

Wireshark 使用教程

1 什么是 wireshark

Wireshark 是世界上最流行的网络分析工具。这个强大的工具可以捕捉网络中的数据，并为用户提供关于网络 and 上层协议的各种信息。与很多其他网络工具一样，wireshark 也使用 pcap network library 来进行封包捕捉。

2 wireshark 的下载与安装

2.12.1 下载 wireshark

访问 wireshark 的官方主页 <http://www.wireshark.org/> 我们可以下载 wireshark 的安装文件，在这里我们既可以下载到最新的发布版本软件安装文件，也可以下载到以前发布的旧版本软件安装文件。

Wireshark 支持多个操作系统，在下载安装文件的时候注意选择与自己 PC 的操作系统匹配的安装文件。下面的介绍我们都是以 windows XP 系统为例。

2.2 安装 wireshark

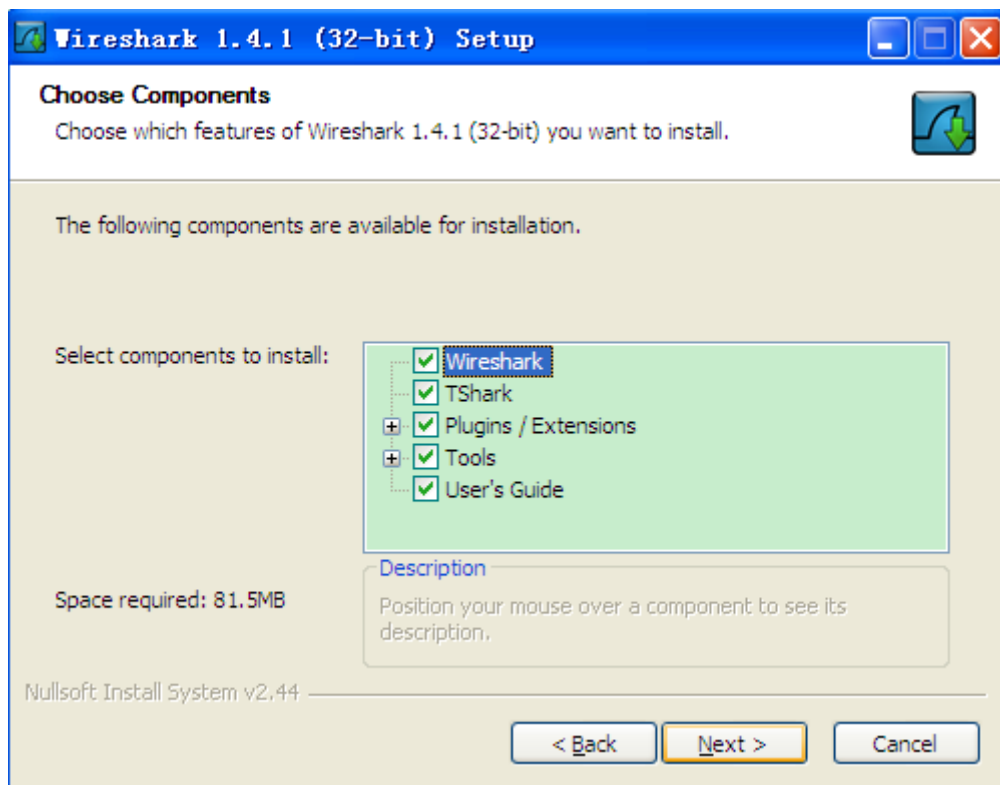
2.2.1 选择组件 (Choose Components)

Wireshark——GUI 网络分析工具

TSshark-TShark ——命令行的网络分析工具

插件/扩展(Wireshark,TShark 分析引擎):

- (1) Dissector Plugins——分析插件：带有扩展分析的插件
- (2) Tree Statistics Plugins——树状统计插件：统计工具扩展
- (3) Mate - Meta Analysis and Tracing Engine (experimental)——可配置的显示过滤引擎。
- (4) SNMP MIBs——SNMP，MIBS 的详细分析。



Tools/工具(处理捕捉文件的附加命令行工具

- (1) Editcap 是一个读取捕捉文件的程序，还可以将一个捕捉文件力的部分或所有信息写入另一个捕捉文件。
 - (2) Tex2pcap 是一个读取 ASCII hex，写入数据到 libpcap 文件的程序。
 - (3) Mergecap 是一个可以将多个捕捉文件合并为一个的程序。
 - (4) Capinfos 是一个显示捕捉文件信息的程序。
- User's Guide 用户手册——本地安装的用户手册。如果不安装用

户手册，帮助菜单的大部分按钮的结果可能就是访问 Internet.

2.2.2 选择附加任务（Select Additional Tasks）

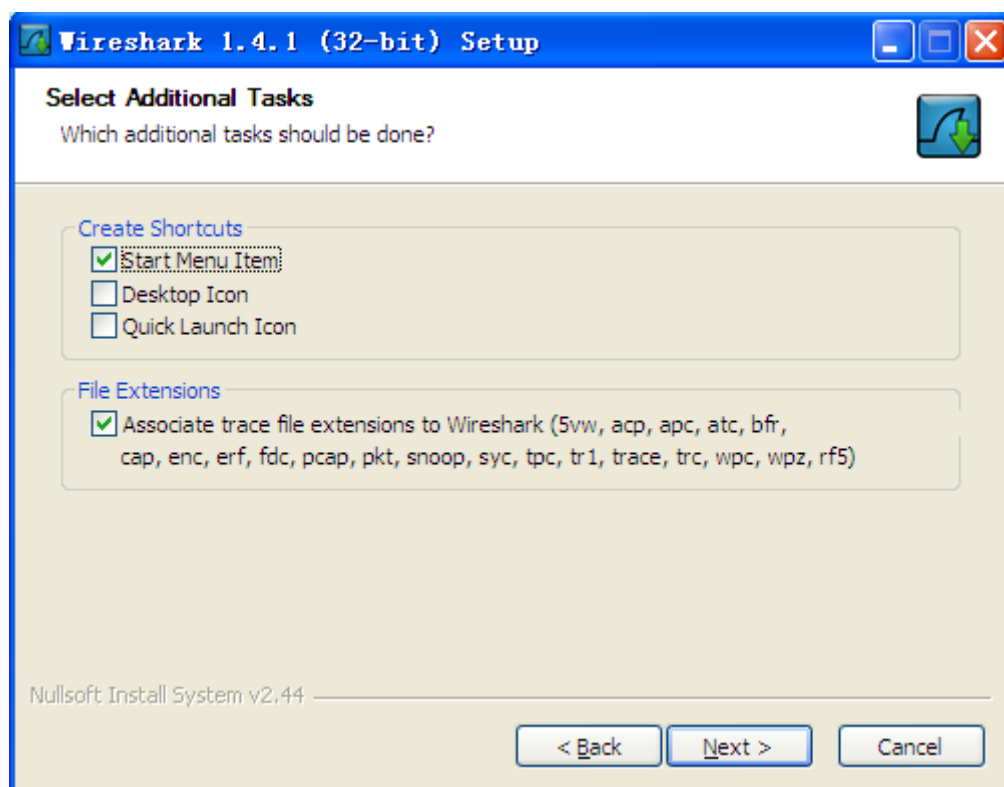
Start Menu Item——增加一些快捷方式到开始菜单

Desktop Icon——增加 Wireshark 图标到桌面

Quick Launch Icon——增加一个 Wireshark 图标到快速启动工具

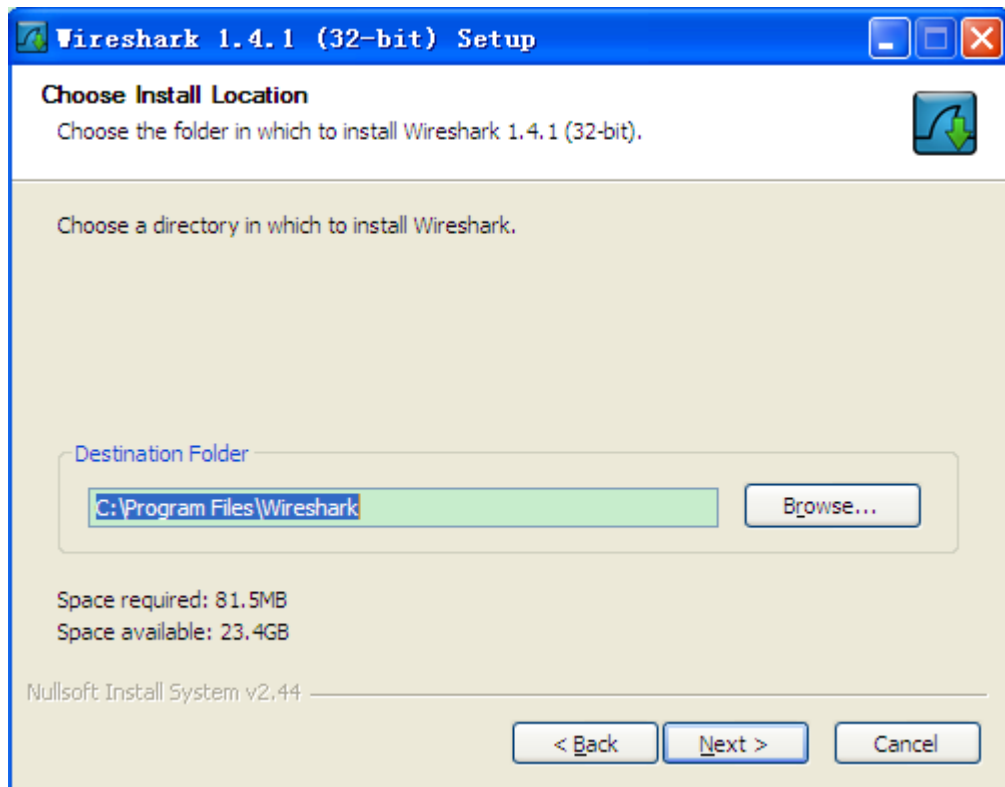
栏

Associate file extensions to Wireshark-Wireshark——将捕捉包默认打开方式关联到 Wireshark



2.2.3 选择安装目录（Choose Install Location）

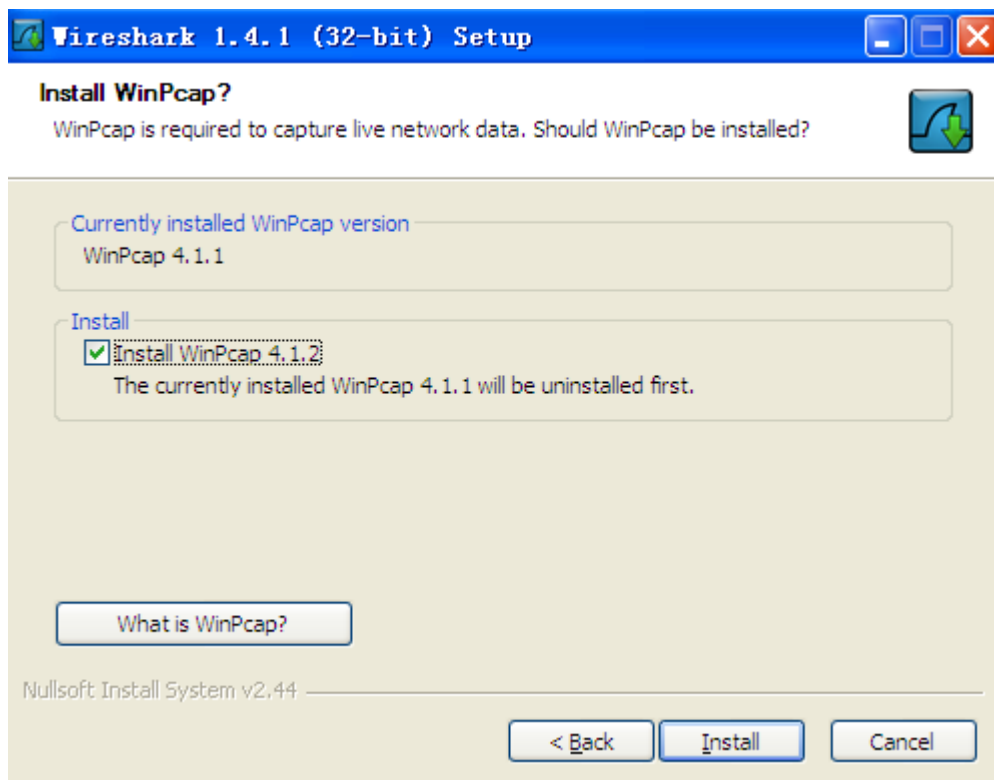
安装路径默认为 C 盘，用户可以根据自己的需求更改默认安装路径。



2.2.4 安装 WinPcap (Install WinPcap)

Wireshark 安装包里包含了最新版的 WinPcap 安装包。如果您没有安装 WinPcap 。您将无法捕捉网络流量。但是您还是可以打开以保存的捕捉包文件。

当一切都选择完成后，点击安装按钮等待完成安装即可。

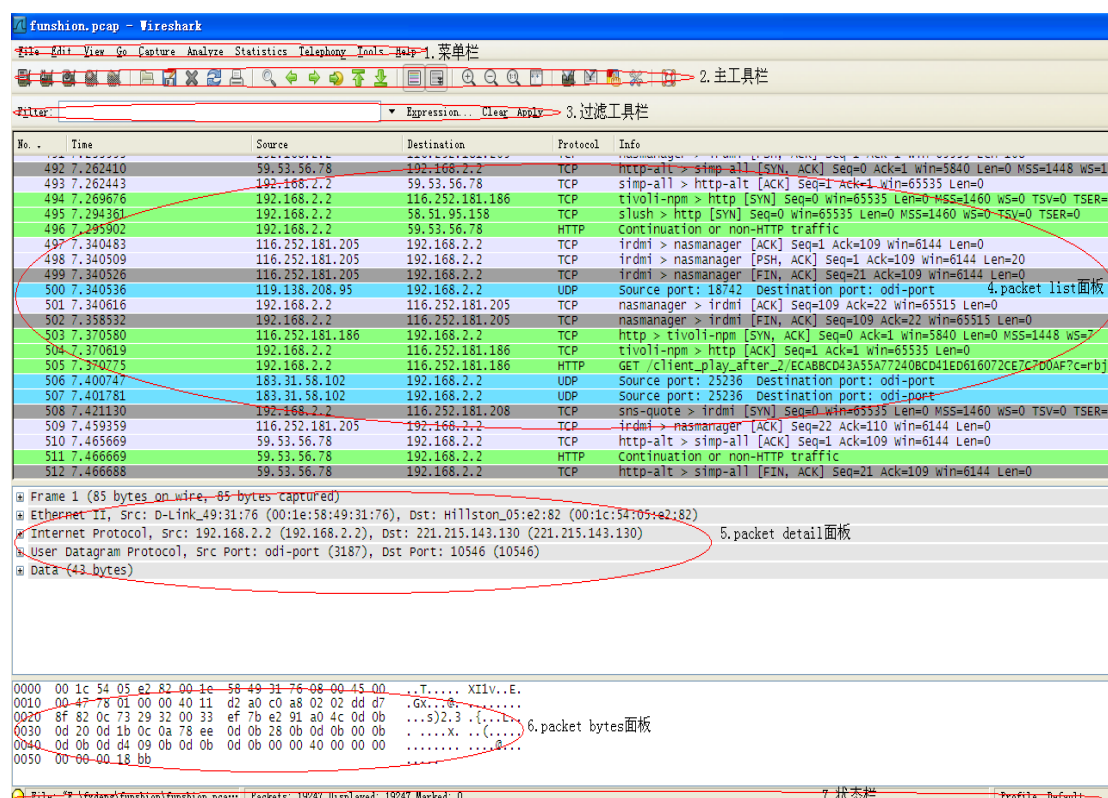


3 用户界面

安装完成后，即可运行 wireshark。打开 wireshark 后的抓包主界面如下图所示。Wireshark 主窗口由如下部分组成：

- （1）菜单——用于开始操作。
- （2）主工具栏——提供快速访问菜单中经常用到的项目的功能。
- （3）Filter toolbar/过滤工具栏——提供处理当前显示过滤得方法。
- （4）Packet List 面板——显示打开文件的每个包的摘要。点击面板中的单独条目，包的其他情况将会显示在另外两个面板中。
- （5）Packet detail 面板——显示您在 Packet list 面板中选择的包的更多详情。
- （6）Packet bytes 面板——显示您在 Packet list 面板选择的包的数据，以及在 Packet details 面板高亮显示的字段。

(7) 状态栏——显示当前程序状态以及捕捉数据的更多详情。



3.1 菜单栏

主菜单包括以下几个项目:

(1) File ——包括打开、合并捕捉文件, save/保存, Print/打印, Export/导出捕捉文件的全部或部分。以及退出 Wireshark 项。

(2) Edit ——包括如下项目: 查找包, 时间参考, 标记一个多个包, 设置预设参数。(剪切, 拷贝, 粘贴不能立即执行。)

(3) View ——控制捕捉数据的显示方式, 包括颜色, 字体缩放, 将包显示在分离的窗口, 展开或收缩详情面版的地树状节点

(4) GO ——包含到指定包的功能。

(5) Capture ——控制抓包的对话框, 包括接口, 选项, 开始/停止/重新开始和过滤器。








(6) **Analyze** ——包含处理显示过滤，允许或禁止分析协议，配置用户指定解码和追踪 TCP 流等功能。


(7) **Statistics** ——包括的菜单项用户显示多个统计窗口，包括关于捕捉包的摘要，协议层次统计等等。





(8) **Help** ——包含一些辅助用户的参考内容。如访问一些基本的帮助文件，支持的协议列表，用户手册。

















3.2 工具栏



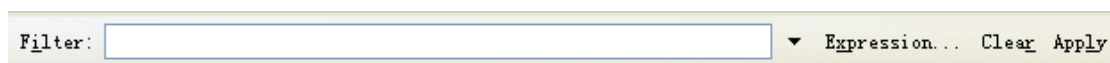
- (1)  ——打开接口列表对话框
- (2)  ——打开捕捉选项对话框
- (3)  ——使用最后一次的捕捉设置立即开始捕捉
- (4)  ——停止当前捕捉
- (5)  ——停止当前捕捉并立即重新开始
- (6)  ——启动打开文件对话框，用于载入文件
- (7)  ——保存当前文件为任意其他的文件，它将会弹出一个保存对话框

注：如果当前文件是临时未保存文件，图标将会显示为

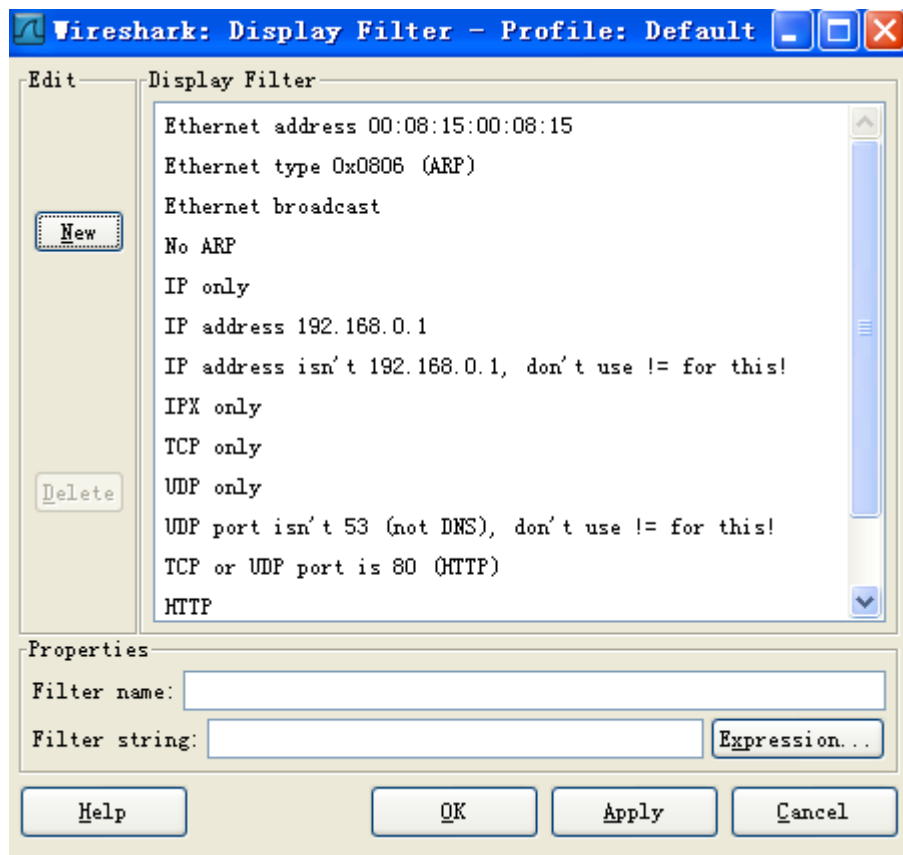
- (8)  ——关闭当前文件。如果未保存，将会提示是否保存
- (9)  ——重新载入当前文件
- (10)  ——打印捕捉文件的全部或部分，将会弹出一个打印对话框
- (11)  ——打开一个对话框，查找包

- (12) ——返回历史记录的上一个
- (13) ——跳转到历史记录中的下一个包
- (14) ——弹出一个设置跳转到指定的包的对话框
- (15) ——跳转到第一个包
- (16) ——跳转到最后一个包
- (17) ——切换是否以彩色方式显示包列表
- (18) ——开启/关闭实时捕捉时自动滚动包列表
- (19) ——增大字体
- (20) ——缩小字体
- (21) ——设置缩放大小为 100%
- (22) ——重置列宽，是内容适合列宽（使包列表内的文字可以显示）
- (23) ——打开对话框，用于创建、编辑捕捉过滤器
- (24) ——打开对话框，用于创建、编辑显示过滤器
- (25) ——定义以彩色方式显示数据包的规则
- (26) ——打开首选项对话框
- (27) ——打开帮助对话框

3.3 过滤工具栏



点击 Filter 按钮会弹出 **display filter** 对话框



这个和在工具栏上输入协议来查找包的结果是一样的，只是它方便点

- (1) **New**——增加一个新的过滤器到列表中。当前输入的 **Filter name**, **Filter string** 将会被使用并被保存，如果这些都为空，将会设置为 “new”。
- (2) **Delete**——删除选中的过滤器。如果没有过滤器被选中则为灰色
- (3) **Filter name**——修改当前选择的过滤器的名称。注：过滤器名称仅用在此处为了区分方便而已，没有其他用处。可以将多个过滤器使用同一个名称，但这样很不方便。
- (4) **Filter string**——修改当前选中过滤器的内容。仅适用显示过滤：在输入时进行语法检查。

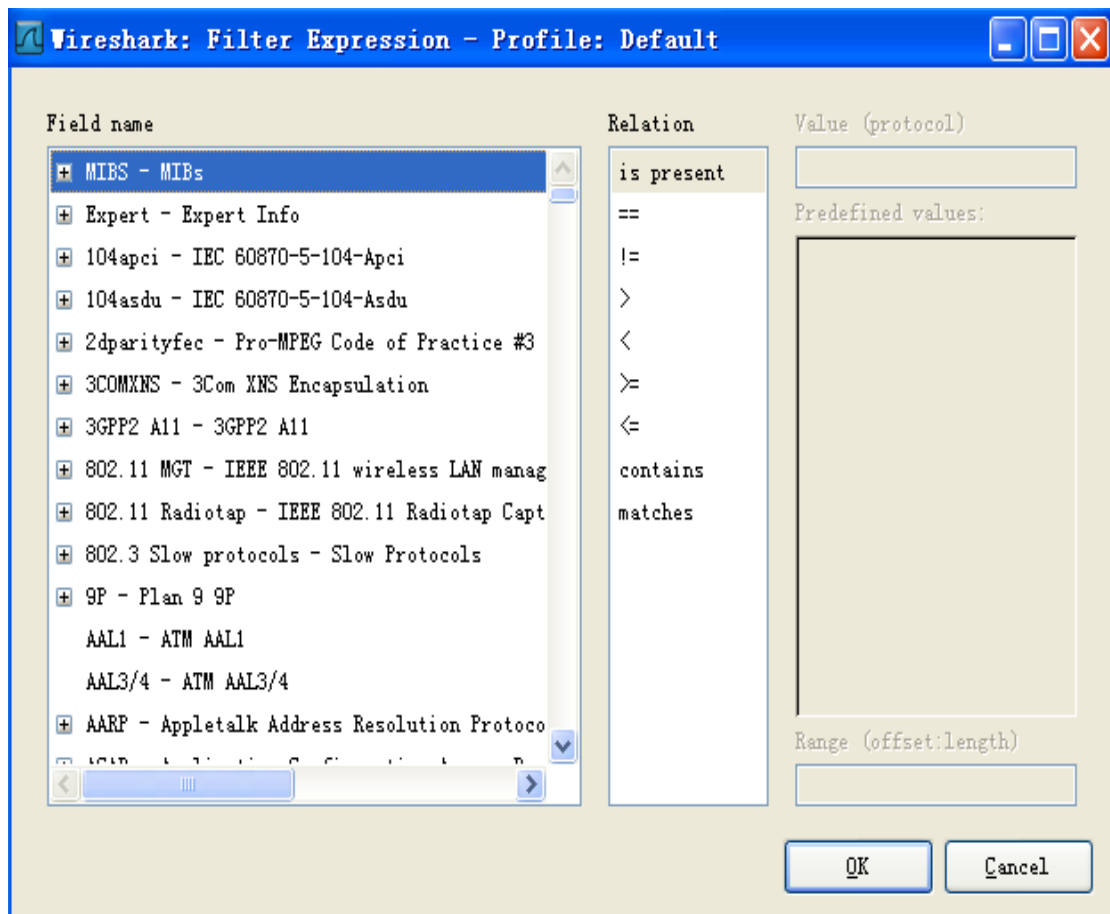
(5) Add expression——仅适用显示过滤：打开增加表达式对话框，辅助创建过滤表达式。

(6) OK——仅适用显示过滤：应用当前显示选择的过滤器，关闭当前对话框。

(7) Apply——仅适用显示过滤：应用当前显示选择的过滤器。

(8) Cancel——放弃当前设置，关闭当前对话框。

点击 Expression 按钮，会出现 Filter Expression 对话框



(1) Field name——从协议字段书中选择协议字段。每个可过滤协议都放在第一级。点击“+”展开列表，可以获得关于那些协议的可过滤字段。

(2) Relation——从可以关系列表中选择关系。Is present 是一元

关系，如果选择的字段存在，表达式为真值。其它关系为二元关系，需附加数据来完成。如果从字段名列表选择一个字段，并选择一个二元关系，您可能需要输入值，也有可能是范围信息。

(3) **Value**——在此输入合适的配置值，输入的值同样要符合你选择的 **field name** 的属性值类型。

(4) **Predefined values**——有些协议字段包含预设值可用，这点和 C 语言中的枚举变量类似。如果选择的协议有这样的值定义，你可以再次选择。

在工具栏上输入



点击在此区域输入或修改显示的过滤字符，在输入过程中会进行语法检查。如果您输入的格式不正确，或者未输入完成，则背景显示为红色。直到您输入合法的表达式，背景会变为绿色。你可以点击下拉列表选择您先前键入的过滤字符。列表会一直保留，即使您重新启动程序。

4 封包列表

| No. ↓ | Time | Source | Destination | Protocol | Info |
|---|-------------------|-------------------|-----------------|-------------------------------------|------------------|
| 123 | 7.921999 | 219.221.206.235 | 10.10.115.3 | UDP | Source port: nxl |
| 124 | 7.922949 | 10.10.115.3 | 211.83.152.49 | UDP | Source port: nxl |
| 125 | 8.011604 | 123.113.108.178 | 10.10.115.3 | UDP | Source port: nxl |
| 126 | 8.406951 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 127 | 8.408285 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 128 | 8.409698 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 129 | 8.422027 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 130 | 8.423371 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 131 | 8.424714 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 132 | 8.432941 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 133 | 8.434280 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 134 | 8.435686 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 135 | 8.437968 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 136 | 8.439378 | Hangzhou_27:33:c3 | Broadcast | ARP | who has 10.10.11 |
| 137 | 8.463546 | 10.10.115.13 | 255.255.255.255 | UDP | Source port: 100 |
| 138 | 8.505134 | 10.10.115.3 | 219.133.62.9 | UDP | Source port: ter |
| 139 | 8.749043 | 10.10.151.132 | 10.10.115.16 | UDP | Source port: bex |
| 140 | 8.973441 | 10.10.115.3 | 222.26.212.64 | UDP | Source port: nxl |
| ▶ Frame 123 (248 bytes on wire, 248 bytes captured) | | | | | |
| ▶ Ethernet II, Src: Hangzhou_27:33:c3 (00:0f:e2:27:33:c3), Dst: Internet_a8:21:1a (00:e0:4d:a8:21:1a) | | | | | |
| ▶ Internet Protocol, Src: 219.221.206.235 (219.221.206.235), Dst: 10.10.115.3 (10.10.115.3) | | | | | |
| ▶ User Datagram Protocol, Src Port: nxlmd (28000), Dst Port: nxlmd (28000) | | | | | |
| ▶ Data (206 bytes) | | | | | |
| 185. | Cisco-L1_2a:fb:9b | 3Com_9b:47:f7 | ARP | who has 192.168.1.2? | Tell 192.168.1.1 |
| 185. | 3Com_9b:47:f7 | Cisco-L1_2a:fb:9b | ARP | 192.168.1.2 is at 00:04:75:9b:47:f7 | |

封包列表中显示所有已经捕获的封包。在这里您可以看到发送或接收方的 **MAC/IP** 地址，**TCP/UDP** 端口号，协议或者封包的内容。如果捕获的是一个 **OSI layer 2** 的封包，您在 **Source**（来源）和 **Destination**（目的地）列中看到的将是 **MAC** 地址，当然，此时 **Port**（端口）列将会为空。

如果捕获的是一个 **OSI layer 3** 或者更高层的封包，您在 **Source**（来源）和 **Destination**（目的地）列中看到的将是 **IP** 地址。**Port**（端口）列仅会在这个封包属于第 4 或者更高层时才会显示。

您可以在这里添加/删除列或者改变各列的颜色：Edit menu -> Preferences。

4.1 封包列表信息

```
▶ Frame 123 (248 bytes on wire, 248 bytes captured)
└─ Ethernet II, Src: Hangzhou_27:33:c3 (00:0f:e2:27:33:c3), Dst: Internet_a8:21:1a (00:e0:4d:a8:21:1a)
    ▶ Destination: Internet_a8:21:1a (00:e0:4d:a8:21:1a)
    ▶ Source: Hangzhou_27:33:c3 (00:0f:e2:27:33:c3)
    Type: IP (0x0800)
└─ Internet Protocol, Src: 219.221.206.235 (219.221.206.235), Dst: 10.10.115.3 (10.10.115.3)
    Version: 4
    Header length: 20 bytes
    ▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 234
    Identification: 0xe930 (59696)
    ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 109
    Protocol: UDP (0x11)
    ▶ Header checksum: 0x3bfc [correct]
```

这里显示的是在封包列表中被选中项目的详细信息。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。



4.216 进制数据


| | 219 221 206 235 (219 221 206 235) | |
|------|---|-------------------|
| 0000 | 00 e0 4d a8 21 1a 00 0f e2 27 33 c3 08 00 45 00 | ..M.!... .'3...E. |
| 0010 | 00 ea e9 30 00 00 6d 11 3b fc db dd ce eb 0a 0a | ...0..m. ;..... |
| 0020 | 73 03 6d 60 6d 60 00 d6 c8 e6 48 75 6e 74 4d 69 | s.m`m`.. ..HuntMi |
| 0030 | 6e 65 5f 4d 41 52 4b e5 29 78 da ab 9a a2 77 f2 | ne_MARK.)x....w. |
| 0040 | e4 e4 84 15 6b 67 2e f0 7f 73 ff 96 3f 0b 83 37 |kg.. .s..?..7 |
| 0050 | 87 ca c9 a0 58 13 df e5 bc 95 9b 7b 0b 75 32 55 |X... ...{.u2U |
| 0060 | 1d 19 19 4e 30 30 30 30 32 e8 30 32 1a ce 08 be | ...N0000 2.02.... |
| 0070 | 0c c2 09 b9 09 b9 30 f6 84 d4 09 a9 8c 0c c9 af |0. |
| 0080 | ed 4e b6 b7 a4 18 7c 8d 36 da 3f d5 7c 82 74 85 | .N.... . 6.? .t. |
| 0090 | 33 03 50 03 48 5b 0a 03 e3 23 81 43 b7 40 38 21 | 3.P.H[. .#.C.@8! |
| 00a0 | 57 ef 12 cf 09 f7 5a 10 1b a2 ed b9 be ed c9 da | w.....Z. |
| 00b0 | 29 0f f9 4c c3 c3 e2 d4 32 1b fa ce 6d 63 07 6a |).L.... 2...mc.j |

“解析器”在 Wireshark 中也被叫做“16 进制数据查看面板”。这里显示的内容与“封包详细信息”中相同，只是改为以 16 进制的格式表述。

5 wireshark 实时捕捉数据包


使用 wireshark 捕捉数据包可以使用下面几种方式：

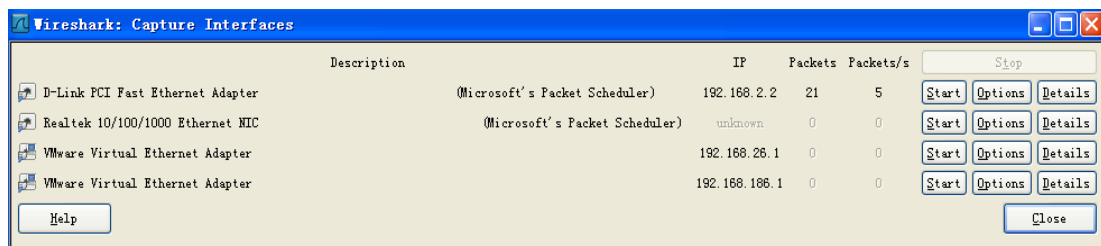
- (1) 使用打开捕捉接口对话框，浏览可用的本地网络接口，选择需要进行捕捉的接口启动捕捉
- (2) 使用"捕捉选项"按钮启动对话框开始捕捉。

(3) 如果前次捕捉时的设置和现在的要求一样，可以点击开始捕捉"按钮或者是菜单项立即开始本次捕捉。

(4) 如果已经知道捕捉接口的名称，可以使用如下命令从命令行开始捕捉：`wireshark -i eth0 -k` 此命令会从 eth0 接口开始捕捉。

5.1 捕捉接口对话框

如果从捕捉菜单选择 **interface** 按钮（或者从主工具栏选择），wireshark 弹出 **Capture Interface/捕捉接口对话框**。



这个对话框只显示本地已知的网络接口，wireshark 可能无法检测到所有的本地接口，wireshark 不能检测远程可用的网络接口，只能列出可用的网络接口。


(1) **IP**——wireshark 能解析的第一个 IP 地址，如果接口未获得 IP 地址（如，不存在可用的 DHCP 服务器），将会显示“unkown”，如果有超过一个 IP 的，只显示第一个（无法确定显示哪一个）。

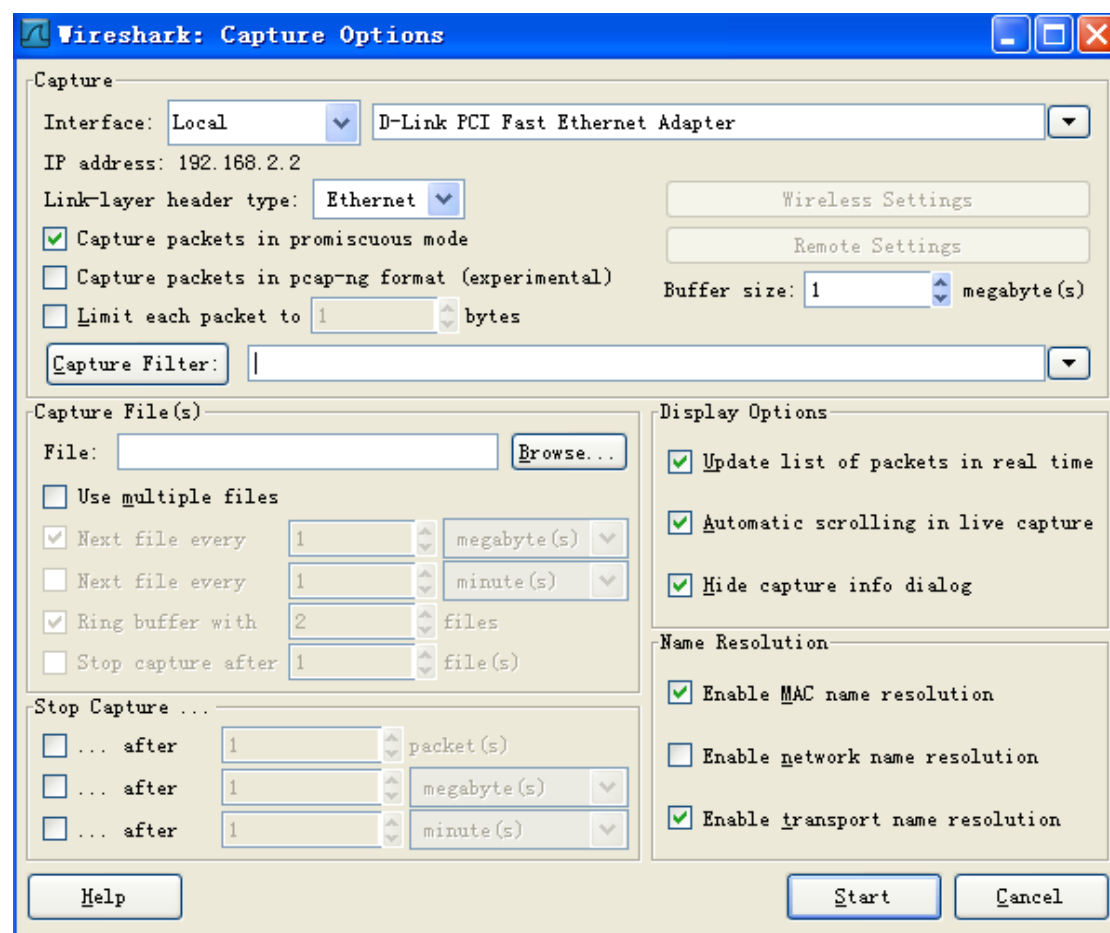
(2) **Packets**——打开该窗口后，从此接口捕捉到的包的数目。如果一直没有接收到包，则会显示为灰色。

(3) **Packets/s**——最近一秒捕捉包的数目。如果最近一秒没有捕捉到包，将会是灰色显示。

- (4) Stop——停止当前包的捕捉。
- (5) Capture——从选择的接口立即开始捕捉，使用最后一次捕捉的设置。
- (6) Option——打开该接口的捕捉选项对话框。
- (7) Details——打开对话框显示接口的详细信息。
- (8) Close——关闭对话框。

5.2捕捉选项对话框

如果从捕捉菜单选择 start 按钮（或者从主工具栏选择），wireshark 弹出 Capture Option/捕捉选项对话框。



- (1) Interface——指定想用于进行捕捉的接口，一次只能使用一

个接口。

(2) IP address——选择接口的 IP 地址。如果系统未指定 IP 地址，将会显示为“unknown”。

(3) Link-layer header type——选择接口的工作层。

(4) Buffer size——输入用于捕捉的缓存大小。

(5) Capture packets in promiscuous mode——指定 wireshark 捕捉包时，设置接口为杂收模式。如果未指定该选项，wireshark 将只能捕捉进出你电脑的数据包（不能捕捉整个局域网段的包）。

(6) Limit each packet to n bytes——指定捕捉过程中每个包的最大字节数。如果机制该选项，默认值为 65535。

(7) Capture filter——指定捕捉过滤。默认情况下是空的。

(8) File——指定用于捕捉的文件名。该字段默认为空白。如果保持空白，捕捉数据将会存储在临时文件夹。

(9) User multiple files——如果指定条件达到临界值，wireshark 将会自动生成一个新文件，不适用于单独文件。

(10) Next file every n megabyte(s)——仅适用于选中 user multiple files，如果捕捉文件容量达到指定值，将会切换到新文件。

(11) Next file every n minutes(s)——仅适用于选中 user multiple files，如果捕捉文件持续时间达到指定值，将会切换到新文件。

(12) Ring buffer with n files——仅适用于选中 user multiple files，如果捕捉文件持续时间达到指定值，将会切换到新文件。

(13) Stop capture after n file(s)——仅适用于 use multiple files，

当生成指定数目文件时，在生成下一个文件时停止捕捉。

(14) After n packet(s)——在捕捉到指定数目数据包后停止捕捉。

(15) After n megabyte(s)——在捕捉到指定容量的数据(byte(s)/kilobyte(s)/megabyte(s)/gigabyte(s))后停止捕捉。如果没有适用“user multiple files”，该选项将是灰色。

(16) After n minute(s)——在达到指定时间后停止捕捉。

(17) Update list of packet in real time——在包列表面板实时更新捕捉数据。如果为选定该选项，在 wireshark 捕捉结束之前将不能显示数据。如果选中该选项，wireshark 将生成两个独立的进程，通过捕捉进程传输数据给显示进程。

(18) Automatic scrolling in live capture——指定 wireshark 在有数据进入时实时滚动包列表面板，一直显示最新数据包。反之，则最新数据包会被放置在行末，但不会自动滚动面板。如果未设置“update list if packets in real time”，该选项竟是灰色不可选的。

(19) Hide capture info dialog——隐藏捕捉信息对话框。

(20) Enable MAC name resolution——设置是否让 wireshark 翻译 MAC 地址为名称。

(21) Enable network name resolution——是否允许 wireshark 对网络地址进行解析。

进行完上述设置以后，点击 Start 按钮进行捕捉。

5.3 停止捕捉

运行中的捕捉线程可以用以下列方法停止：

- (1) 使用捕捉信息对话框上的  stop 按钮停止。
- (2) 使用菜单项 capture  stop
- (3) 使用工具栏项  stop
- (4) 使用快捷键：Ctrl+E
- (5) 如果设置了触发停止的条件，捕捉达到条件时会自动停止。


5.4 重新启动捕捉

运行中的捕捉过程可以被重新启动，这将会移除上次捕捉的所有包。重新启动时一项方便的功能，类似于停止捕捉后，在很短的时间内立即开始捕捉。一下两种法师可以实现冲洗启动捕捉：

- (1) 使用菜单项 "Capture  Restart"
- (2) 使用工具栏 "  Restart"

5.5 文件输出与输入

5.5.1 抓包文件的保存

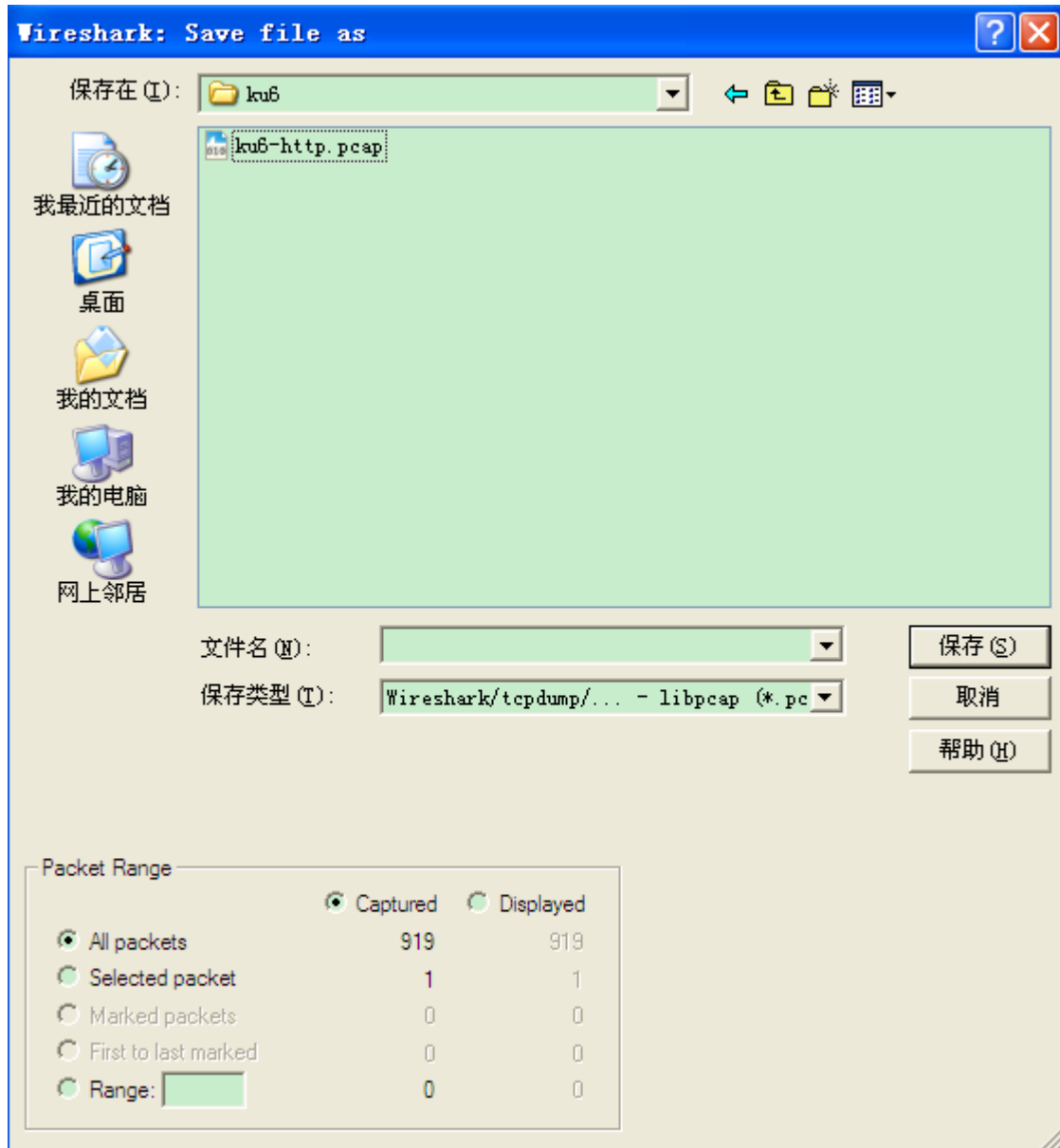
保存捕捉文件时可以通过 File——Save As...菜单或选择住工具栏  保存捕捉文件。

通过对话框，可以执行如下操作：

- (1) 输入指定的文件名。
- (2) 选择保存的目录。
- (3) 选择保存包的范围。

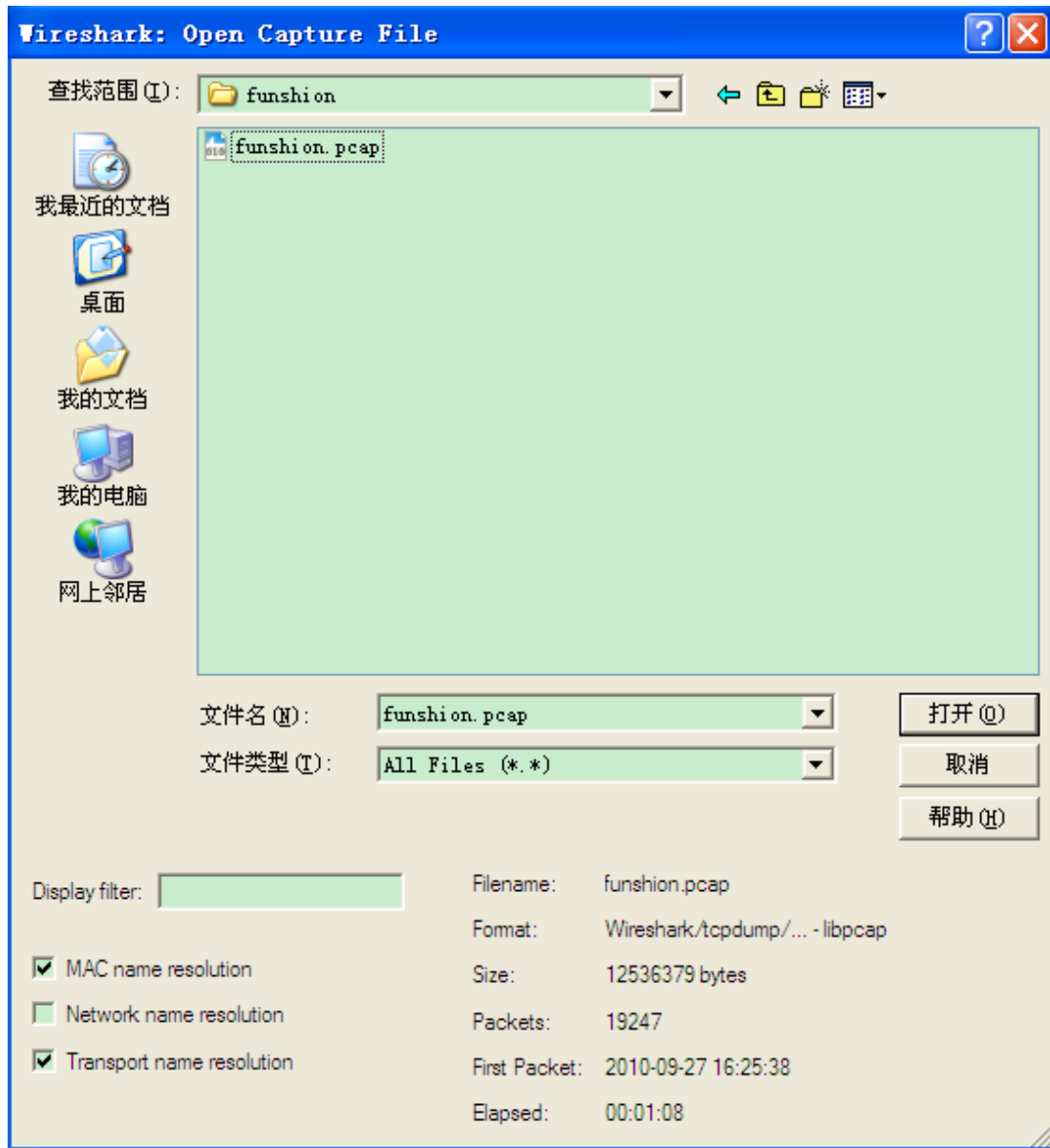
- (4) 通过点击 file type/文件类型下拉表指定保存文件的格式。
- (5) 点击 Save/OK 按钮保存。如果保存时遇到问题，会出现错误提示。
- (6) 点击 Cancel 按钮退出而不保存捕捉包。
- (7) wireshark 捕捉的包可以保存为其原生格式文件（libpcap），也可以保存为其他格式供其他工具进行读取分析。
- (8) Wireshark 可以保存为如下格式：

- 1) Libpcap, tcpdump and various other tools using tcpdump's capture format (*.pcap, *.cap, *.dmp)
- 2) Accellent 5Views (*.5vw)
- 3) HP-UX's nettle (*.TRCO, TRC1)
- 4) Microsoft Network Monitor—NetMon (*.cap)
- 5) Network Associates Sniffer—DOS (*.cap, *.enc, *.trc, *.fdc, *.syc)
- 6) Network Associates Sniffer—Windows (*.cap)
- 7) Network Instruments Observer version 9 (*.bfr)
- 8) Novell LANalyzer (*.tr1)
- 9) Sun snoop(*.snoop, *.cap)
- 10) Visual Networks Visual UpTime traffic (*.*)



5.5.2 wireshark 捕捉文件输入

Wireshark 可以读取以前保存的文件，想读取这些文件，只需选择菜单或工具栏的：“File/📁 Open”。Wireshark 将会弹出打开文件对话框。



常见对话框行为:

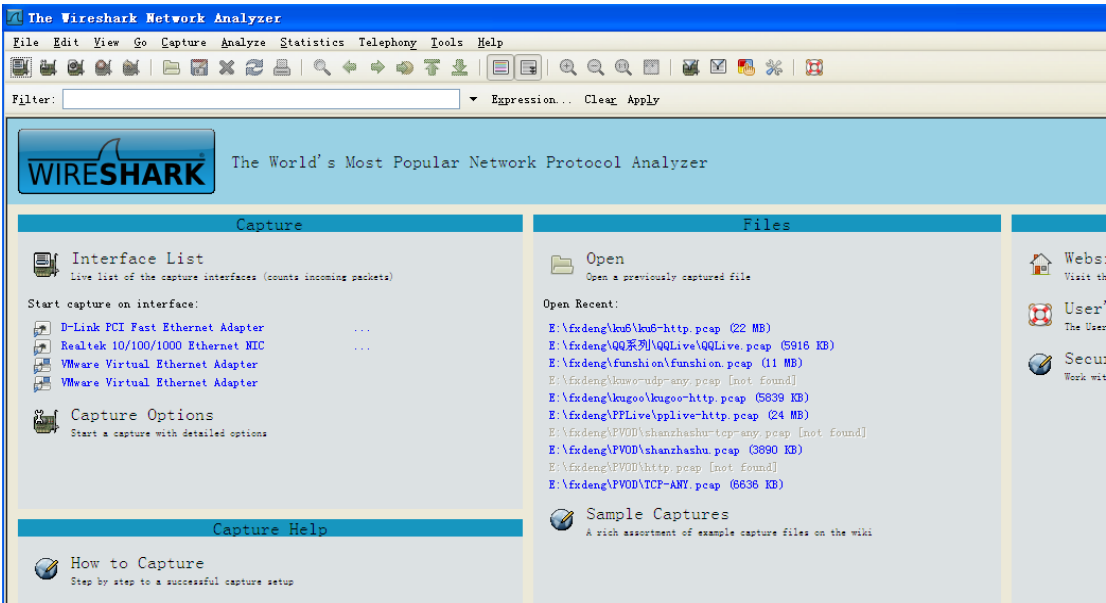
- (1) 选择文件和目录
- (2) 点击 Open/OK 按钮, 选择你需要的文件并打开它
- (3) 点击 Cancel 按钮返回 wireshark 主窗口而不载入任何文件
- (4) Wireshark 对话框标准操作扩展
- (5) 如果选中文件, 可以查看文件预览信息 (文件大小, 包个数...)
- (6) 通过 “Display filter” 对话框, 显示字段指定显示过滤器。


过滤器将会在打开文件后应用。在输入过滤字符时会进行语法检查。如果输入正确背景为绿色，如果错误或输入未结束，背景为红色。载入文件后，点击 **filter** 按钮会打开过滤对话框，用于辅助输入显示过滤表达式。

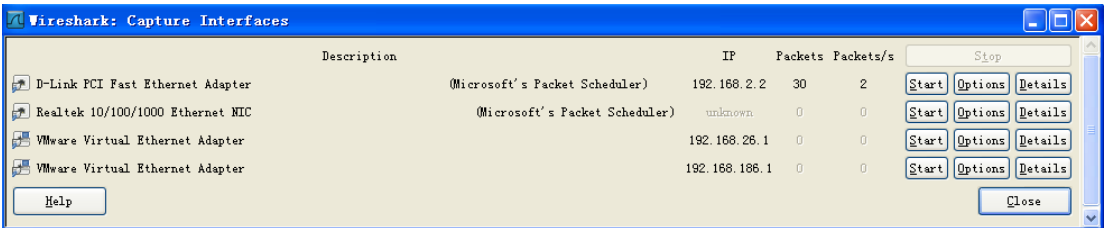
6 应用举例

上面介绍了 **wireshark** 软件的安装与使用方法，下面我们以捕捉本机 PPLive 网络电视流量为例说明一下 **wireshark** 的具体使用过程。

第一步：打开 **wireshark**，会出现 **wireshark** 抓包开始界面。

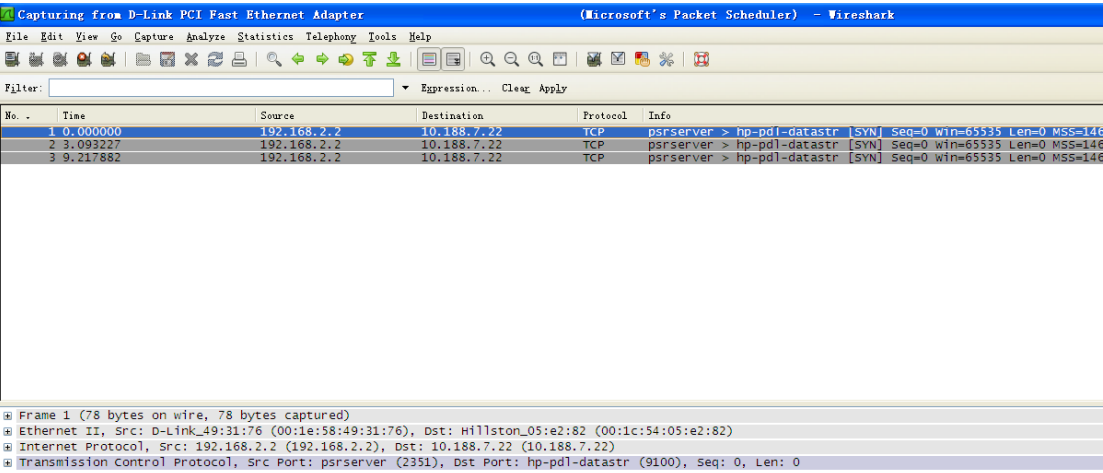


第二步：点击 ，弹出接口对话框

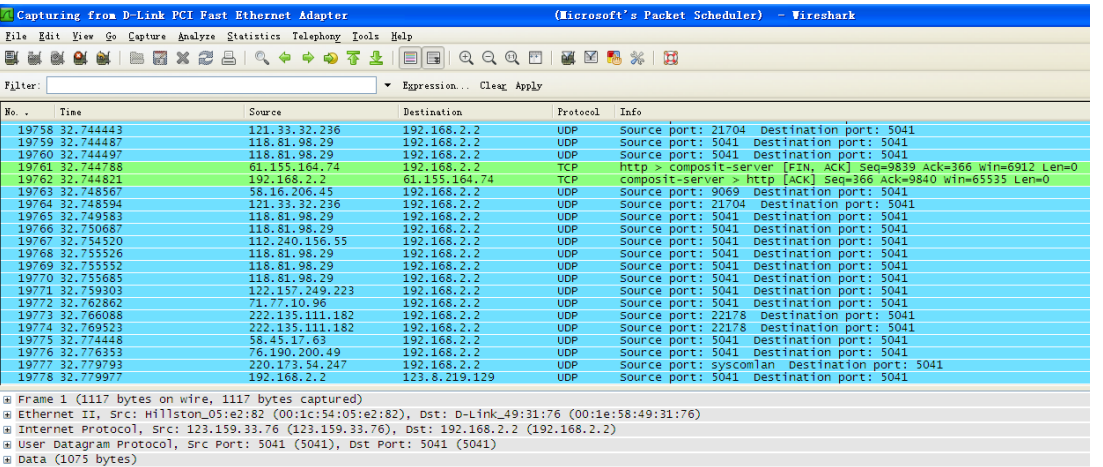


第三步：从接口对话框中可以看到有三个接口，第一个为本地网卡，另外两个为虚拟机。我们要抓取本急流量，所以选择本地网卡接

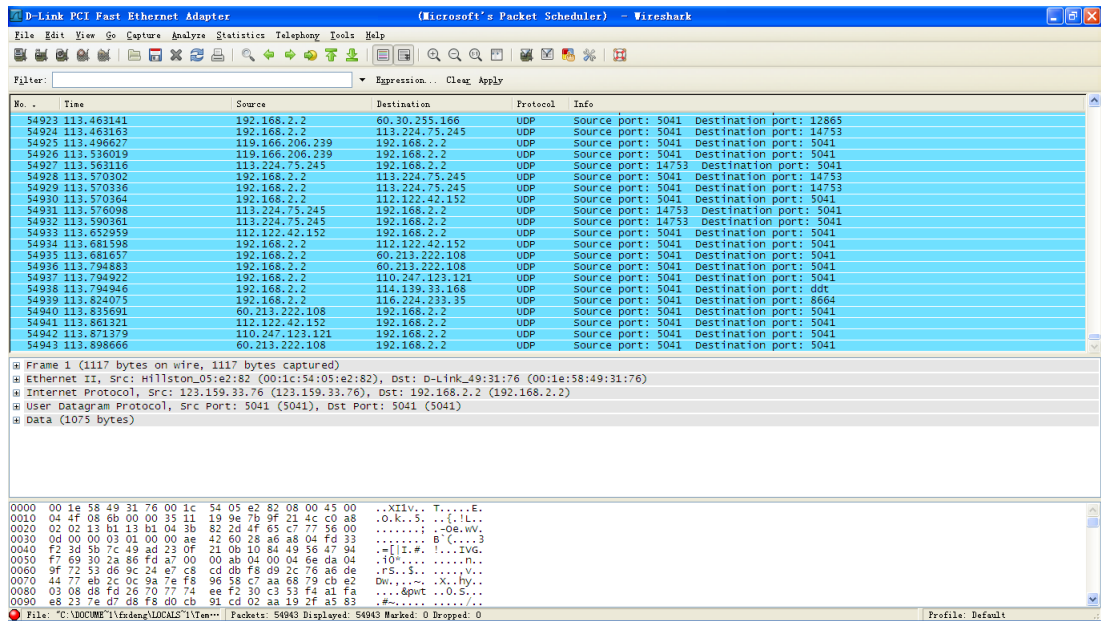
口，点击对应的 Start 按钮，开始捕捉包。




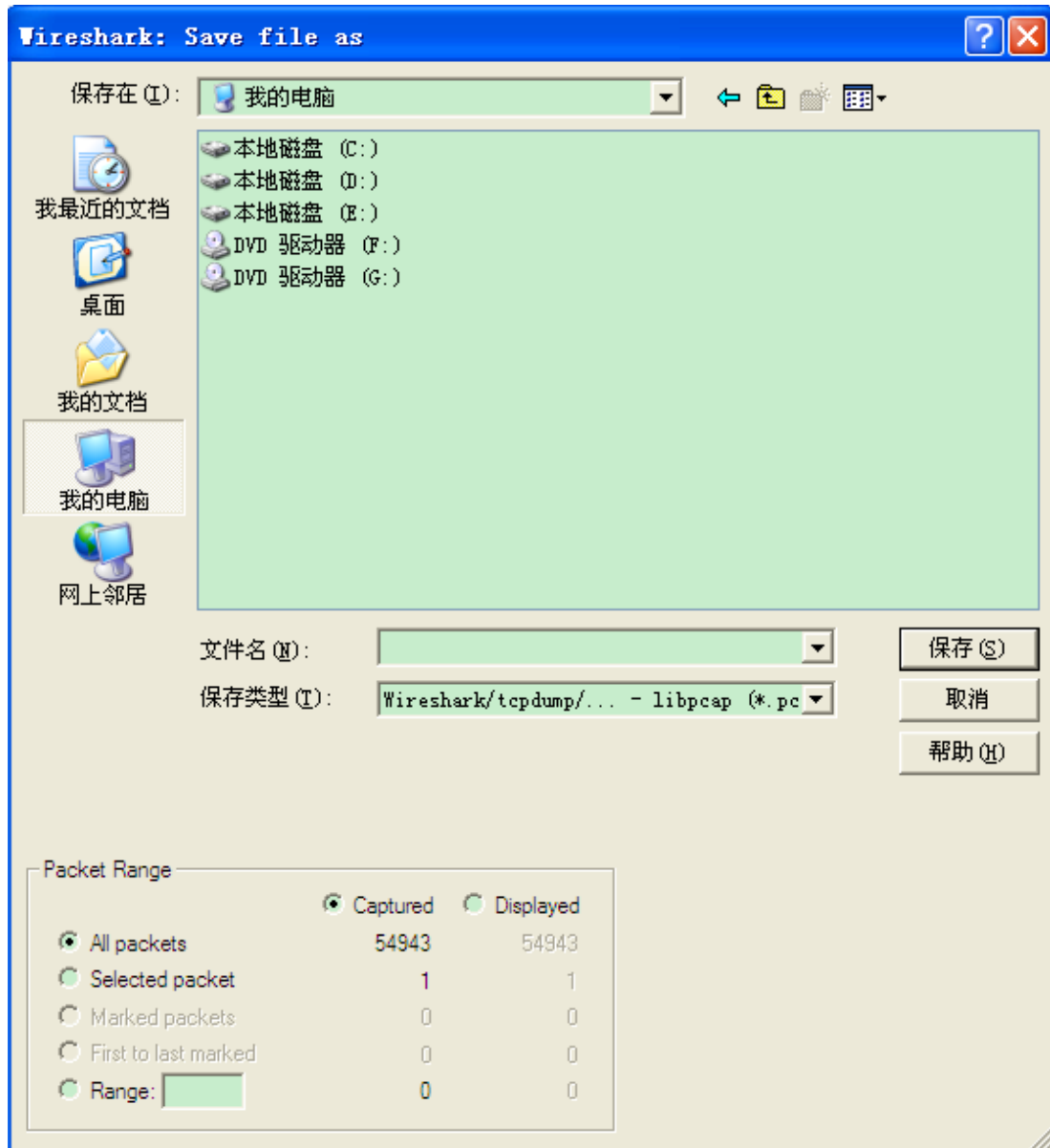
第四步：打开 PPLive 网络电视，选择节目进行播放。可以看到 wireshark 抓包界面不断地更新封包列表。



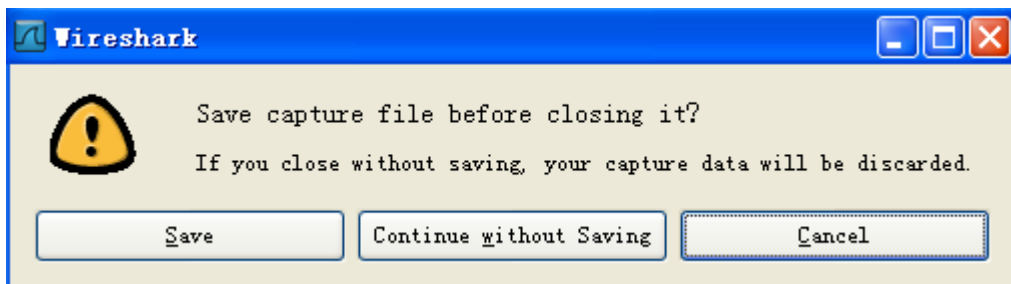
第五步：点击  停止当前包的捕捉



第六步：点击  按钮保存当前捕捉包。选择保存文件的路径及文件名称，保存类型如果没有特殊需求选择 libpcap（注：文件保存类型参考 5.1），选择完成后点击保存即完成一个本地 PPLive 网络电视流量包的捕捉。



第七步：如果不想保存当前捕捉包，点击 按钮，会出现保存提示对话框，点击“Continue without Saving”按钮即关闭当前未保存包并回到 wireshark 抓包开始界面。



如果不想保存当前捕捉包并想立即开始新的捕捉，点击 按钮。