5.4.1 更换解析器

Wireshark 使用解析器来识别每个协议并且决定该如何显示网络信息。不幸的是，Wireshark 在给一个数据包选择解析器时也并不是每次都能选对，尤其是当网络上的一个协议使用了不同于标准的配置时，比如非缺省端口（网络管理员通常会出于安全考虑，或者是员工想要避开访问控制而进行设置）。

当错误地应用解析器时，我们可以人为地干预 Wireshark 的选择。举例来说，打开 wrongdissector.pcapng 这个捕获文件，可以注意到这个文件中包含了大量两台计算机之间的 SSL 通信。SSL 是安全接口层协议（Secure Socket Layer protocol），用来在主机之间进行安全加密的传输。由于其保密性，因此大多数的正常情况下，在 Wireshark 中查看 SSL 流量不会产生什么有用的信息，但这里一定存在着一些问题。如果你单击其中的几个数据包，然后在 Packet Bytes 面板中仔细查看这几个数据包的内容，很快就会发现一些明文流量。事实上，如果你看第 4 个数据包，就会发现其中提到了 FileZilla FTP 服务器程序（FileZilla FTP server application），并且之后的几个数据包清晰地显示了对于用户名和密码的请求与响应。

如果这真是 SSL 流量，那么你应该不会读到数据包中的任何数据，并且你也不会看到以明文传输的所有用户名和密码（见图 5-11）。根据这些信息，我们可以推测出这应该是一个 FTP 流量而不是 SSL 流量，而导致错误选择解析器的原因应该是这个 FTP 流量使用了原本用作 HTTPS（基于 SSL 的 HTTP）标准端口的 443 端口。

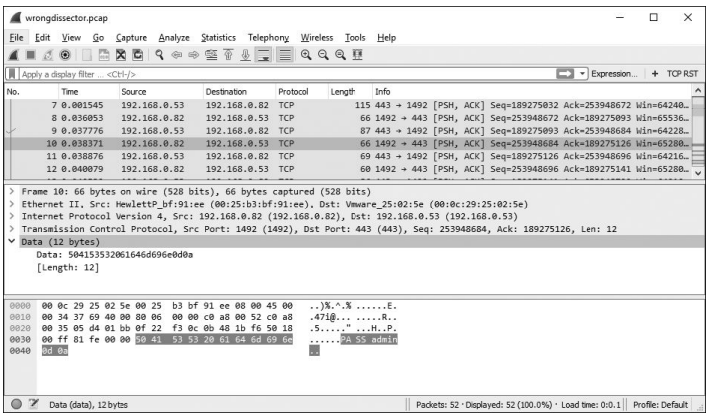

图 5-11　明文用户名和密码？这更像是 FTP 而不是 SSL！

为了解决这个问题，你可以强制 Wireshark 对这个数据包使用 FTP 协议解析器。这个过程被称为强制解码，需要按如下操作。

（1）在协议列右键单击其中一个 SSL 数据包（比如第 30 号包），选择 Decode As。这时会弹出一个对话框，你可以从中选择想要使用的解析器，如图 5-12 所示。

（2）在下拉菜单中选择 destination（443），并在 Transport 选项卡中选择 FTP，以便让 Wireshark 使用 FTP 解析器对所有端口号为 443 的 TCP 流量进行解码（见图 5-12）。

（3）在你选好之后单击 OK，就可以立刻将修改应用到捕获文件中去。

数据已经被解码为 FTP 流量，这时你就可以从 Packet List 面板中对它进行分析，而不是对每一个字节下功夫（见图 5-13）。

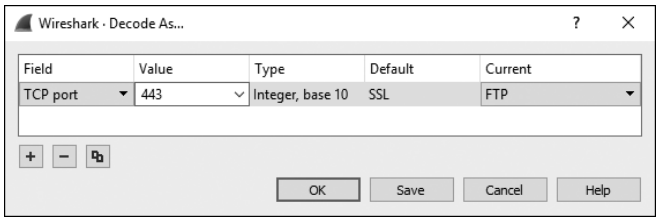

图 5-12　Decode As 对话框可以让你进行强制解码

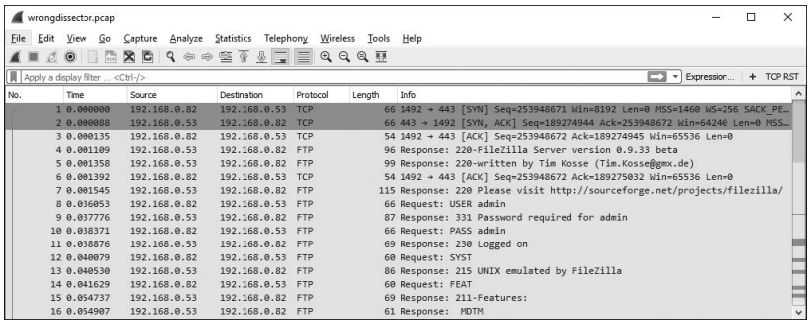

图 5-13　查看被解码为 FTP 的流量

你可以在同一个捕获文件中多次使用强制解码功能。Wireshark 将在 Decode As...对话框中跟踪你的强制解码操作，在这里你可以查看并编辑之前创建的强制解码。

在默认情况下，当你关掉捕获文件时强制解码的设置不会保存。补救方法就是在 Decode As...对话框中单击 Save 按钮。这会将协议解码规则保存到你的 Wireshark 用户配置文件中，因此当你使用该配置文件打开任意捕获文件时，它们将会生效。要移除之前保存的解码规则，你可以在对话框中单击减号按钮。

把保存了的解码规则忘到脑后是很容易的。这会造成很多混乱，因此要多留意强制解码规则。要避免自己掉入这个大坑，我在自己的主要 Wireshark 设置档案里一般避免保存强制解码设置。