ECB Second to solve this challenge!

Misc - 150 points

# Soal

|  |
| --- |
| [ecb.zip](https://ctf.idsecconf.org/download?file_key=128366c96d79cb4e56c942d3d82311513c96c247dccd450ab8901b17600cf566&team_key=2a3d00950bcec988c6f9a00242687028ade2e180c4a337d64a8761b253b2df59) - d9463e866066d577d217aab69eaefdd4 |

# Solusi

Di dalam arsip ZIP ada dua file:

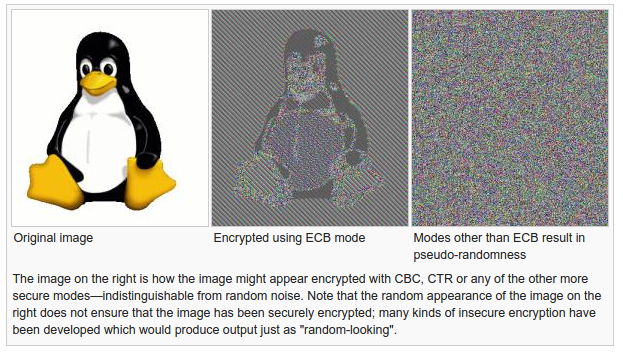
* File ecb.py yang sepertinya script yang dipakai buat mengenkripsi data
* flag.bmp.encrypted, file flag yang terenkripsi

Script mengenkripsi flag dengan AES mode ECB. Di script disebutkan IV tapi itu sebenarnya tipuan karena mode enkripsi ECB tidak menggunakan IV.

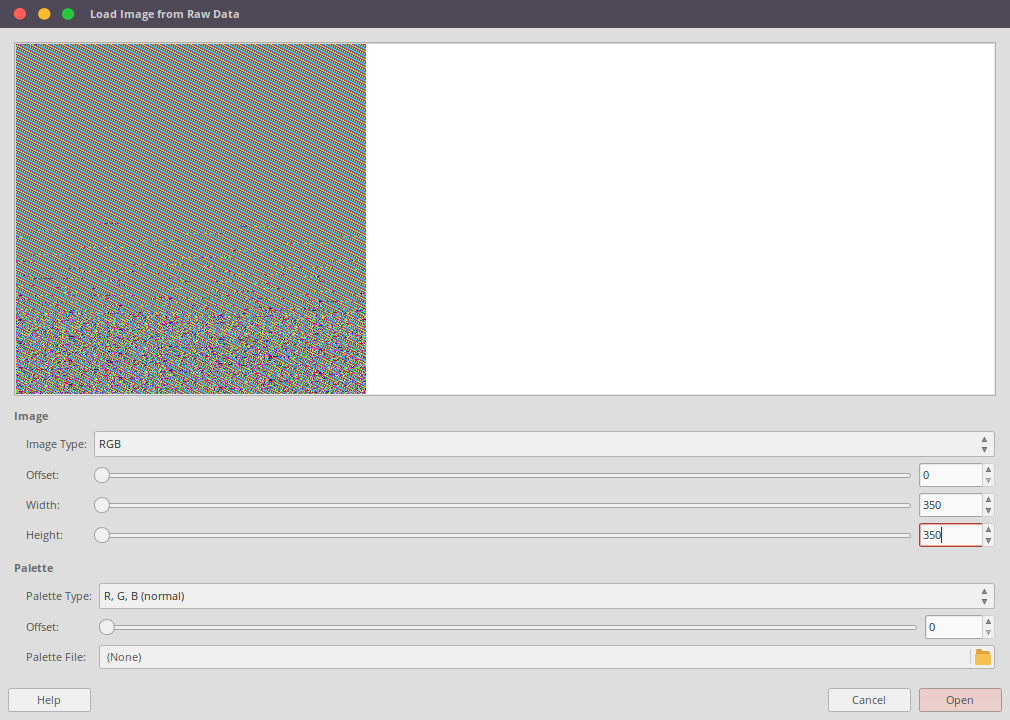
|  |
| --- |
| **from** **Crypto.Cipher** **import** AES **import** **sys** **import** **os** IV\_SIZE = 16 BLOCK\_SIZE = 16  key = sys.argv[1]  mode = AES.MODE\_ECB iv = os.urandom(IV\_SIZE) aes = AES.new(key, mode, iv)  **with** open(sys.argv[2], "rb") **as** f:  data = f.read()  padding = BLOCK\_SIZE - len(data) % BLOCK\_SIZE  data += padding \* "**\x00**"  encrypted = aes.encrypt(data)  **with** open(sys.argv[2] + ".encrypted", "wb") **as** f:  f.write(encrypted) |

Apa yang akan dilakukan? Key-nya tidak diketahui, tidak feasible juga di-bruteforce sepanjang 16 byte. Kita lirik file flagnya. File BMP yang terenkripsi. Seperti yang diketahui, file BMP tidak terkompresi. Kemudian, mode ECB memiliki kelemahan yaitu tidak menyembunyikan pola dari data asli, tapi hanya mengacak polanya saja. Artinya pola dari gambar flag aslinya seharusnya masih terlihat karena BMP.

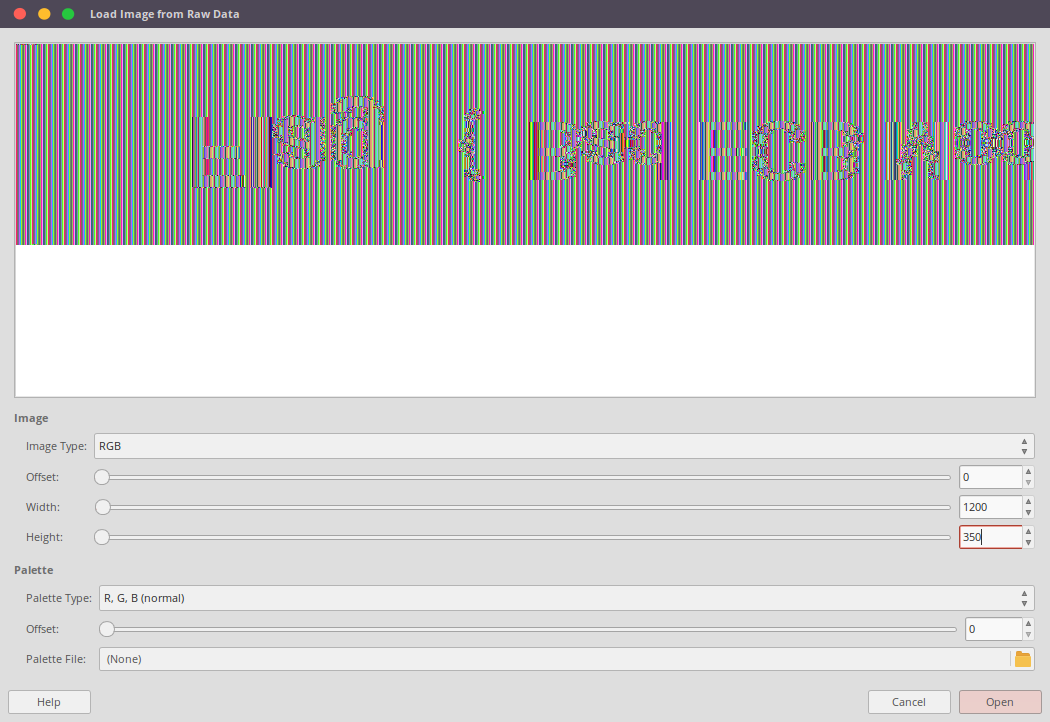
Anda bisa melihat [artikel Wikipedia ini](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation), dengan contoh gambar pinguin ini, terlihat ECB tidak menyembunyikan pola:



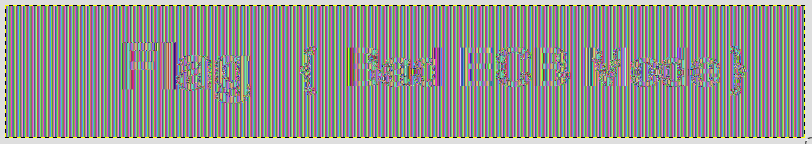
Maka langsung saja kita buka gambar terenkripsi dengan GIMP sebagai raw bytes (diubah ekstensinya menjadi .data).



Di sini kita perlu mencoba-coba nilai width-nya supaya terlihat pola yang jelas. Ternyata pada width = 1200 didapatkan pola:



Setelah dibalik, terbaca suatu kalimat Flag meski agak tidak jelas:



Didapatkan flag yang valid:

**Flag{Bad ECB Mode}**