T-SIGHT TUTORIAL Provided by En Garde Systems, Inc.

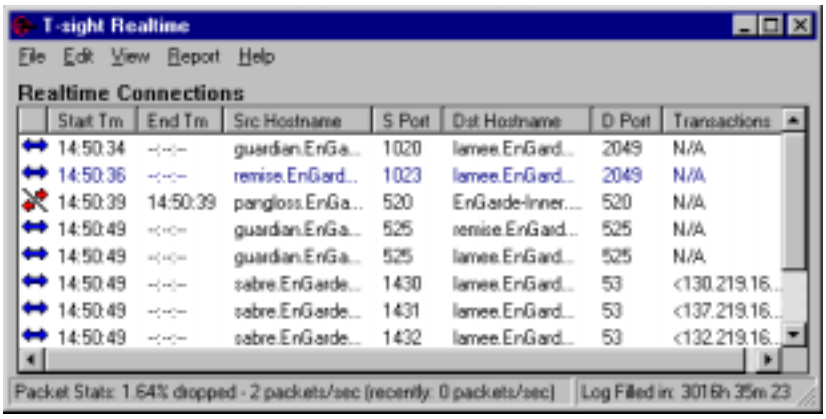
The tutorial can also be found on the CD or on line at:
http://www.engarde.com/software/t-sight/tutorial/.

T-Sight Realtime Tutorial

This section contains a tutorial on how to use T-Sight to monitor your network in realtime for suspicious activity, and then to respond to that activity with T-Sight's Active Countermeasures.

After installing T-Sight under Windows NT 4.0 (including the device driver) and rebooting, you should now be able to run T-Sight Realtime Monitor.

- Go to the "Start" menu, then the T-Sight folder that was added when you installed.
- Run T-Sight Realtime Monitor. (If you don't see it there, use Windows Explorer to go to the directory where you installed T-Sight and run "tsrltime.exe")



This is the main realtime window (Yours will appear differently based upon what traffic is active on your network. If you see none, run the Windows "telnet" program and connect to a server on your network). Its functionality is identical to that of the Post Mortem Analysis program, but you'll notice a few minor changes. First, there is no toolbar along the top. This is because many of the analysis tools are available exclusively in T-Sight PostMortem Analysis. Second, there are network statistics at the bottom of the screen. This doesn't reflect the number of bytes/second, but it is a good indication of how much work T-Sight Realtime (and your Windows NT system) is doing.

In this example, the bottom left status line shows that 1.64% of the packets have been dropped (ie. went by too fast for the monitor and workstation to process) and that since the program was first run, there have averaged 2 packets/second on the network, but most recently (in the last second), 0 packets went by. The bottom right status line shows the estimated time remaining until your disk is filled with TCF logs based upon current network activity. In this case, a sustained rate of around 24Kbits/sec (this number is derived, because I know the 2 packets/sec averaged around 1500 bytes each because I created them) will fill the disk in 106 hours, 39 minutes, 41 seconds. At that time, T-Sight Realtime should be stopped, the TCF file backed up somewhere else, and restarted.

- Find an active session (one with the blue arrow connected icon), and double click it.
- Select "Realtime Playback", and hit "Generate". (Any of the others (Server Text, Client Text, Raw Packet) will also work in realtime, but you won't see both the client and server data)

Again, this is nearly identical to the T-Sight PostMortem Analysis realtime playback window. The primary difference is that Current Time and Next Packet Time aren't displayed (you can look at the clock for the former, and the latter is known only to those higher up than us). Beneath, the Status indicator shows whether this session is Active, Dead (the user logged out), or Hijacked (if you hit the Take Over button).

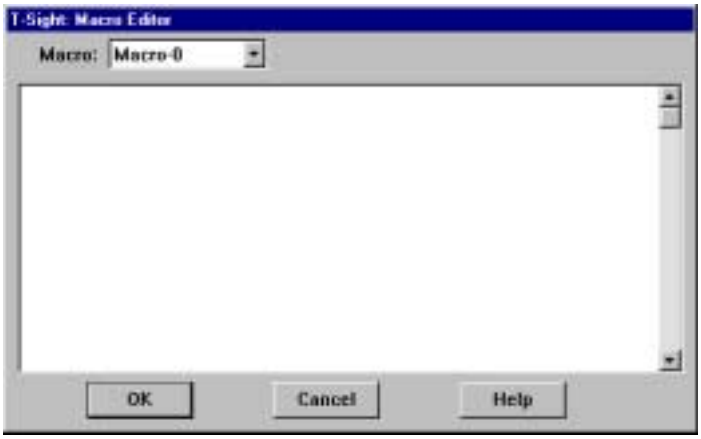
NOTE: In the following, "Spoofing" describes sending packets that are bogus, but have the appearance to be valid. Because Spoofing is ocasionally takes TCP stacks outside the realm of what is defined in the protocol, you must be very careful! Sometimes you'll need to try the countermeasure several times before it works properly. In all cases where the session is hijacked ("Take Over", "Send" (both client and server)), you WILL create an "ACK war". This is a state whereby the two endpoints of a connection no longer know how to communicate to each other properly. As a result, the TCP Stacks (invisible to the user and the server software) will attempt to negotiate a new "ACK" number. This can never succeed and results in an extremely high-speed flood of packets on the network. To terminate this flood, you must hit the "Terminate" signal shortly after hijacking the session and sending the commands you wish. Also, note that this is not a rock-solid protocol like TCP is. It's possible you will have to type commands several times for them to get through. When hijacking, you're at a much lower level that TCP normally provides in terms of reliability, in-order and guaranteed delivery.

The "Terminate" button will instantly kill any active TCP/IP connection by spoofing RST packets in both directions.

The "Take Over" button will hijack the connection, and allow you to type in the server window any commands you have. (Just click in the white window and type your commands as if you were logged into the server). Make sure to hit "Terminate" when you're done. The state "Take Over" puts the network in will rapidly deteriorate to the point that you may only get one command in before you no longer can communicate with the server effectively. If this is a problem, use the "Send Macro" feature as described below.

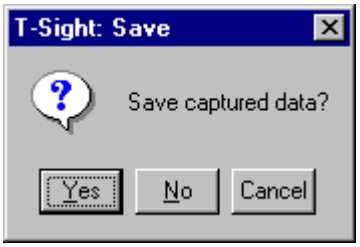
The "Send Macro" buttons will allow you to automatically hijack the connection and send a set of commands in a single packet. You can select which macro to send with the combo box immediately above the "Send Macro" buttons. The "Send Macro (Client)" button will send the predefined macro to the client side of the connection (useful for sending "buzz off" type messages), and the "Send Macro (Server)" button will send a predefined macro to the server side (useful for sending a bunch of commands).

- Select the "Edit" -> "Macros" menu item



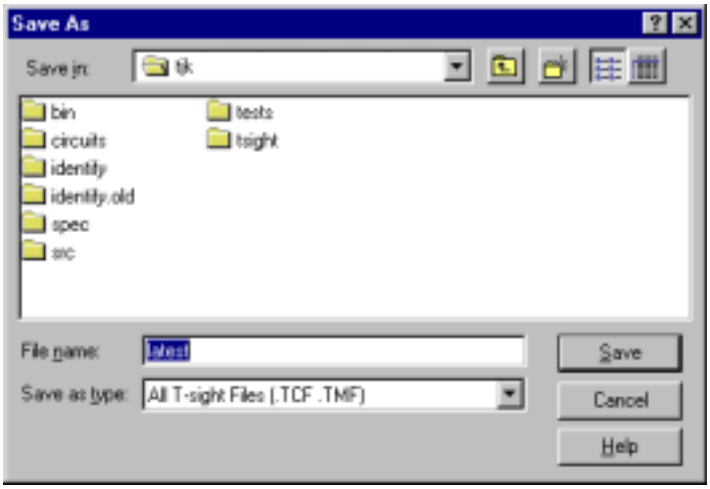
In this window you can define the macros that will be sent. Select the macro from the combo box at the top of the window, and type in (or edit the existing) macro in the edit window. You can use the typical C \ sequences to send special characters (such as \n for newline, \r for return, \e for escape). You can also specify ASCII codes in octal (for example \010 sends a backspace). You can also use control character look-alikes (for example, ^M sends a return, ^H sends a backspace).

- Close the macro and realtime playback window.
- On the main window, select "File" -> "Quit"



This window asks if you want to save all of the data you've captured thus far. If you say "No", it will erase all of the captured data from your disks.

- Click "Yes"

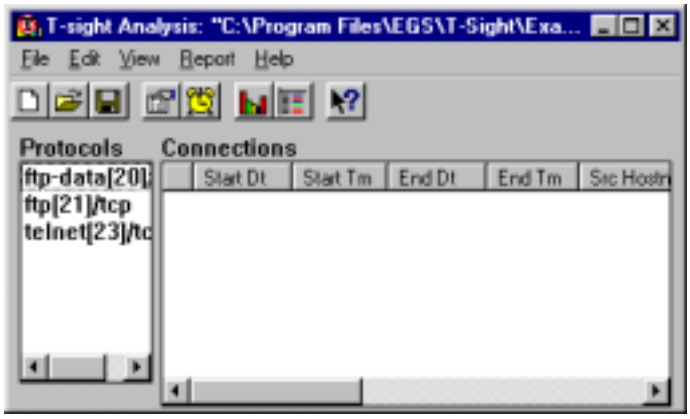


T-Sight PostMortem Tutorial

This section contains a tutorial on how to use T-Sight PostMortem to analyze network traffic. It won't make you an expert user, but it will visit all of the important parts of the program to make sure you've seen everything and understand generally why it's there.

Several example TCF files have been included with the T-Sight distribution. They are in the \Examples directory (either on the CD, wherever you told PackageForTheWeb to use for the T-Sight distribution, or in the T-Sight installation directory if you chose "Custom" install and selected "Example files"). The multi.tcf file included with T-sight is **not** the correct version of the file. Download the new one at: ftp://ftp.engarde.com/pub/t-sight/multi.tcf.

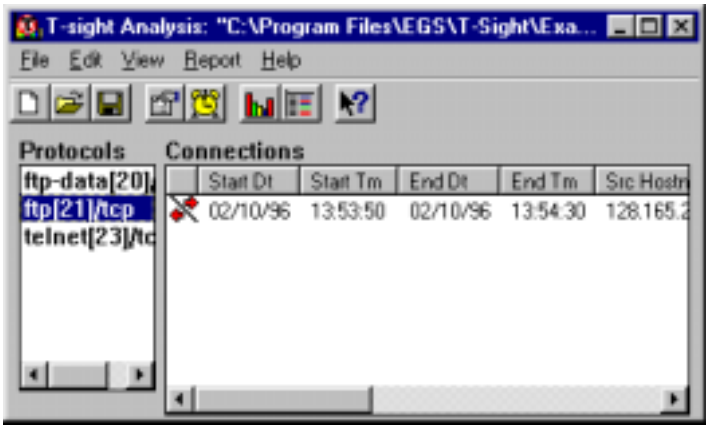
- Using the Windows Explorer, open \Examples\attack.tcf



On the left side, you'll see the Protocols that are contained in this TCF. For example, telnet[23]/tcp means it's the telnet service (port 23), using the TCP protocol. On the right side, you'll see all of the Connections that used the selected Protocol. In this case, no protocol is selected, so no connections are shown.

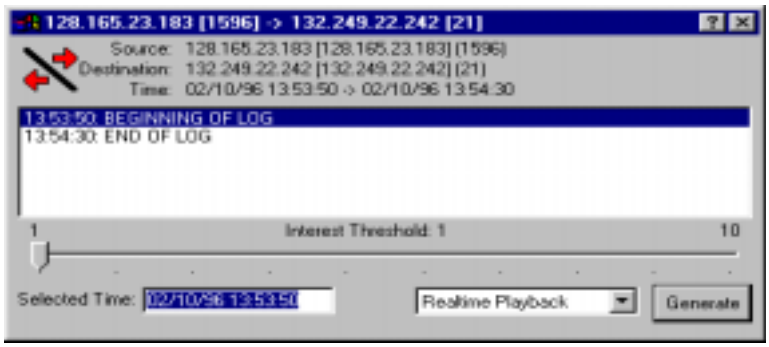
Other display modes are available. Go to the "view" menu and any one of "by Protocol" (what you're seeing now), "by Source", "by Destination", "in Realtime".

- Make sure you're in "by Protocol" mode, and Double-Click the "ftp" protocol list entry, and expand the window width-wise to see more.



In this particular TCF, there is only one FTP connection that was recorded. The red icon indicates the connection is currently broken (the actual end of connection was seen. In some cases, the end of connection was not recorded, so the icon changes to reflect that fact). "Start Dt" is the Date the first packet of the connection was recorded, "Start Tm" is the time the first packet was recorded, and similarly for "End Dt" and "End Tm". "Src IP Addr" is the IP Address of the client of the connection and "S Port" is the TCP port on their end. "Dst IP Addr" is the IP Address of the server, and "D Port" is the TCP Port--in this case 21 (or FTP). The "Transactions" column shows the last, most important transaction that occurred for each connection. In this case, the last most important transaction was the retrieval of the file "normM.2.10".

- Double Click on the only Connection



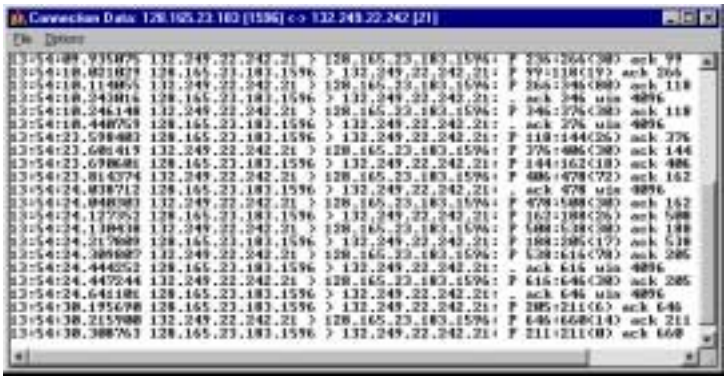
Here you will see information about the specific connection you've chosen. The header contains the source and destination IP Addresses, hostnames (if available--not in this case), and ports, as well as the duration of the connection. In the scrolling list you see every transaction that occurred during this connection. Transactions initiated by the server begin with a "<", transactions initiated by the client begin with a ">". The number beginning with a "+" is the number of minutes and seconds after the beginning of the connection (think of it as the opposite of "T Minus n minutes).

In this case, you will see the server sent its greeting banner, the client sent the "USER" command with a username of "bhass". The server then asked for the Password, and the user sent the "PASS" command with a password of "}{!*144**".

There is significant clutter in this list, and you may not particularly care if the server sent a greeting banner or not. To declutter the display, move the Interest Threshold higher. On Interest Threshold "1", all transactions are displayed regardless of how meaningless. On Interest Threshold "10", nothing is shown but the start and end times of the session. At Interest Threshold "6" you will get only the username, password, and files retrieved. At Interest Threshold "9" you will only get the files retrieved and nothing else.

Suppose you are particularly interested in seeing the contents of the session starting where the user typed his Password.

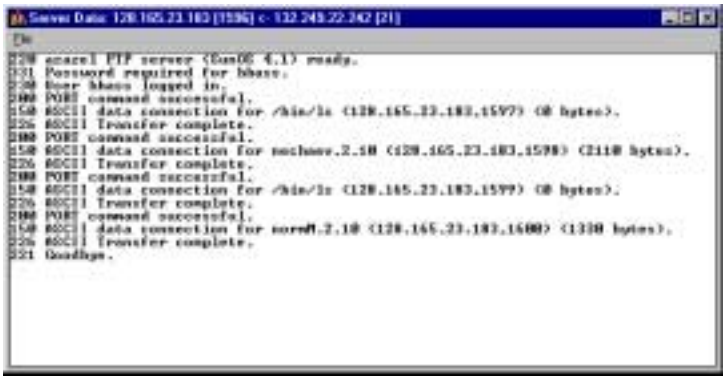
- Double click on the "Password" list item. Note the Selected Time changes to 2/10/96 13:53:59 (or T+000:09)
- Click on the "Realtime Playback" combo box, and select "Raw Packet Trace"
- Click "Generate"



Note that a raw packet trace of the connection in question is displayed in standard Tcpdump text-mode output. Also note that the start time of the transaction you selected appears at the top of the window.

If you check other boxes from the "Options" menu, you can get more (or less) verbose decoding of the individual packets.

This feature is useful if you need to see exactly which options were sent. For example, you see an rlogin connection from outside your network, when it should have been filtered by your firewall. Using this feature, you can easily tell whether the packets were spoofed using a fragmentation attack, or whether it is a hapless insider who made up his own IP Address to use on his workstation.



- Click on the "Raw Packet Trace" combo box and select "Server Text"
- Click "Generate"

This window displays the text that was sent by the server to the client. Note that none of the user commands are visible (they were sent by the client to the server and were not echoed back).

This data window is useful to determine exactly what the server sent over a connection. Similarly, the "Client Text" window will show exactly what the client sent (including passwords, and other commands which aren't normally echoed). Overall, if you're not interested in keystroke timing, or seeing exactly what was typed and when, this window and the "Client Text" window will do exactly what you want.

- Click on the "Server Text" combo box, and select "Realtime Playback"

This window plays back the connection as it actually transpired, including keystroke timing, retransmissions, etc.

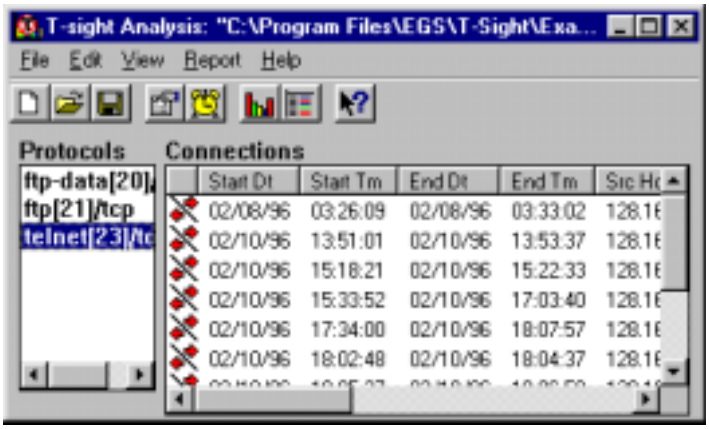
In the large, white, window you'll see all of the data sent by the server to the client. The line immediately underneath that contains the data sent by the client to the server. Underneath that, you see the start time of the connection, the end time of the connection, and the current time being displayed. The bar chart represents the percentage of this connection that has already been played.

Along the right side of the window, the section marked "CT:" displays the "Current Time". That is, if you were watching this connection as it happened on your network that is the time that would be shown on the clock. The next section, marked "LP:" shows the time of the last packet. This is useful to show if there is an ACK war, or other extraneous packets being sent which don't include printable data. The next section, "NP:" shows the time of the next packet. If you have a long wait, it might be useful to hit the "Frame Advance" button (described next).

Underneath the timing information is the control buttons. Most of these will be familiar to anyone who has used a VCR. The top row is "Rewind", "Stop", and "Play" and the second row is "Fast Forward" and "Frame Advance". "Rewind" resets playback to the beginning of the connection. "Stop" stops time where it is, and "Play" continues (or starts) it. "Fast Forward" increases the rate of playback from 1X speed to 8X speed. Clicking it multiple times cycles through all possible playback speeds. "Frame Advance" move the clock forward to the Next Packet time and continues playing from there.

Underneath the control buttons is the status display. It shows whether the session is playing, stopped, or playing at a high speed.

- Close all of the sub windows, and go back to the Main Window (the one we started with)
- Double click the 'telnet' entry in the Protocols list



Now you see many more telnet Connections. This list is mostly presorted for you in all aspects, save for "End Tm" (note the times 18:07:57, 18:04:37, 18:06:50). In all cases, clicking on the heading will sort the list in ascending order by that key.

- Click the "End Tm" header

Note that the list has now been resorted so that the connections are in the order of ascending "End Tm". In more elaborate situations, this feature is useful if you want to find all of the telnet sessions to or from a particular machine. You simply click on the "Src IP Addr" heading, and scroll through the list until you find the IP Address you're looking for.

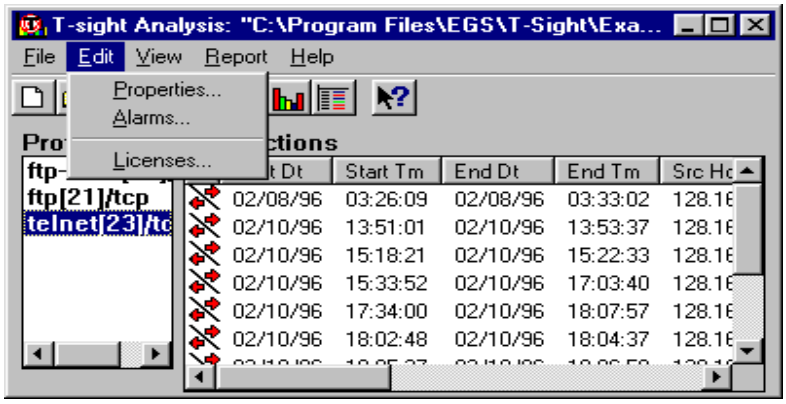
If you are interested in some fields more than others, you can simply grab the column header and drag it to the position you'd like to see it.

- Grab the "Dst IP Addr" and drag it next to the "Src IP Addr" column

Using this technique, you can arrange the columns in any order you prefer.

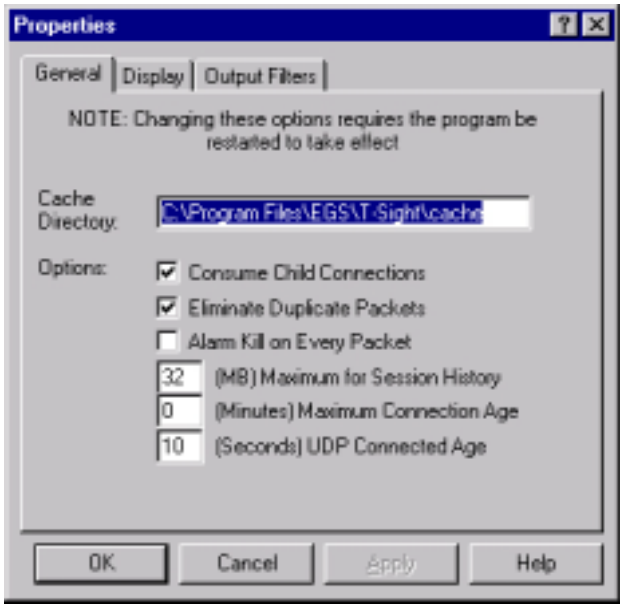
T-Sight PostMortem - Edit Menu

T-Sight configuration options are available under the "Edit" Menu on the main window.



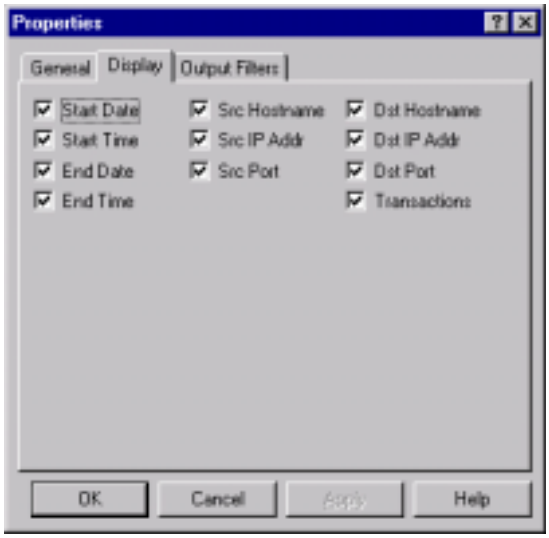
Properties

- Select Edit -> Properties from the menu



This is the General Properties menu. It controls configuration options that affect T-Sight as a whole (both Realtime Monitor and PostMortem Analysis). The Realtime Monitor uses "Cache Directory" to write the TCF files it records. This should have a large amount of disk space, depending on how long you will leave T-Sight Realtime running unattended. Both programs use "Consume Child Connections" to control how the protocol handlers deal with multi-level protocols. For example, a typical FTP connection contains both the FTP control connection (where the client issues RETR, PORT, USER, etc commands) and the FTP-data connection (where the server sends back the requested data to the client). If "Consume Child Connections" is checked, T-Sight will "consume" the child connection (in this case, the FTP-data connection) and report it as part of the parent (in this case, FTP-port 21) connection. With this box unchecked, you would see two protocols (ftp--port 21 and ftp-data--port 20).

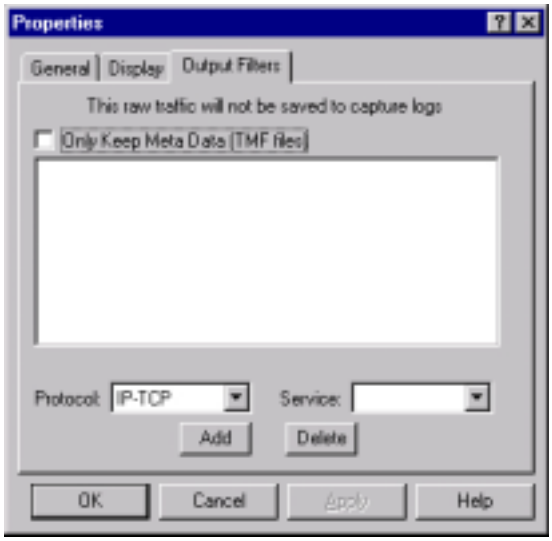
In both cases, you must restart T-Sight to see the changes take effect.



- Click the "Display" tab in the Properties window

These properties control which columns are seen in the "Connections" window.

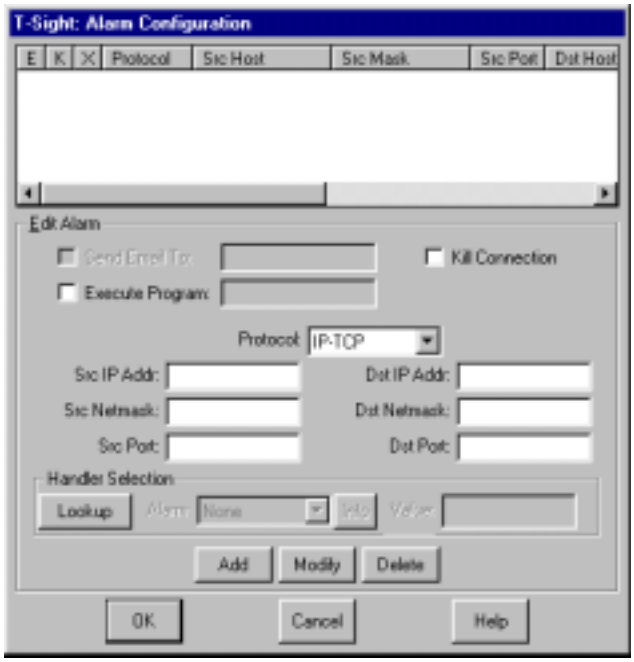
- Click the "Input Filters" tab in the Properties window



These properties control which protocols the Realtime Monitor will save in TCF format. By default, all protocols are logged, but in this particular example, TCP port 25 (or SMTP) will not be logged. If you check the "Only Keep Meta Data" checkbox, then no TCF data will be saved, only the metafile will be output.

Alarms

- Click "Cancel" on the Properties window
- On the main window, select "Edit" -> "Alarms"

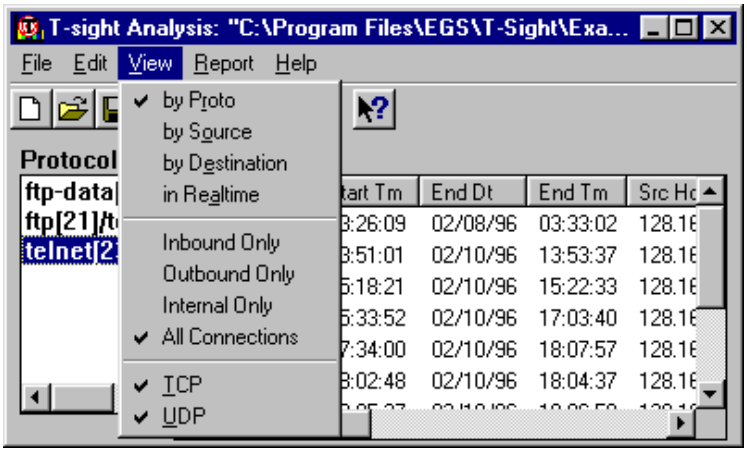


This window manages Alarms. The protocol handlers trigger alarms when an intrusion is detected. As you can see, the responses to an alarm being trigged range from Sending Email to someone, executing another program, to killing the suspected session.

Alarms can be configured to be for specific IP Address ranges, port numbers, or as generic as needed.

T-Sight PostMortem - View Menu

Options for eliminating worthless data from the Protocols and Connections lists are available under the "View" Menu on the main window.



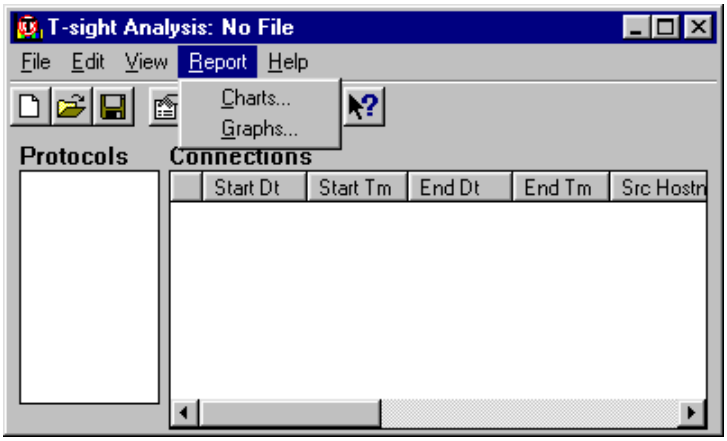
As described in the PostMortem - Main Window section, "by Proto", "by Source", "by Destination", and "in Realtime" control the data that is displayed in the left (major) and right (minor) lists.

"Inbound", "Outbound only", "Both In and Outbound" control whether or not the lists display traffic that is from an external network into the internal network, vice versa, or both.

"TCP", "UDP", and "ICMP" allow the user to turn off individual major protocols he isn't interested in. For example, if he doesn't care about either UDP or ICMP, he can toggle both of those switches off, and they won't be displayed in either the major or the minor list.

T-Sight PostMortem - Report Menu

Graphical Charts and Text Reports are available from the "Report" menu.



The "attack.tcf" file primarily consists of telnet sessions, which aren't terribly interesting to report on. As a result, open another one of the files in the \Example directory

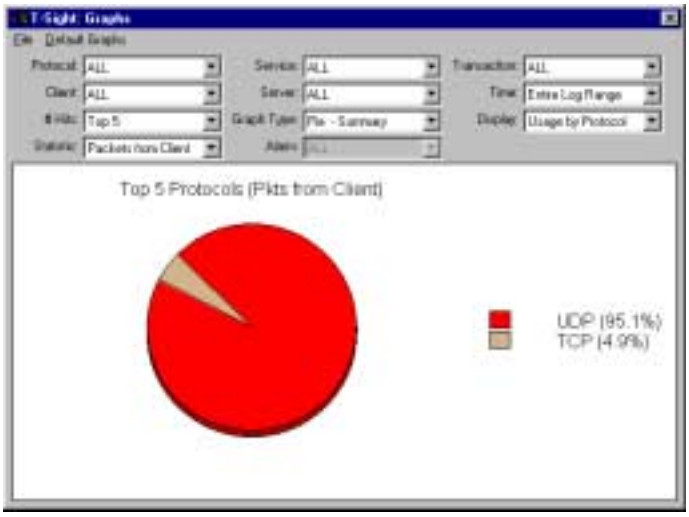
- Select "File" -> "Open" and select the file "multi.tcf" that you downloaded at ftp://ftp.engarde.com/pub/t-sight/multi.tcf.

This message results because Tcpdump defaults to capturing only the first 68 bytes of data from every packet (rather than the whole thing). This won't affect our Reports however (it will make the various "Realtime Playback", "Server Text", etc. look funny, however)

- Click "OK"

Graphs

- Select "Reports" -> "Graphs"

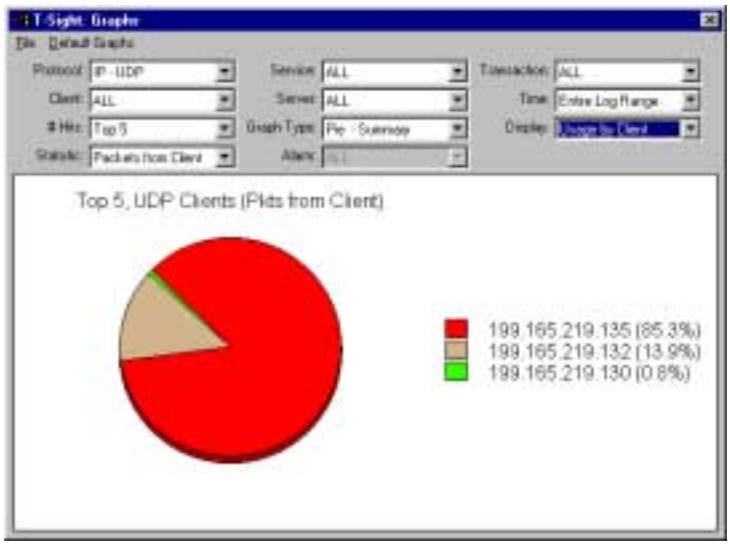


This is the most generic of graphs available. Over the span of the entire log, it shows the percentage usage (in the number of packets sent by every client) by each protocol (TCP/UDP/ICMP). It's easy to manipulate this graph to get other pieces of information.

- Click the "UDP (95.1%)" box

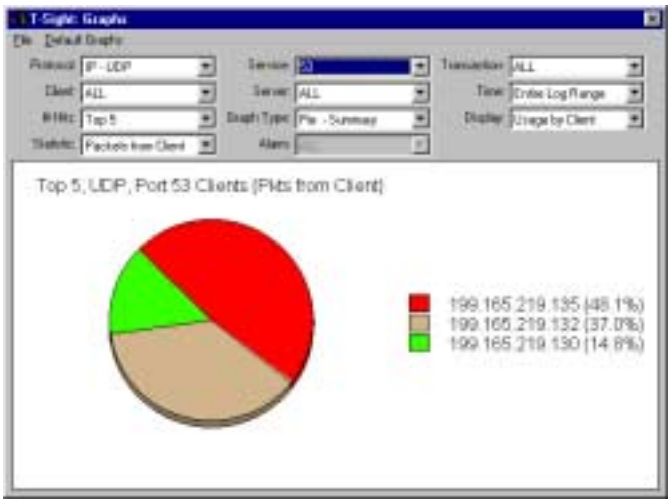
Note that the Protocol window (in the top left) changes to reflect that only UDP is shown. A graph showing percentage usage by protocol for only one protocol isn't terribly useful, so let's change the "Display" combobox.

- Click the "Display" combobox and select "Usage by Client"



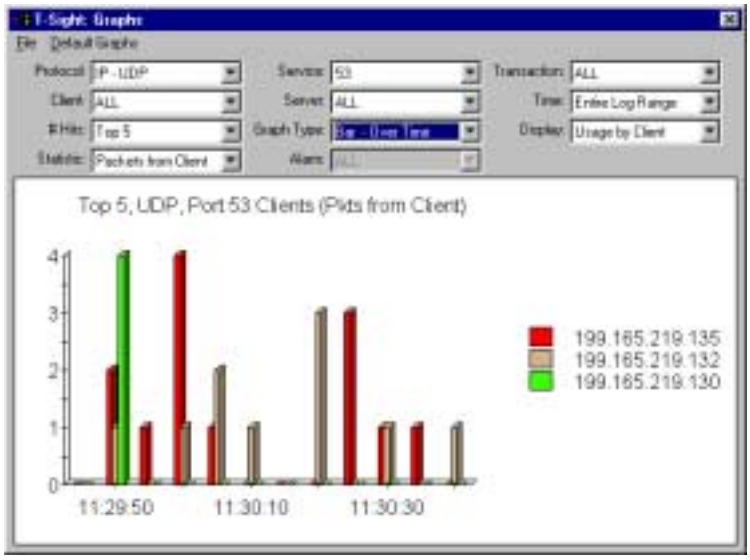
The graph now shows the Top 5 sources of UDP data by IP Address.

- Click the "Service" combobox and select "53" (DNS)



This graph now shows the Top 5, UDP clients making DNS requests (by number of packets sent).

- Click the "Graph Type" combobox and select "Bar - Over Time"

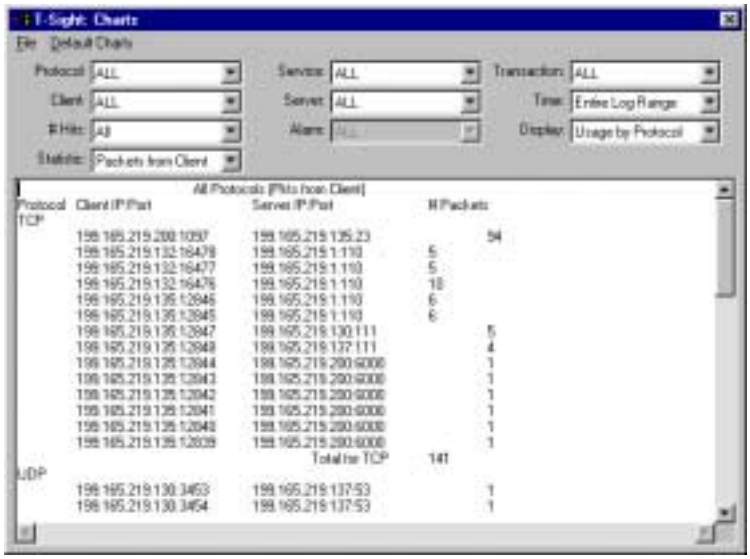


The graph now shows which machines made DNS requests and when.

By manipulating the filter information at the top (or by clicking on individual items in the legend), it's possible to get any graph thinkable.

Charts

- Close the Graph window
- On the Main Window, select "Report" -> "Charts..."



The Chart window works in very similar manner to the Graph window.

Thanks for trying T-sight!

If you have any questions please feel free to contact us!

Contact Information:

En Garde Systems, Inc.
4848 Tramway Ridge Dr. NE Suite 122
Albuquerque, NM 87111

(V) (505) 346-1760
(F) (505) 346-1719

www.engarde.com
info@engarde.com