

实验 2 登录数据包分析

一、实验题目

利用 Wireshark 抓取教务系统以及网络教学平台登录数据包进行对比,并依据两个网站的登陆情况,分别回答以下问题:

- 1、TCP 连接的三次握手在哪里?
- 2、你所登陆的系统是否安全?(即是否以明文形式向远程服务器传输账号和密码)
- 3、有余力的同学可尝试抓取诸如微博、邮箱等的登录数据包分析

二、相关知识

TCP 协议

传输控制协议(TCP, Transmission Control Protocol)是一种面向连接的、可靠的、基于字节流的传输层通信协议。

TCP 握手协议

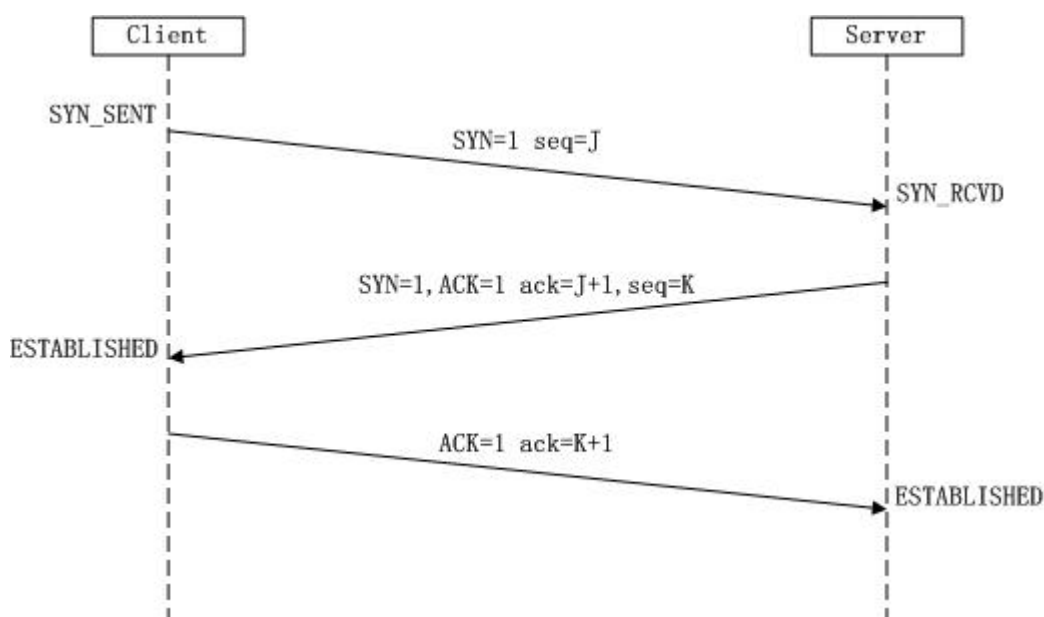
在 TCP/IP 协议中, TCP 协议提供可靠的连接服务,采用三次握手建立一个连接.

第一次握手: 建立连接时,客户端发送 **syn** 包($\text{syn}=j$)到服务器,并进入 SYN_SEND 状态,等待服务器确认;

SYN: 同步序列编号(Synchronize Sequence Numbers)

第二次握手: 服务器收到 syn 包,必须确认客户的 SYN ($\text{ack}=j+1$),同时自己也发送一个 SYN 包($\text{syn}=k$),即 **SYN+ACK** 包,此时服务器进入 SYN_RECV 状态;

第三次握手: 客户端收到服务器的 SYN+ACK 包,向服务器发送确认包 **ACK**($\text{ack}=k+1$),此包发送完毕,客户端和服务器进入 ESTABLISHED 状态,完成三次握手.



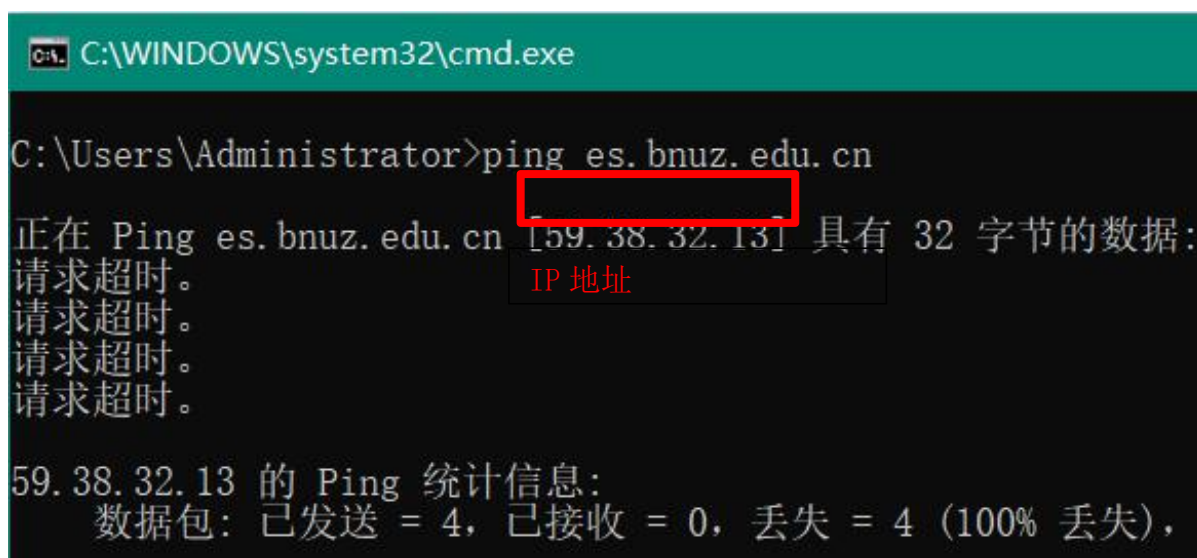
三、实验步骤与结果分析

1. 获取要抓包的 IP 地址（以网络教学平台为例）

①按下 win+r 弹出运行框

②在运行框中输入 cmd 打开命令行窗口

③在命令行窗口中输入 ping 要抓包的地址获取其 IP 地址



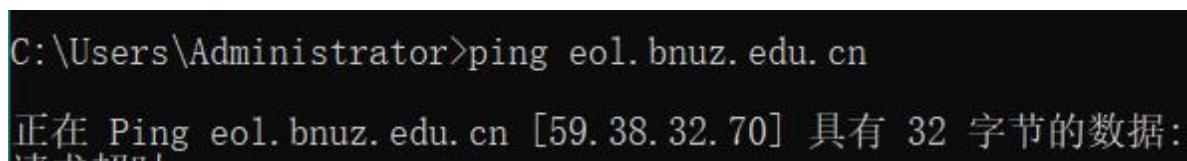
```
C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>ping es.bnuz.edu.cn

正在 Ping es.bnuz.edu.cn [59.38.32.13] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

59.38.32.13 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

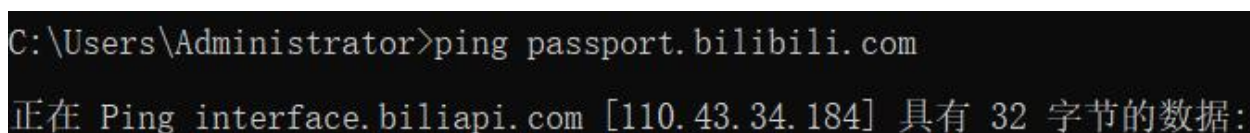
同理得到教学平台的 IP 地址



```
C:\Users\Administrator>ping eol.bnuz.edu.cn

正在 Ping eol.bnuz.edu.cn [59.38.32.70] 具有 32 字节的数据:
请求超时。
```

还有 bilibili 的登录 IP 地址

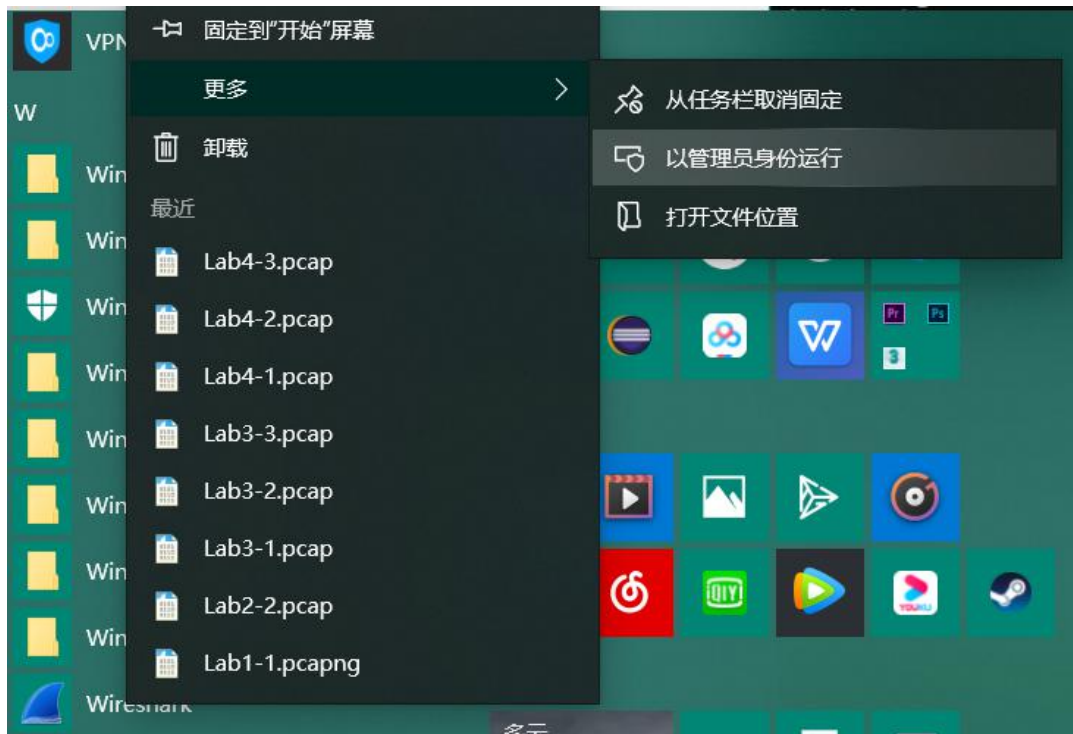


```
C:\Users\Administrator>ping passport.bilibili.com

正在 Ping interface.biliapi.com [110.43.34.184] 具有 32 字节的数据:
请求超时。
```

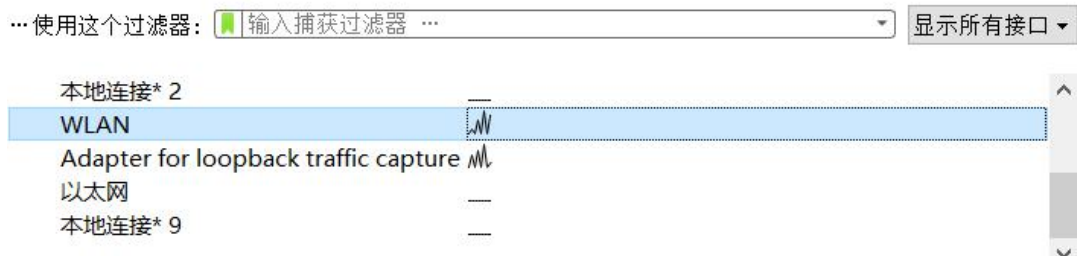
2. 用 Wireshark 进行抓包

①以管理员身份运行 Wireshark



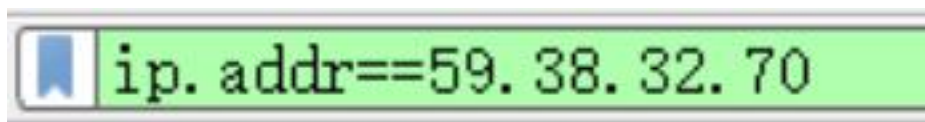
②找到连接线路（我的是无线网络，若连接的是宽带则点击本地连接）

捕获



③登录教学平台和教务系统还有 bilibili 进行抓包

④在筛选器中输入 `ip.addr==你所要抓包的地址` 进行筛选, 然后就可以开始找 TCP 连接三次握手和查看是否以明文形式向远程服务器传输账号和密



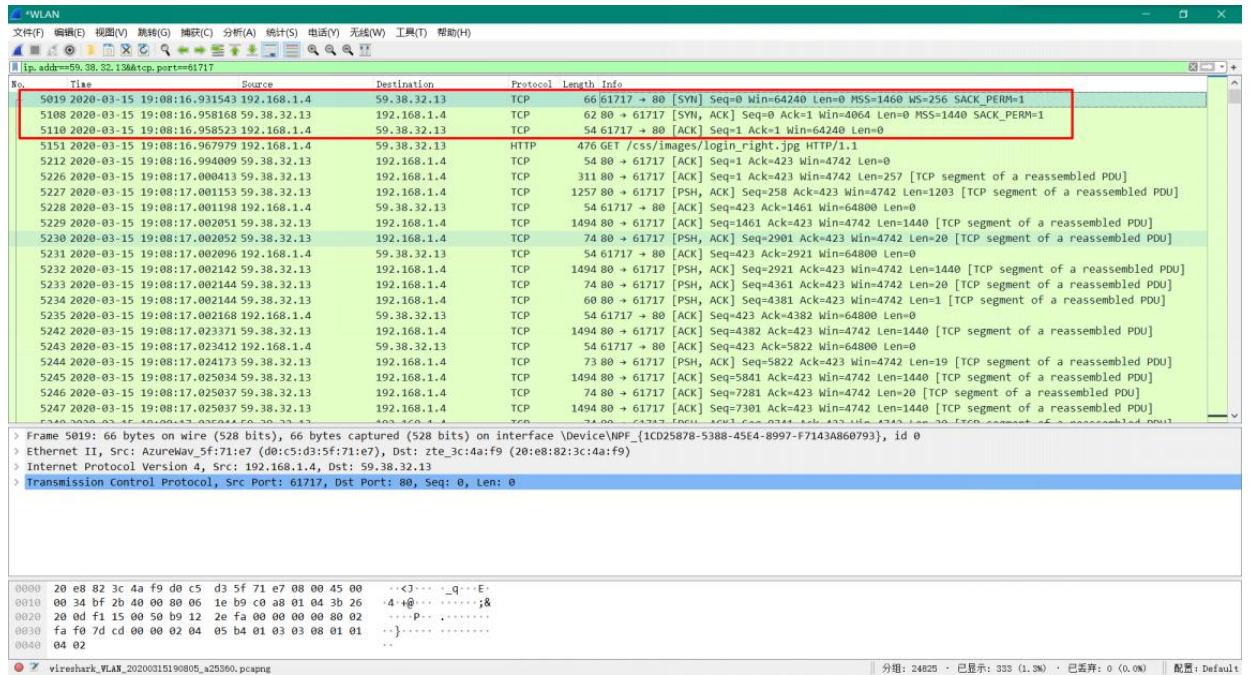
3. TCP 连接三次握手和查看是否以明文形式传输数据在几个网站间的比较

TCP 连接三次握手

教务系统

找到 post 对应的端口号为 61717

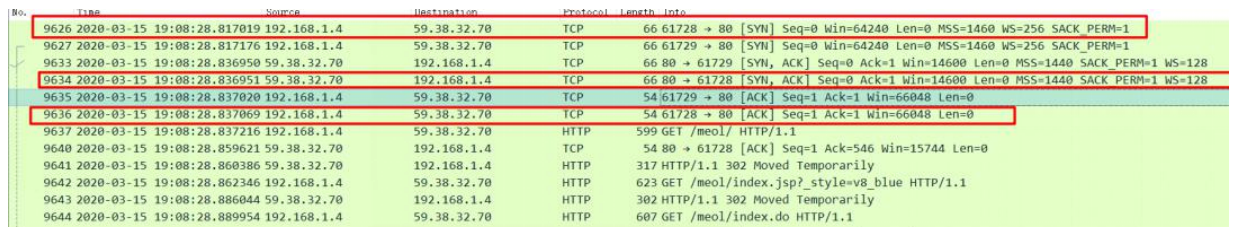
> Transmission Control Protocol, Src Port: 61717, Dst Port: 80, Seq: 423, Ack: 17822, Len: 1118



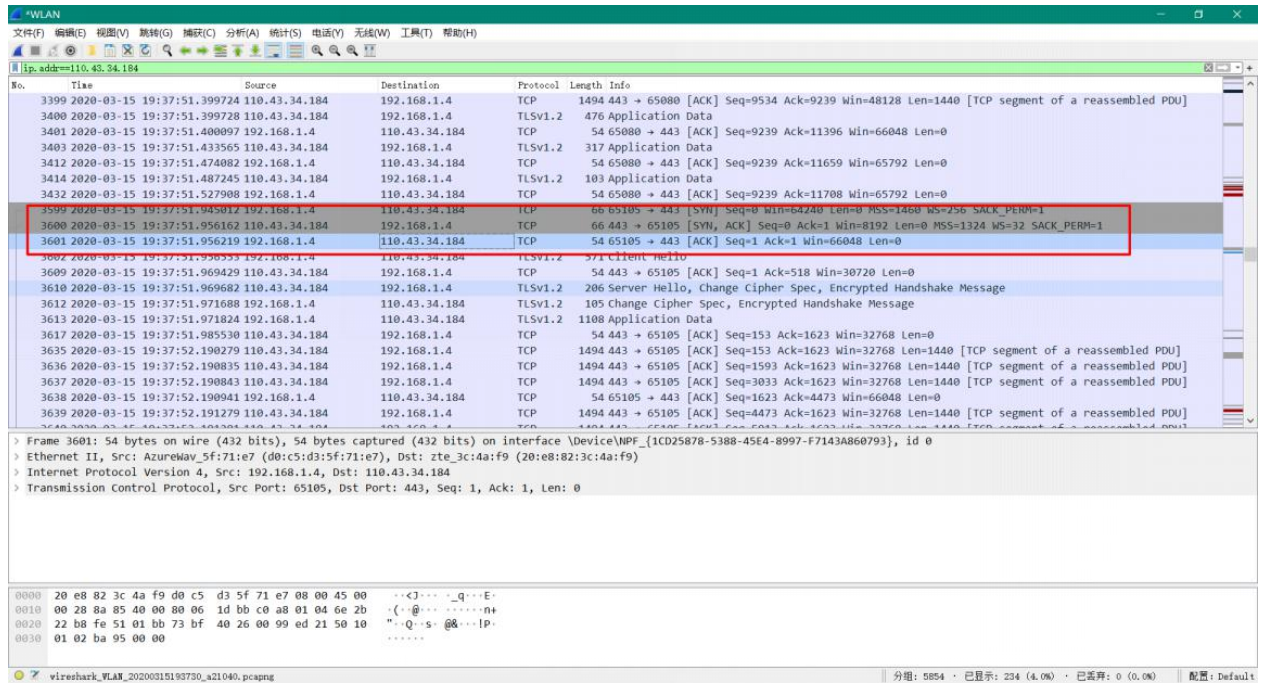
教学平台

找到 post 对应的端口号为 61728

> Transmission Control Protocol, Src Port: 61728, Dst Port: 80, Seq: 2650, Ack: 246554, Len: 785

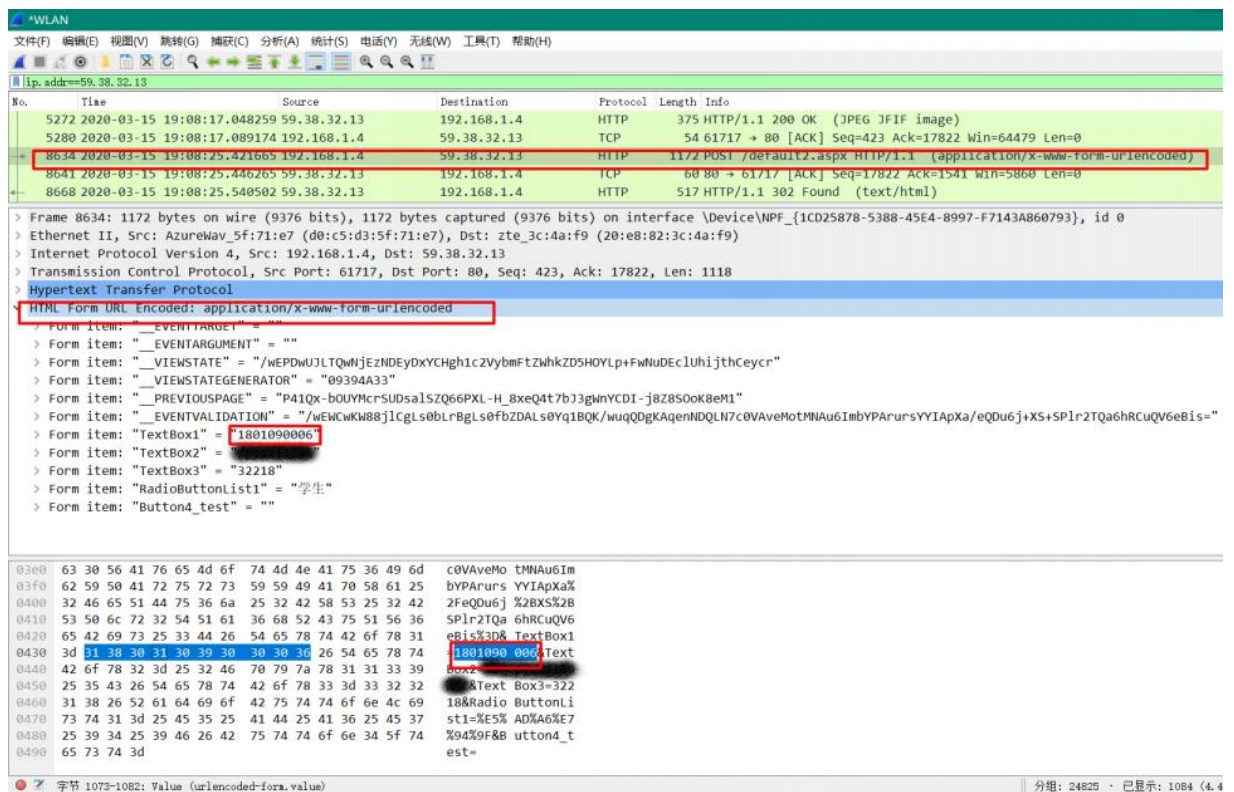


bilibili



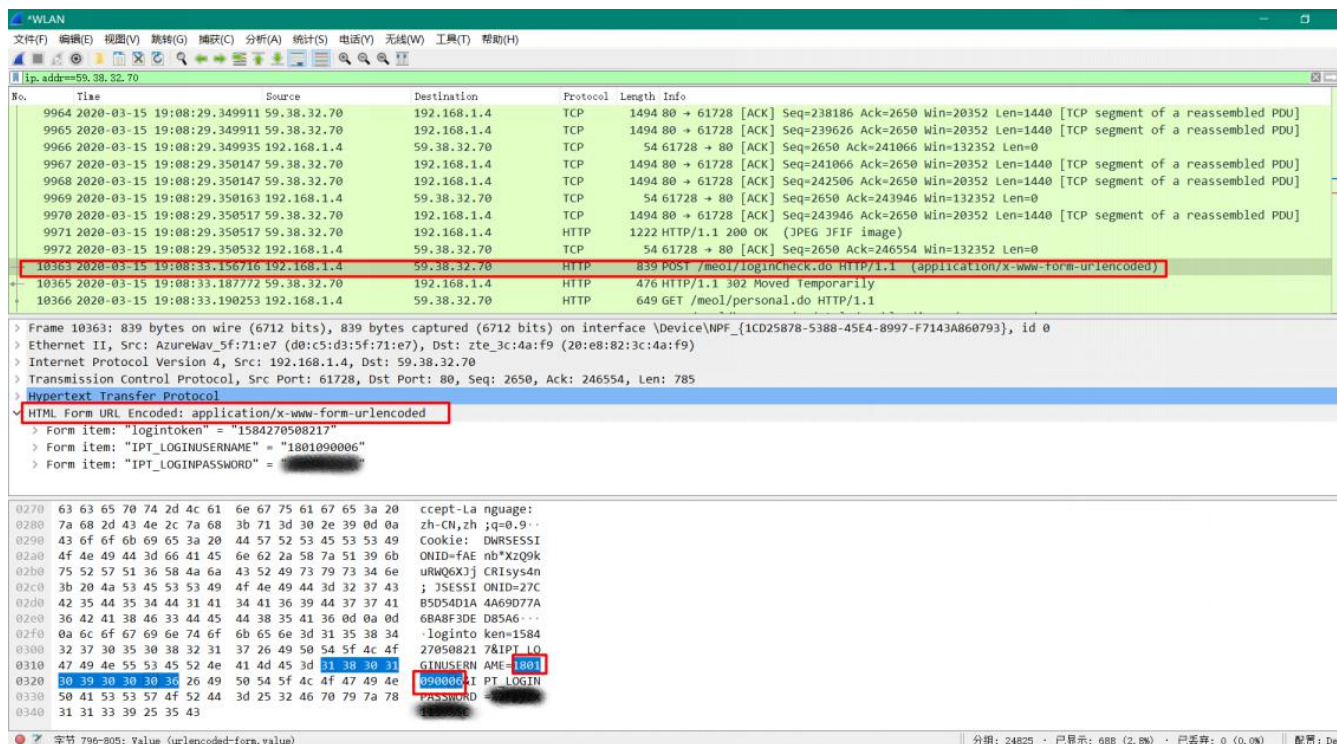
是否明文

教务系统



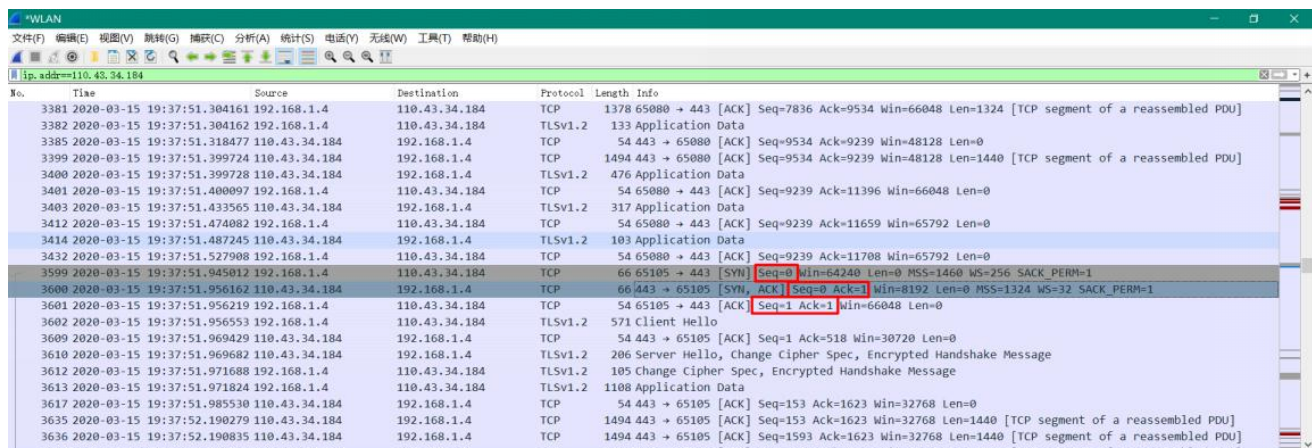
学号为 1801090006

教学平台



可以看到教务系统和教学平台都是以明文形式传输，并不安全。

bilibili



找不到可以看到明文显示的数据包

四、实验收获与总结

通过抓包了解到学校的教学平台和教务系统的登录传输方式皆是明文，结合上一次实验，若发送一个经恶意篡改后的网址给登录该网站的人即可获取个

人信息，这是极不安全的。