# A Comparison of Windows 7 and 8 Registry


## Matthew Brewer B.S., Christopher Vance B.S., Terry Fenger Ph.D., Cpl. Robert J. Boggs

Marshall University Forensic Science Center, 1401 Forensic Science Dr., Huntington, WV 25701
West Virginia State Police: Digital Forensics Unit, 1401 Forensic Science Dr., Huntington, WV 25701



## Abstract

The introduction of Windows® 8 was a big change for Microsoft's® traditional operating system. With changes to the operating system, one would expect changes to the registry, the Windows logging system that records computer functions and user information. The four main registry files: NTUSER.DAT, SAM, SYSTEM, and SECURITY, were examined for changes in subkey locations and recorded information.

Based on the examination of the Windows 8 registry, there were only minimal changes to registry. Subkey locations remained primarily the same with many values being added. Some of the examined registry files did not contain any recorded information but the subkey was in the same location as Windows 7. However, many changes occurred in the recording of user account information. For the first time, Windows 8 allows either local or online user accounts which added a large number of values to the SAM file. Online user SAM subkeys contain more values than a local account, but the number of log-ons are not counted. Local user SAM files contain the F value, V value, and password hint like previous versions of Windows. Applications used to load a particular file extensions were recorded using App ID's, in the NTUSER.DAT file, making it difficult to identify the program. The other root keys did not contain any significant changes.


## Introduction

- Windows 8 was an overhaul of the Windows operating system. Therefore, changes were expected to the Windows Registry
- The Windows registry is a hierarchical data base central to the operations of the Windows operating system
- The registry allows the operating system and programs to access information, software, and hardware essential for proper function. Information in the registry includes, but is not limited to, the user profiles on the machine, installed programs, programs used to execute a particular file extension, and removable media connected to the system
- The main forensically relevant registry hives are: NTUSER.DAT, SAM, SYSTEM, and SOFTWARE
- NTUSER.DAT – each user has its own NTUSER.DAT file, it contains information specific to that user
- SAM – contains all the information about the users of the computer, making it one of the most forensically relevant registry files
- SYSTEM – contains information about the operating system and hardware configuration. Forensic information included is mounted devices and drives, hardware installation, and start up parameters
- SOFTWARE – contains information about installed software and applications

## Materials and Methods

- Windows 8 operating system
- AccessData's FTK Imager3.1.3.2
- AccessData's Registry Viewer 1.5.4.44
- Test hard drive
- Image (Target) hard drive

## Results and Discussion

The SAM registry hive contains information about the user accounts on the computer. Windows 8 offers the option to have two different types of accounts, an online Microsoft account and a standard local account. The Microsoft accounts offers addition features such as cloud storage and interoperability with all Windows 8 devices. The keys found in the SAM file were different for each type of account. The F and V values provided the majority of this data. Offsets within these values provide the user account properties.

| Name | Type | Data |
|---|---|---|
| F | REG_BINARY | 02 00 01 00 00 00 00 00 3F 6D 19 F3 75 60 CE 01 00 00 ... |
| V | REG_BINARY | 00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 1A 00 ... |
| ForcePasswordReset | REG_BINARY | 00 00 00 00 |
| UserPasswordHint | REG_BINARY | 53 00 61 00 6D 00 65 00 20 00 62 00 75 00 74 00 20 00 6... |

Figure 1 – Local user account SAM results

| Name | Type | Data |
|---|---|---|
| F | REG_BINARY | 02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0... |
| V | REG_BINARY | 00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 12 00 ... |
| ForcePasswo... | REG_BINARY | 00 00 00 00 |
| InternetUser... | REG_BINARY | 62 00 73 00 74 00 69 00 6E 00 73 00 6F 00 6E 00 31 00 3... |
| InternetProvi... | REG_BINARY | 8F 88 F9 D7 FC E3 B0 49 9E A6 A8 5B 5F 39 2A 4F |
| InternetUID | REG_BINARY | 30 00 32 00 38 00 31 00 35 00 32 00 30 00 35 00 61 00 6... |
| InternetSID | REG_BINARY | 01 0B 00 00 00 00 00 0B 60 00 00 00 8F 88 F9 D7 FC E3 ... |
| ComplexityL... | REG_BINARY | 00 00 00 00 00 00 00 00 08 00 02 00 |
| ComplexityP... | REG_BINARY | 00 00 00 00 00 00 00 00 06 00 01 00 |
| CachedLogo... | REG_BINARY | 02 00 00 00 8E 09 00 00 48 00 00 00 01 00 00 00 00 00 0... |
| GivenName | REG_BINARY | 42 00 61 00 72 00 6E 00 65 00 79 00 |
| Surname | REG_BINARY | 53 00 74 00 69 00 6E 00 73 00 6F 00 6E 00 |

Figure 2 - Online Microsoft user account SAM results

The online user account resulted in more values, many pertaining to the accounts online interactions. These values are new to the SAM hive and user accounts with Windows 8. This would help an examiner know that the account was an online user account. It would be important to know this in order to subpoena the cloud files and activities from Microsoft.

| Key Properties | |
|---|---|
| Last Written Time | 5/29/2013 17:10:00 UTC |
| SID unique identifier | 1005 |
| User Name | bstin_000 |
| Full Name | Barney Stinson |
| Logon Count | 0 |
| Last Logon Time | Never |
| Last Password Change Time | 5/29/2013 17:10:00 UTC |
| Expiration Time | Never |
| Invalid Logon Count | 0 |
| Last Failed Login Time | Never |
| Account Disabled | false |
| Password Required | true |
| Country Code | 0 (System Default) |
| Has LAN Manager Password | false |
| Has NTLMv2 Password | true |

Figure 3 - Online Microsoft user account properties pane

From Figure 3 it can be seen that the number of recorded log-ins for the online account was 0. The actual total number of log-ins was not recorded within the registry. It may be stored online, however, according to the registry the account has never be logged into. This could prove difficult for an analyst to explain in court. However, showing that other files and programs had been opened using that account, the mistake in the registry should be easily clarified.

Two other user accounts were created, one an online Microsoft Account and the other a local account. The account types were reversed during the project in order to examine artifacts left from switching the accounts. The account that was switched from an online to local account left many values, seen in the other Microsoft account, blank. This would indicated that the account had been an online Microsoft account at one time.

| Name | Type | Data |
|---|---|---|
| F | REG_BINARY | 02 00 01 00 00 00 00 00 9A 38 42 49 76 60 CE 01 00 00 ... |
| V | REG_BINARY | 00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 10 00 ... |
| ForcePasswordReset | REG_BINARY | 00 00 00 00 |
| InternetUserName | REG_BINARY | (value not set) |
| InternetProviderGUID | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
| InternetUID | REG_BINARY | (value not set) |
| InternetSID | REG_BINARY | (value not set) |
| ComplexityLastUsed | REG_BINARY | 00 00 00 00 00 00 00 00 08 00 02 00 |
| ComplexityPolicy | REG_BINARY | 00 00 00 00 00 00 00 00 06 00 01 00 |
| CachedLogonInfo | REG_BINARY | (value not set) |
| GivenName | REG_BINARY | (value not set) |
| Surname | REG_BINARY | (value not set) |
| InternetProviderName | REG_BINARY | (value not set) |
| InternetProviderAttributes | REG_BINARY | (value not set) |

Figure 4 – Microsoft switched to local account

The other tested account was switched from a local account to an online Microsoft account. A value called "UserPasswordHint" remained from the local account stage. This would be a clue to the examiner that the account had once been local. Online Microsoft accounts do not contain the "UserPasswordHint" key.

Table 1– Other Registry Key Locations

| | NTUSER.DAT Results | |
|---|---|---|
| | Windows 7 Location | Windows 8 Location |
| File Extention/Associated Programs | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts |
| Typed URL's | NTUSER.DAT\Software\Microsoft\Internet Explorer\Typed URLs | NTUSER.DAT\Software\Microsoft\Internet Explorer\Typed URLs |
| Task Bar | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband |
| Media Player Recent | NTUSER.DAT\Software\Microsoft\MediaPlayer\Player\RecentFileList | Not Present |
| MRU-Last Visited | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32 | ComDlg32 Not Present |
| MRU-Open Saved | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU | ComDlg32 Not Present |
| MRU Recent Documents | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs |
| Typed Paths | NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths | Present but empty |

| | SYSTEM Results | |
|---|---|---|
| | Windows 7 Location | Windows 8 Location |
| Computer Name | SYSTEM\ContolSet###\Control\ComputerName\ComputerName | SYSTEM\ContolSet001\Control\ComputerName\ComputerName |
| Mounted Devices | SYSTEM\MountedDevices | SYSTEM\MountedDevices |
| Shutdown Time | SYSTEM\ControlSet###\Control\Windows | SYSTEM\ControlSet001\Control\Windows |
| Time Zone | SYSTEM\ControlSet###\Control\TimeZoneInformation\StandardName | SYSTEM\ControlSet001\Control\TimeZoneInformation\StandardName |

| SOFTWARE Results | | |
|---|---|---|
| | Windows 7 Location | Windows 8 Location |
| Last Logged on User | SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI | SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI |
| Install Date | SOFTWARE\Microsoft\WindowsNT\CurrentVersion | SOFTWARE\Microsoft\WindowsNT\CurrentVersion |
| List of installed applications to use for uninstall | SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall | SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall |
| List of executables for installed applications | SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SharedDLLs | SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SharedDLLs |
| List of 32-Bit applications | SOFTWARE\Wow6432Node\<appname> | SOFTWARE\Wow6432Node\<appname> |
| Installed application list | SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\<app name> | SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\<app name> |
| Registered Owner | SOFTWARE\Microsoft\Windows NT\CurrentVersion | SOFTWARE\Microsoft\Windows NT\CurrentVersion |

## Conclusions

The Windows 8 registry has not significantly changed from the Windows 7 operating system. More changes were expected with the overhaul of the operating system. However, it seems that Microsoft continued to use the same software operations with an upgrade to the look and feel. Still, with the availability of online accounts, it could become more difficult for an analyst to develop a timeline for the suspect's actions. Since most of the registry remains the same which means only a small amount of additional training is required for examiners. With many systems moving to Windows 8, the digital forensic analyst will be seeing more and more computers, tablets, and phones running Windows 8. It will be important for the analyst to know how to use the basic registry and applying these new findings to the Windows 8 registry.

## References


AccessData. FTK Registry Viewer. AccessData, Lindon, UT. 2008

AccessData. Registry Quick Find Chart. AccessData, Lindon, UT. 2010.

AccessData. *Windows Forensics – Registry FTK 2*. AccessData, Lindon, UT. 2008

Carvey, H. *Windows Registry Forensics: Advanced Digital Forensics Analysis of the Windows Registry*. Elsevier, Burlington, MA. 2011.

Diskology. *DJ. Forensics*. 2013. http://www.diskology.com/djforensic.html

Steel. C. *Windows Forensics: The Field Guide for Conducting Corporate Computer Investigations.* Wiley Publishing, Indianapolis. 2006.


## Acknowledgments


I thank: Christopher Vance, Cpl. Robert J. Boggs, Dr. Terry Fenger, West Virginia State Police Digital Forensics Unit, and the Marshall University Forensic Science Center