



计算机网络课程设计指导书

《计算机网络》课程组 编著

上海海洋大学海洋智能信息实验教学示范中心

目录

实验一：初识 WIRESHARK.....	3
实验二：802.3 协议分析和以太网.....	7
实验三：PING 命令初探	11
实验四：IP 层协议分析	20
实验五：TCP 协议分析	25
实验六：HTTP 和 DNS 分析	31
实验七：利用 Ethereal 分析 ARP 协议	35
实验八：利用 Ethereal 分析 HTTP 协议.....	40

实验 一 初识 WIRESHARK

一、实验目的

通过实验，了解实验环境 WIRESHARK 的基本使用，观察 PING 命令时抓包情况，观察登陆某一网站时抓包情况。

二、实验环境

WIRESHARK

三、实验理论

分组是目前分组交换网络中传输的格式化数据块，是基本的信息传输单位。它与数据报意义近似，但有微小的区别。分组是一个泛指词，而数据报往往用于不可靠服务场合。分组由控制信息和用户数据 (payload) 构成。

Wireshark(前称 Ethereal)是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark 使用 WinPCAP 作为接口，直接与网卡进行数据报文交换。在 GNUGPL 通用许可证的保障范围底下，使用者可以以免费的代价取得软件与其源代码，并拥有针对其源代码修改及客制化的权利。Ethereal 是目前全世界最广泛的网络封包分析软件之一。

四、实验内容

1. 使用 WireShark 软件过滤，抓取封包

四、实验步骤

1. 使用 WireShark 软件过滤，抓取封包

- 1.1 教师演示 WireShark 抓包过程及过滤器使用方法（略）。

1.2 在 Windows 的命令提示符界面中输入命令：ipconfig /all，会显示本机的网络信息。

1.3 观察运行结果，获得本机的以太网地址，IP 地址。如图 1 所示

```
Ethernet adapter 本地连接:
    Connection-specific DNS Suffix . . . : 
    Description . . . . . : Intel(R) PRO/1000 PL Network Connect
ion
    Physical Address. . . . . : 00-15-58-2F-7E-7E
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 172.16.1.98
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.1.1
    DNS Servers . . . . . : 172.16.2.25
```

图 1

1.4 从 http://openmaniak.com/cn/wireshark_use.php#menus，学习 WIRESHARK 软件使用方法，主要是过滤条件的设置。

1.5 从 <http://product.pconline.com.cn/itbk/wlbg/network/1305/3305248.html#ad=7094>，学习 PING 命令的用法，主要是该命令各个参数的设置。

1.6 PING 旁边同学的 IP，使用软件过滤，抓取封包。

五、实验报告要求：

实验报告参考模板如下：



实验报告

题目： _____

学院：信息学院

专业：

班级：

学号：

姓名：

年 月 日

一、实验目的

通过实验，了解实验环境 WIRESHARK 的基本使用，观察 PING 命令时抓包情况，观察登陆某一网站时抓包情况。

二、实验环境

WIRESHARK

三、实验内容

四、实验步骤（图文方式叙述）

五、实验结果及分析（遇到的问题与解决）

六、实验体会

（可以从下面两个方面作答：1、MAC 地址和 IP 地址的区别是什么？2、给你的某一同学发送封包，使用软件的过滤器，观察该 IP 的封包，说明你发送包的大小及发送 IP。）

实验二 802.3 协议分析和以太网

一、实验目的

分析 802.3 协议，熟悉以太网帧的格式。

二、实验环境

WIRESHARK

三、实验内容

1. 俘获并分析以太网帧

四、实验步骤

1. 俘获并分析以太网帧

1.1 在 IE 窗口中，选择“工具/Internet 选项/删除文件”命令，清空浏览器缓存。如图 1 和图 2 所示



图 1



图 2

1.2 启动 WIRESHARK，开始分组俘获。如图 3 所示

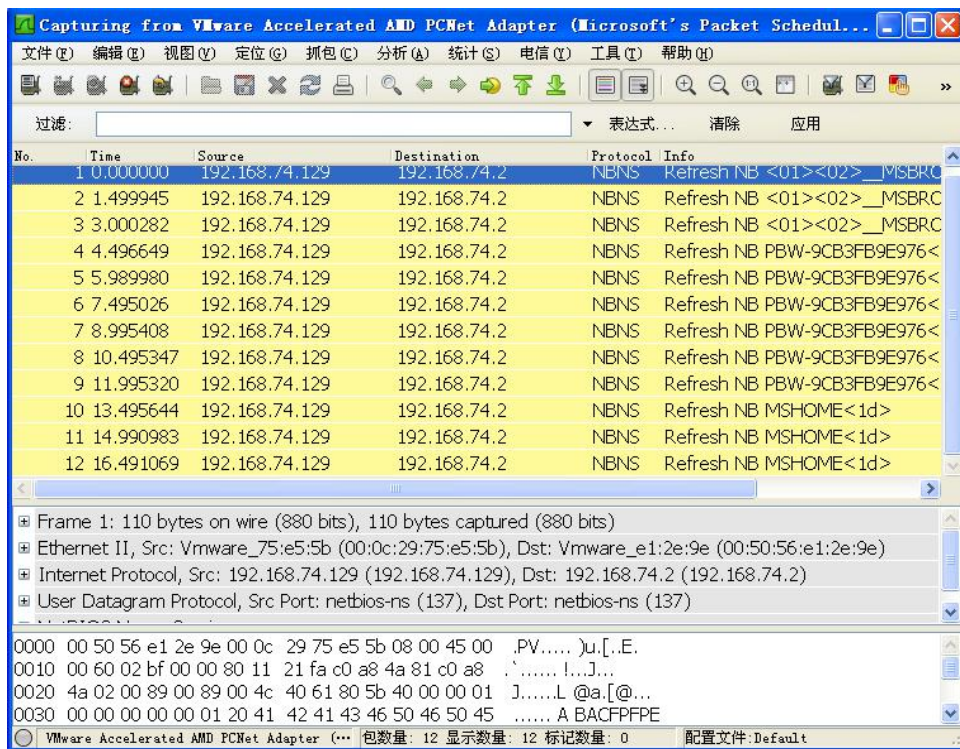


图 3

1.3 在浏览器的地址栏中输入：<http://shou.edu.cn>。如图 4 所示



图 4

1.4 停止分组俘获。首先，找到你的主机向服务器 shou.edu.cn 发送的 HTTP GET 报文的分组序号，以及服务器发送到你主机上的 HTTP 响应报文的序号。如图 5 所示

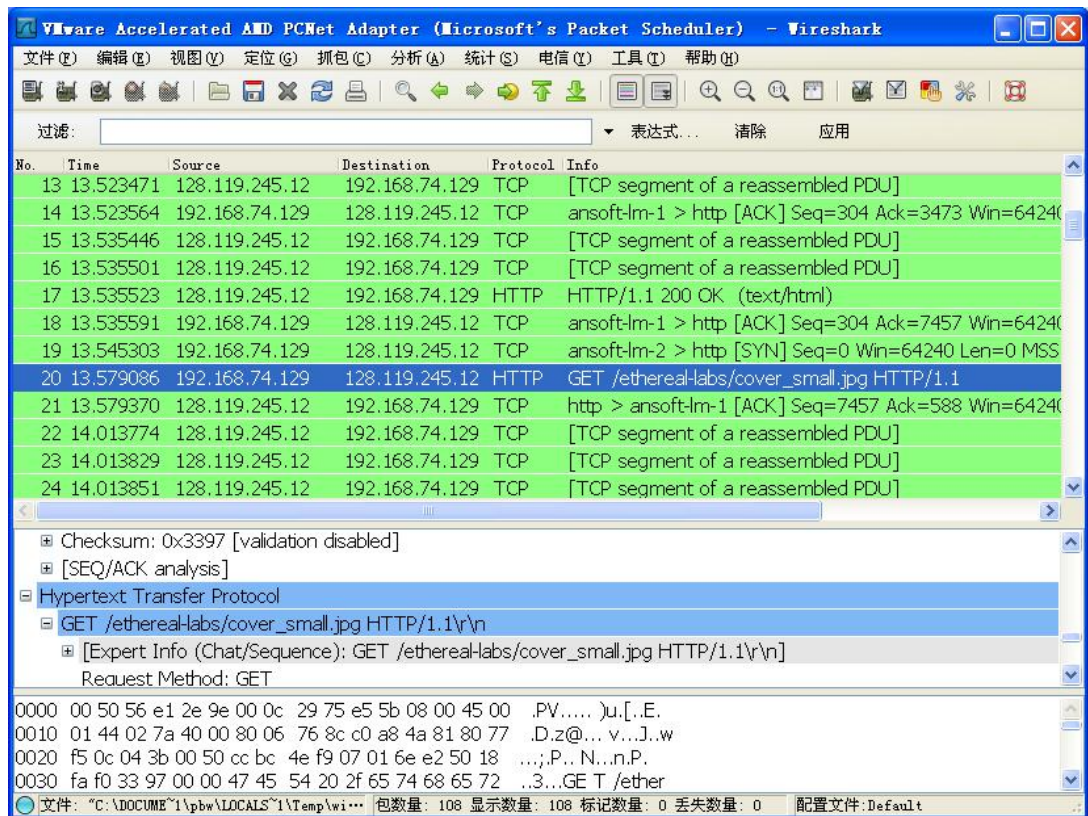


图 5

1.5 选择“Analyze->Enabled Protocols”，取消对 IP 复选框的选择，单击 OK。
如图 6 所示



图 6

五、实验报告要求：

按实验报告模板撰写实验报告

实验三：PING 命令初探

一、实验目的

掌握各种主要命令的作用；掌握各种网络命令的主要测试方法；理解各种网络命令主要参数的含义。

二、实验环境

WIRESHARK

三、实验理论

在网络调试的过程中，常常要检测服务器和客户机之间是否连接成功、希望检查本地计算机和某个远程计算机之间的路径、检查 TCP/IP 的统计情况以及系统使用 DHCP 分配 IP 地址时掌握当前所有的 TCP/IP 网络配置情况，以便及时了解整个网络的运行情况，以确保网络的连通性，保证整个网络的正常运行。在 Windows 中提供了以下命令行程序：

- (1) ping：用于测试计算机之间的连接，这也是网络配置中最常用的命令；
- (2) ipconfig：用于查看当前计算机的 TCP/IP 配置；
- (3) netstat：显示连接统计；
- (4) tracert：进行源主机与目的主机之间的路由连接分析；
- (5) arp：实现 IP 地址到物理地址的单向映射。

四、实验内容

1. 掌握各种主要命令的作用
2. 掌握各种网络命令的主要测试方法

五、实验步骤

1. 掌握各种主要命令的作用

1.1 Ping 命令

一般情况下，用户可以通过使用一系列 Ping 命令来查找问题出在什么地方，或检验网络运行的情况时。典型的检测次序及对应的可能故障如下：

(1) ping 127.0.0.1：如果测试成功，表明网卡、TCP/IP 协议的安装、IP 地址、子网掩码的设置正常。如果测试不成功，就表示 TCP/IP 的安装或运行存在某些最基本的问题。

(2) ping 本机 IP：如果测试不成功，则表示本地配置或安装存在问题，应当对网络设备和通讯介质进行测试、检查并排除。

(3) ping 局域网内其它 IP：如果测试成功，表明本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那么表示子网掩码不正确或网卡配置错误或电缆系统有问题。

(4) ping 网关 IP：这个命令如果应答正确，表示局域网中的网关或路由器正在运行并能够做出应答。

(5) ping 远程 IP：如果收到正确应答，表示成功的使用了缺省网关。对于拨号上网用户则表示能够成功的访问 Internet。

(6) ping localhost：localhost 是系统的网络保留名，它是 127.0.0.1 的别名，每台计算机都应该能够将该名字转换成该地址。如果没有做到这点，则表示主机文件（/Windows/host）存在问题。

(7) Ping www.163.com（一个著名网站域名）：对此域名执行 Ping 命令，计算机必须先将域名转换成 IP 地址，通常是通过 DNS 服务器。如果这里出现故障，则表示本机 DNS 服务器的 IP 地址配置不正确，或 DNS 服务器有故障。

如果上面所列出的所有 Ping 命令都能正常运行，那么计算机进行本地和远程通信基本上就没有问题了。但是，这些命令的成功并不表示你所有的网络配置都没

有问题，例如，某些子网掩码错误就可能无法用这些方法检测到。Ping 命令的常用参数选项如下：

ping IP -t: 连续对 IP 地址执行 Ping 命令，直到被用户以 Ctrl+ C 中断。

ping IP -l 2000: 指定 Ping 命令中的数据长度为 2000 字节，而不是缺省的 32 字节。

ping IP -n: 执行特定次数的 Ping 命令。

ping IP -f: 强行不让数据包分片。

ping IP -a: 将 IP 地址解析为主机名。

1.2 IP 配置程序 Ipconfig

发现和解决 TCP/IP 网络问题时，先检查出现问题的计算机上的 TCP/IP 配置。可以使用 ipconfig 命令获得主机 TCP/IP 配置信息，包括 IP 地址、子网掩码和默认网关。命令格式为 ipconfig /options，其中 options 选项如下：

/?: 显示帮助信息。

/all: 显示全部配置信息。

/release: 释放指定网络适配器的 IP 地址。

/renew: 刷新指定网络适配器的 IP 地址。

/flushdns: 清除 DNS 解析缓存。

/registerdns: 刷新所有 DHCP 租用和重新注册 DNS 名称。

/displaydns: 显示 DNS 解析缓存内容。

使用带/all 选项的 ipconfig 命令时，将给出所有接口的详细配置报告，包括任何已配置的串行端口。使用 ipconfig /all 可以将命令输出重定向到某个文

件，并将输出粘贴到其他文档中，也可以用该输出确认网络上每台计算机的 TCP/IP 配置，或者进一步调查 TCP/IP 网络问题。如图 1 所示。

```
C:\>
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : gq
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : Yes
    WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix . :
    Description . . . . . : IC Plus IP100 10/100 Fast Ethernet A
dapter
    Physical Address. . . . . : 00-50-8D-74-3C-EB
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 10.112.12.66
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.112.12.254
    DNS Servers . . . . . : 202.100.192.68
                          210.37.95.1
```

图 1

1.2.1 另一方法：点击右下角的电脑图像，如图 2 所示



图 2

1.2.2 点击详细信息，如图 3 所示



图 3

1. 2. 3 记下地址信息：IP 地址、子网掩码、默认网关、MAC 地址等信息。

2. 掌握各种网络命令的主要测试方法

2.1 显示网络连接程序 netstat

netstat 命令的功能是显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运作，其命令格式为：

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

参数说明如下：

(1) Netstat -s: -s 选项能够按照各个协议分别显示其统计数据。这样就可以看到当前计算机在网络上存在哪些连接，以及数据包发送和接收的详细情况等等。如果应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的的数据，那么可以用本选项来查看一下所显示的信息。仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

(2) Netstat -e: -e 选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些

统计数据既有发送的数据报数量，也有接收的数据报数量。使用这个选项可以统计一些基本的网络流量。

(3) Netstat -r: -r 选项可以显示关于路由表的信息，类似后面所讲使用 route print 命令时看到的信息。除了显示有效路由外，还显示当前有效的连接。

(4) Netstat -a: -a 选项显示一个所有有效连接信息列表，包括已建立的连接 (ESTABLISHED)，也包括监听连接请求 (LISTENING) 的那些连接。

(5) Netstat -n: 显示所有已建立的有效连接，以数字格式显示地址和端口号。

(6) Netstat -p protocol: 显示由 protocol 指定的协议的连接。protocol 可以是 TCP

或 UDP。如果与 -s 选项并用显示每个协议的统计，protocol 可是 TCP、UDP、ICMP 或 IP。

(7) Netstat interval: 重新显示所选的统计，在每次显示之间暂停 interval 秒。按 Ctrl+B 键停止，重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。我们可以利用 netstat 命令查看本机开放端口的方法来检查自己是否被种了木马或其他黑客程序。进入到命令行下，使用 netstat 命令的 a 和 n 两个参数的组合，如图 4 所示。

```
C:\>netstat -an
Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING
TCP   0.0.0.0:1110           0.0.0.0:0               LISTENING
TCP   0.0.0.0:9800           0.0.0.0:0               LISTENING
TCP   10.112.12.66:139       0.0.0.0:0               LISTENING
TCP   127.0.0.1:1025         0.0.0.0:0               LISTENING
TCP   127.0.0.1:1103        127.0.0.1:1110         CLOSE_WAIT
TCP   127.0.0.1:2210        127.0.0.1:9800         ESTABLISHED
TCP   127.0.0.1:9800        127.0.0.1:2210         ESTABLISHED
UDP   0.0.0.0:500            *:*
UDP   0.0.0.0:1032          *:*
UDP   0.0.0.0:1033          *:*
UDP   0.0.0.0:1748          *:*
UDP   0.0.0.0:2193          *:*
```

图 4

其中，“Active Connections”是指当前本机的活动连接；“Proto”是指连接使用的协议名称；“Local Address”是本地计算机的 IP 地址和连接正在使用的端口号；“Foreign Address”是连接该端口的远程计算机的 IP 地址和端口号；“State”则是表明 TCP 连接的状态，可以看到后面几行的监听端口是 UDP 协议的，所以没有 State 表示的状态。

2.2 路由分析诊断程序 tracert

tracert 命令可以用来跟踪一个报文从一台计算机到另一台计算机所走的路径。入图 5 所示。

命令格式如下：

```
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
```

参数说明如下：

-d: 不进行主机名称的解析。

-h maximum_hops: 最大的到达目标的跃点数。

-j host-list: 根据主机列表释放源路由。

-w timeout: 设置每次回复所等待的毫秒数。

比如用户在网上时，想知道从自己的计算机如何走到网易主页，可在 MS-DOS 方式下输入命令 `tracert www.163.com`。

```
命令提示符
C:\>tracert www.163.com

Tracing route to www.163.com [202.108.36.172]
over a maximum of 30 hops:

  1  <10 ms    10 ms    <10 ms    210.41.232.65
  2  <10 ms    <10 ms   <10 ms    210.41.232.97
  3  <10 ms    <10 ms   <10 ms    172.16.16.1
  4  <10 ms    <10 ms   <10 ms    202.112.14.13
  5  <10 ms    <10 ms   <10 ms    cd0.cernet.net [202.112.53.73]
  6  20 ms     20 ms    20 ms     202.112.46.181
  7  40 ms     40 ms    30 ms     bjwh4.cernet.net [202.112.46.65]
  8  30 ms     40 ms    40 ms     202.112.61.162
  9  *         *        *         Request timed out.
 10 40 ms     40 ms    30 ms     219.158.11.113
 11 40 ms     40 ms    40 ms     202.96.12.30
 12 30 ms     40 ms    40 ms     RTR-BT0-A-F9-1-0.bta.net.cn [202.106.192.225]
 13 30 ms     40 ms    40 ms     RTR-AHL-A-S2-0.bta.net.cn [202.106.192.170]
 14 30 ms     41 ms    40 ms     210.74.176.150
 15 40 ms     30 ms    40 ms     202.108.36.172

Trace complete.
C:\>
```

图 5

最左边的数字称为“hops”，是该路由经过的计算机数目和顺序。“10 ms”是向经过的第一个计算机发送报文的往返时间，单位为 ms。在时间信息之后，是计算机的名称信息。tracert 最多会显示 30 段“hops”，上面会同时指出每次停留的响应时间，以及网站名称和沿路停留的 IP 地址。

2.3 ARP 地址解析协议

ARP 是 TCP/IP 协议族中的一个重要协议，用于把 IP 地址映射成对应网卡的物理地址。如图 6 所示

常用命令选项：

(1) arp -a：用于查看高速缓存中的所有项目。

(2) arp -a IP：如果有多个网卡，那么使用 arp -a 加上接口的 IP 地址，就可以只显示与

该接口相关的 ARP 缓存项目。

(3) arp -s IP 物理地址: 向 ARP 高速缓存中人工输入一个静态项目。该项在计算机引导

过程中将保持有效状态, 或者在出现错误时, 人工配置的物理地址将自动更新该项目。

(4) arp -d IP: 使用本命令能够人工删除一个静态项目。

```
<C> 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\gengqiang646>arp -a

Interface: 10.112.12.66 --- 0x10003
  Internet Address      Physical Address      Type
  10.112.12.254         00-e0-fc-1c-00-fc    dynamic

C:\Documents and Settings\gengqiang646>arp -s 10.112.12.33 11-22-33-ee-ff-aa

C:\Documents and Settings\gengqiang646>arp -a

Interface: 10.112.12.66 --- 0x10003
  Internet Address      Physical Address      Type
  10.112.12.33          11-22-33-ee-ff-aa    static
  10.112.12.254         00-e0-fc-1c-00-fc    dynamic

C:\Documents and Settings\gengqiang646>
```

图6

五、实验报告要求:

按实验报告模板撰写实验报告

实验 四 IP 层协议分析

一、实验目的

理解 IP 层的作用以及 IP 地址的分类方法；理解子网的划分和子网掩码的作用；掌握 IP 数据包的组成和网络层的基本功能。

二、实验环境

WIRESHARK

三、实验内容

1. 查看本机 IP 地址及子网掩码
2. 利用网络协议分析软件捕获并分析 IP 数据包
3. 利用 PING 命令发送 IP 数据包
4. ping 本地主机，分析 IP 协议

四、实验步骤

1. 查看本机 IP 地址及子网掩码

1.1 在运行中输入 cmd，出现界面后输入 ipconfig /all。如图 1 所示

```
G:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : 97ebd74a16b94e6
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接 5:

    Connection-specific DNS Suffix  . :
    Description . . . . . : Attansic L2 Fast Ethernet 10/100 Base-T A
dapter
    Physical Address. . . . . : 00-1B-FC-A6-AE-E2
    DHCP Enabled. . . . . : No
    IP Address. . . . . : 172.16.1.239
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.1.1
    DNS Servers . . . . . : 172.16.1.248
                           202.96.64.68
```

图 1

1.2 观察运行结果，获得本机的 IP 地址及子网掩码，从上图中的显示结果中可以看到，ipconfig /all 命令输出包括主机名称，节点类型等，以及网络接口上的相关配置。从上图中可以看到网络接口配置信息如图 2 所示：

- **MAC 地址:** 00-1B-FC-A6-AE-E2
- **DHCP:** 为未启用
- **IP 地址:** 172.16.1.239
- **子网掩码:** 255.255.255.0
- **默认网关:** 172.16.1.1
- **DNS 服务器:** 172.16.1.248
- 202.96.64.68

图 2

思考 1: 分析本主机属于哪一类 IP 地址，网络号、子网号和主机号分别是什么？

2. 利用网络协议分析软件捕获并分析 IP 数据包

2.1 在本地主机中打开网络协议分析软件，在工具栏中点击“开始”

2.2 在捕获到数据包中，选择 IP 数据包（协议类型为 TCP\IPV4\ICMP）进行分析，如图 3 所示。

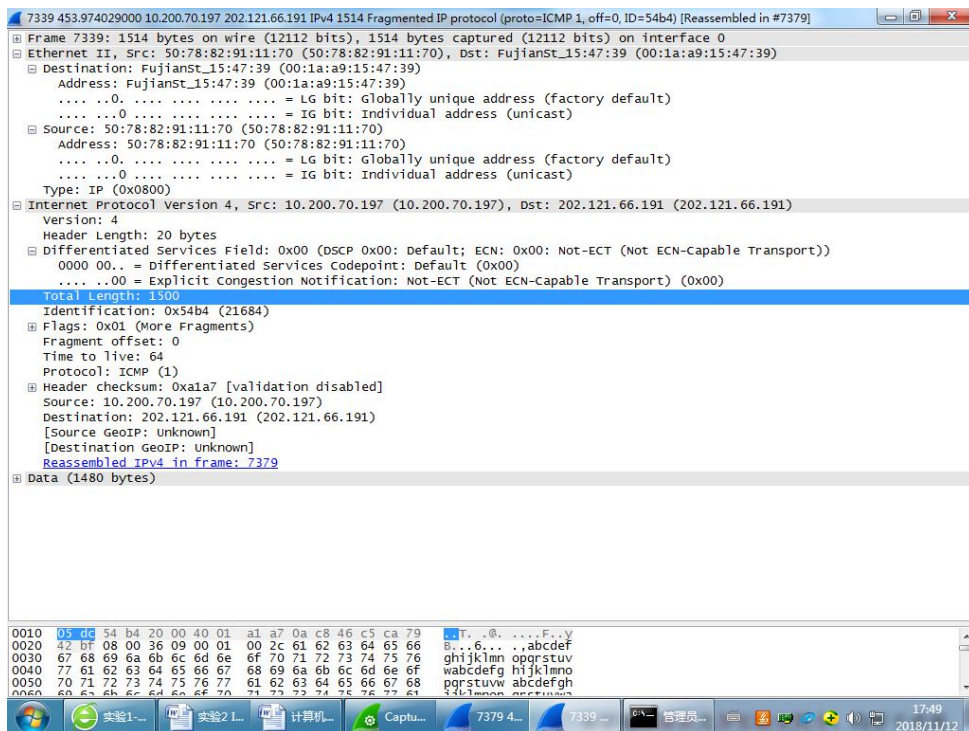


图 3

2.3 分析捕获到的 IP 数据包，在本实验中，只分析数据的 IP 包头部分。如图 4 所示：

- **总长度：** 60，表示总长度为 60 字节。
- **标识：** 0X1F06，此数据包没有进行分片。
- **标志：** 2，二进制为 010，表示此数据包不可分片。
- **分段偏移量：** 0X0000，此数据包没有进行分片。
- **生存时间：** 127，每经过一个路由器，生存时间减 1，当生存时间减小为 0 时，数据包被丢弃而不被转发。
- **源 IP 地址：** 此字段显示了数据包的源地址。
- **目的 IP 地址：** 此字段显示了数据包的目的地址。
- **其他：** 此包头中，没有选项字段，没有填充字段。IP 报头之后的部分为 IP 包中的数据部分。

图 4

思考 2. 所捕获的 IP 数据报，可以发现头部开始并不是版本号，那么头部开始时什么，实际上我们捕获的是什么？

3. 利用 PING 命令发送 IP 数据包

3.1 Ping www.baidu.com -l 2000 (过大的好像会封掉)

3.2 分析捕获到的数据包的 IPv4 报头部分，如图 5 所示：

- **版本信息：**IPv4 报文的版本信息为 4。
- **头部长度：**IPv4 报头不含选项和填充字段长度为 20 字节，是 32 比特的 5 倍。
- **总长度：**总长度包含 IP 报头长度和 IP 包中的数据长度，协议分析软件将 IP 发送时自动将上层协议选择为 TCP，因此数据内容为 TCP 报头共 20 字节以及 20 字节数据，因此接收到的 IP 报文长度为 60 字节。
- **标识、标识、分段偏移量：**均与分片有关。
- **生存时间：**由于数据包从源端到目的端没有经过任何路由器的转发，TTL 值不变为 128。
- **校验和：**由于发包过程中，标识位和分段偏移修改，因此校验和也和发送的数据稍有不同。
- **源目标地址：**源目标地址在 IP 包的发送过程中不做修改。

图 5

用同样的方法，在主机 A 中编辑 IP 包，将目的 MAC 地址和目的 IP 地址修改为另外一组主机的地址如 pc3，发送数据包。注意，封装 IP 包发往不同网段的目的地主机时，目标 MAC 地址选择网关的 MAC 地址，地址本中找不到不同网段的 IP 地址时，手工输入目的 IP 地址。

思考 3. 所捕获到的报文，其最大长度为多少，原因是什么？

4. ping 本地主机，分析 IP 协议

4.1 在地址本中选择与本主机在同一子网中另一主机的 IP 地址(假设为：172.16.1.251)。在本机命令行界面下运行：ping 172.16.1.251。

4.2 在 ping 的目的地址的主机上用协议分析器一端捕获数据，记录源、目的物理地址及源、目的 IP 地址。

4.3 按照地址本中的记录，分析捕获数据的 MAC 地址与 IP 地址的对应关系。

4.4 在 ping 目的主机上通过协议分析器，查看“交互序列图”，了解 PING 程序的会话过程，如图 6 所示。

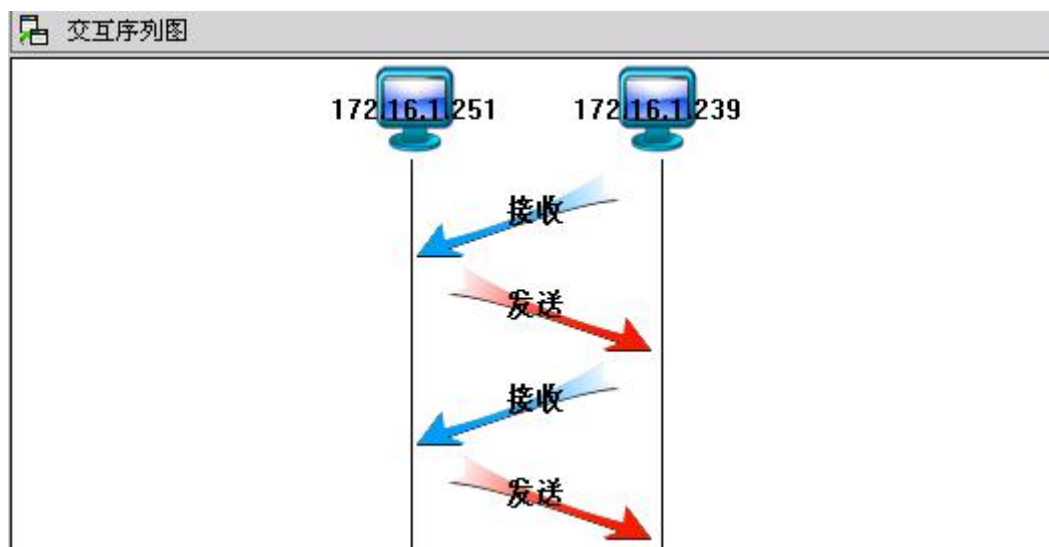


图 6

4.5 选择与本主机属于不同子网另一主机的 IP 地址(假设为: 172.16.2.1), 在命令行方式下运行: ping 172.16.2.1。

4.6 协议分析器端捕获数据, 记录源、目的物理地址和源、目的 IP 地址。

思考 4. 分析捕获数据的 MAC 地址与 IP 地址是否具有对应关系, 比较上面两个实验的结果, 分析二者有何不同?

五、实验报告要求

按实验报告模板撰写实验报告

实验 五 TCP 协议分析

一、实验目的

预习 TCP 报文段首部及端口知识；理解 TCP 协议三次握手，四次握手的含义。

二、实验环境

WIRESHARK

三、实验内容

1. 捕获一个从你电脑到远程服务器的 TCP 数据
2. 掌握 TCP 报文段首部的格式、长度以及各字段的功能
3. 学会通过分析 TCP 报文段首部，理解 TCP 握手机制

四、实验步骤

1. 捕获一个从你电脑到远程服务器的 TCP 数据

1.1 选择一个网站上网冲浪，用” TCP” 为过滤条件，捕获建立连接和断开连接的数据。如图 1 所示：

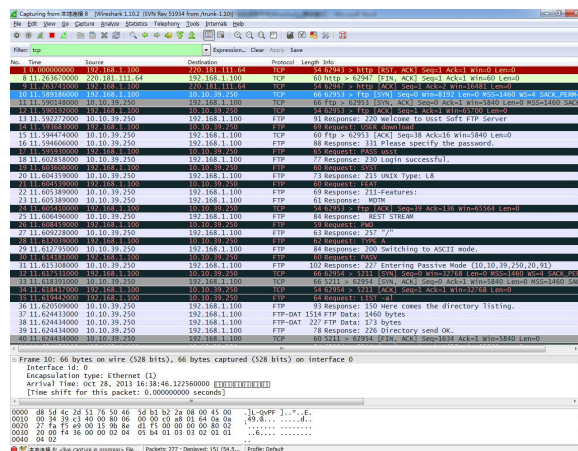


图 1
25 / 43

1.2 建立连接

1.2.1 TCP 连接通过称为三次握手的三条报文来建立的。观察以上数据，其中分组 10 到 12 显示的就是三次握手。第一条报文没有数据的 TCP 报文段（分组 10），并将首部 SYN 位设置为 1。因此，第一条报文常被称为 SYN 分组。这个报文段里的序号可以设置成任何值，表示后续报文设定的起始编号。连接不能自动从 1 开始计数，选择一个随机数开始计数可避免将以前连接的分组错误地解释为当前连接的分组。观察分组 10，Wireshark 显示的序号是 0。选择分组首部的序号字段，原始框中显示“9b 8e d1 f5”。Wireshark 显示的是逻辑序号，真正的初始序号不是 0。如图 2 所示：

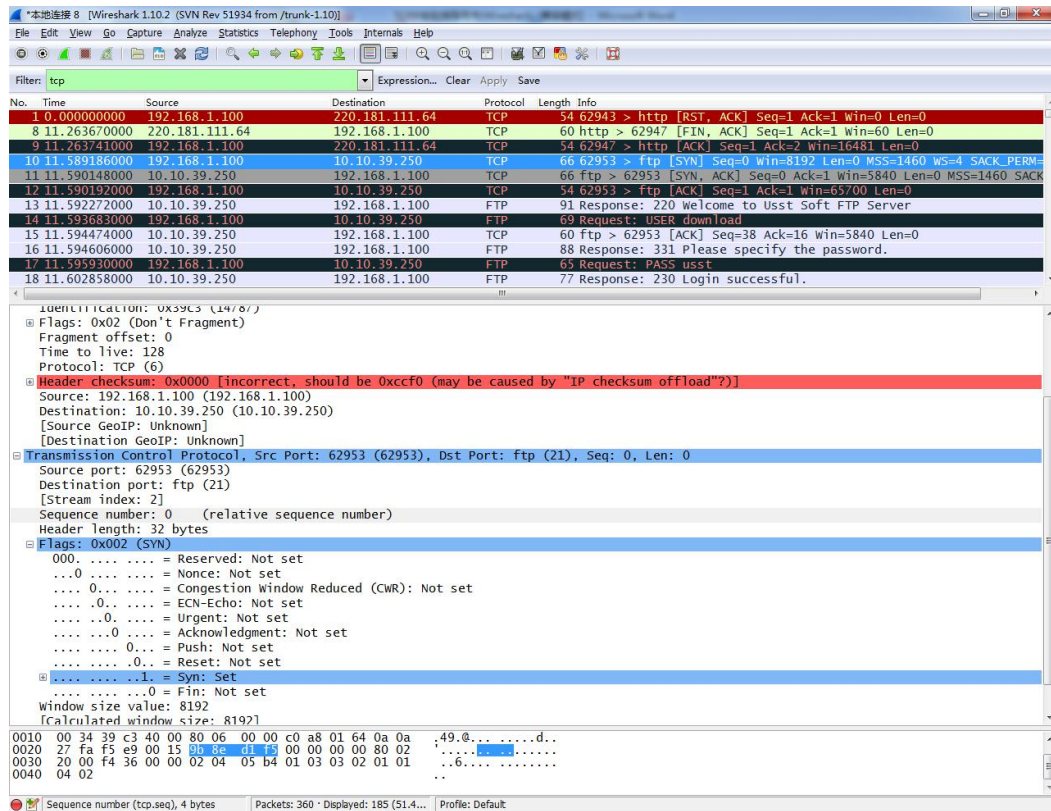


图 2

1.2.2 SYN 分组通常是从客户端发送到服务器。这个报文段请求建立连接。一旦成功建立了连接，服务器进程必须已经在监听 SYN 分组所指示的 IP 地址和端口号。如果没有建立连接，SYN 分组将不会应答。如果第一个分组丢失，客户端通常会发送若干 SYN 分组，否则客户端将会停止并报告一个错误给应用程序。如果服务器进程正在监听并接收到来的连接请求，它将以一个报文段进行相应，这个

报文段的 SYN 位和 ACK 位都置为 1。通常称这个报文段为 SYNACK 分组。SYNACK 分组在确认收到 SYN 分组的同时发出一个初始的数据流序号给客户端。如图 3 所示

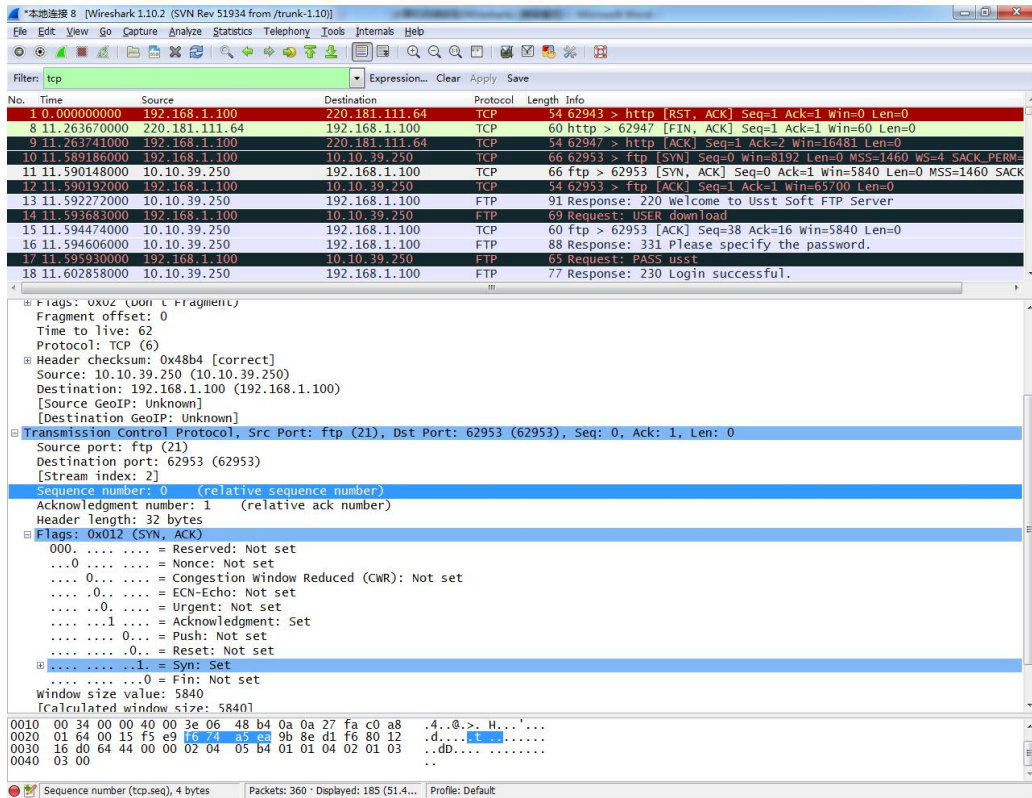


图 3

1.2.3 分组 11 的确认号字段在 Wireshark 的协议框中显示 1，并且在原始框中的值是“9b 8e d1 f6”（比“9b 8e d1 f5”多 1）。这解释了 TCP 的确认模式。TCP 接收端确认第 X 个字节已经收到，并通过设置确认号为 X+1 来表明期望收到下一个字节号。分组 11 的序号字段在 Wireshark 的协议显示为 0，但在原始框中的实际值却是“f6 74 a5 ea”。这表明 TCP 连接的双方会选择数据流中字节的起始编号。所有初始序号逻辑上都视同为序号 0。

1.2.4 最后，客户端发送带有标志 ACK 的 TCP 报文段，而不是带 SYN 的报文段来完成三次握手的过程。这个报文段将确认服务器发送的 SYNACK 分组，并检查 TCP 连接的两端是否正确打开合运行。

1.3 关闭连接

当两端交换带有 FIN 标志的 TCP 报文段并且每一端都确认另一端发送的 FIN 包时，TCP 连接将会关闭。FIN 位字面上的意思是连接一方再也没有更多新的数据发送。然而，那些重传的数据会被传送，直到接收端确认所有的信息。通过分组 43, 44 和 54, 55 我们可以看到 TCP 连接被关闭。如图 4 所示。

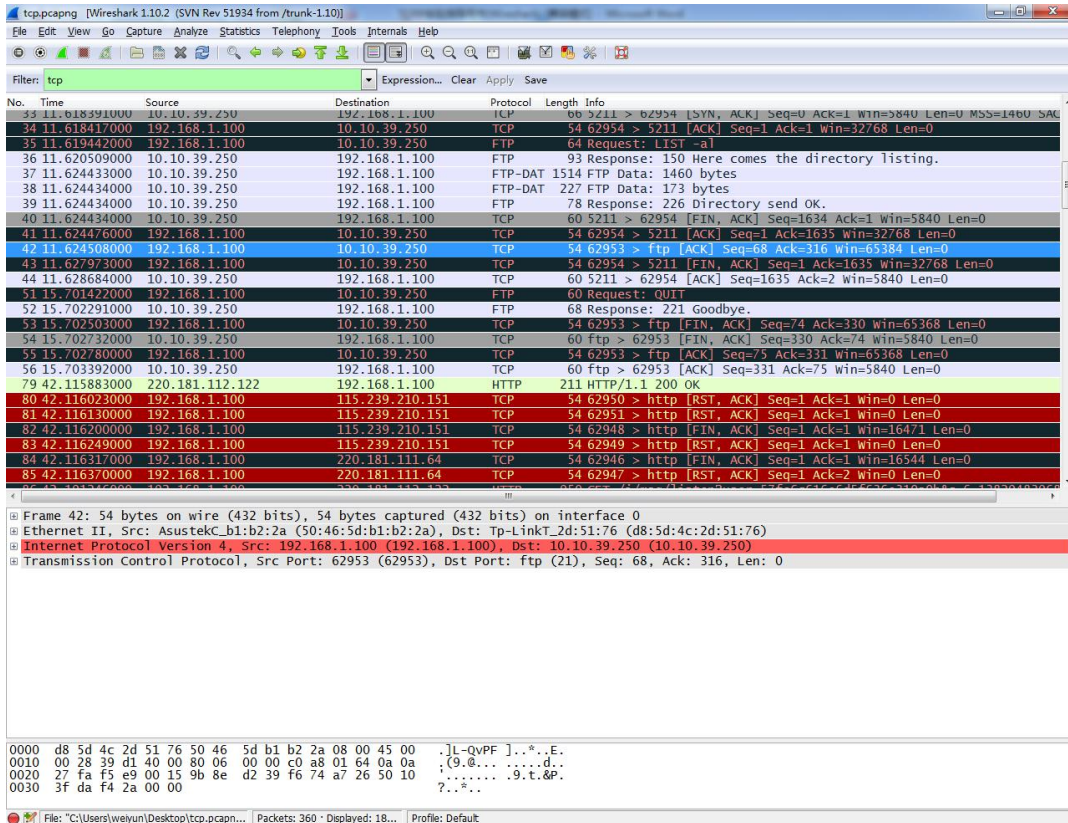


图 4

2. 掌握 TCP 报文段首部的格式、长度以及各字段的功能

2.1 当一个 TCP 发送端传输一个报文段的同时也设置了一个重传计时器。当确认到达时，这个计时器就自动取消。如果在数据的确认信息到达之前这个计时器超时，那么数据就会重传。

重传计时器能够自动灵活设置。最初 TCP 是基于初始的 SYN 和 SYN ACK 之间的时间来设置重传计时器的。它基于这个值多次设置重传计时器来避免不必要的重传。在整个 TCP 连接中，TCP 都会注意每个报文段的发送和接到相应的确认所经历的时间。TCP 在重传数据之前不会总是等待一个重传计算器超时。TCP 也会把一系列重复确认的分组当作是数据丢失的征兆。

2.2 SACK 选项协商

在上面的每次跟踪中，我们能观察建立连接的三次握手。在 SYN 分组中，发送端在 TCP 的首部选项中通过包括 SACK permitted 选项来希望使用 TCP SACK。在 SYN ACK 包中接收端表示愿意使用 SACK。这样双方都同意接收选择性确认信息。SACK 选项如图 5 所示。

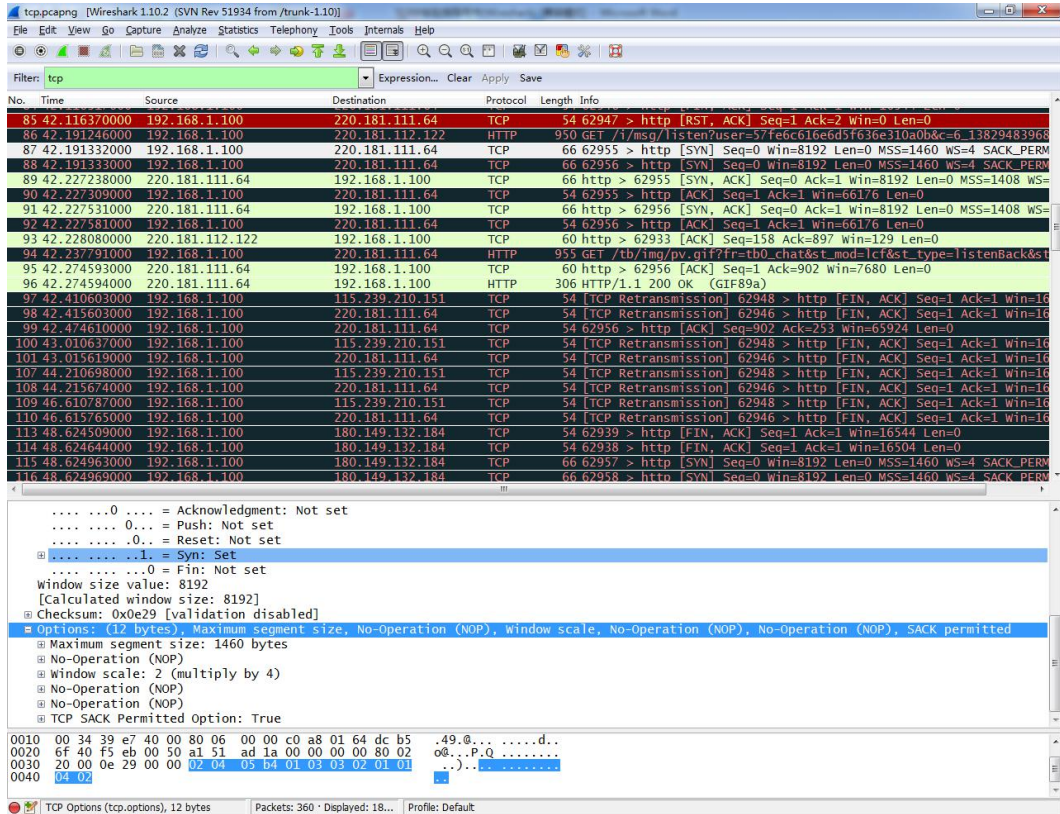


图 5

3. 学会通过分析 TCP 报文段首部，理解 TCP 握手机制

3.1 用显示过滤器 tcp.analysis.retransmission 搜索重传。如图 6 所示。

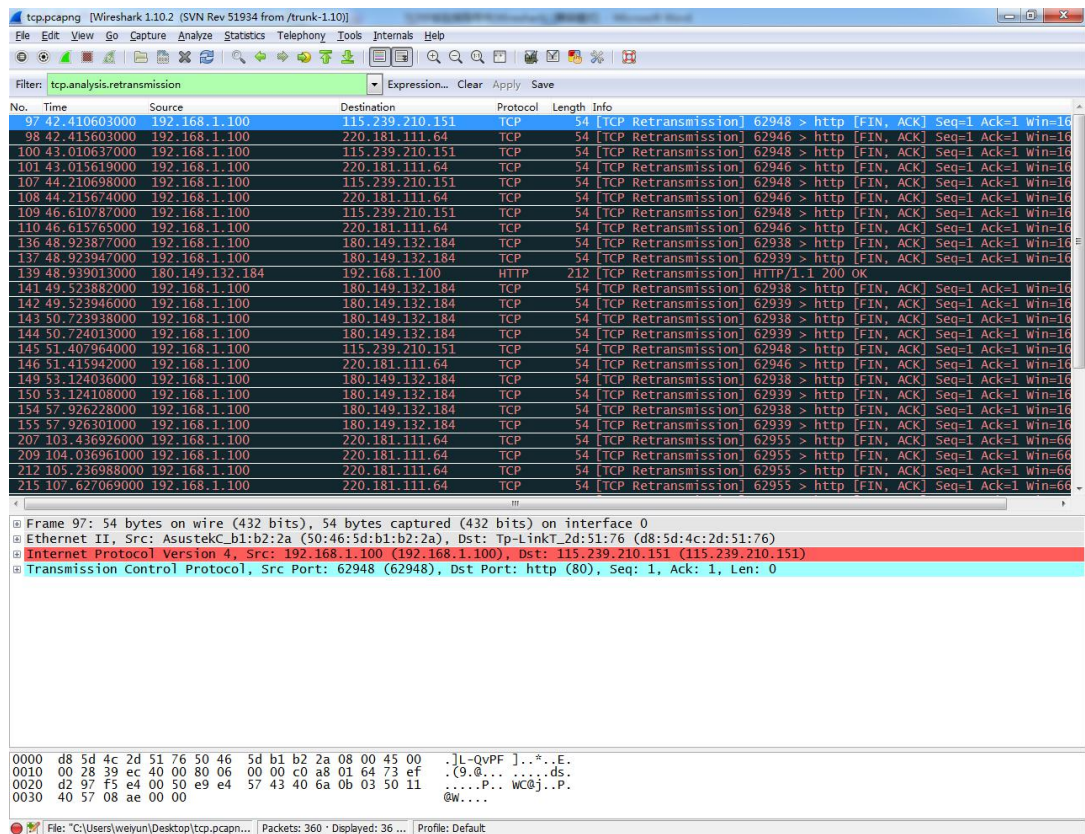


图 6

3.2 通过观察分组的序号、确认号的变化，研究重传行为。

五、实验报告要求

按实验报告模板撰写实验报告

实验六：HTTP 和 DNS 分析

一、实验目的

分析 HTTP 协议，分析 DNS 协议。

二、实验环境

WIRESHARK

三、实验内容

1. HTTP GET/response 交互
2. HTTP 条件 GET/response 交互
3. 获取长文件
4. 嵌有对象的 HTML 文档
5. HTTP 认证
6. 跟踪 DNS

四、实验步骤

1. HTTP GET/response 交互
 - 1.1 启动 Web browser。
 - 1.2 启动 Wireshark 分组嗅探器。在窗口的显示过滤说明处输入“http”，分组列表子窗口中将只显示所俘获到的 HTTP 报文。
 - 1.3 一分钟以后，开始 Wireshark 分组俘获。

1.4 在打开的 Web browser 窗口中输入一下地址（浏览器中将显示一个只有一行文字的非常简单的 HTML 文件）：

<http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html>

1.5 停止分组俘获，如图 1 所示。

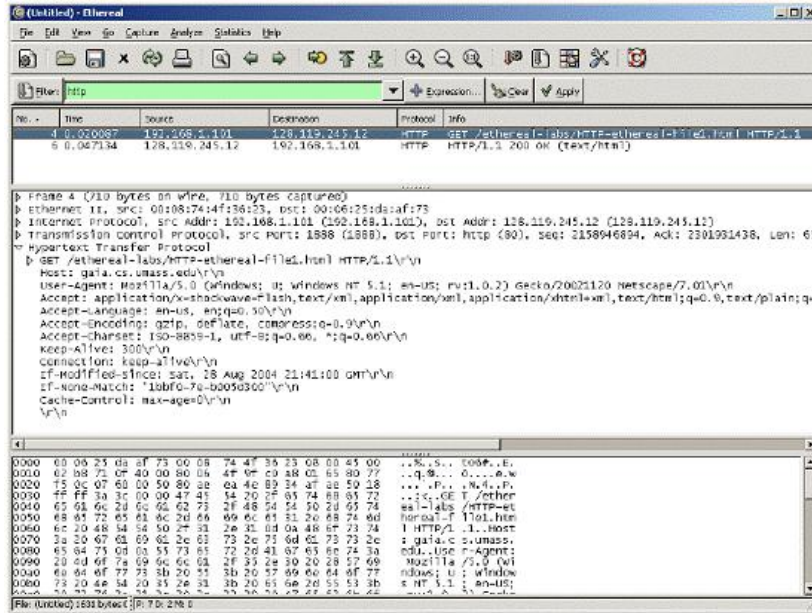


图 1

2. HTTP 条件 GET/response 交互

2.1 启动浏览器，清空浏览器的缓存（在浏览器中，选择“工具”菜单中的“Internet 选项”命令，在出现的对话框中，选择“删除文件”）。

2.2 启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。

2.3 在浏览器的地址栏中输入以下 URL：

<http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file2.html>

你的浏览器中将显示一个具有五行的非常简单的 HTML 文件。

2.4 在你的浏览器中重新输入相同的 URL 或单击浏览器中的“刷新”按钮。

2.5 停止 Wireshark 分组俘获，在显示过滤筛选说明处输入“http”，分组列表子窗口中将只显示所俘获到的 HTTP 报文。

3. 获取长文件

3.1 启动浏览器，将浏览器的缓存清空。

3.2 启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。

3.3 在浏览器的地址栏中输入以下 URL：

`http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file3.html`

3.4 停止 Wireshark 分组俘获，在显示过滤筛选说明处输入“http”，分组列表子窗口中将只显示所俘获到的 HTTP 报文。

4. 嵌有对象的 HTML 文档

4.1 启动浏览器，将浏览器的缓存清空。

4.2 启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。

4.3 在浏览器的地址栏中输入以下 URL：

`http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file4.html`

4.4 停止 Wireshark 分组俘获，在显示过滤筛选说明处输入“http”，分组列表子窗口中将只显示所俘获到的 HTTP 报文。

5. HTTP 认证

5.1 启动浏览器，将浏览器的缓存清空。

5.2 启动 Wireshark 分组俘获器。开始 Wireshark 分组俘获。

5.3 在浏览器的地址栏中输入以下 URL：

`http://gaia.cs.umass.edu/ethereal-labs/protected_pages/HTTP-ethereal-file5.html`

浏览器将显示一个 HTTP 文件，输入所需要的用户名和密码(用户名：`eth-students`，密码：`networks`)。

5.4 停止 Wireshark 分组俘获，在显示过滤筛选说明处输入“`http`”，分组列表子窗口中将只显示所俘获到的 HTTP 报文。

6. 跟踪 DNS

6.1 利用 `ipconfig` 命令清空你的主机上的 DNS 缓存。

6.2 启动浏览器，将浏览器的缓存清空。

6.3 启动 Wireshark 分组俘获器，在显示过滤筛选说明处输入“`ip.addr==your_IP_address`”（如：`ip.addr==10.17.7.23`）。

6.4 开始 Wireshark 分组俘获。

6.5 在浏览器的地址栏中输入：`http://www.ietf.org`

6.6 停止分组俘获。

6.7 开始 Wireshark 分组俘获。

6.8 在 `www.mit.edu` 上进行 `nslookup`（即执行命令：`nslookup www.mit.edu`）。

6.9 停止分组俘获。

6.10 重复上面的实验，只是将命令替换为：`nslookup www.aait.or.kr bitsy.mit.edu`

五、实验报告要求

按实验报告模板撰写实验报告

实验 七 利用 Ethereal 分析 ARP 协议

一、实验目的

利用 Ethereal 捕获发生在 ping 过程中的 ARP 报文，加强对 ARP 协议的理解，掌握 ARP 报文格式，掌握 ARP 请求报文和应答报文的区别。

二、实验环境

Ethereal

三、实验内容

1. 利用 Ethereal 捕获分组
2. 在捕获分组中分析 ARP 协议

四、实验步骤

1. 利用 Ethereal 捕获分组

1.1 桌面双击 Ethereal，启动 Ethereal，如图 1 所示：

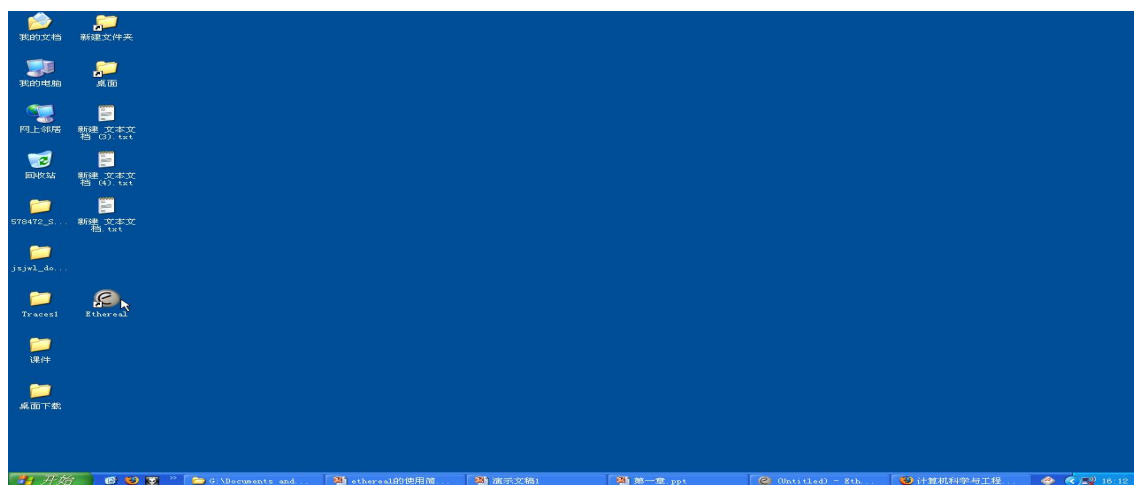


图 1

1.2 对 Capture Options 各个选项进行设置，如图 2 所示：

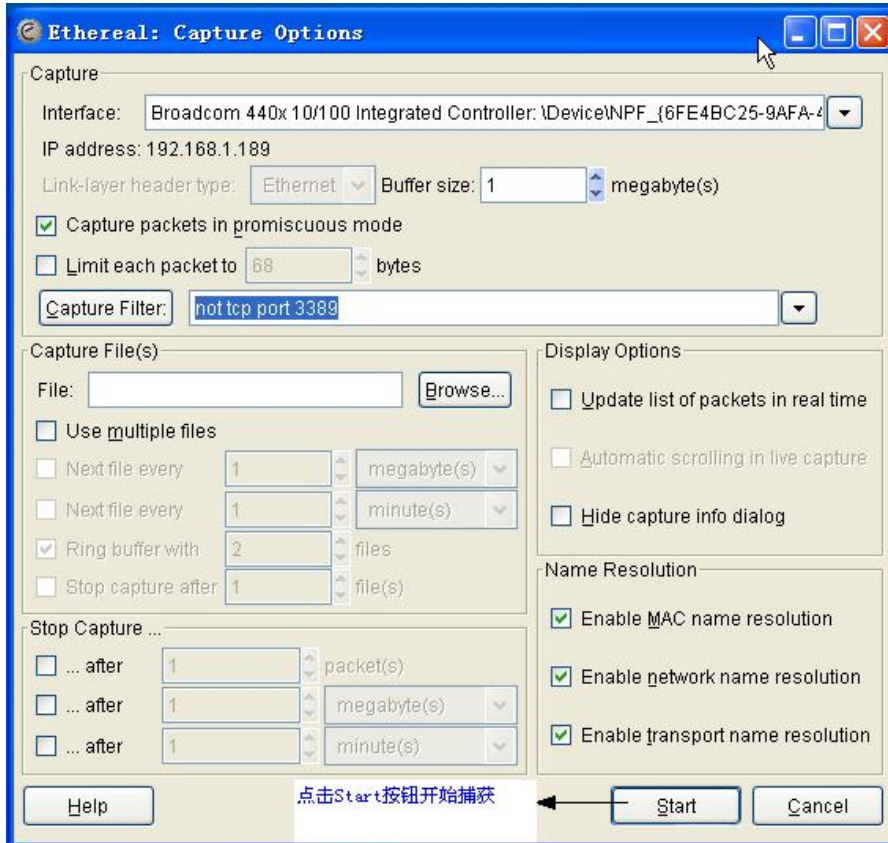


图 2

1.3 点击 Start 按钮开始捕获分组，出现 Capture from... 对话框，如图 3 所示

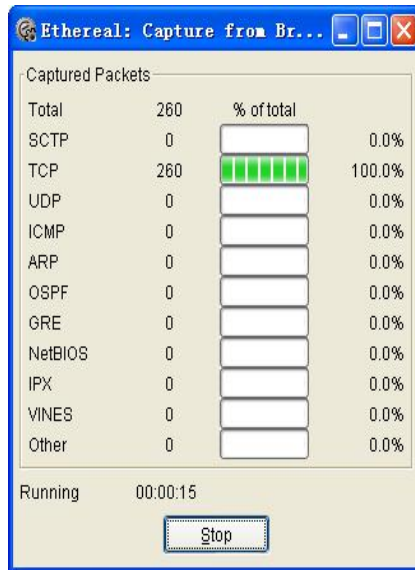


图 3

1.4 点击 Capture from... 对话框中 Stop 按钮结束捕获，如图 4 所示。

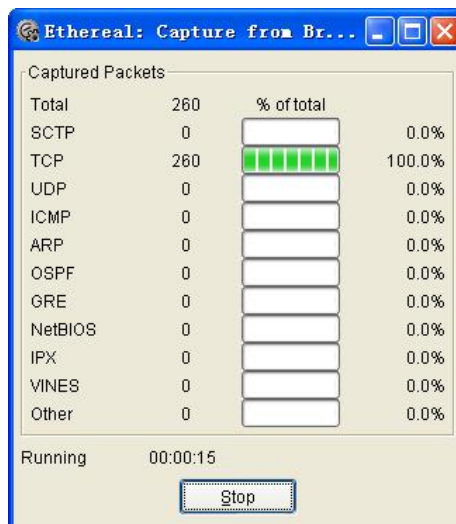


图 4

1.5 得到捕获记录，如图 5 所示。

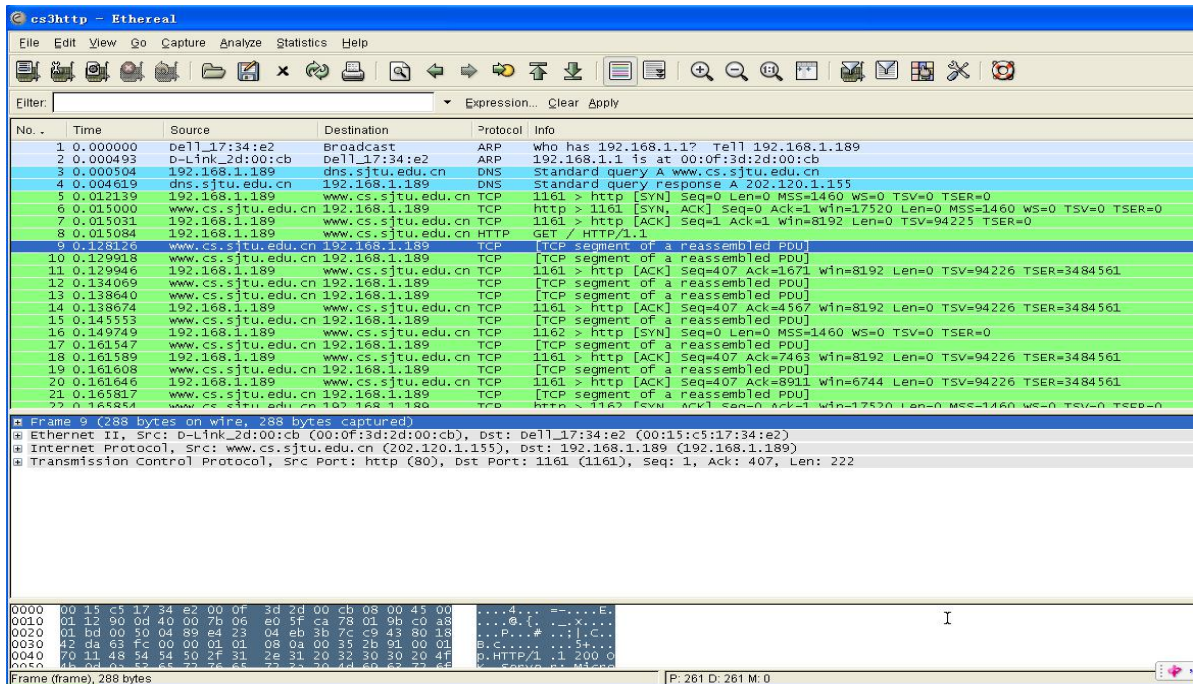


图 5

2. 在捕获分组中分析 ARP 协议

2.1 利用 Summary 观察跟踪记录的统计概要, 包括通信的总字节数, 通信的频率, 分组的大小等统计数据。如图 6 所示。

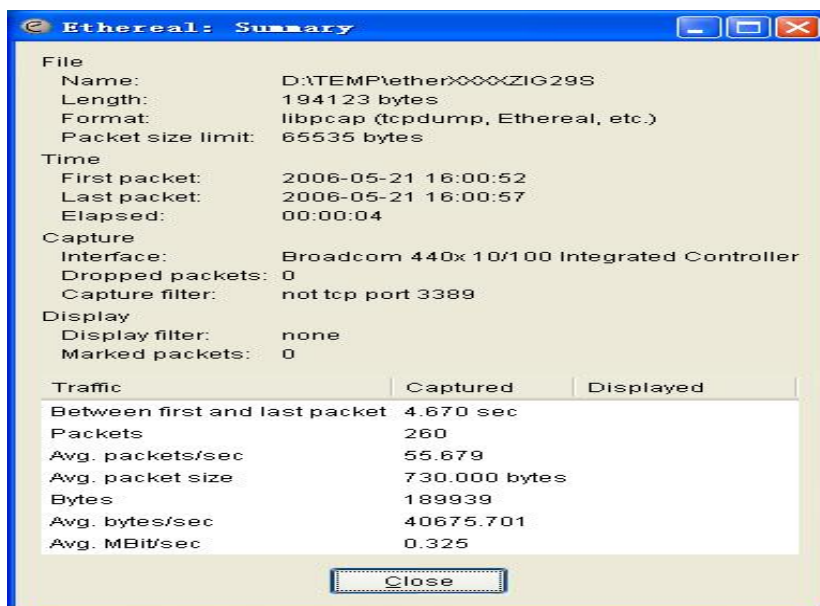
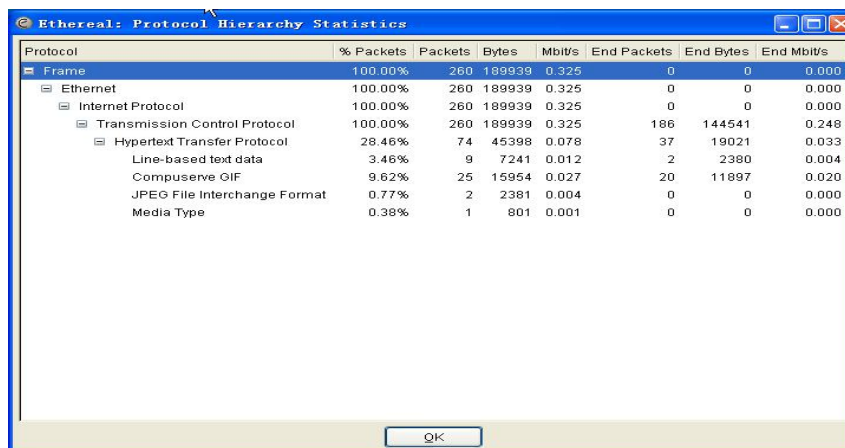


图 6

2.2 利用 Statistics 菜单分析记录，如图 7 所示。



The screenshot shows a window titled "Ethereal: Protocol Hierarchy Statistics". It contains a table with the following data:

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	260	189939	0.325	0	0	0.000
Ethernet	100.00%	260	189939	0.325	0	0	0.000
Internet Protocol	100.00%	260	189939	0.325	0	0	0.000
Transmission Control Protocol	100.00%	260	189939	0.325	186	144541	0.248
Hypertext Transfer Protocol	28.46%	74	45398	0.078	37	19021	0.033
Line-based text data	3.46%	9	7241	0.012	2	2380	0.004
CompuServe GIF	9.62%	25	15954	0.027	20	11897	0.020
JPEG File Interchange Format	0.77%	2	2381	0.004	0	0	0.000
Media Type	0.38%	1	801	0.001	0	0	0.000

图 7

五、实验报告要求：

按实验报告模板撰写实验报告

实验 八 利用 Ethereal 分析 HTTP 协议

一、实验目的

利用 Ethereal 捕获一次网页打开的过程，通过观察整个网页获得全过程，加强对 HTTP 协议的理解，通过观察捕获分组分析和理解 HTTP 协议细节和格式。

二、实验环境

Ethereal

三、实验内容

1. 利用 Ethereal 捕获分组
2. 分析捕获分组中 HTTP 协议细节

四、实验步骤

1. 利用 Ethereal 捕获分组

1.1 桌面双击 Ethereal，启动 Ethereal，如图 1 所示：

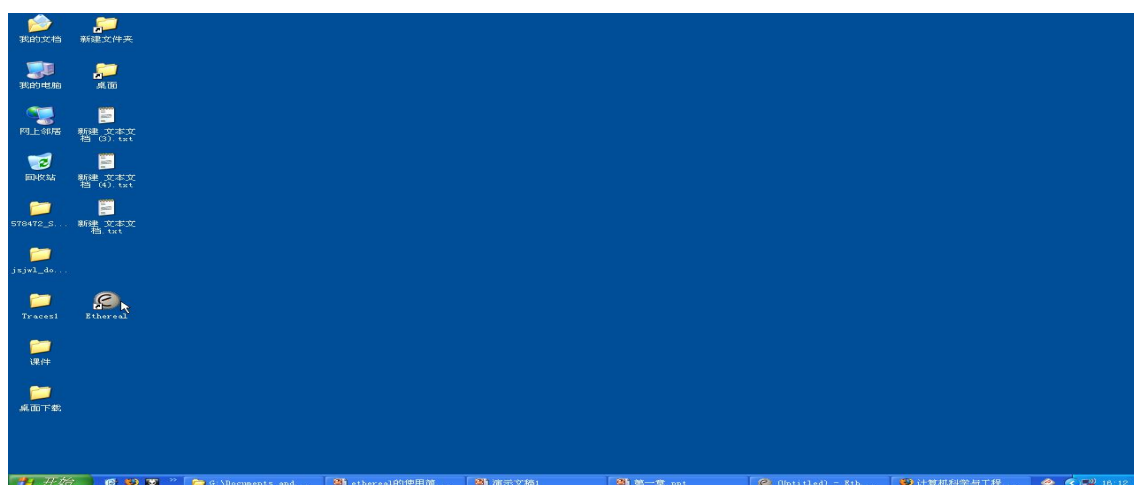
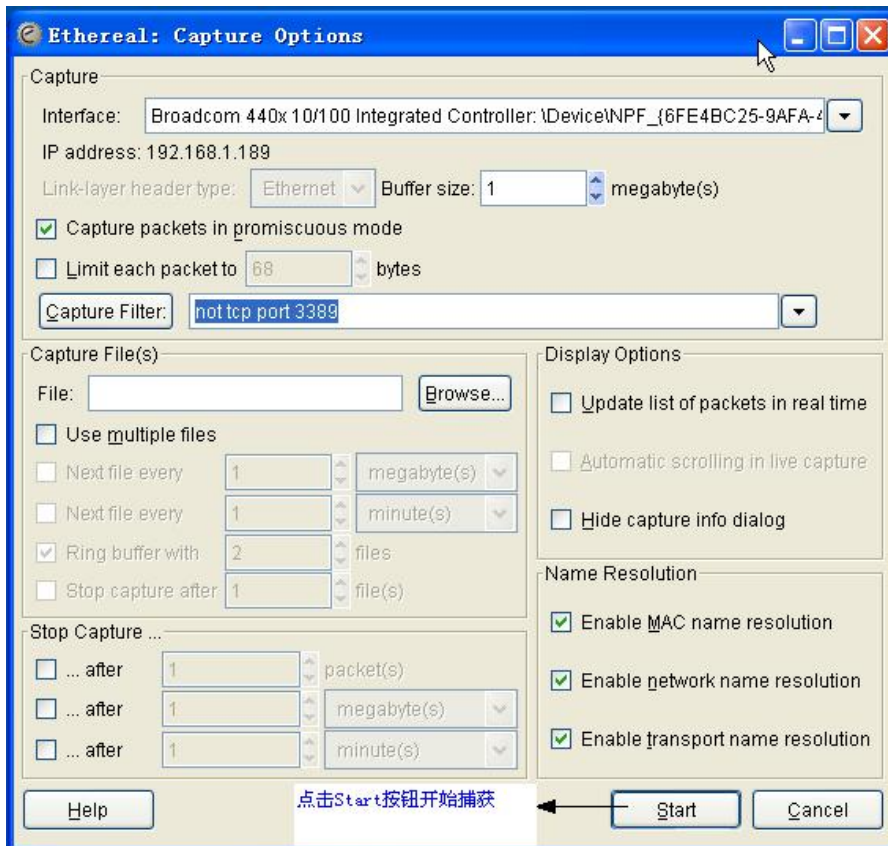


图 1

1.2 对 Capture Options 各个选项进行设置，如图 2 所示：



1.3 点击 Start 按钮开始捕获分组，出现 Capture from... 对话框，如图 3 所示

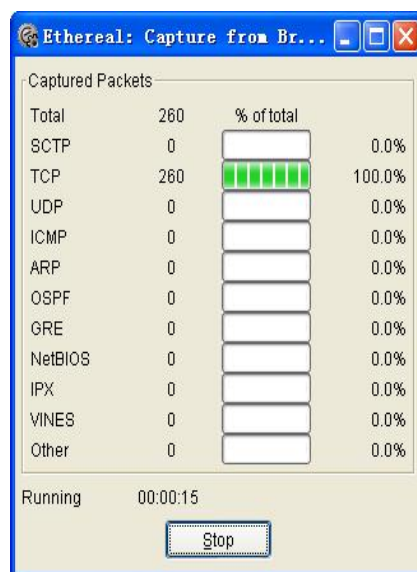


图 3
41 / 43

1.4 点击 Capture from... 对话框中 Stop 按钮结束捕获，如图 4 所示。

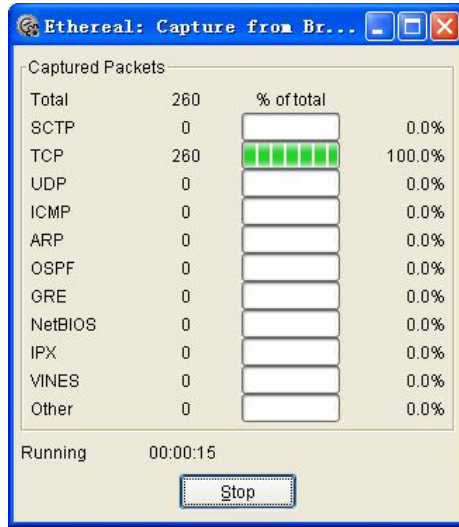


图 4

1.5 得到捕获记录，如图 5 所示。

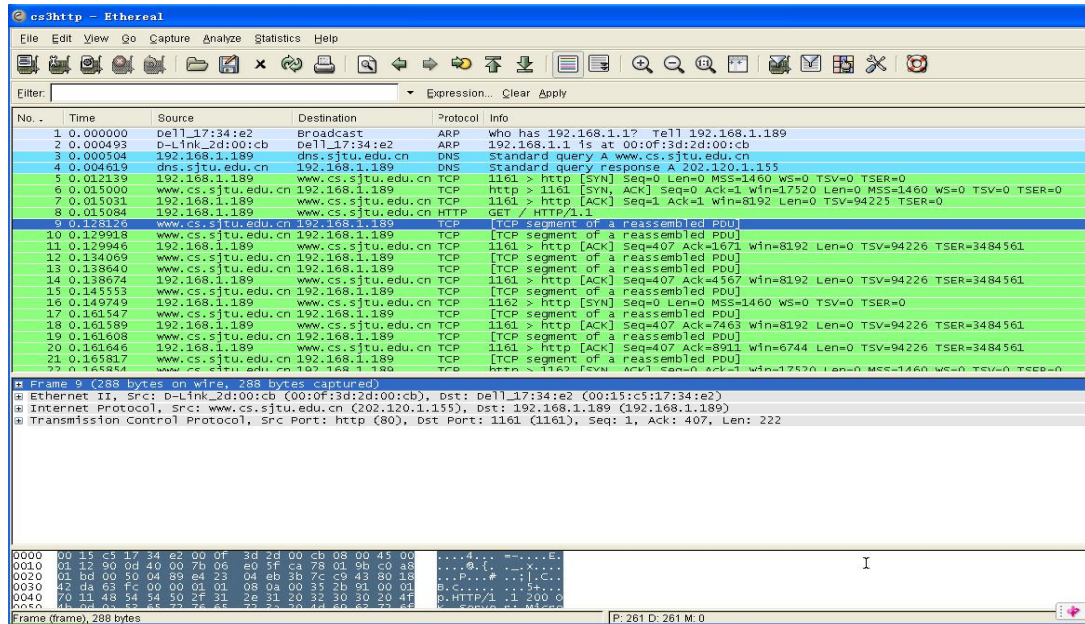


图 5

2. 分析捕获分组中 HTTP 协议细节

2.1 利用 Analyze 菜单 Summary 分析记录。如图 6 所示。



图 6

2.2 利用 Protocol Hierarchy Statistics (协议层次统计) 观察各个协议的统计。如图 7 所示。

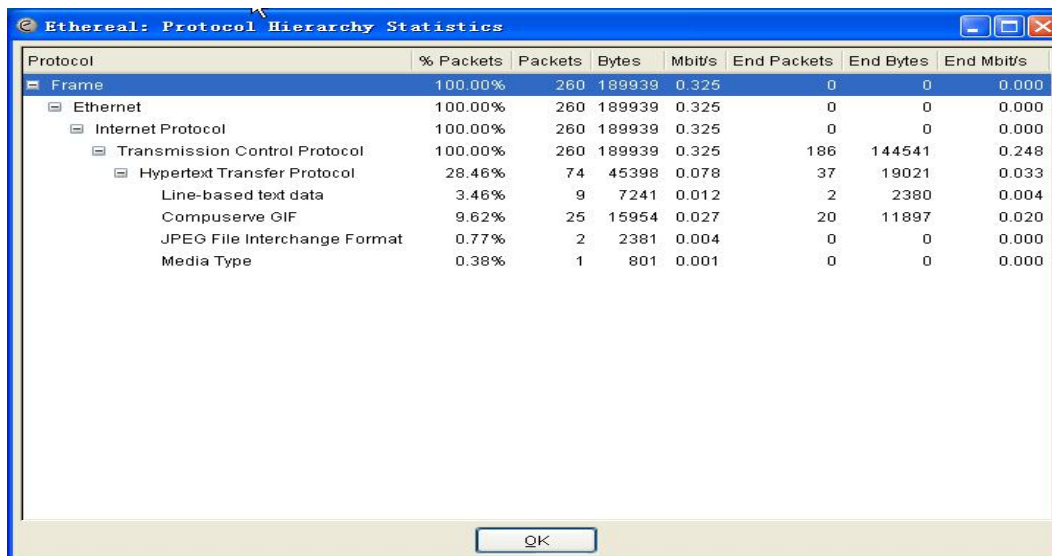


图 7

五、实验报告要求:

按实验报告模板撰写实验报告