7 Previewing and Extracting Traffic from Packet Traces

For accurate results, a Transaction Analyzer model must include only traffic that is relevant to one user-level transaction. The Trace Summary and Trace Explorer windows make it easy to browse large packet traces, filter out irrelevant traffic, find user-level transactions of interest, and import those transactions.

This section has the following topics:

- Trace Summary (for use after import)
- Trace Explorer
- Common Tasks in Trace Explorer/Trace Summary
- Example Workflow: Drilling Down, Searching, Extracting, and Importing
- TCP Segmentation Offloading (TSO) in Packet Traces: What to Do

Trace Summary

The Trace Summary window makes it easy to browse and flitter traffic within Transaction Analyzer.

Use Trace Summary to:

- View traffic in a Transaction Analyzer model
- View detailed protocols (requires AppTransaction Xpert Decode Module license)
- Filter irrelevant traffic and find user-level transactions of interest

For more information, see the following sections:

- Workflow descriptions
  - — Trace Summary: Workflow Description
  - — Example Workflow: Drilling Down, Searching, Extracting, and Importing
- Task descriptions
  - — Filtering Traffic
  - — Finding a User-Level Transaction of Interest
  - — Including Packets for a User-Level Transaction
- User interface descriptions
  - — Traffic Drilldown Pane
  - — Packet Group Organization

Trace Summary: Workflow Description

The following steps outline the overall Trace Summary workflow:

1) From the Transaction Analysis window, open Trace Summary (Edit > Trace Summary…).

2) Navigate through the packets until you find a transaction of interest.

3) Mark all the packets that are relevant to that transaction as “Included”.

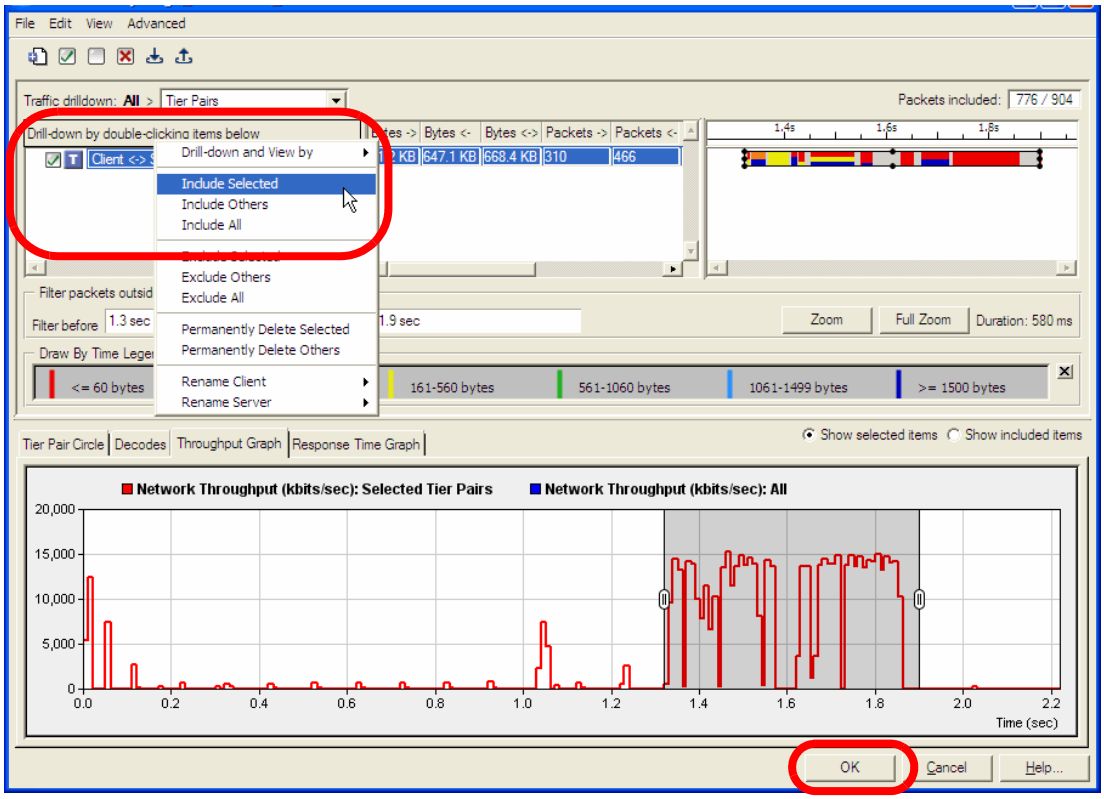
4) Click OK to include/exclude transactions from the Transaction Analyzer model.

Figure 7-1 Trace Summary Window

STEP 1:
Drill down into the capture data until you find the transaction of interest

STEP 2:
Include the transaction of interest by selecting checkboxes in the Traffic Drilldown pane

STEP 3:
Click OK to exclude transactions from the Transaction Analyzer model



The following procedure describes this workflow in detail.

Procedure 7-1 Trace Summary: Exclude Transactions from a Transaction Analyzer Model

1. Open the Transaction Analyzer model.
   (File > Open Model > Transaction Analyzer…)
2. Choose Edit > Trace Summary.

   ➥ The Trace Summary window appears.
3. Use the Drilldown pane (upper-left) to navigate through the traffic and find the user-level transaction that you want to import. For more information, see:
   - Finding a User-Level Transaction of Interest
   - Visualization Panes in Trace Explorer/Trace Summary
   - Example Workflow: Drilling Down, Searching, Extracting, and Importing
4. Mark the packets for the transaction of interest as “Included”. Packets that are marked as Included are saved in the new file. All packets are initially excluded, as indicated by the “Packets included” field in the upper-right corner of the window.

   You can include/exclude groups of packets in the Traffic Drilldown pane; you can include/exclude individual packets in the Decodes tabbed page. For more information, see Including Packets for a User-Level Transaction.
5. Click Next.

End of Procedure 7-1

Related Topics

- *Example Workflow: Drilling Down, Searching, Extracting, and Importing*

Trace Explorer

Note—This feature requires a license for AppTransaction Xpert Decode Module.

In some cases, you might have large packet traces that contain irrelevant traffic or even multiple runs of one or more applications. This is especially true of packet traces generated during scheduled or continuous captures. A packet trace might contain numerous user-level transactions—web-page downloads, FTP transfers, database queries, and so on—captured over an extended time period.

Trace Explorer is a stand-alone window for browsing packet traces and extracting relevant traffic. This window is useful if a packet trace is too large to be imported within a reasonable amount of time. The Trace Explorer window makes it easy to browse large packet traces, filter out irrelevant traffic, find user-level transactions of interest, and import those transactions.

To begin examining or filtering a trace quickly, Trace Explorer extracts basic IP information from the trace, allowing traffic to be classified by tier pairs and connections. Detailed information is then extracted in the background and made available as it is decoded.

Note—Be sure to close Trace Explorer when finished with it to cancel background decoding and to free computing resources.

Use Trace Explorer to:

- Quickly open a large packet trace
- View high-level information about traffic, whether that traffic is relevant to a specific application
- Filter irrelevant traffic and find user-level transactions of interest
- Select traffic of interest and save the traffic to a new, smaller packet trace file, which you can then import

For more information, see the following sections:

- Workflow descriptions
  - Trace Summary: Workflow Description
  - Example Workflow: Drilling Down, Searching, Extracting, and Importing
- Task descriptions
  - Filtering Traffic
  - Finding a User-Level Transaction of Interest
  - Including Packets for a User-Level Transaction
  - Saving Included Packets to a New Packet Trace (Trace Explorer Only)

Trace Explorer: Workflow Description

The following steps outline the general workflow for Trace Explorer:

1) Open the packet trace in Trace Explorer.

2) Navigate through the captured packets until you find a transaction that you want to import.

3) Mark all the packets that are relevant to that transaction as Included.

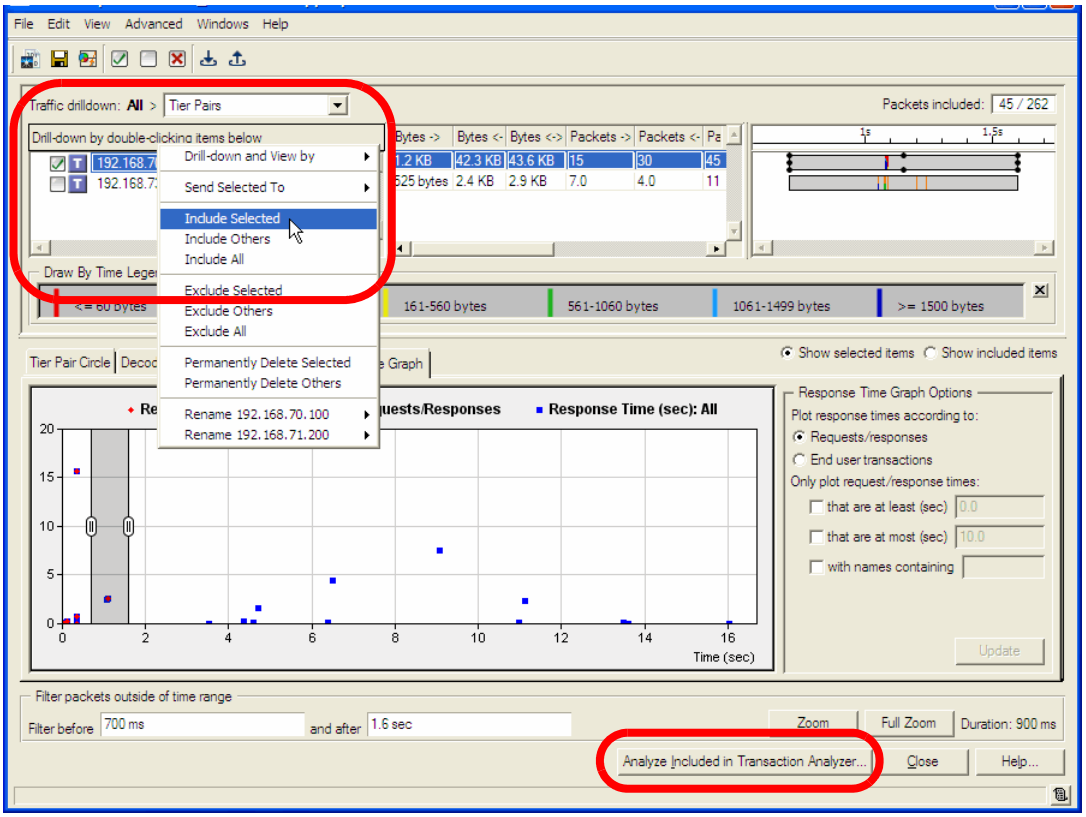
4) Save the included packets to a new packet trace and directly import in Transaction Analyzer.

Figure 7-2 Trace Explorer Window

Step 1:
Drill down into the capture to find the transaction of interest.

Step 2:
Include that transaction by selecting checkboxes in the Traffic Drilldown pane.

Step 3:
Save the transaction of interest to a new packet trace.



The following procedure describes this workflow.

Procedure 7-2 Trace Explorer: Extracting a User-Level Transaction from a Packet Trace

1. Choose File > Open Packet Trace(s) > In Trace Explorer and select the packet trace.

   ➥ The Filter Irrelevant Traffic dialog box appears. For more information, see Filtering Traffic.

2. Filter out all traffic that you know is irrelevant. This makes it easier to navigate through the capture data and find a user-level transaction of interest. Then click Next.

   ➥ The Trace Explorer window appears and shows the capture data from the selected packet trace.

3. Use the Drilldown pane (upper-left) to navigate through the traffic and find the user-level transaction you want to import. For more information, see:

   - Finding a User-Level Transaction of Interest
   - Visualization Panes in Trace Explorer/Trace Summary
   - Example Workflow: Drilling Down, Searching, Extracting, and Importing

   Specify the chart drawing mode for visualizing the traffic data:

   - **Time—**If viewing the traffic data by time (View > Chart Drawing Mode > Time), the chart drawing represents the packet size over time using color-coding.
   - **Bytes—**If viewing the traffic data by bytes (View > Chart Drawing Mode > Bytes), the chart drawing represents the total number of bytes using color-coding.

   Note—You can switch between modes by right-clicking in the chart and selecting “View by Bytes” or “View by Time”.

   To further understand and define the color-coding, you can perform the following options:

   - Display Legend—Choose View > Show Cart Drawing Legend to toggle the display of the color-coding legend. The legend displays below the chart drawing.
   - Smoothing—Choose View > Chart Drawing Coarseness to control the smoothing of the color-coding in the chart bars. The higher the coarseness value, the smoother the chart appears. Choose from 0 to 10. The default is 8.

   If you do not want the color-coding to display in the chart drawings, which may impact the performance of large packet traces, turn off the functionality by setting the ace_quickview_force_old_chart_drawing preference to TRUE. By default, the preference is set to FALSE.

4 Mark all packets for the transaction of interest as “Included”. Packets that are marked as Included (and were not filtered out in step 2) will be saved in the new packet trace. All packets are initially excluded, as indicated in the “Packets included” field in the top-right corner.

   You can include/exclude groups of packets in the Traffic Drilldown pane; you can include/exclude individual packets in the Decodes tabbed page. For more information, see Including Packets for a User-Level Transaction.

5 Save the included packets to a new packet trace.

   There are two possible methods:

   - To save to a .appcapture file, then import immediately, click “Analyze Included in Transaction Analyzer…”. Alternately, choose File > Analyze Included in Transaction Analyzer…

     ➥ A dialog box prompts for the name of the new packet trace.

     ➥ The “Included” packets (that are not filtered) are saved to the new file.

     ➥ The new packet trace opens in the Merge Capture Files Dialog Box. Proceed with the import, as described in Creating a Transaction Analyzer Model.

   - To save to a .appcapture or other file without importing (*Trace Explorer only*), choose one of the following menu operations:

     - File > Export to .Appcapture File…—Save included packets to .appcapture, without importing
     - File > Export to .enc File…—Save included packets to .enc
     - File > Remove TCP Segmentation Offloading…—Save included packets to .appcapture, with TCP segmentation offloading data removed

6 Import the new packet trace.

End of Procedure 7-2

Related Topics

- *Example Workflow: Drilling Down, Searching, Extracting, and Importing*

Common Tasks in Trace Explorer/Trace Summary

This section describes common tasks that are performed with Trace Explorer and/or Trace Summary:

- Filtering Traffic
- Finding a User-Level Transaction of Interest
- Visualization Panes in Trace Explorer/Trace Summary
- Including Packets for a User-Level Transaction
- Example Workflow: Drilling Down, Searching, Extracting, and Importing
- Saving Included Packets to a New Packet Trace (Trace Explorer Only)

Filtering Traffic

Before navigating through a large packet trace, it is good practice to filter out any irrelevant traffic. The Trace Explorer/Trace Summary window includes three options for filtering traffic:

- Filter by traffic type—Some categories of traffic are filtered out by default:
  - Traffic on “one-way-traffic” connections
  - Non-IP traffic
  - Broadcast traffic
  - Non-DNS UDP traffic

  To include traffic from any of these categories, choose Edit > Filter Wizard.
- Filter by host, port, connection, protocol, or broadcast/multicast—To filter out traffic using a standard packet filter, choose Edit > Filter Trace. For more information about these filters, see Packet Filtering.
- Filter by time—Use the “Filter packets outside of time range” fields and sliders to filter out packets based on time.

  You might want to do this initially if you know that the transaction of interest occurred within a specific time window. You might also want to use the time sliders after you drill down into a specific class of traffic.

Finding a User-Level Transaction of Interest

The Trace Explorer and Trace Summary windows provide the following features for navigating packet traces and finding transactions:

- Traffic Drilldown Pane (top left)—Use this pane to navigate through the traffic and include traffic of interest.
- Visualization panes (all others)—Use the other panes in the window to view information about the traffic shown in the Drilldown pane. These panes are described in Visualization Panes in Trace Explorer/Trace Summary.

Traffic Drilldown Pane

The primary mechanism for navigating the packet trace and including packets is the Traffic Drilldown pane in the top-left corner. This pane shows a specific group of packets and arranges them into subgroups. When the Trace Explorer/Trace Summary window first appears, this pane shows all (unfiltered) packets in the capture data and arranges them by top-level protocol.

The following operations can be performed in this pane:

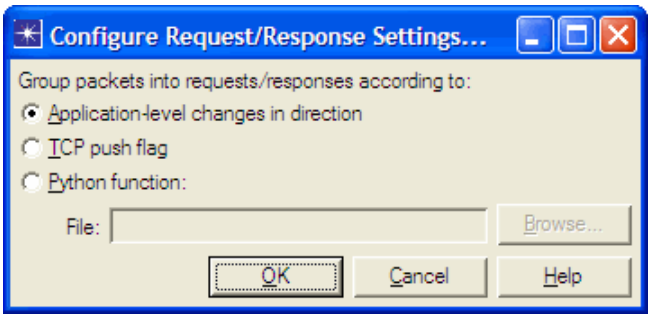
- Drill down into a group of packets—To drill down into a group of packets, double-click on it. Alternately, right-click on an item in the drill-down list and select the “Drill-down and View by” option The labels above the menu are updated to show the current group and all parent groups.
- Drill up to the parent group—To return to a parent group, click on the link above the pane.
- Reorganize the current group of packets—The pull-down window shows how the current group of packets is organized into subgroups. To use a different organization, choose an option from this menu. For more information, see Packet Group Organization.
- Include/Exclude/Delete selected packets—To include, exclude, or delete one or more groups of packets, select the groups, right-click, and choose the operation.

Packet Group Organization

The pull-down menu above the Traffic Drilldown pane enables you to organize the current group of packets. The options are:

- Protocols—Groups packets based on the top-level protocol seen on the connection for each packet
- Tier Pairs
- Tiers
- Connections
- Requests/Responses—By default, this option groups packets into requests/responses based on application-level changes in direction.

  To specify a different organization, choose Edit > Configure Request/Response Settings…



  In the “Configure Request/Response Settings” dialog box, select the following:

  — Application-level changes in direction—Groups packets into requests/responses based on application-level changes in direction. (This is the default setting.)

  — TCP push flag—Groups packets into requests/responses based on TCP Push flags, where a new request/response is created when a tier receives a TCP packet that has its Push flag enabled. This flag indicates to the receiving TCP process that all data has been received and the TCP can push the data to the receiving application.

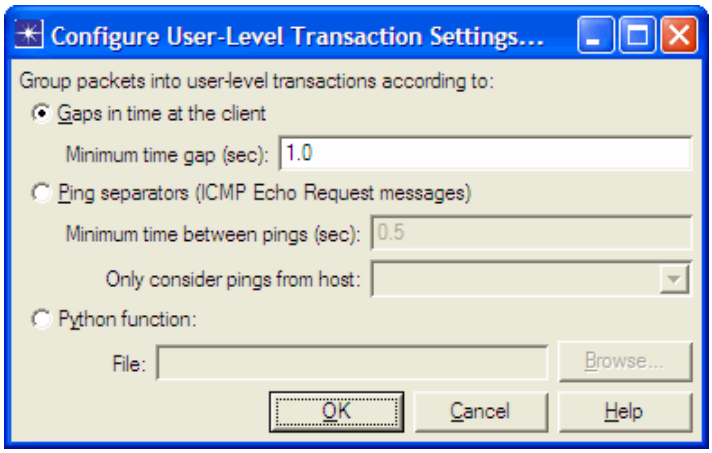
  — Python function—Groups packets into requests/responses based on a custom Python function. For example, the following script will traverse through the packets and associates three packets with each request/response. If you select a request/ response, the Decodes tab will populate with exactly three frames per request/response.

```
import Ace_Qv

def op_lean_main():
task = Ace_Qv.get_current_task()
for i in range (task.get_num_network_packets()):
pkt = task.get_network_packet (i)
if (i % 3 == 0):
rr = task.create_request_response ()
```

```
try:
layer = pkt.get_num_layers()
name = pkt.get_layer_decode_summary (layer-1)
except:
name = "request_response" + str (i)
rr.set_name (name)
rr.add_network_packet (pkt)


task = Ace_Qv.get_current_task()
for i in range (task.get_num_request_responses()):
req = task.get_request_response (i)
if (i % 3 == 0):
ut = task.create_end_user_transaction()
try:
layer = req.get_num_network_packets()
name = req.get_name ()
except:
name = "request_response" + str (i)
ut.set_name (name)
ut.add_request_response ( req )
```

- End-User Transactions—By default, this option groups packets into user-level transactions based on gaps in time at the client.

  To specify a different organization, choose Edit > Configure User-Level Transaction Settings…



  In the “Configure User-Level Transaction Settings” dialog box, select the following:

  — Gaps in time at the client—Groups packets into user-level transactions based on gaps in time at the client. Specify the minimum time gap, in seconds. (This default setting is 1.0 second.)

  — Ping separators (ICMP Echo Request Messages)—Groups packets into user-level transactions based on ICMP Echo Request messages.

  — Python function—Groups packets into user-level transactions based on a custom Python function.

Visualization Panes in Trace Explorer/Trace Summary

The Trace Explorer/Trace Summary window contains the following panes for viewing traffic data:

- Table pane (top center)—Shows statistic data about each packet group currently shown in the Traffic Drilldown pane. To reorder groups based on a specific statistic, click on the column heading in this table.
- Time/Payload pane (top right)—A Gantt-style chart that shows the duration or size (in bytes) of each packet group.To switch between the time view and the size-in-bytes view, right-click in the chart background.
- Tier Pair Circle tabbed page—Shows the tier-pair conversations and their traffic levels for items that are currently selected or included (based on the radio button selected on the right).
- Decodes tabbed page—Shows detailed information, including protocol decodes, for selected/included packets. Use the checkboxes on this tabbed page to include/exclude individual packets.
- Throughput Graph tabbed page—Shows the network throughput levels for all groups and selected/included groups.
- Response Time Graph tabbed page—Shows the response times of individual requests/responses or user-level transactions.

Including Packets for a User-Level Transaction

Your goal in the Trace Explorer/Trace Summary window is to find the user-level transaction that you want to import. After you find the transaction in the Traffic Drilldown pane, make sure that:

1) All packets that relate to that transaction are Included, AND

2) All unrelated (extraneous) packets are Excluded.

Use the following operations to include/exclude packets:

- Include/exclude packet group—Select one or more groups in the Traffic Drilldown pane; right-click on one of the groups; choose Include Selected or Exclude Selected.
- Include/exclude individual packet—Open the Decodes tabbed page (bottom) and set the checkboxes for the individual packets.

The “Packets included” field (top-right) shows the number of packets that are currently included.

Saving Included Packets to a New Packet Trace (Trace Explorer Only)

Note—This section applies to Trace Explorer only, not to Trace Summary.

After including the packets of interest (as described in Including Packets for a User-Level Transaction), you can save the packets as a packet trace and open the file in Transaction Analyzer.

Save to .appcapture and import

To save included packets to a .appcapture file, and then import the new file, click the "Analyze Included in Transaction Analyzer…" button. The following occurs:

- You are prompted for the name of the new packet trace.
- A new packet trace is created that contains all packets that are marked as "Included".

Save to .appcapture or other format without importing

After opening a packet trace in Trace Explorer, there are additional options for saving included packets:

- File > Export To .appcapture File…—Save included packets to .appcapture, without importing
- File > Export To .enc File…—Save included packets to .enc
- File > Remove TCP Segmentation Offloading…—Save included packets to .appcapture, with TCP segmentation offloading data removed

Related Topics

- *Trace Explorer*
- *Trace Summary*

Example Workflow: Drilling Down, Searching, Extracting, and Importing

In this example, we follow an application developer/troubleshooter as she extracts a problematic user-level transaction from a large packet trace. This shows one possible workflow for finding transactions, and illustrates how you can use the different features in Trace Explorer to navigate through your capture data.

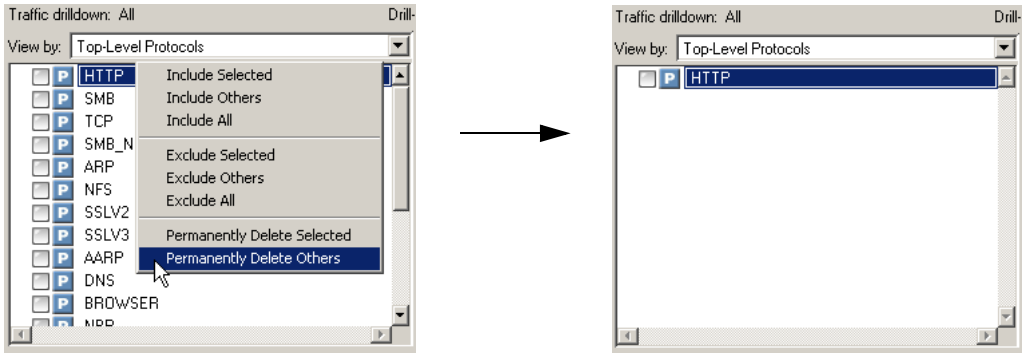
Note—Many of the Trace Explorer features described in this example also apply to Trace Summary. The main differences between Trace Explorer and Trace Summary are:
- Trace Explorer is accessed before packet traces are opened in Transaction Analyzer. Trace Summary is accessed after packet traces are opened in Transaction Analyzer.
- Trace Explorer includes the ability to save included packets to a new packet trace. Trace Summary does not include the ability to save included packets to a new packet trace.

Example, Step 1: User Opens Packet Trace in Trace Explorer

The user has a continuous capture running on a web-server tier in her organization. Her goal is to look for problematic HTTP transactions and troubleshoot them in AppTransaction Xpert. She takes a packet trace that records twenty minutes of traffic and opens it in Trace Explorer.

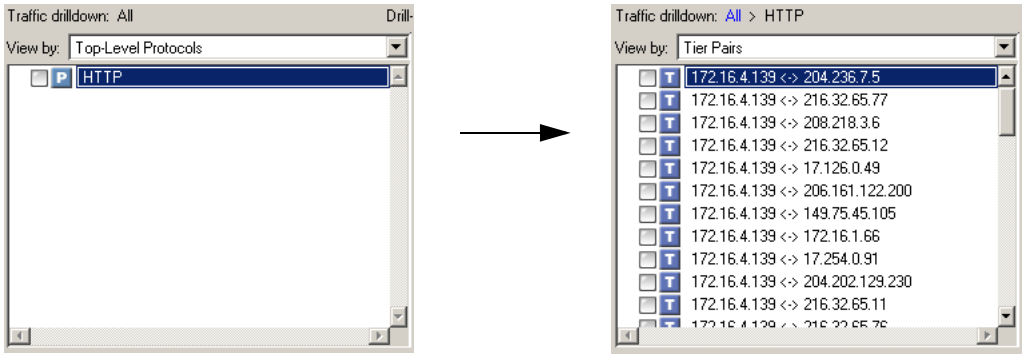
Example, Step 2: User Filters Out Extraneous Traffic

The Drilldown Pane shows traffic that uses a number of different protocols. Because she is only interested in HTTP traffic, she starts by deleting all traffic that uses non-HTTP connections.



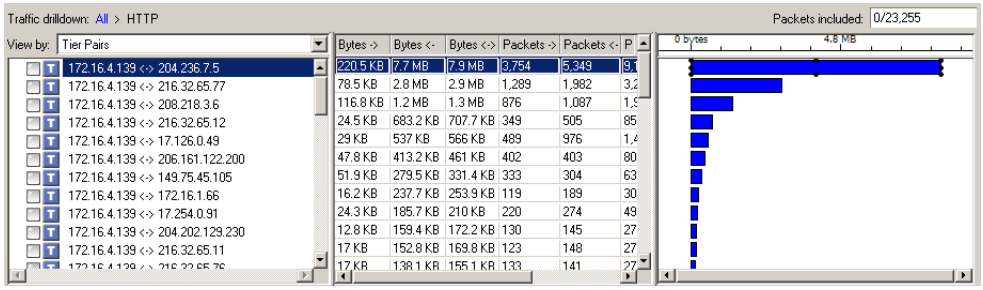
Example, Step 3: User Drills Down One Level

Next, she double-clicks on "HTTP" to drill down one level (from Protocol Connections to Tier Pairs). Now she can see all the tier pairs that are using HTTP connections.

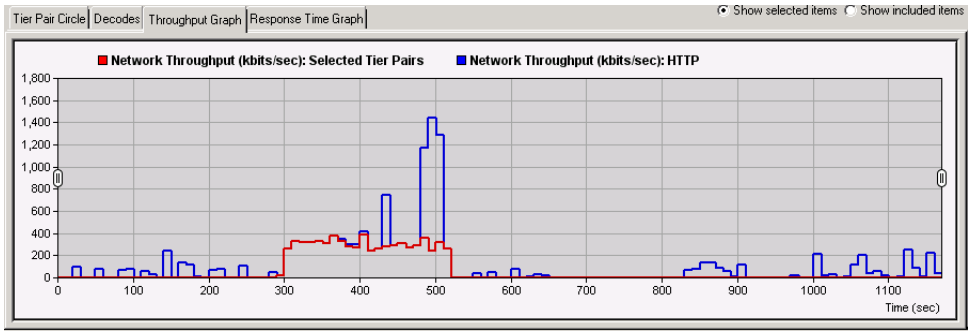


Example, Step 4: User Looks for "Spikes" of HTTP Traffic

Judging from the graph on the right, it appears that one tier is exchanging much more HTTP traffic than the others.

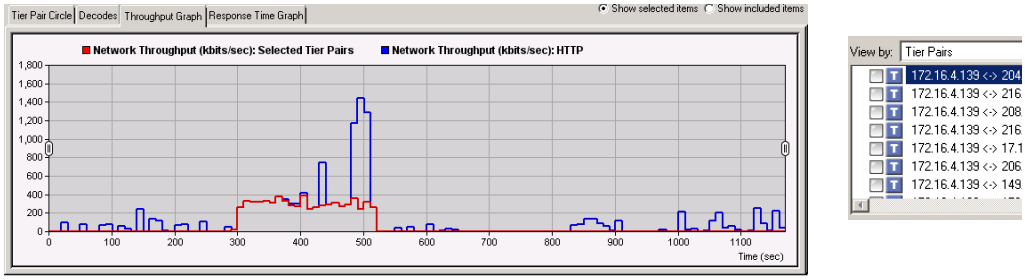


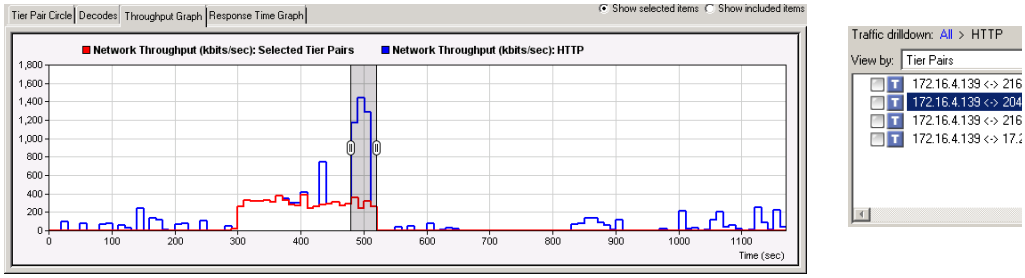
However, when she looks at the Throughput Graph on the bottom, she can see one particular "spike" of HTTP traffic. She decides that this "spike" is worth investigating.



Example, Step 5: User Zooms In on the Time Window of Interest

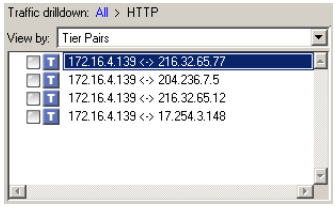
Using the drag handles, she reduces the selected time range to focus on this exchange. As she reduces the time range, the Traffic Drilldown pane hides tier pairs that do not exchange traffic within the selected time range.

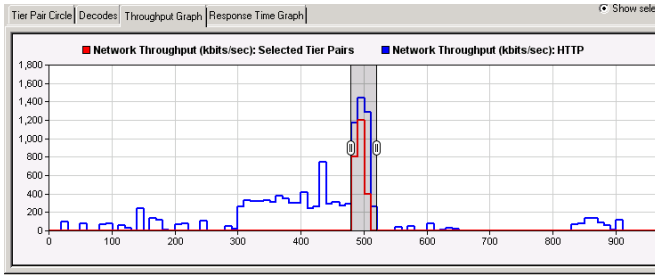




Example, Step 6: User Determines the Tier Pair Responsible for the Spike in HTTP Traffic

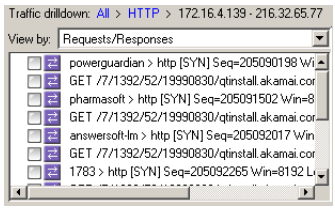
By individually selecting each tier pair in the Drilldown Pane and observing the red line in the Throughput Graph, she can see that one tier pair is responsible for most of this spike. She double-clicks on this tier pair to drill down to the next level.

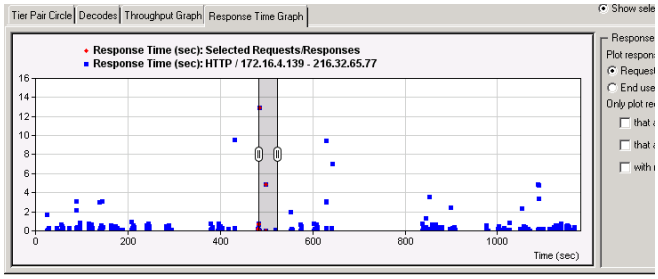




Example, Step 7: User Looks for Long Request/Response Cycles

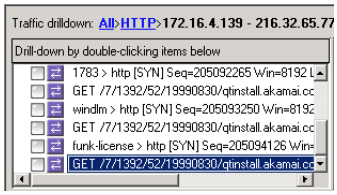
Having found the tier pair responsible for the spike in HTTP traffic, she double-clicks on this tier pair. The Traffic Drilldown goes down one level and shows all request/response cycles for that tier pair. Because response times (rather than traffic levels) are generally of more interest at this level, the Response Time Graph now becomes active.

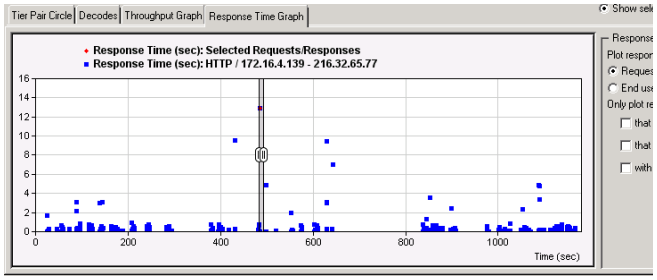




Example, Step 8: User Adjusts Time Window

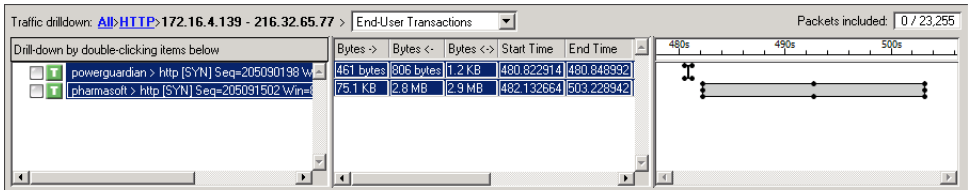
Seeing one particularly long request/response cycle, she adjusts the time window using the drag handles. She then selects items in the Traffic Drilldown Pane one by one until she finds the item that turns the request/response cycle in the time window to red.





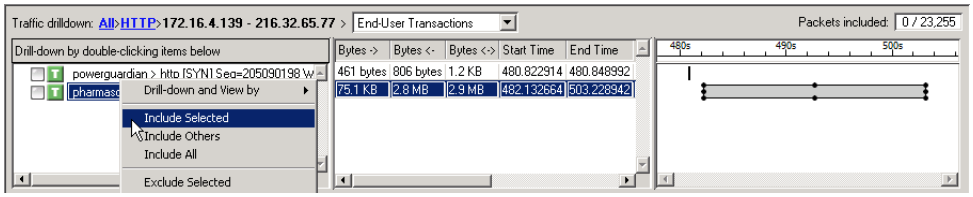
Example, Step 9: User Views End-User Transactions Within Time Window

Now that she sees the time window with the longest request/response cycles, she changes the Drilldown level to End-User Transactions. The Drilldown Pane now shows all end-user transactions for that time window.



Example, Step 10: User Includes Transaction and Opens it Transaction Analyzer

She sees there is a very long transaction, with a response time of 21.1 seconds. She includes this transaction and opens it in Transaction Analyzer.



Related Topics

- *Trace Explorer*

TCP Segmentation Offloading (TSO) in Packet Traces: What to Do

If you see a warning that a packet trace shows evidence of TCP Segmentation Offloading, it is good practice to create an alternative capture that has the TSO removed and then import the alternative file instead of the original.

Note—If you import "unsegmented" capture data, AppTransaction Xpert cannot correctly match the dataful packets with their corresponding ACK messages. As a result, the Transaction Analyzer model will not be as accurate as possible.

This section includes the following topics:

- Saving to a Packet Trace without TSO
- What is TSO?
- Why Did This Message Appear?
- Why is This a Problem?

Saving to a Packet Trace without TSO

Procedure 7-3 Saving a Packet Trace without TCP Segmentation Offloading

1. If you are importing one or more packet traces and the message appears stating that one or more packet traces show signs of TCP Segmentation Offloading, do the following:
   - **1.1** Note the packet traces indicated in the warning dialog box. If there are multiple files, you can generate a bitmap of this window (press Ctrl+T).
   - **1.2** Click OK to cancel the import process.
2. For each packet trace listed in the warning dialog box, do the following:
   - **2.1** Choose File > Open Packet Trace(s) > In Trace Explorer.
   - **2.2** Select the packet trace to open.
   - **2.3** In the Trace Explorer window, choose Edit > Include All.
   - **2.4** In the Trace Explorer window, choose File > Remove TCP Segmentation Offloading…

     ➥ A file browser appears and prompts for the location and name of the new packet trace. This new file will include all traffic in the original file, except for the removed offloading data.
   - **2.5** Specify the location and filename (for example, `<original_filename>_SEGMENTED.appcapture`).
3. Perform the original import, using the new "segmented" packet trace.

End of Procedure 7-3

What is TSO?

TCP segmentation offloading (also referred to as *large segment offloading*, or LSO) is a technique for reducing CPU overhead of TCP/IP on fast networks.

Before a host sends large amounts of data, it must divide the data into smaller segments that can pass through all the network elements (such as routers and switches) between the source and destination host.

This process is referred to as segmentation. Often the TCP protocol on the host computer segments the data. TCP Segmentation Offloading occurs when TCP offloads segmentation to the network card.

Why Did This Message Appear?

The capture agent (or a similar capture tool) records the packet data before it is passed to the network card where it is segmented.

The warning message appears because the packet trace recorded a packet whose length was greater than the threshold of 9,500 bytes. (You can configure this threshold using the “TCP Segmentation Offloading Threshold” preference.)

Frequently when TSO is present, the capture agent might not capture the entire payload since the default maximum packet size is 2000 bytes. If this is the case, the warning mentions that one or more packets were sliced and you should use Capture Manager to increase the maximum packet size for the capture agent.

Why is This a Problem?

If the data is not re-segmented, the import engine cannot match the dataful packets and their corresponding ACKs accurately; as a result, the Transaction Analyzer model will not be as accurate as possible.

For example, suppose a packet trace recorded the following situation:

- Host A had TSO enabled and sent one “logical” 10Kb packet to host B.
- The network card segmented the packet into N physical packets and then transmitted them.
- When host B received the N physical packets, it returned multiple ACKs.

This sequence will *not* be consistent with the data that AppTransaction Xpert believes to have been sent.

If host B does not have TSO enabled, then consider what will happen when AppTransaction Xpert tries to merge the packets from the file captured on host A with the file captured on host B.

Host A Packet Trace (TSO enabled):

A -> B = N packets (due to TSO, M applications messages become N physical packets on the wire)
B -> A = X packets

Host B Packet Trace (no TSO):

A -> B = M packets (where N > M)
B -> A = X packets (Recall, TSO ONLY effects packets SENT.)

The result is that, when AppTransaction Xpert tries to merge the two packet traces, it will not be able to match all packets even though all packets were captured on both sides.

Related Topics

- *Trace Explorer*