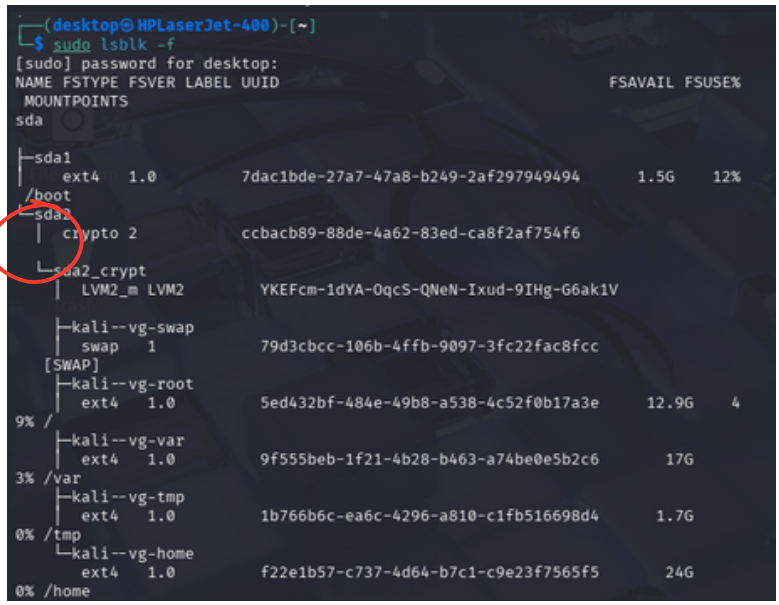
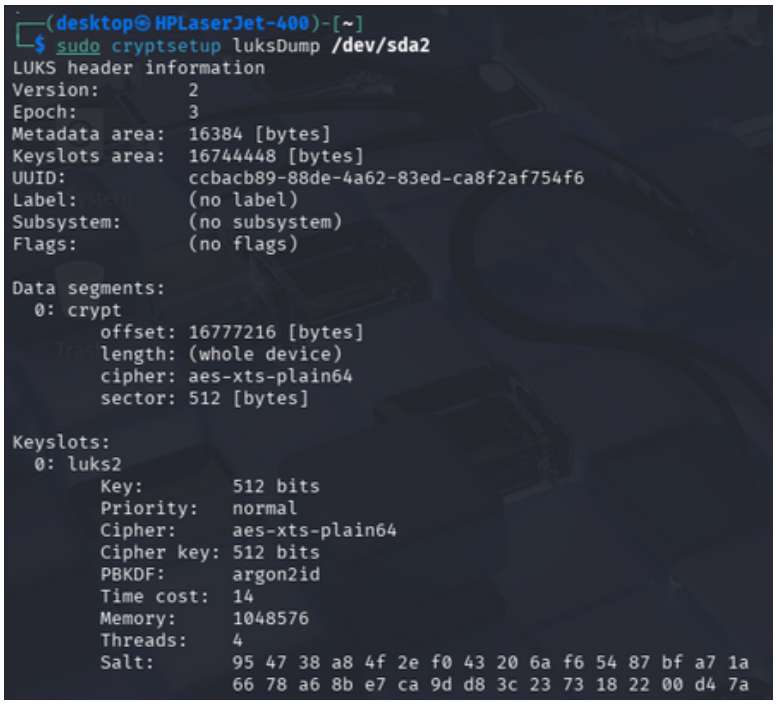
Il backup degli header LUKS è fondamentale per proteggere i tuoi dati crittografati

sudo lsbk -f *per indentificare la partizione criptata, in questo caso* ***sda2***



sudo cryptsetup luksDump /dev/sda2
per visualizzare i metadati dell'header LUKS



sudo cryptsetup luksHeaderBackup /dev/sda2 --header-backup-file ~/luks-header-sda2.img
crea file binario contenente header e l'area dei keyslot

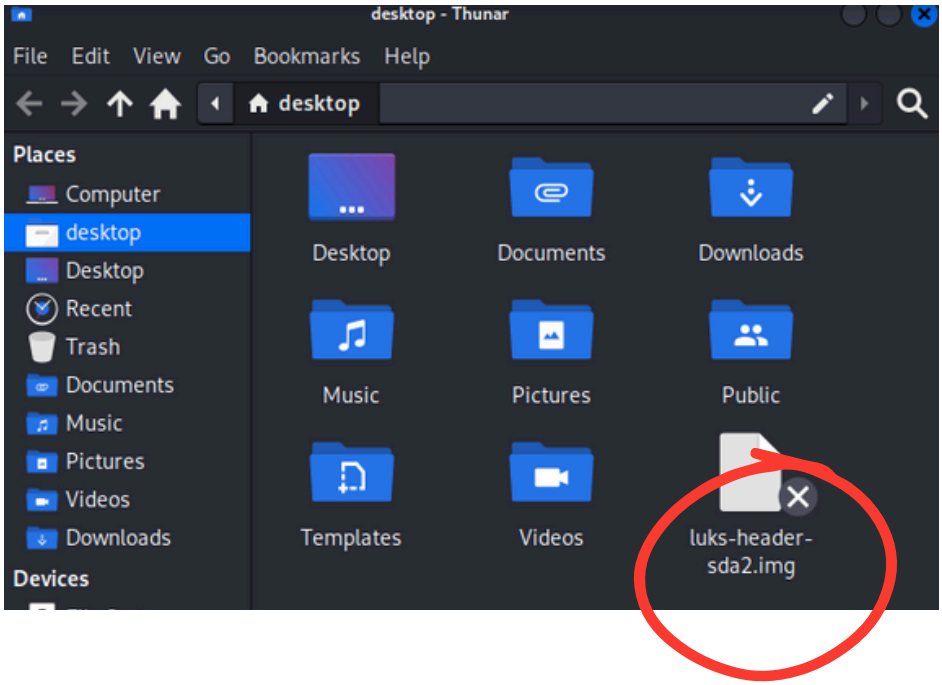
```
┌──(desktop㉿HPLaserJet-400)-[~]
└─$ sudo cryptsetup luksHeaderBackup /dev/sda2 --header-backup-file ~/luks-header-sda2.img
[sudo] password for desktop:

┌──(desktop㉿HPLaserJet-400)-[~]
└─$
```

sudo cryptsetup luksHeaderRestore /dev/sda2 --header-backup-file ~/luks-header-sda2.img
per ripristinare l'header

Precauzioni e Buone Pratiche

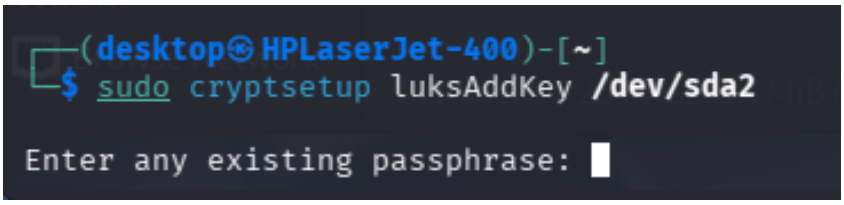
- Backup Offline su dispositivo esterno o usb
- Ubicazioni Multiple
- Crittografa i backup



Generazione Ulteriore Password di Backup

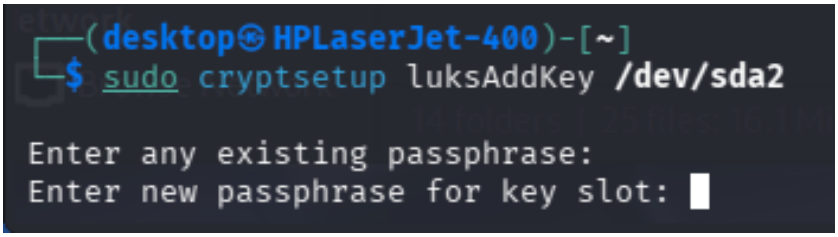
il concetto e' avere una seconda password piu complessa da tenere di backup nel caso la prima andasse persa

sudo cryptsetup luksAddKey /dev/sda2

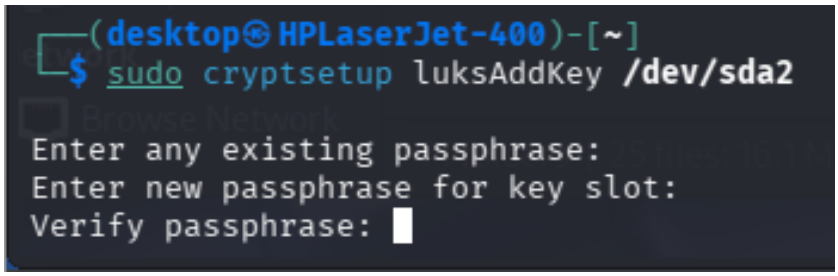


*inserire password/**passphrase** del **disco crittografato** in **LUKS***

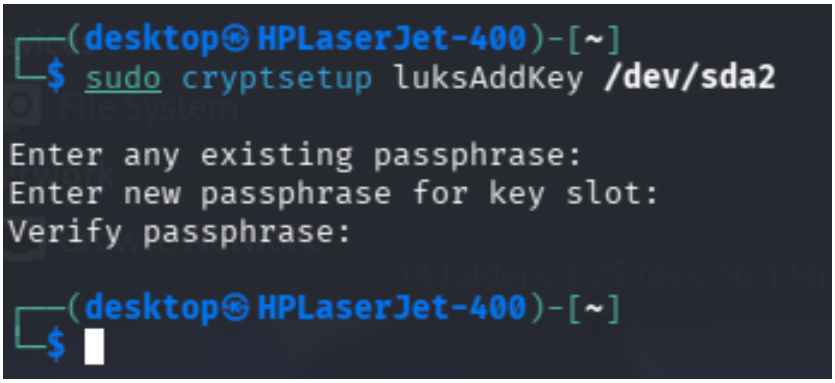
inserire la nuova **passphrase**



ridigitiamola per confermare



se non ci restituisce errori la procedura e' andata a buon fine



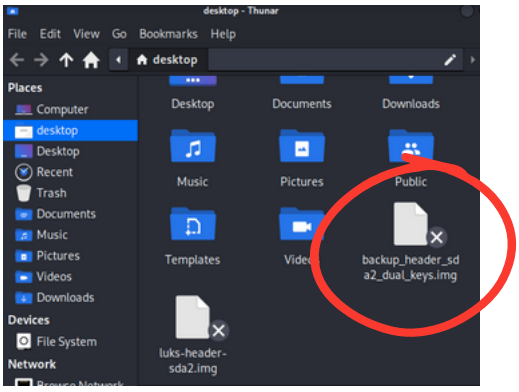
Una volta che abbiamo due chiavi attive, rieseguiamo il backup

sudo cryptsetup luksDump /dev/sda2

ci conferma che abbiamo Keyslots 0 e 1 (le nostre due chiavi)

```
Keyslots:
  0: luks2
        Key:        512 bits
        Priority:   normal
        Cipher:     aes-xts-plain64
        Cipher key: 512 bits
        PBKDF:      argon2id
        Time cost:  14
        Memory:     1048576
        Threads:    4
        Salt:       95 47 38 a8 4f 2e f0 43 20 6a f6 54 87 bf a7 1a
                    66 78 a6 8b e7 ca 9d d8 3c 23 73 18 22 00 d4 7a
        AF stripes: 4000
        AF hash:    sha256
        Area offset:32768 [bytes]
        Area length:258048 [bytes]
        Digest ID:  0
  1: luks2
        Key:        512 bits
        Priority:   normal
        Cipher:     aes-xts-plain64
        Cipher key: 512 bits
        PBKDF:      argon2id
        Time cost:  14
        Memory:     1048576
        Threads:    4
        Salt:       90 06 b3 25 9e 94 75 fd 8f 3b ab 31 89 9c 80 e6
                    4c d2 11 c8 56 ad 70 b9 91 58 29 29 30 4e 58 f0
        AF stripes: 4000
        AF hash:    sha256
```

sudo cryptsetup luksHeaderBackup /dev/sda2 --header-backup-file ~/backup_header_sda2_dual_keys.img



NOTA BENE: la partizione **boot non e' criptata**, se il dispositivo viene lasciato **incustodito** diventa' vulnerabile al aggiunta di **keylogger,** che rivelerebbero le passphrase quando le reinseriamo al nostro accesso o altri tipi di attacchi.

Nel caso si prevede la possibilita' di lasciare il dispositivo incostudito prendere semplicemente le precauzioni adeguate preventivamente al evento.