
Frontline Test System[®]

Ethertest[®]

User's Guide

Table of Contents

INTRODUCTION AND INSTALLATION	6
INTRODUCTION TO FRONTLINE TEST SYSTEM	6
CONTACTING TECHNICAL SUPPORT	6
QUICK START GUIDE.....	7
CONFIGURING THE ETHERNET HARDWARE.....	7
HOW TO CAPTURE DATA.....	7
CIRCUIT STATISTICS	8
LOOKING AT FRAMES.....	8
LOOKING AT DATA BYTES	9
FILTERING	10
EXITING FTS	10
HARDWARE CONFIGURATION.....	11
SELECTING AN ETHERNET CARD.....	11
PROTOCOL STACK WIZARD	12
CREATE A CUSTOM STACK	12
ADDING A NEW PREDEFINED STACK	12
REFRAME FUNCTION	13
UNFRAME FUNCTION	13
CAPTURING DATA	14
CONTROL WINDOW	14
THE CONTROL WINDOW TOOLBAR.....	14
STATUS INFORMATION ON THE CONTROL WINDOW	15
HOW TO CAPTURE DATA TO THE BUFFER	15
HOW TO CAPTURE DATA TO FILE	16
CLEAR CAPTURE BUFFER WARNING	16
NETWORK STATISTICS.....	17
SESSION, RESETABLE AND BUFFER TABS	17
THE INFORMATION IN THE TABLES	17
<i>Statistics Tables</i>	<i>17</i>
<i>Bytes Per Second Table</i>	<i>17</i>
<i>Frames Per Second Table.....</i>	<i>18</i>
<i>Utilization Table</i>	<i>18</i>
<i>Data Table</i>	<i>18</i>
<i>Unfiltered Data Table.....</i>	<i>18</i>
<i>Frame Sizes Table.....</i>	<i>18</i>
<i>Buffer Information Table</i>	<i>19</i>
<i>Errors Table.....</i>	<i>19</i>
STATISTICS GRAPHS	19
<i>Viewing Percentages or Values</i>	<i>20</i>
<i>Graph Options</i>	<i>20</i>
<i>Printing Graphs</i>	<i>20</i>
COPYING STATISTICS TO THE CLIPBOARD	20
OPTIONS	20
<i>Changing Frame Size Ranges.....</i>	<i>20</i>
VIEWING PROTOCOL DECODES.....	22

FRAME DISPLAY WINDOW.....	22
THE FRAME DISPLAY TOOLBAR.....	23
THE PANES IN THE FRAME DISPLAY.....	24
<i>Summary Pane</i>	24
The Summary Layer Toolbar.....	24
Frame Symbols in the Summary Pane.....	25
Customizing Fields in the Summary Pane.....	25
<i>Decode Pane</i>	25
<i>Radix, or Hexadecimal, Pane</i>	26
<i>Character Pane</i>	26
<i>Binary Pane</i>	26
<i>Event Pane</i>	27
WORKING WITH PANES.....	27
SORTING FRAMES.....	27
WORKING WITH MULTIPLE FRAME DISPLAYS.....	28
FILTERS AND MULTIPLE FRAME DISPLAYS.....	28
RED FRAME NUMBERS OR BYTES.....	28
SYNCHRONIZATION BETWEEN THE EVENT AND FRAME DISPLAYS.....	28
PHYSICAL VS. LOGICAL BYTE DISPLAY.....	29
PROTOCOL LAYER COLORS.....	29
<i>What The Color Of Data Bytes Means</i>	29
<i>Changing Protocol Layer Colors</i>	29
ANALYZING BYTE-LEVEL DATA.....	30
EVENT DISPLAY.....	30
THE EVENT DISPLAY TOOLBAR.....	30
OPENING MULTIPLE EVENT DISPLAY WINDOWS.....	31
CALCULATING CRCs OR FCSS.....	31
CALCULATING DELTA TIMES AND DATA RATES.....	32
SWITCHING VIEWING FORMATS.....	32
<i>Switching Between Viewing All Events and Viewing Data Events</i>	32
<i>Switching Between Live Update and Review Mode</i>	32
<i>Switching Between Hex, Decimal, Octal or Binary</i>	33
<i>Switching Between ASCII, EBCDIC and Baudot</i>	33
<i>Viewing Only ASCII (or EBCDIC or Baudot)</i>	33
<i>Viewing Only Hex (Or Decimal or Octal or Binary)</i>	33
<i>Font Size</i>	33
LIST OF ALL EVENT SYMBOLS.....	33
EVENT NUMBERING.....	35
SEARCHING.....	36
SEARCHING FOR FRAME ERRORS.....	36
GO TO.....	36
SEARCHING WITHIN DECODES.....	37
SEARCHING FOR SPECIAL EVENTS.....	37
SEARCH BY PATTERN.....	37
<i>Entering Characters</i>	37
<i>Entering Hex or Binary</i>	37
<i>Entering Control Characters</i>	38
<i>Using Wildcards</i>	38
<i>Examples of Search Strings</i>	38
SEARCHING BY TIME.....	38
<i>Absolute Timestamp Search</i>	38
<i>Relative Timestamp Search</i>	39
<i>Choosing "On or Before" or "On or After"</i>	39
<i>Subtleties of Timestamp Searching</i>	39

CHANGING WHERE THE SEARCH LANDS	39
FILTERING.....	40
HOW TO CREATE AND USE A FILTER.....	40
DIFFERENCE BETWEEN CAPTURE AND DISPLAY FILTERS.....	40
DEFINING FILTERS.....	40
<i>Defining Node and Conversation Filters</i>	40
<i>Defining Protocol Filters</i>	41
<i>Defining Pattern or Offset Filters</i>	41
<i>Using tcpdump to Create a Custom Filter</i>	41
<i>How to Modify a Condition</i>	42
<i>How to Delete a Condition</i>	42
HOW TO APPLY A CAPTURE FILTER.....	42
HOW TO APPLY A DISPLAY FILTER.....	43
HOW TO KNOW WHAT FILTER IS BEING USED.....	43
HOW TO REMOVE A FILTER.....	43
NAMING FILTERS.....	43
SHOWING NAMED FILTERS.....	44
SAVING AND LOADING FILTER FILES.....	44
<i>Saving Filters to File</i>	44
<i>Opening a Filter File</i>	44
FILTER STRING FORMATS.....	44
Berkeley Packet Filtering Man Page.....	46
SAVING DATA TO FILE.....	50
SAVING A PORTION OF A CAPTURE FILE OR BUFFER.....	50
SAVING THE ENTIRE CAPTURE BUFFER.....	50
PRINTING	51
PRINTING FROM THE EVENT DISPLAY.....	51
PRINT PREVIEW.....	51
TROUBLESHOOTING PRINTING PROBLEMS.....	51
EXPORTING	53
EXPORTING AND PRINTING FRAMES.....	53
<i>Frame Export File Format</i>	54
<i>Decode Section</i>	55
Decode Formatting.....	55
<i>Decode Section - Data Display</i>	55
<i>Error Section</i>	55
<i>General Section</i>	55
General Formatting.....	55
<i>Summary Section</i>	55
Summary Formatting.....	56
EXPORTING EVENTS.....	56
<i>Export Fields</i>	56
<i>Export Filter Out</i>	56
<i>Other Export Options</i>	56
<i>Exporting Baudot</i>	57
TEMPLATES.....	58
<i>Export Templates</i>	58
LOADING AND IMPORTING CAPTURE FILES	59
LOADING A CAPTURE FILE.....	59
IMPORTING CAPTURE FILES.....	59
IMPORTING TIMESTAMPS.....	59

SYSTEM SETTINGS AND PROGRAM OPTIONS.....	60
SYSTEM SETTINGS	60
ADVANCED SYSTEM OPTIONS	61
CHANGING DEFAULT FILE LOCATIONS	62
START UP OPTIONS.....	62
MINIMIZING WINDOWS.....	63
TIMESTAMPING OPTIONS	63
<i>Enabling/Disabling Timestamping</i>	63
<i>Switching Between Relative and Absolute Time</i>	63
<i>Changing the Timestamping Resolution</i>	64
<i>Displaying Fractions of a Second</i>	64
TECHNICAL INFORMATION.....	65
PERFORMANCE NOTES.....	65
PERFORMANCE ISSUES FOR HIGH RESOLUTION TIMESTAMPS	66
CLOCK DRIFT	66
PADDING OF SHORT FRAMES	67
CRC!	67
USEFUL TABLES	67
<i>ASCII Codes</i>	67
<i>Baudot Codes</i>	68
<i>EBCDIC Codes</i>	69
<i>Communication Control Characters</i>	69
BPF COPYRIGHT NOTICE.....	70
GLOSSARY	71
BUFFER WRAPPING.....	71
CAPTURE BUFFER.....	71
EVENT	71
FRAME RECOGNIZER	71
FRAME TRANSFORMATION	71
LOGICAL FRAME.....	71
NIC - NETWORK INTERFACE CONTROLLER.....	71
PHYSICAL FRAME	72
RADIX.....	72

Introduction and Installation

Introduction to Frontline Test System

Welcome to the Frontline Test System! Frontline Test System (FTS) is a family of products designed to let you conduct data analysis using your personal computer, of which Ethertest is the Ethernet analysis component. The FTS interface is easy to use without training, but you will want to read the online help to learn how to take maximum advantage of all the features.

Contacting Technical Support

Technical support is available in several ways. The answers to many questions can be found in the online help. Frontline's web site has documentation on common problems, as well as software upgrades and utilities to use with our products.

Web: <http://www.fte.com>, go to the Technical Support Area
Email: tech_support@fte.com
FTP: <ftp.fte.com>

If you need to talk to a technical support representative, support is available between 9am and 5pm, Eastern time, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: (434) 984-4500
Fax: (434) 984-4505

Quick Start Guide

The Quick Start Guide is intended to help you get up and running quickly. As features are discussed, they will often be highlighted in green. Click on the green links to get more information about the feature.

The Quick Start will help you configure your hardware, begin data capture and analyze the data.

FTS is organized around a Control window. From the Control window you have access to the other windows used to view data or perform different functions. In addition, data capture is controlled from the Control window. Each icon on the toolbar represents a window or data capture function. Hold the cursor over each icon, and a tooltip will pop up with the name of each icon. To learn more about what each icon does, read the help topic on the Control Window Toolbar.

The first step is configuring FTS to use the correct Ethernet NIC.

Configuring the Ethernet Hardware






FTS needs to know which NIC to use. Most PCs only have one NIC, so this is not difficult. In order to monitor data, FTS puts the NIC into "promiscuous mode", which tells the NIC to keep every frame on the Ethernet and not just the frames meant for the NIC.

1. You tell FTS which NIC to use in the Hardware Settings window. To open this window, choose *Hardware Settings* from the Options menu on the Control window.
2. In the Use this Network Adapter box, select the adapter to use. Most PCs only have one NIC. If you have had more than one NIC installed on the PC, there may be multiple entries in the list even if there is only one NIC in the machine right now.
3. Click OK.

The next step is learning how to capture data.

How To Capture Data

FTS can capture data to a memory buffer or to a file on disk. Data capture can be initiated from the Control window, the Event Display or the Frame Display, though you do not need any window other than the Control window open to capture data.


1. To capture to the buffer, click the *Start Capture to Buffer* icon .
2. To stop capture and reset the buffer, click the *Clear* icon . Clearing the buffer throws away the data in memory. If you want to save the data in the buffer, Pause capture (see below) and save the buffer before clearing it.
3. To capture to a file, click the *Start Capture to File* icon  and type a filename when prompted.
4. To stop capture and close the file, click the *Close* icon .
5. To pause capture, click the *Pause* icon . Click the Pause icon again to resume capture. Pausing capture means that no data will be added to the capture buffer or file until capture is resumed.
6. To load a capture file, choose *Open* from the File menu on the Control window and select your file. All the functions needed to analyze data will be present, but not the functions needed to capture data. Choose *Go Live* from the File menu on the Control window to return to live mode.

If the buffer becomes full, it will begin to wrap using the First In, First Out rule. ("Buffer" refers to either a memory buffer or a capture file for the purposes of this discussion.) This means that the oldest data will be removed to make room for the newest data. You can tell how full the buffer is by checking the bar graphic next to Capture Status on the status bar of the Control window.

See System Settings for information on how to make the capture buffer larger, or how to turn off buffer wrapping.


Once you've captured some data, you need a way to look at it. FTS provides different ways for viewing different types of data.

Circuit Statistics


Click the Statistics icon  on the Control window toolbar to open the Statistics window.

The Statistics window provides a statistical overview of all the data on the circuit. FTS is always monitoring the circuit and gathering statistics, even when not capturing the data.

There are three tabs on the Statistics window: Session, Resettable and Buffer. The Session tab shows statistics from the time FTS was started. The Resettable tab can be reset to show statistics from the time the Reset icon was last pressed. The Buffer tab shows statistics on the data in the capture buffer. If data capture has not been started or if the buffer has wrapped, most of the statistics on the Buffer tab will be n/a.

Some tables on the Statistics window can display data in graphic form. Click the Graph icon  on any header that has one for a chart of that table.


Looking At Frames


Click the Frame Display icon  on the Control window toolbar to open the Frame Display. The Frame Display window is the main view of frame-level data.


The Frame Display is divided up into "panes", where each pane shows a different type of data. The Summary pane stretches across the top of the display and shows a protocol summary of each frame. The Decode pane has a detailed decode of the frame selected in the Summary pane and is the long pane on the left side. The three smaller panes on the bottom right of the Frame Display show the logical data in hex, binary and ASCII. Select any field in the decode and the corresponding bit(s) or byte(s) will be selected in these three panes.

The green dot next to each frame in the Summary pane means the frame contains the decode listed in the drop-down box at the top of the Summary pane. No dot or a green circle indicates other conditions. The protocol being viewed is listed in the drop-down box at the top of the Summary pane. Click on the arrow to change the protocol.

Frame numbers in red indicate an error in the frame. Select the frame, and look at the top of the Decode pane to determine the source of the error.


Use the Find feature to search for a pattern in the decode or errors in the frames. Click the Find icon  to open the Find window. In the Decode tab, type the pattern you want to look for and click Find Next, or select one of the two radio buttons to search for errors. See the Decode Search topic for more information.

The Duplicate icon  creates a second Frame Display, identical to the first. The advantage of additional Frame Displays is that you can look at two different frames at the same time.


By default, the Frame Display is frozen, which means that it does not automatically update as new data is captured. Click the Freeze/Resume icon  to have the Frame Display Summary pane automatically update as new data is captured.

The Frame Display and the Event Display are synchronized. Select a frame in the Frame Display and the Event Display will automatically update to highlight the bytes in the frame. Select a byte in the Event Display and the Frame Display will update to show the frame containing the byte.

Looking At Data Bytes

Click the Event Display icon  on the Control window toolbar to open the Event Display. The Event Display window is the main view of byte-level data.

By default, the Event Display updates automatically as new data is captured. This lets you see all new data as it comes in, and check that good data is on the circuit and being captured properly by FTS.

To stop the Event Display from updating, click the Freeze icon . Click the Freeze icon again to resume live updates.

Data is displayed in hex on the left and ASCII on the right. The Event Display can also display data in decimal, binary, EBCDIC, or Baudot. Choose the format you would like from the Data menu, or right-click on the Hex/ASCII labels in the headers and select a different format.


Click on a byte in the display. The three status lines at the bottom of the window will update to show a variety of information about the byte, including its value in different radices and any errors associated with the byte. Use the mouse to select several bytes. The status lines change to show the data rate over the range of the selection, the delta time between the first and the last bytes in the selection, and the CRC. To change the algorithm used to calculate the CRC, click

the CRC icon .

Bytes with errors are shown in red. Click on the byte to see what the error is.


FTS displays data other than bytes in the Event Display. For example, flags are used as start-of-frame and end-of-frame markers. These special symbols in conjunction with the data bytes are called events.

Use the Find feature to search for a pattern in the data, a pattern in the decode, or framing errors. Click the Find icon to open the Find window. In the Pattern tab, type the pattern you want to look for and click Find Next. See the Search topic for more information on the different types of searches.

The Duplicate icon  creates a second Event Display, identical to the first. The advantage of additional Event Displays is that you can look at two different groups of data at the same time. For example, you can look at the start of an interaction in one Event Display, and the end of that same interaction in the other and compare the two.

The Event Display and the Frame Display are synchronized. Select a byte in the Event Display and the Frame Display will update to show the frame containing the byte. Select a frame in the Frame Display and the Event Display will automatically update to highlight the bytes in the frame.

Filtering

Click the Filters icon  on the Control window toolbar to open the Filters window.

This overview will describe how to make a simple node or protocol display filter. Creating other types of filters or creating a capture filter follow many of the same procedures. See Filters for more information on the types of filters and how to use them.

There are two basic types of filters. Capture filters look at data as it is being captured, and either keep it or throw it away based on the filter criteria. Display filters look at the data currently in the capture buffer, and either displays it or not depending on the filter criteria.

Exiting FTS

To exit FTS, go to the File menu on the Control window, and choose *Exit FTS*, or close the Control window using the X icon in the top right corner of the title bar.

Hardware Configuration

Selecting An Ethernet Card


The first time FTS is started, the Hardware Settings window will appear. Choose which Ethernet card FTS should use, and click OK.

If you need to change your Ethernet card in the future, choose *Hardware Settings* from the *Options* menu on the Control window, or go to the Start button and choose Programs -> Ethertest -> Ethertest Setup.

FTS checks the registry for Ethernet card entries and puts these in the drop-down list. On some PCs, the Ethernet Controller may be listed, or the Dial-Up Adapter. Be sure to choose the name of the NIC that is connected to the network.

The Ethernet card must use an NDIS driver.

Protocol Stack Wizard

The Protocol Stack wizard is where you define the protocol stack you want FTS to use when decoding frames. To start the wizard, choose *Protocol Stack* from the Options menu on the Control window or click the Protocol Stack  icon on the Frame Display.

Select a protocol stack from the list, and click *Finish*.

Most stacks are pre-defined here. If you have special requirements and need to set up a custom stack, choose *Build Your Own* from the top of the list, and click *Next*.

If you have selected a custom stack (i.e. one that was defined by a user and not included with FTS), the *Remove Selected Item From List* button will become active. Click the *Remove* button to remove the stack from the list. You cannot remove stacks provided with FTS. If you remove a custom stack, you will need to define it again in order to get it back.

Note that if you are changing the protocol stack for a capture file, you may need to reframe. See Reframing for more information.

Create a Custom Stack

There are two steps to creating a stack: defining the protocols in the stack and choosing whether to have FTS automatically determine higher layer protocols (called auto-traversal). There is a third optional step of saving the stack so that it appears in the Protocol Stack List on the first screen of the Protocol Stack Wizard. Defining a custom stack means that FTS will use the stack for every frame. Frames that do not conform to the stack will be decoded incorrectly.

1. Select Protocols

Select a protocol from the list on the left. Click the right arrow button to move it to the Protocol Decode Stack box on the right, or double-click the protocol to move it to the right. To remove a protocol from the stack, double-click it or select it and click the left arrow button.

If you need to change the order of the protocols in the stack, select the protocol you want to move, and click on the Move Up and Move Down buttons until the protocol is in the correct position. The lowest layer protocol is at the top of the list, with higher layer protocols listed underneath.

2. Auto-traversal (Have FTS Determine Higher Layers)

If you need to define just a few layers of the protocol stack, and the remaining layers can be determined based on the lower layers, click the All additional stack layers can be determined automatically button. If your protocol stack is complete and there are no additional layers, click the There are no additional stack layers button. If you select this option, FTS will use the stack you defined for every frame. Frames that do use this stack will be decoded incorrectly.

3. Save the Stack

To save your stack click the *Add To Predefined List* button, give the stack a name, and click *Add*. In the future, the stack will appear in the Protocol Stack List on the first screen of the Protocol Stack wizard. To remove the stack, select it in the first screen and click *Remove Selected Item From List*.

Adding a New Predefined Stack

From the Control window Options menu, choose *Protocol Stack*. Choose *Build Your Own* from the list, and click *Next*. Define your protocol stack, and click the *Add to Predefined List* button.

Give the stack a name, and click *Add*. In the future, the stack will appear with the system provided stacks in the Protocol Stack List on the first screen of the wizard.

To remove a custom stack, open the Protocol Stack window, select the stack from the list, and click *Remove Selected Item From List*. If you remove the stack, you will need to recreate it if you need to use it again.

Reframe Function

If you need to change the protocol stack used to interpret a capture file and the framing is different in the new stack, you will need to reframe in order for the protocol decode to be correct. You can also use the *Reframe* function to frame unframed data. The original capture file is not altered during this process.

1. Load your capture file. To do this, choose *Open* from the File menu on the Control window, and select the file to load.
2. Select the protocol stack. To do this, choose *Protocol Stack* from the Options menu on the Control window, select the desired stack and click *Finish*.
3. If you selected a protocol stack that includes a frame recognizer different from the one used to capture your data, the Protocol Stack Wizard will ask you if you want to reframe your data. Choose *Yes*.
4. FTS will add frame markers to your data, put the framed data into a new file, and open the new file. The original capture file will not be altered.

To manually reframe your data, load your capture file, select a protocol stack, and then select *Reframe* from the File menu on the Control window. *Reframe* will only be available if the frame recognizer used to capture the data is different from the current frame recognizer.

See Unframe Function for instructions on removing framing from data.

Unframe Function

This function will remove start-of-frame and end-of-frame markers from your data. The original capture file is not altered during this process.

1. Load your capture file. To do this, choose *Open* from the File menu on the Control window, and select the file to load.
2. Remove the protocol stack. To do this, choose *Protocol Stack* from the Options menu on the Control window, select *None* from the list, and click *Finish*.
3. The Protocol Stack Wizard will ask you if you want to reframe your data and put it into a new file. Choose *Yes*.
4. FTS will remove the frame markers from your data, put the unframed data into a new file, and open the new file. The original capture file will not be altered.


To manually unframe your data, select *Unframe* from the File menu on the Control window. *Unframe* will only be available if a protocol stack was used to capture the data and there is currently no protocol stack selected.

See Reframe Function for instructions on framing unframed data.

Capturing Data

Control Window

Information in FTS is displayed in multiple windows, with each window showing a different type of information. The Control window is used to provide access to each window as well as give a brief overview of the data in the capture file. Each icon on the toolbar represents a different data analysis function.

Because the Control window can get lost behind other windows, every window has a *Home* icon  that brings the Control window back to the front. Just click on the *Home* icon to restore the Control window.

The title bar of the Control window shows what hardware FTS is using. The status bars (below the toolbar) show the state of the analyzer (Not Active, Paused, Running, etc.), how full the capture buffer or file is, and current utilization.

FTS continuously monitors the circuit and gathers statistics on the data on the circuit, even when not actively capturing the data. This means that if there is data on the circuit, the utilization counters will be active, even if not capturing data.

The Control Window Toolbar

Available options will be in color, while unavailable options will be grayed out. All toolbar buttons have corresponding menu items, most of which can be found in the *Window* menu. The exceptions are *Capture to Buffer*, *Capture to Disk*, *Pause/Resume*, *Clear*, and *Close Capture File*, which are found in the *Live* menu.



Capture to Buffer - Begins data capture to the buffer only.



Capture to Disk - Begins data capture to disk.



Pause/Resume - Available after data capture has started. Click once to pause data capture. Data can be reviewed and saved, but no new data will be captured. Click this button again to Resume capture.



Clear Buffer - Stops data capture to buffer and clears the capture buffer.



Close Capture File - Closes a capture file and stops data capture to disk.



Statistics are kept on the entire session (the time since FTS was started) and for each set of events in the capture buffer or file.



Event Display - Shows events as they are being captured.



Frame Display - Shows summary information and a detailed decode for each data frame.



Filters - Define and apply capture and display filters. Capture filters filter out data while it is being captured, putting only data that matches the filter in the capture buffer. Display filters filter out data in the capture buffer. All data is captured, but only the data matching the filter is displayed in the Frame Display window. Filtering can only be done with framed data.



Transmit - Lets you specify what data to transmit. *This feature not yet available.*



Cascade Windows - Cascades all windows (brings them home), with the first window being placed directly below the Control window.

Status Information on the Control Window








The top status bar shows the hardware Configuration. It gives you the name of the network card being used by FTS and its MAC Address. If FTS cannot find the MAC Address, it lists zeroes after the NIC name.

The bottom status bar of the Control window gives a quick look at what is currently going on. *Capture Status* displays the words *Not Active*, *Paused* or *Running* and refers to the state of data capture. *Not Active* means that FTS is not currently capturing data, *Paused* means that data capture has been suspended, and *Running* means that FTS is actively capturing data.

The next item shows how much of the buffer or capture file has been filled. For example, if you are capturing to disk and have specified a 200K capture file, the bar graph will tell you how much of the capture file has been used. When the graph reaches 100%, capture will either stop or the file will be overwritten, depending on the choices you made in the System Settings. If you are capturing to the buffer, you will know that the buffer has wrapped when the graph reaches 100%. This item displays *N/A used* when data capture is not active.

The second half of the status bar gives the current utilization and total number of events seen on the network. Note that this number is the total number of events monitored, not the total number of events captured. FTS is always monitoring the circuit, even when data is not actively being captured. These graphs allow you to keep an eye on what is happening on the circuit, without requiring you to capture data.








How To Capture Data To The Buffer

1. Click the *Capture to Buffer* icon  to begin capturing to buffer. This icon is located on the Control , Event Display , Frame Display  and Transmit  windows.
2. Watch the status bar on the Control window to find out how full the buffer is. When the buffer is full, it will begin to wrap, throwing out the oldest data to make room for the new.
3. Click the *Pause* icon  to temporarily stop data capture. Click the *Pause* icon again to resume capture.
4. Click the *Clear Capture Buffer* icon  to stop capture.
5. FTS will ask if you want to save your data first. If you do, click *Save First*. FTS will prompt you for a file name. If you don't want to see this prompt again, click the *Don't Show This Warning Again* box. FTS will not show the warning again during this session of FTS. FTS does not remember the state of the warning from session to session as a precaution. You will need to check the box again the next time FTS is started.

To change the size of the capture buffer, choose System Settings from the *Options* menu on the Control window.

To prevent the buffer from wrapping, go to the System Settings.

How To Capture Data To File

1. Click the *Capture to Disk* icon  to begin capturing to a file on disk. This icon is located on the Control , Event Display , Frame Display  and Transmit  windows.
2. Choose a name for your capture file. Files are placed in My Capture Files by default and have a .cfa extension. Choose Directories from the *Options* menu on the Control window to change the default file location.
3. Watch the status bar on the Control window to find out how full the file is. When the file is full, it will begin to wrap, throwing out the oldest data to make room for the new.
4. Click the *Pause* icon  to temporarily stop data capture. Click the *Pause* icon again to resume capture.
5. Click the *Close Capture File* icon  to stop capture and close the file.

To change the size of the capture file, choose System Settings from the *Options* menu on the Control window.

Clear Capture Buffer Warning

If you clear the capture buffer and haven't saved it, FTS asks you if you want to save the buffer before clearing. The three options are:


Save First - asks you for a file name, saves the buffer and then clears it.

Clear Buffer - clears the buffer without saving it.


Cancel - returns to FTS without clearing the buffer.

If you don't want to see the warning again, check the "*Don't show this warning again when clearing buffer*" box. The option is remembered only for the current FTS session. If you exit FTS, you will need to check the box again the next time you run FTS.

Network Statistics

To open the Statistics window, click the Statistics icon  on the Control window toolbar, or choose Statistics from the Window menu on the Control window.

The Statistics window supplies basic information about the data on the network. When reviewing a capture file, the Statistics window shows a summary of the data in the file.

FTS monitors the network and collects statistics all the time, even when data is not actively being captured. Click the Freeze icon  to stop the window from updating. Click the Freeze icon again to resume updating. FTS will continue to monitor network traffic while the Statistics window is frozen, so you may see the numbers jump right after updating has resumed, reflecting all the statistics that were gathered while the window was frozen.

Session, Resetable and Buffer Tabs

Information about all data collected since FTS was started is shown in the Session tab. The Session tab cannot be reset; in this sense, it is like the odometer on a car. The odometer on a car shows you all the miles driven since the car was built, and the Session tab shows you all the data collected since FTS was started.

If you think of the Session tab as the odometer, then the Resetable tab is the trip odometer. It can be reset, and allows you to record statistics for a new "trip." In this way you can effectively start a new session without having to restart FTS.

The Buffer tab shows information on the data that is currently in the capture buffer. The tab will reset when you clear the buffer. If the capture buffer becomes full, FTS will begin to throw out the oldest data and put new data in its place. This is called "wrapping." If the buffer wraps, the count for the total number of events will remain roughly the same, since the buffer will remain full until it is cleared and therefore always contains approximately the same number of events.

Occasionally some of the statistics will read n/a, for Not Available. This happens for various reasons. For example, many of the items on the Buffer tab will become n/a if the buffer should become full and wrap. When this happens, FTS can no longer provide accurate statistics for the data in the buffer, because some of the data that the statistics are based on has been lost.

The Information in the Tables

STATISTICS TABLES

The information on the Statistics window is organized into tables. Fields marked "n/a" are fields for which there is currently no data. This can happen for a variety of reasons. On the buffer tab, fields are n/a when there is no data in the buffer (i.e. no capturing is being done). On the Errors table, some fields may be n/a depending on the statistics supported by your Ethernet card.

BYTES PER SECOND TABLE

Speed	maximum speed of the network expressed in megabits
Current	current number of bytes per second.
Average	average number of bytes per second.
Peak	highest number of bytes per second.

FRAMES PER SECOND TABLE

Current	current number of frames per second.
Average	average number of frames per second.
Peak	highest number of frames per second.

UTILIZATION TABLE

Current	current number of bits per second divided by the maximum speed of the network, expressed as a percentage.
Average	average number of bits per second divided by the maximum speed of the network, expressed as a percentage.
Peak	highest utilization.

DATA TABLE

The information in the Data table relates to the amount of data captured by FTS. If a capture filter is active, this table will show statistics only for the data kept by FTS, i.e. only the data that passes the filter. The Unfiltered Data table will always show statistics for the entire network, regardless of whether a capture filter is active.

Frames	total number of frames captured by FTS. This includes frames received with and without errors, and frames transmitted by the PC running FTS, if the PC is an active node on the network. This field and the Total Frames field in the Unfiltered Data table should be roughly equal, unless a capture filter is active. They will not be exactly equal because the counters are updated at different times.
Bytes	total number of bytes.
Events	total number of events captured. Events include data bytes and start-of-frame and end-of-frame markers. For a description of all events and their symbols, see the List of Event Symbols.
Multicast	total number of multicast frames.
Broadcast	total number of broadcast frames.

UNFILTERED DATA TABLE

The information in the Unfiltered Data table is recorded by NDIS. Some NDIS drivers may not report all of the statistics on this table, in which case the field will be listed as n/a. This table will always reflect the total amount of data on the network.

Rx Frames W/O Errors	total number of frames received with no errors.
Tx Frames W/O Errors	total number of frames transmitted by the NIC with no errors.
Total Frames	total number of frames, including frames with errors. This field and the Frames field on the Data table should be roughly equal, unless a capture filter is active. They will not be exactly equal because the counters are updated at different times.
Bytes	total number of bytes.
Multicast Frames	total number of multicast frames.
Broadcast Frames	total number of broadcast frames.

FRAME SIZES TABLE

To graph, click the bar graph icon  on the Frame Sizes table header.

Displays the number of frames in each size range, and the average frame size at the bottom. To change the ranges used, go to the Options menu and choose Set Frame Size Ranges.

BUFFER INFORMATION TABLE

These errors do not indicate problems on the network, but rather indicate that FTS is not able to keep up with the amount of incoming data. They usually indicate that a faster PC is needed, or capture filters need to be used to decrease the amount of data being captured. See Performance Notes for more information.

Driver Buffer Overflow	number of times FTS lost frames because it could not retrieve them from the driver buffer fast enough.
Frames Missed, No Buffer	number of frames lost because the FTS driver could not retrieve them from the NDIS buffers before they were overwritten by new, incoming frames.
Receive Overrun	number of times that frames are lost because NDIS could not retrieve data quickly enough from the buffer on the network card
Frames Lost	number of frames lost due to driver buffer overflows.

ERRORS TABLE



The Errors table gives the number of each type of error seen on the network. Not all errors are supported by all NDIS drivers. Errors not supported are marked "n/a".

To graph, click the bar graph icon  on the Errors table header.



CRC Errors	number of frames with CRC errors. A CRC error occurs when the frame is properly aligned on a byte boundary but does not pass the Cyclic Redundancy Check. The CRC verifies that the data was not corrupted in transit.
Alignment Errors	number of frames with alignment errors. Alignment errors occur when the frame does not end on a byte boundary. For example, frames may not be 95 and 2 bits long. It must be either 92 or 93 bytes.
Rx Frames With Errors	total number of frames received with errors (includes frames with CRC and Alignment errors)
Tx Frames With Errors	total number of frames transmitted with errors
Tx One Collision	number of frames successfully transmitted after detecting one collision
Tx More Collisions	number of frames successfully transmitted after detecting multiple collisions
Tx Deferred	number of frames successfully transmitted after transmission has been deferred at least once
Tx Max Collisions	number of frames not transmitted due to excessive collisions
Tx Underrun	number of frames not transmitted due to underrun errors
Tx Heartbeat Failure	number of frames transmitted without detecting the collision detection heartbeat
Tx Times CRS Lost	number of times carrier sense was lost during frame transmission
Tx Late Collisions	number of collisions detected after the normal window


Statistics Graphs

To open any graph window



Click on the picture of a graph  on the table header, or choose the graph name from the Graph menu on the Statistics window. To open the Statistics window, click the Statistics  icon on the Control window toolbar.

The Frame Sizes Graph window has Session, Resetable and Buffer tabs that correspond to the tabs on the Statistics window. Each tab shows the data that corresponds to the appropriate tab on the Statistics window.

The Frame Sizes Graph window displays the number of frames of each length in either a pie chart or bar graph format. Click the *Pie* icon  to display a pie chart, and click the *Bar* icon  to display a bar graph.



For networks with more than one side, FTS will display one graph for each side. To view the aggregate of all sides, click the *Aggregate* icon .

VIEWING PERCENTAGES OR VALUES

- Click the Percentages icon  to view data expressed as a percentage. This will make the icon appear pressed down.
- Click the Percentages icon again to view the actual number of items of each type.
- Click the Show Data Grid icon  to view both the number and percentage of the total for each item. FTS will place a grid in the legend.


GRAPH OPTIONS

To open this window

Click the *Statistics* icon  on the Control window. On the Statistics window, click the *Options* icon .

The graphs window refreshes once every second. To change the refresh rate, enter a new refresh rate in milliseconds in the *Window Refresh Rate* box.

PRINTING GRAPHS

Click the *Print* icon  to print the graph. FTS will print exactly what's shown on the window.


Copying Statistics To The Clipboard

To copy the information from an individual table to the clipboard (where it can be pasted into any application), choose the name of the table from the *Edit* menu. To copy the contents of all the tables, choose *Copy All to Clipboard*.

Options

CHANGING FRAME SIZE RANGES

FTS tracks the length of each frame it receives in the Frame Sizes table on the Statistics window. You can change both the minimum and maximum values for each range and the total number of ranges.

To change the frame size ranges, click the Statistics icon  on the Control window toolbar, and choose *Set Frame Size Ranges* from the *Options* menu.

In the Frame Size Range window, click to place the cursor in the High column and enter a new value. FTS will automatically adjust the Low values. To add a new range, place the cursor in the empty last cell in the High column and type in a new value.

If you want to know how many frames are of an exact size, make both the low and high value equal to the size. For example, if you want to know how many 64 byte frames there are on your Ethernet, make the High value 64, and the previous High value end at 63. This will have the effect of creating a row labeled 64-64, and it will count the number of frames that are exactly 64 bytes in length.

You can also type a description of each range (for example, "short" for frames that are too short or "error" for frames that are too large). Place the cursor in the Description column and type in a description. The Preview column shows what the range label on the Frame Sizes table in the Statistics window will look like.


Click OK when you are finished. FTS will remember the new ranges from session to session.

To reset to the default ranges, click *Reset*.

Viewing Protocol Decodes

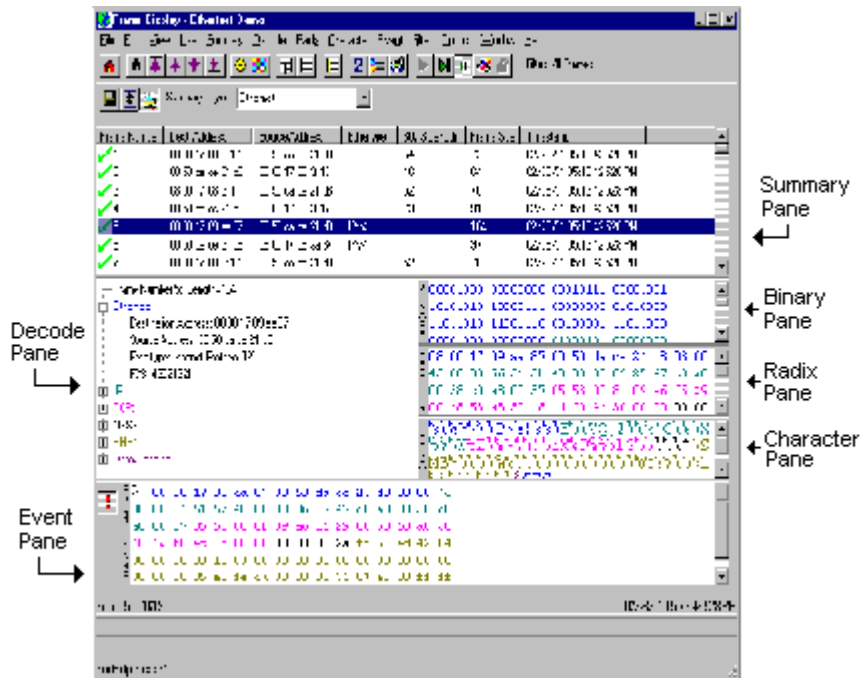
Frame Display Window

To open this window

Click the Frame Display icon  on the Control window toolbar, or select *Frame Display* from the *Window* menu.

Frame Display Panes

The Frame Display window is used to view all frame related information. It is composed of a number of different sections or "panes", where each pane shows a different type of information about a frame. The image below gives the name of each pane. Click on the links below the image to learn more about each pane.



Summary - a one line summary of each frame. Can display a summary for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of arrow and X symbols next to the frame numbers.

Decode - detailed decode of the highlighted frame. Fields selected in the Decode pane have the appropriate bit(s) or byte(s) selected in the Radix, Binary, Character and Event panes.

Radix - logical data bytes in the frame displayed in either hexadecimal, decimal or octal.


Binary - binary representation of the logical data bytes.

Character - character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.

Event - physical data bytes in the frame, as received on the network.

By default, all panes but the Event pane are shown when the Frame Display is first opened.

Comparing Frames

If you need to compare frames, you can open additional Frame Display windows by clicking on the *Duplicate View* icon . You can have as many Frame Display windows open at a time as you wish.

The Frame Display Toolbar



Show Control Window - brings the Control window to the front



Find - search for frame errors or string patterns in the decode



First Frame - moves to the first frame in the buffer



Previous Frame - moves to the previous frame in the buffer



Next Frame - move to the next frame in the buffer



Last Frame - moves to the last frame in the buffer

Note that if the frames are sorted in other than ascending frame number order, the order of the frames in the buffer will be the sorted order. Therefore the last frame in the buffer may not have the last frame number.



Set Timestamp Format - change the format of the timestamps



Select Colors - set the colors used to indicate different protocol layers

The following 5 icons all change how the panes are arranged on the Frame Display.



Reset Pane Positions - returns the panes to their default settings



Show All Panes - display all six panes



Show Minimal Panes - displays the Summary, Decode, Radix and Character panes



Show Summary Only - displays only the Summary pane



Expand Decode Pane - makes the Decode pane taller and the Summary pane narrower



Duplicate View - create a second Frame Display window identical to the first



Define Filter - define a filter



Undo Filter - remove the currently active filter. The active filter is displayed on the far right of the Frame Display toolbar.



Focus Event View - brings up the Event Display window, with the bytes of the currently selected frame highlighted.

Filter Text giving the filter currently in use. If no filter is being used, the text reads "All Frames" which means that nothing is filtered out. To see the text of the entire filter, place the cursor over the text and a tooltip will pop up with the full text of the filter.

The Panes in the Frame Display




SUMMARY PANE

The Summary pane displays a one-line summary of every frame in a capture buffer or file, including frame number, timestamp, length and basic protocol information. The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar). Frames which do not carry the selected protocol are marked by a blue X on the far left next to the frame number.

On a two-channel circuit, the background color of the one-line summary indicates whether the frame came from the DTE or the DCE device. Frames with a white background come from the DTE device, frames with a gray background come from the DCE device.

Frame numbers in red indicate errors, either physical (byte-level) or frame errors. If the error is a frame error in the displayed protocol layer, the bytes where the error occurred will also be displayed in red. The Decode pane will give precise information as to the type of error and where it occurred.

The Summary pane is synchronized with the other panes in this window. Click on a frame in the Summary pane, and the bytes for that frame will be highlighted in the Event pane while the Decode pane will display the full decode for that frame. Any other panes which are being viewed will update accordingly. If you use one pane to select a subset of the frame, then only that subset of the frame will be highlighted in the other panes.

Use the navigation icons, keyboard or mouse to move through the frames. The icons  and  will move you to the first and last frames in the buffer, respectively. Use the Go To icon  to move to a specific frame number.

The Summary Layer Toolbar



Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data



Save - save the currently selected frames or the entire buffer



Go To - opens the Go To dialog, where you can specify which frame number to go to



Show Only Data - changes the summary layer being displayed to Data, which displays just the data in the frame (also called the payload)

Summary Layer drop-down box

Lists all the protocols found in the data in the file. This box does not list all the protocol decoders available to FTS, merely the protocols found in the data. Selecting a protocol from the list changes the Summary pane to display summary information for that protocol.

Text with Protocol Stack

To the right of the Summary Layer box is some text giving the protocol stack currently in use.

Frame Symbols in the Summary Pane

- One green dot means the frame was decoded successfully, and the protocol listed in the Summary Layer drop-down box exists in the frame.
No dot means the frame was decoded successfully, but the protocol listed in the Summary Layer drop-down box does not exist in the frame.
- A green circle means the frame was not fully decoded. There are several reasons why this might happen.

One reason is that the frame compiler hasn't caught up to that frame yet. It takes some time for FTS to compile and decode frames. Frame compilation also has a lower priority than other tasks, such as capturing data. If FTS is busy capturing data, frame compilation may fall behind. When FTS catches up, the green circle will change to either a green dot or no dot.

Another reason is if some data in the frame is context dependent and we don't have the context. An example is a compressed header where the first frame gives the complete header, and subsequent frames just give information on what has changed. If FTS does not capture the first frame with the complete header, it cannot decode subsequent frames with partial header information.

Customizing Fields in the Summary Pane

Changing Column Widths

To change the width of a column, place the cursor over the right column divider until the cursor changes to a solid double arrow. Then click and drag the divider to the desired width.

To auto-size the columns, double-click on the column dividers.

Hiding Columns

To hide a column, drag the right divider of the column all the way to the left. The cursor will change to a split double arrow when a hidden column is present. To show the hidden column, place the cursor over the divider until it changes to a split double arrow, then click and drag the cursor to the right.

The Frame Size and Timestamp columns can be removed entirely by right-clicking on the header and selecting Show Frame Size or Show Timestamp Column. Follow the same procedure to display the columns again.

Moving Columns - Changing Column Order

To move a column, click on the column header and drag the mouse over the header row. A small white triangle indicates where the column will be moved to. When the triangle is in the desired location, release the mouse.

Restoring Default Column Settings

To restore columns to their default locations and show any hidden columns, right-click on any column header and choose *Restore Default Columns*, or select *Restore Default Columns* from the *Summary* menu.


DECODE PANE

The Decode pane is a post-process display that provides a detailed decode of each frame. The decode is presented in a layered format that can be expanded and collapsed depending on which layer(s) you are most interested in. Click on the plus sign to expand a layer. The plus sign will change to a minus sign. Click on the minus sign to collapse a layer. Select Expand Tree or

Collapse Tree from the Decode menu to expand or collapse all the layers. Layers will retain their expanded or collapsed state between frames.

Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the Event, Radix, Binary and Character Panes. The colors are not assigned to a protocol, but are assigned to the layer.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes will highlight the corresponding element in all the other panes.

Click the *Expand Decode Pane* icon  to make the Decode pane taller. This allows for more of a lengthy decode to be viewed without needing to scroll.

RADIX, OR HEXADECIMAL, PANE

The Radix pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the Radix menu, or by right-clicking on the pane and choosing Hexadecimal, Decimal or Octal.

Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes will highlight the corresponding element in all the other panes.

CHARACTER PANE

The Character pane represents the logical bytes in the frame in ASCII, EBCDIC or Baudot. The character set can be changed from the Character menu, or by right-clicking on the pane and choosing the appropriate character set.

Because the Character pane displays the logical bytes rather than the physical bytes, the data in the Character pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes will highlight the corresponding element in all the other panes.

BINARY PANE


The Binary pane displays the logical bytes in the frame in binary. This pane is synchronized with the Decode pane so that individual bit fields can be highlighted.

Because the Binary pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes will highlight the corresponding element in all the other panes.

EVENT PANE

The Event pane shows the physical bytes in the frame. You can choose between displaying only the data events or displaying all events by clicking the *All Events* icon . Displaying all events means that special events, such as Start of Frame/End of Frame and any signal change events, will be displayed as special symbols within the data.

The status lines at the bottom of the pane give the same information as the status lines in the Event Display window. This includes physical data errors, control signal changes (if appropriate), and timestamps.




Because the Event pane displays the physical bytes rather than the logical bytes, the data in the Event pane may be different from that in the Radix, Binary and Character panes. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes will highlight the corresponding element in all the other panes.

Working With Panes

By default, all panes but the Event pane are displayed when the window is first opened.

- To view all the panes, click the *Show All Panes* icon  on the toolbar, or go to the *View* menu and choose *Show [Pane Name]*.
- The *Expand Decode Pane* icon  will make the decode pane longer in order to better view lengthy decodes.
- The *Reset Panes* icon  will return the window to its default setting.
- To close a pane, right-click on the pane and unselect the *Show [Pane Name]* option, or unselect the pane from the *View* menu.
- To open a pane, select *Show [Pane Name]* from the *View* menu.
- To resize a pane, place the cursor over the pane border until a double-arrow cursor appears. Click and drag on the pane border to resize the pane.


Sorting Frames

By default, frames are sorted in ascending numerical sequence by frame number. Click on a column header in the Summary pane to sort the frames by that column. For example, to sort the frames by size, click on the *Frame Size* column header.

An embossed triangle next to the header name indicates which column the frames are sorted by. The direction of the triangle indicates whether the frames are in ascending or descending order, with up being ascending.

Note that it may take some time to sort large numbers of frames.

Working With Multiple Frame Displays

To create a second Frame Display, click the *Duplicate View* icon  on the Frame Display toolbar. This will create another Frame Display window. You can have as many Frame Displays open as you wish. Each Frame Display is given a number in the title bar to distinguish it from the others.

Multiple Frame Displays are useful for comparing two frames side by side. They are also useful for comparing all frames against a filtered subset, or two filtered subsets against each other.

To navigate between multiple Frame Displays, click on the Frame Display icon in the Control window toolbar. A drop-down list will appear, listing all the currently open Frame Displays. Select the one you want from the list and it will come to the front.

Filters and Multiple Frame Displays

When you apply a filter, you can choose to have the filter applied to the current Frame Display or to a new one. The filter being used on any Frame Display is given in the upper right of the toolbar in a tooltip.

If you click the Filter button on the Control window, the assumption is that you are applying the filter to the original, unfiltered Frame Display.

If you click the Filter button on a Frame Display, the filter will be applied to the data in the Frame Display. If the data in the Frame Display is already filtered, the effect is the same as applying two filters to the data.

For example, open the Frame Display to look at some captured data. This data is unfiltered. From the Frame Display, you click the Filter icon and create a filter which keeps only frames where the source IP address is 123.456.0.1 in them. You choose to apply the filter to a new Frame Display. Frame Display #2 is created and only frames with that source IP address are listed in the Summary pane. Now you want to see only those frames from that address carrying HTTP. Click on the Filter icon in Frame Display #2, create an HTTP filter and apply it to a new Frame Display. Frame Display #3 opens and shows only frames where the source IP address is 123.456.0.1 and which carry HTTP. If you wish, you can now go back to Frame Display #2 (which shows all frames where the source IP address is 123.456.0.1), click on the Filter icon and create a filter which keeps all FTP frames. Apply it to a new Frame Display. Frame Display #4 opens, which shows all frames where the source IP address is 123.456.0.1 and which carry FTP.

Red Frame Numbers or Bytes

Red is reserved for bytes or frames with errors. In the Summary pane, frame numbers in red mean there is an error in the frame. This could be a physical error or an error in the protocol decode.

Synchronization Between the Event and Frame Displays

The Frame Display is synchronized with the Event Display. Click on a frame in the Frame Display and the corresponding bytes will be highlighted in the Event Display. Each Frame Display has its own Event Display.

As an example, here's what happens if the following sequence of events occurs.

1. Click on Frame Display icon in Control window toolbar to open the Frame Display.

-
2. Click on Duplicate View icon to create Frame Display #2.
 3. Click on Event Display icon in Frame Display #2. Event Display #2 opens. This Event Display is labeled #2, even though there is no original Event Display, to indicate that it is synched with Frame Display #2.
 4. Click on a frame in Frame Display #2. The corresponding bytes are highlighted in Event Display #2.
 5. Click on a frame in the original Frame Display. Event Display #2 does not change.

Physical vs. Logical Byte Display

The Event Display window and Event Pane in the Frame Display window show the physical bytes. In other words, they show the actual data as it appeared on the circuit. The Radix, Binary and Character panes in the Frame Display window show the logical data, or the resulting byte values after escape codes or other character altering codes have been applied (a process called frame transformation).

As an example, bytes with a value of less than 0x20 (the 0x indicates a hexadecimal value) cannot be transmitted in Async PPP. To get around this, a 0x7d is transmitted before the byte. The 0x7d says to take the next byte and subtract 0x20 to obtain the true value. In this situation, the Event pane will show 0x7d 0x23, while the Radix pane will show 0x03.

Protocol Layer Colors


WHAT THE COLOR OF DATA BYTES MEANS

The color of the data in the panes specifies which layer of the protocol stack the data is from. All data from the first layer is bright blue, the data from the second layer is green, the third layer is pink, etc. The protocol name for each layer in the Decode pane is in the same color. Note that the colors refer to the layer, not to a specific protocol. In some situations, a protocol may be in two different colors in two different frames, depending on where it is in the stack. You can change the default colors for each layer.

Red is reserved for bytes or frames with errors. In the Summary pane, frame numbers in red mean there is an error in the frame. This could be a physical error or an error in the protocol decode.

Searching for Frame (Decode) Errors

CHANGING PROTOCOL LAYER COLORS

Click the *Colors* icon  to change the colors used to differentiate different protocol layers in the Decode, Event, Radix, Binary and Character panes.

To change a color, click on the arrow next to each layer and select a new color.

Analyzing Byte-level Data

Event Display


To open this window


Click the Event Display icon  on the Control window toolbar.

The Event Display window provides detailed information about every captured event. Events include data bytes, data related information such as start-of-frame and end-of-frame flags, and FTS information, such as Data Capture Was Paused. Data bytes are displayed in hex on the left side of the window, with the corresponding ASCII character on the right.

Click on an event to find out more about it. The three status lines at the bottom of the window will update with information such as the time the event occurred (for data bytes, the time the byte was captured), the value of the byte in Hex, Decimal, Octal, and Binary, any errors associated with the byte, and more.

Events with errors are shown in red to make them easy to spot.

When capturing data live, FTS continually updates the Event Display as data is captured. Click the *Freeze* icon  on the toolbar to prevent the display from updating. While frozen, you can review your data, run searches, determine delta time intervals between bytes, and check CRCs. To resume updating the display, click the *Freeze* icon again.

You can have more than one Event Display open at a time. Click the *Duplicate View* icon  to create a second, independent Event Display window. You can freeze one copy of the Event Display and analyze your data, while the second Event Display updates as new data is captured.

The Event Display Toolbar



Home – brings the Control window to the front.



Capture to Buffer - Begins data capture to the buffer only.



Capture to Disk - Begins data capture to disk.



Pause/Resume - Available after data capture has started. Click once to pause data capture. Data can be reviewed and saved, but no new data will be captured. Click again to Resume capture.



Clear Buffer - This will clear the capture buffer and stop data capture to buffer.



Close Capture File - This will close a capture file and stop data capture to disk.



Freeze Display - Freezes the window so you can review a portion of data. Data capture will continue in the background. Click on the button again to unfreeze the window. When you do this, the screen will quickly fill in the data captured since the screen freeze and jump you down to view incoming data again.



Duplicate View - create a second Frame Display window identical to the first.



Frame Display - brings up a Frame Display, with the frame of the currently selected bytes highlighted.



Show Only Data - brings up a Frame Display showing just the data in the frame (also called the payload)



Save - save the currently selected bytes or the entire buffer



Find - search for errors, string patterns,



Go To - opens the Go To dialog, where you can specify which event number to go to



CRC - change the algorithm and seed value used to calculate CRCs. To calculate a CRC, select a byte range, and the CRC will appear in the status lines at the bottom of the Event Display.



Character Only - FTS shows both the number (hex, binary, etc.) data and the character (ASCII, EBCDIC or BAUDOT) data on the same screen. If you do not wish to see the hex characters, click on the Character Only button. Click again to go back to both number and character mode.



Number Only - Controls whether FTS displays data in both character and number format, or just number format. Click once to show only numeric values, and again to show both character and numeric values.



All Events - Controls whether FTS shows all events in the window, or only data bytes. Events include control signal changes and framing information.





Font Size - Brings up the Font Dialog box, allowing you to change the font size.





Timestamping Options – Brings up the timestamping options window which has options for customizing the display and capture of timestamps.

Opening Multiple Event Display Windows

Click the Duplicate View icon  from the Event Display toolbar to open a second Event Display window. You can open as many Event Display windows as you like. Each Event Display is independent of the others and can show different data, use a different radix or character set, or be frozen or live.

The Event Display windows are numbered in the title bar. If you have multiple Event Displays open, click on the Event Display  icon on the Control window toolbar to show a list of all the Event Displays currently open. Select a window from the list to bring it to the front.

Calculating CRCs or FCSs

1. Open the Event Display  window.
2. Click and drag to select the data you want to generate a CRC for.
3. Click on the CRC icon .
4. In the CRC dialog box, click on the down arrow to show the list of choices for CRC algorithms. Choose *CRC 32 (Ethernet)*.
5. Enter a seed value in hexadecimal if desired.


-
- Click OK to generate the CRC. It will appear in the byte information lines at the bottom of the Event Display window. Whenever you select a range of data, a CRC will be calculated automatically.

Ethernet network cards do not normally send the CRC with the frame to the upper layers of the system. The hardware on the card checks that the CRC is correct and then throws it away. FTS marks the place where the CRC would be in the data with "CRC!". When viewing Ethernet capture files made with other programs, the CRC may or may not be included, depending on the specifications of the capturing software/hardware.

The CRC calculated in the Event Display window will be reversed from the CRC shown in the data. CRCs are calculated in network data order (from Most Significant Byte to Least Significant Byte). The Ethernet specification says to send data in host data order (LSB to MSB). Therefore the CRC as captured in the data will be the reverse of the CRC as calculated.

Example: If the CRC in the data is shown as 00 01 02 03, the Event Display will calculate the CRC and show it in the status lines as 03 02 01 00. This is correct.


Calculating Delta Times and Data Rates

- Click on the Event Display icon  on the Control window to open the Event Display window.
- Use the mouse to select the data you want to calculate a delta time and rate for.
- The Event Display window will show the delta time and the data rate in the status lines at the bottom of the window.

Switching Viewing Formats


SWITCHING BETWEEN VIEWING ALL EVENTS AND VIEWING DATA EVENTS

By default, FTS shows all events, which includes data bytes, start-of-frame and end-of-frame characters and FTS events such as Data Captured Was Paused.

Click on the Display All Events icon  to remove the non-data events. Click again to display all events.


SWITCHING BETWEEN LIVE UPDATE AND REVIEW MODE

The Event Display and Frame Display windows can either update to display new data as it is captured, or be frozen to allow data to be analyzed. By default, the Event Display continually updates with new data, and the Frame Display is frozen.

Click the Freeze icon  to freeze the display and prevent it from scrolling. Click the Freeze icon again to resume live update.

FTS will continue to capture data in the background while the display is frozen. When live update is resumed, the display will update with the latest data.


You can have more than one Event Display or Frame Display window open at a time. The Freeze/Resume function is independent on each window. This means that you can have two Event Display windows open simultaneously, and one window can be frozen while the other

continues to update. Click the *Duplicate View* icon  to open additional Event or Frame Display windows.

SWITCHING BETWEEN HEX, DECIMAL, OCTAL OR BINARY

FTS displays data in Hex by default. There are several ways to change the radix used to display data.


1. Go to the View menu and select the radix you want. A check mark next to the radix indicates which set is currently being used.
2. Right-click on the "Hex" header label and choose a different radix.

If you want to see only the numerical values, click on the Numbers Only  icon on the Event Display toolbar.


SWITCHING BETWEEN ASCII, EBCDIC AND BAUDOT

FTS displays data in ASCII by default. There are several ways to change the character set used to display data.


1. Go to the View menu and select the character set you want. A check mark next to the character set indicates which set is currently being used.
2. Right-click on the "ASCII" header label and choose a different character set.

If you want to see only characters, click on the Characters Only  icon on the Event Display toolbar.


VIEWING ONLY ASCII (OR EBCDIC OR BAUDOT)

Click on the Characters Only  icon on the Event Display toolbar. To add the numerical values back to the display, click the Characters Only icon again.

VIEWING ONLY HEX (OR DECIMAL OR OCTAL OR BINARY)


Click on the Numbers Only  icon on the Event Display toolbar. To add the characters back to the display, click the Number Only icon again.

FONT SIZE

1. Click on the *Font Size* icon .
2. Choose a font size from the list.
3. Click OK.





















The font size can be changed on several windows. Changing the font size on one window does not affect the font size on any other window.










List of All Event Symbols

By default, the Event Display shows all events, which includes control signal changes, start and end of frame characters and flow control changes. If you want to see only the data bytes, click on the All Events button . Click again to display all events.

Click on a symbol, and FTS will display the symbol name and sometimes additional information in the status lines at the bottom of the Event Display window. For example, clicking on a control signal change symbol will show you which signal(s) changed.

In addition to data bytes, the events shown are (in alphabetical order):

-
-  Abort
 -  Broken Frame - The frame did not end when FTS expected it to. This occurs most often with protocols where the framing is indicated by a specific character, control signal change, or other data related event.
 -  Buffer Overflow - Indicates a buffer overflow error.
 -  Control Signal Change - One or more control signals changed state. Click on the symbol, and FTS will show you which signal(s) changed at the bottom of the Event Display window.
 -  Data Capture Paused - The Pause icon was clicked, pausing data capture. No data is recorded while capture is paused.
 -  Data Capture Resumed - The Pause icon was clicked again, resuming data capture.
 -  Dropped Frames - Some number of frames were lost. Click on the symbol, and FTS will show how many frames were lost at the bottom of the Event Display window.
 -  End of Frame - Marks the end of a frame.
 -  Flow Control Active - An event occurred which caused flow control to become active (i.e. cause FTS to stop transmitting data). Events which activate flow control are signal changes or the receipt of an XON character.
 -  Flow Control Inactive - An event occurred which caused flow control to become inactive (i.e. cause FTS to transmit data). Events which deactivate flow control are signal changes or the receipt of an XOFF character.
 -  Frame Recognizer Change - A lowest layer protocol was selected or removed here, causing the frame recognizer to be turned off or on.
 -  I/O Configuration Change - A change was made in the Set I/O Configuration window which altered the baud, parity, or other circuit setting.
 -  Long Break
 -  Low Power - The battery in the ComProbe is low.
 -  Short Break
 -  Spy Event (Spy Mode only) - Spy events are commands sent by the application being spied on to the UART.
 -  Start of Frame - Marks the start of a frame.
 -  Begin Sync Character Strip
 -  End Sync Character Strip
 -  Sync Dropped

-
-  Sync Found
 -  Sync Hunt Entered
 -  Sync Lost
 -  Test Device Stopped Responding - FTS lost contact with the ComProbe for some reason, often because there is no power to the ComProbe.
 -  Test Device Began Responding - FTS regained contact with the ComProbe.
 -  Timestamping Disabled - Timestamping was turned off here. Events following this event will not be timestamped.
 -  Timestamping Enabled - Timestamping was turned on here. Events following this event will have timestamps.
 -  Underrun Error
 -  Unknown Event

Event Numbering

This section talks about how events are numbered when they are first captured and how this affects the display windows in FTS. The information in this section applies to frame numbering as well.

When FTS captures an event, it gives the event a number. If the event is a data byte event, it receives a byte number in addition to an event number. There are usually more events than bytes, with the result is that a byte might be listed as Event 10 of 16 when viewing all events, and Byte 8 of 11 when viewing only the data bytes.

The numbers assigned to events that are wrapped out of the buffer are not reassigned. In other words, when event number 1 is wrapped out of the buffer, event number 2 is not renumbered to event 1. This means that the first event in the buffer may be listed as event 11520 of 16334, because events 1-11519 have been wrapped out of the buffer. Since row numbers refer to the event numbers, they work the same way. In the above example, the first row would be listed as 2d00 (which is hex for 11520.)

The advantage of not renumbering events is that you can save a portion of a capture file, send it to a colleague, and tell your colleague to look at a particular event. Since the events are not renumbered, your colleague's file will use the same event numbers that your file does.

Searching

You can search your data in several different ways.

Types of Searches

String or Pattern in the Data

String or Pattern in the Protocol Decode




Frame Error (such as an FCS Error or error in the decode)

Time (move to data captured at a specific time or move through the data by time interval)

Special Event

Go To a Specific Byte or Frame Number

To Begin a Search

1. Capture some data to the buffer, or open a capture file to search.
2. Open the Event Display  or Frame Display  window.
3. Click on the *Find* icon  or choose *Find* from the *Edit* Menu.
4. The Find window has a tab for each type of search. Click on the appropriate tab for the type of search you want to do.
5. Select the parameters for your search, and click *Find Next*. *Find Next* will look for the next occurrence of the search criteria, while *Find Previous* will look for an earlier occurrence of the search criteria.
6. Press F3 to repeat the last search.

Search results are highlighted in the Event or Frame Displays, or both if appropriate. The selection in the Event Display appears on the third line down from the top of the window by default: this value can be changed.

Searching for Frame Errors

There are two options for error searching. Click the appropriate radio button for the type of search you want to perform, and then click *Find Next*.

Search for All Errors will find frame errors as well as frames with byte-level errors (such as parity or CRC errors).

Search for Frame Errors will find Frame specific errors, such as Frame Check errors.

Go To


This type of search allows you to go to a particular frame or event, or to move through the data X number of events or frames at a time. You can move either forward or backwards through the data.

To go to a particular frame, select the *Frame Number* radio button and type the frame number in the box. Then click the *Go To* button. To move forward or backward a set number of frames, type in the number of frames you want to move, and then click the *Move Forward* or *Move Backward* button.

To go to a particular event, select the *Data Event Number* or *All Events Number* radio button, type the number of event in the box, and click the *Go To* button. To move forward or backwards through the data, type in the number of events that you want to move each time, and then click on the *Move Forward* or *Move Backward* button. For example, to move forward 10 events, type the

number 10 in the box, and then click on *Move Forward*. Each time you click on *Move Forward*, FTS will move forward 10 events.

See Event Numbering for why the Data Event Number and All Events Number may be different.

As a general rule, if you have the *Show All Events* icon  pressed down on the Event Display window or Frame Display Event pane, choose All Events Number. If the Show All Events button is up, choose Data Event Number.

Searching within Decodes

Search For String in Decode lets you to do a string search on the data in the Decode Pane of the Frame Display window. You can search one or both sides of the circuit, and your search can include wildcards. You can use characters, hex or binary digits, wildcards or a combination of any of the formats when entering your string.

Searching for Special Events

FTS inserts or marks events other than data bytes in the data stream. For example, FTS will insert start-of-frame and end-of-frame markers into framed data, marking where each frame begins and ends. If a hardware error occurs, FTS will show this using a special event marker.

To search for a special event, check the event or events you want to look for in the list of special events. Then click Find Next. Not all special events are relevant to all types of data. For example, control signal changes are relevant only to serial data and not to Ethernet data.

Search by Pattern

Search by Pattern lets you to do a traditional string search. You can search one or both sides of the circuit, and your search can include wildcards. You can combine any of the formats when entering your string.

ENTERING CHARACTERS

Place the cursor in the Pattern box and type in your string. Click Find Next in order to find the next occurrence of the string. You can click on Find Next as many times as necessary until FTS has searched all the data. Clicking on Find Previous will search the buffer backwards.

You can enter any character from a character set, with the following exceptions: \ \$ & ^ ?. These characters are used as prefixes to let you to enter hex, binary, control or wildcard characters. The escape character is the backslash \. Use this character when you want to search for one of the above restricted characters. For example, to search for a \$, you would enter \\$. To search for a \, enter \\.

Check Ignore Case to do a case-insensitive search.

ENTERING HEX OR BINARY

To enter a hex value, enter a \$ followed by two hex digits. For example, to search for hex 00 01, enter \$00\$01.

If you need to specify the \$ as a character, use \\$.

Just as the \$ symbol tells FTS that the following characters are hex digits, the & symbol tells FTS that a binary number comes next. For example, to search for binary 00001111, you would use &00001111.

If you need to specify the & as a character, use \&.

ENTERING CONTROL CHARACTERS

The ^ (caret) is used to enter the control characters Ctrl-A through Ctrl-Z and Ctrl-@,[,\,]- when using the ASCII character set. For example, ^A specifies Ctrl-A (\$01) and ^@ specifies ASCII NUL (\$00).

If you need to specify the ^ as a character, use \^.

Note that neither the ^ character nor control characters exist in Baudot, so attempts to search for the ^ character will result in an error message. The ^ character exists in EBCDIC, but control characters do not. A search for ^A in EBCDIC will match any occurrence of ^A (\$5F\$C1). You do not need to use the escape character to search for a ^ character in EBCDIC.

USING WILDCARDS

The wildcard character is the question mark (?).

FTS supports wildcard searching at the byte, nibble and bit level. Wildcards can be used in place of characters, hex digits, and binary digits.

If you need to search for a ?, you can use \?.

EXAMPLES OF SEARCH STRINGS

To search for any single byte in the range of hex \$10 through \$1F, type \$1?.

&111111?? will search for binary numbers beginning with 111111 and ending with any combination of 1 and 0. 11111100, 11111101, 11111110, and 11111111 are all strings that match the search criteria.

To search for any four character string which starts with an L and ends with an ES, type L?ES.

You can combine formats in one string. For example, another way to specify a search for the string L?ES is \$4C&???????&01000101S.

Searching by Time

FTS can search by time in two different ways.

An absolute timestamp search means that FTS will search for an event at the exact date and time specified. If no event is found at that time, FTS will go to the nearest event either before or after the selected time, based on the "Go to the timestamp" selection.

A relative search means that FTS will begin searching from whatever event you are currently on, and search for the next event a specific amount of time away. Use the radio buttons to indicate which type of search you would like to do.

Note that some special events like frame markers do not have timestamps and so will be skipped in the search. Data events that do not have timestamps because timestamping was turned off either before or during capture will likewise be skipped.

ABSOLUTE TIMESTAMP SEARCH

Specify the time to search for using the counters in the middle of the window. Click on the arrows next to each item to increase or decrease the value of each counter. By default, the counters are

filled in with the timestamp of the first event in the buffer. When you have finished selecting the time to search for, click on the Go To button to start the search.

Sometimes there can be more than one event with the same timestamp. FTS will highlight all events with the same timestamp.

RELATIVE TIMESTAMP SEARCH

Click on the event in the Event Display window that you want to begin the search from. The event must have a timestamp in order for relative timestamp search to work. In the Find window, use the counters in the middle of the window to specify the time interval you want to jump. You can specify intervals in days, hours, minutes, seconds, and fractions of a second, or any combination of these. When you have specified the time interval you want to use, click on the Move Forward or Move Backward buttons to start the search from the current event.

For example, to search for an event occurring 10 seconds after the currently selected event, choose to do a relative timestamp search, use 10 seconds for your time interval, and click on Move Forward.

As with absolute timestamping, FTS will highlight all events with the same timestamp.

CHOOSING "ON OR BEFORE" OR "ON OR AFTER"

FTS will search for an event that matches the time specified. If no event is found at that time, FTS will go to the nearest event either before or after the specified time. Choose whether to have FTS go to the nearest event before the specified time or after the specified time by clicking the appropriate radio button in the "Go to the timestamp" box.

If you are searching forward in the buffer, you will usually want to choose the "On or After" button. If you choose the "On or Before" option, it may be that FTS will finish the search and not move from the current byte, if that byte happens to be the closest match.

SUBTLETIES OF TIMESTAMP SEARCHING

Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, FTS will ignore data without a timestamp.


Changing Where the Search Lands

When you do a search in FTS, the byte or bytes matching the search criteria are highlighted in the Event Display, with the first selected byte appearing on the third line of the display. To change the line on which the first selected byte appears, open fts.ini (located in the root directory FTS was installed to), go to the [CVEventDisplay] section and change the value for SelectionOffset. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

Filtering

How To Create and Use a Filter

There are two steps to using a filter. First a filter condition must be defined, and then it must be applied as either a capture or display filter. FTS combines both filter definition and application on one window.

1. Click the *Filters* icon  on either the Control or Frame Display window.
2. Click the *Define Conditions* tab.
3. FTS supports four different types of filters.
 - Node and Conversation
 - Protocol
 - Pattern or Offset
 - Custom Filter made using BPF Strings
4. After your filter is defined, click either the *Display Filters* tab or the *Capture Filters* tab. (Capture filtering is not available when viewing a capture file.) Capture filters look at frames as they are being captured and either discard them or put them in the capture buffer based on the filter criteria. Display filters look at the frames in the capture buffer and display only those frames that match the criteria. (Click for more detailed info.)
5. Choose the filter or filters to apply. Here's how to apply a capture filter, and here's how to apply a display filter.
6. Click *OK*. The Filters window will close and the filter will be applied.

Difference Between Capture and Display Filters


There are two types of filters in FTS: display and capture.

A capture filter looks at frames when they are first captured. If the frame satisfies the filter criteria, the frame is kept and put in the capture buffer. If the frame does not satisfy the filter criteria, it is thrown away. Data that is filtered out using a capture filter cannot be recovered. Only one capture filter can be active at a time.

A display filter looks at frames that have already been captured. It looks at every frame in the capture buffer and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. Unlike a capture filter, where data that does not match is thrown away, all the data is kept with a display filter. The filter just displays a subset of the data. Multiple display filters can be used simultaneously, and different windows can be displaying data using different filters.


Defining Filters

DEFINING NODE AND CONVERSATION FILTERS


1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Define Conditions* tab at the top of the window.

-
3. In the tree view on the left, click the words *Node and Conversation*. The right side of the window will change to show the Node and Conversation definition pane.
 4. If you want to include all frames matching your filter, select the *Include* radio button at the center top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button.
 5. In the Node A section, select the radio button for the type of address you want. *All* means to pass all frames. Type the MAC or IP address of the node you wish to filter on.
 6. Choose a direction arrow from the *Direction* box. The left arrow will filter on all frames where Node A is the destination, the right arrow will filter on all frames where Node A is the source, and the double arrow will filter on all frames where Node A is either the source or the destination.
 7. If you want to filter on just one node, stop right here. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the window.
 8. If you want to filter on traffic going between two nodes (i.e. a conversation), select an address type and add the MAC or IP address of the second node in the Node B box. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the window.


DEFINING PROTOCOL FILTERS

1. Click on the Filter icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the Define Conditions tab at the top of the window.
3. In the tree view on the left, click the word Protocol. The right side of the window will change to show the Protocol definition pane.
4. If you want to include all frames matching your filter, select the Include radio button at the top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the Exclude radio button.
5. Select a protocol from the protocol list.
6. Click the Add button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the window.

DEFINING PATTERN OR OFFSET FILTERS

1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Define Conditions* tab at the top of the window.
3. In the tree view on the left, click the words *Pattern Match*. The right side of the window will change to show the Pattern Match definition pane.
4. If you want to include all frames matching your filter, select the *Include* radio button at the top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button.
5. Enter a pattern in the *Look for this Pattern* box. Use \$ to specify a hex byte (e.g. \$00 will look for a null character).
6. Enter the offset and where the offset should start in the *Offset this many bytes from start of* boxes. FTS can begin counting from the start of the frame or the start of a protocol header. An offset of 0 means to look at the first byte, an offset of 1 means to look at the second byte, etc.
7. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the window.


USING TCPDUMP TO CREATE A CUSTOM FILTER

1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Define Conditions* tab at the top of the window.


-
3. In the tree view on the left, click the words *BPF Program (tcpdump syntax)*. The right side of the window will change to show the BPF definition pane.
 4. If you want to include all frames matching your filter, select the *Include* radio button at the top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button.
 5. Enter the BPF string in the *Expression* box.
 6. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the window.

Filtering functionality is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump. The Filter String Formats help topic describes how to write a filter string for the most common types of filters. For the full description of BPF syntax, click here for the instructions from the tcpdump man page.

HOW TO MODIFY A CONDITION


1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Define Conditions* tab at the top of the window.
3. In the tree view on the left, click the condition you want to modify. The right side of the window will change to show the definition pane for the type of condition selected, and put the contents of the condition in the pane.
4. Change the condition to the desired state.
5. Click the *Modify* button at the bottom of the definition pane.

HOW TO DELETE A CONDITION

1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Define Conditions* tab at the top of the window.
3. In the tree view on the left, click the condition you want to delete. The right side of the window will change to show the definition pane for the type of condition selected, and put the contents of the condition in the pane.
4. Click the *Delete* button at the bottom of the definition pane.

How to Apply a Capture Filter


Capture filters are unavailable when viewing a capture file.

1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Capture Filter* tab at the top of the window.
3. In the tree view on the left, click the condition you want to apply, and then click the arrow buttons to move the condition to the *Conditions Selected in Filter* box. You may choose more than one condition to filter on.
4. The *Filter Representation* box at the bottom of the window shows an English version of what the filter will do. Click the checkbox to see the tcpdump syntax.
5. *[Optional]* Click the *Name* button to create a name for your condition or group of conditions. This name will appear in the *Named Filters* box. In the future, you will be able to select the same condition(s) by selecting the name from the box.
6. Click OK. The Filters window will close and FTS will apply the filter.

When a capture filter is being used, the Control window will show "Capture Filters Active" on the status bar. To view the capture filters in use, open the Filters window and click the Un-Apply Filters tab.


Capture filters look at data as it is being captured, and put in the capture buffer only those frames that match the filter criteria.

How to Apply a Display Filter


1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Display Filter* tab at the top of the window.
3. In the tree view on the left, click the condition you want to apply, and then click the arrow buttons to move the condition to the *Conditions Selected in Filter* box. You may choose more than one condition to filter on.
4. The *Filter Representation* box at the bottom of the window shows an English version of what the filter will do. Click the checkbox to see the TCPDump syntax.
5. [Optional] Click the *Name* button to create a name for your condition or group of conditions. This name will appear in the *Named Filters* box. In the future, you will be able to select the same condition(s) by selecting the name from the box.
6. If you opened the Filters dialog from a Frame Display, you have the choice of applying the filter to the same Frame Display or to a new one. At the top of the window, choose whether to apply the filter to a new Frame Display window or to the current Frame Display. (If you opened the Filters dialog from the Control window, the filter will automatically be applied to a new window.)
7. Click OK. The Filters window will close and FTS will apply the filter.

When a display filter is being used, the Frame Display window will show the name of the filter on the toolbar to the far right. If the filter was not named, "no name" will appear in the Filter box. To view the display filters in use, open the Filters window and click the Filters In Use tab.

How To Know What Filter Is Being Used

1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Filters in Use* tab at the top of the window.
3. The left side of the window will show what filters are currently in use.

How to Remove a Filter

1. To remove a display filter, close the Frame Display window that uses the filter.
2. To remove a capture filter, click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
3. Click on the *Capture Filters* tab at the top of the window.
4. The capture filter currently in use will be shown in the *Select Filters to Use* box. Click the condition(s) you want to remove. Use the arrow buttons to move the conditions to the *Available Filters* box on the left, OR click the *Un-Apply Filters* button to remove all conditions.

Naming Filters

Naming filters means putting a name to a condition or group of conditions. It's a convenient way of grouping conditions into one filter set and remembering what the filter does. Named filters can be selected from a list on the Apply Filter tabs, making it very easy to reuse groups of conditions.

To name a filter, move the conditions to the *Select Filters to Apply* box, and click the *Name Filters* button. Give the filter a name.

To delete a named filter, select the filter from the list box, and click the *Delete Filter* button. This will delete the filter only. It will not delete the conditions used in the filter.



Showing Named Filters

The *Show Named Filters* tab displays a list of all named filters and their conditions. Double-click on a filter name to expand it and show the conditions for each named filter.

Naming filters is a good way to group conditions together. Named filters can be selected from the Apply Filter tabs, making it easy to reuse groups of conditions.



Saving and Loading Filter Files

SAVING FILTERS TO FILE

1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click on the *Define Conditions* tab at the top of the window.
3. Define one or more conditions.
4. Click the Save icon  and give your filter file a name.

Saving a filter file saves the conditions you've created. You can combine these conditions in many ways to create different capture or display filters. If you create a condition set (a group of conditions to apply all at the same time) for a capture or display filter and want to save the condition set, name the filter, and then save the filter file. The named filter will be saved as part of the filter file, and will be available the next time the file is opened.

OPENING A FILTER FILE

1. Click on the *Filter* icon  on the Control or Frame Display window toolbar to open the Filter window.
2. Click the Open icon  and browse to the filter file.

Filter files have a .filter extension by default and are located in the My Configurations directory.

Filter String Formats

Filtering functionality in FTS is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump. The instructions that follow describe how to write the most common filter expressions when filtering Ethernet Type II data. For the full description of BPF syntax, click [here](#) for an excerpt from the tcpdump man page.

The filter format consists of one or more "qualifiers", which may or may not be followed by an ID, which identifies the thing to be filtered on.

Qualifiers

There are three kinds of qualifiers: type, direction and protocol.

Type qualifiers tell you what kind of thing the ID refers to. There are three possible types: host, net and port. If no type is given, host is assumed.

Direction qualifiers specify the direction of traffic to or from the ID. There are four possible directions:

- src - source. Filters on frames for which the ID is the source.
- dst - destination. Filters on frames for which the ID is the destination.
- src or dst - source or destination. Filters on frames for which the ID is either the source or the destination.
- src and dst - source and destination. Filters on frames for which the ID is both the source and the destination

If no direction is given, src or dst is assumed.

Protocol qualifiers specify a particular protocol. Possible protocol qualifiers are: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp, where ether stands for Ethernet. If no protocol is given, all protocols consistent with the type are assumed.

IDs, or Identifiers

Identifiers are usually a name or a number identifying a particular node, protocol, network, etc. Examples are Ethernet MAC addresses or IP addresses. To specify a hex value, use 0x before the value. Example: 0x50.

Expressions and Relational Operators

You can combine identifiers using the following:

- 'and' or '&&' - concatenation. Filters on frames where both identifiers are true.
- 'or' or '||' - alternation. Filters on frames where one or both of the identifiers is true.
- 'not' or '!' - negation. Excludes a frame if the identifier is true.

Negation has highest precedence and will be evaluated first. Alternation and concatenation have equal precedence and are evaluated left to right.

Use parentheses to combine expressions. Example: to filter on all frames from Abel and either Baker or Charlie, use: host Abel and (Baker or Charlie)

Filter on MAC Address

To filter on all frames to and from an Ethernet MAC Address, use the following syntax:

```
ether host 00:01:02:03:04:05
```

To filter on all frames to and from two MAC Addresses:

```
ether host 00:01:02:03:04:05 and 06:07:08:09:0a:0b
```

Filter on IP Address

To filter on all frames to and from an IP address, use the following syntax:

```
ip host 100.200.300.4
```

To filter on all frames to and from two IP addresses, use:

```
ip host 100.200.300.4 and 100.200.300.5
```

Filter on Protocol

To filter on a protocol, enter the protocol name in the string box. Possible protocols are: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp, where ether stands for Ethernet. You can also filter on protocols within protocols using the *proto* keyword.

Examples:

ip - filters on all IP frames

ip proto \tcp - filters on all TCP frames (tcp is a keyword and must be escaped using the '\ when used as an ID)
port 80 - filters on all frames 'to and from' a TCP port, in this case port 80 (HTTP)

Filter at an Offset

To specify an offset from a protocol, place the value in brackets.

ether[13]>5 - examines the 13th byte from Ethernet start of frame for a value greater than 5 (remember that the first byte is at offset zero).

Berkeley Packet Filtering Man Page

The following text is taken from the tcpdump man page. References to CShell have been removed, along with some references to escape characters which are relevant only when running tcpdump under CShell and which are not relevant to filtering in FTS.

expression selects which packets will be dumped. If no *expression* is given, all packets on the net will be dumped. Otherwise, only packets for which *expression* is 'true' will be dumped. The *expression* consists of one or more *primitives*. Primitives usually consist of an *id* (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

<i>type</i>	qualifiers say what kind of thing the id name or number refers to. Possible types are host , net and port . E.g., 'host foo', 'net 128.3', 'port 20'. If there is no type qualifier, host is assumed.
<i>dir</i>	qualifiers specify a particular transfer direction to and/or from <i>id</i> . Possible directions are src , dst , src or dst and src and dst . E.g., 'src foo', 'dst net 128.3', 'src or dst port ftp-data'. If there is no dir qualifier, src or dst is assumed. For 'null' link layers (i.e. point to point protocols such as slip) the inbound and outbound qualifiers can be used to specify a desired direction.
<i>proto</i>	qualifiers restrict the match to a particular protocol. Possible protos are: ether , fdi , ip , arp , rarp , decnet , lat , sca , moprc , mopdl , tcp and udp . E.g., 'ether src foo', 'arp net 128.3', 'tcp port 21'. If there is no proto qualifier, all protocols consistent with the type are assumed. E.g., 'src foo' means '(ip or arp or rarp) src foo' (except the latter is not legal syn- tax), 'net bar' means '(ip or arp or rarp) net bar' and 'port 53' means '(tcp or udp) port 53'. ['fdi' is actually an alias for 'ether'; the parser treats them identically as meaning 'the data link level used on the specified network interface.' FDDI headers contain Ethernet-like source and destination addresses, and often contain Ethernet-like packet types, so you can filter on these FDDI fields just as with the analogous Ethernet fields. FDDI headers also contain other fields, but you cannot name them explicitly in a filter expression.]

In addition to the above, there are some special 'primitive' keywords that don't follow the pattern: **gateway**, **broadcast**, **less**, **greater** and arithmetic expressions. All of these are described below. More complex filter expressions are built up by using the words **and**, **or** and **not** to combine primitives. E.g., 'host foo and not port ftp and not port ftp-data'. To save typing, identical qualifier lists can be omitted. E.g., 'tcp dst port ftp or ftp-data or domain' is exactly the same as 'tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain'. Allowable primitives are:

dst host <i>host</i>	True if the IP destination field of the packet is <i>host</i> , which may be either an address or a name.
src host <i>host</i>	True if the IP source field of the packet is <i>host</i> .
host <i>host</i>	True if either the IP source or destination of the packet is <i>host</i> . Any of the above host expressions can be prepended with the keywords, ip , arp , or rarp

	as in: ip host host which is equivalent to: ether proto ip and host host If <i>host</i> is a name with multiple IP addresses, each address will be checked for a match.
ether dst ehost	True if the ethernet destination address is <i>ehost</i> . <i>Ehost</i> may be either a name from /etc/ethers or a number for numeric format.
ether src ehost	True if the ethernet source address is <i>ehost</i> .
ether host ehost	True if either the ethernet source or destination address is <i>ehost</i> .
gateway host	True if the packet used <i>host</i> as a gateway. I.e., the ethernet source or destination address was <i>host</i> but neither the IP source nor the IP destination was <i>host</i> . <i>Host</i> must be a name and must be found in both /etc/hosts and /etc/ethers. (An equivalent expression is ether host ehost and not host host which can be used with either names or numbers for <i>host / ehost</i> .)
dst net net	True if the IP destination address of the packet has a network number of <i>net</i> . <i>Net</i> may be either a name from /etc/networks or a network number for details).
src net net	True if the IP source address of the packet has a network number of <i>net</i> .
net net	True if either the IP source or destination address of the packet has a network number of <i>net</i> .
net net mask mask	True if the IP address matches <i>net</i> with the specific netmask. May be qualified with src or dst .
net net/len	True if the IP address matches <i>net</i> a netmask <i>len</i> bits wide. May be qualified with src or dst .
dst port port	True if the packet is ip/tcp or ip/udp and has a destination port value of <i>port</i> . The <i>port</i> can be a number or a name used in /etc/services. If a name is used, both the port number and protocol are checked. If a number or ambiguous name is used, only the port number is checked (e.g., dst port 513 will print both tcp/login traffic and udp/who traffic, and port domain will print both tcp/domain and udp/domain traffic).
src port port	True if the packet has a source port value of <i>port</i> .
port port	True if either the source or destination port of the packet is <i>port</i> . Any of the above port expressions can be prepended with the keywords, tcp or udp , as in: tcp src port port which matches only tcp packets whose source port is <i>port</i> .
less length	True if the packet has a length less than or equal to <i>length</i> . This is equivalent to: len <= length .
greater length	True if the packet has a length greater than or equal to <i>length</i> . This is equivalent to: len >= length .
ip proto protocol	True if the packet is an ip packet of protocol type <i>protocol</i> . <i>Protocol</i> can be a number or one of the names <i>icmp</i> , <i>igrp</i> , <i>udp</i> , <i>nd</i> , or <i>tcp</i> . Note that the identifiers <i>tcp</i> , <i>udp</i> , and <i>icmp</i> are also keywords and must be escaped via backslash (\).

ether broadcast True if the packet is an ethernet broadcast packet. The *ether* keyword is optional.

ip broadcast True if the packet is an IP broadcast packet. It checks for both the all-zeroes and all-ones broadcast conventions, and looks up the local subnet mask.

ether multicast True if the packet is an ethernet multicast packet. The *ether* keyword is optional. This is shorthand for ``ether[0] & 1 != 0'`.

ip multicast True if the packet is an IP multicast packet.

ether proto protocol
 True if the packet is of ether type *protocol*. *Protocol* can be a number or a name like *ip*, *arp*, or *rarp*. Note these identifiers are also keywords and must be escaped via backslash (\). [In the case of FDDI (e.g., ``fddi protocol arp'`), the protocol identification comes from the 802.2 Logical Link Control (LLC) header, which is usually layered on top of the FDDI header. *Tcpdump* assumes, when filtering on the protocol identifier, that all FDDI packets include an LLC header, and that the LLC header is in so-called SNAP format.]

decnet src host True if the DECNET source address is *host*, which may be an address of the form ```10.123"`, or a DECNET host name. [DECNET host name support is only available on Ultrix systems that are configured to run DECNET.]

decnet dst host True if the DECNET destination address is *host*.

decnet host host True if either the DECNET source or destination address is *host*.

ip, arp, rarp, decnet
 Abbreviations for: **ether proto** *p* where *p* is one of the above protocols.

lat, moprc, mopdl
 Abbreviations for: **ether proto** where *p* is one of the above protocols. Note that *tcpdump* does not currently know how to parse these protocols.

tcp, udp, icmp Abbreviations for: **ip proto** *p* where *p* is one of the above protocols.

expr relop expr True if the relation holds, where *relop* is one of `>`, `<`, `>=`, `<=`, `=`, `!=`, and *expr* is an arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators [`+`, `-`, `*`, `/`, `&`, `[]`], a length operator, and special packet data accessors.

To access data inside the packet, use the following syntax: *proto* [*expr* : *size*]
Proto is one of **ether**, **fddi**, **ip**, **arp**, **rarp**, **tcp**, **udp**, or **icmp**, and indicates the protocol layer for the index operation. The byte offset, relative to the indicated protocol layer, is given by *expr*. *Size* is optional and indicates the number of bytes in the field of interest; it can be either one, two, or four, and defaults to one. The length operator, indicated by the keyword **len**, gives the length of the packet.

For example, ``ether[0] & 1 != 0'` catches all multicast traffic. The expression ``ip[0] & 0xf != 5'` catches all IP packets with options. The expression ``ip[6:2] & 0x1fff = 0'` catches only unfragmented datagrams and frag zero of fragmented datagrams. This check is implicitly applied to the **tcp** and **udp** index operations. For instance, **tcp[0]** always means the first byte of the TCP *header*, and never means the first byte of an intervening fragment. Primitives may be combined using a parenthesized group of primitives and operators.

Negation ('!' or 'not').
Concatenation ('&&' or 'and').
Alternation ('||' or 'or').

Negation has highest precedence. Alternation and concatenation have equal precedence and associate left to right.

Note that explicit **and** tokens, not juxtaposition, are now required for concatenation. If an identifier is given without a keyword, the most recent keyword is assumed. For example, **not host vs and ace** is short for **not host vs and host ace** which should not be confused with **not (host vs or ace)**.

EXAMPLES

To print all packets arriving at or departing from sundown:
host sundown

To print traffic between helios and either hot or ace:
host helios and (hot or ace)

To print all IP packets between ace and any host except helios:
ip host ace and not helios

To print all traffic between local hosts and hosts at Berkeley:
net ucb-ether

To print all ftp traffic through internet gateway snup:
gateway snup and (port ftp or ftp-data)

To print traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuff should never make it onto your local net).
ip and not net localnet

To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host.
tcp[13] & 3 != 0 and not src and dst net localnet

To print IP packets longer than 576 bytes sent through gateway snup:
gateway snup and ip[2:2] > 576

To print IP broadcast or multicast packets that were *not* sent via ethernet broadcast or multicast:
ether[0] & 1 = 0 and ip[16] >= 224

To print all ICMP packets that are not echo requests/replies (i.e., not ping packets):
icmp[0] != 8 and icmp[0] != 0

AUTHORS

Van Jacobson, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA. Full Copyright notice.






Saving Data to File

You can save all or part of a capture buffer. You can also load a previously saved capture file, and save a portion of that file to another file. This feature is useful if someone else needs to see only a portion of the data in your capture file.






For example, you have a ten megabyte capture file and the home office needs to see only two megabytes of that file. You can save only the two megabytes they need to see in a new file.

The Save button and Save menu item are grayed out while data is being captured. You must pause capture before saving.

Saving a Portion of a Capture File or Buffer

1. If you are capturing data, click on the Pause icon  to pause data capture. You cannot save data to file while it is being captured.
2. Open the Event Display  or Frame Display  window, depending on whether you want to specify a range in bytes or in frames.
3. Select the portion of the data that you want to save. Click and drag to select data, or click on the first item, move to the last item and Shift+Click to select the entire range. If the range you want to save is too large to select, note the numbers of the first and last item in the range.
4. Click the Save icon .
5. Click on the radio button labeled Selection. If you selected a range, make sure the starting and ending numbers are correct. To specify a range, type the numbers of the first and last items in the range in the boxes, and select either Events or Frames to indicate whether the numbers are event or frame numbers.
6. Type a filename in the Save As box at the bottom of the screen. Click the Browse icon  to browse to a specific directory. Otherwise your file will be saved in the default capture file directory (usually C:\Program Files\Frontline Test System II\[Product Name]\My Capture Files).
7. Click OK when you are finished.


Saving the Entire Capture Buffer

1. If you are capturing data, click on the Pause icon  to pause data capture. You cannot save data to file while it is being captured.
2. Open the Event Display  or Frame Display  window.
3. Click the Save icon .
4. Click on the radio button labeled Entire Buffer.
5. Type a filename in the Save As box at the bottom of the screen. Click the Browse icon  to browse to a specific directory. Otherwise your file will be saved in the default capture file directory (usually C:\Program Files\Frontline Test System II\[Product Name]\My Capture Files).
6. When you are finished, click OK.

Printing

Printing From The Event Display

Printing from the Event Display prints exactly what is on the screen. If you need to see additional information, such as different radix (hex, decimal, etc.) or timestamps, use the Export feature.

1. Click on the Event Display icon  on the Control window to open the Event Display window.
2. Make sure the data you want to print is displayed in the window. Load a capture file `IDH>Loading_a_Capture_File>Second` if necessary.
3. From the File menu on the Event Display, choose Print.
4. Choose the correct printer and number of pages, and click OK to begin printing.

Print Preview

Print Preview shows you how the data will look printed. You can scroll through the pages and zoom in on the data to get a closer look. The line of buttons across the top of the window controls the functions of the window.

To open the Print Preview window, choose *Print Preview* from the File menu in any window that supports printing. When Print Preview is chosen, the preview display replaces the regular data display in the window.

You can print directly from the Print Preview window. Click on the *Print* button to bring up the print window.

Use the *Next Page* and *Prev Page* buttons to navigate through the data. Next Page will show you the next page in your data will look, while Prev Page will take you back to the previous page.

Two Page will change the display to show two pages of data. When in the Two Page display, the button will read *One Page*. Click on the *One Page* button to return to viewing one page.

Zoom In and *Zoom Out* allow you to change the magnification of the pages. Click on the *Zoom In* to increase the magnification, and on *Zoom Out* to decrease the magnification. When you have reached the limit in either direction, the buttons will be grayed out.

You can also zoom in and out by clicking on the page itself. When the cursor looks like a magnifying glass, you can click on the page to increase the magnification. When you have reached the top level of magnification, the cursor will change back to an arrow. Click on the page to return to normal magnification.

Click on the *Close* button to return to the regular display.

Troubleshooting Printing Problems

Some printer drivers may not be able to handle the FTS True Type fonts correctly in the default mode. When this happens, the printer driver substitutes other fonts for the FTS fonts, resulting in printed data that does not look like the data on the screen. Many printers have several options for handling True Type fonts.

Changing how your printer handles True Type fonts can often be done from the Printer Properties box. Printer Properties can be reached by choosing Printers from the Settings menu on the Start button, and then right-clicking on your printer and choosing Properties. It can also be reached

from the Print window within FTS. Click on the button labelled Properties next to the name of the printer in the Print window.


Every printer handles font substitution a little differently, and every printer puts the font settings in a different place. If you cannot easily find the font settings for your printer, please refer to your printer's documentation for help.

Exporting

The export feature allows you to export your capture files or capture buffer to text or binary format.

Text format is used to create readable text files, which can be printed as is or imported into database programs or spreadsheets. Binary format creates a binary file which can be transmitted by FTS or manipulated by a custom application. The file format for binary export files, along with sample C++ code, is available on our website.

1. To begin exporting, go to the Control or Event Display window, and choose *Export* from the File menu.
2. Select the *Text Output* radio button at the top of the window to create text files, and *Binary Output* to create binary files.
3. Select the fields you want included in the export file. Click on a field in the *Available Fields* box, and then click *Add* to add the field to the list of Displayed Fields. Note: When exporting to binary output, Decimal, Char/Event Name, Hexadecimal and Octal are the same. You only need to choose one.
The *Example* box at the bottom of the window will show you what fields you have added and how they will look in the export file. The *Example* window uses dummy data, not actual data from your capture buffer.
4. Select a filename. The default filename for text files is `export.txt` for a capture buffer or `capture_file_name.txt` for a capture file. Similarly, default filenames for binary files end in a `.bin` extension. Underneath the file name, FTS will show you approximately how big the file will be, and what percentage of free disk space it will take up.
5. Click on the *Export* button to begin exporting. Depending on the amount of data to be exported, the export process may take some time.

By default, your export file will be saved in the My Capture Files directory. Click on the *Browse* icon  if you want to save the export file to another location.

You can choose to export the entire capture buffer or just a portion of it. If you have the Event Display window open and have selected a range in it, the Export window will automatically fill in the range for you.


Exporting and Printing Frames

The Frame Print window allows you to print framed data and the Frame Export window allows you to export it to a text file suitable for importing into a spreadsheet or database program. These windows are very similar and so will be documented together.

Frame Print/Export has a number of formatting options. Some options are available only when exporting, others only when printing. Unavailable options will be grayed out.

The example space at the bottom of the window shows how the file will look. The example window uses dummy data instead of the data from your capture file.

- To export your data, open the Frame Display window and select *Export* from the File menu
- To create a text file in an easily readable format, choose *Print* from the File menu, and select the *Send to File* option in the *Output* section.
- To print your data, open the Frame Display window and choose *Print* from the File menu.

Make your selections from the range of options (for more info on each option, click on the links below), and then choose the range to output in the Output section. You can output the entire buffer or a smaller range of frames. If exporting to file, give the file a name. By default, exported files are stored in the My Capture Files directory. Click the *Browse* icon  to select a different directory location.

FRAME EXPORT FILE FORMAT

The frame export file format is as follows, starting with the first column on the left:

Section marker By default, LSED, where L stands for Summary Label, S for Summary Data, E for Error and D for Decode. These markers can be changed in the General Formatting options.

Frame number The frame number assigned by FTS.

At this point, the columns vary depending on the section.

Summary Label - "L" marker

Label This is the same value as given in the column headers on the Summary pane of the Frame Display window. There is one label for each column.

Summary Data - "S" marker

Data For Summary Data, this is the value listed in the columns of the Summary pane. There is one value for every column given in the summary label section.

Error - "E" marker

Error Location Where the error occurred.

Error Type The type of the error (CRC, Framing, Parity, etc.)

Decode - "D" marker

Layer indent These numbers identify how far into the decode tree the field is. 0 (zero) is the top layer of the tree, 1 is one indentation to the right from the top layer, 2 is two indentations in from the top layer, etc.

Protocol Field The protocol name or protocol field name.

Field Value The value of the protocol field, if present.

Start of Field Offset [optional] The offset to the start of the field expressed in logical or physical bits.

Field Length [optional] The length of the field expressed in logical or physical bits.

Field Data [optional] The data bytes containing the field value.

DECODE SECTION

Choose *All layers* to output the decode for all layers present in the frame.

Choose *Selected layers only* if you want to output the decode for one or more specific layers and don't care about any other layers that may be present. Click the radio button for Selected layers only and then click each layer you want to include in the list box.

Choose *No decode section* if you don't want any decode information to be output.

Decode Formatting

Formatting options for the Decode section are the number of data bytes to display for each frame, and the number of data bytes per line. Decode formatting options are used only when printing, and not when exporting to file.

DECODE SECTION - DATA DISPLAY

Append field linking info will include the start of each field as an offset from the start of the frame and its length in bits to the end of each line of the decode. The offset can be expressed in logical bits or physical bits (this may be the same depending on the protocol stack.)

Append field data bytes (available only when exporting) will include the data bytes for each layer of the decode at the end of the line. Change the radix used to represent the data in the Byte Display Radix box.

Show physical frame (available only when printing) will include all the physical data bytes for the frame at the start of the frame.

Show per-layer logical frame (available only when printing) will include the logical data bytes for each protocol layer in the decode.

ERROR SECTION

Check *Per-frame error section* to include error information on each frame.

Check *Show even if there are no errors* to include the error section even if no errors are present (available only when printing).

GENERAL SECTION

Begin with a file description - includes the capture file name at the start of the printout. This option is available only when printing.

Begin with all summary headers - includes the summary section header labels for every protocol at the start of the output.

General Formatting

General formatting includes the field separator, line width and page height (used only when printing), and the marker to use for the summary header, summary data, errors and decode sections (used only when exporting).

SUMMARY SECTION

First choose how many summary layers to include using the radio buttons. Choose All Layers means that the output will have a summary line for every protocol present in the frame. Visible Layer Only means that only the summary line currently selected in the Frame Display window will

be included in the output, while No Summary Section means that no summary information will be included.

Check *Per-frame header label* section to include the header line from the summary pane above each frame.

Check *Align Columns* to align the summary columns (available only when printing).

Summary Formatting

The formatting option for the Summary section is the column width, used only when printing.

Exporting Events

EXPORT FIELDS

Available fields are:

Byte Number	number of the data byte
Decimal	decimal value of the data byte
Char/Event Name	character value of data bytes, or name of non-data bytes
Errors	includes any errors associated with bytes
Event Number	number of the event (see Event Numbering for why Byte Number and Event Number may be different)
Frame Number	number of the frame the event is in
Hexadecimal	hexadecimal value of the data byte
Octal	octal value of the data byte
Side	shows which side the data byte originated from (valid only for serial data)
Signals	gives the state of the control signals (valid only for serial data)
Timestamp	shows the timestamp of the event
Type	shows whether event was Data or a Special Event (anything other than a data byte)

Note: When exporting to binary output, Decimal, Char/Event Name, Hexadecimal and Octal are the same. You only need to choose one.

EXPORT FILTER OUT

You can filter out data you don't want or need in your text file.

(This option is available only for serial data.) In the *Filter Out* box, choose which side to filter out: the DTE data, the DCE data or neither side (don't filter any data.) For example, if you choose the radio button for DTE data, the DTE data would be filtered out of your export file and the file would contain only the DCE data.

You can also filter out Special Events (which is everything that is not a data byte, such as control signal changes and Set I/O events), Nonprintable characters or both. If you choose to filter out Special Events, your export file would contain only the data bytes. Filtering out the nonprintable characters means that your export file would contain only special events and data bytes classified as printable. In ASCII, printable characters are those with hex values between \$20 and \$7e.

OTHER EXPORT OPTIONS

Use Footer

This option is valid only when doing a binary export. If you are exporting a capture file for the purpose of retransmitting

	the data, uncheck this box. If you will be manipulating the data using the sample export program, check this box. If the data is exported without the footer, the sample export program will not be able to read the export file.
Use Abbreviated Event Names	Check this box to abbreviate the names of the Special Events. This is useful to conserve space in the text file.
Separate Records with CR/LF	Specifies whether to separate each record with a carriage return/line feed. If this option is unchecked, the data will be output as a continuous stream.
Align Columns	Check this box to have the columns be left-justified.
Put Fields in Double Quotes	Check this box to put double quotes around the data in each field.
Output Header	Includes a header at the top of the file with the date and time the file was exported, name of the original capture file or capture buffer, and the event numbers and timestamps for the range exported.
Output Field Name Record	Includes a record at the top of the file with the field names.
Align Field Names with Data	Aligns the field name column with the data columns.
Timestamp Format	Sets the timestamp format. Native format is the month/day/year plus hour:minute:second:millisecond AM/PM in twelve hour format. For other formats, "D" stands for day, "H" stands for hour, "M" stands for minute, "S" stands for second and "m" stands for millisecond.
Character Set	Choose ASCII, EBCDIC or Baudot. (See note on exporting Baudot.)
Signals Characters	Defines how control signal states are indicated. Choose from 1/0, T/F, or X/space. "X", "1" and "T" indicate an "on" or "high" signal state.
Errors Characters	Defines how error conditions are indicated. Choose from 1/0, T/F, or X/space. "X", "1" and "T" indicate that an error occurred.
Field Delimiter	Defines how the fields will be separated. Choices are None (no delimiter will be used), Comma, Tab, Space, Bar and Semicolon. If a delimiter is chosen, FTS will include the delimiter between each field in the export file.

EXPORTING BAUDOT

When exporting Baudot, you need to be able to determine the state of the shift character. In a text export, the state of the shift bit can be determined by the data in the Character field. When letters is active, the character field will show letters and vice versa.

Templates

EXPORT TEMPLATES

Once you've set up an export format, you can save all your options as a template and use it for future exports.

- To create a template, set up all the options on the export window exactly as you want them to be in the template.
- Type a name in the Apply Template box, and click Save Template.
- To retrieve your template, click on the down arrow next to the Apply Template box, and choose your template from the list.

To delete a template, choose the template in the *Apply Template* box, and click the *Delete Template* button. There are several templates supplied with FTS that cannot be deleted.

Loading and Importing Capture Files

Loading a Capture File

1. From the Control Window, go to the *File* menu.
2. Choose a file from the recently used file list, or choose *Open* to load a new file.
3. Capture files have a .cfa extension. Browse if necessary to find your capture file. Click on your file, and then click *Open*.

Importing Capture Files

1. From the Control Window, go to the *File* menu.
2. Choose a file from the recently used file list, or choose *Open* to load a new file.
3. Change the *Files of Type* box to All Importable File Types or All Supported File Types. Select the file and click *Open*.

FTS will automatically convert the file to FTS format while keeping the original file in its original format. You can save the file in FTS format, close the file without saving it in FTS format, or have FTS automatically save the file in FTS format (see the System Settings to set this option.) All of these options will keep your original file untouched.

When you first open the file, FTS will bring up the Protocol Stack window and ask you what protocol decodes, if any, you want to use. You must choose a protocol decode at this point for FTS to decode the data in the file. If you open a file without using any decodes, and decide later that you want to apply a decode, choose Reframe from the File menu on the Control window.

At present, FTS supports the following file types:

Frontline Serialtest® Async and Serialtest ComProbe for DOS – requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps)

Greenleaf ViewComm® 3.0 for DOS - requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps)

Frontline Ethertest® for DOS – requires 3 files: filename.cap, filename.ca0 and filename.ca1.

Sniffer Type 1 – supports files with the .enc extension. Does not support Sniffer files with a .cap extension

Snoop or Sun Snoop – files with a .cap extension based on RFC 1761. For file format, see <http://www.faqs.org/rfcs/rfc1761.html>.

Shomiti Surveyor files in Snoop format – files with a .cap extension. For file format, see <http://www.shomiti.com/support/TNCapFileFormat.htm>.

Importing Timestamps

Serialtest for DOS uses a timebase of Pacific Standard Time during non daylight savings time hours and Pacific Daylight Time during daylight savings time hours. FTS always uses Greenwich Mean Time (also known as Universal Time Coordinates.)

When importing a Serialtest for DOS file, FTS must determine if the file was recorded during daylight savings time or not before converting the timestamps. Because the rules for determining this can change, it is possible for FTS to convert the timestamps incorrectly, resulting in timestamps that are off by one hour.

System Settings and Program Options

System Settings

Open the System Settings window by choosing *System Settings* from the Options menu on the Control window. To enable a setting, click in the box next to the setting to place a checkmark in the box. To disable a setting, click in the box to remove the checkmark. When viewing a capture file, settings related to data capture are grayed out.

Common Options

Wrap Buffer When enabled, FTS will wrap the buffer when it becomes full. The oldest events will be moved out of the buffer to make room for new events. Any events moved out of the buffer will be lost. This option also applies to capture files. When disabled, FTS will pause capture when the buffer becomes full. Either reset the buffer or close your capture file to continue.

Timestamping Options Opens the Timestamping Options window. Options include enabling or disabling timestamping and choosing capture and display resolutions.

Automatically Save Imported Capture Files in FTS Format When enabled, FTS will automatically save imported capture files in the FTS capture file format. See Loading Imported Files for more information.

Start up Opens the Start up Options window. Start up options let you choose whether to start data capture immediately on opening FTS.

Advanced Opens the Advanced System Options window. The Advanced Settings should only be changed on advice of technical support.

Buffer/File Tuning Options

Capture Buffer Size (in K) Enter the maximum size of the capture buffer (data captured in memory). If you enter a number larger than the maximum allowable size, FTS will warn you and automatically set the size to the maximum allowable size.

File Size (in K) Enter the maximum size of the capture file. If you enter a number larger than the maximum allowable size, FTS will warn you and automatically set the size to the maximum allowable size.

Note: In both cases, FTS does not actually use 100% of available memory or disk space. By default, FTS will limit the maximum size of the buffer or file to 50% of the available resources. We strongly recommend not changing this percentage unless absolutely necessary. If you do need to use more resources, you can change the maximum percentage used in the Advanced Options window. Click on the *Advanced* button on the System Settings window. If you want to change the maximum percentage for the buffer, find the setting for *Max Percent of Available Virtual Memory Used for Capture Buffer*. If you want to change the maximum percentage for the file, find the setting for *Max Percent of Free Disk Space for Capture File*. Both of these settings are expressed as a percentage.

We strongly recommend not setting these options to 100%, as this will take all your system resources, leaving none for any other application.

Advanced System Options

These parameters affect fundamental aspects of the software, and it is unlikely that you will ever have to change them. If you do change them and need to return them to their original values, the default value is listed in parentheses to the right of the value box. Most technical support problems are not related to these parameters, and as changing them could have serious consequences for the performance of FTS, we strongly recommend contacting technical support before changing any of these parameters.

To access the Advanced System Options, go to the Control window, and choose *System Settings* from the Options menu. On the System Settings window, click the *Advanced* button.

Max Percent Of Free Disk Space for Capture File

This setting determines what percentage of free hard drive space can be used for the capture file. By default, FTS will limit the maximum size of the capture file to 50% of the available space on the hard drive. If you need to create a larger capture file than the current settings allow, increase this percentage. Then go back to the System Settings window and increase the maximum file size.

Max Percent Of Available Virtual Memory Used for Capture Buffer

This setting determines what percentage of available virtual memory can be used for the capture buffer. By default, FTS will limit the maximum size of the buffer to 50% of the available virtual memory. Increasing this percentage will give you a larger capture buffer, but will leave less virtual memory available for other applications.

Driver Receive Buffer Size in Operating System Pages

This is the size of the buffer used by the driver to store incoming data. This value is expressed in operating system pages. In Windows 95, an operating system page is 4K.

Driver Action Queue Size In Operating System Pages

This is the size of the buffer used by the driver to store data to be transmitted. This value is expressed in operating system pages. In Windows 95, an operating system page is 4K.

Capture Buffer Read Cache Size In Kbytes

Sets the size of the capture buffer cache. This setting is important when reading data. A larger buffer may mean faster read times.

Capture File Write-Through Cache Size In Pages

Sets the size of the capture buffer write cache. This setting is important when writing data to disk.

Return Unused Space in Capture File When Closing (Yes/No answer)

When FTS opens a capture file, it allocates as much disk space as it needs for the maximum capture file size. When the capture file is closed, FTS gives back any unused space. This process can take some time if the maximum capture file size is large. This setting is the threshold that determines if we give back unused space when the file is closed. The default value of "checked" means that FTS will always give back unused space. If unchecked, FTS will not return unused space, which may result in very large, mostly empty capture files.

Maximum Number of Bytes Decoded Per Frame

This is the largest frame size that FTS will attempt to decode. This is used to prevent FTS from attempting to decode very large bad frames. This number should be large enough to ensure that the largest reasonable frame is handled completely.

Maximum Number of Bytes Used to Store Supplementary Capture File Information

Sets the amount of space used to store supplementary information in the capture file. The default value is 100000 bytes.

Capture Buffer System Page Size Multiplier

Data in a capture file is indexed by pages to allow for faster retrieval. The page size multiplier determines how often the file is indexed. The default value of 1 means that the capture file is indexed once every page, or once every 4K.

Non-Realtime Event Queue Size

This is the queue for all non-realtime events.

Companion File Max Size Multiplier

Protocol information is stored in a companion file. The amount of data to be stored may be more or less than the amount of data in the capture file. The companion file size multiplier specifies how large the companion file should be in relation to the capture file. A multiplier of two means that the amount of space allocated for the companion file will be twice the size of the capture file.

Changing Default File Locations

FTS puts user files in specific locations by default. Capture files are placed in the My Capture Files directory and configurations are put in My Configurations. Follow the steps below to change the default locations.

1. Choose *Directories* from the Options menu on the Control window to open the File Locations window.
2. Select the default location you wish to change.
3. Click *Modify*.
4. Browse to a new location. Click *OK*.
5. Click *OK* when finished.

Start Up Options

To open this window

Choose *System Settings* from the Options menu on the Control window. On the System Settings window, click the *Start Up* button.

Choose one of the options to determine if FTS starts data capture immediately on starting up or not.

Don't start capturing immediately.

This is the default setting. FTS begins monitoring data but does not begin capturing data until the *Start Capture to Buffer* or *Start Capture to Disk* icons on the Control, Event Display or Frame Display windows are clicked.

Start capturing to buffer immediately.

When FTS starts up, it will immediately begin data capture to the buffer. This is the equivalent of clicking the *Start Capture to Buffer* icon.

Start capturing to a unique file immediately.

When FTS starts up, it will immediately open a capture file and begin data capture to it. This is the equivalent of clicking the *Start Capture to Disk* icon.

Prompt for a filename, then immediately start capturing.

FTS will ask for a filename, then open a capture file with that name and begin capturing to it.

Start capturing immediately to the following file:

Enter a filename in the box below this option. When FTS starts up, it will immediately begin data capture to that file. If the file already exists, the data in it will be overwritten.

Minimizing Windows

Windows can be minimized individually or as a group when the Control window is minimized.




To minimize windows as a group, go to the Window menu on the Control window, and select *Minimize Control Minimizes All*. FTS will put a check next to the menu item, indicating that when the Control window is minimized, all windows will minimize. Select the menu item again to deactivate this feature.

Windows minimize to the top of the Task Bar.




Timestamping Options

The Timestamping Options window lets you enable or disable timestamping, and change the resolution of the timestamps for both capture and display purposes.




To open this window

Choose *System Settings* from the Options menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Frame Display  window.

ENABLING/DISABLING TIMESTAMPING

1. Choose *System Settings* from the Options menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Frame Display  window.
2. Check the *Store Timestamps* box to enable timestamping. Remove the check to disable timestamping. If you disable timestamping, you will not be able to do delta or rate calculations.

SWITCHING BETWEEN RELATIVE AND ABSOLUTE TIME




1. Choose *System Settings* from the Options menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Frame Display  window.
2. Go to the *Display Options* section at the bottom of the window and find the *Display Relative Timestamps* checkbox.

-
3. Check the box to switch the display to relative timestamps. Remove the check to return to absolute timestamps.

Display Relative Timestamps will show the timestamp as the amount of time that has passed since the first byte was captured. It works just like a stop watch in that the timestamp for the first byte is 0:00:00.0000 and all subsequent timestamps increment from there. The timestamp is recorded as the actual time, so you can flip back and forth between relative and actual time as needed.

The options in this section affect only how the timestamps are displayed on the screen, not how the timestamps are recorded in the capture file.

CHANGING THE TIMESTAMPING RESOLUTION




1. Choose *System Settings* from the Options menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Frame Display  window.
2. Go to the *Capture Options* section of the window.
3. Change the resolution listed in the *Storage Resolution* box. Note that if you change the resolution, you will need to exit FTS and restart in order for the change to take effect.

This option affects the resolution of the timestamp stored in the capture buffer or capture file. The default timestamp is 10 milliseconds for Windows NT and Windows 2000 and 1 millisecond for Windows 95/98. These values are determined by the operating system and are the smallest "normal" resolutions possible for each operating system.

It is also possible to use "high resolution" timestamping. High resolution timestamp values are marked as high resolution in the drop down list. Note that high resolution timestamping may not be available on all Windows 9x systems.

Performance and Capture File Issues when using high resolution timestamps

DISPLAYING FRACTIONS OF A SECOND

1. Choose *System Settings* from the Options menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon  from either the Event Display  or Frame Display  window.
2. Go to the *Display Options* section at the bottom of the window, and find the *Number of Digits to Display* box.
3. Click on the arrows to change the number. You can display between 0 and 6 digits to the right of the decimal point.

The options in this section affect only how the timestamps are displayed on the screen, not the resolution used to capture the data.

Technical Information

The following information is provided to assist you with troubleshooting problems with FTS.

Performance Notes

As a software-based product, the speed of your computer's processor affects FTS's performance. Receive overrun, frames missed and buffer overflow errors are indicators that FTS is unable to keep up with the data. The information below describes what happens to the data as it arrives at the network card, what the types of errors mean, and how various aspects of FTS affect performance. Also included are suggestions on how to improve performance.

Data captured by the network card first goes into the card's buffer. The card generates an interrupt, which tells the NDIS driver to check the port. The FTS driver takes the data from the NDIS driver and counts each byte as they are put into the FTS driver's buffer. The FTS driver tells the FTS user interface that data is ready to be processed. FTS takes the data from the driver's buffer and puts the data into the capture buffer.

Receive overruns occur when the frame buffer on the network card is not emptied by the NDIS driver. Frames Missed, No Buffer errors occur when the FTS driver does not clear out the NDIS driver buffer. In both of these situations, FTS knows that it has lost data, but does not know how much.

Driver Buffer Overflows occur when the FTS user interface does not retrieve frames from the FTS driver quickly enough. The Frames Lost counter on the Statistics window displays the number of frames lost due to driver buffer overflows. Since the driver counts the frames as it retrieves them from the NDIS driver, it not only knows that it has lost data, it also knows how much. Buffer overflows are indicated in the Event Display window by a plus sign within a circle. Clicking on the buffer overflow symbol will show how many frames have been lost. The Statistics window is a good place to check for buffer overflow errors.

All 3 types of errors indicate that data is coming in too quickly for FTS to process. There are several things that you can do to try and solve this problem.

1. Use capture filters to filter out data you don't need to see. Capture filters reduce the amount of data processed by FTS.
2. Close all other programs that are doing work while FTS is running. Refrain from doing searches in the Event Display window or other processor intensive activities while FTS is capturing data.
3. Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the buffer or file. Try turning off timestamping from the Timestamping Options window.
4. Capture to the buffer instead of capturing to disk. Writing data to the buffer is faster than writing to disk, allowing more time for capturing data. This works best when used in conjunction with a capture filter to limit the amount of data kept in the buffer.
5. For Driver Buffer Overflows, change the size of the driver buffer. This value is changed from the Advanced System Settings. Go to the Control Window and choose System Settings from the Options menu. Click on the Advanced button. Find the value *Driver Receive Buffer Size in Operating System Pages*. Take the number listed there and double it.

-
6. For Frames Missed, No Buffer errors, change the number of NDIS buffers. To do this, choose Hardware Settings from the Options menu on the Control window, and double the value listed in *Number of NDIS buffers to use*.
 7. FTS's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause FTS to lose data while the window is being updated. Some windows require more processing time than others because the information being displayed in them is constantly changing. Refrain from displaying data live in the Event Display and Frame Display windows. Try closing the Statistics windows. FTS can capture data with no windows other than the Control window open.
 8. If you are still experiencing receive overruns, frames missed errors and/or buffer overflows after trying all of the above options, then you will need to use a faster PC.

Performance Issues For High Resolution Timestamps

There are two things to be aware of when using high resolution timestamps. The first is that high resolution timestamps take up more space in the capture file because more bits are required to store the timestamp. Also, more timestamps need to be stored than at normal resolutions.

For example, if 10 bytes of data are captured in 10 milliseconds at a rate of 1 byte per millisecond, and the timestamp resolution is 10 milliseconds, then only one timestamp needs to be stored for the 10 bytes of data. If the resolution is 1 millisecond, then 10 timestamps will need to be stored, one for each byte of data. If you have two capture files, both of the same size, but one was captured using normal resolution timestamping and the other using high resolution, the normal resolution file will have more data events in it, because less room was used to store timestamps.

You can increase the size of your capture buffer or file in the System Settings.

The second issue is that using high resolution timestamping may affect performance on slower machines. Under Windows NT, FTS makes a system call to `KeQueryPerformanceCounter` to implement high resolution timestamping. The equivalent call in Windows 9x is `VTD_Get_Real_Time`. The note below is from Microsoft's Device Driver Kit (DDK) for Windows NT, but the same concept applies to Windows 9x.

Use this routine sparingly, calling it as infrequently as possible. Depending on the platform, **KeQueryPerformanceCounter** can disable system-wide interrupts for a minimal interval. Consequently, calling this routine frequently or repeatedly, as in an iteration, defeats its purpose of returning very fine-grained, running time-stamp information. Calling this routine too frequently can degrade I/O performance for the calling driver and for the system as a whole.

However, this note was written several years ago, and it does not define what is meant by frequently. No changes in performance have been noted in our tests as a result of using high resolution timestamping, but if you experience performance problems, try using a normal resolution for your timestamps.

Clock Drift

FTS uses a system call provided by Microsoft to determine the number of times that the PC's clock ticks per second. However, we have noticed that on the same machine, the number of clock ticks is different under Windows 9x than under Windows NT. On the system where we discovered this, the "tick delta" yields a clock drift between the two operating systems of 1 second every 11 days.

Padding of Short Frames

Ethernet requires that frames be a minimum of 60 bytes in length, not including the CRC. If the frame is less than 60 bytes, the NIC pads it before putting it on the wire. Pad characters are usually nulls (hex 00).

Frames transmitted by the PC running FTS are looped back by the NDIS driver so the transmitting PC can see the frame. The loopback occurs before the NIC has added any necessary padding to the end of the frame. FTS compensates for this by using the sequence "Pad", repeated as many times as necessary, as a placeholder. FTS uses only as many characters as needed to bring the frame up to the required 60 bytes, so you may see partial "Pad"s or multiple "Pad"s. For example, you may see "PadPadPad", "PadPa" "Pa", etc.

CRC!

When NDIS receives a frame, it checks that the CRC is good and then discards it before passing the frame up to the next higher layer. FTS adds "CRC!" to the end of Ethernet frames to compensate.

NDIS does not pass up frames with bad CRCs, so there is no way for FTS to capture them. Some (but not all) NDIS drivers record the number of frames received with bad CRCs. The number of CRC errors is shown in the Errors table on the Statistics window.

To manually determine the CRC for a frame, use the CRC function on the Event Display.

Useful Tables

ASCII CODES

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2x	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7x	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL

BAUDOT CODES

DEC	HEX	LETTERS	FIGURES
0	00	BLANK (NUL)	BLANK (NUL)
1	01	E	3
2	02	LF	LF
3	03	A	-
4	04	SP	SP
5	05	S	BEL
6	06	I	8
7	07	U	7
8	08	CR	CR
9	09	D	\$
10	0A	R	4
11	0B	J	'
12	0C	N	,
13	0D	F	!
14	0E	C	:
15	0F	K	(
16	10	T	5
17	11	Z	"
18	12	L)
19	13	W	2
20	14	H	#
21	15	Y	6
22	16	P	0
23	17	Q	1
24	18	O	9
25	19	B	?
26	1A	G	&
27	1B	FIGURES	FIGURES
28	1C	M	.
29	1D	X	/
30	1E	V	;
31	1F	LETTERS	LETTERS

EBCDIC CODES

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	PF	HT	LC	DEL			SMM	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	TM	RES	NL	BS	IL	CAN	EM	CC	CU1	IFS	IGS	IRS	IUS
2x	DS	SOS	FS		BYP	LF	ETB	ESC			SM	CU2		ENQ	ACK	BEL
3x			SYN		PN	RS	UC	EOT				CU3	DC4	NAK		SUB
4x	SP											.	<	(+	
5x	&										!	\$	*)	;	^
6x	-	/										,	%	_	>	?
7x									`	:	#	@	'	=	"	
8x		a	b	c	d	e	f	g	h	i						
9x		j	k	l	m	n	o	p	q	r						
Ax		~	s	t	u	v	w	x	y	z				[
Bx]		
Cx	{	A	B	C	D	E	F	G	H	I						
Dx	}	J	K	L	M	N	O	P	Q	R						
Ex	\		S	T	U	V	W	X	Y	Z						
Fx	0	1	2	3	4	5	6	7	8	9						

COMMUNICATION CONTROL CHARACTERS

Listed below in alphabetical order are the expanded text meanings for common ANSI communication control characters, and FTS's two-character abbreviation for each one. Some abbreviations have forward slash characters between the two letters. This is to differentiate the abbreviations for a control character from a hex number. For example, the abbreviation for Form Feed is listed as F/F, to differentiate it from the hex number FF.

Abbreviation	Control Character	Text
AK	ACK	Acknowledge
BL	BEL	Bell
BS	BS	Backspace
CN	CAN	Cancel
CR	CR	Carriage Return
D/1-4	DC1-4	Device Control 1-4
D/E	DEL	Delete
DL	DLE	Data Link Escape
EM	EM	End of Medium
EQ	ENQ	Enquiry
ET	EOT	End of Transmission
E/C	ESC	Escape
E/B	ETB	End of Transmission Block
EX	ETX	End of Text
F/F	FF	Form Feed
FS	FS	File Separator
GS	GS	Group Separator
HT	HT	Horizontal Tabulation
LF	LF	Line Feed
NK	NAK	Negative Acknowledge
NU	NUL	Null
RS	RS	Record Separator
SI	SI	Shift In
SO	SO	Shift Out
SH	SOH	Start of Heading

SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle
US	US	Unit Separator
VT	VT	Vertical Tabulation

BPF Copyright Notice

This copyright applies to code used in the filter feature. Filtering functionality in FTS is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump.

Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997
The Regents of the University of California. All rights reserved.

This code is derived from the Stanford/CMU enet packet filter, (net/enet.c) distributed as part of 4.3BSD, and code contributed to Berkeley by Steven McCanne and Van Jacobson both of Lawrence Berkeley Laboratory.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

Buffer Wrapping

When the capture buffer becomes full, the oldest events captured are pushed out of the buffer to make room for new events. This is called buffer wrapping, and events are referred to as having been "wrapped" out of the buffer. Any events wrapped out of the buffer are lost and cannot be recovered. Capture files also wrap when they become full. Turn wrap off in the System Settings.

Capture Buffer

FTS can capture data either to memory or to a file on disk. The capture buffer is where FTS stores data in memory. Capturing data to memory is faster than capturing to disk, but capture buffers tend to be smaller than files simply because there is usually more disk space than memory on most computers. Also, data captured to buffer will be lost if not saved to a file before FTS is exited.

Event

An event is anything that happens on the circuit or which affects data capture. Data bytes, control signal changes, and long and short breaks are all events, as are Set I/O Configuration changes and Data Capture Paused and Resumed. See List of All Event Symbols for a list of all the special events shown in FTS and what they mean.

Frame Recognizer

The frame recognizer is the portion of the software that "recognizes" when a frame begins and when it ends. The frame recognizer inserts special markers in the capture file whenever it sees a Start of Frame or End of Frame byte sequence, and these markers allow the protocol decodes to correctly identify the frames. Data is run through the frame recognizer at the time it is captured and only if a protocol that frames data has been selected. In some cases it is possible to frame unframed data after it has been captured.

Frame Transformation

Frame transformation is the process of adding, removing or altering the physical bytes in a frame as necessary to get the frame into a state where it can be decoded. For example, in Async PPP, frame transformation removes escape characters and alters the next byte appropriately. In frames carrying Van Jacobsen Compression (VJC), frame transformation reconstructs the IP header so that it may be decoded properly. The end result of frame transformation is the logical frame.

Logical Frame

The data in a frame after it has been transformed. The logical frame is displayed on the Frame Display window Logical Data panes, and is used when applying display filters. Usually the logical and the physical frames are the same. Cases where they are not include frames with escape characters or compressed headers.

NIC - Network Interface Controller

NIC stands for Network Interface Controller. This is the physical interface between a PC and an Ethernet network.

Physical Frame

The data in a frame before it has been transformed. The physical frame is displayed on the Frame Display window Event Data pane and in the Event Display window, and is used when applying capture filters. Usually the logical and the physical frames are the same. Cases where they are not include frames with escape characters or compressed headers.

Radix

The base of a number system. Binary is base 2, octal is base 8, decimal is base 10 and hexadecimal is base 16.

Index

\$

\$ Hex Character in Searching: 37

&

& Binary Character in Searching: 37

?

? Wildcard Character in Searching: 38

^

^ Control Character in Searching: 38

A

Absolute Time Search: 38

Absolute Timestamp Search: 38

Absolute Timestamps: 63

Adding a New Predefined Stack 12

Advanced System Settings: 61

Aggregate Graphs: 19

Alignment Error: 19

Apply Capture Filter: 42

Apply Display Filter: 43

Arrow Symbol: 33

ASCII

 character set 67

 removing the numbers on the Event Display 33

 searching for ASCII strings 37

 viewing data in 33

ASCII Pane: 26

ASCII: 33, 37, 67

Automatically Save Imported Capture Files in FTS Format: 60

Auto-Sizing Column Widths: 25

Auto-traversal 12

B

Bar Charts: 19

Baudot

 character set 68

 exporting 57

 removing the numbers on the Event Display 33

 viewing data in 33

Baudot: 33, 68

Binary

 removing the characters on the Event Display 33

 searching for 37

 viewing data in binary 33

Binary Export: 53

Binary Pane: 26

Binary: 33, 37

Blue Dots in Summary Pane: 25

<hr/>	
BPF Filter	
copyright notice	70
filter string definition	46
BPF Filter:	41, 46, 70
BPF Format:	44
Buffer	
changing capture buffer size	60
data capture to	15
saving a portion of	50
wrap setting	60
Buffer Information Table:	17, 19
Buffer Tab:	17
Buffer:	15, 50, 60
Byte Colors:	29
Byte Errors:	28
Byte Number Export Field:	56
Bytes	
calculating CRC for	31
go to byte number	36
numbers	35
show bytes in frames	27
switching number sets	33
Bytes Per Second Table:	17
Bytes:	27, 31, 33, 35
C	
Calculating Data Rates:	32
Calculating Delta Times:	32
Capture Buffer	
advanced settings	61
capturing data to	15
changing size of	60
saving a portion of the buffer to file	50
saving to file	50
turn off clear buffer warning	16
Capture Buffer Size:	60
Capture Buffer:	15, 50, 60, 61
Capture File	
data capture to	16
Capture File:	16
Capture Files	
auto-save imported files in FTS format	60
changing default location of	62
changing max size of	60
changing maximum size of	61
export to a binary format	53
export to text format	53
framing captured data	13
importing DOS timestamps	59
loading	59
loading Serialtest for DOS files	59
reframing	13
removing framing markers	13
saving a portion of a file to another file	50
Capture Files:	50, 53, 59, 60, 61, 62
Capture Filters	

applying	42
difference between capture and display	40
remove	43
Capture Filters:	40, 42, 43
Capture Status:	15
Capture to Buffer:	15
Capture To File:	16
Changing Default File Locations:	62
Char/Event Name Export Field:	56
Character	
control character abbreviations	69
searching for	37
Character Pane:	26
Character Set	
ASCII	67
Baudot	68
EBCDIC	69
removing the numbers on the Event Display	33
setting for export files	56
switching in the Event Display	33
Character Set:	33, 56, 67, 68, 69
Character Strings in Searching:	37
Character:	37
Chars/Sec Table:	17
Charts:	19
Clear Capture Buffer Warning:	16
Clock Drift:	66
Color of Data Bytes:	29
Colors:	29
Column Width:	25
Communication Control Character Abbreviations:	69
Conditions	
conversation	40
custom filter strings	41
deleting	42
modifying	42
naming condition sets	43
node	40
offset	41
open filter file	44
pattern	41
protocol	41
saving	44
Conditions:	40, 41, 42, 43, 44
Configuration	
export templates	58
Configuration Info on Control Window:	15
Configuration:	58
Control Character Abbreviations:	69
Control Characters	
searching for	38
Control Characters:	38
Control Signal Symbols:	33
Control Signals	
setting export format for	56
signals export field	56

<hr/>	
Control Window	
minimizing.....	63
status information on.....	15
System Settings.....	60
toolbar.....	14
Control Window:	14, 15, 60, 63
Conversation Filters:	40
Converting Files to FTS Format:	59
Copying Statistics to Clipboard:	20
CRC	
seed value.....	31
CRC Calculation:	31
CRC Error:	19
CRC!:	31, 67
CRC:	31
Create Conversation Filter:	40
Create Custom Filter	
tcpdump string format.....	44
Create Custom Filter:	41, 44
Create Custom Protocol Stack.....	12
Create Node Filter:	40
Create Offset Filter:	41
Create Pattern Filter:	41
Create Protocol Filter:	41
Custom Filter	
tcpdump string format.....	44
Custom Filter:	41, 44
Custom Protocol Stack.....	12
Custom Protocol Stack Setup.....	12
Customizing Fields in the Summary Pane:	25
 D	
D/1.....	69
D/2.....	69
D/3.....	69
D/4.....	69
D/E.....	69
data.....	69
Data	
calculating data rates.....	32
exporting to generic format.....	53
filtering out data when exporting.....	56
filtering with capture filter.....	42
go to byte number.....	36
printing.....	51
reframing.....	13
removing framing markers.....	13
saving.....	50
saving the capture buffer.....	50
switching number sets.....	33
Data Capture	
capture to buffer.....	15
capture to file.....	16
filters.....	42, 43
when to start capture.....	62
Data Capture:	15, 16, 42, 62

Data Rates:	32
Data Table:	17, 18
Data:	13, 32, 33, 36, 42, 50, 51
datadestination	69
Datadestination	69
DCE Data	
filtering out of an export file	56
DCE Data:	56
Decimal	
decimal export field	56
removing the characters on the Event Display	33
viewing data in	33
Decimal:	33, 56
Decode	69
Decode Formatting	55
Decode Pane:	25
Decodes	
searching for strings	37
viewing protocol decodes	22, 25
Decodes:	22, 25, 37
Default File Locations:	62
Define Conversation Filter:	40
Define Custom Filter:	41
Define Node Filter:	40
Define Offset Filter:	41
Define Pattern Filter:	41
Define Protocol Filter:	41
Delete Conditions:	42
Delta Times:	32
Directories:	62
Display Filters	
applying	43
difference between capture and display	40
remove	43
Display Filters:	40, 43
Displaying Named Filters:	44
Dots:	25
Double Arrow Symbol:	33
DTE Data	
filtering out of an export file	56
DTE Data:	56
Duplicate View	
Event Display	31
Frame Display	28
Duplicate View:	28, 30, 31
E	
E/B	69
E/C	69
EBCDIC	
character set	69
removing the numbers on the Event Display	33
searching for EBCDIC strings	37
viewing data in	33
EBCDIC:	33, 37, 69
Enabling/Disabling Timestamping:	63

Errors	
errors export field.....	56
red color used for	28
setting export format for	56
Errors Graph:	19
Errors Table:	17, 19
Errors:	28
Escape Character in Searching:.....	37
Ethernet Card:	11
Ethernet MAC Address Filter:	40
Ethernet MAC Address:.....	15
Ethernet Padding:.....	67
Event Display	
calculating data rates.....	32
calculating delta times.....	32
changing the default position of the selection.....	39
changing the font size	33
control character abbreviations	69
CRC	31, 32
duplicating	30
event numbers.....	35
event symbols	33
Find function.....	36
freeze/resume	32
freezing	30
opening multiple Event Displays	31
overview.....	30
printing.....	51
removing symbol characters	32
saving data	50
searching	36
switching character set.....	33
switching number set	33
synchronization with Frame Display	28
toolbar.....	30
viewing only characters	33
viewing only numbers.....	33
Event Display:.....	28, 30, 31, 32, 33, 35, 36, 39, 50, 51
Event Pane:	27
Events	
event number export field	56
filtering out of an export file	56
go to event.....	36
numbers.....	35
printing.....	51
save selection	50
saving.....	50
searching for	37
Events Info on Control Window:	15
Events:	35, 36, 37, 50, 51
Expand All/Collapse All:.....	25
Expand Decode Pane:	27
Export	
export fields	56
filtering.....	56
format options.....	56

frame export file format	54
frames	54
templates	58
Export Fields:	56
Export Records	
separating	56
Export Records:	56
Export:	53, 54
F	
F/F	69
FCS Calculation:	31
FCS Errors	
searching for	36
FCS Errors:	36
FCS:	31
Field Delimiter:	56
Field Names	
aligning with export data	56
exporting	56, 57
Field Names:	56
Field Width:	25
File	
capture data to file	16
changing capture file size	60
open filter file	44
opening a capture file	59
save filters	44
saving a portion of a capture file to another file	50
File Locations	
changing defaults	62
File Locations:	62
File Types Supported:	59
File:	16, 44, 50, 59, 60
Filter Definition:	40
Filter String Formats:	44
Filter String:	40
Filtering from the Frame Display:	28
Filters	
apply capture filter	42
conversation	41
creating	40
custom	41
deleting conditions	42
difference between capture and display	40
display filters	43
export	56
filter string definitions	46
filters and multiple Frame Displays	28
modifying conditions	42
naming	43
node	41
offset	41
open filter file	44
overview	40
pattern	41

protocol	41
removing	43
save to file	44
show filters in use	43
tcpdump	42
Filters:	28, 40, 41, 42, 43, 44, 46, 56
Find	
binary value	37
character string	37
CRC errors	36
event	37
event number	36
FCS errors	36
frame errors	36
go to frame number	36
hex value	37
how to	36
overview	36
pattern	37
special event	37
string	37
strings in decodes	37
timestamp	38
using wildcards	37
Find:	36, 37, 38
Flag Symbol:	33
Font Size	
changing	33
Font Size:	33
Fonts	
troubleshooting printing of	51
Fonts:	51
Fractions Of A Second	
changing number of digits to display	64
Fractions Of A Second:	64
Frame Check Sequence Errors	
searching for	36
Frame Check Sequence Errors:	36
Frame Display	
Binary Pane	26
changing column widths	25
changing protocol layer colors	29
Character Pane	26
color of the data bytes	29
Decode Pane	25, 26
difference between the Event Pane and other panes	29
display filters	43
duplicating	28
Event Pane	27
filtering	40
filtering from	28
Find function	36
freeze/resume	32
Hex Pane	26
Radix Pane	26
removing columns	25

saving data	50
searching	36
sorting	27
Summary Pane	24
synchronization with Event Display	28
working with panes	27
Frame Display:	22, 24, 27, 28, 29, 32, 36, 43, 50
Frame Errors	
searching for	36
Frame Errors:	28, 36
Frame Export File Format	54
Frame Export:	53
Frame Number	
Go To	36
Frame Number:	36
Frame Print/Export:	53
Frame Size Ranges:	20
Frame Sizes Graph:	19
Frame Sizes Table:	17, 18
Frame Symbols in the Summary Pane:	25
Frames	
calculating FCS	31
displaying frame information	22
frame number export field	56
go to frame number	36
numbers	35
offset filter	41
save selection	50
saving	50
searching for frame errors	36
sorting	27
Frames Per Second Table:	18
Frames/Sec Table:	17
Frames:	22, 31, 35, 36, 41, 50
Framing	
reframing data	13
removing framing markers	13
Framing:	13
Freeze	
Event Display	32
Frame Display	32
Freeze:	32
Frontline	
Technical Support	6
Frontline:	6
FTS Control:	14
FTS:	14
G	
General Formatting	55
Go To	
byte number	36
event number	36
frame number	36
timestamp	38
Go To Event:	36

Go To Frame:	36
Go To:	36, 38
Graph Options:	20
Graph Printing:	20
Graphing	
errors:	19
frame sizes	20
Graphing:	19
Graphs	
view actual value:	20
view as percentage	20
view legend	20
Graphs:	20
Green Dots in Summary Pane:	25
H	
Hardware Configuration:	11
Hardware Settings:	11
Hex	
removing the characters on the Event Display	33
searching for	37
viewing data in hex	33
Hex:	33, 37
Hexadecimal Export Field:	56
Hexadecimal Pane:	26
High resolution timestamping	
performance issues	66
High Resolution Timestamping:	64
I	
Icons in Data on Event Display:	33
Importable File Types:	59
Introduction:	6
IP Address Filter:	40
L	
Layer Colors:	29
Live Update:	32
Load Filter File:	44
Logical Bytes:	29
M	
MAC Address Filter:	40
Main Window:	14
Minimize Control Minimizes All:	63
Minimizing Windows:	63
Modify Filters:	42
Multiple Event Displays:	31
Multiple Frame Displays:	28
N	
N 69	
n/a:	17
Name Filters	
viewing a list of named filters	44
Name Filters:	43, 44

NDIS Driver:	11
Network Card:	11
NIC Padding of Short Frames:	67
NIC:	11
Node Filters:	40
Nonprintables	
filtering out of an export file	56
Nonprintables:	56
Number Set	
removing the characters on the Event Display	33
switching in the Event Display	33
Number Set:	33
Numbers:	35
O	
Octal	
octal export field	56
Octal:	56
Offset Filter:	41
Open	
2nd Event Display	31
capture file	59
files in other formats	59
Open Filter File:	44
Open:	31, 59
Options	
Advanced System Settings	61
Data Capture	62, 63
Frame Size Ranges	20
Graphs	20
Start Up	62
System	60, 61
Timestamping	63
Options:	20, 60, 62, 63
P	
Pad at End of Short Frames:	67
Panes	
closing	27
resizing	27
Panes:	27
Pattern Filter:	41
Percentages:	20
Performance Notes:	65
Physical Bytes:	29
Physical Errors:	28
Physical vs. Logical Byte Values:	29
Pie Charts:	19
Pink Dots in Summary Pane:	25
Predefined Protocol Stacks	12
adding	12
Print Preview:	51
Printing	
data	51
events	51
exporting data	53

graphs.....	20
Print Preview.....	51
troubleshooting	51
Printing:	20, 51
Protocol	
filter.....	41
searching for strings in decodes	37
Protocol Filter:	41
Protocol Stack.....	12
choosing stacks	12
creating a custom stack	12
creating a new predefined stack	12
reframing data.....	13
unframing data	13
Protocol:.....	37, 41
Protocols	12
changing layer colors	29
changing protocol stack	12
creating a custom stack	12
filtering on protocols.....	41
viewing protocol information.....	22
Protocols:	22, 29
Q	
Quick Start Guide:	7
R	
R 69	
Radix	
switching in the Event Display	33
Radix Pane:.....	26
Radix:.....	33
Red Bytes:.....	28
Reframe Function:	13
Relative Time Search:.....	38
Relative Timestamp Search:	39
Relative Timestamps:.....	63
Remove Filter:	43
Removing a Custom Stack.....	12
Removing Columns:	25
Removing Framing Markers:	13
Reports	
saving export formats.....	58
Reports:.....	58
Reset Panes:	27
Resettable Tab:	17
Resolution	
changing timestamp resolution	64
Resolution:	64
Rx Frames with Errors:	19
S	
Save	
a portion of a capture file or buffer	50
capture buffer to file.....	50
export formats	58

overview.....	50
Save Buffer Warning:.....	16
Save Filters:.....	44
Save Imported Capture Files in FTS Format:.....	60
Save Selection:.....	50
Save:.....	50
Scrolling	
how to stop automatic scrolling.....	32
Scrolling:.....	32
Search String Examples:.....	38
Searching	
by timestamp.....	38
entering character strings.....	37
event number.....	37
examples of search strings.....	38
for a binary value.....	37
for a character string.....	37
for a hex pattern.....	37
for a pattern.....	37
for a special event.....	37
for control characters.....	38
for FCS errors.....	36
for frame errors.....	36
for hex or binary characters.....	37
for strings in decodes.....	37
frame number.....	36
how to.....	36
overview.....	36
using wildcards.....	38
wildcards.....	37
Searching:.....	36, 37, 38
Seed Value:.....	31
Selection	
default position of selection on Event Display.....	39
Selection Offset:.....	39
Selection:.....	39
Session Tab:.....	17
Set Capture Filter:.....	42
Set Display Filter:.....	43
Shift Characters:.....	57
Short Frame Padding:.....	67
Show All Events:.....	32
Show All Panes:.....	27
Show Data Grid:.....	20
Show Named Filters:.....	44
Side Export Field:.....	56
Signal Symbols:.....	33
Signals Export Field:.....	56
Size	
capture buffer size.....	60
capture file size.....	60
Size:.....	60
Smiley Face Symbol:.....	33
Sniffer Files	
importing.....	59
Snoop Files.....	59

Sniffer Files:	59
Snoop Files	
importing.....	59
Snoop Files:	59
Sorting Frames:	24, 27
Stack Colors:.....	29
Start Capture To Buffer	
immediately on startup.....	62
Start Capture To Buffer:	62
Start Capture to Disk	
immediately on startup.....	62
Start Capture to Disk:.....	62
Start Up Options:	62
Statistics	
buffer tab.....	17
changing the font size	33
copying to clipboard	20
frame size ranges.....	20
freezing the display.....	17
graphing errors.....	19
graphing frame sizes	19
resetable tab	17
session tab.....	17
statistics kept.....	17
Statistics Graphs:	19
Statistics Window:	17
Statistics:	17, 20, 33
Store Timestamps:	63
String Filter Format:	44
Summary Formatting	56
Summary Pane	
changing column widths	25
removing columns.....	25
sorting	27
toolbar.....	24
Summary Pane Toolbar:	24
Summary Pane:	24
Supported File Types:.....	59
Symbols	
removing from Event Display.....	32
Symbols in Data on Event Display:	33
Symbols:	32, 33
System Options:	60
System Settings	
advanced	61
System Settings:.....	60
T	
Tcpdump	
copyright notice	70
Tcpdump Man Page:.....	46
Tcpdump String Format:.....	44
Tcpdump:	41, 70
Technical Information:.....	65
Technical Support:	6
Templates	

deleting.....	58
saving.....	58
Templates:.....	58
Text Files	
export capture files to text files.....	53
Text Files:.....	53
Time	
go to time.....	38
Time:.....	38
Timestamping	
clock drift.....	66
disabling.....	63
enabling.....	63
high resolution performance.....	66
number of digits to display.....	64
performance issues.....	66
resolution.....	64
searching by timestamp.....	38
viewing absolute timestamps.....	63
viewing relative timestamps.....	63
Timestamping Options:.....	63
Timestamping:.....	38, 63
Timestamps	
format in export files.....	56
importing from DOS.....	59
timestamp export field.....	56
Timestamps:.....	56
Toolbars	
Control Window.....	15
Event Display.....	31
Frame Display.....	23
Summary Pane.....	24
Toolbars:.....	14, 23, 24, 30
Troubleshooting	
printing problems.....	51
Troubleshooting:.....	51
Tutorial:.....	7
Tx Deferred:.....	19
Tx Frames with Errors:.....	19
Tx Heartbeat Failure:.....	19
Tx Late Collisions:.....	19
Tx Max Collisions:.....	19
Tx More Collisions:.....	19
Tx One Collision:.....	19
Tx Times CRS Lost:.....	19
Tx Underrun:.....	19
Type Export Field:.....	56
U	
Un-apply Filter:.....	43
Unfiltered Data Table:.....	18
Unframe Function:.....	13
Utilization Status:.....	15
Utilization Table:.....	17, 18

W

Wildcards:.....	37, 38
Window Refresh Rate:.....	20
Window Synchronization:	28
Windows	
minimizing.....	63
Windows:.....	63
Working with Panes in the Frame Display:	27
Wrap Buffer Setting:.....	60