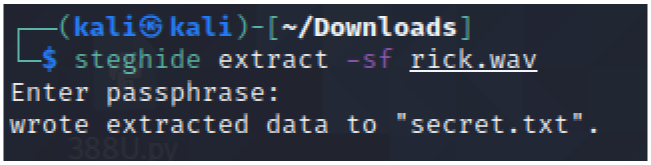
Forensics

1.1

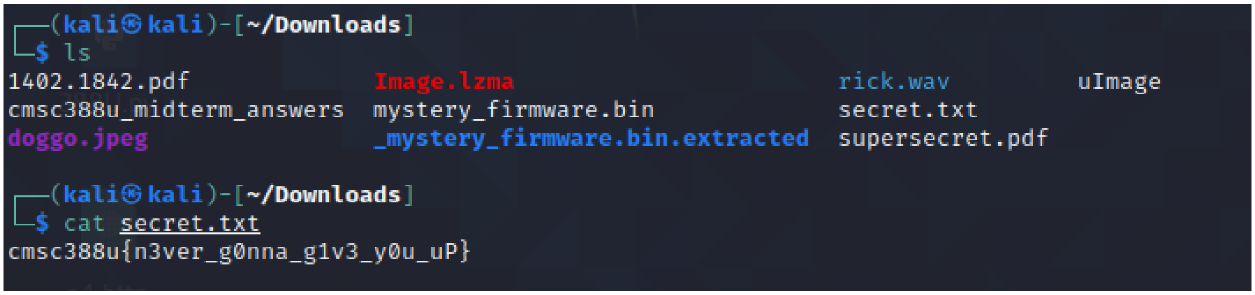
First I downloaded from
http://supersecure.store:7474/rick.wav
This gave me a file which when opened showed this:

To extract data from this file I ran the command `steghide extract -sf rick.wav`



```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf rick.wav
Enter passphrase:
wrote extracted data to "secret.txt".
```

For the passphrase, i simply hit enter. In secret.txt

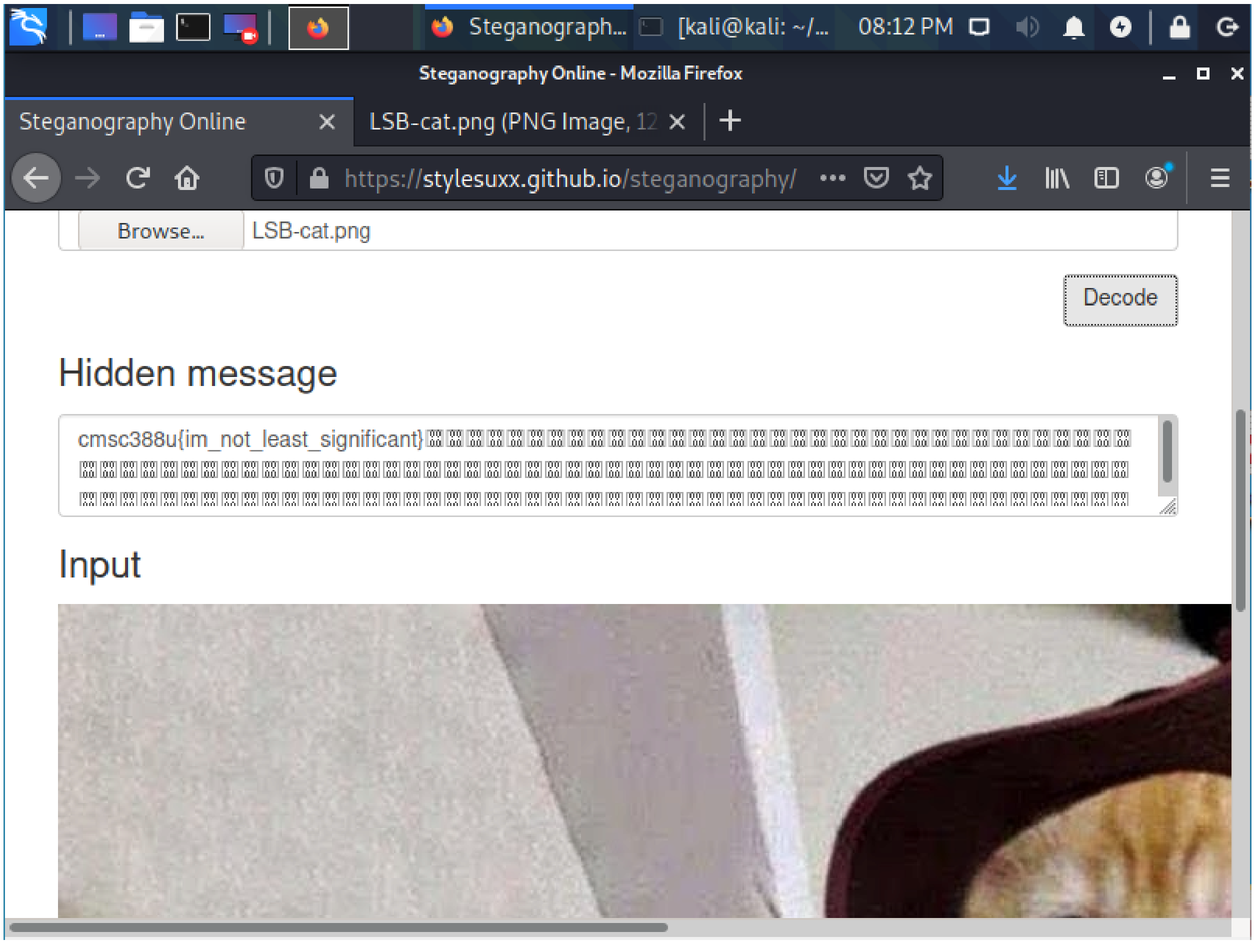


```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
1402.1842.pdf             Image.lzma                        rick.wav        uImage
cmsc388u_midterm_answers  mystery_firmware.bin              secret.txt
doggo.jpeg                _mystery_firmware.bin.extracted   supersecret.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ cat secret.txt
cmsc388u{n3ver_g0nna_g1v3_y0u_uP}
```

The flag is
`cmsc388u{n3ver_g0nna_g1v3_y0u_uP}`

1.2

The site, https://stylesuxx.github.io/steganography/ has both encryption and decryption tabs. Downloading the file from http://supersecure.store:7474/LSB-cat.png we can then upload the file and decode it


Steganograph...
[kali@kali: ~/...
08:12 PM
Steganography Online - Mozilla Firefox
Steganography Online
LSB-cat.png (PNG Image, 12
https://stylesuxx.github.io/steganography/
Browse...
LSB-cat.png
Decode

Hidden message

cmsc388u{im_not_least_significant}

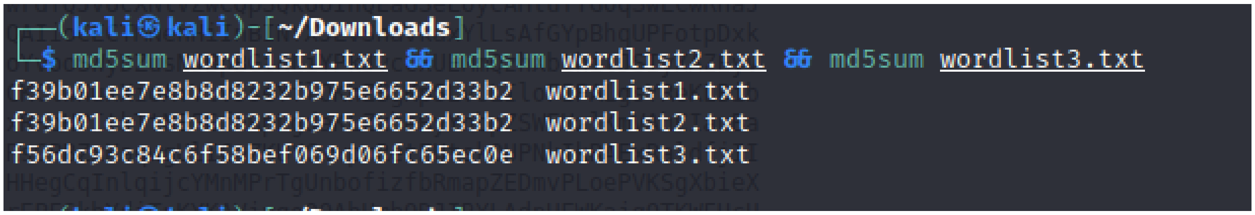
Input

The flag is then
`Cmsc388u{im_not_least_significant}`

2.1

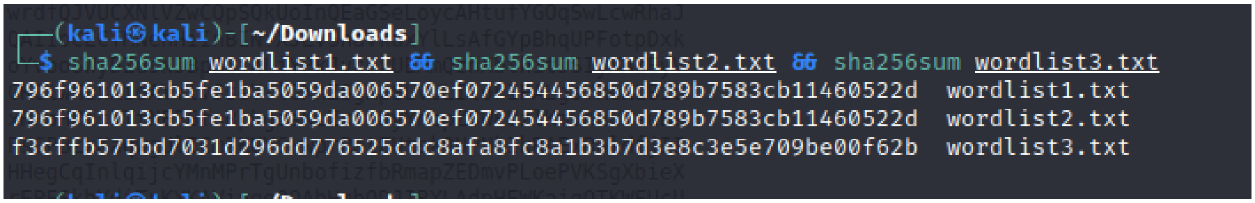
To find the differences in files, we can use the md5 and sha256 hashes to determine which files are the same and which files are different. Using the commands `md5sum` and `sha256sum`

```
md5sum wordlist1.txt && md5sum wordlist2.txt && md5sum
wordlist3.txt
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ md5sum wordlist1.txt && md5sum wordlist2.txt && md5sum wordlist3.txt
f39b01ee7e8b8d8232b975e6652d33b2  wordlist1.txt
f39b01ee7e8b8d8232b975e6652d33b2  wordlist2.txt
f56dc93c84c6f58bef069d06fc65ec0e  wordlist3.txt
```

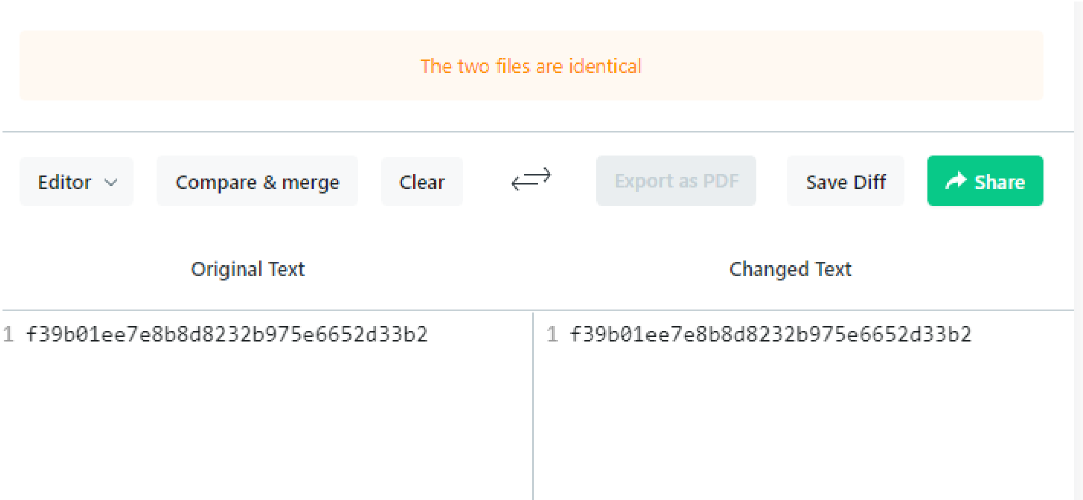
```
sha256sum wordlist1.txt && sha256sum wordlist2.txt && sha256sum wordlist3.txt
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sha256sum wordlist1.txt && sha256sum wordlist2.txt && sha256sum wordlist3.txt
796f961013cb5fe1ba5059da006570ef072454456850d789b7583cb11460522d  wordlist1.txt
796f961013cb5fe1ba5059da006570ef072454456850d789b7583cb11460522d  wordlist2.txt
f3cffb575bd7031d296dd776525cdc8afa8fc8a1b3b7d3e8c3e5e709be00f62b  wordlist3.txt
```

Using https://www.diffchecker.com/, we can compare the MD5 hashes

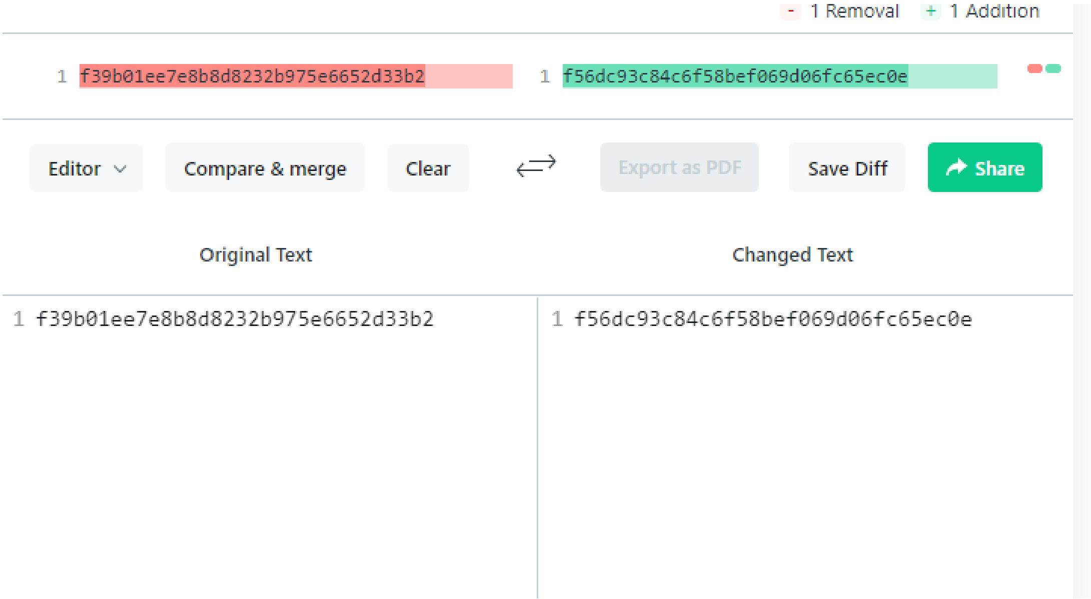
Wordlist1.txt and wordlist2.txt



The two files are identical

Original Text	Changed Text
1 f39b01ee7e8b8d8232b975e6652d33b2	1 f39b01ee7e8b8d8232b975e6652d33b2

Which are the same, then comparing them to wordlist3.txt yields:



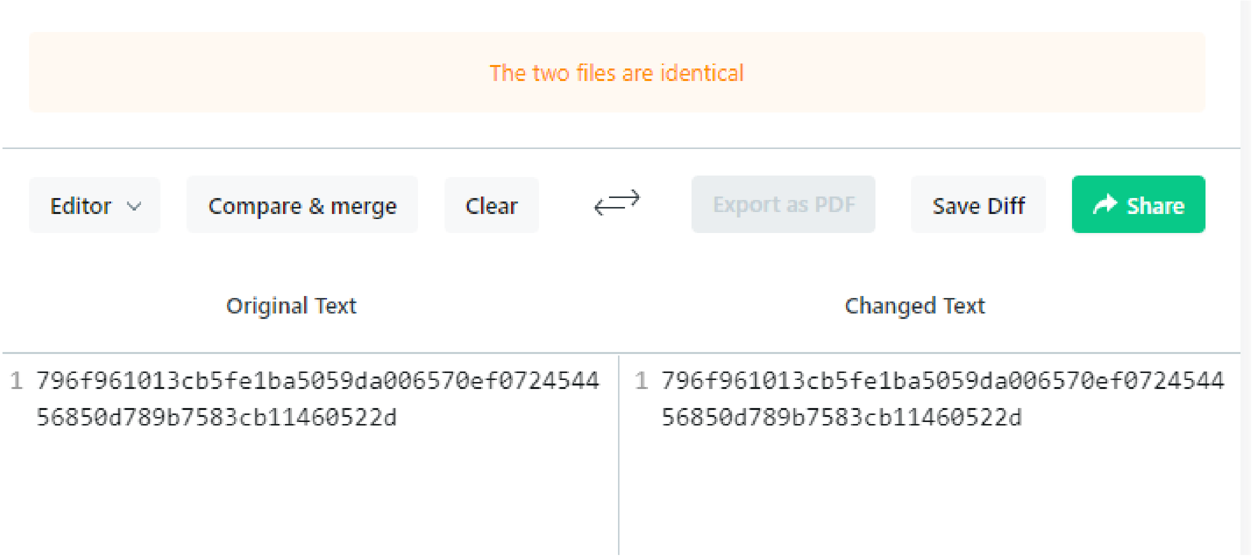
- 1 Removal + 1 Addition

1 f39b01ee7e8b8d8232b975e6652d33b2	1 f56dc93c84c6f58bef069d06fc65ec0e

Original Text	Changed Text
1 f39b01ee7e8b8d8232b975e6652d33b2	1 f56dc93c84c6f58bef069d06fc65ec0e

Using https://www.diffchecker.com/, we can compare the SHA256 hashes

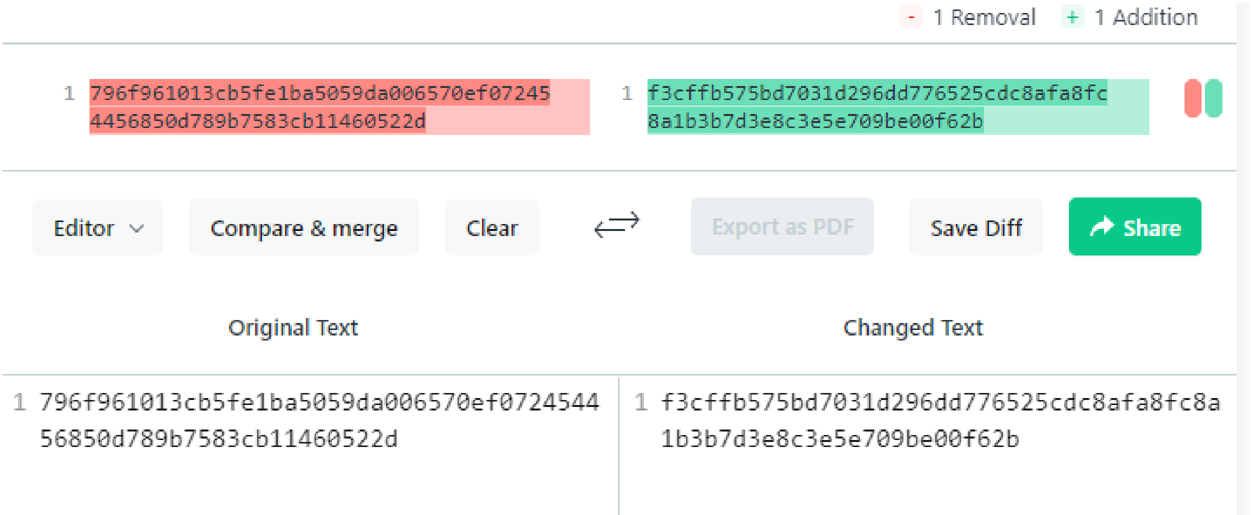
Wordlist1.txt and wordlist2.txt



```
1 796f961013cb5fe1ba5059da006570ef0724544
  56850d789b7583cb11460522d
```

```
1 796f961013cb5fe1ba5059da006570ef0724544
  56850d789b7583cb11460522d
```

Which are the same, then comparing them to wordlist3.txt yields:



```
1 796f961013cb5fe1ba5059da006570ef07245
  4456850d789b7583cb11460522d
```

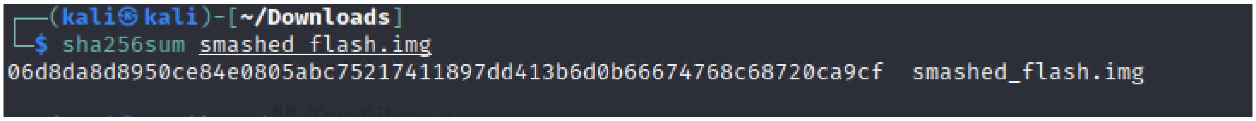
```
1 f3cffb575bd7031d296dd776525cdc8afa8fc
  8a1b3b7d3e8c3e5e709be00f62b
```

```
1 796f961013cb5fe1ba5059da006570ef0724544
  56850d789b7583cb11460522d
```

```
1 f3cffb575bd7031d296dd776525cdc8afa8fc8a
  1b3b7d3e8c3e5e709be00f62b
```

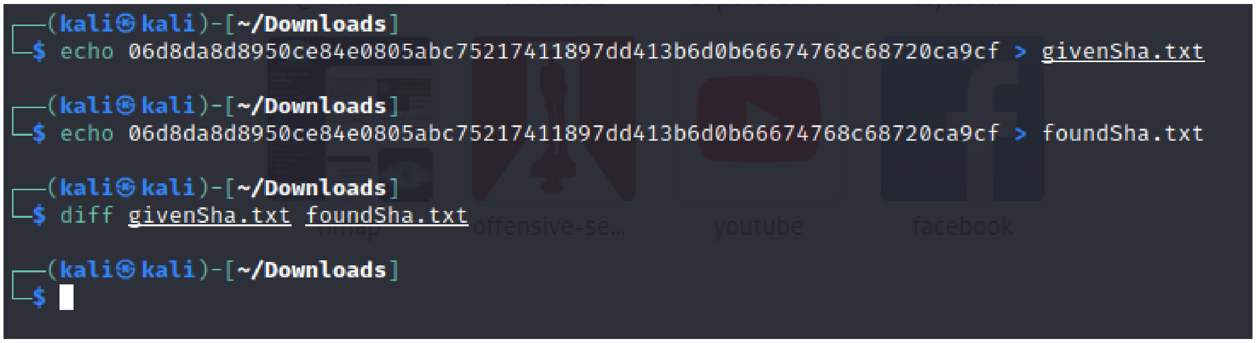
Therefore, using the SHA256 and MD5 hashes, we can determine that the files wordlist1.txt and wordlist2.txt are the same file.

3.1
To get the hash of the smashed_flash.img, I run `sha256sum smashed_flash.img`



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sha256sum smashed_flash.img
06d8da8d8950ce84e0805abc75217411897dd413b6d0b66674768c68720ca9cf  smashed_flash.img
```

Now i can take this output and send it to a .txt and send the given hash to another .txt and run the `diff` command to make sure that they are the same

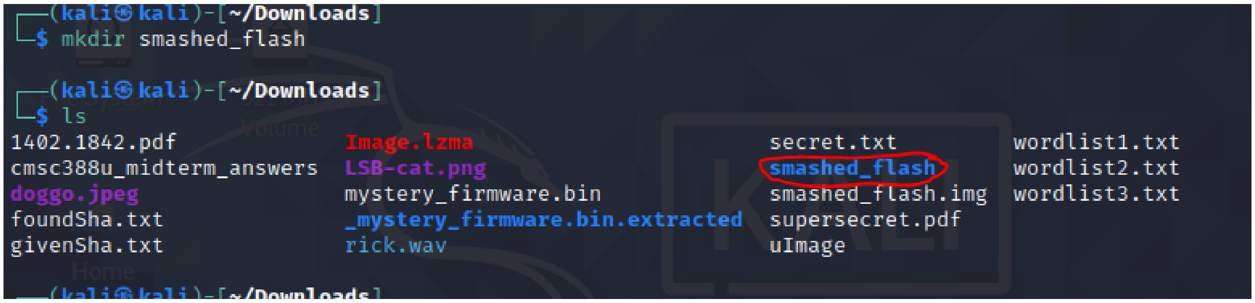


```
┌──(kali㉿kali)-[~/Downloads]
└─$ echo 06d8da8d8950ce84e0805abc75217411897dd413b6d0b66674768c68720ca9cf > givenSha.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ echo 06d8da8d8950ce84e0805abc75217411897dd413b6d0b66674768c68720ca9cf > foundSha.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ diff givenSha.txt foundSha.txt

┌──(kali㉿kali)-[~/Downloads]
└─$ █
```

No output means that the files are the same.

3.2

To get the flag in the smased_flash.img, I first need to `mount` the image. To do this, I made a directory by running `mkdir smashed_flash`



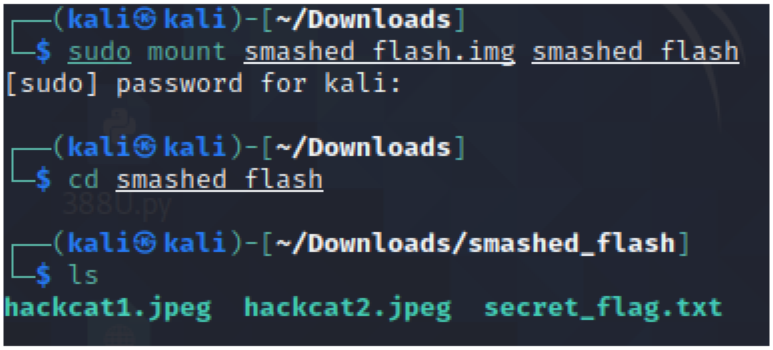
```
┌──(kali㉿kali)-[~/Downloads]
└─$ mkdir smashed_flash

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
1402.1842.pdf              Image.lzma                         secret.txt         wordlist1.txt
cmsc388u_midterm_answers   LSB-cat.png                        smashed_flash      wordlist2.txt
doggo.jpeg                 mystery_firmware.bin               smashed_flash.img  wordlist3.txt
foundSha.txt               _mystery_firmware.bin.extracted    supersecret.pdf
givenSha.txt               rick.wav                           uImage

┌──(kali㉿kali)-[~/Downloads]
```

Next, I made sure that the directory was actually created, which I circled above.

The next step I need to take is to use `mount.` The command needs root privileges, so it needs to have sudo in front of it.

`sudo mount smashed_flash.img smashed_flash`

This should fill up the directory smashed_flash, which I then cd into and did ls.

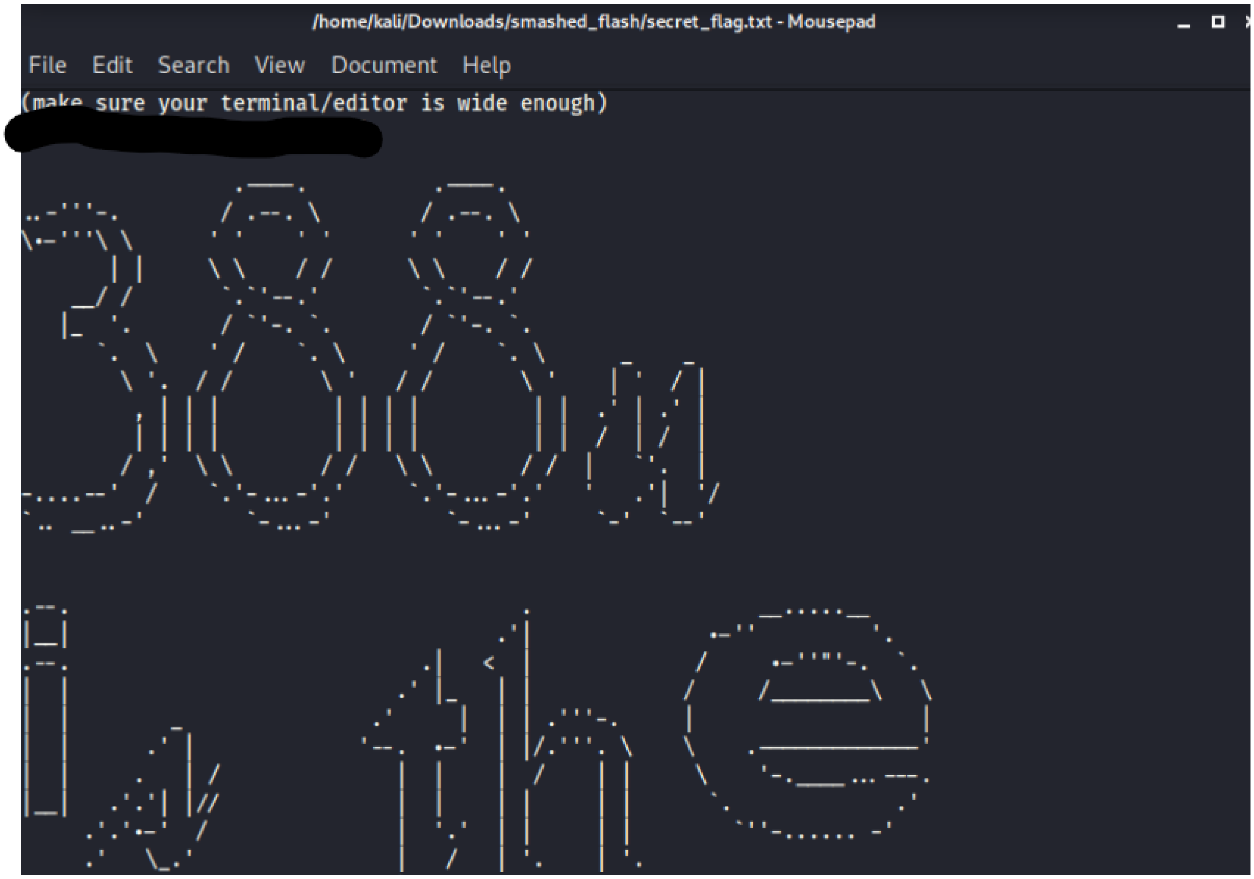


```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo mount smashed_flash.img smashed_flash
[sudo] password for kali:

┌──(kali㉿kali)-[~/Downloads]
└─$ cd smashed_flash

┌──(kali㉿kali)-[~/Downloads/smashed_flash]
└─$ ls
hackcat1.jpeg  hackcat2.jpeg  secret_flag.txt
```

There are 2 .jpeg files and one .txt file. The two .jpeg files consist of

security question: "what was the name of your childhood pet?"
Mr. Cat:
I'm in

Which while they are cool, is not what we are looking for. However, the txt file may be fruitful. Opening it up in a text file, we see:


/home/kali/Downloads/smashed_flash/secret_flag.txt - Mousepad
File
Edit
Search
View
Document
Help

```
(make sure your terminal/editor is wide enough)
[redacted]
```