

LiveAction®

# Omnipeek

---

## Getting Started Guide



LiveAction, Inc.  
圣安东尼奥路 960 号200 帕洛阿尔  
托, CA 94303, 美国  
+ 1 (888) 881-1116 [https://  
www.liveaction.com](https://www.liveaction.com)

版权所有 © 2022 LiveAction, Inc. 保  
留所有权利

20220819-GSG-OP222a

# 内容

## 第1章

### 简介.....

Omnipeek 作为便携式分析仪 .....	1 带有分布式捕获引擎的 Omnip... 证 .....	1 网络取
析 .....	2 IP 语音和视频分	
2 多段分析 .....	2 系统要	
求 .....		
2 .....		
3 续订或升级 Omnip... 本 .....	4 安装捕获引 擎 .....	
4 主程序窗口和开始页 .....	4	

## 第2章

### 将 Omnip... 与捕获引擎一起使用 . ...

显示捕获引擎窗口 .....	6 连接到捕获引 擎 ...
----------------	-------------------

## 第三章

### 捕获窗口 .....

创建 Omnip... 引擎捕 获 .....	9 9 创建捕获
-------------------------------	-------------

## 第四章

### 法医搜索.....

从“文件”选项卡进行取证搜索 .....	
18 从“取证”选项卡进行取证搜 索 .....	27

## 第五章

### 仪表板.....

时间线仪表 板 .....	
------------------	--

## 第六章

### 查看和解码数据包 . ...

数据包视图 .....	48 数据
包解码窗口 .....	49

## 第七章

### 创建过滤器 . ...

启用过滤 器 .....	
54	

## 第八章

### 专家故障排除 . ...

专家视图窗口 .....	
56 使用事件查找器 .....	57 应用程序视 图 ...

---

<b>第九章</b>	多段分析.....	
	关于多段分析 .....	
	66 MSA 项目分析选项 . ...	
<b>第十章</b>	统计分析.....	74
	捕获窗口统计信息.....	...
<b>第十一章</b>	使用对等映射 . ...	
	对等地图视图 . ...	
<b>附录 12</b>	键盘快捷键 . ...	
	索引.....	80

## 介绍

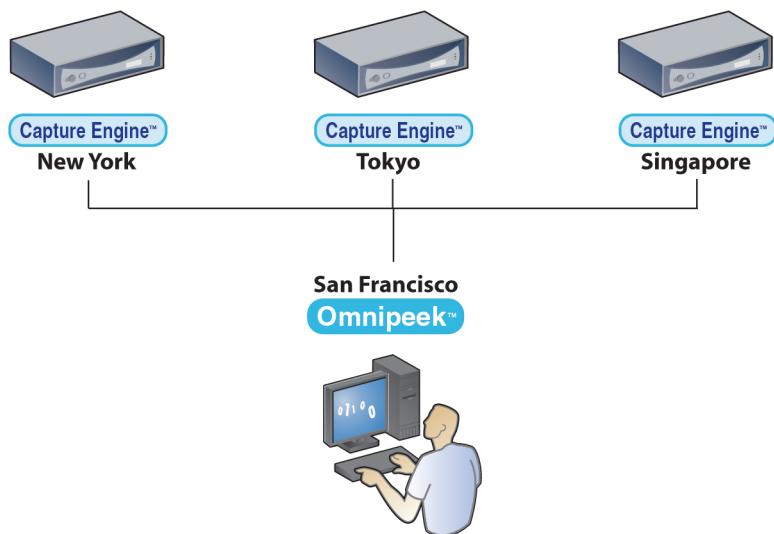
欢迎使用 Omnipack，LiveAction 推出的用于分布式网络分析的网络分析仪和软件控制台！

### Omnipeek 便携式分析仪

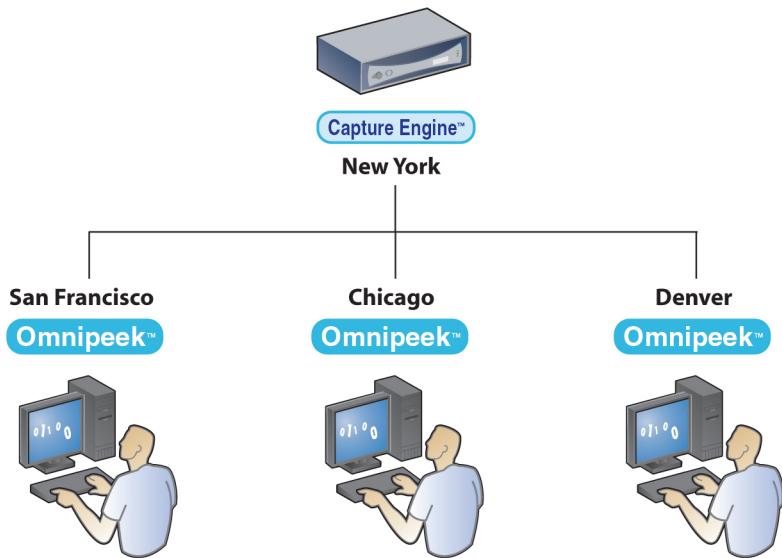
作为一款便携式分析仪，Omnipeek 提供直观、易于使用的图形界面，工程师可利用该界面快速分析和排除企业网络故障。Omnipeek 支持从多个接口进行本地捕获以及从任何网络拓扑（包括 1 Gigabit 和 10 Gigabit 网络、无线网络和本地矩阵交换机）收集数据。

### 具有分布式捕获引擎的 Omnipack

作为捕获引擎的软件控制台，Omnipeek 还可以管理和与无限数量的捕获引擎交互，在网络上的任何位置执行独立的捕获和分析。



Omnipeek 允许网络工程师从单个位置排除故障并对远程段进行统计分析，如上图所示。单个捕获引擎还可以链接到多个 Omnipack 安装，从而实现同时连接和协作，如下所示。



单独购买的捕获引擎没有自己的用户界面。捕获引擎依靠 Omnipeek 通过**捕捉引擎窗口**。有关详细信息，请参阅第 2 章[使用 Omnipeek 与捕获引擎](#)。另请参阅[Omnipeek 捕获引擎入门指南](#)请参阅产品附带的帮助或 Capture Engine Manager 应用程序中的在线帮助。

## 网络取证

网络取证是对网络流量进行回顾性分析，目的是开展调查。您可以使用 Omnipeek 和捕获引擎来捕获、存储和挖掘大量流量数据，以便调查网络问题、安全攻击、人力资源政策违规等问题。

请参阅第 4 章[法医搜索](#)或在线帮助，获取有关如何在您自己的网络上执行取证搜索的信息。

## IP 语音和视频分析

IP 语音和视频可用于呼叫信令和媒体分析[语音和视频捕获窗口视图](#)，提供语音和视频数据流量的同步分析以及主观和客观质量指标。有关语音和视频分析的更多信息，请参阅[Omnipeek 用户指南](#)或在线帮助。

## 指南针仪表板

全方位罗盘仪表板提供关键网络统计数据的交互式取证视图，可以绘制图表、动态交互和报告。凭借其从多个段聚合流量的独特能力，罗盘仪表板为网络工程师提供了更多有关其网络的可见性和洞察力。

这罗盘仪表板提供实时和捕获后高级网络统计数据监控，并具有深入查看选定时间范围内数据包的功能。使用罗盘仪表板，可以同时聚合和分析多个文件。有关更多信息，请参阅[指南针仪表板](#)在第39页。

## 多段分析

多段分析 (MSA) 提供跨多个网络段的应用程序流的可视性和分析，包括网络延迟、数据包丢失和重传。它可以快速查明跨多个段的问题及其根本原因，将有问题的流汇集在一起，并创建分析系统。

sion、报告异常并提供跨网络多个段的图形可视化。有关更多信息，请参阅第 9 章[多段分析](#)。

## 系统要求

Omnipeek 的系统要求是：

- Windows 11、Windows 10、Windows 8.1 64 位、Windows 7 64 位、Windows Server 2019、Windows Server 2016、Windows Server 2012、Windows Server 2012 R2、Windows Server 2008 R2 64 位

**笔记** 对于 Windows 7 和 Windows Server 2008 R2，运行 Omnipeek 需要 SHA-2 代码签名。通常，对于使用 Microsoft Update 自动更新的用户，此功能会自动安装；否则，您需要手动安装 SHA-2 更新。请参阅 Microsoft [KB3033929](#)。

只要满足运行所支持操作系统的基本系统要求，Omnipeek 便支持大多数机架式、台式和便携式计算机。根据流量和 Omnipeek 的特定用途，要求可能会高得多。

建议为 Omnipeek 使用以下系统：

- Intel Core i3 或更高版本的处理器
- 4 GB 内存
- 40 GB 可用硬盘空间

有助于实现卓越性能的因素包括高速 CPU、CPU 数量、RAM 数量、高性能磁盘存储子系统 (RAID 0) 以及保存您计划管理的跟踪文件所需的尽可能多的额外硬盘空间。

支持的操作系统要求用户具有管理员级别权限才能加载和卸载设备驱动程序，或选择程序用于捕获数据包的网络适配器。有关更多信息，请访问我们的网站<https://www.liveaction.com/products/>。

## 支持的适配器和驱动程序

要分析 10 千兆位、千兆位或无线流量，Omnipeek 需要支持的网络分析器卡（例如 LiveAction 捕获适配器）或无线 LAN 适配器。有关网络适配器卡和驱动程序的最新信息，请访问<https://www.liveaction.com/products/>。

有关在 Omnipeek 和捕获引擎中配置无线通道和安全性以及千兆硬件配置文件的信息，请参阅[Omnipeek 用户指南](#)或在线帮助。

## 安装 Omnipeek

**要安装 Omnipeek：**

**1.**运行 Omnipeek 安装程序（例如，*Omnipeek\_xx.xxmsi*）。安装程序将删除所有以前版本的 Omnipeek。

**2.**按照屏幕上显示的安装说明进行操作。

安装过程中，系统会要求您输入有效的产品密钥。出现提示时，您可以从以下选项中进行选择：

- **自动的：**安装程序使用您的互联网连接向激活服务器发送加密消息，激活服务器检索并安装许可证文件。
- **手动的：**安装程序将引导您通过网页生成许可证文件。按照说明访问网页激活页面，填写所需信息，然后您将获得许可证文件。然后安装程序将引导您安装许可证文件。

有关产品激活过程的更多信息，请访问我们的网站：<https://www.liveaction.com/support/frequently-asked-questions/>。

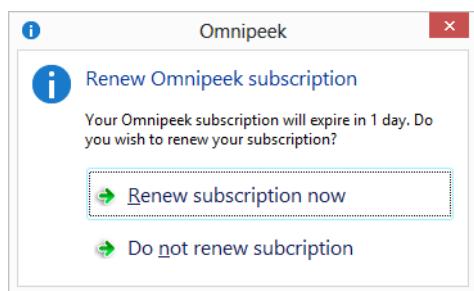
3. 安装程序完成安装程序文件后，您可以选择查看 **自述** 或启动该程序。

#### 笔记

默认情况下，Omnipeek 会安装 Capture Engine Manager。此应用程序允许您配置和更新单独购买的 Capture Engines 的设置。有关信息，请参阅 *Omnipeek 捕获引擎入门指南* 或 Capture Engine Manager 应用程序中的在线帮助。

## 续订或升级 Omnipeek 的订阅版本

如果您使用的是 Omnipeek 的订阅版本，当您的订阅距离到期至少还有 30 天时，无论何时启动 Omnipeek，系统都会提示您续订 Omnipeek 订阅，对话框类似如下：



- 点击 **立即续订** 打开 Omnipeek 激活对话框，您可以在其中更新现有许可证或更新到新许可证。
- 点击 **不续订** 继续使用 Omnipeek 直到您的订阅到期。

## 安装捕获引擎

有关如何安装、配置和更新 Capture Engines 软件和设置的完整说明，请参阅 *Omnipeek 捕获引擎入门指南* 它与捕获引擎一起提供。

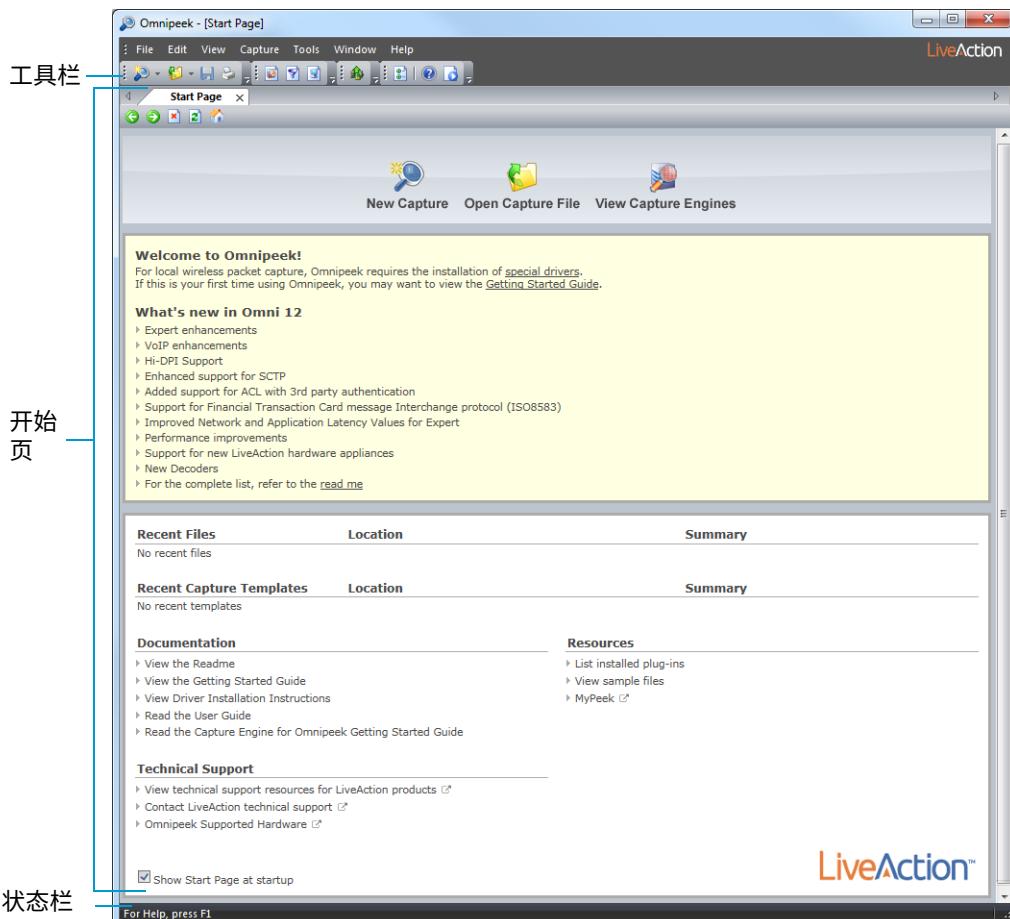
## 主程序窗口和开始页

**要启动 Omnipeek：**

- 在开始菜单，点击 **LiveAction Omnipeek**。

出现主程序窗口和开始页。

主程序窗口的各个部分如下所述。



- **工具栏**: 提供 Omnipacket 中常用任务的按钮。要显示不同的工具栏或自定义工具栏选项, 请在看法菜单, 点击工具栏。
- **开始页**: 提供用于创建新捕获、打开已保存的捕获文件以及查看捕获引擎窗口的按钮。此外, 开始页列出了 Omnipacket 版本中的“新功能”, 并提供了本地和在线有用资源的链接。
- **状态栏**: 在左侧显示简短的上下文相关消息, 在右侧显示当前监视器适配器。要切换状态栏的显示, 请在看法菜单, 点击状态栏。

# 使用 OmniPeek 与捕获引擎

如果您使用 OmniPeek 作为分布式捕获引擎的控制台，则需要从**捕捉引擎**窗口。（如果您仅将 OmniPeek 用作便携式网络分析仪，而不是用作分布式捕获引擎的控制台，则无需查看本节。）

捕获引擎可让您捕获和分析网络上任何位置的数据。捕获引擎通过 OmniPeek 控制台对来自一个或多个网络接口（包括以太网、802.11 a/b/g/n/ac 无线、1 千兆和 10 千兆）的流量执行实时网络分析。

这**捕捉引擎**OmniPeek 中的窗口让您可以查看和与没有自己的用户界面的捕获引擎进行交互。

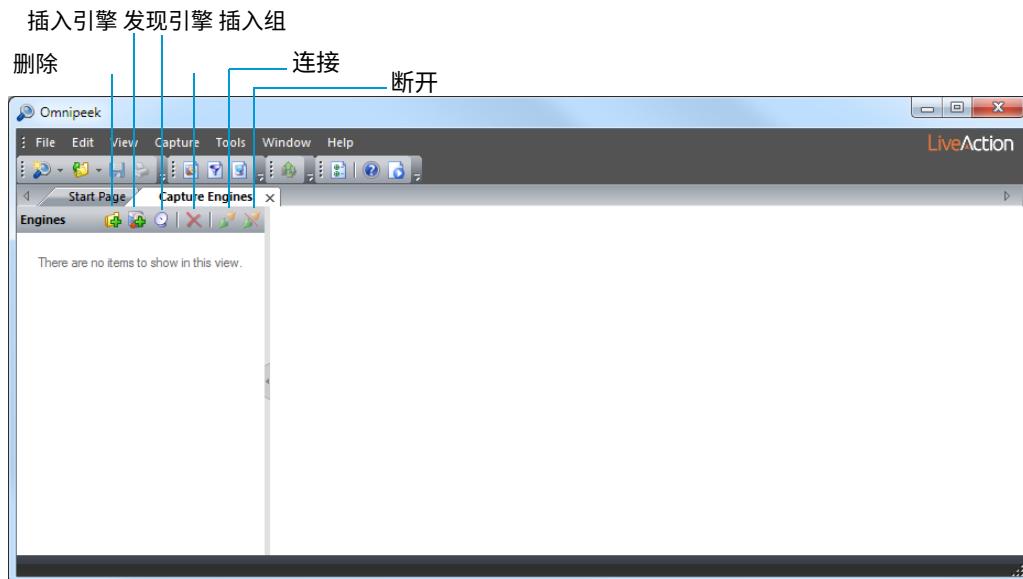
## 显示捕获引擎窗口

执行以下操作之一来显示捕获引擎窗口：

- 在开始页上，单击**查看捕获引擎**
- 在看法菜单，点击**捕捉引擎**

这**捕捉引擎**窗口出现。

**笔记** OmniPeek 和 Capture Engine Manager 都维护相同的捕获引擎列表。在任一程序中进行更改都会自动更新另一个程序中的列表。

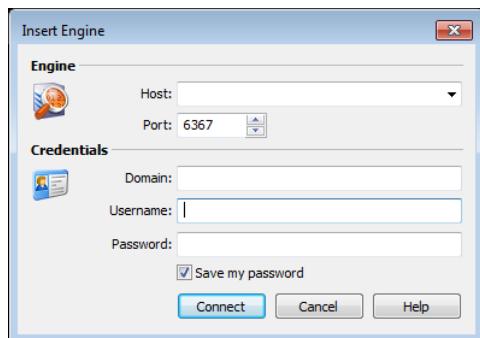


## 连接到捕获引擎

为了查看来自捕获引擎的数据包和数据，您必须首先从这**捕捉引擎**窗口。

## 要连接到捕获引擎：

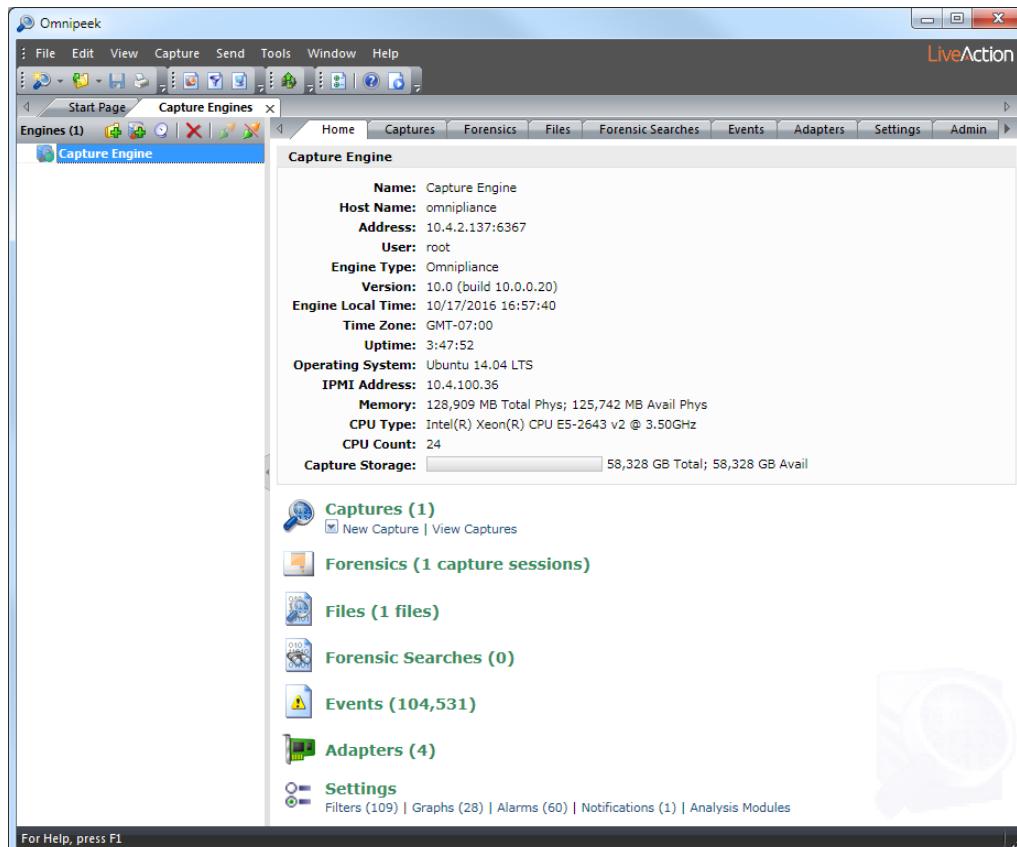
**1.**从捕捉引擎窗口，单击插入引擎。这插入引擎出现对话框。



**2.**完成对话框：

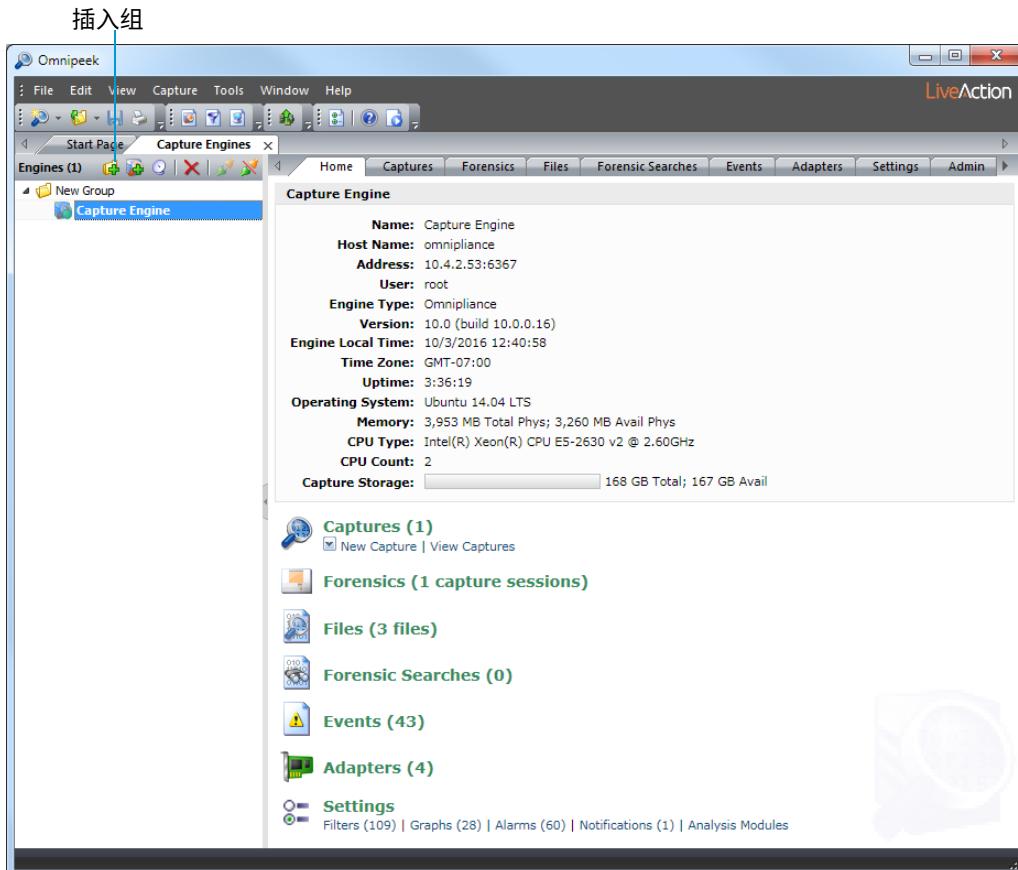
- **主持人**: 输入您想要连接的捕获引擎的 IP 地址。
- **港口**: 输入用于通信的 TCP/IP 端口。端口 6367 是 LiveAction 捕获引擎的默认端口。
- **领域**: 键入用于登录捕获引擎的域。如果捕获引擎不是任何域的成员，请将此字段留空。
- **用户名**: 键入登录捕获引擎的用户名。
- **密码**: 输入登录捕获引擎的密码。

**3.**点击连接。建立连接后，捕获引擎将出现在捕捉引擎窗户。



**提示**您可以添加多个引擎到捕捉引擎单击窗口插入引擎。

4. 点击插入组添加一组新的引擎到捕捉引擎窗口。出现一个新的群组文件夹。



5. 选择捕获引擎组文件夹并单击插入引擎将捕获引擎添加到组。

# 捕获窗口

捕获窗口是显示网络流量分析信息的主要界面。OmniPeek 可让您创建本地捕获的捕获窗口，以及从多个接口到无限数量的分布式捕获引擎的远程捕获窗口。

您可以创建多个可配置的捕获窗口，每个窗口都有自己选择的适配器和捕获设置。您一次可以打开的捕获窗口数量仅受可用系统资源数量的限制。

配置捕获窗口的捕获设置时，请记住窗口的捕获性能可能与您启用的捕获选项的数量和类型直接相关。例如，启用更多选项可能会为您提供更多数据，但代价是更有可能无法捕获所有数据。

决定捕获可以处理多少数据（以及多少个捕获选项）的因素取决于 OmniPeek 或 Capture Engine 计算机的系统内存和 CPU 能力、捕获的数据量和类型以及启用的捕获选项和分析模块的数量。启用捕获选项，例如 **捕获到磁盘**，**专家分析**，和**图表**；并启用分析模块，例如**VoIP 分析**比其他的消耗更多的机器资源。

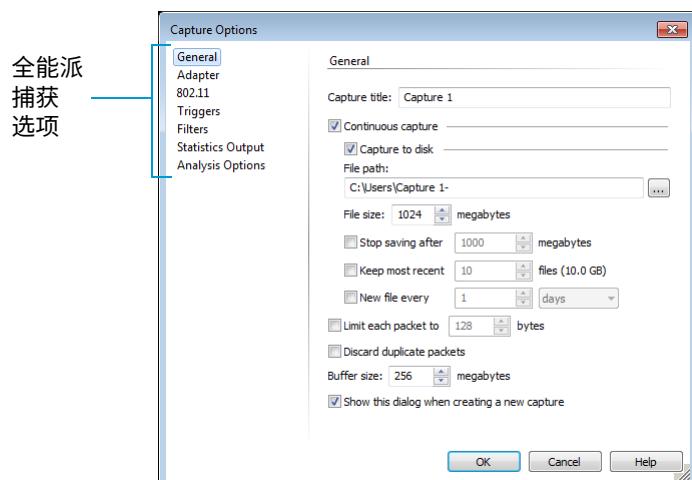
## 创建 OmniPeek 捕获

**要创建 OmniPeek 捕获：**

**1.** 执行以下操作之一来开始新的捕获：

- 点击**新捕获**在开始页上
- 在文件菜单，点击**新捕获…**

这一般的 OmniPeek 的选项**捕获选项**出现对话框。



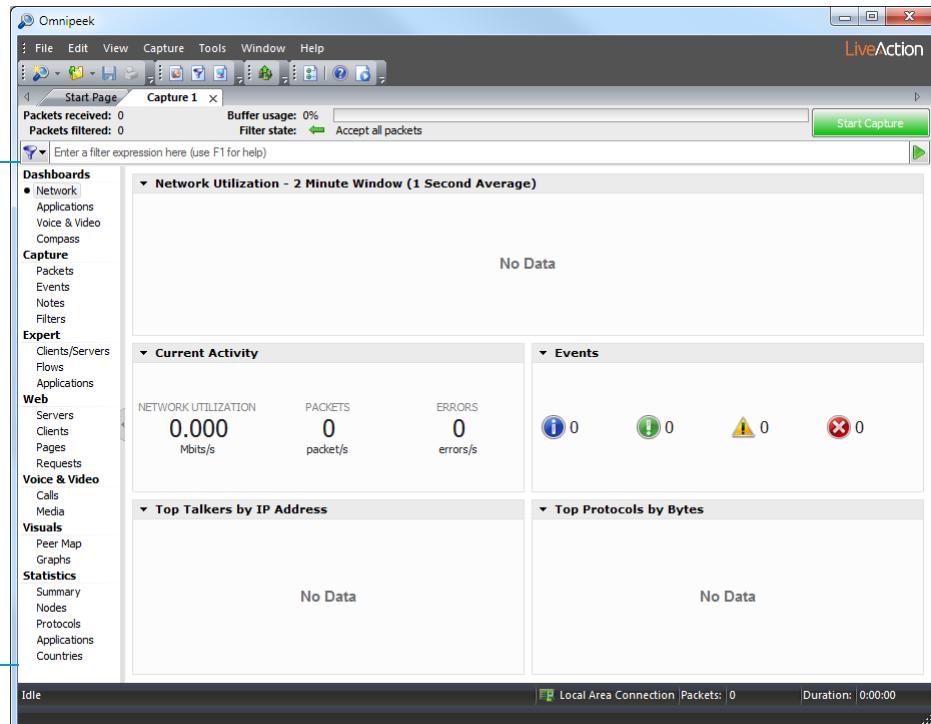
**2.** 配置一般的选项。

**3.** 在适配器选项。

**笔记** 点击帮助有关如何配置这些选项的详细信息，请参阅对话框中的 *OmniPeek 用户指南*或在线帮助。

#### 4.点击好的. 出现一个新的 OmniPeek 捕获窗口。

捕获  
窗户  
视图



5.点击开始捕捉开始捕获数据包。开始捕捉更改为停止捕获流量统计数据开始填充网络捕获窗口的仪表板。

6.单击导航栏中的捕获窗口视图可以查看捕获的数据包、数据的专家和统计分析、Peer Map 显示等。

7.点击停止捕获结束捕获。您可以选择保存、放弃或恢复捕获。

**提示** 要从上次中断的地方继续捕捉，请按住Alt键并单击开始捕捉。要清空捕获缓冲区并开始新的捕获，只需单击开始捕捉再次。

## 创建捕获引擎捕获

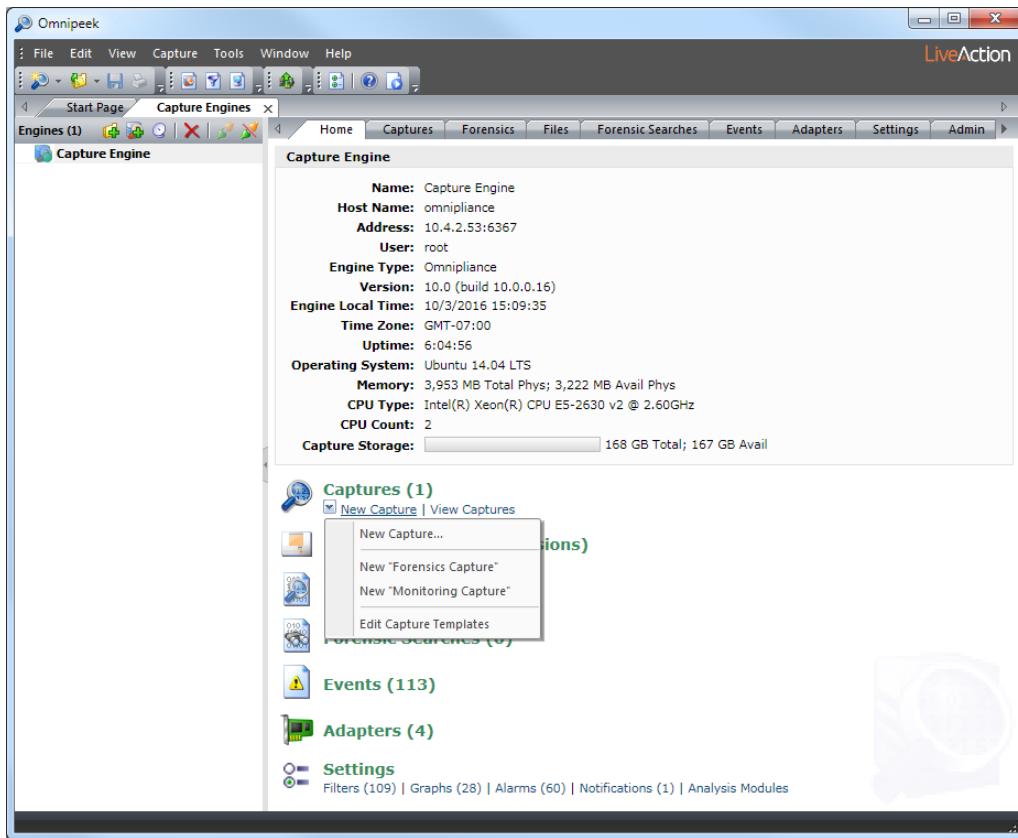
要创建捕获引擎捕获：

1.执行以下操作之一打开捕获引擎窗户：

- 在开始页上，单击查看捕获引擎
- 在看法菜单，点击捕获引擎

这捕获引擎窗口出现。

2.连接到捕获引擎。（要连接到捕获引擎，请参阅[连接到捕获引擎](#)在第 6 页。）家出现捕获引擎的选项卡。



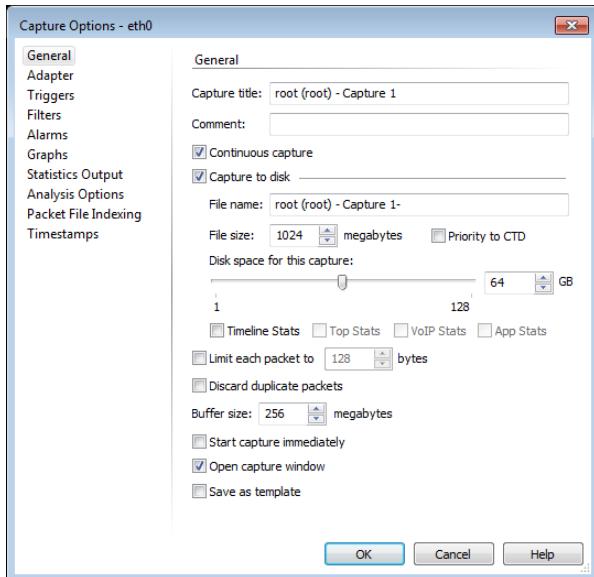
### 3. 从家选项卡，点击新捕获并选择您想要创建的捕获类型：

**笔记** 您还可以从以下选项中选择插入下拉列表可从 捕获选项卡，然后从新捕获可用的选项适配器选项卡。

- 新捕获…：此选项允许您根据您定义的捕获设置创建新的捕获引擎捕获。
- 新的“取证捕获”：此选项允许您根据为捕获后取证分析配置的取证捕获模板创建新的捕获引擎捕获。
- 新的“监控捕获”：此选项允许您根据配置的监控捕获模板创建新的捕获引擎捕获，以便在连续实时捕获中查看更高级别的专家和统计数据。
- 编辑捕获模板：此选项将打开捕获模板对话框并允许您创建新的或编辑现有的捕获模板。

这一般的捕获引擎的选项**捕获选项**出现对话框。

## 捕获引擎常规选项



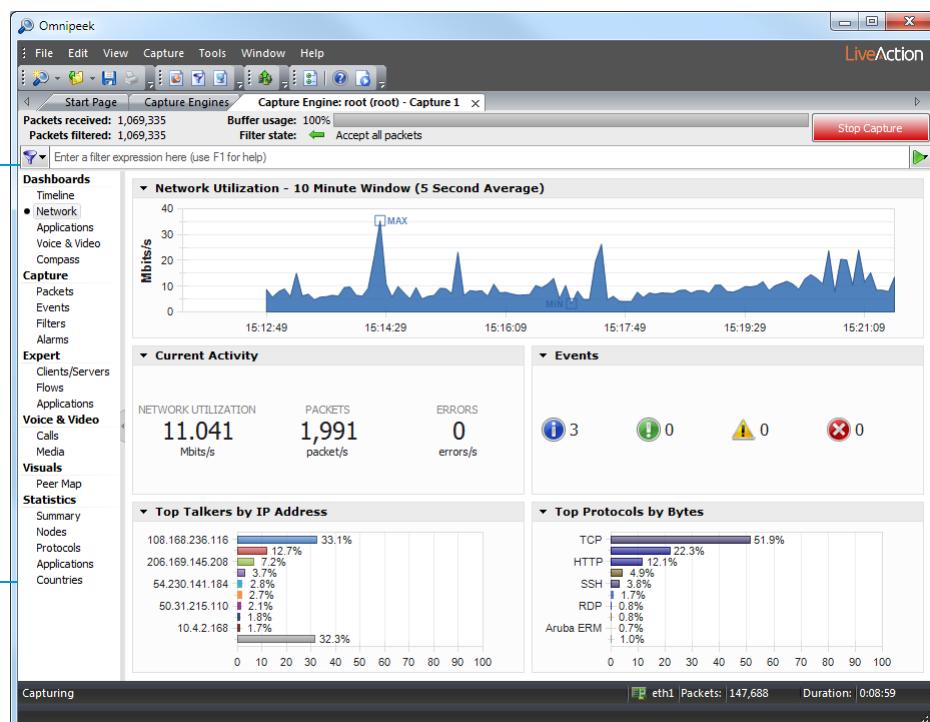
**4. 配置一般的选项。**

**5. 选择捕获适配器 适配器选项。**

**笔记** 点击帮助有关如何配置这些选项的详细信息，请参阅对话框中的 *OmniPeek 用户指南*或在线帮助。

**6. 点击好的. 出现一个新的捕获引擎捕获窗口。**

捕获  
窗口  
视图



**7. 点击开始捕捉开始捕获数据包。开始捕捉更改为停止捕获流量统计数据开始填充网络捕获窗口的仪表板。**

**8. 单击导航栏中的捕获窗口视图可以查看捕获的数据包、专家和数据的统计分析、Peer Map 显示等。**

## 9. 点击停止捕获

当您想要停止将数据包收集到捕获引擎捕获缓冲区时。

**笔记** 无权创建或修改 Capture Engine 捕获窗口的用户将发现功能呈灰色、缺失或收到错误消息，指示不允许执行该任务。有关详细信息，请参阅 *Omnipeek 捕获引擎入门指南*。

# 打开已保存的捕获文件

捕获文件或跟踪文件是保存为各种受支持的捕获文件格式的捕获窗口。您可以打开捕获文件以加载和处理数据包并将其重新放入全能派。

## Omnipeek 捕获文件

要打开 Omnipeek 捕获文件：

1. 执行以下操作之一：

- 在开始页上，单击打开捕获文件。这打开出现对话框。
- 在文件菜单，点击打开。这打开出现对话框。

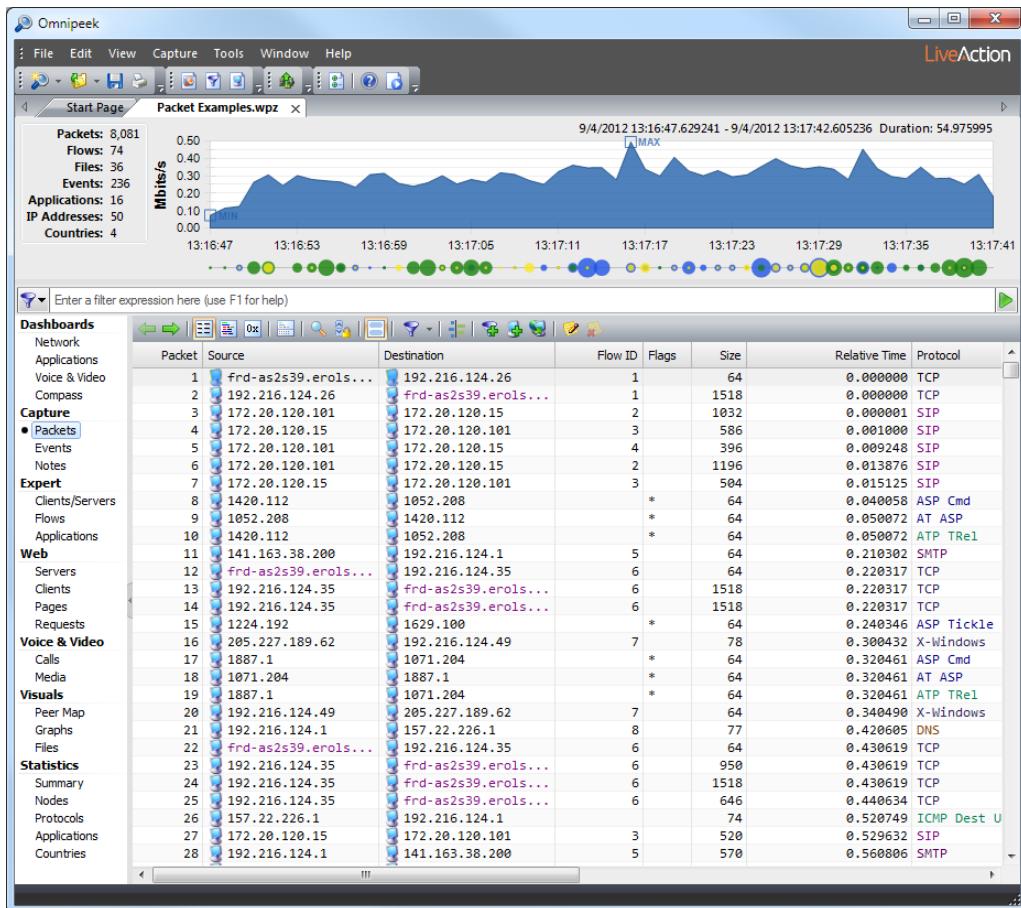
2. 选择捕获文件并单击打开。

**笔记** 打开大文件时，文件窗口状态栏中会出现一个进度条，显示数据包处理的进度。

**提示** 从打开对话框中，您可以点击筛选按钮打开筛选对话框，它允许您选择过滤器和分析选项以应用于您选择打开的每个文件。通过应用一个或多个过滤器，您可以大大减少要打开的数据量，只留下您感兴趣的数据。例如，如果您只想加载与特定 IP 地址匹配的文件中的数据包，您可以从对话框中创建一个简单的过滤器，然后在打开文件时选择该过滤器。

通过禁用分析选项，您可以释放系统资源，从而提高性能。这些分析选项通常显示在捕获窗口的导航窗格中。也可以从捕获菜单（在捕获

菜单，点击分析选项）。



### 3. 点击数据包导航窗格中的视图。

## 捕获文件的概览图

每当您在 OmniPeek 中打开捕获文件时，文件窗口顶部都会显示一个概览图。概览图允许您通过选择时间范围并重新处理所选时间范围内的所有统计数据来“放大”文件的一部分。然后，重新处理的统计数据将显示在文件窗口的下半部分。



概览图由三部分组成：

- **概览图：**概览图最初显示整个捕获文件的数据。单击图表内部并拖动所需的时间范围进行选择时，显示的数据包（以及这些数据包的分析）将限制在选定的时间范围内。可以拖动选择的开始和结束以扩大或缩小选择范围。此外，可以水平拖动选择，移动它同时保持持续时间不变。

- **活动时间表：**事件时间线是概览图下方的一条小线，用于直观显示捕获文件中事件的数量和严重性。它通过大小（点越大，该范围内的事件越多）和颜色（表示这些事件的严重性）来表示事件计数。您可以在概览图内右键单击以显示或隐藏事件时间线。
- **摘要信息：**概览图左侧的摘要信息显示捕获文件中的时间范围和各种计数（数据包、流、文件、事件、应用程序、IP 地址、国家）。  
当在概览图中做出选择时，摘要信息会更新并显示选择的计数以及整个捕获文件的总数。

---

**提示**您可以显示/隐藏概览图看法菜单：在看法菜单，点击概述。

---

在概览图内单击鼠标右键，会出现以下选项：

- **清除选择：**从概览图中删除任何选定的时间范围并显示整个捕获文件的数据。
- **网络利用率：**以网络利用率计数的形式显示概览图。
- **活动：**以事件计数形式显示概览图。
- **活动时间表：**显示或隐藏活动时间表从显示屏上。
- **柱子：**以柱状图形式显示概览图。
- **天际线：**将概览图显示为天际线图。
- **区域：**将概览图显示为面积图。
- **线：区域：**以折线图形式显示概览图。
- **线/点：**将概览图显示为线/点图。
- **线性 (Linear)：**以线性方式显示概览图。
- **对数：**以对数显示方式显示概览图。
- **显示最小值/最大值：**显示概览图的最小值和最大值。
- **同步事件：**根据当前事件集更新概览图活动看法。

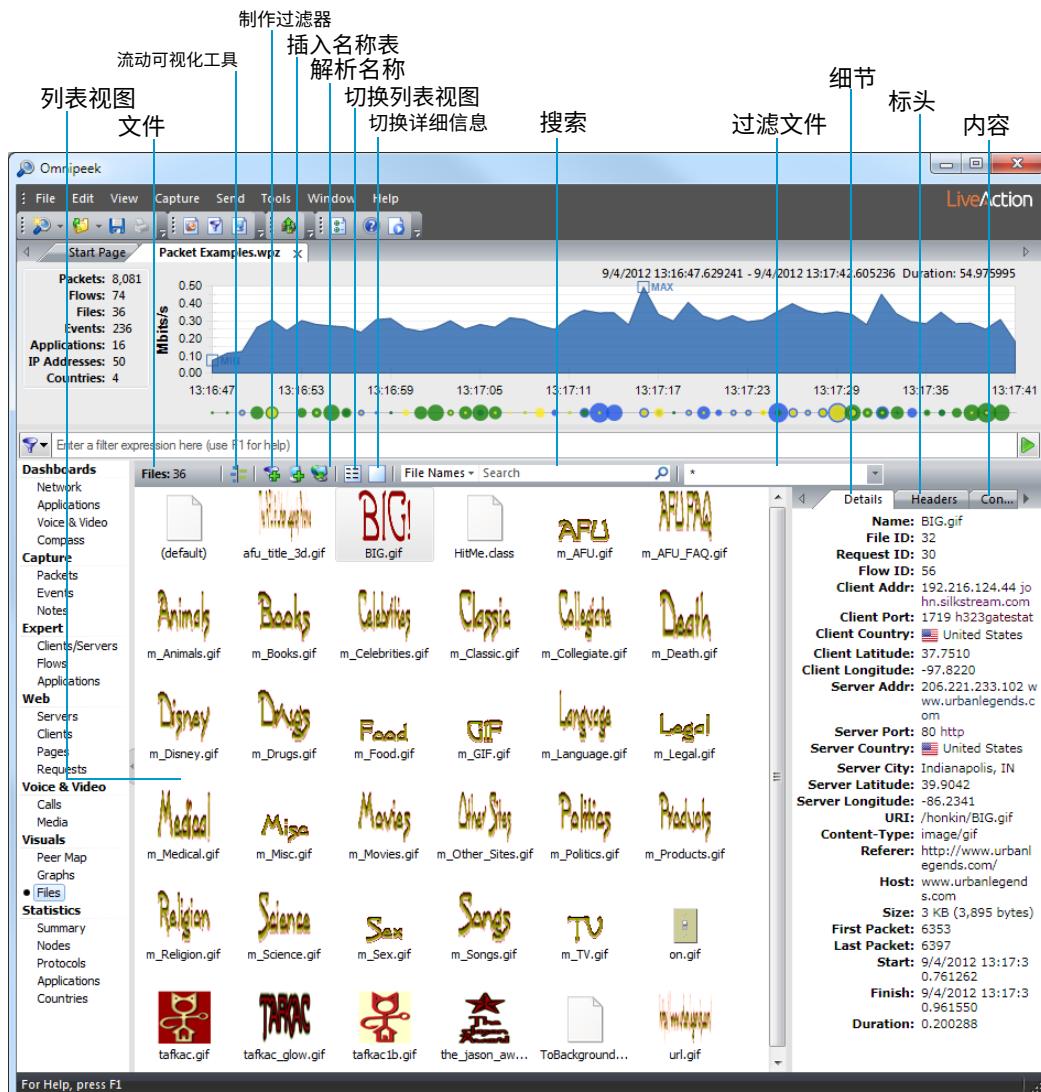
## 在文件视图中工作

这文件视图显示从 OmniPeek 中打开的捕获文件的重新组装 HTTP 负载中提取的文件。此视图可让您快速查看正在通过网络传播的文件。为了缩小搜索范围，您甚至可以根据文件的内容类型对其进行过滤。

---

**笔记**这文件捕获引擎不支持视图。

---



各部分文件视图如下所述。

- **文件:** 显示捕获文件中的文件总数。
- **列表视图:** 显示捕获文件中的文件。
- **流动可视化工具:** 在 Flow Visualizer 选项卡中打开选定的文件。
- **制作过滤器:** 打开插入过滤器对话框根据所选文件创建过滤器。
- **插入名称表:** 打开一个对话框，将所选文件的客户端和服务器节点地址添加到名称表中。
- **解析名称:** 检查 DNS 服务器中的名称以匹配所选文件的客户端和服务器地址。
- **切换列表视图:** 在以下选项之间切换列表视图：
  - **超大图标:** 将列表视图中的文件显示为小图标。图像显示为实际图像，而其他文件则显示与文件内容类型相对应的图标。在图标模式下将鼠标悬停在文件上会显示一个工具提示，其中显示了该文件的其他详细信息。
  - **大图标:** 将列表视图中的文件显示为大图标。图像显示为实际图像，而其他文件则显示与文件内容类型相对应的图标。在图标模式下将鼠标悬停在文件上会显示一个工具提示，其中显示文件的其他详细信息。

- **细节:** 将列表视图中的文件显示为包含多列的详细信息列表。您可以单击列标题以按该列对文件进行排序。您可以右键单击列标题以添加或删除列。您还可以在**细节**详细信息窗格的选项卡。
- **切换详细信息:** 切换详细信息窗格，使其显示在列表视图的下方或右侧（或完全隐藏）。您还可以通过拖动位于详细信息窗格和列表视图之间的调整大小控件来调整详细信息窗格的大小。详细信息窗格包含以下选项卡：
  - **细节:** 显示所选文件的各种信息。您也可以在列表视图中查看这些信息，方法是将列表视图切换到**细节**选项。要将此选项卡中的任何文本复制到剪贴板，请选择文本，右键单击，然后单击**复制**。
  - **标头:** 显示所选文件的请求和响应标头。要将此选项卡中的任何文本复制到剪贴板，请选择文本，右键单击，然后单击**复制**。
  - **内容:** 将文件内容显示为图像、文本或二进制数据。您可以在选项卡内单击鼠标右键，将显示模式更改为汽车，**图像**，**文本**，或者**二进制**。选择汽车将根据文件类型选择最佳模式。在**图像**模式中，在内容选项卡的顶部，一个小区域显示有关图像的信息（比例和颜色信息）。在**文本**模式中，有其他选项可以设置所使用的文本编码。在**二进制**模式中，还有其他选项可以更改数据和偏移的显示。要将此选项卡中的任何文本复制到剪贴板，请选择文本，右键单击，然后单击**复制**。
- **搜索:** 允许您在文件列表中搜索您在文本框中输入的文本字符串。您可以通过选择文本框左侧下拉列表中的选项来搜索文件名、请求/响应标头或文件内容。
- **过滤文件:** 允许您按内容类型过滤文件列表。下拉列表包含常见的内容类型（例如，**图像/\***，**文本/\***）。此外，您还可以输入任何内容类型（例如，**图片/png**）来按该内容类型过滤文件。这实质上充当了显示过滤器 — 仅显示指定类型的文件；不匹配的文件将被隐藏。

## 法医搜索

网络取证是对网络流量进行回顾性分析，目的是开展调查。您可以使用 Omnipacket 捕获、存储和挖掘大量流量数据，以便调查网络问题、安全攻击、人力资源政策违规等问题。

从采集引擎窗口，您可以从文件或者法医学连接的捕获引擎的选项卡。请参见[从“文件”选项卡进行取证搜索](#)第 18 页和[通过“取证”选项卡进行取证搜索](#)在第 21 页。

**笔记** 您还可以直接从“取证捕获”窗口执行取证分析。请参阅[从“取证捕获”窗口进行取证搜索](#)在第 27 页。

### 从“文件”选项卡进行取证搜索

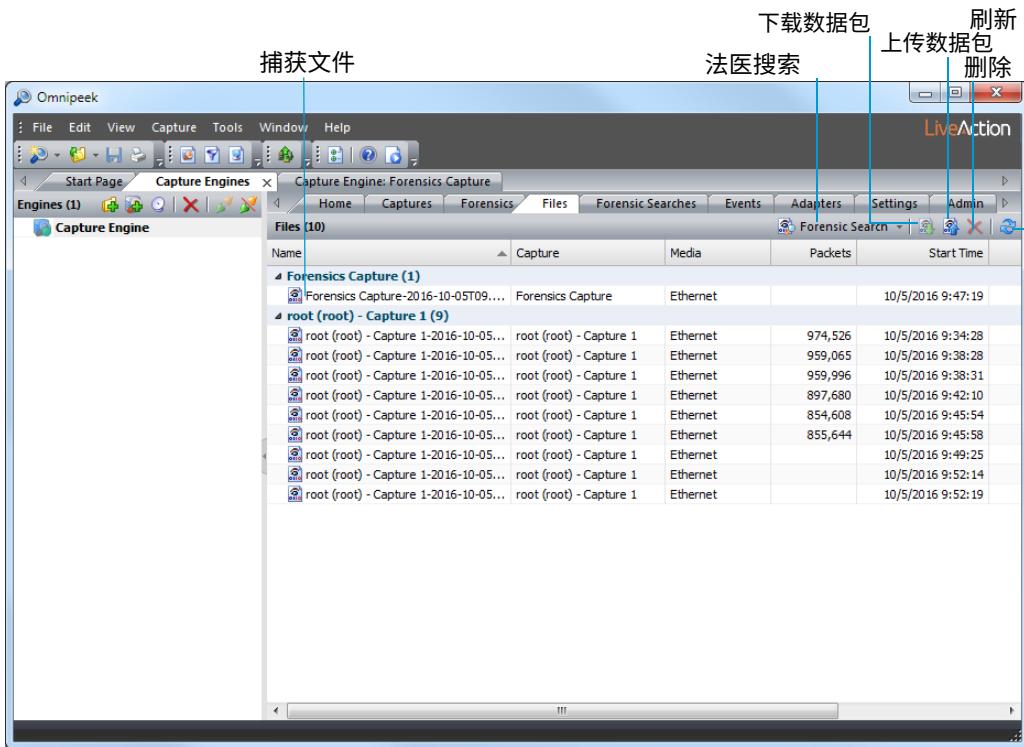
这文件选项卡中的捕捉引擎窗口显示保存到捕获引擎的所有捕获文件的列表。从文件选项卡可让您从一个或多个捕获引擎捕获文件中对数小时甚至数天的网络流量进行分类，以查找您希望进一步分析的特定数据。

**重要的！** 执行取证搜索之前，需要将一个或多个捕获文件保存到捕获引擎计算机。

**要从“文件”选项卡执行取证搜索：**

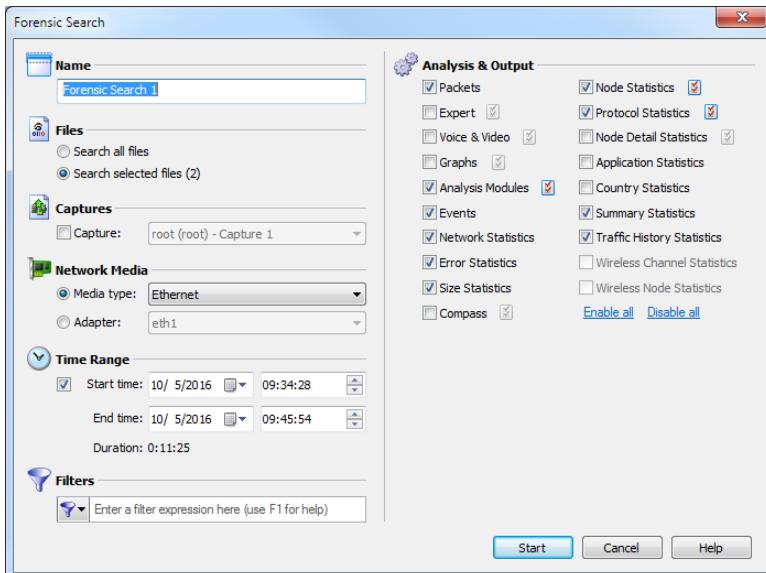
**1.** 从捕捉引擎窗口中，选择文件已连接捕获引擎的选项卡。

**提示** 在文件列表内单击鼠标右键，可以获得执行取证搜索、分组文件、上传和下载数据包、删除文件、将文件同步到硬盘上的文件系统以及刷新显示的附加选项。



2. 选择您想要搜索的一个或多个捕获文件。
3. 点击法医搜索（或点击旁边的小向下箭头法医搜索并选择您想要执行的取证搜索类型）。法医搜索出现对话框。

**笔记** 选择其中一种预定义的取证搜索类型将显示法医搜索与对话分析与输出为该类型的取证搜索预先配置的选项。您可以在单击之前更改任何选项开始。



4. 完成对话框以指定从选定的捕获文件中提取数据的标准：

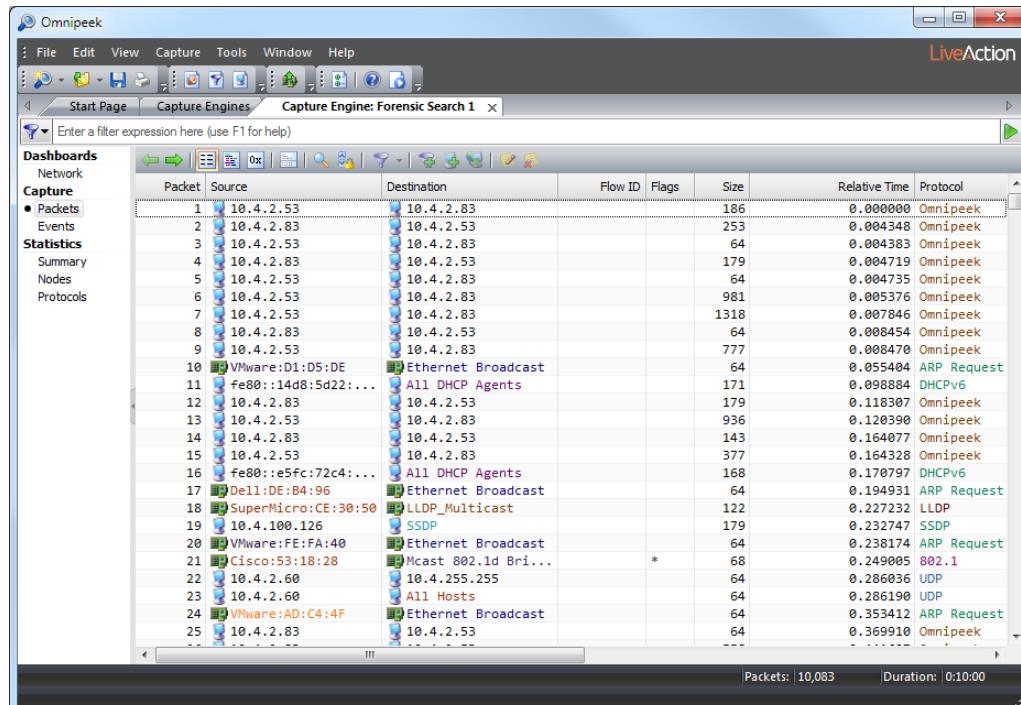
- 姓名：输入取证搜索的名称。
- 文件：选择下列选项之一：

- **搜索所有文件**: 选择此选项可搜索文件选项卡。
  - **搜索选定的文件**: 选择此选项可仅搜索文件选项卡。
  - **捕获**: 选择此选项，然后从“搜索”页的“捕获”列中列出的捕获中选择要搜索的捕获。文件选项卡。
  - **网络媒体**: 选择下列选项之一:
    - **媒体类型**: 选择此选项，然后选择媒体类型以仅提取特定媒体类型的数据。
    - **适配器**: 选择此选项，然后选择适配器以仅提取特定适配器捕获的数据。
  - **时间范围**: 选择此选项，然后配置提取数据的开始和结束时间。
    - **开始时间**: 设置提取数据的开始日期和时间。仅提取在开始时间和结束时间之间捕获的数据。
    - **结束时间**: 设置提取数据的结束日期和时间。仅提取开始时间和结束时间之间捕获的数据。
    - **期间**: 显示指定的开始时间与结束时间之间的时间量。
  - **筛选器**: 单击从显示列表中选择一个过滤器。如果取证搜索未应用任何过滤器，则所有数据包都将被接受。
- 要创建高级过滤器，请点击**筛选器**并选择**插入过滤器**，**插入运算符**，或者**插入表达式**从显示屏上。
- **分析与输出**: 选择一个或多个选项以在新视图中启用并显示该特定视图法医搜索窗口。对于各种分析与输出具有其他可配置设置的选项，请单击选项右侧的子菜单。

## 5. 点击开始.

一个新的法医搜索窗口顶部会出现两个进度条。（单击停止停止搜索，然后完成数据包的处理。

一旦数据包处理完毕，进度条就会消失，新的法医搜索窗口中会填充根据您上面选择的条件找到的数据。



6. 从新的法医搜索窗口，您可以通过执行在 *Omnipeek 用户指南*

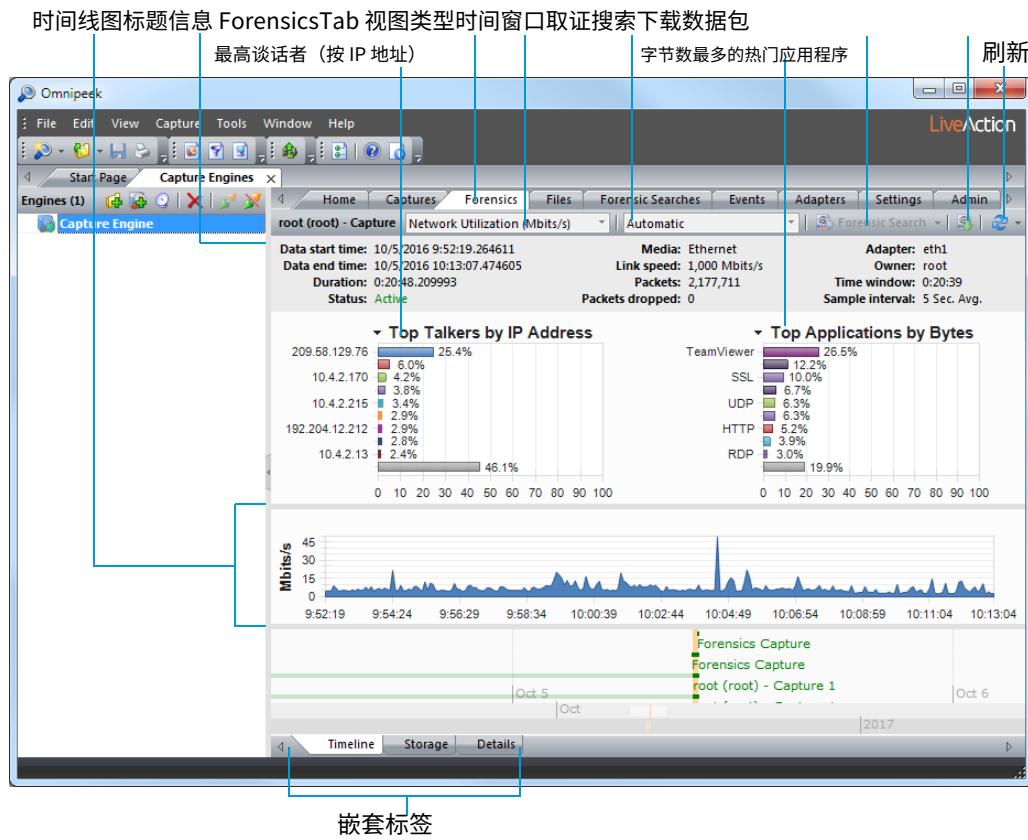
## 通过“取证”选项卡进行取证搜索

这法医学选项卡中的捕捉引擎窗口显示捕获引擎上可用的捕获会话。从法医学选项卡可让您选择其中一个捕获会话，在时间线图中显示其数据，然后对数据的特定部分执行取证搜索。

**重要的！** 您需要在捕获引擎上进行一次或多次取证捕获，然后才能从法医学选项卡。

**要从“取证”选项卡执行取证搜索：**

1. 从捕捉引擎窗口中，选择法医学连接的捕获引擎的选项卡。法医学选项卡显示当前可从捕获引擎的捕获存储空间获得的数据。



各部分法医学选项卡的描述如下：

- **标头信息：** 标头信息显示捕获会话的统计信息（数据开始时间、数据结束时间、持续时间、状态、数据包、丢弃的数据包、适配器等）。
- **最高谈话者 (按 IP 地址)：** 此显示显示了网络上最热门的“用量者”的图表，按以下时间线图中所选区域的节点细分。您可以在显示内单击鼠标右键，按以下方式显示最热门的用量者实际地址，IP 地址，或者 IPv6 地址；或选择一个酒吧或者馅饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含该节点其他详细信息的工具提示。
- **字节数最多的热门应用程序：** 此显示下方时间线图中所选区域的网络顶级应用程序图表。您可以在显示内右键单击以切换显示与顶级协议显示，或选择酒吧或者馅饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含应用程序其他详细信息的工具提示。

- **字节数最多的协议**: 此显示下方时间线图中所选区域的网络顶级协议图表。您可以在显示内右键单击以切换显示与顶级应用程序显示，或选择**酒吧**或者**馅饼**显示。将鼠标悬停在图表的条形图（或切片）上可查看包含协议其他详细信息的工具提示。
- **时间线图**: 时间线图表显示所捕获会话的数据。图表中一次只能显示一个捕获会话。默认情况下，图表以 Mbits/s 为单位显示网络利用率，但也可以绘制其他统计信息，方法是选择**看法**类型。

以下是时间线图其他部分的描述：

- 在图表中单击鼠标右键可执行取证搜索（参见法医搜索下面），下载选定的数据包到捕获文件，刷新窗口，或选择不同的图形格式：**酒吧**，**堆叠条形图**、**天际线**、**区域**，**堆叠面积**、**线**，**线/点**，**线性 (Linear)**，和**对数**。此外，您还可以切换显示图表上每个系列的最小点和最大点。
- 将鼠标悬停在图表中的数据点上，可以查看显示时间戳和大小信息（例如时间和速率、时间和数据包大小等）的工具提示。
- 当屏幕上显示的数据量超过显示量时，图表下方会出现一个滚动条，让您可以查看图表中的不同时间点。（如果**时间窗口**设置为**自动**的，滚动条将永远不会出现。）
- 如果**时间窗口**设置为除**自动**的，图表下方会出现一个滚动条，允许您查看图表中的不同时间点。
- **视图类型**: 选择要在时间线图表中显示的统计信息类型。您可以选择：
  - 网络利用率 (Mbits/s)
  - 网络利用率 (数据包/秒)
  - 单播/多播/广播
  - 数据包大小
  - VLAN/MPLS
  - 协议 (Mbits/s)
  - 协议 (数据包/秒)
  - 通话质量
  - 呼叫与网络利用率
  - 无线数据包 (数据包/秒)
  - 无线重试 (数据包/秒)

**笔记** 显示统计信息**通话质量**或者**呼叫与网络利用率**视图类型，VoIP 统计数据首次创建捕获时必须选择该选项并配置一般的选项  
这捕获选项对话。

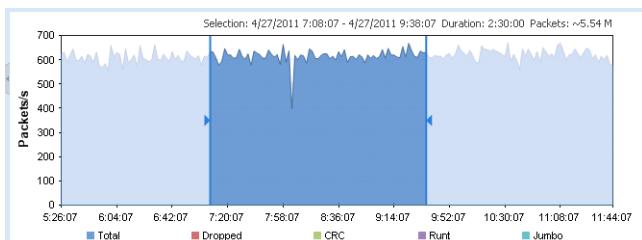
- **时间窗口**: 选择时间轴图中显示的时间间隔。默认情况下，**自动**根据可用数据选择显示最佳窗口。间隔从**5分钟 (平均 1 秒)**到**24 小时 (平均 5 分钟)**也可用。
- **法医搜索**: 单击显示法医搜索对话框中，您可以调整取证搜索设置。单击**法医搜索**显示执行取证搜索的自定义或预配置设置。您可以在单击之前更改任何选项开始：
  - **风俗**: 创建一个法医搜索根据您配置的自定义设置打开窗口。
  - **概述**: 创建一个法医搜索根据设置显示捕获会话中选择的数据概览的窗口。

- **数据包**: 创建一个法医搜索仅包含数据包视图的窗口。
- **专家**: 创建一个法医搜索根据优化的设置窗口 专家分析。
- **语音和视频**: 创建一个法医搜索根据优化的设置窗口 语音和视频分析。
- **下载数据包**: 单击可在选定的时间范围内下载选定捕获会话中的数据包。
- **刷新**: 单击可刷新屏幕。对于活动的捕获会话，您还可以通过从右侧的下拉列表中选择一个间隔来设置自动刷新间隔刷新。
- **嵌套标签**: 在法医学标签：时间线，贮存，和细节。每个选项卡都允许您查看和选择要以各种格式搜索的捕获数据。时间线，贮存，和细节下面详细描述了选项卡。

**2.**在任意嵌套选项卡中，单击（双击细节嵌套选项卡）中，选择要搜索的捕获会话。所选的捕获会话显示为橙色，表示已被选中，并且捕获会话的数据将加载到时间线图表位于顶部。

**重要的！** 一个会议表示从特定接口捕获数据包的连续时间段。每次开始捕获时都会创建一个会话。一次捕获可以有多个会话，每个会话可以由不活动时间段分隔。然后可以对每个会话进行取证分析。会议显示在法医学选项卡。

**3.**在时间轴图表中，拖动以选择要搜索的所选捕获区域。如果未选择图表的任何区域，则默认选择整个捕获。

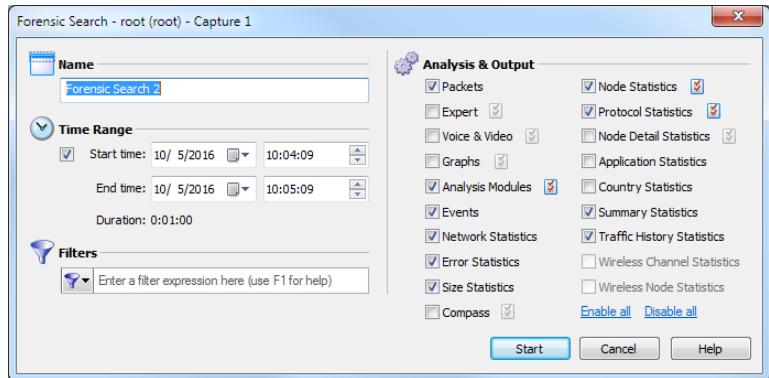


**笔记** 时间线图上方显示的数据包数量是当前选定的数据包的近似值。

**提示** 您可以从法医搜索对话。

**4.**点击法医搜索（或点击旁边的小向下滑头法医搜索并选择您想要执行的取证搜索类型）。法医搜索出现对话框。

**笔记** 选择其中一种预定义的取证搜索类型将显示法医搜索与对话分析与输出为该类型的取证搜索预先配置的选项。您可以在单击之前更改任何选项开始。



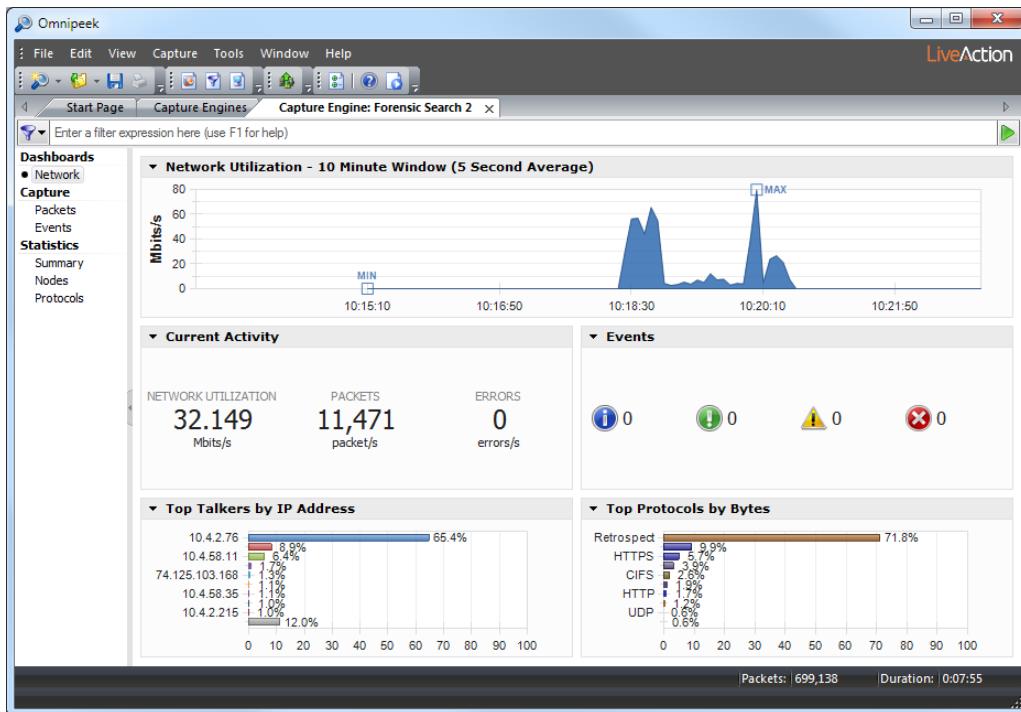
**5. 完成对话框以指定从所选捕获中提取数据的标准：**

**笔记** 如果您希望对处于活动状态且目前正在捕获数据包的捕获会话执行取证搜索，我们建议您先停止捕获，然后再执行取证搜索。如果您继续而不先停止捕获，请确保清除 **数据包** 复选框**法医搜索**单击前的对话框好的。

- **姓名：**输入取证搜索的名称。
  - **时间范围：**选择此选项，然后配置提取数据的开始和结束时间。
    - **开始时间：**设置提取数据的开始日期和时间。仅提取在开始时间和结束时间之间捕获的数据。
    - **结束时间：**设置提取数据的结束日期和时间。仅提取开始时间和结束时间之间捕获的数据。
    - **期间：**显示指定的开始时间与结束时间之间的时间量。
  - **筛选器：**单击从显示列表中选择一个过滤器。如果取证搜索未应用任何过滤器，则所有数据包都将被接受。
- 要创建高级过滤器，请点击**筛选器**并选择**插入过滤器**，**插入运算符**，或者**插入表达式**从显示屏上。
- **分析与输出：**选择一个或多个选项以在新视图中启用并显示该特定视图**法医搜索**窗口。对于各种分析与输出具有其他可配置设置的选项，请单击选项右侧的子菜单。

**6. 点击开始.**一个新的**法医搜索**窗口顶部会出现两个进度条。（单击**停止**停止搜索，然后完成数据包的处理。

一旦数据包处理完毕，进度条就会消失，新的**法医搜索**窗口中会填充根据您上面选择的条件找到的数据。



7. 从新的法医搜索窗口，您可以通过执行在 *OmniPeek 用户指南*。

## 时间轴嵌套选项卡

这时间线嵌套选项卡有三个时间轴带（日、月、年），用于显示捕获引擎存储空间中可用的捕获会话。您可以从日带中选择一个捕获会话，以在上面的时间轴图中显示该会话。



以下是使用时间轴嵌套选项卡：

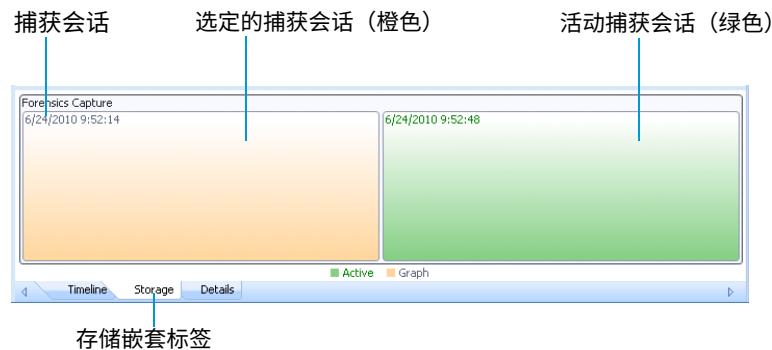
- 捕获会话用水平的绿色或蓝色条以及主父捕获的名称表示。只需单击捕获会话即可在上面的时间线图表中查看其数据。
- 一次只能选择并显示在时间线图中的一个捕获会话。
- 用橙色竖线突出显示的捕获会话表示当前已选中。带有绿色文本的捕获会话表示当前处于活动状态并正在捕获数据包。
- 如果捕获是作为“连续捕获”创建的，则捕获会话可能会被同一捕获中的另一个会话覆盖，并且会话在超出为捕获分配的磁盘空间后会“包装”。

如果捕获会话“结束”，水平绿条或蓝条会以较浅的颜色出现，表示捕获会话已被覆盖。被覆盖的任何数据都不再可供分析。

- 在时间线带内拖动可查看时间线带内的不同时间点。其他时间线带将相应移动。
- 在时间线带内单击鼠标右键，可快速移动到时间线内的各个点。您可以选择：
  - 转到当前**: 移动所有三个时间线带，以便当前选定的捕获会话位于显示的中心。
  - 前往现在**: 移动所有三个时间线带，使得当前时间位于显示屏的中心。
  - 转到最早**: 移动所有三个时间线带，以便最早可用的捕获会话位于显示屏的中心。
  - 转到最新**: 移动所有三个时间线带，以便最新可用的捕获会话位于显示的中心。

## 存储嵌套标签

这**存储嵌套**选项卡将捕获引擎存储空间中可用的每个捕获会话显示为嵌套在较大父容器中的容器。



以下是使用**存储嵌套**选项卡：

- 橙色的捕获会话表示当前已被选中。绿色的捕获会话表示当前处于活动状态并正在捕获数据包。
- 如果捕获是作为“连续捕获”创建的，并且会话在超出为捕获分配的磁盘空间后“结束”，则捕获会话可能会被同一捕获中的另一个会话覆盖。当捕获会话中的数据被新数据覆盖时，旧数据将不再可用于分析。
- 一次只能选择并显示在时间线图中的一个捕获会话。
- 将鼠标悬停在捕获会话容器上即可查看显示有关捕获会话详细信息的工具提示。
- 右键单击捕获会话以显示以下选项：
  - 看法**: 将选定的捕获会话加载到上面的时间线图中。
  - 删除捕获**: 从捕获引擎上的捕获存储空间中删除所选捕获及其所有捕获会话、数据包数据和统计信息。系统将提示您确认任何删除。只能从列表中删除父捕获，而不能删除单个捕获会话。
  - 删除所有捕获**: 从捕获引擎上的捕获存储空间中删除所有捕获、捕获会话、数据包数据和统计信息。系统将提示您确认任何删除。
  - 显示未保留空间**: 显示当前未用作捕获引擎的捕获存储空间的空间量。
  - 显示图例**: 显示捕获会话的颜色图例。

## 详细信息嵌套选项卡

这**细节嵌套选项卡**以表格形式显示捕获引擎存储空间中可用的捕获会话。每个捕获会话都显示在其主父捕获下。主父捕获是一个可折叠列表，可以展开或折叠以隐藏或显示其捕获会话。



迷你图       **详细信息嵌套选项卡**

以下是使用**细节嵌套选项卡**：

- 橙色的捕获会话表示当前已被选中。绿色的捕获会话表示当前处于活动状态并正在捕获数据包。
- 如果捕获是作为“连续捕获”创建的，并且会话在超出为捕获分配的磁盘空间后“结束”，则捕获会话可能会被同一捕获中的另一个会话覆盖。被覆盖的捕获会话不再可用于分析。
- 一次只能选择并显示在时间线图中的一个捕获会话。
- 右键单击列标题可显示或隐藏特定列。单击列标题可对其进行排序。
- 右键单击捕获会话或父捕获以显示以下选项：
  - **看法**: 将选定的捕获会话加载到上面的时间轴图中。只有捕获会话（而非父捕获）才可以加载到时间轴图中。
  - **删除捕获**: 从捕获引擎上的捕获存储空间中删除所选捕获及其所有捕获会话、数据包数据和统计信息。系统将提示您确认任何删除。只能从列表中删除父捕获，而不能删除单个捕获会话。
  - **删除所有捕获**: 从捕获引擎上的捕获存储空间中删除所有捕获、捕获会话、数据包数据和统计信息。系统将提示您确认任何删除。
  - **展开全部**: 展开列表，以便所有捕获会话都显示在父捕获下方。
  - **全部折叠**: 折叠列表，以便所有捕获会话都隐藏在父捕获下方。

## 从“取证捕获”窗口进行取证搜索

如果您创建了“取证捕获”窗口，则可以直接从捕获窗口执行取证搜索。取证搜索会创建新的法医搜索窗口。

**笔记** 您还可以从文件或者法医学标签。参见[从“文件”选项卡进行取证搜索](#)第 18 页和[通过“取证”选项卡进行取证搜索](#)在第 21 页。

要从“取证捕获”窗口执行取证搜索：

- 1.按照以下说明创建“取证捕获”窗口[创建捕获引擎捕获](#)在第 10 页。
- 2.点击时间线仪表板显示新的“取证捕获”窗口。



各部分时间线仪表板描述如下：

- **标头信息：** 标头信息显示捕获会话的统计信息（数据开始时间、数据结束时间、持续时间、状态、数据包、丢弃的数据包、适配器等）。
- **最高谈话者 (按 IP 地址)：** 此显示显示了网络上最热门的“谈话者”的图表，按以下时间线图中所选区域的节点细分。您可以在显示内右键单击以选择酒吧或者馅饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含该节点其他详细信息的工具提示。
- **字节数最多的热门应用程序：** 此显示下方时间线图中所选区域的网络顶级应用程序图表。您可以在显示内右键单击以切换显示与顶级协议显示，或选择酒吧或者馅饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含应用程序其他详细信息的工具提示。
- **字节数最多的协议：** 此显示下方时间线图中所选区域的网络顶级协议图表。您可以在显示内右键单击以切换显示与顶级应用程序显示，或选择酒吧或者馅饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含协议其他详细信息的工具提示。
- **时间线图：** 时间线图表显示捕获窗口的数据。默认情况下，图表以 Mbits/s 为单位显示利用率，但也可以绘制其他统计数据，方法是选择看法类型。

以下是时间线图其他部分的描述：

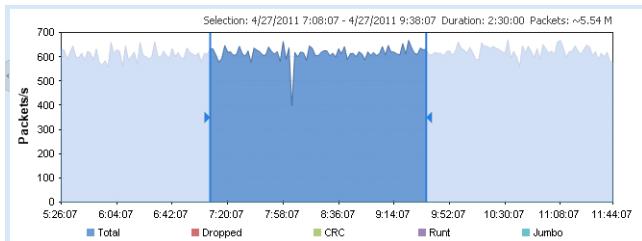
- 在图表中单击鼠标右键可执行取证搜索（参见法医搜索下面），下载选定的数据包到捕获文件，刷新窗口，或选择不同的图形格式：酒吧，堆叠条形图、天际线、区域，堆叠面积、线，线/点，线性 (Linear)，和对数。此外，您还可以切换显示图表上每个系列的最小点和最大点。
- 将鼠标悬停在图表中的数据点上，可以查看显示时间戳和大小信息（例如时间和速率、时间和数据包大小等）的工具提示。

- 当屏幕上显示的数据量超过显示量时，图表下方会出现一个滚动条，让您可以查看图表中的不同时间点。  
(如果时间窗口设置为 **自动的**，滚动条将永远不会出现。)
- 如果 **时间窗口** 设置为除 **自动的**，图表下方会出现一个滚动条，允许您查看图表中的不同时间点。
- 视图类型**: 选择要在时间线图表中显示的统计信息类型。您可以选择：
  - 网络利用率 (Mbps)**
  - 网络利用率 (数据包/秒)**
  - 单播/多播/广播**
  - 数据包大小**
  - VLAN/MPLS**
  - 协议 (Mbps)**
  - 协议 (数据包/秒)**
  - 通话质量**
  - 呼叫与网络利用率**
  - 无线数据包 (数据包/秒)**
  - 无线重试 (数据包/秒)**

**笔记** 显示统计信息 **通话质量** 和 **呼叫与网络利用率** 视图类型，**VoIP 统计数据** 在创建和配置捕获时必须选择选项一般的选项  
的捕获选项对话。

- 时间窗口**: 选择时间轴图中显示的时间间隔。默认情况下，**自动的** 根据可用数据选择显示最佳窗口。间隔从**5分钟 (平均 1 秒)** 到**24 小时 (平均 5 分钟)** 也可用。
- 法医搜索**: 单击显示法医搜索对话框中，您可以调整取证搜索设置。单击**法医搜索** 显示执行取证搜索的自定义或预配置设置。您可以在单击之前更改任何选项开始：
  - 风俗**: 创建一个法医搜索根据您配置的自定义设置打开窗口。
  - 概述**: 创建一个法医搜索根据设置显示捕获会话中选择的数据概览的窗口。
  - 数据包**: 创建一个法医搜索仅包含数据包视图的窗口。
  - 专家**: 创建一个法医搜索根据优化的设置窗口 **专家分析**。
  - 语音和视频**: 创建一个法医搜索根据优化的设置窗口 **语音和视频分析**。
- 下载数据包**: 点击下载所选时间范围内的数据包。
- 刷新**: 单击可刷新屏幕。对于活动的捕获会话，您还可以通过从右侧的下拉列表中选择一个间隔来设置自动刷新间隔刷新。

3. 在时间轴图表中，拖动以选择要搜索的捕获区域。如果未选择图表的任何区域，则默认选择整个捕获。

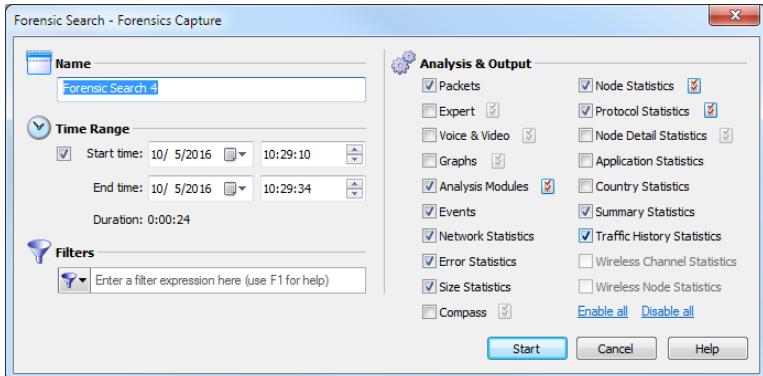


**笔记** 时间线图上方显示的数据包数量是当前选定的数据包的近似值。

**提示** 您可以从法医搜索对话。

#### 4. 点击法医搜索（或点击旁边的小向下滑头法医搜索并选择您想要执行的取证搜索类型）。法医搜索出现对话框。

**笔记** 选择其中一种预定义的取证搜索类型将显示法医搜索与对话分析与输出为该类型的取证搜索预先配置的选项。您可以在单击之前更改任何选项开始。

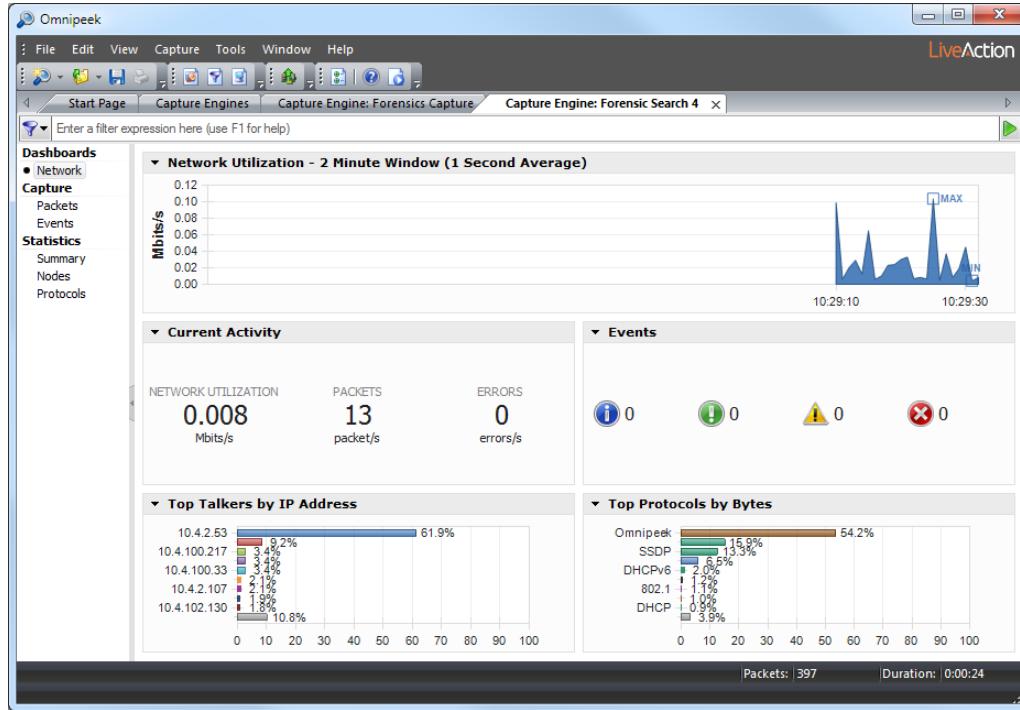


#### 5. 完成对话框以指定从所选捕获中提取数据的标准：

- **姓名：** 输入取证搜索的名称。
- **时间范围：** 选择此选项，然后配置提取数据的开始和结束时间。
  - **开始时间：** 设置提取数据的开始日期和时间。仅提取在开始时间和结束时间之间捕获的数据。
  - **结束时间：** 设置提取数据的结束日期和时间。仅提取开始时间和结束时间之间捕获的数据。
  - **期间：** 显示指定的开始时间与结束时间之间的时间量。
- **筛选器：** 单击从显示列表中选择一个过滤器。如果取证搜索未应用任何过滤器，则所有数据包都将被接受。  
要创建高级过滤器，请点击 **筛选器** 并选择 **插入过滤器**，**插入运算符**，或者 **插入表达式** 从显示屏上。
- **分析与输出：** 选择一个或多个选项以在新视图中启用并显示该特定视图法医搜索窗口。对于各种分析与输出具有其他可配置设置的选项，请单击选项右侧的子菜单。

**6. 点击开始.**一个新的法医搜索窗口顶部会出现两个进度条。（单击停止停止搜索，然后完成数据包的处理。）

一旦数据包处理完毕，进度条就会消失，新的法医搜索窗口中会填充根据您上面选择的条件找到的数据。  
法医搜索窗口将添加到当前活动的取证搜索列表中法医搜索选项卡。



**7. 从新的法医搜索窗口，您可以通过执行在 *OmniPeek 用户指南*。**

# 仪表板

Omnipeek 仪表板显示有关您的网络的图形数据，这些数据汇总为几个易于阅读的显示。Omnipeek 提供五个仪表板：时间轴、网络，应用，语音和视频，和罗盘。

## 时间线仪表板

这时间线仪表板可从具有以下任一功能的捕获引擎捕获窗口访问时间线统计选项中启用捕获选项对话框。仪表板显示捕获引擎的顶级通话者、顶级协议和网络利用率。



各部分时间线仪表板的描述如下。

- **标头信息：**标头信息显示捕获会话的统计信息（数据开始时间、数据结束时间、持续时间、状态、数据包、丢弃的数据包、适配器等）。
- **按IP地址划分的顶级谈话者：**此显示显示了网络上最热门的“谈话者”的图表，按节点细分。您可以在显示内单击鼠标右键，按以下方式显示最热门的谈话者：实际地址，IP地址，或者IPv6地址；或选择一个酒吧或者馅饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含该节点其他详细信息的工具提示。

- 字节数最多的热门应用程序：**此显示时间线图中所选区域的网络顶级应用程序图表。您可以在显示内右键单击以切换显示与顶级协议显示，或选择酒吧或者馅饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含应用程序其他详细信息的工具提示。
- 按字节数排名的顶级协议：**此显示显示了时间线图中所选区域的网络上的顶级协议图。您可以在显示内单击鼠标右键，以在显示与顶级应用程序显示之间切换，或者选择酒吧或者馅饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含协议其他详细信息的工具提示。
- 时间线图：**时间线图表显示所选捕获会话的数据。图表中一次只能显示一个捕获会话。默认情况下，图表以 Mbits/s 为单位显示网络利用率，但也可以绘制其他统计信息，方法是选择看法类型。

以下是时间线图其他部分的描述：

- 在图表内单击鼠标右键，执行取证搜索，将选定的数据包下载到捕获文件，刷新窗口，或选择不同的图表格式：酒吧，堆叠条形图、天际线、区域，堆叠面积、线，线/点，线性 (Linear)，和对数。此外，您还可以切换显示图表上每个系列的最小点和最大点。
- 将鼠标悬停在图表中的数据点上，可以查看显示时间戳和大小信息（例如时间和速率、时间和数据包大小等）的工具提示。
- 当屏幕上显示的数据量超过显示量时，图表下方会出现一个滚动条，让您可以查看图表中的不同时间点。  
(如果时间窗口设置为自动的，滚动条将永远不会出现。)
- 如果时间窗口设置为除自动的，图表下方会出现一个滚动条，允许您查看图表中的不同时间点。
- 视图类型：**选择要在时间线图表中显示的统计信息类型。您可以选择：
  - 网络利用率 (Mbits/s)
  - 网络利用率 (数据包/秒)
  - 单播/多播/广播
  - 数据包大小
  - VLAN/MPLS
  - 协议 (Mbits/s)
  - 协议 (数据包/秒)
  - 应用程序 (Mbits/s)
  - 应用程序 (数据包/秒)
  - 通话质量
  - 呼叫与网络利用率
  - 无线数据包 (数据包/秒) (OmniPeek 捕获引擎 (仅限 Windows))
  - 无线重试 (数据包/秒) (OmniPeek 捕获引擎 (仅限 Windows))

**笔记** 显示统计信息通话质量和呼叫与网络利用率视图类型，VoIP 统计数据首次创建捕获时必须选择该选项并配置一般的选项  
这捕获选项对话。

- 时间窗口：**选择时间轴图中显示的时间间隔。默认情况下，自动的根据可用数据选择显示最佳窗口。间隔从5分钟（平均1秒）到24小时（平均5分钟）也可用。

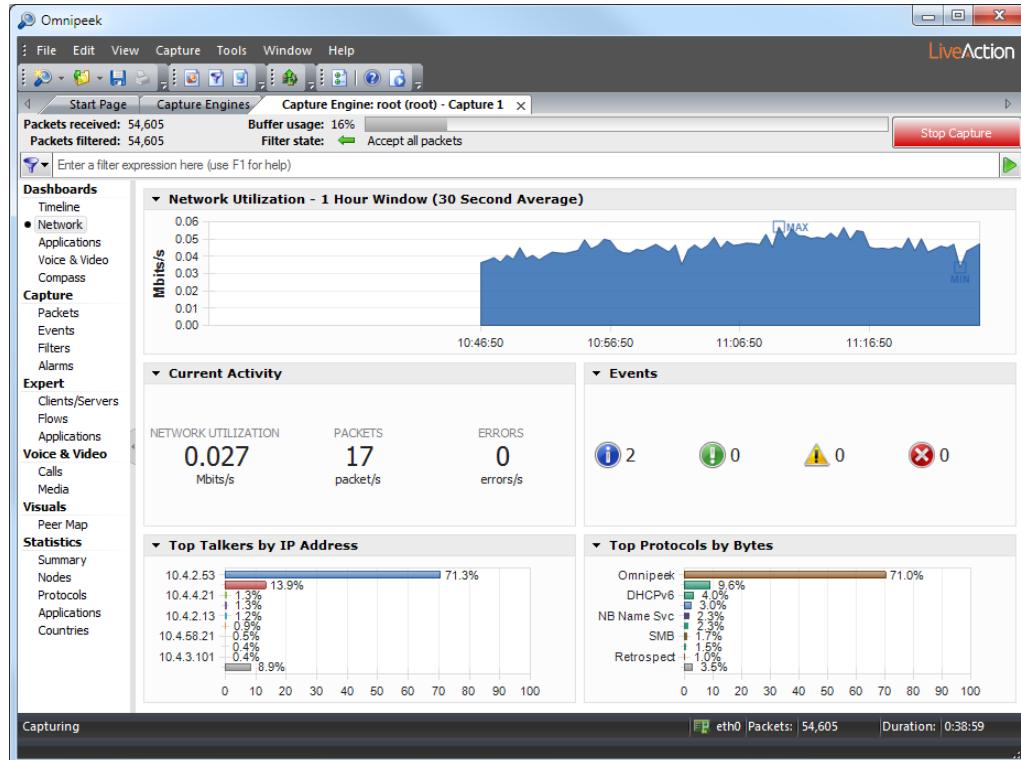
- **法医搜索：**单击显示法医搜索对话框中，您可以调整取证搜索设置。单击法医搜索显示执行取证搜索的自定义或预配置设置。您可以在单击之前更改任何选项好的：

**笔记** 配置时法医搜索对话框中，请记住，取证搜索性能与您启用的选项的数量和类型直接相关。

- **风俗：**创建一个法医搜索根据您配置的自定义设置打开窗口。
- **概述：**创建一个法医搜索根据设置显示捕获会话中选择的数据概览的窗口。
- **数据包：**创建一个法医搜索仅包含数据包视图的窗口。
- **专家：**创建一个法医搜索根据优化的设置窗口专家分析。
- **语音和视频：**创建一个法医搜索根据优化的设置窗口语音和视频分析。
- **下载数据包：**单击可在选定的时间范围内下载选定捕获会话中的数据包。
- **刷新：**单击可刷新屏幕。对于活动的捕获会话，您还可以通过从右侧的下拉列表中选择一个间隔来设置自动刷新间隔刷新。

## 网络仪表板

这网络仪表板显示捕获窗口的关键统计数据。



- **网络利用率：**此显示以 Mbits/秒为单位绘制网络流量图表。您可以在显示内单击鼠标右键以深入查看选定的数据包，或选择柱子，天际线、区域，线，或者线/点展示。

- 无线信号：**此显示以图表形式显示您正在捕获的无线信道或您已配置捕获以扫描的所有信道的无线信号和/或噪声强度（以百分比表示）。仅当选择无线适配器作为捕获适配器或用于无线捕获文件时，此显示才可用。您可以在显示内右键单击以选择要显示的参数。将鼠标悬停在信道上将显示带有其他信道信息的工具提示。
- 目前活动：**此显示内容显示网络利用率（占容量的百分比）、流量（以每秒数据包为单位）和错误率（每秒错误总数）。您可以在显示内容中单击鼠标右键，以数字或仪表形式显示值，或者选择自动的，光，黑暗的，或者干净的显示的背景主题。
- 事件：**此屏幕显示按严重程度生成的通知数量。您可以在屏幕内单击鼠标右键以选择自动，轻便，黑暗的，或者干净的显示的背景主题。单击严重性图标可导航至活动查看并显示与所点击的严重性相对应的事件。
- 按 IP 地址划分的顶级谈话者：**此显示显示了网络上最热门的“谈话者”的图表，按节点细分。您可以在显示内单击鼠标右键，按以下方式显示最热门的谈话者：实际地址，IP 地址，IPv6 地址，或者国家；或选择一个条形图、柱状图、饼图或者油炸圈饼显示。单击图表的条形图（或切片）将打开“详细统计信息”窗口，其中填充了所单击节点的详细信息。

**笔记** 根据监控捕获模板，此功能会自动为捕获引擎捕获启用。使用量最大的用户显示为无法使用使用 Forensic Capture 模板进行 Capture Engine 捕获。请参阅[在捕获引擎上进行取证捕获](#)在第 54 页和[监控捕获引擎上的捕获](#)在第 55 页。

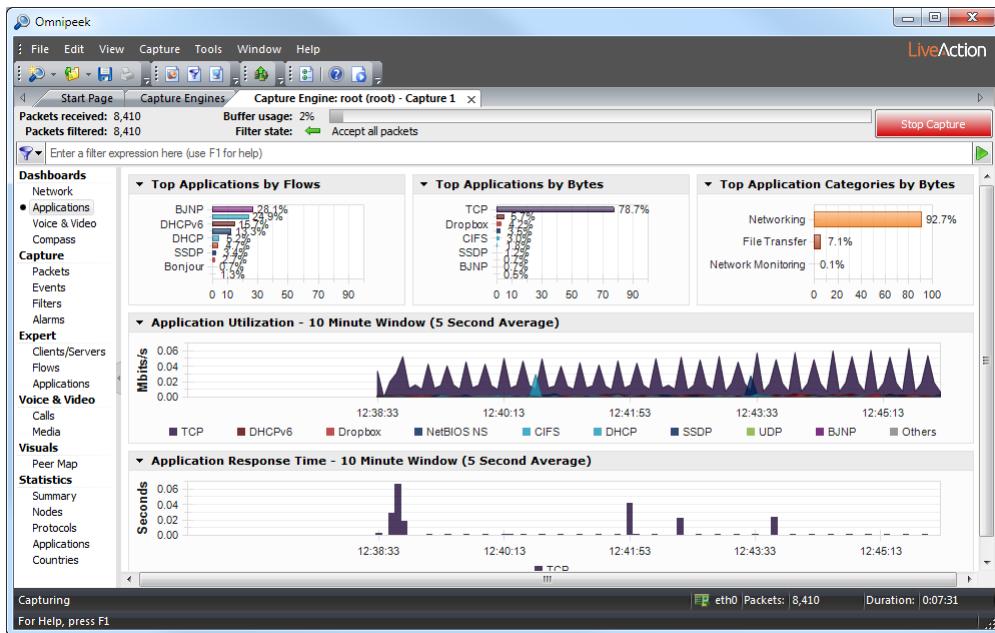
- 热门应用：**此屏幕显示网络上最热门的应用程序图表。您可以在屏幕内单击右键，切换显示顶级协议显示，或选择条形图、柱状图、饼图或者油炸圈饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含应用程序其他详细信息的工具提示。单击图表的条形图（或切片）可打开“详细统计信息”窗口，其中填充了所单击应用程序的详细信息。
- 主要协议：**此显示显示了网络上的主要协议的图表。您可以在显示内单击右键，以切换显示热门应用显示，或选择条形图、柱状图、饼图或者油炸圈饼显示。将鼠标悬停在图表的条形图（或切片）上可查看包含协议其他详细信息的工具提示。单击图表的条形图（或切片）可打开“详细统计信息”窗口，其中填充了所单击协议的详细信息。

**提示** 网络仪表板中的多个显示都支持工具提示。将鼠标悬停在显示上可查看包含其他信息的工具提示。

您还可以通过单击每个显示屏左上角的小箭头或右键单击每个显示屏内部来访问查看每个显示屏的其他选项。

## 应用程序仪表板

这**应用程序仪表板**在捕获窗口中显示应用程序的关键统计数据。此应用程序可见性可让您深入了解一天、一周、一个月或一年中特定时间的用户行为和网络流量模式。它可以帮助分析师更好地了解谁访问了哪些网站以及何时使用了哪些应用程序。



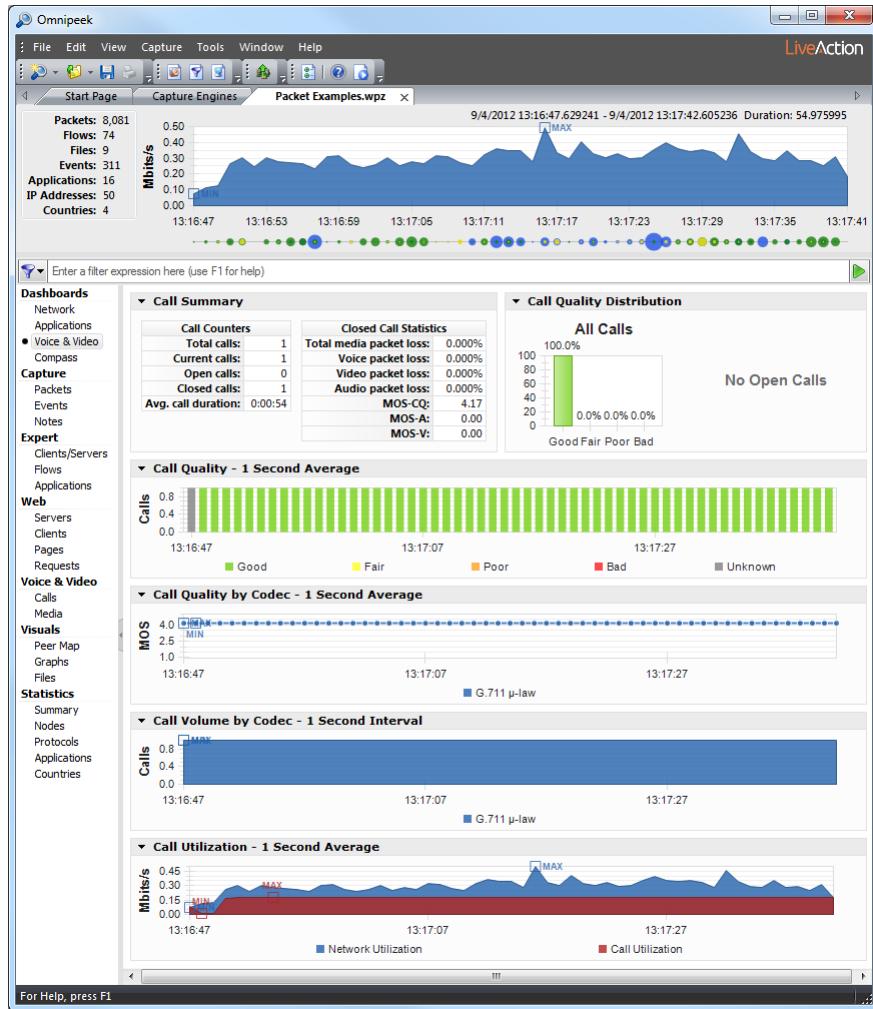
- 按流程分类的热门应用程序:** 此显示按流量计数显示排名靠前的应用程序的图表。单击此显示中的任何应用程序，您可以在 Expert 应用视图。您可以在显示内单击鼠标右键，选择条形图、柱状图、饼图或者油炸圈饼显示；选择自动缩放或者固定比例；或选择一个自动的，光，黑暗的，或者干净的显示的背景主题。
- 字节数最多的热门应用程序:** 此显示按字节数显示排名靠前的应用程序的图表。您可以在显示内单击鼠标右键，以切换显示字节数最多的协议显示；选择一个条形图、柱状图、饼图或者油炸圈饼显示；选择自动缩放或者固定比例；或选择一个自动的，光，黑暗的，或者干净的显示的背景主题。将鼠标悬停在图表的条形图（或切片）上可查看包含应用程序其他详细信息的工具提示。单击图表的条形图（或切片）可打开“详细统计信息”窗口，其中填充了所单击应用程序的详细信息。
- 按字节数排名的顶级协议:** 此显示以字节为单位显示顶级协议的图表。您可以在显示内单击鼠标右键，以切换显示字节数最多的热门应用程序显示；选择一个条形图、柱状图、饼图或者油炸圈饼显示；选择自动缩放或者固定比例；或选择一个自动的，光，黑暗的，或者干净的显示的背景主题。将鼠标悬停在图表的条形图（或切片）上可查看包含协议其他详细信息的工具提示。单击图表的条形图（或切片）可打开“详细统计信息”窗口，其中填充了所单击协议的详细信息。
- 按字节数排名的热门应用程序类别:** 此显示以字节为单位显示排名靠前的应用程序类别的图表。您可以在显示内右键单击以选择条形图、柱状图、饼图或者油炸圈饼显示；选择自动缩放或者 固定比例；或选择一个自动的，光，黑暗的，或者干净的显示的背景主题。将鼠标悬停在图表的条形图（或切片）上可查看带有应用程序类别其他详细信息的工具提示。
- 应用程序利用率:** 此屏幕按每秒位数显示排名靠前的应用程序。您可以在屏幕上单击鼠标右键以选择堆叠柱形图、天际线、堆叠天际线、面积，堆叠面积、线，或者线/点显示；选择是否显示线性 (Linear)或者对数；展示最小/最大值；或者选择一个自动的，光，黑暗的，或者干净的显示的背景主题。您可以选择图表的某个区域，右键单击并选择选择数据包. 仅捕获缓冲区中可用的数据包才可供访问选择数据包。
- 应用程序响应时间:** 此屏幕按响应时间长短显示排名靠前的应用程序的响应时间。您可以在屏幕上单击鼠标右键以选择天际线、区域，线，线/点或者积分显示；选择是否显示线性 (Linear)或者对数；显示最小/最大值；或选择 自动的，光，黑暗的，或者干净的显示的背景主题。您可以选择图表的某个区域，右键单击并选择选择数据包. 仅捕获缓冲区中可用的数据包才可供 选择数据包。

**提示** 应用程序仪表板中的多个显示都支持工具提示。将鼠标悬停在显示上可查看包含其他信息的工具提示。

您还可以通过单击每个显示屏左上角的小箭头或右键单击每个显示屏内部来访问查看每个显示屏的其他选项。

## 语音和视频仪表板

这语音和视频仪表板以直观的方式显示语音和视频通话摘要，以及有用的图表和统计数据，以排除故障并分析语音和视频流量。



各部分语音和视频仪表板标识如下。

- 通话摘要：**此显示屏显示有关语音和视频数据包丢失的“呼叫计数器”信息和“已关闭呼叫统计”。此外，**通话摘要**显示最长通话时间这是达到最大呼叫限制的时间点。**最长通话时间**以红色文本显示，并将动态出现。您可以在显示内单击鼠标右键以选择自动的，光，黑暗的，或者干净的显示的背景主题。
- 通话质量分布：**此屏幕根据 MOS 分数按质量显示未结和已结呼叫。您可以在屏幕上单击右键以选择条形图、柱状图、饼图，或者油炸圈饼显示；或选择一个自动的，光，黑暗的，或者干净的显示的背景主题。

MOS 分数是针对每个媒体流单独计算的，每个通话的质量是其相关媒体流中最低的 MOS 分数。语音媒体使用 MOS-CQ 评分，视频媒体使用 MOS-V 评分，音频媒体使用 MOS-A 评分。

质量阈值如下：

- <2.6 = 差（显示为红色）
- >=2.6 至 <3.1 = 差（显示为橙色）
- >=3.1 至 <3.6 = 一般（显示为黄色）
- >=3.6 = 良好（显示为绿色）

由于我们无法获得这些呼叫的 MOS 值，因此显示中不包含使用不受支持的编解码器的媒体流。此外，显示反映了呼叫和媒体视图中存在的相同数据，因此受到 2000 个呼叫限制的影响。

- **通话质量：**此屏幕显示一段时间内的通话质量，分为好、一般、差、差和未知。您可以在屏幕上右键单击以选择堆叠柱形图、天际线、堆叠天际线、面积，堆叠面积、线，线/点，或者积分展示；显示出最小/最大值；或者选择一个自动的，光，黑暗的，或者干净的屏幕的背景主题。您还可以选择通话质量图形，右键单击并选择选择数据包。
- **通话质量（按编解码器）：**此显示显示了每个正在使用的编解码器的质量随时间变化的线形图。您可以在显示内右键单击以选择线、线/点，或者积分展示；显示出最小/最大值；或者选择一个自动的，光，黑暗的，或者干净的屏幕的背景主题。您还可以选择通话质量图形，右键单击并选择选择数据包。

质量测量采用 MOS 评分。语音媒体采用 MOS-CQ 评分，视频媒体采用 MOS-V 评分，音频媒体采用 MOS-A 评分。

某个时间段的质量应为该时间段内所有开放媒体流的 MOS 分数的平均值。此外，此图表将仅显示受支持的编解码器的 MOS 分数，因为不受支持的编解码器不提供 MOS 测量值。

- **各编解码器的通话音量：**此显示显示了语音和视频呼叫随时间变化的开放呼叫（每个编解码器）图表。此图表反映了来自呼叫和媒体视图，与仪表板中的其他图表不同，通话音量图表包含使用不支持的编解码器的通话数据。您可以在显示内右键单击以选择堆叠柱形图、天际线、堆叠天际线、面积，堆叠面积、线，线/点，或者积分展示；显示出最小/最大值；或者选择一个自动的，光，黑暗的，或者干净的屏幕的背景主题。您还可以选择通话音量图形，右键单击并选择选择数据包。
- **呼叫利用率：**此显示显示了总体网络利用率与 VoIP 协议网络利用率的比较图。您可以在显示内右键单击以选择天际线、区域，线，或者线/点显示；选择是否显示线性 (Linear) 或者对数；展示最小/最大值；或者选择一个自动的，光，黑暗的，或者干净的屏幕的背景主题。您还可以选择通话利用率图形，右键单击并选择选择数据包。

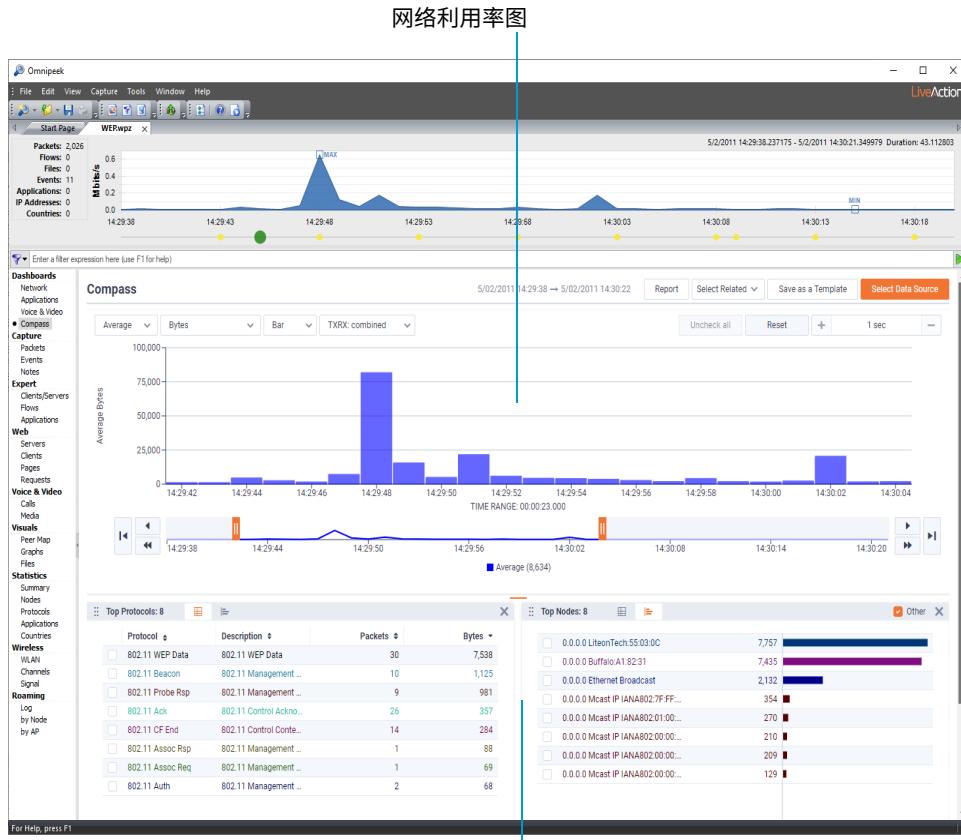
该图显示两个图例：网络利用率和通话利用率。利用率值以 Mbits/秒为单位显示。VoIP 利用率应为所有 VoIP 数据包（即信令、媒体 RTP/RTCP 和不支持的编解码器）的总利用率。

**提示** 语音和视频仪表板中的多个显示都支持工具提示。将鼠标悬停在显示上可查看包含其他信息的工具提示。

您还可以通过单击每个显示屏左上角的小箭头或右键单击每个显示屏内部来访问查看每个显示屏的其他选项。

## 指南针仪表板

这罗盘仪表板是一个交互式取证仪表板，可显示一段时间内的网络利用率，包括事件、协议、流量、节点、通道、WLAN、VLAN、数据速率、应用程序和国家/地区统计信息。这些统计信息显示在可选数据源小部件中，可以从实时捕获或单个受支持的捕获文件中查看。



数据源小部件

各部分罗盘仪表板的描述如下。

- 网络利用率图:** 显示两个交互式时间线图表，允许您选择并显示一系列数据。请参见[网络利用率图](#)在第39页。
- 数据源小部件:** 显示已启用的统计小部件（事件、协议、流量、节点、通道、WLAN、VLAN、数据速率、应用程序和国家/地区）。请参阅[网络利用率图](#)第39页和[数据源小部件](#)在第44页。

**提示** 您可以使用位于网络利用率图和数据源小部件之间的橙色水平分割器来调整显示大小。

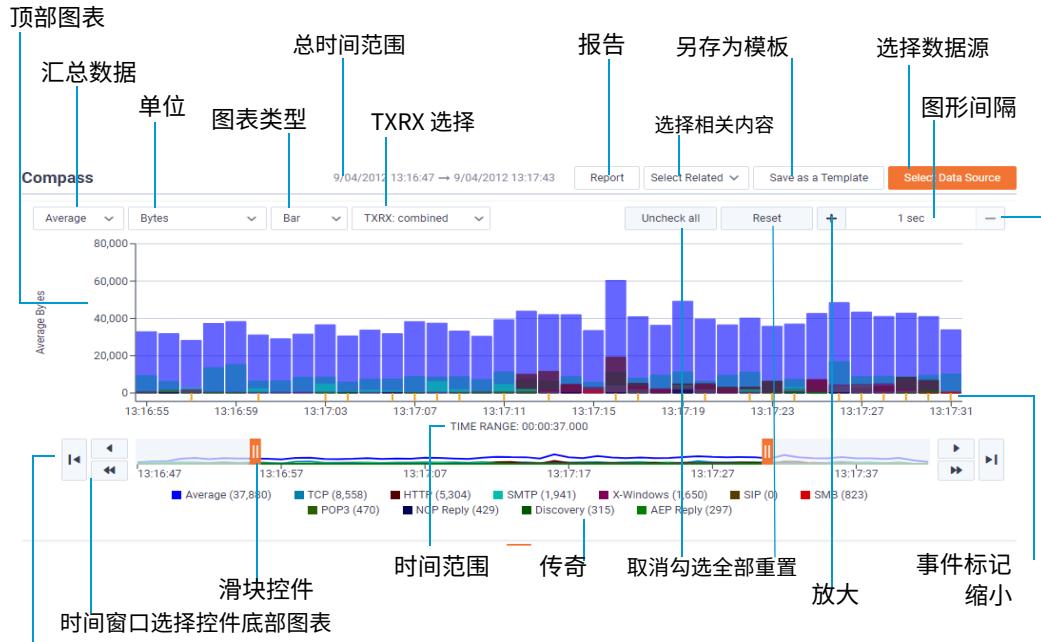
## 网络利用率图

网络利用率图表罗盘仪表板由两个交互式时间线图表组成，可让您查看特定感兴趣的区域。顶部（较大）图表显示选定时间范围内的利用率，而底部图表显示整个时间段的利用率。您需要在顶部图表中拖动并选择一个时间范围才能显示底部图表。

您可以使用以下方式放大或缩小所选时间范围，以便以毫秒、秒、分钟、小时或天为单位进行精确调整（最初，时间范围会根据需要显示的捕获大小进行相应调整）[放大和缩小控制](#)（实时捕获中不可用）。

当您更改所选的时间范围时，数据源小部件将相应更新以反映新的时间段。请参阅[指南针仪表板查看技巧](#)有关使用鼠标在网络利用率图表内导航的更多信息，请参见第 46 页。

**提示** 为了获得最佳效果，建议放大选定的时间范围，直到可以看到感兴趣区域的细节。



网络利用率图的各部分描述如下：

- **顶部图表：**以线、散点图、条形图或面积图的形式显示选定时间范围内的网络利用率。在图表内向左或向右拖动以选择并显示特定时间范围（您也可以使用底部图表选择时间范围）。然后，选定的数据会反映在底部图表中，也会反映在底部的数据源小部件中。
- **底部图表：**以线形图显示整个时间段内的网络利用率。如果顶部图表未完全选择，则底部图表始终显示；如果顶部图表完全选择，则底部图表始终隐藏。

使用滑块控件和时间窗口选择控件来选择特定的时间范围。所选时间范围内的数据随后会反映在顶部图表中以及底部的数据源小部件中。

- **总时间范围：**显示跟踪文件、捕获或取证搜索的总体时间范围，从开始日期和时间到停止日期和时间。
- **报告：**（仅限 OmniPeek）保存当前显示在罗盘仪表板转换为可以从浏览器窗口内部查看的 HTML 报告、多个 CSV 文件或 PDF 文件。
- **选择相关内容：**过滤与数据源小部件中所选项目相关的数据包以及当前在网络利用率图中选定的时间范围。使用“选择相关”时，您还需要在 AND 或 OR 过滤逻辑之间进行选择（在同一个数据源小部件中选择的多个项目将始终使用 OR 逻辑，因为 AND 逻辑将始终使整个表达式无效，但来自不同数据小部件的项目将使用选定的过滤逻辑）。另请参阅[选择相关数据包](#)在第47页。
- **另存为模板：**将当前 Compass 显示的内容保存为模板，以便可以与其他数据集一起使用。显示的窗口小部件的类型、窗口小部件的位置以及窗口小部件的大小都保留在模板中。您可以通过单击来选择已保存的模板[选择数据源](#)。

- **选择数据源:** 启用/禁用 Compass 仪表板内显示的数据源小部件。如果已保存任何 Compass 模板，您可以从此处选择它们。

每个数据源小部件都会在网络利用率图中显示适合所选数据源和所选时间范围的统计数据。小部件可以列表或条形图形形式查看。另请参阅 [数据源小部件](#) 在第44页。

可用的数据源小部件包括：

- 专家活动
- 协议
- 流程
- 节点
- 频道
- 无线局域网
- 虚拟局域网
- 数据速率
- 应用
- 国家

**笔记** 对于有线捕获，以下数据源小部件不可用：频道，无线局域网，和 数据速率。对于无线捕获，虚拟局域网数据源小部件不可用。

- **汇总数据:** 允许您将顶部和底部图表、数据源小部件和图例中的 Y 轴显示为平均值、总计或最大值的聚合：

- **平均的:** 在顶部和底部的图表中，绘制了每个时间间隔的平均值。在各种数据源小部件中，绘制了所选时间范围内统计数据的平均值。如果位，字节，兆位，千兆位，数据包，或者重传率是选定的单位类型，则平均计算结果将包括非值；否则，计算结果中不包括非值。位，字节，兆位，千兆位，数据包，信号强度%，噪音水平%，和 专家活动四舍五入到最接近的整数。
- **全部的:** 在顶部和底部的图表中，绘制了每个时间间隔的总值。在各种数据源小部件中，绘制了所选时间范围内的统计数据的总值。如果双向延迟，响应时间，信号强度%，信号强度 dBm，噪音水平%，噪音等级 dBm，信噪比，或者数据速率是选定的单位类型，那么全部的值不可用。
- **最大限度:** 在顶部和底部的图表中，绘制了每个时间间隔的最大值。在各种数据源小部件中，绘制了选定时间范围内统计数据的最大值。
- **单位:** 允许您在顶部和底部图表、数据源小部件和图例的 Y 轴中设置单位类型。根据数据包类型及其聚合方式，可用的单位类型包括：
  - 位. 以位为单位显示字节数。
  - 字节. 以字节为单位显示字节数。
  - 兆位. 以 Mbits 为单位显示字节数。
  - 千兆位. 显示以 Gbits 为单位的字节数。
  - 数据包. 显示数据包数。
  - 双向延迟. 显示双向延迟。双向延迟是来自客户端的请求和来自服务器的响应之间的时间差。

- **响应时间**。显示响应时间。响应时间是来自客户端的请求数据包与来自服务器的包含数据的响应数据包之间的时间差。
- **信号强度 % (仅限无线流量)**。显示无线数据传输的信号强度，以百分比表示。
- **信号强度 dBm (仅限无线流量)**。显示无线数据传输的信号强度，以 dBm (分贝毫瓦) 表示。
- **噪音水平 % (仅限无线流量)**。显示报告的无线数据传输噪声级别，以百分比表示。
- **噪音等级 dBm (仅限无线流量)**。显示报告的无线数据传输噪声级别，以 dBm (分贝毫瓦) 表示。
- **信噪比 (仅限无线流量)**。显示无线数据传输的信噪比 (SNR)。基本上，它是相对于背景噪声的信号强度的度量。
- **数据速率 (仅限无线流量)**。显示无线数据传输的数据速率。
- **重传率 (仅限无线流量)**。显示无线数据传输的重传率百分比。
- **专家活动**。显示专家事件的总数。只有“事件类型严重性”按钮已启用且在“专家事件数据源”窗口小部件中被选中的专家事件才会被计入计数。如果在“专家事件”视图中未选择任何专家事件，则将包括所有已启用“事件类型严重性”按钮的事件。

**笔记**

选择单位类型兆位或者千兆位，并选择总值平均的，将图表、数据源小部件和图例中的数据显示为图表平均值，而不是平均利用率 (位/秒)。要查看平均利用率 (位/秒)，点击概览查看统计数据在捕获窗口的导航窗格中，查看网络统计数据。

- **图表类型**：将顶部图表显示为折线图、散点图、条形图或面积图。
- **TXRX 选择**：启用或禁用所选统计信息（流量除外）的入站和出站利用率值图表。在图表视图和图例中，出站值显示的颜色比入站值略浅。双向延迟模式、响应时间模式和专家事件模式不提供入站和出站值。
- **取消全部**：单击以清除每个数据源小部件中所有选定项目的复选框。
- **重置**：单击可将网络利用率图重置为其原始状态，就像它已被完全选中一样。
- **放大**：对于选定的一定长度的时间范围，可以启用“放大” (+ 号)，允许您放大选定的时间范围，以便以毫秒、秒、分钟、小时和天为单位增加粒度。您可以将鼠标悬停在放大显示包含可放大的最大时间范围的工具提示。选择小于或等于该值的时间范围将启用放大。（另请参阅图形间隔以下）。

例如，如果图表以秒为单位，平均值为一秒，则可以放大到毫秒，平均值为特定的毫秒；或者，如果图表以小时为单位，则可以放大到分钟。有关特定时间的图表间隔的更多信息，请参阅下面的图表间隔表。实时捕获模式下无法使用放大功能。

- **缩小**：缩小 (- 号) 可让您退出之前的放大选择。实时拍摄模式下无法使用缩小功能。

- 图形间隔:** 图表间隔是图表中每个数据点的时间量，并根据所选时间范围的持续时间自动调整。图表间隔根据下图更新：

图形间隔	最大持续时间
1 毫秒	1800 毫秒
50 毫秒	1.5 分钟
250 毫秒	7.5 分钟
500 毫秒	15 分钟
1 秒	30 分钟
5 秒	2.5 小时
15 秒	7.5 小时
30 秒	15 小时
1 分钟	1 天 6 小时
5 分钟	6 天 6 小时
15 分钟	2 周 4 天 18 小时
30 分钟	5 周 2 天 12 小时
1 小时	10 周 5 天
6 小时	64 周 2 天
12 小时	128 周 4 天
1天	357 周 1 天
2 天	514 周 2 天
4天	1028 周 4 天
(双打) ...	(双打) ...

**笔记**

图形间隔图也适用于确定查看捕获文件时可以放大的最小和最大时间范围。另请参阅放大多于。

此外，毫秒图形间隔不是自动的，仅在放大期间发生，并且对于实时捕获无效。

- 事件标记:** 表示所选时间范围内触发的专家事件。事件标记以颜色编码，以反映专家事件数据源小部件中显示的专家事件严重性。
- 时间范围:** 顶部图表 X 轴下方的时间范围指示器表示当前选定时间范围的持续时间。使用箭头和滑块控件可调整选定的时间范围。
- 时间窗口选择控件:** 单箭头和双箭头选择控件允许您以一个单位增量（单箭头）或整个选择的增量（双箭头）向左或向右移动顶部和底部图表中选定的时间范围。带有线选择控件的单箭头允许您将顶部和底部图表中选定的时间范围一直向左或向右移动。
- 滑块控件:** 两个滑块控件可让您扩大和缩小顶部和底部图表中选定的时间范围。在实时捕获中，滑块控件的工作方式如下：

- 如果将左滑块和右滑块分别推到最左边和最右边，则新数据一经可用就会显示在右侧，而旧数据则保留在左侧。因此，所选时间范围的持续时间不断增加。
- 如果未将左滑块和右滑块分别推到最左侧和最右侧，则新数据在可用时不会显示在右侧，而旧数据仍保留在左侧。因此，所选时间范围的持续时间得以维持。
- 如果将左侧滑块推到最左边，但右侧滑块没有推到最右边，则新数据在可用时不会显示在右侧，而左侧的旧数据仍会保留。因此，所选时间范围的持续时间得以维持。
- 如果左侧滑块没有推到最左边，但右侧滑块被推到最右边，则新数据可用时会显示在右侧，而旧数据会从左侧移除。因此，所选时间范围的持续时间得以保持。

**提示** 您可以向左或向右拖动滑块控件之间的区域来选择顶部和底部图表的不同部分。

- 传奇：**显示图表项目的图例。图例中的值显示为总计、平均值或最大值，具体取决于在“汇总数据”下拉列表中选择的内容。单击图例中的颜色框可显示或隐藏图表中的条目。
- 暂停/播放（仅限实时捕捉）：**在实时更新和不更新图表之间切换。

## 数据源小部件

数据源小部件显示专家事件、协议、流量、节点、通道、WLAN、VLAN、数据速率、应用程序和国家/地区的统计数据。每个小部件都会在网络利用率图中显示与所选数据源和所选时间范围相应的统计数据。您可以在列表视图或条形图中显示这些小部件。

列表视图和条形图始终保持同步。在其中一个窗口小部件中启用某项将反映在所有其他窗口小部件中。以协议数据源窗口小部件为例，下面介绍数据源窗口小部件的各个部分。



- 夹持器**: 允许您将小部件拖到仪表板内的其他位置。
- 类型**: 显示数据源小部件的类型。
- 统计数据**: 显示选定时间范围内，在上限计数内的统计信息数量。
- 列表视图**: 以列表视图显示统计数据。
- 条形图**: 以条形图形式显示统计数据。
- 调整大小**: 拖动以调整数据源小部件的大小。
- 关闭**: 单击可从仪表板禁用该小部件。

## 列表视图

在列表视图中，会显示适合所选统计数据和单位的列。默认情况下，仅列出前 50 个项目。此限制可通过 Compass 选项对话框进行调整。

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 Messag...	1
POP3	Post Office Protocol - ...	1
RTCP	Real-Time Transport C...	1
X-Windows	X-Windows Server	1

在列表视图中，您可以：

- 单击列标题可按升序或降序排序。
- 使用复选框来启用或禁用网络利用率图表中特定统计数据的绘图。启用列表视图中的复选框可在顶部统计条形图中启用相同的统计数据。

## 条形图

统计数据条形图显示前 10 个统计数据，其他所有统计数据均归类为“其他”。



在条形图中，您可以：

- 单击条形图中的复选框可切换网络利用率图中统计数据的显示。此外，单击复选框（除其他的）在列表视图中选中相同统计数据的复选框。
- 将鼠标悬停在某个栏目上即可查看有关特定统计数据的详细信息。
- 选中或清除“其他”复选框以在条形图中显示或隐藏“其他”。

## 指南针仪表板查看技巧

以下是查看时的一些有用提示罗盘仪表板：

- 将鼠标悬停在专家事件标记上会在工具提示中显示以下事件细节：
  - 专家事件发生的图表点的日期和时间。
  - 专家事件类型列表，其中包含图表中该点的相关发生次数。
- 如果单位类型设置为专家活动：
  - 网络利用率图表和数据源小部件表示启用的专家事件严重性。
  - 如果在专家事件视图中未选择任何专家事件，则网络利用率图表将显示所有专家事件，并且数据源小部件将显示与任何专家事件相关的所有项目。
  - 如果在专家事件视图中选择了任何专家事件，则网络利用率图表将显示所选事件，而数据源小部件仅显示与所选专家事件相关的项目。
- 您一次最多只能选择 10 个统计项目的组合（在数据源小部件中）。
- 在统计列表视图中，您可以通过单击复选框列上方来对选定项目进行排序。这样，您可以将选定项目放在列表视图的顶部或底部。

## 指南针仪表板限制

查看 Compass 仪表板时存在一些限制：

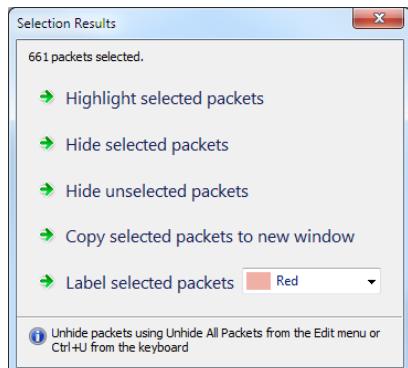
- Compass 仪表板每秒最多可统计 1,000,000 个统计项（协议、流量、节点、通道、WLAN、VLAN、数据速率、应用程序）。
- 对于实时捕获，Compass 仪表板仅显示最近 4 小时的数据。4 小时后，Compass 每隔 10 分钟会截取前 10 分钟的可用数据。此限制可通过 Compass 选项对话框进行调整。
- Compass 希望按升序接收数据包——如果收到的数据包的时间戳早于前一个数据包，则会被丢弃。
- 必须至少有 500MB 的可用磁盘空间，否则 Compass 将停止生成/保存统计信息，直到有足够的磁盘空间为止。

## 选择相关数据包

您可以使用“选择相关数据包”功能从数据源小部件和网络利用率图中过滤选定的项目。

### 选择相关数据包：

1. 从数据源小部件中选择一个或多个统计项，并调整网络利用率图中当前选择的时间范围。
2. 点击选择相关数据包并选择所需的 AND 或 OR 逻辑。与所选统计项匹配的数据包将被过滤并在数据包视图，以及评选结果出现对话框。



3. 点击突出显示选定的数据包，隐藏选定的数据包，隐藏未选定的数据包，将选定的数据包复制到新窗口，或者标记选定的数据包。

**笔记**根据协议选择数据包将包括协议层次结构中的子协议。

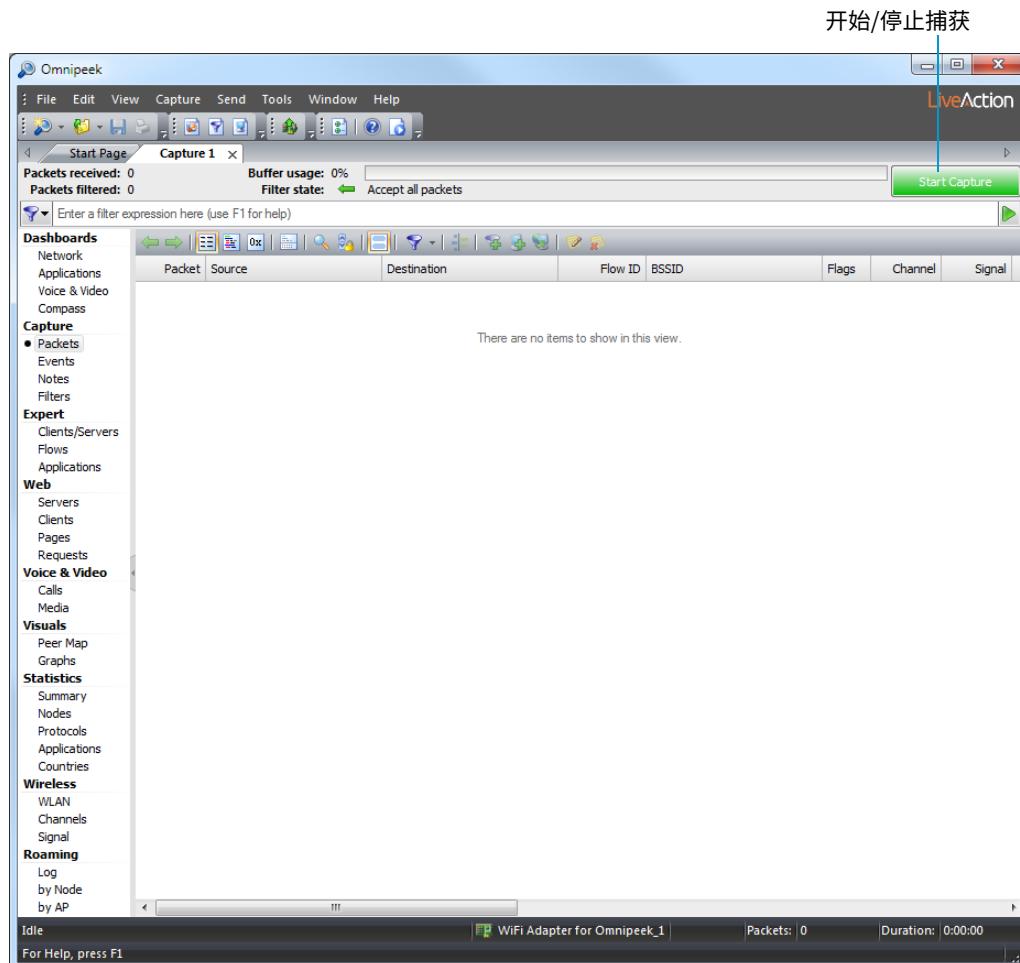
## 查看和解码数据包

数据包是网络上传输的数据单位，也是所有高级网络分析的基础。

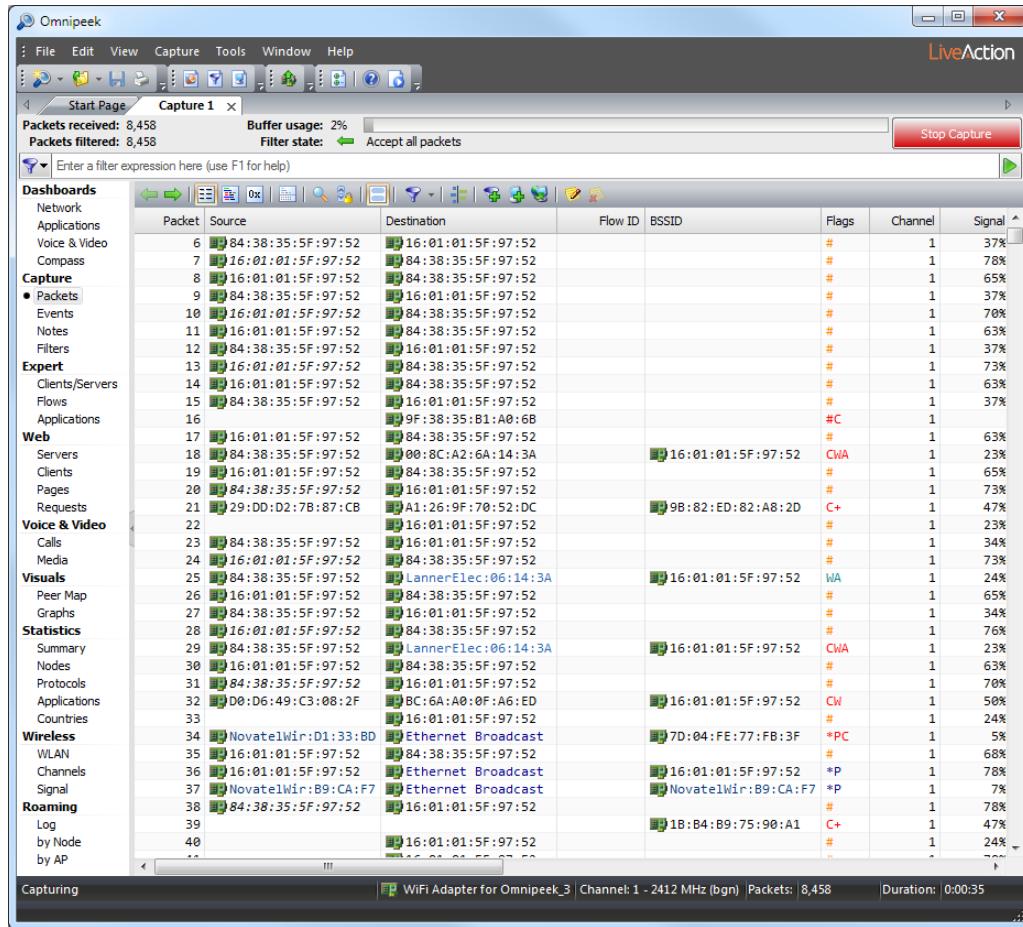
数据包捕获窗口视图是您可以查看网络上传输的各个数据包的信息的地方。捕获窗口还允许您以原始、十六进制和 ASCII 格式查看解码的数据包内容。

### 数据包视图

4. 打开捕获窗口并单击数据包看法。



5. 点击开始捕捉。数据包开始填充捕获窗口。



6. 右键单击列标题可以隐藏或显示可用的列标题。

7. 右键单击数据包行并选择插入名称表...。这插入名称出现对话框。

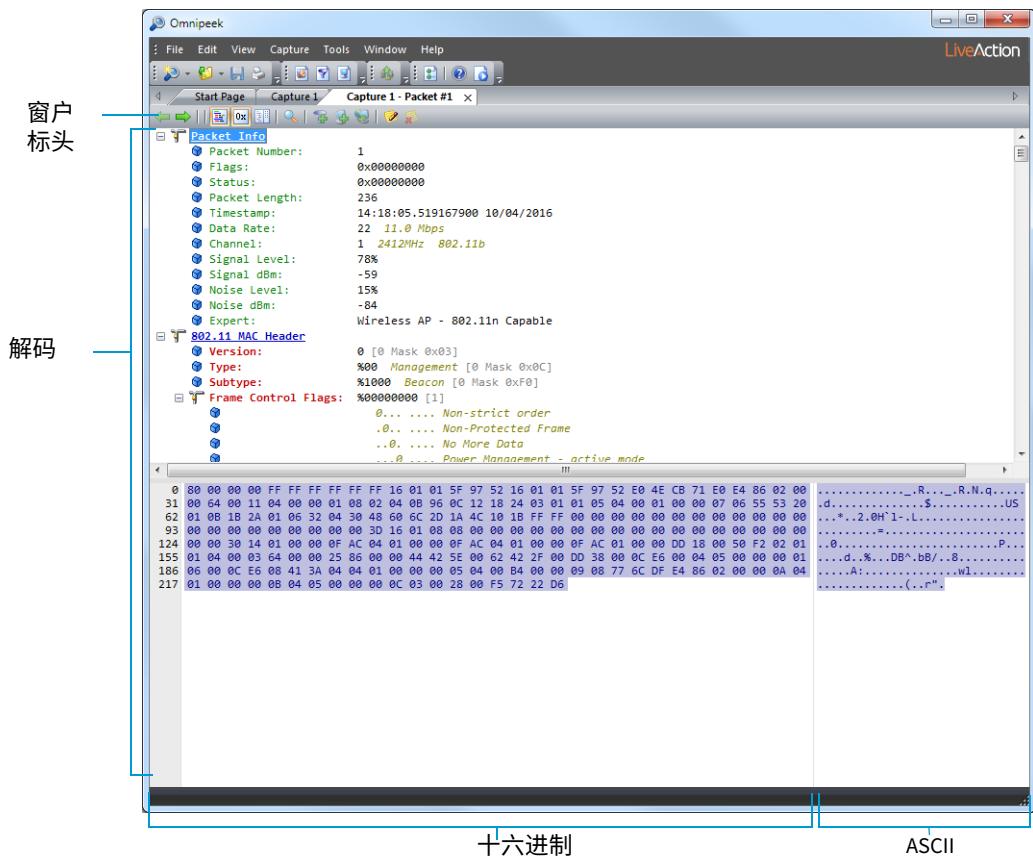
8. 选择一个节点类型图标来表示此数据包。节点类型选项让你选择一个将出现在数据包列表中的图标，例如，工作站，服务器，路由器，或者接入点。

## 数据包解码窗口

通过查看单个数据包中包含的详细信息，可以更快地发现网络问题。查看数据包可以帮助您排除网络故障、追踪安全漏洞或检查协议结构和合规性。

**要查看数据包的解码：**

1. 双击数据捕获窗口的视图。出现数据包解码窗口。解码后的数据包数据按字节顺序从上到下显示。



**提示** 您可以一次打开最多 10 个数据包的单个数据包解码窗口。在活动数据包列表中选择多个数据包时，单击进入将其全部打开。

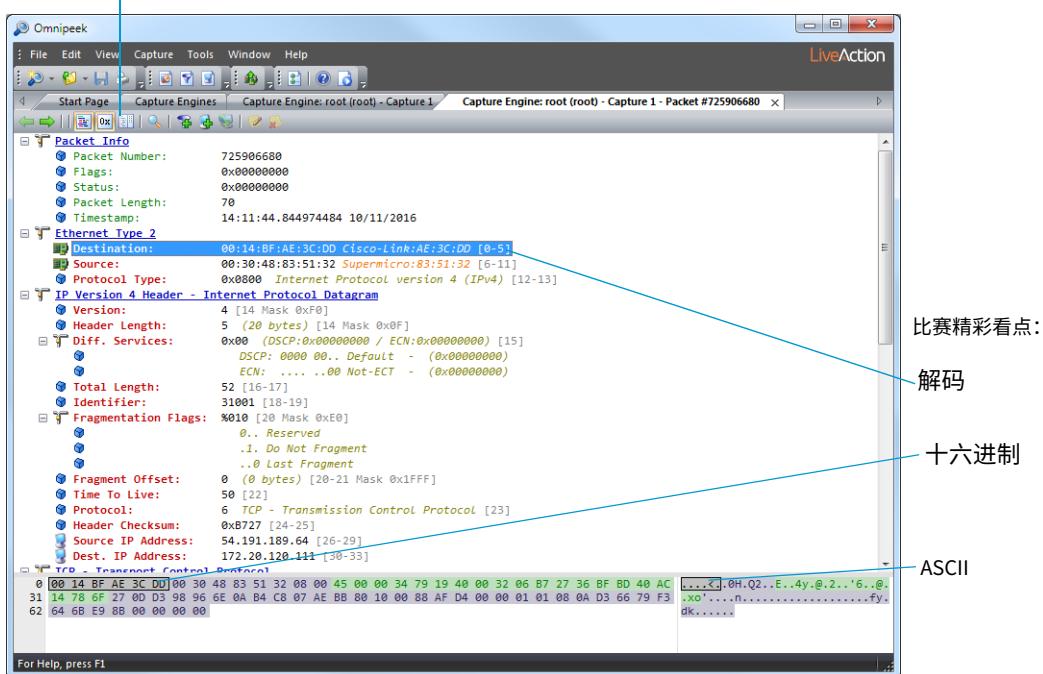
## 2. 点击 - 减去或 + 在边距中添加加号可以折叠或展开任何标题部分的视图。

- **窗口标题：**点击解码上一个或者解码下一个在窗口顶部逐一查看活动捕获窗口的数据包列表中显示的数据包。
- **解码视图：**主体解码视图的布局顺序与数据包中的顺序相同。快速浏览此部分通常可以发现问题的根源。当您看到并比较数据包本身时，可以轻松理解诸如客户端配置错误或不同供应商的同一协议的版本不兼容等问题。
- **十六进制视图：**这十六进制解码窗口底部的视图显示每行第一个字符的偏移量、十六进制的原始数据包数据以及原始数据包数据的 ASCII 版本

## 3. 在窗口的某个部分突出显示某项。数据包的相同字节也会在所有其他视图或窗格中突出显示。突出显示与解码、十六进制和 ASCII 窗格中的突出显示相匹配。

颜色编码用于链接解码查看十六进制十六进制和其 ASCII 等效视图。十六进制和 ASCII 视图又与数据包列表的协议列中显示的协议颜色相关联。

## 切换方向



**提示** 使用切换方向在工具栏中垂直或水平平铺解码和十六进制视图。

## 创建过滤器

过滤器可让您专注于特定流量。如果您要检查两个特定设备（可能是一台计算机和一台打印机）之间的问题，地址过滤器可以仅捕获这两个设备之间的流量。如果您的网络上某个特定功能出现问题，协议过滤器可让您专注于与该特定功能相关的流量。

过滤器的工作原理是针对过滤器中指定的标准测试数据包。内容符合这些标准的数据包将与过滤器匹配。您可以构建过滤器来测试数据包中发现的几乎所有内容：地址、协议、子协议、端口、错误条件等。过滤器的创建非常简单，因为您通常可以在分析网络上的可疑流量时即时创建自定义过滤器。

---

**笔记** 从连接的捕获引擎创建的过滤器仅可用于该捕获引擎。如果您未连接到捕获引擎并创建过滤器，则该过滤器仅适用于本地捕获。

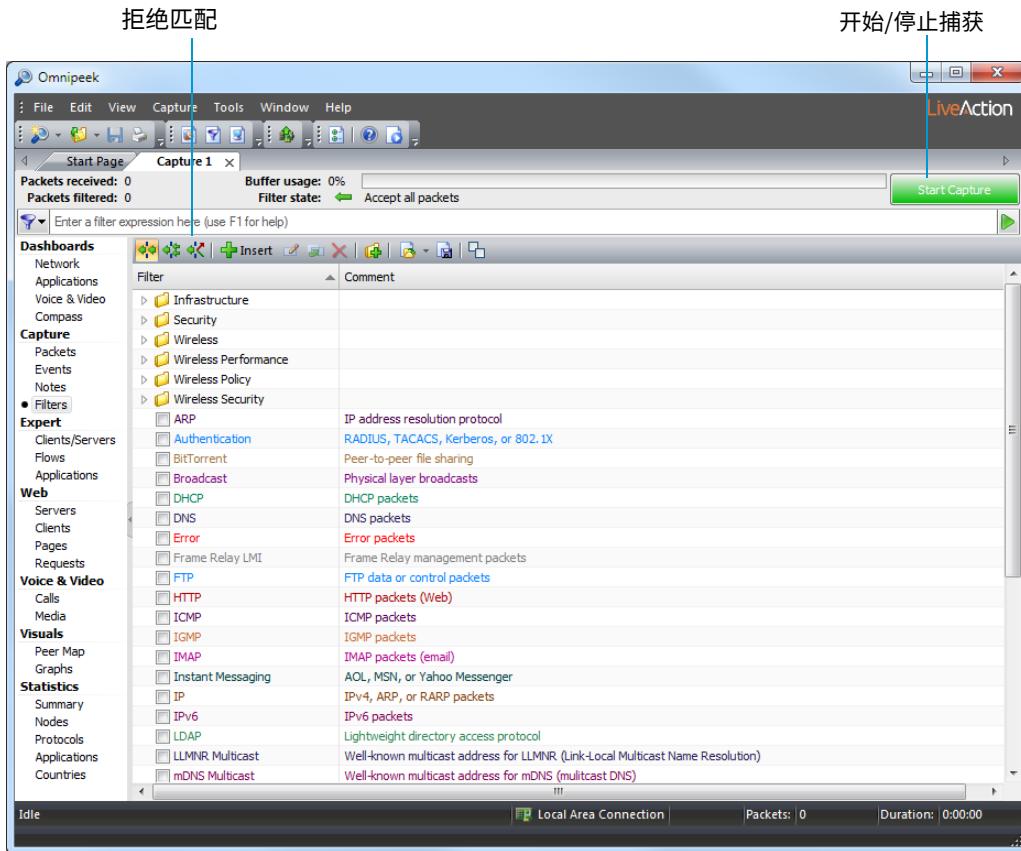
---

### 启用过滤器

除了您创建的过滤器之外，OmniPeek 和捕获引擎还包含许多预定义过滤器。您可以在捕获或监控数据包时启用一个或多个过滤器。

**要在捕获数据包时启用过滤器：**

**4. 点击筛选器在捕获窗口中查看。**



5. 选择您想要启用的一个或多个过滤器。

**笔记** 对于捕获引擎，您需要通过点击工具栏图标下方的栏将选择发送到捕获引擎 **单击此处发送更改**。

6. 点击**开始捕捉**开始捕获数据包。任何与启用的过滤器匹配的数据包都将放入捕获缓冲区。

或者，您可以选择将与过滤器不匹配的数据包放入捕获缓冲区，方法是  
点击**拒绝匹配**。

## 使用 make filter 命令创建过滤器

您可以使用**制作过滤器**命令可以轻松创建基于现有数据包、节点、协议、对话或数据包解码的地址、协议和端口设置的过滤器。

**要使用 Make Filter 命令创建过滤器：**

1. 右键单击捕获窗口中可用的视图之一中的数据包、节点、协议、对话或数据包解码项，然后选择**制作过滤器**。这插入过滤器出现对话框，其中地址、协议和端口设置已使用所选数据包的信息进行配置。
2. 在筛选文本框并进行任何其他更改。
3. 点击**好的**。现在，只要显示可用过滤器列表，就可以使用新过滤器。
4. 要在捕获窗口中启用新过滤器，请点击筛选器视图并选中新过滤器的复选框。即使捕获已在进行中，过滤器也会立即应用。

## 创建一个简单的过滤器

您可以通过手动输入要创建的过滤器的参数来创建简单过滤器。与使用 Make Filter 命令创建过滤器不同，您必须手动定义要创建的过滤器的参数（地址、协议和端口设置）。

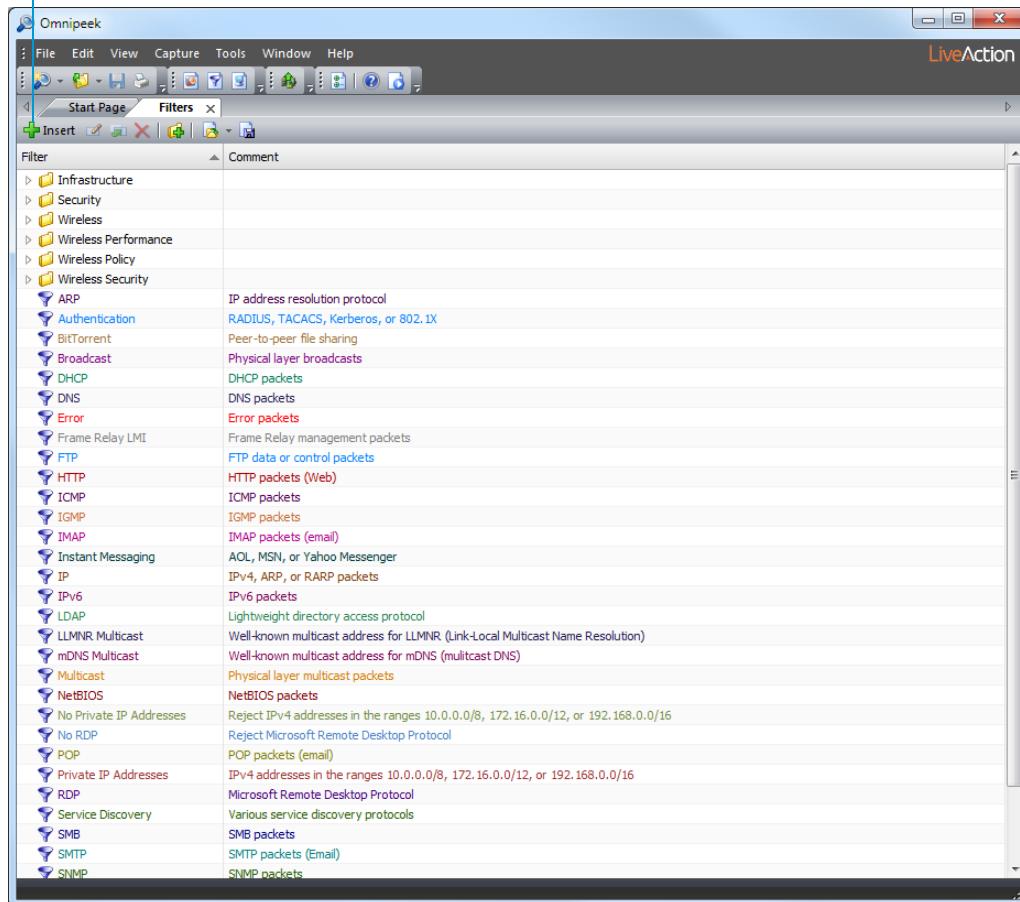
**笔记** 有关创建更高级过滤器的信息，请参阅 *OmniPeek 用户指南* 或在线帮助。

### 通过定义地址和协议来创建简单过滤器：

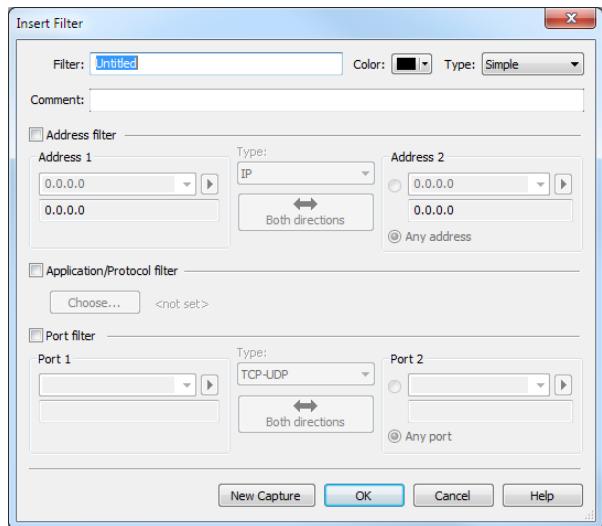
#### 1. 执行以下操作之一打开筛选器看法：

- 在看法菜单，点击筛选器（仅适用于本地捕获的过滤器）
- 点击筛选器在打开的捕获窗口中查看
- 点击筛选器捕获引擎的选项捕获选项对话

插入



#### 2. 点击插入。这插入过滤器出现对话框。



3. 给你的新过滤器命名。

4. 填写地址、协议或端口设置信息并点击好的。现在，只要显示可用过滤器列表，就可以使用新过滤器。

5. 要在捕获窗口中启用新过滤器，请点击筛选器视图并选中新过滤器的复选框。即使捕获已在进行中，过滤器也会立即应用。

**提示** 点击新捕获创建一个新的捕获窗口，该窗口使用您在中定义的过滤器插入/编辑过滤器对话框作为唯一启用的过滤器。

## 专家故障排除

Omnipeek 和捕获引擎中的专家功能可在捕获窗口中以流为中心的流量视图中实时分析响应时间、吞吐量以及各种网络事件和潜在问题。您还可以通过应用程序性能指数 (Apdex) 将最终用户满意度与网络应用程序的性能联系起来，Apdex 是一种定义报告应用程序性能方法的开放标准。请参阅[应用程序视图](#)在第58页。

Expert EventFinder 可检测近 200 种不同的网络事件，并提供按 OSI 层组织的描述、可能的原因和可能的补救措施。根据程序的版本，还会显示与 VoIP、无线、WAN 和用户定义的网络策略项目特别相关的网络事件。请参阅[使用 EventFinder](#)在第57页。

### 专家视图窗口

专家客户端/服务器视图可以轻松跟踪事件并在对等或客户端-服务器流量模式的上下文中查看它们。

**要在专家客户端/服务器视图中显示事件：**

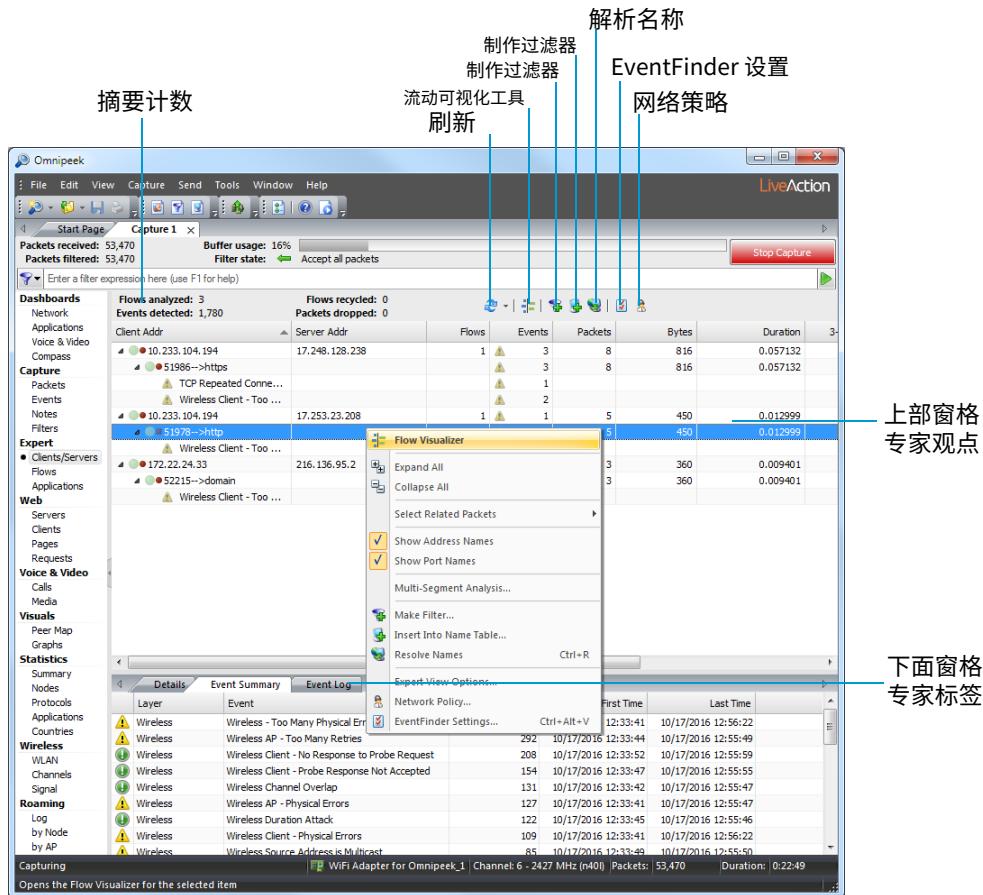
**1.选择客户端/服务器**在下面专家在捕获窗口的导航栏中。

节点对显示在顶层，单个对话（流）显示在节点下，单个事件嵌套在每个流下。颜色编码的流量指示灯显示过去几秒内是否接收到数据包：

- 绿色（活动）
- 浅绿色（不活跃）

当检测到事件时，交通指示灯右侧会出现较小的 LED 灯：

- 红色 LED 指示一个或多个严重程度为“重大”或“严重”的事件。
- 黄色 LED 指示一个或多个事件的严重性为“信息性”或“轻微”。



2. 右键单击上方窗格可折叠或展开层次结构以显示最相关的信息。展开后，专家事件按端口显示。端口以方向箭头显示。

**提示** 在专家客户端/服务器查看，排序依据活动可以帮助查明网络上的潜在问题。

## 使用 EventFinder

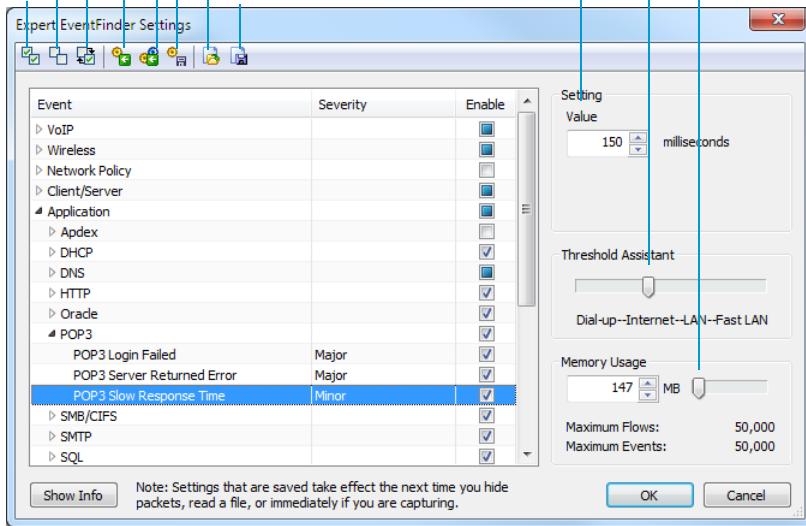
您可以在专家 EventFinder 设置对话。

要打开专家事件查找器设置窗口：

1. 右键单击客户端/服务器查看并选择展开全部。
2. 从扩展的客户端/服务器看法。
3. 点击 EventFinder 设置。这专家 EventFinder 设置出现此专家事件的窗口突出显示，如下所示：

恢复选定的默认值 恢复所有用户默认值  
 全部切换 设置用户默认值  
 全部禁用 导入设置  
 全部启用 导出设置

阈值助手  
 设置内存使用量



**笔记** 您也可以右键单击活动摘要或者事件日志选项卡并选择 EventFinder 设置显示专家 EventFinder 设置窗口。

#### 4. 点击显示信息查看此网络事件的完整描述、可能的原因以及可能的补救措施。

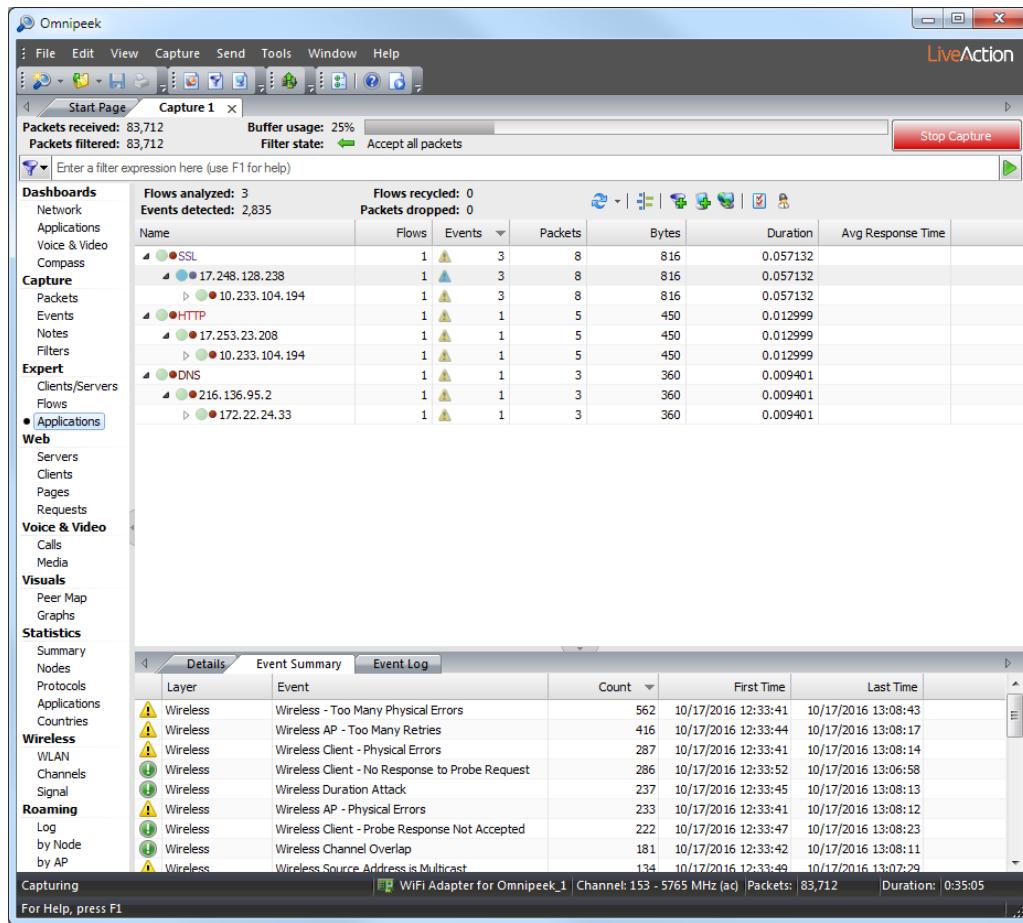
这专家 EventFinder 设置窗口还提供了有关使用什么敏感度或设置值来将此事件标记为重要事件的信息。您可以在 EventFinder 窗口中为每个单独的专家事件配置值、阈值和内存设置。您还可以通过将这些设置导出到文件并在稍后将其导入到另一次捕获中来保存这些设置。

## 应用程序视图

专家应用视图按应用程序对每个流进行分类。流按应用程序分组，提供每个应用程序使用情况的分层视图，首先按服务器，然后按客户端，然后按端口。此视图允许您查看谁在使用您网络上的每个应用程序以及每个应用程序的运行情况。

**要显示应用程序视图：**

- 选择应用在下面专家在捕获窗口的导航栏中。



## 多段分析

### 关于多段分析

Omnipeek 中的多段分析 (MSA) 可让您快速轻松地定位、可视化和分析一个或多个流，因为它们会从端到端穿越网络上的多个捕获点。MSA 可跨多个网络段提供应用程序流的可视性和分析，包括网络延迟、数据包丢失和重传。

MSA 可以快速查明多个段中的问题及其根本原因，将有问题的流程汇集在一起，创建分析会话，报告异常，并提供整个网络多个段的图形可视化。

易于使用的 MSA 向导允许您从网络上的多个捕获引擎或多个现有捕获数据包文件创建 MSA 项目。此外，还可以通过右键单击捕获窗口导航窗格中的各种视图来创建 MSA 项目。

#### 重要的！

Omnipeek 构建和显示 MSA 项目所需的时间取决于段数、流数以及每个流中的数据包数。MSA 限制每个流 100,000 个数据包（可通过多段分析选项进行修改），但项目中包含的段数或流数没有硬性限制。为 MSA 项目选择数据时要谨慎。如果您发现 MSA 项目构建时间过长，则可以取消并减少数据集。

---

为了促进基于取证搜索的 MSA 项目的创建，建议采用以下最佳实践：

- 每个捕获引擎都应有一个唯一的名称。这可以通过捕获引擎管理器或捕获引擎向导来完成。
- 确保所有捕获引擎的时间都是准确的。如果可能，请将捕获引擎配置为使用 NTP 服务器。
- 为每个捕获指定一个唯一的名称。例如，根据网络段命名捕获。
- 一旦 MSA 项目 (.msa 在创建 MSA 项目包文件后，您可能希望保存用于创建 MSA 项目的包文件，原因如下：
  - 如果您想向 MSA 项目添加另一个段，则将再次需要数据包文件。
  - 您可能想要打开与特定段相关的跟踪文件，以查看不同的 Omnipiiek 视图，例如“数据包”或“流”视图。
  - 可能需要重建 MSA 项目才能利用 Omnipiiek 未来版本中的新 MSA 功能。

此外，必须为基于 MSA 的取证搜索启用以下捕获选项设置：

- ‘捕获到磁盘’
- ‘时间线统计’（仅限经典捕获引擎）

**笔记** 基于 MSA 的取证搜索需要时间线统计。经典捕获引擎从 6.8 版开始支持时间线统计。

## MSA 项目窗口

使用 MSA 向导配置和创建后，将显示如下所示的 MSA 项目窗口。MSA 项目窗口由以下部分组成：流程列表、流程图和阶梯图。

**笔记** 在计算流程图和阶梯的延迟值时，MSA 假设客户端在左侧，服务器在右侧。如果您创建包含多个流程的 MSA 项目，则项目中的所有流程都应从同一方向发起。例如，由防火墙私有侧的两个节点发起的流程适合包含在单个 MSA 项目中。由防火墙私有侧的节点发起的流程和由防火墙公共侧的节点发起的流程不适合包含在单个 MSA 项目中。



## 流列表

流列表显示每个捕获源的流的层次结构列表，包括每个流的相关信息（客户端/服务器地址和端口、协议、数据包计数等）。流列表是层次结构的，流位于顶层，捕获段列在流下方。每个捕获段都包含该流的统计信息。选中流旁边的复选框会在下面的流程图和梯形图中显示该流。

**笔记**

对于具有多个流程的 MSA 项目，每次只能在流程列表中选择一个流程。所选流程将显示在流程图和梯形图中。



- 列标题：显示当前选定的列标题。右键单击列标题可启用/禁用列。以下是可用的列：

- 流程/段：流或段的名称。
- 客户端地址：流的客户端地址。
- 客户端端口：客户端或客户端地址在流程中进行通信的端口。
- 服务器地址：流的服务器地址或服务器地址。
- 服务器端口：服务器或服务器地址在流中进行通信的端口。
- 协议：流中的数据包交换所依据的协议。
- 数据包：选定流中的数据包数量。
- 客户端数据包：流中从客户端或客户端地址发送的数据包总数。
- 服务器数据包：流中从服务器或服务器地址发送的数据包总数。
- 数据包分析：Omnipeek 的 MSA 组件分析的流中的数据包总数。除非流中的数据包数量超出 MSA 选项中配置的数据包限制，否则“已分析的 数据包”将与“数据包”相同。
- 数据包丢失：段中丢失的数据包数量。在 MSA 项目中，特定段中被标识为“丢失”的数据包至少出现在另一个段中。

- **客户端数据包丢失:** 客户端方向丢失的数据包数量。
- **服务器数据包丢失:** 服务器方向丢失的数据包数量。
- **客户端重传:** 客户端发送的TCP重传次数。
- **服务器重传:** 服务器发送的 TCP 重传次数。
- **开始:** 流中第一个数据包的时间戳。
- **结束:** 流中最后一个数据包的时间戳。
- **期间:** 从流中第一个数据包到最后一个数据包所经过的时间。
- **TCP 状态:** 注意 TCP 会话是打开还是关闭。
- **列…:** 显示一个对话框，让您启用/禁用和组织列。
- **显示所有列:** 显示所有可用的列。

## 流程图

流程图以图形方式显示所选流程的各个段。流程中的每个段都以端到端的方式显示（左侧为客户端，右侧为服务器），同时显示每个段之间的时间统计信息（平均延迟、最小延迟和最大延迟）。此外，还会显示每个段之间的跳数（段之间云中的小数字）。



## 流程图查看技巧

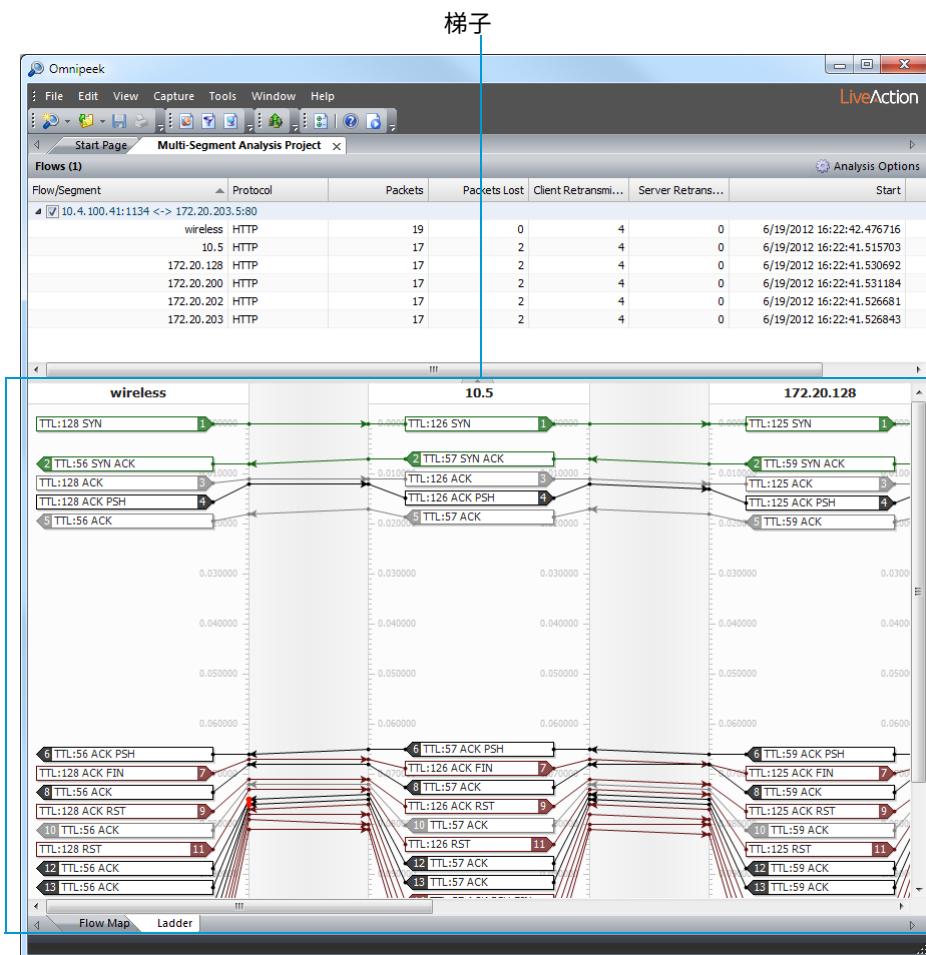
以下是查看流程图内数据时的一些有用提示：

- 将鼠标悬停在片段名称和云上可以查看显示更多数据的工具提示。

- 按下 Ctrl 键并使用滚轮 (Ctrl+Wheel) 来更改段宽度。
- 箭头显示数据流动的方向。
- 客户端和服务器箭头使用与客户端/服务器颜色 (工具>选项)。
- 云中的数字是跳数，由数据包内的生存时间 (TTL) 值决定。如果云中有一个数字，则客户端和服务器跳数相同。如果云中有两个数字，则客户端和服务器跳数不同，表明客户端和服务器路径不同。如果一个方向有多条路径，则不显示此方向的跳数。大于一的跳数以红色显示。每个数据包的 TTL 都可以显示在梯形图中。

## 梯子

梯形图显示捕获源所代表的段之间的数据包流动，以及时间等信息。



## 梯子观看技巧

以下是查看梯形图内部数据时的一些有用提示：

- 将鼠标悬停在数据包框上可以查看显示更多数据的工具提示。
- 箭头显示数据流动的方向。
- 绿色框是打开流程的数据包 (SYN 和 SYN-ACK)。
- 黑匣子是具有非零有效载荷的数据包 (携带数据的数据包)。
- 灰色框是有效载荷为零的数据包 (可能只是 ACK 数据包)。

- 红色框是关闭连接的数据包（FIN或RST）。
- 在图表内单击鼠标右键即可显示/隐藏其他统计数据，或调整阶梯的时间尺度。
- 阶梯显示中提供以下键盘/滚轮快捷键：
  - 滚轮+Ctrl：更改时间尺度。
  - 滚轮+Ctrl+Shift：缩放时间刻度。
  - 滚轮+Ctrl+Shift+Alt：更改段宽度。
  - Ctrl+Alt+Shift+F9：将梯形图显示保存为文本。

## 创建 MSA 项目

要创建 MSA 项目，您必须使用 MSA 向导。MSA 向导将指导您完成 MSA 项目的创建，并包括设置项目参数以及最终显示 MSA 项目窗口的步骤。有多种方法可以启动 MSA 向导。此外，根据您启动向导的方式，MSA 向导有多个入口点。您可以以下方式启动 MSA 向导：

- 从文件菜单，选择新的多段分析项目… MSA 向导出现，并提示您通过在远程引擎上搜索数据包或使用数据包文件来创建 MSA 项目：
  - 在远程引擎上搜索数据包：选择此选项，MSA 向导将首先引导您选择要搜索的时间范围和要应用的过滤器（建议使用 IP/端口对过滤器，但 OmniPeek 支持的任何过滤器都可以使用）。其他向导屏幕将引导您选择要搜索的捕获引擎和每个捕获引擎的捕获会话。

最后，向导执行搜索，并将相关数据包下载到 OmniPeek 进行分析。从那里开始，它的工作方式与从文件进行多段分析的方式相同，只是文件已经为您输入（它们是从捕获引擎下载的文件）。您可以重新排序段、重命名段、更改时间偏移，并将输出保存为。管理事务协调局文件。

- 使用数据包文件：选择此选项，MSA 向导将指导您选择要使用的文件（每个片段一个文件）以及它们之间的时间偏移。您还可以命名每个片段并重新排序。然后，您可以将生成的项目保存为 .管理事务协调局文件，稍后可以重新加载。管理事务协调局文件包含所有分析，因此您不必再次进行任何设置。
- 从数据包在导航窗格中查看：右键单击一个或多个数据包，然后选择多段分析… MSA 向导出现并指导您完成 MSA 项目的创建，首先选择要搜索的时间范围和要应用的过滤器。
- 从任何专家观看次数（客户端/服务器，流程， 和应用）：右键单击一个或多个流程，然后选择多段分析… MSA 向导出现并指导您完成 MSA 项目的创建，首先选择要搜索的时间范围和要应用的过滤器。多段分析… 选项仅适用于 IPv4 TCP 流。MSA 不支持 UDP 或 IPv6 流。
- 从任何网页观看次数（服务器，客户，页面， 和请求）：右键单击一个或多个服务器、客户端、页面或请求，然后选择多段分析… MSA 向导出现并指导您完成 MSA 项目的创建，首先选择要搜索的时间范围和要应用的过滤器。
- 从节点和协议导航窗格中的视图：右键单击一个或多个节点或协议，然后选择多段分析… MSA 向导出现并指导您完成 MSA 项目的创建，首先选择要搜索的时间范围和要应用的过滤器。

### 重要的！

OmniPeek 构建和显示 MSA 项目所需的时间取决于段的数量、流的数量以及每个流中的数据包数量。MSA

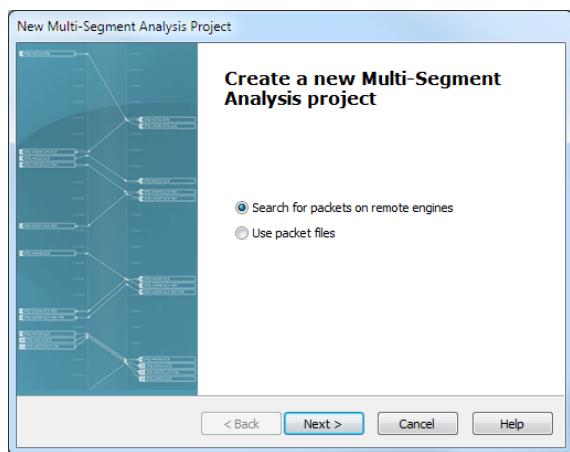
每个流的限制为 100,000 个数据包（可通过多段分析选项进行修改），但项目中包含的段或流的数量没有硬性限制。为 MSA 项目选择数据时要谨慎。如果您发现 MSA 项目的构建时间过长，则可以取消并减少数据集。

## 使用 MSA 向导

MSA 向导将指导您完成 MSA 项目的创建。您可以通过多种方式访问 MSA 向导，具体方法如下[创建 MSA 项目](#)本节介绍 MSA 向导的各个屏幕。

### 创建一个新的多段分析项目

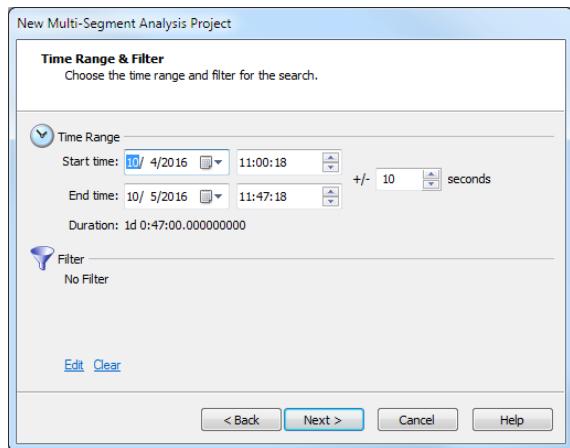
这创建一个新的多段分析项目 MSA 向导的对话框可通过选择文件>新的多段分析…该对话框可让您从头开始创建一个新的多段分析项目。



- 在远程引擎上搜索数据包：选择此选项可根据从一个或多个捕获引擎获得的数据包创建 MSA 项目。
- 使用数据包文件：选择此选项可以基于一个或多个数据包文件创建 MSA 项目。

### 时间范围和过滤器

这时间范围和过滤器 MSA 向导的对话框允许您选择应用于搜索的时间范围和过滤器。

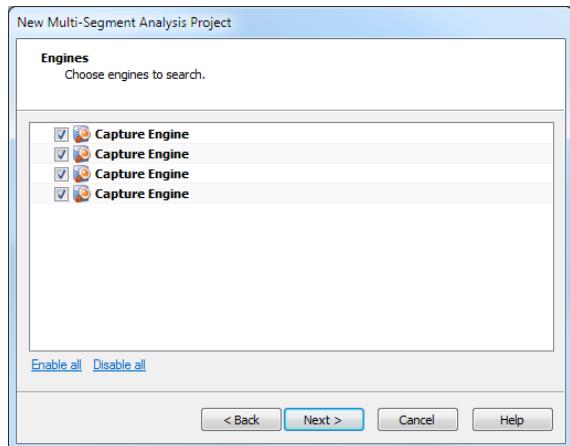


- 开始时间：选择或输入您要搜索的范围的开始日期和时间。

- **结束时间:** 选择或输入您要搜索的范围的结束日期和时间。
- **+/-秒:** 选择或输入在开始时间之前和结束时间之后添加到搜索的秒数。
- **期间:** 显示指定的开始时间和结束时间之间的时间量。
- **筛选:** 显示当前为搜索定义的任何过滤器。
- **编辑:** 单击显示“编辑过滤器”对话框，您可以在其中根据地址、协议和端口的任意组合定义简单和高级过滤器。数据包必须符合指定的所有条件才能匹配过滤器。
- **清除:** 单击可删除当前为搜索定义的任何过滤器。

## 引擎

这引擎对话框显示当前在 Omnipeek 捕获引擎窗口中列出的组和捕获引擎。如果您选择了在远程引擎上搜索数据包在 MSA 向导中，引擎单击后出现对话框下一个在时间范围和过滤器 MSA 向导的对话框。

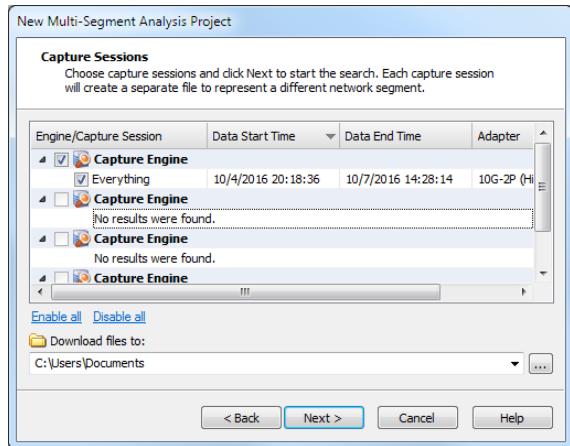


- 选中要在 MSA 项目中搜索的捕获引擎的复选框。如果您尚未连接到捕获引擎，系统将首先提示您通过输入域、用户名和密码信息来连接到捕获引擎。
- **全部启用:** 点击此选项可以选中对话框中显示的所有组和捕获引擎的复选框。
- **全部禁用:** 点击此选项可以清除对话框中显示的所有组和捕获引擎的复选框。

## 捕获会话

这捕获会话对话框显示每个选定的捕获引擎中找到的捕获会话。如果您选择了在远程引擎上搜索数据包在 MSA 向导中，捕获会话单击后出现对话框下一个在引擎 MSA 向导的对话框中。单独的

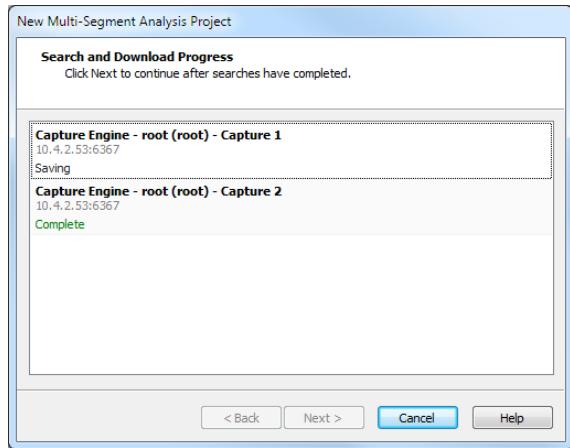
\*.wpz 为每个选定的捕获会话创建一个文件，每个文件代表一个不同的网络段。在进行多段分析时，Omnipeek 使用 \*.章 斯特文件来构建 MSA 项目。



- 列标题:** 显示当前选定的列标题。右键单击列标题可启用/禁用列。以下是可用的列:
  - 引擎/捕获会话:** 先前选择的捕获引擎提供的捕获会话。选中要在 MSA 项目中搜索的捕获会话的复选框。捕获具有 '捕获到磁盘' 和 '时间线统计' 在捕获选项中启用，并且所有具有 '捕获到磁盘' 在捕获选项中启用，出现在捕获会话屏幕中。（基于 MSA 的取证搜索需要 '时间线统计'。）
  - 会议开始时间:** 捕获的开始时间。
  - 数据开始时间:** 捕获中首次出现数据时的开始时间。
  - 数据结束时间:** 捕获中最后出现数据的时间。
  - 尺寸:** 捕获会话的大小（以 MB 为单位）。
  - 数据包:** 捕获会话中的数据包数量。
  - 数据包被丢弃:** 捕获会话中丢弃的数据包数量。
  - 媒体:** 捕获会话的媒体类型。
  - 适配器:** 用于捕获会话的适配器的名称。
  - 适配器地址:** 用于捕获会话的适配器的地址。
  - 链接速度:** 用于捕获会话的适配器的链接速度。
  - 所有者:** 用于捕获会话的适配器的所有者名称。
- 全部启用:** 单击此选项可以选中对话框中显示的所有捕获引擎和捕获会话的复选框。
- 全部禁用:** 单击此选项可以清除对话框中显示的所有捕获引擎和捕获会话的复选框。
- 下载文件:** 选择保存位置 \*.韋斯特为每个选定的捕获会话创建的文件。

## 进步

这**进步**对话框显示保存状态 \*.韋斯特用于多段分析的文件。如果您选择了在**远程引擎上搜索数据包**在 MSA 向导中，单击下一个在**捕获会话**MSA 向导的对话框。



对话框中的每个条目列出以下内容：

- 捕获引擎和捕获会话名称
- 捕获引擎 IP 地址和端口
- 每个文件的当前状态

进度状态消息如下：

- **搜索进度**: 根据向导中指定的时间范围和过滤器，进行取证搜索的进度
- **保存**: 搜索结果保存为。韋斯特引擎上的文件
- **删除搜索**: 引擎上的取证搜索被删除
- **下载进度**: 这。韋斯特文件下载到 Omnipeek 计算机
- **删除远程文件**: 这。韋斯特文件已从引擎中删除
- **完全的**: 整个过程已完成。一旦您看到完全的对于所有捕获片段，点击下一个继续建设 MSA 项目

**提示** 您可以通过右键单击并选择来取消任何一个捕获段的进度  
取消。您可以取消上述任何阶段，但保存阶段。

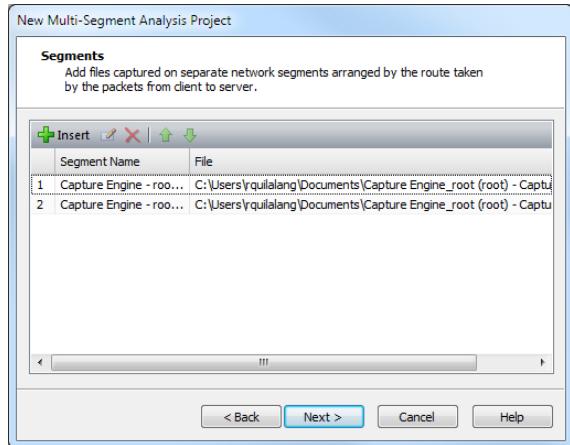
## 细分

这细分对话框允许您将在不同网络段上捕获的支持捕获文件添加到 MSA 项目中。为了使 MSA 分析正确显示在流程图和梯形图中，每个段文件必须按照从客户端到服务器的路径正确排序（在流程图和梯形图中显示时，客户端在左侧，服务器在右侧）。您可以手动选择在对话框中排列文件。

**提示** 如果您没有按照从客户端到服务器的路径手动排列文件，则可以使用分析选项对话框。请参阅[MSA 项目分析选项](#)在第71页。

**笔记** 在计算流程图和阶梯的延迟值时，MSA 假设客户端在左侧，服务器在右侧。如果您创建包含多个流程的 MSA 项目，则项目中的所有流程都应从同一方向发起。例如，防火墙私有侧的两个节点发起的流程适合包含在单个

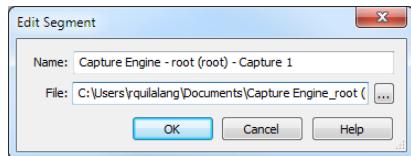
MSA 项目。防火墙私有侧节点发起的流量和防火墙公共侧节点发起的流量不适合包含在单个 MSA 项目中。



- 插入:** 单击可插入新片段。系统将提示您命名该片段并选择支持的捕获文件。
- 编辑:** 单击可编辑选定的片段。您可以选择重命名该片段或为该片段选择其他支持的文件。
- 删除:** 点击可删除选定的片段。
- 上移:** 单击可将选定的段在有序的段列表中向上移动。您也可以按 (Shift 或 Ctrl) + 向上箭头将段在列表中向上移动。
- 下移:** 单击可将选定的段在有序的段列表中向下移动。您也可以按 (Shift 或 Ctrl) + 向下箭头将段在列表中向下移动。
- 列标题:** 显示当前选定的列标题。右键单击列标题可启用/禁用列。以下是可用的列:
  - 段名称:** 片段的名称。
  - 文件:** 片段的位置和文件名。

## 编辑片段

该对话框可让您编辑选定的片段。



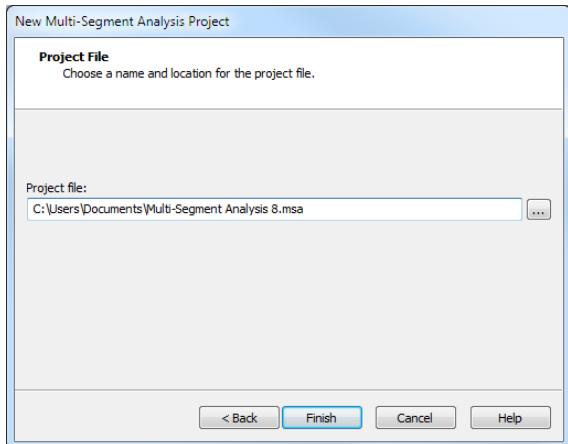
- 姓名:** 显示段的名称。输入其他名称可重命名段。
- 文件:** 显示段文件的位置和名称。

## 项目文件

该项目文件对话框允许您保存 MSA 项目文件 (\*.msa)。保存后，将显示 MSA 项目窗口。

### 笔记

如果您的 MSA 项目窗口是空白的，很可能您选择了 MSA 不支持的流（例如，UDP 或 IPv6），或者它是带有碎片数据包的流。



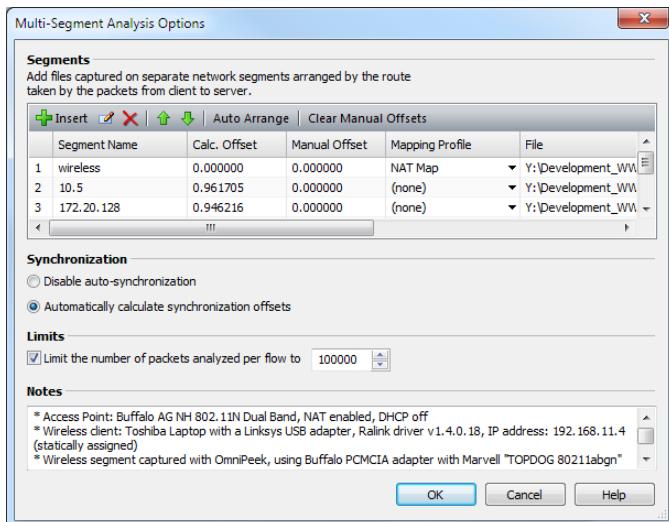
- 项目文件：显示位置和 MSA 项目文件名（\*.msa）。

## MSA 项目分析选项

创建或打开现有 MSA 项目窗口后，您可以访问多段分析选项对话框可编辑段、同步和限制选项。此外，您还可以为项目添加注释。

### 要编辑 MSA 选项：

- 点击分析选项在 MSA 项目窗口中。多段分析选项出现对话框。



- 完成对话框：

- 插入：**单击可插入新片段。系统将提示您命名该片段并选择支持的捕获文件。
- 编辑：**单击可编辑选定的片段。您可以选择重命名该片段或选择其他受支持的捕获文件。
- 删除：**点击可删除选定的片段。
- 上移：**单击可将选定的段在有序段列表中上移。
- 下移：**单击可将选定的段在有序段列表中向下移动。
- 自动排列：**单击可根据数据包中的 TTL 值按从客户端到服务器的顺序排列段。如果您创建包含多个流的 MSA 项目，则项目中的所有流

应从同一方向发起。如果您创建包含 NAT（网络地址转换）段的 MSA 项目，请在选择自动排列。

- **清除手动偏移：**单击可将手动偏移设置为零。
- **列标题：**显示当前选定的列标题。右键单击列标题可启用/禁用列。以下是可用的列：
  - **段名称：**片段的名称。
  - **计算偏移：**自动计算的段同步偏移量。
  - **手动偏移：**用户指定的偏移。可以使用手动偏移来代替或补充自动计算的偏移。
  - **总偏移量：**计算的偏移加上手动偏移。
  - **映射配置文件：**与段关联的映射配置文件。可以创建映射配置文件以将私有地址/端口映射到公有地址/端口。请参阅[创建映射配置文件](#)在第72页。
  - **文件：**MSA 段信息所依据的位置和数据包文件。
  - **列…：**显示一个对话框，让您启用/禁用和组织列。
  - **显示所有列：**显示所有可用的列。
- **禁用自动同步：**选择此选项可禁用自动计算偏移值。
- **自动计算同步偏移：**选择此选项可启用自动计算同步偏移值。所有捕获引擎都应设置为正确的时间，最好通过使用 NTP 服务器。但是，即使使用 NTP 服务器，也可能需要偏移量来调整捕获引擎之间的轻微时间不准确性。同步偏移的自动计算基于 TCP SYN 和 TCP SYN ACK 数据包。如果某个段不包含 SYN 和 SYN ACK 数据包，则计算偏移字段中将出现破折号 (-)。如果 MSA 项目包含多个流，则同步偏移的自动计算基于所有流。
  
  
  
  
  
  
- **限制：**选中此复选框启用每个流分析的数据包数量限制，然后输入或选择流的数量。
- **笔记：**键入要附加到 MSA 项目的任何注释。

### 3.点击好的。

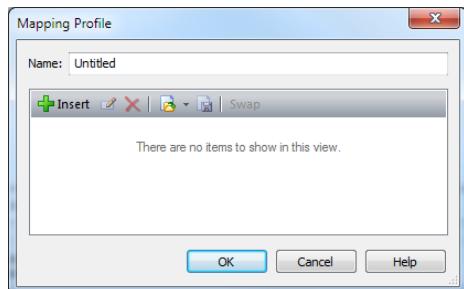
## 创建映射配置文件

映射配置文件用于将私有地址/端口映射到公有地址/端口。

**笔记** 如果您的项目包含网络地址转换 (NAT) 段，则在应用映射配置文件之前不应选择自动排列功能。

### 要创建映射配置文件：

1. 在 MSA 项目窗口中，单击分析选项显示多段分析选项对话。
2. 单击所需段的映射配置文件列中的框。将出现一个弹出菜单。
3. 选择新的。这映射配置文件出现对话框。



**4.完成映射配置文件对话框：**

- **姓名：**输入配置文件的名称。
- **插入：**点击显示地址/端口映射对话。完成对话。
- **编辑：**单击可编辑选定的映射。地址/端口映射对话框出现。完成对话框。
- **删除：**点击，删除选中的映射。
- **进口：**单击以导入 MSA 映射文件 (\*.xml) 。
- **出口：**单击可将映射配置文件导出到 MSA 映射文件 (\*.xml) 。
- **交换：**点击可交换选定映射的方向。

**5.点击好的。**

## 统计分析

Omnipeek 和 Capture Engines 实时计算各种关键统计数据，并以直观的图形显示呈现这些统计数据。您可以保存、复制、打印或自动生成各种格式的这些统计数据的定期报告。（请参阅 *Omnipeek 用户指南* 或在线帮助以获取有关生成统计报告的信息。）

### 捕获窗口统计信息

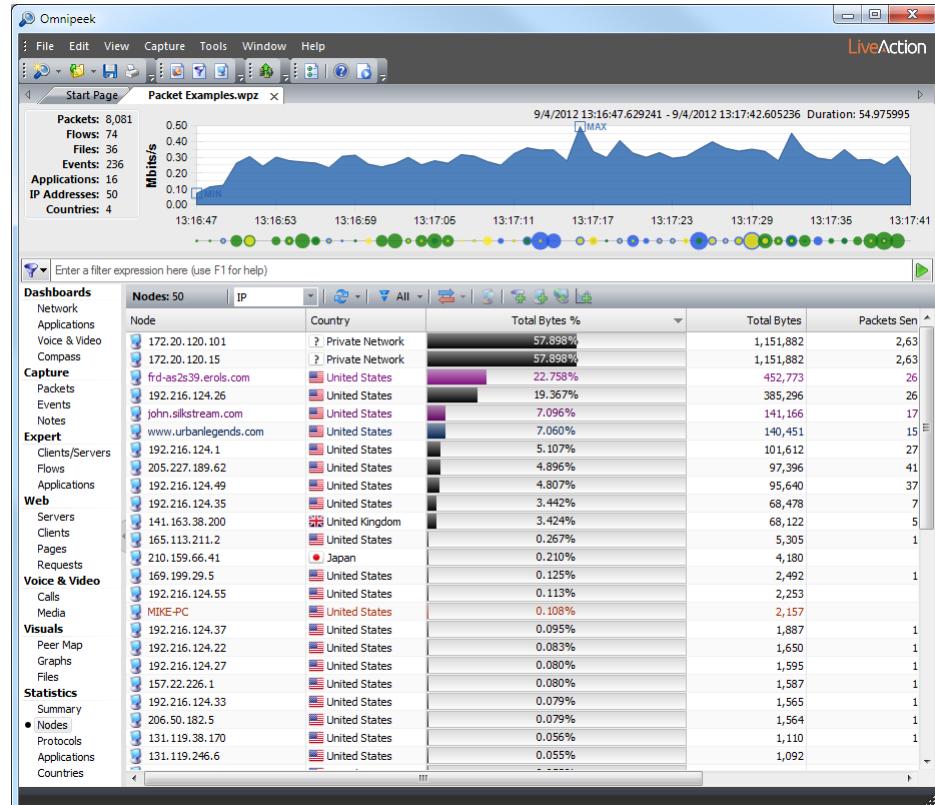
Omnipeek 和 Capture Engine 捕获窗口提供以下统计视图：摘要，节点，协议，应用，和国家（并且，当选择 802.11 适配器时），无线局域网，频道，和信号。

本节介绍节点和无线局域网捕获窗口的视图。

#### 节点视图

节点统计信息显示按网络节点组织的实时数据。您可以在分层视图或各种平面视图中查看节点统计信息。节点统计信息适用于整个网络和捕获窗口。

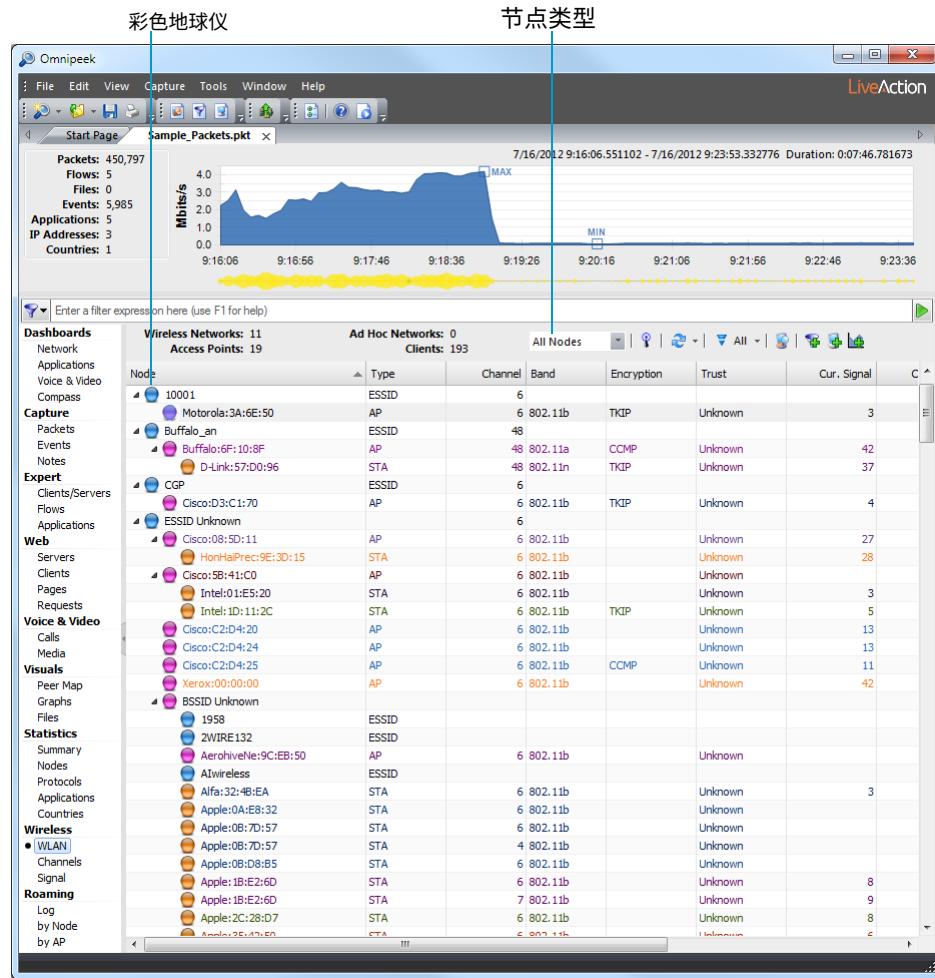
要查看捕获窗口的节点统计信息，请选择 节点在捕获窗口的导航窗格中。



**提示** 双击某个节点可查看有关所选节点的活动及其使用的协议的更多详细信息（或右键单击该节点并选择节点详细信息）。

## WLAN 视图

当选择支持的无线适配器作为捕获适配器时，捕获窗口的 WLAN 统计信息可用。要查看捕获窗口的 WLAN 统计信息，请选择无线局域网在捕获窗口的导航窗格中。



这节点类型下拉列表可让您将显示限制为选定节点（所有节点，客户，接入点，服务集标识符，特别指定，行政，未知，和频道）。当 WLAN 层次结构视图按通道划分时，树的根分支是通道编号，其下方是单独的 WLAN 层次结构视图（ESSID、BSSID、节点等）。

这彩色地球仪通过颜色识别每个节点：

- 蓝色：ESSID
- 粉色：AP（接入点）或 Ad Hoc 等效项
- 橙色：STA 或客户端
- 灰色：管理员或其他未知人员
- 灰色带有（?）：特定节点的迹象相互矛盾或出乎意料。

## 使用对等映射

这同行地图Omnipeek 和 Capture Engines 中的视图是一款功能强大的工具，可用于在捕获窗口中可视化网络流量。Peer Map 以图形方式显示在特定捕获窗口中检测到的所有节点或用户定义的子集。

节点之间的通信用线段表示。节点之间的线可以用颜色编码来显示使用的协议。线的粗细表示节点之间的流量。

### 同行地图视图

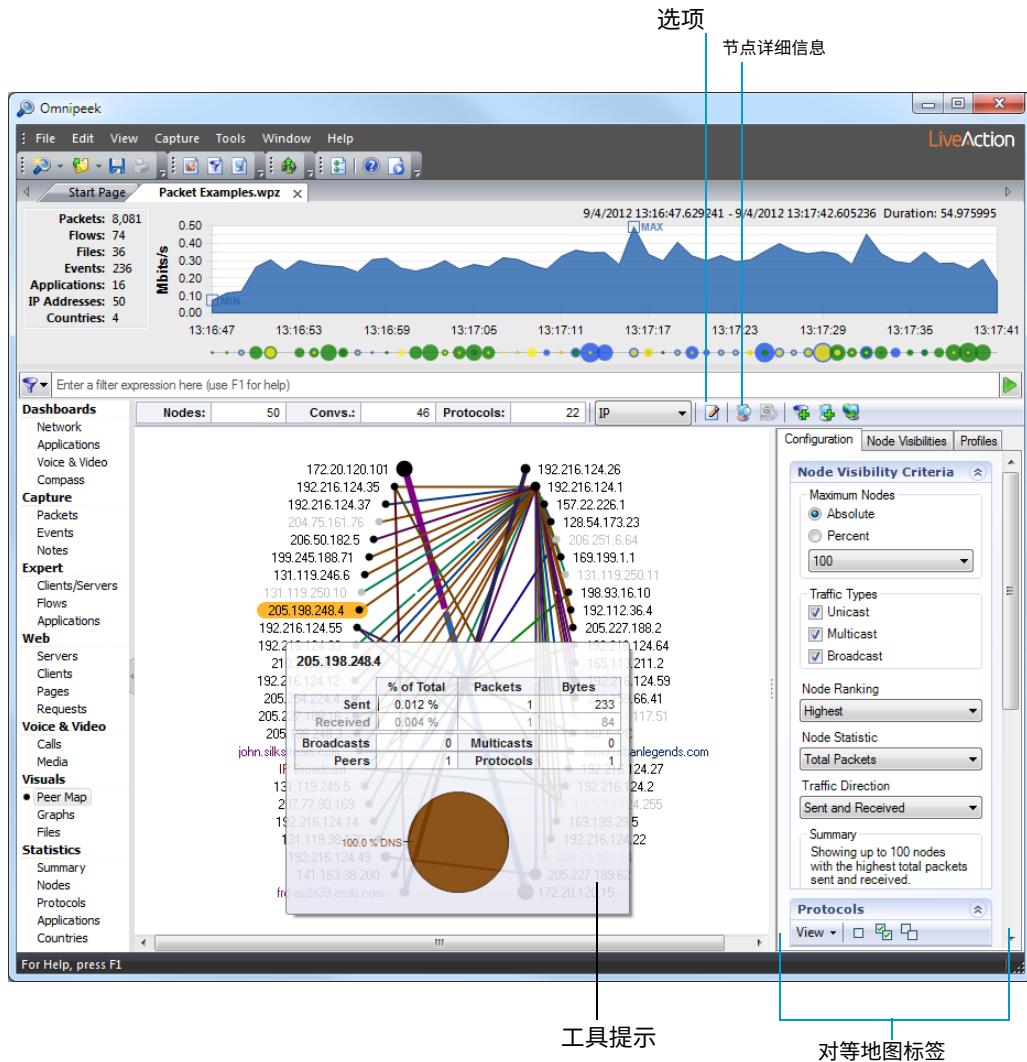
要显示对等地图：

1. 打开捕获窗口并开始捕获流量。
2. 在捕获窗口中，单击同行地图视图。节点对开始填充同行地图视图，其中的对话用连接线表示。

---

**提示** 将光标悬停在对等图上的特定节点上，即可查看包含有关此节点的更多信息的工具提示。您还可以将鼠标悬停在对话行上，以获取包含有关该对话的信息的工具提示。

---



**3.**点击**选项**打开对等映射选项对话框。此对话框允许您选择显示或隐藏可显示的节点类型图标（服务器、工作站等）、节点可见性和协议线段间隙。

**4.**点击**节点详细信息**查看有关此节点的统计信息。

**5.**使用右侧窗格中的**选项卡**配置 Peer Map 设置：

- 配置**：该选项卡可以设置Peer Map的基本参数，显示捕获窗口缓冲区中的哪部分流量，以及协议（线段）在Peer Map中的显示方式。
- 节点可见性**：此选项卡显示节点数以及对等图中显示和隐藏的节点。
- 个人资料**：此选项卡可让您将设置配置到配置文件中，以控制对等地图的外观和布局。

**6.**右键单击节点可以查看其他选项，包括：

- 安排**：如果通过将节点拖拽到新位置而改变了对等地图的外观，此选项会将节点重新排列到对等地图的椭圆形。
- 节点详细信息**：此选项将打开**详细统计**窗口并显示所选节点的详细信息。

# 键盘快捷键

捷径	描述
Ctrl + N	创建一个新的捕获窗口。
Ctrl + O	在新的捕获文件窗口中打开 OmniPeek 捕获文件或其他支持的文件类型。
Ctrl + S	打开 <b>节省</b> 对话框保存活动窗口中的所有数据包。
Ctrl + P	以适合其类型的格式打印活动窗口。
Alt + F4	退出 OmniPeek。
Ctrl + Z	撤消上次编辑。
Ctrl + X	剪切突出显示的项目并复制到剪贴板。
Ctrl + C	将突出显示的项目复制到剪贴板。
Ctrl + V	粘贴剪贴板的当前内容。
Ctrl + B	从活动捕获窗口中删除所有数据包。
Ctrl + A	选择窗口中的所有数据包、文本或项目。
Ctrl + D	删除所有突出显示和选择。
Ctrl + E	打开 <b>选择</b> 对话框，您可以在其中使用过滤器、ASCII 或十六进制字符串、数据包长度和分析模块来选择捕获的数据包。
Ctrl + H	从显示中移除选定的数据包但不删除它们。隐藏的数据包不会被进一步处理。
Ctrl + Alt + Y	开始所有本地捕获。
Ctrl + Shift + H	从显示中移除未选中的数据包，但不删除它们。隐藏的数据包不会被进一步处理。
Ctrl + U	将所有先前隐藏的数据包恢复到正常状态。
Ctrl + G	打开 <b>转至</b> 对话框中，您可以选择要跳转到的数据包编号。如果选择了数据包，则会显示第一个选定数据包的编号。
Ctrl + F	寻找模式。
Ctrl + J	跳至下一个选定的数据包。
Ctrl + M	打开 <b>筛选器</b> 窗口。
Ctrl + L	打开 <b>日志</b> 窗口。
Ctrl + Y	切换数据包捕获功能。
Ctrl + Tab	使序列中的下一个窗口成为活动窗口。
Ctrl + Shift + Tab	使序列中的前一个窗口成为活动窗口。

捷径	描述
F1	启动在线帮助。
F11	在全屏窗口中显示 Omnipeek。

# 指数

## 一个

适配器选项：  
分析选项82  
阿普德克斯67  
应用程序性能指数（Apdex）67 应用程序视图69  
  
应用程序3, 23, 94, 四十四, 64, 75  
, 255 应用程序仪表板四十六 ASCII61

## 碳

通话质量3, 33, : 4, 449 通话质量分布四十八 通话摘要四十八  
呼叫利用率49  
通话量49  
呼叫与网络利用率3, 33, : 44 采集引擎2  
捕获窗口21  
连接7  
文件选项卡二十九  
取证标签三十二  
安装5  
采集引擎管理器5 捕获文件24

捕获选项对话框：  
适配器选项：  
常规选项：  
总体观点3, 33, : 44 捕获会话3, 63, 73, 878 捕获模板22  
捕获窗口：, 59  
新捕获22  
新的取证捕获22 新监视器捕获22 数据包视图59

频道5, 255  
指南针仪表板3, 4, : 5, 15, 758 国家5, 255  
当前活动，仪表板四十六

## 德

仪表板  
应用程序四十六  
罗盘4:  
网络四十五  
时间线43  
语音和视频四十八 数据速率5, 255 详细信息选项卡三十八  
DNS 服务器二十七  
领域8

## 埃

事件标记54  
EventFinder 设置6, 768 事件52  
事件时间表二十六  
事件，仪表板四十六  
专家6, 768

## 弗

文件选项卡二十九  
筛选63  
创建一个简单的过滤器65 启用过滤器63 插入过滤对话框65 制作过滤器命令64 拒绝匹配64

看法65  
流列表72  
流程图7, 274 流量5, 255  
法医搜索2, 92, : 3, : 45 取证捕获2, 22, 938 取证标签3, 238

## 格

常规选项：  
总体观点3, 33, : 44 图表入站/出站53 图形间隔54

图表类型53  
分组文件二十九

## 赫

十六进制视图61  
层次视图67  
主持人8  
HTML 报告51

## 我

入站53  
安装捕获引擎5 IP 地址8, 3, 24, 三十四, 四十四, 647 IPv6 地址3, 24, 346

## 大号

梯子7, 275  
传奇55  
局限性58

## 米

制作过滤器命令二十七  
映射配置文件83  
监视捕获22  
管理咨询委员会71

分析选项82  
捕获会话78  
创建项目76  
发动机78  
流列表72  
流程图7, 274 梯子  
7, 275  
映射配置文件83  
进步79  
项目77  
项目文件81  
项目窗口72  
段7:  
时间范围和过滤器77 巫师  
7, 677  
多段分析71

**否**

名称表2十七  
网络仪表板四十五  
网络取证二十九  
网络利用率图4: 新的取证捕获22  
新监视器捕获22 节点详细信息86

节点统计85  
节点类型图标5, : 88 节  
点5, 255

**俄**

全能派2  
Omnipeek 捕获:  
打开捕获文件24 OSI 层67

出站53  
概览图二十五

**磷**

数据包解码5:  
数据包视图59  
密码8  
暂停/播放55  
对等图8, 788 物理地址3, 24  
, 346 港口8

项目文件81  
协议3, 33, 95, 255

**R**

原始数据包数据61 拒绝  
匹配64  
解析名称二十七

**年代**

选择相关数据包5, 158  
选择结果对话框58 会议3, 738

会议三十六  
滑块控件54  
开始捕获2, 123 开始  
页5  
统计数据85  
停止捕获2, 123 存储  
标签三十七  
简要通话四十八  
摘要信息二十六  
同步文件二十九

**电视**

时间范围和过滤器77 时间范  
围指示器54  
时间窗口选择控件54 时间线仪表板43

**时间线图3, 344 时间线**

选项卡三十六  
热门应用3, 23, 94, 四十四, 64, 755  
热门频道5, 255 排名靠前的国家55

最高数据速率55 顶部流量5  
, 255 顶级节点5, 255 顶  
级协议3, 33, 955

按 IP 地址划分的热门协议4, 四十四, 647 顶  
级谈话者三十九

按 IP 地址划分的顶级谈话者3, 24,  
346 顶级 VLAN5, 255 顶部 WLAN5,  
255

**乌**

单位52  
用户名8

**五**

视图类型四十四  
虚拟局域网5, 255  
语音和视频仪表板四十八 音量,  
呼叫49

**西**

无线局域网4  
无线信号四十六  
无线局域网5, 255

**是**

放大53  
缩小53