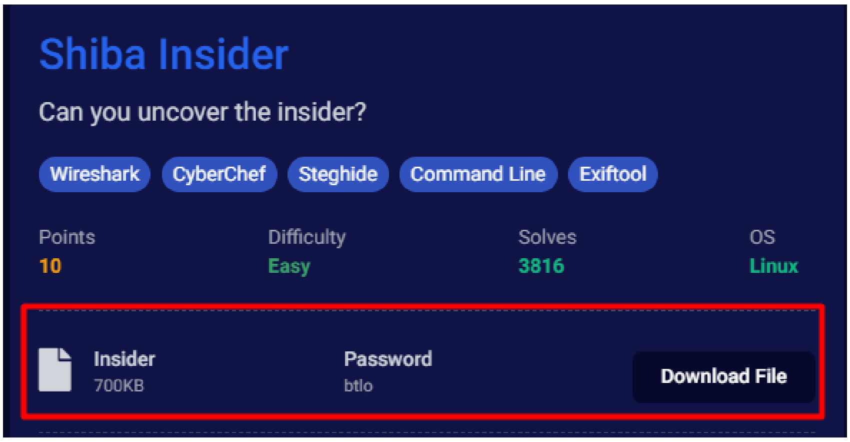
Reference: https://blueteamlabs.online/home/challenge/shiba-insider-5b48123711

Download the zip file from here and start the investigation.



Shiba Insider

Can you uncover the insider?

Wireshark CyberChef Steghide Command Line Exiftool

Points: 10
Difficulty: Easy
Solves: 3816
OS: Linux

Insider
700KB

Password
btlo

Tools used:

1. Wireshark
2. Cyberchef
3. Exiftool
4. Steghide

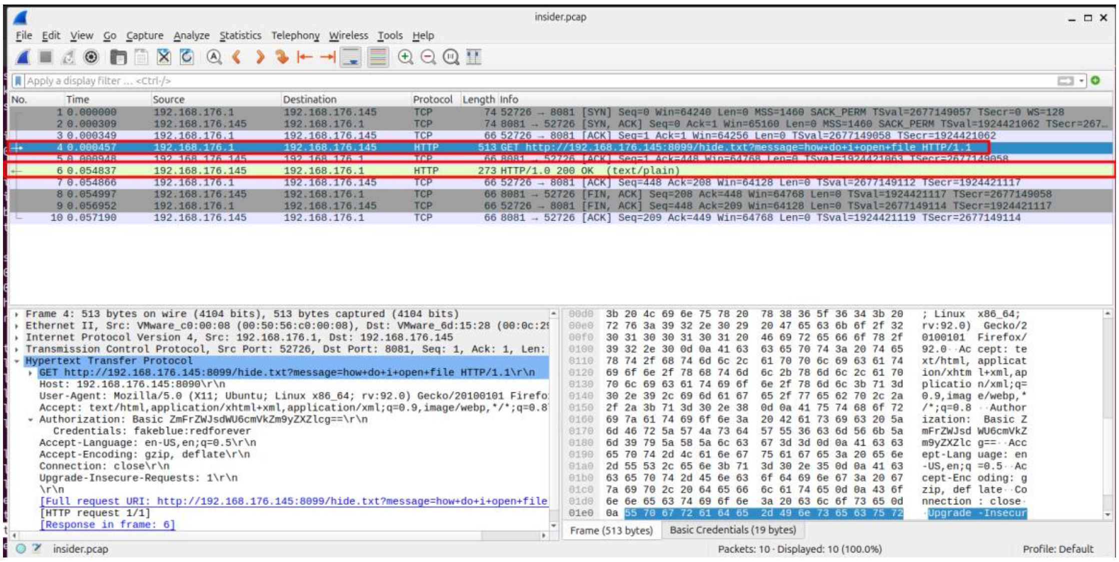
**Install exiftool in linux**

sudo apt install libimage-exiftool-perl

**Install steghide in linux**

sudo apt-get install steghide -y

Wireshark view



insider.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Frame (513 bytes)
Basic Credentials (19 bytes)
insider.pcap
Packets: 10 · Displayed: 10 (100.0%)
Profile: Default

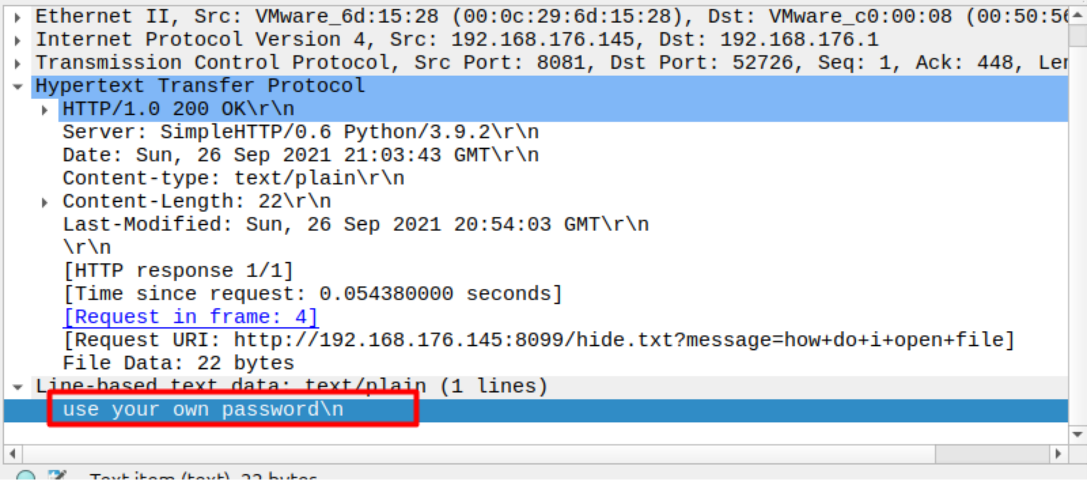
```
No.  Time       Source           Destination      Protocol Length Info
   1 0.000000   192.168.176.1    192.168.176.145  TCP        74 52726 → 8081 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2677149057 TSecr=0 WS=128
   2 0.000309   192.168.176.145  192.168.176.1    TCP        74 8081 → 52726 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1924421062 TSecr=267…
   3 0.000349   192.168.176.1    192.168.176.145  TCP        66 52726 → 8081 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2677149058 TSecr=1924421062
   4 0.000457   192.168.176.1    192.168.176.145  HTTP      513 GET http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file HTTP/1.1
   5 0.000948   192.168.176.145  192.168.176.1    TCP        66 8081 → 52726 [ACK] Seq=1 Ack=448 Win=64768 Len=0 TSval=1924421063 TSecr=2677149058
   6 0.054837   192.168.176.145  192.168.176.1    HTTP      273 HTTP/1.0 200 OK  (text/plain)
   7 0.054866   192.168.176.1    192.168.176.145  TCP        66 52726 → 8081 [ACK] Seq=448 Ack=208 Win=64128 Len=0 TSval=2677149112 TSecr=1924421117
   8 0.054997   192.168.176.145  192.168.176.1    TCP        66 8081 → 52726 [FIN, ACK] Seq=208 Ack=448 Win=64768 Len=0 TSval=1924421117 TSecr=2677149058
   9 0.056952   192.168.176.1    192.168.176.145  TCP        66 52726 → 8081 [FIN, ACK] Seq=448 Ack=209 Win=64128 Len=0 TSval=2677149114 TSecr=1924421117
  10 0.057190   192.168.176.145  192.168.176.1    TCP        66 8081 → 52726 [ACK] Seq=209 Ack=449 Win=64768 Len=0 TSval=1924421119 TSecr=2677149114
```

```
▸ Frame 4: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits)
▸ Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_6d:15:28 (00:0c:29
▸ Internet Protocol Version 4, Src: 192.168.176.1, Dst: 192.168.176.145
▸ Transmission Control Protocol, Src Port: 52726, Dst Port: 8081, Seq: 1, Ack: 1, Len:
▾ Hypertext Transfer Protocol
  ▸ GET http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file HTTP/1.1\r\n
    Host: 192.168.176.145:8090\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefo
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
  ▾ Authorization: Basic ZmFrZWJsdWU6cmVkZm9yZXZlcg==\r\n
      Credentials: fakeblue:redforever
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: close\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file
    [HTTP request 1/1]
    [Response in frame: 6]
```

```
00d0  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux  x86_64;
00e0  72 76 3a 39 32 2e 30 29  20 47 65 63 6b 6f 2f 32   rv:92.0)  Gecko/2
00f0  30 31 30 30 31 30 31 20  46 69 72 65 66 6f 78 2f   0100101  Firefox/
0100  39 32 2e 30 0d 0a 41 63  63 65 70 74 3a 20 74 65   92.0··Ac cept: te
0110  78 74 2f 68 74 6d 6c 2c  61 70 70 6c 69 63 61 74   xt/html, applicat
0120  69 6f 6e 2f 78 68 74 6d  6c 2b 78 6d 6c 2c 61 70   ion/xhtm l+xml,ap
0130  70 6c 69 63 61 74 69 6f  6e 2f 78 6d 6c 3b 71 3d   plicatio n/xml;q=
0140  30 2e 39 2c 69 6d 61 67  65 2f 77 65 62 70 2c 2a   0.9,imag e/webp,*
0150  2f 2a 3b 71 3d 30 2e 38  0d 0a 41 75 74 68 6f 72   /*;q=0.8 ··Author
0160  69 7a 61 74 69 6f 6e 3a  20 42 61 73 69 63 20 5a   ization:  Basic Z
0170  6d 46 72 5a 57 4a 73 64  57 55 36 63 6d 56 6b 5a   mFrZWJsd WU6cmVkZ
0180  6d 39 79 5a 58 5a 6c 63  67 3d 3d 0d 0a 41 63 63   m9yZXZlc g==··Acc
0190  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
01a0  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d 0a 41 63   -US,en;q =0.5··Ac
01b0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
01c0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 43 6f   zip, def late··Co
01d0  6e 6e 65 63 74 69 6f 6e  3a 20 63 6c 6f 73 65 0d   nnection : close·
01e0  0a 55 70 67 72 61 64 65  2d 49 6e 73 65 63 75 72   ·Upgrade -Insecur
```

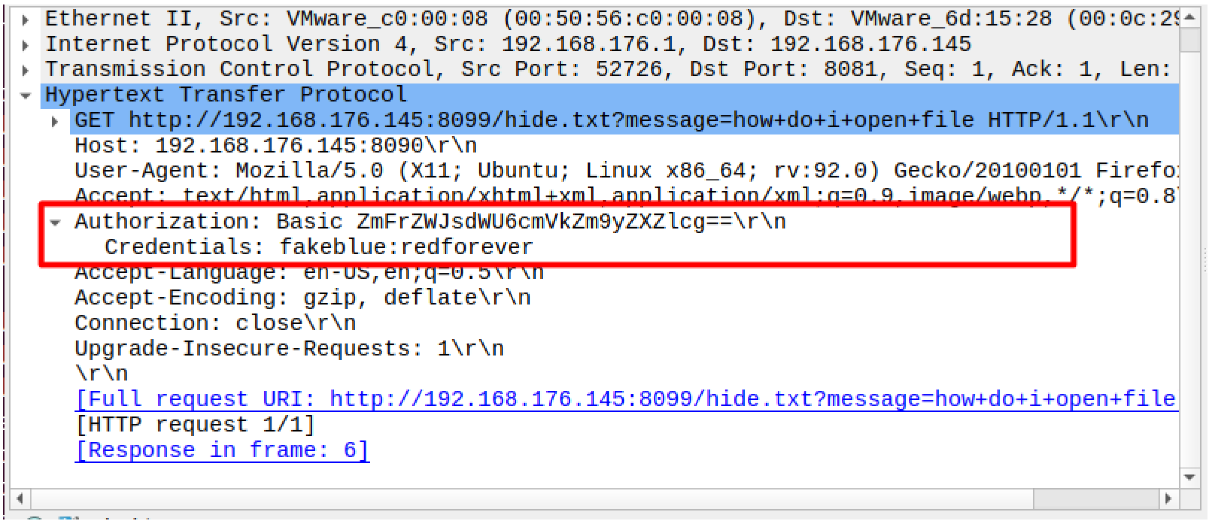
-> Is request <- is response

Response message is: use your own password



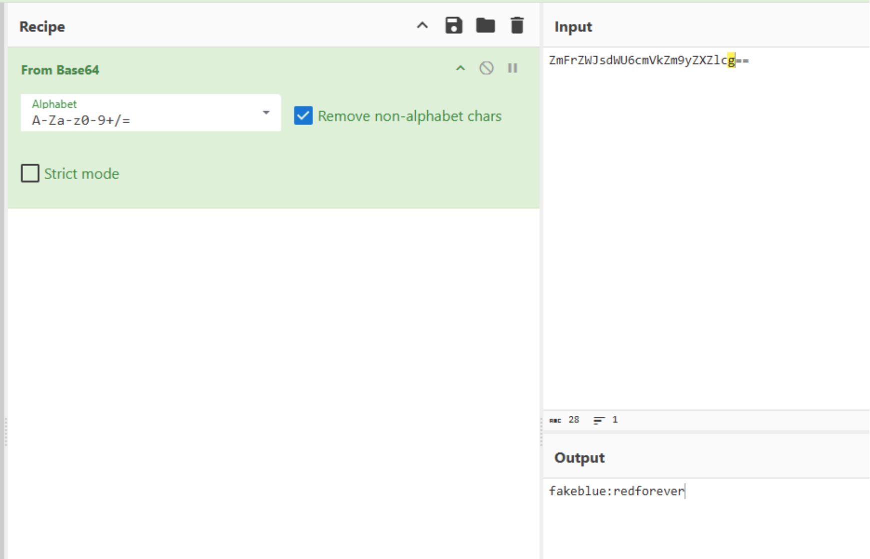
```
Ethernet II, Src: VMware_6d:15:28 (00:0c:29:6d:15:28), Dst: VMware_c0:00:08 (00:50:56
Internet Protocol Version 4, Src: 192.168.176.145, Dst: 192.168.176.1
Transmission Control Protocol, Src Port: 8081, Dst Port: 52726, Seq: 1, Ack: 448, Ler
Hypertext Transfer Protocol
  HTTP/1.0 200 OK\r\n
  Server: SimpleHTTP/0.6 Python/3.9.2\r\n
  Date: Sun, 26 Sep 2021 21:03:43 GMT\r\n
  Content-type: text/plain\r\n
  Content-Length: 22\r\n
  Last-Modified: Sun, 26 Sep 2021 20:54:03 GMT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.054380000 seconds]
  [Request in frame: 4]
  [Request URI: http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file]
  File Data: 22 bytes
Line-based text data: text/plain (1 lines)
  use your own password\n
Text item (text), 22 bytes
```

Password of zip file



```
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_6d:15:28 (00:0c:2
Internet Protocol Version 4, Src: 192.168.176.1, Dst: 192.168.176.145
Transmission Control Protocol, Src Port: 52726, Dst Port: 8081, Seq: 1, Ack: 1, Len:
Hypertext Transfer Protocol
  GET http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file HTTP/1.1\r\n
  Host: 192.168.176.145:8090\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefo
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
  Authorization: Basic ZmFrZWJsdWU6cmVkZm9yZXZlcg==\r\n
    Credentials: fakeblue:redforever
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: close\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file
  [HTTP request 1/1]
  [Response in frame: 6]
```

Also, from cyberchef



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

Input

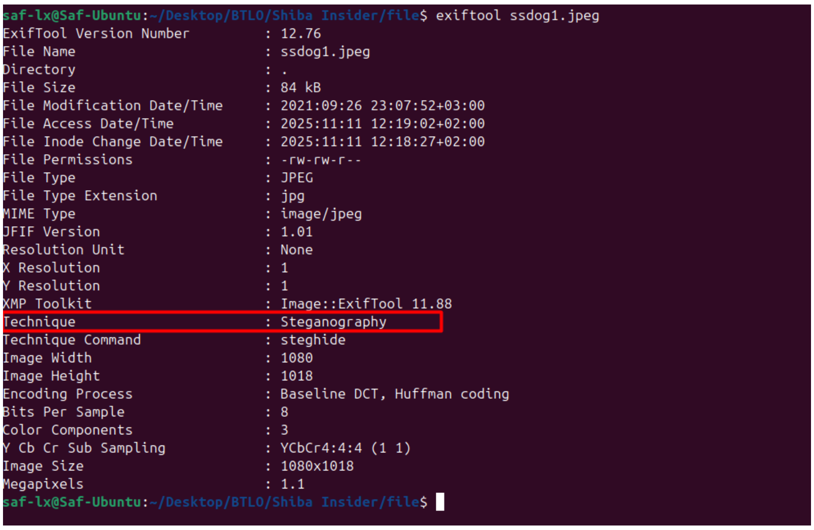
```
ZmFrZWJsdWU6cmVkZm9yZXZlcg==
```

28 1

Output

```
fakeblue:redforever
```

Here user is fakeblue and password is redforever. Open the zip file using password and then extract the metadata.

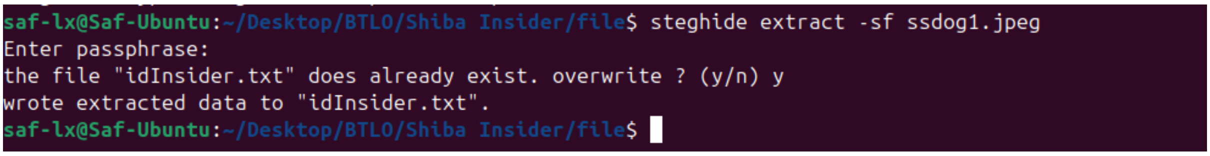


```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Shiba Insider/file$ exiftool ssdog1.jpeg
ExifTool Version Number         : 12.76
File Name                       : ssdog1.jpeg
Directory                       : .
File Size                       : 84 kB
File Modification Date/Time     : 2021:09:26 23:07:52+03:00
File Access Date/Time           : 2025:11:11 12:19:02+02:00
File Inode Change Date/Time     : 2025:11:11 12:18:27+02:00
File Permissions                : -rw-rw-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
XMP Toolkit                     : Image::ExifTool 11.88
Technique                       : Steganography
Technique Command               : steghide
Image Width                     : 1080
Image Height                    : 1018
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                      : 1080x1018
Megapixels                      : 1.1
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Shiba Insider/file$
```

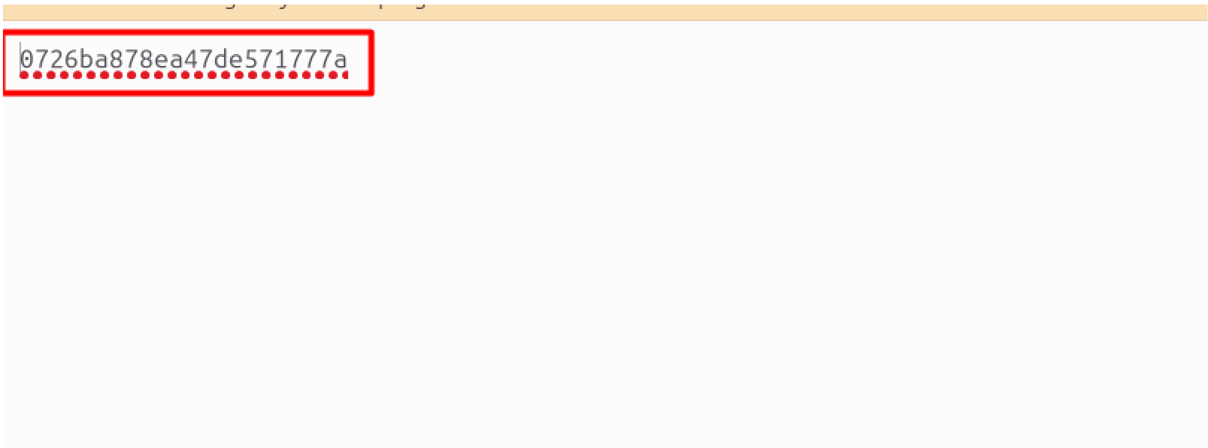
**Steganography** technique has been used to **hide secret information** inside. Usually it looks **normal or harmless**, such as an image, audio file, video, or text. Let's retrieve information of embedded file.

Ssdog1.jpg

Extracting metadata of the image file we can see it extracted the text file idInsider.txt. Let's see what is inside it.

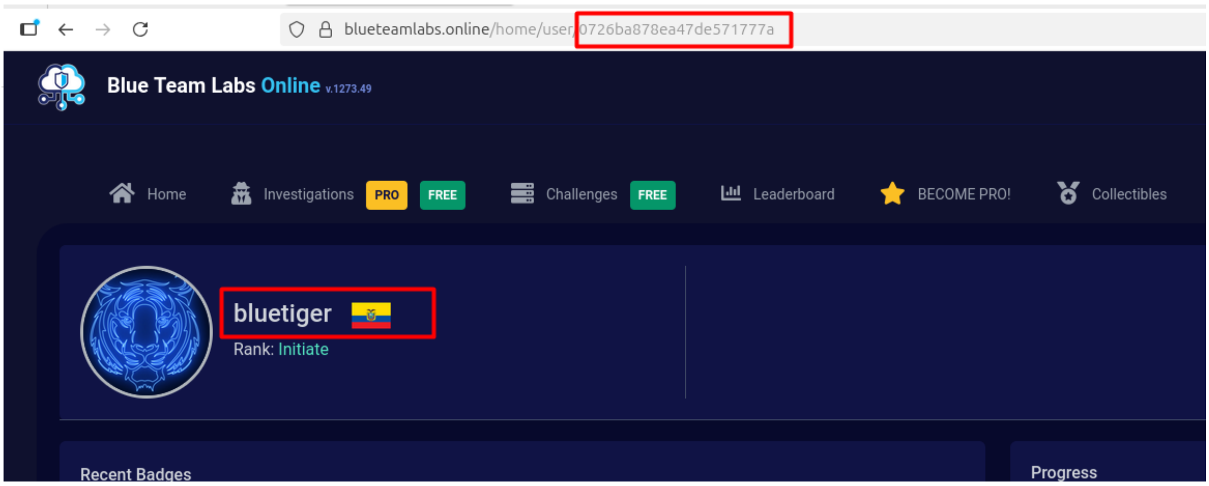


```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Shiba Insider/file$ steghide extract -sf ssdog1.jpeg
Enter passphrase:
the file "idInsider.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "idInsider.txt".
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Shiba Insider/file$
```



0726ba878ea47de571777a

The use ID has been retrieved.



blueteamlabs.online/home/user/0726ba878ea47de571777a

bluetiger

Rank: Initiate

Name of the user.

**Takeaway:**

1. How to use exfitools to extract metadata of file.
2. How to use steghide to extract the hidden information in normal looking file.
3. Know about Steganography technique.