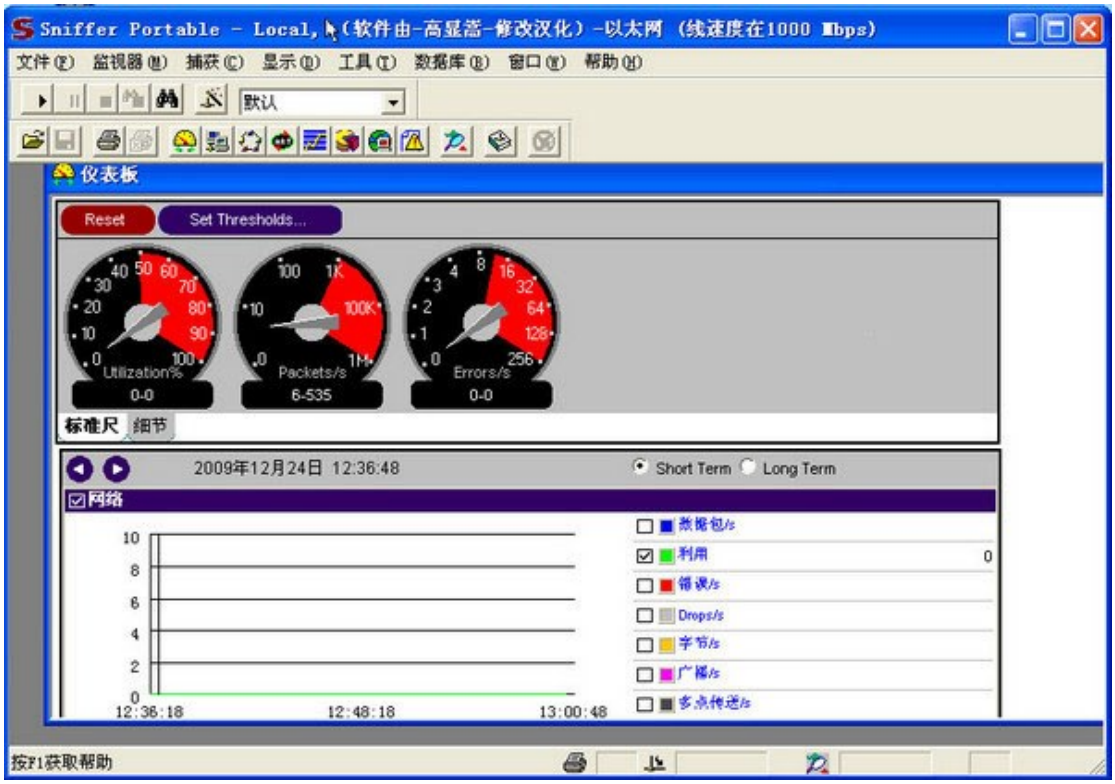
信息安全概论 作业 2　sniffer 类软件的使用

2003007 120L022115-王炳轩

Sniffer，中文可以翻译为嗅探器，也叫抓数据包软件，是一种基于被动侦听原理的网络分析方式。使用这种技术方式，可以监视网络的状态、数据流动情况以及网络上传输的信息。Sniffer 软件是 NAI 公司推出的一款一流的便携式网管和应用故障诊断分析软件，不管是在有线网络还是在无线网络中，它都能够给予网管管理人员实时的网络监视、数据包捕获以及故障诊断分析能力。对于在现场运行快速的网络和应用问题故障诊断，基于便携式软件的解决方案具备最高的性价比，却能够让用户获得强大的网管和应用故障诊断功能。Sniffer Pro 是一款功能强大的网络监控软件，软件可以对网络进行实时监控，帮助用户捕获网络流量进行详细分析，让用户可以完全掌握网络的流通情况，更好的维护网络安全！

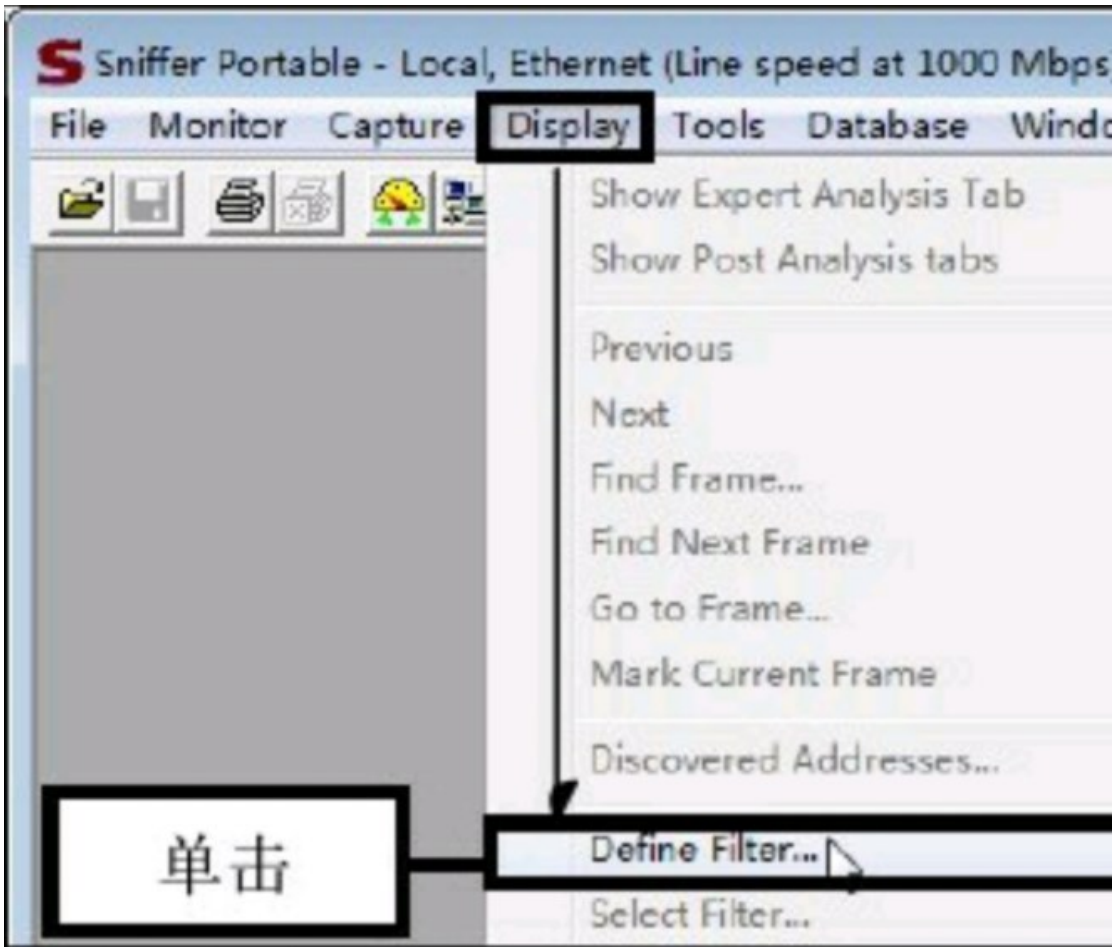


Sniffer Pro 使用说明

1、成功安装 Sniffer Pro 后点击“开始”按钮;

2、在弹出的“开始”菜单中依次点击“所有程序>Sniffer Pro>Sniffer”命令，启动 Sniffer Pro 应用程序。

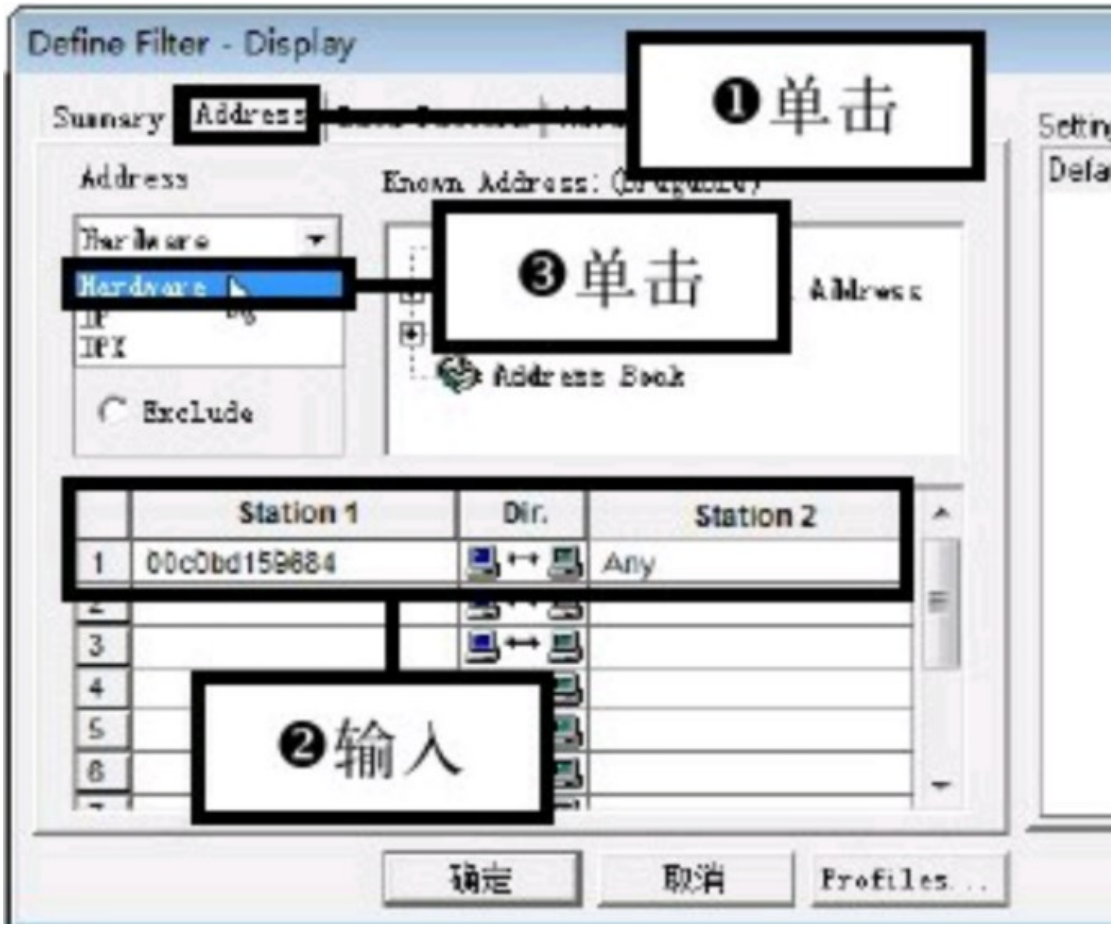
3、单击 Define Filter 命令：打开 Sniffer Pro 主界面，在菜单栏依次单击“Display>Define Filter”命令



4、设置捕获条件：弹出 Define Filter 对话框，切换至 Address 选项卡下，

5、在 Station1 以及 Station2 的列表中输入捕获地址，如在 Station1 下方输入 00c0bd159684，此时 Station2 会自动显示 any,

6、然后在 Address 下拉列表中选择捕获条件，例如选择 Hardware，即基本捕获条件

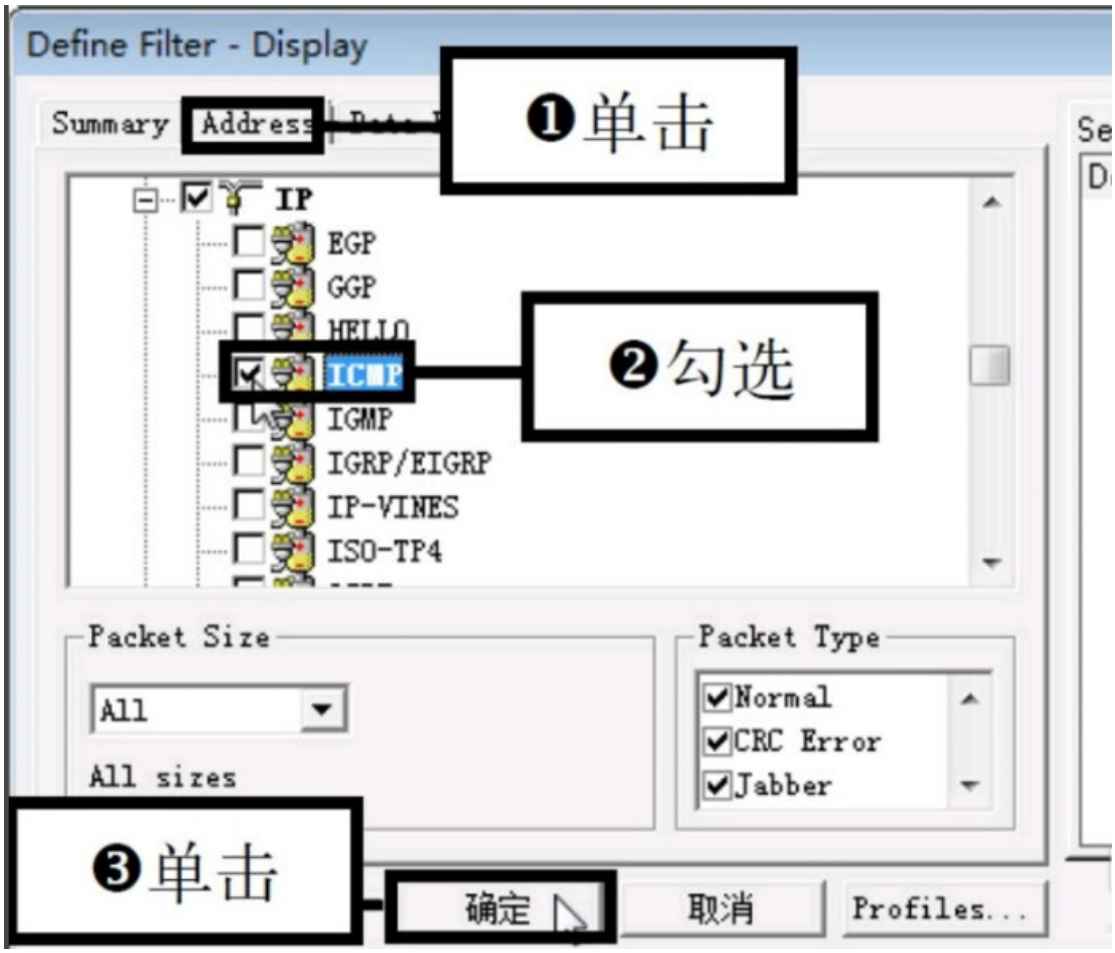


7、编辑协议捕获条件：

（1）切换至 Advanced 选项卡，

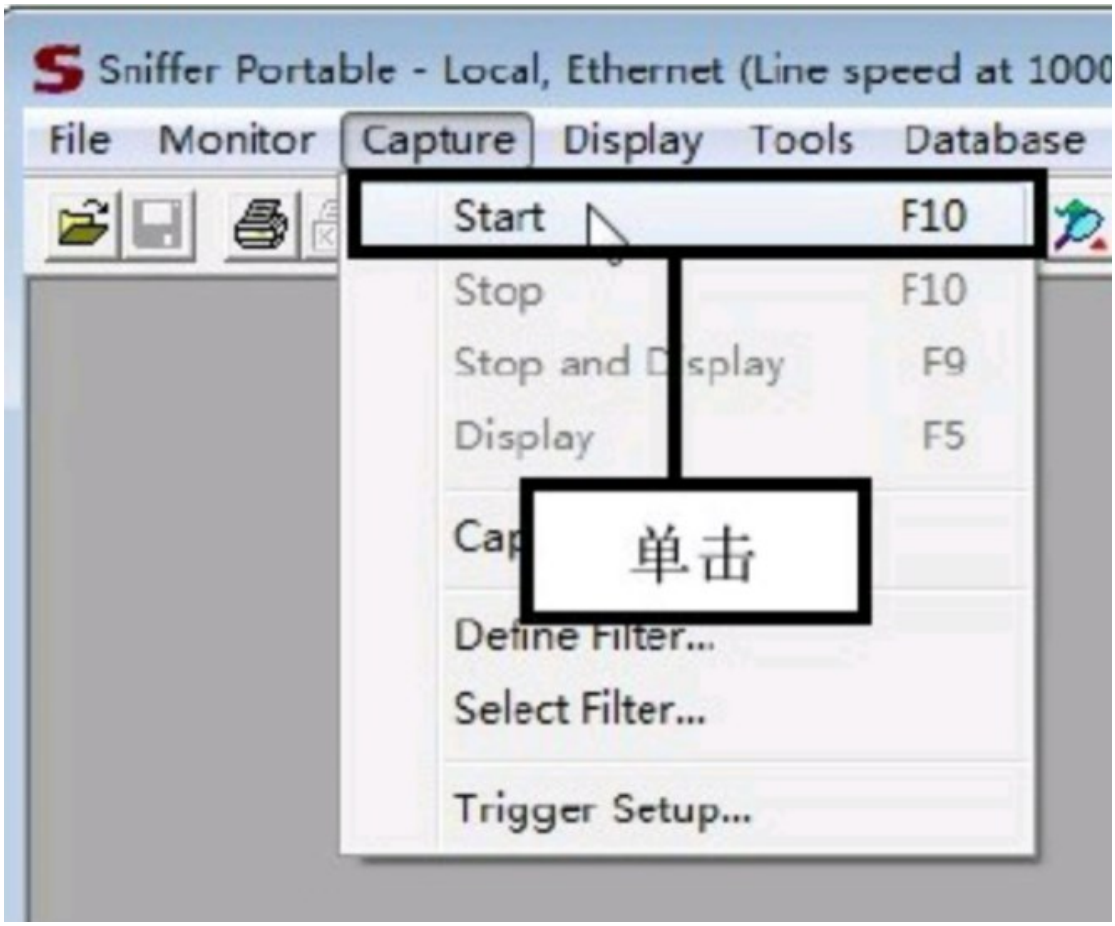
（2）在列表框中选择协议捕获条件，例如依次勾选“IP>ICMP”复选框，即 ICMP 就是要捕获的协议，

（3）然后点击“确定”按钮。



8、开始捕获：

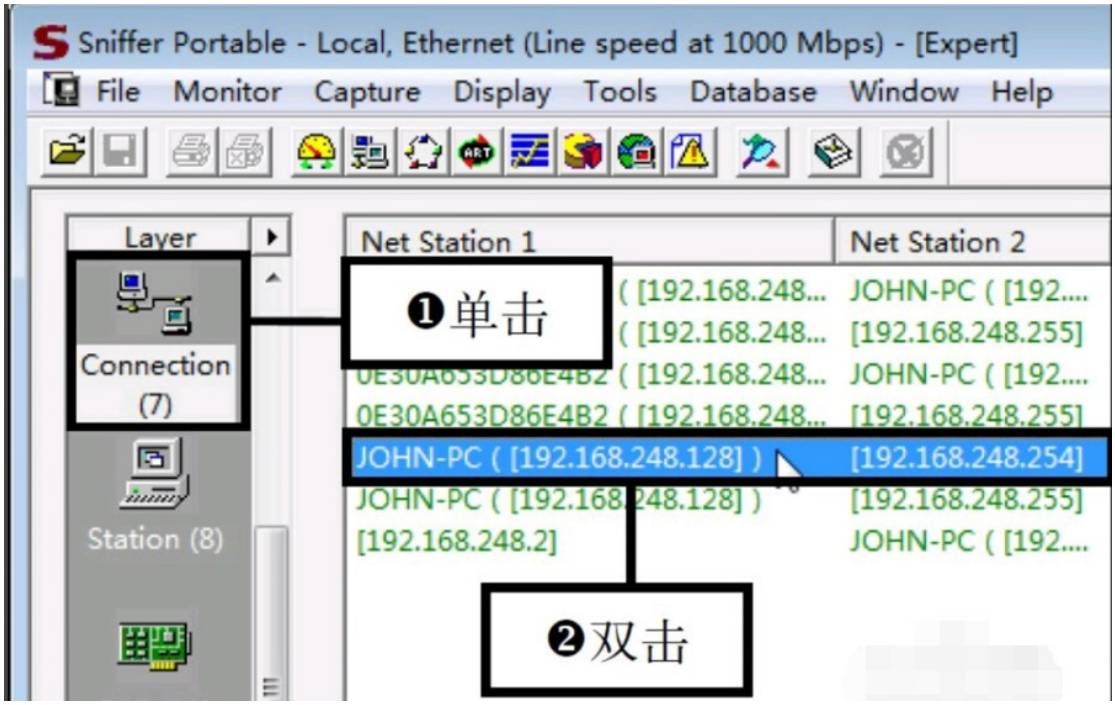
（1）返回 Sniffer Pro 主界面，在菜单栏中依次单击“Capture>Start”命令，开始捕获局域网中的数据包。



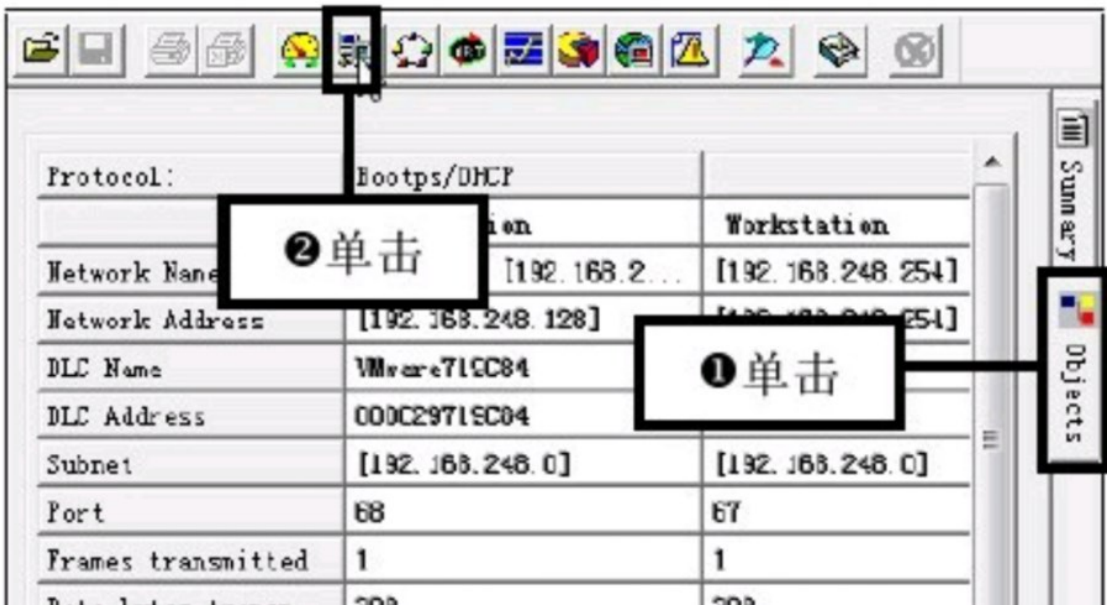
9、查看并选择捕获的数据包信息：

（1）在窗口左侧单击 Connection 选项，此时可在窗口中看见捕获到的信息包以及发送和接收该数据包的计算机地址，

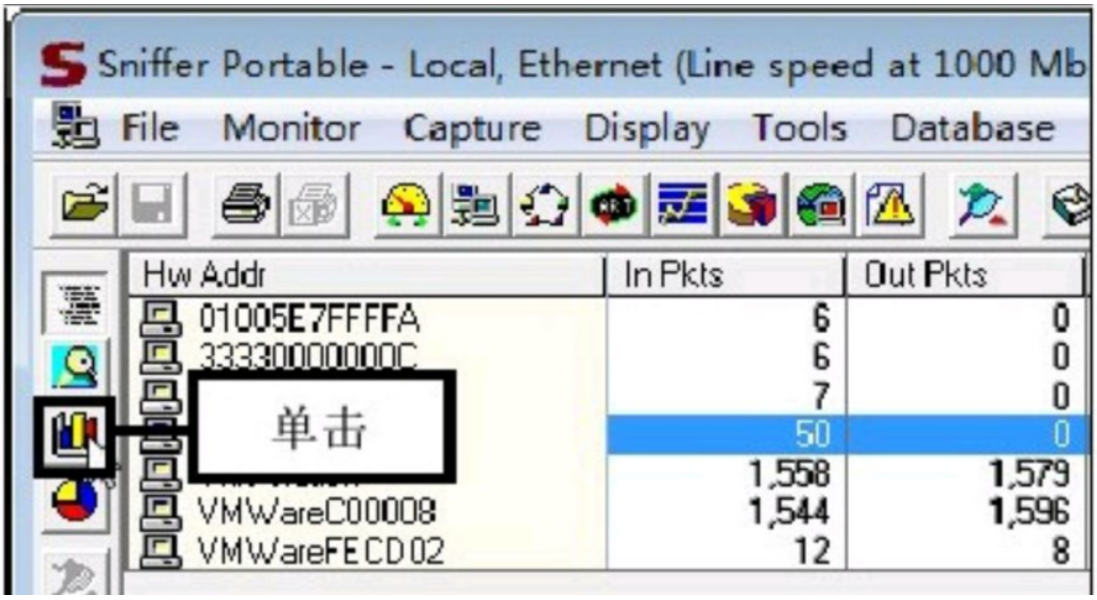
（2）选中任意一条捕获的数据包信息双击对应的选项。



10、查看报文详细信息：切换至 Objects 选项卡，在该界面中显示了该报文的详细信息，单击【Host Table】按钮，查看报文统计。

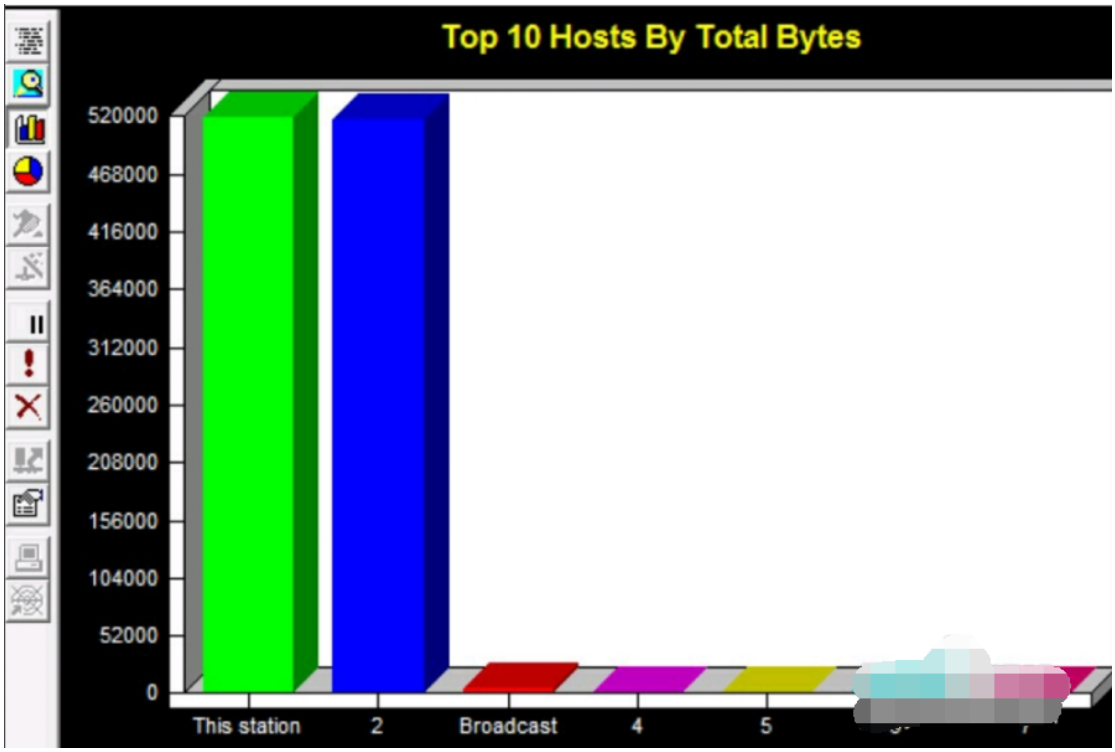


11、查看报文统计信息：此时可在窗口中看见该报文的统计信息，若想查看报文对应的图形统计，可单击左侧的柱形图标按钮。



12、查看报文柱形统计图：

（1）此时窗口中出现了该报文的柱形统计图。纵坐标为数据包，横坐标为捕获地址。



Sniffer Pro 功能介绍

网络安全的保障与维护

1、对异常的网络攻击的实时发现与告警；

2、对高速网络的捕获与侦听；

3、全面分析与解码网络传输的内容；

面向网络链路运行情况的监测

1、各种网络链路的运行情况；

2、各种网络链路的流量及阻塞情况；

3、网上各种协议的使用情况；

4、网络协议自动发现；

5、网络故障监测；

面向网络上应用情况的监测

1、任意网段应用流量、流向；

2、任意服务器应用流量、流向；

3、任意工作站应用流量、流向；

4、典型应用程序响应时间；

5、不同网络协议所占带宽比例；

6、不同应用流量、流向的分布情况及拓扑结构；

强大的协议解码能力，用于对网络流量的深入解析

1、对各种现有网络协议进行解码；

2、对各种应用层协议进行解码；

3、Sniffer 协议开发包（PDK）可以让用户简单方便地增加用户自定义的协议；

网络管理、故障报警及恢复

运用强大的专家分析系统帮助维护人员在最短时间内排除网络故障；

根据用户习惯，Sniffer 可提供实时数据或图表方式显示统计结果，统计内容包括：

网络统计：如当前和平均网络利用率、总的和当前的帧数及字节数、总站数和激活的站数、协议类型、当前和总的平均帧长等。

协议统计：如协议的网络利用率、协议的数、协议的字节数以及每种协议中各种不同类型的帧的统计等。

差错统计：如错误的 CRC 校验数、发生的碰撞数、错误帧数等。

站统计：如接收和发送的帧数、开始时间、停止时间、消耗时间、站状态等。最多可统计 1024 个站。

帧长统计：如某一帧长的帧所占百分比，某一帧长的帧数等。

当某些指标超过规定的阈值时，Sniffer 可以自动显示或采用有声形式的告警。

Sniffer 可根据网络管理者的要求，自动将统计结果生成多种统计报告格式，并可存盘或打印输出。

Sniffer Pro 软件特色

1、捕获网络流量进行详细分析

2、利用专家分析系统诊断问题

3、收集网络利用率和错误等

4、Sniffer Pro 中文版实时监控网络活动

网络的安全性和高可用性是建立在有效的网络管理基础之上的,网络管理包括配置管理、故障管理、性能管理、安全管理和计费管理五大部分。对于企业计算机网络来说，网络故障管理主要侧重于实时的监控，而网络性能管理更看中历史分析。
Sniffer 网络分析仪是一个网络故障、性能和安全管理的有力工具，它能够自动地帮助网络专业人员维护网络，查找故障，极大地简化了发现和解决网络问题的过程，广泛适用于 Ethernet、Fast Ethernet、Token Ring、Switched LANs、FDDI、X.25、DDN、Frame Relay、ISDN、ATM 和 Gigabits 等网络。
网络安全的保障与维护
1. 对异常的网络攻击的实时发现与告警；
2. 对高速网络的捕获与侦听；
3. 全面分析与解码网络传输的内容；
面向网络链路运行情况的监测
1. 各种网络链路的运行情况；
2. 各种网络链路的流量及阻塞情况；
3. 网上各种协议的使用情况；
4. 网络协议自动发现；
5. 网络故障监测；
面向网络上应用情况的监测
1. 任意网段应用流量、流向；
2. 任意服务器应用流量、流向；
3. 任意工作站应用流量、流向；
4. 典型应用程序响应时间；
5. 不同网络协议所占带宽比例；
6. 不同应用流量、流向的分布情况及拓扑结构；
强大的协议解码能力，用于对网络流量的深入解析
1. 对各种现有网络协议进行解码；

2. 对各种应用层协议进行解码；
3. Sniffer 协议开发包（PDK）可以让用户简单方便地增加用户自定义的协议；
网络管理、故障报警及恢复
运用强大的专家分析系统帮助维护人员在最短时间内排除网络故障；
根据用户习惯，Sniffer 可提供实时数据或图表方式显示统计结果，统计内容包括：
网络统计：如当前和平均网络利用率、总的和当前的帧数及字节数、总站数和激活的站数、协议类型、当前和总的平均帧长等。
协议统计：如协议的网络利用率、协议的数、协议的字节数以及每种协议中各种不同类型的帧的统计等。
差错统计：如错误的 CRC 校验数、发生的碰撞数、错误帧数等。
站统计：如接收和发送的帧数、开始时间、停止时间、消耗时间、站状态等。最多可统计 1024 个站。
帧长统计：如某一帧长的帧所占百分比，某一帧长的帧数等。
当某些指标超过规定的阈值时，Sniffer 可以自动显示或采用有声形式的告警。
Sniffer 可根据网络管理者的要求，自动将统计结果生成多种统计报告格式，并可存盘或打印输出。
Sniffer 实时专家分析系统
高度复杂的网络协议分析工具能够监视并捕获所有网络上的信息数据包，并同时建立一个特有网络环境下的目标知识库。智能的专家技术扫描这些信息以检测网络异常现象，并自动对每种异常现象进行归类。所有异常现象被归为两类：一类是 symptom（故障征兆提示，非关键事件例如单一文件的再传送），另一类是 diagnosis（已发现故障的诊断，重复出现的事件或要求立刻采取行动的致命错误）。经过问题分离、分析且归类后，Sniffer 将实时地，自动发出一份警告、对问题进行解释并提出相应的建议解决方案。
Sniffer 与其他网络协议分析仪最大的差别在于它的人工智能专家系统(Expert System)。简单地说，Sniffer 能自动实时监视网络，捕捉数据，识别网络配置，自动发现网络故障并进行告警，它能指出：
网络故障发生的位置，以及出现在 OSI 第几层。
网络故障的性质，产生故障的可能的原因以及为解决故障建议采取的行动。
Sniffer 还提供了专家配制功能，用户可以自已设定专家系统判断故障发生的触发条件。
有了专家系统，您无需知道那些数据包构成网络问题，也不必熟悉网络协议，更不用去了解这些数据包的内容，便能轻松解决问题。