 ISBN- 978-93-5254-640-7

Computer forensics –An Anti-missile to Information Warfare.

Asst. Prof: Prashant N. Wadkar

STE'S Sinhgad Institute of Management and Computer Application, Pune (INDIA)

pnwadkar@gmail.com

Brief Introduction:

"Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. It is often more of an art than a science, but as in any discipline, computer forensic specialists follow clear, well-defined methodologies and procedures, and flexibility is expected and encouraged when encountering the unusual."

Every year numerous cyber crimes go unsolved. And affecting increase in financial losses. India has faced the 26/11 Mumbai terror attack. The Indian Government should have more concentrations in the study and research of computer Forensics. There are many upcoming challenges like net-war. All the countries should be prepared and should make provisions for net-war otherwise it will costs more.

"Sword and neck: Only Sword is not responsible to cut the neck, but due to reason that neck is soft". Similarly for any crime either real-crime or virtual crime, if there are many loop holes, possibility of crime increases.

Case of Information Warfare:

The day of April 27, 2007 was regarded as a black day in the history of Estonia (European country) because within a span of few hours the online portals of Estonia's leading banks crashed keeping the banking operations at bay. All of the principal newspapers' website stopped working and their circulating was badly affected, even the government communications stopped functioning. This is not a result of any nuclear, chemical or biological weapon of mass destruction but due to the Information Warfare(IW) which proved to be more powerful weapon than the other modes of warfare. There has been an apprehension that Russia had a hand behind the attacks. This Case focuses on laying down a legal regime for the worst-case cyber attacks that rise to the level or armed attacks as these have significant impact on both cyberspace and international security.
[ICFAI University journal of cyber law. Vol. VIII Aug/Nov-2009.]

Above case focuses on the necessity and research on Computer Forensics to find out the cyber criminals.

Normally the Forensic Process is adopted as below:

1. Preparation (of the investigator, not the data)
2. Collection (the data)
3. Examination
4. Analysis
5. Reporting

There are many reasons to employ the techniques of computer forensics:

- In legal cases, computer forensic techniques are frequently used to analyze computer systems belonging to defendants (in criminal cases) or litigants (in civil cases).
- To recover data in the event of a hardware or software failure.
- To analyze a computer system after a break-in, for example, to determine how the attacker gained access and what the attacker did.
- To gather evidence against an employee that an organization wishes to terminate.
- To gain information about how computer systems work for the purpose of debugging, performance optimization, or reverse-engineering.

Computer Forensics also has sub branches within it such as **Firewall Forensics, Database Forensics, Mobile Device Forensics.**

Database Forensics

D**atabase Forensics** is a forensic study of databases.

1. The timestamps that apply to the update time of a row in a relational table can be inspected and tested for validity in order to verify the actions of a database user. Additionally copies of database evidence can be made in order to preserve that evidence for future presentation during a legal process.

2. Many database software tools are in general not reliable and precise enough to be used for forensic .There is currently a single book published in this field though more are

destined Additionally there is a subsequent SQL Server forensics book by Kevvie Fowler named SQL Server Forensics which is well regarded also.

3. The forensic study of relational databases requires a knowledge of the standard used to encode data on the computer disk. A documentation of standards used to encode information in well known brands of DB such as SQL Server and Oracle has been contributed to the public domain.

Collecting Digital Evidence

Digital evidence can be collected from many sources. These include computers, cell phones, digital cameras, hard drives, CD-ROM, USB memory devices, and so on. Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags, and web pages (which must be preserved as they are subject to change).

Some of the most valuable information obtained in the course of a forensic examination will come from the computer user. An interview with the user can yield valuable information about the system configuration, applications, encryption keys and methodology. Forensic analysis is much easier when analysts have the user's passphrases to access encrypted files, containers, and network servers.

In an investigation in which the owner of the digital evidence has not given consent to have his or her media examined (as in some criminal cases) special care is taken to ensure that the forensic specialist has the legal authority to seize, copy, and examine the data.

In recent years there has increasingly been an emphasis on performing analysis on live systems. One reason is that many current attacks against computer systems leave no trace on the computer's hard drive---the attacker only exploits information in the computer's memory. Another reason is the growing use of cryptographic storage: it may be that the only copy of the keys to decrypt the storage are in the computer's memory, turning off the computer will cause that information to be lost.

The process of creating an exact duplicate (imaging) of the original evidentiary media is done using a standalone hard-drive duplicator or software imaging tools. This is usually done at the sector level, making a bit-stream copy of every part of the user-accessible areas of the hard drive which can physically store data, rather than duplicating the filesystem. The original drive is then moved to secure storage to prevent tampering. During imaging, a write protection device or application is normally used to ensure that no information is introduced onto the evidentiary media during the forensic process.

Collecting Volatile Data

If the machine is still active, any intelligence which can be gained by examining the applications currently open is recorded. If the machine is suspected of being used for illegal communications, such as terrorist traffic, not all of this information may be stored on the hard drive. If information stored solely in RAM is not recovered before powering down it may be lost. This results in the need to collect volatile data from the computer at the onset of the response.

Several Open Source tools are available to conduct an analysis of open ports, mapped drives (including through an active VPN connection), and open or mounted encrypted files (containers) on the live computer system. Utilizing open source tools and commercially available products, it is possible to obtain an image of these mapped drives and the open encrypted containers in an unencrypted format. Open Source tools for PC's include Knoppix and Helix.

There are many softwares used for computer forensics. Some recommended softwares are:

1. Guidancesoftware's Encase: www.encase.com
2. Acessdata's Forensic Toolkit: www.accessdata.com
3. AccessData Password Recovery Toolkit
4. AccessData's Distributed Network Attack
5. Prodiscover (DFT or IR), www.techpathways.com
6. Safeback, www.forensics-intl.com
7. Quick View Plus, http://www.jasc.com/
8. Thumbs Plus (Shareware), www.cerious.com
9. Irfanview (freeware for non commercial use): www.irfanview.com
10. Brian Carrier's Sleuth Kit is used in many investigations, for analyze specific portions of information.

Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail, temp files, Recycle bin, Recnt Link Files, Internet History and images for review.