# 19 Protocol Decodes

Protocol decodes can “drill down” into the protocol and application data of individual packets. You can view protocol decodes in the Tree View, Data Exchange Chart, and Tier Pair Circle.

AppTransaction Xpert Decode Module includes additional support for detailed, protocol-specific decodes as well as transactional-analysis capabilities and decodes for additional protocols (such as HTTP and Citrix).

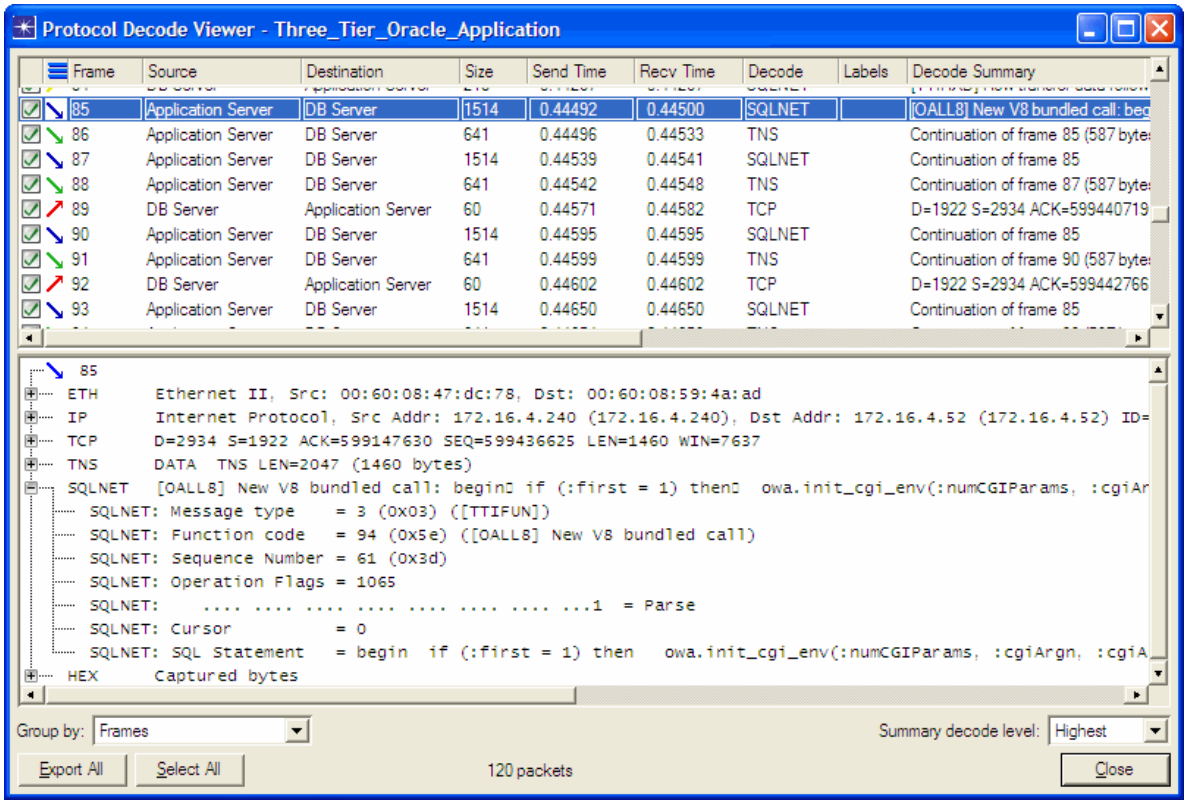
This section has the following topics:

- Protocol Decode Viewer
- Streamed Data Viewer
- Finding Packets
- AppTransaction Xpert Decode Module
- Redecoding Traffic
- Troubleshooting: Incorrectly Identified Protocols

# Protocol Decode Viewer

The Protocol Decode Viewer, shown in the following figure, displays detailed protocol decodes for one or more packets in a Transaction Analyzer model. Use this feature to view detailed decodes of the protocol fields in individual packets. You can also view the captured bytes of individual packets in both HEX and ASCII format by expanding the HEX node in the bottom treeview.

**Figure 19-1 Protocol Decode Viewer**




To view protocol decodes:

1) Select one or more packets or messages in the Tree View, Tier Pair Circle, or Data Exchange Chart.

2) Right-click on the selection and choose "Show Protocol Decodes for Selected Items".

For information about the operations in this window, see:

- Table 19-1 Protocol Decode Viewer: Main Window Options
- Table 19-2 Protocol Decode Viewer: Right-Click Menu Options

If you have a license for AppTransaction Xpert Decode Module, you can view additional data in the Protocol Decode Viewer. For more information, see AppTransaction Xpert Decode Module.

**Table 19-1 Protocol Decode Viewer: Main Window Options**

| Option | Description |
|---|---|
| Group By | Determines how the frames are organized in the treeview:<br>• Frames—All frames are organized in numerical order<br>• Connections—Selected frames are organized by connection<br>• Application Messages—Selected frames are organized by application message<br>Note that if you group by Connections or Application Messages, the treeview shows only the frames you selected to decode—not necessarily all the frames in that connection or message. |
| Export All | Exports decode data for all frames in the viewer to a text (.txt) file.<br>To export a subset, select the frames, right-click, and choose Export Selected.<br>As part of the export, specify whether to include<br>- summary lines<br>- detailed decodes |
| Expand All | Expands all top-level branches (frames, connections or messages) in the treeview. |
| Select All | Selects all frames in the viewer. |
| Summary Decode Level | Determines the protocol layer to show in the Decode and Decode Summary fields. |

The following table lists the menu operations that are available when you right-click on one or more selected frames in the Protocol Decode Viewer.

**Table 19-2 Protocol Decode Viewer: Right-Click Menu Options**

| Option | Description |
|---|---|
| Copy to Clipboard | Copy the selected information to the clipboard. If you select a sub-branch within a frame, only the corresponding decode information is copied. If you select one or more frames, all decode information for those frames is copied. |
| Exclude Others | Exclude all items *except those currently selected* from the Transaction Analyzer model. |
| Exclude Selected Items | Exclude the selected items from the Transaction Analyzer model. |
| Export Selected | Export decode information for the selected frames. This menu item appears only when you right-click on one or more selected frames. |
| Graph Statistics for Selected Items | View statistic graphs for the selected items.<br>For more information, see Viewing Statistics. |
| Permanently Delete Others | Delete all items *except those currently selected* from the Transaction Analyzer model. |
| Permanently Delete Selected Items | Delete selected items from the Transaction Analyzer model. |

**Table 19-2 Protocol Decode Viewer: Right-Click Menu Options (Continued)**

| Option | Description |
|---|---|
| Remove from Selection | Remove the selected frame(s) from the decode viewer tree. This does not remove the frames from the Transaction Analyzer model. |
| Rename <*tier_name*> | Rename the tier manually or using DNS lookup. |
| Set as Time Zero | Changes the Send Time for the selected packet to 0.00000.<br>This operation is useful when you know that this is the first packet sent in the transaction of interest, and that earlier packets are irrelevant. |
| Show Protocol Decodes for Selected Items | View the selected frames in a new Protocol Decode Viewer window. |
| Show Streamed Bytes for Selected Items | View the selected packets in the Streamed Data Viewer.<br>For more information, see Streamed Data Viewer. |
| Zoom to DEC<br>Zoom to Tree | Zoom the Data Exchange Chart or Tree View window to the selected frames. |

### *Related Topics*

- *Protocol Decodes*

# Streamed Data Viewer

The Streamed Data Viewer shows all data transferred over a particular network layer as a single concatenated stream of data. This feature is particularly useful when you want to view all application data (typically all data above TCP) transferred over a single connection or within a single application message.

To open the Streamed Data Viewer:

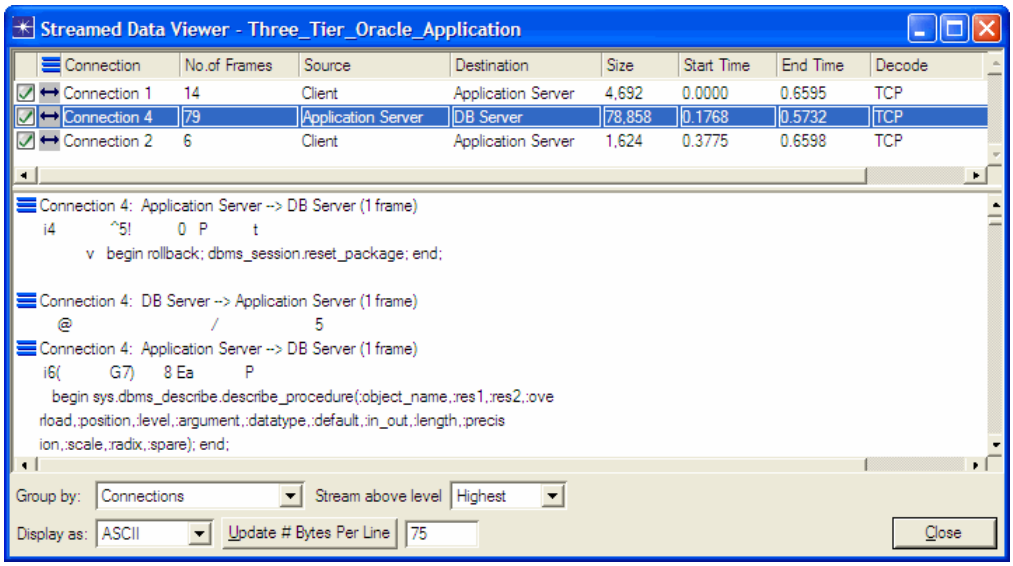
1) Select a group of packets or messages in the Protocol Viewer, Data Exchange Chart, or Tree View window.

2) Right-click and choose “Show Streamed Bytes for Selected Items”.

For information about the operations in this window, see:

- Table 19-3 Streamed Data Viewer: Main Window Options
- The right-click menu operations in the Data Stream Viewer are identical to those in the Protocol Decode Viewer; see Table 19-2 Protocol Decode Viewer: Right-Click Menu Options

**Figure 19-2 Streamed Data Viewer**



The following table lists the main window options for the Streamed Data Viewer.

**Table 19-3 Streamed Data Viewer: Main Window Options**

| Option | Description |
|---|---|
| Display As | Displays the streamed data in ASCII, Hexadecimal, or EBCDIC format |
| Group By | Determines how the streamed data is shown:<br>• Connections—Show a single data stream for each connection<br>• Application Messages—Show a single data stream for each message<br>**Note—**This window shows data for selected items only, and not necessarily all the data in that connection or message. |
| Stream Above Level | Determines the protocol layer above which all data is shown.<br>If this menu is set to 0, the stream includes all data in the stream; if this menu is set to Highest, the stream includes data at the highest (application) layer only.<br>The Highest setting is typically the most useful for viewing streams of application data. |
| Update # Bytes Per Line | Determines the number of bytes to show in each line of the Streamed Data Viewer treeview |

### *Related Topics*

- *Protocol Decodes*

## Finding Packets

You can search for packets based on:

- Protocol data (for example, all packets that contain HTTP data)
- Packet contents (all packets that contain a particular string)
- Frame number (as specified in the original packet trace file)

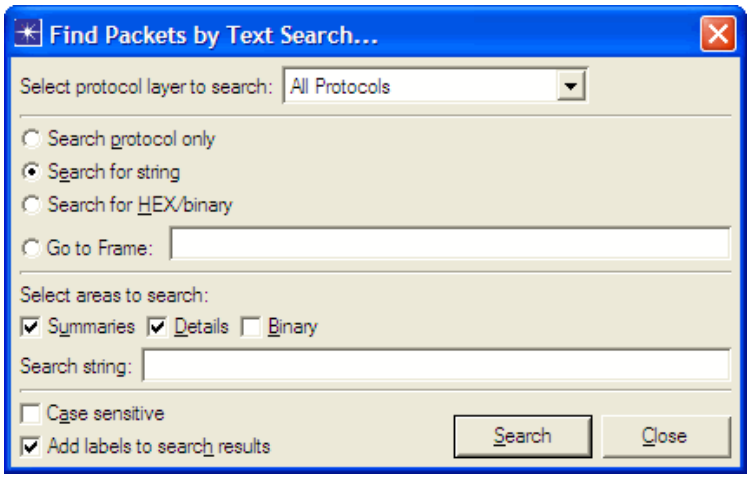
---

**Note—**To search for packets, AppTransaction Xpert must be able to read the packet trace file(s) used to create the model file. If you see a message indicating that the trace files cannot be found, choose File > Trace File Info in the Treeview to specify the location of the packet trace files.

---

To search for specific packets, choose Edit > Find Packets, which opens the "Find Packets by Text Search…" dialog box.

**Figure 19-3 Find Packets by Text Search… Dialog Box**




You can find packets based on a search string, a specific protocol, or a set of frame numbers:

- To search for packets that contain a specific string, select "Search for string" or "Search for Hex/Binary" and enter the search string.

  **Hint—**When performing a search for a string, If the "Add labels to search results" option is selected, then packets containing the search string are labeled in the Data Exchange Chart. Use this option to quickly find and visualize a subset of traffic. This option is also useful for creating a screenshot for a report. Optionally, use the "Colorize Labels" visualization (View > Visualization > Colorize Labels) to color the packets based on search strings. (For example, after searching for "HTTP", use the visualization option to color all packets containing the string "HTTP" with the same color.) The display of labels is cumulative for subsequent string searches. To clear labels from the Data Exchange Chart, choose Edit > Remove All Labels.

- To search for packets that contain a specific protocol, set the “Select protocol layer to search” menu, then select “Search protocol only”.
- To search for packets by frame number, select “Go to Frame” and enter the frame numbers. For example, enter **`21, 25-35`** to find packets 21 and 25 through 35.

After clicking Search, the results are shown in the Protocol Decode Viewer. To view specific packets in the Tree View or Data Exchange Chart, select one or more packets (by shift-clicking or dragging the cursor), right-click, and choose Zoom to DEC or Zoom to Tree.

### *Related Topics*

- *Protocol Decodes*

# AppTransaction Xpert Decode Module

This section describes the features included with AppTransaction Xpert Decode Module:

- Enhanced Protocol Decodes
- Transaction Analysis with AppTransaction Xpert Decode Module
- Packet-Specific Dependencies
- Enhanced HTTP Transaction Analysis with the AppTransaction Xpert Decode Module
- Citrix Decodes in AppTransaction Xpert Decode Module
- Web Services and Transaction Analysis
- MS SQL Decodes
- DB2 Decodes and Transaction Analysis
- CORBA Transaction Analysis
- VoIP Analysis

## Enhanced Protocol Decodes

AppTransaction Xpert Decode Module enables you to pinpoint application-specific messages (for example, SQL statements) and problematic sub-transactions that might be causing delays in your application. This module can decode over 400 protocols and applications.

To display decodes, select a set of packets or messages (in any window), right-click, and choose “Show Protocol Decodes for Selected Items”.

## Transaction Analysis with AppTransaction Xpert Decode Module

With AppTransaction Xpert Decode Module, AppTransaction Xpert can organize a task into separate transactions based on certain protocols. For example, AppTransaction Xpert can decode HTTP messages and organize a task into separate GET and connection open/close transactions. This feature enables you to view a task as a series of protocol-specific transactions (in addition to the standard AppTransaction Xpert organization based on connections, messages and packets).

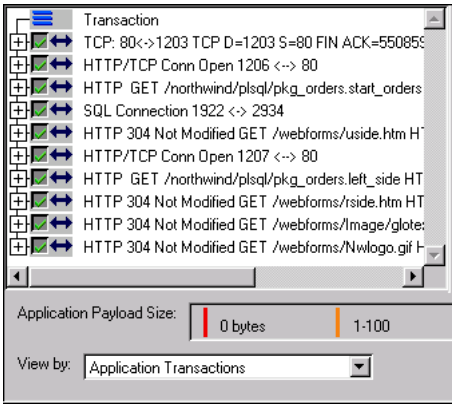
### Viewing Application Transactions

You can view the component transactions of a Transaction Analyzer model in the Tree View page. Set the View By pull-down menu to Application Transactions or Tier Pairs/Application Transactions. (For more information, see Tree View.)

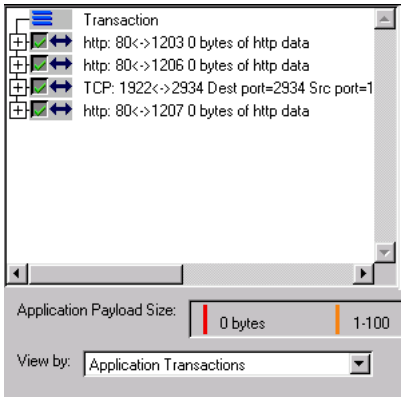
The following figure shows how AppTransaction Xpert reads the same task (a three-tier, web-based transaction) with and without AppTransaction Xpert Decode Module (ADM).

**Figure 19-4 Per-Transaction View of a Web-Based Transaction With and Without AppTransaction Xpert Decode Module**

messages are grouped into HTTP-specific transactions




With ADM




Without ADM

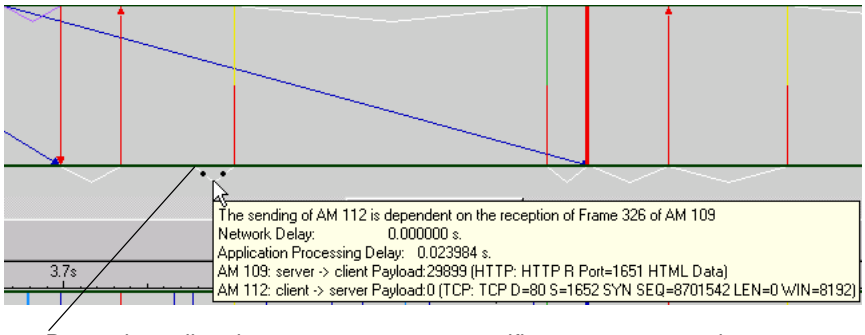
messages are grouped by connection

## Packet-Specific Dependencies

Most dependencies record the cause-and-effect relationship between entire messages. Sometimes a message might depend on a particular packet within a message. These dependencies are known as *packet-specific dependencies*. You can determine that a dependency is packet-specific if it does not visibly connect to an arrow in the Application Message Chart. This is different from a standard dependency line, which visibly connects two message arrows. For more information about dependencies, see Application Message Dependencies.

In the following figure, AppTransaction Xpert determined that Application Message 112 (an HTTP acknowledgement message) depends on the client tier receiving a specific packet in Application Message 109 (long blue arrow).

**Figure 19-5 A Packet-Specific Dependency**




Dependency line does not connect to a specific message, so we know that this is a packet-specific dependency

## Enhanced HTTP Transaction Analysis with the AppTransaction Xpert Decode Module

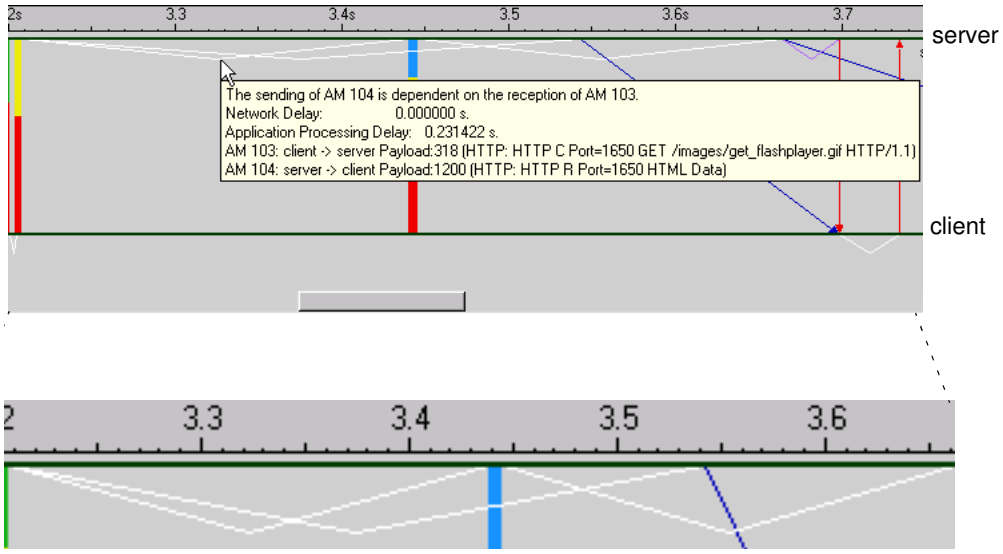
With AppTransaction Xpert Decode Module, AppTransaction Xpert can calculate messages and dependencies based on individual HTTP transactions. This results in more accurate analyses. Examples of HTTP-specific transactions include

- An HTTP/TCP Connection Open or Connection Close
- An HTTP GET request followed by a response

When an HTTP response depends on a request from another tier, AppTransaction Xpert sets up a dependency at the responding tier. This might result in multiple “dependency chains” that track multiple request/response transactions.

The following figure shows an HTTP application as seen with AppTransaction Xpert Decode Module. In this task, a web client (bottom tier) requests a web page that includes multiple GIF files. The Application Message Chart shows multiple dependencies as the server transfers a series of GIF files to the client. Note that AppTransaction Xpert can decode the specific HTTP message from the client to the server (a GET message that requests the file get_flashplayer.gif).

**Figure 19-6 Dependencies for Multiple HTTP Transactions**



You can view the graphic files transferred in an HTTP transaction, as described in the following procedure.

**Procedure 19-1 Viewing a GIF or JPEG File in an HTTP Transaction**

1. Open a Transaction Analyzer model of an HTTP transaction.

   For this procedure to work successfully, the following conditions must be true:

   - AppTransaction Xpert must be able to read the packet trace(s) used to create the Transaction Analyzer model.
   - The file must include at least one GET transaction of a GIF or JPEG file.

2. In the Tree View page, set the View By pull-down menu to Application Transactions.

3. In the treeview (left) pane, select an HTTP GET transaction in which a GIF/JPEG file is transferred. (You might need to resize the treeview pane so that you can see details about the GET transaction.) A GIF/JPEG transaction has a line that reads like this:

   `HTTP GET /<dir_name>/<file_name>.gif HTTP 1.1...`

4. Right-click on the GIF/JPEG transaction and choose HTTP > Save/View Object.

   ➥ The Choose Path for Saving HTTP Object dialog box appears.

5. Make sure that the "View objects in web browser" checkbox is selected, then click Save.

**End of Procedure 19-1**

## Citrix Decodes in AppTransaction Xpert Decode Module

AppTransaction Xpert Decode Module (ADM) can decode Citrix traffic. Use the following features to view Citrix results:

- Tree View tabbed page—When the View By menu is set to “Tier Pairs - Application Transactions”, the treeview groups similar messages together. For example, you might see an “ICA Keyboard” transaction that groups all keystrokes, or an “ICA Initialization” transaction that groups all packets in the initialization sequence.
- AppDoctor window—If a task has Citrix traffic, the AppDoctor window includes a “Citrix ICA” tabbed page that shows summary information and statistics about the Citrix traffic.
- Protocol decodes—ADM can decode CGP- and ICA-specific information in individual packets.

### Capturing Citrix Traffic

Note the following:

- You must capture the Citrix traffic as described in Procedure 19-2.
- For a complete list of supported Citrix versions, see the System Requirements on the Support Center.
- If Citrix is using a non-default port, you must edit the following file to specify the port number:

  <*install_dir*>\sys\configs\protocols_v2.ace_dict

- ADM does not decode encrypted traffic. Before capturing Citrix traffic, set the encryption level to Basic or None. Typically, Basic encryption encrypts only the traffic in which the username and password are exchanged; all other traffic is uninterrupted. For more information, see the following procedure and the Citrix documentation.

**Procedure 19-2 Capturing a Citrix Application**

1. Verify that the encryption level on the Citrix client is set to Basic or None.

   For information about setting the encryption level on the Citrix client, see the Citrix documentation.

2. Start the capture operation on the capture agent or protocol analyzer before connecting to the Citrix server.

   - If using the Citrix Program Neighborhood, start the capture before double-clicking on the ICA connection.
   - If connecting through NFuse, start the capture before clicking on the application or server.

   For general information about capturing application traffic with AppTransaction Xpert and other programs, see Capturing Application Traffic: Overview.

3. Connect to the Citrix server and run the application transaction that you want to capture.

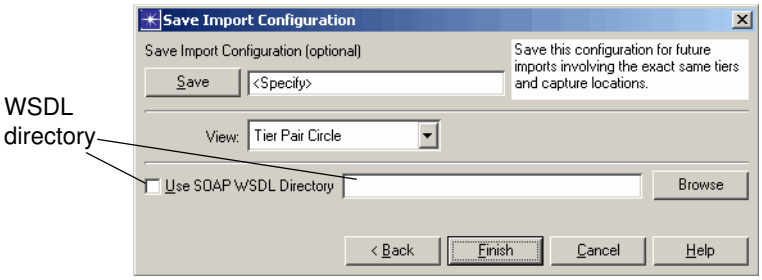
**End of Procedure 19-2**

## Web Services and Transaction Analysis

You can view AppDoctor statistics and transaction information for .Net, SOAP, and UDDI traffic. You can see SOAP-specific information in the Tree View tabbed page, in AppDoctor, and in the Protocol Decode Viewer.

For specific instructions for importing packet trace files, see Creating a Transaction Analyzer Model. If you want to specify a WSDL directory during the import capture operation, use the following Web services dialog box to specify the directory you want. You must specify a WSDL directory in order for AppDoctor analysis to take place.

**Figure 19-7 Web Service Import Configuration Dialog Box**



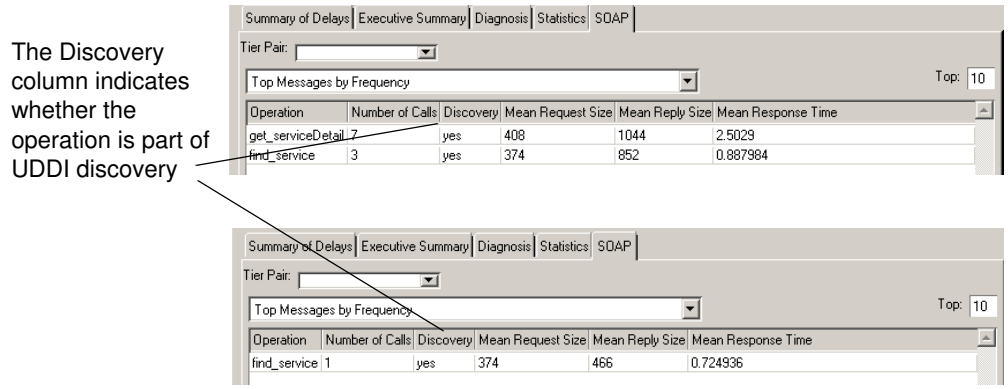

---

**Note—**SOAP will not appear unless you select a WSDL directory during import and the WSDL files contained in this directory match the Web Services Message in the trace.

---

The Web Services Decode statistics page looks similar to the CORBA Decode page described previously. The first example in the following figure shows the statistics for two operations (i.e., function calls) and the second example shows a single SOAP operation.

**Figure 19-8 SOAP Tabbed Page in AppDoctor Window**



The drop-down menu above the statistical display provides four sorting options:

- Top messages by frequency
- Request size (in bytes)
- Reply size (in bytes)
- Speed (with the slowest messages at the top of the list)

In the Tier Pair: drop-down menu, you can view the total of tier pairs or each of the different tier pairs.

The main screen shows a list of the function calls. The default setting is 10 operations. You can edit the number in the Top: text box to show more or fewer operations.

## MS SQL Decodes

AppTransaction Xpert Decode Module can analyze Microsoft SQL transactions. The SQL decode engine is based on the TDS protocol specifications as described in the FreeTDS website (http://www.freetds.org). You can view SQL-specific information in the following windows:

- The Protocol Decodes Viewer shows SQL decode information.
- The Tree View tabbed page organizes a Transaction Analyzer model into transactions based on SQL data.

There are two preferences that control how SQL data is displayed in the Protocol Decodes Viewer:

- ace_decoder_ms_sql_num_rows_per_response—The maximum number of rows that appear for each response.
- ace_decoder_ms_sql_string_display_length—The maximum number of characters shown for each individual SQL string.

## DB2 Decodes and Transaction Analysis

AppTransaction Xpert supports decodes of DB2 versions 8.1, 8.2, 9.0, and 9.2. The Tree View page organizes a Transaction Analyzer model into separate DB2 transactions. The Protocol Decodes Viewer shows details of SQL operations and DRDA commands.

Note the following:

- It is good practice to capture DB2 transactions the same way you capture other types of transactions: start capture => start DB2 transaction => end DB2 transaction => stop capture. This ensures that you capture all the traffic in the transaction of interest.

If your capture data does not include the initial DRDA Environment information, you can still decode the DB2 data. However, you might need to set the following preferences:

— ace_db2_client_is_big_endian

— ace_db2_server_is_big_endian

To view these and other preferences, choose Edit > Preferences and search for “db2”.

- AppTransaction Xpert Decode Module does not decode packets that were encrypted using DB2 security features.
- AppTransaction Xpert Decode Module supports ASCII and EBCDIC encoding schemes only for SQL data.

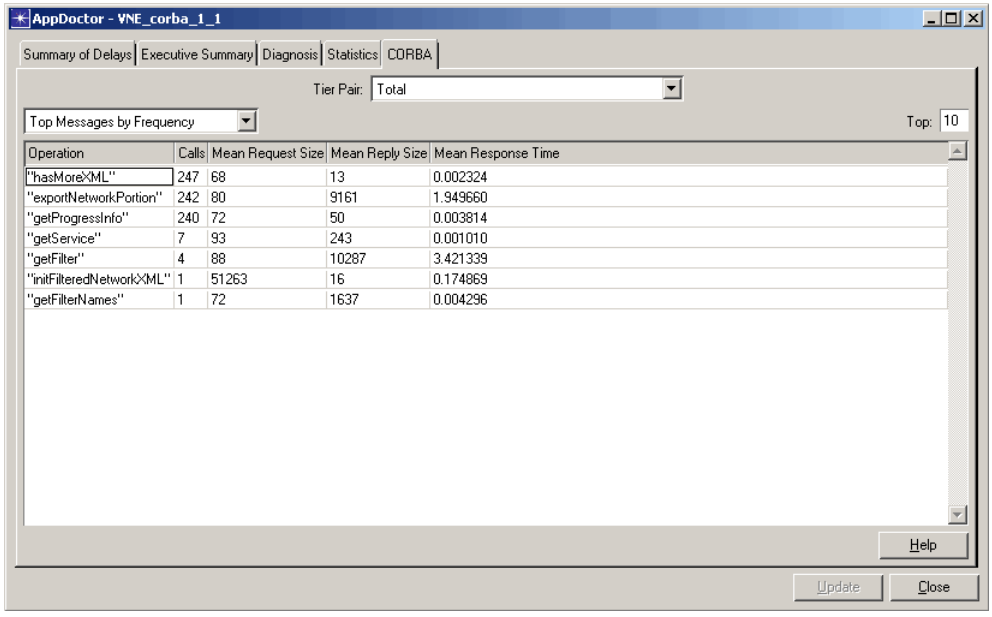
## CORBA Transaction Analysis

If a Transaction Analyzer model contains CORBA traffic, the AppDoctor window incudes a CORBA tabbed page with summary and statistic information. CORBA decode summaries are applicable for request and reply messages only. When working with decode summaries, it is important to remember that the ID number of the request message decode must match the ID number of the corresponding reply message decode.

The CORBA tabbed page summarizes information about CORBA operation invocations contained in the Transaction Analyzer model. There are multiple summary tables available on this page, so you can view the top CORBA operations based on a specific threshold (such as frequency or response time).

The following figure shows a typical CORBA tabbed page.

**Figure 19-9 CORBA Page**



The drop-down menu in the upper-left provides four sorting options:

- Top messages by frequency
- Request size (in bytes)
- Reply size (in bytes)
- Speed (with the slowest messages at the top of the list)

Using the “Tier Pair” drop-down menu, you can select whether summary tables are computed across all tier pairs (Total) or for an individual tier pair.

The main screen shows a list of the function calls. The default setting is 10 operations. You can edit the number in the Top: text box to show more or fewer operations.

## VoIP Analysis

AppTransaction Xpert Decode Module can analyze Voice-over-IP transactions. The Tree View page shows each VoIP call as a separate transaction, and organizes each transaction into the following subtransactions:

- Call Setup—which runs over an application-signaling protocol such as SIP. Each SIP subtransaction is further organized into separate subtransactions based on SIP branch.
- Data Transmission—which runs over RTP. The treeview further organizes RTP connections into separate subtransactions.
- RTCP Connections—which includes information about simple packet loss, jitter, and endpoint times.

If a Transaction Analyzer model contains VoIP traffic, the AppDoctor window includes a VoIP tabbed page that shows the following information for each VoIP call: summary information, packet statistics, and call statistics (such as call setup time, max jitter, out-of-sequence packets, packet loss, max delta, media type, and sampling rate).

### *Related Topics*

- *Protocol Decodes*

# Redecoding Traffic

The “Redcode As” operation allows you to redecode traffic to a specific port as a specific protocol. Note that only a single port for a single tier can be redecoded at a time, and it is applied to all of the selected connections to that port.

The “Redecode As” operation is useful when:

- The Transaction Analyzer model contains traffic that is not automatically decoded when the model is created.
- Updating the external decoder used by AppTransaction Xpert. If the Transaction Analyzer model was created with a previous decoder, you can redecode selected traffic so that the Protocol Decodes Viewer shows decodes from the most recent decoder.

  **Note—**If using the most recent decodes is a priority, it is best to re-create the Transaction Analyzer model so that all decode information is up-to-date.

**Hint—**If the results of the redecode is not as expected, perform the redecode procedure again, but select the other port of the connection from the “Decode traffic to” pull-down menu.

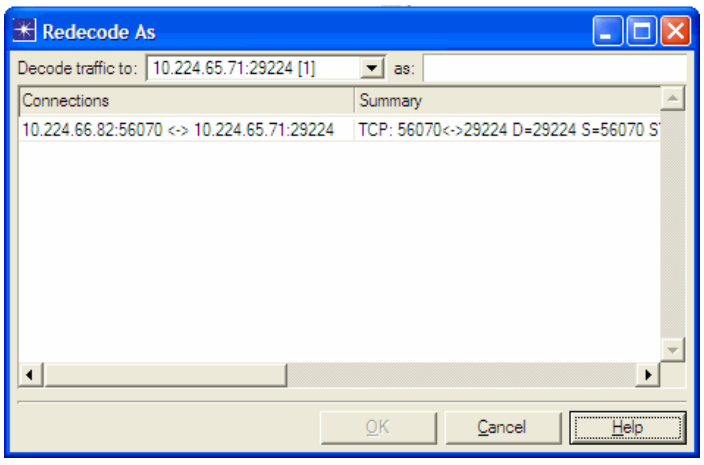
### Procedure 19-3 Redecoding Traffic

1 In the Tree View or Tier Pair Circle page, select one or more connections.

**Hint—**Hold down the Ctrl key to select individual connections. Hold down the Shift key to select a range of connections.

2 Right-click on a selected connection and choose “Redecode As…”.

➥The “Redecode As” dialog box appears.



The dialog box includes the following options and fields:

- "Decode traffic to" pull-down menu—Lists the selected ports (including tier name and port number). The number in the square brackets represents the number of connections selected that match the tier and port. The list is sorted by the number of matching connections.
- "as" pull-down menu—Lists the protocols to which you can redecode traffic.
- Connections column—Lists all of the connections that will be redecoded when OK is selected.
- Summary column—Displays a summary for the connection.

**3** From the "Decode traffic to" pull-down menu, select the server port.

Selecting the correct server port will result in more accurate decodes, particularly for database protocols.

**4** From the "as" pull-down menu, select the TCP/UDP protocol that you want to redecode the traffic as. Alternately, select "Edit…" and manually enter the protocol name.

**5** Click OK.

➥The selected traffic is redecoded.

**End of Procedure 19-3**

---

**Note—**The system configuration files "adm_redecode_as.tcp.ace_dict" and "adm_redecode_as.udp.ace_dict" control the list of items that are displayed in the "as" pull-down menu. To add or delete an item from the list, edit the appropriate file in a text editor. For information about how to persistently force decoding, see FAQ 1202 on the Support Website.

---

## *Related Topics*

- *Protocol Decodes*

# Troubleshooting: Incorrectly Identified Protocols

Protocols are identified by the communication port. AppTransaction Xpert includes a list of default ports and their associated protocols. If your organization uses a different port other than the default port, then the protocols may be misidentified and decoded incorrectly.

To view the default ports associated with protocols, open the <install_dir>\sys\configs\protocols_v2.ace_dict file. If your organization uses a different port than the port specified in the file, then edit and save the file.

### *Related Topics*

- *Protocol Decodes*