it's interesting to understand where the packet came from and where it's going. TTL helps us understand the packet's path. Here's how to build the filter:

1. Click on the ***Packet List Tab***.
2. Choose any IP packet and double-click to open the decode view.
3. Right click on the TTL field under the IP Header section and select *k*.
4. An advanced filter is already made for you!
5. Double Click on the Value box.
6. Change the Operator to '<' (other LAN analyzers do not have this capability).



7. Name the filter and click OK.
8. Go to the ***Filters Tab*** and click on the filter you just created. Packets will then be filtered on the fly!
9. The same filter can be used for post capture analysis, too. EtherPeek doesn't force you to define filters in multiple places.

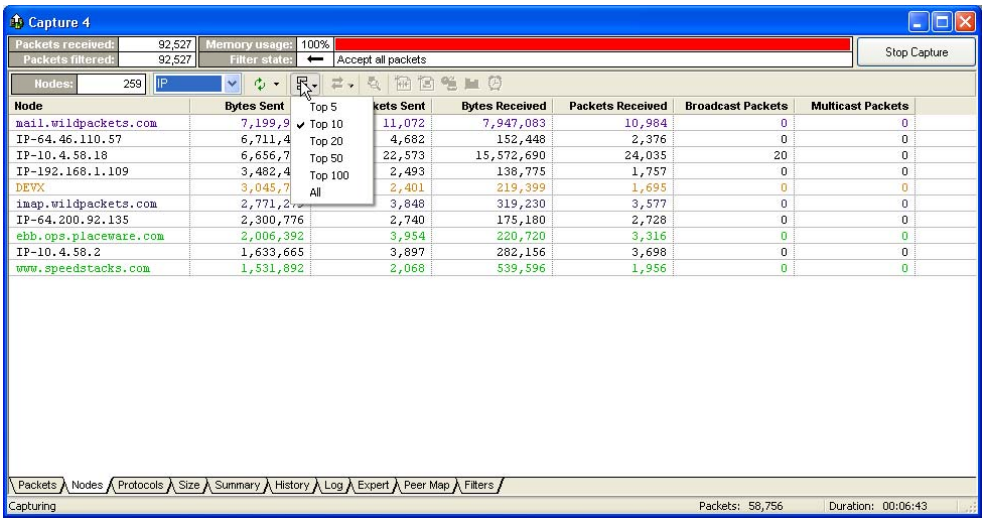
4. Who are the Top Talkers?

Top Talkers is a common troubleshooting statistic. The network is slow, for example, and you may want to see which stations are using the most bandwidth.

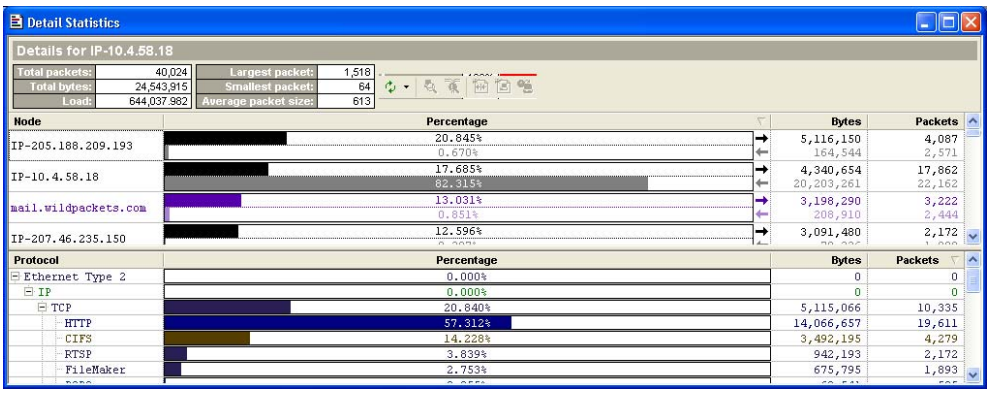
1. Click on the ***Nodes Tab***. By default, the View Type is *Hierarchical*, where logical addresses and symbolic names are nested beneath their physical addresses along with their transmit and receive statistics. However, you can easily change the default view to one showing the Top Talkers.

2. Pull down IP from the View Type, then click on a column to sort on *Bytes* or *Packets* sent or received. Right click on the columns to customize the display.

3. To view a subset of the talkers, choose a value in the *Display Top* drop down.



4. Note that you can see the top 5 or 10 or 100, etc. Double-click on a host to view its protocols in ***Detail Statistics***.

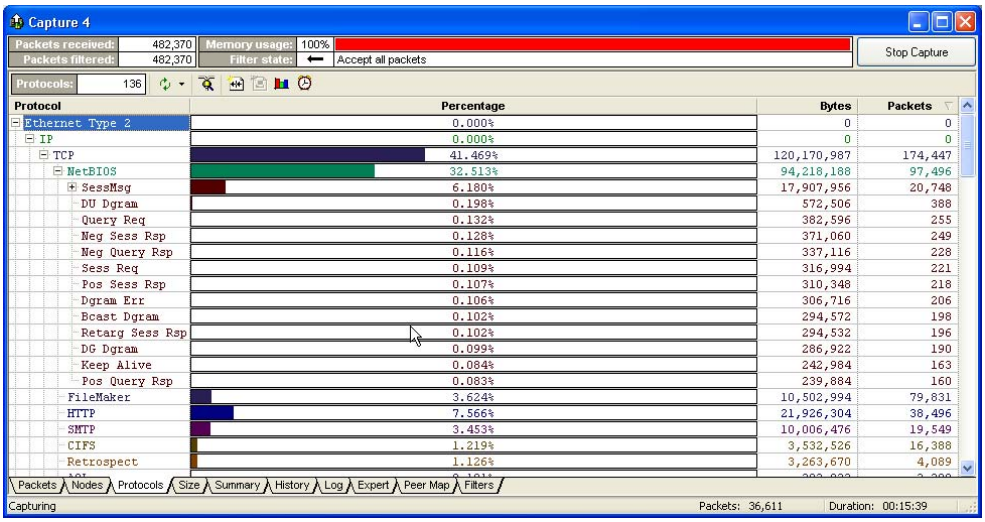


Make a filter, build an alarm, or construct a graph for any of these hosts with just a click of the mouse. EtherPeek provides you with an amazing amount of flexibility. Other analyzers decide for you what statistics will be displayed.

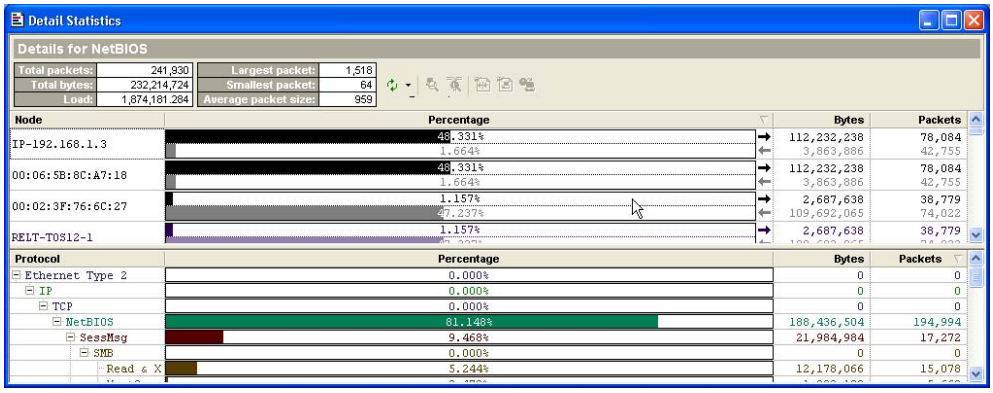
5. What protocols are on your network?

Perhaps, instead of wanting to know what users are using the most bandwidth, you want to know what applications are using up bandwidth. Are any protocol ratios too high? Are there any protocols that shouldn't be on the wire?

1. To see which applications are on your network, click on the ***Protocols Tab***.



2. Double-click on a protocol to see the % of usage by each host.

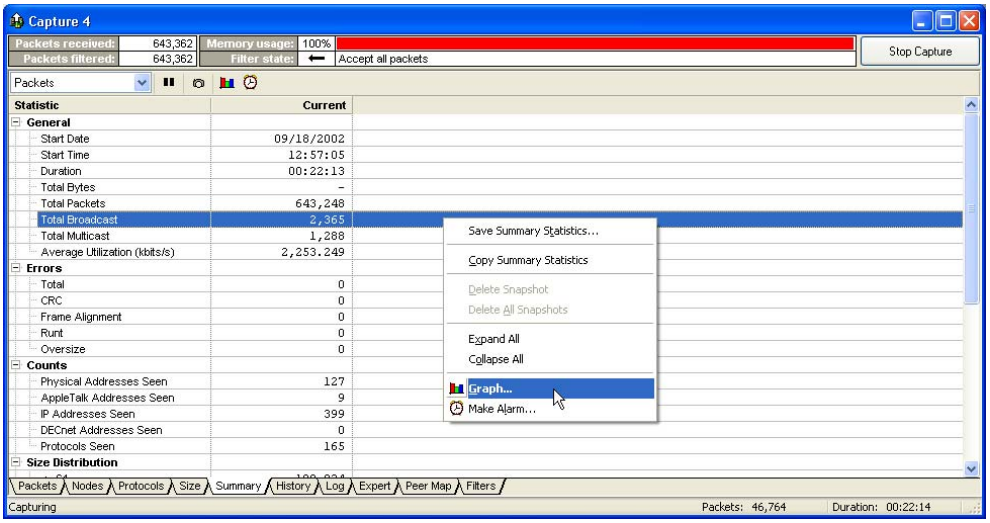


3. Return to the ***Protocols Tab***, right-click on a protocol, and *Select Related Packets*. This is a two-click method of choosing all the packets in the packet list that are talking this protocol. *Select Related* is available throughout the program: the nodes stats, expert problems, Peer Map, etc.

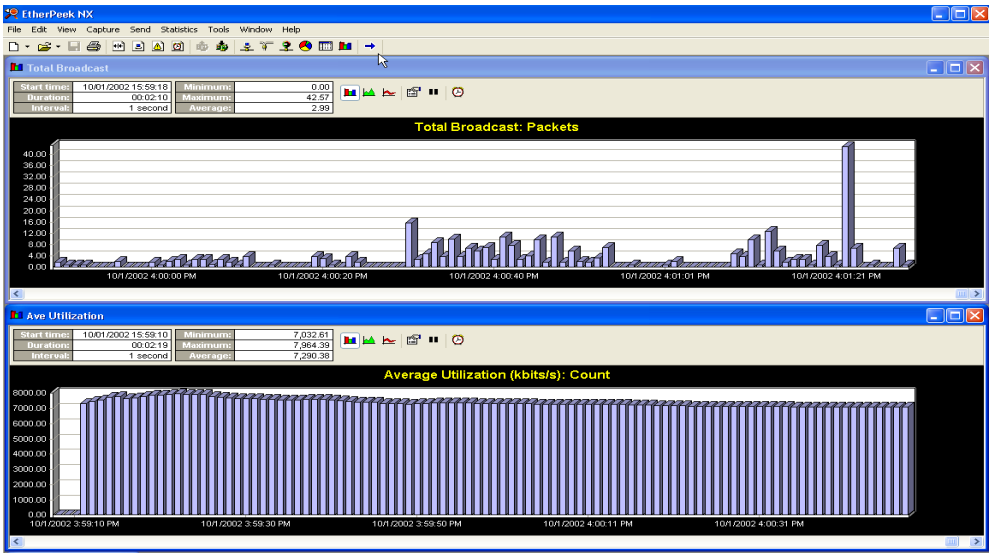
6. Make multiple graphs

EtherPeek's extensive graphing ability enables you to correlate useful statistics. For example, are broadcast packets a significant portion of your utilization?

1. Click on the ***Summary Tab***.
2. Right-click on *Total Broadcast*, and choose **Graph...** Name the graph in the **Graph Data Options** dialog and click OK.



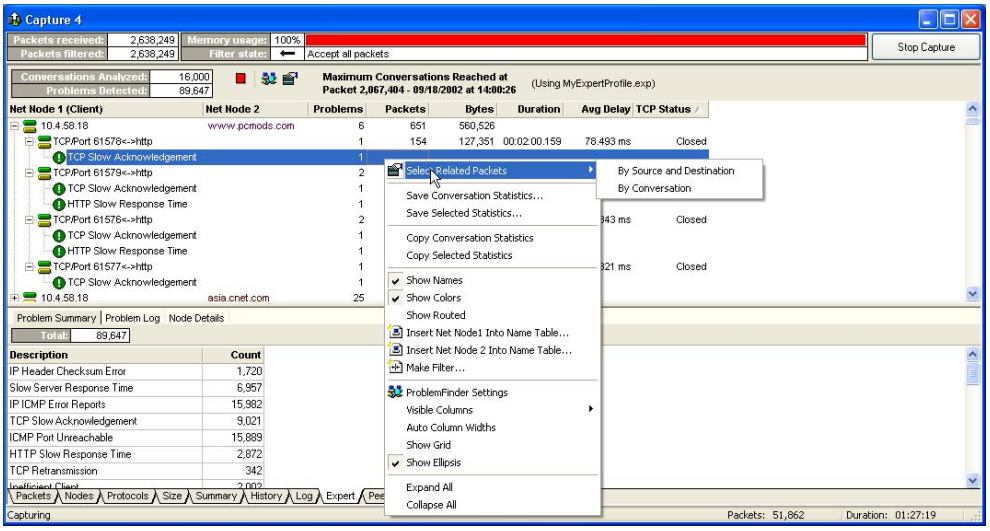
3. Right-click on *Average Utilization* and choose **Graph...** Name the graph in the **Graph Data Options** dialog and click OK.
4. Minimize the capture window and then choose **Window...Tile Horizontally**. (EtherPeek is one of the few analyzers that complies with MS Windows conventions, which is certainly helpful here!)



7. Find problem packets through “Select Related”

EtherPeek NX’s Expert Tab is by far the easiest to use and most up-to-date on the market. Problems are arranged by conversation, rather then by OSI model level. ProblemFinder tests and settings are just one right-click away, as are problem descriptions and possible remedies. Other analyzers force you to hunt and peck for the information you need. EtherPeek NX delivers this information to you automatically. It pinpoints the packets related to a network communications issue, tells you why it’s probably happening, and suggests ways to fix the problem.

1. Click on the ***Expert Tab***.
2. Right-click on the first host, and choose *Expand All*.

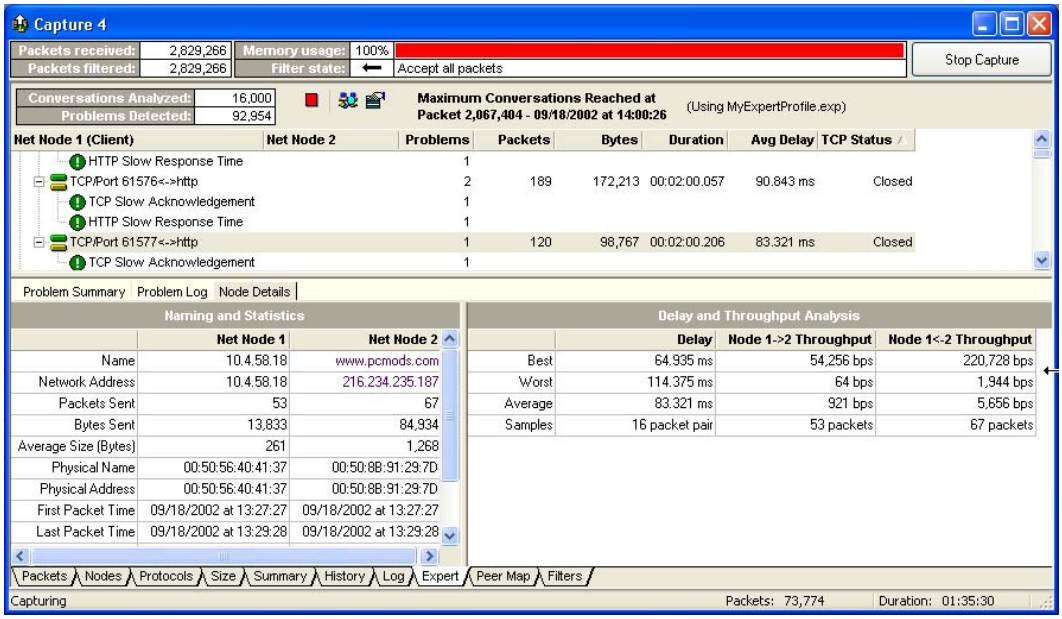


3. Scroll down until you find a particular problem you’d like to look at.
4. Right-click and Choose *Select Related Packets* by *Source and Destination* or by *Conversation*.
5. Alternatively, you can go straight to the ***Problem Summary Log*** and select all packets related to a particular problem. Note how the conversations having this issue are highlighted when you return to the ***Packets*** view.

8. Determine Application Response Time

Application Response Time is available via the ***Expert Tab***, where detailed round trip analysis of command-response packets is available, showing you the best, worst, and average delay. In a similar fashion, throughput is also analyzed.

1. Click on the ***Expert Tab***
2. Click on the *Node Details* tab.

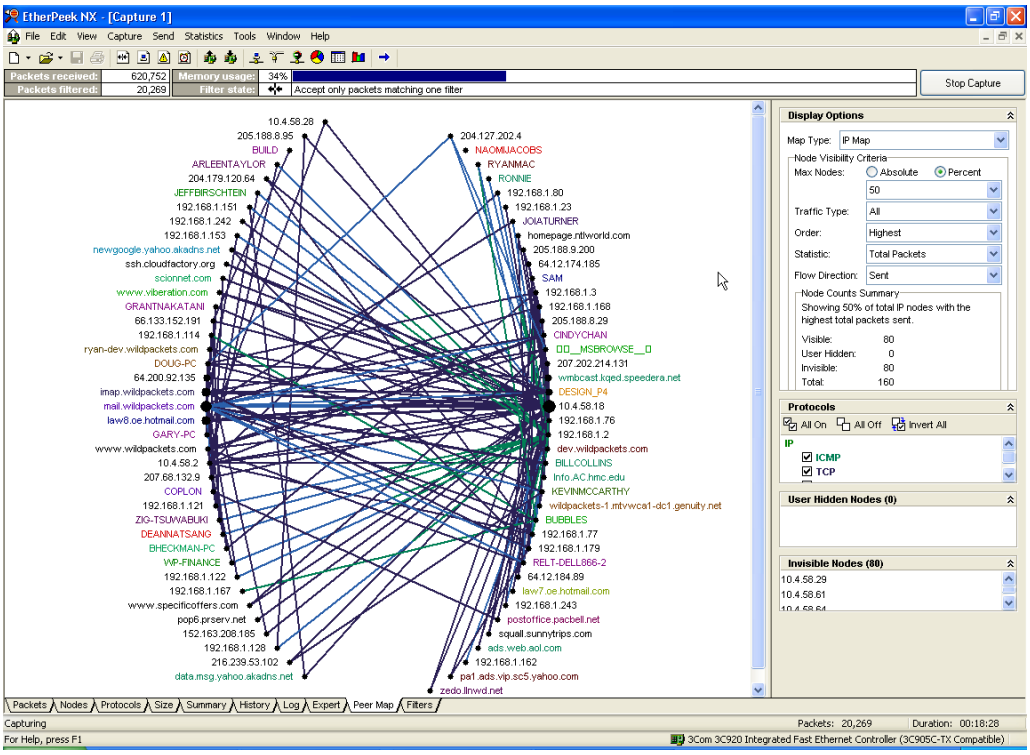


3. Right-click on the first host in the conversation tree, and choose *Expand All*.
4. Walk down the tree until you see an interesting analysis in the *Delay and Throughput Analysis* display in the lower right.

9. Visualize your network with expert mapping

The Peer Map is a great way to get a visual perspective of your network. Not only can you select related packets from hosts on the map, but you can easily create ad hoc filters or look at Top Talkers.

1. Click on the ***Peer Map Tab.***



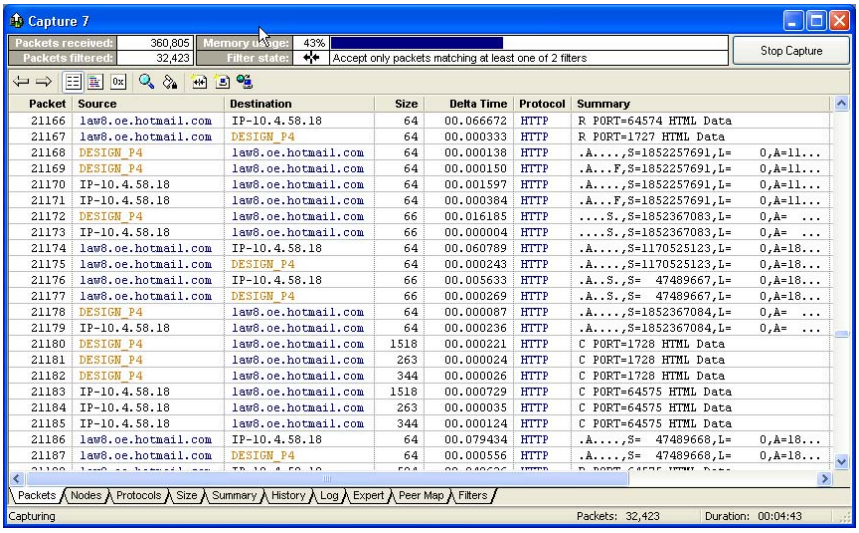
2. Choose *IP Map* from the *Map Type* pull down in the upper right hand corner.
3. In the *Node Visibility Criteria* area just below, you can choose Top Talkers via absolute number or, say, top 10%.

   The amount of traffic through a node is represented by the size of a dot. And if there is one host, such as a mail server or a web server,Top Talkers that is skewing the results you are looking for, you can drag that node into the Hidden Node field.

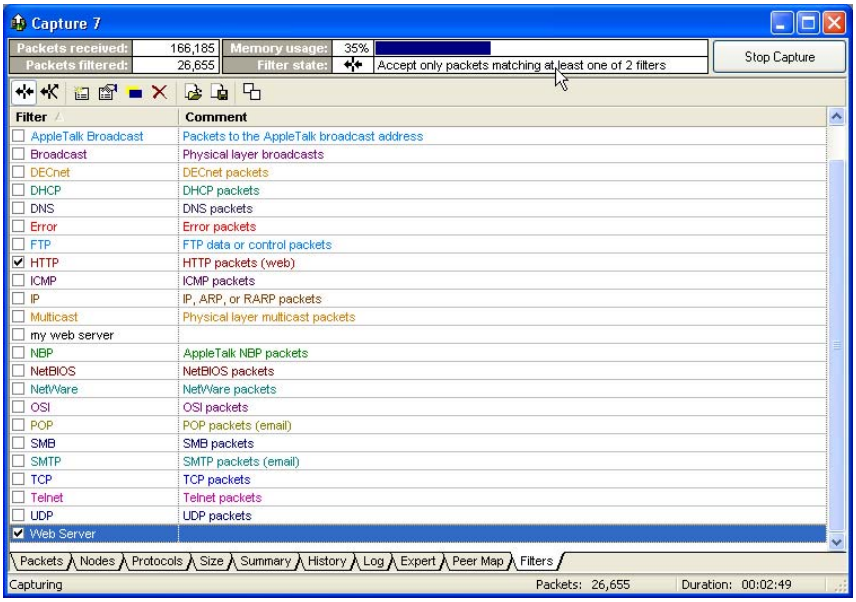
10. Find that slow web server fast

With EtherPeeks' Expert System, you can easily spot slow servers. Here's an example of how to troubleshoot a slow web server.

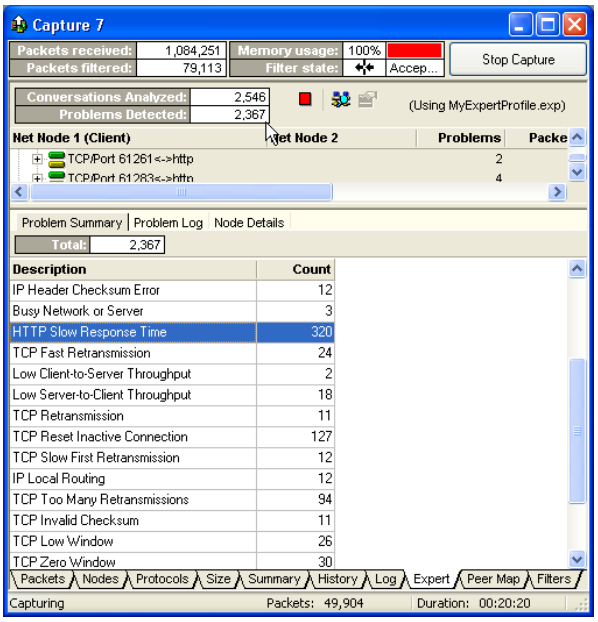
1. Start a new capture.
2. EtherPeek NX ships with many standard filters, including HTTP. Click on the ***Filters Tab*** and check the HTTP filter to immediately activate it.
3. Go back to the ***Packets*** view. Enable Scrolling (Ctrl-K) so you can see incoming packets. Verify that they are HTTP packets.



4. You may see HTTP access from web traffic not associated with your web server, so you will need to add a new filter. Open a browser and go to your web server. You should see your web server in the packet list display. Create a filter by right-clicking on that packet and choosing *Make Filter.*
5. Go to the ***Filters Tab*** and enable the filter you just created.

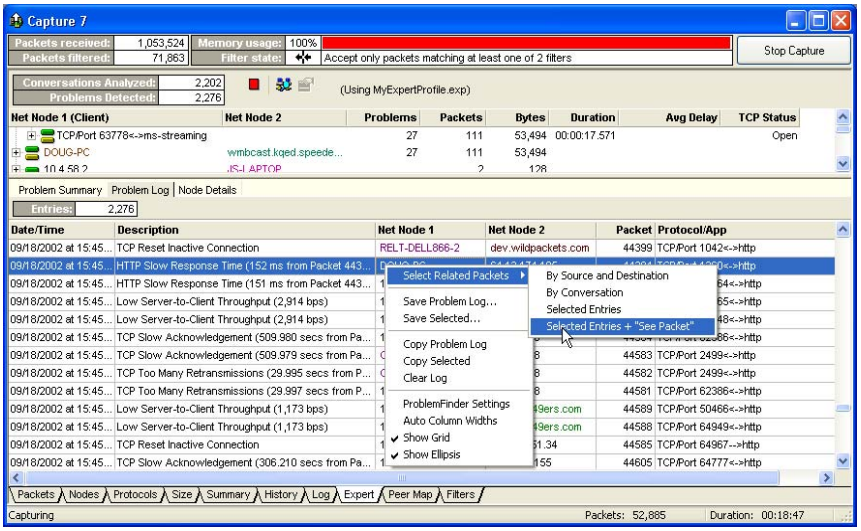


6. Now go to the ***Expert Tab***. Click the *Problem Summary* pane and check for *TCP Resets* or *HTTP Slow Response* time diagnoses.



7. The *Problem Log* pane provides more detail, including actual time delay between specific packets (e.g. 6.472 seconds from Packet 4).

8. Right-click and select related packets by *See Packet*.



9. Go to the ***Packets*** view and your problem packet is highlighted!

10. From there, try and figure out what sort of packet it is. Does it say Data in the *Summary Column*? What is this packet in response to? Click through the packets that preceded the bad packet.

    Unlike other analyzers, EtherPeek's NX expert system ignores the ACKs when determining the HTTP Slow Response diagnosis. Look to see if the ACK was received right away. If so, and it was the data packet that triggered the diagnosis, you know it was the web server that was slow and not the network.

WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

WildPackets Academy

WildPackets Academy provides the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for Ethernet and 802.11 wireless LANs.

In addition to classroom-taught Network Analysis Courses, WildPackets Academy also offers:

- Web-Delivered Training
- On-site and Custom Courseware Delivery
- The Technology, Engineering, and Networking Video Workshop Series
- On-site and Remote Consulting Services
- Instruction and testing for the Network Analysis Expert (NAX™) Certification

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit www.wildpackets.com/academy. NAX examination and certification details are available at www.nax2000.com.

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek NX/EtherPeek and AiroPeek NX/AiroPeek, led by a WildPackets Academy Instructor. Please visit www.wildpackets.com for complete details and scheduling information.

About WildPackets, Inc

WildPackets, a privately-held corporation, was founded in 1990 with a mission to create software-based tools to simplify the complex tasks associated with maintaining, troubleshooting, and optimizing evolving computer networks. WildPackets' patented, core "Peek" technology is the development base for EtherPeek™, TokenPeek™, AiroPeek™, and the NX™ family of expert packet analyzers. All are recognized as the analysis tools of choice for small, medium, and large enterprise customers, allowing IT Professionals to easily maximize network productivity. Information on WildPackets, WildPackets Academy, Professional Services, products, and partners is available at www.wildpackets.com.

WildPackets, Inc.
925-937-7900
www.wildpackets.com