厦門大學

信息学院软件工程系

《计算机网络》实验报告

题　　目 实验四　观察 TCP 报文段并侦听分析 FTP 协议

姓　　名 杨浩然

学　　号 24320182203309

班　　级 软件工程 2018 级 2 班

实验时间 2020 年 3 月 26 日

2020 年 3 月 26 日

1 实验目的

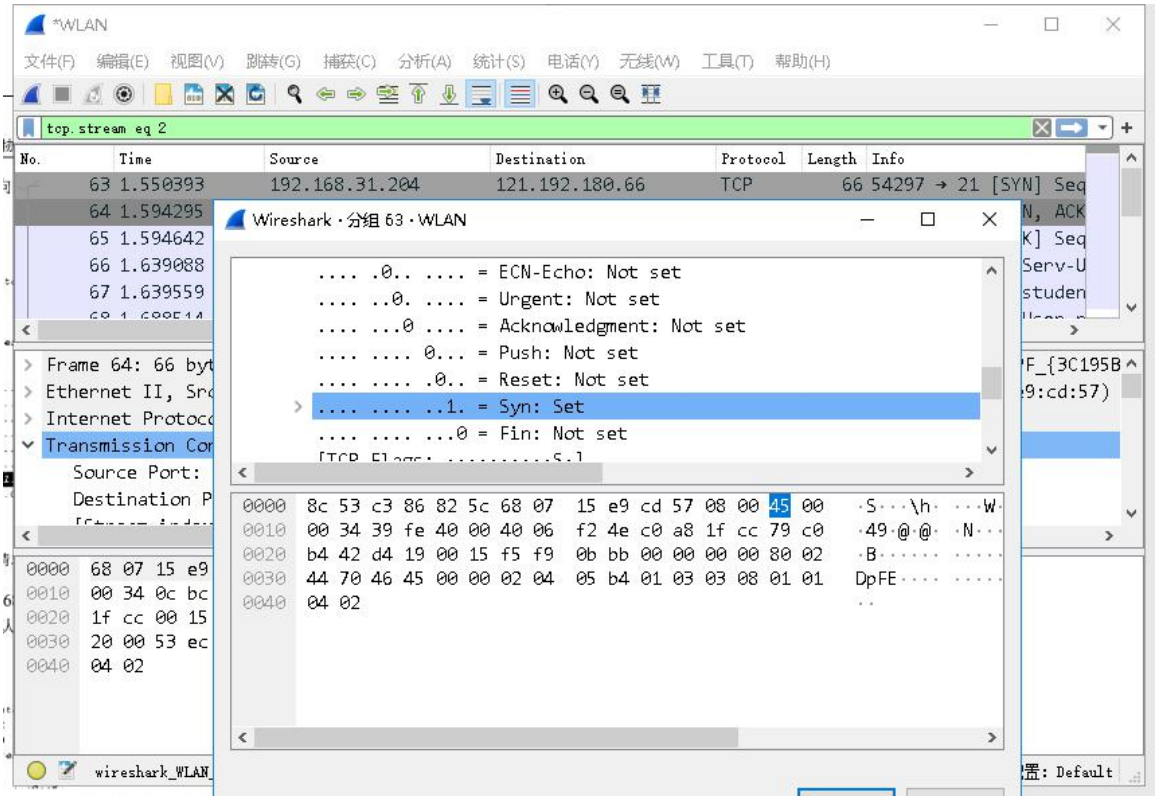
用 Wireshark 侦听并观察 TCP 数据段。观察其建立和撤除连接的过程，观察段 ID、 窗口机制和拥塞控制机制等。将该过程截图在报告中。
用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特征，再总结出提取用户名密码的有效方法。基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

2 实验环境

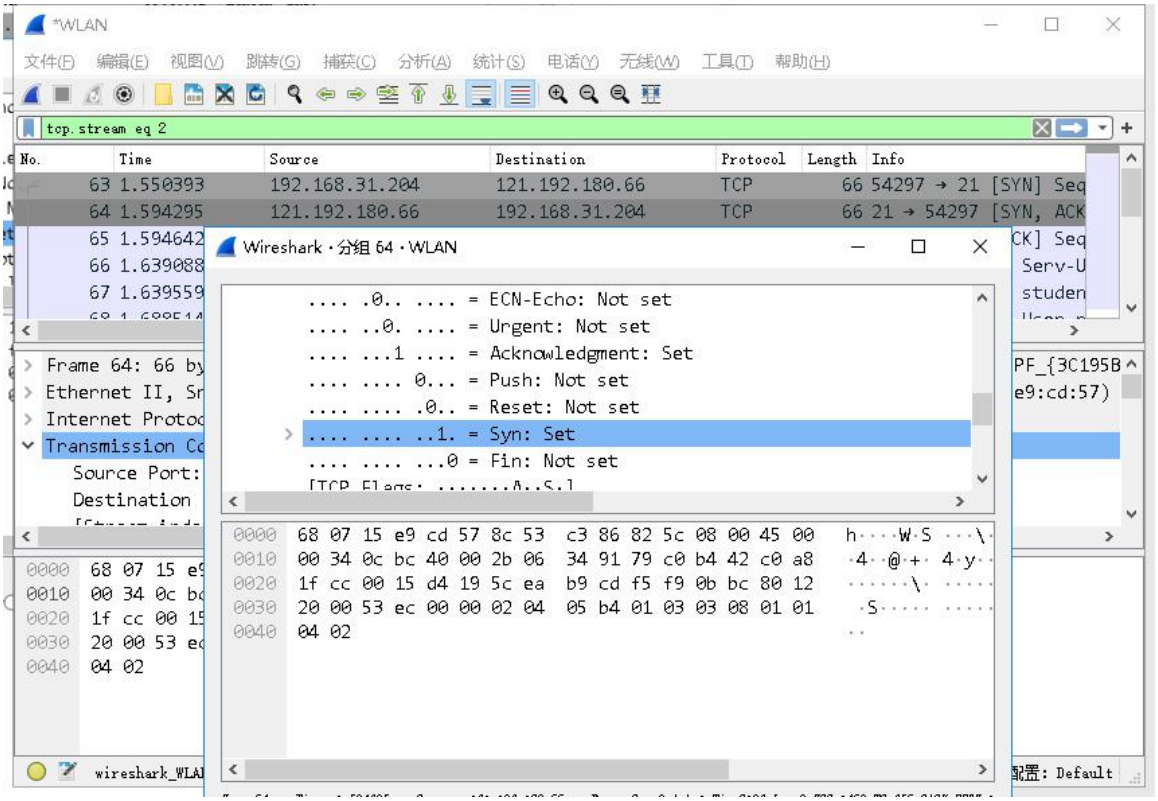
Win10，C++。

3 实验结果

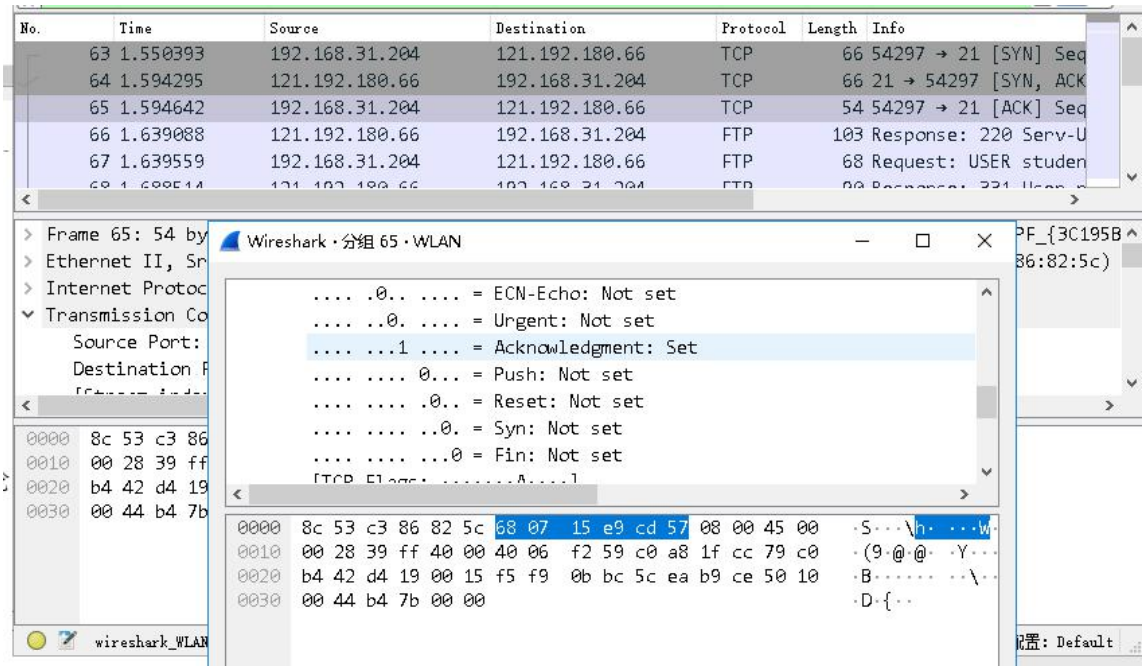
第一个数据包是本机 192.168.31.204 向 FTP 发送连接请求，标志位中只有 Syn



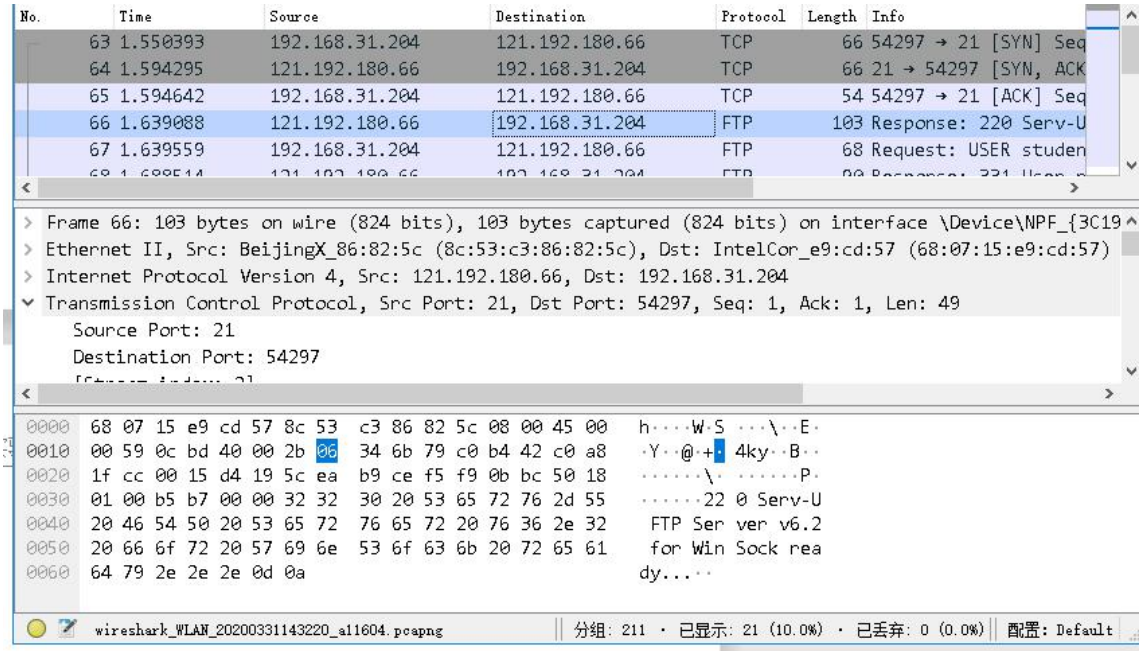
第二个数据包是 FTP 服务器发来的握手信号，里面有同步位和确认位



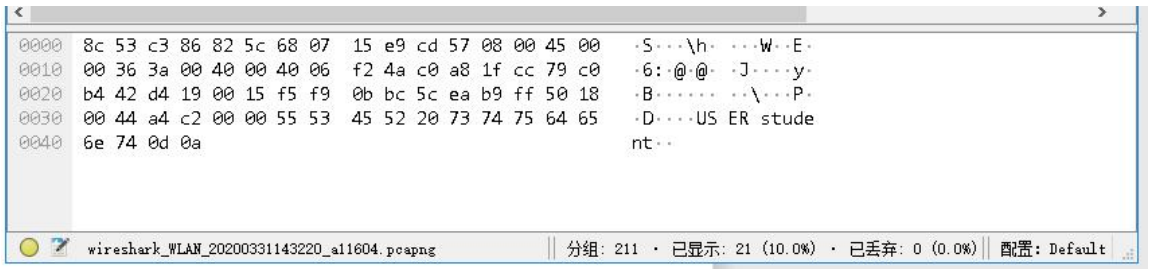
第三个数据包是本机发出的，里面只有一个确认位，也就是做再次确认



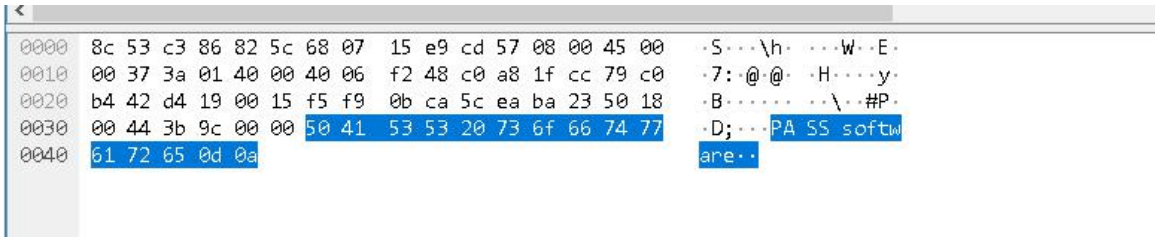
第四个数据包是 FTP 服务器发来的欢迎语句



第五个数据包中含用户名



第七个数据包中含密码



如果登陆成功则以 230 开头

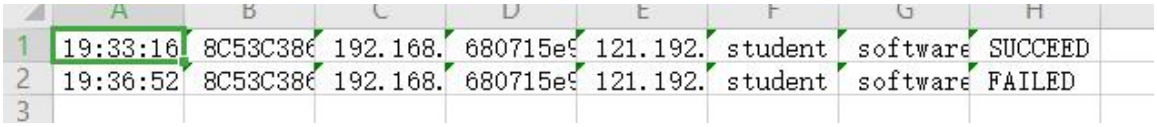
找到用户名及密码前分别有 USER 和 PASS，通过遍历每个包的内容进行筛选

```
//形同特征则输出文件
for (int i = 0; i < length; i++) {
    if (pkt_data[i] == 85 && pkt_data[i + 1] == 83 && pkt_data[i + 2] == 69 && pkt_data[i + 3] == 82) {
        fprintf(fp, "%s, ", timestr);
        for (int i = 0; i < 6; i++) {
            fprintf(fp,"%02X ", mh->src_addr[i]);
        }
        fprintf(fp, ", ");
        for (int i = 0; i < 4; i++) {
            fprintf(fp,"%d.", ih->saddr[i]);
        }
        fprintf(fp, ", ");
        for (int i = 0; i < 6; i++) {
            fprintf(fp,"%02X ", mh->dest_addr[i]);
        }
        fprintf(fp, ", ");
        for (int i = 0; i < 4; i++) {
            fprintf(fp,"%d.", ih->daddr[i]);
        }
        fprintf(fp, ", ");
        for (int j = i + 4; pkt_data[j] != 13; j++)fputc(pkt_data[j],fp);
        fprintf(fp, ", ");
        fclose(fp);
    }
    else if (pkt_data[i] == 80 && pkt_data[i + 1] == 65 && pkt_data[i + 2] == 83 && pkt_data[i + 3] == 83) {
        FILE *fp1 = fopen("user.csv", "a");
        for (int j = i + 4; pkt_data[j] != 13; j++)fputc(pkt_data[j], fp);
        fprintf(fp1, ", ");
        fclose(fp1);
    }
    else if (pkt_data[i] == 50 && pkt_data[i + 1] == 51 && pkt_data[i + 2] == 48) {
```

出现 230 则成功登入，530 则失败登入。以数据 ASCLL 码值对应

```
else if (pkt_data[i] == 50 && pkt_data[i + 1] == 51 && pkt_data[i + 2] == 48) {
    FILE *fp2 = fopen("user.csv", "a");
    fprintf(fp2, "SUCCEED ");
    fclose(fp2);
}
else if (pkt_data[i] == 53 && pkt_data[i + 1] == 51 && pkt_data[i + 2] == 48) {
    FILE *fp2 = fopen("user.csv", "a");
    fprintf(fp2, "FAILED ");
    fclose(fp2);
}
```

得到结果



	A	B	C	D	E	F	G	H
1	19:33:16	8C53C386	192.168.	680715e9	121.192.	student	software	SUCCEED
2	19:36:52	8C53C386	192.168.	680715e9	121.192.	student	software	FAILED
3								

4 实验总结

TCP 建立过程分为三次握手，第一次是客户端发起连接，客户端 TCP 发送一个 Syn 同步记号，申请和服务器连接。

第二次是服务器确认了客户端的 Syn，发送 Acknowledgement 记号和一个 Syn 同步记号。

第三次是客户端确认服务器的 Ack 和 Syn 记号，向服务器发送 Ack，成功建立连接。

每次传输的 TCP 数据包中格式都如版本号 4 位，数据包头部长度 4 位，服务类型 8 位，总长 16 位，重组标识 16 位等。最后才是用户数据。