Wireshark 过滤器和外观设置

**1 过滤器**

Wireshark 有两种过滤器，掌握过滤器的用法可以更轻松的分析捕捉的数据。这两种过滤器分别是：

* 捕获过滤器
* 显示过滤器

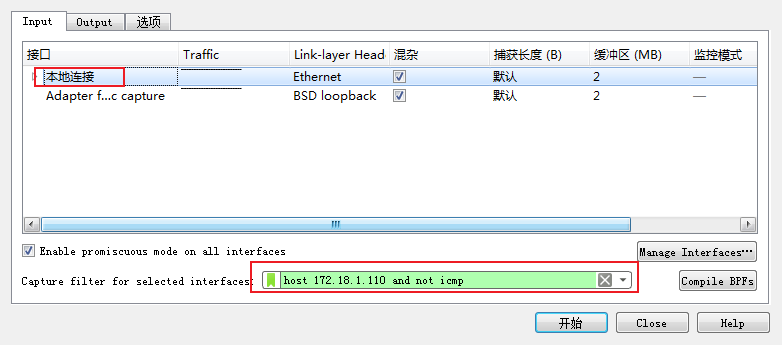
1.1 捕获过滤器 (CaptureFilters)

决定将什么样的信息记录在捕获结果中。

点击如图所示图标，设置捕获过滤器规则。



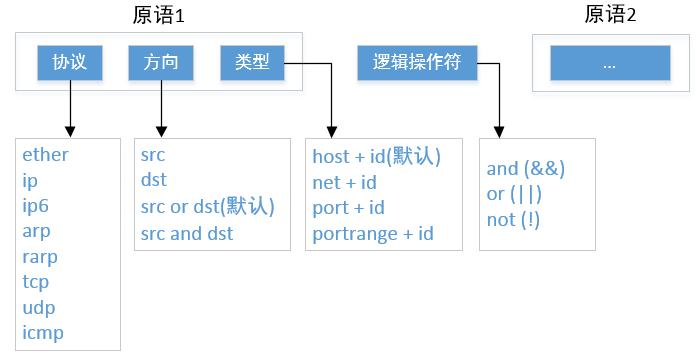
在弹出的“捕获选项”界面中，选择合适的接口，然后在 Capture filter for selected interfaces 输入框中输入捕获过滤器表达式。



**捕获过滤器表达式语法：**

* 滤波器表达式由一个或多个原语（primitive）组成
* 多个原语之间使用逻辑操作符连接
* 原语由一个或多个限定符组成。
* 限定符有三类，分别是：协议、方向和类型

常用的捕获滤波表达式可以用下图描述。



补充说明：

1、协议：如果没有指明 协议，默认是所有协议。

2、方向：

* src ：源
* dst ：目的

3、类型：类型后面需要有 id ，id 为数字或者一个名称

* host：指定主机，可以用主机名或者主机 IP 来指定唯一主机
* net：网络，一般用 IP 地址表示
* port：端口号

捕获过滤器表达式举例：

1、捕获指定IP的数据流

host 172.18.1.2

net 172.18.1.2

host www.baidu.com

2、捕获指定IP对的数据

host 172.18.1.2 and host 172.18.1.110

net 172.18.1.2 and net 172.18.1.110

3、捕获指定IP范围的数据流

net 172.18 //这是正确的表达式,可以只指定一部分IP

net 172.18.0.0/16 //这里'/16'表示16位子网掩码, 等效于:

net 172.18.0.0 mask 255.255.0.0

4、捕获指定端口

port 80 //网络接口上所有80端口数据,包括tcp和udp

tcp port 80 //网络接口上所有80端口TCP数据

host 172.18.1.2 and port 80 //这是两条原语. 捕获IP为172.18.1.2且端口为80的数据

5、捕获指定端口范围

portrange 2000-5000

6、捕获指定IP的TCP协议

tcp host 172.18.1.2

7、捕获指定IP的ARP协议

arp 172.18.1.2

8、捕获指定IP的数据但去除PING包

host 172.18.1.2 and not icmp

**特殊原语：**

1、broadcast 和 multicast

broadcast //只捕获广播包

not broadcast //不捕获广播包

2、包长比较，支持 <= 、 >= 、 > 、 < 、==

host 172.18.1.2 and len > 100 //指定IP的数据包长 >100 字节的数据包,数据包指以太网帧,从目的MAC地址开始

**1.2 显示过滤器 (DisplayFilters)**

**决定从捕获结果中显示什么样的信息。**

在主界面过滤器输入框中输入显示过滤器表达式。



**显示过滤器表达式语法：**

* 滤波器表达式由用一个或多个原语（primitive）组成
* 多个原语之间使用逻辑操作符连接
* 原语由协议、可选的比较操作符及值组成
* 协议具有可选的子类，使用 . 运算符指定。比如：ip.addr，其中 addr 为 IP 协议的子类

常用的显示滤波器表达式可以用下图描述。

补充说明：

1、协议： Wireshark支持2000+种协议，图示为常用协议。每种协议还有多种子类，在举例部分会看到常见协议的不同子类。通过菜单 视图 - 内部 - Supported Protocols，查看Wireshark支持的完整协议。

2、比较运算符

* contains：从数据流（帧头或者应用数据）查找指定数据。值 域为十六进制数字序列或者字符串，如果为16进制数据序列（无需 0x 前缀），字节与字节之间使用 : 分隔符。比如：udp contains 76:69:79、sip.To contains “a1762”

3、逻辑操作符

* in：逻辑操作符后面跟一个大括号括起来的集合，当指定源语属于这个集合，则显示出来。比如：udp.srcport in {4000…8000}。注意集合范围使用两个句点 .. 表示。
* […]：从数据包中查找指定内容，格式为：协议[a:b] == n1:n2:n3…，其中 a 为偏移量，从哪个位置开始的，b 表示要匹配的字节序数目，n1:n2:n3...为要查找的字节序。比如：udp[8:3] == 23:45:76，表示从 udp 数据包（包括 UDP 帧头）偏移地址 8 处开始的连续 3 个字节为 0x23、0x45、0x76。注意，字节序 23:45:76 并不是处于 udp 数据包的任意位置，而是有且只能位于偏移地址8开始的地方！

**显示过滤器表达式举例：**

1、显示指定 IP 地址

ip.addr == 172.18.1.2 //源或目的地址为172.18.1.2

ip.src == 172.18.1.2 //源IP地址为172.18.1.2

ip.dst == 172.18.1.2 //目的IP地址为172.18.1.2

2、显示指定 IP 对

ip.addr == 192.168.50.185 and ip.addr == 106.39.169.231 //这是两条源语

3、显示指定 IP 范围

ip.addr == 192.168.50.0/24 //源或目的地址为 192.168.50.0 ~ 192.168.50.255

ip.addr in {192.168.50.0 .. 192.168.50.255} //和上面表达式等价

ip.src == 192.168.50.0/24 //源地址为 192.168.50.0 ~ 192.168.50.255

ip.dst == 192.168.50.0/24 //目的地址为 192.168.50.0 ~ 192.168.50.255

4、显示指定端口

tcp.prot == 80 //源或目的端口为 80 的 TCP 包

tcp.stcport == 80 //源端口为 80 的 TCP 包

udp.dstport == 8000 //目的端口为 8000 的 UDP 包

5、显示指定端口范围

udp.srcport >= 4000 and udp.srcport <= 8000

udp.srcport in {4000..8000} //和上面表达式等价

6、指定 IP 的 tcp 协议

tcp and ip.addr == 172.18.1.110

7、显示指定IP的数据但去除PING包

ip.addr == 192.168.50.185 and not icmp

8、所有发出去的广播包

eth.dst == ff:ff:ff:ff:ff:ff

9、显示ARP协议并且指定源MAC地址

arp and eth.src == 00:60:37:f2:01:02

10、显示指定内容

udp contains 76:69:79 //UDP数据包（包括UDP帧头）中查找 0x76、0x69、0x79 字节

udp [0:3] == 76:69:79 //UDP数据包（包括UDP帧头）中，查找 0 偏移处的连续 3 字节是 0x76、0x69、0x79

udp.payload[0:3] == 76:69:79 //UDP数据包的数据区域(不含UDP帧头)中, 查找 0 偏移处的连续 3 字节是 0x76、0x69、0x79

注意两种查找内容的区别：

两者都是从协议帧头和协议数据中查找指定数据，区别是：

* 搜索范围不同：contains 从整个指定协议的数据区域内查找，而 [...] 具有偏移量，可以跳过某些数据，搜索范围更精确。
* 搜索位置不同：contains 只要数据区域内有指定的字节序就可以，而 [...] 只能从偏移量指定位置开始的指定数量的字节序。

所以，一般 [...] 用于过滤自定义协议帧。

11、显示指定的MAC地址

eth.addr[0:3]==00:60:37 //[0:3]:0 表示从以太网帧头的 0 偏移处, 3 表示查找的字节序数量为 3，即以太网源MAC地址必须以 00:60:37开头

12、长度大于 100 字节的 IP 包

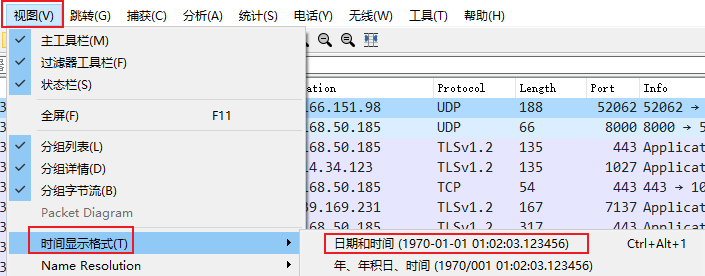
ip.len > 100

**2 设置**

以下设置仅代表作者的个人喜好，请根据自己的风格调整。

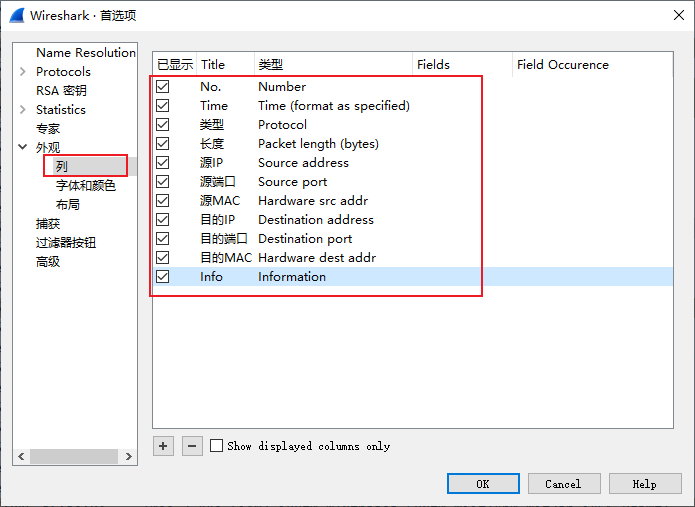
2.1 时间

点击菜单 视图 - 时间显示格式 - 日期和时间。



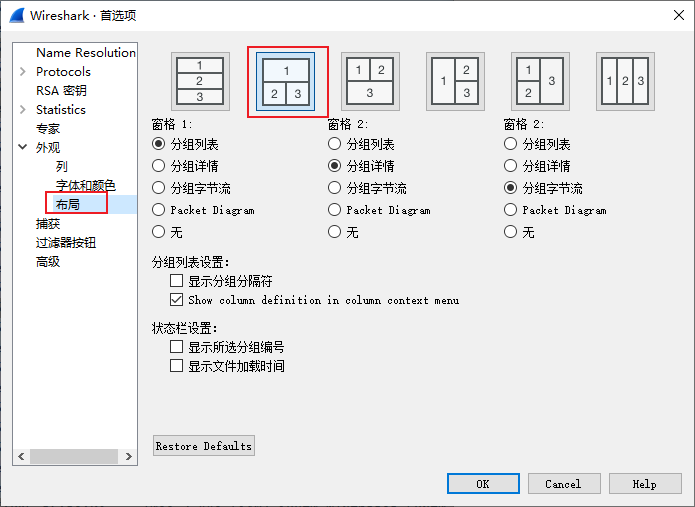
2.2 修改列显示内容

点击菜单 编辑 - 首选项 ，在弹出的首选项对话框中依次展开 外观 - 列，添加并修改显示的列，这里模仿 IPAnalyse 的界面设置。



2.3 窗口排列

点击菜单 编辑 - 首选项 ，在弹出的首选项对话框中依次展开 外观 - 布局，按照图示选择。这里模仿 IPAnalyse 的界面设置。



2.4 禁止解析物理地址

点击菜单 视图 - Name Resolution ，取消 “解析物理地址”。

