Pune Vidyarthi Griha's College of Engineering and Technology & G.K. Pate (Wani) Institute of Management, Pune- 411009.

(Affiliated to Savitribai Phule Pune University)

A Mini Project Report On

"DigiCheck: Digital Forensic Tool for Images"

Submitted in Partial Fulfillment for the Term-work of Fourth year in Computer Engineering of *Savitribai Phule Pune University*.

By

1.	Samruddhi Dhon	0077
2.	Akanksha Lokhande	0071
3.	Jagruti Patil	2089

Under The Guidance of

Prof. A. M. Bhadgale

Department of Computer Engineering

Academic Year: - 2024-2025

Pune Vidyarthi Griha’s College of Engineering and Technology & G.K. Pate (Wani) Institute of Management, Pune- 411009.

(Affiliated to Savitribai Phule Pune University)

CERTIFICATE

This is to certify that the Project report entitled “**DigiCheck: Digital Forensic Tool for Images**” submitted by,

1.	Samruddhi Dhon	0077
2.	Akanksha Lokhande	0071
3.	Jagruti Patil	2089

is a record of bonafide work carried out by him/her, in the partial fulfilment of the Term-work of fourth year in Computer Engineering of Savitribai Phule Pune University at Pune Vidyarthi Griha’s College of Engineering and Technology & G.K. Pate (Wani) Institute of Management, Pune under Savitribai Phule Pune University, Pune. This work is done during the academic year 2022-23.

Date: - 17/10/24

Place: - Pune

Prof. A. M. Bhadgale
Subject Teacher
(Computer Engg.)

Prof. U.M. kalshetti
H.O.D.

CONTENTS

Introduction

In an increasingly digital world, the importance of image forensics cannot be overstated. With the proliferation of smartphones, social media platforms, and digital cameras, images play a pivotal role in both our personal and professional lives. They capture memories, serve as evidence in legal cases, and convey information in a multitude of contexts. However, this widespread use of digital images has also given rise to challenges related to image authenticity, integrity, and security.

DigiCheck, a cutting-edge digital forensic tool for images, emerges as an essential solution to address these challenges. DigiCheck is a powerful software application designed to scrutinize, authenticate, and analyze digital images with the precision and reliability required for legal, investigative, and security purposes. This innovative tool equips forensic experts, law enforcement agencies, and digital investigators with a comprehensive suite of features to delve into the intricate world of digital image analysis.

DigiCheck offers an array of capabilities to verify the authenticity of digital images, uncover hidden information within them, and detect any potential alterations or tampering. It employs advanced techniques such as metadata extraction, error level analysis, and steganography detection to uncover digital footprints and hidden data. This tool can be instrumental in addressing a wide range of issues, from determining the legitimacy of evidence in court to investigating incidents of digital image manipulation and forgery.

Key Features of DigiCheck:

Metadata Analysis: DigiCheck allows users to extract and examine metadata embedded within digital images, including date and time stamps, geolocation data, and device-specific information, which can be crucial for verifying the origin and history of an image.

Error Level Analysis: This tool utilizes error level analysis to detect inconsistencies in the compression levels of an image, helping to identify potential areas of manipulation or tampering.

Steganography Detection: DigiCheck can identify hidden data concealed within images using steganographic techniques, ensuring that no unauthorized information remains undisclosed.

Image Integrity Verification: With DigiCheck, users can assess the integrity of digital images to determine if they have been altered, offering critical insights in legal and investigative scenarios.

User-Friendly Interface: DigiCheck is designed with an intuitive user interface, making it accessible to both experienced forensic experts and newcomers to digital image analysis.

Customizable Reporting: The tool offers comprehensive and customizable reporting features, enabling users to document their findings in a format suitable for courtroom presentations and investigative reports.

Overview

DigiCheck is a powerful and versatile digital forensic tool designed specifically for the examination and analysis of images. In the world of digital forensics, where the need to extract, analyze, and preserve digital evidence is paramount, **DigiCheck** serves as an invaluable resource for investigators, law enforcement agencies, cybersecurity experts, and other professionals in the field.

Key Features and Capabilities:

Image Metadata Analysis:

DigiCheck can extract and scrutinize the metadata embedded in images, including EXIF (Exchangeable Image File Format) data. This metadata can reveal important information about the origin, history, and editing of the image, such as date and time of capture, camera type, geolocation, and more.

Image Integrity Verification:

Ensuring the integrity of digital images is crucial for maintaining the authenticity of evidence. DigiCheck provides tools to verify if an image has been tampered with or altered by comparing it to a reference image, enabling investigators to detect any unauthorized modifications.

Image Recovery:

DigiCheck includes features for recovering deleted or hidden images. It can locate fragments of images in unallocated disk space and restore them, potentially uncovering crucial evidence that an individual may have attempted to conceal.

Forensic Timeline Analysis:

When working with a collection of images, DigiCheck allows investigators to create a timeline of events by analyzing image file timestamps. This feature can help establish a sequence of events and provide valuable context to an investigation.

Hashing and Digital Signatures:

DigiCheck offers the ability to create and verify cryptographic hashes and digital signatures for images. These techniques are essential for ensuring data integrity and authenticity, making it challenging for malicious actors to tamper with image evidence.

Cross-Platform Compatibility:

DigiCheck is designed to work on various operating systems and supports a wide range of image file formats, ensuring compatibility and usability across different digital environments.

User-Friendly Interface:

DigiCheck features an intuitive and user-friendly interface, making it accessible to both novice and experienced digital forensics professionals. The tool streamlines the process of importing, analyzing, and reporting on image data.

Reporting and Documentation:

DigiCheck enables investigators to generate detailed reports and documentation, including information on the methods used, findings, and supporting evidence. This is essential for legal proceedings and maintaining a thorough record of the forensic analysis.

Software and Hardware Requirement

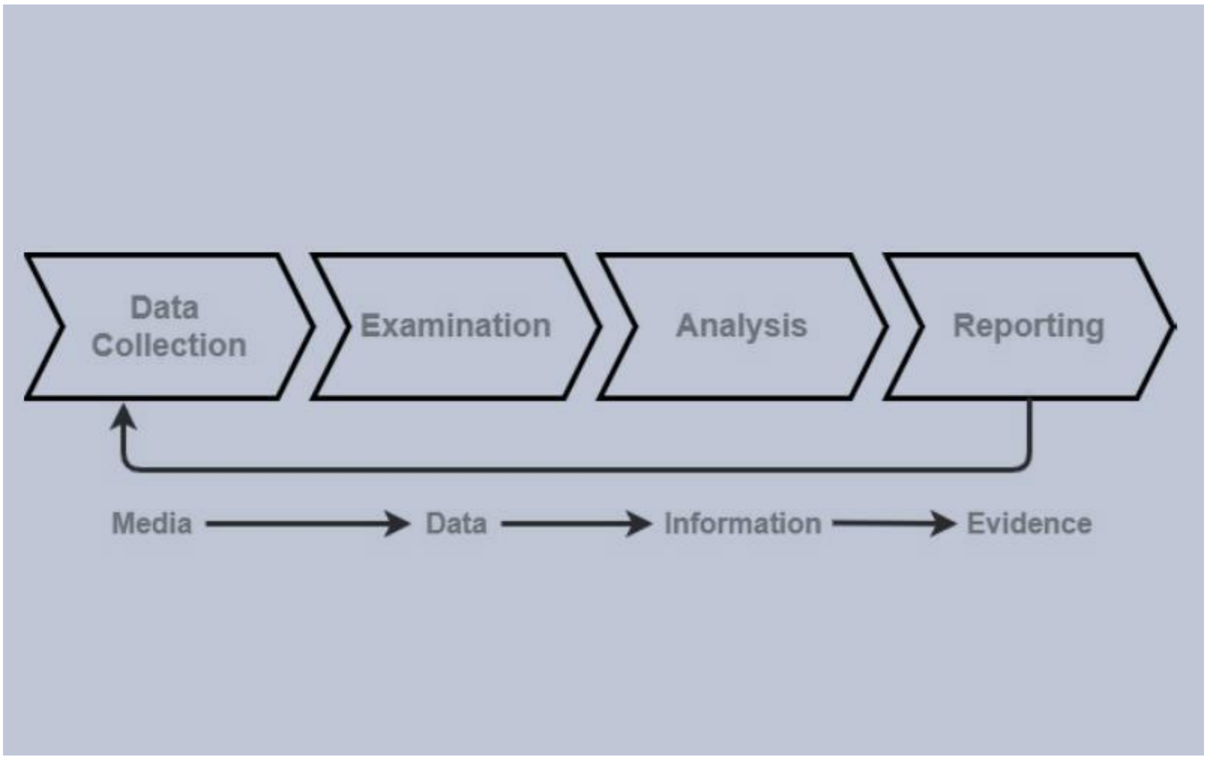
- **Software Requirement:**

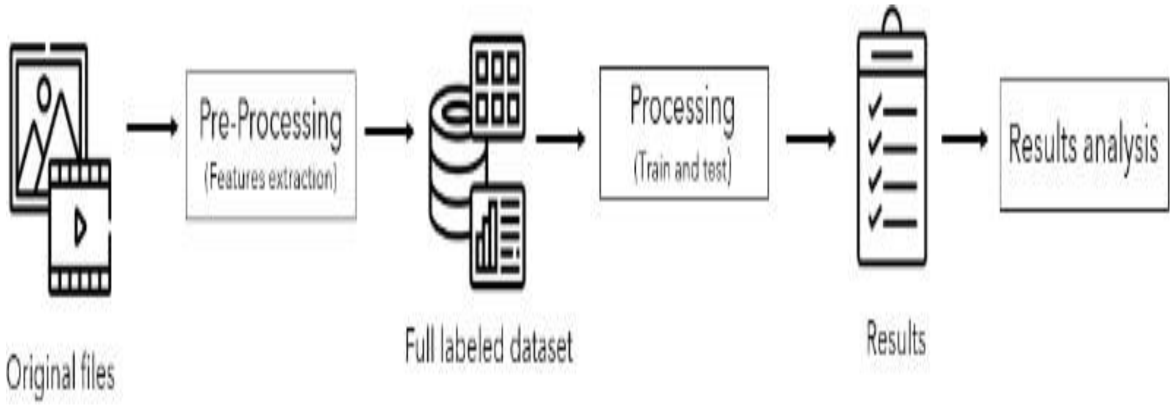
  1) **Operating System Compatibility:** Windows, Linux
  2) **Programming Language:** Python
  3) **Image Format Support:** jpeg, jpg, png
  4) **Image Metadata Extraction:** Exifread File
  5) **Image Analysis Algorithm**: Extraction Algorithm

- **Hardware Requirement:**

  1) **Processor and RAM:** Intel Core i3 and at least 4GB of RAM are recommended for efficient image processing.
  2) **Storage:** Adequate storage space to store images, metadata, and analysis results. Consider using SSDs for faster data access.
  3) **Graphics Processing Unit (GPU):** A dedicated GPU can significantly accelerate image analysis tasks, especially for deep learning-based algorithms.
  4) **Network Connection:** An internet connection for software updates and cloud-based features, if applicable.

Architecture and Workflow Diagrams





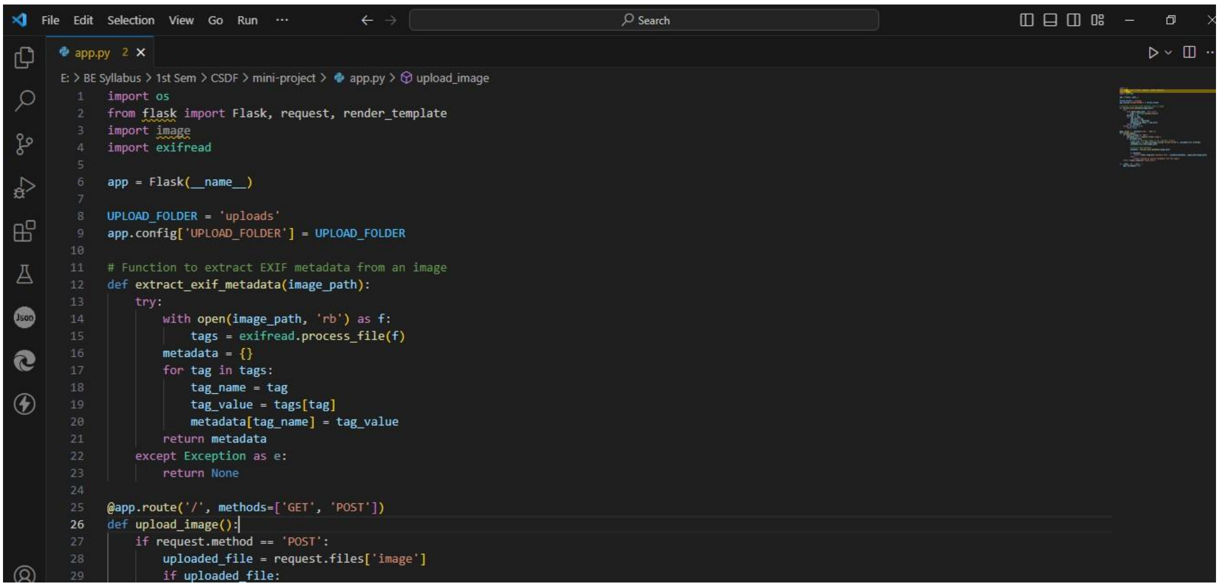
Algorithm

- **Algorithm to extract data:**

```
def extract_exif_metadata(image_path):
   try:
         with open(image_path, 'rb') as f:
         tags = exifread.process_file(f)
      metadata = {}
      for tag in tags:
         tag_name = tag
         tag_value = tags[tag]
         metadata[tag_name] = tag_value
      return metadata
   except Exception as e:
      return None
@app.route('/', methods=['GET', 'POST'])
    def upload_image():
       if request.method == 'POST':
          uploaded_file = request.files['image']
          if uploaded_file:
             # Save the uploaded image to the 'uploads' folder
             image_path=os.path.join(app.config['UPLOAD_FOLDER'],
             uploaded_file.filename)
             uploaded_file.save(image_path)

             # Extract EXIF metadata
             metadata = extract_exif_metadata(image_path)
              if metadata:
                return          render_template('metadata.html',          metadata=metadata,
    image_path=image_path)
             else:
                return "Failed to extract metadata from the image."
       return render_template('index.h’)
```

Implementation


File Edit Selection View Go Run ···
Search
app.py 2
E: > BE Syllabus > 1st Sem > CSDF > mini-project > app.py > upload_image

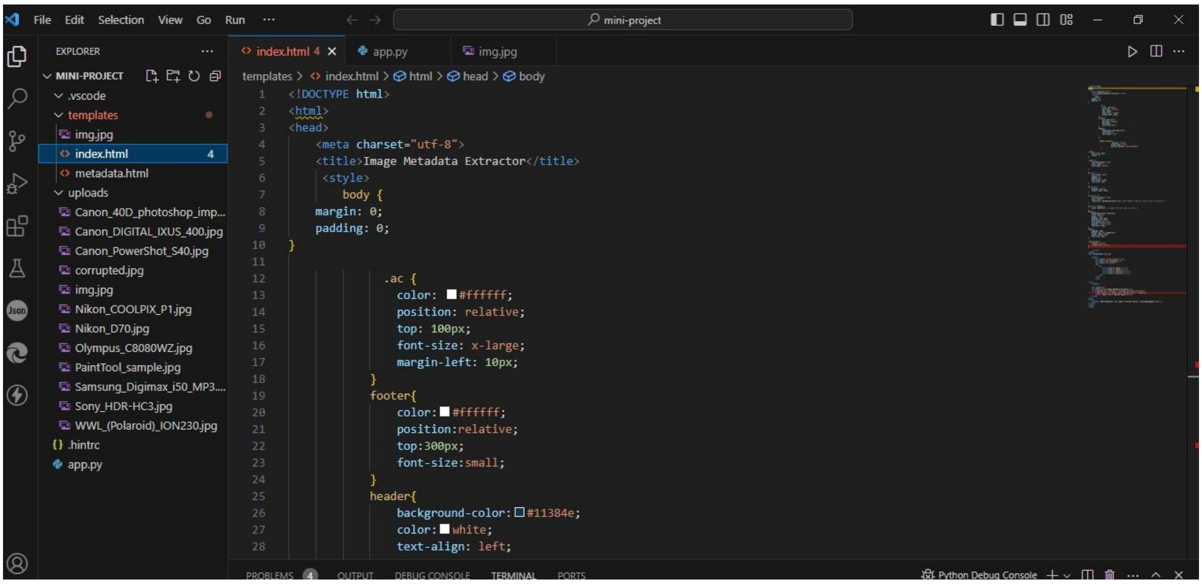
```python
import os
from flask import Flask, request, render_template
import image
import exifread

app = Flask(__name__)

UPLOAD_FOLDER = 'uploads'
app.config['UPLOAD_FOLDER'] = UPLOAD_FOLDER

# Function to extract EXIF metadata from an image
def extract_exif_metadata(image_path):
    try:
        with open(image_path, 'rb') as f:
            tags = exifread.process_file(f)
        metadata = {}
        for tag in tags:
            tag_name = tag
            tag_value = tags[tag]
            metadata[tag_name] = tag_value
        return metadata
    except Exception as e:
        return None

@app.route('/', methods=['GET', 'POST'])
def upload_image():
    if request.method == 'POST':
        uploaded_file = request.files['image']
        if uploaded_file:
```



```html
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <title>Image Metadata Extractor</title>
     <style>
        body {
    margin: 0;
    padding: 0;
}

                .ac {
                    color: #ffffff;
                    position: relative;
                    top: 100px;
                    font-size: x-large;
                    margin-left: 10px;
                }
                footer{
                    color: #ffffff;
                    position:relative;
                    top:300px;
                    font-size:small;
                }
                header{
                    background-color: #11384e;
                    color: white;
                    text-align: left;
```

Result and Outcomes

Digicheck: Website for image Forensic Analysis

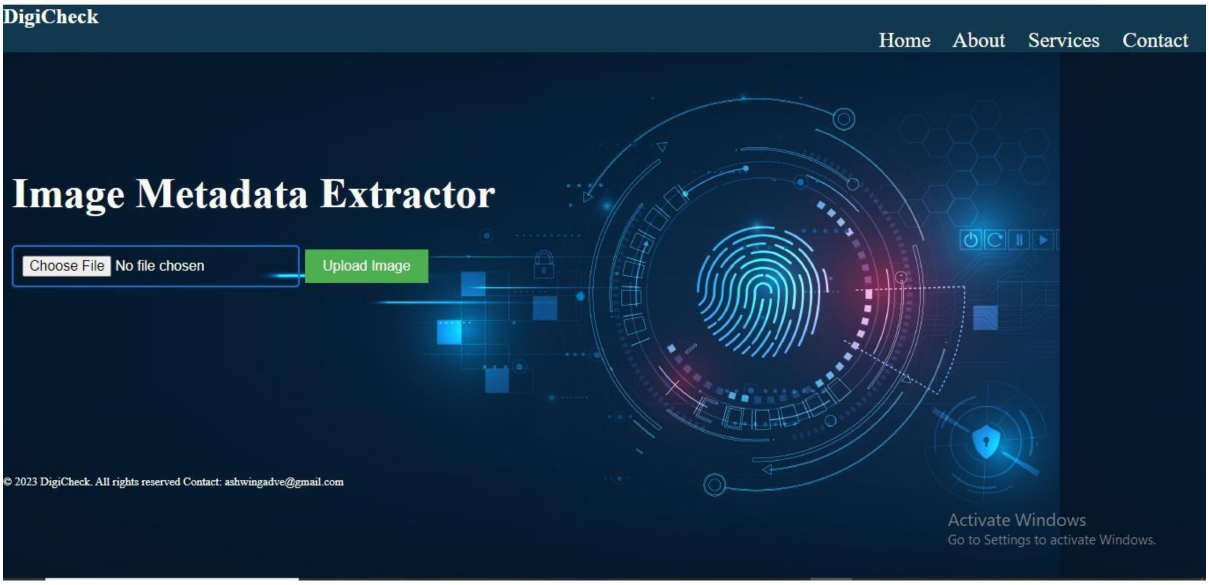


Image Metadata Extractor

© 2023 DigiCheck. All rights reserved Contact: ashwingadve@gmail.com

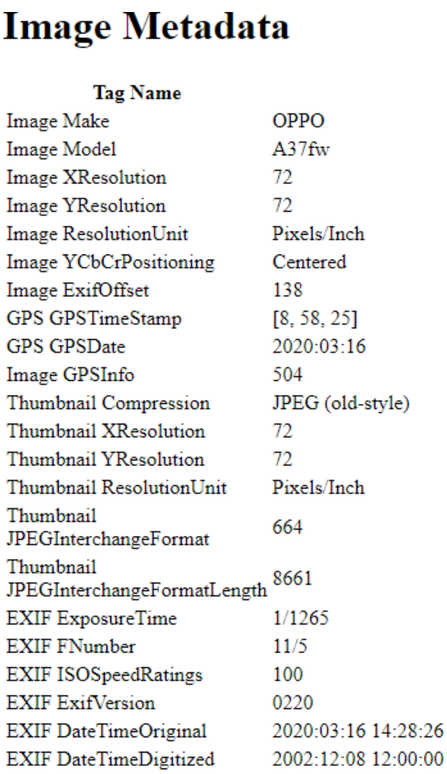


Image Metadata

Tag Name	
Image Make	OPPO
Image Model	A37fw
Image XResolution	72
Image YResolution	72
Image ResolutionUnit	Pixels/Inch
Image YCbCrPositioning	Centered
Image ExifOffset	138
GPS GPSTimeStamp	[8, 58, 25]
GPS GPSDate	2020:03:16
Image GPSInfo	504
Thumbnail Compression	JPEG (old-style)
Thumbnail XResolution	72
Thumbnail YResolution	72
Thumbnail ResolutionUnit	Pixels/Inch
Thumbnail JPEGInterchangeFormat	664
Thumbnail JPEGInterchangeFormatLength	8661
EXIF ExposureTime	1/1265
EXIF FNumber	11/5
EXIF ISOSpeedRatings	100
EXIF ExifVersion	0220
EXIF DateTimeOriginal	2020:03:16 14:28:26
EXIF DateTimeDigitized	2002:12:08 12:00:00

Sample Image 1

Sample Image 1 Metadata

Sample Image 2

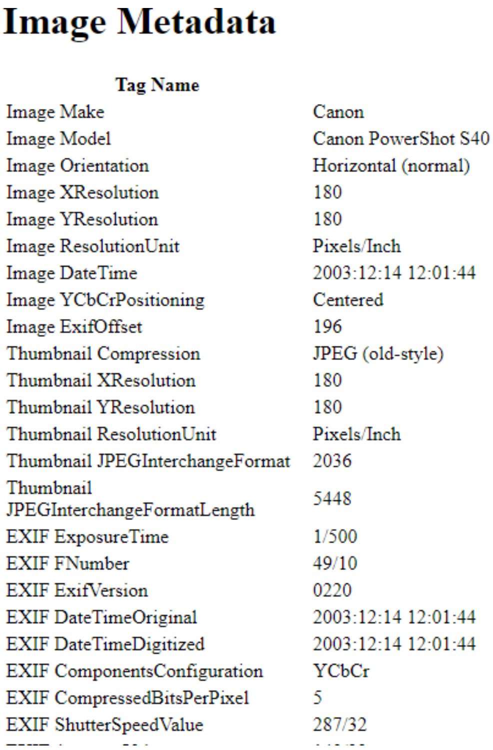


Image Metadata

Tag Name	
Image Make	Canon
Image Model	Canon PowerShot S40
Image Orientation	Horizontal (normal)
Image XResolution	180
Image YResolution	180
Image ResolutionUnit	Pixels/Inch
Image DateTime	2003:12:14 12:01:44
Image YCbCrPositioning	Centered
Image ExifOffset	196
Thumbnail Compression	JPEG (old-style)
Thumbnail XResolution	180
Thumbnail YResolution	180
Thumbnail ResolutionUnit	Pixels/Inch
Thumbnail JPEGInterchangeFormat	2036
Thumbnail JPEGInterchangeFormatLength	5448
EXIF ExposureTime	1/500
EXIF FNumber	49/10
EXIF ExifVersion	0220
EXIF DateTimeOriginal	2003:12:14 12:01:44
EXIF DateTimeDigitized	2003:12:14 12:01:44
EXIF ComponentsConfiguration	YCbCr
EXIF CompressedBitsPerPixel	5
EXIF ShutterSpeedValue	287/32

Sample Image 2 Metadata

Sample Image 3

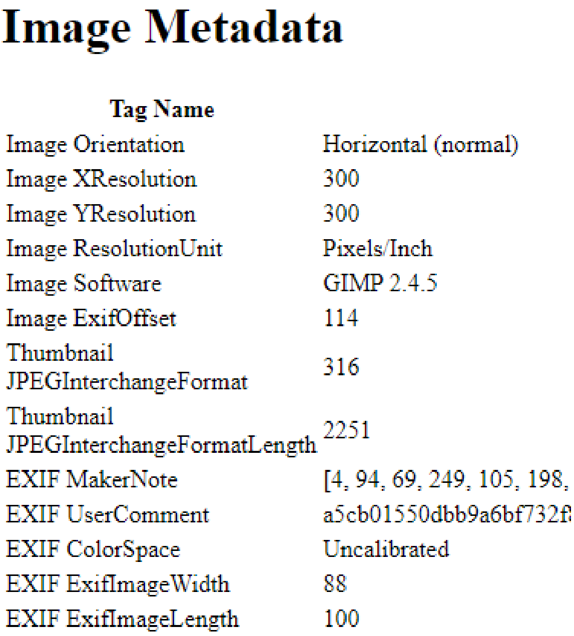


Image Metadata

Tag Name	
Image Orientation	Horizontal (normal)
Image XResolution	300
Image YResolution	300
Image ResolutionUnit	Pixels/Inch
Image Software	GIMP 2.4.5
Image ExifOffset	114
Thumbnail JPEGInterchangeFormat	316
Thumbnail JPEGInterchangeFormatLength	2251
EXIF MakerNote	[4, 94, 69, 249, 105, 198,
EXIF UserComment	a5cb01550dbb9a6bf732f
EXIF ColorSpace	Uncalibrated
EXIF ExifImageWidth	88
EXIF ExifImageLength	100

Sample Image3 Metadata

Conclusion

In conclusion, DigiCheck is a powerful and essential digital forensics tool that plays a crucial role in the field of cybersecurity and law enforcement. This comprehensive software application is designed to assist investigators in the meticulous process of collecting, analyzing, and preserving digital evidence from various sources, including computers, mobile devices, and online platforms. DigiCheck offers several key advantages to its users. It provides a user-friendly interface, making it accessible to both seasoned professionals and newcomers to the field of digital forensics. The tool's robust capabilities for data extraction, recovery, and analysis ensure that investigators can efficiently uncover vital information, whether it be in the form of deleted files, hidden data, or digital artifacts. Furthermore, DigiCheck's ability to maintain data integrity and establish a clear chain of custody is essential for the admissibility of evidence in legal proceedings.

With its diverse range of features, DigiCheck is adaptable to various investigative scenarios, from criminal cases involving cybercrimes to corporate investigations into data breaches and intellectual property theft. The tool allows investigators to scrutinize not only the contents of digital devices but also the metadata and timestamps associated with files, providing invaluable context and chronological information.

In summary, DigiCheck is a crucial tool in the digital forensics arsenal, facilitating the process of digital evidence collection and analysis while upholding the highest standards of integrity and chain of custody. Its adaptability and user-friendliness make it an indispensable asset in the fight against cybercrimes and the protection of digital assets. As digital technology continues to advance, DigiCheck stands as a reliable and cutting-edge solution for investigators and forensic professionals seeking to uncover the truth in the digital realm.

REFERENCES

1. **https://www.tutorialspoint.com/python_forensics/forensics_python_imaging_library.html**
2. **https://medium.com/@18218004/digital-forensics-blog-03-image-forensics-first-time-detecting-image-tampering-b531707563fe.**
3. **https://www.activestate.com/blog/how-to-use-python-for-cyber-forensics/**
4. **https://www.javatpoint.com/python-forensics-and-virtualization.**
5. **https://www.conf42.com/Python_2021_Gajendra_Deshpande_Cyber_Forensic_Application**
6. **https://www.sciencedirect.com/science/article/pii/S2666281723000665**
7. **https://www.sans.org/white-papers/33453/**
8. **https://gbhackers.com/computer-forensics-tools/**