Writeup for Email Incoming

Name : Email Incoming

Description : One fine day Johnny received an E-mail which had just this file. He wonders this might have been sent by one of his friend who was supposed to send a confidential message. But Johnny cannot figure out anything from this file. Can you help him retrieve the message????

No password was received with this file

Difficulty : Hard

Points : 500

Domain : Cryptography

Author : Ankush Kaudi

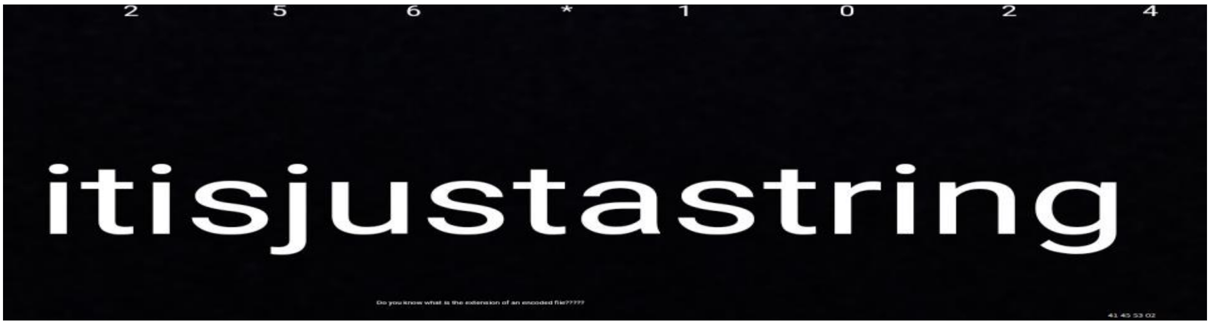
Given files : johny.zip

We have been given with a .zip.

Extracting the .zip file asks for the password which is not given. We can think of cracking the .zip using some tools.

One such tool is John The Ripper. Cracking the .zip using John gives the password as “thunderbird”.

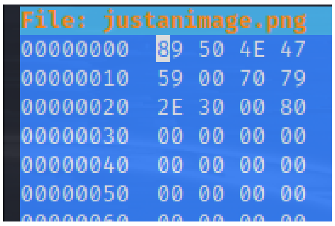
After extracting, 10 jpg image files appears named zero, one,…., nine. justanimage.png and a text file . Text file has the message - “Sometimes, what you see isn't what you get.” .Renaming the files with numbers instead of text as 0,1,…,9 we can see combining it gives the following image. There are 4 messages we can extract from it as


2 5 6 * 1 0 2 4
itisjustastring
Do you know what is the extension of an encoded file?????
41 45 53 02

1. 256*1024

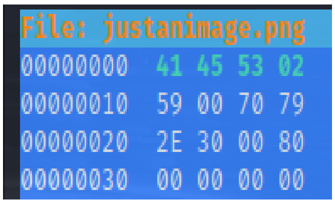
2. itisjustastring
3. Do you know what is the extension of an encoded file????
4. 41 45 53 02

With the text file, we can assume that the .png file might not be an image but something else. From the line 4 considering the numbers to be hexadecimal, we can change the headers of the .png with the given values. Using hexeditor can do this and also from line 3 the extension can be found as .enc save the file with extension as .enc after changing the headers.



```
File: justanimage.png
00000000  89 50 4E 47
00000010  59 00 70 79
00000020  2E 30 00 80
00000030  00 00 00 00
00000040  00 00 00 00
00000050  00 00 00 00
```

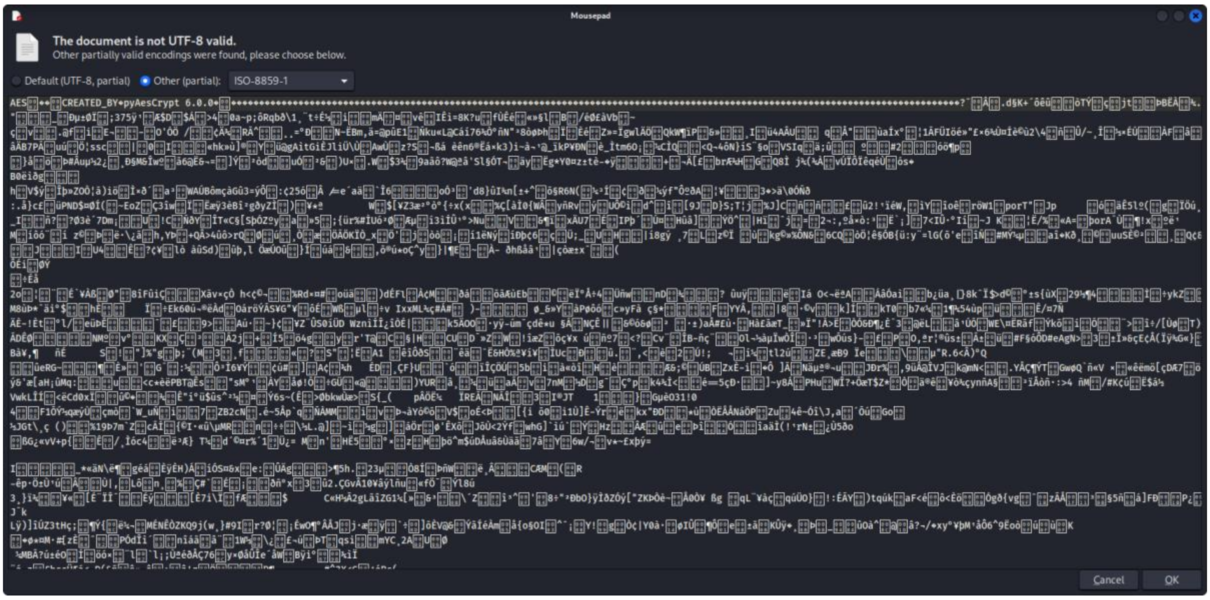
→ before changing the headers.



```
File: justanimage.png
00000000  41 45 53 02
00000010  59 00 70 79
00000020  2E 30 00 80
00000030  00 00 00 00
```

→ after changing the headers.

Opening the .enc with a text editor we'll get the following.



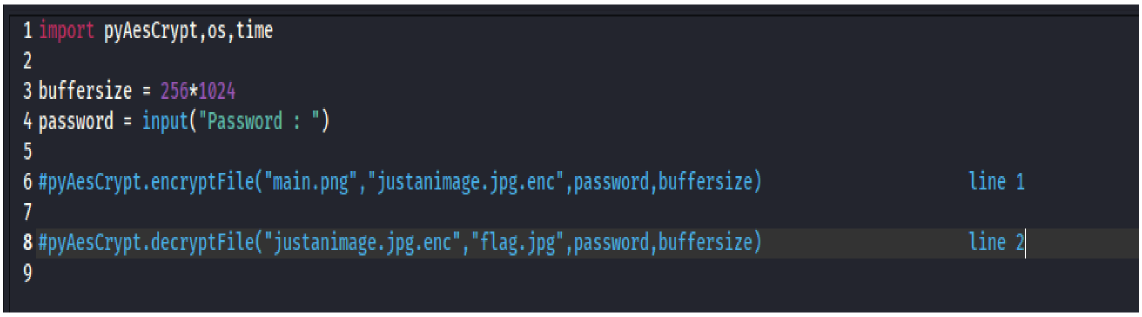
The document is not UTF-8 valid.
Other partially valid encodings were found, please choose below.

○ Default (UTF-8, partial) ● Other (partial): ISO-8859-1

```
AES CREATED_BY pyAesCrypt 6.0.0
```

From the first line we can see "created by pyAesCrypt", we can assume this file has been encrypted with pyAesCrypt of python which is an AES encryption module.

We can encrypt and decrypt with the in-built functions of this module.

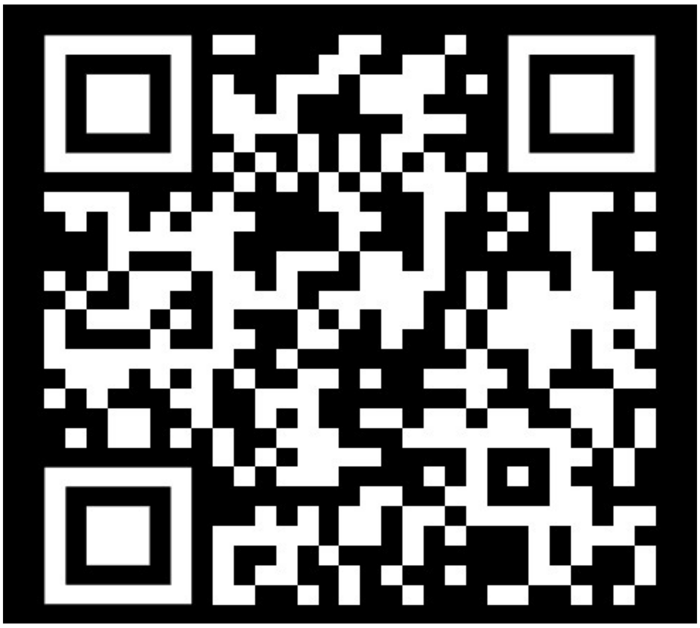


```
import pyAesCrypt,os,time

buffersize = 256*1024
password = input("Password : ")

#pyAesCrypt.encryptFile("main.png","justanimage.jpg.enc",password,buffersize)                    line 1

#pyAesCrypt.decryptFile("justanimage.jpg.enc","flag.jpg",password,buffersize)                    line 2

```

From the above code, line 1 is used to encrypt a file and line 2 is used to decrypt a file with a password.

The password is “itisjustastring” and buffersize is “256 * 1024” which can be obtained from the line 1 and 2.

After decryption, the below image appears which is an inverted qr code



We can invert the colours and obtain the original qr code

Scanning above qr code will give the flag

Flag : VishwaCTF{3ncrypt!0ns_4r3_b0r!ng!!!!}