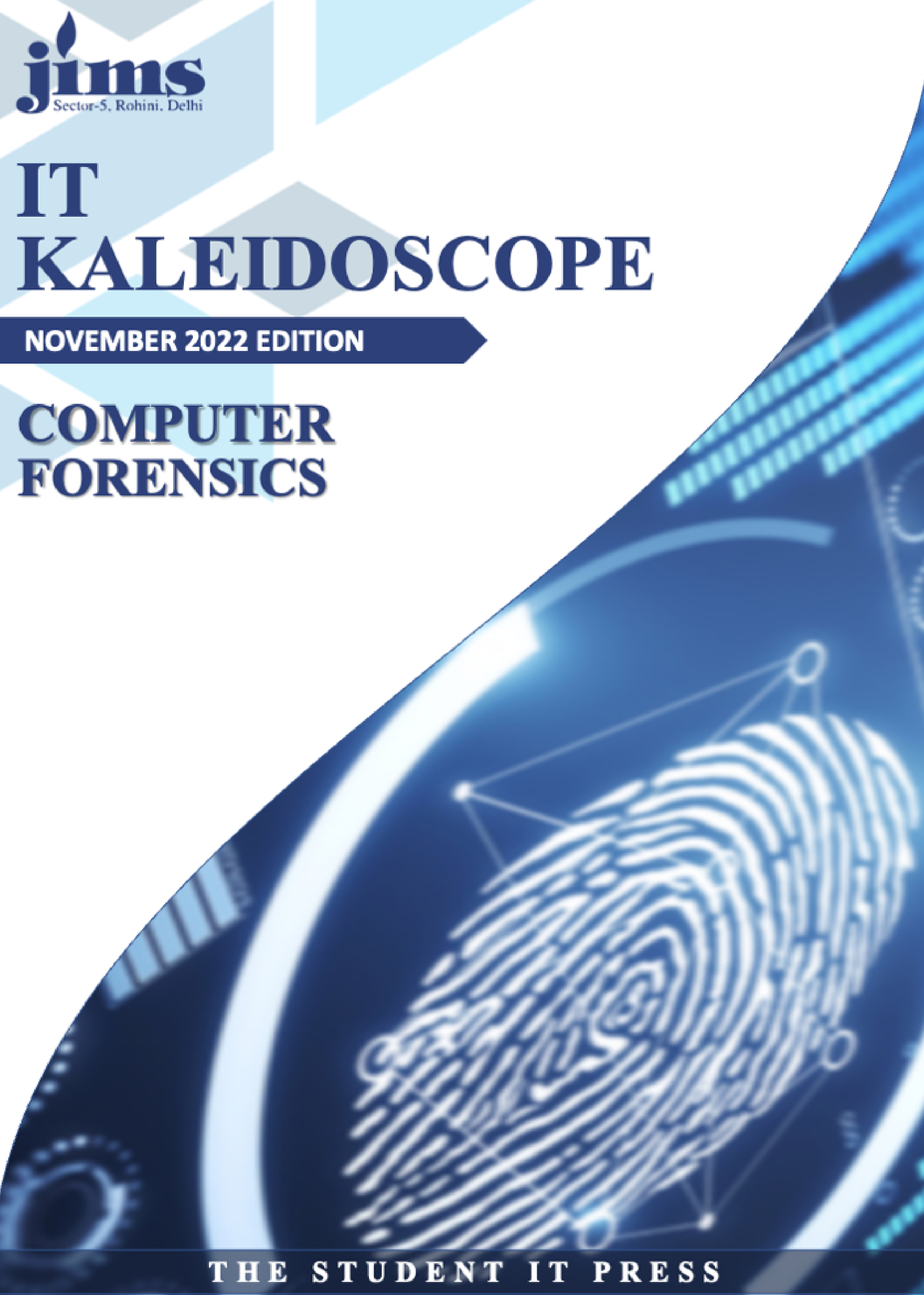
jims
Sector-5, Rohini, Delhi

IT KALEIDOSCOPE

NOVEMBER 2022 EDITION

COMPUTER FORENSICS



THE STUDENT IT PRESS

jims
Sector-5, Rohini, Delhi

STUDENT'S IT PRESS

IT KALEIDOSCOPE

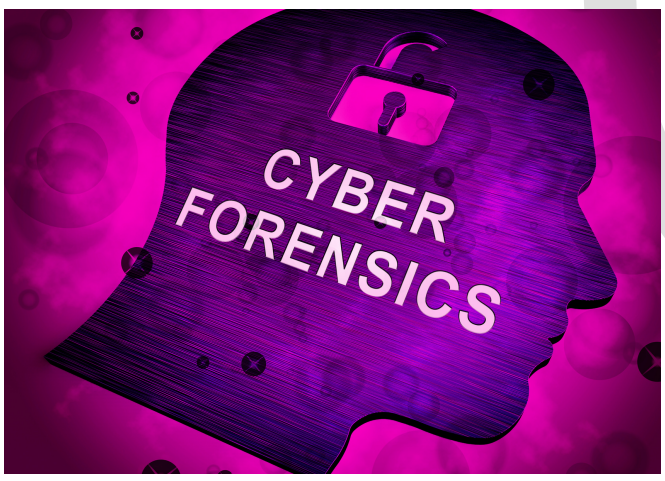
THEME: COMPUTER FORENSICS

NOV 2022 EDITION

Introduction to Computer Forensics:

Computer Forensics (also known as cyber forensics or computer forensics science) is a branch of digital forensics, which deals with examination of the digital media. It is responsible for identifying, preserving, recovering, analysing, and presenting the facts about digital information. It is mainly associated with serious crimes, like child pornography, online scams, cyber-crimes, frauds, murders, etc.

Before 1980s, computers were not accessible to many people. But after early 80s, personal computers became a common thing of daily use by common public. As a result of this, the cyber-crimes also increased as the hackers saw this as a good opportunity to extract ransom or money, or commit some other kind of fraud with the users.



Types of Computer Forensics:

Computer forensics can be of various types, each one dealing with a specific aspect of information technology. its main types are:

Database Forensics: Database forensics relates to the study of databases and some of the related metadata. It follows the normal forensics method and also investigates the database contents and metadata.

Email Forensics: Email forensics offers the recovery and analysis of emails and other information contained in email platforms. It analyses the email and its content to determine its legitimacy, sender, recipient, date, time, and other information regarding the mail.

Malware Forensics: Malware Forensics is used for analyzing the code and searching for any malicious part in the code, its properties, its impact on the system and servers, its entry and how it propagates itself.

Network Forensics: Network Forensics deals with the examination of the network, so that it can identify any network is spreading some malware. Such malwares are used mainly for stealing credentials, like credit card number, important passwords, CVV, etc.

Mobile Forensics: Mobile Forensics is used to examine electronic gadgets such as mobile devices, retrieve and analyse the information they contain like contacts, chats, call record, multi-media, installed applications, etc.

Memory Forensics: Memory Forensics deals with analysis and collection of volatile data from RAM and cache memory. They are mainly conducted to investigate and identify attacks or malicious activities that do not leave easily detectable tracks on physical memory such as hard disks.

Working of computer forensics

A forensic investigator typically follows standard procedures when working with computer forensics, an investigative field that identifies and stores electronic evidence from a computer device. Investigators follow different procedures based on the context of the forensic investigation, the device being investigated, or the information they are seeking. Three steps are generally involved in these procedures:

1.**Collection of data**: It is necessary to collect electronically stored information ethically. Devices are typically isolated physically to prevent accidental contamination or tampering. To maintain the pristine condition of the original device, the examiner makes a digital copy, also referred to as a forensic image, of its storage media.

2.**Analysis:** An investigator uses digital copies of storage media to gather evidence in a sterile environment. The Wireshark network protocol analyzer and Basis Technology's Autopsy help in this process.

3.**Presentation:** In legal proceedings, an investigator's findings are used by a judge or jury to determine the outcome of a lawsuit. A forensic investigator presents the data they recovered from a compromised system in a data recovery situation.

The need for forensics analysis tools has created a large market for cyber security professionals reliant on technology to conduct investigations. Here are a few examples of the most common types of digital forensic tools:

Disk Forensic Tools
Memory Forensic Tools
Database Forensic Tools
Malware Forensic Tools
Email Forensic Tools
Mobile Phone Forensic Tools

A focus on computer forensics alone is not sufficient; one must also be familiar with the areas in which it is used. Computer forensics is used in the following situations:

- Deflation, deception, and negligence are all forms of sexual harassment.
- A person's employment can be terminated in the future based on the information collected.
- Cases involving general criminal and civil law. Computers are sometimes used by criminals to store information.
- After an incident, damage analysis, and assessment are conducted.
- Criminal activity involving white collars. Government or business
- professionals commit these nonviolent, financially motivated crimes.

-Aditi Jain
(BCA 2nd Year 1st Shift)

-Aditya Pandey
(BCA 2nd Year 1st Shift)

jims
Sector-5, Rohini, Delhi

STUDENT'S IT PRESS

IT KALEIDOSCOPE

THEME: COMPUTER FORENSICS

NOV 2022 EDITION

Technology Used in Computer Forensics

Computer forensics investigations are often conducted using the standard digital forensics approach of acquisition, examination, analysis, and reporting. Investigators investigate a compromised device's copy using a number of methodologies and proprietary forensic applications. They search hidden folders and free drive space for copies of lost, encrypted, or damaged files. These analyses are generally performed on static data (disc pictures) rather than live data or live systems, though in the early days of computer forensics, due to a lack of tools, investigators had to work on live data.

Computer forensic investigations use a variety of methods and expertise.

Typical methods include the following:

Reverse Steganography

Data can be concealed using steganography in any kind of digital file, message, or data stream. Computer forensic specialists can undo a steganography attempt by looking at the data hashing in the relevant file. The image or other digital file may appear to be identical before and after if a cybercriminal conceals crucial information inside it, but the underlying hash or string of data that describes the image will change.

Stochastic Forensics

It is a technique for forensically reconstructing digital actions with insufficient digital evidence, allowing for the analysis of new patterns brought about by the stochastic nature of contemporary computers. Stochastic Forensics is commonly used in data breach investigations where the attacker is suspected to be an insider who might not leave behind digital evidence.

Cross-drive analysis

This method searches for, analyses, and preserves material pertinent to an investigation by correlating and cross-referencing data located on several computer discs. Information from other drives is compared to suspicious events to look for patterns and give context. This is also known as anomaly detection. Multi-drive correlation using text searches e.g, email addresses, SSNs, message IDs or credit card numbers is one existing approach.

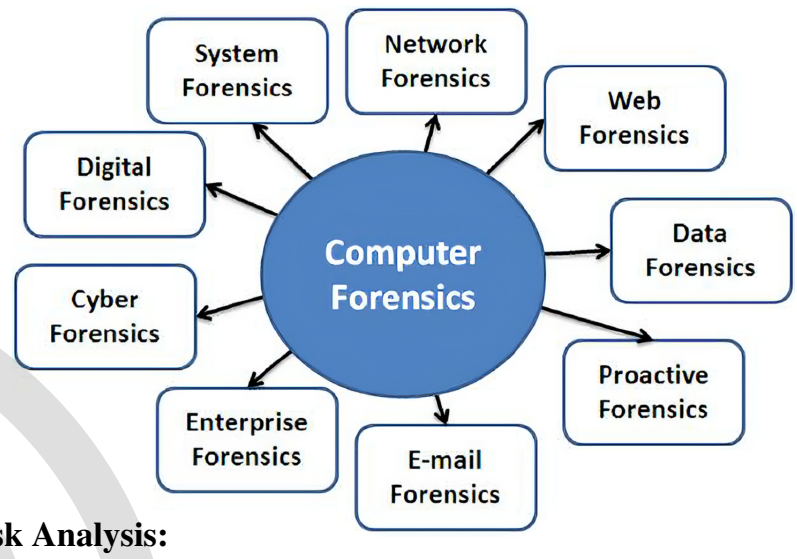
Live Analysis

In this approach, system tools built inside the computer are utilised to evaluate a computer while it is in use, from within the OS. The analysis examines volatile data, which is often kept in RAM or cache. For the sake maintaining the credibility of a chain of evidence, several tools used to retrieve volatile data demand that the computer be in a forensic lab.

Implementation of Computer Forensics Using tools

Digital evidence can be found in a wide variety of formats and on a wide range of platforms. Analysis of documents, emails, network activity, and other relevant artefacts and sources of information about the nature, significance, and attribution of an occurrence are frequently included in forensic inquiry.

Digital forensics tools frequently have diverse expertise because there are so many distinct potential data sources. The most popular and extensively used tools for completing various tasks in a computer forensics investigation are described in the following list:



Disk Analysis:

The two most well-known forensics toolkits are likely Autopsy and the Sleuth Kit. The Sleuth Kit is a command-line tool that does detailed audit of hard drive and smartphone forensic photos. A GUI-based system called Autopsy tends to make use of The Sleuth Kit in the background. Users may simply add new functions to the tools because they are built with a modular and plug-in architecture.

Image Creation:

Hard drive, smartphone, and other disc images can be examined with Autopsy and The Sleuth Kit. The utility of using an image for analysis (rather than a live drive) is that it enables the investigator to demonstrate that they have not made any changes to the drive that would alter the forensic findings. Another tool must be employed because autopsy lacks the
ability to create images.

Memory Forensics:

Although tools like The Sleuth Kit focus on the hard drive, forensic data and artefacts may also be stored in other places on a computer. RAM is a volatile memory that can hold a lot of important forensic information, which needs to be collected correctly and quickly in order to be forensically valid and useful. Volatility is the most well-known and often used tool for analyzing volatile memory. Like The Sleuth Kit, Volatility is free, open-source, and supports third-party plugins. In fact, the Volatility Foundation annually conducts a contest for users to develop the most innovative and practical framework extension.

-Sneha Kaushik
(BCA 2nd Year 1st Shift)

-Rohan Singh
(BCA 2nd Year 1st Shift)

jims
Sector-5, Rohini, Delhi

NOV 2022 EDITION

IT KALEIDOSCOPE

COMPUTER FORENSICS

Our Team

Dr. Praveen Arora
Program Incharge

Dr. Priyanka Gandhi
Faculty Incharge

Sampada Verma
Student Coordinator
BCA 3rd Year 2nd Shift

Sahil Kumar
Student Coordinator
BCA 2nd Year 1st shift

Ishita Jindal
Student Coordinator
BCA 2nd Year 1st shift

Sampada Verma
Designing Team
BCA 3rd Year 2nd Shift

Silviya
Designing Team
BCA 2nd Year 2nd Shift

Siddharth Chaudhary
Designing Team
BCA 2nd Year 2nd Shift

Sahil Kumar
Designing Team
BCA 2nd Year 1st Shift