Society for Computer Technology and Research's

PUNE INSTITUTE OF COMPUTER TECHNOLOGY

S.No.-27, Pune Satara Road, Dhankawadi, Pune-411043

A.Y. 2023-24

Department of Computer Engineering

Laboratory Practice – IV

Batch: Q1

Date:

27/10/23

(SEMESTER-VII)

A REPORT ON

Design and develop a tool for digital forensic of images

Under the guidance of

Prof. U.S.Pawar

Submitted by

Shreyash Dwivedi (41127)
Vinayak Jamadar (41137)
Sanket Jhavar (41138)

TITLE

Digital Forensic of Images

PROBLEM STATEMENT

Design and develop a tool for digital forensic of images.

SYSTEM REQUIREMENT

Operating System:	64-bit Linux or its derivatives / Windows.
FTK Imager	Version: 4.7.1.2

OBJECTIVES

- Students will be able to apply the principles of digital forensics.
- They will also develop skills in image processing for digital forensics.

SCOPE

The primary focus of the project is to create a tool that can perform digital forensic analysis on image files. This includes various tasks such as:

- Metadata extraction: Retrieving information such as date, time, camera details, and geolocation data from image files.
- File integrity verification: Checking the integrity of image files using cryptographic hashing techniques.
- Tamper detection: Detecting any unauthorized alterations or manipulations of image content or metadata.
- Steganography detection: Identifying hidden data within images that may be used for covert communication.
- Content analysis: Analysing the actual image content, including object recognition, face detection, and similarity analysis.

THEORY

DIGITAL FORENSICS

Digital forensics is a branch of forensic science focused on investigating and uncovering digital evidence in criminal cases and cybersecurity incidents. It involves the collection, analysis, and preservation of digital data from various sources such as computers, mobile devices, and networks. Digital forensic experts use specialized tools and techniques to retrieve information, including files, emails, and logs, to reconstruct events, trace cyberattacks, and support legal proceedings. This field plays a critical role in solving cybercrimes, data breaches, and other digital offenses by providing a reliable trail of electronic evidence that can be presented in court to establish culpability or innocence. Digital forensics is essential in today's technology-driven world, ensuring accountability and aiding in the prevention and resolution of digital-related crimes. Digital forensics is a branch of forensic science that uses scientific techniques and technologies to collect, analyse, and present electronic data. Digital forensics is used in cybersecurity to:

- Identify, investigate, and mitigate cybercrime situations
- Identify network vulnerabilities and develop ways to mitigate them
- Secure digital assets

Digital forensics experts:

- Collect, process, preserve, and analyze computer-related evidence
- Retrieve and analyze data from digital devices including computers, and other digital storage media
- Provide critical assistance to police investigations Report any valuable digital information in the digital devices related to the computer crimes

Digital forensics data is commonly used in court proceedings.

IMAGE FORENSICS

Forensic images, in the context of digital forensics, are exact copies of data stored on digital devices like computers, smartphones, or storage media. These images capture the entire contents of a device, including files, deleted data, and system information. Forensic examiners use these images to conduct investigations, analyze digital evidence, and ensure data integrity for legal purposes. They are critical for preserving evidence and preventing contamination, as any alterations to the original data could compromise its validity in a court of law. Forensic images allow experts to examine digital artifacts, recover deleted files, and uncover valuable information crucial for criminal investigations, incident response, and legal proceedings.

NEED FOR A FORENSIC IMAGE

1. In today's world of crime, many cases have been solved by using this technique, as evidence apart from what is available through an operating system, has been found using this technique, as incriminating data might have deleted to prevent discovery during the investigation. Unless that data is overwritten and deleted securely, it can be recovered.
2. One of the advantages includes the prevention of the loss of critical files.
3. When you suspect a custodian of deleting or altering files. A complete forensic image will, to a certain extent, allow you to recover deleted files. It can also potentially be used to identify files that have been renamed or hidden.
4. When you expect that the scope of your investigation could increase at a later date. If you aren't sure about the scope of your project, ALWAYS OVER COLLECT. It's better to have too much data than not enough, and you can't get much more data than a forensic image.

METHODOLOGY

The methodology for designing and developing a tool for digital image forensics should start with a clear understanding of the objectives and requirements. This initial phase involves defining the scope of the tool, including the types of image formats it will support and the specific forensic tasks it will perform, such as detecting tampering, analyzing metadata, or identifying source devices. Next, comprehensive research should be conducted to stay updated with the latest techniques and tools in the field of digital image forensics.

The tool's architecture and user interface should be designed to accommodate the needs of digital forensics experts, making it user-friendly and efficient. The core functionalities, such as image hashing, steganography detection, and metadata analysis, should be implemented with high precision and scalability.

Throughout the development process, rigorous testing and validation procedures are essential to ensure the tool's accuracy and reliability. This includes using benchmark datasets, real-world case scenarios, and collaboration with experts in the field to evaluate its performance.

Once the tool is built, documentation, user guides, and training materials should be created to facilitate its adoption by digital forensics professionals. Continuous improvement and updates are also crucial to adapt to evolving image manipulation techniques and to maintain the tool's effectiveness in a rapidly changing digital landscape.

Moreover, ethical considerations regarding data privacy and legal compliance must be incorporated into the tool's design to ensure it is used responsibly and within the boundaries of the law. In sum, the methodology for designing and developing a digital image forensics tool should encompass planning, research, design, development, testing, documentation, and ongoing refinement, all aimed at providing a robust and valuable resource for the digital forensics community."

OUTCOME

1) Digital Forensic Tool:

The primary outcome is the creation of a functional digital forensic tool capable of analyzing images for evidence of tampering, metadata extraction, and content analysis. This tool can be a valuable asset to investigators and forensic experts.

2) Improved Digital Forensics:

The tool enhances the capabilities of digital forensics professionals by providing them with a comprehensive solution for image analysis, making it easier to uncover tampering or manipulation.

3) Enhanced Efficiency:

Investigators can perform image analysis more efficiently and accurately using the tool, saving time and resources.

SCREENSHOTS

CONCLUSION

In this project we have successfully implemented design and development of a tool for digital forensics of an image.