P17. 图 8-19 显示了 Alice 必须执行 PGP 的操作，以提供机密性、鉴别和完整性。图示出当 Bob 接收来自 Alice 的包时必须执行的对应操作。

P18. 假定 Alice 要向 Bob 发送电子邮件。Bob 具有一个公共 - 私有密钥对（K_B^+，K_B^-），并且 Alice 具有 Bob 的证书。但 Alice 不具有公钥私钥对。Alice 和 Bob（以及全世界）共享相同的散列函数$H(\cdot)$。

a. 在这种情况下，能设计一种方案使得 Bob 能够验证 Alice 创建的报文吗？如果能，用方框图显示 Alice 和 Bob 是如何做的。

b. 能设计一个对从 Alice 向 Bob 发送的报文提供机密性的方案吗？如果能，用方块图显示 Alice 和 Bob 是如何做的。

P19. 考虑下面对于某 SSL 会话的一部分的 Wireshark 输出。

a. Wireshark 分组 112 是由客户还是由服务器发送的？

b. 服务器的 IP 地址和端口号是什么？

c. 假定没有丢包和重传，由客户发送的下一个 TCP 报文段的序号将是什么？

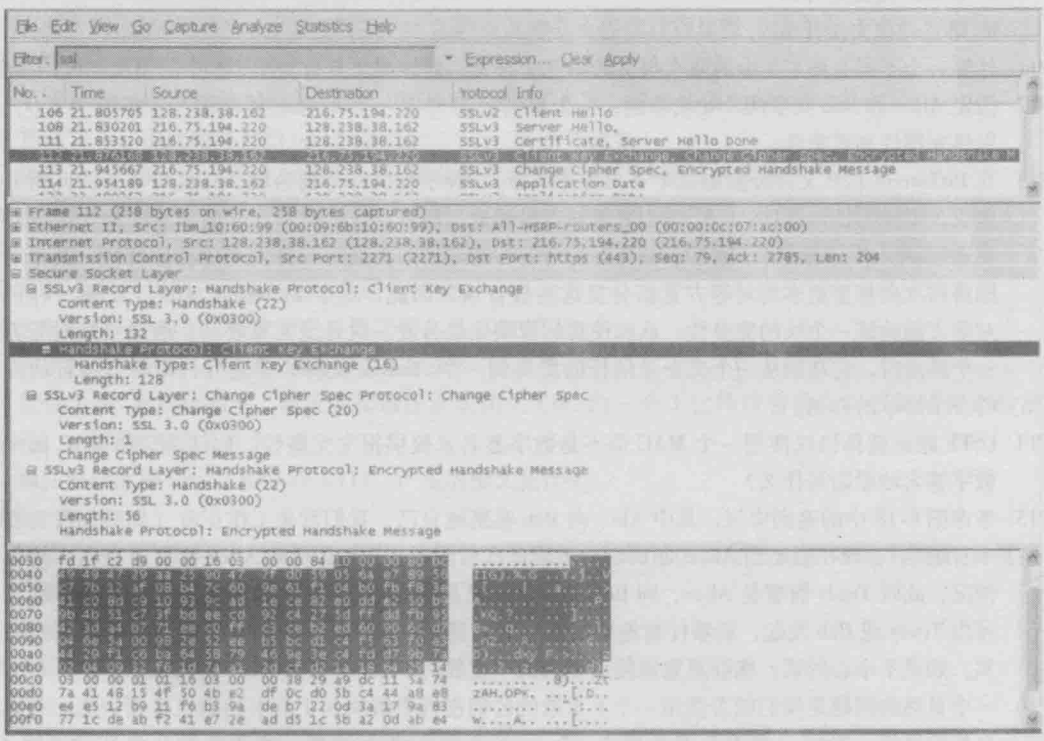
d. Wireshark 分组 112 包含了多少个 SSL 记录？

e. 分组 112 包含了一个主密钥或者一个加密的主密钥吗？或者两者都不是？

f. 假定握手类型字段是 1 字节并且每个长度字段是 3 字节，主密钥（或加密的主密钥）的第一个和最后一个字节的值是什么？

g. 客户加密的握手报文考虑了多少 SSL 记录？

h. 服务器加密的握手报文考虑了多少 SSL 记录？



（Wireshark 屏幕截图的重印获得 Wireshark 基金会的许可）

P20. 8.6.1 节中表明，不使用序号，Trudy（一名中间人）能够在一个 SSL 会话中通过互换 TCP 报文段实施破坏。Trudy 能够通过删除一个 TCP 报文段做某种类似的事情吗？在该删除攻击中，她需要做什么才能成功？它将具有什么影响？

P21. 假定 Alice 和 Bob 通过一个 SSL 会话通信。假定一个没有任何共享密钥的攻击者，在某分组流中插