Trails End Computer Club

Bulletin for the month of JUNE 2013

MONTHLY MEETINGS **EACH Wednesday FOLLOWING THE FIRST MONDAY** Library Room **Program or Lesson** 9:30 - 10:30 **One on One Help** 10:30-?	**SPECIAL INTEREST GROUPS:** If you would like to meet in a small group to discuss special computer related subjects or form a Special Interest Group lets discuss it. Our bulletin is also available on line by visiting tecc.apcug.org and clicking on bulletin.	**Our monthly program or lesson is intended to be of interest to all computer users. Following the program an allotment of time will be available for one on one help to those who want a better understanding of something done during the presentation.**

Upcoming Events

Wednesday June 5, 2013 Meeting
9:15 AM Set up your computer
9:30 AM Lesson
10:30 AM One on One help

What Has Your Computer Been Doing? Free Utility Shows All

by Ira Wilsker

WEBSITES:
http://www.nirsoft.net
http://www.nirsoft.net/utils/computer_activity_view.html
https://www.techsupportalert.com/content/nifty-way-find-out-what-your-windows-computer-has-been-doing.htm

Many of us have encountered frustrations with our computers. Sometimes it appears that running programs crash or otherwise cease functioning without explanation. On older computers, most notoriously those running Windows XP, a cryptic "Blue Screen of Death" (BSOD) sometimes appears when there is a crash of some type, often displaying nonsensical error codes that require extensive research to decode. Some suspicious computer users believe that others are accessing their computer, running unauthorized software or malware. Other wary users may find it interesting seeing what other people may have done on a particular computer, and what programs they may have run, what documents were viewed, and when (what time) the computer was booted and shut down. If a

computer was infected by malware, it may often be of great interest to see what was being run on the computer at the time of infestation, and even identify the malware and its payload. This, and more, can be readily displayed by a tiny, free utility, LastActivityView.

LastActivityView is one of dozens of small free utilities published by a feisty software engineer, Nir Sofer, on his website at www.nirsoft.net. Nir personally writes all of his own software in his spare time, and makes it available to all for free. Many of his utilities are given the highest ratings by a variety of web services and computer publications; all of his software is free of advertising and other pesky irritants, making it popular among his huge and loyal user base. In his spare time, Nir personally maintains his website and updates his software, as well as creates new utilities. One of his newest titles, LastActivityView has caught the attention of computer technicians, forensic experts, hobbyists, and others who really want to know what has really been running on a computer, and when the computer was accessed.

Windows users may be passively aware that their computers save extensive, but often invisible files, about what they have run; LastActivityView has the capability to read these historical files and display additional information about many of the computer's activities. On my primary computer, this record starts on the day it was manufactured, and documents everything that I have done since I first powered it on after removing it from its box. Every piece of software that I ever installed or uninstalled is listed, including date, time, description, filenames, path on the hard drive, and other information. Every boot, shutdown, crash, and other event was also duly recorded. In addition to simply displaying a huge file with all of my computing activities, LastActivityView also has the power to provide additional information for many of the items listed. LastActivityView also can display detailed information about program interactions, and conflicts that caused software and hardware crashes.

The actual program file itself is tiny, only about 100k in size, and requires no installation. It is totally portable, and can be run from any Windows connected device. The LastActivityView program, an exe file, is one of only three components included in the 64k ZIP (compressed) file downloaded from NirSoft; the other two items in the ZIP file are a small "readme.txt" file with simple instructions and other information, and a standard format Windows Help File (chm format) that can be opened with any version of Windows, and displays detailed help and other information. I downloaded the zip file, and using Windows native utility, "unzipped" or uncompressed it into a new directory that I created for it. Total space required for all three files is a miniscule 130k of drive space. I also copied the files to the USB flash drive that I always have on my car keychain, so I can use it whenever and wherever needed.

According to the included readme.txt file, " LastActivityView is a tool for Windows operating system that collects information from various sources on a running system, and displays a log of actions made by the user and events occurred on this computer. The activity displayed by LastActivityView includes: Running .exe file, Opening open/save dialog-box, Opening file/folder from Explorer or other software,

software installation, system shutdown/start, application or system crash, network connection/disconnection and more... " The file created by LastActivityView can be quickly exported in a variety of formats that can be utilized by a variety of other programs that can read csv, tab-delimited, xml, or html formatted information. A simple copy and paste can also place information in other programs, such as an Excel spreadsheet. For those who may wish to customize the execution of LastActivityView, several command line options are available, but most users will find that simply running the file without any additional commands will provide comprehensive and useful information.

In addition to the obvious tracking of what was run on a computer, LastActivityView can also provide additional and valuable information. I was able to prove this to myself when I examined some recent logs, looking for software crashes and conflicts. One of several reasons why I do not use Internet Explorer as my primary browser is that for some reason, it sometimes crashes when open. According to the report, my most recent software crash occurred on May 17, at 9:11:07pm when Internet Explorer, version 10.0.9200 crashed. By right-clicking on the line in the log showing the crash, an options menu appeared which displayed what additional information could be shown. I first selected "Properties", which displayed the Action Time, Description (Software Crash), File Name, Full Path (location on hard drive), and what was most important to me, More Information. Similar information can be displayed as a webpage in HTML by selecting "HTML Report - Selected Item". The More Information line showed precisely the software conflict that caused the crash; in this particular case, according to the display, there was a memory conflict between IEXPLORE.EXE 10.0.9200.16576 and TmBpIe32.dll, which is a module or component of my TrendMicro security suite. Now that I have recorded this conflict, it would be easy to determine whether this is a one-time anomaly or a continuing problem that requires attention and remediation. Doing a quick online search for TmBpIe32.dll, I found that this file is a Trend Micro Browser Plug-In for Internet Explorer that is designed to protect the browser from exploitation. According to Wikipedia, "A browser exploit is a form of malicious code that takes advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach browser security to alter a user's browser settings without their knowledge. Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, and other Web technologies and cause the browser to run arbitrary code." I would not have been able to easily and quickly determine the cause of that particular crash without LastActivityView. This is but one of countless purposes that can be accomplished with LastActivityView.

LastActivityView runs on any version of Windows since Windows 2000, and includes XP, Vista, Windows 7 and Windows 8; both 32-bit and 64-bit systems are supported. For such a tiny, fast, and free program, LastActivityView is a powerful utility that can provide extensive information on what has been done on a Windows computer. For anyone who would like to see for himself what has been running on his computer; what crashed, what caused the crash; files downloaded, installed, or uninstalled; and a wealth of other information, LastActivityView is a very worthwhile program to add to the user's arsenal of utilities.

Submit Your article; deadline for next bulletin is Tuesday noon each week. Only what you write may be published. We cannot publish other peoples work without written permission. Simply click here EDITOR AT TECC and paste your write-up to submit it.
Share your computer experiences with other members. We need articles to publish in the TECC Bulletin each week.

UPDATE YOUR MEMBERSHIP INFORMATION Change your e-mail address, unsubscribe to this bulletin, etc. Use link below.
UPDATE YOUR MEMBERSHIP