# 网络流量分析（高级）实验结果提交

**【验证实验1】**

当Peter的气象数据接收器回复正常工作之后，我们又对气象数据接收器与服务器之间的通信进行了一次数据包捕获工作，捕获到的数据包保存在weather\_working.pcapng文件中，请分析该数据包，并将气象数据接收器与服务器通信时的用户ID和用户口令提取出来并截图证明之。

**【验证实验-2】**

启动Wiresshark工具，对你访问某一个网站的数据交互进行捕获。对捕获的网络数据包进行分析，并回答下列问题：

1）你的计算机配置的默认网关是什么？请截图证明之；

2）你的计算机配置的DNS服务器是什么？请截图证明之；

3）你访问的网站的IP地址是什么？请截图证明之。

**【验证实验-3】**

1. 安装Serv-U，这是一个FTP服务器软件。安装过程中注意配置相应的目录、用户名、口令等信息，其他参数可采用默认参数，不必修改，安装完成之后启动FTP服务器。
2. 两位同学为一组，A同学使用浏览器作为FTP客户端（地址栏中输入：ftp://B同学的地址）访问B同学的FTP服务器并上传一个文件。此时，B同学开启Wireshark捕获网络数据包，从数据包中提取A同学上传的文件，查看并显示该文件。截图说明从捕获数据包中提取图片文件的过程。A、B同学角色互换，重复上述操作。

**【验证实验-4】**

使用Wireshark打开捕获文件***arppoison.pcap***，对数据包进行分析，回答下列问题：

1）从捕获的数据包分析，被攻击的主机MAC地址是什么？

2）攻击发生在什么时候呢？那几个数据包是攻击的关键数据包？请说明攻击关键数据包的序号。

3）正常情况下，被攻击主机的默认网关的MAC地址是什么？请截图证明之。

4）被攻击之后，被攻击主机认为它的默认网关的MAC地址是什么呢？请截图证明之。

5）这样的攻击，将导致什么样的后果？

**【本次实验的心得、体会、收获或者建议】**