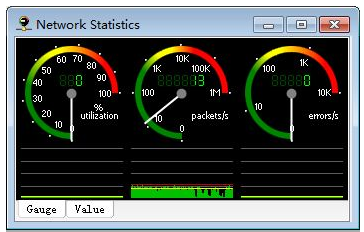
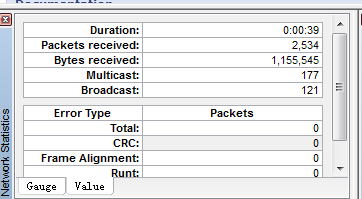
Ominpeek一款网络抓包工具。在测试网络模块中，时不时需要了解网络数据传输，所以发包分析是个常事。Ominpeek是基于网卡底层扫描的。计算机与外界的交流必经过网卡，也就是说这个工具，能检测拿到一切经过网络的数据。

1、下载安装（就是windows下下载安装软件，这里就不多说了）

2、安装完成后，有个网络统计窗口，可以统计网络使用率、数据流量（每秒数据包）、误差率（每秒的总误差）



3、Value选项卡如下，分别有这几个项：**持续时间、收到的数据包、接收的字节数、组播（**此参数显示包处理多播地址从你开始收集监测统计）、**广播（**此参数显示的数据包广播地址从你开始收集监测统计）



4、日志窗口，可以鼠标右键进行关于日志相关操作，主要记录1、 程序的启动或停止，或创建一个新的窗口捕捉；2、在设置对话框中指定的事件；3、 活动指定发送的日志类型通知。

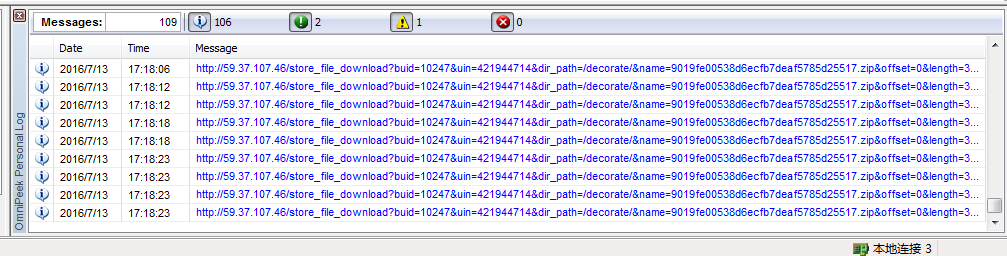
其中**Messages**: 信息总数

**白色i** ：表示请求成功的信息。

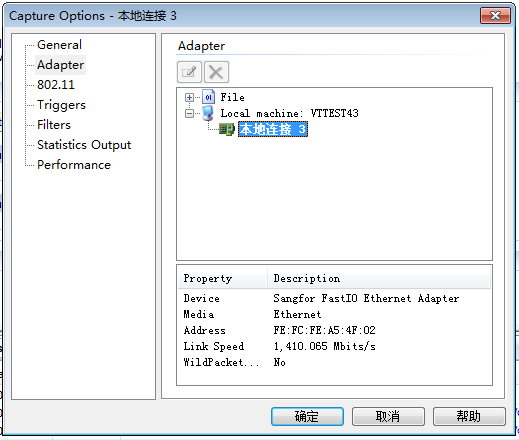
**绿色!** ：表示轻微类型的提示

**黄色!** ：警告信息

**红色x** ：错误信息



5、创建数据捕捉，点击Capture下的“new capture”按钮，在图中鼠标所在的标签下，进行相应网卡设置，比如要对那个网卡进行捕捉。Filters下面是对相关协议包的规则过滤。然后选择相应要抓取的协议类型（只抓此类型的协议），选择完成后，开始点击start capture抓取。



1. 协议分析，它可以进行主机排名，发现网络中通信量最大的主机，对比故障现象与影响范围（这个实际中用的比较多）。协议排名，可以对监控的所有协议进行排名，找到使用最多的协议（比较少用）。还可以进行主机在使用的协议统计。查看某一主机在使用哪些协议。

还可通过PeerMap网络分布图了解主机会话的实时情况（功能比较强大，目前我自己研究比较浅，有兴趣的可以详细研究下）

1. 可以对过程抓到的包，进行双击打开抓到的各种协议，查看协议分析情况，以下是一个http协议的示例。还有很多其他协议tcp和udp的都相当清晰，尤其是tcp的握手过程。还是相当强大的。

