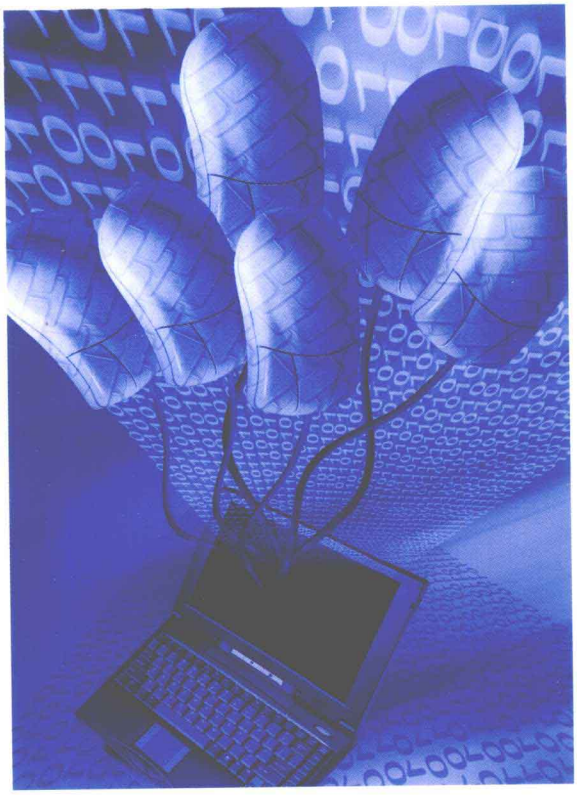
高等学校计算机应用规划教材

计算机网络安全教程

- 网络协议及网络安全基础
- 计算机物理安全
- 操作系统安全
- 密码学基础
- 身份认证与访问控制
- 数据库安全
- 恶意软件概念及防范
- Internet安全协议
- 公钥基础设施——PKI
- 网络安全技术
- 无线网络安全技术
- 数据备份
- 信息安全评测与风险评估
- 计算机网络安全管理



勇　卢浩　黄继军　编著

清华大学出版社

高等学校计算机应用规划教材

计算机网络安全教程

石 勇　卢 浩　黄继军　编著

清华大学出版社
北　京

内 容 简 介

本书从网络安全的理论基础着手，同时兼顾实际工作中的应用，深入浅出地介绍了网络协议的基础知识、网络安全基础、计算机物理安全、操作系统安全基础、密码学基础、身份认证与访问控制、数据库安全、恶意软件概念及防范、Internet 安全协议、公钥基础设施——PKI、网络安全技术、无线网络安全技术、网络应用安全、数据备份、信息安全评测与风险评估和计算机网络安全管理等内容，书中通过大量实例、图文并茂的说明，使读者能在最短的时间内理解消化相关知识，并能学以致用，每章结尾均配有课后习题供读者练习巩固。按照本书的内容，逐步学习，并加以实践操作，即可掌握相关的技术内容。

本书可作为高等学校计算机网络安全课程的教材，也可供广大网络管理员参考。

图书在版编目(CIP)数据

计算机网络安全教程/石勇，卢浩，黄继军 编著. —北京：清华大学出版社，2012.1

(高等学校计算机应用规划教材)

ISBN 978-7-302-26962-5

Ⅰ. 计… Ⅱ. ①石… ②卢… ③黄… Ⅲ. 计算机网络—安全技术—高等学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2011)第 198247 号

责任编辑：刘金喜　胡花蕾

装帧设计：孔祥丰

责任校对：蔡　娟

责任印制：何　芊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座

http://www.tup.com.cn　　**邮　　编**：100084

社　总　机：010-62770175　　**邮　　购**：010-62786544

投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn

质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：三河市君旺印装厂

装 订 者：三河市新茂装订有限公司

经　　销：全国新华书店

开　　本：185×260　**印　张**：21.75　**字　数**：543 千字

版　　次：2012 年 1 月第 1 版　　**印　　次**：2012 年 1 月第1 次印刷

印　　数：1～4000

定　　价：35.00 元

产品编号：033733-01

前　言

计算机网络已逐步深入应用到政治、经济、军事等各个领域，以及人们工作和生活的方方面面，给国家、社会带来了巨大影响和深远变革，伴随而来的网络安全问题也逐步引起了人们的高度关注。

计算机网络安全保障是一项系统工程，包含诸多复杂的环节，任何一个环节的缺陷或问题，都会摧毁整个系统的安全防线。网络安全保障，需要从物理(实体)安全、运行安全、数据(信息)安全、管理(人员)安全几个方面全面着手。

本书共分为16章，编写时采用先理论分析为主，后侧重实践应用的思路。

第1章介绍了TCP/IP协议的基础知识，包括TCP/IP协议体系及其各层协议的主要功能、主要概念。

第2章介绍了网络安全的基础知识，包括网络安全的发展历程、安全威胁、安全需求分析、安全模型。

第3章介绍了物理安全，包括环境安全、机房安全、设备安全、突发事件应急计划。

第4章讲述了操作系统安全，包括Windows系统安全、Linux/UNIX系统安全、操作系统漏洞、操作系统入侵检测等内容。

第5章介绍了密码学基础知识，包括密码学的基本概念、对称密码算法、非对称密码算法、散列函数、数字签名等。

第6章阐述了身份认证与访问控制机制，包括身份认证与访问控制的基本概念、类型等内容。

第7章介绍了数据库安全相关内容，包括数据库安全特性、数据库安全威胁、数据库数据保护、数据库备份与恢复，以及SQL Server数据库安全机制。

第8章介绍了恶意软件概念及防范，包括恶意软件的分类和各类恶意软件的特征、运行症状、防范方法。

第9章介绍了网络安全相关的IPSec、TLS、Kerberos、SET等安全协议。

第10章介绍了PKI(公钥基础设施)，包括其概念、功能、组成、信任模型、相关标准等。

第11章介绍了网络安全相关的技术，包括防火墙、入侵检测、VPN等。

第12章阐述了移动通信网络与无线局域网的安全性分析及安全防护。

第13章介绍了应用安全，包括口令安全、网络监听、网络扫描、钓鱼攻击、Web安全等。

第14章介绍了数据库备份相关的数据存储技术、远程数据备份、个人数据备份。

第15章介绍了信息安全评测与风险评估。

第16章介绍了计算机网络安全管理相关原则、标准、法规。

本书通过大量的实例，力图避免网络协议、网络安全相关书籍枯燥抽象的通病，使读者能在最短的时间内学以致用。书中各章不仅详细介绍了实例的具体操作步骤，而且还配有一定数量的练习题供读者学习使用。读者只需按照书中介绍的步骤一步步地实际操作，就能完全掌握本书的内容。

本书可作为高等学校计算机网络安全课程的教材，也可供广大网络管理员参考。

本书编写人员分工如下：石勇编写第1～5章，卢浩编写第6～8章，黄继军编写第9～11章，程凤娟编写第12～16章。此外，苏兆锋、王雷、许云、苏小平、刘兰、王梅、张宏、孙浩、杨彬、关涛、苏玉林、于文杰等也参与了本书的编写和修改，在此向他们致以诚挚的谢意！

编者力图使本书的知识性和实用性相得益彰，但由于水平有限，书中错误、纰漏之处难免，欢迎广大读者、同仁批评斧正。

编　者

2011年4月

目　录

第1章　网络协议基础

信息革命是继农业革命、工业革命之后，人类历史上的第三次革命，它对整个人类社会及生活产生了深远的影响，目前，这种影响还在以超乎想象的速度持续进行着。

计算机网络是信息技术存在与发展的基石，是通信技术与计算机技术结合的产物。计算机网络利用通信设备和线路，将地理位置不同、功能独立的多个计算机系统相互连接起来，通过网络协议来实现信息传递和资源共享。

高速发展的信息技术，在大幅提高工作效率、提供种种生活便利的同时，也带来了日益严重的安全隐患。电影《虎胆龙威4》中利用计算机网络操纵国家基础设施进行犯罪的情节，绝非危言耸听。事实上，各行各业在信息化进程中，最容易被忽视，出现问题后最难挽回、弥补的一个环节，就是信息安全的保障。信息安全保障涉及多个方面，其中，计算机网络的复杂性、普通用户的低安全防范意识和低安全防范水平，使得计算机网络安全问题尤为突出。

要准确把握计算机网络安全的内涵，掌握计算机网络协议是其基本要求。理解计算机网络协议的基本运行原理，才能掌握看似简单的网络操作背后蕴含的多个环节，才能考察各个环节是否安全，才可能设法保障网络安全。计算机网络安全保障遵循“木桶原理”，一个环节出现问题，整个网络的安全都无从谈起。所以，对网络协议的全面领会，是保障计算机网络安全的基础。

通常，学习网络协议是一个枯燥乏味、令人生厌的过程，很容易让人感觉过于抽象，晦涩难懂，其实这是一个误解。事实上，网络协议时刻体现在每一个细微的网络操作中，本章将通过大量的实践案例，将网络协议的运行过程向读者展现出来，力图使网络协议的学习过程不再枯燥抽象、高深莫测。

本章重点

- TCP/IP 参考模型
- 数据在各层协议间的流动
- 链路层协议的主要功能、以太网、帧的概念
- 网络层协议的主要功能、主机端到端传输概念
- 传输层协议的主要功能、应用程序端到端传输概念
- 应用层 DNS、HTTP、FTP、SMTP、POP3 协议的基本概念

1.1 网络发展概述

根据中国互联网络信息中心(CNNIC)在北京发布的《第25次中国互联网络发展状况统计报告》，截至2009年12月，我国网民规模已达3.84亿，网络出口带宽达到866Gb/s，距1986年中科院高能物理研究所首度与Internet建立电子邮件连接仅20余年时间。计算机网络的迅猛发展，以不可逆转的趋势影响着我们工作和生活的方方面面。

计算机网络的发展，经历了联机系统、计算机互联网络、标准化网络、网络互联与高速网络四个阶段。

联机系统，即以一台中央主计算机连接大量地理上处于分散位置的终端。终端通常指一台计算机的外部设备，包括显示器和键盘，无中央处理器。这一阶段可追溯到20世纪50年代。那时人们开始将彼此独立发展的计算机技术与通信技术结合起来，完成了数据通信与计算机通信网络的研究，为计算机网络的出现做好了技术准备，奠定了理论基础。

从20世纪60年代中期开始，出现了若干个计算机互联的系统，开创了计算机——计算机通信时代。随后各大计算机公司都陆续推出了自己的网络体系结构，以及实现这些网络体系结构的软、硬件产品。1974年IBM公司提出的SNA(System Network Architecture)和1975年DEC公司推出的DNA(Digital Network Architecture)就是两个著名的例子。这种自成体系的系统被称为封闭系统，各厂家提供的网络产品实现互联十分困难，人们迫切希望建立统一的国际标准，渴望得到一个开放的系统。

20世纪70年代中期，计算机网络开始向体系结构标准化的方向发展。1984年国际标准化组织(International Organization for Standaradization，ISO)正式颁布了开放系统互联参考模型(Open System Interconnection，OSI)，简称为ISO/OSI七层参考模型。20世纪80年代，美国电气与电子工程师协会(Institute of Electrical and Electronics Engineers，IEEE)为了适应微型计算机、个人计算机(PC)以及局域网发展的需要，于1980年2月在旧金山成立了IEEE 802局域网标准委员会，并制定了一系列局域网标准。在此期间，各种局域网大量涌现。新一代光纤局域网——光纤分布式数据接口(Fiber Distributed Data Interface，FDDI)网络标准及产品也相继问世。这一阶段典型的标准化网络结构如图1-1所示，通信子网的交换设备主要是路由器和交换机。通信子网之外的部分由各种类型的大量主机构成，信息资源存放于这些主机中，故通常称此部分为资源子网。

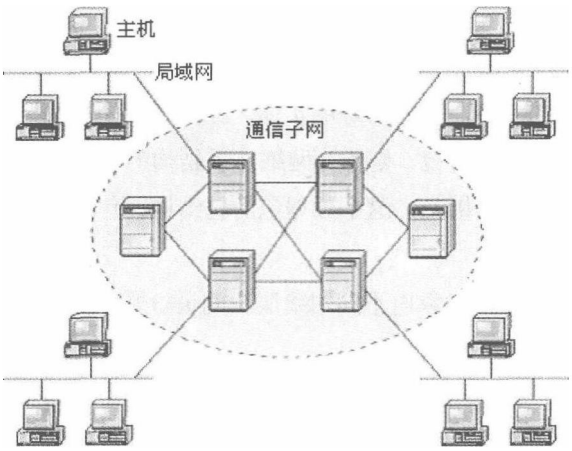


图 1-1　标准化网络

进入 20 世纪 90 年代，随着计算机网络技术的迅猛发展。特别是 1993 年美国宣布建立国家信息基础设施(National Information Infrastructure，NII)后，全世界许多国家都纷纷规划建设本国的NII，从而极大地推动了计算机网络技术的发展，这样计算机网络的发展进入一个崭新的阶段，这就是计算机网络互联与高速网络阶段。目前，全球以 Internet 为核心的高速计算机互联网络已经形成，Internet 已经成为人类最重要的、最大的知识宝库。网络互联和高速网络被称为第四代计算机网络，如图 1-2 所示。

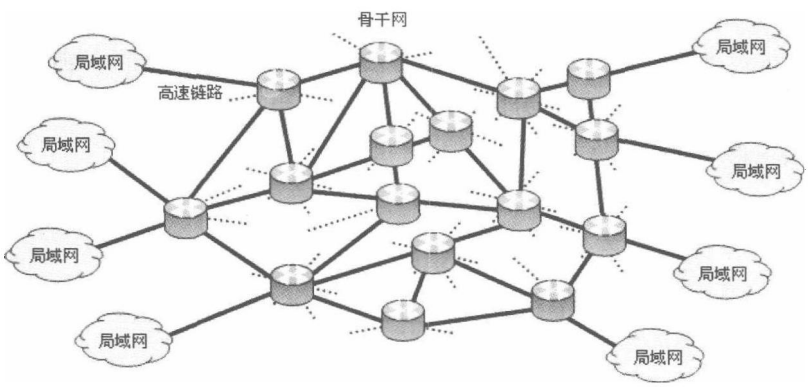


图 1-2　网络互联和高速网络

1.2　网络体系结构

网络体系结构，包含网络协议如何分层、各层协议、层间接口三个方面的内容。

如何分层，是指该协议体系中，共分为几个层次，每个层次的名称、功能分别是什么。例如，OSI 七层参考模型包含物理层、链路层等七个层次，而 TCP/IP 体系结构则分为链路层、网络层、传输层、应用层四个层次。

通过网络进行通信的两个对象都包含着协议体系中的各个层次。两个对象中，处于相同位置的层次，称为对等层。图 1-3 中，用虚线标明了通信中的 A、B 两个对象的对等层示例。对等层内完成通信动作的主体，称为对等层实体，如图 1-3 中的圆形区域。对等层间进行数据交换等通信动作时所遵循的规范，则称为网络体系结构的各层协议。例如，主机 A 的网络层实体发送了一个数据包给主机 B，这个数据包的包结构、包内各字段的定义，都必须遵循网络层协议。

层间接口描述的是某通信对象内不同网络层次间进行数据交换时所遵循的规范，其所处位置见图 1-3 中的方块形区域。

也许有人会问，为什么网络体系结构一定要分层？事实上，基于前人的大量经验，非常确定的是，在设计一个比较复杂的系统时，如果不对系统进行分解，并对分解后的各部分进行独立设计，同时降低各部分间的耦合度，那么在系统后续运行、维护、调整中，系统内大量相互牵扯的因素将导致牵一发而动全身，这些被“动了的全身”进而会引发更多的问题，最终整个系统将变得不可管理、不可维护。

基于上述原因，为了有效运行、管理、维护复杂系统，并提高设计效率，必须将系统进行分解。对复杂系统的分解，通常有分层和分块两种方式。程序设计中的模块化编程、面向对象编程，都是典型的以分块的方式来分解复杂系统的手段，而操作系统的分层设计、网络协议的层次结构，则是分层分解方式的典型。

分层在复杂系统设计中带来的效率、可维护性的提升是不容置疑的，但分层也并非是毫无“副作用”的灵丹妙药。层次的划分，在系统运行过程中需要一定的开销，会造成部分性能损失，随着硬件运行速度的迅猛发展，与设计效率的提高及系统可维护性相比，这种性能损失是完全可以接受乃至忽略不计的。

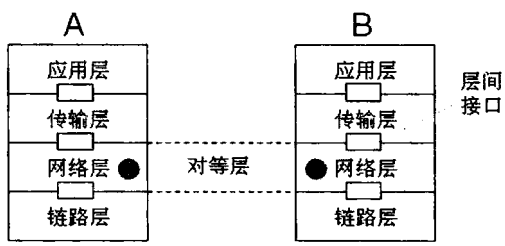


图 1-3　对等层、对等层实体、层间接口

1.2.1　OSI 参考模型

OSI 开放系统互联参考模型把网络分为七个层次，如图 1-4 所示，从下往上，依次称为第一层、第二层，直至第七层。其中物理层、链路层、网络层通常用于在网络中传递数据，构成整个网络的通信子网。而组成资源子网的各类主机，不仅包含第一至第三层协议，还涵盖第三层以上用于保障数据正确传输、实现多种多样网络应用功能的各层协议。

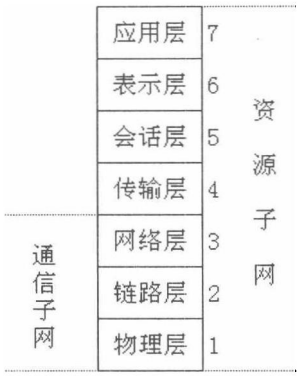


图 1-4　OSI 七层模型示意图

需要注意的是，OSI 与 ISO 常常容易混淆。OSI 是一个具体的规范标准，而 ISO 是制定标准的机构。OSI 是 ISO 制定的标准之一，ISO 还制定了许多其他标准，比如，日程生活中常见的 ISO 9001 标准，就是 ISO 9000 系列所包括的一组质量管理体系的核心标准之一。在许多日用品的包装上可看到 ISO 9001 标志，这通常意味着某种程度上的品质保障。

传输网络数据的光纤、双绞线等物理介质位于物理层之下。而物理层的功能在于，定义网络连接器有多少帧、什么样的信号表示“1”、什么样的信号表示“0”、每个“1”或“0”在信道上持续多长时间等机械、电气规范。

链路层的主要功能是媒体访问控制、帧同步、流量控制。在采用广播信道的网络中，信道被多个主机共享，因而存在对共享信道的访问冲突，媒体访问控制用于管理对共享信道的访问，以减少冲突，并有效处理发生的冲突。帧同步，指的是识别物理传输介质上连续的“0”、“1”比特流，从中分离出一个一个的帧(Frame)，如图 1-5 所示，其中深色部分代表识别出的一个帧。流量控制则用于协调数据发送、接收双方的数据传输率，以实现在数据正确传输的前提下，尽可能提高传输效率。

图 1-5　帧同步示意图

简单地说，网络层的功能在于编址和寻址。编址类似于为某个小区的住户分配门牌号码，其作用是为网络中的不同主机分配不同的地址编码，从而加以区分。寻址，网络专业术语称为路由，或称路径选择，是指根据目的主机的地址，来决定数据包应该走向哪条网络路径。

传输层的功能是对网络层功能的进一步扩展，网络层实现将数据传输至目的主机，但数据将会由目的主机中的哪个应用程序来接收处理，则取决于传输层的机制。可以这样理解，网络层提供的是主机端到端的传输能力，而传输层提供的是主机内应用程序端到端的传输能力。

会话层允许不同主机上的用户之间建立会话，包括对话控制、发言管理、同步等服务。

表示层之下的各层，主要关注如何传递数据，而表示层关注的是所传递信息的语法和语义。不同体系结构的计算机可能会使用不同的数据表示方法，为了让这些计算机间能正确通

信，所交换的数据结构必须以一种抽象的方式来定义。一个典型的例子是，在存储数据时，x86 架构的计算机使用的是低位在前(Little-Endian)的方式，比如一个 16 位二进制数 1234H，在内存的低地址字节存放的是 34H，在高地址字节中存放的是 12H，而 PowerPC、SPARC 和 Motorola 处理器则通常使用的是高位在前(Big-Endian)的方式，同样的 1234H，在内存中存放的两个字节的地址顺序则是相反的。

应用层包含了多种根据用户的不同应用需求而制定的协议。

1.2.2 TCP/IP 参考模型

TCP/IP 参考模型分为链路层、网络层、传输层、应用层四个层次。TCP/IP 参考模型和 OSI 七层模型的对应关系如图 1-6 所示。

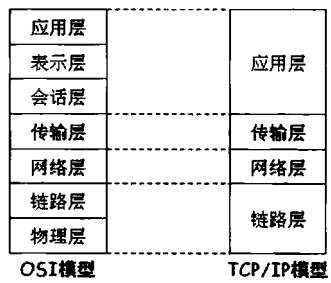


图 1-6　两种网络体系结构对应关系

显而易见的是，TCP/IP 模型简化了 OSI 模型，这也是 TCP/IP 成为当前网络协议的事实标准的主要原因。事实上，OSI 模型作为国际标准化组织制定的一种网络理论体系结构，从未被真正意义上的产品实现过。

TCP/IP 模型中，对链路层并未作出明确限定，根据网络使用的硬件的不同，支持多种不同的链路层、物理层协议，如以太网、令牌环网、FDDI(Fiber Distributed Data Interface，光纤分布式数据接口)、ATM(Asynchronous Transmission Mode，异步传输模式)及 RS-232 串行线路协议等。因此，为了在针对具体协议进行分析时表述方便，通常将 TCP/IP 模型中的链路层分解为类似 OSI 七层模型的链路层协议、物理层协议。以下针对 TCP/IP 协议网络系统进行分析时，均采用这种方式。

对网络协议进行分析，首先需要了解一次通信过程中数据在各层间流动的情况。在一次数据发送操作中，数据在各层间流动的方向是由上往下，从最高的应用层，向下流向传输层、网络层、链路层、物理层，直至物理线路，如图 1-7 所示。需要强调的是，除了从链路层到物理层，数据在其他各层网络协议间由高层向低层流动时，每下降一层，所传递的数据就会被加上一个相应层次的头部(Header，又称首部)信息。

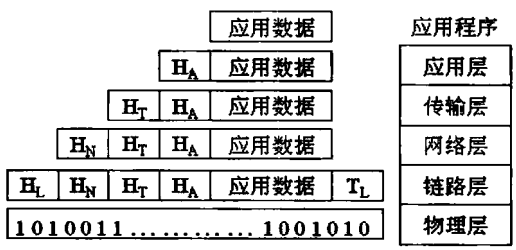


图 1-7　发送过程中，数据在各层间的流动

图 1-7 中，H_A、H_T、H_N、H_L 分别表示应用层头部、传输层头部、网络层头部和链路层头部。数据由高层向低层流动时，除了被加上一个头部信息外，在链路层，还会被加上一个链路层尾部(Tail)，图 1-7 中以 T_L 表示。

下面通过一个实际操作中捕获(Capture)到的网络数据包分析，来验证数据在各层网络协议间的流动过程，如图 1-8 所示。网络数据包的捕获和分析，需要用协议分析工具来完成。网络数据包捕获动作也称为抓包，相关工具的用法将在后文中介绍。

图 1-8 所示是一次 FTP 登录操作中捕获到的网络数据。FTP(File Transfer Protocol，文件传输协议)是被广泛用于在网络上存放、处理文件的协议。

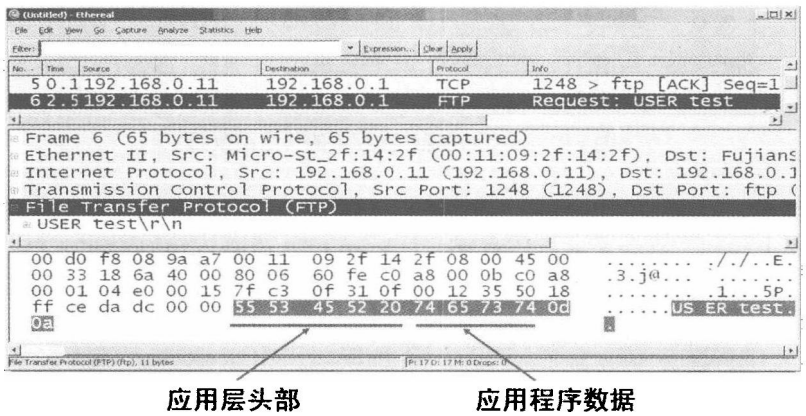


图 1-8　FTP 登录操作过程中的应用层数据

使用 FTP 协议进行网络文件操作，需要输入用户名、口令进行登录。本例中 FTP 客户端的 IP 地址是 192.168.0.11，FTP 服务端的 IP 地址是 192.168.0.1，对应于图 1-8 上方地址信息区域左侧源地址(Source)栏和右侧目的地址(Destination)栏。

图 1-8 中，捕获到的网络数据包被解析为各个层次的协议，见该图中部的协议信息区域。我们从应用层开始对这个数据包进行分析，由图可见，图中部深色部分的“File Transfer Protocol(FTP)”，表明当前的 FTP 操作被准确识别出来了。图下部显示的是当前网络数据包对应的十六进制数据，并在其右侧显示了对应的 ASCII 码。

通过对当前网络数据包十六进制数据及其 ASCII 码的分析，验证了前文所述，应用程序数据在向下流动到应用层时，被加入了应用层头部的概念。本数据包中，应用程序数据是“test”，表明当前要登录 FTP 的用户名是“test”，而当前要做的 FTP 动作是向 FTP 服务器发送用户名，因而被加入的应用层头部信息是“USER”。加入应用层头部信息后，完整的应用层数据在图中数据区以反色方式标记出来。

图 1-9 是当前数据包传输层数据的解析。图中部反色部分，表明当前数据包传输层使用的 TCP(Transmission Control Protocol)，其源端口是 1248，目的端口是 FTP(FTP 协议的控制连接使用的默认端口是 21)。通过对图 1-9 中下方数据的观察，结合图 1-8 可以发现，传输层的头部信息，是紧挨着应用层数据的，从而验证了图 1-7 所述，数据向下层流动时，被加入头部信息的概念。