System forensics - overview research paper example

Business, Company

ASSIGN BUSTER

The basic tasks of a computer forensics specialist

Acquisition of data – A computer forensics specialist works in cooperation with law enforcement for gather of recover data from computer systems. In the case of this company, the forensics expert can recover emails from the hard drive and validate them. They can also get information about the author and date from the internet service provider.

Preservation of data – A computer forensics expert needs to store the recovered data in stable media. This is done to maintain the integrity of the same. The expert should also record all steps taken to obtain the data and any editing done to the same.

Analysis of data – Computer forensic experts recover the data in a raw format. It is then up to them to decide whether the data is relevant for the case at hand. They are also responsible for arranging the information into a format suitable for presentation in a court of law.

Analyze the extent of the cybercrime – When a forensics investigator detects an intrusion or misuse of the system, it is up to him to determine its depth and its effect on the concerned company.

- The Systematic Digital Forensic Investigation model (SRDFIM) is the most recent model developed to guide computer forensics. Its processes are discussed below.

Preparation – It involved understanding the nature of the crime and circumstances surrounding it. It also involves obtaining of a search warrant and considering the rights of the suspect.

Securing the Scene – This involves protecting the scene from unauthorized access. The experts should set up a chain of command to ensure the integrity of the data obtained in the search.

Survey and recognition – In this step, the investigators identify the suitable sources of evidence and formulates a search plan. These sources may include the hard drive, the network, or even the server. They should also try to gather the usernames and passwords from the administrators.

Documenting the scene – The investigators should photograph the scene at its initial state. This would include all the electronic equipment around the computer.

Communication shielding – All communication to the device should be cut. This helps to prevent people from overwriting the data before the evidence has been collected.

Evidence collection – This include volatile and non-volatile evidence collection. Volatile evidence is one stored in Rom. This should be obtained as soon as possible. Nonvolatile includes data stored on external disks.

Preservation – The device and accessories are placed in special evidence bags and the whole process is documented. These are then transported to a secure location for safekeeping.

Examination – This involves retrieving and extracting information from the devices, which is relevant to the case. The experts use patterns and keywords relating to the crime to find the evidence they require. The sources include emails, documents, planners, and text messages.

Analysis – This includes timeframe analysis, hidden data analysis, application analysis and file analysis. The specialists do this to create relationships between the data and observe the data’s significance

Presentation – A report detailing the process of the investigation together with its result will need to be filed in the court. The specialists will also need to testify.

Result and review – The investigators go through all the steps followed in the investigation. This is done with the view of identifying areas requiring improvement.

- Challenges of a computer forensics expert

Forensic experts face the problem of choosing the right tools to use in a particular investigation

Since forensic experts are not lawyers, they face the problem of presenting their findings in a court of law

New technologies emerge daily, and it’s hard for computer forensics experts to keep up and device new tools to access hidden data.

- How computing devices are used in crimes of today and how these crimes affect the company’s data

Denial of service attacks – In these attacks the intruder overloads the company’s server, denying the users access to their data.

Access to private data – The attacker gains access to unauthorized data. This may lead to loss of confidence by the company’s customers.

Infections – The intruder inserts viruses into the network. This may lead to data loss of loss of computing power as the computers become unusable.

- Computer forensics and the law

- Computer forensics regularly provides evidence for prosecution of criminal suspects. They obtain a search warrant to look for evidence in the suspect’s computing devices. After collecting the data, they analyses it and arrange it into information that is relevant to the case. Computer forensics experts are regularly called to testify in court. They have to support the methods they used to obtain the data. They also have to prove the integrity of the results they obtained. The law requires them to obtain this data while respecting the privacy rights of the suspect. They need to prove that the data presented in court has not been modified in any way.

- Potential of Computer forensics in the sexual harassment cases
- The forensics expert will first identify which email systems have been used on the computer. He will then access the archive files, which stores all information relating to emails. This is only possible when the user is operating a client based email system. The specialist will obtain existing and recover deleted emails from this file. These may provide evidence supporting or denying the sexual harassment claims. If the suspect uses browser based systems, the specialist has to obtain information from internet service provider. This is because the emails are not stored in the computer.
- The Board of Directors will have to understand the requirements of the law regarding the privacy of their employees. The company policy will also provide some guidelines on whether corporate email addresses operated by employees can be accessed by an outsider. The specialist would advise them to obtain a search warrant especially It the sexual harassment claims turn into a criminal lawsuit.
- References

Agape Inc. (2008, September 3). Role of a Forensic Investigator. Retrieved from Slideshare: http://www. slideshare. net/tzagape/role-of-a-forensic-investigator-presentation

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic Digital

Forensic Investigation Model. International Journal of Computer Science and Securit, 124-127.

Nikkel, B. J. (2006, May 01). The Role of Digital Forensics Within a Corporate Organization. Vienna.