CYBER FORENSICS: A CHECK ON CYBER CRIME

Shantanu Bihani[1], Eeshha Sharrma[2], Shraddha Deshmukh[3]

[1]UG Student, Department of Mechanical Engineering,

[2,3] UG Student, Department of Computer Engineering, Sandip Foundation's- Sandip Institute of Technology and Research Centre, Nashik, Savitribai Phule Pune University, (India)

ABSTRACT

With the increase in globalization which in turn led the world to be a digital world age of computers dawned. With the computers came the new problems of cyber warfare. Computers further led to the internet exploration which gave rise to cybercrimes. These crimes are the most lethal crimes ever in history of mankind. To prevent the computer users from use malicious things, the reverse technology of prevention of cybercrimes such as cyber theft, online banking frauds, phishing, child pornography etc. this wing of forensics deals with all the ways to prevent the cybercrimes, dismantle cyber threats and to bring down any individual or group found doing so.

Keywords: Digitalization, Computation, Cybercrime, Threat, Forensics, Prevention.

I. INTRODUCTION

Cyber Forensics: Cyber forensics, also called computer forensics or digital forensics, is the process of extracting information and data from computers to serve as digital evidence - for civil purposes or, in many cases, to prove and legally prosecute cybercrime. With technology changing and evolving on a daily basis, cyber forensic professionals must continually keep pace and educate themselves on the new techniques to collect this data. They are tasked with being an expert in forensic techniques and procedures, standards of practice, and legal and ethical principles that will assure the accuracy, completeness and reliability of the digital evidence [1].

Cyber Security: Cyber security is an essential element of computer networks, and computer forensics involves working in data analysis and tracking intrusions into computer systems, while monitoring the security of online networks [1] [2].

II. HISTORY

In the early 1980s personal computers became more accessible to consumers, leading to their increased use in criminal activity (for example, to help commit fraud). At the same time, several new "computer crimes" were recognized (such as hacking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court. Since then computer crime and computer related crime has grown, and has jumped 67% between 2002 and 2003. Today it is used to investigate a wide variety of crime, including child pornography, fraud, espionage, cyber stalking, murder and rape. The discipline also features in civil proceedings as a form of information gathering (for example, Electronic discovery)[1].

Fig.2 Technique of Cyber Forensics

III. TECHNIQUES OF CYBER FORENSICS

Computer forensic investigations usually follow the standard digital forensic process or phases: acquisition, examination, analysis and reporting. Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices where a lack of specialist tools led to investigators commonly working on live data.

A number of techniques are used during computer forensics investigations and much has been written on the many techniques used by law enforcement in particular. See, e.g., "Defending Child Pornography Cases".

- **Cross-drive analysis:** A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.
- **Live analysis:** The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down [2].
- **Deleted files:** A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials [2]
- **Stochastic forensics:** A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft[3].
- **Steganography:** One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes [3][4].

Cyber security is gaining prominence in the light of increasing number of unauthorized attempts to barge into private data with the explicit aim of stealing the same to intimidate or coerce users into information blackmailing. The tools and techniques employed to tackle cyber security concerns are:

- **Authentication:** This fundamental cyber security technique intends to verify the identity of user based on the credentials stored in the security domain of the system. The most common mode of governance is password technology, however there are numerous other implementations like the SIM card inserted in anyone's cell phone. SIM cards are equipped with unique ID numbers which are passed over a secure communication line for identification of a particular cell phone. The main challenge encountered in authenticating process is thwarting attempts of unauthorized people to eavesdrop on the authenticating message. The password transmitted over an insecure medium is liable to be intercepted by dishonest people who can use it to disguise as the original user. This problem is countered by encryption [4].
- **Encryption:** Encryption renders data undecipherable without application of a proper key to unlock the same. To combat an encryption, one would be required to undertake solving complicated mathematical problems like factoring large primes that would consume astronomical amount of computing resources and time. Symmetric encryption utilizes the same key for the purpose of message encoding and decoding, and the security level is similar to that of the key. The distribution of the key will be accompanied by potential security risks. Asymmetric encryption utilizes a public key to encrypt the message and a private key to decrypt the same. A majority of present day security protocols are employing asymmetric encryption for distribution of keys [4][5].
- **Digital signatures:** Digital signatures can be erected out of the same mathematical algorithms that are employed in asymmetric encryption. A user is free to test that he possesses a private key by getting some information encoded with it. Anyone can get the same decrypted by having the public key that will verify the person's credentials. This process is in essence the exact reciprocal of public key encryption and likewise functions on the assumption that the authorized user only has the private key [5].
- **Anti-virus:** The threats of computer viruses or undesirable short programs that trigger unwanted commands without the explicit consent of user have assumed monstrous proportions. Anti-virus software carries out two functions; it prevents the installation of virus in a system and scans the systems for viruses that are already installed. Most viruses have been constructed to target Windows operating system as it is the most preferred computing platform of masses. Apple and Linux users can also come under the attack of viruses exclusively built for such operating systems [4] [5].
- **Firewall:** Firewalls effectively hinders any attempt of unauthorized access to a computer when it is connected on the internet by hackers directly or via other network connections. Firewalls come bundled up with most operating systems and are turned on by default. The help of commercial firewalls can be sought if the security level of the default firewall is not strong enough or if it is posing interference to legitimate network activities [5].

IV. CONCLUSION

As new technological innovations continue to proliferate in our society, so do the opportunities for technology exploitation. Once a mere nuisance, hackers now threaten private citizens, businesses, and government agencies.

Government and law enforcement agencies need skilled professionals who can join the fight against cybercrime, cyber terrorism, identity theft, and the exploitation of minors. Companies and other private sector organizations need skilled professionals with both business acumen and technology skills for recognizing and mitigating vulnerabilities.

The U.S. Bureau of Labor Statistics (bls.gov) predicts there will be over 65,000 new jobs for "Information Security Analysts, Web Developers, and Network Architects" by 2020.The Cyber Forensics and Information Security program combines the disciplines of technology, business, organizational behavior, and law. Students learn techniques used to detect, respond to, and prevent network intrusions. They also master broader concepts such as the responsible use of resources, the appropriate management of risks, and the alignment of information technology with the organization.

REFERENCES

[1] Armstrong H, Russo P., Electronic forensics education needs of law enforcement.

[2] Giordano J, Maciag C. Cyber forensics: a military operations perspective. Available from: http://www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632BFF420389C0633B1B. Pdf; 2002.

[3] Jansen W, Ayers R. Guidelines on PDA forensics [NIST 800-72].Gaithersburg, MD: National Institute of Standards and Technology; 2004.

[4] Casey E. Digital evidence and computer crime: forensic science,computer and the Internet. Boston: Academic Press; 2000.

[5] Casey E. Handbook of computer crime investigation. Boston: Academic Press; 2002.