International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-11, November 2014

Emphasis on Digital Forensic Research

Ankit Yadav, Bharti Godwani

***Abstract*— Computer forensics is a new and fast growing field that involves carefully collecting and examining electronic evidence that assesses the damage to a computer due to an electronic attack and is also helpful in recovering the information which is lost from the systems so as to prosecute the criminal. The proposed framework can be used as a police investigator tool for seizing physical and imaging of the suspect's storage media and hardware for analysis in recovering and presenting the digital information.**

***Index Terms*— Cyber-attack, Information security, Data Integrity, Authentication, Masquerading, Confidentiality, Log Files, Data Theft.**

I. INTRODUCTION

Computer forensics is "the preservation, identification, extraction, interpretation, and documentation of computer evidence, to enclose the rules of evidence, legal and justified processes, integrity of evidence, genuine and factual reporting of the information found, and favouring expert opinion in a court of law or other legal and/or administrative proceeding as to what was found at crime location."[1] To determine the computer incident, find out the criminal, and bring out the whole crime scene in the court is the main objective of all computer forensic phases. The objectives of computer crimes are becoming more common in nature due to increase in computer crime incidents ranging from theft of intellectual property to cyber-terrorism. [2]

To recover, analyse, and preserve the computer and related computer materials in a manner that can be presented as evidence in a court of law. To verify the evidence in short amount of time, also to check the impact of awful activity on the victim and to determine the intent and identity of the criminal, computer forensic is used.

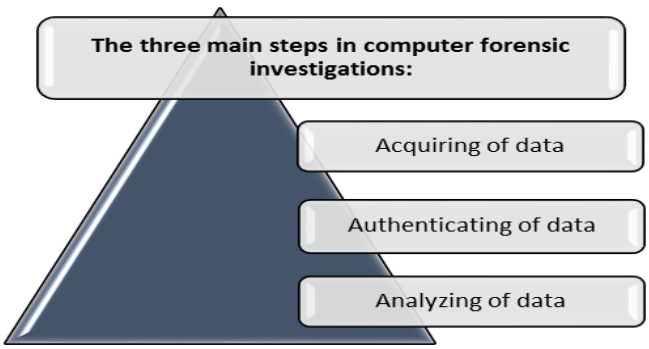

Fig.1 *Shows the main steps in computer forensic investigations*

Manuscript received November 15, 2014.

Ankit Yadav, Student, BE CSE, Swami Vivekananda College of Engineering, Indore, India

Bharti Godwani, Student, BE CSE, Swami Vivekananda College of Engineering, Indore, India

The main steps in any computer forensic investigation are shown in fig.1. Acquiring the data mainly involves creating a bit-by-bit copy of the hard drive. Authentication is the assuring that the copy used to perform the investigation is an exact replica of the contents of the original hard drive by comparing the checksums of the copy and the original. Analysis of the data is the most important part of the investigation since this is where convicting evidence may be found. [2]

II. PROBLEM DOMAIN:

The need for computer forensics has become more credible with the exponential increase in the number of cybercrimes. It has become a must obligation for organizations to employ the services of a computer forensic agency or hire a computer forensic expert in order to protect the organization from computer incidents or solve cases which are required to use the computers and related technologies. [3] In the corporate world, the computer forensics has become a very significant part. There may be organizations which uphold heavy losses because of theft of the data from an organization. For this purposes, computer forensics are used as they help in tracking the criminal.[4] The computer forensics plays a useful role in the backup for single data storing. The data theft and the intentional damage of the data in a single system can also be minimized with the computer forensics so as to increase data security. [5] Computer forensic implies hardware and software that employs the security measures in order to track the changes and the updating of the data or the information in a single system or in any data storage system. The user information is provided in the log files that can be effectively used to produce the evidence in case of any crime in a legal manner. The integrity of the computer system can be also ensured by the computer forensics.[6]

III. PROPOSED SOLUTION:-

The proposed framework will provide the following features to the system at client side as well as channel side:

- **For Security Of Theft Of Data:**

1. ACL:

An access control list (ACL) is a list of access control entries (ACE). Each ACE in an ACL recognizes an administrator and frames the access rights granted, denied, or audited for that administrator. [7] Access lists also filters the network traffic and controls the routed packets to be forwarded or blocked at the router's ports. Each packet is examined by the router that whether the packet has to be forward or drop, on the core of the criteria one specified within the access lists. Access list criteria could be the traffic's source address, the traffic's destination address, the protocol of the upper-layer, or any other information. The sophisticated users can sometimes successfully befool the basic access lists because there is no requirement of authentication. [8]

2. ENCRYPTION:

Encryption is a technique in which the data is converted into a form which is called a cipher text that can't be easily recognized by the unauthorized or malicious people. While decryption is the technique in which the encrypted data is converted back into its original form, so it can be recognized. [9]

❖ **For Security Of The Log Files:**

In computing, a Log Files is a file that basically records the activity performed when a software or operating system runs, or when the user communicates with the computer machine. The act of keeping log files in a recorded manner is called logging. The logging can be done in various ways such as Event logging, message logging and transaction logging. Through these log files, a system administrator can determine what activities are executed on particular system. Thus log files act as most important witness in case of any malicious activity. So securing log files may become a quite big challenge, thus to accomplish log file security and to maintain the record as it is following security measures can be applied: [10]

- **Remote Logging:** - Rather than to store the log entries on the web server, the web server should be configured to send each log entry over the network to a log server.
- **Hash Chaining: -** Another method to secure the log file is to use cryptographic methods to protect the integrity of log records.

❖ **The Integrity Of The Computer System:** The integrity of the system can be maintained by the categorized following ends:

- **CLIENT END:**

1. Antivirus: Antivirus is a software which is used to defend a system from malware, such as computer worms, viruses and Trojan horses. Antivirus software may also be used to take out the spyware and adware, along with malicious programs of various forms of from our system. [11]

2. Firewall: Firewall is a choke point of control and monitoring. It interconnects networks with differing trust. It inflicts limitations on network provided services, only the authorized traffic is allowed within it. [12]

3. IDS (intrusion detection system): Intrusions are the illegal act that tampers the security policy of a system. Intrusion Detection is the process used to determine intrusions. IDS come in a variety of "flavours" and depends upon its approach to the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may pursuit to stop an intrusion's action but this is neither needed nor expected from a monitoring system. There are IDS that simply monitor and alerts when in action, and there are IDS that perform an action or actions in response to a detected threat. Intrusion detection and prevention systems (IDPS) are primarily focused on various practices such as identifying possible incidents, logging information about the intruders and there malicious activity, and reporting attempts. In addition, organizations also use IDPSes for other purposes, such as network monitoring identifying problems with security policies, documenting existing threats and impends individuals from violating security policies and system activities for malicious activity. Now IDPSes have become a necessary part to the security aspects of nearly every organization. [13]

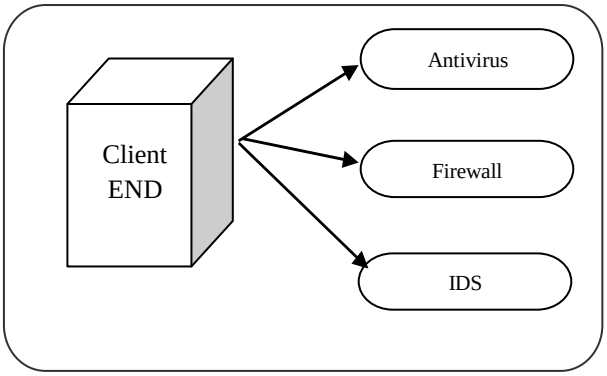

Fig. 3.1 *Shows security measures taken at client site*.

- **CHANNEL END**:

1. HTTPS: The secure hypertext transfer protocol (HTTPS) is a protocol used in communications. Over the World Wide Web it transfers the encrypted information between different computers. HTTPS is http which makes use of Secure Socket Layer (SSL). A secure socket layer is a protocol used for encryption that uses HTTPS, invoked on a Web server. The implementations of the HTTPS protocol mostly involves the exchange or purchasing of private information online. To access a secure server one often requires some type of registration, then login or purchase to access it.[14]

2. EV-SSL: SSL (Secure Sockets Layer) is a standard security technology used to establish an encrypted link between a server and a client. SSL allows sensitive information to be transmitted securely such as social security numbers, login credentials and credit card numbers. Extended Validation SSL Certificate is called ExtendedSSL. EV-SSL customers are authenticated to the highest industry standards. When guest visits a website protected by EV-SSL, the address bar turns green and your organisation name is displayed in the browser interface. It also features phishing detection alert services. [15]

3. VPN: A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote site and enables to create networks using the internet as medium for transporting data. By using a VPN, enables authenticated access to network from external and untrusted environment, businesses ensure security -- anyone intercepting the encrypted data can't read it.[16]

4. TLS: Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. TLS protocol is based on public key cryptography. When a server and client communicate, TLS assures that no third party may monitor or tamper with any message. TLS provides ease of use, strong authentication,

message privacy algorithm flexibility and integrity. Also it is the successor to the Secure Sockets Layer (SSL). [17]

5.

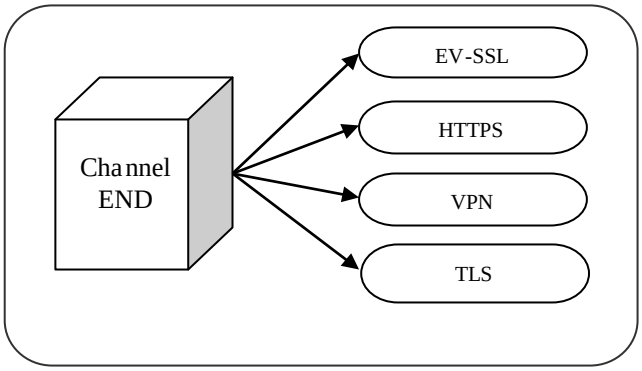

Fig. 3.2 *Shows security measures taken at channel site*.

IV. CONCLUSION:-

A survey to the field of computer forensic methods used to preserve, identify, extract and document the data for any sort of criminal activity. The paper explored various security measures that can be used to prevent and to detect the malicious activity on victim. Next, the computer security for data theft, log file security and integrity of computer system are discussed in the paper. Furthermore, some basic steps to stop and to evaluate the malicious activity were discussed. Lastly, security methods to maintain the integrity of system and to secure data and system integrity were listed.

REFERENCES

[1] Evidence collection http://news.asis.io/sites/default/files/Evidence_Collection_Preservation.pdf accessed on July 15, 2014.
[2] Forensic Investigation - http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf accessed on July 30, 2014.
[3] Need of computer Forensic Sciencehttp://www.computerforensics1.com/computer-forensicneed.html accessed on August 18, 2014.
[4]http://www.krollontrack.co.uk/publications/UK_V5_AP_C F.pdf accessed on August 23, 2014.
[5] Cases in digital forensic - http://forensicswiki.org/wiki/Famous_Cases_Involving_Digital_Forensics accessed on September 29, 2014
[6] Famous criminal cases- http://infosecusa.com/computer-criminal-cases accessed on September 3, 2014
[7] Access control list- http://msdn.microsoft.com/enus/library/windows/desktop/aa374872(v=vs.85).aspx accessed on August 10, 2014
[8] Access Control list methods http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html accessed on July 18, 2014
[9] Encryption Techniques http://searchsecurity.techtarget.com/definition/encryption accessed on August 14, 2014
[10] Log file security - http://security.stackexchange.com/questions/4320/techniquesfor-ensuring-verifiability-of-event-log-files accessed on September 17, 2014
[11] Antivirus - http://www.pctools.com/security-news/whatis-antivirus-software/ accessed on September 20, 2014
[12] Firewall- www.cs.northwestern.edu/~ychen/classes/mitp-458/firewalls.ppt accessed on October 6, 2014
[13] IDS systems - www.csee.wvu.edu/~cukic/CS665/ID.ppt accessed on October 17, 2014
[14] HTTPS protocol- http://msdn.microsoft.com/enus/library/aa767735(v=vs.85).aspx accessed on October 20, 2014
[15] EV-SSL working- https://www.digicert.com/ssl.htm accessed on August 17, 2014
[16] [16] VPN working - http://computer.howstuffworks.com/vpn.htm accessed on September 12, 2014
[17] Transport layer security - http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS accessed on November 3, 2014.