# WRITEUP GEMASTIK 15
# H4ckM3

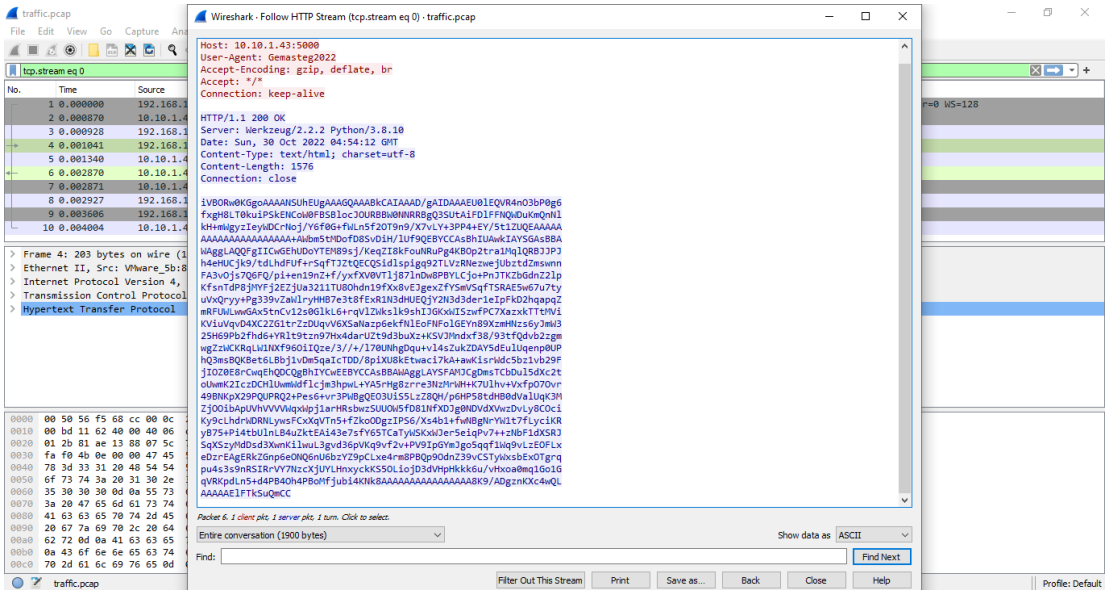
## Forensics

1. Traffic Enjoyer

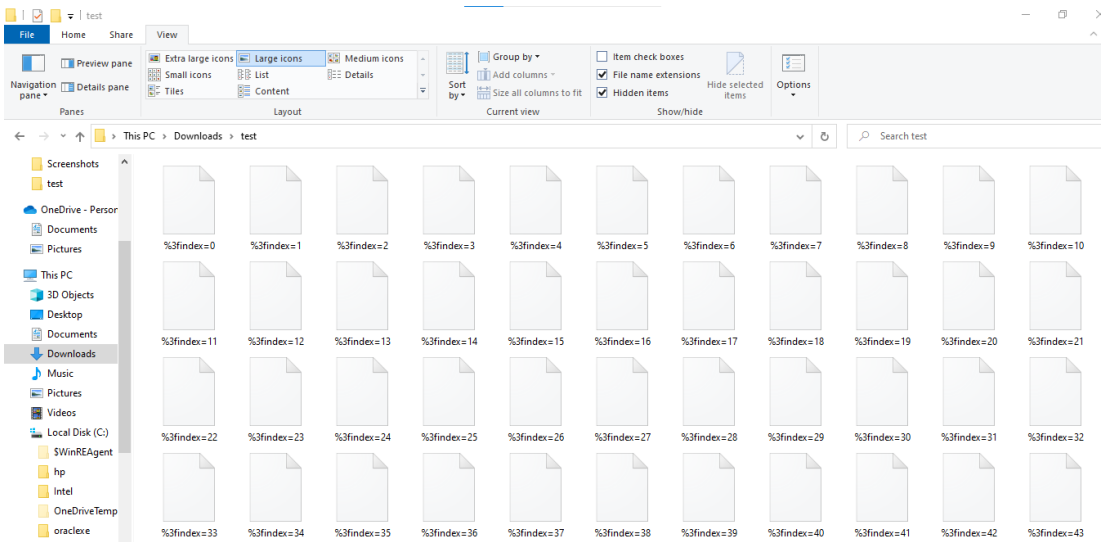
   diberikan sebuah file traffic.pcap

   penyelesaian:

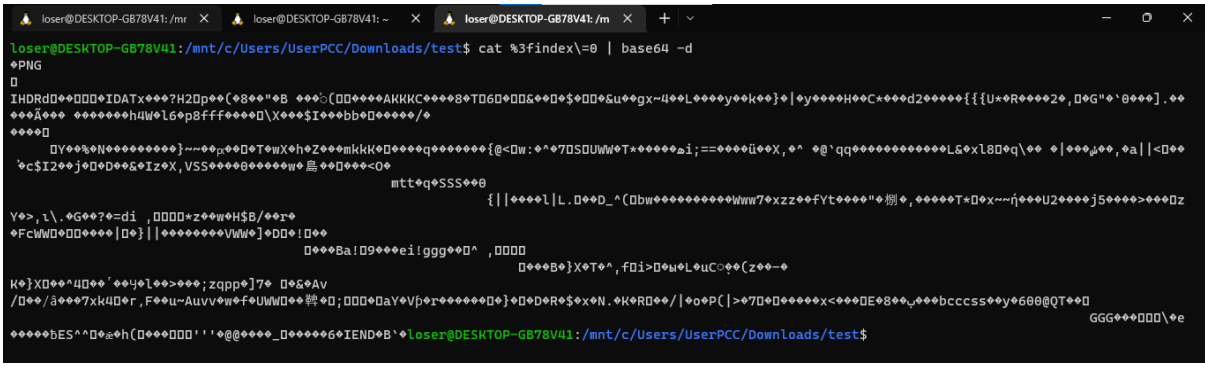
   - buka file traffic.pcap menggunakan wireshark, follow http stream pada salah satu request, terdapat http response yang mengembalikkan base64 encode



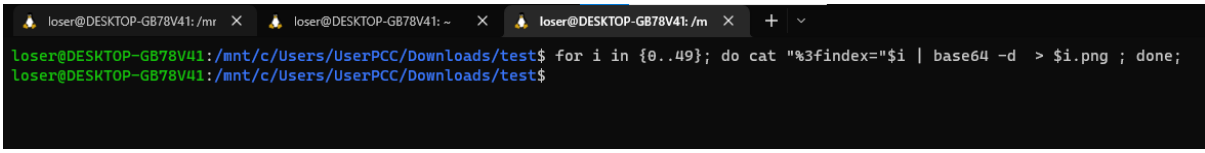

   - extract object HTTP



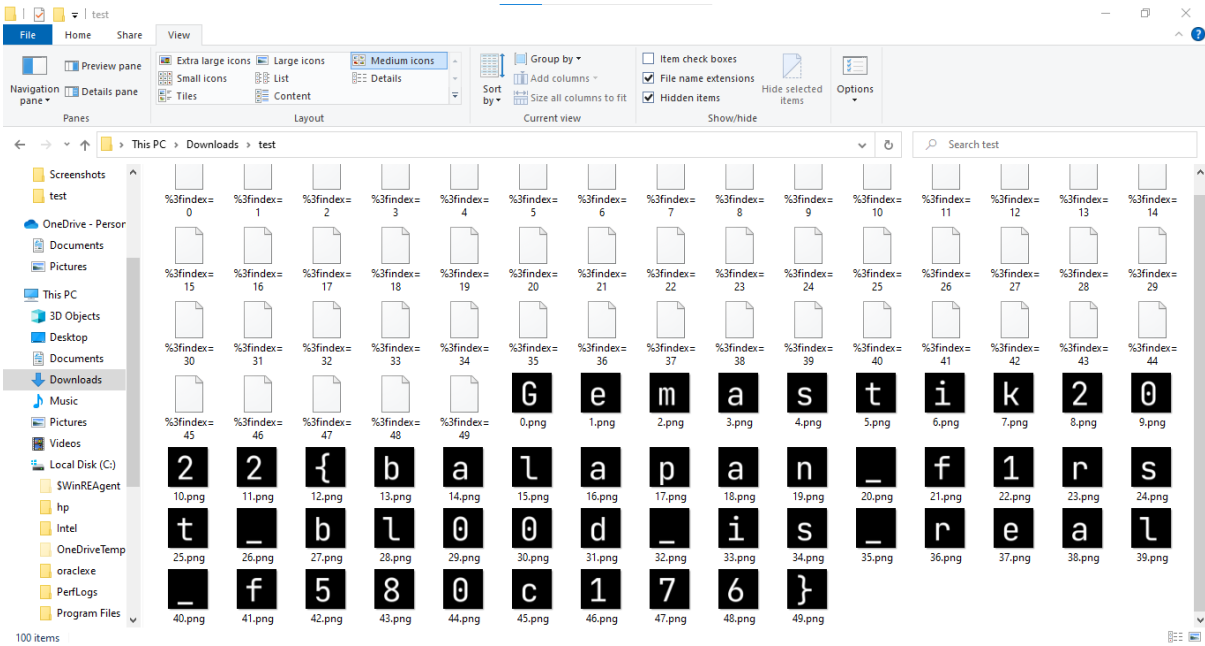
- dari base64 tadi setelah didecode diketahui bahwa ternyata file gambar png




- kemudian lakukan perulangan untuk melakukan base64 decode selanjutnya disimpan sebagai file png




- didapatkan gambar yang berisi kumpulan huruf ketika disatukan menjadi flag

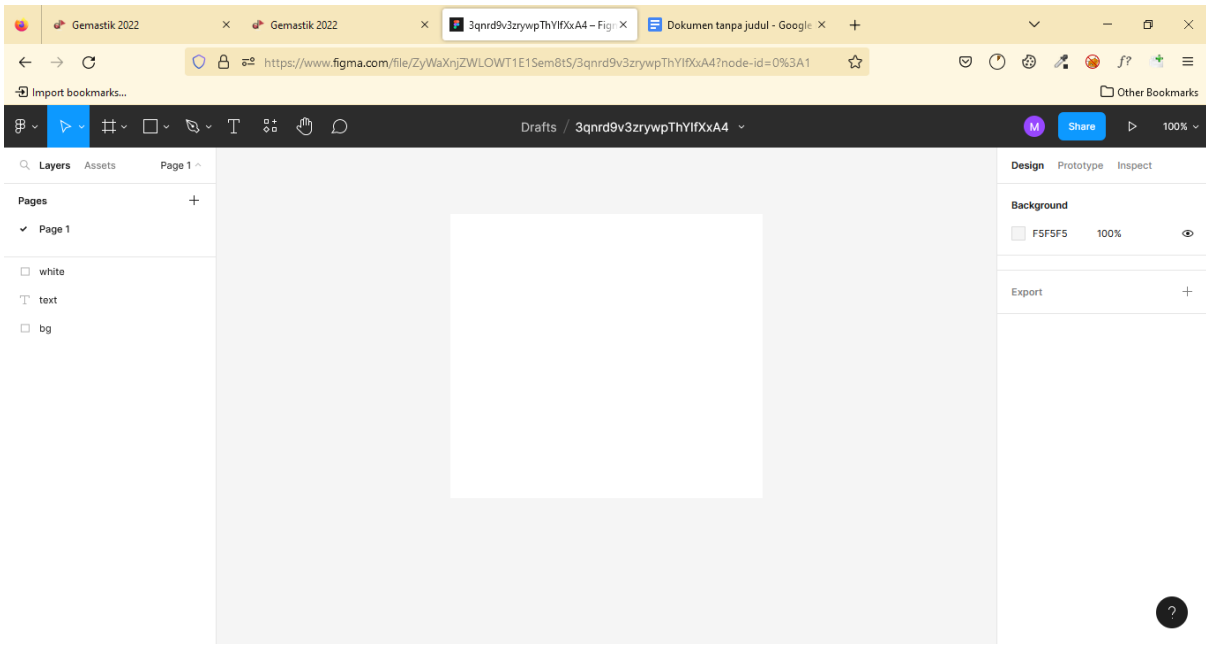



- flagnya: Gemastik2022{balapan_f1rst_bl00d_is_real_f580c176}

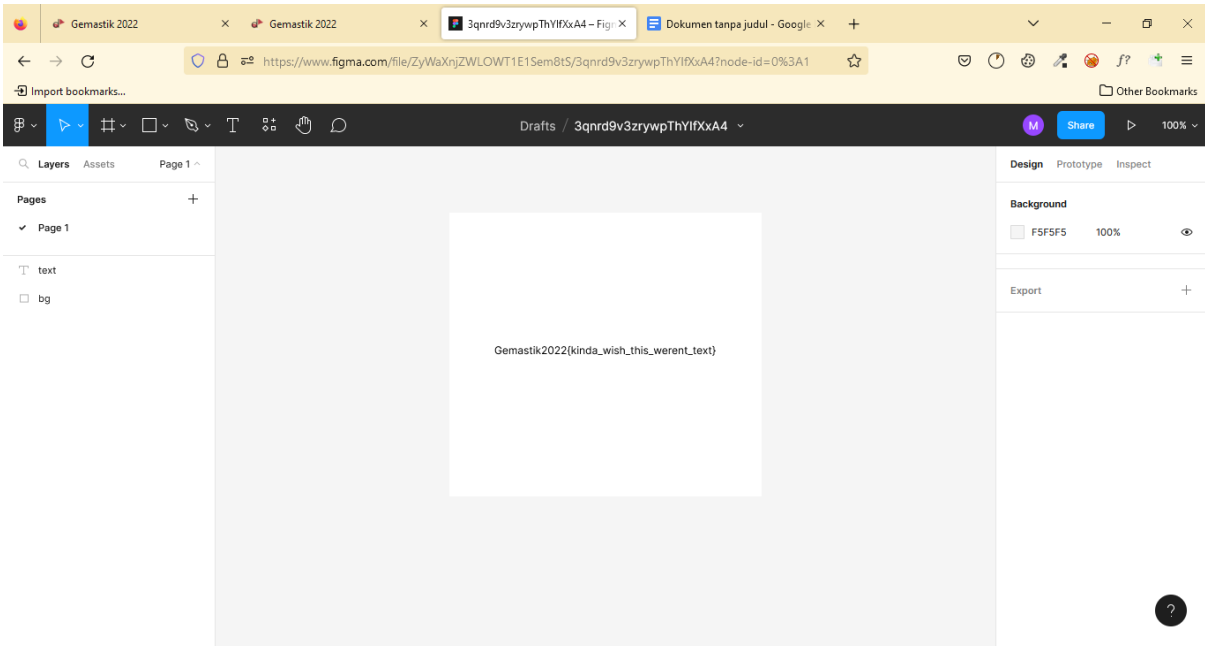
2. Har
   diberikan sebuah file gemasteg.har
   penyelesaian:
   - setelah dianalisis ternyata terdapat url canvas linknya: [3qnrd9v3zrywpThYlfXxA4.fig]


   - ketika dibuka lewat browser didapatkan file figma dengan extensi .fig

   - kemudian coba import file tersebut pada figma



- hapus layer white maka akan muncul text flag




- flagnya: Gemastik2022{kinda_wish_this_werent_text}