DEPARTMENT OF COMPUTER ENGINEERING

Pune Institute of Computer Technology,
Pune
Savitribai Phule Pune University

Laboratory Practical - IV

Cyber Security & Digital Forensics

Mini Project Report

Design and Develop a tool for Digital Forensics of Image

By

Monu Narnaware 41345
Mihir Parte 41349

AIM

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

OBJECTIVE

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

SCOPE

1. Image forensic analysis

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: Analyzing the actual image content, including object recognition, face detection, and similarity analysis.

THEORY

Digital Forensics

Digital forensics is a branch of forensic science that uses scientific techniques and technologies to collect, analyze, 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.

Forensic Images

A forensic image is a copy of unmodified electronic data. It can be a copy of a single file or an entire hard drive. A forensic image is a bit-by-bit, sector-by-sector direct copy of a physical storage device. It includes all files, folders, and unallocated, free, and slack space.

Forensic images are used to:

- Forensically analyze and preserve original data
- Conduct investigations on an exact copy of the source device
- Collect and preserve evidence that can make or break a criminal case

A Forensic Image is most often needed to verify the integrity of the image after an acquisition of a Hard Drive has occurred. This is usually performed by law enforcement for court because, after a forensic image has been created, its integrity can be checked to verify that it has not been tampered with. Forensic Imaging is defined as the processes and tools used in copying an electronic media such as a hard-disk drive for conducting investigations and gathering evidence that will be presentable in the law of court. This copy not only includes files that are visible to the operating system but every bit of data, every sector, partition, files, folders, master boot records, deleted files, and unallocated spaces. The image is an identical copy of all the drive structures and contents.

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.

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.

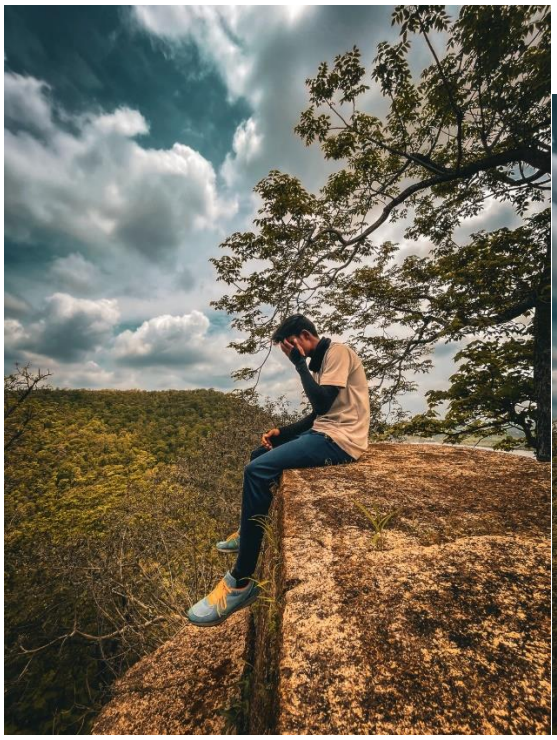
2) Improved Digital Forensics:

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.

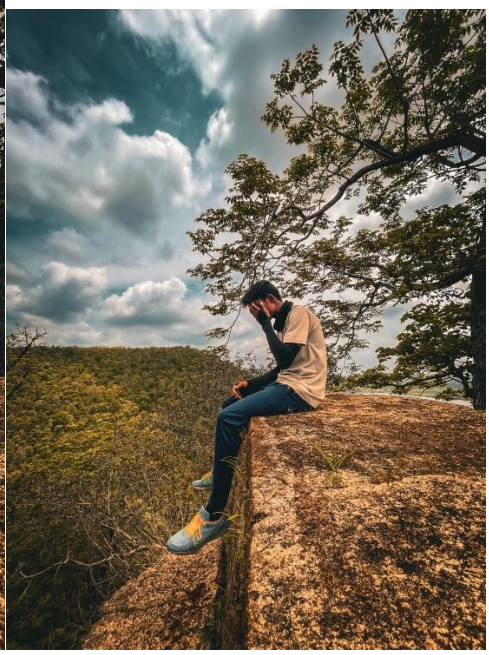
3) Enhanced Efficiency:

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

SCREENSHOTS OF OUTPUT



Original Image



Altered Image

```
Potential forgery detected in block at (0, 800)
Potential forgery detected in block at (0, 816)
Potential forgery detected in block at (0, 832)
Potential forgery detected in block at (0, 848)
Potential forgery detected in block at (0, 864)
Potential forgery detected in block at (0, 880)
Potential forgery detected in block at (0, 896)
Potential forgery detected in block at (0, 912)
Potential forgery detected in block at (0, 928)
Potential forgery detected in block at (0, 944)
Potential forgery detected in block at (0, 960)
Potential forgery detected in block at (0, 976)
Potential forgery detected in block at (0, 992)
Potential forgery detected in block at (0, 1008)
Potential forgery detected in block at (0, 1024)
Potential forgery detected in block at (0, 1040)
Potential forgery detected in block at (0, 1056)
Potential forgery detected in block at (0, 1072)
Potential forgery detected in block at (0, 1088)
Potential forgery detected in block at (0, 1104)
Potential forgery detected in block at (0, 1120)
Potential forgery detected in block at (0, 1136)
Potential forgery detected in block at (0, 1152)
Potential forgery detected in block at (0, 1168)
Potential forgery detected in block at (0, 1184)
...
Potential forgery detected in block at (1184, 1536)
Potential forgery detected in block at (1184, 1552)
Potential forgery detected in block at (1184, 1568)
Potential forgery detected in block at (1184, 1584)
```

Forgery Detected

ELA Result

CONCLUSION

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