

# PHẦN MỀM NORTON COMMANDER & VIRUS TIN HỌC

ThS. LÊ ANH TUẤN

--- oOo ---

I. PHẦN MỀM TIỆN ÍCH NORTON COMMANDER	2
1. Giới thiệu	2
2. Các thao tác căn bản trong NC	3
II. VIRUS TIN HỌC VÀ CÁCH PHÒNG CHỐNG	6
1. Virus tin học là gì?	6
2. Cách phòng chống Virus	7
3. Các chương trình kiểm tra và diệt Virus thông dụng	9

---

---

# PHẦN MỀM NORTON COMMANDER & VIRUS TIN HỌC

ThS. LÊ ANH TUẤN

--- oOo ---

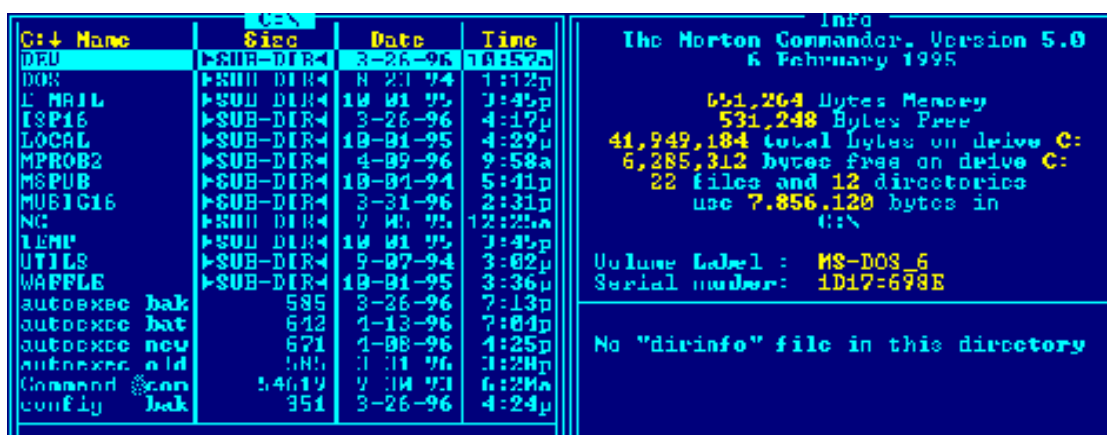
## I. PHẦN MỀM TIỆN ÍCH NORTON COMMANDER

### 1. Giới thiệu

Norton Commander (viết tắt là NC) là một trong những chương trình tiện ích chạy trong môi trường DOS. NC được sử dụng nhiều ở Việt nam và nhiều quốc gia khác. Ưu điểm của NC là đơn giản, dễ sử dụng và không chiếm nhiều không gian, bộ nhớ mà vẫn đủ các chức năng cơ bản và nâng cao. Sử dụng được NC, ta dễ dàng khai thác các trình ứng dụng tương tự như Norton Utilities, PC Tools, Xtree Gold, File Manager trong Windows, v.v...

Phiên bản Norton Commmander được dùng phổ biến hiện nay tại Việt nam là NC version 4.0 và version 5.0. Chúng ta có thể cài đặt toàn bộ hay một phần chương trình. Hai file quan trọng nhất của NC là NC.EXE và MCMAIN.EXE. Thường NC được cài trong phần Path của Autoexec.bat.

Để đi vào NC, từ dấu nhắc của DOS, ta gõ NC rồi nhấn Enter. Khi đó, trên màn hình sẽ xuất hiện hai cửa sổ gọi là Panels, như sau:



Hình 1: Panel làm việc của Norton Commander

Panel có viền sáng được gọi là cửa sổ làm việc hiện thời. Muốn chuyển cửa sổ làm việc ta dùng phím Tab. Trên các panels, có thể đọc được các thông tin:

- Nội dung của các thư mục và files hiện thời
- Cấu trúc thư mục trên đĩa
- Các thông tin về chương trình, bộ nhớ, file trống trên đĩa hiện hành
- Dòng cuối cùng là các "phím nóng" (HotKey) chỉ dẫn các thao tác nhanh.

F1 Help	:	Hướng dẫn
F2 Menu	:	Gọi Thực đơn của người sử dụng
F3 View	:	Xem nội dung file có vệt sáng hiện hành
F4 Edit	:	Soạn thảo, sửa chữa nội dung file
F5 Copy	:	Sao chép files sang nơi khác
F6 RenMov	:	Di chuyển files hoặc đổi tên
F7 Mkdir	:	Tạo thư mục con
F8 Delete	:	Xóa files hoặc thư mục
F9 PullDn	:	Mở menu làm việc của NC
F10 Quit	:	Thoát khỏi chương trình

Tổ hợp phím:

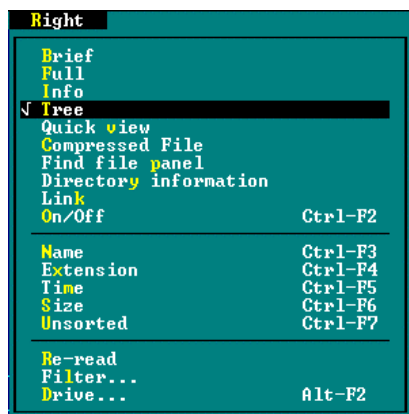
Ctrl + F1	:	dùng để ẩn/ hiện Panel trái
Ctrl + F2	:	dùng để ẩn/ hiện Panel phải
phím Tab	:	chuyển đổi vệt sáng giữa các cửa sổ

## 2. Các thao tác căn bản trong NC



### *Xem cây thư mục*

Nhấn F9 - ta có dòng Menu ở hàng trên, vào Right (Left) nếu muốn cây thư mục xuất hiện ở Panel Phải (Trái tương ứng), gõ Enter. Một bảng như sau xuất hiện:

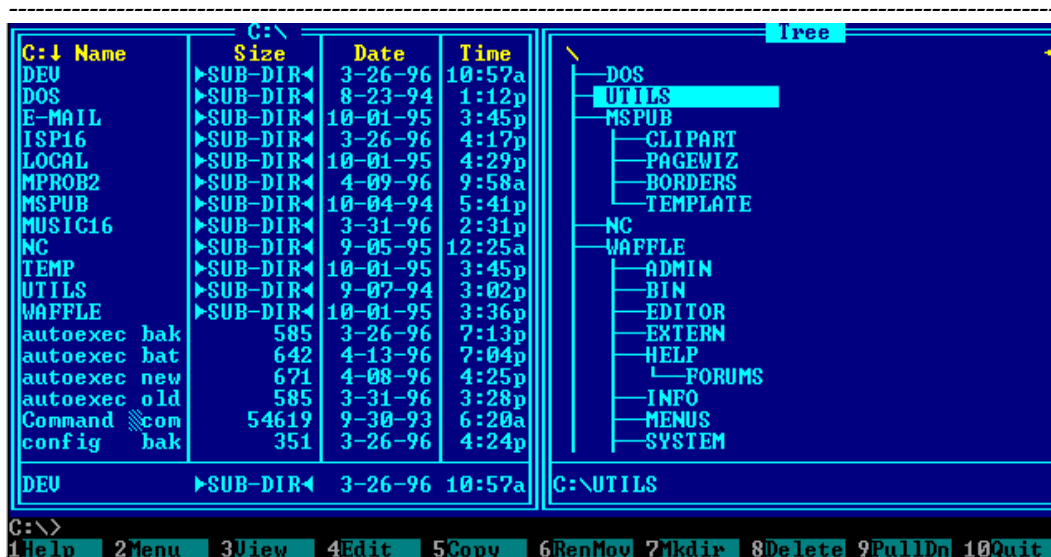


Trong bảng này có nhiều option cho ta lựa chọn, muốn vào mục nào ta kéo vệt sáng (highlight) xuống dòng đó (hoặc nhấn phím chữ có đánh dấu màu) rồi nhấn Enter.

Ví dụ, muốn xem cây thư mục (Tree) thì ta kéo vệt sáng xuống vị trí Tree (hoặc nhấn phím T) rồi nhấn Enter.

Hình 2: Option của Thực đơn Right

Trên màn hình sẽ cho ta hình ảnh sau:



Hình 3: Hình ảnh cây thư mục ở Panel phải

⇒ *Chọn thư mục làm việc hoặc file*

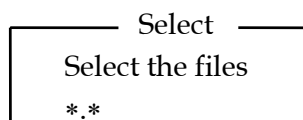
Thư mục (Directory) và file là 2 đối tượng chính của NC. Thư mục thể hiện bằng chữ in hoa, trong khi file thể hiện bằng chữ thường. Ta có thể dùng các phím di chuyển trên bàn phím như ↑, ↓, PageUp, PageDown để đi đến các thư mục và file để chọn. Vệt sáng nằm ở thư mục hay file nào là NC đang làm việc tại thư mục hay file đó. Khi đưa vệt sáng đến các files có phần mở rộng là .BAT, .COM và .EXE và nhấn Enter thì NC sẽ thực hiện ngay lệnh đó trong môi trường của nó. Khi hoàn tất việc thực thi các file đó, chương trình quay trở về NC.

⇒ *Chọn một nhóm files*

Muốn chọn một nhóm files hoặc từng thư mục, ta di chuyển vệt sáng đến các files hoặc thư mục đó và gõ vào nút <Insert> trên bàn phím để chọn, khi đó tên file đã chọn sẽ đổi sang màu sáng trên màn hình panel. Trường hợp muốn hủy việc chọn lựa, ta cũng di chuyển vệt sáng đến chỗ file cần hủy chọn và nhấn <Insert> một lần nữa, khi đó màu sáng của file biến mất.

⇒ *Chọn một nhóm hoặc tất cả các files*

Muốn chọn tất cả các files trong một panel hiện hành hoặc một nhóm các files dựa trên ký hiệu đại diện, ta gõ nút <+> ở vùng phím số, khi đó trên màn hình sẽ xuất hiện hộp thoại:



Khi gõ Enter, tất cả các file trong panel sẽ được chọn và đồng loạt đổi sang màu sáng. Nếu ta chỉ muốn chọn một nhóm tập tin có cùng một kiểu đặt tên nào đó thì có thể sử dụng các ký tự đại diện như ? hay \* và gõ Enter khi đã định xong.

### ⇒ Sao chép, di chuyển và xóa files

Khi các nhóm file đã được chọn thì ta có thể sao chép, di chuyển hoặc xóa bỏ tùy ý. Ở chế độ mặc định, files hoặc thư mục sẽ theo câu lệnh mà sao chép hoặc di chuyển sang thư mục đối diện. Có thể dùng các thao tác sau :

Nhấn F5 (Copy)	:	sao chép files qua thư mục khác
Nhấn F6 (RenMov)	:	đổi tên hay di chuyển files
Nhấn F8 (Delete)	:	xóa files hay thư mục

Để chọn thư mục đích, ta dùng phím Alt-F10 và các phím mũi tên ↑ và ↓ để chỉ định đường dẫn hay gõ trực tiếp tên đường dẫn.

Để bảo vệ files khi bị xóa hoặc chép đè lên, NC luôn đưa ra các thông báo cần thiết để người sử dụng khẳng định lại ý đồ của mình.

### ⇒ Tạo thư mục

Dùng phím F7 để tạo thư mục (Make Directory), sau đó gõ tên thư mục và nhấn Enter. Trường hợp, gõ tên thư mục mà không gõ đường dẫn thì NC mặc nhiên tạo thư mục con trong thư mục của panel hiện hành.

### ⇒ Chuyển thư mục

Cách đơn giản nhất là đưa vệt sáng đến thư mục cần chuyển và ấn Enter.

Tổ hợp phím <Alt + F10> sẽ hiện thị cây thư mục và ta dùng các phím mũi tên để di chuyển đến thư mục cần chuyển và gõ Enter.

### ⇒ Chuyển ổ đĩa

Dùng tổ hợp phím <Alt + F1> và các phím mũi tên để chọn ổ đĩa thích hợp và gõ Enter, khi đó nội dung ổ đĩa vừa chọn sẽ xuất hiện ở panel bên trái. Khi dùng tổ hợp phím <Alt + F2> thì nội dung ổ đĩa sẽ ở panel phải màn hình.

### ⇒ Tìm kiếm file

Để tìm kiếm nhanh một file nào đó trong thư mục hiện hành, ta nhấn giữ phím Alt và đồng thời gõ các ký tự đầu tiên của tên file. Nếu cho các ký tự đầu của tên file càng nhiều thì mức độ tìm kiếm càng nhanh.

Trường hợp không rõ thư mục chứa file hoặc tên file nằm ở các thư mục khác nhau, ta có thể sử dụng tổ hợp phím <Alt + F7>, sau đó gõ tên file cần tìm và nhấn Enter.

Khi gõ tên file ta có thể sử dụng các ký tự ? hoặc \* như trên DOS. NC sẽ tìm kiếm cho đến khi ta chọn **Stop** và Enter để ngưng. Các phím mũi tên ↑ và ↓ được dùng để chọn một file nào đó trong nhóm vừa tìm thấy. Nếu chọn tiếp **ChDir** và Enter, chương trình sẽ đưa ta vào làm việc với thư mục chứa file vừa tìm được. Chức năng “**New search**” của NC cho phép bắt đầu lại việc tìm kiếm. Chức năng “**Change drive**” dùng để chuyển ổ đĩa cần tìm kiếm.

⇒ **Cài đặt thuộc tính cho files**

Trong MS-DOS, các files có thể có các thuộc tính (attributes) sau :

Archive	:	thuộc tính lưu trữ
Read Only	:	thuộc tính chỉ đọc
Hidden	:	thuộc tính ẩn
System	:	thuộc tính hệ thống

NC có thể giúp ta thay đổi thuộc tính cho file hoặc một nhóm file.

- Đánh dấu các files cần đặt/hủy thuộc tính
- Nhấn lần lượt phím F9 và các thực đơn con /File/File attributes. Hộp thoại như sau sẽ xuất hiện:

Attributes		
Change file attributes		
Set	Clear	
[ ]	[ ]	Read only
[ ]	[ ]	Archive
[ ]	[ ]	Hidden
[ ]	[ ]	System
[Set]		[Cancel]

- Dùng các phím mũi tên và phím chọn SPACE để đánh dấu. Cột set là thiết lập, cột clear là hủy bỏ thuộc tính.
- Chọn chức năng set ở hàng dưới cùng để thực hiện lệnh.

## II. VIRUS TIN HỌC VÀ CÁCH PHÒNG CHỐNG

### 1. Virus tin học là gì ?

Virus tin học hay còn gọi là virus máy tính (*computer virus*) là một đoạn chương trình ẩn, có kích thước nhỏ, có khả năng tự sao chép, sinh sôi nảy nở như một virus sinh học, lây lan nhanh và có thể gây nguy cơ phá hoại các phần mềm hệ của hệ điều hành, xóa một phần hay toàn bộ các tập tin dữ liệu, tạo ra các tập tin vô nghĩa chiếm lấy không gian bộ nhớ của máy, hoặc chỉ đơn thuần trêu chọc hay đe dọa người sử dụng, ...

Thoạt đầu, virus tin học là vũ khí của những người viết phần mềm muốn bảo vệ sản phẩm của họ chống việc sao chép bất hợp pháp. Sau một số người tạo ra các virus khác nhằm mục đích phá hoại hay đơn thuần chỉ để tự khẳng định mình và “cấy” vào trong các máy khác gây lây nhiễm trên một diện rộng. Năm 1987, virus Lehigh lần đầu tiên được phát hiện trên máy IBM PC. Cùng lúc đó, virus Brain từ Pakistan xâm nhập vào các trường Đại học của Mỹ. Một virus khác từ Đại học Hebrew, Israel cũng xuất hiện. Từ đó đến nay, hàng ngàn chủng loại virus được thông báo phát hiện gây phá hoại, tê liệt nhiều hệ thống máy trên toàn thế giới gây thiệt hại nhiều triệu dollars.

Virus được chia thành 2 nhóm chính:

+ **B-virus** (Boot-virus) : là các virus chuyên tấn công lên các Boot sector hay Master boot, điển hình như : Brain, Nops, Clock, Stone, Sài Gòn 01/91, ...

+ **F-virus** (File-virus) : là các virus chỉ tấn công lên các file .COM và .EXE, điển hình như : Friday 13th, Yankee Doodle, DataLock, Keypress, VN01, ... Hay một số chuyên phá hoại các file có phần mở rộng .DB\* của các chương trình dBase, FoxBase hay chuyên phá hoại các file văn bản có phần mở rộng là .DOC như virus Concept, Macro, ....

Ngoài ra, một số virus vừa mang cả 2 tính phá hoại Boot và File như virus Dark Avenger .... Người ta còn lo ngại một số người đang cố tình tạo ra các virus còn có thể xâm nhập vào các hệ thống mạng máy tính qua đường truyền thư điện tử (E-mail) hoặc mạng Internet, mạng của các ngân hàng lớn gây đảo lộn các số liệu tài khoản, hoặc xâm nhập vào các hệ thống máy tính quân sự tạo nên những báo động giả rất nguy hiểm ...

Hiện nay, một số nước đã ra những điều luật xem những kẻ cố tình tạo ra các virus tin học phá hoại, lấy cắp mật mã, ... (gọi chung là những kẻ tin tặc - *hackers*) như là những tội phạm hình sự.

## 2. Cách phòng chống virus

- Không chép các chương trình mà bạn không rõ nguồn gốc và đặc biệt chưa qua thủ tục kiểm tra virus.
- Các file dữ liệu quan trọng cần phải được COPY lưu trữ dự phòng và có thể dùng các chương trình PKZIP.EXE hay ARJ.EXE .... để nén lại, tiết kiệm đĩa.
- Có thể sử dụng nhiều phần mềm BACKUP để lưu.
- Dùng lệnh BACKUP và RESTORE của DOS như sau:

Mẫu lệnh:     **BACKUP source destination - drive : [Option]**

Các option là:

/S : lưu trữ cả thư mục con  
/M : chỉ lưu các file bị đổi so với lần lưu cuối cùng  
/A : lưu thêm các file vào đĩa lưu trữ  
/F:[size] : chỉ định kích thước đĩa cần định dạng  
/D:date : Chỉ lưu trữ các file bị thay đổi kể từ ngày ...  
/T:time : Chỉ lưu trữ các file bị thay đổi kể từ thời điểm ...  
/L:[drive:][path]logfile ] : Tạo nên một file nhật ký vào đầu vào để ghi các thao tác lưu trữ

Ví dụ muốn lưu trữ thư mục DOS và các thư mục con của nó vào ổ B, ta gõ:

```
C:\>BACKUP C:\DOS B:/S
```

Máy sẽ thông báo dòng tin:

```
Insert backup diskette 01 in drive B :  
WARNING ! Files in the target drive  
B:\ root directory will be erased  
Press any key to continue ...
```

Sau khi lưu trữ vào B, ta có thể xem trên đĩa có nội dung:

```
C:\>dir B:  
Volume in drive B is BACKUP 001  
Volume Serial Number is 001F- 012B  
Directory of B:\  
BACKUP      001    1,432,246    04-20-96    6:20p  
1 file(s)    1,432,246 bytes  
              7,754 bytes free
```

Chương trình RESTORE là chương trình khôi phục các file trong BACKUP

Mẫu lệnh như sau:

```
RESTORE drive1 : drive2 : [path[filename]] [Option]
```

trong đó: drive1 : chỉ ổ đĩa chứa file backup  
drive2:[path[filename]] : chỉ rõ các file cần phục hồi

các options là:

/S : Phục hồi tất cả file trong các thư mục con trong đường dẫn  
/P : Báo cho ta biết trước khi khôi phục các read-only-files hoặc các file đã thay đổi từ lần backup cuối cùng (nếu các thuộc tính phù hợp được thiết lập).  
/M : Chỉ khôi phục các file có thay đổi kể từ lần backup cuối  
/N : Chỉ khôi phục các file không có trên đĩa nhận



/D : Hiển thị các file trên đĩa backup phù hợp với đặc tả  
/B:date: Chỉ khôi phục các file có thay đổi kể từ trước ngày ....  
/A:date: Chỉ khôi phục các file có thay đổi kể từ sau ngày ....  
/E:time: Chỉ khôi phục các file có thay đổi kể từ trước thời điểm ....  
/L:time: Chỉ khôi phục các file có thay đổi kể từ sau thời điểm ....

Với ví dụ trên, muốn khôi phục thư mục DOS, ta gõ:

```
C:\>RESTORE B: C: /S <Enter>
Insert backup diskette 01 in drive B :
Press any key to continue ...
*** Files were backed up 04 - 20 - 96 ***
*** Restoring files from drive B : ***
Diskette : 01
```

Chú ý: Chúng ta không cần chỉ định rõ thư mục con.

### 3. Các chương trình kiểm tra và diệt virus thông dụng

Ta cần có một số đĩa khác phòng ngừa sự mất mát hệ thống:

- Chương trình NORTON UTILITIES có file RESCUE.EXE giúp bạn tạo một đĩa cấp cứu lưu trữ các bảng FAT, Boot Sector, CONFIG.SYS ... của máy vi tính.
- Tạo một đĩa khởi động máy, chứa các tập tin:  
COMMAND.COM  
IO.SYS  
MSDOS.SYS  
AUTOEXEC.BAT  
CONFIG.SYS  
SYS.COM  
NDD.EXE  
...
- và một số đĩa chứa chương trình quét và diệt virus có phiên bản (*version*) mới nhất, như:
  - SCAN.EXE và CLEAN.EXE của Công ty Mc-Afee, Mỹ
  - VSAFE.EXE của MS-DOS, Mỹ
  - MSAV.EXE của MS-DOS, Mỹ
  - NORTON ANTIVIRUS của Norton, Mỹ
  - ATV.EXE của Ngô Anh Vũ và Phạm Dũ Liêm, ĐH Kinh tế TP. HCM
  - TAV.EXE của Dương Hồng Tấn, Trần Thanh Sơn, Unisoft, TP. HCM
  - D2.COM của Trương Minh Nhật Quang, ĐH Tại chức TP. Cần Thơ
  - BKAV của Đại học Bách khoa Hà Nội
  - v.v...