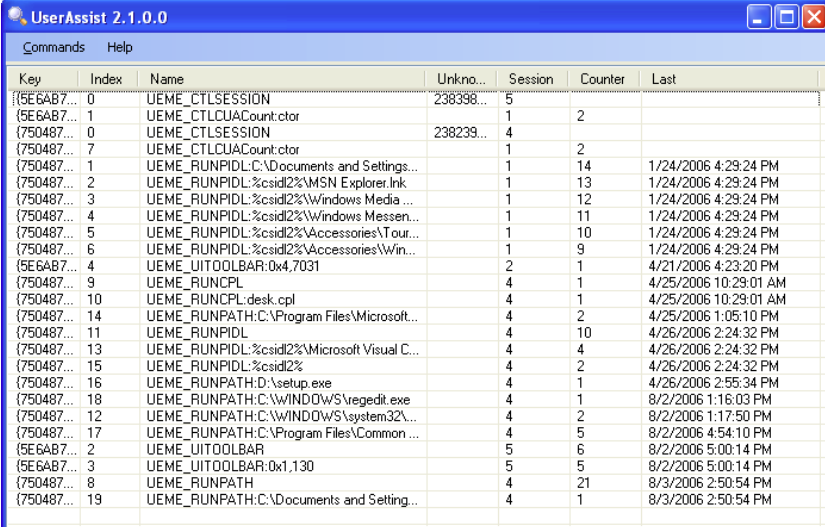


## Didier Stevens

### UserAssist

The UserAssist utility displays a table of programs executed on a Windows machine, complete with running count and last execution date and time.

Windows Explorer maintains this information in the UserAssist registry entries. My program allows you to display and manipulate these entries.



Key	Index	Name	Unkno...	Session	Counter	Last
{5E6AB7...}	0	UEME_CTLSESSION	238398...	5		
{5E6AB7...}	1	UEME_CTLCUACount:ctor		1	2	
{750487...}	0	UEME_CTLSESSION	238239...	4		
{750487...}	7	UEME_CTLCUACount:ctor		1	2	
{750487...}	1	UEME_RUNPIDL:C:\Documents and Settings...		1	14	1/24/2006 4:29:24 PM
{750487...}	2	UEME_RUNPIDL:%csidl2%\MSN Explorer.lnk		1	13	1/24/2006 4:29:24 PM
{750487...}	3	UEME_RUNPIDL:%csidl2%\Windows Media ...		1	12	1/24/2006 4:29:24 PM
{750487...}	4	UEME_RUNPIDL:%csidl2%\Windows Messen...		1	11	1/24/2006 4:29:24 PM
{750487...}	5	UEME_RUNPIDL:%csidl2%\Accessories\Tour...		1	10	1/24/2006 4:29:24 PM
{750487...}	6	UEME_RUNPIDL:%csidl2%\Accessories\Win...		1	9	1/24/2006 4:29:24 PM
{5E6AB7...}	4	UEME_UITOOOLBAR:0x47031		2	1	4/21/2006 4:23:20 PM
{750487...}	9	UEME_RUNCPD		4	1	4/25/2006 10:29:01 AM
{750487...}	10	UEME_RUNCPD.desk.cpl		4	1	4/25/2006 10:29:01 AM
{750487...}	14	UEME_RUNPATH:C:\Program Files\Microsoft...		4	2	4/25/2006 1:05:10 PM
{750487...}	11	UEME_RUNPIDL		4	10	4/26/2006 2:24:32 PM
{750487...}	13	UEME_RUNPIDL:%csidl2%\Microsoft Visual C...		4	4	4/26/2006 2:24:32 PM
{750487...}	15	UEME_RUNPIDL:%csidl2%		4	2	4/26/2006 2:24:32 PM
{750487...}	16	UEME_RUNPATH:D:\setup.exe		4	1	4/26/2006 2:55:34 PM
{750487...}	18	UEME_RUNPATH:C:\WINDOWS\vegedit.exe		4	1	8/2/2006 1:16:03 PM
{750487...}	12	UEME_RUNPATH:C:\WINDOWS\system32\...		4	2	8/2/2006 1:17:50 PM
{750487...}	17	UEME_RUNPATH:C:\Program Files\Common ...		4	5	8/2/2006 4:54:10 PM
{5E6AB7...}	2	UEME_UITOOOLBAR		5	6	8/2/2006 5:00:14 PM
{5E6AB7...}	3	UEME_UITOOOLBAR:0x1130		5	5	8/2/2006 5:00:14 PM
{750487...}	8	UEME_RUNPATH		4	21	8/3/2006 2:50:54 PM
{750487...}	19	UEME_RUNPATH:C:\Documents and Setting...		4	1	8/3/2006 2:50:54 PM

I posted my program (source code and binaries) [here](#). Download the ZIP file, you'll have to extract UserAssist\UserAssist\bin\Release\UserAssist.exe to get my program. There is no setup, it's just one executable. You'll need the [.NET Framework 2.0 runtime](#) to run my program (download it only if you have a problem running my program, if you have an up-to-date version of Windows XP, the .NET 2.0 Framework will already be installed).

I also maintain a [Windows Live CD plugin for my UserAssist utility](#).

Program features and operation is described in the About box:

The program UserAssist displays a list of the programs run by a user on Windows.

Windows Explorer displays frequently used programs on the left side of the standard XP Start menu. The data about frequently used programs is kept in the registry under this key:  
HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerUserAssist

This program decrypts and displays the data found in the registry under the UserAssist key.

When started, the program retrieves the data for the current user and displays it. The display is not refreshed automatically when Windows Explorer updates the registry entries. To refresh the display, execute the 'Load from local registry' command.

Columns in the listview:

**Key:**  
this value is {5E6AB780-7743-11CF-A12B-00AA004AE837} or {75048700-EF1F-11D0-9888-006097DEACF9}  
those are the keys found under the UserAssist key, and are included in the list view to distinguish the entries.

**Index:**  
a running counter, indicating the sequence of values in the registry  
At first, the entries are listed in the sequence they appear in the registry. You can sort columns by clicking on the header.  
To revert to the original sequence, sort the column Index and then the column Key

**Name:**  
The name of the value registry entry. This references the program that was run. This key is ROT13 encrypted, the displayed name is decrypted. There is a registry setting to prevent encryption of the log, but this program does not support this setting.

**Unknown:**  
a 4 byte integer, meaning unknown. It appears to be present only for session entries (UEME\_CTLSESSION).

**Session:**  
This is the ID of the session (a 4 byte integer).

**Counter:**  
This is the number of times the program was ran (a 4 byte integer).

**Last:**  
This is the last time the program was ran (a 8 byte datetime).  
The value is displayed with the timezone of the machine running this UserAssist tool.  
Watch out for time zone differences when importing a REG file from a system with different regional settings.

**Last UTC:**  
This is the last time the program was ran (a 8 byte datetime) in UTC.

**Commands:**  
'Load from local registry'

Displays the data for the current user.

'Load from REG file'

Loads a REG file and imports the UserAssist key.

This command doesn't check the full path of the UserAssist key, thus allowing the analysis of NTUSER.DAT hives loaded and exported with another. Use this command if you cannot run the program on the machine you want to analyze.

Loading the data from a REG file disables editing commands.

'Load from DAT file'

Loads a registry hive file (a DAT file like NTUSER.DAT) and imports the UserAssist key.

The DAT file is temporarily loaded in the registry under the USERSLoadedHive key. Be sure to have the local admin rights to access the file and use this command if you cannot run the program on the machine you want to analyze.

Loading the data from a DAT file disables editing commands.

'Highlight'

Allows you to type in a search string (a regular expression is accepted), each entry matching this string will be highlighted in red.

The highlighting stays active during reloads. Type an empty string to disable the highlighting.

'Save'

This saves the data as a CSV file or a HTML file (choose file type).

'Clear All'

This deletes the {5E6AB780-7743-11CF-A12B-00AA004AE837} and {75048700-EF1F-11D0-9888-006097DEACF9} keys.

All data is lost, and no new data is recorded until Windows Explorer is restarted.

This will impact the frequently run program list on your Start Menu, and maybe other things. I had no other side-effects on my test machines.

This command is disabled when a REG file is loaded.

'Logging Disabled'

Enabling the 'Logging Disabled' toggle allows you to permanently disable the logging of user activity in the UserAssist keys by creating a value HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerUserAssistSettingsNoLog equal to 1.

Disabling the 'Logging Disabled' removes the NoLog value (apparently, setting it to 0 doesn't prevent logging).

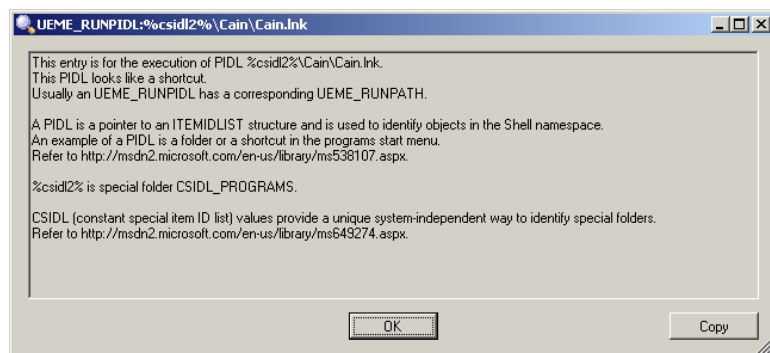
This setting is only effective after Windows Explorer is restarted.

This command is disabled when a REG file is loaded.

Right-clicking an entry will display a menu:

'Clear' will delete the selected entries. The index field of the remaining entries is not changed, they only change after reloading the registry. This command is disabled when a REG file is loaded.

'Explain' will analyse the contents of the name field and try to explain its meaning (based on empirical data).



This program has been tested on Windows XP SP1, SP2, Windows 2003 and Windows Vista.

Microsoft doesn't publish official documentation for UserAssist data. I've found info on the WWW (google for UserAssist) and I discovered the me. In other words: use this program at your own risk.

Ways to restart Windows Explorer:

- 1) Task Manager: kill the explorer.exe process and start a New Task explorer.exe
- 2) logoff / logon
- 3) reboot

Download:

[UserAssist V2.4.3.zip \(https\)](#)

MD5: A5244C7F83E0DE70600E27F5D3B8AD7D

SHA256: 7E2D107BE84FBBF7E79F1BD11703401A374B5138B2F77E4FF8AFE1A3E749CCDA

[Comments \(143\)](#)

## 143 Comments »

1. [...] I've published a BartPE plugin for my UserAssist utility, you can download it here (<https://www.didierstevens.com/files/programs/userassist/v2.4.3.zip>, MD5 D43E519B7BCE90F31EB54884E7AA75C1). And I'm posting another movie. Windows Live CDs are a popular troubleshooting and forensic investigation tool, they allow you to boot a (Windows) PC from a CD. Bart Lagerweij developed BartPE, a tool to create a Windows Live CD (a Windows "pre-install" environment CD), and several people build their own tools based on his work. The Ultimate Boot CD for Windows is based on BartPE. [...]

*Pingback by [A Windows Live CD plugin for my UserAssist utility « Didier Stevens](#) — Monday 18 September 2006 @ 15:24*

2. Nice tool! Questions: I'm not at a programmer. To run the application, do I need only the Bin folder and its contents? Can I delete the Obj and Properties folders? One suggestion is that perhaps you can consider adding a search feature. Thanks!

Jimmy Weg, CFCE

Follow

Agent in Charge, Computer Crime Unit  
 Montana Division of Criminal Investigation  
 303 N. Roberts, Room 371  
 Helena, MT 59620  
 406.444.6681  
 406.439.6185 (cell)  
[jweg@mt.gov](mailto:jweg@mt.gov)

*Comment by Jimmy Weg — Monday 30 October 2006 @ 22:02*

3. 1) you only need UserAssist.exe in folder UserAssist\bin\Release, and you can put it anywhere, e.g. on your desktop.
- 2) yes, you can delete everything, except UserAssist.exe
- 3) I'll probably have a search function in a new version, but for now, you can use the Save function. It creates a CSV file. You can read it with Excel or notepad, and use their search function

*Comment by Didier Stevens — Monday 30 October 2006 @ 22:14*

4. [...] XP saves the full path and name of the program, last access and the number of total executions. UserAssist is a nice little tool that decrypts the information and displays them in its main window. You can [...]

*Pingback by Windows stores information about the programs that you use » gHacks tech news — Monday 22 January 2007 @ 12:50*

5. Great tool ! Thanks for sharing it with the community !

*Comment by Wag — Tuesday 23 January 2007 @ 11:03*

6. Very nice tool! Thanks for sharing. It's nice to have a tool that automatically de-ROTs the values instead of having to run them through another script.

*Comment by Michael H — Wednesday 24 January 2007 @ 0:40*

7. [...] Filed under: My Software — Didier Stevens @ 11:30 My article about my UserAssist forensic tool has been published in the February 2007 issue of (IN)SECURE Magazine [...]

*Pingback by UserAssist article published in (IN)SECURE Magazine « Didier Stevens — Thursday 15 February 2007 @ 11:30*

8. Bad idea!  
 This key and the meanings of its parameters was known by me from 2004, but I published my investigation only for restricted access (only for law enforcement agencies). I consider information about the UserAssist key very important for computer crimes' criminalistic expertises. I can't understand reasons for your publication. This key was a helpful tool for criminalists, and you broke it. Why? The key wasn't dangerous for ordinary users. Now, any computer criminal can read your article, use your utility and hide own unlawful engagement. You are an IT Security Consultant! Are you really think your article is so necessary? I am very disappointed by your publication.

PS. Some years ago Mr. Khizhniak, my compatriot ☺ ((, wrote the book about creating of computer viruses (Part I) and antiviruses (Part II). As result a lot of "Khizhniak-based" viruses was created by so-called "hackers" which indeed couldn't develop any simplest virus singly without the book. None of antiviruses was created. Do you like similar results? After publishing your article will help only computer criminals and create problems for specialists.

Yours sincerely,  
 Ponomaryoff Maxim E.,  
 Information Security Consultant, Yekaterinburg, Russia.

*Comment by Ponomaryoff Maxim E. — Friday 16 March 2007 @ 10:34*

9. > I consider information about the UserAssist key very important for computer crimes' criminalistic expertises.  
 It is, and that's why I published it. Read the comment by Jimmy Weg, Agent in Charge, Computer Crime Unit, Montana Division of Criminal Investigation. He did not know about this technique prior to using my program.

The information is on the web since October 2003 at least, read here: <http://www.personal-computer-tutor.com/abc3/v29/vic29.htm>

Associating me with virus writes is a blow below the belt, it's like a tactic used by corrupt politicians & consorts.

*Comment by Didier Stevens — Sunday 18 March 2007 @ 14:17*

10. Excuse me, if my words offended you. I present you my open-hearted apologies. I didn't associate you with virus writes, moreover I was sure you was leaded by good wishes, but ones could bring to bad results (my example was written only for this aim). I'd read the comment by Jimmy Weg, and I'm glad for him. But soon criminals will clear the UserAssist key with your fine (indeed) utility. What will Mr. Weg do in this case?

As before I consider this information had to be published only for restricted access (only for Mr. Weg and his colleagues).  
 I don't pretend to any priority. I discovered the UserAssist key singly, and didn't know about other publications. Thanks for the link, and sorry for my English.

Yours sincerely,  
 Ponomaryoff Maxim E.

*Comment by Ponomaryoff Maxim E. — Monday 19 March 2007 @ 10:49*

11. > I present you my open-hearted apologies.  
 Apologies accepted! As a non-native English speaker, I also know how sometimes your words can be misunderstood.

I wonder how you bring evidence, based on the UserAssist keys, into court? If you keep the technique secret, has the defense no right to examine your evidence? Does the judge accept the data?

*Comment by Didier Stevens — Monday 19 March 2007 @ 17:31*

Follow

12. [...] Read more... Tags: binary data, didier, encrypted, ive, registry keys, rot13, Spyware, stead, timestamp, treeview, utility windows, windows explorer Posted on Tuesday, March 27th, 2007 at 6:08 pm and under category News. You can read any responses through the RSS 2.0 feed. You can give a response, or trackback from your site. « IE lets attackers hijack network traffic Tools – Fuzzled – a Perl Based Fuzzer » [...]

*Pingback by [Internet Security and Programming » Blog Archive » Didier Stevens - UserAssist utility](#) — Tuesday 27 March 2007 @ 11:09*

13. On XP SP2 I keep getting “The application failed to initialize properly (0xc0000135).” What am I missing?

Thanks!

*Comment by Hank — Thursday 5 April 2007 @ 5:29*

14. Did you install the .NET framework?

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en>

*Comment by [Didier Stevens](#) — Thursday 5 April 2007 @ 6:52*

15. Dear Didier Stevens!

I imagine the answer to your question approximately as follow...

Our national justice has some differences from European or American one.

So when a government investigator needs in special knowledges, he can appoint an expertise (ballistic, graphologic, computer, etc.) He forms a list of questions to the expert. The expert gives a precise answers as far as possible, and writes the expert's report. After when the prosecution presents the expert's conclusion to the court, all employed techniques must be described and be based on some official documents or be validated by an experiments. In our case because Microsoft hasn't still published the official information about the UserAssist key, I'll have to describe my experiments to prove truth of my resumes. But the expert's conclusion also can be used in non-judicial practice (by special officers or special agents. Mostly I cooperate with them but I'm not able to find more correct english term to name them.) In that case I am allowed to describe nothing from my techniques.

PS. I have a small remark to your utility. You use the last time the program was ran in local time mode, and warn about possible differences. I added to your code a new column (Last UTC) because the FILETIME structure kept time exactly in this mode (as you know). When an expert examines a REG-file from another computer, this modification can be very helpful.

PPS. On my XP SP2 your utility works correctly. My version too =)

Yours sincerely,  
Ponomaryoff Maxim E.

*Comment by Ponomaryoff Maxim E. — Friday 27 April 2007 @ 5:51*

16. Thanks for your answer Maxim. Excellent idea to add an UTC column, thanks for the suggestion!

*Comment by [Didier Stevens](#) — Tuesday 1 May 2007 @ 18:34*

17. Great tool! One question... I am curious about the “Counter” field indicating how many times a resource was run. How did you determine that the 4 bytes you use for this are counts? I have been forever looking for a resource that documents this part of the UserAssist keys...

Thanks JS

*Comment by JS — Friday 1 June 2007 @ 18:24*

18. It's explained in an older post: <http://didierstevens.wordpress.com/2006/07/24/rot13-is-used-in-windows-you%E2%80%99re-joking/>  
And also in my article in (IN)SECURE Magazine issue 10: <http://www.net-security.org/dl/insecure/INSECURE-Mag-10.pdf>

*Comment by [Didier Stevens](#) — Wednesday 6 June 2007 @ 16:51*

19. [...] @ 6:29 I was a speaker at the local ISSA chapter last Monday. My talk explained how to use my UserAssist tool for forensic analysis. The audience had great questions for me at the Q&A, some of which I want [...]

*Pingback by [UserAssist Q&A « Didier Stevens](#) — Wednesday 20 June 2007 @ 6:29*

20. Good application. Just wondering if there would be a simple way to save the report in html, and as Jimmy said, a search feature would be great. Thanks

Chad

*Comment by Chad Gish — Thursday 28 June 2007 @ 22:56*

21. Can you suggest a tool to convert NTUSER.DAT files from a user profile to .REG files so that they can be viewed using your tool?

I have tried Registry File Viewer which will export to REGEDIT4 format, but your UserAssist utility says that the file doesn't contain UserAssist data.

*Comment by Sean McLinden — Thursday 5 July 2007 @ 19:23*

22. You can use Regedit. I show it in the movie of this post: <http://didierstevens.wordpress.com/2006/09/18/a-windows-live-cd-plugin-for-my-userassist-utility/>

And I also explain it in my (IN)SECURE Magazine Issue 10 article (page 72): <http://www.net-security.org/dl/insecure/INSECURE-Mag-10.pdf>

*Comment by [Didier Stevens](#) — Thursday 5 July 2007 @ 19:37*

23. @Chad

I'm preparing a new version, HTML export can be included, but I don't know if I want to spend the time programming search. Actually, it's not the Find function that is complex, but the Find Next function.

Follow

*Comment by [Didier Stevens](#) — Thursday 5 July 2007 @ [19:46](#)*

24. I was hoping to avoid using something like UBCD4WIN just because I'll have to make another restore from Encase. But if that is the only way, I guess I'll do it that way.

Importing into a live Windows using Regedit overwrites the existing settings. Bad thing to do with an investigator laptop.

Thanks.

*Comment by [Sean McLinden](#) — Thursday 5 July 2007 @ [20:16](#)*

25. You don't need a live CD, read my article, you can work with a copy of NTUSER.DAT and load the hive. This does not overwrite your settings.

*Comment by [Didier Stevens](#) — Thursday 5 July 2007 @ [20:23](#)*

26. Thanks, that did it.

*Comment by [Sean McLinden](#) — Thursday 5 July 2007 @ [20:49](#)*

27. Is there a commandline version that can be run and dump the output to a txt or cvs or html report?

*Comment by [Brian](#) — Monday 16 July 2007 @ [16:40](#)*

28. [...] Engineering, My Software — Didier Stevens @ 6:05 I'm releasing version 2.3.0 of my UserAssist tool with these new [...]

*Pingback by [UserAssist V2.3.0 « Didier Stevens](#) — Tuesday 17 July 2007 @ [6:05](#)*

29. [...] Stevens has released the latest iteration of his incredibly handy tool UserAssist. This tool, in a nutshell, displays a table of all of the programs executed on a windows machine. [...]

*Pingback by [Liquidmatrix Security Digest » Stevens Releases UserAssist V2.3](#) — Tuesday 17 July 2007 @ [12:14](#)*

30. @Brian

I'll see if I can add command-line support.

*Comment by [Didier Stevens](#) — Tuesday 17 July 2007 @ [13:15](#)*

31. [...] My Software — Didier Stevens @ 8:11 My interview on the CyberSpeak podcast about my UserAssist tool is up. I discovered I speak English with a French accent But I'm not French, I'm [...]

*Pingback by [CyberSpeak interview « Didier Stevens](#) — Monday 23 July 2007 @ [8:12](#)*

32. Didier,

Great tool ... thanks.

Is it possible to get an explanation of the keys that are referenced in the output. I think that the list of possible keys that occur are:

UEME\_RUNPIDL:  
UEME\_RUNPATH:  
UEME\_CTLSESSION  
UEME\_CTLCUACount:  
UEME\_UISCUT:  
UEME\_UIQCUT:  
UEME\_UIHOTKEY:  
UEME\_RUNWMCMD:  
UEME\_RUNCPL:  
UEME\_UITOOLBAR:

I am attempting to use the data from a suspect's imaged hard drive to show that the majority of his time on the computer was spent playing games and on the net. The data shows that there is many uses of Freecell and Hearts but there are even more occurrences of UEME\_UIQCUT, UEME\_RUNPATH, and UEME\_RUNPIDL. What are these keys?

*Comment by [Mark Hallman](#) — Friday 24 August 2007 @ [19:44](#)*

33. Be aware that the UserAssist entries only list how often a program has been started by a user and when it what last started. So it's not the tool to assess how \*long\* programs were running.

UEME\_UIQCUT

Applications launched from the quick launchbar are logged under the entry UEME\_UIQCUT. There is no separate entry with the name or path of the launched application. I think the logic behind this is the following: the UserAssist entries are maintained by Windows Explorer to display the most frequently run applications on the start menu. Applications launched from the quick launchbar have already their "special" place on the GUI Windows, so there's no need to keep stats about their usage.

Follow

## UEME\_RUNPATH

This is logged each time a program is started, look at the path to see which program. When a program is started by double-clicking it in Windows Explorer or by typing its name in the Run command, RUNPATH entries are created/updated but no UEME\_RUNPATH entries are.

A PIDL is a Pointer to an ID List. Every item in Explorer's namespace, whether it's a file, directory, Control Panel applet, or an object exposed by an extension, can be uniquely specified by its PIDL. If the UEME\_RUNPIDL values starts with %csidl2%, then it refers to the start menu. Notice that most UEME\_RUNPIDL values are names of folders in the start menu of shortcuts in the start menu (.lnk)

If you're a programmer, an PIDL is Pointer to IDL, and IDL is short for ITEMIDLIST (<http://msdn2.microsoft.com/en-us/library/ms538107.aspx>). Remember that we're talking about Windows Explorer here, aka the shell, and a PIDL and ITEMIDLIST are shell structures used by programmers.

You can find more information here:

<http://sistersincrimetoronto.on.ca/internetpsysoftware.php>

*Comment by [Didier Stevens](#) — Saturday 25 August 2007 @ [10:05](#)*

34. [...] a key named Settings and under this new key create a DWORD value named NoLog with value 1. My UserAssist tool has a menu toggle (Logging disabled) to do this [...]

*Pingback by [Disabling UserAssist Logging for Windows Vista « Didier Stevens](#) — Saturday 8 September 2007 @ [20:14](#)*

35. [...] programmino, che richiede il .NET Framework è scaricabile qui con i sorgenti. E' anche disponibile un plugin per BartPE [...]

*Pingback by [UserAssist: what is this? « Fare, disfare e rifare](#) — Thursday 20 September 2007 @ [7:13](#)*

36. This functionality is available from within Access Data's program for reading the registry.

*Comment by Anonymous — Thursday 11 October 2007 @ [20:40](#)*

37. And it's also free and open source?

*Comment by [Didier Stevens](#) — Thursday 11 October 2007 @ [21:07](#)*

38. [...] Forensics, My Software — Didier Stevens @ 6:36 The most important feature of this new UserAssist version is the explain command. Now you can right-click an entry, select explain and get a nice explanation [...]

*Pingback by [UserAssist V2.4.1 « Didier Stevens](#) — Tuesday 16 October 2007 @ [6:36](#)*

39. Great tool. Is there a way to connect to a remote registry?

*Comment by John — Tuesday 30 October 2007 @ [13:07](#)*

40. I didn't program that feature, but I'll add it to my todo list.

However, you can connect to the registry of a remote machine with regedit. Export the UserAssist keys and load the exported file in my tool.

Harlan Carvey has scripts that work remotely, but I don't believe his scripts for the UserAssist keys work remotely. They operate on the hive file. His tools are included with his book <http://www.syngress.com/catalog/?pid=4230>.

*Comment by [Didier Stevens](#) — Wednesday 31 October 2007 @ [19:46](#)*

41. [...] UserAssist – Una herramienta relativamente poco conocida de Didier Stevens que nos saca una lista de los programas que se han ejecutado, cuándo, y cuántas veces. [...]

*Pingback by [alfredo reino » Archivo del Blog » Herramientas útiles](#) — Friday 16 November 2007 @ [10:46](#)*

42. [...] under: Forensics, My Software, Update — Didier Stevens @ 9:29 Just a small change in this new version: now you can disable the automatic loading of the local registry data when the UserAssist tool is [...]

*Pingback by [Update: UserAssist V2.4.2 « Didier Stevens](#) — Monday 26 November 2007 @ [9:29](#)*

43. [...] like the UserAssist entries for Windows Server 2008 have the same format as for Windows Vista, my UserAssist tool can also extract the data from Windows Server [...]

*Pingback by [Quickpost: Windows Server 2008 UserAssist Keys « Didier Stevens](#) — Friday 11 January 2008 @ [18:37](#)*

44. [...] From now on, I'll update it each time I release a new version of my UserAssist utility. [...]

*Pingback by [Update: A Windows Live CD plugin for my UserAssist utility « Didier Stevens](#) — Monday 28 January 2008 @ [8:17](#)*

45. Hi Didier,

Can you please explain why I would receive a counter of zero? All my results for PIDL %csidl6% came back with a counter of zero.

Follow

Great tool by the way!

Thanks in advance,

Jenny

*Comment by Jenny — Thursday 7 February 2008 @ 21:15*

46. A counter equal to 0 indicates that the user right-clicked on the item in the start-menu and selected the command to remove the item from the list.

*Comment by [Didier Stevens](#) — Thursday 7 February 2008 @ 21:34*

47. [...] many values include FILETIME objects embedded within their binary data. For example, beneath the UserAssist keys, many of the values found within the Count subkey have 16 bytes of binary data associated with [...]

*Pinback by [Log Analysis Professionals » Blog Archive » The Windows Registry as a Log File](#) — Tuesday 8 April 2008 @ 11:33*

48. Didier. Thanks for the great tools. On UserAssist, (I am not a computer pro – just a power user), the output is generally a history report...yes? Therefore, all entries accessible by a right click can be safely deleted (clear tracks)...yes? Then, recycle bin shredding and overwrite will remove final traces, correct? Thx!

*Comment by Bruce Ades — Wednesday 14 May 2008 @ 11:18*

49. The UserAssist keys contain historical data.  
When you use my UserAssist tool to delete entries, it will actually delete registry keys. Deleted registry keys are not moved to the recycle bin, so there is no need to empty the recycle been.

However, I suspect that deleted registry entries are still present in the registry hive files (like NTUSER.DAT), until their space is reused. Registry compacting should take care of this.

*Comment by [Didier Stevens](#) — Friday 16 May 2008 @ 16:28*

50. Hi,

program looks great but does not run on Windows 2000. It starts without opening a window and keeps the cpu goin' on 100%. When opening using a shortcut and setting the window maximized it opens but does not show data or menu text. Also 100% cpu until I terminate the program.  
Dot.Net2 SP1 installed. Hope you can tweak the program to let it run on W2K.  
In the registry the keys look the same as described everywhere on the 'net.

*Comment by Hans — Saturday 31 May 2008 @ 22:34*

51. I've used it in the past on W2K, it works. I believe that you've so much entries in the UserAssist keys, that it takes a long time for my utility to analyze them all and display the result. Let the program run for some time and see what happens.

*Comment by [Didier Stevens](#) — Sunday 1 June 2008 @ 9:15*

52. Thanks very much for sharing your powerful and handy tool.

Question 1:

What causes the counter to have a negative value?

Question 2:

What causes the counter to have "Removed from list" instead of a number?

I've been using this tool for some time, but today I have encountered above cases for the first time.

*Comment by Nobuyuki Hirato — Monday 4 August 2008 @ 9:01*

53. In fact, the counters are stored inside the binary registry data with an offset of 5. So if a program has been executed exactly once, the counter stored inside the binary registry data is equal to 6, and my UserAssist utility will subtract 5 and display 1. I believe that this +5 offset is a classic programming trick used by the MS programmers to be able to store special values in the same binary format.  
One special value I've identified is 0: this indicates that the program is never to appear in the start menu in the most executed programs list. A user can decide to remove a program from the start menu list by right-clicking the entry and selecting "Remove from this list in de context menu. Internally, this action assigns a value of 0 to the counter. I've programmed UserAssist to display "Removed from list" in the counter column.  
Negative values in the counter column are special values that I've not yet identified. I've had reports of installation programs creating userassist registry entries with values 1 or 2, but I don't know what this implies.

Can you share which programs you've found with 'negative counter values'?

*Comment by [Didier Stevens](#) — Monday 4 August 2008 @ 17:11*

54. Thanks for quick reply.

> Can you share which programs you've found with 'negative counter values'?

Yes.

This time I've encountered two .url files under UEME\_RUNPIDL:%csidl6%\, both indicated with values of -3.

> Internally, this action assigns a value of 0 to the counter. I've programmed UserAssist to display "Removed from list" in the counter column.

Follow

Does it mean all 0's in the counter column should be replaced with "Removed from list"?  
I see a lot of entries with counter 0, apart from ones with "Removed from list". Again, predominantly UEME\_RUNPIDL:%csidl6%\?????.url ones.

*Comment by Nobuyuki Hirato — Tuesday 5 August 2008 @ [3:56](#)*

55. No, a 0 counter in the Counter column of the UserAssist utility means again that this is a special value, but its meaning is unknown.

csidl6 is the special directory with the user's favorites.

Is the last timestamp empty?

*Comment by [Didier Stevens](#) — Tuesday 5 August 2008 @ [18:35](#)*

56. No, both of the two entries having -3 in Counter do have Last timestamps.  
As for the ones having 0 in Counter, Last timestamps are all empty.

*Comment by Nobuyuki Hirato — Wednesday 6 August 2008 @ [2:53](#)*

57. That's normal. I did some testing with favorites, but couldn't reproduce the -3 counter.

If you find more info, please let me know.

*Comment by [Didier Stevens](#) — Thursday 7 August 2008 @ [16:18](#)*

58. OK. I'll inform you when I find out something further.  
Thank you.

*Comment by Nobuyuki Hirato — Friday 8 August 2008 @ [11:13](#)*

59. Thank you for your tool – I am looking for an explanation for "session" Is this an incremental # for every logon/boot. Am I correct that this session number only identifies the last session an application was accessed and need to use restore points to obtain if the application was used on a specific day – Thank you! – Paul

*Comment by Paul Smith — Thursday 23 October 2008 @ [12:42](#)*

60. I have no definite explanation for the session value.  
I've not observed an increase of this value for every logon, but I've observed increments with 1 about every 24 hours, when the machine was on. Not exactly 24 hours, but a bit longer, and the variance looked random.

*Comment by [Didier Stevens](#) — Thursday 23 October 2008 @ [17:55](#)*

61. I went to the old listing for your app (<http://blog.didierstevens.com>) and that led me to "gotdotnet" that no longer exists. Glad I found your new location. I've been using NirSoft's UserAssistView (v1.00) since January09.

*Comment by Ronin Vladiamhe — Tuesday 9 June 2009 @ [21:57](#)*

62. Hi Didier  
First of all I must tell you that your tool is really great!!! Has been really helpful to me, and I'd need your help with something that has been a really big problem to me.  
I need to get all the possible information related to the Quick Launch items, and the applications that have been raised using the Quick Launchbar. In a previous post you said something like this:

Be aware that the UserAssist entries only list how often a program has been started by a user and when it what last started. So it's not the tool to assess how \*long\* programs were running.

UEME\_UIQCUT

Applications launched from the quick launchbar are logged under the entry UEME\_UIQCUT. There is no separate entry with the name or path of the launched application. I think the logic behind this is the following: the UserAssist entries are maintained by Windows Explorer to display the most frequently run applications on the start menu. Applications launched from the quick launchbar have already their "special" place on the GUI Windows, so there's no need to keep stats about their usage.

Would be really great if you could tell me where is this "special" place, that would solve my problem once and for all.  
Sorry my english, and hoping that you can help me soon. I'll be really thankful for your help.  
Yosmel.

*Comment by Yosmel — Thursday 2 July 2009 @ [18:31](#)*

63. @Yosmel

I fear you misunderstood me. With "special place on the GUI Windows", I mean that the Quick Launch items have their fixed place (to the right of the Start button).

Like I wrote: "so there's no need to keep stats about their usage." The UserAssist data doesn't contain info on Quick Launch items

Follow



*Comment by [Didier Stevens](#) — Friday 3 July 2009 @ [15:33](#)*

64. Hi Didier

First of all thanks a lot for your reply.

I just thought that maybe you know where this information was stored on registry.

As you said, "Applications launched from the quick launchbar are logged under the entry UEME\_UIQCUT", and I see that this counter is increased each time you click a quick launch item, so I believe that this information is stored in some place in registry maybe. I'd need to figure out how many times a quick launch item has been clicked, when was the latest time, etc...

But anyway, once again thanks a lot for your reply, and was a pleasure to contact to you. You're a great coder 😊.

My best regards,

Yosmel.

*Comment by Yosmel — Friday 3 July 2009 @ [17:31](#)*

65. Maybe you'll find the data, but personally, I believe it doesn't exist. I'm 100% sure it isn't logged under the UserAssist registry key.

*Comment by [Didier Stevens](#) — Friday 3 July 2009 @ [18:11](#)*

66. Hi Didier

Well, I'll keep trying then. When I saw that the UserAssist registry keep updates the counter for the number of programs that have been launched using quick launch items, I thought that maybe this information was stored in some other registry key. But anyway, thanks a lot for reply.

My best regards,

Yosmel.

*Comment by Yosmel — Friday 3 July 2009 @ [18:23](#)*

67. >>> Well, I'll keep trying then. When I saw that the UserAssist registry keep updates the counter for the number of programs that have been launched using quick launch items, I thought that maybe this information was stored in some other registry key. <<<

Have you tried looking at the Prefetch files? They too keep a counter of how many times an executable has been run.

*Comment by Phillip Rodokanakis — Monday 20 July 2009 @ [20:26](#)*

68. Didier or others...

How accurate is the counter? We found a counter for specific piracy software which is telling us the program was started 3950 times. Is the number to be trusted? Or has Windows some hidden/unknown features that can change/increase the number for some reason?

Kind regards from The Netherlands,

Hans Heins

*Comment by [Hans Heins](#) — Tuesday 4 August 2009 @ [12:41](#)*

69. @Hans

No, I don't know about Windows hidden/unknown features that can increase the number.

In theory, a program could manipulate his counter (increase it) to appear on the most-used list in the start menu. But I've never seen this done in real live.

*Comment by [Didier Stevens](#) — Tuesday 4 August 2009 @ [15:32](#)*

70. Hello Didier,

The time displayed in the column "last" is in UTC if I am right. (UserAssist version 2.4.2.0)

I think it would be very useful if you can change the column name in to something like "Last used – UTC"

(and I think many other investigators) deal with a lot of different tools and also with many different timezones due to our International investigations.

If a tool does not clearly mention which timezone is displayed, we have to figure this out each time we use a nice tool, like UserAssist, to do the job.

Thank you in advance,

Kind regards from the Netherlands

Hans Heins

*Comment by [Hans](#) — Friday 7 August 2009 @ [8:32](#)*

71. Hi Hans,

As we discussed via e-mail, I agree that this is confusing. I've added an extra UTC column: <http://blog.didierstevens.com/2009/08/11/update-userassist-tool-version-2-4-3/>

*Comment by [Didier Stevens](#) — Tuesday 11 August 2009 @ [16:10](#)*

72. [...] My Software, Update — Didier Stevens @ 16:07 I had an interesting discussion with Hans Heins concerning the timestamp displayed by my UserAssist [...]

*Pingback by [Update: UserAssist Tool Version 2.4.3 « Didier Stevens](#) — Tuesday 11 August 2009 @ [16:16](#)*

73. Hi Didier,

Quick question for you please...

Follow

If I have only been given one line of data from a dump of UEME\_RUNPATH value, how can I use UserAssist to find the correct values? Should the data be saved in a particular format so I can load it into the tool and then run it?

Thanks,

Kate

*Comment by Kate — Thursday 1 October 2009 @ [19:29](#)*

74. @Kate

I don't suppose you know how to program in C#, otherwise you just use the UserAssistKey class and call the method to decode?

You can try this:

Create a new user on Windows XP (if your sample is from an XP system). Export the UserAssist registry keys with regedit as a text file.

Edit the reg file with a text editor and replace the UEME\_RUNPATH value with your value.

Import the reg file with my tool.

*Comment by [Didier Stevens](#) — Thursday 1 October 2009 @ [19:42](#)*

75. Hi Didier,

Thank you for the wonderful tool.

Just one problem I found is that the UserAssist 2.4.3 cannot work on Win 7.  
May I know what's the matter?

Thanks

*Comment by Terry — Monday 28 December 2009 @ [3:11](#)*

76. Because the binary data format of the UserAssist values in Windows 7 and Windows 2008 R2 is new and different.

But I've a working version: <http://blog.didierstevens.com/2009/10/21/a-windows-7-launch-party-trick/>

And I've written an article on this for the new Into The Boxes forensic magazine to appear January 1st.

*Comment by [Didier Stevens](#) — Tuesday 29 December 2009 @ [20:17](#)*

77. Love the program. I am curious about something. I'm trying to create a little custom tool utilizing this great tool and was wondering if there was a switch or something I could input into a batch file or command line with the executable that would tell it which file to open.

i.e. if I wanted something like this

c:\utilities\userassist.exe \\server1\Profiles\tse\%E%\ntuser.dat

using %E% as my variable (which scripting will input the correct variable info – so just need userassist.exe to open the file)

Thanks again for a great tool

*Comment by BR — Tuesday 26 January 2010 @ [18:19](#)*

78. @BR

You can do this with Harlan's RegRipper: <http://www.regripper.net/>

That's why I don't add this functionality to my tool, I share my research on the UserAssist keys with Harlan and he integrates it in his tool.

*Comment by [Didier Stevens](#) — Wednesday 27 January 2010 @ [9:50](#)*

79. "Ponomaryoff Maxim"'s comments are ridiculous.

1. These keys were known before you posted about them.

2. If law enforcement relied on those techniques in ANY criminal investigation, they would be public. Disclosure, and all that. Furthermore, police are not "special", and able to "own" information. Her comments are ridiculous in this respect. If she believes what she says, she is more well-advised to spend her time complaining about criminal investigation shows on television, as they "teach" criminals how to get away with murder and are seen by millions every night. Ridiculous.

3. There are countless other reasons why people should know about what their computer does that has nothing to do with law enforcement. For example, my UserAssist had grown to pages and pages of information (mostly from me re-organizing my StartUp shortcuts). I deleted the whole thing and that immediately cut my registry size by 15%.

*Comment by Samo — Sunday 21 February 2010 @ [19:51](#)*

80. [...] in. For examinations involving user activity, I may be most interested in the contents of the UserAssistCount keys (log2timeline extracts this data, as well), but the really valuable information from [...]

*Pingback by [Even More Thoughts on Timelines / Event Viewer](#) — Tuesday 6 April 2010 @ [3:52](#)*

81. I'm trying to find out how to associate a GUID found in the UserAssist Reg key to a program (Is GUID the right term here?). I know that IE has been run multiple times on a system as there is quite a bit of Internet History for the browser but I don't see an entry for it in the UserAssist key. I do have a GUID that has been run over 500 times but how to I associate the program that was run to that GUID? System is Vista.

Entry= UEME\_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0}

Is there a way to find this out?

Follow

*Comment by Dave — Friday 21 May 2010 @ [5:10](#)*

82. @Dave, Yes, search for the GUID in the registry to find out to which programs it is linked.

*Comment by [Didier Stevens](#) — Friday 21 May 2010 @ [6:22](#)*

83. Mr. Stevens,

About a year ago, I mentioned my use of UserAssistView (NirSoft). Your app is quite similar. Two questions; (1) Have you ever looked and compared your app to NirSoft's, (2) Is your app portable?

*Comment by RoninV — Wednesday 2 June 2010 @ [23:50](#)*

84. My answer to (2) is YES, after reviewing a separate thread regarding this app.

*Comment by RoninV — Thursday 3 June 2010 @ [0:06](#)*

85. @RoninV I seem to remember I looked at it some time ago...

*Comment by [Didier Stevens](#) — Thursday 3 June 2010 @ [14:29](#)*

86. [...] Programs of Use <http://blog.didierstevens.com/programs/userassist/> [...]

*Pingback by [UserAssist / Forensic Artifacts](#) — Wednesday 14 July 2010 @ [15:05](#)*

87. Does the USERASSIST program determine if a user's executable has been renamed to something innocuous like NotePad or Excel? If all that is being tracked is what programs are being run, how does UserAssist know that the program is the \*REAL\* program? I don't see how the output from this could be used as evidence if the user could be hiding the execution of some program by appearing to be running some other program.

*Comment by [Bill M.](#) — Thursday 22 July 2010 @ [2:52](#)*

88. @Bill M. No, the UserAssist registry keys record the name of the program, renaming a program is not recorded in these keys. You need other forensic evidence (for example the cache) to establish that notepad.exe is indeed notepad.exe and not another program.

*Comment by [Didier Stevens](#) — Thursday 22 July 2010 @ [19:13](#)*

89. [...] publicó una nueva herramienta llamada UserAssist que nos permite visualizar una lista de los programas que fueron ejecutados en un sistema Windows, [...]

*Pingback by [Descubriendo qué programas fueron ejecutados en Windows « WEB ANTRIX.TK](#) — Sunday 15 August 2010 @ [6:46](#)*

90. [...] ที่นี้ ในการสร้าง keyword ส่วนใหญ่แล้วเราจะกำหนดเป็นคำธรรมดาๆ ภาษาไทยทั่วไป ทำให้ไม่มีทางค้นหาข้อมูลตรงส่วนที่ถูกเข้ารหัสได้ ดังนั้นวิธีการก็คือใช้โปรแกรมช่วย decode ข้อมูลใน registry ออกมา แล้วดูว่าเครื่องนั้นมีโปรแกรมอะไรที่เคยทำการติดตั้งลงไปบ้าง อ่านเพิ่มเติมได้ที่<http://blog.didierstevens.com/programs/userassist/> [...]

*Pingback by [เข้ารหัสข้อความง่ายๆ ด้วย Rot13 / Technology Crime Suppression Division \(TCSD\)](#) — Thursday 2 September 2010 @ [17:11](#)*

91. [...] Más información sobre UserAssist >> [...]

*Pingback by [Herramienta: UserAssist / Informatica Forense – Pericias Informaticas](#) — Thursday 9 September 2010 @ [3:38](#)*

92. Hi.

Would just start by saying that this is a great site that you have.. I have really gathered a lot of information regarding userassist values here. 1 question remains:

Have you ever discovered what causes the -3 values in the counter? I have quite a few of those entries and can't really stand in court and say that i dont really know what causes the negative values.

I've written an EnScript (EnCase) to decrypt and display the values. But once again I do not know what causes the +2 counter values (Which in turn becomes -3 after subtracting 5 in XP)

I COULD just ignore them, but it really bugs me not knowing what they stand for.

I can see that another visitor at this site has asked about the same question, but it remained unresolved...

*Comment by [Rasmus Riis](#) — Monday 27 September 2010 @ [8:11](#)*

93. @Rasmus Riis This -3 value remains an open question. I've not been able to reproduce this, and for obvious reasons, people who reported this were not able to share their sample.

*Comment by [Didier Stevens](#) — Monday 27 September 2010 @ [8:58](#)*

94. Ok... Obviously I cant send you the ntuser.dat that im working on, but if you like, i could e-mail you a sample of an ntuser.dat from my home computer? I know that -3 is in that as well..

*Comment by [Rasmus Riis](#) — Monday 27 September 2010 @ [9:08](#)*

95. [...] UserAssist [...]

*Pingback by [» Free Computer Forensic Tools](#) — Saturday 6 November 2010 @ [3:46](#)*

96. [...] UserAssist [...]

*Pingback by [» Ferramentas Livres para Forense Computacional](#) — Saturday 6 November 2010 @ [3:55](#)*

Follow

97. [...] XP saves the full path and name of the program, last access and the number of total executions. UserAssist is a nice little tool that decrypts the information and displays them in its main window. You can [...]

*Pingback by [Windows stores information about the programs that you use](#) — Wednesday 1 December 2010 @ 21:07*

98. When trying to analyze the ntuser.dat file, UserAssist states “The file didn’t contain UserAssist data”. I noticed someone else had the same issue posted on this site, but when I tried to review the possible solutions...none of it really helped out.

Can you please tell me what would cause this error and how to go about fixing it. Can programs that wipe ntuser.dat have an affect on it as well?

Thanks

*Comment by OMBM — Tuesday 21 December 2010 @ 14:28*

99. @ombm try to load the hive with regedit, when this works, it will work with UserAssist

*Comment by [Didier Stevens](#) — Tuesday 21 December 2010 @ 15:40*

100. Good day, Didier! It’s me again =)  
I’ve spent some time to investigate a new version of the UserAssist key in Windows 7 and have read your article about a new format for the binary value data (Into The Boxes, Jan 2010, [http://intotheboxes.files.wordpress.com/2010/04/intotheboxes\\_2010\\_q1.pdf](http://intotheboxes.files.wordpress.com/2010/04/intotheboxes_2010_q1.pdf)). And now I wanna say about detected problems.

1) You wrote: “From bytes 0 to 3, we find a 32-bit integer that is always zero...”

I checked three randomly selected computers and found that it wasn’t so. I found 0x00000001, 0x0000000A and 0x00000004 values instead of zero. These values are constant for chosen computers. It’s amazing! What do you think about it? Why these values are so various? And what these values can mean? I guess it may be associated with the operating system version, but unfortunately I had too little time to refute or confirm this hypothesis.

2) You wrote: “From bytes 8 to 11, we find another 32-bit counter. This counter is usually larger than the program-execution counter, and I believe it counts the number of times an application receives focus...”

In my case, all these values were never larger than the program-execution counters. For example, when a ProgExec counter was equal 16, the appropriate “focus” counter could be equal 5.

Yours sincerely, P.M.E.

*Comment by P.M.E. — Monday 27 December 2010 @ 11:22*

101. @P.M.E. Thanks for sharing your observations, I’ll need revisit this.

*Comment by [Didier Stevens](#) — Tuesday 28 December 2010 @ 11:21*

102. I try to For advanced users, there’s another key worth looking at as it’s an invite to any Trojan that bypasses your protection.

You can find more info on this by Binging UserAssist

Secure your PC with the following reg changes:

Navigate to

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\

Delete all the subkeys

Add a new sub key called Settings

Add a new Dword entry under Settings named NoEncrypt with a value of 1

Add a new Dword entry under Settings named NoLog with a value of 1

But it doesn’t work and all was recreated again.

Hope you can help me solve this problem.

Gilbert Parent  
Canada

*Comment by [Guil Paré](#) — Friday 21 January 2011 @ 22:31*

103. @Gilbert Disabling logging like you describe it works only till Windows XP. Starting with Windows Vista, you need to use other keys:  
<http://blog.didierstevens.com/2007/09/08/disabling-userassist-logging-for-windows-vista/>

My UserAssist program allows you to enable/disable logging correctly on the different versions of Windows.

*Comment by [Didier Stevens](#) — Friday 21 January 2011 @ 23:06*

104. First of all – thank you Didier for this nice write up. And here’re my 2 cents: those first 4 bytes of UEME\_CTLSESSION’s value are last 4 bytes of FILETIME structure shifted to the left by 29 bits representing the session’s start timestamp. Something like this could get you that date back – `DateFromFileTimeUtc(Convert.ToInt64(first4BytesAsInt32)<<29)`.

*Comment by Vasily Kolobkov — Friday 15 April 2011 @ 23:10*

105. Sorry, made a mistake – initially filetime structure was shifted to the right. Thus we are shifting it to the left to restore the date.

Follow

*Comment by Vasily Kolobkov — Friday 15 April 2011 @ [23:18](#)*

106. @Vasily Kolobkov Thanks for the info Vasily.

*Comment by [Didier Stevens](#) — Saturday 16 April 2011 @ [6:20](#)*

107. Hi,  
I tried v2.4.3 on windows 7 64-bit; it showed nothing even after I clicked "Load from local registry". I assume that's the way to display what is supposed to be currently stored in the registry.

Perhaps you have a later version that I missed?  
Perhaps the utility does not work on windows 7 64-bit?

PS. I ran the utility with and without "as administrator"

*Comment by Dave — Monday 18 April 2011 @ [15:53](#)*

108. @Dave This version doesn't support Windows 7 (the format has changed). Take a look here for Windows 7:  
<http://blog.didierstevens.com/2009/10/21/a-windows-7-launch-party-trick/>

*Comment by [Didier Stevens](#) — Monday 18 April 2011 @ [17:44](#)*

109. Hi,  
I have identified the registry created for my software in "Most often used programs"  
The entry is: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR\_EHACNGU:P\Cebtenz SvyrfCnvag.ARG\CnvagQbgArg.rkr

I wanted to remove my program from the "Most Often Used Programs list, so I deleted the above mentioned registry entry but still it shows up in most often used programs, when I click on "Start". How do I do this programmatically ?

*Comment by Himanshu — Wednesday 27 April 2011 @ [6:53](#)*

110. @Himanshu You restarted explorer.exe?

*Comment by [Didier Stevens](#) — Wednesday 27 April 2011 @ [8:09](#)*

111. [...] UserAssist [...]

*Pingback by [Free computer forensic tools](#) — Wednesday 25 May 2011 @ [11:37](#)*

112. [...] What's not quite as well known, though, is that Windows also maintains a longer and separate history of all the programs launched on your computer, including details like the number of times they've been run, and the last execution date and time. This information is stored in the Registry (HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerUserAssist), but it's encrypted, so you'll need something like the free UserAssist tool to find out more (for Windows 7 use this version –for Windows XP or Vista go here). [...]

*Pingback by [UserAssist uncovers Windows activity logs - Fabtechguy.com](#) — Monday 18 July 2011 @ [23:39](#)*

113. [...] What's not quite as well known, though, is that Windows also maintains a longer and separate history of all the programs launched on your computer, including details like the number of times they've been run, and the last execution date and time. This information is stored in the Registry (HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerUserAssist), but it's encrypted, so you'll need something like the free UserAssist tool to find out more (for Windows 7 use this version –for Windows XP or Vista go here). [...]

*Pingback by [UserAssist uncovers hidden Windows activity logs | Information Technology Leader](#) — Wednesday 20 July 2011 @ [7:54](#)*

114. All I got is blank window, no information at all ☹

*Comment by Jari — Sunday 24 July 2011 @ [8:09](#)*

115. @Jari I assume you're trying this on Windows 7? Then you should read comment 108.

*Comment by [Didier Stevens](#) — Sunday 24 July 2011 @ [8:30](#)*

116. Oh, yes I use Windows 7, my fault. Thank you!

*Comment by Jari — Sunday 24 July 2011 @ [8:52](#)*

117. Do you have any command line switches? Thanks

*Comment by Jim — Sunday 24 July 2011 @ [14:21](#)*

118. Well, it's all very interesting if you're a programmer...I'm an ORDINARY user. Can you explain, in English, the SIMPLE, 1,2,3 steps...go here,click, here, do this or that in order to use this program?  
Thanks,  
Babs

*Comment by Babs — Sunday 24 July 2011 @ [15:48](#)*

119. @Jim No, and that's by design, because you should use Harlan Carvey's RegRipper for command-line operations.

*Comment by [Didier Stevens](#) — Sunday 24 July 2011 @ [15:56](#)*

120. @Babs No, this is a forensic tool, it is not designed for ORDINARY users. You should not use it.

Follow

*Comment by [Didier Stevens](#) — Sunday 24 July 2011 @ [15:57](#)*

121. I have Win XP SP3. When I run UserAssist, I get zero entries in the table. Even after running several programs, there's nothing in UserAssist. What am I missing?

*Comment by [George Rezac](#) — Monday 25 July 2011 @ [0:12](#)*

122. @George Do you know how to use regedit?

*Comment by [Didier Stevens](#) — Monday 25 July 2011 @ [1:40](#)*

123. Yes.

*Comment by [George Rezac](#) — Monday 25 July 2011 @ [12:10](#)*

124. @George OK, then take a look at HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist  
You should find 2 keys ({5E6AB780-7743-11CF-A12B-00AA004AE837} and {75048700-EF1F-11D0-9888-006097DEACF9}), and under these keys you should find many more keys.  
Should these keys be missing, then it explains why you don't see anything.

*Comment by [Didier Stevens](#) — Monday 25 July 2011 @ [12:55](#)*

125. Each key has one subfolder: Count. There are no keys. OK, so that's why your program isn't showing anything, but WHY don't I have any keys there? I sure haven't deleted anything.

*Comment by [George Rezac](#) — Monday 25 July 2011 @ [13:02](#)*

126. @George So there are no REG\_BINARY entries under the count keys? Do you use a registry cleaner, or some other maintenance program? Some of them clean these keys.

*Comment by [Didier Stevens](#) — Monday 25 July 2011 @ [13:08](#)*

127. Each Count folder has the same REG\_BINARY entry: HRZR\_PGYFRFFVBA with a value of all zeroes. In addition to the two keys, UserAssist has one more folder: Settings, with Default (value not set) and NoLog (value 1).  
Yes, I do use various registry cleaners, but I ran your program after opening several applications.

*Comment by [George Rezac](#) — Monday 25 July 2011 @ [13:17](#)*

128. @George It must be the combination of registry cleaners and the NoLog value. When NoLog is equal to 1, no records are added to the registry keys. You can reset NoLog with my UserAssist program.

*Comment by [Didier Stevens](#) — Monday 25 July 2011 @ [13:35](#)*

129. [...] UserAssist [...]

*Pingback by [포렌식 도구 모음 \(Digital Forensics Tools\) | FORENSIC-PROOF \(Digital Forensics Community\)](#) — Thursday 1 September 2011 @ [4:09](#)*

130. [...] UserAssist utility displays a table of programs executed on a Windows machine (It works best for XP but there is a non [...])

*Pingback by [What Has Run On My PC? | Real Coding!!](#) — Thursday 29 September 2011 @ [3:23](#)*

131. [...] blog online. This registry key stores data that is ROT13 encrypted and there are a number of free tools out there to decrypt these values from the [...]

*Pingback by [EnCase EnScript to search for keyword in ROT13 or XOR » Digital Evidence](#) — Saturday 22 October 2011 @ [16:42](#)*

132. [...] adındaki aracı indirip sadece çalıştırarak bu listeye ulaşmanız mümkündür. Aracın XP/Vista sürümünü bu adresten, Windows 7 sürümünü ise bu adresten [...]

*Pingback by [Windows'un sizi izlemekte kullandığı 5 yol! | Haber – Mekan](#) — Tuesday 15 November 2011 @ [16:38](#)*

133. [...] UserAssist database can help. Just install the free UserAssist program (see the comments for a link to a Windows 7-compatible version) to see the database, or disable [...]

*Pingback by [Tutorial: More hidden Windows tips tricks and shortcuts](#) — Sunday 20 November 2011 @ [7:01](#)*

134. [...] from Nirsoft.net userassist from Didier Stevens Categories: Tech Tip Tags: nirsoft, tools, userassist Comments (0) [...]

*Pingback by [Techish Blog » Microsoft Windows UserAssist](#) — Wednesday 30 November 2011 @ [3:25](#)*

135. [...] adındaki aracı indirip sadece çalıştırarak bu listeye ulaşmanız mümkündür. Aracın XP/Vista sürümünü bu adresten, Windows 7 sürümünü ise bu adresten [...]

*Pingback by [Windows'un sizi izlemekte kullandığı 5 yol! | Teknoci](#) — Friday 2 December 2011 @ [6:52](#)*

136. [...] UserAssist [...]

*Pingback by [101 utilidades forenses | Blog de Seguridad Informática](#) — Tuesday 6 December 2011 @ [8:25](#)*

137. I found your program really useful. Is there going to be an update for windows 7? Thanks very much

*Comment by [redesyseguridad](#) — Thursday 8 December 2011 @ [6:21](#)*

138. @redesyseguridad Yes, <http://blog.didierstevens.com/2009/10/21/a-windows-7-launch-party-trick/>

*Comment by [Didier Stevens](#) — Thursday 8 December 2011 @ [20:45](#)*

Follow

139. [...] adındaki aracı indirip sadece çalıştırarak bu listeye ulaşmanız mümkündür. Aracın XP/Vista sürümünü bu adresten, Windows 7 sürümünü ise bu [...]

*Pingback by [Windows sizi gözetliyor! | Chat, Sohbet, chat siteleri, chat odaları](#) — Monday 12 December 2011 @ [19:32](#)*

140. Great tool. I found your program is very useful. It seems working fine and I am able to see all the run count information on XP, Windows 7 and Windows 2008. However, registry values (run count, focus count and focus time) under UserAssist have seen an mysteriously reset somehow: the run count information came back to 0 and starting increment if a program runs again. And I don't recall I have done anything to the registry key/value. This happens on Windows 2008 yesterday, which I thought was an accident and tried to forget it but this happen again on Windows 7 again. I am still watching to see if it happens again but I am not able to reproduce again.

Has anyone seen similar behavior?

*Comment by JamesZ — Thursday 29 December 2011 @ [22:24](#)*

141. I think I've seen this when you disable UserAssist in Windows.

*Comment by [Didier Stevens](#) — Friday 30 December 2011 @ [9:44](#)*

142. Thanks for your quick response.

I don't recall I ever did that twice on different machines. Besides, if it is disabled, does the counter still increment ?

*Comment by JamesZ — Friday 30 December 2011 @ [15:43](#)*

143. @JamesZ No, it would not.

*Comment by [Didier Stevens](#) — Saturday 31 December 2011 @ [13:15](#)*

[RSS feed for comments on this post.](#) [TrackBack URI](#)

## Leave a Reply

Enter your comment here...

Fill in your details below or click an icon to log in:



Email

(Not published)

Name

Website

☐ Notify me of follow-up comments via email.

Post Comment

## . Pages

- [About](#)
- [Links](#)
- [My Software](#)
- [Professional](#)
- [Programs](#)
  - [Ariad](#)
  - [Binary Tools](#)
  - [CASToggle](#)
  - [Disitool](#)
  - [EICARgen](#)
  - [ExtractScripts](#)
  - [FileGen](#)
  - [HeapLocker](#)
  - [Nokia Time Lapse Photography](#)
  - [OLlyStepNSearch](#)
  - [PDF Tools](#)
  - [Shellcode](#)
  - [SpiderMonkey](#)
  - [Translate](#)
  - [USBVirusScan](#)

Follow

- [UserAssist](#)
- [XORSearch](#)
- [ZIPEncryptFTP](#)
- [Public Drafts](#)
  - [Cisco Tricks](#)
- [Reverse Engineering Mentoring](#)
- [Screencasts & Videos](#)
- 

## • Top Posts

- [Calculating a SSH Fingerprint From a \(Cisco\) Public Key](#)
- [PDF Tools](#)
- [Restoring Safe Mode with a .REG file](#)
- ["Is your PC virus-free? Get it infected here!"](#)
- [Howto: Make Your Own Cert With OpenSSL](#)

## • c

Select Category 

## • Fellow Bloggers

- [Bart's Weblog](#)
- [Belgian Security Bloggers](#)
- [DiabloHorn](#)
- <https://kingpinz.info/>
- [Windows Incident Response](#)

## • XML

## • Blog Stats

- 1,777,844 hits

## • [Twitter @DidierStevens](#)

- Just released a little Cisco IOS security tool to start the new year: <http://t.co/PILda03v> [1 day ago](#)
- Happy New Year to all and your families - Received Microsoft MVP award 2012 - Will release new tools this year for Windows and Cisco IOS. [1 day ago](#)
- In case you've not seen my New Year video yet "Happy New Router" <http://t.co/KF9TryBD> [2 days ago](#)
- Submitted White Hat Shellcode workshop to CFP HiTB Amsterdam 2012. [2 days ago](#)
- Wrote small Python program to receive and send SMS, interfaces via serial port to Huawei E220 dongle. [3 days ago](#)

## • Archives

- [January 2012](#)
- [December 2011](#)
- [November 2011](#)
- [October 2011](#)
- [September 2011](#)
- [August 2011](#)
- [July 2011](#)
- [June 2011](#)
- [May 2011](#)
- [April 2011](#)
- [March 2011](#)
- [February 2011](#)
- [January 2011](#)
- [December 2010](#)
- [November 2010](#)
- [October 2010](#)
- [September 2010](#)
- [August 2010](#)
- [July 2010](#)
- [June 2010](#)
- [May 2010](#)
- [April 2010](#)
- [March 2010](#)
- [February 2010](#)
- [January 2010](#)
- [December 2009](#)
- [November 2009](#)
- [October 2009](#)
- [September 2009](#)
- [August 2009](#)

Follow



- [July 2009](#)
- [June 2009](#)
- [May 2009](#)
- [April 2009](#)
- [March 2009](#)
- [February 2009](#)
- [January 2009](#)
- [December 2008](#)
- [November 2008](#)
- [October 2008](#)
- [September 2008](#)
- [August 2008](#)
- [July 2008](#)
- [June 2008](#)
- [May 2008](#)
- [April 2008](#)
- [March 2008](#)
- [February 2008](#)
- [January 2008](#)
- [December 2007](#)
- [November 2007](#)
- [October 2007](#)
- [September 2007](#)
- [August 2007](#)
- [July 2007](#)
- [June 2007](#)
- [May 2007](#)
- [April 2007](#)
- [March 2007](#)
- [February 2007](#)
- [January 2007](#)
- [December 2006](#)
- [November 2006](#)
- [October 2006](#)
- [September 2006](#)
- [August 2006](#)
- [July 2006](#)
- [June 2006](#)

•

January 2012

**M T W T F S S**

[1](#)  
2 3 4 5 6 7 8  
9 10 11 12 13 14 15  
16 17 18 19 20 21 22  
23 24 25 26 27 28 29  
30 31

[« Dec](#)

Theme: [Rubric](#). [Blog at WordPress.com](#).

⌂

Follow