

Picture Puzzle

GejesGejes

Forensics

Write-up Penyelesaian

1. Diberikan sebuah file `blank.jpg` sebagai berikut

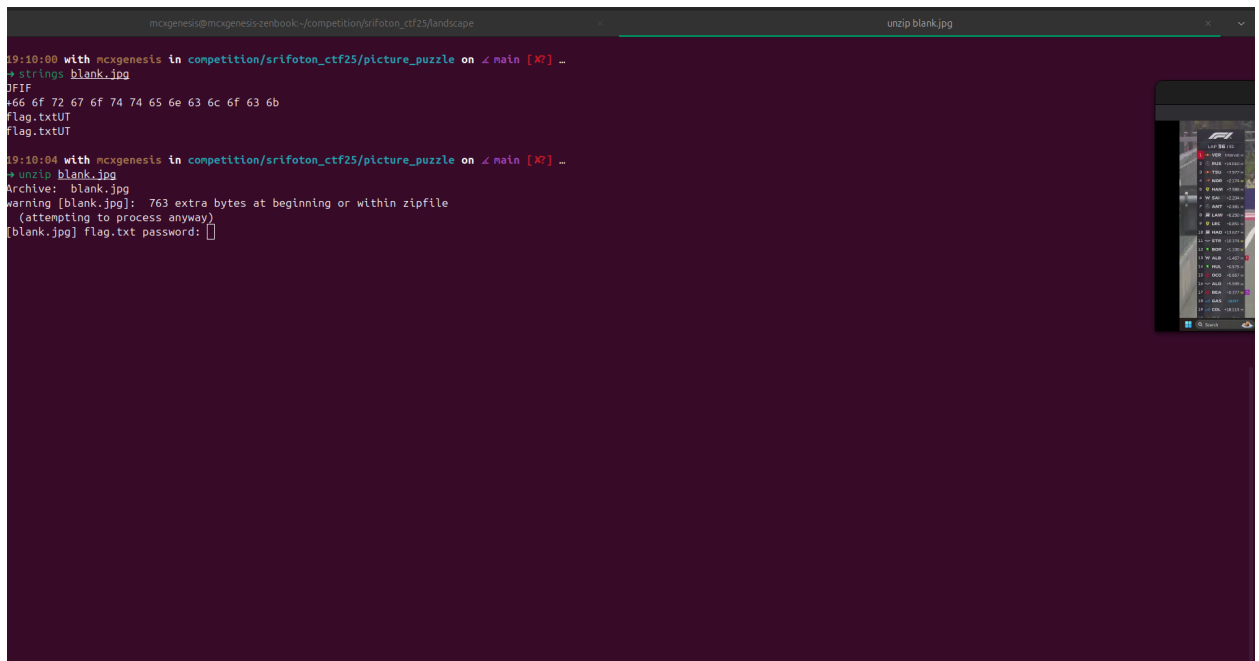


Iya, filenya memang blank.

2. Namun, isinya belum tentu blank. Saya akan mencoba command `strings blank.jpg`

```
mcxgenesis@mcxgenesis-zenbook:~/competition/srifoton_ctf25/landscape
19:10:00 with mcxgenesis in competition/srifoton_ctf25/picture_puzzle on 4 main [X?] ...
+ strings blank.jpg
JFIF
+66 6f 72 67 6f 74 74 65 6e 63 6c 6f 63 6b
Flag.txtUT
Flag.txtUT
19:10:04 with mcxgenesis in competition/srifoton_ctf25/picture_puzzle on 4 main [X?] ...
+
```

3. Tampaknya ada sebuah file di .txt di dalam file gambar tersebut. Saya akan mencoba **unzip blank.jpg**

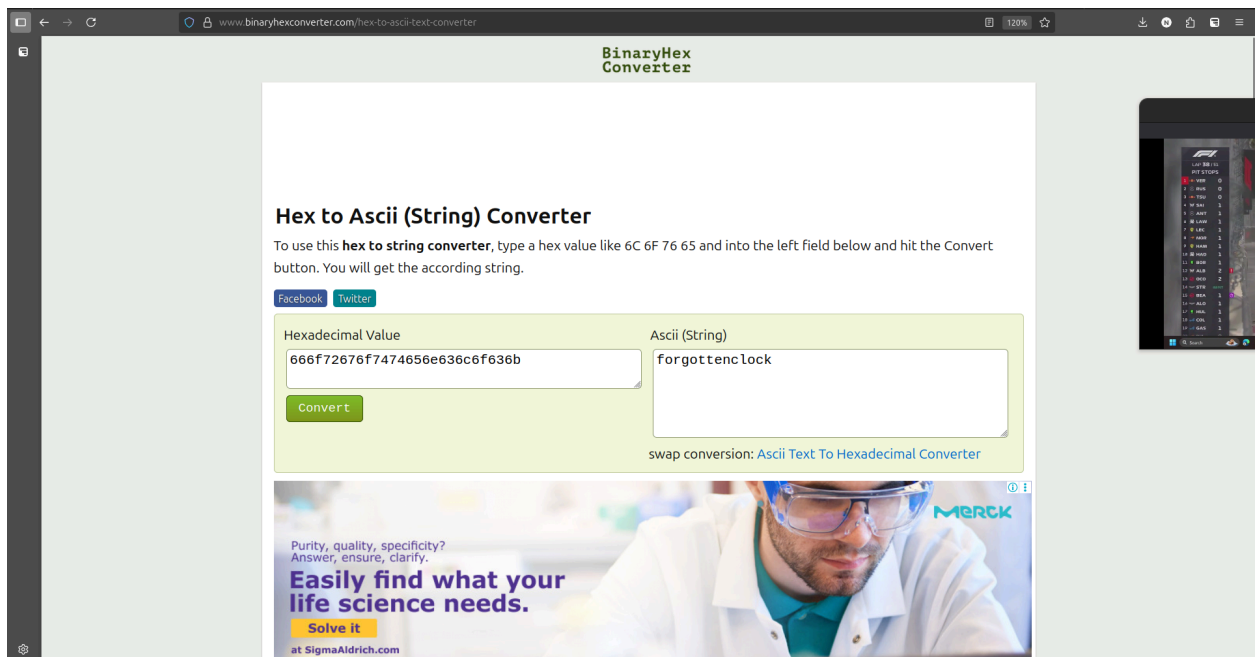


```
mcxgenesis@mcxgenesiszenbook:~/competition/srifoton_ctf25/landscape$ unzip blank.jpg
19:10:00 with mcxgenesis in competition/srifoton_ctf25/picture_puzzle on < main [K?] ...
+ strings blank.jpg
DEF
+66 6f 72 67 6f 74 74 65 6e 63 6c 6f 63 6b
Flag.txtUT
Flag.txtUT

19:10:04 with mcxgenesis in competition/srifoton_ctf25/picture_puzzle on < main [K?] ...
+ unzip blank.jpg
Archive: blank.jpg
Warning [blank.jpg]: 763 extra bytes at beginning or within zipfile
(attempting to process anyway)
blank.jpg Flag.txt password: 
```

Ternyata untuk extract harus menggunakan password.

4. Passwordnya bisa saja berada di dalam text sequence +66 6f 72 67 6f 74 74 65 6e 63 6c 6f 63 6b yang merupakan value hexadecimal dan hasilnya akan berupa text ASCII. Text ini bisa di decode menggunakan tools online.

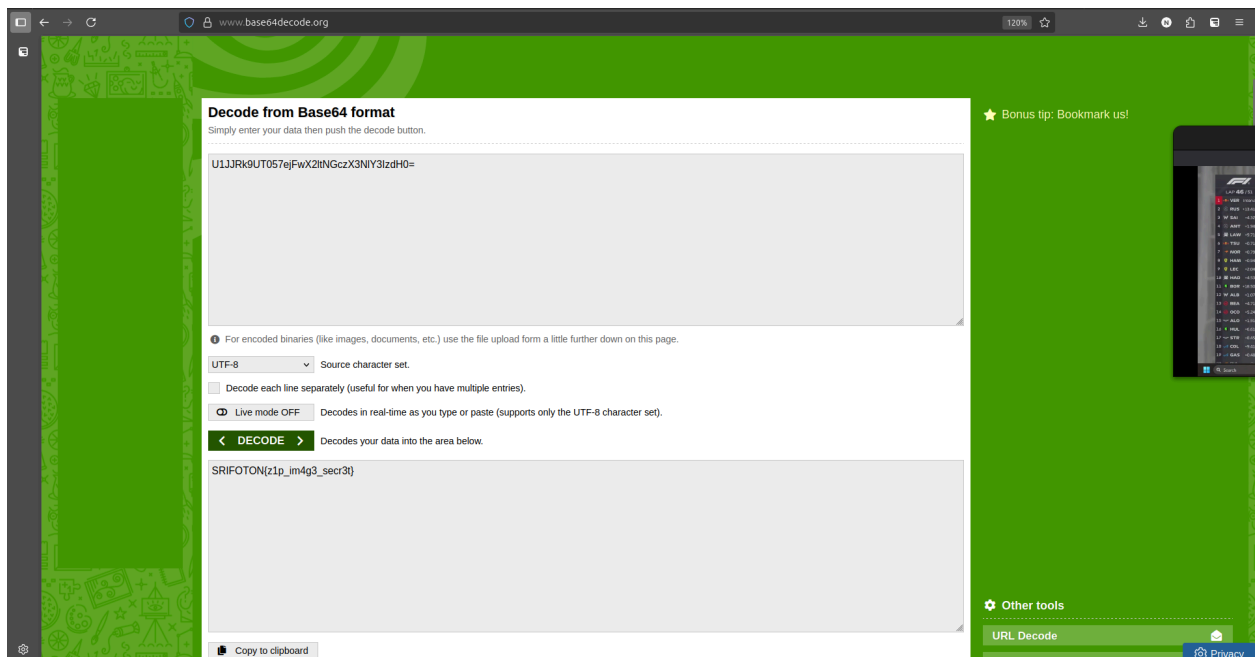


Didapatkan text: forgottenclock

5. Text 'fotgottenclock' akan digunakan sebagai password untuk mengextract file dari blank.jpg

```
mcxgenesis@mcxgenesis-zenbook:~/competition/srifoton_ctf25/landscape$  
19:10:00 with mcxgenesis in competition/srifoton_ctf25/picture_puzzle on 4 main [X?] ...  
+ strings blank.jpg  
DPiF  
+66 6f 72 67 6f 74 74 65 6e 63 6c 6f 63 6b  
flag.txtUT  
flag.txtUT  
  
19:10:04 with mcxgenesis in competition/srifoton_ctf25/picture_puzzle on 4 main [X?] ...  
+ unzip blank.jpg  
Archive: blank.jpg  
Warning [blank.jpg]: 763 extra bytes at beginning or within zipfile  
  (attempting to process anyway)  
[blank.jpg] flag.txt password:  
replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y  
extracting: flag.txt  
  
19:25:24 with mcxgenesis in competition/srifoton_ctf25/picture_puzzle on 4 main [X?] took 13m 23.7s ...  
+ cat flag.txt  
U1JJRk9UT057ejFwX2ltNGczX3NIY3IzdH0=  
  
19:25:38 with mcxgenesis in competition/srifoton_ctf25/picture_puzzle ...  
+  
[]
```

6. Di dalam **flag.txt** masih ada text 'U1JJRk9UT057ejFwX2ltNGczX3NIY3IzdH0=' yang tampaknya di encode dengan base64. Dengan menggunakan online tools, teks tersebut bisa di decode



Flag: SRIFOTON{z1p_im4g3_secr3t}