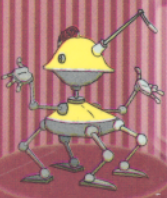
Ban biên dịch CADASA
Chủ biên: NGUYỄN THẾ HÙNG

Những điều cốt yếu mà người sử dụng máy vi tính cần phải biết

VIRUS Cách PHỤC HỒI & PHÒNG CHỐNG



- Công tác bảo dưỡng phòng ngừa
- Các loại virus và hình thức phá hoại
- Cách sao lưu dự phòng và kháng lỗi

N HỌC CHO MỌI NGƯỜI

NHÀ XUẤT BẢN THỐNG KÊ

BAN BIÊN DỊCH **CADASA**
Chủ biên **NGUYỄN THẾ HÙNG**

VIRUS, CÁCH PHỤC HỒI VÀ PHÒNG CHỐNG

NHÀ XUẤT BẢN THỐNG KÊ
- 2001 -

Tổng hợp và biên dịch từ các tài liệu:

- Guide To Managing and Maintaining your PC
  Jean Andrews
- Managing your Hard Disk
  Don Berliner & Chris Devoney
- Multimedia Networking
  Bohdan O. Szuprowicz
- Teach yourself the Internet
  Nei Randall

Lời giới thiệu

Một trong những trở ngại mà bạn thường xuyên gặp phải trong khi làm việc với máy vi tính đó là virus.Virus đã làm rối loạn hoặc hư hỏng hoàn toàn chương trình của bạn, làm bạn mất khá nhiều thời gian và công sức, chưa nói là nó có thể gây nên những "thảm họa".

Việc bảo dưỡng thường xuyên có thể giúp ngăn ngừa thảm họa, giảm thiểu chi phí sửa chữa và giảm thiểu thiệt hại khi có sự cố xảy ra là một công việc cần yếu của bạn.

*Nằm trong tủ sách **NHỮNG ĐIỀU CỐT YẾU MÀ NGƯỜI SỬ DỤNG MÁY VI TÍNH CẦN PHẢI BIẾT**, tài liệu này sẽ đề cập đến hai khía cạnh quan trọng của việc bảo dưỡng phòng ngừa bao gồm việc tạo các bản sao dự phòng đều đặn của các đĩa ổ cứng và việc giải quyết các virus. Ngoài ra, phương pháp bảo dưỡng phần cứng thường xuyên và cách thiết kế một kế hoạch phục hồi sau thảm họa, cũng sẽ được giới thiệu một cách chi tiết trong tài liệu này.*

Mong rằng tài liệu này sẽ là người bạn thân thiết của bạn.

Ban biên dịch CADASA

Mục lục

1 Công tác bảo dưỡng phòng ngừa

Nếu phụ trách các máy PC của một tổ chức, bạn cần thiết kế và triển khai một kế hoạch bảo dưỡng phòng ngừa nhằm giúp ngăn ngừa các sự cố hỏng hóc, đồng thời giảm thiểu chi phí sửa chữa và thời gian ngưng trệ *(downtime)*. Ngoài ra, bạn nên có một kế hoạch phục hồi sau thảm họa để sẵn sàng đối phó với các sự cố hỏng hóc có thể xảy ra bất kỳ lúc nào. Các sự cố máy PC thường do rất nhiều yếu tố con người và môi trường khác nhau gây ra, bao gồm sức nóng, bụi bặm, từ tính, các sự cố bộ nguồn, tĩnh điện, lỗi con người *(chẳng hạn làm đổ chất lỏng hoặc vô tình thay đổi các cấu hình hệ thống, cấu hình phần mềm)* và các virus. Mục tiêu của việc bảo dưỡng phòng ngừa bao gồm (1) để giảm thiểu khả năng xảy ra các sự kiện khiến cho máy PC bị sự cố, (2) để giảm bớt tác hại khi chúng xảy ra. Khi thiết kế một kế hoạch bảo dưỡng phòng ngừa, bạn cần cân nhắc những gì bạn có thể làm để giúp ngăn ngừa mỗi nguyên nhân sự cố và ghi rõ vào kế hoạch này những hành động ngăn ngừa mà bạn có thể thực hiện. Bạn cần

suy luận ra tình huống mà mỗi sự cố sẽ gây ra. Điều gì có thể xảy ra cho máy PC, phần mềm, các dữ liệu, năng suất của người dùng ...vv khi một sự cố hỏng hóc xảy ra? Bạn sẽ phải làm những gì và bạn sẽ cần tới những thứ nào trong tình huống đó? Những gì có thể làm trước để tình huống này trở nên ít nguy hại hơn? Giải đáp cho các câu hỏi trên sẽ giúp bạn tạo nên một kế hoạch bảo dưỡng và một kế hoạch phục hồi sau sự cố hiệu quả hơn.

Ví dụ, chúng ta hãy xem xét sự cố xảy ra do một người dùng vô tình thay đổi CMOS setup. Bạn có thể làm những gì để ngăn ngừa điều này xảy ra? Nếu nó xảy ra, bạn có thể làm những gì để khắc phục? Những gì có thể làm ngay bây giờ để chuẩn bị cho tình huống đó? Bằng cách trả lời ba câu hỏi này, bạn sẽ xác định được các thủ tục bảo dưỡng phòng ngừa và các thủ tục phục hồi như sau: (1) tạo một bản sao dự phòng chứa các thông tin cấu hình *(setup)* trên một đĩa mềm, (2) ghi nhãn rõ ràng cho đĩa này rồi cất giữ nó ở một nơi an toàn, (3) hướng dẫn người dùng để họ biết về tầm quan trọng của các thông tin setup và giải thích lý do tại sao họ không nên thay đổi các thông tin này và (4) giữ một bản ghi chú bảo dưỡng về máy PC này, bao gồm thời điểm sau cùng bạn tạo bản sao của các thông tin cấu hình.

1. MỘT KẾ HOẠCH BẢO DƯỠNG PHÒNG NGỪA

Nếu công ty của bạn đã xây dựng các hướng dẫn dành cho việc bảo dưỡng máy PC ở dạng văn bản chính thức, bạn hãy đọc chúng và bổ sung thêm các thủ tục cần thiết. Nếu công ty của bạn chưa có một kế hoạch, bạn hãy tự thiết kế ra nó. Một kế hoạch bảo dưỡng phòng ngừa thường có xu hướng được rút ra từ lịch sử các sự cố đã từng xảy ra trong phạm vi tổ chức đó. Chẳng hạn, một môi trường nhiều bụi có thể đòi hỏi sự bảo dưỡng nhiều hơn, trong khi một môi trường sạch có thể đòi hỏi sự bảo dưỡng ít hơn. Bảng 1 liệt kê một số hướng dẫn để bạn có thể phát triển một kế hoạch bảo dưỡng phòng ngừa hiệu quả cho riêng mình.

Bụi bặm gây ảnh hưởng xấu cho một máy PC, vì chúng tác động như một lớp phủ cô lập các bộ phận của máy PC, khiến các bộ phận này trở nên quá nóng. Do đó, việc khử sạch bụi bặm cho máy PC là vấn đề quan trọng trong việc bảo dưỡng phòng ngừa. Một số chuyên viên hỗ trợ PC không muốn sử dụng một máy hút bụi bên trong một máy PC vì họ e rằng ESD *(electrostatic discharge)* do máy hút bụi sinh ra có thể làm hư hại các thành phần. Phương pháp an toàn nhất là sử dụng một bình khí nén để

thổi sạch bụi, vì khí nén không gây ra một sự cố ESD. Tuy nhiên, sau đó có thể bạn sẽ muốn sử dụng một máy hút bụi để hút sạch bụi bặm đã được thổi ra bên ngoài khung máy!

Bảng 1 **Các hướng dẫn cho việc phát triển một kế hoạch bảo dưỡng phòng ngừa cho máy PC.**

Thành phần	Công tác bảo dưỡng	Bao lâu?
Bên trong khung máy	• Bảo đảm rằng các khe thông gió đều sạch. • Sử dụng bình khí nén để thổi sạch bụi bặm ra khỏi khung máy, hoặc sử dụng một máy hút bụi để làm sạch các khe thông gió, bộ nguồn cung cấp và quạt làm mát. • Bảo đảm rằng các chip và các card mở rộng được lắp chắc chắn. • Làm sạch các tiếp điểm trên các card mở rộng.	Hàng năm
CMOS setup	Duy trì một bản ghi dự phòng của các thông tin cấu hình *(ví dụ, sử dụng đĩa mềm cứu nguy của Nuts & Bolts).*	Bất kỳ khi nào các thay đổi được thực hiện.
Ổ đĩa mềm	Chỉ chùi đầu đọc/ghi của ổ đĩa mềm khi ổ đĩa này không hoạt động.	Khi ổ đĩa bị sự cố.

Thành phần	Công tác bảo trì	
Ổ đĩa cứng	• Thực hiện sao lưu thường xuyên. • Tự động thi hành một chương trình quét virus khi khởi động. • Thường xuyên khử phân mảnh cho ổ đĩa cứng và phục hồi các liên cung bị thất lạc. • Không cho phép hút thuốc gần máy PC. • Đặt máy PC tại nơi mà nó sẽ không bị va chạm hoặc bị đá phải.	Ít nhất hàng tuần Ít nhất hàng ngày Hàng tháng Luôn luôn Luôn luôn
Bàn phím	• Giữ cho bàn phím luôn sạch sẽ. • Giữ bàn phím tránh xa các chất lỏng.	Hàng tháng Luôn luôn
Con chuột	• Làm vệ sinh cho các trục lăn và bi xoay trong con chuột (quyển tài liệu *"Các kỹ năng giải quyết sự cố cơ bản"*).	Hàng tháng
Monitor	• Lau sạch màn hình bằng một mảnh vải mềm.	Ít nhất hàng tháng
Các máy in	• Dọn sạch bụi bặm và các vụn giấy bằng cách sử dụng một bình khí nén hoặc một máy hút bụi. Các mảnh giấy nhỏ có thể được gắp ra bằng nhíp. • Làm sạch đường đi của giấy và ribbon bằng một mảnh vải không có xơ. • Không thấm mực lại cho các ribbon hoặc sử dụng các cartridge toner được nạp lại.	Ít nhất hàng tháng

Phần mềm	• Nếu được sếp ra lệnh, bạn hãy kiểm tra rằng chỉ có các *phần mềm được cho phép* hiện diện trong máy tính. • Thường xuyên xóa các tập tin trong Recycle Bin và các thư mục \Temp. • Xóa bất kỳ tập tin tạm thời nào trong thư mục \DOS.	Ít nhất hàng tháng
Các bản ghi chép	• Duy trì một bản ghi về tất cả các phần mềm, bao gồm các số hiệu phiên bản và hệ điều hành được cài đặt trên máy PC. • Duy trì một bản ghi về tất cả các thành phần phần cứng được lắp đặt, kể cả các xác lập phần cứng. • Ghi nhận thời điểm và công tác bảo dưỡng được thực hiện. • Ghi nhận bất kỳ công việc sửa chữa nào được thực hiện cho máy PC này.	Bất kỳ khi nào các thay đổi được thực hiện.

Ý tưởng chung của việc bảo dưỡng phòng ngừa là làm tất cả những gì bạn có thể để máy PC bền hơn và gặp càng ít sự cố càng tốt. Bạn cũng có trách nhiệm bảo đảm các dữ liệu được an toàn và được sao lưu dự phòng *(backup)*, các bản quyền phần mềm không bị vi phạm (!) và người sử dụng luôn được hỗ trợ. Như với bất kỳ kế hoạch nào, khi thiết kế kế hoạch bảo dưỡng phòng ngừa của mình, trước hết bạn cần

định nghĩa mục tiêu hay các mục tiêu tổng thể, rồi sau đó thiết kế kế hoạch này một cách phù hợp. Các hướng dẫn được liệt kê trong bảng 1 chủ yếu nhắm tới các sự cố có thể làm giảm tuổi thọ của máy PC và cản trở sự hoạt động bình thường của nó.

Việc duy trì các bản ghi và bảo vệ các tài liệu phần cứng cũng như phần mềm đôi khi bị bỏ qua khi đề cập tới công tác bảo dưỡng phòng ngừa. Một bản ghi chép về những gì đã được thực hiện với máy PC sẽ có giá trị khi các sự cố nảy sinh hoặc khi việc nâng cấp đang được xem xét. Bạn nên cất giữ cẩn thận tất cả các tài liệu phần cứng do hãng sản xuất cung cấp. Người sử dụng, là những người không chịu trách nhiệm về phần cứng, có thể sẽ không nhận thức được tầm quan trọng của một tài liệu hướng dẫn *(user manual)* dành cho một thiết bị phần cứng, chẳng hạn như một card âm thanh hoặc một modem và có thể sẽ không bảo vệ cẩn thận các tài liệu này. Bạn nên sắp xếp các tài liệu này trong cùng một túi hồ sơ kèm theo một nhật ký *(log)* ghi nhận lại những gì đã thực hiện cho máy PC này với mục đích bảo dưỡng *(các công việc cài đặt, sửa chữa và một đĩa mềm khởi động chứa một bản sao của CMOS setup dành cho máy PC này).* Bạn có thể dán túi hồ sơ này ở mặt trong của vỏ máy tính. Điều này đặc biệt hữu ích khi bạn phải phụ trách nhiều máy PC đặt tại các nơi xa mà ở đó có thể không có một tủ đựng hồ sơ. Các thông tin này cũng có thể được lưu trữ trong một sổ tay cùng với các sổ tay

khác tại nơi làm việc của bạn. Hãy ghi nhãn rõ ràng cho mỗi sổ tay này để nhận diện máy PC mà nó đang theo dõi và cũng có thể lưu giữ các bản ghi về tất cả các máy PC mà bạn phụ trách trên một máy PC riêng biệt.

Ổ đĩa cứng cần được dọn dẹp gọn gàng sau khi được cài đặt một hệ điều hành hoặc một ứng dụng. Ví dụ, sau khi cài đặt Windows 3.x hoặc Windows 9x, hãy xóa các tập tin tạm thời trong thư mục \DOS hoặc cài đặt lại DOS. Ngoài ra, khi bạn cài đặt phần mềm cho một máy PC lần đầu, nếu đang sử dụng một phiên bản cũ hơn của DOS, bạn hãy kiểm tra lệnh SET TEMP trong tập tin AUTOEXEC.BAT. Nếu đọc thấy *SET TEMP=C:\DOS*, hãy đổi thành SET TEMP=C:\TEMP rồi tạo ra một thư mục TEMP trên ổ đĩa C. Việc lưu trữ các tập tin tạm thời trong thư mục \DOS có thể gây ra các sự cố.

Ngoài danh sách trong bảng 1, có thể khuyến khích người dùng đảm nhận một số thủ tục thông thường, như là một phần trong kế hoạch bảo dưỡng phòng ngừa của bạn. Ví dụ, một người dùng có thể được yêu cầu bảo toàn không gian đĩa cứng bằng cách thường xuyên xóa bỏ các tập tin trong thư mục \TEMP. Đối với Windows 9x và Windows NT, bạn hãy làm trống Recycle Bin bằng cách xóa tất cả các tập tin trong folder này. Ổ đĩa cứng cũng cần được sao lưu dự phòng đều đặn *(để thực hiện một tiến trình sao lưu dự phòng hiệu quả hơn, bạn có thể chọn chỉ sao lưu các thư mục có chứa dữ liệu)*. Các thông tin về các bản

sao dự phòng ổ đĩa cứng sẽ được giới thiệu ở một phần sau của tài liệu này.

2. KHI VẬN CHUYỂN THIẾT BỊ

Khi một máy PC được vận chuyển, nó có thể bị hư hại do vận chuyển mạnh tay, hoặc do tác động của môi trường bên ngoài *(nước, sức nóng, nhiệt độ thấp)*. Ngoài ra, đôi khi máy PC này có thể bị giao nhầm, bị thất lạc hoặc bị đánh cắp. Khi chuẩn bị vận chuyển một máy PC, bạn nên thực hiện một số biện pháp phòng ngừa để bảo vệ máy PC và các dữ liệu. Những nguyên tắc chung khi chuẩn bị di chuyển một máy PC bao gồm:

- Sao lưu ổ đĩa cứng vào một cartridge băng từ. Nếu không thể truy xuất tới một cartridge băng từ, bạn nên sao lưu tất cả các tập tin hệ thống và các tập tin cấu hình quan trọng vào đĩa mềm. Bất kể sử dụng máy tính làm công việc gì, bạn đừng bao giờ vận chuyển một máy tính nếu như ổ đĩa cứng của nó chứa bản sao duy nhất của các dữ liệu quan trọng hoặc các dữ liệu cần được bảo mật.
- Lấy tất cả các đĩa mềm, cartridge băng từ hay đĩa CD-ROM ra khỏi các ổ đĩa, cần bảo đảm rằng các đĩa hay băng từ chứa các dữ liệu sao lưu được bảo đảm an toàn và được bảo vệ trong khi

vận chuyển. Bạn có thể cân nhắc đến việc vận chuyển chúng riêng.

- Tắt công tắc nguồn của máy PC và tất cả các thiết bị khác.
- Tháo các dây nguồn ra khỏi ổ cắm nằm sau lưng máy và ra khỏi các thiết bị. Tháo rời tất cả các thiết bị ngoại vi ra khỏi máy tính.
- Nếu cho rằng sau này có thể có sự khó khăn trong việc nhận diện các dây cáp và các dây nguồn của mỗi thiết bị, bạn hãy ghi nhãn các nối kết dây cáp và dây nguồn bằng băng keo trắng.
- Quấn gọn tất cả các dây dẫn và cột chắc lại bằng dây cao su hoặc dây plastic.
- Đặt máy tính, monitor và tất cả các thiết bị rời vào trong thùng giấy nguyên thủy của chúng hoặc trong các thùng tương tự được chèn các vật liệu bảo vệ.

3. LOẠI THẢI THIẾT BỊ ĐÃ QUA SỬ DỤNG

Với vai trò một chuyên viên hỗ trợ PC, đôi khi bạn phải đảm trách luôn việc xử lý các thiết bị, các hóa chất và các vật liệu đã cũ, hư hỏng hoặc đã qua sử dụng, chẳng hạn như các bộ pin, các cartridge mực toner, các monitor ...vv. Bảng 2 liệt kê các bộ phận và cách loại thải

chúng. Thông thường, tài liệu hướng dẫn của nhà sản xuất cũng cung cấp các chỉ dẫn về cách thức loại thải sản phẩm của họ và các quy tắc môi trường tại địa phương bạn cũng sẽ chỉ dẫn điều này. Một tài liệu **MSDS** (**M**aterial **S**afety **D**ata **S**heet) sẽ cung cấp nhiều thông tin về cách xử lý thích hợp đối với các hóa chất chẳng hạn như các dung môi hóa chất. Bạn có thể tìm thấy tài liệu này tại Web site www.ilpi.com/msds.

Bảng 2 **Các bộ phận máy tính và cách loại thải chúng.**

Bộ phận	Cách loại bỏ
• Các pin Alkaline bao gồm loại AAA, AA, A, C, D và 9V.	Rác bình thường.
• Các pin dạng nút áo được sử dụng trong các máy camera, Flash Path và các thiết bị nhỏ khác. • Các bộ pin được sử dụng trong các máy tính notebook.	Các pin này có thể chứa oxit bạc, thủy ngân, lithium, hoặc cadmium và được coi là chất thải độc hại. Bạn hãy loại thải chúng bằng cách trả về cho đại lý gốc hoặc đem chúng tới một trung tâm xử lý tái chế (*recycling center*). Nếu địa phương bạn không có một trung tâm tái chế, bạn có thể liên lạc với chính quyền địa phương để biết cách xử lý rác thải tại nơi đó.
• Các cartridge mực toner dành cho máy in laser.	Trả về hãng sản xuất hoặc đại lý để được xử lý tái chế.

Bộ phận	Cách loại bỏ
• Các cartridge mực dành cho máy in phun. • Các máy tính. • Các monitor. • Các dung môi và các can đựng hóa chất	Liên lạc với chính quyền hoặc cơ quan bảo vệ môi trường để biết các luật lệ và các quy tắc về xử lý rác thải tại địa phương. Khi vứt bỏ một monitor, trước hết bạn cần khử điện tích cho nó bằng cách đặt một tuốc-nơ-vít bắt ngang qua chấu cắm nóng và chấu cắm tiếp đất của ổ cắm điện của nó *(xem hình 1-1)*. Thủ tục này sẽ tránh cho một ai đó khỏi bị điện giựt khi họ vô tình mở vỏ monitor ra.

Hình 1 Khử điện tích cho một CRT trước khi vứt bỏ.

2 Các virus và các hình thức phá hoại máy tính khác

Một chuyên viên hỗ trợ máy tính cần phải biết cách bảo vệ máy tính chống lại các hình thức phá hoại *(bao gồm cả các virus)*, cách nhận diện chúng và cách diệt trừ chúng. Việc hiểu rõ về các hình thức phá hoại, cách hoạt động của chúng và những nơi chúng ẩn náu sẽ giúp bạn thành công trong việc giải quyết chúng. Một *chương trình phá hoại* (computer infestation) là bất kỳ chương trình không mong muốn nào được truyền cho một máy tính mà người dùng không ý thức về sự hiện diện của nó, được thiết kế để thực hiện nhiều mức độ phá hoại dữ liệu và phần mềm khác nhau. Các chương trình phá hoại thường không làm hư hại phần cứng máy tính, mặc dù khi các thông tin trong cung khởi động *(boot sector)* của một ổ đĩa cứng bị phá hủy, ta có thể thấy các triệu chứng như thể ổ đĩa cứng này đã bị hư hại về mặt vật lý. Các chương trình vốn thường được nhiều người gọi chung là virus thực sự rơi vào một trong ba dạng chương trình phá hoại sau: các virus, các Trojan *horse (Ngựa thành Troa)*, và các sâu máy tính *(worm)*. Ba dạng chương

trình phá hoại này khác biệt nhau về cách lan truyền, mức độ phá hoại và cách ẩn náu.

Các virus hiển nhiên là loại phổ biến nhất trong số ba dạng chương trình phá hoại nêu trên, do đó một trong những biện pháp bảo vệ quan trọng nhất để chống lại các chương trình phá hoại là *phần mềm chống virus* (**antivirus software**, hay AV software), được thiết kế để phát hiện và diệt trừ virus. Trong phần này chúng ta sẽ xem xét một số chương trình AV và cách sử dụng chúng một cách hiệu quả.

1. TÌM HIỂU VỀ CÁC CHƯƠNG TRÌNH PHÁ HOẠI MÁY TÍNH

Một *virus* là một chương trình có thể tự nhân bản bằng cách gắn bản thân nó vào các chương trình khác. Chương trình bị lây nhiễm phải được thi hành thì một virus mới có cơ hội thi hành. (Chương trình bị lây nhiễm thường được gọi là *chương trình chủ* (host program)) Khi một virus thi hành, nó có thể chỉ đơn thuần nhân bản chính nó, hoặc cũng có thể nó sẽ ra tay phá hoại bằng cách thực hiện ngay một số hành động gây hại. Ngoài ra, một virus có thể được lập trình để được kích hoạt và thực hiện một hành động phá hoại tại một số thời điểm xác định trong tương lai, chẳng hạn vào một ngày cụ thể trong năm (ví dụ, virus "*Thứ Sáu ngày 13*"), hoặc tại thời điểm mà một số logic của chương trình chủ *(host program)* được kích hoạt. Một virus khác với một sâu máy tính. *Sâu máy tính*

2 Các virus và các hình thức phá hoại máy tính khác

Một chuyên viên hỗ trợ máy tính cần phải biết cách bảo vệ máy tính chống lại các hình thức phá hoại *(bao gồm cả các virus)*, cách nhận diện chúng và cách diệt trừ chúng. Việc hiểu rõ về các hình thức phá hoại, cách hoạt động của chúng và những nơi chúng ẩn náu sẽ giúp bạn thành công trong việc giải quyết chúng. Một *chương trình phá hoại* (computer infestation) là bất kỳ chương trình không mong muốn nào được truyền cho một máy tính mà người dùng không ý thức về sự hiện diện của nó, được thiết kế để thực hiện nhiều mức độ phá hoại dữ liệu và phần mềm khác nhau. Các chương trình phá hoại thường không làm hư hại phần cứng máy tính, mặc dù khi các thông tin trong cung khởi động *(boot sector)* của một ổ đĩa cứng bị phá hủy, ta có thể thấy các triệu chứng như thể ổ đĩa cứng này đã bị hư hại về mặt vật lý. Các chương trình vốn thường được nhiều người gọi chung là virus thực sự rơi vào một trong ba dạng chương trình phá hoại sau: các virus, các Trojan *horse (Ngựa thành Troa)*, và các sâu máy tính *(worm)*. Ba dạng chương

trình phá hoại này khác biệt nhau về cách lan truyền, mức độ phá hoại và cách ẩn náu.

Các virus hiển nhiên là loại phổ biến nhất trong số ba dạng chương trình phá hoại nêu trên, do đó một trong những biện pháp bảo vệ quan trọng nhất để chống lại các chương trình phá hoại là *phần mềm chống virus* (**antivirus software**, hay AV software), được thiết kế để phát hiện và diệt trừ virus. Trong phần này chúng ta sẽ xem xét một số chương trình AV và cách sử dụng chúng một cách hiệu quả.

1. TÌM HIỂU VỀ CÁC CHƯƠNG TRÌNH PHÁ HOẠI MÁY TÍNH

Một *virus* là một chương trình có thể tự nhân bản bằng cách gắn bản thân nó vào các chương trình khác. Chương trình bị lây nhiễm phải được thi hành thì một virus mới có cơ hội thi hành. (Chương trình bị lây nhiễm thường được gọi là *chương trình chủ* (host program)) Khi một virus thi hành, nó có thể chỉ đơn thuần nhân bản chính nó, hoặc cũng có thể nó sẽ ra tay phá hoại bằng cách thực hiện ngay một số hành động gây hại. Ngoài ra, một virus có thể được lập trình để được kích hoạt và thực hiện một hành động phá hoại tại một số thời điểm xác định trong tương lai, chẳng hạn vào một ngày cụ thể trong năm (ví dụ, virus *"Thứ Sáu ngày 13"*), hoặc tại thời điểm mà một số logic của chương trình chủ *(host program)* được kích hoạt. Một virus khác với một sâu máy tính. *Sâu máy tính*

worm) là một chương trình gieo rắc các bản sao của chính nó trên toàn bộ một mạng mà không cần tới một chương trình chủ. Một **Trojan horse** *(Ngựa thành Troa)* là một dạng thứ ba của các chương trình phá hoại. Trojan horse giống với sâu máy tính ở chỗ nó không cần một chương trình chủ để hoạt động, mà nó đội lốt một chương trình hợp pháp để che mắt người dùng. Các Trojan horse không thể tự nhân bản chính chúng. (Tuy nhiên, vẫn có thể có các ngoại lệ. Trước đây trên Internet đã từng có một chương trình Trojan horse giả dạng làm một tiện ích sao lưu dự phòng tự động. Khi được sử dụng, chương trình này sẽ tạo ra các bản sao dự phòng và nhân bản chính nó vào các bản sao dự phòng đó. Nó đã được lập trình để phá hoại nhiều hệ thống vào ngày thứ Sáu ngày 13 kế tiếp trong năm. Trong trường hợp này, ta cũng có thể xem nó là một virus do khả năng tự nhân bản của nó). Đôi khi một lỗi (*bug*) trong phần mềm trên máy PC cũng có thể gây ra các sự cố giống như các sự cố do virus, mặc dù không hề có sự dính dáng của virus.

Virus là dạng phổ biến nhất trong số ba dạng chương trình phá hoại. Một sâu máy tính hiếm khi được bắt gặp, ngoại trừ trên một mạng máy tính, nơi mà nó có thể gây ra các sự cố thông qua việc làm cho mạng bị quá tải khi nó tự nhân bản. Tác hại của các sâu máy tính chính là do sự hiện diện của chúng chứ không do một hành động phá hoại cụ thể, như một virus thường làm. Một sâu máy tính sẽ làm quá

tải bộ nhớ hoặc không gian đĩa cứng bằng cách lặp đi lặp lại hành động tự nhân bản và nó cần tới sự can thiệp của con người để có thể di chuyển từ máy tính này sang máy tính khác.

a) Nơi ẩn náu của các virus

Một chương trình được gọi là một virus vì (1) nó có một *"thời kỳ ủ bệnh"* (**incubation**: tức không phá hoại ngay lập tức), (2) nó có tính lây lan (**contagious**: tức có thể tự nhân bản) và (3) nó mang tính phá hoại. Các virus thường được lập trình để ẩn náu, nhằm tránh sự phát hiện của các phần mềm diệt virus. Một virus có thể ẩn náu theo bốn cách. Đôi khi một virus có thể đồng thời sử dụng nhiều hơn một phương thức ẩn náu.

Boot virus. Một *virus cung khởi động* (boot sector virus) là một virus ẩn náu trong chương trình cung khởi động *(boot sector program).* Trên một ổ đĩa cứng, nó có thể ẩn náu trong mã chương trình vốn là một phần của bản ghi khởi động chính *(master boot record),* hoặc trong chương trình bản ghi khởi động dùng để nạp hệ điều hành trên phân vùng tích cực của ổ đĩa cứng này. Trên một đĩa mềm, một virus cung khởi động ẩn náu trong chương trình khởi động của cung khởi động. Một trong những cách lan truyền phổ biến nhất của một virus là từ một đĩa mềm được sử dụng để khởi động một máy PC. Trong quá trình khởi động, khi chương trình khởi động được nạp vào bộ nhớ,

virus cũng sẽ được nạp theo và từ bộ nhớ nó có thể lây lan sang các chương trình khác.

Tuy nhiên, một đĩa mềm không có khả năng khởi động vẫn có thể lây nhiễm virus cho một máy tính. Như bạn đã biết, tất cả các đĩa mềm đều có một cung khởi động vốn chứa một chương trình khởi động. Khi một máy PC được định cấu hình để khởi động từ ổ đĩa A trước ổ đĩa C, nếu một đĩa mềm đang nằm trong ổ khi máy PC này khởi động, BIOS sẽ thi hành chương trình khởi động nằm trên đĩa mềm. Nếu đĩa này không có khả năng khởi động, chương trình khởi động sẽ hiển thị một thông điệp báo lỗi, chẳng hạn *"Nonsystem disk or disk error"*. Nếu sau đó đĩa mềm này được lấy ra khỏi ổ và người dùng nhấn vào một phím bất kỳ, máy PC sẽ khởi động từ ổ đĩa cứng. Tuy nhiên, nếu chương trình khởi động của đĩa mềm có chứa một virus cung khởi động, virus này có thể đã được nạp vào bộ nhớ. Khi hệ thống chuyển sang khởi động từ ổ đĩa cứng, virus này sẽ lây nhiễm vào cung khởi động của ổ đĩa cứng.

Để ngăn ngừa khả năng lây nhiễm này, bạn đừng nhấn một phím để ra lệnh máy PC chuyển sang khởi động từ ổ đĩa cứng, sau khi nó cố gắng khởi động không thành công từ đĩa mềm. Ngoài ra, việc nhấn tổ hợp phím **Ctrl+Alt+Del** có thể không đủ để ngăn ngừa sự lây nhiễm, vì virus được nạp có thể vẫn còn ẩn náu trong bộ nhớ và một số virus có khả năng chắn *(intercept)* tổ hợp **Ctrl+Alt+Del** để nắm quyền kiểm soát máy tính. Cách tốt nhất để

tiếp tục là sử dụng một thủ tục khởi động lạnh *(cold boot)*. Bạn hãy tắt nguồn máy PC, lấy đĩa mềm ra khỏi ổ, rồi bật máy PC lên trở lại. Nguy cơ lây nhiễm virus từ một đĩa mềm là lý do hợp lý để định cấu hình máy PC của bạn sao cho nó luôn khởi động từ ổ đĩa cứng trước, rồi kế đó, nếu ổ đĩa cứng không thể khởi động, mới chuyển sang khởi động từ ổ đĩa mềm. Thứ tự khởi động này thường sẽ ngăn cản BIOS đọc một cung khởi động của một đĩa mềm vốn được đặt trong ổ đĩa trong khi hệ thống khởi động. Bạn có thể chỉ định thứ tự khởi động trong CMOS setup.

Bạn cũng nên lưu ý rằng nhiều CMOS setup có một tùy chọn cho phép ngăn cản việc ghi vào cung khởi động của ổ đĩa cứng và điều này có thể ngăn cản một số, nhưng không phải là tất cả, virus cung khởi động. Tính năng này phải được tắt đi trước khi bạn cố gắng cài đặt Windows 9x hoặc Windows NT, vì cả hai đều sẽ phải ghi vào cung khởi động trong khi được cài đặt. Windows 9x sẽ không báo cho bạn biết rằng bạn phải tắt tính năng này đi trước khi bắt đầu công việc cài đặt, cho tới khi tiến trình cài đặt đã diễn ra được một nửa!

File virus. Một *virus tập tin* (file virus) ẩn náu trong một chương trình thi hành được (.exe hoặc .com) hoặc trong một tài liệu của chương trình xử lý từ có chứa một macro. Một *macro* là một chương trình nhỏ được chứa bên trong một tài liệu và có thể được tự động thi hành khi tài liệu này vừa được mở ra, hoặc có thể được thi

hành sau đó khi người dùng nhấn một phím nóng được định trước. Một ví dụ về một macro là một tính năng xử lý từ vốn tự động đọc ngày tháng hệ thống rồi sao chép nó vào một tài liệu mỗi khi tài liệu này được mở ra. Các virus ẩn náu trong các macro của các tập tin tài liệu được gọi là các *virus macro* (macro virus). Các virus macro là các virus lây lan thông qua e-mail nhiều nhất; chúng ẩn náu trong các macro được đính kèm với các tập tin tài liệu e-mail.

Ví dụ, virus *Melissa* là một virus macro nổi tiếng gần đây. Mellisa được đưa ra vào thứ Sáu ngày 26 tháng 3 năm 1999, trong một macro Word 97 và nó lập tức lan truyền khắp thế giới nội chỉ trong một ngày làm việc. E-mail ban đầu truyền bá Mellisa có dạng như sau:

> **From:** *(tên của người bị lây nhiễm)*
>
> **Subject: Important Message From** *(tên của người bị lây nhiễm)*
>
> **To:** *(50 tên từ một danh sách bí danh)*
>
> **Here is that document you asked for ... don't show any one else ;-)**
>
> **Attachment: LIST.DOC**

Khi người nhận mở tài liệu này ra, một macro nằm bên trong tài liệu sẽ được thi hành nó lập tức e-mail tài liệu LIST.DOC cho 50 địa chỉ e-mail được liệt kê trong sổ địa chỉ *(address book)* của người dùng. Virus này cũng lây nhiễm vào các tài liệu Word khác và do đó, khi

các tài liệu này được *e-mail*, chúng cũng sẽ tiếp tục truyền bá virus.

Mellisa hoạt động khi một tài liệu được mở ra tại một thời điểm mà vào lúc đó số phút của giờ trùng khớp với số ngày của tháng *(ví dụ, vào lúc 09:18 trong ngày thứ 18 của một tháng)*. Tại thời điểm này, Mellisa sẽ chèn vào tài liệu hiện hành một câu lấy ra từ *show* truyền hình Simpsons.

Một loại virus tập tin khác tìm kiếm trên một ổ đĩa cứng các tập tin có phần mở rộng là .exe, rồi tạo ra một tập tin khác có cùng tên, nhưng sử dụng phần mở rộng là .com, sau đó ẩn náu vào đó. Khi hệ điều hành thi hành một chương trình, trước hết nó sẽ tìm tên chương trình có phần mở rộng là .com. Lúc đó hệ điều hành sẽ tìm thấy virus này và thi hành nó. Virus được nạp vào bộ nhớ rồi nạp chương trình cùng tên với nó vốn có phần mở rộng là .exe. Người dùng thấy rằng mình đã kích hoạt đúng chương trình theo ý muốn. Lúc này virus tự do phá hoại hoặc lây nhiễm chính nó vào các chương trình khác.

Một virus không thể hoạt động nếu nó được chứa trong một tập tin dữ liệu không được nhúng kèm macro. Đôi khi một virus, do nhầm lẫn, sao chép chính nó vào một tập tin dữ liệu. Một khi virus đã ở đó, nó sẽ không còn có thể phá hoại được nữa, vì các dữ liệu không phải là một chương trình và do đó không thể được thi hành từ bộ nhớ. Sự hư hại khả dĩ duy nhất trong trường hợp này chính là các dữ liệu, vì

virus đã ghi đè lên các dữ liệu đã có sẵn trong tập tin dữ liệu.

Các virus đa phần. Một *virus đa phần* (multipartite) là một sự kết hợp gồm một virus cung khởi động và một virus tập tin. Nó có thể ẩn náu trong hai nơi này.

b) Các kỹ thuật ẩn náu

Một điều mà một virus được lập trình để thực hiện là ẩn náu nhằm tránh sự phát hiện của phần mềm diệt virus *(AV software)*. Phần mềm diệt virus chỉ có thể phát hiện các virus giống hệt hoặc tương tự với các virus mà nó đã được lập trình trước đó để tìm kiếm và nhận diện một virus mà nó biết là tồn tại bằng cách tìm kiếm các đặc điểm tiêu biểu của virus đó, vốn được gọi là dấu hiệu nhận dạng virus *(virus signature)*, và đây chính là lý do giải thích tại sao bạn cần phải cập nhật thường xuyên cho chương trình diệt virus của mình.

Phần mềm diệt virus không thể phát hiện một virus mà nó chưa biết cách tìm kiếm. Do đó, bạn nên nâng cấp phần mềm diệt virus của mình khi các virus mới được phát hiện.

Một virus có thể sử dụng một trong hai phương thức để lẩn tránh sự phát hiện của phần mềm diệt virus: (1) bằng cách thay đổi các đặc điểm tiêu biểu của nó *(tức thay đổi dấu*

hiệu nhận dạng) và (2) bằng cách cố gắng che đậy sự hiện diện của nó. Ba kiểu virus vốn được phân loại dựa theo các kỹ thuật đội lốt của chúng bao gồm virus đa hình, virus mã hóa và virus tàng hình.

Các virus đa hình. Một *virus đa hình* (polymorphic virus) sẽ thay đổi các đặc điểm tiêu biểu khi nó tự nhân bản. Sự biến hóa theo cách này khiến các phần mềm diệt virus khó phát hiện được sự hiện diện của virus.

Các virus mã hóa. Một dấu hiệu quan trọng mà phần mềm diệt virus thường tìm kiếm để phát hiện virus là khả năng tự nhân bản của một chương trình. Một *virus mã hóa* (encrypting virus) có thể biến đổi chính nó thành một chương trình không có khả năng nhân bản, nhằm tránh sự phát hiện. Tuy nhiên, nó buộc phải biến đổi trở lại thành một chương trình có khả năng nhân bản để có thể lan truyền hoặc nhân bản chính nó. Lúc này nó có thể bị phần mềm diệt virus phát hiện.

Các virus tàng hình. Một *virus tàng hình* (stealth virus) chủ động che giấu chính nó, bằng cách sử dụng một hoặc nhiều kỹ thuật như sau:

- Vì phần mềm diệt virus có thể phát hiện một virus bằng cách để ý sự khác biệt về kích thước tập tin của một chương trình trước khi bị virus lây nhiễm và sau khi bị lây nhiễm, nên virus tàng hình sẽ thay đổi các thông tin của hệ điều hành nhằm

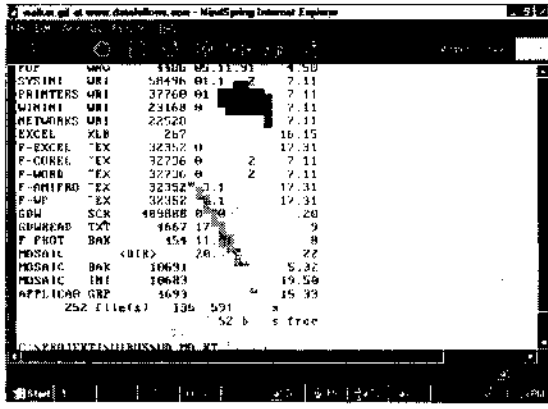
che đậy kích thước của tập tin mà nó đang ẩn náu trong đó.

- Virus tàng hình giám sát những khi các tập tin được mở ra hoặc đóng lại. Khi nó thấy rằng tập tin mà nó đang ẩn náu trong đó sắp được mở ra, nó sẽ tạm thời di chuyển bản thân ra khỏi tập tin này hoặc thay vào bằng *một bản sao vốn không chứa virus* của tập tin này. Virus tàng hình duy trì một bản sao của tập tin không bị lây nhiễm trên ổ đĩa cứng chỉ dành cho mục đích này.

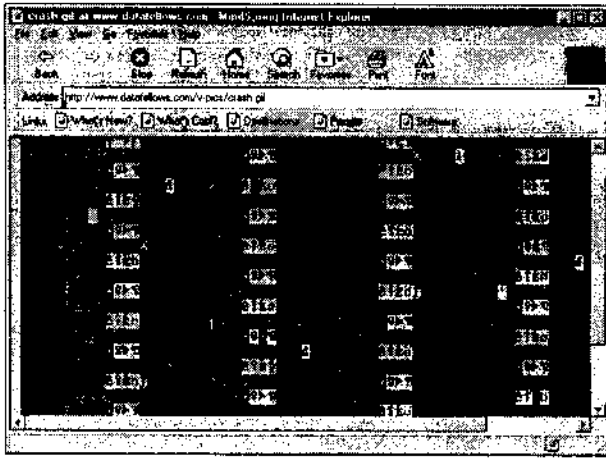
c) Các thiệt hại do một chương trình phá hoại gây ra

Hiện nay, vẫn chưa có virus, sâu máy tính hoặc Trojan horse nào phá hoại một ổ đĩa cứng hoặc các thiết bị phần cứng khác về mặt vật lý. Sự phá hoại do chúng thực hiện bao gồm từ rất nhẹ, chẳng hạn như hiển thị các con sâu bò quanh màn hình, cho tới hết sức nghiêm trọng, chẳng hạn như xóa toàn bộ những gì được ghi trên một ổ đĩa cứng. Hành động phá hoại do một chương trình phá hoại thực hiện được gọi là *payload* và có thể được thực hiện bằng một trong số nhiều cách khác nhau. Một virus có thể được lập trình để ra tay phá hoại chỉ khi một sự kiện khơi mào xảy ra, chẳng hạn như khi đến một ngày tháng nào đó, khi một tập tin được mở ra hoặc một phím nào đó được nhấn.

Hình 2-1 và hình 2-2 cho ta thấy kết quả của hai virus vô hại vốn chỉ hiển thị các rác rưởi trên màn hình.



Hình 2-1 Virus vô hại (lành tính) Walker hiển thị một người đi ngang qua màn hình.



Hình 2-2 Virus Crash có vẻ như mang tính phá hoại, khiến cho màn hình chỉ hiển thị rác rưởi, nhưng thực sự không gây hại cho các dữ liệu trên ổ đĩa cứng.

d) Cách lây lan của các chương trình phá hoại

Việc hiểu rõ về cơ chế lây lan của các chương trình phá hoại là một điều hết sức cần thiết để bạn hiểu được cách bảo vệ máy tính chống lại chúng. Một số máy tính gánh chịu nguy cơ nhiều hơn các máy khác, điều này phần lớn tùy thuộc vào các thói quen của người dùng. Sau đây là một danh sách gồm các hành động của người dùng có thể khiến một máy tính dễ bị lây nhiễm:

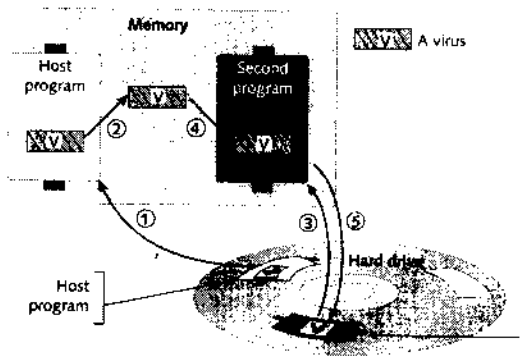
- Trao đổi các đĩa mềm chứa các tập tin chương trình.
- Nối kết máy tính vào một mạng không được bảo vệ.
- Mua phần mềm từ các nguồn không tin cậy.
- Nạp các chương trình xuống từ Internet.
- Sử dụng các đĩa mềm có nguồn gốc không rõ ràng.
- Sử dụng các chương trình mạng dùng chung.
- Sử dụng các đĩa mềm đã được sử dụng và được định dạng từ trước.
- Đọc các e-mail vốn tự động thi hành một trình xử lý từ để đọc các tập tin đính kèm.
- Không bảo vệ chống ghi cho các đĩa mềm chương trình gốc.

Cách nhân bản của một virus. Khi một chương trình có chứa một virus được sao chép vào máy PC của bạn, virus này chỉ có thể lan truyền chính nó khi chương trình bị lây nhiễm được thi hành. Tiến trình này được minh họa trong hình 2-3. Từ các tài liệu trước bạn đã biết rằng bước đầu tiên trong việc thi hành một chương trình, cho dù nó được lưu trữ trong một tập tin chương trình hoặc trong một cung khởi động, là nạp chương trình này vào bộ nhớ. Lúc đó virus ẩn náu trong chương trình sẽ được thi hành từ bộ nhớ. Một virus có thể là một *virus thường trú bộ nhớ* (memory-resident virus) sẽ ở yên trong bộ nhớ và hoạt động cho dù sau khi chương trình chủ đã được chấm dứt, hoặc có thể là một *virus không thường trú bộ nhớ* (non-memory-resident virus), có nghĩa là nó sẽ bị chấm dứt khi chương trình chủ được đóng lại.

Sau khi một virus được nạp vào bộ nhớ, nó sẽ tìm các chương trình khác đang được nạp vào trong bộ nhớ. Khi tìm thấy một chương trình trong bộ nhớ, virus sẽ sao chép chính nó vào chương trình này rồi sau đó là vào tập tin chương trình tương ứng nằm trên đĩa. Từ hình 2-3, bạn có thể thấy rằng một virus càng trở nên nguy hiểm hơn khi nó càng được ở lâu trong bộ nhớ và khi càng có nhiều chương trình được mở. Vì lý do này, nếu bạn sử dụng một máy tính vừa được một người khác sử dụng, chẳng hạn như một máy tính trong phòng lab, bạn nhớ luôn khởi động lại máy tính này trước khi làm việc để

xóa sạch các chương trình ra khỏi bộ nhớ. Hãy sử dụng một thủ tục khởi động cứng *(khởi động lạnh)* để bảo đảm rằng tất cả các chương trình thường trú bộ nhớ *(bao gồm cả một virus thường trú bộ nhớ)* đều được xóa sạch khỏi bộ nhớ.

Khi sử dụng máy tính trong phòng lab, bạn hãy nhớ luôn khởi động cứng cho máy PC này trước khi bắt đầu làm việc, nhằm ngăn ngừa các virus.



① Chương trình chính được copy vào bộ nhớ
② Virus có thể hoặc không tự nó di chuyển vào vùng mới trong bộ nhớ
③ Một chương trình thứ 2 có thể được lấy ra và copy vào bộ nhớ
④ Những virus có thể tự nhân bản để thâm nhập vào bộ nhớ
⑤ Một chương trình mới lây lan xâm nhập vào đĩa cứng

Hình 2-3 Cách nhân bản của một virus.

Cách Trojan horse vào được máy tính của bạn. Trojan horse là một chương trình phá hoại giả dạng làm một chương trình hợp pháp.

Một ví dụ lý thú về một Trojan horse là chương trình AOL4FREE. Ban đầu chương trình này là một chương trình bất hợp pháp dùng để cung cấp khả năng truy xuất trái phép vào mạng *American Online* (AOL). Sau khi sự hữu ích của chương trình này bị AOL ngăn chặn, một chương trình mới đã xuất hiện và cũng tự nhận là AOL4FREE, nó hoàn toàn không phải là một chương trình truy xuất trực tuyến, mà là một Trojan horse mang tính chất phá hoại. Mọi người truyền cho nhau chương trình này và nghĩ rằng nó sẽ cung cấp khả năng truy xuất trái phép vào AOL. Tuy nhiên, nếu được thi hành, chương trình này thực sự sẽ xóa các tập tin trên các ổ đĩa cứng của họ.

Các trò đánh lừa virus. Một *trò đánh lừa virus* (virus hoax) là một lá thư hoặc một e-mail cảnh báo về một virus không tồn tại. Bản thân cảnh báo này là một hình thức phá hoại vì nó làm quá tải sự lưu thông trên mạng. Sau đây là một ví dụ về một e-mail đánh lừa mà chúng tôi đã nhận được:

There is a new virus going around in the last couple of days!! DO NOT open or even look at any mail that you get that say: "Returned of Unable to Deliver". The virus will erase your whole hard drive and attach itself to your computer components and render them useless. Immediately delete any mail items that say this. AOL has indicated this is a very dangerous virus, and there is NO remedy for it at this item. Please

e careful and forward to all your online friends SAP. This is a new a-mail virus and not a lot of eople know about it; just let everyone know, so hey won't be a victim. Please forward this e-nail to your friends!!!

Trước hết, bạn đừng tin vào đoạn nói về một irus có khả năng khiến cho các bộ phận máy nh trở thành vô dụng. Cho đến nay chưa ai phát iện thấy một virus nào thực sự phá hoại phần ứng về mặt vật lý, mặc dù các virus có thể khiến một máy tính trở nên vô dụng bằng cách phá hủy các chương trình hoặc các dữ liệu. Điều thứ hai, bạn đừng tin vào đoạn nói rằng virus này sẽ được kích hoạt chỉ vì bạn mở một thông điệp e-mail ra. Một thông điệp e-mail là một văn bản (*text*) chứ không phải là một chương trình và một virus không thể ẩn náu trong đó. *(Tuy nhiên, virus có thể ẩn náu trong các tài liệu của chương trình soạn thảo văn bản có chứa các macro vốn được đính kèm theo một thông điệp e-mail).* Điều thứ ba, bạn đừng quá cả tin mà gửi thông điệp này tới một người khác. Sự nguy hại tiềm tàng của một trò đánh lừa virus, như nó có thể, là làm quá tải một hệ thống e-mail bằng lưu lượng dữ liệu vô dụng. Khi chúng tôi nhận được e-mail này, đã có một trăm người trong danh sách phân phối.

2. BẢO VỆ MÁY TÍNH TRƯỚC CÁC HÌNH THỨC PHÁ HOẠI

Có rất nhiều điều bạn có thể làm để bảo vệ máy tính của mình chống lại các virus và các hình thức phá hoại khác. Tuyến phòng ngự đầu tiên của bạn là thường xuyên tạo ra các bản sao dự phòng và sử dụng phần mềm diệt virus. Sau đó, bạn hãy quản lý các chương trình một cách khôn ngoan. Sau đây là một số hướng dẫn tổng quát:

- Mua phần mềm diệt virus và đặt cho máy tính của bạn tự động chạy chương trình diệt virus khi khởi động.
- Cập nhật thường xuyên cho phần mềm diệt virus bằng cách định kỳ nạp bản nâng cấp xuống từ Internet.
- Đặt cho một chương trình quét virus tự động quét các tài liệu của chương trình xử lý từ khi chúng được mở ra.
- Lập và thi hành đúng theo một kế hoạch tạo các bản sao dự phòng của ổ đĩa cứng theo lịch trình, để đề phòng sự thiệt hại do một hình thức phá hoại gây ra.
- Chỉ mua phần mềm từ một cửa hàng đáng tin cậy.
- Không trao đổi các tập tin chương trình trên các đĩa mềm.

- Không sử dụng các đĩa mềm có nguồn gốc không rõ ràng và luôn quét virus trên các đĩa mềm bất kể nguồn gốc của chúng.
- Hạn chế nạp các phần mềm xuống từ Internet và sau đó luôn quét các tập tin chương trình để tìm virus trước khi thi hành chúng.
- Không bao giờ sử dụng phần mềm sao chép bất hợp pháp (!).
- Định dạng các đĩa mềm trước khi sử dụng.
- Đặt bảo vệ chống ghi cho các đĩa mềm chứa các chương trình gốc.
- Trong một môi trường kinh doanh, tuân thủ chặt chẽ theo các chính sách của công ty chống lại việc sử dụng các phần mềm không được phép.
- Nếu bạn tìm thấy một máy tính đã được bật sẵn bởi những người đã sử dụng trước đó, hãy khởi động cứng cho máy PC này trước khi sử dụng.
- Đặt các xác lập CMOS setup để khởi động theo trình tự trước hết là ổ đĩa C, rồi sau đó mới tới ổ đĩa A.
- Bật tính năng ngăn ngừa virus cho MBR của bạn trong CMOS setup, nếu được hỗ trợ.

a) Các triệu chứng virus

Bạn cần biết rõ những dấu hiệu cho thấy một virus đang tự nhân bản hoặc đang thực hiện công việc phá hoại. Sau đây là một số dấu hiệu cảnh báo cho thấy rằng có thể có một virus đang hoạt động:

- Một chương trình mất nhiều thời gian hơn để nạp so với bình thường.
- Tần suất và thời gian truy xuất đĩa dường như quá mức đối với các tác vụ đơn giản.
- Các thông điệp báo lỗi bất thường xảy ra đều đặn.
- Bộ nhớ khả dụng còn ít hơn bình thường.
- Các tập tin biến mất hoặc xuất hiện một cách bí ẩn.
- Các hình ảnh kỳ lạ xuất hiện trên monitor, hoặc máy tính phát ra các tiếng ồn lạ tai.
- Không gian đĩa cứng bị thu hẹp lại thấy rõ.
- Hệ thống không thể nhận diện ổ đĩa cứng khi bạn đã khởi động từ một đĩa mềm.
- Hệ thống không thể nhận diện ổ đĩa CD-ROM, mặc dù trước đó nó vẫn hoạt động bình thường.

- Các tập tin thi hành được *(executable file)* thay đổi kích thước.
- Các tập tin thi hành được vốn trước đây hoạt động bình thường, nhưng giờ đây không hoạt động nữa và đưa ra các thông điệp báo lỗi bất ngờ.
- Các đèn báo truy xuất trên ổ đĩa cứng và ổ đĩa mềm bật sáng khi không có bất kỳ hành động nào trên các thiết bị này. *(Tuy nhiên, đôi khi hệ điều hành có thể sẽ thực hiện công việc bảo dưỡng thường lệ sau khi hệ thống vô công một thời gian).*
- Các tập tin liên tục bị hư hại.
- Các thông điệp báo lỗi kỳ lạ xuất hiện trên màn hình.
- Các thông điệp báo lỗi của DOS và Windows về bảng FAT hoặc bảng phân vùng được hiển thị.
- Ổ đĩa cứng đang khởi động bỗng nhiên bị treo trước khi đi vào một dấu nhắc DOS hoặc chế độ Safe Mode của Windows 9x.
- Các phần mở rộng tập tin hoặc các thuộc tính tập tin thay đổi mà không có lý do.
- Một thông điệp được hiển thị từ chương trình quét virus.

- Số lượng các cung bị hư hại vật lý *(bad sector)* trên ổ đĩa cứng liên tục gia tăng.
- Lệnh MEM của DOS cho thấy các TSR *(chương trình thường trú)* xa lạ được nạp vào bộ nhớ.

b) Những điều cần làm khi bạn nghi ngờ một sự phá hoại do virus

Nếu nghi ngờ rằng một virus đang hiện diện, bạn hãy chạy một chương trình quét virus để phát hiện và xóa virus này. Nếu phần mềm diệt virus chưa được cài đặt, bạn vẫn có thể sử dụng nó. Bạn hãy tham khảo tài liệu để biết cách tiếp tục. Trong nhiều trường hợp, tiến trình cài đặt sẽ phát hiện ra virus này và tiêu diệt nó trước khi tiếp tục công việc cài đặt. Tuy nhiên, một virus có thể vẫn hiện diện trong hệ thống cho dù phần mềm diệt virus báo rằng không phát hiện ra virus nào. Khả năng này có thể xảy ra vì virus này không được phần mềm diệt virus biết tới, hoặc vì nó đã lẩn trốn một cách thành công khỏi sự phát hiện của chương trình diệt virus. Nếu phần mềm diệt virus không tìm thấy gì, nhưng bạn vẫn nghi ngờ rằng có sự hiện diện của một virus, bạn hãy tìm bản nâng cấp mới nhất cho phần mềm diệt virus của mình và thử sử dụng nó, hoặc thử sử dụng một chương trình diệt virus khác.

c) Phòng chống virus

Các phần mềm diệt virus không thể ngăn cản không cho một chương trình Trojan horse được sao chép vào máy tính của bạn, báo cho bạn biết rằng một thông điệp e-mail là một trò đánh lừa, hoặc ép buộc bạn quản lý các phần mềm một cách khôn ngoan. Tuy nhiên, ngoài việc chú trọng tới các biện pháp ngăn ngừa một virus xâm nhập vào hệ thống của bạn, việc sử dụng phần mềm diệt virus là phòng tuyến tốt nhất giúp bạn chống lại các virus. Một số phần mềm diệt virus nổi tiếng được liệt kê trong bảng 3.

Bảng 3 **Một số phần mềm diệt virus.**

Tên phần mềm	Web site
Noton AntiVirus của Symantec Corporation	Www.symantec.com
Dr.Solomon's Software	Www.drsolomon.com
McAfee VirusScan của McAfee Associates, Inc.	www.mcafee.com
eSafe của Aladdin Knowledge Systems, Ltd.	www.esafe.com
F-PROT của FRISK Software International	www.complex.is
Command AntiVirus của Command Software Systems	www.commandcom.com

Khi lựa chọn phần mềm diệt virus, bạn cần tìm những tính năng sau:

- Khả năng nạp các bản nâng cấp phần mềm mới từ Internet, để khi các virus mới xuất hiện, phần mềm của bạn biết cách phát hiện và tiêu diệt chúng.
- Khả năng tự động thi hành khi hệ thống khởi động.
- Khả năng phát hiện các macro trong một tài liệu của chương trình xử lý từ khi tài liệu này được nạp bởi trình xử lý từ.
- Khả năng tự động giám sát các tập tin đang được nạp xuống từ Internet.

d) Sử dụng phần mềm diệt virus

Phần mềm diệt virus có thể hoạt động tại những thời điểm khác nhau để quét ổ đĩa cứng hoặc một đĩa mềm của bạn nhằm tìm virus. Hầu hết các phần mềm diệt virus đều có thể được định cấu hình để quét bộ nhớ và cung khởi động của ổ đĩa cứng của bạn mỗi khi máy PC được bật lên. Đôi khi sẽ không thực tế nếu ta để chúng quét toàn bộ ổ đĩa cứng mỗi lần hệ thống khởi động, vì công việc này mất quá nhiều thời gian. Bạn có thể cân nhắc đến việc lập lịch trình *(schedule)* để phần mềm diệt virus hoạt động tại cùng một thời điểm mỗi ngày, chẳng hạn vào giờ nghỉ trưa.

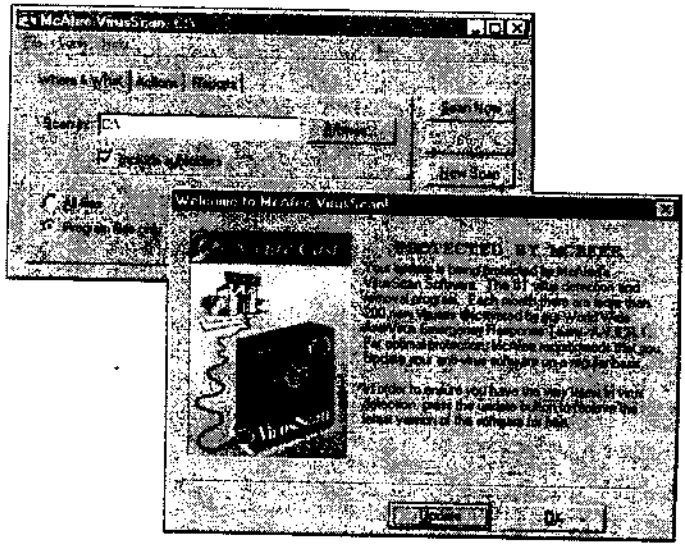
Một số phần mềm diệt virus có thể được đặt để hoạt động liên tục trong chế độ nền

(background) và quét tất cả các chương trình đang được thi hành. Tuy nhiên, phần mềm này có thể gây ra các sự cố cho các phần mềm khác, đặc biệt là trong khi thực hiện các công việc cài đặt. Nếu gặp sự cố khi cài đặt một ứng dụng mới, bạn hãy thử đóng chương trình diệt virus lại trong khi thực hiện công việc cài đặt này.

Bạn cần bảo đảm chắc rằng phần mềm diệt virus của mình có khả năng quét các tập tin khi chúng được nạp xuống từ Internet hoặc từ một mạng, và khả năng quét các tài liệu để tìm các virus macro mỗi khi các tài liệu này được mở ra bởi một chương trình xử lý từ. Phần mềm diệt virus của bạn cũng cần có khả năng quét các tập tin và các cung khởi động của các ổ đĩa cứng và các đĩa mềm. Một phiên bản của phần mềm *McAfee VirusScan* được kèm theo cùng với phần mềm Nuts & Bolts. Khi sử dụng phần mềm này, bạn làm theo các hướng dẫn sau để quét virus cho một ổ đĩa cứng:

1. Đối với Windows 9x, bạn nhấn nút **Start → Programs → Nuts & Bolts → McAfee VirusScan** rồi *chọn* **McAfee VirusScan** từ menu con của phần mềm diệt virus này.
2. Khi phần mềm bắt đầu thi hành, nó sẽ cung cấp cho bạn tùy chọn đăng nhập vào Website của McAfee và nạp xuống bất kỳ bản nâng cấp nào cho phần mềm này *(xem hình 2-4)*. Bạn phải nối kết vào Internet

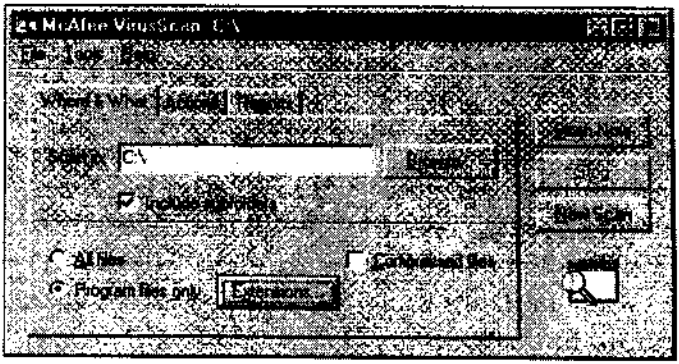
trước khi nhấn nút **Update** để thực hiện công việc nạp xuống.



Hình 2-4 McAfee VirusScan cho phép bạn cập nhật chính nó từ Web site của McAfee nhằm bảo đảm khả năng bảo vệ chống lại các virus mới được phát hiện.

1. Kế đó cửa sổ *McAfee VirusScan* sẽ xuất hiện *(xem hình 2-5)*. Bạn có thể chọn ổ đĩa cần quét, những gì cần làm khi một virus được phát hiện, những báo cáo nào cần được tạo ra và những kiểu tập tin và những vị trí nào cần quét.
2. Sau khi bạn đã thực hiện xong các lựa chọn của mình, bạn nhấn nút **Scan Now** để bắt đầu quét.

3. Bất kỳ virus nào được phát hiện sẽ được liệt kê trong hộp danh sách nằm ở đáy cửa sổ *McAfee VirusScan*.



Hình 2-5 Phần mềm McAfee VirusScan sẵn sàng để thực hiện công việc quét virus.

3 Những điều cần biết về sao lưu dự phòng và kháng lỗi

Chính sự nguy hiểm của các virus khiến chúng ta càng nhận thức rõ hơn về tầm quan trọng của các bản sao dự phòng ổ đĩa cứng và các phương thức bảo vệ dữ liệu khác. Đối với các dữ liệu, các phần mềm, nguyên tắc chung là: nếu bạn không thể thiếu chúng được, hãy sao lưu chúng. Trong phần này chúng ta sẽ xem xét các phần mềm và phần cứng cần thiết để tạo các bản sao dự phòng của các phần mềm và các dữ liệu từ một ổ đĩa cứng. Windows 9x và Windows NT đều cung cấp các công cụ sao lưu và chúng cũng sẽ được chúng ta tìm hiểu trong phần này. Một tác vụ không thể thiếu được trong công tác bảo dưỡng phòng ngừa là nâng cao tính kháng lỗi cho các ổ đĩa cứng. *Tính kháng lỗi* (fault tolerance) là khả năng của một máy tính đáp ứng trước một lỗi hoặc một sự kiện trầm trọng, chẳng hạn như ổ đĩa cứng bị hư hỏng hoặc nguồn điện bị mất, tính năng này có thể giữ được các dữ liệu không bị mất. Nhiều cách tiếp cận để nâng cao tính kháng lỗi cho các ổ đĩa cứng được gọi chung là **RAID**. Thuật ngữ này ban đầu viết tắt cho cụm từ **redundant array of inexpensive disks** (mảng

thừa gồm các đĩa rẻ tiền), nhưng gần đây đã được cập nhật để mang ý nghĩa là **redundant array of independent disks** (mảng thừa gồm *các* đĩa độc lập). Các phương thức RAID khác nhau cũng sẽ được đề cập tới trong phần này.

1. PHẦN CỨNG SAO LƯU

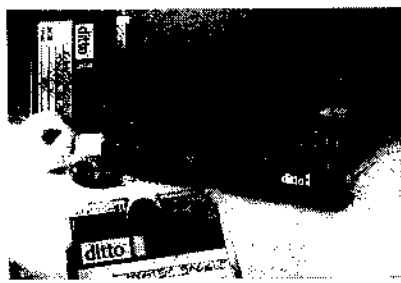
Các thiết bị phần cứng được sử dụng phổ biến để tạo các bản sao dự phòng đĩa cứng trên các máy tính cá nhân độc lập hoặc các máy phục vụ cỡ nhỏ bao gồm các ổ băng từ *(tape drive)*, các ổ Zip, các ổ Jaz và các CD-ROM đọc/ghi. Tuy nhiên, trong một môi trường kinh doanh, nếu một máy PC được nối kết tới một máy phục vụ tập tin, cách tiếp cận sao lưu thực tế nhất là sao lưu các dữ liệu từ ổ đĩa cứng của máy PC tới máy chủ *(File Server)*. Các dữ liệu trên cả máy PC lẫn trên máy chủ *(File Server)* đều có thể trở nên bị hư hại. Tuy nhiên, máy chủ *(File Server)* có thể có riêng một tiện ích sao lưu tự động dùng để sao lưu vào băng từ hoặc một máy mainframe lớn hơn.

Bất kể phương tiện sao lưu của bạn là gì, thực tế nhất vẫn là chỉ sao lưu các dữ liệu mà không sao lưu các phần mềm một cách đều đặn. Bạn có thể chọn sao lưu phần mềm một lần duy nhất ngay sau khi cài đặt nó. Sau này, nếu phần mềm trở nên bị hư hại, nó có thể được cài đặt lại.

Phần này trước hết sẽ đề cập tới việc sử dụng các ổ băng từ, sau đó là các ổ đĩa tháo lắp cho các công việc sao lưu.

a) Các ổ băng từ

Các *ổ băng từ* (tape drive, xem hình 3-1) là một cách rẻ tiền nhất để sao lưu toàn bộ một ổ đĩa cứng hoặc các phần của nó. Đối với công việc sao lưu, các ổ băng từ tiện lợi hơn so với các đĩa mềm hay các kiểu đĩa tháo lắp khác và chúng tương đối rẻ tiền. Các băng từ có thể có dung lượng từ vài trăm KB tới vài GB, chúng bao gồm nhiều kiểu và nhiều định dạng *(format)*. Mặc dù ổ băng từ không đòi hỏi bạn phải sử dụng phần mềm sao lưu đặc biệt để quản lý chúng, nhưng trong đa số trường hợp, bạn sẽ muốn đầu tư vào một phần mềm sao lưu chuyên dụng để quản lý chúng nhằm có thể tạo ra các bản sao lưu một cách hiệu quả và ít tốn công sức nhất. Các ổ băng từ và các băng từ có rất nhiều kiểu, tiêu chuẩn đa dạng. Một số kiểu và tiêu chuẩn thông dụng hơn sẽ được chúng ta tìm hiểu trong phần này.



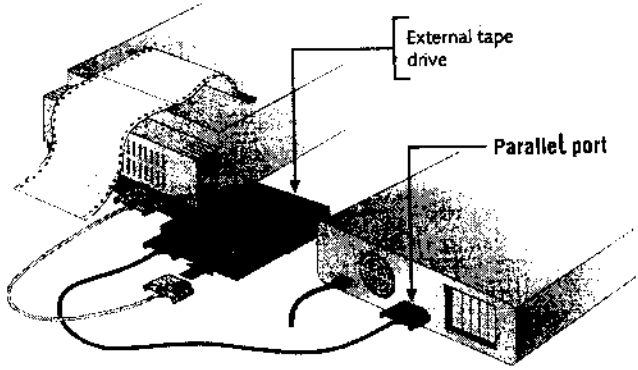
Hình 3-1 Một hệ thống ổ băng từ.

Nhược điểm lớn nhất của các ổ băng từ là các dữ liệu được lưu trữ trên băng từ theo kiểu *truy xuất tuần tự* (sequential access), có nghĩa là, để đọc dữ liệu từ bất kỳ nơi nào trên băng từ, bạn buộc phải bắt đầu từ phần đầu của băng từ rồi đọc cho tới khi bắt gặp các dữ liệu cần tìm. Tính chất truy xuất tuần tự khiến cho việc phục hồi các tập tin trở nên chậm chạp và bất tiện, đây chính là lý do giải thích tại sao các băng từ không được sử dụng cho mục đích lưu trữ dữ liệu đa năng.

Cách thức giao tiếp của ổ băng từ với máy tính. Ổ băng từ có thể thuộc loại lắp trong *(internal)* hoặc loại lắp ngoài *(external)*. Ổ băng từ lắp ngoài đắt tiền hơn, nhưng có thể được sử dụng cho nhiều máy tính. Ổ băng từ có thể giao tiếp với máy tính theo các cách sau:

- Ổ băng từ lắp ngoài có thể sử dụng cổng song song *(xem hình 3-2)* kèm theo một cổng nối thông *(pass-through)* tùy chọn tới máy in *(để ổ băng và máy in có thể sử dụng chung cổng song song)*.
- Ổ băng từ lắp trong hoặc lắp ngoài có thể sử dụng một bus SCSI. Phương thức này đem lại kết quả tốt nếu ổ băng từ và ổ đĩa cứng nằm trên cùng bus SCSI, trong đó chứa lối thông dữ liệu chỉ đối với hệ thống SCSI này.
- Ổ băng từ lắp trong hoặc lắp ngoài có thể sử dụng card kiểm soát độc quyền của riêng chúng.

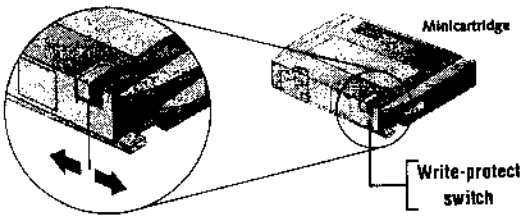
- Ổ băng từ lắp trong hoặc lắp ngoài có thể sử dụng bộ kiểm soát đĩa mềm.



Hình 3-2 Ổ băng từ lắp ngoài có thể sử dụng cổng song song cho xuất/nhập, kèm theo một cổng nối thông tùy chọn tới máy in.

Các băng từ được sử dụng cho ổ băng từ

Các ổ băng từ thích nghi với một trong hai loại băng từ: các *data cartridge* có kích thước 4×6×5/8 inch và các *minicartridge* nhỏ hơn, giống như băng từ trong hình 3-3, có kích thước 3¼×2½×3/8 inch. Trong hai loại này, các minicartridge được sử dụng phổ biến hơn vì các ổ băng của chúng có thể lắp vừa vào một hộc 5½ inch của khung máy PC.



Hình 3-3 Minicatridge dành cho ổ băng từ có một nút gạt bảo vệ chống ghi.

Công nghệ được các ổ băng từ sử dụng để ghi vào các băng từ tương tự như các công nghệ được các ổ đĩa mềm sử dụng (xem tài liệu *"Các ổ đĩa mềm"*). Tại phần đầu của băng từ có một bảng FAT giám sát vị trí của các dữ liệu và các cung bị hư hại trên băng từ này. Băng từ phải được định dạng trước khi bạn có thể ghi các dữ liệu lên nó. Nhiều băng từ được định dạng sẵn từ nhà máy. Bạn hãy mua các băng từ loại này để không phải mất thời gian định dạng cho chúng.

Các tiêu chuẩn dành cho việc ghi dữ liệu vào băng từ chưa phát triển như người sử dụng mong đợi và điều này khiến chúng ta phải cẩn thận chọn lựa kiểu băng từ thích hợp với các ổ băng từ khi mua và sử dụng chúng. Có nhiều tiêu chuẩn được đề ra bởi các tổ chức hoặc các hãng sản xuất khác nhau. Hình 3-4 bao gồm hai bảng, mỗi bảng lấy từ một hãng sản xuất ổ băng từ khác nhau và cho ta thấy các định dạng băng từ và các kiểu băng từ được hỗ trợ bởi mỗi ổ băng từ trong số các ổ băng từ của họ. Hình 3-4a cho thấy rằng ổ băng Ditto 2-GB có thể ghi bằng cách chỉ sử dụng phương thức 2-GB, nhưng có thể đọc các băng từ bằng các phương thức khác nhau. Hình 3-4b cho thấy rằng ổ băng từ dành cho minicartridge Eagle TR-3 có thể sử dụng định dạng QIC-3010 hoặc QIC-3020 và năm kiểu băng từ. Lưu ý rằng các ổ băng này thường cũng có khả năng đọc các

định dạng khác vốn tương thích với các định dạng được liệt kê.

Capacity	Tape Format	Tape Type	Read	Write
2GB	Ditto 2BG	Ditto 2BG	YES	YES
2GB	QIC-3020 Travan	TR-3	YES	NO
2GB	QIC-3020 Wide	3020XLF	YES	NO
2GB	QIC-3020	3020XL	YES	NO
2GB	QIC-80 Travan	TR-1	YES	NO
2GB	QIC-80 Wide	5122	YES	NO
2GB	QIC-80 XL	2120XL	YES	NO
2GB	QIC-80	2080 or 2120	YES	NO
2GB	Irwin 40 and 80	2000	YES	NO

a) Tape compatibility for the Ditto 2GB tape drive

Tape Format	Tape Types				
	Travan TR-3	QIC Wide	MC 3000XL	TR-3 EXtra	MC 3020 EXtra
QIC-3020*	3.2GB	1.7GB	1.4GB	4.4GB	3.2GB
QIC-3020	1.6GB	850MB	680MB	2.2GB	1.6GB
QIC-3010*	1.6GB	840MB	680MB	2.2GB	1.6GB
QIC-3010	800MB	420MB	340MB	1.1GB	800MB

* Using software compression with an assumed 2:1 compression ratio

b) Miniçartridge capacities obtained by the Eagle TR-3 tape drive using five different

Hình 3-4 Các băng từ của hai hãng sản xuất băng từ cho ta thấy vô số định dạng được sử dụng khi đọc và ghi vào các băng từ.

Các định dạng băng từ và các kiểu băng từ. Một trong số những nỗ lực đầu tiên để chuẩn hóa cách thức ghi dữ liệu vào băng từ đã được thiết lập khoảng năm 1993 bởi một nhóm gồm các nhà sản xuất hợp thành tổ chức Quarter-Inch Cartridge Drive Standards, Inc. Các tiêu chuẩn này được gọi là các tiêu chuẩn **QIC** (**Q**uarter-**I**nch **C**ommittee), hay các tiêu chuẩn Quarter-Inch Cartridge. Đã có rất nhiều

tiêu chuẩn QIC được phát triển, nhưng chỉ có một vài tiêu chuẩn còn được sử dụng ngày nay. Hãng 3M đã phát triển một tiêu chuẩn có tên gọi là *Travan*, dựa trên định dạng QIC. Travan là một tiêu chuẩn được hậu thuẫn bởi nhiều hãng sản xuất hàng đầu trong lĩnh vực sản xuất ổ băng từ. Các tiêu chuẩn Travan có nhiều cấp độ khác nhau và được đặt tên lần lượt từ TR-1 tới TR-4, mỗi cấp độ đều dựa trên một tiêu chuẩn QIC khác nhau.

Khi quan sát cột thứ ba của hình 3-4a, nơi cho thấy các kiểu băng từ và các tiêu đề cột của hình 3-4b, bạn có thể thấy rằng có nhiều kiểu băng từ được sử dụng. Tuy hầu hết các hãng sản xuất đều đề nghị rằng bạn nên sử dụng một cartridge băng từ do họ chế tạo cho ổ đĩa của họ, nhưng đôi khi các ổ băng từ có thể hỗ trợ nhiều kiểu băng từ khác nhau. Mặc dù một ổ băng từ có thể sử dụng một minicartridge thay vì một data cartridge, nhưng không phải là tất cả các băng từ minicartridge đều có thể được sử dụng với bất kỳ ổ băng nào. Bạn có thể tham khảo tài liệu hướng dẫn dành cho ổ băng từ để biết những loại băng từ nào bạn có thể sử dụng với ổ băng của mình. Các ổ băng từ minicartridge sử dụng nhiều hơn một kiểu cơ cấu băng từ và nhiều hơn một mật độ được sử dụng để ghi dữ liệu vào một băng từ *(giống như có nhiều hơn một mật độ dành cho các đĩa mềm)*. Ngoài ra, một số ổ băng từ không thể định dạng các băng từ, có nghĩa là

bạn phải mua các băng từ được định dạng sẵn để có thể sử dụng với ổ băng này.

b) Hướng dẫn giải quyết các sự cố ổ băng từ

Sau đây là một danh sách gồm các sự cố ổ băng từ mà bạn có thể gặp phải, kèm theo đó là các đề nghị cách thức giải quyết chúng:

Một minicartridge không hoạt động

- Nếu bạn đang cố gắng ghi dữ liệu, bạn hãy xác nhận rằng minicartridge này đã được đặt cho phép ghi.
- Bạn đã lắp minicartridge vào ổ băng đúng cách chưa? *(Xem tài liệu hướng dẫn).*
- Kiểm tra để chắc rằng bạn đang sử dụng kiểu minicartridge phù hợp (*Xem tài liệu hướng dẫn*).
- Minicartridge này đã được định dạng chưa? Công việc định dạng được thực hiện bởi phần mềm và có thể mất một giờ hoặc hơn.
- Làm căng dây băng. Bạn hãy sử dụng phần mềm sao lưu dữ liệu để thực hiện điều này. Một số ổ băng từ đòi hỏi điều này, nhưng một số ổ băng khác không cần. Công việc *làm căng dây băng* (retensioning) sẽ quay tới và quay lui băng để loại trừ các chỗ bị chùng trên băng từ.

- Lấy minicartridge ra và khởi động lại, sau đó thử lại minicartridge này một lần nữa.
- Thử sử dụng một minicartridge mới. Minicartridge cũ có thể đã mòn.
- Giống như với các đĩa mềm, nếu băng từ được lấy ra khỏi ổ băng trong khi đèn báo ổ băng vẫn đang cháy sáng, các dữ liệu đang được ghi vào thời điểm đó có thể sẽ không đọc được.

Tốc độ vận chuyển dữ liệu chậm

- Phần mềm băng từ có một tùy chọn dành cho tối ưu tốc độ hoặc nén dữ liệu không ? Bạn hãy thử bật một tùy chọn lên, sau đó đến tùy chọn kia, tắt và bật lên trở lại.
- Một số ổ băng từ có thể sử dụng một card tăng tốc để đẩy mạnh tốc độ vận chuyển dữ liệu. Bạn hãy xem lại tài liệu hướng dẫn sử dụng dành cho ổ băng này.
- Thử một minicartridge mới.
- Nếu ổ băng từ có thể hỗ trợ, bạn hãy xóa toàn bộ băng từ rồi định dạng nó lại. Hãy bảo đảm rằng ổ băng từ có khả năng thực hiện thủ tục này trước khi bạn ra lệnh cho phần mềm thực hiện.

- Nếu bạn đã cài đặt một card tăng tốc, bạn hãy xác nhận rằng card này được nối tới ổ băng từ.
- Kiểm tra xem phần mềm băng từ có đủ bộ nhớ để hoạt động không.

Ổ băng không hoạt động sau khi được lắp đặt

- Kiểm tra để chắc rằng chân số 1 được canh chiều đúng với sợi cáp dữ liệu ở cả hai đầu.
- Kiểm tra xem có sự xung đột tài nguyên hay không. Ổ băng từ thường đòi hỏi một IRQ, kênh DMA và địa chỉ I/O.
- Đối với DOS, bạn hãy kiểm tra lại các khoản mục trong các tập tin AUTOEXEC.BAT và CONFIG.SYS.

Ổ băng bị trục trặc không thường xuyên hoặc đưa ra các lỗi

- Băng từ có lẽ đã bị hao mòn. Bạn hãy thử một băng từ mới.
- Chùi đầu đọc/ghi của ổ băng từ *(xem tài liệu hướng dẫn sử dụng để biết cách thực hiện).*
- Đối với một ổ băng từ lắp ngoài, bạn hãy dời ổ đĩa này càng xa monitor và khung máy càng tốt.
- Định dạng lại băng từ.
- Làm căng dây băng.

- Xác nhận rằng bạn đang sử dụng kiểu băng từ và định dạng băng từ thích hợp.

c) Các ổ đĩa tháo lắp

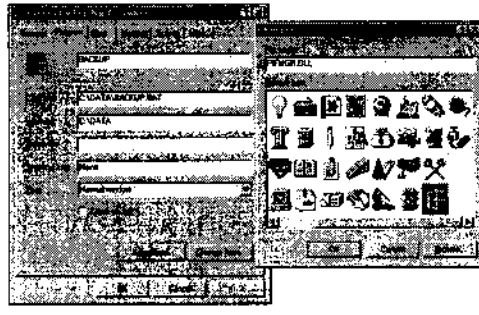
Các phương tiện mới chẳng hạn như các CD read-writable hoặc các ổ Jaz đang ngày càng được sử dụng nhiều hơn cho công việc sao lưu dự phòng, vì chúng còn có thể được sử dụng cho các mục đích khác và vì giá cả của chúng hiện nay đã giảm khá nhiều. Như đã được giới thiệu trong tài liệu *"Các khái niệm cơ bản về ổ đĩa cứng"*, các ổ đĩa Zip được bán ra với các dung lượng 100MB hoặc 250MB. SuperDisk có thể lưu giữ 120MB dữ liệu và các ổ đĩa Jaz có thể chứa 1GB hoặc 2GB dữ liệu. Các ổ đĩa tháo lắp này hết sức lý tưởng cho công việc sao lưu dự phòng với điều kiện là các dữ liệu chứa vừa trên một đĩa. Khi các dữ liệu có thể chứa vừa trên một đĩa tháo lắp đơn, một phương thức nhanh chóng và dễ dàng để sao lưu dữ liệu vào một trong số các đĩa này là tạo ra một biểu tượng tắt *(shortcut)* trên màn hình desktop để thi hành một tập tin batch nhỏ *(tập tin dạng text có phần mở rộng .BAT)*. Ví dụ sau đây sẽ minh họa cách tạo một biểu tượng tắt để sao lưu thư mục \DATA, cùng các tập tin và thư mục con của nó:

1. Bằng cách sử dụng Notepad hoặc WordPad, bạn hãy gõ vào các dòng lệnh sau, trong đó ổ đĩa tháo lắp là ổ đĩa E và thông số /S ra lệnh hệ điều

hành kèm theo các thư mục con khi sao chép. *(Các tập tin ẩn sẽ không được sao chép, nhưng các tập tin dữ liệu thường không mang thuộc tính ẩn):*

```
XCOPY C:\DATA\*.* E: /S
```

2. Lưu tập tin này lại với tên gọi \DATA\BACKUP.BAT rồi thoát khỏi trình biên tập.
3. Tạo một biểu tượng tắt trỏ tới tập tin BACKUP.BAT.
4. Do các tập tin .BAT là các tập tin DOS, nên biểu tượng trên màn hình desktop sẽ là biểu tượng MS-DOS. Để thay đổi biểu tượng này, bạn nhấp nút chuột phải vào nó, chọn **Properties** từ menu xổ xuống, nhấp chọn khung trang **Program**, rồi nhấn vào nút **Change Icon** *(xem hình 3-5)*. Bạn hãy chọn một biểu tượng rồi nhấn nút **OK** hai lần để quay trở lại với màn hình desktop.



Hình 3-5 Thay đổi biểu tượng dành cho biểu tượng tắt BACKUP.BAT

5. Bất kỳ khi nào nếu muốn sao lưu các dữ liệu của mình, bạn hãy đặt một đĩa vào ổ rồi nhấp đôi nút chuột vào biểu tượng tắt BACKUP.BAT.

2. CÁC PHƯƠNG THỨC SAO LƯU

Hiện có nhiều phương thức phức tạp hơn được sử dụng cho việc tạo các bản sao dự phòng, trong đó tiến trình sao lưu có tính lựa chọn, chẳng hạn chỉ sao lưu những gì được thay đổi, những gì hiện chưa được sao lưu...vv. Theo truyền thống, các phương thức này đều liên quan tới việc sao lưu vào các băng từ, vì băng từ thường đủ lớn để chứa toàn bộ bản sao dự phòng. Để minh họa các phương thức này, chúng ta sẽ sử dụng các băng từ làm phương tiện sao lưu. Phương thức con, cha và ông nội là một kế hoạch dành cho việc tái sử dụng băng từ. Các bản sao dự phòng đầy đủ, tăng dần và có phân biệt là các phương thức được sử dụng để đẩy mạnh tiến trình sao lưu, các bản sao dự phòng được định lịch trình được thực hiện để giảm thiểu sự bất tiện cho những người dùng. Các công việc sao lưu có lựa chọn chỉ sao lưu các dữ liệu thường thay đổi trên ổ đĩa cứng. Bằng cách chỉ chọn sao lưu các folder thiết yếu nào đó trên ổ đĩa cứng, tiến trình sao lưu sẽ diễn ra nhanh hơn và việc phục hồi các dữ liệu bị mất sẽ trở nên dễ dàng hơn.

a) Phương thức con, cha và ông nội

Khi bạn phục trách thực hiện thủ tục sao lưu dự phòng cho các ổ đĩa cứng, một trong những điều bạn phải làm trước hết là đặt ra một kế hoạch sao lưu. Một kế hoạch thông dụng dành cho sao lưu dữ liệu, được gọi là *phương thức con, cha và ông nội* (child, parent, grandparent method), sẽ khiến việc tái sử dụng các băng từ trở nên dễ dàng hơn. Bảng 4 giải thích phương thức này. Bạn hãy ghi kế hoạch này ra giấy và duy trì một sổ nhật ký ghi chép các công việc sao lưu đã được thực hiện.

Bảng 4 **Phương thức sao lưu dự phòng con, cha và ông nội**

Tên bản sao lưu	Định kỳ thực hiện	Vị trí lưu trữ	Mô tả
Con	Hàng ngày	Ngay tại chỗ	Duy trì bốn băng sao lưu hàng ngày và luân chuyển chúng sau mỗi tuần. Ghi nhãn bốn băng này lần lượt là thứ Hai, thứ Ba, thứ Tư và thứ Năm. Một bản sao hàng ngày (con) thứ Sáu không được tạo ra, vì vào thứ Sáu bạn sẽ tạo ra bản sao dự phòng cha.
Cha	Hàng tuần	Chỗ khác	Thực hiện sao lưu dự phòng hàng tuần vào ngày thứ Sáu. Duy trì năm băng từ sao lưu hàng tuần, mỗi băng dành cho mỗi ngày thứ Sáu của tháng và luân chuyển chúng sau mỗi tháng. Ghi nhãn các băng từ này lần lượt là thứ Sáu 1, thứ Sáu 2, thứ Sáu 3, thứ Sáu 4 và thứ Sáu 5.

Tên bản sao lưu	Định kỳ thực hiện	Vị trí lưu trữ	Mô tả
Ông nội	Hàng tháng	Chỗ khác, trong một két sắt chống cháy.	Thực hiện công việc sao lưu dự phòng hàng tháng vào ngày thứ Sáu cuối cùng của tháng. Duy trì 12 băng từ, mỗi băng từ dành cho một tháng trong năm. Luân chuyển chúng sau mỗi năm. Ghi nhãn cho các băng này lần lượt là tháng Giêng, tháng Hai, tháng Ba, ...vv.

b) Các bản sao lưu đầy đủ, tăng dần và có phân biệt

Một số phương thức sao lưu dự phòng được thiết kế để làm cho công việc sao lưu trở nên hiệu quả hơn, bằng cách không thực hiện sao lưu toàn bộ các dữ liệu mỗi lần công việc sao lưu được tiến hành. Một thủ tục *sao lưu đầy đủ (full backup)* sẽ sao lưu toàn bộ các dữ liệu từ ổ đĩa cứng. Một thủ tục *sao lưu tăng dần* (incremental backup) sẽ sao lưu chỉ các tập tin đã được thay đổi hoặc các tập tin vừa mới được tạo ra kể từ lần sao lưu sau cùng, *bất kể bản thân thủ tục sao lưu sau cùng này là một thủ tục tăng dần hay đầy đủ.* Các thủ tục *sao lưu có phân biệt* (differential backup) sẽ sao lưu các tập tin đã được thay đổi hoặc đã được tạo ra kể từ lần sao lưu *đầy đủ* sau cùng.

Bạn hãy bắt đầu bằng một thủ tục sao lưu đầy đủ. Lần kế tiếp bạn thực hiện một công việc sao lưu, nếu bạn chọn phương thức tăng

dần, chỉ các tập tin đã thay đổi hoặc được tạo ra kể từ lần sao lưu đầy đủ sau cùng mới được sao lưu. Lần thứ hai bạn thực hiện một thủ tục sao lưu tăng dần, chỉ các tập tin đã thay đổi hoặc được tạo ra kể từ lần sao lưu dự phòng tăng dần sau cùng mới được sao lưu.

Ví dụ, khi đang sử dụng phương thức con, cha và ông nội, một thủ tục sao lưu dự phòng đầy đủ có thể được thực hiện vào mỗi ngày thứ Sáu. Các bản sao lưu từ thứ Hai tới thứ Năm có thể là các bản sao lưu tăng dần. Ưu điểm của phương thức này là các thủ tục sao lưu tăng dần sẽ diễn ra nhanh hơn và đòi hỏi ít không gian lưu trữ hơn các bản sao đầy đủ. Điểm bất lợi của phương thức này là, khi các dữ liệu cần phải được phục hồi, bạn phải bắt đầu từ bản sao dự phòng đầy đủ sau cùng rồi sử dụng qua hết mỗi bản sao lưu tăng dần cho tới thời điểm mà các dữ liệu bị mất. Tiến trình này có thể rất mất thời gian. Nếu bạn sử dụng các bản sao lưu tăng dần, bạn hãy vạch kế hoạch thực hiện một bản sao đầy đủ sau ít nhất mỗi 6 hoặc 7 bản sao lưu tăng dần. Các tiện ích sao lưu của Windows 9x và Windows NT đều hỗ trợ các thủ tục sao lưu tăng dần.

Nếu bạn sử dụng phương thức sao lưu có phân biệt cùng với phương thức con, cha và ông nội, bạn hãy tạo một bản sao dự phòng đầy đủ vào các ngày thứ Sáu. Vào ngày thứ Hai, bạn hãy thực hiện một thủ tục sao lưu tăng dần. Tất cả các tập tin đã thay đổi kể từ ngày thứ Sáu đều được sao lưu. Vào ngày thứ Ba,

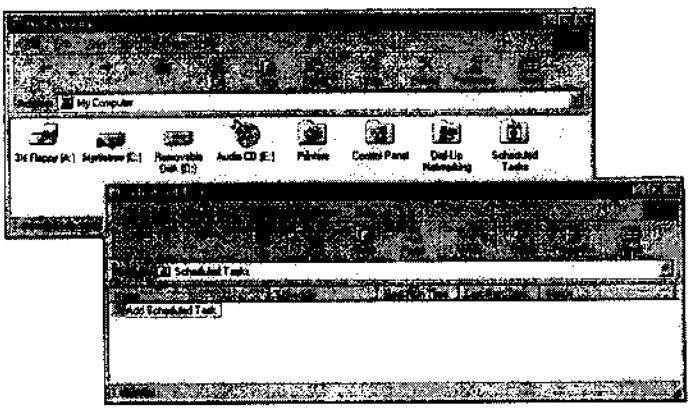
một thủ tục sao lưu có phân biệt cũng sẽ sao lưu tất cả các tập tin đã thay đổi kể từ ngày thứ Sáu (*bản sao dự phòng đầy đủ*). Các thủ tục sao lưu có phân biệt không xem xét xem các thủ tục sao lưu có phân biệt khác đã được thực hiện hay chưa, nhưng sẽ so sánh các dữ liệu chỉ với bản sao lưu đầy đủ sau cùng và đây chính là điểm khác biệt giữa các thủ tục sao lưu có phân biệt và các thủ tục sao lưu tăng dần. Ưu điểm của các thủ tục sao lưu có phân biệt so với các thủ tục sao lưu tăng dần là, nếu bạn cần phục hồi các dữ liệu, bạn chỉ cần phục hồi từ bản sao dự phòng đầy đủ sau cùng và bản sao dự phòng có phân biệt sau cùng. Các thủ tục sao lưu dự phòng có phân biệt không được Windows 95 hỗ trợ, nhưng được hỗ trợ trong Windows 98 và Windows NT.

c) Các bản sao lưu theo lịch trình

Các thủ tục sao lưu có thể được thực hiện một cách tương tác, hoặc có thể được định lịch trình để tự động thực hiện. Các thủ tục sao lưu tương tác được thực hiện bởi người dùng đang ngồi trước máy tính. Một thủ tục sao lưu dự phòng theo lịch trình được định lịch trình để tự động thực hiện bởi phần mềm khi máy tính thường không được sử dụng tới, chẳng hạn như vào giữa đêm. Windows 98 và Windows NT hỗ trợ việc định lịch trình *(schedule)* cho bất kỳ chương trình nào *(bao gồm cả các tác vụ sao lưu)*, sao cho chúng sẽ thi hành vào một thời

điểm *(ngày, giờ)* định trước mà không cần đến sự can thiệp của người dùng. Trong Windows 98, bạn làm như sau để định lịch trình chương trình **BACKUP.BAT** mà chúng ta đã tạo ra trước đây, để nó thi hành vào lúc 11:59 PM của mỗi ngày thứ Hai:

1. Nhấp đôi nút chuột vào biểu tượng **My Computer** trên màn hình desktop. Từ cửa sổ My Computer, bạn nhấp đôi nút chuột vào biểu tượng **Scheduled Task**. Cửa sổ Scheduled Tasks lập tức xuất hiện (*xem hình 3-6*).



Hình 3-6 Bổ sung một tác vụ thi hành theo lịch trình trong Windows 98.

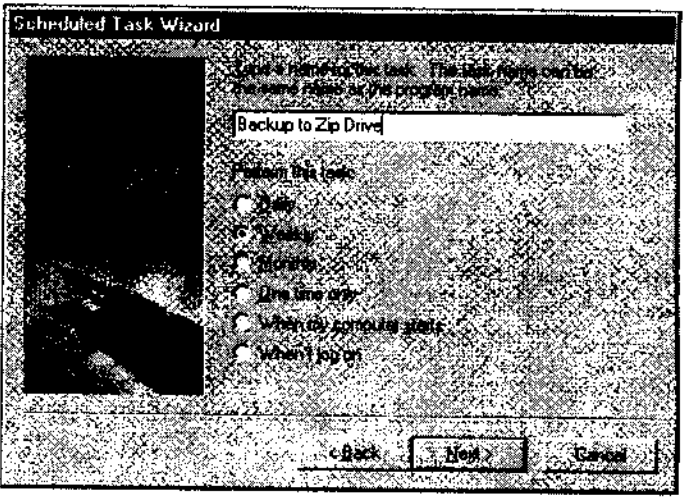
2. Nhấp đôi nút chuột vào biểu tượng **Add Scheduled Task**. Hộp thoại Scheduled Task Wizard liền xuất hiện (xem hình 3-7). Bạn hãy chọn chương trình cần định lịch trình: nhấn nút

Browse, tìm vào nhấp chuột vào tập tin BACKUP.BAT trong folder \DATA, sau đó nhấn nút **Open**.

3. Nhập vào một tên gọi cho tác vụ này, chọn lịch trình thi hành nó, rồi nhấn nút **Next** để tiếp tục.

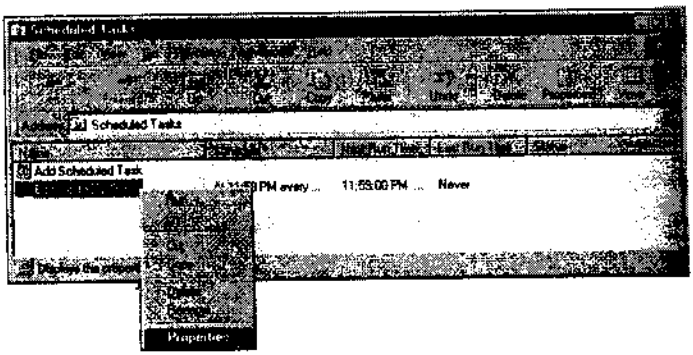
4. Nhập thời gian bắt đầu và ngày trong tuần mà bạn muốn tác vụ này thi hành. Trong ví dụ của chúng ta, bạn nhập vào 11:59 PM, every Monday, rồi nhấn nút **Next** để tiếp tục.

5. Scheduled Task Wizard sẽ báo cáo các thông số của tác vụ được định lịch trình. Bạn hãy nhấn nút **Finish** để hoàn tất tiến trình.



Hình 3-7 Đặt tên cho một tác vụ được định lịch trình và chọn lịch trình để nó hoạt động.

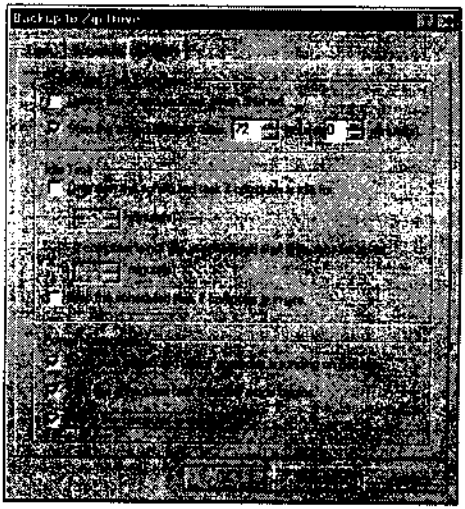
6. Sau này, nếu bạn muốn thay đổi các xác lập cho một tác vụ được định lịch trình, bạn nhấp đôi nút chuột vào biểu tượng **My Computer**, nhấp đôi nút chuột vào biểu tượng **Scheduled Tasks**, rồi nhấp nút phải chuột vào biểu tượng tác vụ cần điều chỉnh trong cửa sổ Scheduled Task. Chọn **Properties** từ menu xổ xuống *(xem hình 3-8)*. Hộp thoại thuộc tính của tác vụ liền xuất hiện *(xem hình 3-9)*.



Hình 3-8 Thay đổi các xác lập cho tác vụ bằng cách sử dụng hộp thoại thuộc tính của nó được liệt kê trong cửa sổ Scheduled Task.

7. Nhấp chọn khung trang **Settings** để thay đổi các xác lập cho tác vụ. Lưu ý tại phần đáy của khung trang này rằng bạn có thể ra lệnh *trình lập lịch* (task scheduler) đánh thức máy PC dậy để thực hiện tác vụ này. Tùy chọn này đòi hỏi bo mạch hệ thống

của bạn phải hỗ trợ việc bật nguồn máy tính bằng phần mềm. Muốn biết bo mạch hệ thống của bạn có hỗ trợ tính năng này hay không, bạn có thể xem trong CMOS setup hoặc trong tài liệu dành cho bo mạch hệ thống. Nếu bo mạch hệ thống của bạn không hỗ trợ, máy PC phải được bật lên thì trình lập lịch mới có thể hoạt động.



Hình 3-9 Với một số máy tính, trình lập lịch tác vụ có thể bật nguồn máy tính lên để thi hành tác vụ.

3. PHẦN MỀM SAO LƯU

Hầu hết các ổ băng từ đều được kèm theo phần mềm sao lưu. Bạn cũng có thể mua một phần mềm sao lưu của hãng thứ ba hoặc sử dụng Windows 9x hoặc Windows NT để sao lưu

đĩa cứng của mình. Khi tìm hiểu về phần mềm sao lưu, bạn cần nhớ rằng phần mềm này chỉ sao lưu các tập tin đang không được sử dụng, do đó bạn hãy đóng tất cả các tập tin và các ứng dụng lại trước khi thực hiện một thủ tục sao lưu.

a) Tiện ích Backup của Windows 9x

Windows 9x cung cấp một tiện ích sao lưu hỗ trợ việc sao lưu tới cả các đĩa mềm lẫn các băng từ. Windows 98 hỗ trợ nhiều thiết bị sao lưu được sử dụng phổ biến hiện nay, bao gồm các thiết bị sử dụng các cổng tuần tự, các thiết bị IDE/ATAPI và các thiết bị SCSI, vốn không được Windows 95 hỗ trợ. Bạn vẫn có thể sử dụng các ổ và các băng từ không được Windows 9x hỗ trợ, nhưng bạn buộc phải sử dụng một số phần mềm sao lưu của hãng thứ ba với chúng.

Trong Windows 9x, nếu thành phần Backup của Windows 9x chưa được cài đặt, bạn có thể cài đặt nó như sau:

1. Nhấn nút **Start → Settings → Control Panel**, rồi nhấp đôi nút chuột vào biểu tượng **Add/Remove Programs.**
2. Trong hộp thoại Add/Remove Programs Properties, bạn nhấp chọn khung trang **Windows Setup**.
3. Dưới mục **Disk Tools** đối với Windows 95 hoặc **System Tools** đối

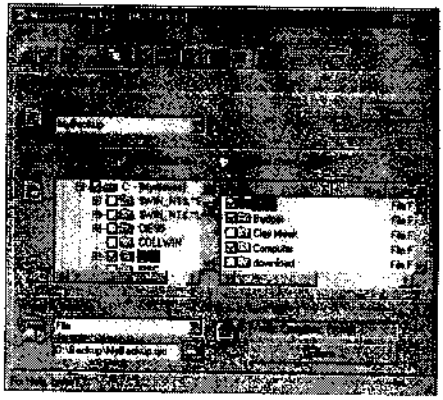
với Windows 98, bạn chọn **Backup**, sau đó nhấn nút **OK** rồi nhấn nút **Apply** để cài đặt thành phần này. Bạn sẽ được yêu cầu cung cấp đĩa CD-ROM hoặc các đĩa mềm gốc của Windows 9x để hệ điều hành có thể hoàn tất công việc cài đặt.

Muốn sử dụng tiện ích Backup của Windows 98, bạn làm như sau:

1. Nhấn nút **Start → Programs → Accessories → System Tools**, rồi chọn **Backup**. Backup Wizard trước hết sẽ tìm kiếm các thiết bị sao lưu, chẳng hạn như các ổ đĩa Zip hoặc các ổ băng từ. Nếu không tìm thấy, nó sẽ hỏi bạn có muốn cài đặt một thiết bị sao lưu hay không. Trái lại, nó sẽ hiển thị một cửa sổ hỏi xem bạn muốn tạo ra một tác vụ sao lưu mới hay mở một tác vụ đã có sẵn. Tiện ích Backup lưu giữ các thông tin về các tác vụ sao lưu dưới một tên gọi do bạn đặt, do đó bạn có thể sử dụng cùng một tác vụ nhiều lần. Bạn hãy chọn **Create a new backup job** rồi nhấn nút **Next** để tiếp tục.
2. Backup Wizard sẽ hỏi bạn về kiểu sao lưu mà bạn muốn sử dụng (*ví dụ, sao lưu tất cả các tập tin hay chỉ sao lưu các tập tin đã thay đổi kể từ*

lần sao lưu sau cùng). Bạn hãy lựa chọn rồi nhấn nút **Next** để tiếp tục.

3. Lúc này tiện ích Microsoft Backup sẽ hiển thị một cửa sổ Backup *(xem hình 3-10).*



Hình 3-10 Microsoft Backup của Windows 98 cho phép bạn lựa chọn các tập tin và các folder cần sao lưu.

4. Muốn sao lưu chỉ các tập tin, folder, hay ổ đĩa luận lý nào đó, bạn đánh dấu kiểm vào các hộp vuông nằm bên trái tên của chúng. Ngoài ra, để hiển thị một danh sách gồm tất cả các folder con trong một folder, bạn hãy nhấp chuột vào hộp mang dấu + nằm bên trái folder này. Backup chỉ ra rằng chỉ có các phần của một folder hoặc ổ đĩa được chọn sao lưu bằng cách đặt một dấu kiểm xám trong hộp vuông tương ứng.

5. Bạn hãy lưu ý khung mang nhãn **Where to backup** nằm ở góc dưới bên trái của cửa sổ Backup trong hình 3-10. Bạn hãy chọn từ danh sách thả xuống này phương tiện và thư mục được sử dụng cho việc sao lưu. Trong ví dụ của chúng ta, phương tiện là ổ đĩa D, một ổ đĩa Zip. Tập tin sao lưu sẽ được đặt trong một folder mang tên \Backup.
6. Nhấp vào nút **Start** để bắt đầu cập nhật.

Muốn phục hồi các tập tin, các folder hoặc toàn bộ ổ đĩa cứng từ bản sao lưu dự phòng, bạn làm theo các hướng dẫn sau:

1. Trên cửa sổ tiện ích Backup *(xem hình 3-10)*, bạn nhấn nút **Restore**, sau đó chọn tác vụ sao lưu mà bạn muốn sử dụng cho tiến trình phục hồi. Tiện ích Backup sẽ hiển thị các folder và các tập tin đã được sao lưu bằng tác vụ này. Bạn có thể chọn các thứ mà mình muốn phục hồi.
2. Nhấn nút **Start** để thực hiện công việc phục hồi.

4. RAID

Ngoài việc duy trì một bản sao dự phòng an toàn, một phương thức bảo vệ dữ liệu khác là ghi liên tiếp hai bản sao của các dữ liệu, mỗi bản

nằm trên một ổ đĩa cứng khác nhau. Phương thức này thường được sử dụng trên các máy phục vụ tập tin cao cấp và đắt tiền, nhưng đôi khi cũng có những tình huống mà một người dùng máy trạm làm việc cũng cần sử dụng.

Các phương thức được sử dụng để cải thiện hiệu suất và/hoặc tự động phục hồi từ một sự cố được gọi chung là **RAID** (**r**edundant **a**rray of **i**ndependent **d**isks: mảng thừa gồm các đĩa độc lập). RAID có nhiều cấp độ, nhưng trong phần này chúng ta chỉ đề cập tới ba cấp độ được sử dụng phổ biến nhất (*xem bảng 5*). Trong số các cấp độ RAID, chỉ có năm cấp độ đầu tiên là thiết thực về mặt tài chính đối với một trạm làm việc độc lập.

Bảng 5 **Ba cấp độ RAID phổ biến nhất.**

[illegible]	[illegible]	[illegible]
RAID 0: *Tách dải đĩa* (*disk striping*) không có chẵn lẻ. (Thuật ngữ *tách dải* (*striping*) ám chỉ tới việc ghi dữ liệu ngang qua nhiều hơn một ổ đĩa vật lý).	Cải thiện hiệu suất hệ thống và sức chứa dữ liệu.	Các dữ liệu được ghi vào hai hoặc nhiều ổ đĩa cứng. Bộ đĩa này được xem là một volume đơn lẻ (*một ổ đĩa ảo đơn*). Do có nhiều hơn một ổ đĩa hoạt động, hiệu suất sẽ tăng lên.

[illegible] và [illegible] thông thường		
RAID 1: *Tạo gương đĩa* (disk mirrioring) hay *tạo song công đĩa* (disk duplexing).	Cung cấp khả năng kháng lỗi.	Các dữ liệu được ghi hai lần, mỗi lần vào một trong số hai ổ đĩa. Kỹ thuật tạo gương đĩa chỉ sử dụng một *bộ điều hợp HD* (HD adapter). Kỹ thuật tạo song công đĩa sử dụng hai bộ điều hợp, mỗi bộ dành cho một ổ đĩa.
RAID 5: Tách dải đĩa có chẵn lẻ.	Cải thiện hiệu suất, sức chứa dữ liệu và cung cấp khả năng kháng lỗi.	Các dữ liệu được ghi vào hai hoặc nhiều ổ đĩa, nhưng các thông tin chẵn lẻ cũng được ghi vào một ổ đĩa thứ ba hoặc ổ đĩa phụ để khi một ổ đĩa bị sự cố, các ổ đĩa còn lại có thể tái tạo lại các dữ liệu được lưu trữ trên ổ đĩa bị sự cố này.

RAID Level 0 gia tăng dung lượng ổ đĩa luận lý bằng cách xem hai ổ đĩa như là một ổ đĩa luận lý đơn, nhưng nó chỉ chứa một bản sao của dữ liệu. Do đó, cấp độ này không cung cấp một cách để phục hồi dữ liệu sau khi xảy ra một sự cố (một tính năng quan trọng của kháng lỗi). RAID 0 là phương thức *tách dải đĩa* (disk striping), một phương thức trong đó nhiều hơn một ổ đĩa cứng được xem như là một volume đơn. Đối với một mảng gồm hai ổ đĩa cứng, một số dữ liệu sẽ được ghi vào một ổ đĩa cứng và một số dữ liệu sẽ được ghi vào ổ đĩa kia; cả hai ổ đĩa tạo nên một ổ đĩa luận lý *(volume)* và các dữ liệu chỉ được ghi một lần.

RAID 0 được Windows NT Workstation hỗ trợ, nhưng không được Windows 9x hỗ trợ.

RAID Level 1 được thiết kế để bảo vệ các dữ liệu khi xảy ra một sự cố ổ đĩa cứng bằng các ghi các dữ liệu hai lần, mỗi lần vào một ổ trong số hai ổ đĩa. Một kiểu của RAID Level 1 có tên gọi là *tạo gương đĩa* (disk mirroring), trong đó hai ổ đĩa cứng sử dụng chung một card điều hợp.

Các ưu điểm của việc tạo gương đĩa RAID bao gồm:

- Nếu một trong hai ổ đĩa bị sự cố, các dữ liệu vẫn an toàn trên ổ đĩa kia.
- Tốc độ đọc đĩa được cải thiện vì bộ điều hợp có hai nơi để đọc.

Các nhược điểm của RAID 1 bao gồm:

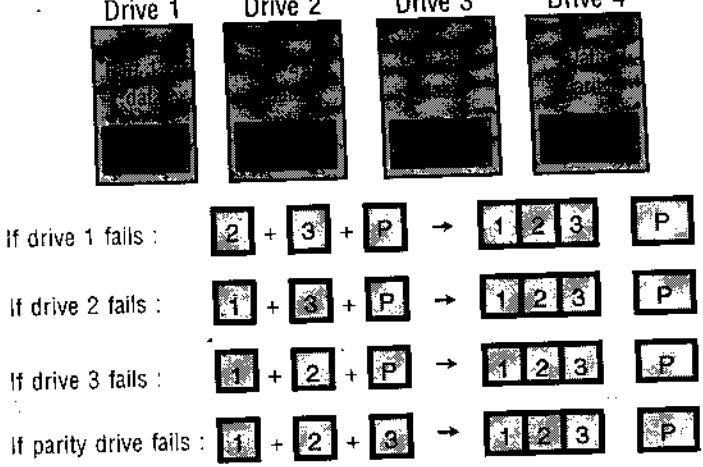
- Việc sử dụng hai ổ đĩa cứng trong cùng một máy tính sẽ tốn kém hơn.
- Do các dữ liệu được ghi hai lần, dùng lượng ổ đĩa cứng bị *"cắt bớt"* còn một nửa.
- Tốc độ ghi đĩa bị giảm xuống vì các dữ liệu phải được ghi hai lần.

Một yếu điểm của kỹ thuật tạo gương đĩa là cả hai ổ đĩa cứng đều sử dụng chung một bộ điều hợp. Nếu bộ điều hợp hư hỏng, cả hai ổ đĩa này đều không thể truy xuất được. Một sự cải tiến của kỹ thuật tạo gương đĩa, còn được xem là RAID 1, là kỹ thuật *tạo song công đĩa* (disk duplexing), trong đó mỗi ổ đĩa cứng có

iêng một card điều hợp. Chi phí ban đầu sẽ cao hơn, nhưng nếu một card điều hợp bị sự cố, bạn có thể tránh được khả năng mất dữ liệu trên cả hai ổ đĩa này. Nếu việc sao lưu dự phòng tới một máy phục vụ trên một mạng không thể thực hiện được, kỹ thuật tạo gương đĩa hoặc tạo song công đĩa có thể thích hợp với một trạm làm việc *(nếu các dữ liệu được xem là đủ giá trị để xứng đáng với chi phí bỏ ra thêm).*

Windows NT Workstation không hỗ trợ RAID 1, do đó nếu muốn sử dụng RAID 1 trên một trạm làm việc, hai ổ đĩa cứng phải được quản lý bởi phần sụn trên các bộ kiểm soát thay vì bởi hệ điều hành. Điều này sẽ làm tăng thêm chi phí phần cứng vì phải cần bộ kiểm soát đĩa cứng phức tạp hơn. Windows NT Server hỗ trợ RAID 1 và RAID 5.

RAID 5, hay kỹ thuật *tách dải đĩa có chẵn lẻ* (disk striping with parity), là một biến thể lý thú gồm RAID 0 kết hợp với RAID 1, trong đó khả năng kháng lỗi và dung lượng ổ đĩa đều được cải thiện. RAID 5 đòi hỏi ít nhất ba ổ đĩa cứng. Trong hình 3-11, RAID 5 được mô tả đang sử dụng bốn ổ đĩa cứng được nhóm lại như một ổ đĩa cứng ảo duy nhất. Khi bất kỳ dữ liệu nào được ghi vào *"ổ đĩa cứng ảo"* này, chúng sẽ được chia ra thành ba đoạn *(segment).* Mỗi đoạn được ghi vào một trong số ba ổ đĩa đầu tiên và các thông tin chẵn lẻ *(parity)* về ba đoạn này sẽ được ghi vào ổ đĩa thứ tư.



Hình 3-11 RAID 5, kỹ thuật tách dải đĩa có chẵn lẻ, cho phép tăng dung lượng đĩa và cung cấp khả năng kháng lỗi: khi bất kỳ ổ đĩa nào bị sự cố, các dữ liệu vẫn có thể được phục hồi.

Nếu một trong số bốn đĩa bị hư hại – bất kể đĩa nào – các dữ liệu đều có thể được phục hồi từ ba ổ đĩa còn lại. Cách thực hiện điều này được mô tả trong phần dưới của hình 3-11. Qua việc sử dụng bất kỳ hai đoạn nào và các thông tin chẵn lẻ, cả ba đoạn đều có thể được tái tạo lại, hoặc, nếu ổ đĩa chứa thông tin chẵn lẻ bị sự cố, ba đoạn dữ liệu vẫn được lưu giữ an toàn trong ba ổ đĩa đầu tiên.

Để hiểu được cách các dữ liệu được phục hồi ra sao từ các thông tin chẵn lẻ, chúng ta sẽ cùng xem xét ví dụ sau. Giả sử bạn có ba con số được lưu trữ trên ba ổ đĩa khác nhau. Nếu bạn lưu trữ tổng của ba con số này và ổ đĩa thứ tư, hay ổ đĩa chẵn lẻ, các thông tin mà bạn

đang có có thể được sử dụng để tính toán bất kỳ con số nào bị mất sau này. Ví dụ, nếu ba con số của bạn là 1, 2 và 6, bạn sẽ lưu trữ tổng của chúng (9) vào ổ đĩa chẵn lẻ. Nếu con số đầu tiên bị mất, nó có thể được tính ra từ tổng nói trên và hai con số còn lại.

Khi một ổ đĩa bị hư hại, các dữ liệu có thể được tái sinh trên ổ đĩa được thay thế bằng cách sử dụng các thông tin từ các ổ đĩa còn lại. Trước hết bạn hãy thay thế ổ đĩa bị hư hại bằng một ổ đĩa mới. Muốn sinh các dữ liệu trên ổ đĩa mới, khi đang sử dụng Windows NT Sever, bạn truy xuất tới Disk Administrator của nhóm Administrative Tools rồi thi hành một lệnh Regenerate. Windows NT sẽ thực hiện nốt phần việc còn lại. Hoạt động này hoàn toàn tự động và bạn có thể vẫn sử dụng cho các hoạt động khác trong khi công việc tái sinh đang diễn ra.

Đối với một máy chủ *(File Server)* sử dụng RAID 5 luôn phải được bật lên và hoạt động liên tục, sẽ là một điều thiết thực nếu hệ thống này sử dụng phần cứng vốn cho phép *tráo đổi nóng* (*hot swapping*), có nghĩa là một ổ đĩa cứng có thể được tháo ra và một ổ đĩa khác được lắp vào mà không cần phải tắt máy tính. Tuy nhiên, các ổ đĩa cứng cho phép tráo đổi nóng có giá đắt hơn đáng kể so với các ổ đĩa cứng bình thường.

5. CHUẨN BỊ CHO VIỆC PHỤC HỒI TỪ THẢM HỌA

Bạn phải chuẩn bị để đối phó với thảm họa trước khi nó xảy ra. Nếu không có sự chuẩn bị từ trước, khi thảm họa – vốn không thể tránh được – xảy ra, sự thiệt hại sẽ lớn hơn rất nhiều. Bạn hãy suy nghĩ về ổ đĩa cứng trên máy PC của mình tại thời điểm này. Giả sử đột nhiên nó ngưng hoạt động và tất cả các thông tin trên đó bị mất hết. Hậu quả sẽ ra sao? Bạn đã chuẩn bị cho biến cố này chưa? Các bản sao dự phòng rất quan trọng, nhưng việc biết cách sử dụng chúng để phục hồi các dữ liệu bị mất cũng quan trọng không kém.Việc biết rõ khi nào bản sao dự phòng này được thực hiện và những gì bạn phải làm để phục hồi các thông tin đã nhập vào kể từ lần sao lưu dự phòng sau cùng cũng hết sức cần thiết. Đây cũng chính là lúc bạn được đền bù xứng đáng với công sức bỏ ra để duy trì cẩn thận các bản ghi chép.

Khi bạn thực hiện một tác vụ sao lưu dự phòng lần đầu hoặc xác lập một tác vụ sao lưu theo lịch trình, bạn cần xác nhận rằng băng từ hoặc các đĩa sao lưu đều có thể sử dụng được để phục hồi các dữ liệu thành công khi cần. Đây là một bước hết sức quan trọng để chuẩn bị cho quá trình phục hồi các dữ liệu đã mất về sau. Sau khi bạn đã tạo ra một băng sao lưu, bạn hãy xóa một tập tin trên ổ đĩa cứng, rồi sử dụng các thủ tục phục hồi để xác nhận rằng

bạn có thể tái tạo lại tập tin này từ bản sao dự phòng. Bạn không chỉ cần xác nhận rằng băng từ hay các đĩa mềm này hoạt động bình thường, mà bạn còn phải xác nhận tính hiệu quả của phần mềm phục hồi và sự hiểu biết của bạn về cách thức sử dụng nó. Sau khi đã tin chắc rằng tiến trình phục hồi hoạt động bình thường, bạn hãy ghi rõ ra giấy cách thức thực hiện tiến trình này.

Hãy xác nhận rằng kế hoạch phục hồi của bạn sẽ đem lại kết quả bằng cách luyện tập nó trước khi một thảm họa xảy ra.

Bạn hãy luôn duy trì các bản ghi chép về các bản sao dự phòng đều đặn của mình trong một bảng cùng với các thông tin sau: các folder hoặc ổ đĩa được sao lưu, ngày tháng thực hiện sao lưu, kiểu sao lưu và tên của băng từ được sử dụng. Bảng này sẽ trở nên vô cùng giá trị khi bạn cần phục hồi các dữ liệu vốn đã bị mất nhiều ngày hoặc nhiều tuần. Bạn có thể giữ các bản ghi này trong một cuốn sổ tay. Bạn cũng có thể ra lệnh phần mềm sao lưu tạo ra một nhật ký hoàn chỉnh trong một *tập tin nhật ký* (*log file, một tập tin nhật ký là một tập tin dùng để ghi nhận các sự kiện xảy ra*) mỗi khi thực hiện công việc sao lưu bạn hãy luôn duy trì các bản sao trên giấy của các tập tin nhật ký này. Bạn có thể nhận thấy rằng phương thức tập tin nhật ký này quá mất thì giờ khi thực hiện hàng

ngày. Vì mặc dù phần mềm sao lưu sẽ tự động ghi nhận các sự kiện vào tập tin nhật ký, nhưng công việc sao lưu dự phòng sẽ diễn ra lâu hơn do hoạt động ghi nhận này và việc in ấn tập tin nhật ký sau đó cũng sẽ mất thì giờ.

Thỉnh thoảng, bạn nên thực hiện định kỳ một thủ tục phục hồi toàn bộ một ổ đĩa cứng mà bạn đã sao lưu. Hãy sử dụng băng từ chứa bản sao lưu đầy đủ và một ổ đĩa cứng khác, sau đó phục hồi ổ đĩa cứng đầu tiên vào ổ đĩa cứng mới rồi so sánh các kết quả nhằm xác nhận rằng, nếu cần thiết, các bản sao lưu dự phòng của bạn có thể làm công việc mà chúng được thiết kế: phục hồi từ một thảm họa.

4 Tóm tắt

- Các hư hỏng máy tính có thể do nhiều yếu tố môi trường và con người khác nhau, bao gồm sức nóng, bụi bặm, từ tính, các sự cố bộ nguồn cung cấp, tĩnh điện, lỗi con người *(chẳng hạn làm đổ chất lỏng hoặc vô tình thay đổi các cấu hình hệ thống và cấu hình phần mềm)* và các virus
- Các mục tiêu của công tác bảo dưỡng phòng ngừa nhằm làm cho máy tính hoạt động bền hơn và tốt hơn, bảo vệ các dữ liệu, các phần mềm và giảm thiểu chi phí sửa chữa.
- Một kế hoạch bảo dưỡng phòng ngừa cho máy PC bao gồm thổi sạch bụi bặm ra khỏi bên trong khung máy, làm sạch các tiếp điểm trên các card mở rộng, duy trì một bản ghi chứa các thông tin cấu hình, sao lưu dự phòng ổ đĩa cứng, làm vệ sinh con chuột, monitor và bàn phím.

- Việc bảo vệ các tài liệu phần mềm và phần cứng là một tác vụ bảo dưỡng phòng ngừa quan trọng.
- Bạn đừng bao giờ vận chuyển một máy PC khi ổ đĩa cứng của nó đang chứa bản sao duy nhất của các dữ liệu quan trọng.
- Các hình thức phá hoại máy tính bao gồm các virus, các Trojan horse và các sâu máy tính. Sự phân loại này dựa trên cách thức lan truyền của chúng.
- Phần mềm diệt virus là lựa chọn tốt nhất của bạn để ngăn ngừa các thiệt hại do các virus gây ra.
- Các virus có thể ẩn náu trong các tập tin chương trình, các cung khởi động và các tài liệu có chứa các macro.
- Các virus cố gắng tránh sự phát hiện của các phần mềm diệt virus bằng cách thay đổi các dấu hiệu tiêu biểu của chúng và bằng cách cố gắng che đậy dấu hiệu về sự tồn tại của chúng.
- Một số virus tương đối vô hại vì chúng chỉ hiển thị các hình ảnh kỳ lạ lên màn hình. Một số khác rất nguy hiểm vì chúng có thể xóa sạch mọi thứ trên ổ đĩa cứng, kể cả các thông tin trong bảng phân vùng.
- Các bước bạn cần tuân thủ để ngăn ngừa virus lây nhiễm vào máy tính

bao gồm không trao đổi các đĩa mềm, chỉ mua phần mềm từ các nguồn đáng tin cậy, chỉ nạp trên Internet xuống các chương trình từ các site đáng tin cậy và sử dụng các mạng một cách thận trọng.

- Một trò đánh lừa của virus được dự tính để làm quá tải sự lưu thông mạng. Nó làm điều này bằng cách đánh lừa mọi người để họ gửi các thông điệp e-mail cho nhau, thông báo với nhau về các virus.
- Để ngăn ngừa sự thiệt hại do virus, bạn hãy sử dụng phần mềm diệt virus và sao lưu ổ đĩa cứng thường xuyên.
- Các ổ băng từ là các thiết bị phần cứng được sử dụng nhiều để sao lưu một ổ đĩa cứng. Chúng có rất nhiều biến thể về chủng loại và định dạng.
- RAID được sử dụng để tạo gương (mirror) cho các dữ liệu trên một ổ đĩa cứng và để gia tăng dung lượng đĩa, bằng cách khiến nhiều hơn một ổ đĩa cứng hoạt động như một ổ đĩa ảo đơn.
- Phương thức sao lưu con, cha và ông nội được sử dụng để tái sử dụng các băng từ theo một kế hoạch đơn giản và dễ dàng.
- Việc sử dụng một bản sao dự phòng đầy đủ, kèm theo các bản sao dự

phòng tăng dần hoặc có phân biệt, sẽ làm tiến trình tạo một bản sao dự phòng diễn ra nhanh hơn.

- Các tác vụ sao lưu dự phòng theo lịch trình được thiết kế để thực hiện khi không có ai đang sử dụng máy tính.
- Windows 9x và Windows NT đều hỗ trợ một tiện ích Backup vốn có thể được sử dụng với nhiều loại băng từ khác nhau. Ngoài ra, Backup của Windows 9x còn có thể sử dụng các đĩa mềm.
- Khi chuẩn bị cho việc phục hồi dữ liệu từ một thảm họa, bạn hãy giữ cẩn thận các bản ghi chép về các bản sao lưu và định kỳ kiểm tra phương pháp sao lưu của bạn để bảo đảm chắc rằng bạn có thể phục hồi dữ liệu thành công khi cần.

5 Các thuật ngữ quan trọng

Antivirus (AV) software (Phần mềm chống virus) – Các chương trình tiện ích ngăn cản sự lây nhiễm, hoặc quét một hệ thống để phát hiện và loại trừ các virus. McAfee Associates VirusScan và Norton AntiVirus là hai gói phần mềm chống virus được sử dụng phổ biến.

Boot sector virus (Virus cung khởi động) – Chương trình lây nhiễm có khả năng thay thế chương trình khởi động bằng một phiên bản sửa đổi, bị lây nhiễm của các tiện ích lệnh khởi động, đôi khi gây ra các sự cố khởi động và các sự cố truy lục dữ liệu.

Child, parent, grandparent backup method (Phương thức sao lưu con, cha, ông nội) – Là kế hoạch sao lưu dự phòng và tài sử dụng băng từ hoặc các đĩa tháo lắp bằng cách luân chuyển chúng sau mỗi tuần *(con)*, mỗi tháng *(cha)* và mỗi năm *(ông nội)*.

Data cartridge – Một kiểu phương tiện băng từ thường được sử dụng cho công tác sao lưu. Các data cardtridge chuẩn có kích thước

4×6×⅝ inch. Một minicartridge có kích thước chỉ 3¼×2½×⅜ inch.

Differential backup (Sao lưu có phân biệt) – Sao lưu chỉ các tập tin đã thay đổi hoặc đã được tạo ra kể từ lần sao lưu *đầy đủ* sau cùng. Khi phục hồi các dữ liệu, chỉ hai bản sao lưu được cần tới: bản sao lưu đầy đủ và bản sao lưu có phân biệt sau cùng.

Disk duplexing (Tạo song công đĩa) – Sự cải tiến của tạo gương đĩa, qua đó các dữ liệu được ghi vào hai hoặc nhiều ổ đĩa và mỗi ổ đĩa cứng có riêng card điều hợp. Kỹ thuật này cung cấp sự bảo vệ tốt hơn so với tạo gương đĩa.

Disk mirroring (Tạo gương đĩa) – Chiến lược qua đó cùng các dữ liệu được ghi vào hai ổ đĩa cứng trong một máy tính, nhằm bảo vệ dữ liệu khi xảy ra sự cố hư hỏng ổ đĩa cứng. Kỹ thuật tạo gương đĩa chỉ sử dụng một bộ điều hợp đơn cho hai ổ đĩa.

Disk striping (Tạo dải đĩa) – Xem nhiều ổ đĩa cứng như là một ổ đĩa luận lý đơn. Các dữ liệu được ghi ngang qua các ổ đĩa này dưới dạng các đoạn nhỏ, nhằm cải thiện hiệu suất và dung lượng đĩa luận lý, khi chẵn lẻ cũng được sử dụng, nhằm cung cấp khả năng kháng lỗi. RAID 5 sử dụng kỹ thuật tạo dải đĩa kèm theo một ổ đĩa bổ sung dành cho các thông tin chẵn lẻ.

Encrypting virus (Virus mã hóa) – Virus có khả năng tự biến đổi chính nó thành một chương trình không có khả năng nhân bản

nhằm tránh sự phát hiện. Virus này sẽ tự biến đổi trở lại thành một chương trình có khả năng nhân bản để lan truyền.

Fault tolerance (Kháng lỗi) – Mức độ mà một hệ thống có thể chịu đựng được các hư hỏng. Việc bổ sung các thành phần phụ trợ, chẳng hạn như trong kỹ thuật tạo gương đĩa hay tạo song công đĩa, là một cách để tích hợp khả năng kháng lỗi cho hệ thống.

File virus (Virus tập tin) – Một loại virus có khả năng chèn mã virus vào một chương trình thi hành được và có thể lan truyền bất kỳ khi nào chương trình này được truy xuất.

Full backup (Sao lưu dự phòng đầy đủ) – Một tác vụ sao lưu dự phòng trọn vẹn, qua đó tất cả các tập tin trên ổ đĩa cứng sẽ được sao lưu mỗi khi thủ tục sao lưu này được thực hiện. Đây là phương thức sao lưu an toàn nhất, nhưng mất thời gian nhất.

Incremental backup (Sao lưu dự phòng tăng dần) – Một phương thức sao lưu tiết kiệm thời gian vốn chỉ sao lưu các tập tin đã thay đổi hoặc vừa được tạo ra kể từ lần sao lưu đầy đủ *hoặc* sao lưu tăng dần sau cùng. Nhiều bản sao lưu tăng dần có thể được cần tới khi phục hồi các dữ liệu đã mất.

Infestation (Sự phá hoại) – Bất kỳ chương trình không mong muốn nào được truyền vào một máy tính mà người dùng không nhận biết và được thiết kế để thực hiện nhiều mức độ phá hoại dữ liệu và phần mềm khác nhau. Có rất

nhiều hình thức phá hoại khác nhau, bao gồm các virus, các Trojan horse, các sâu máy tính và các chương trình bom định giờ (*time bom*), ...vv.

Macro – Là dãy lệnh nhỏ được chứa bên trong một tài liệu và có thể được tự động thi hành khi tài liệu này được nạp, hoặc được thi hành sau này bằng cách sử dụng một phím nóng định trước.

Macro virus (Virus macro) – Một loại virus có khả năng ẩn náu trong các macro của một tập tin tài liệu. Thông thường, các virus không lưu trú trong các tập tin dữ liệu hoặc các tập tin tài liệu.

Material safety data sheet (MSDS) – Là tài liệu cung cấp các thông tin về cách xử lý các chất, chẳng hạn như các dung môi hóa chất, bao gồm các dữ liệu vật lý, tính độc hại, các ảnh hưởng đến sức khỏe, các thủ tục sơ cứu, lưu trữ, thải loại.

Memory-resident virus (Virus thường trú bộ nhớ) – Một loại virus có thể ẩn nấp trong bộ nhớ, cho dù sau khi chương trình chủ đã được chấm dứt.

Minicartridge – Một cartridge ổ băng từ vốn có kích thước chỉ 3¼×2½×⅜ inch. Kích thước này đủ nhỏ để cho phép hai ổ băng lắp vừa vào một hộc chứa 5½ inch của khung máy PC.

Multipartite virus (Virus đa phần) – Là sự kết hợp giữa một virus cung khởi động và một virus tập tin. Nó có thể ẩn náu trong hai loại chương trình này.

Non-memory-resident virus (Virus không thường trú bộ nhớ) – Một loại virus sẽ tự động kết thúc khi chương trình chủ được đóng lại. So sánh với *memory-resident virus.*

Polymorphic virus (Virus đa hình) – Một loại virus có khả năng thay đổi các đặc điểm tiêu biểu của nó khi nó tự nhân bản. Sự biến hóa theo cách này khiến cấc phần mềm diệt virus khó phát hiện được sự hiện diện của virus.

Quarter-Inch Committee hay **quarter-inch cartridge (QIC)** – Tên gọi của một phương thức được chuẩn hóa được sử dụng để ghi các dữ liệu vào băng từ. Các bản sao lưu dự phòng được tạo ra bằng tiện ích Microsoft Backup của Windows 9x có phần mở rộng là *.qic.*

RAID (Redundant array of inexpensive disks: Mảng thừa gồm các đĩa rẻ tiền, hoặc Redundant array of independent disks: Mảng thừa gồm các đĩa độc lập) – Các phương thức định cấu hình nhiều ổ đĩa cứng để lưu trữ các dữ liệu nhằm gia tăng dung lượng volume luận lý và cải thiện hiệu suất và nhằm bảo đảm nếu một ổ đĩa cứng bị hư hại, các dữ liệu vẫn khả dụng từ một ổ đĩa khác.

Retension (Làm căng dây băng) – Là một hình thức bảo dưỡng băng từ bằng cách quay tới rồi quay lui băng từ nhằm loại trừ những chỗ bị chùng trên băng từ.

Sequential access (Truy xuất tuần tự) – Phương thức truy xuất dữ liệu được các ổ băng từ sử dụng, qua đó các dữ liệu được ghi hoặc

được đọc một cách tuần tự từ phần đầu tới phần cuối của băng từ hoặc cho tới khi tìm thấy các dữ liệu muốn tìm.

Stealth virus (Virus tàng hình) – Một loại virus chủ động che dấu chính nó bằng cách tạm thời di chuyển bản thân ra khỏi một tập tin bị lây nhiễm vốn sắp được truy xuất, rồi sau đó giấu một bản sao của chính nó ở một nơi nào đó trên ổ đĩa cứng.

Trojan horse (Ngựa thành Troa) – Một dạng chương trình phá hoại có khả năng ẩn náu hoặc trá hình như là một chương trình hữu ích, nhưng được thiết kế để gây ra những thiệt hại tại một thời điểm sau này.

Virus – Chương trình đôi khi có một thời kỳ ủ bệnh, có tính lây lan và được dự tính để thực hiện các hành động phá hoại. Một chương trình virus có thể phá hủy các dữ liệu và các chương trình khác hoặc phá hoại cung khởi động của một đĩa.

Virus signature (Dấu hiệu nhận dạng của virus) – Các đặc điểm tiêu biểu của một virus cụ thể. Thông thường, các cập nhật về dấu hiệu nhận dạng của virus mới cho phần mềm diệt virus có thể được nạp xuống hàng tháng từ Internet.

Worm (Sâu máy tính) – Là chương trình phá hoại được thiết kế để liên tục sao chép chính nó vào bộ nhớ, lên không gian đĩa, hoặc lên một mạng cho tới khi chỉ còn lại rất ít bộ nhớ hoặc không gian đĩa.

6 Các câu hỏi ôn tập

1. Bạn hãy liệt kê một hoặc hai biện pháp bảo dưỡng phòng ngừa có thể được thực hiện để bảo vệ mỗi thứ sau: khung máy tính, CMOS setup, ổ đĩa mềm, ổ đĩa cứng, bàn phím, con chuột, máy in và phần mềm.
2. Bạn hãy liệt kê ba điều cần thực hiện trước khi di chuyển một hệ thống máy tính.
3. Một bộ pin của một máy tính notebook phải được loại thải như thế nào? Một monitor bị hỏng? Một cartridge mực toner của một máy in laser?
4. Bạn hãy liệt kê và mô tả ba dạng virus khác nhau.
5. Bạn hãy liệt kê ba cách virus lây nhiễm vào hệ thống.
6. Bạn hãy liệt kê ba cách ngăn ngừa virus.

7. Bạn hãy liệt kê các triệu chứng hoặc các sự cố chỉ ra rằng có thể có sự hiện diện của virus.

8. Kỹ thuật tạo gương đĩa khác với kỹ thuật tạo song công đĩa ra sao?

9. Khi một ổ đĩa cứng có thể được tháo ra và một ổ đĩa cứng khác được lắp vào mà không cần tắt nguồn một máy tính, điều này được gọi là

10. Bạn hãy giải thích rõ cách hoạt động của phương thức con, cha, ông nội như là một kế hoạch dành cho việc tái sử dụng các băng từ.

11. Các thủ tục sao lưu có phân biệt khác với các thủ tục sao lưu đầy đủ ra sao, và mỗi kiểu sao lưu này có những ưu điểm nào?

12. Các thủ tục sao lưu có phân biệt khác với các thủ tục sao lưu tăng dần ra sao, và mỗi kiểu sao lưu này có những ưu điểm nào?

13. Tại sao ta lại cần phải *"làm căng dây băng"* cho một băng từ sao lưu?

14. Bạn cho biết hai lý do khiến bạn muốn định lịch trình để công việc sao lưu ổ đĩa cứng diễn ra vào ban đêm.

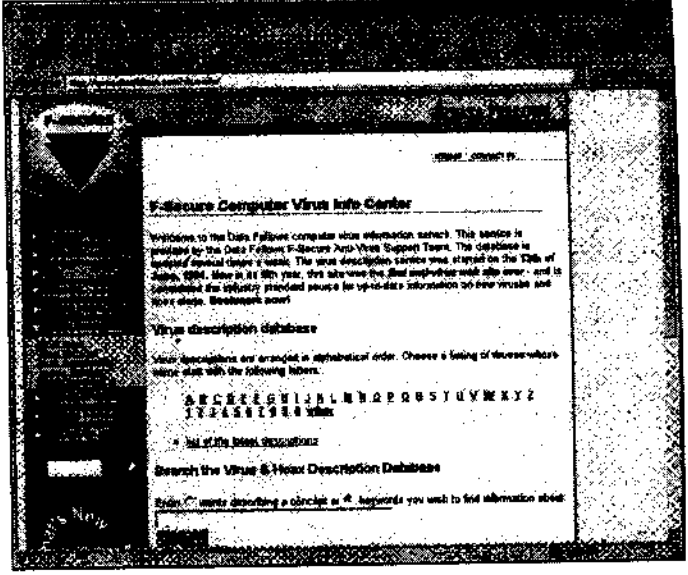
15. Tại sao bạn cần phải xác nhận rằng kế hoạch phục hồi sau thảm họa của bạn hoạt động và ghi kế hoạch này ra giấy?

7 Các dự án

Sử dụng Internet để tìm hiểu về các virus

Trên Web, nguồn thông tin kinh điển về các virus là Data Fellows. Bạn hãy đi tới Web site www.datafellows.com/vir-info/ *(xem hình 7-1)* để biết các thông tin về các virus; các virus trong đó được liệt kê theo thứ tự chữ cái kèm theo các phần mô tả hoàn chỉnh, kể cả bất kỳ nguồn nào được biết tới của virus. Bạn hãy in ra một bản mô tả về ba virus từ Web site này:

1. Một virus phá hủy các dữ liệu trên một ổ đĩa cứng.
2. Một virus vô hại chỉ hiển thị rác rưởi lên màn hình.
3. Một virus ẩn náu trong một cung khởi động.



Hình 7-3 Web site Data Fellows cung cấp các thông tin hoàn chỉnh về các virus.

Nạp phần nâng cấp mới nhất cho phần mềm diệt virús

Nếu đang sử dụng một phần mềm diệt virus, bạn hãy nạp xuống danh sách định nghĩa virus mới nhất từ Internet. Ví dụ, đối với Norton AntiVirus, bạn làm theo các hướng dẫn sau:

1. Đăng nhập vào site NAV:
   www.symantec.com/avcenter
2. Nhấn nút **Dowload Updates**, sau đó trả lời các câu hỏi cần thiết, chẳng hạn:

Product: NAV for Windows 95
Language: English, US
Operating Environment: Windows 95

3. Kế đó bạn làm theo các hướng dẫn để nạp xuống phần cập nhật và danh sách nhận dạng mới nhất dành cho phiên bản phần mềm diệt virus cụ thể của bạn.

4. Trong khi đang trực tuyến, bạn hãy xem thử trên site này có bất kỳ thông tin nào về các trò đánh lừa virus *(virus hoax)* hay không. Bạn hãy tạo một danh sách gồm các trò đánh lừa virus được liệt kê trong site này.

❖ **Sử dụng Nuts & Bolts, phần mềm McAfee VirusScan**

Bằng phần mềm McAfee VirusScan, bạn hãy quét một đĩa mềm để tìm virus.

❖ **Nghiên cứu thị trường ổ băng từ**

Bạn hãy điền vào bảng sau đây hai ổ băng từ mà bạn muốn mua, nhằm đánh giá hai ổ băng này. Ổ băng nào có vẻ thích hợp hơn cho một máy PC độc lập vốn được sử dụng nhiều cho việc nhập dữ liệu và cần được sao lưu dữ liệu hàng ngày? Tại sao?

Tên sản phẩm		
Hãng sản xuất		
Giá		
Bộ tăng tốc (có/không/tùy chọn)		
Phần mềm đi kèm		
Kiểu (lắp trong/lắp ngoài)		
Bảo hành (1 năm/2 năm/ suốt thời gian sử dụng)		
Các định dạng băng từ được hỗ trợ		
Dung lượng tối đa (đồng thời chỉ rõ định dạng băng từ cần thiết để phù hợp dung lượng tối đa này, ví dụ: 4.4GB khi sử dụng QIC-3020).		
Các kiểu cartridge được hỗ trợ.		

❖ Sử dụng Windows 98 để sao lưu các tập tin và các folder

Bài tập này được thiết kế để giúp bạn luyện tập kỹ năng sử dụng tiện ích Microsoft Backup của Windows 98 và để giúp bạn thấy được cách tiện ích Backup quản lý nhiều tình huống ra sao.

Phần 1

1. Bằng cách sử dụng Windows Explorer, bạn hãy tạo ra một folder có tên là Backtest trên một ổ đĩa cứng.
2. Sử dụng Explorer để tìm một tập tin .BAT, rồi sao chép nó vào folder mới này. Sau đó bạn sao chép tiếp hai tập tin khác vào folder Backtest. Tạo một folder con có tên là Subfolder trong folder Backtest rồi sao chép một tập tin thứ tư vào C:\Backtest\Subfolder.
3. Nhấp nút chuột phải vào tập tin .BAT để đổi tên nó thành Overwrite.txt. Nhấp chuột phải vào tập tin thứ hai rồi đổi tên nó thành Delete.txt. Đổi tên tập tin thứ ba thành NoChange.txt. Bốn tập tin này hiện giờ có thể được để yên. Bạn hãy sử dụng Explorer và ghi chép lại kích thước của các tập tin này trước khi thực hiện việc sao lưu.
4. Nhấn nút **Start → Programs → Accessories → System Tools**, rồi chọn **Backup**.
5. Sử dụng các hướng dẫn trong sách này để sao lưu folder Backtest vào một đĩa mềm. Sau đó bạn sử dụng Explorer và so sánh kích thước của tập tin sao lưu với các kích thước tập tin nguyên thủy. Chúng khác nhau ra sao?

6. Xóa tập tin **Delete.txt**. Biên tập và thay đổi nội dung của tập tin Overwrite.txt. Không thực hiện các thay đổi với tập tin NoChange.txt. Sau đó bạn xóa **Subfolder**.

7. Bằng cách sử dụng Microsoft Backup, bạn hãy phục hồi các tập tin từ bản sao dự phòng vào folder nguyên thủy của chúng.

   a. Backup đã làm gì với tập tin Delete.txt?

   b. Backup đã làm gì với tập tin Overwrite.txt?

   c. Backup đã làm gì với tập tin NoChange.txt?

   d. Backup đã làm gì với Subfolder bị mất và tập tin bị mất?

   e. Tên của tập tin sao lưu nằm trên đĩa mềm là gì?

   f. Tên và đường dẫn tới tập tin nhật ký lỗi *(error log)* được Backup tạo ra là gì?

   g. Bạn hãy in tập tin nhật ký lỗi này ra giấy.

Phần 2

1. Bạn hãy sử dụng Windows Explorer để sao chép folder Backtest vào một đĩa mềm thứ hai.

2. Xóa tất cả các tập tin trong folder Backtest trên ổ đĩa cứng.

3. Sử dụng Windows Explorer để sao chép ba tập tin này trở lại folder Backtest.

4. Một lần nữa bạn hãy xóa các tập tin trong folder Backtest trên ổ đĩa cứng.

5. Mở Recycle Bin rồi phục hồi ba tập tin này trở lại folder Backtest, bằng cách chọn chúng rồi sử dụng menu File → tùy chọn Restore. Chúng có quay trở lại đúng folder ban đầu không?

6. Một lần nữa, bạn hãy xóa các tập tin trong folder Backtest trên ổ đĩa cứng.

7. Một lần nữa chọn các tập tin này trong Recycle Bin, nhưng lần này chọn **File → Delete**. Bạn có thể phục hồi các tập tin này được không?

- HẾT -

Chịu trách nhiệm xuất bản

CÁT VĂN THÀNH

Ban biên dịch : **CADASA**

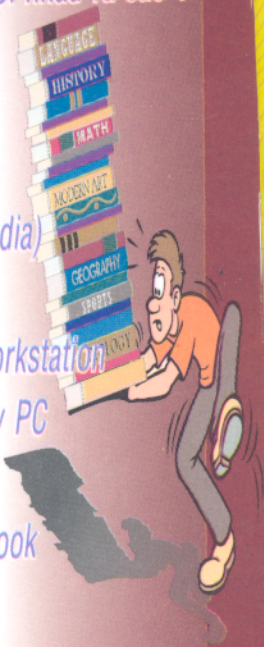
Trình bày bìa : **QUỐC KHÁNH**

Sửa bản in : **ĐỖ THỊ CHÍNH**

In 1.000 cuốn, khổ 12 x 20cm, tại Nhà in Thanh Niên, 62 Trần Huy Liệu – Q. PN. Giấy TNKHXB số : 99/XB – QLXB do Cục xuất bản cấp ngày 17 tháng 1 năm 2001. KHXB số 124-99/XB-QLXB do NXB Thống Kê cấp ngày 28 tháng 3 năm 2001. In và nộp lưu chiểu tháng 7 năm 2001.

Những điều cốt yếu mà người sử dụng máy vi tính cần phải biết (Ban biên dịch CADASA)

1- Máy tính hoạt động như thế nào ?
2- Phần mềm và phần cứng làm việc với nhau ra sao ?
3- Tìm hiểu về quản lý bộ nhớ máy PC
4- Các ổ đĩa mềm
5- Các khái niệm cơ bản về ổ đĩa cứng
6- Công nghệ đa phương tiện (Multimedia)
7- Bo mạch hệ thống của máy PC
8- Tìm hiểu và hỗ trợ Windows NT Workstation
9- Chọn mua hoặc tự lắp ráp một máy PC
10- Mạng và INTERNET
11- Các máy in và các máy tính Notebook
12- Lắp đặt và hỗ trợ ổ đĩa cứng
13- Hỗ trợ các thiết bị nhập xuất
14- Các kỹ năng giải quyết sự cố thường gặp trên máy PC
15- Việc truyền thông qua đường dây điện thoại của máy PC



Tổng phát hành :
Nhà Sách CADASA
16 Võ Văn Tần, Q.3 Tp.HCM
ĐT: 9301906 - 9301907 * Email: cadasa@hcm.vnn.vn

0 9 8 1 2 5 1
15.000đ