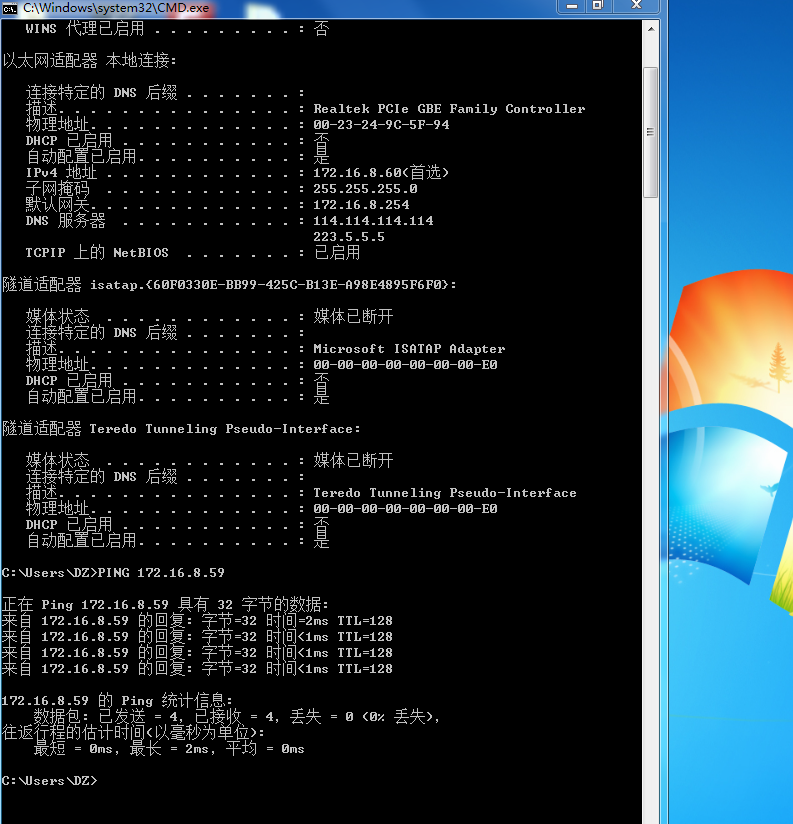
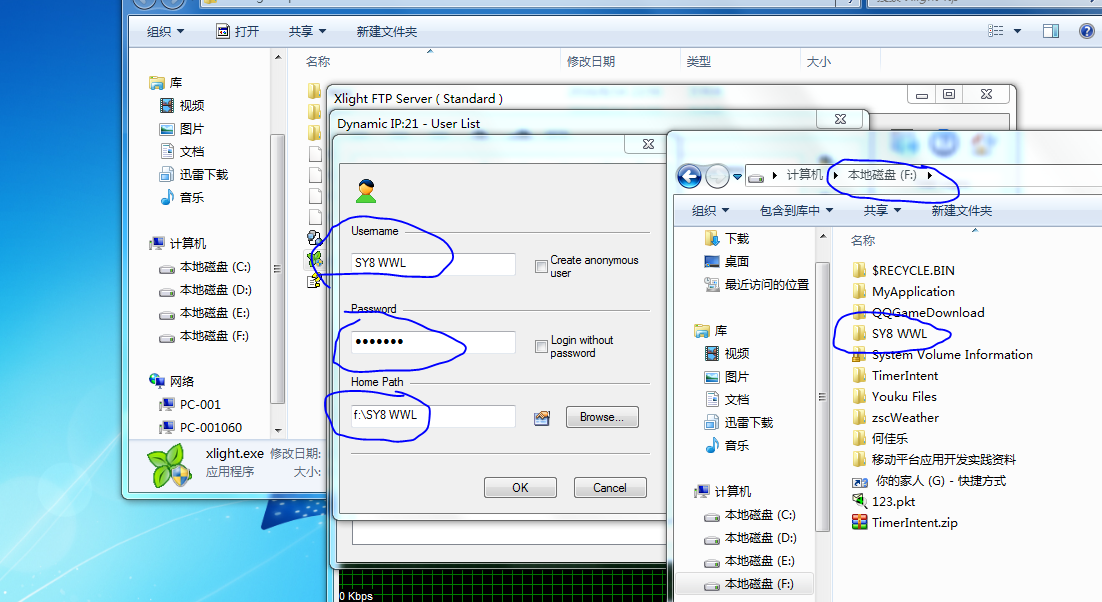
首先在对IP协议和FTP协议以及ICMP协议有了一些基础的了解之后，就是该通过科莱软件来抓包来验证一些IP包和FTP包，ICMP包的组成内容，字段等，把课上的知识得到验证，具体实验步骤如下：

1. 先确定两台主机之间是否通信成功通过PING命令来实现：对于172.16.8.59和172.16.8.60主机

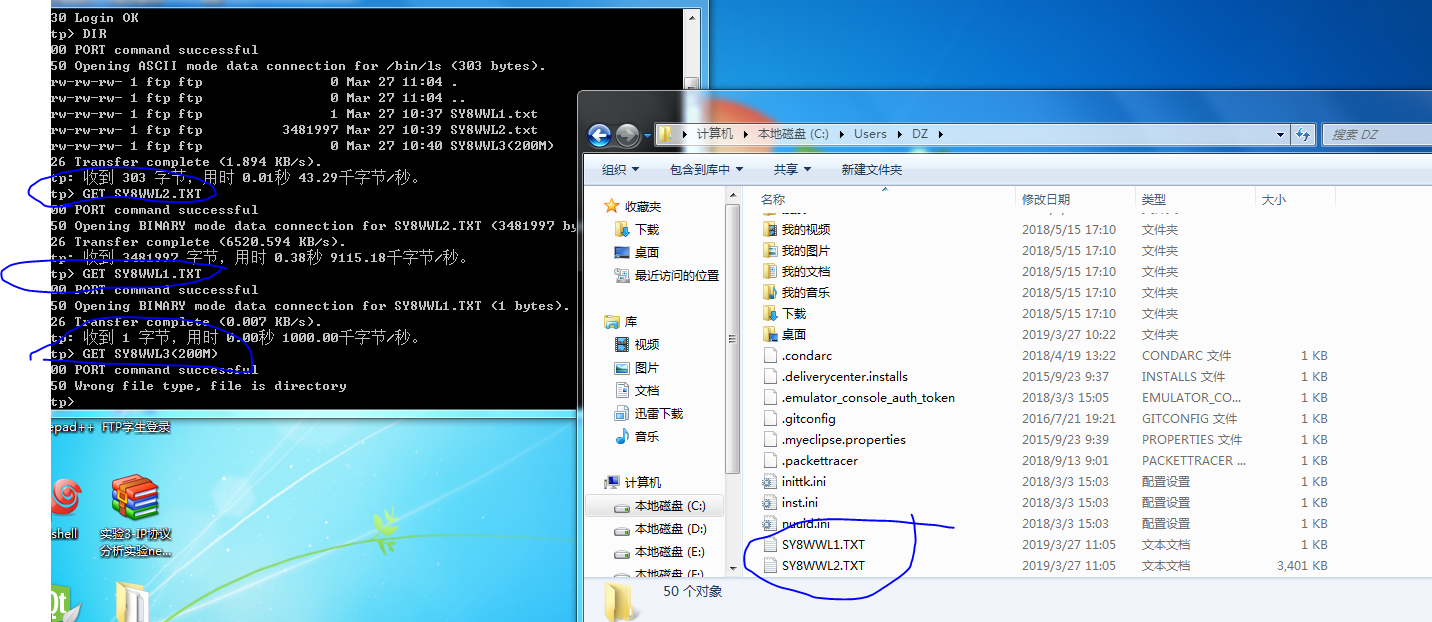


1. 确定了两台主机之间可以通信之后就安装对应的FTP和抓包软件：FTP以172.16.8.59为模仿服务器端：建立：SY8WWL及包含的内容：

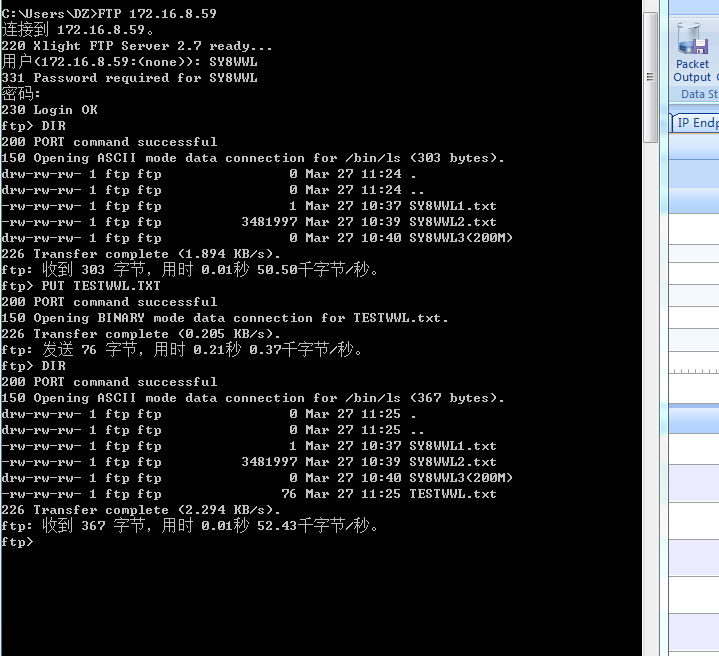


1. 打开两台主机的抓包软件设置好参数：IP和FTP包，运行，之后开始抓包：在确认抓到包之后查看：基本掌握GET,PUT,DIR,QUIT等用法

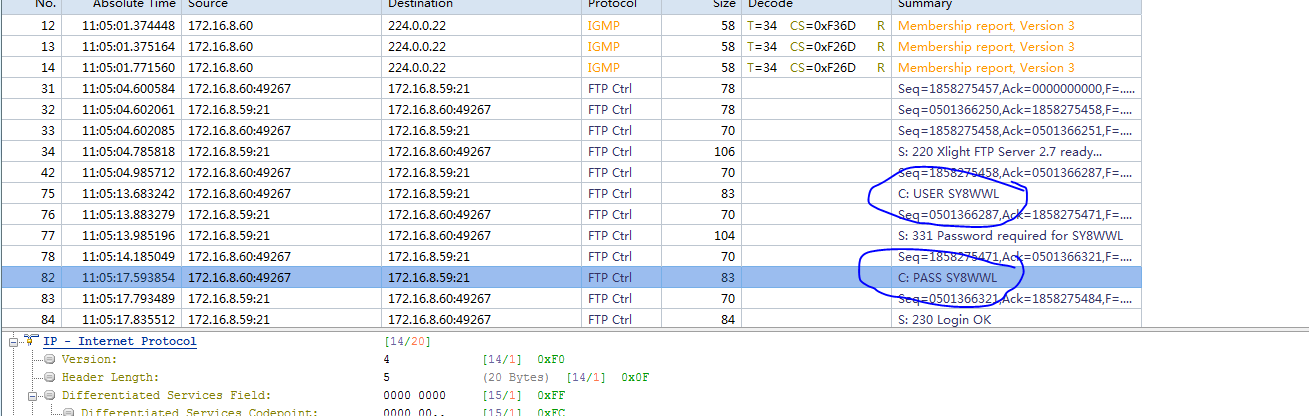
如图，下载了SY8WWL1.TXT(几百字节)和SY8WWL2.TXT(大小为3.几K)



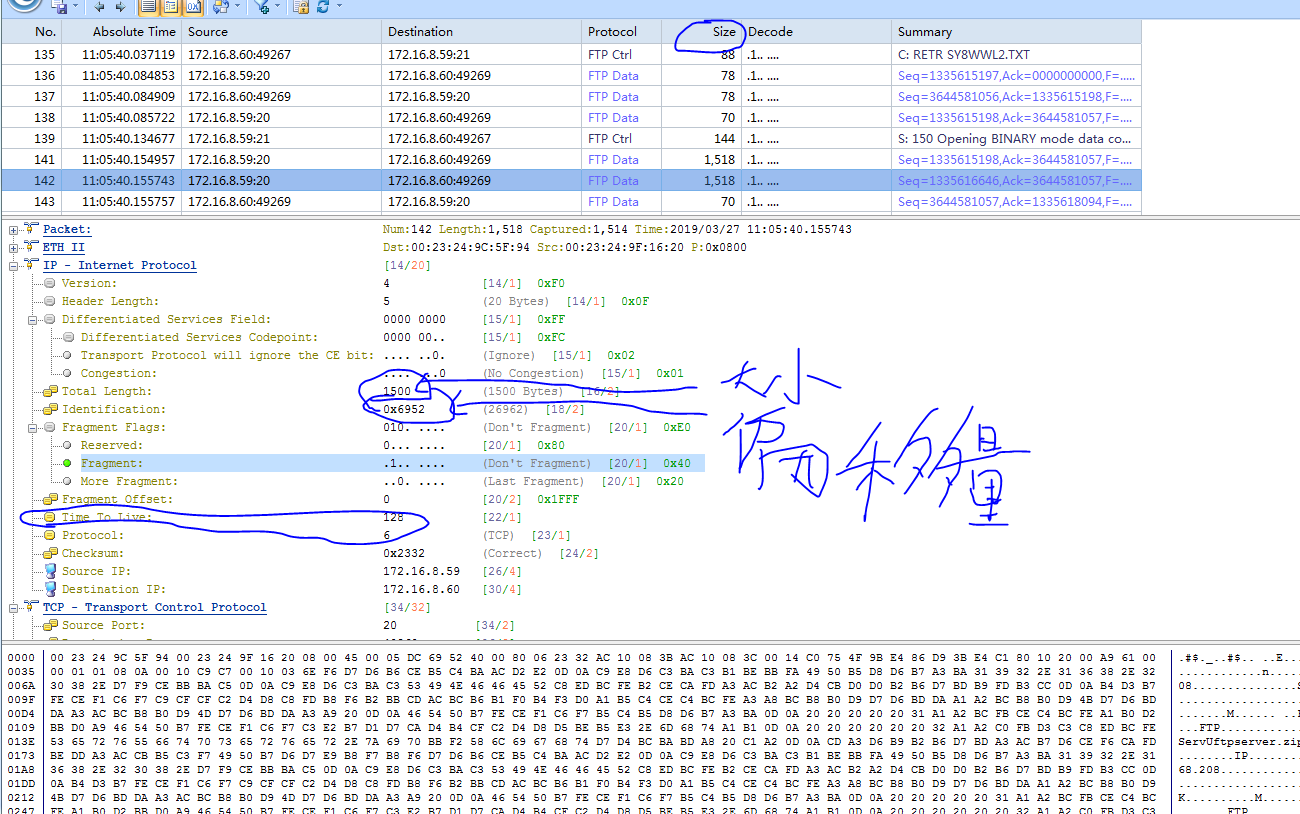
对于上传：上传了TESTWWL.TXT文件：



1. 之后开始查看抓到了什么包：1.由于是通过不可靠传输，所以可以看到用户名和密码：（都是SY8WWL）

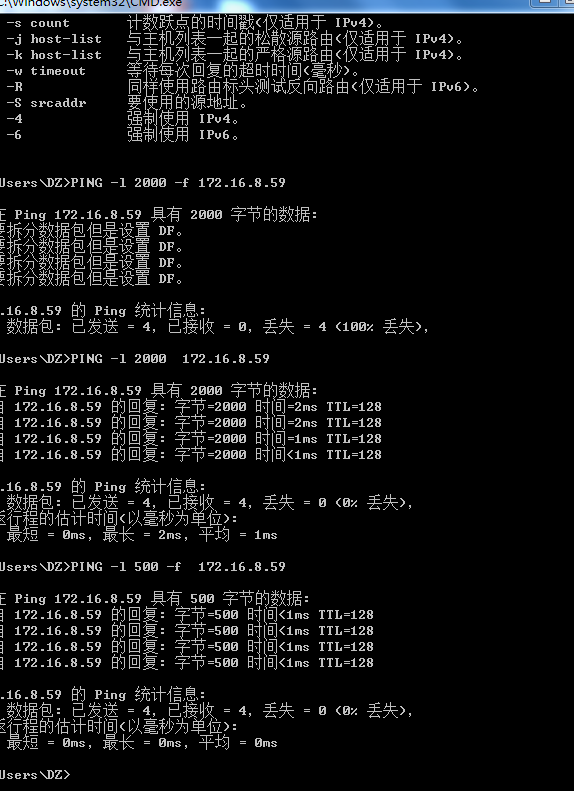


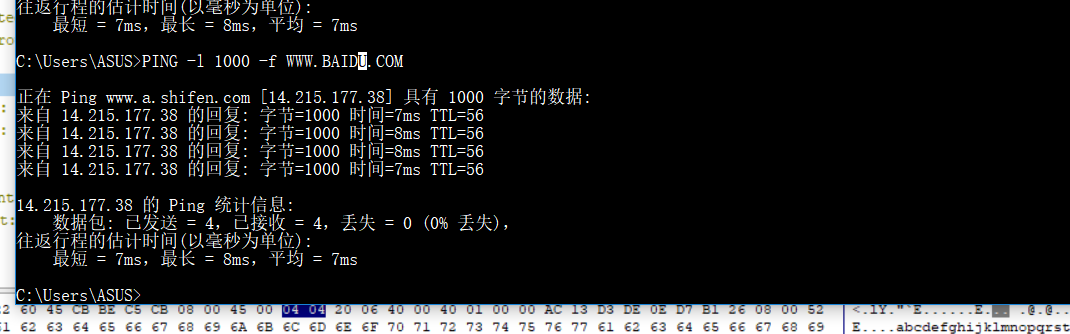
2.对于数据报文字段，有如下参数：版本号（4），头部长度（20BYE=4+4+4+4+4），服务类型(00000000)，总长度（1500），标识（0\*6952后面的为0\*6953），标志（010），分片位移（0也许是第一个….），生存时间（128），协议（6tcp），首部校验和（0\*2332），源IP（172.16.8.59）,目的 IP（172.16.8.60）



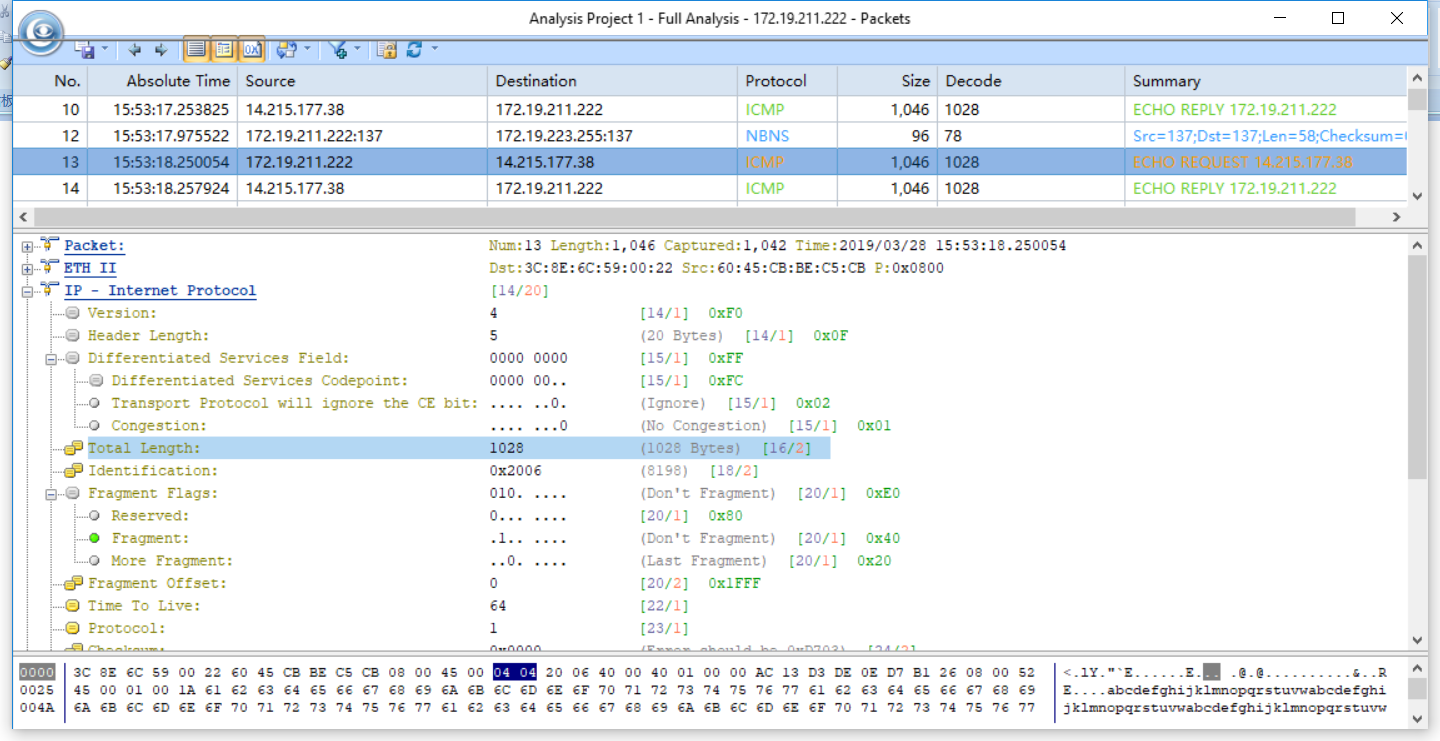
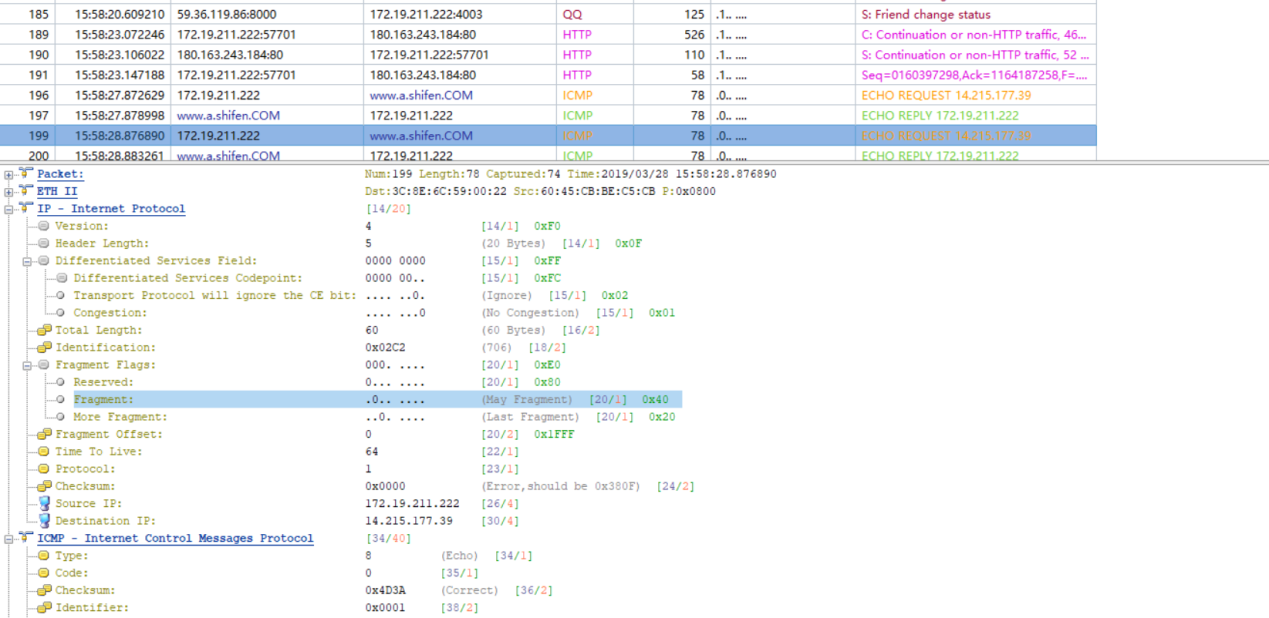
对于PING包：可以优化PING命令：-L表示字段长度 -F表示不分段，即一整段一起发送

,





在接收到包之后可以进行分析：如果不分段，对于数据部分，为1028，标志字段为：（010）即不分段，且为最后一个（也许，不确定…）

 如图，这里标志字段为：（000）即分段，且为最后一个（也许，不确定…）

通过这次实验，总体了解了IP包，ICMP,FTP包的内部结构，把书本上的知识得到了验证，收获较大。同时小组的学习模式也使得几个同学一起进步。