LiveAction®

Omnipeek

Getting Started Guide

LiveAction, Inc.
960 San Antonio Road, Ste. 200
Palo Alto, CA 94303, USA
+1 (888) 881-1116
https://www.liveaction.com

20220819-GSG-OP222a

Contents

Introduction

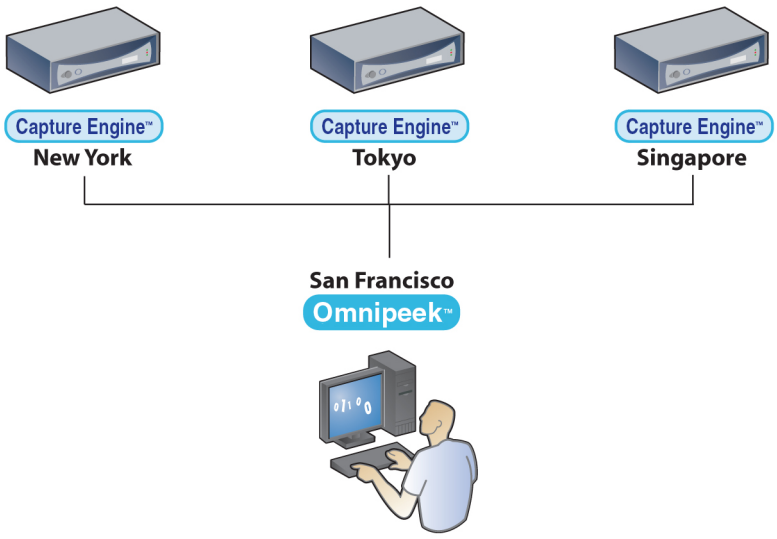
Welcome to Omnipeek, the network analyzer and software console for distributed network analysis from LiveAction!

Omnipeek as a portable analyzer

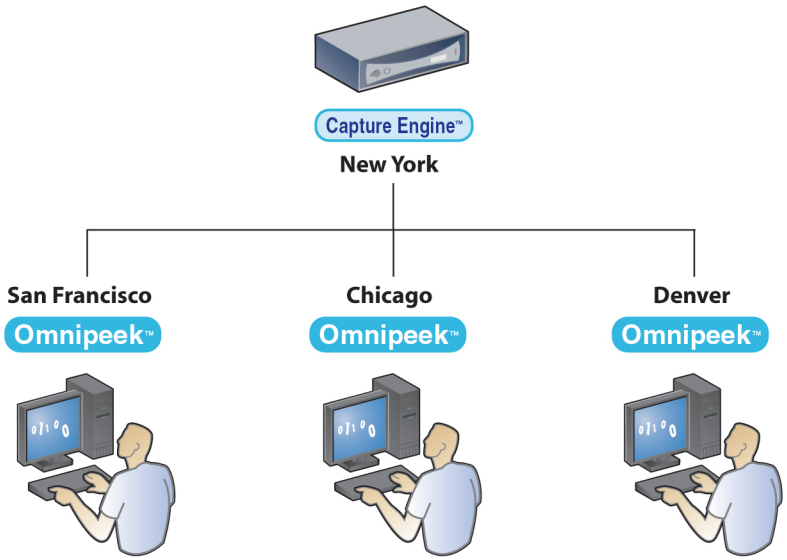
As a portable analyzer, Omnipeek offers an intuitive, easy-to-use graphical interface that engineers can use to rapidly analyze and troubleshoot enterprise networks. Omnipeek supports local captures from multiple interfaces and data collection from any network topology, including 1 Gigabit and 10 Gigabit networks, wireless networks, and local matrix switches.

Omnipeek with distributed Capture Engines

As a software console for Capture Engines, Omnipeek can also manage and interact with an unlimited number of Capture Engines performing independent capture and analysis at any location across the network.



Omnipeek allows network engineers to troubleshoot problems and perform statistical analysis on remote segments from a single location, as shown in the diagram above. A single Capture Engine can also link to multiple installations of Omnipeek, allowing simultaneous connection and collaboration, as shown below.



The separately purchased Capture Engines have no user interface of their own. Capture engines rely on Omnipeek to provide a user interface through the **Capture Engines** window. For more information, see Chapter 2, *Using Omnipeek with Capture Engines*. See also the *Capture Engine for Omnipeek Getting Started Guide* that ships with the product or the online help in the Capture Engine Manager application.

Network forensics

Network forensics is the retrospective analysis of network traffic for the purpose of conducting an investigation. You can use Omnipeek and the Capture Engines to capture, store, and data mine large volumes of traffic data in order to investigate items such as network problems, security attacks, HR policy violations, and more.

See Chapter 4, *Forensic Search* or online help for information on how to perform a forensic search on your own network.

Voice and video over IP analysis

Voice and video over IP is available for call signaling and media analysis in the **Voice & Video** views of capture windows, providing simultaneous analysis of voice and video data traffic with subjective and objective quality metrics. For more information on voice and video analysis, see the *Omnipeek User Guide* or online help.

Compass dashboard

The Omnipeek **Compass** dashboard provides an interactive forensics view of key network statistics, which can be graphed, dynamically interacted with, and reported on. With its unique ability to aggregate traffic from multiple segments, the **Compass** dashboard provides network engineers with more visibility and insight into their networks.

The **Compass** dashboard offers both real-time and post-capture monitoring of high-level network statistics with drill down capability into packets for the selected time range. Using the **Compass** dashboard, multiple files can be aggregated and analyzed simultaneously. For more information, see *Compass dashboard* on page 39.

Multi segment analysis

Multi-Segment Analysis (MSA) provides visibility and analysis of application flows across multiple network segments, including network delay, packet loss, and retransmissions. It can quickly pinpoint problems and their root causes across multiple segments, bring problematic flows together, and create an analysis ses-

sion, report anomalies, and provide graphical visualization of multiple segments across the network. For more information, see Chapter 9, *Multi-Segment Analysis*.

System requirements

The system requirements for Omnipeek are:

- Windows 11, Windows 10, Windows 8.1 64-bit, Windows 7 64-bit, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008 R2 64-bit

> **Note** For Windows 7 and Windows Server 2008 R2, SHA-2 code signing is required to run Omnipeek. Typically, for users that are updated automatically using Microsoft Update, this is installed automatically; otherwise, you will need to install the SHA-2 update manually. See Microsoft *KB3033929*.

Omnipeek supports most rack mount, desktop and portable computers as long as the basic system requirements to run the supported operating systems are met. Depending on traffic and the particular usage of Omnipeek, the requirements may be substantially higher.

The following system is recommended for Omnipeek:

- Intel Core i3 or higher processor
- 4 GB RAM
- 40 GB available hard disk space

Factors that contribute towards superior performance include high speed CPU, number of CPUs, amount of RAM, high performance disk storage subsystem (RAID 0), and as much additional hard disk space as is required to save the trace files that you plan to manage.

Supported operating systems require users to have Administrator level privileges in order to load and unload device drivers, or to select a network adapter for the program's use in capturing packets. For more information, please see our Web site at *https://www.liveaction.com/products/*.

Supported adapters and drivers

To analyze 10 Gigabit, Gigabit, or wireless traffic, a supported network analyzer card (e.g., LiveAction capture adapters) or wireless LAN adapter is required for Omnipeek. For the most recent information on network adapter cards and drivers, please visit *https://www.liveaction.com/products/*.

For information on configuring wireless channels and security, and Gigabit hardware profiles, in Omnipeek and the Capture Engines, please refer to the *Omnipeek User Guide* or online help.

Installing Omnipeek

To install Omnipeek:

1. Run the Omnipeek installer (e.g., *Omnipeek_xx.x.x.msi*). The installer removes any previous versions of Omnipeek.
2. Follow the installation instructions that appear on the screen.

   During installation you are asked to enter a valid product key. When prompted, you can select from the following:

   - **Automatic**: The installer uses your Internet connection to send an encrypted message to an activation server, which retrieves and installs a license file.
   - **Manual**: The installer guides you through generating a license file through a web page. Follow the instructions to access the web activation page, fill in the required information, and you are provided with a license file. The installer then guides you through installing the license file.

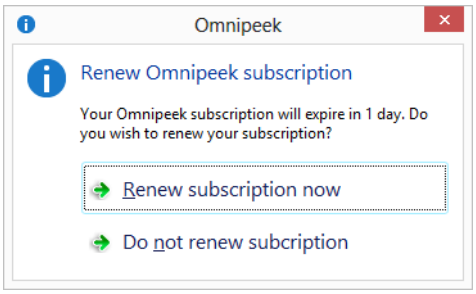
For more information about the product activation process, please see our website at: *https://www.liveaction.com/support/frequently-asked-questions/*.

3. When the Installer has finished installing the program files, you can choose to view the *Readme* or launch the program.

Note The Capture Engine Manager is installed by default with Omnipeek. This application lets you configure and update settings for the separately purchased Capture Engines. For information, see the *Capture Engine for Omnipeek Getting Started Guide* or the online help in the Capture Engine Manager application.

Renewing or upgrading subscription versions of Omnipeek

If you are using a subscription version of Omnipeek, when your subscription is at least 30 days from expiring, and whenever you start Omnipeek, you are prompted to renew your Omnipeek subscription with a dialog similar to the following:



- Click *Renew subscription now* to open the Omnipeek activation dialog where you can renew your existing license, or update to a new license.
- Click *Do not renew subscription* to continue to use Omnipeek until your subscription expires.

Installing a Capture Engine

For complete instructions on how to install, configure, and update software and settings for Capture Engines, see the *Capture Engine for Omnipeek Getting Started Guide* that ships with the Capture Engine.

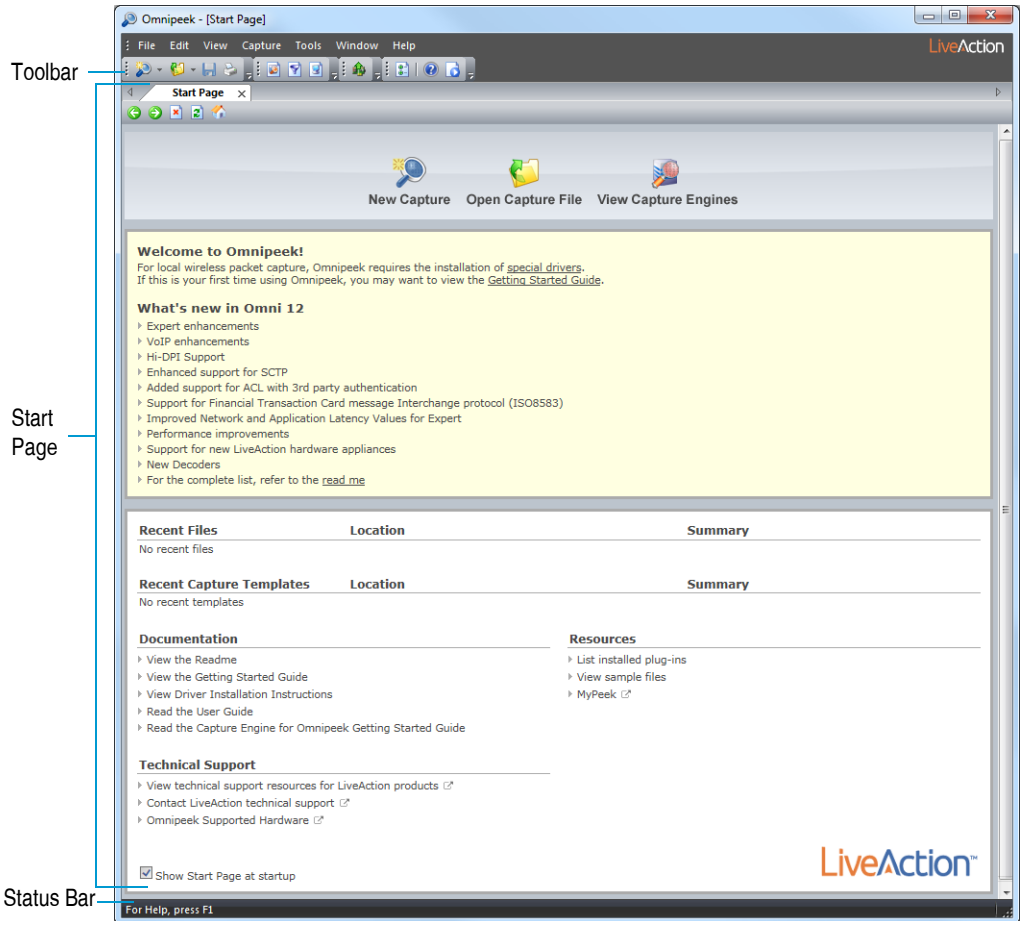
Main program window and Start Page

To start Omnipeek:

- On the **Start** menu, click **LiveAction Omnipeek**.

  The main program window and Start Page appears.

The parts of the main program window are described below.



- *Toolbar:* Provides buttons for frequently-used tasks in Omnipeek. To display different toolbars or to customize toolbar options, on the **View** menu, click **Toolbars**.
- *Start Page:* Provides buttons for creating a new capture, opening saved capture files, and viewing the Capture Engines window. Additionally, the *Start Page* lists 'What's new' in the version of Omnipeek, and also provides links to useful resources, both local and online.
- *Status Bar:* Shows brief context-sensitive messages on the left and the current monitor adapter on the right. To toggle the display of the status bar, on the **View** menu, click **Status Bar.**

Using Omnipeek with Capture Engines

If you are using Omnipeek as a console for distributed Capture Engines, you will need to connect to the Capture Engines from the **Capture Engines** window in Omnipeek. (If you are using Omnipeek as a portable network analyzer only, and not as a console for distributed Capture Engines, you do not need to review this section.)

Capture Engines let you capture and analyze data at any location across the network. Capture Engines perform real-time network analysis from the Omnipeek console on traffic from one or more network interfaces, including Ethernet, 802.11 a/b/g/n/ac wireless, 1 Gigabit, and 10 Gigabit.

The **Capture Engines** window in Omnipeek lets you view and interact with Capture Engines, which have no user interface of their own.

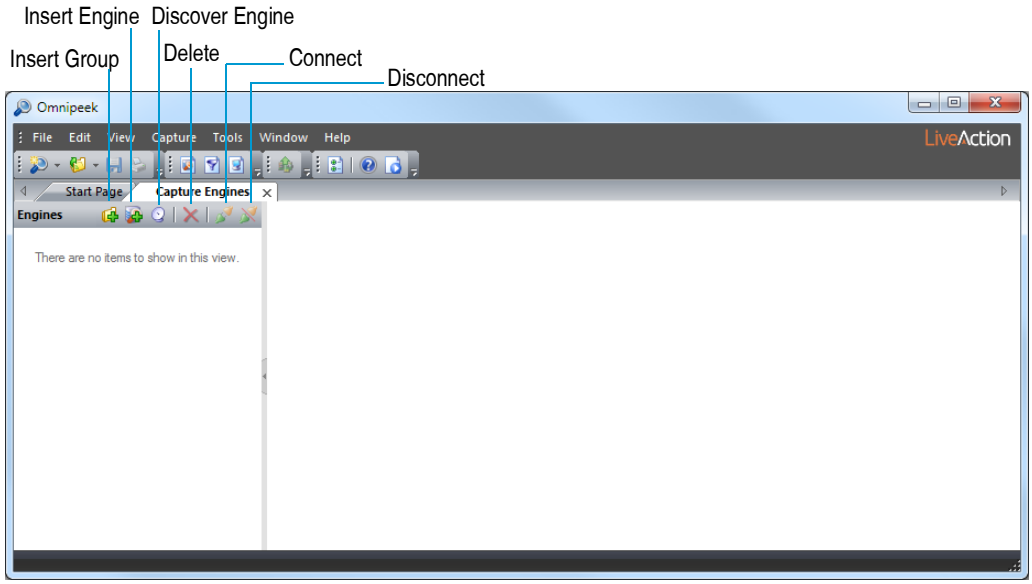
Displaying the Capture Engines window

Do one of the following to display the Capture Engines window:

- On the Start Page, click **View Capture Engines**
- On the **View** menu, click **Capture Engines**

The **Capture Engines** window appears.

Note Both Omnipeek and Capture Engine Manager maintain the same list of Capture Engines. Making a change in either program automatically updates the list in the other program.

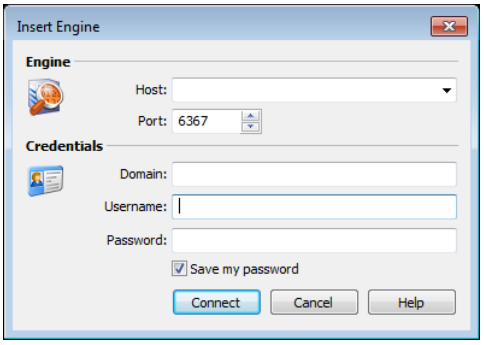


Connecting to a Capture Engine

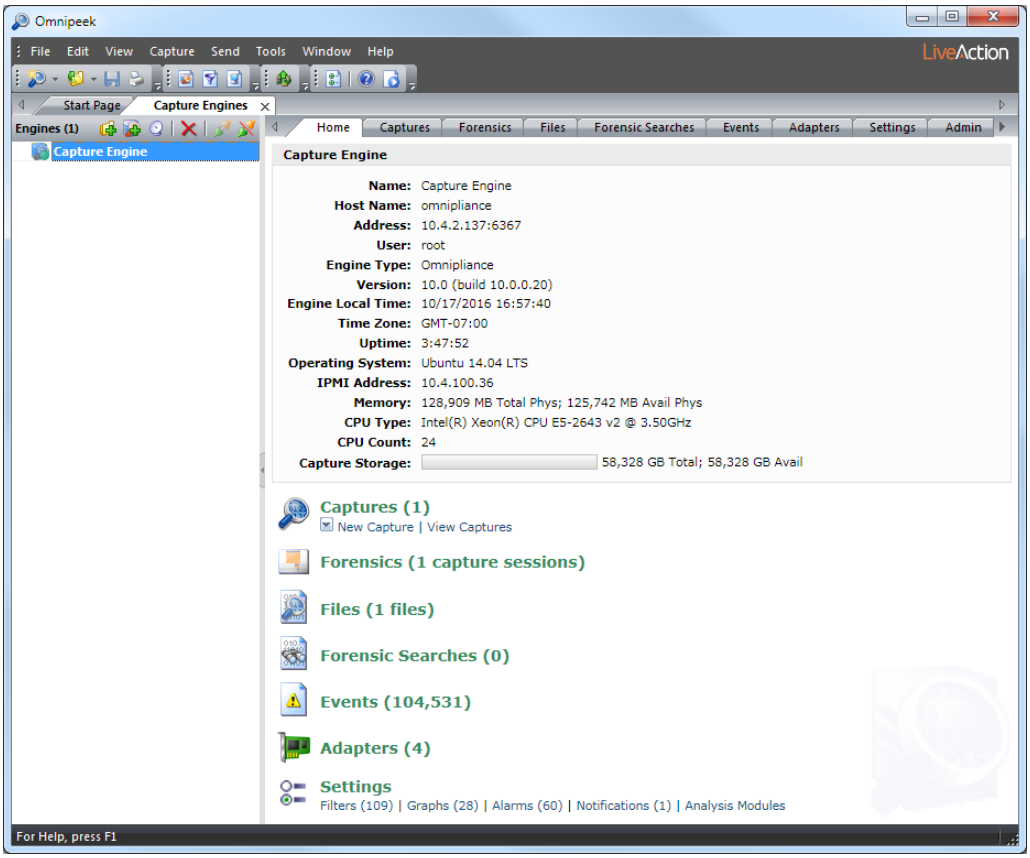
In order to view packets and data from a Capture Engine, you must first connect to the Capture Engine from the **Capture Engines** window.

To connect to a Capture Engine:

1. From the **Capture Engines** window, click *Insert Engine*. The **Insert Engine** dialog appears.

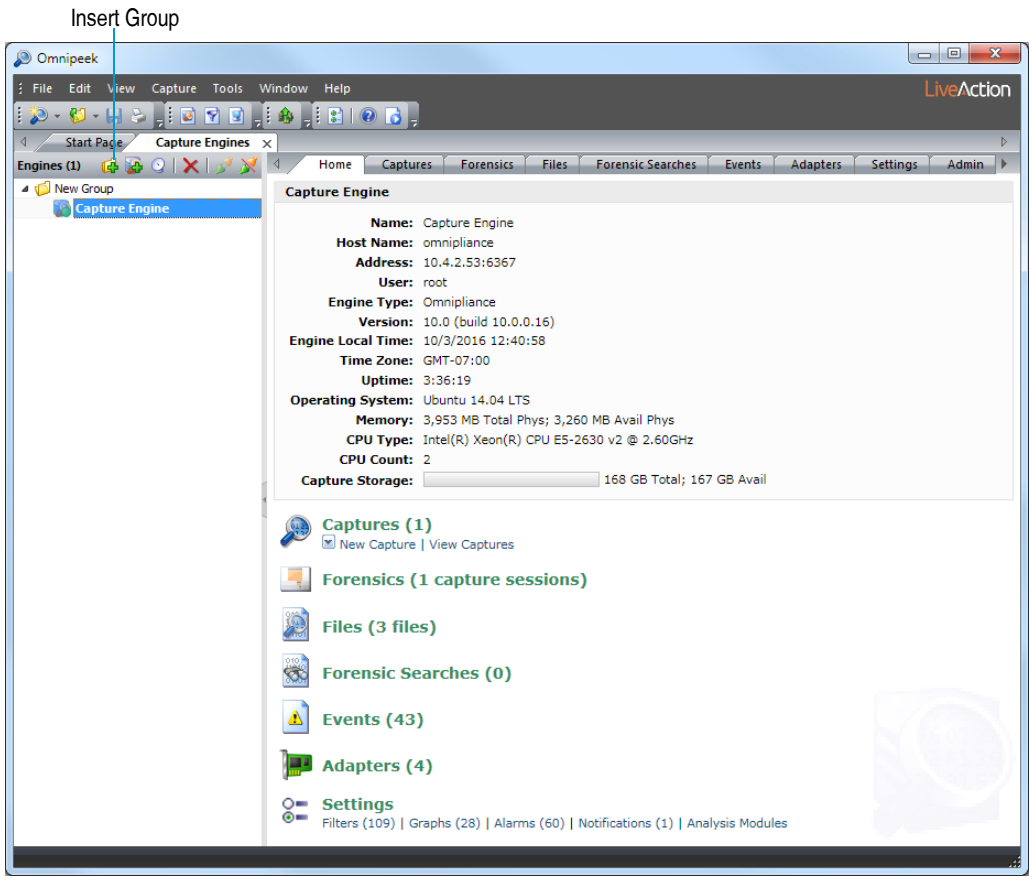


2. Complete the dialog:
   - *Host:* Enter the IP address of the Capture Engine that you want to connect to.
   - *Port:* Enter the TCP/IP Port used for communications. Port 6367 is the default port for the LiveAction Capture Engine.
   - *Domain:* Type the Domain for login to the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
   - *Username:* Type the Username for login to the Capture Engine.
   - *Password:* Type the Password for login to the Capture Engine.
3. Click **Connect**. When the connection is established, the Capture Engine appears in the **Capture Engines** window.



Tip You can add multiple engines to the **Capture Engines** window by clicking **Insert Engine**.

4. Click **Insert Group** to add a new group of engines to the **Capture Engines** window. A new group folder appears.



5. Select the Capture Engine group folder and click **Insert Engine** to add a Capture Engine to the group.

The Capture Window

Capture windows are the main interface for presenting traffic analysis information about your network. Omnipeek lets you create capture windows for local captures, as well as remotely from multiple interfaces to an unlimited number of distributed Capture Engines.

You can create multiple configurable capture windows, each with its own selected adapter and its own capture settings. The number of capture windows you can have open at one time is limited only by the amount of available system resources.

When configuring a capture window's capture settings, keep in mind that the window's capture performance can be directly related to the number and type of capture options that you have enabled. For example, enabling more options may give you more data, but may come at the price of a greater likelihood of not capturing all the data.

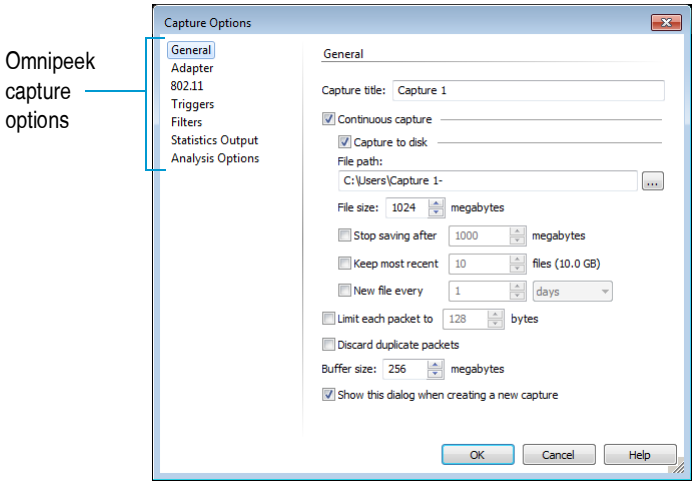
The things that determine how much data (and therefore how many capture options) a capture can handle is determined by the system memory and CPU power of the Omnipeek or Capture Engine computer, the amount and kind of data that is being captured, and the number of capture options and analysis modules that are enabled. Enabling capture options, such as *Capture to disk*, *Expert Analysis*, and *Graphs*; and enabling an analysis module such as *VoIP Analysis* consumes much more machine resources than others.

Creating an Omnipeek capture

To create an Omnipeek capture:

1. Do one of the following to start a new capture:
   - Click **New Capture** on the Start Page
   - On the **File** menu, click **New Capture...**

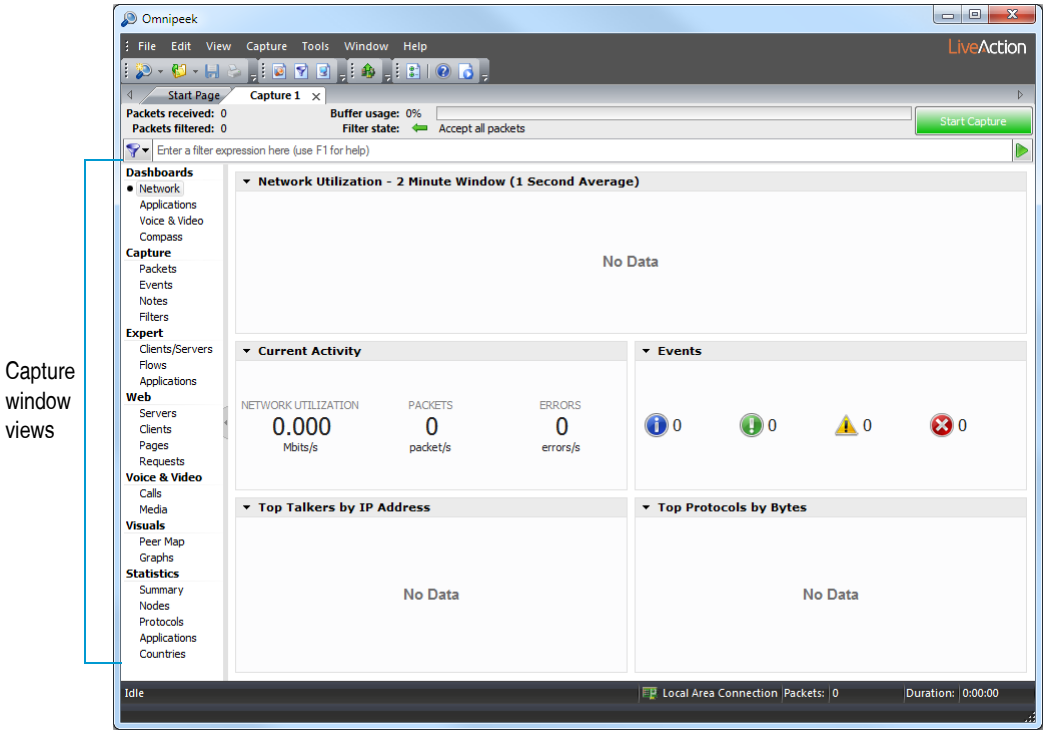
   The **General** options of the Omnipeek **Capture Options** dialog appears.



2. Configure the **General** options.
3. Choose an adapter in the **Adapter** options.

Note Click **Help** on the dialog for more information on how to configure these options. For a description of other configuration options, see the *Omnipeek User Guide* or online help.

4. Click **OK**. A new Omnipeek capture window appears.



5. Click **Start Capture** to begin capturing packets. **Start Capture** changes to **Stop Capture** and traffic statistics begin to populate the **Network** dashboard of the capture window.
6. Click the capture window views in the navigation bar to view captured packets, expert and statistical analysis of the data, the Peer Map display, and more.
7. Click **Stop Capture** to end the capture. You can choose to save, discard, or resume the capture.

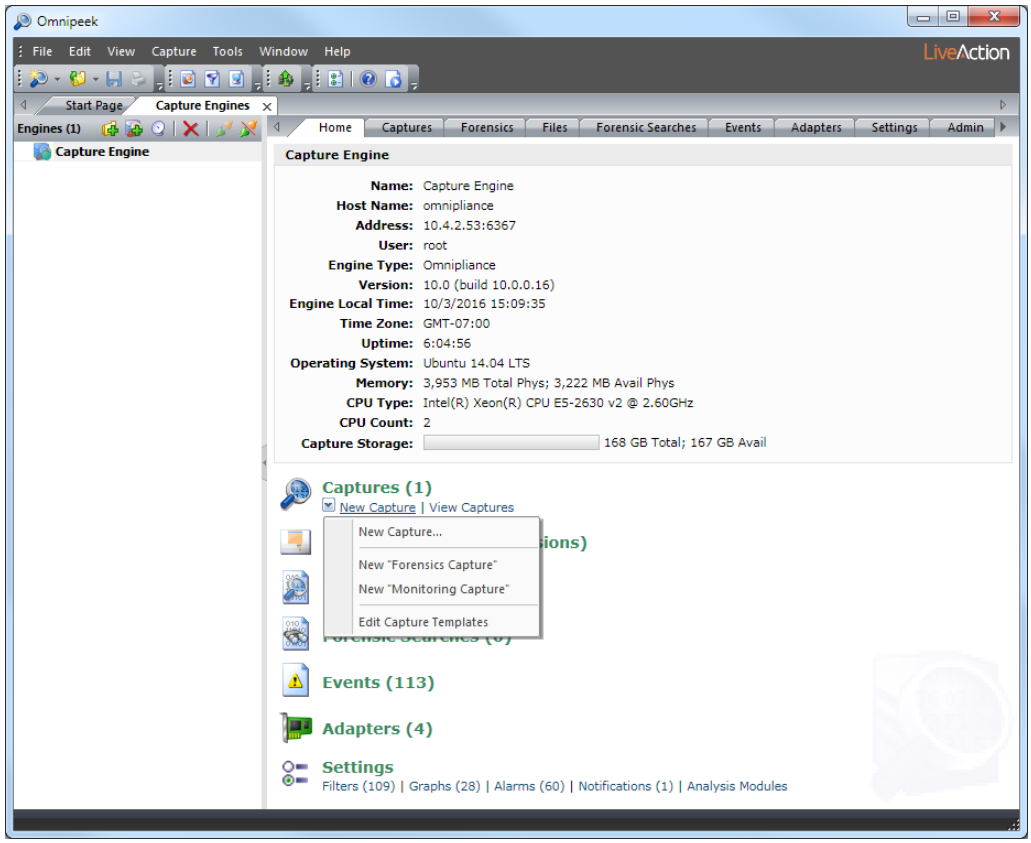
Tip To resume capturing from where you left off, hold down the *Alt* key and click **Start Capture**. To empty the capture buffer and start a new capture, simply click **Start Capture** again.

Creating a Capture Engine capture

To create a Capture Engine capture:

1. Do one of the following to open the **Capture Engines** window:
   - On the Start Page, click **View Capture Engines**
   - On the **View** menu, click **Capture Engines**

   The **Capture Engines** window appears.
2. Connect to a Capture Engine. (To connect to a Capture Engine, see *Connecting to a Capture Engine* on page 6.) The *Home* tab for the Capture Engine appears.



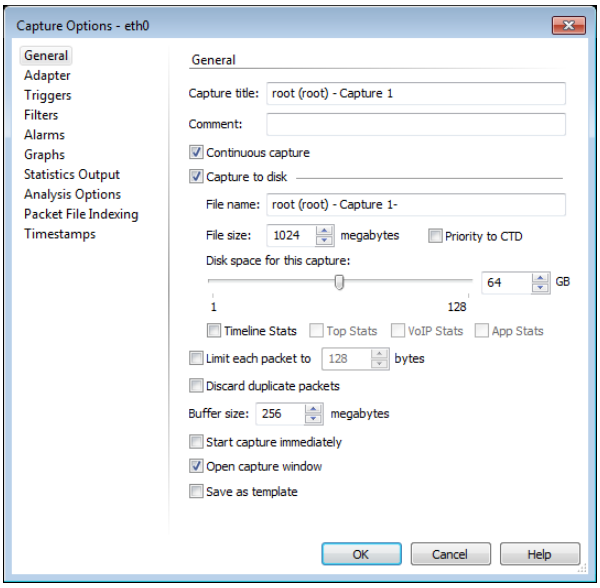
3. From the *Home* tab, click *New Capture* and select the type of capture that you would like to create:

Note You can also select the options below from the **Insert** drop-down list available from the *Captures* tab, and from the *New Capture* options available from the *Adapters* tab.

- *New Capture...:* This option lets you create a new Capture Engine capture based on the capture settings that you define.
- *New "Forensics Capture":* This option lets you create a new Capture Engine capture based on a forensic capture template configured for post-capture forensic analysis.
- *New "Monitoring Capture":* This option lets you create a new Capture Engine capture based on a monitoring capture template configured to view higher level expert and statistical data in a continuous real-time capture.
- *Edit Capture Templates:* This option opens the **Capture Templates** dialog and allows you to create new or edit existing capture templates.

The *General* options of the Capture Engine **Capture Options** dialog appears.

Capture Engine General Options

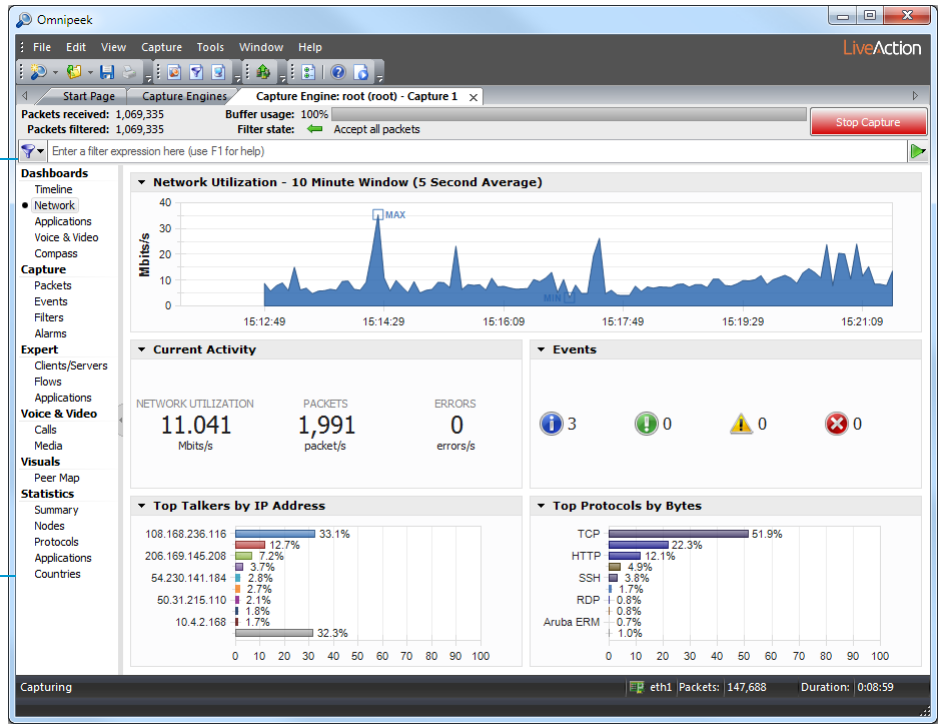


4. Configure the *General* options.
5. Choose a capture adapter in *Adapter* options.

Note Click **Help** on the dialog for more information on how to configure these options. For a description of other configuration options, see the *Omnipeek User Guide* or online help.

6. Click **OK**. A new Capture Engine capture window appears.

Capture window views



7. Click **Start Capture** to begin capturing packets. **Start Capture** changes to **Stop Capture** and traffic statistics begin to populate the **Network** dashboard of the capture window.
8. Click the capture window views in the navigation bar to view captured packets, expert, and statistical analysis of the data, the Peer Map display, and more.

9. Click **Stop Capture** when you want to stop collecting packets into the Capture Engine capture buffer.

Note Users without permission to create or modify Capture Engine capture windows will find features grayed out, missing, or receive an error message indicating the task is not allowed. For details, see the *Capture Engine for Omnipeek Getting Started Guide*.

Opening saved capture files

Capture files, or trace files, are capture windows that were saved to a variety of supported capture file formats. You can open capture files to load and process packets back into *Omnipeek*.

Omnipeek capture files

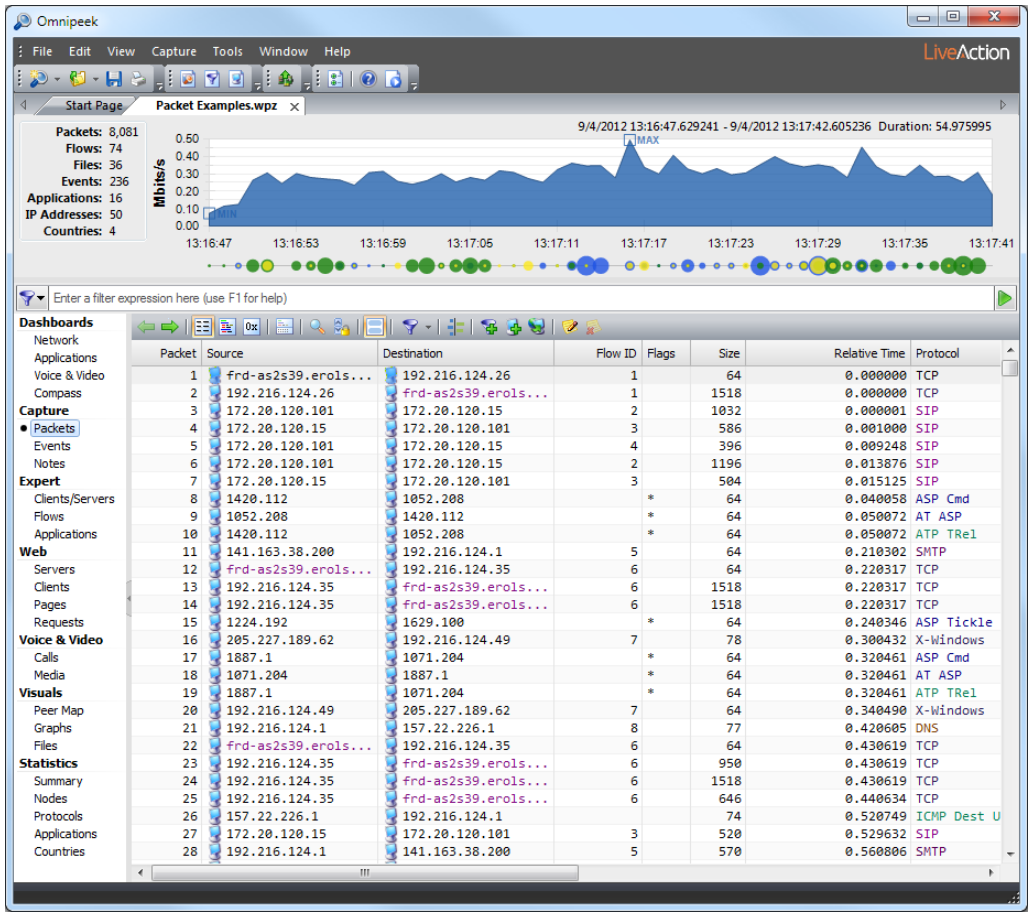
To open an Omnipeek capture file:

1. Do one of the following:
   - On the Start Page, click **Open Capture File**. The **Open** dialog appears.
   - On the **File** menu, click **Open**. The **Open** dialog appears.
2. Select the capture file and click **Open**.

Note When opening large files, a progress bar in the status bar of the file window appears displaying the progress of packet processing.

Tip From the **Open** dialog, you can click the **Filter** button to open the **Filter** dialog, which allows you to select both the filters and analysis options to apply to each of the files that you select to open. By applying one or more filters, you can greatly reduce the amount data you are opening to only the data you are interested in analyzing. For example, if you want to load only the packets from the files which match a particular IP address, you can create a simple filter from the dialog and then select that filter when opening the files.

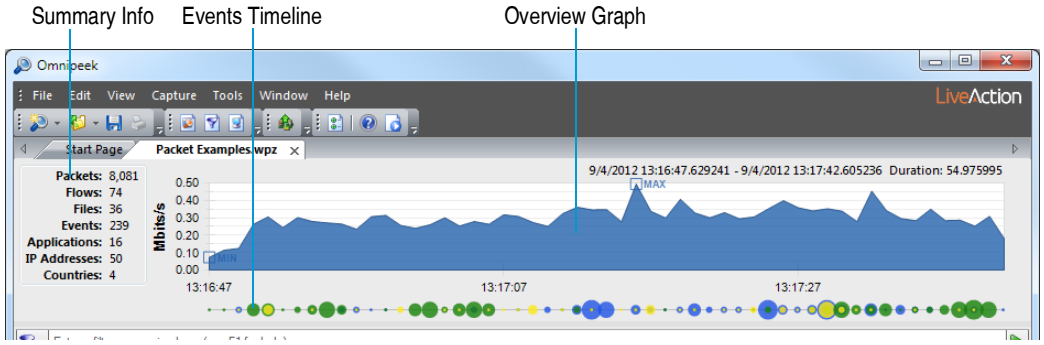
By disabling analysis options, you can free up system resources resulting in faster performance. These analysis options are typically displayed in the navigation pane of a capture window. Enabling/disabling analysis options is also available from the **Capture** menu (on the **Capture** menu, click **Analysis Options**).



3. Click the **Packets** view in the navigation pane.

Overview graph for capture files

Whenever you open a capture file in Omnipeek, an overview graph is displayed at the top of the files window. The overview graph allows you to 'zoom' in on a portion of a file by selecting a time range and reprocessing all statistics within the selected time range. The reprocessed statistics are then displayed in the lower half of the files window.



The overview graph is comprised of three parts:

- *Overview Graph*: The overview graph initially displays data for the entire capture file. When a selection is made by clicking inside the graph and dragging a desired time range, the displayed packets (and the analysis of those packets) are limited to the selected time range. The beginning and end of the selection can be dragged to expand or contract the selection range. Additionally, the selection can be dragged horizontally, moving it while leaving the duration constant.

- *Events Timeline*: The events timeline is a small line below the overview graph which visualizes the volume and severity of events in the capture file. It represents event counts by size (the larger the dot, the more events in that range), and color (representing the severity of those events). You can right-click inside the overview graph to show or hide the events timeline.
- *Summary Info*: The summary info located to the left of the overview graph displays the time range and various counts (packets, flows, files, events, applications, IP addresses, countries) in the capture file. When a selection is made in the overview graph, the summary info is updated and displays the counts for the selection, as well as the totals for the entire capture file.

Tip You can show/hide the Overview graph from the **View** menu: On the **View** menu, click **Overview**.

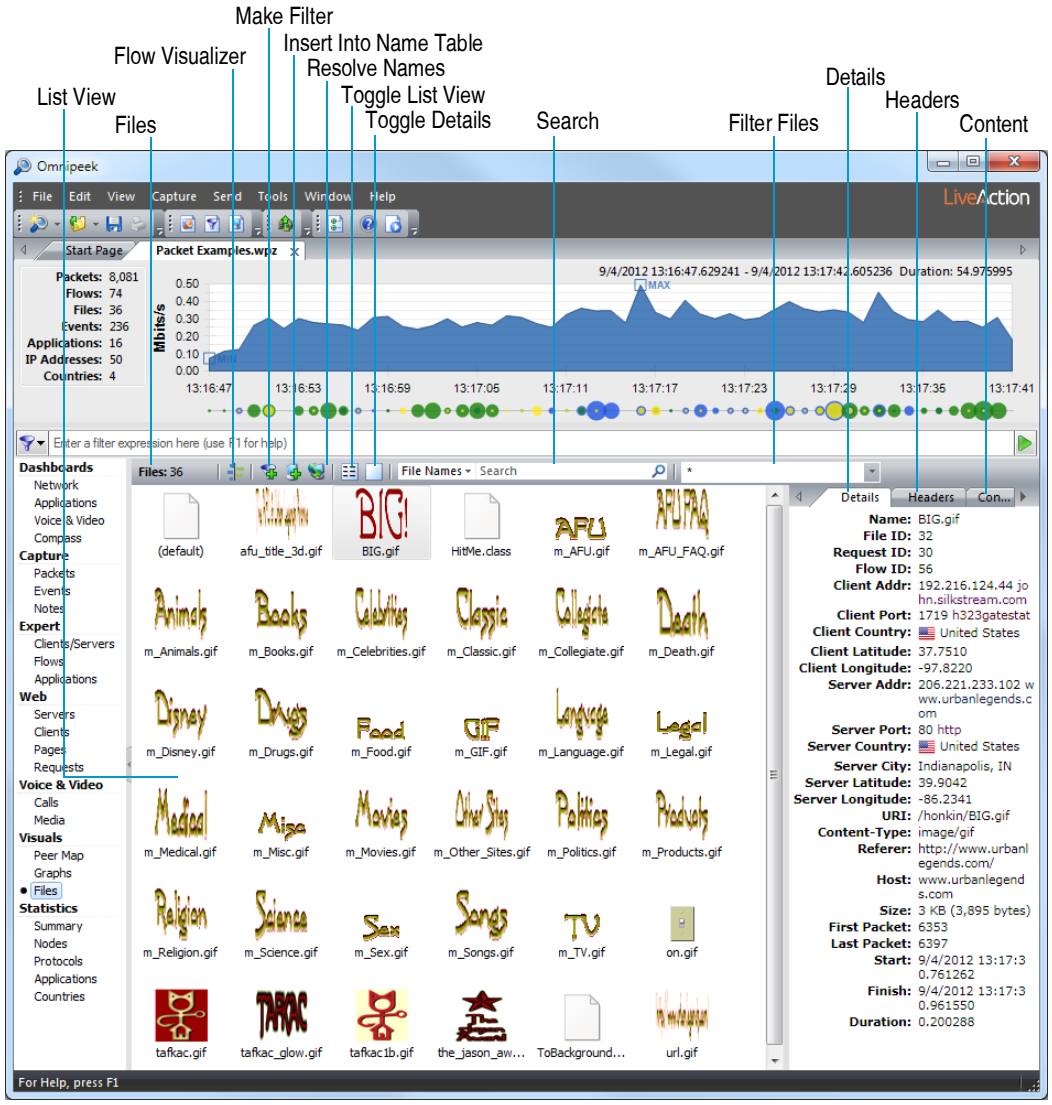
Right-click inside the overview graph for the following options:

- *Clear Selection*: Removes any selected time range from the overview graph and displays data for the entire capture file.
- *Network Utilization*: Displays the overview graph as network utilization counts.
- *Events*: Displays the overview graph as event counts.
- *Events Timeline*: Shows or hides the *Events timeline* from the display.
- *Column*: Displays the overview graph as a column graph.
- *Skyline*: Displays the overview graph as a skyline graph.
- *Area*: Displays the overview graph as an area graph.
- *Line*: *Area*: Displays the overview graph as an line graph.
- *Line/Points*: Displays the overview graph as an line/points graph.
- *Linear*: Displays the overview graph as a linear display.
- *Logarithmic*: Displays the overview graph as a logarithmic display.
- *Show Min/Max*: Displays the minimum and maximum values of overview graph.
- *Synchronize Events*: Updates the overview graph based on the current set of events in the **Events** view.

Working in the Files view

The **Files** view displays files extracted from reassembled HTTP payloads of capture files opened in Omnipeek. This view lets you quickly see the files that are being transmitted across your network. To narrow your search, you can even filter files by its content-type.

Note The **Files** view is not supported in Capture Engines.



The parts of the **Files** view are described below.

- *Files*: Displays the total number of files in the capture file.
- *List View*: Displays the files in the capture file.
- *Flow Visualizer*: Opens the selected file in a Flow Visualizer tab.
- *Make Filter:* Opens the **Insert Filter** dialog to create a filter based on the selected file.
- *Insert Into Name Table:* Opens a dialog to add the client and server node addresses of the selected file into the Name Table.
- *Resolve Names:* Checks the DNS server for a name to match the client and server addresses of the selected file.
- *Toggle List View*: Toggles the list view between the options below:
  - *Extra Large Icons*: Displays files in the list view as small icons. Images are displayed as the actual image, while other files are displayed with the icon corresponding to the content-type for the file. Hovering over a file in an icon mode displays a tooltip showing additional details of the file.
  - *Large Icons*: Displays files in the list view as large icons. Images are displayed as the actual image, while other files are displayed with the icon corresponding to the content-type for the file. Hovering over a file in an icon mode displays a tooltip showing additional details of the file.

    - *Details*: Displays files in the list view as a details list with multiple columns. You can click a column header to sort the files by that column. You can right-click a column header to add or remove columns. You can also view this information in the *Details* tab of the details pane.
- *Toggle Details*: Toggles the details pane to appear either below or to the right of the list view (or hidden completely). You can also resize the details pane by dragging the resize control located between the details pane and list view. The details pane consists of the following tabs:
    - *Details*: Displays various information about the selected file. You can also view this information in the list view by toggling the list view to the *Details* option. To copy any text within this tab to the clipboard, select the text, right-click, and click **Copy**.
    - *Headers*: Displays request and response headers for the selected file. To copy any text within this tab to the clipboard, select the text, right-click, and click **Copy**.
    - *Contents*: Displays file contents as an image, text, or binary data. You can right-click inside the tab to change the display mode to *Auto*, *Image*, *Text*, or *Binary*. Selecting *Auto* will pick the best mode depending on the type of file. In *Image* mode, at the top of the contents tab, a small area displays information about the image (proportions and color information). In *Text* mode, there are additional options to set the text encoding used. In *Binary* mode, there are additional options to change the display of data and offsets. To copy any text within this tab to the clipboard, select the text, right-click, and click **Copy**.
- *Search*: Allows you to search the list of files for the text string that you enter in the text box. You can search file names, request/response headers, or file contents by selecting the option from the drop-down list to left of the text box.
- *Filter Files*: Allows you to filter the file list by content-type. The drop-down list contains common content-types (for example, *image/**, *text/**). Additionally, you can type in any content-type (for example, *image/png*) to filter files by that content-type. This essentially acts as a display filter—only files which are of the type specified are displayed; non-matching files are hidden.

Forensic Search

Network forensics is the retrospective analysis of network traffic for the purpose of conducting an investigation. You can use Omnipeek to capture, store, and data mine large volumes of traffic data in order to investigate items such as network problems, security attacks, HR policy violations, and more.

From the **Capture Engine** window, you can perform network forensics analysis from the *Files* or *Forensics* tab of a connected Capture Engine. See *Forensic search from the Files tab* on page 18 and *Forensic search from the Forensics tab* on page 21.

Note You can also perform forensic analysis directly from a 'Forensics Capture' window. See *Forensic search from the 'Forensics Capture' window* on page 27.

Forensic search from the Files tab

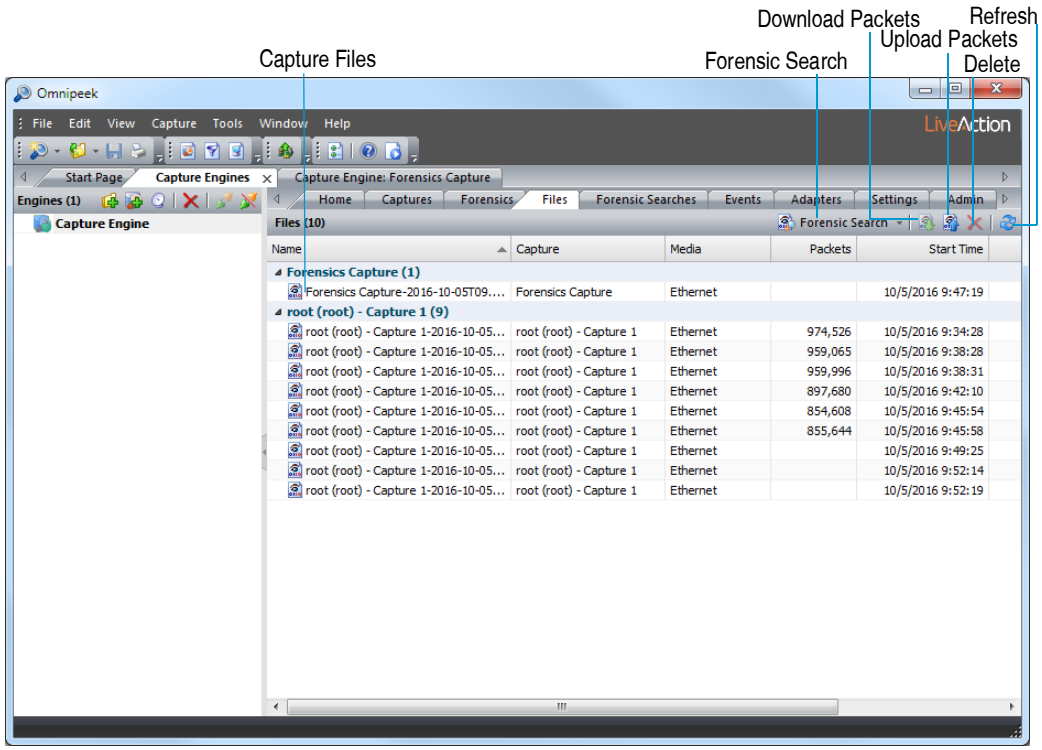
The *Files* tab in the **Capture Engines** window displays a listing of all the capture files saved to the Capture Engine. Performing a forensic search from the *Files* tab lets you sort through hours or even days worth of network traffic, from one or more Capture Engine capture files, for specific data you wish to analyze further.

Important! One or more capture files saved to the Capture Engine computer are required before you can perform a forensic search.

To perform a forensic search from the Files tab:

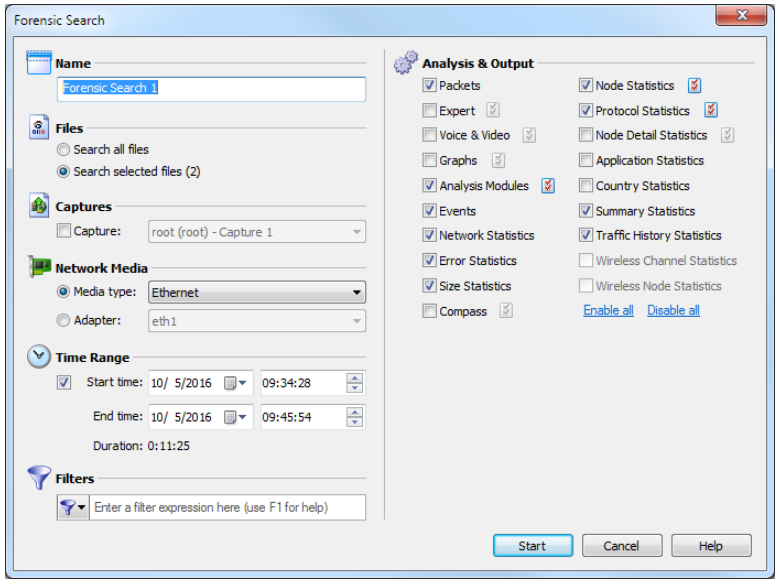
1. From the **Capture Engines** window, select the *Files* tab of a connected Capture Engine.

Tip Right-click inside the list of files for additional options for performing a forensic search, grouping files, uploading and downloading packets, deleting files, synchronizing files to the file system on the hard disk, and refreshing the display.



2. Select one or more capture files you wish to search.
3. Click **Forensic Search** (or click the small down arrow next to **Forensic Search** and select the type of forensic search you wish to perform). The **Forensic Search** dialog appears.

Note Selecting one of the pre-defined types of forensic searches displays the **Forensic Search** dialog with the *Analysis & Output* options pre-configured for that type of forensic search. You can change any option prior to clicking **Start**.



4. Complete the dialog to specify the criteria for extracting data from the selected capture files:
   - *Name:* Enter a name for the forensic search.
   - *Files:* Choose one of the following:

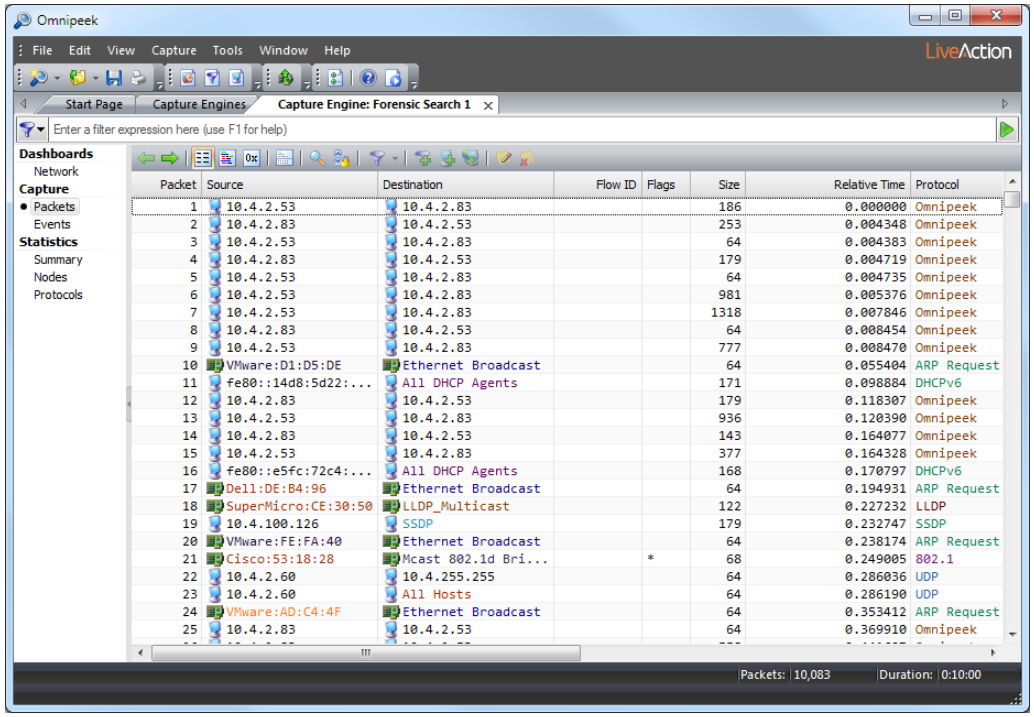
- *Search all files:* Select this option to search through all of the files listed in the *Files* tab.
- *Search selected files:* Select this option to search through only the selected files in the *Files* tab.

- *Captures:* Select this option and then select the capture to search from those listed in the Capture column of the *Files* tab.
- *Network Media:* Choose one of the following:
  - *Media type:* Select this option and then select the media type to extract only the data of a specific media type.
  - *Adapter:* Select this option and then select the adapter to extract only the data captured by a specific adapter.
- *Time Range:* Select this option and then configure the start and end times to extract the data.
  - *Start time:* Set the start date and time for extracting data. Only the data captured between the start time and end time is extracted.
  - *End time:* Set the end date and time for extracting data. Only the data captured between the start time and end time is extracted.
  - *Duration:* Displays the amount of time between the specified start and end times.
- *Filters:* Click to select a filter from the display list. All packets will be accepted if no filters are applied to the forensic search.

  To create an advanced filter, click *Filters* and select *Insert filter*, *Insert Operator*, or *Insert Expression* from the display.
- *Analysis & Output:* Select one or more of the options to enable and display that particular view in the new **Forensic Search** window. For various *Analysis & Output* options that have additional configurable settings, click the submenu to the right of the option.

5. Click **Start**. A new **Forensic Search** window appears along with two progress bars at the top of the window. (Clicking **Stop** stops the search and then completes the processing of the packets.)

   Once the processing of the packets is complete, the progress bars go away and the new **Forensic Search** window is populated with the data found based on the criteria you selected above.



6. From the new **Forensic Search** window, you can further narrow down the data by performing any of the post-capture analysis methods described in the *Omnipeek User Guide*.

Forensic search from the Forensics tab

The *Forensics* tab in the **Capture Engines** window displays the capture sessions available on the Capture Engine. Performing a forensic search from the *Forensics* tab lets you select one of the capture sessions, display its data in the Timeline graph, and then perform a forensic search on specific parts of the data.

Important! One or more forensic captures on the Capture Engine are required before you can perform a forensic search from the *Forensics* tab.

To perform a forensic search from the Forensics tab:

1. From the **Capture Engines** window, select the *Forensics* tab of a connected Capture Engine. The *Forensics* tab displays the data currently available from the capture storage space of the Capture Engine.

The parts of the *Forensics* tab are described here:

- *Header Information*: The header information displays statistics for the capture session (data start time, data end time, duration, status, packets, packets dropped, adapter, etc.).
- *Top Talkers by IP Address*: This display shows a graph of top "talkers" on the network, broken out by node for the selected area in the Timeline graph below. You can right-click inside the display to display top talkers by *Physical Address*, *IP Address*, or *IPv6 Address*; or to select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the node.
- *Top Applications by Bytes*: This display shows a graph of top applications on the network for the selected area in the Timeline graph below. You can right-click inside the display to toggle the display with the Top Protocols display, or to select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the application.

- *Top Protocols by Bytes*: This display shows a graph of top protocols on the network for the selected area in the Timeline graph below. You can right-click inside the display to toggle the display with the Top Applications display, or to select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the protocol.
- *Timeline graph*: The Timeline graph displays the data of the selected capture session. Only one capture session at a time can be displayed inside the graph. By default, the graph shows network utilization in Mbits/s, but other statistics can be graphed as well by selecting the *View* type.

  Here are descriptions of other parts of the Timeline graph:

  - Right-click inside the graph to perform a forensic search (see *Forensic search* below), download selected packets to a capture file, refresh the window, or choose a different graph format: *Bar*, *Stacked Bar, Skyline, Area*, *Stacked Area, Line*, *Line/Points*, *Linear*, and *Logarithmic*. Additionally, you can also toggle displaying the minimum and maximum points for each series on the graph.
  - Mouse over a data point in the graph to view a tooltip displaying timestamp and size information (e.g., time and rate, time and packet size, etc.).
  - Any time there is more data than can be displayed on the screen, a scroll bar appears below the graph and allows you to view different points of time in the graph. (If the *Time window* is set to *Automatic*, the scroll bar will never appear.)
  - If the *Time window* is set to anything other than *Automatic*, a scroll bar appears below the graph and allows you to view different points of time in the graph.
- *View type*: Select the type of statistics to display in the Timeline graph. You can select from:
  - *Network Utilization (Mbits/s)*
  - *Network Utilization (Packets/s)*
  - *Unicast/Multicast/Broadcast*
  - *Packets sizes*
  - *VLAN/MPLS*
  - *Protocols (Mbits/s)*
  - *Protocols (Packets/s)*
  - *Call Quality*
  - *Call vs. Network Utilization*
  - *Wireless Packets (Packets/s)*
  - *Wireless Retries (Packets/s)*

Note To display statistics for a *Call Quality* or *Call vs. Network Utilization* view type, the *VoIP Stats* option must be selected when you first create the capture and configure the *General* options of the **Capture Options** dialog.

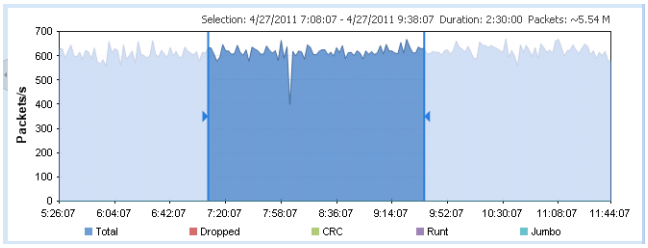
- *Time window*: Select the time interval to display in the Timeline graph. By default, *Automatic* is selected to display the optimum window based on the available data. Intervals from *5 Minutes (1 Sec. Avg.)* to *24 Hours (5 Min. Avg.)* are also available.
- *Forensic search*: Click to display the **Forensic Search** dialog where you can adjust the forensic search settings. Click the small down arrow next to **Forensic Search** to display custom or pre-configured settings for performing a forensic search. You can change any option prior to clicking **Start**:
  - *Custom*: Creates a **Forensic Search** window based on the customized settings that you configure.
  - *Overview*: Creates a **Forensic Search** window based on settings that display an overview of the selected data in the capture session.

  - *Packets*: Creates a **Forensic Search** window containing a packets-only view.
  - *Expert*: Creates a **Forensic Search** window based on settings that are optimized for *Expert* analysis.
  - *Voice & Video*: Creates a **Forensic Search** window based on settings that are optimized for *Voice & Video* analysis.
- *Download Packets*: Click to download the packets from the selected capture session, in the selected time range.
- *Refresh*: Click to refresh the screen. For an active capture session, you can also set an automatic refresh interval by selecting an interval from the drop-down list to the right of **Refresh**.
- *Nested tabs*: There are three nested tabs available from within the *Forensics* tab: *Timeline*, *Storage*, and *Details*. Each tab allows you to view and select the capture data you wish to search in various formats. The *Timeline*, *Storage*, and *Details* tabs are described in detail below.

2. From any of the nested tabs, click (double-click from the *Details* nested tab) the capture session you wish to search. The selected capture session is displayed in orange to indicate it is selected, and the data for the capture session is loaded into the *Timeline* graph at the top.

Important! A *session* represents a contiguous period of time when packets are captured from a particular interface. A session is created each time you start a capture. A capture can have multiple sessions, and each session can be separated by periods of inactivity. Forensic analysis can then be performed on each session. *Sessions* are displayed in any of the nested tabs available from the *Forensics* tab.

3. In the Timeline graph, drag to select the area of the selected capture you wish to search. If no area of the graph is selected, the entire capture is selected by default.

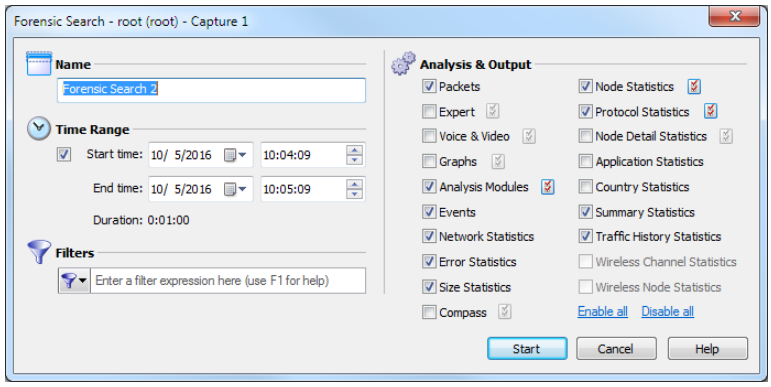


Note The packet count displayed above the Timeline graph is an approximation of the packets currently selected.

Tip You can adjust the exact time range from the **Forensic Search** dialog.

4. Click **Forensic Search** (or click the small down arrow next to **Forensic Search** and select the type of forensic search you wish to perform). The **Forensic Search** dialog appears.

Note Selecting one of the pre-defined types of forensic searches displays the **Forensic Search** dialog with the *Analysis & Output* options pre-configured for that type of forensic search. You can change any option prior to clicking **Start**.



5. Complete the dialog to specify the criteria for extracting data from the selected capture:

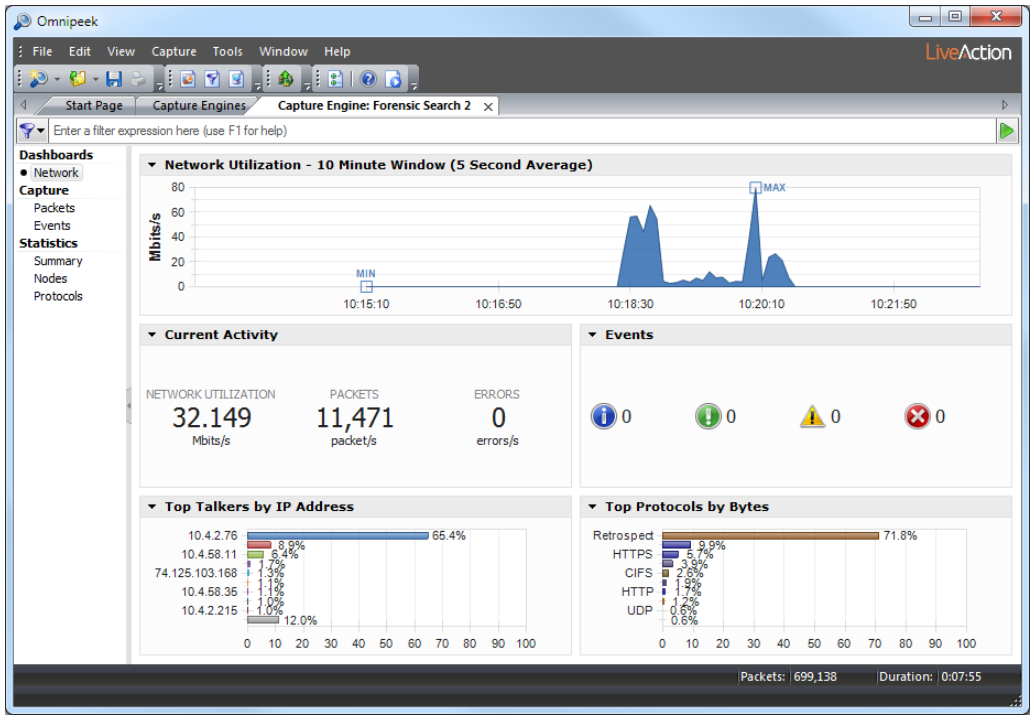
> **Note** If you wish to perform a forensic search on a capture session that is active and is currently capturing packets, we recommend that you stop the capture first before performing the forensic search. If you continue without stopping the capture first, make sure to clear the *Packets* check box in the **Forensic Search** dialog before clicking **OK**.

- *Name:* Enter a name for the forensic search.
- *Time Range:* Select this option and then configure the start and end times to extract the data.
  - *Start time:* Set the start date and time for extracting data. Only the data captured between the start time and end time is extracted.
  - *End time:* Set the end date and time for extracting data. Only the data captured between the start time and end time is extracted.
  - *Duration:* Displays the amount of time between the specified start and end times.
- *Filters:* Click to select a filter from the display list. All packets will be accepted if no filters are applied to the forensic search.

  To create an advanced filter, click *Filters* and select *Insert filter*, *Insert Operator*, or *Insert Expression* from the display.
- *Analysis & Output:* Select one or more of the options to enable and display that particular view in the new **Forensic Search** window. For various *Analysis & Output* options that have additional configurable settings, click the submenu to the right of the option.

6. Click **Start**. A new **Forensic Search** window appears along with two progress bars at the top of the window. (Clicking **Stop** stops the search and then completes the processing of the packets.)

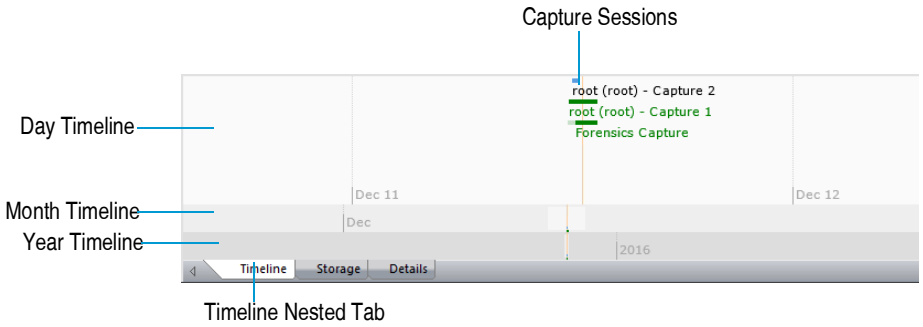
Once the processing of the packets is complete, the progress bars go away and the new **Forensic Search** window is populated with the data found based on the criteria you selected above.



7. From the new **Forensic Search** window, you can further narrow down the data by performing any of the post-capture analysis methods described in the *Omnipeek User Guide*.

Timeline nested tab

The *Timeline* nested tab has three bands of timelines (Day, Month, Year) that are used to display the capture sessions available from the storage space on the Capture Engine. You can select a capture session from the day band to display the session in the Timeline graph above.



Here are some useful notes for using the *Timeline* nested tab:

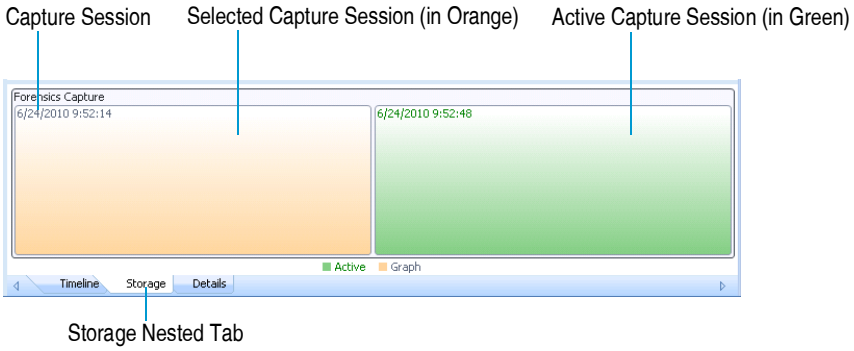
- Capture sessions are represented with a horizontal green or blue bar and the name of the main parent capture. Simply click a capture session to view its data within the Timeline graph above.
- Only one capture session at a time can be selected and displayed in the Timeline graph.
- A capture session that is highlighted with an orange vertical bar indicates it is currently selected. A capture session that has green colored text indicates it is currently active and is capturing packets.
- Capture sessions may be overwritten by another session in the same capture if the capture was created as a 'continuous capture,' and the session 'wraps' after exceeding the disk space allocated for the capture.

  If a capture session 'wraps,' the horizontal green or blue bar appears with a lighter color to indicate that capture sessions were overwritten. Any data that is overwritten is no longer available for analysis.

- Drag inside a timeline band to view different points of time within the timeline band. The other timeline bands will move accordingly.
- Right-click inside a timeline band to quickly move to various points within the timeline. You can select from:
  - *Go to Current*: Moves all three timeline bands so that the currently selected capture session is centered inside the display.
  - *Go to Now*: Moves all three timeline bands so that the current time is centered inside the display.
  - *Go to Earliest*: Moves all three timeline bands so that the earliest available capture session is centered inside the display.
  - *Go to Latest*: Moves all three timeline bands so that the latest available capture session is centered inside the display.

Storage nested tab

The *Storage* nested tab displays each capture session available from the storage space on the Capture Engine as a container nested within a larger parent container.

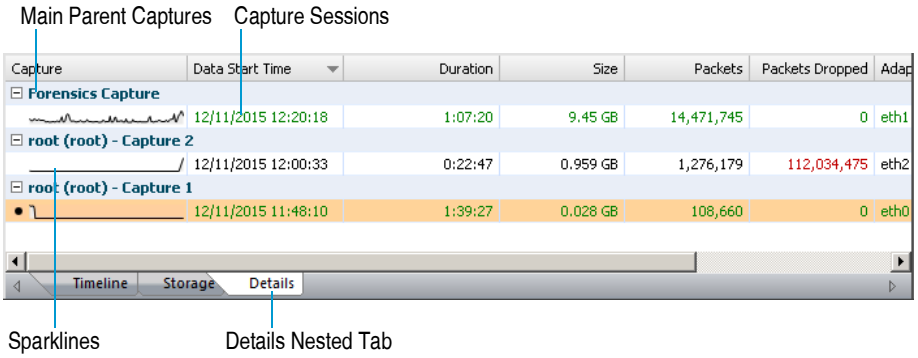


Here are some useful notes for using the *Storage* nested tab:

- A capture session that is colored orange indicates it is currently selected. A capture session that is colored green indicates it is currently active and is capturing packets.
- Capture sessions may be overwritten by another session in the same capture, if the capture was created as a 'continuous capture' and the session 'wraps' after exceeding the disk space allocated for the capture. When data from a capture session is overwritten with new data, the old data is no longer available for analysis.
- Only one capture session at a time can be selected and displayed in the Timeline graph.
- Mouse-over a capture session container to view a tooltip displaying details about the capture session.
- Right-click a capture session to display the following options:
  - *View*: Loads the selected capture session into the Timeline graph above.
  - *Delete Capture*: Removes the selected capture and all of its capture sessions, packet data, and statistics from the capture storage space on the Capture Engine. You will be prompted to verify any deletions. Only a parent capture, and not individual capture sessions, can be deleted from the list.
  - *Delete All Captures*: Removes all captures, capture sessions, packet data, and statistics from the capture storage space on the Capture Engine. You will be prompted to verify any deletions.
  - *Show Unreserved Space*: Displays the amount of space that is not currently being used as capture storage space on the Capture Engine.
  - *Show Legend*: Displays a color-coded legend for the capture sessions.

Details nested tab

The *Details* nested tab displays capture sessions available from the storage space on the Capture Engine as a list in tabular format. Each capture session is displayed under its main parent capture. The main parent capture is a collapsible list that can be expanded or collapsed to hide or show its capture sessions.



Here are some useful notes for using the *Details* nested tab:

- A capture session that is colored orange indicates it is currently selected. A capture session that is colored green indicates it is currently active and is capturing packets.
- Capture sessions may be overwritten by another session in the same capture, if the capture was created as a 'continuous capture' and the session 'wraps' after exceeding the disk space allocated for the capture. An overwritten capture session is no longer available for analysis.
- Only one capture session at a time can be selected and displayed in the Timeline graph.
- Right-click a column heading to display or hide a specific column. Click a column heading to sort its data.
- Right-click a capture session or parent capture to display the following options:
  - *View*: Loads the selected capture session into the Timeline graph above. Only a capture session, and not a parent capture, can be loaded into the Timeline graph.
  - *Delete Capture*: Removes the selected capture and all of its capture sessions, packet data, and statistics from the capture storage space on the Capture Engine. You will be prompted to verify any deletions. Only a parent capture, and not individual capture sessions, can be deleted from the list.
  - *Delete All Captures*: Removes all captures, capture sessions, packet data, and statistics from the capture storage space on the Capture Engine. You will be prompted to verify any deletions.
  - *Expand All*: Expands the list so that all capture sessions are displayed below the parent capture.
  - *Collapse All*: Collapses the list so that all capture sessions are hidden below the parent capture.

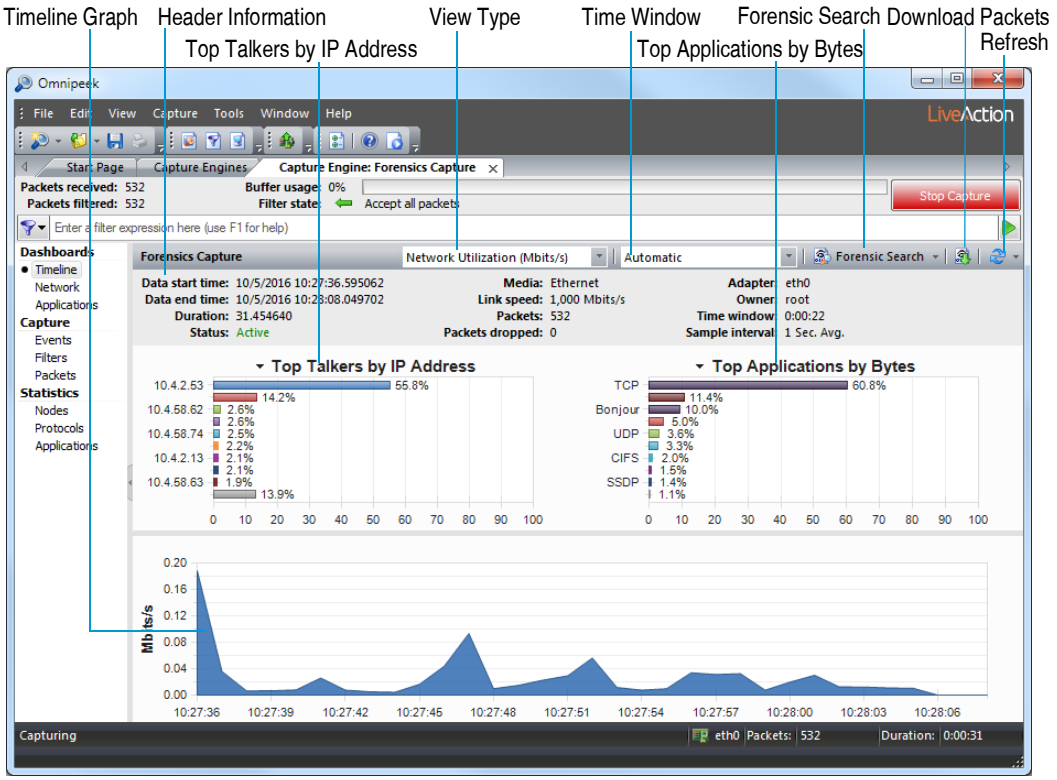
Forensic search from the 'Forensics Capture' window

If you created a 'Forensics Capture' window, you can perform a forensic search directly from the capture window. A forensic search creates a new **Forensic Search** window.

Note You can also perform a forensic search from the *Files* or *Forensics* tab. See *Forensic search from the Files tab* on page 18 and *Forensic search from the Forensics tab* on page 21.

To perform a forensic search from the 'Forensics Capture' window:

1. Create a 'Forensics Capture' window as described in *Creating a Capture Engine capture* on page 10.
2. Click the *Timeline* dashboard to display the new 'Forensics Capture' window.



The parts of the *Timeline* dashboard are described here:

- *Header Information*: The header information displays statistics for the capture session (data start time, data end time, duration, status, packets, packets dropped, adapter, etc.).
- *Top Talkers by IP Address*: This display shows a graph of top "talkers" on the network, broken out by node for the selected area in the Timeline graph below. You can right-click inside the display to select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the node.
- *Top Applications by Bytes*: This display shows a graph of top applications on the network for the selected area in the Timeline graph below. You can right-click inside the display to toggle the display with the Top Protocols display, or to select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the application.
- *Top Protocols by Bytes*: This display shows a graph of top protocols on the network for the selected area in the Timeline graph below. You can right-click inside the display to toggle the display with the Top Applications display, or select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the protocol.
- *Timeline graph*: The Timeline graph displays the data of the capture window. By default, the graph shows utilization in Mbits/s, but other statistics can be graphed as well by selecting the *View* type.

  Here are descriptions of other parts of the Timeline graph:

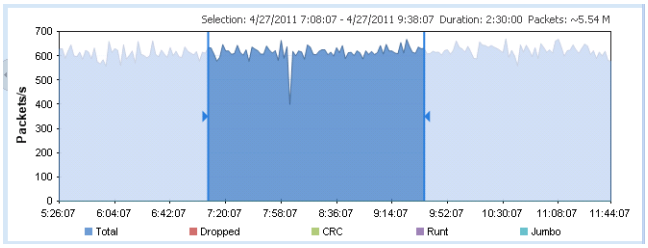
  - Right-click inside the graph to perform a forensic search (see *Forensic search* below), download selected packets to a capture file, refresh the window, or choose a different graph format: *Bar*, *Stacked Bar, Skyline, Area*, *Stacked Area, Line*, *Line/Points*, *Linear*, and *Logarithmic*. Additionally, you can also toggle displaying the minimum and maximum points for each series on the graph.
  - Mouse over a data point in the graph to view a tooltip displaying timestamp and size information (e.g., time and rate, time and packet size, etc.).

  - Any time there is more data than can be displayed on the screen, a scroll bar appears below the graph and allows you to view different points of time in the graph. (If the *Time window* is set to *Automatic*, the scroll bar will never appear.)
  - If the *Time window* is set to anything other than *Automatic*, a scroll bar appears below the graph and allows you to view different points of time in the graph.
- *View type*: Select the type of statistics to display in the Timeline graph. You can select from:
  - *Network Utilization (Mbits/s)*
  - *Network Utilization (Packets/s)*
  - *Unicast/Multicast/Broadcast*
  - *Packets sizes*
  - *VLAN/MPLS*
  - *Protocols (Mbits/s)*
  - *Protocols (Packets/s)*
  - *Call Quality*
  - *Call vs. Network Utilization*
  - *Wireless Packets (Packets/s)*
  - *Wireless Retries (Packets/s)*

Note To display statistics for a *Call Quality* and *Call vs. Network Utilization* view type, the *VoIP Stats* option must be selected when the capture was created and configured in the *General* options of the **Capture Options** dialog.

- *Time window*: Select the time interval to display in the Timeline graph. By default, *Automatic* is selected to display the optimum window based on the available data. Intervals from *5 Minutes (1 Sec. Avg.)* to *24 Hours (5 Min. Avg.)* are also available.
- *Forensic search*: Click to display the **Forensic Search** dialog where you can adjust the forensic search settings. Click the small down arrow next to **Forensic Search** to display custom or pre-configured settings for performing a forensic search. You can change any option prior to clicking **Start**:
  - *Custom*: Creates a **Forensic Search** window based on the customized settings that you configure.
  - *Overview*: Creates a **Forensic Search** window based on settings that display an overview of the selected data in the capture session.
  - *Packets*: Creates a **Forensic Search** window containing a packets-only view.
  - *Expert*: Creates a **Forensic Search** window based on settings that are optimized for *Expert* analysis.
  - *Voice & Video*: Creates a **Forensic Search** window based on settings that are optimized for *Voice & Video* analysis.
- *Download Packets*: Click to download the packets from the selected time range.
- *Refresh*: Click to refresh the screen. For an active capture session, you can also set an automatic refresh interval by selecting an interval from the drop-down list to the right of **Refresh**.

3. In the Timeline graph, drag to select the area of the capture you wish to search. If no area of the graph is selected, the entire capture is selected by default.

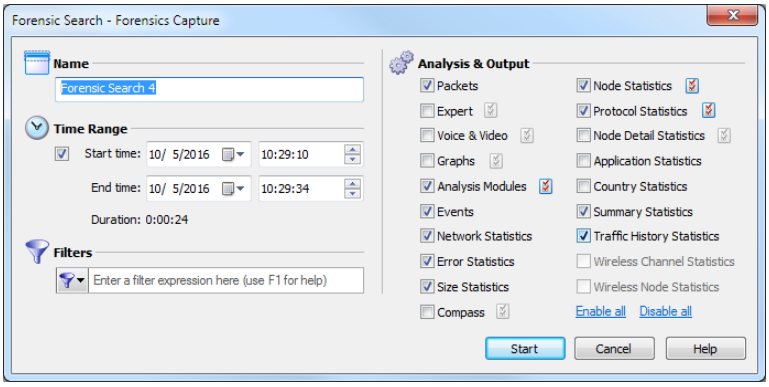


Note The packet count displayed above the Timeline graph is an approximation of the packets currently selected.

Tip You can adjust the exact time range from the **Forensic Search** dialog.

4. Click **Forensic Search** (or click the small down arrow next to **Forensic Search** and select the type of forensic search you wish to perform). The **Forensic Search** dialog appears.

Note Selecting one of the pre-defined types of forensic searches displays the **Forensic Search** dialog with the *Analysis & Output* options pre-configured for that type of forensic search. You can change any option prior to clicking **Start**.

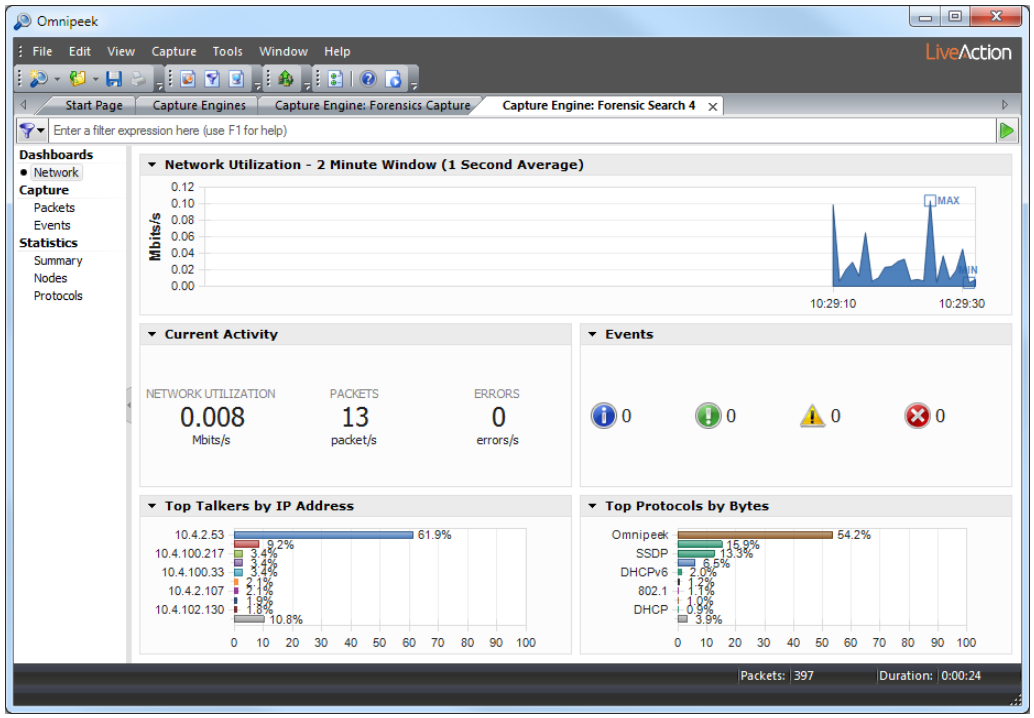


5. Complete the dialog to specify the criteria for extracting data from the selected capture:
   - *Name:* Enter a name for the forensic search.
   - *Time Range:* Select this option and then configure the start and end times to extract the data.
     - *Start time:* Set the start date and time for extracting data. Only the data captured between the start time and end time is extracted.
     - *End time:* Set the end date and time for extracting data. Only the data captured between the start time and end time is extracted.
     - *Duration:* Displays the amount of time between the specified start and end times.
   - *Filters:* Click to select a filter from the display list. All packets will be accepted if no filters are applied to the forensic search.

     To create an advanced filter, click *Filters* and select *Insert filter*, *Insert Operator*, or *Insert Expression* from the display.
   - *Analysis & Output:* Select one or more of the options to enable and display that particular view in the new **Forensic Search** window. For various *Analysis & Output* options that have additional configurable settings, click the submenu to the right of the option.

6. Click **Start**. A new **Forensic Search** window appears along with two progress bars at the top of the window. (Clicking **Stop** stops the search and then completes the processing of the packets.)

   Once the processing of the packets is complete, the progress bars go away and the new **Forensic Search** window is populated with the data found based on the criteria you selected above. The name of the **Forensic Search** window is added to the list of currently active forensic searches in the *Forensic Searches* tab.



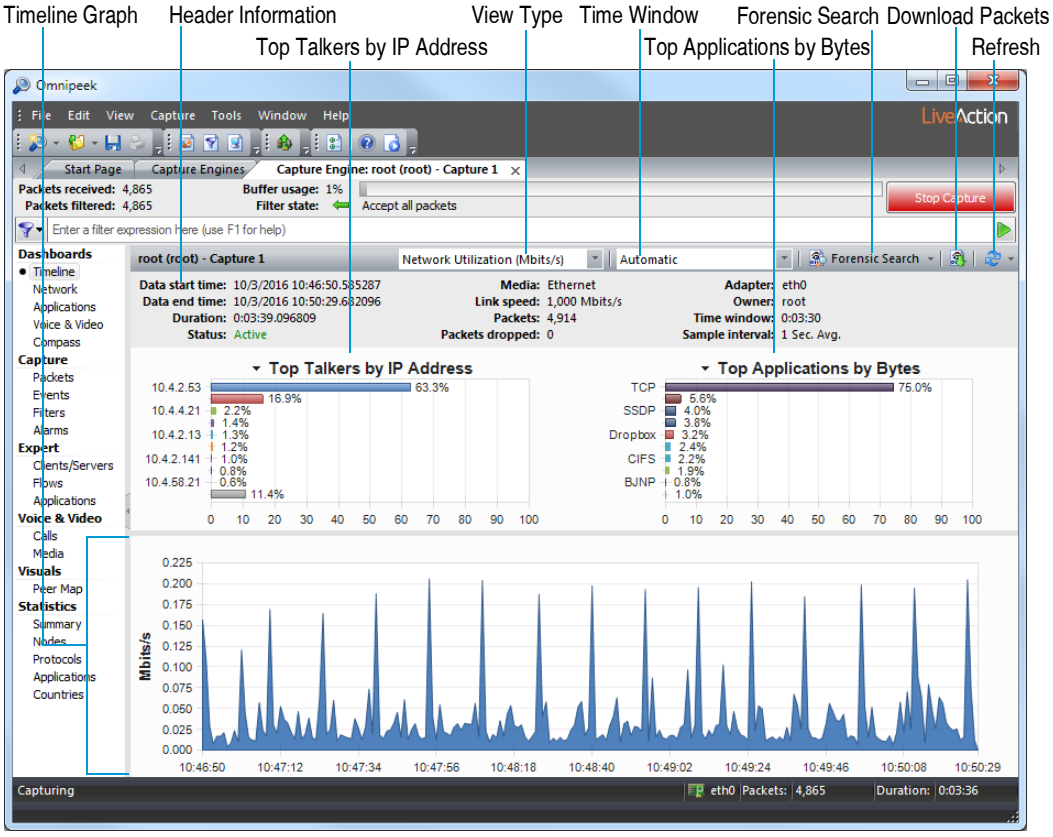
7. From the new **Forensic Search** window, you can further narrow down the data by performing any of the post-capture analysis methods described in the *Omnipeek User Guide*.

Dashboards

The Omnipeek dashboards display graphical data about your network summarized into several easy-to-read displays. There are five dashboards available with Omnipeek: *Timeline*, *Network*, *Applications*, *Voice & Video*, and *Compass*.

Timeline dashboard

The **Timeline** dashboard is available from Capture Engine capture windows that have any of the *Timeline Stats* options enabled in the **Capture Options** dialog. The dashboard displays top talkers, top protocols, and network utilization for the Capture Engine.



The parts of the **Timeline** dashboard are described below.

- *Header Information*: The header information displays statistics for the capture session (data start time, data end time, duration, status, packets, packets dropped, adapter, etc.).
- *Top Talkers by IP Address:* This display shows a graph of top "talkers" on the network, broken out by node. You can right-click inside the display to display top talkers by *Physical Address*, *IP Address*, or *IPv6 Address*; or to select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the node.

- *Top Applications by Bytes*: This display shows a graph of top applications on the network for the selected area in the Timeline graph. You can right-click inside the display to toggle the display with the Top Protocols display, or to select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the application.
- *Top Protocols by Bytes:* This display shows a graph of top protocols on the network for the selected area in the TimeLine graph. You can right-click inside the display to toggle the display with the Top Applications display, or to select a *Bar* or *Pie* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the protocol.
- *Timeline graph*: The Timeline graph displays the data of the selected capture session. Only one capture session at a time can be displayed inside the graph. By default, the graph shows network utilization in Mbits/s, but other statistics can be graphed as well by selecting the *View* type.

  Here are descriptions of other parts of the Timeline graph:

  - Right-click inside the graph to perform a forensic search, download selected packets to a capture file, refresh the window, or choose a different graph format: *Bar*, *Stacked Bar, Skyline, Area*, *Stacked Area, Line*, *Line/Points*, *Linear*, and *Logarithmic*. Additionally, you can also toggle displaying the minimum and maximum points for each series on the graph.
  - Mouse over a data point in the graph to view a tooltip displaying timestamp and size information (e.g., time and rate, time and packet size, etc.).
  - Any time there is more data than can be displayed on the screen, a scroll bar appears below the graph and allows you to view different points of time in the graph. (If the *Time window* is set to *Automatic*, the scroll bar will never appear.)
  - If the *Time window* is set to anything other than *Automatic*, a scroll bar appears below the graph and allows you to view different points of time in the graph.
  - *View type*: Select the type of statistics to display in the Timeline graph. You can select from:
    - *Network Utilization (Mbits/s)*
    - *Network Utilization (Packets/s)*
    - *Unicast/Multicast/Broadcast*
    - *Packets sizes*
    - *VLAN/MPLS*
    - *Protocols (Mbits/s)*
    - *Protocols (Packets/s)*
    - *Applications (Mbits/s)*
    - *Applications (Packets/s)*
    - *Call Quality*
    - *Call vs. Network Utilization*
    - *Wireless Packets (Packets/s)* (Capture Engine for Omnipeek (Windows) only)
    - *Wireless Retries (Packets/s)* (Capture Engine for Omnipeek (Windows) only)

  Note To display statistics for a *Call Quality* and *Call vs. Network Utilization* view type, the *VoIP Stats* option must be selected when you first create the capture and configure the *General* options of the **Capture Options** dialog.

  - *Time window*: Select the time interval to display in the Timeline graph. By default, *Automatic* is selected to display the optimum window based on the available data. Intervals from *5 Minutes (1 Sec. Avg.)* to *24 Hours (5 Min. Avg.)* are also available.

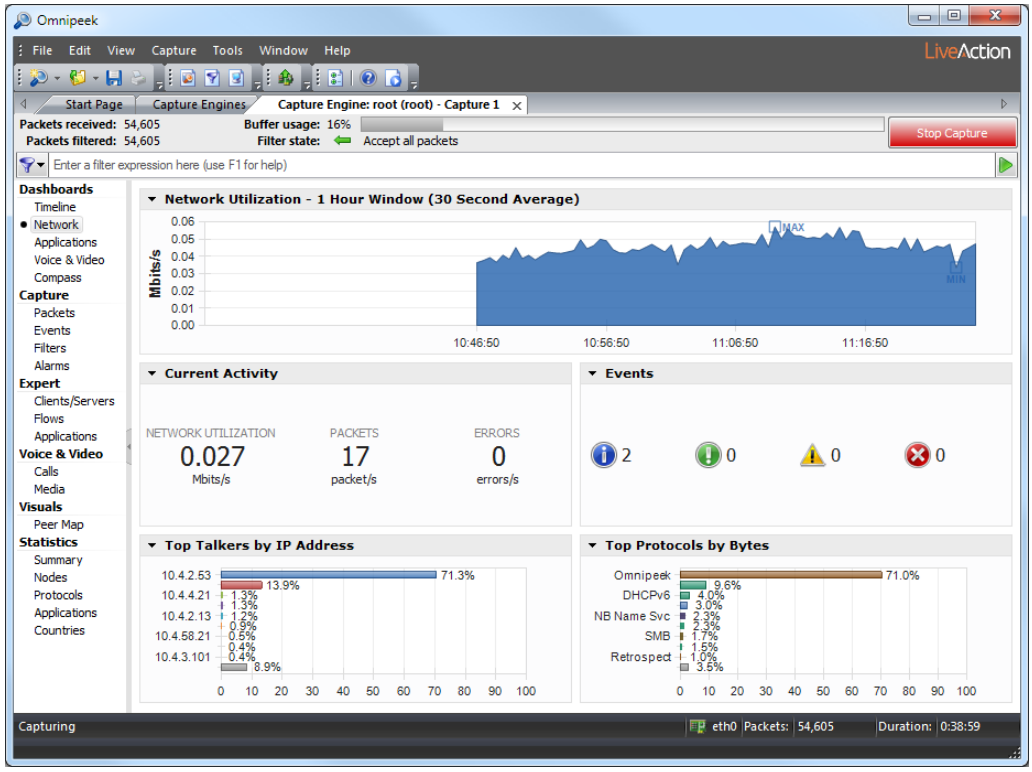
- *Forensic search*: Click to display the **Forensic Search** dialog where you can adjust the forensic search settings. Click the small down arrow next to **Forensic Search** to display custom or pre-configured settings for performing a forensic search. You can change any option prior to clicking **OK**:

Note When configuring the **Forensic Search** dialog, keep in mind that forensic search performance can be directly related to the number and type of options that you have enabled.

  - *Custom*: Creates a **Forensic Search** window based on the customized settings that you configure.
  - *Overview*: Creates a **Forensic Search** window based on settings that display an overview of the selected data in the capture session.
  - *Packets*: Creates a **Forensic Search** window containing a packets-only view.
  - *Expert*: Creates a **Forensic Search** window based on settings that are optimized for *Expert* analysis.
  - *Voice & Video*: Creates a **Forensic Search** window based on settings that are optimized for *Voice & Video* analysis.
- *Download Packets*: Click to download the packets from the selected capture session, in the selected time range.
- *Refresh*: Click to refresh the screen. For an active capture session, you can also set an automatic refresh interval by selecting an interval from the drop-down list to the right of **Refresh**.

Network dashboard

The **Network** dashboard displays key statistics for the capture window.



- *Network Utilization:* This display graphs network traffic in Mbits/second. You can right-click inside the display to drill-down to selected packets, or to select a *Column*, *Skyline*, *Area*, *Line*, or *Line/Points* display.

- *Wireless Signal:* This display graphs wireless signal and/or noise strength (as a percentage) for the wireless channel you are capturing on, or all channels you have configured the capture to scan. This display is available only when a wireless adapter is selected as the capture adapter, or for a wireless capture file. You can right-click inside the display to select the parameters to display. Hovering over a channel will display a tooltip with additional channel information.
- *Current Activity:* This display shows network utilization (as a percent of capacity), traffic volume (in packets per second), and error rate (total errors per second). You can right-click inside the display to display values as numbers or as gauges, or to select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display.
- *Events:* This display shows the number of notifications generated by level of severity. You can right-click inside the display to select an *Automatic, Light*, *Dark*, or *Clean* background theme for the display. Clicking a severity icon navigates to the **Events** view and displays those events corresponding to the severity clicked.
- *Top Talkers by IP Address:* This display shows a graph of top "talkers" on the network, broken out by node. You can right-click inside the display to display top talkers by *Physical Address*, *IP Address*, *IPv6 Address*, or *Country*, or to select a *Bar, Column, Pie* or *Donut* display. Clicking a bar (or slice) of the graph opens a Detail Statistics window populated with details for the node clicked.

  Note This feature is automatically enabled for Capture Engine captures based on the Monitoring Capture template. Top talkers are displayed as *Not Available* for Capture Engine captures using the Forensic Capture template. See *Forensics capture on a Capture Engine* on page 54 and *Monitoring capture on a Capture Engine* on page 55.

- *Top Applications*: This display shows a graph of top applications on the network. You can right-click inside the display to toggle the display with the *Top Protocols* display, or to select a *Bar, Column, Pie* or *Donut* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the application. Clicking a bar (or slice) of the graph opens a Detail Statistics window populated with details for the application clicked.
- *Top Protocols:* This display shows a graph of top protocols on the network. You can right-click inside the display to toggle the display with the *Top Applications* display, or to select a *Bar, Column, Pie* or *Donut* display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the protocol. Clicking a bar (or slice) of the graph opens a Detail Statistics window populated with details for the protocol clicked.

  Tip Several of the displays inside the Network dashboard support tooltips. Hover over the display to view a tooltip with additional information.

  You can also access additional options for viewing each display by clicking the small arrow in the upper left corner of each display, or by right-clicking inside each display.

Applications dashboard

The **Applications** dashboard displays key statistics for applications in the capture window. This application visibility provides insight into user behavior and traffic patterns on the network at certain times of day, week, month, or year. It helps the analysts to better understand who is going to what web sites and using which applications when.

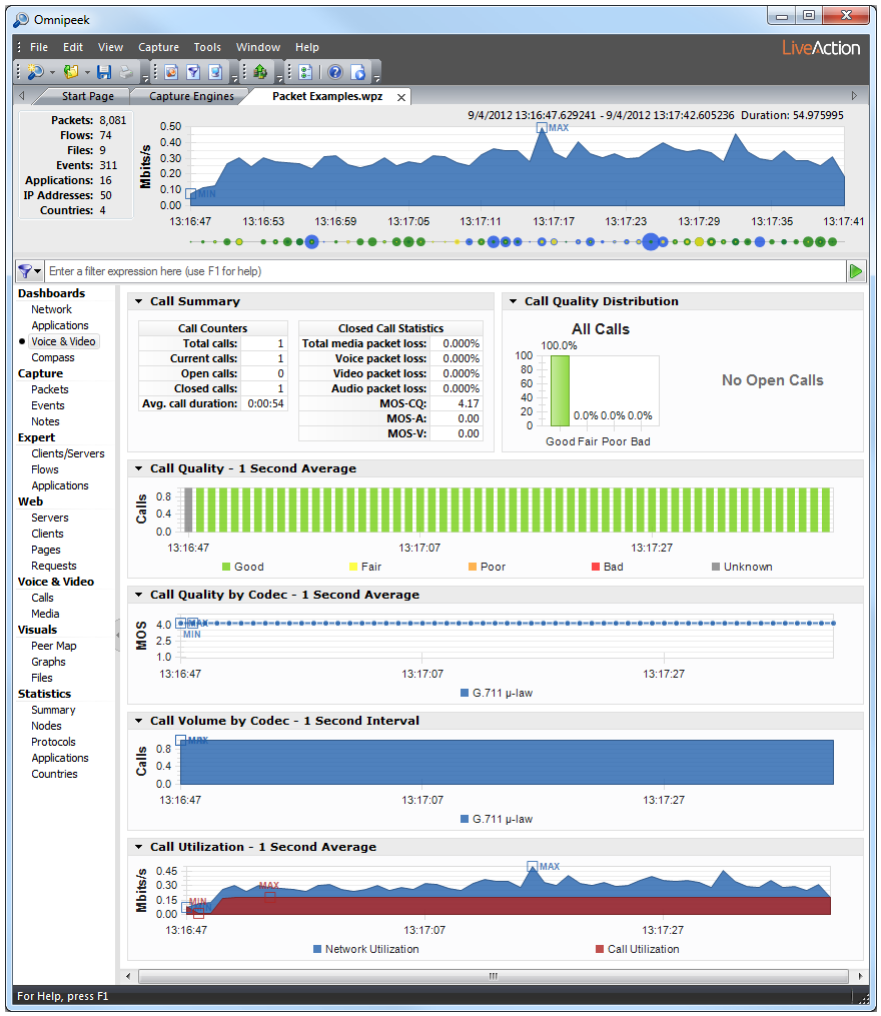
- *Top Applications by Flows:* This display shows a graph of top applications by flow count. Clicking any application in this display lets you drill-down to that application in the Expert **Applications** view. You can right-click inside the display to select a *Bar, Column, Pie* or *Donut* display; select *Auto Scale* or *Fixed Scale*; or to select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display.
- *Top Applications by Bytes*: This display shows a graph of top applications by bytes. You can right-click inside the display to toggle the display with the *Top Protocols by Bytes* display; select a *Bar, Column, Pie* or *Donut* display; select *Auto Scale* or *Fixed Scale*; or to select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the application. Clicking a bar (or slice) of the graph opens a Detail Statistics window populated with details for the application clicked.
- *Top Protocols by Bytes:* This display shows a graph of top protocols by bytes. You can right-click inside the display to toggle the display with the *Top Applications by Bytes* display; select a *Bar, Column, Pie* or *Donut* display; select *Auto Scale* or *Fixed Scale*; or select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the protocol. Clicking a bar (or slice) of the graph opens a Detail Statistics window populated with details for the protocol clicked.
- *Top Application Categories by Bytes:* This display shows a graph of top application categories by bytes. You can right-click inside the display to select a *Bar, Column, Pie* or *Donut* display; select *Auto Scale* or *Fixed Scale*; or to select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. Mouse over a bar (or slice) of the graph to view a tooltip with additional details for the application categories.
- *Application Utilization:* This display shows the top applications by bits per second. You can right-click inside the display to select a *Stacked Column, Skyline, Stacked Skyline, Area, Stacked Area, Line*, or *Line/Points* display; select whether the display is *Linear* or *Logarithmic*; show *Min/Max* values; or select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. You can select an area of the graph, right-click and choose *Select Packets*. Only packets available in the capture buffer will be accessible for *Select Packets*.
- *Application Response Time:* This display shows response time of the top applications by largest response time. You can right-click inside the display to select a *Skyline, Area, Line, Line/Points* or *Points* display; select whether the display is *Linear* or *Logarithmic*; show Min/Max values; or select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. You can select an area of the graph, right-click and choose *Select Packets*. Only packets available in the capture buffer will be accessible for *Select Packets*.

Tip Several of the displays inside the Applications dashboard support tooltips. Hover over the display to view a tooltip with additional information.

You can also access additional options for viewing each display by clicking the small arrow in the upper left corner of each display, or by right-clicking inside each display.

Voice & Video dashboard

The **Voice & Video** dashboard provides a visual display of voice and video call summary, as well as useful graphs and statistics to troubleshoot and analyze voice and video traffic.



The parts of the **Voice & Video** dashboard are identified below.

- *Call Summary:* This display shows "Call Counter" information and "Closed Call Statistics" on voice and video packet loss. In addition, the *Call Summary* displays the *Max Call Time* which is the point and time when the maximum call limit was reached. The *Max Call Time* is displayed in red text and will dynamically appear. You can right-click inside the display to select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display.
- *Call Quality Distribution:* This display shows open and closed calls by quality based on MOS scores. You can right-click inside the display to select a *Bar, Column, Pie*, or *Donut* display; or select an *Automatic*, *Light, Dark*, or *Clean* background theme for the display.

MOS scores are calculated for each media flow independently, and each call's quality is the lowest MOS score of any of its associated media flows. Voice media is scored with MOS-CQ, video media with MOS-V, and audio media with MOS-A.

The quality thresholds are as follows:

- <2.6 = Bad (displayed in Red)
- >=2.6 to <3.1 = Poor (displayed in Orange)
- >=3.1 to <3.6 = Fair (displayed in Yellow)
- >=3.6 = Good (displayed in Green)

Media flows with unsupported codecs are not included in the display since we cannot obtain MOS values for these calls. Additionally, the display reflects that same data present in the Calls and Media views, and therefore is affected by the 2000 call limit.

- *Call Quality*: This display shows call quality over time for calls classified as good, fair, poor, bad, and unknown. You can right-click inside the display to select a *Stacked Column, Skyline, Stacked Skyline, Area*, *Stacked Area, Line*, *Line/Points,* or *Points* display; show *Min/Max* values; or select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. You can also select an area of the *Call Quality* graph, right-click and choose *Select Packets*.
- *Call Quality by Codec*: This display shows a line graph of the quality for each codec in use over time. You can right-click inside the display to select a *Line, Line/Points*, or *Points* display; show *Min/Max* values; or select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. You can also select an area of the *Call Quality* graph, right-click and choose *Select Packets*.

  MOS scores are used for the quality measurement. Voice media shall be scored with MOS-CQ, video media with MOS-V, and audio media with MOS-A.

  The quality for a time period shall be the average of the MOS scores for all open media flows for that time period. In addition, this graph will only display MOS scores for supported codecs as unsupported codecs do not provide MOS measurements.
- *Call Volume by Codec*: This display shows a graph of open calls (per codec) over time for voice and video calls. This graph reflects all calls from the **Calls** and **Media** view, and unlike the other graphs in the dashboard, the **Call Volume** graph includes data for calls using unsupported codecs. You can right-click inside the display to select a *Stacked Column, Skyline, Stacked Skyline, Area*, *Stacked Area, Line*, *Line/Points,* or *Points* display; show *Min/Max* values; or select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. You can also select an area of the *Call Volume* graph, right-click and choose *Select Packets*.
- *Call Utilization:* This display shows a graph of overall network utilization compared to network utilization by VoIP protocols. You can right-click inside the display to select a *Skyline, Area*, *Line*, or *Line/Points* display; select whether the display is *Linear* or *Logarithmic*; show *Min/Max* values; or select an *Automatic*, *Light*, *Dark*, or *Clean* background theme for the display. You can also select an area of the *Call Utilization* graph, right-click and choose *Select Packets*.

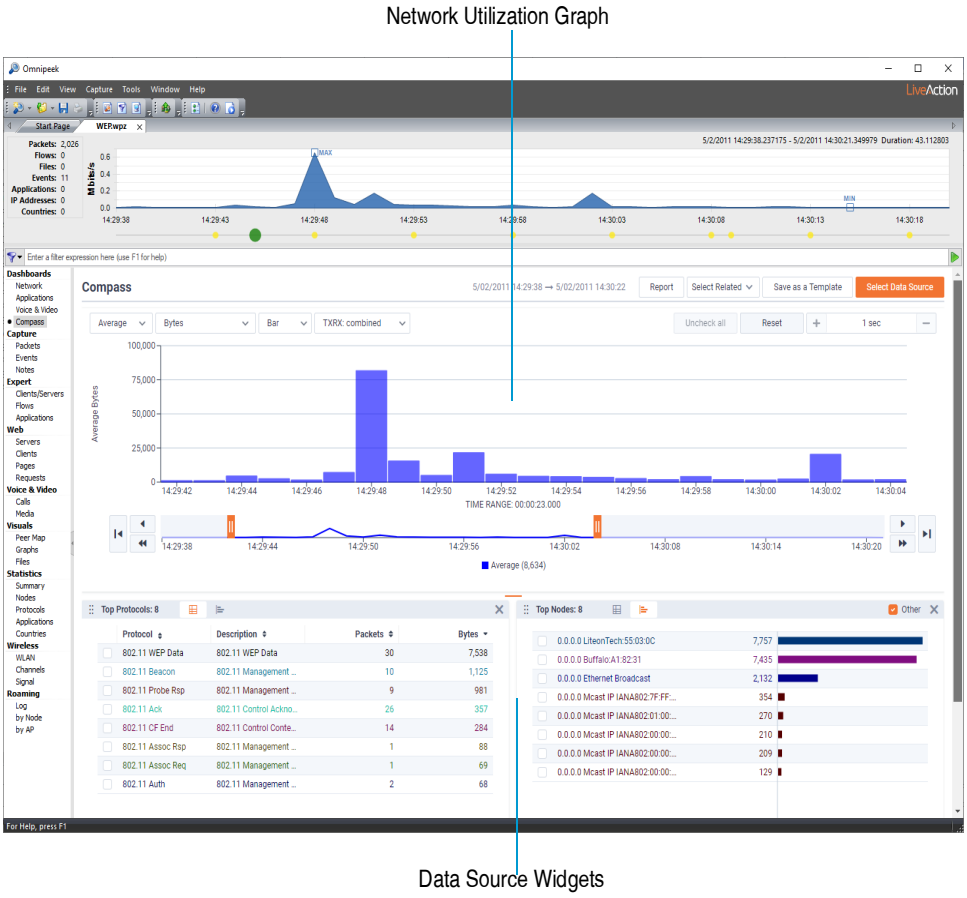
  This graph displays two legends: *Network Utilization* and *Call Utilization*. Utilization values are displayed in Mbits/second. The VoIP utilization shall be the total utilization for all VoIP packets (i.e., signaling, media RTP/RTCP, and unsupported codecs).

Tip Several of the displays inside the Voice & Video dashboard support tooltips. Hover over the display to view a tooltip with additional information.

You can also access additional options for viewing each display by clicking the small arrow in the upper left corner of each display, or by right-clicking inside each display.

Compass dashboard

The **Compass** dashboard is an interactive forensics dashboard that displays network utilization over time including event, protocol, flow, node, channel, WLAN, VLAN, data rate, application, and country statistics. These statistics are displayed in selectable Data Source widgets which can be viewed from a real-time capture or from a single supported capture file.



The parts of the **Compass** dashboard are described below.

- *Network Utilization Graph*: Displays two interactive timeline graphs that allow you to select and display a range of data. See *Network utilization graph* on page 39.
- *Data Source Widgets*: Displays enabled statistics widgets (events, protocols, flows, nodes, channels, WLAN, VLAN, data rates, applications, and countries). See *Network utilization graph* on page 39 and *Data Source widgets* on page 44.

Tip You can use the orange horizontal splitter located between the network utilization graph and the Data Source widgets to resize the displays.

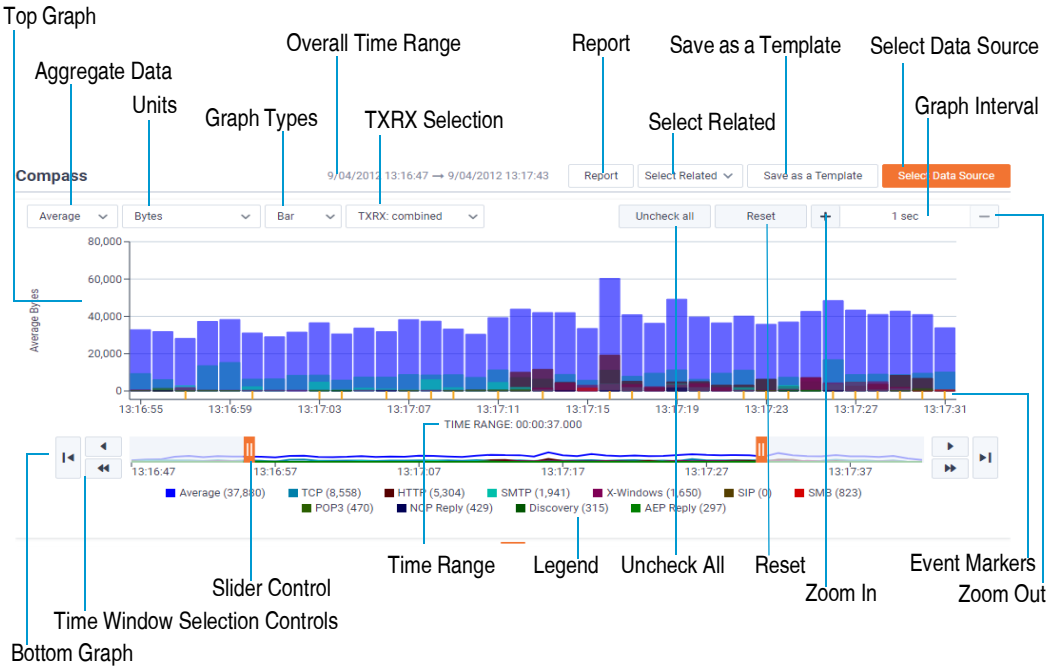
Network utilization graph

The network utilization graph in the **Compass** dashboard consists of two interactive timeline graphs that allow you to view a specific area of interest. The top (larger) graph displays utilization over a selected time range, while the bottom graph displays utilization over the total time period. You will need to drag and select a time range in the top graph in order to display the bottom graph.

You can zoom into or out of the selected time range so that granularity is in milliseconds, seconds, minutes, hours, or days (initially the time range adjusts accordingly depending on how large of a capture needs to be displayed) by using the **Zoom In** and **Zoom Out** controls (not available in real-time captures).

As you change the selected time range, the Data Source widgets will update accordingly to reflect the new period. See *Compass dashboard viewing tips* on page 46 for additional information on using your mouse to navigate inside the network utilization graph.

Tip For best results, it is recommended to zoom in on a selected time range until you can see the details of the area of interest.



The parts of the network utilization graph are described below:

- *Top graph*: Displays network utilization as a line, scatter, bar, or area graph over a selected time range. Drag left or right inside the graph to select and display a specific time range (you can also use the bottom graph to select the time range). The selected data is then reflected in the bottom graph and also in the Data Source widgets at the bottom.
- *Bottom graph*: Displays network utilization as a line graph over the total time period. The bottom graph is always displayed if the top graph is not at full select, and always hidden if the top graph is at full select.

  Use both the slider controls and time window selection controls to select a specific time range. The data for the selected time range is then reflected in the top graph and also in the Data Source widgets at the bottom.
- *Overall Time Range*: Displays the overall time range, from start date and time to stop date and time, of the trace file, capture, or forensic search.
- *Report*: (Omnipeek only) Saves the data currently displayed inside the **Compass** dashboard to an HTML report that can be viewed from inside a browser window, to multiple CSV files, or to a PDF file.
- *Select Related*: Filters packets related to selected items from the Data Source widget and from the time range currently selected in the network utilization graph. You will need to also select between AND or OR filtering logic when using Select Related (multiple items selected within the same Data Source widget will always use OR logic since AND logic will always nullify the entire expression, but items from different Data widgets will use the selected filtering logic). See also *Select related packets* on page 47.
- *Save as a Template*: Saves the contents of the current Compass display as a template so that it can be used again with other data sets. The type of widgets displayed, the location of the widgets, and the size of the widgets are retained in the template. You can select saved templates by clicking *Select Data Source*.

- *Select Data Source*: Enables/disables the Data Source widgets displayed inside the Compass dashboard. If any Compass templates have been saved, you can select them from here.

  Each Data Source widget displays statistics appropriate to the selected data source and for the selected time range in the network utilization graph. The widget can be viewed as a List or Bar chart. See also *Data Source widgets* on page 44.

  The available Data Source widgets include:

  - Expert Events
  - Protocols
  - Flows
  - Nodes
  - Channels
  - WLAN
  - VLAN
  - Data Rates
  - Applications
  - Countries

  Note For wired captures, the following Data Source widgets are not available: *Channels*, *WLAN*, and *Data Rates*. For wireless captures, the *VLAN* Data Source widget is not available.

- *Aggregate Data*: Allows you to display the Y axis in the top and bottom graphs, Data Source widgets, and legend as an aggregate of average, total, or maximum values:
  - *Average*: In the top and bottom graphs, the average value for each time interval is graphed. In the various Data Source widgets, the average value for the statistic over the selected time range is graphed. If *Bits*, *Bytes*, *Mbits*, *Gbits*, *Packets*, or *Retransmission Rate* is the selected unit type, then average calculations include non-values; otherwise, non-values are not included in the calculations. Average calculations for *Bits*, *Bytes*, *Mbits*, *Gbits*, *Packets*, *Signal Strength %*, *Noise Level %*, and *Expert Events* are rounded to the nearest whole number.
  - *Total*: In the top and bottom graphs, the total value for each time interval is graphed. In the various Data Source widgets, the total value for the statistic over the selected time range is graphed. If *2-Way Latency*, *Response Time*, *Signal Strength %, Signal Strength dBm*, *Noise Level %, Noise Level dBm*, *SNR*, or *Data Rate* is the selected unit type, then *Total* values are unavailable.
  - *Maximum*: In the top and bottom graphs, the maximum value for each time interval is graphed. In the various Data Source widgets, the maximum value for the statistic over the selected time range is graphed.
- *Units*: Allows you to set the unit type in the Y axis of the top and bottom graphs, Data Source widgets, and legend. Depending on the packet type and how they are aggregated, the available unit types include:
  - *Bits*. Displays byte count in bits.
  - *Bytes*. Displays byte count in bytes.
  - *Mbits*. Displays byte count in Mbits.
  - *Gbits*. Displays byte count in Gbits.
  - *Packets*. Displays the packet count.
  - *2-Way Latency*. Displays 2-way latency. 2-way latency is the delta time between a request from the client, and a response from the server.

- *Response Time*. Displays response time. Response time is the delta time between a request packet from the client, and a response packet with data from the server.
- *Signal Strength %* (Wireless traffic only). Displays signal strength of the wireless data transmission, expressed as a percentage.
- *Signal Strength dBm* (Wireless traffic only). Displays signal strength of the wireless data transmission, expressed in dBm (decibel-milliWatts).
- *Noise Level %* (Wireless traffic only). Displays noise level reported of the wireless data transmission, expressed as a percentage.
- *Noise Level dBm* (Wireless traffic only). Displays noise level reported of the wireless data transmission, expressed in dBm (decibel milliWatts).
- *SNR* (Wireless traffic only). Displays Signal to Noise Ratio (SNR) of the wireless data transmission. Basically, it is a measure of signal strength relative to background noise.
- *Data Rate* (Wireless traffic only). Displays data rate of the wireless data transmission.
- *Retransmission Rate* (Wireless traffic only). Displays retransmission rate percentage of the wireless data transmission.
- *Expert Events*. Displays the total number of Expert events. Only the Expert events whose Event type severity button is enabled and are selected in the Expert Events Data Source widget are included in the count. If no Expert events are selected in the Expert event view, then all events whose Event type severity button is enabled are included.

Note Selecting a unit type of *Mbits* or *Gbits*, and also selecting an aggregate value of *Average*, displays data in the graphs, Data Source widgets, and legend as a graph average, and not as the *Average Utilization (bit/s)*. To see the *Average Utilization (bit/s)*, click the **Summary** view under *Statistics* in the navigation pane of a capture window, and view the *Network* statistics.

- *Graph Type*: Displays the top graph as a line, scatter, bar, or area graph.
- *TXRX Selection*: Enables or disables graphing of both the inbound and outbound utilization values for the selected statistics (except for flows). The outbound values appear as a slightly lighter color than the inbound values in both the graphs view and legend. Inbound and outbound values are not available for the 2-Way latency mode, Response Time mode, and Expert Events mode.
- *Uncheck All*: Click to clear the check boxes of all the selected items in each of the Data Source widgets.
- *Reset*: Click to reset the Network Utilization Graph to its original state as if it was fully selected.
- *Zoom In*: For selected time ranges of a certain length, Zoom In (+ sign) is enabled and allows you to zoom into the selected time range so that you can increase granularity in milliseconds, seconds, minutes, hours, and days. You can hover the mouse over *Zoom In* to display a tooltip that contains the maximum time range that can be zoomed into. Selecting a time range less than or equal to it will enable Zoom In. (See also *Graph Interval* below).

  For example, if the graph is in seconds with a one second average, you can zoom into milliseconds with a particular millisecond average; or, if the graph is in hours you can zoom into minutes. See the Graph Interval table below for more information as to what the graph interval will be for a particular time. Zoom In is not available in real-time capture mode.
- *Zoom Out*: Zoom Out (- sign) brings you back out of the previous Zoom In selection. Zoom Out is not available in real-time capture mode.

- *Graph Interval*: Graph Interval is the amount of time for each data point in the graph and is automatically adjusted based on the duration of the selected time range. The Graph Interval is updated according to the following chart:

Graph Interval	Maximum Time Duration
1 millisecond	1800 milliseconds
50 milliseconds	1.5 minutes
250 milliseconds	7.5 minutes
500 milliseconds	15 minutes
1 second	30 minutes
5 seconds	2.5 hours
15 seconds	7.5 hours
30 seconds	15 hours
1 minutes	1 day 6 hours
5 minutes	6 days 6 hours
15 minutes	2 weeks 4 days 18 hours
30 minutes	5 weeks 2 days 12 hours
1 hour	10 weeks 5 days
6 hours	64 weeks 2 days
12 hours	128 weeks 4 days
1 day	357 weeks 1 day
2 days	514 weeks 2 days
4 days	1028 weeks 4 days
(doubles)...	(doubles)...

Note The graph interval chart is also valid for determining the minimum and maximum ranges of time that can be zoomed into when viewing capture files. See also *Zoom In* above.

Additionally, millisecond graph intervals are not automatic and only occur during Zoom In and are not valid for live captures.

- *Event Markers*: Indicates triggered Expert events in the selected time range. The event markers are color coded to the Expert event severities displayed in the Expert Events Data Source widget.
- *Time Range*: The time range indicator below the X axis of the top graph indicates the duration of the currently selected time range. Use the arrow and slider controls to adjust the selected time range.
- *Time Window Selection Controls*: The single arrow and double arrow selection controls allow you to move the selected time range in the top and bottom graph left or right in one unit increments (single arrows) or in increments of the entire selection (double arrows). The single arrow with a line selection control allows you to move the selected time range in the top and bottom graph all the way to the left or right.
- *Slider Controls*: The two slider controls allow you to widen and narrow the selected time range in the top and bottom graph. In a real-time capture, the slider controls work as follows:

- If the left and right sliders are pushed all the way to the left and right (respectively), new data is displayed on the right as it becomes available, and old data on the left remains. Thus, the duration of the selected time range continuously increases.
- If the left and right sliders are not pushed all the way to the left and right (respectively), new data is not displayed on the right as it becomes available, and old data on the left remains. Thus, the duration of the selected time range is maintained.
- If the left slider is pushed all the way to the left but the right slider is not pushed all the way to the right, new data is not displayed on the right as it becomes available, and old data on the left remains. Thus, the duration of the selected time range is maintained.
- If the left slider is not pushed all the way to the left but the right slider is pushed all the way to the right, new data is displayed on the right as it becomes available, and the old data is removed from the left. Thus, the duration of the selected time range is maintained.

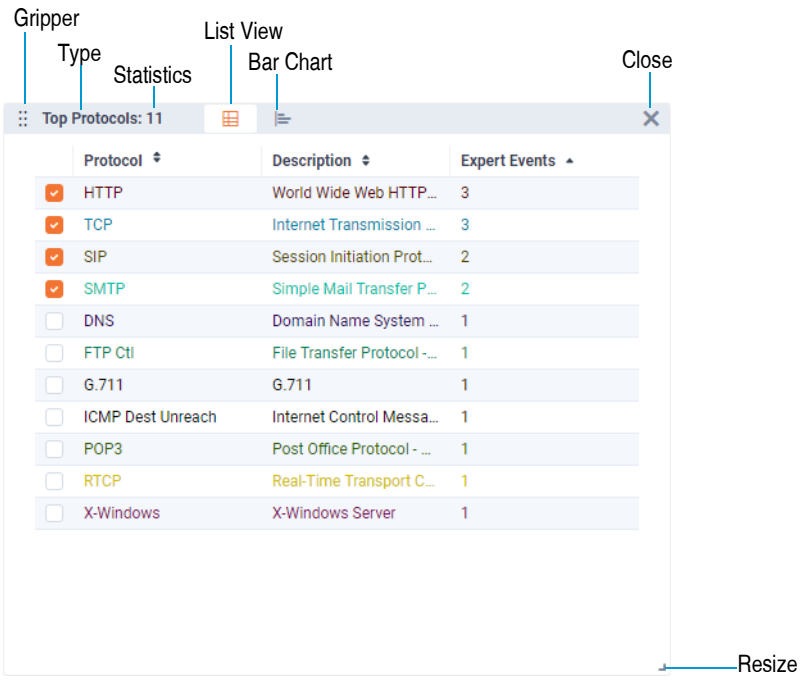
Tip You can drag the area between the slider controls left or right to select different parts of the top and bottom graph.

- *Legend*: Displays a legend of the graphed items. The values in the legend are displayed as a total, average, or maximum depending on what is selected in the Aggregate Data drop-down list. Click the color boxes in the legend to show or hide entries from the graphs.
- *Pause/Play (real-time capture only)*: Toggles between updating and not updating the graphs in real time.

Data Source widgets

The Data Source widgets display statistics for Expert Events, protocols, flows, nodes, channels, WLAN, VLAN, data rates, applications, and countries. Each widget displays statistics appropriate to the selected data source and for the selected time range in the network utilization graph. You can display these widgets in a list view or bar chart.

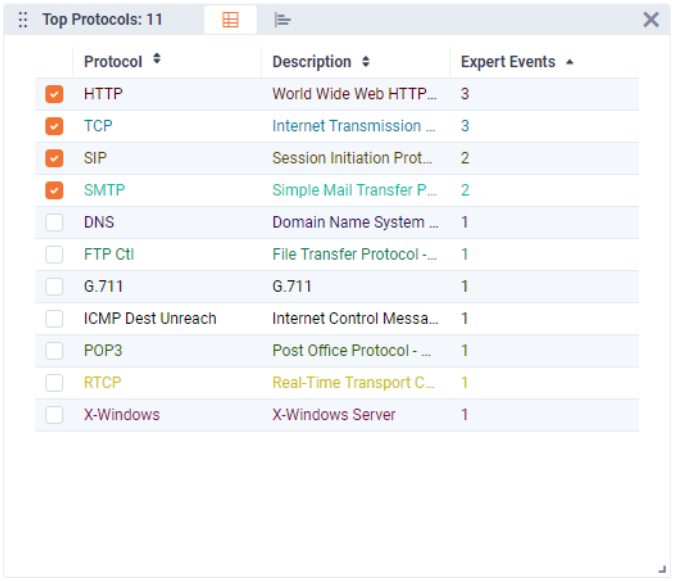
The list view and bar chart are always in sync. Enabling an item in one of the widget will be reflected in all of the other widgets. Using a Protocols Data Source widget as an example, the parts of a Data Source widgets are described below.



- *Gripper*: Allows you to drag the widget to a different location within the dashboard.
- *Type*: Displays the type of Data Source widget.
- *Statistics*: Displays the number of statistics over the selected time range within the top limit count.
- *List View*: Displays statistics in a list view.
- *Bar Chart*: Displays statistics in a bar chart.
- *Resize*: Drag to resize the Data Source widget.
- *Close*: Click to disable the widget from the dashboard.

List view

In the list view, the columns appropriate for the statistic and unit selected are displayed. By default, only the top 50 items are listed. This limit can be adjusted through the Compass options dialog.

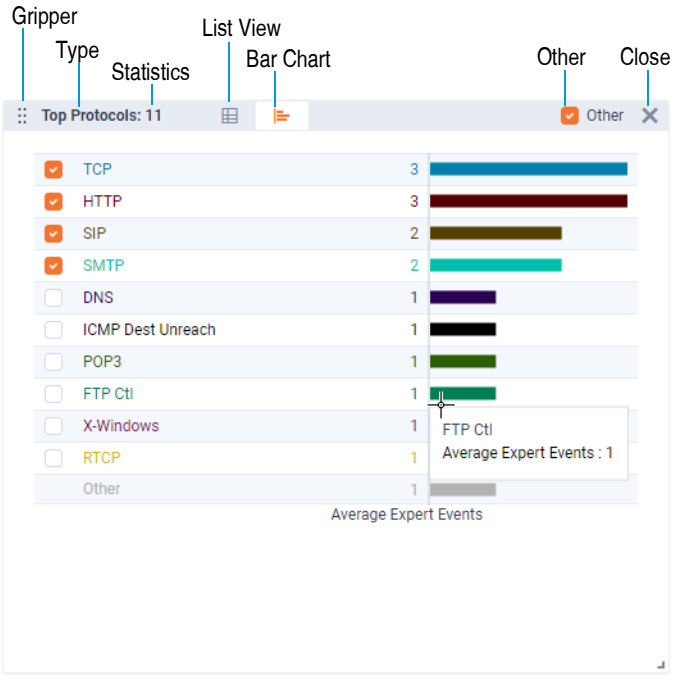


In the list view, you can:

- Click a column header to sort in ascending or descending order.
- Use the check boxes to enable or disable graphing of a specific statistics in the network utilization graph. Enabling a check box in the list view enables the same statistics in the top statistics bar chart.

Bar chart

The statistics bar chart displays the top 10 statistics, with all other statistics grouped as 'Others.'



In the bar chart, you can:

- Click a check box in the bar chart to toggle the display of statistics in the network utilization graph. Additionally, clicking a check box (except for *Others*) selects the check box of the same statistic in the list view.
- Mouse over a bar to see details about a specific statistic.
- Select or clear the 'Others' check box to show or hide 'Others' from the bar chart.

Compass dashboard viewing tips

Here are some useful tips when viewing the **Compass** dashboard:

- Hovering over an Expert event marker displays the following event specifics in a tooltip:
  - The date and time for the graph point where the Expert event(s) have occurred.
  - A list of Expert event types with the associated count of occurrences for that point in the graph.
- If the unit type is set to *Expert Events*:
  - The network utilization graph and Data Source widgets represent the Expert event severities that are enabled.
  - If no Expert events are selected in the Expert event views, the network utilization graph represents all Expert events, and the Data Source widgets display all items that are associated with any Expert event.
  - If any Expert events are selected in the Expert event views, the network utilization graph represents the selected events, and the Data Source widgets only display those items that are associated with the selected Expert events.
- You may only select a maximum combination of 10 statistical items (in the Data Source widgets) at one time.
- In the statistics list views, you can sort selected items by clicking above the check box column. This allows you to keep selected items together at either the top or bottom of the list views.

Compass dashboard limitations

Here are some limitations when viewing the Compass dashboard:

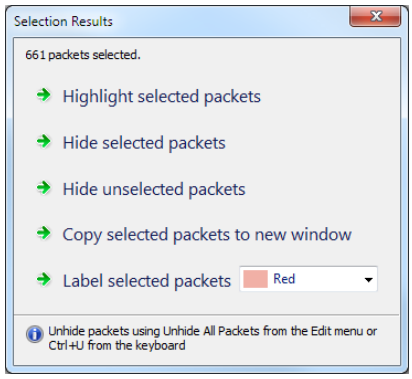
- A Compass dashboard has a limit of 1,000,000 statistic items (protocols, flows, nodes, channels, WLAN, VLAN, data rates, applications) per second.
- For real-time captures, the Compass dashboard shows only the latest four hours of data. Every 10 minutes after the four hour mark, Compass slices off the first 10 minutes of available data. This limit can be adjusted through the Compass options dialog.
- Compass expects to receive packets in ascending order—a packet received with a timestamp earlier than the previous packet is discarded.
- There must be at least 500MB of free disk space or Compass stops generating/saving statistic information until enough disk space is made available.

Select related packets

You can use the 'Select Related Packets' feature to filter selected items from the Data Source widgets and network utilization graph.

To select related packets:

1. Select one or more statistic items from the Data Source widgets, and adjust the time range currently selected in the network utilization graph.
2. Click **Select Related Packets** at the top of the graphs and select the desired AND or OR logic. Packets matching the selected statistic item are filtered and highlighted in the **Packets** view, and the **Selection Results** dialog appears.



3. Click **Highlight selected packets**, **Hide selected packets**, **Hide unselected packets**, **Copy selected packets to new window**, or **Label selected packets**.

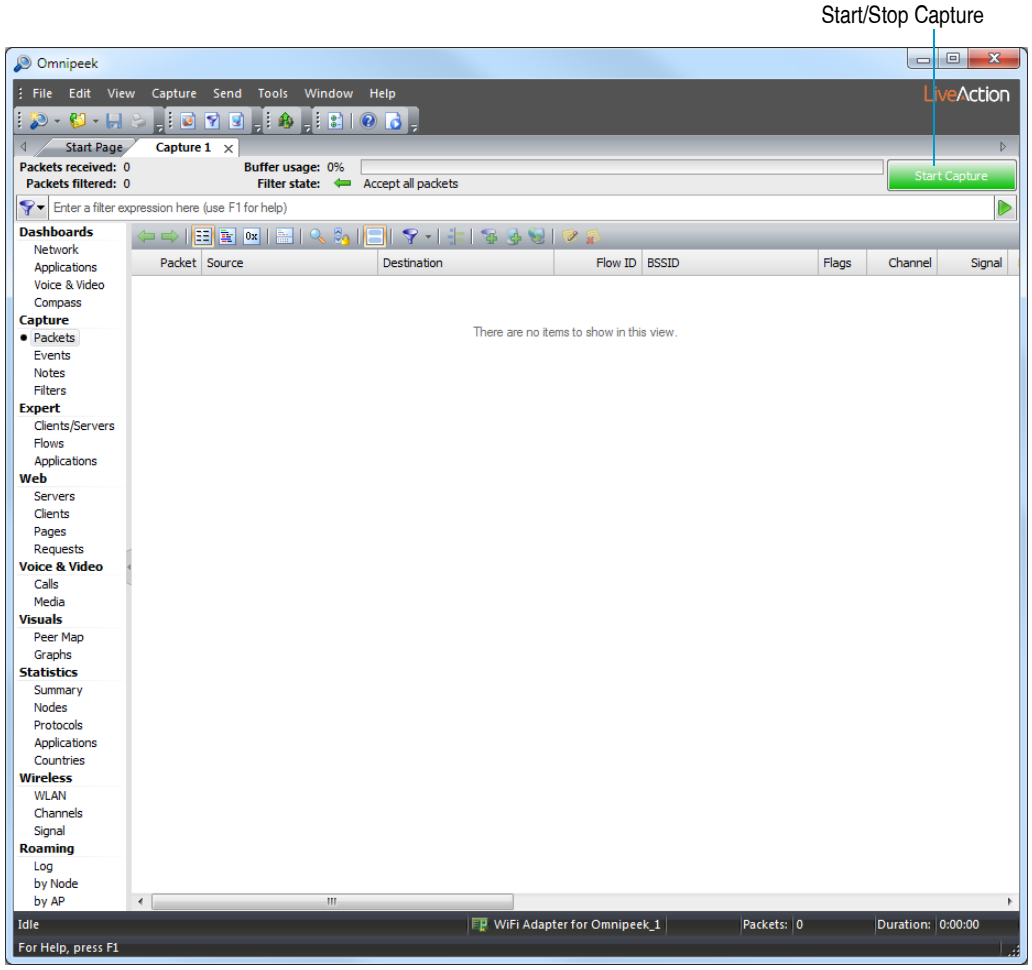
Note Selecting packets based on protocols will include child protocols in the protocol hierarchy.

Viewing and Decoding Packets

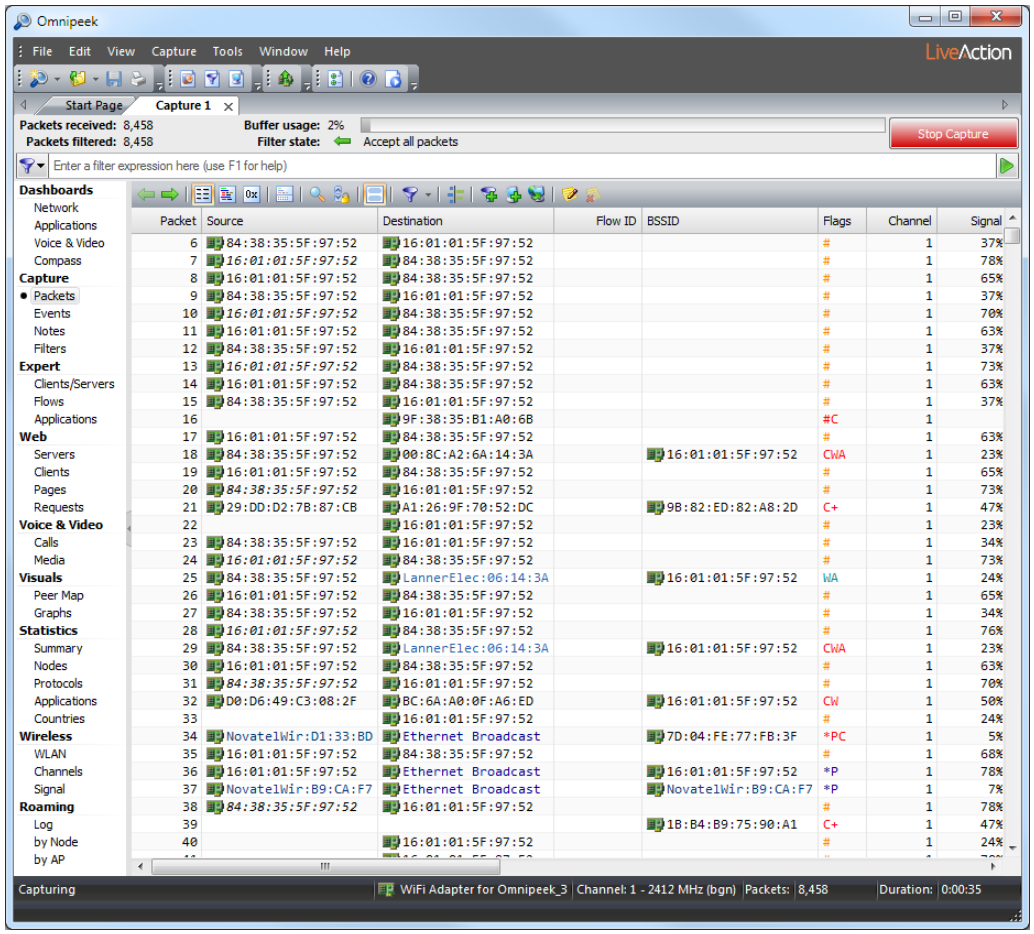
Packets are the units of data carried on the network and the basis for all higher level network analysis. The **Packets** view of a capture window is where you can view information about the individual packets transmitted on your network. Capture windows also allow you to view the decoded packet contents, in raw, hexadecimal and ASCII format.

The packets view

4. Open a capture window and click the **Packets** view.



5. Click **Start Capture**. Packets begin populating the capture window.



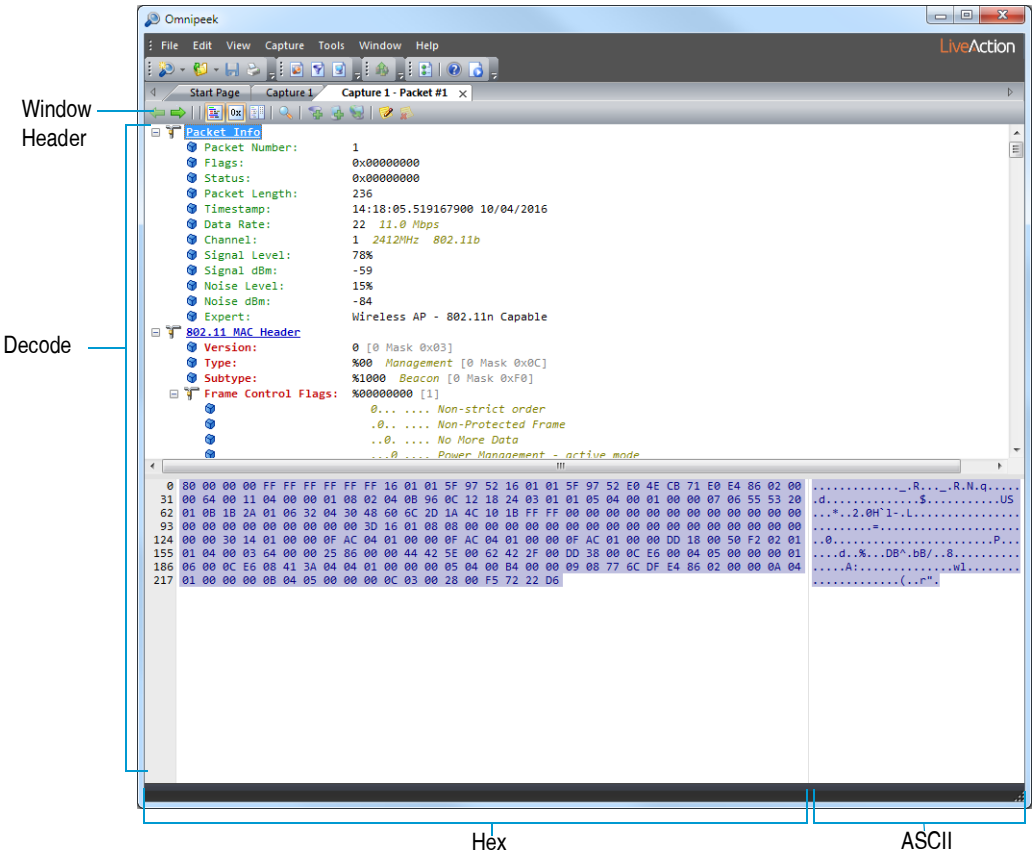
6. Right-click a column heading to hide or display available column headings.
7. Right-click a packet row and select **Insert into Name Table...**. The **Insert Name** dialog appears.
8. Select a *Node type* icon to represent this packet. The *Node type* options let you choose an icon that will appear in the Packet List, for example, *Workstation*, *Server*, *Router*, or *Access Point*.

The packet decode window

Network problems are revealed more quickly by looking at the detailed information contained in individual packets. Looking into the packets can help you troubleshoot your network, track down a security breach, or examine protocol structure and compliance.

To view the decode of a packet:

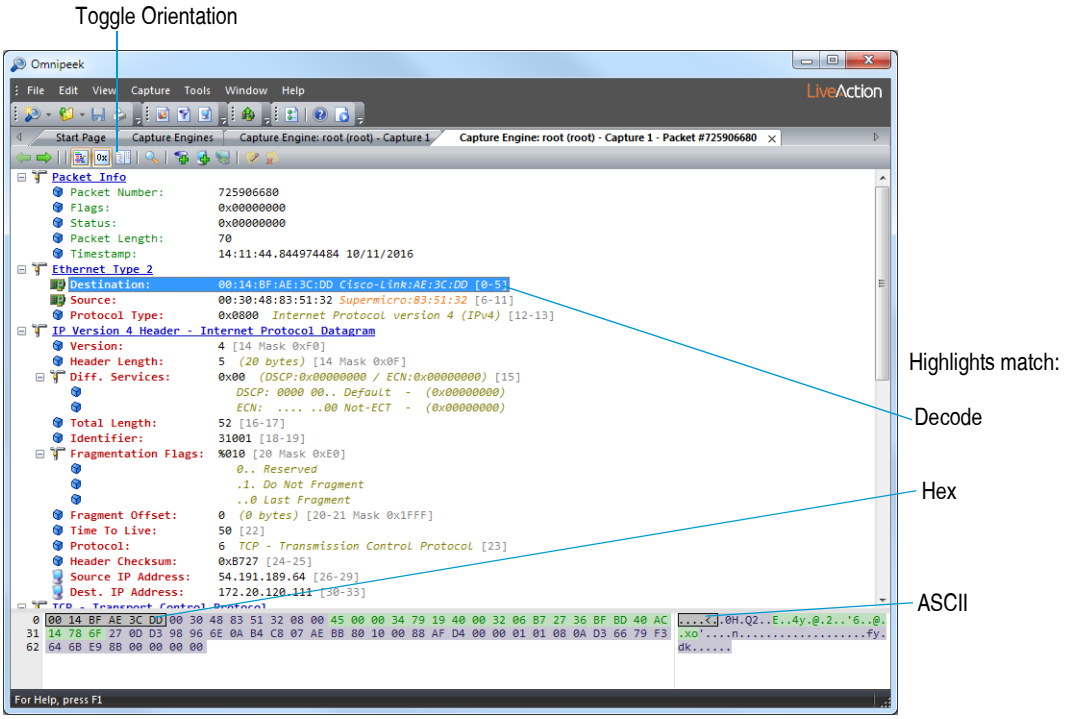
1. Double-click a packet in the **Packets** view of a capture window. The Packet Decode window appears. The decoded packet data is presented in byte order from top to bottom.



Tip You can open individual Packet Decode windows for up to 10 packets at once. When multiple packets are selected in the active Packet List, click **Enter** to open them all.

2. Click on the - minus or + plus signs in the margin to collapse or expand the view of any header section.
   - **Window header**: Click **Decode Previous** or **Decode Next** at the top of the window to step through the packets shown in the Packet List of the active capture window.
   - **Decode view**: The body of the **Decode** view is laid out in the same order as it appears in the packet. A quick glance at this section often reveals the source of trouble. Problems like a misconfigured client, or incompatible versions of the same protocol from different vendors can be easily understood when you can see and compare the packets themselves.
   - **Hexadecimal view**: The **Hex** view at the bottom of the decode window shows the offset of the first character in each line, the raw packet data in hex, and the ASCII version of raw packet data
3. Highlight an item in one part of the window. The same bytes of the packet are highlighted in all the other views or panes as well. The highlight matches in the Decode, Hex, and ASCII panes.

   Color coding is used to link the **Decode** view with the **Hex** view for both Hex and its ASCII equivalent. The Hex and ASCII views are in turn linked to the color of the protocol shown in the Protocols column of the Packet List.



Tip Use **Toggle Orientation** in the toolbar to tile the Decode and Hex views vertically or horizontally.

Creating Filters

Filters let you focus on specific traffic. If you want to check a problem between two particular devices, perhaps a computer and a printer, address filters can capture just the traffic between these two devices. If you are having a problem with a particular function on your network, a protocol filter allows you to focus on traffic related to that particular function.

Filters work by testing packets against the criteria specified in the filter. Packets whose contents meet these criteria match the filter. You can build filters to test for just about anything found in a packet: addresses, protocols, sub-protocols, ports, error conditions, and more. Filters are so easy to create in that you can often create a custom filter on-the-fly while analyzing suspect traffic on your network.

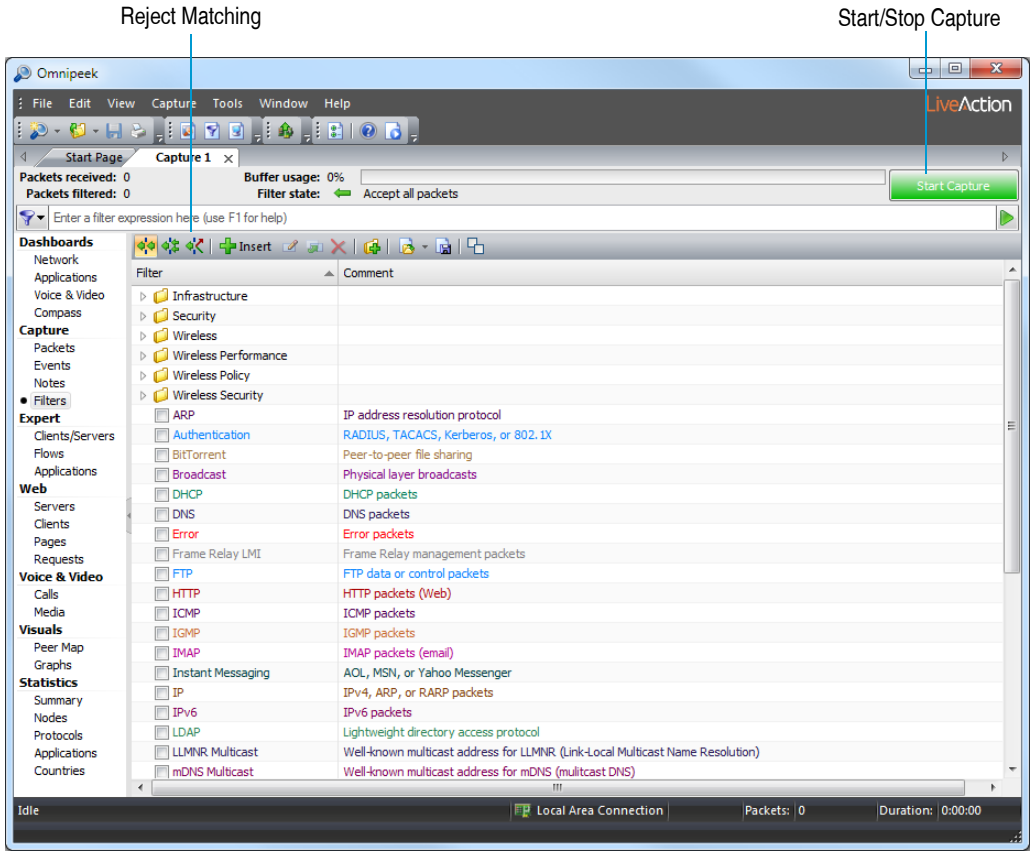
Note Filters created from a connected Capture Engine are available to that Capture Engine only. If you are not connected to a Capture Engine and you create a filter, that filter is available for local captures only.

Enabling a filter

In addition to the filters that you create, the Omnipeek and the Capture Engines include numerous predefined filters. You can enable one or more filters when capturing or monitoring packets.

To enable filters when capturing packets:

4. Click the **Filters** view in a capture window.



5. Select the filter or filters that you want to enable.

> **Note** For a Capture Engine, you will need to send your selections to the Capture Engine by clicking the bar below the toolbar icons labeled *Click here to send changes*.

6. Click **Start Capture** to begin capturing packets. Any packets that match the filters that are enabled are placed into the capture buffer.

   Alternately, you can choose to place the packets that do not match the filter in the capture buffer by clicking **Reject Matching**.

Creating filters with the make filter command

You can use the **Make Filter** command to easily create a filter based on the address, protocol, and port settings of an existing packet, node, protocol, conversation, or packet decode.

To create a filter with the Make Filter command:

1. Right-click a packet, node, protocol, conversation, or packet decode item from one of the views available in a capture window and choose **Make Filter**. The **Insert Filter** dialog appears with the Address, Protocol, and Port settings already configured with the information from the packet that was selected.
2. Enter a new name in the *Filter* text box and make any additional changes.
3. Click **OK**. The new filter is now available whenever a list of available filters is displayed.
4. To enable the new filter in your capture window, click the **Filters** view and select the check box of the new filter. The filter is applied immediately, even if a capture is already under way.

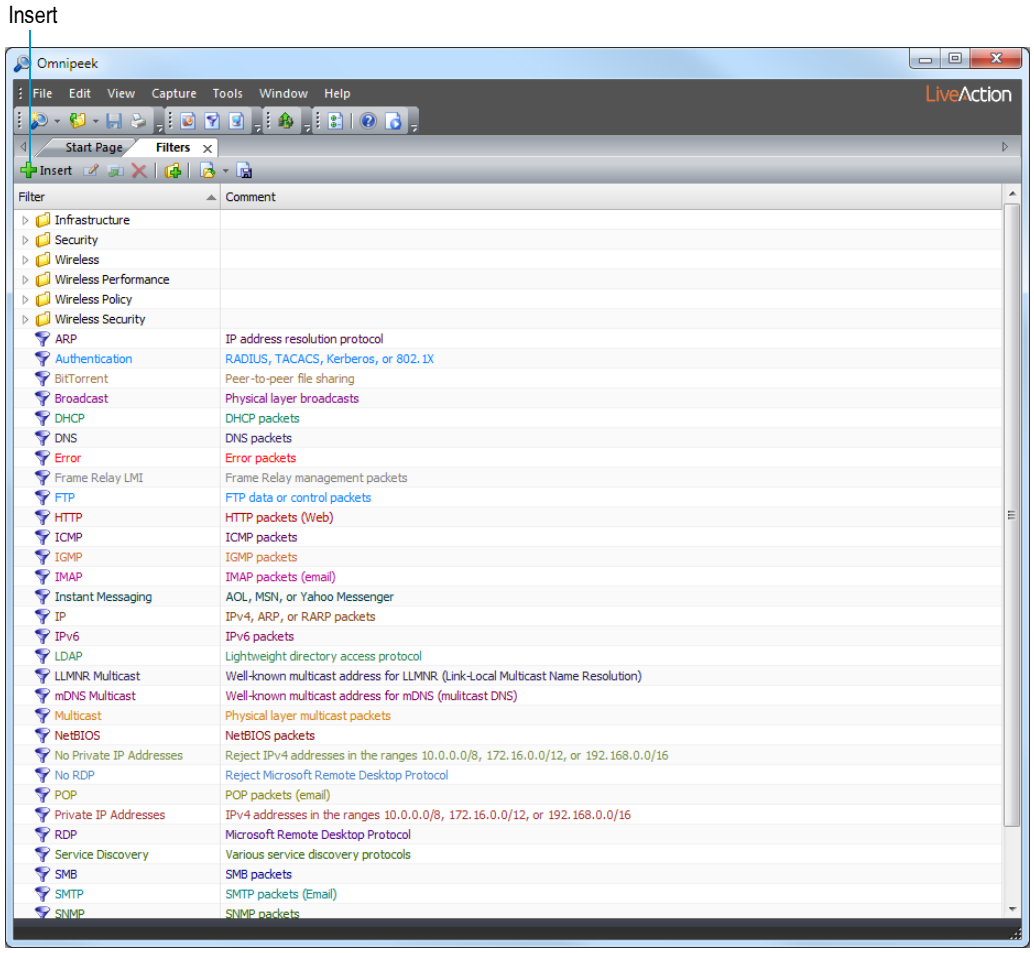
Creating a simple filter

You can create a simple filter by manually entering the parameters for the filter that you want to create. Unlike creating a filter using the Make Filter command, you will have to manually define the parameters (address, protocol, and port settings) for the filter you want to create.

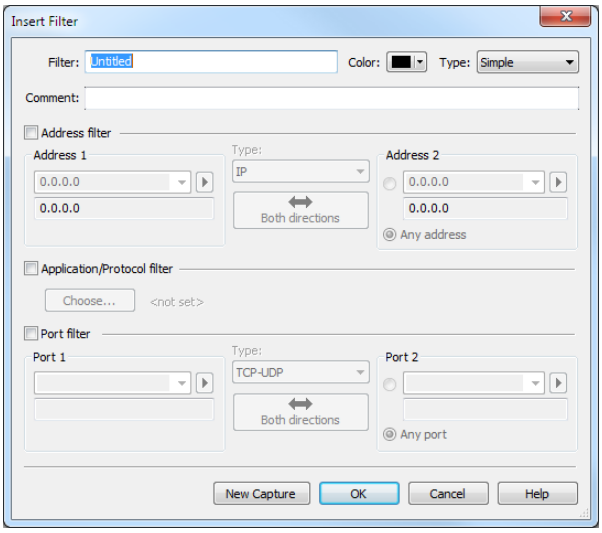
Note For information on creating more advanced filters, refer to the *Omnipeek User Guide* or online help.

To create a simple filter by defining an address and protocol:

1. Do one of the following to open the **Filters** view:
   - On the **View** menu, click **Filters** (filters for local captures only)
   - Click the **Filters** view in an open capture window
   - Click the *Filters* options from the Capture Engine **Capture Options** dialog



2. Click **Insert**. The **Insert Filter** dialog appears.



3. Give your new filter a name.
4. Complete the address, protocol, or port setting information and click **OK**. The new filter is now available whenever a list of available filters is displayed.
5. To enable the new filter in your capture window, click the **Filters** view and select the check box of the new filter. The filter is applied immediately, even if a capture is already under way.

Tip Click **New Capture** to create a new capture window that uses the filter that you are defining in the **Insert / Edit Filter** dialog as the only enabled filter.

Expert Troubleshooting

The Expert features in Omnipeek and the Capture Engines provide real-time analysis of response time, throughput, and a wide variety of network events and potential problems in a flow-centered view of traffic in a capture window. You can also link end-user satisfaction with the performance of a network application through the Application Performance Index (Apdex), an open standard that defines methods for reporting application performance. See *Applications view* on page 58.

The Expert EventFinder detects nearly 200 different network events and provides descriptions, possible causes, and possible remedies organized by OSI layer. Depending on your version of the program, network events specifically related to VoIP, Wireless, WAN, and user-defined Network Policy items are also shown. See *Using the EventFinder* on page 57.

The Expert view window

The Expert **Clients/Servers** view makes it easy to track events and to see them in the context of peer-to-peer or client-server traffic patterns.

To display events in the Expert Clients/Servers view:

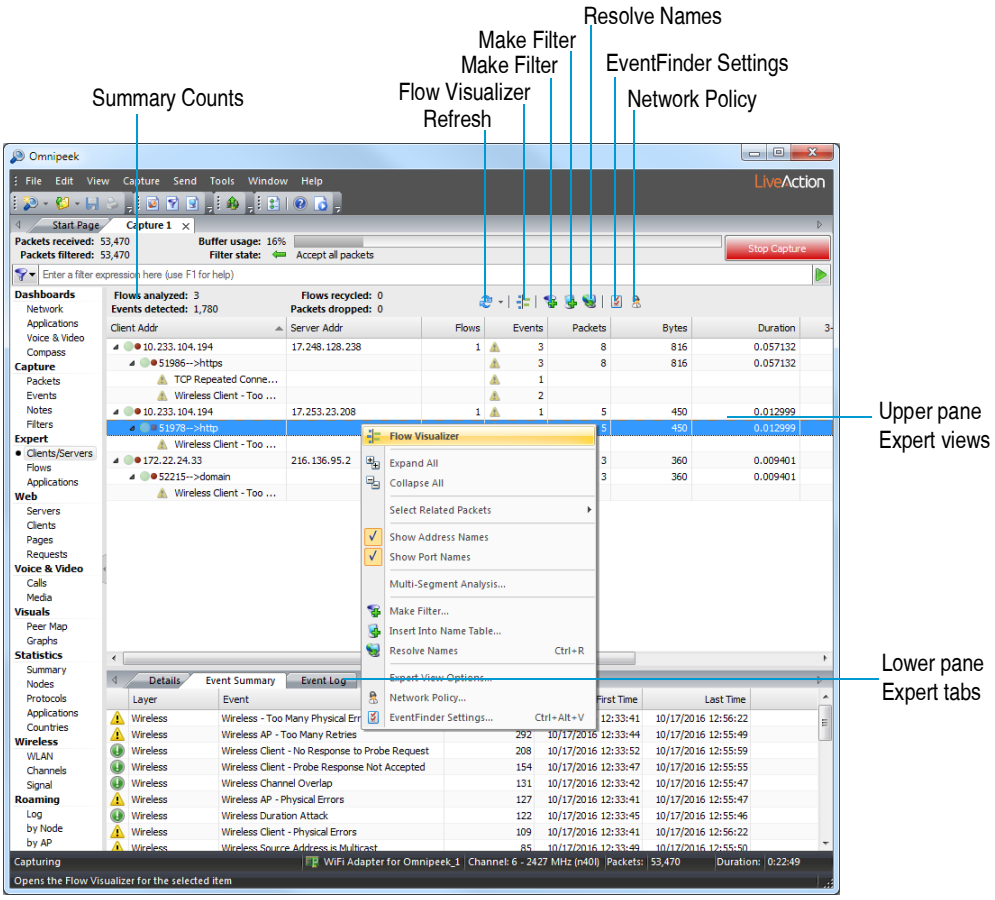
1. Select *Clients/Servers* under **Expert** in the navigation bar of a capture window.

   Pairs of nodes are displayed at the top level, individual conversations (flows) underneath them, and individual events nested under each flow. Color coded traffic indicator lights show whether or not packets were received in the last few seconds:

   - green (active)
   - light green (inactive)

   Smaller LED lights appear to the right of the traffic indicators when an event has been detected:

   - A red LED indicates one or more events whose severity is Major or Severe.
   - A yellow LED indicates one or more events whose severity is Informational or Minor.



2. Right-click in the upper pane to collapse or expand the hierarchy to display the most relevant information. When expanded, Expert events are displayed by ports. Ports are shown with directional arrows.

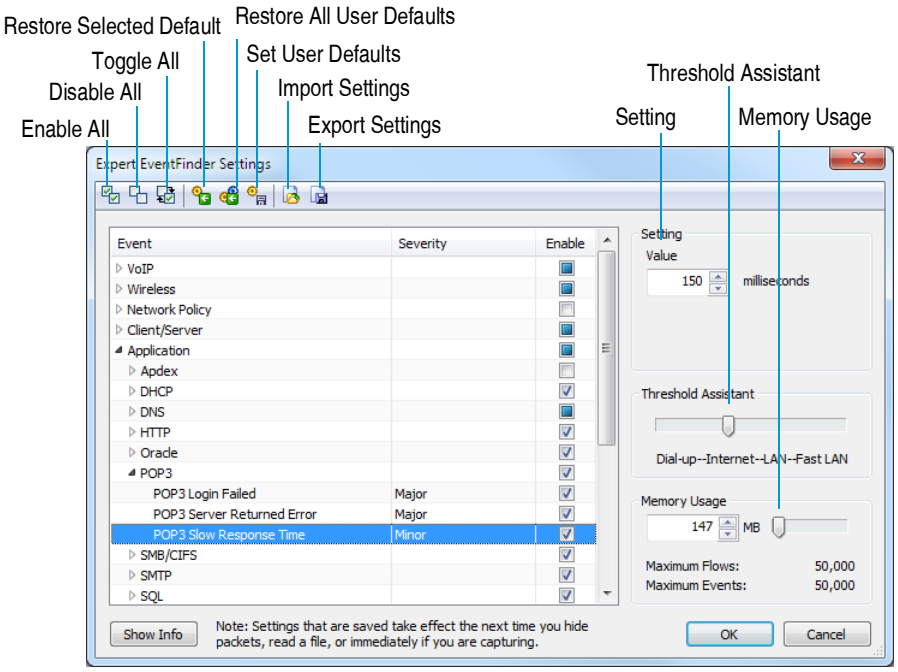
> **Tip** In the Expert **Clients/Servers** view, sorting by *Events* can help pinpoint potential problems on your network.

Using the EventFinder

You can view more details about individual network events in the **Expert EventFinder Settings** dialog.

To open the Expert EventFinder Settings window:

1. Right-click in the **Clients/Servers** view and select **Expand All**.
2. Select an individual expert event from the expanded **Clients/Servers** view.
3. Click **EventFinder Settings**. The **Expert EventFinder Settings** window appears with this expert event highlighted, as shown below:



Note You can also right-click an event inside the *Event Summary* or *Event Log* tab and select **EventFinder Settings** to display the **Expert EventFinder Settings** window.

4. Click **Show Info** to see a complete description, possible causes, and possible remedies for this network event.

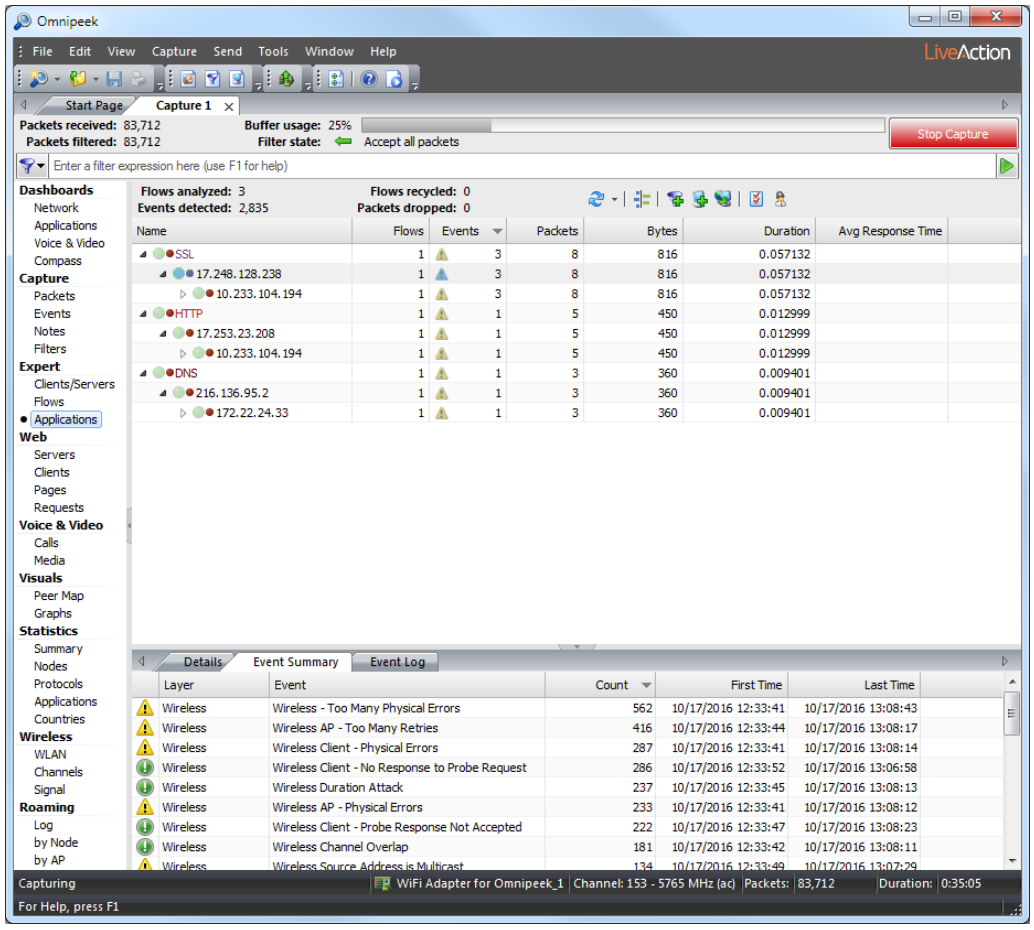
   The **Expert EventFinder Settings** window also provides information on what sensitivity or setting value was used to flag this event as significant. You can configure the value, threshold, and memory settings for each individual expert event in the EventFinder window. You can also save these settings by exporting them to a file and importing them later into another capture.

Applications view

The Expert *Applications* view categorizes each flow by application. Flows are grouped together by application, providing a hierarchical view of the use of each application, first by server, then by client, and then by port. This view allows you to see who is using each application on your network and how each application is performing.

To display the Applications view:

- Select *Applications* under **Expert** in the navigation bar of a capture window.


Omnipeek
File Edit View Capture Send Tools Window Help
LiveAction
Start Page
Capture 1
Packets received: 83,712
Packets filtered: 83,712
Buffer usage: 25%
Filter state: Accept all packets
Stop Capture
Enter a filter expression here (use F1 for help)
Dashboards
Network
Applications
Voice & Video
Compass
Capture
Packets
Events
Notes
Filters
Expert
Clients/Servers
Flows
Applications
Web
Servers
Clients
Pages
Requests
Voice & Video
Calls
Media
Visuals
Peer Map
Graphs
Statistics
Summary
Nodes
Protocols
Applications
Countries
Wireless
WLAN
Channels
Signal
Roaming
Log
by Node
by AP
Flows analyzed: 3
Events detected: 2,835
Flows recycled: 0
Packets dropped: 0
Name
Flows
Events
Packets
Bytes
Duration
Avg Response Time
SSL 1 3 8 816 0.057132
17.248.128.238 1 3 8 816 0.057132
10.233.104.194 1 3 8 816 0.057132
HTTP 1 1 5 450 0.012999
17.253.23.208 1 1 5 450 0.012999
10.233.104.194 1 1 5 450 0.012999
DNS 1 1 3 360 0.009401
216.136.95.2 1 1 3 360 0.009401
172.22.24.33 1 1 3 360 0.009401
Details
Event Summary
Event Log
Layer
Event
Count
First Time
Last Time
Wireless Wireless - Too Many Physical Errors 562 10/17/2016 12:33:41 10/17/2016 13:08:43
Wireless Wireless AP - Too Many Retries 416 10/17/2016 12:33:44 10/17/2016 13:08:17
Wireless Wireless Client - Physical Errors 287 10/17/2016 12:33:41 10/17/2016 13:08:14
Wireless Wireless Client - No Response to Probe Request 286 10/17/2016 12:33:52 10/17/2016 13:06:58
Wireless Wireless Duration Attack 237 10/17/2016 12:33:45 10/17/2016 13:08:13
Wireless Wireless AP - Physical Errors 233 10/17/2016 12:33:41 10/17/2016 13:08:12
Wireless Wireless Client - Probe Response Not Accepted 222 10/17/2016 12:33:47 10/17/2016 13:08:23
Wireless Wireless Channel Overlap 181 10/17/2016 12:33:42 10/17/2016 13:08:11
Capturing
WiFi Adapter for Omnipeek_1
Channel: 153 - 5765 MHz (ac)
Packets: 83,712
Duration: 0:35:05
For Help, press F1

Multi-Segment Analysis

About Multi-Segment Analysis

Multi-Segment Analysis (MSA) in Omnipeek allows you to quickly and easily locate, visualize, and analyze one or more flows as they traverse several capture points on your network from end-to-end. MSA provides visibility and analysis of application flows across multiple network segments, including network delay, packet loss, and retransmissions.

MSA can quickly pinpoint problems and their root causes across multiple segments, bring problematic flows together, and create an analysis session, report anomalies, and provide graphical visualization of multiple segments across the network.

An easy to use MSA wizard allows you to create MSA projects from either multiple Capture Engines located on your network, or from multiple existing capture packet files. Additionally, MSA projects can be created by right-clicking various views from the navigation pane of a capture window.

Important! The time it takes for Omnipeek to build and display an MSA project is dependent on the number of segments, the number of flows, and the number of packets in each flow. MSA includes a limit of 100,000 packets per flow (modifiable from Multi-Segment Analysis Options), but there is no hard limit to the number of segments or flows that can be included in a project. Be selective when choosing data for your MSA projects. If you find that an MSA project is taking too long to build, you can cancel out and reduce your data set.

In order to facilitate the creation of MSA projects based on forensic searches, the following best practices are suggested:

- Each Capture Engine should have a unique name. This can be done via the Capture Engine Manager, or the Capture Engine Wizard.
- Make sure the time is accurate on all of the Capture Engines. If possible, configure the Capture Engine to use an NTP server.
- Give each capture a unique name. For instance, name the captures based on the network segments.
- Once an MSA project (*.msa* file) has been created, you may want to save the packet files that were used to create the MSA project for the following reasons:
  - The packet files will be needed again if you want to add another segment to the MSA project.
  - You may want to open a trace file related to a particular segment, to see different Omnipeek views, such as the Packets or Flows view.
  - It may be necessary to rebuild MSA projects to take advantage of new MSA features in future versions of Omnipeek.

In addition, the following Capture Option settings must be enabled for MSA-based forensic searches:

- 'Capture to disk'
- 'Timeline Stats' (on Classic Capture Engines only)

Note MSA-based forensic searches require Timeline Stats. Classic Capture Engines support Timeline Stats starting with version 6.8.

MSA project window

Once configured and created using the MSA wizard, an MSA project window is displayed as shown below. The MSA project window consists of the following parts: Flow List, Flow Map, and Ladder.

Note When calculating the delay values for the flow map and ladder, MSA assumes that the client is on the left, and the server is on the right. If you create MSA projects that include multiple flows, all of the flows in the project should be initiated from the same direction. For example, flows initiated by two nodes on the private side of a firewall would be suitable to include in a single MSA project. Flows initiated by a node on the private side of a firewall, and flows initiated by a node on the public side of a firewall would not be suitable to include in a single MSA project.

Flow list

The flow list displays a hierarchical list of flows for each capture source, including relevant information for each flow (client/server addresses and ports, protocols, packet counts, etc.) The flow list is hierarchical, with flows at the top level, and capture segments listed below the flow. Each capture segment includes statistics for that flow. Selecting the check box next to a flow displays that flow in the flow map and ladder diagram below.

Note For any MSA project that has multiple flows, only one flow at a time can be selected in the flow list. The flow that is selected is displayed in the flow map and ladder diagram.

- *Column header*: Displays the column headings currently selected. Right-click the column header to enable/disable columns. Here are the available columns:
  - *Flow/Segment*: The name of the flow or segment.
  - *Client Addr*: The address of the client for the flow.
  - *Client Port*: The port on which the Client or Client Addr was communicating in the flow.
  - *Server Addr*: The address of the Server or Server Addr for the flow.
  - *Server Port*: The port on which the Server or Server Addr was communicating in the flow.
  - *Protocol*: The protocol under which the packets in the flow were exchanged.
  - *Packets*: The number of packets in the selected flow.
  - *Client Packets*: The total number packets sent from the Client or Client Addr in the flow.
  - *Server Packets*: The total number of packets sent from the Server or Server Addr in the flow.
  - *Packets Analyzed*: The total number of packets in the flow that were analyzed by Omnipeek's MSA component. 'Packets Analyzed' will be the same as 'Packets,' unless the number of packets in the flow exceeds the packet limit, as configured in MSA options.
  - *Packets Lost*: The number of packets missing in the segment. Packets which are identified as 'lost' in a particular segment appeared in an least one other segment in the MSA project.

- *Client Packets Lost*: The number of packets lost in the client direction.
- *Server Packets Lost*: The number of packets lost in the server direction.
- *Client Retransmissions*: The number of TCP retransmissions sent by the client.
- *Server Retransmissions*: The number TCP retransmissions sent by the server.
- *Start*: The timestamp of the first packet in the flow.
- *Finish*: The timestamp of the final packet in the flow.
- *Duration*: The elapsed time, from the first to the last packet in the flow.
- *TCP Status*: Notes whether the TCP session is open or closed.
- *Columns...*: Displays a dialog that lets you enable/disable and organize columns.
- *Show All Columns*: Displays all available columns.

Flow map

The flow map displays a graphical representation of the segments of the selected flow. Each segment in the flow is displayed from end-to-end (client on the left and the server on the right), along with timing statistics (average delay, minimum delay, and maximum delay) between each segment. Additionally, the hop count between each segment is also displayed (the little number inside the cloud between the segments).

Flow map viewing tips

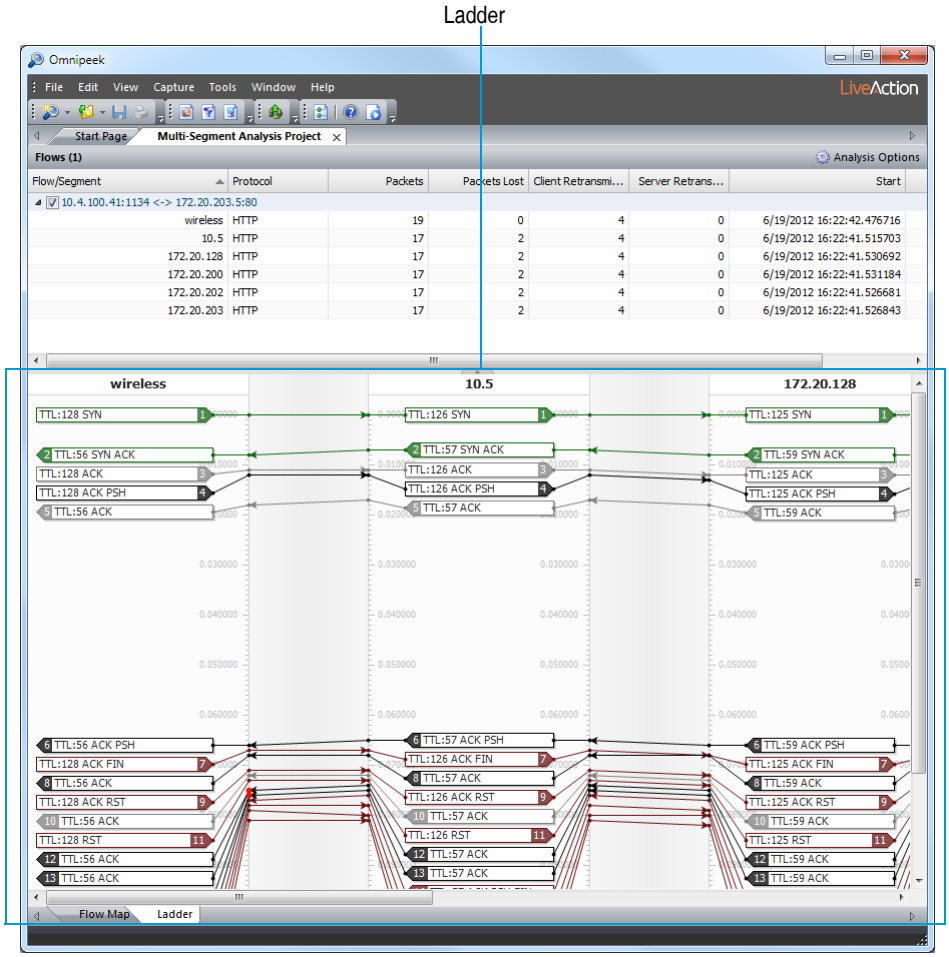
Here are some useful tips when viewing the data inside the flow map:

- Hover over segments names and clouds to view tooltips displaying more data.

- Press the Ctrl key and use your scroll wheel (Ctrl+Wheel) to change segment widths.
- Arrows show the direction in which data flows.
- The client and server arrows use the same colors as from *Client/Server Colors* (**Tools** > **Options**).
- The number in the clouds are hop counts, as determined by the Time to Live (TTL) values within the packets. If there is one number in the cloud, then both the client and server hops are the same. If there are two numbers in the cloud, then the client and server hops are different, indicating that the client and server paths are different. If there are multiple paths in one direction, no hop count is displayed for this direction. Hop counts greater than one are displayed in red. The TTL of each packet can be displayed in the Ladder diagram.

Ladder

The ladder diagram displays the flow of packets amongst the segments represented by the capture sources, along with information such as timing.



Ladder viewing tips

Here are some useful tips when viewing the data inside the ladder diagram:

- Hover over packet boxes to view tooltips displaying more data.
- Arrows show the direction in which data flows.
- Green boxes are the packets that open the flow (SYN and SYN-ACK).
- Black boxes are packets with non-zero payload (packets that carry data).
- Gray boxes are packets that have zero payload (probably just ACK packets).

- Red boxes are packets that close the connection (FIN or RST).
- Right-click inside the diagram to show/hide additional statistics, or to adjust the time scale of the ladder.
- The following keyboard/scroll wheel shortcuts are available from the ladder display:
  - Wheel+Ctrl: Changes the time scale.
  - Wheel+Ctrl+Shift: Zoom the time scale.
  - Wheel+Ctrl+Shift+Alt: Change the segment width.
  - Ctrl+Alt+Shift+F9: Save ladder display to text.

Creating an MSA project

To create an MSA project, you must use the MSA wizard. The MSA wizard guides you through the creation of an MSA project, and includes steps for setting up the project parameters and ultimately, displaying the MSA project window. There are multiple ways to start the MSA wizard. Additionally, depending on which way you start the wizard, there are multiple entry points to the MSA wizard. You can start the MSA wizard in the following ways:

- From the **File** menu, choose **New Multi-Segment Analysis Project**.... The MSA wizard appears, and prompts you to create an MSA project by either searching for packets on remote engines, or using packet files:
  - **Searching for packets on remote engines**: Select this option and the MSA wizard first guides you through choosing a time range to search, and a filter to apply (making a filter for IP/port pairs is recommended, though any filter supported by Omnipeek will work). Additional wizard screens guide you through choosing which Capture Engines and which capture sessions per Capture Engine you wish to search against.

    Finally, the wizard performs the search, and the relevant packets are downloaded to Omnipeek for analysis. From there, it works the same way it does for doing multi-segment analysis from files, except that the files are already entered for you (they're the files downloaded from the Capture Engines). You can reorder the segments, rename the segments, change the time offsets, and save the output to an *.msa* file.
  - **Use packet files**: Select this option and the MSA wizard guides you through choosing which files to use (one file per segment), and the time offsets between them. You can also name each segment, and reorder them. Then you can save the resulting project to an *.msa* file, which can be reloaded later. The *.msa* file contains all the analysis, so you don't have to do any of this setup again.
- From the **Packets** view in the navigation pane: Right-click one or more packets and choose **Multi-Segment Analysis**.... The MSA wizard appears and guides you through the creation of the MSA project, beginning with choosing a time range to search, and a filter to apply.
- From any of the **Expert** views (**Clients/Servers**, **Flows**, and **Applications**) in the navigation pane: Right-click one or more flows and choose **Multi-Segment Analysis**.... The MSA wizard appears and guides you through the creation of the MSA project, beginning with choosing a time range to search, and a filter to apply. The **Multi-Segment Analysis**... option only appears for IPv4 TCP flows. MSA does not support UDP or IPv6 flows.
- From any of the **Web** views (**Servers**, **Clients**, **Pages**, and **Requests**) in the navigation pane: Right-click one or more servers, clients, pages, or requests and choose **Multi-Segment Analysis**.... The MSA wizard appears and guides you through the creation of the MSA project, beginning with choosing a time range to search, and a filter to apply.
- From the **Nodes** and **Protocols** views in the navigation pane: Right-click one or more nodes or protocols and choose **Multi-Segment Analysis**.... The MSA wizard appears and guides you through the creation of the MSA project, beginning with choosing a time range to search, and a filter to apply.

Important! The time it takes for Omnipeek to build and display an MSA project is dependent on the number of segments, the number of flows, and the number of packets in each flow. MSA

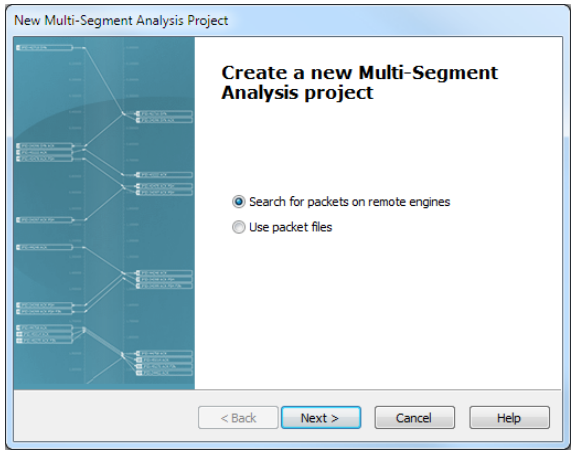
includes a limit of 100,000 packets per flow (modifiable from Multi-Segment Analysis Options), but there is no hard limit to the number of segments or flows that can be included in a project. Be selective when choosing data for your MSA projects. If you find that an MSA project is taking too long to build, you can cancel out and reduce your data set.

Using the MSA wizard

The MSA wizard guides you through the creation of an MSA project. You can access the MSA wizard in numerous ways as described in *Creating an MSA project* on page 65. This section describes the various screens of the MSA wizard.

Create a new multi-segment analysis project

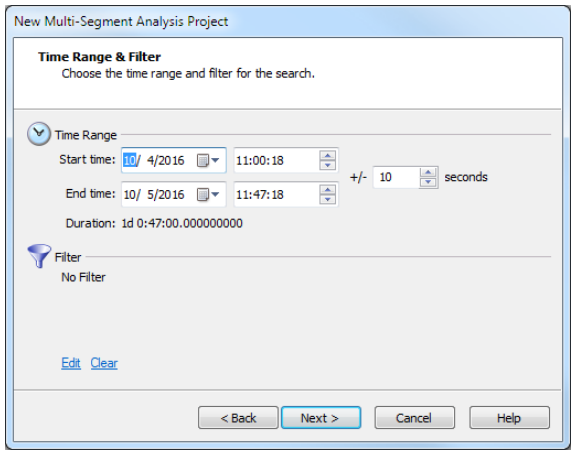
The **Create a new Multi-Segment Analysis project** dialog of the MSA wizard is available by choosing **File** > **New Multi-Segment Analysis**.... The dialog lets you create a new multi-segment analysis project from scratch.



- *Search for packets on remote engines*: Select this option to create an MSA project based on packets obtained from one or more Capture Engines.
- *Use packet files*: Select this option to create an MSA project based on one or more packet files.

Time range & filter

The **Time Range & Filter** dialog of the MSA wizard lets you choose a time range and filter to apply to your search.

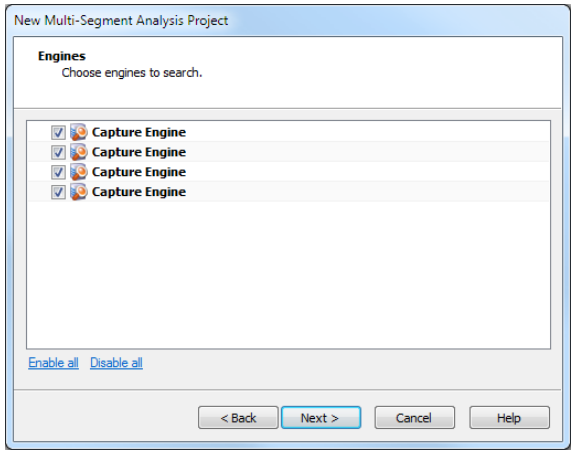


- *Start time*: Select or enter the start date and time of the range you wish to search.

- *End time*: Select or enter the end date and time of the range you wish to search.
- *+/- seconds*: Select or enter the number of seconds to add to the search both before the start time and after the end time.
- *Duration*: Displays the amount of time between the start and end time specified.
- *Filter*: Displays any filters currently defined for the search.
- *Edit*: Click to display the Edit Filter dialog, where you can define simple and advanced filters based on any combination of addresses, protocols, and ports. A packet must match all of the conditions specified in order to match the filter.
- *Clear*: Click to remove any filters currently defined for the search.

Engines

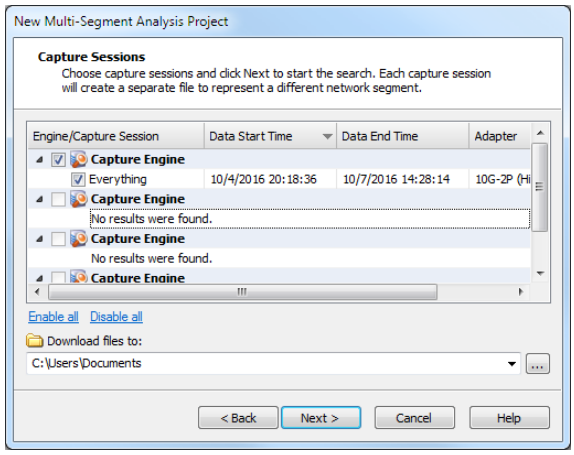
The **Engines** dialog displays the groups and Capture Engines currently listed in the Omnipeek Capture Engines window. If you had selected the option to *Search for packets on remote engines* earlier in the MSA wizard, the **Engines** dialog appears after clicking **Next** in the **Time Range & Filter** dialog of the MSA wizard.



- Select the check box of the Capture Engines you want to search in your MSA project. If you are not already connected to the Capture Engine, you are first prompted to connect to the Capture Engine by entering domain, username, and password information.
- *Enable all*: Click this option to select the check box of all groups and Capture Engine displayed in the dialog.
- *Disable all*: Click this option to clear the check boxes of all groups and Capture Engines displayed in the dialog.

Capture sessions

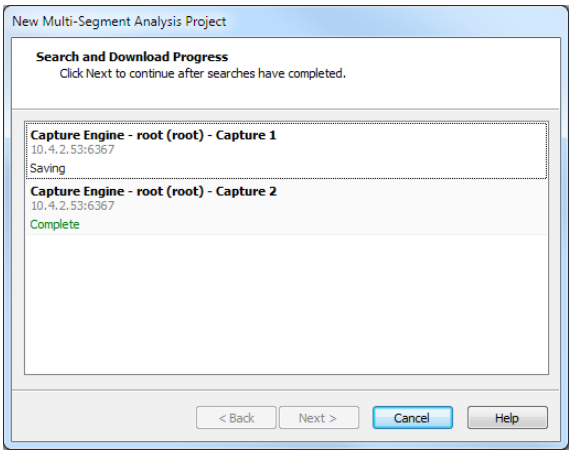
The **Capture Sessions** dialog displays the capture sessions found in each of the of the selected Capture Engines. If you had selected the option to *Search for packets on remote engines* earlier in the MSA wizard, the **Capture Sessions** dialog appears after clicking **Next** in the **Engines** dialog of the MSA wizard. A separate **.wpz* file is created for each capture session selected, and each file represents a different network segment. When performing multi-segment analysis, Omnipeek uses **.wpz* files to build the MSA project.



- *Column header*: Displays the column headings currently selected. Right-click the column header to enable/disable columns. Here are the available columns:
  - *Engine/Capture Session*: The capture sessions available from the Capture Engines selected earlier. Select the check box of the capture sessions you want to search in your MSA project. Capture Engine captures that have both '*Capture to disk*' and '*Timeline Stats*' enabled in the capture options, and all TimeLine network recorder captures that have '*Capture to disk*' enabled in the capture options, appear in the Capture Sessions screen. (MSA-based forensic searches require '*Timeline Stats*.')
  - *Session Start Time*: The start time of the capture.
  - *Data Start Time*: The start time of when data first appeared in the capture.
  - *Data End Time*: The end time of when data last appeared in the capture.
  - *Size*: The size (in MB) of the capture session.
  - *Packets*: The number of packets in the capture session.
  - *Packets Dropped*: The number of dropped packets in the capture session.
  - *Media*: The media type of the capture session.
  - *Adapter*: The name of the adapter used for the capture session.
  - *Adapter Address*: The address of the adapter used for the capture session.
  - *Link Speed*: The link speed of the adapter used for the capture session.
  - *Owner*: The owner name of the adapter used for the capture session.
- *Enable all*: Click this option to select the check box of all Capture Engine and capture sessions displayed in the dialog.
- *Disable all*: Click this option to clear the check box of all Capture Engine and capture sessions displayed in the dialog.
- *Download files*: Choose the location of where to save the **.wpz* files created for each of the selected capture sessions.

Progress

The **Progress** dialog displays the status for saving **.wpz* files used for multi-segment analysis. If you had selected the option to *Search for packets on remote engines* earlier in the MSA wizard, this dialog appears after clicking **Next** in the **Capture Sessions** dialog of the MSA wizard.



Each entry in the dialog lists the following:

- Capture Engine and capture session name
- Capture Engine IP address and port
- Current status for each file

The progress status messages are as follows:

- *Search Progress*: Progress of the forensic search, based on the time range and filter specified in the Wizard
- *Saving*: Search results are saved as a *.wpz* file on the engine
- *Deleting Search*: The forensic search is deleted on the engine
- *Download Progress*: The *.wpz* file is downloaded to the Omnipeek computer
- *Deleting Remote File*: The *.wpz* file is deleted from the engine
- *Complete*: The entire process is complete. Once you see *Complete* for all capture segments, click **Next** to continue building the MSA project

Tip You can cancel the progress of any one of the capture segments by right-clicking and selecting **Cancel**. You can cancel any of the above stages, except for the *Saving* stage.

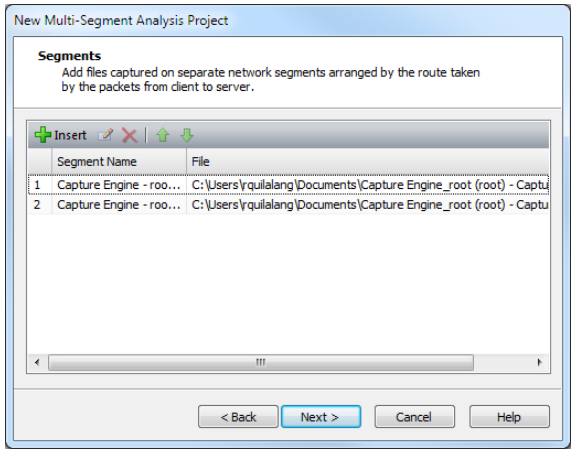
Segments

This **Segments** dialog lets you add supported capture files captured on separate network segments to your MSA project. In order for the MSA analysis to display correctly in your flow maps and ladder diagrams, each segment file must be properly ordered by the route taken from client to server (when displayed in the flow map and ladder, the client is on the left and the server is on the right). You can manually choose to arrange the files in the dialog.

Tip If you do not manually arrange the files by the route taken from client to server, you can use the auto-arrange feature available from the **Analysis Options** dialog. See *MSA project analysis options* on page 71.

Note When calculating the delay values for the flow map and ladder, MSA assumes that the client is on the left, and the server is on the right. If you create MSA projects that include multiple flows, all of the flows in the project should be initiated from the same direction. For example, flows initiated by two nodes on the private side of a firewall would be suitable to include in a single

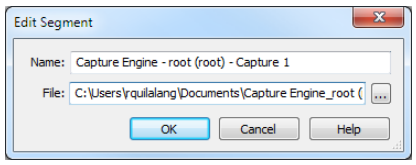
MSA project. Flows initiated by a node on the private side of a firewall, and flows initiated by a node on the public side of a firewall would not be suitable to include in a single MSA project.



- *Insert*: Click to insert a new segment. You will be prompted to name the segment and select a supported capture file.
- *Edit*: Click to edit a selected segment. You can choose to rename the segment or choose another supported file for the segment.
- *Delete*: Click to remove a selected segment.
- *Move Up*: Click to move a selected segment up in the ordered list of segments. You can also press (Shift or Ctrl)+Up Arrow to move the segment up in the list
- *Move Down*: Click to move a selected segment down in the ordered list of segments. You can also press (Shift or Ctrl)+Down Arrow to move the segment down in the list.
- *Column Header*: Displays the column headings currently selected. Right-click the column header to enable/disable columns. Here are the available columns:
  - *Segment Name*: The name of the segment.
  - *File*: The location and file name of the segment.

Edit segment

This dialog lets you edit a selected segment.

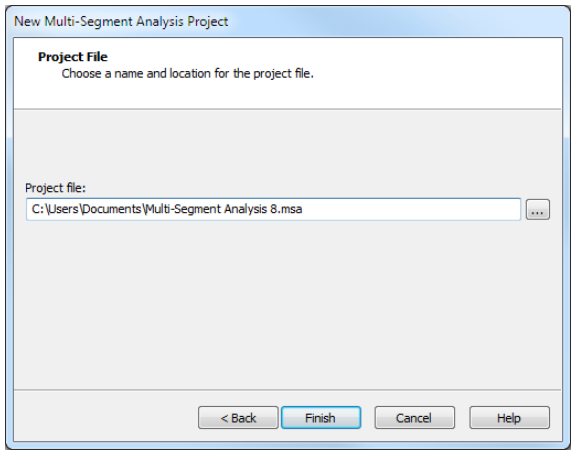


- *Name*: Displays the name of the segment. Type a different name to rename the segment.
- *File*: Displays the location and name of the segment file.

Project file

This **Project File** dialog lets you save the MSA project file (*.*msa*). Once saved, the MSA project window is displayed.

Note If your MSA project window is blank, more than likely you have either selected a flow that is not supported by MSA (for example, UDP or IPv6), or it is a flow with fragmented packets.



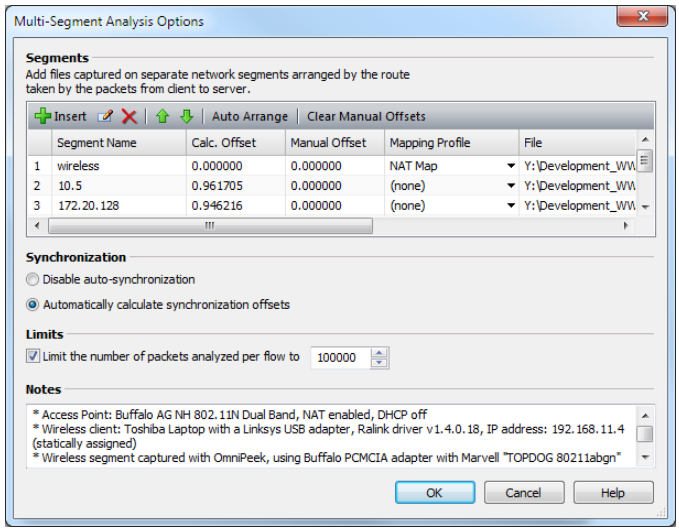
- *Project file*: Displays the location and MSA project file name (**.msa*).

MSA project analysis options

Once you have created or opened an existing MSA project window, you can access the **Multi-Segment Analysis Options** dialog to edit segment, synchronization, and limit options. Additionally, you can add notes for the project.

To edit MSA options:

1. Click **Analysis Options** in the MSA project window. The **Multi-Segment Analysis Options** dialog appears.



2. Complete the dialog:
   - *Insert*: Click to insert a new segment. You will be prompted to name the segment and select a supported capture file.
   - *Edit*: Click to edit a selected segment. You can choose to rename the segment or choose another supported capture file.
   - *Delete*: Click to remove a selected segment.
   - *Move Up*: Click to move a selected segment up in the ordered list of segments.
   - *Move Down*: Click to move a selected segment down in the ordered list of segments.
   - *Auto Arrange*: Click to arrange the segments in order from client to server based on the TTL values in the packets. If you create MSA projects that include multiple flows, all of the flows in the project

should be initiated from the same direction. If you create MSA projects that include NAT (Network Address Translation) segments, apply a Mapping Profile before selecting *Auto Arrange*.

- *Clear Manual Offsets*: Click to set the manual offsets to zero.
- *Column Header*: Displays the column headings currently selected. Right-click the column header to enable/disable columns. Here are the available columns:
  - *Segment Name*: The name of the segment.
  - *Calc. Offset*: The automatically calculated synchronization offset for the segment.
  - *Manual Offset*: The user-specified offset. A manual offset can be used instead of, or in addition to, the automatically calculated offset.
  - *Total Offset*: The calculated offset plus the manual offset.
  - *Mapping Profile*: The mapping profile associated with the segment. A mapping profile can be created to map private addresses/ports to public addresses/ports. See *Creating a mapping profile* on page 72.
  - *File*: The location and packet file on which the MSA segment information is based.
  - *Columns...*: Displays a dialog that lets you enable/disable and organize columns.
  - *Show All Columns*: Displays all available columns.
- *Disable auto synchronization*: Select this option to disable automatically calculating offset values.
- *Automatically calculate synchronization offsets*: Select this option to enable automatically calculating synchronization offset values. All Capture Engines should be set to the correct time, preferably through the use of an NTP server. But, even with the use of NTP servers, offsets may be needed to adjust for slight timing inaccuracies across Capture Engines. Automatic calculation of synchronization offsets is based on the TCP SYN and TCP SYN ACK packets. If a segment does not contain the SYN and SYN ACK packets, there will be a dash (–) in the Calc. Offset field. If the MSA project contains multiple flows, the automatic calculation of synchronization offsets is based on all flows.
- *Limits*: Select this check box to enable the limit on the number of packets analyzed per flow, and then enter or select the number of flows.
- *Notes*: Type any notes to append to the MSA project.

3. Click **OK**.

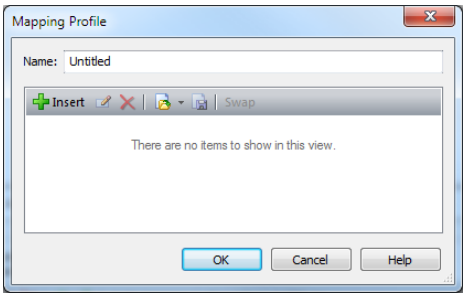
Creating a mapping profile

A mapping profile is used to map private addresses/ports to public addresses/ports.

Note If your project includes a Network Address Translation (NAT) segment, the auto-arrange feature should not be selected until you apply a mapping profile.

To create a mapping profile:

1. From the MSA project window, click *Analysis Options* to display the **Multi-Segment Analysis Options** dialog.
2. Click inside the box in the Mapping Profile column for the desired segment. A popup menu appears.
3. Select **New**. The **Mapping Profile** dialog appears.



4. Complete the Mapping Profile dialog:
   - *Name*: Type a name for the profile.
   - *Insert*: Click to display **Address/Port Mapping** dialog. Complete the dialog.
   - *Edit*: Click to edit a selected mapping. The **Address/Port Mapping** dialog appears. Complete the dialog.
   - *Delete*: Click to delete a selected mapping.
   - *Import*: Click to import an MSA mapping file (**.xml*).
   - *Export*: Click to export a mapping profile to an MSA mapping file (**.xml*).
   - *Swap*: Click to swap directions of a selected mapping.
5. Click **OK**.

Statistics Analysis

Omnipeek and the Capture Engines calculate a variety of key statistics in real time and present these statistics in intuitive graphical displays. You can save, copy, print, or automatically generate periodic reports on these statistics in a variety of formats. (Please refer to the *Omnipeek User Guide* or online help for information on generating statistics reports.)

Capture window statistics

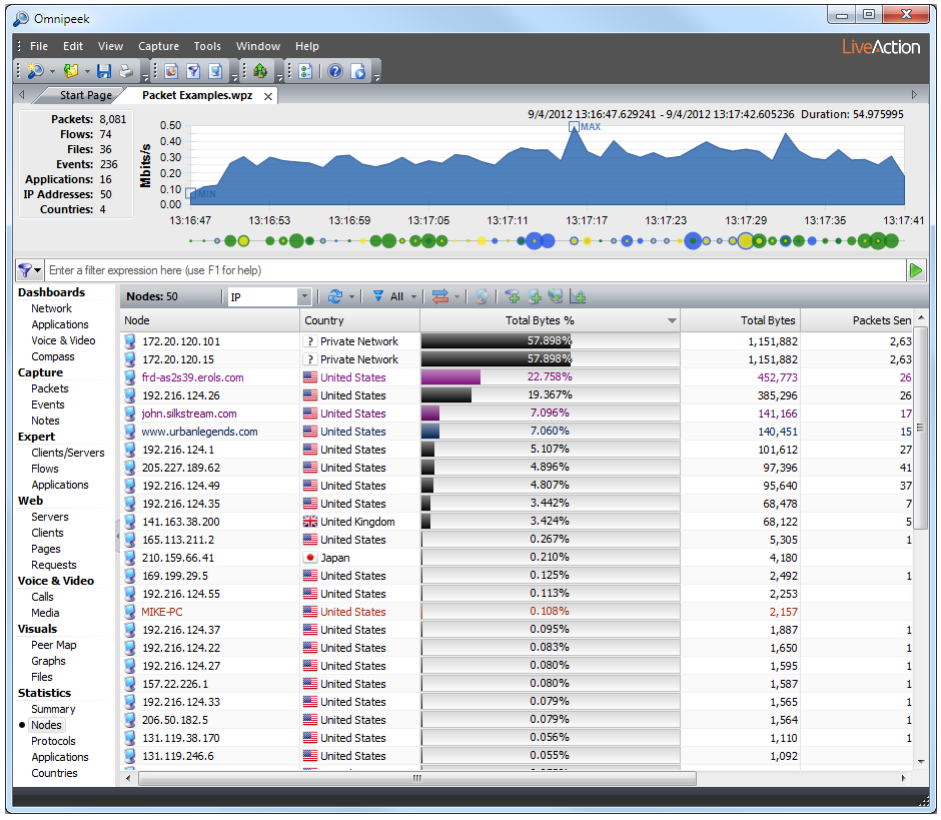
Omnipeek and Capture Engine capture windows provide the following statistics views: **Summary, Nodes**, **Protocols**, **Applications**, and **Countries** (and, when an 802.11 adapter is selected), **WLAN**, **Channels**, and **Signal**.

This section introduces the features in the **Nodes** and **WLAN** views of capture windows.

The Nodes view

Node statistics display real-time data organized by network node. You can view Node statistics in a hierarchical view or in a variety of flat views. Node statistics are available for the entire network and for a capture window.

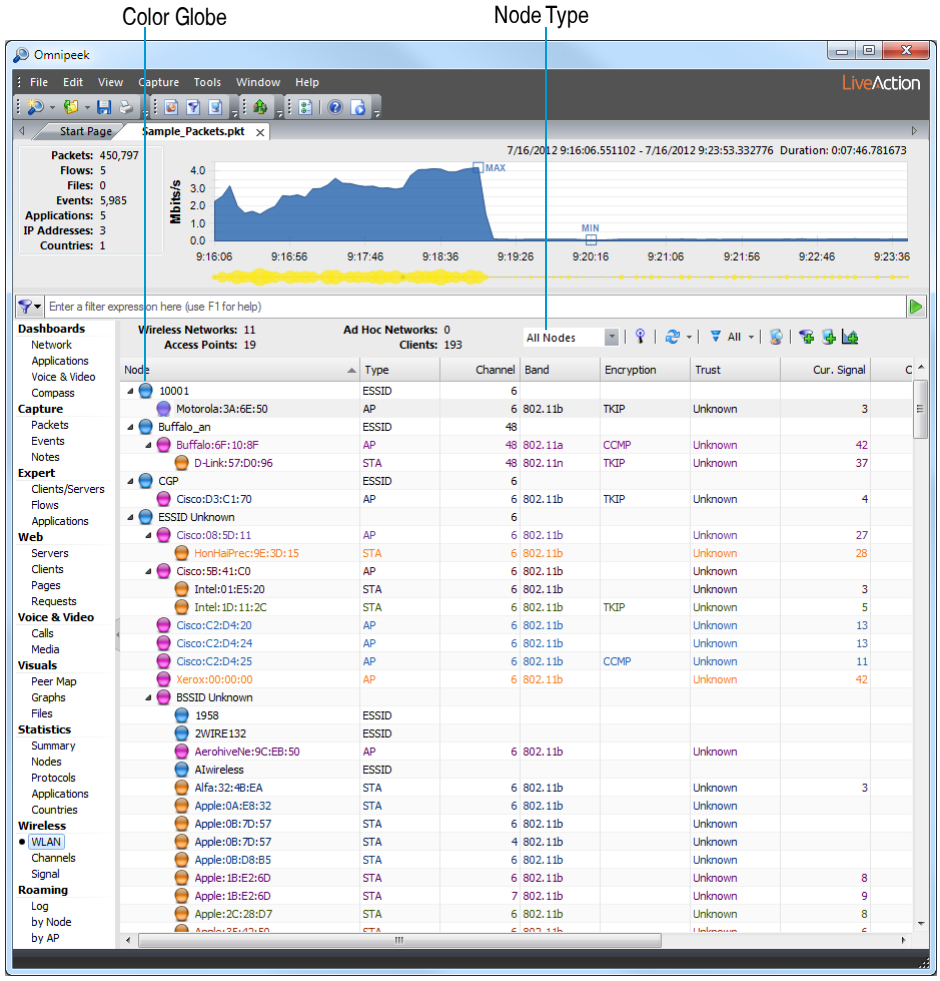
To view Node statistics for a capture window, select *Nodes* in the navigation pane of a capture window.



Tip Double-click a node to see more detail about the activity for the selected node and the protocols it is using (or right-click the node and choose **Node Details**).

The WLAN view

When a supported wireless adapter is selected as the capture adapter, WLAN statistics are available for a capture window. To view WLAN statistics for a capture window, select *WLAN* in the navigation pane of a capture window.



The *Node Type* drop-down list lets you limit the display to selected nodes (*All Nodes*, *Clients*, *Access Points*, *ESSID*, *Ad Hoc*, *Admin*, *Unknown*, and *Channels*). When the WLAN hierarchy view is broken out by channels, the root branches of the tree are channels numbers, with individual WLAN hierarchy views underneath it (ESSID, BSSID, nodes, etc).

The *Color globes* identify each node by color:

- Blue: ESSID
- Pink: AP (access point) or Ad Hoc equivalent
- Orange: STA or client
- Gray: Admin or otherwise unknown
- Gray with (?): Indications for a particular node are contradictory or unexpected.

Using the Peer Map

The **Peer Map** view in Omnipeek and the Capture Engines is a powerful tool for visualizing network traffic in a capture window. The Peer Map graphically displays all of the nodes, or a user-defined subset, detected in a particular capture window.

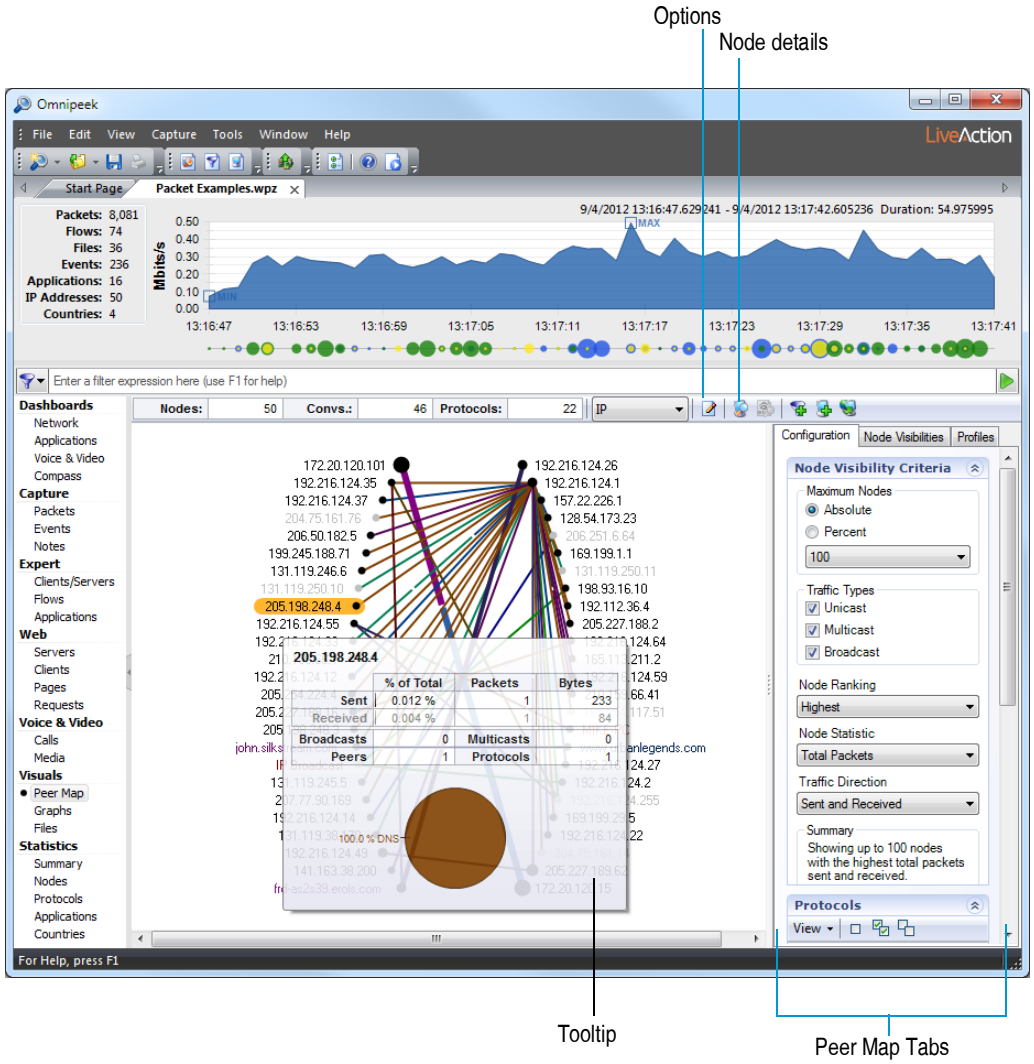
Communications between nodes is indicated with line segments. The line between nodes can be color-coded to show which protocol is used. The thickness of the line indicates the volume of traffic between nodes.

The Peer Map view

To display the Peer Map:

1. Open a capture window and begin capturing traffic.
2. From the capture window, click the **Peer Map** view. Node pairs begin to populate the **Peer Map** view, with conversations indicated by connecting lines.

> **Tip** Hold the cursor over a particular node in the Peer Map to see a tooltip with more information about this node. You can also hover over a conversation line to get a tooltip with information about that conversation.



3. Click **Options** to open the **Peer Map Options** dialog. This dialog lets you choose to show or hide displayable node type icons (server, workstations, etc.), node visibilities, and protocol line segment gaps.
4. Click **Node Details** to view statistics about this node.
5. Use the tabs in the right pane to configure Peer Map settings:
   - *Configuration:* This tab lets you set the basic parameters of the Peer Map, what part of the traffic in the capture window's buffer is displayed, and how the protocols (line segments) are displayed in the Peer Map.
   - *Node Visibilities:* This tab displays node counts and nodes that are both shown and hidden in the Peer Map.
   - *Profiles:* This tab lets you configure settings into a profile that controls the appearance and layout of the Peer Map.
6. Right-click on a node for other options, including:
   - *Arrange:* If you have changed the appearance of the Peer Map by dragging nodes to new positions, this option arranges the node back to the ellipse of the Peer Map.
   - *Node Details:* This option opens the **Detail Statistics** window and shows details of the selected node.

Keyboard Shortcuts

Shortcut	Description
Ctrl + N	Creates a new capture window.
Ctrl + O	Opens an Omnipeek capture file or other supported file type in a new capture file window.
Ctrl + S	Opens the **Save** dialog to save all packets in the active window.
Ctrl + P	Prints the active window in a format appropriate to its type.
Alt + F4	Quits Omnipeek.
Ctrl + Z	Undoes the last edit.
Ctrl + X	Cuts the highlighted item(s) and copies to the clipboard.
Ctrl + C	Copies highlighted item(s) to the clipboard.
Ctrl + V	Pastes the current contents of the clipboard.
Ctrl + B	Deletes all packets from the active capture window.
Ctrl + A	Selects all packets, text, or items in a window.
Ctrl + D	Removes all highlighting and selection.
Ctrl + E	Opens the **Select** dialog, where you can use filters, ASCII or hex strings, packet length, and Analysis Modules to select captured packets.
Ctrl + H	Removes selected packets from the display without deleting them. Hidden packets are not processed further.
Ctrl + Alt + Y	Starts all local captures.
Ctrl + Shift + H	Removes unselected packets from the display without deleting them. Hidden packets are not processed further.
Ctrl + U	Restores all previously hidden packets to normal status.
Ctrl + G	Opens the **Go To** dialog where you can choose a packet number to jump to. If packets are selected, the number of the first selected packet is shown.
Ctrl + F	Finds patterns.
Ctrl + J	Jumps to the next selected packet.
Ctrl + M	Opens the **Filters** window.
Ctrl + L	Opens the **Log** window.
Ctrl + Y	Toggles the packet capture function.
Ctrl + Tab	Makes the next window in sequence the active window.
Ctrl + Shift + Tab	Makes the previous window in sequence the active window.

Shortcut	Description
F1	Launches the Online Help.
F11	Displays Omnipeek in a full screen window.

Index