

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

Copyright © 2022 LiveAction, Inc. All rights reserved

20220819-GSG-OP222a

Contents

Chapter 1	Introduction	
•	Omnipeek as a portable analyzer	I
	Omnipeek with distributed Capture Engines	I
	Network forensics)
	Voice and video over IP analysis 2)
	Compass dashboard 2)
	Multi segment analysis 2)
	System requirements	3
	Supported adapters and drivers	3
	Installing Omnipeek	3
	Renewing or upgrading subscription versions of Omnipeek	ŀ
	Installing a Capture Engine 4	ł
	Main program window and Start Page 4	ŀ
Chanter 2	Using Omnineek with Canture Engines	Ś
	Displaying the Capture Engines window	
	Connecting to a Canture Engine 6	
		,
Chapter 3	The Capture Window)
	Creating an Omnipeek capture)
	Creating a Capture Engine capture)
	Opening saved capture files	3
	Working in the Files view)
Chanter /	Forensis Search	•
Chapter 4		
	Forensic search from the Files lab	ز ۱
	Forensic search from the Forensics Lab	7
	Totensic search norm the Totensics Capture window	
Chapter 5	Dashboards)
•	Timeline dashboard)
	Network dashboard	ŀ
	Applications dashboard	5
	Voice & Video dashboard	7
	Compass dashboard)
Chapter 6	Viewing and Deceding Projects	•
Chaptero		
	The packets view))
	The packet decode window	'
Chapter 7	Creating Filters)
-	Enabling a filter)
	Creating filters with the make filter command	3
	Creating a simple filter	ŀ
Chanter 8	Expert Troubleshooting 54	Ś
	The Expert view window 54	Ś
	Lising the EventFinder 57	,
	Applications view 59	2
		1

Chapter 9	Multi-Segment Analysis	60
•	About Multi-Segment Analysis	
	MSA project window	61
	Creating an MSA project	65
	Using the MSA wizard	
	MSA project analysis options	
Chapter 10	Statistics Analysis	74
•	Capture window statistics	
Chapter 11	Using the Peer Map	76
•	The Peer Map view	
Appendix 12	Keyboard Shortcuts	
	Index	90

CHAPTER 1

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.

	Dennipeek - [Start Page]								
Toolbar -	: File Edit View Capture Tools Window Help		LiveAction						
TUUIDai	4 Start Page ×		⊳						
			A						
	×@	2							
	New Capture Open	Sapture File View Capture Engines							
	Welcome to Omnipeek! For local wireless packet capture, Omnipeek requires the installation of If this is your first time using Omnipeek, you may want to view the <u>Cet</u>	special drivers. ing Started Guide.							
	What's new in Omni 12								
	Expert enhancements VoIP enhancements								
	Hi-DPI Support								
	Enhanced support for SCTP Added support for ACL with 3rd party authentication								
	 Support for Financial Transaction Card message Interchange protocol 	(ISO8583)							
Start	Improved Network and Application Latency Values for Expert								
Page	Support for new LiveAction hardware appliances								
. «ge	▶ New Decoders								
	For the complete list, refer to the <u>read me</u>								
	Recent Files Location	Summary							
	No recent files								
	Recent Capture Templates Location	Summary							
	No recent templates								
	Documentation	Resources							
	▹ View the Readme	List installed plug-ins							
	View the Getting Started Guide	View sample files							
	View Driver Installation Instructions Pead the User Guide	► MyPeek 🗠							
	Read the Capture Engine for Omnipeek Getting Started Guide								
	Technical Support								
	View technical support resources for LiveAction products								
	Contact LiveAction technical support ☑ [*]								
	▷ Omnipeek Supported Hardware C*								
	Show Start Page at startup	l	_iveAction"						

- *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.**

CHAPTER 2

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.

Insert Engine Discover Engine										
Insert Group Delete Connect Disconnect										
Domnipeek Device										
3 File Edit View Capture Tools Window Help	LiveAction									
4 Start Page Capture Engines ×										
Engines (4) (3) C X I S X										
There are no items to show in this view.										

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.

Insert Engine	
Engine	
F Kong	Host: 🗸
-	Port: 6367
Credentials	
Dor	nain:
Userna	ame:
Passw	vord:
	Save my password
	Connect Cancel Help

- 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.

🔊 Omnipeek								
file Edit View Capture Send Tools Window Help								
i 🔊 - 🜍 - 📙 😂 📑 🗟 🗑 😟 .								
Start Page Capture Engines	×							
Engines (1) 🛛 🙀 🚱 💽 🛛 🗶 📝 🚿	Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin							
Capture Engine	Capture Engine							
	Name: Capture Engine							
	Host Name: omnipliance							
	Address: 10.4.2.137:6367							
	User: root							
	Engine Type: Omnipliance							
	Version: 10.0 (build 10.0.0.20)							
	Time Zone: GMT-07:00							
	Uptime: 3:47:52							
	Operating System: Ubuntu 14.04 LTS							
	IPMI Address: 10.4.100.36							
	Memory: 128,909 MB Total Phys; 125,742 MB Avail Phys							
	CPU Count: 24							
	Capture Storage: 58,328 GB Total; 58,328 GB Avail							
	Captures (1)							
	Forensics (1 capture sessions)							
	Files (1 files)							
	Forensic Searches (0)							
	A Events (104,531)							
	Adapters (4)							
	Settings Filters (109) Graphs (28) Alarms (60) Notifications (1) Analysis Modules							
For Help, press F1								

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.

Insert Group	
D Omnipeek	
: File Edit View Capture Tools Window Help : ② • 🚱 • 🛃 • 🙀 😨 👔 😰 😨 😨 💭	LiveAction
4 Start Page Capture Engines ×	4
Engines (1) 🙀 🔬 🔾 🗙 📝 🕺 🖣 Home Captures Fore	nsics Files Forensic Searches Events Adapters Settings Admin 🕨
Capture Engine Capture Engine	
Name: Capture En	gine
Host Name: omnipliance	
Address: 10.4.2.53:	367
User: root	
Version: 10.0 (build	- 10.0.0.16)
Engine Local Time: 10/3/2016	12:40:58
Time Zone: GMT-07:00	
Uptime: 3:36:19	
Operating System: Ubuntu 14.	04 LTS
Memory: 3,953 MB T	otal Phys; 3,260 MB Avail Phys
CPU Type: Intel(R) Xe	on(R) CPU E5-2630 V2 @ 2.60GHZ
Capture Storage:	168 GB Total; 167 GB Avail
-	
👰 Captures (1)	
🖉 🛛 New Capture View Capt	ures
Eorensics (1 captur	e sessions)
Files (3 files)	
Forensic Searches	0)
Levents (43)	
Adapters (4)	
Settings Filters (109) Graphs (28)	Alarms (60) Notifications (1) Analysis Modules

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

CHAPTER 3

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.

	Capture Options	X
Omnipeek capture options	General Adapter 802.11 Triggers Filters Statistics Output Analysis Options	General Capture tile: Capture 1 Capture to disk Fle path: Citysers/Capture 1- Fle size: 1024 @ megabytes Stop saving after 1000 @ megabytes Stop saving after 1000 @ megabytes New fle every 1 @ @ @ gives Discard duplicate packets Buffer size: 256 @ megabytes V Show this dialog when creating a new capture OK Cancel Helo

- 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.

	🔊 Omnipeek										
	🗄 File Edit View	Capture Tools Window Help	0 <u>6</u> ,				LiveAction				
	Start Page Packets received: 0 Packets filtered: 0 Packets filtered: 0 Packets filtered: 0	Start Page Capture 1 x Packets received: 0 Buffer usage: 0% Fackets filtered: 0 Filter state: Accept all packets Start Capture Start Capture									
	Dashboards Network Applications Voice & Video Compass Capture Packets Events Notes Filters Excert	Network Utilization - 2 Minute Window (1 Second Average) No Data									
Capture window views	Expert Clients/Servers Flows Applications Web Servers Clients Pages Requests Voice & Video	Current Activity NETWORK UTILIZATION O.000 Mbits/s packe	TS ERRORS 0 tt/s errors/s	• Events	0	<u> </u>	80				
	Calls Media Visuals Peer Map Graphs Statistics Summary Nodes Protocols Applications Countries	• Top Talkers by IP Address	ata	▼ Top Protoc	cols by Bytes No	Data					
L	Idle			🕎 Local Area C	Connection Packets	: 0	Duration: 0:00:00				

- 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

Capture Options - eth0						
General Adapter	General					
Triggers Filters	Capture title: root (root) - Capture 1					
Alarms	Comment:					
Statistics Output	Capture to disk					
Analysis Options Packet File Indexing	File name: root (root) - Capture 1-					
Timestamps	File size: 1024 v megabytes Priority to CTD					
	GB GB					
	1 128 Timeline Stats Top Stats VoIP Stats App Stats					
	Limit each packet to 128 🚔 bytes					
	Discard duplicate packets					
	Buffer size: 256 🚔 megabytes					
	Start capture immediately					
	Save as template					
	OK Cancel Help					

- 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.



- 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**).

Omnipeek							- • · ×			
File Edit View	Capture	Tools Window Help					LiveActio			
🦥 - 🛃 - 💷 🗴										
Start Page	Packet Exa	amples.wpz ×								
Packets: 8,081 0.50 9/4/2012 13:16:47.629241 - 9/4/2012 13:17:42.605236 Duration: 54.975995										
Flows: 74										
Files: 36	2 0.30									
Applications: 16	0.20									
IP Addresses: 50	0.10	MIN								
Countries: 4	0.00									
	13:16	5:47 13:16:53 13:	16:59 13:17:05 13:17	:11 13:17	:17 13:17:23	13:17:29 13:17	:35 13:17			
	•	· • • • • • • • • • • • • • • • • • • •	••••••••••	••••	••••••	0 • • 0 0 0 0 • • •	••000			
- Entor a filter over	manian hara (u	an El fachola)								
	ression here (u									
Network	⇐ ➡ 🗄	🖹 🛛 🔚 🔍 🎭 📔	Y + 🗄 🕸 🔗 1	2 🔊						
Applications	Packet S	ource	Destination	Flow ID F	lags Size	Relative Time	Protocol			
Voice & Video	1	frd-as2s39.erols	192.216.124.26	1	64	0.00000	TCP			
Compass	2	192.216.124.26	💡 frd-as2s39.erols	1	1518	0.00000	TCP			
apture	3	3 172.20.120.101	3 172.20.120.15	2	1032	0.000001	SIP			
Packets	4	172.20.120.15	3 172.20.120.101	3	586	0.001000	SIP			
Events	5	3 172.20.120.101	3 172.20.120.15	4	396	0.009248	SIP			
Notes	6 (3 172.20.120.101	3 172.20.120.15	2	1196	0.013876	SIP			
opert	7	3 172.20.120.15	3 172.20.120.101	3	504	0.015125	SIP			
Clients/Servers	8	1420.112	3 1052.208		64	0.040058	ASP Cmd			
Flows	9	1052.208	3 1420.112	*	64	0.050072	AT ASP			
Applications	10	1420.112	2 1052.208	*	64	0.050072	ATP TRel			
leb	11	141.163.38.200	3 192.216.124.1	5	64	0.210302	SMTP			
Servers	12	frd-as2s39.erols	3 192.216.124.35	6	64	0.220317	TCP			
Clients	13	192.216.124.35	🛃 frd-as2s39.erols	6	1518	0.220317	TCP			
Pages	14	192.216.124.35	🛃 frd-as2s39.erols	6	1518	0.220317	TCP			
Requests	15	1224.192	1629.100	*	64	0.240346	ASP Tickle			
pice & Video	16	205.227.189.62	3 192.216.124.49	7	78	0.300432	X-Windows			
Calls	17	1887.1	1071.204		64	0.320461	ASP Cmd			
Media	18	1071.204	1887.1	*	64	0.320461	AT ASP			
suals	19	1887.1	3 1071.204		64	0.320461	ATP TRe1			
Peer Map	20	192.216.124.49	205.227.189.62	/	64	0.340490	A-WINDOWS			
Graphs	21	192.210.124.1	102 216 124 25	8	11	0.420605	TCD			
riles	22	102 216 124 2F	192.210.124.55	6	04	0.450619	TCP			
Summary	23	102 216 124.35		6	1519	0.450619	TCP			
Nodes	24	102 216 124 35	fpd-as2s39.ero1s	6	1016	0.450619	TCP			
NUCS	20	157 22 226 1	102 216 124 1	0	74	0.440034	TCMP Dect 1			
Protocole	20	137.22.220.1	172 20 120 101	2	520	0.520749	STD			
Protocols	27	172 20 120 15								
Protocols Applications	27	172.20.120.15	1/2.20.120.101	5	570	0.525052	SMTP			

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.

Lis	Flov t View File	v Visualize s	Make er	e Filte Inse R	er rt Int esolv Tc	o Name ve Nam ggle Li Toggle	e Table es st View Details	Search	ł	Filter	De Files	etails Hea	aders Content
🔊 Omr	ipeek												
File	Edit View Control Control Con	Capture Sen	d Too J	ls Wii A , i ×	vob n	Help 2 👌 🚽		9/4/2	2012 13:16:47.62924	1 - 9/4/2	2012 13:17:42	.605236 Du	LiveAction
Applic IP Add Cou	Flows: 74 Files: 36 Events: 236 ations: 16 resses: 50 intries: 4	0.40 0.30 0.20 0.10 0.00 13:16:47	-	3:16:53		13:16:59	13:17:05	15:17:11	13:17:17 13	:17:23	13:17:2	9 13:	17:35 13:17:41
		• •	• •••	• •	••		•••••••	••••	••••••	•••	0		•••00
¶ ≁ Er	iter a filter expre	sion here (use f	1 for help	o)									
Dashbo	ards Fi	les: 36	= 😵	🛃 😸	🗉	File	Names + Search		× ۹			*	
Applic	ations		1		1				ARI FAA	-	· 4 / C	Details H	eaders Con 🕨
Voice	& Video ass		1 m			DIV		afu	neine			Name: File ID:	BIG.gif 32
Captur	-	(default)	afu_titl	e_3d.gif		BIG.gif	HitMe.class	m_AFU.gif	m_AFU_FAQ.gif		Re	equest ID:	30
Packe Event Notes Expert Client	ts s s/Servers		Bo m_Bo	oks.gif	m_C			Collegiate.gif	Death m_Death.gif		Cl C Clien Client	Flow ID: ient Addr: lient Port: t Country: t Latitude:	56 192.216.124.44 jo hn.silkstream.com 1719 h323gatestat United States 37.7510
Flows Applic Web Serve Client Pages	ations rs s	Disney m_Disney.gif	D m_Dr	ugs.gif	m	Food.gif		m_Language.gif	Legal.gif		Client L Ser Serve	ongitude: rver Addr: rver Port: r Country:	-97.8220 206.221.233.102 w ww.urbanlegends.c om 80 http United States Indianapolis IN
Voice & Calls Media Visuals Peer I Graph	Map r	n_Medical.gif	M m_M	isc.gif	m_	Avies.gif	m_Other_Sites.gif	Politics.gif	Padualy m_Products.gif	E	Server Server L Cont	r Latitude: ongitude: URI: tent-Type: Referer:	-86.2341 /honkin/BIG.gif image/gif http://www.urbanl egends.com/
Files Statisti Summ Nodes Proto Applic	ics ary s cols r rations	Religion.gif	M_ m_Scie	nce.gif	m	Sex.gif	Songs m_Songs.gif	TV m_TV.gif	on.gif		Fir La	Size: st Packet: st Packet: Start:	s.com 3 KB (3,895 bytes) 6353 6397 9/4/2012 13:17:3 0.761262
Count	tries	tafkac.gif	tafkac_	glow.gif	ta	Rac 1b.gif	the_jason_aw	ToBackground	url.gif	-		Finish: Duration:	9/4/2012 13:17:3 0.961550 0.200288
For Help	, press F1												

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 lcons*: 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 lcons: 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.

CHAPTER 4

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.

					D	ownload P	ackets	Refre
	Capt	ure Files			Forensi	s Search	Opioad	
Ø Omnipeek								
File Edit View Capture Tools	Vindov	v Help					l iv	e∆ tion
😥 - 👹 - 📙 🏊 🕴 🖬 🗑 🖢	E 🍙							
Start Page Capture Engines	v C	anture Engine: Forensics Canture	_		_			Þ
Engines (1) Clarke Cupture Engines		Home Cantures Forensic	Files	Forensic Searches	Events	Adapters	Settings	Admin D
	Filer		i ilici	rorensie seurene.	- Cremo	B Enrenzic Se		
	Tiles	(10)				in orensic se		
	Name	^	Capture	Medi	a	Packets	Star	't Time
	⊿ Fo	rensics Capture (1)						
	200	Forensics Capture-2016-10-05T09	Forensics Cap	oture Ethe	rnet		10/5/2016 9	:47:19
	⊿ ro	ot (root) - Capture 1 (9)	and (mail)	Contract Diffe		074 525	10/5/2016 0	.04.00
		root (root) - Capture 1-2016-10-05	root (root) - C	Lapture 1 Ethe	rnet	974,526	10/5/2016 9	:34:28
	6	root (root) - Capture 1-2016-10-05	root (root) - (Capture 1 Ethe	met	959,005	10/5/2016 9	-38-31
	6	root (root) - Capture 1-2016-10-05	root (root) - (Capture 1 Ethe	met	897 680	10/5/2016 9	.42.10
	6	root (root) - Capture 1-2016-10-05	root (root) - (Capture 1 Ethe	met	854 608	10/5/2016 9	-45-54
	6	root (root) - Capture 1-2016-10-05	root (root) - (Capture 1 Ethe	met	855.644	10/5/2016 9	:45:58
		root (root) - Capture 1-2016-10-05	root (root) - 0	Capture 1 Ethe	rnet		10/5/2016 9	:49:25
	6	root (root) - Capture 1-2016-10-05	root (root) - C	Capture 1 Ethe	rnet		10/5/2016 9	:52:14
	3	root (root) - Capture 1-2016-10-05	root (root) - 0	Capture 1 Ethe	rnet		10/5/2016 9	:52:19
	•							

- 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**.

Name				💣 Analysis & Output —		
Forensic Search	1			Packets	Vode Statistics	
•				Expert	Protocol Statistics	
Files				📃 Voice & Video 🛛 🖉	Node Detail Statistics 💈	
 Search all files Search colorth 	s ad filos (7)			🕅 Graphs 📓	Application Statistics	
 Search selection 	eu mes (2)			🔽 Analysis Modules [🗕	Country Statistics	
Captures				V Events	Summary Statistics	
Capture:	root (root) - Captu	re 1	-	Vetwork Statistics	Traffic History Statistics	
Network Media				Error Statistics	Wireless Channel Statistics	
Media type:	Ethernet		•	Size Statistics	Wireless Node Statistics	
O Adapter:	eth1		-	Compass	Enable all Disable all	
) Time Range —						
Start time:	10/ 5/2016	09:34:28	*			
End time:	10/ 5/2016 🔍 🔻	09:45:54	*			
Duration:	0:11:25					
Filters						
S- Entroy Alt		F1 (b-b)				

- 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.

Ø Omnipeek								- • ×
File Edit Viev	w Capture	Tools Window Help						liveAction
:								LIVEACCION
: 🎾 - 🙆 - 💾	🧼 - i 📓 🛛	1 <u>3 ,</u> : » <u>,</u> : E Ø						
Start Page	Capture En	igines Capture Engine: F	orensic Search 1 ×					⊳
Sector a filter ex	pression here (u	se F1 for help)						
Dashboards								
Network		💻 🌇 I 📖 I 🔨 🖄 I 🕅	() P P P P P					
Capture	Packet S	ource	Destination	Flow ID	Flags	Size	Relative Time	Protocol
 Packets 	1	10.4.2.53	10.4.2.83			186	0.000000	Omnipeek 🚽
Events	2	10.4.2.83	3 10.4.2.53			253	0.004348	Omnipeek
Statistics	3 💈	10.4.2.53	3 10.4.2.83			64	0.004383	Omnipeek
Summary	4 🧕	10.4.2.83	3 10.4.2.53			179	0.004719	Omnipeek
Nodes	5	10.4.2.53	3 10.4.2.83			64	0.004735	Omnipeek
Protocols	6 🧕	10.4.2.53	3 10.4.2.83			981	0.005376	Omnipeek
	7	10.4.2.53	3 10.4.2.83			1318	0.007846	Omnipeek
	8 🧕	10.4.2.83	3 10.4.2.53			64	0.008454	Omnipeek
	9 🧕	10.4.2.53	3 10.4.2.83			777	0.008470	Omnipeek
	10 🔳	VMware:D1:D5:DE	Ethernet Broadcast			64	0.055404	ARP Request
	. 11 💈	<pre>fe80::14d8:5d22:</pre>	🛃 All DHCP Agents			171	0.098884	DHCPv6
	. 12 💈	10.4.2.83	2 10.4.2.53			179	0.118307	Omnipeek
	13 💈	10.4.2.53	3 10.4.2.83			936	0.120390	Omnipeek
	14 💈	10.4.2.83	2 10.4.2.53			143	0.164077	Omnipeek
	15 💈	10.4.2.53	2 10.4.2.83			377	0.164328	Omnipeek
	16	<pre>fe80::e5fc:72c4:</pre>	🗟 All DHCP Agents			168	0.170797	DHCPv6
	17 📕	Dell:DE:B4:96	Ethernet Broadcast			64	0.194931	ARP Request
	18 📕	SuperMicro:CE:30:50	LLDP_Multicast			122	0.227232	LLDP
	19 💈	10.4.100.126	SSDP			179	0.232747	SSDP
	20 📕	VMware:FE:FA:40	Ethernet Broadcast			64	0.238174	ARP Request
	21 📕	Cisco:53:18:28	Mcast 802.1d Bri		*	68	0.249005	802.1
	22 🧏	10.4.2.60	3 10.4.255.255			64	0.286036	UDP
	23	10.4.2.60	😼 All Hosts			64	0.286190	UDP
	24 📕	VMware:AD:C4:4F	Ethernet Broadcast			64	0.353412	ARP Request
	25 💈	10.4.2.83	3 10.4.2.53			64	0.369910	Omnipeek 🖕
						Packets: 10.083	Dura	tion: 0:10:00
						1 UCKELS. 10,005	Dula	

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**.

Forensic Search - root (root) - Capture 1		×
Name Forensic Search 2 Time Range Start time: 10/ 5/2015	Analysis & Output Packets Expert Voice & Video	V Node Statistics V Protocol Statistics Node Detail Statistics
End time: 10/ 5/2016 V 10:05:09	Graphs Analysis Modules Contents Revents Revents Revents Contents Revents Revents Statistics	Application Statistics Country Statistics Summary Statistics Fraffic History Statistics
√ Filters	Frror Statistics Size Statistics Compass Start	Wireless Channel Statistics Wireless Node Statistics Enable all Disable all Cancel Help

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.



Timeline Nested Tab

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.

Selected Capture Session (in Oran	ge) Active Capture Session (in Greer
6/24/2010 9:52:48	
Active Graph	
	Active Graph

Storage Nested Tab

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.

Main Parent Capt	ures Capture Sessions	i				
Capture	Data Start Time 🛛 🔻	Duration	Size	Packets	Packets Dropped	Ada
Forensics Capture						
manun	12/11/2015 12:20:18	1:07:20	9.45 GB	14,471,745	0	eth1
🖃 root (root) - Capture	2					
	/ 12/11/2015 12:00:33	0:22:47	0.959 GB	1,276,179	112,034,475	eth2
🖃 root (root) - Capture	21					
•1	12/11/2015 11:48:10	1:39:27	0.028 GB	108,660	0	eth0
•						Þ
d Timeline St	orage Details					⊳
Sparklines	Details Nested Tab)				

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.

	700 T				Selection:	¥/27/2011 7	':08:07 - 4/2	7/2011 9:38	07 Duratic	n: 2:30:00	Packets: ~5	.54 M
	600 ·	Ŵ	when	Jun	M	Mm	handha	mm		July	www	m.
s	500 ·											
cets/	400 ·								L			
Pac	300 ·				1				ſ			
-	200 ·											
	100 -											
	0 - 5:26:	:07	6:04:07	6:42:07	7:20:07	7:58:07	8:36:07	9:14:07	9:52:07	10:30:07	11:08:07	11:44:07
			Total		Dropped		CRC		l Runt		Jumbo	

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**.

Name				3	Analysis & Output	
Forensic Search 4					Packets	Vode Statistics
					Expert	📝 Protocol Statistics 🛛 📓
💋 Time Range —					🔲 Voice & Video 🛛 🕅	Node Detail Statistics
Start time:	10/ 5/2016 🔍 🔻	10:29:10	×		🕅 Graphs 🛛 🖉	Application Statistics
End time:	10/ 5/2016 🔲 🗸	10:29:34	*		🔽 Analysis Modules 🛛 📓	Country Statistics
Duration:	0:00:24				V Events	Summary Statistics
D					Network Statistics	Traffic History Statistics
Filters					Error Statistics	Wireless Channel Statistics
♀▼ Enter a filter expression here (use F1 for help)					Size Statistics	Wireless Node Statistics
					Compass	Enable all Disable all

- 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 Search* tab.

File Edit View	Capture Tools Windo	w Help					LiveAction	
1 Start Page	Capture Engines Cap	ture Engine: Forensics	Capture Capture Er	gine: Forensic Se	arch 4 \times		1	
♀▼ Enter a filter exp Dashboards Network Capture Packets Events Statistics Summary Nodes	vression here (use F1 for help) • Network Utilization 0.12 0.10 0.10 0.00 11 0.00 12 0.00 14 0.00 0.02 0.00	ı - 2 Minute Windo	w (1 Second Avera	je)				
Protocols	 Current Activity 			▼ Events	10:29:30			
	NETWORK UTILIZATION	PACKETS 13 packet/s	errors/s	() 0	0	<u> </u>	0	
	▼ Top Talkers by IP	Address		▼ Top Protocols by Bytes				
	10.4.2.53 10.4.100.217 10.4.100.33 10.4.2.107 10.4.2.107 10.4.102.130 10.8 10.8 10.8 10.8 10.8 10.8 10.8 10.	6	1.9%	Omnipee SSDI DHCPv 802. DHCI	k 15.9% 6.5% 6.5% 1.133% 6.5% 1.15% 1.117% 1.117% 1.117% 1.13% 1.13% 1.13% 1.13% 1.13% 1.15,9% 1	54.2%		
	0 10 20	30 40 50 60	70 80 90 100		0 10 20 30	40 50 60	70 80 90 100	

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*.

CHAPTER 5

Dashboards

The Omnipeek dashboards display graphical data about your network summarized into several easy-toread 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 Ad*
 - **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.

Ø Omnipeek											x
File Edit View	v Capture Tools	Window Hel	p							LiveAc	tion
Start Page Packets received: 8, Packets filtered: 8, S Enter a filter exc	Capture Engine ,410 ,410 pression here (use E1	s Capture En Buffer usage: 2% Filter state: 4	gine: root (root) - Accept all pack	Capture 1 ×						Stop Captu	re e
Dashboards Network Applications Voice & Video Compass Capture Packets Events	Top Applic: BJNP DHCPv6 DHCP SSDP Bonjour	ations by Flow	5 70 90	Top Applic TCP Dropbox CIFS SSDP BJNP 0	ations by B	ytes 78.7%	N	Top Applicat Networkin File Transf etwork Monitorin	tion Categor g er 7.1% g 0.1% 0 20 40	Fries by Bytes 92.7% 60 80 100	
Alarms Expert Clients/Servers Flows Applications	 ✓ Application ✓ 0.06 ✓ 0.04 ✓ 0.02 Ø 0.02 Ø 0.00 	1 Utilization - 1	10 Minute Wind	low (5 Second)	Average)						11
Calls Media	TCP	DHCPv6	12:38:33 Dropbox	12:4 NetBIOS NS	0:13 CIFS	12:41:53 DHCP	SSDP	12:43:33 UDP	12 BJNP	::45:13 ■ Others	
Visuals Peer Map Statistics Summary Nodes Protocols Applications Countries	✓ Application ♥ 0.06 0.04 0.02 0.00	ı Response Tin	ne - 10 Minute 12:38:33	Window (5 Sec	0:13	12:41:53	1	12:43:33	12	45:13	-
Capturing For Help, press F1							P (th0 Packets: 8	,410 D	ouration: 0:07:31	1.4

- 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.

Ø Omnipeek				
File Edit View	Capture Tools Window	Help		LiveAction
🗄 🔊 + 🖏 - 📙 🗧	> , i 💽 🝸 💽 , i 🏤 , i	🗈 I 🛛 🔂 📮		
	Capture Engines Pack	ket Examples.wpz ×		
Packets: 8,081 Flows: 74	0.50	9/4/2	J12 13:16:47.629241 - 9/4/2012 13:17:	42.605236 Duration: 54.975995
Files: 9	0.40 0.30			
Applications: 16	0.20			
IP Addresses: 50 Countries: 4	0.00			
	13:16:47 13:16:53	13:16:59 13:17:05 13:17:1	1 13:17:17 13:17:23 1	3:17:29 13:17:35 13:17:41
	····•	•••••••••••••••••••••••••••••••••••••••		••••••••••
Sector a filter exp	ression here (use F1 for help)			
Dashboards Network	▼ Call Summary		▼ Call Quality Distribution	
Applications	Call Counters	Closed Call Statistics	All Calls	
Voice & video Compass	Total calls: 1 Current calls: 1	Total media packet loss: 0.000% Voice packet loss: 0.000%	100.0%	
Capture	Open calls: 0	Video packet loss: 0.000%	80	No Open Calls
Events	Avg. call duration: 0:00:54	MOS-CQ: 4.17	40	
Notes		MOS-A: 0.00 MOS-V: 0.00	0.0% 0.0% 0.0%	
Clients/Servers			Good Fair Poor Bad	
Flows	 Call Quality - 1 Second 	d Average		
Web	<u>ø</u> 0.8			
Servers Clients	ප් ^{0.4}			
Pages	13:16:47	13:17:07	13:17:27	
Voice & Video	Good	Fair Po	or Bad	Unknown
Calls	▼ Call Quality by Codec			
Visuals	0 4.0 MIN			
Peer Map Graphs	≥ 2.5 1.0			
Files	13:16:47	13:17:07	13:17:27	
Statistics Summary		■ G.71	1 µ-law	
Nodes	▼ Call Volume by Codec	- 1 Second Interval		
Protocols Applications	<u>o</u> 0.8			
Countries	0.4 0.0			
	13:16:47	13:17:07	13:17:27	
		■ G.71	1 µ-law	
	Call Utilization - 1 Sec	ond Average	-	
	0.45 92 0.30		MAX	
	0.15 MIN			
	13:16:47	13:17:07	13:17:27	
		Network Utilization	Call Utilization	
	•	П		۱.
For Help, press F1				

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.



Data Source Widgets

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, Chits, 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.

13	Statistics	3ar Chart		Close
ор		=		~
	Protocol *	Description 🗢	Expert Events 🔺	
~	HTTP	World Wide Web HTTP	3	
~	TCP	Internet Transmission	3	
~	SIP	Session Initiation Prot	2	
~	SMTP	Simple Mail Transfer P	2	
	DNS	Domain Name System	1	
	FTP Ctl	File Transfer Protocol	1	
	G.711	G.711	1	
	ICMP Dest Unreach	Internet Control Messa	1	
	POP3	Post Office Protocol	1	
	RTCP	Real-Time Transport C	1	
	X-Windows	X-Windows Server	1	

- *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.

÷	Тор	Protocols: 11	⊞	=		×
		Protocol +		Description +	Expert Events 🔺	
	~	HTTP		World Wide Web HTTP	3	
	~	TCP		Internet Transmission	3	
		SIP		Session Initiation Prot	2	
	~	SMTP		Simple Mail Transfer P	2	
		DNS		Domain Name System	1	
		FTP Ctl		File Transfer Protocol	1	
		G.711		G.711	1	
		ICMP Dest Unrea	ch	Internet Control Messa	1	
		POP3		Post Office Protocol	1	
		RTCP		Real-Time Transport C	1	
		X-Windows		X-Windows Server	1	
						-

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.'

Grippe Ty	r ype Statistics	List View Bar Ch	nart	0	ther C	lose
∷ Тор	Protocols: 11	⊞ ⊨			Other	×
	TCP		3			
	HTTP		3	_		
	SIP		2		•	
	SMTP		2		•	
	DNS		1			
	ICMP Dest Unread	ch	1			
	POP3		1			
	FTP Ctl		1	_		
	X-Windows		1	FTP Ctl		
	RTCP		1	Average Expert	Events : 1	
	Other		1			
			Average Expe	rt Events		
						4

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.
- 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.

CHAPTER 6

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.

Ø Omnipeek							
<u>Eile</u> Edit Viev	w Capture Tools Window Help					Live	Action
: 🔊 . 📢 . 🗐							Accion
		2 -					
	Capture 1 ×						P
Packets received: 8	3,458 Buffer usage: 2%	cont all packets				Stop C	apture
Packets filtereu: o	1,458 Filter state: 🛶 Au	cept all packets					
The state of the second	(pression here (use F1 for help)						
Dashboards	🗢 🔿 🖽 📰 🛛 🖬 🔍 🎭 🔚	🔄 🛜 - । 🏣 । 😵 🚱 😼 ।	10 🔊				
Applications	Packet Source	Destination	Flow ID	BSSID	Flags	Channel	Signal ^
Voice & Video	6 #184+38+35+5E+97+52	16.01.01.5E.07.52			-	1	37%
Compass	7 16.01.01.55.97.52	10.01.01.01.07.02			-	1	78%
Canture	8 116.01.01.55.97.52	84.38.35.5F.97.52			-	1	65%
Packets	9 10.01.01.01.01.02	16.01.01.5F.97.52			-	1	37%
Events	10 16:01:01:55:97:52	84:38:35:5F:97:52			#	1	70%
Notes	11 11 16.01.01.55.97.52	84.38.35.5F.97.52			-	1	63%
Filters	12 11 84:38:35:5F:97:52	16:01:01:5F:97:52			#	1	37%
Evnert	13 16.01.01.55.97.52	84-38-35-5F-97-52			-	1	73%
Clients/Servers	14 16:01:01:55:97:52	84-38-35-5E-97-52			-	1	63%
Flows	15 1184.38.35.55.97.52	16.01.01.5F.07.52			-	1	37%
Applications	16	■ 9E · 38 · 35 · B1 · 40 · 6B			#C	1	210
Web	17 116:01:01:55:97:52	84:38:35:5F:97:52			#	1	63%
Servers	18 10.01.01.01.01.02	B 00 8 C 0 2 0 6 0 1 4 3 0		16.01.01.5E.97.52	CWA	1	23%
Clients	10 116.01.01.55.07.52	W 01.38.35.5F.07.52		10.01.01.01.07.02	#	1	65%
Pages	20 84.38.35.55.97.52	16.01.01.5F.07.52			-	1	73%
Pequests	21 29 DD D 2 78 87 CB	A1-26-9E-70-52-DC		BB 08 • 82 • FD • 82 • 48 • 2D	- C+	1	47%
Voice & Video	21 mgr25100102170107100	16.01.01.5F.07.52		By 90.02.10.02.A0.20	#	1	23%
Calle	22	16.01.01.5F.97.52			+	1	34%
Media	24 16.01.01.55.07.52	## 84+38+35+5F+07+52			-	1	73%
Visuals	24 84.38.35.55.97.52			16.01.01.5E.97.52	μA	1	24%
Peer Man	25 16.01.01.55.07.52	## 84-38-35-5E-07-52		Mg/10.01.01.01.07.02	#	1	65%
Graphs	27 84.38.35.55.07.52	16.01.01.5F.07.52			-	1	3/1%
Statistics	27 16:01:01:55:07:52	B 24 - 38 - 35 - 5F - 97 - 52			-	1	76%
Summary	20 84.38.35.55.07.52	# 1 apperElec: 06:14:34		16.01.01.5E.07.52	# CMA	1	23%
Nodes	29 16:01:01:55:07:52	10 Caller Clec. 00. 14. 54		Mg/10:01:01:01:07:02	#	1	63%
Protocole	31 84,32,35,55,07,52	16.01.01.5E.07.52			-	1	7.9%
Applications	22 BD0.D6.40.C3.08.2F	PC - 6A - AQ - QE - A6 - ED		16.01.01.5E.07.52	en al cui	1	50%
Countries	32 800.00.45.05.00.21	BC.0A.A0.01.A0.00		H 10.01.01.31.37.32	#	1	24%
Wireless	34 NovatelWic:D1:33:BD	Ethernet Broadcast		# 7D • 04 • FE • 77 • FB • 3F	# *DC	1	5%
WIAN	25 #16.01.01.5F.07.52	104-38-35-5F-07-52		Bg/0.04.10.77.10.5.5		1	68%
Channels	36 116.01.01.55.97.52	Ethernet Broadcast		16.01.01.5E.97.52	*p	1	78%
Signal	37 ##NovatalWip:B0:CA:E7	Ethernet Broadcast		HanovatalWic:BO:CA:E7	*D	1	7%
Peaming	28 #184-38-35-5F-07-52	16.01.01.5F.07.52		MovaceIwin .by.ca.iv	-	1	78%
Koanning	30 2004.00.00.00.00.02	10.01.01.51.57.52		## 18 · 84 · 89 · 75 · 90 · 41	- C+	1	47%
by Node	40	16.01.01.5E.07.52		10.04.09.75.96.AI	#	1	24%
by AP	40				-	-	700
07 0	•						•
Capturing		🕎 WiFi Adapter for Omnipeek	3 Channel: 1	- 2412 MHz (bgn) Packets: 8,4	58	Duration: 0:	00:35

- 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.

Toggle Orientation



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

CHAPTER 7

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.

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.

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.

F	Reject Matching	Start/Stop Captu	ire
Ø Omnipeek			x
File Edit Viev	v Captur <mark>e Tools Window I</mark>	ielp LiveAct	tion
i 🎾 - 🚺 - 📕			
d Start Page	Canture 1 x		Þ
Packets received: 0 Packets filtered: 0	Buffer usage: Filter state:	0% Accept all packets Start Captur	re
Sector a filter ex	pression here (use F1 for help)		
Dashboards	🚧 🗱 👯 📲 Insert 🕜 👼	× @ @ - @ ₽	
Applications	Filter	Comment	<u>^</u>
Voice & Video	Infrastructure		
Compass	Image: Security		
Capture	Vireless		
Packets	Vireless Performance		
Notes	Vireless Policy		
Filters	Vireless Security		
Expert	ARP	IP address resolution protocol	
Clients/Servers	Authentication	RADIUS, TACACS, Kerberos, or 802.1X	=
Flows	BitTorrent	Peer-to-peer file sharing	
Applications	Broadcast	Physical layer broadcasts	
Web	DHCP	DHCP packets	
Servers	DNS	DNS packets	
Pages	Error	Error packets	
Requests	Frame Relay LMI	Frame Relay management packets	
Voice & Video	FTP	FTP data or control packets	
Calls	HTTP	HTTP packets (Web)	
Media	ICMP	ICMP packets	
Visuals	IGMP	IGMP packets	
Peer Map	IMAP	IMAP packets (email)	
Graphs	Instant Messaging	AOL, MSN, or Yahoo Messenger	
Summary	IP IP	IPv4, ARP, or RARP packets	
Nodes	IPv6	IPv6 packets	
Protocols	LDAP	Lightweight directory access protocol	
Applications	LLMNR Multicast	Well-known multicast address for LLMNR (Link-Local Multicast Name Resolution)	
Countries	mDNS Multicast	Well-known multicast address for mDNS (mulitcast DNS)	-
	•	III	•
Idle		🕎 Local Area Connection Packets: 0 Duration: 0:00:00	

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

Insert

0	Omnineek		
-	ommpeek		
1	File Edit View Capture T	ools Window Help	LiveAction
1	🔊 - 💕 - 📙 📚 🚽 💽 🍸) 🖸 👷 🚦 😫 😥 👩 🖕	
⊲	Start Page Filters X		Þ
2	Tinsert 📝 📼 🗙 🖂 🗟	• B	
		Comments	
FI	ter 🔺	Comment	
Þ	Infrastructure		
P	U Security		
P	Wireless		
P	Wireless Performance		
P	Wireless Policy		
P		TP address resolution protocol	
		IP address resolution protocol	
	RitTorrent	Deerstrugeer file charing	
	Second cast	Preel-to-p	
		DHCP nackets	
		DNS packets	
	Second Second	Error packets	
	Server Relay I MI	Frame Relay management packets	
	FTP	ETP data or control packets	
	♥ HTTP	HTTP packets (Web)	=
	✓ ICMP	ICMP packets	
	SA IGMP	IGMP packets	
	Y IMAP	IMAP packets (email)	
	Y Instant Messaging	AOL, MSN, or Yahoo Messenger	
	¶ ₽	IPv4, ARP, or RARP packets	
	Y IPv6	IPv6 packets	
	V LDAP	Lightweight directory access protocol	
	Y LLMNR Multicast	Well-known multicast address for LLMNR (Link-Local Multicast Name Resolution)	
	💎 mDNS Multicast	Well-known multicast address for mDNS (mulitcast DNS)	
	💎 Multicast	Physical layer multicast packets	
	💎 NetBIOS	NetBIOS packets	
	💎 No Private IP Addresses	Reject IPv4 addresses in the ranges 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16	
	Y No RDP	Reject Microsoft Remote Desktop Protocol	
	POP	POP packets (email)	
	Private IP Addresses	IPv4 addresses in the ranges 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16	
	YRDP	Microsoft Remote Desktop Protocol	
	Service Discovery	Various service discovery protocols	
	Y SMB	SMB packets	
	SMTP	SMTP packets (Email)	
	SNMP	SNMP packets	•

2. Click Insert. The Insert Filter dialog appears.

sert Filter		×
Filter: Untitled		Color: Type: Simple •
Comment:		
Address filter		
Address 1	Type:	Address 2
0.0.0.0		▼ 0.0.0.0 ▼ ▶
0.0.0.0		0.0.0.0
	Both directio	(a) Any address
Choose	<not set=""></not>	
Port 1	Type:	Port 2
	TCP-UDP	
	↔	
	Both direction	(Any port

- 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.

CHAPTER 8

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.

S Omnipeek File Edit Vie S • C • L A Stat Page Packets Titlered:	Cummary Cou	nts	Help	ets	Flov	l Ma w Visu Refres	Make I alize h	e Fi Filte Pr	lter er	Re	esol Eve N	ve Nan entFind Network	nes er Sett x Policy	ings y u u u LiveAct	× ion	
Inter a filter est	pression here (use F1 for h	elp)														
Dashboards	Flows analyzed: 3		Flows recycl	ed: 0		á	₽ - •	- 1	s 🔹	-	5	3				
Applications	Client Addr		Server Addr	ea: 0		Flows	F	vents	P	ackets		Bytes		Duration	3-	
Voice & Video	4 0 10 222 104 104		17 349 139 339			1 10113		2		uchell		916		0.057122	~	
Compass	4 951986>httn	¢	17.240.120.230	,			A	3		2	,	816		0.057132		
Capture	A TCP Repe	ated Conne					A	1				010		0.037132		
Events	A Wireless C	lient - Too						2								
Notes	▲ ● 10.233.104.194		17.253.23.208			1	4	1		5	5	450		0.012999		Upper pane
Filters	⊿ @■ 51978>http)						-			5	450		0.012999		
Expert	🛕 Wireless 0	lient - Too			Flow Vis	ualizer										Expert views
Clients/Servers	▲ ● 172.22.24.33		216.136.95.2	•	Expand A	All				2	3	360		0.009401		•
Applications	⊿ ● 52215>dom	ain		E.	Collonce	AU				2	3	360		0.009401		
Web	🛕 Wireless (lient - Too		-9	conapse	All				_						
Servers					Select Re	lated Packe	ts			+						
Clients																
Pages				×	Show Ad	Idress Name	S									
Requests	1			✓	Show Po	rt Names										
Calls	1				Multi-Se	oment Anal	/sis									
Media						,				_						
Visuals				\$	Make Fil	ter										
Peer Map				5	Insert Inf	to Name Tab	le									
Graphs				-	Resolve I	Names			Ctrl+	R						
Summary	-									-6	_				•	Lower pane
Nodes		ent Summary	Event Log		Expert Vi	ew Options				-1					v	Evport tobo
Protocols	Layer	Event		8	Network	Policy				FI	rst Tim	e	Last Time		^	Expert tabs
Applications	A Wireless	Wireless - Too	Many Physical Er	· 遂	EventFin	der Settings	i	Ctr	+Alt+	V 1	2:33:4	1 10/17/20	16 12:56:22		E	
Wireless	Wireless	Wireless AP - T	oo Many Retries				:	292	10/17/3	2016 1	2:33:4	10/17/20	16 12:55:49			
WLAN	Wireless	Wireless Client	- No Response to	Probe	e Request			208	10/17/3	2016 1	2:33:5	2 10/17/20	16 12:55:59			
Channels	U Wireless	Wireless Client	 Probe Respons 	e Not /	Accepted			154	10/17/3	2016 1	2:33:4	7 10/17/20	16 12:55:55			
Signal	Wireless	Wireless Chann	el Overlap					131	10/17/3	2016 1	2:33:4	2 10/17/20	16 12:55:47			
Roaming	/ Wireless	Wireless AP - P	hysical Errors					127	10/17/2	2016 1	2:33:4	1 10/17/20	16 12:55:47			
by Node	Wireless	Wireless Durati	on Attack					122	10/17/3	2016 1	2:33:4	10/17/20	16 12:55:46			
by AP	wireless	wireless client	- Physical Errors					0.0	10/1//	2016 1	2:33:4	10/1//20	10 12:56:22		-	
Capturing	WIPPSS	AND PRESS SOUTO	WIELAC	apter	for Omni	peek 1 Cha	nnel: 6	- 2427	MHz.(n401	Packe	ts: 53.470	Duratio	n: 0:22:49		
Opens the Flow Vis	ualizer for the selected it	em														
spendence now vis	and a selected in			_			_	_	_		_					

- 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:

Restore Selected Default	Restor	e All User D	efaults						
Toggle All	Set U	lser Defaults	s	Т	Threshold Assistant				
Enable All		Export Settings			Setting			Memory Usage	
Expert EventFinder Se	ettings O _R D	3 🖬						×	
Event	Event		Severity	Enable 🔺	Set	ting			
▷ VoIP	▷ VoIP ▷ Wireless				va	lue			
▷ Wireless						150 🍧	millise	onds	
Network Policy									
▷ Client/Server									
Application									
▷ Apdex									
▷ DHCP				V	Thresh			Assistant	
▷ DNS									
▷ HTTP				V			,		
▷ Oracle				\checkmark	1	Dial-upInte	rnetLA	NFast LAN	
4 POP3				v					
POP3 Login Fa	ailed	Ν	1ajor	V	Me	mory Usage			
POP3 Server F	Returned E	Error N	1ajor	V		147			
POP3 Slow Re	sponse Tir	ne N	1inor	V					
> SMB/CIFS				v	Ma	ximum Flow	s:	50,000	
▷ SMTP				V	Ma	ximum Even	its:	50,000	
_ ⊳ SQL				v					
Show Info No	te: Setting ckets, read	s that are saved ta d a file, or immediat	ake effect the ne ely if you are cap	kt time you hide Huring.		0	K	Cancel	

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.

File Edit View Capture Send Tools Window Help LiveAction Image: Status Range Capture 1 × Recept all packets Status Range St	1										- C - X
Image Contrust X Packets futered: 33.712 Filter state: Accept all packets Packets futered: 33.712 Flows recycled: 0 Packets futered: 33.712 Flows recycled: 0 Packets futered: 23.95 Packets foroped: 0 0 0 Packets futered: 23.95 Packets foroped: 0 0 0 0 Packets Packets foroped: 0 0 0 0 0 0 0 Packets Packets Packets Backets foroped: 0 0	File Edit Vie	w Capture Send	Tools Window	Help							LiveActior
Start Reg. Copure 1 × Packets Received: 83,712 Buffer usage: 27% Packets Received: 2,835 Packets Received: 8 Network Applications Voice & Video Control et et et: 2,835 Packets Received: 1,283 1 Periods 1 Packets Received: 1,283 1 Periods 1 1 Periods 1 1 Periods 1 1 3 Periods 1 1 3 Periods 1 1 3 Periods 1 1 3 Perint Count * Frint	🔊 - 👪 - 📖										
Packets Duffer Usage: 25% December 237/12 Packets Duration Avg Response Time Dashboards Name Flows analyzed: 3 Flows recycled: 0 Packets Packets 0.071132 Packets Packets 0.071132 Packets Packets 0.071132 Packets Packets Packets 0.012999 Packets	1 Start Page		<u></u>		_	-	_	_			h
Packets filtered: 33,12 Filter state: Accept all packets Packets filtered: 23,12 Filter state: Accept all packets Power State Flows are present one (use F1 for help) Packets dropped: 0 0 <th0< th=""></th0<>	Packets received:	83 712 E	Buffer usage: 25%			_					
Enter apression here (use F1 for help) Flows recycled: 0 Packet Source	Packets filtered:	83,712	Filter state: 🦛	Accept all pa	ckets					S	top Capture
Dashboards Network Applications Voice & Video Compas Flows recycled: 0 Packets droppet: 0 Packets droppet: 0 Packets droppet: 0 Name Flows Events v Packets droppet: 0 Packets droppet: 0 Avg Response Time Corpuss • • • 12.48, 128, 228, 228 1 3 8 816 0.057132 Capture • • • 12.23, 101, 194 1 3 8 815 0.057132 Packets • • • 12.23, 101, 194 1 5 450 0.012999 Pottos • • • 12.23, 104, 194 1 5 450 0.012999 Centry/Servers • • • • 12.23, 104, 194 1 1 3 360 0.009401 Centry/Servers • • • • 12.23, 2.23 1 1 3 360 0.009401 Centry/Servers • • • • 127, 22, 24, 33 1 1 3 360 0.009401 Centry Filters Event Summary Event Summary Event Summary Event Summary Filters 10/17/2016 12:33:41 10/17/2016 12:33:42 Wolce & Wideo Call Micriess Wreless Wreless Clent - Nyscal Errors 521	💎 🛨 Enter a filter es	expression here (use F1 f	or help)								
Applications Voice & Video Compass Name Flows Events Packets Bytes Duration Avg Response Time Capture Packets ● \$17.249.128.23 1 3 8 816 0.057132 Image: Capture Packets ● \$17.249.128.23 1 3 8 816 0.057132 Image: Capture Packets ● \$17.253.23.208 1 1 5 450 0.012399 Image: Capture Packets ● \$17.253.23.208 1 1 5 450 0.012399 Image: Capture Packets Image: Capture Packets ● \$17.253.23.208 1 1 3 360 0.009401 Image: Capture Packets Image: Cap	Dashboards Network	Flows analyzed: 3 Events detected: 2,	835	Flows recy Packets drop	cled: 0 ped: 0			æ + ∔ = 1	🗣 😼 😼 l 🗵 🕭		
Voice & Video Compass SSL 1 3 8 816 0.057132 Capture Packets • • 0.10,233,104,194 1 3 8 816 0.057132 Events • • • 0.10,233,104,194 1 5 450 0.012999 Notes •<	Applications	Name		Flows	Events	-	Packets	Byte	es Dura	tion Avg Response Ti	ime
Compass Gapture Padets	Voice & Video	⊿ ●SSL		1	<u>A</u>	3	8	8:	16 0.057	132	
Splute p 0 10.233.104.194 1 3 8 816 0.057132 Events 0 17.253.23.208 1 1 5 450 0.012999 0 Filters 0 10.233.104.194 1 1 5 450 0.012999 0 0 Clents/Servers 0 10.233.104.194 1 1 3 360 0.009401 0 Clents/Servers 0.1239 0 1 3 360 0.009401 0 0 Applications • • 1 3 360 0.009401 0	Compass	⊿ ●● 17.248.12	28.238	1		3	8	81	16 0.057	132	
Events 	Packets	▶ ●● 10.233	3.104.194	1	1	3	8	81	16 0.057	132	
Notes Filters • • •	Events			1	A	1	5	45	50 0.012	999	
Filters 0.0233.104.194 1 1	Notes	A 0 17.253.23	3.208	1	A	1	5	45	50 0.012	999	
Cients/Servers • ONS • 11 • 1 • 1	Filters	▶ ●● 10.233	3. 104. 194	1	<u>A</u>	1	5	45	50 0.012	999	
Clients/Servers ■ ● ● 172.22.24.33 1 1 3 360 0.009401 Applications ▶ ● ● 172.22.24.33 1 1 3 360 0.009401 Web Servers Clients ▶ ● 172.22.24.33 1 1 3 360 0.009401 Web Servers Clients Nodes	Expert			1		1	3	36	0.009	401	
Flows Image: Second Secon	Clients/Servers	▲ ● 216,136,9	15.2	1	A	1	3	36	50 0.009	401	
Applications Vertex Nute Image: Superstand Superstext Supred Superstand Superstand Supred Superstand Sup	Flows	▶ ● 172.22	2.24.33	1	A	1	3	36	50 0.009	401	
Web Servers Clents Pages Requests Voice & Video Calls Media Media Fisuals Peer Maph Statistics Statistics Summary Volce & Wieless Wireless Wireless Wireless Wireless </td <td>Applications</td> <td></td> <td>12 1100</td> <td>-</td> <td><u></u></td> <td>-</td> <td>-</td> <td></td> <td></td> <td>101</td> <td></td>	Applications		12 1100	-	<u></u>	-	-			101	
Servers Clents Pages Requests Voice & Video Calis Media Mission Summary Details Fortocols Layer Event Summary Count Nodes Layer Event Summary Count Applications A Wireless Wireless Signal Wireless Wireless	Neb										
Calis Pages Requests Voice & Video Calis Media Media Mission Peer Map Graphs Statistics Summary Nodes Layer Event Summary Vireless Nodes Layer Protocols Layer Applications Mireless Wireless Wireless Wireless Wireless Wireless Wireless Clent - Physical Errors Signal Wireless Wireless Wireless Probe Request Signal Wireless Wireless Wireless Rachamed Covertage Wireless Wireless Rachamed Covertage Vireless Wireless Clent - Probe Response Not Accepted Signal Wireless Wireless Wireless Clent - Probe Resp	Clients										
Requests Valce & Video Calls Media Stausts Peer Map Graphs Statistics Summary Nodes Layer Event Summary Protocols Layer Event Summary Protocols Layer Event Summary Wireless	Pages										
Applications A Wireless Wireless Wireless Wireless Wireless Output Summary Count First Time Last Time Applications A Wireless Wireless Count v First Time Last Time Applications A Wireless Wireless Too Many Physical Errors 562 10/17/2016 12:33:41 10/17/2016 13:08:43 Countries A Wireless Wireless AP - Too Many Physical Errors 562 10/17/2016 12:33:41 10/17/2016 13:08:43 Countries A Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:17 VLAN Wireless Wireless Wireless 10/18/10/17/2016 12:33:41 10/17/2016 13:08:13 Signal Wireless Wireless Wireless 10/18/10/17/2016 12:33:41 10/17/2016 13:08:13 Voaming Wireless Wireless Wireless P- Probysical Errors 233 10/17/2016 12:33:41 10/17/2016 13:08:12 Log Wireless Wireless AP - Physical Errors 233 10/17/2016 12:33:41 10/17/2016 13:08:12 Log Wireless Wireless AP - Probe Response to Probe Request 233											
Cals Media Media Media Peer Map Graphs Graphs Suttistics Summary Nodes Protocol Layer Event Log Applications M Wreless August Stress Wireless Wireless Wireless (Line Physical Errors Souming M Wreless Wireless Wireless (Line Physical Errors Signal Wireless Wireless Wireless (Line Physical Errors Log Wireless	Requests										
Media /isuals Paer Map Graphs Statistics Statistics Statistics Statistics Statistics Statistics Statistics Statistics Applications A Wireless Applications Mireless Mireless Wireless Wireless Wireless Client - Physical Errors Signal Wireless Wireless Wireless Probe Response Not Accepted Signal Wireless Wireless Wireless Norte Response Not Accepted Signal Wireless Wireless Wireless Nore Response Not Accepted	Requests										
Visuals Peer Map Graphs Visuals Visuals Summary Image: Statistics Image: Statistics <t< td=""><td>Calls</td><td>-</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Calls	-									
Peer Map Graphs Graphs Satstics Summary Nodes Image: Count of the second of the	Requests /oice & Video Calls Media	1									
Graphs Statistics Protocols Layer Event Count	Requests Voice & Video Calls Media Visuals										
Statistics Summary Details Event Summary Event Log Nodes Layer Event Count First Time Last Time Applications A Wireless Wireless Too Many Physical Errors 562 10/17/2016 12:33:41 10/17/2016 13:08:13 Wireless Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:14 WLAN Image: Stress Wireless Client - No Response to Probe Request 286 10/17/2016 12:33:41 10/17/2016 13:08:14 Channels Image: Wireless Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:13 Signal Image: Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:13 Roaming Image: Wireless Wireless Client - No Response Not Accepted 222 10/17/2016 12:33:41 10/17/2016 13:08:12 Log Image: Wireless Wireless Wireless P - Physical Errors 233 10/17/2016 12:33:42 10/17/2016 13:08:23 by Node Image: Wireless Client - Probe Response Not Accepted 222 10/17/2016 1	Requests Voice & Video Calls Media Visuals Peer Map										
Summary Image: Source Address is Militaat Event Log Nodes Layer Event Log First Time Last Time Applications Mireless Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:43 VLAN Mireless Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:14 VLAN Wireless Wireless Wireless Wireless 10/17/2016 13:08:14 Signal Wireless Wireless Wireless 10/17/2016 13:08:13 10/17/2016 13:08:13 Log Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:13 Log Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:12 Log Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:12 Log Wireless Wireless Wireless Not Accepted 222 10/17/2016 12:03:47 10/17/2016 13:08:12 Log Wireless Wireless Client - Probe Response Not Accepted 222 <t< td=""><td>Requests Voice & Video Calls Media Visuals Peer Map Graphs</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Requests Voice & Video Calls Media Visuals Peer Map Graphs										
Notes Layer Event Count First Time Last Time Applications A Wireless Wireless Wireless 10/17/2016 12:33:41 10/17/2016 13:08:43 Countries A Wireless Wireless Wireless Wireless 10/17/2016 13:08:43 WLAN A Wireless Wireless Client - Physical Errors 287 10/17/2016 12:33:41 10/17/2016 13:08:14 Channels Wireless Wireless Client - No Response to Probe Request 286 10/17/2016 12:33:41 10/17/2016 13:08:13 Signal Wireless Wireless Wireless Client - Probe Request 233 10/17/2016 12:33:41 10/17/2016 13:08:13 Roaming A Wireless Wireless Client - Probe Response Not Accepted 222 10/17/2016 12:33:47 10/17/2016 13:08:12 Log Wireless Wireless Wireless Client - Probe Response Not Accepted 222 10/17/2016 12:33:47 10/17/2016 13:08:12 Log Wireless Wireless Client - Probe Response Not Accepted 222 10/17/2016 12:33:47 10/17/2016 13:08:12 Log	Requests Voice & Video Calls Media Visuals Peer Map Graphs Statistics	1									
Applications Countries Wireless Wireless Wireless Wireless Environment 10/17/2016 13:08:43 Countries M Wireless Wireless Wireless 10/17/2016 12:03:44 10/17/2016 13:08:43 Wireless Wireless Wireless Wireless 10/17/2016 12:03:44 10/17/2016 13:08:17 WLAN M Wireless Wireless Wireless Wireless 10/17/2016 12:03:44 10/17/2016 13:08:17 Signal Wireless Wireless Wireless Wireless 10/17/2016 12:03:45 10/17/2016 13:06:58 Signal Wireless Wireless Wireless Wireless 10/17/2016 12:03:45 10/17/2016 13:06:58 Signal Wireless Wireless Wireless 10/17/2016 13:08:11 10/17/2016 13:08:12 Log Wireless Wireless Wireless Wireless 10/17/2016 13:08:12 10/17/2016 13:08:12 Log	Requests Voice & Video Calls Media Visuals Peer Map Graphs Statistics Summary Nodes	d Details	Event Summary	Event Log	3		\. .				Ø
Countries Writeless Writeless Writeless Writeless 10/17/2016 12:03:12 10/17/2016 13:08:17 Wineless Writeless Writeless Writeless 410/17/2016 12:03:14 10/17/2016 13:08:17 WLAN A Writeless Writeless Writeless 10/17/2016 12:03:14 10/17/2016 13:08:17 WLAN A Writeless Writeless Writeless 10/17/2016 12:03:14 10/17/2016 13:08:17 Channels Writeless Writeless Writeless 10/17/2016 12:03:14 10/17/2016 13:08:17 Roaming I Wireless Wrieless Wrieless 10:17/2016 13:08:13 Log III Wireless Wrieless Wrieless 10:17/2016 13:08:12 10/17/2016 13:08:12 Log IIII Wrieless Wrieless Wrieless 10:17/2016 13:08:12 10/17/2016 13:08:12 Log IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Requests Voice & Video Calls Media Visuals Peer Map Graphs Statistics Summary Nodes Protocols	4 Details	Event Summary	Event Log				Count v	First Time	Last Time	1
Wireless	Requests Voice & Video Calls Media Visuals Peer Map Graphs Statistics Summary Nodes Protocols Applications	4 Details Layer Microsoft	Event Summary Event	Event Log				Count v	First Time	Last Time	5
WLAN Wireless Wireless Guent - Finystal Errors 267 10/17/2016 12:33:47 20/17/2016 13:06:58 Channels Image: Wireless Guent - No Response to Probe Request 286 10/17/2016 12:33:45 10/17/2016 13:06:58 Signal Image: Wireless Guent - No Response to Probe Request 286 10/17/2016 12:33:45 10/17/2016 13:06:58 Roaming Image: Wireless Wireless AP - Physical Errors 233 10/17/2016 12:33:47 10/17/2016 13:08:12 Log Image: Wireless Wireless Clent - Probe Response Not Accepted 222 10/17/2016 12:33:47 10/17/2016 13:08:13 by Note Image: Wireless Source Address is Multicated 131 10/17/2016 13:08:11 10/17/2016 13:08:12	Requests Voice & Video Calls Media Visuals Peer Map Graphs Statistics Summary Nodes Protocols Applications Countries	Details Layer Wireless	Event Summary Event Wireless Too 1	Event Log Many Physical I	Errors			Count • 562	First Time 10/17/2015 12:33:41	Last Time 10/17/2016 13:08:43	ł
Channels Wireless Wireless Wireless Duration Attack 237 10/17/2016 12:33:45 10/17/2016 13:08:13 Signal Image: Comparison of the second state of the sec	kequests /oice & Video Calls Media //suals Peer Map Graphs Statistics Summary Nodes Protocols Applications Countries Wireless	Details Layer Wreless Wireless Wireless	Event Summary Event Wireless - Too 1 Wireless AP - Too	Event Log Many Physical I Doo Many Retrie	Errors es			Count ▼ 562 416	First Time 10/17/2016 12:33:41 10/17/2016 12:33:41	Last Time 10/17/2016 13:08:43 10/17/2016 13:08:17 10/17/2016 13:08:17	3
Signal Wireless Wireless Duration Attook 2.57 10/17/2016 12:33:41 10/17/2016 13:08:13 Roaming Mireless Wireless Wireless Wireless 233 10/17/2016 12:33:41 10/17/2016 13:08:12 Log Wireless Wireless Wireless Wireless 221 10/17/2016 12:33:47 10/17/2016 13:08:23 by Node Wireless Wireless Channel Overlap 181 10/17/2016 12:33:42 10/17/2016 13:08:23 by AP Mireless Wireless is Multicast 134 10/17/2016 13:08:27:99	kequests Voice & Video Calls Media isuals Peer Map Graphs Statistics Summary Nodes Protocols Applications Countries WLAN	Details Layer Layer Wireless Wireless Wireless Wireless	Event Summary Event Wreless - Too 1 Wreless AP - To Wreless Clent	Event Log Many Physical I oo Many Retrie - Physical Error	Errors :s			Count ▼ 562 416 287 296	First Time 10/17/2016 12:33:41 10/17/2016 12:33:44 10/17/2016 12:33:42	Last Time 10/17/2016 13:08:43 10/17/2016 13:08:17 10/17/2016 13:08:19	Þ
Koaming A Wireless Wireless Pro-Physical Errors 233 10/17/2016 12:33:47 10/17/2016 13:08:12 Log Image: Mireless Wireless Wireless Wireless 10/17/2016 12:33:47 10/17/2016 12:33:47 10/17/2016 13:08:12 by Node Image: Wireless Wireless Wireless 10/17/2016 13:08:12 10/17/2016 13:08:12 by AP Image: Wireless Wireless Source Address is Miltrast 134 10/17/2016 13:08:12 10/17/2016 13:08:12	Kequests Voice & Video Calls Media Visuals Peer Map Graphs Statistics Statistics Summary Nodes Protocols Applications Countries Vireless WkAN Channels	Details Layer Layer Wreless Wireless Wireless Wireless Wireless	Event Summary Event Wreless - Too 1 Wreless AP - T Wreless Client Wreless Client	Event Log Many Physical I oo Many Retrie - Physical Error - No Response	Errors es rs to Probe I	Reque	st	Count ▼ 562 416 287 286	First Time 10/17/2016 12:33:41 10/17/2016 12:33:44 10/17/2016 12:33:42	Last Time 10/17/2016 13:08:43 10/17/2016 13:08:14 10/17/2016 13:06:58	Ē
Log Wireless Wireless Wireless Wireless Ultraction	Kequests Voice & Video Calis Media Visuals Peer Map Graphs Statistics Summary Nodes Protocols Applications Countries Wirka Kireless Wirka Channels Signal	Details Layer Layer Wreless Wireless Wireless Wireless Wireless Wireless	Event Summary Event Wreless - Too 1 Wreless AP - T Wreless Clent Wreless Clent	Event Log Many Physical I o Many Retrie - Physical Error - No Response on Attack	Errors es rs to Probe I	Reque	st	Count ▼ 562 416 287 286 237	First Time 10/17/2016 12:33:41 10/17/2016 12:33:41 10/17/2016 12:33:42 10/17/2016 12:33:45 10/17/2016 12:33:45	Last Time 10/17/2016 13:08:43 10/17/2016 13:08:17 10/17/2016 13:08:14 10/17/2016 13:08:13 10/17/2016 13:08:13	
by Node Wireless Wireless Channel Overlap 181 10/17/2016 12:53:42 10/17/2016 13:03:11 by AP Wireless Wireless Source Address is Multicast 134 10/17/2016 12:33:49 10/17/2016 13:07:29	Kequests Voice & Video Cals Media Vesuals Peer Map Graphs Statistics Summary Nodes Statistics Summary Nodes Protocols Applications Countries Wireless WLAN Channels Signal Roaming		Event Summary Event Wreless - Too 1 Wreless AP - Tr Wreless Client Wreless Durati Wreless Durati	Event Log Many Physical I oo Many Retrie - Physical Error No Response on Attack hysical Errors	Errors ts to Probe I	Reque	st	Count	First Time 10/17/2016 12:33:41 10/17/2016 12:33:44 10/17/2016 12:33:45 10/17/2016 12:33:45 10/17/2016 12:33:45	Last Time 10/17/2016 13:08:43 10/17/2016 13:08:17 10/17/2016 13:08:18 10/17/2016 13:08:13 10/17/2016 13:08:13 10/17/2016 13:08:13	
Wreless Wireless Source Address is Millrast 134 10/17/2016 12:33:49 10/17/2016 13:07:29	kequests Voice & Video Calls Media Visuals Peer Map Graphs Statistics Summary Nodes Protocols Applications Countries Wireless WUAN Channels Signal Roaming Log by None	☐ Details Layer A Mireless ▲ ▲ Wireless ● Wireless	Event Summary Event Wreless - Too 1 Wreless Clent Wreless Clent Wreless Durati Wreless AP - PI Wreless Clent	Event Log Wany Physical Too Physical Errors - No Response on Attack - Probe Response	Errors es 's to Probe P	Reque	st d	Count v 562 416 287 286 237 233 222 232	First Time 10/17/2016 12:33:41 10/17/2016 12:33:44 10/17/2016 12:33:45 10/17/2016 12:33:45 10/17/2016 12:33:41 10/17/2016 12:33:47	Last Time 10/17/2016 13:08:43 10/17/2016 13:08:17 10/17/2016 13:08:18 10/17/2016 13:08:13 10/17/2016 13:08:12 10/17/2016 13:08:23	5
	Kequests Voice & Video Calis Media Visuals Peer Map Graphs Statistics Statistics Statistics Statistics Nodes Protocols Applications Countries Wireless Wireless Wireless Signal Roamig Log by Node hv Ap	↓ Details Layer ↓ ▲ Wireless ● Wireless ● Wireless ● Wireless ● Wireless	Event Summary Event Wreless - Too 1 Wreless Clent Wreless Clent Wreless Clent Wreless Clent Wreless Clent Wreless Clent	Event Log Many Physical al oo Many Retrie - No Response on Attack hysical Errors - Probe Response el Overlap	Errors es to Probe I nse Not Ac	Reque	st	Count Co	First Time 10/17/2016 12:33:41 10/17/2016 12:33:41 10/17/2016 12:33:42 10/17/2016 12:33:45 10/17/2016 12:33:45 10/17/2016 12:33:47 10/17/2016 12:33:42	Last Time 10/17/2016 13:08:43 10/17/2016 13:08:17 10/17/2016 13:08:17 10/17/2016 13:08:13 10/17/2016 13:08:23 10/17/2016 13:08:23 10/17/2016 13:08:23	

CHAPTER 9

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 Map Ladder

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

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.

File Edit View Capture To	ools Window He	elp				LiveAct
🔊 - 🖏 - 📙 😂 📜 🖬 😭	9 , 1					
Start Page Multi-Segm	ent Analysis Project	×				
lows (1)			-			🌍 Analysis Op
ow/Segment	 Protocol 	Packets	Packets Lost	Client Retransmi	Server Retrans	Star
☑ 10.4.100.41:1134 <-> 172.20.2	03.5:80					
wireles	s HTTP	19	0	4	0	6/19/2012 16:22:42.47671
10.	5 HTTP	17	2	4	0	6/19/2012 16:22:41.51570
172.20.12	8 HTTP	17	2	4	0	6/19/2012 16:22:41.53069
172.20.20		17	2	4	0	6/19/2012 16:22:41.53118
172.20.20	2 HIIP 3 HTTP	17	2	4	0	6/19/2012 16:22:41.52008
	-				-	-,,
		III				
wireless			10.5			172.20.128
TL:128 SYN	0000	► 0.0000 TTL:126 5	/N	1 00000		TTL:125 SYN
		2 TTL:57	SYN ACK			
TIL:50 STN ACK	0000 -	0.0100 TTL:126 A	СК	3010000	- 0.010	TIL:59 STN ACK
TL:128 ACK DSH		TTL:126 A	CK PSH	4	*	TTL:125 ACK DEH
TTL:56 ACK	0000 -	0.0200 5 TTL:57	ACK	20000	- 0.020	TTL:59 ACK
		0.030000				
0.04		0.040000		0.040000	E 0.040	0.00
		0.050000				
0.06		0.060000		0.060000	E 0.060	000 0.0
TTL:56 ACK PSH		6 TTL:57	ACK PSH			6 TTL:59 ACK PSH
TL:128 ACK FIN 7		TTL:126 A	UK FIN	7000		TTL:125 ACK FIN 7
TTL:56 ACK	1		AUK			8 TTL:59 ACK
TL:128 ACK RST		101 TT -5	7 ACK		1	TTL:125 ACK RST
UU TTL:56 ACK		TTL:126 B	ST		2	10 1TL:59 ACK
		12 TTL:5	7 ACK			11 TEL:125 RST 11
	F4HHI -	E WIAA			- 1111	12 11L:59 ACK
		13 TTL:5	7 ACK	¥//// =	- 1111	12 TTL FO ACK

Ladder

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.

New Multi-Segment Analysis P	roject
	Create a new Multi-Segment Analysis project
	 Search for packets on remote engines Use packet files
	< Back Next > Cancel Help

- 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.

New Multi-Segment Analysis Project
Time Range & Filter Choose the time range and filter for the search.
V Time Range
Start time: 10/ 4/2016 v 11:00:18 +/- 10 seconds
End time: 10/ 5/2016
Duration: 1d 0:47:00.00000000
Tilter
No Filter
<u>Edit</u> <u>Llear</u>
< Back Next > Cancel Help

• 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.

Engines	s Project			
Choose engines to sea	arch.			
💷 🐼 Caabuua Easia	_			
Capture Engin	e 8			
Capture Engin	e			
Capture Engin	e			
Cupture Engin	-			
Enable all Disable all				
	< Back	Next >	Cancel	Help

- 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.

Capture Sessions Choose capture session will create a separate f	ns and dick Next to start the ile to represent a different n	search. Each capture se etwork segment.	ession
Engine/Capture Session	Data Start Time 🔍	Data End Time	Adapter 🔺
4 👿 😰 Capture Engine	1		
V Everything	10/4/2016 20:18:36	10/7/2016 14:28:14	10G-2P (Hi =
🔺 📃 返 Capture Engine			
No results were f	ound.		
🔺 📃 返 Capture Engine			
No results were f	ound.		
🔺 🥅 🐼 Capture Engine			-
•			•
nable all Disable all			
Download files to:			
C:\Users\Documents			•

- *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.
Search and Downloa Click Next to contin	d Progress ue after searches have con	npleted.	
Capture Engine - root 10.4.2.53:6367 Saving	(root) - Capture 1		
Capture Engine - root 10.4.2.53:6367 Complete	(root) - Capture 2		

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.

5	Segments Add files captured on separate network segments arranged by the route taken by the packets from client to server.			
ł	Insert 📝 🗙 🛛 🕆 🛛	9		
	Segment Name	File		
1	Capture Engine - roo	C:\Users\rquilalang\Documents\Capture Engine_root (root) - Capt		
2	Capture Engine - roo	C: Users Yourialang Documents Lapture Engine_Tool (root) - Capt Capture Engine_Tool (root) - Capture		
	[

- *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 Choose a name and lo	cation for the project file.		
Project file:			
C:\Users\Documents\Multi-9	Geoment Analysis 8.msa		
	-		

• *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.

ken	Insert 🕜 🗙 🔞	dient to server.	ige Clear Manua	al Offsets		
	Segment Name	Calc. Offset	Manual Offset	Mapping Profile	File	-
1	wireless	0.000000	0.000000	NAT Map	▼ Y:\Development_W	N ⊑
2	10.5	0.961705	0.000000	(none)	 Y:\Development_W 	N
3	172.20.128	0.946216	0.000000	(none)	 Y:\Development_W 	- N
< [m				-
) Dis	sable auto-synchroni itomatically calculate	synchronization offs	ets			

- 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.

🕶 📄 🛛 Swap	
re no items to show ir	n this view.
ОК	Cancel Help
3	 - <a>Swap are no items to show in

- 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.

CHAPTER 10

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, Pro-tocols, 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.

Dimnipeek 🔊					
File Edit View	Capture Tools Window	/ Help			LiveAction
i 🔊 - 🖏 - 📙 🛛	🖕 ; 💽 🍸 💽 , i 🏤				
	Packet Examples.wpz ×				⊳
Packets: 8,08:	1 0.50		9/4/2012 13:16:47.6	29241 - 9/4/2012 13:17:42.605236	Duration: 54.975995
Flows: 74	0.40				
Events: 236	2 0.30				
Applications: 16	Q 0.20				
IP Addresses: 50	0.10				
Countries: 4	13:16:47 13:16	53 13:16:59	13:17:05 13:17:11 13:17:17	13:17:23 13:17:29	13:17:35 13:17:4
Ther a filter exp	pression here (use F1 for help)				
Network	Nodes: 50 IP	२ - ¥ AI	■ • 🚝 • § § § § 😔 🗠		
Applications	Node	Country	Total Bytes %	 Total Bytes 	Packets Sen
Voice & Video	3 172.20.120.101	? Private Network	57.898%	1,151,882	2,63
Compass	3 172.20.120.15	? Private Network	57.898%	1,151,882	2,63
Capture	💂 frd-as2s39.erols.com	United States	22.758%	452,773	26
Packets	192.216.124.26	United States	19.367%	385,296	26
Events	john.silkstream.com	United States	7.096%	141,166	17
Evport	www.urbanlegends.com	United States	7.060%	140,451	15
Clients/Servers	192.216.124.1	United States	5.107%	101,612	27
Flows	205.227.189.62	United States	4.896%	97,396	41
Applications	192.216.124.49	United States	4.807%	95,640	37
Web	192.216.124.35	United States	3.442%	68,478	7
Servers	141.163.38.200	United Kingdom	3.424%	68,122	5
Clients	165.113.211.2	United States	0.267%	5,305	1
Pages	210.159.66.41	• Japan	0.210%	4,180	
Requests	169.199.29.5	United States	0.125%	2,492	1
Calle	192.216.124.55	United States	0.113%	2,253	
Media	MIKE-PC	United States	0.108%	2,157	
Visuals	192.216.124.37	United States	0.095%	1.887	1
Peer Map	192,216,124,22	United States	0.083%	1,650	1
Graphs	192,216,124,27	United States	0.080%	1,595	1
Files	157.22.226.1	United States	0.080%	1,587	1
Statistics	192,216,124,33	United States	0.079%	1,565	1
Summary	206.50.182.5	United States	0.079%	1,564	1
Rectocols	131, 119, 38, 170	United States	0.056%	1,110	1
Applications	131, 119, 246, 6	United States	0.055%	1,092	_
Countries					
					*

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.

	Color Globe		No	de Type	9			
Omnipeek								2 X
File Edit Vie	w Capture Tools Window He	In	_		_		Live	Action
The Luit Vie	w capture roots window rie	ιν ····						ACCION
🔊 - 😰 - 💾	🛸 👔 🖬 🍸 🖻 🚽 👬	😢 🚺 🚽						
1 Start Page	Sample_Packets.pkt ×							⊳
Packets: 45	0.797		7/	16/20 <mark>12 9:16</mark> :	06.551102 - 7/16/	2012 9:23:53.332776	Duration: 0:07:46	.781673
Flows: 5 Files: 0 Events: 5,9 Applications: 5 IP Addresses: 3 Countries: 1	4.0 9 3.0 1 2.0 1 0 1 0	9:17:46 9:	18:36 9:19	:26 9:2	20:16 9:21:	06 9:21:56	9:22:46	9:23:36
				••••				•••••
Free a filter e	xpression here (use F1 for help)							
Network	V/ireless Networks: 11 Access Points: 19	Ad Hoc Networks Clients	: 0 : 193	All Nodes	💌 🦞 🗳	🖻 - 🔻 All - 💈) 😵 😼 🕍	
Applications Voice & Video	Node	🔺 Туре	Channel	Band	Encryption	Trust	Cur. Signal	C
Compass	a 🔵 10001	ESSID	6					
apture	Motorola:3A:6E:50	AP	6	802.11b	TKIP	Unknown	3	
Packets	⊿ 🔵 Buffalo_an	ESSID	48					
Events	▲ 🔴 Buffalo:6F:10:8F	AP	48	802.11a	CCMP	Unknown	42	
Notes	D-Link: 57:D0:96	STA	48	802.11n	TKIP	Unknown	37	
xpert		ESSID	6					
Clients/Servers	Cisco:D3:C1:70	AP	6	802, 11b	TKIP	Unknown	4	
Hows	A C ESSID Unknown		6					
Applications	4 Cisco:08:5D:11	AP	6	802, 11b		Unknown	27	
Servers	HonHaiPrec:9E:3D:15	STA	6	802.11b		Unknown	28	
Clients	Gisco:58:41:C0	AP	6	802.11b		Unknown		
Pages	Intel:01:E5:20	STA	6	802.11b		Unknown	3	
Requests	Intel: 1D: 11:2C	STA	6	802.11b	TKIP	Unknown	5	
oice & Video	Cisco:C2:D4:20	AP	6	802, 11b		Unknown	13	
Calls	Cisco:C2:D4:24	ΔΡ	6	802.11b		Unknown	13	
Media	Cisco:C2:D4:25	ΔΡ	6	802.11b	CCMP	Unknown	11	
Deer Man	Xerox:00:00:00	AP	6	802.11b		Unknown	47	
Graphs	A BSSID Unknown						14	
Files	1958	ESSID						
tatistics	2WIRE132	ESSID						
Summary	AerobiveNe:9C-FR-50	AP	6	802.11b		Unknown		
Nodes	Alwireless	ESSID	0			Still With		
Protocols	Alfa: 32:48:EA	STA	6	802.11b		Unknown	3	
Applications	Apple:04:E8:32	STA	6	802.11b		Unknown	5	
Countries	Apple:08:70:57	STA	6	802.11b		Unknown		
WIAN	Apple:08:70:57	STA	4	802.11b		Unknown		
Channels	Apple:08:08:08:	STA	4	802.11b		Upknown		
Signal	Apple: 18:E2:60	STA	6	802.11b		Unknown		
oaming	Apple: 18:E2:60	STA	7	802.11b		Unknown	0	
Log	Apple: 10.02.00	STA		902.11b		Unknown	9	
by Node	Apple: 20:28:07	STA	6	002.11D		Unknown	8	
			. 4					

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.

CHAPTER 11

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 colorcoded 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.



- 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.

CHAPTER 12

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

A

adapter options . analysis options , & Apdex * + Application Performance Index (Apdex) * + application view * applications ' & ; (((; (+))) applications dashboard (* ASCII * %

С

call quality ' ',' , (((call quality distribution (, call summary (, call utilization (call volume (call vs. network utilization ' ',' , ((Capture Engine & capture window & % connect + files tab & forensics tab ' & installation) Capture Engine Manager) capture file & (capture options dialog. adapter options. general options. general view ' ;' ,((capture session ' ;' +' ,+ , capture templates & & capture window.,) new capture & & new forensics capture & & new monitor capture & & packets view) channels) &) Compass dashboard ', (,) % +), countries) &) current activity, dashboard (*

D

dashboard applications (* Compass (. network () timeline (' voice & video (, data rates) &) details tab ' , DNS server & + domain ,

event markers) (EventFinder settings * + *, events) & events timeline & * events, dashboard (* Expert * + *, F files tab & filter * ' creating a simple filter *) enable a filter * ' insert filter dialog *) make filter command * (reject matching * (view *) flow list + & flow map + &+ (flows) &) forensic search &, &, ', () forensics capture & & , ', forensics tab '&',

G

Ε

general options . general view ' ',' ,((graph inbound/outbound) ' graph interval) (graph type) ' grouping files & -

Η

hexadecimal view * % hierarchy view * + host , HTML report) %

I

inbound) ' installing Capture Engine) IP address,,' &(',(((* + IPv6 address ' &(',(*

L

ladder + &+) legend)) limitations) ,

Μ

make filter command & + mapping profile , ' monitor capture & & MSA + %

analysis options, & capture sessions + , creating project + * engines + , flow list + & flow map + &+ (ladder + &+) mapping profile, ' progress + project + +project file, % project window + &segments + . time range & filter + + wizard + *+ + multi-segment analysis + %

N

name table & + network dashboard () network forensics & network utilization graph (. new forensics capture & & new monitor capture & & node details, * node statistics,) node type icon),,, nodes) &)

0

Omnipeek & Omnipeek capture . opening a capture file & (OSI layer * + outbound) ' overview graph &)

P

packet decode) . packets view) password, pause/play)) peer map, +,, physical address' &(',(* port, project file, % protocols' ',' -,) &))

R

raw packet data * % reject matching * (resolve names &+

S

select related packets) $\,\%\,$, selection results dialog) , session ' $\,$ +' ,

sessions ' * slider controls) (start capture & % ' start page) statistics ,) stop capture & % ' storage tab ' + summary call (, summary info & * synchronizing files & -

T

time range & filter + + time range indicator) (time window selection controls) (timeline dashboard (' timeline graph ' ', ((timeline tab ' * top applications ' $\& \frac{1}{2}$ ((((((())))top channels) &) top countries)) top data rates)) top flows) (&)) top nodes) &) top protocols ' ', ' ,)) top protocols by IP address (((; (+ top talkers ' top talkers by IP address ' & ', (* top VLAN) &) top WLAN) &)

U

view type ((VLAN) &)) voice & video dashboard (, volume, call (-

W

wireless LAN (wireless signal (* WLAN) &)

Ζ

zoom in) ' zoom out) '

units) &

username,