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 وامیدواریم 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

Cmdچیست؟

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

Dosچیست؟

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؟

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.

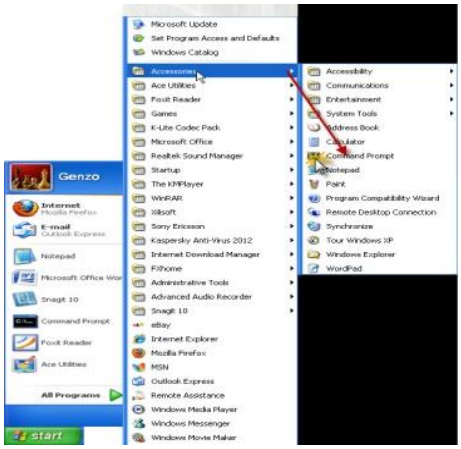
{نکته: cmd هیچ وقت از زبان فارسی پشتیبانی نمی کند و هر نوع نوشتار فارسی در آن تبدیل به خط چینی می شود.}

Cmdرا از کجا اجرا کنیم؟

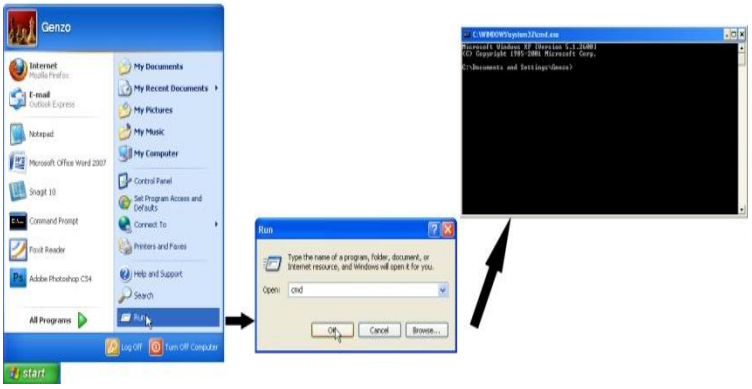
برای اجرای Cmd ۴ راه داریم:

به آدرس های زیر می رویم:

۱) Start\All program\Accessories\command prompt



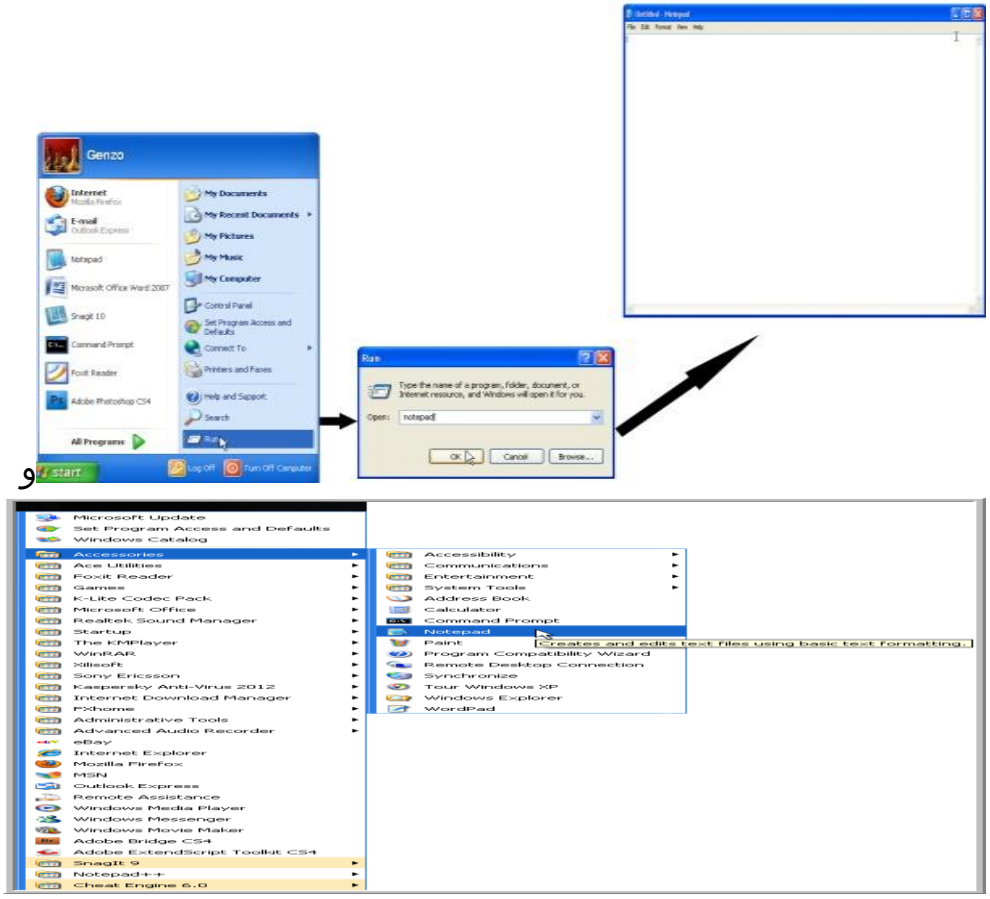
۲) وارد منوی Start شده و روی Run کلیک کرده تا باز شود سپس در کادر دستور آن می نویسیم:cmd



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

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

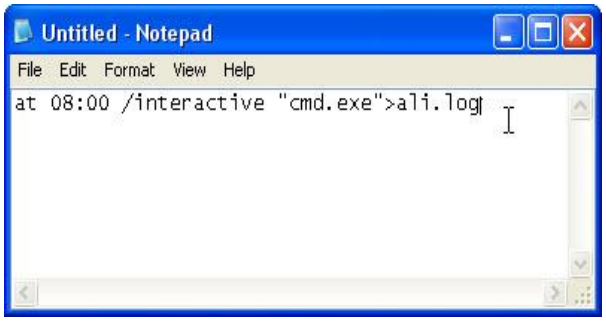
{نکته:برای باز کردن Notepad هم می توانید از منوی Start\All program\Accessories\Notepad آنرا اجرا کنید و هم در کادر فرمان Run بنویسید:notepad}



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.}

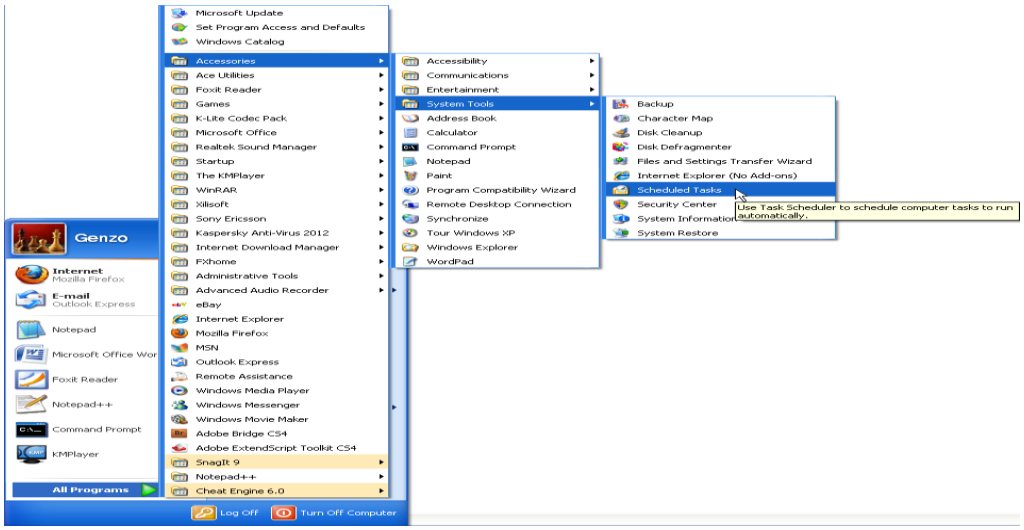
{نکته:می توانید در قسمت آخر دستور هر نامی را بنویسید ولی با پسوند log. برای مثال من نوشتم ali.log}

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

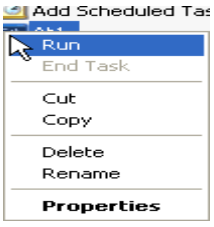
و در قسمت Save as type ، روی گزینه All files کلیک می کنیم،

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.batرا 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.

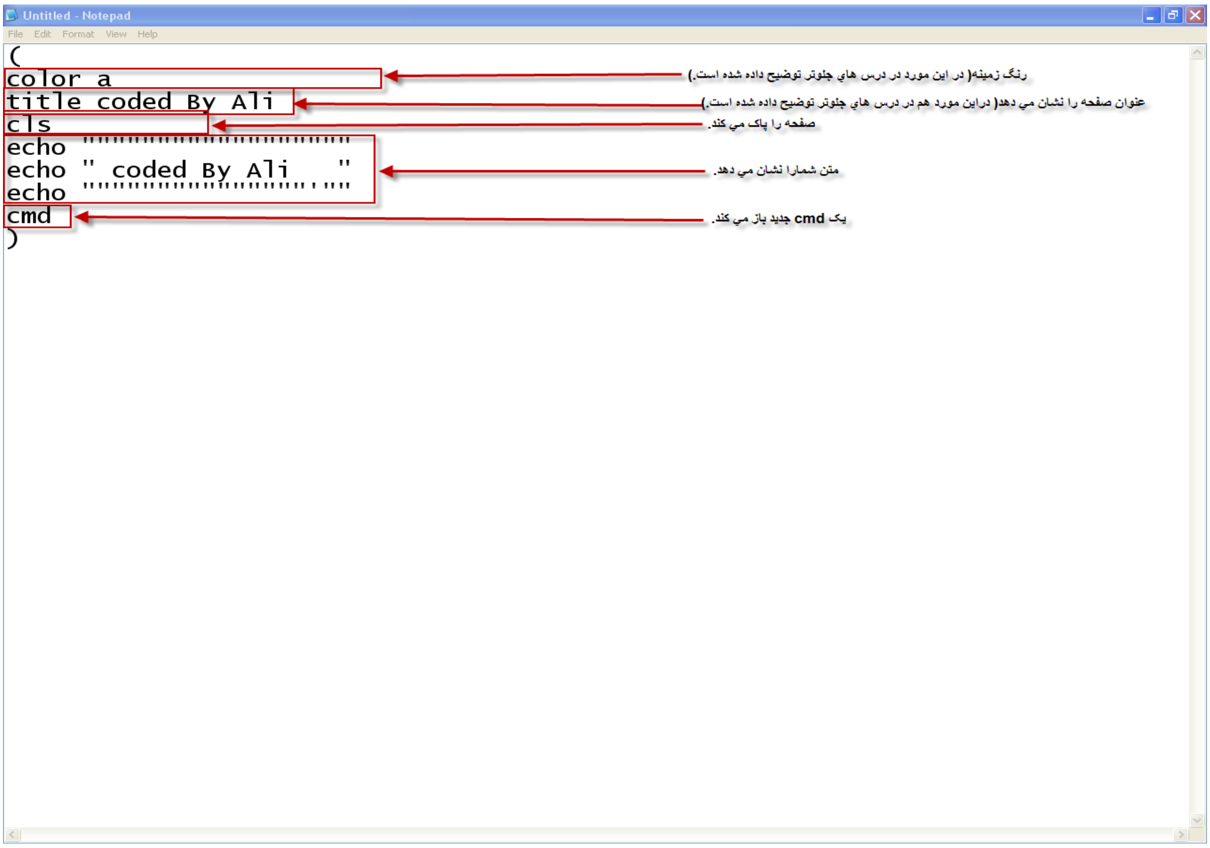


{نکته:البته می توانید تنظیمات بیشتری را در بخش زمان بندی ویندوز انجام دهید که به دلیل دور شدن از موضوع از گفتن آن خودداری می کنم.}

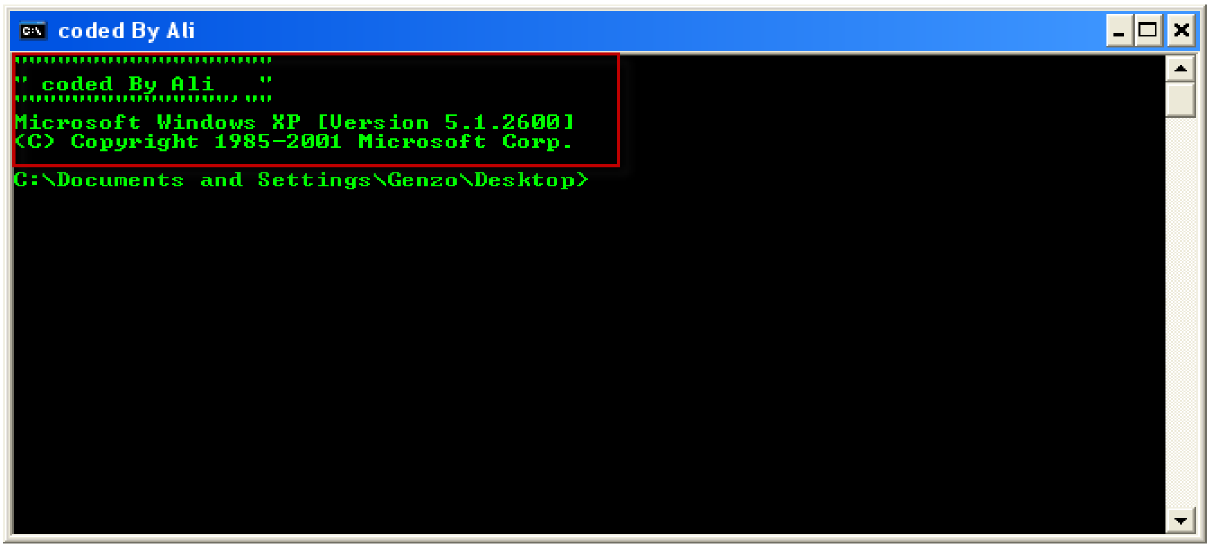
{نکته:اهمیت این کار زمانی معین می شود که ویندوز ما دچار خرابی شده و توانایی اجرای cmd در دو حالت اول امکانپذیر نباشد.}

۴) ساخت یک cmdشخصی!

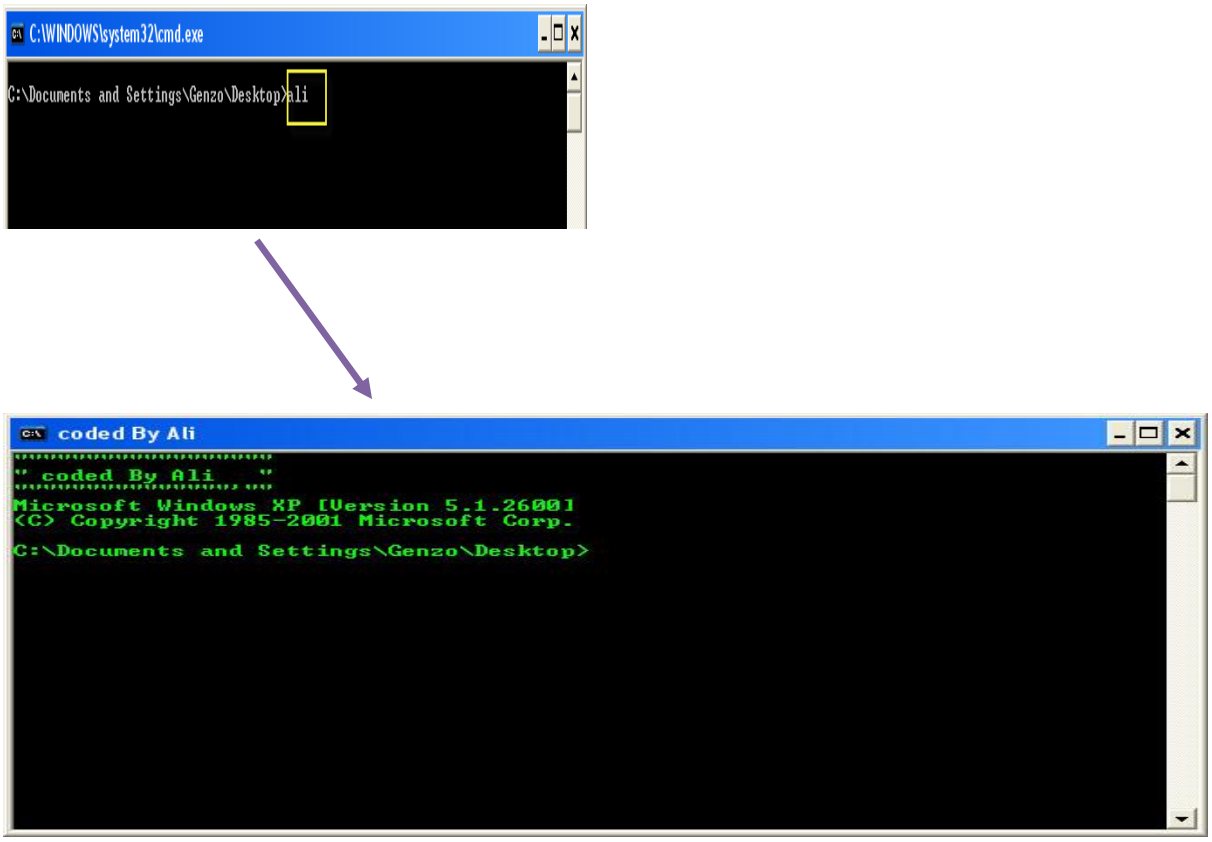
برای ساخت ابتدا نرم افزار notepad را باز کرده و به صورت زیر عمل می کنیم:



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

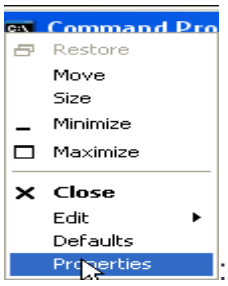


حال اگر می خواهید از هر جایی به cmdشخصی خود بروید کافیست در خط فرمان نام cmd شخصی خود را بنویسید،مثال:



درسنامه دوم:تنظیمات cmd

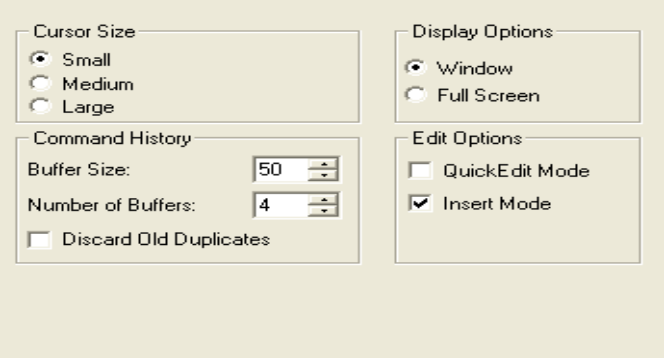
ابتدا cmdرا اجرا می کنیم،سپس در نوار عنوان آن کلیک راست کرده و روی گزینه Properteis را انتخاب می کنیم. تب هایی را مشاهده می کنیم که می تواند نیازهای ظاهری cmd ما را تامین



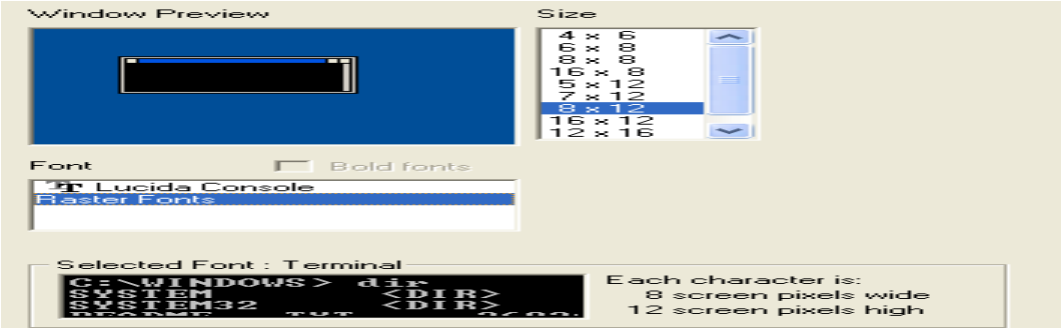
کند،شروع به توضیح هر کدام میکنیم:

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 cmdرا به حالت تمام صفحه در بیاوریم و برعکس.دربخش سوم یعنی Command History می توانیم بازگشت به عقب cmd را به

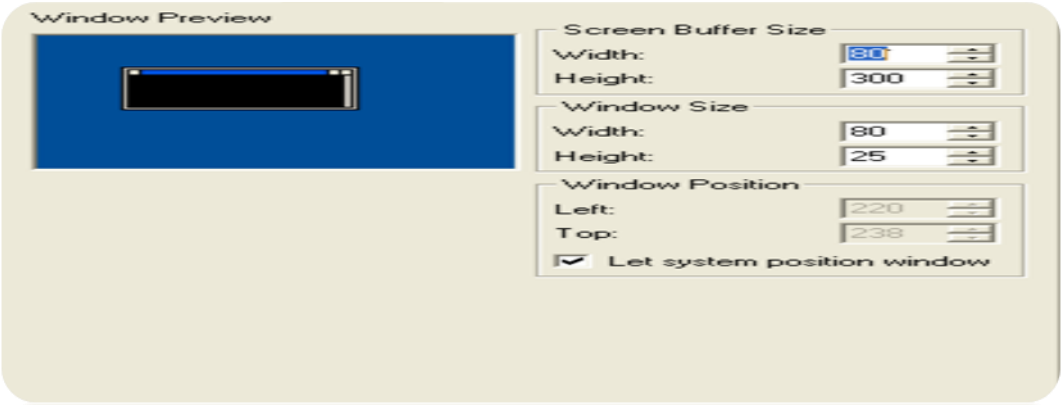
دلخواه مورد تغییر قرار دهیم.در بخش چهارم یعنی Edit Option می توانیم نحوه تنظیمات را مناسب با نیاز خود تنظیم کنیم.



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

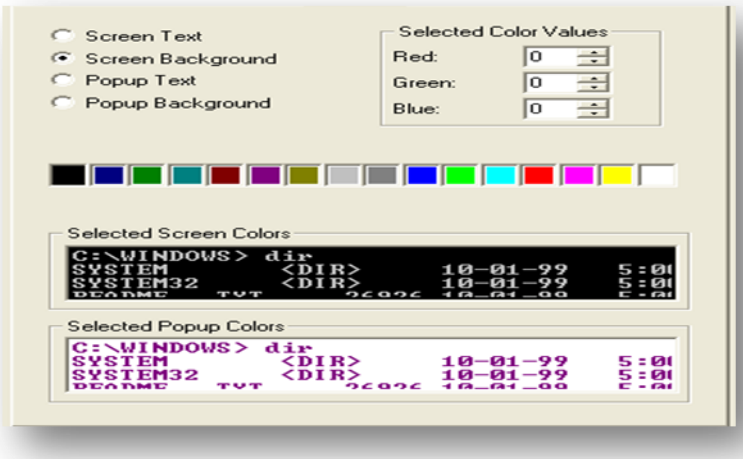


۳)Tab Layout: می توانید اندازه دلخواه cmd را از بالا و پایین،چپ و راست تنظیم



کنید

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



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

درسنامه سوم:آشنایی با بعضی از دستورات پر کابرد 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	ویرایش فایل
ECHO OFF	پنهان کردن ادرس های پشت فرمان
ECHO ON	نمایان 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:

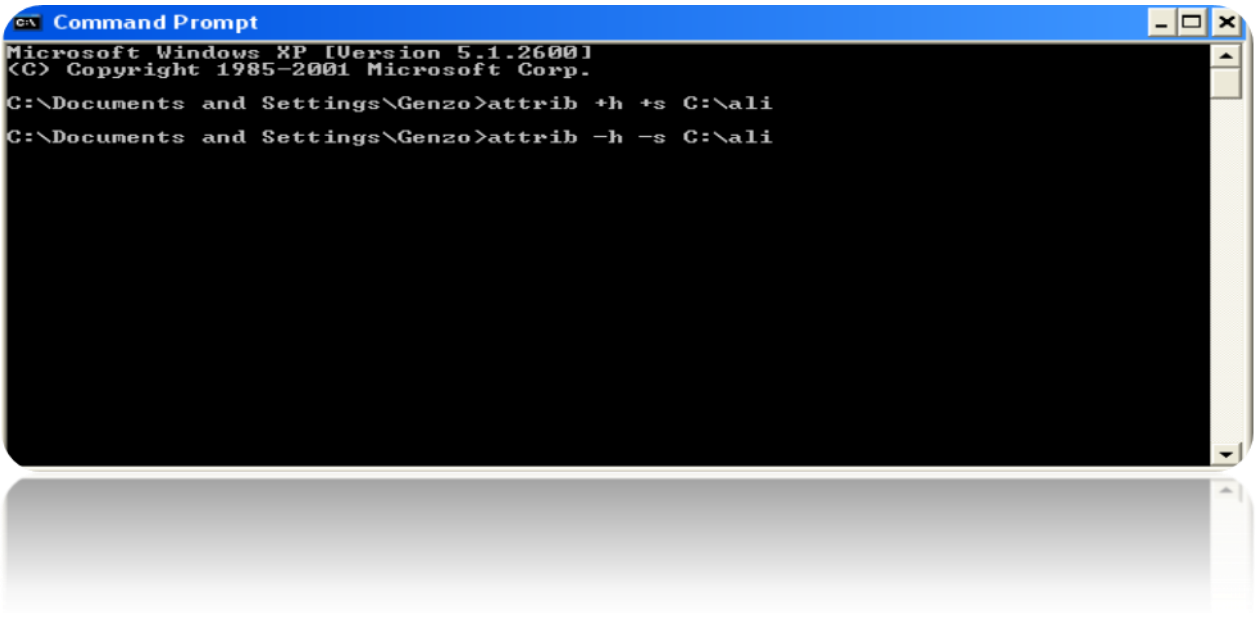
ابتدا پوشه مورد نظر را ایجاد کرده یا در نظر بگیرید.{نکته پس از نوشتن هر دستور با زدن دکمه Enter روی صفحه ی کلید آن را اجرا می کنیم.}

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

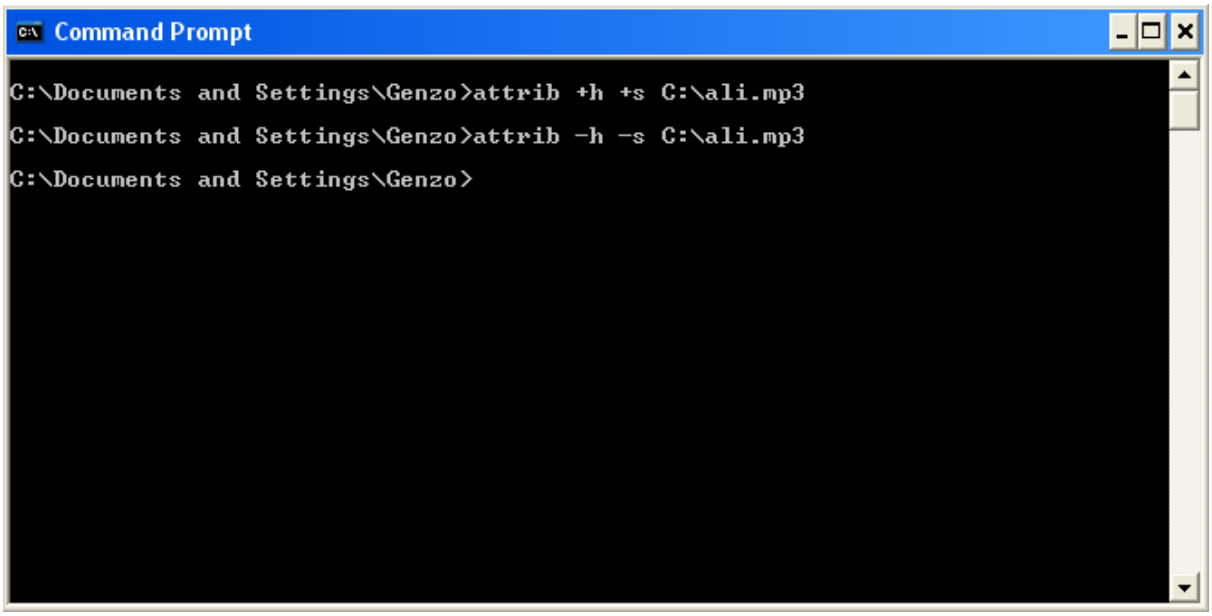


ولی برای مخفی سازی فایل هایی مانند عکس و فیلم یا آهنگ و... باید پسوند فایل در آخر آن ذکر شود.

به مثال توجه کنید:

Attrib +h +s C:\ali.mp3

Attrib –h –s C:\ali.mp3

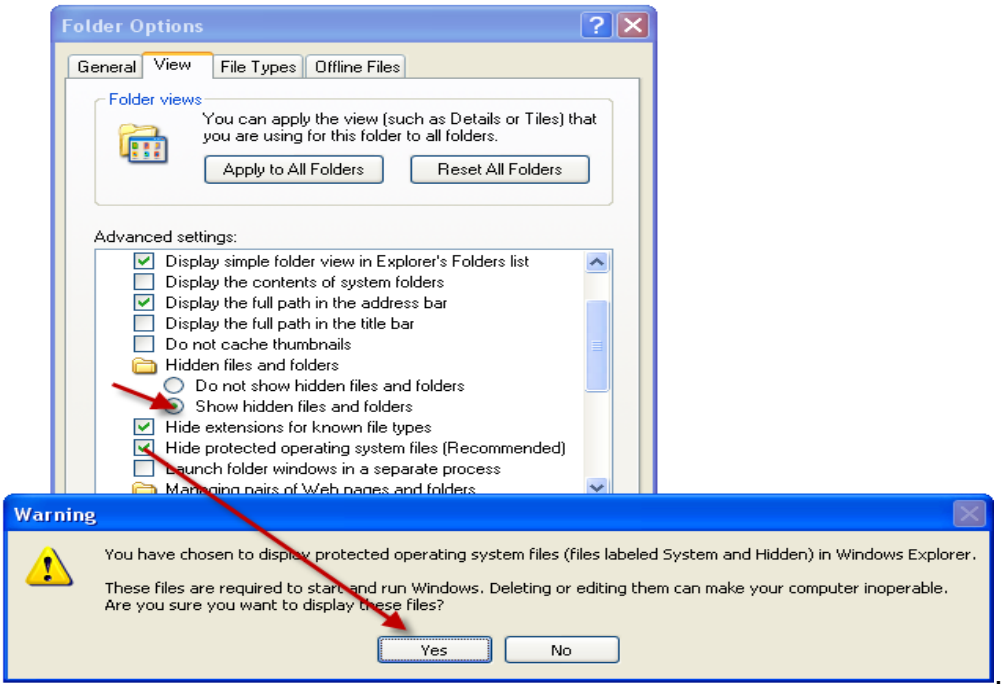


نکته:اگر آدرس را اشتباه وارد کنید با خطای {پیدا نشد،Not Found} مواجه می شوید!

نکته:برای دیدن این فایل در محیط ویندوز می توانید از این ادرس 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:

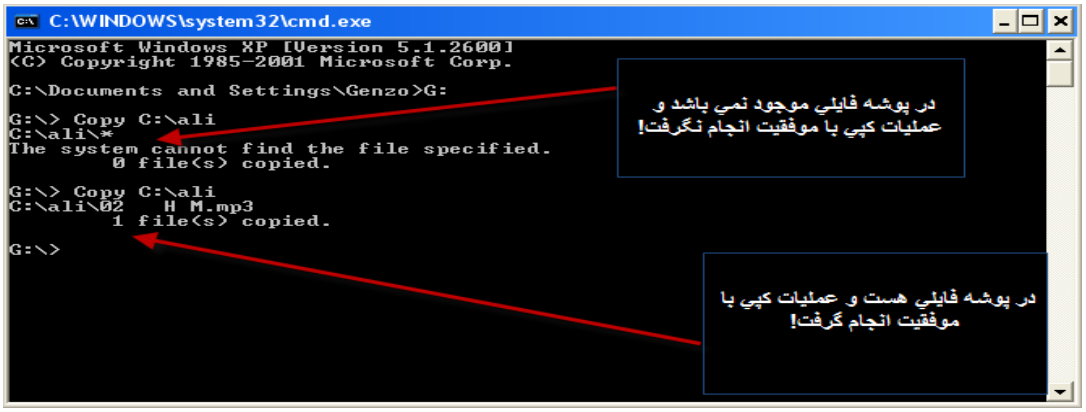
در cmd ۲ راه برای کپی کردن یک فایل داریم:

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

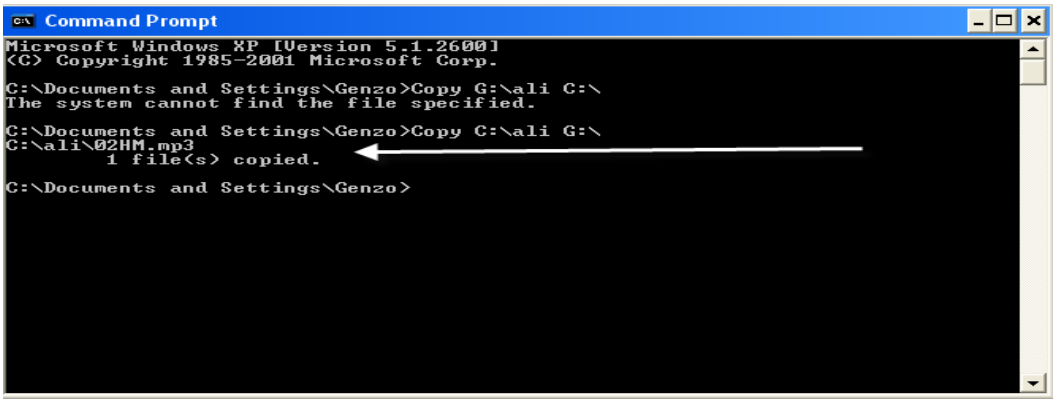


نکته باید پوشه aliکه در بالا ذکر شده باشد برای انجام عملیات کپی فایلی در آن موجود باشد.

۲)راه دوم :

Copy ۱ فایل ۲ فایل

Copy C:\ali G:\



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

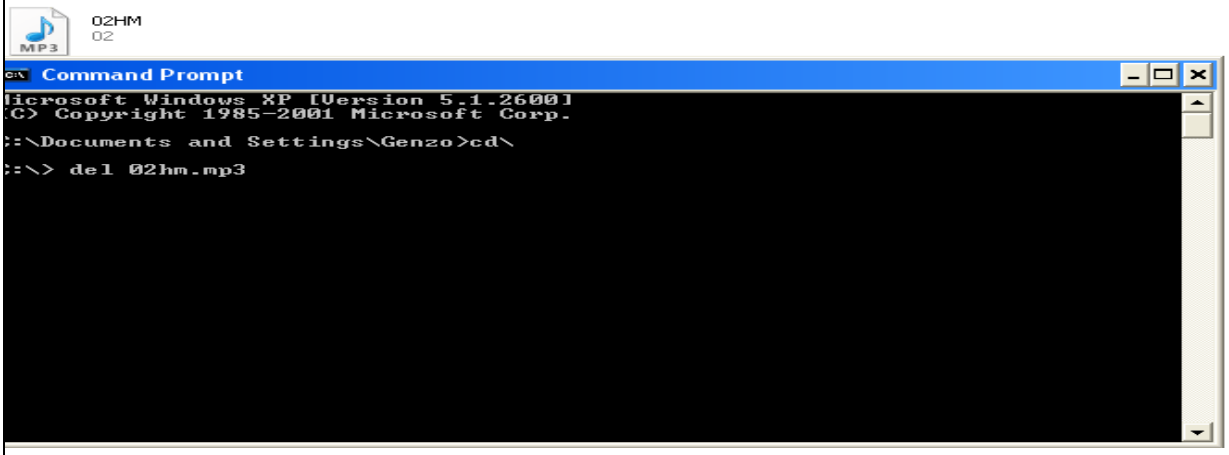
Copy C:\ali\02hm.mp3 G:\

عملیات با موفقیت به پایان رسید!

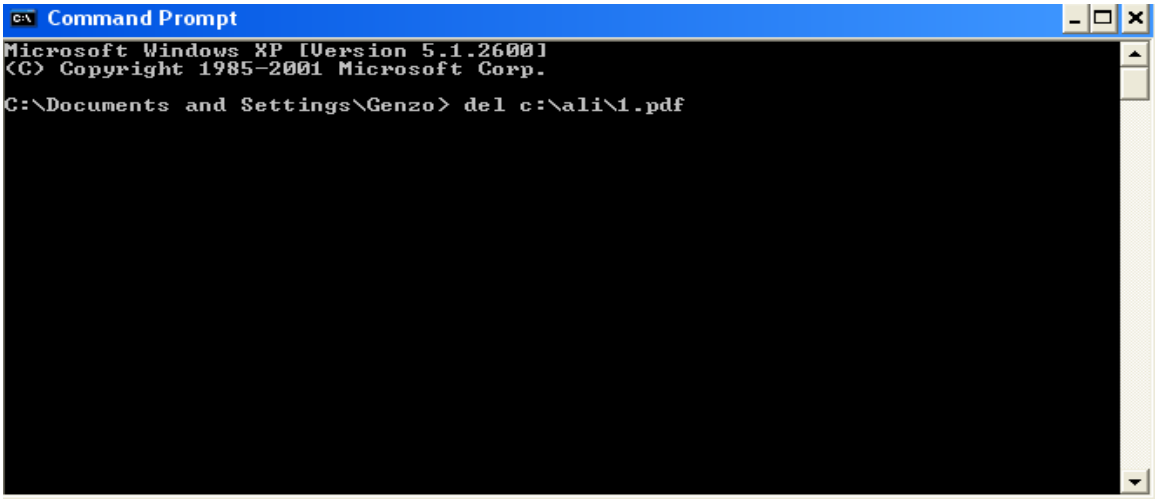
پاک کردن یک فایل:

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:



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



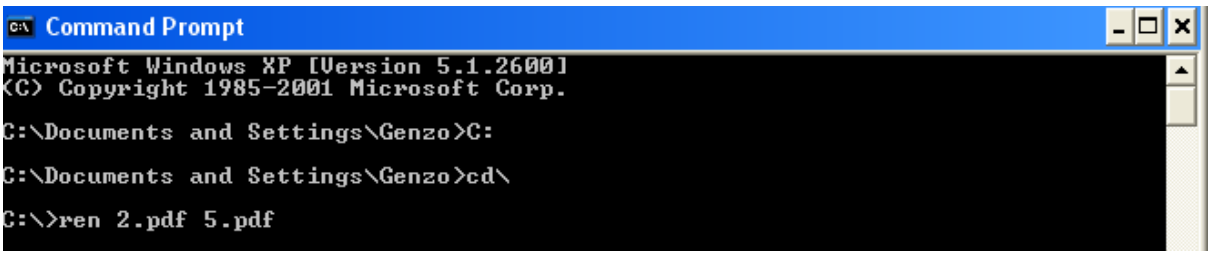
تغییر نام:برای تغییر نام باید از روش زیر کار را انجام دهیم:

انتخاب درایو مورد نظر که فایل مشخص شده در آن موجود باشد:

من درایو Cرا انتخاب کردم،ولی برای درایو Cنمی توانیم ازدستور :C استفاده کنیم و باید از دستور CD\ استفاده کنیم:

CD\

Ren 2.pdf 5.pdf



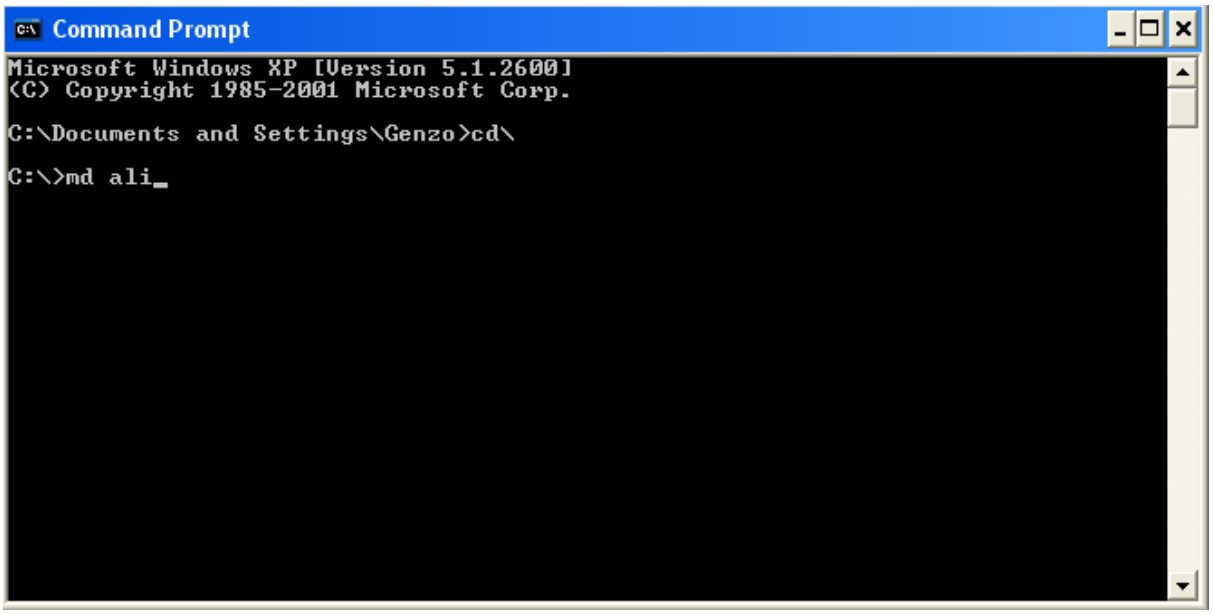
درسنامه ششم: ساخت پوشه

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\

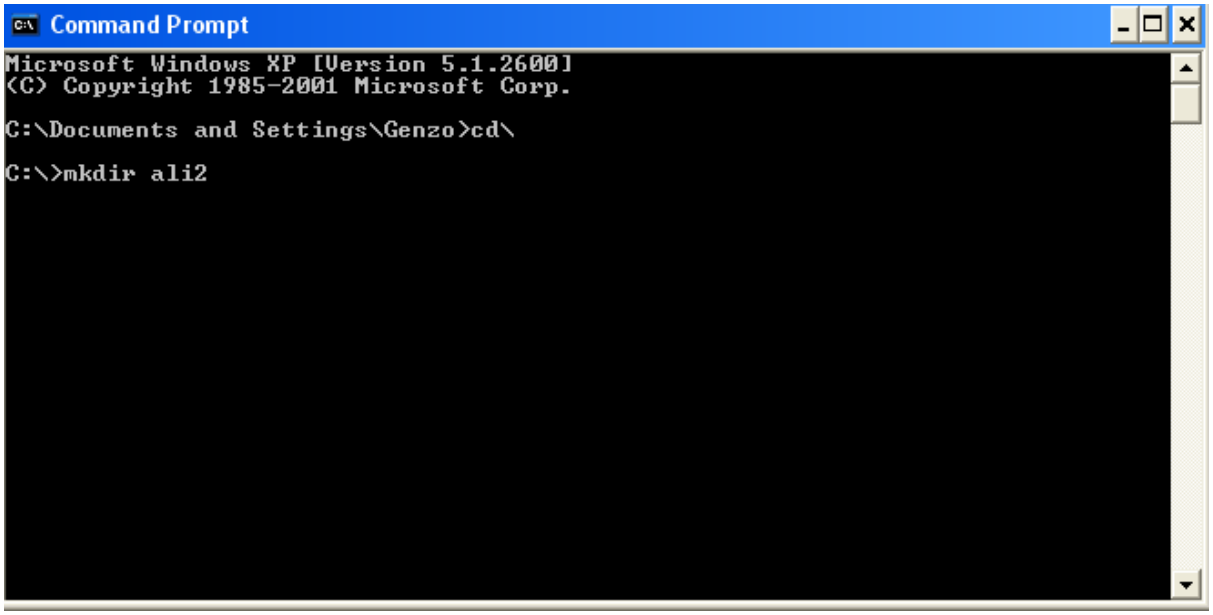
Md ali



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

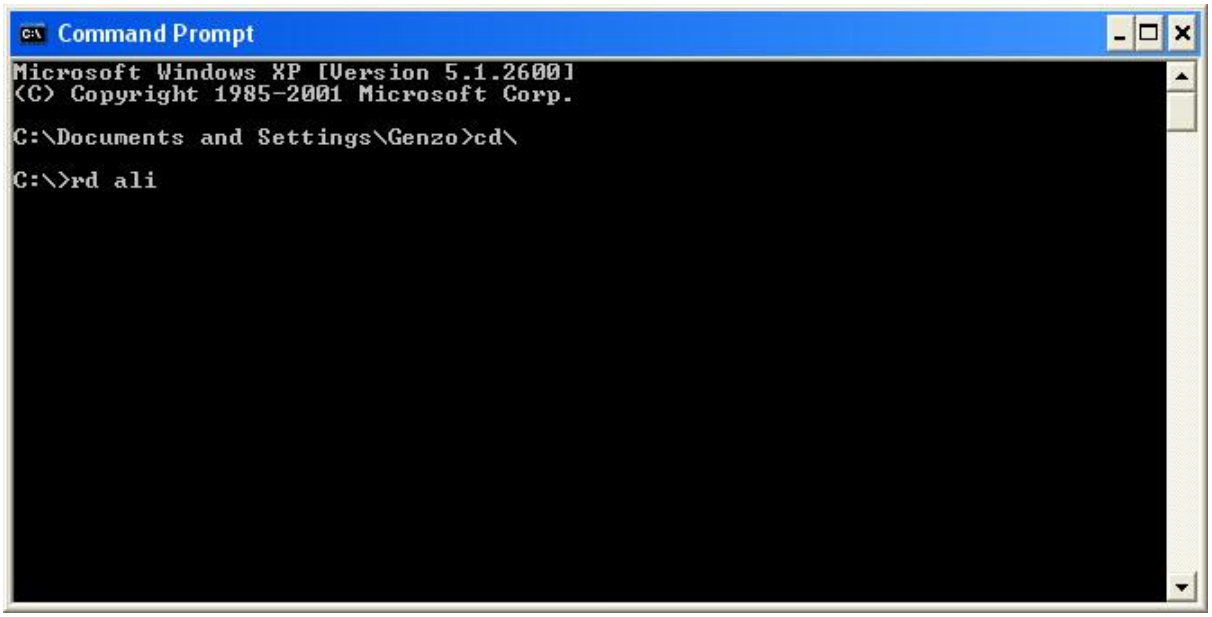
Cd\

Mkdir ali2



حذف پوشه های ساخته شده:

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



درسنامه هفتم:ساخت پوشه ها با اسامی غیر مجاز

بعضی از اسم ها هستند که ویندوز از پذیرش آن خود داری می کند وبه قول معروف آن را پس میزند ولی ما در این درسنامه با بعضی از این اسامی خاص آشنا خواهیم شد وهمچنین می آموزیم چطور 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

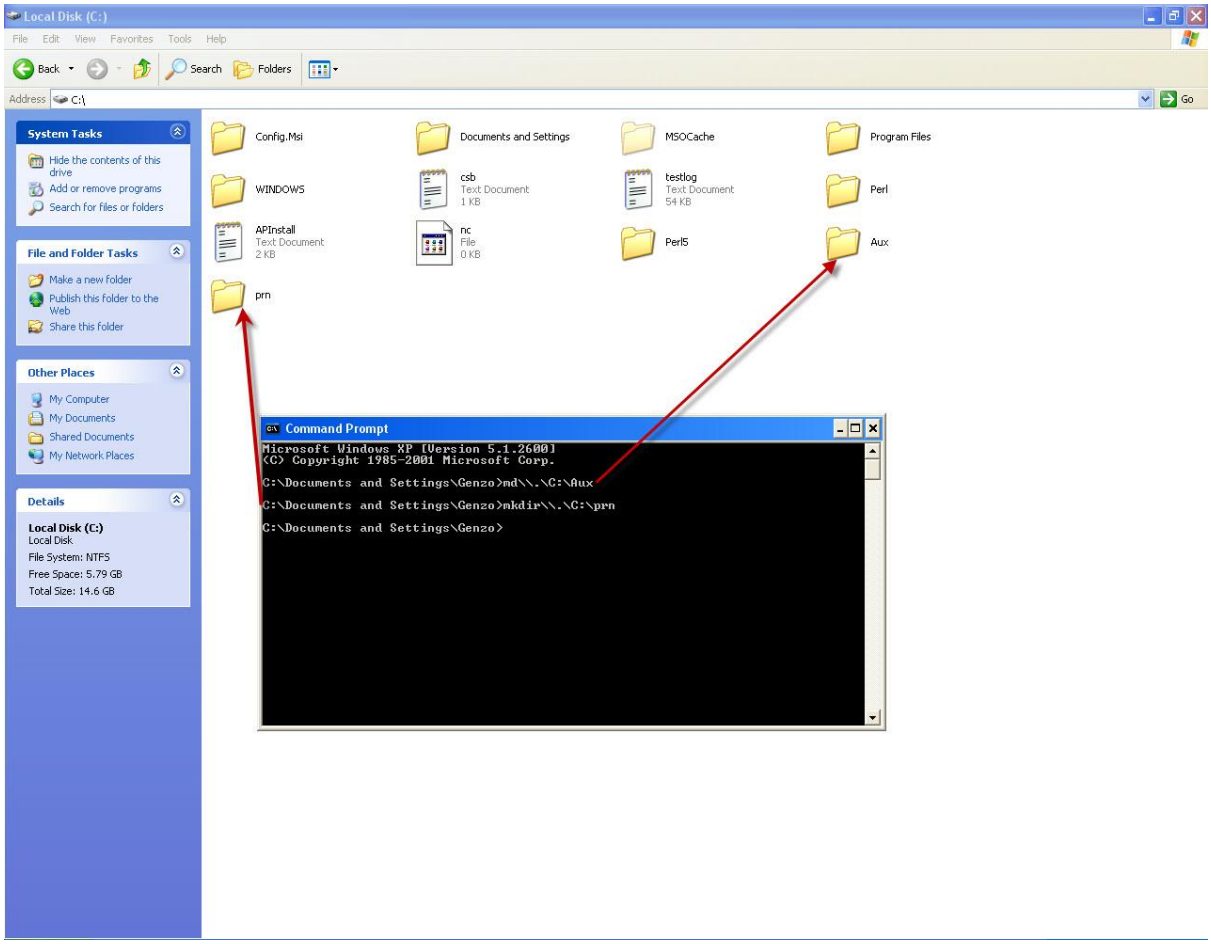
LPT6, LPT7, LPT8, LPT9 , CON

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

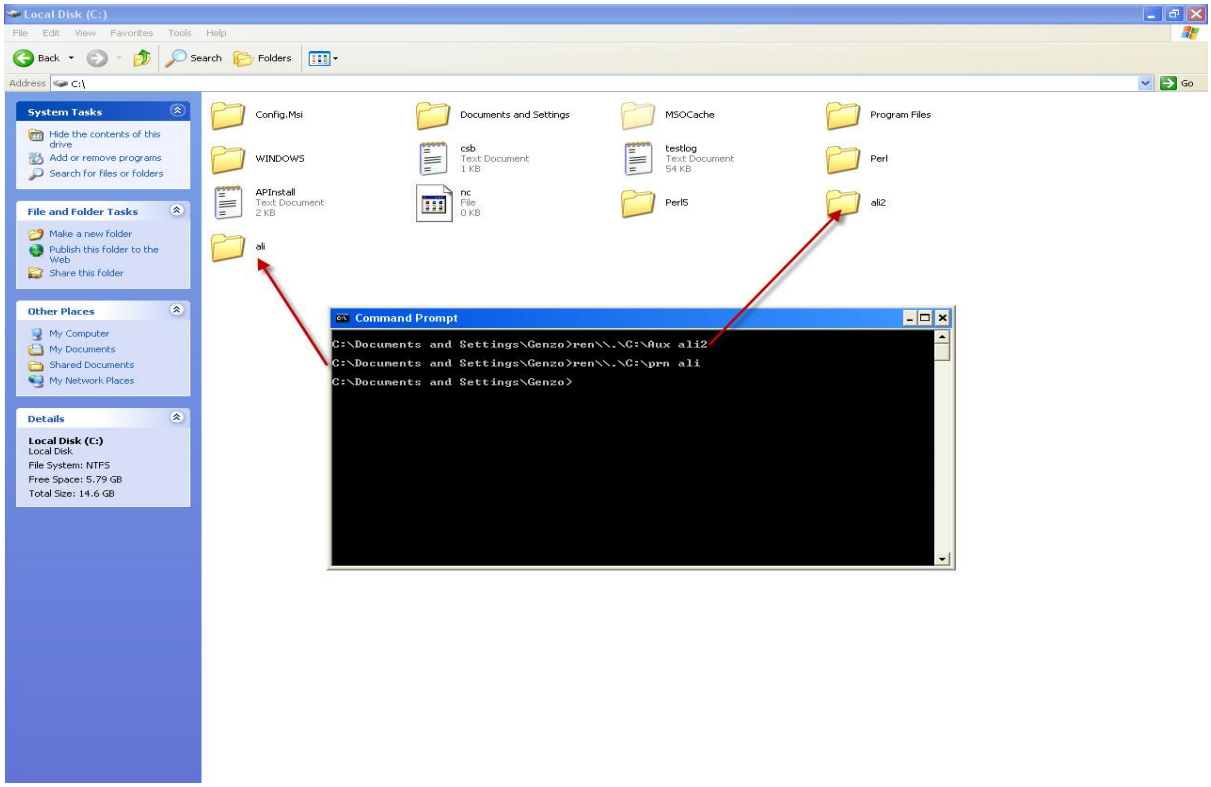
2) mkdir\\.\C:\prn



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

ren\\.\c:\prn ali

ren\\.\c:\Aux ali2



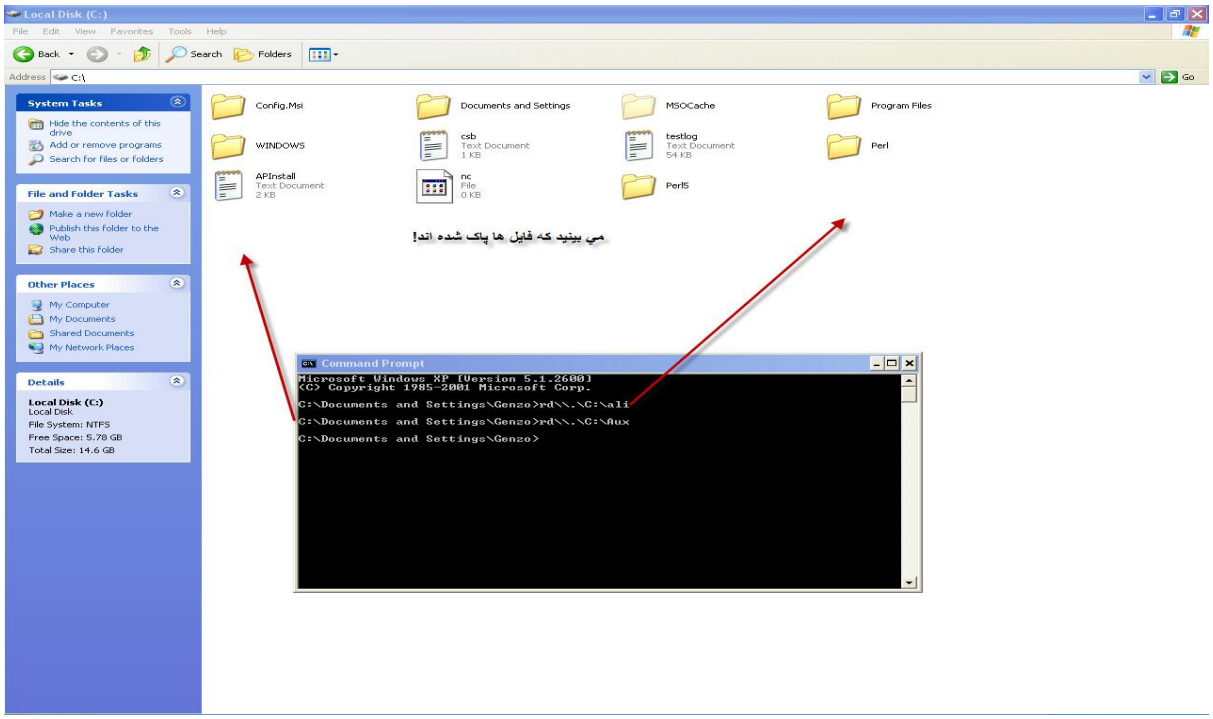
برای پاکسازی این پوشه ها می توانیم از دستور زیر استفاده کنیم:

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.



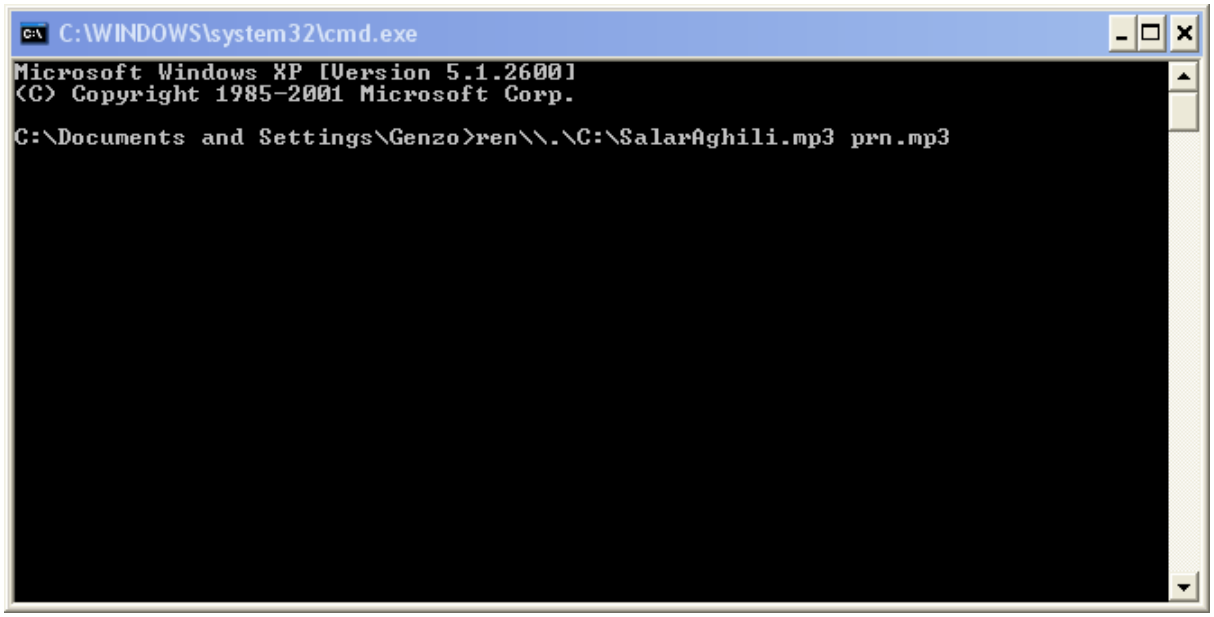
درسنامه هشتم:محافظت از فایل های با ارزش

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 هارا از ویندوزمان پاک کنند.

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

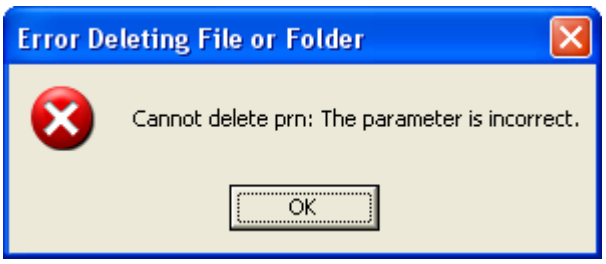
آهنگ مورد نظر را مشخص می کنم و من آنرا در درایو C می گذارم،سپس برای اینکه این فایل براحتی پاک نشود اسم آنرا به یکی از اسامی غیر مجاز تبدیل می کنم.

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



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.

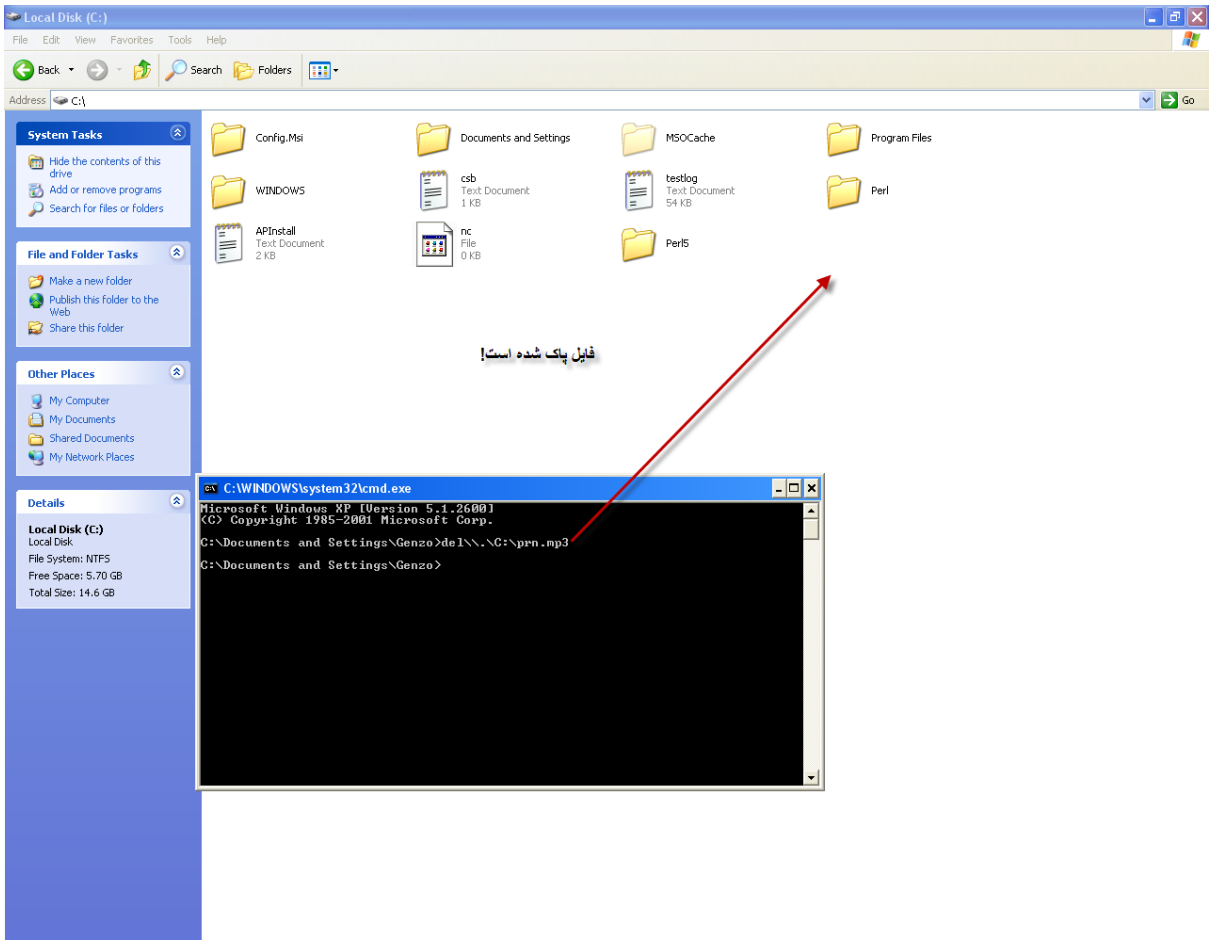


حال اگر خودمان بخواهیم آنرا پاک کنیم چه کنیم؟

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 mkdirرا دادیم،اکنون نیز یک پوشه می سازیم:

برای فهمیدن بهتر این درس ابتدا یک پوشه به نام aliمی سازیم وسپس آنرا پاک می کنیم:

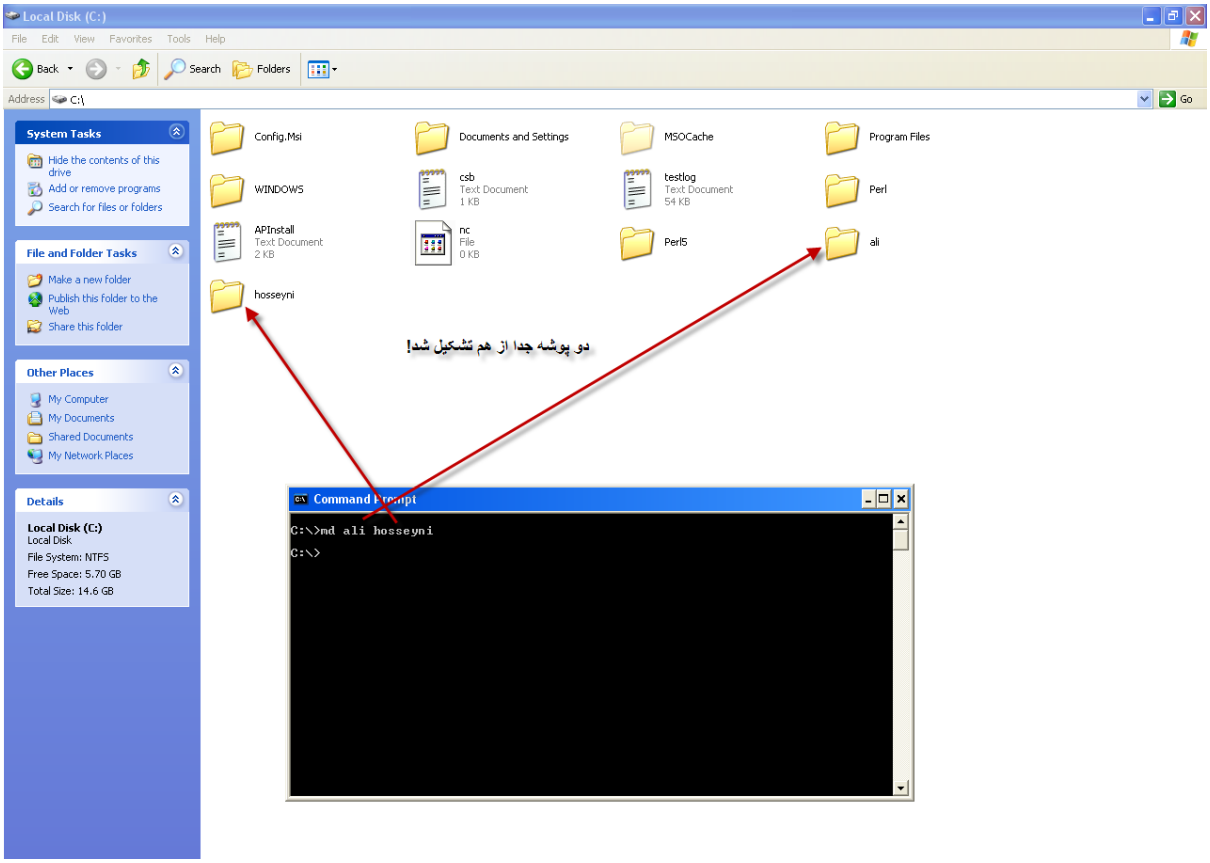
Cd\

Md ali

Rd ali

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

Md ali hosseyni



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:

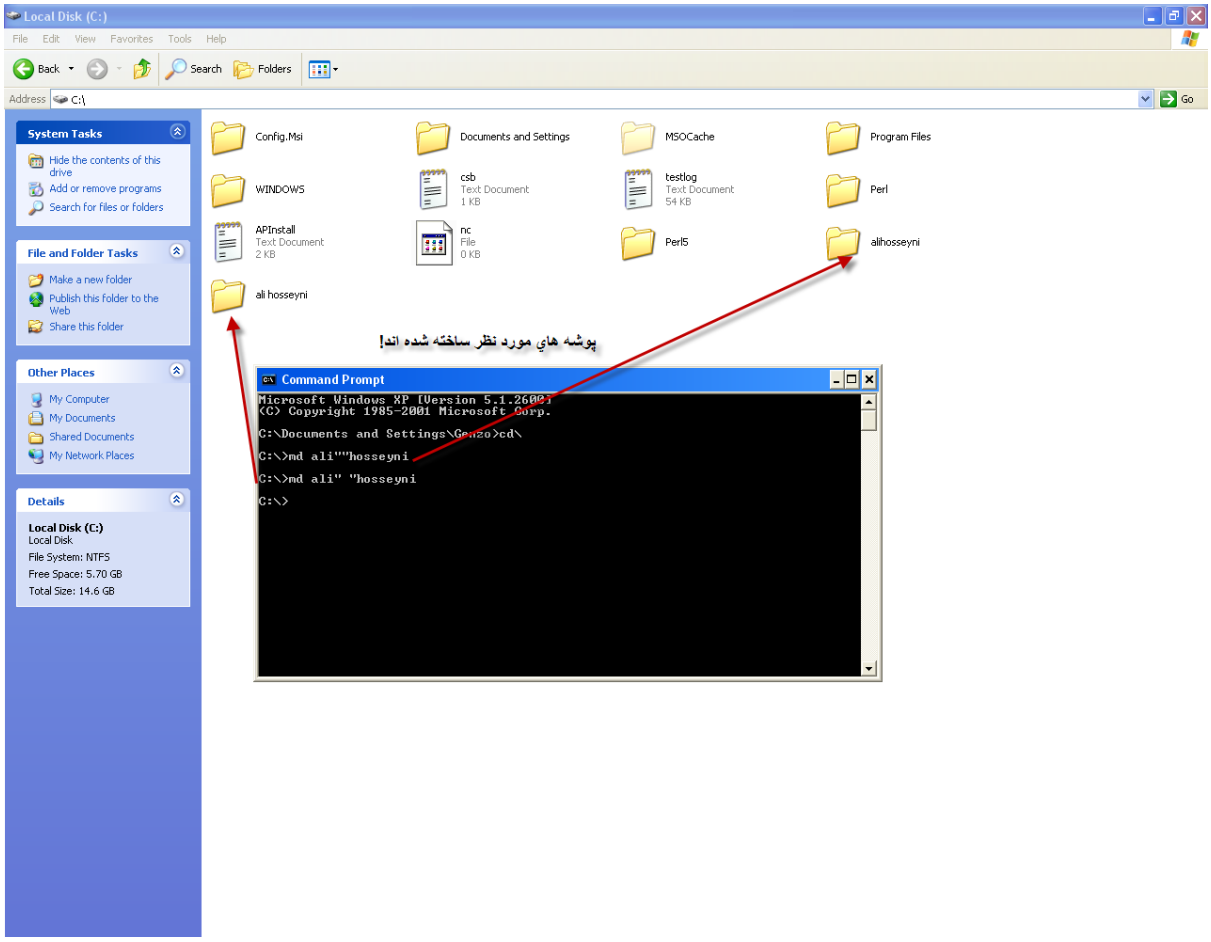
Md ali""hosseyni

Md ali" "hosseyni

یا

Mkdir ali""hosseyni

Mkdir ali" "hosseyni

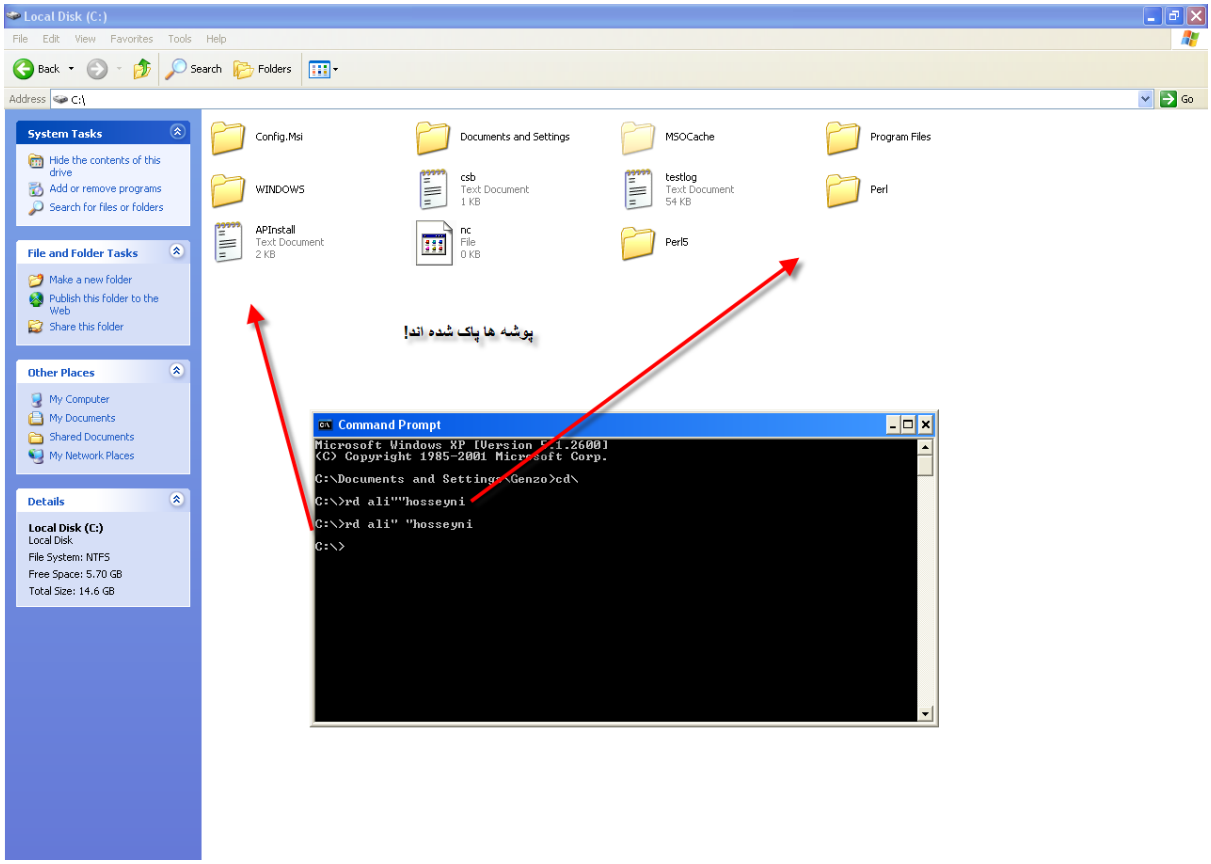


نکته:می توانید بین دو " " مقدار فاصله را نیز تنظیم کنید.

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 Cانجام داده ام)

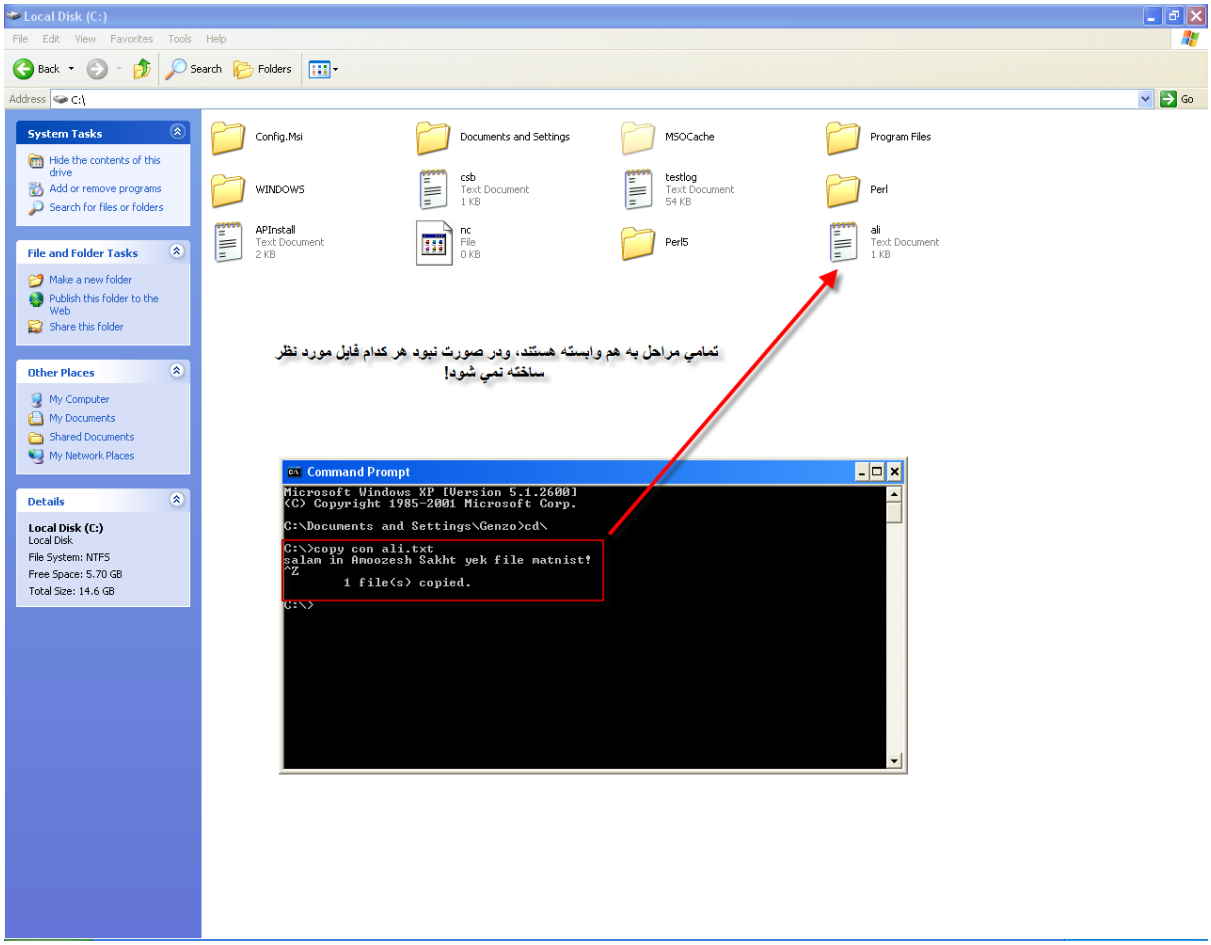
```
Cd\
```

من اسم فایل را ali انتخاب کرده ام: Copy con Ali.txt

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

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

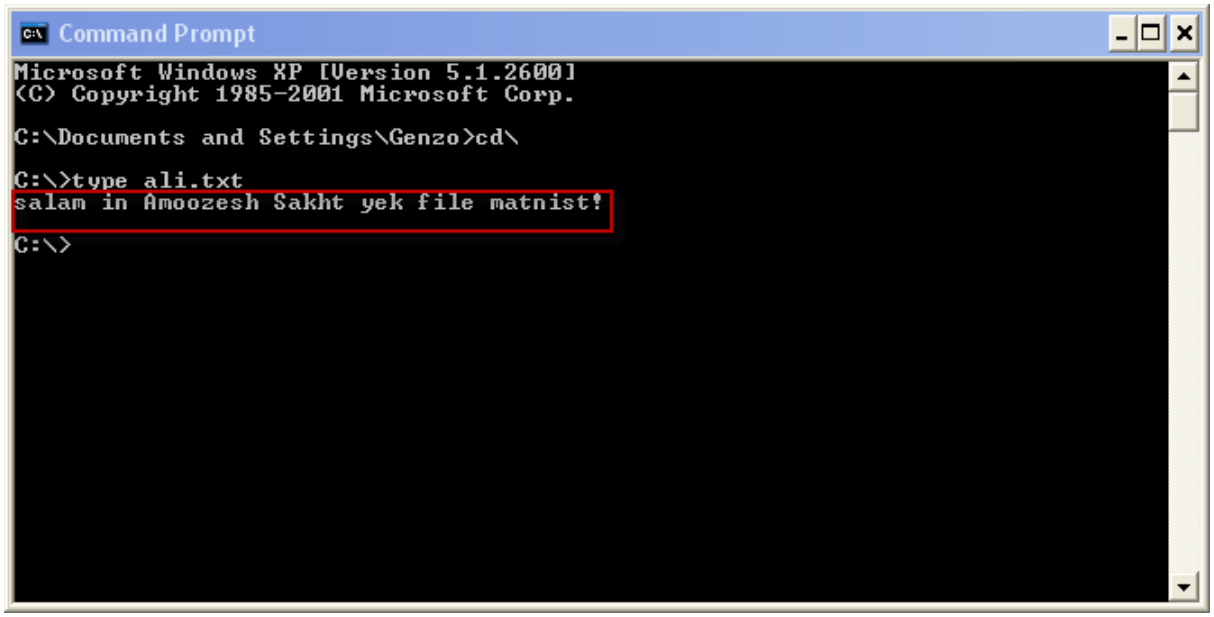
تمامی مراحل بالا به هم وابسته هستند ودر صورت نبود هر کدام فایل ایجاد نمی شود.



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



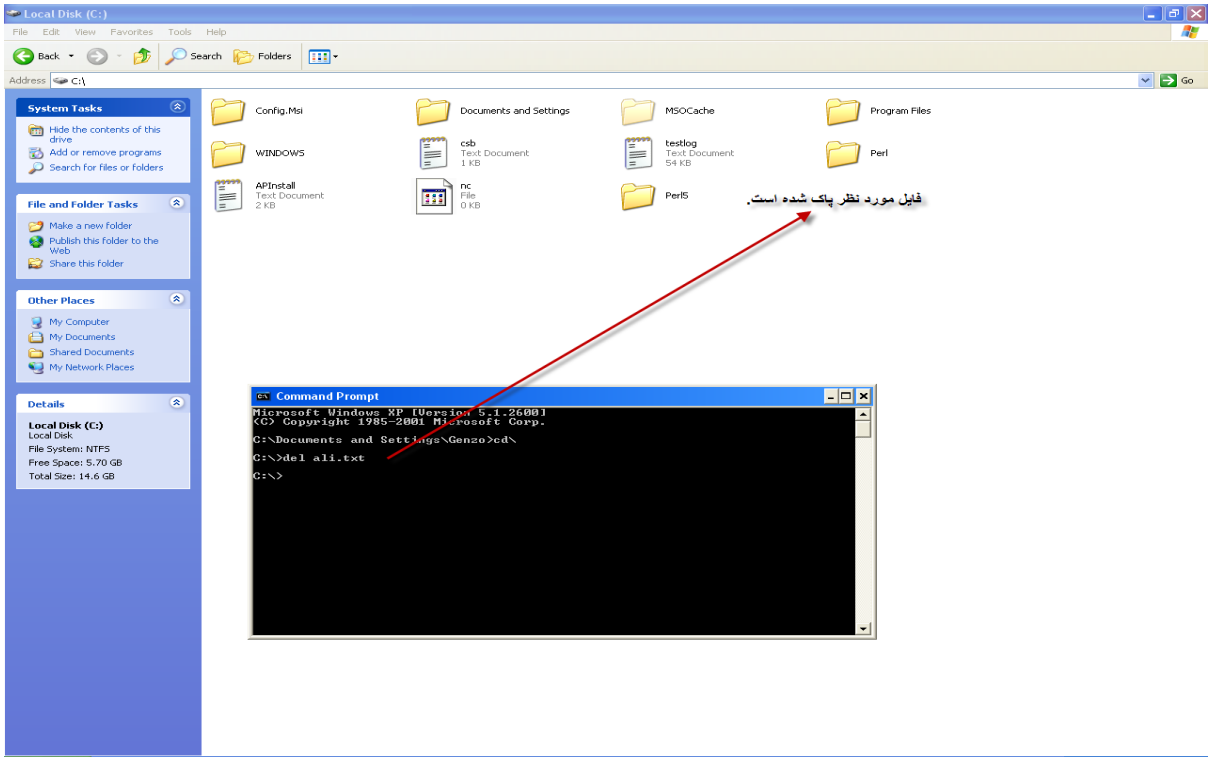
می بینید که متن ما را مورد نمایش قرار داد!

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

با دستور روبرو 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



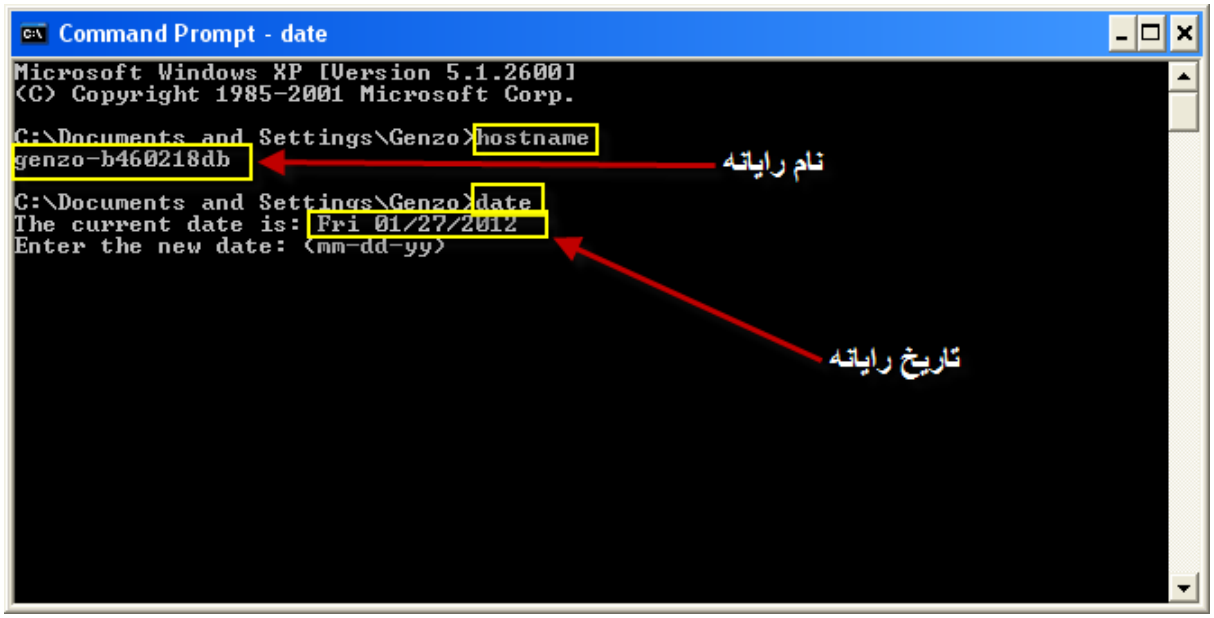
درسنامه یازدهم:نشان دادن مشخصات کامپیوتر

برای دیدن نام رایانه خود از دستور زیر استفاده کنید:

hostname

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

date

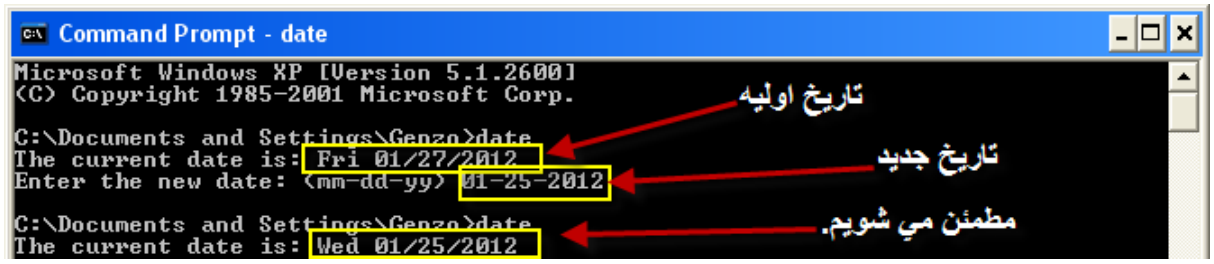


برای تغییر تاریخ باید به ترتیب زیر عمل کنیم:

mm-dd-yy

به جای mmشماره ی ماه رو بنویسیم،به جای dd شماره ی روز و به جای yyشماره ی سال.

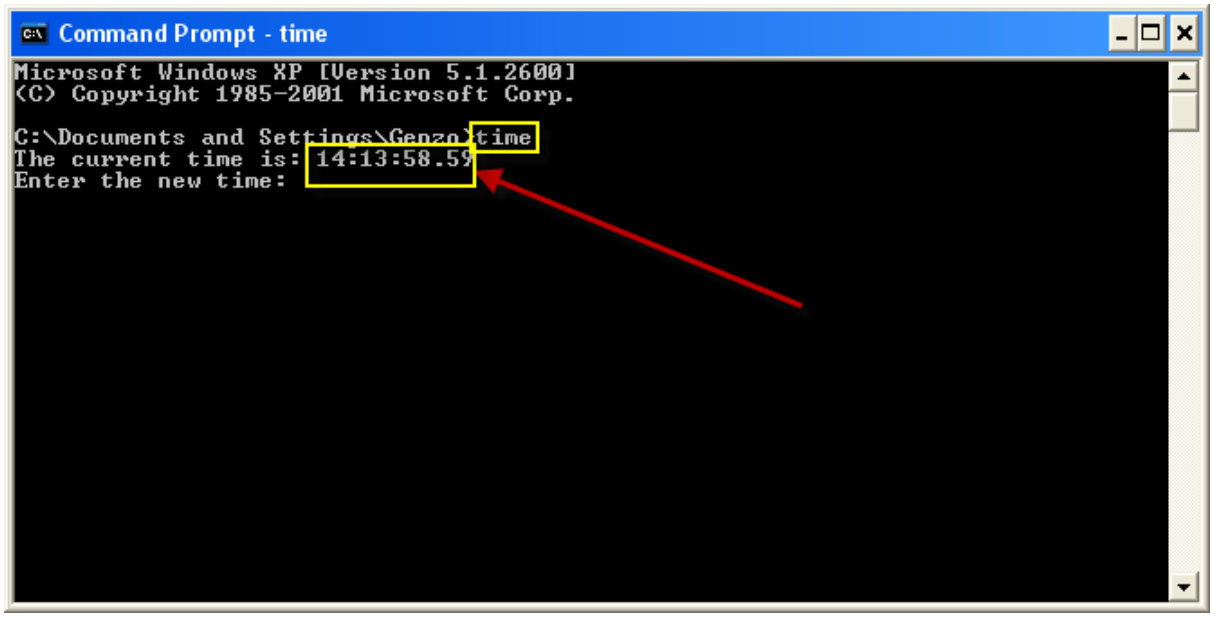
01-25-2012



برای اطمینان یافتن از حاصل کار دوباره دستور dateرا وارد می نماییم.

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

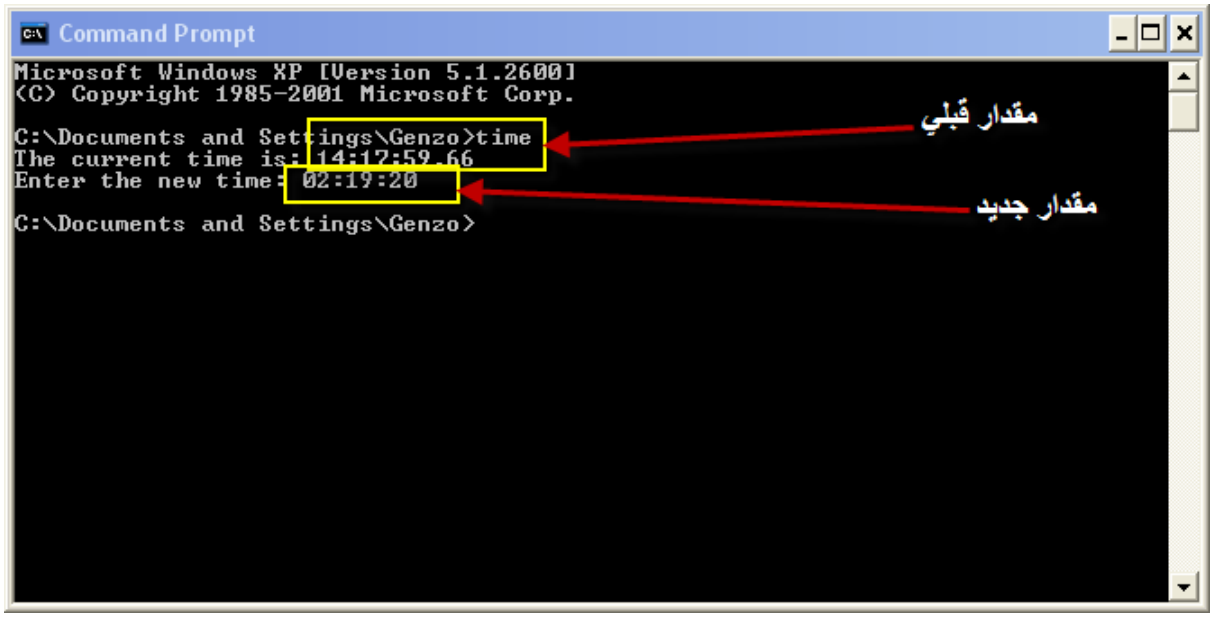
time



برای تغییر آن باید قانون زیر را رعایت کرد:

ثانیه:دقیقه:ساعت

برای مثال من نوشتم: 02:19:20

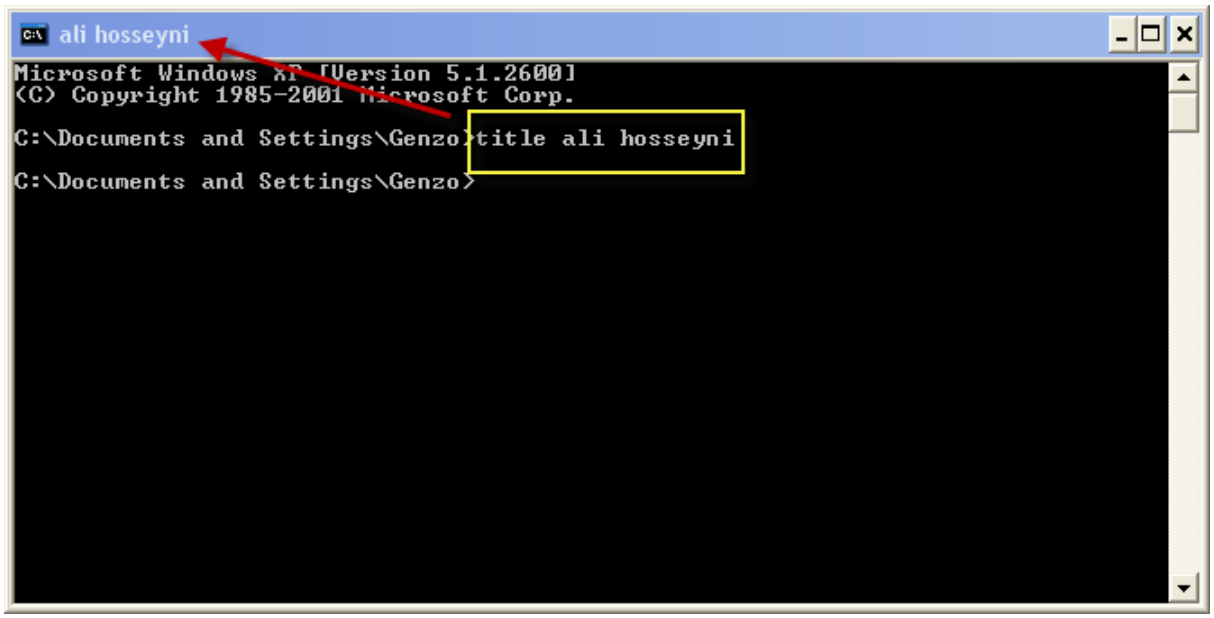


تغییر عنوان و رنگ Cmd

برای تغییر عنوان cmdمی توانیم از دستور زیر استفاده کنیم:

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

Title ali hosseyni



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

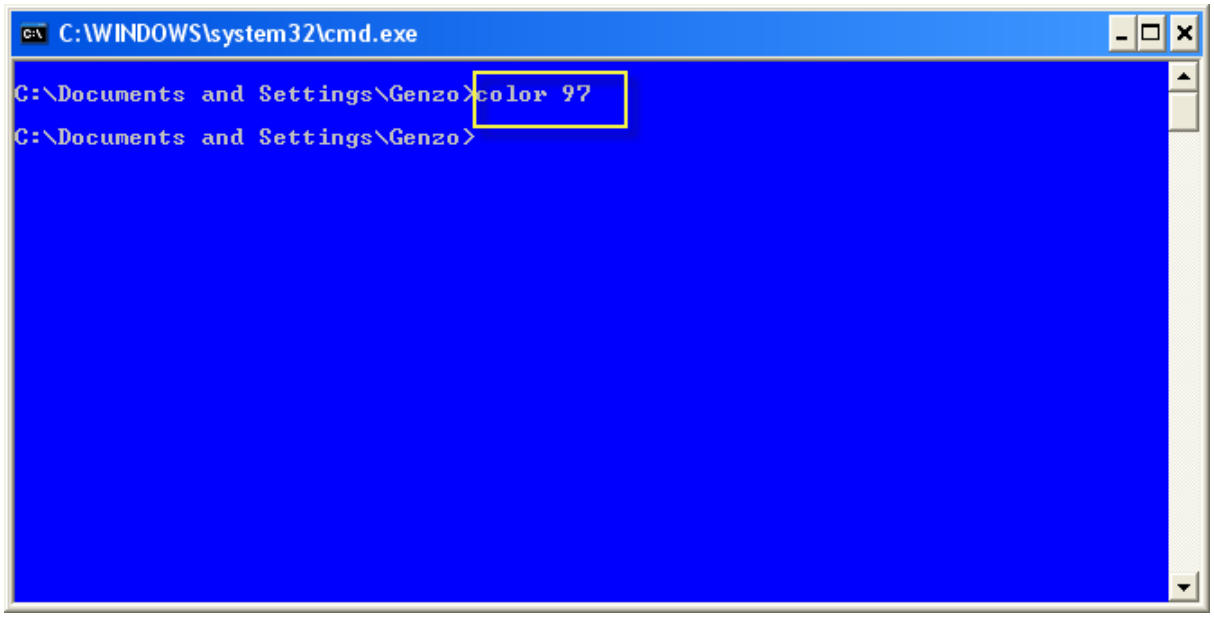
{نکته: اگر عملکرد دستوری را نمی دانید روبروی آن علامت سوال قرار دهید

سپس کلید Enter را روی صفحه کلید فشار دهید وبا جزییات 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.



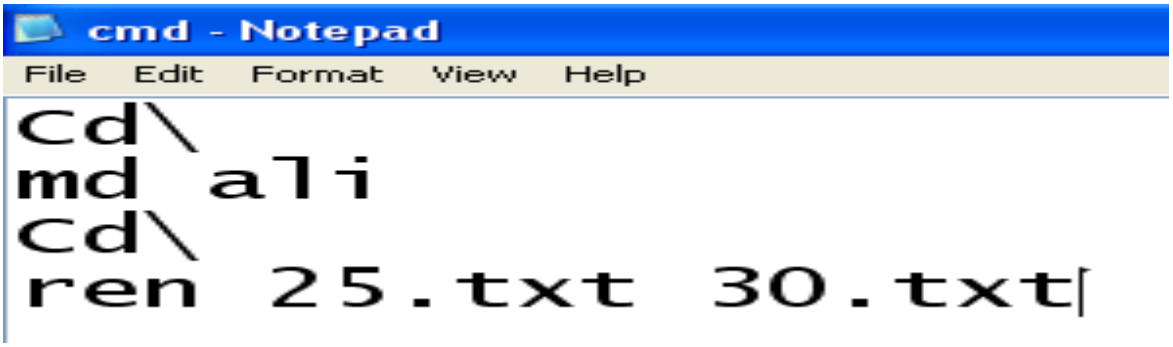
درسنامه دوازدهم:نوشتن دستورات در notepad و اجرای خودکار آن

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

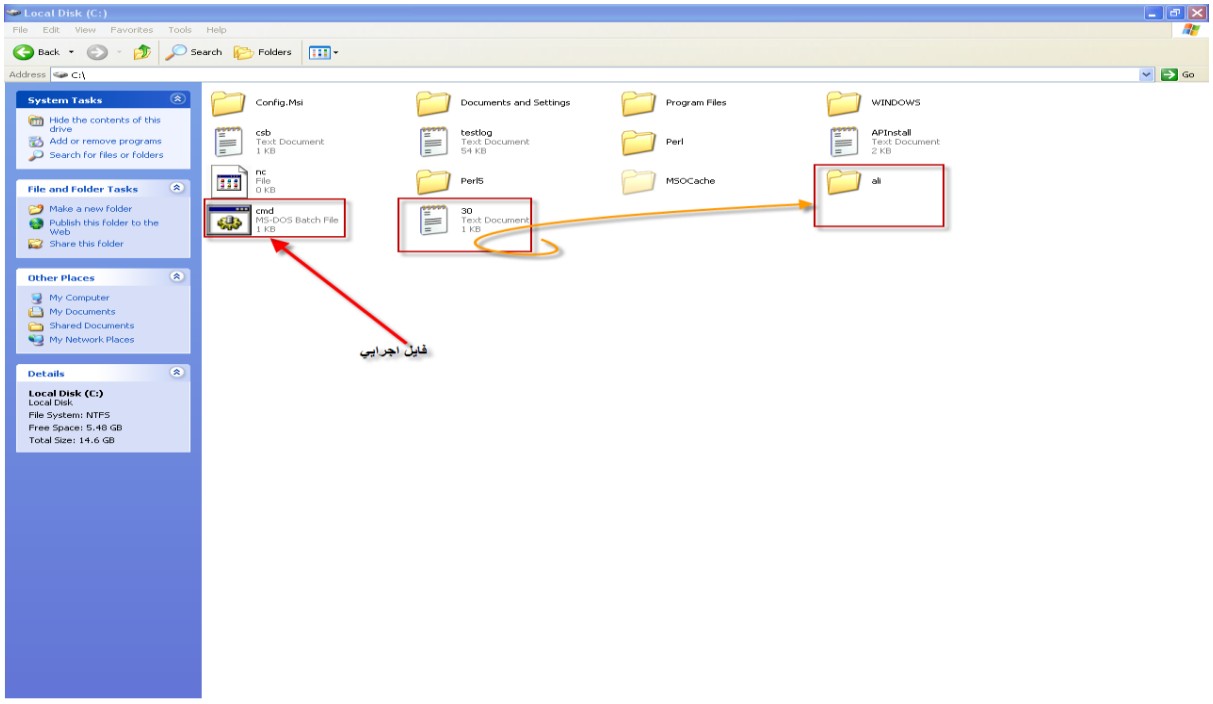
{نکته:هر دستور در notepadباید در یک خط باشد.

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

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



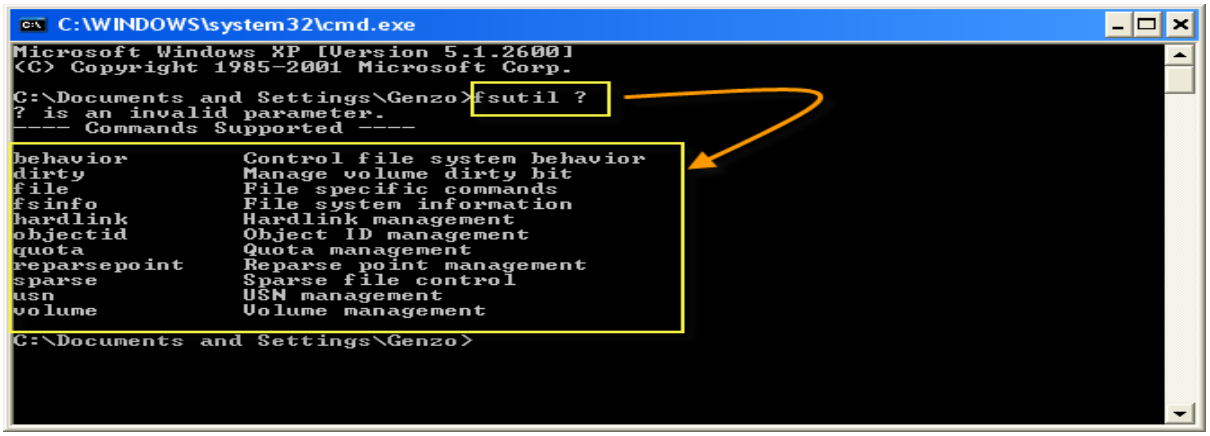
برای ذخیره کردن File>Save As>cmd.bat را انتخاب می کنیم.البته در قسمت Save As Type گزینه all filesرا انتخاب کنید.



درسنامه سیزدهم:ضد ویروس 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 اینترنال 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 ?



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
```

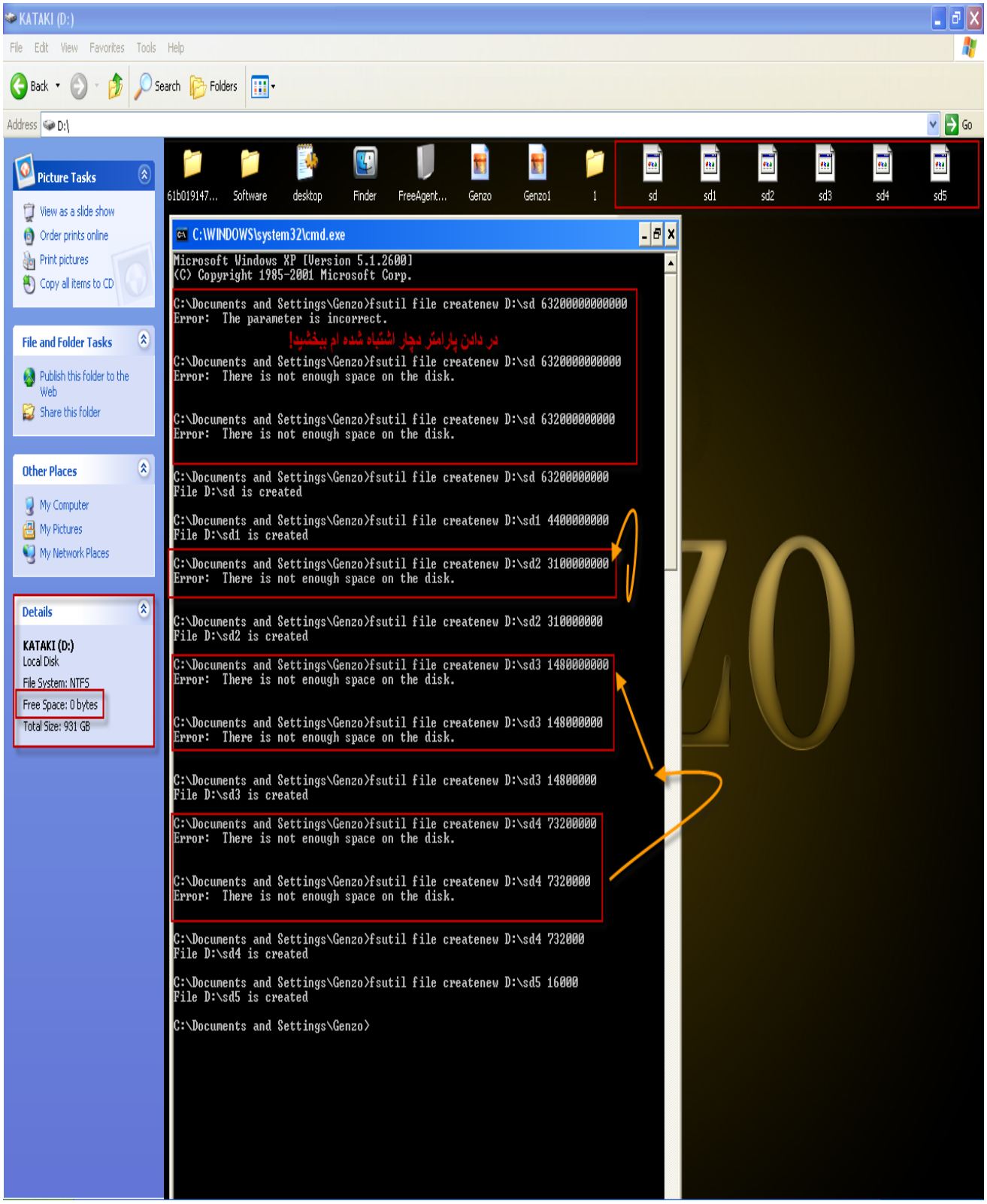
شما باید آنقدر به ساختن این نوع فایل ها طبق دستور بالا بسازید تا فضای خالی حافظه شما پر شود.

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.



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 دستورهای مهم می پردازیم و برای پراکنده نشدن وطولانی نشدن به همین ها هم اکتفا می کنیم البته شما خودتان بروید و تمرین کنید (تکلیف)

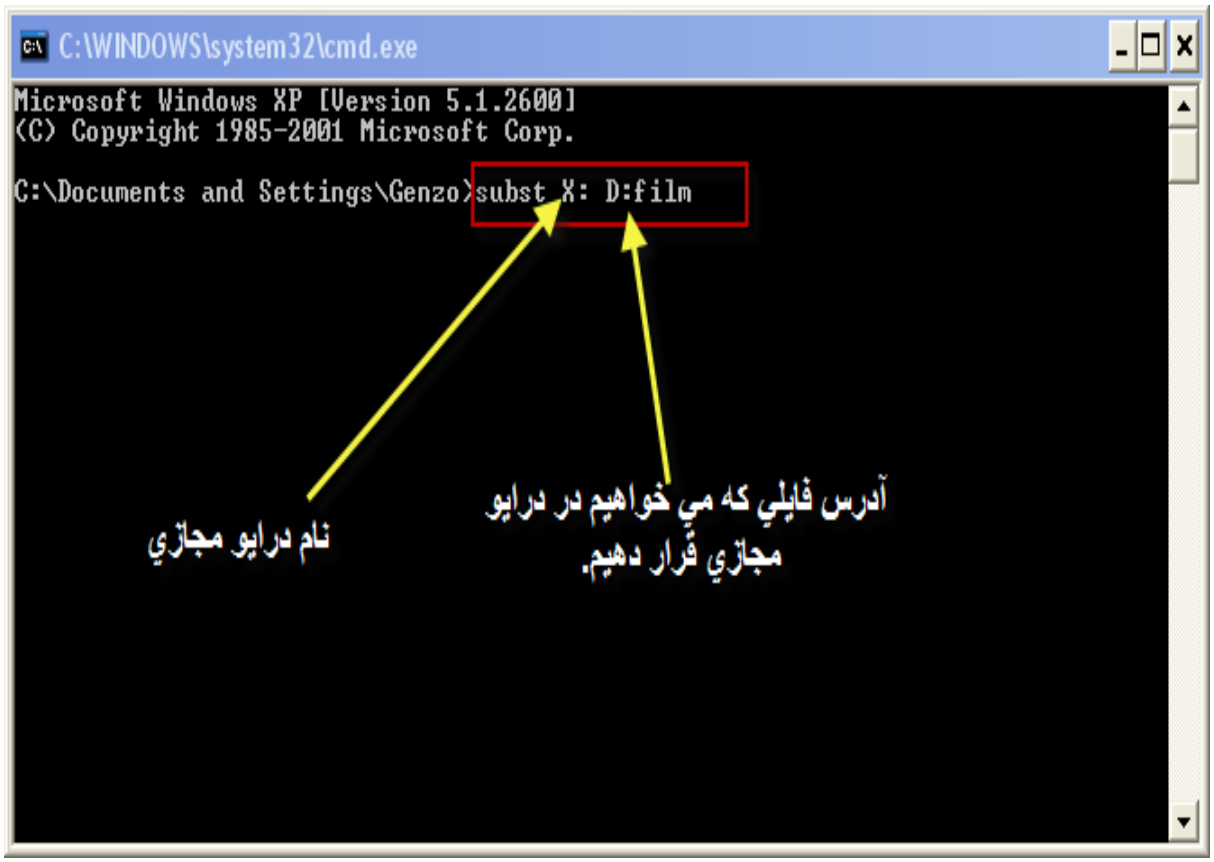
حالا بریم یک درایو مجازی بسازیم:

برای اینکار باید دستور زیر را وارد کرد:

Subst X: D:film

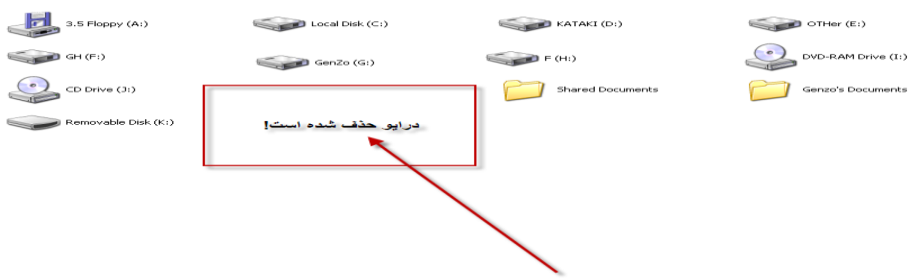
جای x می توانید نام درایو مجازی خود را به دلخواه انتخاب کنید.

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



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 passwordهم رمز عبور را وارد می کنیم، برای وصل شدن بدین صورت عمل می کنیم:

Rasdial /connect ali 256312

وبرای قطع شدن اینترنت از دستور زیر استفاده می کنیم:

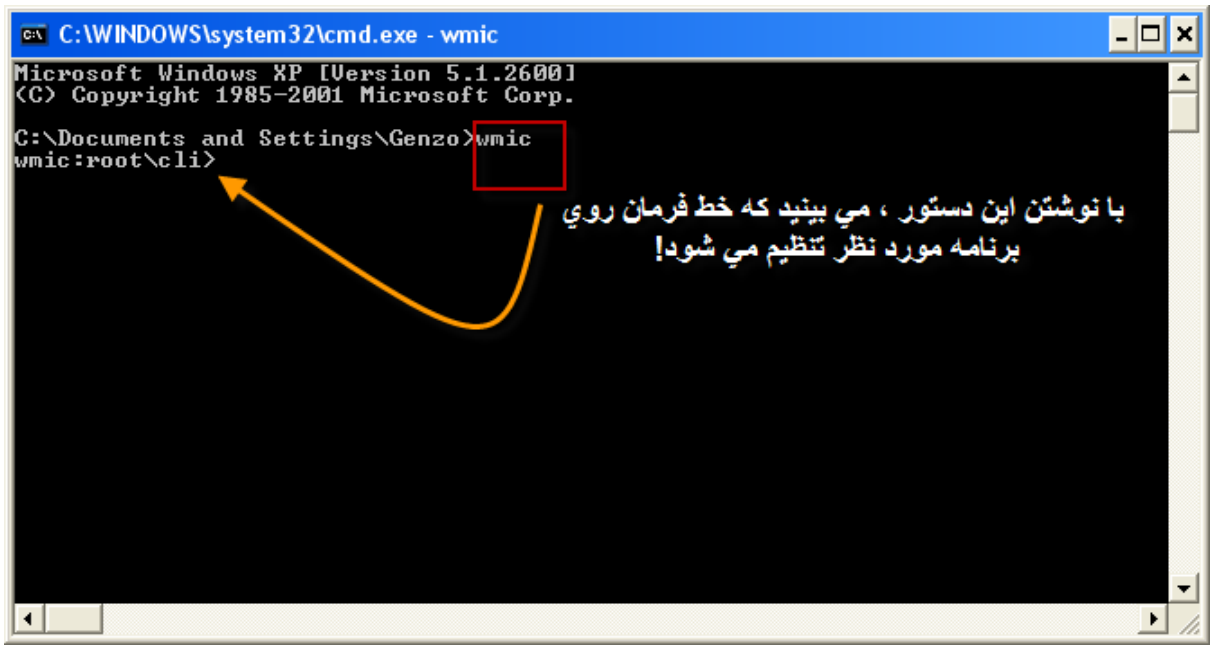
Rasdial /disconnect

!!

درسنامه شانزدهم:نحوه Unistall 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 cmdدر آن می نویسیم :   wmic

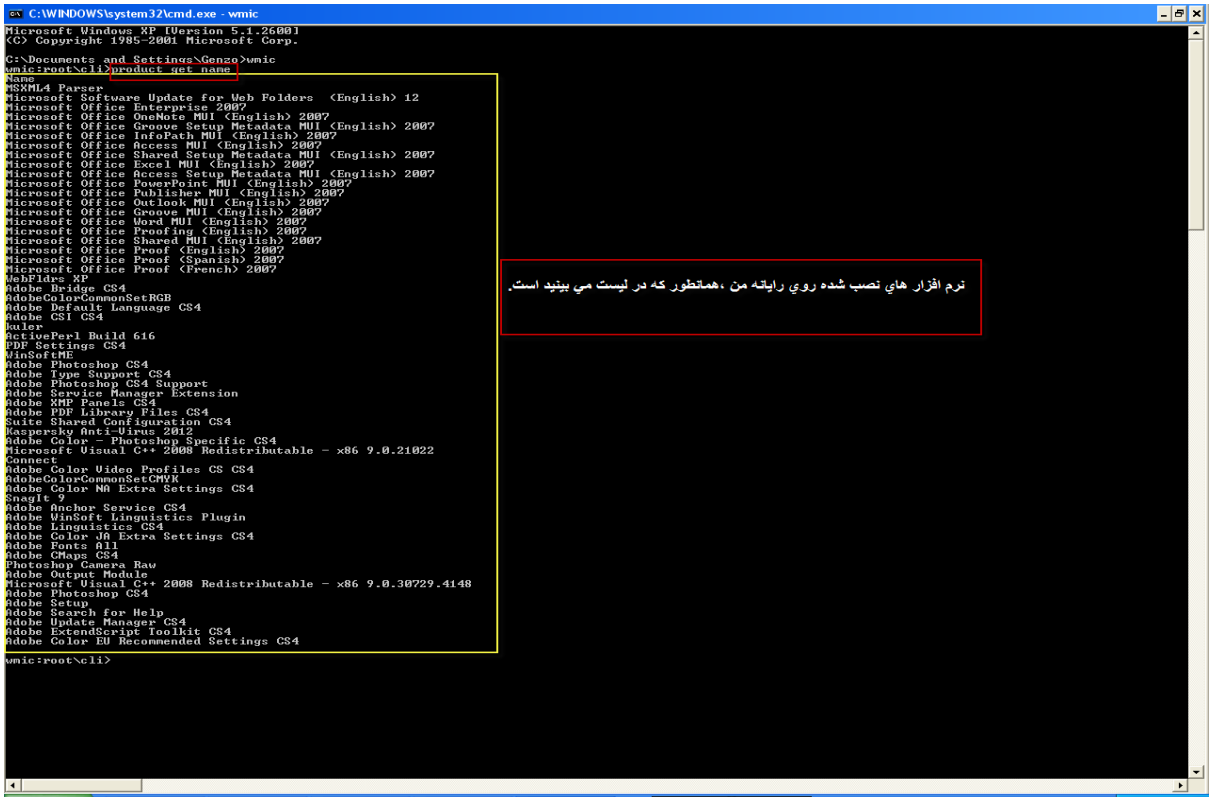


می بینیم می نویسد« برنامه در حال نصب است لطفا صبر کنید»

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

Product get name

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



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

product where name="snagIt 9" call uninstall

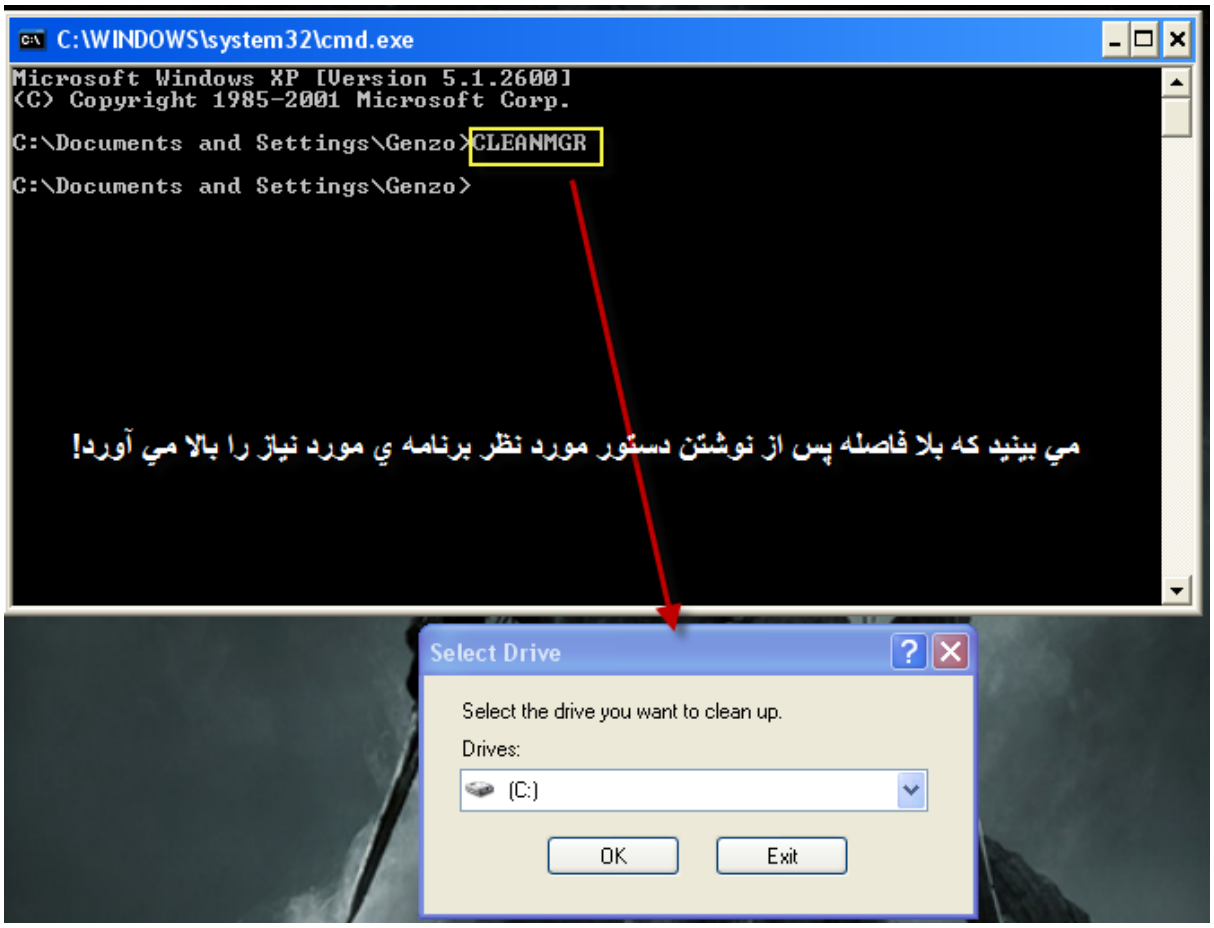
با نوشتن دستور بالا نرم افزار snagIt 9 را حذف می کنیم،من چون الان به این نرم افزار نیاز دارم آنرا حذف نمی کنم و دستور بالا فقط برای مثال بود،خودتون نرم افزار هایی را نصب و حذف کنید،اینم تمرینتون.

درسنامه هفدهم:حذف فایلهای اضافه (disk cleanup)

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

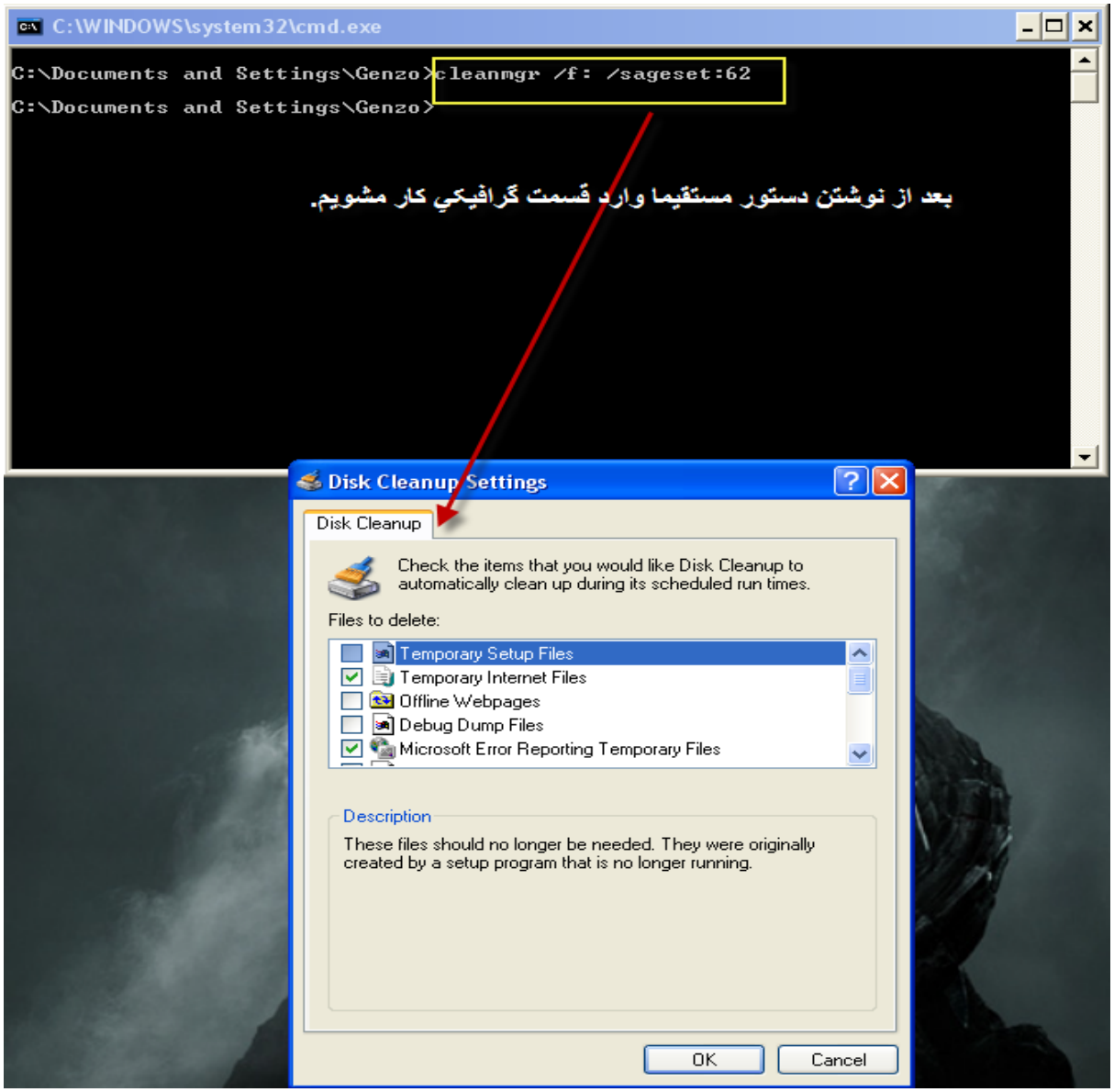
برای اینکار در cmd می نویسیم:

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 fاست وسما نی توانید به طور دلخواه آنرا عوض کنید.

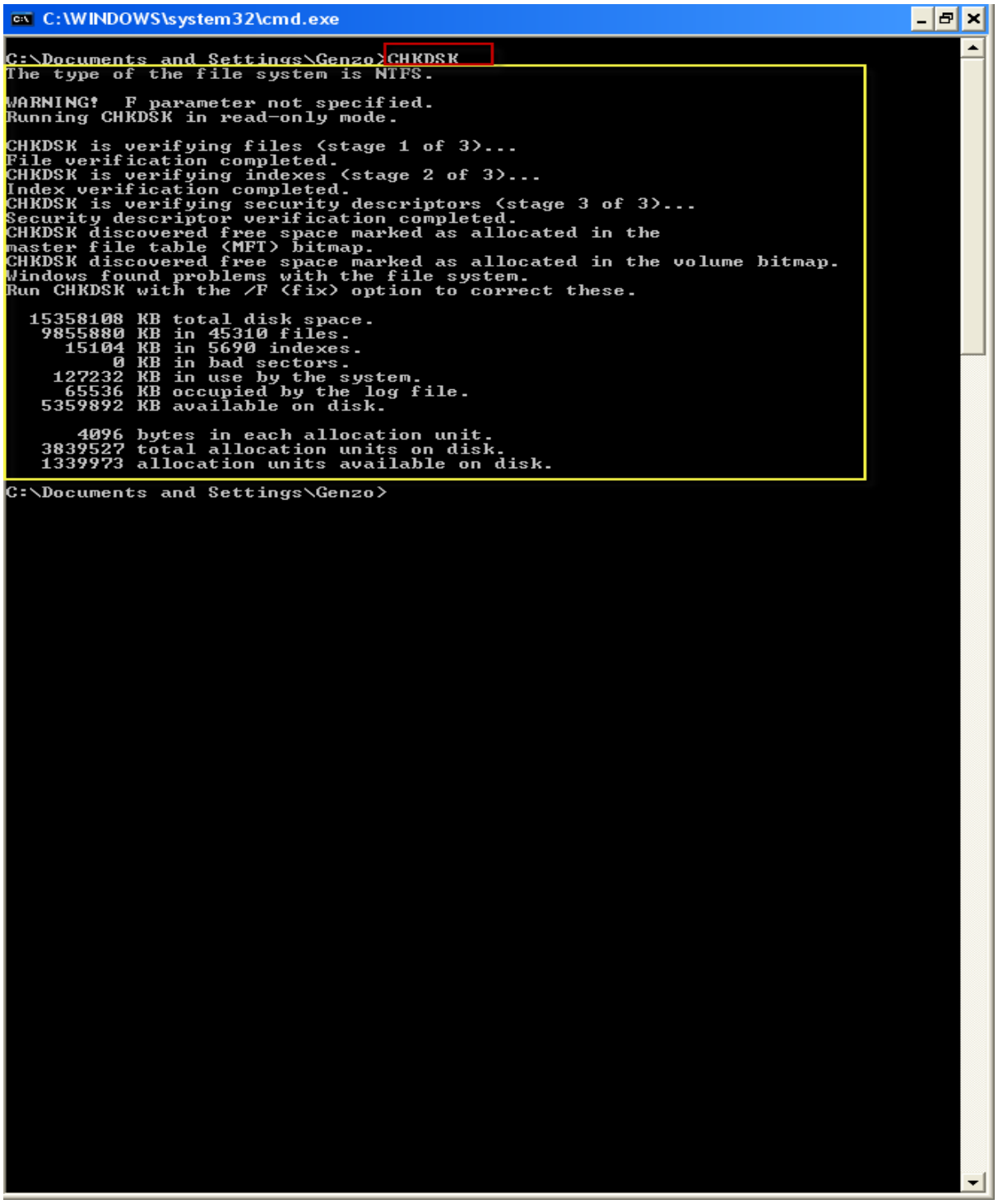
Sageset تنظیمات دیسک کلین آپ را نشان می دهد، وعدد بعد از آن نیز در رجیستری ذخیره شده است که می تواند از 0تا 65535 باشد.

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

گاهی اوقات درایو های ما دچار مشکل هایی می شوند که می توان آن هارا با استفاده از خود ویندوز برطرف کرد مانند دستور chech disk

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

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



به صورت خودکار مشکلات سیستم را درست می کند: f/

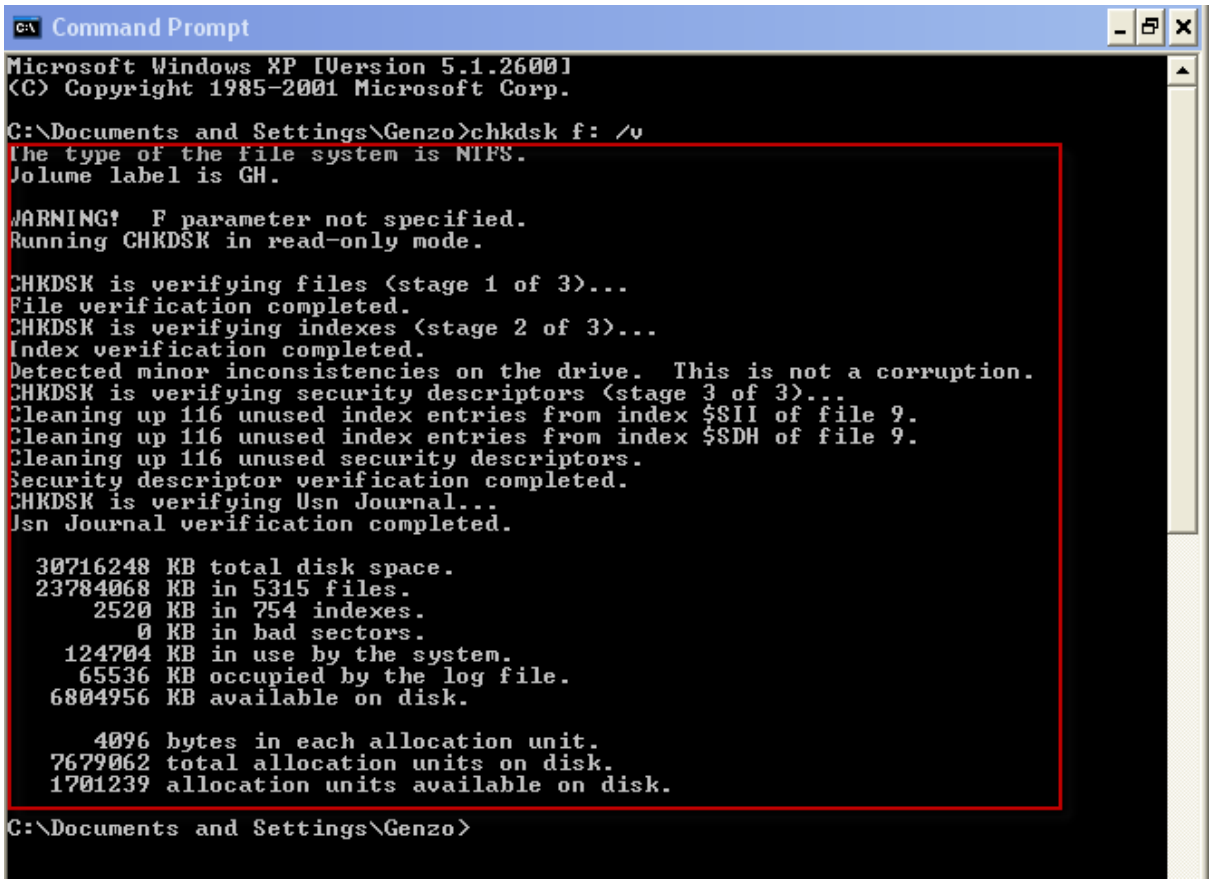
کار دستور بالا را هم انجام می دهد ولی با این تفاوت که با فضای اولیه آغاز میشود: x/

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

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

برای مثال می نویسیم:

Chkdsk f: /v



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 جزییات مهم این دستور آشنا می شویم:

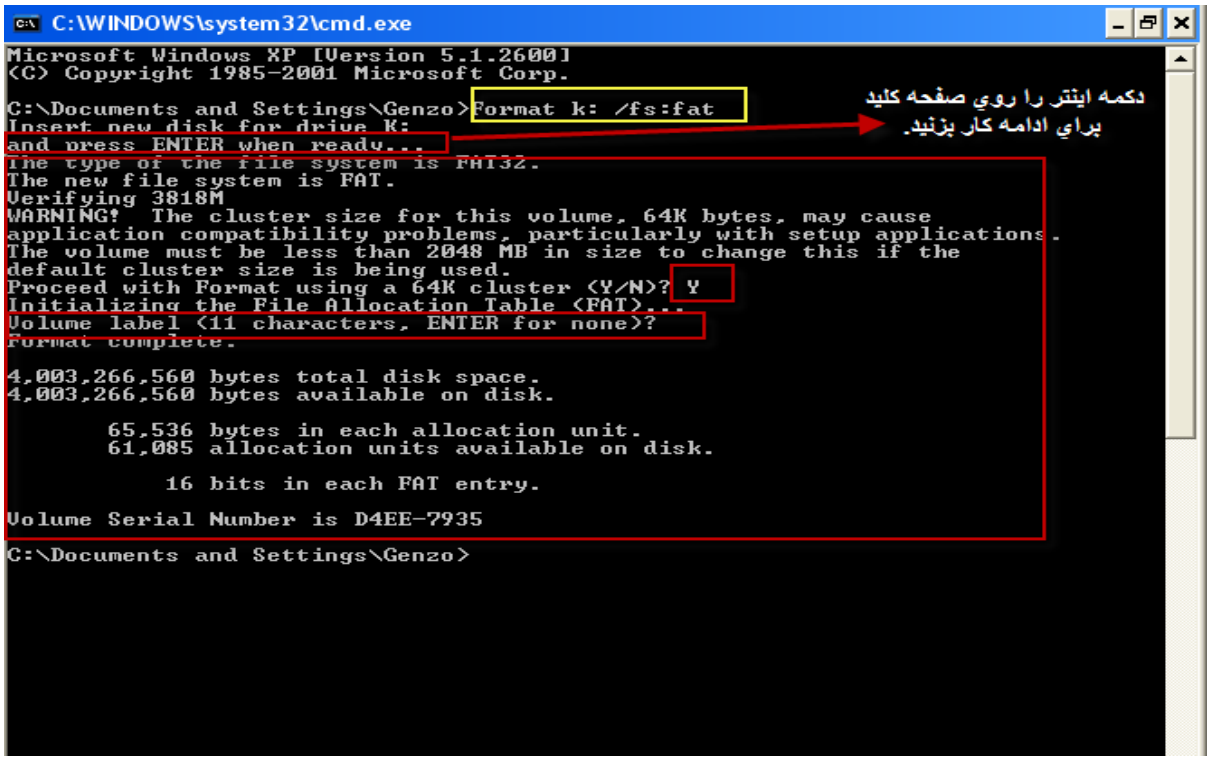
فایل سیستم از نوع ntfsباشد یا fat /fs

فرمت سریع(Quick Format) /q

فایل های فشرده (Compressed) /C

شکل کلی دستور به این صورت است:

Format k: /fs:fat



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

درسنامه بیستم:دستور defragment

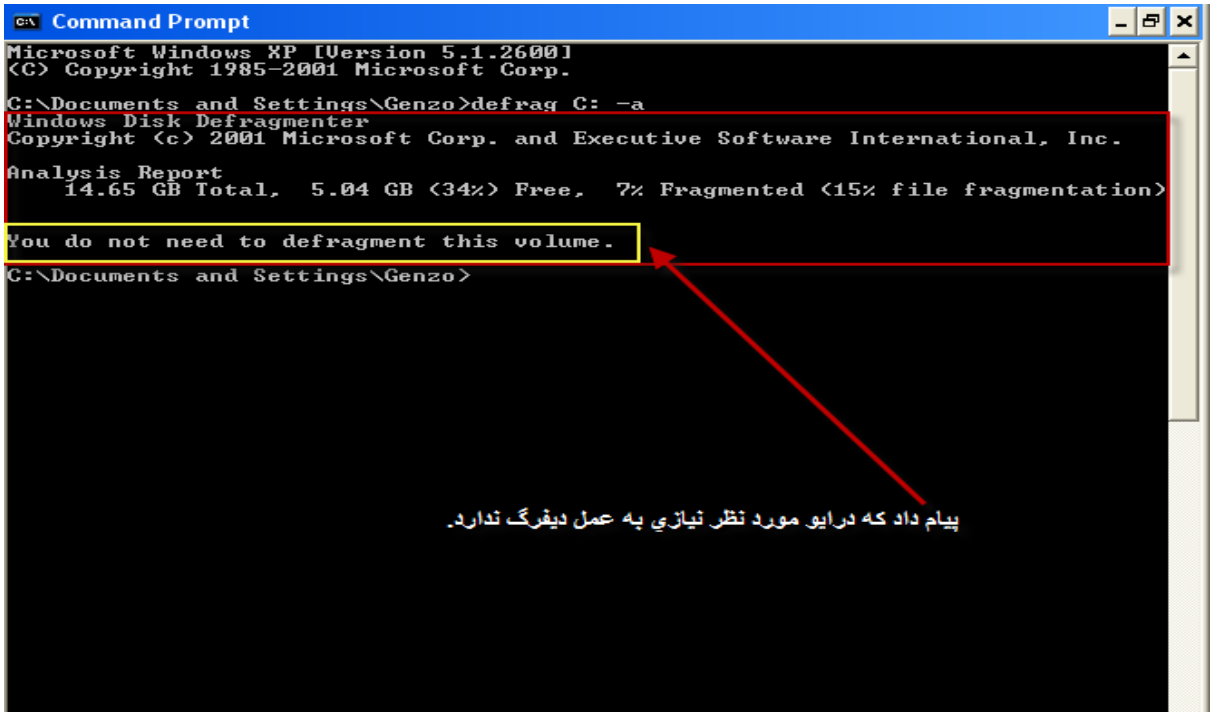
در اینجا ما می خواهیم درایوی را دیفرگ کنیم ، ابتدا جزییات مهم این دستور را یاد می گیریم:

فقط آنالیز می کند: -a

دیفرگ کردن: -f

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

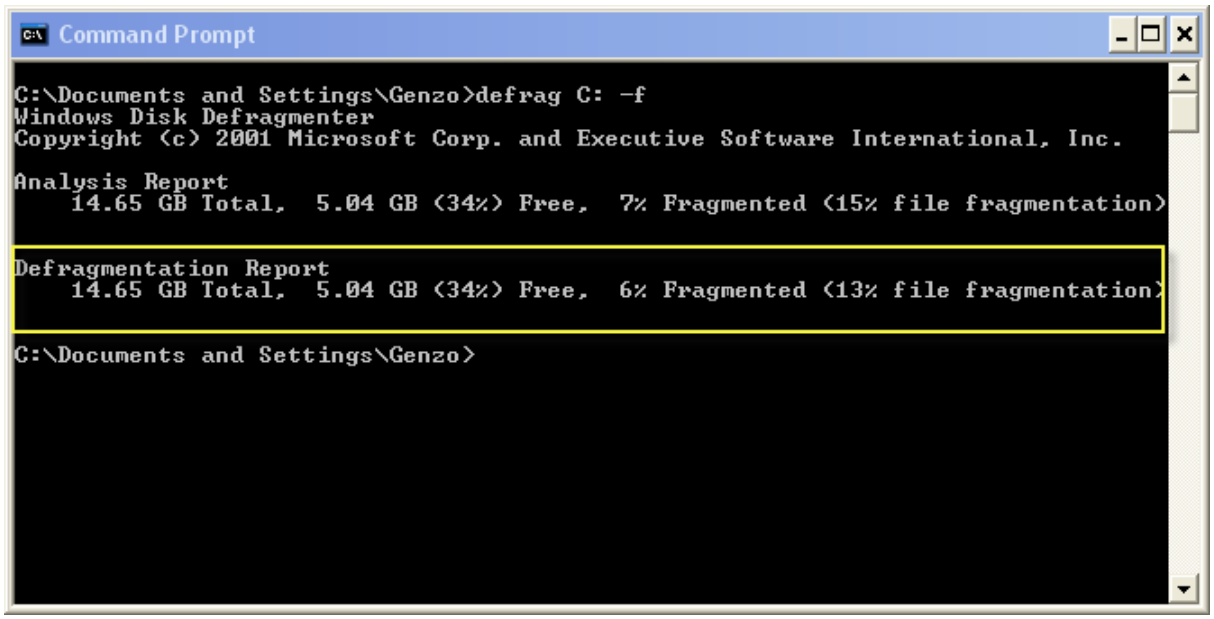
Defrag C: -a



طبق عکس بالا ما دستور آنالیز درایو c را دادیم و برنامه این پیام رابه 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

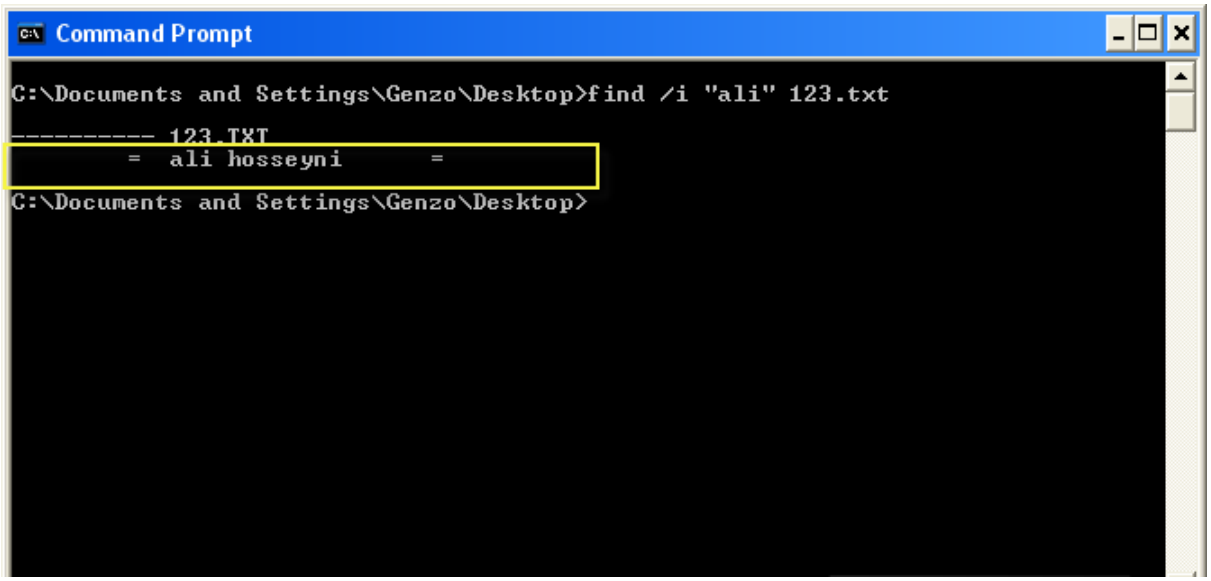


درسنامه بیست و یکم:دستور Find

دراین درسنامه یاد می گیرید که چطور یک فایلی را با دستور findپیدا کنید،برای اینکار من یک فایل متنی در صفحه اصلی رایانه ام (desktop) کپی می کنم، و می خواهم کلمه ali که در آن است را با دستور findمشاهده کنم،خوب اینکار را میکنیم:

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

در دستور بالا کلمه aliرا در فایل متنی ۱۲۳ می خواهم پیدا کنم.



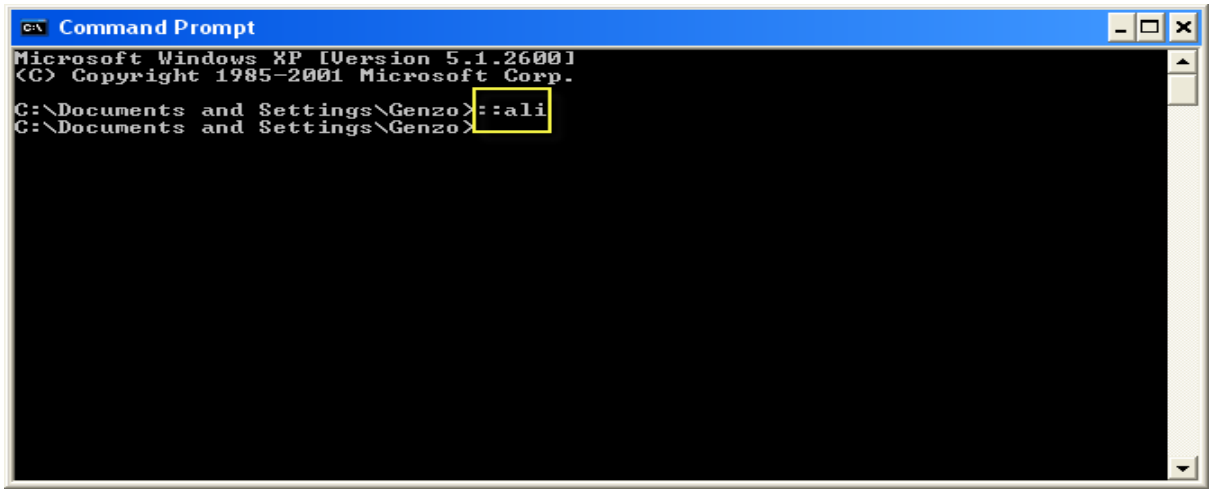
پیدا کرد!!!!

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

در این درس با سه دستور مهم cmdآشنا می شوید که باید بلد باشید!

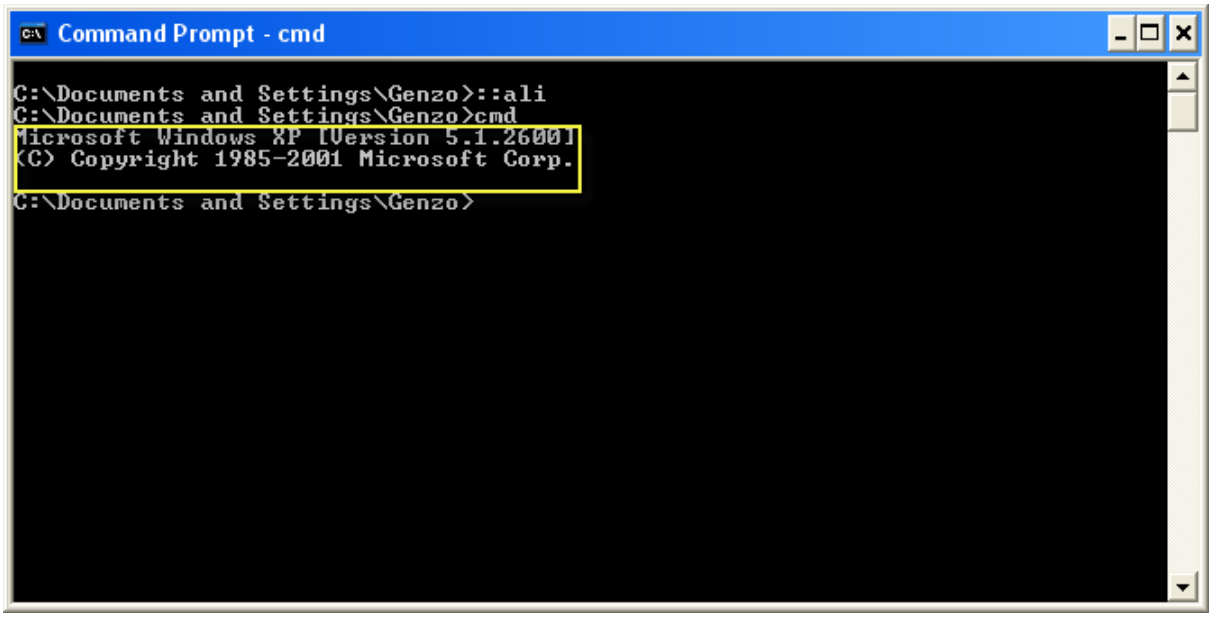
در زبانهای برنامه نویسی دستوری با نام commenting وجود دارد که برای هر کدام متفاوت با دیگری است،البته cmd برنامه نویسی نیست!

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

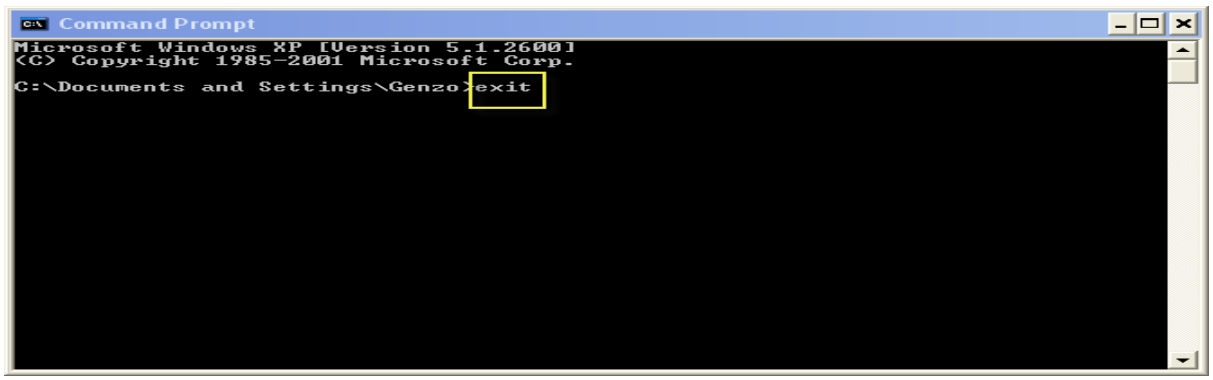


اگر : : استفاده نمی کردیم برنامه error می داد.

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

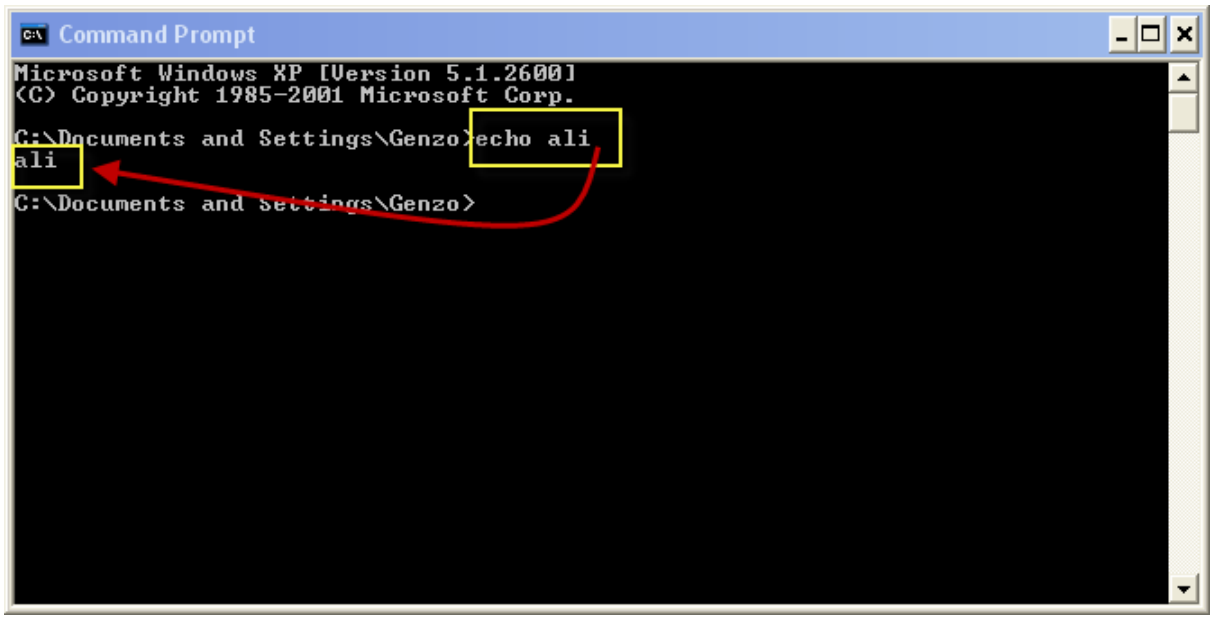


دستور سوم:دستور exit شما را از خط فرمان خارج می کند.



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 رابررسی کنید:



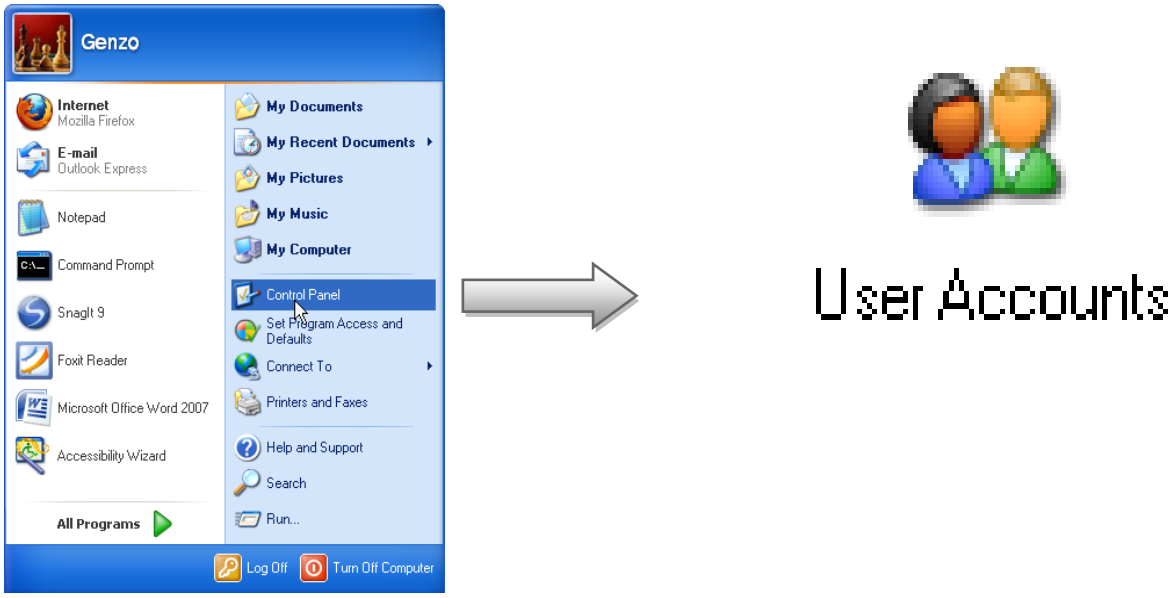
به برنامه گفتیم بگوید ali ، پس گفت!

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

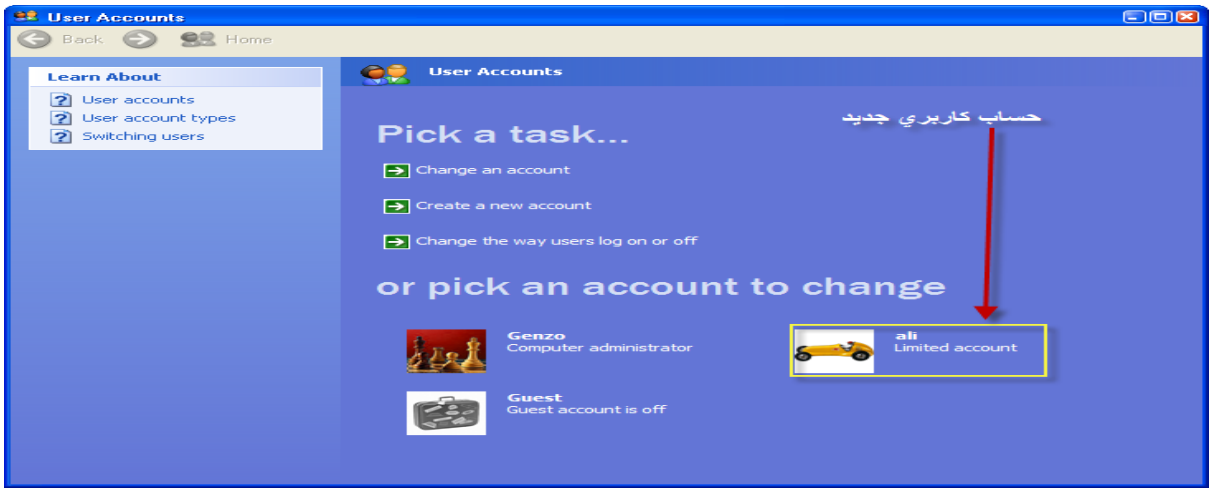
پس از نوشته شدن دستور در خط فرمان می بینید که یک فایل متنی به نام 0121 ساخته شده است!

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 :



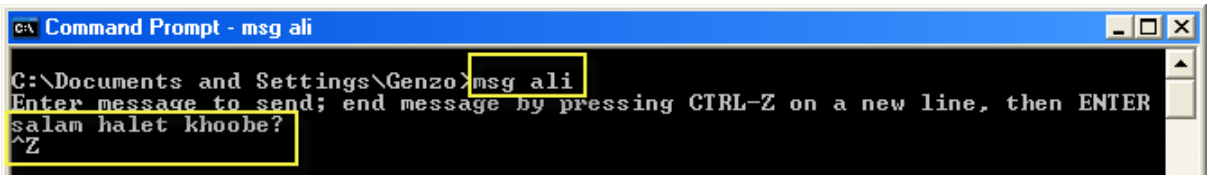
از دادن توضیحات بیشتر وطولانی شدن آموزش خودداری می کنیم،مثلا من یک حساب کاربری با نام Aliساخته ام و می خواهم پیامی را برای آن بفرستم پس به ترتیب زیر عمل می کنم:



سپس cmdرا باز کرده و به صورت زیر عمل می کنیم:

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

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:



پیام با موفقیت ارسال شد!

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

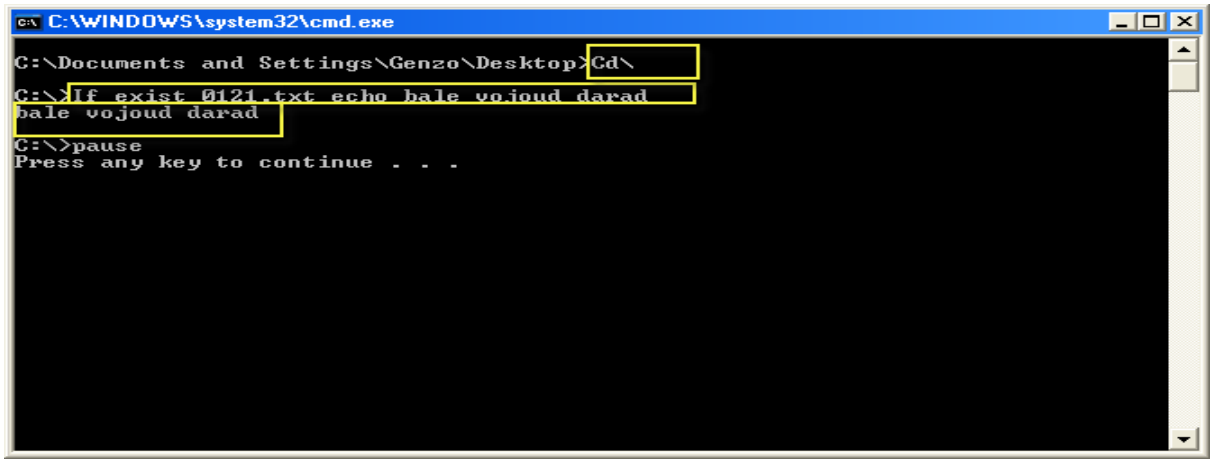
کلمه exist در لغت به معنای وجود داشتن است و ما با استفاده از آن می خواهیم از وجود یا عدم وجود یک فایل یا پوشه مطلع شویم،برای مثال من فایلی را در درایو c قرار داده ام و حال می خواهم ببینم آیا این فایل در این درایو موجود است اگر هست پیامی ظاهر شود، ابتدا نرم افزار notepad راباز کرده و دستور زیر را در آن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

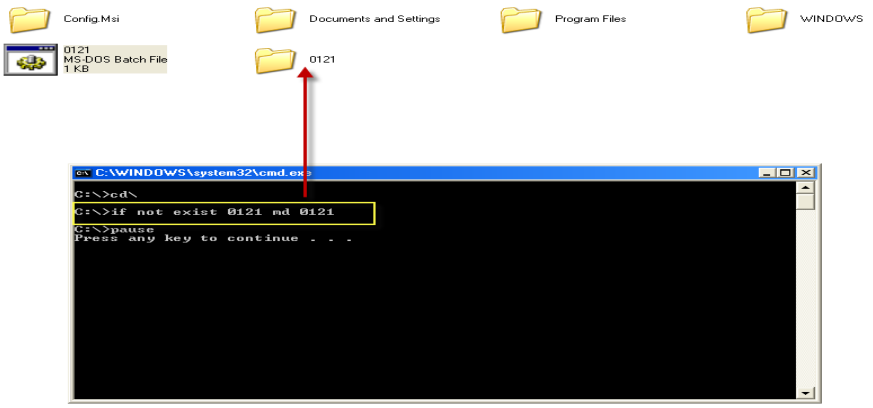


همانطور که می بینید پیغام (بله وجود دارد) را به ما نشان داد!

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

```
cd\
if not exist 0121 md 0121
pause
```

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

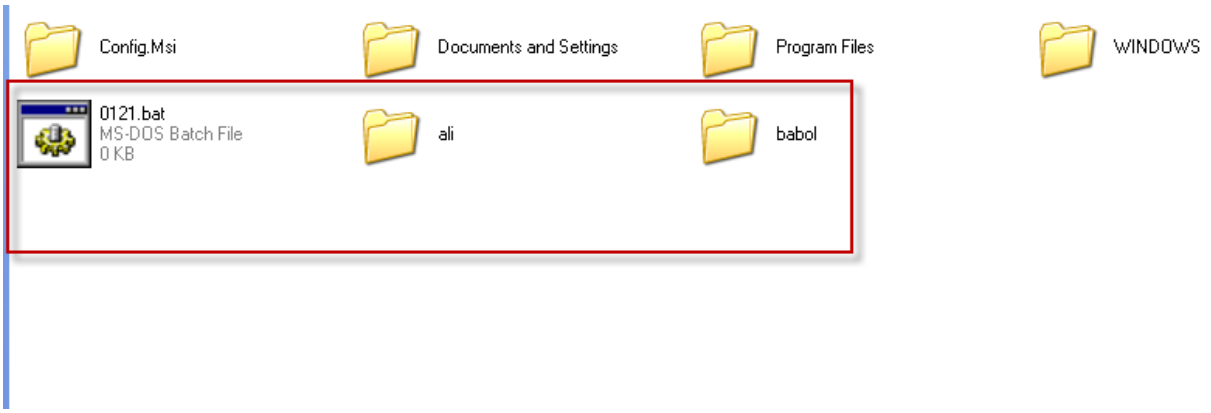


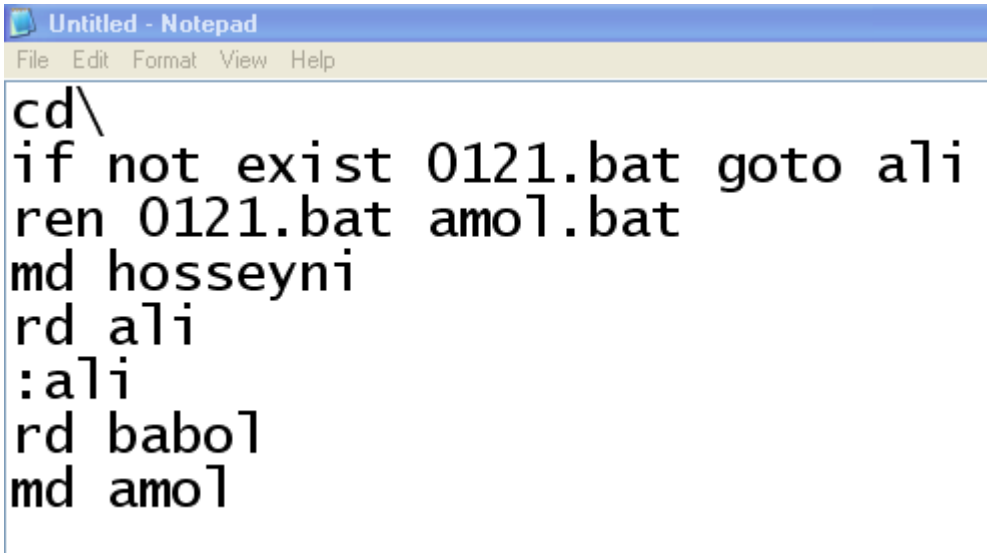
همانطور که میبینید پوشه 0121ساخته شده است.

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 dاست ولی d: 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:





شروع به دادن توضیحات برای هر دستور می کنیم:

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

در خط دوم به برنامه می گوییم اگر بَچ فایل 0121 وجود ندارد به مکان ali برود.

در خط سوم درخواست تغییر نام بچ فایل 0121 رابه amolداریم.

در خط چهارم و پنجم به برنامه می گوییم تا پوشه hosseyniرا بسازد و پوشه aliرا پاک گرداند.

در خط ششم از برنامه می خواهیم به مکان aliبرود .

در خط هفتم و هشتم از برنامه می خواهیم تا پوشه babolرا حذف کند و پوشه amolرا 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
```

در دستور بالا من نام حساب کاربری را aliو 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 ازدستور زیر استفاده کنید:

Net user ali 256312 /add /tohid1234

برای برداشتن دامنه اضافه شده می توانید از به جای jladd delete اسفاده 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 آنرا 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؟

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

Sبه معنای اینکه ما گزینه shutdownرا انتخاب کردیم.پس از اجرا این کد رایانه شروع به شمارش زمان داده شده می کند تا خاموش شود حال پطور جلوی این دستور را بگیریم؟

برای این کار کد زیر را وارد میکنیم:

```
Shutdown -a
```

برای ریستارت کردن رایانه از طریق cmdباید 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 offکردن رایانه از دستور زیر استفاده می کنیم که لحظه ای است (یعنی در لحظه عمل می کند و نمی توان از آن جلوگیر کیرد)

```
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
```

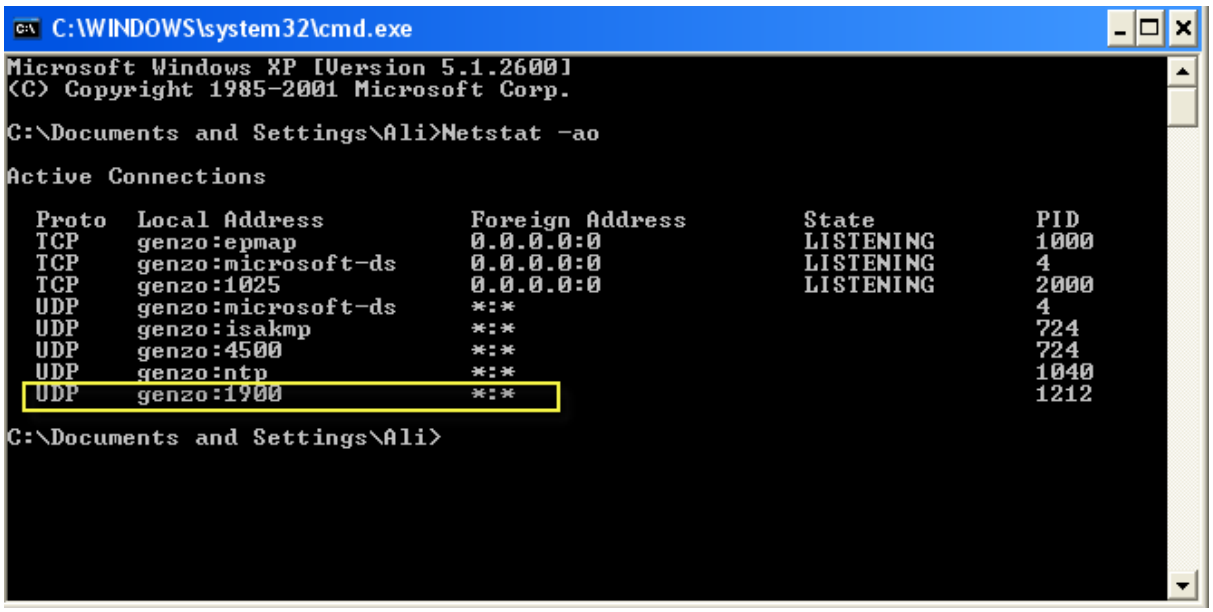
خوب اگه بخواهیم هر لحظه از پورت های باز یا بسته مطلع شید باید هی این دستور رو تایپ بکنیم!!!!

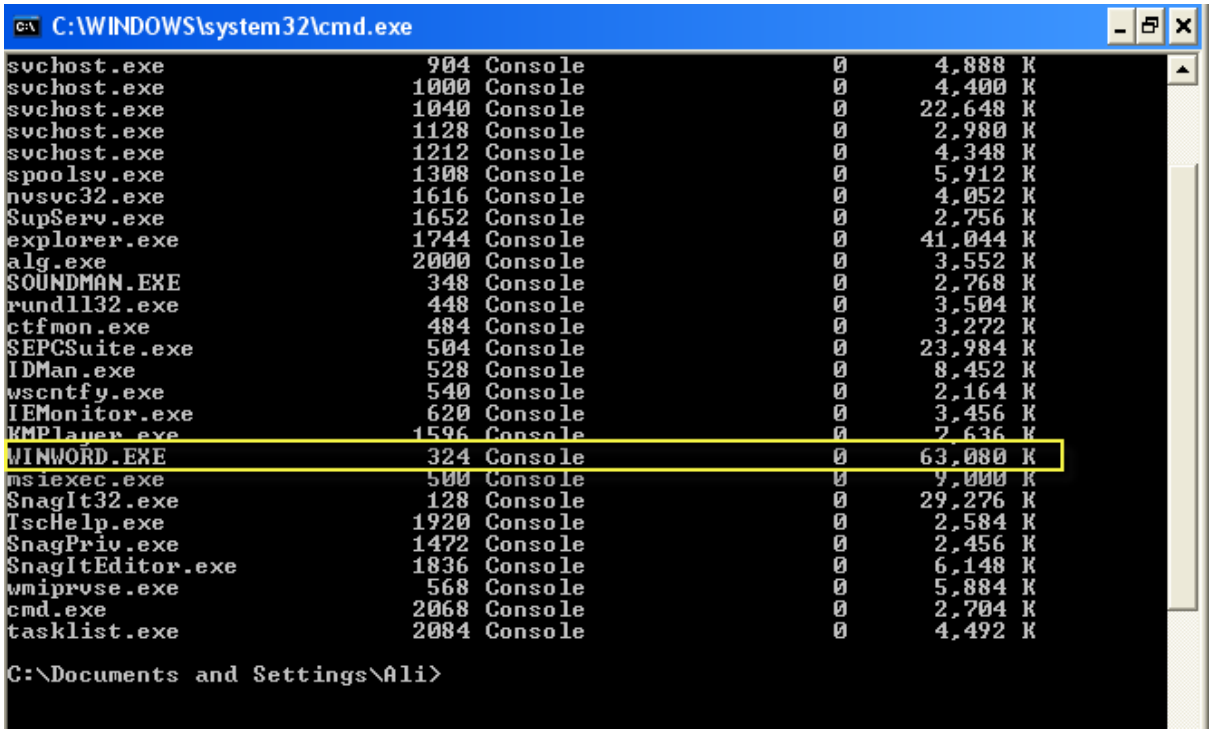
این دستور تمام پورت های باز رو به همراه شماره پروسه ای که اونو باز کرده نمایش می دهد حالا برای بدست اوردن پروسه ها و غیر فعال کردن آنها دستور:

Tasklistیاnetstat –abnیاqprocess

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:





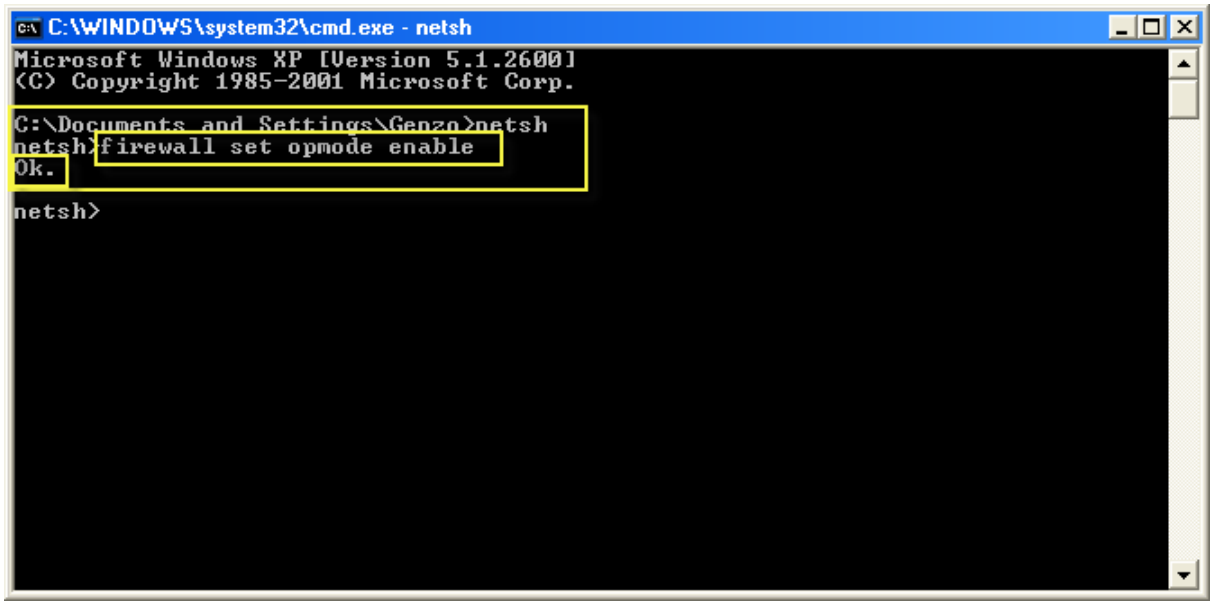
در این قسمت می آموزید چطور با دستوری فایروال را خاموش و یا روشن کرد و این کار را به صورت یک بچ فایل هم نیز انجام دهید!

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:

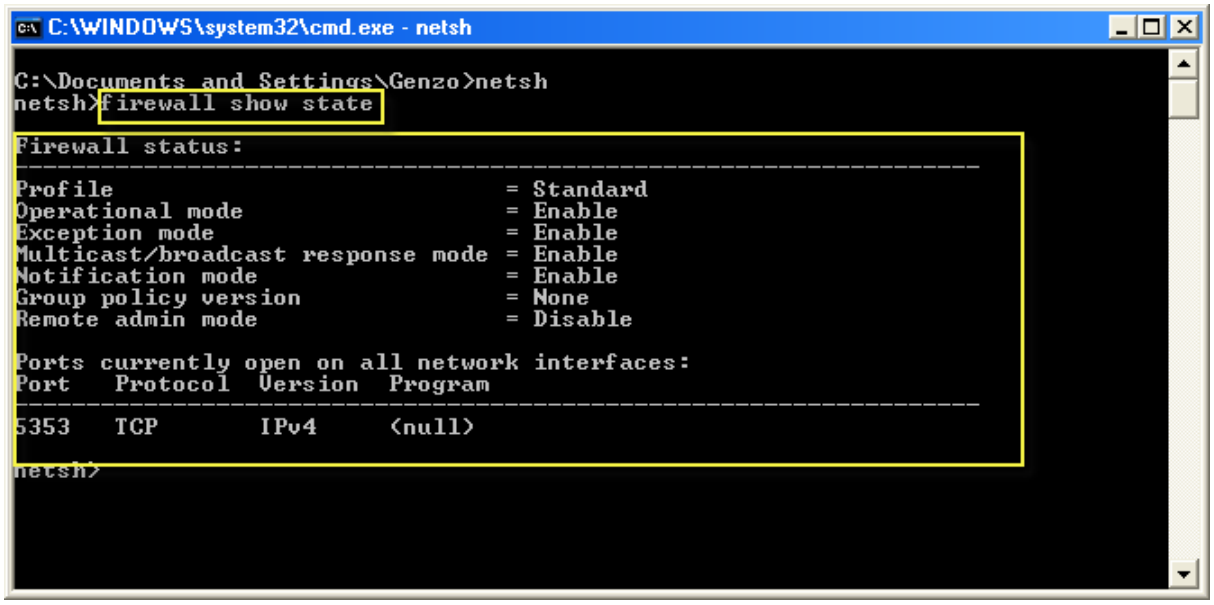
firewall Set opmode enable



برای غیر فعال کردن آن نیز باید جای enable ، disableگذاشت!

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

Firewall show state

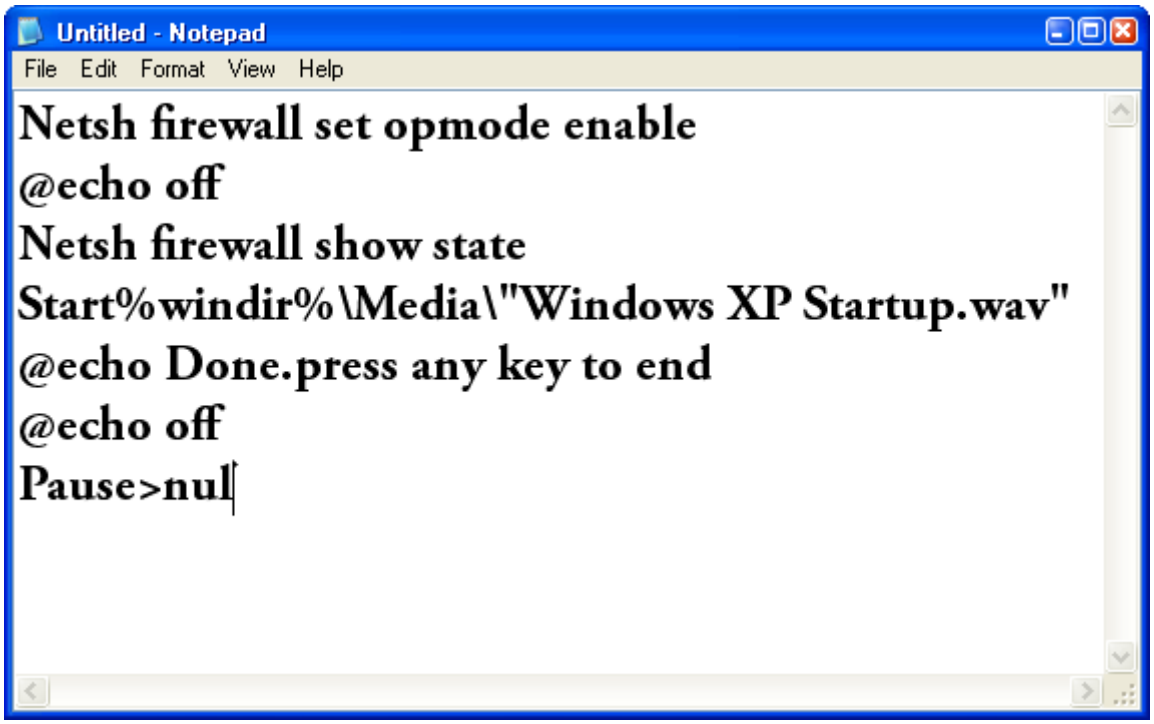


برای اینکه اینکار به صورت خودکار انجام بشه ونیازی به طی مراحل بالا نباشد اینکار را به صورت یک بچ فایل انجام داده و در پوشه استارت آپ ذخیره کنید.

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

روی startکلیک راست کرده و گزینه openرا انتخاب کنید سپس programراباز کنید ودر اخر پوشه start upرا باز کرده و بچ فایل را در آن کپی کنید.

حال بریم سراغ طراحی بچ فایل:



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 بازدن دکمه ای مثل Enter از بچ فایل خارج می شوید.

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

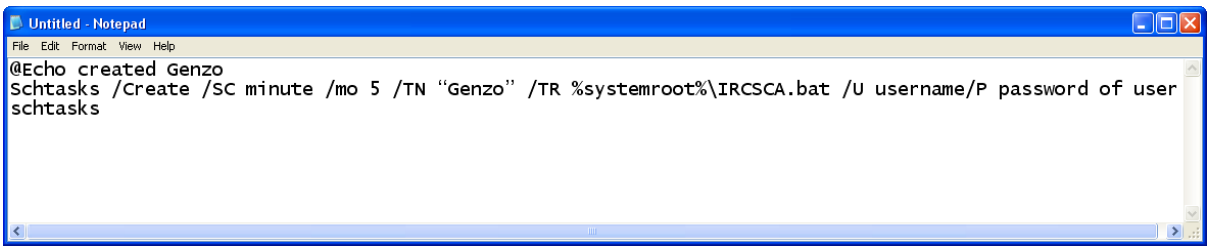
دستور Schtasks:

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 همرا 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>nul
```

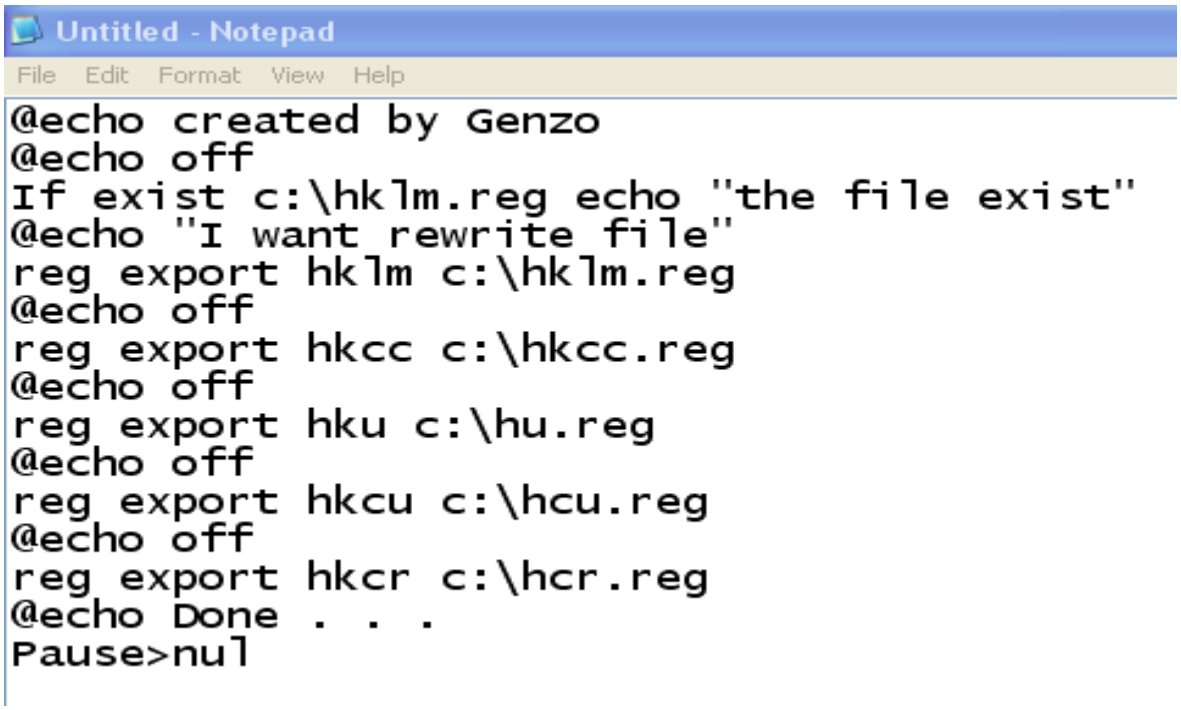
۲-این بچ فایل را یکبار اجرا کنید:



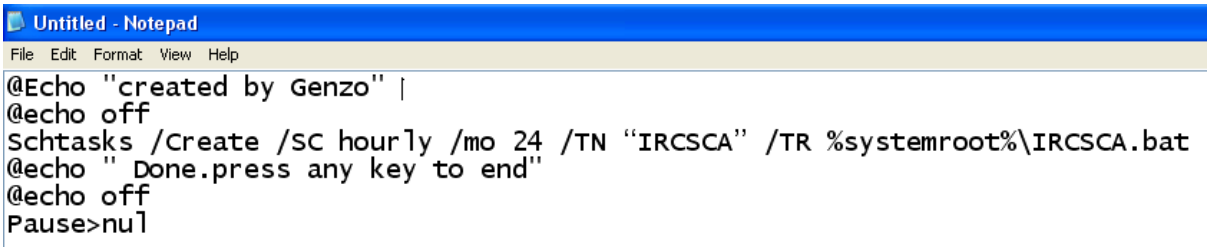
یه نفوذگر می تواند از دستور بالا طوری استفاده کند که وقتی کاربر در حال خروج از سیستم هست وظیفه مورد نظرش انجام بشه با این کار سیستم های امنیتی را می تواند دور بزند و کاربر هم مشکوک نشود، حالا چطور ممکنه!!!

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

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

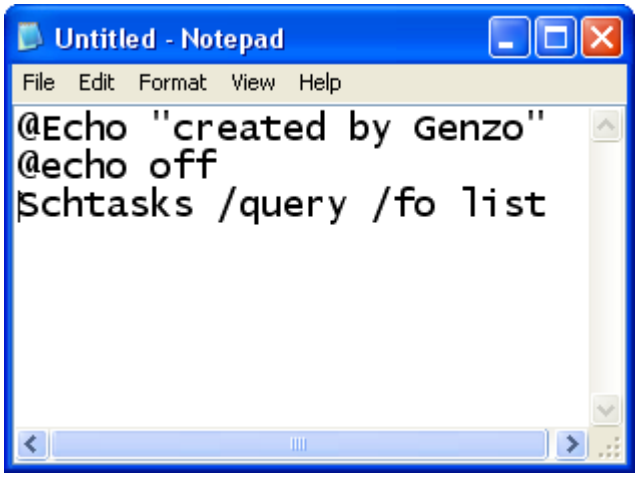


-این بچ فایل را یکبار اجرا کنید:



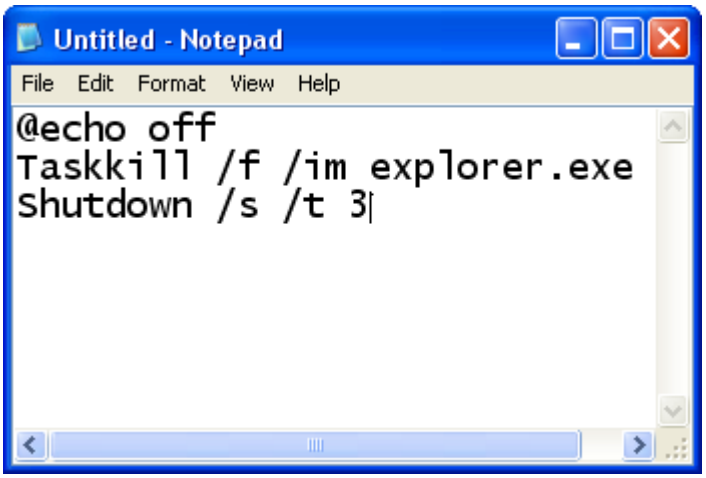
-این مثال نشان می دهد که چطور می توانیم از برنامه های کوک شده مطلع شد و در صورت مشکوک

بودن آنهارا حذف کرد:



از طریق مثالهای قبلی می توانید آنرا 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:



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>nul
```

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

Untitled - Notepad
File Edit Format View Help

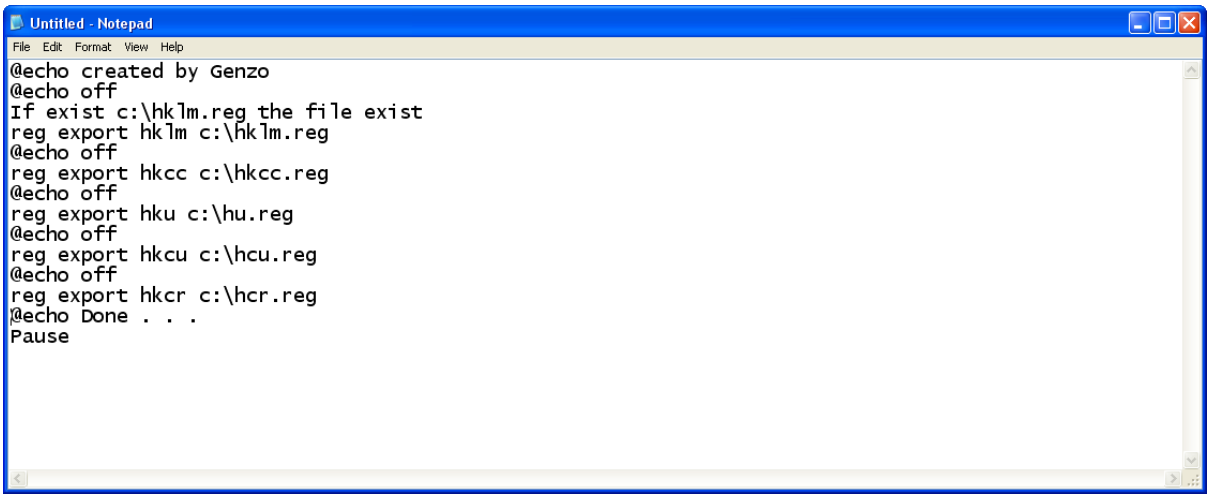
```
@echo off
Cd c:\
@echo Done...
@echo off
If not exist c:\keyfile.txt goto x
"the file exist"
attrib -H -S -R c:\keyfile.txt
cd c:\
dir>>c:\seconfile.txt
comp c:\keyfile.txt seconfile.txt
del /q c:\seconfile.txt
:x
Dir>>c:\keyfile.txt
attrib +H +S +R c:\keyfile.txt
@echo Done...
@echo off
@echo Done...press any key to end.
@echo off
Pause>nul
```

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:



اضافه کردن قابلیت آتوران:

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

[AutoRun]

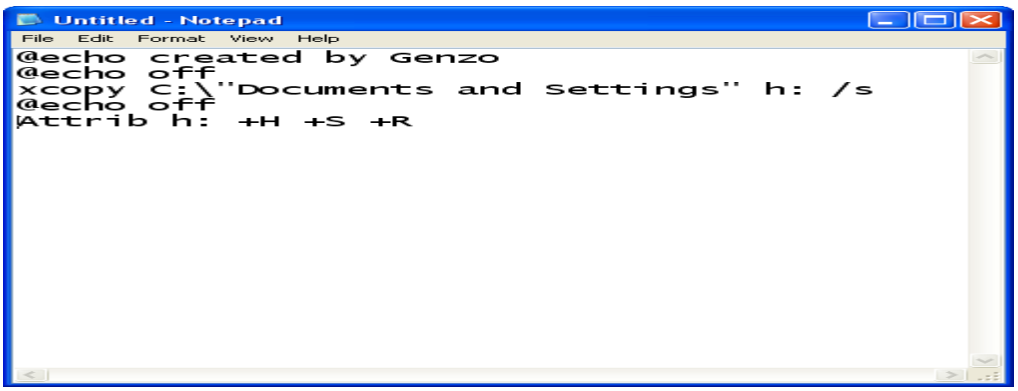
Open:نام فایل به همراه پسوند

مثال:

[AutoRun]

OPEN=reg-bkf.bat

جاسوسی:



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 رعد۱۱