Comparative Study and Simulation of Digital Forensic Tools

Varsha Karbhari Sanap
Ramrao Adik Institute of Technology
Nerul, Navi Mumbai, India

Vanita Mane
Ramrao Adik Institute of Technology
Nerul,Navi Mumbai, India

ABSTRACT
The cyber crimes such as online banking fraud, credit card theft, child pornography, intellectual property theft, identity theft, unauthorized intrusion, money laundering, digital piracy etc. are growing rapidly with technology. Desktops, smartphones, laptops, digital cameras, GPS devices and even watches all can be used to aid a fraud. All this devices leave behind a digital footprint. Gathering electronic evidence and preserving it requires a special set of deliberations. Without a complete understanding of digital forensics, evidence could be compromise and which may cause evidence inadmissible in the court. To analyze the digital crime, the forensic technique is used. It is use to track where exactly the crime has been taken place and where the valuable data is hidden. To analyze the data and to recover the deleted or hidden data from the digital devices, the digital forensic tools are used. Paper presents the comparison of three digital forensic tools WinHex, Active file recovery, and ProDiscover Basic based on the parameters such as File examination, Log examination, Deleted File Indexing, Memory Dump Analysis, supported file systems, supported disk images.

Keywords
cyber crime; digital evidence; digital forensics; digital forensic tools

1. INTRODUCTION
As computers, networks and digital devices are used worldwide, the chances of cyber crimes which demand such devices and networks will increase.

In order to take actions against such crimes, first we need to gather evidence in adequate quantity to support any criminal or civil charges, and as the evidence will be in the digital form, it must be handled properly to maintain the integrity and value of the data so that the evidence will be admissible in court. Hence we need a deliberate, well planned process for collecting digital data in the first place; for that we require Digital forensics.

Digital forensics is the process of identifying preserving, analyzing and presenting digital evidence for a legal proceeding.

1.1 Basic Digital Forensic Investigation Process
Digital forensics is a comprehensive branch comprises branches like computer forensics. Computer forensics is defined as the collection, preservation, analysis, and court presentation of computer related evidence. Digital Forensic investigation process comprises the proper acquisition and preservation of computer evidence, authentication of collected data for court presentation, and recovery of available data including deleted files. This process has to go through three phases acquisition, analysis, reporting [1]. The basic digital forensic investigation process is shown in Fig. 1.

1.1.1 Acquisition
In this phase, the state of digital devices is saved so that it can be analyzed later. Forensic tools are used to copy all information from the suspect storage device to a trusted device. The contents and structure of a disk volume or entire data storage device are replicated. This process is known as imaging or cloning of disk.

1.1.2 Analysis
In this phase, deleted data is recovered using different methodologies to identify the digital evidence. Also slack space, hidden disk area, encrypted/protected data are analyzed for identification of evidence.

1.1.3 Reporting
To reorganize the actions and to accomplish conclusions, analysis of evidence is performed. After thorough investigation, investigator submits his data or information, generally in the form of a written report. A forensic examination report must list software used and their versions, the hash results, all storage media numbers, model, make. It must be in simple language and must be supported by photographs.

1.2 Digital Evidence
Digital evidence is important in the investigation of cybercrimes. Basically, computer forensics experts need digital evidence in cases involving data acquisition, preservation, recovery, analysis and reporting [8]. Sources of evidence are slack space, free space, swap memory, event logs, registry, application files, temp files, E-mail, browser history and cache, spool, recycle bin. The primarily goal of the investigation is to collect evidence using acceptable methods to make the evidence accepted and admitted in the court room for judgment. The final report of investigation should consist of four things: who did, what did, when did, how did.

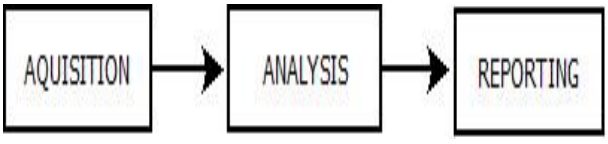

Fig. 1: Basic Digital Forensic Investigation Process

2. RELATED WORK
If crime is committed through any of the digital devices then events or evidence can be reconstructed using the technique introduced by Gulshan Shrivastava, Kavita Sharma and Akansha Dwivedi [1].

Sivaprasad, A., Jangale, S. [2] review the basic model for investigation and the tools and techniques for imaging of the

disk, investigating the registry content, checking the integrity of the disk image using hash code with the help of WinHex.

Raghavan, S., Raghavan, S.V. [3] present a systematic study of recent forensic and analysis tools using a hypothesis based review to identify the different functionalities supported by these tools.

3. FORENSIC TOOLS

Tools have made the investigation process as effective and efficient. The investigation process will take huge time to find the evidences; this has been made easy by the tools. As the features of the tools are increasing there are newer methods to do crime. It is similar to the virus and the anti-virus which is available in the current world [2].

Forensic image of the source is provided as input to all the forensic tools. And give binary abstraction to raw data which allows read whole source as a binary series of data [3].

Analysis tools are specialized for examining files, memory dumps, log files, network packet captures and so on. Some examples of such analysis tools are PyFlag for log files and network packet captures,Volatility, libevt GrokEvt, AWStats for web browser logs and Event Log Parser for Windows event logs, python-registry, RegRipper, Forensic Regisry Editor, Wireshark and tcpdump for network packet captures and Win32Registry for Windows Registry[4]. In this we will discuss three forensic tools WinHex, Active File Recovery, ProDiscover Basic.

3.1 WinHex

It is made by X-Ways Software Technology AG of Germany, is a powerful tool for data analysis, editing, and recovery [2]. WinHex is a global hexadecimal editor, useful in the field of computer forensics, low level data processing, data recovery, and IT security. It scrutinizes and edits all sorts of files, recover missing data or deleted files from digital devices. It supports FAT, NTFS, Ext2/3, ReiserFS, CDFS, UDF. It provides built-in interpretation of RAID systems and dynamic disks. Also it is a RAM editor, disk editor, data interpreter [5].

3.2 Active File Recovery

It is a data recovery tool which helps to retrieve files from formatted hard disks or partition. Also recovers data from the Recycle Bin in Windows which have been emptied. The software supports all digital devices used by Windows, Macintosh or Linux. The latest edition has significantly faster scan times due to the 64-bit executable version. It scans faster due to the more processing power and memory. Version 12 of active file recovery supports file signatures for files of rarer types in addition to the dozen of file signature of older version. Files may also be sorted based on different kinds of attributes [6].

3.3 ProDiscover Basic

The ARC Group ProDiscover Basic edition is a forensic tool used for the examination of hard disk security. It has a built-in reporting tool to present findings as evidence for legal proceedings. It helps to gather time zone data, drive information, Internet activity. It has robust search capabilities for capturing unique data, file names and file types, data patterns, date ranges, etc. [7]. It allows content view and cluster view of data.

4. CASE STUDY

Pornography Case: M/s. Jonson Corp. has complaints from staff officials about one of the young employee Mr. John for misuse of computer system. Company has a doubt that he is using the computer system for viewing and downloading of pornographic images. Company approaches us as cyber crime investigator to find the evidence against him. During search of physical material from his drawer we found one floppy disk of 1.44 mb capacity, John/bootable is written on the label of floppy disk. Investigate.

In general, the cyber crime investigator follows the following steps for investigation:

Step 1: Take permission from authority to search and seize.

Step 2: Secure the crime scene.

Step 3: Document the chain of custody of every item that was seized.

Step 4: Acquire the digital evidence from the device by using forensically sound methods and tools to create a forensic image of the evidence. Before creating the image of the digital evidence, calculate the hash value of it for authenticity.

Step 5:Examine and analyze the forensic image of the evidence. Don't use original evidence for analysis to maintain the integrity of the evidence.

Step 6: Describe the analysis and findings in clearly and easy-to-understand written report.

Above mentioned steps of cyber crime investigation are followed for investigating this pornography case.

4.1 Case study solved using WinHex

Steps involved:

Step 1: Maintain chain of custody of evidence which is floppy disk in this case.

Step 2: Calculate md5 hash value of floppy disk. Copy this hash value in new file with date and time for record.

Step 3: Create image of floppy disk using WinHex.

Step 4: Recover data from the floppy image. To recover data from image select 'file recovery by type' option. Then select output folder to save recovered data.

Step 5: File carving: we found one database file after recovery. Now to recover the images we need to do file carving. Open found database file in WinHex then search for the header FFD8 and mark F as Beginning of block. Similarly search for the footer FFD9 and mark 9 as End of the block. Now, edit the block and copy it into a new file. Save it as a jpeg file.

Step 6: The recovered image which was deleted from the floppy disk is shown in figure 2.

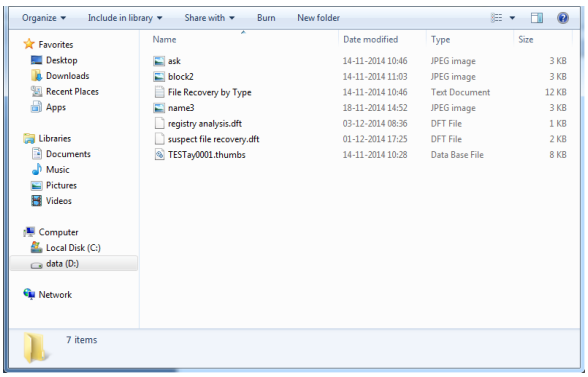

Fig 2: Recovered files using WinHex

4.2 Case study solved using Active File Recovery

Steps involved are as follows:

Step 1: Maintain Chain of Custody. And calculate the hash value of image.

Step 2: Open disk image in active file recovery tool.

Step 3: Then scan the disk image. And the files will be recovered from the disk image. There are two options in this tool for scanning QuickScan and SuperScan We can perform any one of them based on our requirement.

Step 4: Recovered image is shown in fig. 3.

4.3 Case study solved using ProDiscover Basic

Steps involved are as follows:

Step 1: Launch ProDiscover Basic. Enter project number and project file name which creates the project.

Step 2: Add image file.

Step 3: In the left pane, there is option content view. Click plus sign to expand images.

Step 4: Click on the image to view the content. Then in the right pane, we can see the content of the disk image. We can the two .BEAUTY1.jpg and BEAUTY2.jpg files which were deleted from the floppy disk. Refer figure 4.

Step 5: Recovered files are shown in fig. 4.

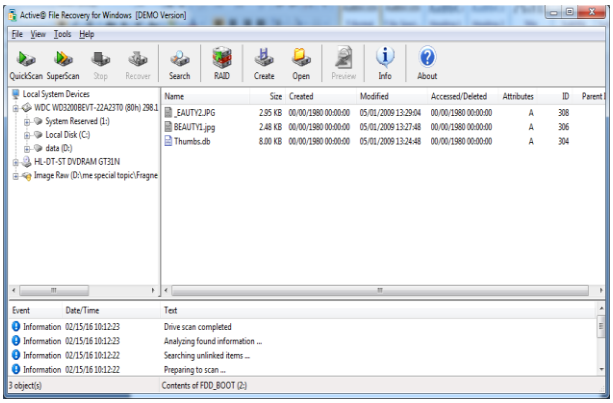

Fig 2: Recovered files using Active File Recovery

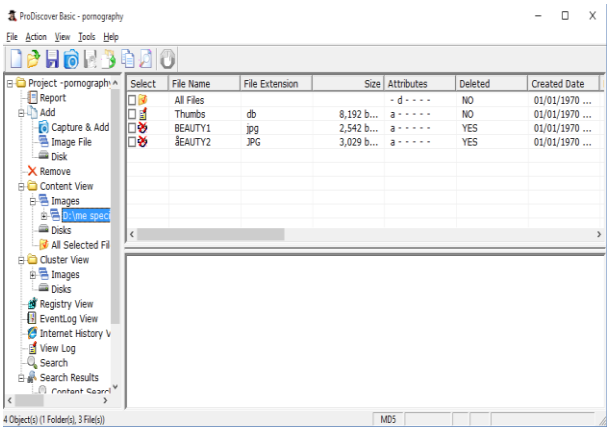

Fig 2: Recovered files using ProDiscover Basic

5. COMPARISON AND ANALYSIS

Comparative study of WinHex, Active File Recovery and ProDiscover is shown below in Table I. This Table 1 compares the tools based on the parameters such as File system supported by these tools, disk image formats supported by tools for storing evidence, examination and analysis.

From above simulation results it has been analyzed that WinHex is one of the best tool for low level editing of data. Using WinHex the files can be analyzed to determine the type of data recovered.

Active file recovery tool is one of the best tools for data recovery. It recovers the lost files and directories. It supports almost all file systems, storage devices. It can recover data from large drives having size more than 2 terabytes. It allows recovering files by file signatures.

Table 1. Comparative study of Digital Forensic Tools

Parameters	WinHex	Active File Recovery	ProDiscover Basic
Supported File System	FAT12/16/32, NTFS, Ext2/3, ReiserFS, CDFS, UDF	NTFS/NTFS5/NTFS+EFS, FAT12/16/32, exFAT, HFS+, Ext2/3/4/BtrFS, FreeBSD Unix UFS, CD/DVD/Blue-ray UDF, ISO9600	FAT 12/16/32, NTFS, Solaris UFS, CD/DVD
Supported Disk Images	Raw DD	Raw DD, DIM(Active File recovery's own format)	Raw DD, eve(ProDiscover's own format)
File Examination	Yes	Yes	Yes
Log Examination	Yes	Yes	Yes
Deleted File Indexing	No	Yes	Yes
File Indexing	Yes	Yes	Yes
Memory Dump Analysis	Yes	Yes	Yes

Active file recovery tool can recover the files even though files are deleted from the recycle bin. It recovers the files damage by virus attacks, lost due to accidental disk formatting, power failure, or malicious program, photos and pictures lost after formatting Memory Card or deleted from a USB flash.

ProDiscover Basic provides hard disk security examination. It gives details about what happens with every cluster of hard disk. It automatically analyze the system volume information. It generates report automatically along with required information to be submitted as evidence in legal proceedings.

6. CONCLUSION

This topic presents discussion of digital forensics, need of digital forensics, digital forensic process, digital evidence and digital data. In this study, three digital forensic tools WinHex, Active file recovery, ProDiscover Basic has been compared

on basis of parameters such as supported disk images, supported file systems, file examination, log examination, deleted file indexing, file indexing, memory dump analysis and performed simulation using the mentioned tools. A case study on pornographic case is investigated. The mentioned tools recovered the deleted data from the evidence by following digital forensic process. Each tool has its own advantage and disadvantages which are discussed in various sections. The selection of tool is depending on the application and requirement.

7. REFERENCES

[1] Gulshan Shrivastava, Kavita Sharma, Akansha Dwivedi, 2012. Forensic Computing Models: Technical Overview, CS and IT-CSCP, 2012.

[2] Sivaprasad A., Jangale S., 21-22 March 2012. A complete study on tools and techniques for digital forensic analysis,Interntional Conference on Computing, Electronics and Electrical Technologies (ICCEET), vol., no., pp.881-886.

[3] Raghavan S., Raghavan S. V.,21-22 Nov 2013 A study of forensic and analysis tools," International workshop on Systematic Approaches to Digital Forensic Engineering(SADFE), vol., no., pp. 1,5.

[4] K. K. Sindhu, B. B. Meshram, 2012. Digital Forensics and Cyber Crime Data Mining, Journal of Information Security, 3, 196-201.

[5] Winhex tool, Download tool from: http://www.x-ways.net/winhex/

[6] Active file recovery tool, Download tool from: http://www.file-recovery.com/

[7] ProDiscover Tool, Download tool from: http://www.arcgroupny.com/product/prodiscover-basic/

[8] Sunit belapure, Nina Godbole, "Cyber Security: Understanding cyber crimes, computer forensicsand legal perspectives," First Edition, Wiley India.