

A Comparison Between the Windows 8 & Windows 7 Registries

Matthew Brewer B.S., Dr. Terry Fenger, Corporal Robert J. Boggs, Christopher Vance B.S.

Marshall University Forensic Science Center, Huntington, West Virginia

West Virginia State Police, Crimes Against Children Unit, Huntington Detachment

Abstract

The introduction of Windows 8 was a big change for Microsoft's traditional operating system. Microsoft hoped to stream line all their devices to the same set-up and operations. 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. A controlled environment was created by following a specific plan to generate records in the registry.

Based on the examination of the Windows 8 registry, there were not any changes in registry locations from Windows 7, based on the examined areas. Some of the examined areas did not contain any recorded information but the subkeys were in the same location. 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 made many values in the SAM file change. Online user accounts 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. The other root keys did not contain any significant changes. Forensic examination of the Windows 8 registry will not take any additional education for the examiner. Close examination of the suspects user account will be necessary. If the user has an online

account, additional steps may need to be taken to prove the user was actually using the system at the time of the crime. However, compared to the major overhaul of the operating system, the registry did not significantly change.

Introduction

The Windows registry is a hierarchical data base central to the operations of the Windows computer 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 registry was initially added to the Windows operating system with the release of Windows 98. The registry has been developed and modified to meet the needs of the system and is still used in the newest versions of Windows 8.

Windows 8 represents a huge overhaul for Microsoft in the look and feel of their operating system. With the popularity of touch screens, tablets, and the release of Microsoft's line of cells phones, there was a push to have compatibility and make one operating system universal to all these devices. With this revolution of the operation system, it should be expected that there would be just as many changes to the registry.

The most modern version of the registry comes from Windows 7, however the basic structure and idea of the registry has not changed since its invention. The top and outermost part of the registry are hives which serve as the starting point for the tree structure. There are 6 hives in Windows 7: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG, and

HKEY_DYN_DATA. However, these files just serve as a way to organize the registry when the system is in operation. The registry is generated each time the system is booted. These hives serve as a way to arrange the registry the same way each time. This creation process is performed by the Configuration Manager. The true registry only exists when the system is on, when shut down occurs the registry disassembles and all the information is stored in the registry files.

The actual data stored in the registry is represented in files below the hives called root keys. The Configuration Manager uses symbolic links to generate the registry by linking hives to each other and to the root keys. The root keys serve as the on-disk storage that saves the data used by programs in the form of logical files. There are five main root keys within the registry: SAM, SYSTEM, SOFTWARE, SECURITY, and NTUSER.DAT. Several other root keys exist but do not contain any valuable forensic information or are not stored on the disk. Below these root keys are many subkeys that are organized like a file system. Certain subkeys may also contain subkeys within themselves. The information that is stored in subkeys are called values. The values are known offsets within the hexadecimal data of the subkey.

The SAM root key is located below the HKEY_LOCAL_MACHINE hive. This key contains all the information about the users of the computer, making it one of the most forensically relevant registry files. Each user that logs into the machine will be given a unique RID, or relative identifier. The admin account will always have the RID of 500. A guest account is native to all Windows operating systems with the RID 501. User created user accounts will begin with the RID 1001 and increase in increments of one as accounts are created. The RID will be written in hexadecimal when viewed in the SAM file. (Figure 1) Within each Windows 7 SAM user file are the user's F & V values, another way to uniquely identify the user, and the password hint for the user's log-on. The properties pane for the SAM file will display the last

written time for that account, the user's RID, the actual username of the account, the numbers of times logged on, and the last time the password was changed. (Figure 2) These values in the properties pane are generated from the F value using known offsets. The SAM file can also be used in conjunction with the SYSTEM root key to decrypt user passwords.

The SYSTEM root key contains data about the current and previous states of the operating system. It is also located below the HKEY_LOCAL_MACHINE hive. Significant forensic data listed in this area includes the mounted devices, previously used USBs, printer information, and the last shutdown time. This key can help the investigator collect all the potentially relevant storage devices the suspect might have used. It could also be useful in establishing a time line or corroborating a suspect's testimony.

Next, is the SOFTWARE key, it includes information about applications installed on the computer and how the operating system and files interact with them. The SOFTWARE key is the last key under the HKEY_LOCAL_MACHINE hive. The Windows 7 SOFTWARE key shows a list of installed applications, the last user that logged on to the system, a list of the programs that automatically run when the system starts up, and any wireless networks the system accessed. The next to last key is the SECURITY file which holds very little forensically relevant material.

The last registry root key is the NTUSER.DAT file which may be the most significant file because it contains the most information about the users. It is stored under the HKEY_CURRENT_USER hive. It is also vital because each user account on the computer has an individual NTUSER.DAT file. It contains the user's internet explorer settings, typed URLs, most recently opened files and applications, most recently saved files, the search terms the user entered on the start menu, and the most recently opened or edited word document. It becomes

important to use the NTUSER.DAT to verify the information found in the SAM folder. Also, the NTUSER.DAT helps to generate a timeline and prove that a specific user was using the computer at the time of the crime, opened a file, or visited a specific website.

Materials and Methods

The registry artifact locations in Windows 7 were previously located, verified, and are available in a Quick Find Chart from AccessData. Therefore, the research process will be to look at the location listed in the chart, then, a compare it to the location and the type of information in that location in Windows 8. A plan was developed before beginning to use the Windows 8 machine in order to maintain a controlled environment.

An 80GB SATA hard drive was wiped clean with a Disk Jockey Pro by Diskology. The instrument wipes the disk in two phases. The first, a simple one pass erase and the second the NSA standard three pass wipe. This ensured that the disc was free of any coherent data before the operating system was installed. The 64-bit version of Windows 8 was then installed on the hard drive. Once the operating system formatted the drive for NTFS, the express set-up settings were selected. After the operating system was fully loaded, the first local user account was created so that the machine would be operational.

The operating system was updated through the Windows 8 Action Center. This step was taken to make sure the most current version was being used when examining the registry, since possible changes to the registry could have taken place since older versions. The native apps and programs on the Windows 8 Start screen were updated through the Windows Store app.

Windows 8 offers two types of user accounts on the system: a local user account and a Microsoft account that requires a connection to the internet and provides extra amenities such as

the Skydrive. Once the account is created, it can be switched to the other type of account at any time. Four separate accounts were created to test all the types of possible scenarios. The local user account Matthew Misde was created first and used as the main research account. The Matthew Misde account was used to browse the internet to a specific list of websites available in Appendix A. All of the major search engines were accessed and used: Google, Yahoo, and Bing. The word green was searched on all three engines and then two individual words were searched on each separate engine. The searched terms are also located in Appendix A.

Another local user account was created, John Smith, and then later converted to an online Microsoft account. The third account, Charlie Brown, was originally created as a Microsoft account and then switched to a local user account. Barney Stinson, the last account, was created and remained as a Microsoft account throughout the experiment. All accounts were logged into and out of multiple times.

On a separate machine, 12 JPEG images, 3 GIF images, and 3 PNG images were transferred to a 128MB Dell NTFS USB flash drive. Two videos, one MP4 and one WMV, were transferred to a 2GB Rally FAT32 USB flash drive. Then, both flash drives were plugged into the Windows 8 machine, while Matthew Misde was logged in, and transferred to the My Pictures and My Videos folders, respectively.

On June 3rd, 2013, Charlie Brown was switched to local user account and John Smith was switched to a Microsoft account. Both accounts were logged into and out of one more time. Then, the test hard drive was removed from the machine. The hard drive was imaged using FTK Imager provided by AccessData. Imaging is the process of making an exact forensic duplicate of the hard drive. By working off of and analyzing an exact copy, it prevents the original hard drive

from being changed. The information is copied from the test hard drive through the use of a write blocker which prevents the machine from writing to the test hard drive. At the end of the copying process, the copy and the original are confirmed to be exact replicas through the use of hash values. A hash value is like a fingerprint for digital items. An algorithm is used to generate a unique string of numbers and letters, 0-9 and A-F, which are unique to each piece of data. A one bit change to an item of data will change the hash value. Therefore, if two hard drives have the same hash value, it can be confirmed they are exact duplicates.

The registry files were extracted from the hard drive image. The location of the registry files are listed in [Appendix C](#). Once extracted, the registry files were viewed and analyzed using Registry Viewer, also provided by AccessData.

Results

As mentioned above, the SAM registry file contains the information about all the user accounts on the computer. The registry location comparisons for the SAM file can be seen in [Appendix B](#). The accounts on the Windows 8 system and their RIDs were: 500 was the Administrator account, 501 the Guest Account, 1001 was Matthew Misede, 1002 UpdatusUser, 1003 John Smith, 1004 C. Brown, and 1005 was the RID for bstin_000 (Barney Stinson). The properties information listed for each user account is the last written time, the RID, the user name, logon count, last logon time, last password change time, account expiration time, invalid logon count, last failed login time, account disabled, and password required.

The information panel for the Matthew Misede account can be seen in Figure 3, showing the values with known offsets within the user account registry file. All the values listed above can also be seen in the properties pane in the lower left hand corner of Figure 3. The Matthew

Misde SAM subkey has 4 values listed: F value, V value, force password reset, and the password hint. The Microsoft account Barney Stinson has 12 values listed, seen in Figure 4. Also, in Figure 5 it can be seen that this account has been logged on 0 times, when, in fact, multiple log-ons took place during the method execution. The John Smith account has 13 values listed in the user information, the additional value from the Stinson account was the user password hint, and this can be seen in Figure 6. The C. Brown account has 14 values listed which can be seen in Figure 7.

The SYSTEM key contains information about the current and previous states of the system. The information found in the SYSTEM key included the two USB devices plugged into the machine to transfer the media files. It was found under the mounted devices value. The Rally and Dell USB devices can be seen in Figure 8 and Figure 9. Other values in this location include the other mounted hard drives and available empty media drives. (Figure 10) Also within the SYSTEM key is the time zone information of the system. It is important for the analyst to understand when files were written to based off the dates and times which will be adjusted to the machines time zone settings. (Figure 11) There were not any printers used during this testing, but the printer information would also be found in the SYSTEM key.

The information about the operating system, such as the owner of the machine, can be found in the SOFTWARE key. Under the CurrentVersion value, Figure 12, the registered system owner, the install date, and the current version and type of windows operating system can all be extracted. Under the LogonUI value, the last user logged into the machine when it was shutdown can be found. That users SID and RID are available under this value as well. (Figure 13)

The user's personal settings and actions are stored in the NTUSER.DAT key. The program used to execute each file extension is listed in the NTUSER.DAT file. Examples of the results can be seen in Figure 14 and Figure 15. Figure 14 represents the program used to execute .jpeg files and Figure 15 .gif files. Figure 16 displays the last time the system was shut down in the properties pane. Within the Internet Explorer subkey, a list of typed URLs is available. (Figure 17) The file locations of the main Windows operating system files, eg. My Pictures, can be viewed in the Shell Folders subkey. (Figure 18) The last found result, Figure 19, indicates which programs are pinned to the task bar.

Discussion

Each of the four user accounts on the system was set up to produce different results. Matthew Misede the local account produced only 3 values in the account subkey, while all the other accounts that were a Microsoft account at some point produced 12 to 14 values. This makes it is easy to determine when an account is strictly local to the machine. The Misede account produced the same values that would have been seen in a user account subkey within Windows 7. The Barney Stinson account was the only user to remain a Microsoft account throughout the experiment and the log-on count was listed at 0. However, the Misede account had the correct number of log-ins, so it can be assumed that Microsoft account log-ons are not recorded in the registry. When the John Smith account was switched to a Microsoft account the recorded log-ons should have ended. Also, the last recorded log-on in the properties pane would be a time close to when the account was changed. The last account, Charlie Brown, was converted to a local account from a Microsoft account. The first recorded log-on will be after the account was switched to a local status. The number of log-ons before being a local account will be unknown. The last password change time could show the time at which the account as switched, if the user

had not changed their password since then. Also, in the values of the Charlie Brown subkey, Figure 7, it can be seen that most of the values do not contain information. This confirms that the account was switched to a local account. These values would have contained data when the account was a Microsoft account.

All the information that was tested for in the SYSTEM key was discovered. Both USB drives, the Dell and Rally, were recorded in the mounted drives subkey. The information that was transferred from the drives was not recorded. The other drives and drive slots that had been used or were empty were also recorded in this subkey.

The SOFTWARE key contains information on the state of the operating system on the machine. Figure 12 shows the main user account or owner of the machine. This would allow an investigator to know which account was used to set up the machine and most likely the main account that was used. The version of the operating system currently installed can also be found. Another subkey, the LogonUI shows which user was last logged on to the machine before it was shut down or since someone else has logged on. This would be extremely important for an investigation if all the accounts or user of interest were online Microsoft accounts. This subkey could show that an account has at least been logged on once and was the last person to use the machine. Even though user created data on the account would prove that it had in fact been used, a smart defense attorney could point out the 0 number of log-ons from the SAM file. If the user of interest was the last person logged-on, this subkey would overrule the SAM hive.

The last key to be discussed is the NTUSER.DAT, which lists the user's preferences. One of the important parts of a media investigation is knowing which programs were used to open and view pictures and videos. If a suspect is not using default program, such as VLC, to play

videos it could mean the suspect has a higher level of computer competency. Smarter criminals are better at hiding evidence and it is important for the examiner to take that advanced knowledge into account when processing a case. Also, knowing the executable program allows the examiner to look at the most recently opened files by that program. This could prove the suspect has watched or opened the files of interest. Figure 12 and 13 display the FileExt subkey which shows all the possible file extensions and which programs are used to open them. Figure 12 is the program identifier for .JPEG files and Figure 13 .GIF files. However, the identifier of the program is not linked to any specific program name, at least within the registry itself. The default pictures app on Windows 8 was used to open both these file extensions. The program identifier in Figure 12 and Figure 13 is the same which leads to an assumption that the identifier points to the native Pictures application on Windows 8; but there is not any direct evidence of this within the registry.

Figure 15 shows the most recently typed URLs. The registry records the URLs physically typed into the URL bar in Internet Explorer. Windows 7 typically stores up to 25 of the most recently typed URLs. 17 URLs were typed into Internet Explorer during the course of the experiment. Figure 15 lists 16 URLs but the bottom two listed were not URL's typed during the experimentation phase. MUVPN was typed to access the internet on the system initially and the last listed as go.microsoft.com is always listed even though it was not typed by the user. Therefore, only 14 of 17 of the URL's used in the experiment were present in the registry. The possible number of recorded URL's could have decreased for Windows 8, further experimentation would be required.

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 a big vanity 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. Most of the registry remains the same, meaning little advanced training 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.

Figures

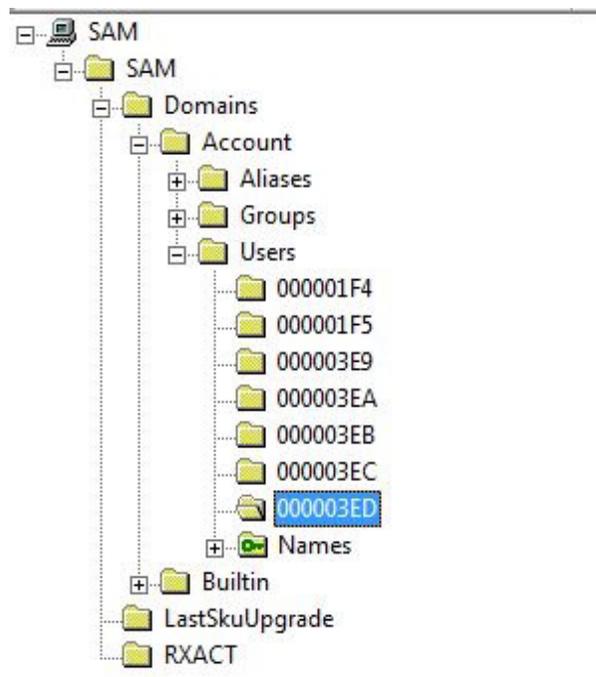


Figure 1 - User RID's in SAM File

Key Properties	
Last Written Time	6/3/2013 16:18:14 UTC
SID unique identifier	1001
User Name	Matthew Misde
Logon Count	21
Last Logon Time	6/3/2013 16:18:14 UTC
Last Password Change Time	5/21/2013 19:04:48 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	5/23/2013 13:27:00 UTC
Account Disabled	false
Password Required	false
Country Code	0 (System Default)
Has LAN Manager Password	false
Has NTLMv2 Password	true

Figure 2 - SAM User Properties

Name	Type	Data
F	REG_BINARY	02 00 01 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...

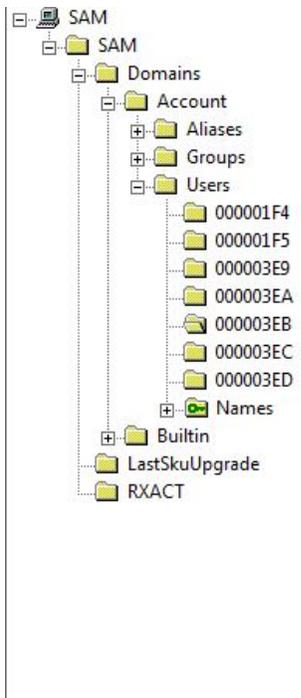
Key Properties	
Last Written Time	6/3/2013 16:18:14 UTC
SID unique identifier	1001
User Name	Matthew Misde
Logon Count	21
Last Logon Time	6/3/2013 16:18:14 UTC
Last Password Change Time	5/21/2013 19:04:48 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	5/23/2013 13:27:00 UTC
Account Disabled	false
Password Required	false
Country Code	0 (System Default)
Has LAN Manager Password	false
Has NTLMv2 Password	true

00 53 00 61 00 6d 00 65 00-20 00 62 00 75 00 74 00	S-a-m-e- -b-u-t-
10 20 00 6d 00 6f 00 72 00-65 00	-m-o-r-e-

Figure 3 - Matthew Misde SAM File

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 5 - B. Stinson Properties Pane



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 98 CE 0A 50 60 60 CE 01 00 00 ...
V	REG_BINARY	00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 14 00 ...
ForcePasswo...	REG_BINARY	00 00 00 00
UserPasswor...	REG_BINARY	68 00 6F 00 6D 00 65 00 6C 00 61 00 6E 00 64 00
InternetUser...	REG_BINARY	4A 00 6F 00 68 00 6E 00 53 00 6D 00 69 00 74 00 68 00 ...
InternetProvi...	REG_BINARY	8F 88 F9 D7 FC E3 B0 49 9E A6 A8 5B 5F 39 2A 4F
GivenName	REG_BINARY	4A 00 6F 00 68 00 6E 00
Surname	REG_BINARY	53 00 6D 00 69 00 74 00 68 00
InternetUID	REG_BINARY	34 00 32 00 33 00 32 00 35 00 35 00 35 00 36 00 38 00 3...
InternetSID	REG_BINARY	01 0B 00 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 03 00
ComplexityP...	REG_BINARY	00 00 00 00 00 00 00 00 06 00 01 00
CachedLogo...	REG_BINARY	02 00 00 00 BE 09 00 00 48 00 00 00 01 00 00 00 00 00 0...

Key Properties	
Last Written Time	6/3/2013 13:43:22 UTC
SID unique identifier	1003
User Name	John Smith
Full Name	John Smith
Logon Count	9
Last Logon Time	6/3/2013 13:43:21 UTC
Last Password Change Ti	6/3/2013 13:43:22 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	6/3/2013 13:40:04 UTC
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Has LAN Manager Passw	false
Has NTLMv2 Password	true

00	02 00 01 00 00 00 00 00 00-98	ce 0a 50 60 60 ce 01î·P`î·
10	00 00 00 00 00 00 00 00 00-58	59 8b 50 60 60 ce 01XY·P`î·
20	ff ff ff ff ff ff ff 7f-c1	5d 46 da 5f 60 ce 01	ÿÿÿÿÿÿÿ·Á]FÚ_î·
30	eb 03 00 00 01 02 00 00-10	02 00 00 00 00 00 00	è.....
40	00 00 09 00 00 00 00 00-00	00 00 00 00 00 00 00

Figure 6 - John Smith SAM File

Name	Type	Data
F	REG_BINARY	02 00 01 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)

Key Properties	Value
Last Written Time	6/3/2013 16:20:39 UTC
SID unique identifier	1004
User Name	C. Brown
Logon Count	3
Last Logon Time	6/3/2013 16:20:39 UTC
Last Password Change Time	6/3/2013 13:39:15 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

00	02 00 01 00 00 00 00 00 00-9a 38 42 49 76 60 ce 018Biv`i-
10	00 00 00 00 00 00 00 00 00-3a e3 32 bd 5f 60 ce 01:82%`i-
20	ff ff ff ff ff ff ff 7f-00 00 00 00 00 00 00 00 00	yyyyyy.....
30	ec 03 00 00 01 02 00 00-10 02 00 00 00 00 00 00 00	i.....
40	00 00 03 00 00 00 00 00 00-00 00 00 00 00 00 00 00

Figure 7 - C. Brown SAM File

00	5f 00 3f 00 3f 00 5f 00-55 00 53 00 42 00 53 00	_ . ? . ? . _ . U . S . B . S .
10	54 00 4f 00 52 00 23 00-44 00 69 00 73 00 6b 00	T . O . R . # . D . i . s . k .
20	26 00 56 00 65 00 6e 00-5f 00 4f 00 43 00 5a 00	& . V . e . n . _ . O . C . Z .
30	26 00 50 00 72 00 6f 00-64 00 5f 00 52 00 41 00	& . P . r . o . d . _ . R . A .
40	4c 00 4c 00 59 00 32 00-26 00 52 00 65 00 76 00	L . L . Y . 2 . & . R . e . v .
50	5f 00 31 00 31 00 30 00-30 00 23 00 41 00 41 00	_ . 1 . 1 . 0 . 0 . # . A . A .
60	30 00 34 00 30 00 31 00-32 00 37 00 30 00 30 00	0 . 4 . 0 . 1 . 2 . 7 . 0 . 0 .
70	34 00 30 00 37 00 33 00-35 00 34 00 26 00 30 00	4 . 0 . 7 . 3 . 5 . 4 . & . 0 .
80	23 00 7b 00 35 00 33 00-66 00 35 00 36 00 33 00	# . { . 5 . 3 . f . 5 . 6 . 3 .
90	30 00 37 00 2d 00 62 00-36 00 62 00 66 00 2d 00	0 . 7 . - . b . 6 . b . f . - .
a0	31 00 31 00 64 00 30 00-2d 00 39 00 34 00 66 00	1 . 1 . d . 0 . - . 9 . 4 . f .
b0	32 00 2d 00 30 00 30 00-61 00 30 00 63 00 39 00	2 . - . 0 . 0 . a . 0 . c . 9 .
c0	31 00 65 00 66 00 62 00-38 00 62 00 7d 00	1 . e . f . b . 8 . b . } .

Figure 8 - Rally USB

00	5f 00 3f 00 3f 00 5f 00-55 00 53 00 42 00 53 00	_·?·?·_·U·S·B·S·
10	54 00 4f 00 52 00 23 00-44 00 69 00 73 00 6b 00	T·O·R·#·D·i·s·k·
20	26 00 56 00 65 00 6e 00-5f 00 4d 00 2d 00 53 00	&·V·e·n·_·M·-·S·
30	79 00 73 00 54 00 35 00-26 00 50 00 72 00 6f 00	y·s·T·5·&·P·r·o·
40	64 00 5f 00 44 00 65 00-6c 00 6c 00 5f 00 4d 00	d·_·D·e·l·l·_·M·
50	65 00 6d 00 6f 00 72 00-79 00 5f 00 4b 00 65 00	e·m·o·r·y·_·K·e·
60	79 00 26 00 52 00 65 00-76 00 5f 00 35 00 2e 00	y·&·R·e·v·_·5·_·
70	30 00 30 00 23 00 30 00-37 00 41 00 31 00 41 00	0·0·#·0·7·A·1·A·
80	41 00 34 00 31 00 32 00-30 00 45 00 31 00 37 00	A·4·1·2·0·E·1·7·
90	42 00 35 00 33 00 26 00-30 00 23 00 7b 00 35 00	B·5·3·&·0·#·{·5·
a0	33 00 66 00 35 00 36 00-33 00 30 00 37 00 2d 00	3·f·5·6·3·0·7·-·
b0	62 00 36 00 62 00 66 00-2d 00 31 00 31 00 64 00	b·6·b·f·-·1·1·d·
c0	30 00 2d 00 39 00 34 00-66 00 32 00 2d 00 30 00	0·-·9·4·f·2·-·0·
d0	30 00 61 00 30 00 63 00-39 00 31 00 65 00 66 00	0·a·0·c·9·1·e·f·
e0	62 00 38 00 62 00 7d 00-	b·8·b·}·

Figure 9 - Dell USB

	Name	Type	Data
SYSTEM	\DosDevices\C:	REG_BINARY	34 45 C1 1C 00 00 10 00 00 00 00 00
ControlSet001	\\?\Volume{63394979-c25c-11e2-be66-806e6f6e6963}	REG_BINARY	34 45 C1 1C 00 00 10 00 00 00 00 00
DriverDatabase	\\?\Volume{63394986-c25c-11e2-be66-806e6f6e6963}	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 43 00 53 00 49 00 23 00 ...
HardwareConfig	\\?\Volume{6339498b-c25c-11e2-be66-806e6f6e6963}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
MountedDevices	\\?\Volume{6339498c-c25c-11e2-be66-806e6f6e6963}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
RNG	\\?\Volume{6339498d-c25c-11e2-be66-806e6f6e6963}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
Select	\\?\Volume{6339498e-c25c-11e2-be66-806e6f6e6963}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
Setup	\\DosDevices\D:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
WPA	\\DosDevices\E:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
	\\DosDevices\F:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
	\\DosDevices\G:	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
	\\DosDevices\H:	REG_BINARY	5C 00 3F 00 3F 00 5C 00 53 00 43 00 53 00 49 00 23 00 ...
	\\?\Volume{e13b849e-c870-11e2-be6d-485b3924311f}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...
	\\?\Volume{e13b84c1-c870-11e2-be6d-485b3924311f}	REG_BINARY	5F 00 3F 00 3F 00 5F 00 55 00 53 00 42 00 53 00 54 00 4...

Figure 10 - Mounted Drives

The screenshot shows the Windows Registry Editor with the left pane expanded to 'TimeZoneInformation'. The right pane displays a list of registry values:

Name	Type	Data
DaylightBias	REG_DWORD	0xFFFFFC4 (4294967236)
DaylightName	REG_SZ	@tzres.dll,-111
StandardStart	REG_BINARY	00 00 08 00 01 00 02 00 00 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-112
Bias	REG_DWORD	0x0000012C (300)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Eastern Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x000000F0 (240)

Figure 11 - Time Zone Settings

The screenshot shows the Windows Registry Editor with the left pane expanded to 'Windows NT > CurrentVersion'. The right pane displays a list of registry values:

Name	Type	Data
SystemRoot	REG_SZ	C:\Windows
SoftwareType	REG_SZ	System
RegisteredOwner	REG_SZ	Matthew Misde
InstallDate	REG_DWORD	0x519BC552 (1369163090)
CurrentVersion	REG_SZ	6.2
CurrentBuild	REG_SZ	9200
RegisteredOrganization	REG_SZ	(value not set)
CurrentType	REG_SZ	Multiprocessor Free
InstallationType	REG_SZ	Client
EditionID	REG_SZ	Enterprise
ProductName	REG_SZ	Windows 8 Enterprise
Productid	REG_SZ	00178-90000-00011-AA119
DigitalProductId	REG_BINARY	A4 00 00 00 03 00 00 00 30 30 31 37 38 2D 39 30 30 ...
DigitalProductId4	REG_BINARY	F8 04 00 00 04 00 00 00 30 00 30 00 30 00 30 00 2...
CurrentBuildNumber	REG_SZ	9200
BuildLab	REG_SZ	9200.win8_gdr.130410-1505
BuildLabEx	REG_SZ	9200.16581.amd64fre.win8_gdr.130410-1505
BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffff
PathName	REG_SZ	C:\Windows

Figure 12 - Current Version

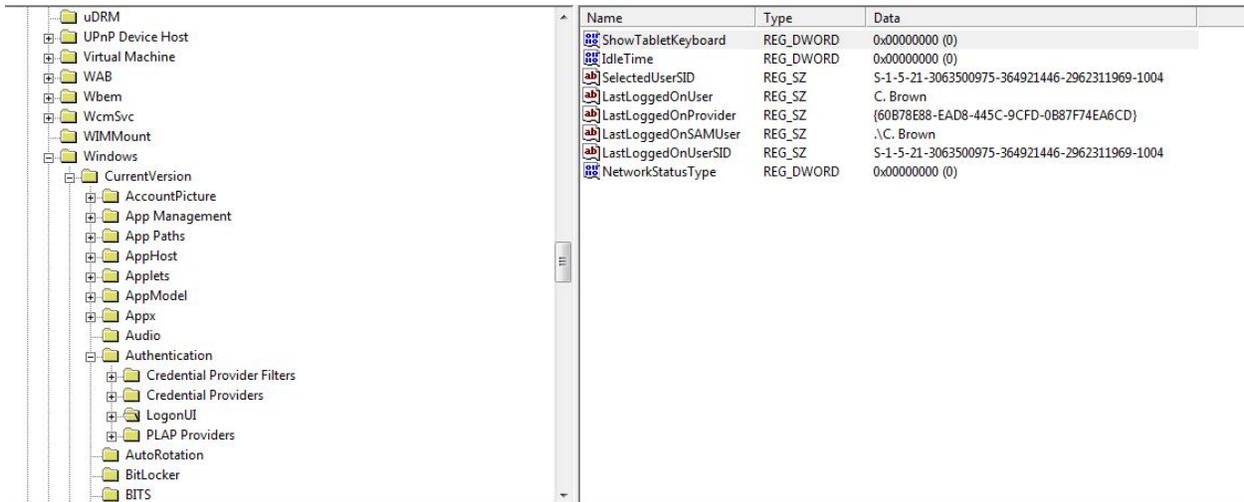


Figure 13 - Last Log On

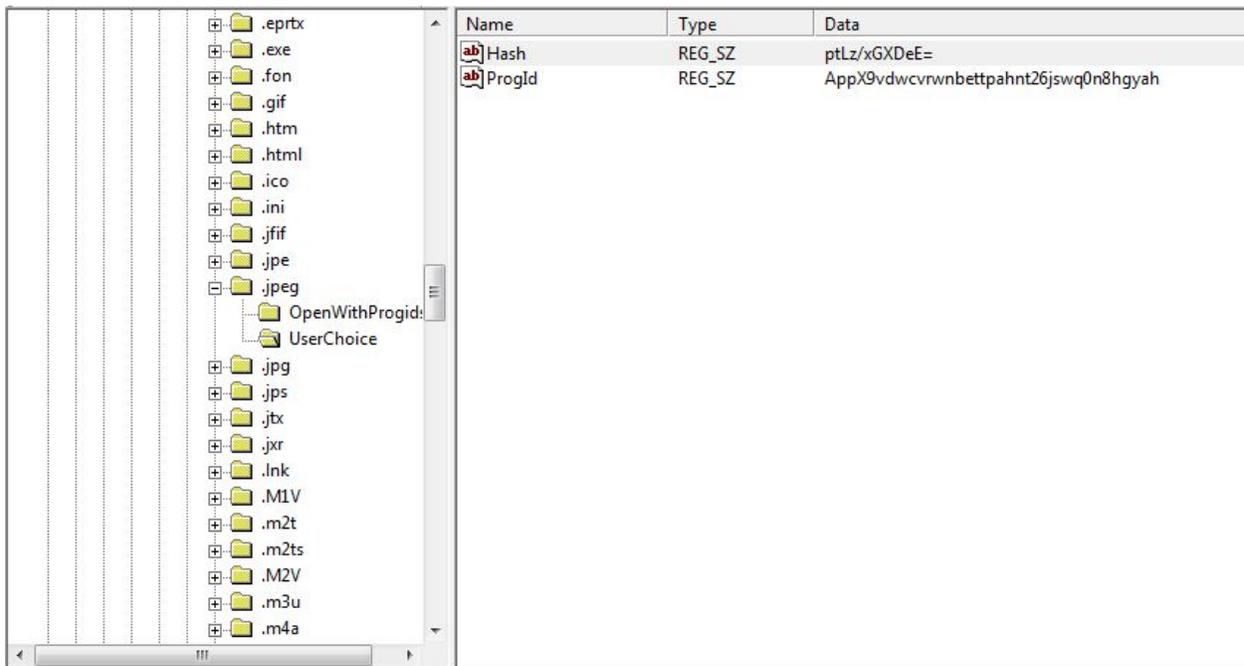


Figure 14 - JPEG Execution

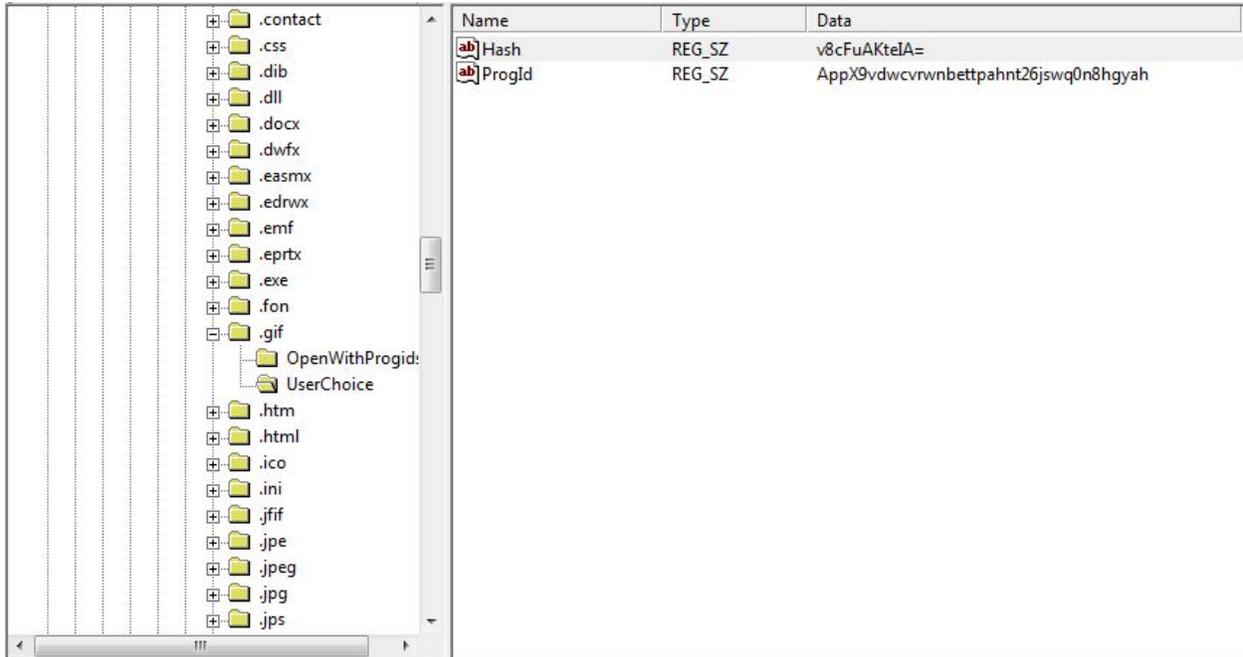


Figure 15 - GIF Execution

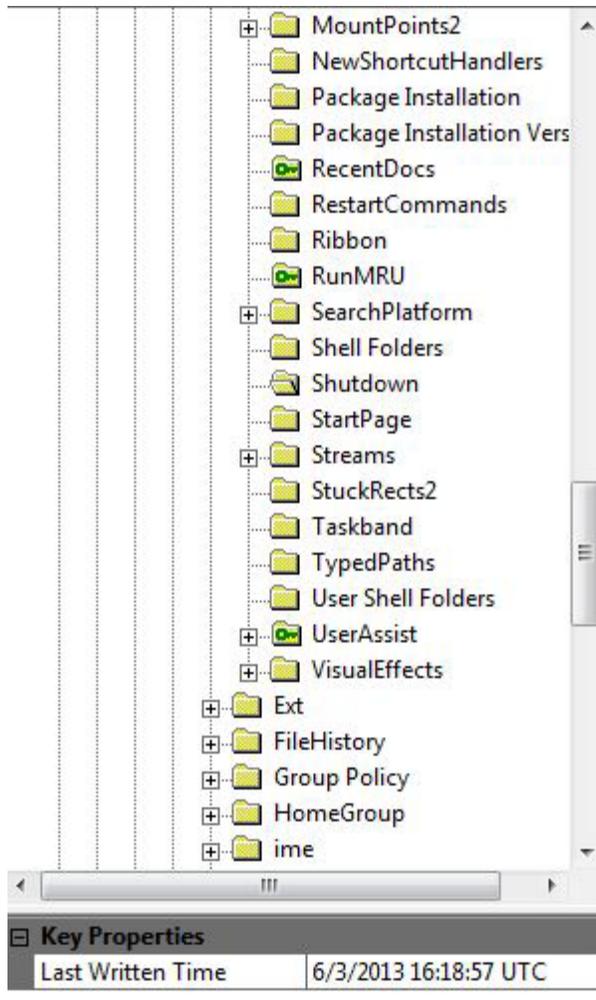


Figure 16 - Last Shut Down

Name	Type	Data
url1	REG_SZ	http://gmail.com/
url2	REG_SZ	http://msnbc.com/
url3	REG_SZ	http://cnn.com/
url4	REG_SZ	http://bing.com/
url5	REG_SZ	http://yahoo.com/
url6	REG_SZ	http://google.com/
url7	REG_SZ	http://ecu.edu/
url8	REG_SZ	http://www.marshall.edu/
url9	REG_SZ	http://accessdata.com/
url10	REG_SZ	http://armorgames.com/
url11	REG_SZ	http://foxnews.com/
url12	REG_SZ	http://wsj.com/
url13	REG_SZ	http://kongregate.com/
url14	REG_SZ	http://bbc.com/
url15	REG_SZ	http://muvpn.marshall.edu/
url16	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

Figure 17 - Matthew Misd Typed URL's

Name	Type	Data
!Do not use this registry key	REG_SZ	Use the SHGetFolderPath or SHGetKnownFolderPath ...
AppData	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming
Local AppData	REG_SZ	C:\Users\Matthew Misd\AppData\Local
My Video	REG_SZ	C:\Users\Matthew Misd\Videos
{1B3EA5DC-B587-4786-B4EF-BD1DC...	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
My Pictures	REG_SZ	C:\Users\Matthew Misd\Pictures
Desktop	REG_SZ	C:\Users\Matthew Misd\Desktop
History	REG_SZ	C:\Users\Matthew Misd\AppData\Local\Microsoft\...
NetHood	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
{56784854-C6CB-462B-8169-88E35A...	REG_SZ	C:\Users\Matthew Misd\Contacts
{00BCFCSA-ED94-4E48-96A1-3F6217...	REG_SZ	C:\Users\Matthew Misd\AppData\Local\Microsoft\...
Cookies	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
Favorites	REG_SZ	C:\Users\Matthew Misd\Favorites
SendTo	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
Start Menu	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
My Music	REG_SZ	C:\Users\Matthew Misd\Music
Programs	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
Recent	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
CD Burning	REG_SZ	C:\Users\Matthew Misd\AppData\Local\Microsoft\...
PrintHood	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
{7D1D3A04-DEBB-4115-95CF-2F29D...	REG_SZ	C:\Users\Matthew Misd\Searches
{374DE290-123F-4565-9164-39C4925...	REG_SZ	C:\Users\Matthew Misd\Downloads
{A520A1A4-1780-4FF6-BD18-167343...	REG_SZ	C:\Users\Matthew Misd\AppData\LocalLow
Startup	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
Administrative Tools	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
Personal	REG_SZ	C:\Users\Matthew Misd\Documents
{BF89D5E0-C6A9-404C-B2B2-AE6DB...	REG_SZ	C:\Users\Matthew Misd\Links
Cache	REG_SZ	C:\Users\Matthew Misd\AppData\Local\Microsoft\...
Templates	REG_SZ	C:\Users\Matthew Misd\AppData\Roaming\Micros...
{4C5C32FF-B89D-43B0-B5B4-2D72E5...	REG_SZ	C:\Users\Matthew Misd\Saved Games
Fonts	REG_SZ	C:\Windows\Fonts

Figure 18 - Shell Folders

```

0 .....$.....
3 ...Á.....C:\Us
4 ers\Matthew Misd
5 e\AppData\Roamin
5 g\Microsoft\Inte
5 rnet Explorer\Qu
0 ick Launch\User
9 Pinned\TaskBar\I
2 nternet Explorer
0 .lnk...`.....X.
0 .....misd.....
0 .....ÁB,`c-E-Û
7 ÚYJ ..c°Ñ\ÁÁ·%g
0 H[9$1·ÁB,`c-E-Û
7 ÚYJ ..c°Ñ\ÁÁ·%g
0 H[9$1.....L.
0 .....Á.....
6 ·F.....·y´·5VV
a Í·y´·5VVÍ·6B·¥×j
0 Í.....
0 .....>.....
3 È'4··\·B²··ãR·Öh
1 R·1.....µB¹··Ta
2 skBar·<.....iµB
0 ¹·µB¹·*··¼4.....
0 .....
0 T·a·s·k·B·a·r...
0 ··Ö·2.....û@·×·
0 FILEEX~1.LNK·x·
0 ···iµB¹·µB¹·*·
0 ··z4.....
0 ··N.....F·i·l·e·
0 ··E·x·p·l·o·r·e·
0 r··l·n·k···@·s·
0 h·e·l·l·3·2··d·
0 l·l·,··-·2·2·0·6·
0 7.....B.....iµB¹·
0 M·i·c·r·o·s·o·f·
0 t··W·i·n·d·o·w·
0 s··E·x·p·l·o·r·
0 e·r.....×.....
0 .....
0 ··f.....·8
0 Á.....C:\Users\
0 Matthew Misd\Ap
9 pData\Roaming\Mi
4 crosoft\Internet
0 Explorer\Quick
3 Launch\User Pinn
0 ed\TaskBar\File
0 Explorer.lnk...`·
9 .....X.....mi
2 sde.....ÁB
a ,`c-E-ÛÚYJ ..d°
2 Ñ\ÁÁ·%gH[9$1·ÁB
a ,`c-E-ÛÚYJ ..d°
0 Ñ\ÁÁ·%gH[9$1...

```

Figure 19 - Programs on Task Bar

Appendix A

Typed URLs

1. CNN.com
2. NBCnews.com
3. BBC.com
4. Kongregate.com
5. WSJ.com
6. Foxnews.com
7. Armorgames.com
8. Weather.com
9. USAtoday.com
10. Accessdata.com
11. Facebook.com
12. Marshall.edu
13. ECU.edu
14. Yahoo.com
15. Google.com
16. Bing.com

Searched Terms

1. Google
 - a. Green
 - b. Circle
 - c. Square
2. Yahoo
 - a. Green
 - b. France
 - c. Germany
3. Bing
 - a. Green
 - b. Chimpanzee
 - c. Baboon

Appendix B

	Windows 7 Location	Windows 8 Location
<u>SAM</u>		
Local Users	SAM\Domains\Account\Users\Names	SAM\Domains\Account\Users\Names
User Name and SID	SAM\Domains\Account\Users\V Key	SAM\Domains\Account\Users\V Key
Last Failed Login	SAM\Domains\Account\Users\F Key	SAM\Domains\Account\Users\F Key
Last Logon Time	SAM\Domains\Account\Users\F Key	SAM\Domains\Account\Users\F Key
Last Password Change	SAM\Domains\Account\Users\F Key	SAM\Domains\Account\Users\F Key
Logon Count	SAM\Domains\Account\Users\F Key	SAM\Domains\Account\Users\F Key
<u>NTUSER.DAT</u>		
File Extention/ Associate d 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

<i>SOFTWARE</i>		
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\WindowsNT\CurrentVersion	SOFTWARE\Microsoft\WindowsNT\CurrentVersion
<i>SYSTEM</i>		
Computer Name	SYSTEM\ControlSet###\Control\ComputerName\ComputerName	SYSTEM\ControlSet001\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

Appendix C

Registry Locations

1. SAM
 - a. C:\Windows\System32\config
2. SYSTEM
 - a. C:\Windows\System32\config
3. SECURITY
 - a. C:\Windows\System32\config
4. SOFTWARE
 - a. C:\Windows\System32\config
5. NTUSER.DAT
 - a. C:\Users\

References

1.