KEDACOM 苏州科达科技有限公司
Suzhou Keda Technology Co.,Ltd.

关于 Wireshark 的基础使用说明

（仅供内部使用）

版　本　号：	V0.1
保 密 等 级：	■秘密　□机密　□绝密
编 制：	胡懿敏
审 核：	王磊

修订记录

日期	版本号	描述	作者
2010-8-26	0.1	初稿完成	胡懿敏
2010-8-27	1.0	校订完成	王磊

目录

	关于 **Wireshark** 的基础使用说明	■秘密 □机密 □绝密

关键词：

Wireshark、显示过滤、捕获过滤、抓包文件保存、音视频动态载荷、QoS设置确认

摘 要：

本文简要说明了 Wireshark 的基本使用方法，如捕获过滤条件的设置、显示过滤条件的设置以及根据显示内容保存抓包文件的方法，并列举了一些我们目前常用的过滤条件的描述方法，同时还简单说明了一些通过抓包文件我们可以了解的一些内容。

1 案例描述

由于目前关于抓包工具的说明只有一些比较深入的，相对比较适合研发人员学习使用的文档，对于新入职的测试人员查看这类文档会感觉无从入手。

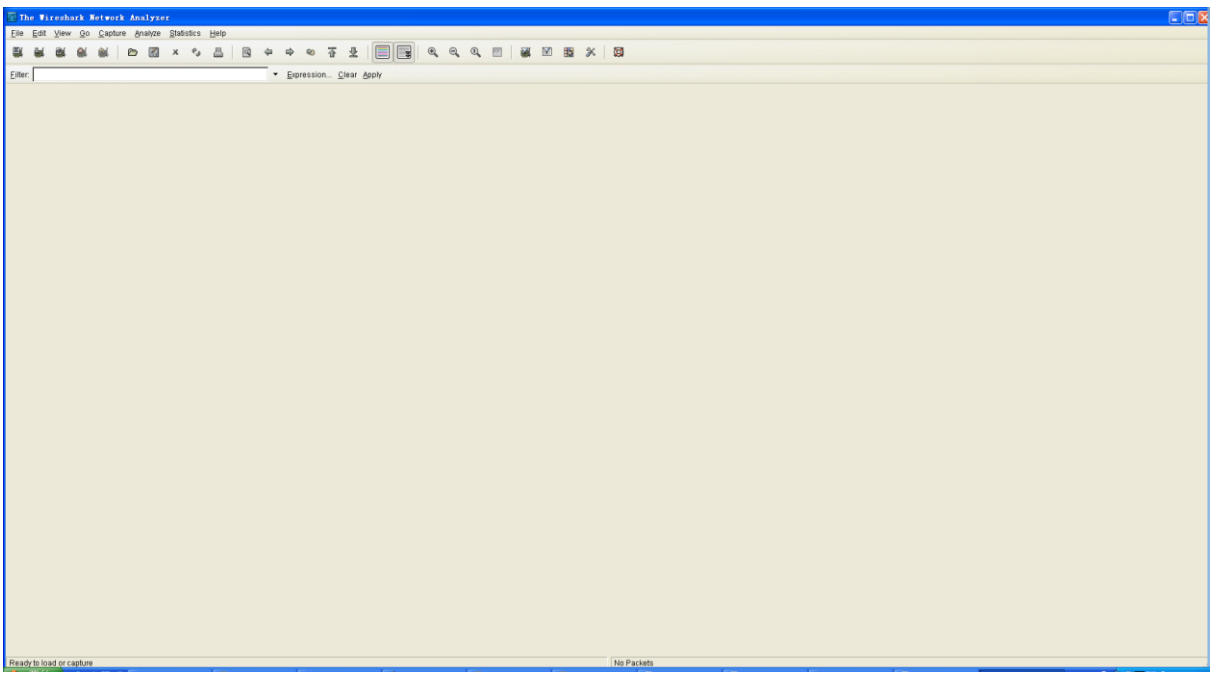
2 案例分析

新入职的测试人员原来对视频会议系统本身就了解不深，再加上对网络协议也只是一些表面上的学习、了解，而以前可能从未使用过此类工具，因此，他们首先需要了解的是此工具的基本使用，而不是对码流的深入分析，只有了解了此工具的基本使用方法，才可以使其在使用的过程中深入学习、了解该工具的使用。

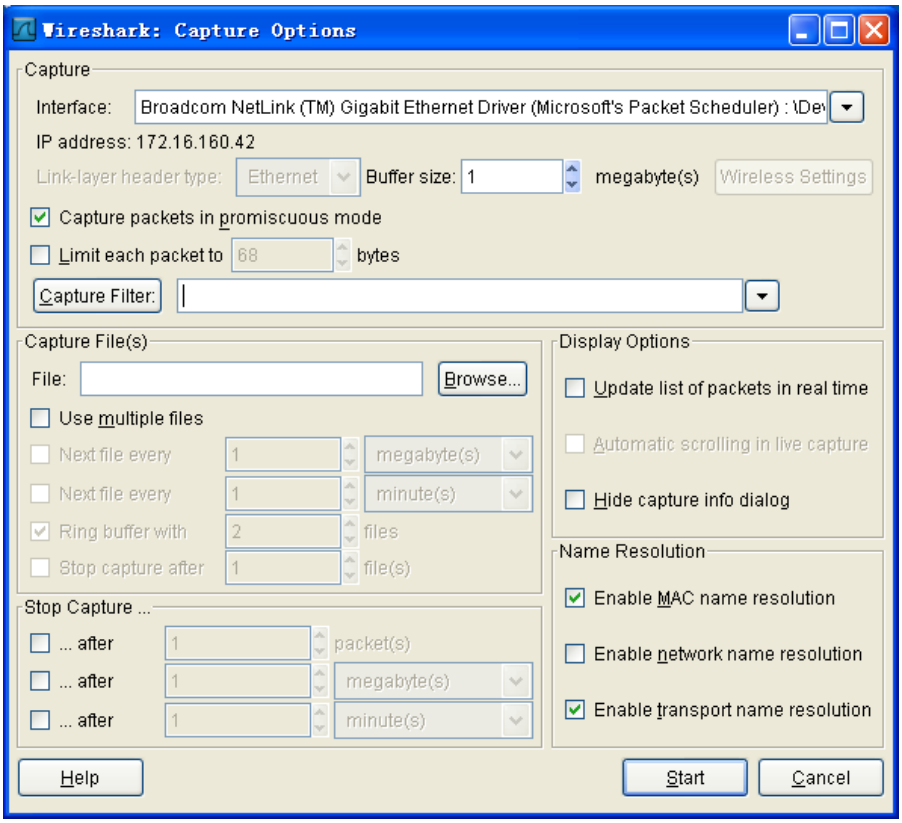
3 解决过程

基于上述考虑我将针对 Wireshark 的基本使用在此进行说明，方便初次使用 Wireshark 的人员进行学习。

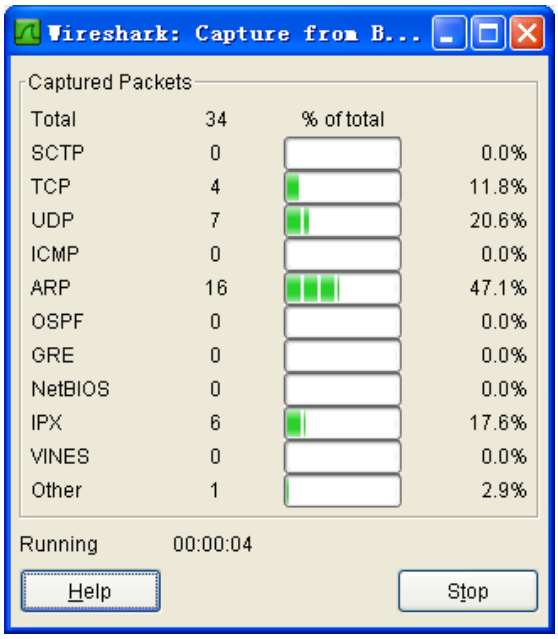
鉴于大家都是学计算机的我相信对于此软件的安装都是没有问题的，只需双击安装包即可，安装完成后，直接打开 Wireshark，界面如下：



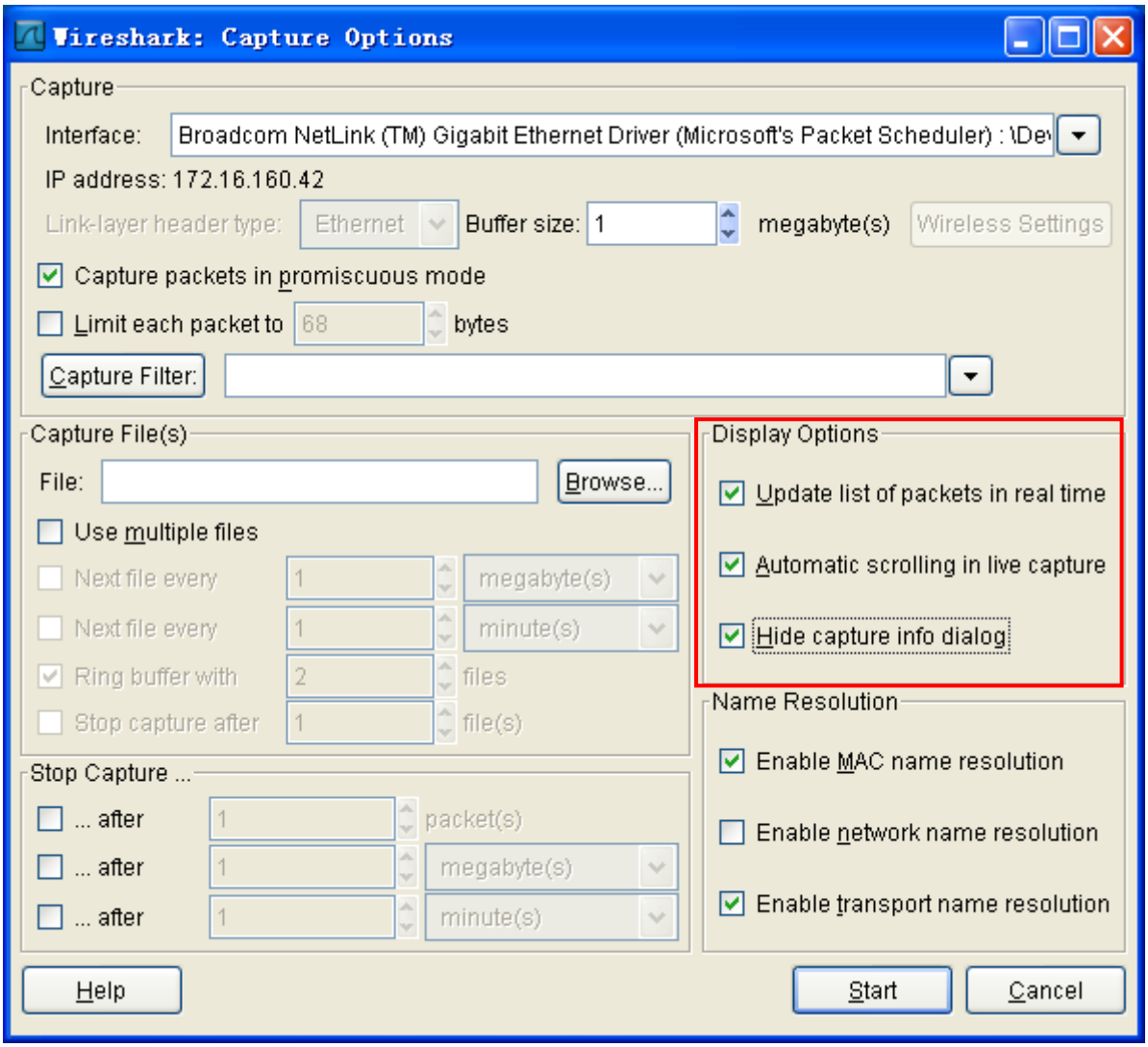
选择“Capture→Options…”就会弹出抓包的选项如下：



在此需要选择要使用的网卡，例如我的是“Broadcom NetLink（TM） Giabit Ethernet Driver（Microsoft’s Packet Scheduler)”，然后点击“Start”就开始抓包，点击“Stop”就停止抓包。

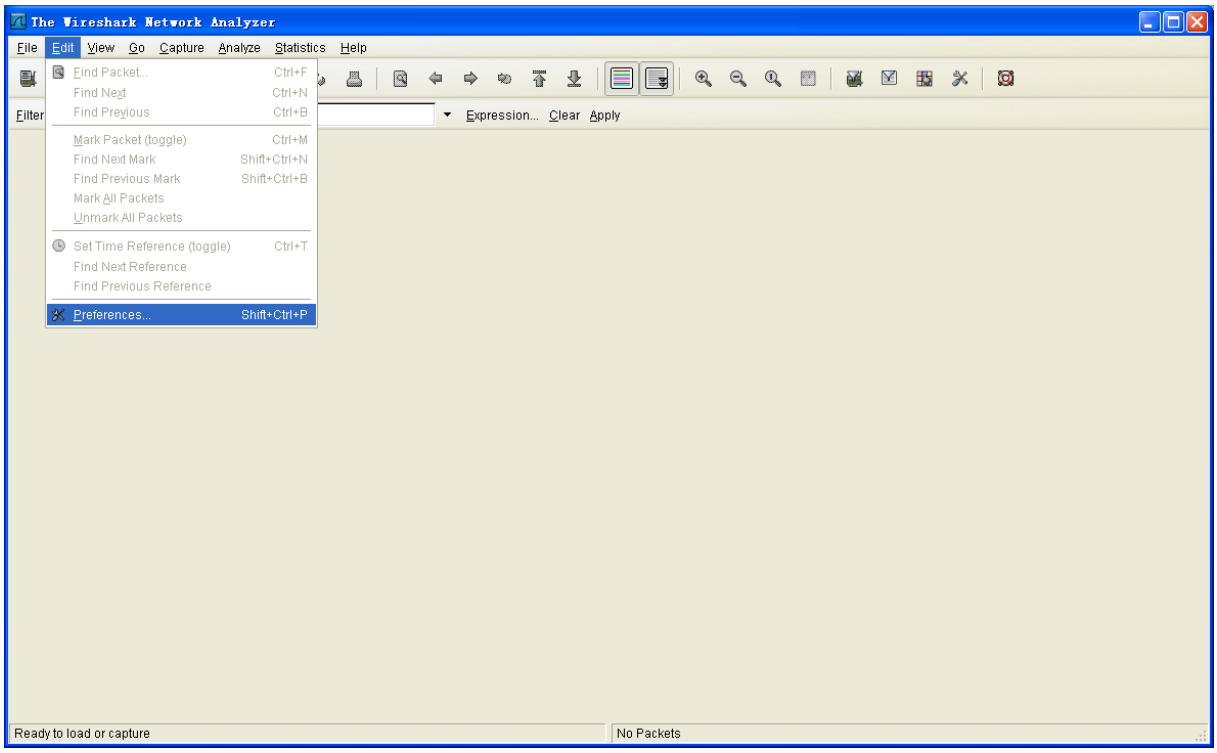


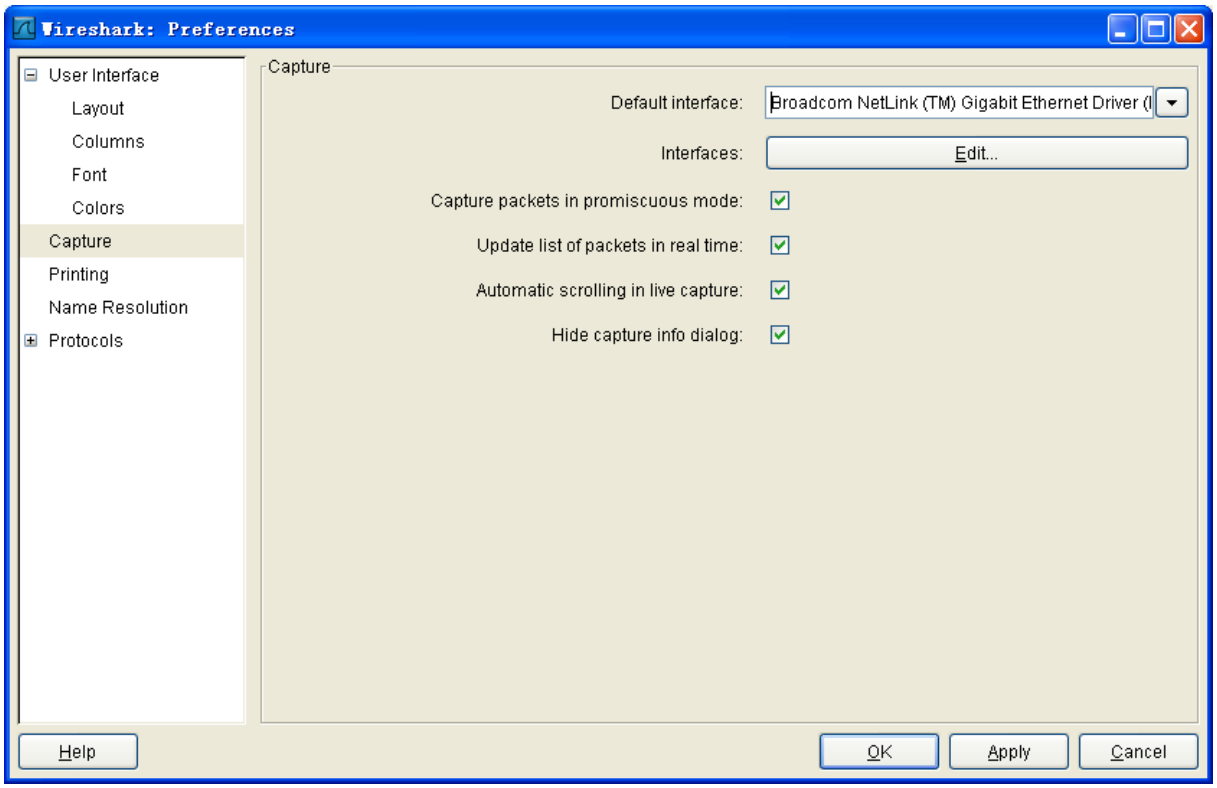
Wireshark 有两种显示方式，一种是默认的在抓包时显示捕获包的数量的统计数据，在停止捕获后显示分析好的捕获数据；另一种是实时分析和显示捕获的数据，此显示方式需要在抓包前，在抓包选项的 Display Options 中勾选“Update list of packet in real time”。（注：Automatic scrolling in live capture 选中此项是指抓包的时候自动滚动到最后的数据；Hide capture info dialog 选中此项是指不显示捕获包的数量的统计数据）



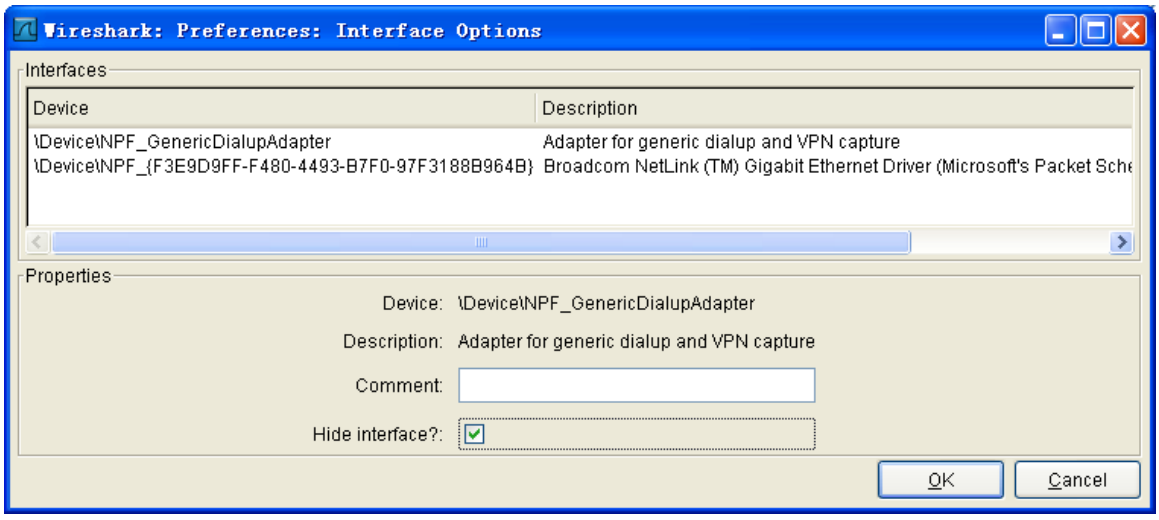
对于大多数只有一个网卡的主机，我们可以通过设置简化上述操作。

选择“Edit→Preferences…”就会弹出如下设置对话框，然后选择“Capture”

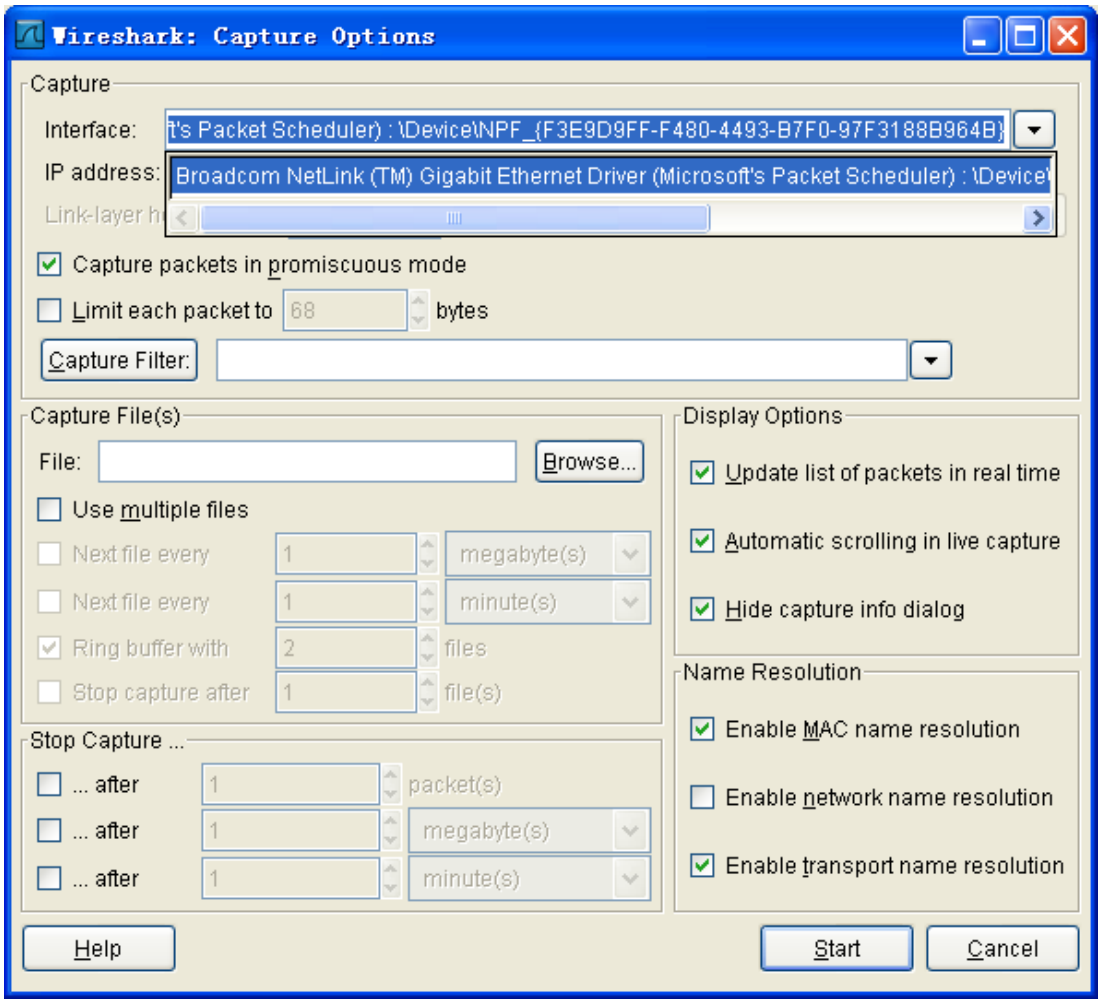




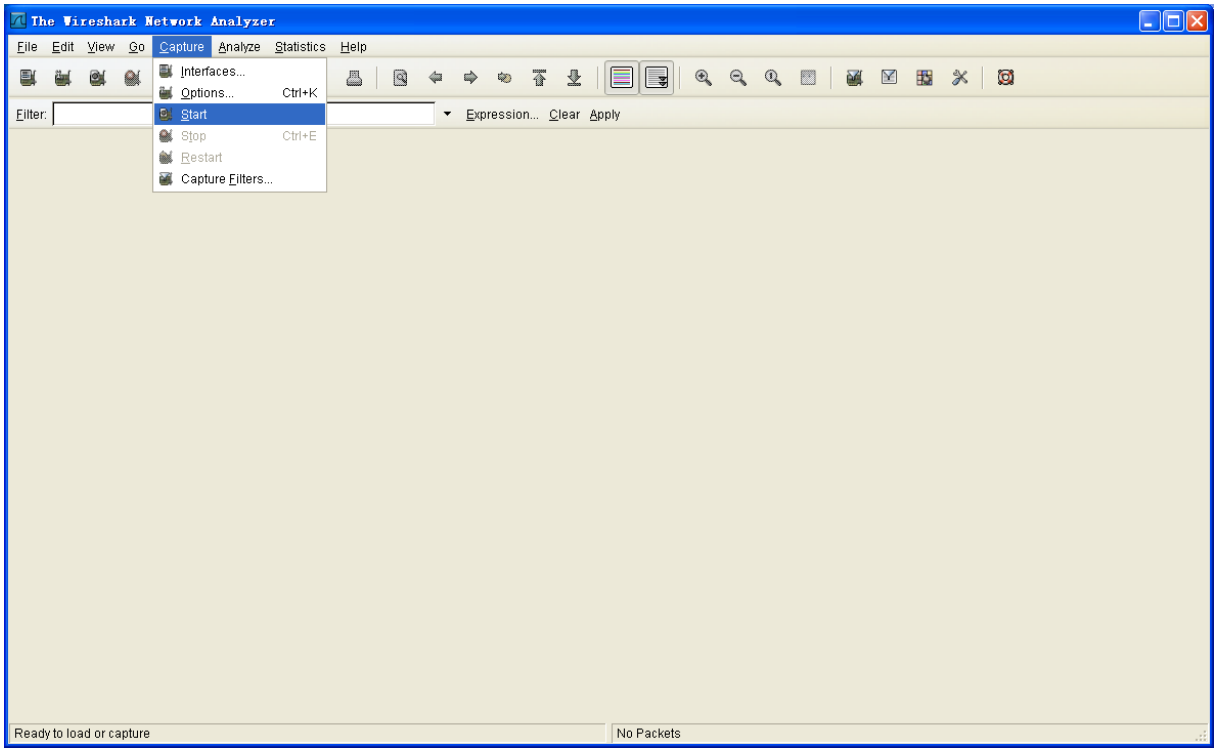
在 Default interface 中选择实际的网卡，点击“Edit…”勾选“Hide interface?”可隐藏不使用的网卡。



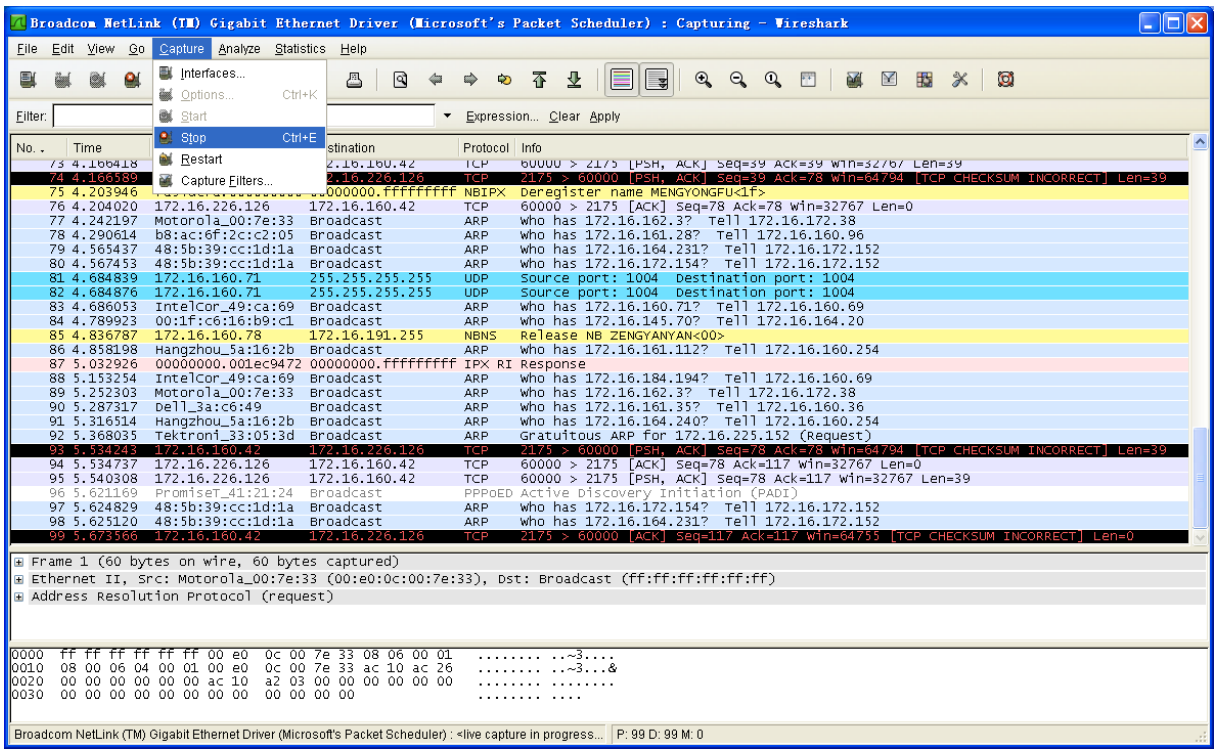
通过这样设置以后，我们可以在抓包选项的 Interface 中看到只有一个我们实际使用的网卡了，这样我们就可以更简单的开始/停止抓包了：



选择“Capture→Start”即可开始抓包



选择“Capture→Stop”即可停止抓包



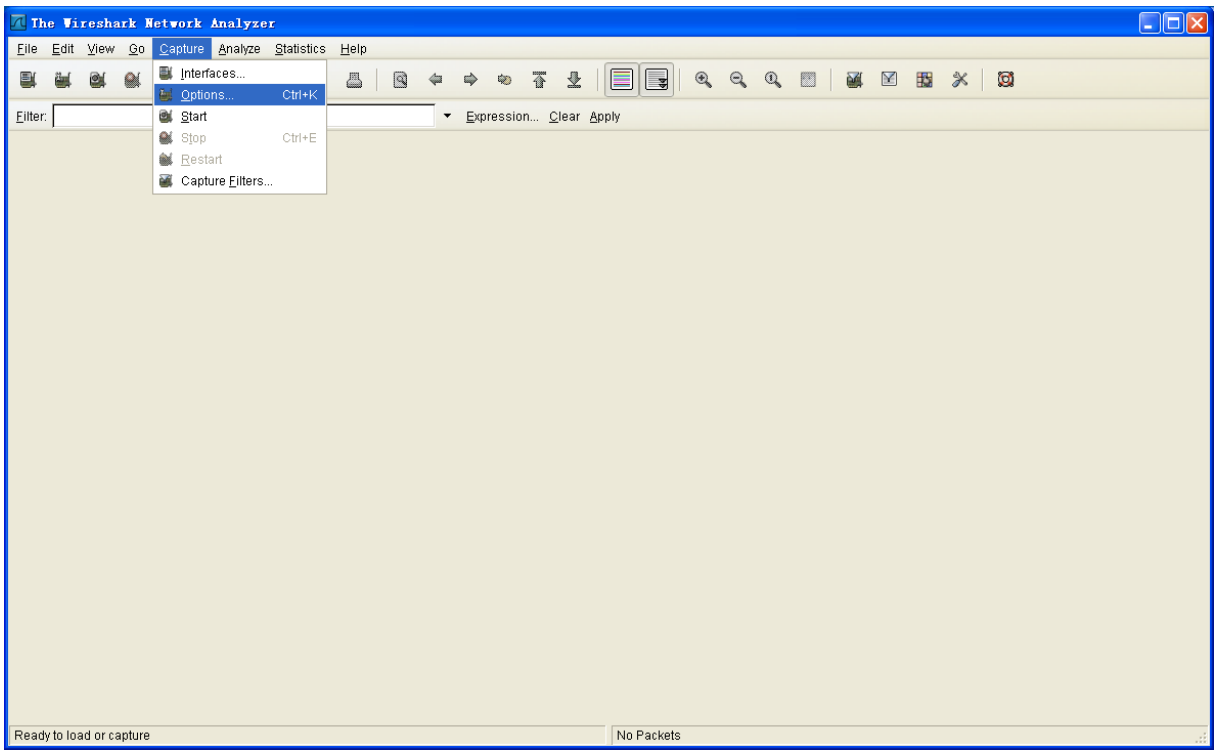
说明：在抓包过程中可以通过选择“View→Automatic scroll in live capture”来停止/开启自动滚

动。

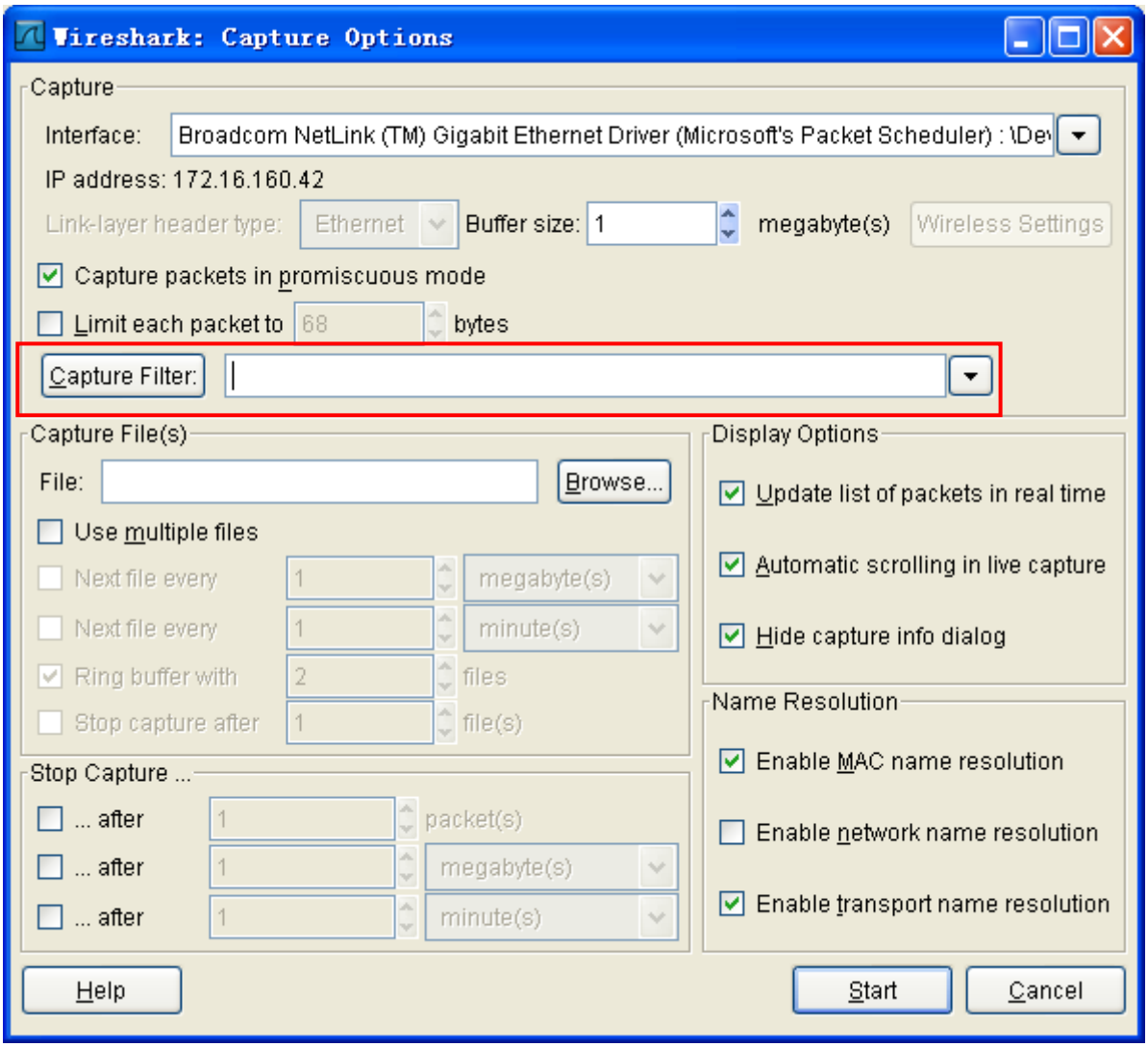
对于捕获到的数据我们往往只关心其中的一部分数据，这样就需要我们对所捕获到的数据进行过滤。Wireshark 提供两种过滤器，一种是抓包过滤器，一种是显示过滤器。抓包过滤器是数据经过的第一层过滤器，它用于控制捕捉数据的数量，以避免捕捉过多数据不便于查询；显示过滤器是一种更为强大（复杂）的过滤器。它允许您在已捕获的数据文件中迅速准确地找到所需要的数据记录，下面我们将对这两种过滤器的使用及语法进行简要的介绍。

首先说一下抓包过滤器，设置抓包过滤器的步骤是：

- 选择 capture -> options。



- 填写“capture filter”栏或者点击“capture filter”按钮为你的过滤器起一个名字并保存，以便在今后的抓包中继续使用这个过滤器。



- 点击开始（Start）进行抓包。

下面对抓包过滤器的语法做一下说明

语法	Protocol	Direction	Host(s)	Logical Operations	Other expression
例子	tcp	dst	172.16.160.42	and	tcp dst 10.2.2.2 3128

✧ Protocol（协议）

可能的值: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp.

如果没有特别指明是什么协议，则默认使用所有支持的协议。

✧ Direction（方向）

可能的值: src, dst, src and dst, src or dst

如果没有特别指明来源或目的地，则默认使用 "src or dst" 作为关键字。

例如，"host 10.2.2.2"与"src or dst host 10.2.2.2"是一样的。

✧ Host(s)

可能的值： net, port, host, portrange.

如果没有指定此值，则默认使用"host"关键字。

例如，"src 10.1.1.1"与"src host 10.1.1.1"相同。

✧ Logical Operations（逻辑运算）

可能的值：not, and, or.

否("not")具有最高的优先级。或("or")和与("and")具有相同的优先级，运算时从左至右进行。

例如，

“not tcp port 3128 and tcp port 23”与“（not tcp port 3128） and tcp port 23”相同。

“not tcp port 3128 and tcp port 23”与“not （tcp port 3128 and tcp port 23）”不同。

例子：

udp dst port 60040

显示目的 UDP 端口为 60040 的封包。

ip src host 172.16.226.126

显示来源 IP 地址为 172.16.226.126 的封包。

host 10.1.2.3

显示目的或来源 IP 地址为 10.1.2.3 的封包。

src portrange 60040-60042

显示来源为 UDP 或 TCP，并且端口号在 60040 至 60042 范围内的封包。

not imcp

显示除了 icmp 以外的所有封包。（icmp 通常被 ping 工具使用）

src host 172.16.226.126 and not dst net 172.16.160.42/16

显示来源 IP 地址为 172.16.226.126，但目的地不是 172.16.160.42/16 的封包。

(src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst portrange 200-10000 and dst net 10.0.0.0/8

显示来源 IP 为 10.4.1.12 或者来源网络为 10.6.0.0/16，目的地 TCP 端口号在 200 至 10000 之间，并且目的位于网络 10.0.0.0/8 内的所有封包。

上面主要说了抓包过滤器的使用方法并列举了一些常用的过滤条件，接下来再说一下显示过滤器的使用。

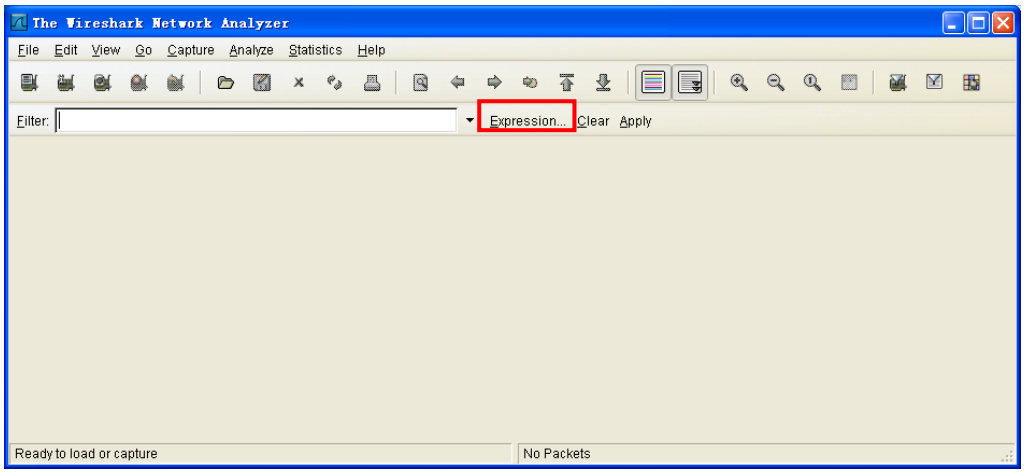
通常经过抓包过滤器过滤后的数据还是很复杂。此时你可以使用显示过滤器进行更加细致的查找。它的功能比抓包过滤器更为强大，而且在你想修改过滤器条件时，并不需要重新捕捉一次。

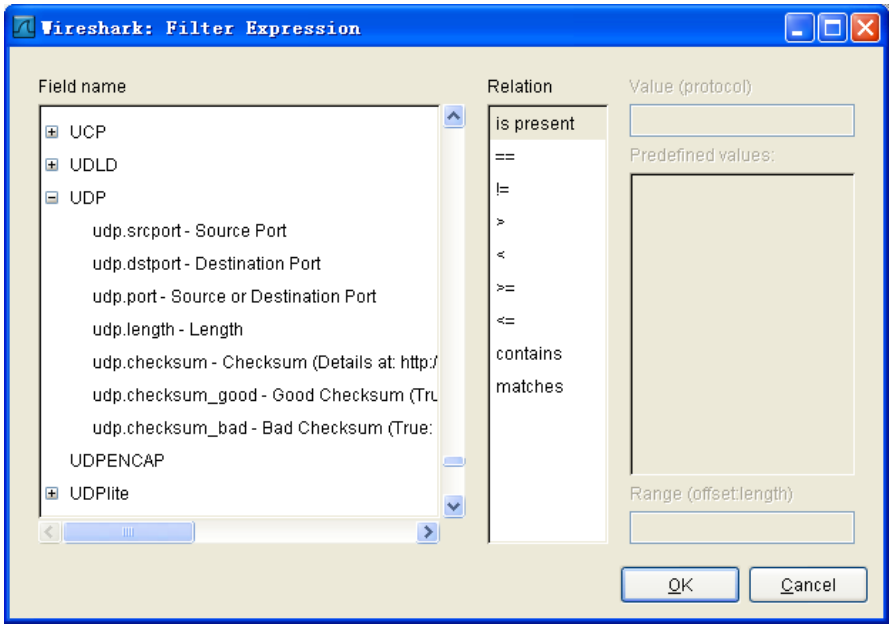
语法	Protocol	String 1	String 2	Comparison operator	Value	Logical Operations	Other expression
例子	udp	port	可选	==	60040	&&	ip.dst==172.16.160.42

✧ Protocol（协议）：

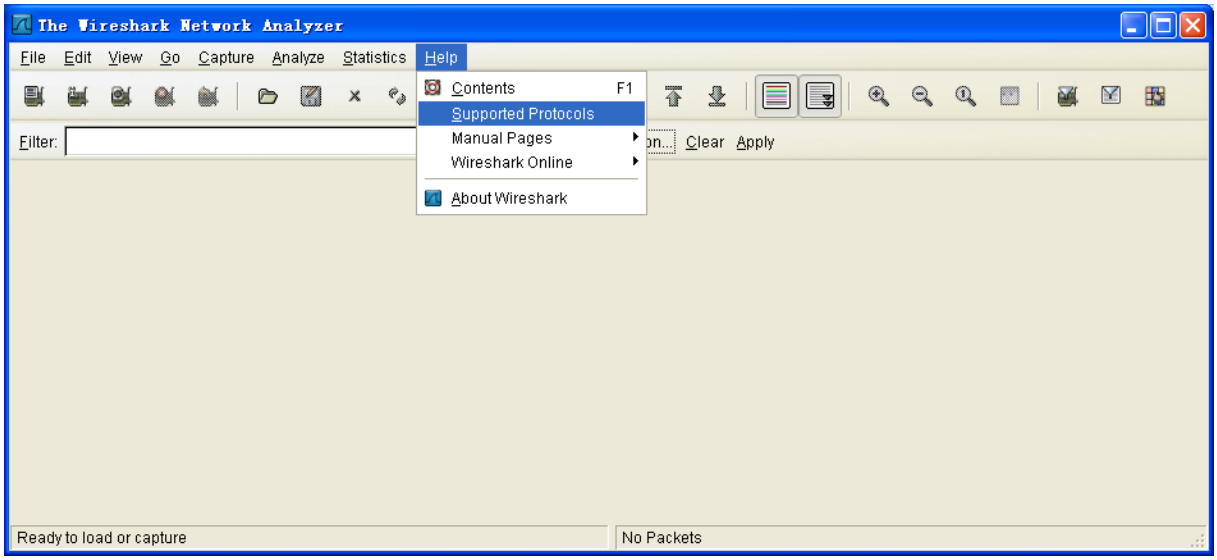
你可以使用大量位于 OSI 模型第 2 至 7 层的协议。点击"Expression..."按钮后，您可以看到它们。

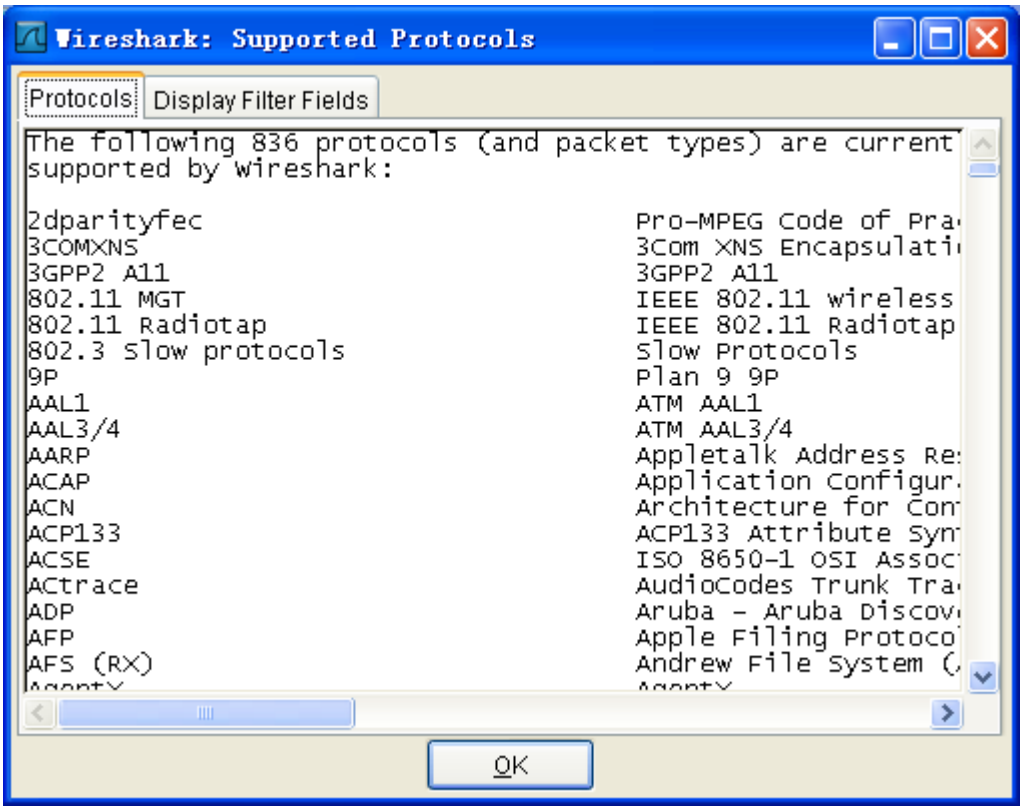
比如：IP，TCP，DNS，SSH





你同样可以在 Help 中找到所支持的协议

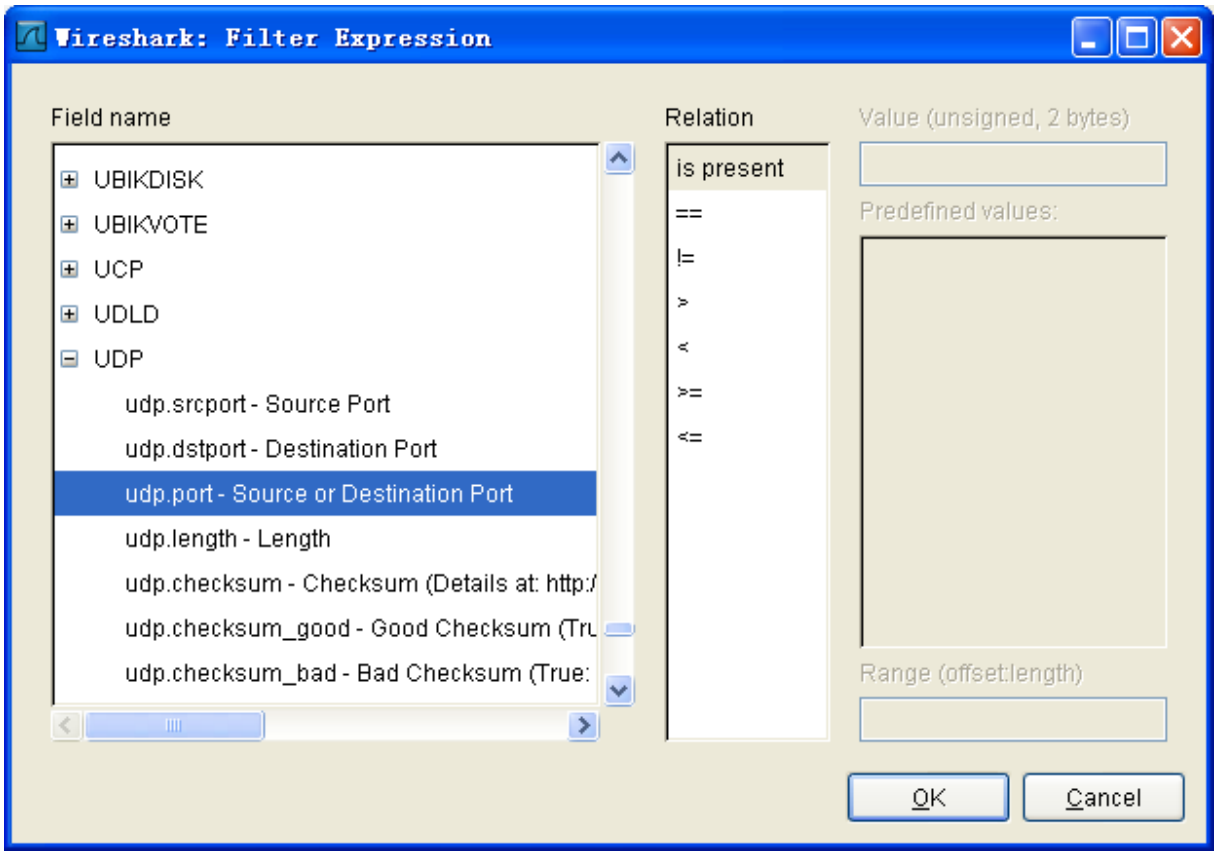




✧ String1, String2 (可选项):

协议的子类。

点击相关父类旁的"+"号，然后选择其子类。



✧ Comparison operators （比较运算符）：

可以使用 6 种比较运算符：

英文写法	C 语言写法	含义
eq	==	等于
ne	!=	不等于
gt	>	大于
lt	<	小于
ge	>=	大于等于
le	<=	小于等于

✧ Logical expressions（逻辑运算符）：

可以使用 4 种逻辑运算符：

英文写法	C 语言写法	含义
and	&&	逻辑与

or	||	逻辑或
xor	^^	逻辑异或
not	!	逻辑非

被程序员们熟知的逻辑异或是一种排除性的或。当其被用在过滤器的两个条件之间时，只有当且仅当其中的一个条件满足时，这样的结果才会被显示在屏幕上。

让我们举个例子：

“tcp.dstport 80 xor tcp.dstport 1025”

只有当目的 TCP 端口为 80 或者来源于端口 1025（但又不能同时满足这两点）时，这样的封包才会被显示。

例子：

h225 || h245

显示 h225 或 h245 的信令数据，通过此过滤方式可以只显示呼叫建立和释放的包信息

ip.src==172.16.226.126

显示数据包源的 IP 地址为 172.16.226.126 的所有信息，通过此过滤方式可只显示 IP 地址为 172.16.226.126 的主机所发出的所有数据包

ip.dst==172.16.160.42

显示数据包目的 IP 地址为 172.16.160.42 的所有信息，通过此过滤方式可只显示 IP 地址为 172.16.160.42 的主机所收到的所有数据包

udp.srcport==60048

显示 udp 包源端口地址为 60048 的所有信息，通过此过滤方式可只显示源端口地址为 60048 所发出的所有 udp 包

udp.dstport==60042

显示 udp 包目的端口地址为 60042 的所有信息，通过此过滤方式可只显示目的端口地址为 60042 所收到的所有 udp 包

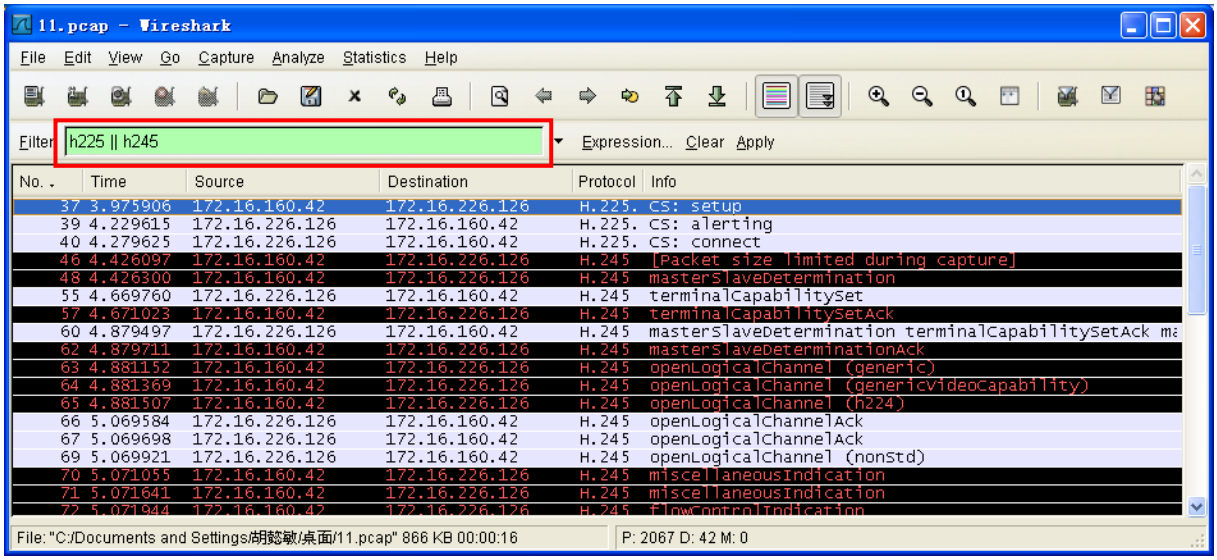
ip.src==172.16.226.126 && udp.srcport==60048

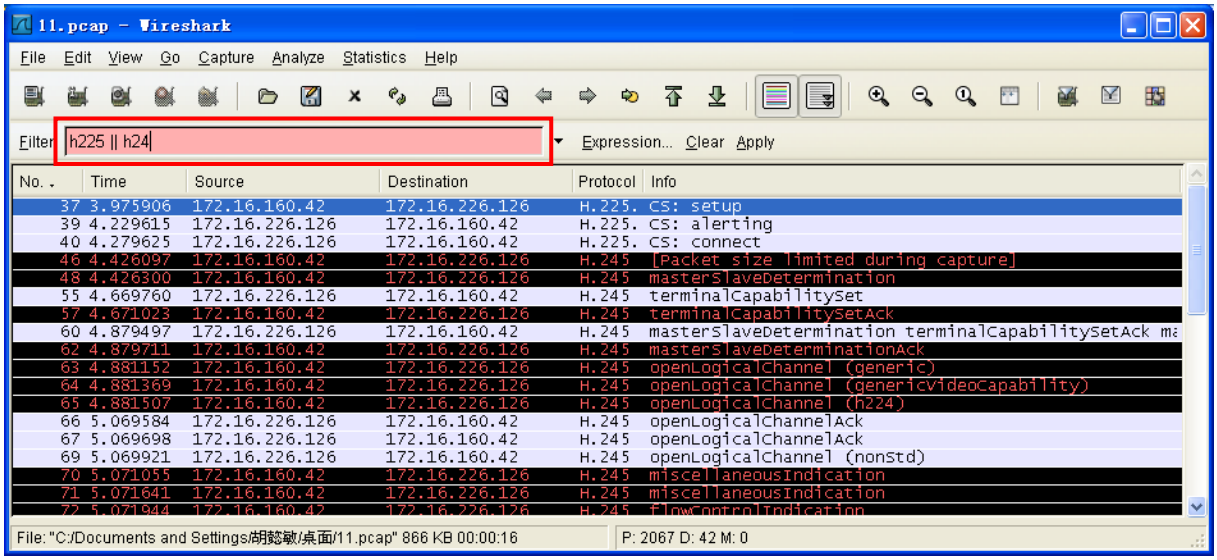
显示数据包源的 IP 地址为 172.16.226.126 并且 udp 包源端口地址为 60048 的所有信息，通过此过滤方式可只显示 IP 地址为 172.16.226.126 的主机且由其 60048 端口所发出的所有 udp 包

ip.dst==172.16.160.42 && udp.dstport==60042

显示数据包目的 IP 地址为 172.16.160.42 并且 udp 包端口地址为 60042 的所有信息，通过此过滤方式可只显示 IP 地址为 172.16.160.42 的主机且由其 60042 端口所收到的所有 udp 包

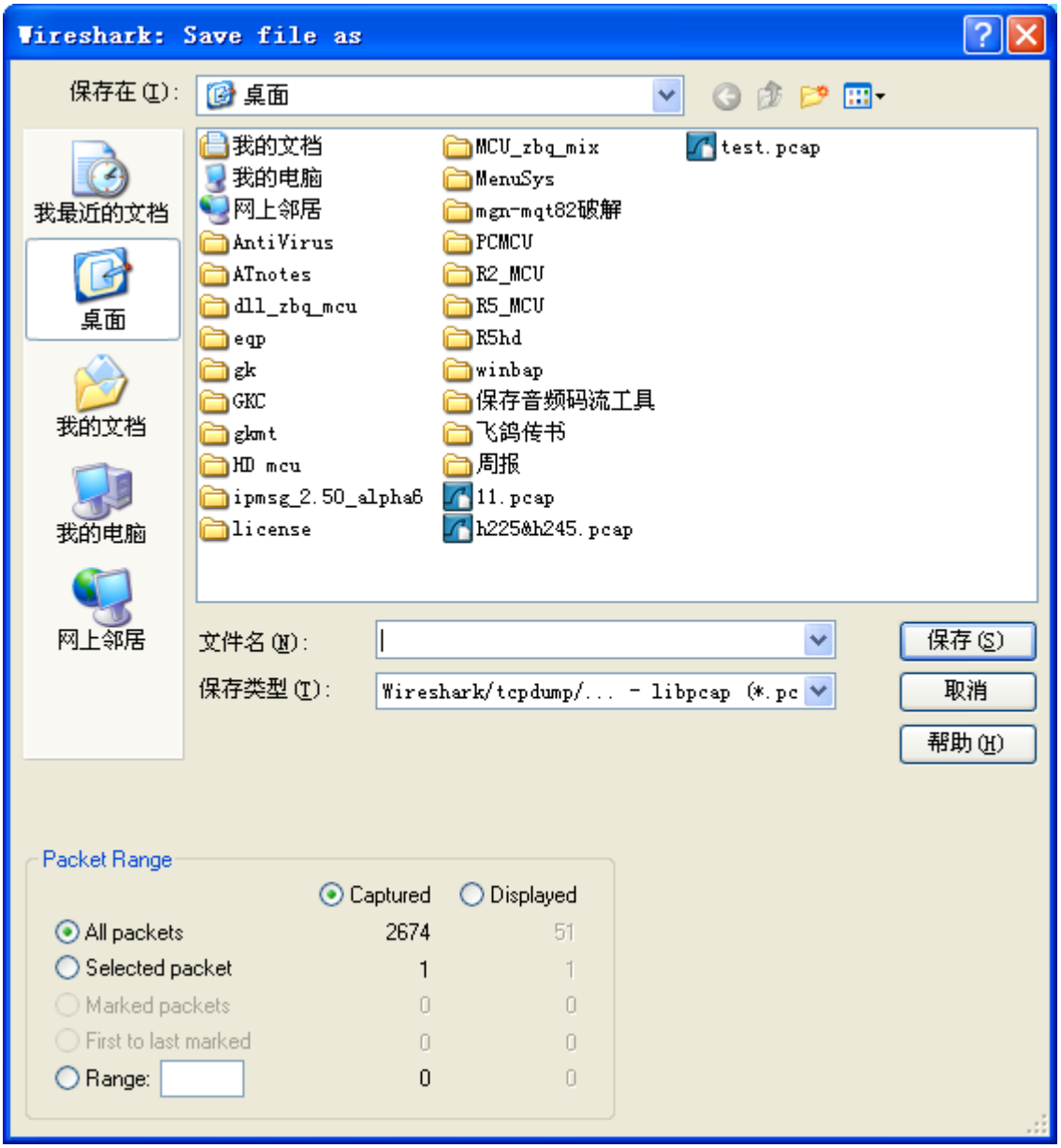
如果过滤器的语法是正确的，表达式的背景呈绿色。如果呈红色，说明表达式有误。



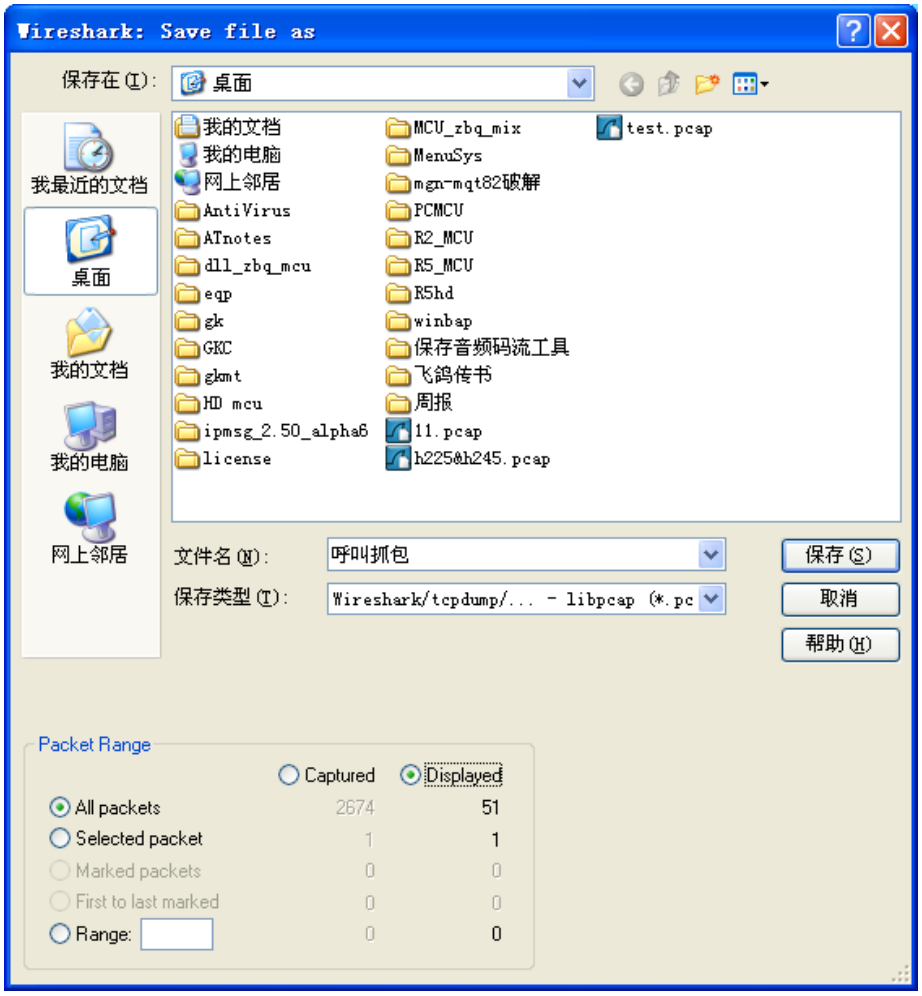


为了便于分析及节省存储空间，我们可以只保存符合我们过滤条件的包，具体方法如下：

完成显示过滤条件的设置并进行过滤，然后选择 File→Save As…，系统打开保存对话框，如下图所示：

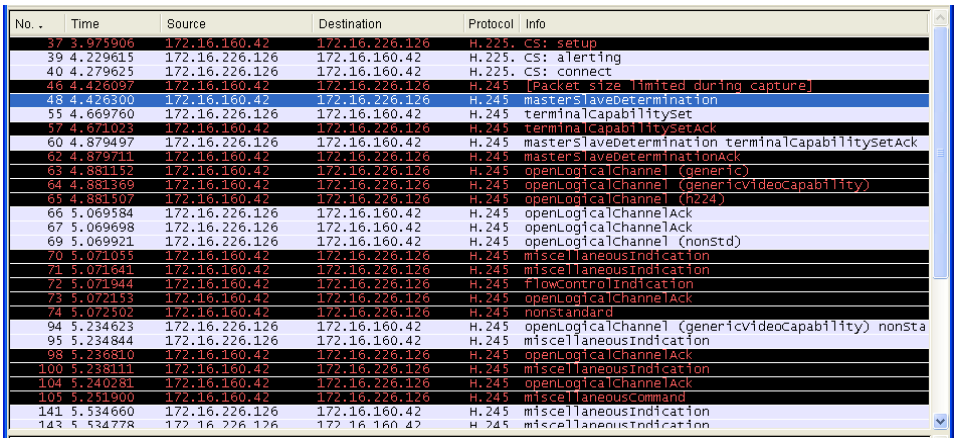


在上图所示对话框中设置该抓包文件保存的文件名，并选中“Displayed”然后点击“保存”按钮即可。

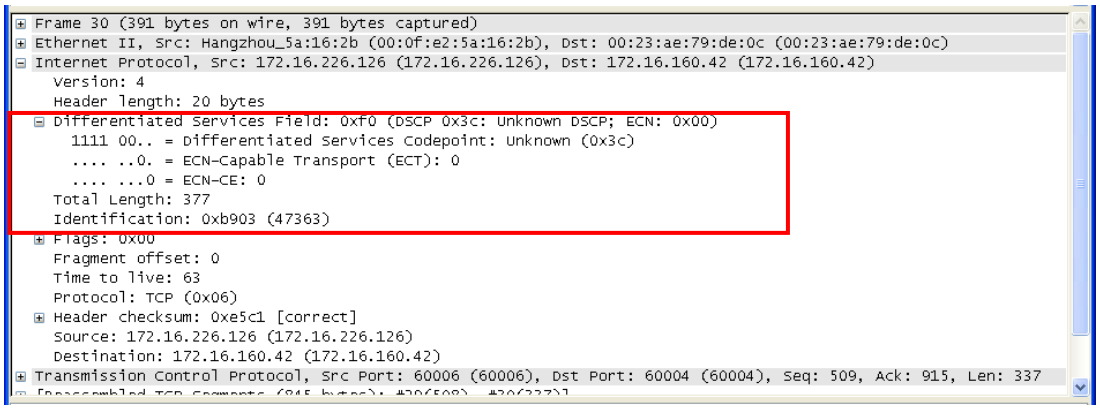


上面主要说了如何通过 Wireshark 进行抓包以及对所捕获的数据包如何进行过滤和保存，下面针对我们所捕获到的数据包中所包含的我们所关心的一些常规信息做一下简要的说明。

下图显示的是封包列表显示区中显示的内容，在此区域中你可以看到满足你显示条件的数据包的发送和接收端的 IP 地址、协议及该数据包的基本信息。

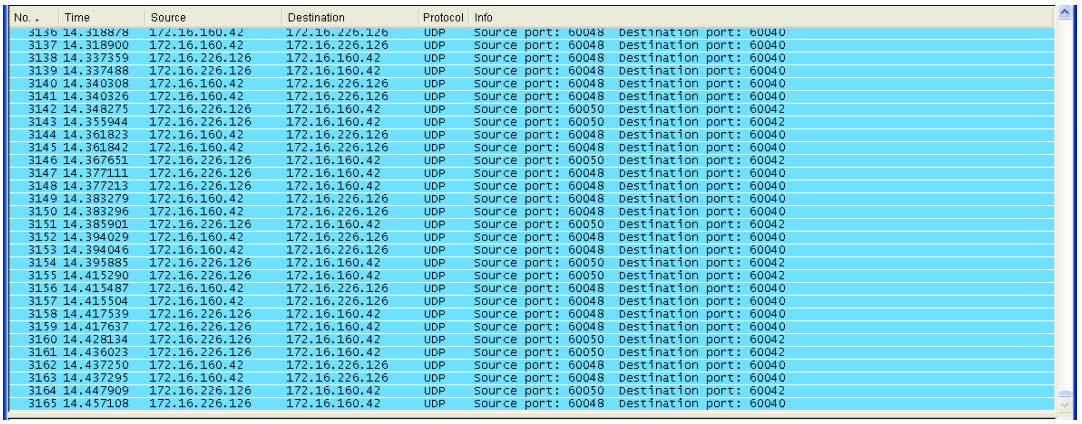


下图显示的是在封包列表显示区中你所选中的某一个封包的详细内容，所有信息按照不同的 OSI layer 进行了分组，您可以展开每个项目查看，如下图红框标示部分显示的就是此终端的 QoS 设置情况为：信令服务等级为 7 并启用最小延迟。

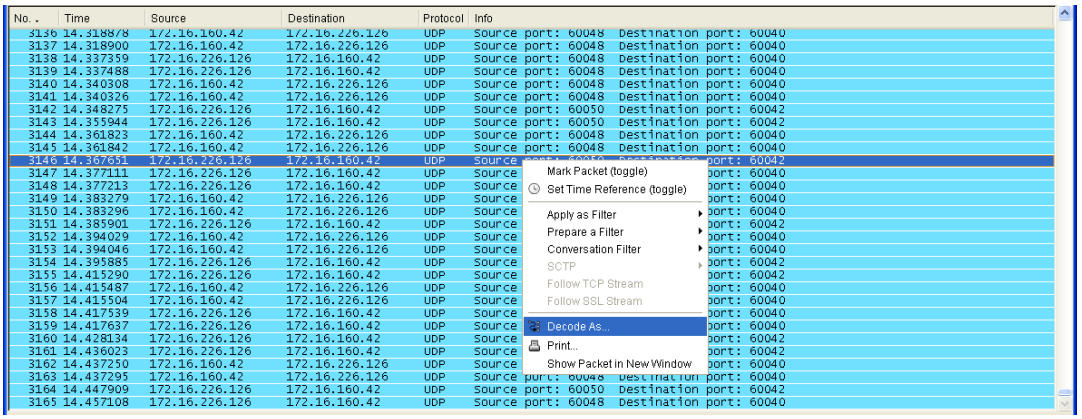


对于不同的数据包中包含的 Differentiated Services Field 字段信息的分析可以确认 QoS 中对于音频包、视频包、数据包及信令包的服务等级，对于区分服务而言该字段的最后两位不启用，使用其前六位以二进制的方式表示其 0~63 中各级服务等级，对于 IP 优先而言该字段的最后一位不启用，使用其前七位，其中第一至第三位以二进制的方式表示其 0~7 中各级服务等级，后四位表示其使用的服务类型，第四位表示其是否启用最小延迟，第五位表示其是否启用最大吞吐量，第六位表示其是否启用最高可靠性，第七位表示其是否启用最小开销。

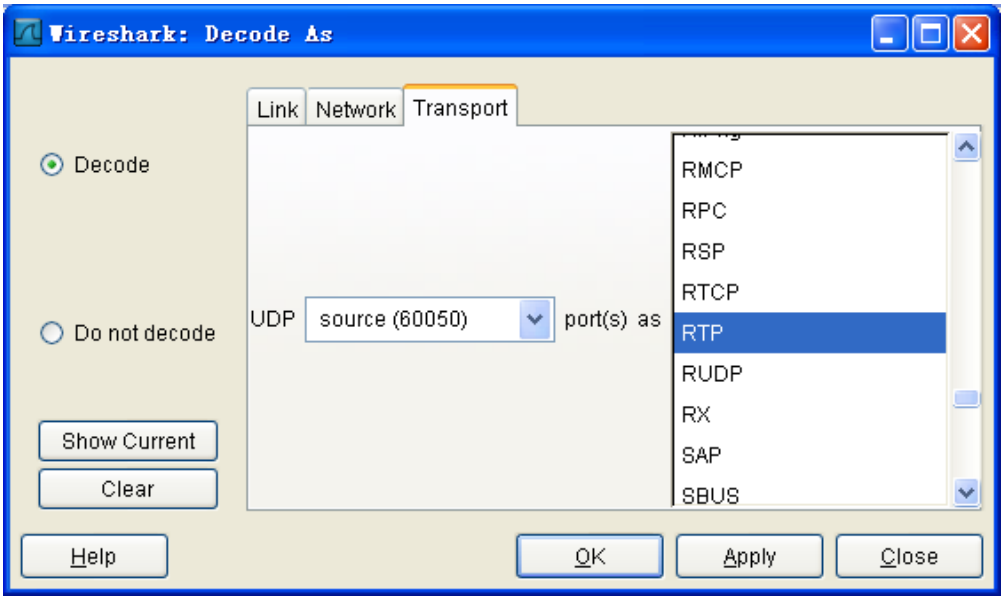
对于 UDP 包我们在封包列表区的 Info 列中可以了解源端口与目的端口的地址，如下图所示：



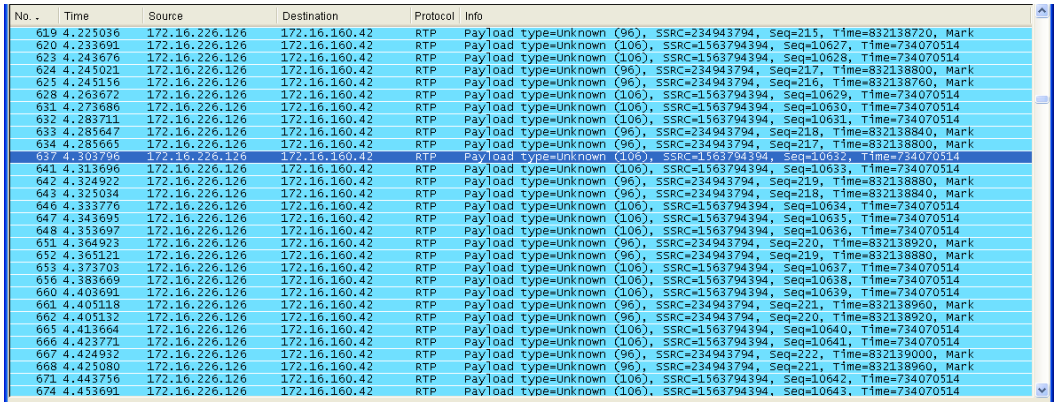
在上图所示的封包列表区选中你要进行协议转换的数据包然后点击鼠标右键显示如下图所示的快捷菜单：



点击“Decode As…”出现如图所示对话框：

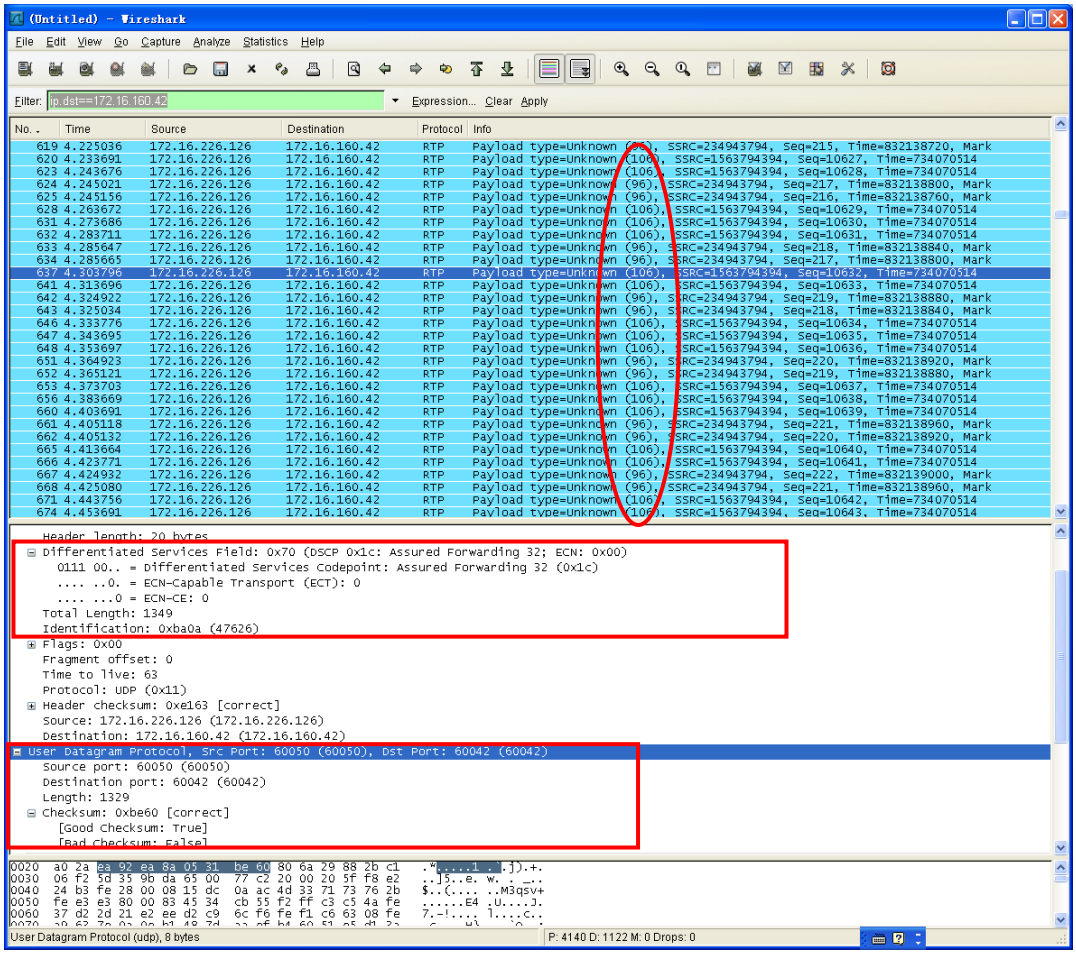


在上图所示的对话框的最右侧的列表中选中“RTP”然后点击“OK”即可完成转换，封包列表区即会显示如下图所示内容：

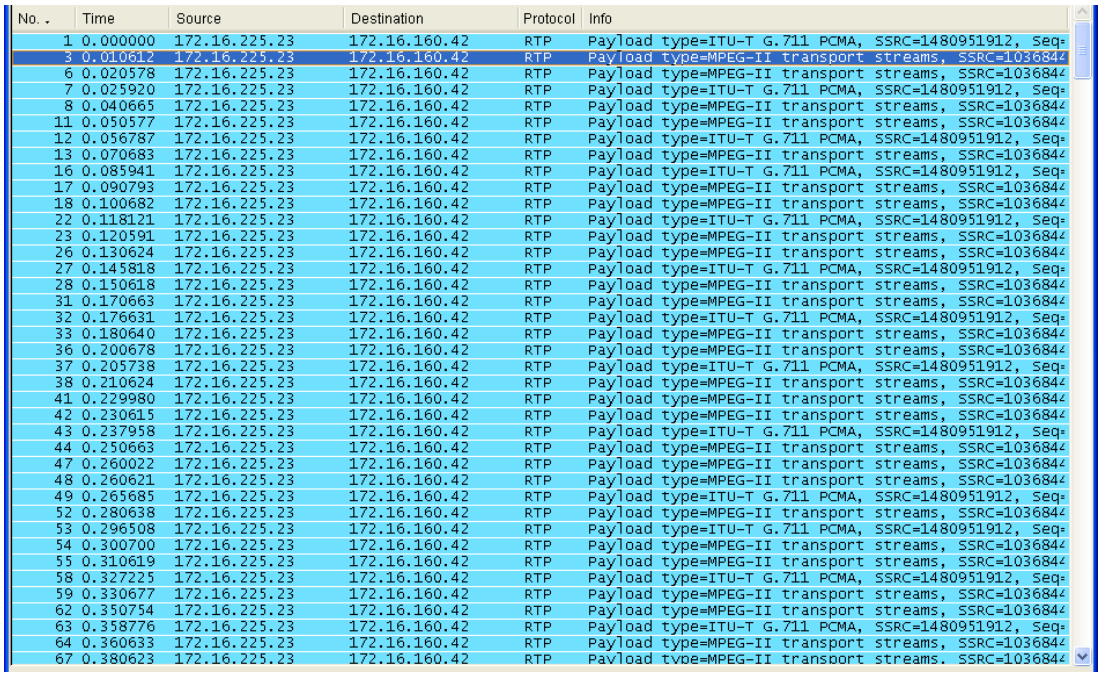


No.	Time	Source	Destination	Protocol	Info
619	4.225036	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=215, Time=832138720, Mark
620	4.233691	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10627, Time=734070514
623	4.243676	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10628, Time=734070514
624	4.245021	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=217, Time=832138800, Mark
625	4.245156	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=216, Time=832138760, Mark
628	4.263672	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10629, Time=734070514
631	4.273686	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10630, Time=734070514
632	4.283711	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10631, Time=734070514
633	4.285647	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=218, Time=832138840, Mark
634	4.285665	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=217, Time=832138800, Mark
637	4.303796	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10632, Time=734070514
641	4.313696	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10633, Time=734070514
642	4.324922	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=219, Time=832138880, Mark
643	4.325034	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=218, Time=832138840, Mark
646	4.333776	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10634, Time=734070514
647	4.343695	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10635, Time=734070514
648	4.353697	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10636, Time=734070514
651	4.364923	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=220, Time=832138920, Mark
652	4.365121	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=219, Time=832138880, Mark
653	4.373703	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10637, Time=734070514
656	4.383669	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10638, Time=734070514
660	4.403691	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10639, Time=734070514
661	4.405118	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=221, Time=832138960, Mark
662	4.405132	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=220, Time=832138920, Mark
665	4.413664	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10640, Time=734070514
666	4.423771	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10641, Time=734070514
667	4.424932	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=222, Time=832139000, Mark
668	4.425080	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (96), SSRC=234943794, Seq=221, Time=832138960, Mark
671	4.443756	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10642, Time=734070514
674	4.453691	172.16.226.126	172.16.160.42	RTP	Payload type=Unknown (106), SSRC=1563794394, Seq=10643, Time=734070514

通过上述转换我们即可在封包列表区看到当前 UDP 包是音频包还是视频包，以及该包的具体音频/视频格式，而在封包详细信息显示区中可了解该 UDP 包的 QoS 设置情况以及该 UDP 包的源端口和目的端口，如下图所示：

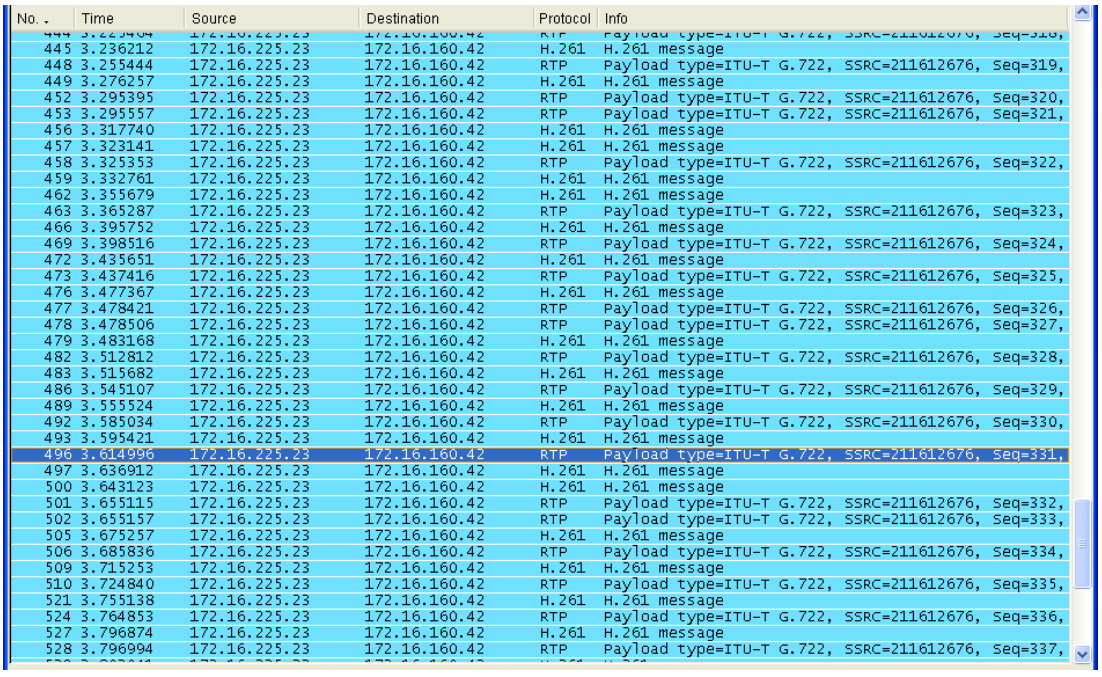


上图红色矩形框中标注的就是在封包列表区中选中的 UDP 包的 QoS 设置及其源端口和目的端口信息，而红色圆圈标注的就是各 UDP 包的音视频动态载荷值，通过该信息你可以了解相应的 UDP 包是音频包还是视频包及其具体的音视频格式，不过对于一些音视频格式在封包列表区的 Info 列中会直接显示其格式，如下图的音频：G711，视频：Mpeg2



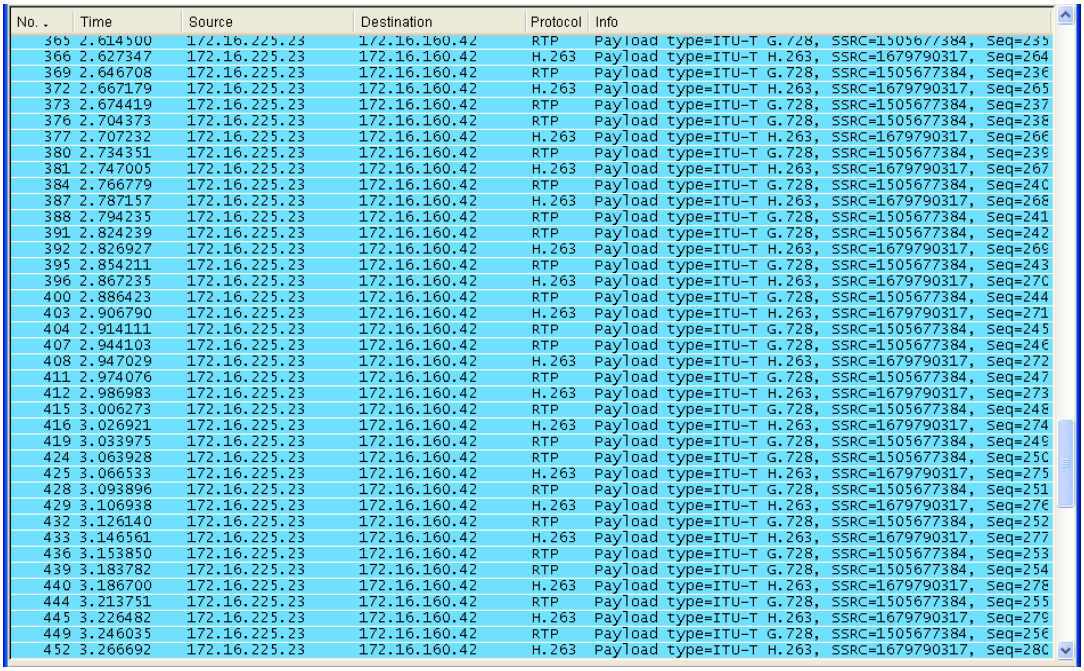
No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
3	0.010612	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
6	0.020578	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
7	0.025920	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
8	0.040665	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
11	0.050577	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
12	0.056787	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
13	0.070683	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
16	0.085941	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
17	0.090793	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
18	0.100682	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
22	0.118121	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
23	0.120591	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
26	0.130624	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
27	0.145818	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
28	0.150618	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
31	0.170663	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
32	0.176631	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
33	0.180640	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
36	0.200678	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
37	0.205738	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
38	0.210624	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
41	0.229980	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
42	0.230615	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
43	0.237958	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
44	0.250663	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
47	0.260022	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
48	0.260621	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
49	0.265685	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
52	0.280638	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
53	0.296508	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
54	0.300700	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
55	0.310619	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
58	0.327225	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
59	0.330677	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
62	0.350754	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
63	0.358776	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1480951912, Seq=
64	0.360633	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684
67	0.380623	172.16.225.23	172.16.160.42	RTP	Payload type=MPEG-II transport streams, SSRC=103684

又如下图的音频：G722，视频：H.261



No.	Time	Source	Destination	Protocol	Info
445	3.236212	172.16.225.23	172.16.160.42	H.261	H.261 message
448	3.255444	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=319,
449	3.276257	172.16.225.23	172.16.160.42	H.261	H.261 message
452	3.295395	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=320,
453	3.295557	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=321,
456	3.317740	172.16.225.23	172.16.160.42	H.261	H.261 message
457	3.323141	172.16.225.23	172.16.160.42	H.261	H.261 message
458	3.325353	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=322,
459	3.332761	172.16.225.23	172.16.160.42	H.261	H.261 message
462	3.355679	172.16.225.23	172.16.160.42	H.261	H.261 message
463	3.365287	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=323,
466	3.395752	172.16.225.23	172.16.160.42	H.261	H.261 message
469	3.398516	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=324,
472	3.435651	172.16.225.23	172.16.160.42	H.261	H.261 message
473	3.437416	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=325,
476	3.477367	172.16.225.23	172.16.160.42	H.261	H.261 message
477	3.478421	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=326,
478	3.478506	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=327,
479	3.483168	172.16.225.23	172.16.160.42	H.261	H.261 message
482	3.512812	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=328,
483	3.515682	172.16.225.23	172.16.160.42	H.261	H.261 message
486	3.545107	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=329,
489	3.555524	172.16.225.23	172.16.160.42	H.261	H.261 message
492	3.585034	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=330,
493	3.595421	172.16.225.23	172.16.160.42	H.261	H.261 message
496	3.614996	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=331,
497	3.636912	172.16.225.23	172.16.160.42	H.261	H.261 message
500	3.643123	172.16.225.23	172.16.160.42	H.261	H.261 message
501	3.655115	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=332,
502	3.655157	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=333,
505	3.675257	172.16.225.23	172.16.160.42	H.261	H.261 message
506	3.685836	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=334,
509	3.715253	172.16.225.23	172.16.160.42	H.261	H.261 message
510	3.724840	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=335,
521	3.755138	172.16.225.23	172.16.160.42	H.261	H.261 message
524	3.764853	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=336,
527	3.796874	172.16.225.23	172.16.160.42	H.261	H.261 message
528	3.796994	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.722, SSRC=211612676, Seq=337,

又如下图音频：G728，视频：H.263

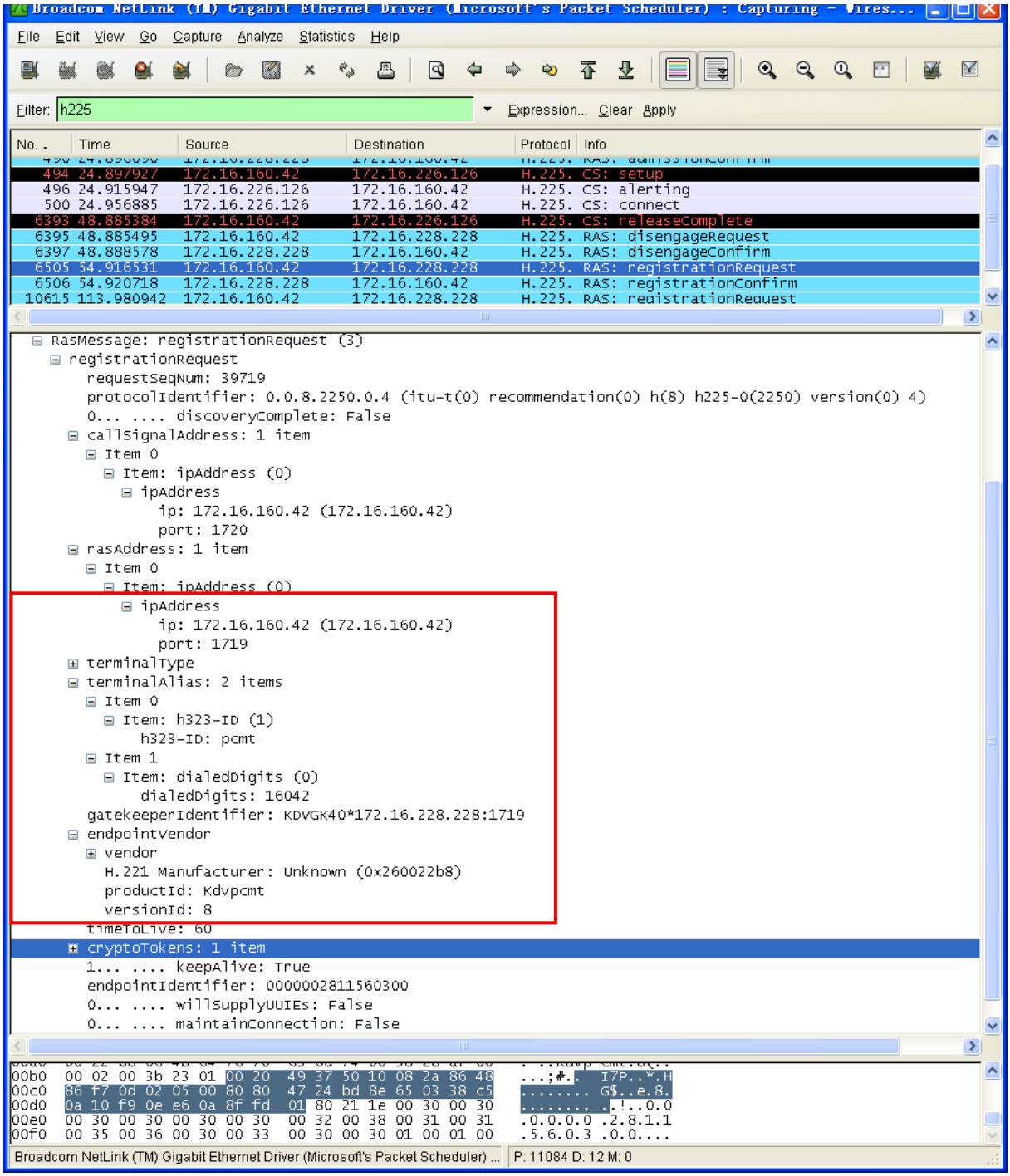


No.	Time	Source	Destination	Protocol	Info
365	2.614500	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=235
366	2.627347	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=264
369	2.646708	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=236
372	2.667179	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=265
373	2.674419	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=237
376	2.704373	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=238
377	2.707232	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=266
380	2.734351	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=239
381	2.747005	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=267
384	2.766779	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=240
387	2.787157	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=268
388	2.794235	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=241
391	2.824239	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=242
392	2.826927	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=269
395	2.854211	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=243
396	2.867235	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=270
400	2.886423	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=244
403	2.906790	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=271
404	2.914111	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=245
407	2.944103	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=246
408	2.947029	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=272
411	2.974076	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=247
412	2.986983	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=273
415	3.006273	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=248
416	3.026921	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=274
419	3.033975	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=249
424	3.063928	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=250
425	3.066533	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=275
428	3.093896	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=251
429	3.106938	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=276
432	3.126140	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=252
433	3.146561	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=277
436	3.153850	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=253
439	3.183782	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=254
440	3.186700	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=278
444	3.213751	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=255
445	3.226482	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=279
449	3.246035	172.16.225.23	172.16.160.42	RTP	Payload type=ITU-T G.728, SSRC=1505677384, Seq=256
452	3.266692	172.16.225.23	172.16.160.42	H.263	Payload type=ITU-T H.263, SSRC=1679790317, Seq=280

下表列出了各音视频格式所对应的动态载荷值通过查询此表可确认所捕获的 UDP 包的具体的音视频格式。

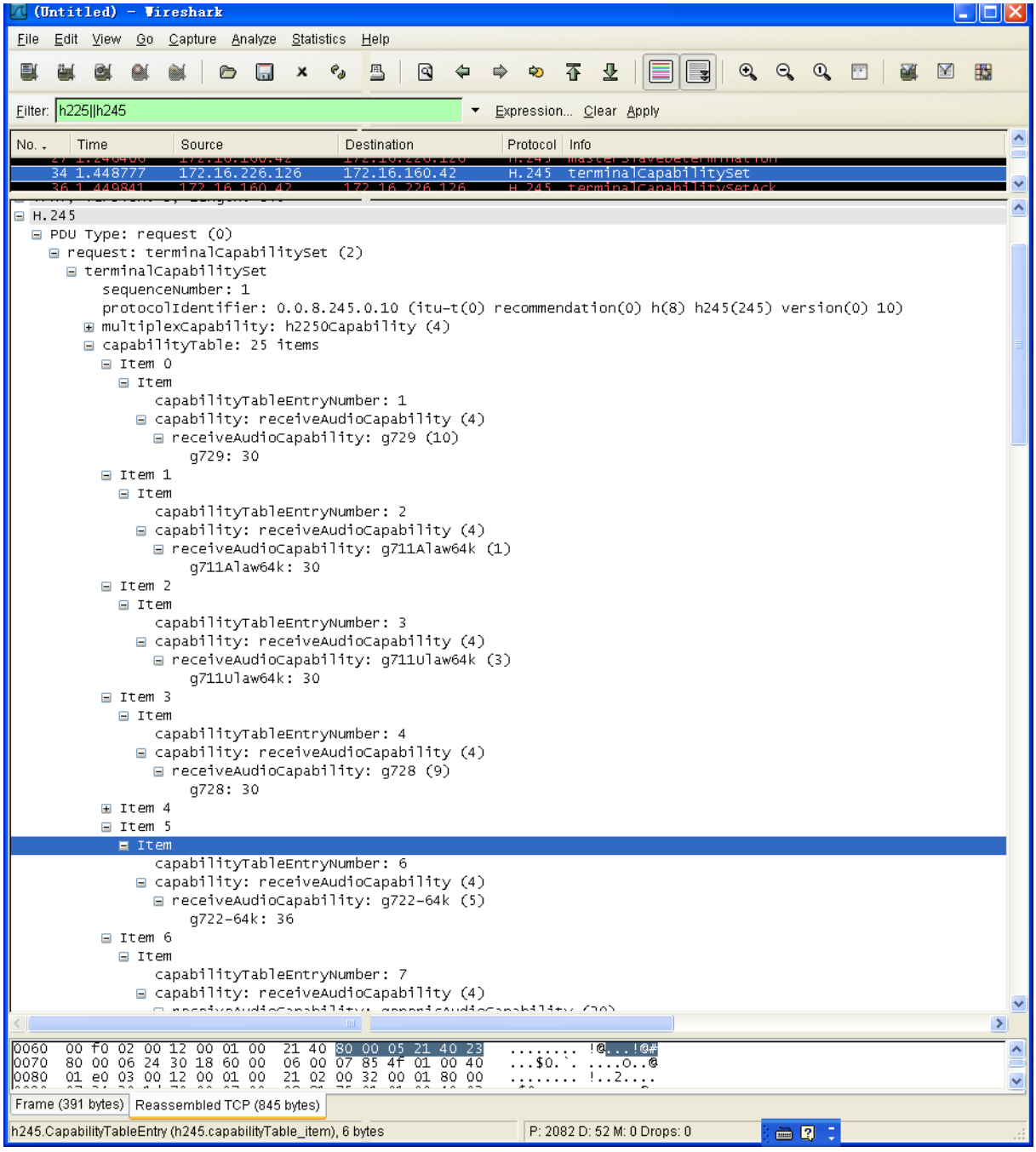
视频格式	动态载荷
H261	31
Mpeg2	33
H263	34
Mpeg4	97
H264	106
音频格式	动态载荷
G711A	8
G722	9
G722.1.C Polycom	98
G728	15
Mp 3	96
MPEG4 AAC-LC	102

同样通过对所捕获的包信息进行分析我们还可以了解设备注册 GK 的信息，如一台 IP 地址为 172.16.160.42 的 PCMT 其 E164 号为 16042，H323ID 为 PCMT 以及其产品名称（kedapcmt），这些信息在下图所示的抓包信息中都可以获取

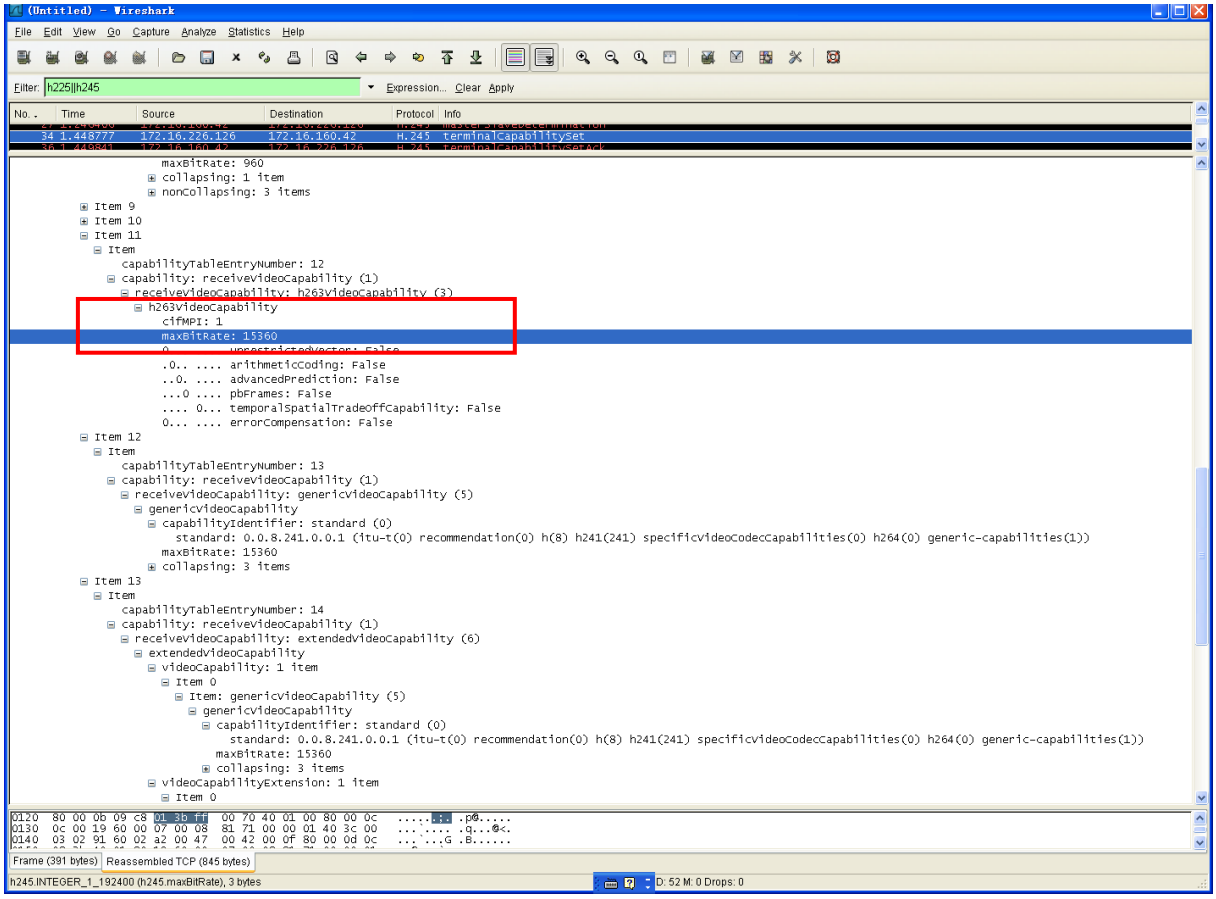


而在呼叫建立的过程中两台终端之间需要进行音视频能力集的交互，这些交互信息同样可以在

抓包信息中获取，如下图所示



上图主要显示了音频能力集，下图显示的是视频能力集及其呼叫码率



本文中所用的所有列子全部是通过 PCMT 捕获的包，若在测试过程需要对终端或 MCU 的码流进行抓包，在需要通过 HUB 进行连接。

通过抓包可方便我们分析测试中遇到的呼叫失败、通道未打开或打开不正确等问题，同样也可以帮助我们理解 H323 协议。

4 解决结果

希望通过上述说明可以使首次接触 Wireshark 抓包工具的同事能更方便快捷的了解掌握此工具的使用。