June 2018

Windows Registry Forensic Tool Test Assertions and Test Plan

Draft 2 of Version 1.0 for Public Comment

National Institute of Standards and Technology
U.S. Department of Commerce

31

Abstract

This document defines assertions and test cases for Windows registry forensic tools capable of parsing the registry hive file format as well as extracting interpretable objects from registry hive files, and to determine whether a specific tool meets the requirements producing measurable results. The assertions and test cases are derived from the requirement defined in the document entitled: *Windows Registry Forensic Tool Specification*, located on the CFTT web site, www.cftt.nist.gov. Test cases describe the combination of test parameters required to test each assertion. Test assertions are described as general statements of conditions that can be checked after a test is executed. Each assertion appears in one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

As this document evolves updated versions will be posted at www.cftt.nist.gov.

[*] NIST does not endorse nor recommend products or trade names identified in this paper. All products used in this paper are mentioned for use in research and testing by NIST.

47

Table of Contents

71

1. Introduction

There is a critical need in the law enforcement community to ensure the reliability of digital forensic tools. A capability is required to ensure that forensic software tools consistently produce accurate and objective results. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing forensic software tools. We adhere to a disciplined testing procedure, established test criteria, test sets, and test hardware requirements, that result in providing necessary feedback information to toolmakers so they can improve their tool's effectiveness; end users benefit in that they gain vital information making them more informed about choices for acquiring and using computer forensic tools, and lastly, we impart knowledge to interested parties by increasing their understanding of a specific tool's capability. Our approach for testing forensic tools is based on established well recognized international methodologies for conformance testing and quality testing. For more information on this project, please visit us at: www.cftt.nist.gov.

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS), and the National Institute of Standards and Technology Special Program Office (SPO) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, the National Institute of Justice (NIJ), and the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensic tools and subsequent testing of specific tools against those specifications.

The Windows registry is a system-defined database in which applications and system components store and retrieve configuration data. The Windows operating system provides registry APIs to retrieve, modify, or delete registry objects such as keys, values and data. Note that the Windows registry in this specification means Windows NT registry (i.e. not Windows 3.1 or Windows 95/98/ME).

From digital forensics point of view, the Windows registry is one of primary targets for Windows forensics as a treasure box including not only configurations of the operating system and user installed applications, but also meaningful data that can be useful for identifying users' behaviors and reconstructing their past events. Although Windows registry analysis techniques are already generally being used in Windows forensics, there is a lack of objective and scientific evaluation efforts on digital forensic tools (dedicated registry forensic tools as well as digital forensic suites having registry-related features), which can parse and interpret Windows registry internals and various traces stored within the registry.

2. Purpose

This document defines test assertions and test cases derived from requirements for Windows registry forensic tool capable of extracting interpretable objects from Windows NT registry hive files. The test cases describe the combination of test parameters required to test each assertion. The test assertions are described as general statements of conditions that can be checked after a test is executed. Each assertion generates one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

3. Scope

The scope of this document is limited to software tools capable of handling the Windows NT registry hive format v1.3 and v1.5 generally used in modern Windows operating systems.

The test assertions for Windows registry forensic tools are based on the following assumptions.

- The tools are used in a forensically sound environment.
- The individuals using these tools adhere to forensic principles and have control over the environment in which the tools are used.
- The type of input data for registry-related tools may be one of the follows: hive file(s), hive set(s), and disk image file(s) containing at least one Windows system partition. We should note that the current version of test assertions does not include partial registry objects that can exists in unallocated areas of file systems or volatile memory-related areas. In addition, the transaction log file is not considered in this version of tool testing.
- The files used as test input to Windows registry forensic tools were created in a process that develops a reference registry dataset with ground truth data. For more information on the test dataset, please visit us at: www.cfreds.nist.gov.

4. Definitions

This glossary provides context in the absence of definitions recognized by the digital forensics community.

Analysis – The examination of acquired data for its significance and probative value.

Artifact – An object created as a result of the use of a digital device or software that shows usage history by users and includes potential digital evidence. Thus, digital forensic activities usually handle a multitude of forensic artifacts stored within various digital data storages including volatile and non-volatile storage devices.

ASCII – American Standard Code for Information Interchange.

Examination – A technical review that makes the evidence visible and suitable for analysis; as well as tests performed on the evidence to determine the presence or absence of specific data.

Extraction – A process by which potential digital evidence is parsed, processed, or interpreted for the examination and analysis.

File system – A software mechanism that defines the way that files are named, stored, organized, and accessed on logical volumes of partitioned memory.

FILETIME – A time structure that contains a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 (UTC).

Hive file – An offline registry file that physically stores registry objects including keys, values and data. A primary hive file may exist along with multiple transaction log files.

Hive set – A hive set consists of primary hives and their transaction log files generally including (but not limited to) SAM, SYSTEM, SOFTWARE, SECURITY and pairs of [NTUSER, USRCLASS] for each Windows account. Multiple hive sets can be found from Restore Points (Windows XP and earlier) as well as Volume Shadow Copies (Windows Vista and later) stored within a Windows system partition if relevant features are turned on.

Registry – A hierarchical database that contains data that is critical for the operation of Windows and the applications and services running on Windows.

Registry Key – An object within the registry that contains values and additional subkeys like a directory (folder) in a hierarchical file system.

Registry Value – Registry name/value pair associated with a registry key analogous to a file in a hierarchical file system.

Unicode – A standard for the consistent encoding, representation, and handling of text expressed in most of writing systems in the world (e.g., UTF-8 and UTF-16).

Volume Shadow Copy – A technology included in modern Microsoft Windows that allows taking manual or automatic backup copies of volumes, even when they are in use.

5. Test Assertions

The primary goal of the test assertions, presented below in Section 5.1 and 5.2, is to determine a tool's ability to accurately process specific registry objects stored within a reference registry dataset. The 'ID' column identifies each assertion. For instance, WRT-CA-01 (i.e., Windows Registry Tool-Core Assertion-01) is a core assertion derived from a core requirement for Windows registry forensic tools. In addition, an assertion for optional features, WRT-AO-01 (i.e., Windows Registry Tool-Assertion Optional-01) is an optional assertion and only tested if a tool supports the feature. The 'Test Assertion' column states each assertion, and the 'Comments' column provides additional information pertaining to the assertion.

5.1. Core Assertions (CA)

ID	Test Assertion	Comments
WRT-CA-01	If a Windows registry forensic tool provides the user with an "Open Individual Hive File", then the tool shall complete the opening process without error if the file is normal.	- Select file(s); Begin the process - Some tools (especially, digital forensic suites having registry-related features) may support processing hive files only if the files are identified as the registry hive format among previously loaded files (i.e., disk images or a set of files).
WRT-CA-02	If a Windows registry forensic tool provides the user with an "Open Multiple Hive Files", then the tool shall complete the opening process without error if the files are normal.	
WRT-CA-03	If a Windows registry forensic tool processes files in abnormal states (i.e., corrupted or manipulated hive files), then the tool shall notify the user that the file has invalid fields or structures without application crash.	- Select file(s); Begin the process
WRT-CA-04	If a Windows registry forensic tool completes the opening of the target hive file without error, then the tool shall have the ability to present all registry objects in a useable format via a preview-pane view, generated report or output file.	- Review processed results; Review data for readability in a useable format
WRT-CA-05	If a Windows registry forensic tool completes the opening of the target hive file without error, then all registry objects (i.e., Key, Value and Data) as well as associated metadata (i.e., timestamp of a key, tree structures of keys, key/value list, size of data, etc.) shall be presented without modification in a useable format.	- Review processed results; Review interpretation of registry objects

ID	Test Assertion	Comments
WRT-CA-06	If a Windows registry forensic tool completes the opening of the target hive file without error, then all STRING data containing non-ASCII characters shall be presented in their native format.	- Review processed results; Review interpretation of data containing non-ASCII characters

183

184 ## 5.2. Assertions Optional (AO)

ID	Test Assertion	Comments
WRT-AO-01	If a Windows registry forensic tool provides the user with the ability to recover deleted registry objects inside the target hive file, then the tool shall have the ability to recover deleted (but complete) registry objects without error.	- Open a file; Begin deleted object recovery
WRT-AO-02	If a Windows registry forensic tool completes deleted registry object recovery without error, then the tool shall have the ability to present all recovered results in a useable format via a preview-pane view, generated report or output file.	- Review recovered results; Review data for readability in a useable format
WRT-AO-03	If a Windows registry forensic tool completes deleted registry object recovery without error, then all recovered registry objects (i.e., Key, Value and Data) as well as associated metadata (i.e., timestamp of a key, tree structures of keys, key/value list, size of data, etc.) shall be presented without modification in a useable format.	- Review recovered results; Review interpretation of registry objects
WRT-CA-04	If a Windows registry forensic tool completes deleted registry object recovery without error, then all recovered STRING data containing non-ASCII characters shall be presented in their native format.	- Review recovered results; Review interpretation of data containing non-ASCII characters
WRT-AO-05	If a Windows registry forensic tool provides the user with the ability to extract registry forensic artifacts well-known in the field of Windows forensics, then the tool shall have the ability to interpret related registry data without error.	- Open a file; Begin artifact extraction (if necessary)
WRT-AO-06	If a Windows registry forensic tool completes extraction of well-known registry forensic artifacts without error, then the tool shall have the ability to	- Review extracted results; Review data for readability in a useable format

ID	Test Assertion	Comments
	present all extracted data (interpreted artifacts) in a useable format via a preview-pane view, generated report or output file.	
WRT-AO-07	If a Windows registry forensic tool completes extraction of well-known registry forensic artifacts without error, then all supported registry forensic artifacts (e.g., OS configuration, user account, external device, application, etc.) shall be presented in a useable format.	- Review extracted results; Review interpretation of registry artifacts - Given that differences exist among Windows registry forensic tools, this assertion will be tested by comparing extracted results from each tool with known data. That is, the aim of this assertion is not to evaluate how many artifacts can be extracted, but to verify whether artifact extraction features of each tool are correctly implemented. Thus, each test report for a specific tool will include a list of registry artifacts checked by tool testers.
WRT-AO-08	If a Windows registry forensic tool completes extraction of well-known registry forensic artifacts without error, then all STRING data containing non-ASCII characters shall be presented in their native format.	- Review extracted results; Review interpretation of data containing non-ASCII characters

185

186

6. Assertion Measurement

The following sections provide an overview of how individual test assertions are measured.

6.1. Target File Processing

Assertions	**WRT-CA-01** If a Windows registry forensic tool provides the user with an "Open Individual Hive File", then the tool shall complete the opening process without error if the file is normal.
	WRT-CA-02 If a Windows registry forensic tool provides the user with an "Open Multiple Hive Files", then the tool shall complete the opening process without error if the files are normal.
	WRT-AO-01 If a Windows registry forensic tool provides the user with the ability to recover deleted registry objects inside the target hive file, then the tool shall have the ability to recover deleted (but complete) registry objects without error.
	WRT-AO-05 If a Windows registry forensic tool provides the user with the ability to extract registry forensic artifacts well-known in the field of Windows forensics, then the tool shall have the ability to interpret related registry data without error.
Test Action	Perform user actions relating to opening hive files, recovering deleted registry objects, or extracting registry forensic artifacts by specifying an input variation.
Conformance Indicator	Successful completion without application crash or severe error.

6.2. Abnormal Notification

Assertions	**WRT-CA-03** If a Windows registry forensic tool processes files in abnormal states (i.e., corrupted or manipulated hive files), then the tool shall notify the user that the file has invalid fields or structures without application crash.
Test Action	Perform user actions relating to opening hive files in abnormal states.
Conformance Indicator	Notification of abnormal conditions.

6.3. Data Presentation

Assertions	**WRT-CA-04** If a Windows registry forensic tool completes the opening of the target hive file without error, then the tool shall have the ability to present all registry objects in a useable format via a preview-pane view, generated report or output file.
	WRT-AO-02 If a Windows registry forensic tool completes deleted registry object recovery without error, then the tool shall have the ability to present all

	recovered results in a useable format via a preview-pane view, generated report or output file.
	WRT-AO-06 If a Windows registry forensic tool completes extraction of well-known registry forensic artifacts without error, then the tool shall have the ability to present all extracted data (interpreted artifacts) in a useable format via a preview-pane view, generated report or output file.
Test Action	Perform user actions relating to opening hive files, recovering deleted registry objects, or extracting registry forensic artifacts by specifying an input variation.
Conformance Indicator	All processed and interpreted data is presented in a usable format via a preview-pane view, generated report or output file.

195

196 6.4. Registry Object Extraction and Interpretation

Assertions	**WRT-CA-05** If a Windows registry forensic tool completes the opening of the target hive file without error, then all registry objects (i.e., Key, Value and Data) as well as associated metadata (i.e., timestamp of a key, tree structures of keys, key/value list, size of data, etc.) shall be presented without modification in a useable format.
	WRT-AO-03 If a Windows registry forensic tool completes deleted registry object recovery without error, then all recovered registry objects (i.e., Key, Value and Data) as well as associated metadata (i.e., timestamp of a key, tree structures of keys, key/value list, size of data, etc.) shall be presented without modification in a useable format.
	WRT-AO-07 If a Windows registry forensic tool completes extraction of well-known registry forensic artifacts without error, then all supported registry forensic artifacts (e.g., OS configuration, user account, external device, application, etc.) shall be presented in a useable format.
Test Action	Perform user actions relating to opening hive files, recovering deleted registry objects or extracting registry forensic artifacts, along with a reference Windows registry dataset having ground truth data.
Conformance Indicator	Processed data matches ground truth data.

197

198 6.5. Non-ASCII Character

Assertions	**WRT-CA-06** If a Windows registry forensic tool completes the opening of the target hive file without error, then all STRING data containing non-ASCII characters shall be presented in their native format.
	WRT-AO-04 If a Windows registry forensic tool completes deleted registry object recovery without error, then all recovered STRING data containing non-ASCII characters shall be presented in their native format.
	WRT-AO-08 If a Windows registry forensic tool completes extraction of well-known registry forensic artifacts without error, then all STRING data containing non-ASCII characters shall be presented in their native format.

Test Action	Perform user actions relating to opening hive files, recovering deleted registry objects or extracting registry forensic artifacts, along with a reference Windows registry dataset having ground truth data.
Conformance Indicator	Non-ASCII data is presented in its native format.

199

200

7. Test Data Creation

A set of registry hive files was created as reference data for execution of test cases. Table 1 and Table 2 list data codes that are linked to registry files for testing core features and an optional feature relating to recovering deleted registry objects. In addition, well-known registry hive files from reference Windows systems with ground truth data were prepared to test an optional feature on extracting Windows registry forensic artifacts. In that regard, Table 3 shows several artifact groups considered for populating the reference Windows systems (Vista, 7, 8, 8.1, 10 and 10RS1) to limit the scope of tool testing. For more information, the dataset and related documents can be obtained from: www.cfreds.nist.gov.

Table 1. Dataset for Testing Core Features

Category	Code	Description	Comments
Normal Registry Hive File	NR-01	Possible data types	◦ All supported data types (total 12 types)
	NR-02	Simple tree structure	-
	NR-03	Tree structure with the maximum levels	◦ 512 levels
	NR-04	Maximum key name length	◦ Log key name (255 and 256 bytes)
	NR-05	Maximum value name length	◦ Long value name (16,383 bytes)
	NR-06	Big data	◦ Big data (> 16,344 bytes)
	NR-07	Non-ASCII characters	-
	NR-08	Naming convention	◦ Unusual (but valid) key and value names
Corrupted Registry Hive File	CR-01	A hive bin with Root key	-
	CR-02	A hive bin	◦ Random selection
	CR-03	Last half	-
	CR-04	Multiple fragments with hbin header	◦ Random selection
	CR-05	Base block	◦ All blocks are valid except for ‘base block’
Manipulated Registry Hive File	MR-01	Hide a root key	◦ ‘root cell offset’ in the base block
	MR-02	Hide key names	◦ ‘key name size’ in the key (nk) cell ◦ ‘key cell size’ in the key (nk) cell
	MR-03	Hide subkeys of a key	◦ ‘number of subkeys’ in the key (nk) cell ◦ ‘subkey-list cell size’ in the key (nk) cell ◦ ‘number of subkeys’ in the subkey-list cell ◦ ‘subkey offset’ items in the subkey-list cell
	MR-04	Hide values of a key	◦ ‘number of values’ in the key (nk) cell ◦ ‘value-list cell size’ in the value-list cell ◦ ‘value offset’ items in the value-list cell
	MR-05	Hide value names	◦ ‘value name size’ in the value (vk) cell ◦ ‘value cell size’ in the value (vk) cell
	MR-06	Hide data of a value	◦ ‘data size’ in the value (vk) cell ◦ ‘data cell size’ in the data cell ◦ ‘data offset’ in the value (vk) cell ◦ ‘data type’ in the value (vk) cell
	MR-07	Hide big data of a value	◦ ‘data size’ in the value (vk) cell
	MR-08	Infinite key loop	◦ ‘subkey offset’ in the subkey-list cell
	MR-09	Invalid integer data size	◦ ‘data size’ in the value (vk) cell
	MR-10	Invalid binary data size	◦ ‘data size’ in the value (vk) cell
	MR-11	Invalid string data size	◦ ‘data size’ in the value (vk) cell

Category	Code	Description	Comments
	MR-12	Version mismatch (big data processing)	◦ 'minor version value' in the base block
	MR-13	Ambiguous key name	◦ 'encoding flag' in the key (nk) cell
	MR-14	Ambiguous value name	◦ 'encoding flag' in the value (vk) cell
	MR-15	Ambiguous encodings	◦ text encoded by various encoding standards

211

212 **Table 2. Dataset for Testing an Optional Feature: Recovering Deleted Registry Objects**

Category	Code	Description	Comments
Normal Registry Hive File with Deleted Registry Data	NRD-01	Delete keys with values, but without subkeys	-
	NRD-02	Delete a key with values and subkeys	-
	NRD-03	Delete a key without values and subkeys	-
	NRD-04	Delete a value with normal data	-
	NRD-05	Delete a value with big data	-
	NRD-06	Delete multiple values in a key	-

213

214 **Table 3. Artifacts considered for Testing an Optional Feature: Extracting Forensic Artifacts**

Windows	Artifact group	Description and related elements (**D**: description, **C**: check points, **R**: related paths) * The paths (R) show representative examples although there may exist other paths.	
Vista+ The '+' symbol signifies later versions.	Account	D	Accounts
		C	Name, type, login count, timestamps (login, pw reset, failed), etc.
		R	SAM\SAM\Domains\Account\Users\ SAM\SAM\Domains\Builtin\Aliases\ SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\
	Application	D	Installed programs
		C	Name, vendor, version, installed path, timestamp, etc.
		R	SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\?SID?\Products\ SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ SOFTWARE\Classes\Installer\Products\ USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Repository\Packages\
	Application Experience & Compatibility (Shimcache)	D	Windows Application Compatibility related data
		C	File name, file size, timestamp, etc.
		R	SYSTEM\?ControlSet?\Control\Session Manager\AppCompatCache\
	Auto Run	D	Programs that start automatically when a user logs on
		C	Name, executable path, timestamp, etc.
		R	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run\ NTUSER.DAT\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce\ NTUSER.DAT\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\
	Dialog Usage	D	Dialog box related user actions
		C	Name, timestamps, etc.
		R	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU\ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\
	External Device	D	External devices (like USB storages) plugged into the system
		C	Vendor, product, serial number, connected date, drive letter, etc.

Windows	Artifact group	Description and related elements (**D**: description, **C**: check points, **R**: related paths) * The paths (R) show representative examples although there may exist other paths.	
		R	SYSTEM\MountedDevices\ SYSTEM\?ControlSet?\Control\DeviceClasses\ SYSTEM\?ControlSet?\Enum\ SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EMDMgmt\ SOFTWARE\Microsoft\Windows Portable Devices\Devices\ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
	Network Connection	D	Configurations of interface cards and network connection history
		C	Name, IP, gateway, MAC, SSID, DNS, etc.
		R	SYSTEM\?ControlSet?\Services\Tcpip\Parameters\Interfaces\ SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\ SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\ SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\
	Network Drive	D	Network connection history to external systems
		C	Name, IP, account drive letter, type, timestamp, etc.
		R	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU\
	OS Information	D	Installed OS (Windows) information
		C	Version, install date, computer name, owner, shutdown time, etc.
		R	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ SYSTEM\?ControlSet?\Control\Windows\ SYSTEM\?ControlSet?\Control\ComputerName\
	Recently Opened File and Directory	D	Recently opened files and directories
		C	Name, timestamp, etc.
		R	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\?APP_NAME?\Recent File List\ NTUSER.DAT\Software\Microsoft\MediaPlayer\Player\RecentFileList\ NTUSER.DAT\Software\Microsoft\Office\?VERSION?\?APP_NAME?\User MRU\ NTUSER.DAT\Software\Adobe\Acrobat Reader\?VERSION?\AVGeneral\cRecentFiles\ NTUSER.DAT\Software\Adobe\Acrobat Reader\?VERSION?\AVGeneral\cRecentFolders\
	Remote Desktop	D	Network connection history to external systems
		C	IP, account ID, timestamp, etc.
		R	NTUSER.DAT\Software\Microsoft\Terminal Server Client\Default\ NTUSER.DAT\Software\Microsoft\Terminal Server Client\Servers\?IP?\
	Run Command History	D	Recently used commands from Windows Run
		C	Command, timestamp, etc.
		R	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\
	Service and Driver	D	Service and driver list
		C	Display name, description, type, start, image path, etc.
		R	SYSTEM\?ControlSet?\Services\?NAME?\
	Shared Directory	D	Shared directory list
		C	Name, directory path, type, timestamp, etc.
		R	SYSTEM\?ControlSet?\Services\LanmanServer\Shares\
	ShellBag	D	Directories or files accessed by each user account (Database to track user's window viewing preferences)
		C	Directory or file path, timestamp, etc.
		R	NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags\ NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU\ NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bags\ NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\BagMRU\

Windows	Artifact group	Description and related elements (**D**: description, **C**: check points, **R**: related paths) * The paths (R) show representative examples although there may exist other paths.	
			USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags\ USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\ USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\ShellNoRoam\Bags\ USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\ShellNoRoam\BagMRU\
	Timezone	D	Timezone information
		C	Timezone name, time offset, etc.
		R	SYSTEM\?ControlSet?\Control\TimeZoneInformation\
	UserAssist	D	Programs executed by each user account (executable and link files)
		C	Account, file name, run count, timestamp, etc.
		R	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\
Win 7 and Win 8	Search	D	Search history using Windows Search feature
		C	Search keyword, timestamp, etc.
		R	Win 7: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery\ Win 8: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\SearchHistory\Microsoft.Windows.FileSearchApp\ (Vista, 8.1 and 10 does not save search keywords into the registry.)
Win 7+	Application Experience & Compatibility (Amcache)	D	Windows Application Compatibility related data
		C	App name, executable path, hash value, timestamp, etc.
		R	Amcache.hve\Root\File\?VOLUME_GUID?\ Amcache.hve\Root\Programs\?PROGRAM_ID?\

Additional test registry hive files can be created by the tester to cover other areas of interest.

8. Test Cases

Each test case is described below. It should be noted that a test case can consist of multiple subcases according to certain conditions and methods used for generating reference data.

As mentioned in Section 7, test data for each test case were created in a process that develops a reference registry dataset with ground truth data.

8.1. Test Cases for Core Features

ID	Test Case
WRT-TC-NR-01	◦ Process a primary file containing values with various data types (total 12)
WRT-TC-NR-02	◦ Process a primary file containing a simple tree structure
WRT-TC-NR-03	◦ Process a primary file containing an experimental tree structure that is 512 or more levels deep
WRT-TC-NR-04	◦ Process a primary file containing keys with long names (255 or more bytes)
WRT-TC-NR-05	◦ Process a primary file containing values with long names (16,383 or more bytes)
WRT-TC-NR-06	◦ Process a primary file containing values with big data (> 16,344 bytes)
WRT-TC-NR-07	◦ Process a primary file containing keys and values with non-ASCII characters
WRT-TC-NR-08	◦ Process a primary file containing keys and values with unusual (but valid) names
WRT-TC-CR-01	◦ Process a corrupted primary file that contains a wiped hive bin (having root key)
WRT-TC-CR-02	◦ Process a corrupted primary file that contains a wiped hive bin (randomly selected)
WRT-TC-CR-03	◦ Process a corrupted primary file that contains wiped hive bins (last half)
WRT-TC-CR-04	◦ Process a corrupted primary file that contains wiped multiple blocks (randomly selected among blocks having the hbin header structure)
WRT-TC-CR-05	◦ Process a corrupted primary file that contains a wiped base block (all other blocks are valid)
WRT-TC-MR-01	◦ Process a manipulated primary file that contains hidden keys
WRT-TC-MR-02	◦ Process a manipulated primary file that contains hidden key names
WRT-TC-MR-03	◦ Process a manipulated primary file that contains hidden subkeys
WRT-TC-MR-04	◦ Process a manipulated primary file that contains hidden values
WRT-TC-MR-05	◦ Process a manipulated primary file that contains hidden value names
WRT-TC-MR-06	◦ Process a manipulated primary file that contains hidden data
WRT-TC-MR-07	◦ Process a manipulated primary file that contains hidden big data
WRT-TC-MR-08	◦ Process a manipulated primary file that contains an infinite key loop
WRT-TC-MR-09	◦ Process a manipulated primary file that contains an invalid integer data size
WRT-TC-MR-10	◦ Process a manipulated primary file that contains an invalid binary data size
WRT-TC-MR-11	◦ Process a manipulated primary file that contains an invalid string data size
WRT-TC-MR-12	◦ Process a manipulated primary file that contains a mismatched version indicator (focusing on big data processing)
WRT-TC-MR-13	◦ Process a manipulated primary file that contains a mismatched key name encoding flag
WRT-TC-MR-14	◦ Process a manipulated primary file that contains a mismatched value name encoding flag
WRT-TC-MR-15	◦ Process a manipulated primary file that contains key names, value names and data encoded by unsupported encoding standards

8.2. Test Cases for Optional Features: Recovering Deleted Registry

ID	Test Case
WRT-TC-NRD-01	◦ Process a primary file that contains deleted keys with values but without subkeys
WRT-TC-NRD-02	◦ Process a primary file that contains a deleted key with values and subkeys
WRT-TC-NRD-03	◦ Process a primary file that contains a deleted key without values and subkeys
WRT-TC-NRD-04	◦ Process a primary file that contains a deleted value with data
WRT-TC-NRD-05	◦ Process a primary file that contains a deleted value with big data
WRT-TC-NRD-06	◦ Process a primary file that contains deleted multiple values in a key

8.3. Test Cases for Optional Features: Extracting Forensic Artifacts

ID	Test Case
WRT-TC-FA-01	◦ Process primary files containing Account related data
WRT-TC-FA-02	◦ Process primary files containing Application related data
WRT-TC-FA-03	◦ Process primary files containing Application Compatibility (Amcache) data
WRT-TC-FA-04	◦ Process primary files containing Application Compatibility (Shimcache) data
WRT-TC-FA-05	◦ Process primary files containing Auto Run related data
WRT-TC-FA-06	◦ Process primary files containing Dialog Usage related data
WRT-TC-FA-07	◦ Process primary files containing External Device related data
WRT-TC-FA-08	◦ Process primary files containing Network Connection related data
WRT-TC-FA-09	◦ Process primary files containing Network Drive related data
WRT-TC-FA-10	◦ Process primary files containing OS Information related data
WRT-TC-FA-11	◦ Process primary files containing Recently Opened File and Directory related data
WRT-TC-FA-12	◦ Process primary files containing Remote Desktop related data
WRT-TC-FA-13	◦ Process primary files containing Run Command History related data
WRT-TC-FA-14	◦ Process primary files containing Search related data
WRT-TC-FA-15	◦ Process primary files containing Service and Driver related data
WRT-TC-FA-16	◦ Process primary files containing Shared Directory related data
WRT-TC-FA-17	◦ Process primary files containing ShellBag related data
WRT-TC-FA-18	◦ Process primary files containing Timezone related data
WRT-TC-FA-19	◦ Process primary files containing UserAssist related data

9. History

Rev	Issue Date	Section	History
1.0 draft 1	2018-04-12	All	- The first release for public comments
1.0 draft 2	2018-06-25	4	- Updated several definitions
		7	- Added ‘Test Data Creation’ section
		8	- Changed ‘Abstract Test Cases’ to ‘Test Cases’