Exercise 10

12/10/2021

Recovering Deleted Partitions and Deleted Files

Cyber criminals often try to wipe clean a hard disk or other storage media such as Solid State Drives, USB flash drives, CDs, DVDs, magnetic tapes, RAID sub-systems etc. before they depart. They may do this by deleting everything on the storage media or reformatting it. In dealing with such cases, and to conduct a forensic investigation, an investigator needs to use many techniques and often proprietary forensic tools to examine a copy of the storage media and search hidden folders and unallocated disk space for copies of encrypted, deleted, or damaged files.

Partition recovery and file recovery allows you to recover important documents and files that have been lost perhaps by accidental deletion, intentional deletion to conceal evidence, an operating system crash, malfunction of a storage device, logical failure of a storage device, due to a virus, a software malfunction, or even sabotage. Forensic recovery of deleted partitions and files is achieved by using data recovery tools that identify the contents of these lost partitions or files on the storage media and allow for recovering and preserving the data forensically.

The following data recovery situations are some of the common possibilities:

Recovery of deleted or lost files emptied from the Recycle Bin

Disk recovery after a hard disk crash

Data recovery from a hard drive that has been reformatted or repartitioned

Recovery of important documents such as financial records

Recovery from a USB drive, memory card, memory stick, camera card, zip disk, floppy disk, or other storage media

Recovery of files with the original date and timestamp

Finding partitions automatically, even if the boot sector or FAT has been erased or damaged

Exercise 1 Identification of lost or deleted partitions

When a partition is deleted or if the partition table is corrupted, the file systems remain on the disk but their location is unknown and no data can be accessed. Many utilities allow search for partitions and can rewrite the partition table with the partitions chosen by the user. One such open source software for doing this is TestDisk. It was primarily designed to help recover lost partitions and/or make non-booting disks bootable again. It is available at

https://www.cgsecurity.org/wiki/TestDisk

It has many features. It can run under various OS including Windows and Linux.

Create a partition in your drive (may be a USB flash drive) using appropriate tools. Make and copy files of various file types (such as jpg, mp3 etc). Then delete the partition. Check if you are able to detect the files which were there earlier. Use a utility such as TestDisk to recover the partition and then the files.

Refer https://www.cgsecurity.org/wiki/TestDisk_Step_By_Step for step by step instructive examples

Exercise 2 Restoring Lost or Deleted Hard Disk Drive Partition

Download a trial version of EaseUS partition recovery software to restore lost or deleted hard drive partitions in Windows 10/8/7 from the link http://down.easeus.com/product/drw_trial

Follow the steps at the following link for restoring lost or deleted hard disk drive partition

https://www.easeus.com/data-recovery/partition-recovery-software/restore-lost-hard-disk-drive-partition.htm

Exercise 3 Recovering Files and Folders from Deleted Partitions

Use the software at http://www.active-undelete.com/undelete.htm and follow the instructions at

http://www.active-undelete.com/howto_recover_from_deleted.htm

For more data recovery tools look at

https://forensicswiki.xyz/wiki/index.php?title=Tools:Data_Recovery

If a particular tool does not work you may use alternative tools.

Include screenshots in your submission.