号，通过在 MAC 的计算中包括适当的序号，使她验证一条记录的数据完整性。SSL 序号的使用阻止了 Trudy 执行诸如重排序或重放报文段等中间人攻击。（为什么?）

4. SSL 记录

SSL 记录（以及类 SSL 记录）显示在图 8-26 中。该记录由类型字段、版本字段、长度字段、数据字段和 MAC 字段组成。注意到前三个字段是不加密的。类型字段指出了该字段是握手报文还是包含应用数据的报文。它也用于关闭 SSL 连接，如下面所讨论。在接收端的 SSL 使用长度字段以从到达的 TCP 字节流中提取 SSL 记录。版本字段是自解释的。

图 8-26 SSL 记录格式

8.6.2 更完整的描述

前一小节涉及了类 SSL 协议；其目的是让我们对 SSL 的工作原理和工作过程有一个基本理解。既然我们已经对 SSL 有了基本了解，就能够更深入地研究实际 SSL 协议的要点了。为了配合阅读对 SSL 协议的描述，鼓励读者完成 Wireshark SSL 实验，它在本书配套的 Web 网站上可供使用。

1. SSL 握手

SSL 并不强制 Alice 和 Bob 使用一种特定的对称密钥算法、一种特定的公钥算法或一种特定的 MAC。相反，SSL 允许 Alice 和 Bob 在握手阶段在 SSL 会话开始时就密码算法取得一致。此外，在握手阶段，Alice 和 Bob 彼此发送不重数，该数被用于会话密钥（E_B，M_B，E_A 和 M_A）的生成中。真正的 SSL 握手的步骤如下：

1）客户发送它支持的密码算法的列表，连同一个客户的不重数。

2）从该列表中，服务器选择一种对称算法（例如 AES）、一种公钥算法（例如具有特定密钥长度的 RSA）和一种 MAC 算法。它把它的选择以及证书和一个服务器不重数返回给客户。

3）客户验证该证书，提取服务器的公钥，生成一个**前主密钥**（Pre-Master Secret，PMS），用服务器的公钥加密该 PMS，并将加密的 PMS 发送给服务器。

4）使用相同的密钥导出函数（就像 SSL 标准定义的那样），客户和服务器独立地从 PMS 和不重数中计算出**主密钥**（Master Secret，MS）。然后该 MS 被切片以生成两个密码和两个 MAC 密钥。此外，当选择的对称密码应用于 CBC（例如 3DES 或 AES），则两个初始化向量（Initialization Vector，IV）也从该 MS 获得，这两个 IV 分别用于该连接的两端。自此以后，客户和服务器之间发送的所有报文均被加密和鉴别（使用 MAC）。

5）客户发送所有握手报文的一个 MAC。

6）服务器发送所有握手报文的一个 MAC。

最后两个步骤使握手免受篡改危害。为了理解这一点，观察在第一步中，客户通常提供一个算法列表，其中有些算法强，有些算法弱。因为这些加密算法和密钥还没有被协商好，所以算法的这张列表以明文形式发送。Trudy 作为中间人，能够从列表中删除较强的