Windows Forensic Analysis

Dedicated to incident response and computer forensic analysis topics, with respect to Windows 2000, XP, 2003, and Vista operating systems

WFA: Locating indications of CD burning in a Windows image

Windows systems record a great deal of user and system activity, and much of this information is recorded and maintained automatically, without any user interaction (though some specifics steps may be taken to prevent the data from being recorded). This data can be extremely valuable to a forensic analyst pursuing an investigation.

A question that comes up during data leakage or theft investigations (as well as investigations involving illicit images) is whether or not the user created or burned a CD or DVD. Indications of this kind of activity may possibly be retrieved from several locations within an acquired image.

Throughout this article, I will be demonstrating artifacts that can be observed during the forensic analysis of an acquired Windows image. On a Dell Latitude D820 laptop, I have the Roxio Creator Plus application (from Sonic Solutions) installed. This application shipped with the system from Dell. I had an opportunity to burn a DVD, so I used that opportunity to look for artifacts that would indicate to an analyst that a user had created a CD or DVD. While this work was performed on a live system, the artifacts can also be retrieved from a system image.

Registy – UserAssist Keys

An excellent place to begin looking for information regarding a particular user's use of CD- or DVD-ROM burning software is to check that user's UserAssist key entries. As I had created a DVD on my own system, I checked for entries within the HKEY_CURRENT_USER hive, and found the following entry:

```
UEME_RUNPATH:C:\Program Files\
  Common Files\Sonic Shared\
  Sonic Central\Main\Mediahub.exe
```

The timestamp for this entry was:

1/15/2008 8:49:21 AM

What this entry from the UserAssist key shows is that the last time I launched this application was at almost 8:50AM on 15 January 2008. The UserAssist key provides an excellent place to start when attempting to determine applications a user may have launched or accessed via the Windows Explorer shell. This Registry key can provide some clues not only to what applications a particular user launched, but on systems with multiple users an analyst may be able to determine which of the users launched an application. In this case, the analyst (me) is able to determine that a user (me) accessed an application that is used to create CDs and DVDs, and when that access last occurred.

> On Windows XP systems, the *.pf files in the %WinDir%\Prefetch folder may provide clues as to which applications were launched on the system. However, keep in mind that the *.pf files are not user-specific, and apply to the entire system. On multi-user systems, an analyst will not be able to tell which user launched an application based solely on the *.pf files.

Registry – SOFTWARE\Sonic

As stated earlier, the system I was working on had a specific application installed for creating CDs and DVDs. As such, my next thought was to see what artifacts are left by the use of the application itself. I first located the following Registry key:

HKCU\Software\Sonic\MediaHub\
Preference\Plugins\{BBD5C82E-73E5-42F8-835B-5F1C61472F30}\ImageList

This Registry key contains a most recently used (MRU) list of ISO images that I had burned to CD or DVD on this system. These images are all *.iso files (Linux CDs, etc.) that I had downloaded and burned to CD.

On another system, a different version of the Sonic Solutions software is installed. This application is the RecordNow! product. This product maintains an MRU list of burned images beneath the following Registry key:

HKCU\SOFTWARE\Sonic\RecordNow\
Preferences\MRUImages

The value names are numbered sequentially beginning at 1, with the most recently burned image (in this case, “ubuntu-7.10-desktop-i386.iso”) being named/numbered “1”.

I then located another Registry key of interest:

HKCU\Software\Sonic\MediaHub\
Preference\Plugins\{C4A5D5A4-1511-4610-8660-683A39805F7F}

Within this key is a Registry string value named “LastAddFilePath” that points to the last directory that I opened when adding content to my DVD (i.e., “G:\book2\DVD\”). When creating a data disc through the Roxio UI, I had to click on the “Add Data” button (illustrated in figure 1) in order to add content to my DVD.

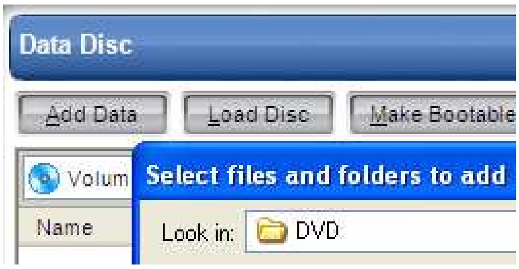

Figure 1

System Event Log

On the day that I created a DVD, I had booted the system at 5:30am, as indicated by an event ID 6009 in the System Event Log. The timestamp from my UserAssist key entries shows that I launched the Roxio Creator Plus application at approximately 8:49AM. At 8:48AM, the Service Control Manager generated an event record with event ID 7035 to the System Event Log, stating that the “IMAPI CD-Burning COM service was successfully sent a start control”. “IMAPI[1]” refers to the Image Mastering API within Windows. This event record was followed by several others that indicated that the service entered a running state, and then was stopped, and then at 8:49AM, the service was again “successfully sent a start control”.

On Windows 2003, the IMAPI CD-Burning COM service is disabled[2] by default, so users may have difficulty when attempting to burn CDs.

There did not appear to be any relevant entries in either the Security or Application Event Logs around those times.

Project Files

Some CD/DVD creation applications allow the user to create a project file that contains a listing of files burned to the media. For example, the version of Roxio CD Creator that I used allows you to save your project

[1] http://msdn2.microsoft.com/en-us/library/aa364806.aspx
[2] http://support.microsoft.com/kb/326982

file as a *.sonic file (the default filename is "MyProject").

To see the list of files burned to the media, open the *.sonic file in hex editor. While the *.sonic file has a binary format, the names of the files included in the project are clearly visible.

Sonic Solutions' RecordNow! application allows the user to save the project file as a *.pxj file, with the default filename including the date and time that the project was saved. For example, saving a project on 16 Jan 2008 at 2:52PM results in a default filename of "Data_080116_1452.pxj".

As with *.sonic files, *.pxj files are saved in a binary format, but the files included in the project are visible when the file is viewed in a hex editor.

CD Burning

With Windows XP in particular, additional software is not required in order to create or burn CDs. By default, Windows XP has the ability to write to CD-Rs, as well as write to and erase data from CD-RWs[3] (there is also a similar KB article[4] for Windows 2003). Files meant to be burned to CD via Windows XP are placed in a staging directory, located in the user's profile in the following path:

{username}\Local Settings\
  Application Data\Microsoft\
  CD Burning

Prior to being burned to CD, the selected files are "copied to a monolithic disk image file" named "CD Burning stash file.bin".

In order to locate the CD Burning directory for a specific user, navigate to the following key:

HKCU\Software\Microsoft\Windows\
  CurrentVersion\Explorer\Shell Folders

Beneath this key, locate the value named "CD Burning". The string data for this value points to the staging area used by Windows XP for the user to burn CDs.

The examiner should remember that users can also use Windows Media Player and RealPlayer to create or "burn" CDs.

Summary

Forensic analysis of an acquired Windows image can lead to significant artifacts indicating the use of CD/DVD creation software. Values in the UserAssist key will provide indications of applications launched or accessed by the user, and product-specific Registry keys within the user's Software hive may provide additional information. Further artifacts may be recovered from other sources, such as the application directory, log files, or the System and Application Event Logs.

Resources

- **WFA: The UserAssist Registry Keys Explained**
- **ISORecorder[5] PowerToy Utility for Windows XP, 2003, and Vista**

Harlan is a forensic analyst located in the metro DC area, and is the author of three books related to live response and forensic analysis of Windows systems. He also presents at conferences and provides training on those same topics, as well. He can be reached at keydet89@yahoo.com.

[3] http://support.microsoft.com/kb/279157

[4] http://support.microsoft.com/kb/317525

[5] http://isorecorder.alexfeinman.com/isorecorder.htm