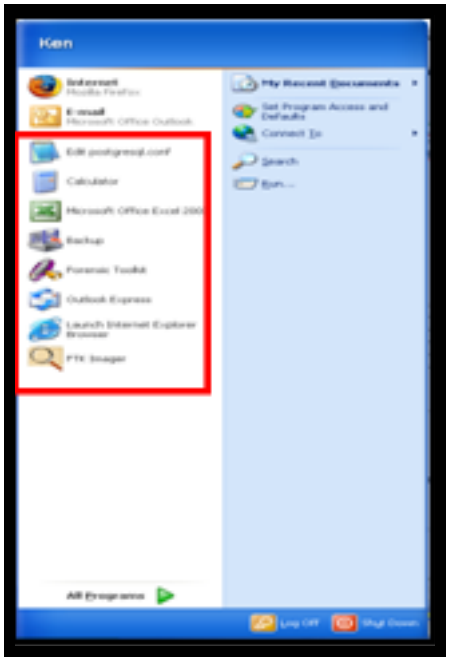
ACCESSDATA SUPPLEMENTAL APPENDIX

Understanding the UserAssist Registry Key

The purpose of this appendix is to explain some of the functionality of the UserAssist Key and how it might relate to artifact evidence found in the registry. At the time of this writing, the information contained in this paper is not published by Microsoft and is based on personal research. As such, please consider validating these results prior to relying on them as the basis for any conclusions. Please keep in mind that as with all Windows artifact behavior, the information contained in this appendix is subject to change at any time. In addition to the conditions stated below, there may be additional user actions that could contribute to these entries.

The following information is based on a new install of Windows XP-SP2 with all critical security updates installed as of July 2006.

THE BASICS



As shown in the figure above, the Start menu has a "UserAssist" area that holds shortcuts to applications most frequently used. This area is automatically populated from the UserAssist Key described below. Users can also manually place shortcuts above this area in a location referred

to here as the “user-definable” area. They can do so by dragging the shortcut to this area or through options described below.

Dragging a shortcut from the UserAssist area to the user-definable area will remove the shortcut from the UserAssist area in the **Start** menu, but do so will not remove the entry from the UserAssist Key described below. Removing an item from either the UserAssist area or the user-definable area (right-click > **Remove**) will delete the corresponding entries from the UserAssist Key.

The number of UserAssist entries displayed in the **Start** menu can vary depending on how much room is available to display them; however, entries continue to be created and updated in the UserAssist Key.

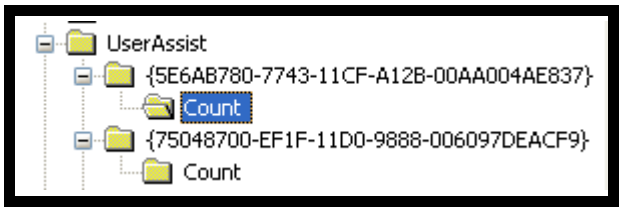
One obvious side effect of this feature is that the UserAssist key tracks the use of applications as well as shortcuts and other items. These are tracked by both frequency (total uses) as well as when they were last used.

The UserAssist registry key resides in the NTUSER.DAT file on disk at

Software\Microsoft\Windows \CurrentVersion\Explorer\UserAssist

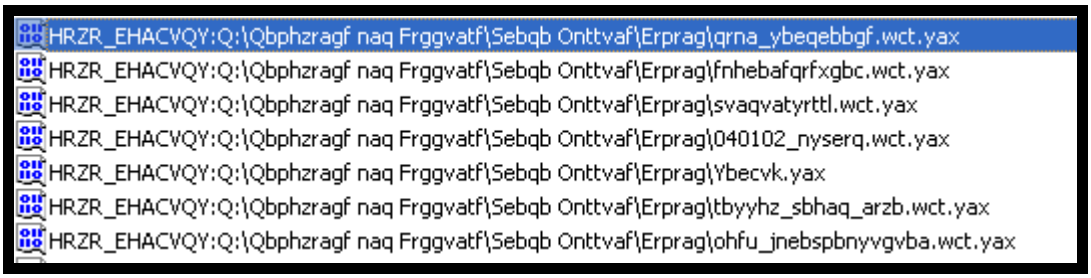
or, in the live registry, at

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



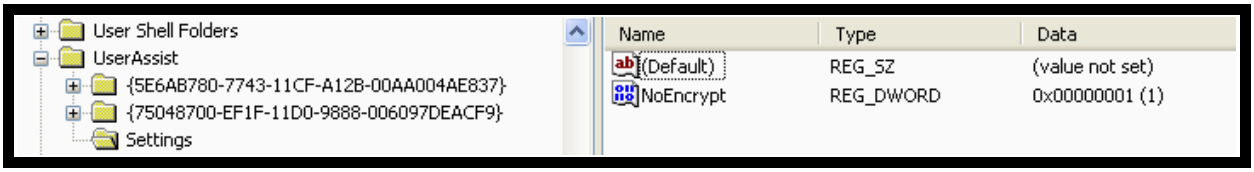
At this location you will find two GUID numbers, as shown in the figure. These GUIDs will be discussed individually. It is important to note that these numbers are globally unique and are the same across platforms. Inside each GUID is a key named Count, which holds the actual information discussed in this appendix.

Natively, the information in the Count key is obfuscated using a method called ROT13. In this method, the alphanumeric characters are rotated 13 spaces (N=A, O=B, and so on).



By adding a Settings key to the UserAssist area, then adding a value to that key named NoEncrypt, you can disable the UserAssist obfuscation by setting that value to 1. After making these keys, you must delete each GUID. The GUIDs will be re-created when you reboot, and any added values will be "plain-text". This will give a better understanding of what occurs in this key.

Important: Do not attempt this procedure unless you are familiar with registry editing and have backed up your registry.



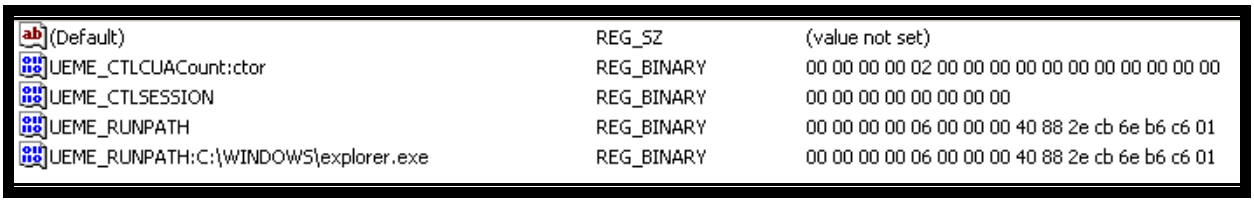
Note: The GUID values in this key can be deleted and will be re-created upon user login.

75048700-EF1F-11D0-9888-006097DEACF9/Count

When the Count key under the GUID ending ACF9 is initially created, the key holds two values. As shown in the figure above, these values are UEME_CTLCUACount:ctor and UEME_CTLSESSION.

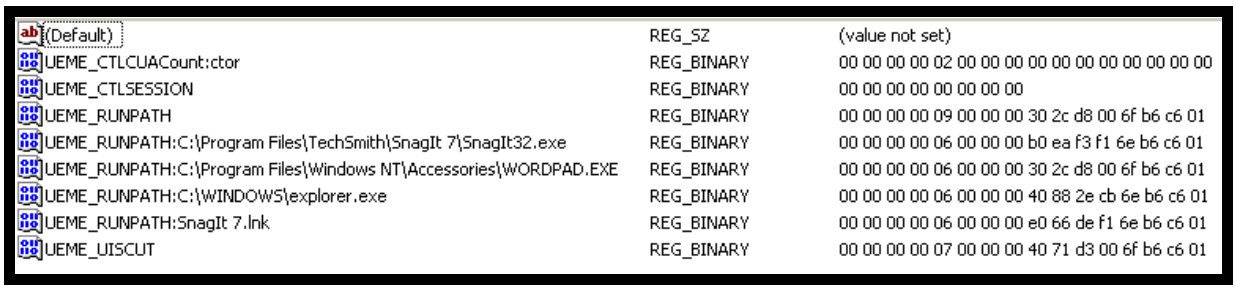
The first value UEME_CTLCUACount:ctor, does not seem to increment or change with time or use of this key. Research is still being conducted on its actual function.

The second value, UEME_CTLSESSION, is an eight-byte value divided into two four-byte segments (DWORDs). These two segments will be referred to here as the Session Number and the Session Date/Time. The UEME_CTLSESSION value will be discussed later in this appendix. For now, it is important to know that the Session Number DWORD is responsible for setting the first four bytes (DWORD) of any values placed in this key. In the above example, the Session Number is 0 (zero). As a result, all new or updated entries in this key will also receive the Session Number of 0.



In the figure above, the Explorer process has been stopped and restarted via the Task Manager. This has resulted in two new entries being placed in this key. One key is the path to the executable explorer.exe. The second entry, UEME_RUNPATH, is essentially a counter that increments each time a RUNPATH type value is added or changed. This value will be referred to here as the BASE RUNPATH. The format of any RUNPATH value appears to be the same.

The first four bytes (DWORD) is the Session Number. As the Session is currently 00 (as indicated by CTLSESSION), then this value is also 00. The next DWORD is a counter that increments each time an entry is updated. For unknown reasons, this value starts at 6, indicating a use count of 1. The next eight bytes is a 64-bit Date and Time value. Note in this example that the Date and Time values for the two new entries are identical.



(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 09 00 00 00 30 2c d8 00 6f b6 c6 01
UEME_RUNPATH:C:\Program Files\TechSmith\SnagIt 7\SnagIt32.exe	REG_BINARY	00 00 00 00 06 00 00 00 b0 ea f3 f1 6e b6 c6 01
UEME_RUNPATH:C:\Program Files\Windows NT\Accessories\WORDPAD.EXE	REG_BINARY	00 00 00 00 06 00 00 00 30 2c d8 00 6f b6 c6 01
UEME_RUNPATH:C:\WINDOWS\explorer.exe	REG_BINARY	00 00 00 00 06 00 00 00 40 88 2e cb 6e b6 c6 01
UEME_RUNPATH:SnagIt 7.lnk	REG_BINARY	00 00 00 00 06 00 00 00 e0 66 de f1 6e b6 c6 01
UEME_UISCUT	REG_BINARY	00 00 00 00 07 00 00 00 40 71 d3 00 6f b6 c6 01

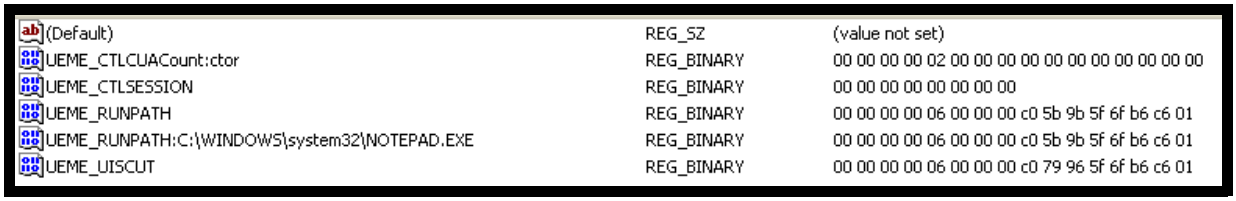
The figure above resulted from first opening the program SnagIt via a desktop shortcut. A WordPad document was then opened by double-clicking it and letting Windows call the appropriate program.

The first action (SnagIt) resulted in the addition of the RUNPATH value for SnagIt.lnk, as a desktop shortcut was used to launch it (note that it has a use count of 06). This action also updated the BASE RUNPATH value by incrementing the use counter to 07 (not shown), then updating the date and time value (not shown). The action also caused the value UEME_UISCUT to be generated with a use count of 6 and an updated date and time (not shown). This new value is referred to here as UISCUT (for “User Interface-Shortcut”).

The shortcut I used in turn called the program SnagIt.exe, which caused the addition of the RUNPATH value for SnagIt.exe. This caused the BASE RUNPATH value’s counter to be updated to 08 (not shown) and its date and time to be updated (not shown).

The next action, double-clicking a WordPad document, incremented the UISCUT value and updated its date and time. Windows then called WordPad, resulting in the addition of the WORDPAD.EXE RUNPATH value and the updating of the BASE RUNPATH to 09 with a current date and time. It is important to note that the updating the UISCUT value did not increment the BASE RUNPATH value. In the figure below, the BASE RUNPATH value has a date and time value identical to the value

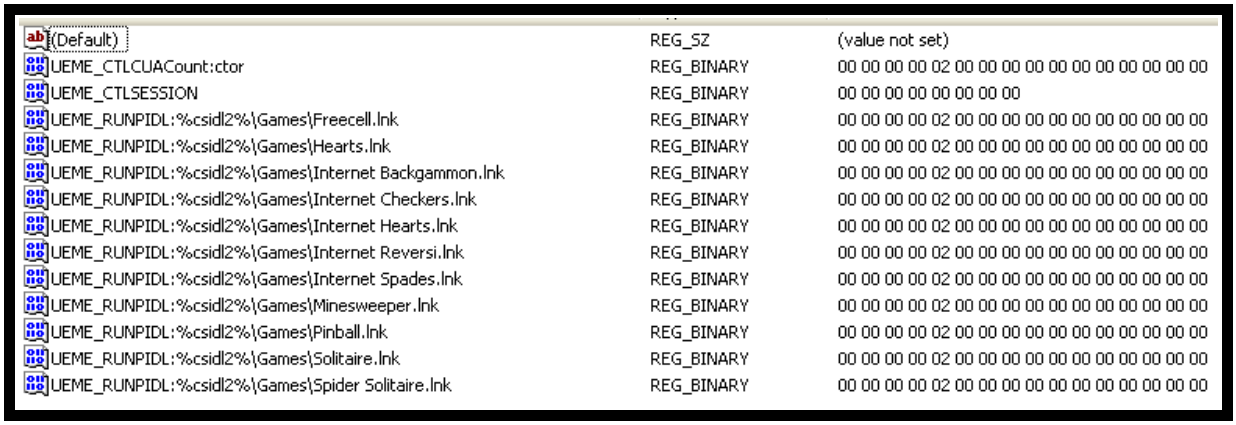
in WORDPAD.EXE. It is also important to note that the date-and-time value in UISCUT is actually only a few milliseconds from the date and time in the BASE RUNPATH value.



(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 06 00 00 00 c0 5b 9b 5f 6f b6 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\NOTEPAD.EXE	REG_BINARY	00 00 00 00 06 00 00 00 c0 5b 9b 5f 6f b6 c6 01
UEME_UISCUT	REG_BINARY	00 00 00 00 06 00 00 00 c0 79 96 5f 6f b6 c6 01

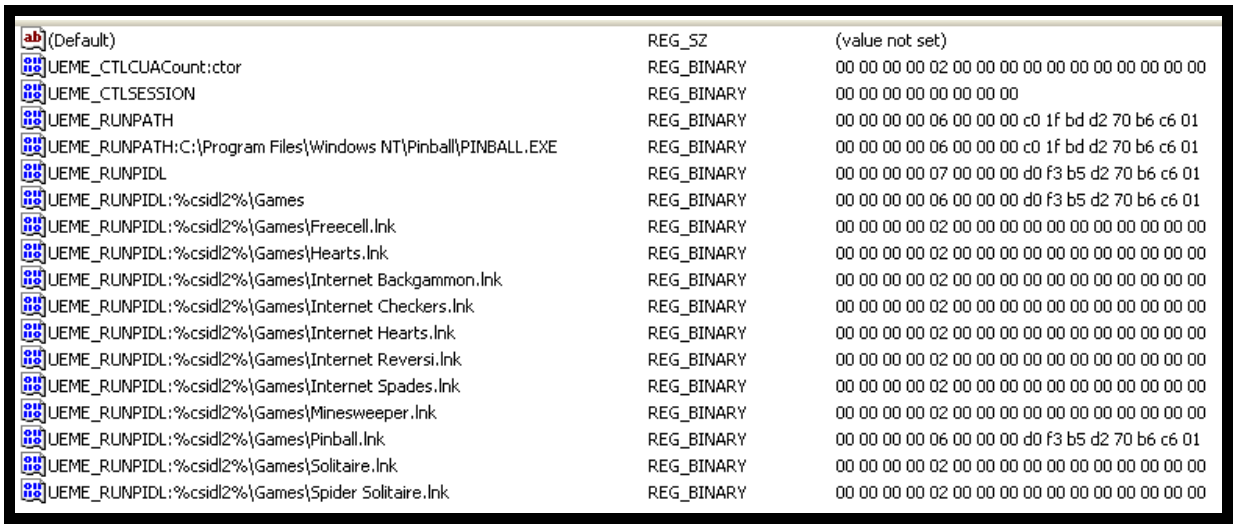
As an additional example, shown in the figure above, the count key was cleared, then a single text document was opened by double-clicking it. Again, the UISCUT and BASE RUNPATH values each incremented only one time.

START MENU



(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Freecell.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Hearts.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Backgammon.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Checkers.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Hearts.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Reversi.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Spades.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Minesweeper.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Pinball.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Solitaire.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Spider Solitaire.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00

As shown in the figure above, the Count Key was cleared again, prior to navigating to **Start** > **Programs** > **Games**. From this location, the mouse was held over, but not clicked on, each item in the list. In this instance, every item "moused" over is displayed in the list; however; each entry has a use count of 2. Note that these items start with UEME_RUNPIDL. None of the entries have a date or time entry. Note that, over several tests, this information was not written consistently.



(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 06 00 00 00 c0 1f bd d2 70 b6 c6 01
UEME_RUNPATH:C:\Program Files\Windows NT\Pinball\PINBALL.EXE	REG_BINARY	00 00 00 00 06 00 00 00 c0 1f bd d2 70 b6 c6 01
UEME_RUNPIDL	REG_BINARY	00 00 00 00 07 00 00 00 d0 f3 b5 d2 70 b6 c6 01
UEME_RUNPIDL:%csidl2%\Games	REG_BINARY	00 00 00 00 06 00 00 00 d0 f3 b5 d2 70 b6 c6 01
UEME_RUNPIDL:%csidl2%\Games\Freecell.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Hearts.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Backgammon.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Checkers.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Hearts.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Reversi.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Spades.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Minesweeper.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Pinball.lnk	REG_BINARY	00 00 00 00 06 00 00 00 d0 f3 b5 d2 70 b6 c6 01
UEME_RUNPIDL:%csidl2%\Games\Solitaire.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Spider Solitaire.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00

Next, Pinball was started from the **Start** menu. The figure above shows that a value named RUNPIDL was created and was given a use count of 06; this value will be referred to here as the BASE RUNPIDL. The BASE RUNPIDL value appears to track items accessed from the **Start** menu similarly to how the BASE RUNPATH value tracks executed programs and link files. Next, an entry was created for the RUNPIDL value Pinball.lnk. This entry was also given the use count value of 06. Next, the BASE RUNPIDL value was updated to 07 and an entry was created for the **Games** folder.

It is interesting to note that all three of these entries (RUNPIDL, Pinball.exe and the **Games** folder) have the same date-and-time value. In additional testing, it was noted that the **Games** folder entry and the Pinball.lnk entry did have different date-and-time values, although they were within a few milliseconds. In all cases, the entry for the folder was made after the entry for the link file.

After these entries were made, the BASE RUNPATH entry was updated and the entry was made for PINBALL.EXE (as shown in the figure above).

When an item in the **Start** menu is more then one folder deep, entries are made for each folder. The entries are made from the deepest folder back. The figure below is from the program named Regmon that can monitor writes to registry keys. The Regmon program was used to monitor writes to this key when opening FTK Imager from the **Program** menu. The figure shows the order in which the entries are actually written (read from the top down).

_RUNPIDL	SUCCESS	00 00 00 00 0B 00 00 00 ...
_RUNPIDL:%csidl2%\AccessData\FTK Imager\FTK Imager.lnk	SUCCESS	00 00 00 00 06 00 00 00 ...
_RUNPIDL	SUCCESS	00 00 00 00 0C 00 00 00 ...
_RUNPIDL:%csidl2%\AccessData\FTK Imager	SUCCESS	00 00 00 00 06 00 00 00 ...
_RUNPIDL	SUCCESS	00 00 00 00 0D 00 00 00 ...
_RUNPIDL:%csidl2%\AccessData	SUCCESS	00 00 00 00 06 00 00 00 ...
_RUNPATH	SUCCESS	00 00 00 00 0D 00 00 00 ...
_RUNPATH:C:\Program Files\AccessData\AccessData FTK Imager\FTK Imager.exe	SUCCESS	00 00 00 00 06 00 00 00 ...

As a further example, the NOTEPAD.EXE program was started from the **Start** menu. Values are created and updated as expected, as shown in the figure below.

(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 07 00 00 00 d0 c6 c9 04 71 b6 c6 01
UEME_RUNPATH:C:\Program Files\Windows NT\Pinball\PINBALL.EXE	REG_BINARY	00 00 00 00 06 00 00 00 c0 1f bd d2 70 b6 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\notepad.exe	REG_BINARY	00 00 00 00 06 00 00 00 d0 c6 c9 04 71 b6 c6 01
UEME_RUNPIDL	REG_BINARY	00 00 00 00 09 00 00 00 d0 55 c7 04 71 b6 c6 01
UEME_RUNPIDL:%csidl2%\Accessories	REG_BINARY	00 00 00 00 06 00 00 00 d0 55 c7 04 71 b6 c6 01
UEME_RUNPIDL:%csidl2%\Accessories\Notepad.lnk	REG_BINARY	00 00 00 00 06 00 00 00 d0 55 c7 04 71 b6 c6 01
UEME_RUNPIDL:%csidl2%\Games	REG_BINARY	00 00 00 00 06 00 00 00 d0 f3 b5 d2 70 b6 c6 01
UEME_RUNPIDL:%csidl2%\Games\Freecell.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Hearts.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Backgammon.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Checkers.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Hearts.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Reversi.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Internet Spades.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Minesweeper.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Pinball.lnk	REG_BINARY	00 00 00 00 06 00 00 00 d0 f3 b5 d2 70 b6 c6 01
UEME_RUNPIDL:%csidl2%\Games\Solitaire.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_RUNPIDL:%csidl2%\Games\Spider Solitaire.lnk	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00

Lastly, it appears that the RUNPIDL information is recorded only when the Windows XP **Start** menu is used. If the "classic" **Start** menu is used, RUNPIDL information is not recorded. In the figure below, the Solitaire program was opened from the **Start** menu while using the "classic" menu.

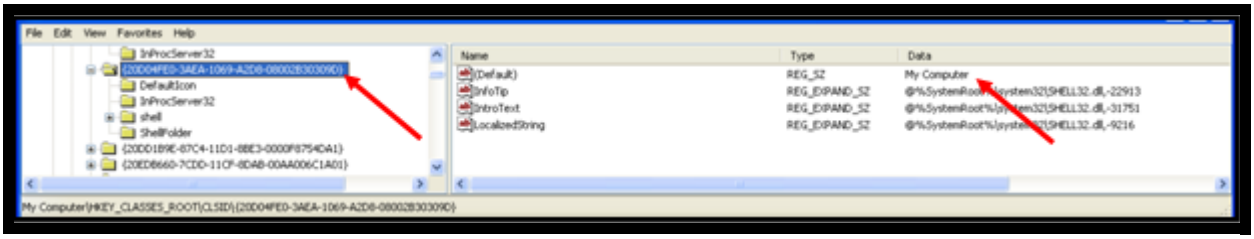
Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 06 00 00 00 90 44 08 b3 7a b9 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\sol.exe	REG_BINARY	00 00 00 00 06 00 00 00 90 44 08 b3 7a b9 c6 01

DESKTOP ITEMS

Starting from a fresh Count Key, My Computer was opened by double-clicking the icon on the desktop. This resulted in a UISCUT value being created (or updated). It also caused the expected change to the BASE RUNPATH value. The value created for the actual shortcut was not called My Computer. Instead, a GUID entry was used.

(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 06 00 00 00 30 4b 3c 5d 71 b6 c6 01
UEME_RUNPATH:::{20D04FE0-3AEA-1069-A2D8-08002B30309D}	REG_BINARY	00 00 00 00 06 00 00 00 30 4b 3c 5d 71 b6 c6 01
UEME_UISCUT	REG_BINARY	00 00 00 00 06 00 00 00 30 4b 3c 5d 71 b6 c6 01

Many instances were found where GUID entries are used. Some examples are My Computer, My Network Places and the Recycle Bin. By searching the registry for this GUID value, it can be identified as belonging to "My Computer" via the CLSID Key located in the SOFTWARE registry file at \classes\CLSID or in a live registry at HKEY_CLASSES_ROOT\CLSID\. In the example below, the CLSID key identifies this GUID as belonging to My Computer.



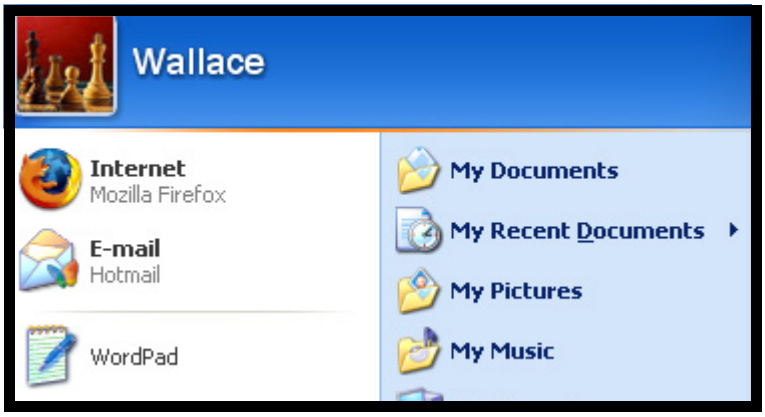
The following figure shows other examples of GUIDs created from various Desktop Icons. In this example:

- 208D2C60-3AEA-1069-A2D7-08002B30309D = My Network Places
- 20D04FE0-3AEA-1069-A2D8-08002B30309D = My Computer
- 450D8FBA-AD25-11D0-98A8-0800361B1103 = My Documents
- 645FF040-5081-101B-9F08-00AA002F954E = Recycle Bin

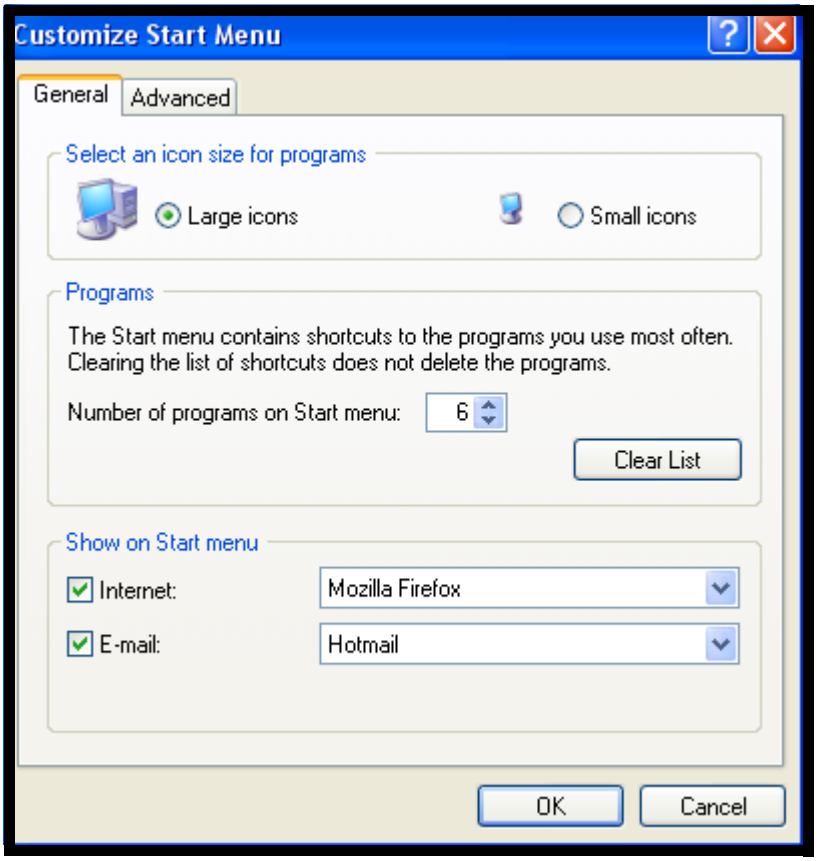
Desktop icons without corresponding GUIDs appear to be treated as any typical link file.

Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 09 00 00 00 a0 65 c3 0f db 2d c7 01
UEME_RUNPATH:::{208D2C60-3AEA-1069-A2D7-08002B30309D}	REG_BINARY	00 00 00 00 06 00 00 00 50 19 4d 0e db 2d c7 01
UEME_RUNPATH:::{20D04FE0-3AEA-1069-A2D8-08002B30309D}	REG_BINARY	00 00 00 00 06 00 00 00 f0 41 46 0b db 2d c7 01
UEME_RUNPATH:::{450D8FBA-AD25-11D0-98A8-0800361B1103}	REG_BINARY	00 00 00 00 06 00 00 00 b0 37 f8 0c db 2d c7 01
UEME_RUNPATH:::{645FF040-5081-101B-9F08-00AA002F954E}	REG_BINARY	00 00 00 00 06 00 00 00 a0 65 c3 0f db 2d c7 01
UEME_UISCUT	REG_BINARY	00 00 00 00 09 00 00 00 a0 65 c3 0f db 2d c7 01

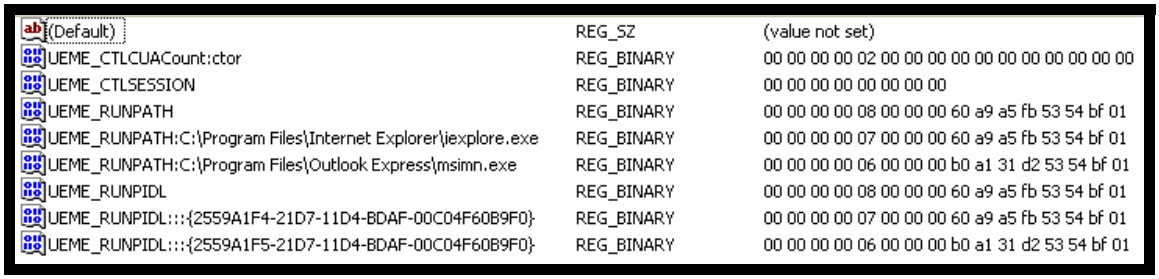
Another interesting set of entries found in this key comes from use of the Internet and email shortcuts that can be optionally added to the **Start** menu. The example in the figure below shows these icons. The icon for WordPad is from the UserAssist key. There is a very faint line separating the two sections.



The **Customize Start Menu** settings can be managed through the start menu properties.



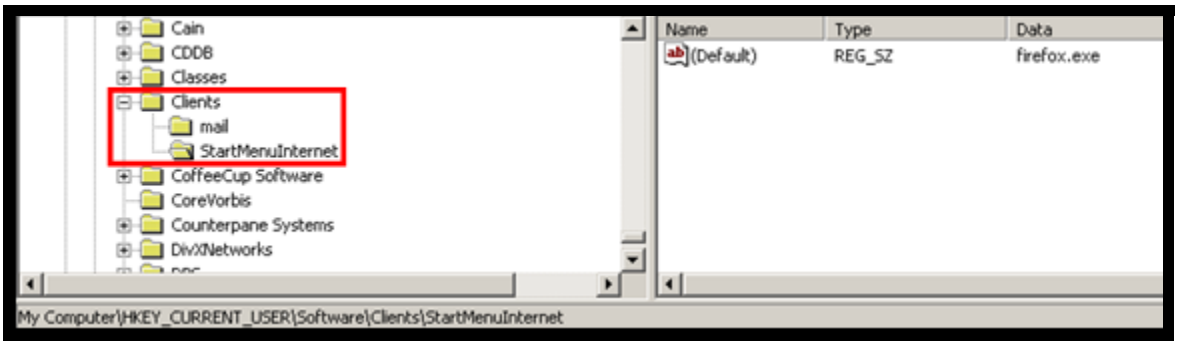
Using these shortcuts also results in GUID entries. Tracing these entries through the CLSID key shows that 2559a1f4-21d7-11d4-bdaf-00c04f60b9f0 = Internet, and 2559a1f5-21d7-11d4-bdaf-00c04f60b9f0 = email. Note that there are also corresponding entries for the actual programs.



(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 08 00 00 00 60 a9 a5 fb 53 54 bf 01
UEME_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe	REG_BINARY	00 00 00 00 07 00 00 00 60 a9 a5 fb 53 54 bf 01
UEME_RUNPATH:C:\Program Files\Outlook Express\msimn.exe	REG_BINARY	00 00 00 00 06 00 00 00 b0 a1 31 d2 53 54 bf 01
UEME_RUNPIDL	REG_BINARY	00 00 00 00 08 00 00 00 60 a9 a5 fb 53 54 bf 01
UEME_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0}	REG_BINARY	00 00 00 00 07 00 00 00 60 a9 a5 fb 53 54 bf 01
UEME_RUNPIDL:::{2559A1F5-21D7-11D4-BDAF-00C04F60B9F0}	REG_BINARY	00 00 00 00 06 00 00 00 b0 a1 31 d2 53 54 bf 01

There is a location in the registry where you can identify which program is associated with each of the above settings. These values are at HKEY_CURRENT_USER\Software\Clients\ in a live registry and in a user's NTUSER.DAT file at SOFTWARE\Clients. The figure below shows the value StartMenuInternet holding the value Firefox.exe. The value Mail (not shown) indicates Hotmail.

Note: Similar values are stored at HKEY_LOCAL_MACHINE\SOFTWARE\Clients; however, these values do not always coincide with the active StartMenu choices.



In the example in the figure below, the StartMenuInternet option was originally set to Firefox. Using that menu item resulted in the GUID ending in B9F0 (StartMenuInternet) and also the entry for Firefox.exe itself. Next, the option was changed to Internet Explorer in the Start Menu properties, then that menu item was executed again. This resulted in a new entry for iexplorer.exe, and the GUID value remained the same with an updated time. The entry for explorer.exe existed prior to this test.

Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 08 00 00 00 20 b8 2b 07 e6 13 c7 01
UEME_RUNPATH:C:\PROGRA~1\MOZILL~1\FIREFOX.EXE	REG_BINARY	00 00 00 00 06 00 00 00 50 db 41 d5 e5 13 c7 01
UEME_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe	REG_BINARY	00 00 00 00 06 00 00 00 20 b8 2b 07 e6 13 c7 01
UEME_RUNPATH:C:\WINDOWS\explorer.exe	REG_BINARY	00 00 00 00 06 00 00 00 80 33 5d b9 e5 13 c7 01
UEME_RUNPIDL	REG_BINARY	00 00 00 00 07 00 00 00 20 b8 2b 07 e6 13 c7 01
UEME_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0}	REG_BINARY	00 00 00 00 07 00 00 00 20 b8 2b 07 e6 13 c7 01

Starting with a fresh Count Key, the Time and Date control was opened from the Desktop. This resulted in an entry named RUNCPL, which will be referred to as the BASE RUNCPL (below). The behavior of this key is identical to the RUNPATH and RUNPIDL in that it increments each time a corresponding value is added. In this instance, a value named timedate.cpl was added.

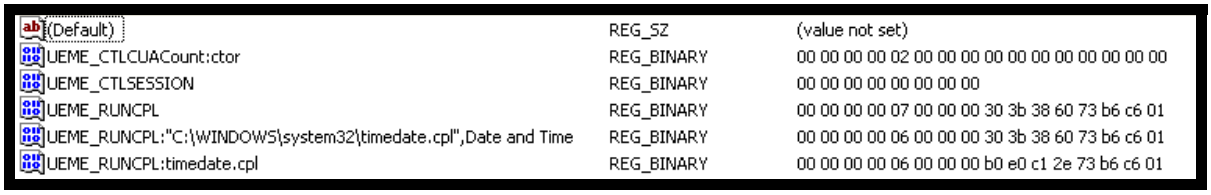
Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNCPL	REG_BINARY	00 00 00 00 06 00 00 00 40 f1 47 a9 7e b9 c6 01
UEME_RUNCPL:timedate.cpl	REG_BINARY	00 00 00 00 06 00 00 00 40 f1 47 a9 7e b9 c6 01

Next, the Time and Date control was opened from the Control Panel in the **Start** menu. This still resulted in the BASE RUNCPL value being

updated; however, it also resulted in a different individual value ending in the words “Date and Time” (in the figure below). This may be important in investigations where a user is alleged to have altered date and time information.

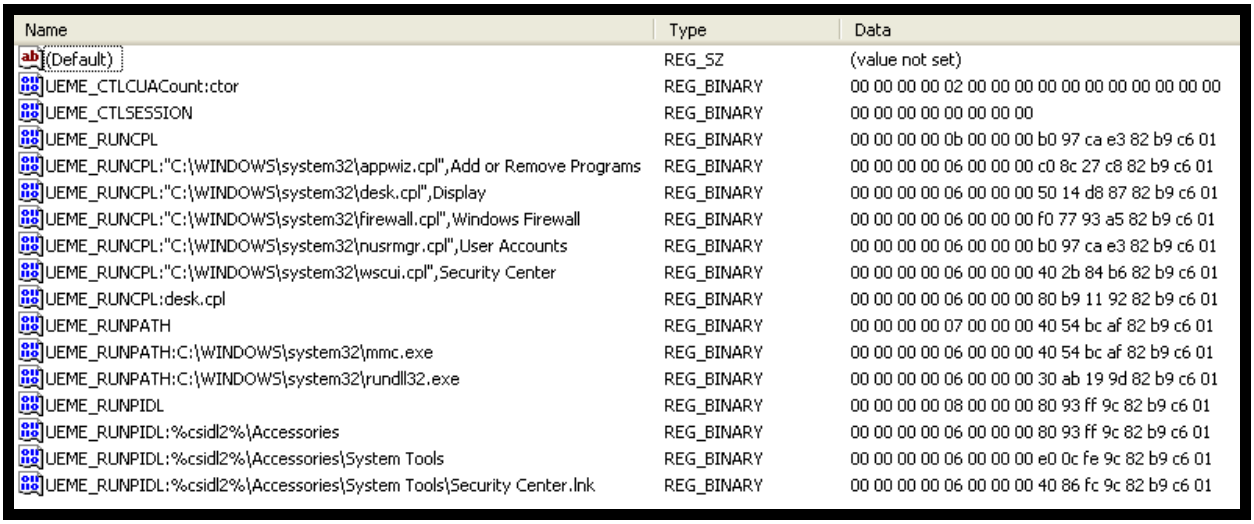
Note: The date and time recorded is captured when the item is accessed. For example, if you open the Time and Date Control console on July 31, 2006, change the date to July 31, 2010 and close the control console, the date and time recorded will be the 2006 date. If you were to open the console to change the date back to 2006, the new date and time would reflect the 2010 date.

The Session ID and Session Time may also assist in determining chronological ordering of these events (see *Session ID* on page 14).



(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNCPL	REG_BINARY	00 00 00 00 07 00 00 00 30 3b 38 60 73 b6 c6 01
UEME_RUNCPL:"C:\WINDOWS\system32\timedate.cpl",Date and Time	REG_BINARY	00 00 00 00 06 00 00 00 30 3b 38 60 73 b6 c6 01
UEME_RUNCPL:timedate.cpl	REG_BINARY	00 00 00 00 06 00 00 00 b0 e0 c1 2e 73 b6 c6 01

The figure below some other example of items in the Control Panel, as well as opening the Security Center via the **Start** menu.



Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNCPL	REG_BINARY	00 00 00 00 0b 00 00 00 b0 97 ca e3 82 b9 c6 01
UEME_RUNCPL:"C:\WINDOWS\system32\appwiz.cpl",Add or Remove Programs	REG_BINARY	00 00 00 00 06 00 00 00 c0 8c 27 c8 82 b9 c6 01
UEME_RUNCPL:"C:\WINDOWS\system32\desk.cpl",Display	REG_BINARY	00 00 00 00 06 00 00 00 50 14 d8 87 82 b9 c6 01
UEME_RUNCPL:"C:\WINDOWS\system32\firewall.cpl",Windows Firewall	REG_BINARY	00 00 00 00 06 00 00 00 f0 77 93 a5 82 b9 c6 01
UEME_RUNCPL:"C:\WINDOWS\system32\nusrmgr.cpl",User Accounts	REG_BINARY	00 00 00 00 06 00 00 00 b0 97 ca e3 82 b9 c6 01
UEME_RUNCPL:"C:\WINDOWS\system32\wscui.cpl",Security Center	REG_BINARY	00 00 00 00 06 00 00 00 40 2b 84 b6 82 b9 c6 01
UEME_RUNCPL:desk.cpl	REG_BINARY	00 00 00 00 06 00 00 00 80 b9 11 92 82 b9 c6 01
UEME_RUNPATH	REG_BINARY	00 00 00 00 07 00 00 00 40 54 bc af 82 b9 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\mmc.exe	REG_BINARY	00 00 00 00 06 00 00 00 40 54 bc af 82 b9 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\rundll32.exe	REG_BINARY	00 00 00 00 06 00 00 00 30 ab 19 9d 82 b9 c6 01
UEME_RUNPIDL	REG_BINARY	00 00 00 00 08 00 00 00 80 93 ff 9c 82 b9 c6 01
UEME_RUNPIDL:%csidl2%\Accessories	REG_BINARY	00 00 00 00 06 00 00 00 80 93 ff 9c 82 b9 c6 01
UEME_RUNPIDL:%csidl2%\Accessories\System Tools	REG_BINARY	00 00 00 00 06 00 00 00 e0 0c fe 9c 82 b9 c6 01
UEME_RUNPIDL:%csidl2%\Accessories\System Tools\Security Center.lnk	REG_BINARY	00 00 00 00 06 00 00 00 40 86 fc 9c 82 b9 c6 01

QUICK LAUNCH TOOLBAR

The Quick Launch Toolbar appears to have two sections. They will be referred to here as Resident (residing in the actual toolbar) and Nonresident (in the extended ">>" area of the toolbar).

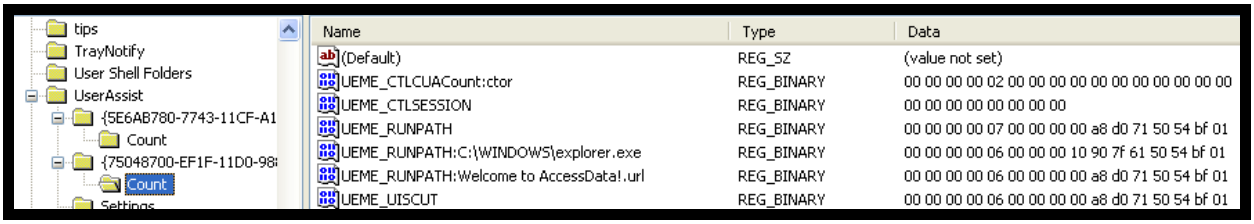
Running programs whose icons are "resident" will not place records in the Key; however, the UEME_UIQCUT item will be updated each time. In the below example, starting with a clean Count Key, Internet Explorer was started from the Quick Launch Toolbar.

Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_UIQCUT	REG_BINARY	00 00 00 00 06 00 00 00 c0 21 d5 07 d7 bf c6 01

Running an extended item such as Media Player (shown above) will cause a value to be written but will not increment UEME_UIQCUT (shown below).

Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	00 00 00 00 00 00 00 00
UEME_RUNPATH	REG_BINARY	00 00 00 00 06 00 00 00 d0 2b a6 21 d7 bf c6 01
UEME_RUNPATH:C:\Program Files\Windows Media Player\wmplayer.exe	REG_BINARY	00 00 00 00 06 00 00 00 d0 2b a6 21 d7 bf c6 01
UEME_UIQCUT	REG_BINARY	00 00 00 00 06 00 00 00 c0 21 d5 07 d7 bf c6 01

Lastly, the Count Key was again deleted, and an Internet shortcut was created on the Desktop and executed. This resulted in the entries being made in the Count Key for the GUID ending in ACF9, as shown in the figure below. Note that they include entries for the URL, the executable, and UISCUT.



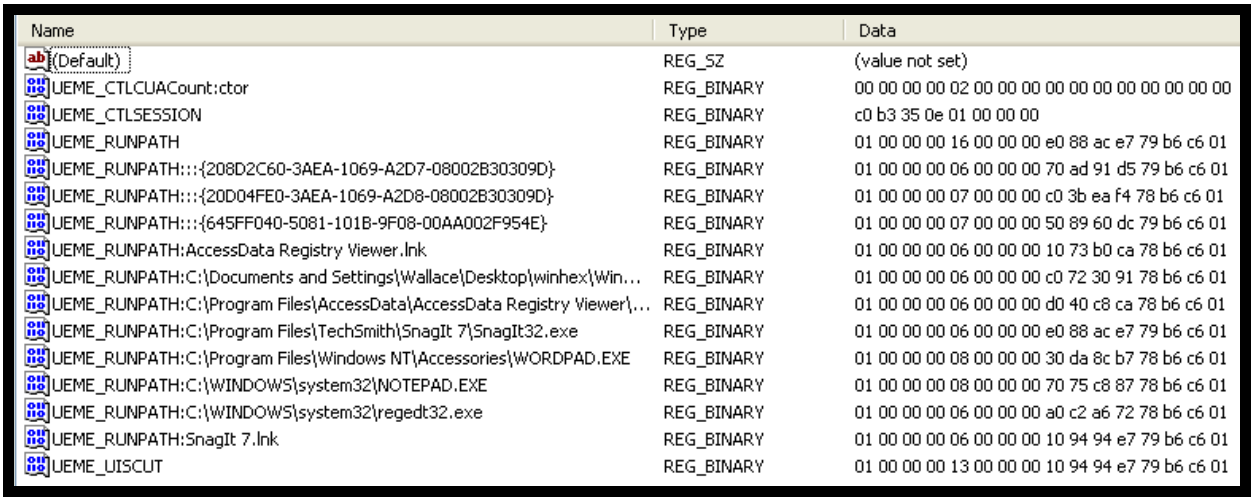
SESSION ID

In an apparent effort to group these entries chronologically, the first DWORD of each entry holds a numeric value that will be referred to here as the Session ID. At some point, the value CTLSESSION will be updated to hold two pieces of information. Testing thus far indicates that a new session is created in somewhere between 12 hours and 24 hours. The factors (such as activity) that may affect this are unknown. Initially the value is 00 with no timestamp. Rebooting or waiting a few minutes appears to create the initial Session ID, regardless of the elapsed time. As far as has been observed, the session ID number continues to increment and does not reset.

The first DWORD of this value is actually a date and time reference for this particular Session number (to be discussed in the next paragraph). The second DWORD is the session number itself. As shown in the figure below, the current session number is 01. This will cause any entry that is created or updated to have that session number. Any existing entries from prior sessions will keep their respective session ID numbers until they are accessed again. At that time, they will be updated to the current session.

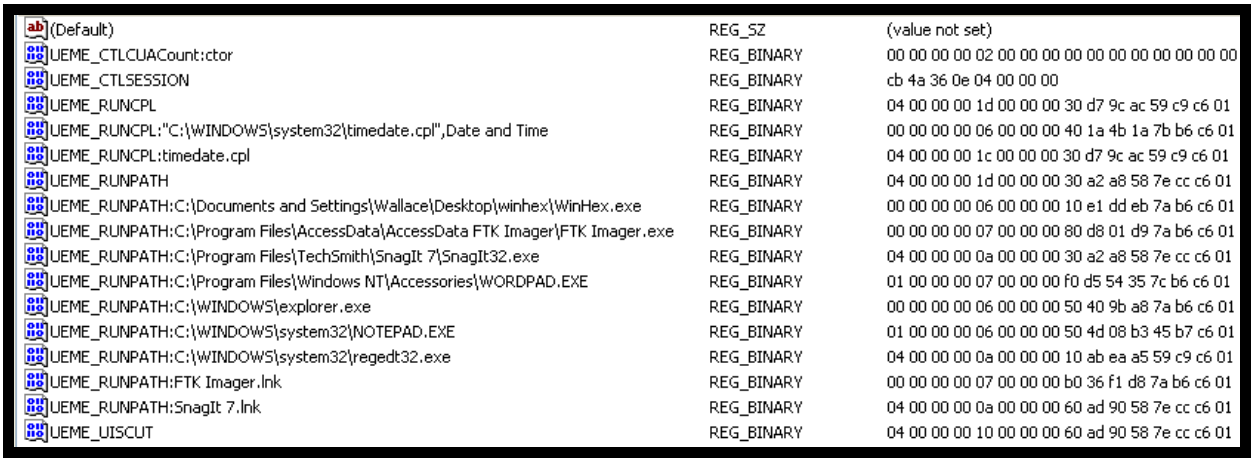
The format for the date and time stored in the CTLSESSION value is actually a standard 64-bit FILETIME, right-shifted 29 bits and stored in a four-byte value. These can be converted by multiplying the stored value by 536,870,911 (1FFFFFFF hex). In the example below, 0e 35 b3 c0 hex is decimal 238400448. That value multiplied by 536,870,911 (1FFFFFFF hex) is 127990265700568128 decimal or 01C6B677F1CA4C40. This value, when plugged into many date and time utilities, shows the following:

8/2/2006 14:09:30



Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	c0 b3 35 0e 01 00 00 00
UEME_RUNPATH	REG_BINARY	01 00 00 00 16 00 00 00 e0 88 ac e7 79 b6 c6 01
UEME_RUNPATH:::{208D2C60-3AEA-1069-A2D7-08002B30309D}	REG_BINARY	01 00 00 00 06 00 00 00 70 ad 91 d5 79 b6 c6 01
UEME_RUNPATH:::{20D04FE0-3AEA-1069-A2D8-08002B30309D}	REG_BINARY	01 00 00 00 07 00 00 00 c0 3b ea f4 78 b6 c6 01
UEME_RUNPATH:::{645FF040-5081-101B-9F08-00AA002F954E}	REG_BINARY	01 00 00 00 07 00 00 00 50 89 60 dc 79 b6 c6 01
UEME_RUNPATH:AccessData Registry Viewer.lnk	REG_BINARY	01 00 00 00 06 00 00 00 10 73 b0 ca 78 b6 c6 01
UEME_RUNPATH:C:\Documents and Settings\Wallace\Desktop\winhex\Win...	REG_BINARY	01 00 00 00 06 00 00 00 c0 72 30 91 78 b6 c6 01
UEME_RUNPATH:C:\Program Files\AccessData\AccessData Registry Viewer\...	REG_BINARY	01 00 00 00 06 00 00 00 d0 40 c8 ca 78 b6 c6 01
UEME_RUNPATH:C:\Program Files\TechSmith\SnagIt 7\SnagIt32.exe	REG_BINARY	01 00 00 00 06 00 00 00 e0 88 ac e7 79 b6 c6 01
UEME_RUNPATH:C:\Program Files\Windows NT\Accessories\WORDPAD.EXE	REG_BINARY	01 00 00 00 08 00 00 00 30 da 8c b7 78 b6 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\NOTEPAD.EXE	REG_BINARY	01 00 00 00 08 00 00 00 70 75 c8 87 78 b6 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\regedt32.exe	REG_BINARY	01 00 00 00 06 00 00 00 a0 c2 a6 72 78 b6 c6 01
UEME_RUNPATH:SnagIt 7.lnk	REG_BINARY	01 00 00 00 06 00 00 00 10 94 94 e7 79 b6 c6 01
UEME_UISCUT	REG_BINARY	01 00 00 00 13 00 00 00 10 94 94 e7 79 b6 c6 01

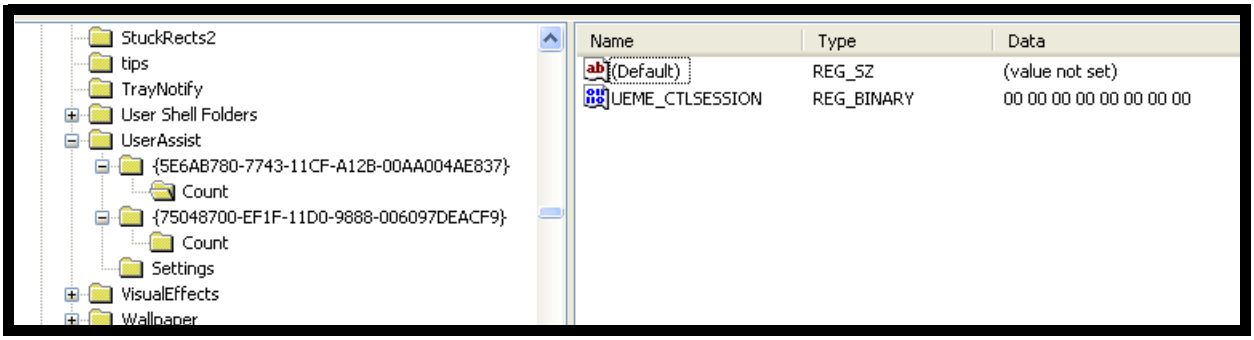
The figure below shows how the Session number is updated only for those items accessed, or for new items that are created.



(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	cb 4a 36 0e 04 00 00 00
UEME_RUNCPL	REG_BINARY	04 00 00 00 1d 00 00 00 30 d7 9c ac 59 c9 c6 01
UEME_RUNCPL:"C:\WINDOWS\system32\timedate.cpl",Date and Time	REG_BINARY	00 00 00 00 06 00 00 00 40 1a 4b 1a 7b b6 c6 01
UEME_RUNCPL:timedate.cpl	REG_BINARY	04 00 00 00 1c 00 00 00 30 d7 9c ac 59 c9 c6 01
UEME_RUNPATH	REG_BINARY	04 00 00 00 1d 00 00 00 30 a2 a8 58 7e cc c6 01
UEME_RUNPATH:C:\Documents and Settings\Wallace\Desktop\winhex\WinHex.exe	REG_BINARY	00 00 00 00 06 00 00 00 10 e1 dd eb 7a b6 c6 01
UEME_RUNPATH:C:\Program Files\AccessData\AccessData FTK Imager\FTK Imager.exe	REG_BINARY	00 00 00 00 07 00 00 00 80 d8 01 d9 7a b6 c6 01
UEME_RUNPATH:C:\Program Files\TechSmith\SnagIt 7\SnagIt32.exe	REG_BINARY	04 00 00 00 0a 00 00 00 30 a2 a8 58 7e cc c6 01
UEME_RUNPATH:C:\Program Files\Windows NT\Accessories\WORDPAD.EXE	REG_BINARY	01 00 00 00 07 00 00 00 f0 d5 54 35 7c b6 c6 01
UEME_RUNPATH:C:\WINDOWS\explorer.exe	REG_BINARY	00 00 00 00 06 00 00 00 50 40 9b a8 7a b6 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\NOTEPAD.EXE	REG_BINARY	01 00 00 00 06 00 00 00 50 4d 08 b3 45 b7 c6 01
UEME_RUNPATH:C:\WINDOWS\system32\regedt32.exe	REG_BINARY	04 00 00 00 0a 00 00 00 10 ab ea a5 59 c9 c6 01
UEME_RUNPATH:FTK Imager.lnk	REG_BINARY	00 00 00 00 07 00 00 00 b0 36 f1 d8 7a b6 c6 01
UEME_RUNPATH:SnagIt 7.lnk	REG_BINARY	04 00 00 00 0a 00 00 00 60 ad 90 58 7e cc c6 01
UEME_UISCUT	REG_BINARY	04 00 00 00 10 00 00 00 60 ad 90 58 7e cc c6 01

5E6AB780-7743-11CF-A12B-00AA004AE837/COUNT

The Count key for the GUID ending in E837 contains information relating to the use of Favorite Places in IE, as well as possibly other actions not yet discovered. When newly created, this key holds only the CTLSESSION value. The CTLSESSION value appears to operate the same as the corresponding value in the previously discussed Count Key. It was observed, however, that they are not the same date and time (meaning that they operate independently).



The entries in the figure below result from using a Favorite Place entry in Internet Explorer. The URL entry is created regardless of whether the address is actually reached. The UITOOLBAR values were created when any item in the standard toolbar was accessed. The value UITOOLBAR:0x1,126 was created from clicking the **Favorites** button within the toolbar. UITOOLBAR appears to increment with every use of a toolbar button. The individual entries appear to be incremented once when they are opened and again if the button is used to close that tool.

Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	71 9f 38 0e 01 00 00 00
UEME_RUNPIDL	REG_BINARY	01 00 00 00 06 00 00 00 40 7b f8 4e ee 13 c7 01
UEME_RUNPIDL:%csidl6%\103.5 The Fox.url	REG_BINARY	01 00 00 00 06 00 00 00 e0 01 fa 4e ee 13 c7 01
UEME_UITOOLBAR	REG_BINARY	01 00 00 00 07 00 00 00 60 ed 7b 4d ee 13 c7 01
UEME_UITOOLBAR:0x1,126	REG_BINARY	01 00 00 00 07 00 00 00 60 ed 7b 4d ee 13 c7 01

The figure below shows this key after the use of several different tools such as Favorites, Search, Research, Print etc. How individual UITOOLBAR entries are identified is still being researched.

Name	Type	Data
(Default)	REG_SZ	(value not set)
UEME_CTLCUACount:ctor	REG_BINARY	01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
UEME_CTLSESSION	REG_BINARY	71 9f 38 0e 01 00 00 00
UEME_RUNPIDL	REG_BINARY	01 00 00 00 08 00 00 00 00 52 69 68 f0 13 c7 01
UEME_RUNPIDL:%csidl6%\103.5 The Fox.url	REG_BINARY	01 00 00 00 06 00 00 00 e0 01 fa 4e ee 13 c7 01
UEME_RUNPIDL:%csidl6%\AccessData Corporation.url	REG_BINARY	01 00 00 00 06 00 00 00 00 72 a0 57 f0 13 c7 01
UEME_RUNPIDL:%csidl6%\http--www.sata-io.org-docs-serialata - a co...	REG_BINARY	01 00 00 00 06 00 00 00 00 52 69 68 f0 13 c7 01
UEME_UITOOLBAR	REG_BINARY	01 00 00 00 19 00 00 00 60 90 4b 56 f0 13 c7 01
UEME_UITOOLBAR:0x1,104	REG_BINARY	01 00 00 00 06 00 00 00 e0 d5 0f 09 f0 13 c7 01
UEME_UITOOLBAR:0x1,123	REG_BINARY	01 00 00 00 07 00 00 00 c0 c5 7c 8c ee 13 c7 01
UEME_UITOOLBAR:0x1,126	REG_BINARY	01 00 00 00 0d 00 00 00 60 90 4b 56 f0 13 c7 01
UEME_UITOOLBAR:0x1,2001	REG_BINARY	01 00 00 00 08 00 00 00 a0 fc cb c5 ef 13 c7 01
UEME_UITOOLBAR:0x1,2003	REG_BINARY	01 00 00 00 06 00 00 00 d0 12 32 4c ef 13 c7 01
UEME_UITOOLBAR:0x4,104	REG_BINARY	01 00 00 00 06 00 00 00 e0 d5 0f 09 f0 13 c7 01
UEME_UITOOLBAR:0x4,2001	REG_BINARY	01 00 00 00 08 00 00 00 a0 fc cb c5 ef 13 c7 01
UEME_UITOOLBAR:0x4,2003	REG_BINARY	01 00 00 00 06 00 00 00 d0 12 32 4c ef 13 c7 01

In conclusion, the UserAssist key can provide significant information regarding suspect activity such as which programs are consistently used, evidence of uninstalled programs, evidence of a file's existence, and so on. As with most registry contents, this is uncharted territory. While the described behavior has been found to be consistent, different platforms and user configurations may produce different results. Anyone with additional information or differing behavior is urged to contact the author so that updates and additional research can be conducted.