实验 1：使用网络协议分析仪 Wireshark

1. 实验目的

1)能够正确安装配置网络协议分析仪软件 Wireshark。

2)熟悉使用 Wireshark 分析网络协议的基本方法，加深对协议格式、协议层次和协议交互过程的理解。

2. 实验环境

1)运行 Windows 2008 Server/Windows XP/Windows 7 操作系统的 PC 一台。

2)每台 PC 具有以太网卡一块，通过双绞线与局域网相连。

3)Wireshark 程序(可以从 http://www.wireshark.org/下载)和 WinPcap 程序(可以从 http://www.winpcap.org/下载。如果 Wireshark 版本为 1.2.10 或更高，则已包含了 WinPcap 版本 4.1.2)。

3. 实验步骤

1) 安装网络协议分析仪

安装 Wireshark 版本 1.2.10。双击 Wireshark 安装程序图标，进入安装过程。根据提示进行选择确认，可以顺利安装系统。当提示“Install WinPcap 4.1.2”时，选择安装；此后进入安装 WinPcap 版本 4.1.2，并选择让 WinPcap 在系统启动时运行。此后，Wireshark 将能安装好并运行。

2) 使用 Wireshark 分析协议

(1) 启动系统。点击 “Wireshark”图标，将会出现如图 1 所示的系统界面。

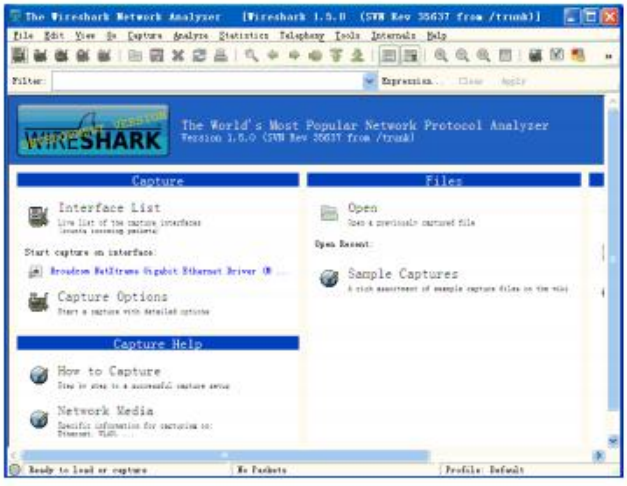

图 1　Wireshark 系统界面

其中“俘获(Capture)”和“分析(Analyze)”是 Wireshark 中最重要的功能。

(2) 分组俘获。点击“Capture/Interface”菜单，出现如图 2 所示界面。

图 2 俘获/接口界面

如果该机具有多个接口卡，则需要指定希望在哪块接口卡俘获分组。点击“Options”，则出现图 3 所示的界面

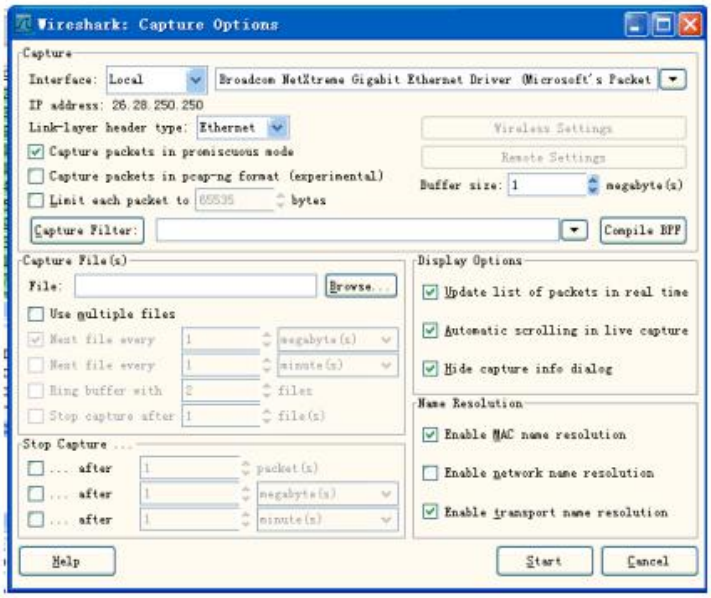

图 3 俘获/接口/选项界面

在该界面上方的下拉框中将列出本机发现的所有接口；选择一个所需要的接口；也能够在此改变俘获或显示分组的选项。

此后，在图 2 或者图 3 界面中，点击“Start(开始)”，Wireshark 开始在指定接口上俘获分组，并显示类似于图 4 的界面。

当需要时，可以点击“Capture/Stop” 停止俘获分组，随后可以点击“File/Save”将俘获的分组信息存入踪迹(trace)文件中。当需要再次俘获分组时，可以点击“Captuer/Start”重新开始俘获分组。

(3) 协议分析。系统能够对 Wireshark 俘获的或打开的踪迹文件中的分组信息(用 File/Open 功能)进行分析。如图 4 所示，在上部“俘获分组的列表”窗口中，有编号(No)、时间(Time)、源地址(Source)、目的地址(Destination)、协议(Protocol)、长度(Length)和信息(Info)等列(栏目)，各列下方依次排列着俘获的分组。中部“所选分组首部的细节信息”窗口给出选中帧的首部详细内容。下部“分组内容”窗口中是对应所选分组以十六进制数和 ASCII 形式的内容。

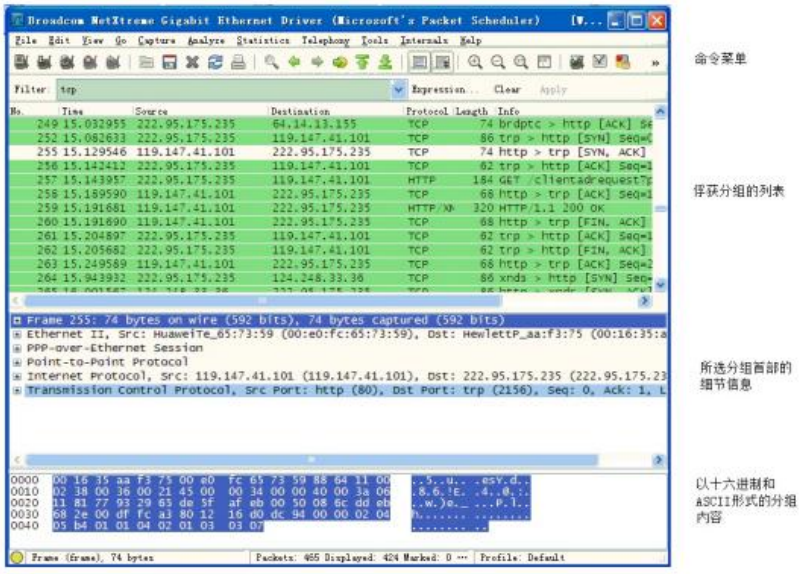

图 4 Wireshark 的俘获分组界面

若选择其中某个分组如第 255 号帧进行分析。从图 4 中的信息可见，该帧传输时间为俘获后的 15.129546 秒；从源 IP 地址 119.147.41.101 传输到目的 IP 地址 222.95.175.235；帧的源 MAC 地址和目的 MAC 地址分别是 00.e0.fc.65.73.59 和 00.16.35.aa.f3.75 (从中部分组首部信息窗口中可以看到)；分组长度 74 字节；是 TCP 携带的 HTTP 报文。

从分组首部信息窗口，可以看到各个层次协议及其对应的内容。例如，对应图 5 的例子，包括了 Ethernet II 帧及其对应数据链路层信息(参见图 5)，可以对应 Ethernet II 帧协议来解释对应下方协议字段的内容。接下来，可以发现 Ethernet II 协议上面还有 PPP-over-Ethernet 协议、Point-to-Point 协议、IP 和 TCP 等，同样可以对照网络教材中对应各种协议标准，分析解释相应字段的含义。

注意：当我们分析自行俘获分组时，即使无法得到与如图 4 所示完全一样的界面，但也能够得到非常相似的分析结果。在后面的实验中，读者应当有意地改变相应的报文内容或 IP 地址等，培养这种举一反三能力的能力。

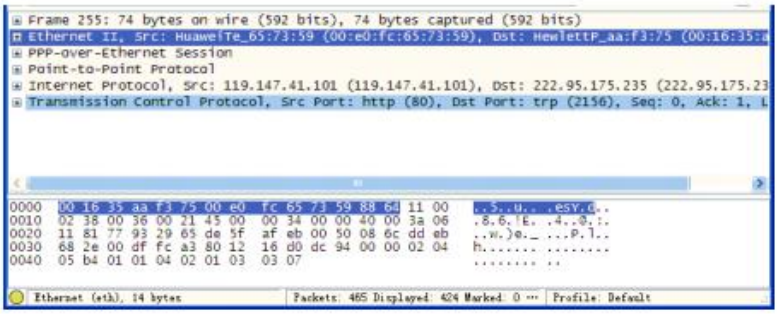

图 5　Ethernet 帧及其对应数据链路层信息

当俘获的分组太多、类型太杂时，可以使用 Analyze 中的“使能协议(Enabled Protocols)”和过滤器(Filters)等功能，对所分析的分组进行筛选，排除掉无关的分组，提高分析效率。

3) 其他

(1)通过使用 Wireshark 协议分析仪，应当理解 Wireshark 的工作原理，对于与之相关的网络接口(指出网络接口卡类型)、网络地址(指出 IP 地址、MAC 地址)、网络协议(指出发现的集中协议)等重要概念有基本的理解。

(2)在图 7 上部“俘获分组的列表”窗口中，有编号(No)、时间(Time)等字段信息。对于一段时间范围内往返于相同源和目的地之间的相同类型的分组，这些编号、时间等能否构成分析网络协议运行、交互轨迹的信息？

4. 相关概念

1) Wireshark 简介。Wireshark 是一种具有图形用户界面的网络协议分析仪，可以用于从实际运行的网络俘获分组或从以前保存的踪迹文件中交互地浏览、分析处理分组数据。Wireshark 是一个免费软件，因商标原因从 Ethereal 改名而得，是能够在 Windows、Linux/Unix 和 Mac 计算机上运行的免费分组嗅探器(packet sniffer)。Wireshark 能够读取 libpcap 俘获文件，也能够读取包括用 Tcpdump 俘获的文件，以及 snoop，atmsnoop, LanAlyzer, Sniffer (压缩和非压缩的), Microsoft Network Monitor, AIX 的 iptrace, NetXray, Sniffer Pro, Etherpeek, RADCOM 的 WAN/LAN analyzer, Lucent/Ascend router debug output, HP-UX 的 nettl, Cisco 的安全入侵检测系统以 IPLog 格式输出的 pppd 日志文件。它能够自行分析文件类型，即使用 gzip 进行压缩也是如此。

Wireshark 对于在实践中分析和调试网络协议，特别是对初学者理解网络协议都是十分有用的工具。当在家中或在实验室中使用桌面计算机运行网络应用程序时，可以用 Wireshark 观察本机基于网络协议与在因特网别处执行的协议实体交互和交换报文情况。因此，Wireshark 能够使用户计算机成为真实动态实验的有机组成部分，通过动手实验来观察网络的奥秘，进而深入理解和学习它们。能够得到极大地深化读者的网络概念和提升实验技能：观察网络协议的动作和动手操作它们，即观察两个协议实体之间交换的报文序列，钻研协议运行的细节，使协议执行某些动作，观察这些动作及其后果。

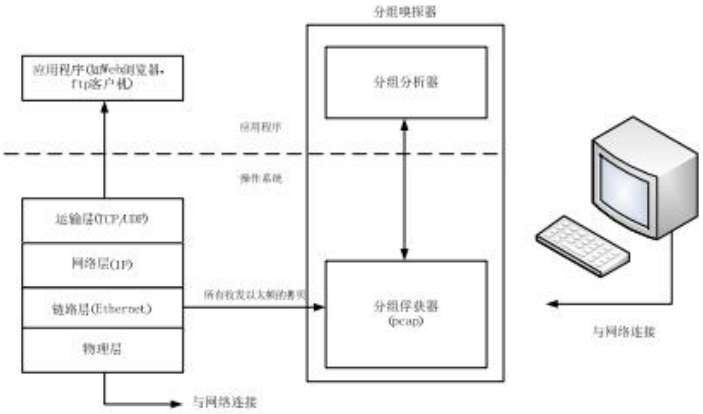

图 6 分组嗅探器结构

2) Wireshark 的结构。作为分组嗅探器，Wireshark 俘获从计算机发送接收的报文，通常也能够存储和显示这些俘获的报文中各个协议字段的内容。分组嗅探器自身是被动的，观测运行在计算机中的应用程序和协议所发送及接收的报文，但自身并不发送分组。类似地，接收到的分组决不会显式地以分组嗅探器为目的地址，它们仅是在机器上运行的应用程序和协议收发分组的副本。图 6 显示了分组嗅探器的结构。图中的计算机通常运行着应用程序及其协议，显示在图中方框内的分组嗅探器是计算机中附加的一个普通软件，它由两部分组成。分组俘获器接收计算机收发的每个链路层帧的副本。大家知道较高层协议如 HTTP、FTP、TCP、UDP、DNS 或 IP 之间交换的报文全都逐个封装在链路层帧中，并在物理介质如以太电缆上传输。如果图中的物理介质是以太双绞线等，则所有高层协议则将封装在以太帧中。俘获所有链路层帧从而使读者能够观察到在计算机中执行的所有应用程序和协议收发的报文。

嗅探器的第二部分是分组分析器，它显示协议报文的所有字段的内容。为了实现该功能，分组分析器必须要能理解协议交换的所有报文结构。例如，如果想要显示图中由 FTP 交换报文的各个字段，则该分组分析器需要理解以太帧格式，这样才能识别以太帧中的 IP 数据报，进而通过分析 IP 数据报才能从中提取 TCP 报文段。只有理解了 TCP 段结构，才能提取包含在 TCP 段中的 FTP 报文。最终，只有理解了 FTP 协议，才能正确显示“USER”、“PASS”或“LIST”等命令。

5. 注意事项

1) 安装 Wireshark 网络协议分析仪前应安装 WinPcap 网络监测驱动程序。

2) 俘获分组前应注意选择正确的网络接口。

3) 协议分组的俘获结果可以保存在指定的文件中，并可以在以后再行使用。

4) Wireshark 网络协议分析仪还具有其他丰富的功能，读者可以参阅随软件的“Wireshark 帮助”文档自行学习。