OTTAWA PC NEWS

Volume 30, Number 6 June 2013

PRODUCT REVIEW

Win+X Menu Editor for Windows 8

by Chris Taylor

Windows 8 has a split personality. There's the old familiar desktop, and the new Metro interface – now officially known as the *Modern UI*. Whether you like it or not, you *will* use both.

Two distinct personalities

The desktop is where all non-Metro apps run. This means pretty much all the apps I use, such as Corel PaintShop Pro, Total Commander, Google Earth, FotoSketcher, Microsoft Office, Adobe Photoshop Elements, Foxit Reader, Irfanview, etc. And it includes millions of other Windows applications.

Metro-style apps run full screen in the Metro interface. You can't run them in arbitrarily-sized windows. You can't overlap windows – a "feature" last seen in Windows 1.0. In a nod (I guess) to the fact that for over 27 years people have worked with multiple Windows applications visible at once, Microsoft allows two applications to be visible at once, but only side-by-side in a strict ¼ - ¾ division, even if you are on a desktop computer with a 26" screen. I've seen Microsoft demos where they monitor an app such as email, weather, or stock quotes in the ¼ screen while working on a document in the ¾ window. They showed how easy it is to quickly switch the monitored window to full screen or ¾ size so you can more easily interact with it. Want to see three apps at once? Sorry, you are out of luck in Metro.

I think the Metro interface on a desktop computer is just dumb and inefficient. Same goes for any computer with a keyboard, mouse, and a screen over 10". For the foreseeable future, I see almost all my time being spent with desktop applications, which by definition only run on the Windows desktop, not the Metro interface.

Microsoft taketh away

Which would be fine … if Microsoft hadn't neutered the desktop. I would have much preferred if Windows 8 allowed full Windows functions from both Metro and the desktop. There's no reason why they couldn't have designed both Metro's *PC Settings*, and the desktop's *Control Panel* to have complete and identical functionality. There is no reason why they couldn't have left a Start button on the desktop. A button that could have optionally synchronized with the contents of the Metro Start screen.

But Microsoft didn't.

Quick Link menu

Microsoft did implement a very nice feature in both the Metro and desktop environments – the Quick Link menu, which gives easy access to many admin tools. From the Metro interface or the desktop, press the Windows logo key+X and the Quick Link menu will pop up. With a mouse – in either interface – point to the bottom-left corner. When the little Start square appears, right click and the Quick Link menu will appear. Interestingly, it doesn't appear possible to use a touch gesture to access the Quick Link menu in either Metro or desktop mode.

It's clear from the list of items on the Quick Link menu *(see Figure 1 on page 6)* that it's intended as a power user's tool. I think power user tools are great! They bypass clutter and roundabout ways of doing things and let you cut to the chase.

I like some of the choices Microsoft put on the Quick Link menu, but not all. I can get a run dialog box by pressing Win+R. I can get File Explorer by pressing Win+E. I can start a search by typing at the Start screen. Of course, being a power user tool, the Quick Link menu is highly customizable so I can remove entries I don't want and add my own.

Right?

Unfortunately, no. Oddly, it is completely *un*-customizable!

(Continued on page 6)

Inside this issue:

PIZZA at 6:30 pm, WEDNESDAY, June 12th, 2013

June Raffle

Courtesy of McAfee Canada, we have a copy of **McAfee All Access 2012** *(to be confirmed).*

"All your devices. All your stuff. All protected." That is how McAfee describes All Access 2012. This powerhouse gives you complete anti-virus, anti-spyware, anti-phishing, anti-spam, anti-bot, 2-way firewall, safe web searching, encryption, wireless network security, digital file shredding, web content filtering, URL shortening, social network monitoring, on-line activity monitoring, and more.

And this one-user license will do this for all the devices you own - PCs, laptops, Android tablets, Macs, and smartphones (iPhone, Android, BlackBerry, or Symbian.)

McAfee All Access 2012 is valued at $100.

Tickets are, as always, a good deal at $1 for one, a great deal at $2 for three or the unbelievable bargain of $5 for ten!

May Prize Winners

Eldon Gaw was the winner of the raffle at the OPCUG meeting on May 8th. He took home a copy of McAfee Total Protection 2013.

Thanks again to McAfee Canada for the prize donation.

Coming Up…

▶Wednesday June 12th, 2013

PIZZA PARTY (6:30 pm)

For the SIXTH straight year, the OPCUG is pleased to host a Pizza night to thank its members for their continued support. Please come early to ensure you have a choice of several popular varieties of Pizzas.

As usual, we will also supply several varieties of soft drinks, plus water and dessert.

The food will arrive at 6:30 pm under the big tent in the front yard of the Canada Science and Technology Museum. Guests are welcome.

NOTE: The museum now charges for parking.
RATE: $1 per half hour, maximum $6 per day

At 7:30 the regular meeting will take place *(see bottom next page)*

2013 CALENDAR

Meetings	Date	Time and Venue
OPCUG General Meeting	Wednesday, June 12th	7:30 p.m. Auditorium of the **Canada Science and Technology Museum**, 1867 St. Laurent Blvd. http://www.sciencetech.technomuses.ca/english/index.cfm
Beginners' SIG	Wednesday, June 12th	Immediately following the OPCUG General Meeting.
Linux / Open Source SIG	Wednesday, June 12th	Immediately following the OPCUG General Meeting.
Beer BOF (Wing SIG East)	Wednesday, June 12th	10:00 p.m. (after all other SIGs) at Liam Maguire's, St. Laurent Blvd. at Innes Rd.

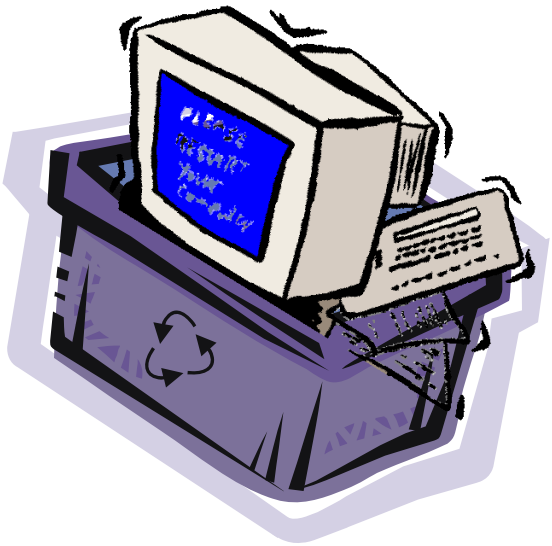
Please note that unless otherwise noted, SIGs meet at 9:00 p.m. (immediately following the OPCUG General Meeting).

OPCUG eWaste Event

On June 12th, 2013, at the Canada Science and Technology Museum, the OPCUG will be partnering with the KRC (Knights Refurbishing Computers - http://www.krc-refurb.org/) INC in an eWaste collection, under the auspices of the Ontario Electronic Stewardship Council (http://www.ontarioelectronicstewardship.ca/), and their agent, Evolu-tic (http://www.evoluticoutaouais.ca/index_en.php/) of Gatineau. Items that can be reused for the KRC program will be retained and refurbished, while all other older or not-useful electronic items will be taken to the processing plant and properly disposed of, according to the very strict OES guidelines (http://www.ontarioelectronicstewardship.ca/program/accepted-electronics). Everyone is invited to rid their homes of items no longer required.

For both KRC and OPCUG, there will be some revenue generated as well. KRC is provided with the princely sum of $150 per metric tonne of items accepted for disposal - so the big old heavy TVs and such are happily taken away; the revenue earned will be split with the OPCUG.

The OPCUG thanks the museum for the permission to hold the event and to Doug Drouillard of the KRC for providing all the technical support.



Wednesday June 12th, 2013
REGULAR MEETING (7:30 pm after the Pizza—*see previous page*)

Speaker: Hugh Chatfield, President - CyberSpace Industries 2000 INc.
Topic: Is it Canada's turn to implement e-invoicing with UBL?

Today, over 190 countries are implementing e-invoicing networks using the OASIS Universal Business Language (UBL) as the means for expressing the content of an e-invoice. UBL 1.0 was release in 2004, and is now at release 2.1 where UBL now describes over 65 different business documents (Invoice, PO, Shipping record, etc) that are typically exchanged between two business partners.

The country of Denmark was an early adopter of UBL, legislating the use of UBL for invoicing the government, and providing an infrastructure (Nemhandel - "Easy Trade") for all businesses large and small. Today a large percentage of the countries businesses use Nemhandel for both B2G and B2B invoicing. The EU moved to implement UBL technology for the 17 countries that make up the EU. The idea is to provide an opportunity for any business in the EU to work with any government/business in the EU and be able to invoice directly in an electronic form.

Unfortunately Canada has been extremely slow in moving in this direction. The talk asks the question "Is it Canada's Turn to Implement an e-invoicing Infrastructure?", and explores UBL and what it would take for Canada to do so.

W. Hugh Chatfield
President - CyberSpace Industries 2000 INc.
XML Training and Consulting
Documentary/Multimedia Development
http://CyberSpace-Industries-2000.com
UBL is in your future: http://goUBL.com

ARTICLE

Malware false positives

by Chris Taylor

Antimalware programs are having a tough time. Most focus on positive malware identification through signature files of known malware. According to the *Sophos Security Threat Report Mid-Year 2011*, there are 150,000 new, unique pieces of malware *per day*. So it's easy to see how antimalware programs are becoming less effective; it's just too hard to keep up.

While not as bad as missing an actual malware infected file, false positives – when a file is mistakenly identified as malware – can be a problem.

False positives won't compromise your privacy. They won't cause your computer to become part of a botnet that attacks other computers or delivers spam. And they won't corrupt your data files.

But they may cause problems for you. Imagine if a false positive happens to be the executable for your favourite word processor. The file gets quarantined or deleted and your word processor no longer works. Or what if it is a critical file for the operation of Windows itself? Maybe Windows won't boot when the file is removed. Ouch!

False positives rare

But rare does not mean they don't happen…

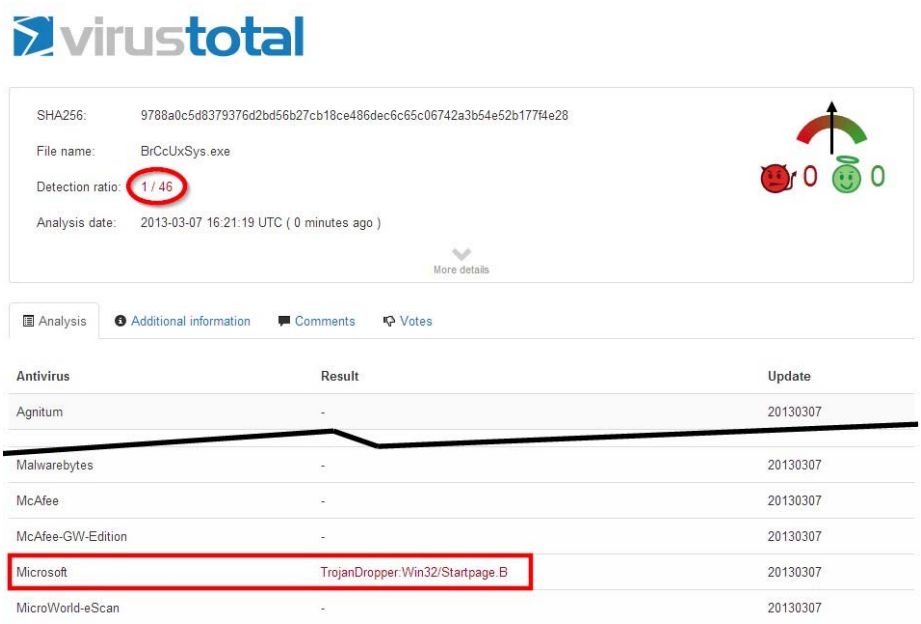
In February I bought a new laser printer. I installed the driver and the companion programs that came with the printer. And I started happily using the printer. Nice printer, by the way – a Brother MFC-7460DN.

On March 7th Microsoft Security Essentials decided one of the files (BrCcUxSys.exe) installed as part of the package was malware; *TrojanDropper:Win32/Startpage.B*. A dropper program is one that can allow attackers to install any other program on your computer. Definitely not good.

But it seemed odd to me. I doubted that the original program on the CD was infected. Not impossible, but unlikely. I also thought it unlikely that a program in this particular directory got infected after the installation.

VirusTotal to the rescue

Microsoft Security Essentials quarantined the file. I retrieved it and uploaded it to VirusTotal.com, which checks files using 46 different anti-malware programs with up-to-date signatures. Of the 46, only Microsoft identified it as malware. VirusTotal.com first saw this *exact* file (a SHA-256 hash pretty much guarantees uniqueness) almost 2 years ago.



Only Microsoft reports it as malware

I was convinced at this point that it was a false positive. But I wanted to see how Microsoft would react to a report of a false positive. I submitted a copy to Microsoft's Malware Protection Center. For the heck of it, I also submitted a copy to McAfee's AVERT Labs.

Within 10 minutes, an email from McAfee AVERT Labs said there was no evidence of malware. Within an hour, Microsoft emailed me to say there was no evidence of malware. So false positive it was.

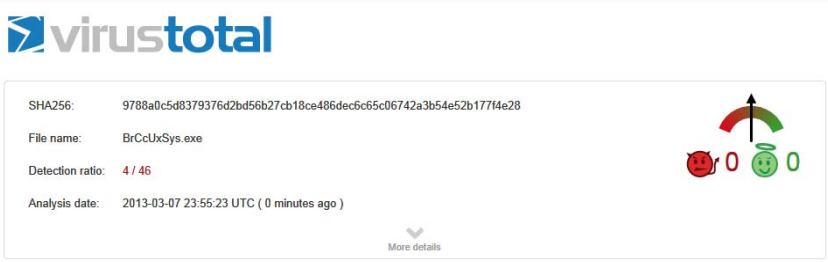
(Continued on page 5)

Malware false positives *(Continued from page 4)*

Curious thing happens…

Later that day, I resubmitted a copy to VirusTotal.com. Microsoft was no longer calling it malware. Kudos to Microsoft for quickly rectifying the situation.

But four other companies were now saying it contained malware; Avast, Emsisoft, G Data, and Ikarus!



Four others report it as malware

Over the next couple of days, three of them stopped calling it malware. Emsisoft kept insisting it was malware for another 10 days.

Along the way another company, Antiy Labs, started calling it malware.

How and why would five other companies come to have a false positive on this same file? Are they blindly sharing malware signature files? If so, why would they identify it as malware days or weeks after Microsoft fixed their signature files?

Antiy Labs had insisted the longest that the file was malware. I sent them an email asking them for clarification but never got a response.

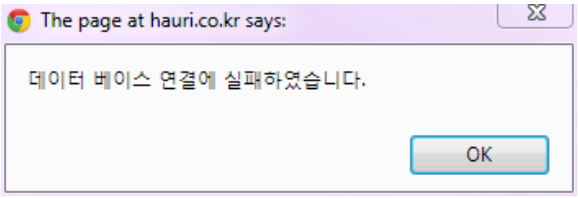
On March 24th, eSafe started identifying it as malware. I emailed SafeNet, the company that makes eSafe. I explained the situation and asked if they would like a sample of the file so they could verify it was not malware and correct their signature files. They replied that they had no record of my owning a copy of eSafe and was therefore not entitled to support. With support like that, I will not be rushing out to buy a copy of eSafe, that's for sure!

On Mar 28, VBA32 from VirusBlokAda in Belarus started calling it "Trojan.FakeMS.clr" which looks suspiciously like they are copying from Antiy Labs, which calls it "Trojan/Win32.FakeMS.gen". I sent them an email asking if I could send them a sample of the file so they could verify it was a false positive and correct their signature files. They never responded.

On March 29, Antiy Labs finally stopped calling it malware.

On April 4, ViRobot from Hauri started saying it was infected with Trojan.Win32.A.Black.1204224.E. I went to the ViRobot web site to report it as a probable false positive and submit a sample. The site insisted I use a specific program to submit samples. To be safe, I submitted the program – InnoMP_Win.exe – to VirusTotal.com and imagine my surprise when it was reported by TrendMicro Housecall as infected with TROJ_GEN.F47V0808. I reported the suspected false positive to TrendMicro, who were very responsive and corrected the false positive by April 6th.

Now fairly certain Hauri's file uploader didn't contain malware, I submitted a copy of BrCcUxSys.exe. In the submission report, I clearly indicated why I was fairly certain the detection was a false positive. Within 10 minutes, a reply said the file was infected. The email included a link on the malware name, so I clicked it to see more details. I was taken to a web site http://hauri.co.kr/virusInfo/Virus_detail.html?name=Trojan.Win32.A.Black.1204224.E which gave a blank page and a pop-up that clearly told me what the problem was.



Clear messaging from Hauri

The email told me "Please do not reply to this e-mail as it is being sent from an unmonitored e-mail account. To contact us, use a method indicated in this e-mail.", but since the email did not contain any information about another way to contact them, I gave up.

It would appear a false positive may be hard to clear up totally. Through this whole fiasco, only Microsoft, McAfee and TrendMicro responded in what I would consider a good, responsible fashion. Avast, Ikarus and G Data (although I never contacted them) corrected their signature files quickly. Well done to these six companies. A pox on Antiy Labs (AVL), SafeNet (eSafe), VirusBlokAda (VBA32), and Hauri (ViRobot). These companies either did not respond or responded totally inadequately. As of April 7, a full month after the fiasco began, eSafe, VBA32 and ViRobot still say the file contains malware.

♦♦♦

Win+X Menu... *(Continued from page 1)*

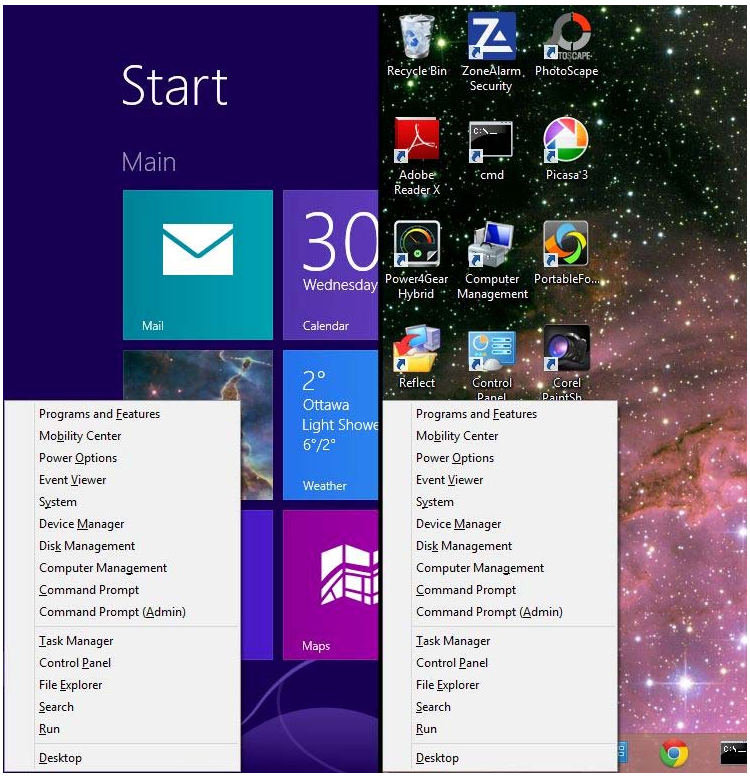
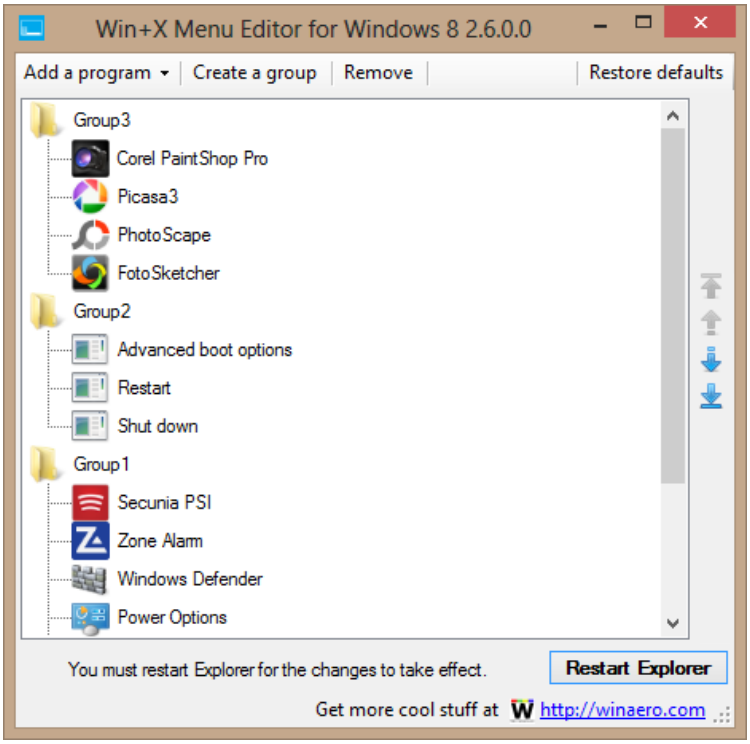


***Figure 1. Quick Link menu in Metro** (left) **and on the desktop** (right)*

But a company called WinAero figured out how to do it. Enter *Win+X Menu Editor for Windows 8* (what a mouthful!). This great little free app allows you to customize the Quick Link menu.



Win+X Menu Editor is very simple to use. Some presets for Windows tools that power users often use are available with a couple of clicks. It's easy to add any other executable you would like on the menu. Up and down arrows let you re-order items. One click will delete entries you don't want.

Beware – there is no undo option and there is no save option (saving is immediate and automatic). There is an option to reset to the default menu. You have to restart Explorer in order to see changes you have made to the Quick Link menu. Win+X provides a handy button to do this.

There are a few enhancements I would like to see: the ability to save a particular configuration; drag & drop of a shortcut or program to have Win+X create a menu entry; and the ability to re-order menu groups.

But all these are minor quibbles. For me, *Win+X Menu Editor* is a great way to make up for the missing Start button on the Windows 8 desktop and makes Windows 8 more useable. Kudos to WinAero for making this great utility available for free!

My modified Quick Link menu

Bottom line:

Program: Win+X Menu Editor for Windows 8
Cost: free
Publisher: WinAero
http://winaero.com/comment.php?comment.news.30

OPCUG Free Software Guide – Part 41

Compiled by Alan German and Chris Taylor

This guide features an annotated list of free computer programs. The software mentioned has not been reviewed (except where noted) nor have any tests necessarily been conducted. Consequently, no guarantees are provided that the individual programs will perform as described. Rather the list of available software is provided for the information of our members who may find one or more of the programs useful.

LibreOffice
This office suite is a fork of OpenOffice. Actively maintained by the open-source community and The Document Foundation, LibreOffice contains applications for word processing, spreadsheets, presentations and database management.
Current Release: Version 4.0.2.2
Web Site: http://www.libreoffice.org/

Arsclip
The Windows clipboard is very useful but it only handles one item at a time. Wouldn't it be nice if you could store multiple clips - permanently? Arsclip lets you do just that. This open-source utility monitors the clipboard and keeps track of multiple entries. View all the entries in a pop-up window, make your selection, and paste it into the current application.
Current Release: Version 4.9
Web Site: http://www.joejoesoft.com/vcms/97/

Menu Uninstaller Lite
This program adds an "Uninstall" option to the (right-click) context menu for any shortcut on your computer, letting you easily remove a program without going through the Windows Control Panel.

Web Site: https://sites.google.com/site/leizersoftware/home

Expired Cookies Cleaner
Internet Explorer stores cookies but never deletes them even they have expired. This little utility searches for such useless files and removes them from your computer.

Current Release: Version 1.03
Web Site: http://preview.tinyurl.com/la4a2

Privatefirewall
This personal firewall includes host intrusion prevention software (HIPS) to protect both 32- and 64-bit Windows machines from malware and unauthorized use. The program ranks among the best performing desktop defense applications tested against the industry's most rigorous leak, general bypass, spying and termination tests.

Current Release: Version 7.0.29.1
Web Site: http://preview.tinyurl.com/yep36c3

PhotoFiltre
This complete image retouching program allows you to do either simple or advanced adjustments to an image and apply a vast range of filters. It is simple and intuitive to use, and has an easy learning curve.
Current Release: Version 6.5.3
Web Site: http://photofiltre.free.fr/frames_en.htm

PC-Wizard
The developers claim that this utility is among the most advanced system information programs on the market. The program will detect your computer's hardware, analyze any problems, display a wide range of information, and even benchmark system performance.
Current Release: Version 2012.2.11
Web Site: http://www.cpuid.com/softwares/pc-wizard.html

YouTube Downloader HD
This free tool will download a video from YouTube and save it to your local computer. Video files can be converted to AVI video format or to MP4.
Current Release: Version 2.9.6
Web Site: http://www.youtubedownloaderhd.com/

LiberKey
Do you have a spare USBkey that you don't know what to do with? How about turning it into a portable utilities powerhouse? Liberkey offers three sets of freeware applications – the basic, standard, and ultimate suites – ready for downloading and using right from the stick.
Current Release: Version 5.7
Web Site: http://www.liberkey.com/

OTTAWA PC NEWS

Ottawa PC News is the newsletter of the Ottawa PC Users' Group (OPCUG), and is published monthly except in July and August. The opinions expressed in this newsletter may not necessarily represent the views of the club or its members.

Member participation is encouraged. If you would like to contribute an article to Ottawa PC News, please submit it to the newsletter editor (contact info below). Deadline for submissions is three Sundays before the next General Meeting.

Group Meetings

OPCUG meets on the second Wednesday in the month, except July and August, at the Canada Science and Technology Museum, 1867 St. Laurent Blvd, Ottawa. Meetings are 7:30–9:00 p.m. and Special Interest Groups (SIGs) go until 10 p.m.

OPCUG Membership Fees:	$25 per year
Mailing Address:	3 Thatcher St., Nepean, Ontario, K2G 1S6
Web address:	**http://opcug.ca**
Bulletin board—The PUB (BBS)	**http://opcug.ca/default.htm**
Follow us on Twitter:	**http://twitter.com/opcug**

President and System Administrator		
Chris Taylor	**chris.taylor@opcug.ca**	613-727-5453
Meeting Coordinator		
(Mr.) Jocelyn Doire	**jocelyn.doire@opcug.ca**	
Treasurer		
Alan German	**alan.german@opcug.ca**	
Secretary		
Gail Eagen	**gail.eagen@opcug.ca**	
Membership Chairman		
Mark Cayer	**mark.cayer@opcug.ca**	613-823-0354
Newsletter		
Brigitte Lord (editor/layout)	**brigittelord@opcug.ca**	
(Mr.) Jocelyn Doire (e-mail distribution)	**jocelyn.doire@opcug.ca**	
Public Relations		
Morris Turpin	**PR@opcug.ca**	613-729-6955
Facilities		
Bob Walker		613-489-2084
Webmaster		
Brigitte Lord	**opcug-webmaster2@opcug.ca**	
Privacy Director		
Wayne Houston	**privacy2@opcug.ca**	
Special Events Coordinator		
Bob Gowan	**bob.gowan@opcug.ca**	
Beginners' SIG		
Chris Taylor	**chris.taylor@opcug.ca**	613-727-5453
Linux / Open-Source SIG		
(vacant)		

OPCUG

Users helping users

Reduce, Reuse, Recycle

Bring your old computer books, software, hardware, and paraphernalia you want to GIVE AWAY to the General Meetings, and leave them at the table near the auditorium's entrance. Please limit magazines to publication dates of less than two years old.

You may TAKE AWAY any items of use to you.

Any items left over at the end of the meeting have to be taken back home by those who brought them in.