# 实验二：《网络监听工具的安装使用》

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **课 程** | 计算机网络基础 | **实验项目** | 《网络监听工具的安装使用》 | **成 绩** |  |
| **专业班级** | **软件工程1702** | **指导教师** | 刘传林 |
| **姓 名** | **李文毅** | 学 号 | 201731062208 |

**一、基本信息**

项目编码：07011111 项目学时：2

项目类型：综合 项目属性：必修

大纲执笔：陈雁 大纲审批：计算机科学学院学术委员会 主管院长：王杨

**二、实验目的**

掌握网络监听工具ethereal的基本使用，并了解如何捕获数据报进行分析

**三、教学要求**

1. 安装使用网络监听工具ethereal；
2. 使用ethereal网络分析器对局域网的数据包进行识别、分析。

**四、主要仪器设备**

Windows 2000以上操作系统，可上Internet网络的计算机若干，ethereal安装包

**五、考核方式及要求**

实验报告

**六、主要内容**

本次实验需在小组合作的基础之上完成。每个小组由两位成员组成，相互之间通信，通过网络监听工具截取通信数据包，分析数据包完成实验内容。

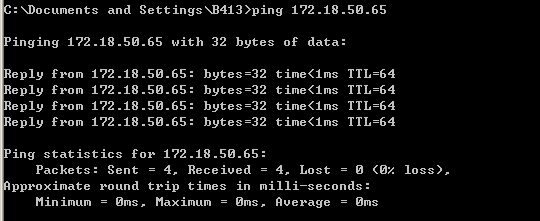
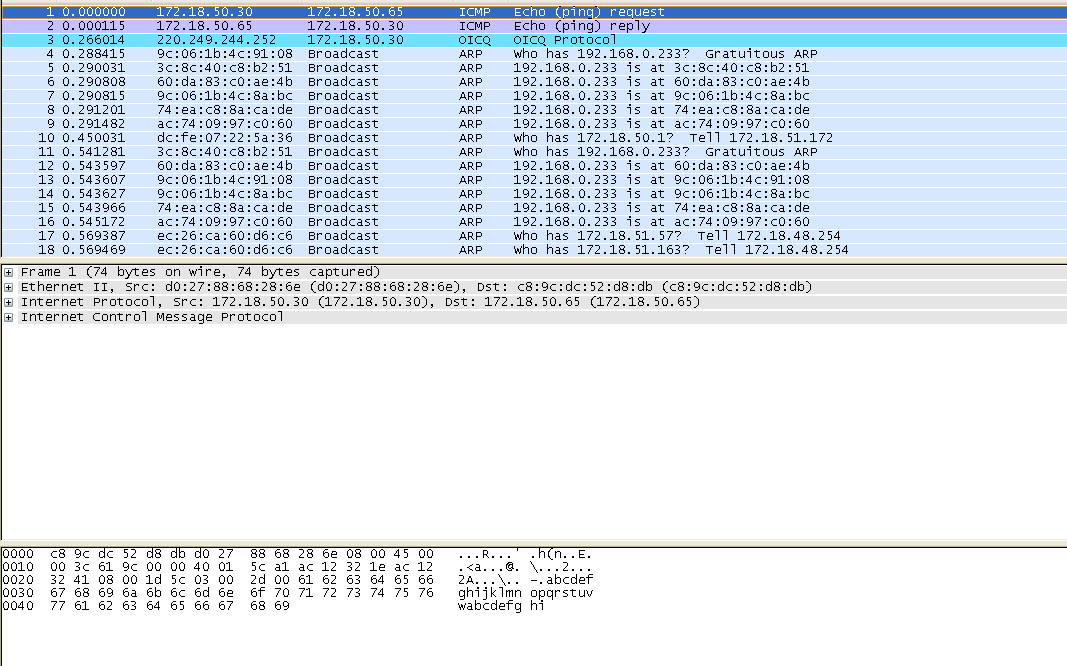
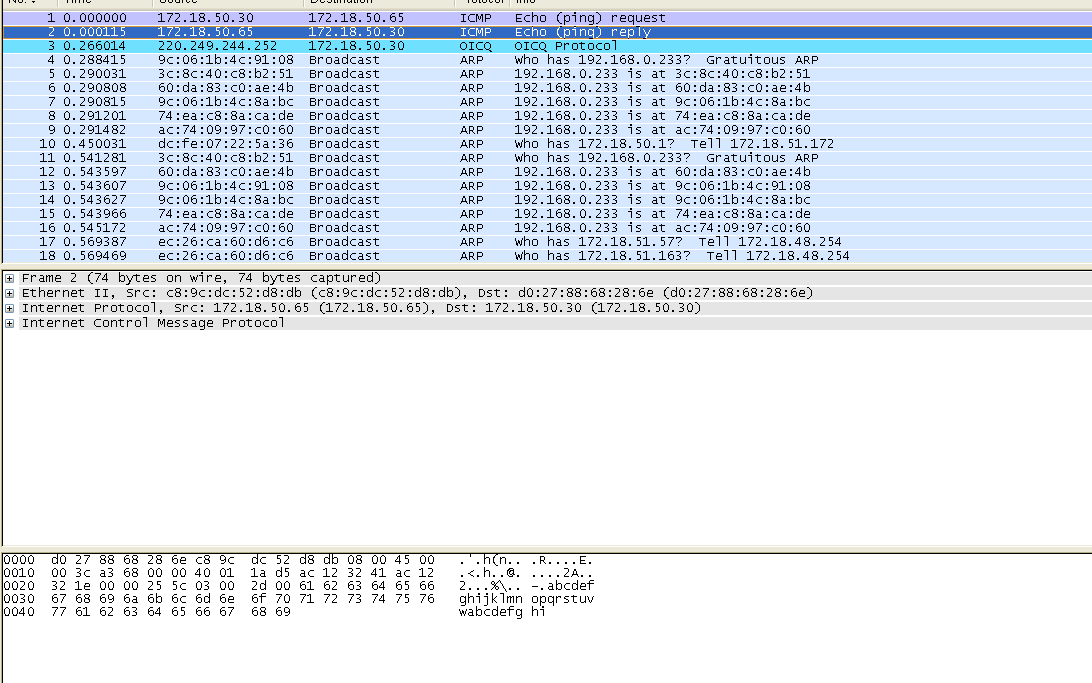
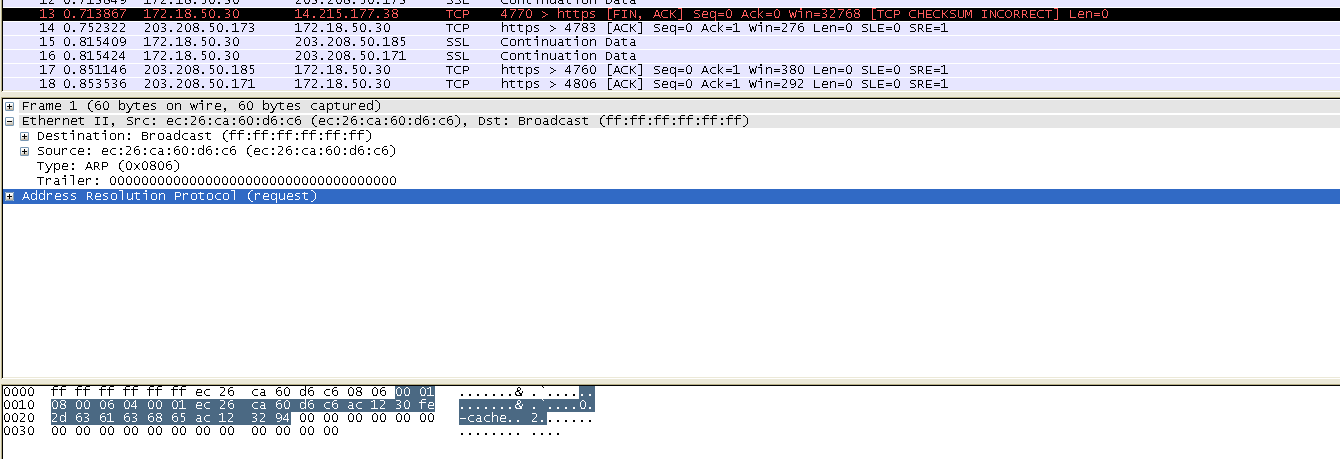
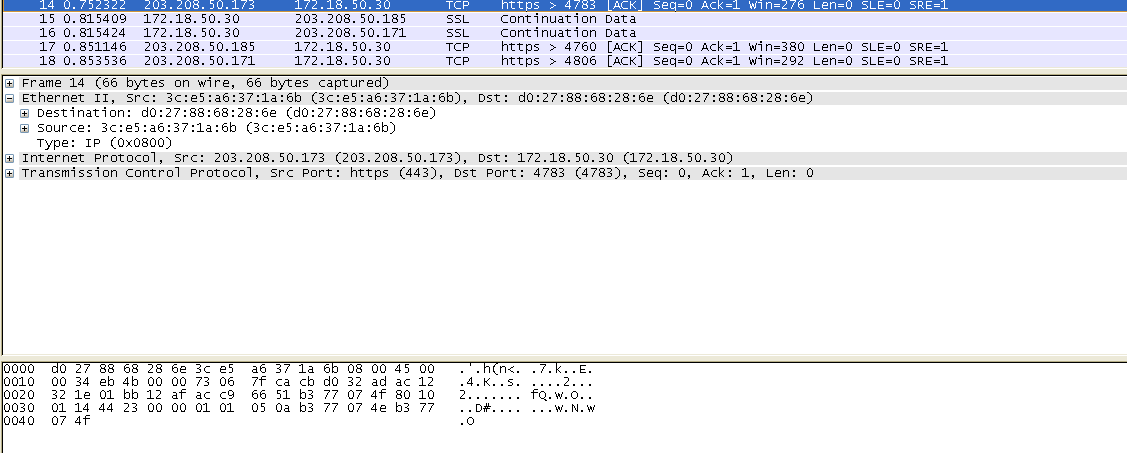
小组情况表:

|  |  |  |
| --- | --- | --- |
| 小组成员姓名 | 成员机器IP地址 | 本机IP地址 |
| 李文毅 | 172.18.50.65 | 172.18.50.30 |
| 刘豪 | 172.18.50.30 | 172.18.50.65 |

1. 通过ipconfig命令获取本机IP地址,并填写上面的小组情况表。
2. 下载网络监听工具ethereal和winpcap并安装；

（1）首先安装winpcap；

（2）安装ethereal。

1. 从本机ping小组另一位成员的计算机，使用ethereal截取ping过程中的通信数据。
2. 
3. 
4. 
5. 
6. 
7. 分析截取的由于第3步操作而从本机发送到目的机的数据帧中的IP数据报并填写下表。

|  |  |
| --- | --- |
| IP协议版本号 | IPV4 |
| 服务类型 | Dscp |
| IP报文头长度 | 20 |
| 数据报总长度 | 60 |
| 标识 | 0x619d |
| 数据报是否要求分段 | no |
| 分段偏移量 | no |
| 在发送过程中经过几个路由器 | 0 |
| 上层协议名称 | icmp |
| 报文头校验和 | 0x5ca0 |
| 源地址 | 172.18.50.30 |
| 目标地址 | 172.18.50.65 |

1. 分析截取的由于第3步操作而从目的机返回到本机的数据帧中的IP数据报并填写下表。

|  |  |
| --- | --- |
| IP协议版本号 | IPV4 |
| 服务类型 | dscp |
| IP报文头长度 | 20 |
| 数据报总长度 | 60 |
| 标识 | 0xbffd |
| 数据报是否要求分段 | No |
| 分段偏移量 | No |
| 在返回过程中经过几个路由器 | 0 |
| 上层协议名称 | Icmp |
| 报文头校验和 | 0xfe3f |
| 源地址 | 172.18.50.65 |
| 目标地址 | 172.18.50.30 |

1. 从本机通过ethereal截取http通信过程中的通信数据，然后填写下表。

先启动ethereal抓包，然后访问任意Http服务器，使用截取操作中的通信数据。

分析截取的由于第6步操作而从本机发送到目的机的数据帧中的TCP数据报并填写下表。

|  |  |
| --- | --- |
| 数据发送端口号 | 4770(4770) |
| 通信目标端口号 | https(443) |
| TCP报文序号 | 0 |
| TCP报文确认号 | 0 |
| 下一个TCP报文序号 | 0 |
| 标志位含义（如“确认序号有效”） | no |
| 窗口大小 | 32768 |
| 校验和 | 0x9e48 |
| 源IP地址 | 172.18.50.30 |
| 目标IP地址 | 14.215.177.38 |

1. 分析截取的由于第6步操作而从目的机返回到本机的数据帧中的TCP数据报并 填写下表。

|  |  |
| --- | --- |
| 数据发送端口号 | https(443) |
| 通信目标端口号 | 4783(4783) |
| TCP报文序号 | 0 |
| TCP报文确认号 | 1 |
| 下一个TCP报文序号 | 0 |
| 标志位含义（如“确认序号有效”） | no |
| 窗口大小 | 276 |
| 校验和 | 0x4423 |
| 源IP地址 | 14.215.177.38 |
| 目标IP地址 | 172.18.50.30 |