

Cats - 450

Problem:

```
I had fun once, it was horrible.  
Password: F3lyn34LifE!  
cats_51474229fe0d9bbd8da500fe3f74b383d175cee1.zip
```

Link:

https://d34j1dfl6n327i.cloudfront.net/cats_51474229fe0d9bbd8da500fe3f74b383d175cee1.zip

Video Walkthrough Link:

<https://www.youtube.com/watch?v=zoWxoGbVd8Q>

Solution:

First you download the file. As always, make sure you take the SHA-1 checksum of the file before doing anything and see if it matches up with the filename, to make sure you downloaded the right file and not a virus or something.

In this challenge, we are given a virtual machine of someone who evidently really likes cats. Of course, we will not log in to the VM - this is a no-no in forensics for multiple reasons:

- We lose forensic integrity
- Temporary files may be lost
- Memory locations get overwritten (deleted files, etc)
- Unwanted programs may run, etc.

Actually, we shouldn't even boot from the VM's hard disk. Instead, we use it as an unmounted hard disk in Kali. But first, take a snapshot of the VM, just in case you accidentally make some mistakes (and so that

we don't lose any extra-volatile data, in case those are necessary). In order to do all these things, we:

1. Go over to our virtualization software (hypervisor) of choice. In this case, we used VirtualBox, but you could use VMWare or Parallels too. (This is where the snapshot can be taken.)
2. In the CD/DVD slot, we insert a Kali Linux ISO. Find one at <https://www.kali.org/downloads/>.
3. When prompted, boot into forensics mode. Forensics mode makes sure nothing ever happens to the hard drive without direct user interaction (<http://docs.kali.org/general-use/kali-linux-forensics-mode>).



4. In Kali, we first get a SHA-1 checksum of the partition, which we will check later again to make sure nothing changed. We run `openssl sha1 /dev/sda1`, and get back `ccef3f6b74e943d0e020de56c992bccd21de09af`.
5. Mark the virtual hard drive as read only: `blockdev --setro /dev/sda`
6. We now mount the hard drive:
`mkdir /mnt/cats, then mount -r /dev/sda1 /mnt/cats`
(<http://askubuntu.com/questions/20680/what-does-it-mean-to-mount-something>). As long as we don't add or change any files on the hard drive, we maintain forensic integrity.

```
root@kali: /mnt/cats/home/cats
File Edit View Search Terminal Help
root@kali:~# mkdir /mnt/cats
root@kali:~# lsblk
NAME        MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda           8:0    0    8G  0 disk
|-sda1        8:1    0    7G  0 part
|-sda2        8:2    0     1K  0 part
`-sda5        8:5    0 1022M  0 part
sr0          11:0    1   2.9G  0 rom  /lib/live/mount/medium
loop0        7:0    0   2.6G  1 loop /lib/live/mount/rootfs/filesystem.squashfs
root@kali:~# openssl sha1 /dev/sda1
SHA1(/dev/sda1)= ccef3f6b74e943d0e020de56c992bccd21de09af
root@kali:~# blockdev --setro /dev/sda
root@kali:~# mount -r /dev/sda1 /mnt/cats
root@kali:~# cd /mnt/cats/home/cats
root@kali:/mnt/cats/home/cats# ls
Desktop    Downloads  Pictures  Templates  catz
Documents  Music      Public    Videos     examples.desktop
root@kali:/mnt/cats/home/cats# ls -a
.          .cache    .profile  Public
..         .compiz   .xsession-errors  Templates
.ICEauthority .config   .xsession-errors.old  Videos
.Xauthority  .dbus     Desktop    catz
.bash_history .dmrc     Documents  examples.desktop
.bash_history~ .gconf    Downloads
```

Now, onto actually looking through this VM for a flag.

First, we look into the user's bash history (`.bash_history` or the backup file `.bash_history~` , in `/mnt/cats/home/catz/`) to see if they did anything in the terminal recently. We do this because there is often useful information in the `bash_history` , and it will likely point us in the right direction on how to solve this problem. In the `.bash_history` file, we only see `clear` , but in the backup of the bash history (`.bash_history~`) we get:

```
root@kali: /mnt/cats/home/cats
File Edit View Search Terminal Help
history
veracrypt --help
veracrypt -t -k "" --protexr-hidden=no catz /home/cats/catz
veracrypt -t -k "" --protect-hidden=no catz /home/cats/catz
veracrypt catz /media/veracrypt
gedit ~/.bash_history
ls
clear
clear
history
clear
veracrypt dismount
veracrypt dismount catz
veracrypt -help
veracrypt -d catz
clear
veracrypt -t -k "" --protect-hidden=no catz /home/cats/catz
veracrypt catz /media/veracrypt
veracrypt -d catz
clear
sudo gedit ~/.bash_history
cd var
clear
cd ..
cd var
clear
ls
cd ..
ls
cd vara
cd var
ls
cd log
ls
gedit logkeys.log
cat logkeys.log
```

It seems that there is some volume that has been encrypted by VeraCrypt (<https://veracrypt.codeplex.com/>)! This volume is conveniently located at `/home/cats/catz`, or in our case, `/mnt/cats/home/cats/catz` since we mounted the drive there.

In addition, we see many mentions of `logkeys.log`. What could it be? Let's take a look at that log file, in case it's relevant. We run `nano /mnt/cats/var/log/logkeys.log` and we see:

```
root@kali: /mnt/cats/home/cats
File Edit View Search Terminal Help
GNU nano 2.2.6 File: /mnt/cats/var/log/logkeys.log

sudo apt-get install build-essential
wget https://logkeys.googlecode.com/files/logkeys-.01.1a.tar.gz
wget https://logkeys.googlecode.com/files/logkeys-0.1.1a.tar.gz
tar xvzf logkeys-0.1.1a.tar.gz
cd logkeys-0.1.1a/
./configure
make
sudo make install
sudo locale-gen
sudo logkeys -s
sudo gedit ~/.bash_history
clear
clear
veracrypt -t -c
1
/home/cats/catz
128 M
1
2
2
Me0wL3tMeInPl$
Me0wL3tMeInPl$
vyiiviviparapvraivpyvriyfyipefiyewyfwvpfiyewvfhnfzslc hvbhawbvkLvhbsizbc awhbvua vawenvlfjvba;i vaw;vil;Vbhif$

"the quieter you become, the more you are able to hear"

^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```

From this, it seems that there was a keylogger running on the computer that logged everything that the user typed. This gives us the passphrase to decrypt the VeraCrypt (Me0wL3tMeInPl\$)!

(Note: this keylogger seems to have somehow logged its own installation. lol)

In order to decrypt the VeraCrypt in our Kali LiveCD, we have to first install VeraCrypt. Note: we aren't installing VeraCrypt on the hard disk, only on the Kali LiveCD that we're running from, so we maintain forensic integrity. We want the same version of the software that was used to create the encrypted volume, so that changes made in the newer versions will not affect the output. In order to find the version of VeraCrypt, we `grep -r "veracrypt"`, and we see that they used `veracrypt-1.0e`.

```
root@kali: /mnt/cats
File Edit View Search Terminal Help
ZZZ/grooming.pdf'
home/cats/.cache/upstart/dbus.log:RegisterDocument process pending invocations for URI file:///media/veracrypt/C
ATZZZ/grooming.pdf
home/cats/.cache/upstart/dbus.log:UnregisterDocument URI 'file:///media/veracrypt/CATZZZ/grooming.pdf'
Binary file home/cats/.cache/thumbnails/large/29c620ce768fa579c272a91d4c826911.png matches
Binary file home/cats/.cache/thumbnails/large/12b46e7a79809d7bf36cc1f2c59634ea.png matches
Binary file home/cats/.cache/thumbnails/large/fbc0e7f500e8e285a834c99fe54eb922.png matches
Binary file home/cats/.cache/thumbnails/large/16d24603dd56bc4e2c16840b9b771064.png matches
Binary file home/cats/.cache/thumbnails/large/44c7d0601865933a6d06850315d71984.png matches
Binary file home/cats/.cache/thumbnails/large/89f10a9bdd38bb86ac3b1f2f22ed72a2.png matches
Binary file home/cats/.cache/thumbnails/large/62bde07902c574514b0a9e9c3ce1f69c.png matches
Binary file home/cats/.cache/thumbnails/large/69e4e530b05f2e2f3d47b858bf4513a8.png matches
Binary file home/cats/.cache/thumbnails/large/d51aa4871380f0cb506d4fdeb83b99b2.png matches
Binary file home/cats/.cache/thumbnails/large/e929811a17933cad4745a7295bc78b7b.png matches
Binary file home/cats/.cache/thumbnails/large/01bab32c2794f68427bbafbfb5961efa.png matches
Binary file home/cats/.cache/thumbnails/large/77f70122124cecb3e6f00f18b0314044.png matches
Binary file home/cats/.cache/thumbnails/large/a85089f20f5fced874d1fb35f6fc432b.png matches
Binary file home/cats/.cache/thumbnails/large/6b3039a831c22e6febb5971679e5e675.png matches
Binary file home/cats/.cache/thumbnails/large/de12263ddb0717e7fd0cb5e944fff087.png matches
Binary file home/cats/Documents/Pictures/veracrypt-1.0e-setup-gui-x64 matches
Binary file home/cats/Documents/Pictures/veracrypt-1.0e-setup-console-x64 matches
Binary file home/cats/Documents/Pictures/veracrypt-1.0e-setup-console-x86 matches
Binary file home/cats/Documents/Pictures/veracrypt-1.0e-setup-gui-x86 matches
home/cats/.bash_history~:veracrypt --help
home/cats/.bash_history~:veracrypt -t -k "" --protectr-hidden=no catz /home/cats/catz
home/cats/.bash_history~:veracrypt -t -k "" --protect-hidden=no catz /home/cats/catz
home/cats/.bash_history~:veracrypt catz /media/veracrypt
home/cats/.bash_history~:veracrypt dismount
home/cats/.bash_history~:veracrypt dismount catz
home/cats/.bash_history~:veracrypt -help
home/cats/.bash_history~:veracrypt -d catz
home/cats/.bash_history~:veracrypt -t -k "" --protect-hidden=no catz /home/cats/catz
home/cats/.bash_history~:veracrypt catz /media/veracrypt
home/cats/.bash_history~:veracrypt -d catz
^C
root@kali:/mnt/cats#
```

So, we just fire up a browser and install veracrypt-1.0e .

VeraCrypt - Download: VeraCrypt version 1.0e - Iceweasel

VeraCrypt - Downlo... x

https://veracrypt.codeplex.com/releases/view/132239

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB

CodePlex Project Hosting for Open Source Software Register Sign In Search all projects

VeraCrypt


HOME SOURCE CODE **DOWNLOADS** DOCUMENTATION DISCUSSIONS ISSUES PEOPLE LICENSE

Subscribe

VeraCrypt version 1.0e

Rating: ★★★★★ Based on 3 ratings Reviewed: 1 review Downloads: 69258 Change Set: 06a3ab63efee	Released: Sep 4, 2014 Updated: Dec 2, 2014 by idrassi Dev status: Stable ?
--	---

RECOMMENDED DOWNLOAD

 VeraCrypt version 1.0e
application, 5609K, uploaded Sep 4, 2014 - 42852 downloads

OTHER AVAILABLE DOWNLOADS

OTHER DOWNLOADS

Released | Planned

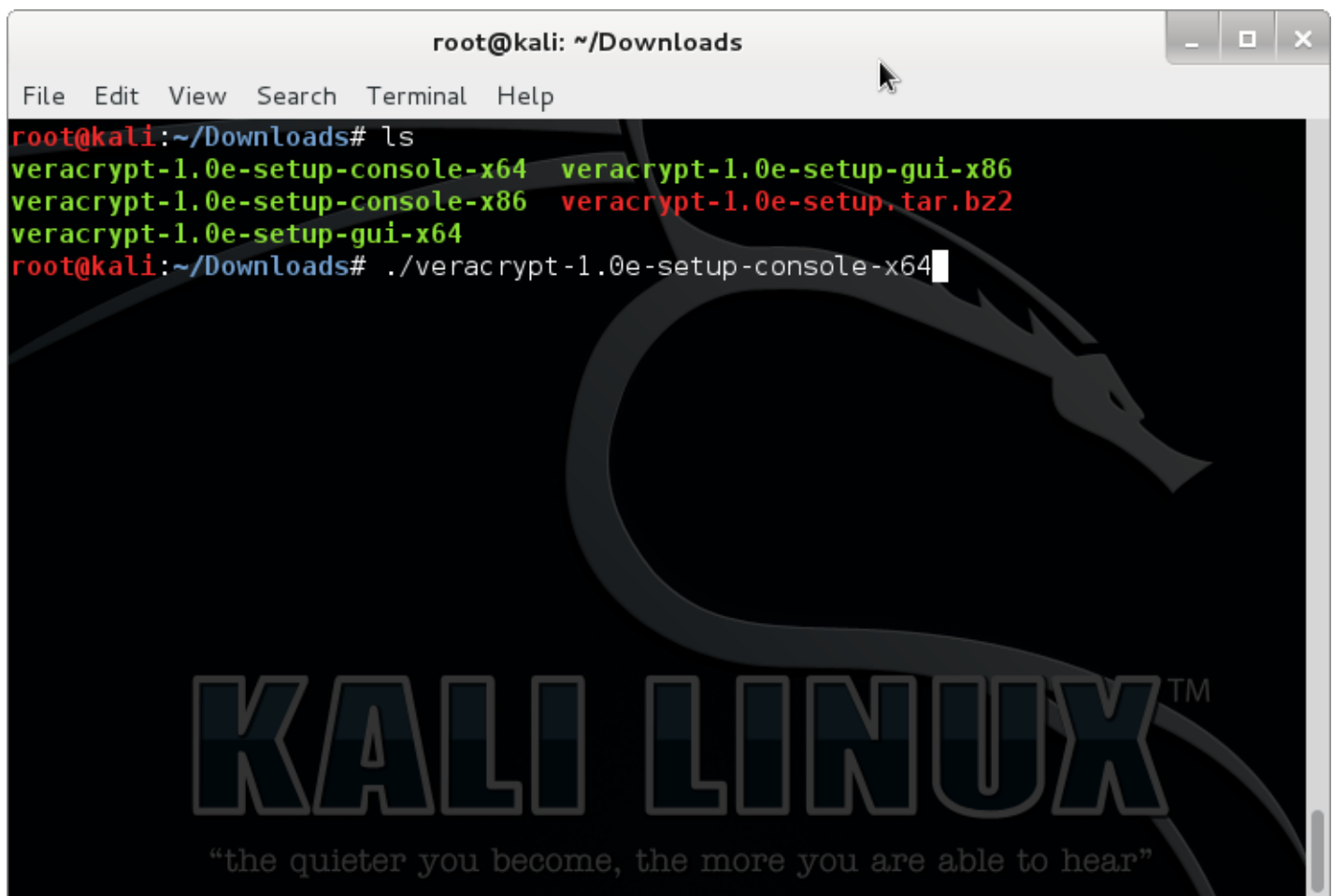
- ★ VeraCrypt version 1.16
Oct 7, 2015, Stable
★★★★★
- VeraCrypt version 1.0f-2
Apr 5, 2015, Stable
★★★★★
- VeraCrypt version 1.0f Beta3
Dec 20, 2014, Beta
★★★★★
- VeraCrypt version 1.0f Beta
Oct 26, 2014, Beta
★★★★★

Release notifications

After downloading the Linux version, we install it by unzipping the file, going to the file location (~/Downloads) and then running:

`./veracrypt-1.0e-setup-console-x64` , selecting install, and accepting the terms and conditions.

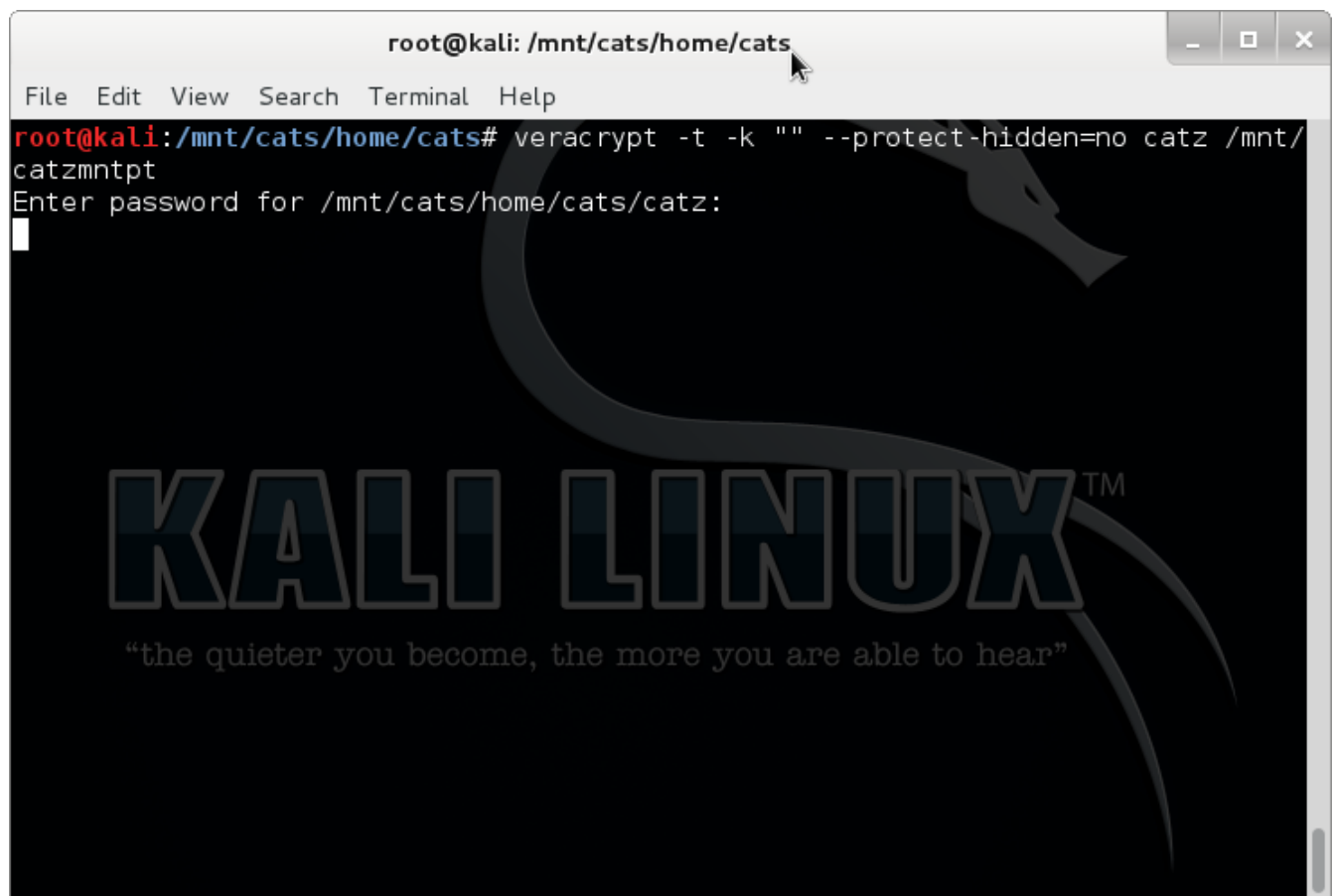

```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# ls
veracrypt-1.0e-setup-console-x64  veracrypt-1.0e-setup-gui-x86
veracrypt-1.0e-setup-console-x86  veracrypt-1.0e-setup.tar.bz2
veracrypt-1.0e-setup-gui-x64
root@kali:~/Downloads# ./veracrypt-1.0e-setup-console-x64
```



After installing, we just use VeraCrypt to decrypt the encrypted `catz` file!

All we need to do is copy pretty much everything we find in the `logkeys.log` file. After a while, VeraCrypt successfully decrypted the file and mounted it. What we typed was:


1. First make the mount point. `mkdir /mnt/catzmntpt`
2. Decrypt and mount the file: `veracrypt -t -k "" --protect-hidden=no catz /mnt/catzmntpt`



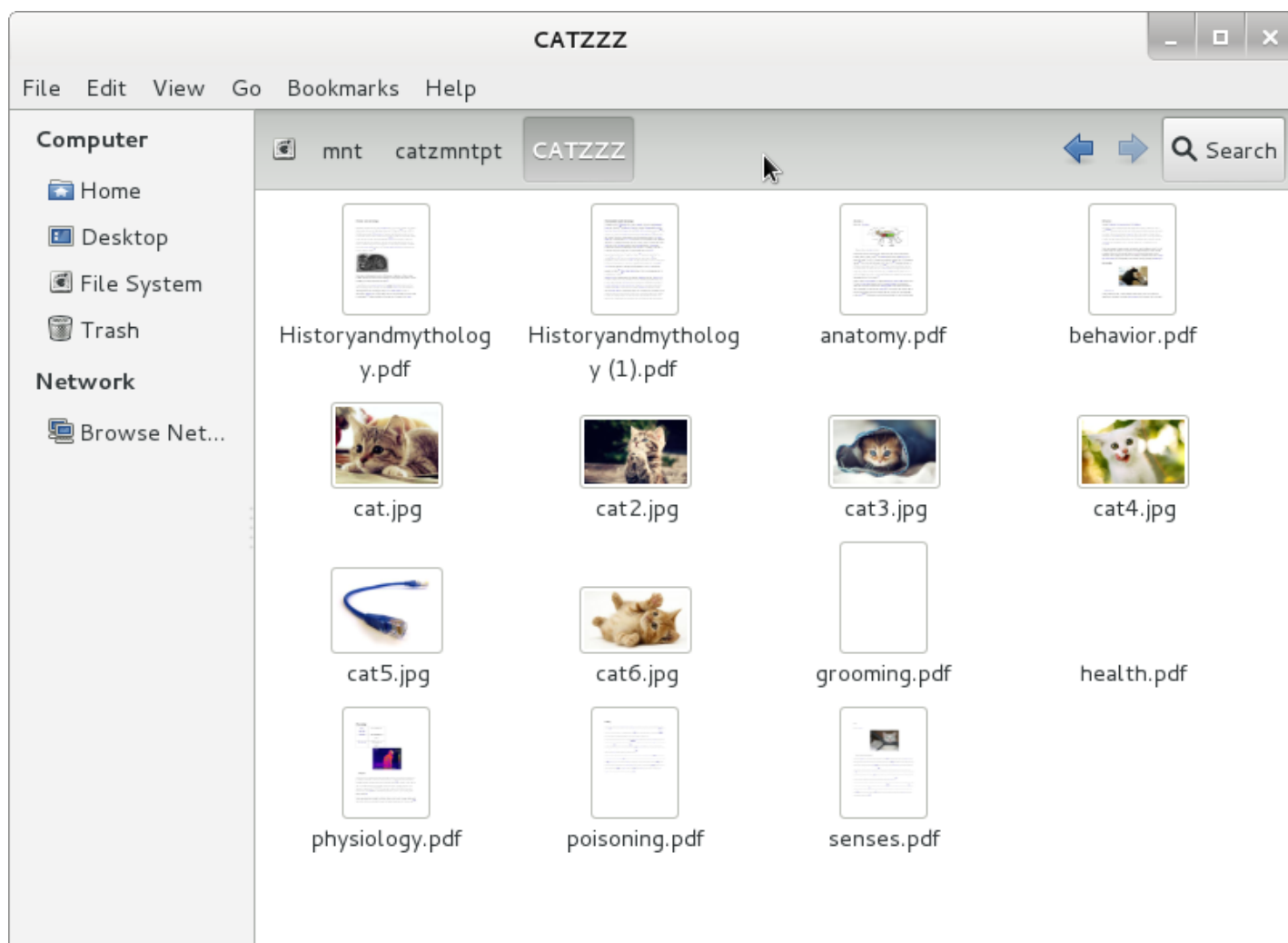
3. Password: Me0wL3tMeInPl\$

In the newly mounted drive, we see a CATZZZ folder, which has lots of files.

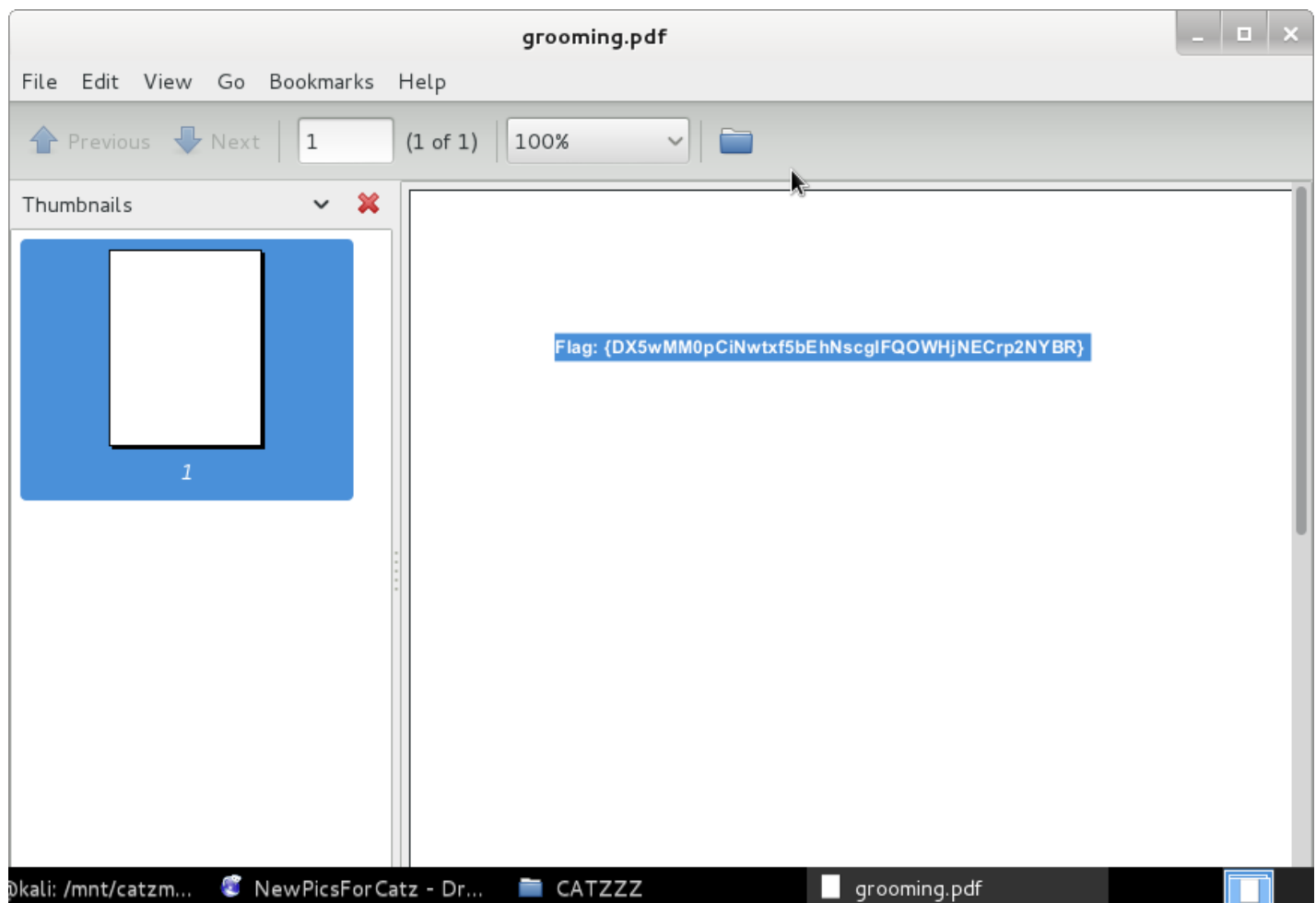
```
root@kali: /mnt/catzmntpt/CATZZZ
File Edit View Search Terminal Help
root@kali:/mnt/catzmntpt# ls -a
.  ..  .bash_history  .cache  .config  .local  CATZZZ
root@kali:/mnt/catzmntpt# cd CATZZZ
root@kali:/mnt/catzmntpt/CATZZZ# ls -a
.  ..  anatomy.pdf  cat3.jpg  grooming.pdf  senses.pdf
.  ..  behavior.pdf  cat4.jpg  health.pdf
Historyandmythology (1).pdf  cat.jpg  cat5.jpg  physiology.pdf
Historyandmythology.pdf  cat2.jpg  cat6.jpg  poisoning.pdf
root@kali:/mnt/catzmntpt/CATZZZ#
```



In file viewer, we see that many of these files have pictures and/or text in them. However, the thumbnail of grooming.pdf is blank.



That seems pretty suspicious. So, we open it, and select all.



There's the flag!

```
{DX5wMM0pCiNwtxf5bEhNscglFQOWHjNECrp2NYBR}
```

If this were a real forensic investigation, though, it wouldn't be over yet. Now we need to show that we made no changes to the hard disk. To do this, we just hash `/dev/sda1` again (`openssl sha1 /dev/sda1`), and out we get:

```
ccef3f6b74e943d0e020de56c992bccd21de09af
```

```
root@kali: /mnt/catzmntpt/CATZZZ
File Edit View Search Terminal Help
root@kali:/mnt/catzmntpt/CATZZZ# ls
Historyandmythology (1).pdf  cat.jpg      cat5.jpg      physiology.pdf
Historyandmythology.pdf     cat2.jpg     cat6.jpg      poisoning.pdf
anatomy.pdf                 cat3.jpg     grooming.pdf  senses.pdf
behavior.pdf                cat4.jpg     health.pdf
root@kali:/mnt/catzmntpt/CATZZZ# openssl sha1 /dev/sda1
SHA1(/dev/sda1)= ccef3f6b74e943d0e020de56c992bccd21de09af
root@kali:/mnt/catzmntpt/CATZZZ#
```

It matches with our first hash! So we have maintained forensic integrity while getting ourselves 450 points.

Writeup by PHS Absol.

Work Division:

Downloaded the VM and found stuff on it, made the video - Plato2000

Gave forensic integrity tips, wrote the writeup - Neptunia

Found the flag in the decrypted files - Flareboot