Computer Forensic Technology

Bharat Bhushan[#1], Yashpal Singh[*2] Joni Birla[3]
[1,2,3]Department of Computer Science &Engineering,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, India

***Abstract*— The present era undoubtedly is an era of technological revolution which has witnessed unprecedented growth in use of electronic devices especially the mobiles and computers. In fact every facet of our life, directly or indirectly, to a large extent is dependent on computers. The Computer/Mobiles, the intelligent devices, are not limited to performing official responsibilities only; rather these have occupied an important place to perform one's day to day functions in just one click whether it is SMS, MMS, Internet access or Online Transactions etc. However, this advancement in technology has also raised the concerns over misuse of these machines by anti-social elements and it becomes essential for the security agencies to remain ahead with regularly update about the tools and techniques available to identify and investigate a crime done with the help of Mobile/Computer.**

***Keywords*— *Computer forensic, Types of Computer Forensic Technologies, Military Computer Forensic Technology, Scope of Research in Computer Forensic, Computer Forensic Covers, tools used in Forensic System*.**

I. INTRODUCTION

1.1 Definition of Computer Forensic:

The responsibilities of computer forensic professionals include preservation, collection, and analyzing data/evidence traced on computers to determine the facts in question. They must also provide credible and reliable expert testimony even in court, if necessary. Though this sounds very straightforward, but it is not a child's play. A computer forensics' examination involves vast aspects to be covered; therefore documentation of information which is informative, consolidated, and accurate is paramount to the success of the case. Computer Forensics place distinctive force on the sound treatment of potential evidence to clog it from being altered or tampered with. It is also referred as Digital Forensics.

1.2 Traditional Forensic & Computer Forensic:

The primordial principles of computer forensics are identical to that of traditional forensic regimentation. These start with exorbitant variability among a large number of merits and advances are targeted at enhancing the identification, characterization and correlation of the evidences and their modality. Whereas an MD-5# may recognize a digital document to the exception of all others, the tailings of a removed Netbus application ensconced in unallocated space may help correlate a suspect to victim's firewall log data of scans on port 543165 coming from the suspect's IP address. Forensic techniques are designed to uncover these identifying, characterizing and correlative properties more precisely, more accurately, faster and with limited evidences available for examination. For e.g., a comparison of analysis development between digital data and biological data (blood) would exemplify how A/B/O typing give way to RH factors, which was supplanted by DNA typing via RFLP (Restriction Fragment Length Polymorphism) and PCR (Polymerase Chain Reaction) – which results in the same evidence source being used for characterization and then positively identifies persons to the heteroclite of all others. Similarly, forensic inquest techniques for digital evidence has yielded # libraries (to recognize data files), file signatures (to mark out files by collation filename and file type) and mirror imaging software (to copy abundant amounts of evidence sans altering the prime evidence). Nonchalant of whether the discipline is computer forensics or fingerprinting, the effusion question is not whether evidence exists but, rather, can investigators uncover and contextualize the evidence. Henceforth, the challenges are: Where to look? What techniques will make the evidence glaring? Is the evidence licit? Just like a pathologist who can infer by observing the lack of water in a person's lungs that he was betimes dead when his car sank to the depths of a lake, similarly a computer forensic examiner should be capable to analyze file modification/access/ creation times to determine if intellectual property was transferred after an employee was fired. Just like that the sources of biological evidence can be blood, saliva or hair shafts found on clothing, cigarette butts and weapons; the digital evidence can be found on any number of media sources (hard drive, floppy disk, CD-ROM, PDA) and in locations such as print spooler files, hidden partitions, registries, system logs, bad clusters, and/or metafiles. In the biological realm, techniques such as PCR, RFLP, and STR (short tandem repeats) exist to identify DNA in a drop of dried blood which is not visible to the naked eye. In computer forensics, techniques exist to recover deleted data; recover passwords; analyze file slack, unallocated space and swap files; reconstruct user and application activity on a system; and search email for source and content information. Finally, in terms of admissibility hurdles, the technology to recover deleted data has been accepted, but what is contested is the inclusiveness of the software that undertakes to recover it – in other words, Are there measurable error rates for the software that address the likelihood of missing potentially exculpatory evidence? Likewise, insofar as DNA fingerprinting technology has been accepted in the courtroom, certain techniques (like STR) remain open to challenge.

1.3 History of Computer Forensic:

1970s: Crimes cases involved computers for financial fraud

1980's:

- Financial investigators and courts realize that in some cases all the records and evidences were only on computers.
- Norton Utilities, "Un-erase" tool created
- Association of Certified Fraud Examiners began to seek training which subsequently evolved in computer forensics
- SEARCH High Tech Crimes training created
- Regular classes began to be taught to Federal agents in California and at FLETC in Georgia
- HTCIA formed in Southern California

1984: FBI Magnetic Media Program created, which later on become Computer Analysis and Response Team (CART)

1987: Access Data – Cyber Forensic Company formed

1988:

- Creation of IACIS, the International Association of Computer Investigative Specialists
- First Seized Computer Evidence Recovery Specialists (SCERS) classes held

1993: First International Conference on Computer Evidence held

1995: International Organization on Computer Evidence (IOCE) formed

1997: The G-8 countries in Moscow declared that "Law enforcement personnel must be trained and equipped to address high-tech crimes".

1998: In March, G-8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence

1998: INTERPOL Forensic Science Symposium

1999: FBI CART case load exceeds 2000 cases, examining 17 terabytes of data

2000: First FBI Regional Computer Forensic Laboratory established

2003: FBI CART case load exceeds 6500 cases, examining 782 terabytes of data

II. TYPES OF COMPUTER FORENSIC TECHNOLOGY

2.1 Disk Forensics

Disk forensics is the science of extracting forensic information from digital storage media like; Hard disk, USB devices, Firewire devices, CD, DVD, Flash drives, Floppy disks etc.. The process of Disk Forensics are:

1. Identify digital evidence
2. Seize & Acquire the evidence
3. Authenticate the evidence
4. Preserve the evidence
5. Analyze the evidence
6. Report the findings
7. Documenting

2.2 Tools Used in Disk Forensics

2.2[a] ADS LOCATOR

The ADS Locator can be used to locate files that have alternate ADS streams attached. ADS is a technology used to store additional data related to files, and has a lot of legit uses by the system. So this tool will only find those ADS entries that are of the user type "alternate," which is sometimes used by spyware, malware, and viruses.

Fig 1: Data Forensics

2.2[b] DISK INVESTIGATOR helps you to discover all that is hidden on your computer hard disk. It can also help you to recover

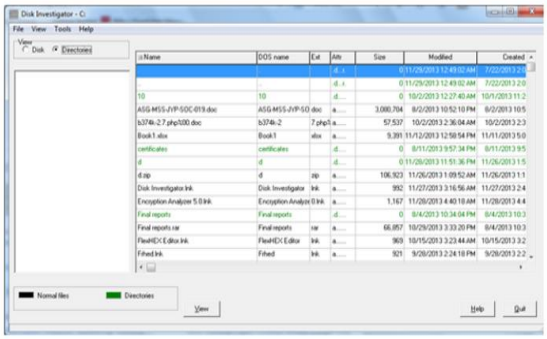

Fig 2: Disk Investigator

lost data. Display the true drive contents by bypassing the operating system and directly reading the raw drive sectors. It helps to view and search raw directories, files, clusters, and system sectors. Verify the effectiveness of file and disk wiping programs. Un-delete previously deleted files.

2.2[c] RECUVA is a free file recovery program that is capable of recovering lost or deleted files from local drives and external drives. The integrated wizard, guides users through the whole recovery process with ease. It also supports removable media such as smart media, secure digital cards, a memory stick, digital cameras, flash cards, and many more.

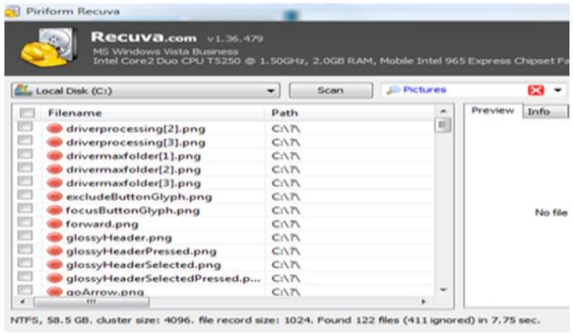

Fig 3: RECUVA

2.2[d] ENCRYPTED DISK DETECTOR (EDD) is a command-line tool that checks the local physical drives on a system for TrueCrypt, PGP or Bitlocker encrypted volumes. If no disk encryption signatures are found in the MBR, EDD also displays the OEM ID and, where applicable, the volume label for partitions on that drive, checking for Bitlocker volumes.

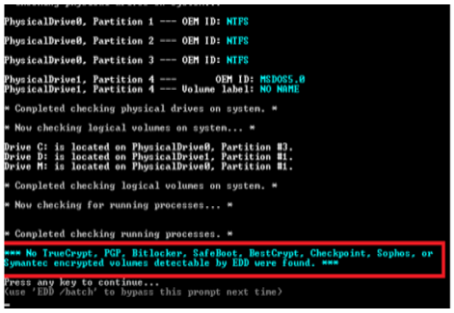

FIG 4: EDD

Encrypted Disk Detector is useful during incident response to quickly and non-intrusively check for encrypted volumes on a computer system. The decision can then be made to investigate further and determine whether a live acquisition needs to be made in order to secure and preserve the evidence that would otherwise be lost if the plug was pulled.

2.2[e] Password Encryption Manager

This tool scans a computer for password-protected and encrypted files, and reports encryption complexity and decryption options for each file. With EA you get all password recovery and decryption options that are available for the files and hard disk images of the cases you are investigating.

2.3 Network Forensics

Network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation. Network Forensic experts are not only hired by lawyers, rather their services are needed by insurance companies also to discover evidence to decrease the amount paid in an insurance claim. In addition, individuals may also hire Network Forensic experts to support a claim of wrongful termination, sexual harassment, or discrimination.

Network forensics generally has two uses. The first, relating to security, involves monitoring a network for anomalous traffic and identifying intrusions. An attacker might be able to erase all log files on a compromised host; network-based evidence might therefore be the only evidence available for forensic analysis. The second form of Network forensics relates to law enforcement. In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions.

III. MILITARY FORENSIC TECHNOLOGY

The directorate entered into a partnership with the National Institute of Justice via the auspices of the National Law Enforcement and Corrections Technology Center (NLECTC) located in Rome, New York, to test these new ideas and prototype tools. The Computer Forensics Experiment 2000 (CFX-2000) resulted from this partnership. This first-of-a-kind event represents a new paradigm for transitioning cyber forensic technology from military research and development (R&D) laboratories into the hands of law enforcement. The experiment used a realistic cyber crime scenario specifically designed to exercise and show the value added of the directorate-developed cyber forensic technology. XRY is designed to recover the contents of a device in a forensic manner so that the contents of the data can be relied upon by the user. Typically it is used in civil/criminal investigations, intelligence operations, data compliance and electronic discovery cases. XRY has been tested by various different government organizations as suitable tool to meet their requirements and is being used globally.

IV. AREA OF RESEARCH IN COMPUTER FORENSIC

1. Disk Forensics
2. Network Forensics
3. Mobile Device Forensics
4. E-Mail Forensic
5. Live Forensics.
6. Memory Forensics
7. Multimedia Forensics
8. Internet Forensics
9. Source and Object Code Forensics
10. System Development Forensics

V. COMPUTER FORENSIC COVERS

- ✓ Scoping and freezing the crime scene.
- ✓ Bit-wise imaging of all memory devices.
- ✓ Searching for un-erased data in temporary files, swap space, spool areas, slack space, etc., specifically the use of an EnCase Forensic demonstrator (EnCase, 2008).
- ✓ Scanning for the presence of Trojans, remote administration tools, root-kits, back-doors, etc.
- ✓ Checking system logs/audit trails for evidence of malfeasance.
- ✓ Performing internet trace-backs via ISP log-files
- ✓ Performing cyber-profiling
- ✓ Legal issues, The **Information Technology Act 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of

the Indian Parliament (No 21 of 2000) notified on October 17, 2000.

5.1 Real world cyber crime investigations in Computer Forensics:

- ✓ Income Tax Raid case
- ✓ Source Code theft case
- ✓ Digital Signature Fraud case
- ✓ Cyber Sabotage case
- ✓ Lottery Fraud case
- ✓ Social engineering and cognitive hacking
- ✓ Cyber-squatting
- ✓ Trojan horses
- ✓ Phishing attacks
- ✓ Commercial espionage and sabotage
- ✓ Biometrics: fingerprint analysis
- ✓ DNA cryptography
- ✓ Digital IPR and music piracy
- ✓ Cyber-stalking
- ✓ Anti-forensics
- ✓ Virtual crime
- ✓ Cognitive hacking pump-and-dump schemes
- ✓ Computer virtualization in forensic investigations
- ✓ Scams by cyber-criminals
- ✓ Motivation of malware creators
- ✓ Trends in cyber-warfare and national security in the internet age
- ✓ e-Banking fraud

VI. FORENSIC SYSTEM USED TOOLS

- ✓ Microsoft tools : TCPView, Sysinternals GUI, Sysinternals Terminal.
- ✓ Helix3 Forensics: live CD based on Ubuntu
- ✓ NirSoft tools : Freeware Utilities for Windows tools, ActiveXHelpe, IECookiesView, IEHistoryView, IEPassView, PNetInfo, Messenger Pass, Opened FilesView, ProduKey, RegScanner, ShellExView, USBDeview, Mail Pass View.
  Neuber : Pc On/Off Time tool.
- ✓ Encase
- ✓ Undeleteunerase : Recover Files tool.
- ✓ AccessData : The Forensic Toolkit Imager (FTK Imager) Lite
  Foundstone : Fport tool.
- ✓ Pyflag (forensic and log analysis GUI) : FLAG is advanced forensic tool for the analysis of large volumes of log files and forensic investigations. PyFlag is available under the terms of the GPL for anyone to use, modify and improve.
- ✓ WinAudit : Computer audit and inventory software.

VII. DISK IMAGING TOOLS IN COMPUTER FORENSIC

Forensics experts and companies have various terms and definitions for disk imaging as under:

Jim Bates, Technical Director of Computer Forensics Ltd. –

"An image of the whole disk was copied. This was regardless of any software on the disk and the important point was that the complete content of the disk was copied including the location of the data. Disk imaging takes sector-by-sector copy usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered. It does not necessarily need the same geometry as the original as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquired image."

Tech Assist, Inc. –

"Term given to creating physical sector copy of a disk and compressing this image in the form of a file. This image file can then be stored on dissimilar media for archiving or later restoration."

Into straightforward words, disk imaging can be clearly stated as to make a secure forensically salubrious copy to media that can conserve the data for extensive period. Disk imaging is also one of the stand-point for backup sans that backup only copies the active file. In backup, pervasive data will not be copied. This is a tract where the most crucial source for the evidence could be found. Vast data stored in Windows swap file, unallocated space and file slack. The outcome of the inquest also can be imitated to another media using disk imaging tool. A splendid imaging tool will not transform the prime evidence. It can copy entire knowhow from the drive and make the contents available for forensic analysis. Even pervasive data that is unapproachable to the residential of operating system will be copied. From the definition of the disk imaging, several disks imaging tool has been discovered. In 1991 the first imaging tool was sold by Computer Forensics Ltd and now it's sold under the trademark DIBS.

7.1 Examples of disk imaging tool:

The SC InfoSecurity Magazine(September 2000) has provide a report on forensic tools evaluation. They found that Linux dd, SafeBack and SnapBack DatArrest as the best product to do fast and completely accurate copying of hard disks.

7.2 Products Features Image file/internal verification, Imaged to appropriate media, Imaging SCSI / IDE drive, Copying sector-by sector / file-by-file.

1. Safe Back Version 2.0, CRC checksum, Hard drive, tape, removable media, IDE drive, Sector-by-sector.
2. SnapBack DatArrest Version 4.12, MD5 checksum, Hard drive, tape, removable media, SCSI drive, Sector-by-sector.
3. Linux "dd" Version 7.0, MD5 checksum, Hard drive, tape, removable media, SCSI drive and IDE drive,**S**ector-by-sector and file-by-file.
4. DIBS PERU (Portable Evidence Recovery Unit), DIVA, Optical media, SCSI drive and IDE drive, Sector-by-sector.

5. DIBS RAID (Rapid Action Imaging Device), DIVA, Optical media, SCSI drive and IDE drive, Sector-by-sector.

7.3 Career Prospectus:

1. Advisors to the web developers
2. Advisors in the Ministry of Information and Technology or Corporate Houses.
3. Cyber Consultant in an IT Firm, Police Department or in Banks.
4. Research Assistants in a Law firm.
5. Research Assistants in Technology firm.
6. Security Auditors and Network Administrators in Technology firms.
7. Trainers in law schools and Multinational Corporations.

V. CONCLUSION

In recent past there have been several cases of Computer Crime & Computer Hacking. To investigate such cases as well as to aware the users as how to be safeguard themselves from these attacks or to enhance knowledge, Computer Forensic is must. Computer Forensics experts are often called as "Cyber Cops", "Cyber Investigators" or "Digital Detectives". The cyber law market is growing fast and it will continue to grow manifold beyond imagination. Every individual is a potential victim to cyber crime. Everything is becoming cyber and the concerns of maintaining security of the information over the internet is also growing. Therefore, there are tremendous career opportunities in almost every field as already explained above. To sum up, Computer Forensic is a field which has a lot of scope for research besides providing a challenging career no limits for learning.

REFERENCES

[1]. Computer Forensics computer crime scene investigation,2nd edition by John R. Vacca
[2]. www.pc-history.org/forensics.htm
[3]. http://www.forensics-research.com/index.php/computer-forensics/computer-forensics-history/
[4]. Vanderburg, Eric and Liptak, John (Spring 2013). "Not without a trace: Uncovering computer forensic evidence". ABA Section of Science and Technology Law 4 (2): 13–19.
[5]. http://www.tripwire.com/state-of-security/incident-detection/free-computer-tools-disk-forensics-3/
[6]. http://www.cyberforensics.in/%28A%28YFMf49VLzAEkAAAAMWE3NDQ2ZTEtNjg5MC00Mjc5LWE0NjQtNTc2NDQxNjRlNTdhxwC8Rqlzd2-ICCb20r6htoqh1sI1%29%29/Research/DiskForensics.aspx?AspxAutoDetectCookieSupport=1
[7]. An overview of Disk Imaging Tool in computer forensics by Madihah. Mohd. Saudi.
[8]. Development of master modules in computer forensics and cybercrime for computer science and forensic science students by Richard E. Overill
[9]. Law,Investigations, And Ethics "Computer Forensics Today" by Kelly J.(KJ) Kuchta,2000
[10]. Policies to enhance computer and network forensics by Alec Yasinsac and Yanet Manzano,2001
[11]. The magazine of usenix and sage, The law Kenneally:Computer Forensics byErin Kenneally,2002
[12]. http://en.wikipedia.org/wiki/XRY_%28software%29
[13]. http://en.wikipedia.org/wiki/Information_Technology_Act_2000
[14]. http://en.wikipedia.org/wiki/Network_forensics