# DIGITAL FORENSIC TOOLS: A COMPARATIVE APPROACH

**Dhwaniket Ramesh Kamble[1], Nilakshi Jain[2]**

*[1,2]Faculty of Information Technology, Shah and Anchor Kutchhi Engineering College, University of Mumbai, (India)*

## ABSTRACT

*Digital forensic is part of forensic discipline that absolutely covers crime that is related to computer technology. A key or an important factor of digital investigation process is that, it is capable to map the events of an incident from different sources in obtaining evidence of an incident to be used for other secondary investigation aspects. Due to the application of computer used to investigate computer-based crime, has led to development of a new field called Digital forensics. Digital Forensic provide foundation and new ideas for the betterment and understanding the concepts. This paper studies the comparative approach of the digital forensic tools, its origins, its current position and its future directions.*

***Keywords : Integrated Digital Forensic Process Model, Award Key Logger, Recuva, OpenPuff, WinHex.***

## I. INTRODUCTION

The field of digital forensics has become increasingly more important over the last few years as both the computer and the cellular market has grown. Digital forensics describes the process of going into a technological device such as a computer or a cell phone in order to monitor the activity on these items and determine if the item has been hacked previously and/or is being watched. We may think that we don't have much to hide on your technological device, so this warning need not apply to us. But just because we have hit a 'delete' button doesn't mean that a good hacker can't find a copy of it somewhere on our machine. Computers can yield evidence of a wide range of criminal and other unlawful activities, criminals engaged in network-based crimes are not the only ones who store information on computers. Many criminals engaged in murder, kidnapping, sexual assault, extortion, drug dealing, auto theft, espionage and terrorism, gun dealing, robbery/burglary, gambling, economic crimes, confidence games, and criminal hacking e.g. Web defacements and theft of computer files, maintain files with incriminating evidence on their computer. Sometimes the information on the computer is key to identifying a suspect and sometimes the

computer yields the most damning evidence.The use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.[1] A digital forensic investigation process[1] is a special case of a digital investigation where the procedures and techniques that are used will allow the results to be entered into a court of law. For example, an investigation may be started to answer a question about whether or not illegal imports digital images exist on a computer.

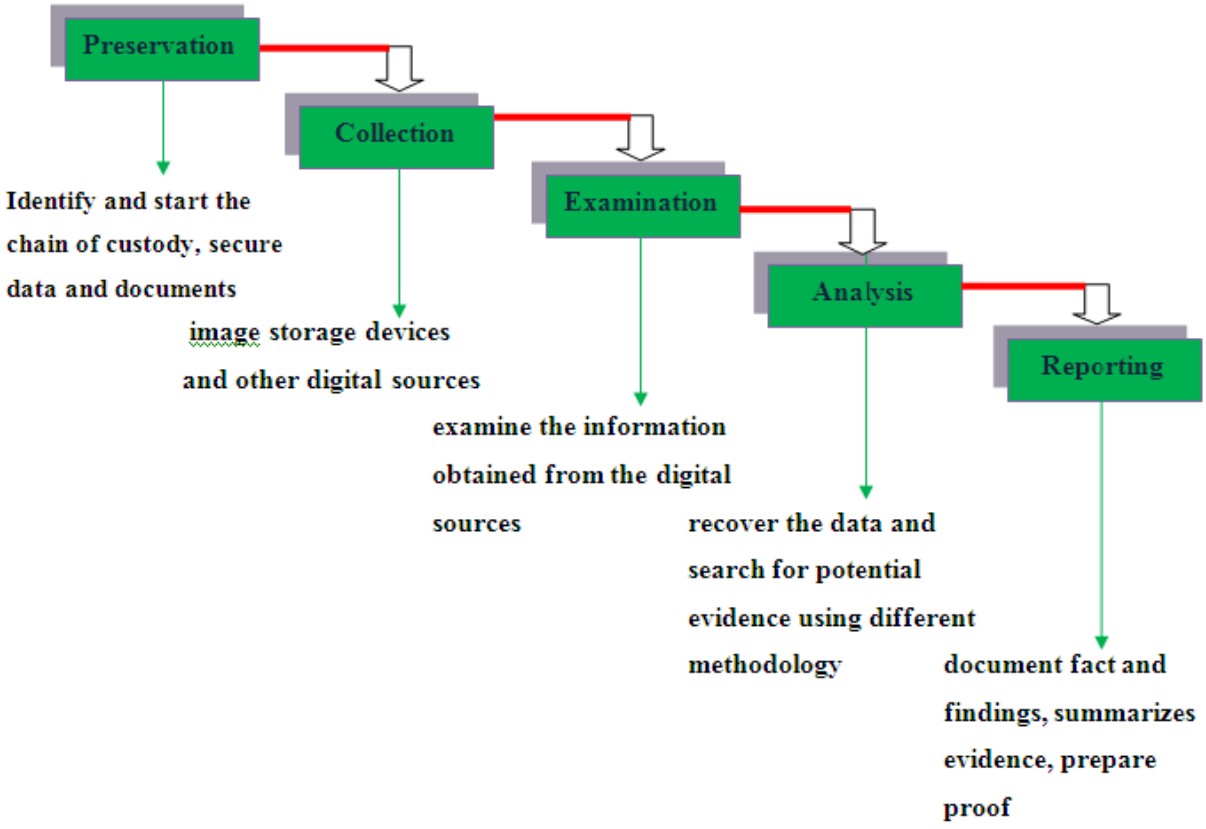


**Fig.1 Digital Forensic Investigation Process[1]**

The process is mainly used in computer and mobile forensic investigations and consists of five steps which are listed below[1]:

- **Preservation:** Preserving digital evidence early, is a critical first step toward increasing our chances of a successful investigation, litigation, or incident response.

- **Collection:** Since digital information is stored in computers, collection of digital information means either collection of the equipment containing the information, or recording the information on some medium.
- **Examination:** Examination is best conducted on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence.
- **Analysis:** During the analysis an investigator usually recovers evidence material using a number of different methodologies (and tools), often beginning with recovery of deleted material.
- **Reporting:** When an investigation is completed the information is often reported in a form suitable for non-technical individuals. Reports may also include audit information and other meta-documentation.

## II. DIGITAL FORENSIC: A BRIEF HISTORY

Prior to the 1980s crimes involving computers were dealt with using existing laws. The first computer crimes were recognized in the 1978 Florida Computer Crimes Act, which included legislation against the unauthorized modification or deletion of data on a computer system. Over the next few years the range of computer crimes being committed increased, and laws were passed to deal with issues of copyright, privacy, harassment e.g., cyber bullying, cyber stalking, and online predators and child pornography. It was not until the 1980s that federal laws began to incorporate computer offences. Canada was the first country to pass legislation in 1983. Throughout the 1990s there was high demand for these new, and basic, investigative resources.Since 2000, in response to the need for standardization, various bodies and agencies have published guidelines for digital forensics. A European lead international treaty, the Convention on Cybercrime, came into force in 2004 with the aim of reconciling national computer crime laws, investigative techniques and international co-operation.

The treaty has been signed by 43 nations (including the US, Canada, Japan, South Africa, UK and other European nations). A February 2010 report by the United States Joint Forces Command concluded that through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In 2010 Simon Garfunkel identified issues facing digital investigations in the future, including the increasing size of digital media, the wide availability of encryption to consumers, a growing variety of operating systems and file formats, an increasing number of individuals owning multiple devices, and legal limitations on investigators[2].

### 2.1. IDFPM Framework

Integrated Digital Forensic Process Model consist of following processes: Preparation, Incident, Incident response, Physical Investigation, Digital Forensic Investigation, Presentation and the processes are performed by qualified personnel.[2] The documentation process is included in the IDFPM as a continuous process. The documentation process includes investigation on documents and chain of custody recorded as accurately as possible in the entire investigation. The infrastructure and operational readiness process is also a process that occurs in parallel.

- **Preparation:**

  This is encapsulated process by stating that forensic readiness has two main objectives, firstly to maximize the collection of credible digital evidence from an incident environment, and secondly to minimize the cost of a forensic incident response. Any defects may be exploited during presentation of the digital evidence findings.

- **Incident:**

  An incident may be detected by an automated incident detection system, or a similar set of event sequences is recognized by an investigator, based on possible previous experience. Incidents are often detected secretly and dealt with secretly within an organization. In these instances it is imperative that the organization's policies and procedures are studied to determine any possible investigative limitation.

- **Incident Response:**

  Depending on the type of investigation, witnesses need to be safeguarded, suspects need to be detained as soon as possible after arrival and potential evidence must be secured. The first responder is the first custodian to maintain the chain of evidence and custody of potential digital evidence. The first responder must be able to accurately describe the scene in the initial drafting of documentation; these include photographs, video and sketches.

- **Digital forensic Investigation:**

  The physical investigation process occurs in parallel with the digital investigation if the crime is not isolated to the digital space. The focus of the physical investigation is to analyze DNA, fingerprints and other possible physical evidence obtained from the incident scene.

- **Presentation:**

  Based on the presentation report, a decision is made regarding the person to whom the incident can be attributed. The decision must be recorded in some database for future reference. All other relevant documentation that was compiled during the investigation and that might be relevant in reaching a decision is included in the final presentation report. The legal processes of court case, if applicable, will become the focus of the processes that follow.

## 2.2 Study of Tools

Tools are the predefined software or methods which are available for application of digital forensic.

Some of the following tools are listed below:

- **FTK (Forensic Toolkit)**[6][7]

IT is an advanced Code Breaking and Password Recover. This tool is full Unicode and provides code Page Support. It also gives advanced Email support. Powerful Search Functionality. Registry Supplemental Reports are provided by FTK. It is very easy to use as interface.

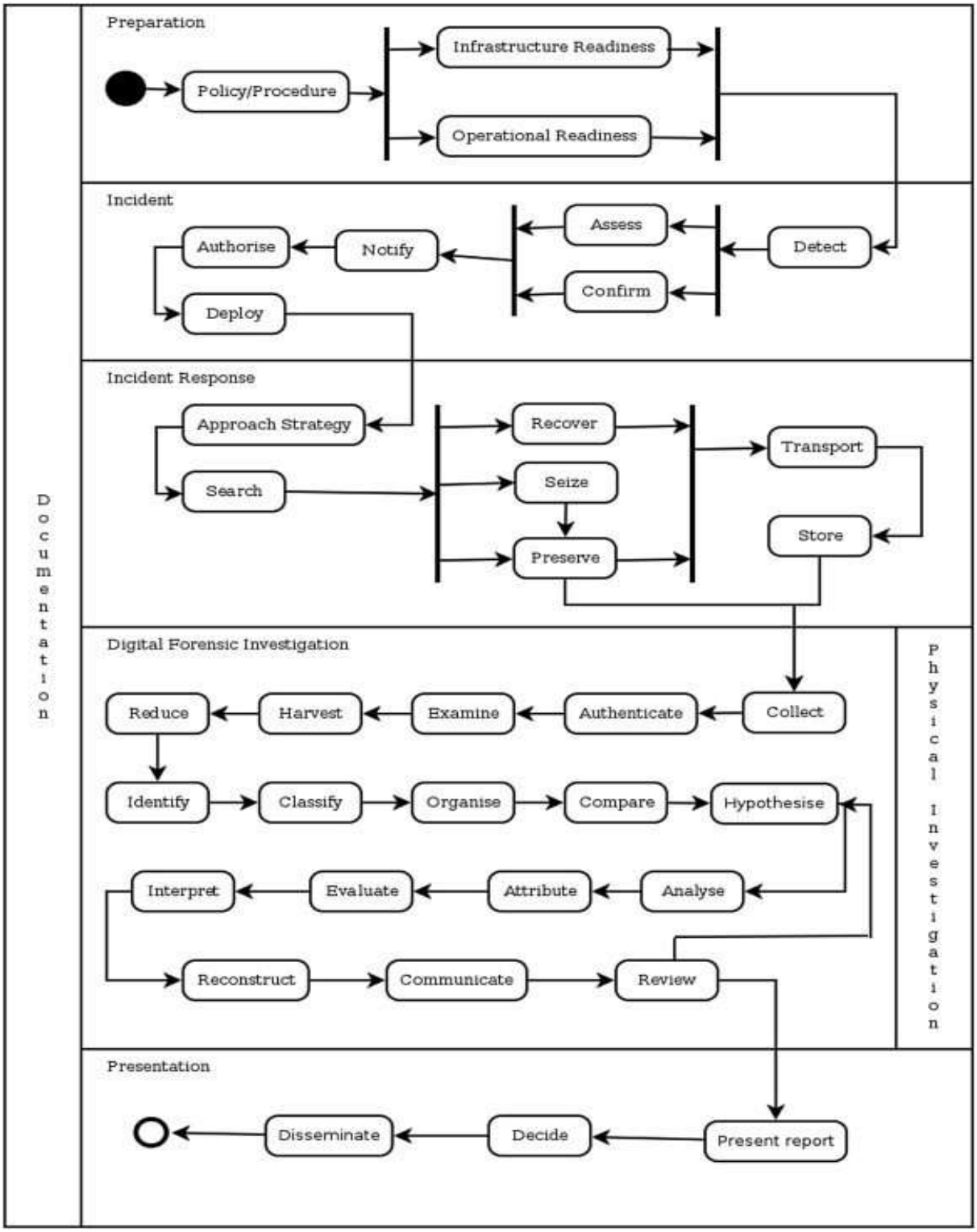


**Fig.2 Integrated Digital Forensic Process Model Framework [2]**

- **Encase**[6][7]

It securely investigate/analyze many machines simultaneously. Limit incident impact and eliminate system downtime with immediate response capabilities. Investigates and analyze multiple platforms. Efficiently collect only potentially relevant data. Audit large groups of machines for sensitive or classified information. Identify fraud, security events and employee integrity issues.

- **Sleuthkit**[7]

Collection of UNIX-based command line file and volume system forensic analysis tools. Analyzes raw, Expert Witness (i.e. Encase) and AFF file system and disk images. Various analysis Techniques-meta-data structure analysis, time line generation, sort files based on their types etc.

- **Autopsy**[7]

It is a GUI for Sleuthkit[7]. Dead analysis and live analysis is done with the help of autopsy. Case management using client server model. Various analysis Techniques-meta-data structure analysis, keyword search, time line generation, sort files based on their types etc.

- **FIT4D (Forensic Investigation Toolkit 4 Developing countries):**

A software toolkit utilizes the limited resources in developing countries. Improves the efficiency, privacy and usability. Addresses the problem of lack of forensic experts in developing countries. A low-cost, distributed infrastructure to deploy the FIT4D software toolkit.

## III. PRESENT INVESTIGATION

There are two fundamental problems with the design of today's computer forensic tools:

- Today's tools are designed to help examiners find specific pieces of evidence, not to assist in investigations.[8]
- Today's tools are created for solving crimes committed against people where the evidence resides on a computer, they were not created to assist in solving typical crimes committed with computers or against computers.[8]

Digital forensics tools play a critical role in providing reliable computer analysis and digital evidence collection to serve a variety of legal and industry purposes. These tools are typically used to conduct investigations of computer crimes by identifying evidence that can be used in a court of law. In addition to criminal investigation, these same tools are used for purposes of maintenance, debugging, data recovery, and reverse engineering of computer systems in private settings. Digital forensics tools are designed for use by forensics investigators. It is important to consider the background, computer expertise, workflow, and practices of these users. [7]

Suppose we consider five tools which are used presently.

### 3.1 Award Key Logger[4]

Award Key logger[4] is a program for tracking key presses on a keyboard. The program is an easy-to-use surveillance tool, and its invisibility can find out what other people do with your computer while we are away. Award Key logger[4] records every keystroke to a log file, which will reflect everything that is typed (Google searches, visited sites, etc. ) during your absence. The program can send the log files secretly by email or FTP to a specific receiver. On the other hand, the program can also detect specific keywords and take a screenshot whenever one is typed.

### 3.2 Recuva

Recuva is an important file recovery[3] software used to back up deleted file data information accidentally done by the user from their Windows PC, recycle bin or from an MP3 player. Everyone of us has witnessed the problem of accidentally deleting files containing some useful information from their computer.

But what if, that file is permanently deleted from the hardware of the system? We may have come across the situation on our Windows PC where we delete files from your computer, delete all the necessary rubbish from your Recycle Bin and start to wonder did you mistakenly deleted our most important file for our office or personal use? All these questions have one solution - Recuva. Even if we delete a particular file, we can undo the same from our recycle bin.

### 3.3 USBDeview[6]

USBDeview[6] is a small utility that lists all USB devices that currently connected to your computer, as well as all USB devices that you previously used. For each USB device, extended information is displayed: Device name/description, device type, serial number (for mass storage devices), the date/time that device was added, VendorID, ProductID, and more.

USBDeview[6] also allows you to uninstall USB devices previously used, disconnect USB devices that are currently connected to your computer, as well as to disable and enable USB devices. We can also use USBDeview[6] on a remote computer, as long as you login to that computer with admin user. USBDeview[6] is a free application for Windows computers that provides a useful tool for USB devices plugged to Windows-based computers.

### 3.4 WinHex

WinHex is in its core a universal hexadecimal editor, particularly helpful in the realm of computer forensics, data recovery[3], low-level data processing, and IT security. An advanced tool for everyday and emergency use, inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards.

### 3.5 OpenPuff[5]

OpenPuff is a professional steganography tool, with unique features we won't find among any other free or commercial software.[5] OpenPuff is 100% free and suitable for highly sensitive data covert transmission.[5] OpenPuff[5] is used primarily for anonymous asynchronous data sharing, i.e. the sender hides a hidden stream inside some public available carrier files (password + carrier files + carrier order are the secret key) and the receiver unhides the hidden stream knowing the secret key.

**Table 3.1 Comparison of considered tools on the basis of features**

| | **Award Key Logger** | **Recuva** | **USBDeview** | **OpenPuff** | **WinHex** |
|---|---|---|---|---|---|
| **Software License** | Commercial | Freeware | Freeware | Freeware | Commercial |
| **Platform Support** | Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, Windows NT4, Windows ME, Windows 98 | Windows 7 (32 bit), Windows 7 (64 bit), Windows 8, Windows Vista (32 bit), Windows Vista (64 bit), Windows XP | Windows 7 (64 bit), Windows 8, Windows Vista (64 bit) | Windows 7 (32 bit), Windows 7 (64 bit), Windows Vista (32bit), Windows Vista (64bit), Windows XP | Windows 7 (32 bit), Windows 7 (64 bit), Windows 8, Windows Server, Windows Vista (32bit), Windows Vista (64bit), Windows XP |
| **Developer** | Award-soft | Piriform | NirSoft | EmbeddedSW | X-Ways Software Technology AG |

| | | | | | |
|---|---|---|---|---|---|
| **Performance** | High | Less | High | High | High |
| **Cost** | 15237 INR | Free | Free | Free | 15486 INR |
| **Purpose of Utilization** | Both Good and Bad | Good | Good | Both Good and Bad | Both Good and Bad |

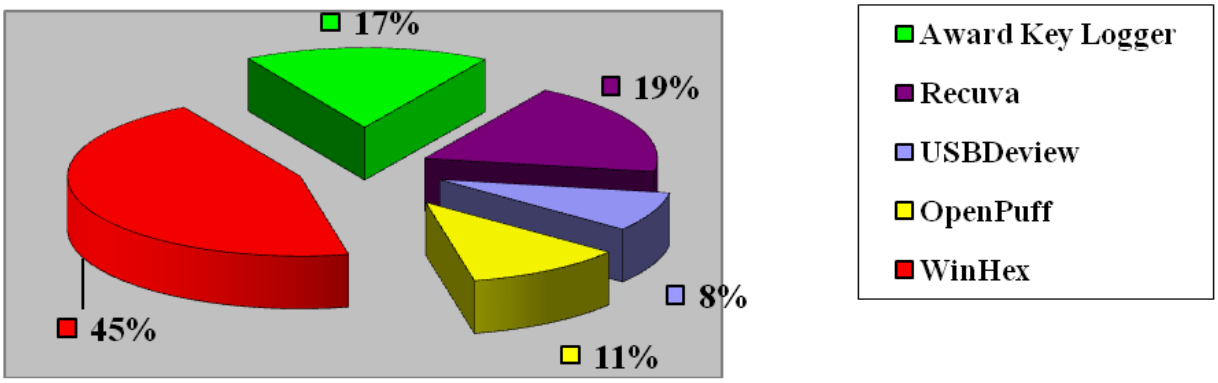


**Fig.3 Utilization of Tools in terms of percentage**

**Table 3.2 Comparison of considered tools on the basis of Digital Forensic Investigation Process**

| | **Preservation** | **Collection** | **Examination** | **Analysis** | **Reporting** |
|---|---|---|---|---|---|
| **Award Key Logger** | **Yes** | **Yes** | **Yes** | **No** | **Yes** |
| **Recuva** | **Yes** | **Yes** | **No** | **Yes** | **Yes** |
| **USBDeview** | **Yes** | **Yes** | **No** | **No** | **No** |
| **WinHex** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** |
| **OpenPuff** | **No** | **No** | **Yes** | **No** | **Yes** |

**Table 3.3 Comparison of considered tools on the basis of IDFPM Framework**

| | Preparation | Incident | Incident Response | Digital Forensic Investigation | Presentation |
|---|---|---|---|---|---|
| **Award Key Logger** | ✓ | ✓ | × | ✓ | ✓ |
| **Recuva** | ✓ | × | ✓ | ✓ | ✓ |
| **USBDeview** | ✓ | ✓ | × | ✓ | × |
| **WinHex** | ✓ | ✓ | ✓ | ✓ | ✓ |
| **OpenPuff** | ✓ | ✓ | × | × | ✓ |

- **Justification for the Difference:**

The Comparison is done among five tools which are Award Key Logger[4], Recuva, USBDeview[6], OpenPuff[5] and WinHex. As we compare our tools on the basis of feature, investigation process and IDFPM[2] model framework we notice that among the five tools WinHex is said to be the better tool. WinHex not only has all five properties of Investigation process but also has the properties defined in the IDFPM[2] process. WinHex is an advanced tool for everyday and emergency use which inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems, data wiping and disk cloning. WinHex also analyzes the data and compares the file. So in comparison among other five tools, WinHex is the best in terms of utilization, characterization and performance.

## IV. RESULTS AND DISCUSSIONS

Computer related crime is growing as fast as the Internet itself. Today, enterprises focus on implementing preventative security solutions that reduce vulnerabilities, with little concern for systematic recovery or investigation. We have reviewed the literatures in Digital forensics and identified three main categories of activity in Digital forensics. The three research categories are framework, Digital forensics Investigation process, and Tools. The advances such as framework, process and tools of Digital Forensic have been reviewed and discussed. We

should not leave everything to Digital forensics experts. If we are going to find a solution to the computer crime problem, it will be through a collaborative effort. Everyone from individual users, to company owners have to get involved. The considered tools, investigation process, and the framework, enhance the forensics of computer security by helping experts in the field do their job faster and more efficiently. It is up to the companies and users to adopt these policies according to their needs.

## V. FUTURE SCOPE

A multidisciplinary approach is required to fully foresee the future of cybercrime forensics. The most obvious change will be in the type, size and speed of storage media, memory, and processors. In the next 5 years, standard computers will come with 5TB of storage while flash drives will carry 250 GB of data. Thus, there will a significant greater amount of data to sort through than there is today. However, computers will become up to 7 or 8 times faster (this is not even considering the development of quantum computing). The forensics field will broaden in terms of expertise. Forensics tools will advance, developing the ability to automate data collection and preliminary processing. This means that less-trained people will be able to use forensics tools. However, computers themselves will probably evolve to a complexity that we are not used to, being able to understand human speech and make rational decisions. Thus, the future expert forensics examiner will need to specialize even further, to deal with the sophisticated knowledge needed to handle software and hardware.

## VI. CONCLUSION

This paper results to provide strong evidence that current digital forensics tools are not considered user-friendly and that they lack intuitive interfaces. It is a challenge for investigators to directly find answers to their high level, case-related questions. Usability is a critical issue in the tools because misunderstanding that leads to false interpretations may impact real-life cases. Computer forensics is a vital part of the computer security process. As more knowledge is obtained about how crimes are committed with the use of computers, more forensic tools can be fine tuned to gather evidence more efficiently and combat the crime wave on technology. Digital forensics is important for solving crimes with digital devices, against digitial devices, against people where evidence may reside in a device. Several sound tools and techniques exist to search and analyse digital data. Regardless of existing tools, evolving digital age and development of technology requires heavier research in digital forensics. This paper discussed a number of important definitions that are connected to a digital forensic investigation, definitions for digital forensic and Integrated Digital Forensic Process Model[2] Framework. We also have reviewed in Literature survey that the Integrated Digital Forensic Process Model[2] is standardized after considering all the process descriptions as discussed previously. We conclude that we studied a detailed comparative approach of Digital Forensic Tools and also guarantee that the future research should sample a larger number of respondents, collect detailed demographics information and not only look at identifying issues, but also obtain feedback on methods for addressing the issues.

## VII. ACKNOWLEDGMENT

I would like to sincerely thank Assistant Prof. Nilakshi Jain for her advice and guidance at the start of this article. Her guidance has also been essential during some steps of this article and her quick invaluable insights have always been very helpful. Her hard working and passion for research also has set an example that I would like to follow. I really appreciate her interest and enthusiasm during this article. Finally I thank the Editor in chief, the Associate Editor and anonymous Referees for their comments.

## REFERENCES

[1] Ravneet Kaur, Amandeep Kaur, *Digital Forensics*. International Journal of Computer Applications, *Volume 50 – No.5*, India (2012).

[2] M.D. Kohn, M.M. Eloff, J.H.P. Eloff, *Integrated digital forensic process model*. computers & security 38, *pp. 103-115*, South Africa (2013).

[3] Arvind Kumar,Sunil Kumar Sahu,Saurav Tyagi,Vikas Sangwan, Prof. Rupali Bagate, *Data Recovery Using Restoration Tool*. International Journal of Mathematics and Computer Research, *Volume 1 issue 3, pp. 119-122*, Pune, India (2013).

[4] Preeti Tuli, Priyanka Sahu, System, *Monitoring and Security Using Keylogger*. International Journal of Computer Science and Mobile Computing, *Vol. 2, Issue. 3,pp. 106-111*, Chhattisgarh, India (2013).

[5] Michael Chesbro, *OpenPuff Steganography & Watermarking Tool*, CCIA, CCIP (2014).

[6] Mark Simms, *Portable Storage Forensics: Enhancing the Value of USB Device Analysis and Reporting* (2012).

[7] Hanan Hibshi, Timothy Vidas, Lorrie Cranor, *Usability of Forensics Tools: A User Study*. Sixth International Conference on IT Security Incident Management and IT Forensics, USA (2011).

[8] Simson L. Garfinkel, *Digital forensics research: The next 10 years*. Digital investigation 7, *pp.S64-S73*, USA, (2010).