Cyber Forensic Investigation Plan
Dr. K. Purushothaman, Dr. R. Hashemnejad

ABSTRACT
Cyber crime proves to be dangerous at times when they go beyond only hacking and crack of commercial software or stealing the credit card details or making any ecommerce fraud. The range of cyber crime can extend up to hijacking the satellite and sensitive information from the army or other security services that serve the country. The need for cyber forensic investigation is very important considering the seriousness of the case. The investigation has some particular requirements based on the technical and human resources. The paper proposes and investigation plan for executing the evidence searching and investigation with help of FTK tool.

KeyWords
Cyber Crime, Forensic Engineering, Digital Forensics, Cyber crime investigation, Investigation Plan, FTK tool.
INTRODUCTION

Mark F. (August, 2008) says that Cyber Crime is the theft online which included the theft of credit cards, frauds in online share trading, stealing of the software’s and other commercials causing massive loss to the developers and owners. The crime investigation is a challenge in its own way finding evidences with or without support of investigative tools. The investigative evidences are hidden codes and images called steganography, protected files, encrypted in pdf documents, deleted emails and hidden files and folders. King G. L. (June 2006) states that Digital evidences be the collection of sabotage, attacks related information, sensitive information, email hijacking, organized and unorganized crime related information, hacking and cracking and many more such data and information.

Digital forensics have requirement of very high end technical gadgets and tools to perform the investigation. The main requirements are establishment of the spare secured web server so in crisis time the data could be shifted to the secured server until the investigations are performed. There are few investigative tools which reduce the time of investigation and provide optimum results; here we would perform investigation with help of FTK tool and a strategy plan for the investigation.

The report is a detailed cyber crime investigation plan which will include network forensic, remote computer forensic, intrusion detection systems which help in detection of intruders if any, use of forensic tools that allow forensic analysis of the system compromising by the data accessing and footprints left behind if any. The report also concentrates on the future preventive measures like best suited implementation of intrusion prevention systems on both application level and network level.

ROLE OF INVESTIGATOR

The way there is need for high end technical requirement for forensic investigation the same way the person who is investigating the attack/case also needs to be skill full and enough and some times more than enough qualified to deal with the threats. The investigator should be handy with the computer and network forensics tools and well educated to understand the new and upcoming tools in the markets for better performances. Below are the investigation points considering an Role of investigator for an threat in an organization.

1. Performing Digital information analysis, ability to understand standard forensic with evidence handling techniques.
2. The evidences of network computer intrusion should be thoroughly indentified and the procedures should be sound and effective.
3. The examining of malicious files should be checked with all the employee tool editions as internal security issues.
4. The employee tools should be well equipped for handling the techniques like cracking encrypted files and system passwords.
5. Unknown Cyber Crime investigators from Asian Institutes of Cyber Law say that the investigator should have enough knowledge to decode the encrypted data and stegnography files and some time also be able to retrieve the deleted files from the hard drive.
6. The investigator should have a fore sight on the investigation with proper handling of the evidences and should have control on the procedures.
7. Mark F (2008) and King GL. (2006) say that the evidences should be stacked and stored for the presentation in court room which will help in taking necessary action against the attacker.

INVESTIGATION PROCEDURE

The unknown group of Cyber Crime Investigators (2012) from Institute of Asian Cyber groups state few investigation procedures as described below considering a threat in an organization.

1. The plan has to set forth in primary stage and all the required support is to be collected in the beginning itself.
2. The primary investigation plan should include the locking of the suspected areas with no one to reach other then the investigators team.
3. The primary investigation should be performed with the permission of the authorities of the company and necessary evidences should be collected.

4. The suspected case here in an organization the security department has to take permission from the higher authorities by mentioning the seriousness of the complaint received from the executive.

5. Nikkel B.J. (2005) explains in network and computer forensics that the network and the computer of that particular branch should be taken in control for the evidence collection.

6. With reference to Nikkel B.J. (2005) the security cell of the organization if in case of remote location; as an instant response action a remote connection should be establish to the network and computer of the victim.

7. The security analyst are well educated with the technique of remote working and monitoring the network on remote basis to record the behavior of the computer and its incoming and outgoing data transmissions.

8. Network forensic tools should be installed over the affected network to detect the intrusions and the level of intrusions.

9. Nikkel B.J. (2005) explains in network and computer forensics that the Computer forensic tools should be installed on the victim’s computers to perform the scan in order to get the evidences from the cookies, deleted files, encrypted images, protected data files, auto installed application in the operating system programs and all such suspects.

10. The computer forensic tools are well equipped with their individual modules and working components concentrating on the registry updating, image scanning and decoding the encrypted emails and files shared over internet.

11. The preview of all the scanning action can be noticed from the server side and some instant solutions can be proposed by the security analysts.

12. The scan reports and the evidences are collected and documented, when the reporting is done the seriousness of the attack is concluded and if it is any false alarm then all the technical specifications are updated.

13. The attack is determined by the result and consequences of the attack if there has been any theft or any malpractice with the sensitive information or any fraud.

14. The team of investigator decides the seriousness of the attacks and files a case in cyber cell of the local police where the victim is located. The next step is to locate the IP address of the attacker and start searching for the suspect.

15. One team will be on search of the attacker and others will be on mission to strengthen other location networks and computers and installing new and advance intrusion detection systems and self equipped instance response handling tools on the network and the computer both.

DIGITAL FORENSIC TOOL

The FTK Imager (2001, guide no. 3) forensic computer tools have changed from command line environment to easy and handy graphical user interface based tools for the sophisticated usage with very useful and informative user manuals for the ease of usage. These tools are very handy very helpful for the advance investigation patterns. The computer forensic tolls are available for all types of investigations with free and commercial editions that support tests in scientific manner. National Institute of Standard and Technology proposed a computer forensic tool and its framework defines functional and requirement characteristics of such tools meet specified requirements.

Forensic ToolKit (FTK) from AccessData Corporation (AccessData Corporation, 2006) is a well known and very commonly used forensic tool.
tool for computer investigation purpose. This is a leading tool that performs email analysis as explained by (Prosise et al., 2003). FTK operates flawlessly on windows systems starting from Windows xp and 2000 editions.

Forensic Tool Kit is a bundle of several components like registry viewing, known file filtering, and many such components are included. All the components require their own installation module. The image module is essentially imaging component which covers the acquisition of media, image files, and folder content on disk.

Fei B.K.L. (2007) elaborates that there are choices to be made once the FTK tool is launched, the investigator has to choose the preview or acquire mode and the future working is based on the selections made. The screen elaborates about the working of the FTK Tool.

Fig: 1. Results of the acquisition process for FTK.

Table: Acquisition Results

<table>
<thead>
<tr>
<th>Component</th>
<th>Hash Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sector count</td>
<td>224647</td>
</tr>
<tr>
<td>Computed hash</td>
<td>81F2959BF61E039F443C54D722460231</td>
</tr>
<tr>
<td>Report Hash</td>
<td>81F2959BF61E039F443C54D722460231</td>
</tr>
<tr>
<td>Verify result</td>
<td>Match</td>
</tr>
</tbody>
</table>

Fig: 2. Wizard for creating a new case in FTK.

Fig: 3. Processes to perform in FTK.

Fei B.K.L. (2007) elaborates that in the FTK Imager by Accessdata once the wizard is completed the tools starts accordingly its working based upon the selection made as preview or acquiring. This offers many analytical features got acquiring the evidences from the victim’s computer. This is sophisticated graphical user interfaced tools which reduces the time for the investigator as everything is visible right in front and only a clicks second procedure starts. The FTK Imager (2001, guide no. 3) also explains that there are few analytical features which
are discussed below

- **Overview window**: The Overview window provides an overview of the case at hand.

- **Explore window**: Using the Explore window, the investigator can view the hierarchical structure of files, folders and storage media on a computer system in a similar way to that used by Windows Explorer.

- **Graphics window**: The Graphics window displays graphical images as thumbnails which facilitates quicker analysis and access.

- **E-Mail window**: The E-Mail window enables the investigator to view email mailboxes, including their related messages and attachments.

- **Search window**: FTK offers two separate search modes: live and indexed. The live search involves an item-by-item comparison with search terms specified by the investigator, while the indexed search involves the use of a powerful search engine known as dtSearch (dtSearch Corporation, 2006).

- **Bookmark window**: In this window, the investigator can view any items that have been bookmarked.

**Fig: 4. Overview window**

![Overview window](image)

**Fig: 5. Explore window.**

![Explore window](image)

**Fig: 6. Graphics window.**

![Graphics window](image)

**Fig: 7. E-Mail window.**

![E-Mail window](image)
CONCLUSION

The plan elaborates the whole working and collecting evidences from network as well as from the computer by using few highly recommended forensic tools like FTK which is most recommended tool for collecting evidences from the remote computer and also the registry of that computer system.

REAL WORLD CYBER CRIME

Nagpal R. (2008, ch:23) Explains that credit cards are the most commonly used for online purchase and booking tickets for every kind of transportation like airways and railways, these are also used for online financial transactions like purchasing products online, shares, bank transaction and many such ecommerce services are dependent on credit card payment. The instances of credit card fraud are increasing day by day. These ecommerce web sites are strongly secured with SSL certificated and servers.

The scenario: The credit card information is hacked from the website’s database or while performing online transaction which is later reused for online purchase like airline tickets, software purchase and many such online marketing.

The law: The Information Technology Act states the section 43 and 66. The court section penal code is cheating case under section 420.

Who is liable? The liability is given to the person who steals the information and also the one who misuses the credit card information.

The motive: illegal financial growth and tendency of easy money access.

Scenarios

Scenario 1: The criminal or the suspect uses keyloggers while accessing in public computers like internet cafes, air ports, coffee bars with free wifi internet where the suspect can easily access the victim’s sensitive information from internet and make the online transactions. The suspect uses the techniques by which the victim’s information is sent by email and the stealing is done as simple as it was his own credit card.
Scenario 2: the most common place where almost everyone uses credit card at petrol pump or gas stations, hotel receptions and few such places where the employees get access to victims credit card and that information is transferred to the intelligent hackers who get access to these credit cards sensitive information and the transactions are performed without any information to the original credit card holder.

Recommendations

Nikkel B.J. (2005) generalizes that SSC firm should consider the following evaluations which are commonly used while examining the security issues in an organization. There are several areas of evaluations that should be followed by organization which varies from level of organization and also level of attack performed. Coleman. K. (Aug 2012, A-20) provides the following list of areas which are to be considered for evaluations.

- Control the Access
- Maintenance and development of applications
- Security in communications
- Programming compliances
- Planning the continuity
- Security of assets and data
- Controlling the external security issues
- Security to Human Resources
- Investigations on incidents and instant response
- Securities to portable devices and mobile devices
- Monitoring the operational threats
- Securing the physical commodities
- Handling the intelligent security threats
- Clear security policies
- Security for the supply chain wing
- Analytics of security
- Training and awareness of security terms and issues
- Operational management’s security
- Organizational security on over all
- Program management and security terminology

These security areas should be assessed and graded on numerical scores from 1 to 5 scoring system which is required for the senior level of security threat analysis.
REFERENCES


