

Re: Thinking of reinstalling Windows...

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2006-05/msg03225.html>

- *From:* "cquirke (MVP Windows shell/user)" <cquirkenews@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 09 May 2006 00:06:54 +0200
-

On Mon, 8 May 2006 14:19:35 +1000, "ntuser"

First, a little background: I've had my PC for a couple of years now and i've made several user accounts in that time. Everything has always worked

The present day: Lately, I deleted those previous accounts except 1 and created a new limited user account (for my PC inept family). After logging in and importing the files from the deleted accounts I noticed that the picture files (.jpg, .gif etc) were now represented by that icon for file extensions that windows don't recognize (in windows explorer). I then tried to double click and open them

....and to summarize, nothing worked and attempts to Open With a new permanent association failed to "take". Same failure for changes made in Tools, Options, File Types to "take". Attempts to create fresh arbitrary extension associations worked. Then...

I deleted the account and created a new administrator account and logged in. This time whenever I double clicked a .jpg/.gif etc file type; it would open with...you guessed it – the Windows picture and Fax viewer! I thought things were finally working.

I've read this issue in another thread, and it sounded like this...
– the prototype per-user registry gets corrupted (no visible hassle)
– a new account is created with this bad registry prototype
– bad file association entries mask system-level associations
– attempts to fix via UI fail, due to HKCU vs. HKLM contention
– other (existing) user accounts work fine
....but this is new news; that a freshly-created Admin account (presumably based on the same prototype registry) is OK.

That suggests some permissions issue. In fact, silent failure of

Re: Thinking of reinstalling Windows...

settings changes to "take" is typical for permissions blockage.

In windows explorer; the files were still relegated the unknown file type icon. Despite the fact that they would open with the appropriate program – Windows couldn't associate the .jpg/.gif etc as a "JPEG image/GIF image" etc.

Don't confuse the default action, the "open" action, and the icon displayed – they can all be different, and set independently. Often the icon is set according to the default or "open" action, but not always – and if so, that's a function of the UI code through which you set the associated action. Non–UI changes (corruption, Regedit) will not sync the two, and this may be a diagnostic pointer in itself.

When you rt–click, the action in bold is the default action.
When you double–click or Enter, the default action runs.
If you Start an associated file, the action called "open" runs.
The legacy "Open With" list is built from actions called "open"

IOW, in some contexts you can have one action that runs because it is called "open", and other contexts you can have a different action that runs because it is set as the default action.

For the *same* file type.

I then went to take a look at the My Computer>Tools>Folder Options>File types window and sure enough; the .jpg/.gif file types weren't there! And of course, I encountered the same cyclical problem as before.

What you see in that UI is mediated by EditFlags settings held within that file association data, as seen via RegEdit HKCR.

But HKCR is itself an abstraction built by overlaying the system–wide Classes from HKLM with the account–specific Classes from HKCU.

Your pattern suggests a problem at the HKCU level, which may be why UIs that combine both as "HKCR" get confused and fall over.

Counterspy (anti–spyware software that suspiciously enough looks to have the identical features of Windows defender

Giant subbed out their code to Counterspy
MS acquired Giant, dev'd it to MSAS and now Defender
MS agreed to maintain data compatibility with Counterspy for a while

Re: Thinking of reinstalling Windows...

So both MSAS/Defender and Counterspy have equally valid and legal ancestry in Giant's original product (which was a good one)

... the testing of various registry 'cleaner' programs.

There's the headstone! Those *SUUUCK*, unless you need practicals for a study course in "Troubleshooting Classic Registry Disasters".

Despite Noron Internet security 2005 catching the "reger.exe" virus and deleting; I was infested with multiple pieces of incredibly annoying spyware (alexa etc etc).

Alexa is waved as something of a false-positive by SpyBot, wherever IE is present (i.e. in just about any Windows system).

This all happened at once. It was if I was hit by a spyware bomb.

You may have been, but not in the way you'd expect (tho that is possible too). You may have picked up one of 200+ fake "antispyspyware" (f)utilities that charge you money to clean up fake detections.

The only way I was able to remove the infections was through a combination of Counterspy (which I re-installed) and the multiple registry cleaning software

Not really the right approach – registry cleaners use the wrong criteria when deciding what to automatically clean (and commonly cause problems due to unanticipated dependencies on material that appears to be :unused" and thus OK to "clean").

Instead, my approach would be:

- formally [*1] scan for intra-file infectors
- do automated scans for commercial malware
- manually inspect integration points
- reversably disable suspect entries in the above
- de-bulk the load by moving all Temp, TIF, DPF
- purge SR when happy that all is well

[*1] i.e. without running ANY of the infected code base.
Google(Bart PE), Google(Maintenance OS).

Re: Thinking of reinstalling Windows...

It's unlikely that these events are the source of my file association problem but I thought I'd mention it.

It's quite likely that registry cleaners did this to you. Did you keep a log and/or Undo for everything these idiots did?

Additional remedie steps taken:

1. sfc /scannow off the xp disc

I doubt if that would help – that replaces the bricks, whereas your problem is the cement that glues them together

2. The attempted application of downloadable stable registry entries as suggested by this newsgroup. However I now encountered a new type of error when attempting to merge these stable reg entries into my registry. I would receive a "Cannot import "file": Error accessing the registry".

O...K... – could be a fake error from some permissions issue.

Most "quick" advice .REG will be HKCR or HKLM, and merging a .REG seldom *removes* troublesome entries. You may need to find and remove something germaine in HKCU, rather than HKLM, and the "easy" HKCR may not be helpful in resolving HKLM vs. HKCU feuds.

I was able to merge these reg keys into my last remaining old user account "Registry entries merged successfully". This led me to believe that the error may be due to a corrupted nuser.dat file and thus a corrupted Default user profile that all new user accounts copy off from.

Now you're talkin' :-) Could be a bad exit when a registry cleaner was grinding thru that hive?

One thing didn't make sense however

....the new Admin account worked, and that's built on the same Default data that you (and I) suspected was corrupted.

The hkey_classes_root reg hive had different registry entries for the .jpg file type between the new user accounts and the old working account.

Re: Thinking of reinstalling Windows...

Sure, that's because HKCU trumps HKLM when building what you see as HKCR, and things get messy if tools only work on HKLM.

Different user, different HKCU picked out of HKU, thus YMMV.

hkey_classes_root reg hive is actually assembled as thus:

The HKCR hive itself does not really exist, it's a combination of HKLM\SOFTWARE\Classes (default settings) and HKCU\Software\Classes (user settings) while HKCU\Software\Classes is dominant if the values of identical settings differ. Therefore, HKEY_CLASSES_ROOT is both system *and* user related.

Yep.

The only other things I have noticed is that this problem also effects the default administrator only accessible through safe mode.

Now that's interesting. State-chart this:

Safe Mode Normal Mode
Default administrator account Bad ?
OK user account ? OK

So there you have it; the scanario in full. Hopefully you have better luck in ascertaining the source of the problem then I did.

We seem to have reached the same conclusions :-)

The most accurate diagnostic instrument
in medicine is the Retrospectoscope
