实验 2 用 wireshark 分析数据包的结构

中国科学技术大学 曾凡平

2.1 实验目的

1. 掌握网络协议分析器与仿真编辑器的使用方法；
2. 用 wireshark 分析以数据链路层、网络层和传输层的网络协议单元的结构、理解网络协议的工作过程。

2.2 实验内容

1. 安装和配置 wireshark 协议分析软件；
2. 用 wireshark 分析以太网的数据包；
3. 用 wireshark 分析网络层的数据包；
4. 用 wireshark 分析 TCP 协议的工作过程。

2.3 实验步骤

启动 Window2003 虚拟机，在虚拟机上进行实验。

2.3.1 安装和配置 wireshark 协议分析软件

从 http://www.wireshark.org/下载稳定版本的 wireshark 软件(或直接使用虚拟机中预装的 wireshark 软件)。双击安装文件(Wireshark-win32-1.10.6.exe)，按照提示进行安装。安装过程如图 1 至图 4 所示。

图 1 欢迎界面

点击 Next 进入安装的下一步。

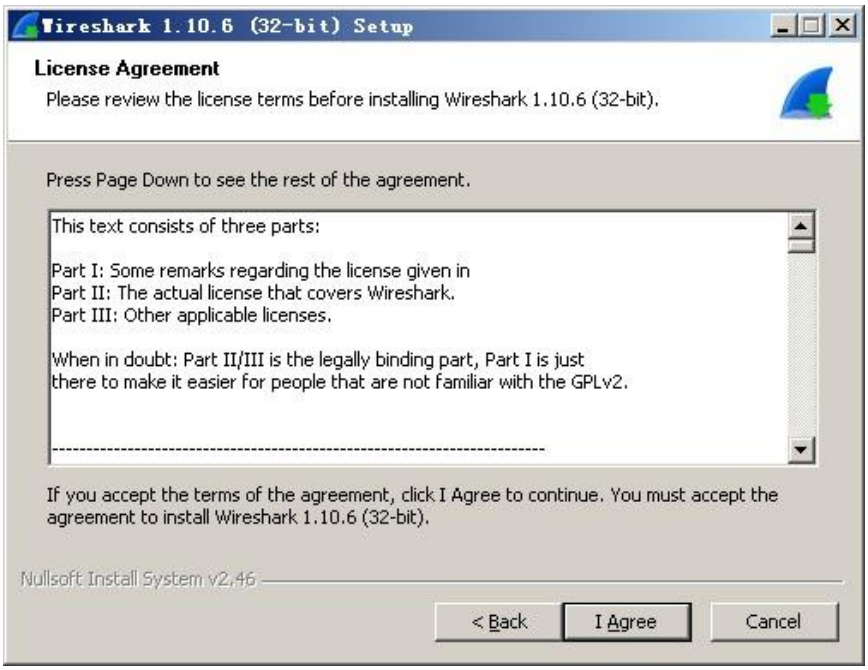

图 2 License Agreement 界面

点击 I Agree，选择安装所有的组件。

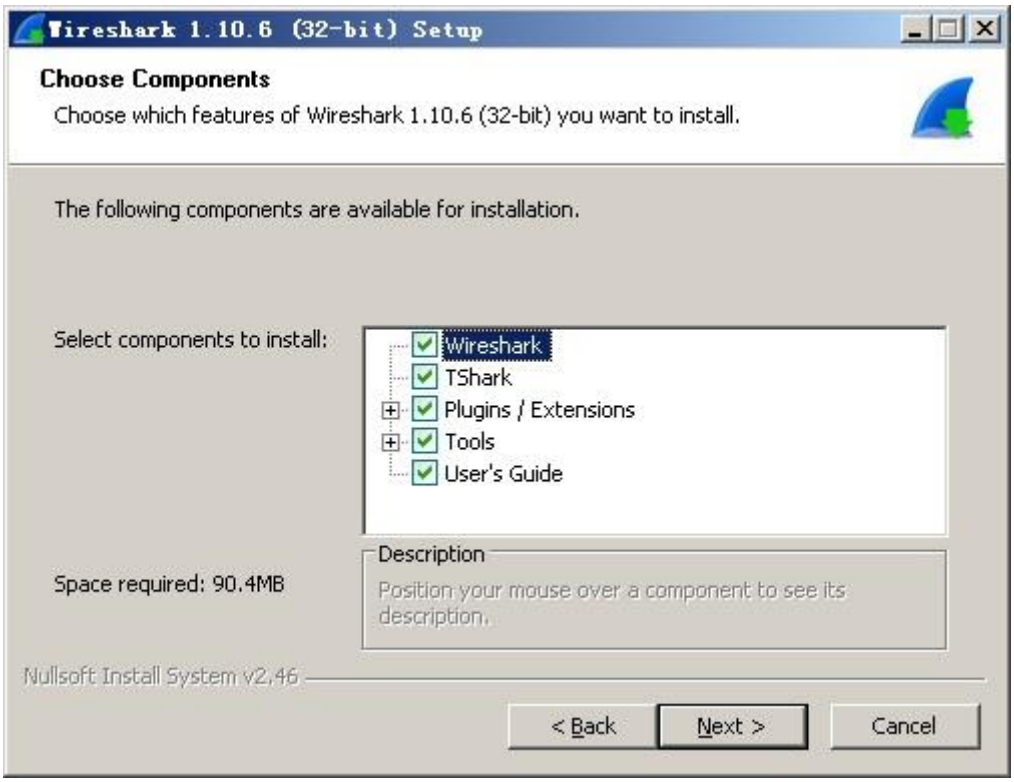

图 3 组件选择界面

点击 Next 后将进入快捷方式选项界面。

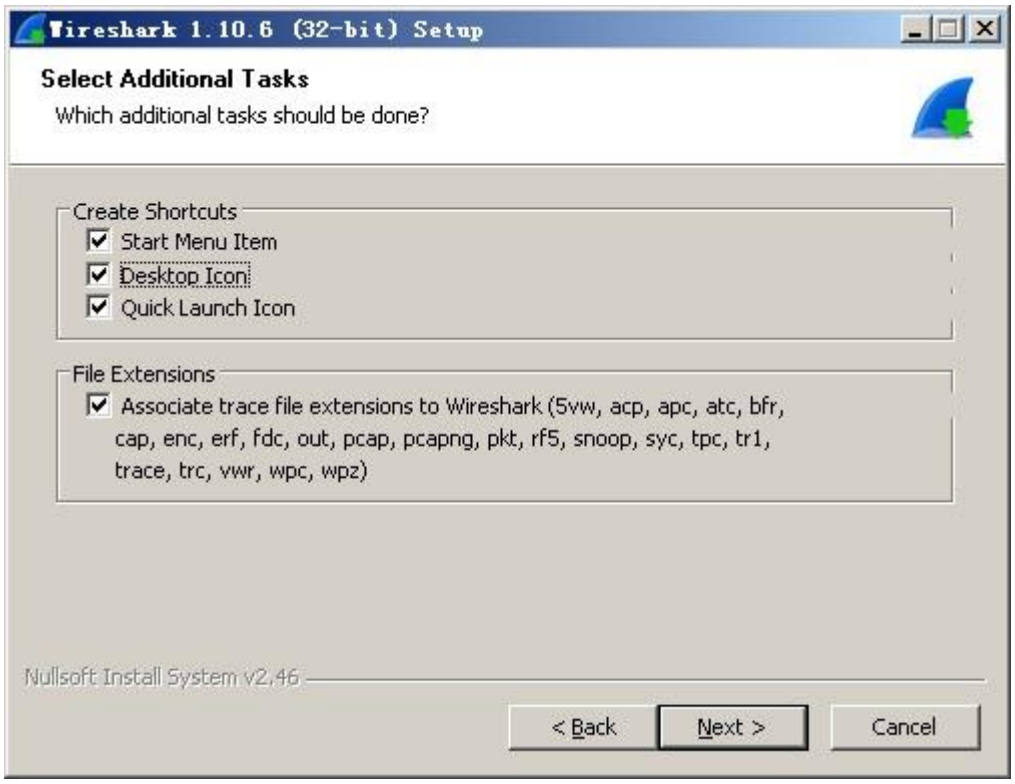

图 4

点击 Next 后将选择安装目录，再次点击 Next 后将看到如下界面：

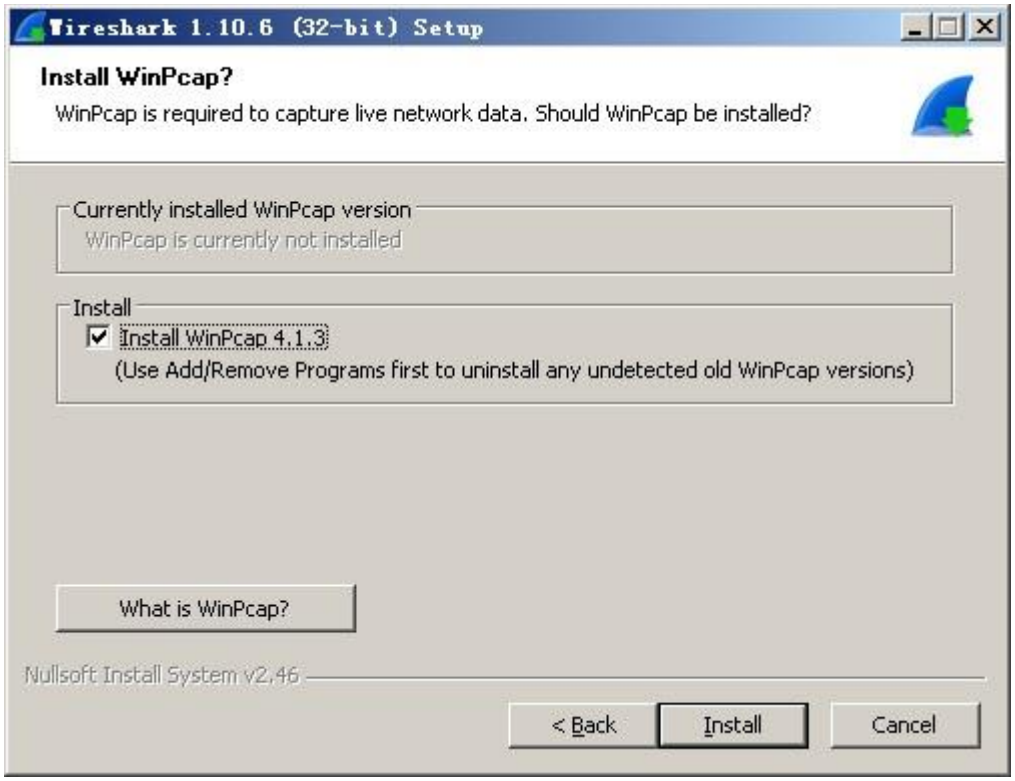

图 5

由于 wireshark 利用了 WinPcap 网络编程库，必须选择安装该库。点击 Install 后将安装所选择的软件。

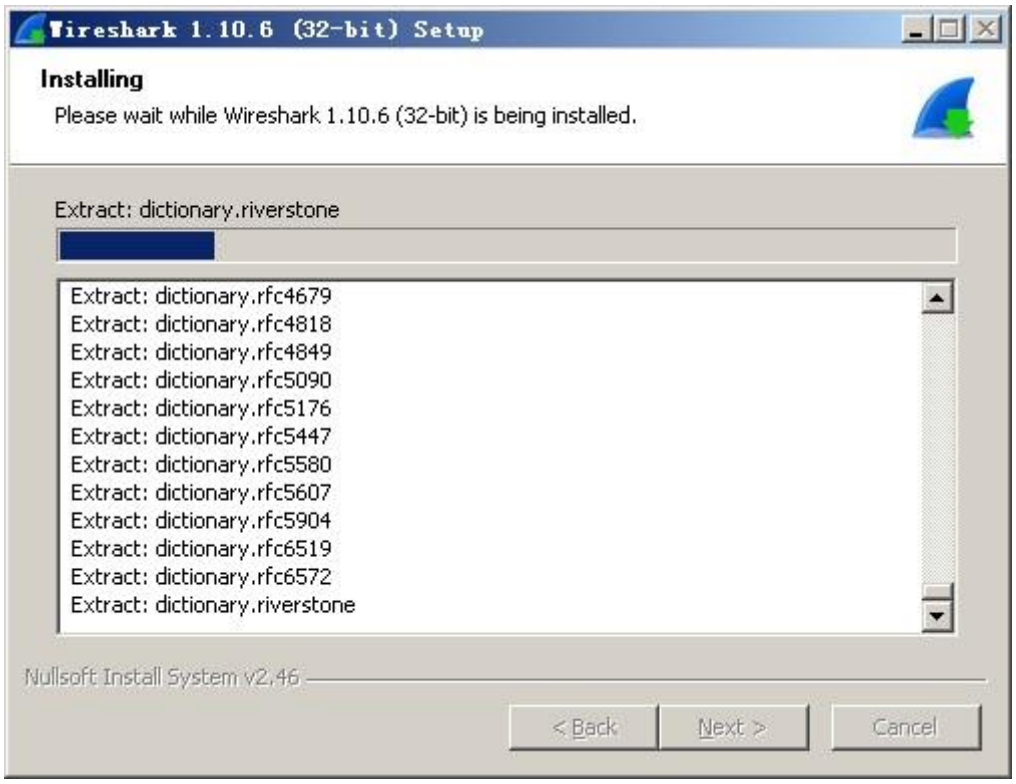

图 6

安装完毕后启动 wireshark，初始界面如图所示。

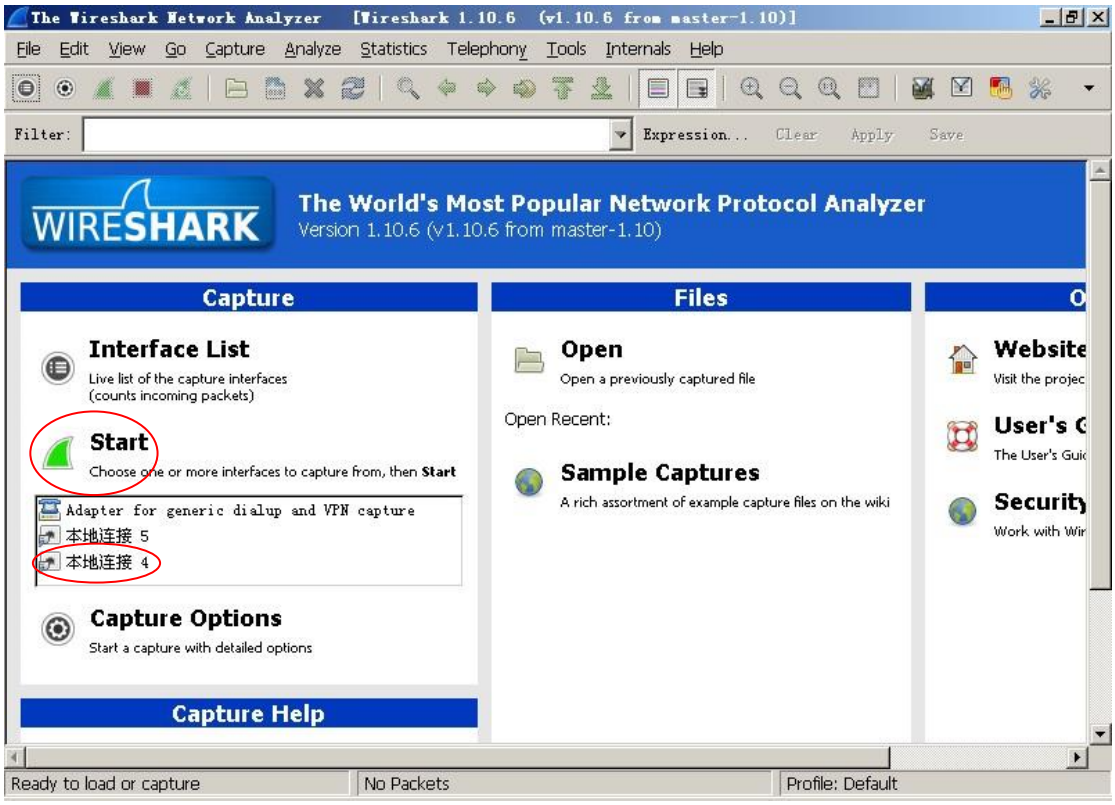

图 7 wireshark 初始界面

2.3.2 用 wireshark 分析以太网的数据包

选择一个接口(如“本地连接 4”，图 7 中的红色椭圆圈住的)，然后点击 Start（图 7 中的红色椭圆圈住的)，则 Wireshark 获取相应的接口上的所有数据包，并按协议的层次结构对数据包进行解析。

启动另一个虚拟机 ClientA，在命令提示符下输入：ping 192.168.11.203，则 SereverA 中的 wireshark 将捕获数据包，如下图所示：

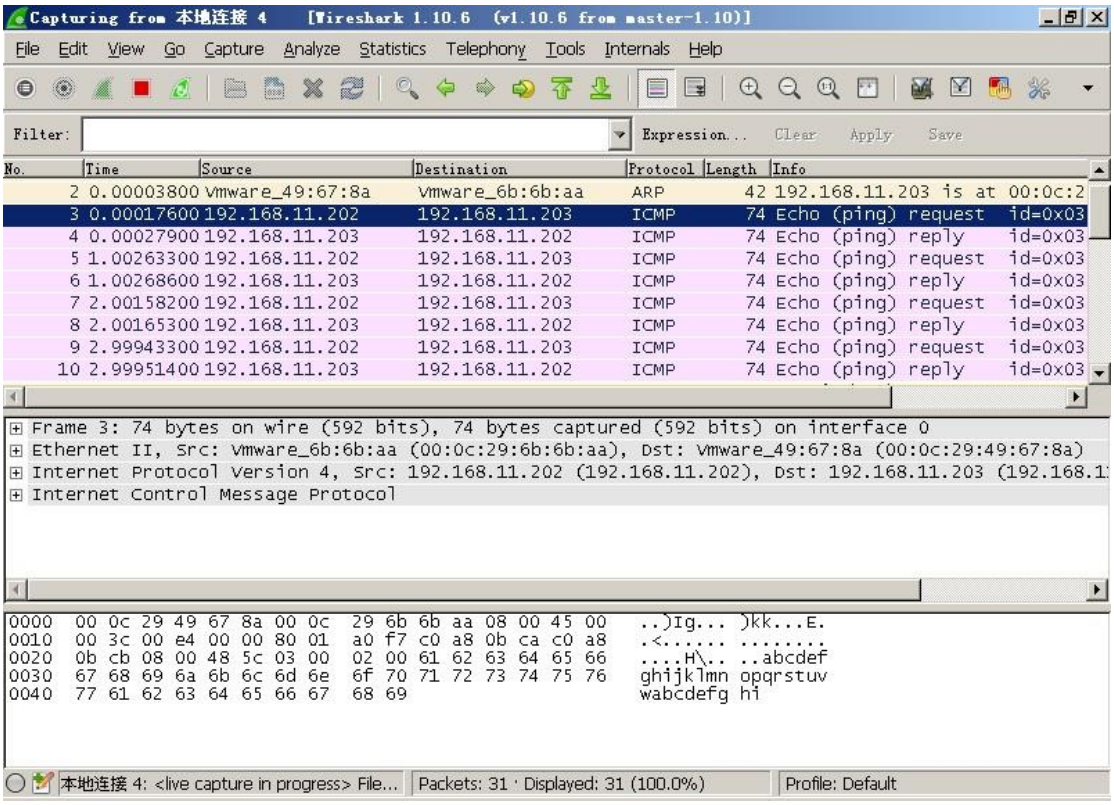

图 8 捕获的数据包

图 8 显示了三部分内容：

第 1 部分按序显示捕获的数据包及其简况，如源 IP 地址、目标 IP 地址、协议类型等。图 8 显示了第 2 至第 10 个数据包。如果用鼠标点击某行，则在第 2 部分、第 3 部分显示该数据包的详细内容。

第 2 部分按层次解析协议。图 8 的示例表示第 3 个数据包是 ICMP request 数据包，点击“+”将展开更详细的信息。

第 3 部分显示数据包的字节内容。

点击第 2 部分 Ethernet 旁边的“+”，则可以分析以太网数据包的结构，如图 9 所示：

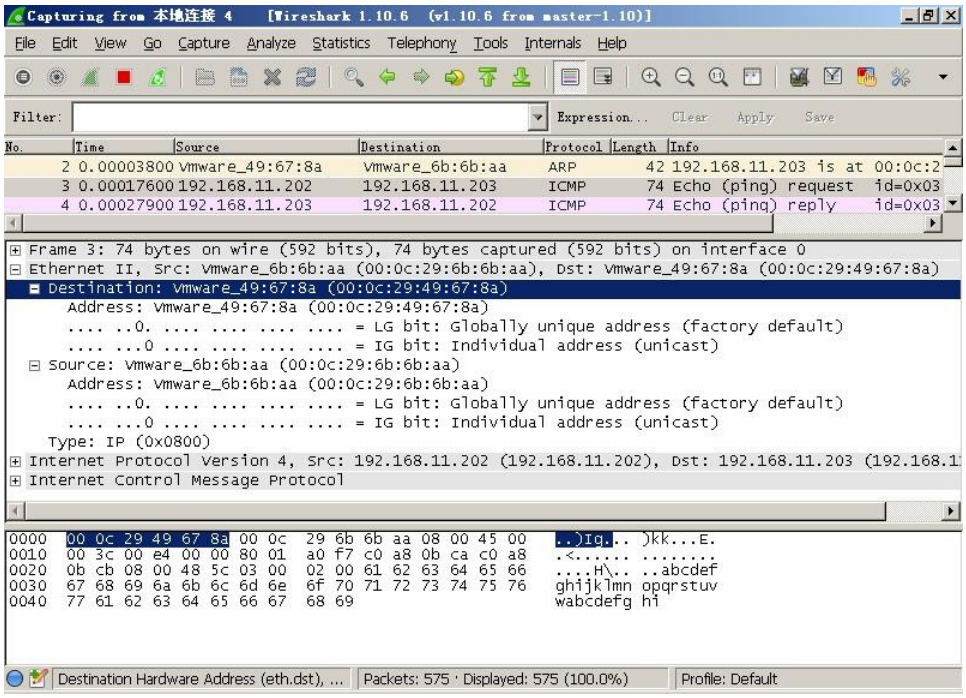

图 9 以太数据包的结构

从图 9 可知，源 MAC 地址为 00 0c 29 49 67 8a，目标 MAC 地址为 00 0c 29 6b 6b aa，类型为 0x0800（表示数据部分为 IP 协议）。

2.3.3 用 wireshark 分析网络层(IP)的数据包

点击第 2 部分 Internet Protocol Version4 旁边的“+”，则可以分析 IP 数据包的结构，如图 10 所示：

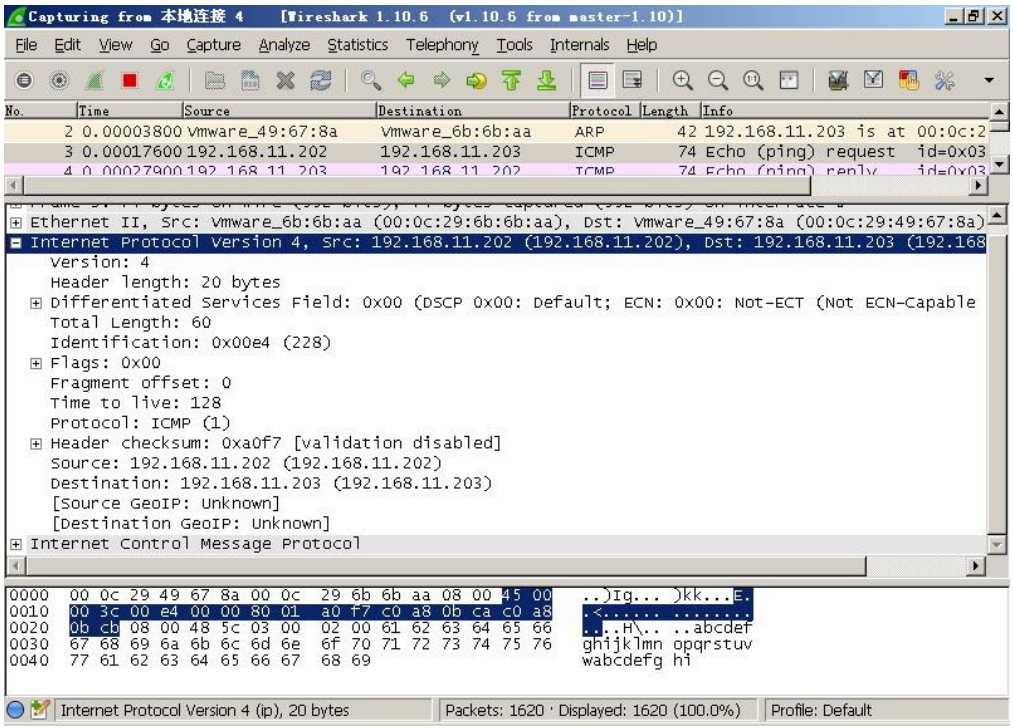

图 10

IP 数据包的结构可见，该 IP 数据包的首部 20 字节，首部最后的 8 字节为 4 字节源 IP 地址和 4 字节的目标 IP 地址。本例中，原 IP 地址为 0xc0a80bca(192.168.11.202)，目标 IP 地址为 0xc0a80bcb(192.168.11.202)

2.3.4 用 wireshark 分析 TCP 协议的工作过程

通过计算机管理启用 telnet 服务，如下图所示：

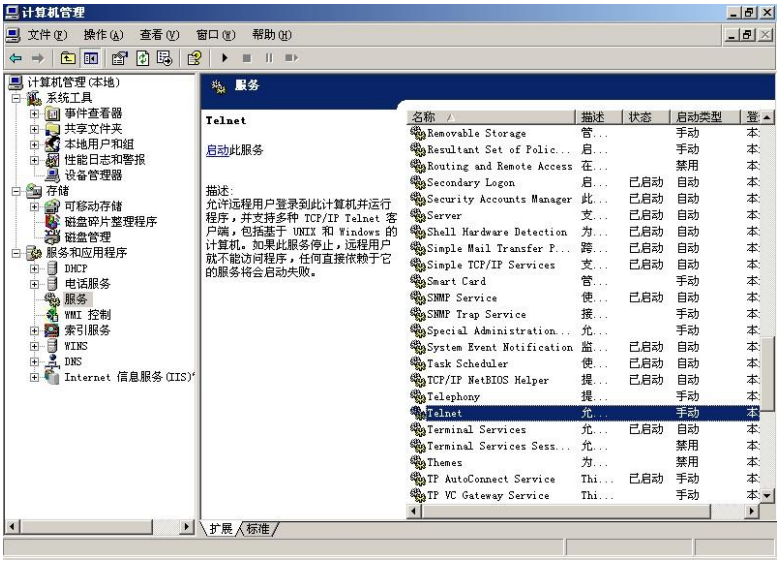

图 11

双击后启用 telnet 服务，在 ClientA 中输入：telnet 192.168.11.203，则 wireshark 可以捕获到 TCP 连接的三次握手的建立过程，如下图所示：

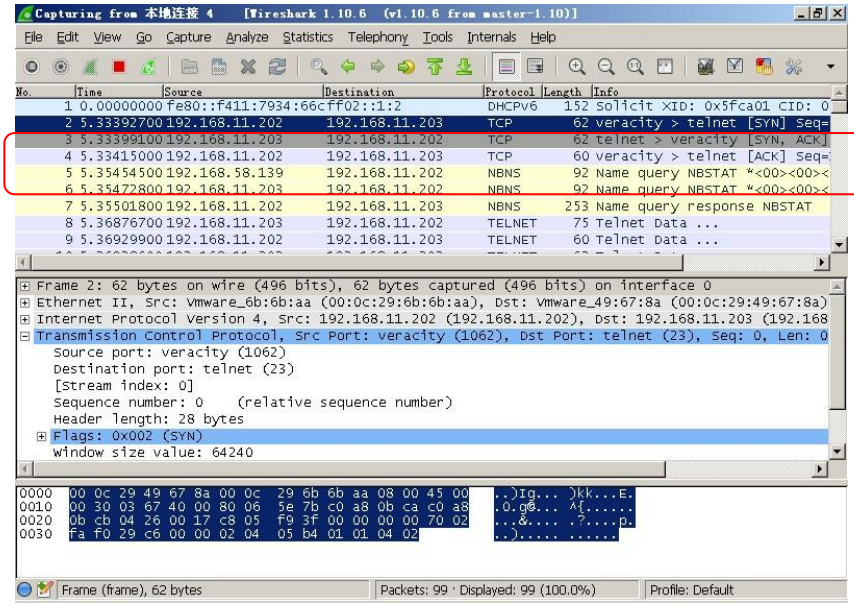

图 12

2.4 上机实践

用浏览器访问课程主页，分析浏览器和 Web 服务器的信息交换过程。 完成实验报告上交。