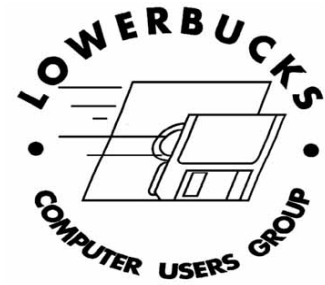


ASCIIriber

THE JOURNAL OF THE LOWER BUCKS COMPUTER USERS GROUP

Volume 34 • Issue 5 May, 2015



Lightroom 6

Adobe has just launched Lightroom 6. As with all new releases, additional features have been added.

The three big ones are:

- Merging HDR images (high dynamic range) photos within Lightroom
- Creating panoramas from multiple images within Lightroom
- Facial recognition

Another change is that Lightroom is now available to the user in two different venues: as a standalone program and in the cloud.

The standalone version of Lightroom costs \$149. Upgrade prices haven't been released but will probably be between \$79 and \$99. Student and teacher editions should be about the same.

The other option is the CC (Creative Cloud) Photography Plan. This costs \$9.99 a month and gives you access to both Lightroom and Photoshop. You also get a mobile version of Lightroom, something not included in the standalone version.

There are additional pluses and minuses to each plan. We'll talk about them at the meeting.

See you on Sunday

NEXT MEETING:

SUNDAY, May 3, 2 P.M.

Clean up your PC or wipe and install Linux – the option is your and the instructions are here, thanks to Jim McGorry

- Protect yourself from ransomware
- Free Duplicate Cleaner Part 1
- Free Duplicate Cleaner Part 1
- Go to the library with your PC
- Installing Linux Ubuntu
- Metro becomes Windows
- Revive an ancient PC with Puppy Linux – Part 1
- Revive an ancient PC with Puppy Linux – Part 2
- Safely Test File and Image Backups

From: The Desk of Jim McGorry

Excerpts taken from the Windows Secrets Periodical

HOW TO DEFEND YOURSELF FROM RANSOMWARE

Despite the CryptoLocker headlines, ransomware is still a growing threat to both individual PC users and small-to-medium businesses.

Though our malware defenses have improved, ransomware authors are finding new ways to infect our systems. Fortunately, we have options and solutions.

The evolving forms of ransomware

It's a computer user's worst nightmare. You boot your PC, and a big warning box pops up on your screen. No, it's not a Windows error; the message states that all your files have been encrypted and you'll have to pay a ransom to get the key.

The first strain of this pernicious form of malware/ransomware was CryptoLocker. It was a profitable scheme — until anti-malware apps adapted to this new threat. But as with any successful infection, CryptoLocker soon mutated into new variations such as CryptoWall and TorrentLocker. Whatever they're called, all these strains of malware have a common thread: they don't destroy data but simply lock it up until you pay the ransom. Even when the infection is removed, the data remains encrypted. And in some cases, even backup files are made unusable — unless you buy the key.

Most ransomware infections arrive via email attachments or phishing attacks. They can even be hidden in cloud-based file-sharing sites such as Box, Dropbox and ShareFile. They can be .exe files, ZIP files, or fake PDF files that are in fact executables used to install malicious code.

Ransomware seems to be especially adept at evading anti-malware tools. Its encryption engine is similar to those we regularly use on our PCs, and its pattern or signature can change rapidly. A recent US-CERT [notice](#) describes a specific type of malicious code used to download ransomware: "AAEH is a polymorphic downloader with more than two million unique samples. Once installed, it morphs every few hours and rapidly spreads across the network. AAEH has been used to download other malware families, such as Zeus, CryptoLocker, ZeroAccess, and Cutwail."

That adaptability makes keeping anti-malware detection current a real challenge.

Hackers are constantly learning new ways to attack us. For example, they initially targeted only the local drives. Then they went after any network-mapped drives with an assigned drive letter (e.g., **F:** or **I:**). Now, any network location that a workstation can access is vulnerable.

Again, if you don't have a clean backup, you'll have to pay the ransom to get access to your data. The going rate is typically \$300 or more in *bitcoins*, purchased from a reputable vendor such as [coinbase.com](#).

If you're lucky enough (relatively speaking) to be infected by one of the early versions of CryptoLocker, you *might* be able to recover your files by using the FireEye/Fox-IT [site decryptcryptolocker.com](#). To use the site, you submit an encrypted file — which is then matched against a recovered CryptoLocker encryption-key database. (A copy of the database was obtained by Operation Tovar — [more info](#).)

The encryption process uses two types of keys. The public key is used to encrypt files; the private key handles decryption and is held only by the data's owner. A CryptoLocker attacker uses the public key to lock your files. Because the thieves hold the private key, they effectively own the files. You pay ransom to have your data unlocked — you might or might not get the actual key. Again, because the attackers use standard encryption techniques, the encryption process usually goes undetected by anti-malware programs.

Keeping up on the latest ransomware variants

One of the best resources for new information on ransomware is the CryptoLocker/ransomware [page](#) at [bleepingcomputer.com](#) (so named for the frustration one gets from using computers). As noted on that page, CryptoLocker first appeared in September 2013, targeting XP, Vista, Win7, and Win8 systems. The ransom demands started at \$100 to \$300; if you didn't pay the ransom within four days, the encryption key would be deleted and you'd have no way to recover the files. Fortunately, the original CryptoLocker delivery system is now disabled.

Unfortunately, there are new variations of ransomware that are not easily defeated. For example, [bleepingcomputer.com](#) [notes](#) that nothing can save you from *CryptoWall* short of paying the ransom. Another variant — CoinVault — is fairly

new. A Kaspersky Securelist [page](#) describes the difficulty of even analyzing this ransomware. But the company claims its software can now detect this type of malware, and it has set up another [page](#) that might help recover CoinVault-encrypted files.

Keeping ransomware off your home computers

There are several techniques and tools that can help prevent ransomware infections. For example, FoolishIT.com's **CryptoPrevent** ([more info](#)) defeats the original CryptoLocker infection by blocking temporary file locations used by the ransomware.

To protect yourself from newer "crypto" infections, ensure that whatever email service you use has filtering enabled to remove malicious attachments. Or forward your mail through Gmail, which generally does a good job of blocking suspect attachments. I also recommend using OpenDNS ([site](#)) to block known malicious websites.

Most important, be sure to have a local, recent, full backup of your important data. (Again, files archived to cloud-based storage can become infected.) Be sure that your backup system (such as Win7's **Backup and Restore**) hides your external, USB backup drive — i.e., it doesn't show up in Windows Explorer and so ransomware should not be able to access it. (Windows 8 doesn't hide dedicated USB backup drives.)

One early recovery solution was to use Windows' shadow-file copies. But the latest ransomware now disables and/or deletes those files. If you use a cloud-storage service to back up your data, be sure that **versioning** is turned on. If ransomware encrypts your local files, the synched version in the cloud might also be encrypted. But you should still have access to the previous versions of the files. The best solution is both cloud and local backups, rotating between two or more local backup devices. (Never connect both backup drives at the same time.)

Keeping your anti-malware up to date is important, but as already noted, ransomware is often adept at dodging security software.

On the other hand, **application whitelisting**, in which only known applications are authorized to run on your system, can be quite effective at blocking "crypto" malware. But here's the rub: it's not easy finding an app-whitelisting solution for home PCs. Microsoft provides it only on enterprise versions of Windows — and that currently includes Windows 10's AppLocker. (Enterprise versions of Windows are available only via Microsoft's volume licensing. You can try the trick ([more info](#)) of buying one copy of corporate Windows plus four of the cheapest items on Microsoft's sales listing, but even then AppLocker [[more info](#)] isn't easy to use.)

I'm currently testing a free application-whitelisting program — SecureAPlus ([site](#); Figure 1) — that's specifically designed for home users. I have some initial reservations about this product; I've been unable to find much third-party information about the program or its publisher. But it does let me lock down my system so that only applications I've approved will run.



Figure 1. SecureAPlus starts by scanning your system to create an initial application whitelist.

For example, SecureAPlus won't let me install an unapproved driver downloaded from a random website. When I tried to install LogMeIn, it warned that it didn't trust the installation file. But it did let me review the installation and approve the LogMeIn application (Figure 2). If I don't run across some glaring issue with this software, I'll recommend it for enhancing home-PC security.

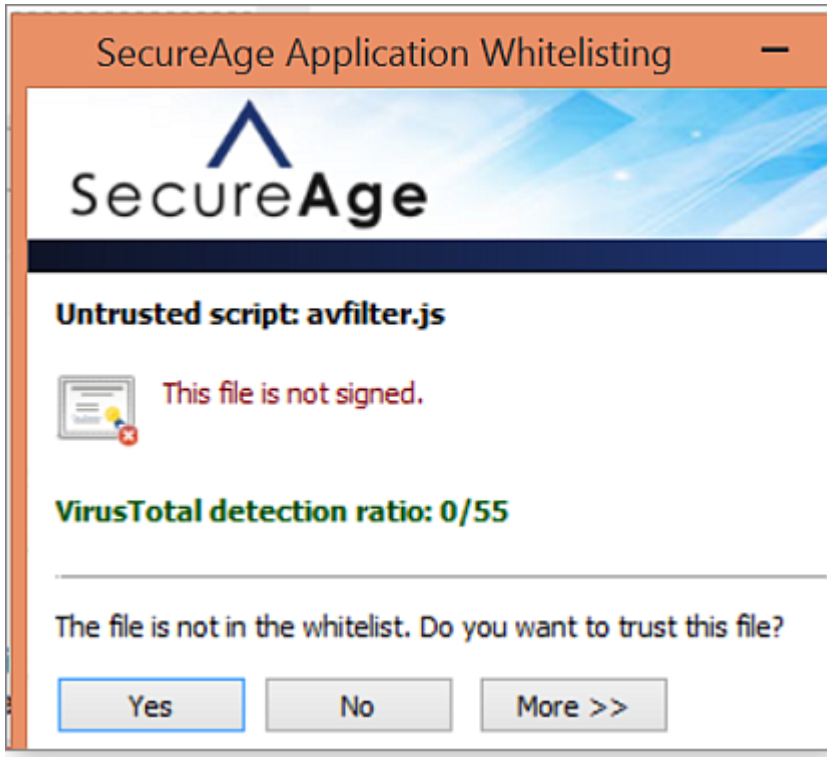


Figure 2. SecureAPlus blocks an unapproved file from running.

Anti-ransomware options for small businesses

For the most part, small businesses are similar to home users. They have limited resources and most application-whitelisting solutions are built for large enterprises. Businesses with a few PCs might benefit from a product such as SecureAPlus, but they should also review their firewall options. They need a robust system that can keep up with the threats we see on a daily basis. For example, at my office I've installed the Sophos **UTM & Next-Gen Firewall** device ([more info](#)), which scans all Web browsing and downloading.

For those comfortable with Windows' Group Policy and who have a domain controller on their network, Third Tier's Cryptolocker Prevention Kit ([site](#)) includes temp file-location blocking that works across networks. I use it in my own firm and help put together CryptoLocker-resistant group policies.

Advanced home-PC users can check out the free, software-based Sophos UTM Home Edition ([site](#)). But I have to warn you: while it will help protect a home network from malicious activity, you must learn how to build exceptions for those sites from which you download files.

If you're comfortable with VirtualBox or Hyper-V, you can download the Sophos UTM Home Edition (Figure 3) and run it on a virtual machine. Set the machine up to have two network connections, and the Sophos firewall will filter all your Internet traffic. (Or install it in an old piece of hardware that has two network cards.) This is not for the faint of heart, but there are help resources and YouTube [videos](#) if you get stuck.

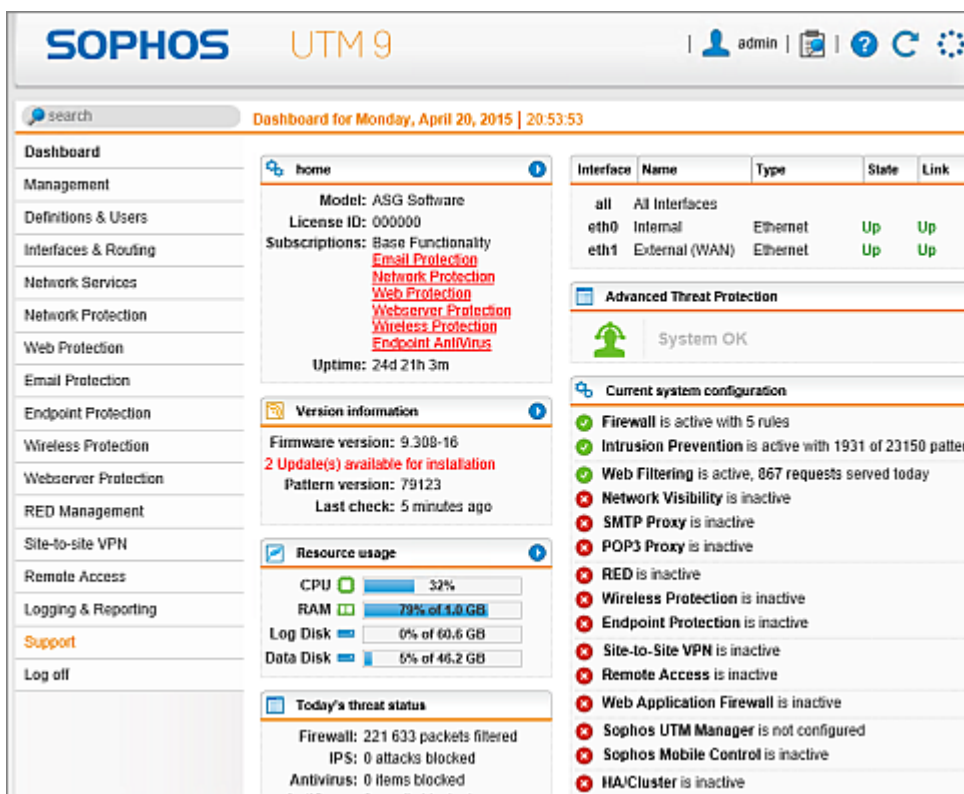


Figure 3. The SOPHOS Home Edition's management dashboard

Help from Windows' SmartScreen technology

Windows 8/8.1, and Windows 10 have Microsoft's SmartScreen Filter, which includes anti-phishing, application-reputation, and anti-malware tools ([more info](#)). (In Windows 7, the technology is built into Internet Explorer only — [info](#).) SmartScreen is far from foolproof, but it's another layer of security. Whether this technology can block ransomware remains to be seen.

Best practices: A multilayered approach

As with all security systems, there's no one-size-fits-all solution, no silver bullet for all malware threats. You need to ensure that you have multiple layers of protection. That includes tested and secured backups, email-attachment filtering, and a strong firewall. It might also include using OpenDNS and other third-party security tools.

Above all else, always be aware of the techniques used by attackers. For example, don't open attachments from unknown sources or that you were not expecting. Don't assume that any Web browser is immune to exploits, and frequently review your installed browser add-ons. Always keep Flash, Java, and Silverlight up to date — or remove them if they're not absolutely needed. Beware of random Web browsing, and keep in mind that malicious Web sites might piggyback onto news links. Visit only trusted websites on PCs containing sensitive information, and do your casual browsing on another device such as a tablet.

The attackers are getting smarter; it's important that we stay one step ahead of them. I'll be giving a ransomware presentation on May 14 at the Microsoft MVP [Virtual Conference](#). I hope to virtually see some of you there!

Weekly Download Section

from Jim McGorry

Welcome members and visitors alike to this new section I hope it will be of interest and use to you.

Each month I will try and have interesting and useful programs for you to download and try on your systems as you see fit. Some are free and some may have a nominal fee.

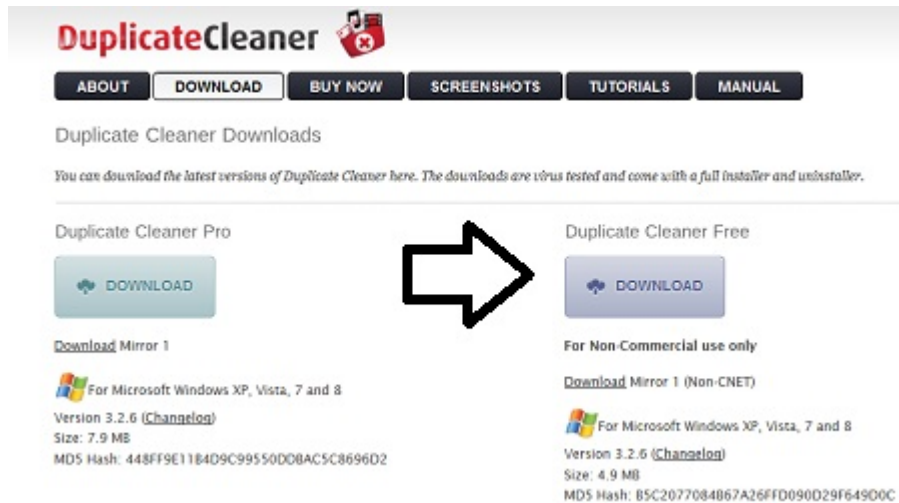
A brief write-up and link to download page will be displayed here so you can determine if you wish to get it and use it.

ALSO NOTE: Some web addresses may not be a direct link. If not, then just copy and paste the address into the "Address Location" window and hit enter.

GET RID OF DUPLICATE FILES: DOWNLOAD & INSTALL DUPLICATE CLEANER, PART 1

I've got the answer to a question we get asked a lot around here: How do I find and remove duplicate files? Try using Duplicate Cleaner. It's a free download. There is a paid version, but for most people I think the Duplicate Cleaner Free will work just fine.

Start by clicking here to go to the download link. Make sure to select Duplicate Cleaner Free and click Download.



The screenshot shows the 'Duplicate Cleaner' website. At the top, there are navigation buttons: ABOUT, DOWNLOAD, BUY NOW, SCREENSHOTS, TUTORIALS, and MANUAL. Below this, the 'Duplicate Cleaner Downloads' section is visible. It contains two columns of download options. The left column is for 'Duplicate Cleaner Pro' and the right column is for 'Duplicate Cleaner Free'. A large black arrow points from the 'Duplicate Cleaner Pro' section towards the 'Duplicate Cleaner Free' section. Each section has a 'DOWNLOAD' button and a 'Download Mirror 1' link. Below the links, there is a Windows logo icon and text indicating compatibility with Microsoft Windows XP, Vista, 7, and 8, along with version information (3.2.6), size (7.9 MB for Pro, 4.9 MB for Free), and MD5 hashes.

A wizard will walk you through the installation.

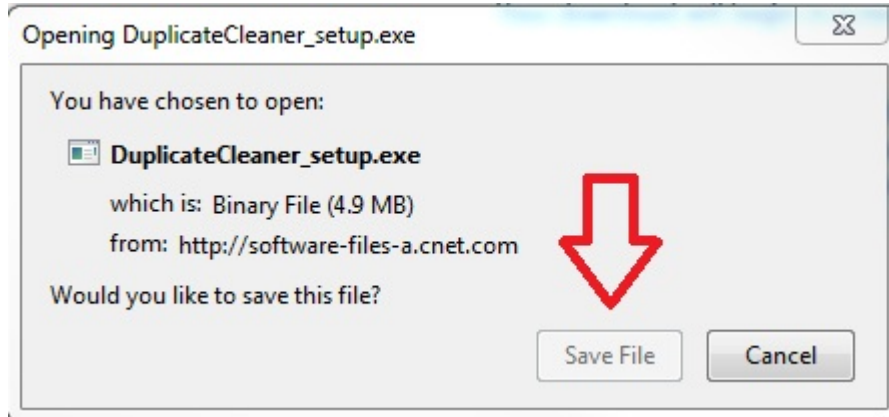


You'll be prompted to begin the Download. Make sure you click the button for Duplicate Cleaner and not the one to the right for Windows Drivers or the one below for Slimware utilities. One of the hazards of free downloads, even good

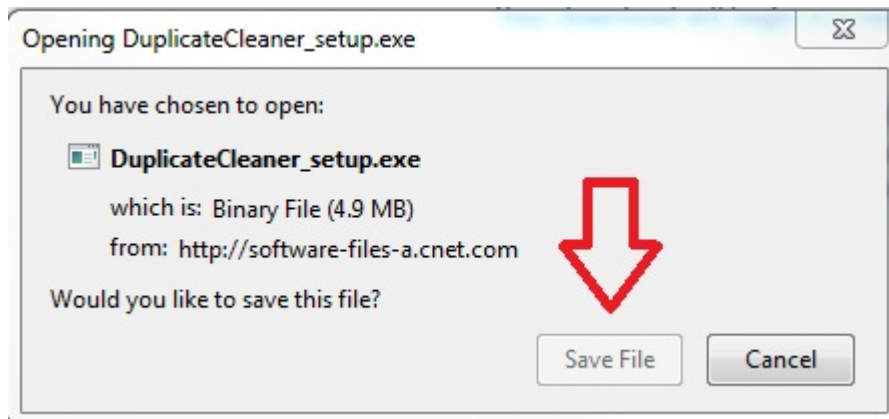
ones, is that you're often prompted to download other programs and might end up doing it accidentally if you aren't careful.



You'll be prompted to save the download. Click Save File.



Duplicate Cleaner will now be saved in your Downloads folder. Double-click to start installation.



You'll need to give the program permission to make changes to the computer and then select a language.



When installation is finished, click finish and Duplicate Cleaner will open.

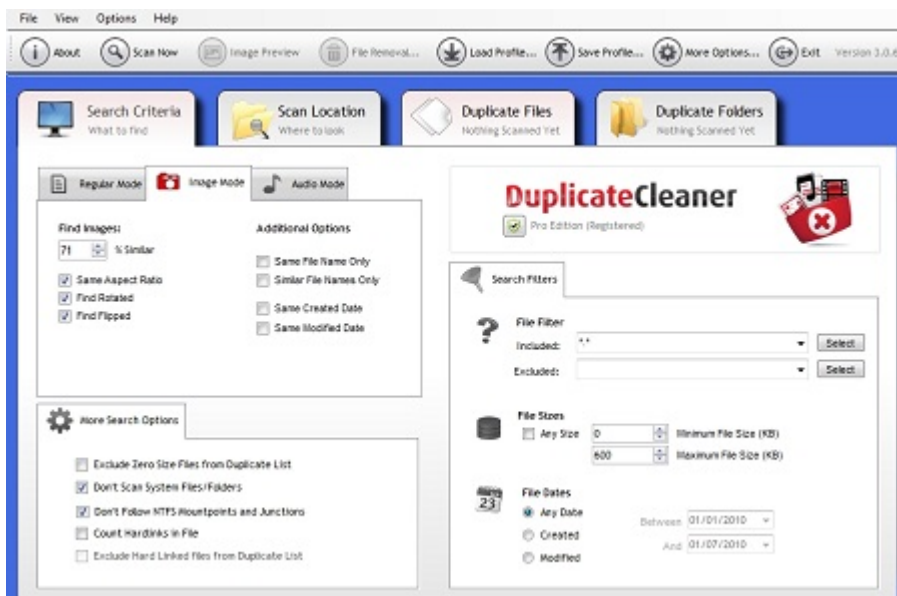


In part 2 of this article, we'll put this program to work cleaning up your computer.

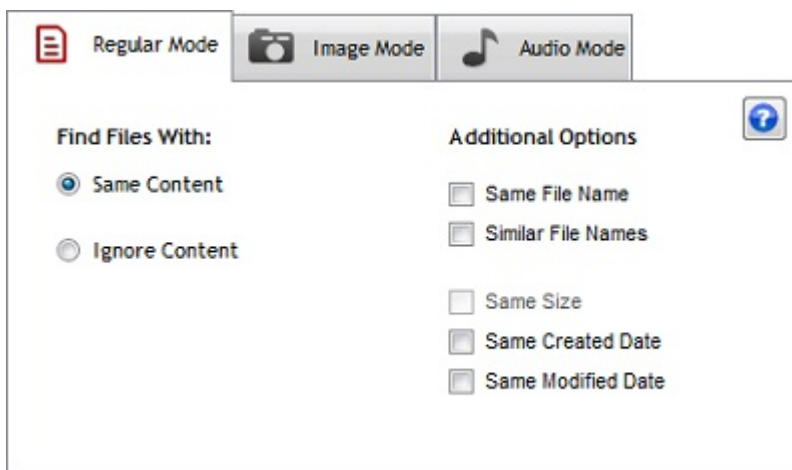
FREE DUPLICATE CLEANER, PART 2

In Part 1 of this article, I showed you how to download and install Duplicate Cleaner, a free program that helps you remove duplicate files from your computer. If you haven't checked out those instructions yet, [click here](#) to read the tip.

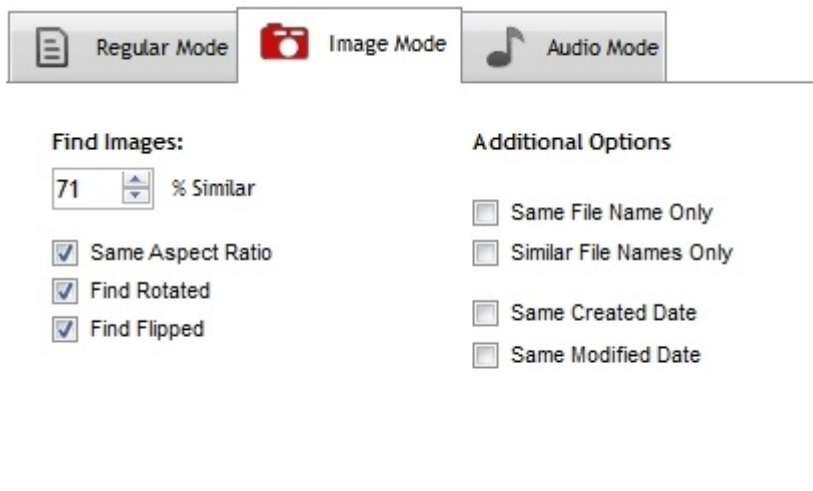
When you open the program, you can set up your search criteria for duplicate folders.



In Regular Mode, you can search for files with the same content and also add additional filters such as same or similar name or create date.



In the Image mode, you can look for images not only with the same name and create date, but also sort by aspect ratio or if they've been altered.



Under Audio mode, you can filter by Artist and Album as well as file name.

The screenshot shows the 'Audio Mode' search settings. At the top, there are three tabs: 'Regular Mode', 'Image Mode', and 'Audio Mode' (which is selected). Below the tabs, there are two main sections: 'Match Audio Tags' and 'Additional Options'. The 'Match Audio Tags' section has a radio button selected for 'Match Audio Tags' and another for 'Match Audio Data only'. Under 'Match Audio Tags', there are two columns of checkboxes: 'Same Artist' (checked), 'Similar Artist', 'Same Title' (checked), 'Similar Title', 'Same Album', and 'Similar Album'. The 'Additional Options' section has five checkboxes: 'Same File Name', 'Similar File Names', 'Same Created Date', and 'Same Modified Date'. A help icon is visible in the top right of the settings area.

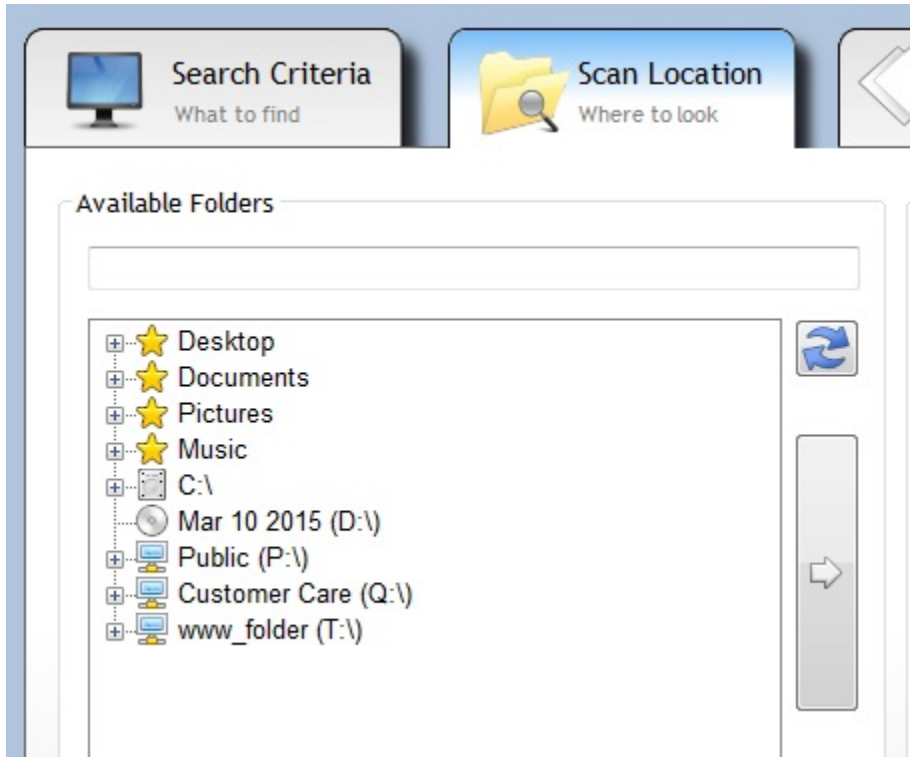
More search options are available, such as excluding zero size files and skipping system files.

The screenshot shows the 'More Search Options' settings panel, which is a sub-section of the search settings. It contains five checkboxes: 'Exclude Zero Size Files from Duplicate List' (unchecked), 'Don't Scan System Files/Folders' (checked), 'Don't Follow NTFS Mountpoints and Junctions' (checked), 'Count Hardlinks in File' (unchecked), and 'Exclude Hard Linked files from Duplicate List' (unchecked).

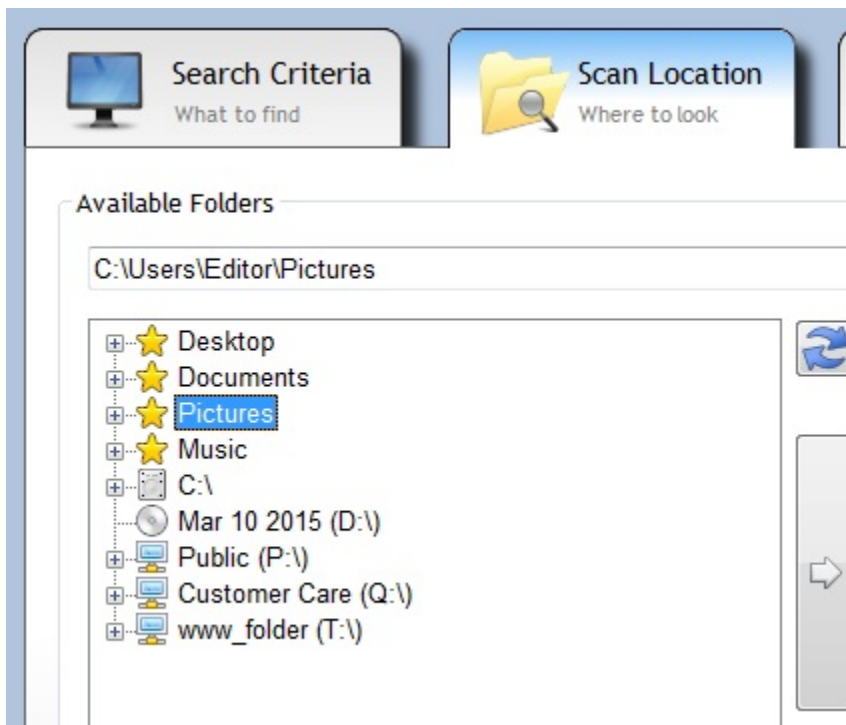
You can also set up additional search filters by name, size or dates.

The screenshot shows the 'Search Filters' settings panel. It is divided into three sections: 'File Filter', 'File Sizes', and 'File Dates'. The 'File Filter' section has a question mark icon and two dropdown menus: 'Included:' with the value '*.*' and a 'Select' button, and 'Excluded:' with an empty dropdown and a 'Select' button. The 'File Sizes' section has a disk icon and two input fields: 'Minimum File Size (KB)' with the value '0' and 'Maximum File Size (KB)' with the value '600'. The 'File Dates' section has a calendar icon and three radio buttons: 'Any Date' (selected), 'Created', and 'Modified'. Below the radio buttons, there are two date input fields: 'Between' with the value '01/01/2010' and 'And' with the value '01/07/2010'.

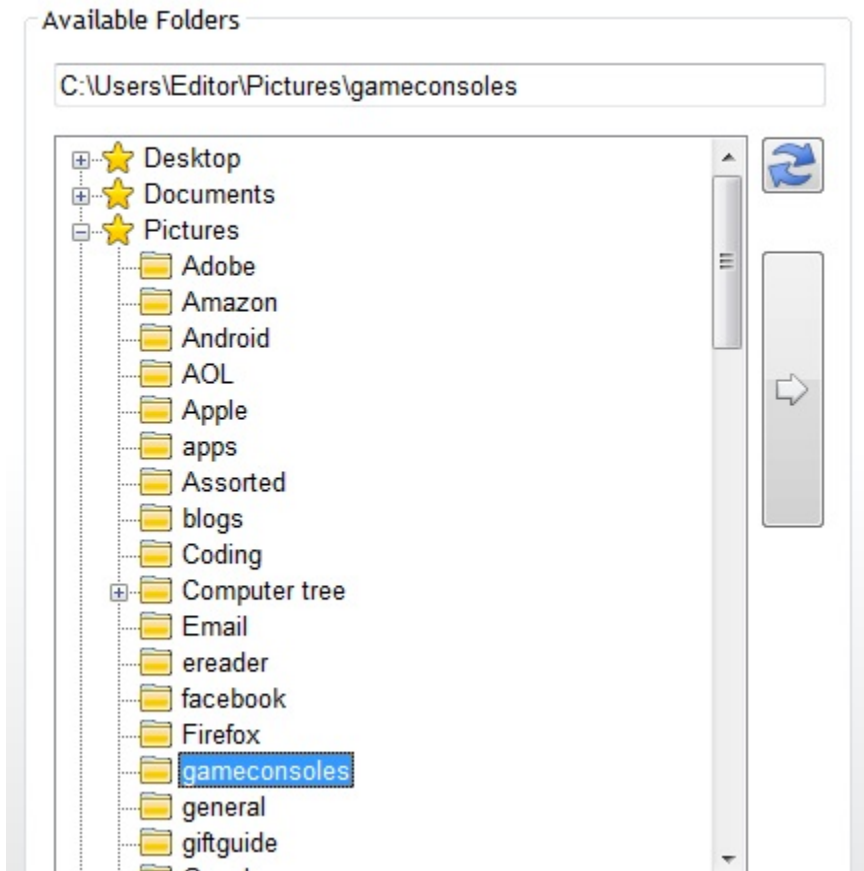
Select the locations where you want to search for files by clicking the Scan Location tab.



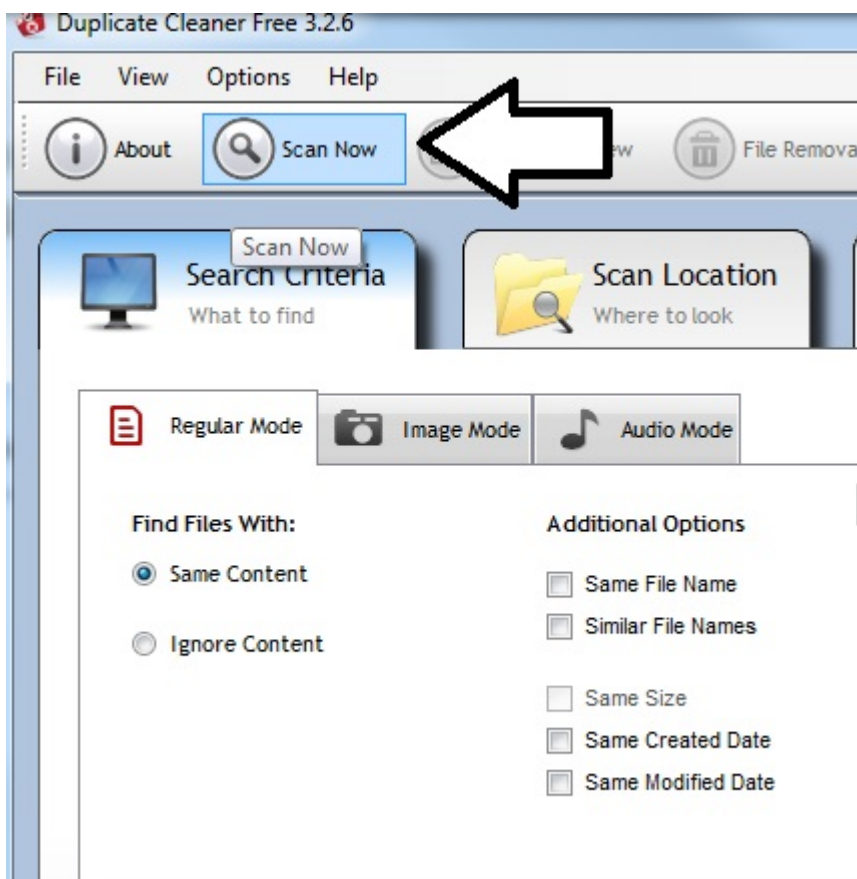
Then select the location you want to scan.



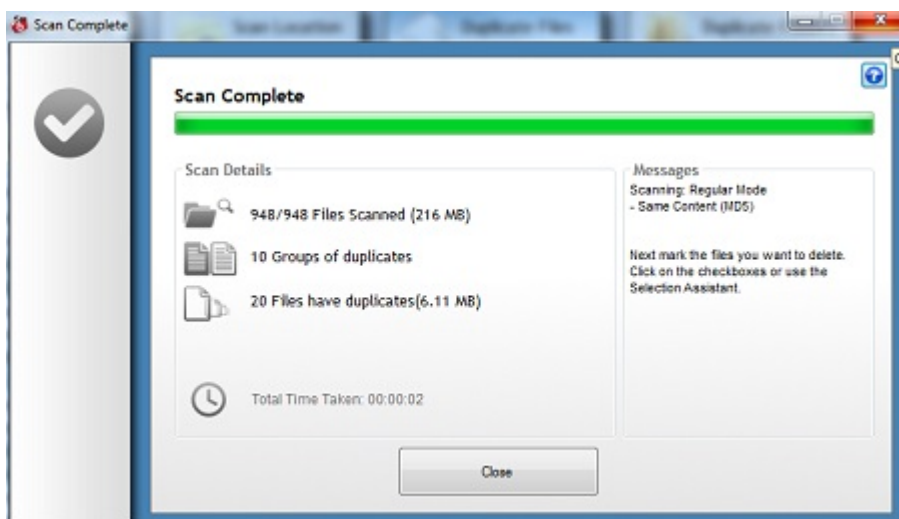
Then select the folders you'd like scanned.



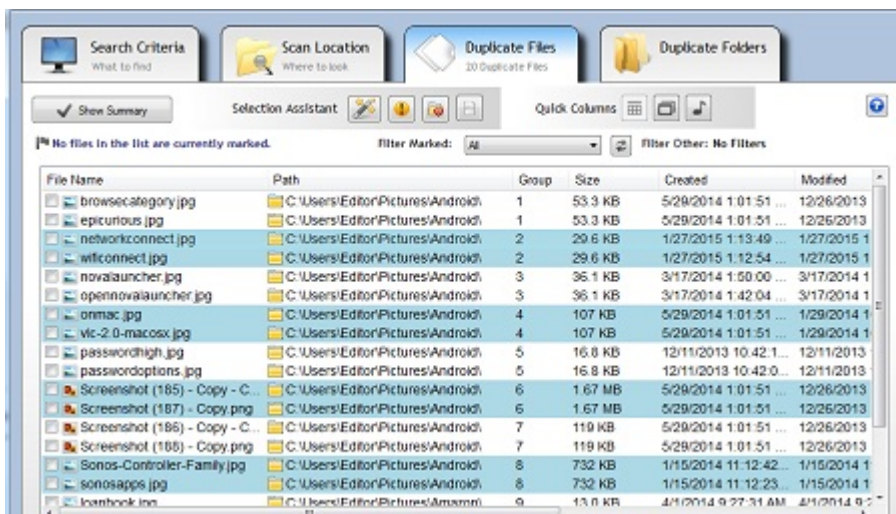
When you have your search filters and location selected, just click the magnifying glass at the top of the page to scan now.



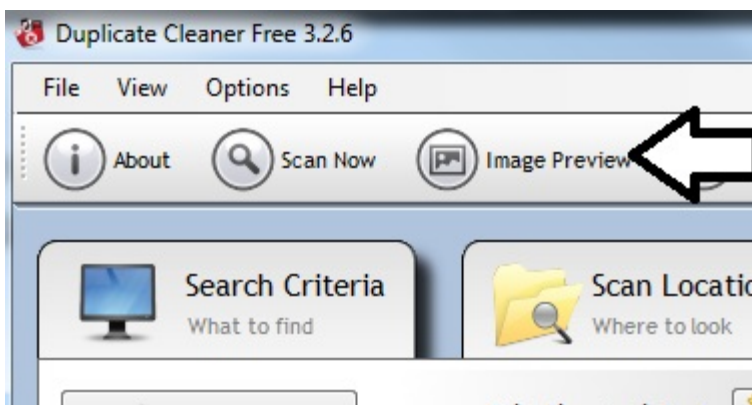
You'll be notified when the scan is finished.



You'll see a list of duplicate files.



For image files, you can click Image Preview



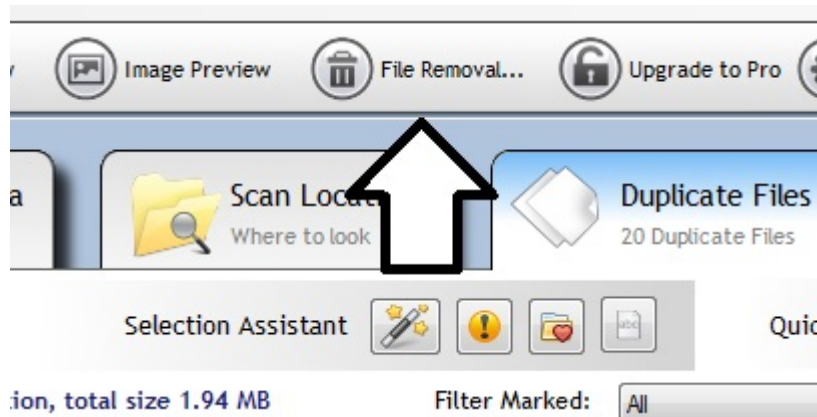
Then you'll be able to what the actual images look like.



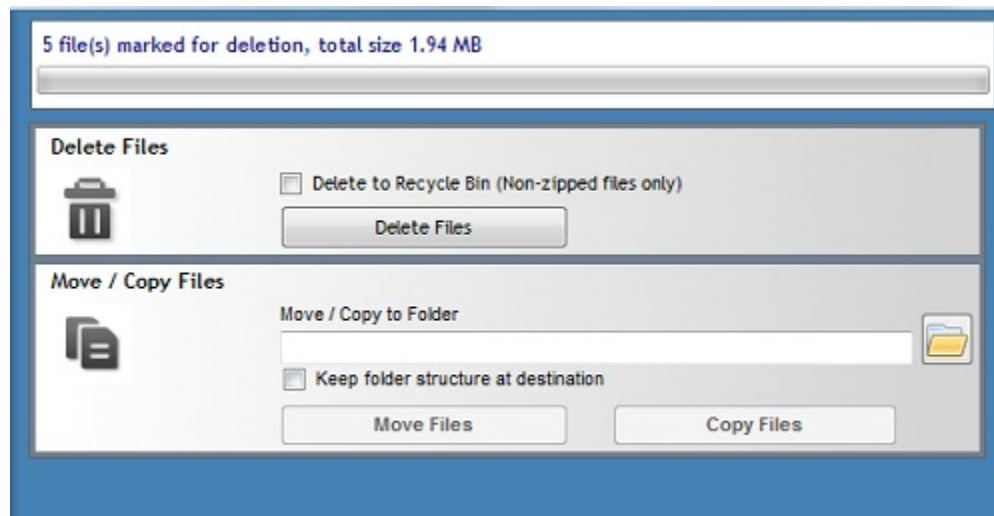
To mark a suspected duplicate file for deletion or a name change, just put a check beside it.

File Name	Path	Group	Size
<input type="checkbox"/> browsercategory.jpg	C:\Users\Editor\Pictures\Android\	1	5
<input type="checkbox"/> epicurious.jpg	C:\Users\Editor\Pictures\Android\	1	5
<input checked="" type="checkbox"/> networkconnect.jpg	C:\Users\Editor\Pictures\Android\	2	2
<input checked="" type="checkbox"/> wificonnect.jpg	C:\Users\Editor\Pictures\Android\	2	2
<input type="checkbox"/> novalauncher.jpg	C:\Users\Editor\Pictures\Android\	3	3
<input type="checkbox"/> opennovalauncher.jpg	C:\Users\Editor\Pictures\Android\	3	3
<input checked="" type="checkbox"/> onmac.jpg	C:\Users\Editor\Pictures\Android\	4	4
<input type="checkbox"/> vlc-2.0-macosx.jpg	C:\Users\Editor\Pictures\Android\	4	1
<input type="checkbox"/> passwordhigh.jpg	C:\Users\Editor\Pictures\Android\	5	1
<input type="checkbox"/> passwordoptions.jpg	C:\Users\Editor\Pictures\Android\	5	1
<input checked="" type="checkbox"/> Screenshot (185) - Copy - C...	C:\Users\Editor\Pictures\Android\	6	4
<input type="checkbox"/> Screenshot (187) - Copy.png	C:\Users\Editor\Pictures\Android\	6	1
<input checked="" type="checkbox"/> Screenshot (186) - Copy - C...	C:\Users\Editor\Pictures\Android\	7	4

Then click the File Removal icon.



You'll then have options to delete, rename or move duplicate files to other locations.



This tip should be enough to get you started, but the great thing about Duplicate Cleaner is that they have a full manual available online as well as video tutorials. You can check it out [by clicking here](#).

Weekly Download Section

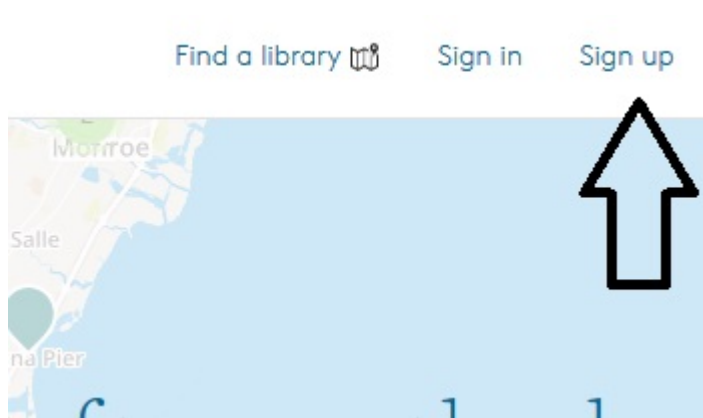
from Jim McGorry

GO TO THE LIBRARY ON YOUR PC

You don't need to buy an eReader or tablet or spend a lot of money to have access to millions of books and movies. All you need is your library card. If your local library is one of thousands that use the OverDrive app, you can go to the library right on your PC.

We've discussed the OverDrive app for phones and tablets before, but I've never give you a tour of the PC version. Start by heading over to OverDrive.com.

Then click Sign up in the upper right of the page. If you already have an OverDrive account, you can just log in.



You can sign up with Facebook or enter your name and e-mail address, then set a password.

Sign up with Facebook

or

Enter your details:

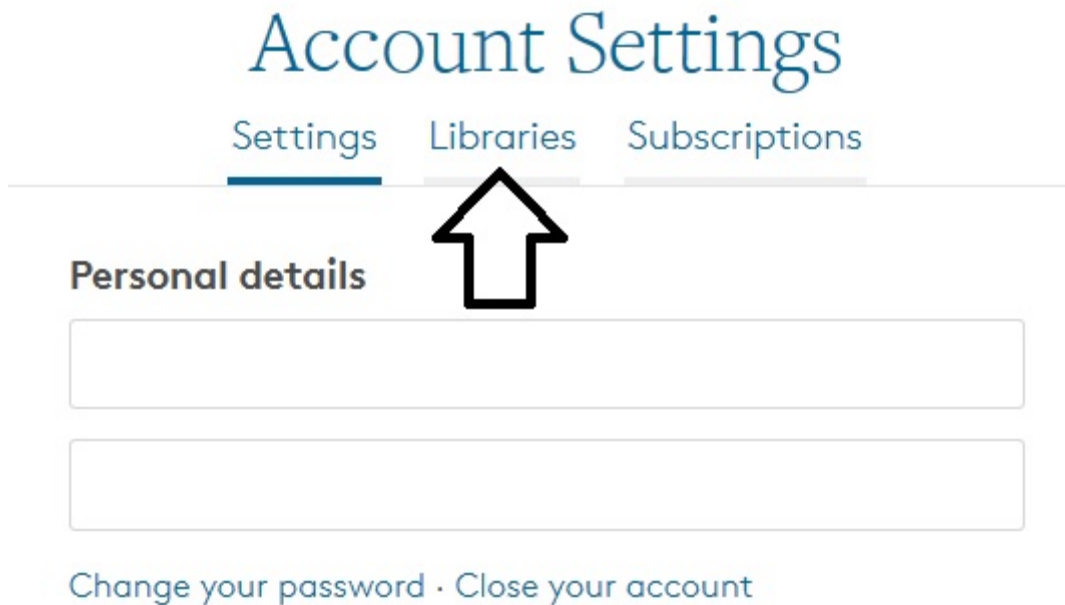
Set a password:

Your password must be at least 8 characters.

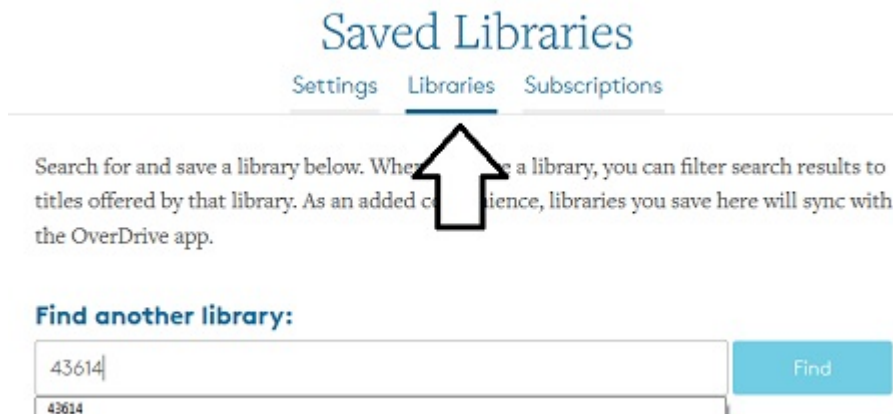
You'll receive an e-mail that asks you to verify your account. Click on the link in that e-mail to verify.



You'll be taken to your account settings.



Click libraries and you can find your local library if it's a member of Overdrive. Type in the ZIP code or name of your library.



When you find your system, you can hit Save so that OverDrive remembers it.

Find a library near you:

Toledo-Lucas County Public Library

- Heatherdowns
- South
- Toledo Heights
- Mott



Now let's look for a book. Click the Search icon in the upper right of the page.



You can either search my Title or Author or choose to browse by subjects like Fiction or Technology.

Search for a title or author Everything [Find a library near you](#)

[FICTION](#) [CHILDREN](#) [BUSINESS](#) [YOUNG ADULT](#)
[ROMANCE](#) [BIOGRAPHY](#) [TECHNOLOGY](#) [SCIENCE FICTION](#)

[More »](#)

Here, I'll choose Fiction and see a selection of books to choose from.



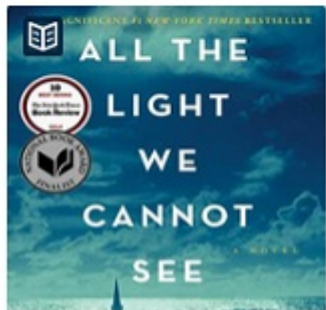
The Girl on the Train

Paula Hawkins (2015)



Gone Girl

Gillian Flynn (2012)



All the Light We Cannot See

Anthony Doerr (2014)

When you find a title you like, click on it. You'll get information about the book including a synopsis, reviews and what types of formats it's available in. To Borrow, just click the borrow button.

The Girl on the Train

A Novel
Paula Hawkins ·  EBOOK



Times Bestseller

was more fun with unreliable narration than *Girl*. . . [It] is liable to draw a large, '—*The New York Times*

ly blasts through the stagnation of these lon and the reader cannot help but turn lobe

BORROW

from Toledo-Lucas County Public Library

In libraries nearby: 

Toledo-Lucas County Public Library

[View](#)

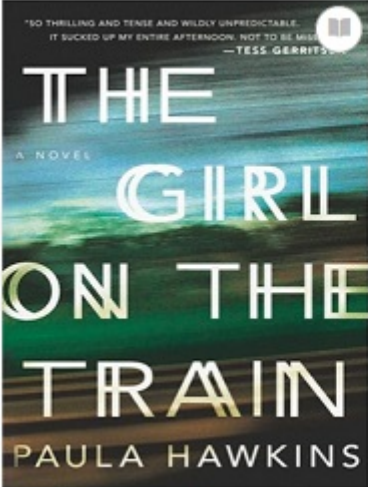
The Ohio Digital Library

[View](#)

Woodlands Library Cooperative

[View](#)

Then you'll have the option to immediately borrow or place a hold. Just as with physical books, libraries have a limited number of copies of eBooks that they are allowed to own. For popular books, you may need to wait awhile.



The Girl on the Train
A Novel
by Paula Hawkins

[Place a Hold](#)


[Add to Wish List](#) [Buy It Now](#)

★★★★★
Sign in & rate this title.

Instant #1 *New York Times* Bestseller

"*The Girl on the Train* has more fun with unreliable narration than any chiller since *Gone Girl*. . . [It] is liable to draw a large, bedazzled readership."—*The New York Times*

You'll then have to enter your library card and PIN number. If you haven't set that up with your local library yet, you will need to make sure you have a card and a password or PIN number to log in.



**Toledo-Lucas
County Public Library**

Enter your Library card number and PIN to sign in.

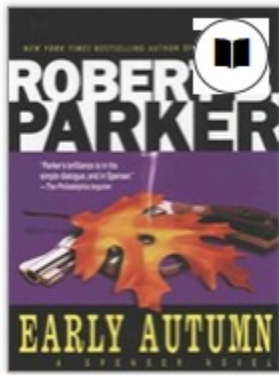
Library card number

PIN

[Sign In](#)

Remember my login information on this device.

You can then download a version of the book to read in a reading app or read it in your browser.



Early Autumn
Robert B. Parker

Download
(EPUB eBook)

Read
(In your browser)

Expires in 21 days

Return Title

The book looks like this in the browser.

of the advertising agency across the street a young black-haired woman in high-waisted gray trousers leaned over a drawing board. Her back was toward the window.

"My compliments to your tailor," I said out loud. My voice sounded odd in the empty room. The black-haired woman went away and I sat at my desk and looked at the picture of Susan Silverman. It was the blowup of a color picture taken last summer in her backyard. Her tanned face and pink blouse were bright against the dark green of the muted trees. I was still looking at Susan's face when my office door opened and a client came in carrying a belted poplin raincoat over one arm.

She said, "Mr. Spenser?"

I said, "I knew my clientele would upgrade when I moved in over a bank."

She smiled wonderfully at me. She had blond hair that contrasted handsomely with her black eyes and dark eyebrows. She was small and very trim and elegant. She had on a tailored black suit and vest, white shirt, black bow tie with long ends like Brett Maverick used to wear, and black boots with very high narrow heels. She was wearing gold and it looked real: gold earrings, gold watch, gold chains around the neck, gold chain bracelets, a wide gold wedding band, and a large diamond in a gold setting. I

was optimistic about my fee.

She said, "You are Mr. Spenser?"

I said, "Yes," and stood up and held a chair for her. She had a precise walk and a very nicely integrated figure and she sat erect in the chair. I went around behind my desk again and sat down and smiled. Time was they started to undress when I smiled, but I guess the smile had lost a step. The black eyes looked at me very carefully. The hands folded still in the lap. Ankles crossed, face serious. She looked at my face, both shoulders, my chest, and as much of my stomach as showed behind the desk.

I said, "I have a puckered scar on the back of my right, ah, thigh where a man shot me about three years ago."

She nodded.

"My eyes look maybe a little funny because I used to be a fighter. That's scar tissue."

"Apparently people hit you in the nose quite often too," she said.

"Yes," I said.

She looked at me some more. At my arms, at my hands. Would I seem forward if I offered to drop trou? Probably.

You can also download audio books and movies using your OverDive account.

Have you checked out eBooks from your local library? How about movies and music?

From: The Desk of Jim McGorry

Excerpts taken from the Windows Secrets Periodical

LINUX FOR WINDOWS USERS: INSTALLING UBUNTU

In a February article, we gave a brief introduction to Linux and its history, showing why some Windows users might want to experiment with this open-source OS.

This follow-up story will tell you how to install and run one of the more popular Linux distributions — Ubuntu (pronounced, "oo-boon-too").

To quickly recap the Feb. 19 **Top Story**, "An introduction to Linux for Windows users," Linux has become an immensely important operating system, mostly for back-end services and standalone devices. On the consumer side of things, it's the basis for Android phones and tablets, routers, network-attached hard drives, and many other devices. Linux might soon be the central operating system in your car.

In that previous article, I also noted that — contrary to what many Windows users believe — versions of Linux have intuitive and familiar graphical user interfaces. In fact, one of the more interesting aspects of Linux is the broad selection of desktop designs. And while Linux has fewer consumer and business applications than are available for Windows, you can find an app for almost any need.

As promised in the February introduction, this article will walk you through installing Ubuntu Linux, one of the most user-friendly distributions (distros) — and one that's earned a reputation for innovative interface designs.

Linux rarely comes preinstalled on a newly purchased computer (an Ubuntu [page](#) has an official list of supported desktops and laptops). So users typically get lots of experience with the installation process. It's essentially no more difficult than installing Microsoft Office from a CD. Many Linux users run the OS alongside Windows or OS X — and in some cases, both — using a multi-boot configuration. If you're just getting started with Ubuntu, running it on a virtual computer system is another excellent option. Or, if you have a retired-but-still-functional PC sitting in a corner of your office, Linux is a great way to put the hardware back into service.

For help with setting up multi-boot and virtual configurations, see the following stories. They discuss other operating systems, but the information can be applied to installing Linux.

- "How to safely test-drive Win10 — step by step" – Oct. 16, 2014, [Top Story](#)
- "Two ways to put Windows 7 and 8 on the same PC" – April 4, 2013, Best Practices [article](#) (paid content)
- "How to run Google's Android OS on a Windows PC" – March 13, 2014, [Top Story](#)
- "Setting up a Win7/Win8 dual-boot system" – April 11, 2013, Best Practices [article](#) (paid content)
- "How to avoid Win7/Win8 dual-boot hassles" – Feb. 12 LangaList [column](#) (paid content)

Using a virtual machine is almost always easier and safer than configuring a dual-boot setup. But if you choose dual-boot, I strongly recommend taking the precaution of backing up your main operating system (typically Windows). Also, I'm assuming that Ubuntu will not be your full-time OS — this article is for Windows users who want to experiment with Linux. So I won't discuss how to transfer your working data from Windows to Ubuntu.

Once you have Linux up and running, I think you'll find, as I do, that working with Ubuntu is a fun way to spend a spare hour here and there, learning something new about the world of Linux computing.

Step 1: Download an Ubuntu distribution

Installing Ubuntu starts with downloading the bits and creating a bootable installation disk or USB drive. You can find the free ISO file on the Ubuntu [site](#); beginning users should go with the recommended Ubuntu 14.04.2 LTS (Long Term Support) version. Select the edition appropriate for your system processor — 32-bit or 64-bit — and click the big Download button. That will take you to a nag page for contributions; click the "Not now, take me to the download" link — or feel free to contribute a few dollars to future Ubuntu development.

Note that the installation file is about a gigabyte, so the download will take some time. (BitTorrent users can click the "Alternate downloads and torrents" link directly below the Download button for much faster downloads.)

If you're going to set up a multi-boot system or install Ubuntu on a spare PC, burn the downloaded ISO to a CD/DVD or load it onto a USB drive. Be sure to select the settings that will make the media or drive bootable. (Simply copying the file won't produce a bootable disk.) For more on creating a bootable flash drive, see the April 25, 2013, LangaList Plus [column](#), "Tools for creating a bootable flash drive" (paid content), and the Oct. 17, 2013, Best Practices [column](#), "A complete Windows repair kit — in your pocket."

If you're going to set up a virtual machine, put the ISO somewhere on your local hard drive where you can easily find it.

Step 2: Check the hardware (or virtual machine) setup

Ubuntu recommends the following minimum hardware setup:

- 700MHz processor (Intel Celeron or better)
- 512MB of system memory
- 5GB of free hard-drive space
- 1024 by 768 screen resolution
- CD/DVD drive or a USB port
- Internet access

Web access is important because the installer will attempt to download the latest software and security updates from Ubuntu. In my experience, it's best not to rely on Wi-Fi during installation — use an Ethernet connection to your router.

And if you're installing Ubuntu on an old PC, be sure there's no valuable, unarchived data on the hard drive!

Step 3: Start the installation process

Insert the optical media or USB drive and boot the system. After a couple of minutes, you should see a welcome screen (Figure 1) offering a choice that Windows (and Mac) users might find surprising. (Note: When I installed Ubuntu in a VirtualBox ([site](#)) machine, I received a couple of error messages on booting. I simply ignored them and waited for the Ubuntu welcome screen to appear.)

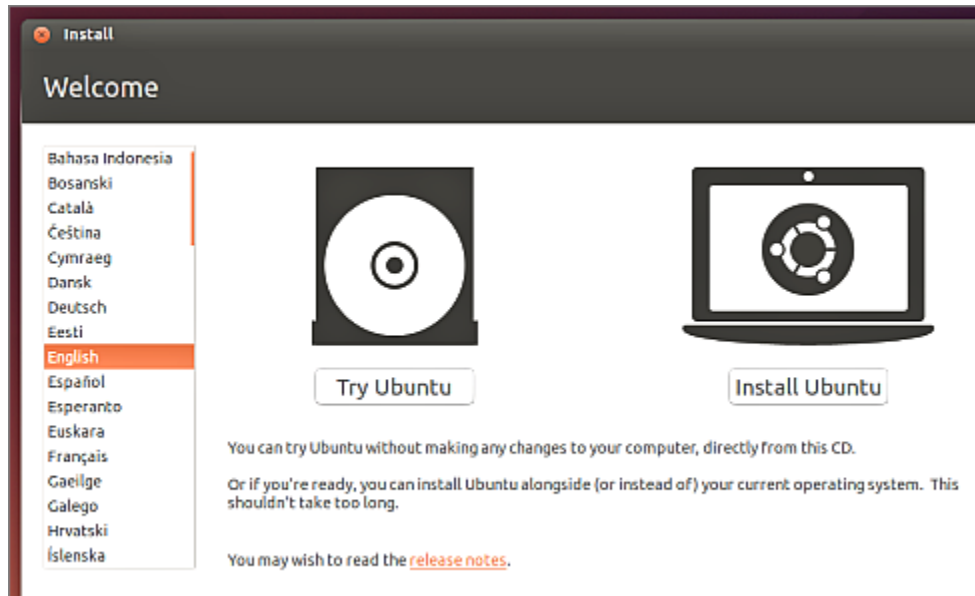


Figure 1. The Ubuntu installation tool lets you try the OS directly from an optical disc or flash drive.

As the welcome screen notes, the "Install Ubuntu" option will set up the OS on the hard drive. The "Try Ubuntu" option is a feature common to most Linux distros — a so-called "live system" runs directly from an optical disc or USB drive. It's a more-or-less complete Linux system that can load into system memory without touching the computer's hard drive.

An optical disc is read-only, but USB-based live systems can have writeable partitions that allow settings and data to be saved across sessions. Live CDs were originally used as cross-platform utility disks, but they quickly evolved into a convenient Linux marketing tool. Because a live system doesn't affect Windows, you can try a Linux environment without committing yourself to anything.

(Live CD/USB systems are also used in ultra-secure Linux distributions such as Tails [\[more info\]](#), which hardens a full range of applications with encryption and anonymity. It can be used on any machine without leaving traces of the user's activity.)

To start, I'll take advantage of Ubuntu's live-system option to give a brief tour of Ubuntu's Unity desktop. You'll be able to resume the installation from inside the running live system.

Step 4: A quick tour through the *Unity* interface

When you click Try Ubuntu, your computer (or virtual machine) will reboot into the sign-in-free — but otherwise normal — Ubuntu Unity desktop, shown in Figure 2.

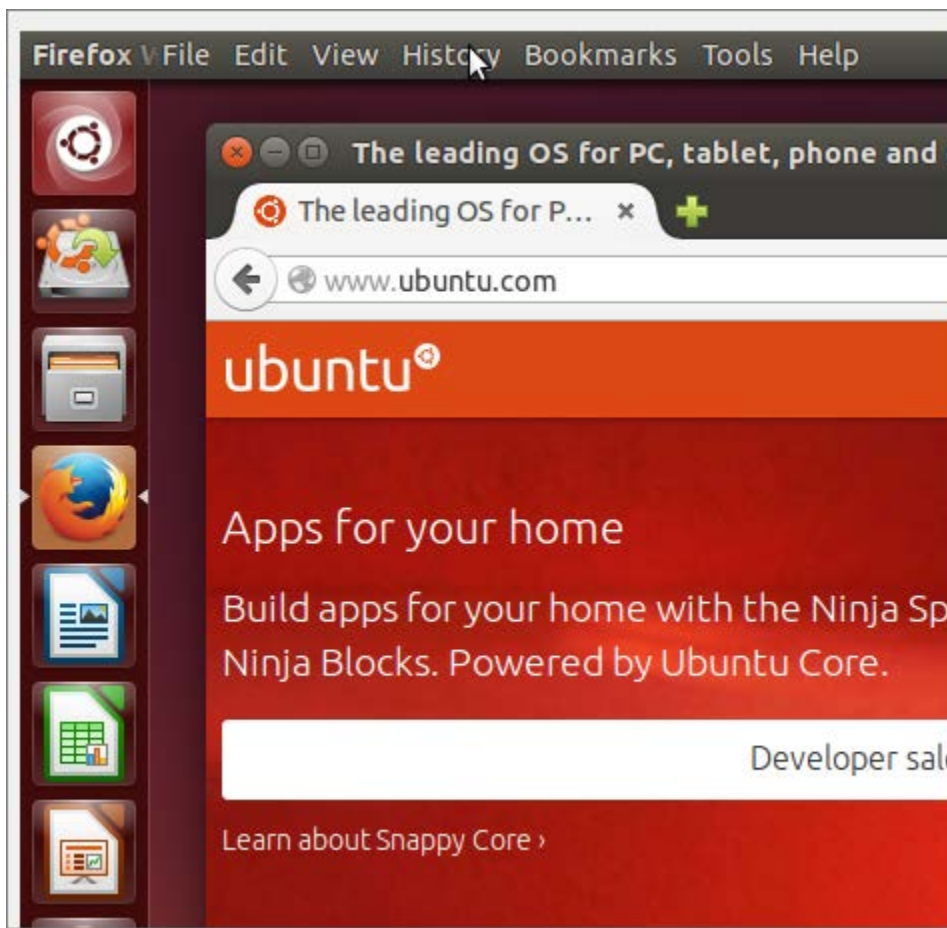


Figure 3. On Ubuntu, applications such as Firefox (shown above) use a blend of Windows and OS X UI features.

In short, Unity treats applications in a fairly conventional way, supporting multiple, resizable app windows and a standard Windows Explorer–like file manager. Unity has features in common with Windows 8: Ubuntu's developers emphasize the use of search — and that means using the **Dash**, accessed via the **Super key** (typically, the Windows key on most keyboards) pops up a search-box window (Figure 4); holding it down displays a list of keyboard shortcuts, shown in Figure 5.

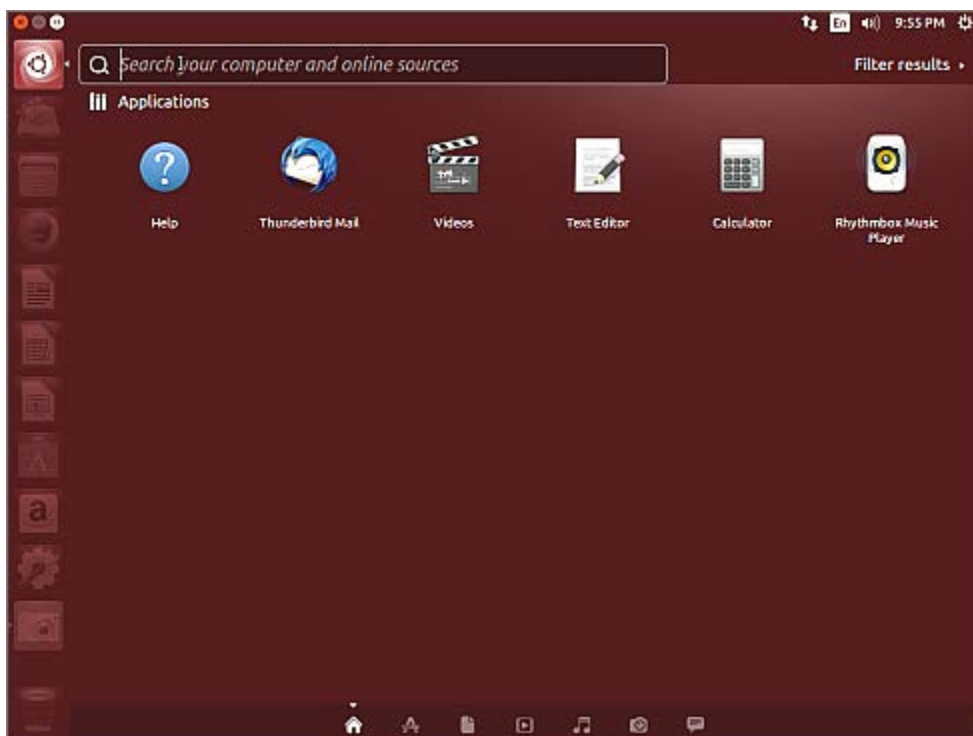


Figure 4. Clicking the Super key pops up a Win8-like search box with filters for common applications.



Figure 5. Holding down the Unity *Super* key displays a list of common keyboard shortcuts.

The initial Dash window includes various icons for quick search filtering by applications, files, video, music, photographs, and social-network messages. Typing a search term triggers immediate searches — for example, typing "vid" (see Figure 6) quickly returns several video-related applications.



Figure 6. Entering a search term — in this case, *vid* — immediately returns related applications and files.

The Dash has elements that will be familiar to both Windows 8 and Yosemite OS X users. Each of these three search-centric interfaces attempts to dispense with static menus and mouse-clicks by imitating the auto-complete environment pioneered by Google. They also blur the line between client-side and browser-based resources. That might not be ideal for personal security, but it's fully in line with the vision of the mobile future currently embraced by the tech world.

For example, selecting the Dash's application category and entering "terminal" returns terminal emulators included with Ubuntu (hey, it's Linux) as well as applications that can be downloaded from the Net. Selecting the video category and entering "roller derby" brings up a mix of YouTube videos, retail offerings from Amazon, and other sites. (The presence of an Amazon icon in the launcher suggests that Ubuntu is receiving some revenue from that online retailer, which *might* have some influence on search results.)

Now that you've had a quick introduction to the Unity interface, it's time to move on to the full installation. But first, you might find a video [demonstration](#) of Unity's heads-up display (HUD) interesting. HUD is yet another approach to dispensing with hierarchical menus and guessing what the user is actually looking for.

And for a taste of the flashier capabilities of the Unity interface — including multiple virtual desktops (a Linux staple), crazy 3-D rotating cube displays, and wiggly windows — have a look at another YouTube [video](#).

Step 5: Completing the installation process

Back at the Unity desktop, double-click the Install Ubuntu icon (see Figure 7) to set up the operating system on your hard drive.



Figure 7. Click the Install Ubuntu icon to fully set up the OS on a physical or virtual machine.

From this point on, installation should be relatively familiar to anyone who has installed Windows from a CD — although, in this case, the installer runs inside a window of the still-running live system. (Note: You could have started the full installation by clicking **Install Ubuntu** back on the original welcome screen.)

A wizard steps you through the process, starting with language selection. The next screen lets you select check boxes for downloading software updates and for installing third-party utilities such as codecs for playing MP3 files and MPEG videos (Figure 8).

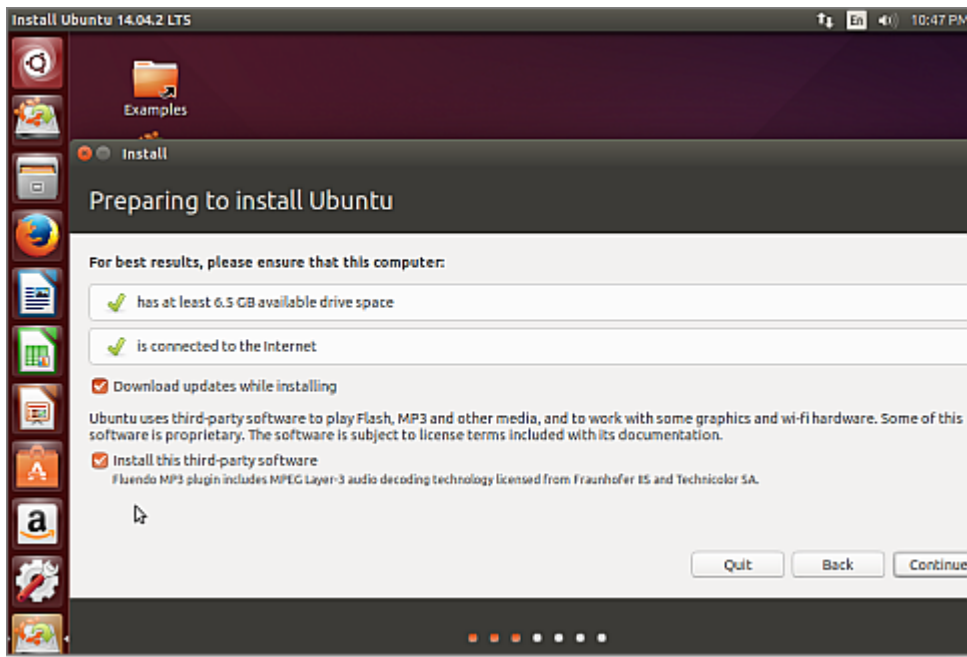


Figure 8. Ensuring that Ubuntu is ready to install

Note: Ubuntu is based on the Debian Linux distribution, which excludes restrictively licensed proprietary software from its core repositories. For user convenience and to be competitive with commercial operating systems, Ubuntu has licensing agreements with Fraunhofer ([site](#)) and Technicolor ([site](#)), giving MPEG support for users who opt in. (Such agreements are controversial [[more info](#)] in the free-software community.)

Click Continue when ready.

Next, choose the installation type. The default, shown checked in Figure 9, is to let Ubuntu erase your hard drive and handle all drive configuration. You can also choose to encrypt your drive, configure volume management, and manually partition the drive — all of which are beyond the scope of this introduction. Click Install Now to continue.

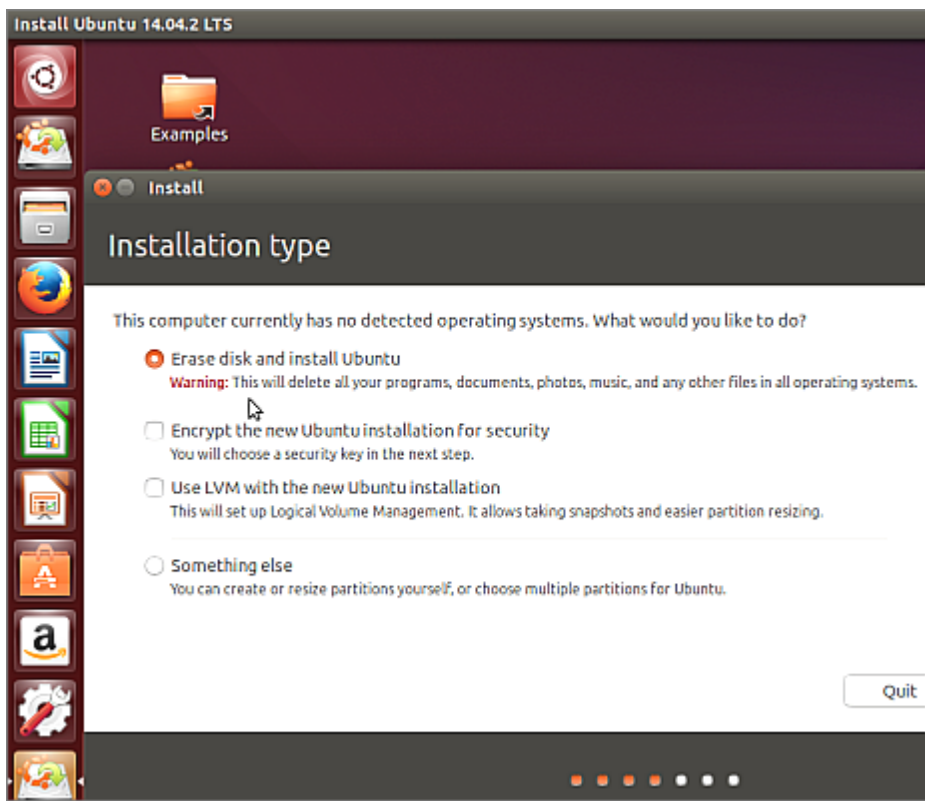


Figure 9. Ubuntu offers several installation types; using the default setting will erase all data on the target drive.

The installation wizard will then pop up a warning that your drive will be erased. If you're sure you're ready, click Continue. Next, on successive screens, select the time zone, keyboard layout, and sign-in information.

Enter your name, the computer's name, a username, and a password (see Figure 10). The wizard will rate the strength of your password as you type it in. You should click "Require my password to log in." You also have an option to encrypt your home folder (again, a topic beyond the scope of this Linux introduction). Click Continue when done.

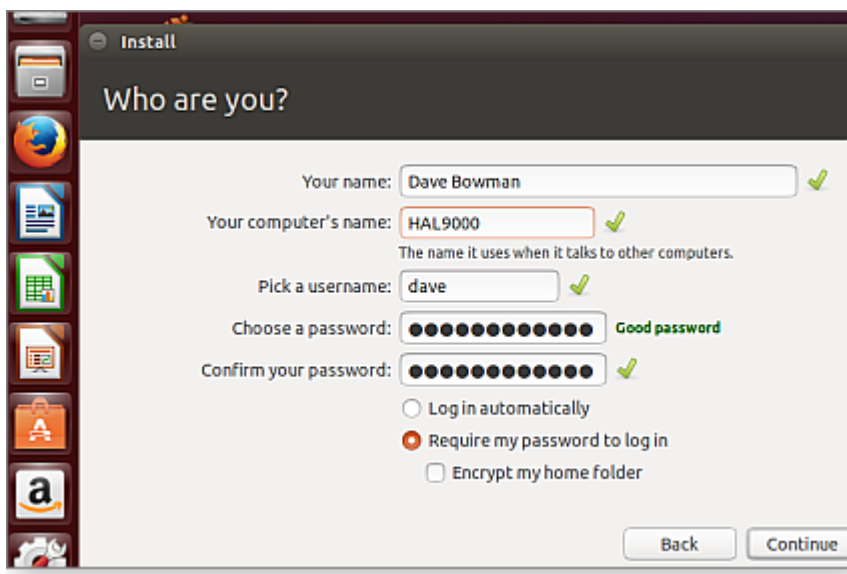


Figure 10. When you add your new sign-in credentials, Ubuntu rates your password strength.

Wait while the installation wizard finishes setting up Ubuntu on your hard drive. The wizard will entertain you with pretty pictures and user tips. Eventually, you'll be prompted to reboot. On physical systems, before clicking the Restart Now button, be sure to remove the CD or USB drive.

When the computer reboots, Ubuntu will welcome you with its standard sign-in screen, shown in Figure 11.

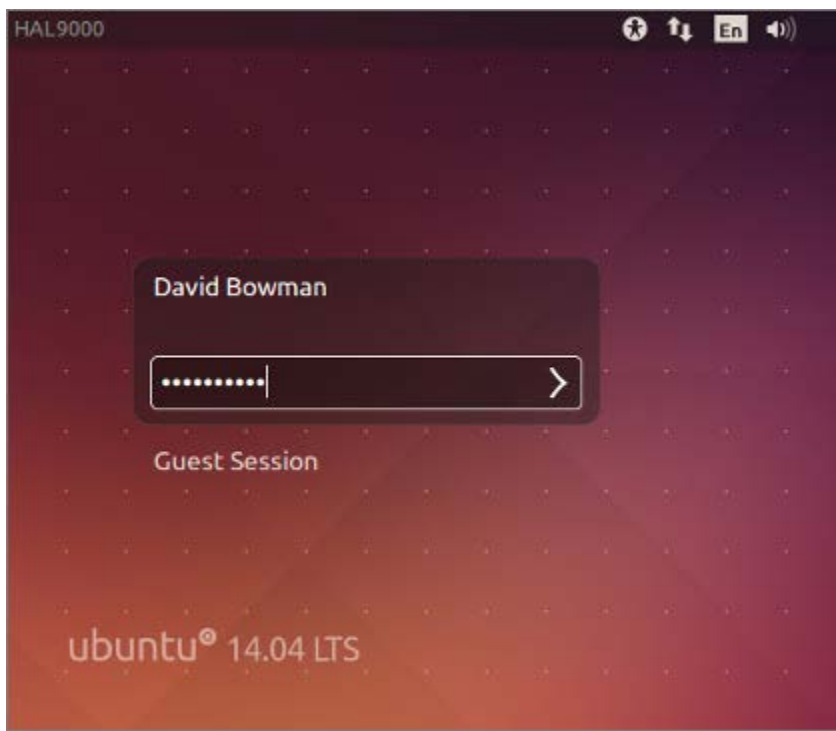


Figure 11. You're now ready to experiment with a fully installed version of Ubuntu Linux

Note: If you're running Ubuntu on a VirtualBox machine, be sure to install the **Guest Additions**. In the virtual machine's toolbar, click **Devices/Insert Guest Additions CD image**. Once the virtual CD is mounted in Ubuntu, click the CD icon to open it and then click the Run Software button in the upper-right of the window. This process adds services and drivers that make Ubuntu more usable.

Now, the real fun begins. In a final installment of this introduction-to-Linux series, I'll talk about features that are uniquely Linux — things that might at first mystify both Windows and Mac users. That'll include essential configuration options, basic system

CHANGING NAMES AGAIN: 'METRO' BECOMES 'WINDOWS'

An obscure notice that 'Metro apps' are now 'Windows apps' leaves more than a few Windows observers confused.

Microsoft has a long history of bungled product branding, but its latest decision plumbs new depths.

How *not* to announce a major branding change

Microsoft recently announced a significant change in the terminology for programs that run under Windows 8 and 10. You and I, our co-workers, our friends and family, even passers-by on the street will soon be asking whether our Windows computer can run Windows apps — and/or Windows desktop applications. As is all too common with Microsoft branding, the answer is far more complex than it should be.

You'd expect such a major change to be announced with explosive fanfare, dancing office-worker ads, a Super Bowl spot — and a lot of education for the beleaguered customer base.

You would be wrong!

Instead, the announcement was buried in a presentation by Microsoft Distinguished Engineer Don Box in a one-hour WinHEC (the Windows Hardware Engineering Conference) presentation in Shenzhen, China. You can see the full [presentation](#) on Microsoft's Channel 9.

The presentation was a discussion of drivers for hardware developers. But eight minutes into the talk, Box shows some interesting terminology. A slide (Figure 1) clearly explains the differences between Windows 10 for PCs, Windows 10

for phones, Windows 10 on Xbox (it's true), and Windows for the so-called *Internet of Things* (a term I intensely dislike): refrigerators, toasters, Raspberry Pi devices, and so forth.



Figure 1. At last, we have an official Microsoft chart that gives some names to the different Windows 10 flavors.

This slide is remarkable because, for the first time that I can recall, Microsoft officially talks about the branching of Windows 10. In the past we've heard the marketing-inspired phrase, "Everything will run Windows 10" — which is something you'd expect to hear from someone who's trying to sell you something. It's not in the least bit illuminating.

Finally, it seems, we're getting official names for what will certainly become different flavors of Windows 10. The delineation also adds some urgency to the question: What version of Win10 will the various Windows tablets run? We don't have a definitive statement on that part yet, although it's becoming increasingly apparent that there will be a huge gulf between Intel-based tablets and ARM-based tablets — not unlike the current Windows 8 distinction between Windows and Windows RT.

But the real surprise came 15 minutes into Box's presentation. He defines two types of applications: *Windows apps* and *Windows desktop applications*. Figure 2 shows the slide that makes the differences between the two types completely clear.

The slide has a blue background with white text. The title is 'Windows apps defined'. Below the title, it says 'Apps built on the Windows universal app platform are called *Windows apps*' and 'In contrast with *Windows desktop applications* that run on PCs only'. At the bottom is a table with two columns: 'Windows app' and 'Windows desktop application'.

Windows app	Windows desktop application
Runs on all Windows device families	Runs on PCs only
Can access WinRT, COM, and subset of Win32 APIs	Can access WinRT, COM, and Win32 APIs
Has strong app identity (static and dynamic)	Raw EXEs and processes
Declarative APPX manifest	Opaque binaries
Self-contained APPX package	Loose files or MSI
Isolated per-user/per-app storage (local and roaming)	Shared user profile
Participate in app resource management and PLM	Process-level lifecycle

Figure 2. Metro becomes Modern becomes Universal becomes — Windows apps! — and not to be confused with Windows desktop applications.

Box states: "We have Windows apps and Windows desktop applications. Windows apps are the universal ones. Desktop applications are PC only. ... Windows apps run everywhere *and* we still continue to run Windows desktop apps on PCs."

Apparently, that brief discussion constituted the official announcement of Microsoft's new app terminology — no press releases for online and print news, no song-and-dance in a major presentation by Microsoft leadership. No, the company has quietly re-re-redefined "Metro apps" as "Windows apps."

What a long, strange riff it's been

(Our apologies to the Grateful Dead.) If you've been following the tortured evolution of Windows 8, you know that Microsoft decided to build a flat, tiled interface with very distinctive typography. Microsoft called it "Metro" — for a while — and everyone else has used it ever since. Metro apps are written to interact with the WinRT API, which I talked about in the March 19 [Top Story](#).

As best I can determine, Microsoft first used the term "Metro" back in October 2010 to describe the Windows Phone 7. The next year, Microsoft unveiled Windows 8 and called the new operating system's native, WinRT-based programs "Metro apps." (I first wrote about Metro apps in the June 9, 2011, [Top Story](#), "What you need to know now about Windows 8.")

Then, in August 2012, quoting from a leaked internal Microsoft memo, The Verge's Tom Warren [reported](#):

"[In the memo], Microsoft reveals that 'discussions with an important European partner' led to the decision to 'discontinue the use' of the Metro branding for Windows 8 and other Microsoft products — one that employees must adhere to immediately. The Windows team is 'working on a replacement term,' according to the memo, 'and plans to land on that by the end of this week.' Until then, employees have been advised to refer to the Metro style user interface as the 'Windows 8 style UI.'"

That "partner" was Metro AG, a large German retailer and purveyor of Microsoft products. Metro AG objected to Microsoft's use of "Metro," and Redmond backed down. This was before the production version of Windows 8 was even released. So Microsoft had relatively little to lose.

Microsoft essentially claimed that there never was a name change. "Metro" was always a code word for the new interface. Henceforth, the WinRT-based apps would be called "Windows Store apps." Perhaps, but there's no denying that the conflict with Metro AG pushed Redmond to quickly drop the Metro label — and it began the bumpy, roller-coaster ride of Win8 interface branding.

A week after Warren's leaked memo, ZDNet's Mary Jo Foley [reported](#):

"Here's the official guidance, my sources say: Anything currently/formerly known as a 'Metro-Style application' (with or without a hyphen) will now be known officially as a 'Windows 8 application.' References to the 'Metro user interface' will now be replaced by 'Windows 8 user interface.' And instead of saying 'Metro design,' the Softies and those adhering to their official guidelines will be using the words 'Windows 8 design.'"

Microsoft's official labeling notwithstanding, repeatedly referring to the new interface as "Windows 8 user interface" was simply too much for everyone else — "Metro" stuck in the popular vernacular.

In fact, for many of us who follow technology, "Metro" now refers to a style, layout, and typography. Thus, it's entirely possible to build a program that looks "Metro" but doesn't use the WinRT API. You could argue that other developers have "Metro"-ized their programs and interfaces — even those that have nothing to do with Windows. (For a while, there were rumors that Apple's OS X would evolve — or devolve, to some — into a Metro-style, tiled interface.) But I think that Windows Media Center, which predates Win8 by years, is Microsoft's first widespread use of the Metro look.

Unfortunately, Microsoft could never seem to settle on a suitable name for its new interface and apps. In October 2012, Metro was called "Microsoft Design Language" at the Build 2012 conference. Calling the programs "Windows Store apps" made no sense at all — the Store was branching out to non-WinRT apps.

Microsoft has also used "Modern apps" and, most recently, "Universal apps."

It's no surprise that Microsoft's customers are mightily confused. Metro, Metro Style, Windows 8-style UI, Modern, Universal, and all the other labels that quickly came and disappeared referred to more or less the same thing — the tiled interface and WinRT-based apps. It's a marketing manager's nightmare.

Inflicting unending confusion on MS customers

It's easy to chalk all this up to just another dropped ball in a long, long line of fumbled Microsoft branding. But I'd argue that the convoluted transition from "Metro" to "Windows" is the worst ever (though calling the Metro-only version of Win8 *Windows RT* comes awfully close).

"Windows RT" branding left a lot of Microsoft customers wondering why their Windows programs wouldn't run on their new Surface tablet or third-party convertible. (I still get emails with that question.) I firmly believe that name confusion doomed Windows RT right from the start. If something's called "Windows," it should darned well run standard Windows programs! Shouldn't it? (I talked about this issue in the Aug. 23, 2012, [Top Story](#), "Where we're all headed with Windows RT.")

Fast-forward to this March 18, and — essentially given as a footnote in that WinHEC presentation — we're informed that WinRT/Metro apps will henceforth be called "Windows apps" and classic Win32 apps will become "Windows desktop applications."

I fully expect to see an entirely new round of mail asking why a Windows user can't run his bass-fishing program on a brand-new Windows tablet — or why that nice new Netflix app (assuming there is a new Netflix app) runs on her Win10 laptop, but she can't even find it for her Win7 desktop. After all, it's a Windows apps, right?

And there will be questions on what, specifically, a "Windows desktop application" is. I can hear it now: "I have a Windows RT tablet. It has a desktop; it's just hidden by all those fancy tiles. Why won't it run Windows desktop applications?" (It appears that Windows RT will eventually disappear altogether. The newest Surface tablets all use full Windows.)

The "Windows app" versus "desktop app" is more than the typical Microsoft *nom du jour* issue. Just as we're getting past the dark side of Windows 8, Microsoft comes up with labeling that further obfuscates the important differences between WinRT-based and Win32-based applications. It could be a world-class problem for both Microsoft and its customers.

Windows 10 is shaping up to be a tremendous product, a worthy successor to Windows 7. But the Windows app/desktop app confusion will remain — and many Win10 users will be left wondering why there are two types of applications. It'll be sad (and potentially costly) if Microsoft compromises Win10's technical excellence just because the company can't come up with clear, intuitive product labeling.

Weekly Download Section

from Jim McGorry

Welcome members and visitors alike to this new section I hope it will be of interest and use to you.

Each month I will try and have interesting and useful programs for you to download and try on your systems as you see fit. Some are free and some may have a nominal fee.

A brief write-up and link to download page will be displayed here so you can determine if you wish to get it and use it.

ALSO NOTE: Some web addresses may not be a direct link. If not, then just copy and paste the address into the "Address Location" window and hit enter.

[Revive An Ancient PC With Puppy Linux, Part 1](#)

Have you ever cleaned your house one day and accidentally stumbled upon an old laptop or PC that you're not using anymore? Is it too slow to run Windows 8, Windows 7 or even XP? If you're anything like me, then you probably do have at least one of them lying around simply because you don't want to throw it away. The answer to your dilemma is to Linux, a free operating system (OS) with a huge number of versions which can cater to just about everything from a full OS like Windows or something a little lighter.

Head over to [Distrowatch.com](#) and you'll see a large amount of Linux distributions that are free to download.

The screenshot shows the DistroWatch website. On the left, there's a 'Latest Distributions' list with entries like 'Ubuntu 12.04', 'Debian 7', etc. The main content area features articles from 'Distrowatch Weekly, Issue 598' dated 2015-02-23, discussing RISC OS and ClearOS. A red arrow points to a link in the article. On the right, a table lists various Linux distributions with columns for Rank, Distribution, and H.P.D. (Hours Per Day).

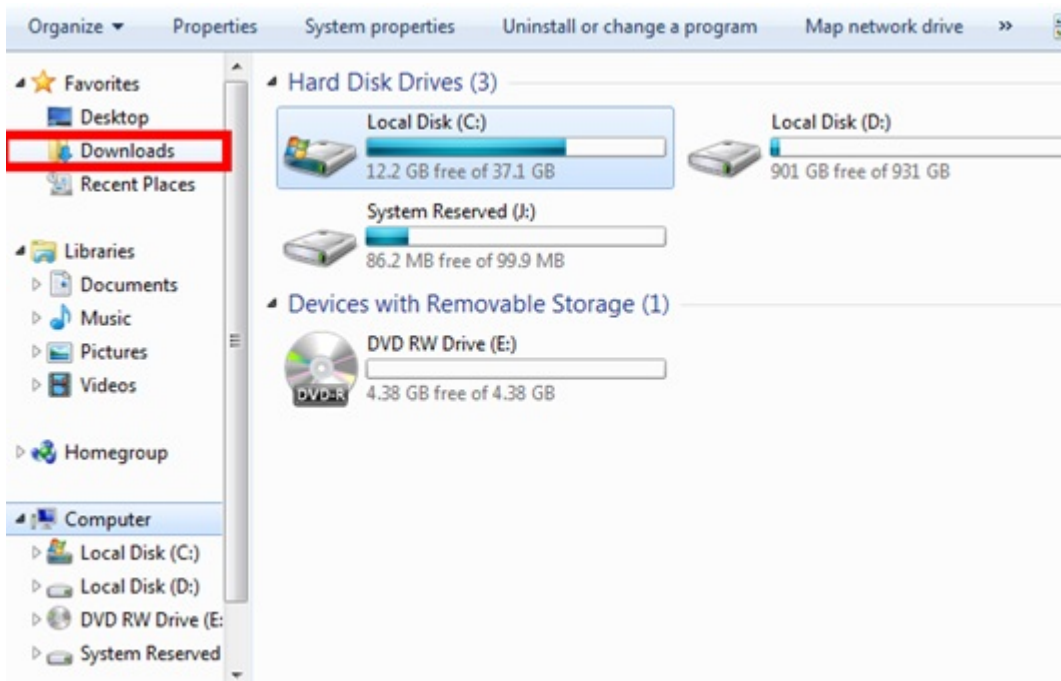
Rank	Distribution	H.P.D.
1	Mint	2540
2	Ubuntu	1837
3	Debian	1623
4	openSUSE	1456
5	Fedora	1333
6	Mageia	1127
7	CentOS	1117
8	Arch	1038
9	elementary	979
10	LXLE	824
11	Androidx86	800
12	Puppy	749
13	Kali	722
14	PCLinuxOS	721
15	Lubuntu	709
16	Manjaro	694
17	Deepin	672
18	Zenit	647
19	Bodhi	608
20	FreeBSD	560
21	Redhat	526
22	SteamOS	500
23	Sinfulix	496
24	SpookyLinux	464
25	Lite	451
26	Q4OS	448
27	Ultimate	444
28	Tails	442
29	Xubuntu	431

On the right side of the site, you'll find a list of Linux distributions. They'll run on almost any system, but if your computer is a really old model, along the lines of Pentium III, then I highly recommend getting [Puppy Linux](#), but Arch and Lubuntu are good choices too.

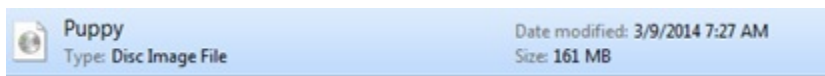
Once you've decided on which distribution you want to download, simply click on the name and it will take you the overview page. I will be using Puppy Linux here as the PC I'll be installing it on is Pentium III.

Puppy Linux Summary	
Distribution	Puppy Linux
Home Page	http://www.puppylinux.com/
Mailing Lists	--
User Forums	http://www.murga-linux.com/puppy
Documentation	http://puppylinux.org/wikka/
Screenshots	linuxscreenshots.org
Download Mirrors	http://www.puppylinux.com/download
Bug Tracker	--
Related Websites	PuppyLinux.org • Puppy Linux News • Wikipedia • Dotpups.de (Germ) • Hungary • Puppy Japan • Puppy Poland
	5 x: Distrowatch • Make Tech Easier • Linux Insider • Linux User • Distrowatch • Blogspot • OS News • Distrowatch • PCWorld • Tech • 4 x: I WN • Distrowatch • Tech Exposures • Defrimed • Blogspot • I

You will usually find it in your default Download folder by clicking on Start>Computer>Downloads



Linux distributions can be anything from 100 MB to around 1.5 GBs and will be classified as a “Disk Image File.”



Now that you have the new Operating System, all you need is to get this on your laptop. We'll use the USB method of doing this and for that you'll need [LinuxLive USB Creator](#).

LinuxLive USB Creator

www.linuxliveusb.com/

LinuxLive USB Creator is a free and open-source software to easily create Live USB.

[Download](#)

Download LILi rosette Version 2.9.2 drive 5.9 MB. Last update ...

[User's Guide](#)

Preparation - Step 3: Persistence - Choosing a USB key - ...

[Features](#)

Download · Features · Help · User's Guide · FAQ ... HomeFeatures ...

[New stable version 2.9](#)

New stable version 2.9. with lots of improvements.

[Supported Linux distributions](#)

Blog · List of supported Linux ... currently supporting these ...

[Help & Guide](#)

HomeHelp. agt_support. It is advised to read the online user ...

[More results from linuxliveusb.com »](#)

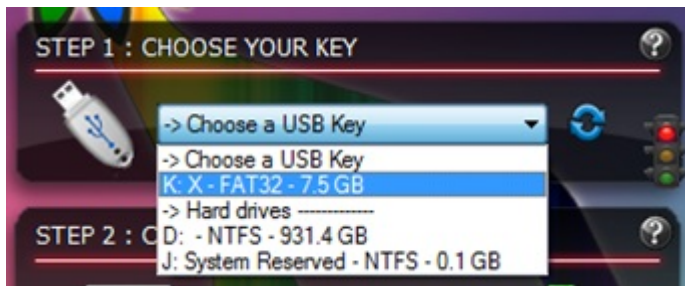
Click on the download tab and you'll be reconnected the download page.



Then click on the download button to start the download. You don't have to worry about viruses as these sites are legit. When the download finishes, install LinuxLive USB Creator and start the program. If you can't find the LinuxLive program, go to Start and type LiLi on the search bar.

When you have LinuxLive running, plug in any USB of your choice and make sure that it has enough storage to save your chosen distribution.

Once you have your USB plugged in, **press the Refresh button on the right side** and click on the drop down menu for Step 1.



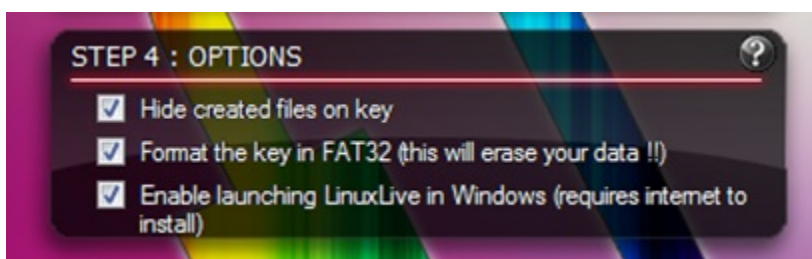
Look for the USB that you're going to use and click on it. It should be listed under the "Choose a USB Key" tab.



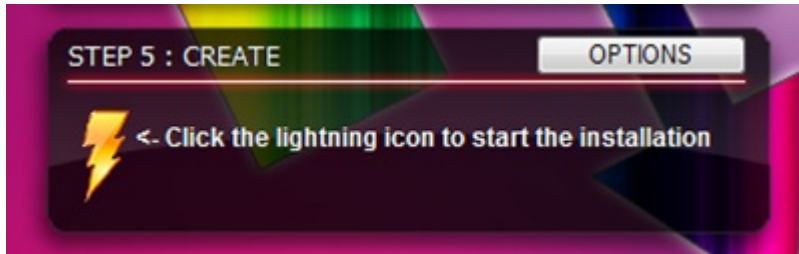
Now move on to step 2, **click on the "ISO/IMG/ZIP"** option and browse for the Linux version that you downloaded. I placed mine on the desktop for easy browsing. The program will read the file for a while, but it shouldn't take more than a couple of minutes to finish. You may also get the "This Linux is not in the compatibility list. However, LinuxLive USB Creator will try to use the same install parameters as for (other distribution)." Don't mind it; the installation will still work perfectly even if you get this message.

Ignore Step 3, this can be either a more advanced option or the distribution you downloaded will automatically fill it out for you.

Moving on to Step 4, you'll have three checkboxes to click on:



If you're going to use this USB for something else, then I would suggest that you check the "Hide created files" option. If the USB has some important file in it, be sure to back it up before ticking the "Format the key in FAT32" option. You can leave the last option unchecked. Finally, click on the lightning button on Step 5.



This extraction process will take anywhere from 5 to 15 minutes, maybe longer or shorter depending on your computer set up and if you chose to format the USB. When it finishes, disconnect your USB from your PC and plug it in your old Laptop or PC.

In part 2 of this article, we'll look at how to install Puppy Linux on your old PC.

[Install Puppy Linux & Revive Your Old PC](#)

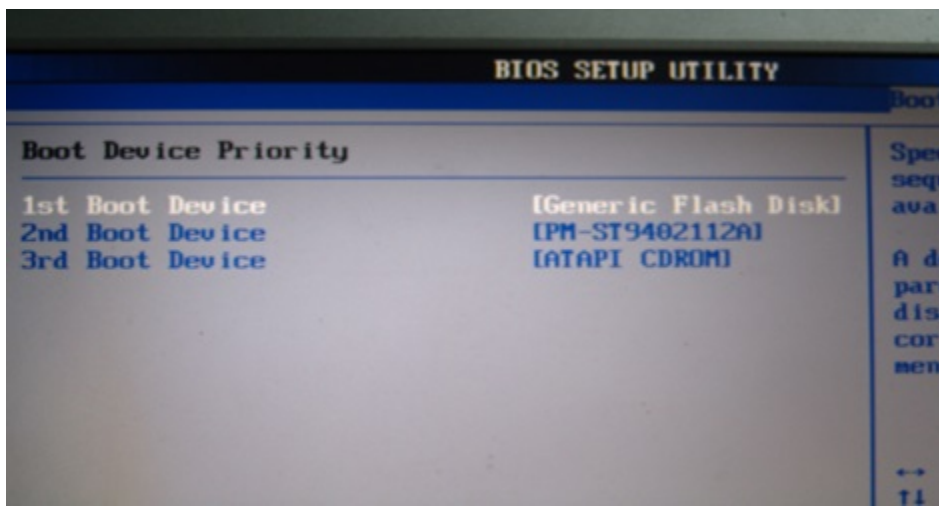
How would you like to be able to revive your old PC for free? In part one of this article, we told you how Puppy Linux can revive PCs with Operating Systems before XP. Yep, ancient PCs. Click here to learn how to find and download Puppy Linux for free.

Today, we'll look at how to install Puppy Linux from the USB drive we created in part 1. Plus that drive into the old computer's USB port.

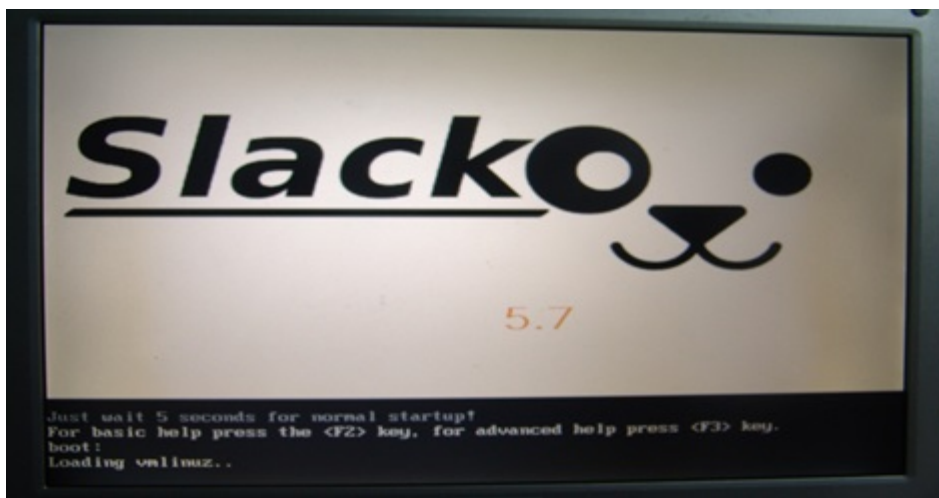
Start your old machine up and **get into the bios**. The way to enter the bios will be different from machine to machine, but the most common is by pressing F2 on the bios boot up.



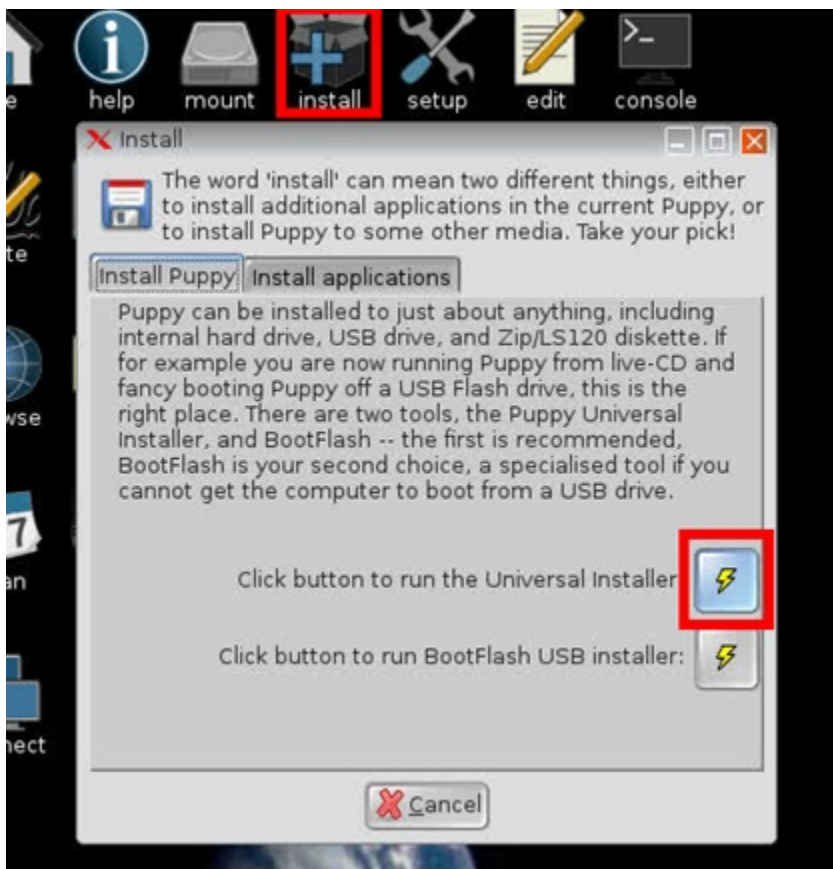
Go to the "Boot" tab and go down to the "Boot Device Priority" tab



Select your **USB**, usually named as a Generic Flash Disk as your main boot device. Then move to the “Exit” tab and choose to save changes. The machine will reboot by itself after saving your settings.



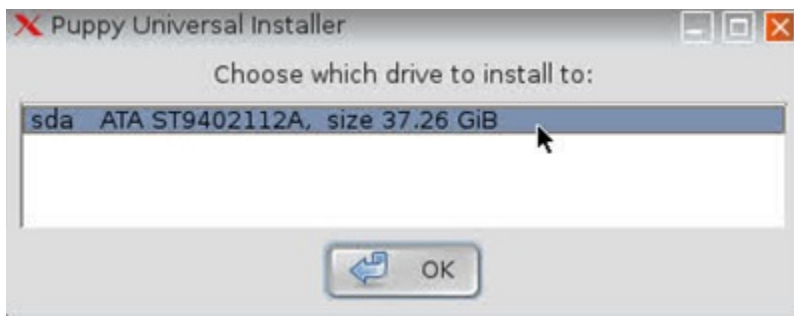
Your machine will now start and boot into the Linux that’s installed in your USB. You can stop here and carry the USB around as a portable PC, or you can permanently install the Linux distribution on your laptop/PC.



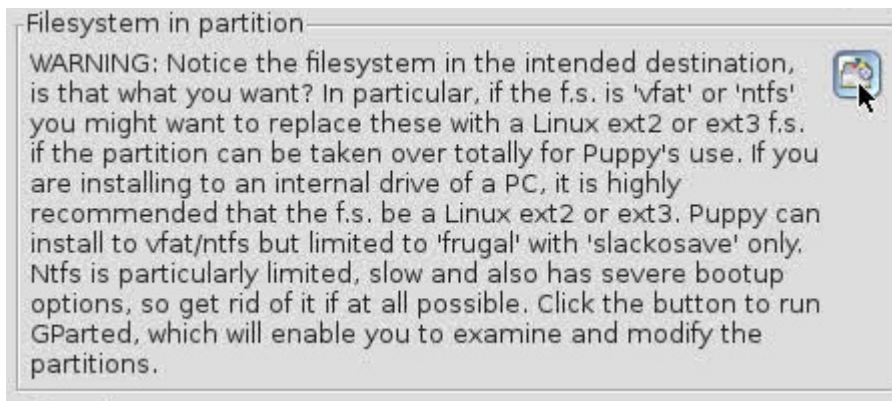
After booting up from the USB, **click on the “Install” button** that’s on the desktop. A window will pop-up, choose the first option “Universal Installer” to continue with the installation.



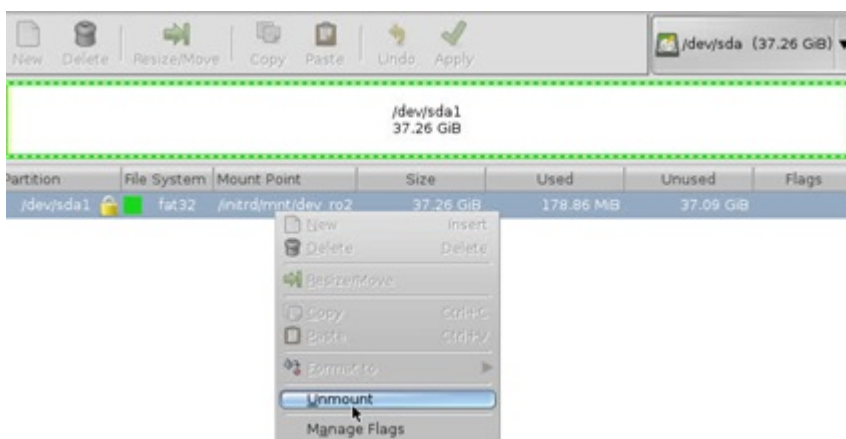
Select the option “Internal (IDE or Sata) hard drive” to install it directly on your machine, or USB Flash drive if you’re going to install it as a full operating system into the USB, then click okay.



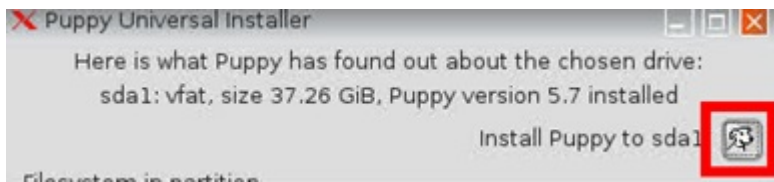
Select the hard drive that you'll use. You can check which hard drive you have inside the machine in the bios by going to Boot>hard drives, although usually a laptop/PC will only have one by default. Click okay, once you've selected it.



In the next page there will be three buttons. **Click the one to the right of the Filesystem partition box to open G-parted.**



Select the drive that you're going to install in and right click on it. **Unmount the drive**, then format it into ext2 or ext3, then click on the apply button at the top right corner of the window. Now close G-parted and you'll be taken back to the previous window.



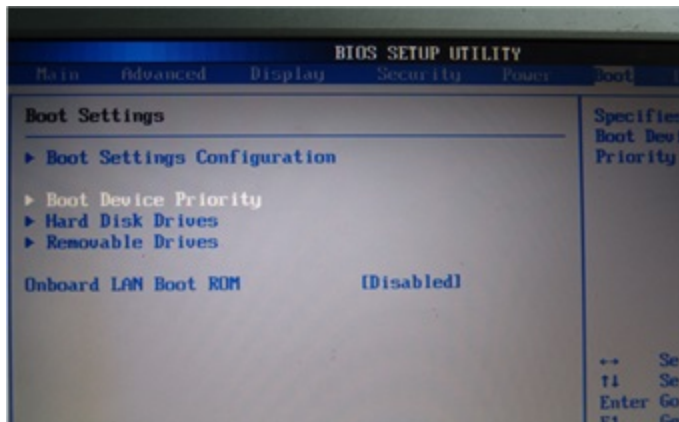
Select the first button on the page to install puppy on your hard drive. Click okay on the next page and wait for it to create a folder for you. Then restart your machine without saving any changes and voila! An old PC that runs as fast as any other PC out there!

Revive Your Ancient PC with Puppy Linux, Part 2

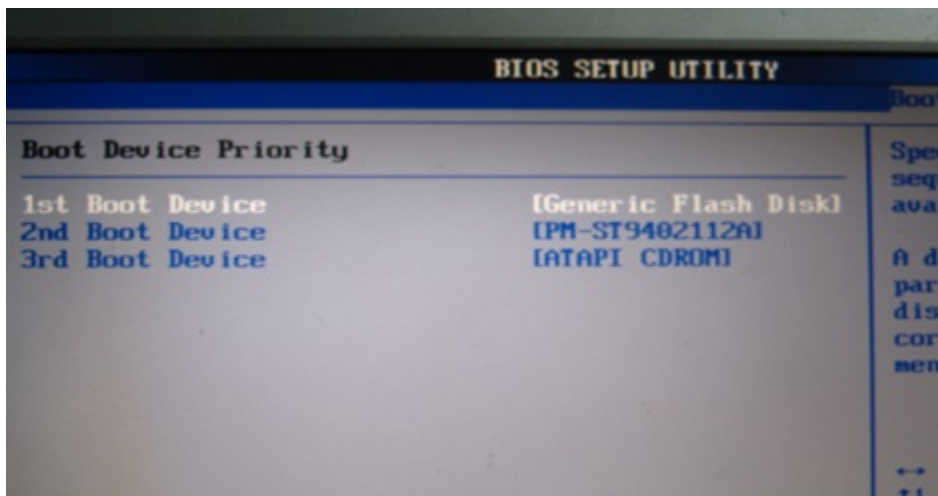
How would you like to be able to revive your old PC for free? In part one of this article, we told you how Puppy Linux can revive PCs with Operating Systems before XP. Yep, ancient PCs. Click here to learn how to find and download Puppy Linux for free.

Today, we'll look at how to install Puppy Linux from the USB drive we created in part 1. Plus that drive into the old computer's USB port.

Start your old machine up and **get into the bios**. The way to enter the bios will be different from machine to machine, but the most common is by pressing F2 on the bios boot up.



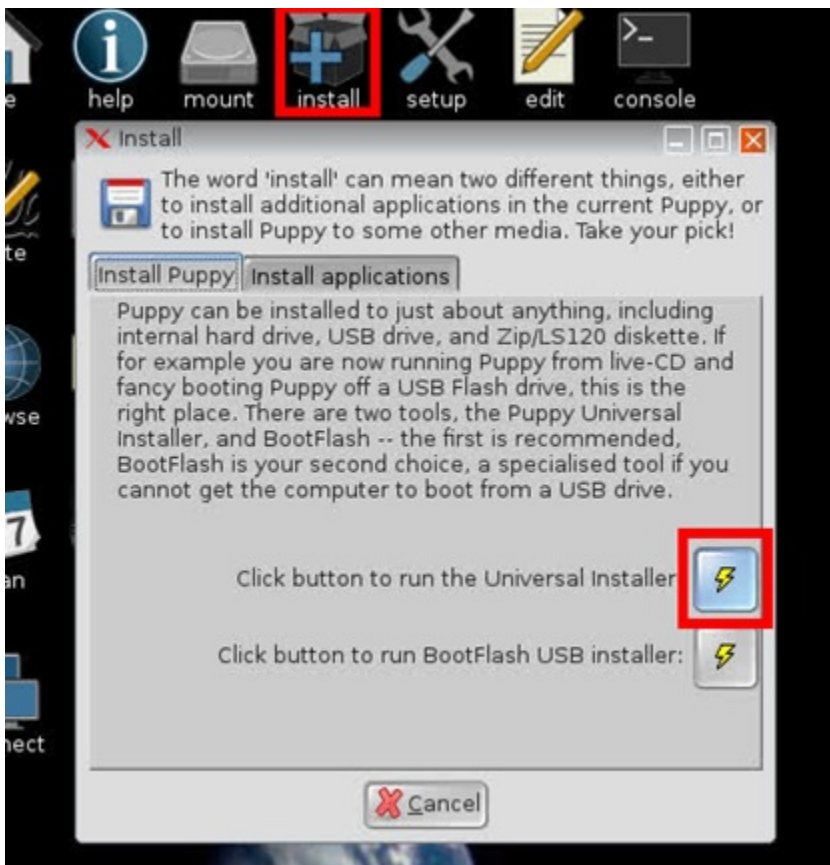
Go to the “Boot” tab and go down to the “Boot Device Priority” tab.



Select your USB, usually named as a Generic Flash Disk as your main boot device. Then move to the “Exit” tab and choose to save changes. The machine will reboot by itself after saving your settings.



Your machine will now start and boot into the Linux that's installed in your USB. You can stop here and carry the USB around as a portable PC, or you can permanently install the Linux distribution on your laptop/PC.



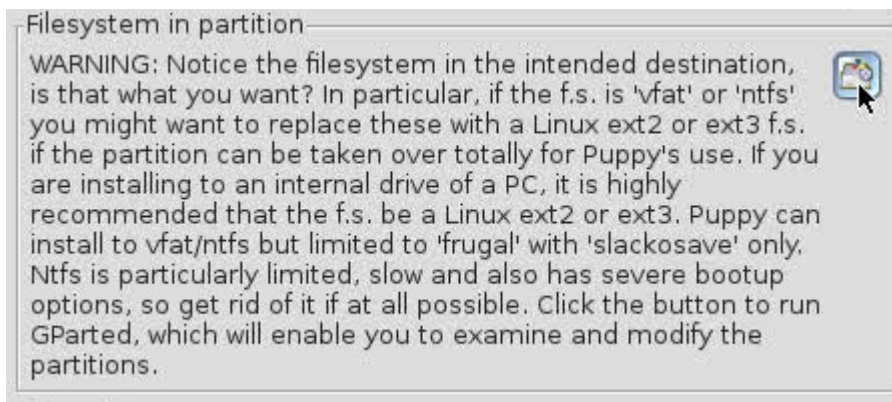
After booting up from the USB, **click on the "Install" button** that's on the desktop. A window will pop-up, choose the first option "Universal Installer" to continue with the installation.



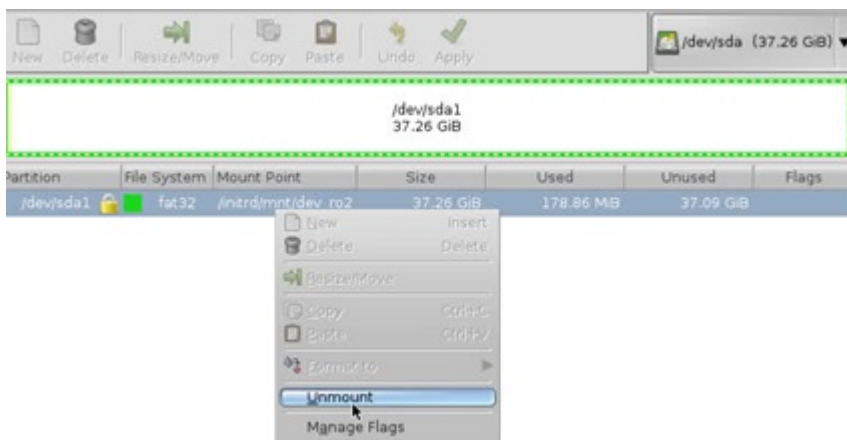
Select the option **“Internal (IDE or Sata) hard drive”** to install it directly on your machine, or USB Flash drive if you’re going to install it as a full operating system into the USB, then click okay.



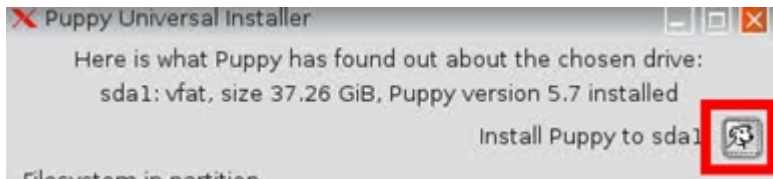
Select the hard drive that you’ll use. You can check which hard drive you have inside the machine in the bios by going to Boot>hard drives, although usually a laptop/PC will only have one by default. Click okay, once you’ve selected it.



In the next page there will be three buttons. **Click the one to the right of the Filesystem partition box to open G-parted.**



Select the drive that you're going to install in and right click on it. **Unmount the drive**, then format it into ext2 or ext3, then click on the apply button at the top right corner of the window. Now close G-parted and you'll be taken back to the previous window.



Select the first button on the page to install puppy on your hard drive. Click okay on the next page and wait for it to create a folder for you. Then restart your machine without saving any changes and voila! An old PC that runs as fast as any other PC out there!

From: The Desk of Jim McGorry

Excerpts taken from the Windows Secrets Periodical

HOW TO SAFELY TEST FILE AND IMAGE BACKUPS

Imagine this: You've lost important files, but when you go to restore them, you discover that your backups are completely unusable — and your next words are unprintable.

Fortunately, this nightmare is completely avoidable; here's how to ensure that your backup files are valid, complete, and usable.

Testing file-by-file backups and full images ("backups" for short) verifies that they were created correctly, they contain all the files you want protected, and you're able to restore them when and as needed.

There are, of course, dozens of backup tools available, both third-party products and tools built into all versions of Windows. But there are really only four safe ways to test and verify your backup files. (By "safe," I mean nondestructive tests that don't overwrite or harm any live files on your PC — or any files in the backup set.)

Starting with the easiest, the four methods include:

- A full, preliminary verification of the just-completed backup;
- Spot-checking file-by-file backups;
- Spot-checking system images;

- Fully testing a file backup or image.

The first and last methods — preliminary verification and full-test — are the most thorough, but not all systems and software allow them.

Spot-checking backups is not as thorough but works with virtually any system setup and backup software.

Keep in mind that the steps I'll give will vary somewhat from system to system and with the various backup tools. If any one of the following testing concepts doesn't fit your needs or preferences, or is incompatible with your setup, just move on to the next. One of them will almost surely work for you!

Use preliminary verification when available

Many backup tools offer some sort of simple *verify after creation* option that checks the contents of just-created backup files against the original working files. For example, Figure 1 shows this option in Macrium's Reflect Home Edition ([more info](#)). Any discrepancies between backup and original will be caught and corrected immediately, ensuring that all backups are accurate and accessible right from the start.

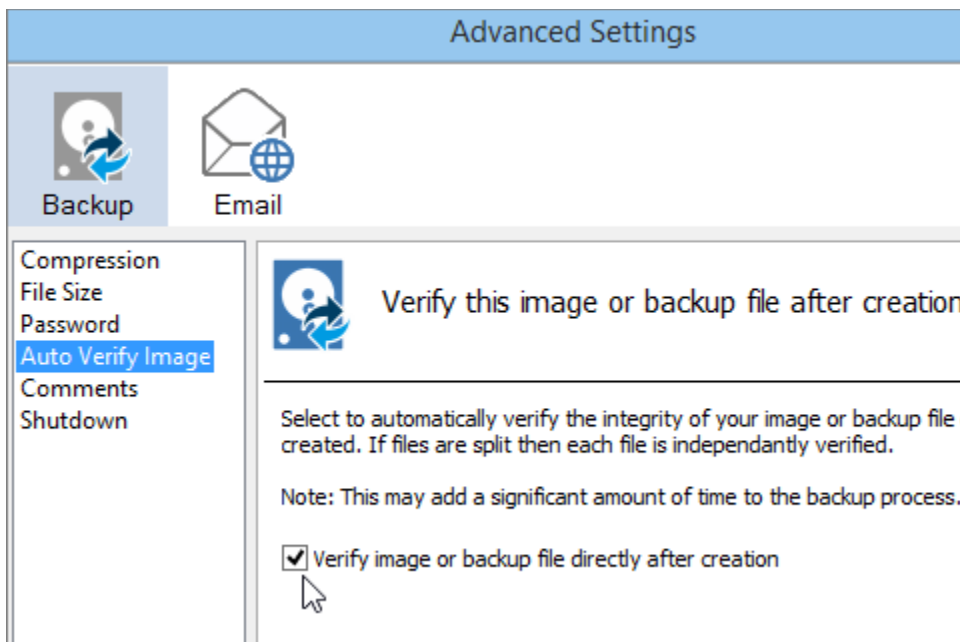


Figure 1: Use your backup tool's *verify after creation* option, if available (shown, Macrium Reflect Home). (Shown: Macrium Reflect Home.)

Note that the verify step can take almost as much time as creating the backup. To avoid this possible additional impact on PC performance, schedule the backup-and-verify process when your PC is least needed — such as in the middle of the night.

Again, not all tools offer this kind of automatic verification — including the imaging and file-by-file backup tools built into Windows. However, one or more of the following methods will work on almost any backup type.

An overview of backup spot-checking techniques

An advantage of spot checks is that they can be run whenever you like — right after a backup has been created or days, months, and even years later. (Yes, backups can go bad; hard drives can hiccup, system maintenance can go astray, hardware or software might change, optical discs can get scratched or otherwise damaged, and so on. The list of potential troubles is long.)

As the name suggests, spot checks do not verify the full contents of a backup set. Rather, it's an approach that relies on *probabilities* — if some of the data files in a backup set are okay, than it's likely they all are.

There are various ways to apply spot-checking; for example, you can check that the archived and original files' timestamps and file sizes match, or check that backups can be opened or restored correctly (typically

to another location so you don't overwrite a current working file). The more files you test successfully, the greater the odds that the backup set is fully usable.

How many files do I spot-check? When I'm trying a new backup method or tool, I check a *bunch* of files to make sure everything's OK. But as time goes on and I become confident of the backup tool, my spot-checks become, er, spottier.

Spot-checking isn't hard and usually takes little time — once you know how. The methods vary depending on whether you're checking traditional file-by-file backups or system images. Let's start with the former.

Spot-checking file-by-file backup sets

Many file-oriented backup tools — including Windows' own — make spot checks simple. They let you browse archived files directly within a backup set, often just as you would with the live files on a standard drive, partition, or folder tree.

Here's how to spot-check the file-oriented backups created by Windows' built-in tools. If you're using a third-party backup tool, it's likely to have similar options and functions.

Windows 8's File History: File History makes near-real-time, incremental backups of files and folders in your Windows libraries (by default, Documents, Music, Pictures, and Videos; see references at the end of this item for more info).

The easiest way to verify File History's operation is with its Restore tool; here's how you access it:

- Click Control Panel/System and Security/File History.
- Select **Restore personal files** from the left side of the dialog box.
- A new window, something like what's shown in Figure 2, will open.

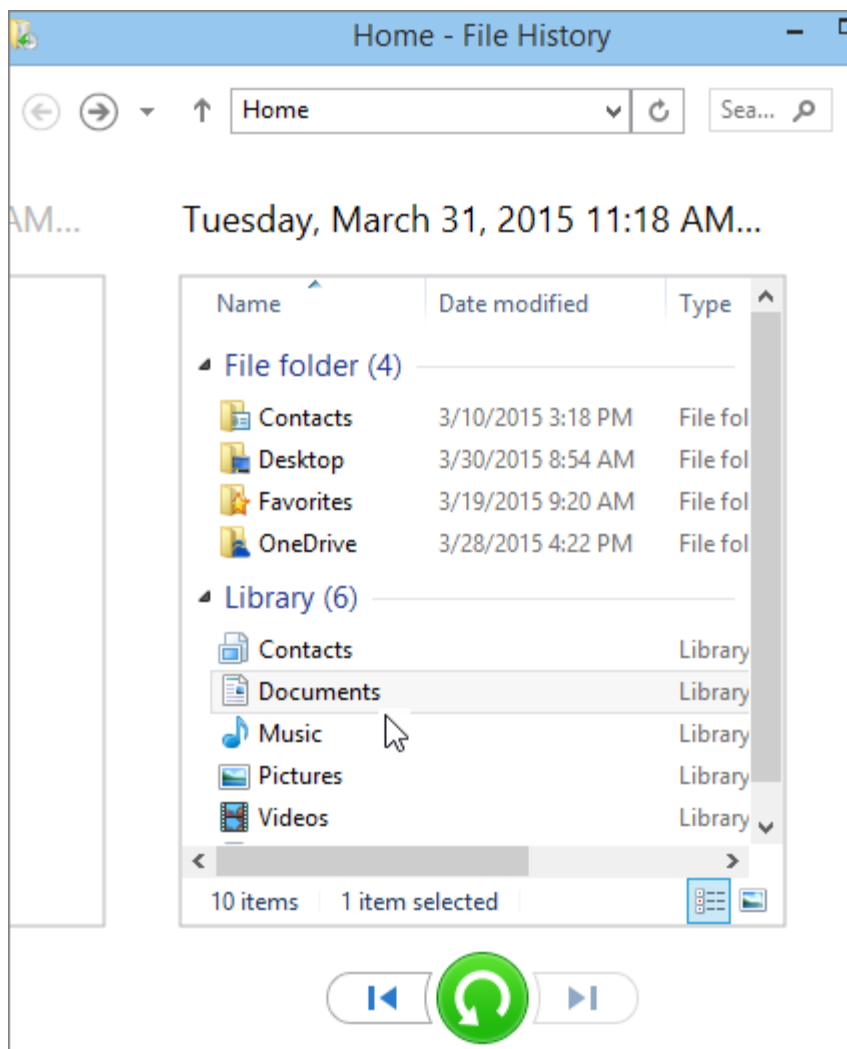


Figure 2. Win8's File History lets you directly view, open, and test-restore files in your backups.

The initial restore window will show the most recently saved versions of your backup files. Use the left arrow at the bottom of the File History window to scroll backwards in time to earlier saved versions.

If you wish to verify the contents of a file, click it (or right-click it and select Preview) — many types of files will open right within File History.

To test-restore a file, right-click it, select **Restore to**, and then select a safe location such as an empty folder or any location away from the original copy on your hard drive. Once the file's been restored, open it normally and verify that its contents are correct.

You don't have to use File History's Restore; you can directly access and explore the archive folders with File Explorer, just as you do with any working folder. The File History archive folder is located on the drive you designated when you first set up File History. By default, it's called — obviously enough — **FileHistory**.

Keep in mind that the direct-access method might be harder to use because the raw backup files lack the organization-by-date structure provided by the File History applet. Use the applet, if you can. For more info, see:

- "Understanding Windows 8's File History" – July 11, 2013, [Top Story](#)
- "Mastering Windows 8's backup/restore system" – Jan. 15 [Top Story](#)
- "Customize File History's backups with ease" – Oct. 9, 2014, LangaList Plus [column](#) (paid content)

Windows 7 and Vista restore: The standard backup tools in Win7 and Vista have a **Restore** option that lets you browse the contents of backups — either by file or by folder.

To access **Win7's** tool:

- Click Control Panel/System and Security/Backup and Restore.
- Click the **Restore my files** button.
- In the Restore Files dialog box, click either **Browse for files** or **Browse for folders** (see Figure 3).

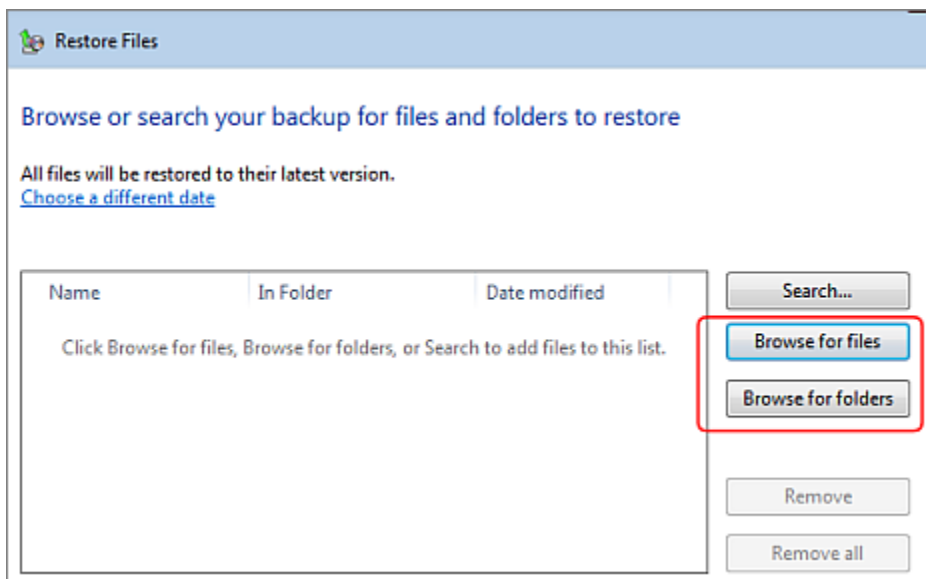


Figure 3. In Win7 and Vista, the Restore tool lets you browse files or folders to ensure that important backups are present, correct, and accessible.

Vista's tool is similar:

- Click Control Panel/System and Maintenance/Backup and Restore Center.
- Click the **Restore files** button.
- When prompted, select the backup set you want to explore.

- Click **Add files** to explore individual files or **Add folders** to explore folders.

Once you've made your selection in either Win7 or Vista, you can view the backup files' sizes and timestamps and compare them with the original files on your hard drive. You also can do nondestructive test restores by following the Restore tool's standard dialog prompts. When you're asked for a location for saving the restored file, choose an empty folder or other safe location away from the original file. Once the file is restored, open it normally and verify that its contents are correct.

In a pinch, you also can navigate directly to the Win7/Vista backup file location using Windows Explorer. The backups will be in whatever backup location you assigned, in a restricted-access folder that usually has the same name as the PC that made the backups. For example, if the backups were made by "Fred's-PC," the folder name will usually be "Fred's-PC" (see Figure 4).

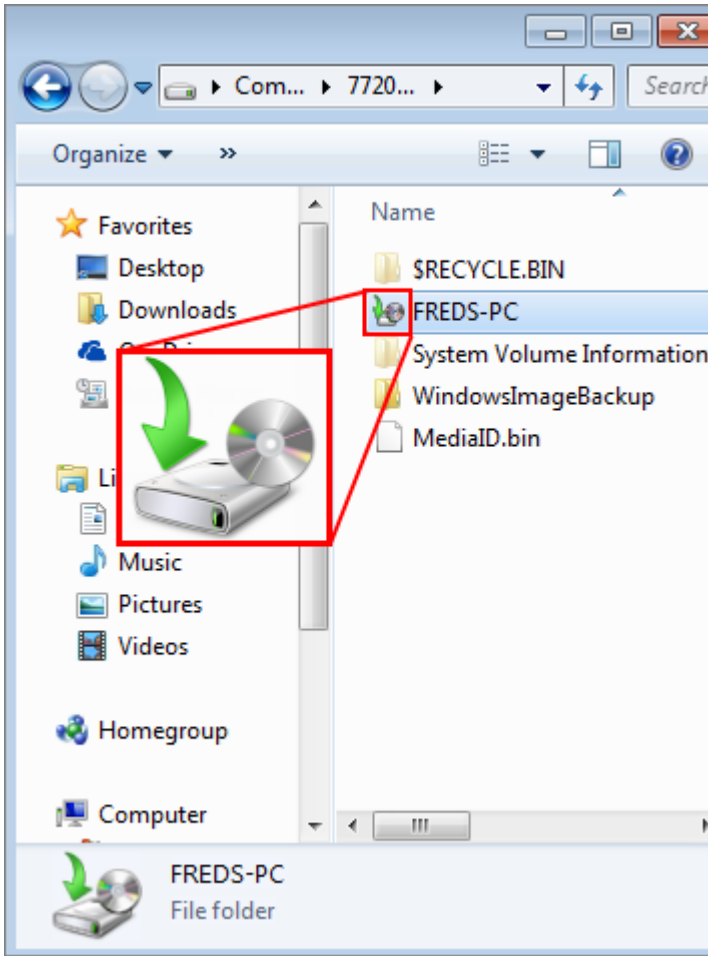


Figure 4. Standard Vista and Win7 backup folders are usually highlighted with a distinctive icon and have the same name as the PC that created the backup.

Access the backup files from an admin account. Right-click the backup folder, select Open, and, if requested, click the Continue button to gain access. You can then navigate the folder contents normally. (Depending on how your system is set up, you might encounter multiple permission prompts.) The actual backup files are usually several folder-levels deep, stored in plain-vanilla, unencrypted **.zip** files. Windows Explorer or any **.zip** tool can access these files.

Although this direct-access method works, it's clumsy and the files are organized in a way that only software could love. For normal backup access, the Restore tool is a better choice.

For more info on Win7 and Vista backup and restore, see:

- "Build a complete Windows 7 safety net" (also includes Vista info) – May 12, 2011, [Top Story](#)
- "A Guide to Windows Vista backup technologies" – MS TechNet [article](#)

Spot-checking system-image backup sets

System-imaging tools are generally intended to back up an entire hard drive, partition, or other discrete chunk of a PC's setup — all at once. When you run a restore, a system image returns *everything* (software, settings, files, and so forth) to the target location in exactly the same state it was in when the image was created.

System images are usually stored as large **WIM** (Windows Imaging Medium; [info](#)) files, **VHD** (virtual hard disk; [info](#)) files, or some other vendor-specific file format.

Most imaging tools give you a way to browse directly inside an image file; often you can navigate the image as if it were a standard drive, partition, or folder tree. You can then run the spot-check verifications mentioned earlier: file timestamp and size, test-restoration to a safe location, and, in some cases, opening backed-up files directly.

Image checking is typically where third-party tools far outshine Windows' capabilities, providing options that are much more polished and easy to use. For instance, Macrium Reflect's Home Edition lets you open an image or backup in Windows Explorer with just a couple of clicks, as shown in Figure 5.

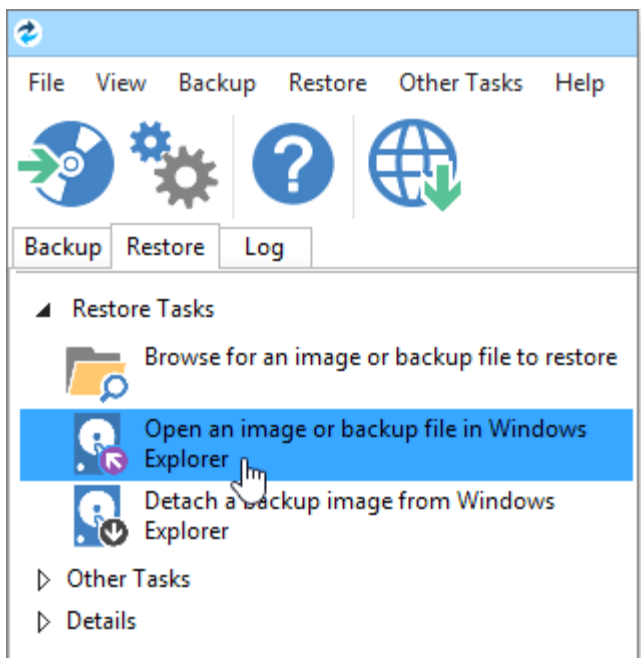


Figure 5. Some third-party tools let you easily open backup and image files for direct exploration via Windows Explorer (shown, Macrium Reflect Home).

Microsoft provides tools that perform similar functions, but these complex command-line programs with dozens-to-hundreds of available option switches are much harder to use. They're also aimed more at business IT operations than at end users.

For example, Microsoft's **ImageX** (Image eXtract; [more info](#)) is intended for working with the VHD image files produced by the **Windows Complete PC Backup and Restore** utility included with Business, Ultimate, and Enterprise editions of Vista. **DISM** (Deployment Image Servicing and Management; [info](#)) is intended for Win7's VHD image files and Win8's WIM files. However — and confusingly — there's considerable overlap in what the tools can do and the file types they support.

Although there's nothing to make these tools a breeze to use, there are add-ons and alternatives that can provide a more intuitive graphic interface — see the following list. There's also plenty of documentation available online. That's good, because you'll probably need it! (As I did.) Here's more info:

Win8/7's DISM:

- "WADK: Windows Assessment and Deployment Kit for Win8" (includes DISM; also runs on Win7) – Microsoft info and download [page](#)
- "Mount and modify a Windows image using DISM" – TechNet [article](#)
- "Mounting WIMs with DISM" – North Carolina State University [tutorial](#)

- "Windows 7 DISM — how to mount, manage, and service WIM images" – 4sysops [article](#)

Vista's ImageX

- "Windows Automated Installation Kit (WAIK) user's guide for Windows Vista" (WAIK includes ImageX) – Microsoft info and download [page](#)
- "Walkthrough: Service a virtual hard disk image offline" – TechNet [article](#)
- "ImageX and WIM image format" – [TechNet article](#)

Other WIM/VHD tools, add-ons, and more:

- "Windows Explorer context menu for managing WIM files" – Anything about IT [blog](#)
- "Mounting WIM images from Windows Explorer" – [WindowsNow blog](#)
- "VHD Attach 4.01" – Josip Medved's [site](#)
- "Open/Extract WIM file with freeware on Windows/Mac/Linux" – [e7z.org page](#)
- "Convert WIM files to VHD or VHDX" – [TechOnTip blog](#)

A nondestructive, full test for backups

The gold standard of backup testing is, of course, a full, live, for-real restore.

This once required access to a spare PC because no one in his right mind would choose to test-restore a backup or image to its original location, overwriting — and destroying — the data there.

Today's large hard drives offer a more convenient solution: a virtual PC (VPC).

The idea is simple: You create a new, empty, VPC whose virtualized hardware roughly mimics the real, physical PC that produced the backup you wish to test. (No, the VPC drive doesn't have to be full-sized.)

You then boot the VPC with your imaging tool's emergency boot disk (aka recovery disk, restoration disk, or whatever the bootable medium is called) and restore the backup or image to the VPC's hard drive.

Alternatively, some virtual PC software can directly read a VHD file; you can then mount the image directly inside a VPC, in one step.

Note that a VPC-based full-backup test requires the *temporary* use of a substantial amount of disk space — but maybe not as much as you might think.

You can ballpark-estimate the minimal amount of space you'll need by checking the actual, physical hard drive that produced the image. (Right-click the drive and select Properties.) Figure 6 shows an example. Obviously, the VPC's hard drive must be at least as large as the total space used by the original files. But you'll also need a skosh more room for hidden and system files.

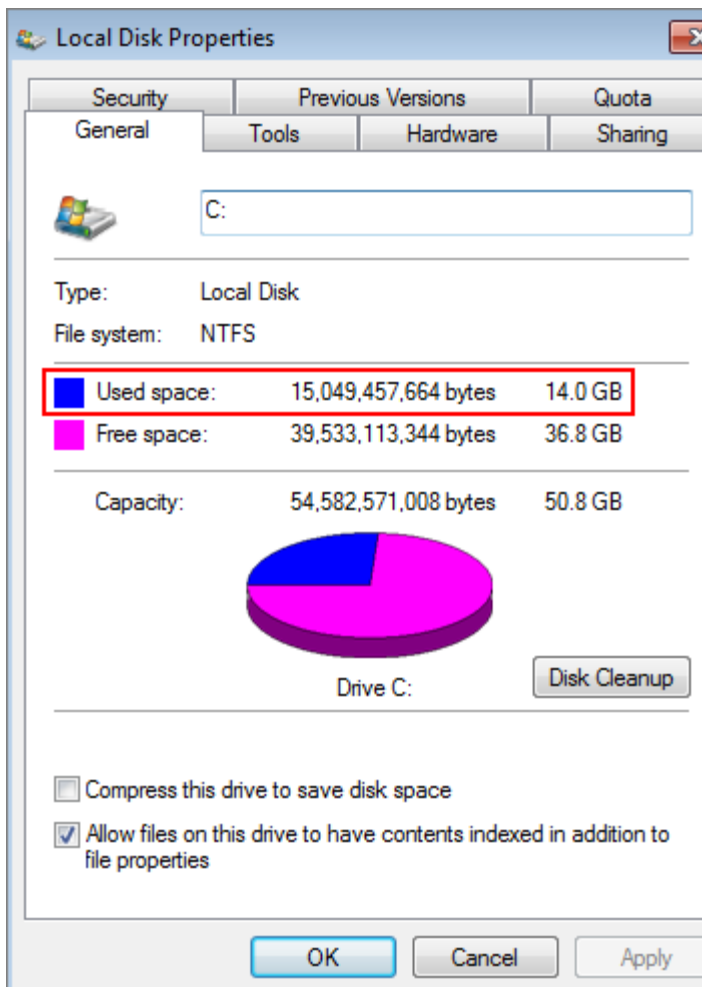


Figure 6: A VPC's hard drive needs to hold the actual files in the backup plus some system files — not the entire, original drive space.

In the above example, the original files occupy around 14GB of disk space. At a minimum, a VPC's hard drive would need to be around 20GB to accommodate the original files plus hidden and system files — and include a bit of breathing room.

You can place the VPC's hard drive wherever you have free, physical disk space — even on an external drive.

Most image-restoration tools will check the size of a target drive and adjust the backup's partition (or partitions) to suit. If your test-restore fails due to lack of space on the VPC drive, just wipe out the VPC and try one with a larger drive. Remember: You'll get this space back when testing's over and you delete the VPC.

A word of warning: A VPC will not and cannot be 100 percent identical to the physical PC that produced the backup or image. For example, there will be driver mismatches that will likely cause glitches and hiccups when you try to boot the VPC. The VPC will also likely fail Microsoft Activation because the Windows Product Key is already in use on the real PC. (Two or more installations using the same key violate the license.)

These aren't show-stopping issues because you're producing a temporary setup — you're not going to use the VPC for a permanent, fully functional clone. You're just ensuring that the image can be restored correctly to a hard drive.

If the VPC boots correctly, you then can use Windows to check that your most important files were restored and are usable. If the VPC won't let you get that far, you still can use an external tool — such as an emergency boot disk — to explore the VPC's hard drive and ensure that key files were properly restored — with the correct timestamps and file sizes.

If your restore passes muster in the rough-fit environment of a VPC, you can have some confidence that it will work with the PC configuration the files came from.

After your restoration test, wipe out the VPC and delete its virtual hard drive. Again, you'll recover the borrowed hard-drive space.

To create VPCs, I use Oracle's VirtualBox (free; [site](#)) because it works with all current Windows versions and editions, whether they're 32 or 64 bits. Plus, you can't beat the price.

There are, of course, other virtualization tools available. Users of 64-bit Win8 Pro or Enterprise editions can use the built-in copy of the excellent Windows Hyper-V Client (MS [info](#)). Other users might prefer a commercial, IT-oriented tool such as VMware ([site](#)).

It's not hard to set up a VPC; you can get the gist of it by reading the following:

- "Step by step: How to safely test-drive Win8" – March 14, 2012, [Top Story](#)
- "How to safely test-drive Win10 — step by step" – Oct. 16, 2014, [Top Story](#)

A backup you can't restore is no backup at all. And you don't want to learn that hard lesson when you really need your backups. Take the time now to ensure that you can successfully restore both individual files and your entire system. Have confidence that you'll never lose important data.