Forensic Analysis of Windows Thumbcache files

Completed Research Paper

Darren Quick
University of South Australia
darren.quick@mymail.unisa.edu.au

Christopher Tassone
University of South Australia
christopher.tassone@mymail.unisa.edu.au

Kim-Kwang Raymond Choo
University of South Australia
raymond.choo@unisa.edu.au

Abstract

A range of court cases and forensic investigations have involved thumbnail pictures contained within operating system files, such as thumbcache and thumbs.db. In many of these cases, the thumbnail image has been the evidence presented to a court. Further analysis may locate additional information relating to thumbnail pictures, such as being able to link a thumbnail to a picture file on storage media, or locating information relating to the original file used to create the thumbnail, such as the full path and original file name. Using real-world law enforcement and test data, we demonstrate the application of our proposed operational methodology to conduct analysis of thumbcache files. We also propose a reporting and visualisation methodology to present the evidence to investigators, legal counsel, and court, which then forms the basis of our software prototype. Insider threat cases which involve pictures of intellectual property can potentially benefit from our proposed method.

Keywords

Digital Forensic Analysis, Thumbcache, Microsoft Windows, Computer Forensics

Introduction

Various computer operating systems include the ability to view picture and other files within a folder as smaller thumbnail images, representative of the file contents. In Microsoft Windows, this was introduced in Windows 95B and is enabled by storing thumbnail images in system container files, such as Thumbs.db, or later; Thumbcache.db files. These, and other system files, store a range of information such as the original filename, and dates and times, which is of great interest in forensic examinations.

Picture files are often associated with a range of crime types, such as sexually related crimes (McMillan et al. 2013), drug offences, and insider threat cases, where pictures can potentially exist as thumbnail entries within operating system files. Thumbnail images have previously been evidence in court cases, and the term ‘thumbnails’ has been defined in case law. In United States v Romm [2006] USCA9 387; 455 F.3d 990 (24 July 2006), it is said that ‘the term "thumbnail," which derives from an artist's thumbnail sketch, refers to "a small image of a graphics file displayed in order to help you identify it” Downing, supra at 495’. Thumbnail images have been discussed in a number of court cases in various jurisdictions, including USA, Australia, and the United Kingdom. In many cases, it is the thumbnail image alone that has been the

evidence presented to court. However, there may be additional information in hidden and system files which may provide relevant evidence and further explain the origin of specific files. In an insider threat case, a suspect could be selling intellectual property in the form of pictures of new and unreleased technology to competitors. If a suspect has erased pictures, there may still be evidence in thumbcache files, but this alone may not be enough to provide grounds for legal action. By conducting further analysis, there may be associated data relating to the erased pictures residing in the windows.edb file, which, in association with the thumbnails, may be enough to provide grounds for legal action.

In this paper, we first provide background information relating to the various versions of Microsoft Windows thumbnail stores. We then review criminal cases which mention thumbnail pictures, and current literature regarding thumbnail forensic analysis methods and opportunities to locate additional information. We also discuss current forensic and other software available for thumbcache analysis. Next, we outline our proposed operational methodology using a common forensic framework as applied to thumbcache analysis. We then propose a method to visualise the thumbcache information and a software prototype to extract and present information to an examiner and produce a report. The last section summarises the research findings and outlines potential future research opportunities.

Our contributions are two-fold:

1. An operational methodology for thumbcache analysis to identify files associated with a thumbnail, including timestamps, original file location, and other metadata where this is available.
2. A reporting and visualisation methodology and software prototype in relation to thumbcache analysis and presentation of the resulting information.

Overview of Microsoft Windows Thumbnail stores

Windows 95, 98, ME, 2000, XP, 2003

Microsoft Windows 95B introduced the ability to view a folder in Windows Explorer as thumbnails rather than as file details or icons (Casey 2002; Hurlbut 2005). This feature was carried through into subsequent versions, such as; Windows 98, Multimedia Edition (ME), 2000, XP, and 2003. Initially to enable this feature, a hidden system file is created in the folder the files are stored in, called 'thumbs.db' which store a database of miniature images. In addition, 'the early versions of thumbs.db files as they appeared in Windows ME and Windows 2000 contained not only the thumbnail image of the parent file, but also the filename, drive letter, and path to that image. Later versions, Windows XP and Windows 2003, store the image and its filename but not the path' (Hurlbut 2005). This information is of great assistance to a forensic examiner.

Windows Vista

Windows Vista introduced a new method of caching thumbnail images, named; Thumbcache.db, and reduced the use of thumbs.db database files. As outlined by Stewart (2007) Vista provided scalable thumbnails, such as medium and larger sizes, and uses a centralised thumbnail cache for each user located at:

C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer\

At this location are numerous thumbnail cache files named; Thumbcache_32.db, Thumbcache_96.db, Thumbcache_256.db & Thumbcache_1024.db (Purcell and Lang 2008). These contain JPG, BMP and PNG files in various corresponding maximum pixel sizes; 32x32, 96x96, 256x256 and 1024x1024 (Stewart 2007). Also stored with each thumbnail is a unique ID number for each associated thumbnail, the ThumbnailcacheID. Within the thumbcache folder location, there is a file named 'thumbcache_idx.db' which is an index file containing the ThumbnailcacheID for the thumbnails and a Windows FILETIME value for when the parent file was created [5].

The hash algorithm used to produce the ThumbnailcacheID value is outlined by Khatri [9]. Research was undertaken by Khatri to determine the hash algorithm, and states that; 'to generate the ThumbnailcacheID windows uses the volume GUID (that the file resides on), the FILEID (for NTFS

volumes), the extension of the file (.xxx) and the file last modified time (as a DOS GMT date). The values 'are 'blended and mangled' using a hash function' [9]. It is also concluded that due to the hashing format, it is not possible to reverse the ThumbnailcacheID to return the original path.

Parsonage (2012) explains that Windows Vista did not discard the 'thumbs.db' files, and these files can still be located with the operating system. Using Windows Vista, it is demonstrated that thumbs.db files are created in a folder when pictures are accessed via a Universal Naming Convention (UNC) path and displayed in thumbnail view (medium, large or extra-large size). The thumbnails in these thumbs.db files are 256x256 pixels. Access via the UNC path can be undertaken via a network share or from a local computer (Parsonage 2012). In our experiments, we determined that this also applies to Windows 7, for example, using the UNC path for a localhost; '\\127.0.0.1\c$', in Windows Explorer will open the root C:\ drive as a network share. If there is a picture file at this location, a thumbs.db file will be created, even though the image itself is not viewed. If a user then copies and pastes a picture to this location, a thumbs.db file will be created with a thumbnail of the picture, even though a user has not viewed this picture.

The forensic value of thumbnails is also discussed by Parsonage (2012), relating to a commonly held opinion that the presence of thumbnails is an indicator of guilty knowledge; i.e. 'for the pictures to exist in the thumbnail database the folder containing the pictures must have been opened in Windows Explorer in a thumbnail view thus implying that the user must have knowledge of them', which is then refuted by Parsonage (2012) and Morris and Chivers (2011) as there are occasions when pictures can be created in thumbs.db and thumbcache files without a user seeing the picture in question. This is also confirmed in our experiments.

Windows 7

In Windows 7, the structure of the thumbcache_idx.db index file is different to Vista, and does not store the windows FILETIME value (ESCForensics 2012). Also, the Windows Desktop search file, Windows.edb, stores additional information for some ThumbnailcacheIDs (ESCForensics 2012; Morris and Chivers 2011). As well as storing thumbnail pictures, the thumbcache files in Windows 7 also contain the names of networked computers, GUIDs and drive letter information. Morris and Chivers (2011) outline the behaviour of Windows 7 and the creation and modification of records in the thumbcache files, and they conclude that there are situations when a record may be created for a file which has not been viewed.

As discussed by Morris and Chivers (2011), it is also possible to locate ThumbnailcacheID references in the Windows desktop search database, Windows.edb. The Windows.edb file is described by ESCForensics (2012) and Chivers and Hargreaves (2011) and stores ThumbnailcacheID values with other metadata for some files. The Windows.edb and associated files are located at;

C:\ProgramData\Microsoft\Search\ Data\Applications\Windows\

Software such as, WDSCarve.exe (Chivers and Hargreaves 2011) or Woanware's EseDbViewer (http://www.woanware.co.uk) can be used to view the contents of Windows.edb files. Often when trying to access an extracted windows.edb file there will be errors reported. It is necessary to use a Windows command line utility to repair the file, and in our experiments often required multiple passes to repair the database. The process outlined by Chivers and Hargreaves (2011) also includes using MSS.log files to repair the Windows.edb file;

esentutl -r MSS -d

If the MSS.log files are not available, the following command can be entered on a command line;

esentutl /p windows.edb

Within the Windows.edb file is a table named SystemIndex_0A, which can be exported to a comma-separated value (CSV) file for viewing as a spreadsheet. Undertaking a search for a ThumbnailcacheID value in the CSV file will determine if there is a corresponding entry. Information available in the Windows.edb file can include the original full path, file size, extension, type, and other metadata information.

Windows 8

Windows 8 introduced tiles in the place of the previous Start menu functionality to provide for a greater application in relation to tablet and touch screen computers. In relation to the thumbnail storage, there are similar files as Windows 7, and also additional files of interest to a forensic examiner. As well as the various Thumbcache.db files (32, 96, 256 and 1024), there are also Thumbcache.db files with the following pixel dimensions; 16, 48, and WIDE. As in the previous Windows thumbcaches, the format can be BMP, JPG or PNG thumbnails for the various pixel sizes. In addition, there are now IconCache.db files in dimensions 32, 96, 256, 1024, 16, 48, and WIDE, and also files named; Tilecache.dat, Default, StartView, Logo, and Tickle in the Explorer file. In addition to the Windows Desktop Search Windows.edb database, there is a ModernPhoto.edb database file, which is a potential valuable resource as it includes JPEG thumbnail pictures within the file. The Windows 8 Windows.edb database can be read by Woanware software to display the associated ThumbnailcacheID, path, and other information, now in a table named 'SystemIndex_PropertyStore'. Table 1 summarises the files and information for the various Microsoft Windows thumbnail files.

Windows	thumbnail store	location
95B, 98, ME, 2000, XP, 2003	Thumbs.db	in folder with pictures
Vista	Thumbcache_32, 96, 256, 1024	AppData\Local\Microsoft\Windows\Explorer\
network access	Thumbs.db	in folder with pictures
Windows 7	Thumbcache_32, 96, 256, 1024	AppData\Local\Microsoft\Windows\Explorer\
network access	Thumbs.db	in folder with pictures
Windows 8	Thumbcache_16, 32, 48, 96, 256, 1024, WIDE	AppData\Local\Microsoft\Windows\Explorer\
	Iconcache_16, 32, 48, 96, 256, 1024, WIDE	AppData\Local\Microsoft\Windows\Explorer\
network access	Thumbs.db	in folder with pictures

Table 1 – Windows Thumbnail formats

Review of court transcripts relating to thumbnail evidence

There have been a number of court cases involving thumbnail images. For example, in Jersey Island (UK), [2010] JRC088, the Royal Court (Samedi Division) in the matter of the Attorney General -v- Roberts discusses forensic analysis of a seized computer which located 354 images. 'All of the said photographs were located in the thumbnail caches, as the originals had been deleted.' Furthermore, '[a] later examination of the machine by forensic experts showed that it had been used to search for and download, and in some cases view, a large selection of video files with filenames suggesting that they contained child pornography. However, all of the said material had been deleted by Roberts.'

In R v DM [2010] ACTSC 137 (5 November 2010) (Australia), pictures were located on a seized computer in thumbnail format. The original pictures were not located, and it could not be ascertained whether they had been converted to thumbnails or removed. The examiner was asked in court about the thumbnails, and could confirm when they were created, but not when the original picture had been copied to the computer. It is not stated whether these were windows operating system thumbnails, such as thumbcache or thumbs.db, or generated by other software, such as image editing software.

In United States of America, Plaintiff-Appellee, v Alexander Montagu Hay, Defendant-Appellant [2000] USCA9 526; 231 F.3d 630 (9th Cir. 2000) (24 October 2000) (USA), it is stated that there was evidence

that the defendant had viewed images 'based on the thumbnail images he created when he viewed them on his computer screen as well as the existence of many of the images on his own FTP and web sites.'

In Colbourn v R [2009] TASSC 108 (10 December 2009) (Australia) at Paragraph 29, the matter of Latham (supra) is mentioned and states that in that matter the respondent had stopped undertaking relevant activity approximately ten months prior to a police search of his premises, and 'over 90 per cent of still images were small thumbnails automatically generated by his computer when he downloaded files that he had subsequently deleted. He had forgotten about the thumbnails. I understand that thumbnails cannot be enlarged.' This is also discussed in R v Talbot [2009] TASSC 107 (18 December 2009) (Australia). Referring to Director of Public Prosecutions v Latham [2009] TASSC 101 (12 November 2009) (Australia), the thumbnails mentioned appear to be associated with Google Hello software chat logs.

Further cases mentioning thumbnails, include;

- AAT v R [2011] NSWCCA 17 (21 February 2011) (Australia) discussing seven thumbnail pictures in an email message.
- Director of Public Prosecutions v Kear [2006] NSWSC 1145 (9 October 2006) (Australia), in excess of 5,000 thumbnail images were found in temporary internet cache folders.
- R v Silva [2009] ACTSC 108 (4 September 2009) (Australia), a number of images had been saved as thumbnails and were not able to be enlarged.
- R v. WAF & SBN [2009] QCA 144 (29 May 2009) (Australia), there were 260 thumbnail images of photographs found on a computer.
- Western Australia v Willcott - BC201240239, 'the majority of the files were small thumbnail-sized pictures'.
- Waleed Hassan Rashid Alnaqbi V R - Bc20100835 (Australia), 'when an officer viewed the external hard drive he found a page of approximately 30 thumbnails'
- United States v Riccardi [2005] USCA10 92; 405 F.3d 852 (19 April 2005), 'during forensic examination of the computer, Agent Finch came across images of child pornography in thumbnail form'
- [2006] EWCA Crim 560 (Australia), 'the remaining 2700 still images were saved in a database of a programme called ACDSee. This programme is designed for viewing graphical images and is used by photographers. When opened in the "gallery view", the programme creates "thumbnail" images of the pictures viewed. These would originally have been larger images associated with each thumbnail.'

As outlined, there are court cases in which thumbnail pictures have been evidence. Whilst the matters outlined above have mentioned thumbnail pictures, there is little discussion in the court transcripts in relation to whether additional analysis was undertaken to determine the origin of the thumbnail pictures. As we will outline in the next section, there are software and analysis techniques that can be undertaken which may provide additional information in relation to thumbnail pictures. Whilst this will not always be conclusive, and in many instances may not produce any additional explanatory information, it is worthwhile pursuing additional analysis methodologies to gain a greater understanding where possible.

Current Thumbnail Analysis Software

To undertake research into current thumbnail analysis software, we created test data using Windows Vista (WV), Windows 7 (W7) and Windows 8 (W8) Operating Systems installed into new virtual machines (VM) using VM Player software. A control image of each was preserved as an E01 (i.e. an image file). Each VM (WV, W7, and W8) was then started, and Windows File Explorer was used to browse to the User\Pictures folder and view it as 'Large Icons' to initiate thumbnails being stored in the thumbcache.db files. In Windows 7, the Sample Pictures folder was viewed in Large Icons view, and one picture was opened in Windows Picture Viewer (to enable a 1024 thumbnail to be created). In Windows 8, there is no 'sample pictures' folder, and a folder was created and pictures from C:\Windows\Web\ were copied to the new folder and viewed in Large Icons view. The Windows File Explorer was then used to open a UNC path

to the root C:\ drive where three sample pictures were copied without being viewed (to create associated thumbs.db files). Each VMDK file was then preserved using FTK Imager 3.1.2 and an E01 file was created. Analysis was then undertaken on the six E01's (WV, W7, and W8; 'control' and 'thumbnails'). A range of software was examined, including Technology Pathways ProDiscover, Vinetto, and MiTeC Windows File Analyzer, but these did not provide the ability to examine thumbcache files. The following sections outline software available at the time of this research which provides functionality to examine thumbcache files.

Guidance Software EnCase

EnCase 6.19.6.8 and Encase 7.06.00.172 were used to examine the six E01 files. EnCase 6 parsed thumbs.db and Windows Vista thumbcache.db files using the 'View file Structure' option, and also associated a thumbnail with an existing file. Windows 7 and 8 thumbcache files were not able to be viewed or associated with an existing file with EnCase 6. EnCase 7 parsed Windows 7 and 8 thumbcache.db files and display the ThumbnailcacheID value for each thumbnail.

X-Ways Forensic Analysis

X-Ways Forensic 17.0 was used to examine the E01 files. The 'Specialist-Refine Volume Snapshot-Uncover embedded data' functionality was run across thumb.db and thumbcache files. This resulted in the thumbnails and the associated ThumbnailcacheID value for each thumbnail in thumbcache and thumbs.db files to be parsed and viewable, including Windows 8 ThumbnailcacheID values.

AccessData Forensic ToolKit (FTK)

AccessData Forensic ToolKit (FTK) versions 1.81.6 and 5.1.1.4 were used to examine Thumbcache files and the E01 files. Data carving was undertaken on the entire E01 image, and also on single Thumbcache files. Thumbnail pictures were carved from the Thumbcache files, but without the associated ThumbnailcacheID value for each thumbnail.

ThumbnailExpert

Thumbnail Expert by Dec Software (www.thumbnailexpert.com) provides a capability to examine thumbnails from a wide range of applications, including image viewers, video editors, file managers, and mobile phones. The demonstration version of Thumbnail Expert 2.8 was used to examine the test E01 files mounted as virtual drives using FTK Imager 3.1.2. The thumbcache_idx.db file was located by the software, and the thumbnails and associated ThumbnailcacheID were displayed. The ability to produce a report was also possible. It was also possible to drag individual thumbcache files into the software and view the thumbnails. Windows 8 ThumbnailcacheID values were not always reported for thumbnail files.

Thumbnail Database Viewer 2.0 Free

IT Samples Thumbnail Database Viewer 2.0 (available at http://www.softpedia.com/get/Multimedia/Graphic/Graphic-Viewers/Thumbnail-Database-Viewer.shtml) is a free software to view the contents of thumbnail database files, and will display the contents of Windows 7 thumbcache files (but not Windows 8). There is no reporting option available, and many of the ThumbnailcacheID values contained question-mark values (for example; 968d879af89?????).

Thumbscan

Elinski (2010) produced Thumbscan software to conduct a recursive search of an entire hard drive, including a standard file system and unallocated space, to locate thumbnail cache files, extract embedded thumbnails, and generate a report. The published software is only intended for research-based applications, and limitations of the software include the modification of timestamp information, and therefore, is not recommended to be used for legal purposes (Elinski 2010).

Thumbcache-viewer (Google project)

Eric Kutcher's Thumbcache Viewer is a software that extracts thumbnail images from thumbcache and iconcache database files in Windows Vista, 7 and 8, (available at http://code.google.com/p/thumbcache-viewer/). When used on a running computer, it also provides the functionality of matching a thumbnail image to an existing file (Map File Paths). This is useful for forensic examiners as a forensic image can be mounted as a physical drive with software such as FTK Imager or Mount Image Pro, and then the Operating System run in a virtual machine using software such as Virtual Forensic Computing (VFC). Running the Thumbcache-viewer software within the VM of a forensic image will scan the mounted drive/s and match thumbnail images to existing files. Unfortunately, there is no reporting capability in the software, so manual reports have to be produced. However, the functionality of matching thumbnail images to existing files has potential value in a forensic examination.

There is also Thumbs Viewer software which extracts thumbnail images from Windows thumbs.db files, but the software does not match the thumbnails to existing files, or produce reports, which limits its usefulness in a forensic examination.

Woanware's EseDbViewer

As discussed by ESCForensics (2012) and Morris and Chivers (2011), ThumbnailcacheID entries can be found in Windows.edb files. To examine Windows.edb files, EseDbViewer software (http://www.woanware.co.uk/?page_id=89) by Woanware can be used to read the Windows.edb file, and output this to a comma-separated-value (csv) file, which can be reviewed with Microsoft Office Excel or other spreadsheet software.

WDSCarve

In addition to the research conducted by Chivers and Hargreaves (2011), they also produced software to export the contents of Windows.edb files to a comma separated value file which can be opened as a spreadsheet. WDSCarve includes the ability to scan other files, such as pagefile.sys or hiberfil.sys, and also across a disk image (DD) file and collect data from the entire drive, including unallocated space data. This may locate additional ThumbnailcacheID entries, which may not be present in Windows.edb if they have been deleted (but not yet overwritten on the original media). WDSCarve did not parse Windows 8 edb files though.

Our proposed thumbnail analysis methodology and case studies

Using the forensic computer analysis framework of; Identify, Preserve, Analyse, Present (McKemmish 1999) we outline a process using various tools to undertake analysis in relation to thumbnail files (Figure 1). The process is mapped to the framework of McKemmish (1999) to provide a methodology for forensic practitioners to map to the digital forensic process. This involves the following operational methodology.

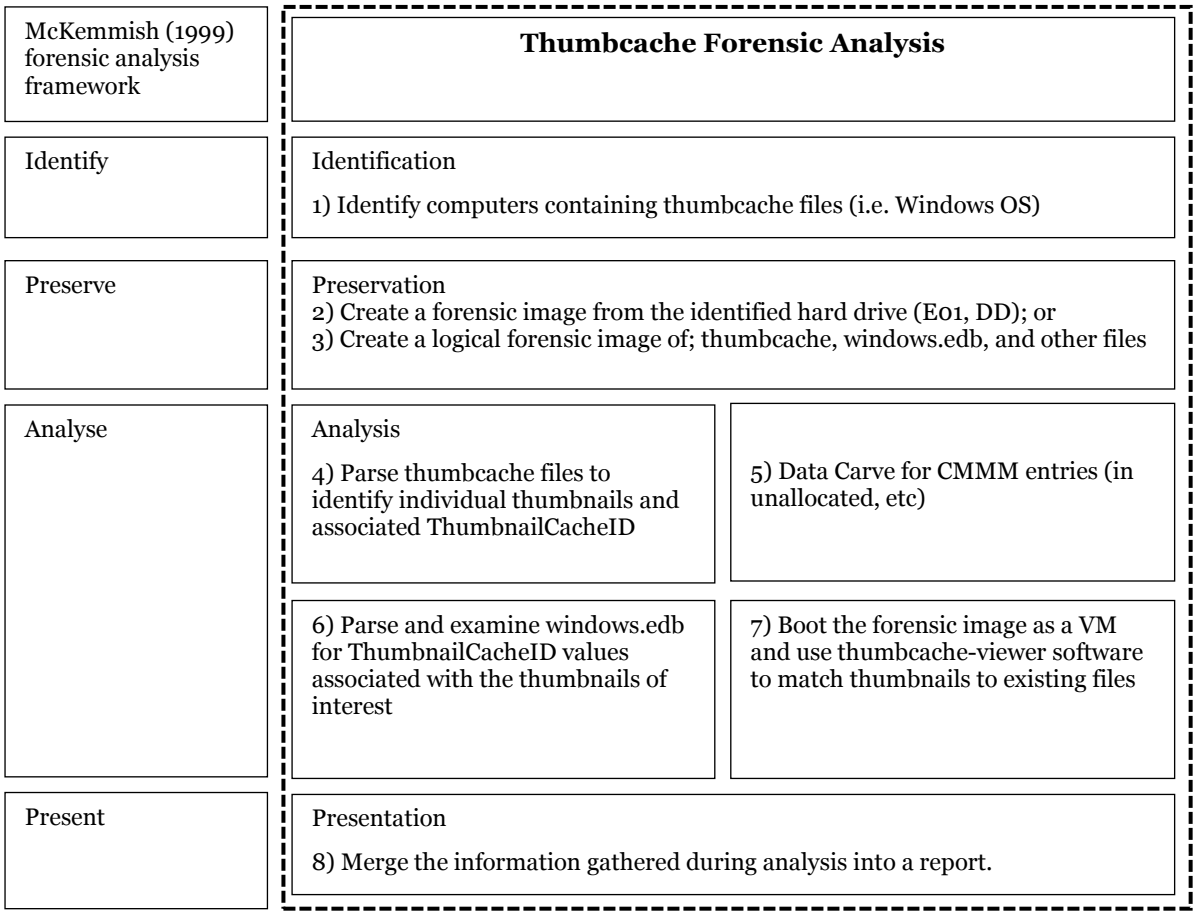

Figure 1 – Thumbcache Forensic Analysis

Identify

The first stage of forensic analysis is the identification of data and potential evidence. In the case of thumbnail analysis, it is preferable to examine the entire file system preserved as a forensic image. If it is not possible to preserve an entire hard drive, thumbcache and other files can be preserved in logical evidence containers. Files such as the thumbcache*.db, thumbs.db, iconcache*.db, windows.edb, MSS.log files, and $MFT, could be identified and preserved in a logical evidence container, for example by using forensic software such as; EnCase, FTK Imager, or X-Ways.

Preserve

The preservation of a hard drive using standard forensic image formats should be undertaken as a physical image of a hard drive (as an E01 or other forensic image type). If it is not possible to preserve a full forensic image (for example, a failing hard drive, or a covert acquisition), then preserve identified files into a logical container, such as an L01, AD1, or CTR format.

Analyse

Currently, no one piece of software provides complete functionality to conduct thorough thumbnail analysis. The use of multiple software tools is necessary to conduct full analysis. Steps 4-7 are not necessarily undertaken in order, and not all steps need to be applied in all cases. Steps 4-7 involve the following examples;

(4) Use EnCase 7, X-Ways, or ThumbnailExpert to identify the thumbnail images within Thumbcache.db files and associated ThumbnailcacheID entries relevant to an investigation.

(5) Use forensic or data recovery software to locate Thumbcache.db file remnants within unallocated space or other locations within a forensic image, for example, searching for the header of thumbnail entries; "CMMM". As discussed by Podhradsky and Streff (2011), data remnants can remain after common sanitization techniques are deployed, and hence historical thumbcache data may be present.

(6) Use WDSCarve or EseDbViewer to convert Windows.edb files to a spreadsheet and examine the data to identify ThumbnailcacheID entries associated with the thumbnails relevant to an investigation.

(7) Use FTK Imager or Mount Image Pro (MIP) and Virtual Forensic Computing (VFC) to create a virtual machine of the forensic image. Then run Thumbcache-Viewer software within the VM and open the thumbcache entries. Use the 'Map-File-Path' functionality to locate any existing files and identify the ThumbnailcacheID entries associated with the relevant thumbnails.

Once the original filenames and paths are known for relevant thumbnails, or an existing file which matches a thumbnail is identified, additional analysis can be undertaken to provide further information. This could include information from link files, registry files, MFT entries, prefetch, and other sources (the scope of this additional analysis is too broad to explain fully in this paper).

Presentation

The next stage is to present the information located in the analysis steps. This could comprise; (1) the location of a thumbnail picture with no additional information, (2) a thumbnail picture which matches an existing file, or (3) a thumbnail picture with associated Windows.edb information, in a report.

Case Studies

This research was initiated from a real-world law enforcement investigation involving thumbnail pictures located in thumbcache files. Some of the thumbnails of interest had associated picture files, others had entries in the Windows.edb (Steps 4, 6 & 7 were applied in this case). Research was also undertaken using the Digital Forensic Corpora sample image files (Garfinkel et al. 2009) and it was possible to locate matching Windows.edb entries for many of the thumbnail pictures located in thumbcache.db files (Steps 4 & 6). Carving for CMMM entries (Step 5) was also conducted on the Digital Forensic Corpora sample image files, and it was possible to export the matching CMMM entries and associated data to a file and view this with Thumbnail-Expert software to parse the thumbnails and ThumbnailcacheID values for the carved data. The thumbcache analysis process (steps 4 & 6) was also applied to test data from Quick and Choo (2013a; 2013b; 2014) and Quick, Martini and Choo (2014) and it was possible to locate Windows.edb entries for associated thumbnail pictures in Thumbcache.db files, including the image (E01) files where the original pictures had been erased using erasing software. The thumbcache analysis process has also been used in a variety of subsequent real-world investigations and important information has been located matching Windows.edb entries to thumbcache thumbnails, and match thumbnail pictures to original files (Steps 4, 6 & 7).

The methodology outlined can be applied in investigations involving insider threats whereby a suspect has sold pictures of intellectual property to a competitor and has erased the original picture files. In a case such as this, there may still be thumbnails stored in the thumbcache files, which alone may not be enough to initiate legal proceedings. However, if information is located in the windows.edb file to identify the camera details or original file locations, legal proceedings may be possible.

Our Visualisation and Thumbcache Analysis Software Prototype

There is currently no software which provides the ability to read from thumbcache files and also source relevant information from the Windows.edb in one package. The current process requires practitioners to spend considerable time to manually match up the various sources of information and compile a report. As thumbcache files can contain many thousands of thumbnails, and the Windows.edb file can contain

potentially hundreds of thousands of entries, the manual process can be extremely time consuming, whereas a software solution has the potential to parse and match information in a timely fashion.

Using the proposed thumbnail analysis methodology, we designed a software prototype to undertake the process of parsing thumbcache files and matching the ThumbnailcacheID values to entries in Windows.edb files. The software enables an examiner to view the contents of thumbcache.db files, reporting the ThumbnailcacheID value for each stored thumbnail, and provides a visualisation of the thumbnails. The user can then load in the associated and parsed Windows.edb file (in CSV format) and the software will match ThumbnailcacheID entries with the stored thumbnail. The software is also able to produce a report, including the additional information available from within the Windows.edb file, such as the original filepath, dates and times, and importantly, the camera type and other metadata (when stored) which may identify a user or original source of the picture. Figure 2 details the internal logic and processes undertaken in our prototype software. Highlighted in the center of the diagram (green) are the comparison and data matching steps. These are unique to our prototype software, and serve to streamline the (currently manual) data matching process, which contributes to a major gap and is lacking in current software offerings.

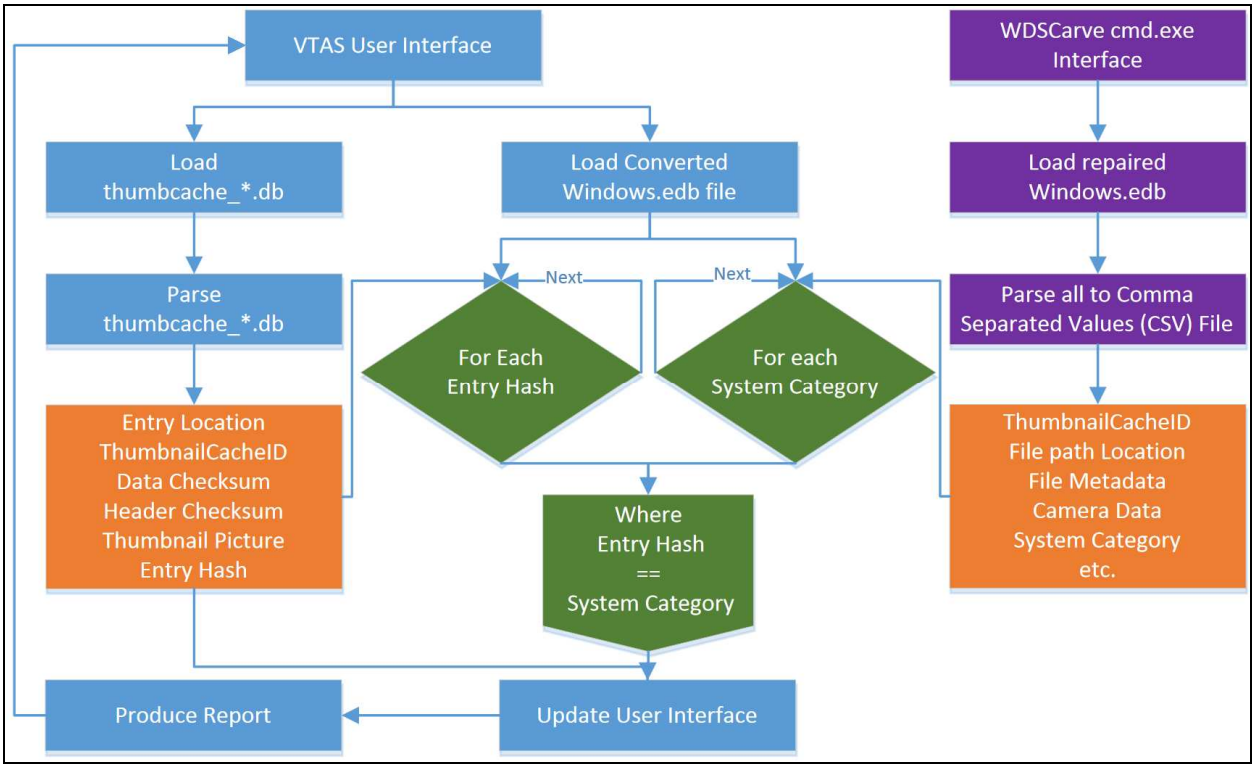

Figure 2 – Block Diagram of Visualisation and Thumbcache Analysis Software (VTAS)

An example screenshot from the prototype is included in Figure 3. The software prototype merges the information from various disparate sources to provide a much greater understanding of the background and history of picture files. In a legal environment, this information may be invaluable to prosecution, defense, or legal counsel.

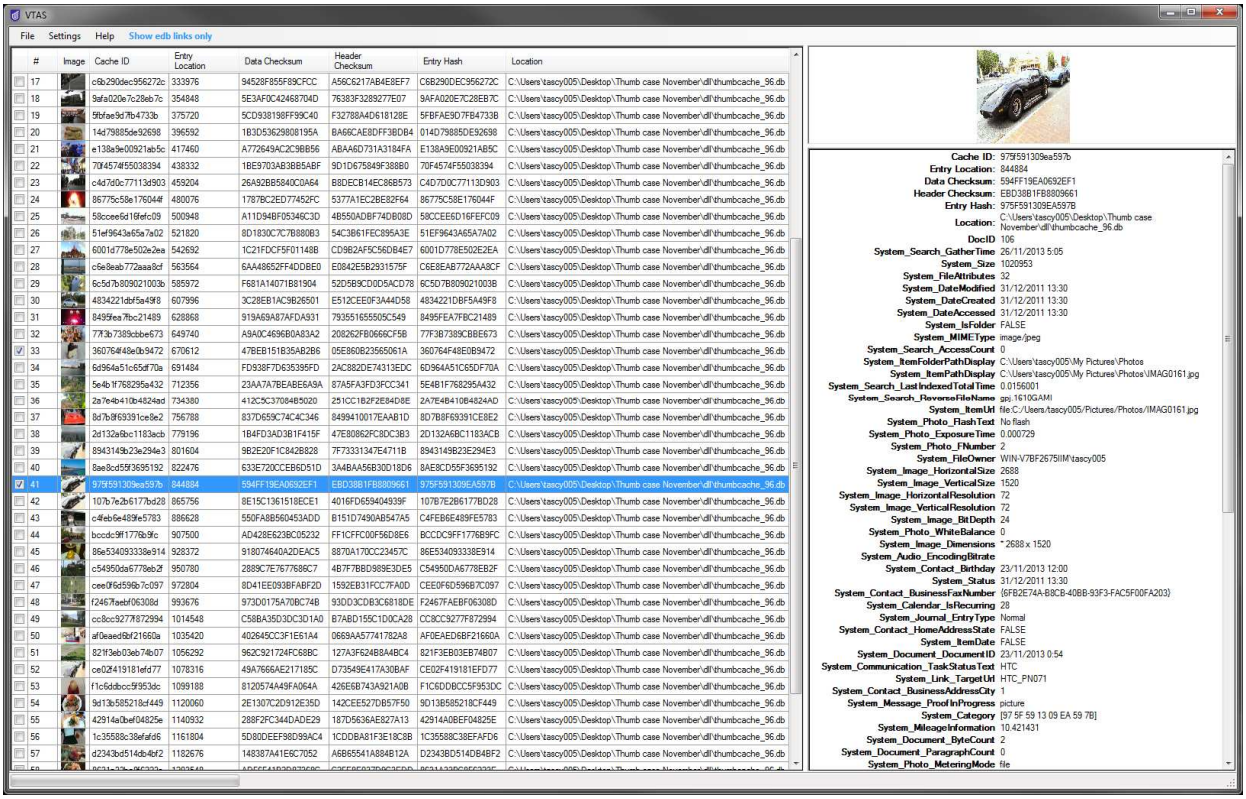

Figure 3 – Screenshot of software application developed to apply proposed method

We ran our software over the six E01's ('control' and 'thumbnails' for WV, W7 and W8), and were able to extract ThumbnailcacheID values and the thumbnails from Vista, W7 and W8 caches. The software matched ThumbnailcacheID values to existing files, and also reported information from the Windows.edb where possible. Table 2 outlines a summary of the capabilities of the forensic and other software examined in the previous section, including our software prototype.

Software	Summary	Extracts ThumbnailcacheID with image	Match ThumbnailcacheID to picture	read windows.edb	matche thumbnailID to windows.edb
EnCase 6	View Thumbs.db and Vista thumbcache associating thumbnail with existing file	✓ (Vista)	✓ (Vista)	✗	✗
EnCase 7	display W7 and W8 thumbcache thumbnails with ThumbnailcacheID	✓	✗	✗	✗
X-Ways	thumbnails and ThumbnailcacheID extracted	✓	✗	✓	✗
FTK 1.81.6 and FTK 5.1.1.4	data carve used to extract images, but not ID	✗	✗	✗	✗
ThumbnailExpert	thumbnails and ThumbnailcacheID extracted	✓	✗	✗	✗
Thumbnail Database Viewer	Thumbnails extracted	✗	✗	✗	✗
Thumbcache-viewer	extracts information from Thumbcache and matches to exisiting files	✓	✓	✗	✗
EseDbViewer	converts Windows.edb to CSV	-	-	✓	✗
WDSCarve	convert Windows.edb to CSV	-	-	✓(not W8)	✗
Our prototype	identifies thumbnails and ThumbnailcacheID, matches to edb entries	✓	✗	✗	✓

Table 2 – Software comparison

Conclusion

There are a range of court cases and forensic investigations that have relied upon the presence of thumbnail pictures contained within Microsoft Windows operating system files, such as thumbcache.db and thumbs.db. In the cases reviewed, the thumbnail image has been the evidence presented to a court. As we have outlined, by conducting further analysis it is sometimes possible to locate additional information relating to thumbnail pictures. This includes being able to link a thumbnail to a picture file on storage media, and also locating information relating to the original file used to create the thumbnail including the full path and original file name. The additional information may be crucial in insider threat investigations, where the original pictures have been erased.

In this paper, we demonstrated that our proposed operational methodology for thumbcache analysis was able to identify files and file information associated with thumbnails, including timestamps and other metadata where this is available. In our research, when the methodology to examine several seized devices in a real-world law enforcement forensic investigation, we were able to provide additional information for many of the identified thumbnails. In subsequent case studies, we applied our methodology in a range of other law enforcement forensic cases and we were able to identify information critical to the investigations. In one instance, camera make and model details were included in the Windows.edb file, and this provided valuable information as part of an ongoing investigation.

Our software prototype was able to extract ThumbnailcacheID values and thumbnails from our case study data and a visualization of the thumbnails with associated Windows.edb data was provided. Benefits of our methodology include the bringing together of additional information which can provide greater understanding relating to thumbnail pictures, such as the path and location of the original picture, and associated metadata from within picture files, even though the original file may not be present.

Future research opportunities exist to expand this research to other operating system's thumbnail stores, such as; Apple Mac OSX, Linux, Apple iOS, Google Android, and Windows Phone operating systems.

REFERENCES

Casey, E. 2002. *Handbook of Computer Crime Investigation: Forensic Tools and Technology*. London: Academic Press.

Chivers, H., and Hargreaves, C. 2011. "Forensic Data Recovery from the Windows Search Database," *Digital Investigation* (7:3-4), pp. 114-126.

Elinski, J. 2010. "Thumbscan: A Lightweight Thumbnail Search Tool." Retrieved 29 March, 2013, from https://ritdml.rit.edu/bitstream/handle/1850/13297/JElinskiThesis11-18-2010.pdf?sequence=1

ESCForensics. 2012. "Analyzing Thumbcache." Retrieved 2 March, 2013, from http://escforensics.blogspot.com.au/2012/11/analyzing-thumbcache.html

Garfinkel, S., Farrell, Roussev, and Dinolt. 2009. "Bringing Science to Digital Forensics with Standardized Forensic Corpora, Dfrws 2009, Montreal, Canada." Retrieved 9 September, 2013, from http://digitalcorpora.org/corpora/disk-images

Hurlbut, D. 2005. "Thumbs Db Files Forensic Issues." *AccessData Training Document* Retrieved 23 February, 2014, from http://marketing.accessdata.com/acton/attachment/4390/f-00ab/0/-/-/-/-/file.pdf

McKemmish, R. 1999. "What Is Forensic Computing?," in: *Trends and Issues in Crime and Criminal Justice, Australian Institute of Criminology*. pp. 1-6.

McMillan, J.E.R., Glisson, W.B., and Bromby, M. 2013. "Investigating the Increase in Mobile Phone Evidence in Criminal Activities," in: *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. IEEE, pp. 4900-4909.

Morris, S., and Chivers, H. 2011. "An Analysis of the Structure and Behaviour of the Windows 7 Operating System Thumbnail Cache," *Proceedings from 1st Cyberforensics Conference*, University of Strathclyde, Glasgow, UK.

Parsonage, H. 2012. "Under My Thumbs – Revisiting Windows Thumbnail Databases and Some New Revelations About the Forensic Implications." Retrieved 29 March, 2013, from http://computerforensics.parsonage.co.uk/downloads/UnderMyThumbs.pdf

Podhradsky, A.L., and Streff, K. 2011. "Testing Data Sanitization Practices of Retired Drives with the Digital Forensics Data Recovery Project," in: *Proceedings of 17th Americas Conference on Information Systems, AMCIS 2011*. Detroit, Michigan, USA.

Purcell, D., and Lang, S.-D. 2008. "Forensic Artifacts of Microsoft Windows Vista System," in: *Intelligence and Security Informatics*. pp. 304-319.

Quick, D., and Choo, K. 2013a. "Digital Droplets: Microsoft Skydrive Forensic Data Remnants," *Future Generation Computer Systems* (29:6), pp. 1378 - 1394.

Quick, D., and Choo, K. 2013b. "Dropbox Analysis: Data Remnants on User Machines," *Digital Investigation* (10:1), pp. 3-18.

Quick, D., Martini, B., and Choo, K.-K.R. 2014. *Cloud Storage Forensics*. Syngress: An Imprint of Elsevier.

Stewart, B. 2007. "Forensic Implications of Windows Vista." Retrieved 29 March, 2013, from http://whereismydata.files.wordpress.com/2009/09/forensic-implications-of-windows-vista.pdf