# How to fully degunk a PC to get rid of crapware

Version 2.0
June 28, 2007

**By George Ou**

One of the most hated things on the personal computer is crapware. It slows your PC to a crawl, often causes instability and crashes, eats up valuable screen real estate, and may even border on malware. I started on this topic a few months ago with a partial solution, but it wasn't the total solution that really scrubbed the computer clean. This time, I'm going to show you thoroughly scrub a PC of crapware, but first I'm going to give a few definitions.

## Definition of crapware

Crapware is software you don't want on your computer. Not everyone will agree on what is and what isn't crapware because a piece of software that one person wants might be something that another person doesn't. Some software will fall in the gray area where people need—or they think they need—certain features of the software but it causes them grief by resulting in system slowdown or instability. Although we can technically define malware, spyware, or adware as crapware because it's software that people definitely don't want, those three typically get put in to the category of malware.

## Examples of crapware

Crapware might come in the form of a bloated driver CD that installs additional junk on top of the required driver. It might be software that came with a router, printer, or broadband service that the typical user unwittingly installs. Or it's the stuff that came preinstalled on the PC you purchased. Oftentimes, you try to install something to play a simple video and it installs a massive music library manager. Or you install a piece of software and you get an extra toolbar added to your Web browser even though you never asked for it.

At the end of the day, it comes down to companies fighting each other for every inch of your screen real estate, monetizing every search and every click, and capturing every glance you make—which turns your computer in to a messy battleground. What every user wants to know is this: How do you get rid of that unwanted crap and take back your PC? The following techniques aren't guaranteed to get rid of every piece of crapware on your Windows (2000, XP, or Vista) computer, but it is one of the most thorough methods available that a modestly computer literate person should be able to follow. The two free tools you will need to download are:

- Autoruns
- CCleaner

**Note #1**
A few people have complained that Autoruns broke some device drivers, such as the keyboard, or caused a BSOD (Blue Screen Of Death).This should never happen with a healthy PC, but in the event you find yourself locked out of Windows due to one of these problems, tap the F8 key as soon as Windows starts booting up and use the Last Known Good boot option. That will undo the registry changes made by Autoruns and put your computer in the state it was previously in. If you are uncomfortable with this recovery procedure or you're not sure how to execute it, stop reading at this point and do not attempt this procedure, because you won't be able to repair your computer if anything bad happens.

A properly designed device driver should never rely on anything that Autoruns can disable, and it should never stop functioning (especially the keyboard) just because Autoruns disabled the extra startups. If you find some devices need some of the startup settings, Autoruns will allow you to enable individual components. If your computer crashes because you stripped out all of the unofficial unsigned Microsoft startup entries, that could be an indicator of a deeper problem with your computer and could be a sign of malicious tampering. If a piece of malware modifies a legitimate file to piggyback on it, that will invalidate the Microsoft digital signature and Autoruns will treat it as an unofficial unsigned entry. Then, it that tampered entry is disabled, Windows may crash on startup. If you find that using Autoruns to disable all unsigned Microsoft entries causes your computer to crash, it might be a good time to do a wipe and reload of Windows since there is possibility of malicious tampering.

**Note #2**

It appears that some people may be having problems even with legitimate software. After checking with master programmer and Technical Fellow Mark Russinovich of Microsoft (formerly SysInternals), it appears that some people might be running device drivers that haven't gone through WHQL (Windows Hardware Quality Laboratories), which means that Autoruns will not hide it from the user. If those unsigned drivers get disabled by the user, Windows may get a BSOD or have certain devices like keyboards fail on startup. Ideally, users should never trust unsigned drivers, but it's an unfortunate reality that we have to deal with sometimes.

In the event that you disable everything unsigned (unauthorized) by Microsoft and have the misfortune of not being able to boot Windows, you will need to go in to Windows using the F8 during startup with either the Last Known Good or safe mode. Last Known Good should put your computer back the way it's supposed to be, but if that fails, you'll need to go in with safe mode and re-enable everything in the Drivers tab of Autoruns. If you want to play it safe, you can leave everything in the Drivers tab enabled, but ideally you shouldn't need anything checked that isn't authorized and signed by Microsoft. Russinovich also did a Webcast last year where he used a combination of Autoruns and Process Explorer for "Advanced Malware cleaning," and I highly recommend it.

Autoruns is a startup cleaner utility that is similar to the MSCONFIG utility but far more comprehensive and accurate. MSCONFIG shows you only startup and services, and it doesn't check digital signatures—which means anything can hide from it. With Autoruns, nothing can hide and there's no need to use MSCONFIG at all.

After you have downloaded Autoruns from the official Microsoft Web site, you'll need to unzip it. You do not need to install anything, just extract the content anywhere on your computer. Windows XP and Vista have built-in ZIP support, so you can just right-click on the file and hit Extract. Windows 2000 users will need to download a FREE utility like IZArc, which also comes in handy for Windows XP or Vista because it supports a wide range of compressed files. After you extract the files to a folder, simply double-click on the file named autoruns.exe. Vista users will have to elevate UAC privileges when running this application.

Once opened, you'll see the application shown in **Figure A**. You'll need to enable Verify Code Signatures and Hide Signed Microsoft Entries. **DO NOT SKIP THIS STEP!** After checking these two items, hit the F5 key to refresh the scan.

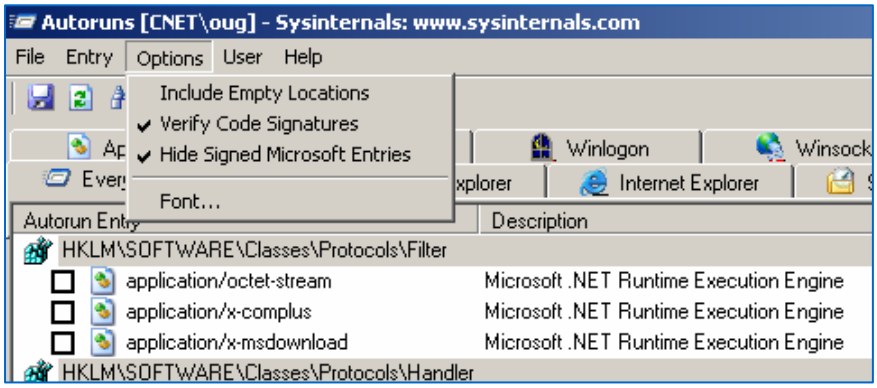


**Figure A**

The beauty of Autoruns is that it can verify the authenticity of everything being loaded into Windows through rigorous cryptographic signatures, so it can't be fooled by registry entries masquerading as something legitimate and it will recognize files that have been tampered with. By hiding all of the verified Microsoft entries, you can single out every piece of software that was added to our computer that isn't officially from Microsoft. Autoruns is effectively a spotlight that highlights all the potential crapware on your computer and it makes it easy for you to disable anything you don't want.

Take **Figure B**, for example. This is a list of stuff that popped up that wasn't signed as Microsoft code. Some of it may have been legitimate Microsoft code, but I don't need any of this stuff to make Windows run. Even the Adobe stuff is unnecessary, and my Acrobat Reader works fine without it. We can safely uncheck all of these entries and everything will work just fine.

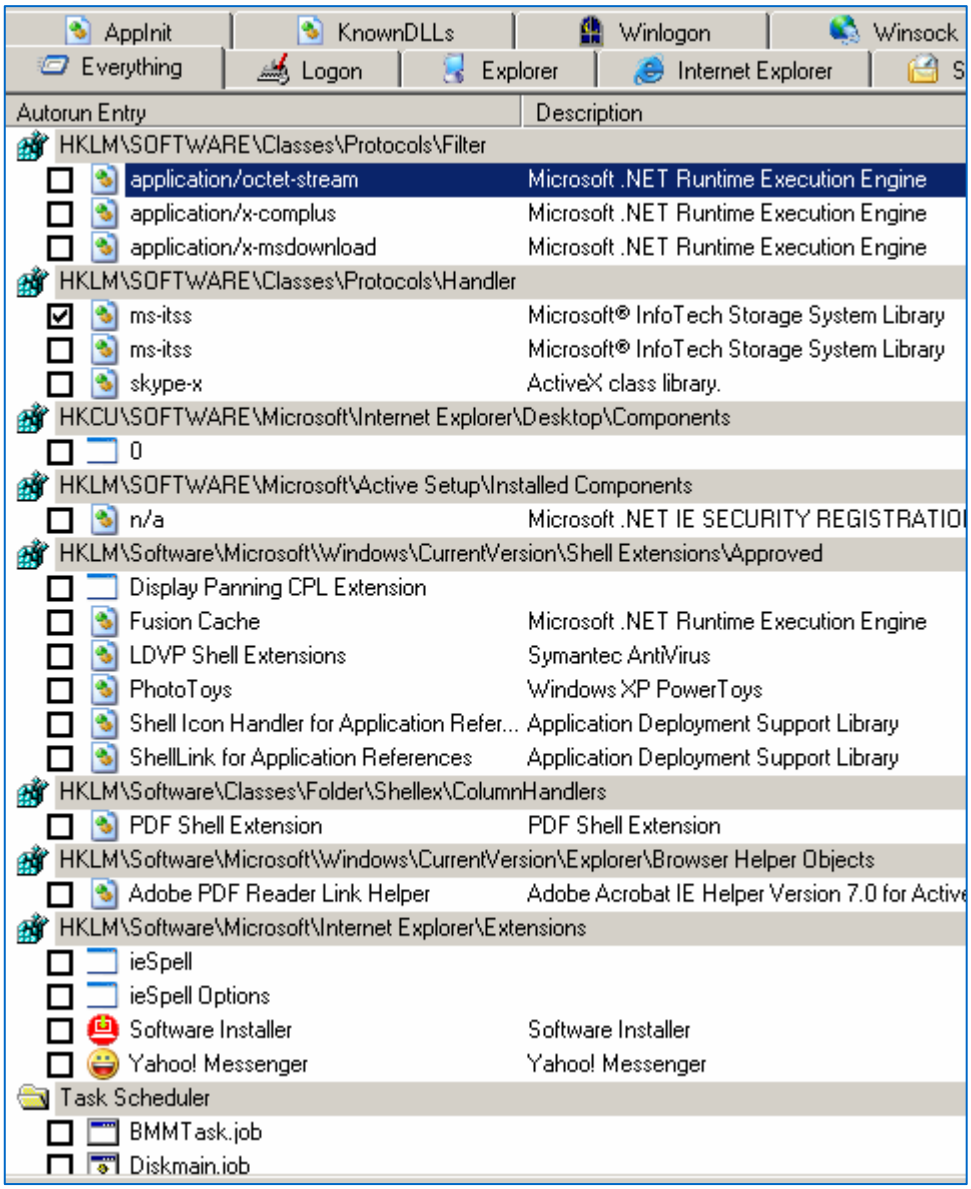


**Figure B**

In the unlikely event that any of the stuff on your list is actually needed for a critical application, you can always come back and re-enable certain parts bit by bit. These changes are nondestructive and there are no risky registry changes that need to be made.

Whenever I'm troubleshooting a computer, I disable everything in that list. Chances are, a lot of strange issues will disappear. I generally like to keep everything unchecked. You might want to leave the antivirus stuff checked, but I generally consider that one of the worst forms of crapware (though it may be a necessary evil for most people especially prior to Windows Vista).

Once you clean out the startup with Autoruns, you'll need CCleaner to flush out all the junk files and bad registry entries on the computer. You'll need to download CCleaner from this Web site and install it. Ironically, there is some crapware bundled with CCleaner in the form of a major search engine toolbar. You can choose not to install it, which I recommend. It helps finance this free utility, but at least you can uncheck it and avoid installing it.

Once installed, you'll launch the CCleaner application, shown in **Figure C**.

The Advanced section on the bottom isn't checked by default, but I usually select it. Note that flushing the Menu Order Cache will mean that all your bookmarks and shortcuts will be alphabetically arranged instead of chronologically. Click on Run Cleaner and it will flush all the junk files on your computer. This can easily clear a gigabyte on some computers, and I've seen some systems where I've cleared out 2 gigabytes.

Next, we have the Issues section, shown in **Figure D**. This is a two-step process to clean out the Windows Registry. You first click on Scan For Issues and wait for the results. Then, you click on Fix Selected Issues and it will flush out all those bad entries. Note that it gives you an opportunity to save the changes in an REG file. which you can double-click to undo the deletions from the registry.

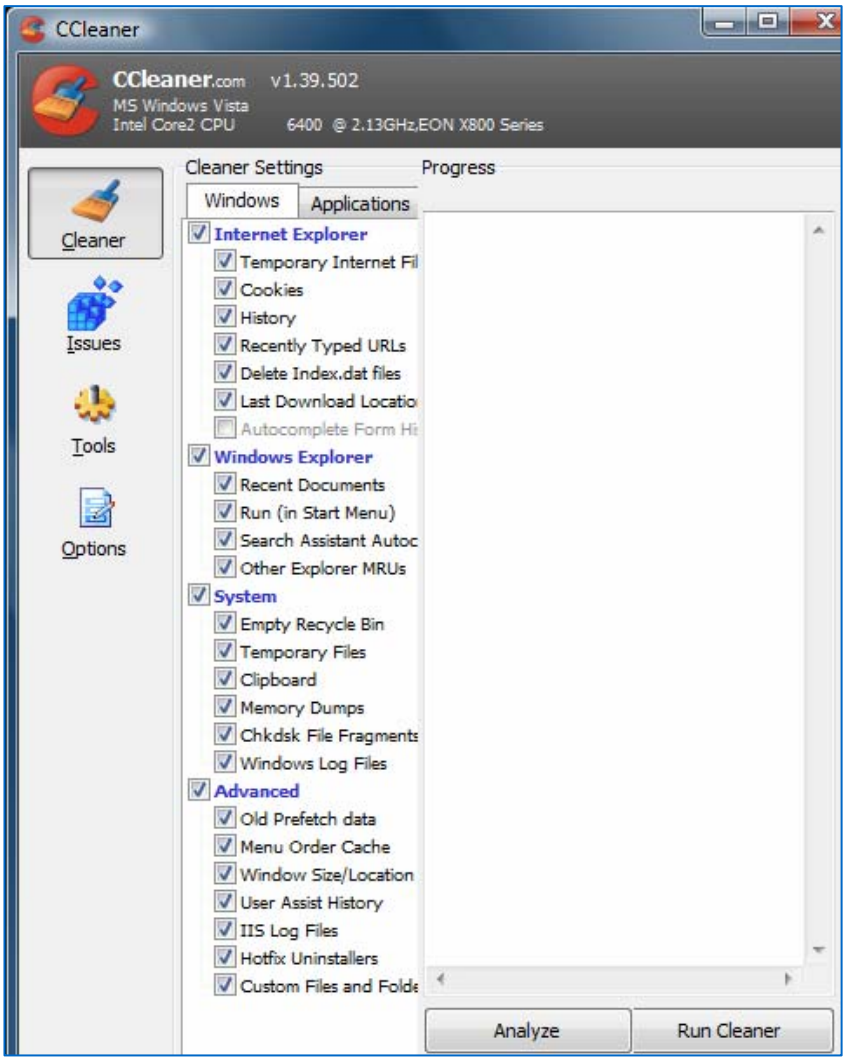


**Figure C**

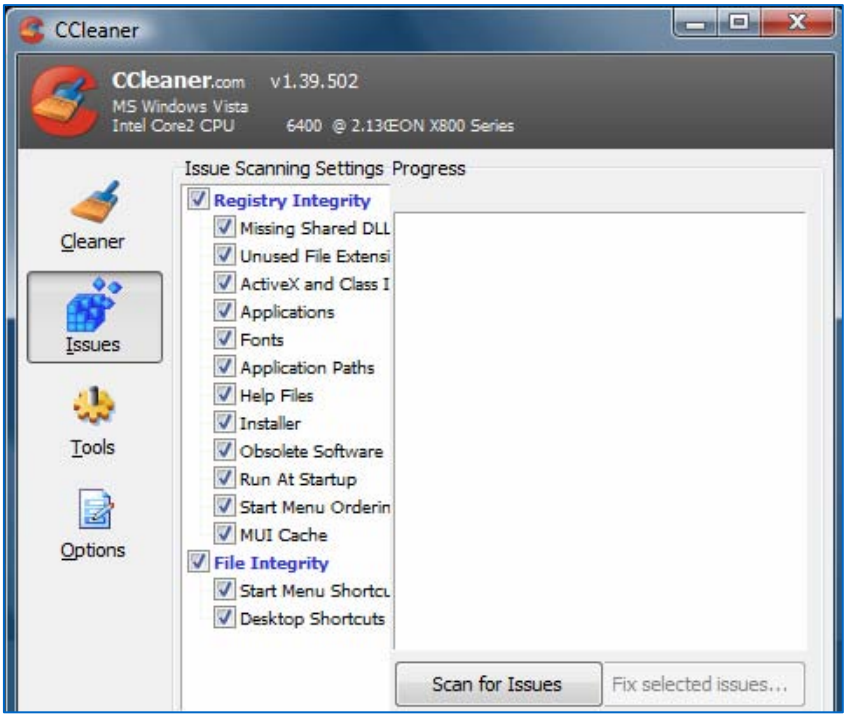


**Figure D**

**Figure E** shows the optional Tools section. I use this section for uninstalling applications I don't use. I don't use the Startup button because Autoruns does a much better job with that and it makes nondestructive changes you can easily undo.

The Uninstall feature is handy to have, though you can use Windows Control Panel to uninstall applications as well. However, CCleaner's uninstaller does a much nicer job because it can see many more items on a more granular level that you can uninstall.

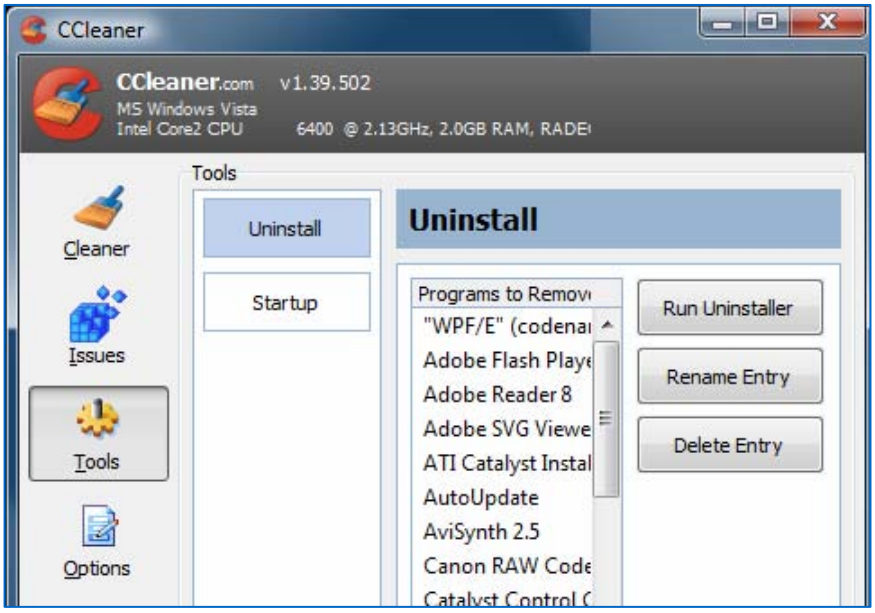


**Figure E**

Once you've performed all the Autoruns and CCleaner tasks, it's time to reboot your computer. Once rebooted, your computer will feel as fresh and fast as the day you first installed Windows. It might even feel better than the day you purchased the PC, which was already preloaded with a ton of crapware.

It isn't uncommon to see computers that use to take three minutes to boot all of a sudden drop to 40 seconds boot time. Many of those strange pauses when you use your computer will disappear. If your computer still takes a long time to boot, remains unstable, and often has pauses, chances are there is a faulty device driver or antivirus program causing the problems.

## Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for TechRepublic's Downloads Weekly Update newsletter
- Sign up for our Desktops NetNote
- Check out all of TechRepublic's free newsletters
- Follow these tips to boost Vista performance (TechRepublic download)
- Monitor and optimize Windows XP Pro system performance and reliability (TechRepublic download)
- Take control of Windows XP system properties during both startup and shutdown (TechRepublic download)

### Version history

**Version**: 2.0 (Note #2 added)
**Published**: June 28, 2007

### Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team