March, 2017

Amcache and Shimcache Forensics

When and how to leverage Amcache and Shimcache artifacts

LIFARS

your digital world, secured

Contents

Overview

Amcache and Shimcache can be a powerful source of evidence to help expedite forensic investigations. Having such evidence can provide a timeline of which program was executed and when it was first run and last modified. In addition, these artifacts provide program information regarding the file path, size, and hash depending on the OS version.

Amcache

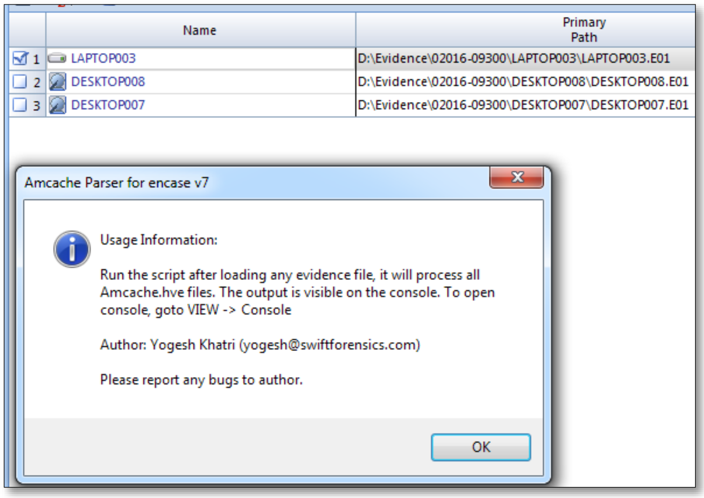
The Amcache.hve file is a registry file that stores the information of executed applications. These executed applications include; the execution path, first executed time, deleted time, and first installation. Using the Amcache.hve file in combination with information from Windows Prefetch and Iconcache.db files, creates an overall timeline of applications.

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.

On Windows 8, Amcache.hve replaces RecentFileCache.bcf and uses the Windows NT Registry File (REGF) format. A common location for Amcache.hve is:

C:|Windows|AppCompat|Programs|Amcache.hve

Amcache.hve file is also an important artifact to record the traces of anti-forensic programs, portable programs, and external storage devices. One of the Enscripts called "Amcache Parser for Encase v7" can be used for Amcache parsing as below.



		Name	Primary Path
☑	1	LAPTOP003	D:\Evidence\02016-09300\LAPTOP003\LAPTOP003.E01
☐	2	DESKTOP008	D:\Evidence\02016-09300\DESKTOP008\DESKTOP008.E01
☐	3	DESKTOP007	D:\Evidence\02016-09300\DESKTOP007\DESKTOP007.E01

Amcache Parser for encase v7

Usage Information:

Run the script after loading any evidence file, it will process all Amcache.hve files. The output is visible on the console. To open console, goto VIEW -> Console

Author: Yogesh Khatri (yogesh@swiftforensics.com)

Please report any bugs to author.

Figure 2. Amcache parser for Encase 7

```
*****************************************************************************
Processing Root\File\0d5b9245-d310-11e4-8a68-806e6f6e6963
File Reference = 10000012ddf
Volume GUID = {0d5b9245-d310-11e4-8a68-806e6f6e6963}
Possible First Run Timestamp (Last Modified on key) = 07/27/16 11:13:43 PM
Modified Time2 = 05/19/15 01:40:17 PM
File path = c:\program files\microsoft office
15\root\vfs\programfilescommonx86\microsoft shared\smart tag\FPERSON.DLL
Program ID = 0000bcdd5c7b5c4e8e4df2fa092abc33069a0000ffff
SHA1 hash = 00007f0bd70795c93863843b381473debb9ebb01dfa9
-----------------------------------------------------------------------------
File Reference = 10000013b02
Volume GUID = {0d5b9245-d310-11e4-8a68-806e6f6e6963}
Possible First Run Timestamp (Last Modified on key) = 07/27/16 11:13:42 PM
Modified Time2 = 05/28/16 11:06:12 AM
File path = c:\program files\microsoft office 15\root\office15\addins\OUTLVBA.DLL
Program ID = 0000bcdd5c7b5c4e8e4df2fa092abc33069a0000ffff
SHA1 hash = 000058c3920d85057d4e63ac04cc61870ad009daccbb
```

Figure 3. Results for Amcache parser for Encase 7

Shimcache

Shimcache, also known as AppCompatCache, is a component of the Application Compatibility Database, which was created by Microsoft and used by the Windows operating system to identify application compatibility issues. This helps developers troubleshoot legacy functions and contains data related to Windows features. It is used for quick search to decide whether modules need shimming for compatibility or not.

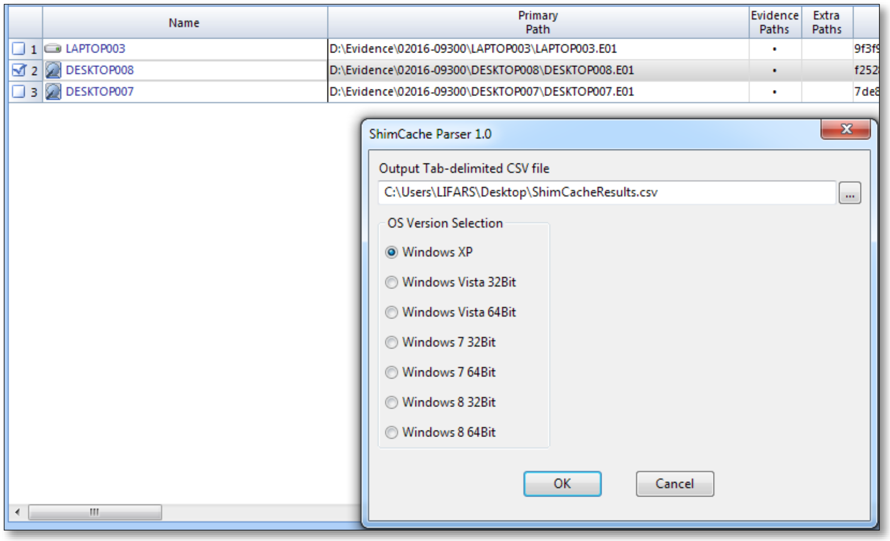
A Shim is a small library that transparently handles the applications interworking's to provide support for older APIs in a newer environment or vice-versa. Shims allow backwards and forwards compatibility for applications on different software platforms.

The Registry Key related to this cache can be found and located as below.

HKLM|SYSTEM|CurrentControlSet|Control|SessionManager|AppCompatCache|AppCompatCache

Forensic examiners can use indicators they find in the ShimCache data to triage other data sources, such as AmCache.hve file, Prefetch files with sources such as "Service Control Manager" in a timeline. The Service Control Manager starts, stops, and interacts with Windows services via the API that Microsoft Management Console (MMC) and Service Control Utility (SC) also use.

There is an EnPack called "shimcache_parser.enpack" for Encase 7 that can be used for Shimcache parsing as below.



	Name	Primary Path	Evidence Paths	Extra Paths	
□ 1	LAPTOP003	D:\Evidence\02016-09300\LAPTOP003\LAPTOP003.E01	•		9f3f9
☑ 2	DESKTOP008	D:\Evidence\02016-09300\DESKTOP008\DESKTOP008.E01	•		f252
□ 3	DESKTOP007	D:\Evidence\02016-09300\DESKTOP007\DESKTOP007.E01	•		7de8

ShimCache Parser 1.0

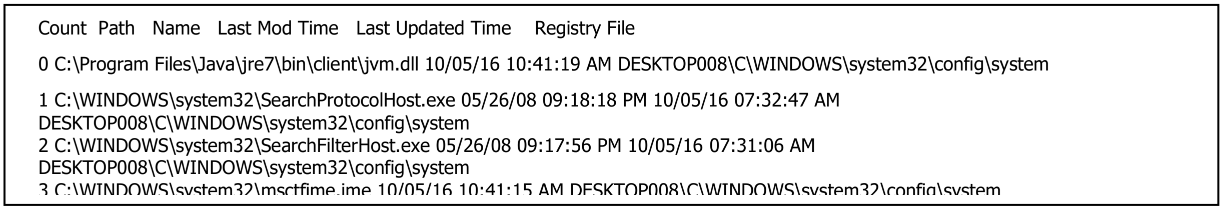
Output Tab-delimited CSV file

C:\Users\LIFARS\Desktop\ShimCacheResults.csv

OS Version Selection

● Windows XP
○ Windows Vista 32Bit
○ Windows Vista 64Bit
○ Windows 7 32Bit
○ Windows 7 64Bit
○ Windows 8 32Bit
○ Windows 8 64Bit

Figure 4. Shimcache parser for Encase 7



```
Count  Path   Name   Last Mod Time   Last Updated Time    Registry File

0 C:\Program Files\Java\jre7\bin\client\jvm.dll 10/05/16 10:41:19 AM DESKTOP008\C\WINDOWS\system32\config\system

1 C:\WINDOWS\system32\SearchProtocolHost.exe 05/26/08 09:18:18 PM 10/05/16 07:32:47 AM
DESKTOP008\C\WINDOWS\system32\config\system
2 C:\WINDOWS\system32\SearchFilterHost.exe 05/26/08 09:17:56 PM 10/05/16 07:31:06 AM
DESKTOP008\C\WINDOWS\system32\config\system
3 C:\WINDOWS\system32\msctfime.ime 10/05/16 10:41:15 AM DESKTOP008\C\WINDOWS\system32\config\system
```

Figure 5. Results for Shimcache parser for Encase 7

Leveraging Amcache and Shimcache artifacts

Forensic investigators can use these Amcache and Shimcache artifacts to find the below information when they analyze forensic images for a case:

- The Shimcache tracks metadata such as the full file path, last modified date, and file size
- Amcache.hve records the recent processes that were run
- The events in Shimcache.hve are listed in chronological order with the most recent event first
- Amcache.hve records the programs SHA1 so it can be researched with databases like VirusTotal for easy identifiacation
- The Shimcache only contains the information prior to the system's last startup, as current entries are stored only in memory
- The Amcache.hve lists the path of the files that's executed which can then be used to find the executed program
- Use Shimcache along with your timelines to recreate and determine malicious activities