

# SOURCE CODE FOR DIGITAL FORSENICS

---

```
import os

def analyze_file(file_path):

    # Extract file metadata

    file_name = os.path.basename(file_path)

    file_size = os.path.getsize(file_path)

    file_creation_time = os.path.getctime(file_path)

    file_modification_time = os.path.getmtime(file_path)


    # Calculate file hash (MD5)

    with open(file_path, 'rb') as f:

        file_content = f.read()

        file_hash = hashlib.md5(file_content).hexdigest()


    # Perform keyword search

    keywords = ['password', 'hack', 'malware']

    with open(file_path, 'r') as f:

        file_content = f.read()

        for keyword in keywords:

            if keyword in file_content:

                print(f'Keyword "{keyword}" found in file: {file_name}')
```

```
# Print file metadata
```

```
print(f'File Name: {file_name}')
```

```
print(f'File Size: {file_size} bytes')
```

```
print(f'File Creation Time: {file_creation_time}')
```

```
print(f'File Modification Time: {file_modification_time}')
```

```
print(f'File MD5 Hash: {file_hash}')
```

```
# Example usage
```

```
file_path = 'example.txt'
```

```
analyze_file(file_path)
```