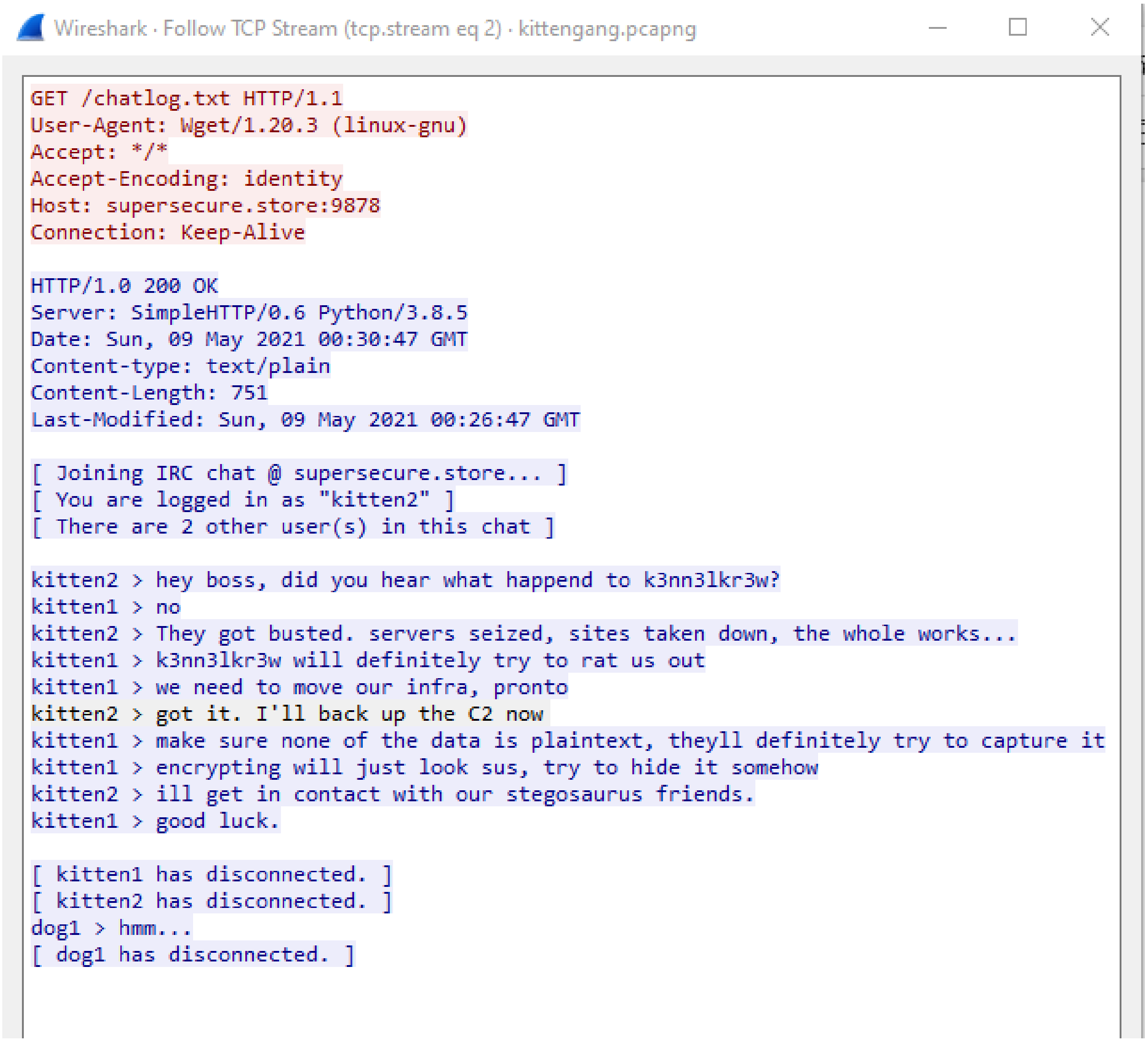
Part 1

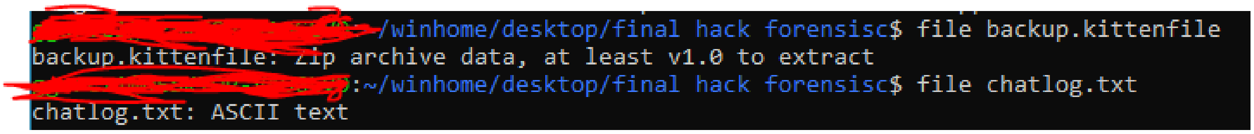
For the first part, I followed the TCP stream
I found this, which appears to be a chat log between two users, kitten2 and kitten1


Wireshark · Follow TCP Stream (tcp.stream eq 2) · kittengang.pcapng

```
GET /chatlog.txt HTTP/1.1
User-Agent: Wget/1.20.3 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: supersecure.store:9878
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.5
Date: Sun, 09 May 2021 00:30:47 GMT
Content-type: text/plain
Content-Length: 751
Last-Modified: Sun, 09 May 2021 00:26:47 GMT

[ Joining IRC chat @ supersecure.store... ]
[ You are logged in as "kitten2" ]
[ There are 2 other user(s) in this chat ]

kitten2 > hey boss, did you hear what happend to k3nn3lkr3w?
kitten1 > no
kitten2 > They got busted. servers seized, sites taken down, the whole works...
kitten1 > k3nn3lkr3w will definitely try to rat us out
kitten1 > we need to move our infra, pronto
kitten2 > got it. I'll back up the C2 now
kitten1 > make sure none of the data is plaintext, theyll definitely try to capture it
kitten1 > encrypting will just look sus, try to hide it somehow
kitten2 > ill get in contact with our stegosaurus friends.
kitten1 > good luck.

[ kitten1 has disconnected. ]
[ kitten2 has disconnected. ]
dog1 > hmm...
[ dog1 has disconnected. ]
```

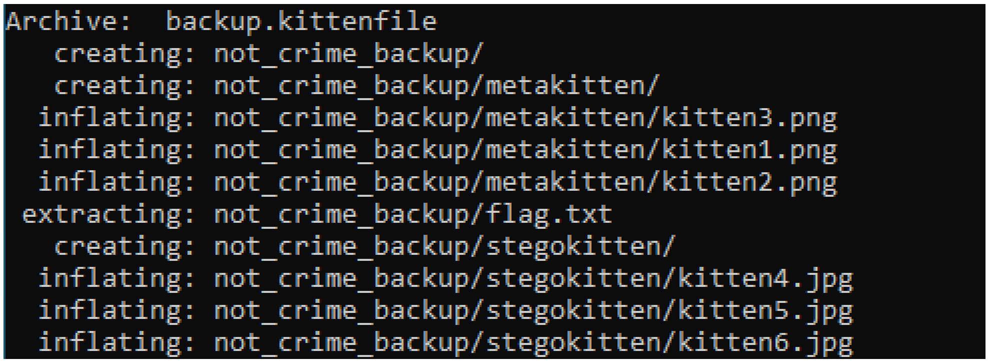
In the chat, they decide to hide the data in plain text as encrypting it will look suspicious. They mention “ill get in contact with our stegosaurus friends”, which may mean they are hiding it in a steganographic manner.

I followed the HTTP stream and found two files of interest which I then ran the `file` command on



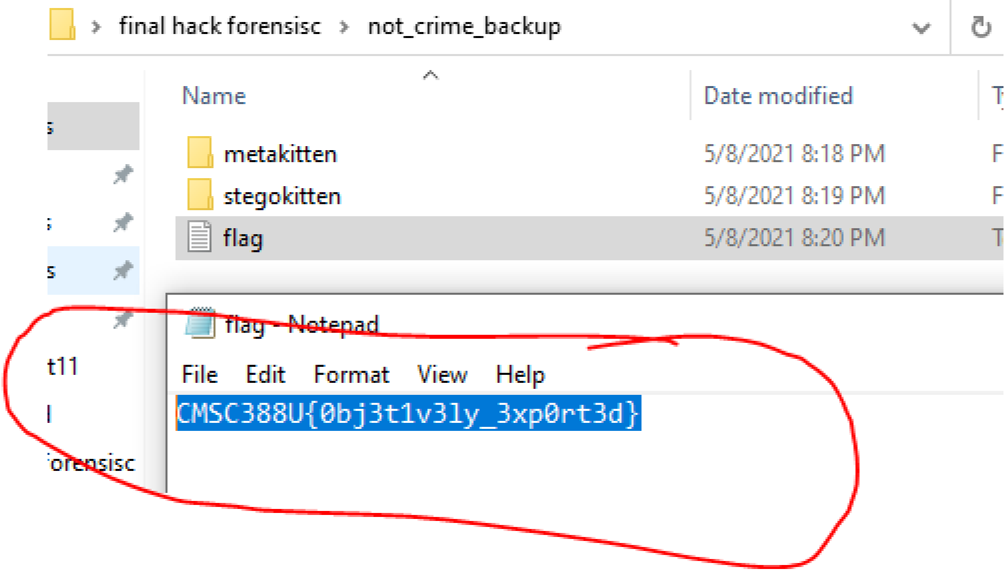
```
[redacted]/winhome/desktop/final hack forensisc$ file backup.kittenfile
backup.kittenfile: zip archive data, at least v1.0 to extract
[redacted]:~/winhome/desktop/final hack forensisc$ file chatlog.txt
chatlog.txt: ASCII text
```

backup.kittenfile is zipped, so unzipped it



```
Archive:  backup.kittenfile
   creating: not_crime_backup/
   creating: not_crime_backup/metakitten/
  inflating: not_crime_backup/metakitten/kitten3.png
  inflating: not_crime_backup/metakitten/kitten1.png
  inflating: not_crime_backup/metakitten/kitten2.png
 extracting: not_crime_backup/flag.txt
   creating: not_crime_backup/stegokitten/
  inflating: not_crime_backup/stegokitten/kitten4.jpg
  inflating: not_crime_backup/stegokitten/kitten5.jpg
  inflating: not_crime_backup/stegokitten/kitten6.jpg
```

This resulted in a directory "not_crime_backup" being created. Entering this directory we can see two folders and one text file titled flag.



final hack forensisc › not_crime_backup
t11
orensisc
flag - Notepad
File Edit Format View Help

Name	Date modified	T
metakitten	5/8/2021 8:18 PM	F
stegokitten	5/8/2021 8:19 PM	F
flag	5/8/2021 8:20 PM	T

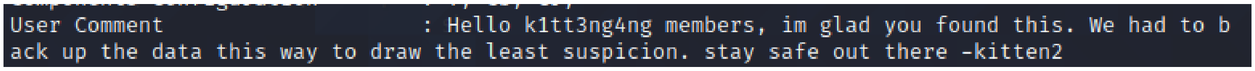
```
CMSC388U{0bj3t1v3ly_3xp0rt3d}
```

The flag is `CMSC388U{0bj3t1v3ly_3xp0rt3d}`

Part 2

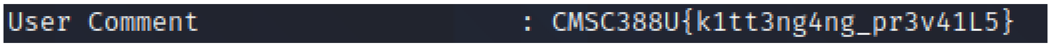
The second flag is noted to be located in the 'metakitten' folder. Looking in this folder, there are 3 images with .png extensions. Using the `file` command on each of these confirm that they are in fact all png images. I tried to use `steghide` but the file format was not supported, so i moved to the `exiftool` command.

The file kitten1.png has user content:



```
Components Configuration        : Y, Cb, Cr,
User Comment                    : Hello k1tt3ng4ng members, im glad you found this. We had to b
ack up the data this way to draw the least suspicion. stay safe out there -kitten2
```

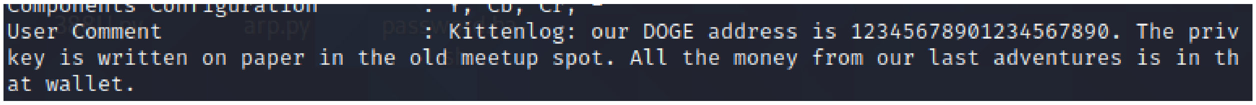
The file kitten2.png has user content:



```
User Comment                    : CMSC388U{k1tt3ng4ng_pr3v41L5}
```

Thus the flag is `CMSC388U{k1tt3ng4ng_pr3v41L5}`

The file kitten3.png has user content:



```
Components Configuration        : Y, Cb, Cr, -
User Comment                    : Kittenlog: our DOGE address is 12345678901234567890. The priv
key is written on paper in the old meetup spot. All the money from our last adventures is in th
at wallet.
```

Part 3

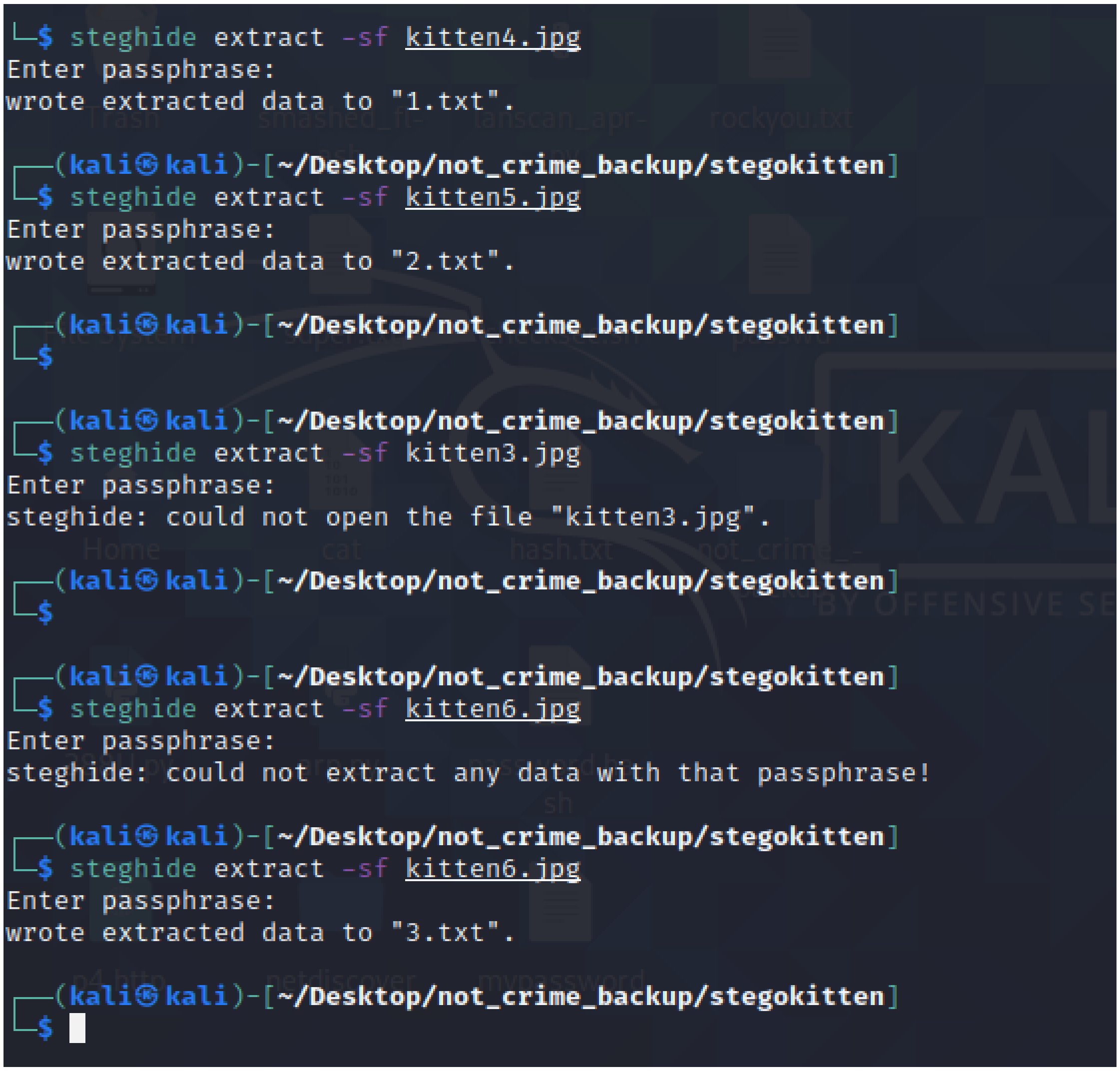
The second flag is noted to be located in the stegokitten. Looking in this folder, there are 3 images with .jpg extensions. Using the `file` command on each of these confirm that they are in fact all png images.

Using the command

```
steghide extract -sf kitten5.jpg
```

And the password as

```
K1tt3ng4ng
```



```
└─$ steghide extract -sf kitten4.jpg
Enter passphrase:
wrote extracted data to "1.txt".

┌──(kali㉿kali)-[~/Desktop/not_crime_backup/stegokitten]
└─$ steghide extract -sf kitten5.jpg
Enter passphrase:
wrote extracted data to "2.txt".

┌──(kali㉿kali)-[~/Desktop/not_crime_backup/stegokitten]
└─$ 

┌──(kali㉿kali)-[~/Desktop/not_crime_backup/stegokitten]
└─$ steghide extract -sf kitten3.jpg
Enter passphrase:
steghide: could not open the file "kitten3.jpg".

┌──(kali㉿kali)-[~/Desktop/not_crime_backup/stegokitten]
└─$ 

┌──(kali㉿kali)-[~/Desktop/not_crime_backup/stegokitten]
└─$ steghide extract -sf kitten6.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!

┌──(kali㉿kali)-[~/Desktop/not_crime_backup/stegokitten]
└─$ steghide extract -sf kitten6.jpg
Enter passphrase:
wrote extracted data to "3.txt".

┌──(kali㉿kali)-[~/Desktop/not_crime_backup/stegokitten]
└─$ 
```

We get 3 text files containing:

```
k1tt3ng4ng:
This is yuor leader, kitten1.

k3nn3lkr3w recently got busted so we're backing up all our data,
itll be hidden in images where no one will suspect.

When everything blows over, we're going to meet on ever second
thursday of the month, at the old meetup.

k1tt3ng4ng prevails!

-kitten1
```

And

It turns out there wasnt anything important to back up on the servers
-kitten2

```
                            ___......__             _
                        _.-'          ~-_       _.=a~~-_
--=====-.-.-_----------~   .--.      _    -.__.-~ ( ___===>
              '''--...__  (    \ \\\ { )      _.-~
                        =_ ~_  \\-~~~//~~~~-=-~
                         |-=-~_ \\   \\
                         |_/   =. )   ~}
                         |}      ||
                        //       ||
                      _//        {{
                   '='~'          \\_   =
                                   ~~'
```

```
                         .       .
                        / `.   .' \
                .---.  <    > <    >  .---.
                |    \  \ - ~ ~ - /  /    |
                 ~-..-~             ~-..-~
             \~~~\.'                    `./~~~/
   .-~~^-.    \__/                        \__/
 .'  O    \     /               /       \  \
(_____,    `._.'               |         }  \/~~~/
 `----.          /       }     |        /    \__/
       `-.      |       /      |       /      `. ,~~|
           ~-.__|      /_ - ~ ^|      /- _      `..-'   f: f:
                |     /        |     /     ~-.     `-. _||_||_
                |_____|        |_____|         ~ - . _ _ _ _ _>
```

And

```
               __
              / _)
     _.----._/ /
    /         /
```

```
 __/ (  | (  |
/__.-'|_|--|_|

CMSC388U{d1n0s4ur5_am0gu5}
```

Therefore the flag is `CMSC388U{d1n0s4ur5_am0gu5}`