Free research paper on computer forensics specialists computer investigations

Law, Criminal Justice

Introduction

Computer forensics describes that part of forensic science that is involved in providing legal evidence obtained from computers and other digital storage devices. It helps in the thorough examination of digital devices in order to determine, preserve, recover and present actual information. The main procedures applied in this field require principles of recovering data in digital media where investigation is carried out to curb crimes that emerge or are conducted in computers. Over the years the use of computers has extensively enhanced the development of computer crimes hackers have engaged in activities that deprive companies and individuals off their valuable property in terms of information. These activities have brought about the emergence of computer forensic that was used in the recovery and investigation processes to provide evidence in court.

This paper will discuss the importance of computer forensics or computer investigations in curbing computer crimes or carrying out investigations. This will be coupled with the procedures and strategies applied in the use of computer forensics as well the techniques that ensure that evidence is properly analyzed and reported. This will also involve the various stages used in cybercrime investigations in order to bridge the gap between technology examination and law enforcement investigation. It will also bring out the various features used in the techniques applied while investigating computer crimes.

The use of forensic knowledge and techniques helps in explaining the modern status of application in the digital world. This involves the storage devices such as hard disks or CD-ROM as well documents transferred by use

of emails (Vacca, 2010). The processes involved require comprehensive analysis which ranges from retrieving information to reconstruction of events in the way they occurred. This helps in preserving the information which is then followed by identifying and extracting it in a way that will allow the investigators to document it and interpret it to meaningful facts that will be presented at the court. The entire process requires proper skills that will enable the investigators to apply various methodologies that entail flexible strategies relevant to the law and to the outside world (Vacca, 2010).

The various stages used in this process offer sufficient response to the threats that occur due to cybercrimes. They have enable law enforcers to bridge the gap between technology used in the recovery and examination of digital forensic in order to overcome the technical challenges faced by law enforcers (Vacca, 2010). The various stages used in this process portray the logic steps and primary considerations that are important in investigating crimes related to cyber as well as the apprehension of the criminals (Vacca, 2010). The process involves the basic resources applied within the law enforcement mainstream as well as agencies that partner with the technical services that help in the investigation process. These stages include: initiation of the investigation, the models used, assessment of the information, the impacts and risks, plans put in place, the various tools, necessary actions that should be taken and the outcome expected from the investigation (Vacca, 2010).

These processes require the involvement of the law enforcement agencies and the experts from the outside world who might give their insight on the currents used. They describe the objectives of the data followed by the

exploitation tactics that will be applied, the methods of attack that will be used as well as the networked technology that will offer more details on the impact in the global environment and the intentions of the criminals space (Newman, 2009). The initiation of the investigation requires clear analysis of the aspects of the digital media that are involved in the cybercrime. Forensic experts make use of X-ways or rather Win Hex which offers various features that help in analyzing the disk space (Newman, 2009). It also helps in capturing the free space in the disk and partitions it to create detailed drive contents table that gives the files in existence as well those that have been deleted. It also helps in imaging and cloning through tools that create mirrors that read the formats used in the drive and the types of media space (Newman, 2009).

This feature helps in recovering of information from disks and storage devices that are used in computers by incorporating several automated file recovery mechanisms. It also allows manual recovery of data in a convenient manner space (Newman, 2009). This is applicable through the search functions that are sophisticated, flexible and very fast in scanning the whole media space (Newman, 2009). It helps recover data that may have initially been deleted or even hidden. In addition to this, there are more features that are used in the recovery and assessment steps. These features include: the disk editor and the file editor as well as the RAM editor which provide access to all files and sectors in the computer. Similarly there is the directory browser for NTFS, ISO 9660, and UDF just to mention but a few spaces (Newman, 2009). They are similar to the windows explorer but they provide the files that exist as well as those that have been deleted in the directories

in order to allow cluster chains in the navigation of the disk editor.

Other features used in this field include the cloning and imaging of the disk through Windows and DOS applications. They allow the investigators to work on the copy available in the free space while images are compressed or split into independent archives. This is accompanied by data recovery features that retrieve data in the directories space (Newman, 2009). The mechanisms used here include: File recovery by name, by type and many more. The partition recovery and boot record recovery uses tailored templates such as FAT 16, FAT32, NTFS just to mention but a few space (Newman, 2009). In the assessment step the hard disks are cleansed and wiped in order to remove any traces of files, viruses and partitions. This is coupled with the capture of file slacks and unused space (Newman, 2009).

After assessing the information recovered, the forensic investigators then create catalogs in the disks in order to examine the contents and limit the search to the specified investigation. This is then followed by creation of reports where the information on the active disks or files is indicated (Nelson, 2010). The information is then interpreted in order to make meaningful sense to the reader. This information is then presented in court as digital evidence which is authentic and can be relied upon (Nelson, 2010). These crucial steps have been widely used in criminal law for providing evidence. This is made possible through the various techniques used through the investigation where they provide reliable information that can be used to apprehend criminals in jail. The various techniques that should be acquired by forensic investigators include: ability to analyze the drives, ability to conduct live analysis where computers are examined from within the

operating system in order to retrieve evidence which might be used as evidence (Nelson, 2010).

These techniques are facilitated by applications that allow the retrieval of data stored in the RAM. These applications range from Microsoft’s COFFEE tool to the Windows SCOPE that provide evidence as well allow analysis and achievement of the physical memory on a computer that has been locked (Nelson, 2010). The forensic investigators review the material available on the computer through a manual process. This includes going through the windows registry in order to acquire any suspicious data. The process may also involve the investigators to crack passwords or even discover them through proper search of the keywords related to the criminal activity. It may also extend to the actual extraction of emails and reviewing the pictures in order to obtain relevant information (Nelson, 2010). These methods have helped law enforcers to get hold of criminals who are involved in such activities as well as assured the general public of safety over their information. However people are advised to ensure security over their gadgets in order to prevent cyber crimes. This should be done through installing anti-viruses and passwords that are not easily predictable (Nelson, 2010).

References

Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to computer forensics and investigations. Boston, MA: Course Technology Cengage Learning.

Newman, Robert. (2009). COMPUTER FORENSICS FRAUD INVESTIGATIONS. Journal of Forensic Studies in Accounting & Business, 1(1), 69-81.

Vacca, J. R., & Rudolph, K. (2010). System forensics, investigation, and response. Sudbury, MA: Jones & Bartlett Learning.