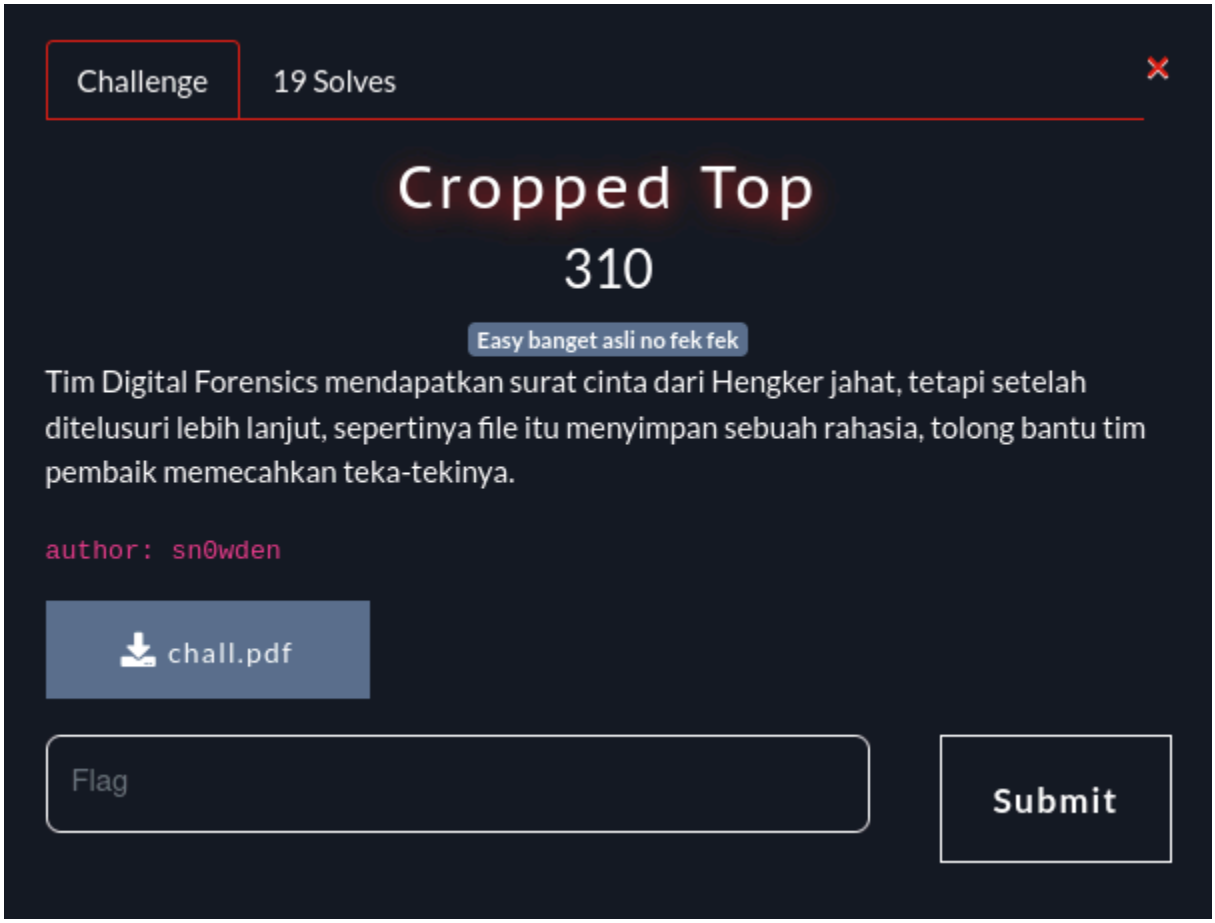
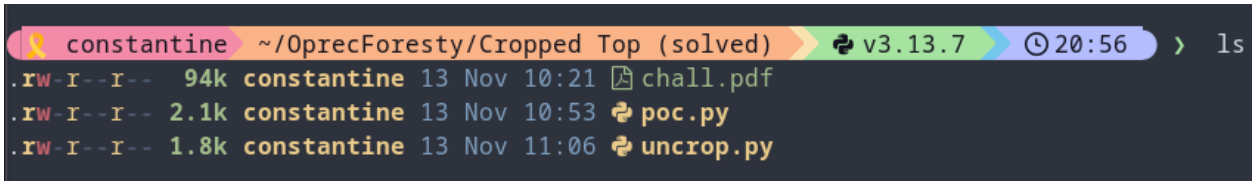
Cropped Top

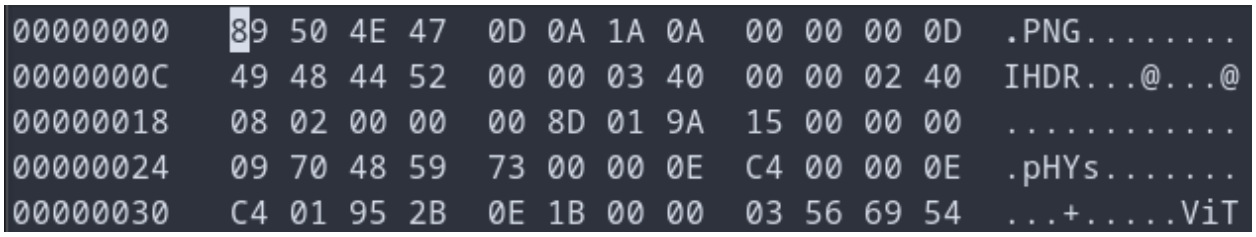
Player: constantine
Kategori: Forensik

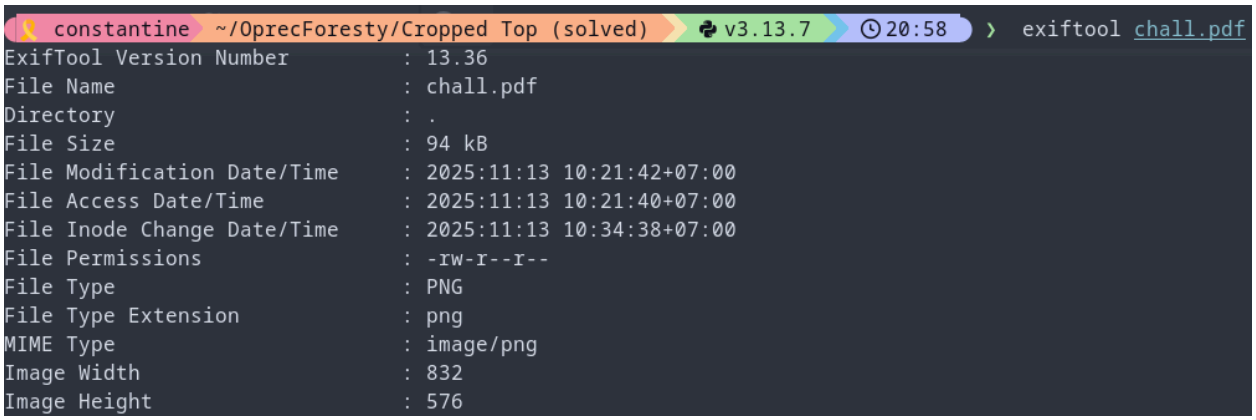


Phase 1: Initial Recon



File awal bernama *chall.pdf*. Saat dibuka, viewer melaporkan file corrupt. Langkah pertama adalah mengecek tipe file sebenarnya.



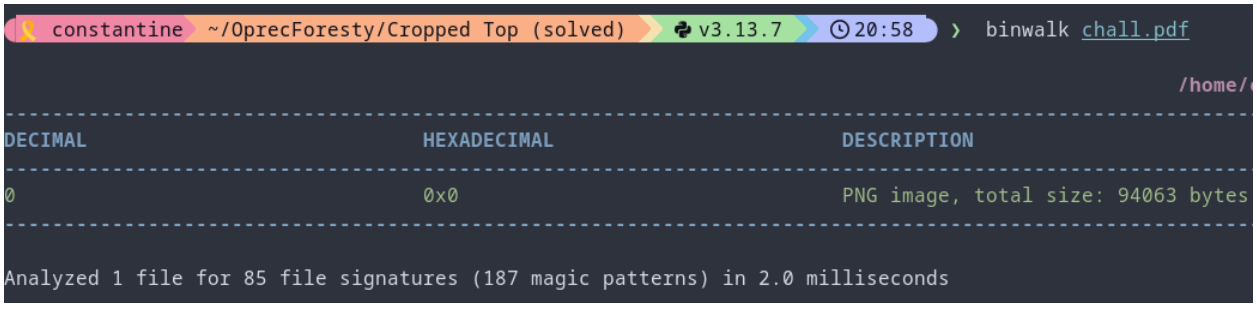


Setelah dicek menggunakan exiftool dan hex view, terlihat bahwa:

- Ekstensi adalah .pdf
- **Magic bytes menunjukkan PNG** (89 50 4E 47 0D 0A 1A 0A)

Dengan kata lain, ini adalah **PNG yang disamarkan sebagai PDF**.

Phase 2: Structural Validation



Analisis menggunakan binwalk menunjukkan:

- Satu buah PNG image

- Tidak ada payload tambahan (ZIP, embedded file, dsb)

```
constantine ~/OprecForesty/Cropped Top (solved) v3.13.7 20:58 ❯ zsteg chall.pdf
extradata:imagedata ..
    00000000: 00 f8 f8 f8 f8 f8 f8 f8  f8 f8 f8 f8 f8 f8 f8 f8  |................|
    00000010: f8 f8 f8 f8 f8 f8 f8 f8  f8 f8 f8 f8 f8 f8 f8 f8  |................|
    *
```

```
'String#index': incompatible encoding regexp match (BINARY (ASCII-8BIT) regexp with UTF-8 string) (Encoding::CompatibilityError)
```

Menggunakan zsteg muncul indikasi error pada metadata Adobe XMP, namun tidak ditemukan stego Saat dicoba dibuka sebagai PNG (rename → .png), viewer tetap gagal load.

Phase 3: Repairing the Broken PNG

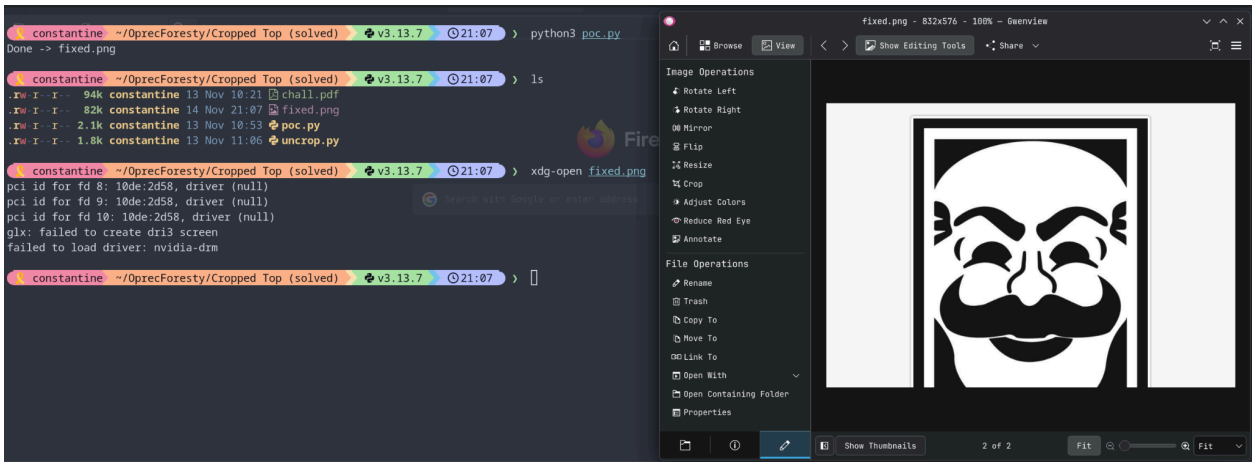
Saya menggunakan ChatGPT untuk membuat scriptnya, poc.py:

```
#!/usr/bin/env python3
import struct, zlib

FNAME = "chall.pdf"

data = open(FNAME, "rb").read()

assert data[:8] == b"\x89PNG\r\n\x1a\n", "Not a PNG file"

pos = 8
ihdr_data = None
other_chunks = []
idat_data = b""

while pos + 8 <= len(data):
    length = int.from_bytes(data[pos:pos+4], "big")
    ctype  = data[pos+4:pos+8]
    pos   += 8
    if pos + length + 4 > len(data):
        break

    cdata = data[pos:pos+length]
```

```
    crc   = data[pos+length:pos+length+4]
    pos  += length + 4

    if ctype == b"IHDR":
        ihdr_data = cdata
    elif ctype == b"IDAT":
        idat_data += cdata
    elif ctype == b"IEND":
        break
    else:
        other_chunks.append((ctype, cdata))

assert ihdr_data is not None, "IHDR not found"
assert idat_data, "No IDAT data"


decomp = zlib.decompressobj()
raw = b""
chunk = idat_data

try:
    raw = decomp.decompress(chunk)
except Exception as e:
    raw += decomp.unconsumed_tail

if not raw:
    raise SystemExit("Failed to decompress IDAT")

def make_chunk(ctype, cdata):
    length = len(cdata).to_bytes(4, "big")
    crc = zlib.crc32(ctype + cdata) & 0xFFFFFFFF
    crc = crc.to_bytes(4, "big")
    return length + ctype + cdata + crc

new_idat = zlib.compress(raw, 9)

out = b"\x89PNG\r\n\x1a\n"
out += make_chunk(b"IHDR", ihdr_data)

for ctype, cdata in other_chunks:
    out += make_chunk(ctype, cdata)

out += make_chunk(b"IDAT", new_idat)
```

```
out += make_chunk(b"IEND", b"")

open("fixed.png", "wb").write(out)
print("Done -> fixed.png")
```

Tinggal jalankan [poc.py](poc.py):



Muncullah gambar bertema fsociety dari Mr.Robot, namun **bagian bawah terpotong**. Berarti **height pada IHDR tidak sesuai jumlah scanline sebenarnya**.

Phase 4: Image Reconstruction

Kita gunakan ChatGPT untuk membuat python script agar IHDRnya sesuai, uncrop.py:

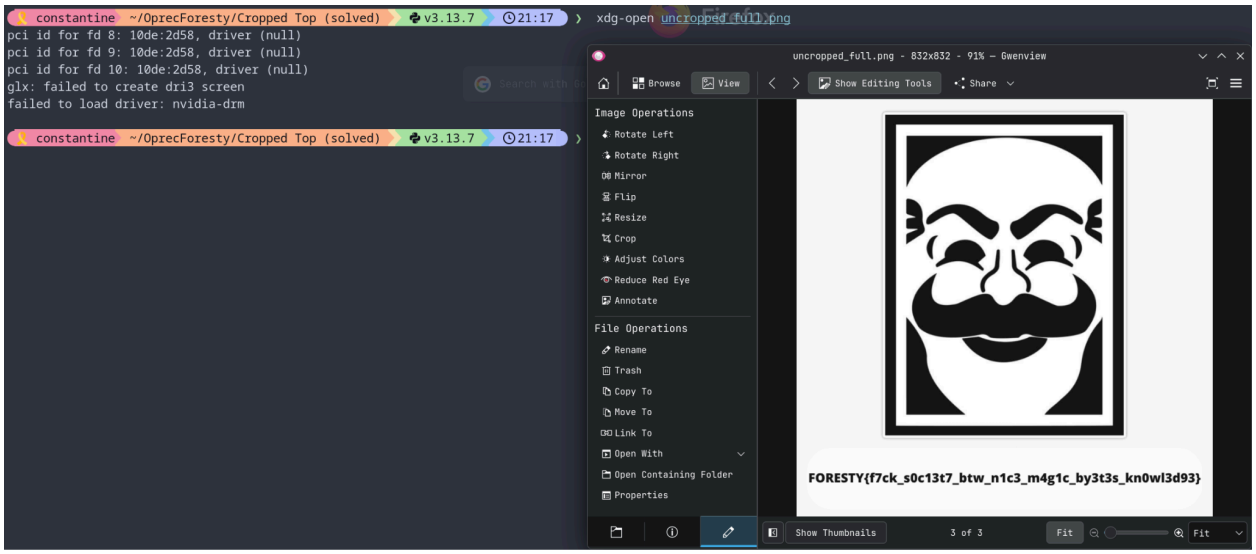
```
#!/usr/bin/env python3
import struct, zlib

FNAME = "chall.pdf"
data = open(FNAME, "rb").read()
assert data[:8] == b"\x89PNG\r\n\x1a\n", "Not a PNG"

pos = 8
ihdr = None
idat = b""

# --- parse IHDR & IDAT ---
while pos + 8 <= len(data):
```

```
    length = int.from_bytes(data[pos:pos+4], "big")
    ctype  = data[pos+4:pos+8]
    pos   += 8
    cdata = data[pos:pos+length]
    pos   += length
    crc   = data[pos:pos+4]
    pos   += 4

    if ctype == b"IHDR":
        ihdr = cdata
    elif ctype == b"IDAT":
        idat += cdata
    elif ctype == b"IEND":
        break

assert ihdr is not None, "IHDR not found"
assert idat, "No IDAT data"

# --- info asli dari IHDR ---
width, height, bit_depth, color_type, comp, filt, inter = \
    struct.unpack(">IIBBBBB", ihdr)

bpp_map = {0:1, 2:3, 3:1, 4:2, 6:4}
bpp = bpp_map[color_type]
rowlen = 1 + width * bpp

print("old height =", height)
print("rowlen =", rowlen)

# --- decompress semua IDAT ---
raw = zlib.decompress(idat)
print("len(raw) =", len(raw))

total_rows = len(raw) // rowlen
print("total_rows =", total_rows)

new_height = total_rows

# --- build IHDR baru ---
new_ihdr = struct.pack(">IIBBBBB",
                       width, new_height,
                       bit_depth, color_type,
                       comp, filt, inter)
```

```
new_idat = zlib.compress(raw, 9)

def chunk(ctype, cdata=b""):
    length = len(cdata).to_bytes(4, "big")
    crc = zlib.crc32(ctype + cdata) & 0xFFFFFFFF
    return length + ctype + cdata + crc.to_bytes(4, "big")

png = b"\x89PNG\r\n\x1a\n"
png += chunk(b"IHDR", new_ihdr)
png += chunk(b"IDAT", new_idat)
png += chunk(b"IEND")

open("uncropped_full.png", "wb").write(png)
print("Wrote uncropped_full.png")
```

Height pada IHDR diubah menjadi **832**, kemudian:

1. Raw image data disusun ulang menggunakan seluruh scanline
2. IDAT dikompres ulang
3. PNG baru dibangun dari awal (IHDR + IDAT + IEND)



Hasilnya gambar berhasil terbuka penuh dan bagian yang hilang muncul.

Di bagian paling bawah terdapat flag yang jelas.

Final Flag

FORESTY{f7ck_s0c13t7_btw_n1c3_m4g1c_by3t3s_kn0wl3d93}