CY2002 Digital Forensics

Assignment 04

Submission Deadline = 23 October 2024, 23:59:59

Deliverables + Guidelines

Q no 1)

a) Create a file ADS_YourRollnumner_Name.txt with resident data inside, Append Alt stream to file by including your name as hidden data and name the alt stream file as HIDDEN01_yourRollNumber
   i. Append second file as Non-resident alt stream to your file as HIDDEN02_yourName
   ii. Add non-resident data to file (HIDDEN02_yourName) by inserting your name, course name, university details, and any specialization details that is unique for you.

b) Create EFS_YourRollnumner_Name.txt, add resident data, encrypt this file with EFS.

Check MFT records for each case above

Highlight all attribute IDs, attribute length (size), file names, resident/non-resident flag, data runs, decode data runs and identify Alt-streams.

For part b, EFS encrypted file, highlight attribute 0x100 with FEK and FEKI parts clearly with labels. (Use WinHex for labelling, do not use Active@Undelete for this part)

Check $Bitmap entries against file for extra credit. (Optional)

0xB0 = $Bitmap: This file keeps track of all the clusters of the volume and whether or not each cluster is currently in use. That's how we can quickly determine how much free space you have. We just ask $Bitmap.

See also at https://whereismydata.wordpress.com/2009/06/01/forensics-what-is-the-bitmap/

Q no 2)

Move both files (ADS_YourRollnumner_Name.txt and EFS_YourRollnumner_Name.txt) to Recycle Bin and analyze MFT records.

Highlight all attribute IDs, length (size), file names, resident/non-resident flag, data runs for both files.

Compare both MFTs (MFT of original / non deleted files and MFT of deleted files). Explain in detail the difference you identified.

Check $Bitmap entries against file for extra credit. (Optional)

Q no 3)

Bypass Recycle Bin and use command prompt to delete file permanently or empty Recycle Bin for permanent delete.

Highlight all attribute IDs, length (size), file names, resident/non-resident flag, data runs for both files.

Compare both MFTs (MFT of MFT of simple deleted files {files in Recycle Bin) and MFT of Permanent deleted files). Explain in detail the difference you identified.

Check $Bitmap entries against file for extra credit. (Optional)

Maximum Marks = 100

Note: Use already provided report template. Submit docx file with naming conventions as A4_YourRoll_YourName.docx. Include full screen (including title and task bar) screenshots where necessary.