Assignment 6: Chanakya Gaur: Recycle Bin

1. What is the Recycle Bin on a computer running a Windows operating system?

Recycle Bin is the location where files deleted by the user are stored.

2. What are the two ways a user can delete a file without sending it to the Recycle Bin?

* Select the file and press shift+delete
* Press shift and then drag the file to the recycle bin.

3. What is the “Machine Active Time Bias” as this term is applied to files that are in the Recycle Bin?

Difference between timestamp of the deleted file and the actual time of the time zone where the files were deleted is Machine Active Time Bias

4. The name of the folder that contains the deleted files varies with the type of file system upon which the operating system is installed. What are the names of these folders that are associated each of the FAT and NTFS file systems?

* Recycled - FAT
* Recycler - NTFS

5. What is the INFO2 file, and how is it different when created on the FAT file system vs. the NTFS file system?

The INFO2 file maintains information about the deleted file. NFO2 file maintains a 280-byte record containing the long filename and the date and time the file was deleted in FAT.

The INFO2 file maintains a 800-byte record that contains the longfile name, a long Unicode filename, and the date and time the file was deleted in NTFS.

6. When a file is deleted, on an NTFS file system, a record of that deleted file is maintained within the Recycler folder in the following format.

D <drive where the file was originally located> <number of the deletion> . <file extension of the original file>

(p. 608)

What is the name of record file for a Word file (.doc) that was originally on the “e” drive, and was the 13th file to be deleted?

De13.doc

7. A ‘deleted file’ can be removed from the Recycle Bin in two ways. It can be restored to its original location, or it can be ‘deleted’ from the Recycle Bin. Regardless of how a ‘deleted file’ is removed from the Recycle Bin, what happens to the record of that deleted file within the INFO2 file?

The placeholder gets deleted, and the drive letter gets deleted from the INFO2 file.

8. What is contained within the Forensic Toolkit (FTK) “Orphan” folder?

The FTK Orphan folder contains the folders and files whose parent folder cannot be determined.

9. Open the Washer.E01 image file with Forensic ToolKit. Navigate to the Root/Recycler directory. Notice that the name of the directory is “Recycler”. Also notice that the file system is NTFS. Notice which sub-folders are present, and which ones are absent. Recycle Bin folders (the sub-folders to the Recycler folder) are created when the first item for that user (that SID) is deleted. There are no sub-folders associated with SIDs 1000, 1001, and 1002 because these users most likely did not delete any files. (See the picture below)

What is the original name of this file, before it was deleted?

DCP\_1430.JPG

Where was this file located when it was deleted?

C:\Documents and Settings\Administrator\Desktop

When was it deleted if the deletion occurred in the Eastern Time Zone, during Daylight Savings Time?

9:32:12 PM Eastern Daylight Savings Time on 8/3/2007.

10. Assume the Dc2.piz file is associated with illegal software that is used to validate stolen credit cards (in other words, it is software that helps prove the stolen credit cards still work). If you were going to send a subpoena to Yahoo in order to find out more information about the software developer, what Yahoo account would you get the subpoena for?

Arpan4017@yahoo.com

11. If we assume the DCP\_1430.JPG was the last file to be `deleted’ and sent to the Recycle Bin, how many files were removed from the Recycle Bin (either by being restored or being deleted permanently)?

Dc1.<extension unknown>

Dc3.<extension unknown>

Dc4.<extension unknown>

12. What is a Thumbs.db?

The Thumbs.db is a mini-database of JPG images which is used to support the viewing of the contents of a directory.

13. On a Windows 2000 FAT32 partition, the JPG graphic thumbnail pictures are stored within a Thumbs.db. Where are these JPG graphic thumbnail pictures stored on a Windows 2000 NTFS partition?

On a Windows 2000 NTFS partition, the graphic JPG thumbnail pictures are stored within alternate data streams.

14. On an operating system that uses the Thumbs.db for storing thumbnail images of files, is the thumbnail image deleted when the original corresponding file is deleted?

No

15. In the case of Power Point and movie files, what will the thumbnail image show?

The thumbnail image will show the first Power Point slide or first movie frame.

16. Find the file named “Cross Eyed.bmp”. It is a picture of a cross eyed cat, as shown below. Assume the “Cross Eyed.bmp” file is an illicit picture. Is there any Thumbs.db evidence that suggests this picture was viewed by a user?

Yes.

17. Examine the Mantooth.E01 evidence file with FTK. What are the names of the two files for which there is evidence that someone attempted to print them?

The two files are prescription.gif and nationaltall.bmp which were attempted to be printed on port LPT1.

18. What is an EMF file and how does it relate to a spool file?

An Enhanced Metafile inside a spool file represents the individual pages that were sent to a printer.

19. What is a “shadow file” (SHD) as this term relates to spool files?

An SHD file is a small administrative-type file that is created when a spool file is created. It contains information about the print job and printer it was sent to.

20. FTK classifies SHD files as “Unknown Types.” Find the SHD file associated with the “nationaltall.bmp” file and review the file content with the FTK HEX view tool. Based on the information that you find, what make and model of printer was being used?

Epson Stylus Photo RX420

21. What is an “alternate data stream” and why is it included in an NTFS file system?

An alternate data stream is an NTFS feature that allows the file system to be compatible with the Macintosh Hierarchical File System (HFS).

22. On a Windows operating system, go to the “Run” feature on the Start menu and run the following command “notepad C:\test.txt:secret1.txt”. [If you are working on a remote computer, you need to use a location where you have Administrator rights. You may have to modify the command to use the path of the new location. For example, the new command might be similar to this. What message do you get?

Cannot find the f:\test.txt:secret1.txt file

23.Use FTK to find the two (2) ADS files associated with the file named “readthis.txt”. What does one of the files state is the password for the “readthis.txt” file?

Supercallifragilistic

24. What is the Windows Prefetch?

The Windows Prefetch monitors applications as they are initialized in the first 10 seconds of startup for that application. Prefetch records the loading order of files and uses this information optimize the initialization of that application for the next time it is run. Prefetch loads the required files into memory in an optimized order so the booting/initialization of individual program is faster.

25. View the Clampet18.aff evidence file with FTK. There are four (4) ways that Prefetch can be configured (see p. 677). What is the Prefetch configuration setting for the Clampet18.aff evidence file? (Hint: You will need to use Registry Viewer as described on p. 683).

Boot and Application Launch Prefetching is enabled

26. View the Clampet18.aff evidence file with FTK. Navigate to the Prefetch record for Internet Explorer (IEXPLORE.EXE-27122324.pf) and answer the following questions

What is the execution path for Internet Explorer?

\device\harddiskvolume1\program files\internet explorer\iexplore.exe

How many times ahs this program been executed/run?

84

When was the last time this program was executed/run?

10/16/2009, 7:46 AM

27. Within the Preftech folder for the Clampet18.aff evidence file, there is a file named “Layout.ini”. What is the purpose of the Layout.ini file?

The Layout.ini file is a special file that tracks the order of loading by the application of the specific areas of the drive which that application needs in sequence.

28. How can the Layout.ini file be used to detect programs that have been deleted?

The Layout.ini file records the programs that have been executed on the computer. If there is a record within the Layout.ini file for a program that is not installed or found on the computer, this suggests that the program was once installed, or at least the program was once able to be executed from the computer.