tcp协议中序列号和确认号的变化遵守以下规则：

1.SYN和FIN占用一个序列号，所以SYN和FIN进行握手和挥手时虽然不传送数据但依然会改变SEQ号和ACK号。

2.每个SOCKET都维护自己的SEQ号和ACK号，当要发送数据时从本地的SEQ号和ACK号中读取它们的值并写入报文中。

(1)本地SEQ号变化的情况为：当要发送一个报文时，直接读取本地SEQ号写入要发送的报文中。发送报文后本地SEQ号加上要发送的字节大小成为新的本地SEQ号。（如果发送的是SYN和FIN报文，虽然发送的数据字节数为0但要在发送之后SEQ自加1）

(2)本地ACK号变化的情况为：当接收到一个报文时，接收到的报文中的SEQ号加上接收到的数据字节数就成为本地ACK号的新值。（如果接收到的是SYN和FIN报文，虽然接收到的数据字节数为0但本地ACK号也要自加1）

3.TCP建立连接后SEQ号是从一个随机值开始。wireshark中之所以显示是从0开始是因为它显示的是相对的SEQ号。

4. 通常T C P在接收到数据时并不立即发送A C K；相反，它推迟发送，以便将ACK与需要沿该方向发送的数据一起发送（有时称这种现象为数据捎带ACK）。绝大多数实现采用的时延为 200 ms，也就是说，TCP将以最大200 ms的时延等待是否有数据一起发送。