Digital Investigation 11 (2014) 102–110

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Structure and application of IconCache.db files for digital forensics

Chan-Youn Lee, Sangjin Lee*

Center for Information Security Technologies (CIST), Korea University, Anam-Dong, Seongbuk-Gu, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 3 February 2014
Received in revised form 20 May 2014
Accepted 21 May 2014
Available online 11 June 2014

Keywords:
Anti-forensics
Digital forensics
Icon
IconCache.db
User behavior

ABSTRACT

Anti-forensics has developed to prevent digital forensic investigations, thus forensic investigations to prevent anti-forensic behaviors have been studied in various area. In the area of user activity analysis, "IconCache.db" files contain icon cache information related to applications, which can yield meaningful information for digital forensic investigations such as the traces of deleted files. A previous study investigated the general artifacts found in the IconCache.db file. In the present study, further features and structures of the IconCache.db file are described. We also propose methods for analyzing anti-forensic behaviors (e.g., time information related to the deletion of files). Finally, we introduce an analytical tool that was developed based on the file structure of IconCache.db. The tool parses out strings from the IconCache.db to assist an analyst. Therefore, an analyst can more easily analyze the IconCache.db file using the tool.

Introduction

Digital evidence is becomes increasingly important in court cases, thus anti-forensic techniques have been developed that delete or hide digital evidence.

Thus, research into the detection of anti-forensic behaviors has been conducted actively. Analysis of the Windows Registry (Carvey, 2005) and PreFetch folder (Carvey, 2009) are representative methods that are used to detect anti-forensic behaviors. However, deleting data in certain Windows Registry keys and PreFetch folder is also a basic anti-forensic method. They can be deleted easily using cleaner applications (e.g., CCleaner) that can be downloaded from the Internet.

IconCache.db file records the traces of applications that have been executed or deleted on a user's computer or an external storage device (Collie, 2013). The recorded icon cache information remains undeleted even when applications, the Windows Registry, and PreFetch folder have been deleted. Therefore, IconCache.db is useful for the analyzing anti-forensic behaviors. Although the IconCache.db file is useful in the area of digital forensics, the IconCache.db file has not been researched actively by forensic analysts as an analytical method for detecting anti-forensic behaviors.

Previous research into the IconCache.db file has been conducted only by Collie (Collie, 2013), who studied the general characteristics of the IconCache.db file, such as the number of icons created by Windows OS and the traces of icon cache information related to the files executed for the first time. The research of Collie is pretty meaningful in that it found additional artifacts for analyzing anti-forensic behaviors in digital forensic aspects.

This article extends the foundational work in Collie and delves deeper into the IconCache.db file structure. In the present study, therefore, we analyzed the overall structure, the mechanism that records the file paths, and the characteristics of IconCache.db files to suggest the more effective methods for their utilization in digital forensics.

* Corresponding author. Fax: +82 2 3290 4738.
E-mail addresses: liebich@korea.ac.kr (C.-Y. Lee), sangjin@korea.ac.kr (S. Lee).

http://dx.doi.org/10.1016/j.diin.2014.05.017
1742-2876/

We examined research into three Microsoft Windows operating systems: Windows Vista, 7, and 8. Although these are currently issued operating systems, there is no existing tool to support the analysis of IconCache.db files in these operating systems. Therefore, we have developed a new analysis tool for these systems.

We describe the structure of IconCache.db files, including a method for analyzing the file paths, and the attributes of IconCache.db files are illustrated. Based on the structure and attributes of the IconCache.db file, we propose methods to trace anti-forensic behaviors for digital forensic analysis. Finally, we introduce an analytical tool for IconCache.db files, which was developed based on the results of this study.

IconCache.db file structure

IconCache.db files have been used since Windows 95 but their names and storage paths differ according to the version of Windows. The storage paths of the IconCache.db file in Windows XP, Vista, and 7 were described in a previous study (Collie, 2013). The present study describes the storage paths for IconCache.db file in Windows 8 and earlier versions of Windows XP, where the details are shown in Table 1.

The ThumbnailExpert[1] was used to analyze the IconCache.db file but this tool (ThumbnailExpert) can only analyze the IconCache.db files in Windows XP and earlier versions. This tool only shows the icon images of the IconCache.db files in Windows Vista and 7, and it does not support Windows 8. Unfortunately, the ThumbnailExpert program cannot be downloaded from its official website. However, you can download its demo version easily from the Internet.[2]

Therefore, to develop a tool that can analyze IconCache.db files in Windows Vista, 7, and 8, we focused on the overall structure of IconCache.db files in these versions.

Overall structure

As shown in Fig. 1, the IconCache.db file structures differ in Windows Vista, 7, and 8. In Windows Vista and 7, the IconCache.db file is separated into three parts: header, the paths of icons, and image data. The file classifies each icon image according to its resolution and stores it as a BMP image. The size of the IconCache.db file increases in proportion to the icon cache data.

In Windows 8, however, the IconCache.db file records the file paths for icons without image data. The image data are stored separately in other files, as shown in Fig. 2. Windows 8 stores the image data for the IconCache.db file in the path "%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer" by classifying the data according to their resolution. The icon data are stored at a higher resolution (96, 256, or 1024) than that used in Windows Vista and 7.

The IconCache.db file header was described in a previous study. The present study analyzed the structure of the file paths and the image data area. The file paths for icons are stored next to the header information. The file paths are divided and stored into three sections, as shown in Fig. 3. In Windows XP, however, an unknown data area exists between the header and the first section, but the present study focuses on the IconCache.db of Windows Vista, 7, and 8.

Table 1
Names and storage paths of IconCache.db files in versions of Windows.

File name	Win ver.	File path
ShellIconCache	95	%SystemDrive%\Windows\ShellIconCache
	NT/2000	%SystemDrive%\Winnt0\ShellIconCache
IconCache.db	XP	%SystemDrive%\Documents and Settings\Username\Local Settings\Application Data\IconCache.db
	Vista/7/8	%UserProfile%\AppData\Local\IconCache.db

The first 4 bytes at the beginning of each section represents how many file paths are stored in the section. When analyzing the IconCache.db file, the first 4 bytes can be used as a marker to distinguish among sections.

In the first section, the IconCache.db file stores the default file paths for the icons that are installed during Windows installation. When a user executes, views, and copies the applications, the icon information for the applications is stored in order. In the second section, the file paths for links or shortcuts are stored. In the third section, the file paths for applications that are executed, viewed, copied, and installed by a user are stored in order after Windows installation. In other words, all of the file paths in the IconCache.db file of Windows Vista, 7, and 8 are stored in the order in which they are utilized by a user (copied, executed, installed, or viewed). The details of this process are described in Section Recording order and data creation in IconCache.db.

Detail structure of the file paths

The file path structure of Windows Vista, 7, and 8 is described in Fig. 4. As mentioned earlier, the numbers of the file paths follow the first 4 byte in each section. The signature and the string length for the file path are stored in front of the file path. The location information of the icon image data is stored after the file path.

The signature differs according to the version of Windows. The method used to calculate the string length of the file path also differs according to the signature, which depends on whether a string type in Unicode or ASCII code can be recognized by signatures. There are two methods for calculating the string length, which are shown in Table 2.

As shown in Fig. 4, the signature of the file path is '01 00' and the string length of the file path is '20 00'. The string length of the file path can be calculated as shown in Table 2, i.e.,'20 h × 2 = 40 h.' Therefore, the string length is '40 h'.

However, the file path structure of the first section differs from that of the second and third sections, because the file path does not have a signature in the second and third sections, as shown in Fig. 5.

[1] http://www.forensicswiki.org/wiki/ThumbnailExpert.
[2] http://rghost.net/43965785.