April 2018

Windows Registry Forensic Tool Test Assertions and Test Plan

Steering Committee Draft of Version 1.0 for Public Comment

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

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.

[1] 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.

Table of Contents

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. This is accomplished by the development of both specific and common rules that govern tool specifications. 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), the National Institute of Justice (NIJ), 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, 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 a digital forensics point of view, the Windows registry is one of the 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 actions. 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 Windows registry forensic tool specification is general and capable of being adapted to digital forensic suites having registry-related features as well as dedicated registry forensic tools.

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.
- 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 storage devices 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.

Hive set – A hive set consists of hive 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 lower) as well as Volume Shadow Copies (Windows Vista and higher) 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 consisting of the registry that contains values and additional subkeys like a directory (folder) in a hierarchical file system.

Registry Value – An object consisting of the registry that contains data like 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 2.6.1 and 2.6.2, 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

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

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 present all extracted data (interpreted	- Review extracted results; Review data for readability in a useable format

	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

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.

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.

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.

7. Abstract Test Cases

Abstract test cases describe the combinations of test parameters required to fully test each assertion and the results expected for the given combination of test parameters. The test cases are abstract in that they do not prescribe the exact environment in which the tests are to be performed. They are written at the next level above the actual test environment, thus abstract test cases allowing substitution and variation of setup environment variables under dissimilar products and options prior to engagement in official testing.

It should be noted that the type of input data for registry forensic 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. The test data for each test case were created in a process that develops a reference registry dataset with ground truth data. For more information on this test dataset, please visit us at: www.cfreds.nist.gov.

7.1. Test Cases for Core Features

ID	Test Case
WRT-01	Begin data processing on the target hive file using tool-supported user interfaces, and check behaviors of a running Windows registry forensic tool.
WRT-02	Begin data processing on the target hive file having corrupted or manipulated parts, and check behaviors of a running Windows registry forensic tool.
WRT-03	Perform data processing on the target hive file, and review data output.

7.2. Test Cases for Optional Features

ID	Test Case
WRT-04	Recover deleted registry objects in the target hive file, and review data output.
WRT-05	Extract Windows registry forensic artifacts stored within the target hive file, and review data output.

8. Traceability Matrices

The following traceability matrices relate core requirements to core assertions. The requirements are defined in the document entitled: *Windows Registry Forensic Tool Specification*, located on the CFTT web site, www.cftt.nist.gov.

Requirements to Core Assertions

Requirements (Core Features)		01	02	03	04	05	06
	WRT-CR-01	•	•				
	WRT-CR-02			•			
	WRT-CR-03				•	•	•

The following traceability matrices relate optional requirements to optional test assertions.

Requirements to Assertions Optional

Requiremen ts (Optional Features)		01	02	03	04	05	06	07	08
	WRT-RO-01	•	•	•	•				
	WRT-RO-02					•	•	•	•

The following traceability matrices relate core assertions to core test cases.

Requirements to Test Cases for Core Features

Assertions (Core Features)		01	02	03
	WRT-CA-01	•		
	WRT-CA-02	•		
	WRT-CA-03		•	
	WRT-CA-04			•
	WRT-CA-05			•
	WRT-CA-06			•

The following traceability matrices relate optional assertions to optional test cases.

Requirements to Test Cases for Optional Features

		01	02
Assertions (Optional Features)	WRT-AO-01	•	
	WRT-AO-02	•	
	WRT-AO-03	•	
	WRT-AO-04	•	
	WRT-AO-05		•
	WRT-AO-06		•
	WRT-AO-07		•
	WRT-AO-08		•