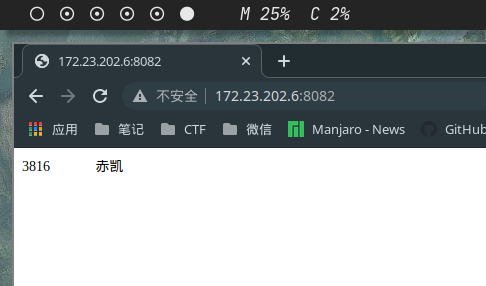
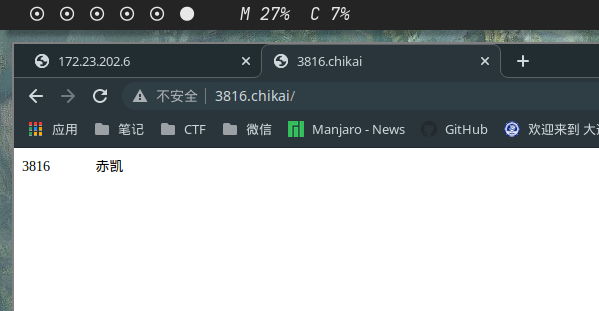
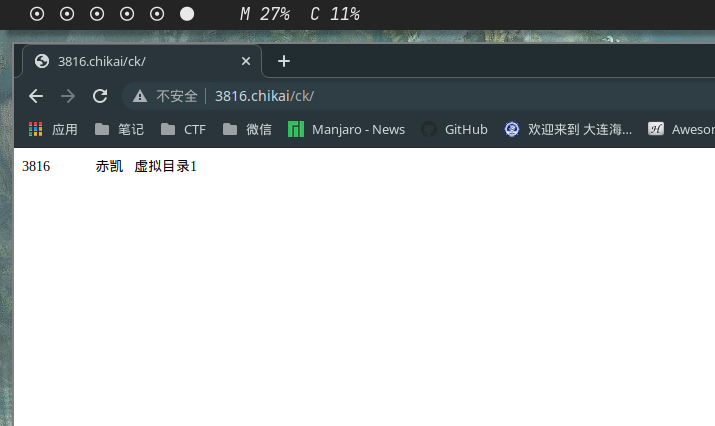
**使用客户机使用时**





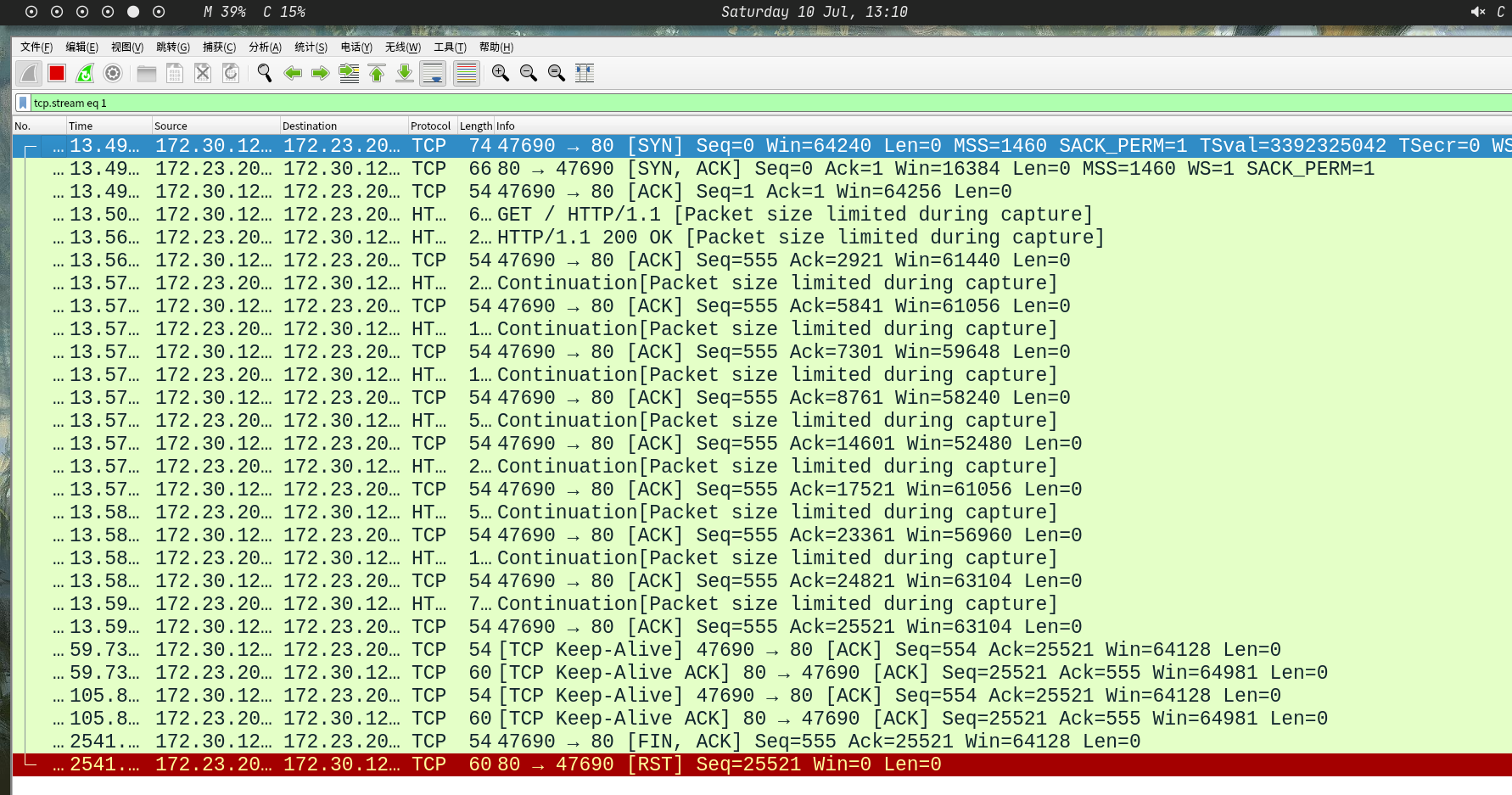


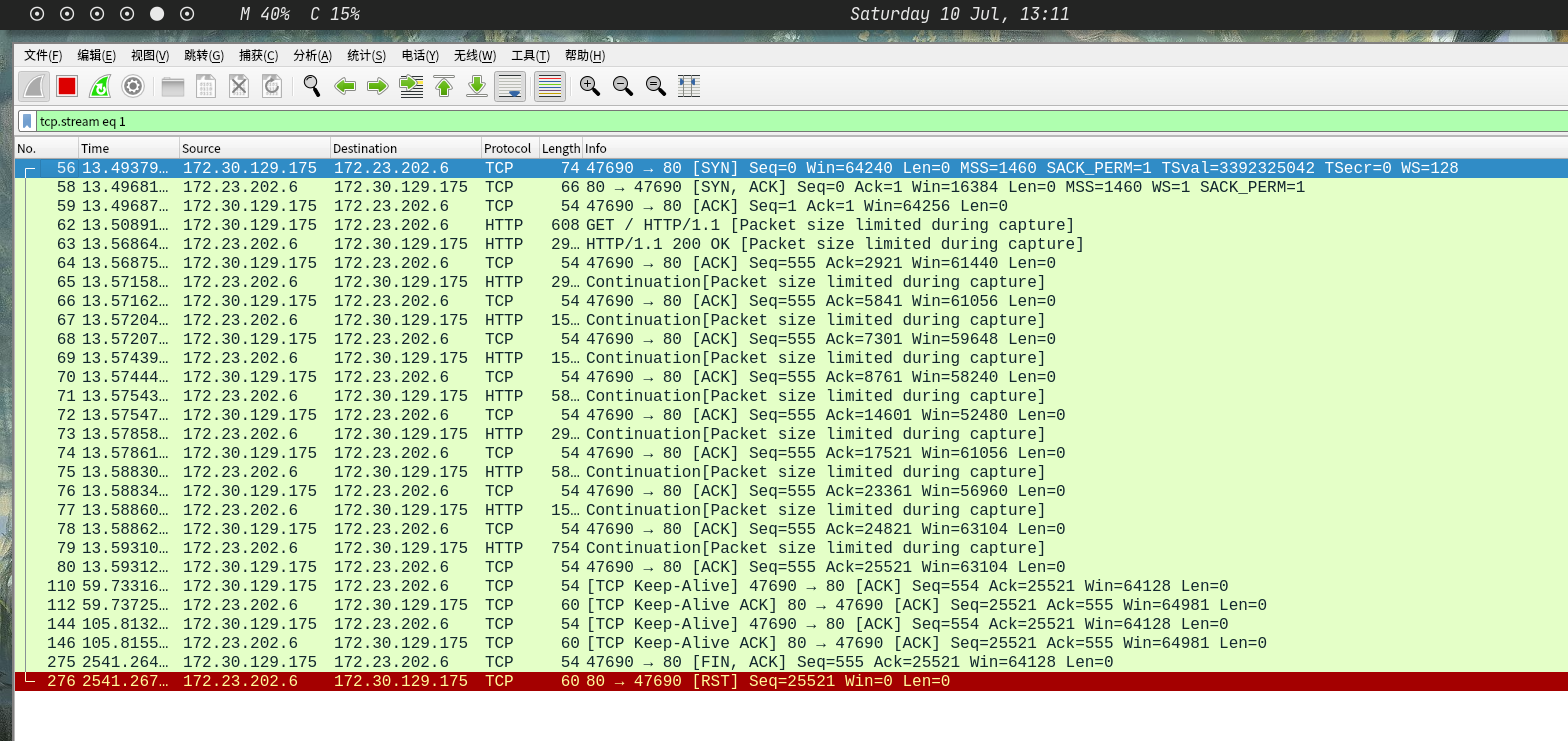


在请求网站时，抓tcp的数据

筛选条件为 tcp && ip.addr == 172.23.202.6

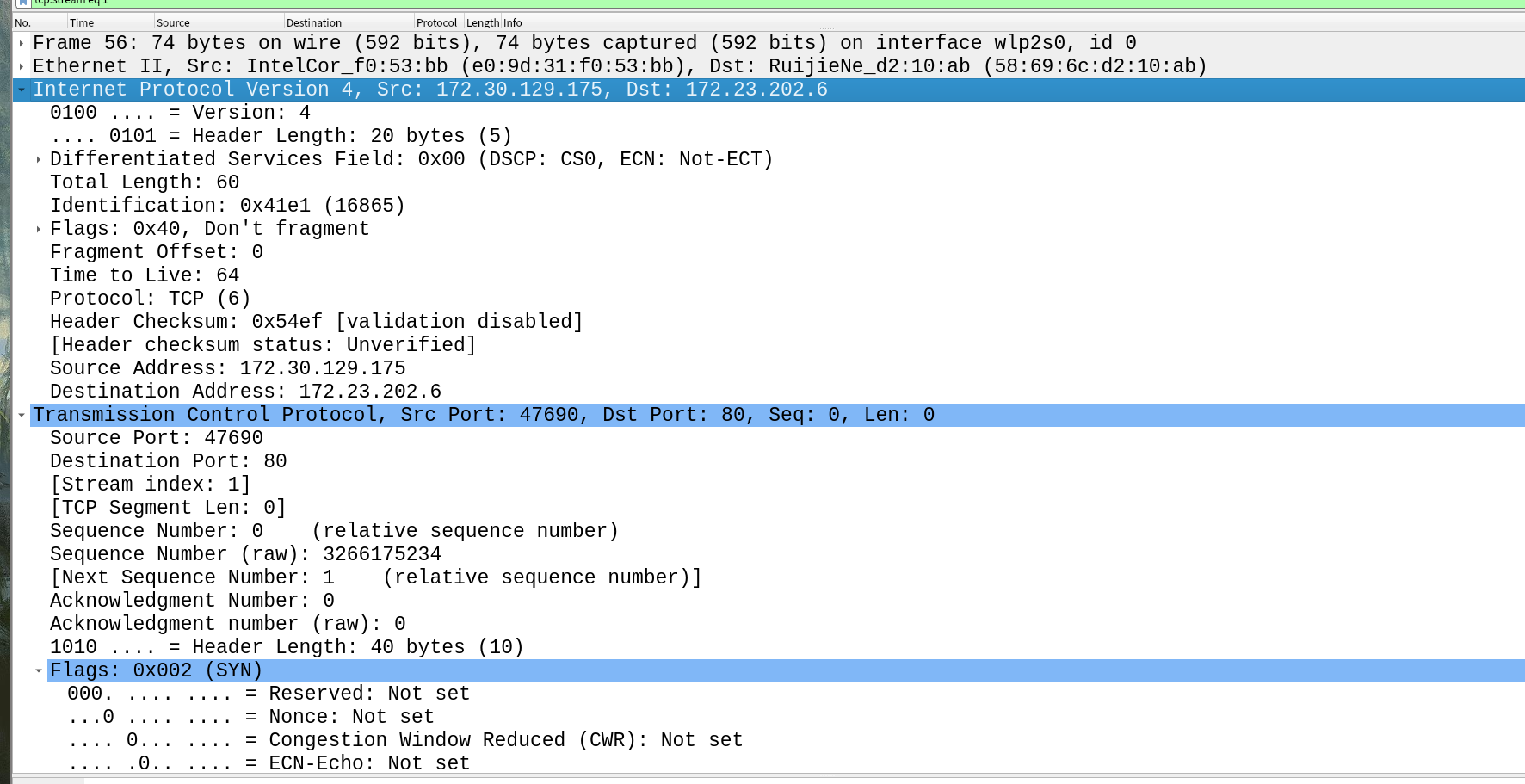
追踪其中一个流





由图可知： 56，58,59 为建立TCP链接的报文

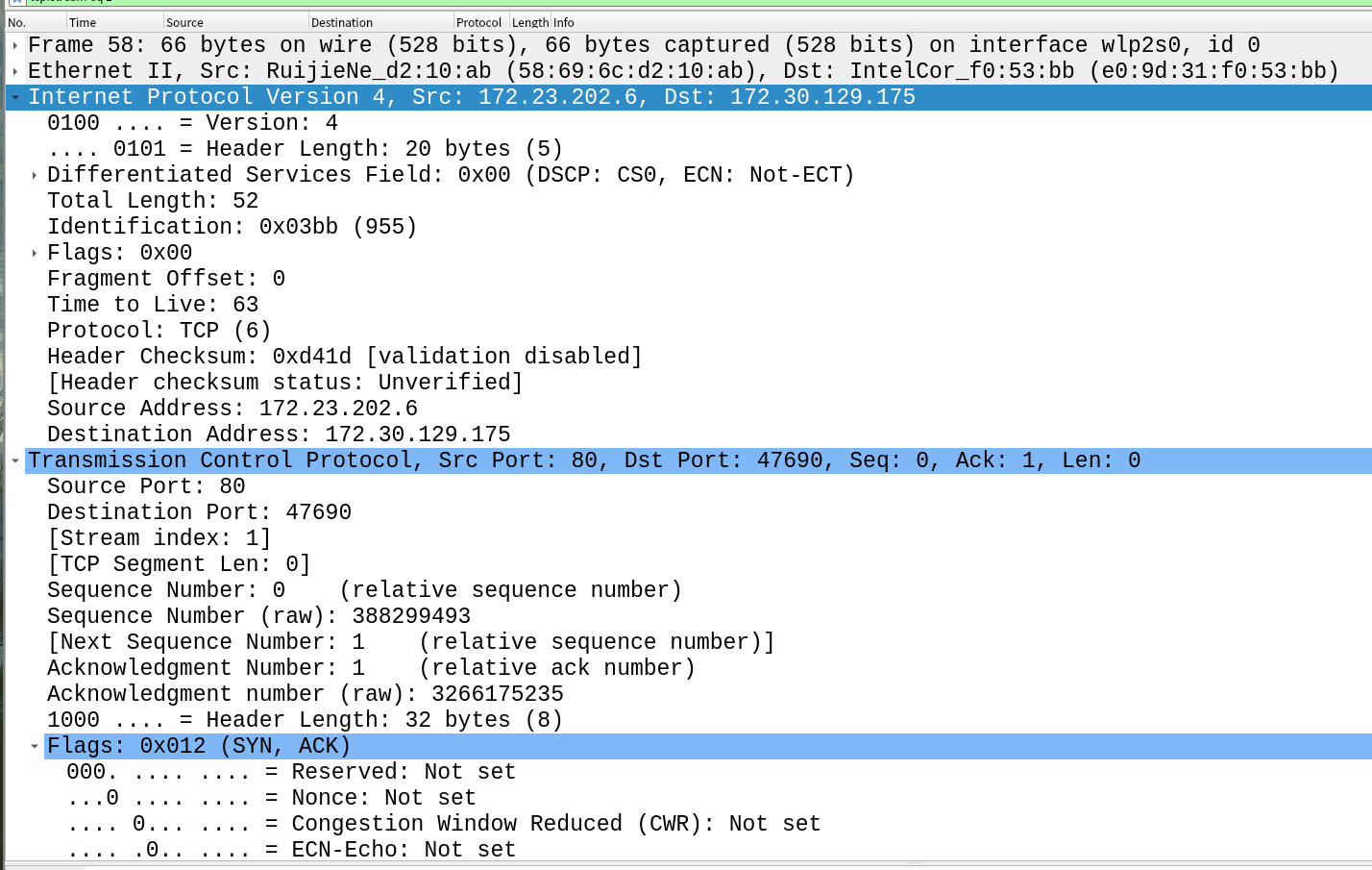
56 :



源端口 为 47690 目的端口为 80

SYN 同步报文 序号为 0

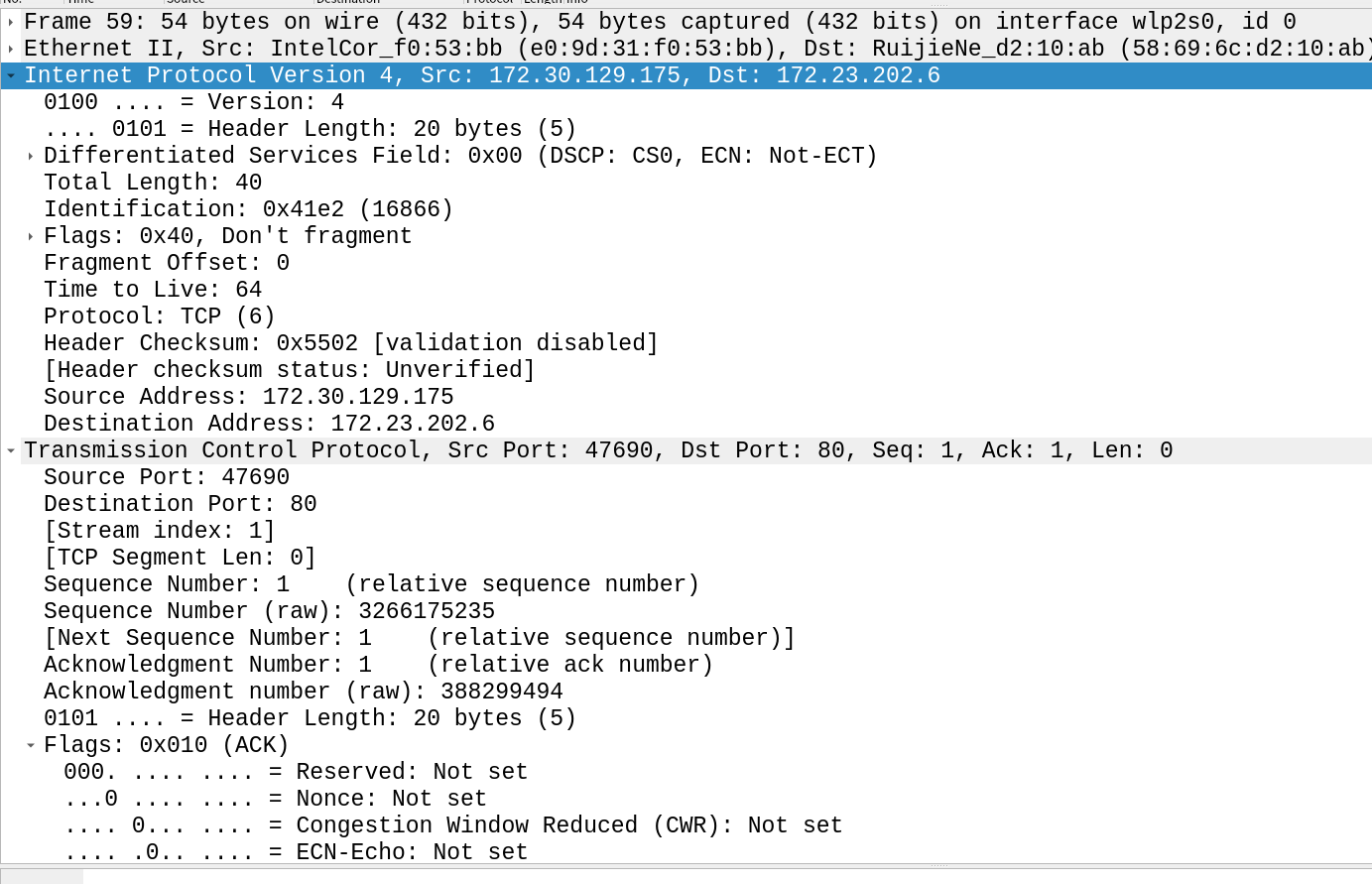
58 服务器回复一个 SYN ACK 报文



源端口为 80 目的端口为47690

序号为 0 ACK 为 1

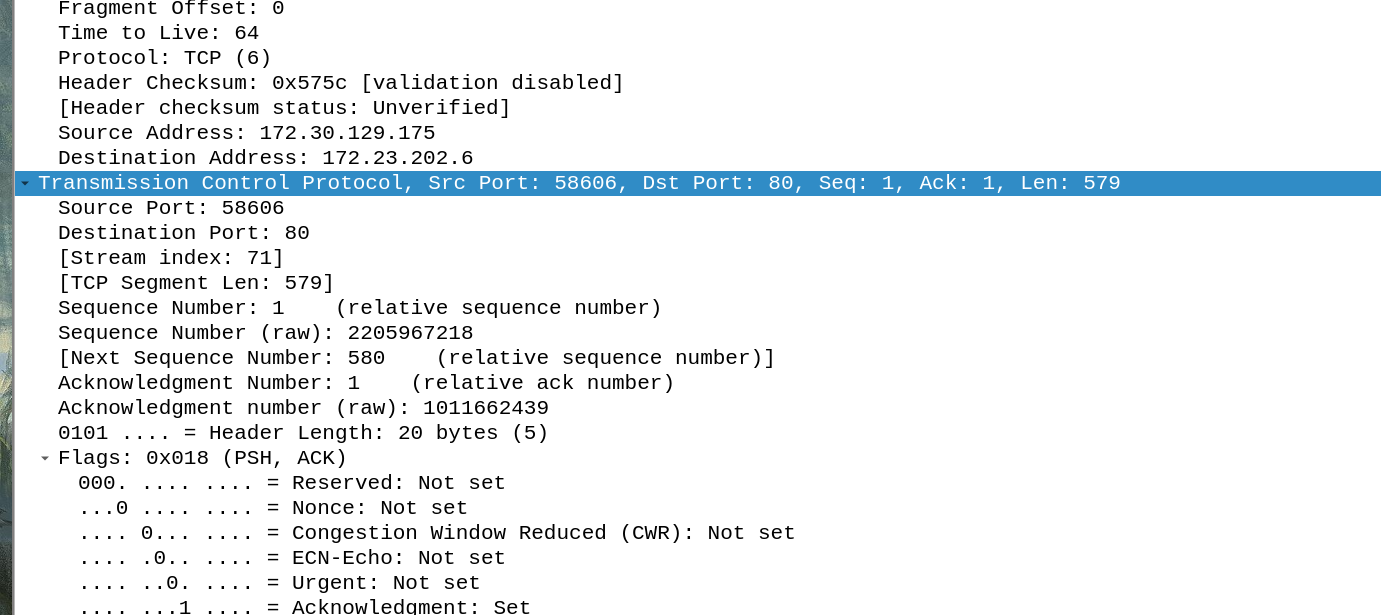
客户机收到后发送一个 ACK 报文



序号为 1 ,ACK 确认号为 1

从 62 到 80 是 http 报文：

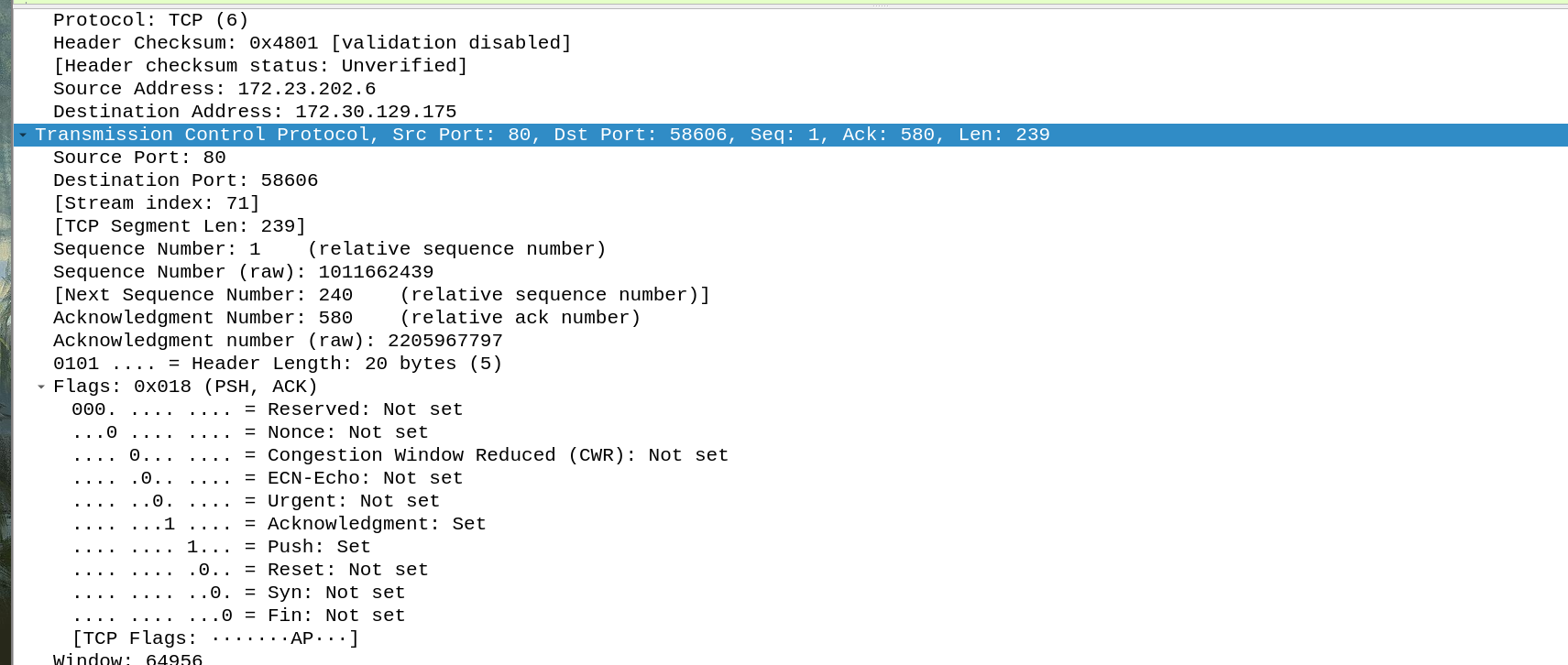
62：



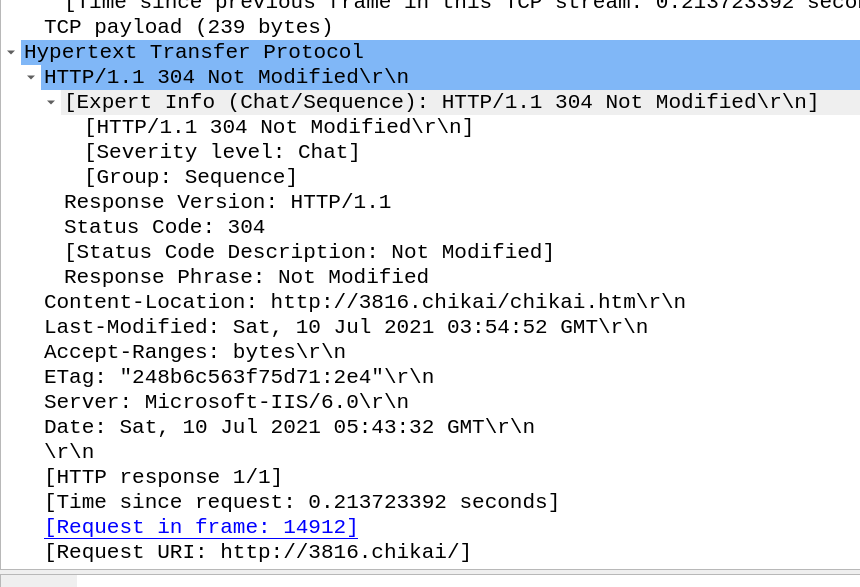
报文序号为 1,确认号1,长度579

flags 标识位为 PSH ACK 完整的URL 为 <http://172.23.202.6>

63:



序号为 1 ACK确认号为 580 长度为239



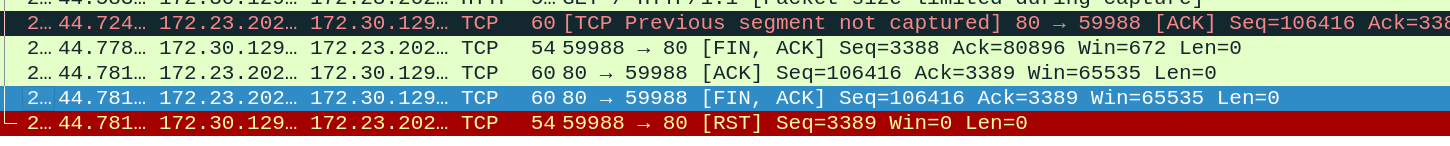
返回的http 报文 状态码 304

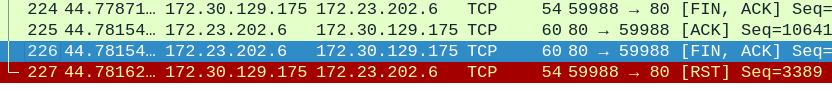
说明在客户端存在缓存，通过 Last-Modified 字段判断修改时间

服务器端网页没有修改就直接用缓存的内容，

这样可以提高访问体验

断开链接





从 224 到 227 为四次挥手断开链接

224 ： 客户机发送一个 FIN 报文，同时携带对上一个报文的确认

这时客户端处于半关闭状态

225,226 ： 服务端 发送一个对 FIN 报文的ACK 确认

有发送一个 FIN ACK 关闭链接报文

服务端处于半关闭状态

227： 客户端收到ACK 报文后 发送一个 RST 置位报文，然后完全关闭链接

服务端收到RST 重置链接，链接关闭