UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA

MALIBU MEDIA, LLC Plaintiff, v. KELLEY TASHIRO Defendants	Case No. 1:13-cv-00205-WTL-MJD

DECLARATION OF DELVAN NEVILLE

1. My name is Delvan Neville. I am over the age of 21 and competent to execute this Declaration.

2. I am the owner of Amaragh Associates, LLC, a digital forensics company specialized in BitTorrent investigation. I am an ACE (AccessData Certified Examiner) as well as the author of a BitTorrent monitoring suite, EUPSC2k. Before entering the field, I have engaged in freelance computer repair and troubleshooting since the late 1990s, including recovering lost data from storage devices.

3. On March 10th, 2014, I received a Western Digital disk drive, in a Rocketfish external USB enclosure, shipped to me from the Defendant by UPS (tracking number: 1Z2W97W20326835411). The serial number for this hard drive is WMAD14522138. I created a forensically sound image of the hard drive using a Wiebetech Forensic UltraDock v5 write-blocker and AccessData FTK Imager 3.1.4.6. I imported this image into a new case in Forensic Toolkit 5.2.1.2.

4. I have read the declaration of Patrick Paige regarding the analysis of this hard drive. In it, he contends that "Malibu Media, LLC's copyrighted content could have been deleted from the drive during Defendant's mass erasure" *See Doc 76 at 28.*

5. I concur with Mr. Paige's finding that there were many files and folders deleted on 22 December 2013. Specifically, one root directory was deleted, "N.C.Tashiro", and subsequently all other child folders and files were deleted.

6. I dissent from Mr. Paige's findings as to whether any of the deleted files could be Malibu Media, LLC's copyrighted content. To explain the cause for my dissention, some background on how files are stored and recovered is necessary first.

Background

7. The file-system present in the sole partition on this disk is the New Technology File System (NTFS). NTFS tracks files and directories in a Master File Table (MFT). The MFT contains two basic varieties of records: file records and directory records.

8. A directory record includes attributes (among others not relevant to this discussion) such as a

pointer to its parent directory (i.e. the folder it is contained within), the time and date the directory was first created, last modified, last accessed and when the record itself has been modified last, as well as a flag identifying whether it has been deleted. If the directory contents are small[1], a list of all files and sub-directories that it contains (with pointers to the appropriate file & folder records) are located directly in the MFT. If it is large, the list of contents are stored elsewhere on the disk and the MFT merely includes a pointer to that location.

9. File records similarly contain a pointer back to the parent directory record, file creation, access, record and modification times, and a flag identifying whether the file is deleted. As above, if the file is small, the contents of the file itself are stored in the MFT. If it is large, the contents are stored elsewhere on the disk and the MFT merely includes a pointer to that location.

10. When a user or an automated process deletes[2] a file:
    a. The file record in the MFT is flagged as deleted. *Note: the rest of the file record remain intact.*
    b. If the file contents were stored outside of the MFT (typically they are), the clusters that held the data are flagged as available. *Note: The file contents are not over-written, merely marked as "okay to overwrite with another file"*
    c. The parent directory is updated by removing the file from its listing of contents.

11. Deletion of a directory proceeds similarly: the directory record is marked as deleted (but is otherwise intact), the clusters that held the directory contents (if stored outside the MFT) are marked as available, and its parent directory is updated by removing it from the list. All files and folders that were contained in that folder are also deleted in the same manner.

12. So long as the clusters[3] that contain the file have not been over-written by newly created files, deleted files may still be recovered from a hard drive in a few key ways.
    a. Although the file system ignores file records marked as deleted in the MFT, software designed for recovery can read these file records and recover all attributes associated with a file as well as locate its location on disk, provided the file record has not yet been overwritten.
    b. Even if there is no longer a file record in the MFT, the data may still be recovered from the disk by "carving": searching through the hard drive for specific series of bytes that identify the type of file one seeks to recover. For instance, the start of a *.avi file begins with "RIFF".
    c. If the directory record is no longer present or the file is only recoverable by carving, the file is an *orphan*: the file is recovered but it is unknown what directory name it used to reside in.

13. Even when parts of the file has been overwritten, video files may still be playable to some extent.
    a. VLC Media Player can often play broken or damaged AVI files so long as enough of the beginning of the file remains intact.
    b. ffmpeg can extract individual screen images from many damaged video files that VLC

1 By default, both the file record and the file contents cannot total more than 1,024 bytes if the file contents are to be stored in the MFT.

2 The default action in Windows after a user chooses to delete a file is actually to "move" the file to the Recycle Bin, a special directory meant to give an additional level of protection against accidental deletion. Unless the file is very large or the user overrides this behavior, the deletion process does not actually begin until the Recycle Bin is "emptied".

3 The smallest unit of space to be addressed by a hard drive is a sector. However, to speed up access times, the smallest unit of space allocated by the file-system are clusters, which are groups of sectors.

cannot play, though it handles Quicktime (*.mov) files poorly and does not support video protected by Digital Rights Management (DRM).

c. Defraser is able to recognize and extract video and audio fragments not only based on file type signatures (like those used when "carving") but also by the signatures of specific video and audio codecs used within those files.

Analysis

14. Upon my examination of the image, I found that all of the files recorded in the MFT as deleted had creation dates no recent than 24 October 2011. The most recent modification date was 19 September 2012 for a temporary file produced by the operating system. The only files created more recently were attribute files[4] created by the operating system as part of the act of deletion on 22 December 2013.

15. Since the 22 December 2013 deletion event, only *a single file* has been created or modified in the interim: a 129 byte "desktop.ini" file, which is automatically created by the Windows operating system to store user preferences for how to display a directory.

a. Because of its small size, this file's contents were stored directly in the MFT. Thus, while it is possible it over-wrote part of a single deleted file or directory record in the MFT, no file contents on the disk would have been overwritten.

b. As this file was created on 17 February 2014, the MFT record number now occupied by this file would have still contained its previous data when examined by Mr. Paige.

16. As there had been no new writes to the hard drive following the deletion, any copyrighted media present on the drive before the deletion event would have remained intact when examined by Mr. Paige.

17. As no writes outside of the MFT[5] have occurred in the interim between the deletion and my own imaging of the hard drive, the file contents of any copyrighted media present at that time would remain intact on the image I collected. Further, the .torrent[6] files associated with the 18 works Defendant is alleged to have downloaded would also remain intact on this image had they been deleted on 22 December 2013.

18. I conducted a search for copyrighted Malibu Media, LLC works or files associated with infringement on those works.

a. I recovered the contents for all file records (deleted or intact) associated with .torrent files and video files

b. I carved for .torrent files as well as a wide variety of video formats located anywhere on the image: slack space, unused space, unallocated space as well as inside existing files.

c. I exported all unused/unallocated space and slack space from the image, and analyzed these for audio and video fragments with Defraser version 1.3.5 (32-bit) for various containers and codecs used for digital video: 3GPP/QT/MP4, ASF/WMV, AVI/RIFF, MPEG-1/2 Systems,

4 Attribute files are part of the file system and are not directly accessible to the user. Deleted attribute files from 22 December 2013 are Recycle Bin files used to record the original location for four .torrent files that were deleted that day. The actual .torrent files themselves have creation and last access dates of 7 June 2009.

5 If by chance that single file record overwrote a record of evidentiary significance, I would still recover it during carving, I would merely be missing metadata like the file name and the access/modification/creation times.

6 A .torrent file can in theory fit inside the MFT, but only for torrents with a few very small files. A .torrent uses a few hundred bytes or more to describe the names of files and the trackers to contact, plus 20 bytes per piece. For instance, the .torrent file for the work "Want You", with an infohash of 0CE92EF780541EB7BFFD89D9ED528733B3D83B16, is 5,429 bytes long

MPEG-1/2 Video, MPEG-4 Video/H.263. I then exported all child media objects as independent files.

d. I used ffmpeg version N-59852-g785dc14 to extract screen images for every 5 seconds of video from all potential media files collected in steps a, b and c.
e. I examined all of the resulting captured images for stills from Malibu Media, LLC's works
f. I used VLC media player version 1.1.11 to examine extracted media files for which ffmpeg is not 100% reliable at analyzing (3GPP/QT/MP4).
g. None of the .torrent files nor video files recovered were for Malibu Media, LLC's works.

19. Further, the .torrent files that had records present in the MFT (deleted or intact) had creation dates ranging from 2006 to 2009 at the most recent, predating all of the copyrighted works in question.

20. Torrent files that were only recoverable by carving have, by definition, no associated MFT entry present any longer. However, .torrent files often contain an internal creation date field that specifies when the original seeder created the torrent. Where present, these creation dates range from 2005 to 2009, which corroborates well with the range of torrent activity indicated by the MFT.

21. Of the 111 BitTorrent files still listed in the MFT, 107 are orphans that were deleted some time ago (long enough that new files or folders had been created after their parent folders were deleted). Thus, only 4 of the BitTorrent files in question were deleted during the 22 Dec 2013 deletion. All four of those files were previously located in "K:\N.C.Tashiro\Local Settings\Temp\".

22. Finally, I did a case-insensitive text search for the title of each of the 18 works in question across the entire image, allowing any character between words (e.g. "A.Girls.Fantasy" or "a-gIRlS fantasy" would both results in a match). I exported the context surrounding each result and reviewed each of them, confirming that each result was unrelated to Malibu Media, LLC's works.[7]

23. Satisfied that the search for evidence of the copyrighted works had been exhausted, I sought the cause of the deletion that occurred on 22 December 2013. Although there are parts of a Windows installation present on the disk image, examination of the most recent SAM registry file confirms no user has logged into it since 12 January 2011. Without conducting an examination of an image of the machine from which the deletion was started, I cannot say for certain who or what initiated the deletion.

24. In summary, I found no evidence that any of Malibu Media, LLC's works nor .torrent files related to them were ever present on this hard drive. The most recent creation, modification and access dates for BitTorrent related activity on the hard drive predate the earliest of the "hit-dates" reported in the original complaint. Although many files and folders were marked as deleted on 22 Dec 2013, a thorough examination of the MFT and the serendipity that no users created or modified files following that deletion demonstrates that had any relevant videos or .torrent files been present before the 22nd, they would have remained present when the hard drive was imaged the following day[8].

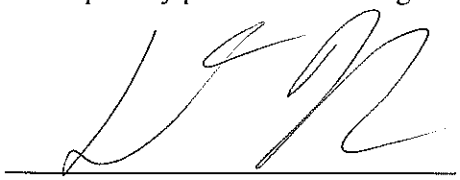
7 Because the works include titles as generic as "Daydream" and "Farewell", everyday documents that happened to use the same words as the title also matched the search.

8 Presumably, Mr. Paige would have reported such evidence had he found such during his analysis.

Further declarant sayeth naught.

Pursuant to 28 USC Sec. 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and based upon my personal knowledge.

Executed March 25, 2014



Delvan Neville
Amaragh Associates, LLC
570 NW Walnut Blvd
Corvallis, OR 97330-3849