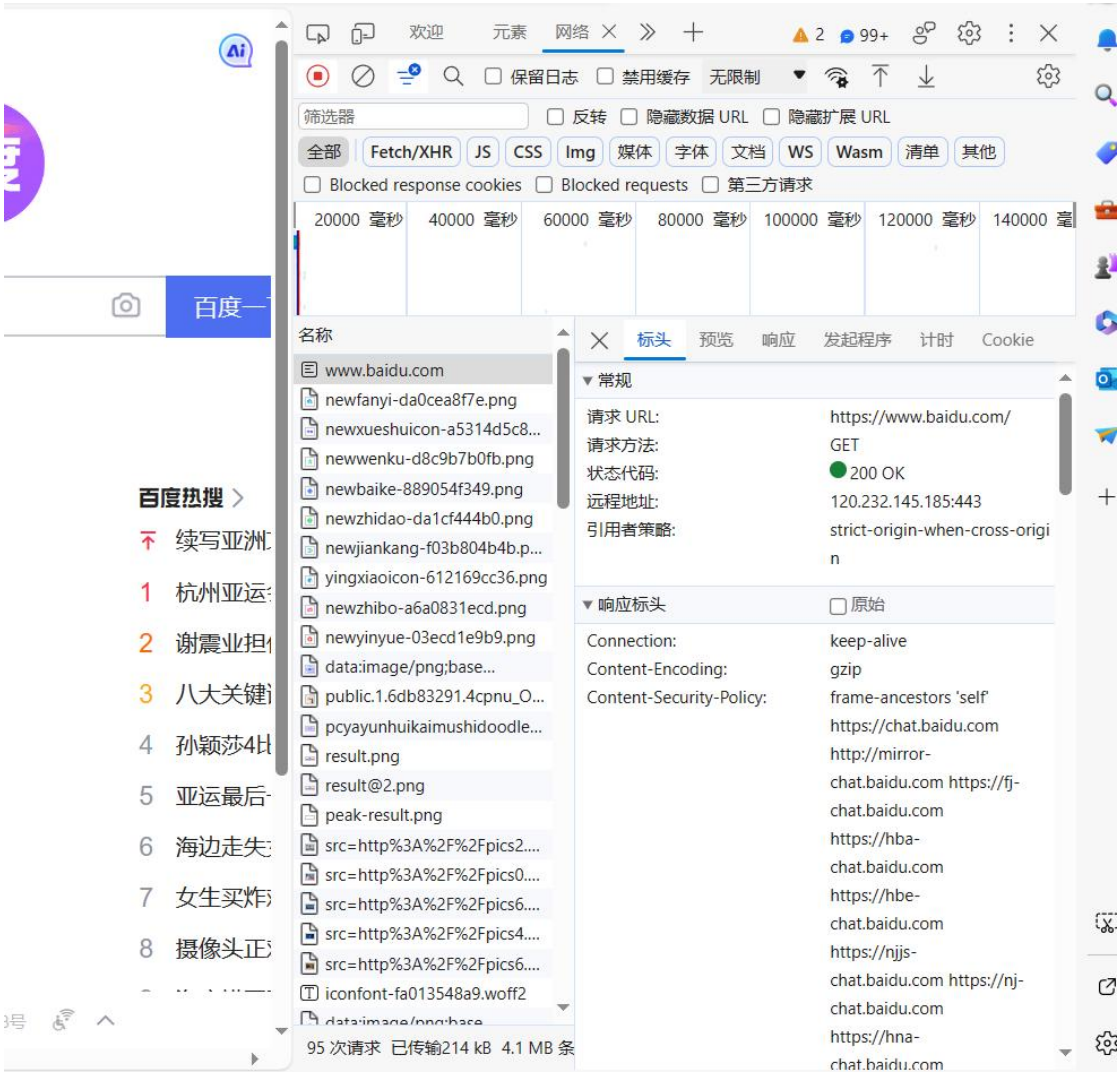
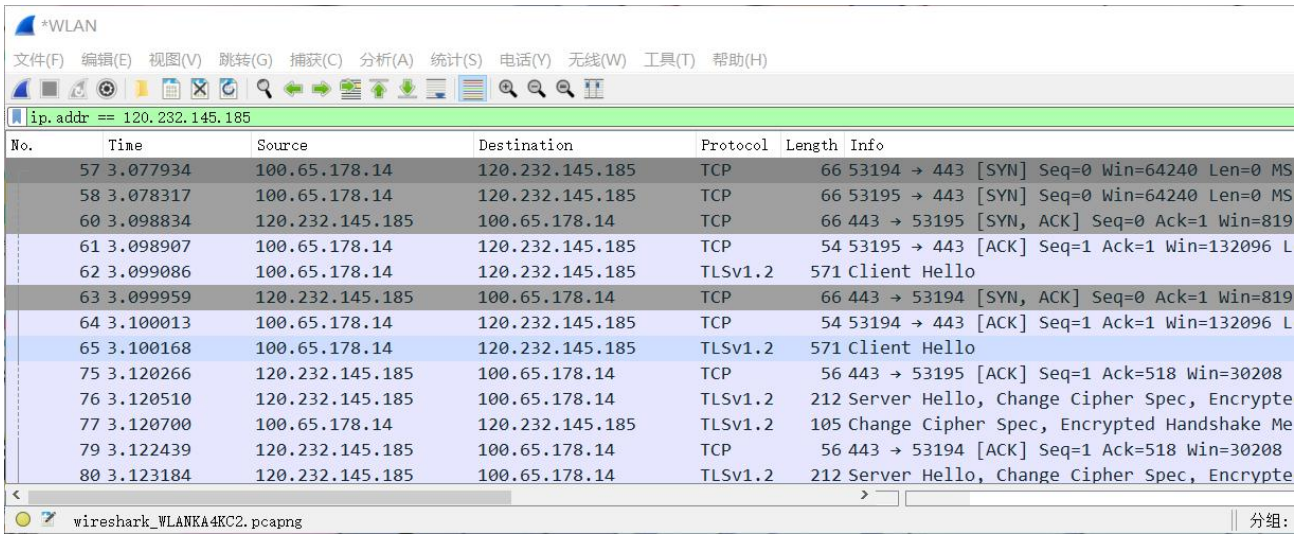
一、Https：通过非对称加密的方式来传递对称加密所需要的秘钥

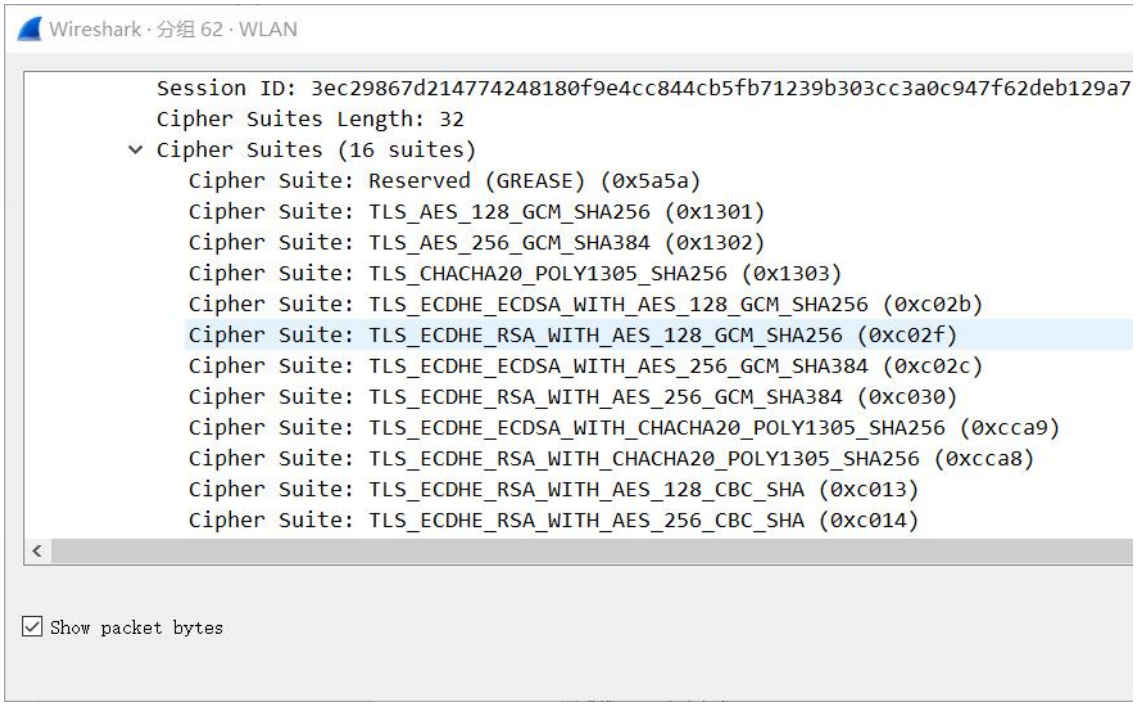
(1) 向百度一下，你就知道 (baidu.com)发送请求



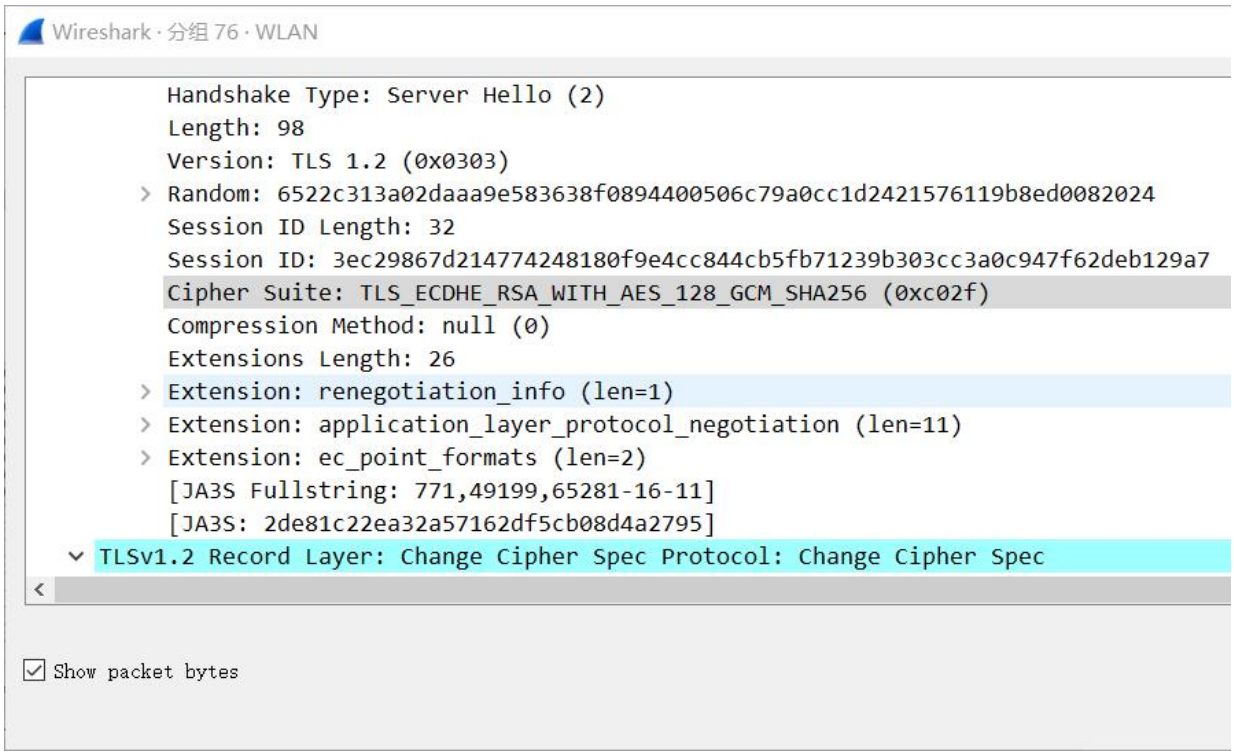
(2) 从第二条开始的三条分别带有【**SYN**】,【**SYN,ACK**】,【**ACK**】为三次握手。



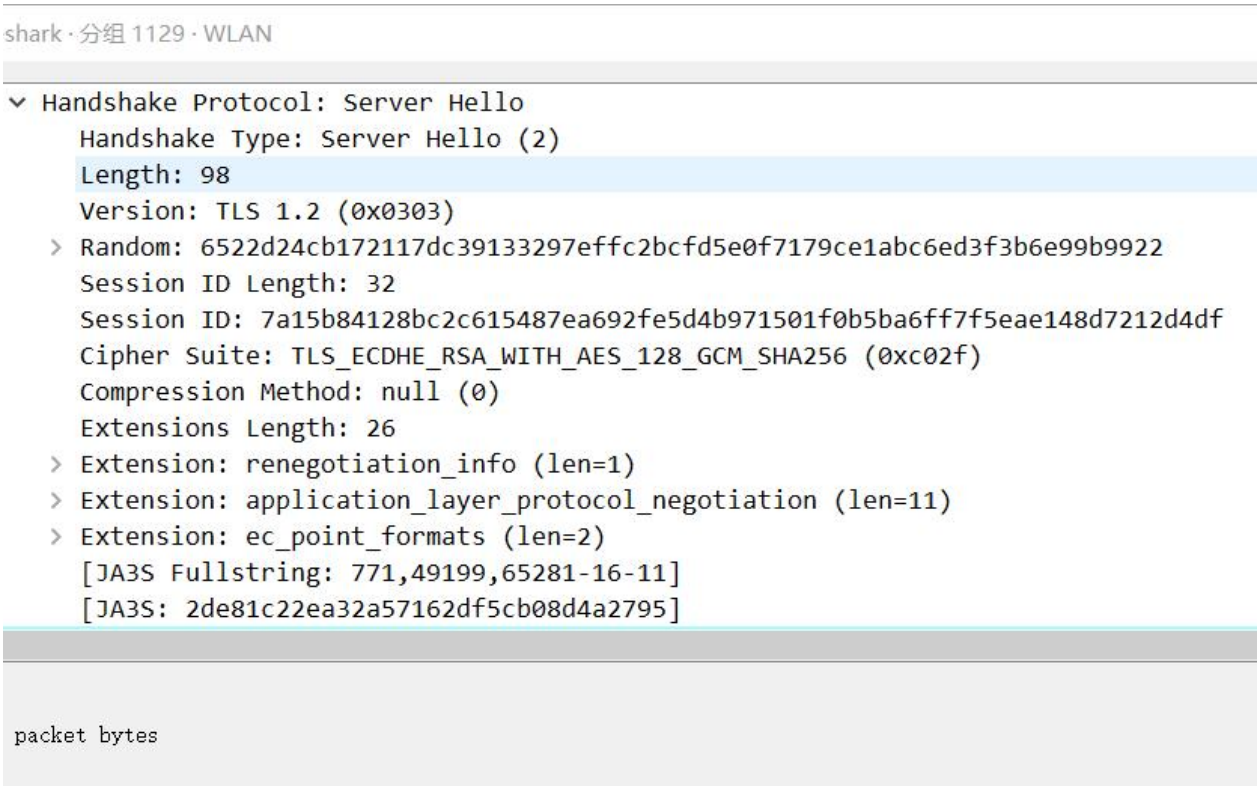
(3) 点开第一个 **info** 为 **Client Hello** 的分组，可以观察到客户端支持的各种加密方式



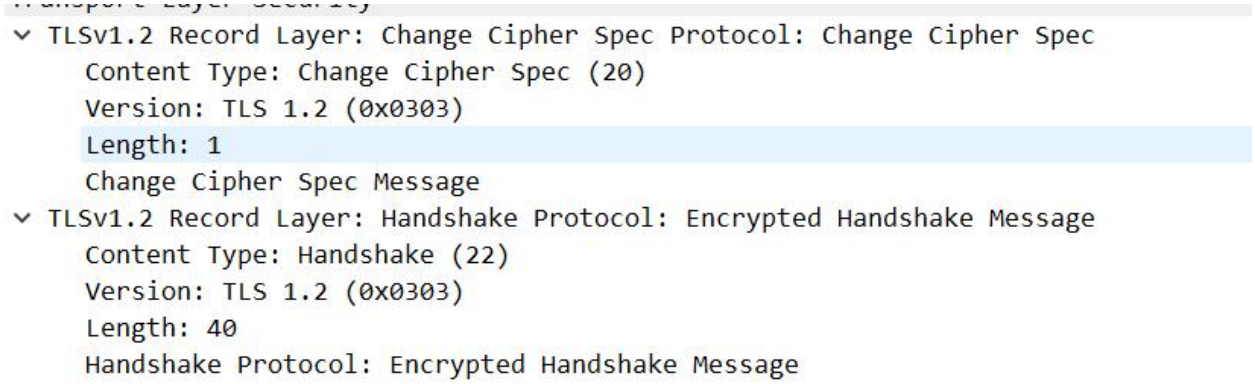
(4) 点开 **info** 为 **server Hello** 的分组，可以观察到服务器支持的加密方式为客户端的一个子集



(5) 分析 **SSL/TLS** 交换证书过程，打开带有 **server hello**，**change cipher spec** 的分组



(6) 交换密钥，打开 **change cipher spec** 的分组

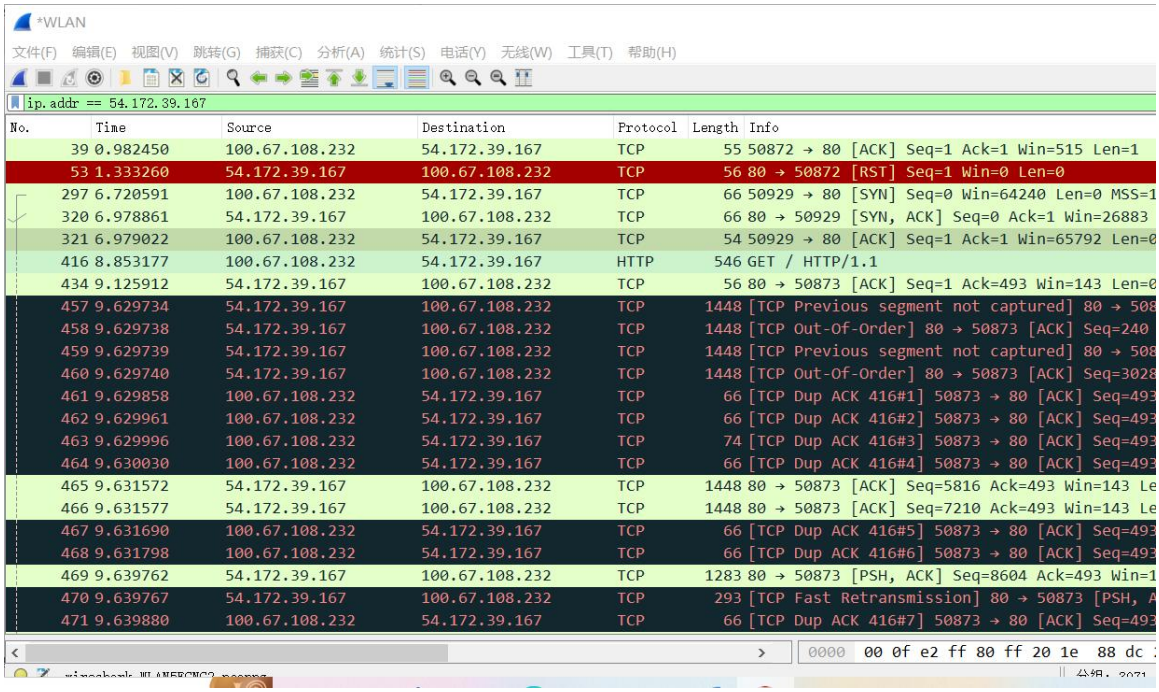


(7) 开始数据交互，即带有 **Application Data** 字样的分组。

二、Http

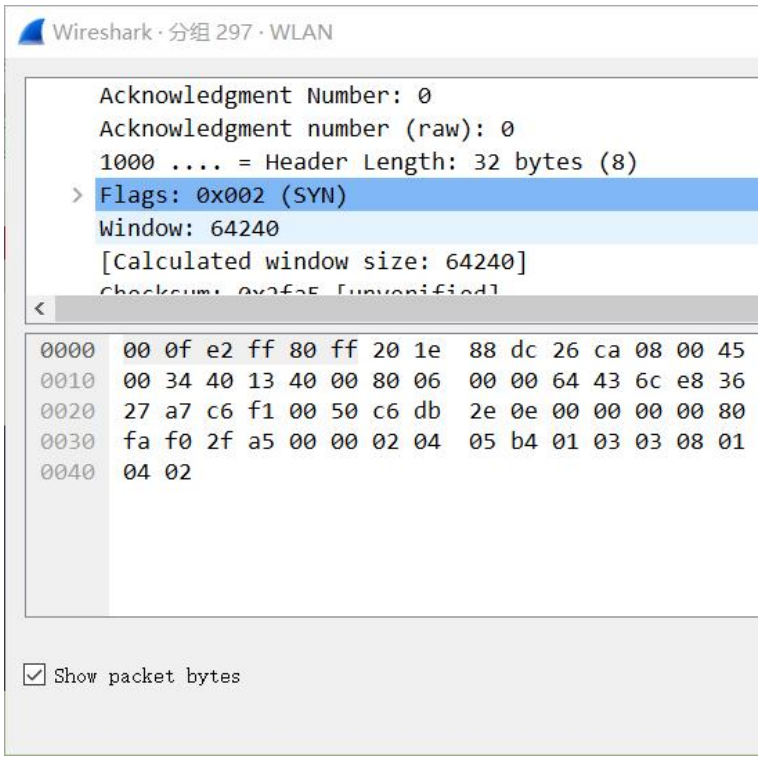
(1) 三次握手：

访问 http://httpbin.org/,得到如下图：

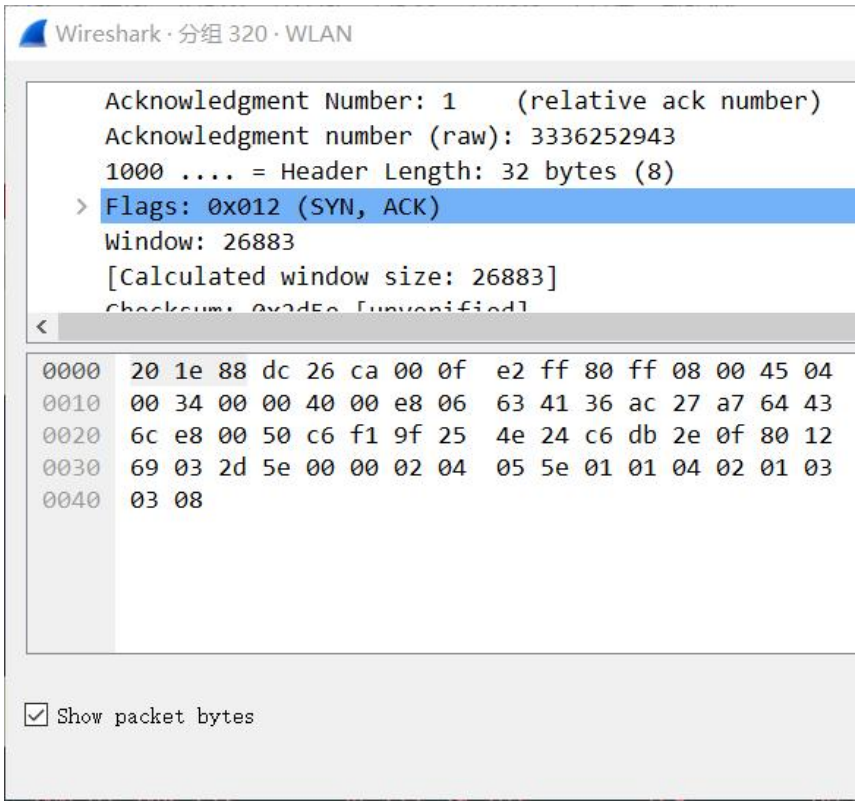


TCP 三次握手为带有【SYN】,【SYN,ACK】,【ACK】的三条分组

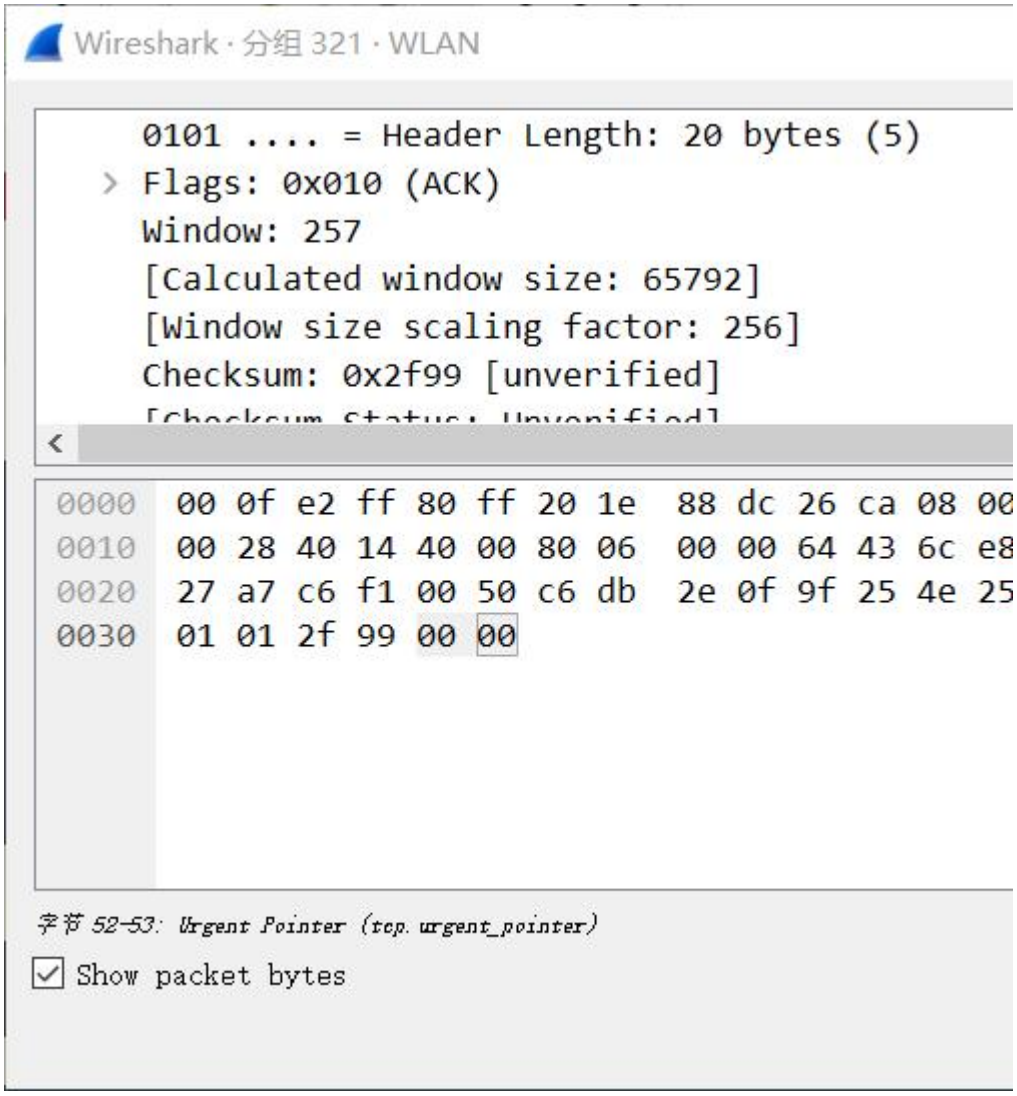
第一次握手时，客户端给服务器发送 SYN 标志位



第二次握手时，服务器给客户端发送 SYN，ACK 标志位



第三次握手时，客户端给服务器发送 ACK 标志位



(2) 四次挥手：实为三次挥手，服务器的确认和挥手合为一个分组

第一次挥手：客户端向服务器挥手

100.67.108.232	54.172.39.167	TCP	54 51963 → 80 [FIN, ACK] Seq=2513 Ack=153250 Win=131840 Len=0

第二次挥手：服务器对客户端的挥手确认以及对客户端挥手

54.172.39.167	100.67.108.232	TCP	56 80 → 51963 [FIN, ACK] Seq=153250 Ack=2514 Win=33536 Len=0

第三次挥手：客户端确认挥手

100.67.108.232	54.172.39.167	TCP	54 51963 → 80 [ACK] Seq=2514 Ack=153251 Win=131840 Len=0