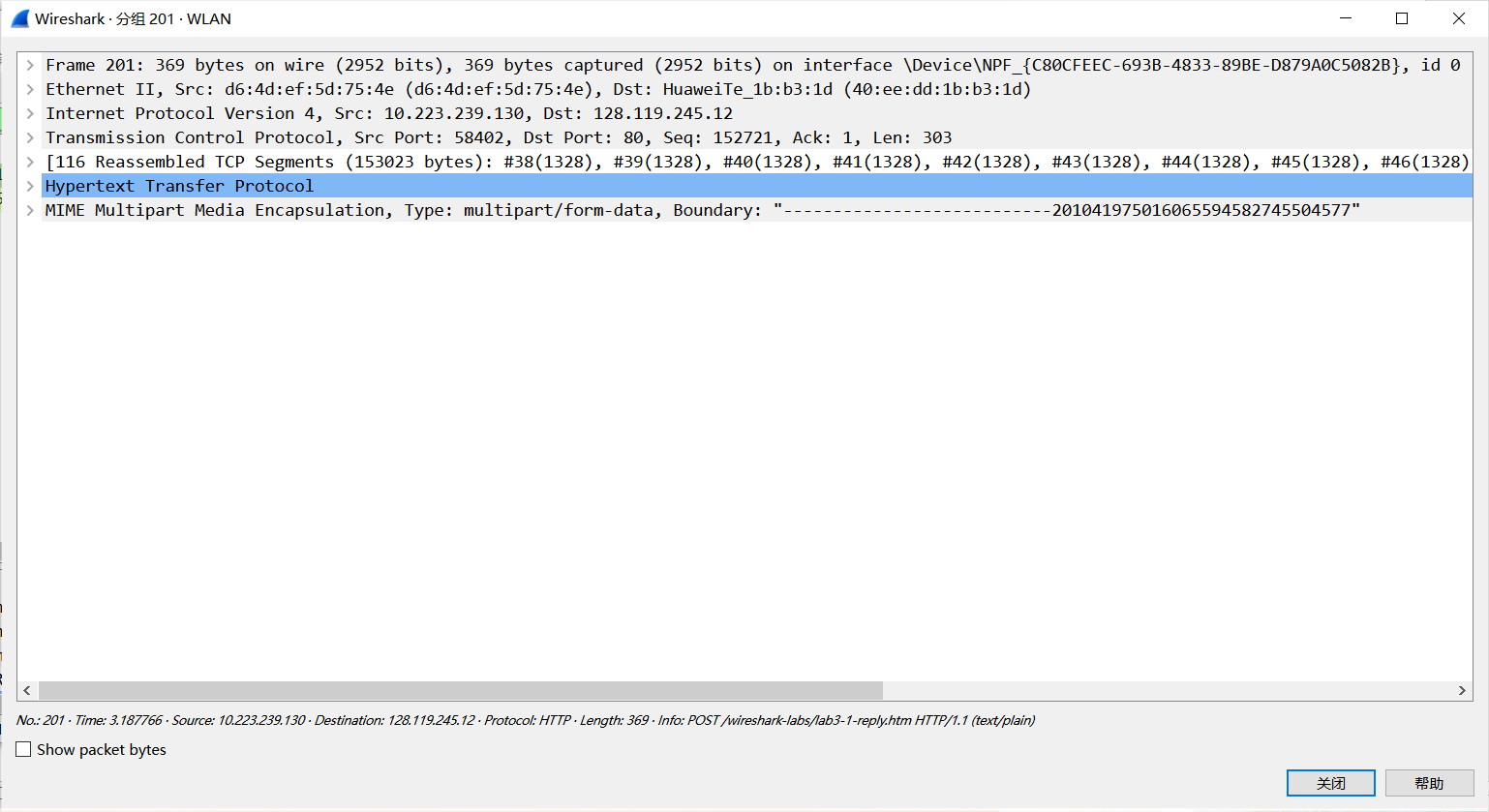
2. 查看捕获结果

（1）将文件传输到服务器的源IP地址和源TCP端口号是什么？筛选出对应 HTTP 消息并查看用于携带此 HTTP 消息的 TCP 数据包的详细信息。



源ip地址为10.223.239.130

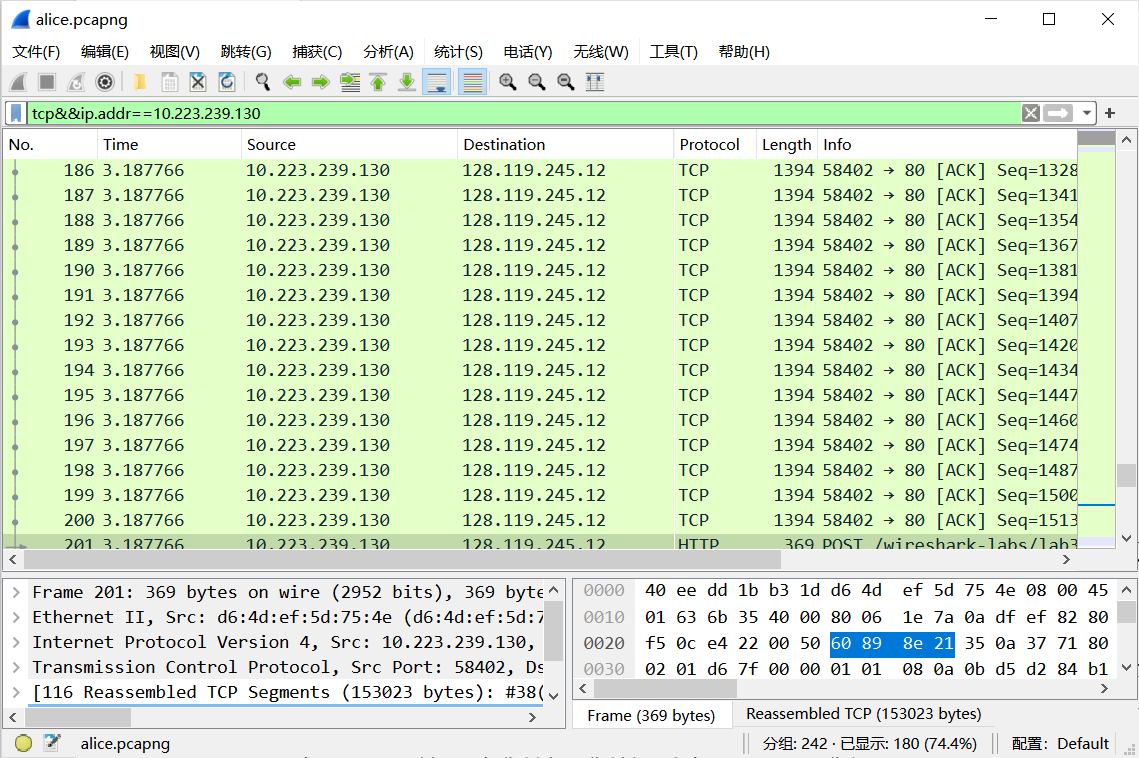
源TCP端口号为58402

（2）服务器的IP地址是什么？端口号是哪个？

服务器的ip地址为128.119.245.12

服务器端口号为80

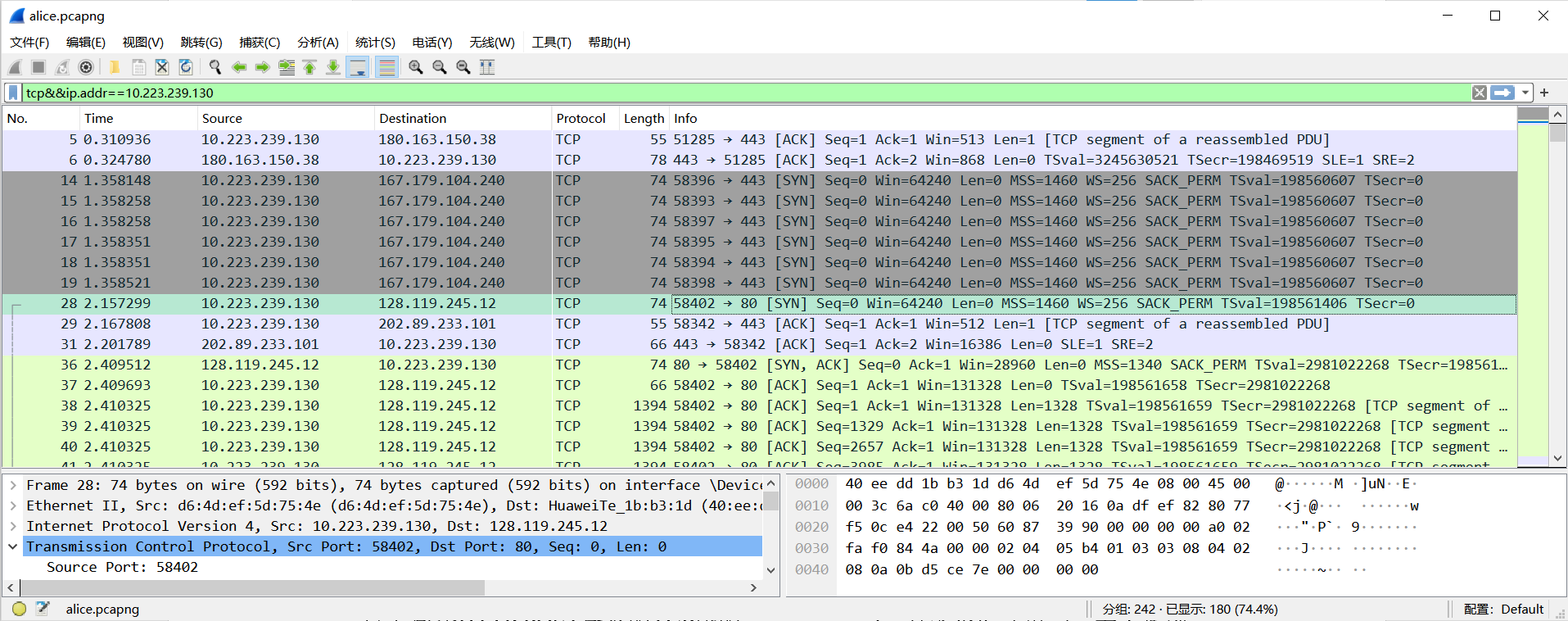
接着根据本地ip地址或源ip地址，以及tcp条件进行筛选。



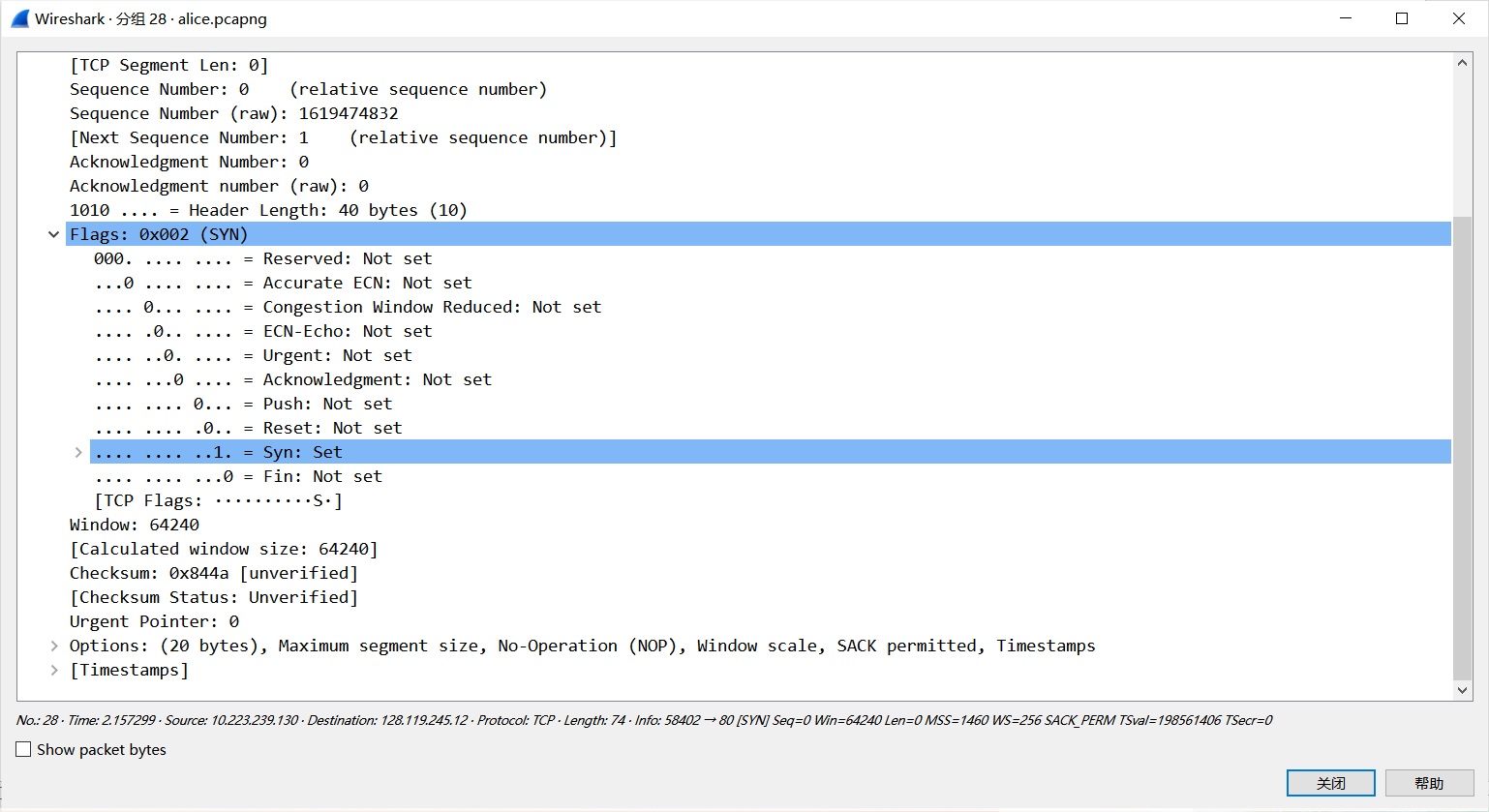
3. TCP 基础

根据TCP段的内容回答以下问题：

（3）用于启动客户端计算机与服务器之间TCP连接的TCP SYN段的sequence number是多少？是什么字段将该段标识为SYN段？



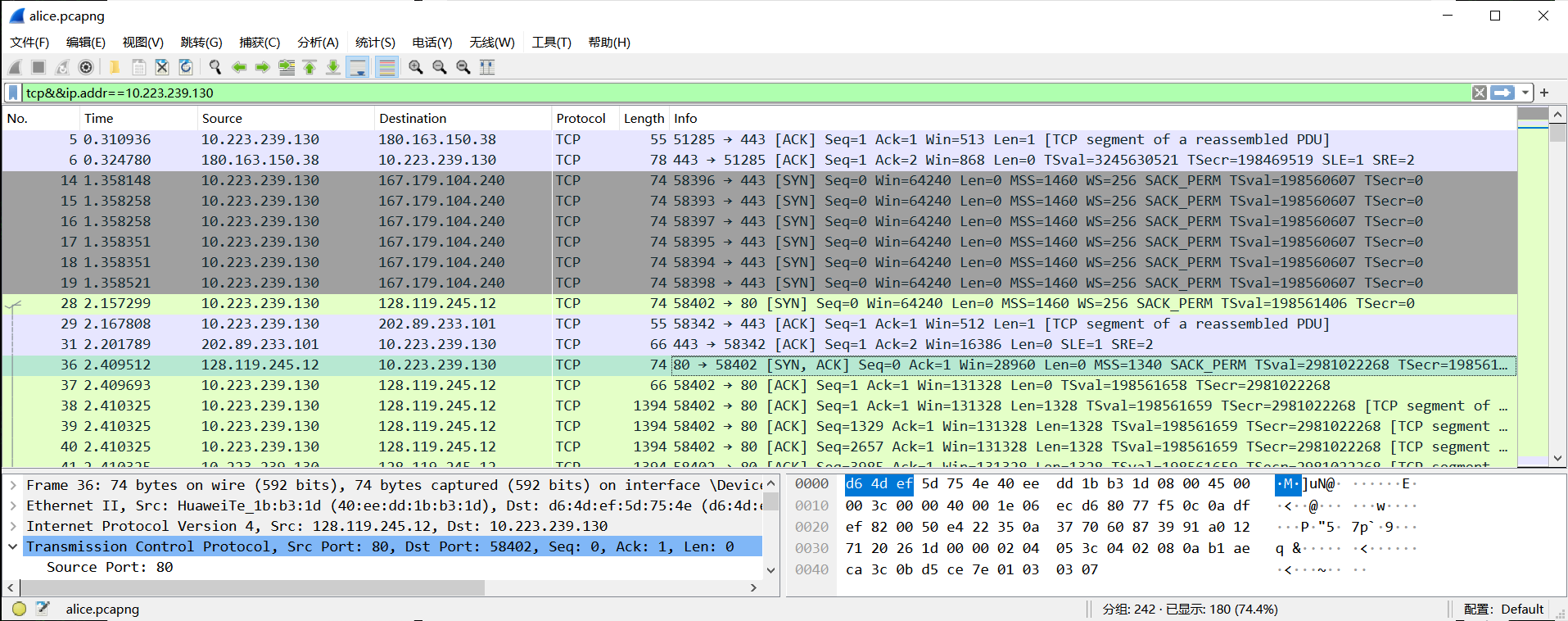
Seq=0。



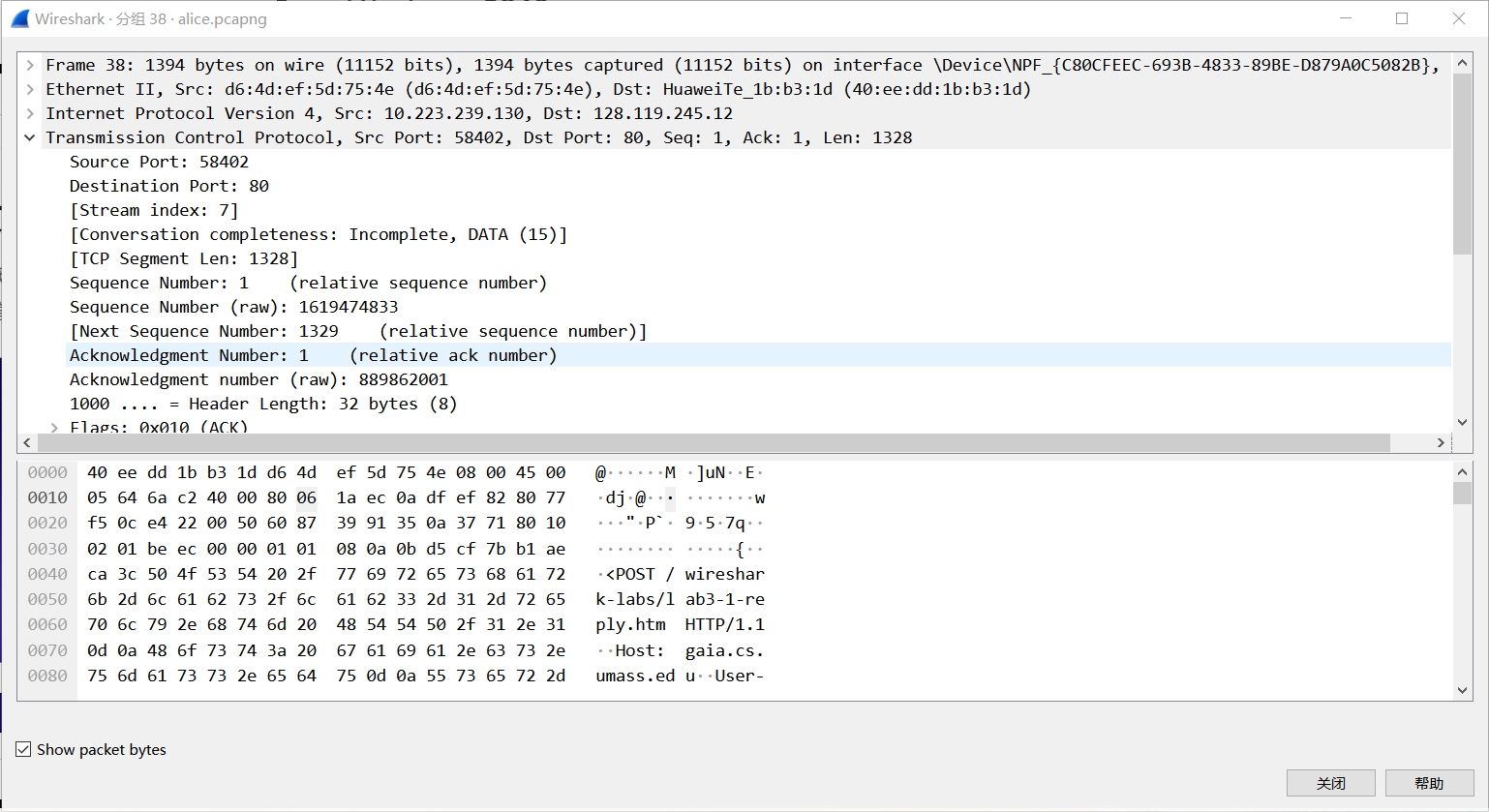
可以看见，flags中只有Syn字段有效，将该段标识为SYN段。

（4）服务器发送给客户端计算机来回复SYN的SYNACK段的sequence number是多少？ SYNACK 段中的 Acknowledgment 字段的值是多少？服务器是如何确定该值的？是什么字段将该段标识为SYN ACK段？

Seq=0，ack=1。ACK字段用于表示确认字段中的值是有效的，说明服务器成功接收了我们发出的连接请求。Acknowledgment和Syn字段将该段标识为SYN ACK段。

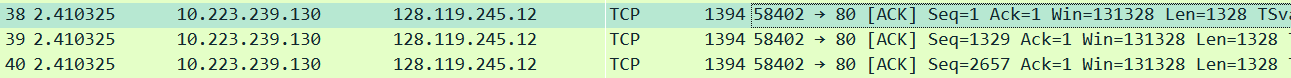


（5）包含HTTP POST命令的TCP段的sequence number是多少？（提示：为了找到 POST 命令，需要查看 Wireshark 窗口底部的“16进制数据查看面板”中带有“POST”）



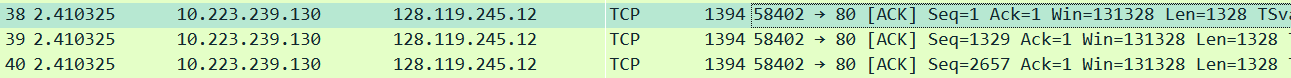
Seq=1

（6）将包含 HTTP POST 的 TCP 段视为 TCP 连接中的第一个段。 TCP 连接的前三个段（包括包含 HTTP POST 的段）的sequence number分别是多少？

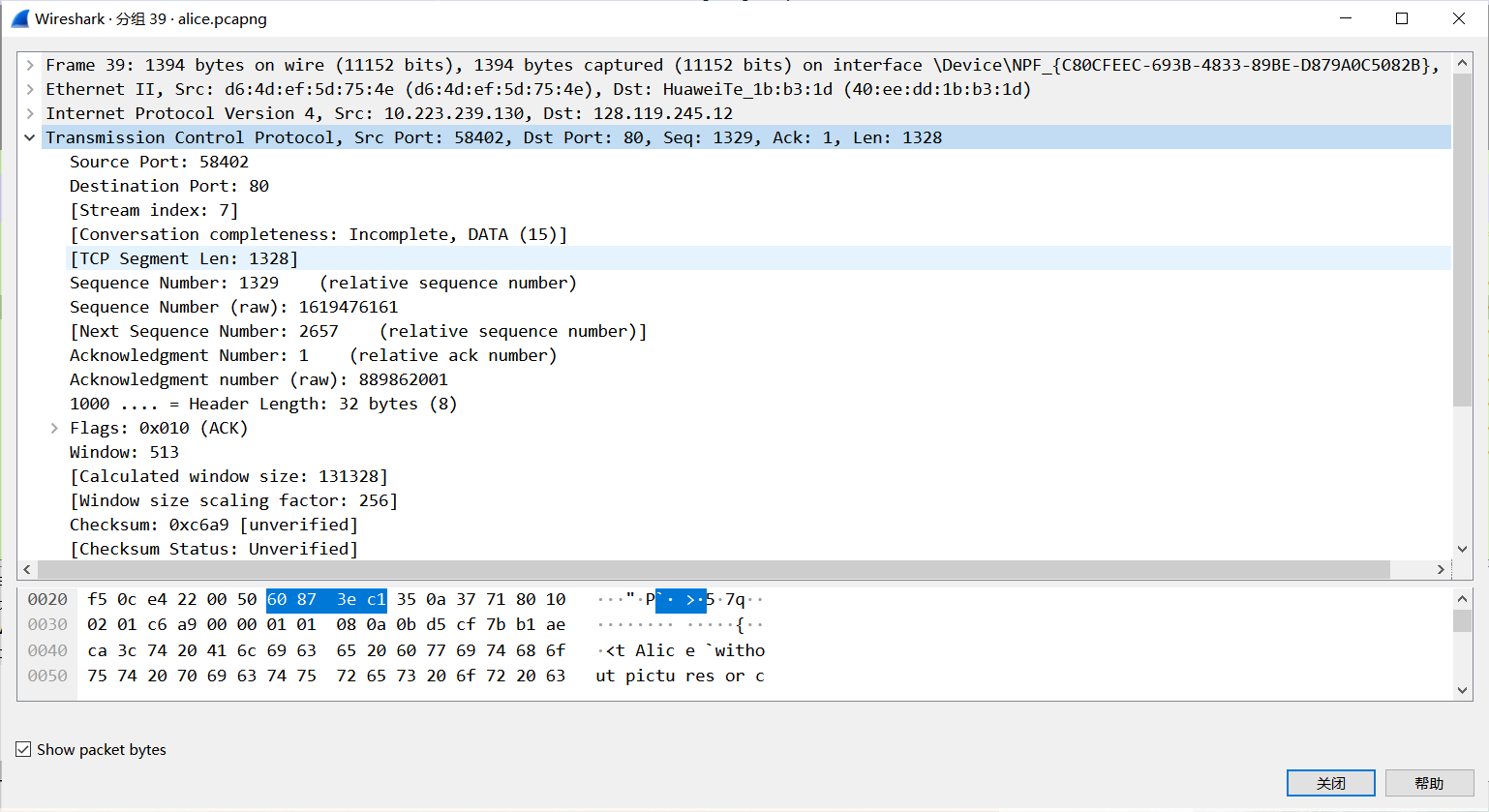


Seq分别是1，1329，2657

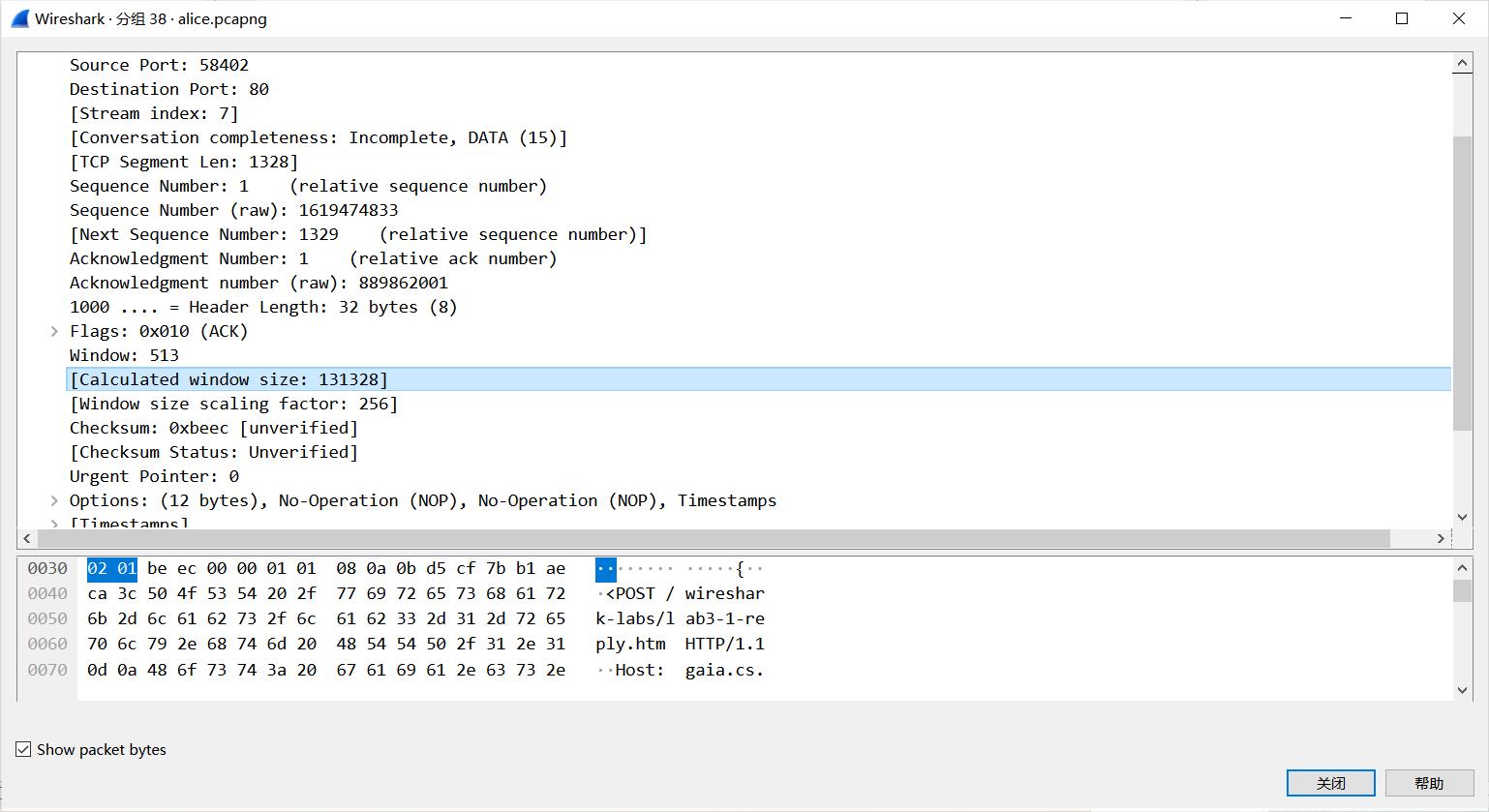
（7）包含 HTTP POST 的 TCP 段之后的那个TCP段的长度（TCP Segment Len）是多少？



在含POST的TCP段之后的TCP长度为1328



（8）可用缓冲区大小（看包含 HTTP POST 的 TCP 段的Win字段，即calculated window size）是多少？



Win的大小为131328