嗅探器试验报告

目录

一、 实验目的.....1
二、 试验环境.....1
三、 试验原理.....1
1. sniffer 原理.....1
1) 网络技术与设备简介.....2
2) 网络监听原理.....2
3) Sniffer 分类.....2
4) 网络监听的目的.....3
2. 电子邮件协议.....3
3.sniffer 软件使用方法.....4
四、 实验步骤及结果截图.....5
1. 设置捕获数据包的过滤规则.....5
2. 打开捕获数据包.....8
3. 打开一个网页，输入用户名和密码.....9
4. 分析捕获的数据包获得用户名和密码.....11

一、实验目的

1. 熟悉 sniffer 使用方法，熟悉嗅探器原理。
2. 使用 sniffer 捕获数据包，获取邮箱用户名和密码。

二、试验环境

1. 系统环境：WinXP
2. 使用软件：sniffer

三、试验原理

1.sniffer 原理

当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置在监听模式，便可以将网上传输的源源不断的信息截获。Sniffer 技术常常被黑客们

用来截获用户的口令，据说某个骨干网络的路由器网段曾经被黑客攻入，并嗅探到大量的用户口令。但实际上 Sniffer 技术被广泛地应用于网络故障诊断、协议分析、应用性能分析和网络安全保障等各个领域。

1)网络技术与设备简介

在讲述 Sniffer 的概念之前，首先需要讲述局域网设备的一些基本概念。

数据在网络上是以很小的称为帧（Frame）的单位传输的，帧由几部分组成，不同的部分执行不同的功能。帧通过特定的称为网络驱动程序的软件进行成型，然后通过网卡发送到网线上，通过网线到达它们的目的机器，在目的机器的一端执行相反的过程。接收端机器的以太网卡捕获到这些帧，并告诉操作系统帧已到达，然后对其进行存储。就是在这个传输和接收的过程中，嗅探器会带来安全方面的问题。

每一个在局域网（LAN）上的工作站都有其硬件地址，这些地址惟一地表示了网络上的机器（这一点与 Internet 地址系统比较相似）。当用户发送一个数据包时，这些数据包就会发送到 LAN 上所有可用的机器。

如果使用 Hub/即基于共享网络的情况下，网络上所有的机器都可以“听”到通过的流量，但对不属于自己的数据包则不予响应（换句话说，工作站 A 不会捕获属于工作站 B 的数据，而是简单地忽略这些数据）。如果某个工作站的网络接口处于混杂模式（关于混杂模式的概念会在后面解释），那么它就可以捕获网络上所有的数据包和帧。

但是现代网络常常采用交换机作为网络连接设备枢纽，在通常情况下，交换机不会让网络中每一台主机侦听到其他主机的通讯，因此 Sniffer 技术在这时必须结合网络端口镜像技术进行配合。而衍生的安全技术则通过 ARP 欺骗来变相达到交换网络中的侦听。

2)网络监听原理

Sniffer 程序是一种利用以太网的特性把网络适配卡（NIC，一般为以太网卡）置为杂乱（promiscuous）模式状态的工具，一旦网卡设置为这种模式，它就能接收传输在网络上的每一个信息包。

普通的情况下，网卡只接收和自己的地址有关的信息包，即传输到本地主机的信息包。要使 Sniffer 能接收并处理这种方式的信息，系统需要支持 BPF，Linux 下需要支持 SOCKET 一 PACKET。但一般情况下，网络硬件和 TCP／IP 堆栈不支持接收或者发送与本地计算机无关的数据包，所以，为了绕过标准的 TCP／IP 堆栈，网卡就必须设置为我们刚开始讲的混杂模式。一般情况下，要激活这种方式，内核必须支持这种伪设备 Bpfilter，而且需要 root 权限来运行这种程序，所以 sniffer 需要 root 身份安装，如果只是以本地用户的身份进入了系统，那么不可能嗅探到 root 的密码，因此不能运行 Sniffer。

也有基于无线网络、广域网络(DDN, FR)甚至光网络(POS、Fiber Channel)的监听技术，这时候略微不同于以太网络上的捕获概念，其中通常会引入 TAP (测试介入点)这类的硬件设备来进行数据采集。

3)Sniffer 分类

Sniffer 分为软件和硬件两种，软件的 Sniffer 有 Sniffer Pro、Network Monitor、PacketBone 等，其优点是易于安装部署，易于学习使用，同时也易于交流；缺点是无法抓取网络上所有

的传输，某些情况下也就无法真正了解网络的故障和运行情况。硬件的 Sniffer 通常称为协议分析仪，一般都是商业性的，价格也比较昂贵，但会具备支持各类扩展的链路捕获能力以及高性能的数据实时捕获分析的功能。

基于以太网络嗅探的 Sniffer 只能抓取一个物理网段内的包，就是说，你和监听的目标中间不能有路由或其他屏蔽广播包的设备，这一点很重要。所以，对一般拨号上网的用户来说，是不可能利用 Sniffer 来窃听到其他人的通信内容的。

4)网络监听的目的

当一个黑客成功地攻陷了一台主机，并拿到了 root 权限，而且还想利用这台主机去攻击同一（物理）网段上的其他主机时，他就会在这台主机上安装 Sniffer 软件，对以太网设备上传送的数据包进行侦听，从而发现感兴趣的包。如果发现符合条件的包，就把它存到一个 LOg 文件中去。通常设置的这些条件是包含字“username”或“password”的包，这样的包里面通常有黑客感兴趣的密码之类的东西。一旦黑客截获得了某台主机的密码，他就会立刻进入这台主机。

如果 Sniffer 运行在路由器上或有路由功能的主机上，就能对大量的数据进行监控，因为所有进出网络的数据包都要经过路由器。

Sniffer 属于第 M 层次的攻击。就是说，只有在攻击者已经进入了目标系统的情况下，才能使用 Sniffer 这种攻击手段，以便得到更多的信息。

Sniffer 除了能得到口令或用户名外，还能得到更多的其他信息，比如一个重要的信息、在网上传送的金融信息等等。Sniffer 几乎能得到任何在以太网上传送的数据包。

2.电子邮件协议

当前常用的电子邮件协议有 SMTP、POP3、IMAP4，它们都隶属于 TCP/IP 协议簇，默认状态下，分别通过 TCP 端口 25、110 和 143 建立连接。下面分别对其进行简单介绍。

1）SMTP 协议

SMTP 的全称是“Simple Mail Transfer Protocol”，即简单邮件传输协议。它是一组用于从源地址到目的地址传输邮件的规范，通过它来控制邮件的中转方式。SMTP 协议属于 TCP/IP 协议簇，它帮助每台计算机在发送或中转信件时找到下一个目的地。SMTP 服务器就是遵循 SMTP 协议的发送邮件服务器。SMTP 认证，简单地说就是要求必须在提供了账户名和密码之后才可以登录 SMTP 服务器，这就使得那些垃圾邮件的散播者无可乘之机。增加 SMTP 认证的目的是为了使用户避免受到垃圾邮件的侵扰。

2）POP 协议

POP 邮局协议负责从邮件服务器中检索电子邮件。它要求邮件服务器完成下面几种任务之一：从邮件服务器中检索邮件并从服务器中删除这个邮件；从邮件服务器中检索邮件但不删除它；不检索邮件，只是询问是否有新邮件到达。POP 协议支持多用户互联网邮件扩展，后者允许用户在电子邮件上附带二进制文件，如文字处理文件和电子表格文件等，实际上这样就可以传输任何格式的文件了，包括图片和声音文件等。在用户阅读邮件时，POP 命令所有的邮件信息立即下载到用户的计算机上，不在服务器上保留。

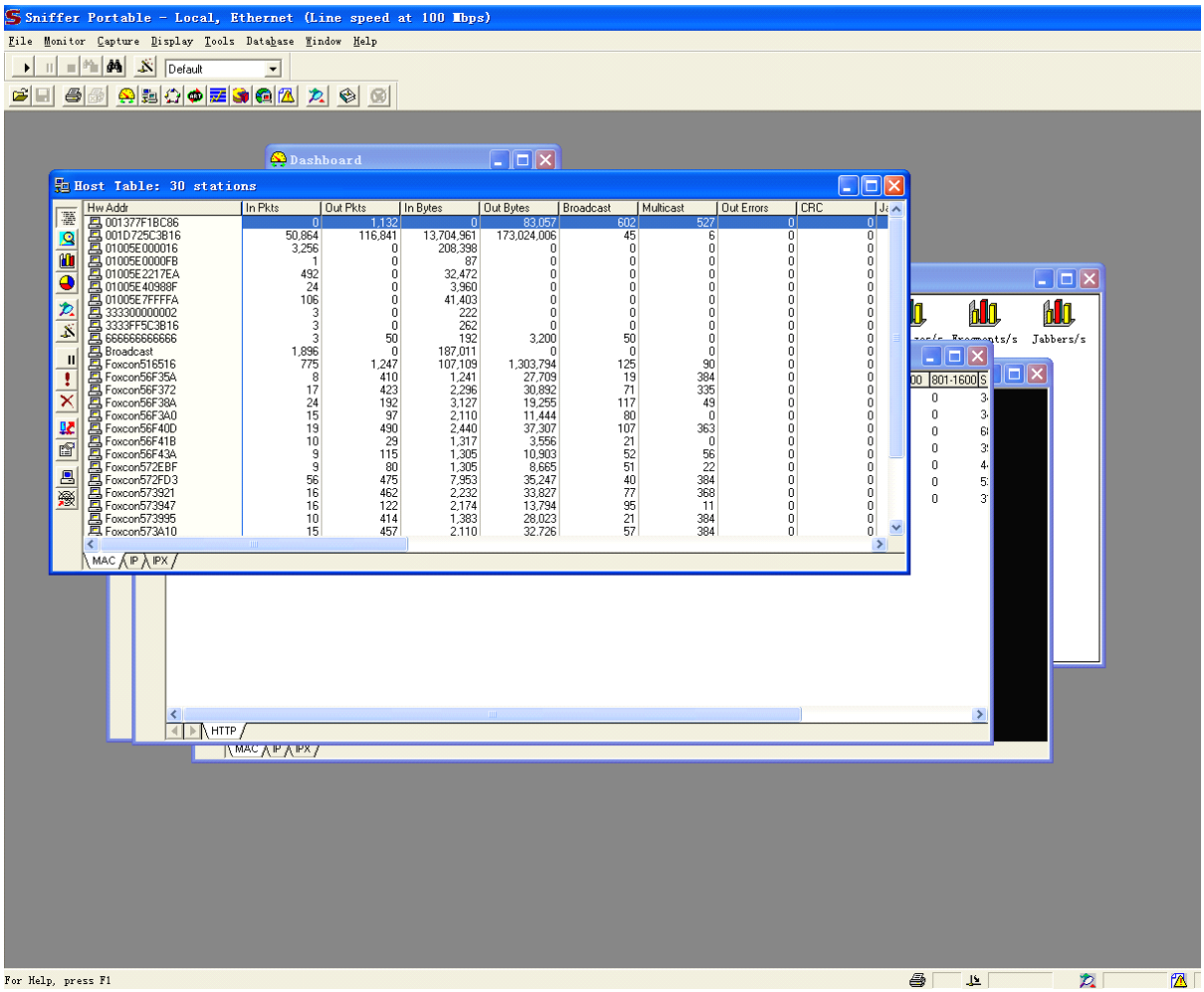
3）IMAP 协议

互联网信息访问协议（IMAP）是一种优于 POP 的新协议。和 POP 一样，IMAP 也能下载邮件、从服务器中删除邮件或询问是否有新邮件，但 IMAP 克服了 POP 的一些缺点。例

如，它可以决定客户机请求邮件服务器提交所收到邮件的方式，请求邮件服务器只下载所选中的邮件而不是全部邮件。客户机可先阅读邮件信息的标题和发送者的名字再决定是否下载这个邮件。通过用户的客户机电子邮件程序，IMAP 可让用户在服务器上创建并管理邮件文件夹或邮箱、删除邮件、查询某封信的一部分或全部内容，完成所有这些工作时都不需要把邮件从服务器下载到用户的个人计算机上。

3.sniffer 软件使用方法

sniffer 软件开始界面如下图所示：



下面是基本工具栏介绍：

通常使用工具栏如下：

下图是开始捕获数据包按钮：

该按钮开始一个新的捕获数据包的工作。

下图是暂停捕获按钮：

该按钮是当前捕获数据包暂停。

下图是终止捕获按钮：

该按钮终止当前捕获数据包的工作。

下图是禁止查看信息按钮：

该按钮禁止查看捕获到数据包的相应代码等信息。

下图是查看信息按钮：

该按钮允许查看捕获到的数据包的详细信息。

下图是设置过滤规则按钮：

该按钮设置捕获数据包的过滤规则。
上述就是本次试验将要用到的相应的工具按钮。

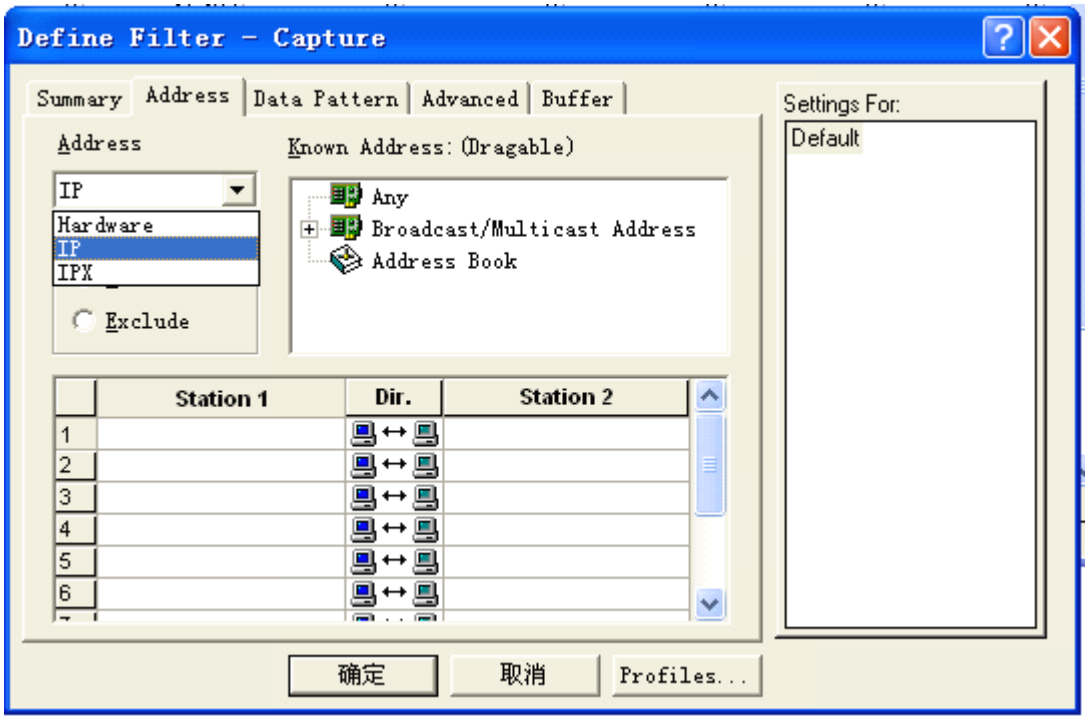
四、实验步骤及结果截图

1. 设置捕获数据包的过滤规则

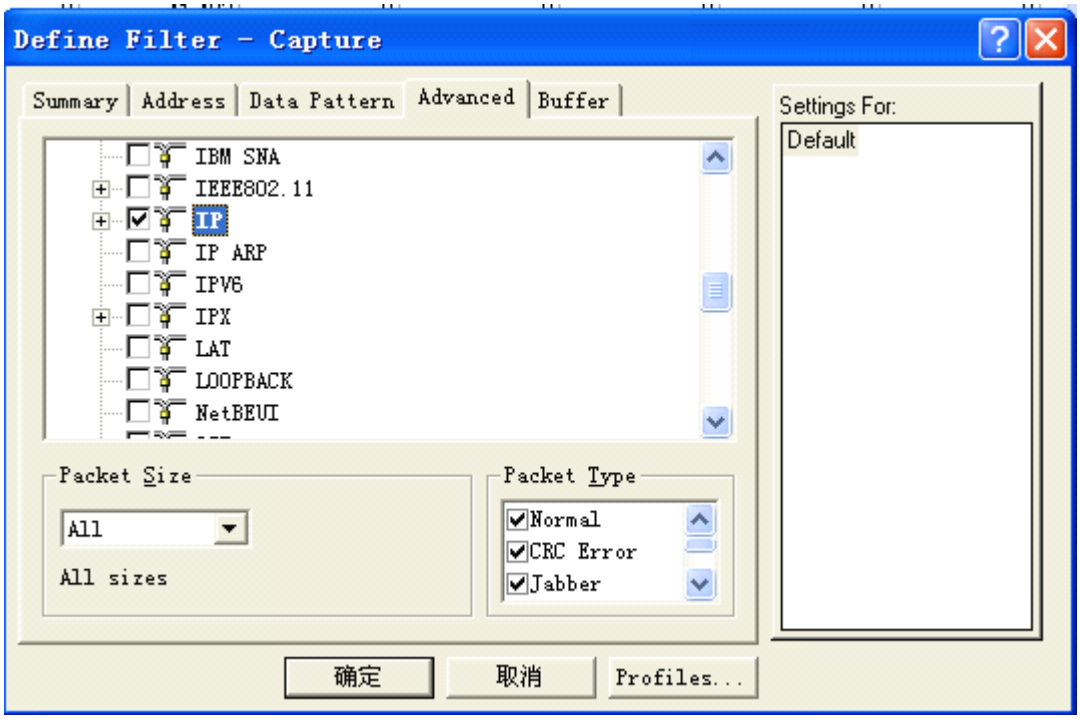
设置捕获数据包的相应规则，使捕获数据包为 TCP 协议包。

1） 点击设置过滤器按钮,打开过滤器设置。

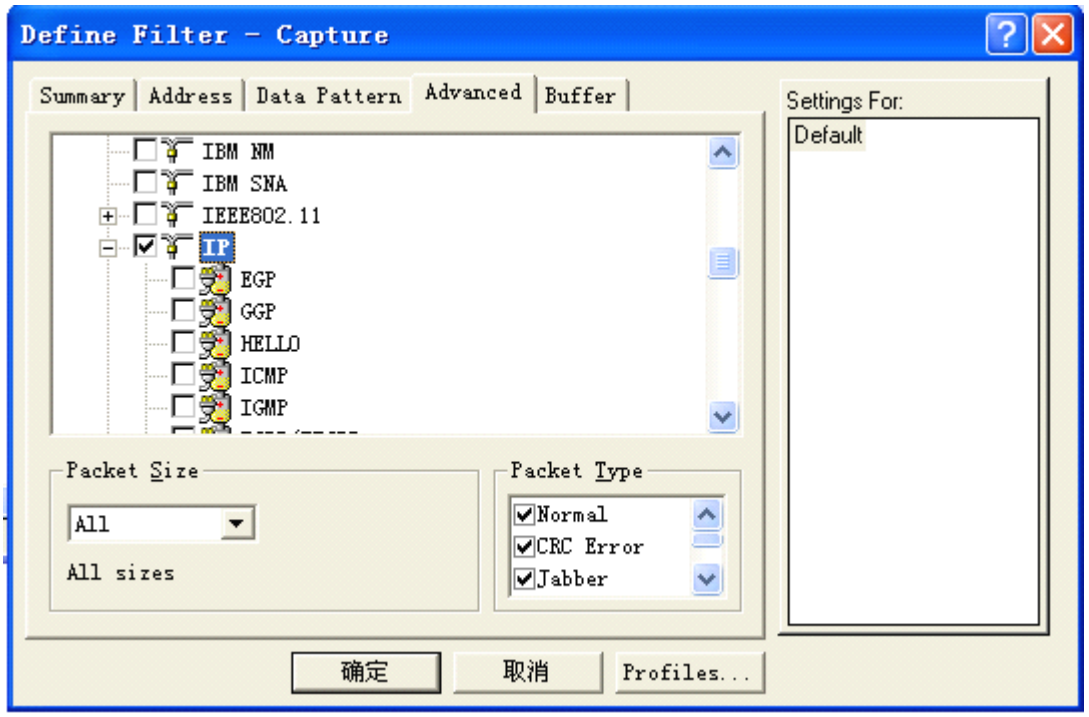
2） 在过滤器设置窗口中“address”栏“address”项下选择“IP”。



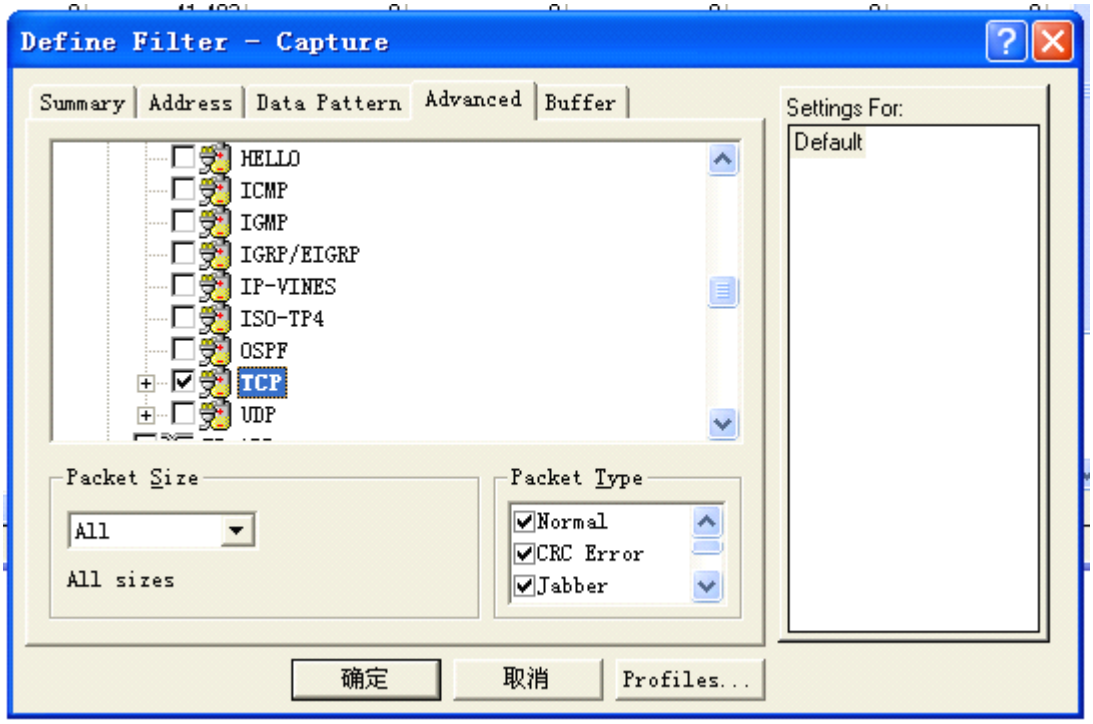
3） 在过滤器设置窗口中“advance”栏“IP”项前打钩。



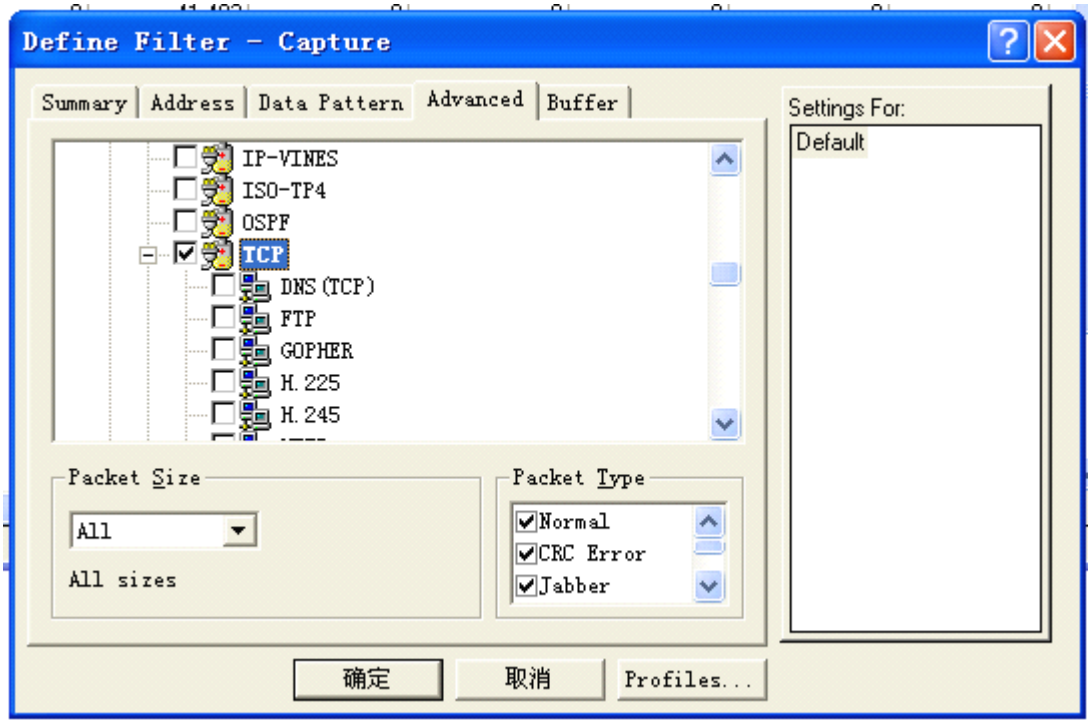
打开 IP 栏查看。



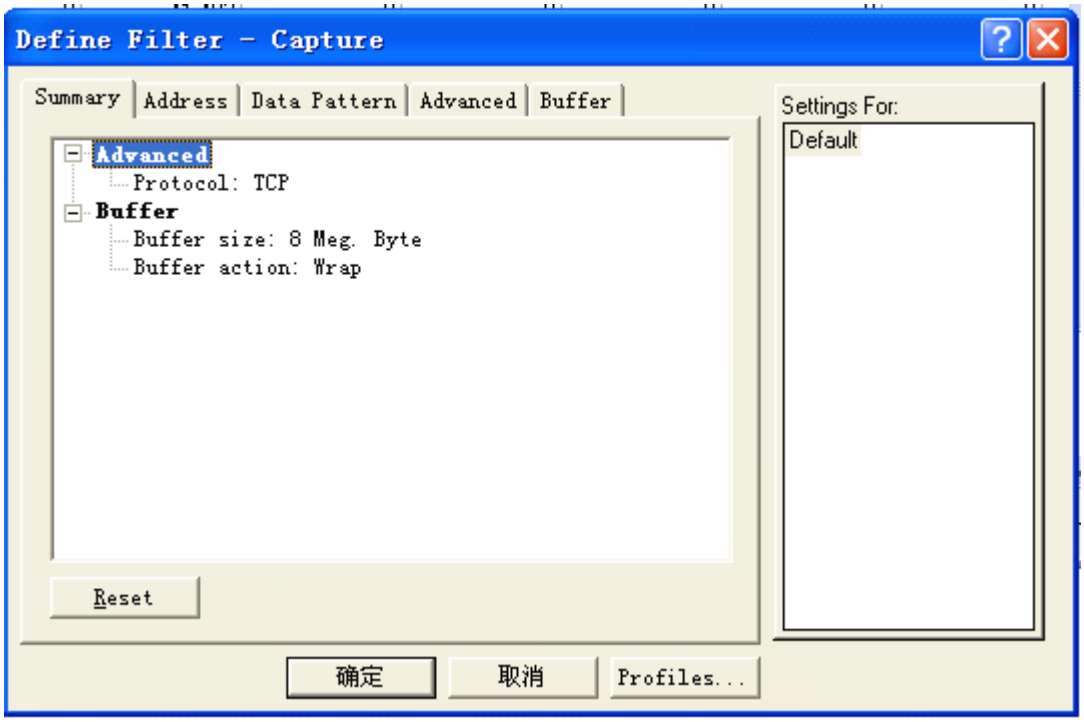
4） 在过滤器设置窗口中“advance”栏“IP”项内“TCP”项前打钩。



查看“TCP”项下内容。



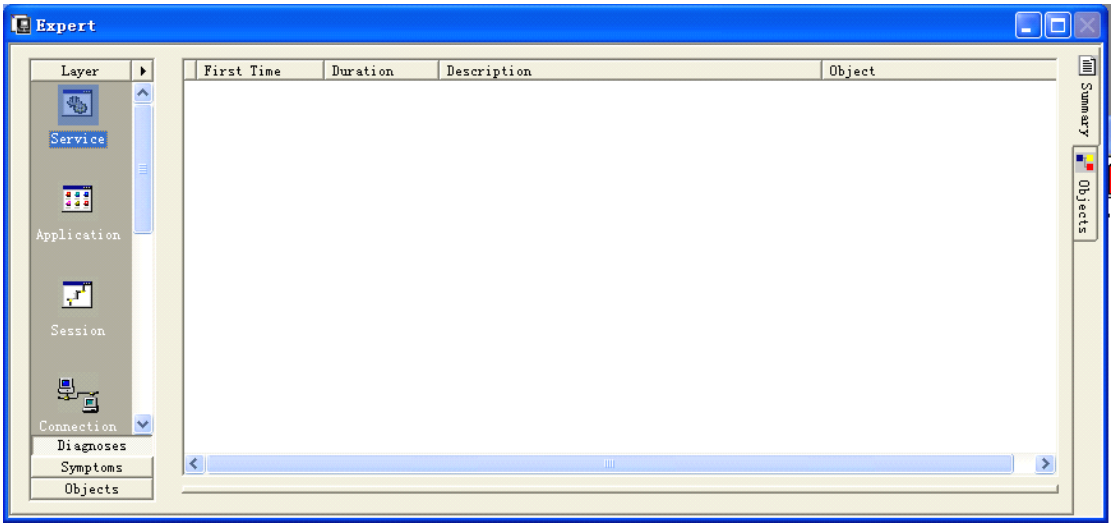
5） 查看综合设置信息，并确定设置。



2. 打开捕获数据包

1）点击数据包捕获开始按钮。

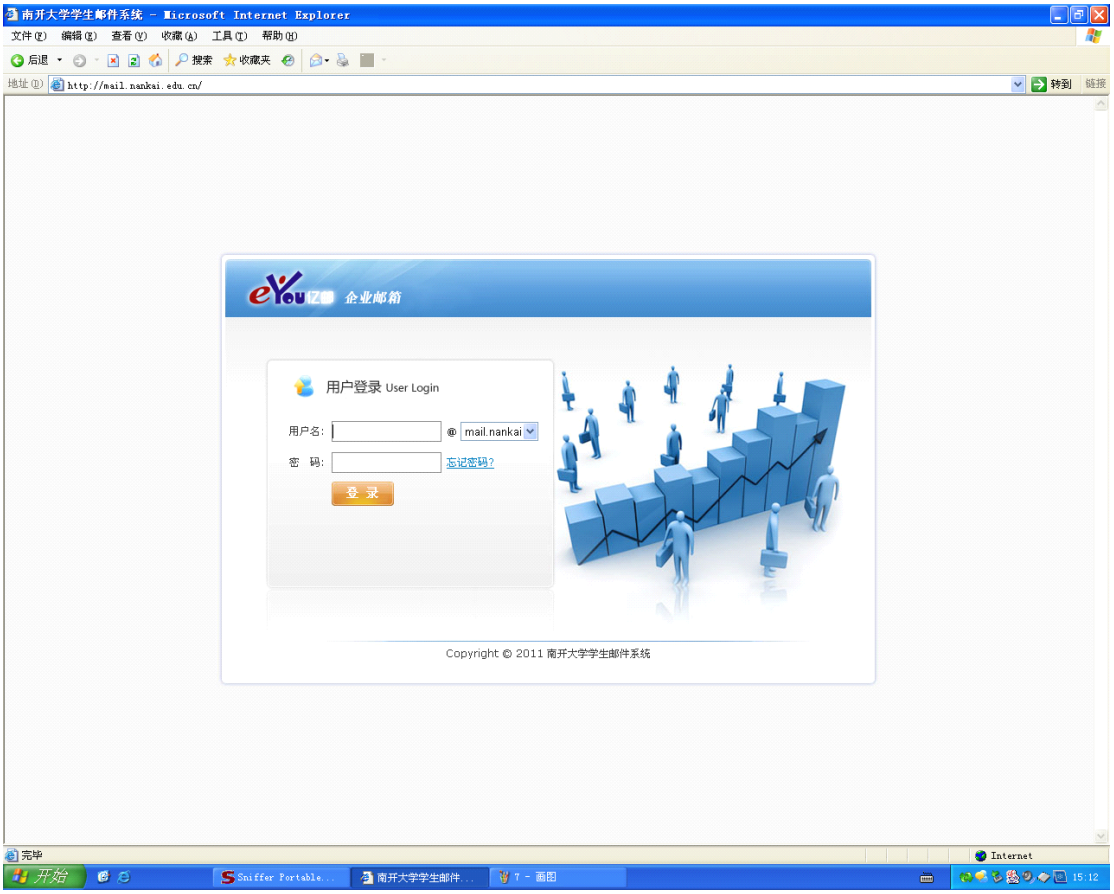
2）弹出新的捕获数据包窗口。



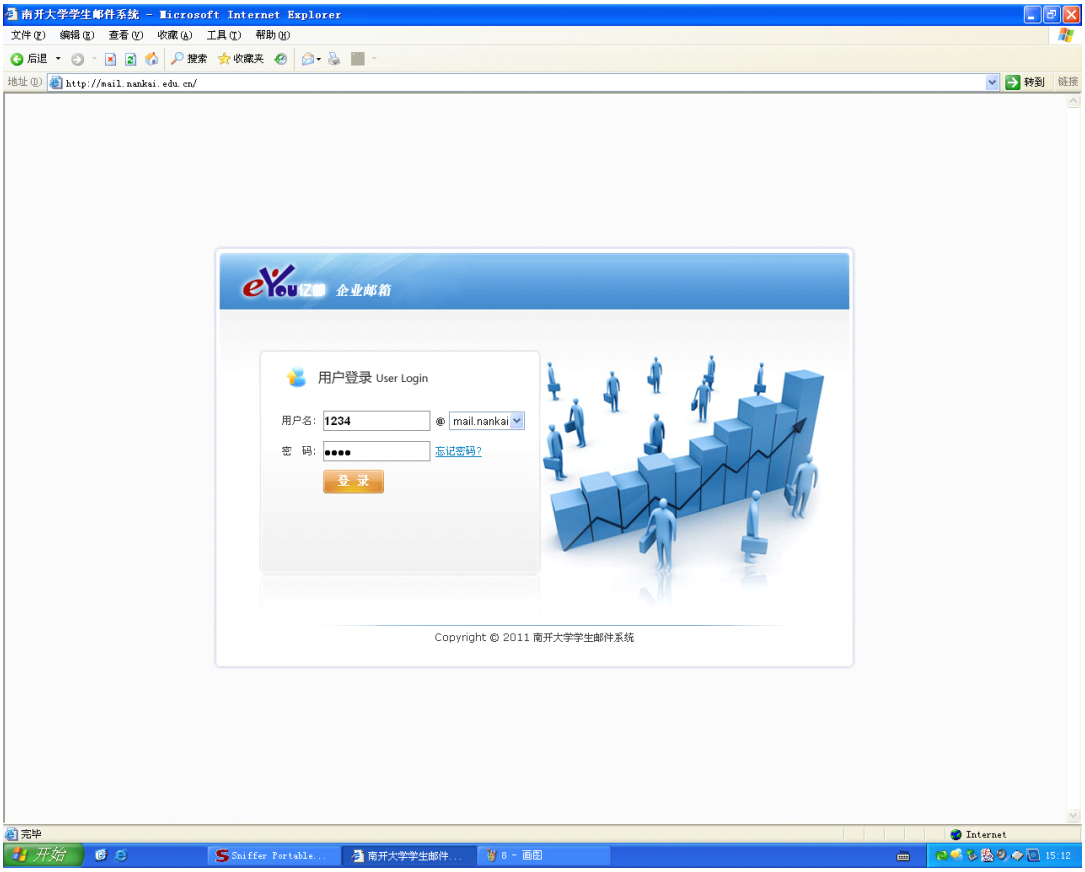
3. 打开一个网页，输入用户名和密码

1） 打开邮箱登陆界面。

打开南开邮箱登陆界面。

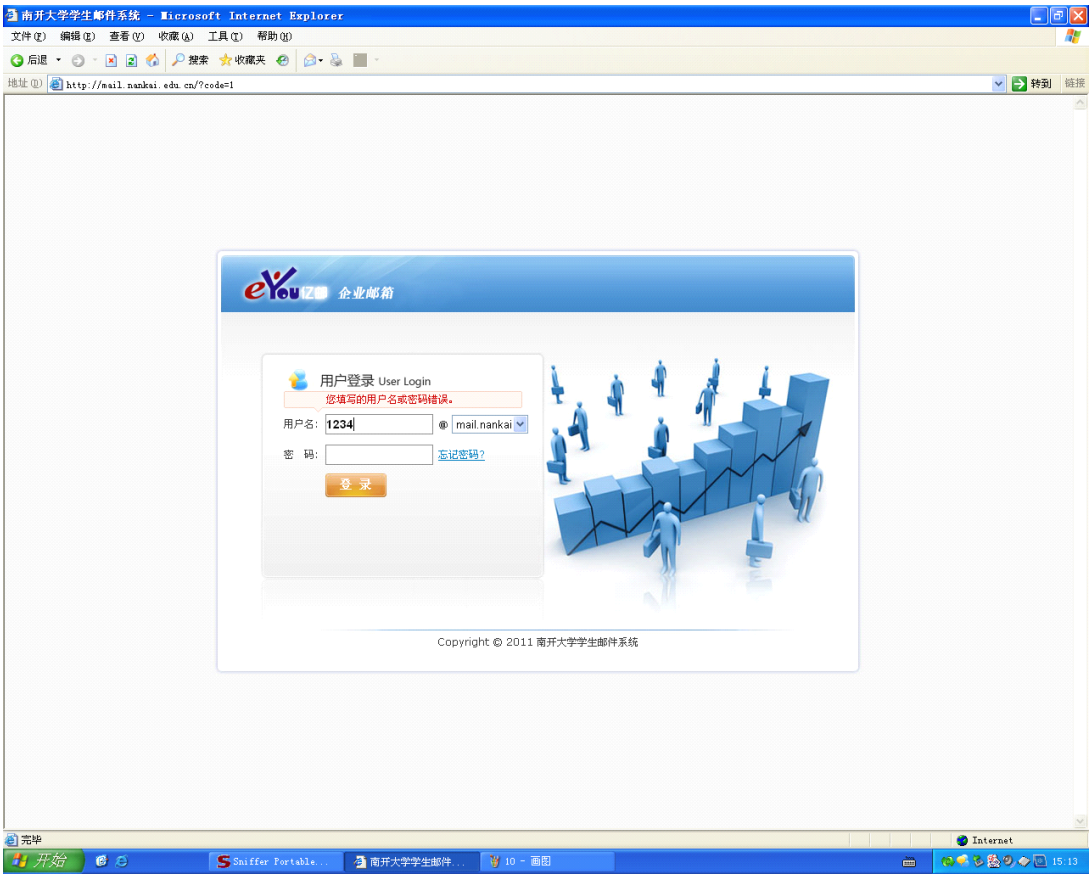


2） 输入用户名和密码。



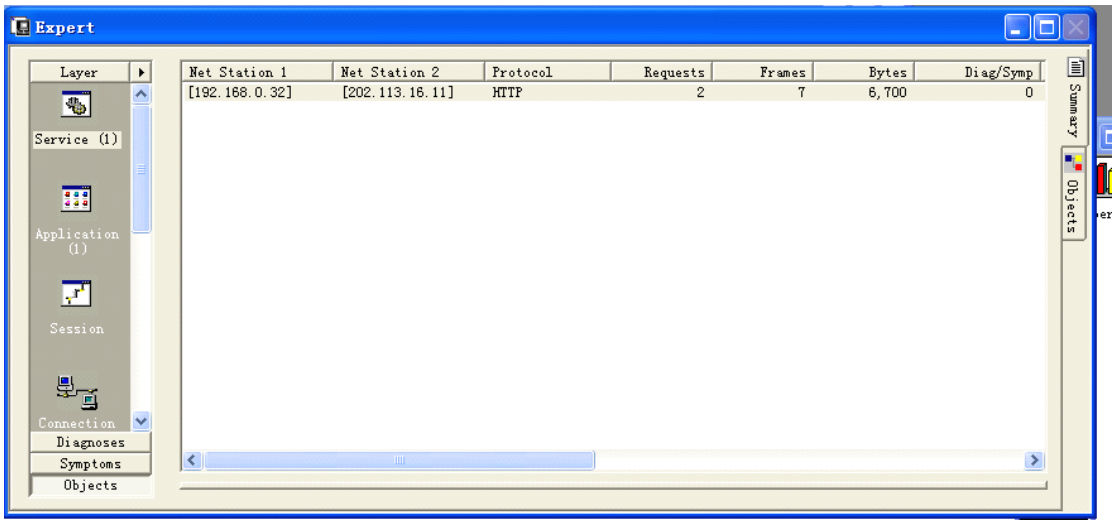
3） 点击登录。

点击登录后显示用户名或密码错误。



4. 分析捕获的数据包获得用户名和密码

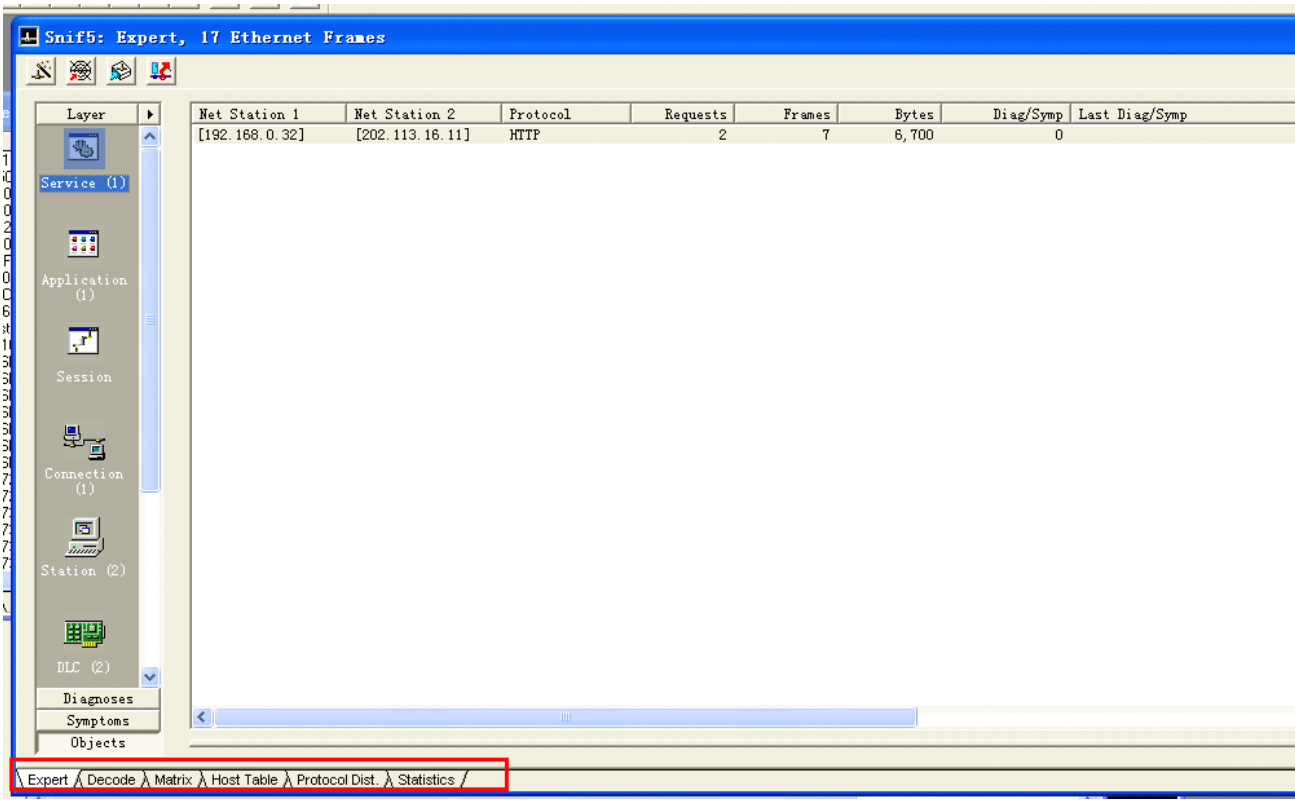
1） 查看数据包捕获窗口，显示捕获到了数据包。



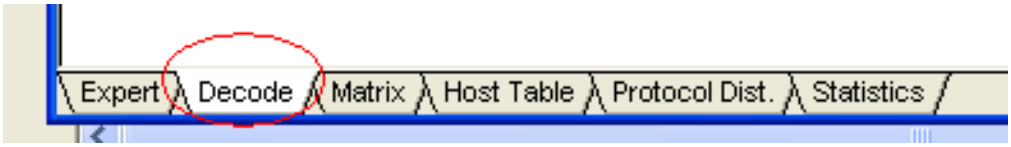
2） 点击终止按钮，终止数据包捕获。

3） 点击查看按钮，允许查看数据包相应信息。

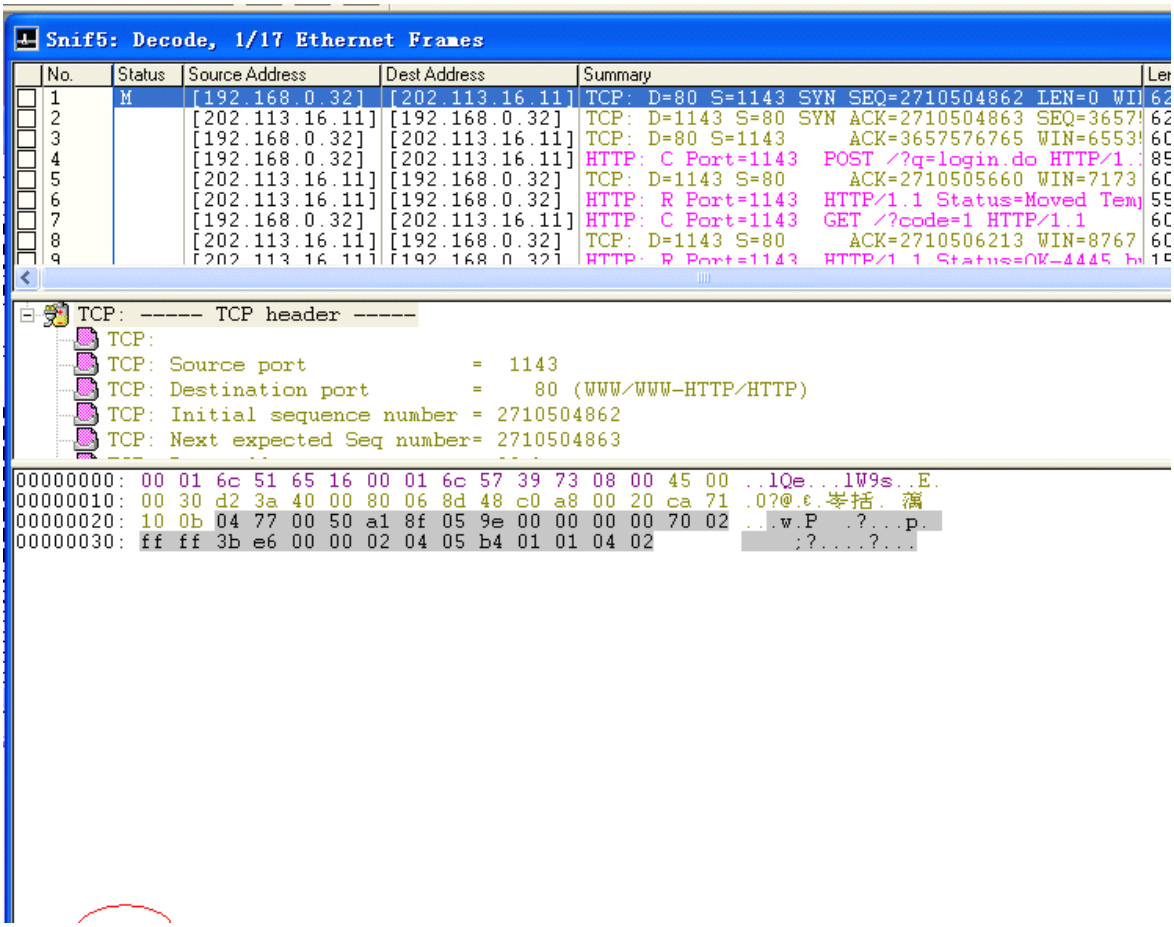
数据包窗口下出现相应的查看按钮。



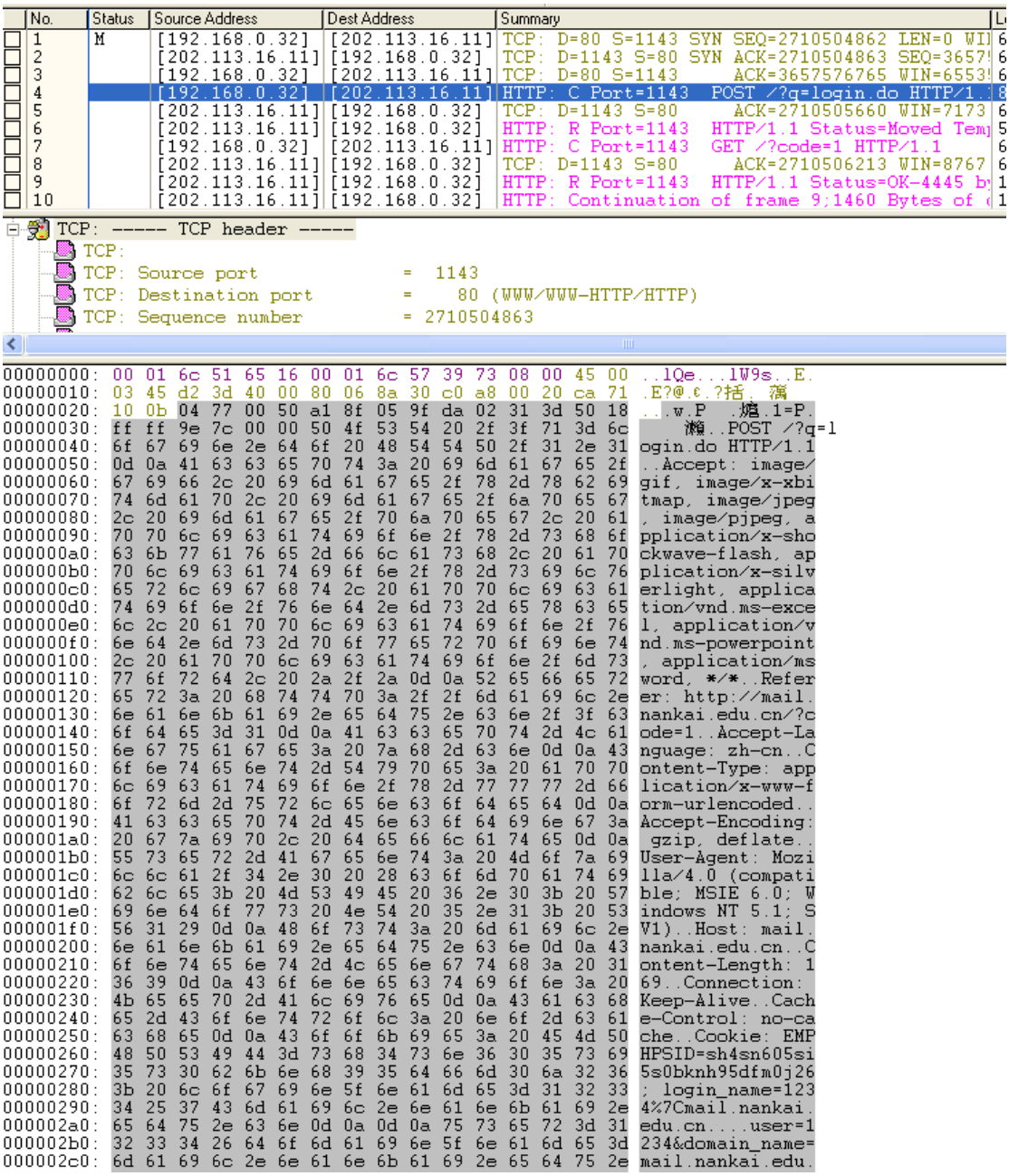
4） 点击“decode”栏，查看相应数据包的相应代码。



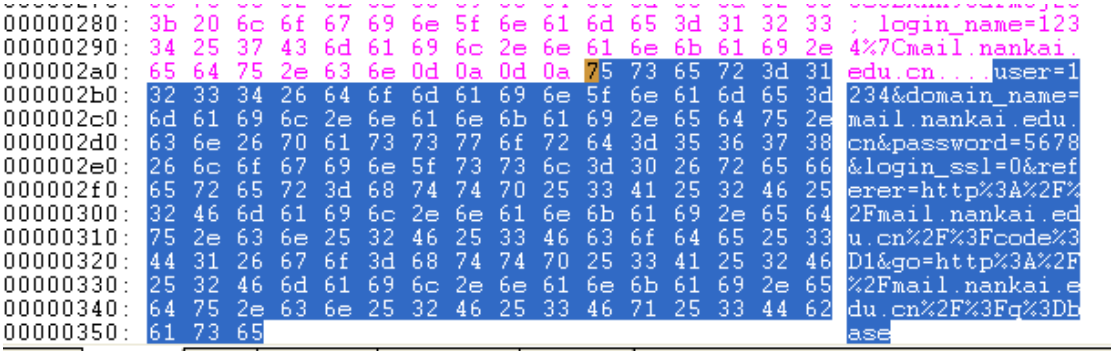
显示数据包相应代码：



5） 找到含有邮件用户名和密码信息的数据包，显示相应数据包内容。



6） 找到数据包中包含邮件用户名和密码的数据段。



分析数据可发现：

输入的用户名为：1234@mail.nankai.edu.cn

输入的密码为 5678