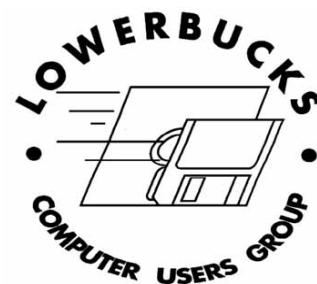


The ASCIIriber

THE JOURNAL OF THE LOWER BUCKS COMPUTER USERS GROUP

Volume 33 • Issue 3, March, 2014



Gone again and a free book

Once again I have to travel to corporate HQ in Raleigh and will have to miss the meeting.

Hopefully this will be the last time this will happen for a few months but who knows.

In the past we've talked a lot about Lightroom. What would be nice would be an easy to read and understand user's manual to help when the program is new to you. Even better if it was free.

It's here: <http://www.lightroomqueen.com/free-downloads/quickstart/lr5/>

The author, Victoria Bampton, is a Lightroom expert and the author of Lightroom books since the program first appeared.

I hope you enjoy it and I'll see you in a month.

NEXT MEETING:

SUNDAY, March 2, 2 P.M.

Staying with XP? Thinking about getting a solid state drive? Need a media player? Jim McGorry's articles have the information you need.

- Last reprieve for XP
- PC Backups
- Trading up to SSD's
- VLC Media Player

From: The Desk of Jim McGorry
Excerpts taken from the Windows Secrets Periodical

A LAST REPRIEVE FOR THE ENDURING WINDOWS XP?

By now, every Windows XP user and his third cousin should know that on April 8, the clock runs out on the venerable OS.

But recent developments might give XP users a bit of a reprieve. When and how Microsoft will blink are the open questions.

Microsoft's Original Stance: The End Is the End

The folks in Redmond continue to insist that XP is well and truly done on April 8. But there could be half a billion XP computers still out there humming away, depending on how you count them and what assumptions you're willing to make. Getting an accurate count is exceptionally difficult, because many of them aren't connected to the Internet via a browser. Consequently, they don't appear in independent Internet stats. But whatever the precise number, a huge number of PCs are officially *end of life* in just over two months.

Contrary to what some XP users believe, "end of life" *doesn't* mean that XP computers will stop working, that XP can no longer be installed, or that existing security patches will be pulled from Windows Update. It means that officially, on April 8, Microsoft will no longer support XP — there will be no more updates for the OS.

Regular Windows Secrets readers have seen numerous stories on living with XP for the long term. See, for example:

Preparing Windows XP for the long haul – Aug. 12, 2010, [Top Story](#)

Building your own XP Service Pack 4 – Dec. 1, 2011, [Top Story](#)

PC security after XP's official end of life – Sept. 19, 2013, [LangaList Plus](#)

Securing XP PCs after Microsoft drops support – Dec. 19, 2013, [Top Story](#)

If you've been reading this newsletter, you know that XP's end is coming. But you probably didn't know that Microsoft's moved the goalposts — repeatedly. What *end of life* means, precisely, has been redefined by Microsoft at least three times in the past couple of months. And there's a strong possibility that the definition will change again before April — to the confusion of most XP users.

So what *did* end of life mean? Back in the good old days — say, three months ago — Microsoft's description of the April deadline suggested nothing less than the complete end of any XP support: no tech-support help, no new enhancements, and no security updates. (That, as it turns out, isn't quite correct. As I'll discuss below, Microsoft will no longer give away updates — but businesses with corporate-licensing plans can *pay* for them after April 8.)

Then, in early January, Microsoft altered its official XP obituary [page](#), adding that "Microsoft will also stop providing Microsoft Security Essentials for download on Windows XP." That certainly sounds threatening!

Backpedaling a Bit on a Hardline Stance

To date, I've not seen an official clarification of what "stop providing Microsoft Security Essentials" precisely means. For example, it could mean that you can't download MSE using an XP-based browser. If so, it's silly — you just download MSE on a different machine and install on XP. Or perhaps MSE's installer might simply block XP. In that case, what happens if you reinstall XP? (Microsoft will require XP activation, even after EOL.) You can't reinstall MSE, either? Even Microsoft wouldn't be that callous — I hope.

To add to the confusion, in mid-January Microsoft's Malware Protection Center announced in a TechNet [blog](#) that it would continue to provide updates to MSE for XP machines for another 15 months. The blog states, "To help organizations complete their migrations, Microsoft will continue to provide updates to our anti-malware signatures and engine for Windows XP users through July 14, 2015."

That's certainly a customer-friendly development — although I'm still scratching my head about blocking MSE downloads on XP. It's possible that somebody at the Malware Protection Center ran a simulation of the fallout from some nasty virus compromising half a billion XP machines after April 8. That could cause something of a hiccup on the Internet!

That MPC statement is noteworthy because Microsoft will not only update MSE signatures but the MSE engine, too. Bravo.

In a more recent development, Computerworld broke the news in a Jan. 26 [story](#) that Microsoft will update the Malicious Software Removal Tool (MSRT) for Windows XP through July 14, 2015. MSRT isn't a first-line-of-defense AV tool, but it's effective at removing existing infections. It's also delivered via Microsoft Update, so most XP machines will get it.

Some Safe Assumptions, Some Wild Speculations

If Microsoft's backpedaling were limited to just those two AV products, I'd not be very impressed. Many third-party vendors offer better anti-malware protection and have publicly stated that they'll continue support for XP. But I am impressed by Microsoft's willingness to soften its XP end-of-life stance. The company has nothing to gain and everything to lose if it completely alienates its millions of XP users.

Many believe XP deserves to die because it's been around for 12 years. I take issue with that. XP was first released in October 2001, so technically it's 12 years old. But it was rewritten for Service Pack 2, which appeared in August 2004. And Microsoft sold XP through its System Builders program until Jan. 31, 2009. That's just five years ago.

During the unfortunate Vista era, many PC buyers went out of their way to get XP. So as far as I'm concerned, XP hit the bit bucket only when Windows 7 shipped in July 2009. That makes XP, by my admittedly jaundiced reckoning, a sprightly four and a half years old!

That said, there's no doubt that those running XP are living on borrowed time. Windows 7 and 8x offer enhanced security and better compatibility with modern software and peripherals. Most XP users should be planning to replace XP.

But it's also a bit disingenuous to effectively **force** Windows users to buy Win7 or Win8 — then force them to line Microsoft's coffers once again a few years later when those operating systems are made obsolete. Here's a parting tip: If you work for a company that has a Microsoft volume license and a suitable Windows retirement contract, you can buy "Custom Support" for XP, as reported in a Computerworld [story](#). That service costs U.S. \$200 per PC per year and includes updates to XP itself. Rather than cut off individual XP users, I think Microsoft should offer a personal "Custom Support" option for, say, \$20 or \$30 a year. That would do a lot of good for the millions of XP users — and earn Microsoft some much-needed customer loyalty.

Hey! I can always hope.

From: The Desk of Jim McGorry
Excerpts taken from the Windows Secrets Periodical

SORTING OUT THE REVOLUTION IN PC BACKUPS: PART 1

Over the past few years, backup technology has improved so much that you're virtually guaranteed you'll never lose important files or other data.

But with so many good options available, it can be difficult to settle on the backup method — or methods — exactly right for you.

Today's mainstream backup options range from Windows' built-in tools and an internal hard drive to automated applications that archive files to the cloud. In between are old-school backups on optical discs and new-school network-attached drives that let you access your data from anywhere — locally ***and over the Web.***

Each backup option brings its own particular mix of strengths and weaknesses. In this two-part series, I'll sort out the differences — in both use and speed.

In Part 1, I give an overview of the five leading types of backup technology available today for Windows users. These capsule summaries should help you quickly sort through the benefits and limitations of each option.

In an upcoming issue, Part 2 will provide additional details — plus a Windows Secrets exclusive: real-world timing tests that show how long it takes to back up file sets of various sizes using each of the five backup types. Combined, Parts 1 and 2 will help you decide the type of backup technology that best fits your needs.

Five Ways to Archive Windows and Your Data

Personal-computer backups are best grouped by where the backup files are stored. The five mainstream options I'll review are these:

Internal drives

Optical discs (typically DVDs and CDs)

USB-connected external drives **Networked drives** (such as in another PC or a standalone, network-attached storage device)

Cloud-based data-storage services

There are, of course, variations of each type. For example, networked drives can be accessed either via Wi-Fi or by hard-wired Ethernet. Wi-Fi can be more convenient, especially in the home, but a wired connection is typically about 10 times faster than wireless, so there's a huge speed difference.

Some other forms of backup don't warrant coverage here. For example, USB flash drives might be fine for backing up selected files and folders, but most commonly used flash drives are too small to hold a complete, whole-PC backup.

It might be hard to believe, but tape drives and floppies — about as old school as it gets — are still in use. But they're far, far out of the mainstream and are typically not up to the needs of modern personal computers. Optical networks and gigabit Wi-Fi will become more widespread in coming years, but they're still minor players, today.

So, now that we have the context of this backup discussion, here are my capsule summaries of the five commonly used options.

Back Up to a Secondary, Internal Hard Drive

In this setup, your system files and data reside on the primary (typically, C:) drive; your backups live on a second, physically-separate drive inside the PC.

Pro: Fast, Easy, and Inexpensive.

A secondary internal drive offers the fastest form of backup — and restoration. The backup process is easy to set up; all standard backup programs can read and write to a secondary hard drive. A second internal disk drive is relatively cheap. A 1TB desktop-class drive costs as little as U.S. \$60.

Con: Low Data Security.

Secondary drives share the same physical, electrical, and operating system environment as the primary drive, so anything that compromises the primary drive (malware, mechanical or electrical malfunction, fire, flood, theft, and so on) might also compromise the secondary drive.

Storing backups on a secondary internal drive is a *better-than-nothing* approach.

Back Up to Optical Discs (DVDs and CDs)

Most desktops and laptops still have optical drives. PCs without an optical drive can be connected to an external DVD/CD drive, but there are few viable reasons to bother.

Pro: Can be highly secure.

Once written, optical discs are immune to new malware infections. Optical discs can also be very long lived. If you store optical-disc backups away from the main PC, in a climate-controlled location that's fire- and theft-proof, your backups can last for decades — safe from just about all the misfortunes that can affect a PC and its data. (For more on accessing files over decades, see the Feb. 21, 2013, Best Practices [story](#) "Preserving files for the generations.")

Con: Slow, Labor Intensive, Expensive, Bulky, and Requires Careful Handling.

Backing up files to optical discs is an inherently slow process, often requiring disc changes, labeling, and careful storage, which makes automated backups effectively impossible. A single full-system backup could span large numbers of discs, adding to the cost and complicating the task of storage and eventual disposal.

Without good climate control (i.e., constantly cool, dark, dry storage), optical discs can degrade fairly quickly (see these National Institute of Standards and Technology [publications](#)). Also, to protect them from unintended destruction, such as fire or theft, the discs need to be stored in a fire-proof safe or at another site.

Back Up to a USB-Connected External Drive

The explosive growth of space-consuming media such as digital music, videos, and digital photos has made one or more external drives a must-have addition for many (if not most) Windows PCs.

Pro: Easy to Use, Good Speed, and Low to Moderate Cost.

Installing an external, USB-attached drive is usually just a matter of plugging it in. It's hard to imagine a backup medium that's easier to set up.

All major Windows-based backup programs can write to USB-attached storage, and Win8's built-in **File History** can automatically use external drives for near-continuous archiving. (See the July 11, 2013, [Top Story](#), "Understanding Windows 8's File History.")

USB 3.0 drives usually give excellent high-speed data transfers; USB 2.0 drives are slower, but still acceptable for most backup needs. A good 1TB external drive currently costs about \$80 and up).

Con: Mixed Data Security.

Backups to a USB-connected external drive should be highly secure — if, after a backup is made, the drive is disconnected from the PC and stored in a safe location. But USB drives are rarely used that way, and Win8's File History requires that the drive be more or less permanently attached.

When a USB drive is left attached, it's vulnerable to many of the same events that can take down the primary drive, including malware, mechanical or electrical malfunctions, theft, and other disasters.

Back Up to a Networked Drive or Second PC

Storage sitting on the local network can make backing up multiple PCs easier. The newest network-attached drives, such as the Western Digital My Book Live (more info), also let you share media and access their contents from the Web.

Pro: Generally Easy to Set Up, Acceptable to Good Speed, Moderate Cost and Complexity, and Some Resistance to Simple Malware.

Nearly all Windows PCs have networking abilities built in, and almost all homes with PCs have networks with Wi-Fi and/or hard-wired Ethernet. So it's usually not hard to back up files over the network to an attached storage device or a second PC's hard drive. (You can, for example, put an old PC back to use as a sort of poor man's file server.)

Backup speeds over a network can be good — especially with 100Mbps Ethernet, which often yields real-world throughputs about 10 times faster than 802.11g Wi-Fi. If used properly, network backups can also be resistant to some forms of spreading malware (more in the **Con**, below).

Con: Requires Extra Steps for Good Security.

Ideally, a networked drive should be far away from the system being backed up. It should have separate physical security and be powered by a separate electrical circuit. Otherwise, the networked drive might be lost along with the backed-up (client) PC, in the event of some accident, theft, or disaster.

Networked drives are usually accessed two ways: **drive mapping** — assigning a drive letter such as **Z:** — and **Uniform Naming Convention** (UNC; [more info](#)) — assigning a network name such as **\\{name of drive or PC}**. Drive mapping is less secure because relatively simple malware on the client PC can access the mapped, networked drive as easily as a local drive. To help thwart such malware, it's better to use UNC for accessing networked drives.

Back Up to a Subscription-based Cloud Service

Cloud-storage/backup services are now extremely common. Depending on your computing needs, they can be either the primary backup system or supplementary backup.

Pro: High Security, Low to Moderate Cost, and Easy to Set Up and Use.

The primary benefit of cloud backup is **offsite** storage. Even if your PC and all local backups are lost, you'll still have copies of your files in the cloud.

Most cloud services use reasonable safeguards (password protection and encryption) to prevent unauthorized access to your stored files. But you can make your cloud storage **virtually hack-proof** through the use of free or low-cost third-party tools. (See the Dec. 12, 2013, [Top Story](#), "Pre-encryption makes cloud-based storage safer.")

Cloud-storage costs are low to moderate, depending on the size of your data sets. (Most general cloud services offer some small amount of free storage, typically 2–15GB.) Microsoft's **SkyDrive** (soon to be renamed

OneDrive; [site](#)) costs about \$0.50 per gigabyte annually, above its free 7GB. So 107GB of storage will run \$50 per year. **Google Drive** ([site](#)) gives you the first 15GB free, then charges about \$0.60 per GB per year (115GB for \$60/yr). Fees for backup-specific services such as **Mozy** ([site](#)) and **Carbonite** ([site](#)) are in the same general ballpark.

Setting up cloud-based backup is usually easy. For example, Microsoft's OneDrive/SkyDrive is built into Win8. Third-party apps such as Mozy and Carbonite install easily and offer a high degree of automation.

Con: Slow, Could Incur Significant Secondary Costs, and Depends on Middleman Services.

As you might expect, cloud backup can be extremely slow — especially when moving large numbers of files. It can take literally *days* to fully restore a PC from cloud-based backups. Moving large amounts of data via the Web also can choke your local Internet connection. Moreover, if your ISP or cloud-service provider imposes data-transfer limits, backing up your entire system to the cloud can lead to substantial surcharges. Using a cloud-based service also makes you dependent on middlemen. If your ISP or cloud-service provider goes down for any reason (technical, criminal, financial, or some other cause), you'll lose access to your cloud-stored backups.

Next Up: Real-world Timing Tests and More

Stay tuned for Part 2 of this series. In that article, you'll see how the above five major backup types compare in live timing tests using small, medium, and large file sets. You'll also receive advice on the types of backups to use for different file types (multimedia, images, documents, and so forth) and under different circumstances. Stay tuned!

From: The Desk of Jim McGorry
Excerpts taken from the Windows Secrets Periodical

GOING SMALL(ER): TRADING SPINNING DISKS FOR SSDS

Solid-state drives can give a significant boost to system performance, but at the cost of storage space.

Here's how to sort out the data on a big spinning-platter drive and fit what you can onto a smaller SSD.

Migrating down to a Smaller System Drive

Install a solid-state drive, and it's love at first boot. The minutes it took to load Windows suddenly become seconds. Everything is faster; you'll never want to go back. There is, however, a cost to that extra speed. SSDs cost far more per gigabyte than hard drives and typically come in smaller sizes. As I write this, a 120GB SSD typically goes for U.S. \$90 to \$100; a 256GB drive will set you back about \$200. A 512GB SSD from one of the well-known drive manufacturers could cost you \$400. By comparison, you can buy a traditional 1TB hard drive for just \$70.

So unless you're rolling in cash or need only a small amount of storage space, trading your primary spinning-disk drive for an SSD requires making some hard decisions about which files you'll keep on the new drive. Moreover, the simple task of cloning your old drive to a new one probably won't work — you can't clone 500GB worth of files onto a 120GB drive.

Bottom line: Migrating to an SSD will probably be more complex than you might at first assume. Along with those hard decisions, the process of transferring Windows and data to a new SSD will require a few more steps. I'll discuss those steps below.

Using an SSD on Desktops vs. Laptops

In most cases, adding an SSD to a desktop system is considerably easier than upgrading a notebook. Technically speaking, the issue isn't really desktop versus laptop; it's whether the system has room for two internal drives. But practically speaking, the vast majority of desktop PCs have extra drive bays — and most laptops don't. With multiple drive bays, you can easily keep all files within the computer. Whatever doesn't fit on the SSD stays on the old hard drive — which remains in the computer. The performance boost will be almost as good as having everything on an SSD.

With most laptops, the files that won't fit on the new SSD will have to be kept on an external drive. This can be clumsy, especially when you're on the road. And if your laptop doesn't have a USB 3.0 port, you're going to suffer a major performance hit when you access big files or large batches of files from the external (non-SSD) drive.

If you're upgrading a laptop, keep in mind that the new SSD needs to fit completely within the hard-drive enclosure. Check the SSD retailer's return policies so that you're not stuck with the new drive if it doesn't fit. Also, check out Fred Langa's July 5, 2012, Top Story, "Some ugliness installing an after-market SSD."

What Goes to the SSD; What Stays Behind

Assuming you *can't* fit all your data on the new SSD, what should you transfer and what should you leave behind on the old drive?

That decision could be based on several factors such as your work habits; the ease of separating current projects from older ones; and/or the size, number, and type of files. Documents associated with current projects, files you open regularly, recent photos, and possibly a few favorite songs are all good candidates for the SSD. Files rarely accessed should stay on the original hard-disk drive.

My work habits made this file reorganization fairly easy. I keep my current and recent projects within the Dropbox folder in My Documents. I also keep recent and favorite photos in Dropbox. It's the only folder I really need to have with me at all times. Any file stored elsewhere is one I rarely need to access.

Once you've decided how to divide up your files, it's time to get to work on your SSD upgrade.

The Basics of Transferring Files to a New Drive

So you've got a brand-new SSD; what else do you need? A screwdriver is probably the only physical tool you'll need. If you've got a desktop, you might need an adapter bracket to fit the drive into a full-sized bay. (If you're lucky, an adapter came packaged with the SSD.)

On laptops, you'll need a SATA-to-USB enclosure (or docking station or connector kit) to set up the new SSD as a temporary external drive. (With an enclosure, you can turn the old hard-disk drive into a more or less permanent external drive.) You can buy an enclosure for as little as \$10 to \$20. Whether enclosure or connector kit, be sure it supports USB 3.0. You might also need an external drive — but we'll get to that later.

Your first step before anything gets transferred, of course, will be to make a full image backup of your current system. (It should go without saying, but I'm obligated to say it anyway.)

With that done, you're ready to connect the SSD to your PC. On a desktop, install the SSD into a spare drive bay and connect the data and power cables. If you have a laptop, connect the new drive with your SATA-to-USB enclosure. (Use the laptop's USB 3.0 port if it has one.)

Next, if the SSD came with cloning software, give it a try. But keep your expectations in check — the app included with my **Samsung SSD 840 EVO** ([more info](#)) was, for the most part, useless. It would not let me select specific folders — just file types, and only a limited number of those. If the SSD's bundled software proves inadequate to the task, try one or more of the following options.

The Free Method (with a Spare External Drive)

This process requires paring down your old hard drive so that what remains will fit on the new SSD. To do that, you'll need an external hard drive with enough spare room to store all files removed from the primary drive. Plug in the drive

and create folders with names such as Extra Documents, Extra Music, Extra Pictures, Extra Video, etc.

Now open your Windows library and move the extra files and folders (see Figure 1) to the folders you created on the external drive. Don't move the library folders themselves (e.g., **C:\Users\{user name}\My Documents**, **C:\Users\{user name}\My Pictures**, and so on) — just move their contents (or, more precisely, the parts of their contents you don't want on the SSD).

On my system, for example, I would open My Documents, press **Ctrl + A** to select everything in the folder, then hold down Ctrl and click the Dropbox folder to deselect it. Next, I would drag the highlighted folders and files to the external drive's Extra Documents folder. (You can also use **Ctrl + X** and **Ctrl + V** on smaller batches of files if you have difficulty with drag-and-drop.) Repeat the process with the other libraries.

Once the total data content on the primary drive is small enough, any decent cloning program should let you migrate Windows, apps, and data to the SSD. I recommend EaseUS Todo Backup Free ([more info](#)), which clones as well as backs up. (At this point, to be completely safe, you might want to make an image backup of the slimmed-down primary drive.)

Once the program is up, select Clone/Disk Clone. Select your old HDD as the source and the SSD as the target, as shown in Figure 2. At the bottom of the drive-selection window, check **Optimize for SSD**, but leave **Sector by sector clone** unchecked. If you click Next and get an error message, you need to move more files off the HDD and try again.



Figure 2. EaseUS Todo Backup Free is an easy-to-use cloning tool — and it's completely free

Once the SSD becomes the system boot drive (more on that below), you can move the extra files back to the old hard drive.

A Faster, Simpler, and Relatively Cheap Solution

With a smart drive-cloning program, you shouldn't have to bother with moving your files to an external backup drive. I know of only one program adept enough to do this properly — Paragon Migrate OS to SSD (\$20; [more info](#)).

The program's wizard walks you through the steps. The really impressive options are found on the **Change copy options** page. There, you can select specific files and folders to transfer— or not to transfer.

NOTE: Paragon Migrate OS to SSD isn't perfect. When I booted the newly cloned SSD for the first time, Windows Explorer failed to launch, and Windows put up a "Server execution failed" error. It Windows was looking for the default library folders in now nonexistent locations. Fortunately, the fix was easy — as I'll explain below. I can't say whether this is a common problem.

Setting Up the SSD as Your New Primary Drive

With cloning over, it's time to make the SSD your boot drive.

On a desktop, launch BIOS setup and change the boot order so that the SSD is higher on the list than the old HDD. I won't tell you explicitly how to make the change because it varies with the brand and version of BIOS. If you need a refresher, the PC's manual should have instructions.

With laptops, you're going to have to perform a hard-drive transplant. Remove the old drive from the laptop and replace it with the SSD. Then put the old drive into the external enclosure that formerly housed the SSD. Assuming that goes well, the SSD should boot on powerup, and the old drive — with your excess files — will be available on the external drive.

Once you're booted from the SSD (and recovered from the speed rush), make sure that your libraries are where they belong. Try opening Windows Explorer. If it opens, follow the instructions below. On the other hand, if you get the aforementioned "Server execution failed" error, open Notepad, press **Ctrl + S**, and follow those steps *inside Notepad's Save dialog box*.

Click Libraries in the left panel. Right-click Documents and select Properties. The Documents folder on the SSD (which should be **C:**) should have a checkmark next to it.

If the new **C:** drive isn't listed, click **Include a folder** and add it to the list. If it doesn't have the checkmark, select that folder and click **Set save location** (which basically means "Make it the library's default location").

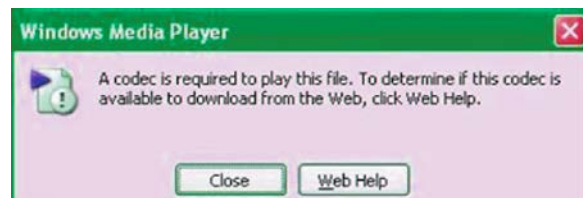
You might want to add your old Documents folder — now on the old hard drive — to the list. But don't make it the checked "Save location" folder (the default Documents folder). You can add a folder on an external drive to a library, but you should never make it the default location.

Repeat with all of your libraries. For the time being, you can keep your old hard drive as your secondary drive — either internal or external. You might one day want to remove Windows from it or even reformat it. But you can save that chore for another day.

Weekly Download Section from Jim McGorry

Can't Play A File? VLC Player Saves The Day

Have an audio or video file that you can't seem to open on your computer? Let me tell you about a great, free program that can make your life a whole lot easier. VLC Player is the answer to your codec error problems. What's a codec you might ask. My flip answer is that codecs are the devil, but the more technically correct answer is that a codec is a device or program that compresses data for faster transmission and then decompresses the data. You'll see a codec error when the programs on your computer don't recognize the program that compressed the data in the file you're trying to open.



I worked for many, many years in television and codec errors were the bane of our existence. A commercial made on a particular editing system would refuse to open on another one. Sometimes a file would refuse to open on the same system running a different version of software. Where it really caused problem was when we tried to open surveillance video provided to us by various law enforcement agencies. Every single one of them used a different format. Good luck finding America's most wanted when you can't open the video. Thankfully, a very wise engineer introduced me to VLP. It's free and I've yet to find anything it won't open. VLC Play was developed by VideoLAN organization, a non-profit the promotes free, open-source multimedia solutions. You can choose to donate if you wish, but it's not required.

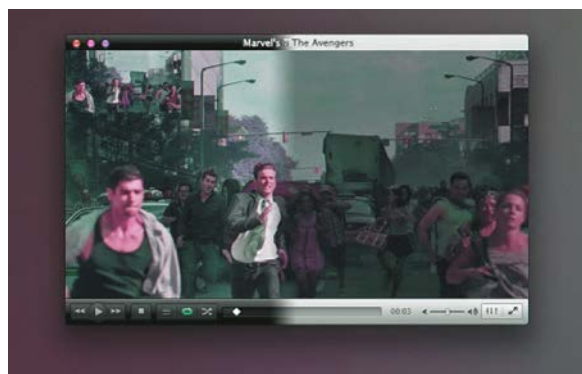


Take a look at the video formats it supports:

	MP4	OGG	FLV
MPEG-1/2	✓	✓	✓
DIVX (1/2/3)	✓	✓	✓
MPEG-4 ASP, DivX 4/5/6, XviD, 3ivX D4	✓	✓	✓
H.261	✓	✓	✓
H.263 / H.263i	✓	✓	✓
H.264 / MPEG-4 AVC	✓	✓	✓
Cinepak	✓	✓	✓
Theora	✓	✓	✓
Dirac / VC-2	✓	✓	✓
MJPEG (A/B)	✓	✓	✓
WMV 1/2	✓	✓	✓
WMV 3 / WMV-9 / VC-1	✓	✓	✓
Sorenson 1/3 (Quicktime)	✓	✓	✓
DV (Digital Video)	✓	✓	✓
On2 VP3/VP5/VP6	✓	✓	✓
Indeo Video v3 (IV32)	✓	✓	✓
Indeo Video 4/5 (IV41, IV51)	✗	✗	✗
Real Video 1/2	✓	✓	✓
Real Video 3/4	✓	✓	✓

And the audio formats:

Whether you're using MAC...



Windows Vista, Windows 7 or Windows 8... (This is especially great for Windows 8, since it doesn't come with a built-in DVD player)



Or Linux. This is a great free, tool.



To learn more about VLC and to download it for free: <http://www.videolan.org/>