National College of Ireland

Configuration Manual

MSc Internship
Cyber Security

Rohan Bhangale
Student ID: 18147119

School of Computing
National College of Ireland

Supervisor: Ben Fletcher

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Rohan Bhangale……

Student ID: 18147119……

Programme: Cybersecurity…… **Year:** 2019……..

Module: MSc Internship……

Lecturer: Ben Fletcher……

Submission Due Date: 12/12/19……

Project Title: Secure Image Metadata using Advanced Encryption Standard……

Word Count: 344…… **Page Count:** 6……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ……

Date: 12/12/2019……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Rohan Bhangale
Student ID: 18147119

1 Summary

The proposed paper describes the procedure to secure image metadata using EXIF data stripping and encryption. Python scripts are developed for enabling AES encryption and decryption process while use of tools such as exiv2[1] and exiftool[2] was made for enabling stripping and embedding EXIF data. Nano[3] editor was used for development of the python script while a base Linux machine shell with python libraries was used for executing them

2 Tools

The implementation required three major components viz. EXIFTOOL, Python[4], EXIV2 on a base linux machine.

1. exiftool: Used for reading, extracting and striping the image metadata
2. nano: For editing script, nano editor is used
3. python: Used for developing scripts for encrypting and decrypting metadata files using AES
4. exiv2: Used to manipulate image metadata tags

3 Download and Installation

- Git[5]: sudo apt-get install git

- exiftool: sudo apt-get install exiftool

```
root@1onehawk:~# sudo apt-get install exiftool
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libimage-exiftool-perl' instead of 'exiftool'
libimage-exiftool-perl is already the newest version (11.77-1).
The following package was automatically installed and is no longer required:
  libhwloc5
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 221 not upgraded.
```

- python: sudo apt-get install python && apt-get install python3

```
root@1onehawk:~# sudo apt-get install python && apt-get install python3
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
python is already the newest version (2.7.17-2).
The following package was automatically installed and is no longer required:
  libhwloc5
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 221 not upgraded.
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
python3 is already the newest version (3.7.5-1).
The following package was automatically installed and is no longer required:
  libhwloc5
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 221 not upgraded.
root@1onehawk:~# sudo apt-get install python && apt-get install python3
```

- exiv2: sudo git clone https://github.com/exiv2/exiv2

```
root@1onehawk:~# git clone https://github.com/Exiv2/exiv2.git
Cloning into 'exiv2'...
remote: Enumerating objects: 190, done.
remote: Counting objects: 100% (190/190), done.
remote: Compressing objects: 100% (98/98), done.
remote: Total 43597 (delta 102), reused 150 (delta 91), pack-reused 43407
Receiving objects: 100% (43597/43597), 89.70 MiB | 25.72 MiB/s, done.
Resolving deltas: 100% (32485/32485), done.
```

- exif-samples[6]: sudo git clone https://github.com/ianare/exif-samples
- python AES scripts: sudo git clone https://github.com/1onehawk/simua

4 Configuration and Execution

1. exiftool
   - Extracting Image Metadata

     $exiftool image.jpg > metadata.txt

   - Striping Image Metadata

     $exiftool -all= image.jpg

2. nano
   - For opening file nano file.py
   - For saving file ctrl+o
   - For exiting file ctrl+x

3. python

- Installing cryptography package

  $pip install cryptography

```
root@1onehawk: ~
root@1onehawk:~# pip install cryptography
Requirement already satisfied: cryptography in /usr/lib/python2.7/dist-packages (2.6.1)
```

- For Encryption and Key Derivation

  $python aespassenc.py

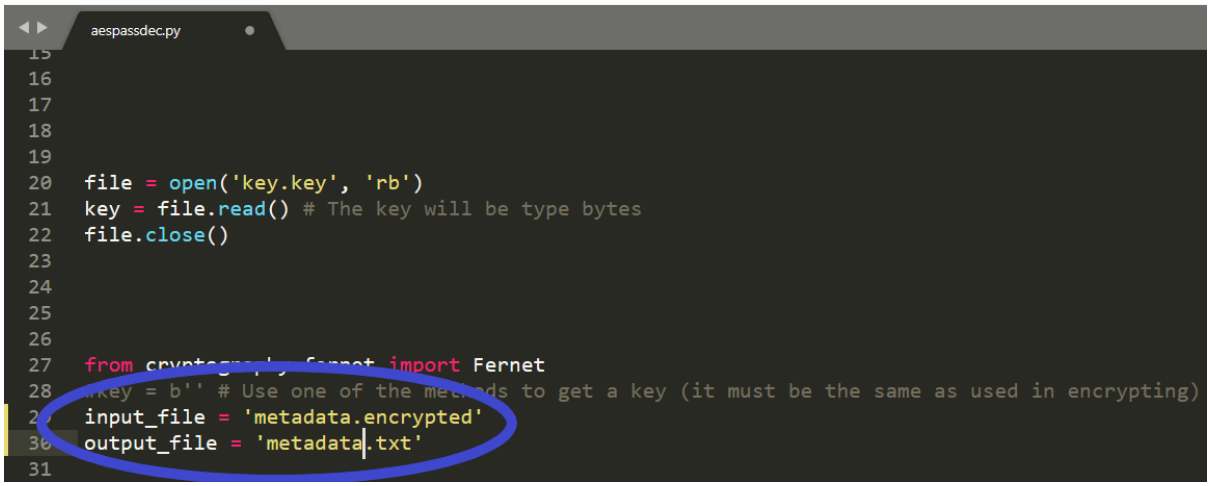
User has to manually specify the file name as the input, inside the script before running it

```
aespassenc.py
21
22
23  file = open('key.key', 'wb')
24  file.write(key) # The key is type bytes still
25  file.close()
26
27
28
29
30  from cryptography.fernet import Fernet
31  #key = ... # use one of the methods to get a key (it must be the same when decrypting)
32  input_file = 'metadata.txt'
33  output_file = 'metadata.encrypted'
34
35  with open(input_file, 'rb') as f:
36      data = f.read()
37
38  fernet = Fernet(key)
39  encrypted = fernet.encrypt(data)
40
41  with open(output_file, 'wb') as f:
42      f.write(encrypted)
43
44  # You can delete input_file if you want
45
46  import timeit
47  code_to_test = """
48  a = range(100000)
49  b = []
50  for i in a:
```

- For Decryption

  $python aespassdec.py

User has to manually specify the file name as the input, inside the script before running it



4. exiv2

•Add Image Description (Custom Tag)
$exiv2 -M"add Exif.Image.ImageDescription Ascii ajwdnkjawndkjabdw" mo img1.jpg

•Reading Metadata
$exiv2 -p a img1.jpg

References

[1]
"Exiv2 - Image metadata library and tools." [Online]. Available: https://www.exiv2.org/. [Accessed: 12-Dec-2019]

[2]
"ExifTool by Phil Harvey." [Online]. Available: https://exiftool.org/. [Accessed: 12-Dec-2019]

[3]
"GNU nano." [Online]. Available: https://www.nano-editor.org/. [Accessed: 12-Dec-2019]

[4]
"Welcome to Python.org," *Python.org*. [Online]. Available: https://www.python.org/. [Accessed: 12-Dec-2019]

[5]
"Git." [Online]. Available: https://git-scm.com/. [Accessed: 12-Dec-2019]

[6]
ianaré sévi, *ianare/exif-samples*. 2019 [Online]. Available: https://github.com/ianare/exif-samples. [Accessed: 12-Dec-2019]

[7]
"Linux.org," *Linux.org*. [Online]. Available: https://www.linux.org/. [Accessed: 12-Dec-2019]