

[Capture The Flag]

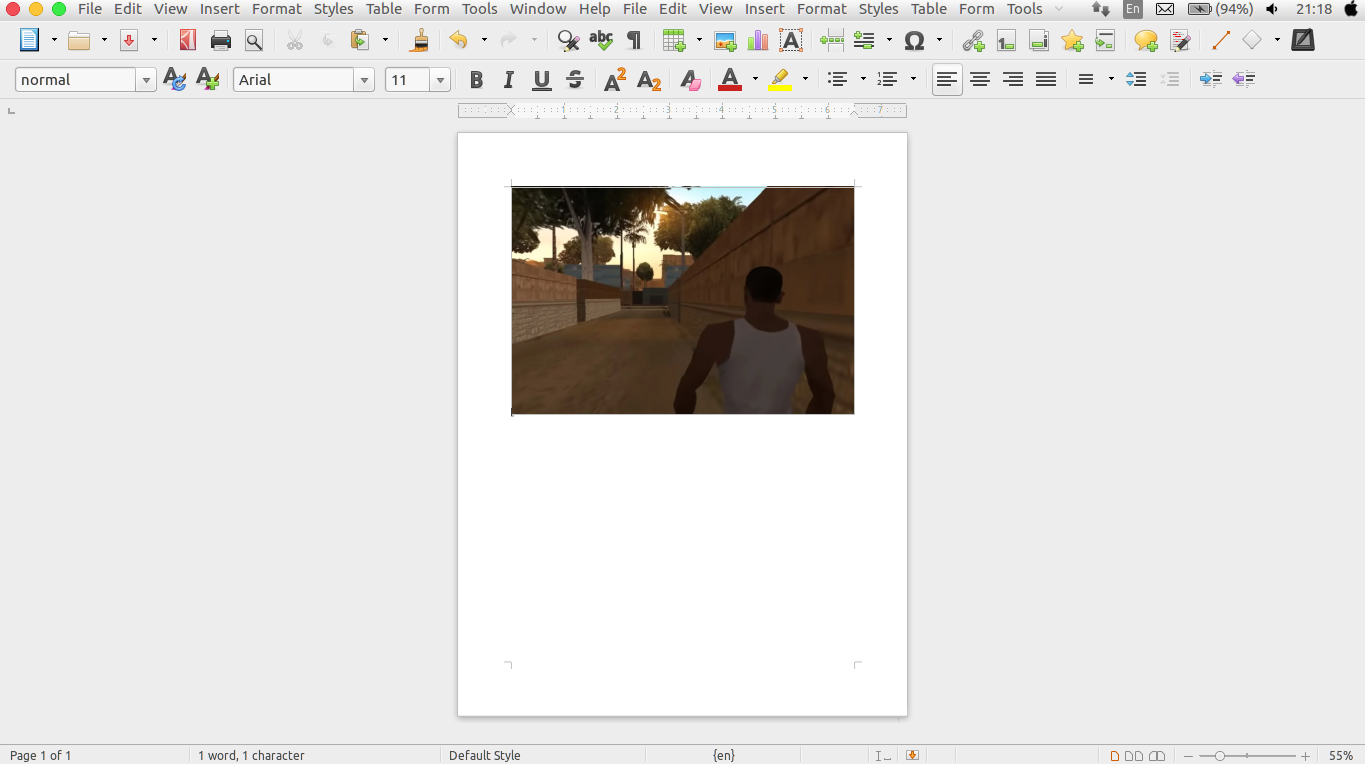
**NAMA TIM : Kandas***\*Ubah sesuai dengan nama tim anda*

Sabtu 7 September 2019

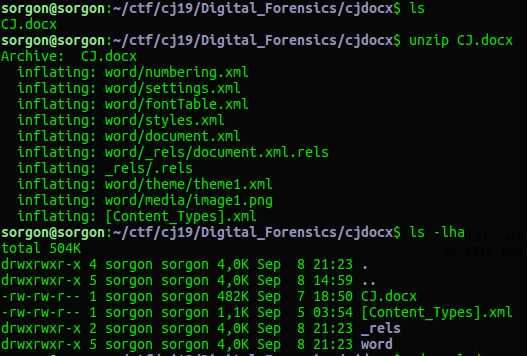
|  |  |
| --- | --- |
| **Ketua Tim** | |
| **1.** | Sorgon |
| **Member** | |
| **1.** | Codeparty |
| **2.** |  |

**1. CJ.docx { *Digital Forensic ;* 100 point }**

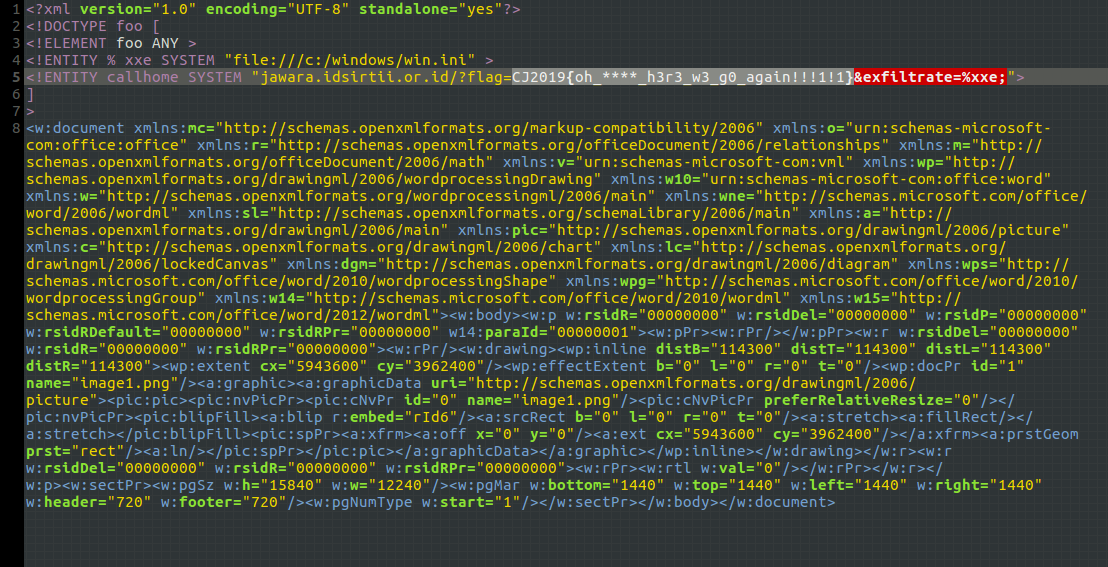
Diberikan File CJ.docx berisikan gambar yang bisa didengar.

**

Lalu akhirnya kami mencoba untuk mengekstrak file CJ.docx karena mungkin ada yang menarik di dalamnya.



Setelah kami buka satu persatu menggunakan ‘gedit’, ternyata muncul di word/document.xml

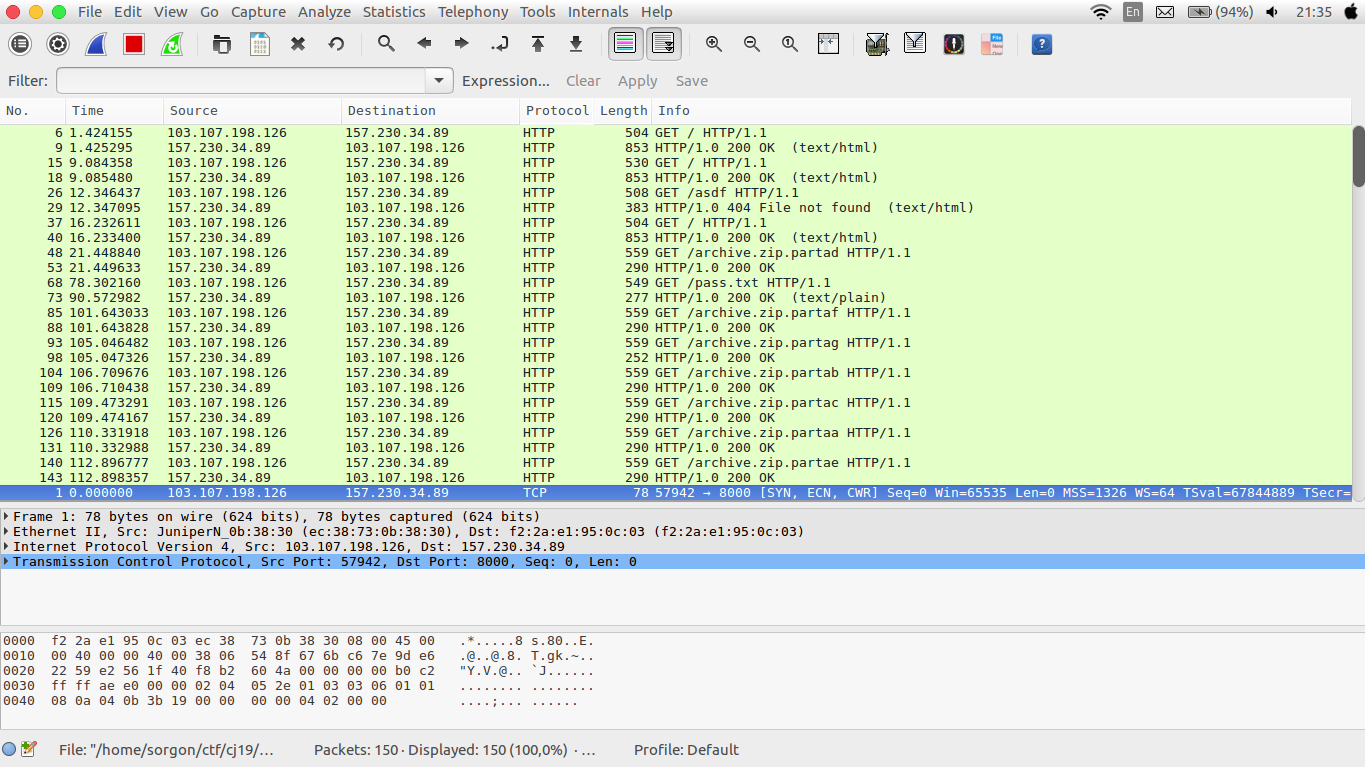


flag : **CJ2019{oh\_\*\*\*\*\_h3r3\_w3\_g0\_again!!!1!1}**

**2. Split { *Network* ; 100 point }**

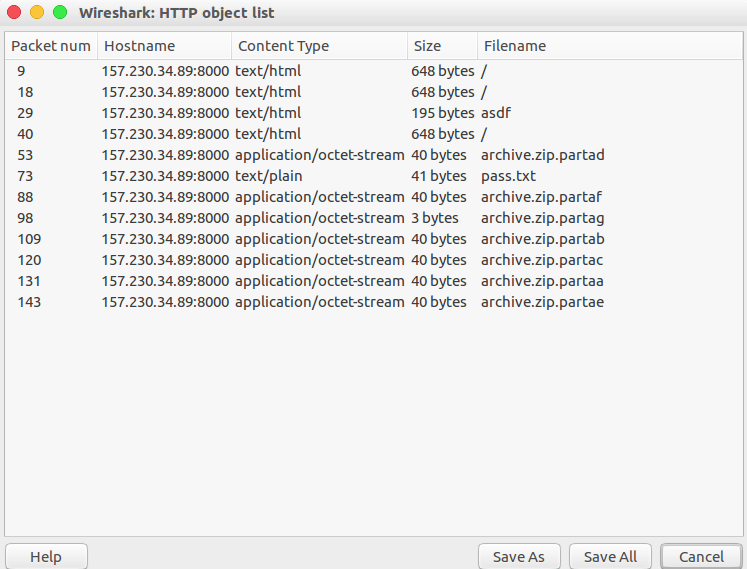
Diberikan file split.pcap yang dimana case nya mencari file yang terpisah kemudian disatukan kembali aku dan dia.

Oke , langsung kami buka dengan wireshark.

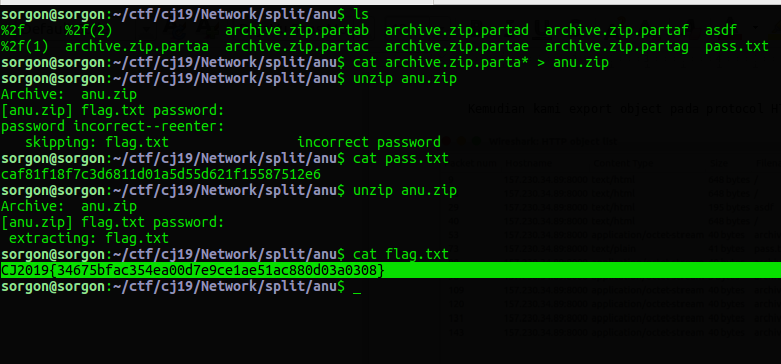


So, langsung kami sort by protocol , kemudian ada petunjuk di protocol HTTP yang berisi file zip yang terdiri dari 7 part dan satu key.

Kemudian kami export object pada protocol HTTP-nya



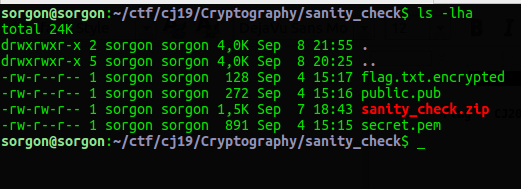
setelah kami ekstrak, muncul 7 file yang terpisah tadi, dan kegunaan pass.txt untuk membuka file zip yang akan disatukan.



**Flag : CJ2019{34675bfac354ea00d7e9ce1ae51ac880d03a0308}**

**3. Sanity Check { *Cryptography* ; 100 point }**

Diberikan 3 files yaitu file encrypted , public key dan private key.



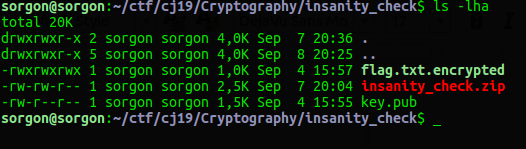
karena sudah diberikan private key nya , kami langsung buka dengan openssl



**flag : CJ2019{w3lc0m3\_to\_Cyber\_Jawara\_quals}**

**4. Insanity Check { *Cryptography* ; 100 point }**

Diberikan case yang mirip dengan challenge sanity check, hanya saja tidak diberikan private key nya.



Lalu kami ingat bahwa ada RsaCtftools yang berguna untuk membuka file encrypted tanpa private key.



Setelah kami eksekusi dengan command tersebut , tiba tiba tibaaa



Ada flag yang terpampang paling bawah.

**Flag : CJ2019{breaking\_insecure\_rsa\_is\_not\_so\_hard}**

P

P

P

P

P

P

Punten.