

Wireshark 实验指导书

实验说明

Wireshark 是目前最主流的网络协议分析软件，被广泛的用于网络部署、维护、管理和安全等场合。通过对 wireshark 的了解和掌握，可以帮助我们深入了解网络中正在流动的各种数据报文，以及各种数据报文之间的关系。

本实验分为两个小实验。

如果已经熟悉了 wireshark 的安装使用，可以不做第一个实验，直接做第二个实验，并在任务五中使用。

实验一 Wireshark 的安装与使用

一、实验目的

- 1、熟悉并掌握 Wireshark 的基本使用；
- 2、了解网络协议实体间进行交互以及报文交换的情况。

二、实验环境

与因特网连接的计算机，操作系统为 Windows，安装有 Wireshark、IE 等软件。

三、预备知识

要深入理解网络协议，需要观察它们的工作过程并使用它们，即观察两个协议实体之间交换的报文序列，探究协议操作的细节，使协议实体执行某些动作，观察这些动作及其影响。这种观察可以在仿真环境下或在因特网这样的真实网络环境中完成。

观察正在运行的协议实体间交换报文的基本工具被称为分组嗅探器（packet sniffer），又称分组捕获器。顾名思义，分组嗅探器捕获（嗅探）你的计算机发送和接收的报文。

图 1 显示了一个分组嗅探器的结构。

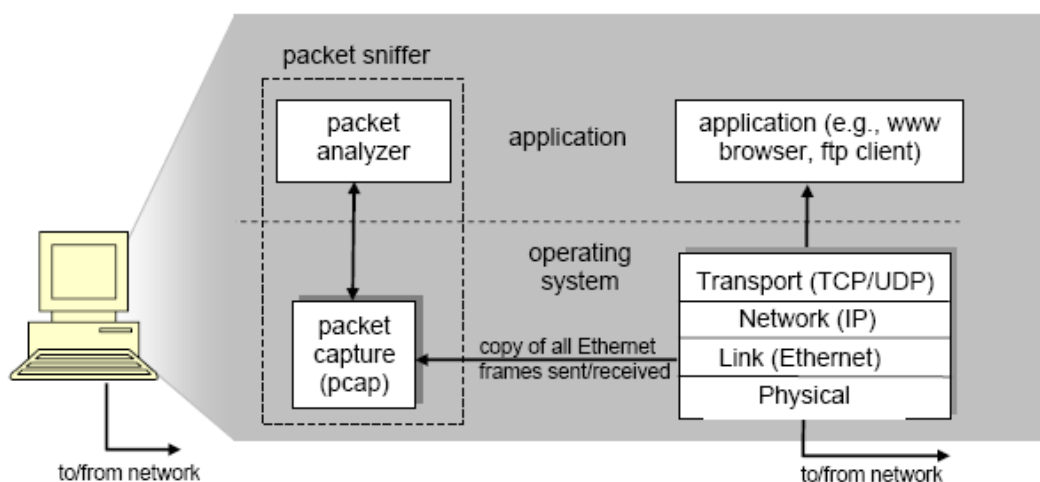


图 1

图 1 右边是计算机上正常运行的协议和应用程序（如：Web 浏览器和 FTP 客户端）。分组嗅探器（虚线框中的部分）主要有两部分组成：第一是分组捕获器，其功能是捕获计算机发送和接收的每一个链路层帧的拷贝；第二个组成部分是分组分析器，其作用是分析并显示协议报文所有字段的内容（它能识别目前使用的各种网络协议）。

Wireshark 是一种可以运行在 Windows, UNIX, Linux 等操作系统上的分组嗅探器, 是一个开源免费软件, 可以从 <http://www.wireshark.org> 下载。

运行 Wireshark 程序时, 其图形用户界面如图 2 所示。最初, 各窗口中并无数据显示。Wireshark 的界面主要有五个组成部分:

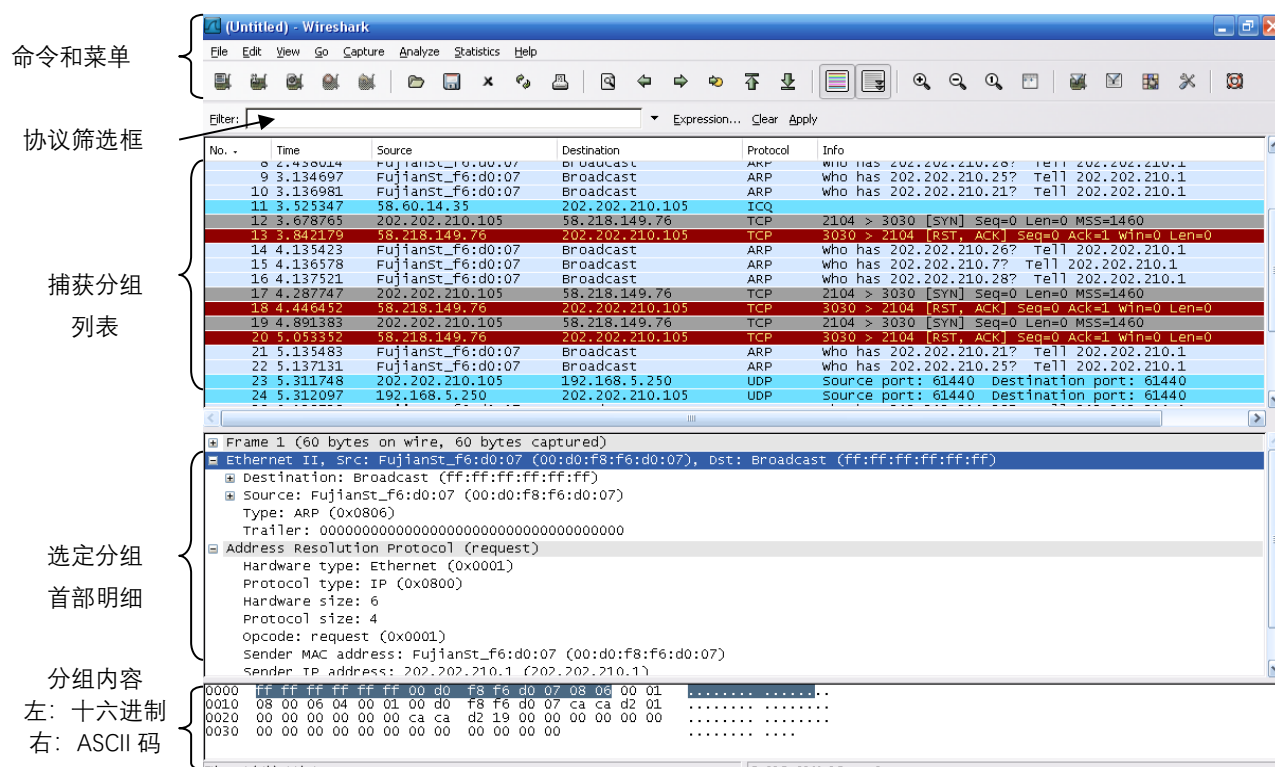


图 2

- **命令菜单 (command menus):** 命令菜单位于窗口的最顶部, 是标准的下拉式菜单。

- **协议筛选框 (display filter specification):** 在该处填写某种协议的名称, Wireshark 据此对分组列表窗口中的分组进行过滤, 只显示你需要的分组。

- **捕获分组列表 (listing of captured packets):** 按行显示已被捕获的分组内容, 其中包括: 分组序号、捕获时间、源地址和目的地址、协议类型、协议信息说明。单击某一列的列名, 可以使分组列表按指定列排序。其中, 协议类型是发送或接收分组的最高层协议的类型。

- **分组首部明细 (details of selected packet header):** 显示捕获分组列表窗口中被选中分组的首部详细信息。包括该分组的各个层次的首部信息, 需要查看哪层信息, 双击对应层次或单击该层最前面的“+”即可。


- **分组内容窗口 (packet content):** 分别以十六进制 (左) 和 ASCII 码 (右)

两种格式显示被捕获帧的完整内容。

四、实验步骤

1. 启动 Web 浏览器（如 IE）；

2. 启动 Wireshark；

3. 开始分组捕获：单击工具栏的按钮，出现如图 3 所示对话框，[options] 按钮可以进行系统参数设置，在绝大部分实验中，使用系统的默认设置即可。当计算机具有多个网卡时，选择其中发送或接收分组的网络接口（本例中，第一块网卡为虚拟网卡，第二块为以太网卡）。单击“Start”开始进行分组捕获；

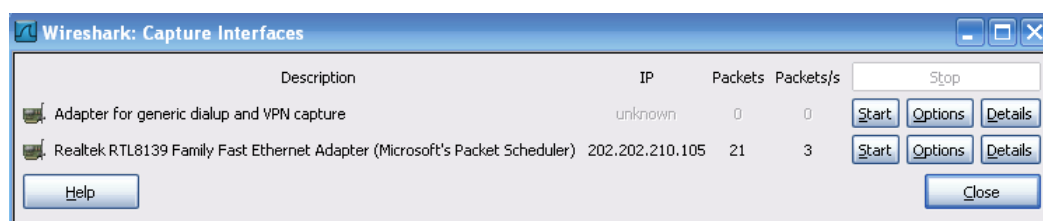


图 3

4. 在运行分组捕获的同时，在浏览器地址栏中输入某个网页的 URL，如：
<http://www.sohu.com>

5. 当完整的页面下载完成后，单击捕获对话框中的“stop”按钮，停止分组捕获。此时，Wireshark 主窗口显示已捕获的你本次通信的所有协议报文；

6. 在协议筛选框中输入“http”，单击“apply”按钮，分组列表窗口将只显示 HTTP 协议报文。

7. 选择分组列表窗口中的第一条 http 报文，它是你的计算机发向服务器（如：www.sohu.com）的 HTTP GET 报文。当你选择该报文后，以太网帧、IP 数据报、TCP 报文段、以及 HTTP 报文首部信息都将显示在分组首部子窗口中，其结果如图 4。

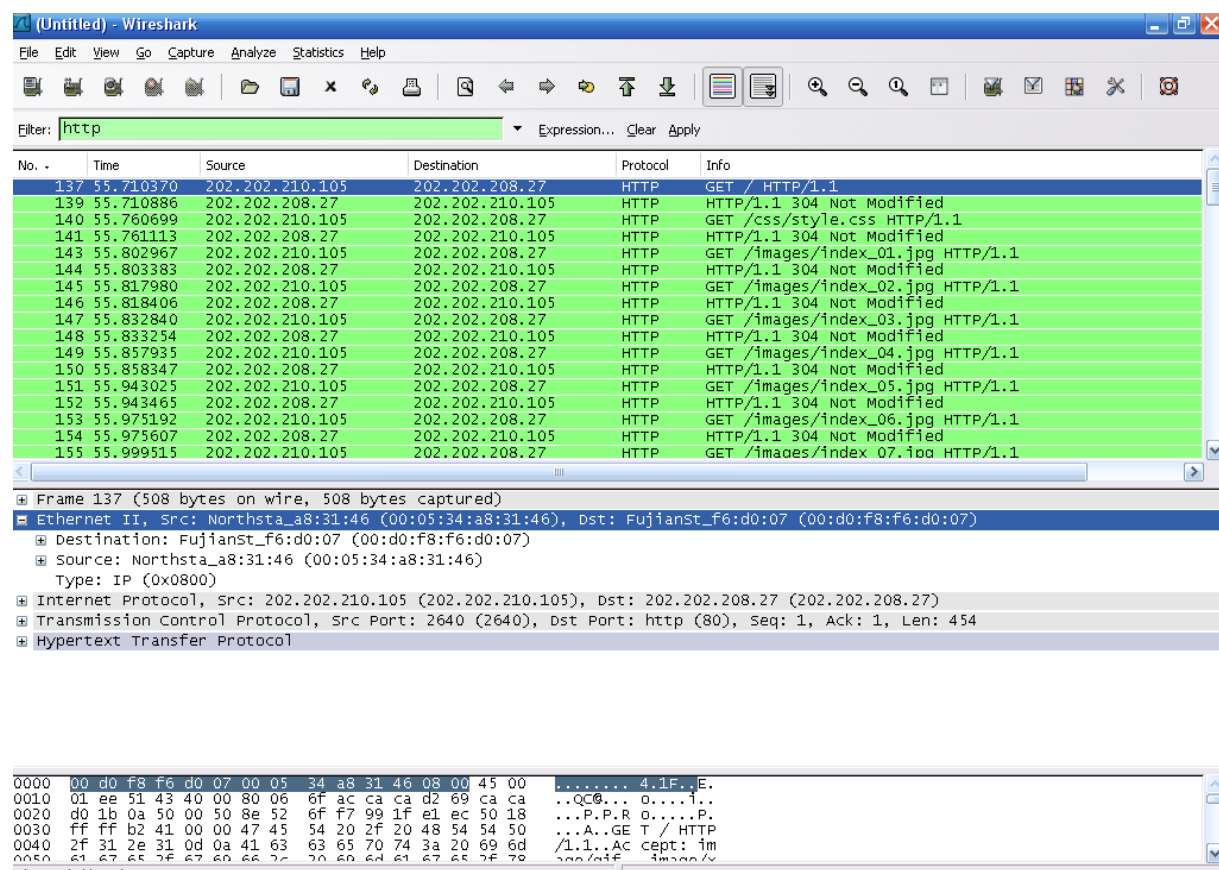


图 4

五、实验报告内容

在实验基础上，回答以下问题：

- (1) 列出在第 5 步中分组列表子窗口所显示的所有协议类型；
- (2) 从发出 HTTP GET 报文到接收到对应的 HTTP OK 响应报文共需要多长时间？（分组列表窗口中 Time 列的值是从 Wireshark 开始追踪到分组被捕获的总的时间数，以秒为单位）
- (3) 你主机的 IP 地址是什么？你访问的服务器的 IP 地址是什么？

实验二 使用 Wireshark 分析以太网帧与 ARP 协议

一、实验目的

分析以太网帧，MAC 地址和 ARP 协议

二、实验环境

与因特网连接的计算机网络系统；主机操作系统为 windows；使用 Wireshark、IE 等软件。

三、实验步骤：

IP 地址用于标识因特网上每台主机，而端口号则用于区别在同一台主机上运行的不同网络应用程序。在链路层，有介质访问控制（Media Access Control, MAC）地址。在局域网中，每个网络设备必须有唯一的 MAC 地址。设备监听共享通信介质以获取目标 MAC 地址与自己相匹配的分组。

Wireshark 能把 MAC 地址的组织标识转化为代表生产商的字符串，例如，00:06:5b:e3:4d:1a 也能以 Dell:e3:4d:1a 显示，因为组织唯一标识符 00:06:5b 属于 Dell。地址 ff:ff:ff:ff:ff:ff 是一个特殊的 MAC 地址，意味着数据应该广播到局域网的所有设备。

在因特网上，IP 地址用于主机间通信，无论它们是否属于同一局域网。同一局域网间主机间数据传输前，发送方首先要把目的 IP 地址转换成对应的 MAC 地址。这通过地址解析协议 ARP 实现。每台主机以 ARP 高速缓存形式维护一张已知 IP 分组就放在链路层帧的数据部分，而帧的目的地址将被设置为 ARP 高速缓存中找到的 MAC 地址。如果没有发现 IP 地址的转换项，那么本机将广播一个报文，要求具有此 IP 地址的主机用它的 MAC 地址作出响应。具有该 IP 地址的主机直接应答请求方，并且把新的映射项填入 ARP 高速缓存。

发送分组到本地网外的主机，需要跨越一组独立的本地网，这些本地网通过称为网关或路由器的中间机器连接。网关有多个网络接口卡，用它们同时连接多个本地网。最初的发送者或源主机直接通过本地网发送数据到本地网关，网关转发数据报到其它网关，直到最后到达目的主机所在的本地网的网关。

1、俘获和分析以太网帧

（1）选择 工具->Internet 选项->删除文件

（2）启动 Wireshark 分组嗅探器

(3) 在浏览器地址栏中输入网址：<http://gaia.cs.umass.edu/wireshark-labs> 就进入了美国麻省理工大学计算机学院的 wireshark 实验室网站。

(4) 停止分组俘获。在俘获分组列表中 (listing of captured packets) 中找到 HTTP GET 信息和响应信息，如图 1 所示。(如果你无法俘获此分组，在 Wireshark 下打开文件名为 *ethernet--ethereal-trace-1* 的文件进行学习)。

HTTP GET 信息被封装在 TCP 分组中，TCP 分组又被封装在 IP 数据报中，IP 数据报又被封装在以太网帧中)。在分组明细窗口中展开 Ethernet II 信息 (packet details window)。回答下面的问题：

- 1、你所在的主机 48-bit Ethernet 地址是多少？
- 2、Ethernet 帧中目的地址是多少？这个目的地址是 gaia.cs.umass.edu 的 Ethernet 地址吗？

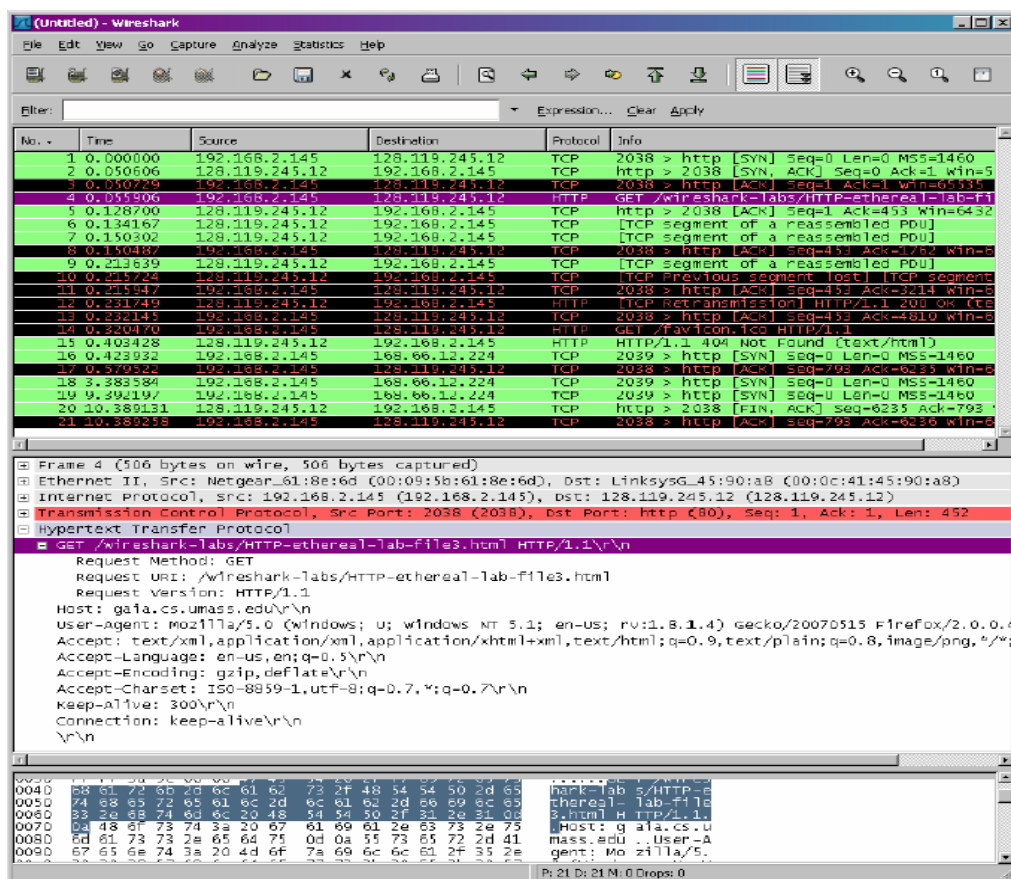


图1 HTTP GET信息和响应信息

2、分析地址 ARP 协议

(1)ARP Caching

ARP 协议用于将目的 IP 转换为对应的 MAC 地址。Arp 命令用来观察和操作缓存中的内容。虽然 arp 命令和 ARP 有一样的名字，很容易混淆，但它们的作用是不同的。在命令提示符下输入 arp 可以看到在你所在电脑中 ARP 缓存中的内容。为了观察到你所发电脑发送和接收 ARP 信息，我们需要清除 ARP 缓存，否则你所在主机很容易找到已知 IP 和匹配的 MAC 地址。

步骤如下：

(1)清除 ARP cache,具体做法:在 MSDOS 环境下,输入命令 arp -d * command , The -d 表示清除操作,* 删除 all table entries.

(2) 选择 工具->Internet 选项->删除文件

(3) 启动 Wireshark 分组俘获器

(4) 在浏览器地址栏中输入如下网址：

[http://gaia.cs.umass.edu/wireshark-labs/ HTTP-wireshark-lab-file3.html](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html)

(5) 停止分组俘获。

(6) 选择 Analyze->Enabled Protocols->取消 IP 选项->选择 OK。如图 3 所示：

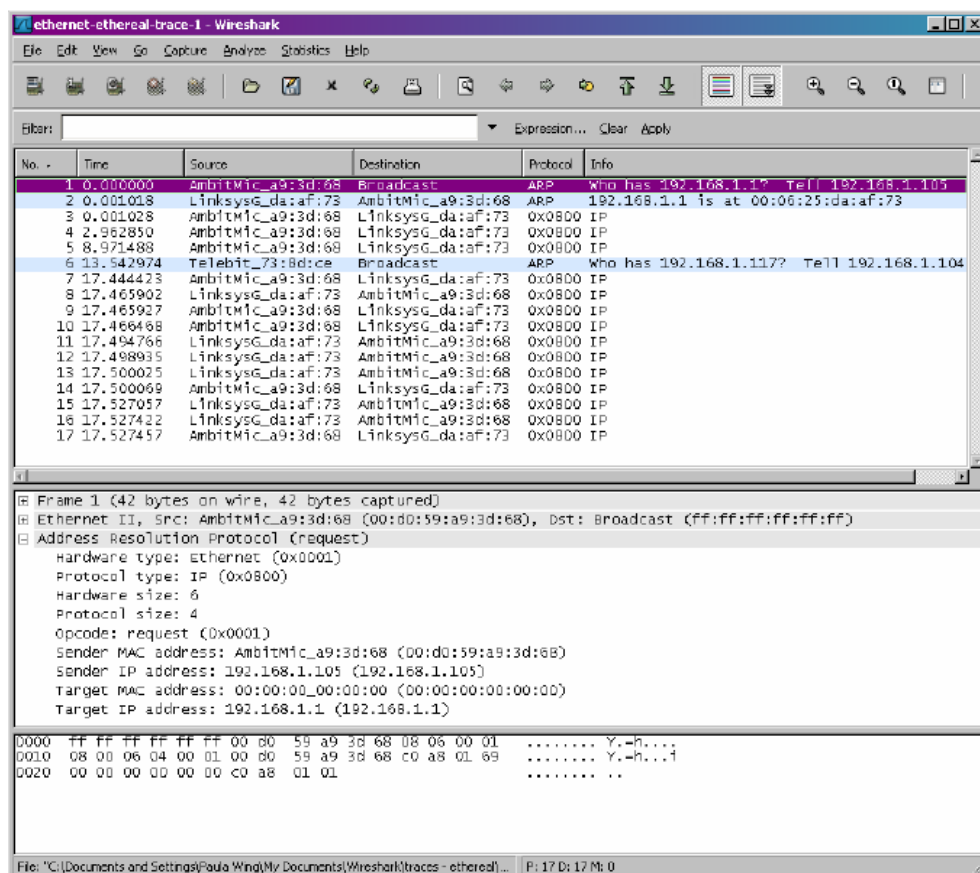


图3 利用Wireshark俘获的ARP分组

四、实验报告

根据实验，回答下面问题：

由于此实验是关于 Ethernet 和 ARP 的，所以，只需在分组俘获列表中显示 IP 层下面的协议，具体做法为：选择 Analyze->Enabled Protocols->不选择 IP 协议 ->select ok 如图 2 所示：

