

## COMPLEX\_HASHING\_MECHANISM

1. First thing is calculating MD5 hash for the image and storing in a text file and extract the meta data and segregate the important data like

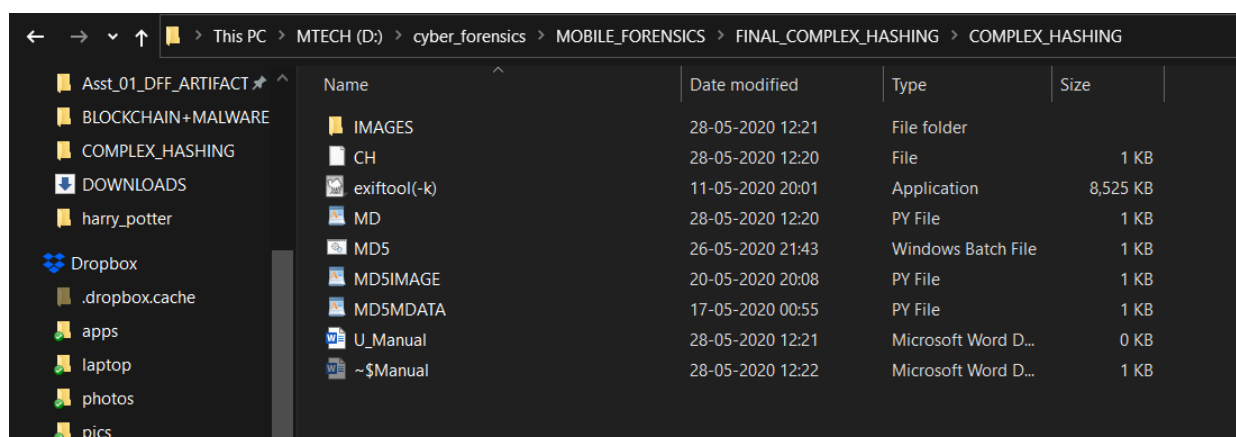
- a. File Name
- b. Directory
- c. File Size
- d. File Modification Date/Time
- e. File Creation Date/Time
- f. File Permissions
- g. File Type
- h. File Type Extension
- i. MIME Type

Where the above metadata are important for the image file which should be considered for the forensics purpose while investigation.

2. Now Hash the metadata which is extracted and stored in the text file and that has to be hashed and append the hash to the image hash which have been stored previously.

### Procedure:

1.



## 2.python script to calculate MD5 for image

```

from PIL import Image
import hashlib
import sys

#md5hash = hashlib.md5(Image.open('1.png').tobytes())
#print(md5hash.hexdigest())

#import base64
#from PIL import Image
#import hashlib

s = sys.argv[1]
with open(s, "rb") as imageFile:
    #str = base64.b64encode(imageFile.read())
    str = imageFile.read()
    #print (str)

#hash_obj = hashlib.md5(str)
#print(hash_obj.hexdigest())

st=hashlib.md5(str).hexdigest()
Thash=st.upper()
#image_file = Image.open('1.png')
#print(hashlib.md5(str).hexdigest())
new_file = open("CH", "w+")
new_file.write(Thash)
new_file.close()
print(Thash)

```

Note: This is command line exif tool which will extract the metadata in cmd prompt and that we have to store in the text file

```

D:\cyber_forensics\MOBILE_FORENSICS\FINAL_COMPLEX_HASHING\COMPLEX_HASHING\exiftool(-k).exe
NAME
    exiftool - Read and write meta information in files

RUNNING IN WINDOWS
    Drag and drop files or folders onto the exiftool executable to display
    meta information, or rename to "exiftool.exe" and run from the command
    line to access all exiftool features.

    This stand-alone Windows version allows simple command-line options to
    be added to the name of the executable (in brackets and separated by
    spaces at the end of the name), providing a mechanism to use options
    when launched via the mouse. For example, changing the executable name
    to "exiftool(-a -u -g1 -w txt).exe" gives a drag-and-drop utility which
    generates sidecar ".txt" files with detailed meta information. As
    shipped, the -k option is added to cause exiftool to pause before
    terminating (keeping the command window open). Options may also be added
    to the "Target" property of a Windows shortcut to the executable.

SYNOPSIS
    Reading
    exiftool [*OPTIONS*] [--TAG*...] [--TAG*...] *FILE*...

    Writing
    exiftool [*OPTIONS*] -*TAG*[+<]=[*VALUE*]... *FILE*...

    Copying
    exiftool [*OPTIONS*] -tagsFromFile *SRCFILE* [--SRCTAG*[>*DSTTAG*]...]
    *FILE*...

-- More --

```

### 3.python script to calculate MD5 for Metadata

```
from PIL import Image
import hashlib
import sys
ap=sys.argv[1]
hifen="-"
md5_hash = hashlib.md5()

a_file = open(ap, "rb")
content = a_file.read()
md5_hash.update(content)

digest = md5_hash.hexdigest()
Thash=digest.upper()
#print(Thash)
new_file = open("CH", "a")
new_file.write(hifen)
new_file.write(Thash)
new_file.close()
```

### 4.python script to get important Metadata

```
import sys
a=sys.argv[1]
a_file = open(a, "r")
lines = a_file.readlines()
a_file.close()
del lines[0]
del lines[4]
del lines[9:]

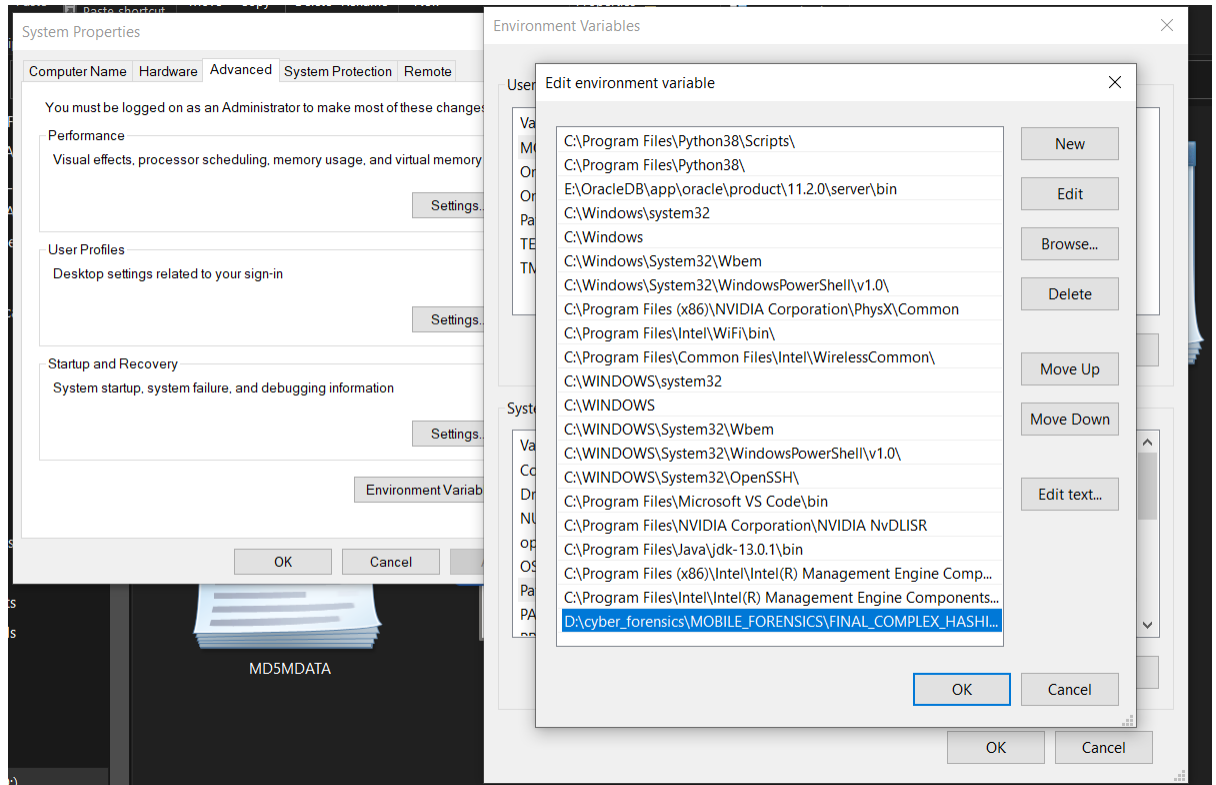
new_file = open(a, "w+")
for line in lines:
    new_file.write(line)
new_file.close()
```

### 5.Batch script for Automation of the hash generation

```
@echo off
echo "Please Add the path of this directory in Windows "PATH" system variable"
echo -----
echo -----
python -m pip install --upgrade pip
pip install Pillow
set /p input= "Enter Your File Path For Metadata : "
"exiftool(-k).exe" %input% > %input%.txt
python MD5IMAGE.py %input%
python MD.py %input%.txt
python MD5MDATA.py %input%.txt
start notepad CH
pause
```

**EXECUTION:**

1. Add the folder path to avoid errors in the time of execution so that file at any location can be calculated



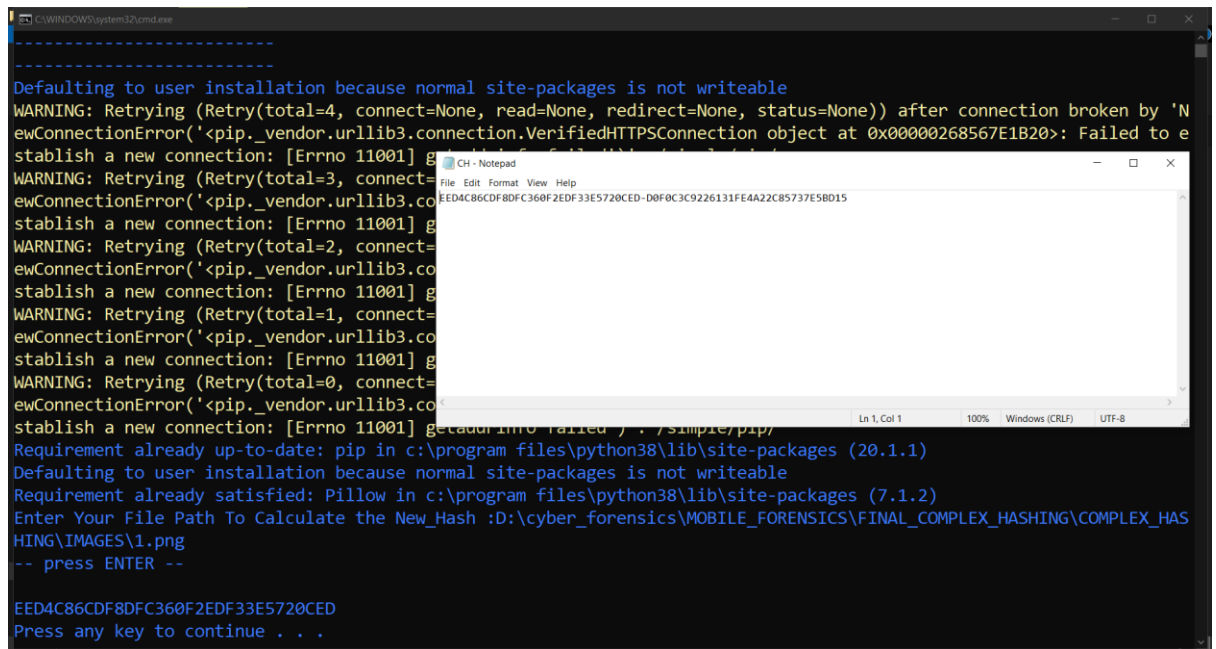
2. Use the bat script for generating the hash which can be done by double click

```

C:\WINDOWS\system32\cmd.exe
"Please Add the path of this directory in Windows "PATH" system variable"
-----
Defaulting to user installation because normal site-packages is not writeable
WARNING: Retrying (Retry(total=4, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError(<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x0000020667AB1B20>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed')': /simple/pip/
WARNING: Retrying (Retry(total=3, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError(<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x0000020667AB1CD0>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed')': /simple/pip/
WARNING: Retrying (Retry(total=2, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError(<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x0000020667ACD3D0>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed')': /simple/pip/
WARNING: Retrying (Retry(total=1, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError(<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x0000020667AE5370>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed')': /simple/pip/
WARNING: Retrying (Retry(total=0, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError(<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x0000020667AE5190>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed')': /simple/pip/
Requirement already up-to-date: pip in c:\program files\python38\lib\site-packages (20.1.1)
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: Pillow in c:\program files\python38\lib\site-packages (7.1.2)
Enter Your File Path To Calculate the New_Hash :

```

### 3. Now it will ask the image file to extract the metadata and calculate the hash

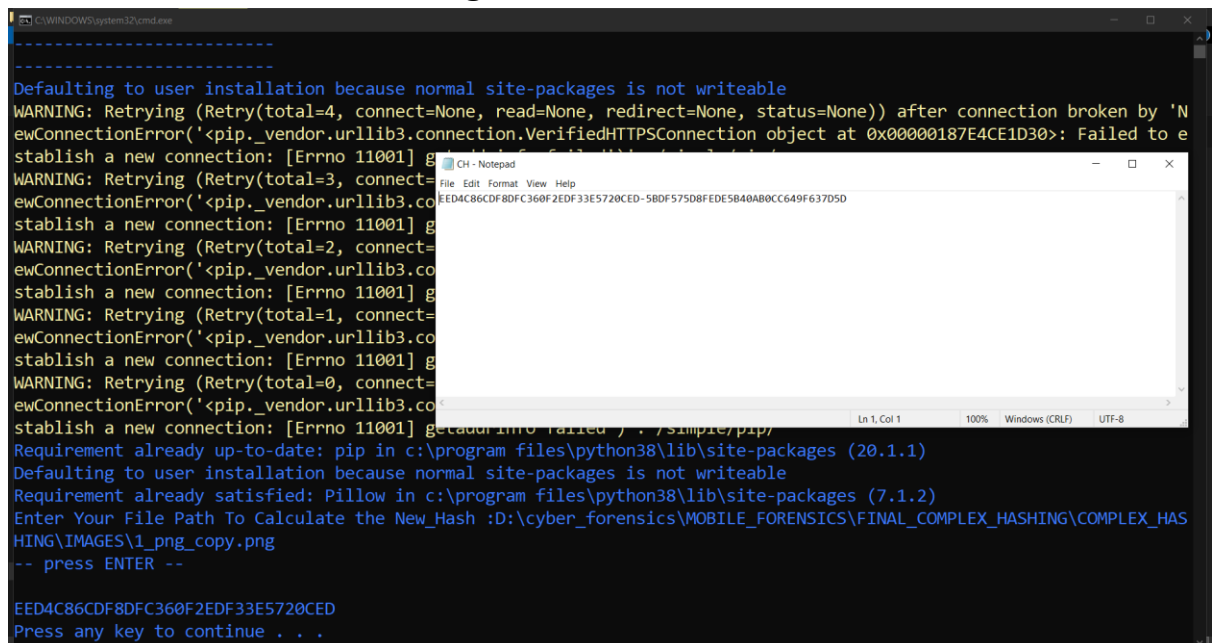


```

-----
Defaulting to user installation because normal site-packages is not writeable
WARNING: Retrying (Retry(total=4, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000268567E1B20>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
WARNING: Retrying (Retry(total=3, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000268567E1B20>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
WARNING: Retrying (Retry(total=2, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000268567E1B20>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
WARNING: Retrying (Retry(total=1, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000268567E1B20>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
WARNING: Retrying (Retry(total=0, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000268567E1B20>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
Requirement already up-to-date: pip in c:\program files\python38\lib\site-packages (20.1.1)
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: Pillow in c:\program files\python38\lib\site-packages (7.1.2)
Enter Your File Path To Calculate the New_Hash :D:\cyber_forensics\MOBILE_FORENSICS\FINAL_COMPLEX_HASHING\COMPLEX_HASHING\IMAGES\1.png
-- press ENTER --

EED4C86CDF8DFC360F2EDF33E5720CED
Press any key to continue . . .
  
```

### 4. For same image copy the hashing will varies since the metadata is not same as the original



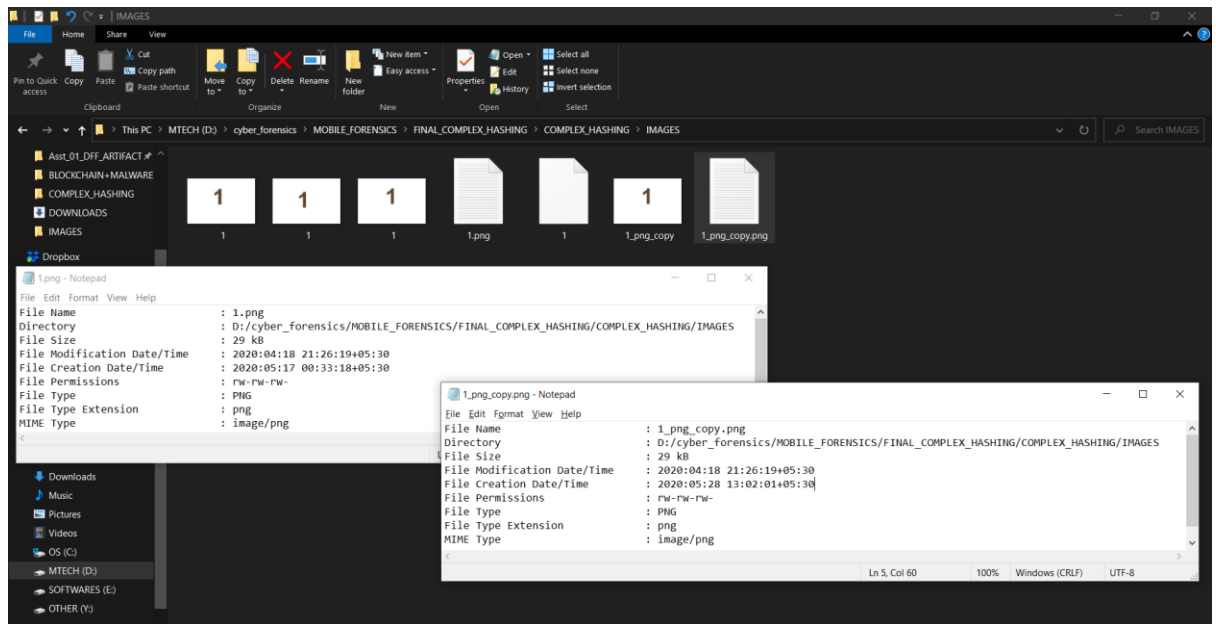
```

-----
Defaulting to user installation because normal site-packages is not writeable
WARNING: Retrying (Retry(total=4, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000187E4CE1D30>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
WARNING: Retrying (Retry(total=3, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000187E4CE1D30>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
WARNING: Retrying (Retry(total=2, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000187E4CE1D30>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
WARNING: Retrying (Retry(total=1, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000187E4CE1D30>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
WARNING: Retrying (Retry(total=0, connect=None, read=None, redirect=None, status=None)) after connection broken by 'NewConnectionError('<pip._vendor.urllib3.connection.VerifiedHTTPSConnection object at 0x00000187E4CE1D30>: Failed to establish a new connection: [Errno 11001] getaddrinfo failed )' : /simple/pip/
Requirement already up-to-date: pip in c:\program files\python38\lib\site-packages (20.1.1)
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: Pillow in c:\program files\python38\lib\site-packages (7.1.2)
Enter Your File Path To Calculate the New_Hash :D:\cyber_forensics\MOBILE_FORENSICS\FINAL_COMPLEX_HASHING\COMPLEX_HASHING\IMAGES\1_png_copy.png
-- press ENTER --

EED4C86CDF8DFC360F2EDF33E5720CED
Press any key to continue . . .
  
```

Note: Image have same MD5 hash but not the metadata so combination of both hashes will make difference

## 5. Metadata for same image copies



- 1.This image hashing is used for forensic investigation to identify the original file and along with the location
- 2.It can also use to avoid hash collisions
- 3.using the MD5 algorithm this mechanism works to form the hash
- 4.It is not meant for checksum
- 5.Only for investigation and this can be stored in mobile itself to identify the original image to copied image.
- 6.It can be done to the other files also like txt, videos, apks, audios, etc. in future scope
- 7.Can also identify the multiple files with this technique and find original so delete copied files to reduce the junk files.