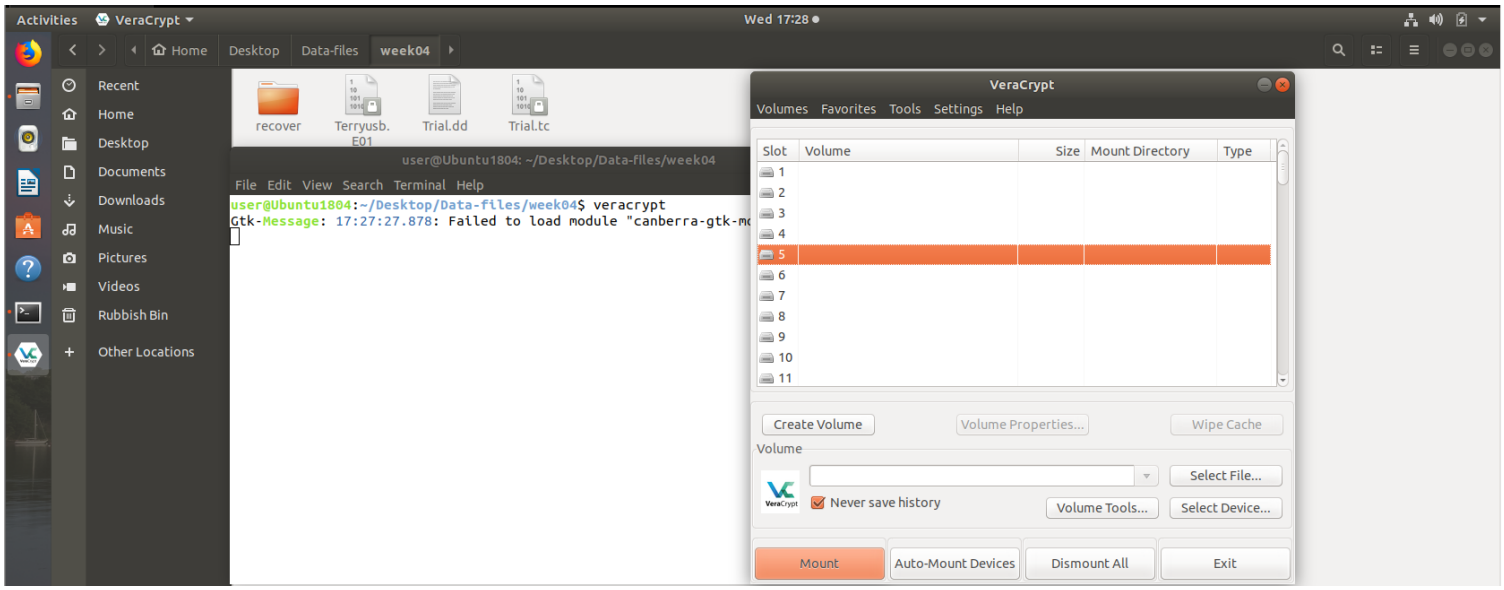
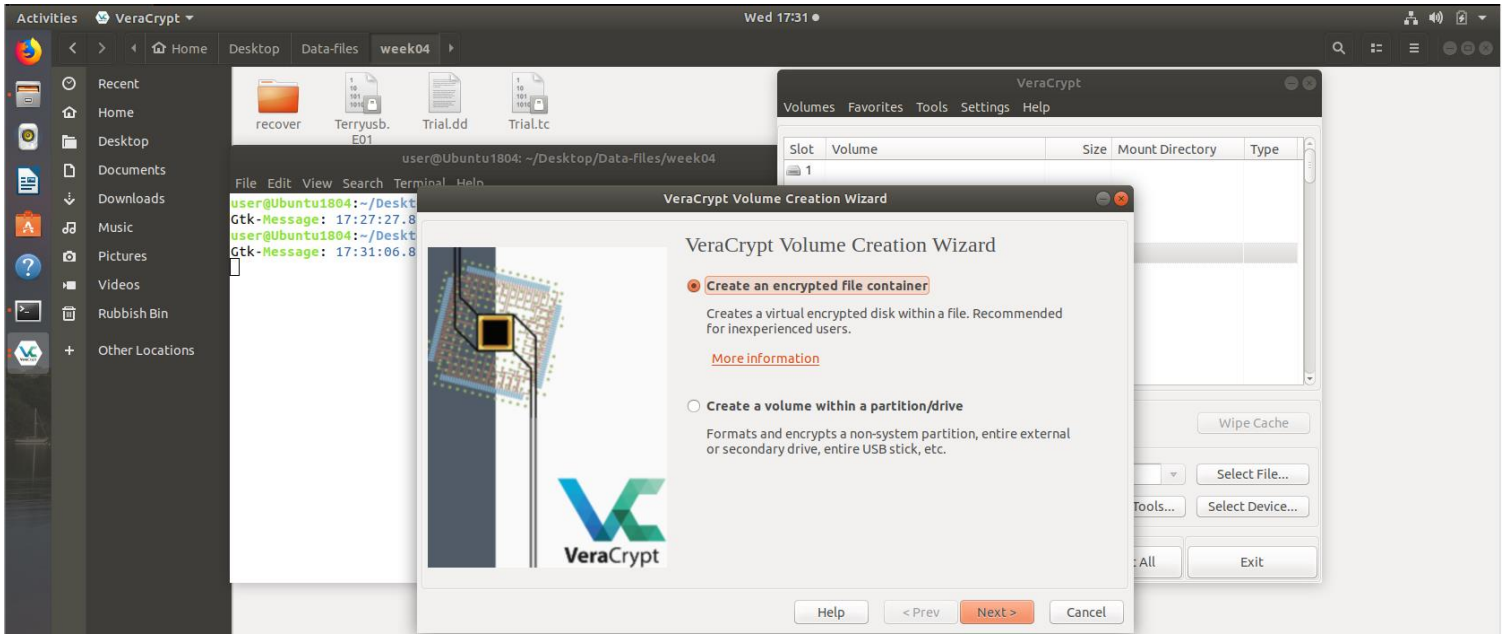
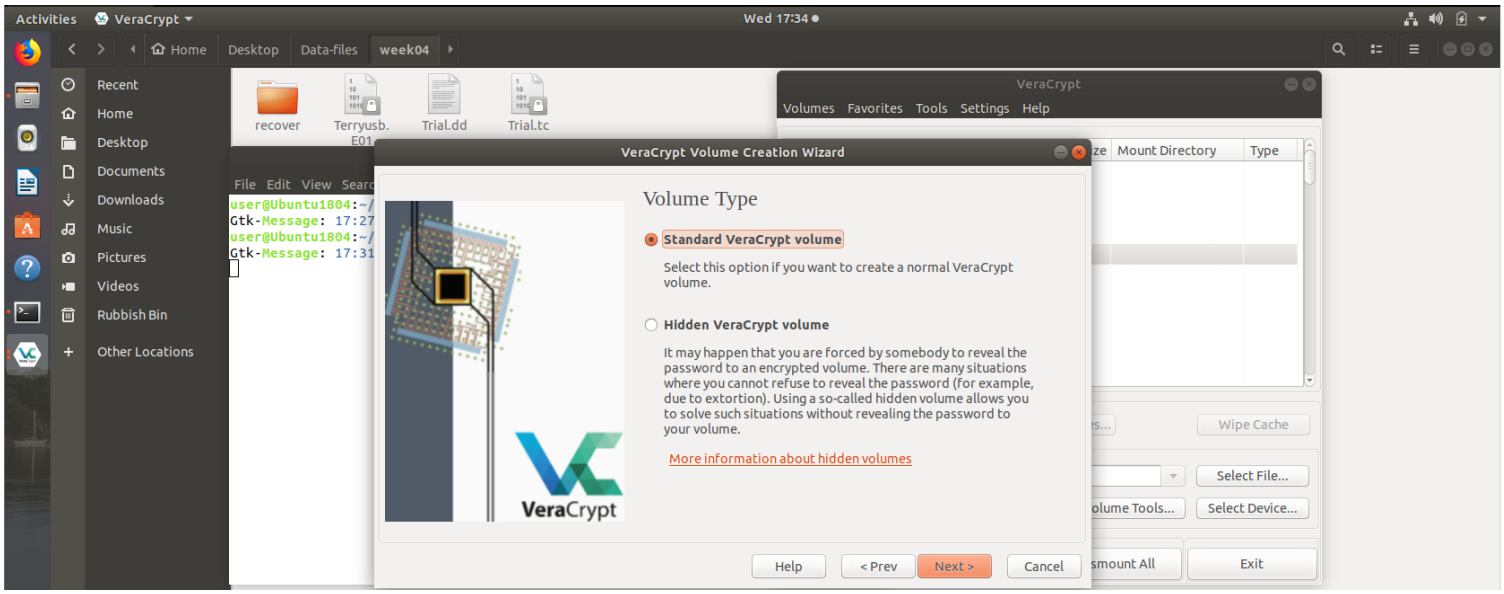
Introducing VeraCrypt

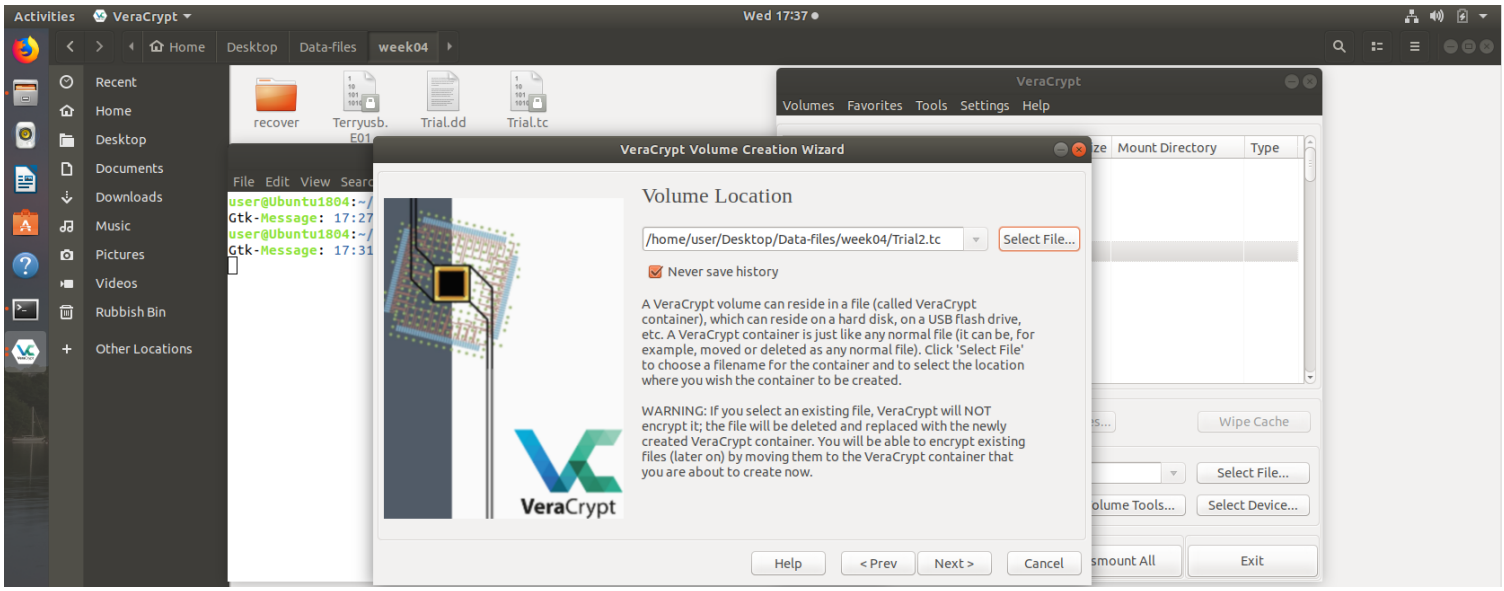
I start by studying about VeraCrypt, which is a program that replaced TrueCrypt. I start a new encrypted volume by opening VeraCrypt from the terminal and carefully following the instructions to make sure I don't lose any current files.



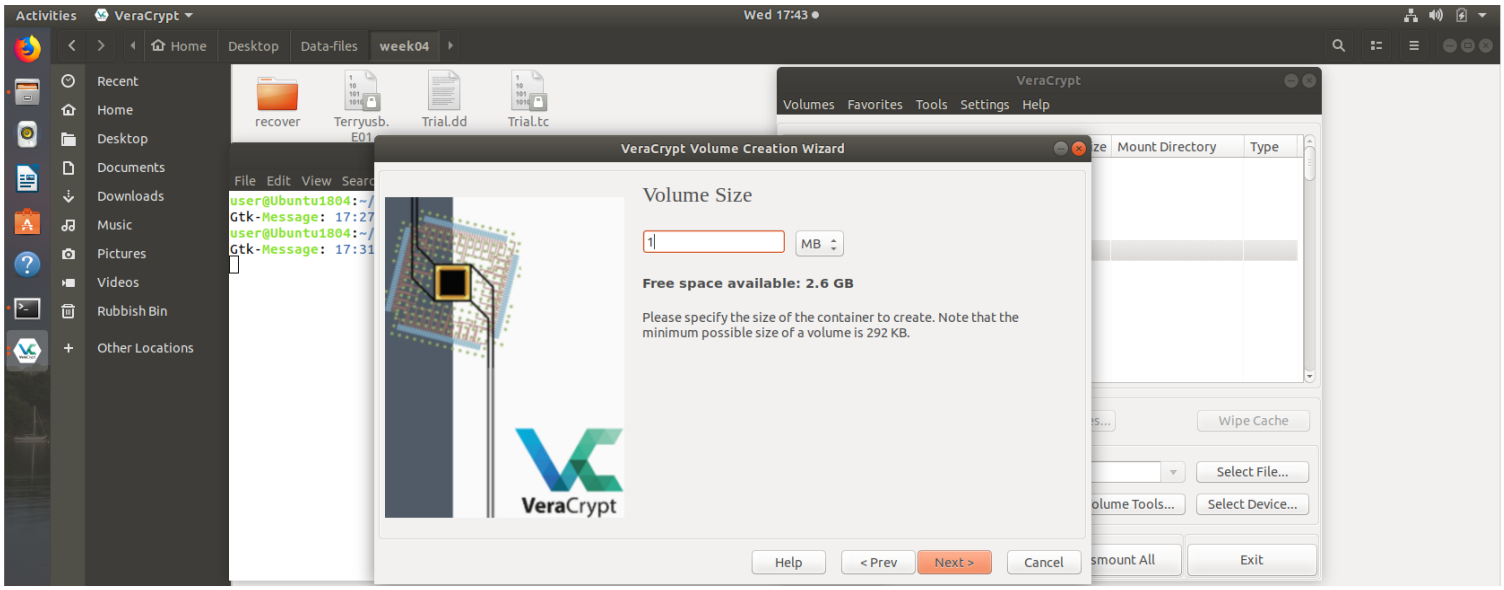
I utilize the ~/Desktop/Data-files/week04 directory and use the password deakin to create a file called Trial2.tc. I use the FAT file system to format it.



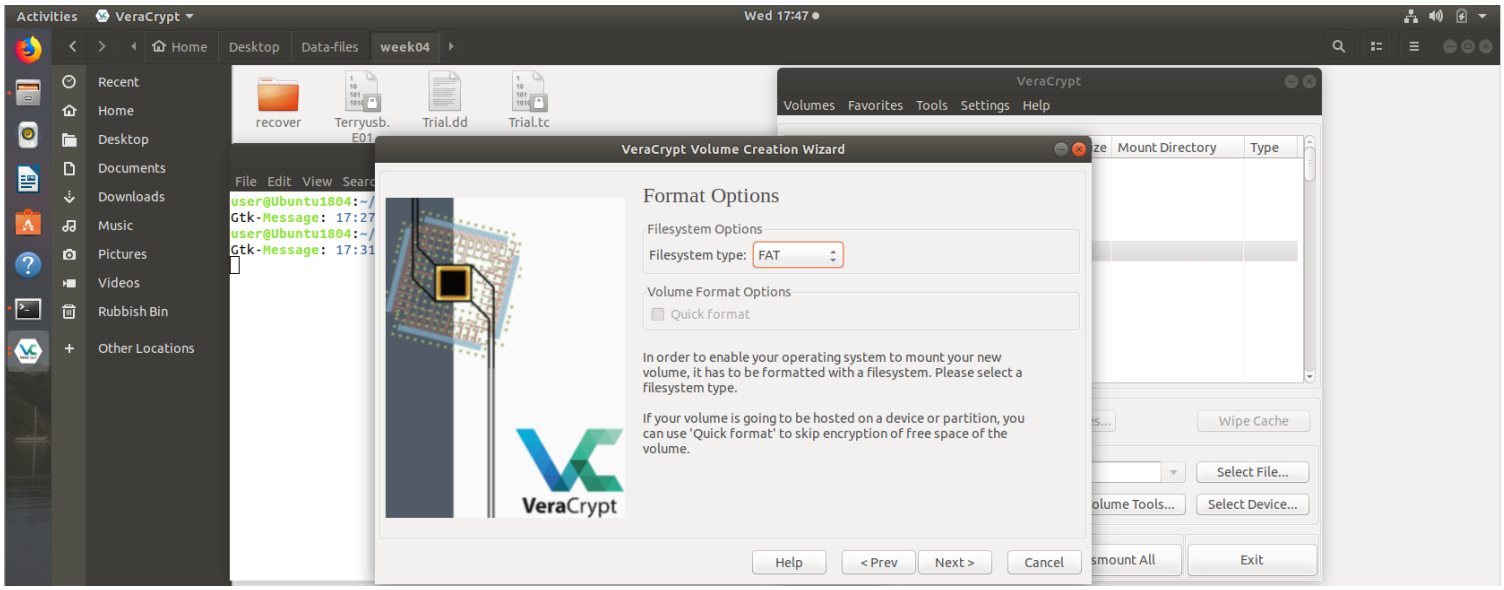

Activities
VeraCrypt
Wed 17:34
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.
Trial.dd
Trial.tc
VeraCrypt
Volumes Favorites Tools Settings Help
Mount Directory
Type
Wipe Cache
Select File...
Select Device...
Exit
VeraCrypt Volume Creation Wizard
Volume Type
Standard VeraCrypt volume
Select this option if you want to create a normal VeraCrypt volume.
Hidden VeraCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More information about hidden volumes
Help
< Prev
Next >
Cancel

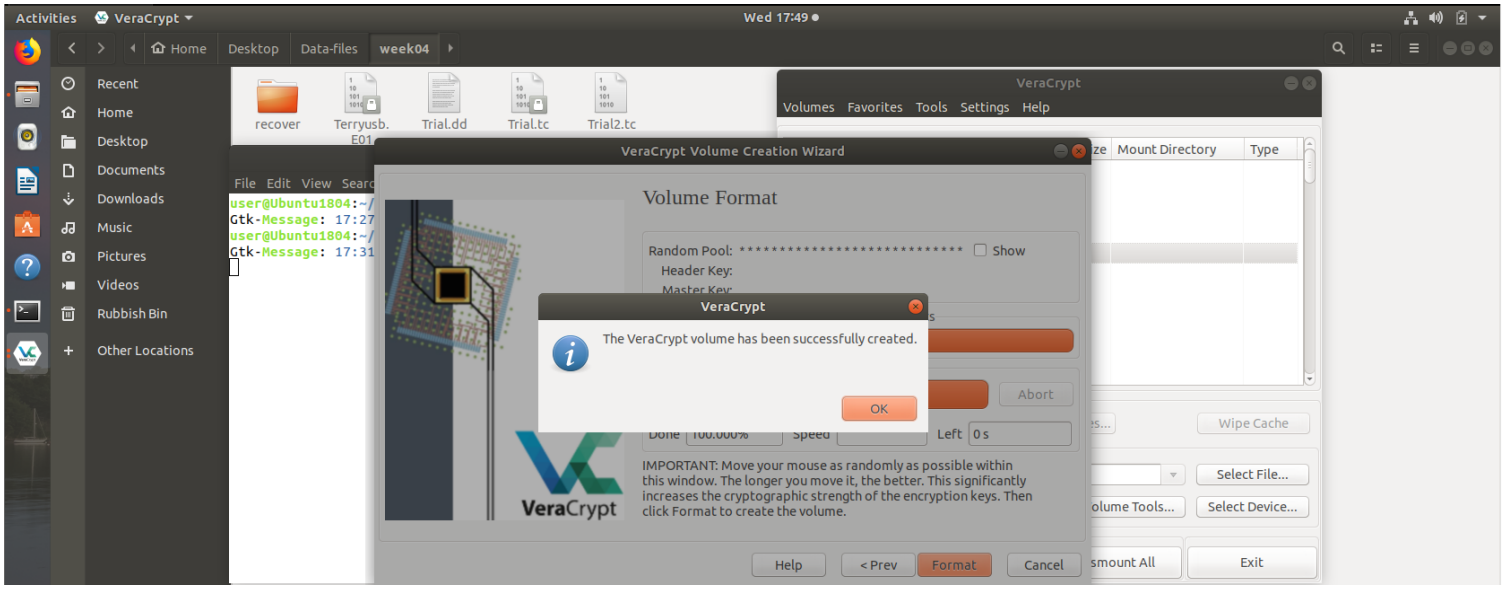

Activities
VeraCrypt
Wed 17:37
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.
Trial.dd
Trial.tc
VeraCrypt
Volumes Favorites Tools Settings Help
Mount Directory
Type
Wipe Cache
Select File...
Select Device...
Exit
VeraCrypt Volume Creation Wizard
Volume Location
/home/user/Desktop/Data-files/week04/Trial2.tc
Select File...
Never save history
A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.
Help
< Prev
Next >
Cancel


Activities
VeraCrypt
Wed 17:42
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.
Trial.dd
Trial.tc
VeraCrypt
Volumes Favorites Tools Settings Help
Mount Directory
Type
Wipe Cache
Select File...
Select Device...
Exit
VeraCrypt Volume Creation Wizard
Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
SHA-512
Information on hash algorithms
Help
< Prev
Next >
Cancel

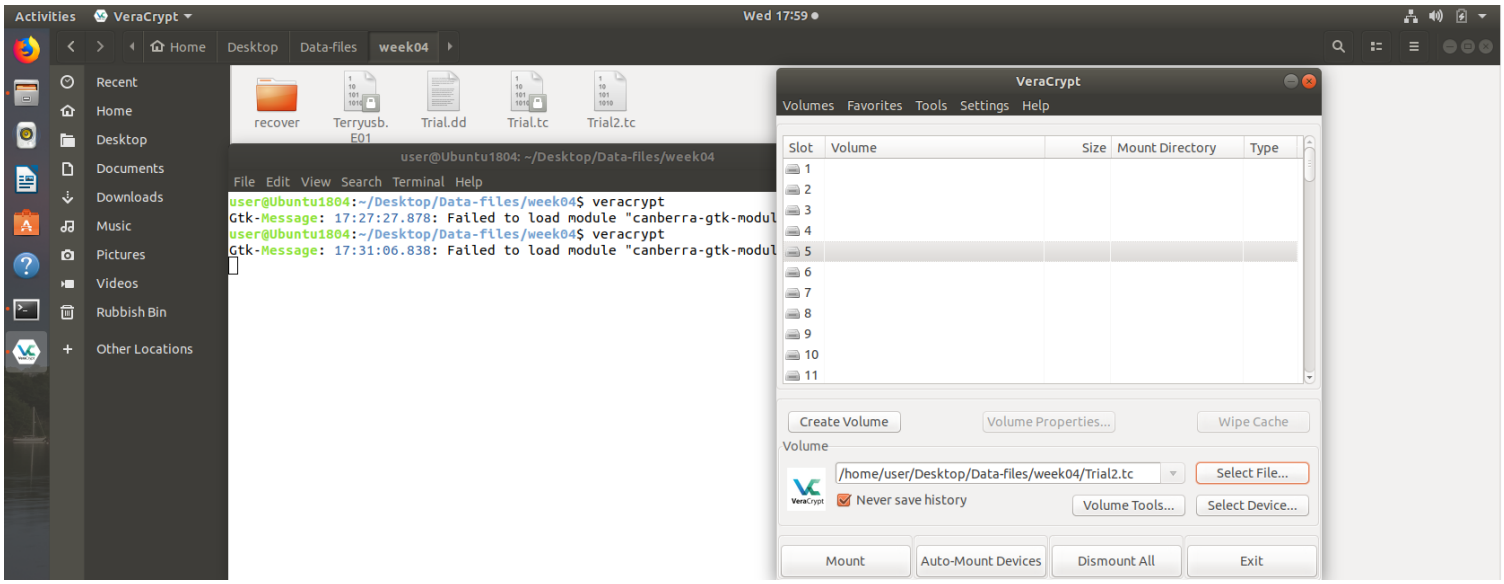

Activities
VeraCrypt
Wed 17:43
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.E01
Trial.dd
Trial.tc
VeraCrypt Volume Creation Wizard
Volume Size
1
MB
Free space available: 2.6 GB
Please specify the size of the container to create. Note that the minimum possible size of a volume is 292 KB.
VeraCrypt
Help
< Prev
Next >
Cancel
VeraCrypt
Volumes
Favorites
Tools
Settings
Help
Mount Directory
Type
Wipe Cache
Select File...
Select Device...
Exit

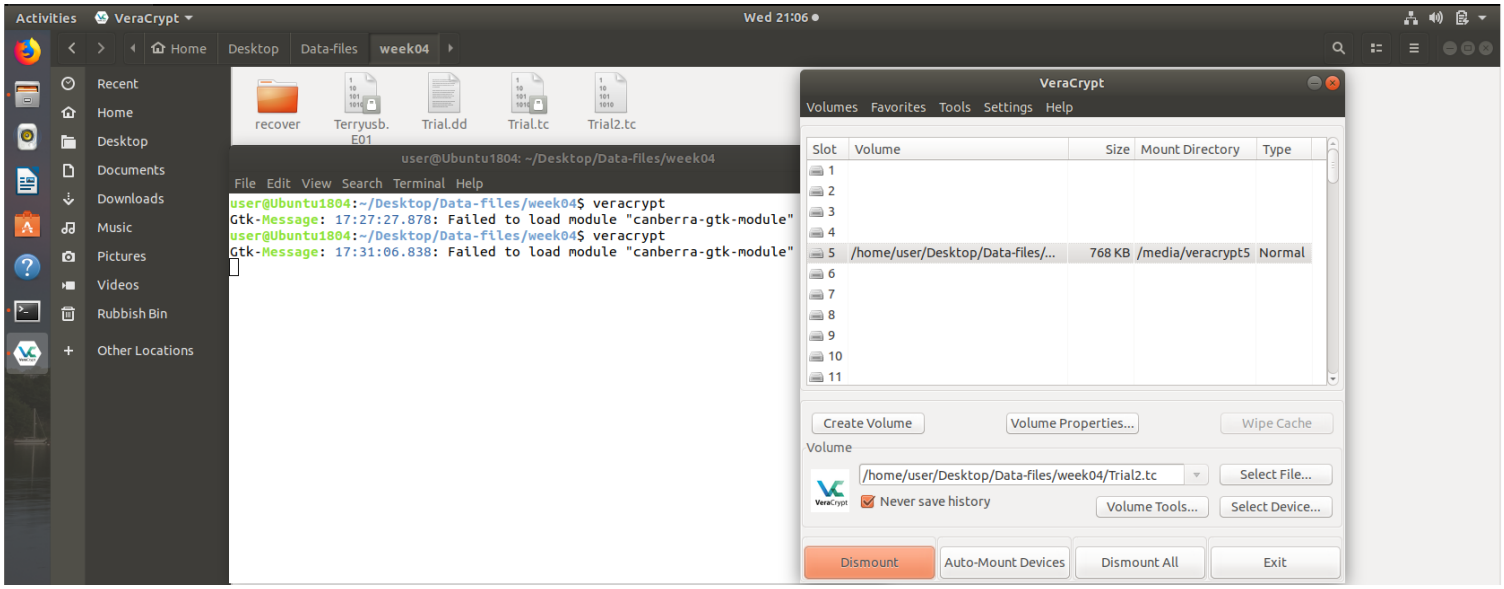

Activities
VeraCrypt
Wed 17:44
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.E01
Trial.dd
Trial.tc
VeraCrypt Volume Creation Wizard
Volume Password
Password: deakin
Confirm password: deakin
Use PIM
Display password
Use keyfiles
Keyfiles...
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters.
VeraCrypt
Help
< Prev
Next >
Cancel
VeraCrypt
Volumes
Favorites
Tools
Settings
Help
Mount Directory
Type
Wipe Cache
Select File...
Select Device...
Exit


Activities
VeraCrypt
Wed 17:47
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.E01
Trial.dd
Trial.tc
VeraCrypt Volume Creation Wizard
Format Options
Filesystem Options
Filesystem type: FAT
Volume Format Options
Quick format
In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type.
If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.
VeraCrypt
Help
< Prev
Next >
Cancel
VeraCrypt
Volumes
Favorites
Tools
Settings
Help
Mount Directory
Type
Wipe Cache
Select File...
Select Device...
Exit

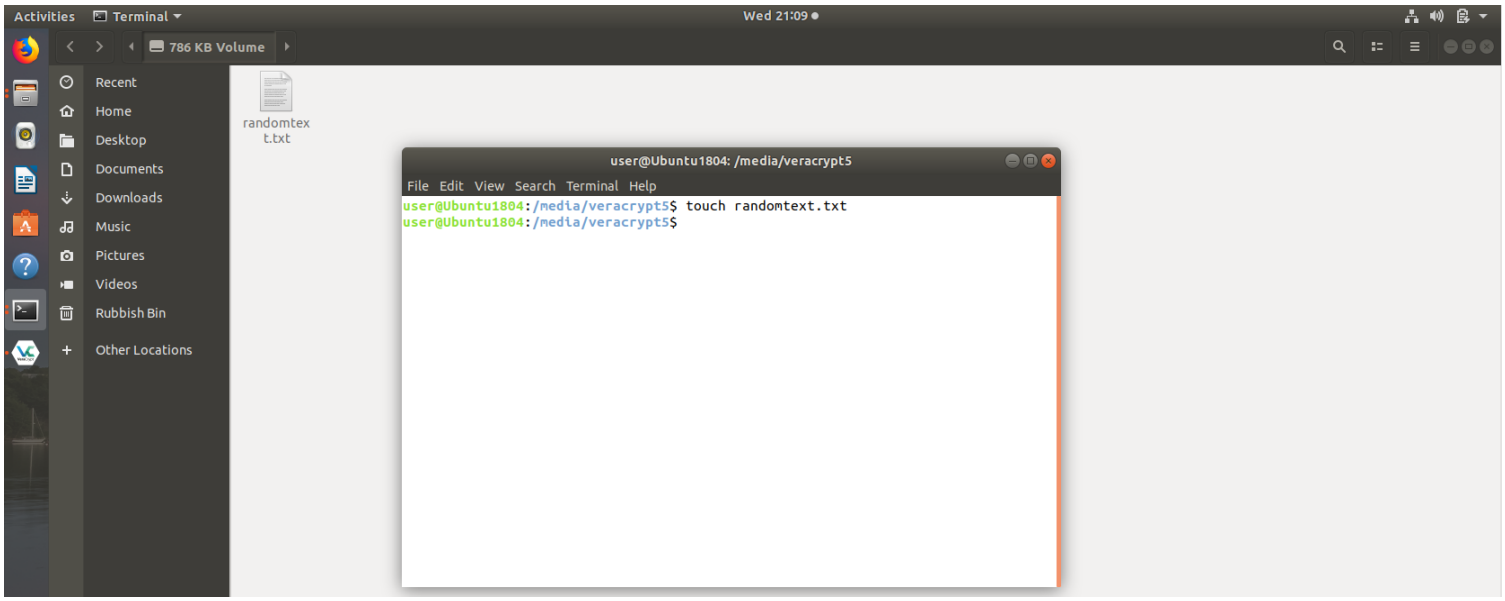

Activities
VeraCrypt
Wed 17:49
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.E01
Trial.dd
Trial.tc
Trial2.tc
VeraCrypt
Volumes Favorites Tools Settings Help
Mount Directory
Type
VeraCrypt Volume Creation Wizard
Volume Format
Random Pool:
Show
Header Key:
VeraCrypt
The VeraCrypt volume has been successfully created.
OK
Abort
Left 0 s
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help
< Prev
Format
Cancel
Wipe Cache
Select File...
Select Device...
Exit
File Edit View
user@Ubuntu1804:~/
Gtk-Message: 17:27
Gtk-Message: 17:31


Activities
VeraCrypt
Wed 17:51
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.E01
Trial.dd
Trial.tc
Trial2.tc
VeraCrypt
Volumes Favorites Tools Settings Help
Mount Directory
Type
VeraCrypt Volume Creation Wizard
Volume Created
The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next.
Otherwise, click Exit.
Help
< Prev
Next >
Exit
Wipe Cache
Select File...
Select Device...
Exit
File Edit View
user@Ubuntu1804:~/
Gtk-Message: 17:27
Gtk-Message: 17:31

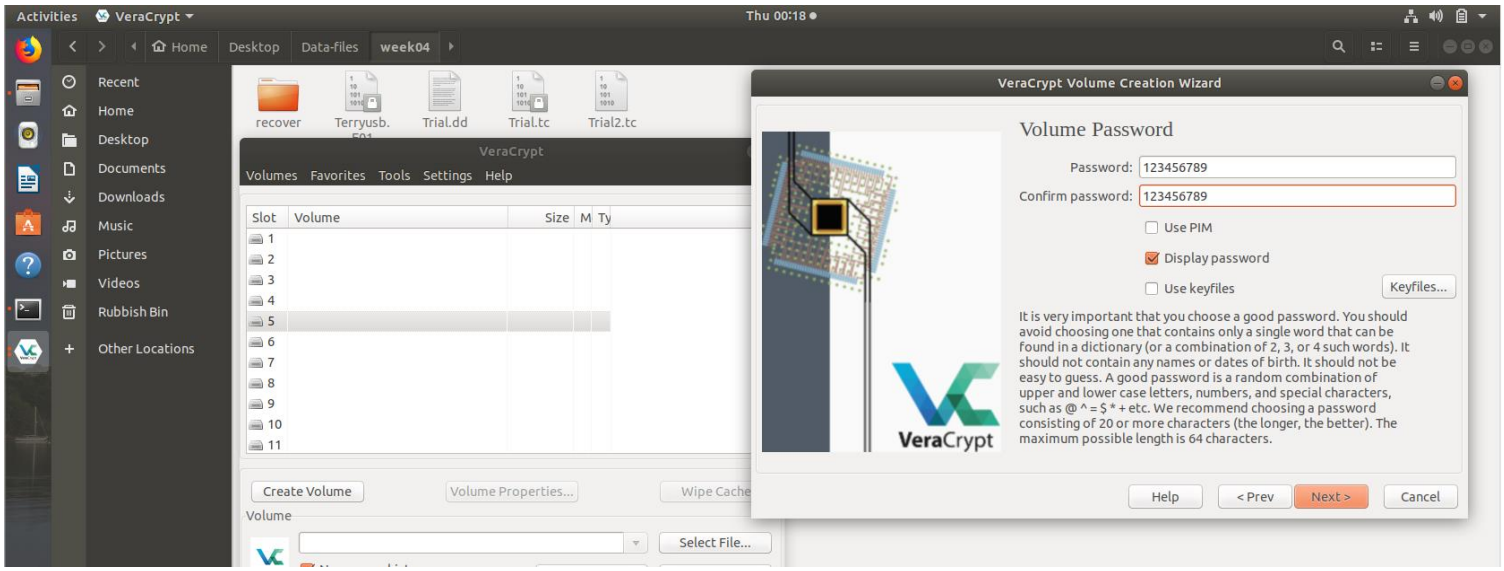

Activities
VeraCrypt
Wed 17:59
Home
Desktop
Data-files
week04
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Rubbish Bin
Other Locations
recover
Terryusb.E01
Trial.dd
Trial.tc
Trial2.tc
user@Ubuntu1804: ~/Desktop/Data-files/week04
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week04$ veracrypt
Gtk-Message: 17:27:27.878: Failed to load module "canberra-gtk-modul
user@Ubuntu1804:~/Desktop/Data-files/week04$ veracrypt
Gtk-Message: 17:31:06.838: Failed to load module "canberra-gtk-modul
VeraCrypt
Volumes Favorites Tools Settings Help
Slot
Volume
Size
Mount Directory
Type
1
2
3
4
5
6
7
8
9
10
11
Create Volume
Volume Properties...
Wipe Cache
Volume
/home/user/Desktop/Data-files/week04/Trial2.tc
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

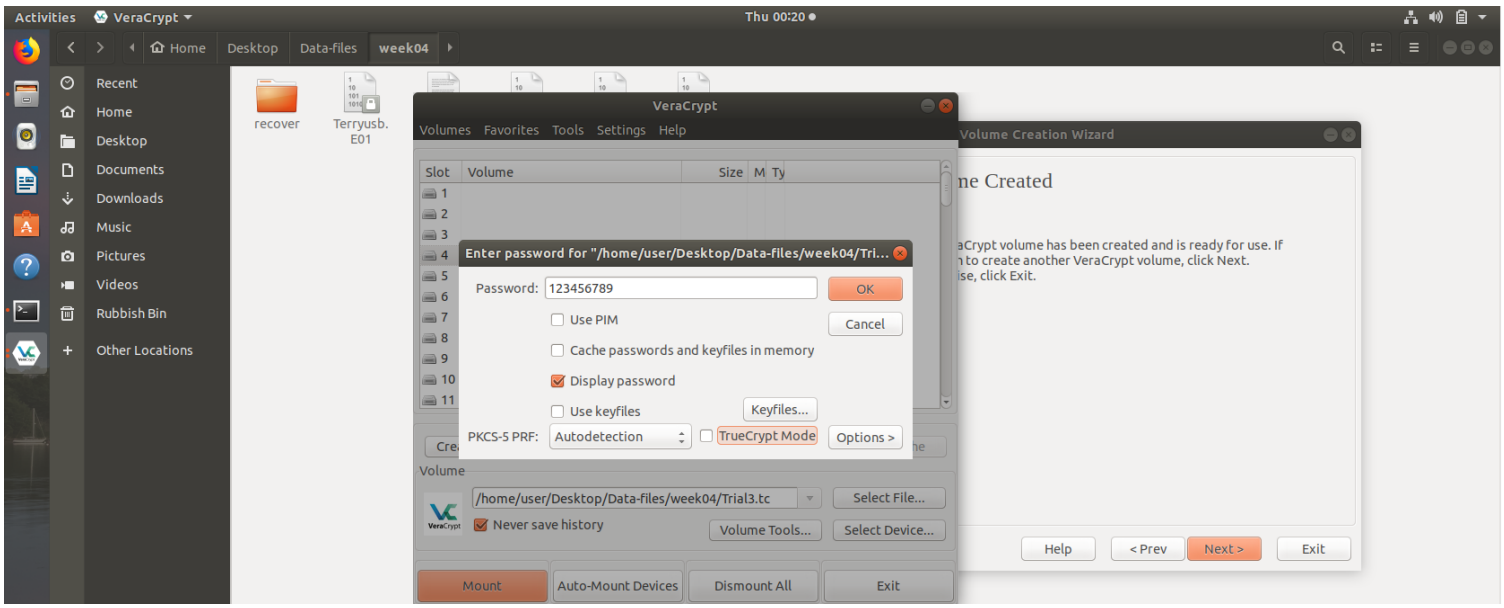


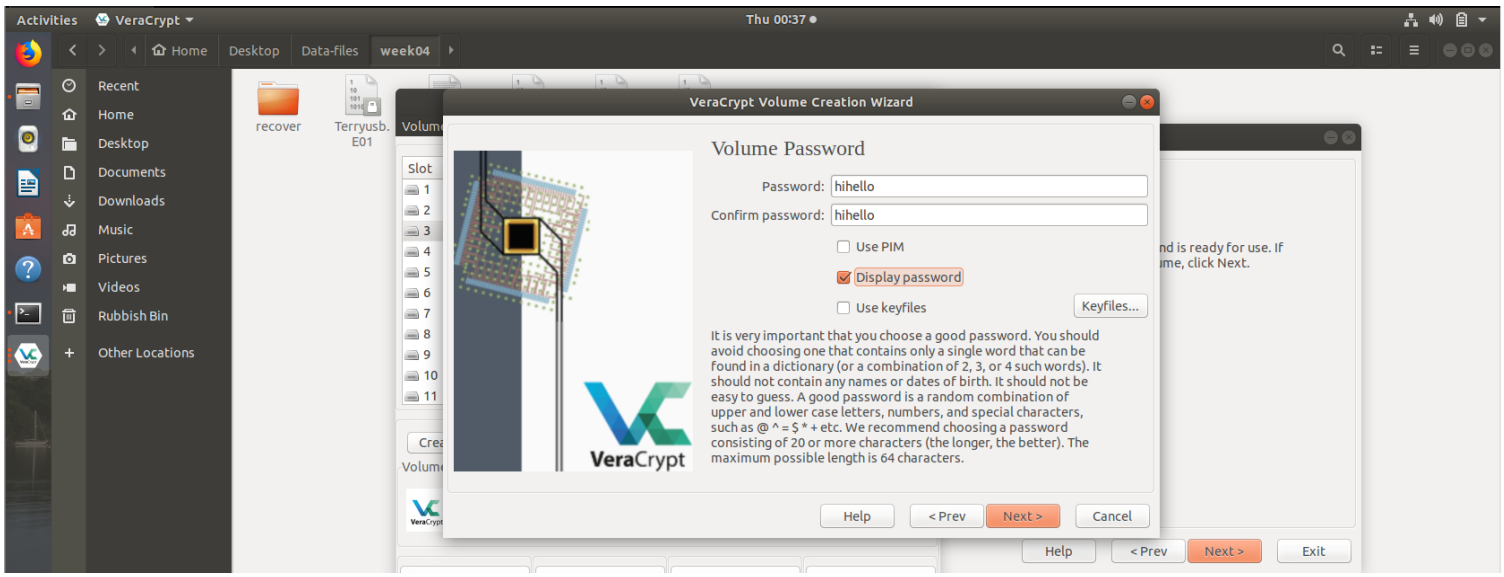
I created the volume, mounted it to Drive 5, put some text on it at random, unmount it, and then close VeraCrypt.

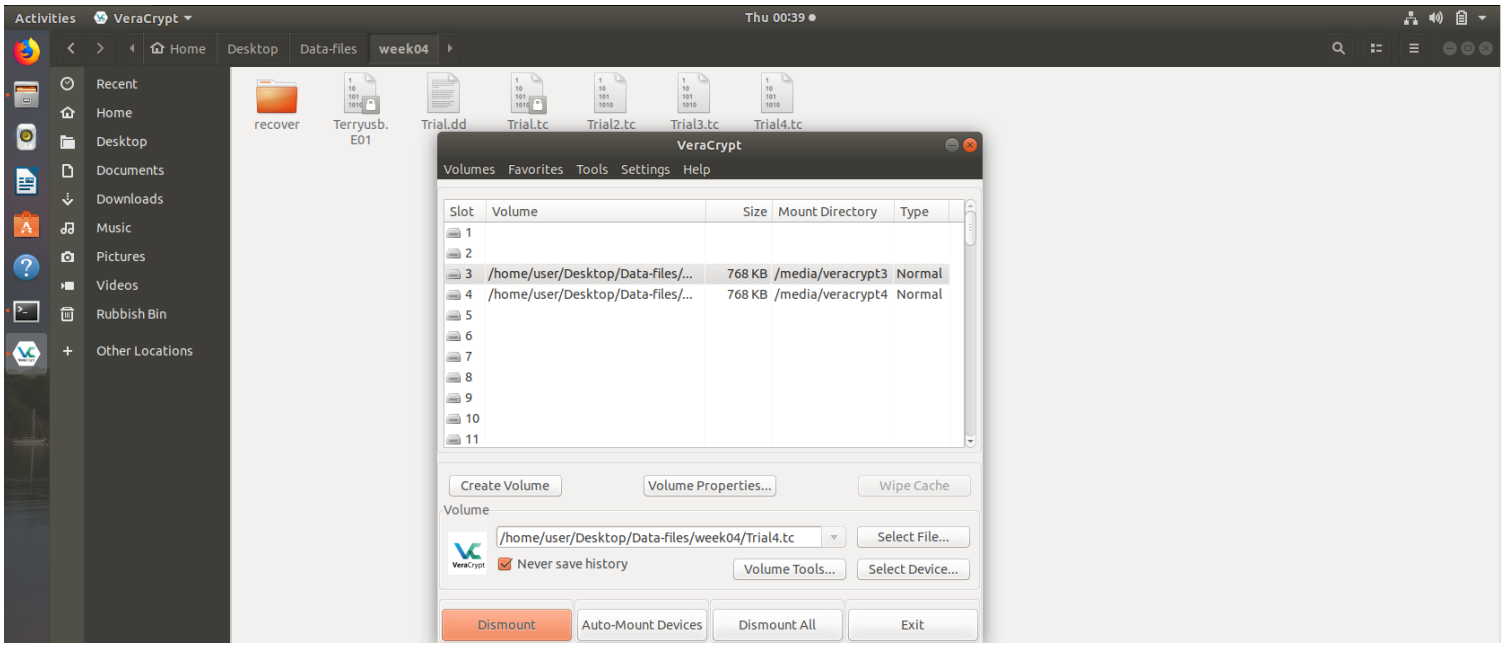


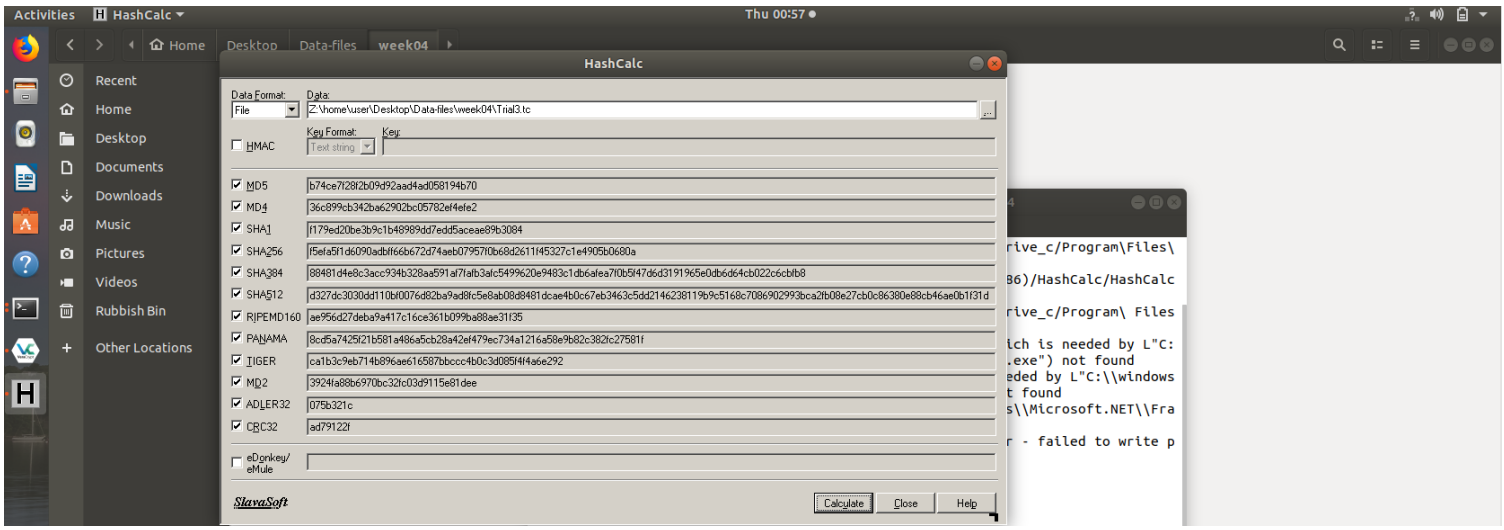
I encrypt two 1MB VeraCrypt volumes using distinct passwords in order to comprehend the encryption patterns. I then compare the hash values of the volumes to see if any patterns can be found.

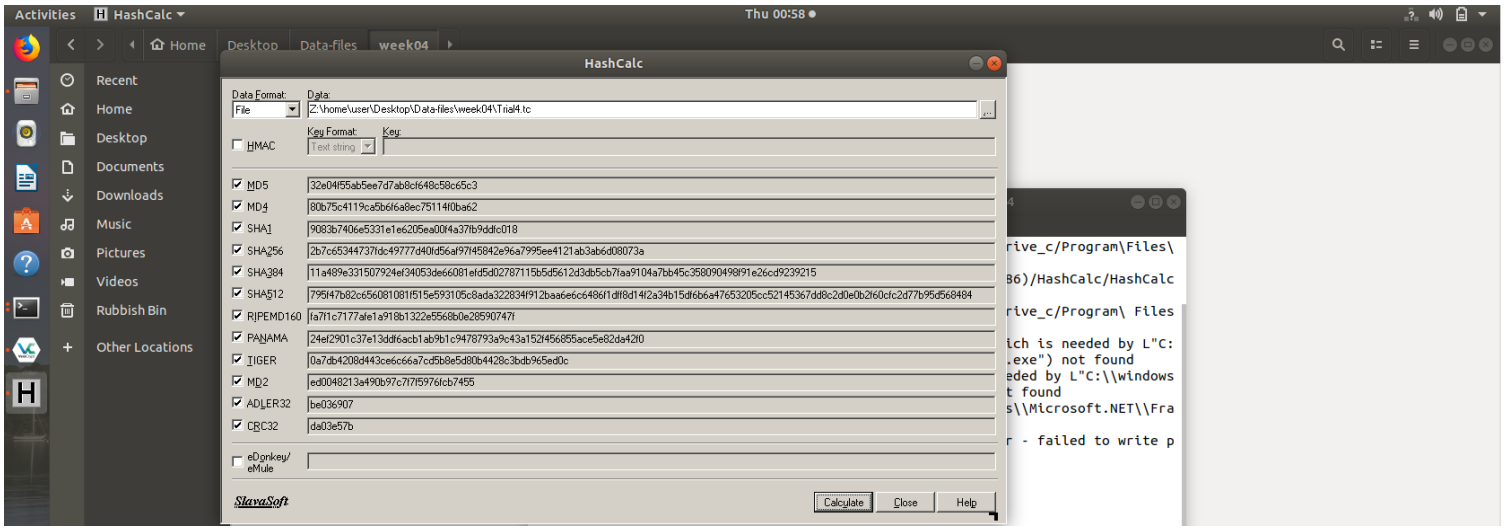










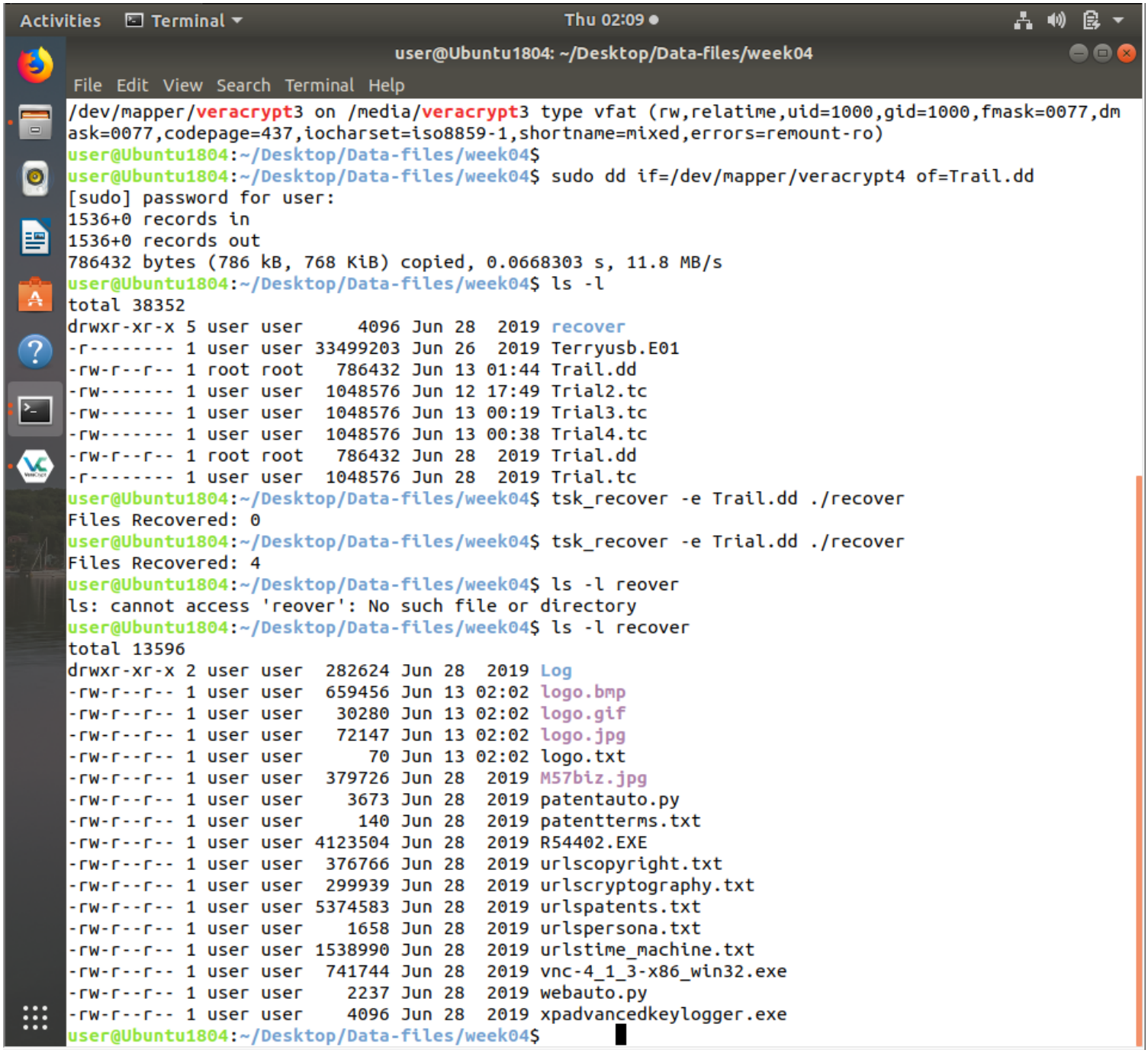


The hash values are not the same for the 2 volumes created using different passwords

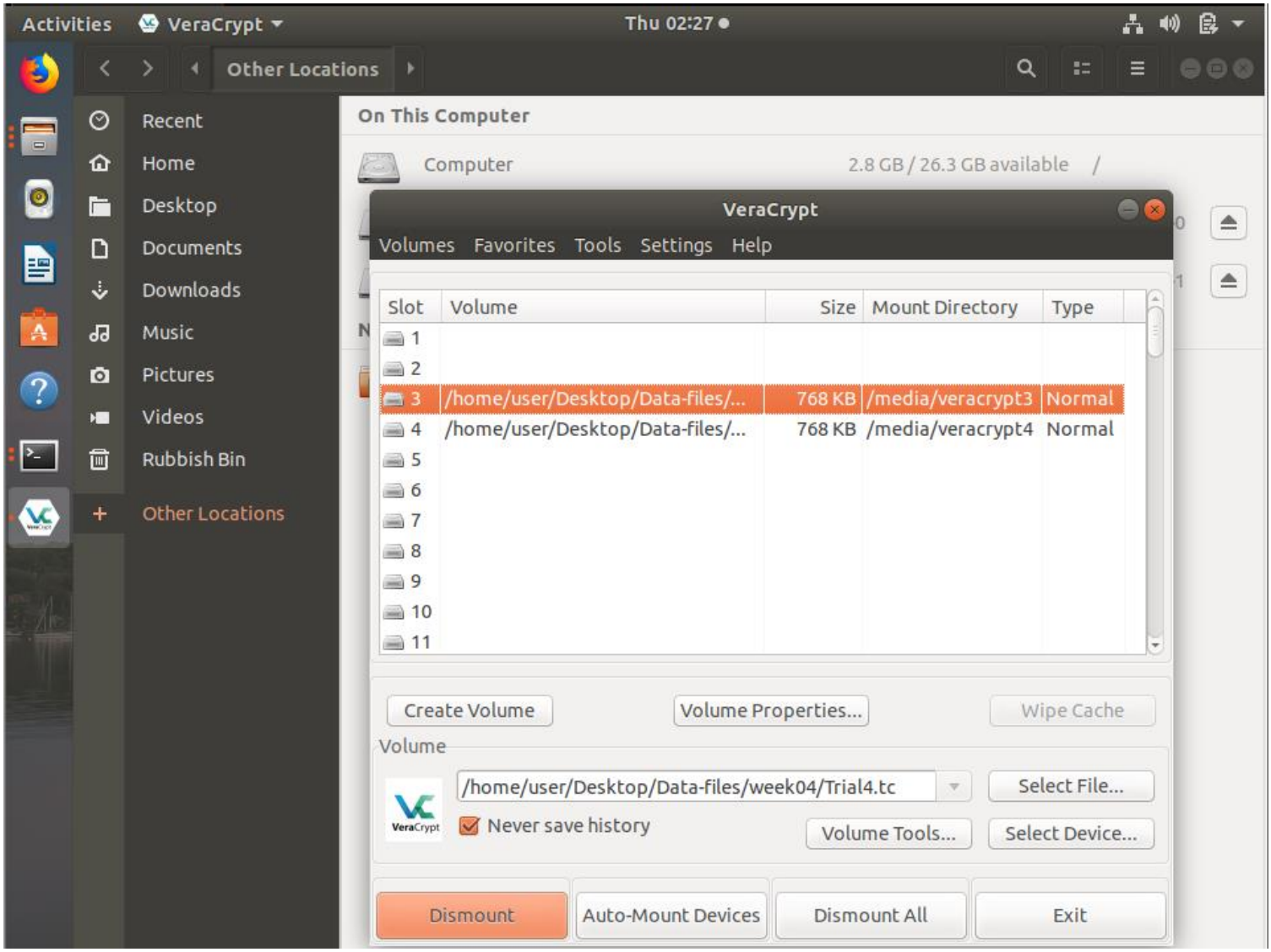
Recovering Items of a Mounted VeraCrypt Volume

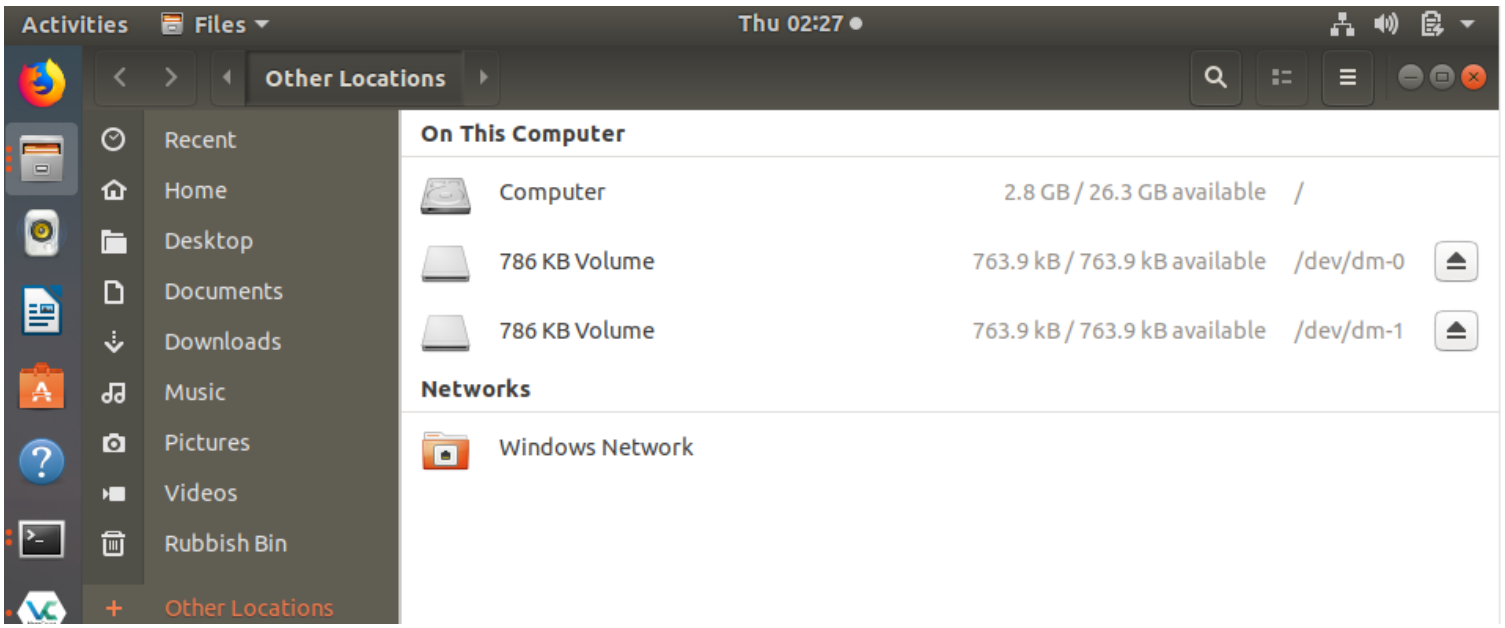
I practice file recovery using a sample encrypted volume called Trial.tc. Before the photos were erased, the disk had three image files and a text file.

I mount the volume, make a forensic copy with dd, and then extract every item—including the deleted ones—using the Sleuth Kit's tsk_recover program.



Then I spent 30 mins to create a VeraCrypt volume of my own with some deleted files. Use this method to recover the files from the mounted volume.





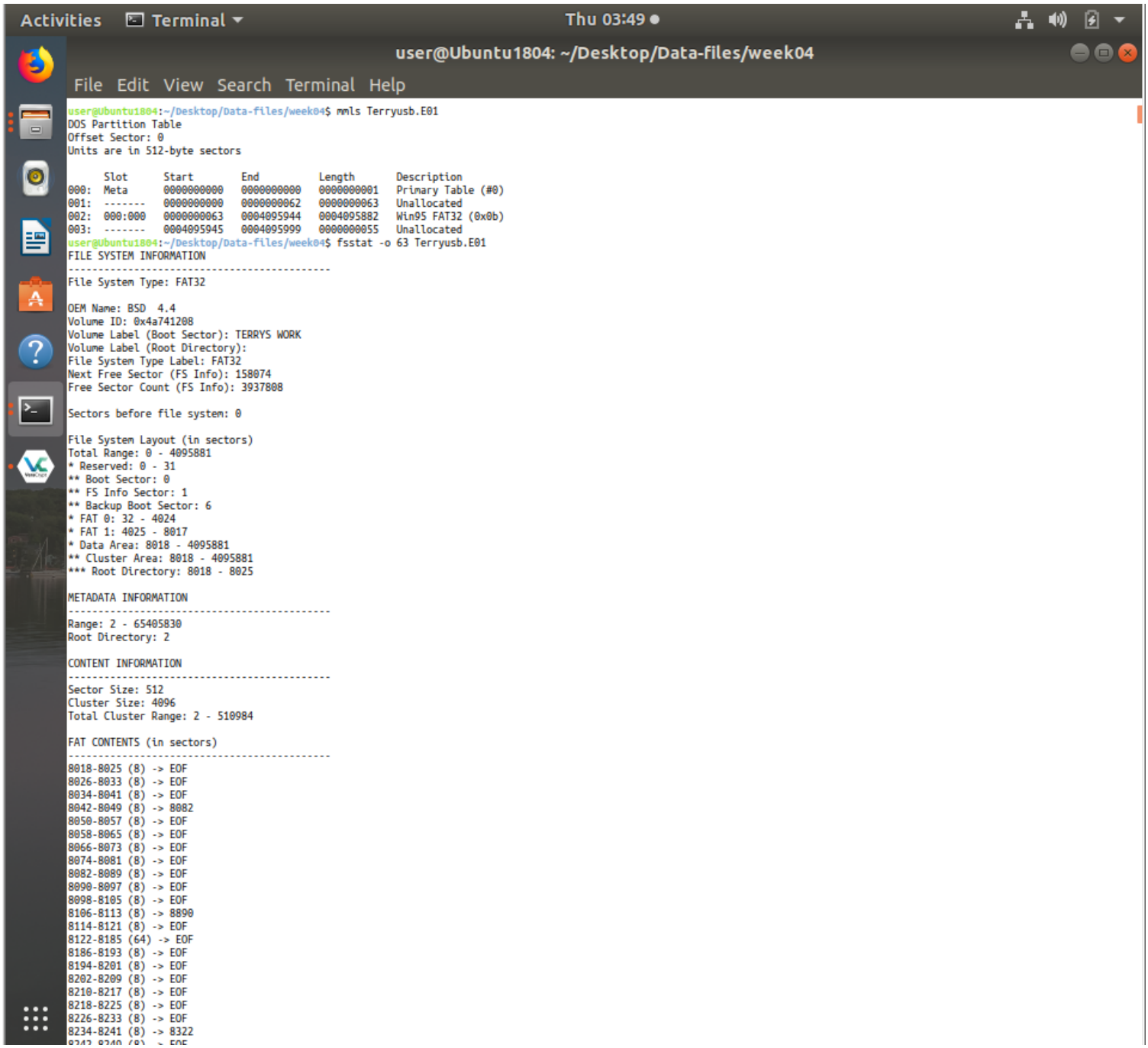

Activities
Terminal
Thu 03:43
user@Ubuntu1804: ~/Desktop/Data-files/week04
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week04$ mount | grep "veracrypt"
veracrypt on /tmp/.veracrypt_aux_mnt1 type fuse.veracrypt (rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other)
/dev/mapper/veracrypt4 on /media/veracrypt4 type vfat (rw,relatime,uid=1000,gid=1000,fmask=0077,dmask=0077,codepage=437,iocharset=iso8859-1,shortname=mixed,errors=remount-ro)
veracrypt on /tmp/.veracrypt_aux_mnt2 type fuse.veracrypt (rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other)
/dev/mapper/veracrypt3 on /media/veracrypt3 type vfat (rw,relatime,uid=1000,gid=1000,fmask=0077,dmask=0077,codepage=437,iocharset=iso8859-1,shortname=mixed,errors=remount-ro)
user@Ubuntu1804:~/Desktop/Data-files/week04$
user@Ubuntu1804:~/Desktop/Data-files/week04$ dd if=/dev/mapper/veracrypt3 of=test.dd
dd: failed to open '/dev/mapper/veracrypt3': Permission denied
user@Ubuntu1804:~/Desktop/Data-files/week04$ sudo dd if=/dev/mapper/veracrypt3 of=test.dd
[sudo] password for user:
1536+0 records in
1536+0 records out
786432 bytes (786 kB, 768 KiB) copied, 0.0286947 s, 27.4 MB/s
user@Ubuntu1804:~/Desktop/Data-files/week04$ tsk_recover -e test.dd ./recover2
Files Recovered: 3
user@Ubuntu1804:~/Desktop/Data-files/week04$ ls -l recover2
total 216
-rw-r--r-- 1 user user 118226 Jun 13 03:43 pic1.png
-rw-r--r-- 1 user user 96773 Jun 13 03:43 pic2.png
-rw-r--r-- 1 user user 512 Jun 13 03:43 'Screenshot from 2024-06-13 02-33-01.png'
user@Ubuntu1804:~/Desktop/Data-files/week04$

Advanced Usage of the Sleuth Kit

I examine a USB drive image named Terryusb.E01 before switching to the Sleuth Kit's more sophisticated instruments.

I collect data about the USB drive's partitions, file system, and directories using tools like mmls, fsstat, and fls.

I spend time investigating various commands from the Sleuth Kit documentation and experiment extracting particular files using the inode number with the icat command.



```
user@Ubuntu1804:~/Desktop/Data-files/week04$ icat -o 63 -r Terryusb.E01
Missing image name and/or address
usage: icat [-hrRsvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o imgoffset] image [images] inum[-typ[-id]]
        -h: Do not display holes in sparse files
        -r: Recover deleted file
        -R: Recover deleted file and suppress recovery errors
        -s: Display slack space at end of file
        -i imgtype: The format of the image file (use '-i list' for supported types)
        -b dev_sector_size: The size (in bytes) of the device sectors
        -f fstype: File system type (use '-f list' for supported types)
        -o imgoffset: The offset of the file system in the image (in sectors)
        -v: verbose to stderr
        -V: Print version
user@Ubuntu1804:~/Desktop/Data-files/week04$
```