

# Wireshark

[EN](#) | [ZH](#)

## Wireshark 常用功能介绍

### 显示过滤器

显示过滤器可以用很多不同的参数来作为匹配标准，比如 IP 地址、协议、端口号、某些协议头部的参数。此外，用户也用一些条件工具和串联运算符创建出更加复杂的表达式。用户可以将不同的表达式组合起来，让软件显示的数据包范围更加精确。在数据包列表面板中显示的所有数据包都可以用数据包中包含的字段进行过滤。

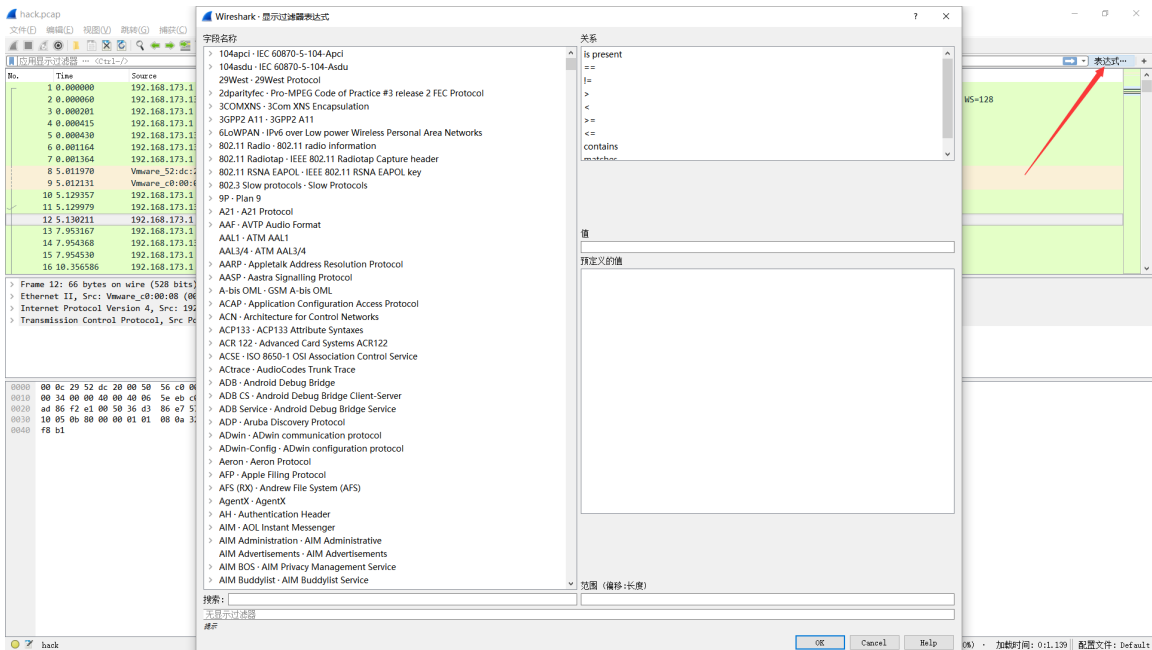
```
[not] Expression [and|or] [not] Expression
```

经常要用到各种运算符

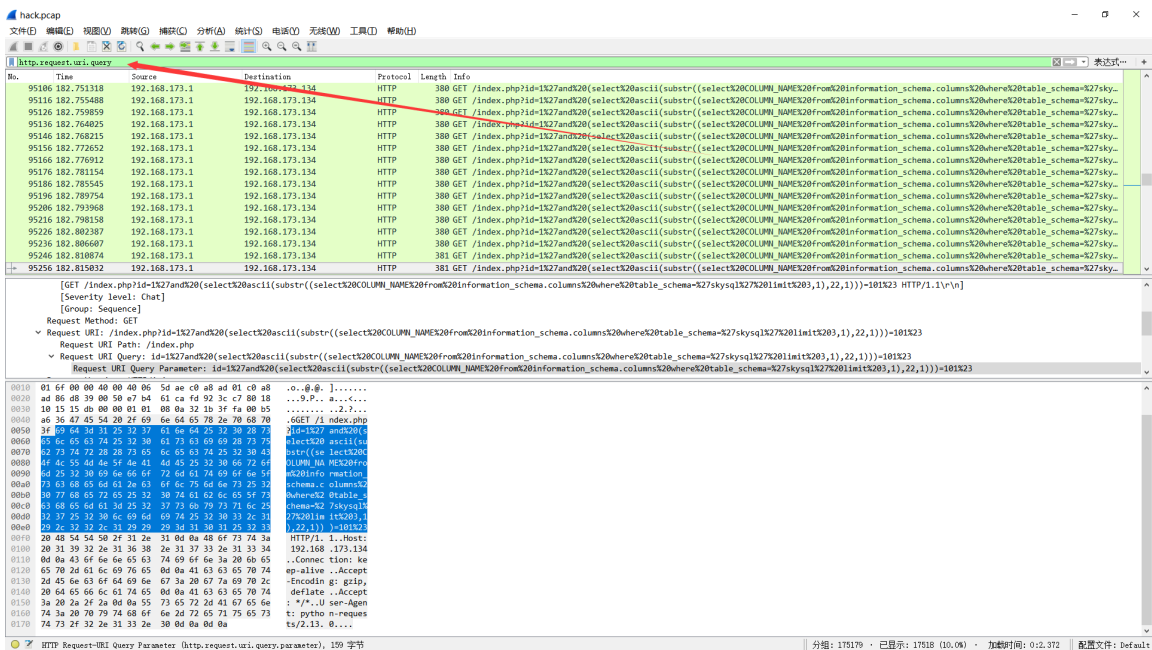
运算符	说明
==	等于
!=	不等于
>	大于
<	小于
>=	大于等于
<=	小于等于
与	and , &&
或	or ,
非	! , not

### 配置方法

## 1. 借助于过滤器窗口



## 1. 借助于工具条的输入栏



## 1. 将数据包某个属性值指定为过滤条件

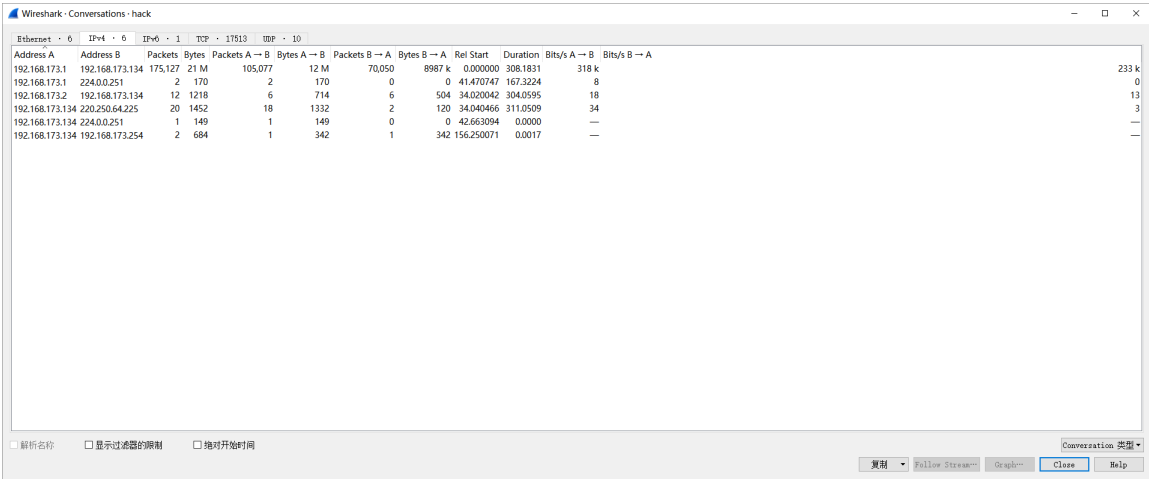


名称	含义
Protocol:	协议名称
% Packets:	含有该协议的包数目在捕捉文件所有包所占的比例
Packets:	含有该协议的包的数目
Bytes:	含有该协议的字节数
Mbit/s:	抓包时间内的协议带宽
End Packets:	该协议中的包的数目（作为文件中的最高协议层）
End Bytes:	该协议中的字节数（作为文件中的最高协议层）
End Mbit/s:	抓包时间内的协议带宽（作为文件中的最高协议层）

这一功能可以为分析数据包的主要方向提供依据

Conversation(对话)

发生于一特定端点的 IP 间的所有流量.

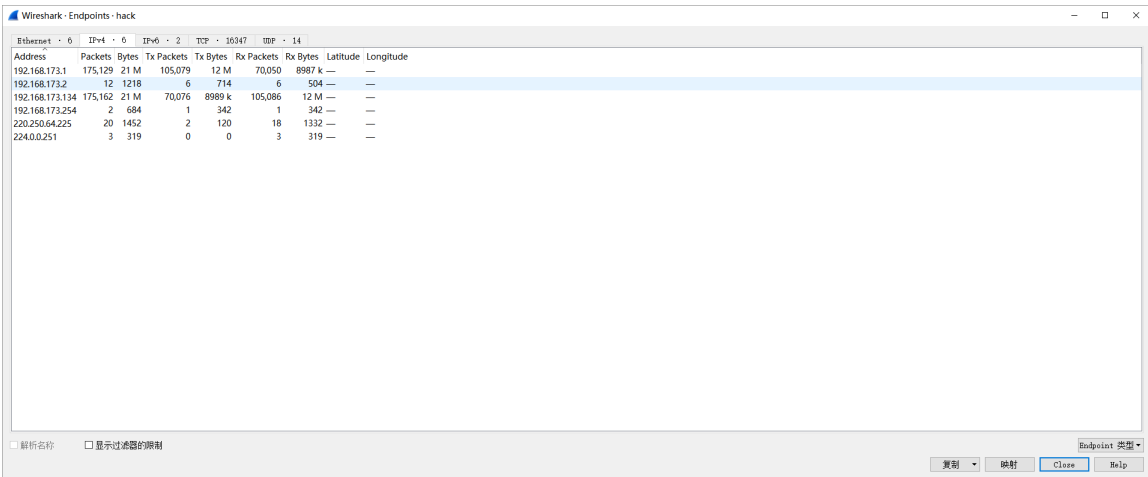


**Note**

- 查看收发大量数据流的 IP 地址。如果你知道的服务器（你记得服务器的地址或地址范围），那问题就解决了；但也有可能只是某台设备正在扫描网络，或仅是一台产生过多数据的 PC。
- 查看扫描模式（scan pattern）。这可能是一次正常的扫描，如 SNMP 软件发送 ping 报文以查找网络，但通常扫描都不是好事情

## EndPoints(端点)

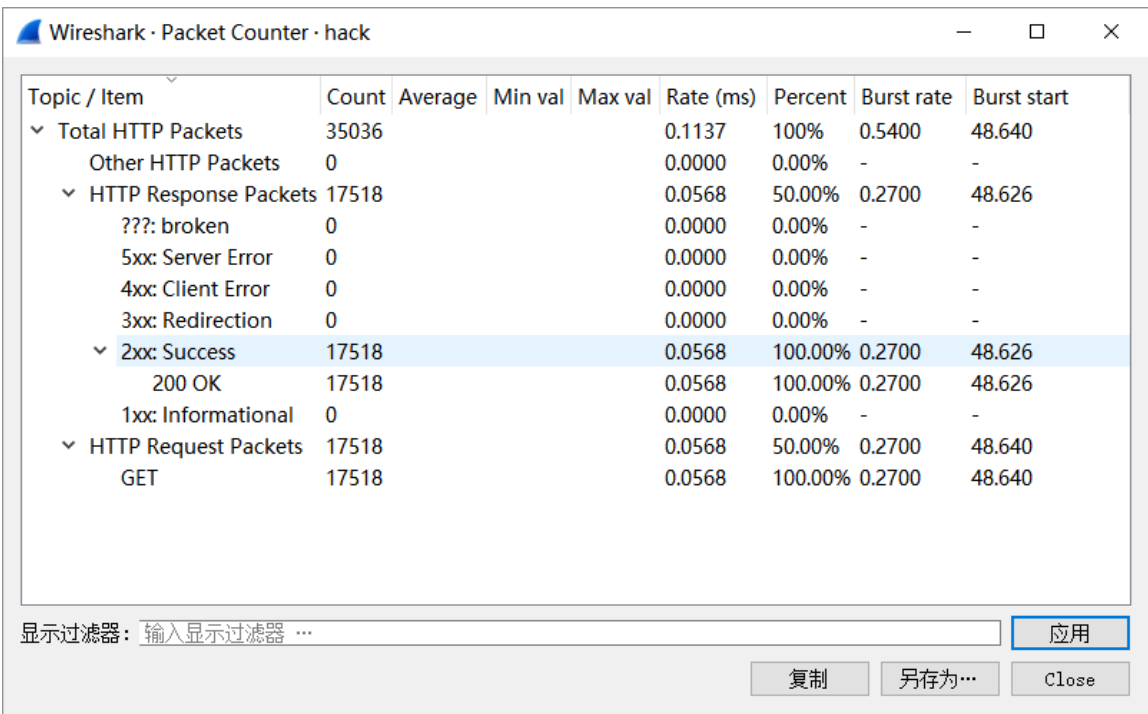
这一工具列出了 Wireshark 发现的所有 endpoints 上的统计信息



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
192.168.173.1	175,129	21 M	105,079	12 M	70,050	8987 k	—	—
192.168.173.2	12	1218	6	714	6	504	—	—
192.168.173.134	175,162	21 M	70,076	8989 k	105,086	12 M	—	—
192.168.173.254	2	694	1	342	1	342	—	—
220.250.64.225	20	1452	2	120	18	1332	—	—
224.0.0.251	3	319	0	0	3	319	—	—

## HTTP

- Packet Counter



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Total HTTP Packets	35036				0.1137	100%	0.5400	48.640
Other HTTP Packets	0				0.0000	0.00%	-	-
▼ HTTP Response Packets	17518				0.0568	50.00%	0.2700	48.626
??? : broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
▼ 2xx: Success	17518				0.0568	100.00%	0.2700	48.626
200 OK	17518				0.0568	100.00%	0.2700	48.626
1xx: Informational	0				0.0000	0.00%	-	-
▼ HTTP Request Packets	17518				0.0568	50.00%	0.2700	48.640
GET	17518				0.0568	100.00%	0.2700	48.640

## 参考

- <http://blog.jobbole.com/73482/>
- <http://www.vuln.cn/2103>

## 信息统计 进阶版