信息安全技术第二次实验报告

**一、实验目的**

学习虚拟机安装，版本控制软件、抓包软件使用及初步具备协议分析能力

**二、实验工具**

服务器端Centos7，客户端windows10，GitHub，Tcpdump，Wireshark

**三、过程记录**

实验A

首先使用ifconfig指令确定服务器网卡号和IP地址，如图1所示：

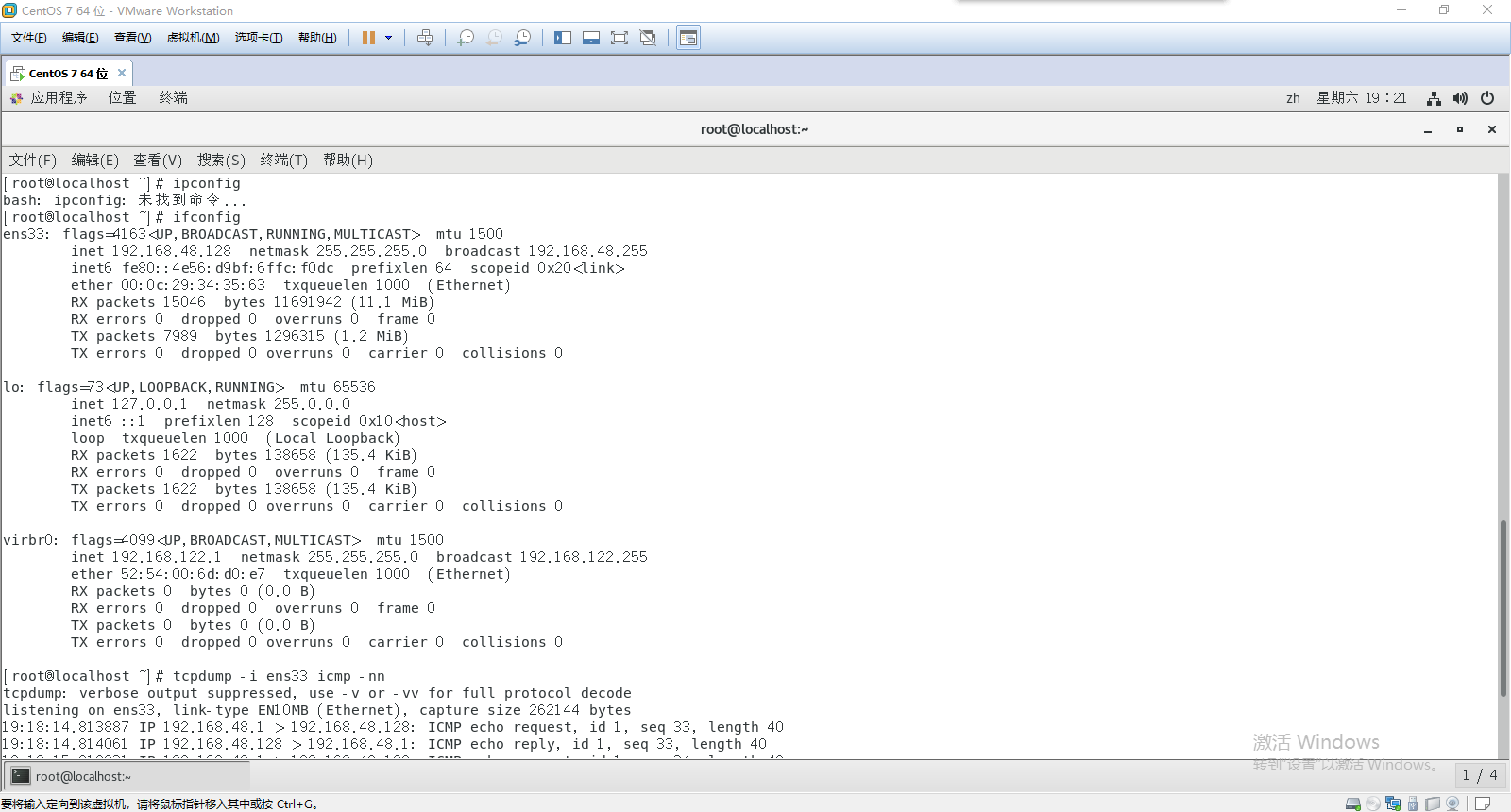


图1 查询网卡和IP

使用tcpdump –i ens33 icmp -nn指令开启服务器端的抓包功能，抓取通过ens33端口收到的ICMP协议报文，同时也可以用and host 限定主机IP，用-c限定抓包个数等，如图2所示：

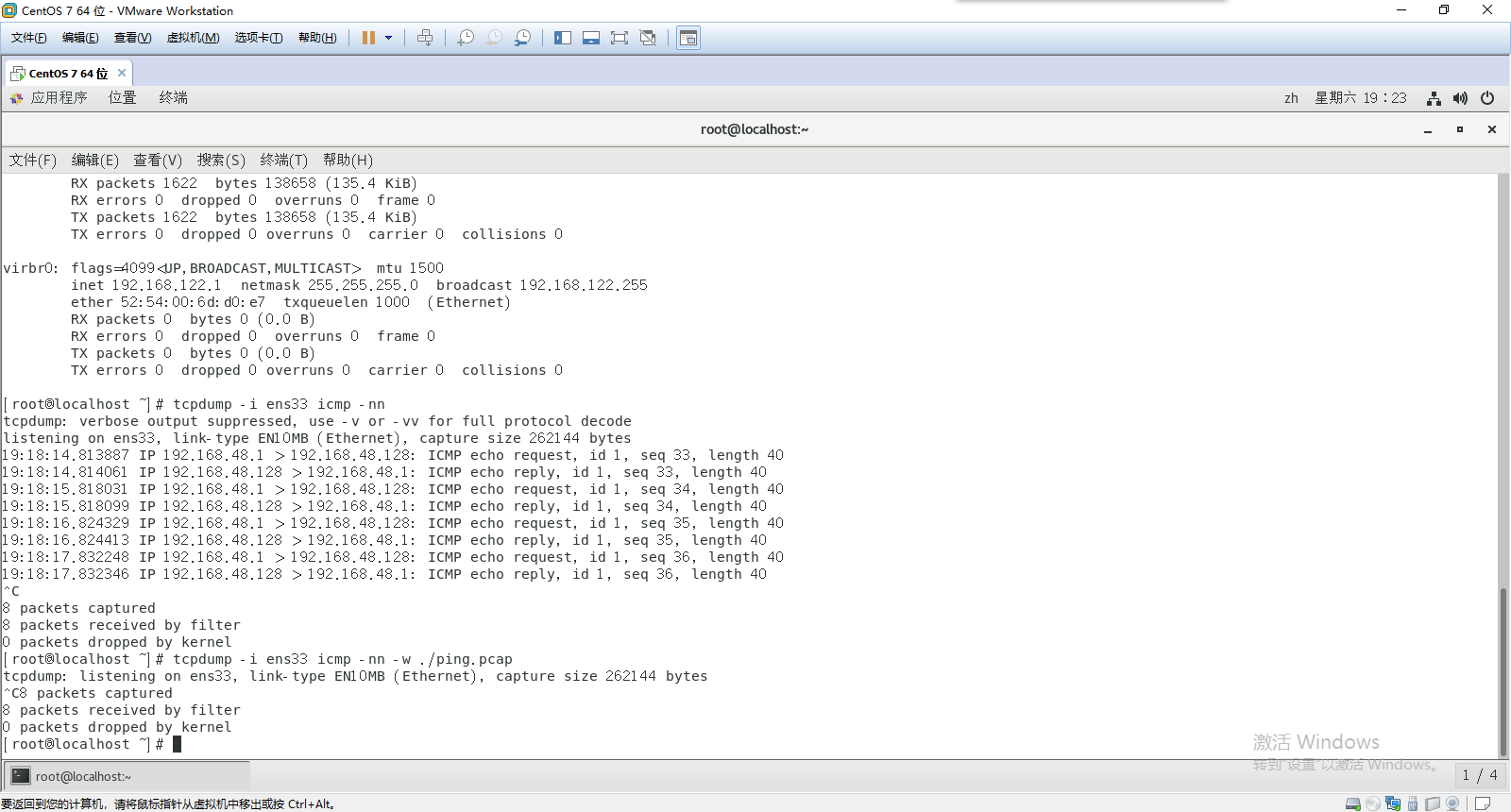


图2 tcpdump抓包

之后在客户端用ping 192.168.48.128指令通过ICMP协议访问服务器，在服务器端抓取到的ICMP包信息，如图3，图4所示：

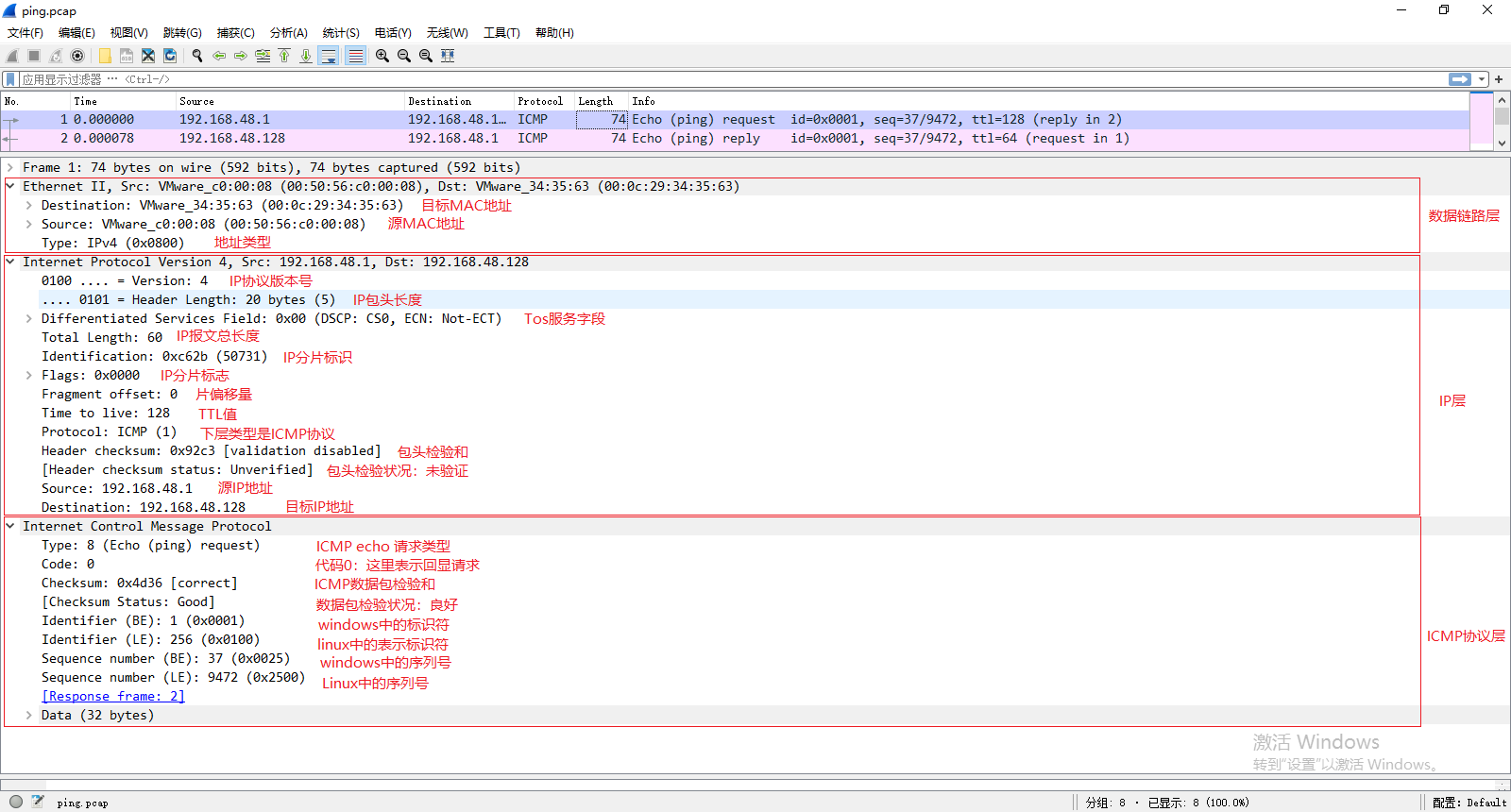
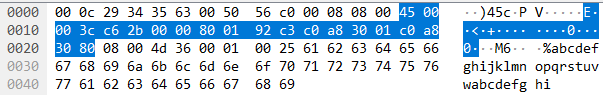


图3 请求报文解析



4500+003c+c62b+0000+8001+0000+c0a8+3001+c0a8+3080=36d39

0003+6d39=6d3c 取反可得 Checksum=92c3

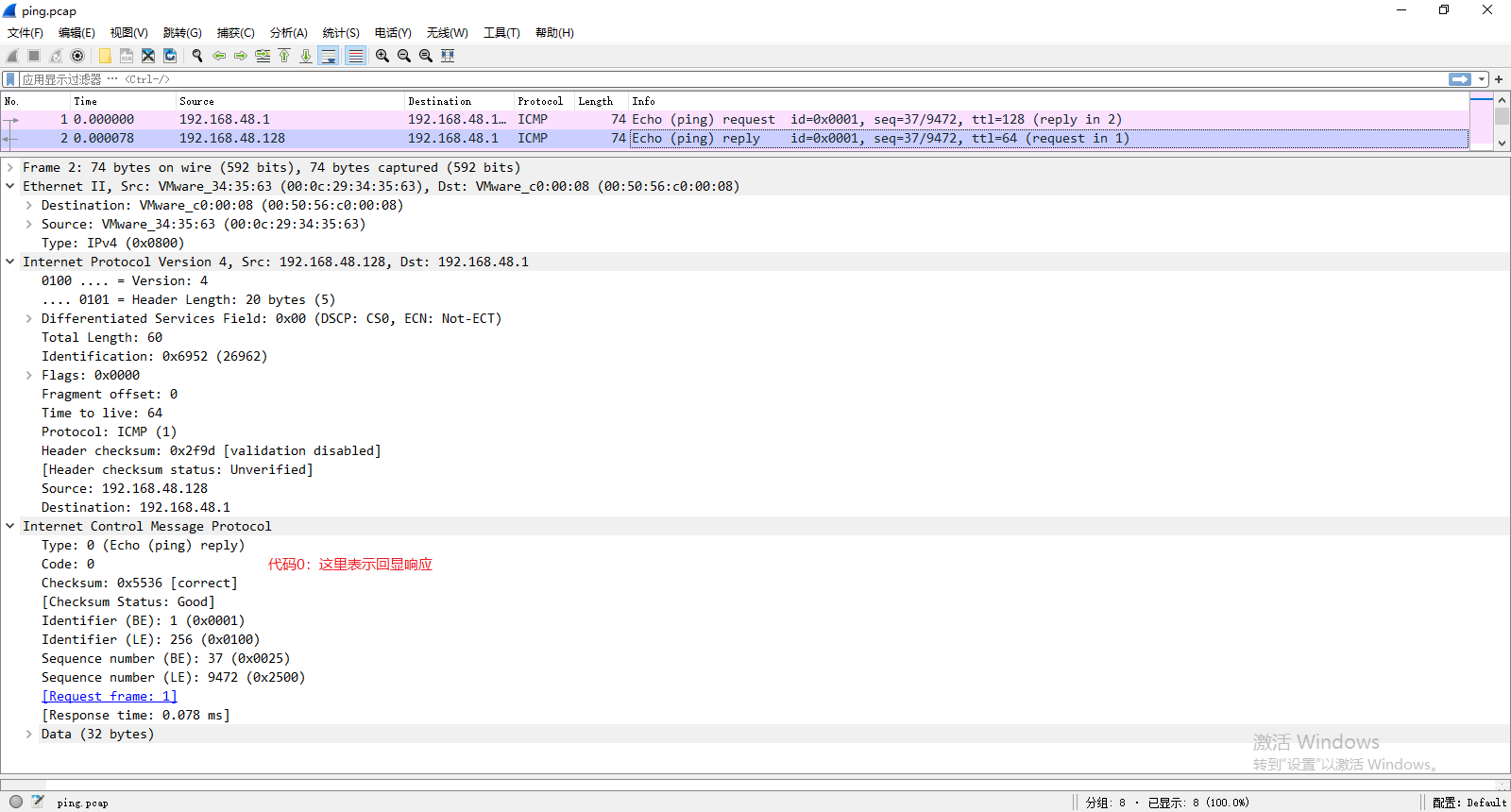
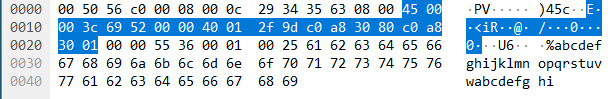


图4 应答报文解析



4500+003c+6952+0000+4001+0000+c0a8+3080+c0a8+3001=2d060

0002+ d060= d062 取反可得 Checksum=2f9d

实验B

首先利用firewall-cmd指令检测80端口和http协议是否打开，确认打开后在客户端利用curl指令对服务器进行访问，访问结果如图所示。

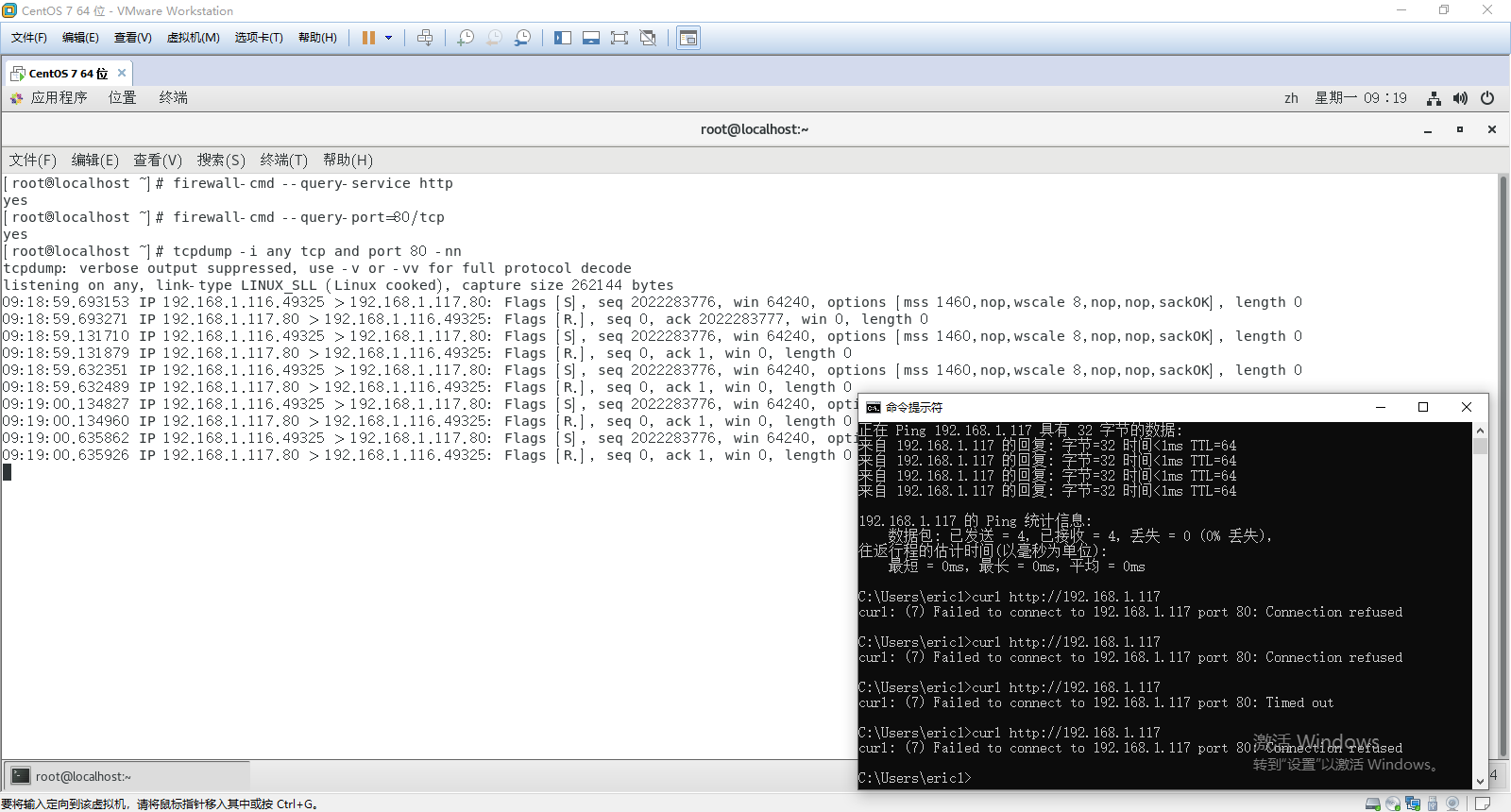
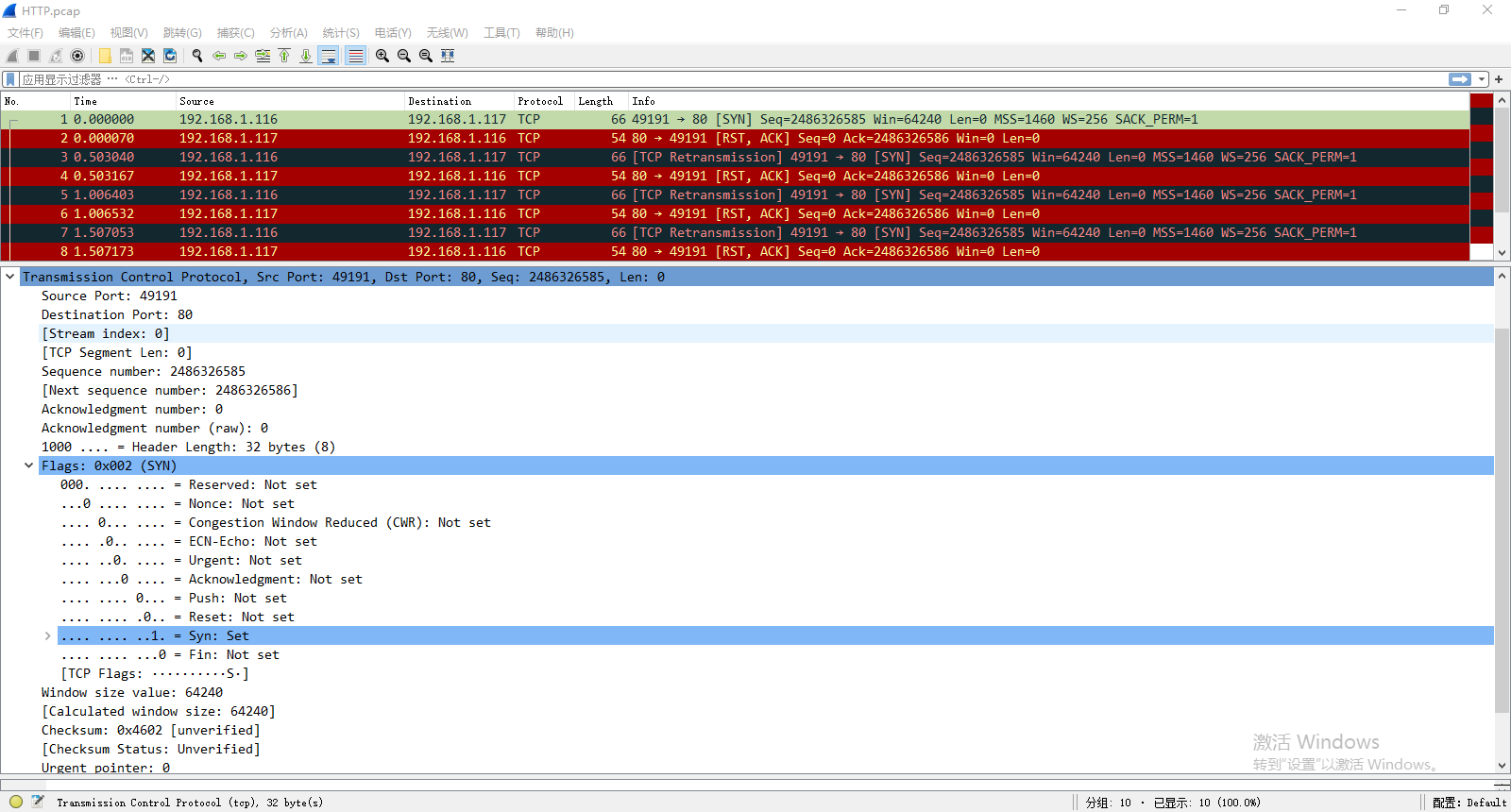


图5 http协议访问

三次握手实验结果如图6，图7所示，但是本实验因为某种原因失败，客户端发出curl指令后被拒绝访问，三次握手无法建立，目前未找到可行解决方案，先在以下结果的基础上进行相关分析，分析其中SYN，ACK，FIN等标志及 Sequence number，Acknowledgement number数值在握手连接中的变化情况。

图6 握手请求报文

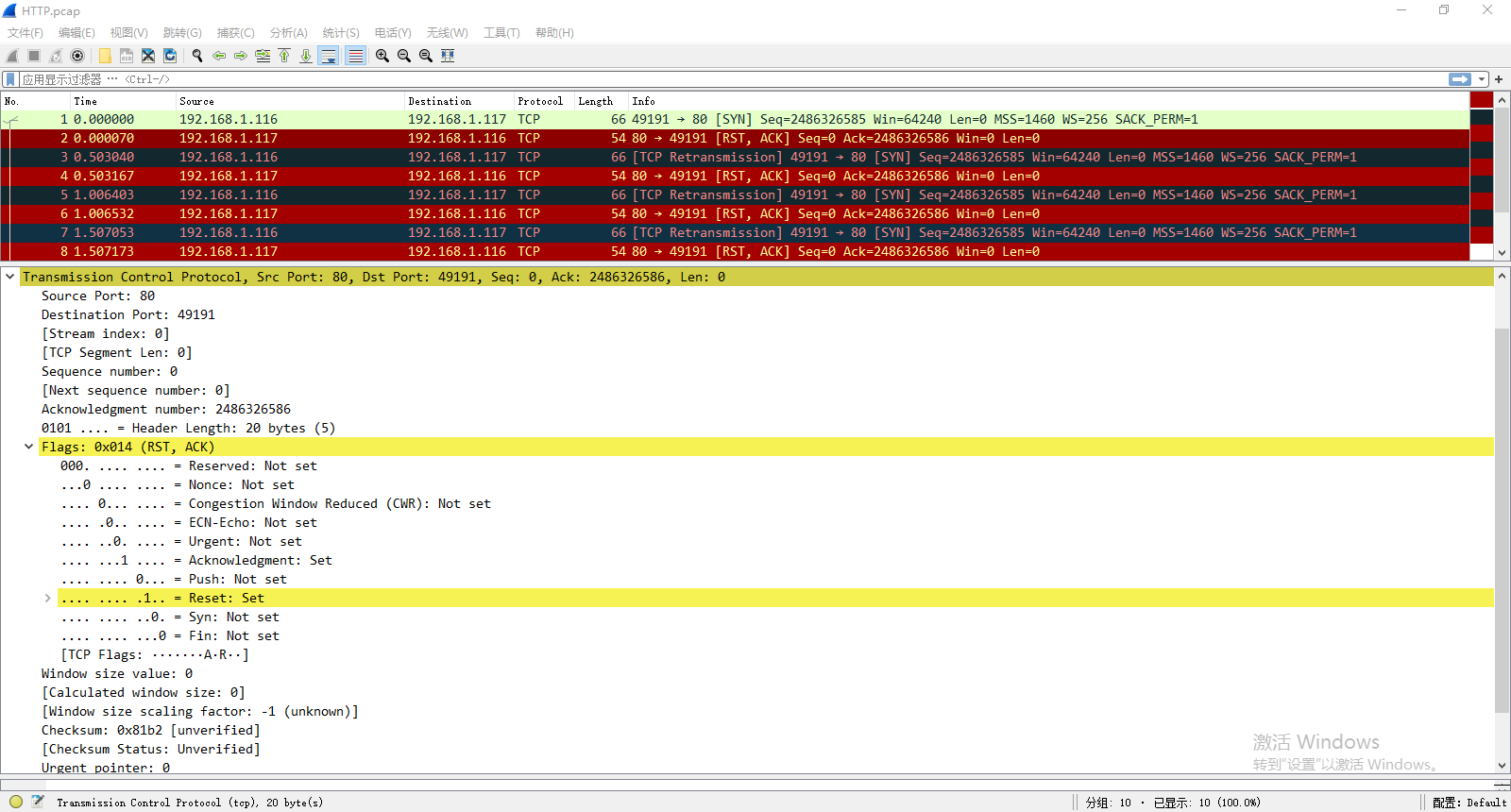


图7 握手响应报文

从图6中可以看到第一次握手时请求报文中SYN=1，ACK=0，FIN=0，Sequence number =2486326585，Acknowledgement number=0，从图7中可以看到第一次握手是应答报文中SYN=0，ACK=1，FIN=0，Sequence number =0，Acknowledgement number=2486326586，由此看出SYN的作用是表示SYN报文，ACK表示Acknowledgement number有意义即做出应答表示ACK报文，FIN表示是否有数据需要发送，另外Sequence number 是发送的数据包中第一个字节的序列号Acknowledgement number是确认序列号，另外结合后面三个重复报文，可以看出这里的RET是指再次发送报文，出现建立连接。

因三次握手实验失败导致后续四次挥手和实验C无法按预期正常进行，后续我会再查阅相关资料，对实验问题进行分析，补充完善，提交完整报告。

**四、参考文献**

[1]ICMP协议：<https://baike.baidu.com/item/ICMP/572452?fr=aladdin>；

[2]搭建http协议服务：<https://www.cnblogs.com/snake553/p/8856729.html>；

[3]tcpdump抓包实现：<http://www.hansongda.cn/post/tcpdumpshakes>；

[4]TCP协议详解：<https://blog.csdn.net/qq_37884273/article/details/82188586>