tim wangy wangy



Felicia Sutandijo

Fransiskus Febryan Suggoitanoshi

Josep Marcello

# Foren

## Watashi no uso

Diberikan file watashi\_no\_uso.wav yang jika didengarkan adalah sebuah file musik, tapi ketika dimainkan pada awal musik terdengar suara-suara aneh. Pertama dicurigai, ini adalah SSTV dengan musik di salah satu channel dan audio SSTV di channel lain. Tapi, ketika dibuka di Audacity, kedua channel memiliki spektogram yang sama.

Akhirnya, dicoba untuk dibuka menggunakan hexedit. Ketika di-scroll, terlihat ada ciri khas file gambar JPEG, yaitu tulisan “JFIF.” Dicurigai ini adalah LSB atau MSB, tapi ketika dicoba keduanya gagal. Akhirnnya, dihitung jarak antara byte yang mengandung huruf “J” dan “F” adalah 130 bytes. Akhirnya, disimpulkan bahwa jarak antar-bytes untuk file gambarnya adalah 130 bytes. Selain itu, didapatkan juga lokasi pertama byte header untuk file JFIF-nya adalah byte ke-0x26C.

Untuk menyelesaikannya, dibuat sebuah script Python untuk memecah file musik tadi setiap 130 bytes lalu digabungkan kembali.

| wav = '' **with** open('./watashi\_no\_uso.wav', 'rb') **as** f:  wav = f.read()  dec = [i **for** i **in** wav] startByte = 0x26C dec = dec[startByte:] print(dec[:50]) dec = [dec[i] **for** i **in** range(0, len(dec), 130)] print(dec[:50]) bytes = bytearray(dec)  **with** open('./solv.jpg', 'wb') **as** f:  f.write(bytes) |
| --- |

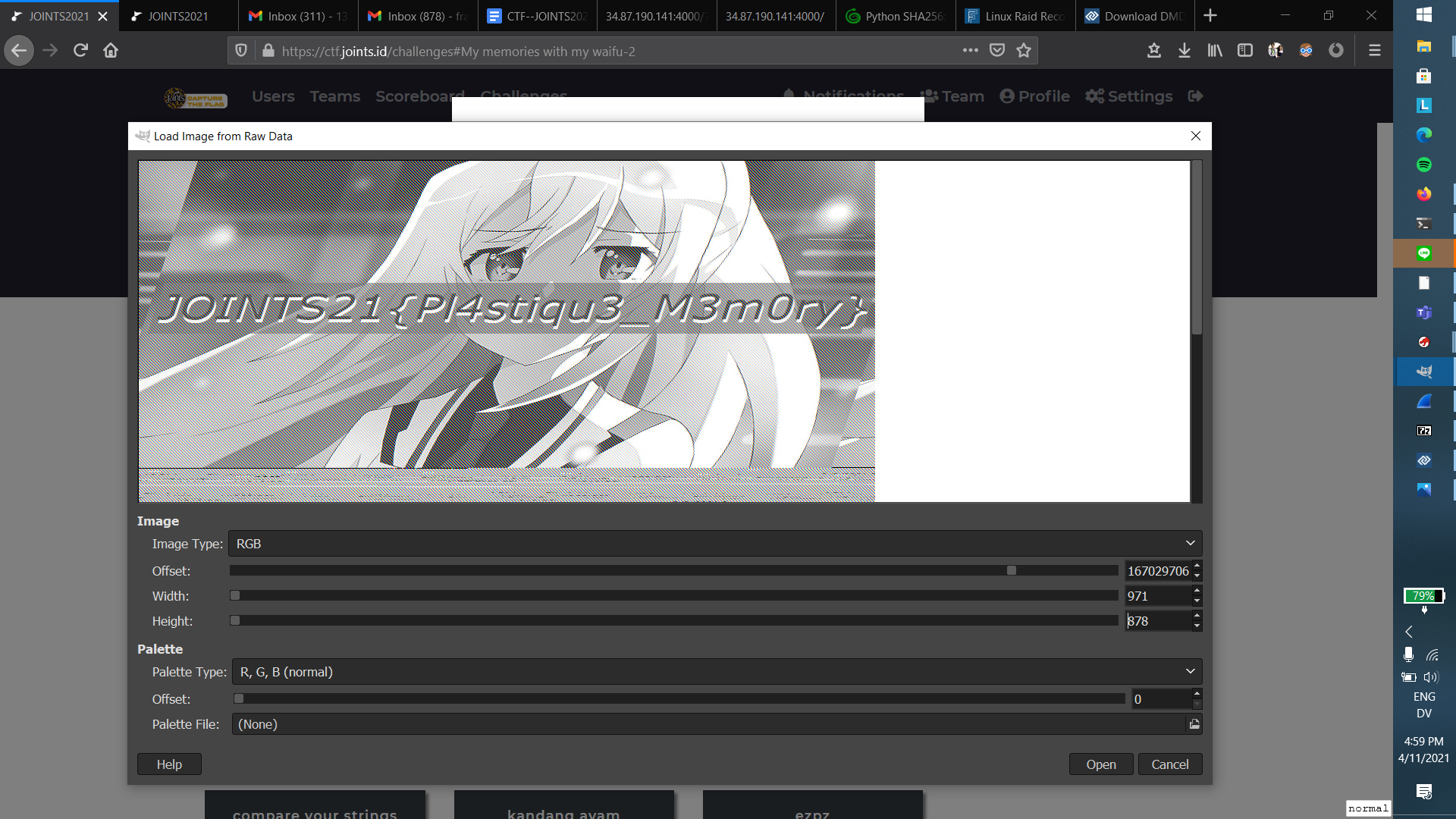
Ketika script dijalankan, didatpakan file JPG:



Flag: JOINTS21{I\_hope\_this\_reaches\_you}

## My memories with my waifu

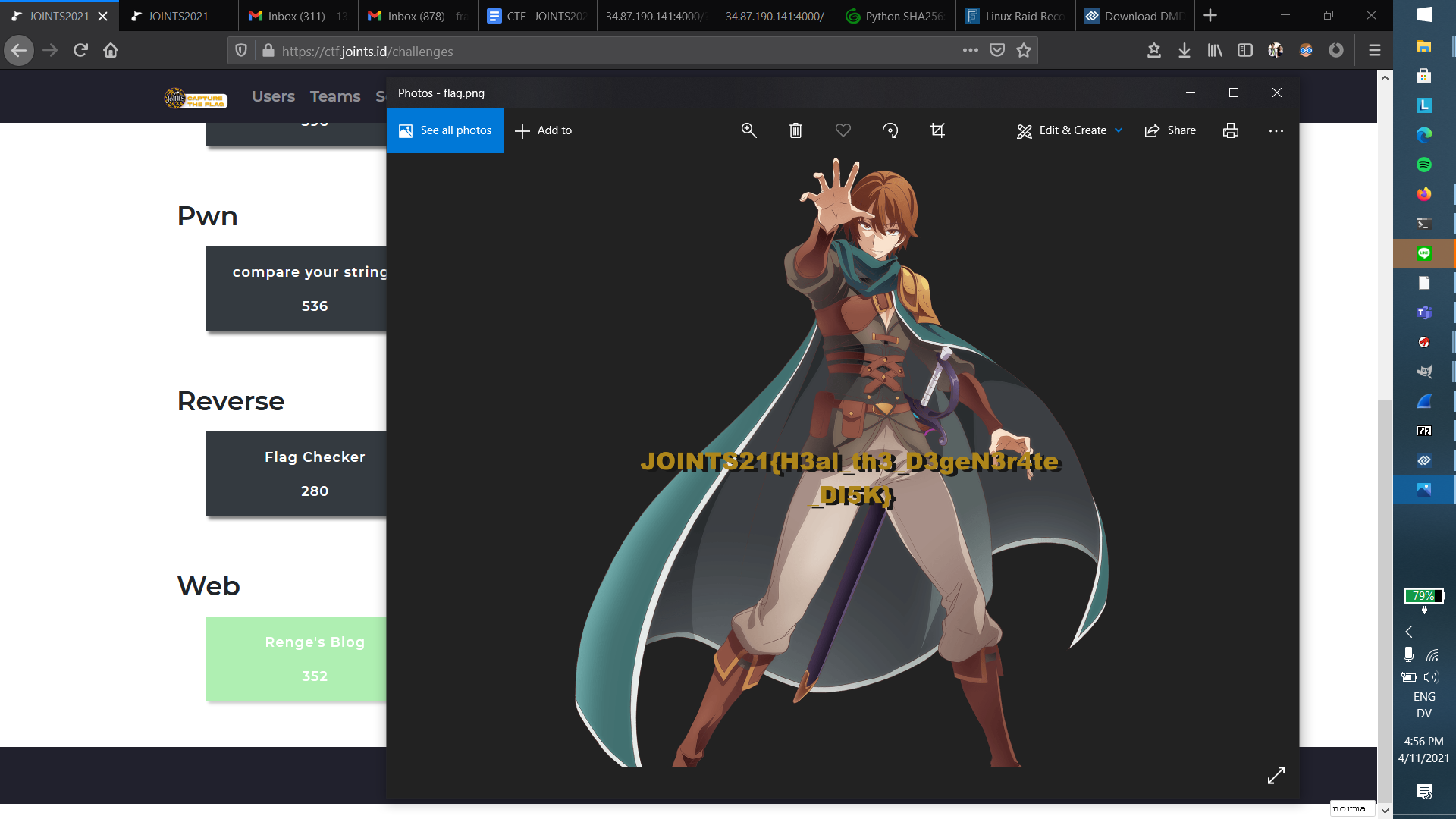
Diberikan memory dump MEMORY.DMP. Analisis dengan volatility, setelah dilihat proses yang ada, ada satu proses yang menarik perhatian yaitu NotMyFault.exe. Namun, setelah ditelusur lebih jauh, dengan `volatility windows.cmdline`, terlihat bahwa flag sebenarnya ada di mspaint.exe. Untuk mencari flagnya, buka memory dump dengan gimp sebagai raw data, lalu cari sampai ketemu. :D



Flag: JOINTS21{Pl4stiqu3\_M3m0ry}

## Where is the file

Diberikan satu file zip yang berisi 4 image. Awalnya dipikir 4 image hasil dump dari memory, ternyata bukan itu. Lalu mikir, mungkin hasil disk dump. Setelah dicoba mount, ternyata tebakannya lumayan dekat. Keempat image tersebut adalah bagian dari RAID :D. Awalnya mikir gimana cara nyatuinnya, karena belum pernah pegang RAID sama sekali. Setelah googling sedikit, didapatlah DMDE, tapi stripe size nya nebak. Ditebaklah beberapa kali, sampe dapet nilainya: 512KB. Ketemu deh, filenya!



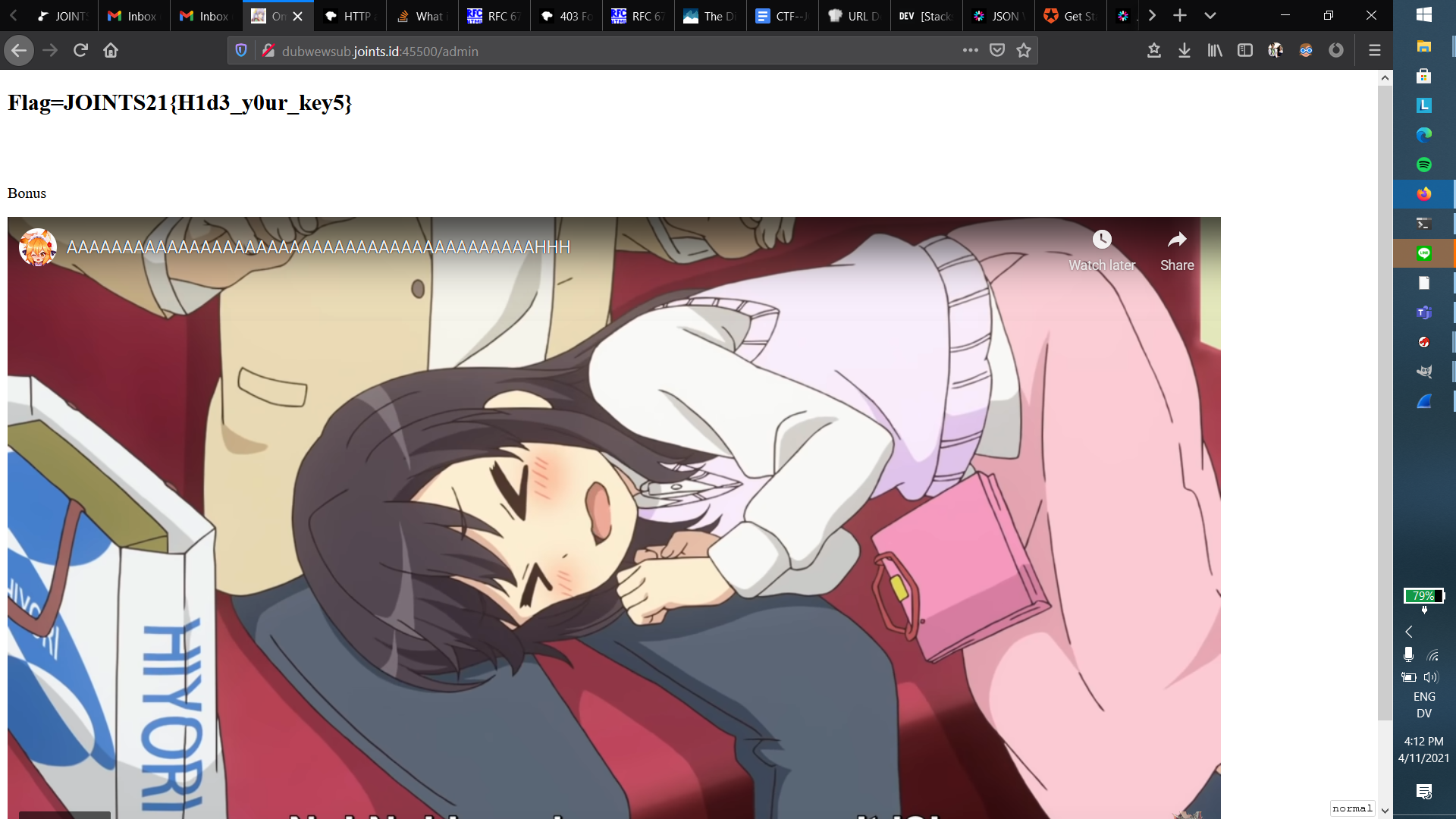
Flag: JOINTS21{H3al\_th3\_D3geN3r4te\_DI5K}

# 

# Web

## Renge’s Blog

Insting pertama yang dilakukan setelah membuka web: tentu saja inspect element! Lalu dari situ, muncul sesuatu yang menarik: public.key. Dicoba akses bisa. Tapi setelahnya stuck, lari ke soal lain dulu. Setelah merenungi sekian lama, lalu terpikir “kalau ada public, berarti ada private key?” Ternyata benar, ada public.key juga. Setelah itu stuck lagi. Tidak lama setelahnya, muncul ide JWT. Ternyata betul pake JWT, di bagian client ada cookie yang bernama “token”, isinya JWT :D ubahlah isinya sedikit (ada field admin, ganti jadi true), masuk deh ke admin!



Flag: JOINTS21{H1d3\_y0ur\_key5}