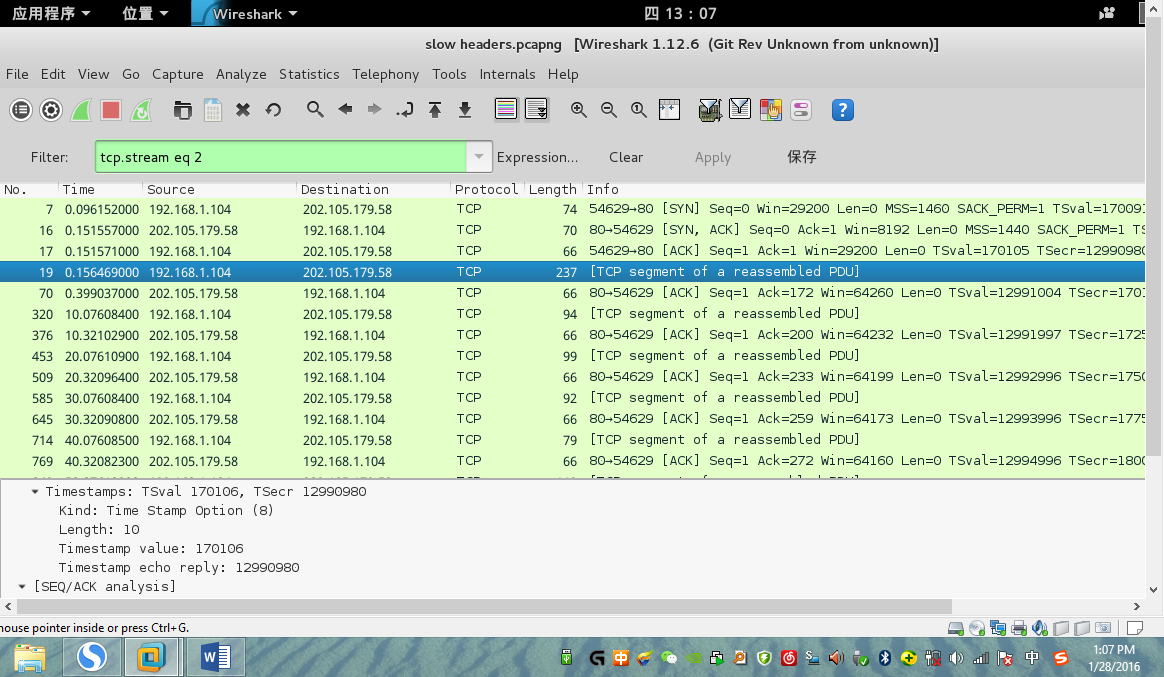
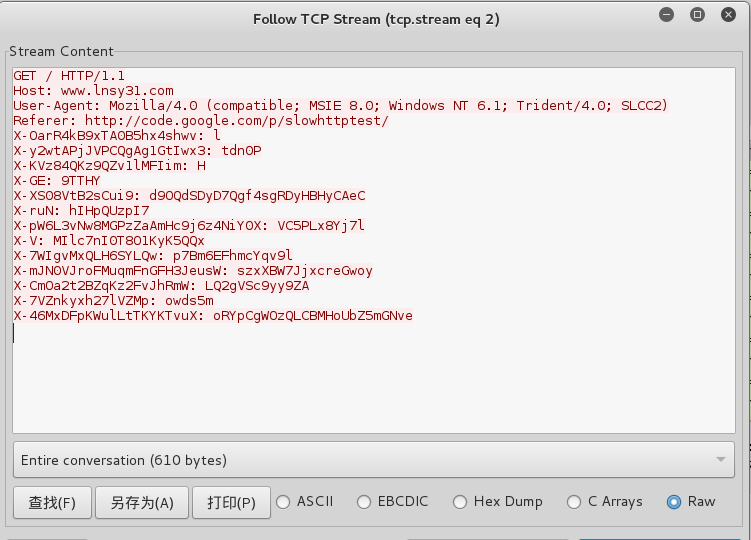
Slowhttptest一共有三种攻击方式：

Header ，body 和 range and read

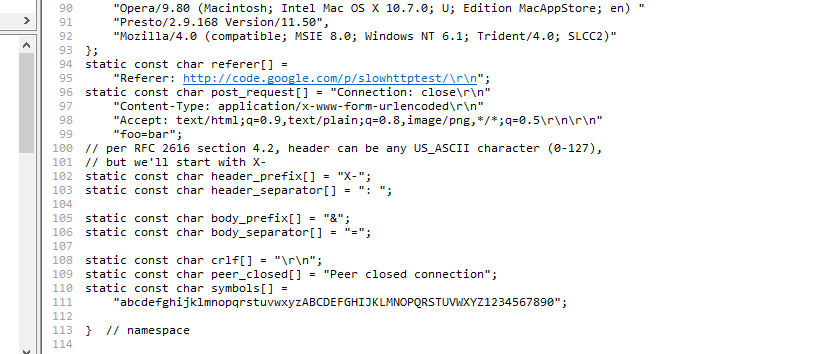
1. header

header这种攻击方式简单的来说是对HTTP服务器送出不完全的HTTP请求，并且试着让它保持不被HTTP服务器超时，如此一来HTTP服务器可开启的最大socket就会 满了，最后导致HTTP服务器无法提供服务。Slowloris是用perl脚本编写的。slowloris在这里又被称为slow headers，攻击截图如下：

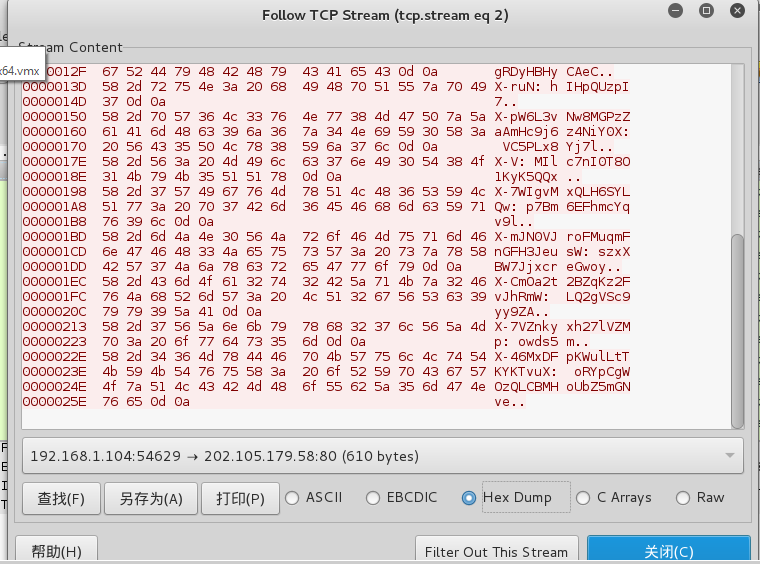
数据包截图如下：



源代码验证：

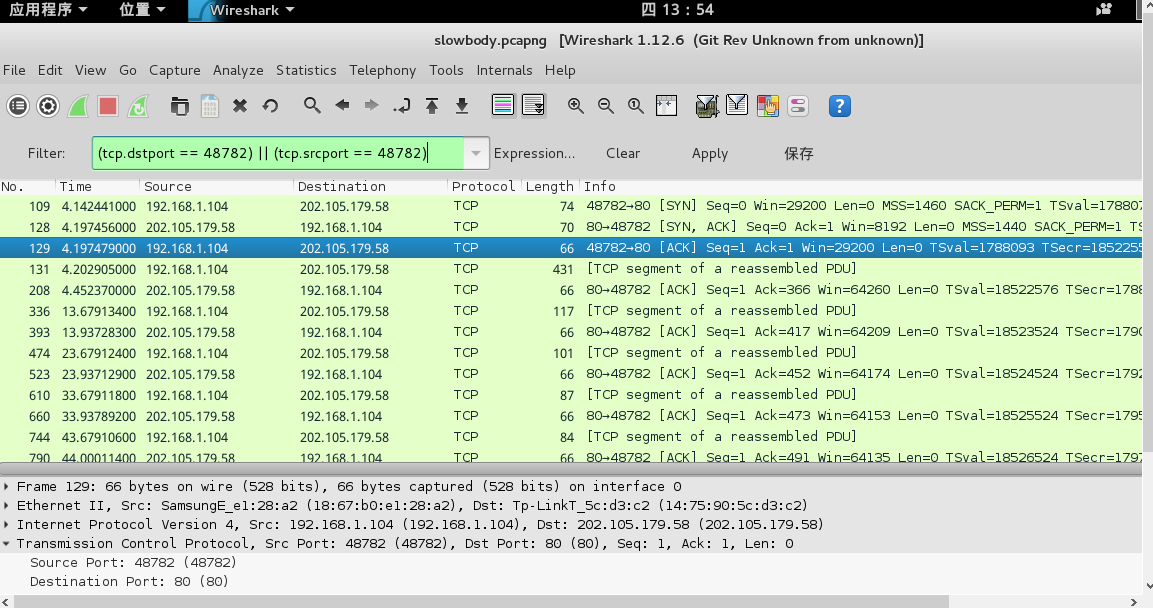


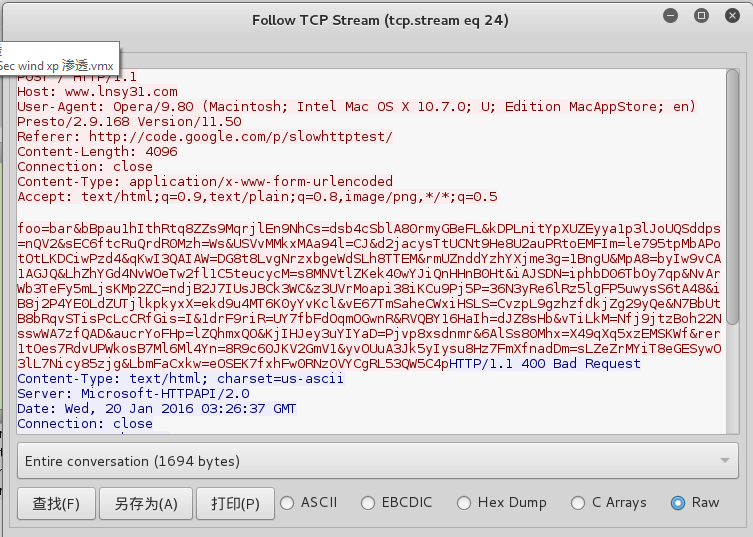
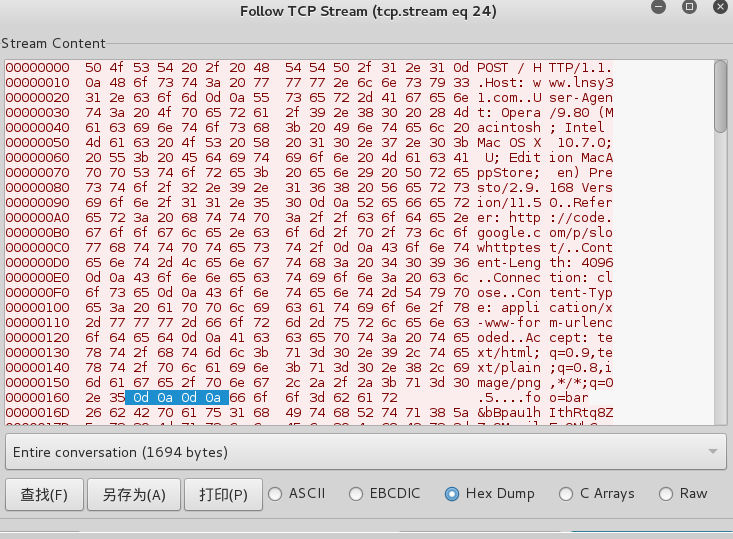
其基本原理是制造不完整的header。完整的http请求头结尾应该是“0d0a0d0a”，而但攻击工具只发送“0d0a”。然后以固定的时间间隔，反复发送随机的key-value键值对，迫使服务器持续等待（至超时）。最终通过不间断的并发连接耗尽系统的最大连接数直至服务端DOS。 切换至HEX显示如下：



2. slow body

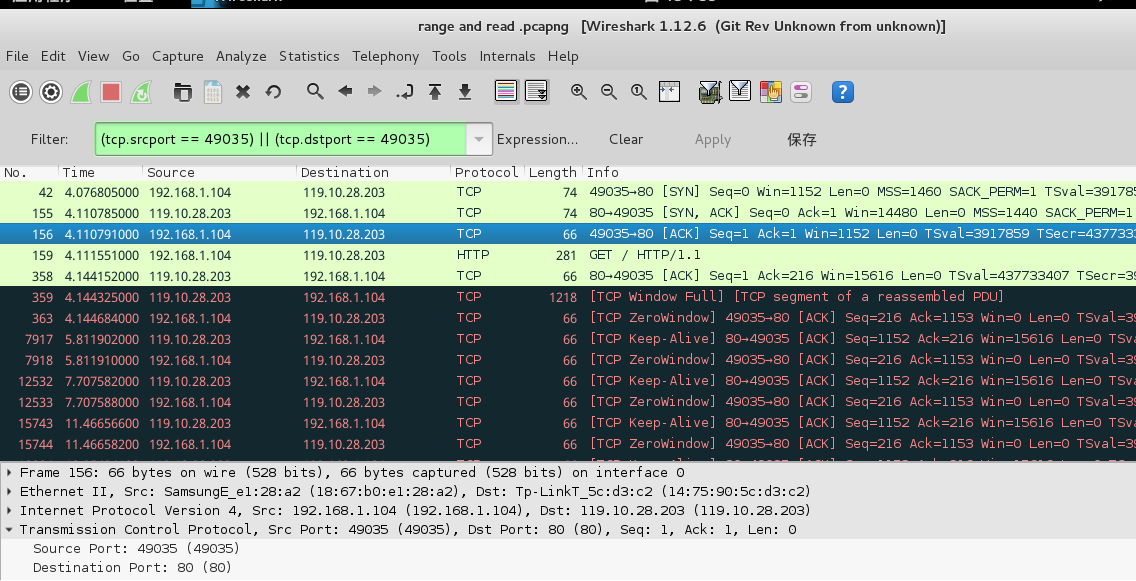
这是一种POST形式的攻击，在这种攻击中，http header数据已被完整发送（0d0a0d0a），只是将http header中content-length字段设置为一个很大的值（这里是4096），同时不在一个包中发送完整post数据而是每间隔10秒（此值攻击者可以调整）发送随机的key-value键值对。可以看出，任何可以接收http post请求的网站，都有可能遭受此类攻击。同样我以48472端口举例：



3. slow range and read

Slow read攻击简单说就是，通过调整TCP协议头中的window size来控制双方的数据流速率，尽可能长的保持单次连接的交互时间，直至超时。



在这里我选择了49035这一个端口和服务器的通讯情况，可以看到，窗口大小被设置为1152。客户端缓冲区在被来自服务的数据填满后，发出了[TCP ZeroWindow]告警，迫使服务端等待。从交互开始到断开，一共用时3分多。（Arrival Time: Jan 20, 2016 13:44:50.368444000 CST Arrival Time: Jan 20, 2016 13:48:06.758724000 CST）