【课外拓展】

关于防止数据丢失的 3 个方法

1. 永远不要将文件数据保存在操作系统的同一驱动盘上

我们知道大部分文字处理器会将用户创建的文件保存在“我的文档”中，然而这恰恰是最不适合保存文件的地方。对于影响操作系统的大部分电脑问题（不管是因为病毒问题还是软件故障问题），通常唯一的解决方法就是重新格式化驱动盘或者重新安装操作系统，如果是这样的话，驱动盘上的所有数据都会丢失。

另外一个成本相对较低的解决方法就是在电脑上安装第二个硬盘，当操作系统被破坏时，第二个硬盘驱动器不会受到任何影响，如果还需要购买一台新电脑时，这个硬盘可以安装在新电脑上，而且这种硬盘安装非常简便。

还有一个很好的选择，就是购买一个外接式硬盘，外接式硬盘操作更加简便，可以在任何时候用于任何电脑，而只需要将它插入 USB 端口或者 FireWire 端口。

2. 定期备份文件数据，不管它们被存储在什么位置

将文件全部保存在操作系统是不够的，应该将文件保存在不同的位置，并且需要创建文件的定期备份，这样我们就能保障文件的安全性，不管备份是否会失败：光盘可能被损坏，硬盘可能遭破坏，软盘被清除等原因。如果想要确保能够随时取出文件，那么可以考虑进行二次备份，如果数据非常重要的话，甚至可以考虑在防火层保存重要的文件。

3. 提防用户错误

事实上，很多时候是因为我们自己的问题而导致数据丢失。可以考虑利用文字处理器中的保障措施，例如版本特征功能和跟踪变化。用户数据丢失最常见的情况就是当他们在编辑文件的时候，意外地删除掉某些部分，那么在文件保存后，被删除的部分就丢失了，除非你启用了保存文件变化的功能。

如果觉得那些功能麻烦，那么建议在开始编辑文件之前将文件另存为不同名称的文件，这个办法不像其他办法一样组织化，不过能起到很好的预防作用，但能够解决数据丢失的问题。

任务 4　杀毒软件

【任务描述】

（1）了解计算机病毒的概念、特点及常见病毒的种类。

（2）掌握计算机安全防护的方法。
（3）正确使用常见的杀毒软件、防火墙工具。

【任务分析】

本任务的关键点：

（1）认识计算机病毒。
（2）了解计算机病毒工作原理。
（3）会使用杀毒软件。

【预备知识】

杀毒软件（Antivirus Software）用于侦测、移除计算机病毒、计算机蠕虫和特洛伊木马程序。杀毒软件通常含有实时程序监控识别、恶意程序扫描和清除及自动更新病毒数据库等功能，有的杀毒软件附加损害恢复等功能，是计算机防御系统（包含杀毒软件，防火墙，特洛伊木马程序和其他恶意软件的防护及删除程序，入侵防御系统等）的重要组成，如图 5.39 所示。

图 5.39　杀毒软件

2014 年，病毒总体数量比去年同期增长 93.01%，呈现出一个爆发式的增长态势。其中主要以木马和感染型病毒为主，通过盗号、后台数据窃取而进行隐私信息贩售的黑色产业链现已具规模。比特币、电视选秀节目、留学生 QQ 和 Cookie 成为黑客及网络诈骗者重点关注的对象。黑客制作病毒盗取比特币，并控制用户电脑组成僵尸网络。同时，电视选秀节目类钓鱼网站开始在互联网上疯狂传播，为用户的网络生活带来巨大风险。在移动互联网方面，智能手机 APP 暴露出众多安全隐患，既有资费损失，又会丢失个人信息。大量手机病毒传播者使用远程控制的手法，在中毒手机上安装推广软件、后台订购付费服务、窃取用户手机里的个人信息，如图 5.40 所示。

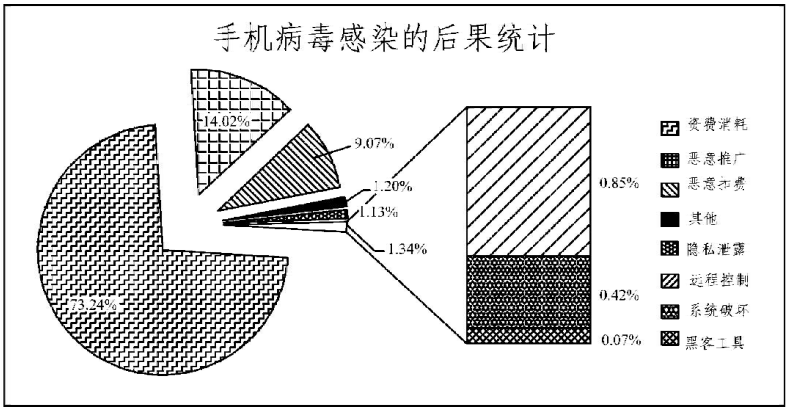

图 5.40　手机病毒

杀毒软件就是一个信息分析的系统，它监控所有的数据流动（包括：内存—硬盘网络—内存网络—硬盘），当它发现某些信息被感染后，就会清除其中的病毒。信息的分析（或扫描）方式取决于其来源，杀毒软件在监控光驱、电子邮件或局域网间数据移动时，工作方式是不同的。

杀毒软件主要负责监控内存及文件。内存监控：当发现内存中存在病毒的时候，就会主动报警；监控所有进程；监控读取到内存中的文件；监控读取到内存的网络数据。文件监控：当发现写到磁盘上的文件中存在病毒，或者是被病毒感染，就会主动报警。

全球知名杀毒软件：俄罗斯的卡巴斯基、罗马尼亚的 BitDefender、德国的 G Data、芬兰的 F-Secure、斯洛伐克的 ESET NOD32、捷克的 Avast 等。

【任务实施】

360 杀毒是中国使用人数最多的杀毒软件，也是迄今国内唯一包揽 AV-C、AV-TEST、VB100、CheckMark、ICSA、OPSWAT 等各大国际评测“全满贯”的杀毒软件。与 4.0 版相比，5.0 正式版启用了全新的产品界面，引入了更为丰富的交互方式。

（1）360 杀毒软件安装，如图 5.41 所示。

图 5.41　安装 360 软件

（2）操作 360 杀毒软件主界面，如图 5.42 所示。

图 5.42　360 杀毒软件界面

（3）设置 360 杀毒软件，如图 5.43 所示。

图 5.43　360 杀毒软件设置界面

（4）使用 360 杀毒软件杀毒，如图 5.44 所示。

图 5.44　360 杀毒软件杀毒界面

【课堂实践】

通过杀毒软件的学习，完成 360 杀毒软件“功能大全”选项卡里面的操作，如图 5.45 所示。

图 5.45　杀毒软件功能大全

【课外拓展】

你应该知道的杀毒软件常识

（1）杀毒软件不可能查杀所有病毒。

（2）杀毒软件能查到的病毒，不一定能杀掉。

（3）一台电脑每个操作系统下不能同时安装两套或两套以上的杀毒软件（除非有兼容或绿色版，现在其实很多杀软兼容性很好，国产杀毒软件几乎不用担心兼容性问题），另外建议查看不兼容的程序列表。

（4）杀毒软件目前对被感染的文件杀毒有多种方式：

① 清除：清除被蠕虫感染的文件，清除后文件恢复正常。相当于如果人生病，清除是给这个人治病，删除是人生病后直接杀死。

② 删除：删除病毒文件。这类文件不是被感染的文件，本身就含毒，无法清除，可以删除。

③ 禁止访问：禁止访问病毒文件。在发现病毒后用户如选择不处理则杀毒软件可能将病毒禁止访问。用户打开时会弹出错误对话框，内容是“该文件不是有效的 Win32 文件”。

④ 隔离：病毒删除后转移到隔离区。用户可以从隔离区找回删除的文件。隔离区的文件不能运行。

⑤ 不处理：不处理该病毒。如果用户暂时不知道是不是病毒，可以暂时先不处理。

大部分杀毒软件是滞后于计算机病毒的。所以，除了及时更新升级软件版本和定期扫描的同时，还要注意充实自己的计算机安全以及网络安全知识，做到不随意打开陌生的文件或者不安全的网页，不浏览不健康的站点，注意更新自己的隐私密码，配套使用安全助手与个人防火墙等。这样才能更好地维护好自己的电脑以及网络安全。

任务 5　硬盘、内存检测

【任务描述】

学习“预备知识”所述内容，练习硬盘和内存检测工具的使用方法。

【任务分析】

本任务的关键点：

（1）了解硬盘和内存出现问题导致 Ghost 安装的中断，不能正确地复制文件。

（2）掌握硬盘分区出现问题可以导致 Ghost 不能正确地认出硬盘及硬盘和内存检测工具的使用方法。

（3）了解 RST 内存检测软件的使用方法。

【预备知识】

硬盘分区而出现错误提示或者是硬盘有坏道，数据在复制到坏道的过程中由于不能正确地复制而导致出现一些常见的错误提示，从而导致 Ghost 安装的中断，如果怀疑硬盘出现问题可以先对硬盘进行重新分区看能否解决问题，如果重新分区后仍不能解决问题，那么可以用专业的硬盘检测工具对硬盘进行检测，看有无坏道。

【任务实施】

1. 硬盘的扫描

硬盘的扫描大多采用 MHdd29，下面我们以 MHdd29 为例进行讲解。

放入工具盘，从 DOS 工具箱启动，如图 5.46 所示。

图 5.46　启动 DOS 工具箱

在 DOS 下运行 Mhdd29：输入命令 Mhdd29，按回车，出现主界面，如图 5.47 和 5.48 所示。

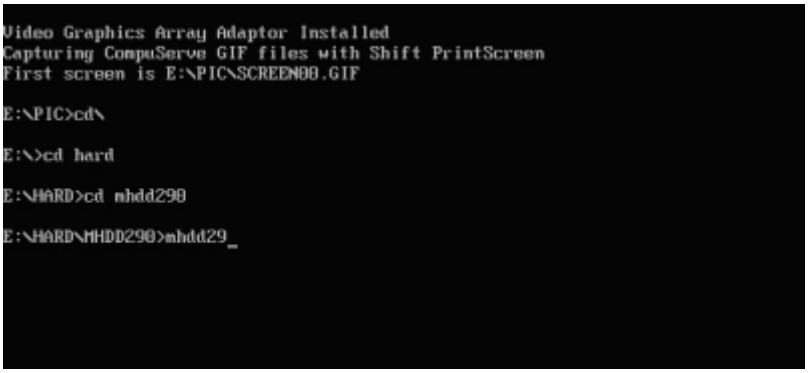

图 5.47　启动 Mhdd29

图 5.48　Mhdd29 主界面

主界面列出了 Mhdd 的所有命令，下面主要讲解 Mhdd 的几个常用命令。

PORT；ID；SCAN；HPA；RHPA；NHPA；PWD；UNLOCK；DISPWD；ERASE；AERASE；STOP。

（1）输入命令 PORT（热键是“Shift+F3”），按回车。这个命令的意思是扫描 IDE 口上的所有硬盘，如图 5.49 所示。

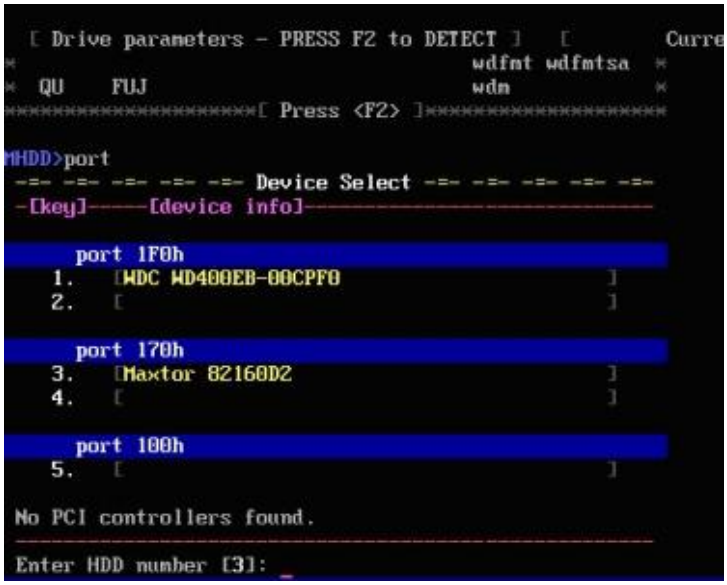

图 5.49　PORT 命令效果

现在能看到有两个硬盘，一个是西数 40 G，一个是迈拓 2 G。（说明：1、2 是接在 IDE1 口上的主从硬盘，3、4 是接在 IDE2 口上的主从硬盘，5 是接在 PC3000 卡上的。如果我们要修的硬盘接在 PC3000 上，就会在这里显示）。下面是选择要修哪个硬盘，输入 3，回车，如图 5.50 所示。

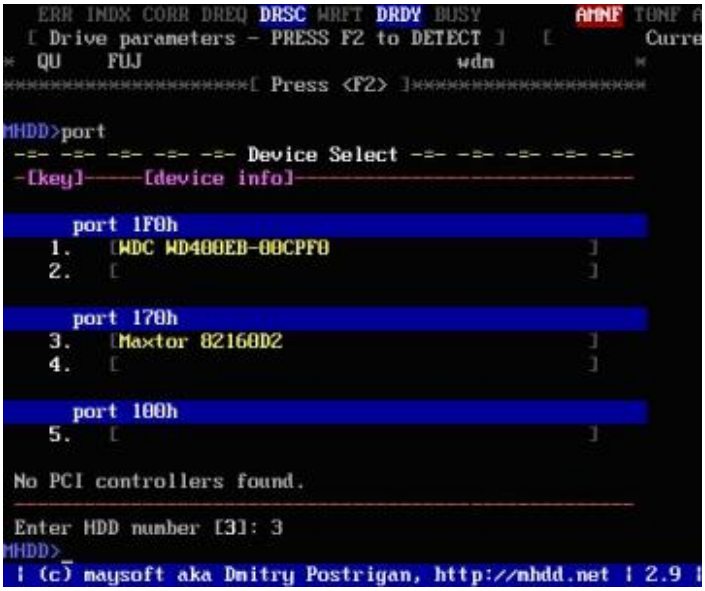

图 5.50　选择硬盘

（2）输入命令 ID（以后直接按“F2”也可以）回车，显示当前选择的硬盘的信息，如图 5.51 所示。

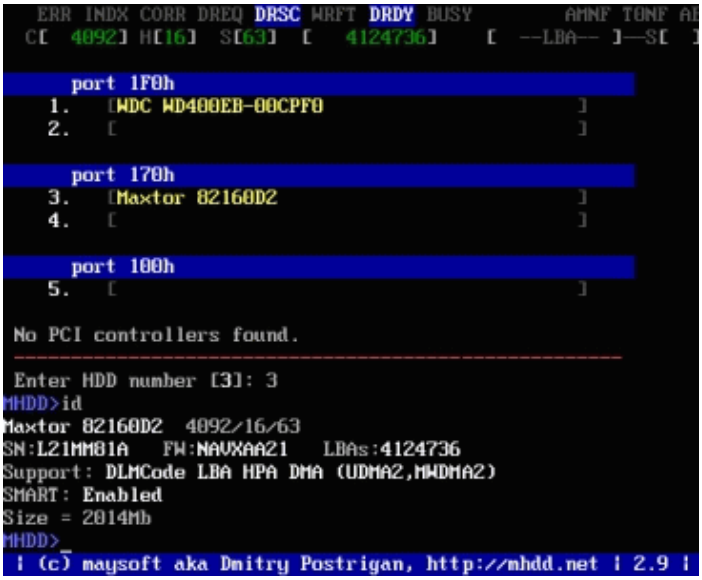

图 5.51　ID 命令

（3）输入命令 SCAN（热键：F4），回车。这个命令的意思是扫描硬盘，共有 12 行要修改的参数，如图 5.52 所示。

图 5.52　SCAN 命令

① 选择扫描方式：LBA/CHS 建议选择 LBA 方式扫描，CHS 只对 500 M 以下的老式硬盘有效。

② 设定开始的柱面值（一般不用）。

③ 设定开始的 LBA 值（常用，按空格键输入新的 LBA 值）。

④ 是否写入日志：ON/OFF（建议打开）。

⑤ 是否地址重映射：ON/OFF 是否修复坏扇区（如果打开这一项，可以不破坏数据修坏道。此项与第 12 项不能同时打开）。

⑥ 设定结束的柱面（一般不用）。

⑦ 设定结束的 LBA 值（常用）。

⑧ 设定超时值（秒）：25 Erase WAITS 的时间默认为 250 毫秒，数值可设置范围为 10～10 000。此数值主要用来设定 Mhdd 确定坏道的读取时间值（即读取某扇区块时如果读取时间达到或超过该数值，就认为该块为坏道，并开始试图修复），一般情况下更改此数值不要太大也不要太小，否则会影响坏道的界定和修复效果。

⑨ 是否写入高级日志：ON/OFF（此项被禁用）。

⑩ 扫描完后是否关闭电机：ON/OFF（扫描结束后关闭硬盘马达，这样即可使 SCAN 扫描结束后，电机能够自动切断供电，但主板还是加电的。适合无人值守状态，一般不用）。

⑪ 是否循环测试，修复：ON/OFF（如果此项为 ON，当第一次扫描结束后，就会再次从开始的 LBA 到结束的 LBA 重新扫描修复，如此循环）。

⑫ 是否删除等待：ON/OFF（此项与第五项不能同时打开，此项主要用于修复坏道，而且修复效果要比 REMAP 更为理想，尤其对 IBM 硬盘的坏道最为奏效，但要注意被修复的地方的数据是要被破坏的，因为 EraseWAITS 的每个删除单位是 255 个扇区）。

以上 12 个参数如果要修改，都是先按空格键。一般情况下先看看硬盘什么情况，这里直接按“F4”（或者按“Ctrl+Enter”）就开始扫描了，如图 5.53 所示。

图 5.53　硬盘扫描

屏幕第一行的左半部分为状态寄存器，右半部分为错误寄存器。在屏幕第一行的中间（在 BUSY 和 AMNF 之间）有一段空白区域，如果硬盘被加了密码，此处会显示 PWD；如果硬盘用 HPA 做了剪切，此处会显示 HPA；屏幕第二行的左半部分为当前硬盘的物理参数（虚拟的，当然不会真的有 16 个磁头），右半部分为当前正在扫描的位置；屏幕右下角为计时器，Start 表示开始扫描的时间，Time 表示已消耗的时间，End 表示预计结束的时间，结束后会再显示 Time Count，表示总共耗费了多长的时间；在扫描时，每个长方块代表 255 个扇区（在 LBA 模式下）或 63 个扇区（在 CHS 模式下）。

这里要解释一下 CHS：Cylinder Head Sector 这三个单词的第一个字母组合，意思是柱面、磁头、扇区。LBA 是扇区（线性地址）的意思。

扫描过程可随时按 ESC 键终止；方块从上到下依次表示从正常到异常，读写速度由快到

慢。正常情况下，应该只出现第一个和第二个灰色方块，如果出现浅灰色方块（第三个方块），则代表该处读取耗时较多。

① 如果出现绿色和褐色方块（第三个和第四个方块），则代表此处读取异常，但还未产生坏道。

② 如果出现红色方块（第六个，即最后一个方块），则代表此处读取吃力，马上就要产生坏道。

③ 如果出现问号“？”以下的任何之一，则表示此处读取错误，有严重物理坏道，如图 5.54 所示。

图 5.54　扫描情况

（4）ERASE，即快速擦除命令，有低格和清零的功效，但此命令一点不影响硬盘寿命，有时对坏道和红绿块擦除能起到意想不到的作用。输入命令，按回车，如图 5.55 所示。

图 5.55　ERASE 命令

问是否继续，输入 Y，输入开始的 LBA 值（就是从哪个地方开始有坏道或红绿块），比

如我们输入零，回车，再输入结束的 LBA 地址，我们输入 10000，回车，输入 Y，回车，开始擦除，并显示擦除了多少兆字节，速度非常快，如图 5.56 所示。

图 5.56　擦除完成

2. 内存常见问题

内存出现问题也能导致 Ghost 恢复过程中死机或者提示不能正确地复制文件，这是由于内存自身的问题导致文件不能正确地传输到硬盘就会在 Ghost 完成后出现 c:\windows\ system 32\xxxx 文件丢失，请重新放入系统安装盘。

内存扫描工具市面上有很多，我们以 Ram Stress Test 为例。

（1）打开内存扫描工具，如图 5.57 所示。

图 5.57　内存扫描工具

（2）启动内存检测，如图 5.58 所示。

图 5.58　内存检测

（3）查看扫描结果，如图 5.59 所示。

图 5.59　内存扫描

下面是 512 MB 的双面内存，从 256 M 开始区分红色的是 A 面，绿色的是 B 面，如图 5.60 所示。

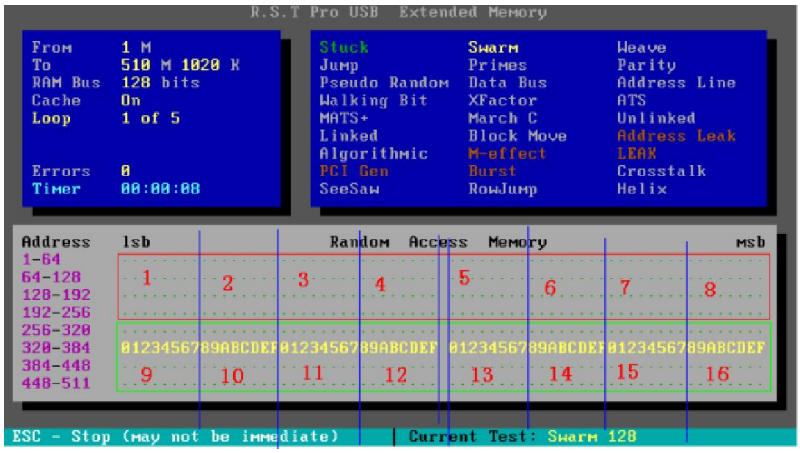

图 5.60　512M 双面内存

图 5.61 中是 128 M 母条带双面 512 M 检测条，1 M～128 M 是母条，128 M～639 M 就是 512 M 的内存条，绿色是内存条的 A 面，红色的是 B 面。

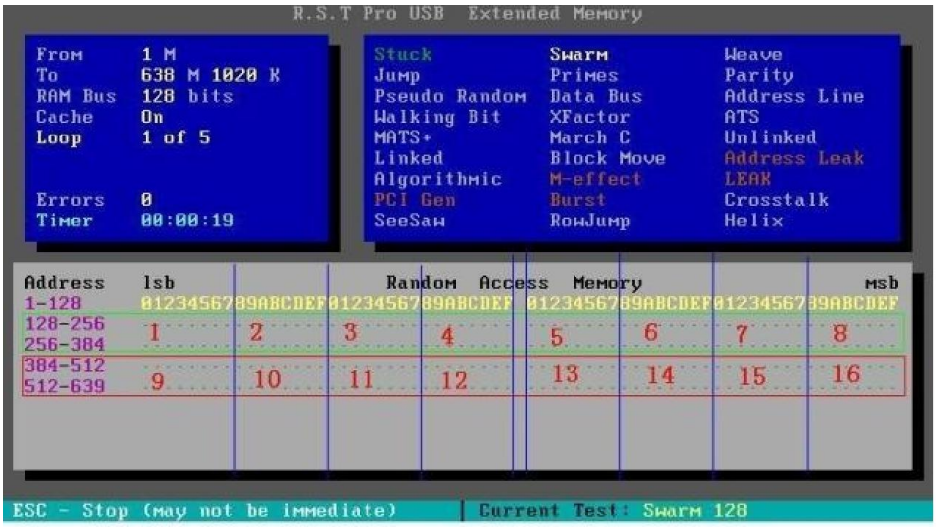

图 5.61　内存扫描结果

3. 注意事项

（1）要求最好用独立显卡主板，如果使用集成显卡，由于有几兆内存会划给显存，所以不能全测到。

（2）检测过程中，软件会回写信息资料，请勿检测过程中拔出。

（3）本软件可选版本 IDE，SATA，电子盘，U 盘，网络 PXE，版定制。

（4）有条件尽量使用频率高的 CPU 进行测试，可以加快测试速度。

① 纠正：R.S.T Pro3 不支持如 2G 16 颗芯片的内存，前 1G 代表正面，后 1G 代表背面的判别逻辑。

② RST 系列软件虽然不支持此上述判别逻辑，但我们可以通过刷写 SPD 的方法，来区分是正面还是反面。

当检测到双面坏位时，将内存烧录一半的容量（此时背面会屏蔽掉，等于没有）再测试，如果 OK 了，说明是背面对应的颗粒坏了；反之则正面。

【课堂实践】

通过检测工具使用方法学习，完成以下操作：

（1）将一台硬盘出现问题的主机进行检测，分析其问题。

（2）练习如何使用检测工具。

【课外拓展】

多认识和了解有关修复和检测的工具和软件，并掌握其使用方法。

任务 6　操作系统密码破解

【任务描述】

使用软件工具破解操作系统的用户密码。

【任务分析】

本任务的关键点：

（1）了解工具软件的破译、绕过口令功能。

（2）使用工具软件绕过、破译、删除用户口令。

【预备知识】

我们在使用计算机过程中，为了保护数据安全，常会设置系统账户登录密码或者是开机启动密码。但有时却会忘记所设密码。

如今电脑软驱早已被光驱所取代。随着主板的支持，U 盘启动逐渐成为一种趋势。因此，我们可到网上搜索下载，如深度、电脑公司等系统装机版，其内都集成了 DOS 和 PE 工具（注意校验 MD5 码），然后制作成光盘或 U 盘方式的启动盘以备用。

【任务实施】

下面以 XP 系统为例，讲解行之有效的在各种状态下对应破解密码的方法。

1. 破解系统管理员登录密码

采用设置为系统管理员密码方式的用户较多。当电脑启动进入系统时会弹出输入密码的提示框，如图 5.62 所示。

运行系统工具光盘到菜单，选择运行“系统登录密码破解”项（有的 PE 内也带有清除密码的工具，甚至可以重置密码），如图 5.63 所示。

图 5.62　密码登录框

图 5.63　系统登录密码破解

在“请输入序号”后敲入“2”自动在所有硬盘和分区上搜索 SAM 文件，回车，会自动显示出 SAM 文件所在的位置，回车继续，如图 5.64 所示。

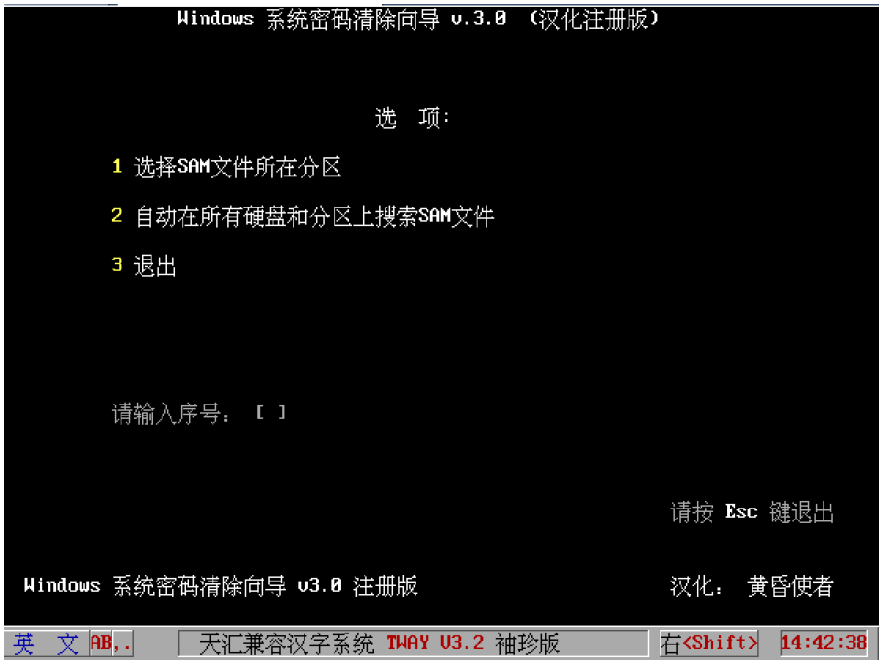

图 5.64　自动搜索

选择输入要清除的用户序列号，如我们这里选择 Administrator [0]，回车，如图 5.65 所示。

图 5.65　选定用户破解

按空格选中“清除此用户密码”,之后按“Y”保存更改。然后重启计算机密码清除成功。

注意：光盘带有这种功能其实就是一种写好的批处理文件（.bat）刻成盘，当然也可以自己编写。

2. 破解 BIOS 设置密码（即设置了 SETUP 密码）

我们如果忘了 SETUP 密码就设置不了 BIOS。这时，可进入 DOS，运行 DEBUG 编辑器来清除 BIOS 密码。在 DOS 命令提示符状态下输入命令：DEBUG，即可进入 DEBUG 编辑界面。

在命令符状态下输入命令行后，重新启动电脑即可清除 CMOS 密码。下面给出五个清除 CMOS 密码的命令行。

方法一	方法二	方法三	方法四	方法五
-o 70 16	-o 70 11	-o 70 10	-o 70 23	-o 70 10
-o 71 16	-o 71 ff	-o 71 10	-o 71 34	-o 71 ff
-q	-q	-q	- q	-q

重新启动电脑，将会出现诸如“CMOS Checksum Error-DeFaults Loaded”，那就是提示你 CMOS 检测出错,请重新设置其内容,这时你只需进入 BIOS 设置程序,选择主菜单中的“LOAD BIOS DEFAULT”（装入 BIOS 缺省值）或“LOAD SETUP DEFAULT”（装入设置程序缺省值），然后重启电脑即可。

说明:如果 BIOS 中禁用了光驱启动,我们可以用带命令的安全模式或 U 盘等来启动 DOS。

【课堂实践】

通过 Win 7 操作系统密码的破解，完成图 5.66 中的操作。

图 5.66　绕过 Win 7 密码

【课外拓展】

通过自学了解如何实现 WIFI 密码的破解。