Windows XP Hacks

Part II

ناگفته های پیشرفته ویندوز ایکس پی

(مقاله دوم)

www.worldbook.ir

Windows Explorer

محمد بشیری

تشکر و مقدمه:

سلام بر همه دوستان خوبم

خدا را شاکرم که توفیق داد با قسمت دوم ناگفته های پیشرفته ویندوز xp در خدمت شما باشم. از همه عزیزان که به بنده لطف دارند و همیشه ایمیل میزنند سپاسگزارم. اگه قسمت اول رو نخوندید پیشنهاد می کنم که بخونید، البته این مقاله ربط آنچنانی به مقاله قبلی نداره ولی میتونید از سایت هایی که براتون توی صفحه اول گذاشتم قسمت اول رو بگیرید و بخونید.

از دوست خوبم آقای **رضا یاوری** هم به خاطر زحماتشون در سایت Bashiry.ir تشکر می کنم .

در این مقاله شما با ساختار و زیر و بم Windows Explorer آشنا خواهید شد و چیزهایی یاد می گیرید که تا حالا هیچ جایی ندیدید.

نمیخوام زیاد صحبت کنم بریم سر اصل مطب

هک ۲-۱- در این بخش یاد خواهید گرفت که با راست کلیک ماوس یک منو بسازید که یک سری عملیات رو بنا به خواست شما انجام بده. مثلا لیستی از تمام فایلهای پوشه یا قابلیت ویرایش و چاپ ایجاد کنه و ... .

برای اینکه به راحتی محتوای یک پوشه و یا ساختار آن را داشته باشیم یک منو خواهیم ساخت. برای انجام این کار یک batch فایل خواهیم ساخت. Batch فایل، فایلی هست با پسوند bat که حاوی یک سری دستورات هست.

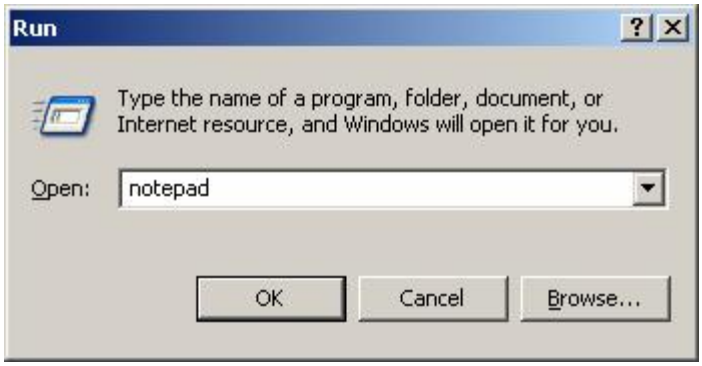
فرمت این batch فایل به صورت زیر هست:

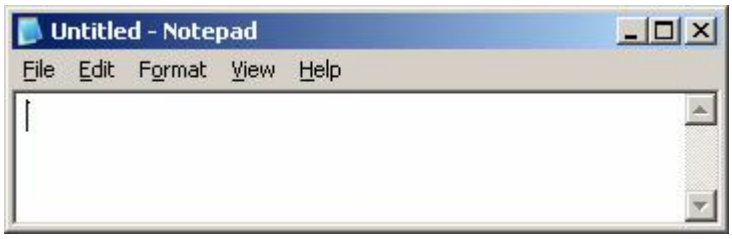
```
Dir /a /-p /o:gen  >filelisting.txt
```

عبارت filelisting.txt دلخواه است و شما هر نامی که دوست دارید میتوانید بنویسید البته با پسوند txt .

در زیر روش ساخت batch فایل رو قدم به قدم برای دوستان تازه کار توضیح خواهم داد:

۱-برنامه notepad رو باز کنید

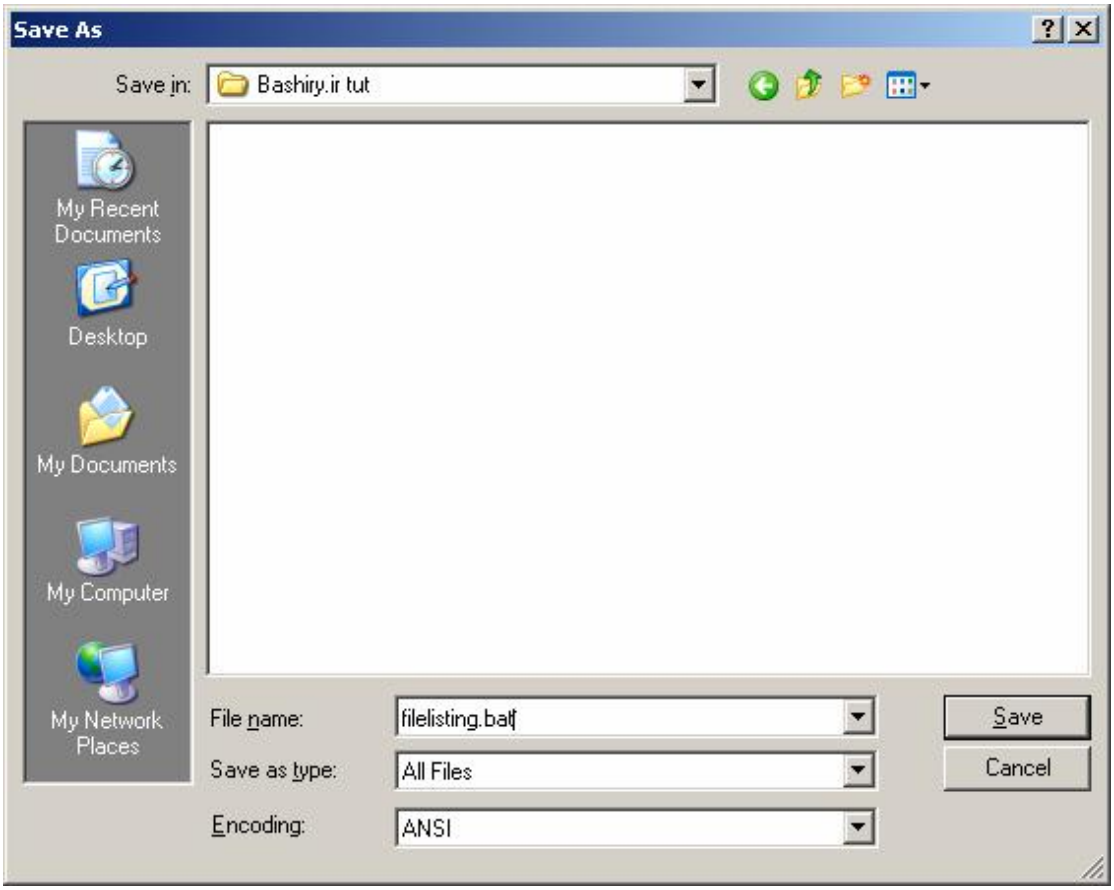




۲-داخل برنامه notepad متن زیر را بنویسید:

۳- حالا نوبت به ذخیره کردن فایل با پسوند bat میرسه. برای این کار از منوی file گزینه save رو انتخاب کنید تا کادر محاوره ای ذخیره سازی مطابق شکل زیر ظاهر شود:

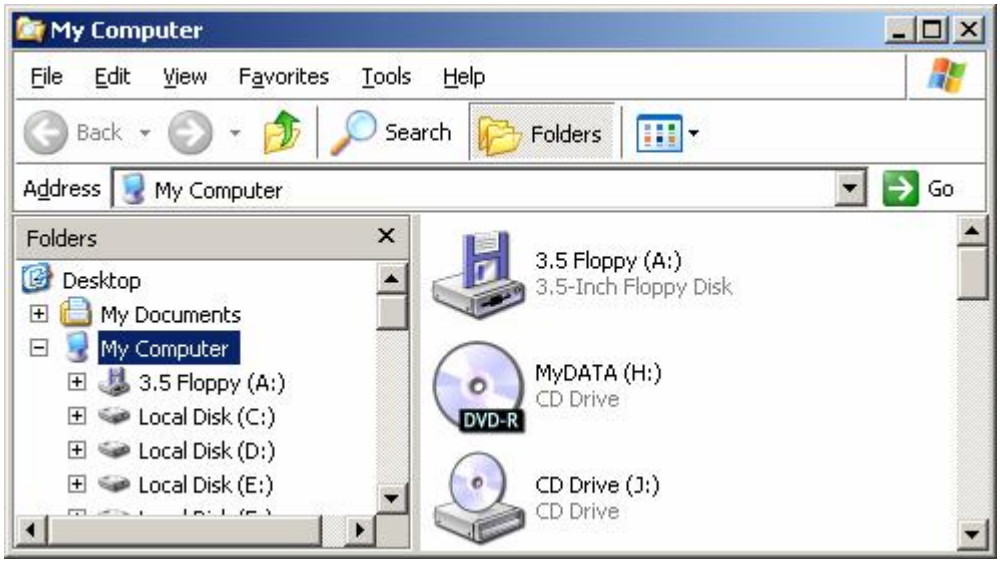
۴- قبل از ذخیره کردن تنظیمات رو مطابق با شکل زیر انجام دهید. توجه کنید پسوند فایل bat باشد و در ضمن بخش save as رو روی all files و همچنین encoding رو روی ANSI قرار بدید.



بعد از انجام تنظیمات مطابق تصویر فایل رو در یک مسیر دلخواه ذخیره کنید.

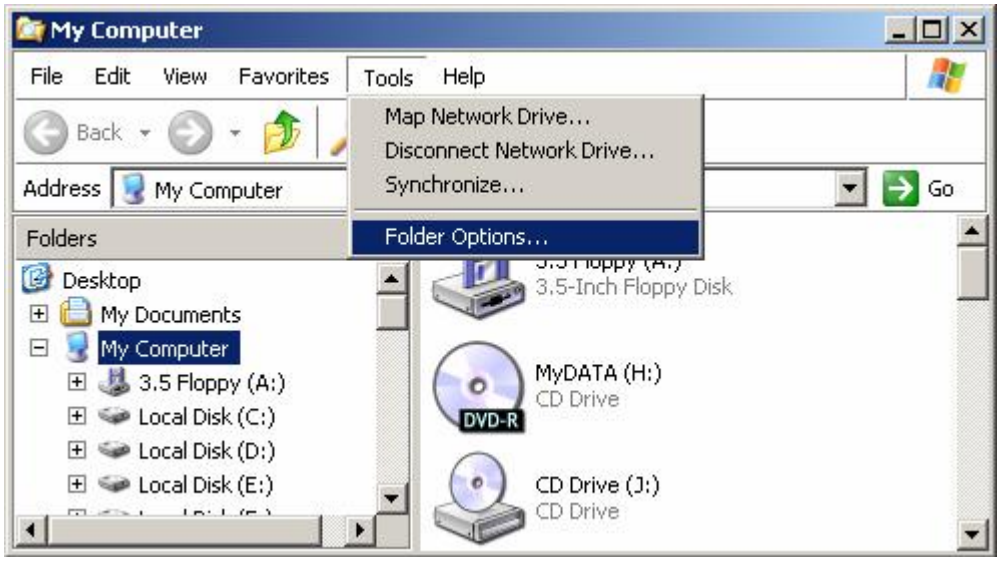
۵- تا الان bat فایل ما ساخته شد. نوبت به ساختن یک action برای منوی راست کلیک ماوس میرسه. برای این کار به صورت زیر عمل نمایید:

الف: window explorer رو باز کنید (یا my computer). برای اجرای ویندوز اکسپلورر می توانید روی دکمه start کلیک راست کنید و بعد explorer رو بزنید یا از کلیدهای ترکیبی ویندوز+ E استفاده کنید.

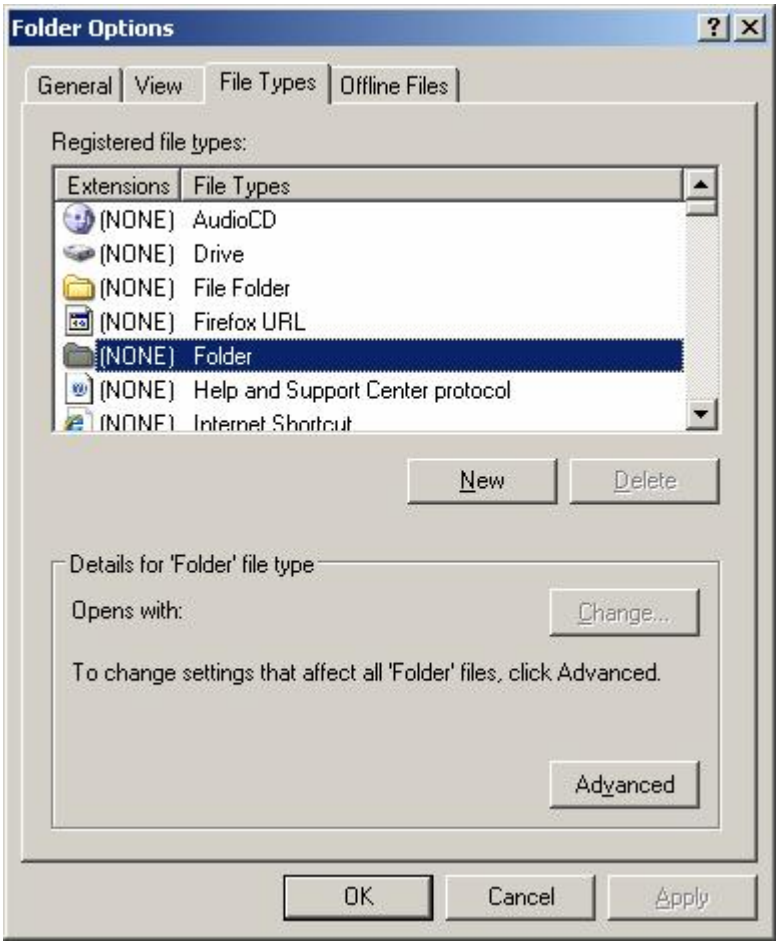


ب: به منوی tools برید

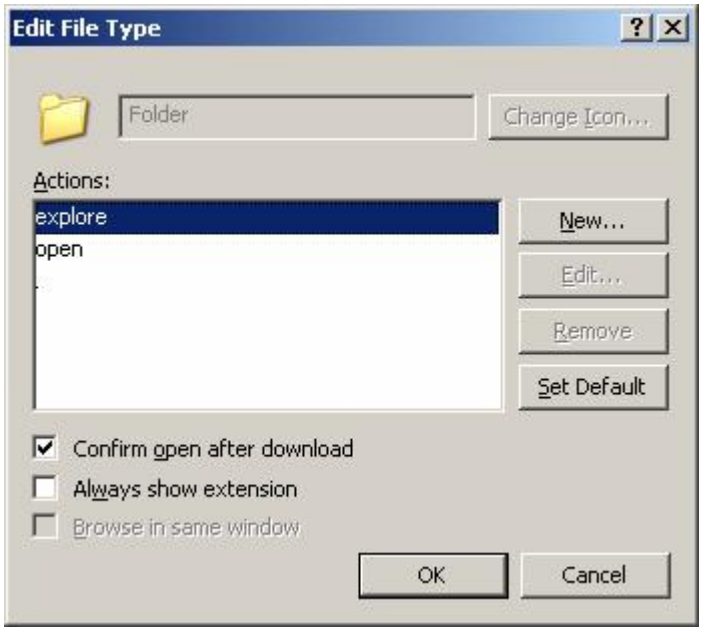
ج: روی folder option کلیک کنید (اگر این گزینه را ندارید احتمال ۹۹ درصد سیستمتون ویروسی هست !!!!)



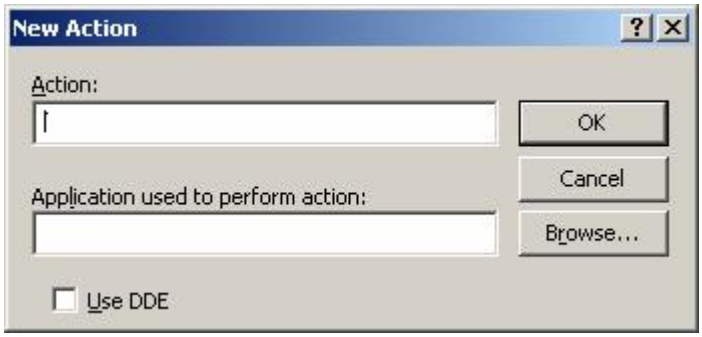
د: به سربرگ یا تب file type برید و بعد از لیست folder رو انتخاب کنید.



ه: روی دکمه advanced کلیک کنید تا پنجره ای همانند شکل زیر ظاهر بشه



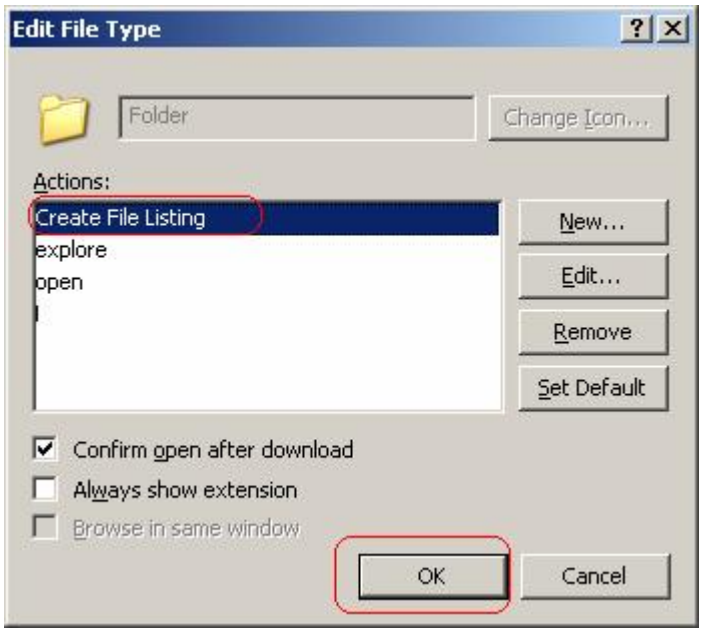
و: روی دکمه new کلیک کنید :



ز: برای ایجاد منوی context فیلدها رو مثل زیر پر کنید و تایید کنید

در بخش action هر متنی رو که میخواهید در منو ظاهر بشه بنویسید. در بخش زیرین هم همون بچ فایلی که ساخته بودیم بهش میدیم و ok می کنیم.

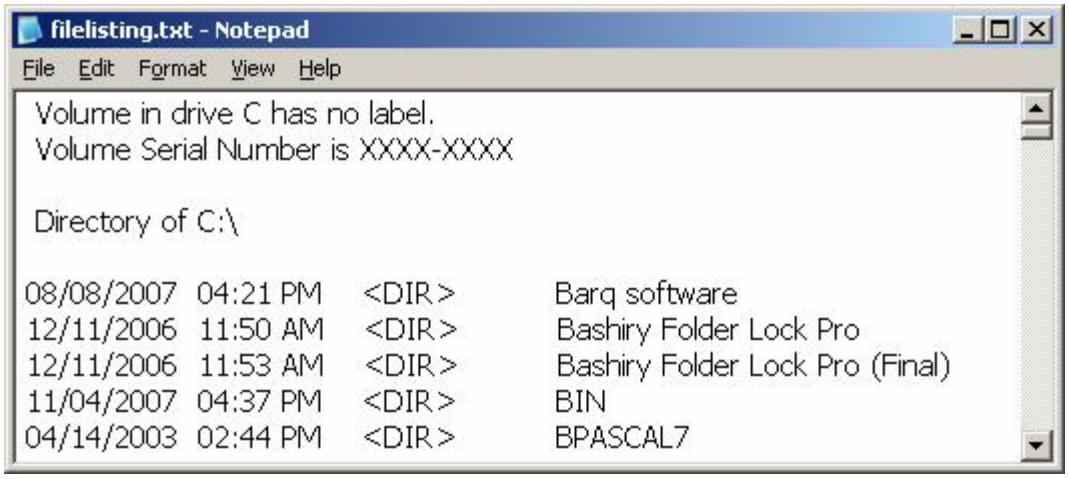
بعد از ok مشاهده می کنید که action ما به لیست اضافه شده (شکل زیر)



خوب Ok می کنیم تا این پنجره هم بسته بشه.

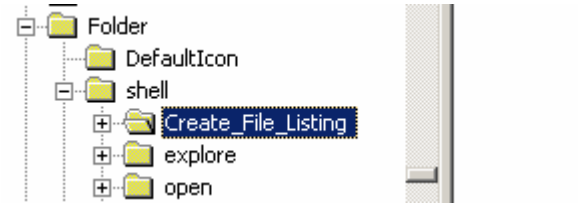
خیلی عالی. کار به همین سادگی تمام شد. کافیه با پوشه ای که می خواهید لیست فایلهاش رو بگیرید مراجعه کنید و بعد راست کلیک روی اون پوشه و ....

دیدید چه جالب یه بخشی به راست کلیک ماوس اضافه کردیم که کارهایی که دلمون میخواد برامون انجام میده. بعد از اینکه من کلیک کردم یه فایل ساخته میشه به اسم filelisting.txt که محتوای این فایل تمام محتویات اون مسیر هست . و آماده برای ویرایش و چاپ هست. (شکل زیر)



نکته: اگر بنا به هر دلیلی خواستید این گزینه اضافه شده به منوی سمت راست رو حذف کنید باید به رجیستری و مسیر زیر برید سپس کلید Create_File_listing رو از قاب سمت چپ حذف کنید و سپس رجیستری رو ببندید و سیستم رو reboot کنید.

```
HKEY_CLASSES_ROOT\Folder\shell\Create_File_Listing
```



روش دوم برای کاربران outlook XP:

اگر از outlook xp استفاده کنید روش دومی هم بدون نیاز به ویرایش سیستم هست که لیست دایرکتوری ها رو می گیره. با استفاده از outlook bar تنها با یک کلیک قادر به انجام این کار خواهید بود. مرحل انجام کار به صورت زیر هست

۱- برنامه outlook رو باز کنید

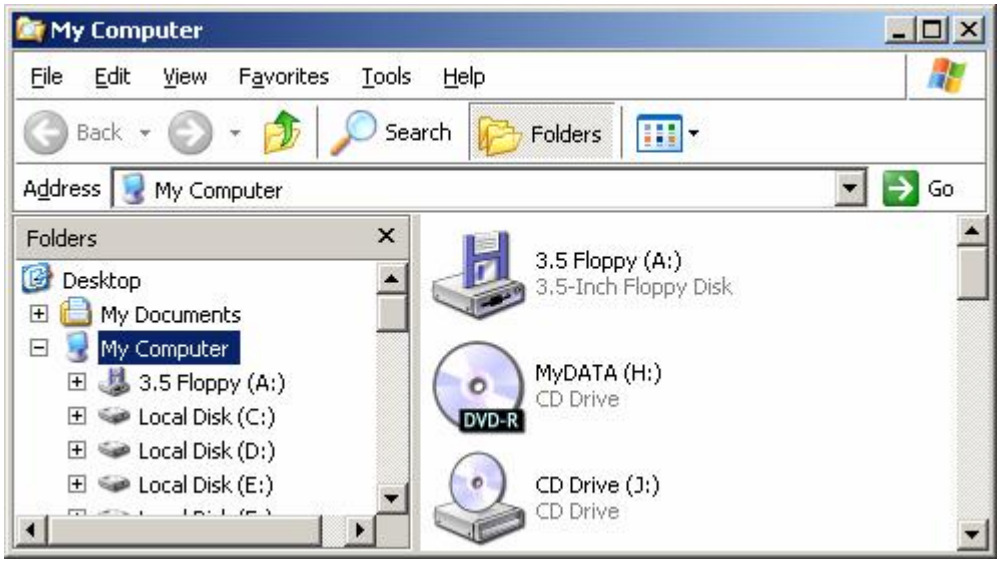
۲- View را انتخاب و سپس Outlook bar و بعد از آن Other shortcts

۳- به مسیری که می خواهید برید و بعد روی outlook bar دکمه print رو فشار بدید و تمام.

هک ۲-۲ – کنترل کردن windows explorer با دستورات میانبر خط فرمان

در این آموزش یاد خواهید گرفت که چگونه explorer رو با خط فرمان سفارشی کنید و هر نمایش رو به صورت جداگانه و به صورت میانبر در میز کار خودتون ذخیره کنید.

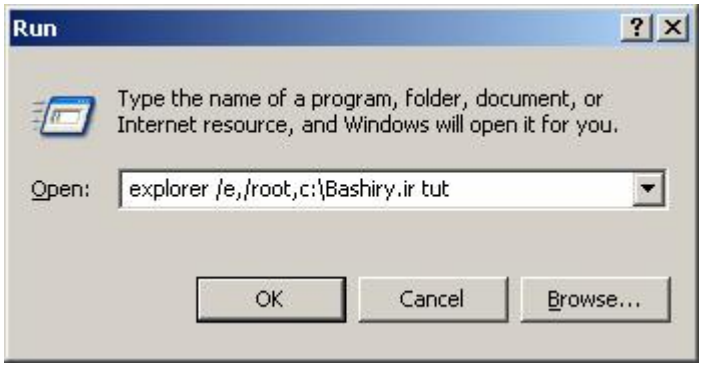
windows explorer به صورت پیش فرض باز می شود:



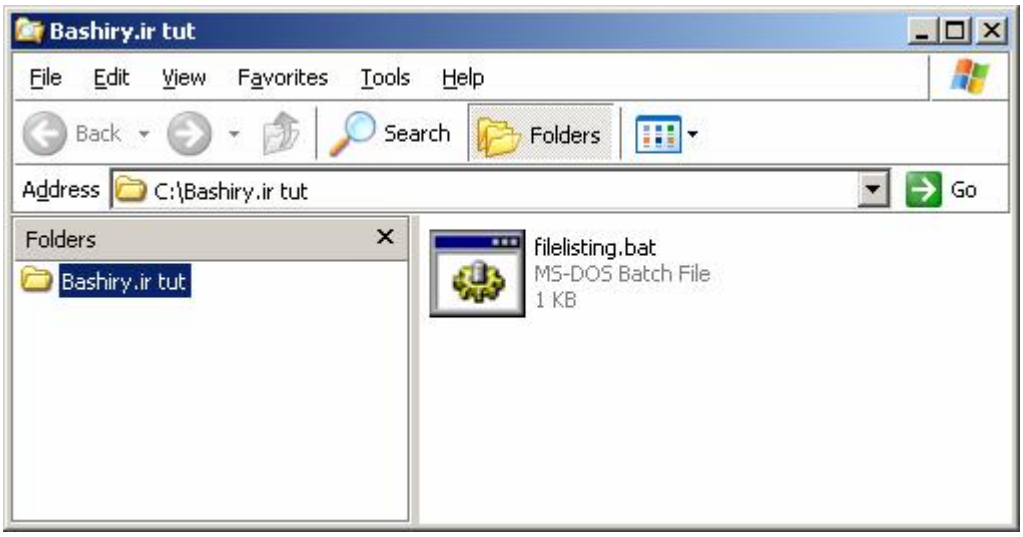
در عوض می خواهم که با یک سری دستورات اون رو سفارشی کنم که مثلا بخش نمایش folder در سمت چپ رو خاموش و یا روشن کنم. این کار با دادن یک سری پارامتر در خط فرمان قابل انجام است.

فرض کنید میخواهیم windows explorer رو فقط در زیر پوشه c:\ Bashiry.ir tut باز کنم بدون دیدن هیچ پوشه دیگری و همچنین به folder bar هم نیاز دارم. برای این کار خط فرمان را باز می کنیم و دستورات زیر رو همینطور که هست وارد می کنیم. (شکل زیر)

```
explorer /e,/root,c:\Bashiry.ir tut
```



و خروجی کار خیلی جالب و جذاب هست:



در مقایسه این خروجی با خروجی معمول می بینید که در سمت چپ دیگر درایو ها و پوشه ها ظاهر نشده و فقط همان پوشه ای که می خواستیم با زیر پوشه هایش نشان داده شده است.

این فقط یکی از دستورات windows explorer بود که با هم دیدیم.

در کل ساختار خط فرمان به صورت زیر هست:

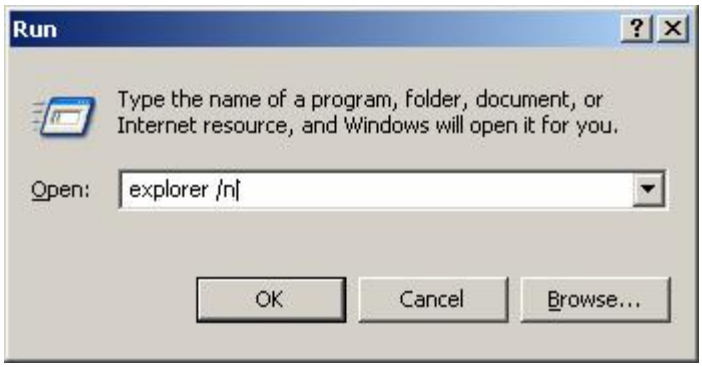
```
Explorer [/n] [/e] [,root,object] [[,/select],subobject]
```

در صورتی که تنها از explorer استفاده کنید نمایش به صورت پیش فرض هست .

حال به توضیح پارامتر ها می پردازم:

پارامتر n/

پنجره explorer رو بدون نشان دادن folder bar باز می کنه. (شکل زیر)

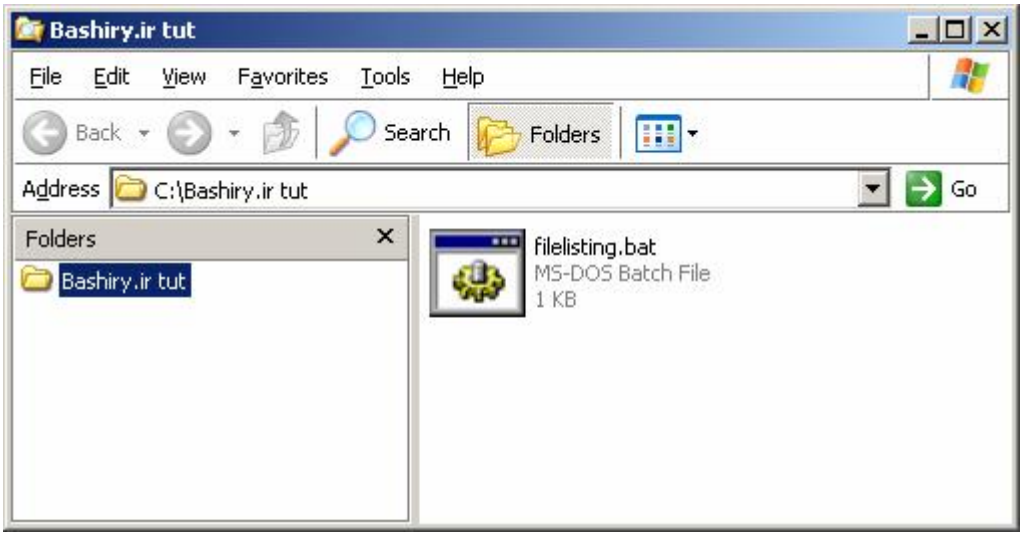


پارامتر e/

پنجره explorer رو همراه با folder bar باز می کنه:

پارامتر root,object/

پنجره explorer رو با یک شی خاص مثل پوشه بدون نشان دادن پوشه های بالای آن باز می کنه. مثل همین تصویر زیر که قبلا دیدید.



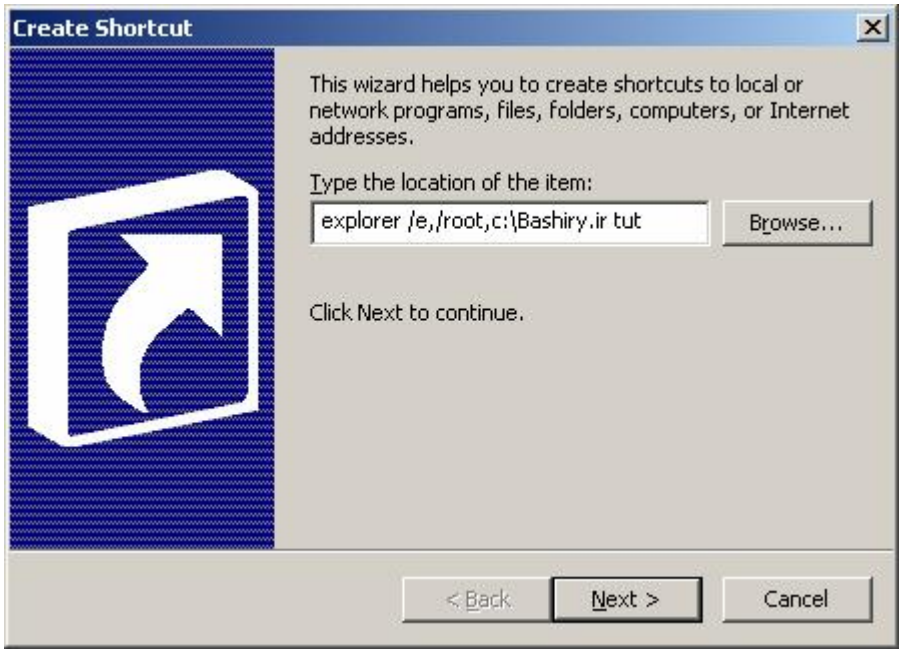
پارامتر [[,/select],subobject]

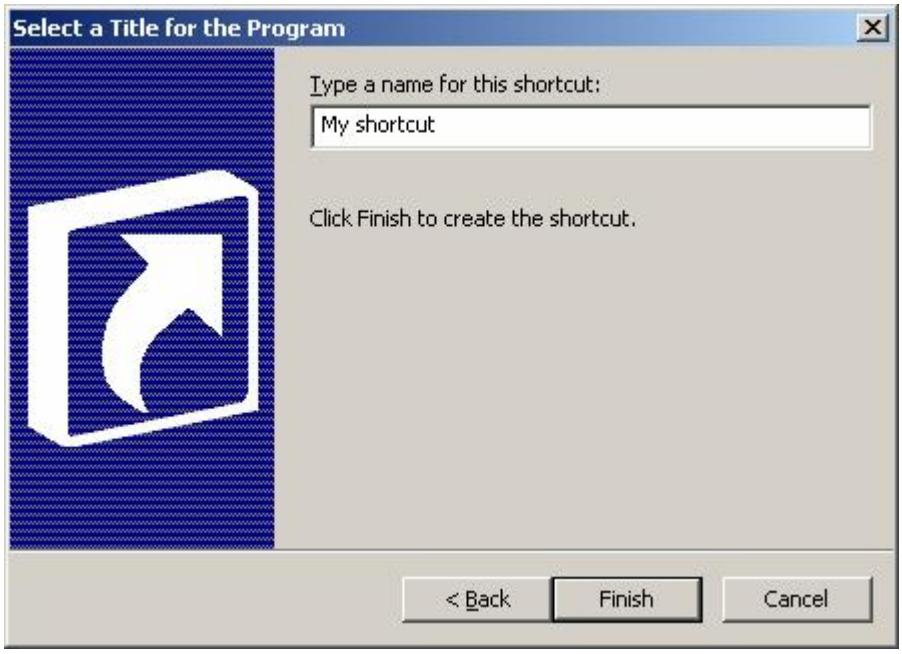
پنجره explorer را به یک فایل یا یک پوشه خاص که انتخاب یا expand شده اند، باز می کند. همچنین می توانید از فرمان subobject بدون استفاده از select استفاده کنید. زمانی که فرمان شامل select/ هست شاخه هایی که expand (باز) نشده اند، پوشه highlight شده و همچنین subobject در پنجره سمت راست highlight می شود.

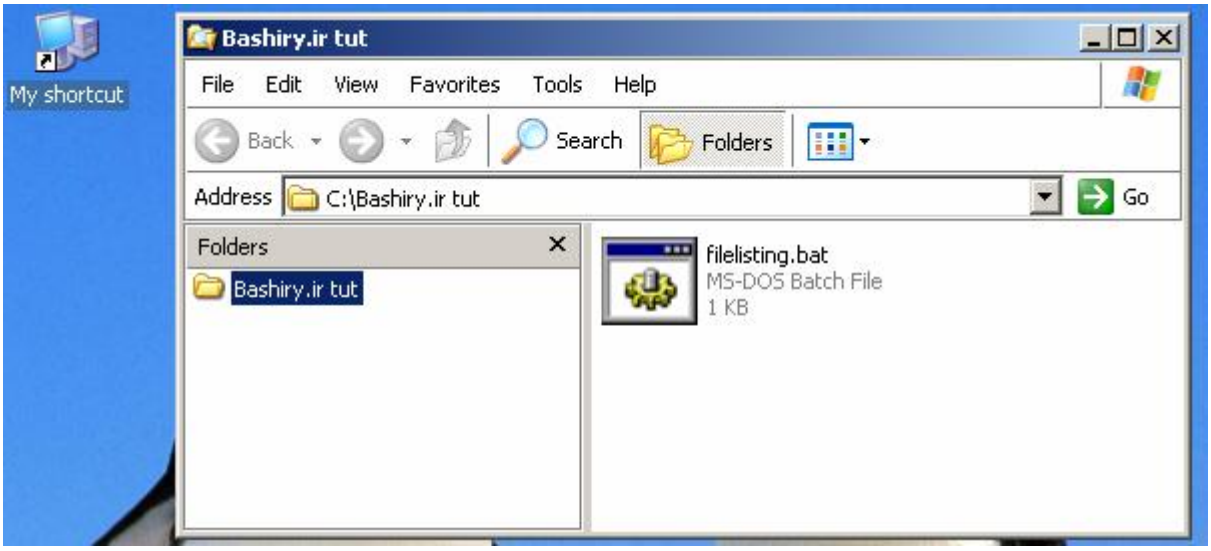
۲-۲-۱- ایجاد میانبر یا شورتکات برای explorer

برای ایجاد شورتکات یا میانبر به این صورت عمل کنید که روی میز کار راست کلیک کنید وبعد new و سپس Shortcut .

در پنجره ظاهر شده دستورات خط فرمان خودتون رو بنویسید بعد نام مناسب برای آن در نظر بگیرید و بعد تایید کنید تا میانبر ساخته بشه..


Create Shortcut
This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.
Type the location of the item:
explorer /e,/root,c:\Bashiry.ir tut
Browse...
Click Next to continue.
< Back
Next >
Cancel


Select a Title for the Program
Type a name for this shortcut:
My shortcut
Click Finish to create the shortcut.
< Back
Finish
Cancel

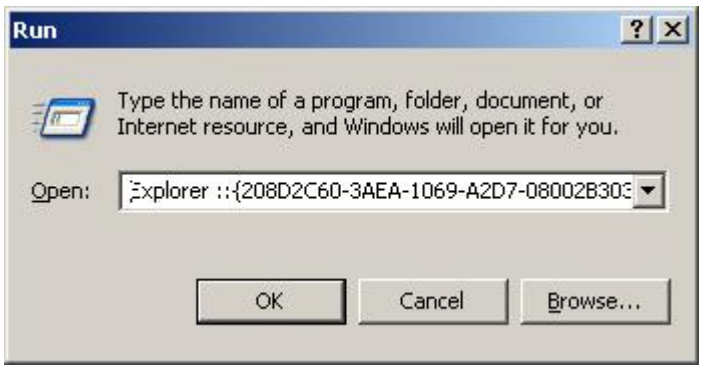


در تصویر بالا میانبر ساخته شده و بعد از کلیک عملیات مورد نظر انجام خواهد شد.

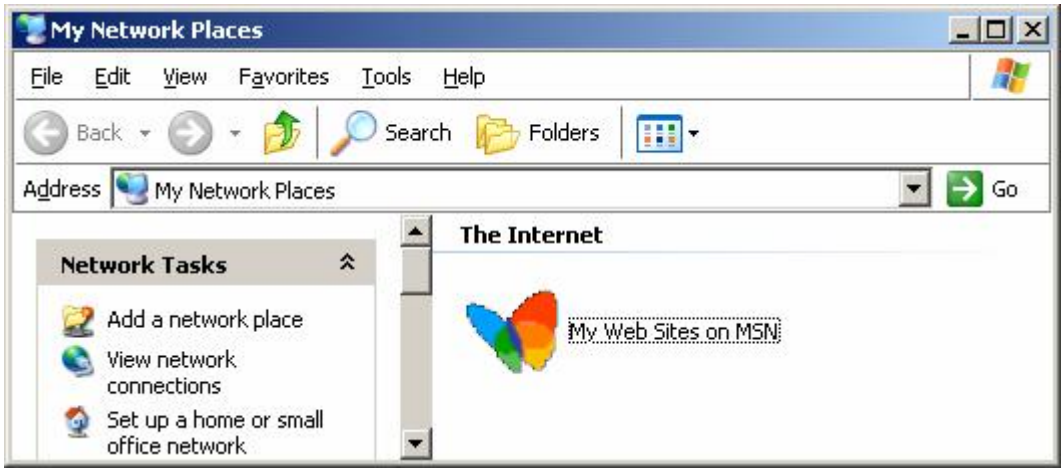
۲-۲-۲- استفاده از Global Unique identifier یا (GUIDs) با سوئیچ های خط فرمان

بعضی وقتها می خواهید فولدرهای خاص مثل my network place و یا my computer و از این قبیل موارد رو باز کنید . پس باید از روش GUIDs استفاده کنید بدین ترتیب که ابتدا کلمه explorer رو مینویسید و بعدش دو علامت کالن پشت سر هم و سپس شناسه سراسری واحد مورد نظر و یا همان به اصطلاح لاتین Global Unique identifier

```
Explorer ::{208D2C60-3AEA-1069-A2D7-08002B30309D}
```



حاصل خروجی فرمان فوق به صورت زیر است:



جالبه نه؟!!!!

اگر هم بخواهید از پارامترها استفاده کنید بعد از پارامتر یک فاصله میزارید و بعد همون علامت دو نقطه و در ادامه شناسه یکتا رو می نویسید.

Explorer /e, ::{208D2C60-3AEA-1069-A2D7-08002B30309D}

شناسه های مختلف رو که هر کدام عملیاتی رو انجام میدن رو در زیر نوشتم. مثل حالت قبل برای هر کدام میتونید میانبر بسازید و استفاده کنید.

فرمان اجرا شده	شناسه عمومی واحد برای هر دستور
My Computer	{20D04FE0-3AEA-1069-A2D8-08002B30309d}
My network place	{208D2C60-3AEA-1069-A2D7-08002B30309D}
Network Connections	{7007ACC7-3202-11D1-AAD2-00805FC1270E}
Printer and Faxes	{2227A280-3AEA-1069-A2DE-08002B30309D}
Recycle bin	{645FF040-5081-101B-9F08-00AA002F954E}
Scheduled Tasks	{D6277990-4C6A-11CF-8D87-00AA0060F5BF}

هک ۲-۳- جستجوی فایلها با استفاده از سرویس پرس و جوی شاخص گذاری پیشرفته یا به عبارت بهتر

Mastering the Indexing Service's Query Language

فکر کنید که کلی فایل روی هارد خودتون دارید که مربوط به سالیان سال هست و میخواهید با سرعت به اونها دسترسی داشته باشید. بهترین راه استفاده از سرویس پرس و جوی پیشرفته شاخص گذاری هست.

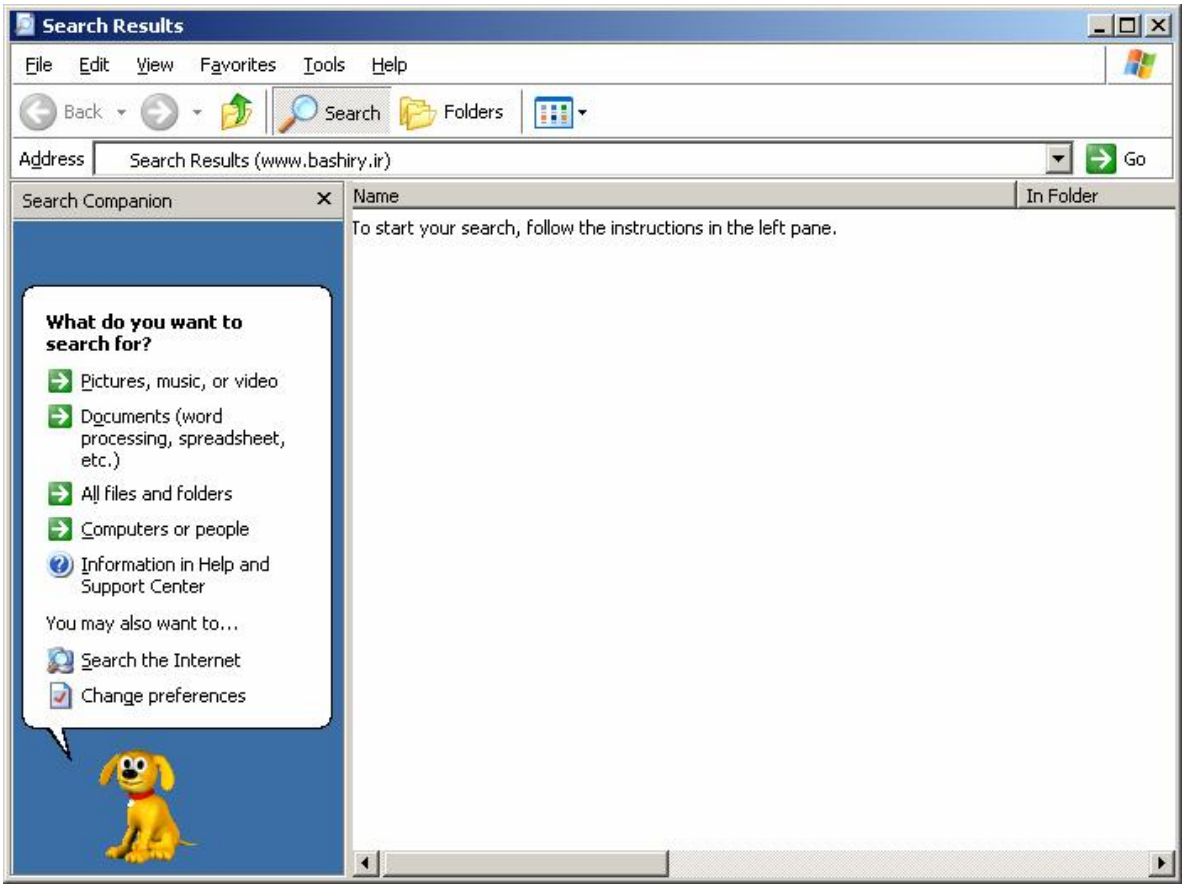
در ویندوز های ایکس پی جستجو ها کند هست و گاهی اوقات جستجویی که خروجی را محدود می کند و سریعتر است. ولی این نوع جستجو قابلیت جستجو بر اساس خصوصیات فایل مثل آخرین فایل چاپ شده و یا لغتی در یک فایل و یا استفاده از یک زبان جستجوی پیشرفته را ندارد.

سرویس شاخص گذاری یا Indexing service در ابتدا توسط Internet information Services یا IIS استفاده می شد. این ابزار کمی ناشناخته و در عین حال قدرتمند هست. میتوان جستجو های پیچیده و سخت را در مدت زمان خیلی کم و با سرعت انجام داد. روش کار به این صورت است که از یک بخش زبان پرس و جو یا Query تشکیل شده است. در اصل فایل های کامپیوتر همگی ایندکس می شوند و وقتی شما جستجو می کنید در اصل روی همه هارد جستجو خواهید کرد.

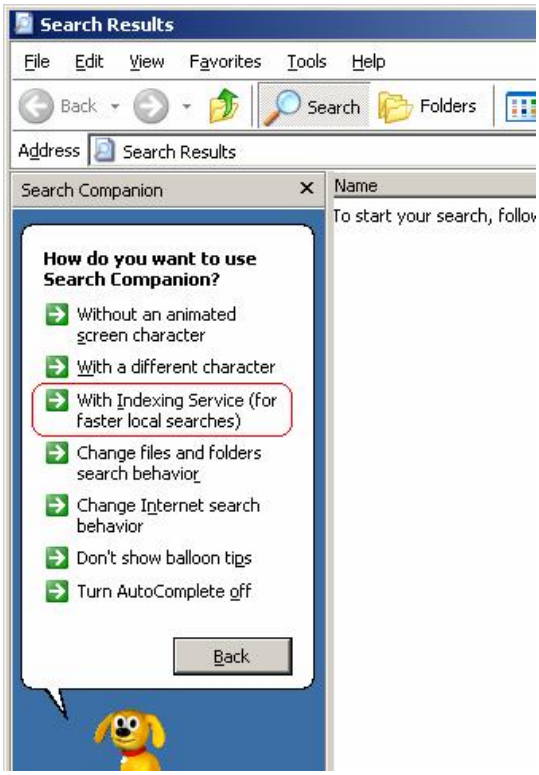
خوب دیگه حاشیه بسته. بریم سر اصل مطلب که میدونم همه شما منتظرید ببینید اصلا این چیزی که میگم چیه !!!

به طور معمول این سرویس خاموش هست برای فعال کردنش باید ابتدا search رو باز کنید:

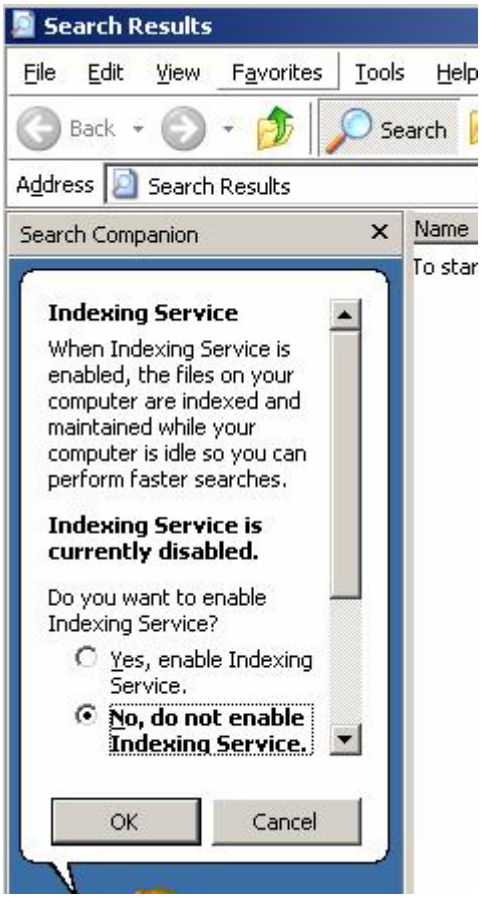
Start →Search[→ For Files or Folders].



از اینجا گزینه Change preferences رو بزنید:



اگر در این بخش گزینه with Indexing Service رو ندیدید بدین مفهوم هست که قبلا این سرویس روی سیستم شما فعال شده. به محض کلیک بر روی این سرویس پنجره ای دیگر ظاهر می شه که شما باید از اون پنجره سرویس رو فعال کنید و تایید کنید (شکل زیر)



بعد از فعال کردن این گزینه بسته به قدرت پردازنده شما و همچنین فایلهایی که روی هارد دارید شاخص گذاری فایلها طول میکشه. صبر کنید و برید چند تا چایی بخورید تا مراحل شاخص گذاری کامل بشه.

برای غیر فعال کردن این سرویس هم مثل قبل جستجو رو باز کنید بعد change preferences رو بزنید و بعدش without indexing رو کلیک کنید. توجه کنید با غیر فعال کردنش به حالت جستجو معمولی میریم و فایلهای شاخص گذاری شده همونطور باقی می مانند. به این ترتیب هر وقت خواستید اون رو فعال کنید و هر وقت هم دوست داشتید غیر فعالش کنید.

۲-۳-۱- استفاده از سرویس زبان پرس و جوی شاخص گذاری

استفاده از این سرویس به شما اجازه جستجو در properties فایل رو می دهد، از قبیل مولف سند ، یا تعداد بایت های سند و همچنین استفاده از عملگر ها دو دویی یا boolean و غیره.

برای جستجوی یک عبارت مثلا: "bashiry.ir is Computer library " پرس و جو به صورت زیر می تواند باشد:

```
{phrase} bashiry.ir is Computer library  {/phrase}
```

دو روش برای جستجوی متن در روش پرس و جو وجود دارد یکی استفاده از phrase و دومی هم استفاده از freetext هست. عبارت phrase دنبال لغت به همان صورت و به همان ترتیب می گردد. مثلا

```
{phrase} old dog barks backwards {/phrase}
```

دقیقا به دنبال فایلهایی می گردد که شامل دقیقا همان عبارت باشد.

استفاده از freetext مثل قبلی نیست و در اصل اینطور فکر کنید که بین هر لغت یک or وجود دارد. کافیه که فایل مورد نظر دارای یکی از آن کلمات باشد، پس به عنوان مورد پیدا شده برگردانده می شود.

```
{freetext} old dog barks backwards {/freetext}
```

قطعا نتیجه حاصل شده بیشتر از حالت قبلی هست که از phrase استفاده کردیم.

۲-۳-۲-جستجو در properties ها یا خصوصیات

ساختار دستور به صورت زیر هست:

```
{prop name=property name} query {/prop}
```

که property name ، نام property هست که به طور کامل مقدار این پارامتر در جدول شماره ۲-۳-۱ آورده شده است.

Query هم متنی هست که می خواهید جستجو کنید. برای مثال جستجوی سندی که آخرین باز توسط mohamad bashiry ویرایش شده به صورت زیر هست:

```
{prop name=DocLastAuthor} Mohamad Bashiry {/prop}
```

همچنین پرس و جو می تواند شامل کلمات ویژه * و ؟ هم باشد. برای استفاده از عبارات منظم باید از تگ {regex} که مخفف همان regular expression (عبارت منظم) استفاده نمود.

```
{prop name=filename} {regex} *.xl? {/regex} {/prop}
```

شاخص کردن در این سرویس فقط روی متن هر سند انجام نمیشود بلکه شامل همه اطلاعات ضروری در هر فایل هست. (برای دیدن summary هر متن روی آن فایل راست کلیک کنید و بعد به بخش properties برید و بعد تب summary)

برای جستجو در خصوصیات این اطلاعات (summary) می توانید از جدول ۲-۳-۱ استفاده کنید. این جدول شامل لیست مهمترین خواص هست که می توانید در جستجو از آنها استفاده کنید.

جدول شماره ۲-۳-۱ – مهمترین خصوصیات برای جستجو از طریق سرویس شاخص گذاری

خصوصیت	توضیح
Access	آخرین باری که سند دسترسی داشته
All	همه خصوصیات در دسترس. با پرس و جوی متنی کار می کند نه عددی.
AllocSize	آخرین فضای دیسک که به سند اختصاص یافته شده است.
Contents	محتوای سند
Created	زمان آخرین سند ایجاد شده
Directory	مسیر کامل، جایی که سند در آنجا قرار گرفته
DocAppName	نام برنامه ای که سند توسط آن ایجاد شده
DocAuthor	مولف سند
DocByteCount	تعداد بایتهای داخل سند
DocCategory	نوع سند
DocCharCount	تعداد کاراکترهای داخل سند
DocComments	توضیحات مربوط به سند
DocCompany	نام شرکتی که سند را نوشته

DocCreatedTime	زمان ایجاد سند
DocHiddenCount	تعداد اسلاید های مخفی درون اسناد برنامه پاور پوینت
DocKeyWords	کلید واژه درون سند
DocLastAuthor	نام آخرین شخصی که سند را ویرایش کرده
DocLastPrinted	آخرین زمانی که سند چاپ شده
DocLineCount	تعداد خطوط محتوای سند
DocLastSavedTm	آخرین زمانی که سند ذخیره شده
DocManager	نام مدیر مولف سند
DocNoteCount	تعداد صفحات شامل note در اسناد پاورپوینت
DocPageCount	تعداد صفحات سند
DocParaCount	تعداد پاراگراف های سند
DocPartTitles	نام بخشی از سند مثل نام صفحات گسترده در اکسل یا نام اسلایدها در پاور پوینت
DocRevNumber	آخرین شماره نسخه سند
DocSlideCount	تعداد اسلایدها در سند پاور پوینت
DocTemplate	نام قالب سند
DocTitle	عنوان سند
DocWordCount	تعداد لغات سند
FileName	اسم فایل سند
Path	مسیر سند ، شامل اسم فایل سند
ShortFileName	نام فرمت ۸,۳-سند
Size	اندازه سند مورد نظر به بایت
Write	تاریخ و زمانی که سند ویرایش شده

۲-۳-۳- جستجو با استفاده از عملگرها و عبارت

زبان پرس و جو شامل طیف وسیعی از عملگرها و عبارات برای جستجوی متنی یا عددی هست.

عملگرهای EQUALS و CONTAINS

هنگامی که یک پرس و جو با استفاده از متن ایجاد می کنید استفاده از عملگر EQUALS یا مساوی دقیقا به همون صورتی که عبارت جستجو رو نوشتیم جستجو می کنه.

```
{prop name=DocTitle} EQUALS First Draft of Final Novel {/prop}
```

این جستجو تمام عباراتی را جستجو می کند که در عنوانشان عبارت First Draft of Final Novel وجود داشته باشه.

این عملگر مثل phrase که قبلا گفته شد عمل می کنه.

در ضمن استفاده از CONTAINS هم مثل freetext عمل می کنه که قبلا تشریح شد.

عملگرهای رابطه ای:

- عملگر مساوی یا =
- عملگر مخالف یا = !
- عملگر کوچکتر یا <
- عملگر کوچکتر مساوی =<
- عملگر بزرگتر >
- عملگر بزرگتر مساوی =>

عبارت زمان و تاریخ:

از فرمت زیر برای جستجوی تاریخ و زمان می توانید استفاده کنید:

```
yyyy/mm/dd hh:mm:ss
yyyy-mmmm-dd hh:mm:ss
```

از این عبارات می تواند به صورت ترکیبی با عملگرهای رابطه ای نیز استفاده کنید:

```
{prop name=Created} >-2d {/prop}
```

جستجوی بالا دنبال فایلهایی می گردد در در عرض دو روز گذشته ایجاد شده اند.

از جدول ۲-۳-۲ برای دیدن اختصارهای تاریخ و زمان استفاده کنید:

جدول ۲-۳-۲ – کلمات اختصاری تاریخ و زمان

Abbreviation	Meaning	Abbreviation	Meaning
Y	Year	D	Day
Q	Quarter	H	Hour
M	Month	N	Minute
W	Week	S	Second

عملگرهای دودویی یا boolean:

جزئیات عملگرهای دو دویی را در جدول زیر میتوانید مشاهده کنید:

جدول ۲-۳-۳- عملگرهای دودویی

Boolean Operator	Long Form	Short Form
AND	&	AND
OR	|	OR
Unary NOT	!	NOT
Binary NOT	&!	AND NOT

عملگر not رو میشه به صورت زیر به کار برد:

```
{prop name=DocSlideCount} NOT = 7 {/prop}
```

این جستجو تمام اسناد پاورپوینتی رو پیدا می کنه ۷ اسلاید ندارند.

نمونه دیگری در استفاده از not به صورت زیر است:

```
{prop name=DocAuthor} Preston Gralla {/prop} NOT
{prop name=DocTitle} Chapter 10 {/prop}
```

جستجوی بالا همه اسنادی رو پیدا می کنه که مولف آن سند Preston Gralla هست و در عنوان سند عبارت chapter 10 وجود نداره.

استفاده از دو علامت ستاره پشت سر هم باعث می شود که حالت های ثانویه فعلا مورد نظر نیز مورد قبول باشد مثلا:

```
{prop name=Contents} run** {/prop}
```

همه اسنادی رو پیدا خواهد کرد که شامل لغت 'ran' یا لغت 'run' باشد.

۲-۳-۴- ترتیب نتایج جستجو

گاهی اوقات نتایج جستجو زیاد هست و شما می خواهید با ترتیب خاصی نتایج به شما نشان داده شود. با استفاده از تگ weight می توانید این کار را انجام دهید. توجه داشته باشد تگ weight تگ خاتمه {/weight} را ندارد.

```
{weight value = n} query
```

رنج پارامتر بین 0.000 و 1.000 هست.

اگر شما دنبال سه عبارت "fire" ، "ice" و "slush" بگردید و قصد داشته باشید که وزن "Fire" بیشتر باشد و "ice" دومین وزن و در انتها "slush" در رده سوم قرار بگیرد از عبارت جستجوی زیر در یک خط میتوانید استفاده کنید:

```
{weight value=1.000}fire AND {weight value=.500}ice AND {weight value=.250}slush
```

۲-۳-۵- فیلتر کردن لغاتی برای جستجو

آخرین مبحثی که از این بخش باقی مانده این است که قادرید یک سری لغات رو تعیین کنید که اصلا جستجو نشوند. در اصل یک حالت فیلتر برای کلمات در نظر می گیریم.

یک فایل به اسم noise.eng در ریشه درایو ویندوز و پوشه system32 هست که شامل لیست لغات فیلتر شده است.

توجه کنید پسوند eng. مربوط به انگلیسی هست. Noise.deu آلمان، noise.fra فرانسه و ... است. برای اضافه کردن لغتی که می خواهید در جستجو از آن صرفنظر شود میتوانید با notepad آنرا ویرایش کنید و لغات خود را به آن اضافه کنید.

برای اینکه ببینید ساختار فایل چطور هست من بخشی از فایل noise.eng رو در زیر براتون آوردم :

about
1
after
2
all
also
3
an
4
and
5
another
6
any
7
are
8
as
9
at
0
be
$
because
been
before
being
Between
.
.
.

محتوای این فایل حروف اضافه، ضمیرها، شکل های گوناگون فعل ها، واژه ها و ... است. در اصل این فایلها یک نوع قانون را

برای این روش جستجو مشخص می کنند. با ویرایش این فایل جستجو بر اساس قوانین جدید دنبال می شود.

هک ۲-۴- مخفی کردن فایلها و پوشه ها با استفاده از سیستم رمز گذاری فایل

Hiding Folders and Files with the EncryptingFile System

اگر از ویندوز xp نسخه pro استفاده می کنید برای اینکه فایلهایتان را از چشم های دیگران مخفی کنید می توانید از سیستم رمز نگاری فایل یا EFS استفاده کنید. این امکان برای ویندوز xp نسخه home غیر قابل دسترس است.

EFS فایلها یا پوشه های انتخابی شما را انکریپت یا به اصطلاح رمز نگاری می کند. اگر پوشه را انکریپت کنید تمام فایلهای داخل آن نیز encrypt می شوند. فایلها و پوشه های انکریپت شده در explorer به رنگ سبز نمایش داده می شوند. فایلها یا پوشه ها بعد از اینکه انکریپت شدند مثل بقیه فایلها هستند و به همان راحتی می توان به آنها دسترسی داشت، آنها را باز کرد و ... .

هر کاربر در ویندوز ایکس پی فقط می تواند فایلهای انکریپت شده خودش را ببیند و به آنها دسترسی داشته باشد. فرض کنید یک کاربر در ویندوز به اسم mohamad فایلی رو انکریپت کرده. حالا یوزر mahdi وارد حساب کاربری خودش می شود دیگر کاربر mahdi فایلهای انکریپت شده توسط mohamad را نمی بیند. مگر اینکه این کاربر حق دسترسی به فایل مربوطه را داشته باشد. (پسورد mohamad را کش رفته باشد !!!!)

هر فایلی که انکریپت می شود یک عدد تصادفی که به نام FEK یا کلید رمز نگاری فایل توسط EFS به آن اختصاص می یابد. EFS از FEK برای انکریپت کردن محتوای فایل همراه با اطلاعات گوناگون الگوریتم رمز نگاری استاندارد (DES[1]) که DESX نامیده می شود استفاده می کند. (DESX قدرت بیشتری در انکریپت کردن نسبت به DES دارد). FEK با استفاده از کلید عمومی RSA به خوبی رمزگذاری شده است.

EFS یکسری محدودیت های جزئی دارد که شما باید از آن آگاه باشید:

[1] Data Encryption Standard

- EFS فقط در فت[۲] ، ntfs کار می کند. اگر از fat یا fat32 استفاده می کنید باید اول آن را به ntfs تبدیل کنید.
- EFS روی فایلهای فشرده کار نمی کند.پس ابتدا فایلها را از حالت فشرده خارج کنید بعد انکریپت کنید.

همچنین اگر فایل انکریپت شده را بخواهید فشرده کنید ابتدا باید آنرا دکریپت (برعکس انکریپت) کنید. یعنی آنرا از حالت فشرده خارج کنید.

- EFS قابلیت فشرده کردن فایلهای سیستمی C:\windows را ندارد.

اگر با فایلها یا پوشه های انکریپت شده استفاده می کنید فکر می کنید که دقیقا همانند فایلها یا پوشه های معمولی هستند ولی در واقع اینطور نیست و کمی از لحاظ رفتاری فرق دارد.

رفتارها در زیر آورده شده است:

- حرکت یا کپی فایلهایی که انکریپت نشده اند به پوشه ای که انکریپت شده باعث می شود که فایلها به صورت خودکار انکریپت شوند.
- حرکت یا کپی فایلهای انکریپت شده از یک پوشه ای که انکریپت شده است به جایی که انکریپت نشده، فایلها به همان صورت انکریپت شده باقی خواهند ماند.
- حرکت یا کپی فایلهای انکریپت شده از یک پوشه انکریپت شده به محلی که فت NTFS ندارد نتیجه زیر را دارد:

فایلها دکریپت می شوند اگر پیغامی ظاهر شود و شانسی برای لغو عملیات حرکت یا کپی بدهد.

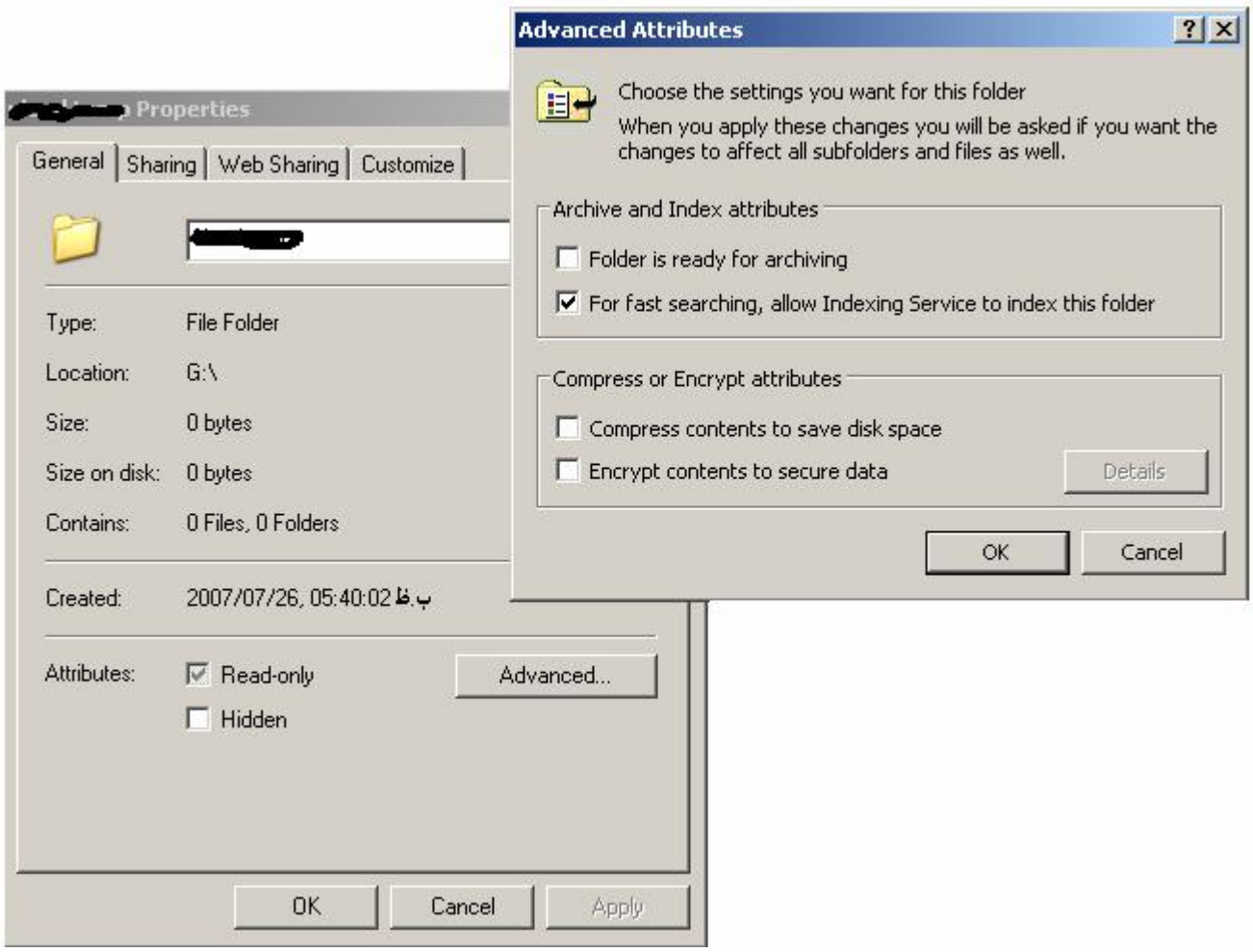
---

[2] fat

- پشتیبان گرفتن از فایلها با استفاده از ابزار پشتیبان گیری ویندوز ایکس پی نتیجه ای که در بر دارد اینست که همانطور فایلها را پوشه ها انکریپت می مانند.
- تغییر نام فایل انکریپت شده هم تغییر ندارد و فایل همانطور بعد از تغییر نام انکریپت شده باقی می ماند.
- حذف فایل انکریپت شده اگر به سطل بازیافت منتقل شود فایلهای درون سطل باز یافت همچنان انکریپت شده باقی خواهند ماند.

۲-۴-۱- انکریپت کردن فایلها و پوشه ها

برای انکریپت کردن فایلها رو پوشه ها روی آن فایل و یا پوشه راست کلیک کنید و بعد properties ، بعد از این مرحله به تب general رفته بعد دکمه advanced را کلیک کنید. (شکل زیر) (توجه کنید که قبلا گفته شد فت شما باید NTFSباشد)



گزینه Encrypt Contents to secure data را تیک بزنید. توجه کنید که نمیتوانید همزمان گزینه Compress Contents to save disk space را با این گزینه فعال کنید و در هر لحظه فقط حق انتخاب یکی از آنها را دارید. پس فقط یا قابلیت فشرده سازی را دارید و یا رمز گذاری و ونه هردو به صورت همزمان.

حال ok را بزنید و مجددا ok. اگر یک پوشه را انکریپت کنید پنجره تایید تغییر خصوصیات به شکل تصویر زیر ظاهر خواهد شد

اگر گزینه اول را فعال کنید فقط پوشه انکریپت میشه نه فایلها و پوشه های داخل این پوشه. اما اگر یک فایل جدید ایجاد کنید، یا جابجا کنید و یا کپی کنید این فایها انکریپت خواهند شد.

در صورت انتخاب گزینه دوم، تمام فایلها و پوشه های داخل آن پوشه انکریپت می شوند.

حال اگر سعی کنید که یک فایل را که در یک پوشه انکریپت نشده قرار دارد انکریپت کنید پیغامی ظاهر می شود (شکل زیر)

ما در اینجا باید گزینه دومی یا encrypt the file only یا گزینه اول را انتخاب کنیم . یک قانون عمومی وجود داره که اگه بخواهید یه فایل رو به تنهایی انکریپت کنید پوشه پدر اون هم باید انکریپت بشه زیرا اگر فایل به تنهایی انکریپت بشه ممکنه به راحتی دکریپت بشه. برخی برنامه ها هستند که از فایل یک کپی می گیرند و فایل اصلی رو پاک می کنند. در این موقع برای ویرایش کردن فایل توسط آنها دکریپت میشه.

در اینجا همان گزینه اول را که پیش فرض انتخاب شده هست رو باقی بگذارید و ok کنید.

توجه: فایلهای سیستمی که بیشتر در c:\windows و زیر پوشه هایش را نمیتوانید انکریپت کنید.

۲-۴-۲- دکریپت کردن فایلها و پوشه ها

برای این کار مثل قبل عمل کنید با این تفاوت که اینبار به جای زدن تیک ، اون رو بردارید پس مراحل اینطوری میشه:

راست کلیک روی فایل یا پوشه

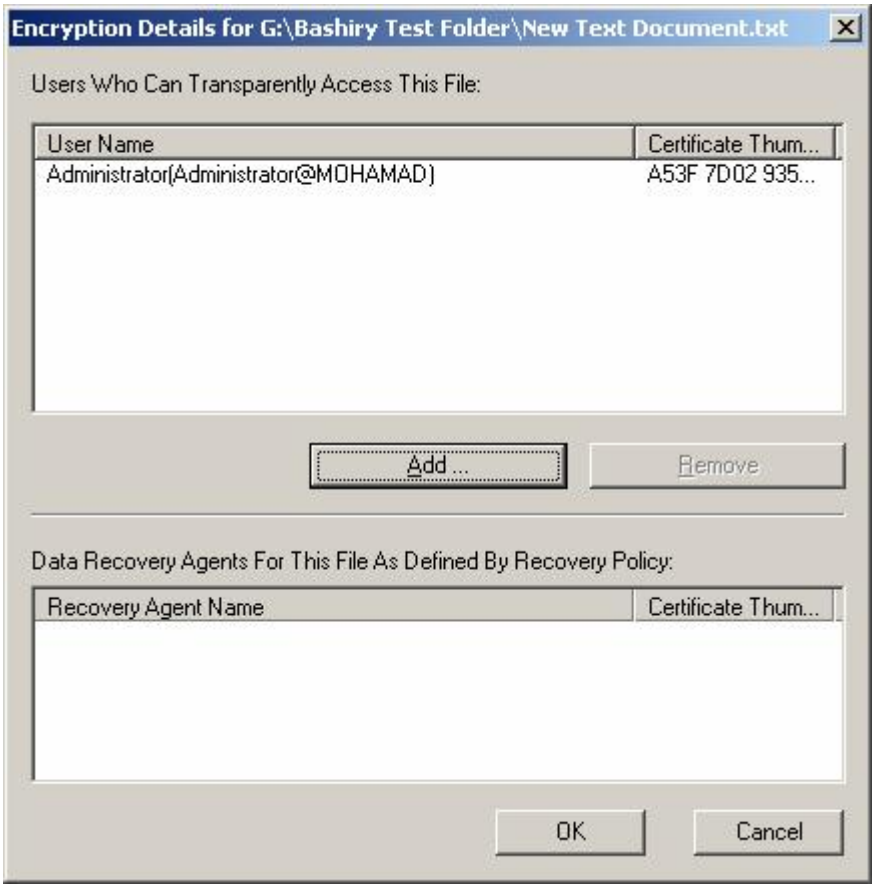
- انتخاب گزینه properties
- زدن دکمه advanced
- تیک کنار Encrypt contents to secure data را بردارید.
- دکمه ok را بزنید و دوباره ok

۲-۴-۳-استفاده دیگر در انکریپت کردن فایل

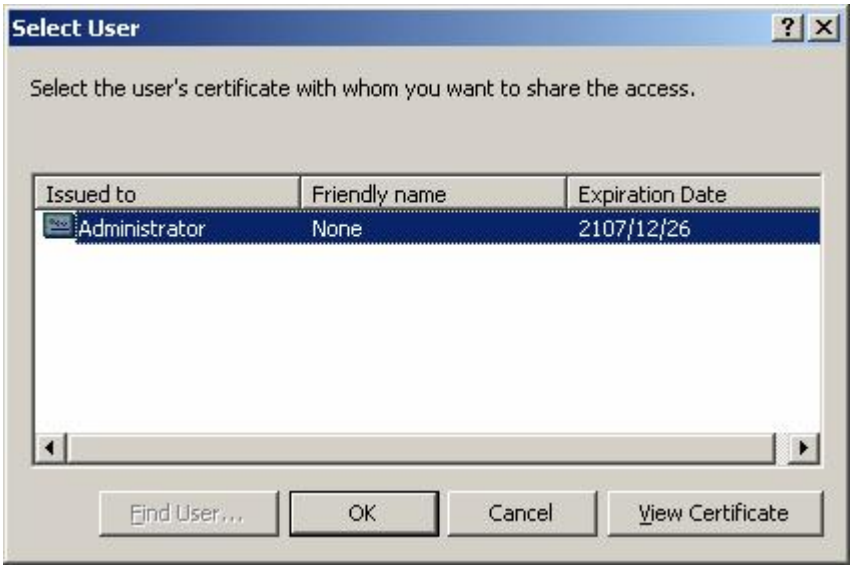
مبحث جالب دیگر که وجود داره این هست که میتوانید به بعضی کاربران روی شبکه یا روی کامپیوتر فعلی اجازه دسترسی به فایل های انکریپت شده را بدهید و به کدام اجازه ندهید. با این روش مثل فایلهای انکریپت نشده یا به اصطلاح ویندوز xp فایلهای "transparently." اجازه به اشتراک گذاری را میدهید.

برای این کار روی فایل انکریپت نشده راست کلیک کنید و سپس properties و بعد general و advanced را انتخاب کنید.

پنجره Advanced attributes باز می شود. در اینجا روی details کلیک کنید تا جزئیات فایل encrypt شده به نمایش در بیاد



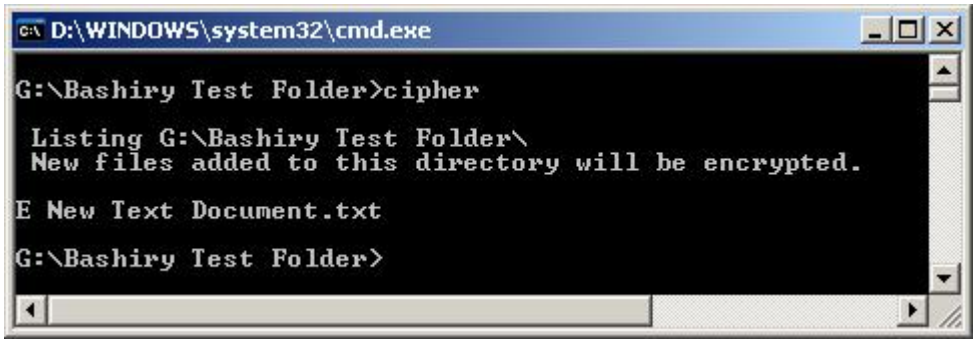
در این لیست، لیست همه کاربرای مشاهده می شود که می توانند به فایلهای transparently دسترسی داشته باشند. (فایلهای انکریپت نشده) روی دکمه add کلیک کنید. بعد از کلیک پنجره ای مثل شکل زیر باز خواهد شد:



کاربرانی که قصد دارید به فایلهای انکریپت شده دسترسی داشته باشند را انتخاب کنید تا به لیست اضافه شوند.

۲-۴-۴- انکریپت کردن و دکریپت کردن از طریق خط فرمان

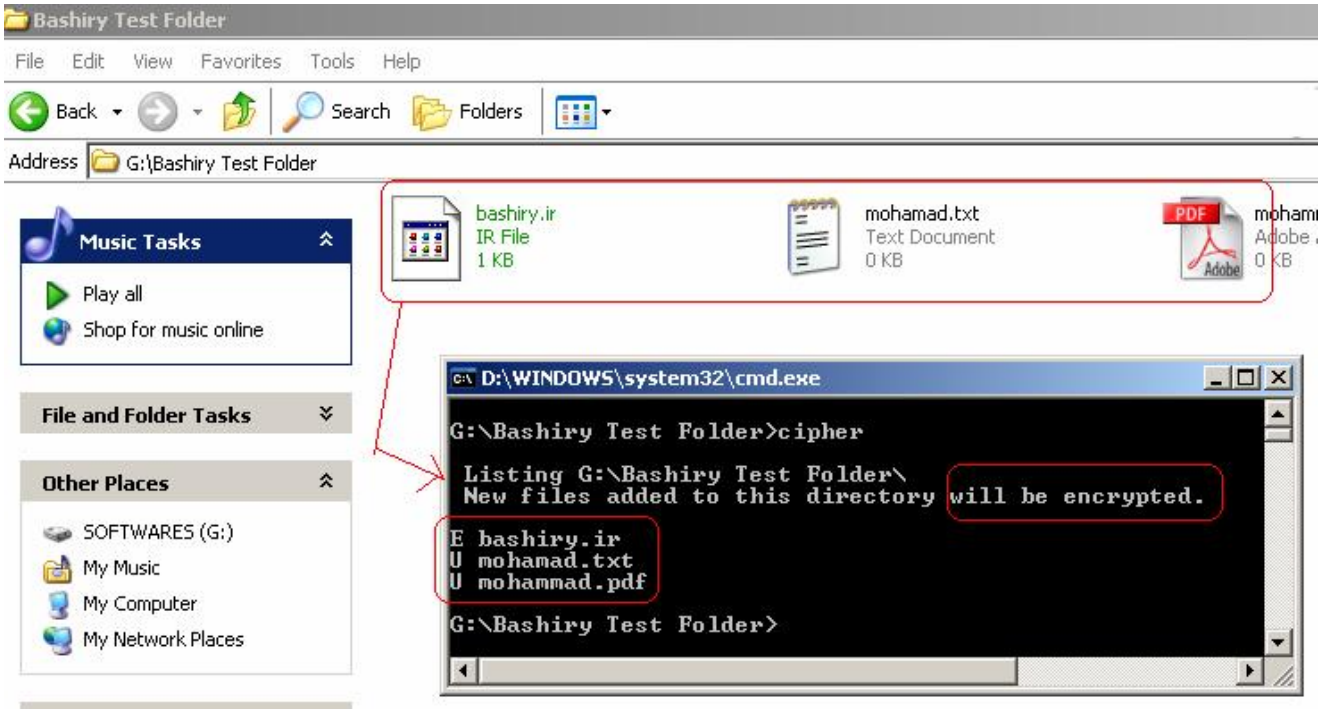
با استفاده از ابزار خط فرمان cipher.exe می توانید که عملیات انکریپت سازی و دکریپت سازی را انجام دهید. برای مشاهده وضعیت encryption پوشه جاری از عبارت cipher بدون هیچ پارامتری استفاده کنید.



مشاهده می کنید که نوشته شده که فایل انکریپت شده است.

همانطور که ملاحظه می کنید در اول فایل کلمه E به معنای انکریپت شده اضافه شده. اگر U اضافه می شد به این مفهوم بود که فایل انکریپت نشده است.

مثالی دیگر از هر دو نوع فایل:



با استفاده از نوشتن پارامترهای cipher میتوان فایل ها یا پوشه ها را انکریپت یا دکریپت کرد. برای انجام دادن این کار نیاز به نوشتن مسیر کامل فایل یا پوشه مربوطه دارید. لیست کامل سوئیچ های خط فرمان در جدول زیر به طور کامل آورده شده است. (جدول ۲-۴-۱)

استفاده از سوئیچ E/ فایل یا پوشه را انکریپت می کند و D/ آنرا دکریپت خواهد کرد. برای نوشتن چند دستور می توان آنها را با فاصله از هم جدا کرد.

برای مثال انکریپت کردن پوشه هایsecret و topsecret به صورت زیر هست:

```
cipher /E \Secret \Topsecret
```

نکته بسیار جالب اینجاست که در خط فرمان بر خلاف محیط گرافیکی قادرید به صورت دسته ای یا batch چندین و چند فایل و پوشه را منطبق با یک pattern نوشته شده انکریپت یا دکریپت کنید. در اصل استفاده از کاراکترهای معروف wildcard مثل ستاره، علامت سوال و ... .

مثلا: می خواهیم هر فایل با پسوند doc درون دو پوشه secret و topsecret انکریپت شوند و فایلهای دیگر دست نخورده باقی بمانند. پس اینطوری می نویسیم:

```
cipher /E /A \Secret\*.DOC \Topsecret\*.DOC
```

جدول ۲-۴-۱ – لیست سوئیچ های خط فرمان ابزار cipher

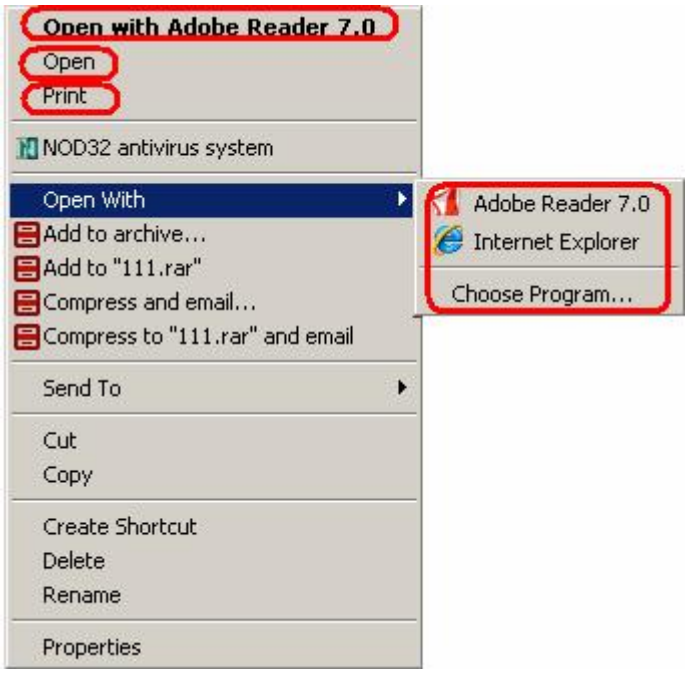
Switch	What it does
/A	Acts on individual files within folders.
/D	Decrypts the specified folder.
/E	Encrypts the specified folder.
/F	Forces encryption on all specified objects, including those that have already been encrypted.
/H	Displays all files in a folder, including those that have hidden or system attributes. By default, hidden or system attributes are not displayed when using the cipher command.
/I	Continues to perform the specified operation, even if errors are encountered. By default, cipher halts when errors are encountered.
/K	Creates a new file encryption key for the user running cipher. If this option is chosen, all the other options will be ignored.
/R	Generates an EFS recovery agent key and certificate, then writes them to a *.pfx* file (containing the certificate and a private key) and a *.cer* file (containing only the certificate).
/S	Performs the operation on the folder and all its subfolders.
/U	Updates the user's file encryption key or recovery agent's key on every encrypted file.
/U /N	Lists every encrypted file and does not update the user's file encryption key or recovery agent's key.
/Q	Lists only basic information about the file or folder.
/W	Wipes data from available, unused disk space on the drive. Normally, when a file is deleted in XP, only the entry in the filesystem table is deleted; the data itself remains untouched until another file overwrites it. This switch deletes all the data in those previously deleted files. It does not harm existing data.

این جدول رو هم میتونید با نوشتن cipher /? در خط فرمان ببینید.

هک ۲-۵- استفاده های دیگر از windows explorer

۲-۵-۱- ساختن یک منوی میانبر برای دسترسی به فایل با پسوند خاص

در explorer هنگامی که روی فایلی راست کلیک می کنید منوی میانبری مشاهده می کنید که شامل لیستی از برنامه هایی است که می توانید آن فایل را باهاش باز کنید.



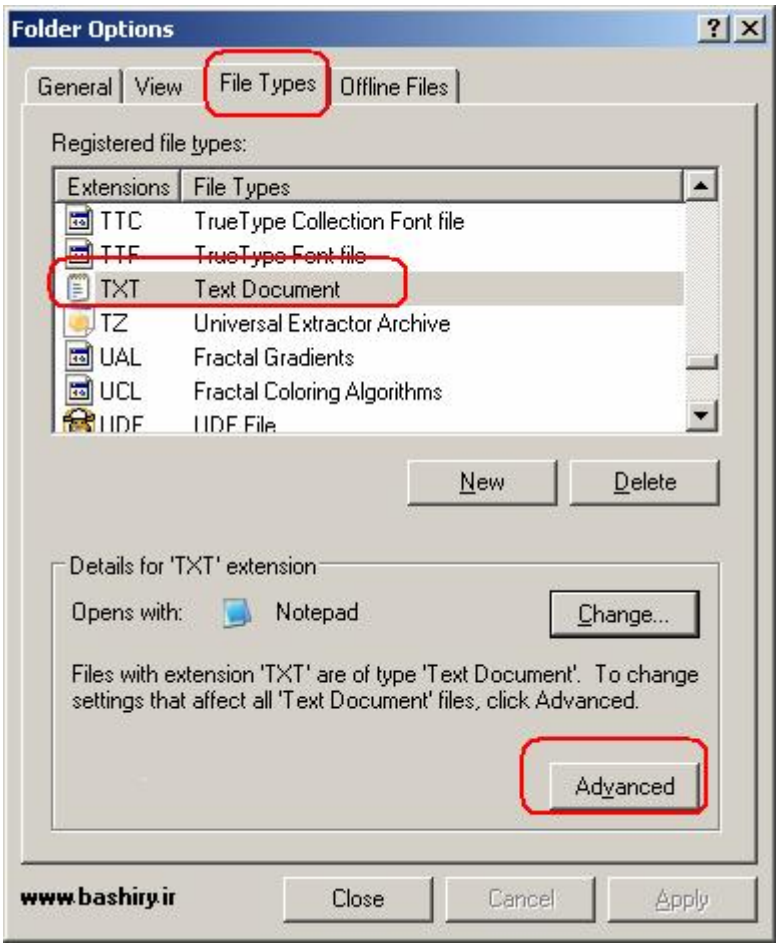
حالا اگه برنامه مورد نظرتون توی این لیست نباشه چی؟ به راحتی با روشی که در ادامه خواهم گفت قادرید این کـار رو بکنیـد. تصمیم داریم تمام فایلهای با پسوند txt. رو با یک برنامه مثلا Acrobar Reader باز کنیم . این فقط برای تمرین هست. شـما مـثلا می توانید تمام فایلهای با پسوند gif رو با برنامه irfan view که در سایت www.irfanview.com هست باز کنید و غیره.

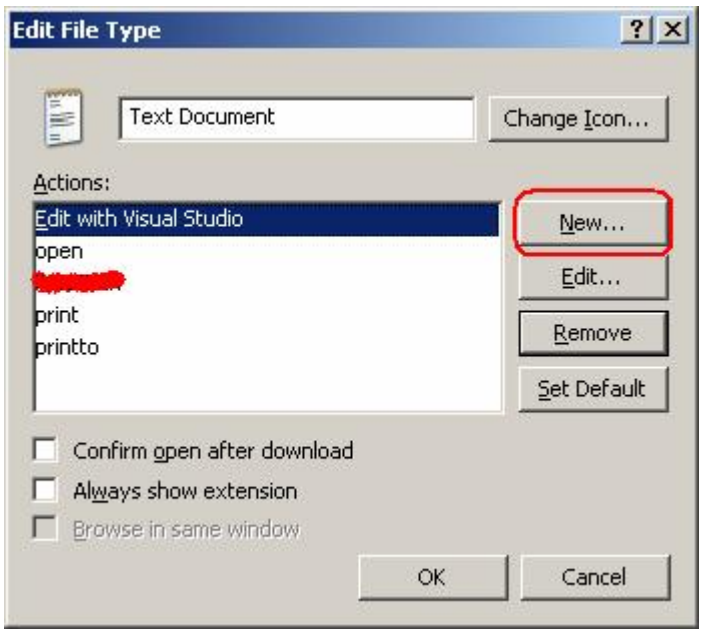
حالا بگذریم بریم سر اصل مطلب که مطمئن هستم که مشتاقید زودتر ببینید چطوری.

در windows explorer به مسیر زیر برید:

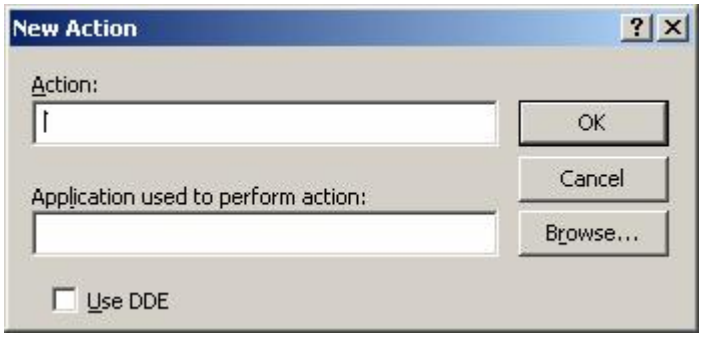
Tools→folder option → file type

در لیست به دنبال پسوند فایلی بگردید که میخواهید با اون کار کنید . در مثال ما پسوند txt پسوند فایل هست. بعد از پیدا کردن آن را انتخاب کنید و سپس advanced و بعد new را برای ایجاد action جدید کلیک کنید:



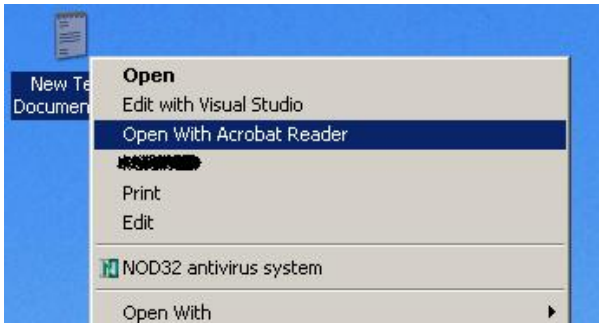


بعد از کلیک بر روی دکمه new پنجره آشنای به شکل زیر ظاهر خواهد شد:



در اولین بخش اسم دلخواه خودمون رو می نویسیم که قصد داریم وقتی روی فایل راست کلیک می کنیم در لیست فایلها نشون داده بشه و در بخش دوم هم مسیر فایل notepad رو میدیم. به صورت زیر

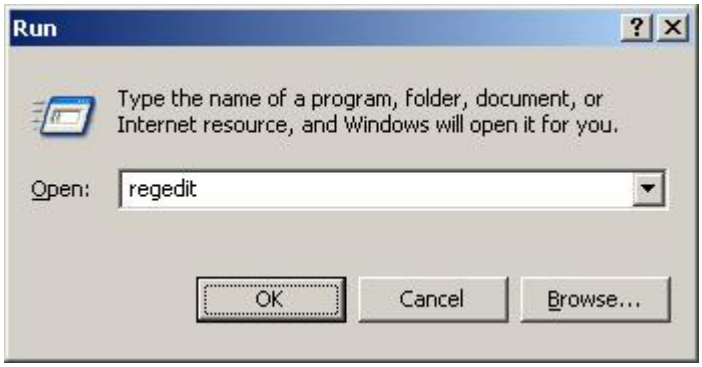
به بخش فیلد دوم کمی بیشتر دقت کنید. چیز جالبی هست. اطراف فایل مورد نظر رو با علامت نقل قول احاطه کردم و بعد در ادامه به صورتی که می بینید از "%1" با یک فاصله استفاده کردم. "%1" یک placeholder هست. در اصل یک جایگاه اختصاصی براش درست می کنیم. بعد از انجام همه تنظیمات دکمه ok رو بزنید و بقیه پنجره های هم تایید کنید و ببندید. برید روی فایل و حاصل کار رو مشاهده کنید (شکل زیر)



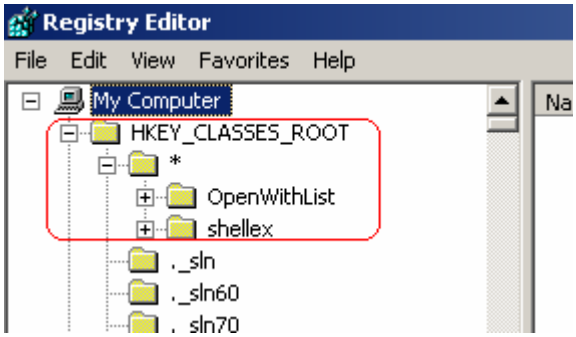
۲-۵-۲- اضافه کردن میانبر عمومی برای چندین فایل با پسوند مختلف

فکر کنید که یک فایل داریم که با طیف وسیعی از برنامه های مختلف با انواع پسوند ها قابل اجرا شدن هست. در مثال قبل به برای فایل txt یک میانبر ساختیم حالا می خواهیم کاری کنیم که روی هر فایل رفتیم گزینه مورد نظر ما ظاهر بشه نه فقط روی فایلهای txt. این عملیات با یک ترفند رجیستری قابل انجام هست.

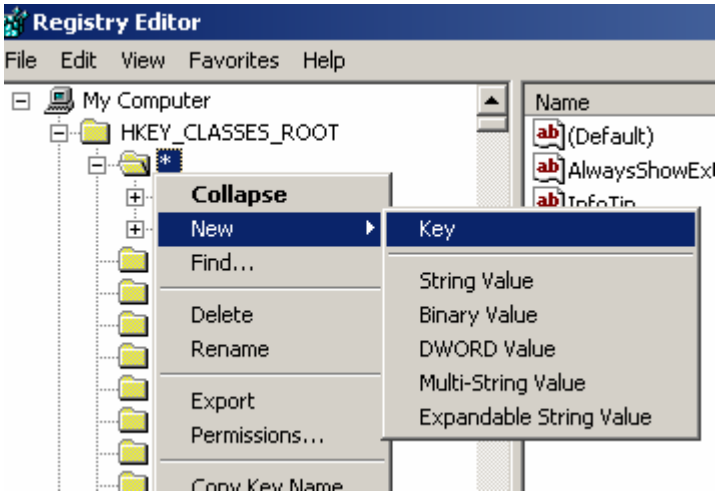
رجیستری رو باز کنید:

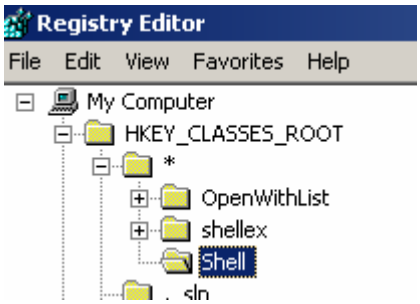


به بخش HKEY_CLASSES_ROOT* برید

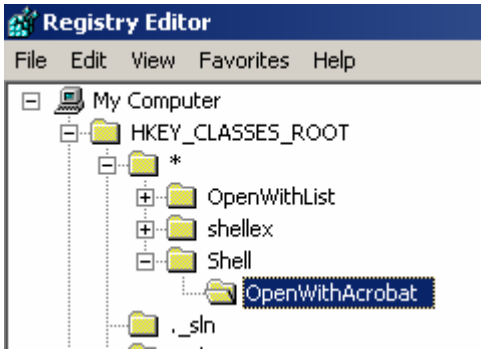


یک زیر کلید به اسم Shell بسازید (در صورتی که وجود ندارد)

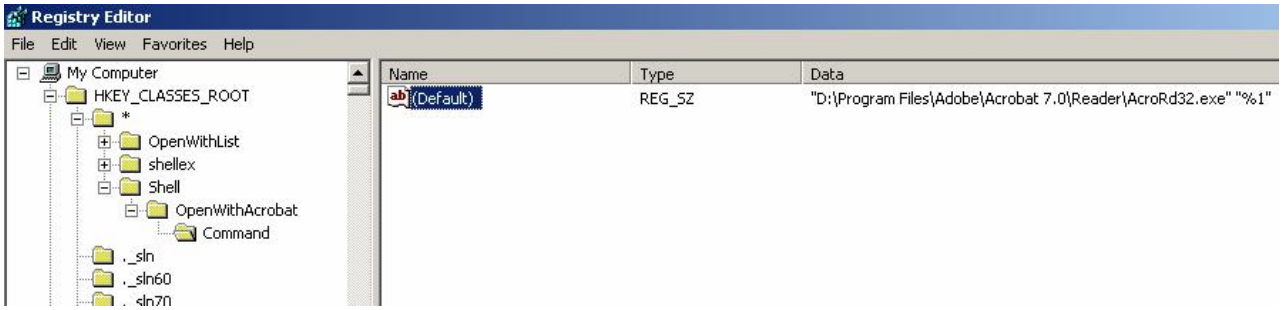




حال یک زیر کلید برای shell که ساختیم ایجاد کنید و اسمش را هم اسم دستور مورد نظرمون که می خواهیم نشون داده بشه قرار میدیم. مثلا OpenWithAcrobat

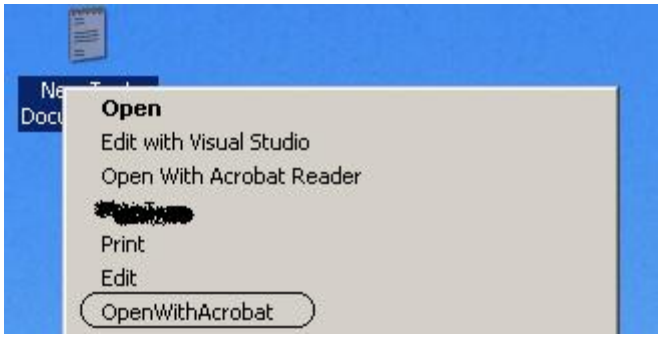


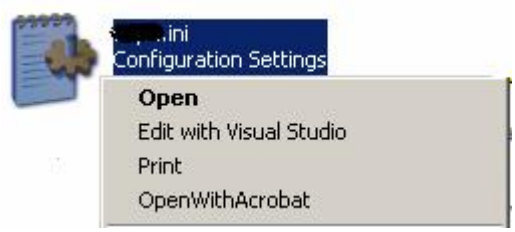
دوباره یک زیر کلید به اسم Command ایجاد کنید. در بخش Default Value مسیر فایل رو بنویسید. (به صورت زیر)



از رجیستری خارج شود و سیستم رو یه باز مجددا راه اندازی کنید تا تغییرات اعمال بشه(در صورت اعمال نشدن تغییرات). از

این به بعد روی هر فایل راست کلیک کنید گزینه OpenWithAcrobat رو داره.



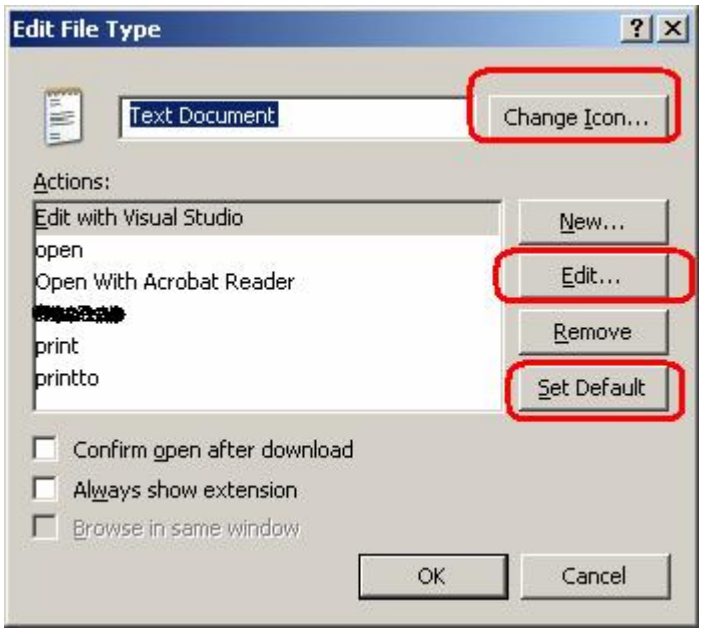


۲-۵-۳- ویرایش پسوندهای اختصاص داده شده به فایلها

تا الان دیدید فایلهای متنی با پسوند txt با notepad باز میشه. فایلهای با پسوند doc با word باز میشه و غیره. حالا

میخواهیم بریم سراغ دستکاری اینها و ویرایششون کنیم.

مثل حالت قبل به explorer→tools→folder option→file type میریم. پسوند مورد نظر رو انتخاب می کنیم و بعد advanced را می زنیم. دیگه زیاد توضیح نمیدم چون سادست با زدن دکمه edit قادر به ویرایش هستید و حتی قادرید icon رو هم عوض کنید



زیاد روی این بخش تمرکز نمی کنم . فکر نکنم به اون صورت نکته جدیدی داشته باشه.

۲-۵-۴- حذف گزینه های موجود در منوی کلیک سمت راست

مثلا برای حذف کردن دو مورد از منوی tools

مثلا گزینه اول و دوم map Network Drive و Disconnect Network Drive

در رجیستری به آدرس زیر می رویم:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

یک ورودی DWORD به اسم NoNetConnectDisconnect میسازیم و مقدار ۱ به آن می دهیم. از رجیستری خارج شوید و

اگر تغییرات اعمال نشد سیستم را راه اندازی مجدد کنید . برای برگشتن به حالت اولیه مقدار ۱ رو به صفر تبدیل کنید.