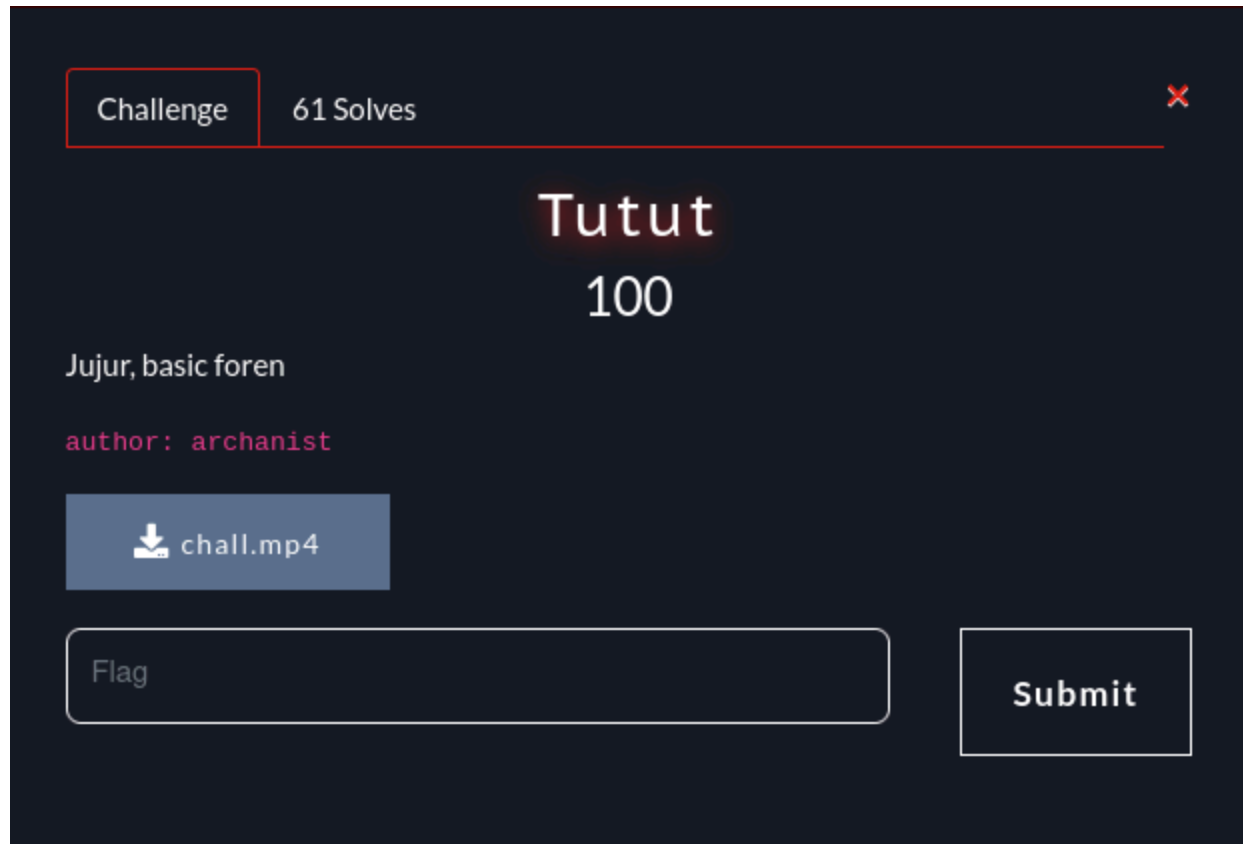


Write-Up: Tutut

Player: Constantine

Kategori: Forensik

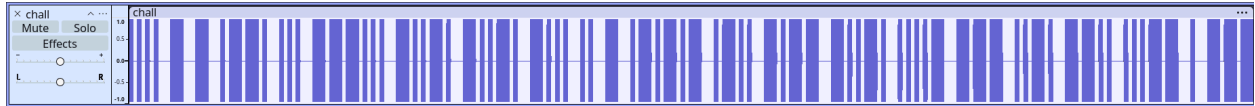


Konteks Dikit

Challenge ini dimulai dengan sebuah file audio chall.wav, di dashboard challenges namanya chall.mp4 mungkin typo. Gak ada petunjuk teks yang eksplisit, hanya file audio tersebut. Namun, penyelesaiannya ternyata membutuhkan beberapa layer investigasi, mulai dari steganografi audio sampai ekstraksi metadata gambar.

Phase 1: Audio Reconnaissance

Langkah pertama, seperti biasa saat menghadapi file audio tak dikenal di CTF, adalah analisis spektrum dan waveform. Aku langsung buka file chall.wav pakai **Audacity**. Secara visual, waveform menunjukkan ada burst suara pendek, panjang, sama hening. Ini jelas signaturnya Morse Code.



Phase 2: Decoding & HUMINT Tipis-Tipis

Aku pakai website [Morse Code World Adaptive Audio Decoder](#). Tools online ini bisa langsung translate file audio .wav menjadi teks. Setelah proses decoding selesai, output yang keluar bukan flag, melainkan sebuah URL:

Link ini adalah trigger. Link bit.ly ini adalah token yang harus diserahkan kepada author challenge ini, yaitu [archanist](#) alias **Bang Paul**. Langsung saja kita melakukan 3-way handshake dengan Bang Paul via WhatsApp dan mengirimkan link hasil decode tersebut sebagai bukti progress.



Bang Pawul



August 22, 2025

🔒 Messages and calls are end-to-end encrypted.
Only people in this chat can read, listen to, or
share them. Learn more.

Wednesday

bang paul, dah nemu tutut ni <http://bit.ly/40FZ3EM> 23:17 ✓✓



Proton Drive

The safest way to store or share your files

Proton Drive

Securely store, share, and access your
important files and photos. Anytime,
anywhere.

bit.ly

<https://bit.ly/4oFZ3eO> lanjut
make ini ya

23:18



okee bang 23:18 ✓✓



Message



Responnya positif. Bang Paul langsung kasih link yang valid menuju Proton Drive.

Phase 3: Image Forensics & Extraction

Link Proton Drive tersebut berisi satu file gambar bernama flag.png. Aku download file tersebut. Gambar tersebut corrupt, langsung curiga flag disembunyikan di dalam metadata file. Aku pakai Exiftool di terminal untuk membedah metadata gambar tersebut:

```
constantine ~/OprecForesty/tutut (solved) 09:13 > ls
-rw-r--r-- 129k constantine 12 Nov 20:11 chall.wav
-rw-r--r-- 7.2k constantine 12 Nov 23:20 flag.png

constantine ~/OprecForesty/tutut (solved) 09:14 > exiftool flag.png
ExifTool Version Number      : 13.36
File Name                    : flag.png
Directory                    : .
File Size                    : 7.2 kB
File Modification Date/Time   : 2025:11:12 23:20:40+07:00
File Access Date/Time        : 2025:11:12 23:20:40+07:00
File Inode Change Date/Time   : 2025:11:12 23:20:51+07:00
File Permissions              : -rw-r--r--
File Type                    : PNG
File Type Extension           : png
MIME Type                    : image/png
Warning                      : PNG image did not start with IHDR [x5]
Palette                      : (Binary data 660 bytes, use -b option to extract)
Artist                      : FORESTY{m0rs3333_4nDD_m3t4d44t44_4r3_b451c5} this is real flag btw :v

constantine ~/OprecForesty/tutut (solved) 09:14 > _
```

Benar aja, di antara tumpukan data gambar, ada satu baris di bagian Artist yang berisi format flag.

Flagnya adalah **FORESTY{m0rs3333_4nDD_m3t4d44t44_4r3_b451c5}**