# 防止隨身碟病毒的保護方法


保護自己，也保護別人，大家一起來。

# 沒有中毒

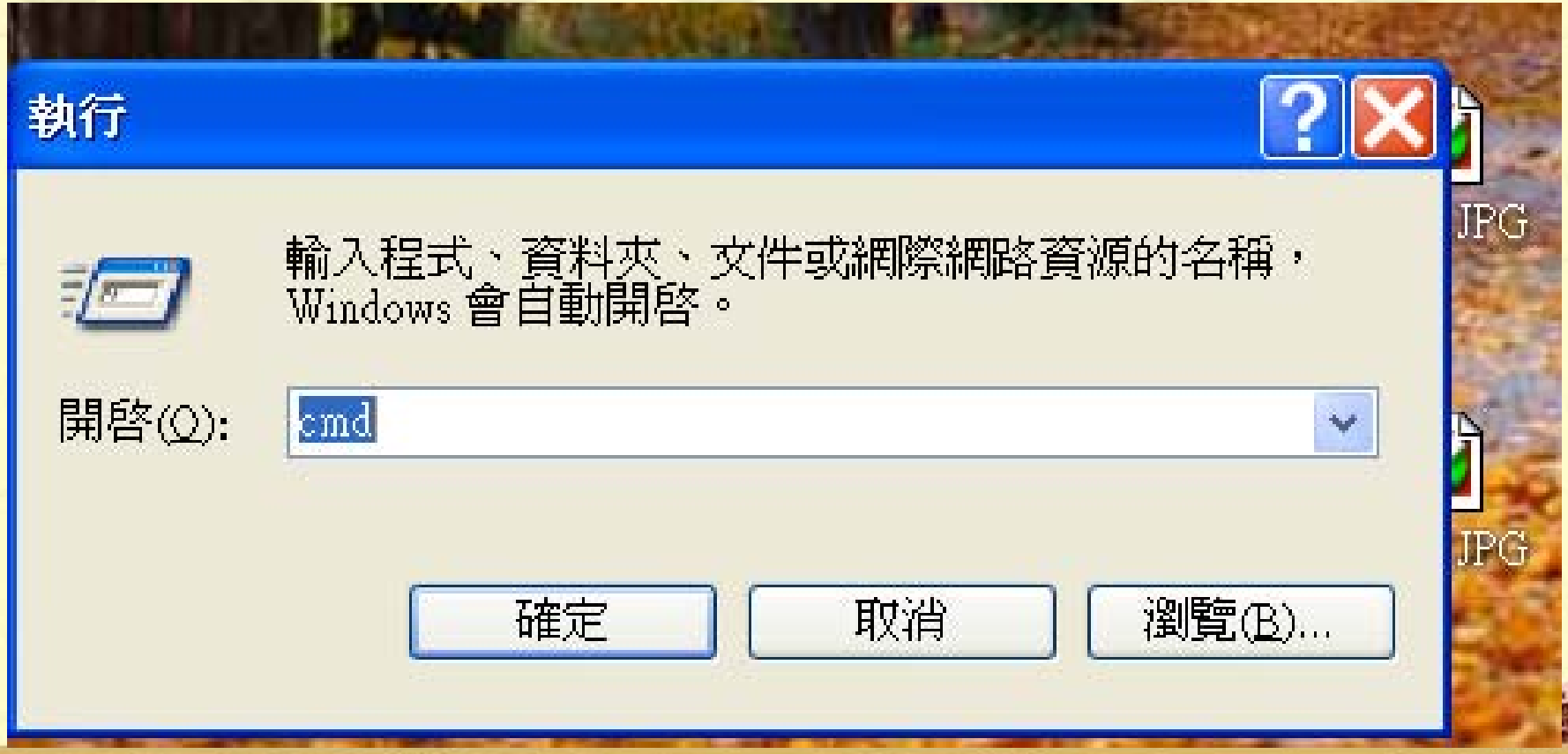
- 在隨身碟建立 AUTORUN.INF 資料夾，使病毒無法建立 AUTORUN.INF檔案。

# 如何知道您的隨身碟有沒有中毒？

- 請按(開始) → (執行) →輸入(cmd)鍵入隨身碟磁碟機代號，如：(F:)，輸入(dir /a)，若看到 autorun.inf 和奇怪的****.exe 檔，則表示可能已中毒。

# 示範步驟1

開始 → 執行 → cmd



# 示範1

```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\teachernote23>f:

F:\>dir /a
 磁碟區 F 中的磁碟沒有標籤。
 磁碟區序號:  78E5-D69D

 F:\ 的目錄

2007/05/06  下午 12:08    <DIR>          常用軟體h
2007/08/20  下午 09:23    <DIR>          tsaikl
2007/09/22  上午 11:05    <DIR>          autorun.inf
               0 個檔案              0 位元組
               3 個目錄     611,188,736 位元組可用

F:\>
```

若找到沒有〈dir〉（資料夾）的autorun.inf檔或*.exe檔就要當心了

# 步驟2


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\teachernote23>cd..
C:\Documents and Settings>cd..
C:\>dir c:\a
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號: 50CD-CE6D
c:\ 的目錄
2007/05/22 下午 03:05 <DIR> history10
2007/06/01 下午 03:44 38,244 debug.log
2007/09/22 上午 02:33 <DIR> autorun.inf
2007/08/16 下午 12:11 <DIR> 道教
2002/07/03 下午 03:10 6,191,421 tea250k.wmv
2007/09/03 下午 02:08 <DIR> 254CANON-b1-3
2007/08/29 下午 10:11 <DIR> 00taiwanhis
（2）輸入cd..
（3）輸入cd..
這是進入C槽的方法
（4）輸入dir c:/a或\/a
若找到沒有〈dir〉（資料夾）的autorun.inf檔就要當心了

# 清除隨身碟autorun.inf等病毒檔

```
F:\>del autorun.inf/A:rh

F:\>md  autorun.inf

F:\>CD  autorun.inf

F:\autorun.inf>
```

autorun.inf是隱藏檔，所以要加A:RH才能清除。其他的*.exe檔也一樣。

在隨身碟建立 **AUTORUN.INF** 資料夾，使病毒無法建立 **AUTORUN.INF**檔案。

恭喜！你已建立AUTORUN.INF 資料夾了

# 步驟9

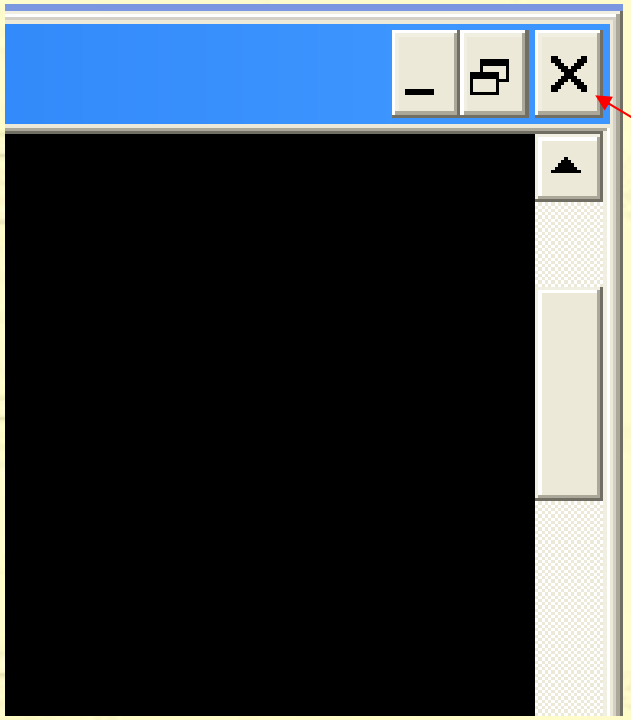
```
              25 個檔案    1,080,871,392 位元組
              34 個目錄    9,264,201,728 位元組可用

C:\>del c:ntdelect.com/A:RH
找不到 C:\ntdelect.com

C:\>
```

若發現隨碟有ntdelect.com病毒檔也比照刪除，注意確定隨身碟的槽別是f:或e:等

病毒檔為什麼找不到，因為已被我清除了

每個硬碟槽都要清除相關病毒檔，建立 AUTORUN.INF 資料夾，使病毒無法建立 AUTORUN.INF檔案。

結束隨身碟防毒設定，也可比照設定C、D等槽，加入〈autorun.inf〉資料夾避免autorun.inf侵入C、D等槽。



要結束時
按一下

- autorun.inf 目錄（資料夾）的**屬性必需記得設定為【唯讀】與【隱藏】**，在autorun.inf資料夾按右鍵，選（內容），再設定即可。

# 補充：wincab.sys木馬程式、「W32.Gammima.AG」病毒

- 這些木馬為USB專門病毒，舉凡隨身碟、硬碟、記憶卡等都會感染！！！

只要感染的隨身碟，插到哪裡就感染到哪裡，很可怕！

- 身邊的所有的USB儲存裝置，都要清查裡頭是否有兩個隱藏檔
- Autorun.inf
  ntdelect.com
  如有快把它殺了，千萬別執行它，因為就是這兩檔會自動執行而感染的。

- 清除方法見前面說明。

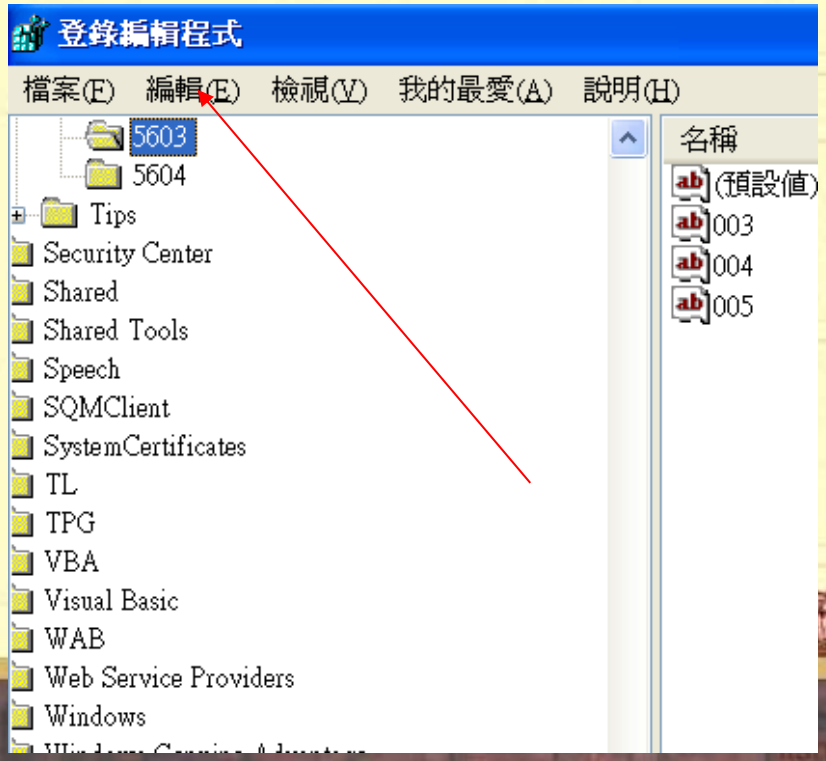
- 千萬別小看這些木馬程式，有很多的掃毒軟體是掃不出來的，其實他有相關的程式隱身在系統裡如下

C:\WINDOWS\system32\kavo.exe
C:\WINDOWS\system32\kavo.dll
C:\WINDOWS\system32\kav0.dll
C:\WINDOWS\system32\kav1.dll
C:\ntdelect.com

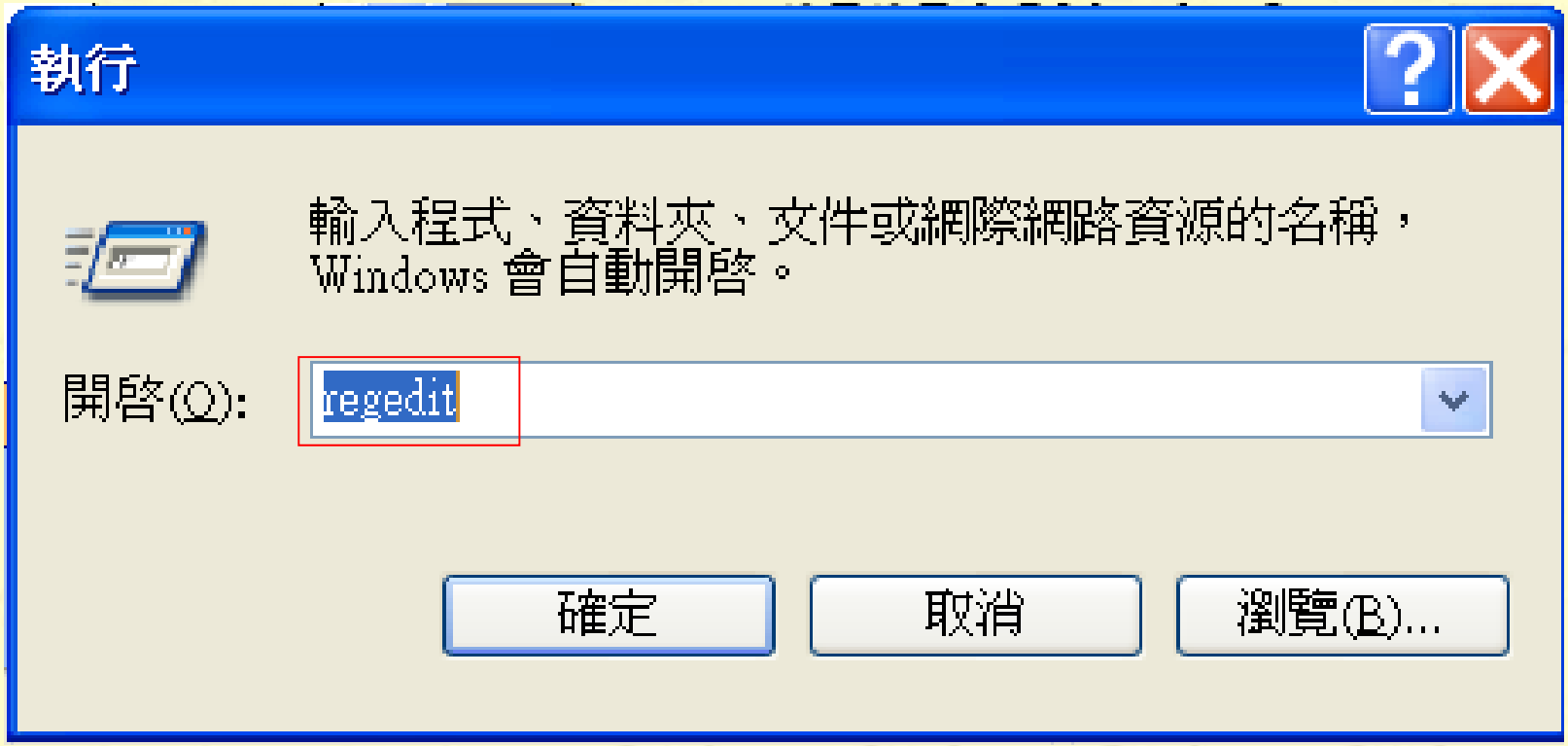
（系統裡有ntdetect.com千萬別刪除看清楚！！病毒是 l，系統檔是t）
但您也別太高興！因為它把系統全部隱藏起來了
無論您麼改顯示統檔案，一跳出設定他又隱藏了起來了！
這就是此病毒的特色。

# 清除方法

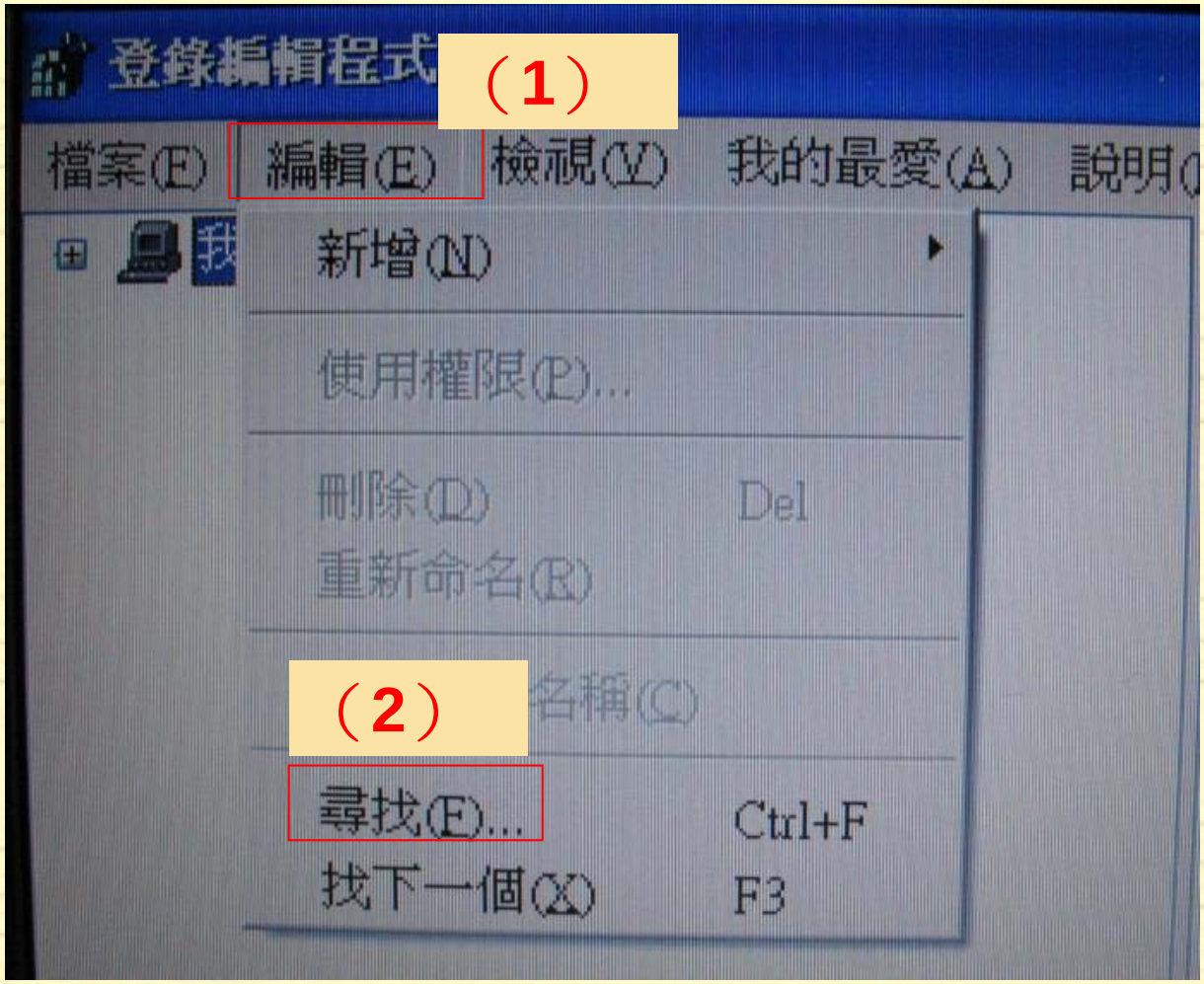
- 開完機後要去修改註冊機碼（regedit）
  在開始→執行中，輸入【regedit】，會出現如下視窗，打開〈尋找〉，輸入要清除的檔案如：
  autorun.inf、
  kavo.exe、
  ntdelect.com等，
  不管找到多少個
  統統殺掉即可。



# 示範1


執行
輸入程式、資料夾、文件或網際網路資源的名稱，
Windows 會自動開啓。
開啓(O):
regedit
確定
取消
瀏覽(B)...

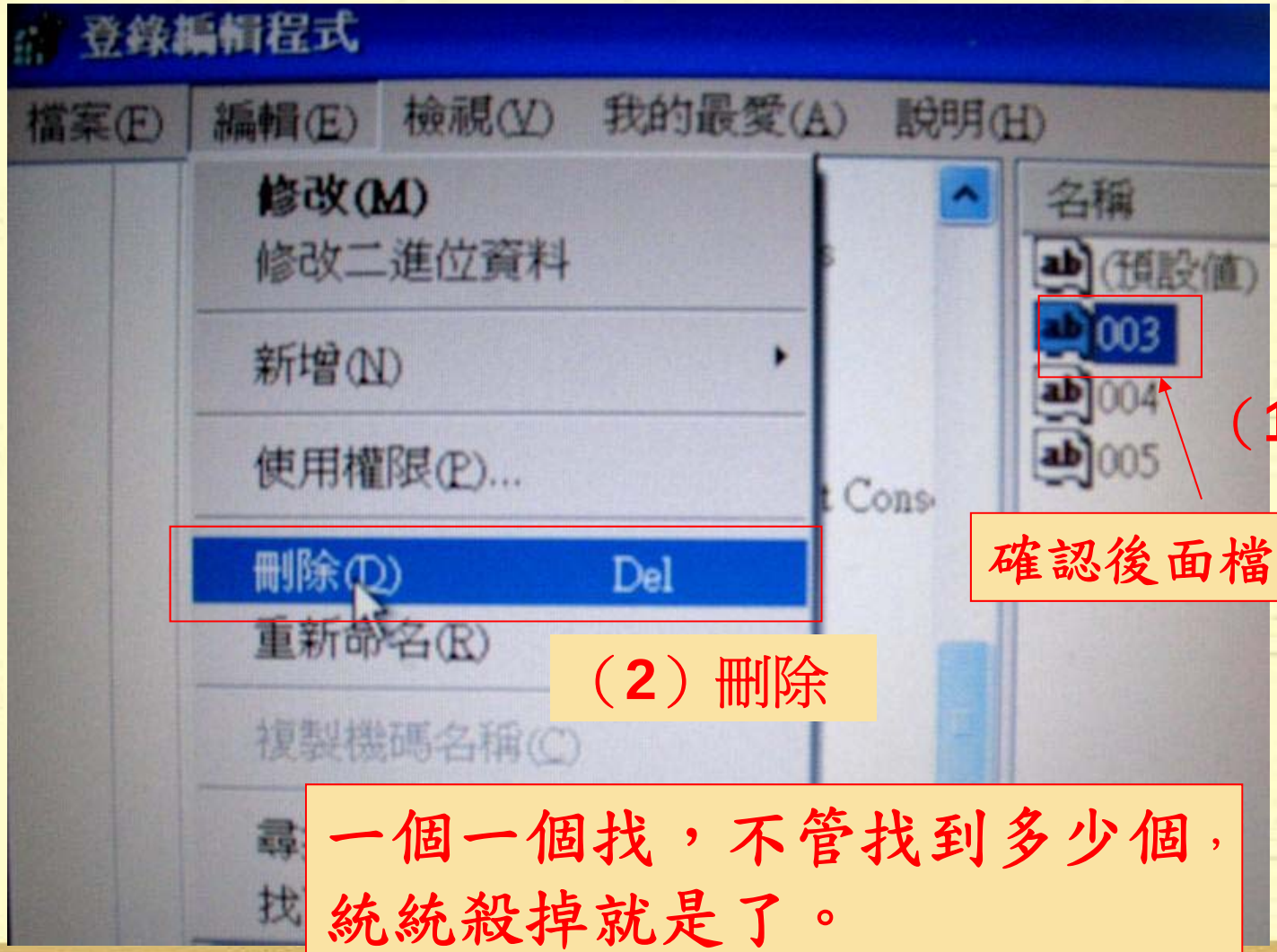
# 示範2


登錄編輯程式
（1）
檔案(F)
編輯(E)
檢視(V)
我的最愛(A)
說明(
新增(N)
使用權限(P)...
刪除(D) Del
重新命名(R)
名稱(C)
（2）
尋找(F)...
Ctrl+F
找下一個(X)
F3

# 示範3


尋找
（1）輸入要刪的檔案名稱
（2）
尋找目標(N):
autorun.inf
找下一個(F)
取消
查看
機碼(K)
值(V)
資料(D)
字串須完全相符(W)

# 示範4




一個一個找，不管找到多少個，統統殺掉就是了。

# 如何殺掉c槽、d槽等的Autorun.inf、ntdelect.com檔

- 除以上方法，也可以用命令提示字元來確認、刪除。方法就是：
- 「開始」、「執行」輸入「**cmd**」按確定可以叫出命令提示字元
- 輸入「**dir c:\ /a**」可以列出 **c:** 下所有的檔案，包含隱藏檔。
- 要刪除的話，可以透過「**del** 檔案名稱**/A:RH**」
  如：「**del ntdelect.com/A:RH**」
  來刪除唯讀隱藏的檔案。

- wincab.sys補充
  這一隻是新的隨身碟類型（ autorun.inf 引導 ）的病毒，中毒的症狀:
  1. 出現 wincab.sys 訊息。
  2. 無法將檔案總管的顯示隱藏檔功能開啟，病毒會將其改回去。

  解毒方式 :
  將所有磁碟中的 autorun.inf & ntdelect.com刪除。
-

  注意 ntdelect.com 跟 C:\ 系統檔案 的 ntdetect.com 有一字之差。

# 主要參考來源：

- http://www.cses.chc.edu.tw/teach_doc/how_to_avoid_usbdisk_get_virus.htm
- http://www.yaes.tnc.edu.tw/school/menu/index.php
- http://heresy.spaces.live.com/blog/