

## Re: File Summary/ Knowing when a file is created and deleted/ The first program started when windows starts

**Source:** <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.mfc/2004-03/3647.html>

---

**From:** Christopher J. Holland (*msnews\_at\_microsoft.com*)

**Date:** 03/31/04

Date: Tue, 30 Mar 2004 16:52:14 -0800

Thanks,

I found something better from the information you gave me.

"To avoid these disadvantages, the NTFS file system maintains a change journal in Microsoft® Windows® 2000 and later. When any change is made to a file or directory in a volume, the change journal for that volume is updated with a description of the change and the name of the file or directory"

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/fileio/base/change\\_journal\\_records.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/fileio/base/change_journal_records.asp)

That helps out a whole lot. All I have to do is read the Journal.

The problem now is when?

Once daily, hourly, weekly? (Factor is System Performance Degradation.

Investigation is needed)

After a program is Installed/Deinstalled (YES)

Upon startup (YES)

IP Operations (Unsure. This could be a critical factor)

FSUTIL Reference:

[http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/fsutil\\_usn.msp](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/fsutil_usn.msp)

USN Journal Reference

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/featusability/msjntfs5.msp>

<http://www.microsoft.com/msj/1099/journal2/journal2.aspx>

Thanks for your help,

"David Crow [MCSD]" <david.nospam.crow@pbsnow.nospam.com> wrote in message news:11hac.11821\$7F7.6422@newssvr22.news.prodigy.com...

> *ReadDirectoryChangesW()* and *FindFirstChangeNotification()* is one place to

> start. The *FileMon* utility

> (<http://www.sysinternals.com/ntw2k/source/filemon.shtml>) is another.

>

> "Christopher J. Holland" <msnews@microsoft.com> wrote in message  
> news:uQnZeDjFEHA.3404@TK2MSFTNGP10.phx.gbl...  
> > Hi,  
> >  
> > I was infected with a few viruses/spyware/ads, etc.I was able to clean  
> them  
> > up.  
> > I also got some program that cleans disk of 0 byte, bak, tmp files and  
> such.  
> > (Hopefully I didn't delete any important files.)  
> > I also started browsing directories and I see files that I have no idea  
> what  
> > they are and who they belong to.  
> > Some of the files have "Version information", which I can only assume is  
> > correct.  
> > I click properties of some files and notice a "Summary", with no  
> > information. Is it good file bad file, obsolete, or ?  
> > I also know that a lot of programs don't get rid of files and  
directories  
> > after the program is uninstalled.  
> > I am tired of these problems.  
> >  
> > I am doing a feasibility study of a project that monitors the Hard Drive  
> for  
> > added /deleted files  
> > and reports them. Then maybe filling in the Summary window with  
infomation  
> > about the file.  
> > That way the user would know if some file is inadvertantly added without  
> > consent.  
> > The Remove programs would "really" work.  
> > I could scan the entire hard drive periodically, but may there is some  
API  
> > that would  
> > alert my program of a newly created file.  
> > I suppose I would have to ignore some directories like temp and such.  
> > No program should be able to install to anywhere without an option to  
> remove  
> > every associated file.  
> >  
> > Can you point me to some API/information to automatically know if any  
file  
> > is added or deleted?  
> > Can you point me to some API/information on how to fill in Summary  
> > information?  
> >  
> > Also, the program needs to be the first thing started, for it to be able  
> to  
> > monitor  
> > when some program adds files before the windows UI is launched.  
> > There are programs that install upon reboot of Windows and before other

> > *programs are launched. So, it needs to launch before any other program.*  
> *Even*  
> > *with windows service packs and such. Maybe having to scan the harddrive*  
> > *after those type of programs is necessary?*  
> >  
> > *Maybe I would not have to add Summary information, but have a list of*  
> > *programs and their associated files.*  
> > *when I right click a selected a file and choose "Associated Program",*  
the  
> > *Monitor Program would launch and*  
> > *tell me when the program was installed and who the file belongs to. Then*  
I  
> > *would know if the file was safe to delete.*  
> >

=====  
> > == *Monitor Program*  
> >

=====  
> > *The program would monitor the hard drive to see if file is being*  
created.  
> > *Some thing would flash in the taskbar to alert the user.*  
> > *After each program installation, the user would have to add summary*  
> > *information.*  
> > *(Deleted files would be noted. They are not as important as added files.*  
> > *The deleted files would just be removed from the programs associated*  
> > *files)*

> > ----- *Program*  
> *Layout* -----  
> > *Programs installed – Date – Directories – Associated Files*  
> > *–Windows Basic – 01/01/04*  
> >  
> *notepad.exe*  
> > *System32*  
> >  
> *freecell.exe*  
> > *+Windows SP1 – 01/02/04*  
>  
>

-----  
> --  
> >  
> > *I would like to seperate Programs from data. A layered approach.*  
> > *Programs usually save the data to the same drive, with an option to save*  
> > *elsewhere.*  
> > *This would keep the program to minimal operation.*  
> >  
> > *CDrive: Executable programs only*  
> > *DDrive: Data only*  
> >  
> > *Thanks for your help,*  
> > *Christopher J. Holland*

microsoft.public.vc.mfc: Re: File Summary/ Knowing when a file is created and deleted/ The first program started when windows sta

> > *Monday, March 29, 2004*

> >

> >

>

>

Re: File Summary/ Knowing when a file is created and deleted/ The first program started when windows sta