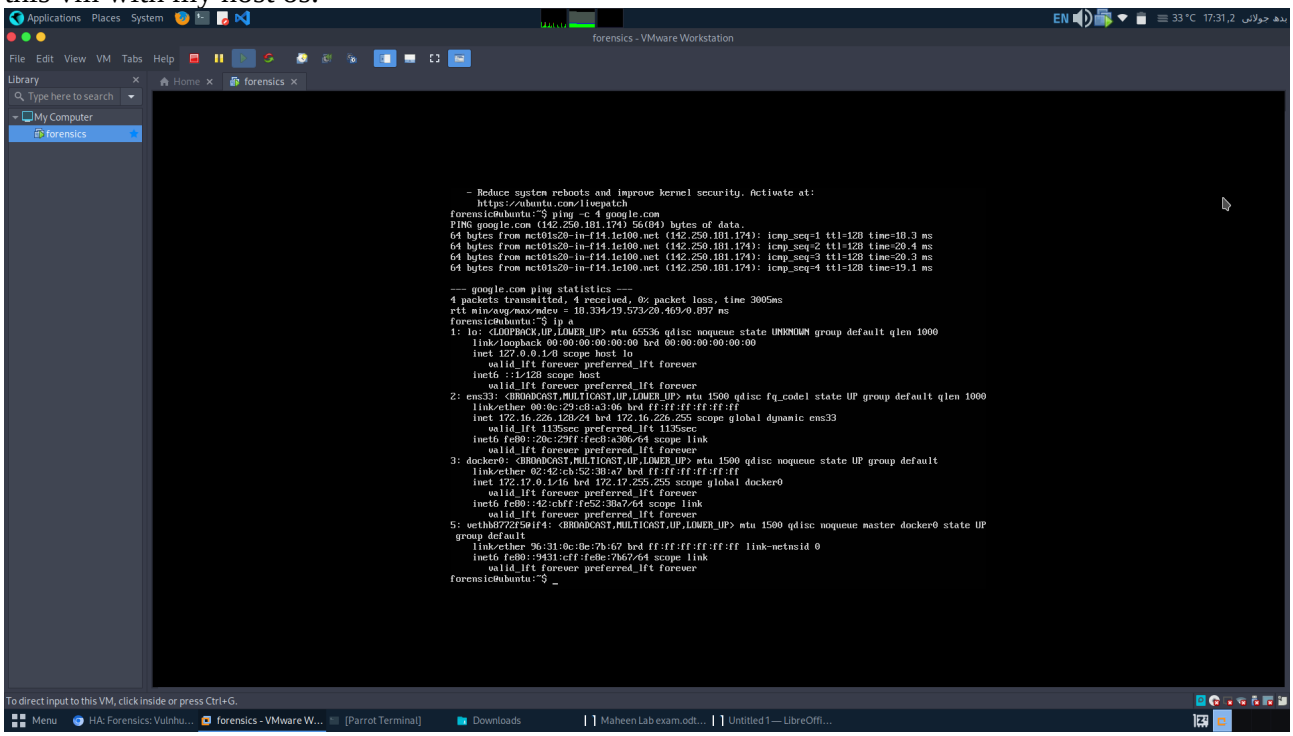
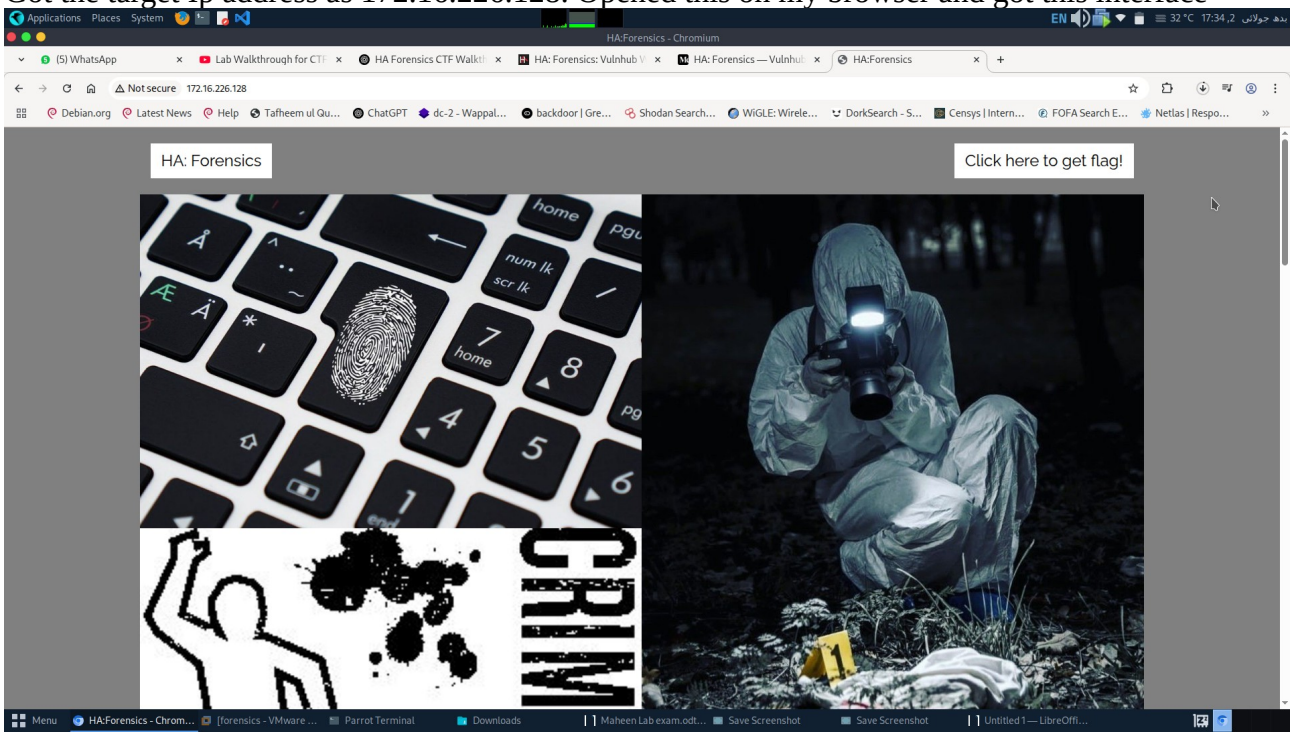
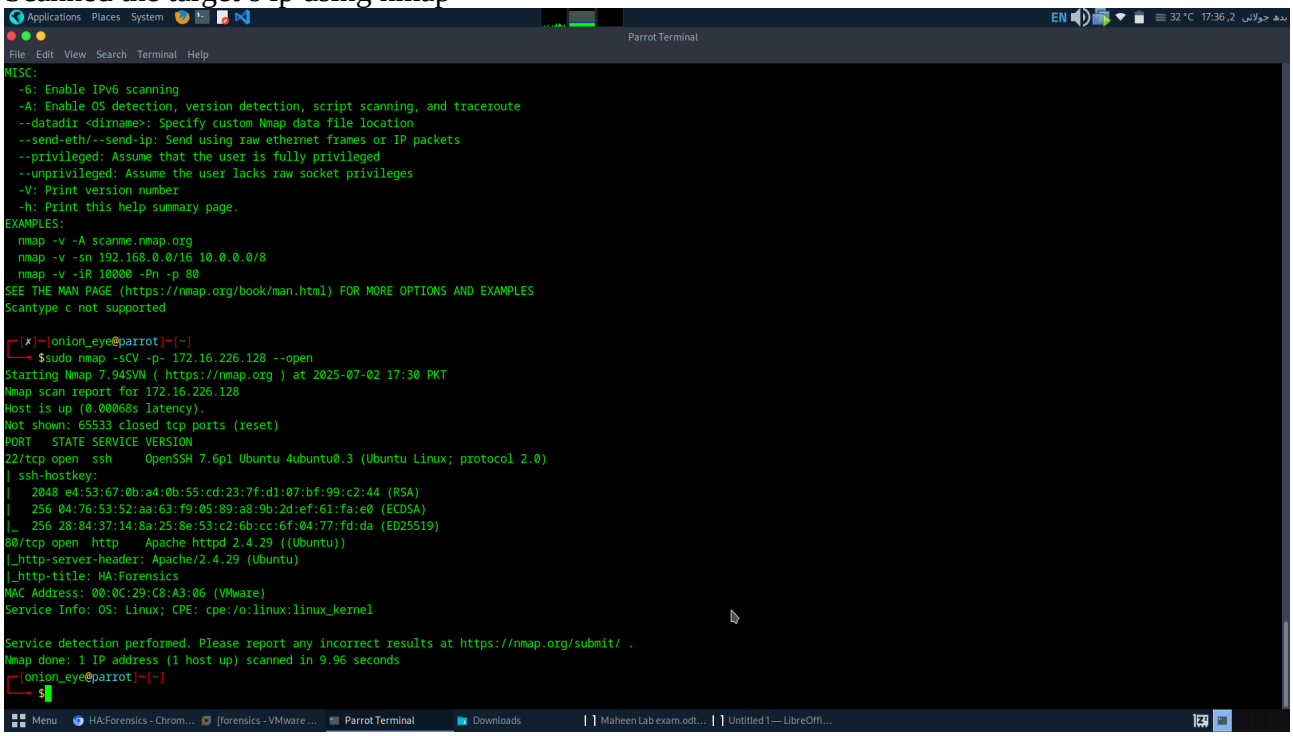
I have installed the vmware workstation on my parrot os host machine and set it to NAT to connect this vm with my host os.



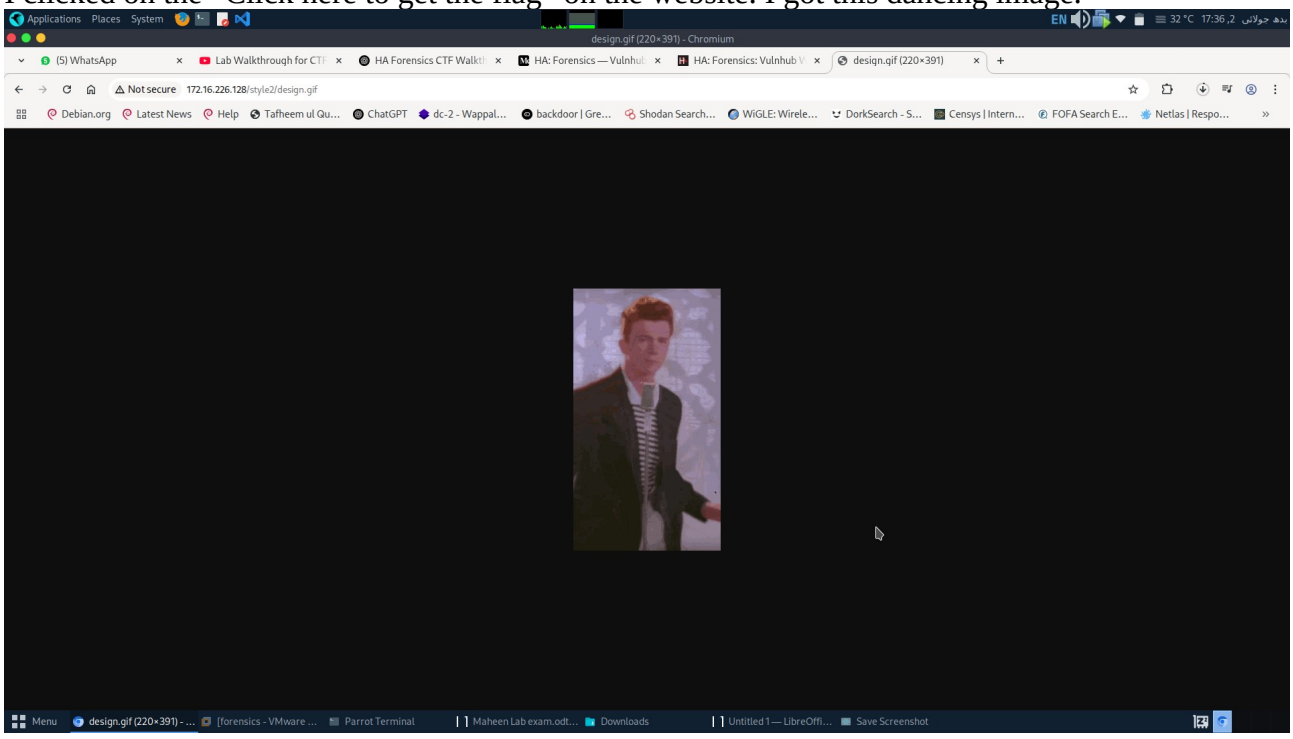
Got the target Ip address as 172.16.226.128. Opened this on my browser and got this interface



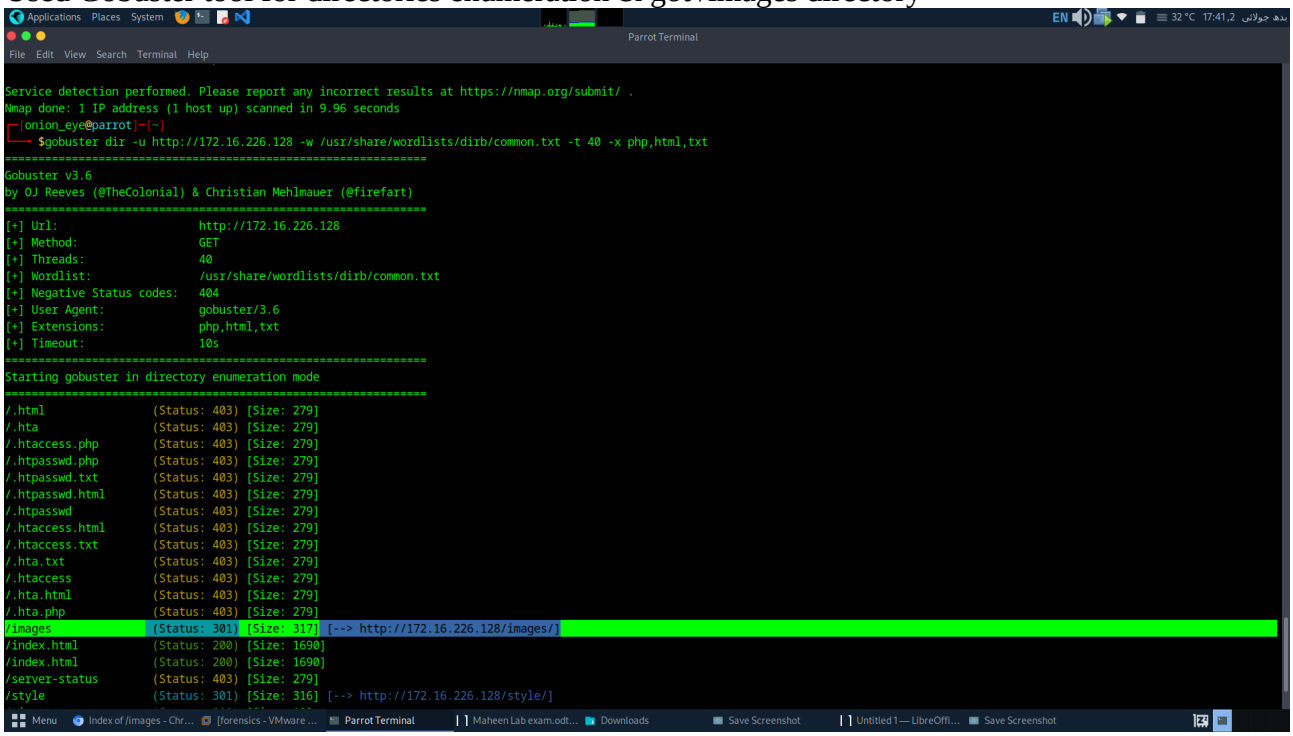
Scanned the target’s ip using nmap



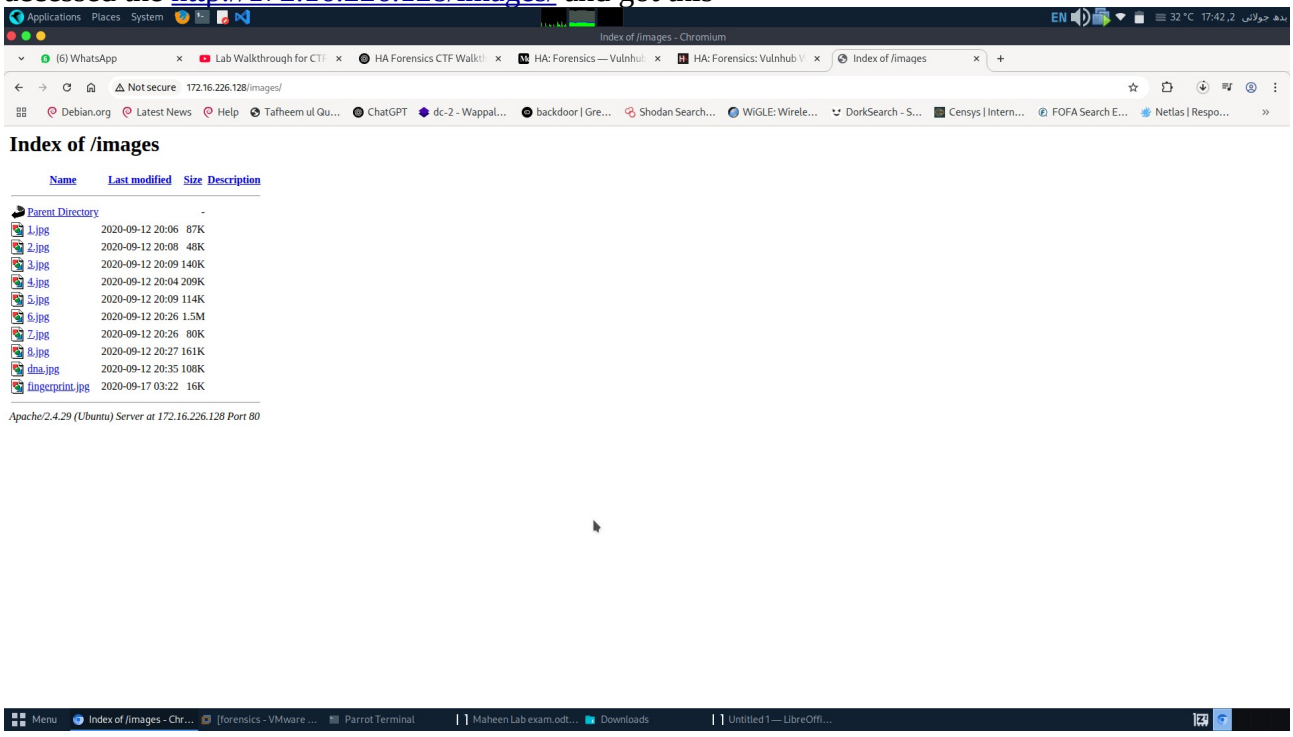
I clicked on the “Click here to get the flag” on the website. I got this dancing image.



Used Gobuster tool for directories enumeration & got /images directory

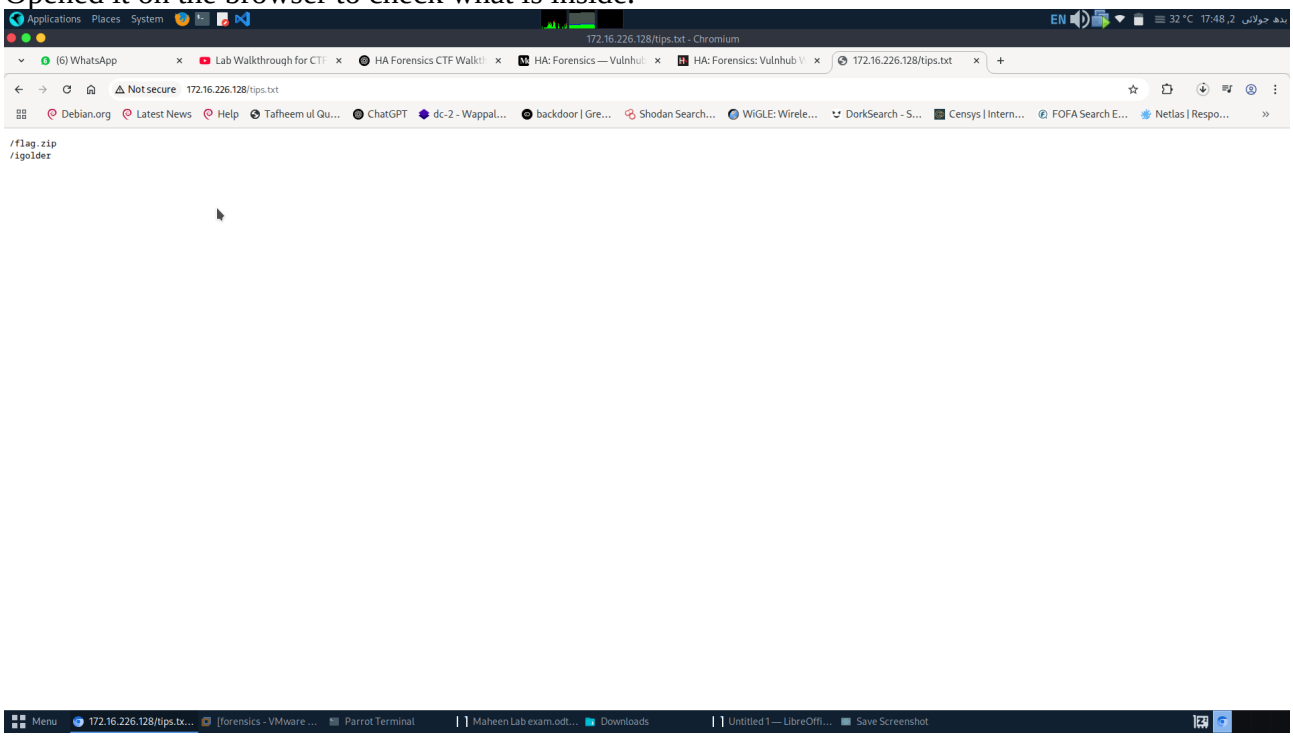


accessed the http://172.16.226.128/images/ and got this

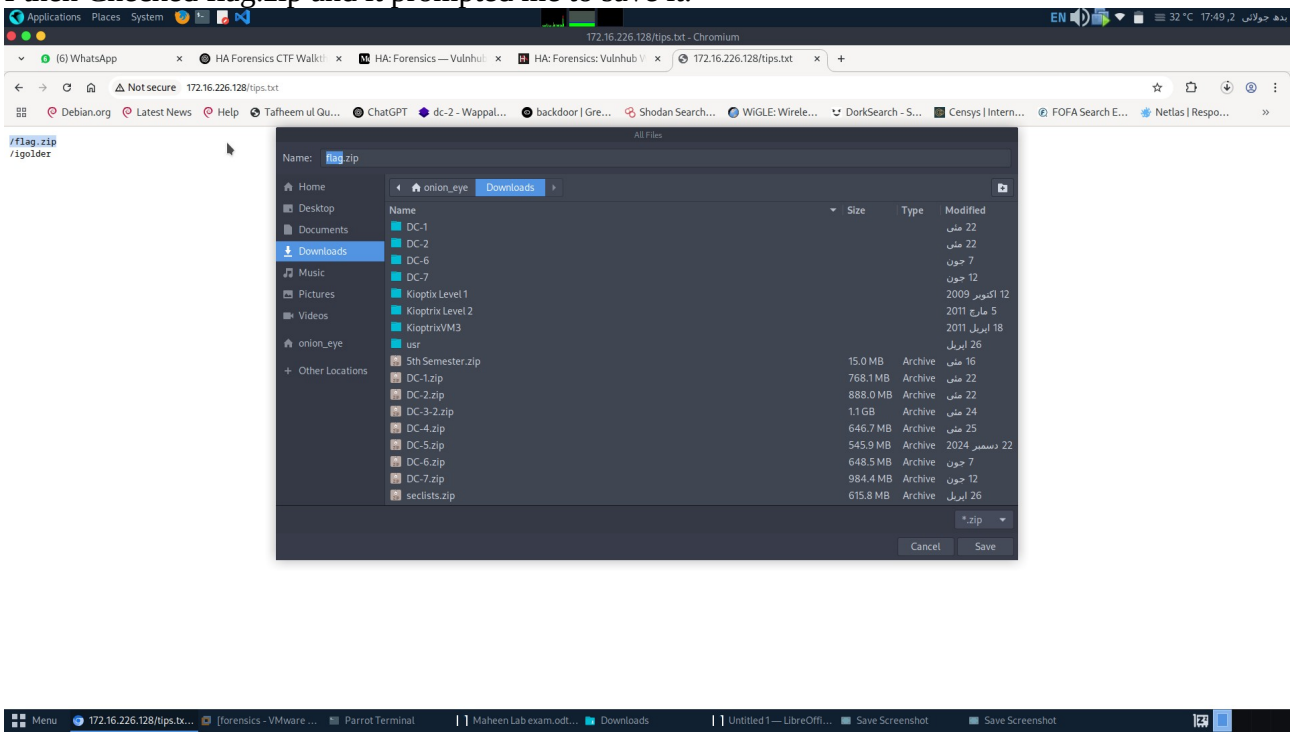


Downloaded the fingerprint.jpg file to further anaylze it. Ran exiftool on this picture and got this the **FIRST FLAG**.

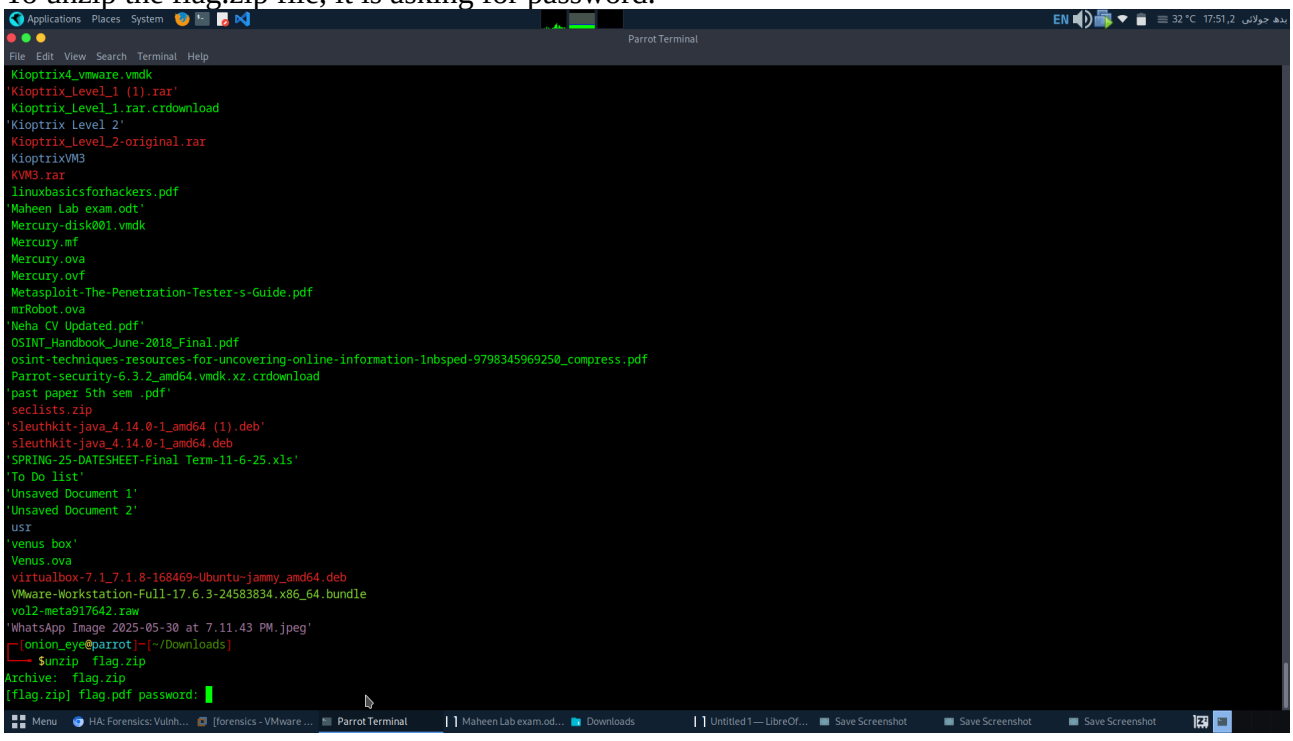
I got another directory using nmap scanning that is /tips.txt
Opened it on the browser to check what is inside.



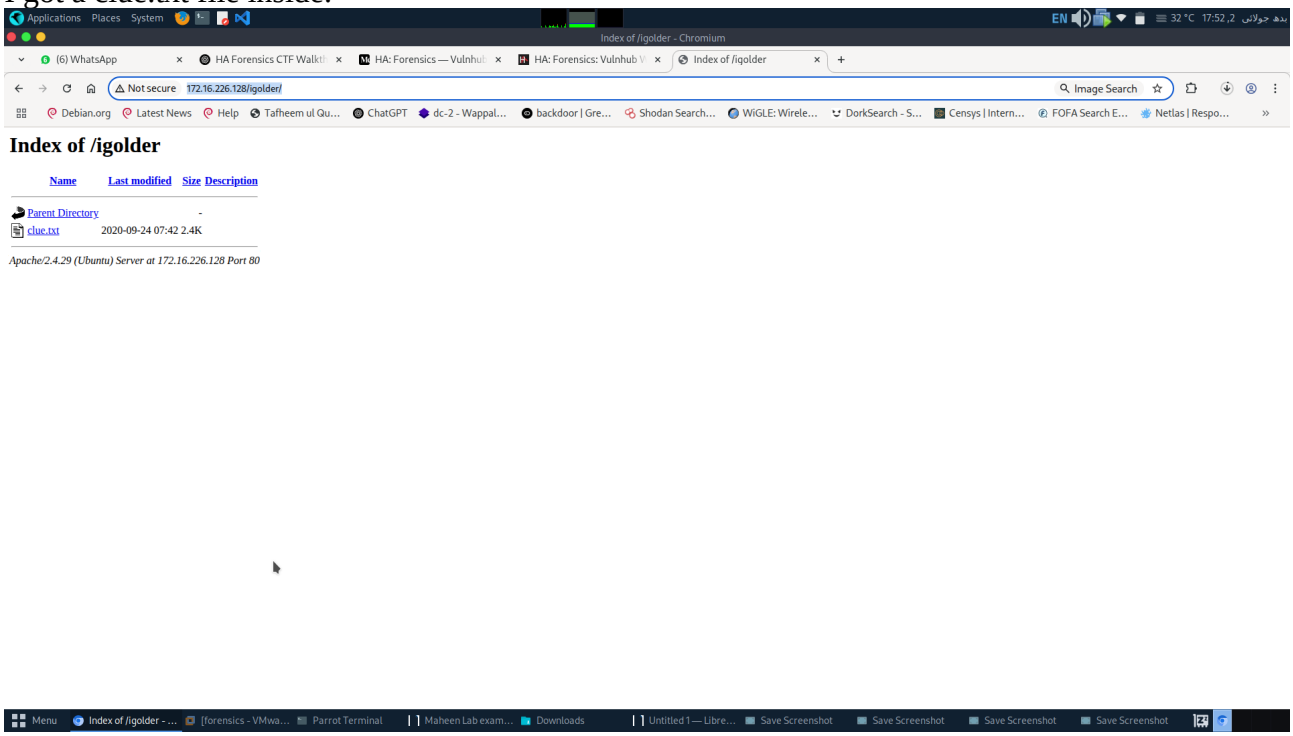
I then Checked flag.zip and it prompted me to save it.



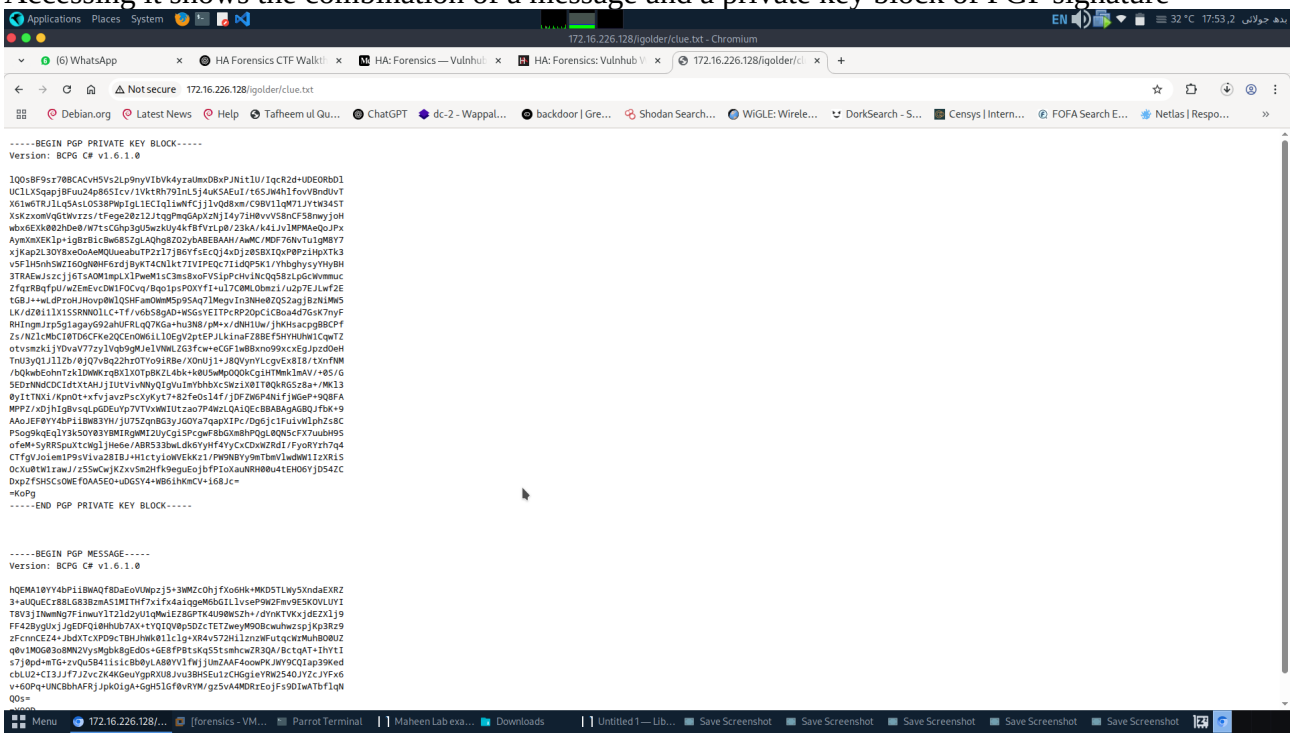
To unzip the flag.zip file, it is asking for password.



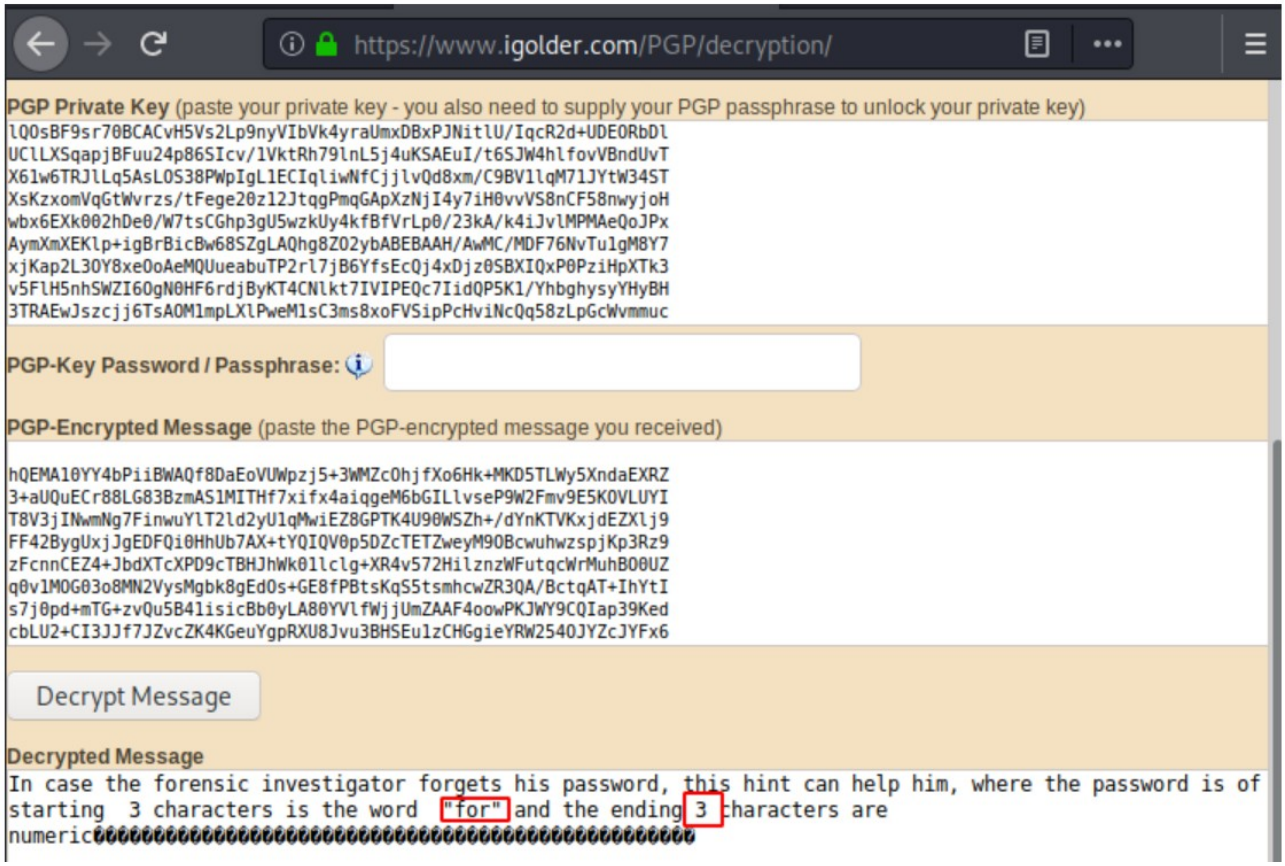
I will be looking for a password in the other directory called http://172.16.226.128/igolder/
I got a clue.txt file inside.



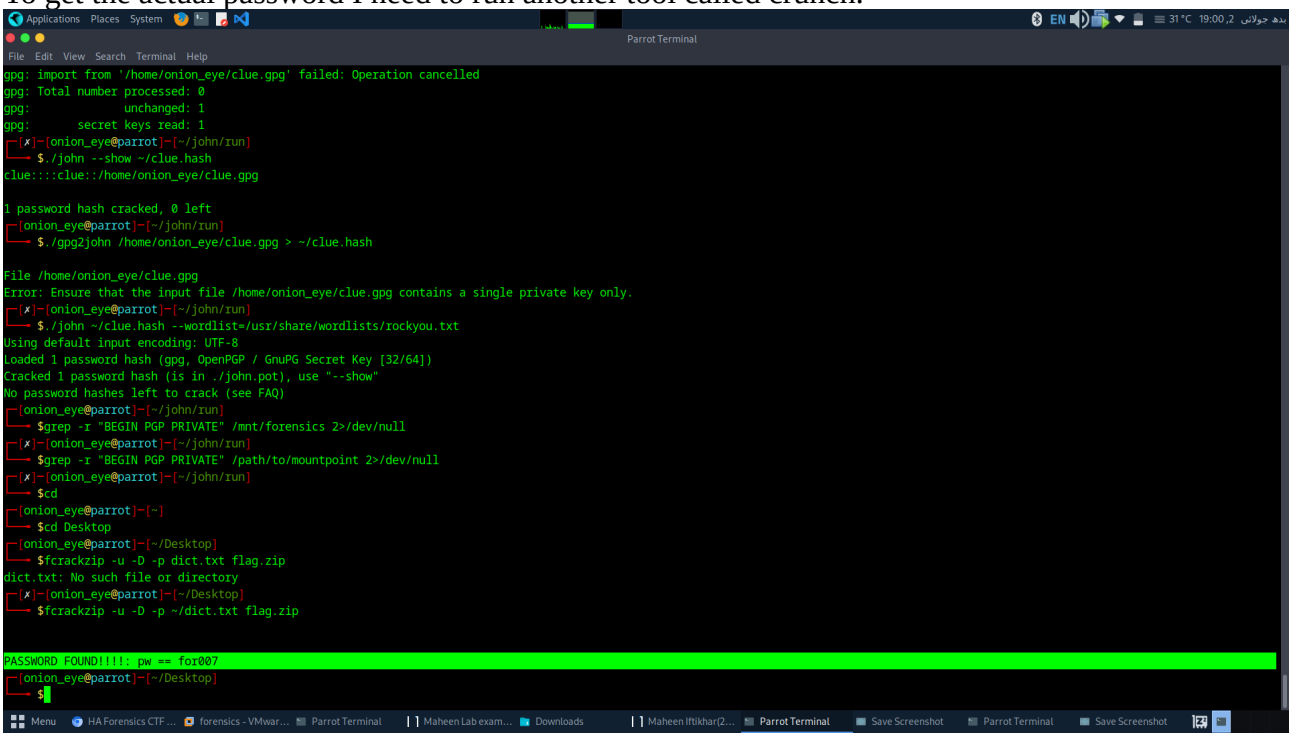
Now I will be looking inside this file for a clue or a password.
Accessing it shows the combination of a message and a private key block of PGP signature



To decrypt the PGP signature I got to igholder website and pasted the key and the message and got the decrypted message.

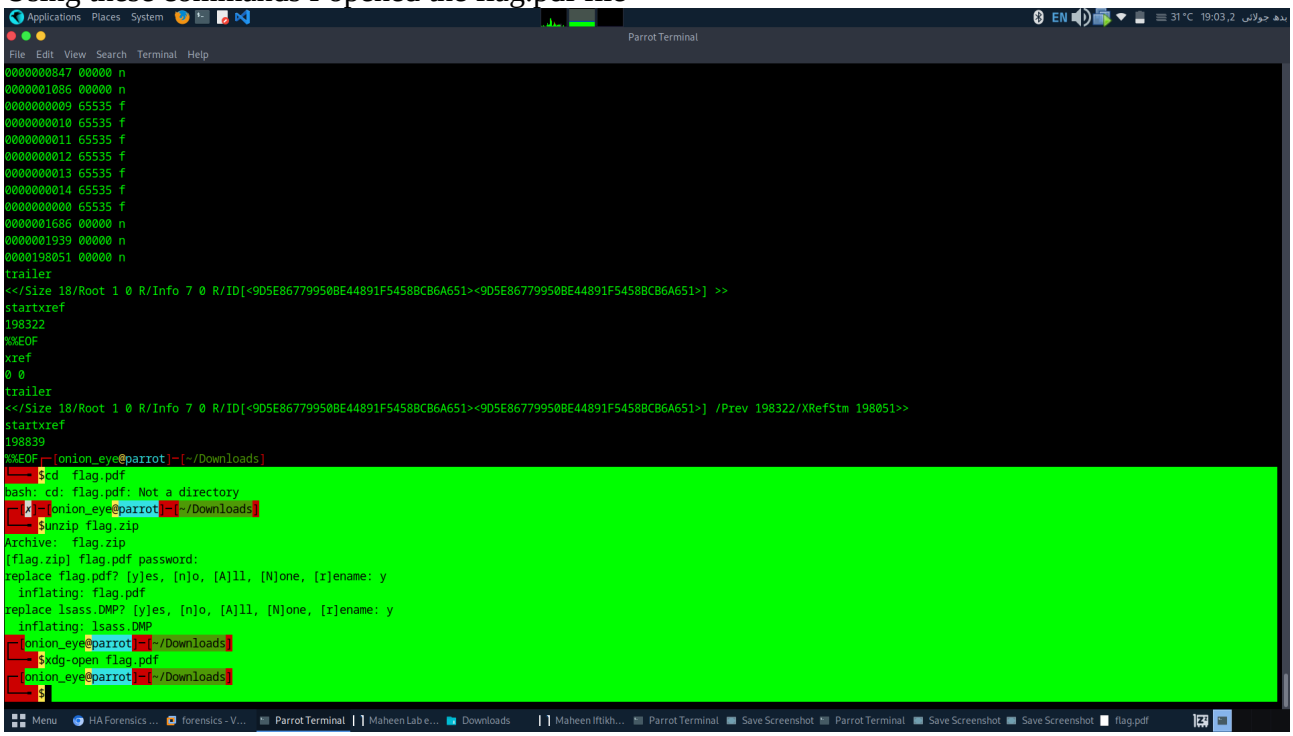


Here I got the password hint and not the actual password.
To get the actual password I need to run another tool called crunch.

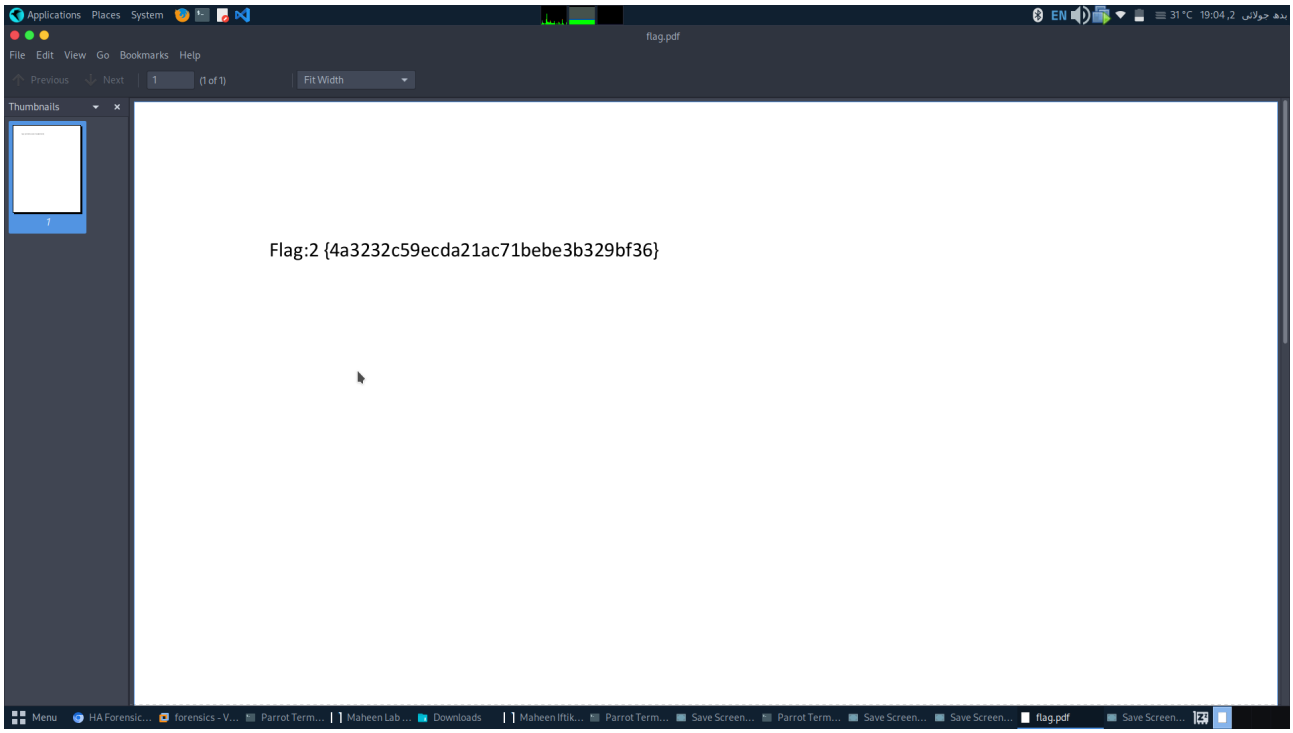


Got the password.

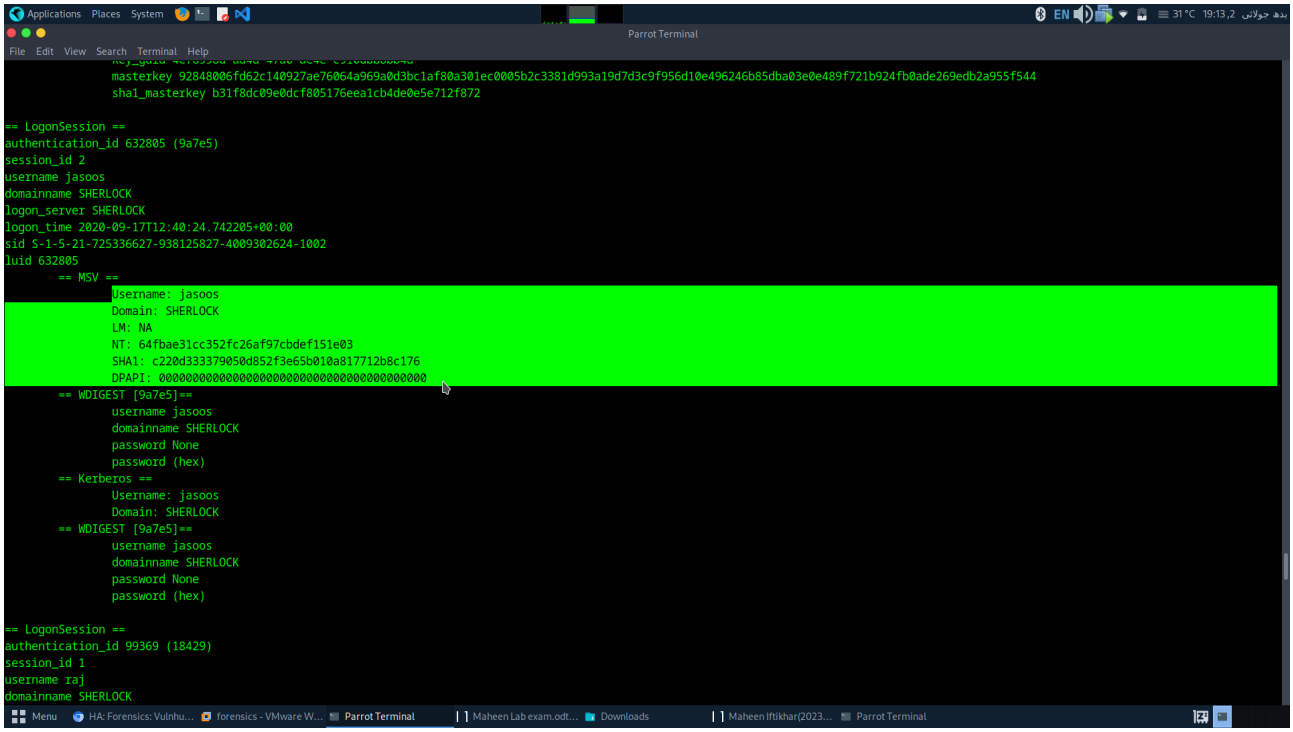
Using these commands I opened the flag.pdf file



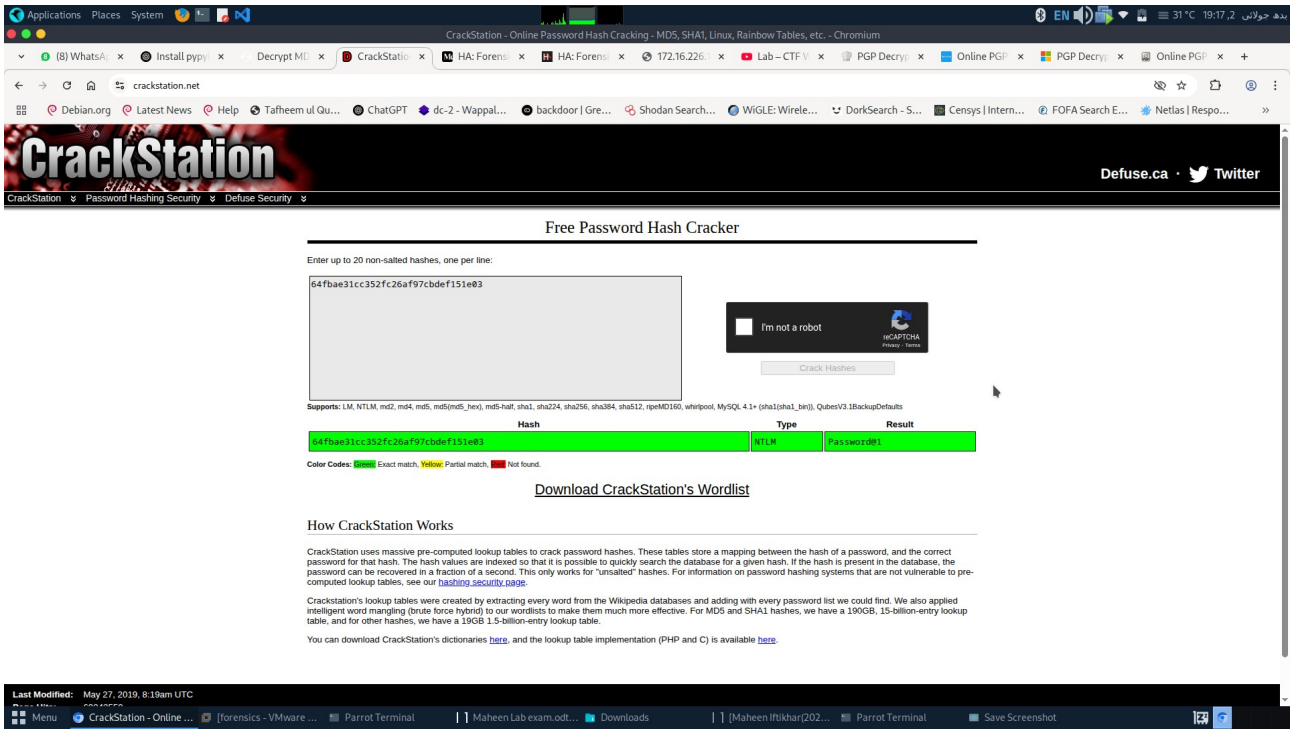
Got the **SECOND FLAG**



The other file we got was the DMP file. This is a dump file and can be inspected using pypykatz. Got these usernames.

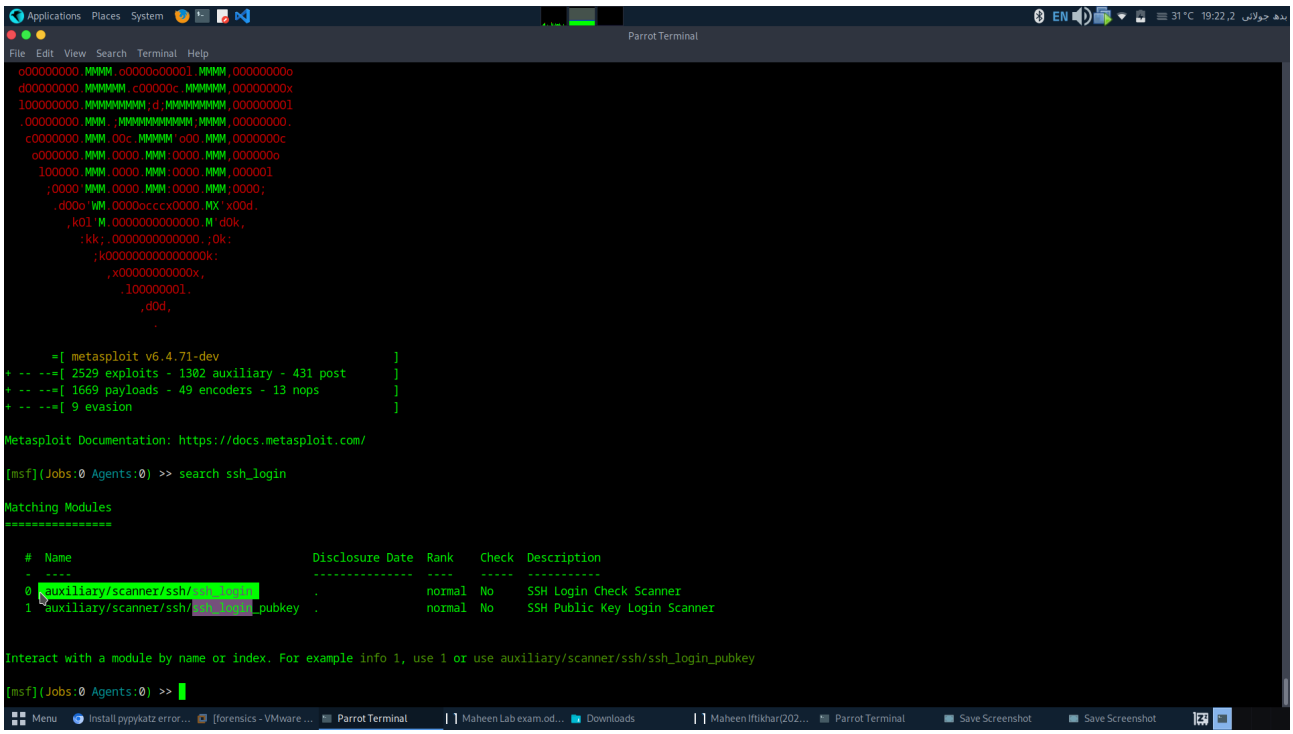


I found a username Jasoos that seems suspicious. I got the hash so I will be cracking the hash using crackstation.

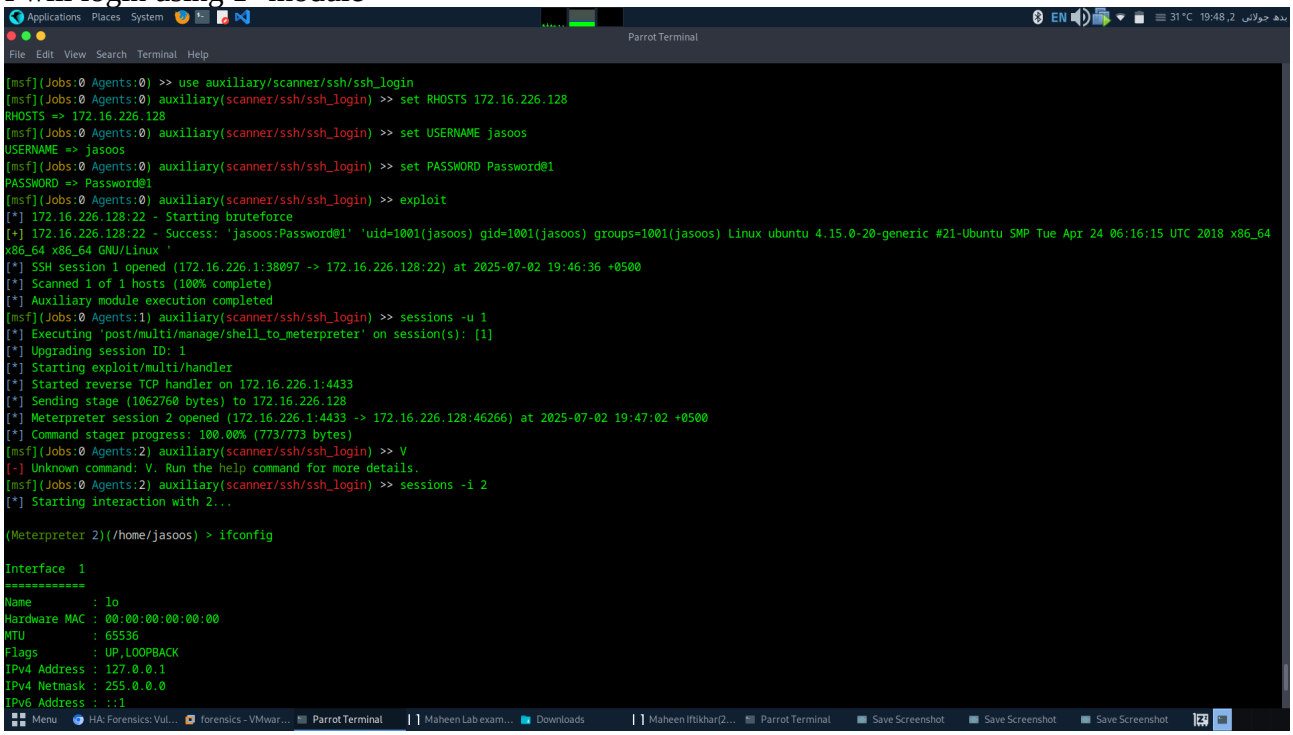


Got the password as Password@1

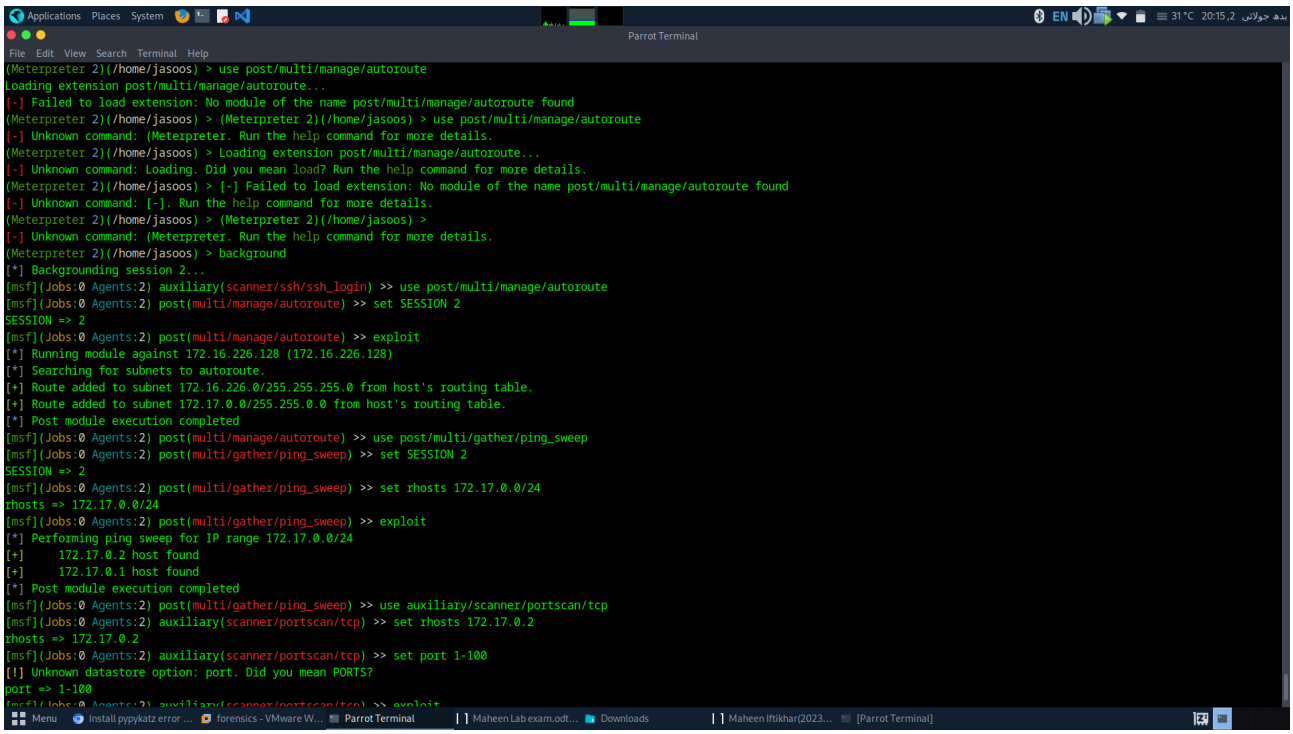
Now we have the target's ip and password that we just now cracked. I will now use metasploit and login it via 2nd open port found in nmap SSH.



I will login using 1st module



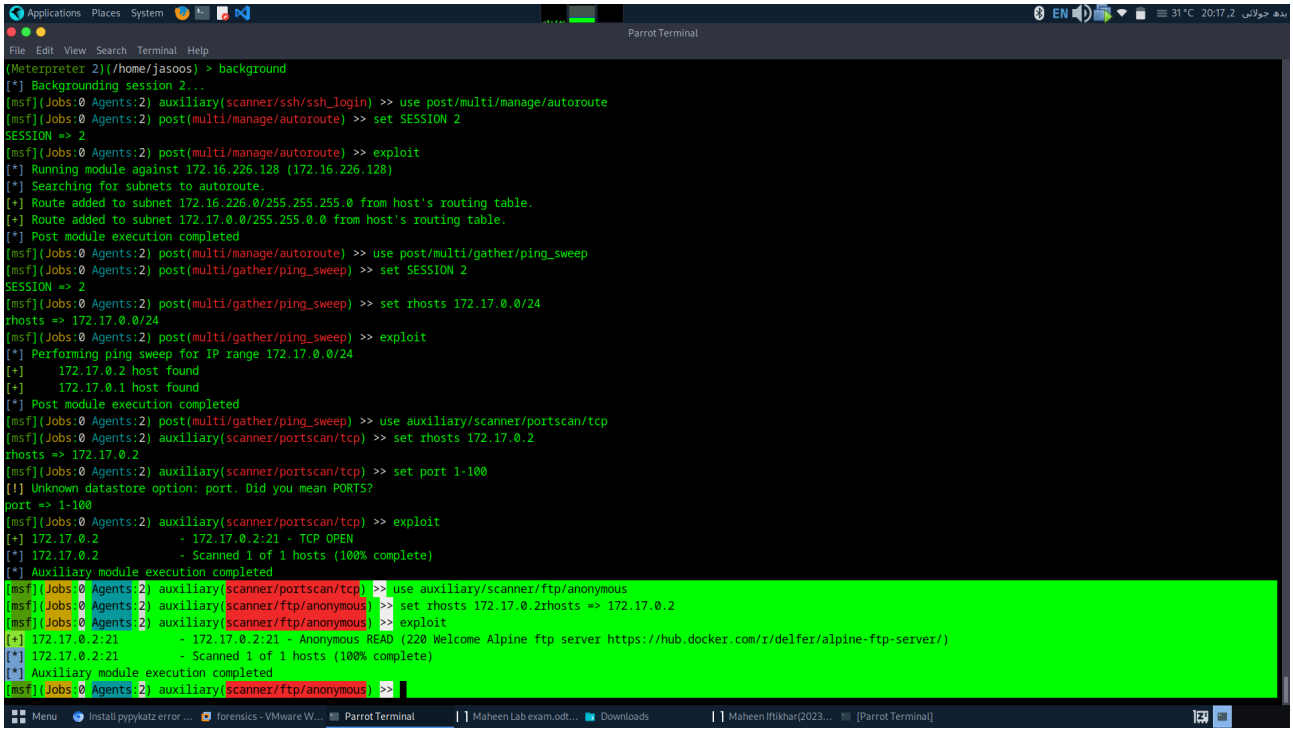
Here I see the **network interfaces** on the target machine. I identified that the target runs Docker containers because of the `docker0` interface.
I will now Use **Metasploit's `autoroute` module** on session 2 to add routes for internal pivoting, allowing access to the target's Docker subnet.



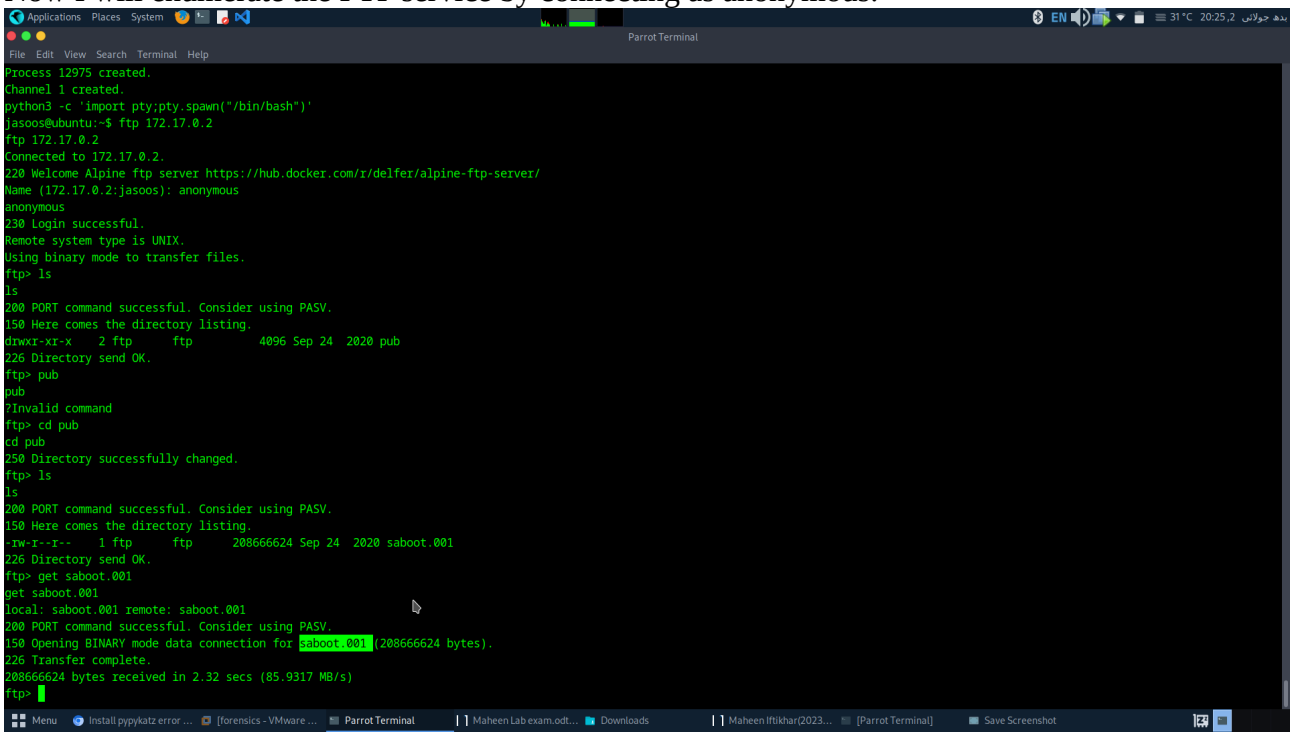
Prepared to perform:

- A **ping sweep** on the Docker subnet to discover live containers or hosts.
- A **port scan** on discovered IPs (e.g., `172.17.0.2`) to identify open services.
- An **anonymous FTP login check** on the target's FTP service.

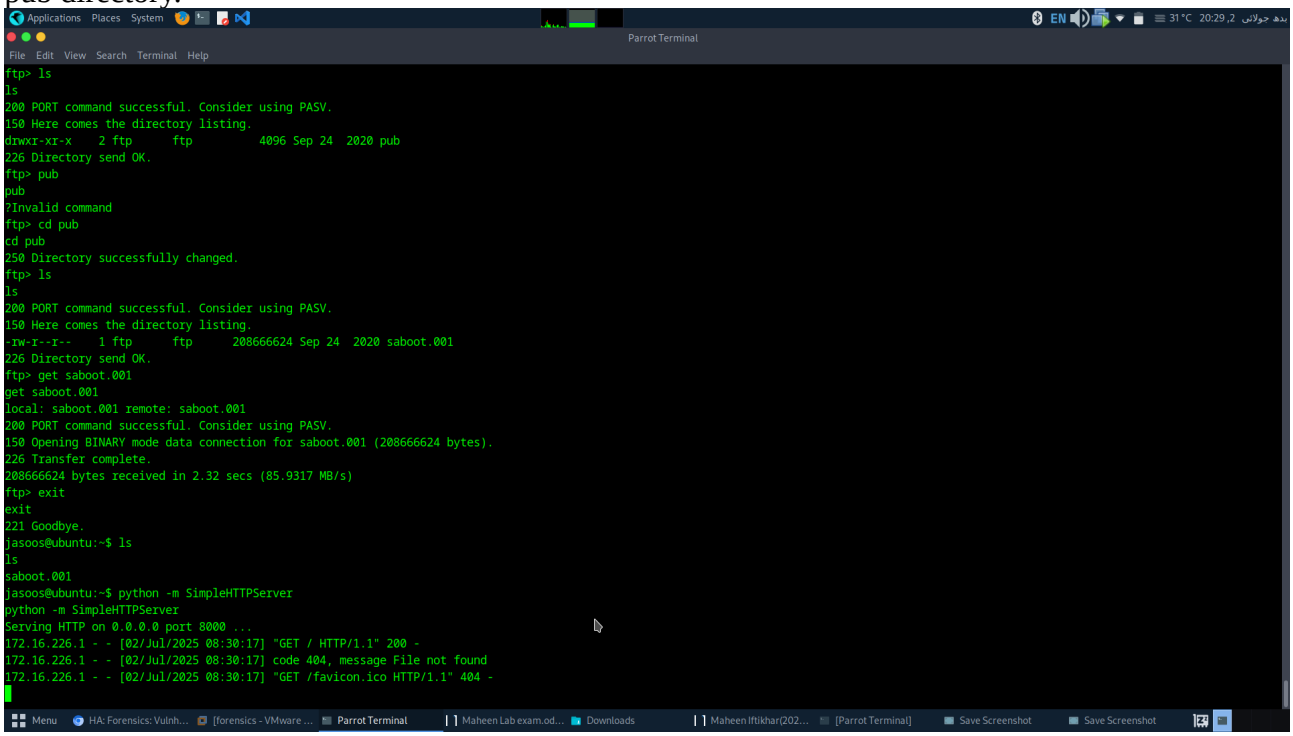
  I got the ftp server here on the target machine that allows anonymous services.



Now I will enumerate the FTP service by connecting as anonymous.

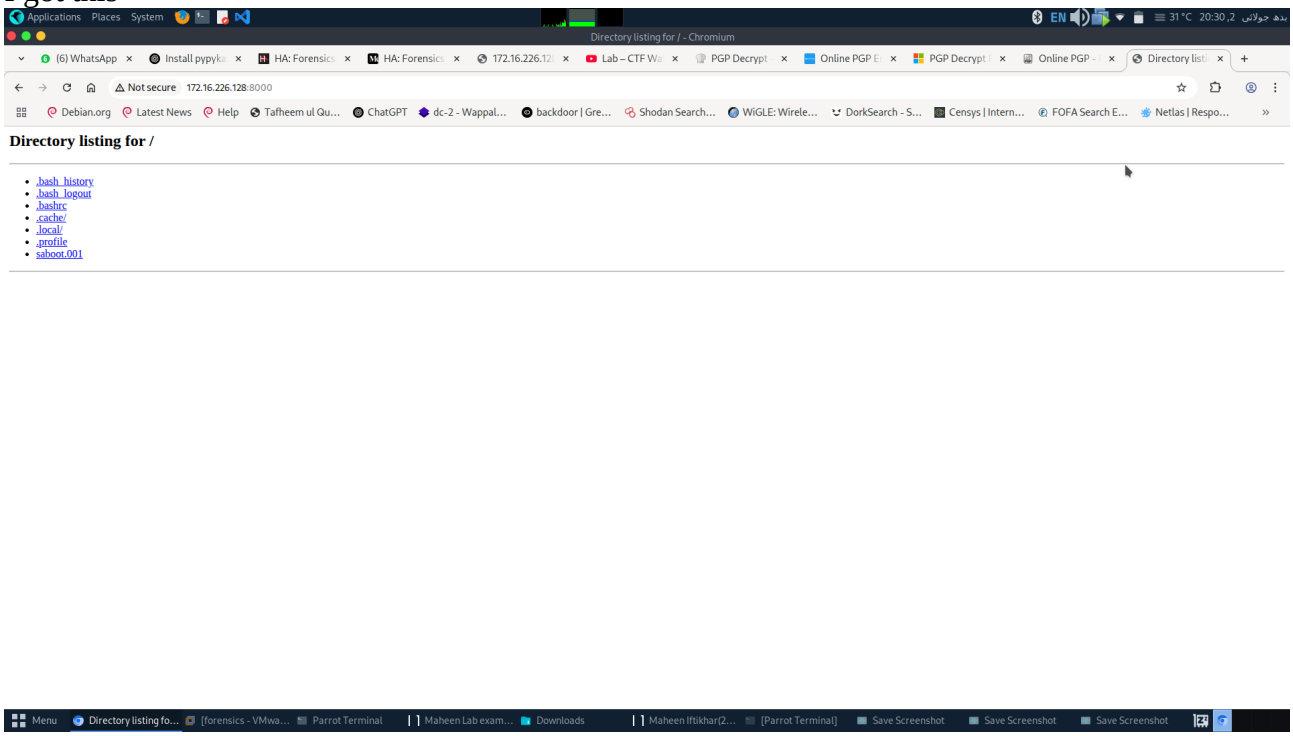


I got a file here with the name saboot(evidence) using ftp server on the target machine inside the pub directory.

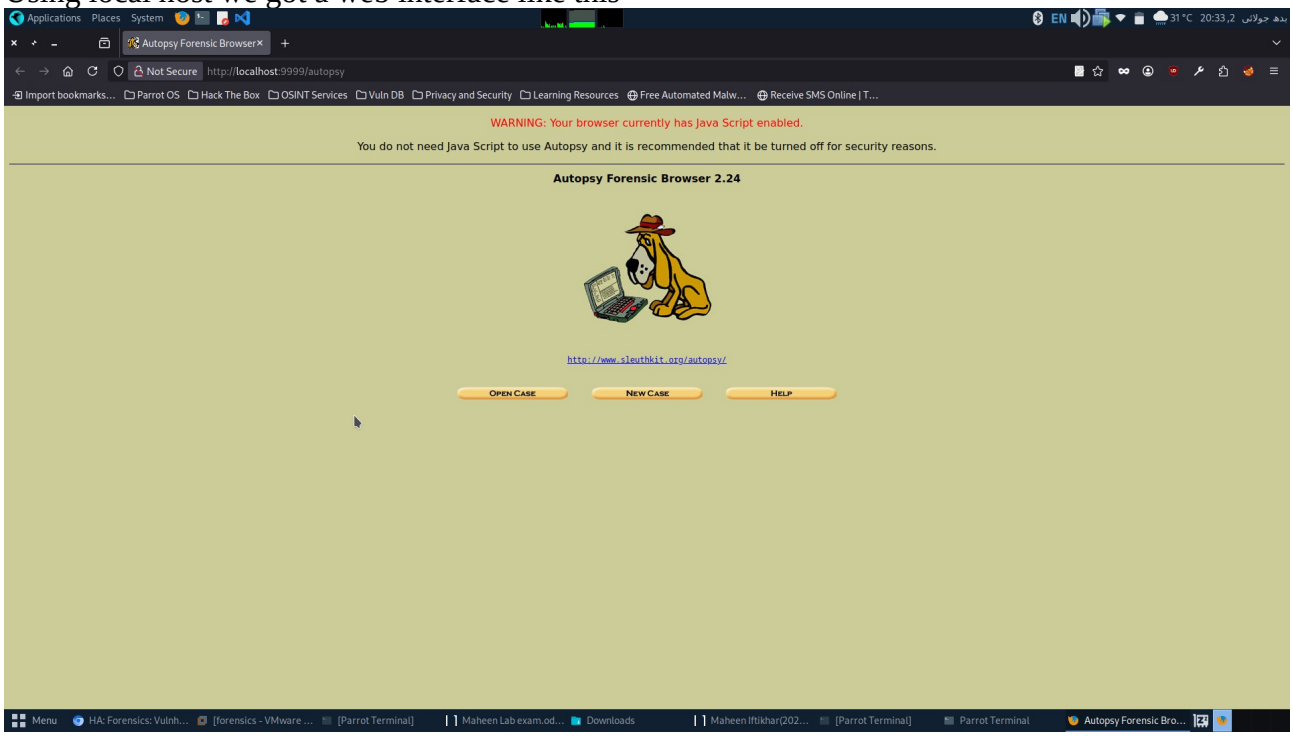


Using HTTP server we transfer the file from the target machine to our local system or the attacker system.

I got this

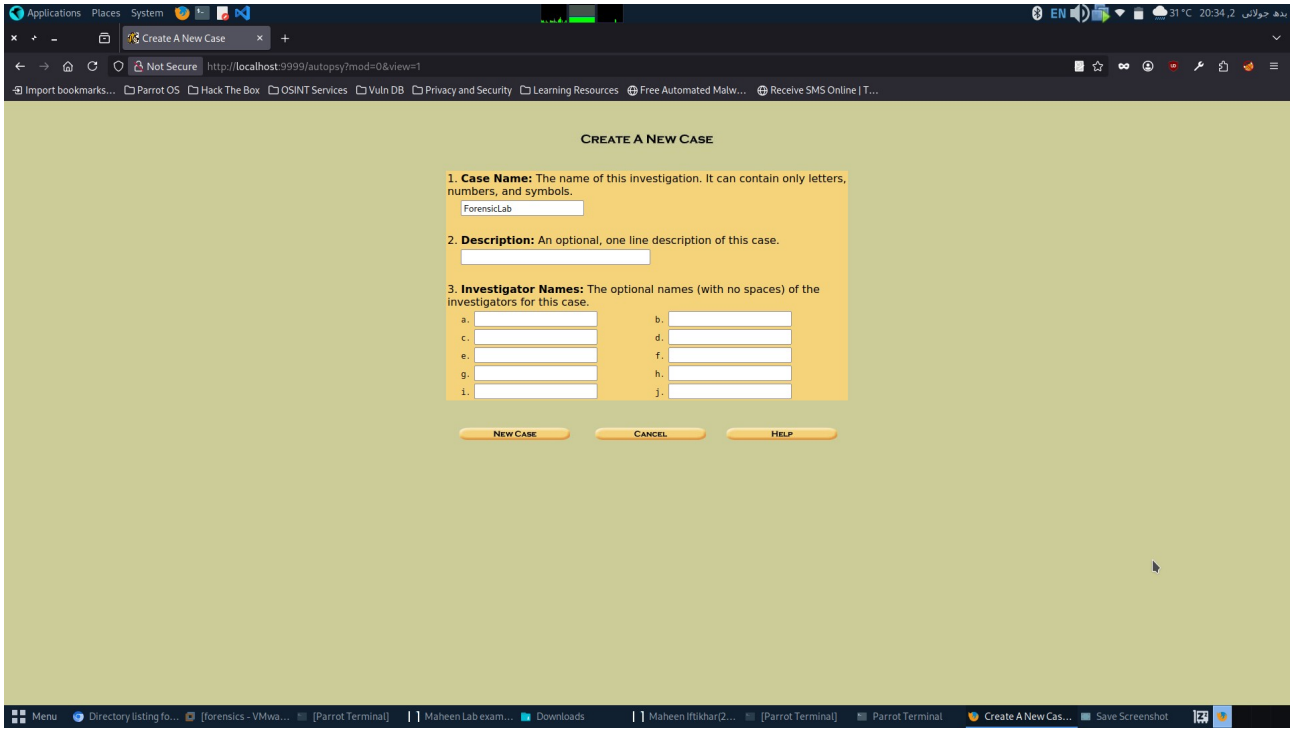


Now I will use autopsy tool to investigate the image captured.
Using local host we got a web interface like this

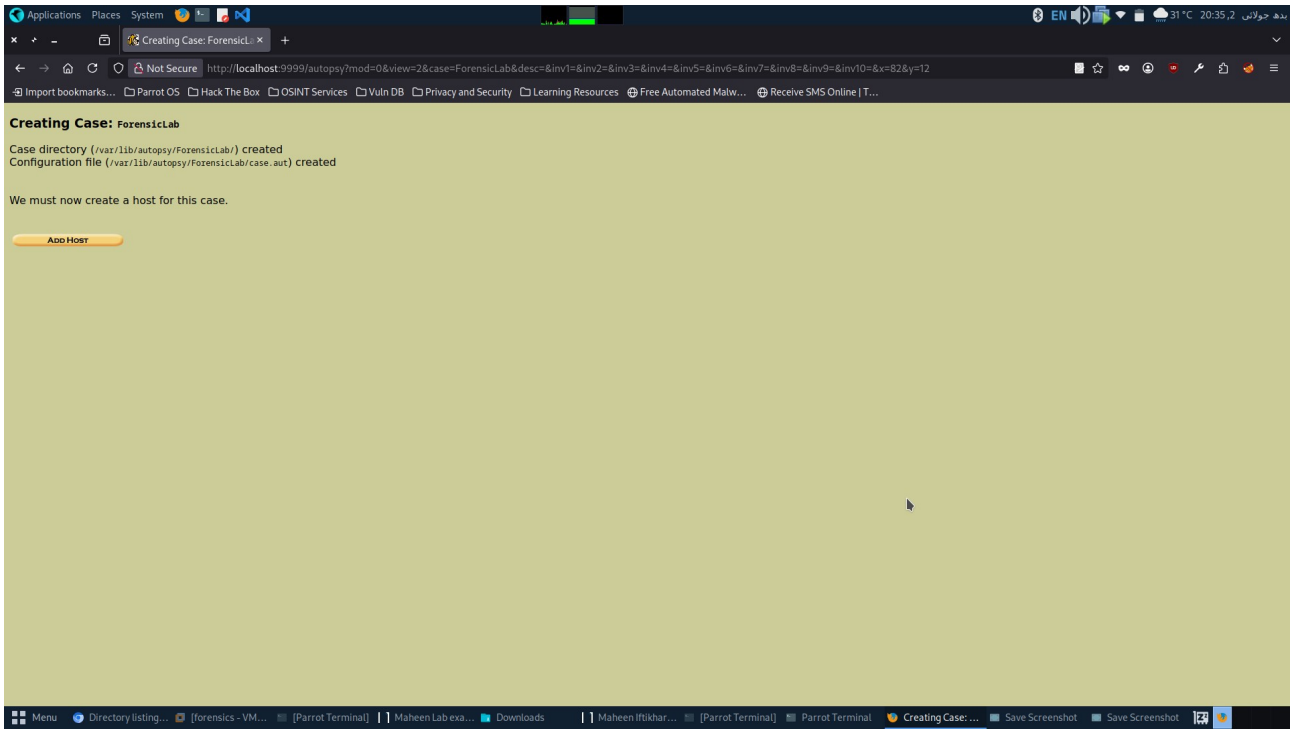


Click on New case.

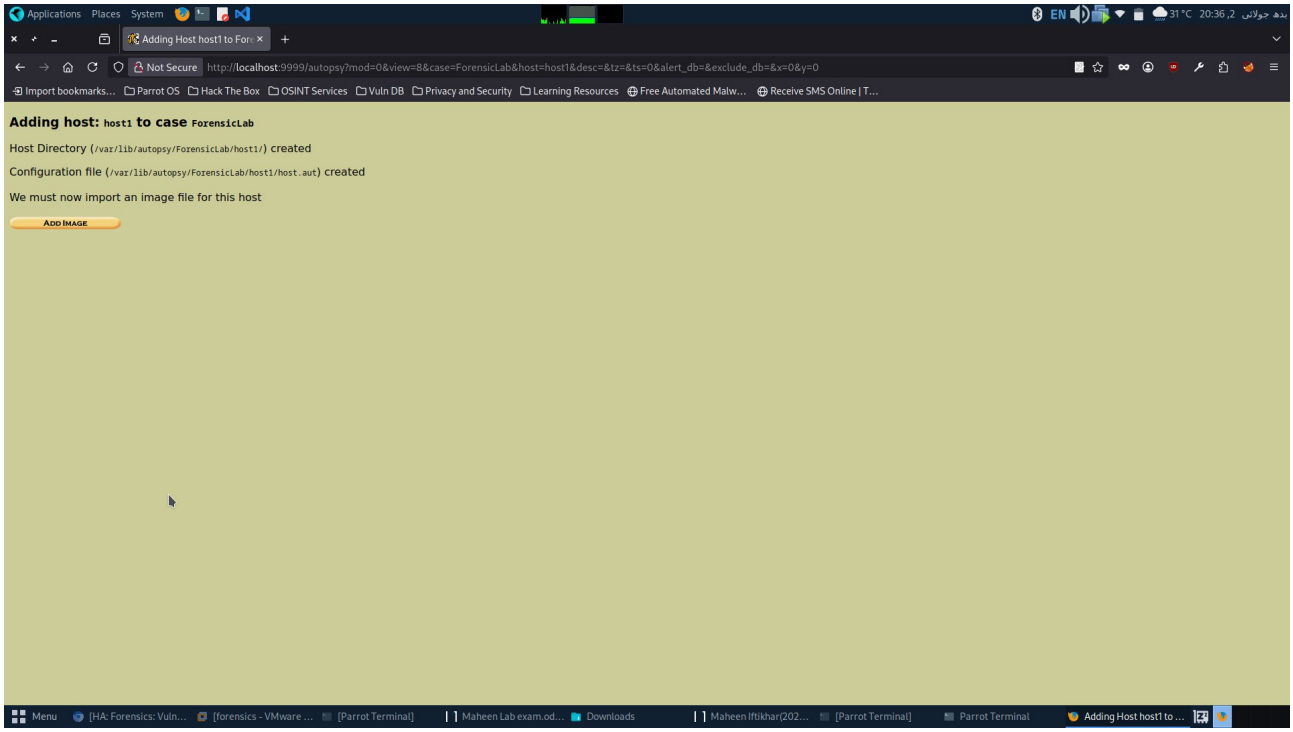
I will name the case as ForensicLab



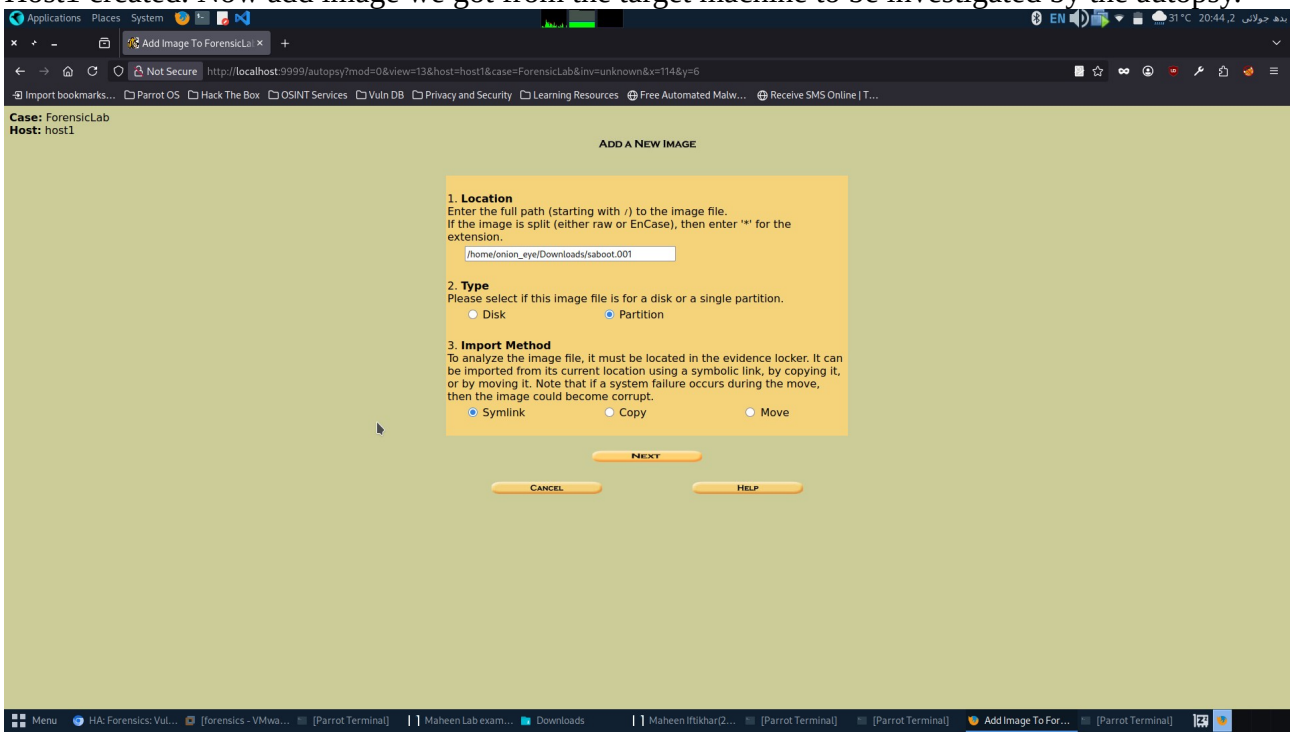
This create a new case



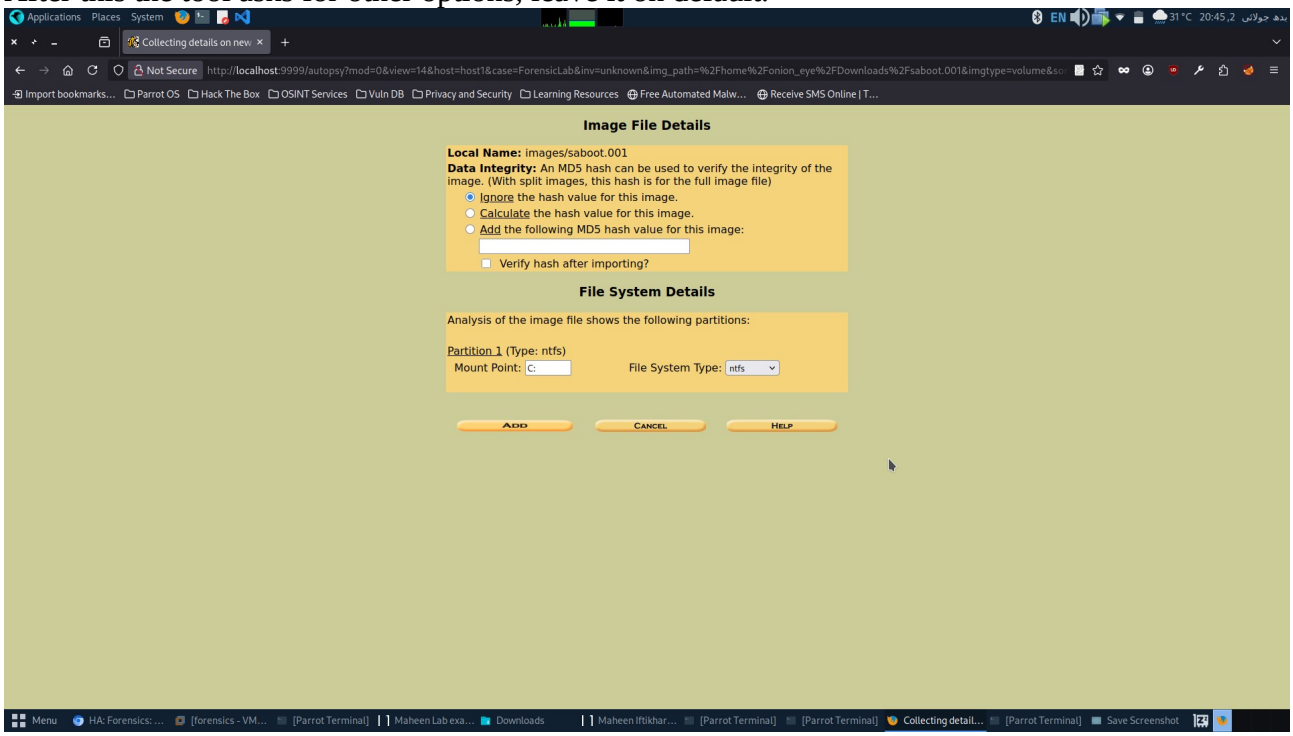
Now add host.



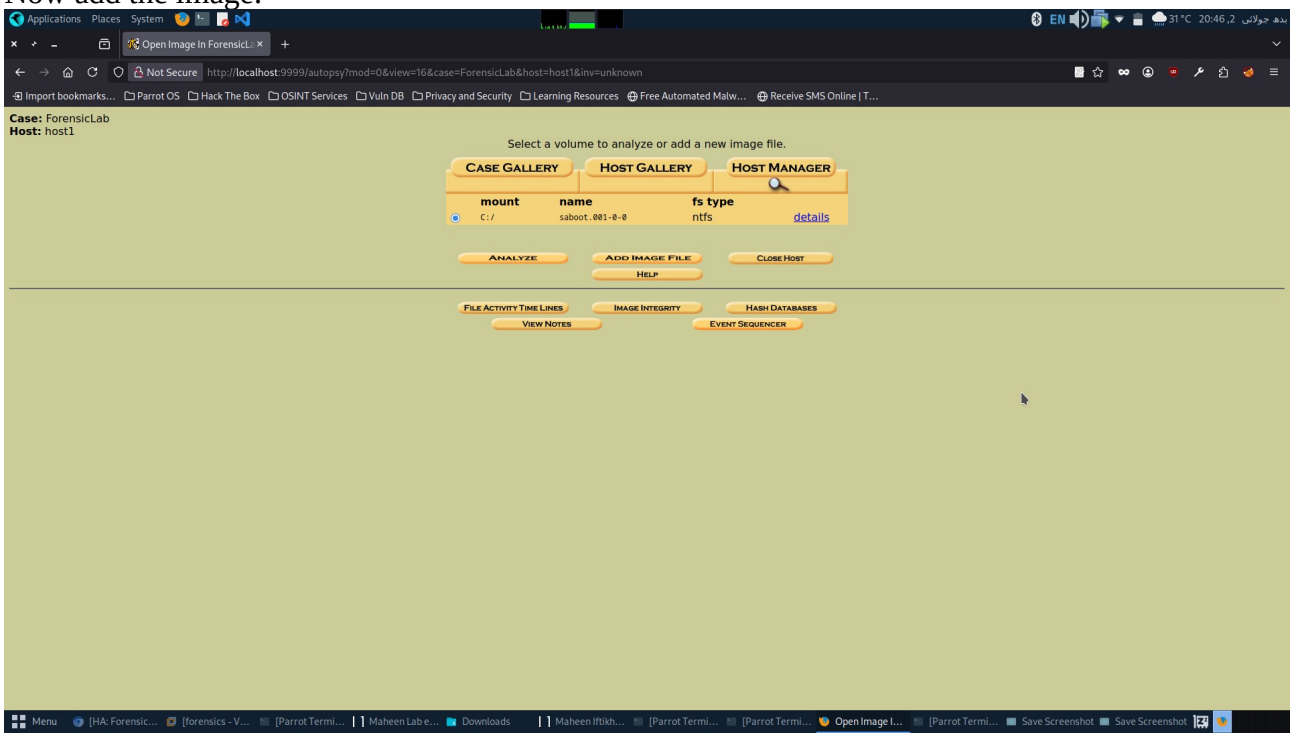
Host1 created. Now add image we got from the target machine to be investigated by the autopsy.



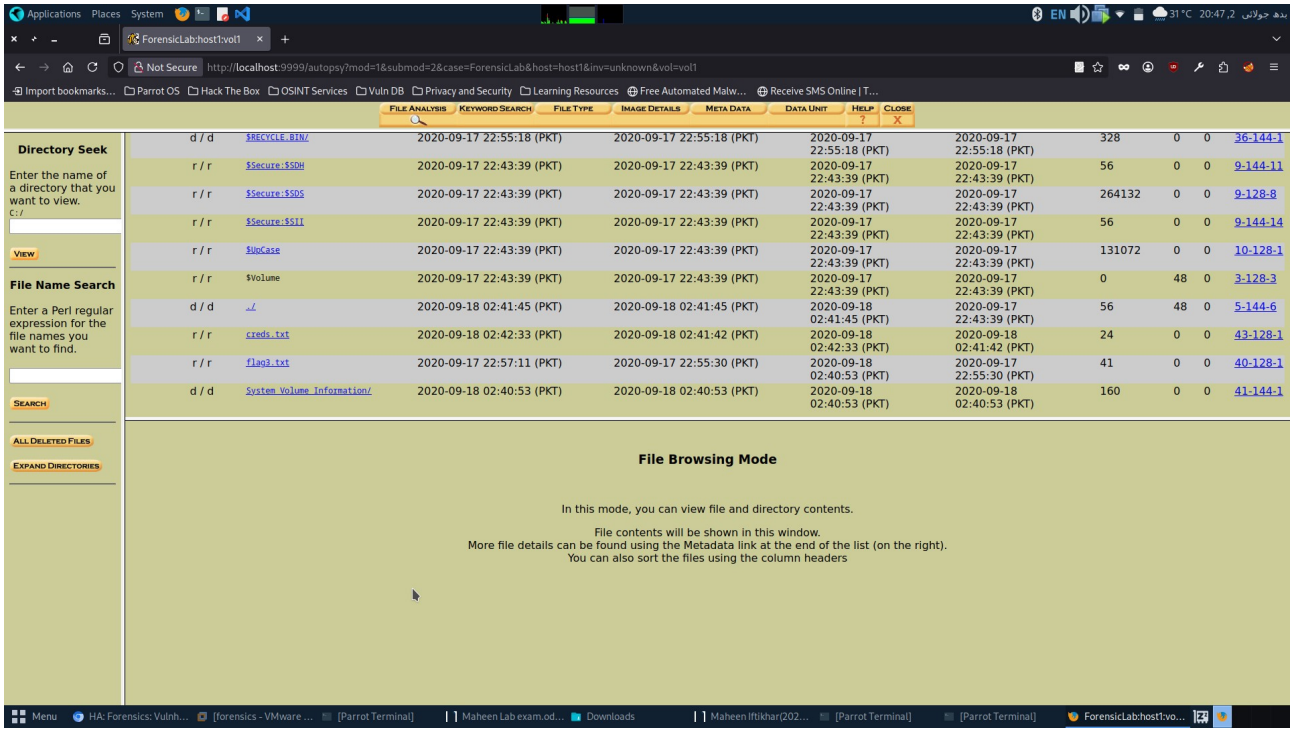
After this the tool asks for other options, leave it on default.



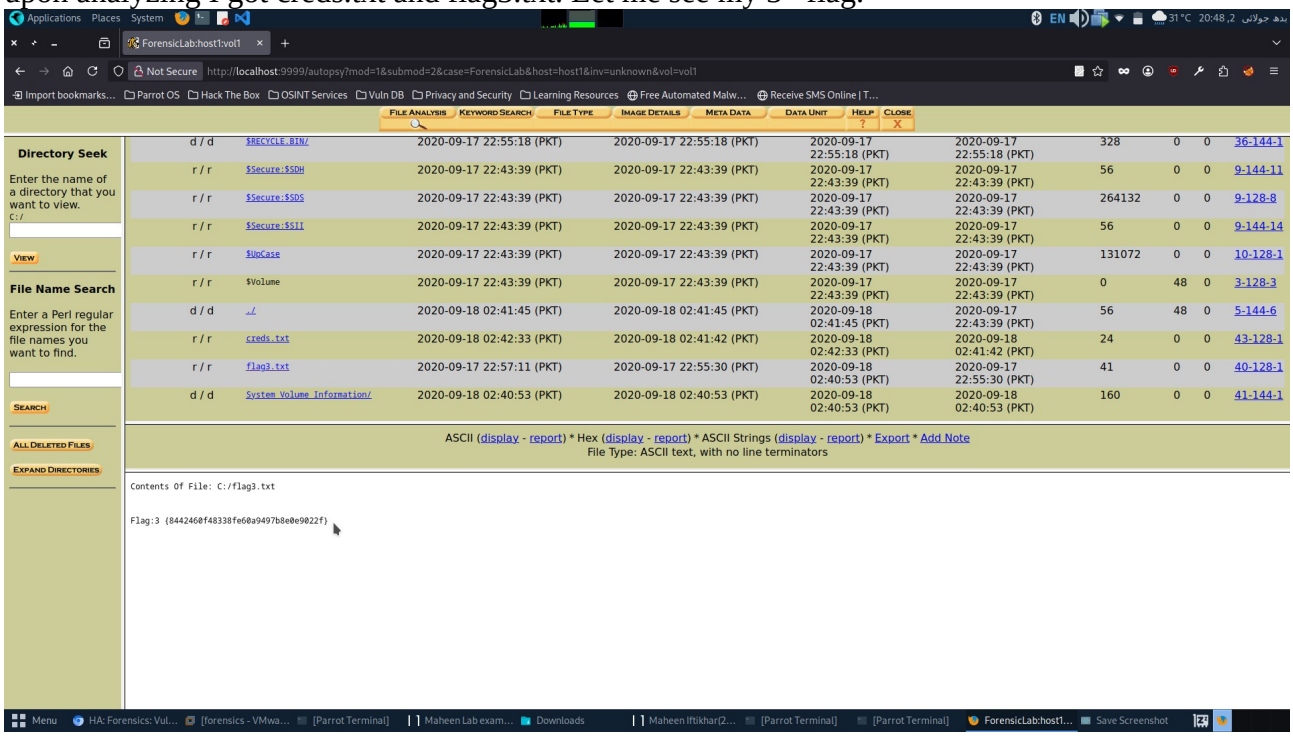
Now add the image.



Our image has been mounted. Analyze it

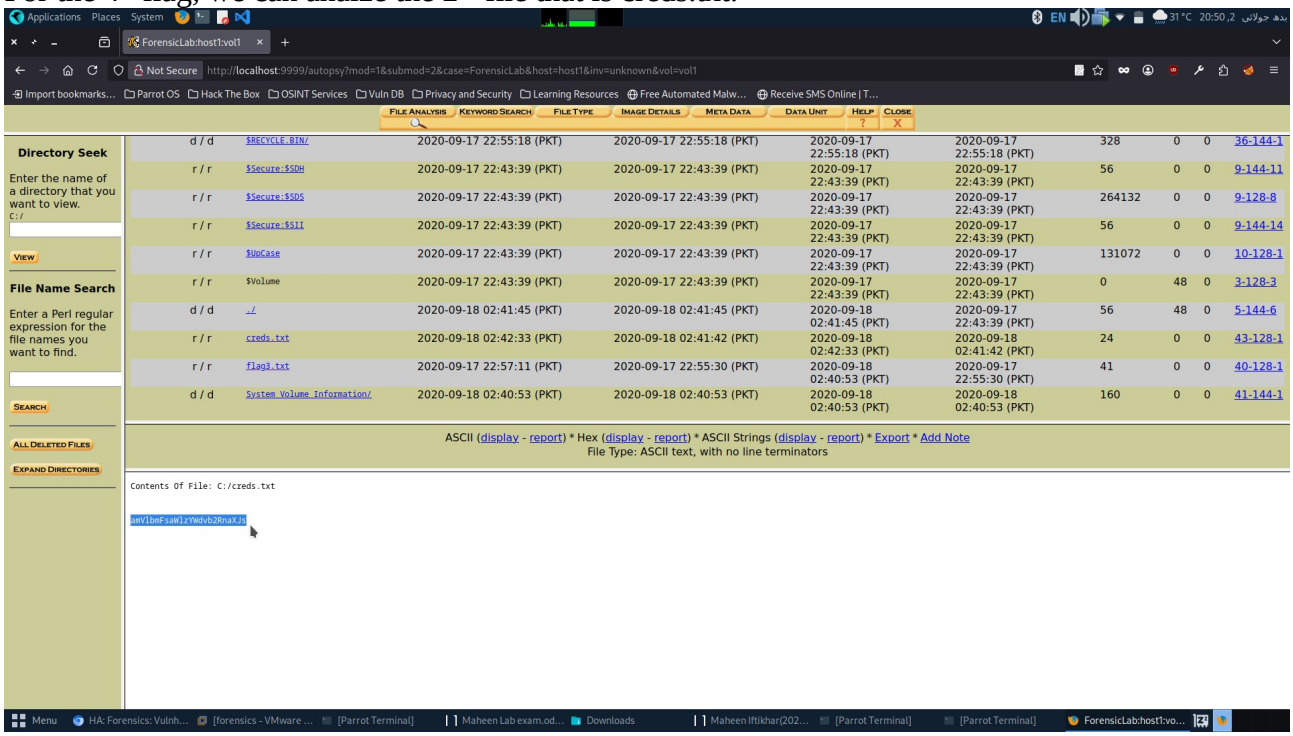


upon analyzing I got creds.txt and flag3.txt. Let me see my 3rd flag.

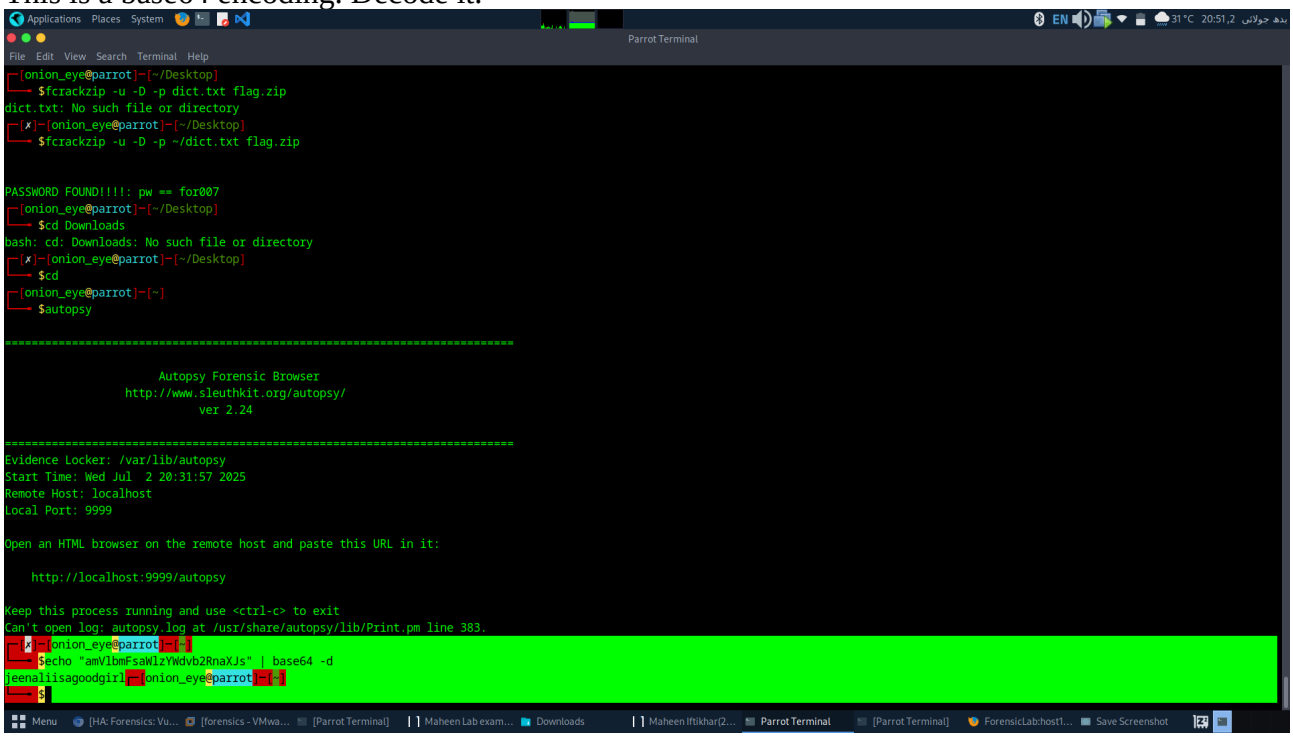


Found **THIRD FLAG.**

For the 4th flag, we can analze the 2nd file that is creds.txt.



This is a base64 encoding. Decode it.



Using the **jeenaliisagoodgirl** password for the forensic user I got the **FOURTH FLAG**