An Investigation on Computer Forensics

Abhishek Kaushik[1] Sudhanshu Naithani[2]
[1, 2] Computer Science and Information Technology Department
[1]Kiel University of Applied Sciences, Germany
[2]NC college of Information Technology, India

Abstract— Computer forensic uses many techniques for investigating and getting evidence regarding activity of computer, which is acceptable in court of law. The need of digital evidence is becoming crucial. For this purpose Computer forensic science is the application of science to find legal evidence from computers and other storage devices, so that truth comes out. The goal of forensic science is to provide valid and trustworthy information to investigator and the court.
In old days forensic science was limited to fingerprint comparison, trace evidence, tool marks, toxicology and serology. But now it is expanded by including DNA analysis, explosion analysis, risky material analysis and audio/video analysis. That's how forensic science has become powerful weapon to investigate and control crimes. The evidence which is provided by forensic science has become "true fact of life", because it tells about incident step by step. Evidence related to theft, extortion, hacking, even murder has been exposed with the help of forensic science. This new technology has become foremost part in law sanction circles.
In today's world awareness of applicable laws in practice of computer forensic is necessary for all type of organizations. Like for network administrators and security staff needs to know all issues regarding to computer forensics.
Employees of corporate governance, legal departments or IT should be known about all aspect of computer forensics. Forensics required employees with balanced combination of technical skill, legal acumen and ethical conduct who is known as computer forensic specialist. Cyber-crime rates are increasing and computer forensic science has power to control these cyber-crimes. The utilization of personal computer is very wide, data exchange is more than ever before and high-tech crimes are on increase. That's why we need to have computer forensic service to get successful prosecutions in court of low.
Main purpose of this paper is to conduct a little investigation on computer forensic science or computer forensics.

I. INTRODUCTION

Human race has become so technical that we can use computer for legal issues. Today use of computer is on increase, which makes our life easier but sometimes adulterated also. Computers are easy way to commit crimes. Criminals are utilizing computers to clone mobile phones, to store their transaction ledgers, to do hacking. One more negative effect is made by pornography distributors on our society. They use internet to conduct their pages and websites, which makes serious impact on our children.
Now on account of misuse of computers some crimes are proliferating day and night like sexual harassment, blackmail, identity theft, document theft and practice of employing spies in government and private sector. To investigate these types of crimes we have a technique which is called computer forensic science (also known as computer forensics).

II. MEANING OF COMPUTER FORENSICS

Computer forensics (computer forensic science) is most recently introduced type of forensic science. It is combination of two words. First one is computer, which is known to all and second one is forensics (forensics means to bring to the court), which is operation of using scientific facts for collecting, analyzing and presenting evidence to the courts.
The word 'computer forensics' is defined as "Science of acquiring, preserving, retrieving and presenting data that has been processed electronically and stored on computer media". Because computer forensics is new discipline it was not so recognized as a formal "scientific" discipline. But now it is on path to become popular way for investigation. Computers are being used massively by criminals so computer forensics is best way to investigate these crimes because best and perhaps only technique which recover data in white collar crimes also.
Definitions:

"The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable". (McKemmish,1999).
"Gathering and analyzing data in a manner as freedom distortion or bias as possible to reconstruct data or what has happened in the past on a system".(Farmer & Vennema, 1999)

"What is forensic computing? A methodical series of techniques and procedures for gathering evidence from computing equipment and various storage devices and digital media that can be presented in a court of law in a coherent and meaningful format".-Dr. H.B Wolfe

III. HISTORY OF COMPUTER FORENSICS

History of forensics is about of 100 years long. As time passes we got to know about new technique, tools and invention which were helpful in investigation.
Now if we talk about these inventions from start Francis Galton (1822-1911) invented recorded study of fingerprints first time. Leone Lattes did find blood grouping (A, B, AB &O). Albert Osborn (1858-1948) found indispensable appearance of document examination, Calvin Goddard (1891-1955) discovered bullet comparison which helped to solve many cases. Hans Gross was first man who made utilization of scientific facts on topic of criminal investigations. Meanwhile in 1923 U.S. Federal courts did try to establish standards of forensic science. After it Frye

court defined two conditions. These two conditions were compulsory for the output f scientific testing.

1 The science should be acknowledged with applicable community.
2 Published in journals with scientific manner.

This test was known as Frye rule and became standard for forensic science.

First time when any investigation agency provided forensic services to their field agents and law authorities was FBI in 1932. They set up a lab for forensic services. That's how use of forensic science increased as time passes.

IV. PROCESSING OF COMPUTER FORENSICS

Computer related crime or cyber-crimes are mishap of today's global and technical society. Wide use of technology is making crimes somehow easy to happen. Today evidences are more electronic or digitalized, which is true for all cyber-crimes.

When any incident happens we first need to examine whether we require computer forensic or nat. When computer forensic applied its first aim is to preserve the evidence. If we fail to do so, it could ruin entire investigation. A forensic task in a particular crime will depend on evidence required. If result of investigation is not enough to prove crime then there will be low requirement to take case to the court.

Computer Forensic Field Triage Process Model (CFFTPM)**:**

This model gives an onsite resemble to provide identification, analysis and interpretation of evidence (digital) in scanty time contrive. This model has already been used in many real world cases. And its importance and approach has already been defined.

The focal of model are:

1 To find true evidence
2 Identify victims
3 Guide the current investigation
4 To know potential charges
5 Accurate danger to society by offender

Meanwhile make all evidence safe for further examination and analysis.

In this model we have six phases of investigation process. There phases are: planning, triage, user profiles, timeline/chronology and internet activity and at last case specific evidence. Here every phase is having some consideration and sub-tasks which do varies according to case, file system and operating system under forensic process .(see fig.1)

V. COMPUTER FORENSICS ASSISTANCE TO HUMAN RESOURCES

Computer forensic is becoming very helpful to business. Computer can keep safe evidence of many crimes like sexual harassment, wrong termination, fobbing can be found in employee's computer, hard disk and e-mail. Investigation for any cyber-crime should be done by forensic specialist otherwise case would be thrown out of the court.

Employer Safeguard Program:

Computer has become more powerful and useful in business nowadays. Employer should be more careful to safeguard business information. Unfortunately today lots of ways by which important information and data can be damaged, replaced or destroyed on account of wrong intention.

For example-if an employer wants to terminate a employee, a forensic expert should duplicate data present in employee's computer so that in case of damaged or deleted data employer can recover data and get to know what activity happened on that computer.

Now if you are looking for evidence in a cyber-crime case you have to know what was criminal doing with their computer in last few days or several months, so that you can find a clue to detect whole story. For example you should be known about facts that:

1 What websites have been visited?
2 What files have been downloaded?
3 When file accessed last time.
4 Any attempt to destroy evidence.

5: Fax and e-mails which were sent and received in last several days.

VI. USER OF COMPUTER FORENSIC EVIDENCE

Computer forensic evidence can be used by prosecutors, which is revealed by forensic specialist. Users of computer forensics evidence are following:

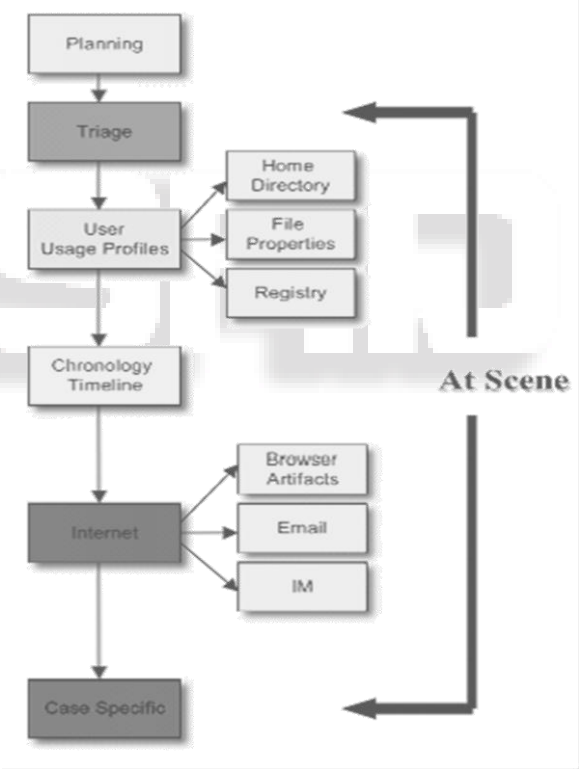

Fig. 1: CFFTPM Phases

(Reference by-- Computer Forensics Field Triage Process Model by Marcus K. Rogers, James Goldman, Rick Mislan (all 3 from Purdue University), Timothy Wedge (National White Collar Crime Center), Steve Debrota (U.S. Attorney's Office – Southern Indiana))

1 Criminal prosecutors utilize forensic evidence in various criminal cases like homicides, fraud and child pornography also.
2 Civil litigation can do use of records found on computer machine in investigation of harassment, divorce, fraud And discrimination cases
3 Corporations also appoint computer forensic expert to Find evidence in case of sexual harassment, theft,

Embezzlement and internal and confidential data

4 Insurance companies can also appoint computer forensic evidence for any type of fraud which is possible in accident, compensation cases and arson cases.

5 Sometimes individuals also hire forensic expert to get claim for wrongful termination, sexual harassment or age discrimination.

METHODES	DESCRIPTION
1 – Protect	Protect subject computer system from alteration, data corruption, virus infection, and physical Damage
2 – Discover	Uncover all files: normal, hidden, deleted, encrypted, password-protected
3– Recover	Recover as many of the deleted files as possible
4 – Reveal	Reveal the contents of hidden and temporary files
5 – Access	Access the protected and encrypted files, if legal
6 – Analyze	Analyze all relevant data, including data located in unallocated file space and file slack
7 – Report	Print out a listing of all relevant files, and provide an overall opinion on the system examination
8 Testimony	Provide expert testimony or consultation, if required

Table1. General Methods Used in Computer Forensics

VII. TOOLS USED IN COMPUTER FORENSICS

The internet is a connection of large number of computer devices which are being used in business, communication and data exchange throughout the globe.

Computer based crimes contain fraud, theft of secrets, theft or slaughter of intellectual property etc. intellectual property and trade secrete works as foundation for any organization. It means intellectual property and trade secrets are basic of organizations upon which organization is built. If this information gets leak, organization could easily cost millions.

One more renowned type of cyber-crime is cyber obscenity such as child pornography is on increase day and night, which is not good for our social health especially for children.

To catch the criminal, after committing crime, is not so easy task because criminal could be anywhere across the globe. At this point forensic expert needs some specialized software known as tools. Like other forensic sciences computer forensic science also has some tools and devices to do continuous investigation. This type of investigation does pursue some rigid type of methodology to maintain soundness and credibility of involved devices. The general methodologies are described in table.1 above

VIII. METHODES DESCRIPTION

1 Protect
Protect subject computer system from alteration, data corruption, virus infection, and physical

2 Damage
Discover Uncover all files: normal, hidden, deleted, encrypted, and password-protected

3 Recover
Recover as many of the deleted files as possible

4 Reveal
Reveal the contents of hidden and temporary files

5 Access
Access the protected and encrypted files, if legal

6 Analyse
Analyse all relevant data, including data located in unallocated file space and file slack

7 Report
Print out a listing of all relevant files, and provide an overall opinion on the system examination

8 Testimony Provide expert testimony or consultation, if required

Here we present overview of some forensic tools:

A. *EnCase*

EnCase is a forensic tool which was introduced in market in 1998 by Guidance Software. Guidance Software states that "encase provides a much simpler way to conduct a search of computer system, document the finding, and make evidentiary and discovery copies" .Function of EnCase are disk imaging, verification and data analysis. EnCase has another important feature which is called recovery of data.

A computer forensic specialist starts investigation by imaging store devices which are to be investigated. EnCase acquires evidence as an evidence file (EF) which is bit-stream image of the storage devices. After it EnCase checks soundness of image file and storage device by using hash function. This tool also provides cluster-by-cluster view of file and vital information like last access, time of creation, last modification of a file. In fig.2we can see that first column "File Name" tells names of files and forth column "Description" shows status of each file.

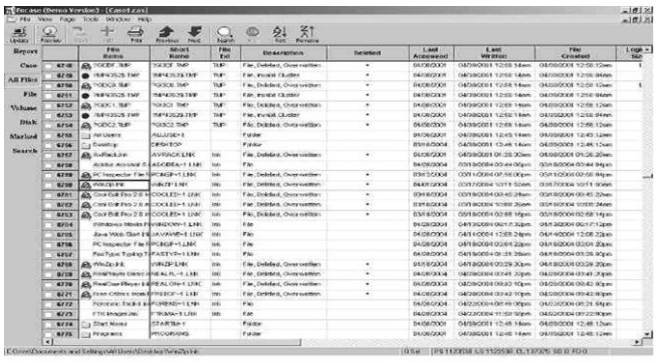

Fig. 2: Data discovery view with Encase.
(Reference by--AN INVESTIGATION INTO COMPUTER FORENSIC TOOLS† by K.K. Arthur & H.S. Venter (University of Pretoria))

B. *Using EnCase to Capture a Criminal*

Software tools have helped in many cases by bringing criminal to justice. For example –we take a case of PayPal Inc. which is an online payment processing company. Once they got to know that about forty accounts were buying expensive goods on eBay.com auctions. Cyber criminals used their mock PayPal site to get user log-ins and password and that's how theft of thousands of credit cards numbers

was conducted by criminals. The criminals were acting as seller and buyer in same auction and then paying by stolen credit cards. A fraud investigator IP address of criminal was same as IP address of questionable PayPal accounts. When criminals got arrested, mirror-image copies of criminal's hard drive were subjected to EnCase keyword and pattern searching mechanism. Then they uncover EnCase to get data. They caught the criminals because they established link between criminal IP address and Perl script, which was used by criminals to open account on PayPal's system. So use of software tools can help us to find cyber-criminal.

C. Disk Imaging Software

Disk imaging is a process of duplicating each bit of data from one physical media to another, similar media. Sometimes source and destination media is identical. And sometimes destination media should have same size as source media. This type of copy of data is known as physical or direct copy. Other type of copy operation only copies files and files name, not data which is present in media but is not part of any file. Both copy operation are important for examine point of view. Examiner decides whether to make a physical copy, a logical copy or both after analyzing these factors:

1) Duration

How much time examiner takes to do copy operation?

Creating physical copy takes more time then logical copy because in physical copy whole data copies without having idea what part of disk contain data. While in logical copy examiner is able to specify small set of data to copy. So logical-copy contains fast speed then physical copy.

2) Integrity Checking

While performing bit by bit operation some software performs integrity checking to make sure that all data is copied without error. The common techniques used to confirm data integrity is digital signature (hashing function or message digest) or a checksum algorithm. Good hashing algorithm make small change in input file which produces corresponding change in hashing result. On account of its advantages many laboratories are using hashing algorithm.

3) Store Image as a File

When software is busy in making physical copy some product stores image copy of original media in a file. This approach gives palpable advantages.

Software with this feature have a Jazz, Zip or other removable media drive which is attached to computer by external interface and then data gets copied from original drive. This software also support restore mechanism by doing image copy of disk drive onto a compatible media.

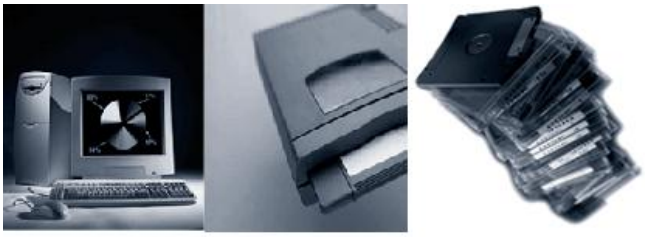

Fig. 3: Creating an Image Copy
Evidentiary Comput External Storage Drive Image Copy Software (Jazz, Zip, etc)
(Reference by Computer Forensics: Tools & Methodology by Michael Noblett & Adam Feldman)

4) Password Recovery Tools:

A password recovery tool helps us to get over password. Password cracker tries to match password hash to all hash words in dictionary. If match is found the password hash is matching dictionary word. That's how we can get recovered password.

a) *@Stake*

LOphtCrack application has 5 versions. Version 5th is latest one. It is an award winning recovery application which is being used worldwide. This application uses large number of method to decrease security risk to network administrators by:

1. Identifying and resolving security problems.
2. Recovering windows and UNIX account password.
3. Rapidly processing accounts by using pre-computer password tables.

b) *MS Access Database Password Decoder*

This password decoder was designed to decrypt master password of Microsoft Access database. This decoder contains two utilities in ZIP file to decode Access95, Access97, Access2000 and Access XP etc.

IX. CONCLUSION

Today computer forensics has become an important and sharp way to catch criminal in short duration of time. It depends on computer forensic specialist to find important facts about crime and present them in court of law. Although software's are much effective but there are some shortcomings also present in these software. If we make required improvement in these tools, the prosecution of cyber-crime will surely increase. As FBI told "in the year 2000 there was 2032 cases opened involving cyber-crime. Of those cases only 921 were closed. Of those closed cases only 54 convictions were handed down in court" (Insert 2003)

That's why we need to make our tools and specialist more powerful and skilled. With the passes of time cyber-crime will increase as well as technologies. So well-trained computer forensic specialist would be needed to control these crimes and to maintain peace in the society, and most important to maintain believe of people on the court of law.

REFERENCES

A. BOOKS

[1] Computer Forensics: Tools & Methodology by Michael Noblett & Adam Feldman
[2] Computer Forensics: Computer Crime, Scene Investigation (Second Edition) by John R. Vacca
[3] George Mohay, Alison Anderson, Byron Collie, Olivier de Vel, Rodney McKemmish, Computer and Intrusion Forensics‖, Addison Wiley, 2001

B. JOURNALS

[1] Computer Forensics: An Essential Ingredient for Cyber Security by Dr. Richard Bassett, Linda Bass and Paul O'Brien (Western Connecticut State University),Jist 3(1),2006

[2] AN Investgesation Into Computer Forensic Tools† by K.K. Arthur & H.S. Venter (University of Pretoria),vol 1, 2008
[3] Computer Forensics Field Triage Process Model by Marcus K. Rogers, James Goldman, Rick Mislan (all 3 from Purdue University),Timothy Wedge (National White Collar Crime Center),Steve Debrota (U.S. Attorney's Office – Southern Indiana),2006

C. WEBSITES

[1] www.computerforensicsworld.com
[2] www.computer-forensic.com
[3] www.cio.com/article/30022/Computer_Forensics_IT _Autopsy

