Windows Artifacts Exercise

BitCuratorEdu
Last Updated: January 18, 2022
About This Exercise

Author
Cal Lee

Description
This hands-on exercise introduces students to forensic artifacts produced by Windows operating systems and tools to analyze them. These slides are excerpted from Cal Lee’s SAA “Advanced Digital Forensics” class. The sample data referenced in these slides is available here: https://github.com/BitCurator/bcc-dfa-sample-data/

Learning object type
Lesson plan/materials

Learning objectives
This learning object might be used in a lesson to satisfy the following learning objectives:

● Practice using tools in the BitCurator Environment.
Windows Artifacts
Desktop Operating System Market Share

https://www.netmarketshare.com/operating-system-market-share.aspx
Let’s make sure you can see all of the files on your computer.
Folder Options

Advanced settings:
- Hide empty drives in the Computer folder
- Hide extensions for known file types
- Hide protected operating system files (Recommended)
- Launch folder windows in a separate process
- Restore previous folder windows at logon
- Show drive letters
- Show encrypted or compressed NTFS files in color
- Show pop-up description for folder and desktop items
- Show preview handlers in preview pane
- Use check boxes to select items
- Use Sharing Wizard (Recommended)
- When typing into list view

Warning
You have chosen to display protected operating system files (files labeled System and Hidden) in Windows Explorer.
These files are required to start and run Windows. Deleting or editing them can make your computer inoperable.
Are you sure you want to display these files?

[Yes] [No]
Windows Registry

- Information about:
  - Applications installed
  - Application settings
  - Hardware installed
  - Hardware settings
  - User interface and system preferences
  - User accounts
  - Locations of files and recent activities, e.g. Most Recently Used (MRU)
  - Lots of online activities, e.g. user names and passwords, browsing and search query history
## Five Main Registry Files

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTUSER.DAT</td>
<td>One for each user account, includes information such as Most Recently Used (MRU) file lists, desktop settings, default application behaviors</td>
</tr>
<tr>
<td>SAM (Security Accounts Manager)</td>
<td>User account information (including passwords) and security settings</td>
</tr>
<tr>
<td>SECURITY</td>
<td>User and group security policies, e.g. which accounts can load device drivers, get remote access to the machine</td>
</tr>
<tr>
<td>SOFTWARE</td>
<td>Information about all install programs, including settings and directory paths</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>Windows systems settings, such as drive letter mappings, storage volume information, system boot profile, last known good configuration, system name, Windows setup information, hardware profile information</td>
</tr>
</tbody>
</table>
Where are They Located?
Registry Hives

Structure:

- **Hive**
  - **Key**
    - **Subkey**
      - **Value**

Example:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

What do you think this is?
## Registry Hives

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_CLASSES_ROOT</td>
<td>Just points to HKEY_LOCAL_MACHINE\Software\Classes</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER</td>
<td>User setting information, which is generated dynamically from HKEY_USERS when a user logs into Windows</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE</td>
<td>Hardware and software settings that are specific to this computer but shared across users (generated at startup from SYSTEM.DAT)</td>
</tr>
<tr>
<td>HKEY_USERS</td>
<td>Information about each of the user accounts on the computer, e.g. desktop settings, default software behaviors - generated at startup from NTUSER.DAT files, and when user logs out of applications or out of Windows, data are written back to the ntUSER.DAT files</td>
</tr>
<tr>
<td>HKEY_CURRENT_CONFIG</td>
<td>Just points to HKEY_LOCAL_MACHINE\Config</td>
</tr>
</tbody>
</table>

Question: Where would you find these registry hives on a disk image? (Hint: This is a trick question)
# Registry Hive Value Data Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG_BINARY</td>
<td>Raw binary data displayed as hexadecimal*</td>
</tr>
<tr>
<td>REG_DWORD</td>
<td>32-bit unsigned integer (4 bytes)</td>
</tr>
<tr>
<td>REG_EXPAND_SZ</td>
<td>Variable-length string, usually in UTF-16 (Unicode)</td>
</tr>
<tr>
<td>REG_FULL_RESOURCE_DESCRIPTOR</td>
<td>Series of nested arrays used by a hardware device, binary data displayed as hexadecimal*</td>
</tr>
<tr>
<td>REG_LINK</td>
<td>Symbolic link to another registry key (Unicode)</td>
</tr>
<tr>
<td>REG_MULTI_SZ</td>
<td>Ordered list of strings (multi-string value), usually in UTF-16</td>
</tr>
<tr>
<td>REG_NONE</td>
<td>No specific type – displayed as hexadecimal*</td>
</tr>
<tr>
<td>REG_QWORD</td>
<td>64-bit integer (8 bytes)</td>
</tr>
<tr>
<td>REG_RESOURCE_LIST</td>
<td>Series of nested arrays used by a hardware device, binary data displayed as hexadecimal*</td>
</tr>
<tr>
<td>REG_RESOURCE_REQUIREMENTS_LIST</td>
<td>Series of nested arrays used by a hardware device, binary data displayed as hexadecimal*</td>
</tr>
<tr>
<td>REG_SZ</td>
<td>Fixed-length text string, usually in UTF-16</td>
</tr>
</tbody>
</table>

*Can open in hex viewer or hex editor using View and Edit menus, respectively.*
Security ID (SID)

- One assigned to each user account
- Associated with various resources, including files, folders and Recycling Bins
SID Example

S-1-5-21-1180590209-877416012-3186324384-1002
Always an “S”, indicating that this is an SID.
Rev 19

Revision level (version of the SID specification being used).
Authority that issued the SID. Value is usually “5”, indicating NT Authority.
Domain identifier – value can be up to 500.
Account or group on a domain or local machine
Relative Identifier (RID), designating a specific user in the SAM file. Those below 1000 are default accounts (e.g. 500 = Administrator), and those 1000 or above are created for specific groups or users.
Examining an NTUSER.DAT File

- The files on your flash drive in registry.zip were extracted from a full-drive (including the operating system) disk image

- The following is an example of how these files can be extracted using FTK Imager
- Navigate to: Partition 1 > [root] > Documents and Settings > Charlie > NTUSER.DAT
- Right click on NTUSER.DAT and select Export Files.
Then export the other four registry files from Windows\System32\config.
Performing these same tasks using the BitCurator environment
- Navigate to Forensics Tools and double-click on the RegRipper icon
- NOTE: **IGNORE** examples that it presents, because they use commands and syntax for Windows, not Linux
- Issue each of the following commands:*  
  - `perl rip.pl -r ~/Desktop/sample-data/registry/SYSTEM > ~/Desktop/system-report -f system`

*Enter each command in its entirety before hitting enter (line breaks above are simply to fit the text onto the slide, not ones that you should type yourself). Remember that the up arrow and tab can save you time when typing commands.
• Create a folder on your desktop called regripper-exercise
• Go to \das-forensics-flash-drive-files\Sample Data\n• Extract contents of registry.zip to Desktop\regripper-exercise
RegRipper Instructions – Windows II

- Navigate to \das-forensics-flash-drive-files\reg-ripper
- Run rr.exe
- The next set of steps will be run 5 times—once for each of the files in regripper-exercise\registry
- Next to the Hive File window, select Browse
  - Navigate to regripper-exercise\registry and select the first Hive File
  - E.g., NTUSER.DAT
- Next to Report File, select Browse
  - Create a new file in regripper-exercise that corresponds to the Hive File above
  - E.g., NTUSER_report.txt
- In the Profile dropdown, select the appropriate profile
  - E.g., ntuser
- Select Rip It.
- Repeat the above steps for SAM, SECURITY, SOFTWARE, and SYSTEM
RegRipper Output Questions

Examine ntuser-report.txt
Are you able to identify files that the user recently opened? If so, what were they? Can you determine what the most recently opened files of specific types (e.g. txt) were?

Examine sam-report.txt
How many accounts were there on the computer that is represented in the disk image? What is the Relative Identifier (RID) for the user account you’re examining? What other interesting information can you gain from the SAM report about this user account and how might you use that information?

Examine security-report.txt
What is the Machine SID for the computer represented in the disk image? Why would you want to know this? How does it relate to the RID that you identified above?

Examine software-report.txt
Identify three different applications that were installed on the computer and the file paths where the applications were stored.

Examine system-report.txt
Find the devclass output. What does this output tell you? How might this information be useful?
RegRipper Output Discussion: ntuser-report

• Are you able to identify the files that the user recently opened? If so, what were they?
  • How did you go about finding this information?
  • What line number(s) points to this information?

• Can you determine what the most recently open files of specific types (e.g. txt) were?
  • How did you go about finding these?
  • What line numbers have this information?

• Look at lines 1109-1117—what type of information are you looking at?

• Is there any other information you find particularly compelling in this report?

• What might you do with this information?
RegRipper Output Discussion: sam-report

• How many accounts were there on the this computer?
  • How did you go about finding this information?
  • What line number(s) points to this information?

• What was the Relative Identifier (RID) for the user account you’re examining?
  • How did you go about finding this?

• How many logins did Pat make on this machine?

• Is there any other information you find particularly compelling in this report?

• What might you do with this information?
RegRipper Output Discussion: security-report

- What is the Machine SID for the computer represented here?
  - How did you go about finding this information?
  - What line number(s) points to this information?

- Why would you want to know this information?

- How does this relate to the RID in the previous report?
RegRipper Output Discussion: software-report

- Identify three different applications that were installed on this computer
  - How did you go about finding this information?
  - What line number(s) points to this information?

- Why would you want to know this information?

- How might it aid description?

```plaintext
1 Launching appinitdlls v.20130425
2 appinitdls v.20130425
3 (Software) Gets contents of AppInit_DLLs value
4
5 AppInit_DLLs
6 Microsoft\Windows NT\CurrentVersion\Windows
7 LastWrite Time Fri Nov 20 18:55:34 2009 (UTC)
8 AppInit_DLLs : (blank)
9 LoadAppInit_DLLs : 1
10 *LoadAppInit_DLLs value globally enables/disables AppInit_DLLs.
11 0 = disabled (default)
12
13 Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows not found.
14 Analysis Tip: The AppInit_DLLs value should be blank; any DLL listed
15 is launched with each user-mode process.
16 ------------------------------
17 apppaths v.20120524
18 (Software) Gets content of App Paths subkeys
19
20 App Paths
21 Microsoft\Windows\CurrentVersion\App Paths
```
RegRipper Output Discussion: system-report

- Find the devclass output
- What does this output tell you?
- How might this information be useful?
Viewing and Copying Registry Information if You’re Running the Original Environment

- What if you’re actually running the original computer? How might you get information out of the registry?
- What if you wanted to replicate that registry information on another computer?
- Hint: There are tools built into Windows for this.
Restore Points

- Snapshots of Registry hives and some other essential system (including .EXE, .INI, .LNK) files. They’re created:
  - when there are major system changes, e.g. installing software
  - at regularly scheduled intervals
  - if the user manually creates one

- Let’s look at some restore points: Start Button > All Programs > Accessories > System Tools > System Restore [or just “System Restore” in the Start box]
Examining the Recycle Bin

1. In the start menu box, type “cmd”
2. Type: “cd c:\$recycle.bin” (What is this doing?)
3. Type “dir /a” (What is this doing?)
4. Type “dir *.* /s” (What is this doing?)
5. Put one or more files into the Recycle Bin (by moving there or by deleting)
6. Repeats steps 2-4. What do you see now?
A Brief Discussion of Mac Forensics

- No Registry, so where is all the good stuff stored?
Archival Importance and Role of SID

- If the volume is NTFS, you can find the SID associated with a specific file.
- If you also have registry files from the original computer (particularly SAM.DAT), you can get information associated with that SID, such as the name of the user/group, last time he/she logged in, and various other account details.
setuplog.txt

- See disk image example below: Partition 1 > [root] > WINDOWS > setuplog.txt

- What do you see in this file?
- What information could be useful for digital curation? When/how might you use it?
This resource was released by the BitCuratorEdu project and is licensed under a Creative Commons Attribution 4.0 International License.

Most resources from the BitCuratorEdu project are intentionally left with basic formatting and without project branding. We encourage educators, practitioners, and students to adapt these materials as much as needed and share them widely.

The BitCuratorEdu project is a three-year effort funded by the Institute of Museum and Library Services (IMLS) to study and advance the adoption of digital forensics tools and methods in libraries and archives through professional education efforts. This project is a partnership between Educopia Institute and the School of Information and Library Science at the University of North Carolina at Chapel Hill, along with the Council of State Archivists (CoSA) and several Masters-level programs in library and information science.