第3章

电子数据取证基础知识

在有力推进社会信息化进程的同时，计算机技术及其应用的快速发展为各类违法犯罪活动提供了环境和手段，涉及电子数据证据的案件也随着计算机应用的快速普及而日趋增多，电子数据证据逐渐成为被当事人接纳及法庭认可的有效法律证据。作为一项专门技术，电子数据取证涉及哪些主要的技术问题？取证人员需要具备哪些基础知识？本章内容将围绕这些核心问题展开。

3.1 计算机基础知识

计算机又称为电子计算机或电脑，是一种能够按照程序约定，自动、高速、精确地完成各种信息存储、数据处理、数值计算、过程控制和数据传输的电子设备。从 1946 年 2 月世界上第一台计算机 ENIAC(electronic numerical integrator and computer)在美国宾夕法尼亚大学问世以来，已经历了电子管计算机、晶体管计算机、集成电路计算机、大规模和超大规模集成电路计算机 4 个阶段(四代)，将信息采集、存储处理、通信和人工智能结合在一起的新一代计算机正在研制过程中。

3.1.1 计算机系统的组成

一个完整的计算机系统由硬件和软件两部分组成。其中，硬件指构成计算机的物理设备，而软件指计算机系统中的程序、数据以及开发、使用、维护程序所需文档的集合。通常，将没有配置任何软件的计算机称为裸机。计算机系统的组成如图 3-1 所示。

1. 计算机硬件的组成

被称为计算机之父的美籍匈牙利数学家冯·诺依曼(von Neumann)在世界上第一台电子计算机 ENIAC 诞生后便提出了“存储程序和程序控制”的计算机工作原理，奠定了计算

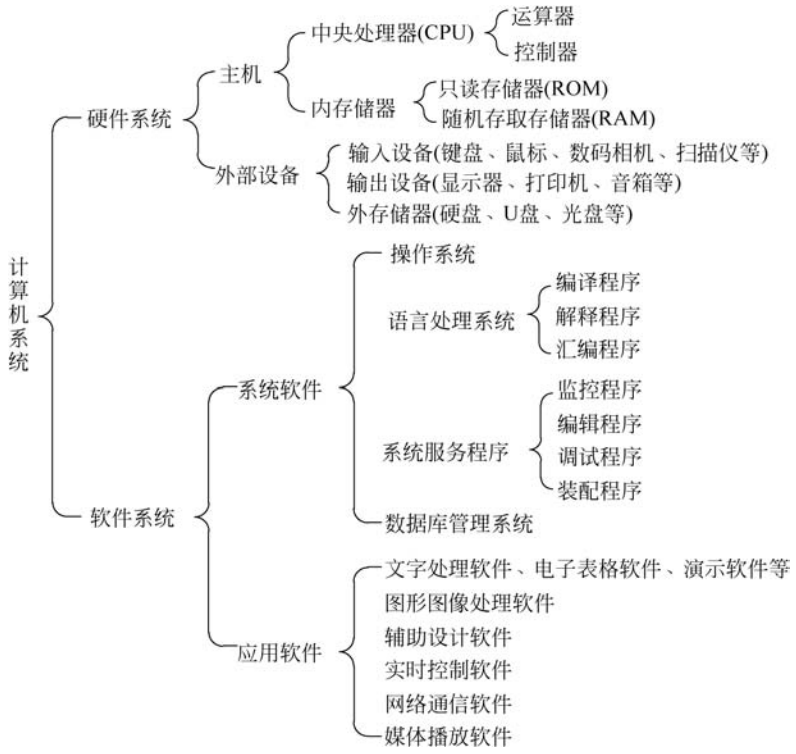


图 3-1　计算机系统的组成

机硬件的基本结构。在冯·诺依曼计算机体系结构中，计算机由运算器、控制器、存储器、输入/输出设备 5 个基本部分组成，不同部分之间通过系统总线互连，传递数据、地址和控制信号。这些系统总线按传输信号类型分为数据总线、地址总线和控制总线 3 种类型。

中央处理单元(central processing unit，CPU)是整个计算机的核心，它由运算器和控制器组成。存储器分为内存储器(简称内存)和外存储器(简称外存)两种类型。CPU、内存储器、总线等构成了计算机的“主机”。输入设备和输出设备统称为 I/O(input/output)设备。I/O 设备和外存储器通常称为计算机的“外部设备”(简称外设)。图 3-2 是计算机硬件系统组成结构示意图。

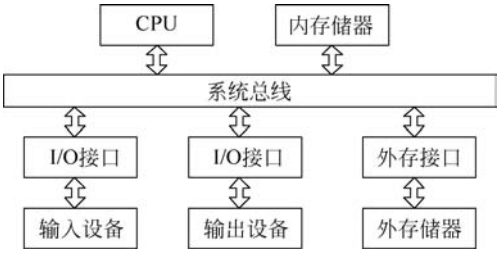


图 3-2　计算机硬件系统组成结构示意图

2. 计算机软件及其分类

广义的软件指程序及其相关数据和文档的集合；狭义的软件则指设计比较规范、功能比较齐全、具有某种使用价值的程序。其中，程序是对计算任务的处理对象和处理规则的描

述，文档是为了便于了解程序所需的说明性的资料，程序是软件的主体。

软件是智力活动的结果，受到知识产权的保护。版权是授予软件作者某种独占权利的一种合法的保护形式，版权所有者唯一享有该软件的复制、发布、修改、署名、出售等权利。用户购买了一款软件，仅仅得到了该软件的使用权，并没有获得其版权。

1）根据功能不同进行分类

根据应用功能的不同，计算机软件分为系统软件和应用软件两大类。

（1）系统软件。

系统软件指控制和协调计算机及外部设备，并支持应用软件开发和运行的一类特殊的软件，系统软件使得计算机使用者和其他软件将计算机当作一个整体而不需要考虑底层每个硬件是如何工作的。系统软件泛指基本输入/输出系统（BIOS）、操作系统（如 Windows、Linux 等）、数据库管理系统（如 Oracle、Access、DB2 等）、程序设计语言处理系统（如 C 语言编译器）等。其中，操作系统是用于管理计算机硬件与软件资源的计算机程序，是一类特殊的系统软件。

（2）应用软件。

应用软件泛指那些为了解决某一类问题而单独开发的软件。应用软件的多样性丰富了计算机的功能。

2）按照软件权益处理方式进行分类

按照软件权益的处理方式，计算机软件分为商品软件、共享软件、自由软件三种类型。

（1）商品软件。

商品软件指用户需要付费才能使用的软件，它除了受版权保护外，还受到软件许可证的保护。

（2）共享软件。

共享软件指一种“买前免费试用”的具有版权的软件。它通常允许用户试用一段时间，期间允许用户复制和分发。如果过了试用期还想使用时，就需要进行注册（需要缴纳一定的费用）。共享软件是一种为了节约市场营销费用而采用的软件销售策略。

（3）自由软件。

自由软件是一类可以不受限制地进行复制、修改、分发、使用和研究的软件，如 TCP/IP 软件、Linux 操作系统等。通常自由软件是以“自由软件授权协议”的方式发布，公开软件源代码。

除此之外，还有一类软件称为免费软件，它指一种不需付费就可取得的软件。但与自由软件不同的是，免费软件用户没有修改权。大多数自由软件是免费的，但免费软件不全是自由软件。

3.1.2 计算机中信息的表示

信息是事物运动状态及状态变化的描述。哪里有运动的事物，哪里就存在反映该事物运动状态及其变化的信息。信息、物质、能源构成了当代社会物质文明的三大要素。如果要让计算机等智能机器能够识别和处理信息，首先必须将信息转换成能够被其识别的符号，即完成信息的符号化过程，其结果称为数据。电子数据取证工作的主要对象是分别以文字、数字、图像等形式表示的数据。所以，数据是信息的具体表现形式，是信息的载体，也是电子数据取证工作的主要对象。

1. 信息的基本单位及其表示

信息在计算机介质中存储或网络中传输时，为了对其进行量化处理，都需要以具体的单位来表示。

1）比特

比特(bit)是计算机系统处理、存储和传输信息的最小单位，1个比特表示计算机中的一个数字0或数字1，单位用b表示。在电子数据取证操作中，一般每个西文字符需要用8bit表示，而一个汉字至少需要16bit表示，图像、视频等则需要更多的比特才能表示。

2）字节

字节(Byte)也是一种信息的计量单位，通常用B表示，1B=8b。

3）信息存储容量的表示

在计算机系统中，所有被符号化的数据都保存在存储器中，存储器的容量通常使用2的整数次幂字节来表示。信息存储容量的常用表示单位包括如下：

(1) 千字节。千字节(Kilobyte，KB)，$1KB=2^{10}B=1024B$。

(2) 兆字节。兆字节(Megabyte，MB)，$1MB=2^{20}B=1024KB$。

(3) 吉字节。吉字节(Gigabyte，GB)，$1GB=2^{30}B=1024MB$。

(4) 太字节。太字节(Terabyte，TB)，$1TB=2^{40}B=1024GB$。

另外，目前在计算存储容量时还用到了PB(Petabyte)和EB(Exabyte)，其中，$1PB=2^{50}B=1024TB$，$1EB=2^{60}B=1024PB$。

4）信息传输的表示

在计算机网络中，信息是以比特为单位传输的。由于比特在网络中是以串行方式传输的，所以通常用每秒传输的比特数来表示传输的速率，经常使用的传输单位如下：

(1) 比特/秒。比特/秒(bit/s，b/s，bps)。

(2) 千比特/秒。千比特/秒(kb/s)，$1kb/s=10^3b/s=1000b/s$，其中k表示1000。

(3) 兆比特/秒。兆比特/秒(Mb/s)，$1Mb/s=10^6b/s=1000kb/s$。

(4) 吉比特/秒。吉比特/秒(Gb/s)，$1Gb/s=10^9b/s=1000Mb/s$。

(5) 太比特/秒。太比特/秒(Tb/s)，$1Tb/s=10^{12}b/s=1000Gb/s$。

2. 计算机中信息的表示

通常使用()加下角标表示不同的进制数。例如，二进制数使用$()_2$表示，十进制数使用$()_{10}$表示，等等。也可以在数字后面用特定的字母表示该数的进制，例如，B表示二进制，D表示十进制，O表示八进制，H表示十六进制等。

(1) 二进制。当信息被符号化为数据后存储在计算机中时采用二进制表示，即由0和1两个不同的数字符号组成来表示一定的数，其特点是“逢二进一”。

(2) 八进制。八进制由0～7共8个数字符号组成，其基数为8，特点是“逢八进一”。

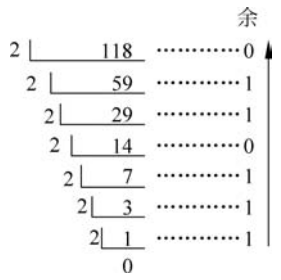
(3) 十六进制。十六进制由0～9共10个数字符号和A～F共6个英文字母组成，其基数为16，特点是“逢十六进一”。

3. 不同进制之间的转换

1）十进制整数转换成二进制整数

将十进制整数转换成二进制整数时采用的方法是“除2取余”，即用2不断地去除被转

换的十进制数，直到商为 0 时，将所得的余数从最后向前连接起来便是这个数的二进制表示。例如，将十进制整数$(118)_{10}$转换成为二进制整数，具体过程如下：



所以，$(118)_{10}=(1110110)_2$。

2）二进制数转换为十进制数

二进制数转换为十进制数的方法为，将二进制数按权展开求和。例如：

$$(1110110)_2=1\times2^6+1\times2^5+1\times2^4+0\times2^3+1\times2^2+1\times2^1+0\times2^0$$
$$=64+32+16+0+4+2+0$$
$$=118$$

同理，如果要将一个非十进制数转换成十进制数，只需要把各个非十进制数按权展开求和即可。

3）二进制数转换成八进制数

由于一个八进制数可以由一个 3 位的二进制数表示，即$8=2^3$，所以在将二进制数转换成八进制数时，具体的转换方法为，以二进制数的小数点为起点，整数部分向左 3 位形成一组，小数部分向右 3 位形成一组，不足 3 位的用 0 补足，然后分组求得二进制数的八进制表示即可。例如，将$(1110110.1101)_2$转换为八进制数，具体方法为：

001 110 110 . 110 100
↓ ↓ ↓ ↓ ↓
1 6 6 6 4

即$(1110110.1101)_2=(166.64)_8$。

4）八进制数转换成二进制数

一个八进制数转换为二进制数的方法为，将八进制数的每一位用相应的 3 位二进制数替代，再将两端多余的 0 去掉。例如，将$(166.64)_8$转换为二进制数的方法为：

6 6 6 . 6 4
↓ ↓ ↓ ↓ ↓
001 110 110 110 100

即$(166.64)_8=(1110110.1101)_2$。

5）二进制数转换为十六进制数

由于一个 4 位的二进制数可以对应于一个 1 位的十六进制数，所以二进制数转换为十六进制数的方法为，以二进制数的小数点为起点，整数部分向左 4 位形成一组，小数部分向右 4 位形成一组，不足 4 位的用 0 补足，然后分组求得二进制数的十六进制表示即可。例如，将$(1110110.1101)_2$转换为十六进制数，具体方法如下：

$$\begin{array}{cccc} 0111 & 0110 . & 1101 \\ \downarrow & \downarrow & \downarrow \\ 7 & 6 & D \end{array}$$

即$(1110110.1101)_2=(76.D)_{16}$。

6）十六进数转换为二进制数

十六进制数转换为二进制数的方法与八进制数转换为二进制数相似，即：将十六进制数的每一位用相应的4位二进制数替代，再将两端多余的0去掉。例如：

$$(76.D)_{16}=(01110110.1101)_2=(1110110.1101)_2$$

7）十进制整数与N进制整数之间的转换

掌握了十进制整数与二进制整数之间的转换方法后，很容易理解十进制整数与N进制整数之间的转换方法：将一个十进制整数转换为N进制整数时采取“除N取余”的方法，即用N反复去除被转换的十进制整数，直到商为0，将所得的余数从最后向前连接起来便是这个数的N进制表示；将一个N进制整数转换为十进制整数时，可将N进制数按权展开求和。

4. 西文字符的编码

西文文字是由拉丁字母、数字、标点符号以及一些特殊符号组成的字符集。在计算机系统中，常用的西文字符编码方式有ASCII码和EBCDIC码。其中，ASCII码主要用于微型计算机和小型机，EBCDIC码则主要用于IBM大型机。

1）ASCII码

ASCII(American standard code for information interchange)码是目前计算机系统中普遍使用的一种编码方式，存在7位和8位两个版本，国际上普遍使用7位版本。7位版本的ASCII码称为标准ASCII码或基础ASCII码，它由128(2^7)个字符组成，其中包括33个控制字符和95个可打印字符。由于计算机系统中的存储单位是字节，所以一般使用一字节(8bit)存放一个ASCII码，其中最高位为“0”。

8位版本的ASCII码称为扩展ASCII码，由256(2^8)个字符组成，它是在标准ASCII码的基础上将最高位(在标准ASCII码中为“0”)用于确定附加的128个特殊字符、外来语字母和图形符号。许多基于x86的系统都支持使用扩展ASCII码。

2）EBCDIC码

EBCDIC(extended binary coded decimal interchange code)是IBM公司于1963年推出的字符编码，采用8位二进制表示，共有256(2^8)种不同的编码，可表示256个字符，主要用于IBM大型机中。

5. 汉字的编码

作为一种编码，由于汉字数量庞大、字形复杂，所以汉字在计算机中的存储和处理要比西文字符复杂和困难。为了使原本存储和处理西文字符的计算机系统能够“接受”汉字，需要对汉字设计相应的编码。目前，常用的汉字编码方案有以下几种：

1）GB 2312编码

为了满足国内在计算机中使用汉字的需要，中国国家标准总局发布了一系列的汉字字符集国家标准编码，其中最有影响的是于1980年发布的《信息交换用汉字编码字符集·基

本集》,标准号为 GB2312-1980。GB 2312 编码方案共收录了 6763 个常用汉字和 682 个非汉字字符(图形、符号),其中一级汉字 3755 个(以汉语拼音为序排列),二级汉字 3008 个(以偏旁部首进行排列)。

由于字符数量较大,GB2312 采用了二维矩阵编码法对所有汉字字符进行编码。首先构造一个 94×94 的方阵,每一行称为一个“区”,每一列称为一个“位”,每个汉字在方阵中都有一个唯一的位置,这个位置可以用区号和位号合成表示,称为字符的区位码。

为区别于 ASCII 码,GB2312 编码共占用 2 字节(16bit),每字节的最高位规定为“1”,如图 3-3 所示。

2) GBK 汉字内码扩充规范

GB2312 虽然得到了广泛使用,但由于该编码仅包括 6763 个汉字,所以无法满足日常应用要求。为此,1995 年我国又发布了代号为 GBK 的《汉字内码扩展规范》。GBK 一共包含 21003 个汉字和 883 个图形符号,除了 GB2312 中的全部汉字和符号外,还收录了包括繁体字在内的大量汉字和符号。

GBK 汉字编码也使用双字节。由于与 GB2312 保持向下兼容,因此所有与 GB2312 相同的字符,其编码也保持不变,新增加的符号和汉字则另外编码,它们的第 1 字节最高位必须为“1”,第 2 字节的最高位没有要求,如图 3-4 所示。

图 3-3 GB2312 汉字编码方式

图 3-4 GBK 汉字编码方式

3) UCS/Unicode

前文介绍的 ASCII 码、GB2312 编码以及 GBK 汉字编码都是为了解决某一国家或地区语言文字的信息编码而提出的方案,具有应用上的局限性。而 UCS 是由国际标准化组织(ISO)制订的一个可以容纳全世界所有语言文字的编码标准,对应的工业标准称为 Unicode。UCS 只规定如何编码,并没有规定如何传输和保存这个编码,具体实现已经在 UTF-8、UTF-16、UTF-32 等方案中得到了体现。例如,在各类 Web 浏览器中广泛使用 UTF-8、UTF-16 等。

4) GB18030

GB18030 全称为国家标准 GB18030-2005《信息技术 中文编码字符集》,是我国制订和执行的新的汉字编码国家标准,它与 GB2312 和 GBK 保持向下兼容,并扩充了 UCS/Unicode 中的字符。GB18030 采用多字节编码,每个字符可以由 1、2 或 4 字节组成,编码空间较大,支持我国少数民族的文字。

5) 汉字的字形码

汉字的字形即汉字的形状描述,针对某一编码标准(如 GB2132),用于描述所有汉字字形信息的集合称为字库。字库通常分为点阵字库和矢量字库,目前汉字字库多采用点阵字库。点阵字库即用点阵表示汉字的字形代码,根据汉字输出精度要求的不同,有 16×16 点阵、24×24 点阵、32×32 点阵等。点阵中的每一个点用二进制的“0”或“1”来表示,其中“0”表示对应位置处是空白,“1”表示对应位置处是黑点。

点阵字库中每一个汉字字形码所占用的存储空间较大,例如一个 24×24 点阵的汉字字

形码需要用到 72(24×24÷8=72)字节存储空间。所以,汉字字形点阵只能用来构造存放于硬盘等外部存储介质上的字库,而不能用来替代机内码用于机内存储。一个完整的字库存放着每一个汉字的字形点阵代码,同一汉字的不同字体(如宋体、黑体、仿宋、楷体等)对应着不同的字库。

在输入汉字(屏幕显示或打印)时,计算机要先到字库中查找对应汉字的字形描述信息,然后再把字形送去输出。

6. 二进制数的基本运算

二进制数的基本运算主要包括算术运算和逻辑运算两类。

1) 二进制数的算术运算

二进制数的算术运算包括加、减、乘、除四则运算。

(1) 二进制数的加法。根据"逢二进一"规则,二进制数加法的法则如下:

0+0=0

0+1=1+0=1

1+1=10(进位为 1)

(2) 二进制数的减法。根据"借一有二"的规则,二进制数减法的法则如下:

0-0=0

1-1=0

1-0=1

0-1=1(借位为 1)

(3) 二进制数的乘法。二进制数乘法过程可仿照十进制数乘法进行。但由于二进制数只有 0 或 1 两种可能的乘数位,导致二进制乘法更为简单。二进制数乘法的法则如下:

0×0=0

0×1=1×0=0

1×1=1

(4) 二进制数的除法。二进制数除法与十进制数除法很类似。可先从被除数的最高位开始,将被除数(或中间余数)与除数相比较,如果被除数(或中间余数)大于除数,则用被除数(或中间余数)减去除数,商为 1,并得相减之后的中间余数,否则商为 0。再将被除数的下一位移下补充到中间余数的末位,重复以上过程,就可得到所要求的各位商数和最终的余数。例如,二进制数$(100110)_2$除以二进制数$(110)_2$:

```
        110    商
    ------------
110 ) 100110
      110
      ---
      111
      110
      ---
       10    余数
```

即二进制数 100110÷110=110 余 10。

2) 二进制数的逻辑运算

二进制数的逻辑运算包括逻辑或(也称"加"运算,用符号 OR 或 ∨ 表示)、逻辑与(也称为"乘"运算,用符号 AND 或 ∧)以及逻辑非(也称"取反"运算,用符号 NOT)。

(1) 逻辑或。逻辑或运算的法则为：0∨0=0,0∨1=1,1∨0=1,1∨1=1。

(2) 逻辑与。逻辑与运算的法则为：0∧1=0,0∧1=0,1∧0=0,1∧1=1。

(3) 逻辑非。逻辑非指将原逻辑变量的状态求反，当逻辑变量为 0 时，其“非”运算的结果为 1；逻辑变量为 1 时，其“非”运算的结果为 0。

3.1.3 虚拟化与云计算

虚拟化技术实现了信息技术资源的逻辑抽象和统一表示，在桌面应用(如桌面虚拟化)、大规模数据中心管理以及解决方案交付等方面发挥着重要支撑作用，是构建云计算最重要的技术基石。

1. 虚拟化技术

虚拟化是一个广义的术语，指计算元件在虚拟的而不是真实的基础上运行，是一个为了简化管理、优化资源的解决方案。从应用的角度，通过虚拟化可以在一台物理设备上虚拟出多个独立的系统，也能够将多台独立的物理设备虚拟成一个逻辑的设备。

1) 虚拟化的概念

无论对虚拟化如何定义，也不管其实现方式如何，就其技术实质来讲，至少包括 3 方面的含义。

(1) 虚拟化的对象是各类资源，这里的资源一般为计算机系统、进程、网络、存储、内存等，分别对应系统虚拟化、进程虚拟化、网络虚拟化、存储虚拟化、内存虚拟化等。

(2) 虚拟化后形成的逻辑资源对用户隐藏了不必要的细节，用户只关心应用，而不必考虑具体的实现细节。

(3) 根据应用需要，用户可以在虚拟环境中几乎实现其在真实环境中全部功能。

2) 虚拟化的分类

根据实现方式的不同，虚拟化技术可以分为硬件虚拟化、操作系统虚拟化、应用程序虚拟化等类型。

(1) 硬件虚拟化。硬件虚拟化是通过软件方式虚拟出一台标准的计算机，虚拟化对用户隐藏了真实的物理计算机。硬件虚拟化的结果是一台虚拟的裸机，使用时就像在物理裸机上安装操作系统一样，同样需要在虚拟的裸机上安装所需要的操作系统。

硬件虚拟化一般有两种方式：一种是在现有操作系统上通过安装虚拟机软件，再由虚拟机软件虚拟出一台虚拟裸机，然后在虚拟裸机上安装新的操作系统，从而形成“系统里有系统”的形式；另一种方式是直接在物理裸机上安装虚拟机，然后通过虚拟机产生虚拟的裸机，再在虚拟的裸机上安装所需要的操作系统。两种方式相比较，后者占用内存、CPU 等资源较少，性能较好。硬件虚拟化的代表产品有 VMware、Virtual PC、VirtualBox 等。

(2) 操作系统虚拟化。操作系统虚拟化指对操作系统的克隆，克隆后的操作系统与原操作系统完全相同，只是操作系统 ID 标识不同。操作系统虚拟化可以根据需要，基于某一原操作系统克隆出多个应用功能完全相同的操作系统，管理较为方便。不过，如果原操作系统出现问题，被克隆后的操作系统也会出现相同的问题。操作系统虚拟化的代表产品有 SWSoft 公司的 Virtuozzo。

(3) 应用程序虚拟化。应用程序虚拟化是将应用程序与操作系统解耦合，为应用程序

提供一个虚拟的运行环境。在虚拟化环境中，运行主体是应用程序的可执行文件，运行环境是执行该程序所需要的操作系统环境。从本质上讲，应用程序虚拟化是通过虚拟化技术，把应用程序对所依赖的低层操作系统以及硬件抽象出来，根据应用程序的要求按需配置和调用运行环境，可以解决版本不兼容的问题。

应用程序虚拟化领域的代表性产品主要包括 Microsoft Application Virtualization (App-V)、VMware ThinApp、Symantec Software Virtualization Solution (SVS)、InstallFree、SandBoxie、云端软件平台(softcloud)等。

在三类虚拟化应用中，硬件虚拟化和操作系统虚拟化技术主要应用于专业服务器和企业信息平台的构建，目的是通过虚拟化提供完整且真实的操作系统。而应用程序虚拟化是以应用需求为导向，为不同用户的应用提供所需要的运行环境。

2. 云计算

虚拟化是云计算的一项基础性技术。云计算(cloud computing)是基于分布式计算、网格计算和虚拟化等技术，在信息基础设施和网络应用共同发展到一定阶段时出现的一种新型信息服务方式，它使效用计算(utility computing)逐步变成了现实。云计算通过网络将庞大的计算处理程序自动拆分成无数个较小的子程序，再交由多个服务器所组成的庞大系统经搜寻、计算分析之后将处理结果回传给用户。通过这项技术，网络服务提供者可以在较短时间内处理海量信息，提供具有超级计算机同样强大效能的网络服务。云计算将计算功能分布在大量的分布式计算机上，而非本地计算机或远程服务器上，意味着计算能力可以自由按需获取。

虽然云计算是对已有技术的继承和创新，但其产生和发展适应了当前互联网环境的具体要求，具有如下明显的特点：

(1) 弹性服务。服务的规模可快速伸缩，以自动适应业务负载的动态变化。用户使用的资源同业务的需求相一致，避免了因为服务器性能过载或冗余而导致的服务质量下降或资源浪费。

(2) 资源池化。资源以共享资源池的方式统一管理。利用虚拟化技术，将资源分享给不同用户，资源的配置、管理与分配策略对用户透明。云计算最关键的特点是计算资源能够被动态地有效分配，消费者(最终用户、组织或者信息技术部门)能够最大限度地使用计算资源但又无须管理底层复杂的技术。

(3) 按需服务。以服务的形式为用户提供应用程序、数据存储、基础设施等资源，并可以根据用户需求，自动分配资源，而不需要系统管理员干预。

(4) 服务可计费。监控用户的资源使用情况，并据此对服务计费。

(5) 泛在接入。用户可以利用各种终端设备(如个人计算机、笔记本电脑、智能手机等)随时随地通过互联网访问云计算服务。

正是因为云计算具有的上述特性，使得用户只需连上网络就可以源源不断地使用计算机资源，实现了“互联网即计算机”的构想。

3.1.4　大数据

大数据(big data)从产生到现在，其概念和外延一直在随着技术和应用的发展而不断拓

展，本节主要介绍大数据的基本概念和特征，以使读者对大数据有一个总体的认识。

1. 大数据的概念

大数据的相关技术及其应用是在互联网快速发展中诞生的。随着互联网应用的快速发展，每天新增的网页数量以千万级计算，使用户检索信息越来越不方便。针对互联网信息检索带来的问题，在 2000 年前后，Google(谷歌)等公司率先建立了覆盖数十亿网页的索引库，开始提供较为精确的搜索服务，大大提升了人们使用互联网的效率，这是大数据应用的起点。

当时搜索引擎要存储和处理的数据，不仅数量之大前所未有，而且以非结构化数据为主，传统技术无法应对。为此，Google 提出了一套以分布式为特征的全新技术体系，即后来陆续公开的分布式文件系统(Google file system，GFS)、分布式并行计算(MapReduce)和分布式数据库(BigTable)等技术，以较低的成本实现了之前技术无法达到的规模。这为当前大数据技术奠定了基础，可以认为是大数据技术的源头。

伴随着互联网产业的崛起，这种创新的海量数据处理技术在电子商务、定向广告、智能推荐、社交网络等方面得到应用，并取得巨大的商业成功。这启发了全社会开始重新审视数据所蕴含的巨大价值，于是金融、电信、公共安全等拥有大量数据的行业开始尝试这种新的理念和技术，取得初步成效。与此同时，业界也在不断对 Google 提出的技术体系进行扩展，使之能在更多的场景下使用。2011 年，麦肯锡、世界经济论坛等知名机构对这种数据驱动的创新进行了研究总结，随即在全世界兴起了一股大数据热潮。

虽然大数据已经成为全社会热议的话题，但到目前为止，“大数据”尚无公认的统一定义。本书采用目前业界公认的定义：大数据指无法用现有的软件工具提取、存储、搜索、共享、分析和处理的海量复杂数据集合。同时也指新一代架构和技术，能够更经济、有效地从高频率、大容量、不同结构和不同类型的数据中获取价值。大数据中的数据规模超出传统数据库软件采集、存储、管理和分析等能力的范畴，多种数据源、多种数据种类和格式冲破传统的结构化数据范畴，社会向着数据驱动型的预测、发展和决策方向转变，决策、组织、业务等行为日益基于数据和客观分析来提出结果。

2. 大数据的基本特征

目前，人们对于大数据特征的研究归纳起来可以分为规模、变化频度、种类和价值密度等几个维度，具体从数量(Volume)、多样性(Variety)、速度(Velocity)、价值(Value)以及真实性(Veracity)5 方面(5V)进行认识和理解。

1) 数量

聚合在一起供分析的数据规模非常庞大。Google 执行董事长艾瑞特·施密特曾说，现在全球每两天创造的数据规模等同于从人类文明至 2003 年间产生的数据量总和。“大”是相对而言的概念，对于搜索引擎，EB 级属于比较大的规模，但是对于各类数据库或数据分析软件而言，其规模量级会有比较大的差别。

2) 多样性

数据形态多样，按生成类型的不同可分为交易数据、交互数据、传感数据；按数据来源不同可划分为社交数据、传感器数据、系统数据；按数据格式的不同可分为文本、图片、音频、视频、光谱等；从数据关系的角度可划分为结构化、半结构化、非结构化数据；从数据所

有者的角度来划分又可分为公司数据、政府数据、社会数据等。

3）速度

一方面是数据的增长速度快，另一方面是要求数据访问、处理及交付等速度快。美国的马丁·希尔伯特说，数字数据储量每3年就会翻1倍。人类存储信息的速度比世界经济的增长速度快4倍。

4）价值

尽管我们拥有大量数据，但是发挥价值的仅是其中非常小的部分，大数据背后所潜藏的价值巨大。例如，美国社交网站Facebook有10亿用户，通过对这些用户信息进行分析后，广告商可根据结果精准投放广告。对广告商而言，10亿用户的数据价值可达到上千亿美元。

5）真实性

一方面，确保虚拟网络环境所产生大量的数据需要的真实性、客观性，是大数据技术及其业务发展的迫切需求；另一方面，通过对大数据的分析，真实地还原并预测事物的本来面目也是大数据未来发展的趋势。

在以上介绍的大数据的5个基本特征中，“多样性”和“价值”最被大家所关注。其中“多样性”之所以被关注，在于数据的多样性使得其存储、应用等各方面都发生了变化，针对于多样化数据的处理需求也成为技术重点攻关方向。而“价值”则不言而喻，不论是数据本身的价值还是其中蕴含的价值都是企业、部门、政府机关所重视的。因此，如何将如此多样化的数据转化为有价值的存在，是大数据所要解决的重要问题。目前，大数据正在改变经济社会的管理方式、促进行业整合发展、推动产业转型升级、助力智慧城市建设、提升公安机关防控能力等方面发挥着重要作用。

3. 大数据的技术架构

大数据技术的战略意义不在于拥有海量的数据，而在于能够从这些杂乱的数据中分析挖掘出有价值的信息，即大数据技术的应用是以价值为导向。大数据的研究目标和工作重点是发现有价值的信息，而不是单纯地将数据堆砌起来，简单堆砌后形成的并无利用价值的数据只能称为“电子垃圾”，除浪费存储资源外，别无意义。

大数据很难用单台设备进行处理，需要采用并行计算技术。大数据技术涉及多个技术领域，主要包括数据存储、数据管理、数据挖掘、并行计算、云计算、分布式文件系统、分布式数据库、虚拟化等。从数据在信息系统中的生命周期看，大数据从数据源经过分析挖掘到最终获得价值一般需要经过5个主要环节，如图3-5所示，包括数据准备、存储管理、计算处理、数据分析和知识展现，每个环节都面临不同程度的技术上的挑战。

1）数据准备环节

在进行存储和处理之前，需要对数据进行清洗、整理，传统数据处理体系中称为ETL（extracting、transforming、loading，提取、转换、加载）过程。与以往数据分析相比，大数据的来源多种多样，包括企业内部数据库、互联网数据和物联网数据，不仅数量庞大、格式不一，质量也良莠不齐。这就要求数据准备环节既要规范格式，便于后续存储管理，又要在尽可能保留原有语义的情况下去粗取精、消除噪声。

2）存储管理环节

当前全球数据量正以每年超过50%的速度增长，数据存储的成本和性能面临非常大的

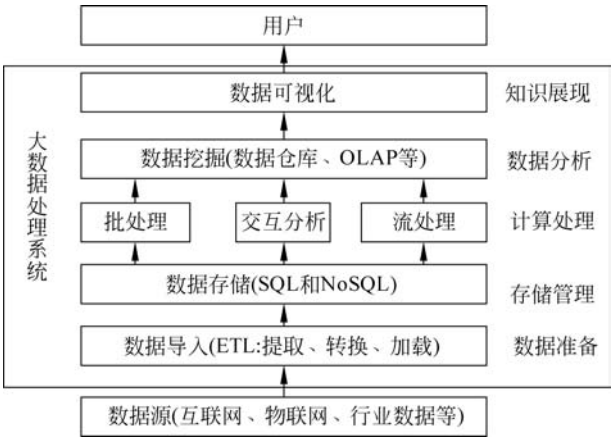


图 3-5 大数据技术框架

压力。大数据存储系统不仅需要以极低的成本存储海量数据,还要适应多样化的非结构化数据管理需求,具备数据格式上的可扩展性。

3) 计算处理环节

需要根据处理的数据类型和分析目标,采用适当的算法模型,快速处理数据。海量数据处理要消耗大量的计算资源,对于传统单机或并行计算技术来说,速度、可扩展性和成本都难以适应大数据计算分析的新需求。分而治之的分布式计算成为大数据的主流计算架构,但在一些特定场景下的实时性还需要大幅提升。

4) 数据分析环节

从纷繁复杂的数据中发现规律并提取新的知识的数据分析环节,是大数据价值挖掘的关键。传统数据挖掘对象多是结构化、单一对象的小数据集,挖掘更侧重根据先验知识预先人工建立模型,然后依据既定模型进行分析。对于非结构化、多源异构的大数据集的分析,往往缺乏先验知识,很难建立显式的数学模型,这就需要发展更加智能的数据挖掘技术。

5) 知识展现环节

在大数据服务于决策支撑场景下,以直观的方式将分析结果呈现给用户,是大数据分析的重要环节。如何让复杂的分析结果易于理解是一个不小的挑战。

3.1.5 人工智能

随着计算机辅助功能的广泛应用,电子数据取证工作也需要人工智能的支撑,尤其在网络动态取证中,人工智能技术能够发挥极其重要的作用。1997 年,IBM 的深蓝(deep blue)机器人战胜国际象棋世界冠军卡斯帕罗夫,引发了人类对于人工智能的思考;2016 年 3 月,基于搜索技术与深度学习方法相结合的人工智能围棋系统 AlphaGo 以 4∶1 的优势战胜了世界围棋高手李世石,再一次使人工智能引发全球的高度关注。

1. 人工智能的概念

人工智能最早起源于 1936 年,英国数学家 A. M. Turing 在论文《理想计算机》中提出了图灵机模型,然后 1956 年在《计算机能思维吗》一文中提出机器能够思维的论述(图灵实

验)。之后,计算机的发明和信息论的出现为人工智能发展奠定了良好的基础。1956 年在达特茅斯会议上,Marvin Minskey、John McCarthy 等科学家围绕“机器模仿人类的学习以及其他方面变得智能”展开讨论,并明确提出了“人工智能”一词。

人工智能(artificial intelligence,AI)指由人类所制造的智能,也就是由机器制造和实现的智能。在理解人工智能之前,先来了解人类所具有的智能。人类的智能指为了不断提升生存发展的水平,人类利用知识去发现问题、定义问题(认识世界)和解决问题(改造世界)的能力。然而,机器没有生命,也没有自身的目的,难以自行建立直觉、想象、灵感、顿悟和审美的能力,必须借助人的智慧来让机器模拟人的思维和行为。

人工智能的研究是让计算机能够模拟人的某些思维过程和智能行为(如学习、推理、分析、判断等)的一门学科,主要研究内容包括计算机实现智能的原理、制造类似于人类的智能的计算机,使计算机能够实现更高层次的应用。人工智能是研究让计算机去完成以往需要人的智能才能胜任的工作,也就是研究如何利用计算机来模拟人类某些行为的技术。

需要说明的是,人工智能不是人类的智能,只是能够让机器像人一样去思维和从事某项工作,机器所具有的智能永远也不会超过人类的智能。

2. 人工智能的主要技术

人工智能技术的发展是与计算机科学技术的发展紧密联系的。人工智能主要研究和解决人类发展过程中某些领域需要由机器代替人类工作的技术问题。除计算机科学外,人工智能还涉及信息论、控制论、自动化、仿生学、生物学、哲学等众多学科,主要技术包括计算机视觉、自然语言处理、智能机器人、模式识别等内容。

1) 计算机视觉

计算机视觉是运用计算机及相关技术,在相关设备的支持下,实现对生物视觉的模拟,其技术手段主要是对采集的图像或视频进行处理以获得图像或视频中的信息。目前,以图像识别和人脸识别为代表的感知技术已经发展成熟并得到广泛应用,并在交通、医疗、安防等领域产生了巨大影响。计算机视觉技术的主要目的是使计算机能同人类一样观察和理解世界,并拥有自主适应环境的能力。

人脸识别是计算机视觉相关技术发展最好、应用最广的领域之一。人脸识别技术是将人脸图像或者相关视频输入系统,然后分析每张脸的大小、特征以及面部各器官的位置信息,其技术原理如图 3-6 所示。

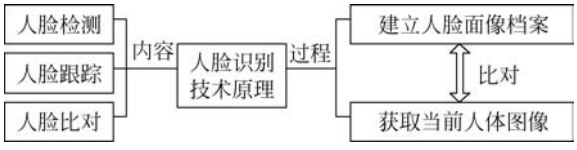


图 3-6　人脸识别技术原理

2) 自然语言处理

语言是信息的载体,是人类思维、沟通与交流的工具。自然语言处理通常指用计算机对人类的自然语言进行有意义的分析与操作。以中文信息处理为例,自然语言处理的研究内容是利用计算机对中文的音、形、义等语言文字信息进行加工和操作,包括对字、词、短语、句子、篇章进行输入、输出、识别、转换、压缩、存储、检索、分析、理解和生成等。它是语言学、计

算机科学、认知科学、数学等多学科交叉的边缘学科。

对于自然语言来说，有意义的最小单位应该是词，而对汉语来讲基本单元是字。对于汉语，自然语言处理应该包括对字、词、句以及段落与篇章的处理，如图 3-7 所示。

图 3-7　自然语言处理分解示意图

自然语言处理的研究方法分成基于规则和基于统计的两种，基于规则的方法是人工获取语言规则，而基于统计的方法则是通过对大规模语料库的统计分析，实现对自然语言的处理。

3）智能机器人

机器人是靠自身动力和控制能力来实现各种功能的一种机器。到目前为止，机器人技术的发展大致经历了 3 个阶段：第一代为可编程示教再现型机器人，其特征是机器人能够按照事先教给它们的程序进行重复工作；第二代机器人（20 世纪 70 年代）是具有一定的感觉功能和自适应能力的离线编程机器人，其特征是可以根据作业对象的状况改变作业内容，即所谓的“知觉判断机器人”；第三代机器人（20 世纪 80 年代中期以后）是智能机器人，这种机器人带有多种传感器，能够将多种传感器得到的信息进行融合，有效地适应变化的环境，具有很强的自适应能力、学习能力和自治功能。智能机器人至少具备以下功能：

（1）感觉功能。主要用来认识周围环境状态。

（2）运动功能。对外界做出反应性动作。

（3）思考功能。根据感觉功能所得到的信息，思考采用什么样的动作。

4）模式识别

模式识别是人工智能的基础技术，是通过计算机用数学方法对物理量及其变化过程进行描述与分类的一门技术，通常用来对图像、文字、照片以及声音等信息进行识别、处理和分类。

要让机器具有人的模式识别能力，人们首先需要研究人类的识别能力，因此模式识别是研究人类识别能力的数学模型，并借助于计算机技术让计算机模拟人类识别行为的科学。也就是说，模式识别是研究如何让机器观察周围环境，学会从背景中识别感兴趣的模式，并对该模式的类属作出准确合理的判断。模式识别研究主要集中在两方面：一是研究生物体（包括人）如何感知对象；二是研究在给定的任务下，如何用计算机实现模式识别的理论和方法。

如图 3-8 所示，一个完整的模式识别系统由数据获取、预处理、特征提取和选择、分类决策或模型匹配 4 部分组成。

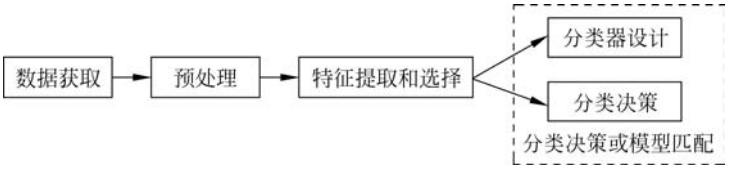


图 3-8　模式识别系统的组成

（1）数据获取。数据获取指利用各种传感器把被研究对象的各种信息转换为计算机可以接受的数值或符号（串）集合。

（2）预处理。数据预处理是为了消除输入数据或信息中的噪声，排除不相关的信号，只留下与被研究对象的性质或是与采用的识别方法密切相关的特征（如表征物体的形状、周长、面积等）。

（3）特征提取和选择。特征提取指从滤波数据中衍生出有用的信息，从许多特征中寻找出最有效的特征，以降低后续处理过程的难度。

（4）分类决策或模型匹配。基于数据处理生成的模式特征空间，人们就可以进行模式识别的最后一部分：模式分类或模型匹配。该阶段最后输出的可能是对象所属的类型，也可能是模型数据库中与对象最相似的模式编号。

人工智能正在给各行业带来变革和重构：一方面，将人工智能技术应用到现有的产品中，可以创新产品并发展新的应用场景；另一方面，人工智能技术的发展正在颠覆传统行业，人工智能对人工的替代成为不可逆转的趋势。目前，人工智能主要应用到工业、医疗、安防、金融等领域。

3.1.6　集成电路技术

集成电路（integrated circuit，IC）产业作为整个信息技术产业链的上游产业，是培育发展国家战略性新兴产业、推动中国信息化和工业化深度融合的基础。

1. 集成电路的概念

集成电路是20世纪50年代后期发展起来的一种微型电子器件或部件。它是一种新型半导体器件，利用技术或工艺手段，把电路中所需的晶体管、电阻、电容和电感等元件及布线互连一起，制作在一小块或几小块半导体晶片或介质基片上，然后封装在一个管壳内，成为具有所需电路功能的微型结构；其中所有元件在结构上已组成一个整体，使电子元件向着微小型化、低功耗、智能化和高可靠性等方面迈进了一大步。

目前，半导体工业大多数使用的是基于硅的集成电路。集成电路技术包括芯片制造技术与设计技术，主要体现在加工设备、加工工艺、封装测试、批量生产及设计创新的功能上。

2. 集成电路的特点

集成电路是在同一块半导体材料上，利用各种不同的加工方法，同时制作出许多极其微小的电阻、电容及晶体管等电路元器件，并将它们相互连接起来，使之具有特定的电路功能。集成电路具有体积小、重量轻、可靠性高以及成本低廉等特点。

根据所包含电子元件数量的多少，集成电路可以分为小规模集成电路、中规模集成电路、大规模集成电路和超大规模集成电路等类型。单个集成电路所包含的电子元件数量称为集成度。集成度小于100的集成电路称为小规模集成电路（SSI），集成度为100～3000的集成电路称为中规模集成电路（MSI），集成度在3000～10万的集成电路称为大规模集成电路（LSI），集成度为10万～100万的集成电路称为超大规模集成电路（VLSI），超过100万个电子元件的集成电路称为极大规模集成电路（ULSI）。目前，一般不区分VLSI和ULSI，而统称为VLSI。

集成电路芯片是微电子技术发展的结晶，它是计算机、通信和所有电子设备的硬件核心，是现代信息产业的基础。目前的计算机、智能手机、电视机、数码相机、摄像机、音响设

备、网络设备等电子产品均以集成电路作为硬件核心。集成电路产业的发展非常迅速，以集成电路为基础的电子信息产品成为世界第一大产业。

集成电路产业是现代电子信息产业的重要核心，其发展状况对国家经济与科技发展具有重要影响。集成电路的发展推动了传统工业的变革，促进产业升级并且加速了信息化产业的发展进程。集成电路技术目前已经向 7nm 技术、5nm 技术的方向发展。同时，集成电路的创新程度已成为一个国家创新型发展的重要标志。我国集成电路产业应该抓住发展机遇，加大在集成电路技术关键领域的研究力度，积极鼓励技术创新，不断发挥技术人才储备作用，实现跨越式发展。

3.2 计算机硬件

计算机系统由硬件和软件两部分组成，其中硬件指计算机系统中由电子、机械和光电元件等按系统结构组成的各种物理装置的总称。计算机系统的各项操作是硬件与软件协同的过程和结果。本节先介绍计算机硬件的相关知识。

3.2.1 典型计算机系统的硬件组成

冯·诺依曼提出的“存储程序”逻辑架构是电子计算机的逻辑结构设计基础和基本设计原则，目前的电子计算机无论在性能和用途上都有了不同，但都遵循冯·诺依曼结构，仍然以冯·诺依曼结构为基础。

1. 冯·诺依曼计算机

1）冯·诺依曼计算机结构

典型的冯·诺依曼计算机结构如图 3-9 所示，主要工作部件包括以下几方面：

（1）由运算器、控制器、存储器、输入设备和输出设备 5 个基本部件组成。

（2）所有指令和数据均用二进制表示。

（3）每条指令由操作码和地址码两部分组成。其中，操作码用于指出指令的操作类型（如数据的加、减、乘、除等）；地址码指出操作数和操作结果存放的位置。

（4）采用“存储程序”工作原理。根据要解决的问题，需要事先编写程序，并将程序和数据放入存储器，当程序要执行时需要从存储器调入 CPU，且根据程序中规定的顺序自动逐条执行指令直至执行结束，程序执行过程中还可能会从存储器中读取数据。

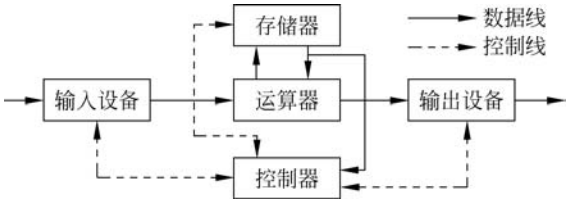


图 3-9 典型的冯·诺依曼计算机结构示意图

2）冯·诺依曼计算机的功能

冯·诺依曼计算机结构各组成部分的主要功能描述如下：

(1) 运算器。运算器(arithmetic unit)是负责对数据进行处理的部件,主要完成数据的算术运算和逻辑运算。其中,算术运算指对数据的加、减、乘、除以及乘方、开方等数学运算;逻辑运算主要指对二进制数进行的与、或、非等逻辑运算。

(2) 控制器。控制器(control unit)的主要功能是协调计算机各部件之间的协同操作,就像人的大脑一样,通过对正在执行指令的分析,将产生的控制信号送到相应的部件,以此来协调计算机各部件之间的操作。

(3) 存储器。存储器(memory)主要用于存储程序和数据,并在计算机运算过程中完成程序和数据的存取。由于计算机中使用 0 和 1 来表示数据,所以存储器也提供了具有两种稳定状态的"记忆"元件来分别表示 0 和 1。

(4) 输入设备。输入设备(input device)用来向计算机输入数据和程序。由于程序、数字、文本、图像、音频、视频等信息无法直接被计算机识别,所以在输入计算机之前首先需要将其转换成二进制代码。常见的输入设备有鼠标、键盘、摄像头、数码相机、扫描仪等。

(5) 输出设备。输出设备(output device)用于把计算机中存储、处理或传送来的二进制信息以人们能够直接辨别的数字、文本、图像、声音等形式表现出来。

2. 典型计算机系统的硬件组成

冯·诺依曼结构依然是现代计算机系统遵循的结构。一个典型计算机系统的硬件组成如图 3-10 所示(该图以 Intel Pentium 系统为模型,其他系统与此类似)。

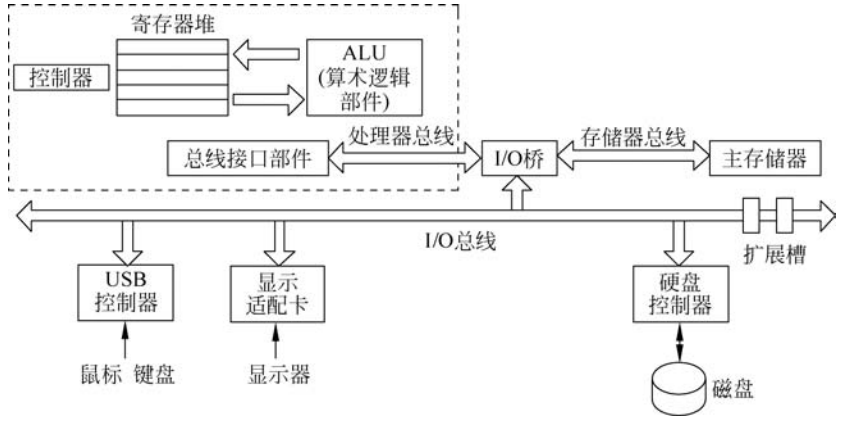


图 3-10　典型计算机系统的硬件组成示意图

1) 中央处理器

由于冯·诺依曼计算机系统采用"存储程序"工作方式,计算机的所有功能都是通过执行程序完成的。程序由不同数量的指令构成,专门用来执行指令的部件就是处理器。中央处理器(Central processing unit,CPU)是计算机系统的最核心部件,主要运行系统软件和应用软件。

早期的计算机使用的是分立晶体管,处理器由多个独立单元构成,运算器和控制器之间采用外部连线。自从 20 世纪 70 年代出现了集成电路,运算器和控制器以内部连线的方式集成在一个芯片内部,这类处理器称为微处理器。随着超大规模集成电路技术的发展,更多的功能逻辑被集成到 CPU 芯片中,甚至一个 CPU 芯片中集成了多个处理器核,从而形成了由数据通路(data path)和控制部件(control unit)组成的 CPU。其中,将指令执行过程中数据所经过的路径,包括路径上的部件称为数据通路;其余部件便是控制部件。

2）存储器

存储器技术的发展强有力地推动了计算机的广泛应用。计算机中的存储器主要指主存储器和外部存储器(硬盘和磁盘)。主存储器是一个临时存储设备,在 CPU 执行程序时,用来存放程序和程序处理的数据。外部存储器是一个能够长期存储程序和数据的设备,CPU 不能直接访问外部存储器,外部存储器上的程序和数据只有在需要时调入主存储器后才能提供给 CPU 使用。

3）总线

总线(bus)是贯穿整个系统的共享信息传输的通道。在计算机系统中必须相互连接的各功能部件之间,一般采取两种连接方式：一种是通过单独的连线互连,这种方式称为分散连接；另一种是将多个部件连接到一组公共信息传输线上,这种方式称为总线连接。

早期的计算机基本采用分散连接方式,运算器、控制器、存储器和输入/输出设备等组成部件之间基本都由单独的连接线连接。这种连接方式可以获得较高的数据传输速度,但扩展性和灵活性差；现代计算机系统多采用总线结构,且根据功能不同提供了多种类型的总线,为部件之间的连接和信息交换提供通路。总线结构的优点是系统结构清晰、灵活性强且成本低。

4）输入/输出设备

一个计算机系统提供了功能丰富的多种多样的输入/输出(I/O)设备,以满足不同的应用需要。主要的输入设备有鼠标、键盘、扫描仪等,主要的输出设备有显示器、打印机等。

5）I/O 接口

每一个 I/O 设备都通过一个控制器或适配卡与 I/O 总线相连。控制器与适配卡之间的区别在于它们的封装方式不同,控制器一般置于 I/O 设备本身或系统的主印制电路板(通常称为主板)的芯片组中,而适配卡是一块插在主板插槽上的功能卡。控制器和适配卡的功能都是在 I/O 总线和 I/O 设备之间传递信息,因此统称为 I/O 接口。

3.2.2 中央处理器

中央处理器是计算机中负责读取指令,对指令译码并执行指令的核心部件,其功能主要是解释计算机指令以及处理计算机软件中的数据。

1. 指令与指令系统

计算机是通过执行指令来执行某种操作或处理某个数据的,用机器语言编写的程序中每一条语句称为一条指令。每一条指令由一组有意义的二进制代码组成,准确地表述某种语义,命令计算机执行某种操作。

机器语言是根据计算机硬件功能提供的一种编程语言,用机器语言编写的程序称为机器语言程序。机器语言能被计算机自身识别,所以机器语言程序可以在计算机上直接执行。而 C、Python 等高级语言程序无法直接在计算机上执行,只有经过编译程序的编译生成二进制形式的机器语言程序后才能执行。

通常,一条指令包含操作码和地址码两部分,其基本格式如图 3-11 所示。其中,操作码来用来指明指令所要完成的操作,如加、减、乘、除、移位、传送等；地址码用来指出该指令的操作数地址(数据来源)、结果的地址(操作结果的去向)或者下一条指令的地址。

一台计算机能够执行的所有指令的集合便构成了这台计算机的指令系统，如图 3-12 所示。指令系统为计算机软件与硬件之间的沟通提供了所需要的界面。通过指令系统，一方面硬件为软件提供服务，另一方面软件可以使用硬件的功能。

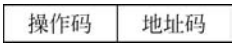


图 3-11　指令格式

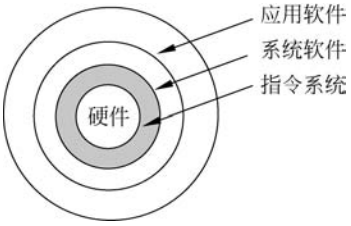


图 3-12　指令系统功能示意图

随着计算机系统从早期的晶体管到现在超大规模集成电路的发展，所支持的指令系统也越来越丰富。尤其到了 20 世纪 70 年代，高级程序已经非常成熟，并得到广泛应用。为了使高级语言得到更多计算机系统的支持，通过缩小机器指令系统与高级语言语义之间的差距，设置一些功能复杂的指令，把一些原来由软件实现的常用功能改由硬件指令来实现，这类计算机就称为复杂指令集计算机(complex instruction set computer，CISC)。

20 世纪 80 年代快速发展起来的精简指令集计算机(reduced instruction set computer，RISC)的思想是尽量简化计算机指令功能，只保留那些功能简单、能够在一个时钟周期内执行完成的指令，而把较复杂的功能用一段子程序来实现。

CISC 和 RISC 是 CPU 所采用的两种类型的指令集，是当前 CPU 的两种不同架构。CISC 和 RISC 的区别在于不同的 CPU 设计理念和方法，它们都是试图在体系结构、操作运行、软件硬件、编译时间和运行时间等众多因素中找到某种平衡，以求达到高效性。不同的 CPU 之间，如果具有相同的基本结构和共同的基本指令集，则指令系统是兼容的，这些兼容计算机上的软件基本可以通用。不同公司生产的 CPU 可能使用相同的指令集，也可能采用各自不同的指令集。例如，AMD 公司和 Intel 公司生产的采用 x86 指令集的 CPU 在软件上是兼容的(图 3-13)；IBM 公司的 Power PC 采用 RISC 指令集，而 Intel 公司的酷睿 CPU 采用 CISC 指令集，两种计算机之间则不兼容。目前，大量工业控制系统、移动终端等嵌入式产品大量采用低功耗的 RISC 处理器，大多数智能手机内部使用的 ARM 处理器也采用 RISC 处理器(图 3-14)。

图 3-13　采用 CISC 指令集的 CPU

图 3-14　采用 RISC 指令集的 CPU

2. CPU 的基本组成

从 1946 年冯·诺依曼计算机产生以来，计算机的 CPU 结构从分散连接到基于总线式，再到流水线式，以及现在广泛使用的多核结构，虽然其结构越来越复杂，但都可以看成是由寄存器、运算器和控制器组成。

1）寄存器

寄存器具有较快的存取速度，用于临时存放数据和状态信息。根据存放信息的不同，寄存器可以分为指令寄存器（instruction register，IR）、程序计数器（PC）、地址寄存器（address register，AR）、数据寄存器（data register，DR）、累加寄存器（AC）、程序状态字寄存器（PSW）等类型。

例如，数据寄存器用来暂时存放由主存储器读出的一条指令或一个数据字；反之，当向主存存入一个数据字时，也暂时将其存放在数据寄存器中。数据寄存器主要作为 CPU 与主存、外设之间信息传输的中转站。

指令寄存器用来保存当前正在执行的一条指令。当执行一条指令时，先把该指令从主存读取到数据寄存器中，然后再传送至指令寄存器。

地址寄存器用来保存 CPU 当前所访问的主存单元的地址。由于在主存和 CPU 之间存在操作速度上的差异，所以必须使用地址寄存器来暂时保存主存的地址信息，直到主存的存取操作完成为止。当 CPU 和主存进行信息交换，即 CPU 向主存存入或取出数据时，或者 CPU 从主存中读出指令时，都要使用地址寄存器和数据寄存器。

2）运算器

运算器是计算机中用于实现数据加工处理等功能的部件，它接收控制器的命令，负责完成对操作数据的加工处理任务。运算器的核心部件是算术逻辑部件（arithmetic logic unit，ALU），ALU 是用来对二进制数据进行加、减等各种基本算术运算，或与、或、非等逻辑运算的部件。

3）控制器

计算机的所有功能都是通过执行程序完成的，而程序由若干条指令组成。CPU 的基本功能就是周而复始地执行指令，控制指令执行的部件就是控制器。在控制器的指挥控制下，运算器、存储器和输入/输出设备等部件协同工作，构成了一台完整的通用计算机。

3. CPU 的性能指标

CPU 的性能对整个计算机系统的性能起着关键作用。CPU 性能主要指 CPU 运行用户程序代码的时间，主要包括以下几方面：

1）机器字长

机器字长指 CPU 一次能够处理数据的位数，通常是 CPU 中整数寄存器和定点运算器的宽度，即一次二进制整数运算的宽度。机器字长越长，数的可表示范围越大，精度越高。如果机器字长较短，那么位数较多的数据必须经过多次的处理才能完成运算，相应地增加了程序的执行时间。按照机器字长，CPU 可以分为 4 位、8 位、16 位、32 位和 64 位几种，目前个人计算机中 CPU 字长有 32 位和 64 位两种，其中较新的 Intel Core i3/i5/i7 等采用 64 位的处理器。

2）主频

主频指 CPU 工作的时钟频率，即在 CPU 内部数字脉冲信号振荡的速度，单位为 Hz。

与主频对应的另一个名词是时钟周期，它是主频的倒数，表示数字脉冲信号振荡一次的时间间隔。

需要说明的是，对于两个不同的 CPU，由于其内部实现结构可能存在差异，所以不同 CPU 的运算速度不能简单地用主频来直接比较，也就是说 CPU 的主频不完全代表 CPU 的运算速度，但是提高主频对于提高 CPU 运算速度起着重要作用。

3）CPU 总线速度

CPU 总线指前端总线，其工作频率影响着 CPU 与内存直接数据交换的速度。根据公式

$$\text{数据带宽} = \frac{\text{总线频率} \times \text{数据位宽}}{8}$$

数据传输最大带宽取决于所有同时传输的数据的宽度和传输频率。在 CPU 性能确定的情况下，总线速度越快则 CPU 性能的发挥越充分。

4）内核数量

早期的 CPU 一直通过提高主频来提升性能，但随着主频的提升其功耗也随之增大，带来了处理器的散热问题。从 2005 年开始，提升处理器性能的方式由单纯地提高 CPU 主频向多核微处理器架构发展。多核技术的基本思路是：简化单个处理器的复杂性，在单个芯片上集成多个处理器核，以多核并行计算来提升 CPU 的性能。例如，一个“8 核”微处理器就是在一个芯片中集成了 8 个处理器核，每个核其实就是一个独立的处理器，CPU 运行时 8 核同时工作，提高了 CPU 的整体性能。

伴随着大规模和超大规模集成电路的迅速发展，芯片的集成密度越来越高，CPU 可以集成在一个半导体芯片上，这种具有 CPU 功能的大规模或超大规模集成电路器件称为“微处理器”。微处理器的发展非常迅速，从 20 世纪 70 年代初 Intel 公司推出 4 位 Intel4004 微处理器以来，微处理器的字长已经到了 64 位，并已广泛应用于个人计算机、嵌入式应用和服务器应用等领域。除用作处理通用数据的 CPU 外，还根据不同的应用出现了专用的处理器，如专用于图像数据处理的图形处理器（graphics processing unit，GPU）、专用于音频数据处理的音频处理单元（audio processing unit，APU）等。

3.2.3　存储器

随着技术的快速发展，出现了多种类型的存储器，以满足不同性能和功能的应用需要，同时同类存储器在性能上得以快速提升。

1. 存储器的分类

数据必须保存在存储介质上。根据计算机的工作原理，存储介质必须具备两个截然不同的物理状态，以分别代表数字“0”和“1”。目前使用的存储介质主要有半导体器件、磁性材料和光介质。其中，由半导体器件构成的存储器称为半导体存储器，由金属或塑料材料的表面涂一层磁性材料作为记录介质的存储器称为磁盘面存储器（主要有磁盘、磁带等），应用激光在记录介质（磁光材料）上进行读/写的存储器称为光盘存储器。

1）按存取方式进行分类

存储器的存取方式主要分为随机存取方式、顺序存储方式和直接存取方式 3 种类型。

(1) 随机存取。随机存取方式的特点是存储器中任何一个单元的内容可以随机存取,且存取时间是一个常数,与存取单元的物理位置无关,如 RAM 存储器。

(2) 顺序存储。顺序存储方式的特点是对存储单元读/写操作时,需按其物理位置的先后顺序访问,存取时间取决于信息的存放位置,如磁带存储器。

(3) 直接存取。直接存取方式兼顾了随机访问和顺序访问的特点,首先可直接选取所需信息的所在区域,然后按顺序存取,如磁盘存储器。

2) 按断电后存储信息是否丢失分类

按断电后存储器中的信息是否丢失,可将存储器分为易失性存储器和非易失性存储器。

(1) 易失性存储器。易失性存储器是断电后原来存储的所有信息将全部丢失,如 RAM 芯片。

(2) 非易失性存储器。非易失性存储器指断电后原来存储的信息仍然存在的存储器,如 ROM 芯片、磁盘、光盘等。

3) 按在计算机系统中的作用分类

按在计算机系统中发挥的作用,可以将存储器主要分为高速缓冲存储器、主存储器和辅助存储器 3 种类型。

(1) 高速缓冲存储器。高速缓冲存储器(cache)是一类存取速度接近于 CPU 的工作速度,介于主存储器与 CPU 之间,用于存放当前 CPU 经常访问的指令和数据的存储器。

(2) 主存储器。主存储器主要用来存放被启动的程序及其数据。

(3) 辅助存储器。辅助存储器主要用来存放不能被 CPU 直接访问的暂时不用的程序和数据。

4) 按 CPU 的可访问性分类

按 CPU 的可访问性,计算机中的存储器可分为内存(内部存储器)和外存(外部存储器)两种类型。

(1) 内存。内存与 CPU 高速连接,保存 CPU 正在执行的程序和处理的数据,其容量相对较小,但速度较快,高速缓冲存储器(cache)和主存储器都属于内存。

(2) 外存。外存与 CPU 不直接相连,其容量相对较大,且成本低,但速度相对较慢,外存用于长久存放大容量的各种程序和数据,主要有磁盘、U 盘等。

2. 存储器的主要性能指标

目前实际使用的存储器中,虽然介质类型多样,主要用途存在差异,但其性能评价指标主要包括容量和速度。

1) 存储器的容量

存储器的容量指存储器可以存放二进制信息的大小,通常用构成存储器的字节数来计量,单位是位(bit,b)、字节(byte,B),目前常见的单块物理存储器的容量大小单位有 GB、TB 等。

计算机主存储器由大量的存储单元组成,每个存储单元都编有一个从 0 开始的线性地址,以便于 CPU 按地址访问。如图 3-15 所示,该存储器采用 6 位地址编址方式(地址数为 $2^6=64$ 个),每个存储单元存放一字节(8 位)二进制数,所以该存储器的容量为 $2^6\times 8b=64B$。目前使用的个人计算机,每个主存储器单元一般存放 1B 的信息,存储容量单元用 MB 或 GB 表示。

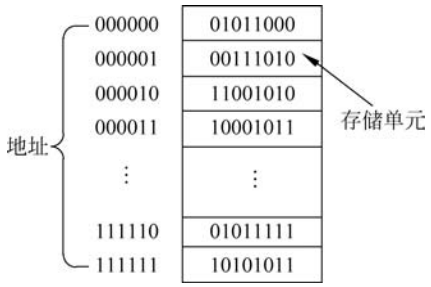


图 3-15　主存储器地址和存储单元

2）存储器的速度

常用于描述存储器速度的指标有存取时间、存储周期和带宽。

（1）存取时间。存取时间指存储器从接到读/写命令开始，到存储器读出/写入数据所需要的时间，即存储器完成一次完整的读/写操作所需要的时间。

（2）存储周期。存储周期指存储器两次连续的存储操作（读/写）之间所需要的时间间隔，存储周期应大于存取时间。

（3）带宽。存储器的带宽指存储器被频繁访问时，可以提供的最大数据传输速率，通常用每秒传送信息的位数来衡量。

3. RAM 和 ROM

RAM（random access memory，随机存储器）和 ROM（read only memory，只读存储器）同属于一种以半导体集成电路作为存储介质的存储器。

1）RAM

根据存储机理，RAM 可分为 DRAM（动态随机存储器）和 SRAM（静态随机存储器）两种类型。

（1）DRAM。DRAM 的集成度高，容量大，功耗小，成本相对较低，但速度慢，主要用于主存（主存储器）。受集成度和功耗等因素的限制，一个 DRAM 芯片的容量有限，通常将多个 DRAM 芯片扩展后集成到一个内存条上，可根据配置需要将多个内存条组合成一台计算机的主存储器 RAM 空间，如图 3-16 所示。

（2）SRAM。SRAM 的集成度低，功耗大，容量相对较小，但速度快，主要用于高速缓冲存储器，目前大多与 CPU 集成于同一个芯片中。

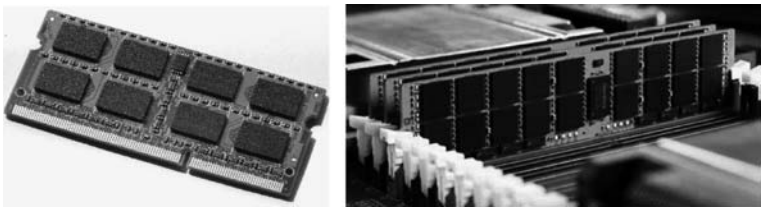


图 3-16　内存条和安装在计算机主板上的内存条

2）ROM

ROM 是一种只读存储器，ROM 中的信息一旦写入，通常情况下只能读取而不能写入。ROM 中的信息在断电后不会丢失。随着技术发展和应用需求的变化，现在某些 ROM 中的

信息也可以写入。例如，闪存(flash memory)在计算机中用于 BIOS 存储器，保存操作系统中的基本输入/输出系统软件。目前广泛使用的 U 盘以及智能产品(如智能手机、数码相机)中的存储器也都使用闪存构成。

4. 常用的外部存储器

随着技术的发展，外部存储器变得非常丰富，软盘作为较早使用的外部存储介质已经被淘汰，目前主要使用的外部存储器主要有以下几类：

1) 硬盘

从 IBM 公司 1956 年开始使用磁盘以来，硬盘成为计算机中主要使用的一种外部存储器。硬盘是一种非易失性存储器，可以长久保存大量的程序和数据。目前的硬盘主要包括两种类型：机械式硬盘和固态硬盘。

(1) 机械式硬盘。机械式硬盘主要由磁记录介质、硬磁盘驱动器和磁盘控制器 3 部分组成。其中，磁记录介质用来保存信息；硬磁盘驱动器主要由多张(一般为 1～5 张)盘片和磁头、电子机、移动臂及控制电路等密封在一个盒子中形成，其内部结构和工作示意图如图 3-17 所示；磁盘控制器是主机与硬磁盘驱动器之间的接口，提供了主存储器与硬盘之间的高速数据传输。目前，服务器一般使用 SCSI(small computer system interface，小型计算机系统接口)、SAS(Serial Attached SCSI，串行 SCSI)和 FC(fibre channel，光纤通道)等接口，而个人计算机主要使用 IDE(integrated drive electronics，电子集成驱动器)和 SATA (Serial ATA，串行 ATA)接口。

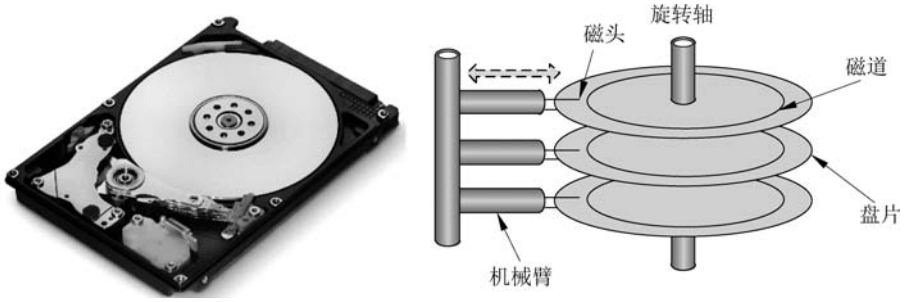


图 3-17　硬盘的内部结构及工作示意图

盘片一般由铝合金或玻璃制成，在上面涂一层磁性材料，通过磁性材料的磁化来记录数据。磁头是实现“磁”信号与“电”信号之间信息转换的元件。如图 3-18 所示，当电动机带动盘片旋转时，磁头处于某一位置上，磁头会在盘片表面划出一个圆形轨迹，每个同心的圆形轨迹称为一个磁道(track)，每个磁道都有一个编号，处于最外面的是 0 磁道。在由多个盘片组成的硬盘中，处于同一半径圆的多个不同盘面的磁道组成一个圆柱面(cylinder)。盘片上的每个磁道被分为多个弧段(一般为 100～500)，每个弧段称为一个扇区(sector)，每个扇区的容量一般为 512B 或 4KB，其中硬盘第一个扇区称为引导扇区。磁盘上的数据以扇区为单位进行读写，所以硬盘上定位数据的地址需要 3 个参数：磁头号(盘面号)、磁道号和扇区号。在操作系统中，将相邻的多个扇区组合在一起形成一簇，以便于操作系统对硬盘文件进行管理，所以簇是操作系统中硬盘文件存储管理的最小单位。

硬盘存储器的平均存取时间与硬盘的旋转速度、磁头的寻道时间和数据的传输速率有

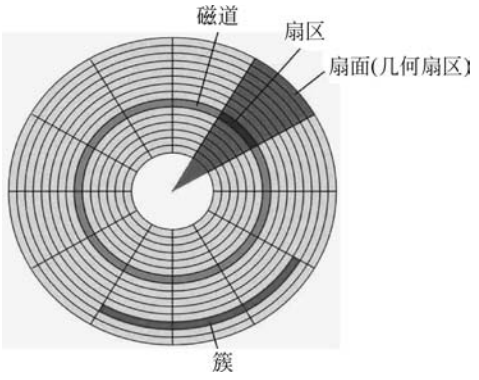


图 3-18　一张盘片上磁道、扇区和簇之间的关系示意图

关。在硬盘工作时，由于盘片的旋转和磁头的径向移动都是机械运动，所以机械式硬盘的速度较慢。目前的硬盘速度一般有 5400r/min、7200r/min、100 00r/min 和 15 000r/min（其中，r/min 表示 revolutions per minute，即每分钟的转数）。

（2）固态硬盘。固态硬盘（solid state drives，SSD）由控制单元和固态存储单元组成。根据所采用存储介质的不同，主要分为采用 Flash 芯片（闪存）的固态硬盘和采用 DRAM 芯片的固态硬盘两种类型。目前使用的固态硬盘多采用 Flash 芯片作为存储介质。

图 3-19 所示是固态硬盘的内部结构和工作原理示意图。一个 SSD 主要由一个或多个闪存芯片和闪存转换层（flash translation layer，FTL）组成。其中，闪存芯片相当于用来存放程序和数据的磁盘，FTL 相当于磁盘控制器，负责控制如何访问这些闪存以及与外部总线的交互。具体来说，FTL 主要有两大功能：①将操作系统对闪存的访问操作虚拟成为磁盘操作，以便于操作系统像访问磁盘一样访问闪存；②实现对存储单元的均衡使用，即磨损平衡（wear leveling）处理，以提高 SSD 的使用寿命。

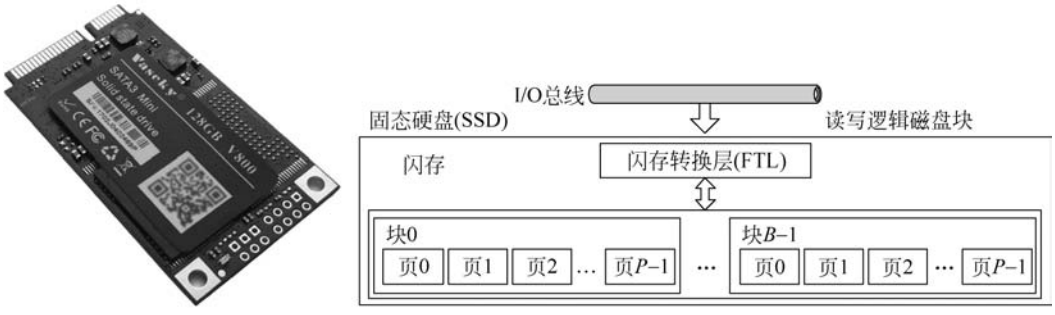


图 3-19　固态硬盘的内部结构与工作示意图

一个闪存由多个块组成，每个块一般由 128～256 页组成，每页的大小为 4～8KB。数据以页为单位进行读写，数据在被正确写入一页之前，页面必须保持清空状态。闪存一次只能擦除一个块，而不是一页，在一个块被擦除后，块中每页都可以写一次。由于闪存块的擦除次数是有限的，如果对其中的某页进行了频繁的写操作，则该页所在的闪存块可能提前达到使用寿命而损坏。所以，为了提高闪存的使用寿命，FTL 采用了磨损平衡处理算法来均衡对闪存中页的操作。

与机械式硬盘相比，SSD 的速度快，噪声低，防震性好，启动速度快。但 SSD 的读写次数受限，一旦出现数据损坏，恢复比较困难。目前，在计算机中广泛使用 SSD 来替代机械式硬盘。

2）光盘存储器

光盘是一种辅助存储器，主要由光盘盘片和光盘驱动器组成。其中，光盘的盘片是一种耐热的有机玻璃，通过在盘片上压制凹坑从而形成“坑”与“岸”来分别表示二进制数“0”和“1”，这种“坑”与“岸”实际上是一种物理信号；光盘驱动器实现对光盘数据的读写，读写头是用半导体激光器和光路系统组成的光头，利用光头发出的激光束来进行信息读写。

根据所采用激光类型的不同，光盘分为使用红光的 CD 盘与 DVD 盘，以及使用蓝光的 BD 盘 3 种类型。其中，CD 盘和 DVD 盘的物理大小相同，但所使用的激光波长、光斑直径、“坑”与“岸”间的宽度等参数不同；另外，DVD 盘有单层单面、单层双面、双层单面、双层双面几种类型，其容量要远远大于 CD 盘。一般的 CD 盘容量为 650MB，而单层单面 DVD 盘可以达到 4.7GB。BD（blu-ray disc，蓝光光盘）是目前容量较大的一类光盘，它利用波长更短的蓝光激光来读写信息，单层盘片的容量可达到 25GB，读写速度可以达到 432Mb/s。

根据是否具备读写功能的不同，光盘可分为只读光盘、一次性写入光盘和可擦写光盘 3 种类型。其中，只读光盘存储的内容由生产厂家预先用激光在盘片上蚀刻而成，信息不能改写，CD-ROM、DVD-ROM 和 BD-ROM 都是只读光盘；一次性写入光盘指用户可以写入一次，但写入后不能再次擦写，只能将数据追加在盘片的空白位置处的光盘，CD-R、DVD-R、DVD＋R 和 BD-R 都属于一次性写入光盘；可擦写光盘指像硬盘一样可重复进行读写的光盘，CD-RW、DVD-RW、DVD＋RW 和 BD-RW 都属于可擦写光盘。光盘驱动器的类型与光盘类型是一一对应的。

3）移动硬盘

移动硬盘（mobile hard disk）其实质就是硬盘，只是为了满足移动应用，将硬盘安装在外围的盒子中，再通过计算机提供的 USB、eSATA 、Thunderbolt 雷电等有线接口以及 Wi-Fi、蓝牙（blue tooth）等无线方式，为数据的读写提供支撑。

4）U 盘

U 盘（USB flash disk）也称为“优盘”，是一种使用 USB 接口的无须物理驱动器的微型高容量移动存储产品，通过 USB 接口与计算机连接实现即插即用。U 盘通常使用塑料或金属外壳，内部含有一张小的印制电路板，通过闪存（flash memory）进行数据存储。

5）存储卡

存储卡是一种以插卡的形式，主要用于智能手机、数字照相机、数码播放机等数据产品的独立存储介质。存储卡也是以闪存作为存储介质，其容量大小与 U 盘相当。存储卡的兼容性较好，而且具有体积小、使用便捷等特点，所以应用较为广泛。

存储卡的种类较多，目前主要有 MMC 系列、SD 系列、记忆棒、CF 卡、TF 卡等类型。其中，MMC（multi media card，多媒体卡）主要用于数码相机、智能手机等产品；SD（secure digital card，安全数据卡）主要用于数码相机、平板电脑、智能手机等产品；CF（compact flash card，紧凑闪存卡）主要用于数码相机；TF（trans flash card，反式闪存卡）也称为 micro SD 卡，可插 SD 卡转换器作为 SD 卡使用，在摩托罗拉产品中较常使用；记忆棒（memory stick）是由日本索尼公司最先研发出来的移动存储媒体，主要用于索尼和爱立信的数码产

品中，当用于笔记本电脑时，相当于计算机的硬盘。

读卡器(card-reader)指将存储卡作为移动存储设备进行读写的接口设备。由于存储卡的类型较多，所以对应的读卡器也有多种类型。例如，按照端口类型不同可分为串行口读卡器、并行口读卡器和 USB 读卡器等；按照操作时是否与存储卡直接接触，分为接触式读卡器和非接触式读卡器。当存储卡插入智能手机、数字照相机、笔记本电脑对应的插槽时，这些设备将实现读卡器的功能。图 3-20 所示是目前常见的存储卡以及取证工作中使用的专业读卡器(在一台设备上可同时读取多种类型的存储卡)。

图 3-20　存储卡和多功能读卡器

3.2.4　总线与 I/O 接口

计算机内部各元器件之间以及计算机与外部设备之间进行数据交换时，都需要借助相应的通道，并遵循相应标准规范，计算机总线与 I/O 接口就负责完成这些功能。

1. 总线

现代电子计算机采用冯·诺依曼“存储程序”工作方式，计算机所有功能的实现都是依赖程序的执行。程序在执行过程中，需要在 CPU、存储器和 I/O 模块之间频繁地交换指令和数据，总线的作用便是连接不同功能部件，为不同部件之间提供规范化的数据(包括指令)交换方式。

带宽(也称为总线带宽)是衡量总线性能的一个非常重要的指标，表示单位时间内总线上能够传输的最大数据量。带宽的计算公式为

带宽(MB/s)＝数据线宽度(bit/8)×总线工作频率(MHz)×每个总线周期的传输次数

计算机系统中存在多种类型的总线，不同类型的总线在不同层次上为部件之间的连线和数据交换提供共享通道。计算机中的总线按功能和规范可分为 5 大类型。

1) 数据总线

数据总线(data bus)是在 CPU 与 RAM 之间共享需要处理或存储的数据通道。数据总线的位数是衡量计算机性能的一个重要指标，通常与微处理器字长相一致。例如 Intel 酷睿 i7 的字长是 64 位，其数据总线宽度也是 64 位。常见的数据总线有 ISA、EISA、VESA、PCI、PCI-E 等。图 3-21 所示是各类 PCI 和 PCI-E 插卡和主板上对应的插槽。

需要说明的是，数据的含义是广义的，它可以是真正的数据，也可以是指令代码或状态信息，有时甚至是一个控制信息。因此，在实际工作中，数据总线上传送的并不一定仅仅是真正意义上的数据。

2) 地址总线

地址总线(address bus)是专门用来传送地址的一种总线类型。由于地址是 CPU 访问

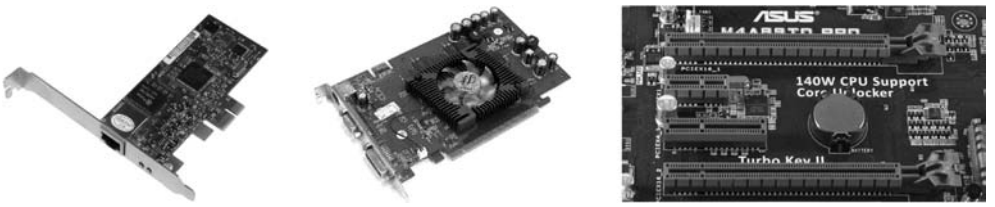


图 3-21　各类 PCI 和 PCI-E 插卡和插槽

外部存储器或 I/O 接口的标识，所以地址总线的位数决定了 CPU 可直接寻址的内存空间大小。一般来说，如果地址总线为 n 位，则可寻址空间为 2^n。例如，一个 32 位地址总线的可寻址空间为 $2^{32}=4$GB。

3）控制总线

控制总线(control bus)用来传送控制信号和时序信号。控制信号中，有的是微处理器送往存储器和 I/O 接口电路的，如读/写信号、中断响应信号等；也有的是其他部件反馈给 CPU 的，例如中断申请信号、复位信号、设备就绪信号等。因此，控制总线的传送方向由具体控制信号而定，数据一般是双向的。

4）扩展总线

扩展总线(expansion bus)是外部设备和计算机主机进行数据通信的总线，例如 ISA 总线、PCI 总线等。

5）局部总线

局部总线(local bus)是用于取代更高速数据传输的扩展总线。

以上 5 类总线中，数据总线、地址总线和控制总线也统称为系统总线，即连接 CPU、存储器和 I/O 模块之间的总线。

2. I/O 接口

I/O 接口的功能是通过制订规范的速度、时序、信息格式、信息类型等参数，将 I/O 设备与主机(CPU 和内存)联系在一起，实现主机与 I/O 设备之间的数据交换。在计算机中，鼠标和键盘等设备的功能相对简单，其 I/O 控制器集成在主板上，而显示器、网络、音/视频等设备的功能相对复杂，其 I/O 控制器有些集成在主板上，而有些则以扩充卡(或适配卡)的形式插在主板的扩展插槽(如 PCI-E 总线插槽)中。图 3-22 所示是计算机中显示器连接的示意图和逻辑组成图，其中显卡插在主板的扩展插槽中，一端通过电缆连接显示器，另一端通过主板上的总线(如 PCI-E 总线)与 I/O 总线连接。

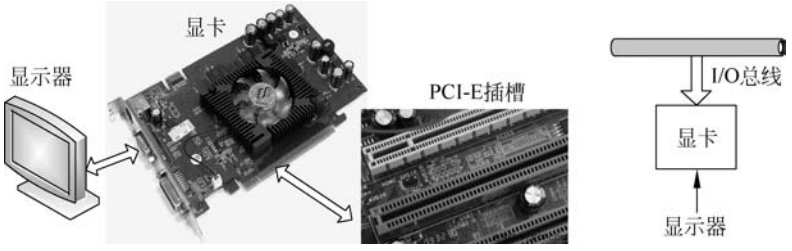


图 3-22　显示器连接示意图和逻辑组成图

严格地讲，I/O 接口是 I/O 控制器和对应的连接器的总称，I/O 接口的一端连接 I/O 总线，进一步与主机连接，另一端连接电缆，进一步与 I/O 设备连接。I/O 接口为 I/O 设备与主机之间的数据通信提供连接服务，所以 I/O 接口也称为 I/O 设备接口。通常情况下，把用于连接 I/O 设备的连接器接头（插座或插头）和相应的通信规程及电气特性称为 I/O 接口。

随着计算机应用的快速发展，I/O 设备的种类日益丰富的同时，也使得同一设备类型快速迭代，导致不同设备之间的连接速度存在较大差异；另外，当 I/O 设备与 CPU 通信时，都需要由 I/O 接口提供一个数据缓冲区来匹配两者之间的速度。同时，为了保证不同组件之间能够正常通信，需要由 I/O 接口对数据格式进行转换，通过 I/O 接口，主机把输入/输出的任务发送给外设，同时把外设的工作状态反馈给主机。例如，在进行打印操作时，主机把打印任务通过 I/O 接口发送给打印机（外设），同时 I/O 接口接收打印机的当前状态（如卡纸故障）并反馈给主机。常用的 I/O 设备接口有 PS/2 接口、USB 接口、VGA 接口、以太网接口、HDMI 接口等，如图 3-23 所示。

图 3-23　计算机主板提供的常见 I/O 设备接口类型

1）视频输出接口

目前常见的视频输出接口有 VGA、DVI 和 HDMI。其中，VGA（video graphics array，视频图形阵列）是 IBM 公司于 1987 年提出的使用模拟信号的计算机显示标准，其工作原理是将计算机内的数字信号转换为模拟信号后发送给显示器；DVI（digital visual interface，数字视频接口）可以直接发送未压缩的数字视频数据到显示器，其接口又分为 DVI-D、DVI-I 和 DVI-A 共 3 种类型，DVI-D 接口只能发送数字信号，DVI-I 接口可以同时兼容模拟和数字信号，而 DVI-A 只能发送模拟信号；HDMI（high definition multimedia interface，高清多媒体接口）是一种全数字化视频和音频发送接口，在同一条线缆上同时发送未压缩的音频及视频信号，主要用于计算机、机顶盒、DVD 播放机、数字电视等设备。

2）USB 接口

USB（universal serial bus，通用串行总线）是一种输入/输出接口技术规范和串口总线标准。通过“USB 集线器”，一个 USB 接口理论上最多可以连接 127 个即插即用设备，广泛

应用于计算机、数字电视、游戏机等数字设备，并逐渐取代了传统的并行口、串行口、PS/2、COM 等接口类型。

1996 年推出的第一代 USB 1.0 的最大数据传输速率只有 1.5Mb/s，1998 年推出的升级版 USB1.1 最大传输速率提升到 12Mb/s；2002 年推出的第二代 USB 2.0，最大传输速率达到了 480Mb/s，并与 USB1.0/1.1 保持了兼容；2008 年推出的第三代 USB3.0 最大传输速率达到了 5.0Gb/s，且向下兼容 USB2.0；最新一代的 USB3.1，其传输速率达到了 10Gb/s。

3）e-SATA 接口

e-SATA 接口是一种外置的 SATA 接口规范，用于外接硬盘。e-SATA 接口使用主板上的 SATA 2 总线资源，其速度要比 USB2.0 快。e-SATA 接口的缺点是无法实现自身供电，需要外接电源。

为了解决 e-SATA 接口无法自身供电的缺陷，推出了 USB Plus 接口。USB Plus 接口是 e-SATA 与 USB2.0 接口的结合体，已开始集成到计算机主板上。

4）IEEE1394 接口

IEEE 1394 接口是苹果公司开发的串行标准，又称火线（firewire）接口。由于 IEEE1394 的传输速率目前可达到 400Mb/s，所以作为一个工业标准的高速串行总线，已广泛应用于数字摄像机、数码相机、电视机顶盒、家庭游戏机、计算机及其外围设备。

3.2.5 输入/输出设备

输入/输出（I/O）设备用于计算机与外部设备之间进行信息交互，是实现人与机器之间联系的关键设备。

1. 输入设备

输入设备（input device）是计算机从外部获取数据和信息的设备，是计算机与用户或其他设备通信的桥梁。输入设备的任务是把数据、指令及某些标志等信息输送到计算机中。计算机既接收数值型数据，也可以接收各种非数值型数据（如图形、图像、声音等）。数值型数据和非数值型数据都可以通过不同类型的输入设备输入计算机后进行存储、处理和输出，常见的输入设备有键盘、鼠标、摄像头、扫描仪、光笔、手写输入板、游戏杆等。

1）键盘

键盘是最常用也是最主要的输入设备，所有英文字母、数字、标点符号等数据和指令的输入都需要借助键盘来完成。计算机上早期使用的键盘为 AT 接口或 PS/2 接口，目前大量使用 USB 接口和无线键盘。根据不同应用，键盘可以分为台式机键盘、笔记本电脑键盘、工控机键盘、智能手机键盘等类型。随着软件技术和应用需求的发展，在某些场景中还使用利用软件模拟键盘功能的“软键盘”。另外，为了提高数据输入的安全性，在某些应用场景中还提供了按键动态变化的软键盘。图 3-24 所示的是 Windows 操作系统自带的软键盘，可通过运行 C:\Windows\system32 目录下的“Osk.exe”程序打开。

2）鼠标

鼠标是一类手持式输入设备，也是一种针对计算机屏幕显示的定位设备，能方便地控制屏幕上的光标移动到指定位置，并通过按键完成各种操作。鼠标按其工作原理可以分为机械鼠标和光电鼠标，其中机械鼠标的底部有一个可运动的圆球，通过圆球的转动来触发 4 个

图 3-24　Windows 操作系统自带的软键盘

方向的电位器，测得上下左右 4 个方向的相对位移量，再通过软件处理和转换，控制屏幕光标箭头相对移动；光电鼠标在其底部的洞里有一个小型感光头，面对感光头的是一个每秒向外发射 1500 次光波的发光管，感光头的作用是将接收到的光波回馈给鼠标的定位系统，以此来实现准确的定位。与机械鼠标相比，光电鼠标具有精度高、可靠性强和耐用等特点。有线鼠标使用 AT 接口、PS/2 接口或 USB 接口，无线鼠标主要利用红外线和蓝牙技术，把鼠标在 X 轴或 Y 轴上的移动、按键按下或抬起的信息转换成无线信号并发送给主机。

3D 震动鼠标是一种新型的鼠标器，它不仅可以当作普通的鼠标器使用，而且具有全方位立体控制能力，具有前、后、左、右、上、下 6 个移动方向，而且可以组合出前右、左下等移动方向，另外还具有震动功能，即触觉回馈功能。例如，在玩某类游戏时，当玩者被敌人击中时，会感觉到鼠标也在震动。

3）触摸屏

与鼠标、键盘等设备一样，触摸屏(touch screen)也是一种定位设备，用户可以直接用手指向计算机输入信息。触摸屏通常是在显示器上覆盖了一层透明的对压力有高敏感性的触摸面板，当触头施加压力在触摸屏上时会产生电流信号，以确定压力源的位置，并对其进行动态跟踪。触摸屏是一种绝对定位设备，它使用绝对坐标，触碰点就是定位点，不需要光标移动。根据触摸的感知数量，触摸屏可分为单点触摸屏和多点触摸屏，其中多点触摸屏可以同时感知触摸屏上的多个触摸点，以方便用户多个手指同时操作屏幕。

4）扫描仪

扫描仪(scanner)是利用光感器件，将检测到的光信号转换成电信号，再将电信号通过模拟/数字(A/D)转换为数字信号后传输到计算机中的一种输入设备。在自然界中，当光束照射物体表面时会发生折射和反射两种现象，扫描仪就利用了这一原理。扫描仪工作时会发出特定波长的强光束到被扫描介质(书稿、照片、胶片等)上，其中没有被折射(吸收)的光束被反射到扫描仪的光学感应器上。光学感应器接收到这些光信号后，将其传送到 A/D 转换器，再由该 A/D 转换器将光信号转换成为计算机可以读取的由“0”和“1”组成的数字信号，同时通过驱动程序将信息显示在显示器上。被扫描介质可以分为反射稿和透射稿，其中反射稿指报纸、书籍、照片等不透明介质的稿件，而透明稿主要有幻灯片(正片)或底片(负片)等类型。

扫描仪的核心部件是 A/D 转换器和感光元件，其中 A/D 转换器的功能是将感光元件接收到的模拟信号(光信号)转换成为计算机可以读取的数字信号；感光元件将感光面上的

光信号转换为与光信号成相应比例关系的电信号，常用的感光元件有 CCD(charge coupled device，电荷耦合器件)和 CIS(contact image sensor，接触式图像传感器)。

CCD 于 1969 年由美国贝尔研究室开发，它使用一种高感光度的半导体材料制成，表面受到光线照射时，每个感光单位会将电荷反映在组件上，即把光线转变成电荷。所有的感光单位所产生的信号加在一起，就构成了一幅完整的画面。CCD 扫描的图像质量高，具有一定的景深，能够扫描凹凸不平的物体，但扫描仪的体积相对较大。

CIS 用在扫描仪中，将感光单元紧密排列，直接收集被扫描介质反射的光线信息。由于 CIS 是接触式扫描(必须与被扫描介质保持很近的距离)，所以只能使用 LED 光源，景深、分辨率以及色彩表现目前都不如 CCD 感光器件，也不能用于扫描透明稿，但 CIS 扫描仪具有体积小、重量轻、生产成本低等优点。

光学分辨率是反映扫描仪扫描图像清晰度的一个重要指标，单位为 DPI(Dots Per Inch，每英寸长度上扫描图像的取样点个数)，其值在 300～2400。DPI 数值越大，扫描图像的质量越高；色彩位数是反映扫描能够产生色彩范围的一个参数，用二进制数表示，其值越大，色彩位数越多，扫描图像的色彩越丰富。例如，1 位的图像，每像素点可以携带 1 位(0 或 1)的二进制信息，只能产生黑或白两种不同色彩，8 位的图像可以给每像素点 8 位的二进制信息，可以产生 $2^8=256$ 种色彩等。

5) 数码相机

数码相机集成了影像信息的转换、存储和传输等部件，是集光学、机械、电子一体化的产品。光线通过镜头(或镜头组)进入相机，经过数码相机成像元件转化为数字信号，数字信号通过影像运算芯片存储在存储设备中，具体过程如图 3-25 所示。

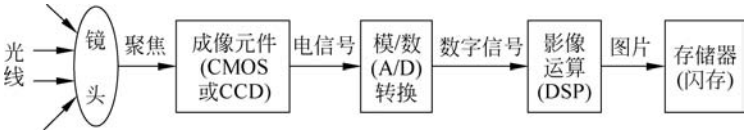


图 3-25　数码相机的成像过程

数码相机的成像元件主要采用 CCD 和 CMOS(complementary metal oxide semiconductor，互补金属氧化物半导体)，两者都是利用感光元件进行光电转换，将图像转换为数字数据，而其主要差异是数字数据传送的方式不同。CMOS 的信号是以点为单位的电荷信号，而 CCD 是以行为单位的电流信号，前者更为敏感，成像速度更快。

数码相机与传统胶片相机在捕捉信号的前端设备上是相同的。数码相机也是使用镜头光圈和快门来聚焦图像，这与传统胶片相机并无区别。但是，传统相机将通过镜头透镜的成像聚焦到感光银盐胶片上，胶片感光将影像以光学模拟信号的方式记录下来。而数码相机则聚焦到 CCD 或 CMOS 图像传感器半导体芯片上，通过扫描产生电子模拟信号，然后经过 A/D 转换形成电子数字信号，再经过压缩，最后以数字文件形式保存在内置的存储器芯片、可拔插的存储卡或外置存储介质上。

像素(pixel)是衡量数码相机成像质量的一个重要指标。像素具体是组成图像的小方格，这些小方格都有一个明确的位置和被分配的色彩数值，众多的小方格决定了该图像所呈现出来的样子。像素是由数码相机里的光电传感器上的光敏元件数目决定的，一个光敏元件就对应一个像素。因此像素越大，意味着光敏元件越多，相应的成本就越高。在使用数码

相机拍照时，经常会有几组数字供使用者选择，如 1024×768、1600×1200、2048×1536 等，每一组数字中，前一数字表示在照片的长度方向上所含的像素点数，后一数字表示在宽度方向上所含的像素点数，两者的乘积就是像素数。例如，1600×1200＝1920000≈2000000，即通常讲的 200 万像素。这 200 万就代表着数码相机的像素数。在具体应用中，像素在一定程度上决定着数码相机的图像质量，但是当像素高于一定数值时就失去了实际的意义，因为目前使用的显示器的分辨率一般为 1366×768 或 1920×1200，如果在这样分辨率的显示器上显示像素过高的图片时，图片将被压缩至当前屏幕的大小，此时有的图片就会出现锐利度过高的情况而失真。同样，在高分辨率的显示器上显示低像素的图片时，需要通过算法在相邻像素之间进行填补，图片将会出现颗粒状，变得很模糊。

6）传感器

传感器与通信、计算机被称为现代信息系统的三大支柱。传感器（sensor/transducer）是能够感受规定的被测量并按一定规律转换成可用输出信号的器件或装置的总称。通常被测量是非电物理量，输出信号一般为电量。如图 3-26 所示，传感器一般由敏感元件、转换元件、变换电路和辅助电源四部分组成。其中，敏感元件用于接收外界的被测量信息，并输出与测量有关的物理量信号，根据感知功能的不同，敏感元件主要分为热敏元件、光敏元件、湿敏元件、气敏元件、力敏元件、声敏元件、磁敏元件、色敏元件、味敏元件和放射性敏感元件等大类；转换元件用于将敏感元件输出的物理量信号转换为电信号；变换电路负责将转换元件输出的电信号进行放大、调制等处理；辅助电源用于为系统提供电能。

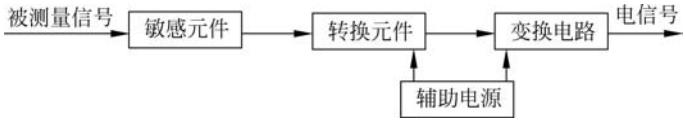


图 3-26　传感器的组成示意图

目前，传感器经历了三个发展阶段。其中，1969 年之前属于第一阶段，主要表现为结构型传感器，它利用结构参量变化来感受和转化信号。例如，电阻应变式传感器，它是利用金属材料发生弹性形变时电阻的变化来转化电信号。1969 年之后的 20 年属于第二阶段，主要表现为固态传感器。这种传感器由半导体、电介质、磁性材料等固体元件构成，是利用材料某些特性制成的。例如，利用热电效应、霍尔效应、光敏效应，分别制成热电偶传感器、霍尔传感器、光敏传感器等。1990 年到现在属于第三阶段，主要表现为智能传感器。智能传感器由传感元件、信号调理电路、控制器（或处理器）组成，具有数据采集、转换、分析甚至决策功能。智能化可提升传感器的精度，降低功耗和体积，从而扩大传感器的应用范围，使其发展更加迅速有效。智能化、微型化、仿生化是未来传感器的发展趋势。

传感器的应用非常普遍。例如，大家广泛使用的智能手机就集成了加速度、方向、磁力、陀螺仪、光线、压力、距离、温度等众多的传感器，用来丰富手机的应用功能。

2. 输出设备

输出设备（output device）用于把计算或处理的结果或中间结果以人能识别的各种形式（如数字、符号、字母等）表示出来，常见的输出设备有打印机、显示器、绘图仪、影像输出系统、语音输出系统、磁记录设备等。

1）打印机

打印机是将计算机的中间处理过程或运算结果以人所能够识别的数字、字母、符号和图形等形式，按照规定的格式输出到介质（如纸张）的设备。根据实现技术的不同，打印机主要分为针式打印机、喷墨打印机和激光打印机。

（1）针式打印机。针式打印机是通过打印头中的多根针（主要有 9 针和 24 针）来击打色带，色带上的油墨在打印纸上印出字符或图形。针式打印机由打印机械装置和控制与驱动电路两部分组成，针式打印机在正常工作时有三种运动：打印头的横向运动，打印纸的纵向运动和打印针的击打运动。目前，针式打印机还广泛应用于表格和票据处理等领域。

（2）喷墨打印机。喷墨打印机在工作时会从喷头喷出小墨滴，从而在纸上形成输出图案。在一个打印喷头上一般至少有 48 个独立的喷嘴，每个喷嘴会根据打印需要喷出不同颜色的墨滴，不同颜色的墨滴落在同一点上便形成不同的复色。目前，喷墨打印机在大尺寸输出（如巨幅广告等）领域的应用非常广泛。

（3）激光打印机。激光打印机是将激光扫描技术和电子照相技术相结合的打印输出设备。打印机从计算机接收二进制信息，然后通过视频控制器转换成视频信号，再由视频接口/控制系统把视频信号转换为激光驱动信号，接着由激光扫描系统产生载有字符信息的激光束，最后由电子照相系统将激光束成像并转印到介质（如纸张）上。由于激光打印机的打印速度快、成像质量高且成本逐步降低，所以目前的应用最为广泛。

衡量打印机的指标主要有分辨率、速度、幅面大小和功耗等，其中分辨率最为重要。打印机分辨率又称为输出分辨率，指在打印输出时横向和纵向两个方向上每英寸最多能够打印的点数，通常以 DPI（dot per inch，点/英寸）表示。打印机分辨率越高，输出的效果就越精密。打印分辨率一般包括纵向和横向两个方向，一般情况下激光打印机在纵向和横向两个方向上的输出分辨率几乎相同，而针式打印机和喷墨打印机在纵向和横向两个方向上的输出分辨率相差较大。一般情况下，喷墨打印机的分辨率指横向喷墨表现力，例如 800×600DPI，其中 800 表示打印幅面上横向方向显示的点数，600 则表示纵向方向显示的点数。

2）3D 打印机

普通打印机只能在平面介质上打印输出字符、图形等资料，而 3D 打印机理论上可以打印出房子、衣服、汽车等物品。3D 打印技术也称为增材制造技术，是相对于传统的机加工等“减材制造”技术而言的，基于离散/堆积原理，通过材料的逐渐累积来实现制造的技术。3D 打印机利用计算机将成型零件的 3D 模型切成一系列一定厚度的“薄片”，3D 打印设备自下而上地制造出每一层“薄片”最后叠加成三维的实体零件。这种制造技术无须传统的刀具或模具，可以实现传统工艺难以或无法加工的复杂结构的制造，并且可以有效简化生产工序，缩短制造周期。

近年来，3D 打印技术取得了快速的发展，所用的材料种类越来越丰富，成型结构越来越复杂，零件的精度越来越高，应用范围不断扩大。3D 打印技术具有如下特点和优势：

（1）数字制造。借助 CAD（computer aided design，计算机辅助设计）等软件将产品结构数字化，驱动机器设备加工制造成器件。

（2）降维制造（分层制造）。把三维结构的物体先分解成二维层状结构，逐层累加形成三维物品。因此，原理上 3D 打印技术可以制造出任何复杂的结构，而且制造过程更柔性化。

（3）直接堆积制造。采取“从下而上”的堆积方式，一次性直接“打印”出任何高性能难

成型的部件，不需要通过组装拼接等复杂过程即可实现。

（4）快速制造。3D打印制造工艺流程短、全自动，可实现现场制造，因此，制造更快速、更高效。

3）显示器

显示器是计算机系统和各类电子设备中最基本的输出设备。计算机中的显示器通过显示适配卡（显卡）与计算机相连，将计算机中的数字信号转换为光信号后直接在屏幕上显示出来。根据制造材料的不同，显示器可分为阴极射线管（cathode ray tube，CRT）显示器、液晶显示器（liquid crystal display，LCD）和等离子（plasma display panel，PDP）显示器等类型。

（1）阴极射线管。阴极射线管显示器是一种早期广泛使用的显示器，在荧光屏上涂满了按一定方式紧密排列的红、绿、蓝（R、G、B）三种颜色的荧光粉点或荧光粉条，称为荧光粉单元，相邻的红、绿、蓝荧光单元各一个组成一组称为像素。每像素中都拥有红、绿、蓝三基色。电子枪发射电子束，电子束聚焦到荧光屏，激发屏幕内表面的荧光粉来显示图像。由于其体积庞大，制造和使用成本较高，CRT显示器已逐步被市场淘汰。

（2）液晶显示器。液晶显示器是一种采用液晶为材料的显示器。液晶是介于固态和液态之间的有机化合物。液晶具有旋光效应，在电场作用下，液晶分子会发生排列上的变化，当通电时导通，液晶有序地排列，使光线通过；不通电时液晶排列混乱，阻止光线通过。在彩色LCD面板中，每一个像素都由3个液晶单元格构成，其中每一个单元格前面都分别有红色、绿色或蓝色的过滤器。显示器根据需要控制每一个液晶粒子转动到不同颜色的面，来组合成不同的颜色。通过对电场的控制，经过不同单元格的光线就可以在屏幕上显示出不同的颜色，达到显示图像的目的。LCD相对于CRT体积更小更轻便，且成本低、能耗低，目前已替代CRT成为主流。

（3）LED显示器。LED（light emitting diode，发光二极管）显示器指直接以LED作为像素发光元件的显示器，组成阵列的发光二极管直接发出红、绿、蓝三色的光线，进而形成彩色画面。但由于发光二极管本身直径较大，因此同色像素之间的距离也较大，所以LED显示器通常来说只适于大屏幕显示。目前，LED显示器已广泛应用于大型广场、商业广告、体育场馆、信息传播、新闻发布等场景。

需要说明的是，LED显示器和LED背光显示器是两个完成不同的概念。液晶本身并不发光，需要使用另外的光源。传统的液晶显示器使用CCFL（cold cathode fluorescent lamp，冷阴极荧光灯管）作为背光源，现在可以用LED作为背光源，于是在LCD显示器的基础上出现了LED背光显示器。所以，LED背光显示器是液晶显示器的一种类型。

（4）等离子显示器。等离子显示器（plasma display panel，PDP）是采用了高速发展的等离子平面屏幕技术的显示设备，其成像原理是在显示屏上排列大量密封的小低压气体室，通过电流激发使其发出人类肉眼看不见的紫外光，再由紫外光碰击后面玻璃上的红、绿、蓝三色荧光体发出肉眼可以看见的可见光，以此成像。PDP具有不受磁力和磁场影响、机身薄、屏幕大、色彩鲜艳、画面清晰等优点。

（5）3D显示器。传统的3D电影采用互成角度的两台摄影机拍摄，从而同一时刻在荧幕上有两组图像（来自不同摄影机），观众戴上偏光镜后通过消除重影，让一只眼只接收一组图像，从而形成视差，产生立体感。平面显示器要形成立体感的图像，必须至少提供两组相位不同的图像。还有一种不用戴上眼镜来观看立体影像的“真3D技术”，它是利用“视差栅

栏”提供存在90°相位差的两组图像，使两只眼睛分别接收不同的图像，从而形成立体效果。

3.2.6 智能手机的硬件

1993年，美国IBM公司推出世界上第一款智能手机Simon，为智能手机的发展奠定了基础。2007年，美国苹果公司发布了第一代iPhone，并于2008年7月11日推出了iPhone 3G，从此智能手机进入了一个快速发展的时代。

1. 智能手机的硬件组成

从技术实现看，智能手机就是一台个人计算机，具有独立的操作系统和运行空间，用户可以根据需要自行安装软件（如即时通信、导航、在线支付等），并可以通过移动通信网络（如4G、5G等）或Wi-Fi等无线方式接入网络。智能手机的硬件主要包括CPU、RAM、ROM、GPU、触摸屏、摄像头、射频芯片等。

1）CPU

与个人计算机一样，CPU是智能手机的核心，其中核数和主频是CPU的重要指标。智能手机伴随着个人计算机进入多核时代，从单核发展到双核、四核、八核等，多核使智能手机具有更高的性能；单纯从技术看，主频的提升有利于性能的提高，但会带来更大的功耗，所以智能手机CPU不能单纯地提升CPU的主频，而应向着多核发展。

2）RAM和ROM

与个人计算机相同，智能手机的RAM主要为程序的运行提供空间；ROM用于安装智能手机操作系统和应用程序，同时为各类文档（照片、文本、视频等）提供存储空间。

3）GPU

GPU的功能类似于个人计算机的显卡，是一种专门用于在个人计算机、平板电脑、智能手机等上进行图像和图形运算的微处理器。GPU使显卡减少了对CPU的依赖，并进行部分原本CPU的工作，尤其是在进行3D图形处理时，GPU提供了强大的处理能力。

4）触摸屏

智能手机的触摸屏又称为触控面板，相当于个人计算机的鼠标、键盘和显示器，是最基本的输入/输出部件。触控屏是一个可接收触头等输入信号的感应式液晶显示装置，当接触了屏幕上的图形按钮时，屏幕上的触觉反馈系统可根据预先编写的程序来驱动各种连接装置，用以取代机械式的按钮面板，并借由液晶显示画面制造出生动的影音效果。与个人计算机的显示器一样，触摸屏的分辨率越高，显示效果越好。

5）摄像头

摄像头已经成为智能手机的标准配置，主要包括内置和外置两种，内置摄像头指手机内部集成的摄像头，外置摄像头指通过数据线或者其他方式将手机与数码相机进行连接，以此实现拍摄。分辨率是衡量智能手机摄像头性能的主要参数之一，主要由图像传感器决定，分辨率越高，图像就越细腻，效果也越好，但所拍摄图像占用存储空间越大。

6）射频芯片

射频（radio frequency，RF）一般指300kHz～300GHZ范围之间的高频交流变化电磁

波。射频芯片是将无线电通信信号转换成一定的无线电信号波形，并通过天线谐振发送出去的一个元器件(模块)，它包括功率放大器、低噪声放大器和天线开关。智能手机中的射频芯片负责射频收发、频率合成和功率放大，根据应用功能主要有 GPS 导航天线、Wi-Fi 无线网络芯片、蓝牙通信芯片等，这些芯片的数量和性能决定了智能手机的功能和性能。

2. 智能手机的处理器

根据处理器架构的不同，目前智能手机的 CPU 类型主要分为基于精简指令集计算机(RISC)的 ARM 架构和基于复杂指令集计算机(CISC)的 x86 架构。

1) ARM 架构

ARM(advanced RISC machines)是一种精简指令集计算机(RISC)处理器架构，广泛地应用于电信基台、汽车喷射引擎、音响系统、相机引擎等各种嵌入式系统中。ARM 架构仅保留了所必需的指令，实现了对指令集的大幅简化，可以让整个处理器更为简约，所以 ARM 处理器非常适用于移动通信领域，具有低成本、高性能和低耗电的特性。苹果的 iPhone 为 ARM 架构智能手机发展开创了先河，而 Google Android 的出现为其他智能手机厂商针对 ARM 架构进行产品差异化发展提供了平台支撑，ARM＋Android 成为通信领域的一大主流。

2) x86 架构

x86 架构是 Intel 公司推出的一种复杂指令集计算机(CISC)处理器架构，其性能要比 ARM 架构强。x86 架构除广泛应用于个人计算机和服务器领域外，也开始应用在智能手机。2012 年，Intel 公司与联想公司合作开发了全球首款基于 x86 架构的联想 K800 Android 智能手机，x86 架构开始应用于智能手机和平板电脑等终端。

3. SoC 芯片

随着设计与制造技术的发展，集成电路的设计从晶体管发展到逻辑门，现在又发展到 SoC(system on chip，片上系统)设计技术。狭义的 SoC 指信息系统核心的芯片集成，是将系统关键部件集成在一块芯片上；广义的 SoC 指一个同时将微处理器、模拟 IP(intellectual property，知识产权)核、数字 IP 核和存储器(或片外存储控制接口)集成在单一芯片上所形成的微小型系统。

SoC 芯片的应用，意味着在单个芯片上就能完成一个电子系统的功能，而这个系统以前往往需要一个或多个电路板，以及板上的各种电子器件、芯片和互连线共同配合来实现。SoC 有两个显著的特点：硬件规模庞大，通常基于 IP 设计模式；软件比重大，需要进行软硬件协同设计。SoC 在性能、成本、功耗、可靠性以及适用范围等方面都有明显的优势，它是集成电路设计发展的必然趋势。在性能和功耗要求较高的智能手机等终端芯片领域，SoC 已占据主导地位。

3.3　操作系统

硬件是基础，软件是灵魂。人们利用计算机进行科学计算、通信、信息处理、模拟仿真等应用，都是通过相应的软件来实现的。本节重点介绍操作系统的组成和功能。

3.3.1 操作系统概述

1946年世界第一台计算机诞生，此时还没有出现操作系统，计算机工作需要采用手工操作方式；到了20世纪50年代中期，出现批处理系统，它是加载在计算机上的一个系统软件，在其控制下，计算机能够自动地、成批地处理一个或多个用户的作业（这些作业包括程序、数据和命令）；后来，为了改善CPU的利用率，又出现了可以同时把多个程序放入内存，并允许它们交替在CPU中运行且共享系统中的各种硬、软件资源的多道程序系统；再后来，出现了把处理机的运行时间分成很短的时间片，然后按时间片轮流把处理机分配给各联机作业使用的分时系统；紧接着，出现了系统能够及时响应随机发生的外部事件，并在严格的时间范围内完成对该事件处理的实时系统；现在所使用的操作系统可以称为通用操作系统，它可以同时兼有多道批处理、分时和实时处理的功能，或其中两种以上的功能。回顾操作系统的发展，其主要特征是提高资源利用率和增强计算机系统性能，伴随着计算机技术本身及其应用的日益发展，逐渐形成、发展和完善起来。

1. 操作系统的功能

操作系统是用于控制、管理、调配计算机中所有软、硬件资源，并组织控制整个计算机的工作流程的系统软件。如图3-27所示，操作系统在计算机系统中发挥的功能主要体现在以下几方面：

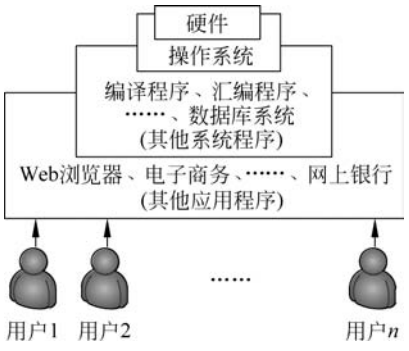


图3-27 操作系统在计算机中发挥的功能

1）管理系统资源

当多个程序同时运行时会需要使用计算机系统资源（硬件资源和软件资源），操作系统则承担着对系统软、硬件资源进行动态调度和分配的任务，从而使不同程序既能够得到运行所需要的资源，又避免了冲突的发生。

2）提供人机交互界面

不管是早期的字符界面，还是目前普遍使用的窗口操作，操作系统都需要提供人机交互界面来实现人与计算机之间的信息交互，使人可以更方便、直观地使用计算机。

3）提供高效率的平台

针对应用程序，操作系统屏蔽了几乎所有硬件的技术细节，从而为开发和运行其他系统软件及各种应用软件提供了一个规范、高效的平台。

2. 操作系统的组成

在现代计算机系统中，作为一种大规模、复杂的系统软件，操作系统一般由内核（kernel）和图形用户界面程序、常用应用程序等配套的软件，以及为支持应用软件开发和运行的各种软件组成。操作系统的组成如图3-28所示。

对于一个操作系统来说，内核是其最核心的部分。内核是为众多应用程序提供对计算机硬件的安全访问的一部分软件，这种访问是有限的，并且内核决定一个程序在什么时候对

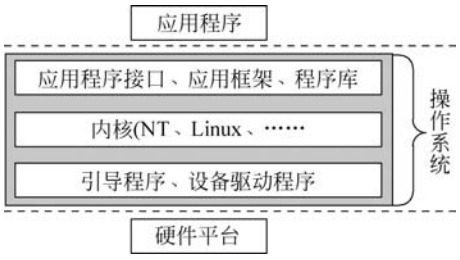


图 3-28　操作系统的组成

某部分硬件操作多长时间。内核是基于硬件的第一层软件扩充，提供操作系统的最基本的功能，是操作系统工作的基础，它负责管理系统的进程、内存、设备驱动程序、文件和网络系统，决定着系统的性能和稳定性。

现代操作系统设计中，为减少系统本身的开销，往往将一些与硬件紧密相关的（如中断处理程序、设备驱动程序等）、基本的、公共的、运行频率较高的模块（如时钟管理、进程调度等）以及关键性数据结构独立开来，使之常驻内存，并对它们进行保护。通常把这一部分称为操作系统的内核。

需要说明的是，内核并不是完整的操作系统。软件公司还需要在操作系统内核的基础上再进行开发，配置各种程序库和应用架构，设计用户界面，提供常用的应用程序和实用程序，然后才能作为一个完整的软件产品供用户使用。用户使用 Linux 操作系统时，经常说某某系统与某某系统使用相同的内核就是这个原因。

当用户使用服务器、个人计算机、智能手机或平板电脑等设备时，实现人机交互功能的就是操作系统。目前，常用的服务器操作系统有 UNIX/Linux、Windows Server、NetWare 等，个人计算机操作系统有 Windows、Linux 等，平板电脑和智能手机操作系统有谷歌公司的 Android、苹果公司的 iOS、塞班公司的 Symbian（后被诺基亚公司收购）、微软公司的 Windows Phone 和加拿大 RIM（research in motion）公司的 BlackBerry OS 等。

3. 操作系统的启动过程

目前，操作系统的启动主要有 BIOS（basic input/output system，基本输入/输出系统）和 UEFI（unified extensible firmware interface，统一可扩展固件接口）两种方式。

1）BIOS 启动方式

BIOS 启动方式也称为 Legacy 启动方式，是在计算机加电时，CPU 首先执行主板上的 BIOS 中的自检程序，测试计算机中主要部件的工作状态是否正常。如果正常，CPU 继续执行 BIOS 中的引导加载程序 bootloader，将系统盘引导程序读入内存，由引导程序继续将硬盘中的操作系统加载到内存。操作系统加载成功后，便接管并控制整个计算机的运行。BIOS 启动的详细过程如图 3-29 所示。

2）UEFI 启动方式

UEFI 用来定义操作系统与系统固件之间的软件界面，作为 BIOS 的替代方案。从本质上讲，UEFI 和 BIOS 的功能都是用于引导操作系统的启动，只是 UEFI 在功能上进行了扩展，最直观的是 UEFI 提供了图形界面操作，允许植入硬件驱动，同时可以减少启动时自检操作，缩短启动过程。UEFI 本身已经发展为一个微型操作系统，支持文件系统，可以使用

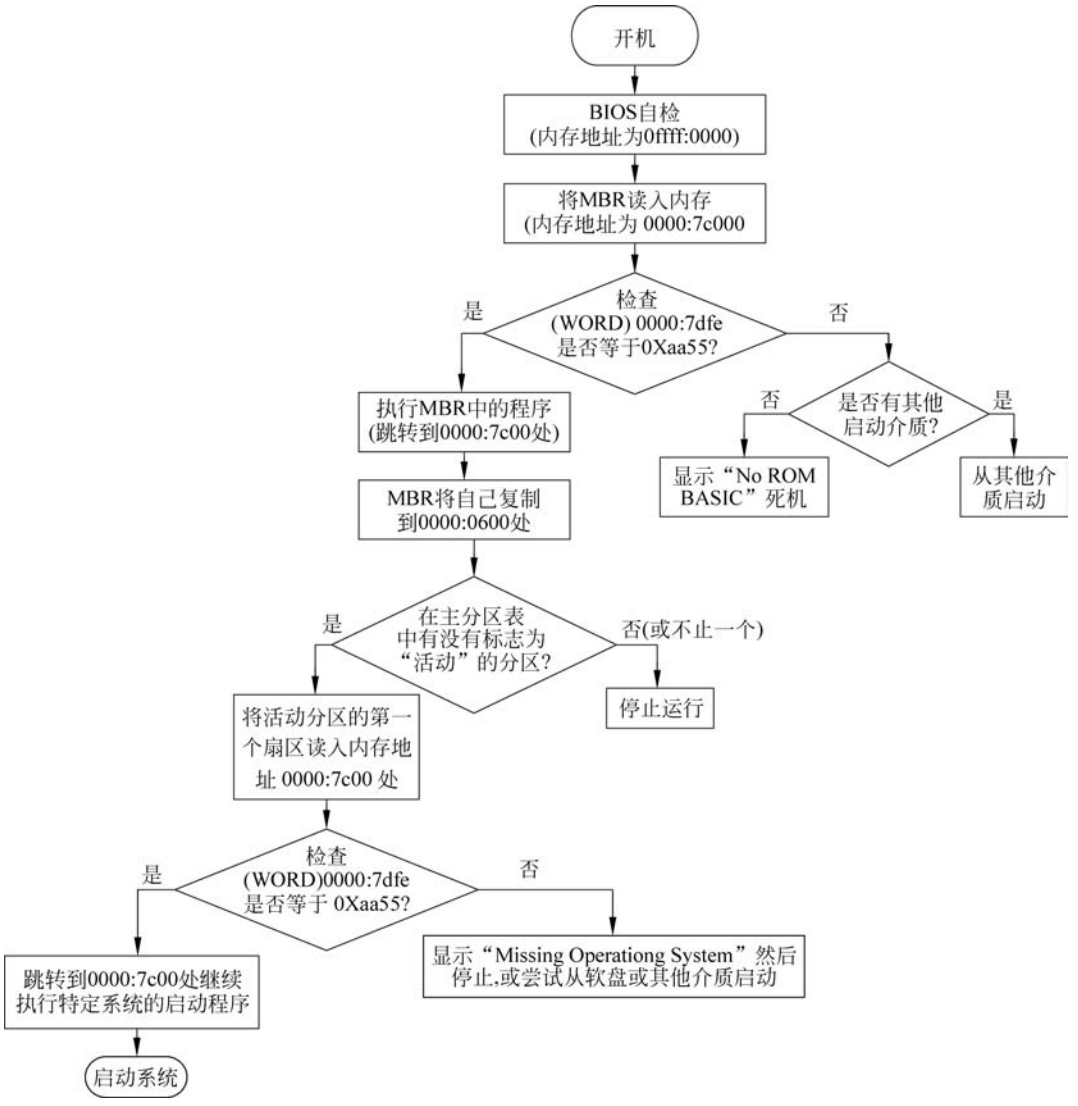


图 3-29　BIOS 启动的详细过程

C 语言在 UEFI 环境下开发应用程序。微软公司从 Windows 8 开始全面支持 UEFI,并默认以 UEFI 方式启动操作系统。目前,各大主板厂商都开始支持 UEFI 启动方式。BIOS 和 UEFI 启动的操作界面分别如图 3-30(a)和图 3-30(b)所示。

(a) BIOS启动方式　　(b) UEFI启动方式

图 3-30　启动方式的操作界面

3.3.2　操作系统的资源管理

操作系统的主要功能是最大限度地利用计算机资源来为用户提供各类服务。操作系统的资源管理主要包括处理器管理、存储管理、文件管理、设备管理等。

1. 处理器管理

处理器是整个计算机的核心。从运行速度来看，处理器要比其他硬件具有明显的优势，而且其他硬件的运行都需要处理器的支持。因此，有效地管理处理器、充分利用处理器的资源是操作系统的首要管理任务。

1）多任务操作系统和单任务操作系统

为了提高 CPU 的利用率，操作系统一般都支持多任务处理功能，即允许多个应用程序同时运行，每一个运行的应用程序称为一个任务。例如，当用户浏览 Web 页面时，同时还在播放音乐或下载文件，这些同时独立运行的应用程序之间互不干扰。Windows 操作系统采用并发多任务方式来支持系统中多个任务的执行。事实上，任何时刻只有一个任务正在被 CPU 执行，其他任务处于等待执行状态。为了实现并发多任务操作，操作系统提供了处理器调度程序负责把 CPU 时间分配给各个任务，这样才能使用户感觉到多个任务在“同时”执行。调度程序其实是一个时分管理程序，按照程序运行需要把 CPU 的一个周期划分为多个时间段，每个时间段称为一个“时隙”，在一个 CPU 周期内，每个程序只能在对应的时隙内运行。

对于具体的操作系统来说，如果允许用户在同一时间运行多个应用程序，则该操作系统称为多任务操作系统；如果一个用户在同一时间只能运行一个应用程序，则该操作系统称为单任务操作系统。

根据在同一时间使用计算机用户的数量，操作系统又分为单用户操作系统和多用户操作系统。其中，单用户操作系统指一台计算机在同一时间只能由一个用户使用，如早期的 DOS 操作系统；而多用户操作系统指一台计算机在同一时间允许由多个用户同时使用，Windows XP 是单用户多任务操作系统，目前广泛使用的 Windows 7/8/10、Windows Server、Linux/UNIX 是多用户多任务操作系统。在多用户操作系统中，可以在同一个操作系统上为多个用户分别创建各自的账户，用户可以利用这些账户通过各自的终端同时使用这台计算机的软硬件资源。

2）进程和线程

为了描述多任务的并发执行，操作系统引入了进程的概念。从技术实现来讲，进程是具有一定独立功能的程序关于某个数据集合上的一次运行活动，是系统进行资源分配和调度的一个独立单位；从应用效果来讲，进程可以看作是正在执行的程序，操作系统通过进程管理来调度多个程序之间的关系。线程是进程的一个实体，是 CPU 调度和分派的基本单位，它是比进程更小的能独立运行的基本单位。线程只是一个进程中的不同执行路径，同一个进程中的多个线程之间可以并发执行。简而言之，一个程序至少有一个进程，一个进程至少有一个线程。从逻辑角度来看，多线程的意义在于一个应用程序中有多个执行部分可以同时执行，但操作系统并没有将多个线程看作多个独立的应用来实现线程的调度和管理以及资源分配，这就是进程和线程的重要区别。

2. 存储管理

存储管理的主要任务是为程序的运行提供所需要的环境支撑，以方便用户使用存储器，在有效利用存储器的同时根据程序运行需要扩充内存。现代操作系统中，存储管理的功能特征主要包括内存分配和回收、内存共享和保护、内存扩充等。

1）内存分配和回收

根据应用特点，内存空间划分为系统区和用户区。其中，系统区用于操作系统的运行；用户区用来存放正在运行的应用程序，每个应用程序运行时都需要属于自己的运行空间，用来存储应用程序的代码和数据。存储管理为每个任务分配存储空间，任务结束后负责收回。

2）内存共享和保护

内存共享指让正在运行的应用程序共享内存空间，从而提高内存空间的利用率。内存保护指使每个程序只在自己的内存空间中运行，彼此互不干扰，且每个应用程序的私有区域不被其他程序修改，同时保护操作系统所在区域不被应用程序修改。

3）内存扩充

内存是外存与 CPU 进行沟通的桥梁，计算机中所有程序的运行都在内存中进行。由于物理内存的容量相对有限，有时难以满足应用程序运行的需要。当内存不够使用时，需要对存储空间进行扩充，把内存和外存结合起来管理。虚拟存储技术是实现内存扩充的主要手段，它把外存当作内存的直接延伸，从而将有限的物理内存与大容量的外存统一组织成一个远大于物理内存的虚拟存储器。一个程序运行时，当所访问的信息不在内存时，则由操作系统负责调入所需部分，其他部分则存于外存。

3. 文件管理

文件管理是操作系统中实现文件统一管理的一组软件、被管理的文件以及为实施文件管理所需要的一些数据结构的总称。文件管理的任务是有效地支持文件的存储、检索和修改等操作，解决文件的共享和安全问题，以使用户方便、安全地访问文件。文件管理涉及文件组织方法、文件的存取和使用方法、文件存储空间的管理、文件的目录管理、文件的共享和安全性等内容。

1）文件

在计算机系统中，所有信息资源都是以文件形式存放在外存储器上，需要时由操作系统调入内存。文件是存储在外存储器上的一组相关信息的集合。计算机中的程序、数据、文档、图像、声音等都组成文件存放在外存储器中，并以文件为单位进行存取操作。

为便于操作，每个文件都有一个文件名，用来标识文件，方便用户访问。一个完整的文件名包括：[盘符名：][路径]<文件名>[.扩展名]。其中，文件名可以由字母、数字和一些特殊字符（如 $、#、@、%、(、)、^、－、＋、}、{、!等）组成，但不能使用\、/、:、*、?、<、>、|、”等字符。在 Windows 操作系统中，文件名可以达到 255 个字符；文件扩展名用于指定文件的类型，用户可以根据文件扩展名来识别某一文件属于哪一类型的文件。另外，为了便于管理，每个文件还包括文件大小、文件时间、文件属性等信息，这些附属信息与文件内容是分开存放的，前者保存在该文件所属的目录中，后者则保存在磁盘的数据区中。

2）文件夹

文件夹也称为目录，是操作系统用来存放和管理文件的方式。文件夹采用树形结构，当

一个磁盘被格式化后就建立了一个根文件夹(根目录),在此基础上可以存放文件和创建子文件夹,以此类推。不同级的文件夹或文件可以同名,但同级的子文件夹或文件不能同名。

3) 文件系统

文件系统的作用是管理文件在外存储器中的存储方式。常见的文件系统有 FAT、NTFS、CDFS、UDF 和 FTL 等。在具体应用中,可以将硬盘划分成多个分区,每个分区可作为逻辑上独立的一个磁盘供用户使用。以 FAT 文件系统为例,在将一个磁盘或分区进行格式化操作后,操作系统将该磁盘或分区划分为 4 部分:

(1) 引导扇区。引导扇区(boot sector)通常指分区的第 1 个扇区,包含本分区使用的文件系统的类型、数据区的大小(共多少个簇)、根目录区允许的目录项最大数目等信息。硬盘的 0 柱面、0 磁头、1 扇区称为主引导扇区,也叫主引导记录(master boot record,MBR),该记录占用 512 字节,是计算机开机以后访问硬盘时所必须读取的第一个扇区,它用于硬盘启动时将系统控制权转给用户指定的、在分区表中登记了的某个操作系统分区。

(2) 文件分配表。文件分配表(file allocation table,FAT)在磁盘格式化时自动生成,一式两份,其中一份作为备份。FAT 用来记录文件所在位置的表格,它以簇号为序,记录每一个簇处于“使用、空闲、损坏”中的某一状态。它对于硬盘的使用是非常重要的,如果文件分配表丢失,那么硬盘上的数据将因无法定位而不能使用。

(3) 文件目录表。文件目录表(file directory table,FDT)是用来存放根目录下的文件的目录项的技术。分区引导扇区中 11H～12H 偏移处的两字节的含义为“根目录项数”,该值一般为 512,即 FDT 中最多只能存放 512 个目录项,假设每个目录项的大小为 32 字节,那么这个 FDT 所占的扇区个数就为 32,假设每个目录项的大小为 64 字节,那么这个 FDT 所占的扇区个数就为 64。如果文件系统支持长文件名,则每个表项为 64 字节,其中,前 32 字节为长文件链接说明,后 32 字节为文件属性说明,包括文件长度、起始地址、日期、时间等。如不支持长文件名,则每个表项为 32 字节的属性说明。

需要说明的是,FAT 分区下,数据在被删除之后,文件对应的文件目录项的第一字节会被改为“E5H”,表示该文件被删除,而文件目录项的其他字节没有变化,所以被删除的文件仍旧能够找到其开始的地方,即该文件是可恢复的。

(4) 数据区。数据区(data area)是紧跟在 FDT 的下一个扇区,直到逻辑盘的结束地址。数据区用于存储所有的数据,存放着本分区所有文件和文件夹的内容。

需要说明的是,即使文件目录被破坏,根据 FDT 和数据区的信息,仍然可能从磁盘里把信息读出,这也就是硬盘数据恢复的依据。

4. 设备管理

设备管理用于管理计算机系统中的所有外部设备,主要功能包括完成用户进程提出的 I/O 请求、为用户进程分配其所需要的 I/O 设备、提高 CPU 和 I/O 设备的利用率、提高 I/O 速度、方便用户使用 I/O 设备等。

3.4　计算机网络

计算机网络是计算机技术与通信技术相结合的产物,是现代信息社会的基石。随着技术的迅猛发展和应用需求迅速变化,计算机网络得到了快速发展,无论是实现技术还是用户

接入方式以及通信质量都在不断迭代中发生着显著变化。本节基于计算机网络的分层模型，以数据特征为基础，从电子数据取证的角度介绍计算机网络的实现技术和应用特点。

3.4.1 计算机网络概述

信息化和全球化是当今世界知识经济的两个重要特点，而信息化和全球化的实现必须依靠完善的网络。这里所说的网络是广义的网络，包括电信网络、有线电视网络和计算机网络，统称为“三网”。三网的核心是计算机网络，目前发展最快的也是计算机网络。本节介绍的重点也是计算机网络。

1. 什么是计算机网络

从技术上讲，计算机网络是计算机技术和通信技术相结合的产物，通过计算机来处理各种数据，再通过各种通信线路实现数据的传输。从组成结构来讲，计算机网络是通过外围设备和连线，将分布在相同或不同地域的多台计算机连接在一起所形成的集合。从应用的角度，只要将具有独立功能的多台计算机连接在一起，能够实现各计算机间信息的互相交换，并可共享计算机资源的系统便可称为网络。综合各方面的因素，我们对计算机网络的定义为：将分布在不同地理位置的多台具有独立功能的计算机通过外围设备和通信线路互连起来，在功能完善的管理软件的支持下实现相互资源共享的系统。此定义强调了计算机网络应具备的 3 个主要特征：

（1）建设计算机网络的主要目的是实现不同计算机之间资源的共享。

（2）组建网络的计算机是分布在不同地理位置的具有独立处理能力的“自治计算机”。

（3）同一网络中的计算机必须使用相同的通信协议。

2. 计算机网络的组成

计算机网络不存在地域的限制，只需要根据连接距离的远近采取不同的连接方式，都可以实现不同计算机之间的互联，并进行计算机之间的资源共享和通信。一个完整的计算机网络包括以下三个组成部分：

1）计算机

根据在网络中所提供的服务的不同，可分为服务器和工作站（也称为客户机）。其中，服务器提供网络中的共享资源，而工作站主要用于访问服务器中的资源。

2）外围设备

包括连接设备和传输介质两部分，其中主要的连接设备有网卡、交换机（早期也使用集线器）、路由器、防火墙等，传输介质主要有同轴电缆、双绞线、光纤、微波和红外线等。

3）通信协议

通信协议是计算机之间在通信时必须遵守的规则，是通信双方使用的通信语言。协议是一组规则的集合，是进行交互的双方必须遵守的约定。在网络系统中，为了保证计算机之间能够正确地进行通信，针对通信中的各种问题，制订了一整套约定，将这套约定称为通信协议。通信协议是一套语义和语法规则，用来规定有关功能部件在通信过程中的操作。

由于网络体系结构具有层次性，所以通信协议也是分层的。通信协议可分成多个层次，每个层次内部又被分成不同的子层，不同层次负责不同的操作。网络协议由以下 3 个要素组成：

(1) 语法。语法是数据与控制信息的结构或格式,包括数据格式、编码、信号电平等。

(2) 语义。语义是用于协调和进行差错处理的控制信息,包括需要发出何种控制信息,完成何种操作,做出何种应答等。

(3) 同步(定时)。同步是对事件实现顺序的详细说明,包括速度匹配、排序等。

通信协议对通信软件和硬件的开发具有指导作用。通信协议描述要做什么,对于怎么做不进行限定。这一特征为软硬件开发商便提供了便利,他们只需要根据协议要求开发出产品,至于选择什么电子元件、使用何种语言开发则不受约束。

3. 计算机网络的分类

可从不同的角度对计算机网络进行分类。例如,根据数据交换方式的不同,可以把计算机网络分为电路交换、报文交换、分组交换和混合交换(同时采用电路交换和分组交换)4 种;按通信介质的不同可以分为有线网络、无线网络和混合网络(有线和无线混合网络)3 种;根据网络连接范围的大小,可以将计算机网络分为局域网、城域网和广域网 3 种;根据使用范围的不同,可以将计算机网络分为公用网和专用网两类;根据传输方式的不同,计算机网络分为广播式网络和点对点式网络两种类型等。

不同的分类方法体现了计算机网络所具有的某一特征,对认识计算机网络的工作原理、组网方式和应用特点是有帮助的,也是在电子数据取证过程中首先要确定的内容。

4. 计算机网络的结构

计算机网络是由多台具有独立功能的计算机组成的一个集合,如何将这些计算机有机组织起来关系到网络的性能。因此,研究计算机网络结构的组成、功能及表示方式对从事电子数据取证工作非常重要。

1) 网络拓扑的概念

拓扑学是几何学的一个应用分支,它是从图论演变过来的。设计网络图时首先需要学会用不同的图标代表不同的设备(如服务器、工作站、交换机、路由器等),然后再用一定的连线将这些设备连接起来,即用不同的连线代表不同的网络连线(即传输介质,如细缆、双绞线、光纤、微波、红外线等)。在网络中,将不同设备根据不同的工作方式进行连接称为拓扑(topology),又称为设计(design)、图解(diagram)、映像(map)、物理布局(physical layout),等等。各种不同计算机网络系统的拓扑结构是不同的,同时不同拓扑结构的网络其功能、可靠性、组网成本等方面也不相同。

由于计算机局域网和广域网的连接范围不同,所采用的技术、连接方式也不一样,所以网络拓扑结构也存在一定的区别。

2) 局域网的结构

目前,局域网中常见的标准拓扑结构有总线型(bus)、星型(star)和环型(ring)三种类型。

(1) 总线型(bus)。如果网络上的所有计算机都通过一条电缆线相互连接起来,这种拓扑结构就称作总线型网络结构,如图 3-31(a)所示。总线型网络结构是最简单的网络结构,其中不需要任何其他的连接设备。网络中的每台计算机均可以接收从某一节点传送到另一节点的数据,所以这种拓扑结构是共享介质的拓扑结构。随着以双绞线和光纤为主的标准化布线的推行,总线型网络已基本退出了网络布线。

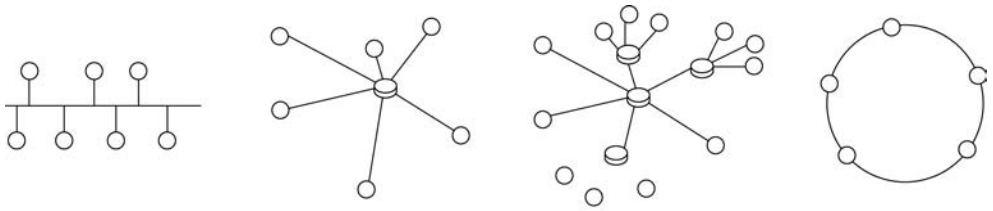


图 3-31　局域网中常见的三种拓扑结构

(2) 星型(star)。早期的计算机之间如果需要相互通信,就要将这些计算机同时连接到一台中央主机上,由主机进行转接,而不是直接进行通信,这就是星型网络拓扑结构的雏形。在现代的星型拓扑结构中,所有的计算机通过各自的一条电缆线与一台中央集线器或交换机相连,如图 3-31(b)所示。

(3) 环型(ring)。环型拓扑结构中的每台计算机都与相邻的两台计算机相连,构成一个封闭的环状,如图 3-31(c)所示。整个结构既没有起点,也没有终点,所以也就不需要总线型拓扑结构中必须要有的终结器。信号在环型结构中沿着固定的方向传播,轮流经过每一台计算机,网上的每台计算机都相当于一台中继器,不仅要接收上一台计算机(先行计算机)发来的信号,而且要放大信号并将它传送到下一台计算机(后继计算机),直到到达它的目的地为止。所以这种网络又称作主动式拓扑结构,在这种网络结构中,任何一台计算机出现故障都会造成环网的中断,从而对整个网络产生影响。

3) 广域网的结构

由于广域网的连接范围较广,其中包括了大量的城域网和局域网,所以广域网的网络结构是城域网和局域网的有机结合。随着网络技术的发展,原来相对独立的计算机网络、公共电话交换网(PSTN)、有线电视网络(CATV)开始走向融合,广域网的组成结构已不再是由单纯的计算机和局域网组成,而是多种网络的有机结合。同时,随着无线射频通信技术的发展,无线局域网和无线城域网技术已成熟,成为广域网中的一个重要组成分支。为此,从接入端来看,今天的广域网中同时包括了局域网、PSTN、CATV、无线局域网和无线城域网等类型,形成了不同类型的接入网。大量的接入网根据地域或管理模式上的划分,组成地区级主干网的城域网。城域网通过光纤或微波与卫星信道等高速线路互联,形成地区级或国家级的广域网。Internet 就是将多个地区级和国家级的广域网互联后,形成的覆盖全球的计算机网络,如图 3-32 所示。

需要说明的是,图 3-32 只是一个广域网的结构示意图,强调了广域网的分层结构以及复杂的接入和互联形式。以 Internet 为主的广域网技术正在飞速发展,相应的网络结构也在发生着变化。

5. 物联网

自计算机技术、互联网和移动通信技术所产生的划时代影响以及创造的丰厚价值之后,物联网(internet of things,IoT)被人们期待成为全球信息产业的又一次产业浪潮,受到了全球许多国家政府、企业、科研机构的高度关注。物联网是现代信息技术发展到一个特定历史阶段时融合了多学科知识的产物,是基于人与人之间的通信方式在快速发展过程中出现“瓶颈”时力求突破现有模式,进而实现人与物、物与物之间通信的应用创新。物联网的出现和

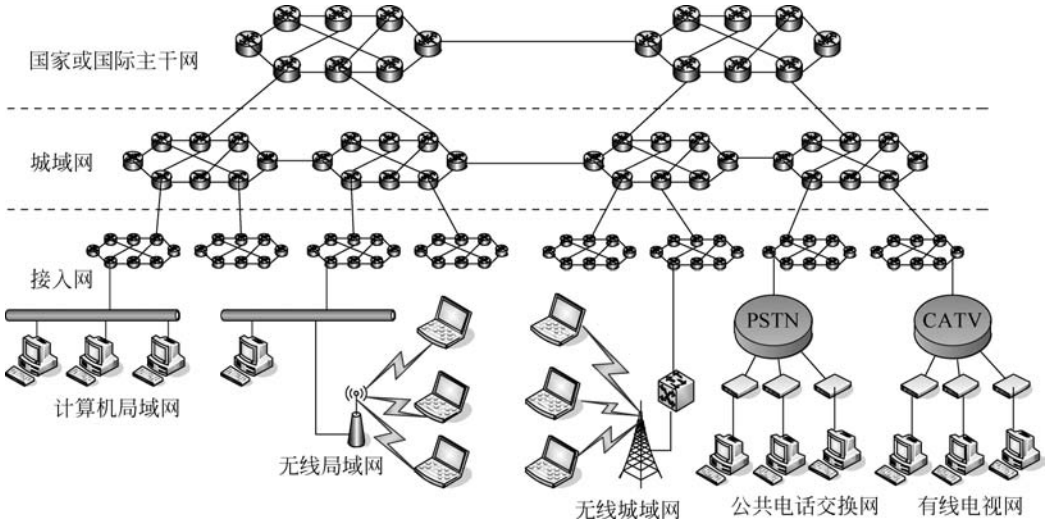


图 3-32　广域网的拓扑结构

应用，代表着信息社会这一客观的发展需求和方向，也标志着互联网的发展步入了一个崭新的阶段，基于智能感知和智慧服务功能的后互联网时代已经到来。

1）物联网的概念

2005 年国际电信联盟（ITU）提出了物联网的概念：物联网是在现有互联网的基础上，利用射频识别（RFID）、无线数据通信、计算机、分布式数据库等技术，构造的一个主要由物品组建的互联网络。2011 年 11 月，ITU-T 下设的物联网全球标准化工作组（IoT-GSI）对物联网给出了一个基本的概念：物联网是全球信息社会的基础设施，物理的和虚拟的物与物之间通过现有的和演进的信息通信技术进行互联，从而提供更加先进的服务。虽然 ITU 在不同时期对物联网概念的描述存在一定的差异，但却给出了物联网的本质特征：物联网是通过 RFID、传感器、摄像机、GPS 等具有标识、感知、定位和控制功能的智能设备来获取物体（虚拟的和物理的）的信息，然后通过通信网络进行互联与管理，利用互联网这一成熟的信息平台为社会各行各业提供面向物体的各类服务。

2）物联网的特征

可将物联网的特征概括如下：

（1）物联网是在现有互联网基础上发展起来的，也称为后互联网，是互联网发展到一定阶段后的必然产物，也是信息技术从以人为主的社会维度应用到物理世界的产物。

（2）嵌入物理对象中实现对象系统智能化的嵌入式系统，是实现物体联网功能的核心，传感器、RFID、摄像机、GPS 等终端都通过嵌入式系统实现与互联网的信息交互，成为物联网的感知神经末梢。

（3）物联网是互联网发展到高级阶段，并在发展中遇到了阻力时的产物。互联网发展到现在，在技术和应用中都遇到了瓶颈，下一代网络（NGN）、云计算、传感网等被认为是有效的解决技术，这些技术正是构成物联网的基本要素。

（4）物联网是计算机学科、通信学科、电子技术学科、微电子学科等多学科交叉融合后形成的一个综合应用技术，从技术现状和发展趋势来看，物联网所需要的不仅仅是单学科的

研究成果，更需要多学科间的交叉融合，但这种融合不是简单的集成，必须解决大量已知和未知的技术与非技术问题。

(5) 智能化、自动化、实时性、可扩展性是物联网必须具备的特征。

3.4.2 计算机网络的分层模型及数据单元

体系结构和通信协议是计算机网络的两大核心内容。了解了体系结构，便能将虚拟的网络空间通过分层模型给出完整的组织结构和清晰的功能划分；掌握了通信协议，便能清楚每一类设备和每一类应用的工作原理和过程。

1. TCP/IP 分层模型

1974 年，美国 IBM 公司公布了 SNA(system network architecture，系统网络体系结构)，这一网络标准只能用于 IBM 大型机之间的互联；1984 年，ISO(international organization for standardization，国标标准化组织)正式发布了开放系统互连(open system interconnect，OSI)参考模型，其结构如图 3-33(a)所示；1983 年 1 月，ARPAnet(Internet 的雏形)已经成为一个纯 TCP/IP 的网络。TCP/IP 模型由应用层、传输层、网际层(也称为 Internet 层)和网络接口层共 4 层组成，其结构如图 3-33(b)所示。在具体应用中，为了便于理解和管理，将 TCP/IP 中的网络接口层细分为物理层和数据链路层，如图 3-33(c)所示。

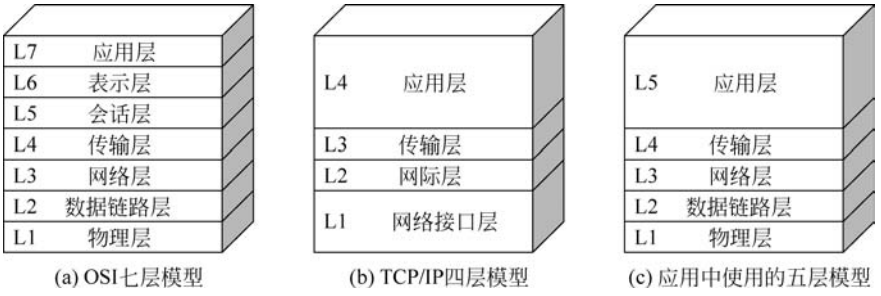


图 3-33 常见的计算机网络分层模型

2. 物理层

物理层负责将二进制的数据位(bit)流从一台计算机发送给另一台计算机。物理层不关心数据位流的具体含义，只关注如何将数据位流通过传输介质(铜缆、光纤或电磁波)从一个节点传输到另一个节点，是完全面向硬件的。物理层定义物理的或电气的特征，包括如何表示数据 0 和 1、网络连接器的接口类型、数据如何同步以及网卡何时发送或接收数据等。物理层的工作模式如图 3-34 所示。

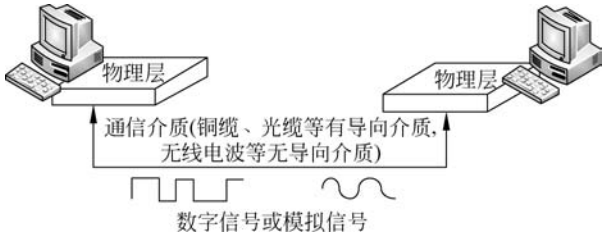


图 3-34 物理层工作模式

根据对所传输的数据流是否可实现控制的不同，计算机网络中的传输介质可以分为有导向和无导向2类。由有导向传输介质组成的系统称为有线传输系统，将使用无导向传输介质的系统称为无线传输系统。其中，有导向传输介质为信号的传输提供物理路径，信号沿着固定的方向传输，主要包括双绞线、同轴电缆和光纤。而无导向传输利用天线实现数据信号在空气、真空和水中的传播。除计算机网络外，无导向传输技术通常用于无线电广播、微波以及卫星通信系统。另外，红外线也在近距离的数据通信中被应用。

物理层的设备有中继器和集线器。中继器又称为转发器，其功能是简单地放大或刷新通过的数据流，以扩大数据的传输距离，主要用于连接同类型的网络和延伸同类型网络的距离。集线器(hub)是对网络进行集中管理的最小单元，像树的主干一样，它是各分枝的汇集点。hub是一个共享设备，其实质是一个中继器。集线器和中继器的区别仅在于集线器能够提供更多的端口服务，所以集线器是中继器的一种，是一种多端口的中继器。

3. 数据链路层

数据链路层负责在两个相邻节点之间建立一条可靠的数据传输通道。如图3-35所示，当两台计算机之间要实现通信时，需要在每台计算机上安装一块网卡(也称为“网络适配器”)，两块网卡之间通过一条“链路”(Link)连接，这条链路即一段物理线路。

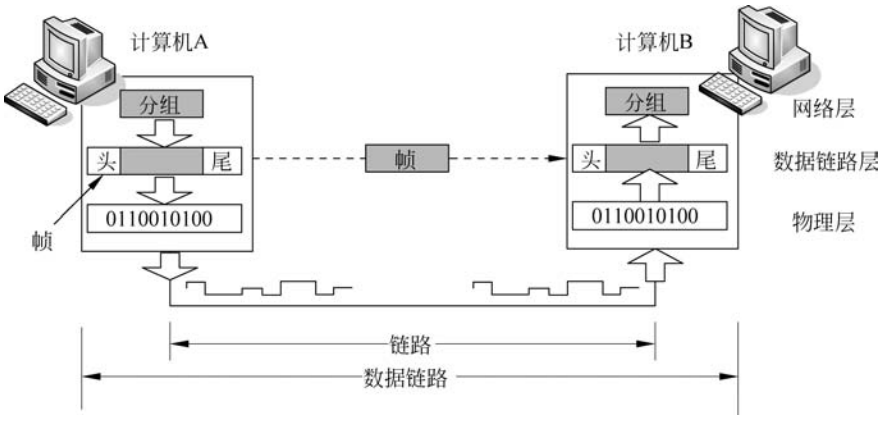


图3-35　两台计算机之间通过网卡联网后的通信过程

帧(frame)即数据帧，是数据链路层的数据单元，是添加了数据链路层的通信控制协议后构成的数据单元。假设计算机A与计算机B之间通过TCP/IP进行通信，而且数据从计算机A发送到计算机B。其中，计算机A的数据链路层在接收到网络层传下来的分组(IP数据报)后，在其前后分别加上头部和尾部，从而形成数据帧。所以，成帧(framing)就是在分组的前后分别加上代表数据链路层特征的头部和尾部的过程。帧到达物理层后，根据所使用的信道特性，将编码后的比特流发送到计算机B。计算机B在接收到比特流后，根据发送端成帧时所使用的规程(协议)以及隐含的定界信息，从连接的比特流中提取一个个帧。如果接收到的帧经检测后无差错，便去掉头部和尾部，将得到的分组交给网络层处理。

在电子数据取证工作中，针对数据链路层的主要取证对象便是“帧”。由于单位的局域网通常都是利用工作在数据链路层的交换机互联而成，交换机处理的数据对象便是帧。以太网中的帧结构如图3-36所示，说明该数据帧从哪里来(源地址)、到哪里去(目标地址)。

在通过任何一台交换机后，都可以看到该交换机上所连接的计算机（MAC 地址），所以在局域网中进行电子数据取证时，获得交换机的地址列表（图 3-37）是基础。

目标地址	源地址	控制信息	数据	校验

图 3-36　以太网的帧结构

```
图文中心机房RG-S8606#show mac
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- --------------------
   1        001a.a917.83a6       DYNAMIC  GigabitEthernet 1/4
   1        1414.4b1b.9de9       DYNAMIC  GigabitEthernet 1/3
   1        1414.4b1b.d9d0       DYNAMIC  GigabitEthernet 1/1
   1        1414.4b1b.d9d1       DYNAMIC  GigabitEthernet 1/1
   1        1414.4b1b.daba       DYNAMIC  GigabitEthernet 1/3
   1        1414.4b1b.dabb       DYNAMIC  GigabitEthernet 1/3
2004        001a.a917.83a7       DYNAMIC  GigabitEthernet 1/4
图文中心机房RG-S8606#
```

图 3-37　以太网交换机的 MAC 地址列表

4. 网络层

数据链路层研究和解决的是两个相邻节点之间的数据传输问题，其目的是实现两个相邻节点之间透明、无差错的以“帧”为单位的数据传输。而网络层的目的，则是实现两个端系统（如位于不同地区或国家的两台计算机）之间的数据透明传输。

以互联网中普遍使用的分组传输为例，当端系统（如一台计算机）要发送一个报文（原始文件）时，先将报文拆分成若干个带有序号和地址信息的分组，然后依次发给网络节点。此后，各个分组单独选择自己的路径，分别传输到目的节点。由于在分组传输中，各分组不能保证按顺序到达目的节点，有些分组甚至还可能在途中丢失，需要进行重传。当每个分组传输到目的节点后，将根据它的序号，恢复为原始报文。网络层分组的传输过程如图 3-38 所示。

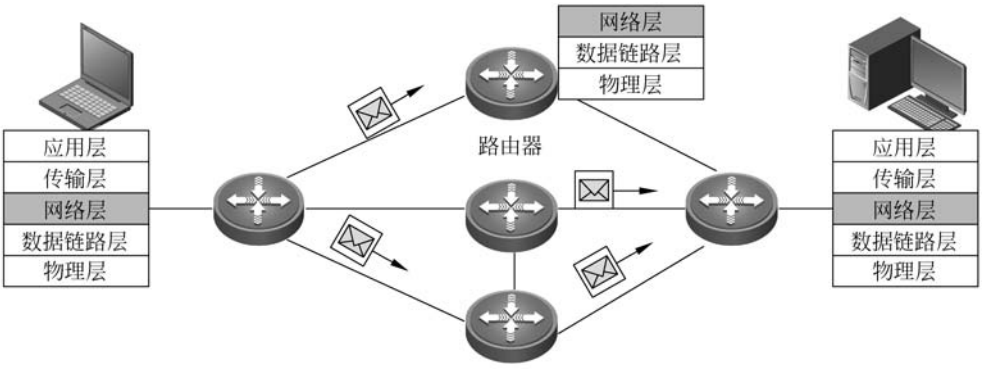


图 3-38　网络层分组传输过程

网络层最关键的设备是路由器。路由器的主要功能是在接收到一个分组（分组结构见图 3-39）时，首先从分组头部中提取“目的 IP 地址”，再在路由表中进行地址匹配，当匹配成功后通过对应的端口转发出去。以此类推，分组便会从源主机发送到目的主机。

在电子数据取证过程中，当涉及某个具体的通信时，就需要判断该分组从哪里来（源 IP 地址），并发往何处（目的 IP 地址）。目前，利用 Sniffer、Wireshark 等工具，都可以在抓取数据包后对其进行分析。图 3-40 所示的是 Wireshark 软件的操作界面，可以对指定的数据包

图 3-39　IP 分组的头部格式

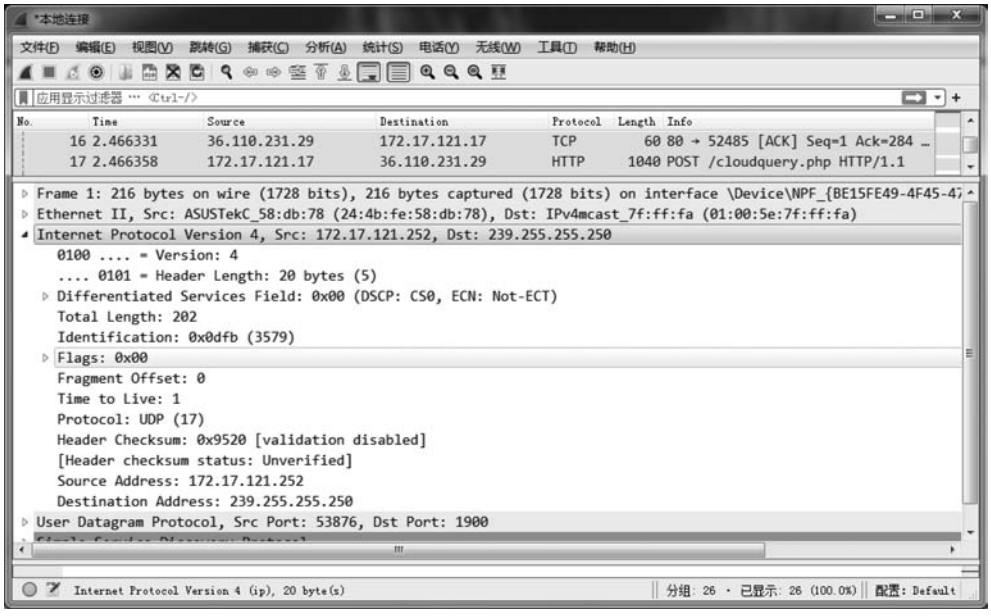


图 3-40　Wireshark 软件的操作界面

分别对物理层、数据链路层、网络层、传输层和应用层的数据结构进行分析。

网络地址转换(network address translator,NAT)是网络层一个非常重要的功能,也是电子数据取证工作中需要关注的热点技术。NAT 可以将多个内部地址映射成少数几个甚至一个合法的公网 IP 地址,让内部网络中使用私有 IP 地址的计算机通过“伪 IP”访问 Internet 资源,从而更好地解决 IPv4 地址空间枯竭问题。NAT 技术在高校、企业等网络中普遍使用。在这些单位中,一般情况下,内部主机使用私有 IP 地址,在网络出口处转换成公网 IP 地址,此转换过程依据 NAT 设备的映射表来完成。也就是说,只有 NAT 设备才能知道什么时候某一私有 IP 地址转换成某一公网 IP 地址后访问了公网上的某一资源。NAT 映射表如图 3-41 所示。

NAT 映射表作为 NAT 设备的日志来保存。《中华人民共和国网络安全法》规定:采取

```
Router-A>en
Router-A#show ip nat trans
Router-A#show ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
icmp 210.28.1.21:1     172.16.1.10:1      192.168.1.2:1      192.168.1.2:1
icmp 210.28.1.21:2     172.16.1.10:2      192.168.1.2:2      192.168.1.2:2
icmp 210.28.1.21:3     172.16.1.10:3      192.168.1.2:3      192.168.1.2:3
icmp 210.28.1.21:4     172.16.1.10:4      192.168.1.2:4      192.168.1.2:4
icmp 210.28.1.21:5     172.16.1.10:5      192.168.1.2:5      192.168.1.2:5
icmp 210.28.1.21:6     172.16.1.10:6      192.168.1.2:6      192.168.1.2:6
icmp 210.28.1.21:7     172.16.1.10:7      192.168.1.2:7      192.168.1.2:7
icmp 210.28.1.21:8     172.16.1.10:8      192.168.1.2:8      192.168.1.2:8
icmp 210.28.1.22:1     172.16.1.11:1      192.168.1.2:1      192.168.1.2:1
icmp 210.28.1.22:2     172.16.1.11:2      192.168.1.2:2      192.168.1.2:2
icmp 210.28.1.22:3     172.16.1.11:3      192.168.1.2:3      192.168.1.2:3
icmp 210.28.1.22:4     172.16.1.11:4      192.168.1.2:4      192.168.1.2:4

Router-A#
```

图 3-41　NAT 映射表示例

监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于 6 个月。做出此规定的主要原因是对于用户上网的 NAT 映射表、访问日志等重要信息要进行留存审计，需要时作为取证工作的重要信息依据。

5. 传输层

传输层是整个网络体系结构中的关键层，其任务是在源主机与目的主机之间提供可靠的、性价比合理的数据传输服务，并且与当前所使用的物理网络完全隔离。传输层位于端系统，而不是通信子网。传输层提供了数据缓存功能，当网络层服务质量较差时，传输层通过提高服务质量，以满足高层的要求。当网络层服务质量较好时，传输层只需要做很少的工作。另外，传输层还可实现复用和分用功能，通过复用和分用可在一个网络连接上创建多个逻辑连接。掌握传输层的内容，以下几个知识点非常重要。

1）传输层协议

在 TCP/IP 体系结构中，根据应用程序的不同要求，传输层主要提供了两个协议：传输控制协议(TCP)和用户数据报协议(UDP)。其中，TCP 是一个可靠的面向连接的协议，通过 TCP 传输的数据单元称为报文段(segment)；UDP 是不可靠的无连接的协议，通过 UDP 传输的数据称为数据报。TCP 报文段和 UDP 数据报的单元格式完全不同，TCP 要比 UDP 复杂得多，但两者都包含了“源端口”和“目的端口”。

2）进程

在计算机网络中，面向用户的是各类应用(如 FTP 下载、Web 页面浏览、电子邮件收发等)程序，而面向通信的是应用进程。所以，一台主机要与其他主机实现通信，就需要启用相应的进程，进程将具体的网络应用(应用层程序)与相应的通信过程结合了起来，掌握了进程就掌握了主机上正在运行着哪些网络应用程序。

3）端口

在传输层必须建立起进程名字与进程地址之间的映射关系，并且通过名字服务程序完成进程名字与进程地址之间的转换。进程地址即端口，不同的端口具有唯一的端口号(port number)。端口号是 TCP 和 UDP 与应用程序连接的服务访问点(SAP)，是 TCP 和 UDP 软件的一部分。TCP/IP 的设计者采用一种混合方式实现端口地址的管理。系统能够提供的端口号为 0～65535(2^{16})，目前端口号的分配情况可分为以下两种类型：

(1) 服务器端使用的端口号。又可分为 3 类：第 1 类是熟知端口号或公用端口号，这些

端口号的值小于255；第2类是公共应用端口号，是由特定系统应用程序注册的端口号，其值为255～1023。例如，FTP使用TCP21端口、DNS使用UDP53端口等。当在Internet中有新的应用程序出现时，需要向IANA进行注册，让Internet上的应用进程知道，以便成为熟知端口；第3类端口号称为登记端口号，当在Internet中使用一个未曾用过的应用程序时，就需要向IANA申请注册一个其他应用程序尚未使用的端口号，以便在Internet中能够使用该应用程序，这类端口号的值为1024～49151。

(2) 客户端使用的端口号。这类端口号仅在客户端进程运行时临时选择使用，所以也称为临时端口号，其值为49152～65535。在客户机/服务器(C/S)模式下，当服务器进程接收到客户端进程的报文时，就可以知道客户端进程所使用的端口号，因而可以把数据发送给客户端进程。当本次通信结束后，不管是服务器端还是客户端，刚才所使用过的客户端端口号已释放，这个端口号便可以提供给其他的客户端进程使用。

针对传输层的网络取证工作，主要是分析针对具体的通信过程所使用的传输层协议类型(UDP或TCP)、所使用的端口以及打开的通信进程，以此再进一步确定在主机上运行的应用程序。

6. 应用层

应用层是网络体系结构的最高层，在应用层之上不存在其他的层，所以应用层的任务只是为最终用户提供服务。每一种应用层协议都是为了解决某一类问题(如Web页面浏览、FTP文件下载、QQ即时通信等)，而每一类问题都对应一类应用程序，在应用层中运行的每一个应用程序称为一个应用进程。应用进程将应用层的功能与传输层联系了起来。

互联网应用的丰富性是由位于应用层的应用程序决定的。大量的功能各异的应用程序丰富了互联网的应用，如DNS提供了域名解析服务、HTTP/HTTPS提供了Web服务、Telnet提供了远程登录服务等。为了规范互联网应用，针对不同类型的服务分别制订了相应的协议，而对协议的具体实现方式可以是多样的。例如，所有Web浏览器都需要遵循HTTP/HTTPS协议，但在具体应用中用户可以选择使用不同的Web浏览器软件，如IE、Mozilla Firefox、Google Chrome、360极速浏览器、搜狗浏览器等。

针对应用层的取证工作相对复杂，需要综合多方面的知识做出最后的判断。例如，具体到某个网络应用时，需要同时确定通信进程、应用层协议、具体的应用程序名称等内容，还要考虑应用程序的启动方式(本地手工启动还是远程启动)、运行时间、访问方式(是谁在何时以什么方式进行了访问，进行了哪些操作)等信息，对于提供访问日志的应用程序(系统)，还要对日志文件进行详细分析。

3.5　数字媒体

数字媒体技术(digital media)指以二进制数的形式记录、处理、传播、获取的信息载体，这些载体包括数字化的文字、图形、图像、声音、视频影像和动画等可被人体感觉的媒体。数字媒体技术是以计算机技术和网络通信技术为主要通信手段，综合处理文字、声音、图形、图像等媒体信息，实现数字媒体的表示、记录、处理、存储、传输、显示、管理等各个环节，使抽象的信息变成可感知、可管理和可交互的一种技术。

3.5.1 文本

传统的手工书写虽然利于信息的记载，但却影响了信息的传输范围；印刷术的出现方便了信息的大范围传播，但却无法实现信息的快速编辑和修改；计算机技术在文字处理中的应用，实现了信息的记载、修改、编辑和传输等方面质的飞跃。

1. 文本和文本文件

文本(text)是文字信息在计算机中的表示，它由一系列字符组成。计算机中存储文本的文件称为文本文件，它是一种典型的顺序文件，文本文件中除了存储文件有效字符信息(包括用 ASCII 码字符表示的回车、换行等信息)外，不能存储其他任何信息。文本文件指一种容器，而文本指一种内容。根据文本排版格式的不同，文本文件可以分为简单文本文件和丰富格式文本文件两类。

1) 简单文本文件

简单文本文件又称为纯文本文件，指文件内容由一连串字符或汉字编码组成，且不包含其他格式信息和结构信息的文件，文件扩展名.txt。简单文本文件没有格式约束，一般的文字处理软件都可以识别和处理。

2) 丰富格式文本文件

丰富格式文本文件是在简单文本文件的基础上，在内容编辑时增加了一些控制格式和结构说明信息，以丰富内容的展现形式。例如，可以对文本设置字体、字号、颜色等控制信息，也可以插入图片、视频、声音等媒体信息。不同软件生成的丰富格式文本文件之间通常是不兼容的，这些文件的扩展名常见的有.doc、.docx、.pdf、.wps 等。

传统的文本组织结构是线性的，阅读者一般需要按照文本事先的顺序进行逐行阅读。而丰富格式文本可以打破这种限制，实现内容之间的跳转。例如，使用 HTML 排版的超文本文件(.html 网页文件)，通过在文本中设置超链接可以实现同一个文本内容之间的跳转以及不同文件之间的链接。

2. 文本处理

文本处理指利用外部输入设备将信息输入到计算机，并对文本进行处理(如添加、删除、修改、设置字体与字号、设置段落格式等)，然后以某种方式(如显示、打印等)呈现给用户的过程。

1) 文本输入

从外部设备向计算机内部输入字符的方法主要有人工输入和计算机自动识别输入两种方式，如图 3-42 所示。其中，人工输入可以通过键盘、手写输入或语言输入等设备输入信息；而自动识别输入则是将介质(如纸张)上的文字符号通过光电扫描技术进行文本转换变成字符的编码，或使用其他设备自动输入信息。

2) 文本编辑

根据应用需求，通常需要利用文本编辑器(文本编辑软件)对文本进行排版处理。不同文本编辑器可实现对文本内容的不同处理效果。常见的文本编辑器有 Linux/UNIX 操作系统中的 vi 编辑器、Windows 操作系统中的“记事本”、macOS 中的 TextEdit 等。通常情

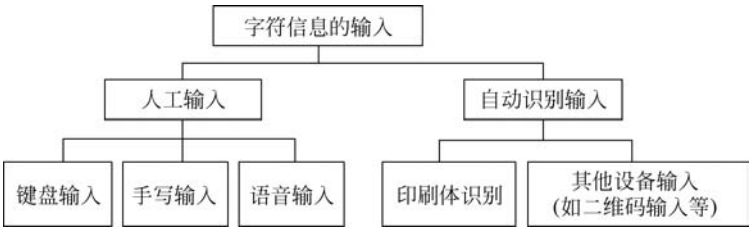


图 3-42　字符输入方式

况下，用户多使用微软公司的 Word 或金山公司的 WPS 等专业字处理软件进行文本的编辑工作。

3.5.2　图形与图像

随着信息技术的快速发展，多媒体技术的应用日新月异，信息的呈现形式日趋丰富。图形和图像属于多媒体中的基本信息类型，因其直观、形象而得到用户的普遍青睐。

1. 图形与图像的概念

图形(graph)和图像(image)都是多媒体系统中的可视元素，两者之间存在较大的差异。

1) 图形

图形是矢量图(vector drawn)，它是根据几何特性来绘制的。组成图形的元素主要有点、直线、弧线等。矢量图常用于框架结构的图形处理，应用非常广泛，如计算机辅助设计(CAD)系统中常用矢量图来描述较为复杂的几何图形，适用于直线以及其他可以用角度、坐标和距离来表示的图，如图 3-43(a)所示。图形只保存生成图形的算法和图上的某些特征点信息，在计算机还原时，相邻的特征点之间用特定的很多段小直线连接形成曲线，也可通过着色算法来填充图形的指定区域的颜色，所以图形文件占用存储空间较小，图形任意放大或者缩小后，其清晰度不会受到影响。但是，由于每次屏幕显示图形时都需要重新计算，所以图形的显示速度较慢。图形是人们根据客观事物制作生成的，它不是客观存在的。

2) 图像

如图 3-43(b)所示，图像是位图(bitmap)，它所包含的信息是用像素来度量的。就像细胞是组成人体的最小单元一样，像素是组成一幅图像的最小单元。分辨率和像素是描述图像的主要参数，分辨率越高、像素越大，图像文件占用存储空间就越大，图像也就越清晰。图像可以直接通过拍照、扫描、摄像等方式得到，也可以通过绘制得到。

2. 图形处理

从处理技术来看，图形主要分为由线条组成的图形(如工程图、等高线地图、曲面图、曲框图等)和类似于照片的真实感图形[图 3-43(a)]两类。计算机通过相应的算法，根据被描述的物体的特征(如点、线、面、体之间的关系等)、形态、大小、表面材料等，构建相应的模型，计算机根据模型生成相应的图形。这一过程实际上是图形的绘制，生成的图形都是矢量图。

图形绘制过程中，每一像素的颜色及其亮度都要经过大量的计算才能得到，因此绘制过程的计算量较大，对计算机性能的要求较高，特别是三维图形和动画。计算机绘制的图形是

(a) (b)

图 3-43 图形和图像

矢量图形，相应的绘制软件通常有 3D MAX、CorelDraw、Adobe Illustrator、Auto CAD 等。

计算机图形的应用主要包括：计算机辅助设计与制造(CAD/CAM)；利用计算机生成地图、交通图、气象图、海洋图等；通过计算机模拟军事训练，公安机关对案件现场进行重构等；计算机动画等。

3. 图像处理

图像操作包括图像采集、存储、处理、传输、输出等工作过程。其中，图像采集指从现实世界获得数字图像的过程，所使用的设备主要有扫描仪和数字照相机。

1) 图像的基本属性

分辨率、像素深度和颜色空间是图像的三个基本属性。其中，分辨率在前文已经进行了介绍。

(1) 像素深度。像素深度指每个像素的颜色分量的二进制位数之和，它决定了构成图像的每个像素的颜色数(彩色)或灰度级数(黑白)。例如，某个彩色图像的像素用 R、G、B 共 3 个分量表示，且每个分量用 8 位表示，那么每个像素共用 $3\times8=24$ 位表示，即像素的深度为 24，每个像素可表示 2^{24} 种颜色。像素深度值越大，每个像素能够反映的颜色越丰富，图像的显示效果越细腻。

(2) 颜色空间。颜色空间也称为颜色模型，是对彩色图像所使用的颜色描述方法。颜色空间的种类较多，常用有 RGB、CMY、HSV、HSI 等。

RGB 分别表示 R(red、红)、G(green、绿)和 B(blue、蓝)，它是依据人眼识别的颜色定义出的空间，可表示大部分颜色。RGB 是图像处理中最基本、最常用和面向硬件的颜色空间种类，人们采集到的彩色图像一般被分为 R、G、B 的成分加以保存。

CMY 分别表示 C(cyan，青)、M(magenta，品红)和 Y(yellow，黄)，它是工业印刷采用的颜色空间，它与 RGB 对应。RGB 来源于是物体发光，而 CMY 是依据反射光得到的。例如，彩色打印机中采用的四色墨盒，即由 CMY 加黑色构成。

HSV 分别表示 H(hue，色调)、S(saturation，饱和度)和 V(value，亮度)，是根据颜色的直观特性建立的一种颜色空间，对用户来说是一种直观的颜色模型。其中，H(色调)用角度度量，取值范围为 0°～360°，从红色开始按逆时针方向计算，R 为 0°，G 为 120°，B 为 240°，之间的补色分别是：Y 为 60°，C 为 180°，M 为 300°；S(饱和度)表示颜色接近光谱色的程度。一种颜色，可以看成是某种光谱色与白色混合的结果。其中光谱色所占的比例越大，颜色接

近光谱色的程度就越高，颜色的饱和度也就越高。饱和度高，颜色则深而艳。S的取值范围为0～100%，值越大，颜色越饱和；V(亮度)表示颜色明亮的程度，对于光源色，明度值与发光体的光亮度有关。V的取值范围为0(黑)到100%(白)。由于HSV是一种比较直观的颜色模型，所以在许多图像编辑工具中应用比较广泛，如Adobe Photoshop。

常见的图像文件有.bmp、.gif、.jpeg、.jpg或.png等，普通用户最常使用的图像处理软件有Adobe Photoshop、Adobe Illustrator、CorelDRAW等。目前，数字图像的应用非常广泛，主要包含图像通信、遥感、工业生产、机器人视觉、医疗诊断、军事、公安以及档案管理等。

2) 图像压缩技术

为了便于图像的存储和网络传输，在满足一定保真度的前提下，通常需要对图像数据进行变换、编码和压缩，去除多余数据，减少数字图像的数据量。

(1) 图像压缩的原因。图像数据之所以能被压缩，就是因为数据中存在着冗余。图像数据的冗余主要表现为：图像中相邻像素间的相关性引起的空间冗余；图像序列中不同帧之间存在相关性引起的时间冗余；不同彩色平面或频谱带的相关性引起的频谱冗余。数据压缩的目的就是通过去除这些数据冗余来减少表示数据所需的比特数。

(2) 图像压缩的分类。图像压缩可以分为有损数据压缩和无损数据压缩两类。其中，无损数据压缩是可逆的，从压缩后的数据可以完全恢复原来的图像，信息没有损失；有损数据压缩是不可逆的，从压缩后的数据无法完全恢复原来的图像，信息有一定损失。对于绘制的技术图、图表或者漫画优先使用无损压缩，这是因为有损压缩方法，尤其是在低的位速(bit-rate)或者压缩比条件下将会带来压缩失真。如医疗图像或者用于存档的扫描图像等这些有价值的内容的压缩也尽量选择无损压缩方法。有损方法非常适合于自然的图像，例如一些应用中图像的微小损失是可以接受的(有时是无法感知的)，这样就可以大幅减小位速或提高压缩比。

(3) 典型压缩算法。目前常用的压缩算法主要有JPEG(joint photographic experts group，联合图像专家组)，它是用于连续色调静态图像压缩的一种标准，也是目前网络上最流行的图像格式，文件后缀名为.jpg或.jpeg。JPEG采用有损数据压缩方式，在采取高压缩比的情况下仍然能够获得丰富生动的图像。JPEG提供了多种压缩级别，压缩比率通常为10∶1～40∶1，压缩比越大，压缩后的图像品质越差。例如，可以将一个1.37MB的BMP位图文件压缩到20.3KB。JPEG2000格式作为JPEG的升级版本，在提高了压缩比(约30%)的同时，可支持有损数据压缩和无损数据压缩。渐近传输是JPEG2000格式具有的一个非常重要的特征，它可先传输图像的轮廓，然后逐步传输数据，不断提高图像质量，让图像显示时逐渐由朦胧变得清晰。渐近传输非常适合于图像的互联网传输。

3.5.3　数字音频

声音是人与人之间进行交流的重要媒体形式，也是人类了解和认识大自然的有效途径。声音包含语音、音乐、大自然声音等类型。利用计算机技术，可以对声音进行采集、模拟、编码、重构、编辑等处理。

1. 音频

如图3-44所示，声音是一种振荡波，是随时间连续变化的量。振幅和频率是声音的重

要指标，其中振幅指波形的高低幅度，表示声音的强弱；频率表示声音每秒钟的振动次数，以 Hz 为单位。

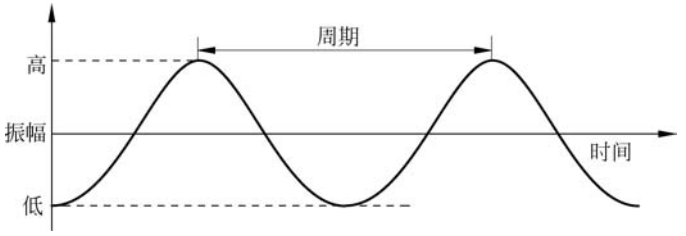


图 3-44　声音的波形表示

自然界存在各种声音，按声音的频率范围可以分为次声、可听声、超声和特超声。人类的听觉范围为 20Hz～20kHz，其中电话话音、调幅广播、调频广播、音响等均为可听声，而次声、超声和特超声对人类是不可听见的。不同声音种类的频率范围如表 3-1 所示。

表 3-1　不同声音种类的频率范围

声音种类	频率范围	声音种类	频率范围
次声	0～20Hz	调频广播	20Hz～15kHz
音响	20Hz～20kHz	超声	20kHz～1GHz
电话语音	300Hz～3400Hz	特超声	1GHz～10THz
调幅广播	50Hz～7kHz		

声音有两种最基本的表示形式：模拟音频和数字音频。自然界中的声音是连续变化的，它是一种模拟量，而计算机中存储和处理的数字音频是由 0 和 1 表示的离散值。所以，将自然界中的声音要转变为计算机能够识别的数字音频时需要进行模/数转换，相应的将计算机中存储的数字音频要通过耳机、音响等设备播放时则需要进行数/模转换。计算机中的声卡就承担着声音处理和转换的功能，如图 3-45 所示。声卡的主要功能包括：模/数转换和数/模转换、声音的合成和控制、音频文件的压缩和解压缩等，同时为外接设备（如耳机、音响等）提供相应的接口。

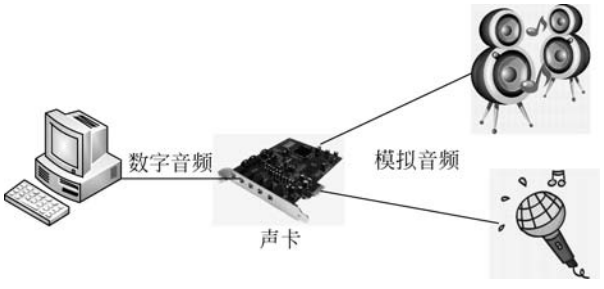


图 3-45　利用声卡实现数字音频与模拟音频之间的转换

2. 音频数据的处理

数字化的声音数据就是音频数据。本节主要介绍音频数据的压缩方法，以及针对音频数据的计算机合成方法。

1）音频数据的压缩

音频数据是一种用进制表示的、按时间先后顺序组织的串行比特流。通常情况下，直接采样得到的音频数据量较大，不利于存储和网络共享。为了降低存储成本并提高通信效率，需要对音频数据进行压缩处理。

声音信息中包含大量的冗余信息，还包含人的听觉无法直接感知的信息。所以，可以对音频数据进行压缩处理，根据压缩编码方式的不同分为无损数据压缩和有损数据压缩两大类。其中，有损与无损指经过压缩编码后，新文件所保留的声音信号相对于原来的数字音频信号是否存在削减。有损数据压缩是去除了一些人耳难以分辨的声音，虽然音质可能变差，但数据量小了很多。

常见的数字音频未压缩编码格式有 CD 格式和 WAV 格式，有损数据压缩格式有 MP3 格式和 WMA 格式，无损数据压缩格式有 FLAC 编辑格式和 APE 编码格式。

2）声音的计算机合成

利用计算机合成声音包括计算机语音合成和计算机音乐合成两种。

（1）计算机语音合成。随着人工智能和计算机技术的发展，人们期待着以语音方式进行人机交流。语音合成的目的是让计算机说话。语音合成系统又称为文语转换（text to speech，TTS）系统，即从文字到语音的转换系统。语音合成技术追求的目标是合成出的语音可懂、清晰、自然，具有表现力。语音合成是一门跨学科的前沿技术，涉及的研究领域有自然语言理解、语言学、语音学、信号处理、心理学、声学等。只有将上述领域的研究成果结合在一起，语音合成才能实现追求的目标。近年来，TTS 系统取得了长足发展。该技术在通信、人机交互、互联网等领域都有着广阔的应用前景。目前，合成语音的质量日益提高，已经可以合成出具有较高清晰度和可懂度的语音。

（2）计算机音乐合成。通常情况下，人们对音乐的理解是音乐家根据简谱或五线谱编写出乐谱，演奏人员再根据乐谱演奏出音乐。计算机中使用的 MIDI（musical instrument digital interface，乐器数字接口）类似于五线谱，可称为“计算机能理解的乐谱”。MIDI 是一种音乐标准格式，它用二进制数形式表示出音符、定时、速度、音色等各种音乐元素，也规定了演奏控制器、音源、计算机等相互连接时的通信规程。MIDI 是一种计算机和数字乐器使用的音乐语言，用 MIDI 编写的乐谱以. mid 或. midi 为扩展名存储在计算机中。计算机中使用的媒体播放器软件（如 Media Player、QQ 音乐、XMPlay 等）从磁盘中读取某个 MIDI 文件，识别文件中的内容后，可以逐条向声卡中的音乐合成器发出 MIDI 指令，音乐合成器根据 MIDI 指令对各种音乐元素的描述，合成供人们欣赏的音乐。

计算机音乐合成技术彻底改变了传统的音乐制作和演奏方式。记录音乐的方式由原来的乐谱变成了 MIDI 文件，音乐作品也可以任意编辑和修改，强大的计算机处理功能不仅提高了音乐表现的精确性，而且使音乐制作大众化。在此情况下，针对原始声音的篡改变得相对容易和普遍，成为电子数据取证研究的一个方向。

3.5.4　数字视频

相对于模拟视频来说，数字视频是以二进制数字形式记录的视频。数字视频存在着不同的生成、存储和播出方式。

1. 视频

人类具有“视觉暂留”特性，即人的眼睛看到一幅画面或一个物体后，视觉形象在1/24s内不会消失。利用这一原理，在一幅画面还没有消失之前紧接着播放另一幅画面，就会给人造成一种流畅的视觉变化效果。电影采用了24帧(幅)/s画面的速度拍摄和播放，电视采用25帧/s(PAL制式)或30帧/s(NSTC制式)画面的速度拍摄和播放。如果以每秒低于24帧画面的速度拍摄或播放，就会产生停顿感。

视频(video)是多幅静止图像与连续的音频信息在时间轴上同步运行的混合媒体。多帧图像随时间变化而产生运动感，因此视频也称为运动图像。视频处理泛指一系列静态图像以电信号的方式加以捕捉、记录、存储、处理、传送与重现的各种技术。常见的视频有电视(电影)和计算机动画。其中，电视(电影)是用影像技术对真实场景中图像和声音的记录与播放，计算机动画是计算机制作的图像序列，是一种计算机合成的视频。

按照视频的存储与处理方式可以分为模拟视频和数字视频两类。其中，早期视频的获取、存储和传输都是采用模拟方式，而数字视频是以0和1形式记录的视频。不同于模拟视频，数字视频在复制和传输时不会引起信号质量的下降，而且方便视频中图像信息的编辑处理，传输过程中抗干扰能力强，也易于实现加密传输。目前，有线电视系统中使用的都是数字视频，可以直接用数字电视机收看节目。如果要使用早期的模拟电视机收看数字视频，则需要配置一台负责将数字信号转换成模拟信号的转换器(机顶盒)。

2. 数字视频处理

数字视频既可以直接通过数字设备(如数码摄像机)直接获得，也可以通过模拟视频设备(如录像机)获得模拟信号后再由视频采集卡将其转换为数字视频文件。通常情况下，可以对数字视频文件进行压缩处理和编辑操作。

1) 数字视频文件的压缩

数字视频文件占用的空间较大，对磁盘存储和网络传输提出了挑战。例如，一个常见的1024×768分辨率、24位/像素的彩色图像的数据量为1024×768×24÷8÷1024÷1024=2.25MB，如果以25帧/s的帧率显示运动图像，1s就需要2.25×25=56.25MB数据量。为此，针对数字视频文件的压缩和编码成为计算机存储和处理的前提。

视频数据中含有大量的冗余信息，压缩算法就是去除数据中的冗余信息，以降低信息数据量。例如，相邻帧之间的数据大部分信息是相同的，压缩时检查每一帧数据，仅保存从一帧到另一帧变化的部分；同一帧画面中某一区域可能包含颜色相同的像素，压缩算法可以将这一区域的颜色信息作为一个整体对待，而不是分别存储每一像素的颜色信息；利用人类视觉的不敏感性，也可以提升压缩比等。所以，压缩技术包含帧内图像数据压缩技术、帧间图像数据压缩技术和熵编码压缩技术。

压缩编码方式可分为有损数据压缩和无损数据压缩。其中，在无损数据压缩中，压缩后重构的图像在像素级等同于压缩前的图像，压缩前后的显示效果没有区别；在有损数据压缩中，虽然提高了压缩比，但压缩后重构的图像质量要比压缩前差。

国际电信联盟(ITU-T)和国际标准化组织(ISO)是国际上制订视频编解码技术标准的两个组织。其中，ITU-T制订的视频编解码技术标准主要有H.261、H.263、H.264等，例如采用H.264标准可以在获得高压缩比的同时还拥有高质量的图像，在网络传输过程中对

带宽的要求相对较低；ISO 制订的视频编解码技术标准主要有 MPEG-1、MPEG-2、MPEG-4 等，MPEG(moving pictures experts group，动态图像专家组)是 ISO 与 IEC(international electrotechnical commission，国际电工委员会)于 1988 年成立的专门针对运动图像和语音压缩制订国际标准的组织，先后研发制订了多个标准，以适应不同带宽和数字影像质量的要求。目前，MPEG-1 标准广泛应用于 VCD、数码相机、数字摄像机等，MPEG-2 标准用于数字卫星电视、数字有线电视和 DVD 等，MPEG-3 标准最初为高清晰度电视(HDTV)研发，后来被 MPEG-2 取代，MPEG-4 技术可利用较窄的带宽获得较佳的图像传输质量，主要用于视频电话、监控和智能手机等领域。

为了适应视频存储的需要，设定了不同的视频文件格式，把视频和音频集成在一个文件中，以方便同时回放。目前，常用的视频文件格式有微软视频(.avi、.wmv、.asf)、Real Player(.rm、.rmvb)、MPEG 视频(.mpg、.mpeg、.mpe)、手机视频(.3gp)、Apple 视频(.mov)、Sony 视频(.mp4、.m4v)、Adobe 视频(.flv、.f4v)以及其他视频(如.dat、.mkv、.vob 等)，其中在网络流媒体播放中广泛使用的视频格式有.asf、.wmv、.mov、.rm、.rmvb、.flv、.f4v 等。由于不同播放器支持不同的视频文件格式，所以一些视频播放软件本身仅支持指定的视频文件格式，如果要播放其他格式的视频文件，就需要通过格式转换软件进行视频格式转换，或安装相应的插件(解码器)。

2) 数字视频的编辑

数字视频的编辑就是在计算机上利用各种编辑软件来编辑视频，如视频剪接、添加字幕、转场特效、多轨合成甚至 3D 动画等。例如，Windows 操作系统自带的数字视频编辑软件 Windows Movie Maker 提供了在计算机上快速制作视频的功能，另外 Adobe 公司的 Premiere Pro 软件提供了专业的视频编辑功能。由于视频文件的可编辑性，为视频文件的证据确定提出了更高要求，掌握以下视频文件的主要编辑步骤，可以为针对视频文件的取证提供帮助。

(1) 将录制或硬盘中保存的视频、音频或静止图上图片导入计算机。

(2) 使用视频编辑软件创建场景、重新排列场景并删除不需要的部分。

(3) 完成对视频或音频的编辑，包括对素材的剪辑，添加字幕、音乐、图片、片头、过渡或特技效果等。

(4) 预览编辑后的视频，将最后形成的视频以文件形式进行保存。

(5) 使用媒体播放器播放视频。

3. 动画

动画是通过把人物的表情、动作、变化等分解后绘制成许多动作瞬间的画幅，再用摄像机连续拍摄成一系列画面，给视觉造成连续变化的图画。它的基本原理与电影、电视一样，都是视觉暂留原理。不同于一般的影视，动画的一个重要特征是利用设计者的想象和虚幻创造出来的，不是原本存在的。所以，动画是靠人的想象力绘制出来的画面。

计算机动画指采用图形和图像的数字处理技术，借助于程序或动画制作软件生成一系列的景物画面，是用计算机技术辅助制作的动画。根据空间角度的不同，计算机动画可分为二维动画和三维动画；根据动画形成方式的不同，计算机动画分为帧动画和矢量动画。其中，帧动画是以帧为基本单位的传统动画，如以传统平面绘图为基础的动画、颜色流动效果的动画、主体变形效果的动画等；矢量动画是计算机中使用数学方式来描述屏幕上的曲线，

利用图形的抽象运动特征来记录变化的画面信息的动画。由于矢量动画占用存储空间较小，所以适合在网络中使用。另外，矢量动画可以实现窗口大小的自适应，而且不降低画面质量。

常用的动画制作软件有 Animator Pro、Animation Studio、Flash MX、GIF Construction Set Pro、3D Studio Max、Cool 3D、Maya 等，不同软件在功能和制作效果上存在一定的差异。计算机动画都是以文件形式保存在计算机中，动画文件占用空间较大，可以通过压缩技术进行处理。动画文件的种类与格式主要包括 FLC、GIF、SWF 等。计算机动画的应用范围较为广泛，目前已应用到产品演示、教学课件、广告、影视作品等领域。

3.6 数据库

数据库和信息系统的出现是计算机技术和网络应用发展的必然结果。其中，计算机信息系统是现代信息应用与管理的基础，而数据库技术是计算机信息系统的核心。本节主要结合电子数据取证工作需要，介绍数据库技术的概念、原理和应用特点。

3.6.1 数据库基础

数据库是按照数据结构来组织、存储和管理数据的仓库，是一个长期存储在计算机内的、有组织的、可共享、可统一管理的大量数据的集合。数据库的主要功能是实现数据管理，数据管理是应数据处理的客观要求出现和发展的。数据处理具体指数据的分类、组织、编码、存储、查询、统计、传输等操作，目的是向用户提供有价值的信息。

需要说明的是，由于数据与信息之间的关联性，在一般情况下经常将数据处理也称为信息处理；数据处理中的数据可以是数值型数据，也可以是字符、文字、图表、图形、图像、声音等非数值型数据。

1. 数据处理的 3 个阶段

数据处理是随着数据类型和计算机技术的发展而不断发展和完善的。目前，随着大数据技术的发展，数据处理技术和方式也都发生着变化。本小节以数据管理为对象，将数据处理简要分为 3 个不同阶段。

1）人工管理阶段

在计算机应用于数据管理的初期，数据处理主要依靠人工进行，程序员不仅要规定数据的逻辑结构，还要考虑数据的存储位置和读取方式等问题。在该阶段，最突出的特点是数据依附于应用程序，数据独立性差，数据无法实现共享。

2）文件管理阶段

为了克服人工管理存在的不足，在 20 世纪 50 年代后期出现了数据以独立于应用程序之外的文件管理模式，即数据以文件形式存储，应用程序通过操作系统对数据文件进行打开、读写、关闭等操作。文件管理模式解决了应用程序与数据之间的过度依存问题，在一定程度上实现了数据共享。图 3-46 是应用程序和数据文件之间的关系，可以看出，一个应用程序可以访问多个数据文件，一个数据文件也可被多个应用程序使用。

文件管理阶段有力推动了计算机在数据处理领域中的应用，但该模式仍然存在着数据

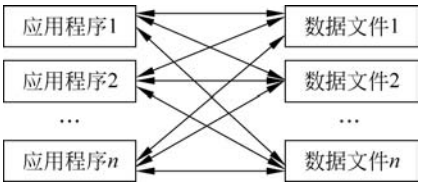


图 3-46　文件管理模式中应用程序与数据文件之间的关系

独立性差、数据冗余度大、数据处理效率低、数据的安全性与完整性无法得到有效控制等不足。

3）数据库管理阶段

为了克服文件系统存在的弊端，适应迅速发展的大量复杂数据处理的需要，20 世纪 60 年代后期出现了以数据统一管理和数据共享为特征的数据库管理系统（database management system，DBMS），IDS（integrated data stor，集成数据存储）是美国通用电气公司于 1963 年研制出的世界上最早的数据库管理系统。如图 3-47 所示，DBMS 接手了不同应用程序对数据库的直接访问，应用程序在访问数据库时都需要通过 DBMS 的管理。

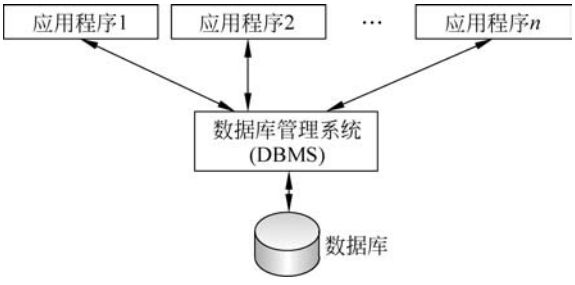


图 3-47　数据库系统工作原理示意图

2. 数据库系统

数据库系统（database system，DBS）是由数据库、数据库管理系统（DBMS）、应用程序、数据库管理系统赖以执行的计算机软硬件环境及数据库维护使用人员的总称。

1）数据库

数据库（data base，DB）是存放数据的仓库。在数据库中不仅保存了用户直接使用的数据，而且保存了定义这些数据的数据类型、模式结构等数据（元数据）。数据库是一个按数据结构来存储和管理数据的计算机软件系统。数据库的概念具体包括两层含义：数据库是一个实体，它是能够合理保管数据的“仓库”，用户在该“仓库”中存放要管理的事务数据；数据库是数据管理的新方法和技术，它能实现更合适的组织数据、更方便的维护数据、更严密的控制数据和更有效的利用数据。

2）数据库管理系统

数据库管理系统是为管理数据库设计的专门软件（如 Oracle、SQL Server、MS Access 等），主要由以下几部分组成（图 3-48），其中模式更新、数据查询和数据更新是数据库管理系统接口接收的 3 种输入类型。

（1）模式更新。模式更新涉及对数据模式的修改。数据模式的修改指对数据的逻辑结

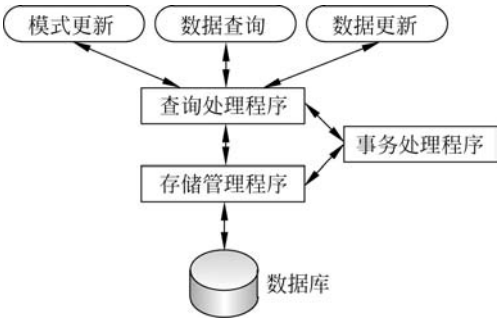


图 3-48 数据库管理系统组成示意图

构的修改，可以增加新的数据对象或对已存在数据对象结构进行修改。例如，在一个学生学籍管理数据中增加获奖信息，或对某个已有数据的结构或属性进行修改等。模式更新一般只能由数据库管理员进行操作。

(2) 数据查询。数据查询指对数据库进行查询和统计，一般有两种方式：一种是通过联机终端直接进行交互式查询；另一种是通过应用程序访问数据库中的数据。

(3) 数据更新。数据更新指对数据进行插入、修改或删除操作。像数据查询一样，数据更新同样存在交互式和程序两种方式。

(4) 查询处理程序。查询处理程序在接收到一个由较高级语言所表示的数据库操作指令后，对该指令进行解释、分析和优化，然后提交给存储管理程序来执行。

(5) 存储管理程序。根据查询处理程序的请求，存储管理程序可以更新数据库中的数据，也可以在获取数据库中的数据后将其反馈给查询处理程序。

(6) 事务处理程序。事务处理程序控制着查询处理程序和存储管理程序的执行。这里的“事务”指一组按顺序执行的操作单位，这组操作要么全部执行，要么一条也不执行，以此来保证数据库数据的一致性。事务处理类似于在 ATM 上取款，在取款的同时要对用户账户进行记账，只拿钱而不记账，或只记账而拿不到钱都是不允许的，在这一过程中取款和记账便形成了一个具体的事务。

3) 应用程序

应用程序通常指为完成用户业务功能而用高级语言(如 VB、Delphi、C＃等)编写的程序，应用程序通过数据库提供的接口对数据库中的数据进行插入、删除、修改、查询、统计等操作。

4) 计算机软硬件环境

计算机软硬件环境指数据库系统、应用程序赖以执行的环境，主要包括计算机硬件设备、网络环境、操作系统及应用系统开发工具等。

5) 相关人员

相关人员指在数据库系统的设计、开发、维护和使用过程中所有涉及的人员，主要有数据库管理员(dataBase administrator，DBA)、系统分析设计人员、系统程序员以及用户等，其中数据库管理员在大型数据库应用中主要负责对数据库进行有效的管理和控制，解决系统设计和运行中出现的各种问题。

数据库、数据库管理系统、数据库系统是不同的概念，在使用中应加以有效区分。数据

库系统所具有的数据结构化、数据冗余小、数据共享、数据独立性强、数据统一管理与管制等功能，提供了强有力的数据管理功能。

3. 数据库系统的结构

在电子数据取证工作中，在许多场景下都离不开数据库系统，而不同的数据库系统结构对数据的管理不尽相同。为此，熟悉数据库系统的体系结构，掌握不同结构中数据管理的特点，对电子数据取证起着十分重要的作用。

1）集中式数据库系统

早期的 DBMS 以分时操作系统为运行环境，采用的是集中式数据库管理方式，用户通过终端访问数据库系统。在这种模式中，数据集中存储在主机上，数据实现集中管理。

2）客户机/服务器结构

随着互联网技术的发展，数据库系统体系结构也开始从早期的集中式逐渐过渡到客户机/服务器(client/server，C/S)结构模式。C/S 结构如图 3-49 所示，其中客户机指运行专门应用程序的用户计算机，它直接面向用户，接收并处理用户发出的任务，并将其中涉及对数据库的操作交由服务器去执行；而服务器响应客户机的请求，完成对数据库的操作(如更新、查询等)，并将结果反馈给客户端。从数据管理角度，C/S 结构仍然属于集中式管理，只是用户是分布的。

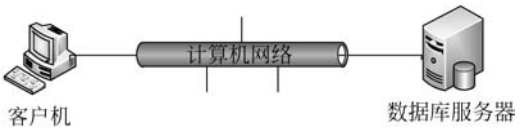


图 3-49　C/S 结构示意图

3）浏览器/服务器结构

浏览器/服务器(browser/server，B/S)结构是随着 Internet 的发展而出现和快速发展起来的一种互联网数据管理模式，它由 Web 浏览器、Web 服务器和数据库服务器 3 部分组成，如图 3-50 所示。其中，Web 浏览器扮演着 C/S 结构中客户端程序的角色，只是在 C/S 结构中不同的应用系统分别使用不同的客户端程序，而在 B/S 结构中所有的应用系统都使用通用的 Web 浏览器以网页形式对数据库中的数据进行操作；Web 服务器上运行应用系统，方便了应用系统的部署和日常维护；数据库服务器专门用于存放系统中所使用的数据库。B/S 结构中的数据仍然是集中管理。

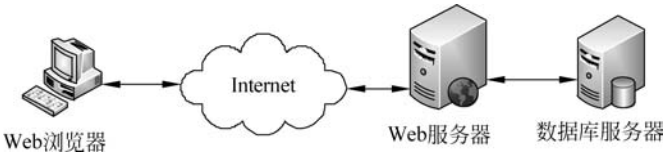


图 3-50　B/S 结构示意图

4）分布式数据库

数据丰富了互联网应用，然而在互联网应用快速发展过程中，数据的集中式管理为数据的高效访问提出了挑战。分布式数据库技术将数据按一定的策略(如来源、用途等)分散保存在不同地理位置的多台计算机节点上，供不同的用户访问。数据在物理上分布，由系统统

一管理。

数据库技术的快速发展为用户带来了不同的应用体验。近年来，并行数据库系统、工程数据库系统、空间数据库系统、多媒体数据库系统、模糊数据库系统、主动数据库系统等针对特定应用领域开发的数据库系统在互联网环境中得到广泛应用，对数据库的研究和学习提出了更高要求。

3.6.2 数据仓库与数据挖掘

近年来，社会各个行业对数据处理提出了更高要求，数据库技术开始广泛应用于决策领域，引出了数据仓库、数据挖掘等概念。

1. 数据仓库

计算机的数据处理方式可分为操作型处理和分析型处理两种类型，前者属于事务型，后者属于决策型。其中，操作型事务处理常见于企业的管理信息系统（management information system，MIS），用于企业各部门日常工作管理，如产品入库登记、生产资料管理等，反映的是企业当前的运行状态，这类应用也称为联机事务处理（on line transaction processing，OLTP）；分析型数据处理主要用于管理人员的决策分析，如决策支持系统（decision support system，DSS），经常需要访问大量的历史数据，通过对这些历史数据的分析，从中发现管理决策中所需要的重要信息，这类应用也称为联机分析处理（on line analytical processing，OLTP）。

为了提高决策分析的效率和有效性，需要将分析型与操作型处理的数据相分离，按照DSS处理的需要，对数据分析在空间和时间维度上进行重新组织，建立单独的分析处理环境。数据仓库（data warehouse，DW）正是为了构建这种新的分析处理环境而出现的一种数据存储和维护技术。

数据仓库是为企业或组织的决策制订过程，提供所有类型数据支持的数据集合。数据仓库的最大目标是提供高效的决策分析。无论是DB还是DW，核心都是数据，数据仓库中的数据具有以下特点：

（1）面向主题的数据。传统DB是面向应用来组织和存储数据的，而DW中的数据是面向主题进行组织的。主题是一个抽象的概念，一个组织的业务可以划分为多个主题领域。例如，一个商业公司的业务可划分为制造、销售、人事、财务等主题领域。

（2）数据仓库是集成的。数据仓库中的数据来自分散的操作型数据，将所需数据从原来的数据中抽取出来，进行加工与集成、统一与综合之后才能进入数据仓库。

（3）只读的数据。数据仓库中的数据主要供企业决策分析使用，所涉及的数据操作主要是数据查询，一般情况下并不进行修改操作。

（4）数据仓库中的数据是随时间变化的。数据仓库中的数据是基于时间的数据，也就是说数据仓库随时间变化不断增加新的数据内容，同时数据仓库中包含大量的综合数据，而且这些综合数据与时间有关，即数据仓库的数据都必须带有时间标志，可以让用户获取与他们的分析时间有关的数据。

（5）多级数据。数据仓库必须按不同的层次组织数据，从简单的数据到高度概括和聚合的数据，因为决策者做决策时，会从不同层次去分析数据。

（6）多维数据。数据仓库的数据结构应该是多维数据结构，因为决策者往往要从多个

维度去考察数据。

2. 数据仓库技术

数据仓库技术指一种解决问题的方案，具体地说，是以传统的数据库技术作为存储数据和管理资源的基本手段，以统计分析技术作为分析数据和提取信息的有效方法，以人工智能技术作为挖掘知识和发现规律的科学途径。

3. 数据仓库系统

数据仓库系统的核心部分是数据仓库，但同时向外延伸到事务处理系统中的 DB，以及用来集成数据的程序和分析数据的工具。数据仓库系统由数据抽取工具、数据仓库、元数据、数据仓库管理系统和数据仓库访问工具组成，如图 3-51 所示。

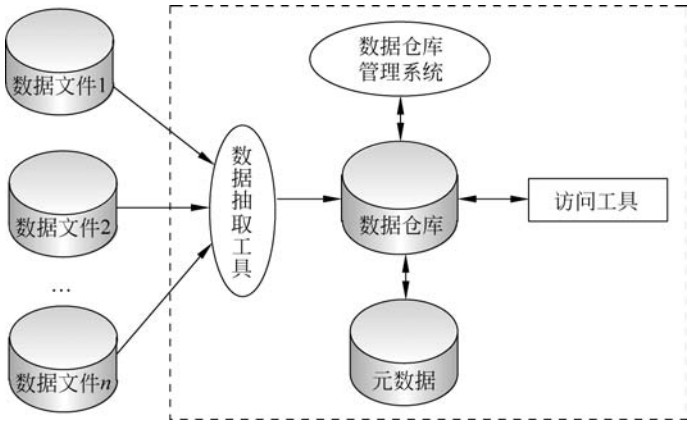


图 3-51　数据仓库系统组成示意图

1）数据抽取工具

数据抽取工具的主要功能是将面向 OLTP 应用的数据库中已有的数据抽取出来，并按照主题组织成决策分析所需要的综合数据。数据抽取工具一般包括监视器和集成器两部分，其中监视器负责感知数据源中数据所发生的变化，并对变化的数据按数据仓库的主体需求进行抽取；集成器将从 OLTP 数据库中提取的数据经过转换、计算、综合等操作，集成后追加到数据仓库中。

2）数据仓库

存储已经按主题组织的数据，供决策分析处理使用。数据仓库是数据仓库系统的核心，是数据分析和挖掘的基础。根据不同的分析要求，数据仓库中的数据一般按不同的综合程度（等级）存储。

3）元数据

元数据是数据仓库运行和维护的中心，为访问数据仓库提供了一个目录，该目录全面描述了数据仓库中有哪些数据，这些数据是怎么得到的，以及怎么访问这些数据等信息。

4）数据仓库管理系统

数据仓库管理系统（data warehouse management system，DWMS）是整个数据仓库系统的管理引擎，负责提供数据定义、数据操作和系统运行管理等功能。目前的 DWMS 一般都是在 DBMS 中增加一些 DW 管理所需要的组件来实现，例如 MS SQL Server 2016 就是

一个 DWMS 与 DBMS 共存的集成系统。

5）访问工具

访问工具用于用户访问数据仓库，主要包括数据查询和报表工具、应用开发工具、联机分析处理工具、数据挖掘工具等。只有通过高效的访问工具，数据仓库才能真正发挥应有的作用。

4. 数据挖掘

数据挖掘（data mining，DM）也称为知识发现，是通过仔细分析大量数据来揭示有意义的新的关系的过程。数据挖掘是一门交叉性学科，融合了人工智能、数据库技术、模式识别、机器学习、统计学和数据可视化等多个领域的理论和技术。

数据挖掘的任务就是发现隐藏在数据中的模式，通常情况下存在两种类型：描述型（Descriptive）模式和预测型（Predictive）模式。其中描述型模式是对当前数据中存在的事实做出规范描述，刻画当前数据的一般特性；预测型模式则是以时间为关键参数，对于时间序列型数据，根据其历史和当前的值去预测其未来的值。根据模式特征，可将模式大致细分为分类模式、聚类模式、回归模式、关联模式、序列模式、偏差模式等类型。

数据挖掘的对象除传统数据库和数据仓库外，目前已扩展到 Internet 环境下的 Web 数据挖掘等众多领域。

3.6.3 关系数据库

在数据库发展历史上先后经历了层次数据库、网状数据库和关系数据库等阶段，目前关系数据库已经成为数据库产品中最重要的一员，几乎所有的数据库厂商的数据库产品都支持关系数据库，即使一些非关系数据库产品也几乎都有支持关系数据库的接口。

1. 数据模型

数据模型（data model）是对现实世界数据特征的抽象，是用来描述数据的一组概念和定义。由于计算机无法直接处理现实世界中的具体事物，所以人们必须事先把具体事物转换成计算机能够处理的数据，即按 DBMS 支持的数据模型来组织数据。通常，一个数据库的数据模型由数据结构、数据操作和数据约束条件 3 部分组成。

由于数据库中的数据是按照一定的结构（数据模型）来组织、描述和存储的，所以常见的数据模型有层次数据模型、网状数据模型、关系数据模型和面向对象数据模型几种类型。

（1）层次数据模型。层次数据模型是按树状结构描述客观事件及其联系的一种数据模型。

（2）网状数据模型。网状数据模型是按网状结构描述客观事物及其联系的一种数据模型。

（3）关系数据模型。关系数据模型是按二维表结构描述客观事物及其联系的一种数据模型。基于关系数据模型的关系数据库管理系统主要有 Visual FoxPro、Access、Oracle、Sybase、SQL Server 等。

（4）面向对象数据模型。面向对象数据模型用更接近人类的思维方式来描述客观世界的事物及其联系，而且描述问题的问题空间和解决问题的方法空间在结构上尽可能一致，以

便对客观实体进行结构模拟和行为模拟。

由于关系数据模型能够用二维表来表示事物之间的联系，因此得到了广泛应用。

2. 关系数据模型

在关系数据模型中，所有的信息都用二维表来表示，每一张二维表称为一个关系(Relation)或表(Table)，用来表示客观世界中的事物。如表 3-2 所示，一个表由表名、行和列组成，其中每一行称为一个元组，每一列称为一个属性。

表 3-2　学生基本信息表

学号	姓名	性别	出生年月	院系	专业	政治面貌
2021101	刘墙东	男	1972-02-08	商学院	市场营销	
2021102	马芸	男	1968-06-19	商学院	市场营销	党员
2021001	李燕红	女	1973-04-11	计算机学院	软件工程	
2021002	马花腾	男	1973-09-20	计算机学院	软件工程	团员
2021201	王剑玲	男	1962-02-21	建筑学院	建筑设计	党员
2021203	潘四一	男	1969-11-23	建筑学院	室内设计	团员

关系数据库是采用关系模型作为数据组织方式的数据库。关系数据库的特点在于它将每个具有相同属性的数据独立地存储在一个表中，对于任一表而言，用户可以插入、删除或修改表中的数据，而不会影响表中的其他数据。在关系数据模型中，表与表之间通常是存在联系的，常见的联系方式主要有以下 3 种：

(1) 一对一联系。一对一联系指对于表 A 中的任一元组，在表 B 中有一个唯一的元组与其对应。例如，一个班级有一个班长，那么班级与班长之间的联系就是一对一联系。

(2) 一对多联系。一对多联系指表 A 中的每一个元组，在表 B 中会存在多个元组与其对应；而对于表 B 中的每一个元组，表 A 中只有一个元组与之对应。

(3) 多对多联系。多对多联系指表 A 中的每一个元组，表 B 中有多个元组与之对应；而对于表 B 中的每一个元组，表 A 中也有多个元组与之对应。假设一位老师可以同时教授多门课程，而同一门课程由多位老师教授，则课程表中老师与课程之间的联系就属于多对多联系。

3. 关系数据库的基本操作

在关系数据库系统中，常见的关系操作主要有插入、删除、更新、选择、投影和连接等。

1) 选择

选择操作属于一元操作，它应用于一个关系并产生另一个新关系，新关系中的元组(行)是原关系中元组的子集。选择操作根据要求从原关系中选择部分元组，结果关系中的属性(列)与原关系相同，即保持不变。例如，从学生基本信息表中查询出所有“性别”为“男”的学生记录，即为对该表进行了选择操作。

2) 投影

投影操作属于一元操作，它作用于一个关系并产生另一个新关系。新关系中的属性(列)是原关系中属性的子集。一般情况下，虽然新关系中的元组属性减少了，但其元组(行)的数量与原关系保持不变。例如，从学生基本信息表中查询所有学生的“学号”“姓名”和“专业”，即为对该表进行了投影操作。

3）连接

连接操作是一个二元操作，它基于共有属性把两个关系组合起来。根据应用需要，连接操作会存在多种方式。例如，查询每门课程所有学生成绩，即为对课程表和选课表进行连接操作。

4）更新

更新操作用于改变关系属性的值。例如，将课程代号为“210001”课程的所有成绩增加10分，即为对选课表的更新操作。

5）删除

删除操作用于删除关系中的元组。例如，删除学生基本信息表中所有“专业”为“软件工程”的记录，即为对该表的删除操作。

4. SQL 语言

SQL(structured query language，结构化查询语言)是用来访问和操作数据库系统的一种通用语言。SQL 语句既可以查询数据库中的数据，也可以添加、更新和删除数据库中的数据，还可以对数据库进行管理和维护操作。不同的数据库都支持 SQL，这样，通过学习 SQL 这一语言，就可以操作各种不同的数据库。SQL 语言是关系数据库的标准语言，具有功能丰富、使用灵活、语言简单易用等特点。

虽然 SQL 已经被标准化，但在应用中大部分数据库都在标准 SQL 上做了扩展。也就是说，如果仅使用标准 SQL，所有的数据库都可以支持，但如果使用某个特定数据库的扩展 SQL，换一个数据库就可能无法执行。例如，Oracle 把自己扩展的 SQL 称为 PL/SQL，Microsoft 把自己扩展的 SQL 称为 T-SQL。现实情况是，如果只使用标准 SQL 的核心功能，那么所有数据库通常都可以执行。不常用的 SQL 功能，不同的数据库支持程度不尽相同。

5. 结构化数据、非结构化数据和半结构化数据

随着大数据技术的发展，针对数据结构的分类及处理问题得到普遍重视。根据数据的组织和管理形式的不同，可将大数据环境中的数据细分为结构化数据、非结构化数据和半结构化数据三种类型。

1）结构化数据

结构化数据指由二维表结构来逻辑表达和实现的数据(表 3-2)，严格地遵循数据格式与长度规范，主要通过关系型数据库(如 MySQL、Oracle、SQL Server 等)进行存储和管理。

结构化数据管理的一般特点是：数据以行为单位，一行数据表示一个实体的信息，每一行数据的属性是相同的。结构化的数据的存储和排列很有规律，这对查询和修改等操作很有帮助。但是，结构化数据的扩展性较差，例如在一张二维表中要增加一列时，需要在表中添加一个全新的“属性”字段。

从数据处理的角度，结构化数据时只需要创建一个二维表，然后将每一个实体以行为单位添加到表中，数据处理相对简单。

2）非结构化数据

非结构化数据是数据结构不规则或不完整，没有预定义的数据模型，不方便用数据库二维逻辑表来表现的数据，它包含全部格式的办公文档、文本、图片、XML、HTML、各类报表、