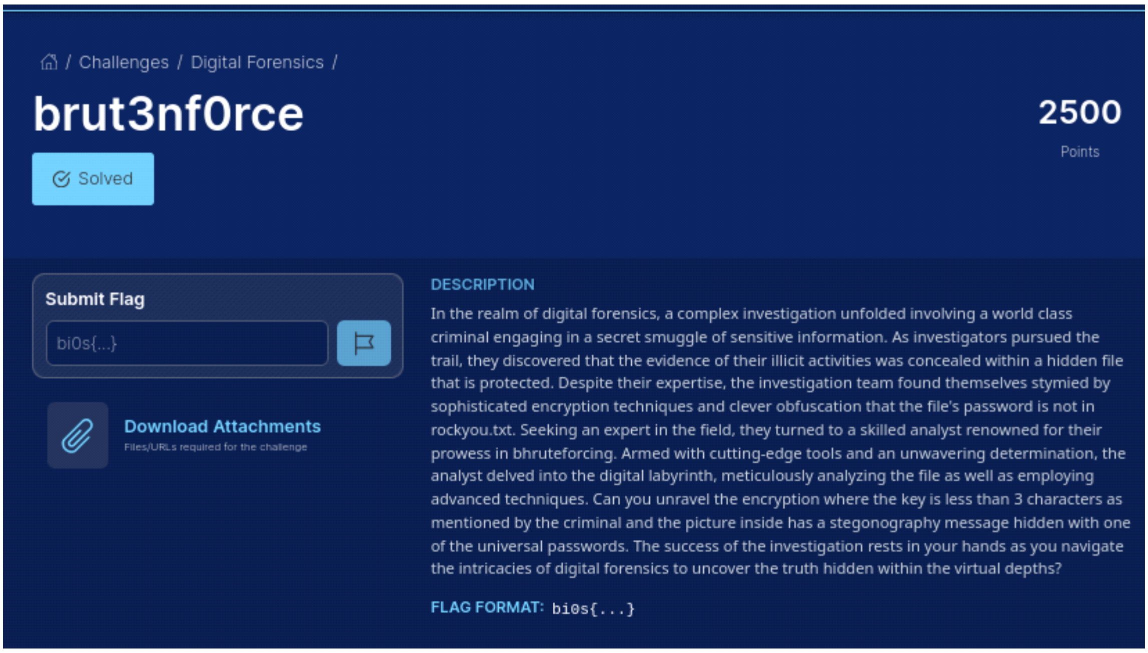
Brut3nf0rce

bi0s{bruting_satisfaction_for_real}

08 July 2023 12:33



⌂ / Challenges / Digital Forensics /

brut3nf0rce

2500 Points

✓ Solved

Submit Flag

bi0s{...}

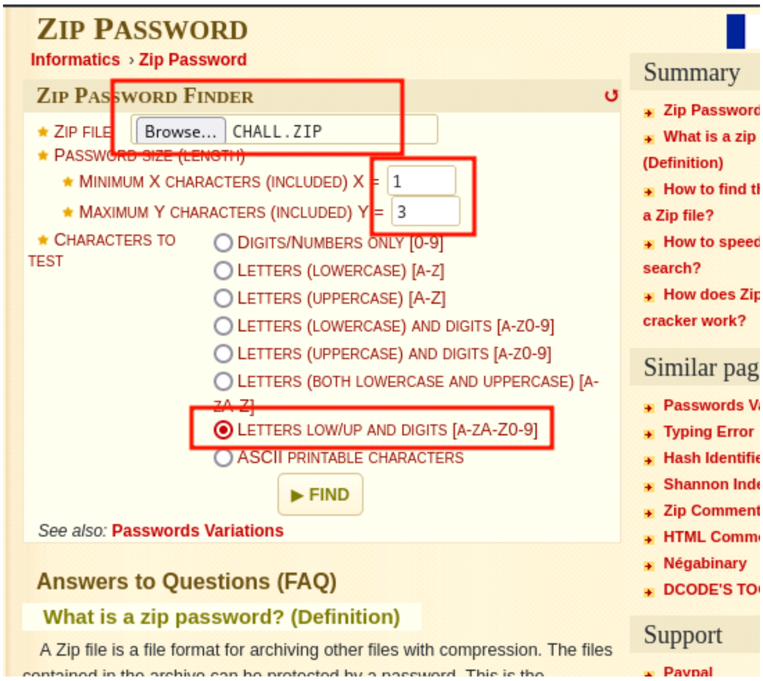
Download Attachments
Files/URLs required for the challenge

DESCRIPTION

In the realm of digital forensics, a complex investigation unfolded involving a world class criminal engaging in a secret smuggle of sensitive information. As investigators pursued the trail, they discovered that the evidence of their illicit activities was concealed within a hidden file that is protected. Despite their expertise, the investigation team found themselves stymied by sophisticated encryption techniques and clever obfuscation that the file's password is not in rockyou.txt. Seeking an expert in the field, they turned to a skilled analyst renowned for their prowess in bhruteforcing. Armed with cutting-edge tools and an unwavering determination, the analyst delved into the digital labyrinth, meticulously analyzing the file as well as employing advanced techniques. Can you unravel the encryption where the key is less than 3 characters as mentioned by the criminal and the picture inside has a stegonography message hidden with one of the universal passwords. The success of the investigation rests in your hands as you navigate the intricacies of digital forensics to uncover the truth hidden within the virtual depths?

FLAG FORMAT: `bi0s{...}`

https://www.dcode.fr/zip-password



ZIP PASSWORD

Informatics › Zip Password

ZIP PASSWORD FINDER

★ ZIP FILE Browse... CHALL.ZIP

★ PASSWORD SIZE (LENGTH)

★ MINIMUM X CHARACTERS (INCLUDED) X = 1

★ MAXIMUM Y CHARACTERS (INCLUDED) Y = 3

★ CHARACTERS TO TEST

○ DIGITS/NUMBERS ONLY [0-9]
○ LETTERS (LOWERCASE) [A-Z]
○ LETTERS (UPPERCASE) [A-Z]
○ LETTERS (LOWERCASE) AND DIGITS [A-Z0-9]
○ LETTERS (UPPERCASE) AND DIGITS [A-Z0-9]
○ LETTERS (BOTH LOWERCASE AND UPPERCASE) [A-ZA-Z]
● LETTERS LOW/UP AND DIGITS [A-ZA-Z0-9]
○ ASCII PRINTABLE CHARACTERS

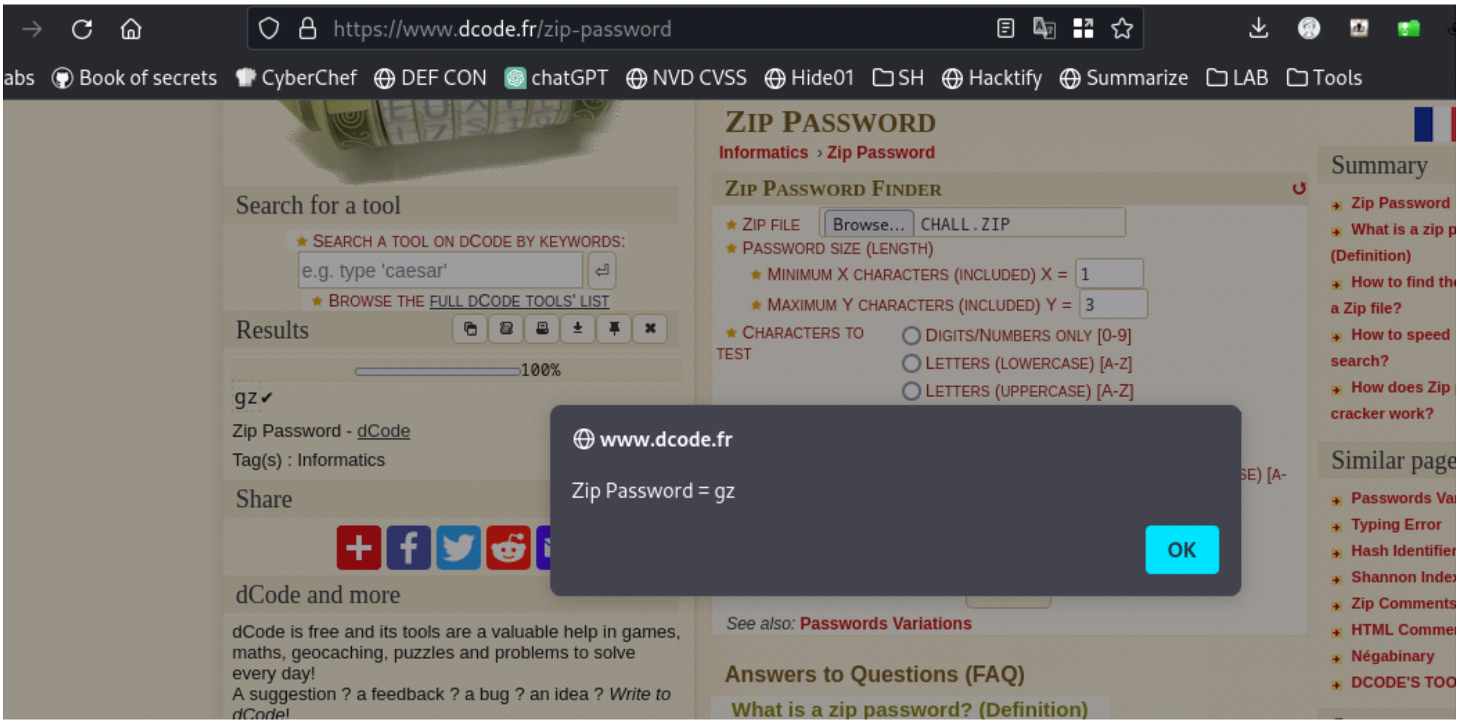
▶ FIND

See also: Passwords Variations

Answers to Questions (FAQ)

What is a zip password? (Definition)

A Zip file is a file format for archiving other files with compression. The files contained in the archive can be protected by a password. This is the



ZIP PASSWORD

Informatics › Zip Password

ZIP PASSWORD FINDER

★ ZIP FILE Browse... CHALL.ZIP

★ PASSWORD SIZE (LENGTH)

★ MINIMUM X CHARACTERS (INCLUDED) X = 1

★ MAXIMUM Y CHARACTERS (INCLUDED) Y = 3

★ CHARACTERS TO TEST
○ DIGITS/NUMBERS ONLY [0-9]
○ LETTERS (LOWERCASE) [A-Z]
○ LETTERS (UPPERCASE) [A-Z]

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'

★ BROWSE THE FULL DCODE TOOLS' LIST

100%

gz✓

Zip Password - dCode

Tag(s) : Informatics

www.dcode.fr

Zip Password = gz

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode!*

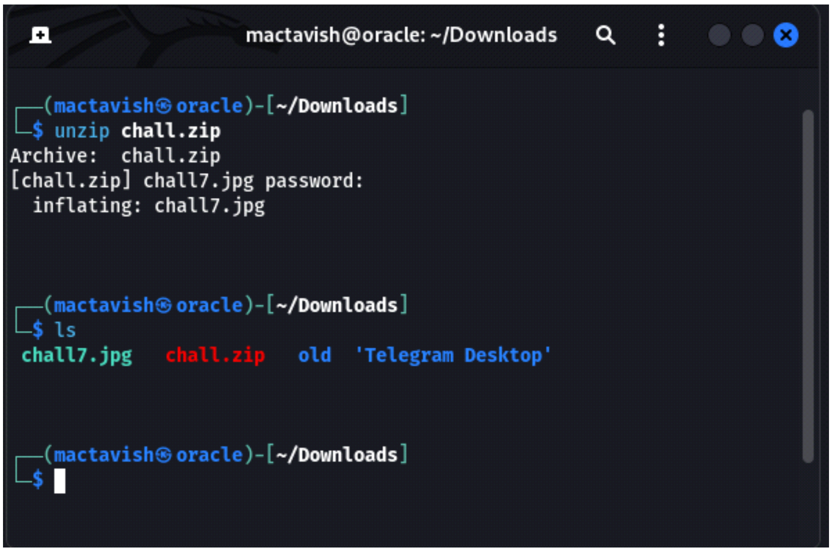
See also: Passwords Variations

Answers to Questions (FAQ)

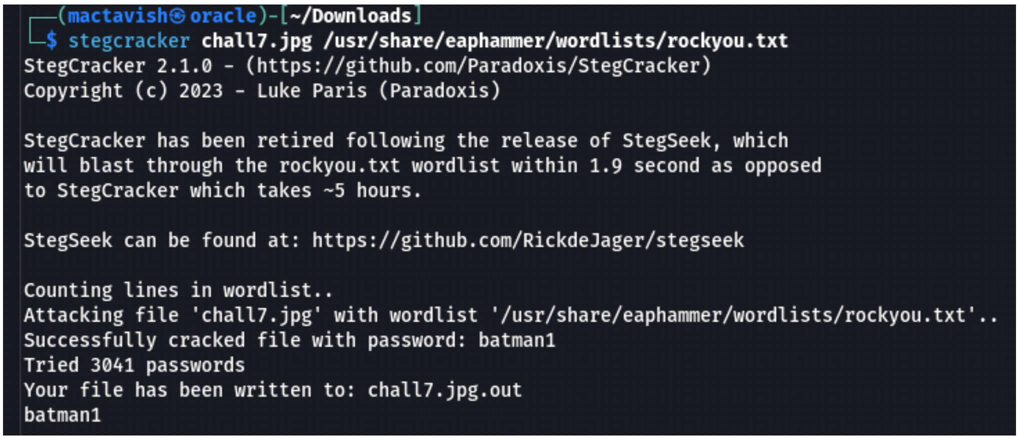
What is a zip password? (Definition)

- Zip Password
- What is a zip p (Definition)
- How to find th a Zip file?
- How to speed search?
- How does Zip cracker work?

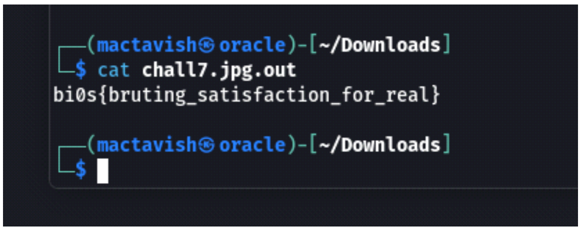
- Passwords Va
- Typing Error
- Hash Identifier
- Shannon Index
- Zip Comments
- HTML Comme
- Négabinary
- DCODE'S TOO



```
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ unzip chall.zip
Archive:  chall.zip
[chall.zip] chall7.jpg password:
  inflating: chall7.jpg


┌──(mactavish㉿oracle)-[~/Downloads]
└─$ ls
 chall7.jpg   chall.zip   old  'Telegram Desktop'


┌──(mactavish㉿oracle)-[~/Downloads]
└─$ 
```



```
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ stegcracker chall7.jpg /usr/share/eaphammer/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2023 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'chall7.jpg' with wordlist '/usr/share/eaphammer/wordlists/rockyou.txt'..
Successfully cracked file with password: batman1
Tried 3041 passwords
Your file has been written to: chall7.jpg.out
batman1
```

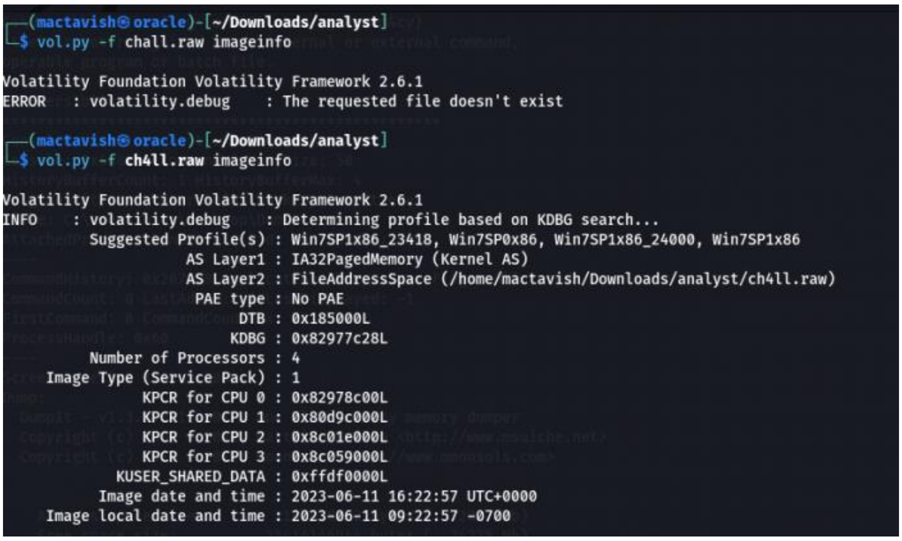


```
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ cat chall7.jpg.out
bi0s{bruting_satisfaction_for_real}

┌──(mactavish㉿oracle)-[~/Downloads]
└─$ 
```

7h3_Analyst

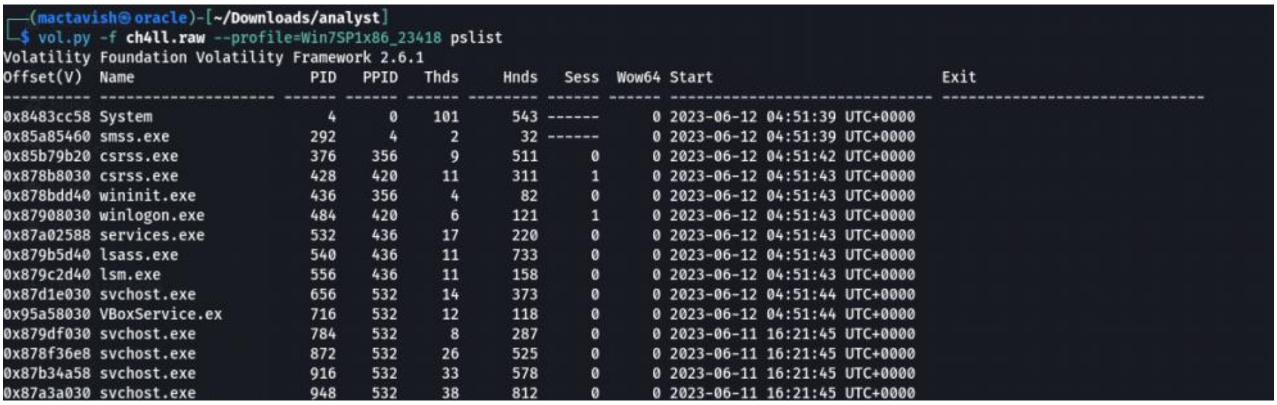
bi0s{7h1s_w45_ch4ll3ng1ng_tbh_76543}

08 July 2023 16:02



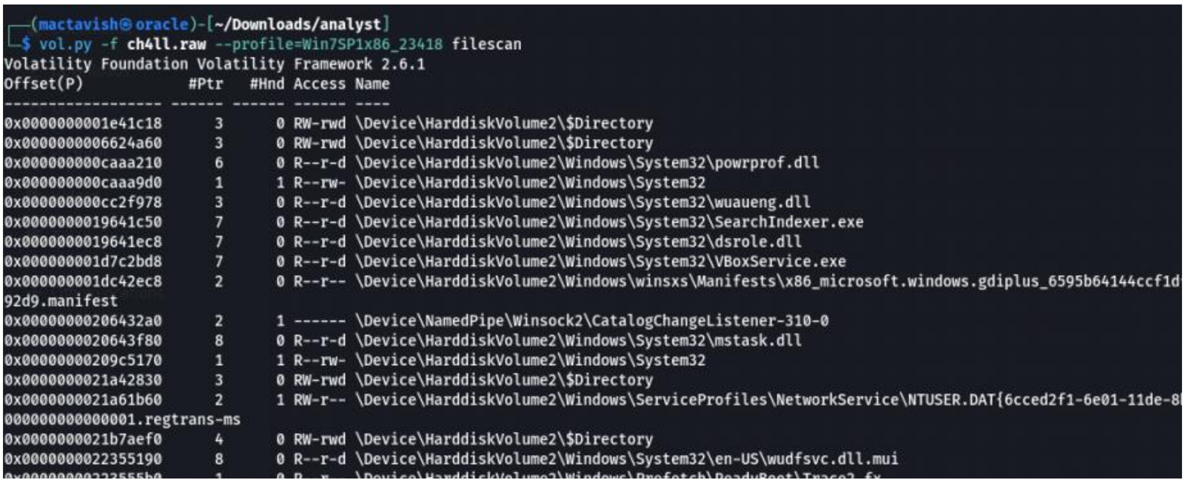
```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f chall.raw imageinfo

Volatility Foundation Volatility Framework 2.6.1
ERROR   : volatility.debug    : The requested file doesn't exist

┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw imageinfo

Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/mactavish/Downloads/analyst/ch4ll.raw)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x82977c28L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82978c00L
                KPCR for CPU 1 : 0x80d9c000L
                KPCR for CPU 2 : 0x8c01e000L
                KPCR for CPU 3 : 0x8c059000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2023-06-11 16:22:57 UTC+0000
     Image local date and time : 2023-06-11 09:22:57 -0700
```

Firstly we are going to check the present profiles



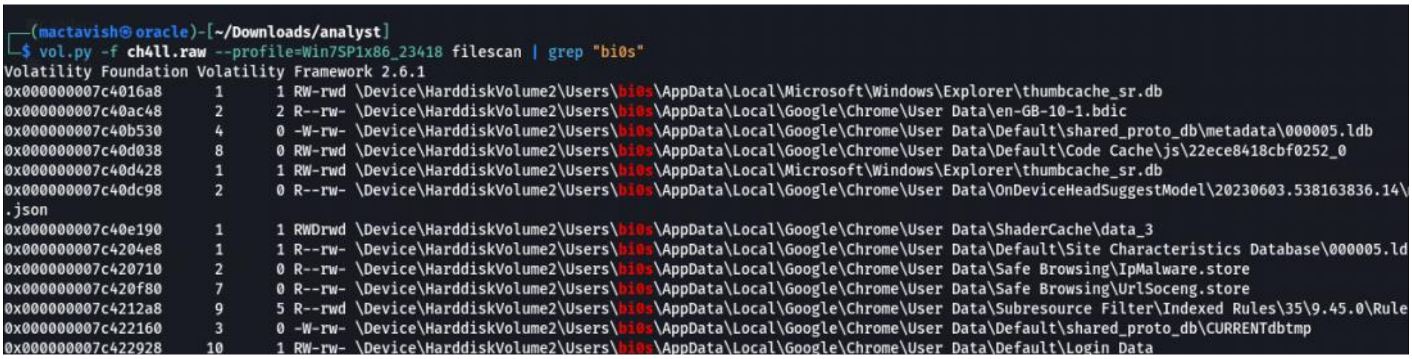
```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8483cc58 System                    4      0    101      543 ------      0 2023-06-12 04:51:39 UTC+0000
0x85a85460 smss.exe                292      4      2       32 ------      0 2023-06-12 04:51:39 UTC+0000
0x85b79b20 csrss.exe               376    356      9      511      0      0 2023-06-12 04:51:42 UTC+0000
0x878b8030 csrss.exe               428    420     11      311      1      0 2023-06-12 04:51:43 UTC+0000
0x878bdd40 wininit.exe             436    356      4       82      0      0 2023-06-12 04:51:43 UTC+0000
0x87908030 winlogon.exe            484    420      6      121      1      0 2023-06-12 04:51:43 UTC+0000
0x87a02588 services.exe            532    436     17      220      0      0 2023-06-12 04:51:43 UTC+0000
0x879b5d40 lsass.exe               540    436     11      733      0      0 2023-06-12 04:51:43 UTC+0000
0x879c2d40 lsm.exe                 556    436     11      158      0      0 2023-06-12 04:51:43 UTC+0000
0x87d1e030 svchost.exe             656    532     14      373      0      0 2023-06-12 04:51:44 UTC+0000
0x95a58030 VBoxService.ex          716    532     12      118      0      0 2023-06-12 04:51:44 UTC+0000
0x879df030 svchost.exe             784    532      8      287      0      0 2023-06-11 16:21:45 UTC+0000
0x878f36e8 svchost.exe             872    532     26      525      0      0 2023-06-11 16:21:45 UTC+0000
0x87b34a58 svchost.exe             916    532     33      578      0      0 2023-06-11 16:21:45 UTC+0000
0x87a3a030 svchost.exe             948    532     38      812      0      0 2023-06-11 16:21:45 UTC+0000
```

Then we are going to make a list of all the running programs in the image file

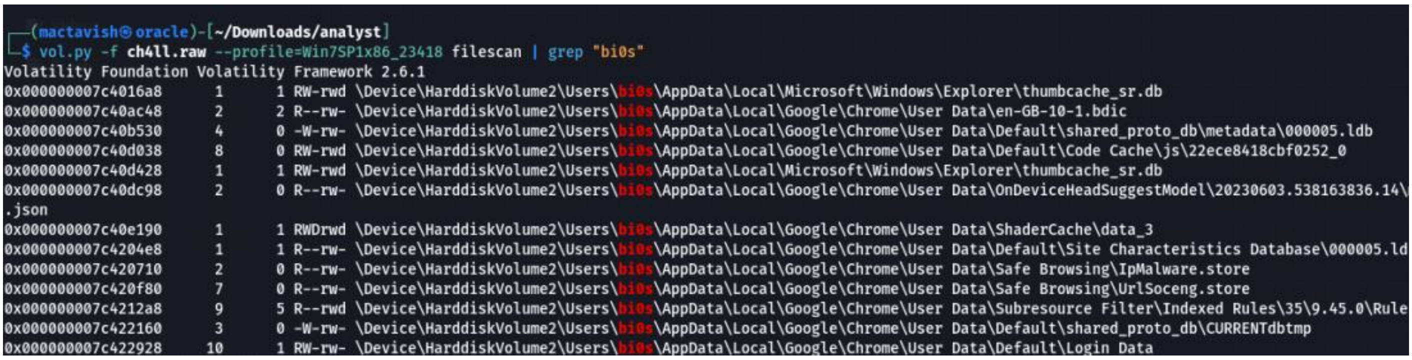


```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 filescan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)            #Ptr   #Hnd Access Name
------------------ ------ ------ ------ ----
0x000000001e41c18       3      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x0000000006624a60      3      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x000000000caaa210      6      0 R--r-d \Device\HarddiskVolume2\Windows\System32\powrprof.dll
0x000000000caaa9d0      1      1 R--rw- \Device\HarddiskVolume2\Windows\System32
0x000000000cc2f978      3      0 R--r-d \Device\HarddiskVolume2\Windows\System32\wuaueng.dll
0x0000000019641c50      7      0 R--r-d \Device\HarddiskVolume2\Windows\System32\SearchIndexer.exe
0x0000000019641ec8      7      0 R--r-d \Device\HarddiskVolume2\Windows\System32\dsrole.dll
0x000000001d7c2bd8      7      0 R--r-d \Device\HarddiskVolume2\Windows\System32\VBoxService.exe
0x000000001dc42ec8      2      0 R--r-- \Device\HarddiskVolume2\Windows\winsxs\Manifests\x86_microsoft.windows.gdiplus_6595b64144ccf1d
92d9.manifest
0x00000000206432a0      2      1 ------ \Device\NamedPipe\Winsock2\CatalogChangeListener-310-0
0x0000000020643f80      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\mstask.dll
0x00000000209c5170      1      1 R--rw- \Device\HarddiskVolume2\Windows\System32
0x0000000021a42830      3      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x0000000021a61b60      2      1 RW-r-- \Device\HarddiskVolume2\Windows\ServiceProfiles\NetworkService\NTUSER.DAT{6cced2f1-6e01-11de-8
000000000000001.regtrans-ms
0x0000000021b7aef0      4      0 RW-rwd \Device\HarddiskVolume2\$Directory
0x0000000022355190      8      0 R--r-d \Device\HarddiskVolume2\Windows\System32\en-US\wudfsvc.dll.mui
0x00000000223555b0      1      0 R--r-- \Device\HarddiskVolume2\Windows\Prefetch\ReadyBoot\Trace2.fx
```

Next we will run a filescan for checking the files

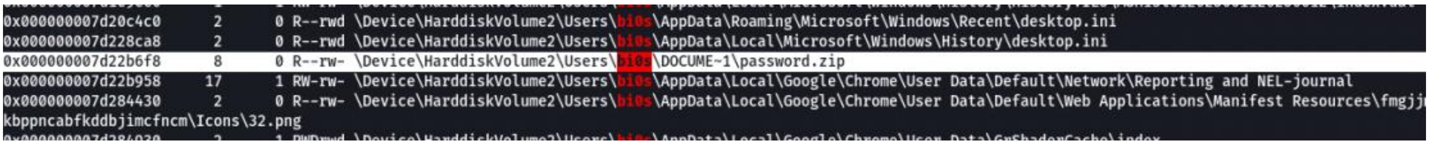


```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 filescan | grep "bi0s"
Volatility Foundation Volatility Framework 2.6.1
0x000000007c4016a8      1      1 RW-rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
0x000000007c40ac48      2      2 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\en-GB-10-1.bdic
0x000000007c40b530      4      0 -W-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\000005.ldb
0x000000007c40d038      8      0 RW-rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22ece8418cbf0252_0
0x000000007c40d428      1      1 RW-rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
0x000000007c40dc98      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\OnDeviceHeadSuggestModel\20230603.538163836.14\
.json
0x000000007c40e190      1      1 RWDrwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\ShaderCache\data_3
0x000000007c4204e8      1      1 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\000005.ld
0x000000007c420710      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Safe Browsing\IpMalware.store
0x000000007c420f80      7      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlSoceng.store
0x000000007c4212a8      9      5 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\35\9.45.0\Rule
0x000000007c422160      3      0 -W-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\CURRENTdbtmp
0x000000007c422928     10      1 RW-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\Login Data
```



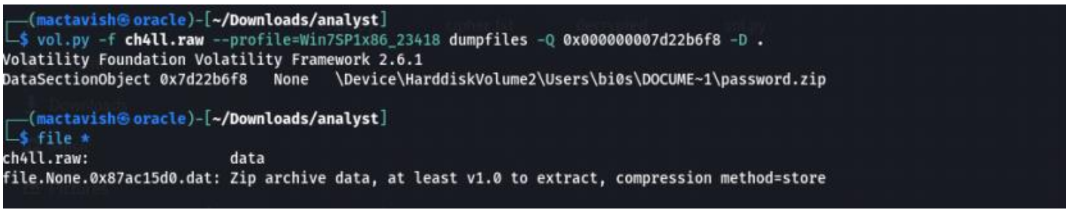
```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 filescan | grep "bi0s"
Volatility Foundation Volatility Framework 2.6.1
0x000000007c4016a8      1      1 RW-rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
0x000000007c40ac48      2      2 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\en-GB-10-1.bdic
0x000000007c40b530      4      0 -W-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\000005.ldb
0x000000007c40d038      8      0 RW-rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22ece8418cbf0252_0
0x000000007c40d428      1      1 RW-rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
0x000000007c40dc98      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\OnDeviceHeadSuggestModel\20230603.538163836.14\
.json
0x000000007c40e190      1      1 RWDrwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\ShaderCache\data_3
0x000000007c4204e8      1      1 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\000005.ld
0x000000007c420710      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Safe Browsing\IpMalware.store
0x000000007c420f80      7      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Safe Browsing\UrlSoceng.store
0x000000007c4212a8      9      5 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\35\9.45.0\Rule
0x000000007c422160      3      0 -W-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\CURRENTdbtmp
0x000000007c422928     10      1 RW-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\Login Data
```

We need to grep the files of bi0s



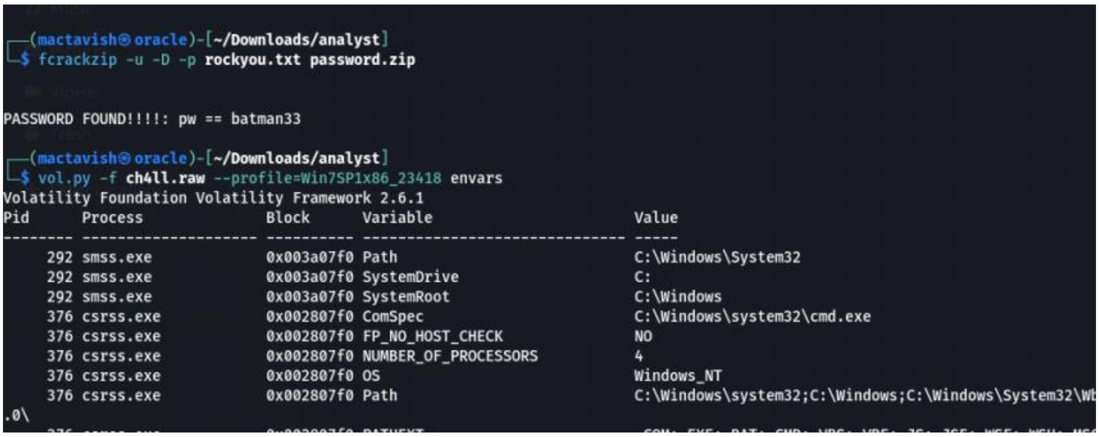
```
0x000000007d20c4c0      2      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini
0x000000007d228ca8      2      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\History\desktop.ini
0x000000007d22b6f8      8      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\DOCUME~1\password.zip
0x000000007d22b958     17      1 RW-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\Network\Reporting and NEL-journal
0x000000007d284430      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\Web Applications\Manifest Resources\fmgjj
kbppncabfkddbjimcfncm\Icons\32.png
```

We come across a zip file as hinted in description



```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000007d22b6f8 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7d22b6f8   None   \Device\HarddiskVolume2\Users\bi0s\DOCUME~1\password.zip

┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ file *
ch4ll.raw:                 data
file.None.0x87ac15d0.dat: Zip archive data, at least v1.0 to extract, compression method=store
```

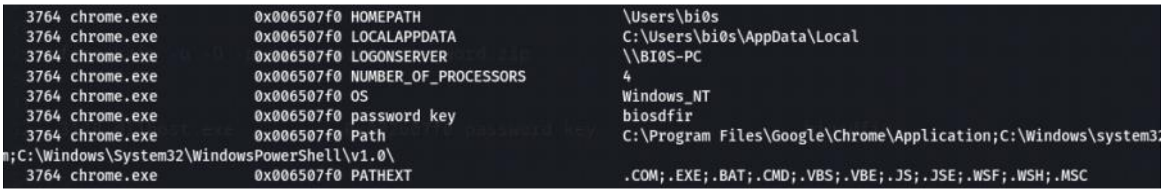
We can dump it using the dumpfiles function



```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ fcrackzip -u -D -p rockyou.txt password.zip


PASSWORD FOUND!!!!: pw == batman33

┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 envars
Volatility Foundation Volatility Framework 2.6.1
Pid      Process              Block      Variable                       Value
-------- -------------------- ---------- ------------------------------ -----
     292 smss.exe             0x003a07f0 Path                           C:\Windows\System32
     292 smss.exe             0x003a07f0 SystemDrive                    C:
     292 smss.exe             0x003a07f0 SystemRoot                     C:\Windows
     376 csrss.exe            0x002807f0 ComSpec                        C:\Windows\system32\cmd.exe
     376 csrss.exe            0x002807f0 FP_NO_HOST_CHECK               NO
     376 csrss.exe            0x002807f0 NUMBER_OF_PROCESSORS           4
     376 csrss.exe            0x002807f0 OS                             Windows_NT
     376 csrss.exe            0x002807f0 Path                           C:\Windows\system32;C:\Windows;C:\Windows\System32\Wb
.0\
```

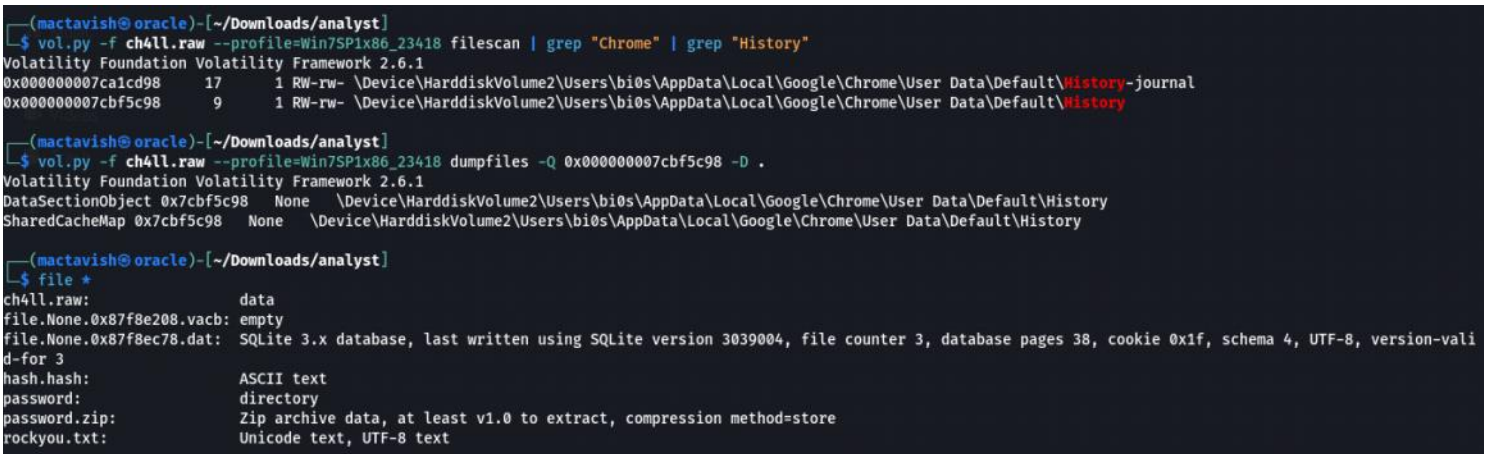
We crack the password and find it to be **Batman33**

The content inside is a text file containing a text
bhfshqsejovlgkqi



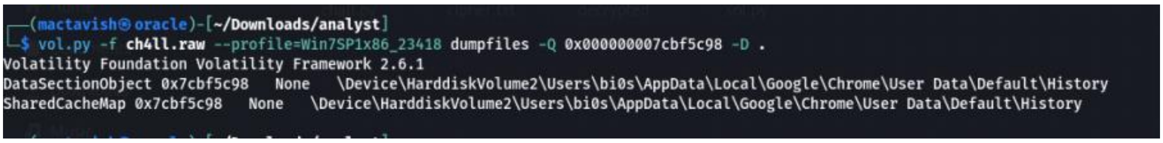
```
   3764 chrome.exe            0x006507f0 HOMEPATH                       \Users\bi0s
   3764 chrome.exe            0x006507f0 LOCALAPPDATA                   C:\Users\bi0s\AppData\Local
   3764 chrome.exe            0x006507f0 LOGONSERVER                    \\BI0S-PC
   3764 chrome.exe            0x006507f0 NUMBER_OF_PROCESSORS           4
   3764 chrome.exe            0x006507f0 OS                             Windows_NT
   3764 chrome.exe            0x006507f0 password key                   biosdfir
   3764 chrome.exe            0x006507f0 Path                           C:\Program Files\Google\Chrome\Application;C:\Windows\system32
n;C:\Windows\System32\WindowsPowerShell\v1.0\
   3764 chrome.exe            0x006507f0 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
```

Upon checking environment variables we come across a password key called
biosdfir



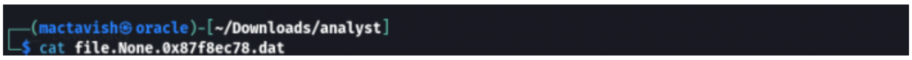
```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 filescan | grep "Chrome" | grep "History"
Volatility Foundation Volatility Framework 2.6.1
0x000000007ca1cd98     17      1 RW-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\History-journal
0x000000007cbf5c98      9      1 RW-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\History

┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000007cbf5c98 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7cbf5c98   None   \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\History
SharedCacheMap 0x7cbf5c98   None   \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\History

┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ file *
ch4ll.raw:                  data
file.None.0x87f8e208.vacb:  empty
file.None.0x87f8ec78.dat:   SQLite 3.x database, last written using SQLite version 3039004, file counter 3, database pages 38, cookie 0x1f, schema 4, UTF-8, version-vali
d-for 3
hash.hash:                  ASCII text
password:                   directory
password.zip:               Zip archive data, at least v1.0 to extract, compression method=store
rockyou.txt:                Unicode text, UTF-8 text
```

Let us now keep it aside and check the contents of the user's chrome history

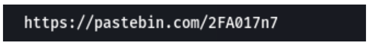


```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ vol.py -f ch4ll.raw --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000007cbf5c98 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7cbf5c98   None   \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\History
SharedCacheMap 0x7cbf5c98   None   \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Google\Chrome\User Data\Default\History
```

Here we find a suspicious file which leads us to a pastebin link

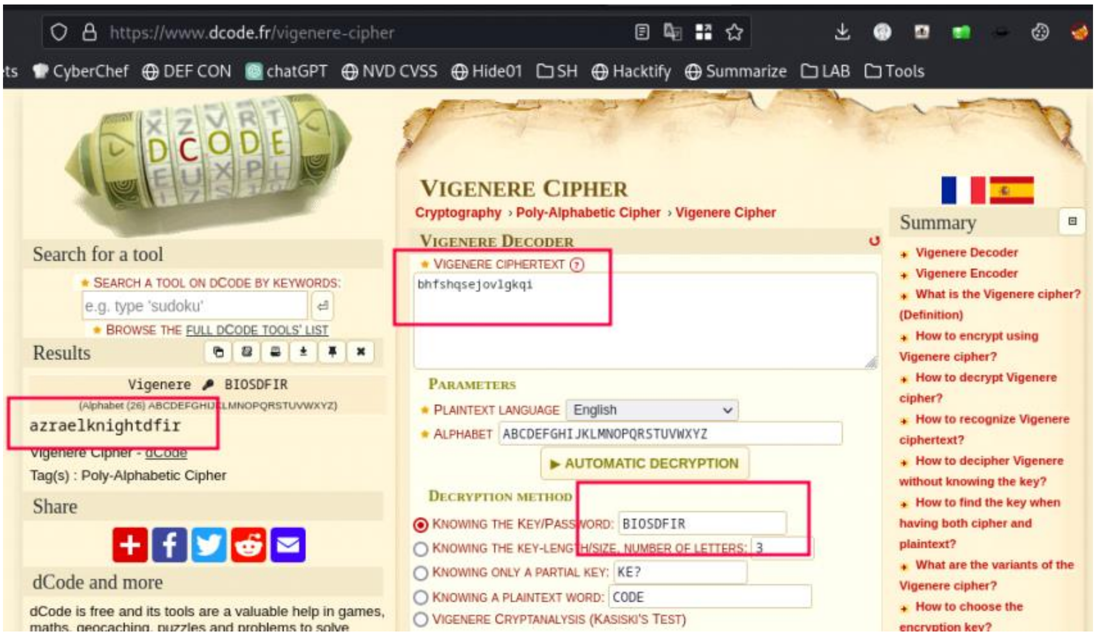


```
┌──(mactavish㉿oracle)-[~/Downloads/analyst]
└─$ cat file.None.0x87f8ec78.dat
```



```
https://pastebin.com/2FA017n7
```

https://pastebin.com/2FA017n7



https://www.dcode.fr/vigenere-cipher

ts
CyberChef
DEF CON
chatGPT
NVD CVSS
Hide01
SH
Hacktify
Summarize
LAB
Tools
Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'sudoku'
BROWSE THE FULL DCODE TOOLS' LIST
Results
Share
dCode and more
Summary
Vigenere Decoder
Vigenere Encoder
What is the Vigenere cipher? (Definition)
How to encrypt using Vigenere cipher?
How to decrypt Vigenere cipher?
How to recognize Vigenere ciphertext?
How to decipher Vigenere without knowing the key?
How to find the key when having both cipher and plaintext?
What are the variants of the Vigenere cipher?
How to choose the encryption key?

Vigenere 🔑 BIOSDFIR
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)
azraelknightdfir
Vigenere Cipher - dCode
Tag(s) : Poly-Alphabetic Cipher

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve

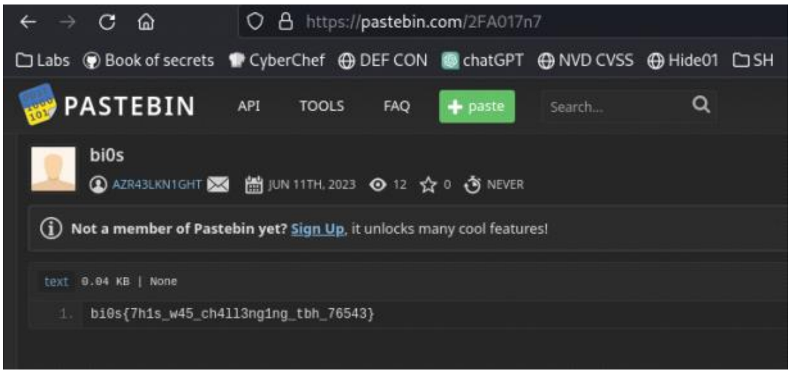
VIGENERE CIPHER
Cryptography › Poly-Alphabetic Cipher › Vigenere Cipher

VIGENERE DECODER
VIGENERE CIPHERTEXT: bhfshqsejovlgkqi

PARAMETERS
PLAINTEXT LANGUAGE: English
ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ
▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD
● KNOWING THE KEY/PASSWORD: BIOSDFIR
○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3
○ KNOWING ONLY A PARTIAL KEY: KE?
○ KNOWING A PLAINTEXT WORD: CODE
○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

We use the text in the zip and the key to decrypt what seems to be a vingenere cipher and find the password t be
azraelknightdfir



https://pastebin.com/2FA017n7

bi0s
AZR43LKN1GHT JUN 11TH, 2023 12 0 NEVER

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 0.04 KB | None

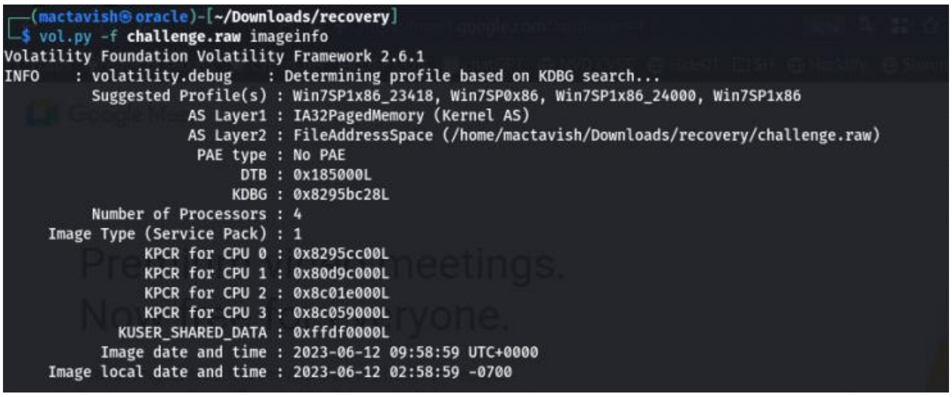
```
bi0s{7h1s_w45_ch4ll3ng1ng_tbh_76543}
```

Finally we open the pastebin link using the password and find our flag

R3c0v3rytxt

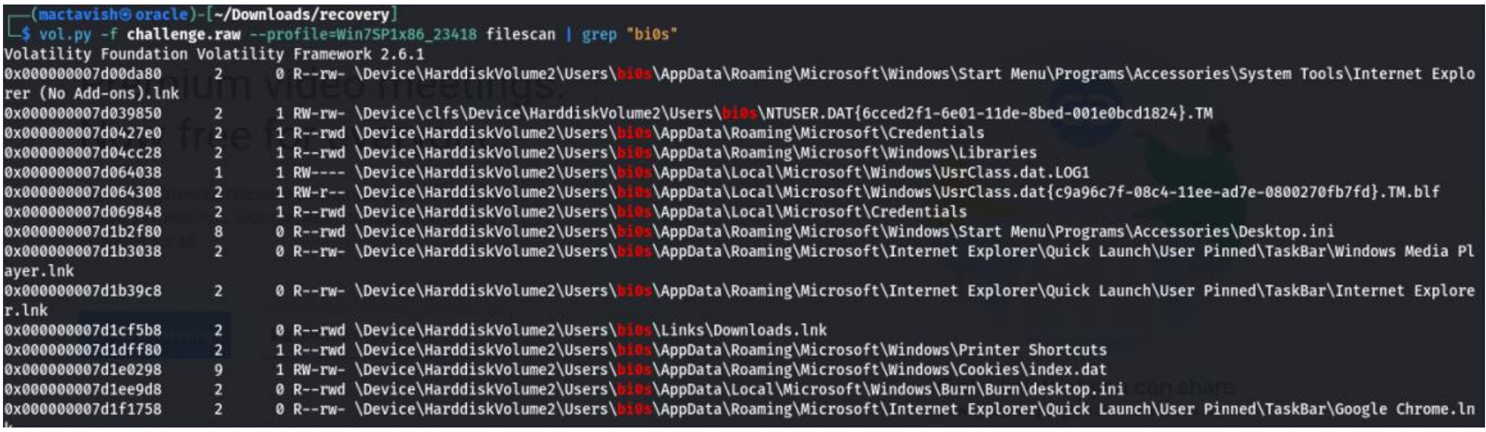
bi0s{fil3dump_mastery_rec0very}

08 July 2023 16:03



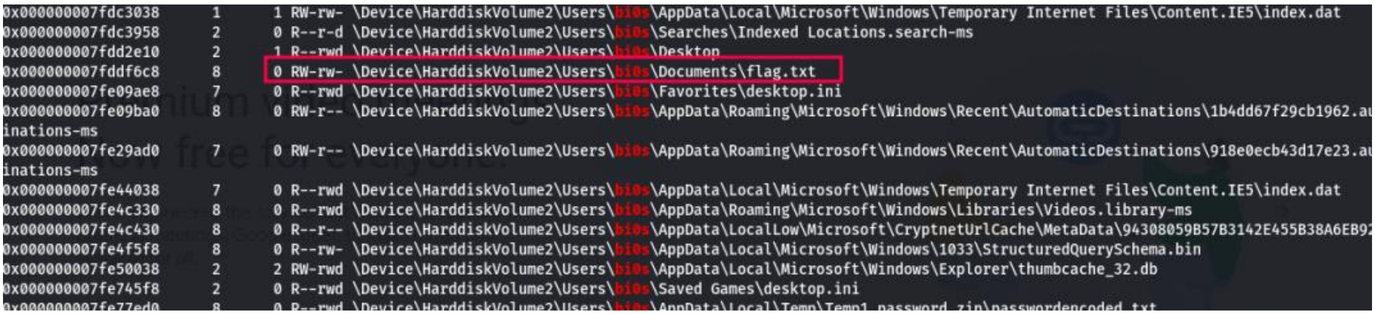
```
┌──(mactavish㉿oracle)-[~/Downloads/recovery]
└─$ vol.py -f challenge.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/mactavish/Downloads/recovery/challenge.raw)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x8295bc28L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x8295cc00L
                KPCR for CPU 1 : 0x80d9c000L
                KPCR for CPU 2 : 0x8c01e000L
                KPCR for CPU 3 : 0x8c059000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2023-06-12 09:58:59 UTC+0000
     Image local date and time : 2023-06-12 02:58:59 -0700
```

Firstly we are going to check the present profiles



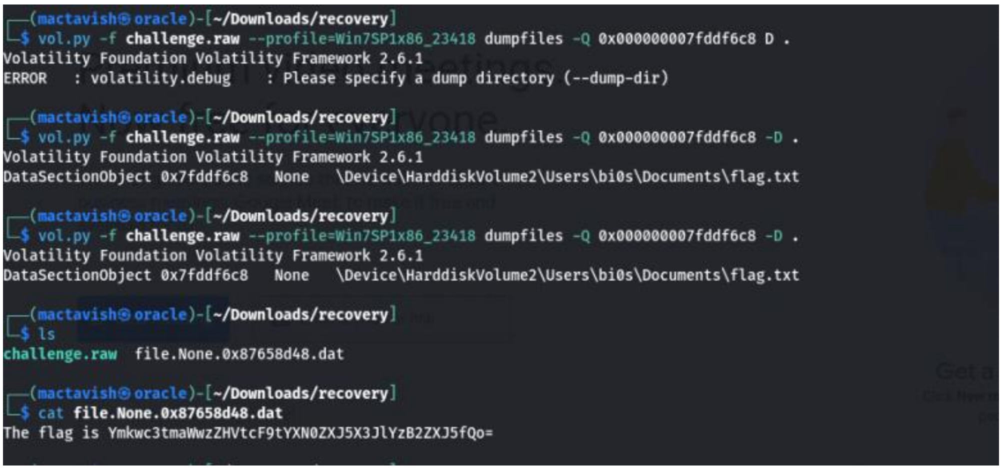
```
┌──(mactavish㉿oracle)-[~/Downloads/recovery]
└─$ vol.py -f challenge.raw --profile=Win7SP1x86_23418 filescan | grep "bi0s"
Volatility Foundation Volatility Framework 2.6.1
0x000000007d00da80      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Internet Explo
rer (No Add-ons).lnk
0x000000007d039850      2      1 RW-rw- \Device\clfs\Device\HarddiskVolume2\Users\bi0s\NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM
0x000000007d0427e0      2      1 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Credentials
0x000000007d04cc28      2      1 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Libraries
0x000000007d064038      1      1 RW---- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
0x000000007d064308      2      1 RW-r-- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\UsrClass.dat{c9a96c7f-08c4-11ee-ad7e-0800270fb7fd}.TM.blf
0x000000007d069848      2      1 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Credentials
0x000000007d1b2f80      8      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
0x000000007d1b3038      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows Media Pl
ayer.lnk
0x000000007d1b39c8      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Internet Explore
r.lnk
0x000000007d1cf5b8      2      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\Links\Downloads.lnk
0x000000007d1dff80      2      1 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
0x000000007d1e0298      9      1 RW-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
0x000000007d1ee9d8      2      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini
0x000000007d1f1758      2      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Google Chrome.ln
```

We need to grep the files of bi0s



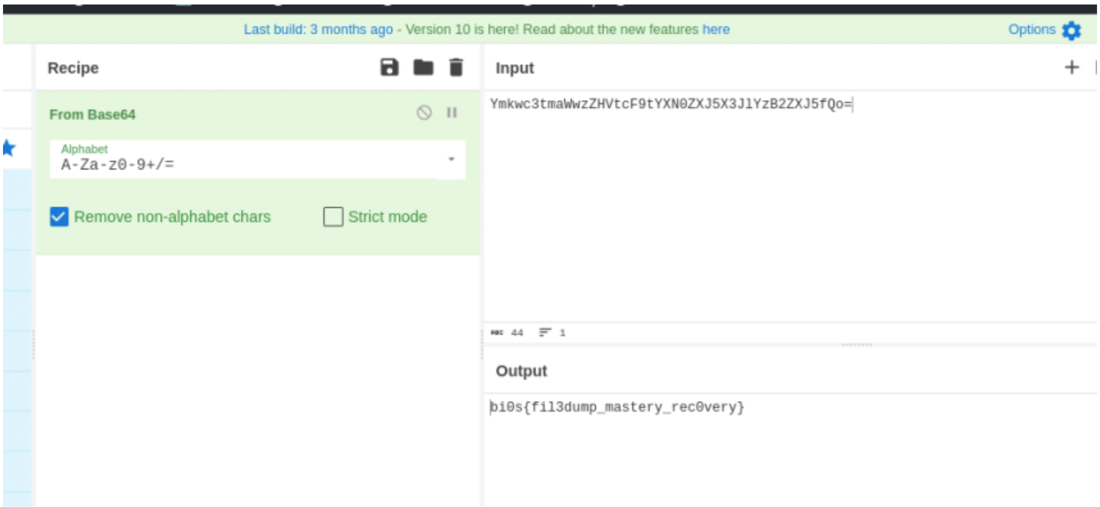
```
0x000000007fdc3038      1      1 RW-rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
0x000000007fdc3958      2      0 R--r-d \Device\HarddiskVolume2\Users\bi0s\Searches\Indexed Locations.search-ms
0x000000007fdd2e10      2      1 R--rwd \Device\HarddiskVolume2\Users\bi0s\Desktop
0x000000007fddf6c8      8      0 RW-rw- \Device\HarddiskVolume2\Users\bi0s\Documents\flag.txt
0x000000007fe09ae8      7      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\Favorites\desktop.ini
0x000000007fe09ba0      8      0 RW-r-- \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.au
inations-ms
0x000000007fe29ad0      7      0 RW-r-- \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\918e0ecb43d17e23.au
inations-ms
0x000000007fe44038      7      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
0x000000007fe4c330      8      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms
0x000000007fe4c430      8      0 R--r-- \Device\HarddiskVolume2\Users\bi0s\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB9
0x000000007fe4f5f8      8      0 R--rw- \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\1033\StructuredQuerySchema.bin
0x000000007fe50038      2      2 RW-rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
0x000000007fe745f8      2      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\Saved Games\desktop.ini
0x000000007fe77ed0      8      0 R--rwd \Device\HarddiskVolume2\Users\bi0s\AppData\Local\Temp\Temp1_password.zip\passwordencoded.txt
```

Here we find a flag.txt file



```
┌──(mactavish㉿oracle)-[~/Downloads/recovery]
└─$ vol.py -f challenge.raw --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000007fddf6c8 D .
Volatility Foundation Volatility Framework 2.6.1
ERROR   : volatility.debug    : Please specify a dump directory (--dump-dir)

┌──(mactavish㉿oracle)-[~/Downloads/recovery]
└─$ vol.py -f challenge.raw --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000007fddf6c8 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7fddf6c8   None   \Device\HarddiskVolume2\Users\bi0s\Documents\flag.txt

┌──(mactavish㉿oracle)-[~/Downloads/recovery]
└─$ vol.py -f challenge.raw --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000007fddf6c8 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7fddf6c8   None   \Device\HarddiskVolume2\Users\bi0s\Documents\flag.txt

┌──(mactavish㉿oracle)-[~/Downloads/recovery]
└─$ ls
challenge.raw  file.None.0x87658d48.dat

┌──(mactavish㉿oracle)-[~/Downloads/recovery]
└─$ cat file.None.0x87658d48.dat
The flag is Ymkwc3tmaWwzZHVtcF9tYXN0ZXJ5X3JlYzB2ZXJ5fQo=
```

We dump it and check the contents to find
Ymkwc3tmaWwzZHVtcF9tYXN0ZXJ5X3JlYzB2ZXJ5fQo=
Which clearly looks like a base64 encoded cipher



Last build: 3 months ago - Version 10 is here! Read about the new features here
Options
Recipe
Input
Output

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars
□ Strict mode

```
Ymkwc3tmaWwzZHVtcF9tYXN0ZXJ5X3JlYzB2ZXJ5fQo=
```

44 1

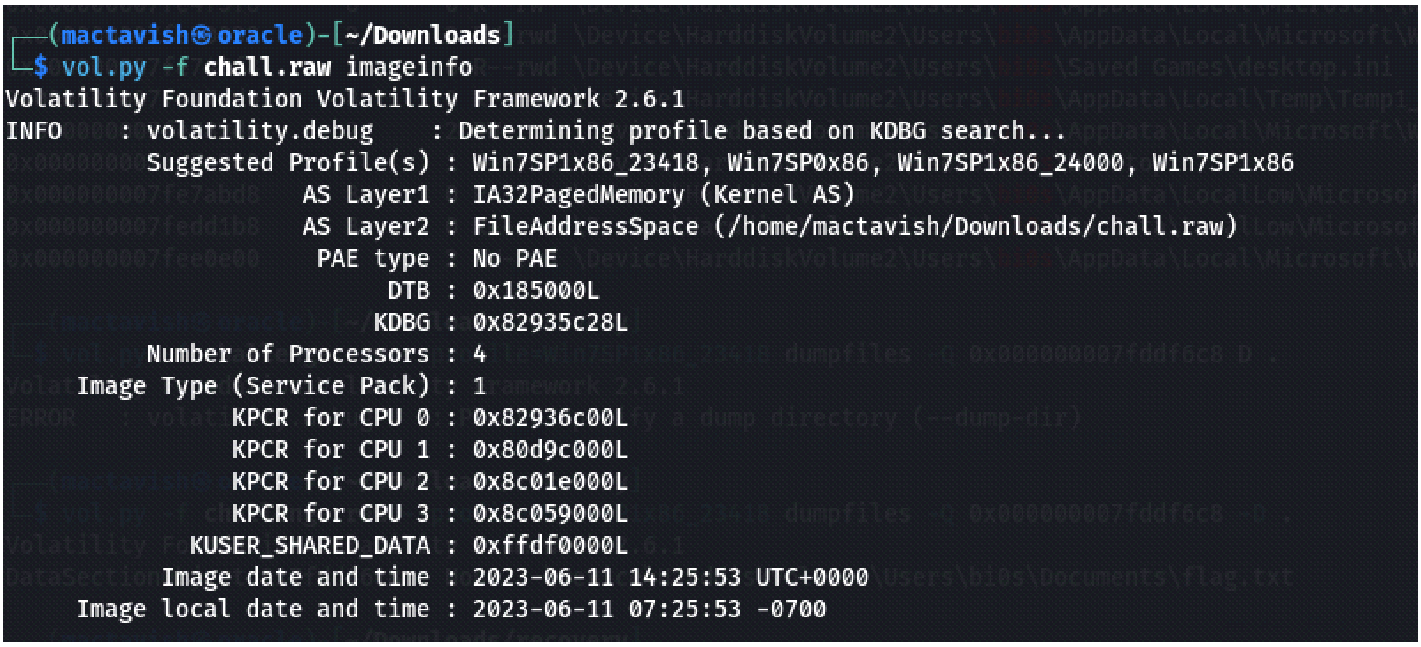
```
bi0s{fil3dump_mastery_rec0very}
```

We decode it to find the value of the flag

bl4ckscr33n_ex3cuti0n

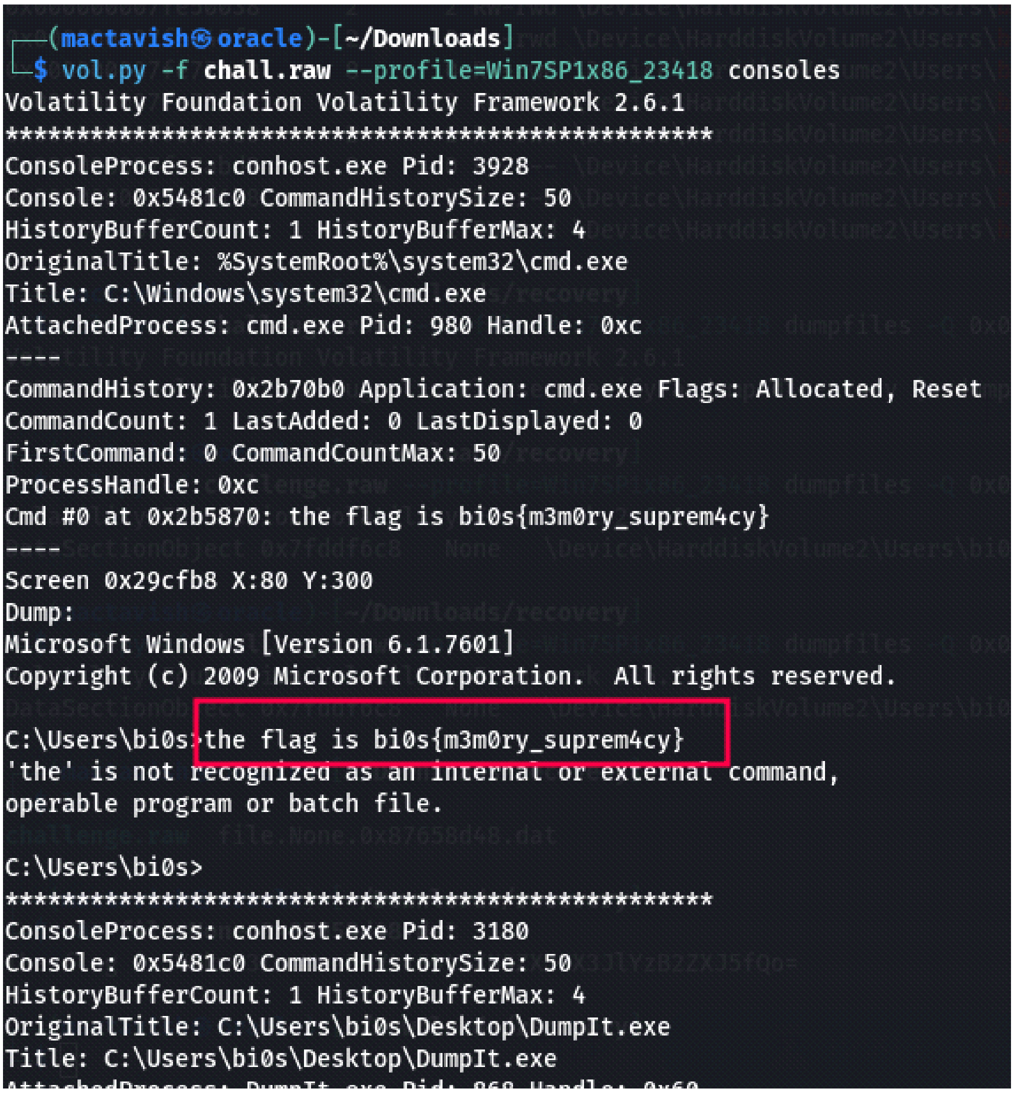
bi0s{m3m0ry_suprem4cy}

08 July 2023 16:11



```
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ vol.py -f chall.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/mactavish/Downloads/chall.raw)
                      PAE type : No PAE
                           DTB : 0x185000L
                          KDBG : 0x82935c28L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82936c00L
                KPCR for CPU 1 : 0x80d9c000L
                KPCR for CPU 2 : 0x8c01e000L
                KPCR for CPU 3 : 0x8c059000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2023-06-11 14:25:53 UTC+0000
     Image local date and time : 2023-06-11 07:25:53 -0700
```

Firstly we are going to check the present profiles



```
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ vol.py -f chall.raw --profile=Win7SP1x86_23418 consoles
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 3928
Console: 0x5481c0 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 980 Handle: 0xc
----
CommandHistory: 0x2b70b0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0xc
Cmd #0 at 0x2b5870: the flag is bi0s{m3m0ry_suprem4cy}
----
Screen 0x29cfb8 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\bi0s>the flag is bi0s{m3m0ry_suprem4cy}
'the' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\bi0s>
**************************************************
ConsoleProcess: conhost.exe Pid: 3180
Console: 0x5481c0 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\bi0s\Desktop\DumpIt.exe
Title: C:\Users\bi0s\Desktop\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 868 Handle: 0x60
```

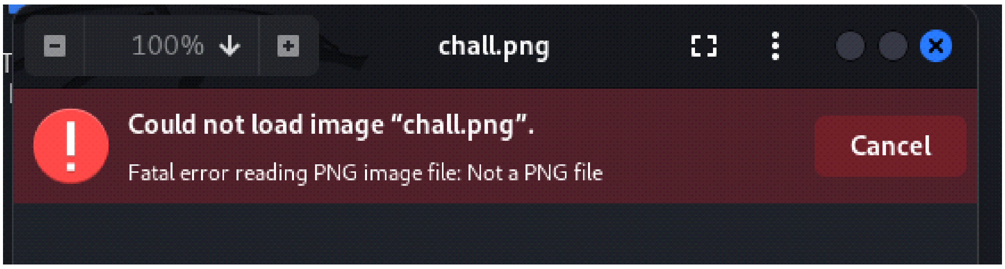
Since the challenge description says it has crashed we can look for the consoles and here we get the flag

consoles plugin finds commands that attackers typed into cmd.exe or executed via backdoors. However, instead of scanning for COMMAND_HISTORY, this plugin scans for CONSOLE_INFORMATION. The major advantage to this plugin is it not only prints the commands attackers typed, but it collects the entire screen buffer (input and output). For instance, instead of just seeing "dir", you'll see exactly what the attacker saw, including all files and directories listed by the "dir" command

Upgr4d3d_f1xm3

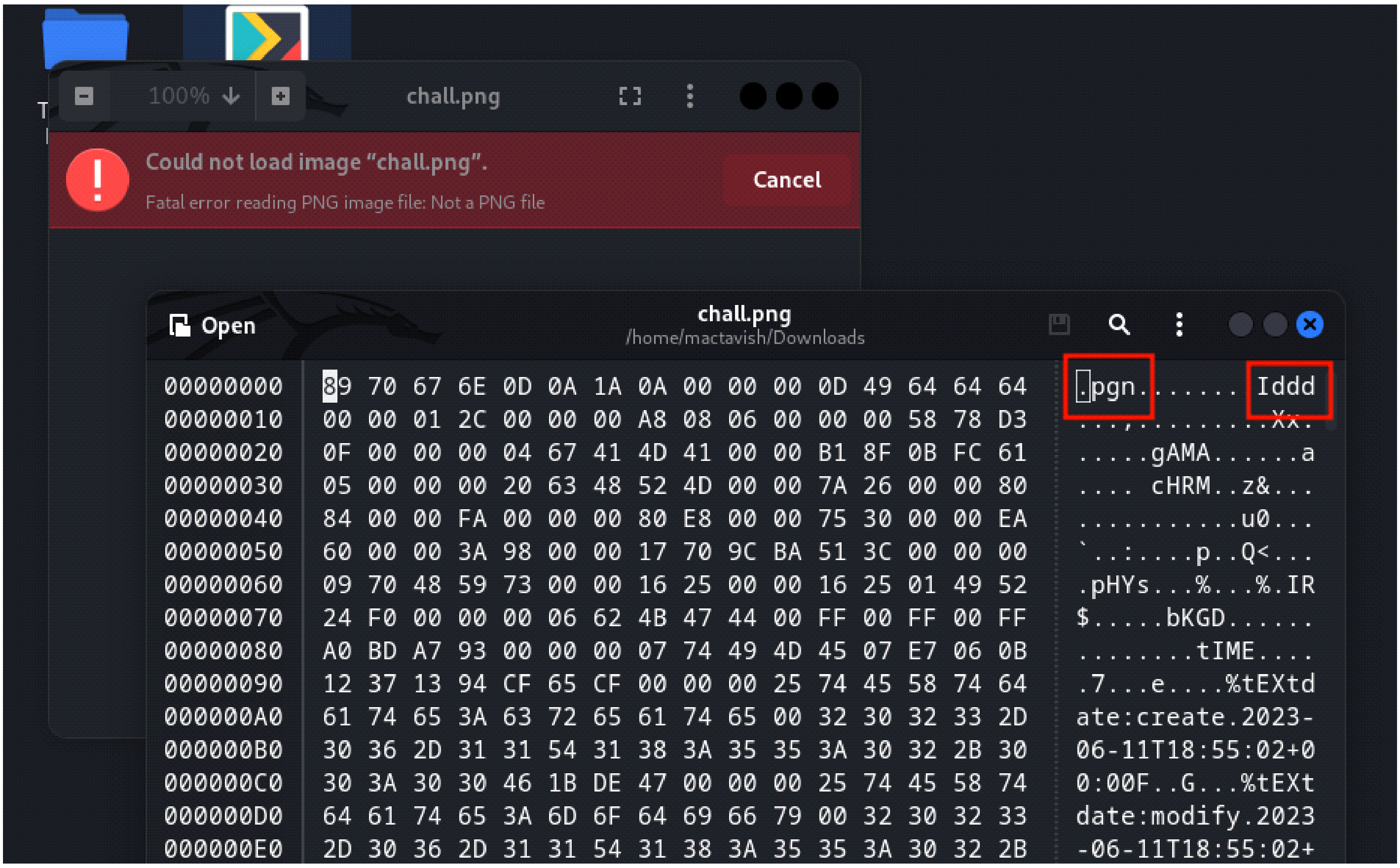
bi0s{m3m0ry_suprem4cy}

08 July 2023 16:13



Could not load image “chall.png”.

Fatal error reading PNG image file: Not a PNG file

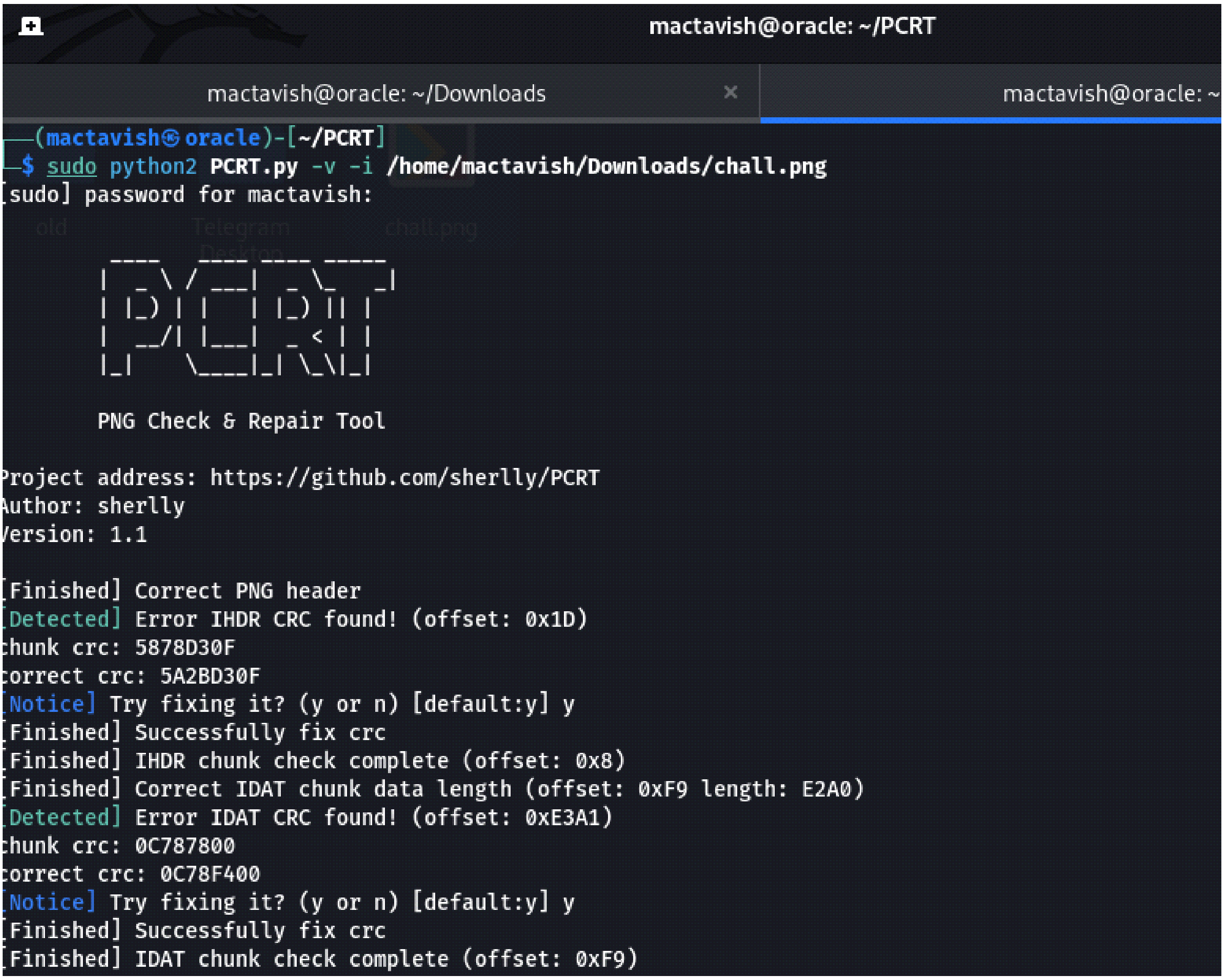


Could not load image “chall.png”.

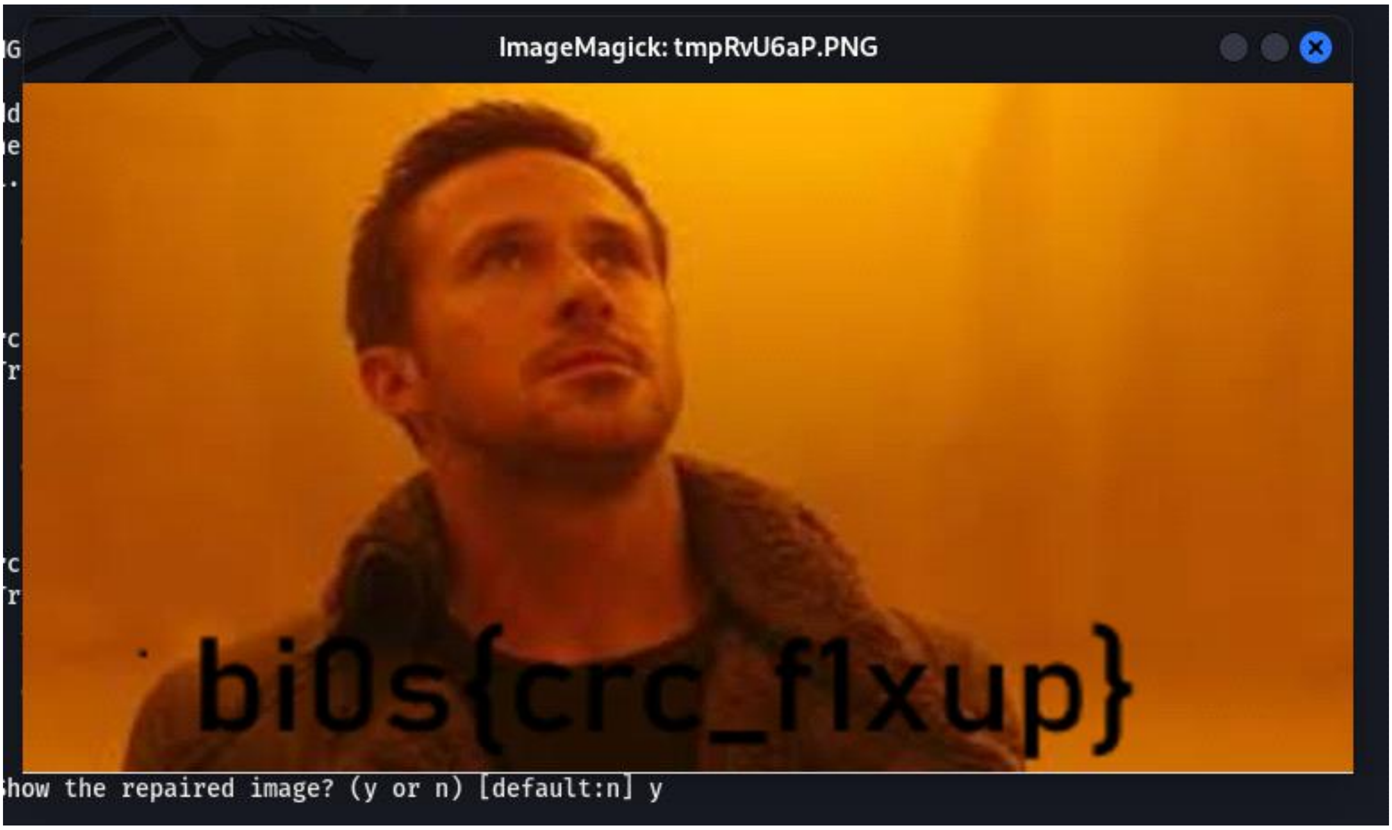
Fatal error reading PNG image file: Not a PNG file

```
00000000  89 70 67 6E 0D 0A 1A 0A 00 00 00 0D 49 64 64 64  .pgn.......Iddd
00000010  00 00 01 2C 00 00 00 A8 08 06 00 00 00 58 78 D3  ...,.........Xx.
00000020  0F 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61  .....gAMA......a
00000030  05 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80  .... cHRM..z&...
00000040  84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA  ...........u0...
00000050  60 00 00 3A 98 00 00 17 70 9C BA 51 3C 00 00 00  `..:....p..Q<...
00000060  09 70 48 59 73 00 00 16 25 00 00 16 25 01 49 52  .pHYs...%...%.IR
00000070  24 F0 00 00 00 06 62 4B 47 44 00 FF 00 FF 00 FF  $.....bKGD......
00000080  A0 BD A7 93 00 00 00 07 74 49 4D 45 07 E7 06 0B  ........tIME....
00000090  12 37 13 94 CF 65 CF 00 00 00 25 74 45 58 74 64  .7...e....%tEXtd
000000A0  61 74 65 3A 63 72 65 61 74 65 00 32 30 32 33 2D  ate:create.2023-
000000B0  30 36 2D 31 31 54 31 38 3A 35 35 3A 30 32 2B 30  06-11T18:55:02+0
000000C0  30 3A 30 30 46 1B DE 47 00 00 00 25 74 45 58 74  0:00F..G...%tEXt
000000D0  64 61 74 65 3A 6D 6F 64 69 66 79 00 32 30 32 33  date:modify.2023
000000E0  2D 30 36 2D 31 31 54 31 38 3A 35 35 3A 30 32 2B  -06-11T18:55:02+
```

https://alielasfoury.github.io/writeups/nahamcon-ctf-pang.html
https://github.com/sherlly/PCRT



```
—(mactavish㉿oracle)-[~/PCRT]
└$ sudo python2 PCRT.py -v -i /home/mactavish/Downloads/chall.png
[sudo] password for mactavish:

         ____   ____ ____ _____
        |  _ \ / ___|  _ \_   _|
        | |_) | |   | |_) || |
        |  __/| |___|  _ < | |
        |_|    \____|_| \_\|_|

        PNG Check & Repair Tool

Project address: https://github.com/sherlly/PCRT
Author: sherlly
Version: 1.1

[Finished] Correct PNG header
[Detected] Error IHDR CRC found! (offset: 0x1D)
chunk crc: 5878D30F
correct crc: 5A2BD30F
[Notice] Try fixing it? (y or n) [default:y] y
[Finished] Successfully fix crc
[Finished] IHDR chunk check complete (offset: 0x8)
[Finished] Correct IDAT chunk data length (offset: 0xF9 length: E2A0)
[Detected] Error IDAT CRC found! (offset: 0xE3A1)
chunk crc: 0C787800
correct crc: 0C78F400
[Notice] Try fixing it? (y or n) [default:y] y
[Finished] Successfully fix crc
[Finished] IDAT chunk check complete (offset: 0xF9)
```

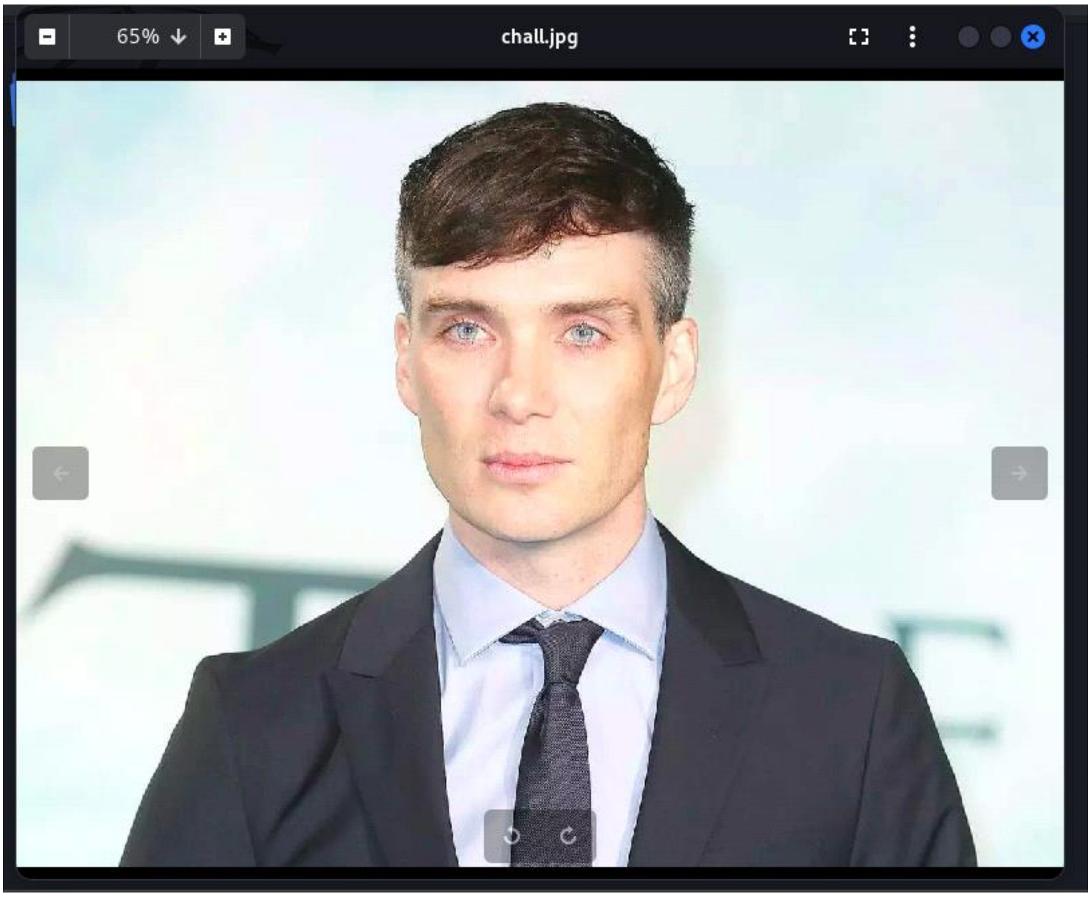


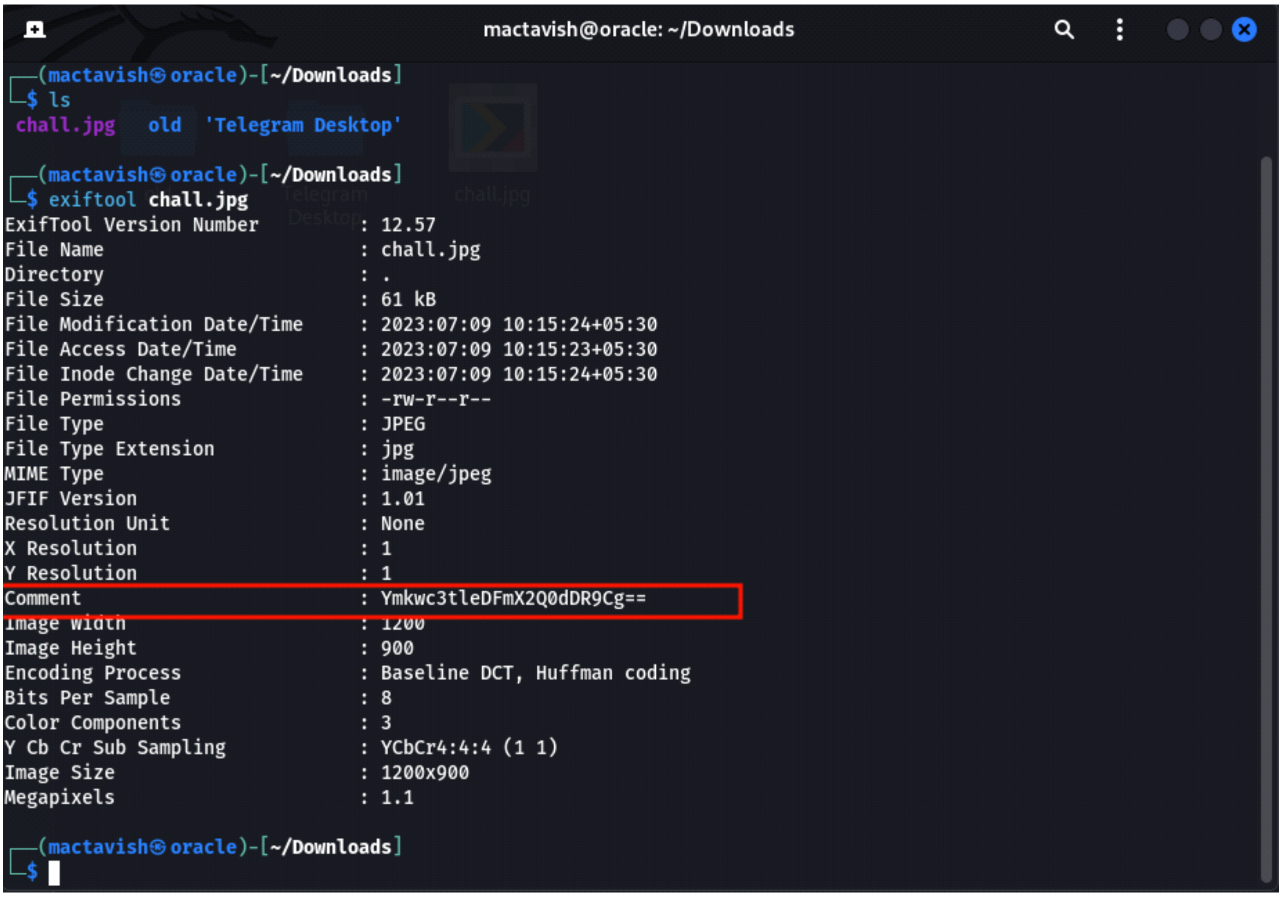
```
Show the repaired image? (y or n) [default:n] y
```

Pr0ject_M3t4

bi0s{ex1f_d4t4}

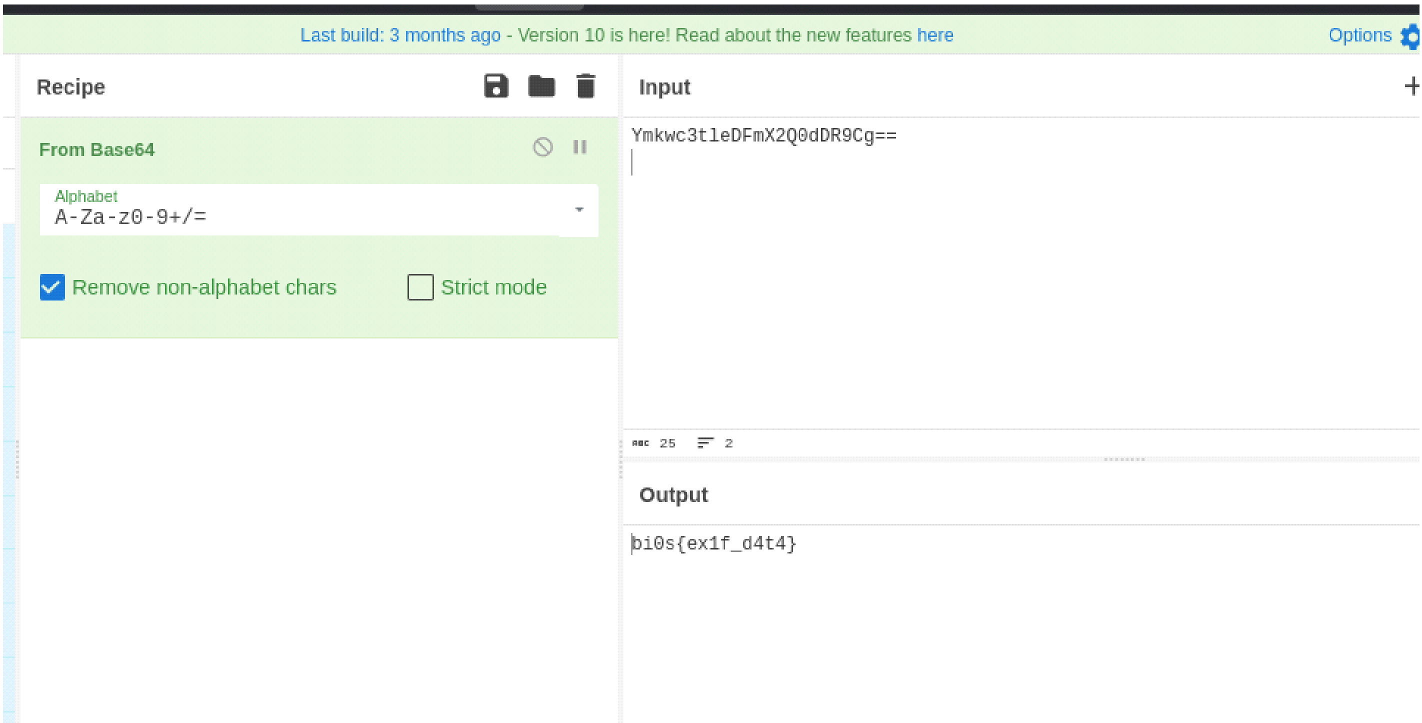
08 July 2023 16:18





```
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ ls
chall.jpg   old  'Telegram Desktop'

┌──(mactavish㉿oracle)-[~/Downloads]
└─$ exiftool chall.jpg
ExifTool Version Number         : 12.57
File Name                       : chall.jpg
Directory                       : .
File Size                       : 61 kB
File Modification Date/Time     : 2023:07:09 10:15:24+05:30
File Access Date/Time           : 2023:07:09 10:15:23+05:30
File Inode Change Date/Time     : 2023:07:09 10:15:24+05:30
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Comment                         : Ymkwc3tleDFmX2Q0dDR9Cg==
Image Width                     : 1200
Image Height                    : 900
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 1200x900
Megapixels                      : 1.1

┌──(mactavish㉿oracle)-[~/Downloads]
└─$ 
```

Ymkwc3tleDFmX2Q0dDR9Cg=


Last build: 3 months ago - Version 10 is here! Read about the new features here
Options
Recipe
Input
Output

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars   □ Strict mode

```
Ymkwc3tleDFmX2Q0dDR9Cg==
```

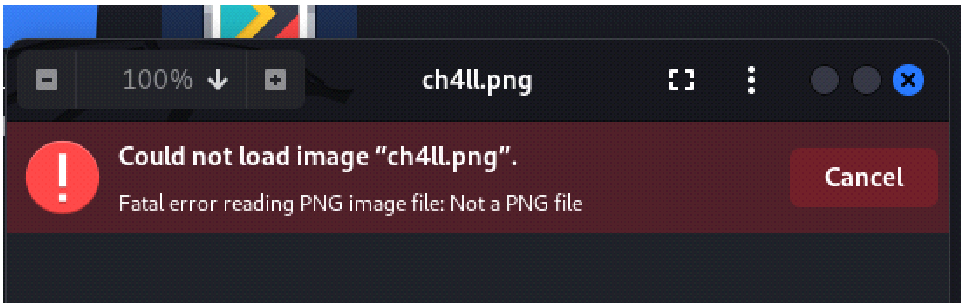
abc 25 ≡ 2

```
bi0s{ex1f_d4t4}
```

f1xm3

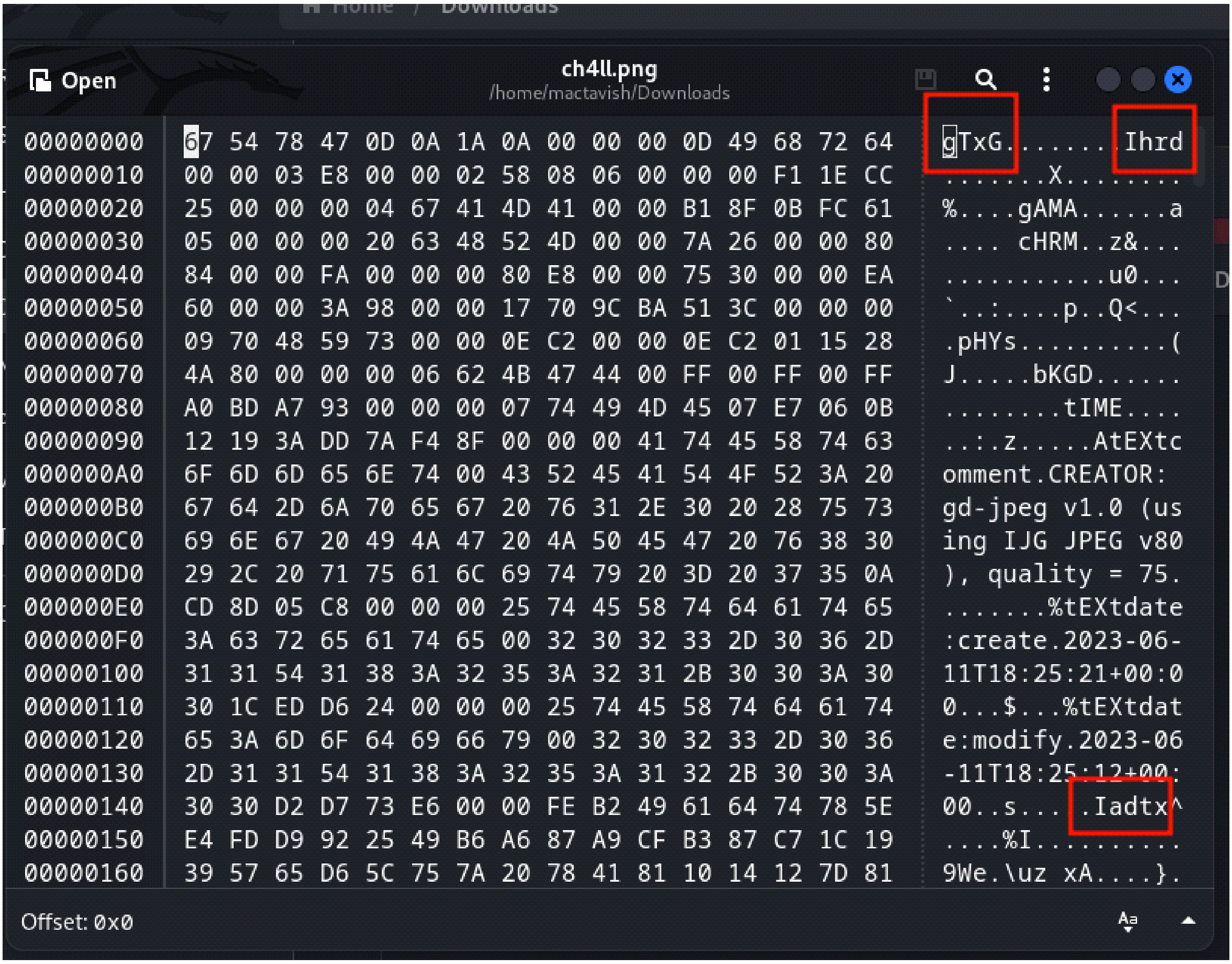
bi0s{g00d_f1x_g00d_solv3}

08 July 2023 16:19



Could not load image “ch4ll.png”.

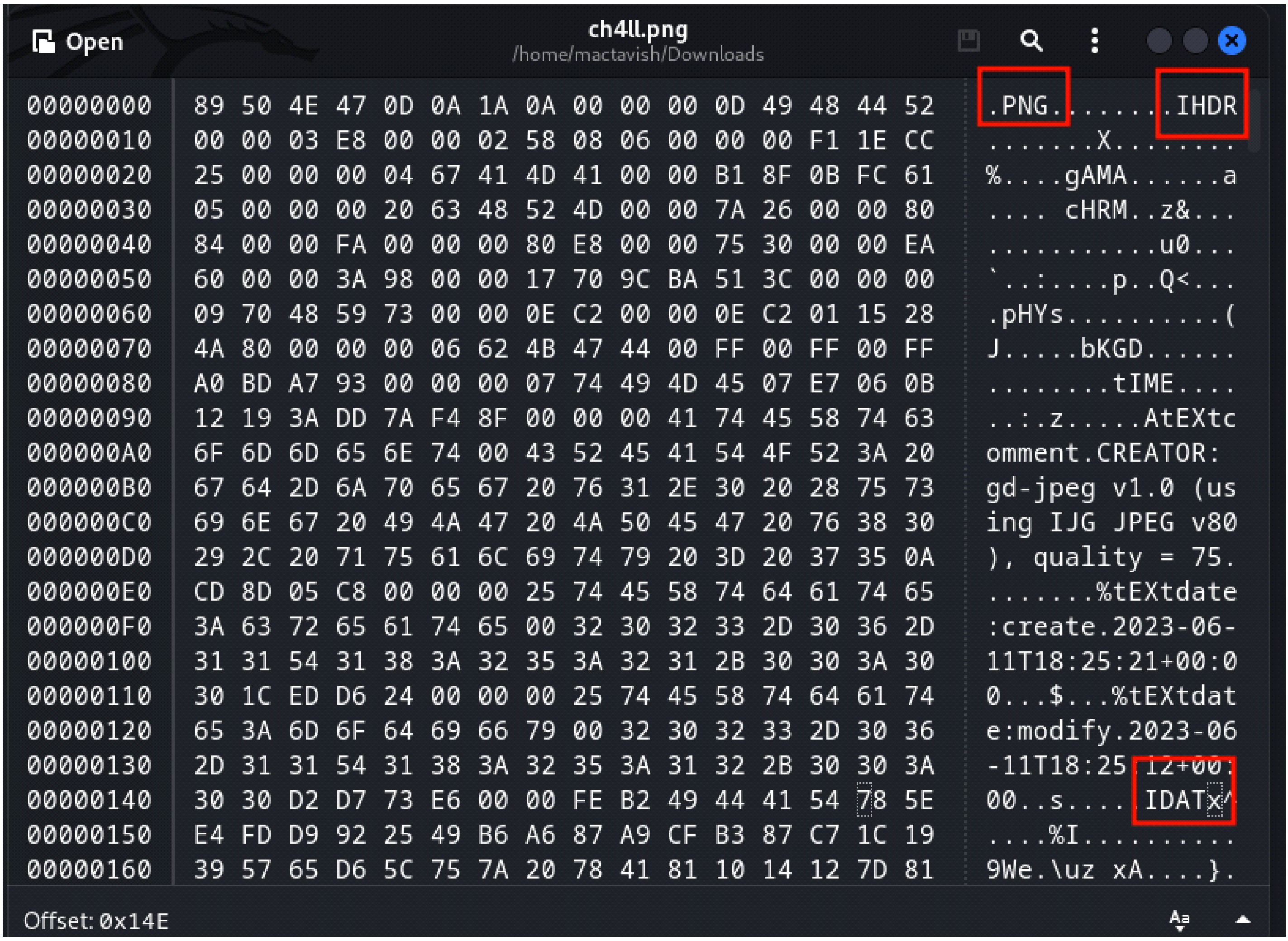
Fatal error reading PNG image file: Not a PNG file



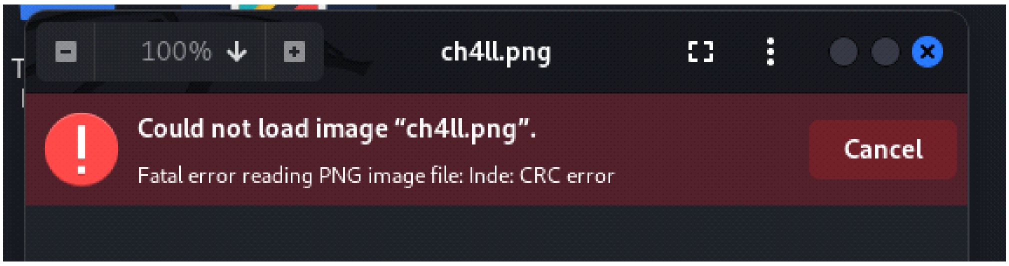
```
00000000  67 54 78 47 0D 0A 1A 0A 00 00 00 0D 49 68 72 64  gTxG........Ihrd
00000010  00 00 03 E8 00 00 02 58 08 06 00 00 00 F1 1E CC  .......X........
00000020  25 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61  %....gAMA......a
00000030  05 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80  .... cHRM..z&...
00000040  84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA  ...........u0...
00000050  60 00 00 3A 98 00 00 17 70 9C BA 51 3C 00 00 00  `..:....p..Q<...
00000060  09 70 48 59 73 00 00 0E C2 00 00 0E C2 01 15 28  .pHYs..........(
00000070  4A 80 00 00 00 06 62 4B 47 44 00 FF 00 FF 00 FF  J.....bKGD......
00000080  A0 BD A7 93 00 00 00 07 74 49 4D 45 07 E7 06 0B  ........tIME....
00000090  12 19 3A DD 7A F4 8F 00 00 00 41 74 45 58 74 63  ..:.z.....AtEXtc
000000A0  6F 6D 6D 65 6E 74 00 43 52 45 41 54 4F 52 3A 20  omment.CREATOR: 
000000B0  67 64 2D 6A 70 65 67 20 76 31 2E 30 20 28 75 73  gd-jpeg v1.0 (us
000000C0  69 6E 67 20 49 4A 47 20 4A 50 45 47 20 76 38 30  ing IJG JPEG v80
000000D0  29 2C 20 71 75 61 6C 69 74 79 20 3D 20 37 35 0A  ), quality = 75.
000000E0  CD 8D 05 C8 00 00 00 25 74 45 58 74 64 61 74 65  .......%tEXtdate
000000F0  3A 63 72 65 61 74 65 00 32 30 32 33 2D 30 36 2D  :create.2023-06-
00000100  31 31 54 31 38 3A 32 35 3A 32 31 2B 30 30 3A 30  11T18:25:21+00:0
00000110  30 1C ED D6 24 00 00 00 25 74 45 58 74 64 61 74  0...$...%tEXtdat
00000120  65 3A 6D 6F 64 69 66 79 00 32 30 32 33 2D 30 36  e:modify.2023-06
00000130  2D 31 31 54 31 38 3A 32 35 3A 31 32 2B 30 30 3A  -11T18:25:12+00:
00000140  30 30 D2 D7 73 E6 00 00 FE B2 49 61 64 74 78 5E  00..s.....Iadtx^
00000150  E4 FD D9 92 25 49 B6 A6 87 A9 CF B3 87 C7 1C 19  ....%I..........
00000160  39 57 65 D6 5C 75 7A 20 78 41 81 10 14 12 7D 81  9We.\uz xA....}.
```

Offset: 0x0

https://stackoverflow.com/questions/26150797/idat-chunk-of-png-file-format

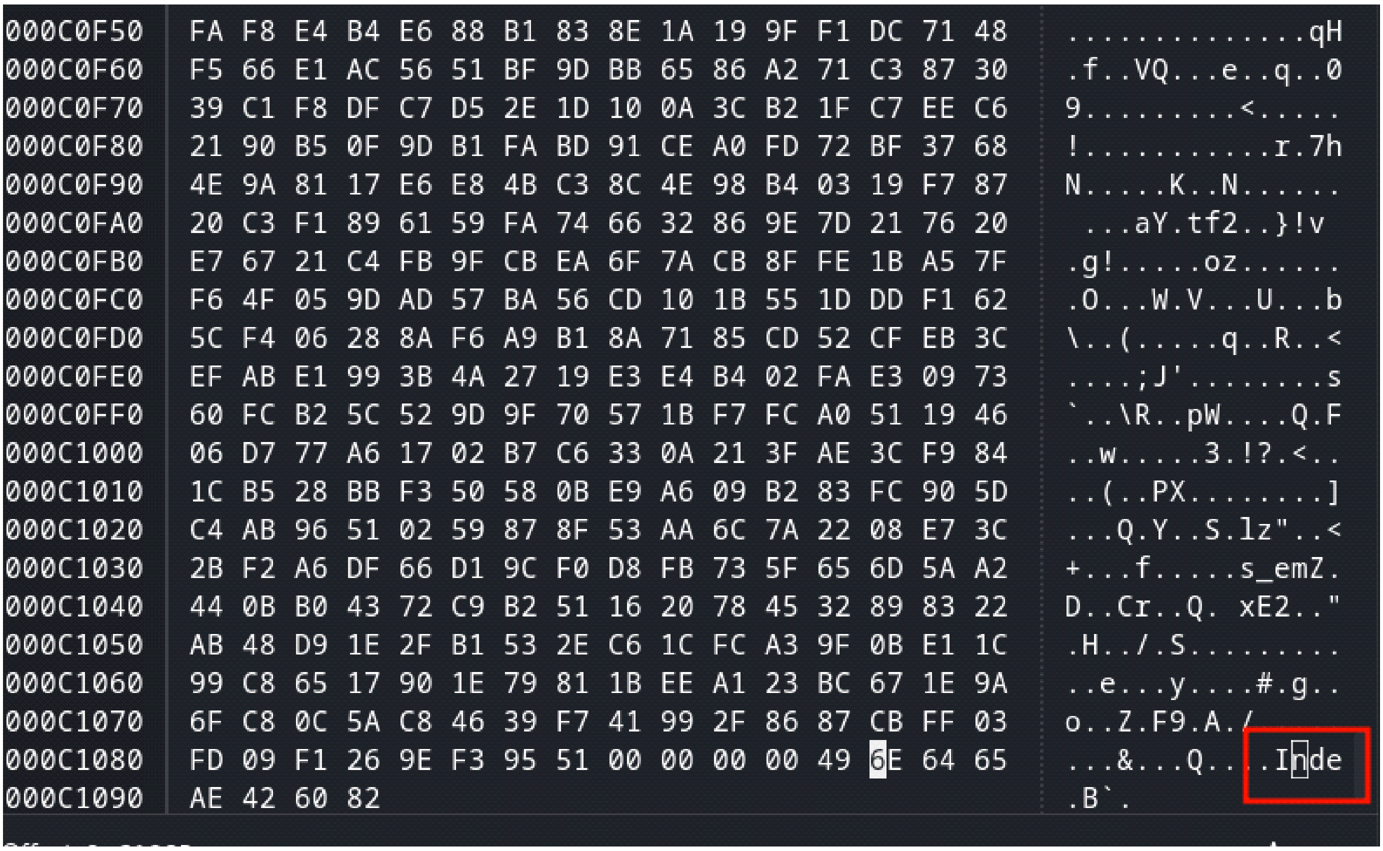


```
00000000  89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  .PNG........IHDR
00000010  00 00 03 E8 00 00 02 58 08 06 00 00 00 F1 1E CC  .......X........
00000020  25 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61  %....gAMA......a
00000030  05 00 00 00 20 63 48 52 4D 00 00 7A 26 00 00 80  .... cHRM..z&...
00000040  84 00 00 FA 00 00 00 80 E8 00 00 75 30 00 00 EA  ...........u0...
00000050  60 00 00 3A 98 00 00 17 70 9C BA 51 3C 00 00 00  `..:....p..Q<...
00000060  09 70 48 59 73 00 00 0E C2 00 00 0E C2 01 15 28  .pHYs..........(
00000070  4A 80 00 00 00 06 62 4B 47 44 00 FF 00 FF 00 FF  J.....bKGD......
00000080  A0 BD A7 93 00 00 00 07 74 49 4D 45 07 E7 06 0B  ........tIME....
00000090  12 19 3A DD 7A F4 8F 00 00 00 41 74 45 58 74 63  ..:.z.....AtEXtc
000000A0  6F 6D 6D 65 6E 74 00 43 52 45 41 54 4F 52 3A 20  omment.CREATOR: 
000000B0  67 64 2D 6A 70 65 67 20 76 31 2E 30 20 28 75 73  gd-jpeg v1.0 (us
000000C0  69 6E 67 20 49 4A 47 20 4A 50 45 47 20 76 38 30  ing IJG JPEG v80
000000D0  29 2C 20 71 75 61 6C 69 74 79 20 3D 20 37 35 0A  ), quality = 75.
000000E0  CD 8D 05 C8 00 00 00 25 74 45 58 74 64 61 74 65  .......%tEXtdate
000000F0  3A 63 72 65 61 74 65 00 32 30 32 33 2D 30 36 2D  :create.2023-06-
00000100  31 31 54 31 38 3A 32 35 3A 32 31 2B 30 30 3A 30  11T18:25:21+00:0
00000110  30 1C ED D6 24 00 00 00 25 74 45 58 74 64 61 74  0...$...%tEXtdat
00000120  65 3A 6D 6F 64 69 66 79 00 32 30 32 33 2D 30 36  e:modify.2023-06
00000130  2D 31 31 54 31 38 3A 32 35 3A 31 32 2B 30 30 3A  -11T18:25:12+00:
00000140  30 30 D2 D7 73 E6 00 00 FE B2 49 44 41 54 78 5E  00..s.....IDATx^
00000150  E4 FD D9 92 25 49 B6 A6 87 A9 CF B3 87 C7 1C 19  ....%I..........
00000160  39 57 65 D6 5C 75 7A 20 78 41 81 10 14 12 7D 81  9We.\uz xA....}.
Offset: 0x14E
```

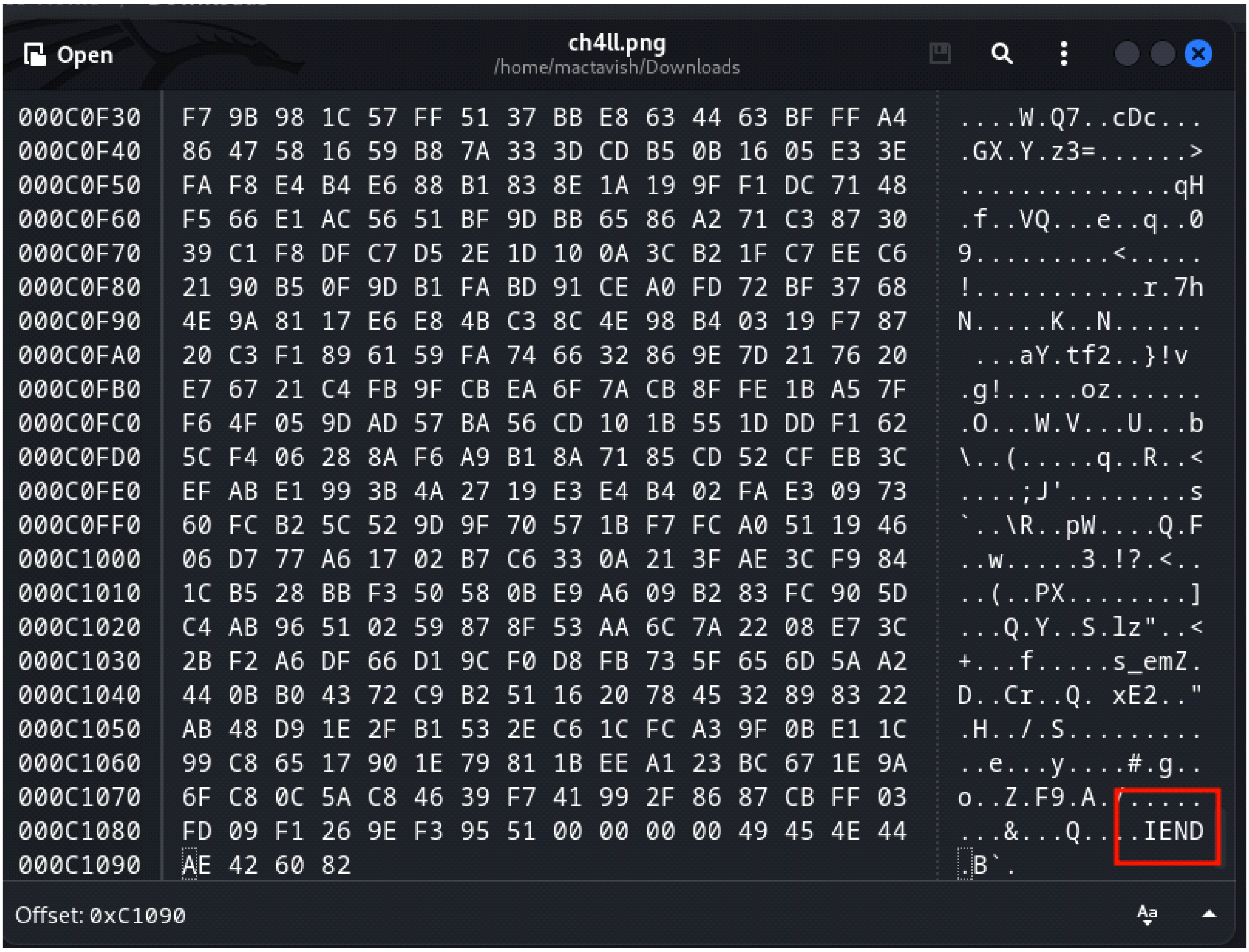


Could not load image "ch4ll.png".

Fatal error reading PNG image file: Inde: CRC error



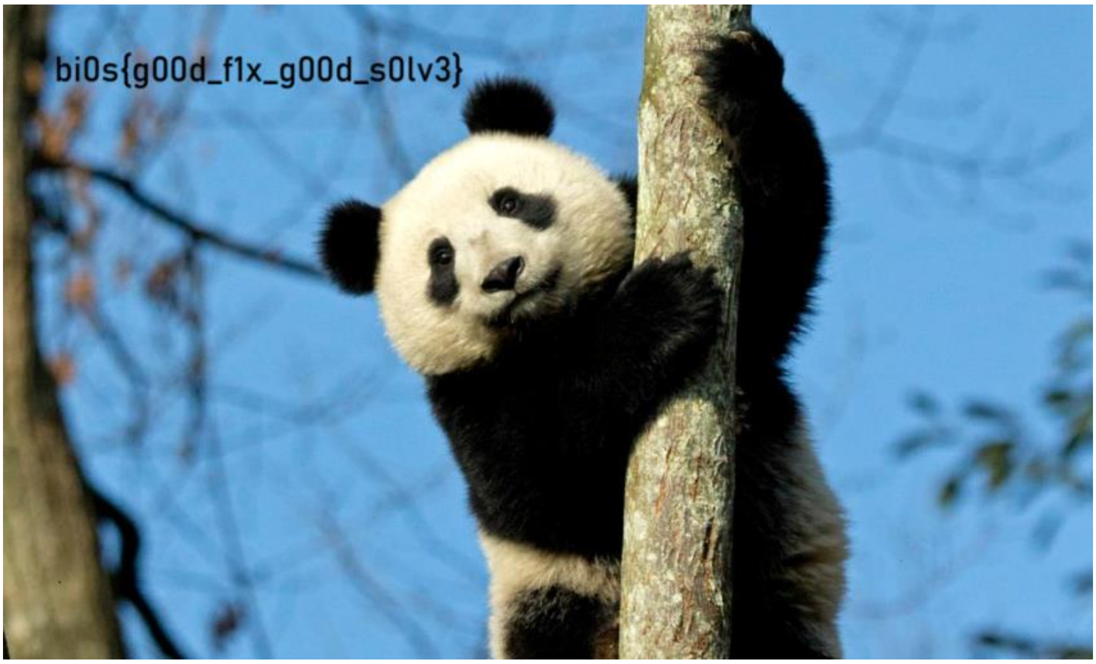
```
000C0F50   FA F8 E4 B4 E6 88 B1 83 8E 1A 19 9F F1 DC 71 48   ..............qH
000C0F60   F5 66 E1 AC 56 51 BF 9D BB 65 86 A2 71 C3 87 30   .f..VQ...e..q..0
000C0F70   39 C1 F8 DF C7 D5 2E 1D 10 0A 3C B2 1F C7 EE C6   9.........<.....
000C0F80   21 90 B5 0F 9D B1 FA BD 91 CE A0 FD 72 BF 37 68   !...........r.7h
000C0F90   4E 9A 81 17 E6 E8 4B C3 8C 4E 98 B4 03 19 F7 87   N.....K..N......
000C0FA0   20 C3 F1 89 61 59 FA 74 66 32 86 9E 7D 21 76 20    ...aY.tf2..}!v 
000C0FB0   E7 67 21 C4 FB 9F CB EA 6F 7A CB 8F FE 1B A5 7F   .g!.....oz......
000C0FC0   F6 4F 05 9D AD 57 BA 56 CD 10 1B 55 1D DD F1 62   .O...W.V...U...b
000C0FD0   5C F4 06 28 8A F6 A9 B1 8A 71 85 CD 52 CF EB 3C   \..(.....q..R..<
000C0FE0   EF AB E1 99 3B 4A 27 19 E3 E4 B4 02 FA E3 09 73   ....;J'........s
000C0FF0   60 FC B2 5C 52 9D 9F 70 57 1B F7 FC A0 51 19 46   `..\R..pW....Q.F
000C1000   06 D7 77 A6 17 02 B7 C6 33 0A 21 3F AE 3C F9 84   ..w.....3.!?.<..
000C1010   1C B5 28 BB F3 50 58 0B E9 A6 09 B2 83 FC 90 5D   ..(..PX........]
000C1020   C4 AB 96 51 02 59 87 8F 53 AA 6C 7A 22 08 E7 3C   ...Q.Y..S.lz"..<
000C1030   2B F2 A6 DF 66 D1 9C F0 D8 FB 73 5F 65 6D 5A A2   +...f.....s_emZ.
000C1040   44 0B B0 43 72 C9 B2 51 16 20 78 45 32 89 83 22   D..Cr..Q. xE2.."
000C1050   AB 48 D9 1E 2F B1 53 2E C6 1C FC A3 9F 0B E1 1C   .H../.S.........
000C1060   99 C8 65 17 90 1E 79 81 1B EE A1 23 BC 67 1E 9A   ..e...y....#.g..
000C1070   6F C8 0C 5A C8 46 39 F7 41 99 2F 86 87 CB FF 03   o..Z.F9.A./.....
000C1080   FD 09 F1 26 9E F3 95 51 00 00 00 00 49 6E 64 65   ...&...Q....Inde
000C1090   AE 42 60 82                                       .B`.
```



ch4ll.png
/home/mactavish/Downloads

```
000C0F30   F7 9B 98 1C 57 FF 51 37 BB E8 63 44 63 BF FF A4   ....W.Q7..cDc...
000C0F40   86 47 58 16 59 B8 7A 33 3D CD B5 0B 16 05 E3 3E   .GX.Y.z3=......>
000C0F50   FA F8 E4 B4 E6 88 B1 83 8E 1A 19 9F F1 DC 71 48   ..............qH
000C0F60   F5 66 E1 AC 56 51 BF 9D BB 65 86 A2 71 C3 87 30   .f..VQ...e..q..0
000C0F70   39 C1 F8 DF C7 D5 2E 1D 10 0A 3C B2 1F C7 EE C6   9.........<.....
000C0F80   21 90 B5 0F 9D B1 FA BD 91 CE A0 FD 72 BF 37 68   !...........r.7h
000C0F90   4E 9A 81 17 E6 E8 4B C3 8C 4E 98 B4 03 19 F7 87   N.....K..N......
000C0FA0   20 C3 F1 89 61 59 FA 74 66 32 86 9E 7D 21 76 20    ...aY.tf2..}!v 
000C0FB0   E7 67 21 C4 FB 9F CB EA 6F 7A CB 8F FE 1B A5 7F   .g!.....oz......
000C0FC0   F6 4F 05 9D AD 57 BA 56 CD 10 1B 55 1D DD F1 62   .O...W.V...U...b
000C0FD0   5C F4 06 28 8A F6 A9 B1 8A 71 85 CD 52 CF EB 3C   \..(.....q..R..<
000C0FE0   EF AB E1 99 3B 4A 27 19 E3 E4 B4 02 FA E3 09 73   ....;J'........s
000C0FF0   60 FC B2 5C 52 9D 9F 70 57 1B F7 FC A0 51 19 46   `..\R..pW....Q.F
000C1000   06 D7 77 A6 17 02 B7 C6 33 0A 21 3F AE 3C F9 84   ..w.....3.!?.<..
000C1010   1C B5 28 BB F3 50 58 0B E9 A6 09 B2 83 FC 90 5D   ..(..PX........]
000C1020   C4 AB 96 51 02 59 87 8F 53 AA 6C 7A 22 08 E7 3C   ...Q.Y..S.lz"..<
000C1030   2B F2 A6 DF 66 D1 9C F0 D8 FB 73 5F 65 6D 5A A2   +...f.....s_emZ.
000C1040   44 0B B0 43 72 C9 B2 51 16 20 78 45 32 89 83 22   D..Cr..Q. xE2.."
000C1050   AB 48 D9 1E 2F B1 53 2E C6 1C FC A3 9F 0B E1 1C   .H../.S.........
000C1060   99 C8 65 17 90 1E 79 81 1B EE A1 23 BC 67 1E 9A   ..e...y....#.g..
000C1070   6F C8 0C 5A C8 46 39 F7 41 99 2F 86 87 CB FF 03   o..Z.F9.A./.....
000C1080   FD 09 F1 26 9E F3 95 51 00 00 00 00 49 45 4E 44   ...&...Q....IEND
000C1090   AE 42 60 82                                       .B`.
```

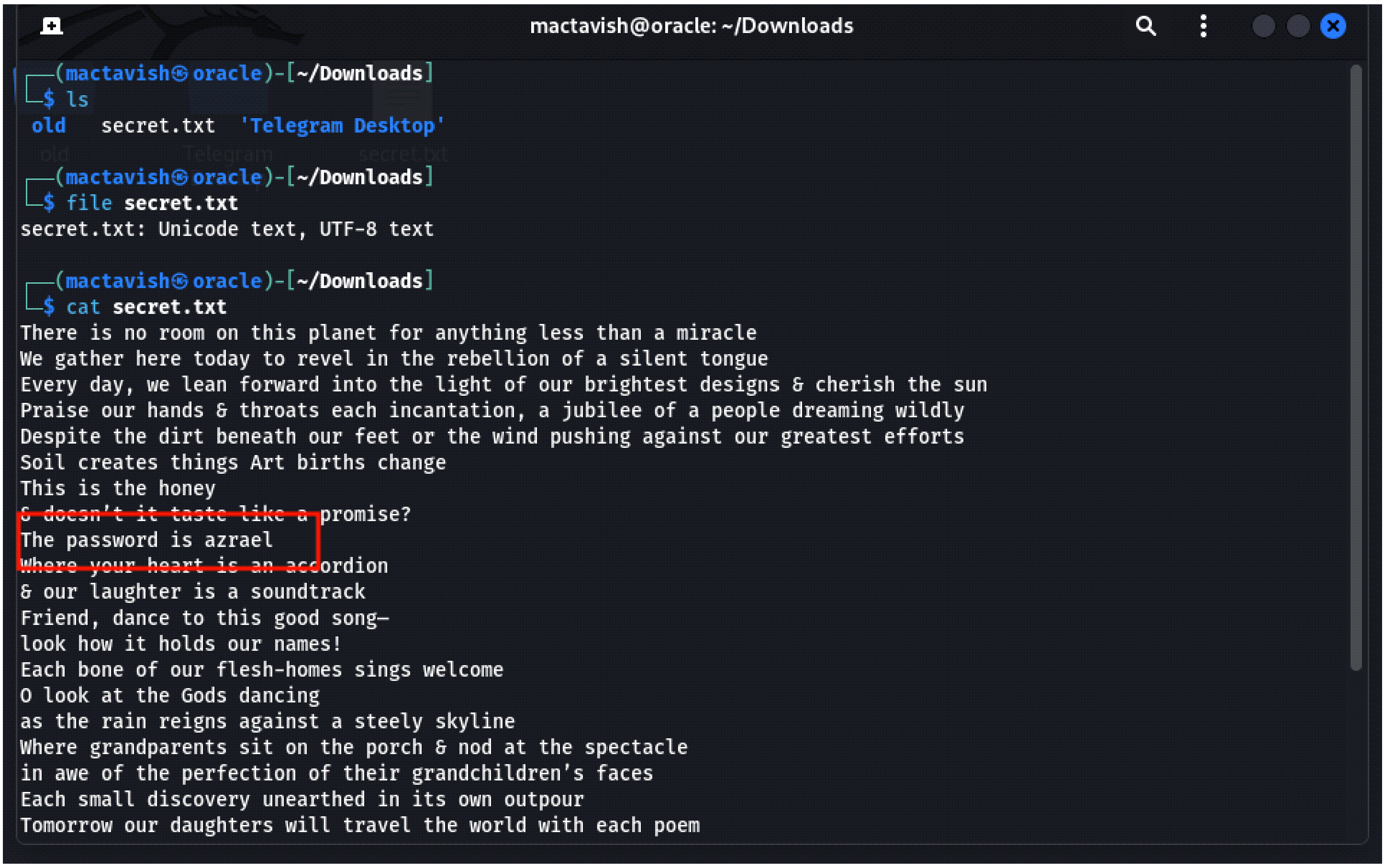
Offset: 0xC1090


bi0s{g00d_f1x_g00d_s0lv3}

C4pt4inC0ld

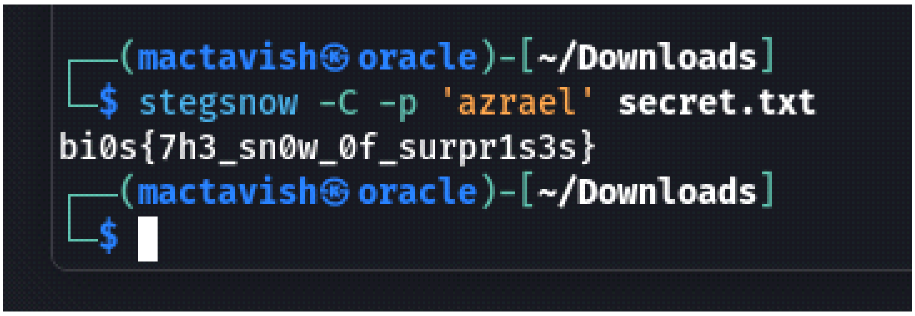
bi0s{7h3_sn0w_0f_surpr1s3s}

08 July 2023 16:20



```
mactavish@oracle: ~/Downloads

┌──(mactavish㉿oracle)-[~/Downloads]
└─$ ls
 old   secret.txt  'Telegram Desktop'

┌──(mactavish㉿oracle)-[~/Downloads]
└─$ file secret.txt
secret.txt: Unicode text, UTF-8 text

┌──(mactavish㉿oracle)-[~/Downloads]
└─$ cat secret.txt
There is no room on this planet for anything less than a miracle
We gather here today to revel in the rebellion of a silent tongue
Every day, we lean forward into the light of our brightest designs & cherish the sun
Praise our hands & throats each incantation, a jubilee of a people dreaming wildly
Despite the dirt beneath our feet or the wind pushing against our greatest efforts
Soil creates things Art births change
This is the honey
& doesn't it taste like a promise?
The password is azrael
Where your heart is an accordion
& our laughter is a soundtrack
Friend, dance to this good song—
look how it holds our names!
Each bone of our flesh-homes sings welcome
O look at the Gods dancing
as the rain reigns against a steely skyline
Where grandparents sit on the porch & nod at the spectacle
in awe of the perfection of their grandchildren's faces
Each small discovery unearthed in its own outpour
Tomorrow our daughters will travel the world with each poem
```

The password is azrael

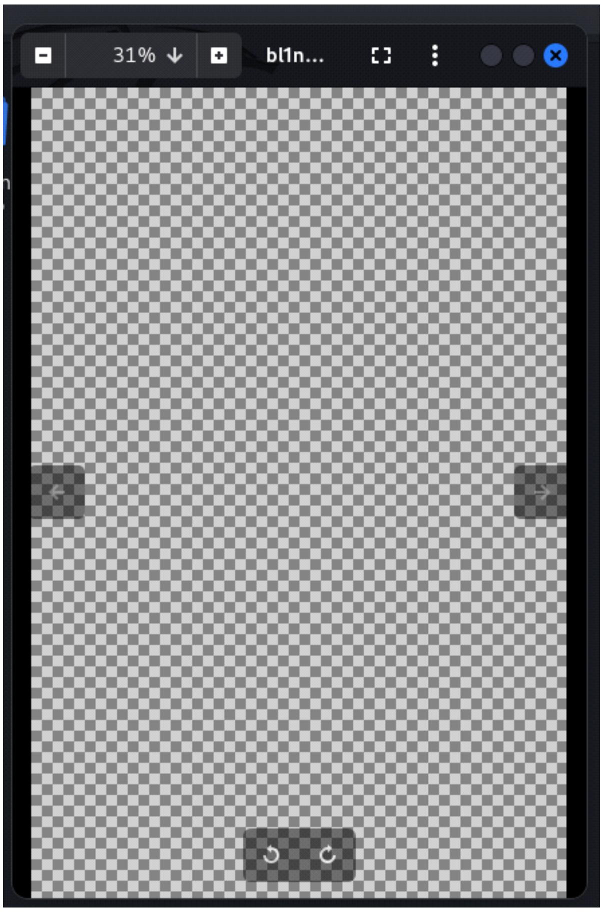


```
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ stegsnow -C -p 'azrael' secret.txt
bi0s{7h3_sn0w_0f_surpr1s3s}
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ 
```

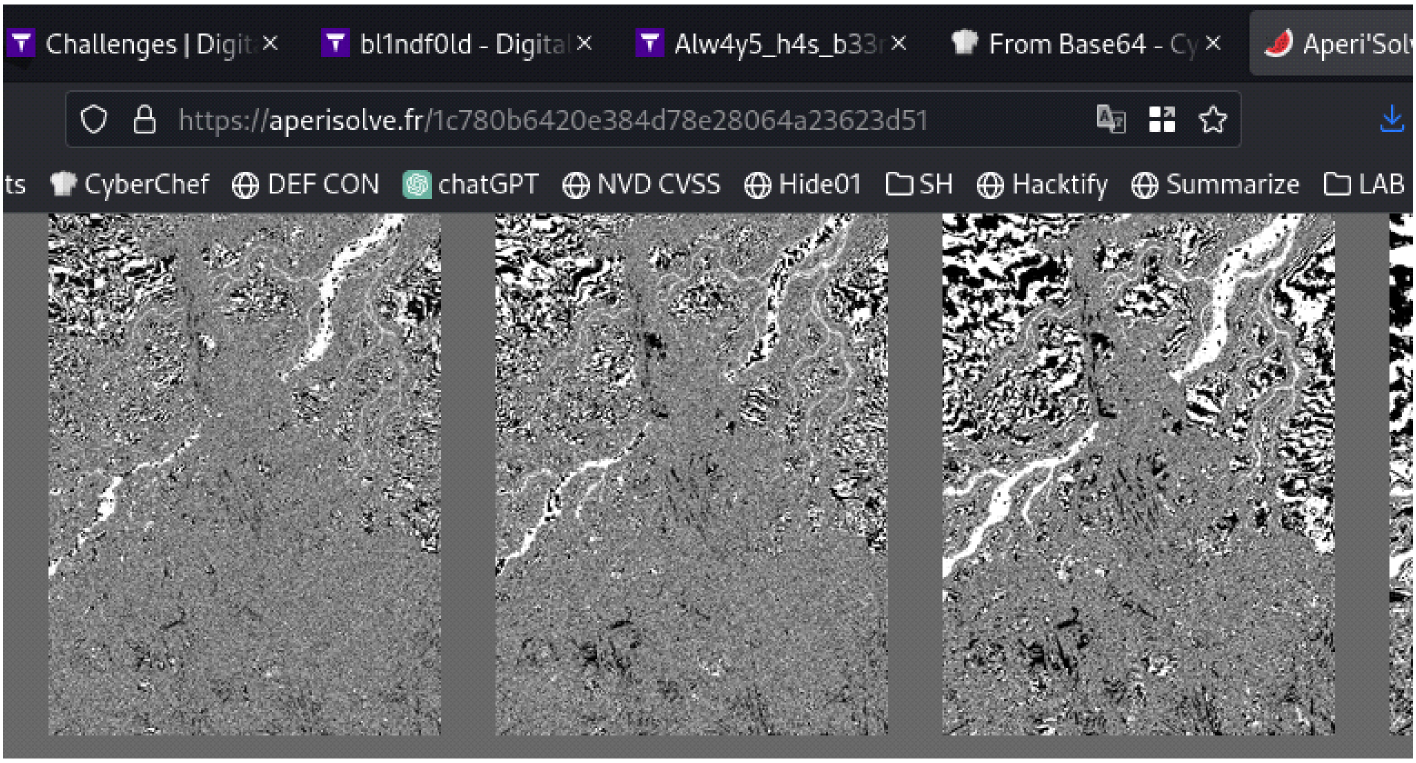
Bl1ndf0ld

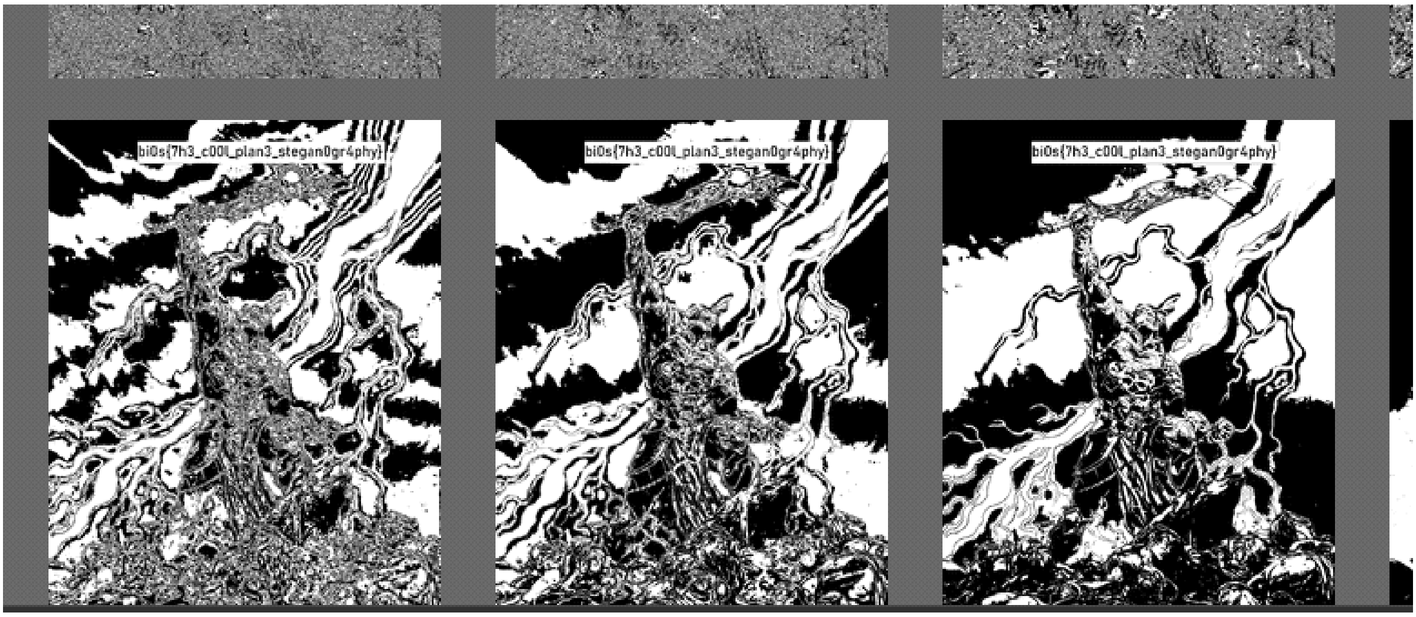
bi0s{7h3_c00l_plan3_stegan0gr4phy}

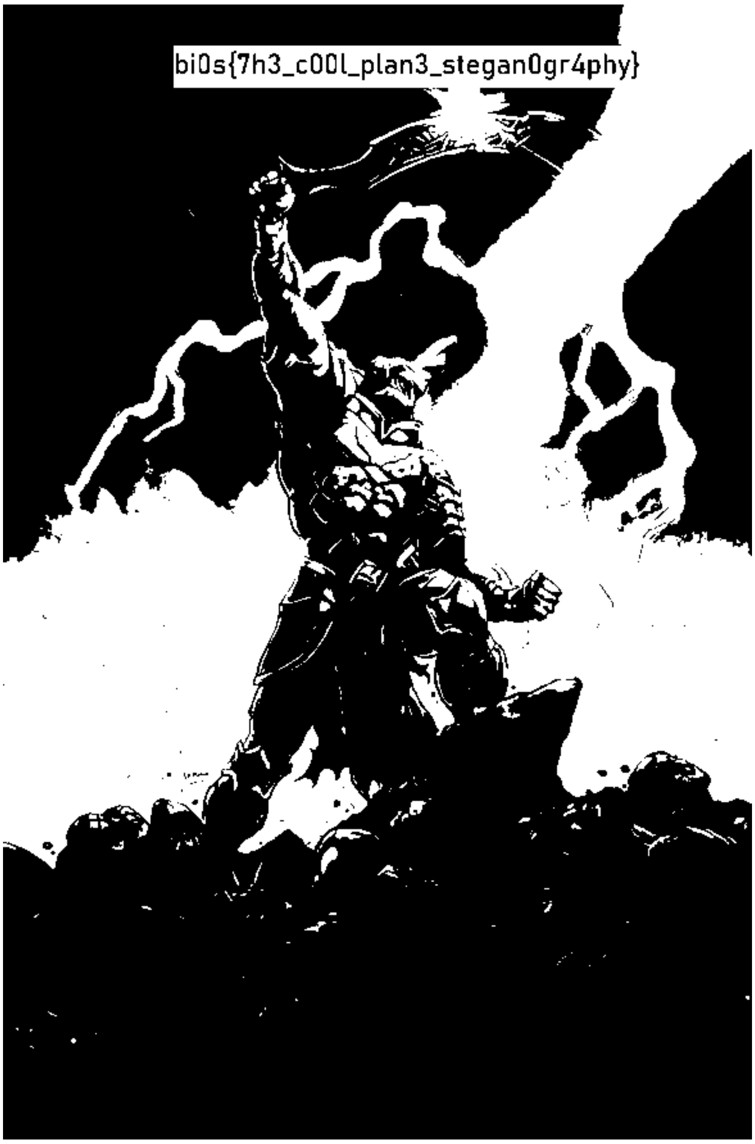
08 July 2023 16:21



https://aperisolve.fr



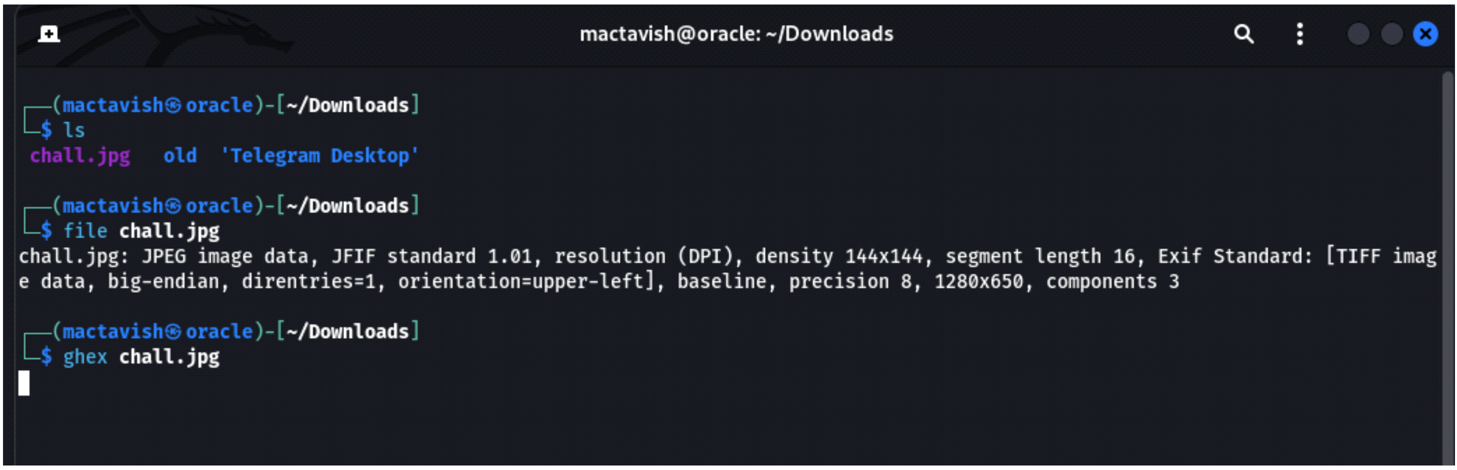

bi0s{7h3_c00l_plan3_stegan0gr4phy}
bi0s{7h3_c00l_plan3_stegan0gr4phy}
bi0s{7h3_c00l_plan3_stegan0gr4phy}


bi0s{7h3_c00l_plan3_stegan0gr4phy}

Alw4y5_h4s_b33n

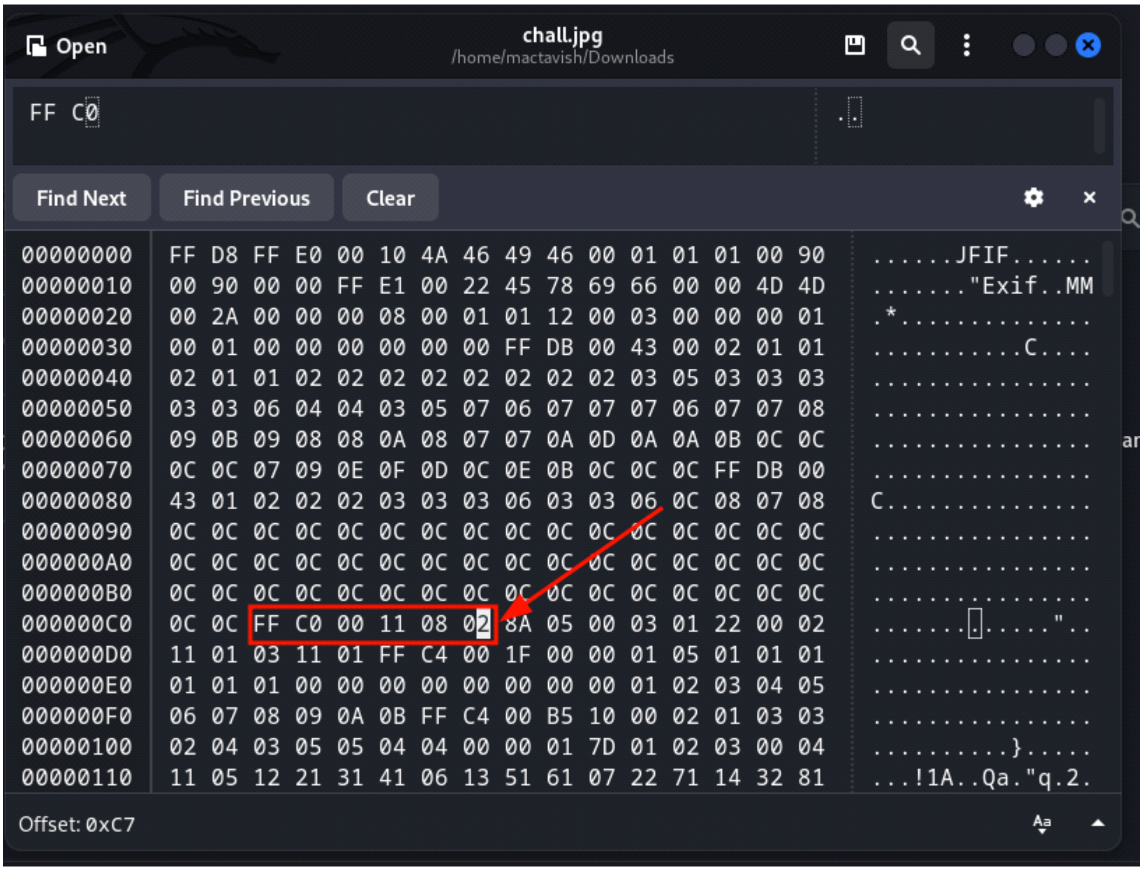
bi0s{th3_dimention_tr1ck}

08 July 2023 16:23



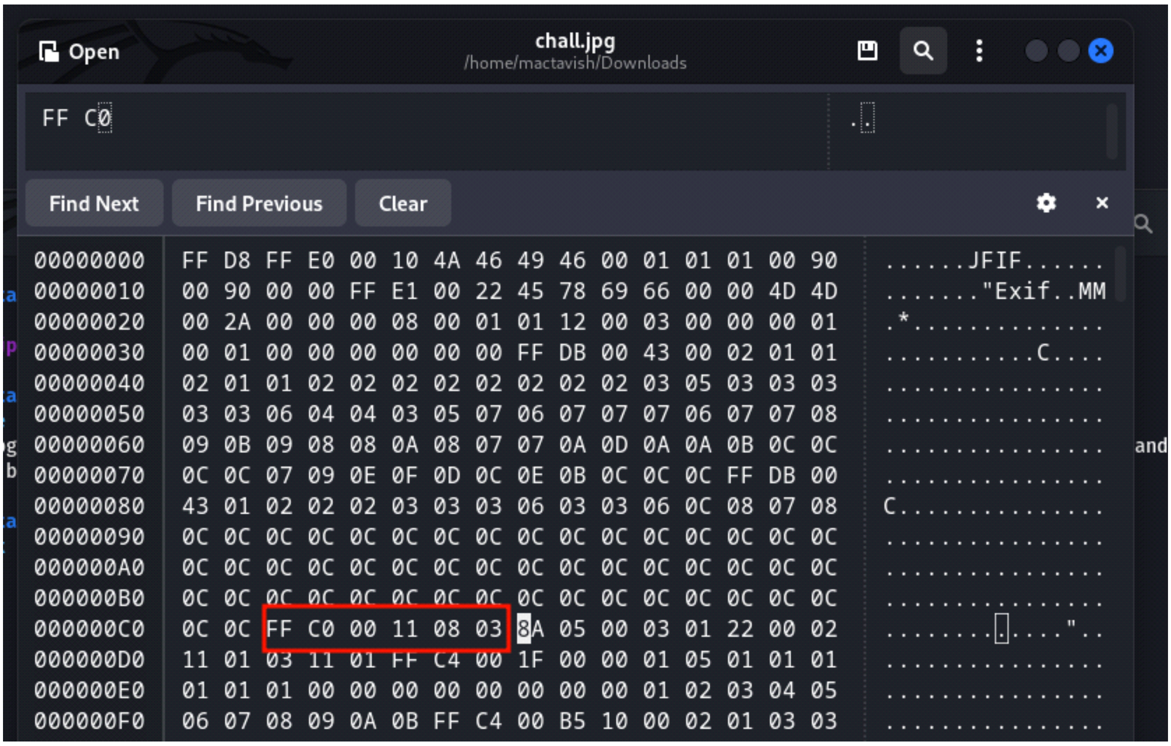
```
┌──(mactavish㉿oracle)-[~/Downloads]
└─$ ls
 chall.jpg   old  'Telegram Desktop'

┌──(mactavish㉿oracle)-[~/Downloads]
└─$ file chall.jpg
chall.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 144x144, segment length 16, Exif Standard: [TIFF imag
e data, big-endian, direntries=1, orientation=upper-left], baseline, precision 8, 1280x650, components 3

┌──(mactavish㉿oracle)-[~/Downloads]
└─$ ghex chall.jpg
█
```

https://www.experts-exchange.com/questions/11416918/How-to-Read-JPG-Height-and-Width-from-Binary-Hex-data.html

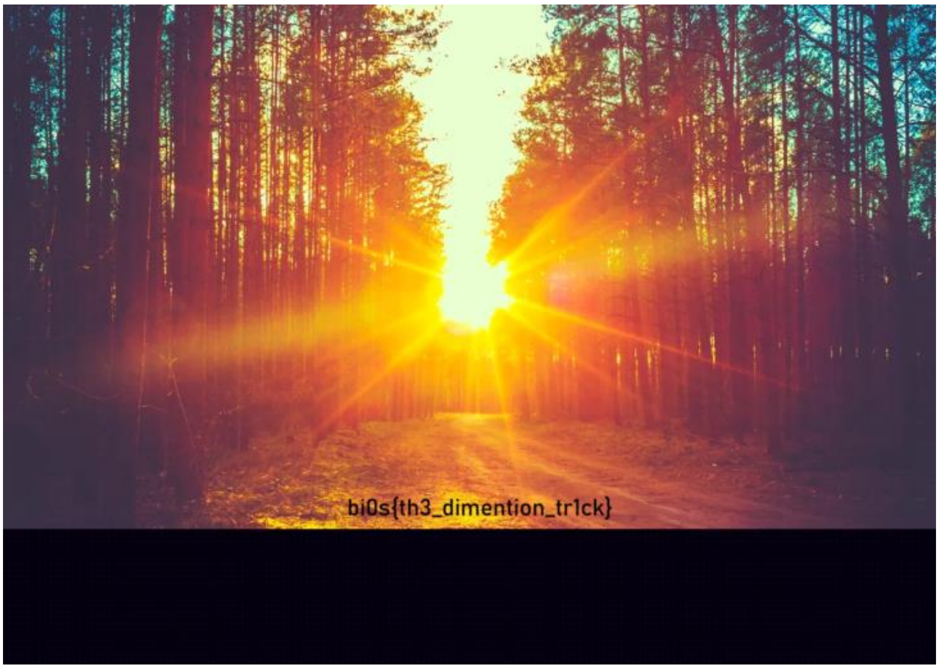


```
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 90  ......JFIF......
00000010  00 90 00 00 FF E1 00 22 45 78 69 66 00 00 4D 4D  ......."Exif..MM
00000020  00 2A 00 00 00 08 00 01 01 12 00 03 00 00 00 01  .*..............
00000030  00 01 00 00 00 00 00 00 FF DB 00 43 00 02 01 01  ...........C....
00000040  02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03  ................
00000050  03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08  ................
00000060  09 0B 09 08 08 0A 08 07 07 0A 0D 0A 0A 0B 0C 0C  ................
00000070  0C 0C 07 09 0E 0F 0D 0C 0E 0B 0C 0C 0C FF DB 00  ................
00000080  43 01 02 02 02 03 03 03 06 03 03 06 0C 08 07 08  C...............
00000090  0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
000000A0  0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
000000B0  0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
000000C0  0C 0C FF C0 00 11 08 02 8A 05 00 03 01 22 00 02  ............."..
000000D0  11 01 03 11 01 FF C4 00 1F 00 00 01 05 01 01 01  ................
000000E0  01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05  ................
000000F0  06 07 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03  ................
00000100  02 04 03 05 05 04 04 00 00 01 7D 01 02 03 00 04  ..........}.....
00000110  11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81  ...!1A..Qa."q.2.
```

Offset: 0xC7



```
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 90  ......JFIF......
00000010  00 90 00 00 FF E1 00 22 45 78 69 66 00 00 4D 4D  ......."Exif..MM
00000020  00 2A 00 00 00 08 00 01 01 12 00 03 00 00 00 01  .*..............
00000030  00 01 00 00 00 00 00 00 FF DB 00 43 00 02 01 01  ...........C....
00000040  02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03  ................
00000050  03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08  ................
00000060  09 0B 09 08 08 0A 08 07 07 0A 0D 0A 0A 0B 0C 0C  ................
00000070  0C 0C 07 09 0E 0F 0D 0C 0E 0B 0C 0C 0C FF DB 00  ................
00000080  43 01 02 02 02 03 03 03 06 03 03 06 0C 08 07 08  C...............
00000090  0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
000000A0  0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
000000B0  0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
000000C0  0C 0C FF C0 00 11 08 03 8A 05 00 03 01 22 00 02  ............."..
000000D0  11 01 03 11 01 FF C4 00 1F 00 00 01 05 01 01 01  ................
000000E0  01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05  ................
000000F0  06 07 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03  ................
```


bi0s{th3_dimention_tr1ck}