Project

Technology, Information Technology

Acquiring an image from Linux Operating system. A lot of research has been undertaken in the field of computer forensics inorder to protect data stored in a computer from copying and many companies have come up with a number of technologies which are able to accelerate the process of imaging. The speed of acquiring an image is normally based on both the physical state of the media, the processor and the type of operating system in use. Initially, images could be easily acquired from computers using the DISKCOPY command since the amounts of data involved were small in size [1]. Different methods have been developed to cater for the different operating systems and large file sizes include Smartsector for windows and Linux dd for the Linux operating system which are able to operate in both file by file and sector by sector modes of imaging hence increasing the speed of fragmentation. These new technologies are also able to image from more than a single storage device including hard drives, removable media devices and tapes.

In order to acquire an image disk from a Linux operating system, various methods of acquiring images have been developed including: Safeback version 2. 0 technique which is able to acquire images on various operating systems on the IDE drives of computers using the sector by sector method; the snapback DataArrest technique which acquires images on SCSI drives of computers using the sector by sector method and DIBS RAID technique which performs optical acquisition of images on both the SCSI drive and the IDE drive of the computer using both the sector by sector and the file by file methods. These methods hold a major strength in the fact that they are able to handle large amounts of data unlike the traditional methods.

However, the most appropriate tool to use is the Linux dd version 7. 0. This tool acquires images from the hard drive of the computer. External storage devices such a removable disks, tapes, flash drives and compact disks can also be used with this tool to perform imaging in a Linux environment. Linux dd version 7. 0 is able to perform image verification by AMD5 checksum verification method [2]. This tool shows high levels of strength in computing complexity and it is very good in detection modification. The probability of programs collision is very low. Imaging is then done on the SCSI drive of the computer unlike other methods of imaging that perform imaging in the IDE drive. Copying of data into the hard drive is normally done using both modes of imaging which are sector by sector and file by file. This tool is able to eliminate any form of slowdown in imaging and it is not affected by fragmentation of the files in the hard drive of the computer [2]. However, acquiring an image using this tool can be affected by corruption of data and possible failure of the system.

Conclusion

Imaging is a very crucial process in computer forensics in order to ensure that the data stored in computers is secured. While performing this process, it is important to choose the right type of tool and methodology in order to avoid problems that result from poor imaging. The field of computer forensics is growing each day and new technologies are emerging thus improving the efficiency of the process of imaging. It is also important to be considerate of the type of operating system while acquiring images from different platforms.

References

[1] Holley, James. “ Computer Forensics.” On-line SC InfoSecurity Magazine. September 2000. Retrieved from: http://www. scmagazine. com/scmagazine/2000_09/survey/survey. html. Viewed on 20th march 2015.

[2] “ Computer Forensics Definition.” New Technologies Armor, Inc. 25 April 2001. Retrieved from: http ://www. forensics-intl. com/define. html. Viewed on 20th march 2015.