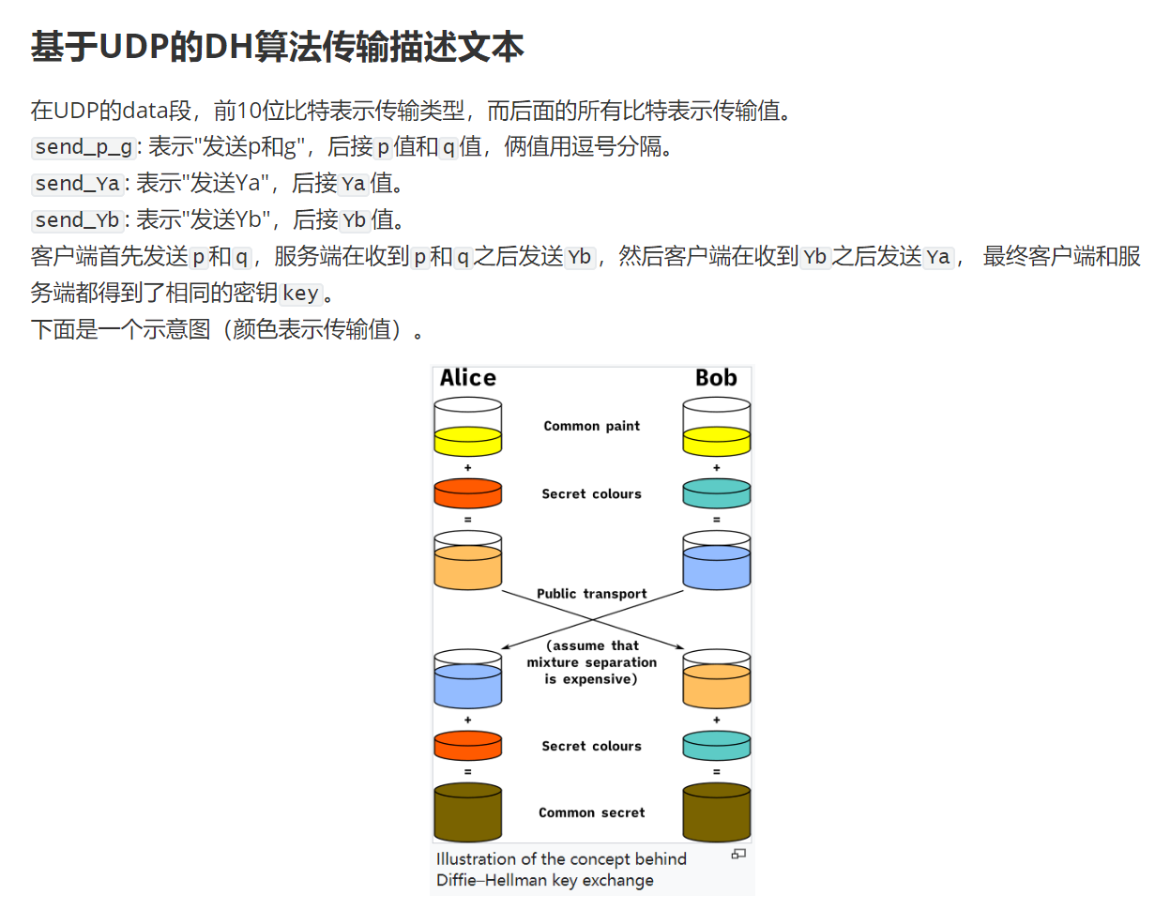
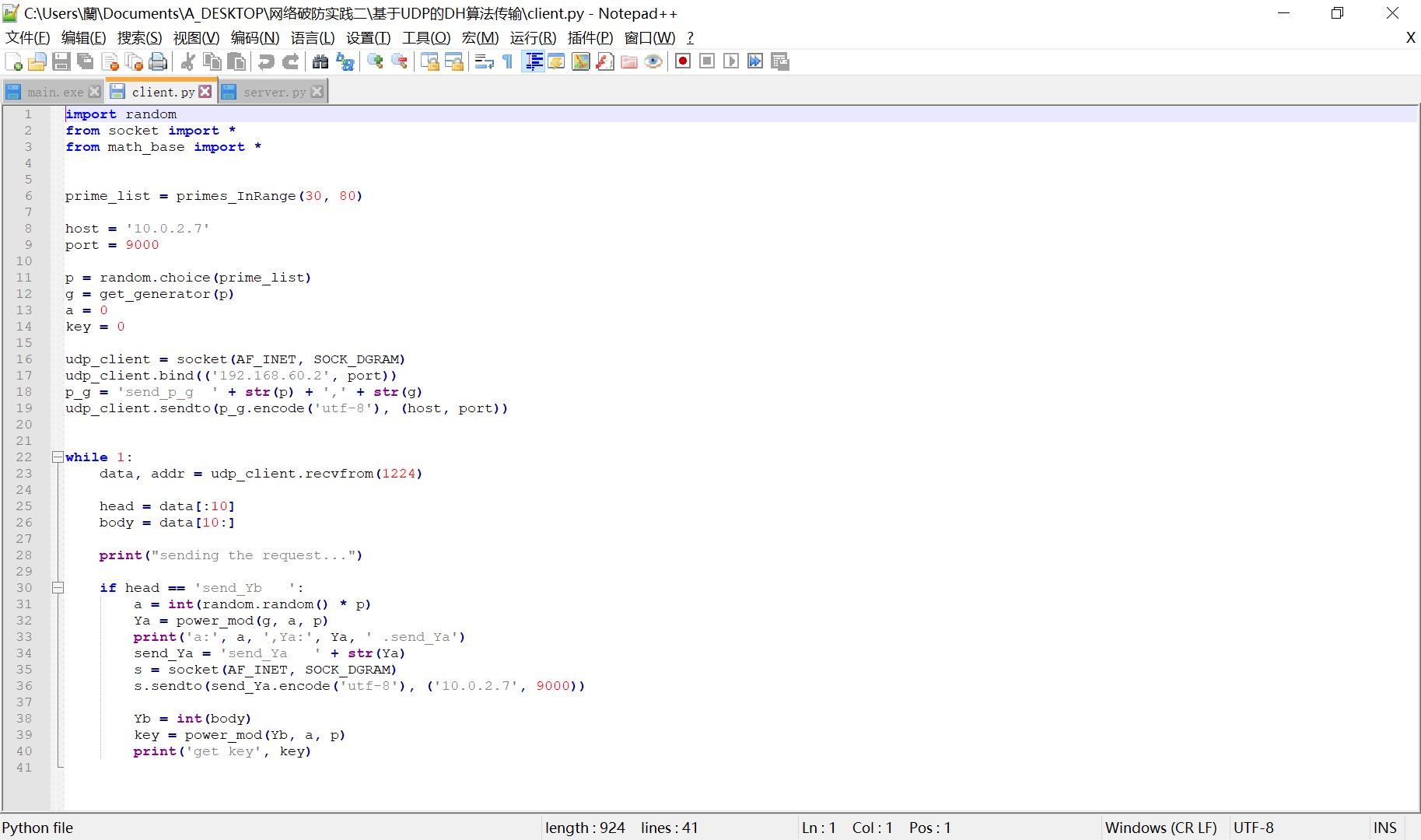
**第一题**

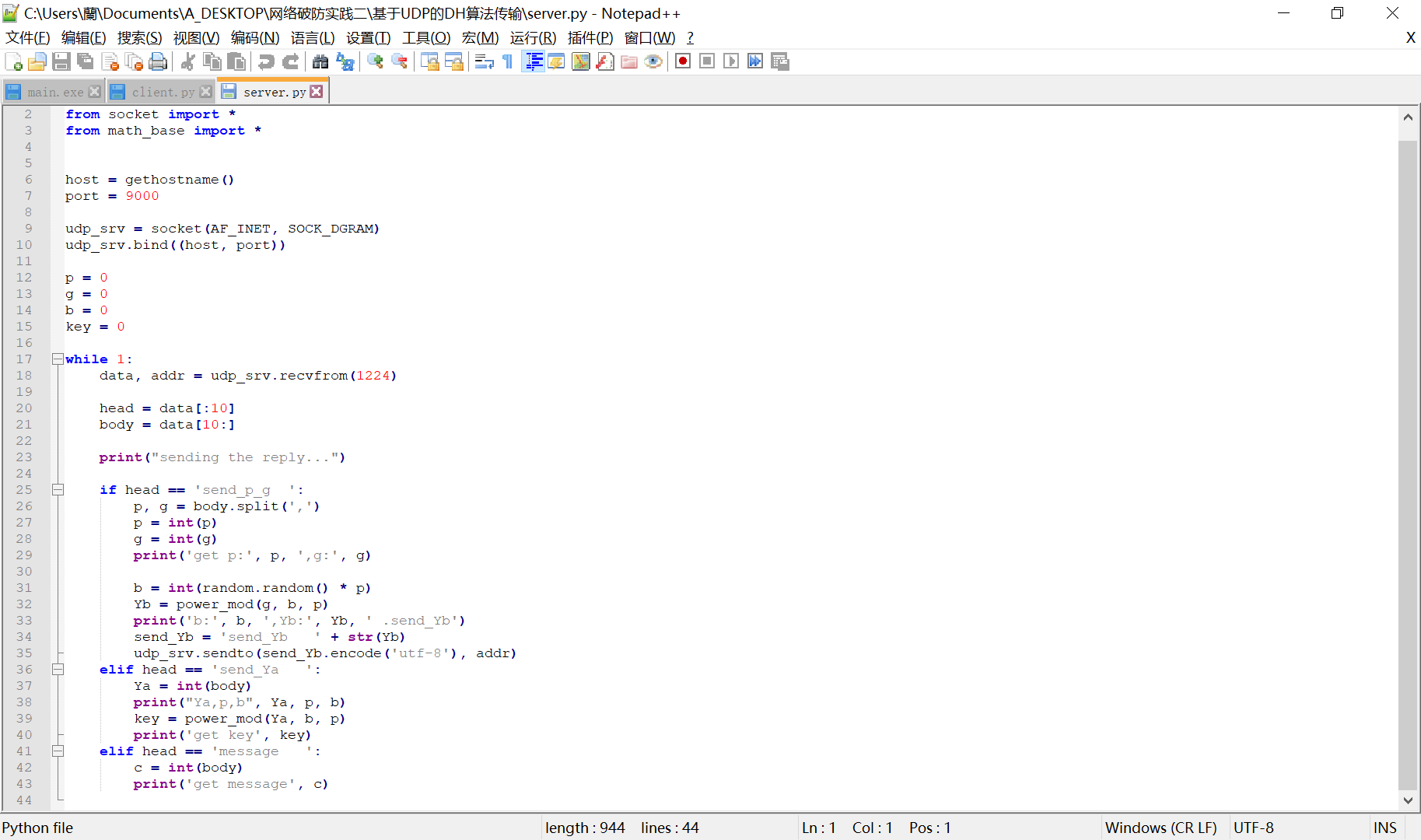
1. DH密钥协商描述文本如markdown所示：



2. 客户端程序如下：



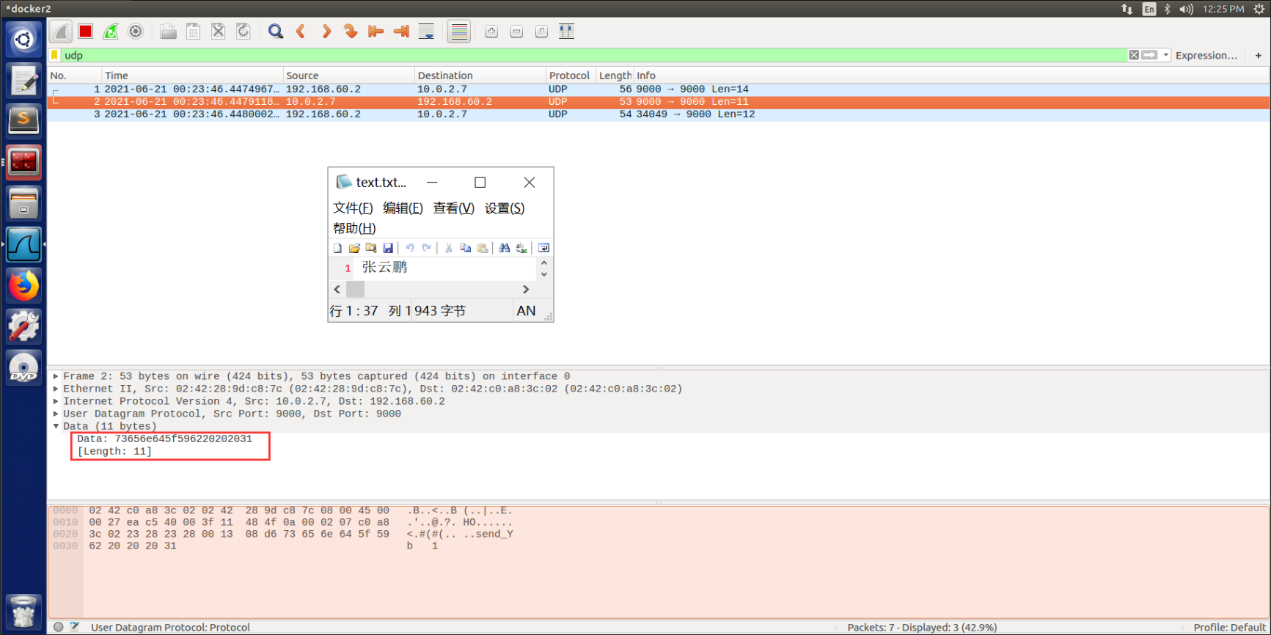
服务端程序如下：



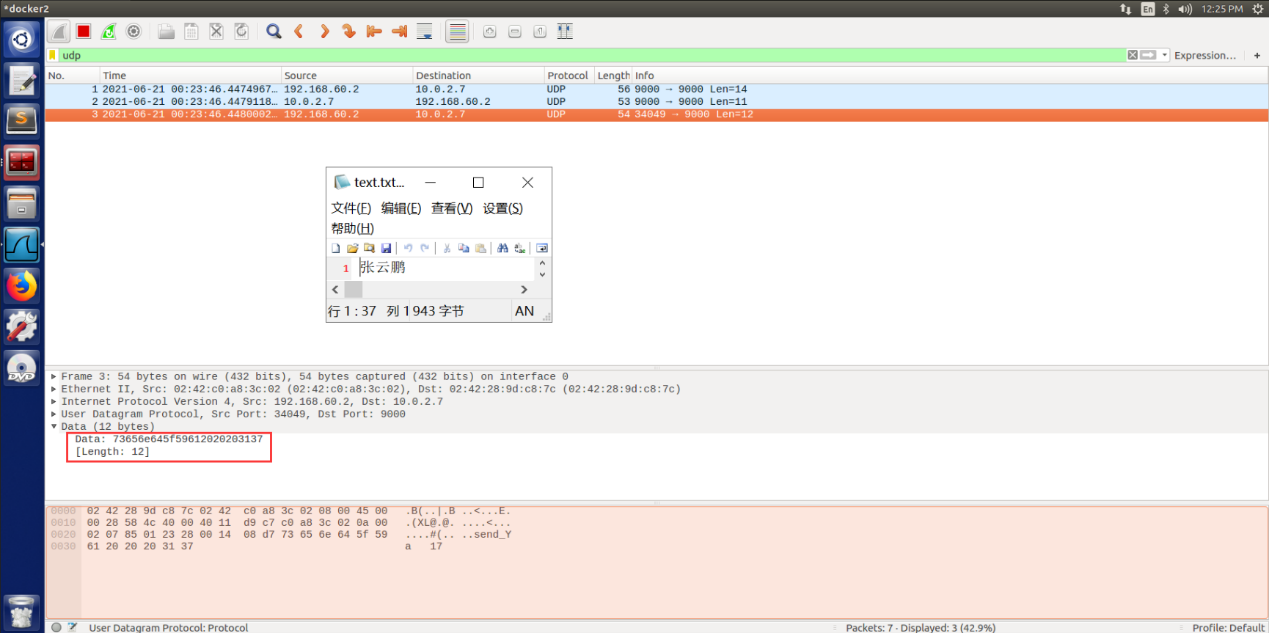
3. send\_p\_q:



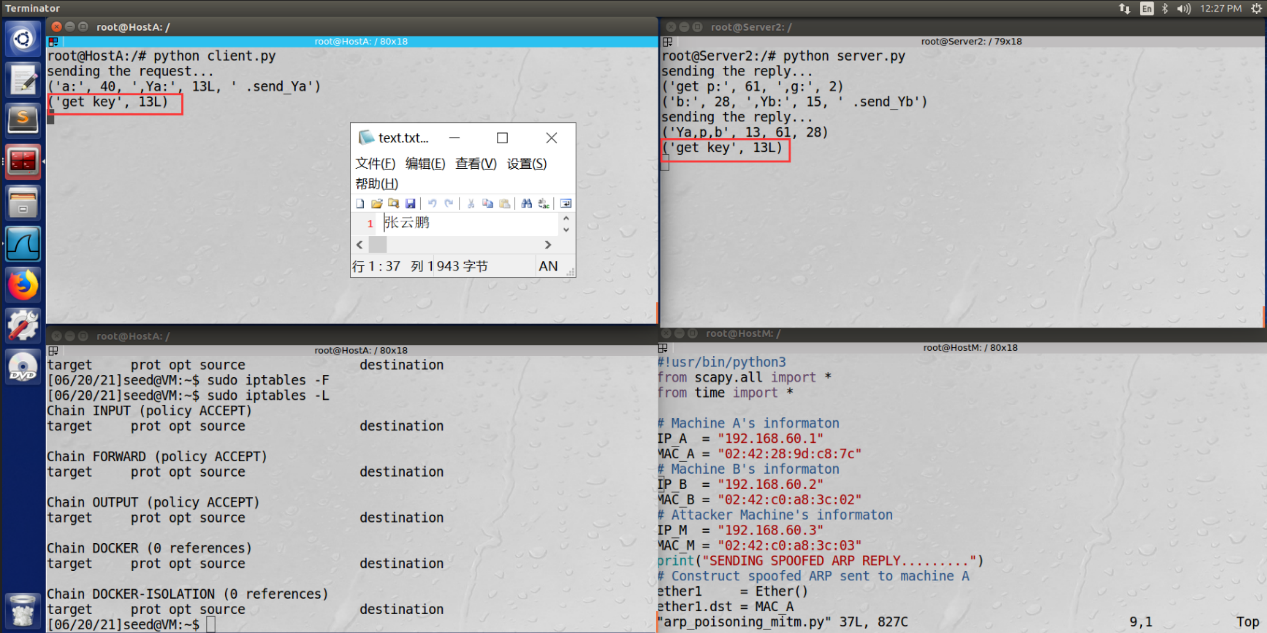
send\_Yb:



send\_Ya:

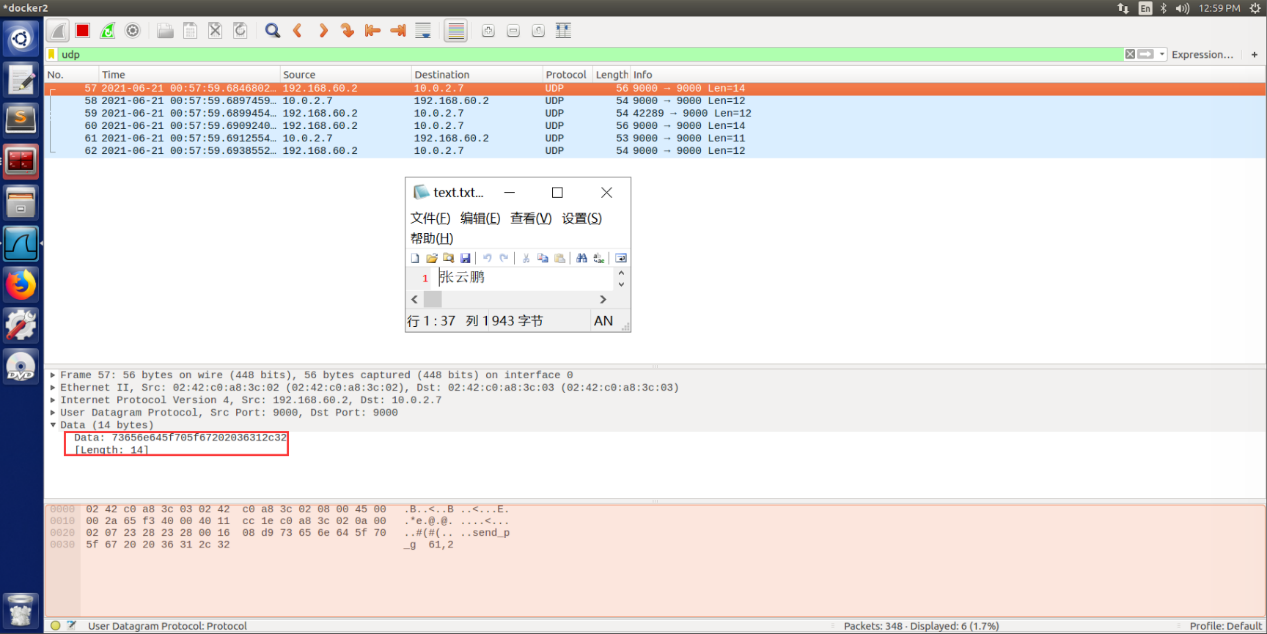


4. 会话密钥结果如下：

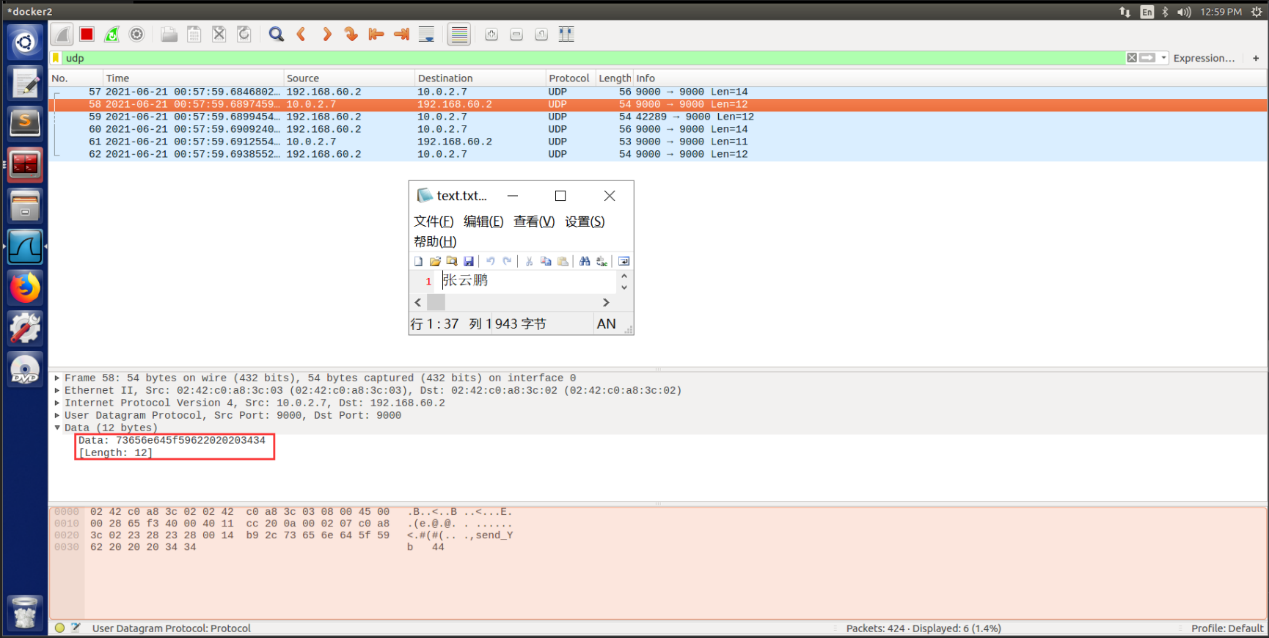


**第二题**

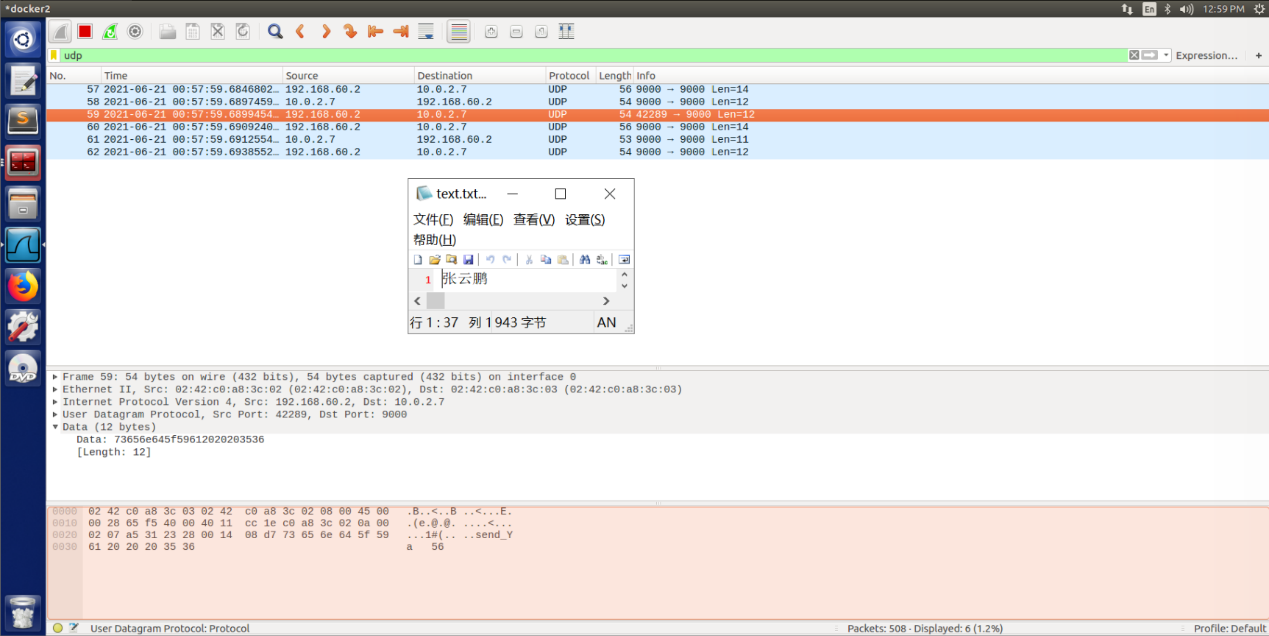
1. A先发送send\_p\_g给M:



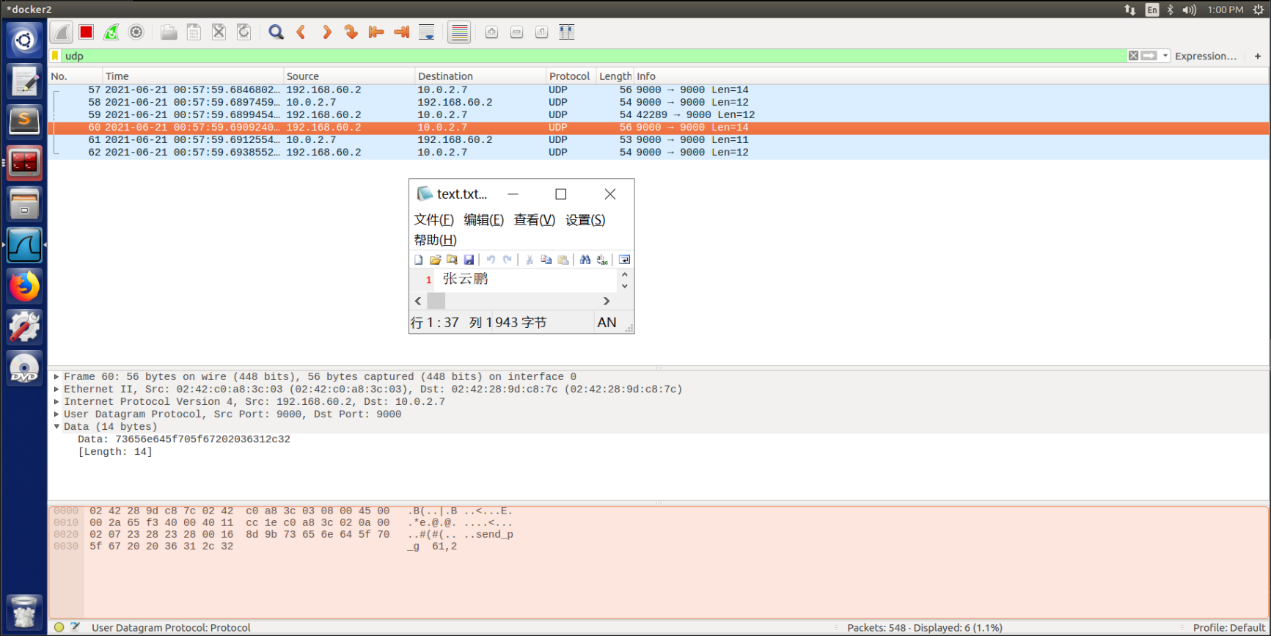
M冒充Server2回复A的send\_Yb：



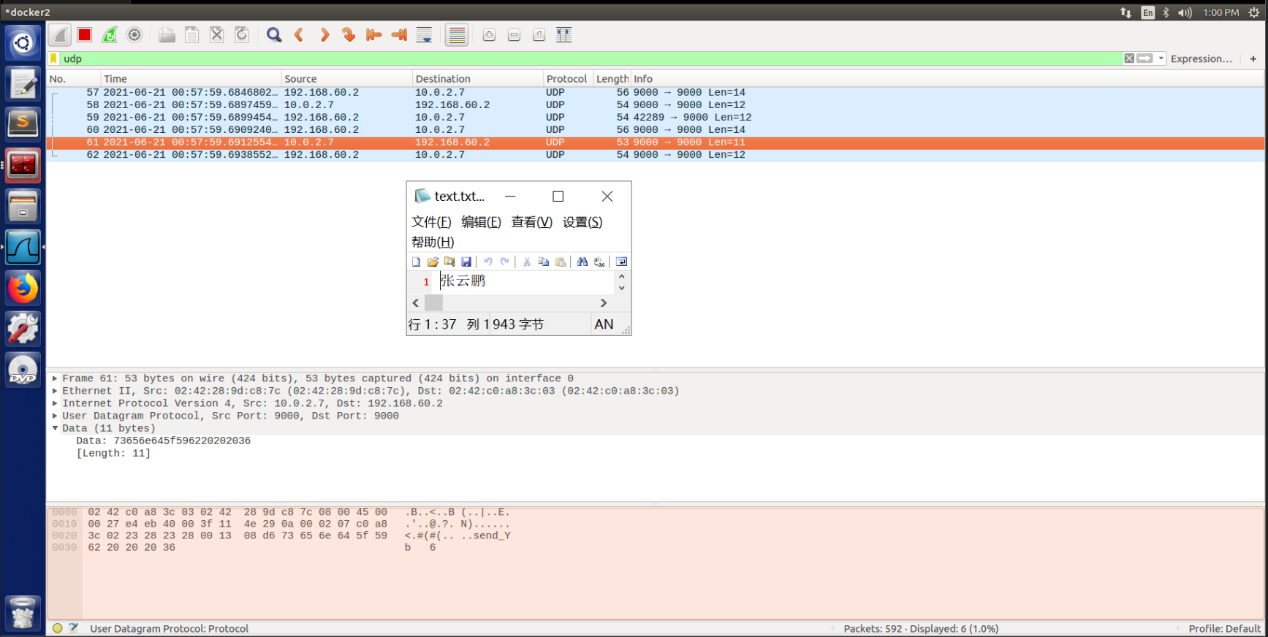
A回复M的send\_Ya：



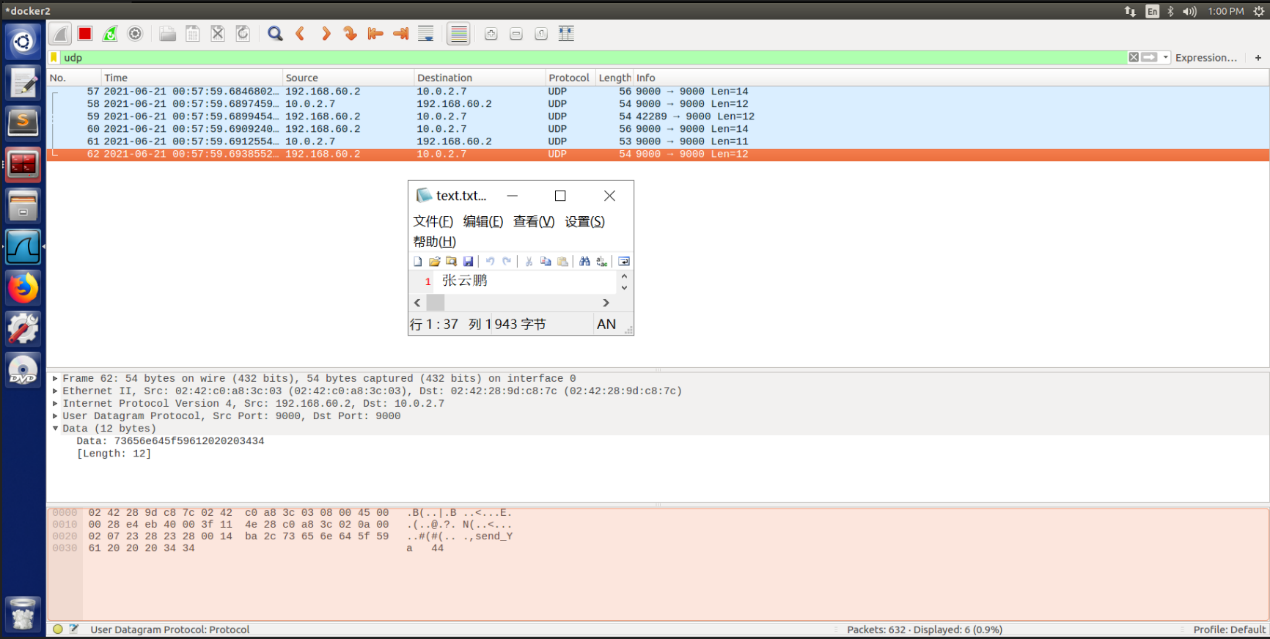
2. M冒充A给S发的send\_p\_g:



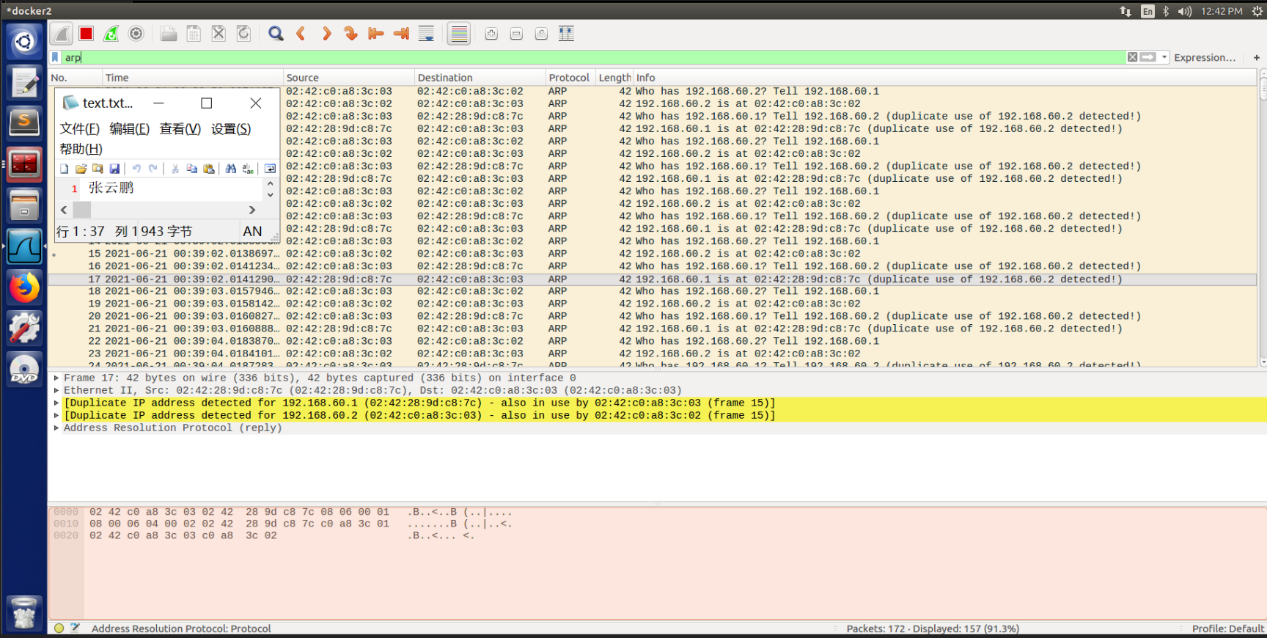
S返回给M的send\_Yb:



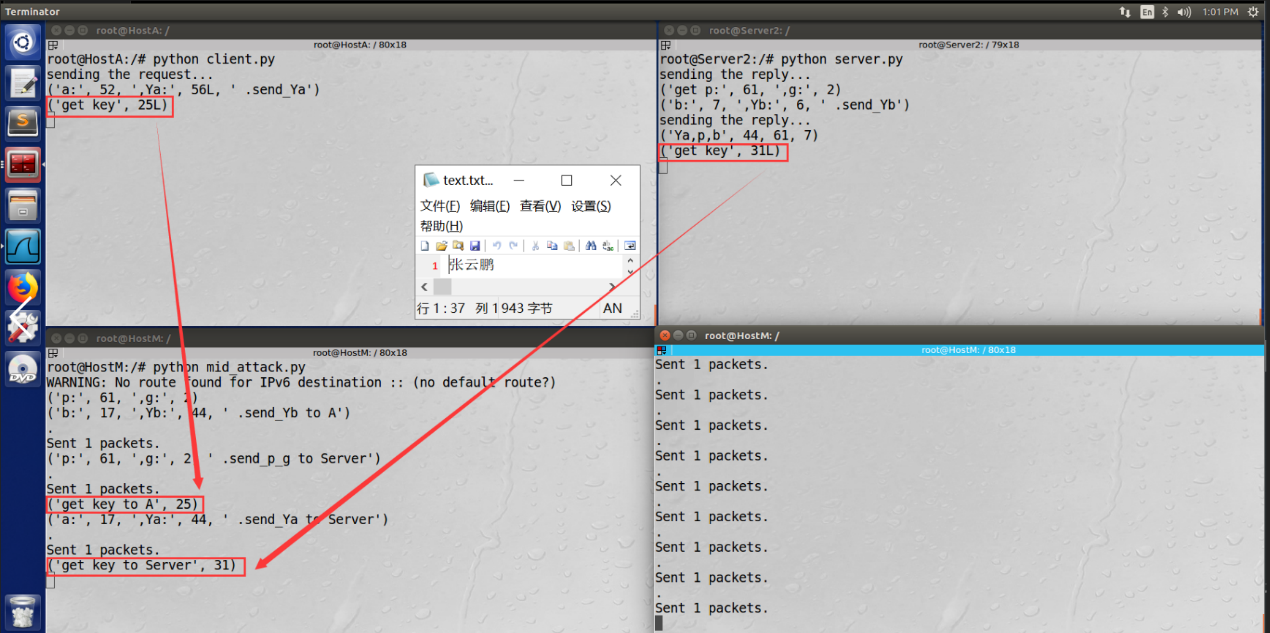
M返回给S的send\_Ya:



3. 期间我们用到了王美珍老师教的arp欺骗，欺骗过程如下：



协商密钥结果如下：

​

可见结果相同，中间人攻击成功。