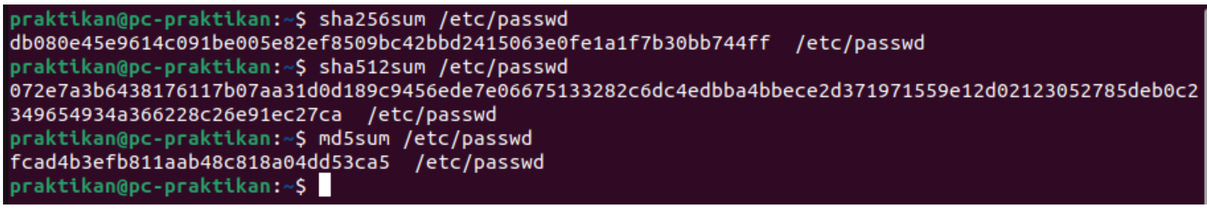
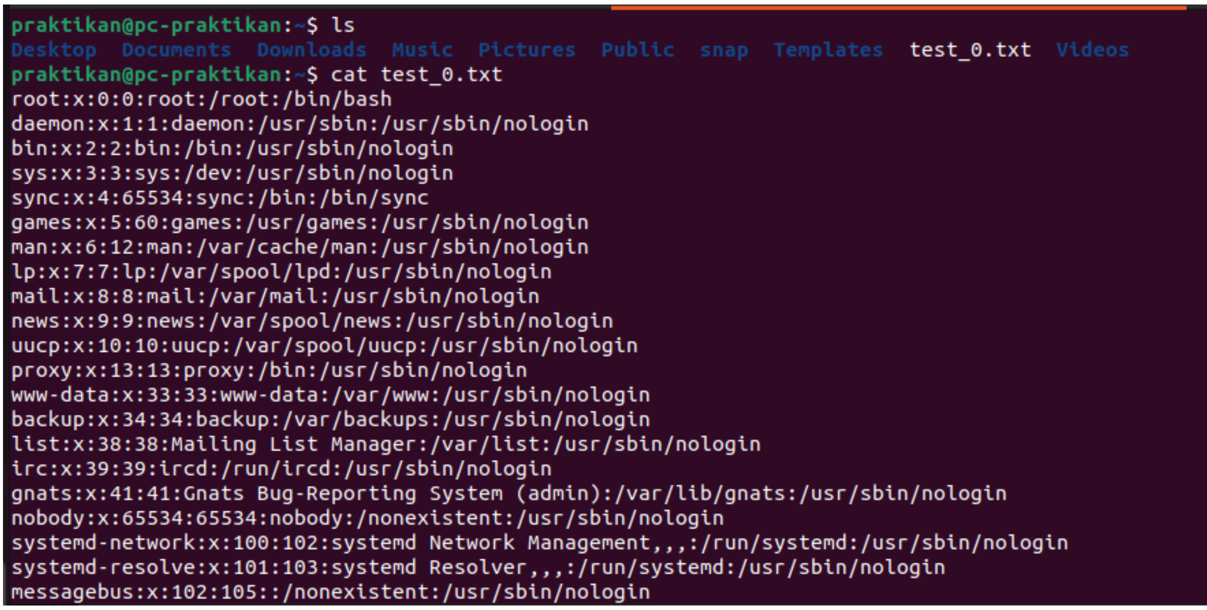
I.G.N. Brindawan Tri Guna Yoga (103012580016)

1. Asd
   a. Lakukan hash SHA256, SHA512 dan MD5 untuk file /etc/passwd. Berapa nilai hash dari file /etc/passwd? Screenshot nilai hash dari file tersebut



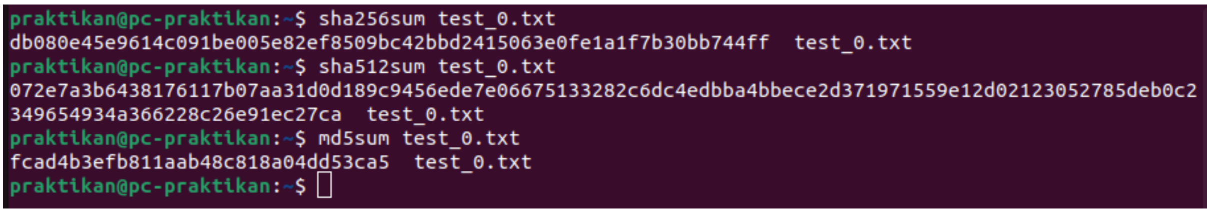
```
praktikan@pc-praktikan:~$ sha256sum /etc/passwd
db080e45e9614c091be005e82ef8509bc42bbd2415063e0fe1a1f7b30bb744ff  /etc/passwd
praktikan@pc-praktikan:~$ sha512sum /etc/passwd
072e7a3b6438176117b07aa31d0d189c9456ede7e06675133282c6dc4edbba4bbece2d371971559e12d02123052785deb0c2
349654934a366228c26e91ec27ca  /etc/passwd
praktikan@pc-praktikan:~$ md5sum /etc/passwd
fcad4b3efb811aab48c818a04dd53ca5  /etc/passwd
praktikan@pc-praktikan:~$ 
```

   b. Cat



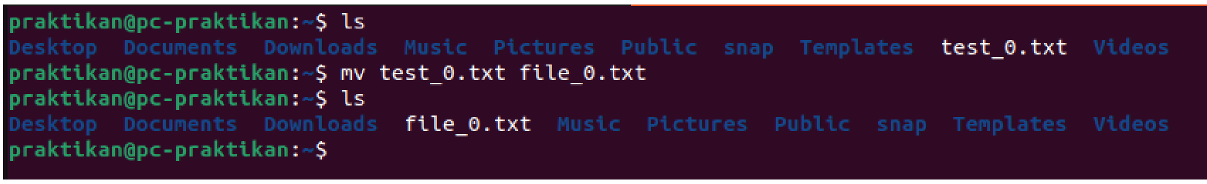
```
praktikan@pc-praktikan:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  test_0.txt  Videos
praktikan@pc-praktikan:~$ cat test_0.txt
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
```

   c. Sha256, sha512, md5 sum

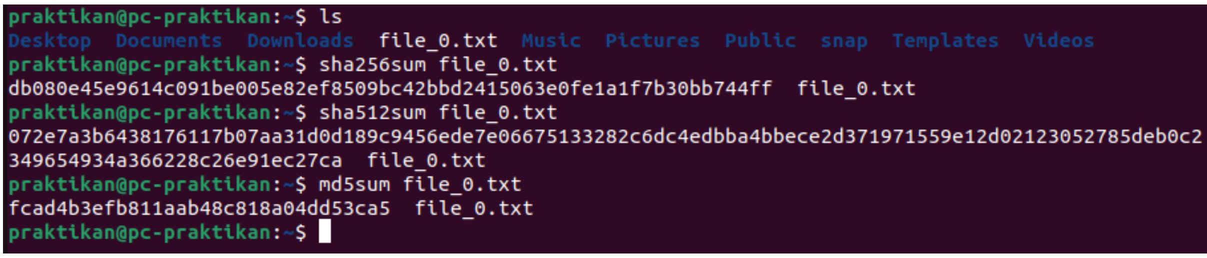


```
praktikan@pc-praktikan:~$ sha256sum test_0.txt
db080e45e9614c091be005e82ef8509bc42bbd2415063e0fe1a1f7b30bb744ff  test_0.txt
praktikan@pc-praktikan:~$ sha512sum test_0.txt
072e7a3b6438176117b07aa31d0d189c9456ede7e06675133282c6dc4edbba4bbece2d371971559e12d02123052785deb0c2
349654934a366228c26e91ec27ca  test_0.txt
praktikan@pc-praktikan:~$ md5sum test_0.txt
fcad4b3efb811aab48c818a04dd53ca5  test_0.txt
praktikan@pc-praktikan:~$ 
```

   d. Rename & hash



```
praktikan@pc-praktikan:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  test_0.txt  Videos
praktikan@pc-praktikan:~$ mv test_0.txt file_0.txt
praktikan@pc-praktikan:~$ ls
Desktop  Documents  Downloads  file_0.txt  Music  Pictures  Public  snap  Templates  Videos
praktikan@pc-praktikan:~$
```

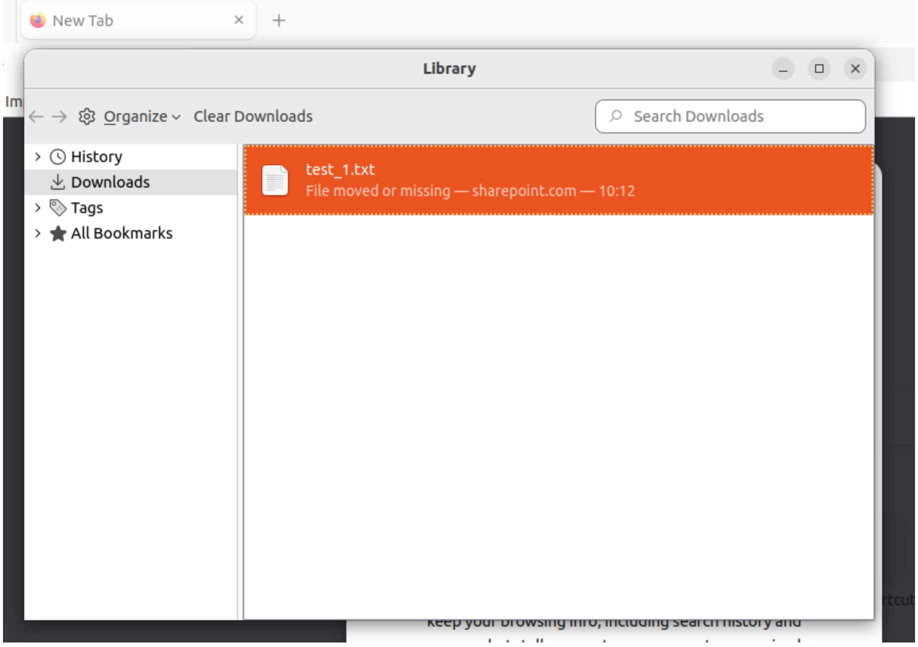


```
praktikan@pc-praktikan:~$ ls
Desktop  Documents  Downloads  file_0.txt  Music  Pictures  Public  snap  Templates  Videos
praktikan@pc-praktikan:~$ sha256sum file_0.txt
db080e45e9614c091be005e82ef8509bc42bbd2415063e0fe1a1f7b30bb744ff  file_0.txt
praktikan@pc-praktikan:~$ sha512sum file_0.txt
072e7a3b6438176117b07aa31d0d189c9456ede7e06675133282c6dc4edbba4bbece2d371971559e12d02123052785deb0c2
349654934a366228c26e91ec27ca  file_0.txt
praktikan@pc-praktikan:~$ md5sum file_0.txt
fcad4b3efb811aab48c818a04dd53ca5  file_0.txt
praktikan@pc-praktikan:~$ 
```

e. Yang berbeda hanya nama file nya, hasil dari hash nya tetap sama karena isinya sama

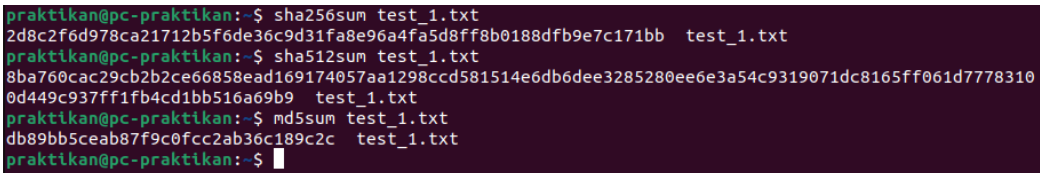
2. No 2

   a. Download Test_1.txt



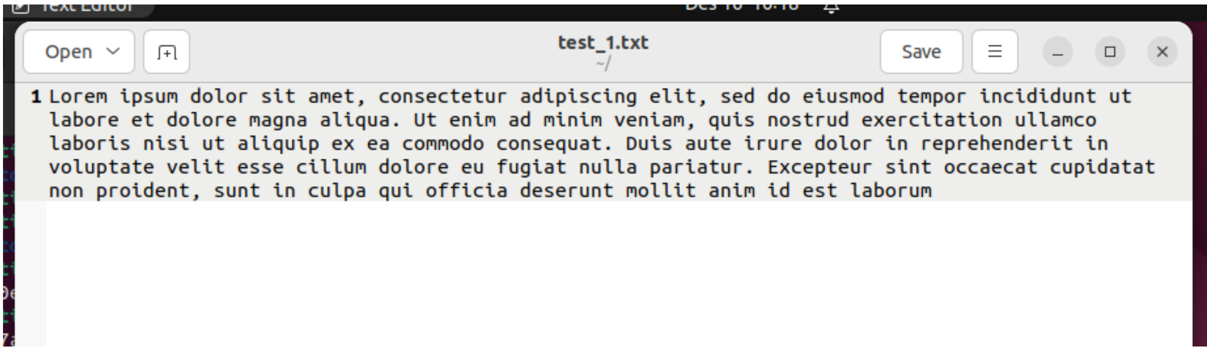
test_1.txt
File moved or missing — sharepoint.com — 10:12

   b. Hash text_1.txt



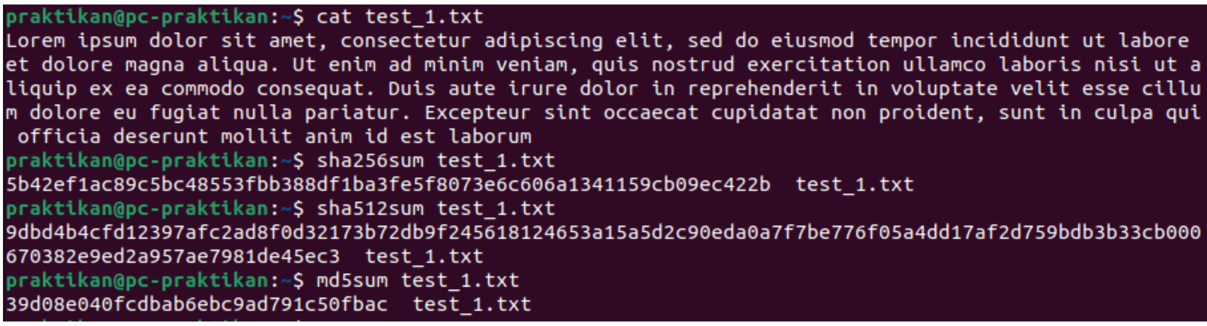
```
praktikan@pc-praktikan:~$ sha256sum test_1.txt
2d8c2f6d978ca21712b5f6de36c9d31fa8e96a4fa5d8ff8b0188dfb9e7c171bb  test_1.txt
praktikan@pc-praktikan:~$ sha512sum test_1.txt
8ba760cac29cb2b2ce66858ead169174057aa1298ccd581514e6db6dee3285280ee6e3a54c9319071dc8165ff061d7778310
0d449c937ff1fb4cd1bb516a69b9  test_1.txt
praktikan@pc-praktikan:~$ md5sum test_1.txt
db89bb5ceab87f9c0fcc2ab36c189c2c  test_1.txt
praktikan@pc-praktikan:~$ 
```

   c. Hapus titik



```
1 Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut
  labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco
  laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in
  voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat
  non proident, sunt in culpa qui officia deserunt mollit anim id est laborum
```

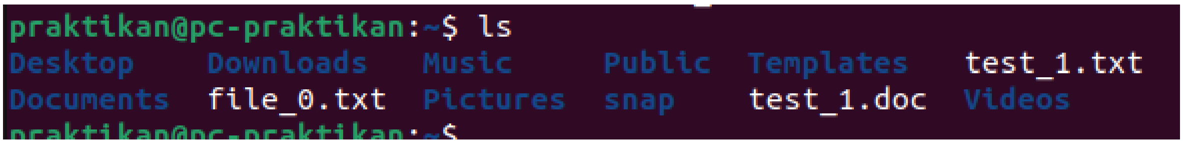
   d. Hasilnya berbeda



```
praktikan@pc-praktikan:~$ cat test_1.txt
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore
et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut a
liquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillu
m dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui
 officia deserunt mollit anim id est laborum
praktikan@pc-praktikan:~$ sha256sum test_1.txt
5b42ef1ac89c5bc48553fbb388df1ba3fe5f8073e6c606a1341159cb09ec422b  test_1.txt
praktikan@pc-praktikan:~$ sha512sum test_1.txt
9dbd4b4cfd12397afc2ad8f0d32173b72db9f245618124653a15a5d2c90eda0a7f7be776f05a4dd17af2d759bdb3b33cb000
670382e9ed2a957ae7981de45ec3  test_1.txt
praktikan@pc-praktikan:~$ md5sum test_1.txt
39d08e040fcdbab6ebc9ad791c50fbac  test_1.txt
```

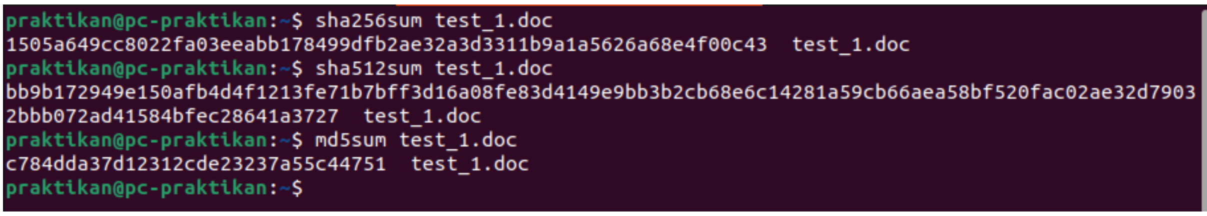
e. Dengan hanya menghilangkan 1 titik hasil hash nya berubah seluruhnya

3. Test1_doc
   a. Download



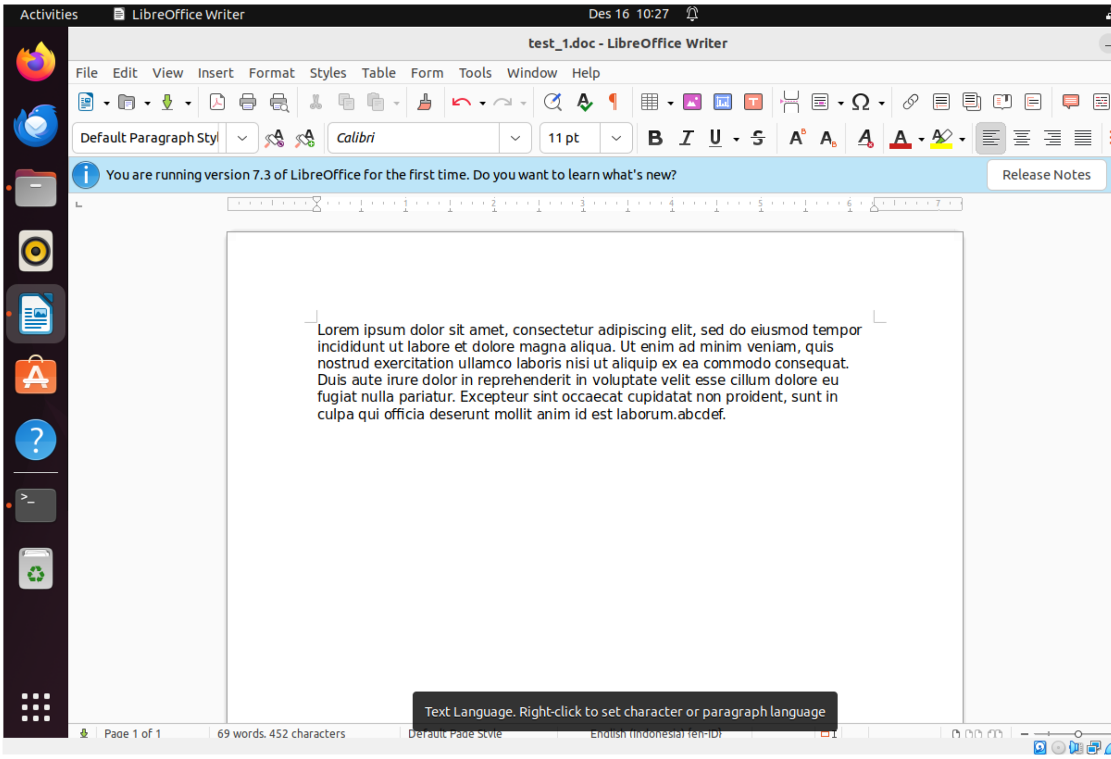
```
praktikan@pc-praktikan:~$ ls
Desktop     Downloads   Music      Public  Templates   test_1.txt
Documents   file_0.txt  Pictures   snap    test_1.doc  Videos
praktikan@pc-praktikan:~$
```

   b. Hash test_1.doc



```
praktikan@pc-praktikan:~$ sha256sum test_1.doc
1505a649cc8022fa03eeabb178499dfb2ae32a3d3311b9a1a5626a68e4f00c43  test_1.doc
praktikan@pc-praktikan:~$ sha512sum test_1.doc
bb9b172949e150afb4d4f1213fe71b7bff3d16a08fe83d4149e9bb3b2cb68e6c14281a59cb66aea58bf520fac02ae32d7903
2bbb072ad41584bfec28641a3727  test_1.doc
praktikan@pc-praktikan:~$ md5sum test_1.doc
c784dda37d12312cde23237a55c44751  test_1.doc
praktikan@pc-praktikan:~$
```

   c. Penambahan dan pengurangan
      i. Penambahan abcdef.



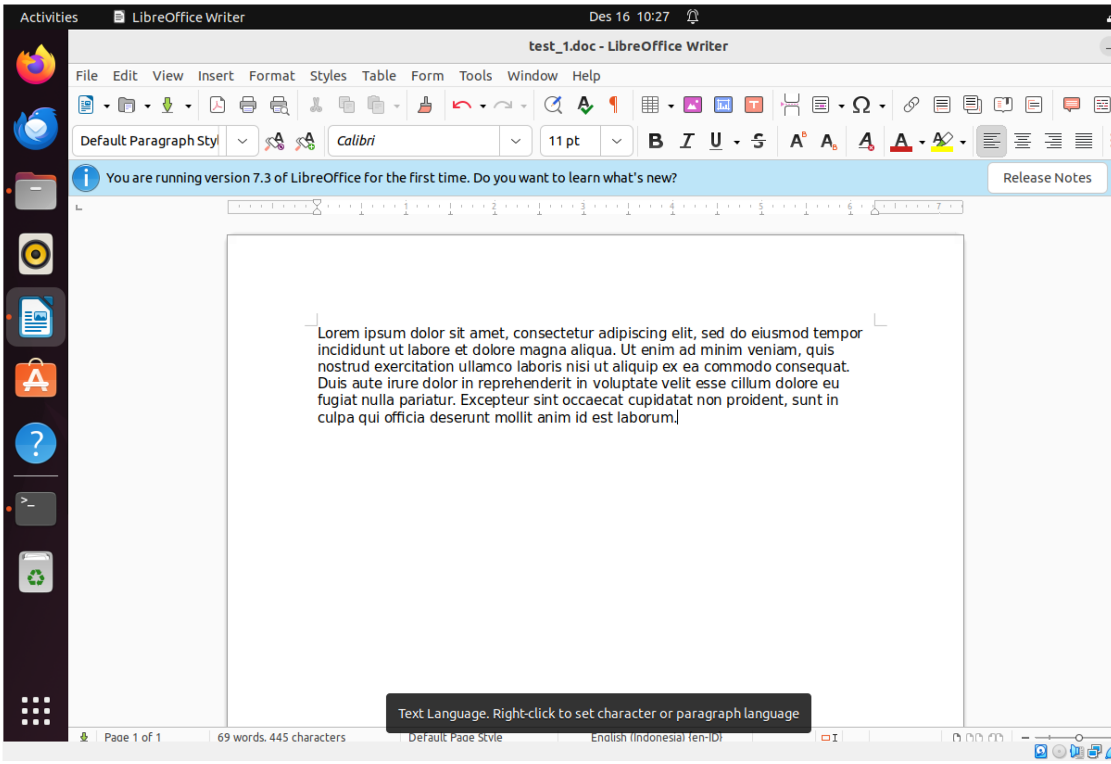
Activities
LibreOffice Writer
Des 16 10:27
test_1.doc - LibreOffice Writer
File Edit View Insert Format Styles Table Form Tools Window Help
Default Paragraph Styl
Calibri
11 pt
Release Notes
Text Language. Right-click to set character or paragraph language

You are running version 7.3 of LibreOffice for the first time. Do you want to learn what's new?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.abcdef.

Page 1 of 1 | 69 words, 452 characters | Default Page Style | English (Indonesia) (en-ID)

ii. Pengurangan abcdef.


Activities
LibreOffice Writer
Des 16 10:27
test_1.doc - LibreOffice Writer
File Edit View Insert Format Styles Table Form Tools Window Help
Default Paragraph Styl
Calibri
11 pt
Release Notes

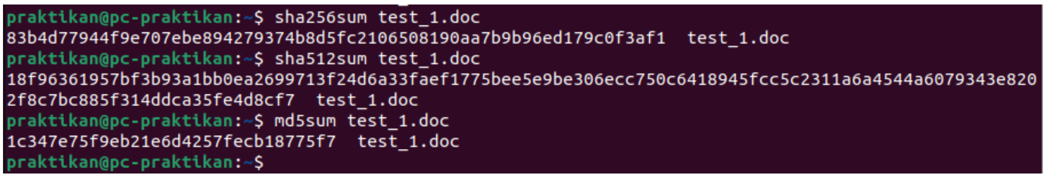
You are running version 7.3 of LibreOffice for the first time. Do you want to learn what's new?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Text Language. Right-click to set character or paragraph language

Page 1 of 1 | 69 words, 445 characters | Default Page Style | English (Indonesia) {en-ID}

d. Melakukan hash lagi

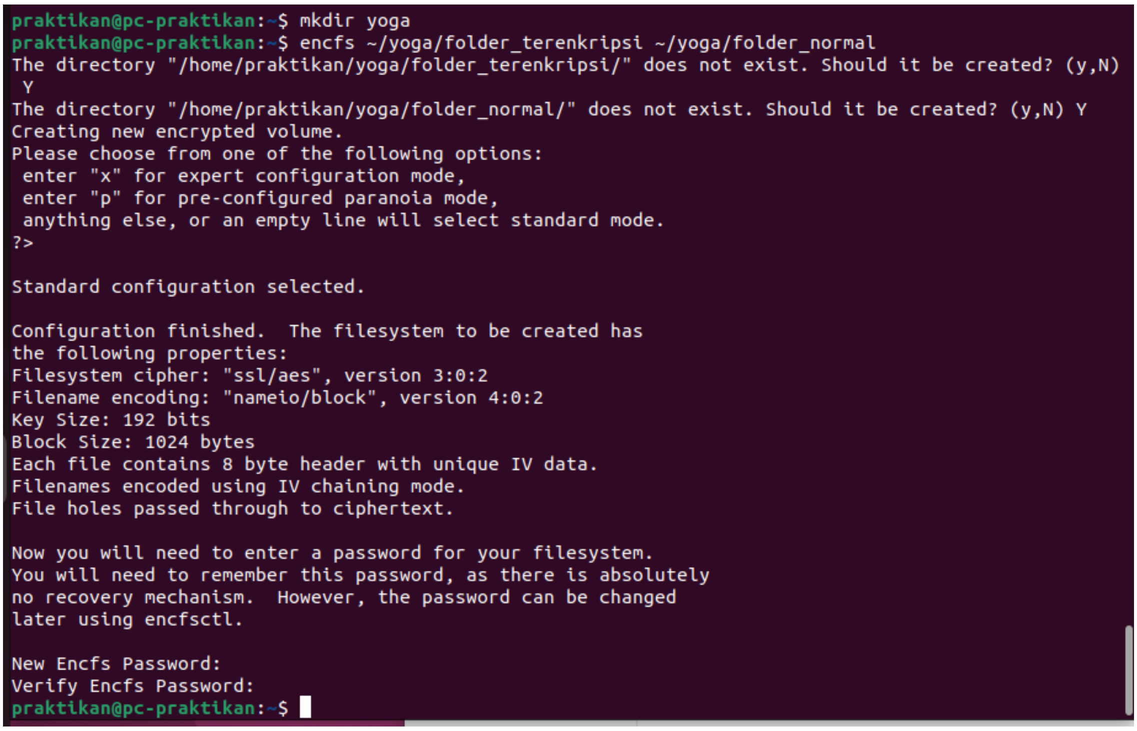


```
praktikan@pc-praktikan:~$ sha256sum test_1.doc
83b4d77944f9e707ebe894279374b8d5fc2106508190aa7b9b96ed179c0f3af1  test_1.doc
praktikan@pc-praktikan:~$ sha512sum test_1.doc
18f96361957bf3b93a1bb0ea2699713f24d6a33faef1775bee5e9be306ecc750c6418945fcc5c2311a6a4544a6079343e820
2f8c7bc885f314ddca35fe4d8cf7  test_1.doc
praktikan@pc-praktikan:~$ md5sum test_1.doc
1c347e75f9eb21e6d4257fecb18775f7  test_1.doc
praktikan@pc-praktikan:~$
```

e. Ada perubahan pada hasil hash, ini terjadi mungkin karena file dengan ekstensi khsusus (selain .txt .sh dan serupa) tidak menyimpan history file atau format khusus lainnya di dalamnya.

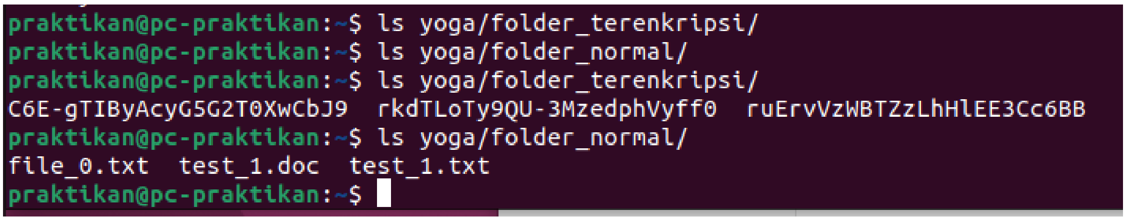
4. Asd

   a. Membuat folder



```
praktikan@pc-praktikan:~$ mkdir yoga
praktikan@pc-praktikan:~$ encfs ~/yoga/folder_terenkripsi ~/yoga/folder_normal
The directory "/home/praktikan/yoga/folder_terenkripsi/" does not exist. Should it be created? (y,N)
 Y
The directory "/home/praktikan/yoga/folder_normal/" does not exist. Should it be created? (y,N) Y
Creating new encrypted volume.
Please choose from one of the following options:
 enter "x" for expert configuration mode,
 enter "p" for pre-configured paranoia mode,
 anything else, or an empty line will select standard mode.
?>

Standard configuration selected.

Configuration finished.  The filesystem to be created has
the following properties:
Filesystem cipher: "ssl/aes", version 3:0:2
Filename encoding: "nameio/block", version 4:0:2
Key Size: 192 bits
Block Size: 1024 bytes
Each file contains 8 byte header with unique IV data.
Filenames encoded using IV chaining mode.
File holes passed through to ciphertext.

Now you will need to enter a password for your filesystem.
You will need to remember this password, as there is absolutely
no recovery mechanism.  However, the password can be changed
later using encfsctl.

New Encfs Password:
Verify Encfs Password:
praktikan@pc-praktikan:~$ 
```

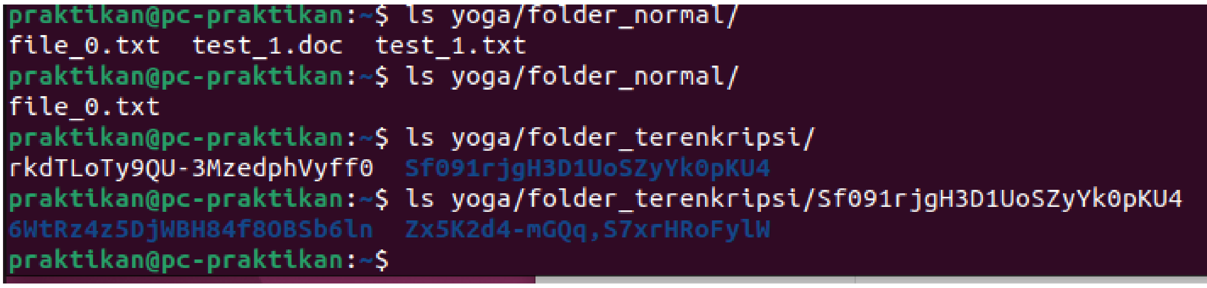
   b. Menambahkan file pada folder normal dan mengamatinya



```
praktikan@pc-praktikan:~$ ls yoga/folder_terenkripsi/
praktikan@pc-praktikan:~$ ls yoga/folder_normal/
praktikan@pc-praktikan:~$ ls yoga/folder_terenkripsi/
C6E-gTIByAcyG5G2T0XwCbJ9  rkdTLoTy9QU-3MzedphVyff0  ruErvVzWBTZzLhHlEE3Cc6BB
praktikan@pc-praktikan:~$ ls yoga/folder_normal/
file_0.txt  test_1.doc  test_1.txt
praktikan@pc-praktikan:~$ 
```

   Muncul file enkripsi Ketika folder normal di isikan file, atau dengan kata lain folder terenkripsi sync dengan folder normal

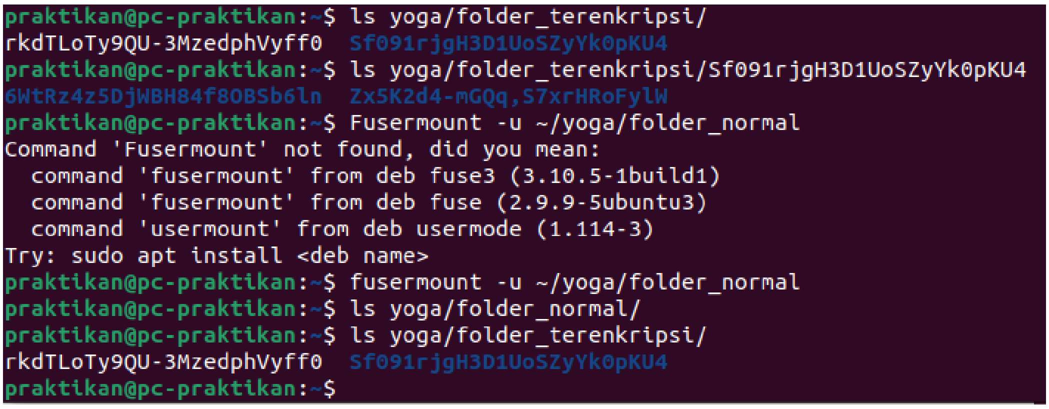
   c. Menghapus dan mengamati



```
praktikan@pc-praktikan:~$ ls yoga/folder_normal/
file_0.txt  test_1.doc  test_1.txt
praktikan@pc-praktikan:~$ ls yoga/folder_normal/
file_0.txt
praktikan@pc-praktikan:~$ ls yoga/folder_terenkripsi/
rkdTLoTy9QU-3MzedphVyff0  Sf091rjgH3D1UoSZyYk0pKU4
praktikan@pc-praktikan:~$ ls yoga/folder_terenkripsi/Sf091rjgH3D1UoSZyYk0pKU4
6WtRz4z5DjWBH84f8OBSb6ln  Zx5K2d4-mGQq,S7xrHRoFylW
praktikan@pc-praktikan:~$
```

   Ketika menghapus file pada folder normal pada folder terenkripsi juga terjadi perubahan, terdapat direktori enkripsi baru yang di dalamnya terdapat folder lagi, ini sepertinya history dari folder yang di hapus

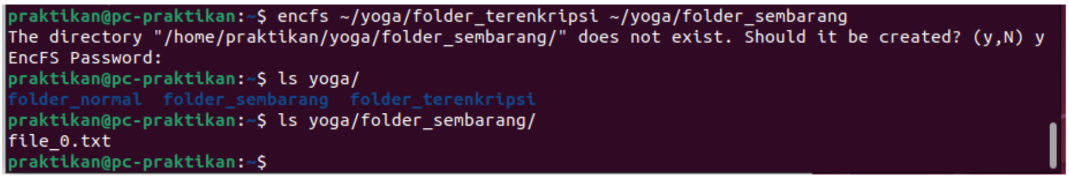
d. fusermount



```
praktikan@pc-praktikan:~$ ls yoga/folder_terenkripsi/
rkdTLoTy9QU-3MzedphVyff0  Sf091rjgH3D1UoSZyYk0pKU4
praktikan@pc-praktikan:~$ ls yoga/folder_terenkripsi/Sf091rjgH3D1UoSZyYk0pKU4
6WtRz4z5DjWBH84f8OBSb6ln  Zx5K2d4-mGQq,S7xrHRoFylW
praktikan@pc-praktikan:~$ Fusermount -u ~/yoga/folder_normal
Command 'Fusermount' not found, did you mean:
  command 'fusermount' from deb fuse3 (3.10.5-1build1)
  command 'fusermount' from deb fuse (2.9.9-5ubuntu3)
  command 'usermount' from deb usermode (1.114-3)
Try: sudo apt install <deb name>
praktikan@pc-praktikan:~$ fusermount -u ~/yoga/folder_normal
praktikan@pc-praktikan:~$ ls yoga/folder_normal/
praktikan@pc-praktikan:~$ ls yoga/folder_terenkripsi/
rkdTLoTy9QU-3MzedphVyff0  Sf091rjgH3D1UoSZyYk0pKU4
praktikan@pc-praktikan:~$
```

isi pada folder normal hilang, namun pada folder terenkripsi ada

e. encfs dengan folder sembarang

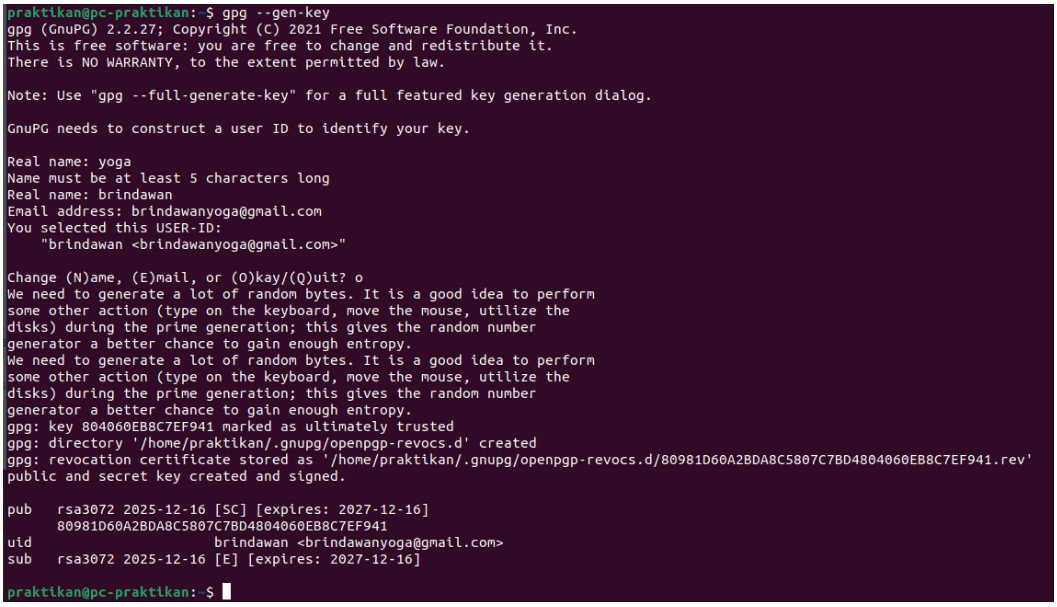


```
praktikan@pc-praktikan:~$ encfs ~/yoga/folder_terenkripsi ~/yoga/folder_sembarang
The directory "/home/praktikan/yoga/folder_sembarang/" does not exist. Should it be created? (y,N) y
EncFS Password:
praktikan@pc-praktikan:~$ ls yoga/
folder_normal  folder_sembarang  folder_terenkripsi
praktikan@pc-praktikan:~$ ls yoga/folder_sembarang/
file_0.txt
praktikan@pc-praktikan:~$
```

Hasilnya muncul file yang sebelumnya ada pada folder normal, file tersebut tersimpan dan terenkripsi pada folder terenkripsi, Ketika di unmount maka file itu akan hilang, dan di mount lagi dengan memasukkan password yang sama maka akan muncul Kembali

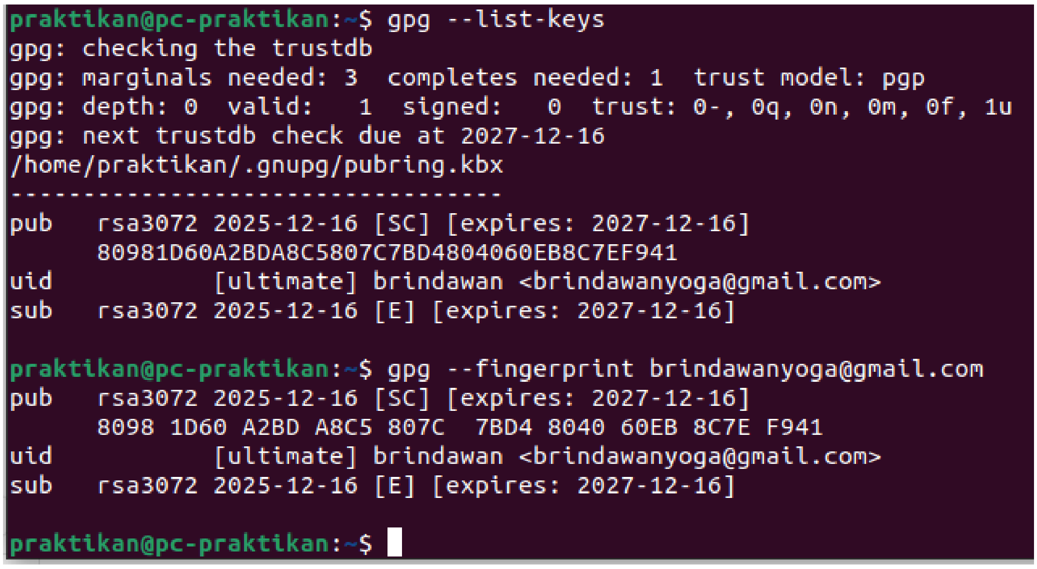
5. Konfidensialitas: gpg

a. Gpg baru



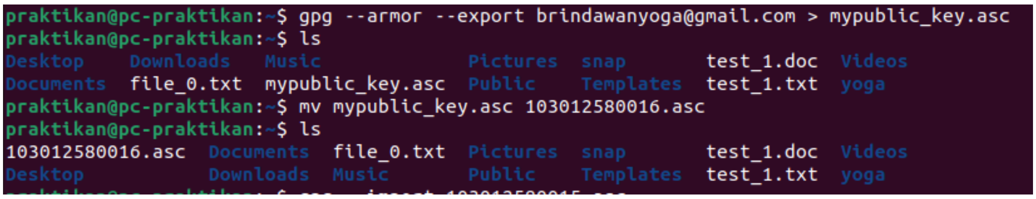
```
praktikan@pc-praktikan:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: yoga
Name must be at least 5 characters long
Real name: brindawan
Email address: brindawanyoga@gmail.com
You selected this USER-ID:
    "brindawan <brindawanyoga@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 804060EB8C7EF941 marked as ultimately trusted
gpg: directory '/home/praktikan/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/praktikan/.gnupg/openpgp-revocs.d/80981D60A2BDA8C5807C7BD4804060EB8C7EF941.rev'
public and secret key created and signed.

pub   rsa3072 2025-12-16 [SC] [expires: 2027-12-16]
      80981D60A2BDA8C5807C7BD4804060EB8C7EF941
uid                      brindawan <brindawanyoga@gmail.com>
sub   rsa3072 2025-12-16 [E] [expires: 2027-12-16]

praktikan@pc-praktikan:~$
```

b. List gpg key



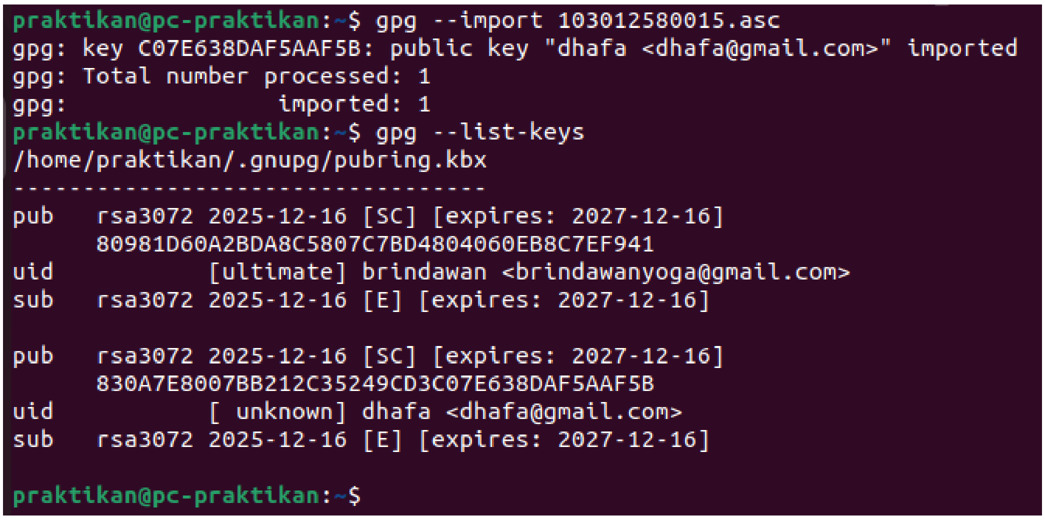
```
praktikan@pc-praktikan:~$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2027-12-16
/home/praktikan/.gnupg/pubring.kbx
----------------------------------
pub   rsa3072 2025-12-16 [SC] [expires: 2027-12-16]
      80981D60A2BDA8C5807C7BD4804060EB8C7EF941
uid           [ultimate] brindawan <brindawanyoga@gmail.com>
sub   rsa3072 2025-12-16 [E] [expires: 2027-12-16]

praktikan@pc-praktikan:~$ gpg --fingerprint brindawanyoga@gmail.com
pub   rsa3072 2025-12-16 [SC] [expires: 2027-12-16]
      8098 1D60 A2BD A8C5 807C  7BD4 8040 60EB 8C7E F941
uid           [ultimate] brindawan <brindawanyoga@gmail.com>
sub   rsa3072 2025-12-16 [E] [expires: 2027-12-16]

praktikan@pc-praktikan:~$ 
```

c. Export & rename



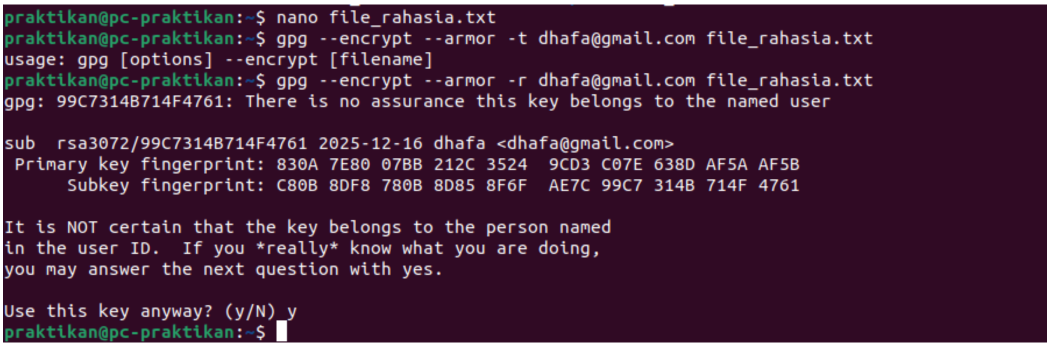
```
praktikan@pc-praktikan:~$ gpg --armor --export brindawanyoga@gmail.com > mypublic_key.asc
praktikan@pc-praktikan:~$ ls
Desktop    Downloads  Music             Pictures  snap       test_1.doc  Videos
Documents  file_0.txt  mypublic_key.asc  Public    Templates  test_1.txt  yoga
praktikan@pc-praktikan:~$ mv mypublic_key.asc 103012580016.asc
praktikan@pc-praktikan:~$ ls
103012580016.asc  Documents  file_0.txt  Pictures  snap       test_1.doc  Videos
Desktop           Downloads  Music       Public    Templates  test_1.txt  yoga
```

d. Import key teman



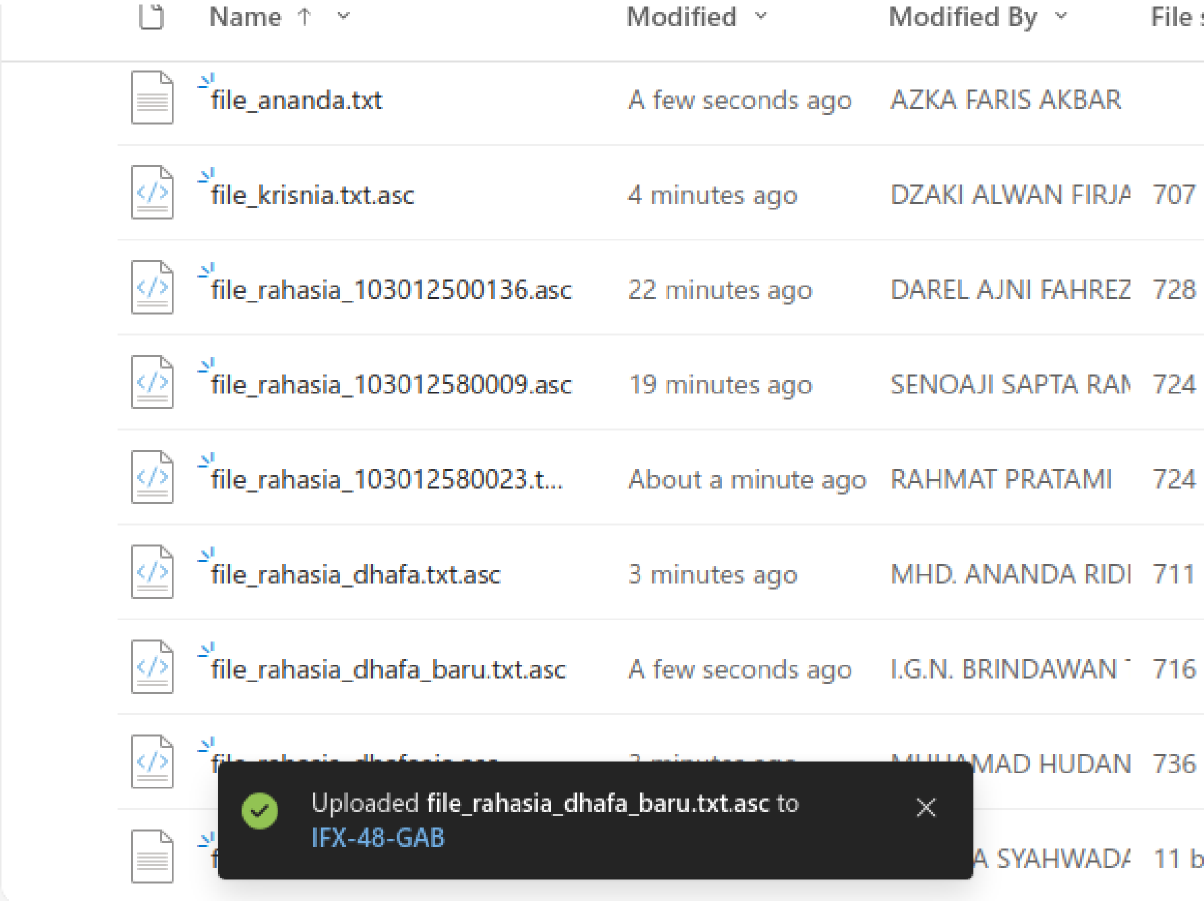
```
praktikan@pc-praktikan:~$ gpg --import 103012580015.asc
gpg: key C07E638DAF5AAF5B: public key "dhafa <dhafa@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
praktikan@pc-praktikan:~$ gpg --list-keys
/home/praktikan/.gnupg/pubring.kbx
----------------------------------
pub   rsa3072 2025-12-16 [SC] [expires: 2027-12-16]
      80981D60A2BDA8C5807C7BD4804060EB8C7EF941
uid           [ultimate] brindawan <brindawanyoga@gmail.com>
sub   rsa3072 2025-12-16 [E] [expires: 2027-12-16]

pub   rsa3072 2025-12-16 [SC] [expires: 2027-12-16]
      830A7E8007BB212C35249CD3C07E638DAF5AAF5B
uid           [ unknown] dhafa <dhafa@gmail.com>
sub   rsa3072 2025-12-16 [E] [expires: 2027-12-16]

praktikan@pc-praktikan:~$
```

e. Buat file dan kirim



```
praktikan@pc-praktikan:~$ nano file_rahasia.txt
praktikan@pc-praktikan:~$ gpg --encrypt --armor -t dhafa@gmail.com file_rahasia.txt
usage: gpg [options] --encrypt [filename]
praktikan@pc-praktikan:~$ gpg --encrypt --armor -r dhafa@gmail.com file_rahasia.txt
gpg: 99C7314B714F4761: There is no assurance this key belongs to the named user

sub  rsa3072/99C7314B714F4761 2025-12-16 dhafa <dhafa@gmail.com>
 Primary key fingerprint: 830A 7E80 07BB 212C 3524  9CD3 C07E 638D AF5A AF5B
      Subkey fingerprint: C80B 8DF8 780B 8D85 8F6F  AE7C 99C7 314B 714F 4761

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
praktikan@pc-praktikan:~$ 
```

f. Kirim file



Name ↑	Modified	Modified By	File s
file_ananda.txt	A few seconds ago	AZKA FARIS AKBAR	
file_krisnia.txt.asc	4 minutes ago	DZAKI ALWAN FIRJA	707
file_rahasia_103012500136.asc	22 minutes ago	DAREL AJNI FAHREZ	728
file_rahasia_103012580009.asc	19 minutes ago	SENOAJI SAPTA RAN	724
file_rahasia_103012580023.t...	About a minute ago	RAHMAT PRATAMI	724
file_rahasia_dhafa.txt.asc	3 minutes ago	MHD. ANANDA RIDI	711
file_rahasia_dhafa_baru.txt.asc	A few seconds ago	I.G.N. BRINDAWAN	716
file_rahasia_dhafasia.asc	3 minutes ago	MUHAMAD HUDAN	736
f		A SYAHWADA	11 b

Uploaded file_rahasia_dhafa_baru.txt.asc to IFX-48-GAB