

# Windows Forensic Analysis

Dedicated to incident response and computer forensic analysis topics, with respect to Windows 2000, XP, 2003, and Vista operating systems

## WFA: The UserAssist Registry Keys Explained

Windows systems record a great deal of user activity, and much of this information is recorded and maintained automatically, without any user interaction (though some specifics steps may be taken to prevent the data from being recorded). This data can be extremely valuable to a forensic analyst pursuing an investigation.

There are Registry keys within the user's Registry hive file (NTUSER.DAT, located within the user's profile directory) that record a good deal of activity when the user interacts with the shell (i.e., Windows Explorer). Specifically, when the user clicks on a Windows shortcut file, or clicks through the Start Menu to launch an application via the Program Menu, or double-clicks an icon to launch an application, this information is recorded in the UserAssist keys.

The path to the UserAssist key is:

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

Beneath this key you should see at least two subkeys with names that are globally unique identifiers, or GUIDs. The first is

{5E6AB780-7743-11CF-A12B-00AA004AE837}

According to class identifiers located within the Registry, this GUID refers to the "Microsoft Internet Toolbar".

The second GUID is

{75048700-EF1F-11D0-9888-006097DEACF9}

According to class identifiers located within the Registry, this GUID refers to the "ActiveDesktop" and is the Registry key that forensic analysts will be most interested in.

There may be a third GUID available, which is

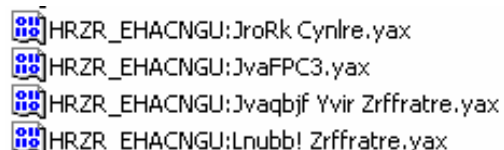
{0D6D4F41-2994-4BA0-8FEF-620E43CD2812}

This GUID is present if IE 7.0 has been installed on the system.

Beneath each of the GUID subkeys is a "Count" key, which contains the information we are most interested in.

Throughout the rest of this article, the term "UserAssist key" will be used to refer to the contents of the "Count" key located beneath the GUID key that refers to the ActiveDesktop class identifier.

Navigating to the UserAssist key in RegEdit, you're likely to see a number of values, as illustrated in figure 1.



HRZR\_EHACNGU:JroRk Cynlre.yax  
HRZR\_EHACNGU:JvaFPC3.yax  
HRZR\_EHACNGU:Jvaqbif Yvir Zrffratre.yax  
HRZR\_EHACNGU:Lnubb! Zrffratre.yax

Figure 1

These value names don't make a great deal of sense, as they are ROT-13<sup>1</sup> encrypted.

<sup>1</sup> <http://en.wikipedia.org/wiki/ROT13>

However, this “encryption” is easily reversed using Perl code such as the following:

```
$name =~ tr/N-ZA-Mn-za-m/A-Za-z/;
```

Reading each of the value names and translating them will produce something understandable, with respect to the action taken by the user.

These values are all binary data types, and many of the values will have 16 bytes of data, the last 8 of which represent a FILETIME<sup>2</sup> object, which corresponds to the last time the user took that action. The data from four values within the UserAssist key is illustrated in figure 2.

```
fa 01 00 00 41 16 00 00 20 ca 80 11 30 52 c8 01
f6 01 00 00 06 00 00 00 f0 28 a6 0c 16 4f c8 01
ba 01 00 00 07 00 00 00 20 9f 22 42 91 1c c8 01
ba 01 00 00 06 00 00 00 90 27 a7 f5 b5 1c c8 01
```

**Figure 2**

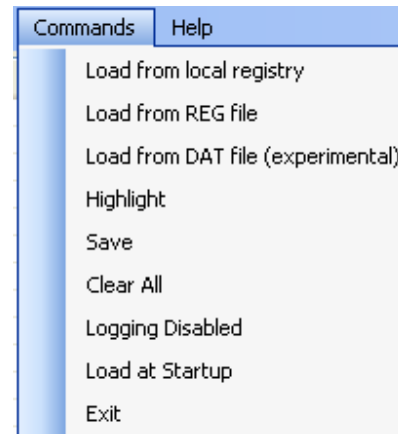
The second 4-byte segment (DWORD) of the data represents the number of times that the action has been taken, with the increment starting at 5, rather than 1. Whenever a previously performed action is taken again, the “runcount” is updated along with the timestamp value. This information tells the forensic analyst how many times the user performed an action, and when was the last time that they performed that action.

Didier Stevens has spent a good deal of time researching the UserAssist key contents and developing his UserAssist application that allows the analyst to easily view and understand the contents of the key. Launching the UserAssist application (version 2.4.2.0 was available at the time that this article was written) will automatically load the contents of the



UserAssist

UserAssist key for the currently logged on user. However, as illustrated in figure 3, there is an option available to load an NTUSER.DAT Registry hive file, as well.



**Figure 3**

The UserAssist application lists its output in seven columns, after decrypting the value names. The final column, which contains the translated timestamps, can be sorted based in order to view at timeline of user activity.

Figure 4 illustrates a translation of several UserAssist value names.

UEME_RUNPATH:C:\WINDOWS\system32\mspaint.exe
UEME_RUNPIDL:%csidl2%\Accessories
UEME_RUNPIDL:%csidl2%\Accessories\Paint.lnk
UEME_RUNPATH:C:\WINDOWS\regedit.exe

**Figure 4**

You can see from figure 4 that the user accessed regedit.exe, as well as mspaint.exe (apparently by choosing the Paint shortcut from the Program menu). Each of the shortcuts or applications is preceded by an identifier that begins with “UEME”. Didier has done considerable work in attempting to identify what each of these identifiers means. If you choose an entry in the interface for his UserAssist application and right-click, you will see a menu appear with two choices...Clear and Explain. Choosing

<sup>2</sup> <http://support.microsoft.com/kb/188768>

Explain will pop up a dialog box with a brief explanation of what the value name indicates. For example, choosing Explain for the regedit.exe entry indicates that the UEME\_RUNPATH identifier specifies that the user launched an application (in this case, RegEdit).

According to MS, a “PIDL<sup>3</sup>” is a “pointer to an item identifier list”. UserAssist key “UEME\_RUNPIDL” identifiers apparently refer to items in a menu (such as the Program Menu) path, as well as Windows shortcuts, and lead to actual applications (\*.exe files “pointed to” by the shortcut files). One or more UEME\_RUNPIDL identifiers may precede a UEME\_RUNPATH identifier.

Perl scripts such as UAssist.pl can be used to extract, parse, and translate the information within the UserAssist key for the analyst. The following is an extract of the output available from the UAssist.pl Perl script:

Mon Sep 26 23:33:06 2005 (UTC)  
UEME\_RUNPATH:C:\WINDOWS\system32\notepad.exe;10

Mon Sep 26 23:26:43 2005 (UTC)  
UEME\_RUNPATH:Z:\WINNT\system32\sol.exe;6

Mon Sep 26 23:22:30 2005 (UTC)  
UEME\_RUNPATH:Downloads.lnk;6

Mon Sep 26 23:16:26 2005 (UTC)  
UEME\_RUNPATH:C:\Program Files\Morpheus\Morpheus.exe;6

Mon Sep 26 23:16:25 2005 (UTC)  
UEME\_RUNPATH:Morpheus.lnk;6

From this example output, we see that the user clicked on the Morpheus<sup>4</sup> shortcut from the Program Menu, and then immediately afterward, the shell launched Morpheus via the application EXE file. The output extract further indicates that the user also launched the Solitaire and Notepad applications.

<sup>3</sup> <http://support.microsoft.com/kb/167834>

<sup>4</sup> <http://morpheus.com>

Additional programmatic means may be used to display and sort the contents of the UserAssist keys. ProDiscover from Technology Pathways utilizes Perl as its scripting language, referred to as “ProScripts”.

### UserAssist\Settings Key

Beneath the UserAssist key itself, you should expect to see two, or possibly three (if IE7 has been installed) GUID subkeys. There is a little known MS KB article that discusses troubleshooting using the instrumented version of Word 2000<sup>5</sup>. This KB article mentions a UserAssist subkey named “Settings”, as well as a value named “NoEncrypt”. If this DWORD value is set to 1, then entries made to the UserAssist keys will not be ROT-13 encrypted. There is additional information available on the Internet that indicates that if a DWORD value named “NoLog” is set to 1, logging of activity via the UserAssist key will be disabled.

### Summary

The data recorded in the UserAssist key can be extremely valuable to a forensic analyst. Not only can it show a timeline of the user’s activity on the system...what the user did, when they last did it, and how many times they did it...but the timestamp information can also be used to develop a timeline of when a user was accessing the system via the shell (i.e., local console login, remote login via Remote Desktop, etc.). As there does not seem to be a limit to the number of entries that can be recorded in the UserAssist keys, the analyst may also find information regarding the installation, use, and removal of applications by the user, long after the user deleted or removed the application itself. The UserAssist key may also contain references to the “Add or Remove Programs” or “Date and Time” Control Panel applets, providing indications of additional user activity (adding or

<sup>5</sup> <http://support.microsoft.com/kb/239062>

removing applications, modifying the system time).

When a user accesses a Control Panel applet, the decoded entry in the UserAssist key begins with "UEME\_RUNCP". When the user accesses the "Add or Remove Programs" applet, the decoded entry may look like:



UEME\_RUNCP:C:\WINDOWS\system32\appwiz.cpl",Add or Remove Programs"

When a user accesses the "Date and Time" Control Panel applet, the decoded entry may look like:



UEME\_RUNCP :timedate.cpl

It may be possible to locate additional UserAssist key entries by performing keyword searches of unallocated space, the pagefile, or even of memory dumps, looking for the presence of "HRZR\_". However, this will return only the value name string. Looking for the Registry values (based on "magic number" identifiers) and then parsing the rest of the data from there may also return the timestamp data, as well. One thing to keep in mind though is that data found in this manner may not be associated with a particular user. However, if the timestamp data is retrieved, the analyst may be able to correlate that information with other information that shows users logged onto the system during the same time period.

Harlan is a forensic analyst located in the metro DC area, and is the author of three books related to live response and forensic analysis of Windows systems. He also presents at conferences and provides training on those same topics, as well. He can be reached at [keydet89@yahoo.com](mailto:keydet89@yahoo.com).

## Resources

- Didier Stevens' UserAssist utility<sup>6</sup>
- Lance Mueller's EnScript<sup>7</sup> for parsing UserAssist keys

6

<http://blog.didierstevens.com/programs/userassist/>

7

<http://www.forensickb.com/2007/07/userassist-registry-keys.html>