Windows Recycle Bin Intro

Sandy (3D)

refer to CHFI v9 Module 05. Defeating Anti-forensics Techniques

Outline

- What happens when files are deleted in Windows
- How Windows Recycle Bin work
- How to deal with damaged files/recycle bin

What happens when files are deleted in Windows

- FAT
  - The OS replace the first byte of *Directory Entry* of deleted file w/ 0xe5
  - The corresponding cluster of that file in FAT is marked as unused, although it will continue to contain data until is it overwritten
- NTFS
  - The OS mark the file as deleted in the *Master File Table(MFT)*
  - The cluster allocated to the deleted file are marked as free in $Bitmap ($Bitmap file is one of entry in MFT. It records all used/unused clusters)
  - The OS now notice those empty clusters are available for storing new file
  - The deleted file can be recovered if the space is not allocated to other file

How Windows Recycle Bin work

Windows OS	Windows 98 and prior	Windows 2000, NT, XP	Windows Vista and later
File System	FAT	NTFS	
1.Actual location of recycle bin	Drive:\RECYCLED	Drive:\RECYCLER	Drive:\$Recycle.Bin
2.The directory to store files in recycle bin	Dumped into single Drive:\RECYCLED directory	Categorized into sub directories based on user's Windows Security Identifier(SID) [ex.] Drive:\{recycle bin dir}\S-1-5-21-XXXX…	
3.How to store files in recycle bin	(1) Renamed as D<original drive letter of file><#>.<original extension> [ex.] De7.doc (A .doc file was deleted from E drive, it is the 8th file received by recycle bin) (2) The information about the deleted files is stored in database file called INFO2 a. Locate in the directory to store files in recycle bin b. Contains original file name, original file size, date and time of deletion, …etc.		(1) Renamed as $R<#>.<original extension> (2) The corresponding metadata file is created at the same time: $I<#>.<original extension>, contains original file name, original file size, data and time of deletion (3) <#> represents a set of random letters and numbers, example: $RHEP7WW.txt $IHEP7WW.txt

How to deal with damaged files/recycle bin

- Damaged INFO2 file (prior to Windows Vista)
  - No files appear in the recycle bin
  - Solutions
    - (not tested yet) Delete the hidden INFO2 file and restart Windows to re-create INFO2 file
    - Restore using data recovery tool
- Damaged files in recycle bin
  - No files appear in the recycle bin
  - Solution
    - (not tested yet) Create a copy of Desktop.ini file in the recycle bin folder and save it in another folder. Then delete all files in the recycle bin. Finally, restore the Desktop.ini file to the recycle bin folder. If the Desktop.ini is not present or damaged, re-create by adding following info to a blank Desktop.ini file: [.ShellClassInfo]CLSID={645FF040-5081-101B-9F08-00AA002F954E}

How to deal with damaged files/recycle bin (Cont.)

- Damaged recycle bin
  - Files can be deleted, but the content of recycle bin cannot be viewed, and the “Empty the recycle bin” command is unavailable
  - Solution
    - Delete the Drive:\{recycle bin dir} folder and restart
      (Note) This action will delete all files reside in recycle bin

Thanks for listening