

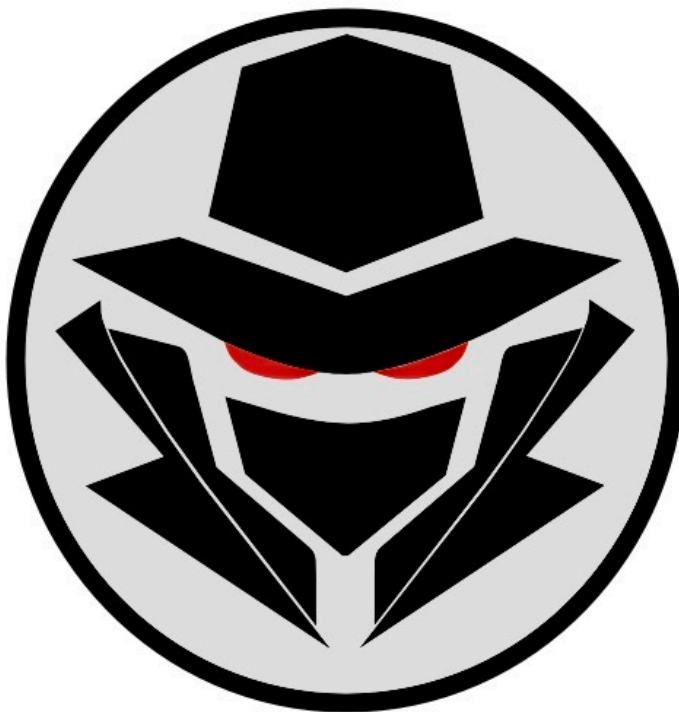
ROT
I might be hidden deep, You need to find me ASAP.

Flag:- HTB{M0naC0h@sBeeNPwn3d}

Category:- EASY, OSINT

Writeup:-

1. We have been given an image in the challenge.



2. We analyze the image's metadata and found two pastebins link.

The screenshot shows the analysis results for the image uploaded on metapicz.com. The image itself is a black and white version of the alien mask from the previous step.

Metadata Fields:

- Camera:** Camera info not found.
- Author and Copyright:** Copyright not found.
- Location:** GPS coordinates not found.
- EXIF:**

ModifyDate	2020:08:22 14:28:33
DateTimeOriginal	2020:08:22 14:28:33
CreateDate	2020:08:22 14:28:33
SubSecTimeOriginal	085
SubSecTimeDigitized	085
- XMP:**

XMPToolkit	XMP Core 5.4.0
ArtworkContentDescription	https://pastebin.com/EFBmzQFk https://pastebin.com/00b4GktP
CreateDate	2020:08:22 14:28:33
ModifyDate	2020:08:22 14:28:33
DateCreated	2020:08:22 14:28:33

ROT

I might be hidden deep, You need to find me ASAP.

3. <https://pastebin.com/EFBmzQFk>

A screenshot of a web browser displaying a Pastebin page. The URL in the address bar is <https://pastebin.com/>. The page header includes the Pastebin logo, navigation links for GO PRO, API, TOOLS, FAQ, and a '+ paste' button. On the right side, there are 'SIGN IN' and 'SIGN UP' buttons. A sidebar on the right lists several other pastes with their titles, languages, and ages. The main content area shows a paste titled 'monacohackhackmonaco@gmail.com' posted by a guest on August 22nd, 2020. The paste content is as follows:

```
1. monacohackhackmonaco@gmail.com
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19. 00110001 00110010 00110111 00101110 00110000 00101110 00110000 00101110 00110001
20.
```

Below the paste, there is a 'RAW Paste Data' section containing the same text. A note at the bottom right of the page states: "We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the [Cookies Policy](#). [OK, I Understand](#)".

4. <https://pastebin.com/00b4GktP>

A screenshot of a web browser displaying a Pastebin page. The URL in the address bar is <https://pastebin.com/00b4GktP>. The page structure is identical to the previous screenshot, featuring the Pastebin logo, navigation links, and a '+ paste' button. The sidebar on the right shows recent pastes. The main content area displays a guest post by 'monacohackhackmonaco' on August 22nd, 2020. The paste content is:

```
1. 01000110 00110011 01101100 01101100 01101111 01010111 01101101 01101111 01001110 01100001 01000011 00110000 00100001
00100001
```

The rest of the page, including the sidebar and cookie notice, is identical to the first screenshot.

ROT
I might be hidden deep, You need to find me ASAP.

5. We got one email/username monacohackhackmonaco@gmail.com and some binary.
6. Putting them through binary to text convertor, we got IP and a Pass.

The screenshot shows a web browser window with the following elements:

- Title Bar:** monacohackhackmonaco@gmail.com - Pastebin.com
- Content Area:** A "Binary to Text Converter | Binary Translator" tool from [rapidtables.com](http://www.rapidtables.com). It has a text input field containing binary code: 00110001 00110010 00110111 00101110 00110000 00101110 00110000 00101110 00110001. Below it is a dropdown for "Character encoding (optional)" set to "ASCII/UTF-8". Buttons for "Convert", "Reset", and "Swap" are present. The converted text "127.0.0.1" is displayed in a large text area. At the bottom are "Copy" and "Save" buttons.
- Right Side:** An advertisement for a "Fiber Laser Cutting Machine" by **bodor**. It features an image of the machine, the text "Economical Model Help Resume Production", and a red button labeled "Inquiry Now".
- Bottom Right:** A "NUMBER CONVERSION" sidebar with a list of options: ASCII,Hex,Binary,Decimal converter; ASCII text to binary converter; ASCII text to hex converter; Base converter; Binary converter; Binary to ASCII text converter; and Binary to decimal converter.

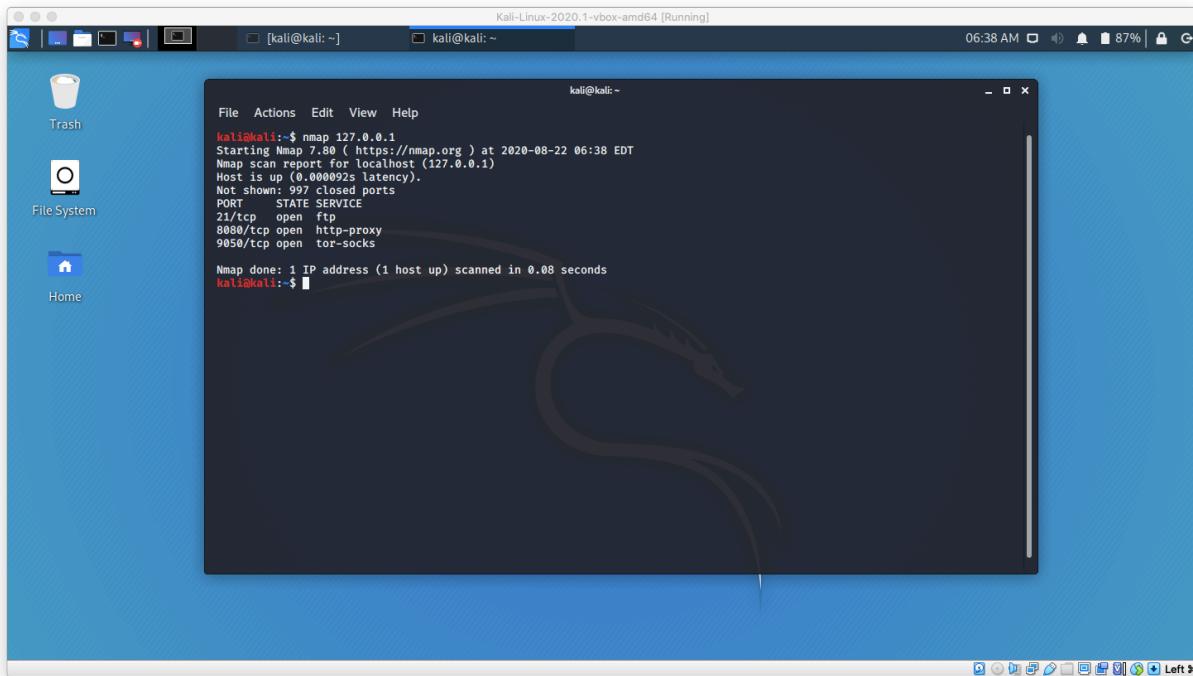
The screenshot shows a web browser window with the following elements:

- Title Bar:** monacohackhackmonaco - Pastebin.com
- Content Area:** A "Binary to Text Converter | Binary Translator" tool from [rapidtables.com](http://www.rapidtables.com). It has a text input field containing binary code: 01000110 00110011 01101100 01101100 01101111 01010111 01101101 01101111 01000110 01100001 01000011 00110000 00100001 00100001. Below it is a dropdown for "Character encoding (optional)" set to "ASCII/UTF-8". Buttons for "Convert", "Reset", and "Swap" are present. The converted text "F3ll0Wm0NAC0!!" is displayed in a large text area. At the bottom are "Copy" and "Save" buttons.
- Right Side:** An advertisement for a "Fiber Laser Cutting Machine" by **bodor**. It features an image of the machine, the text "Economical Model Help Resume Production", and a red button labeled "Inquiry Now".
- Bottom Right:** A "NUMBER CONVERSION" sidebar with a list of options: ASCII,Hex,Binary,Decimal converter; ASCII text to binary converter; ASCII text to hex converter; Base converter; Binary converter; Binary to ASCII text converter; and Binary to decimal converter.

7. IP= 127.0.0.1 (local for now)
- Password= F3ll0Wm0NAC0!!

ROT
I might be hidden deep, You need to find me ASAP.

8. NMAP the IP.

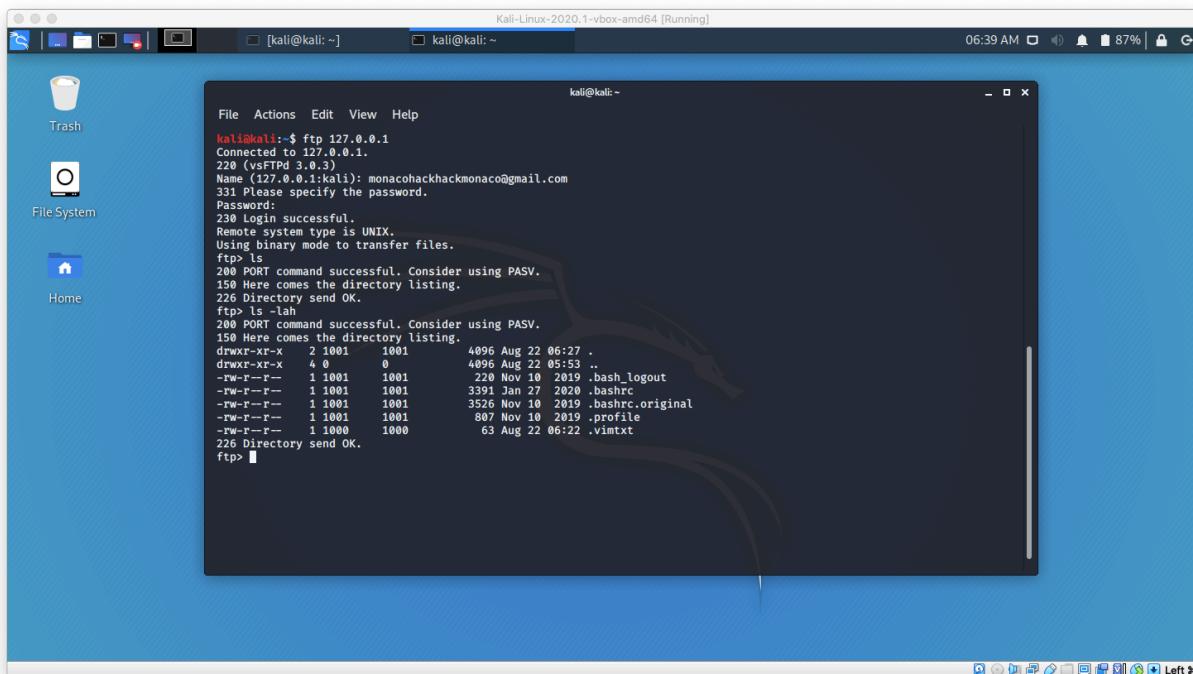


```
Kali-Linux-2020.1-vbox-amd64 [Running]
[ kali@kali: ~ ] [ kali@kali: ~ ]
06:38 AM 87% | Left

File Actions Edit View Help
kali@kali:~$ nmap 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-22 06:38 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000092s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
8080/tcp  open  http-proxy
9050/tcp  open  tor-socks

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
kali@kali:~$
```

9. Got FTP open, Lets Try the Creds as monacohackhackmonaco@gmail.com: F3lloWmoNaC0!!



```
Kali-Linux-2020.1-vbox-amd64 [Running]
[ kali@kali: ~ ] [ kali@kali: ~ ]
06:39 AM 87% | Left

File Actions Edit View Help
kali@kali:~$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.3)
Name (127.0.0.1:kali): monacohackhackmonaco@gmail.com
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -lah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1001   1001  4096 Aug 22 06:27 .
drwxr-xr-x  4  0       0     4096 Aug 22 05:53 ..
-rw-r--r--  1 1001   1001  220 Nov 10 2019 .bash_logout
-rw-r--r--  1 1001   1001  3391 Jan 27 2020 .bashrc
-rw-r--r--  1 1001   1001  3526 Nov 10 2019 .bashrc.original
-rw-r--r--  1 1001   1001  807 Nov 10 2019 .profile
-rw-r--r--  1 1000   1000   63 Aug 22 06:22 .vimtxt
226 Directory send OK.
ftp>
```

ROT
I might be hidden deep, You need to find me ASAP.

10. We are in and got .vimtext as a file in ftp transfer it over to the local machine and cat it.

A screenshot of a Kali Linux desktop environment. In the foreground, a terminal window titled 'kali@kali: ~' shows an FTP session. The user has connected to '127.0.0.1' and transferred a file named '.vimtext'. The terminal output is as follows:

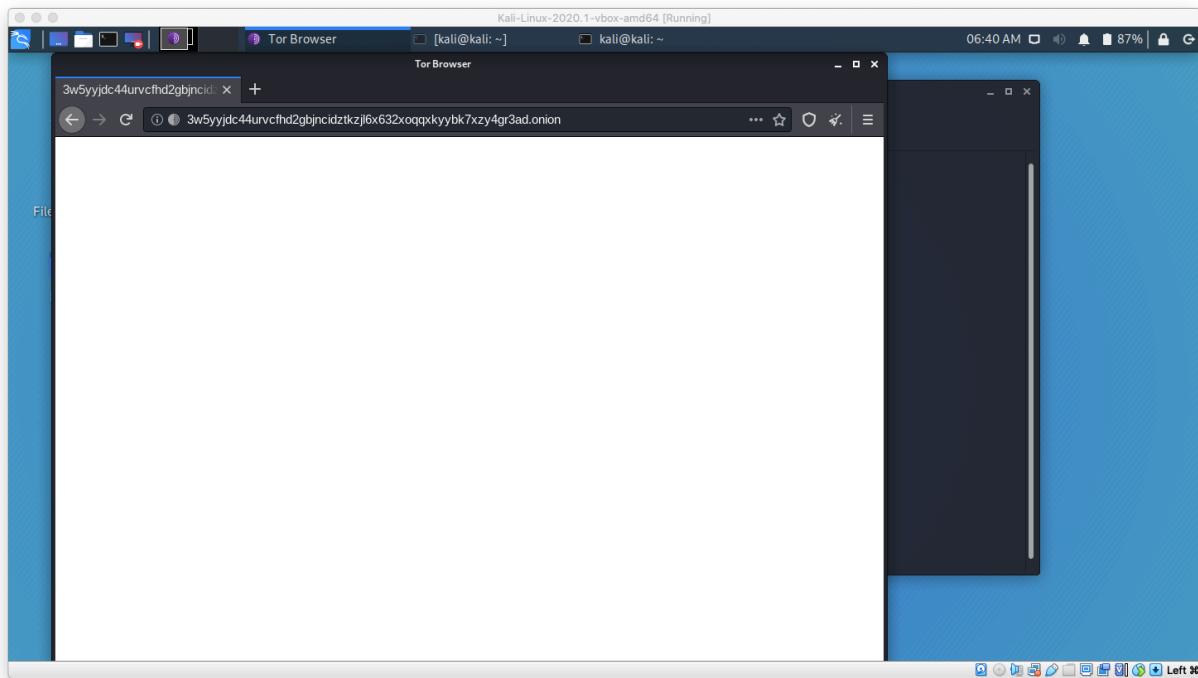
```
kali@kali:~$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.2)
Name (127.0.0.1:kali): monacohackhackmonaco@gmail.com
533 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -lah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1001   1001  4096 Aug 22 06:27 .
drwxr-xr-x  4 0       0       4096 Aug 22 05:53 ..
-rw-r--r--  1 1001   1001   220 Nov 10 2019 .bash_logout
-rw-r--r--  1 1001   1001   336 Jan 21 2020 .bashrc
-rw-r--r--  1 1001   1001   3526 Nov 10 2019 .bashrc.original
-rw-r--r--  1 1001   1001   807 Nov 10 2019 .profile
-rw-r--r--  1 1000   1000   63 Aug 22 06:22 .vimtext
226 Directory send OK.
ftp> get .vimtext
local: .vimtext remote: .vimtext
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .vimtext (63 bytes).
226 Transfer complete.
63 bytes received in 0.00 secs (1.1336 MB/s)
ftp> 
```

A screenshot of a Kali Linux desktop environment. In the foreground, a terminal window titled 'kali@kali: ~' shows the contents of the file '.vimtext' after it was transferred from the previous screen. The terminal output is as follows:

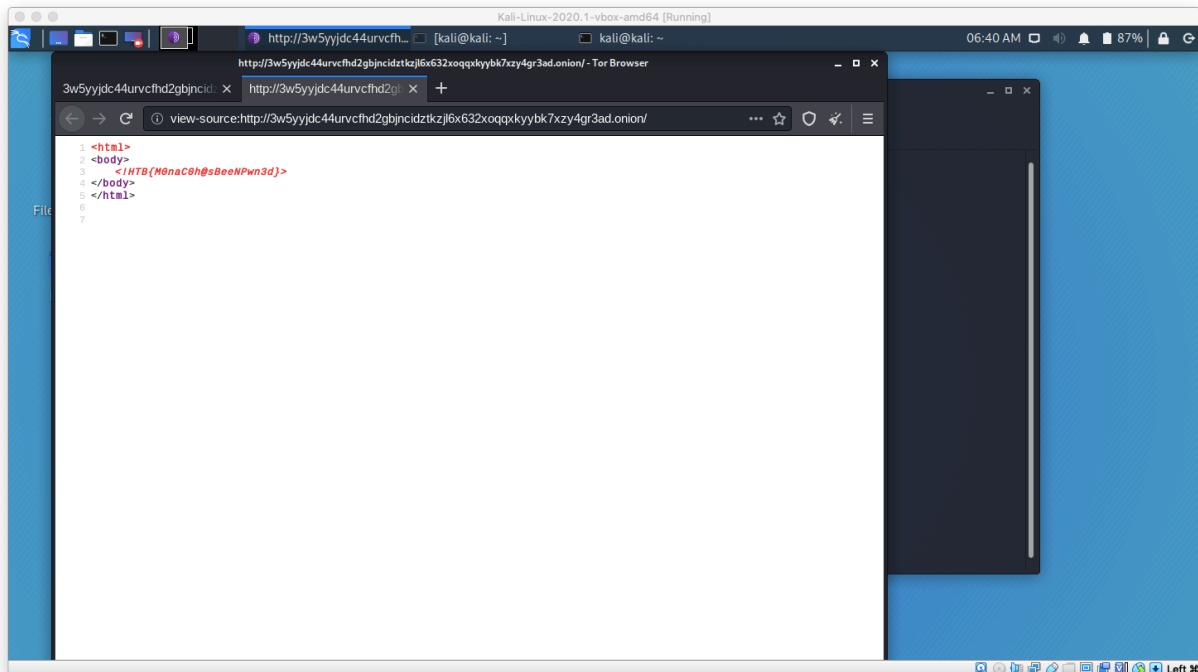
```
kali@kali:~$ cat .vim
.viminfo .vimtext
kali@kali:~$ cat .vimtext
3w5yyjd44urvcfh2gbjnidztkzjl6x632xoqqxkyyb7xzy4gr3ad.onion
kali@kali:~$ 
```

ROT
I might be hidden deep, You need to find me ASAP.

11. We got an ONION url,
<http://3w5yyjdc44urvcfhd2gbjncidztkzjl6x632xoqqxkyyb7xzy4gr3ad.onion/>
Lets bootup the torbrowser and see if we got anything.



12. View Source and we got the flag.



Sources Used for Setup of TOR :- <https://null-byte.wonderhowto.com/how-to/host-your-own-tor-hidden-service-with-custom-onion-address-0180159/>