

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

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

```
(desktop@HPLaserJet-400)-[~]
$ sudo lsblk -f
[sudo] password for desktop:
NAME FSTYPE FSVER LABEL UUID                                FSAVAIL FSUSE%
MOUNTPOINTS
sda
├─sda1
│   └─ext4 1.0          7dac1bde-27a7-47a8-b249-2af297949494    1.5G    12%
│   /boot
├─sda2
│   └─crypto 2          ccbacb89-88de-4a62-83ed-ca8f2af754f6
│       └─sda2_crypt
│           └─LVM2_m LVM2          YKEFcm-1dYA-0qcS-QNeN-Ixud-9IHg-G6ak1V
│               └─kali--vg-swap
│                   └─swap 1          79d3cbcc-106b-4ffb-9097-3fc22fac8fcc
│                       [SWAP]
│               └─kali--vg-root
│                   └─ext4 1.0          5ed432bf-484e-49b8-a538-4c52f0b17a3e    12.9G    4
│                       9% /
│               └─kali--vg-var
│                   └─ext4 1.0          9f555beb-1f21-4b28-b463-a74be0e5b2c6      17G
│                       3% /var
│               └─kali--vg-tmp
│                   └─ext4 1.0          1b766b6c-ea6c-4296-a810-c1fb516698d4      1.7G
│                       0% /tmp
│               └─kali--vg-home
│                   └─ext4 1.0          f22e1b57-c737-4d64-b7c1-c9e23f7565f5      24G
│                       0% /home
```

`sudo cryptsetup luksDump /dev/sda2`

per visualizzare i metadati dell'header LUKS

```
(desktop@HPLaserJet-400)-[~]
$ sudo cryptsetup luksDump /dev/sda2
LUKS header information
Version:          2
Epoch:           3
Metadata area:    16384 [bytes]
Keyslots area:    16744448 [bytes]
UUID:             ccbacb89-88de-4a62-83ed-ca8f2af754f6
Label:            (no label)
Subsystem:        (no subsystem)
Flags:            (no flags)

Data segments:
  0: crypt
      offset: 16777216 [bytes]
      length: (whole device)
      cipher: aes-xts-plain64
      sector: 512 [bytes]

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
```

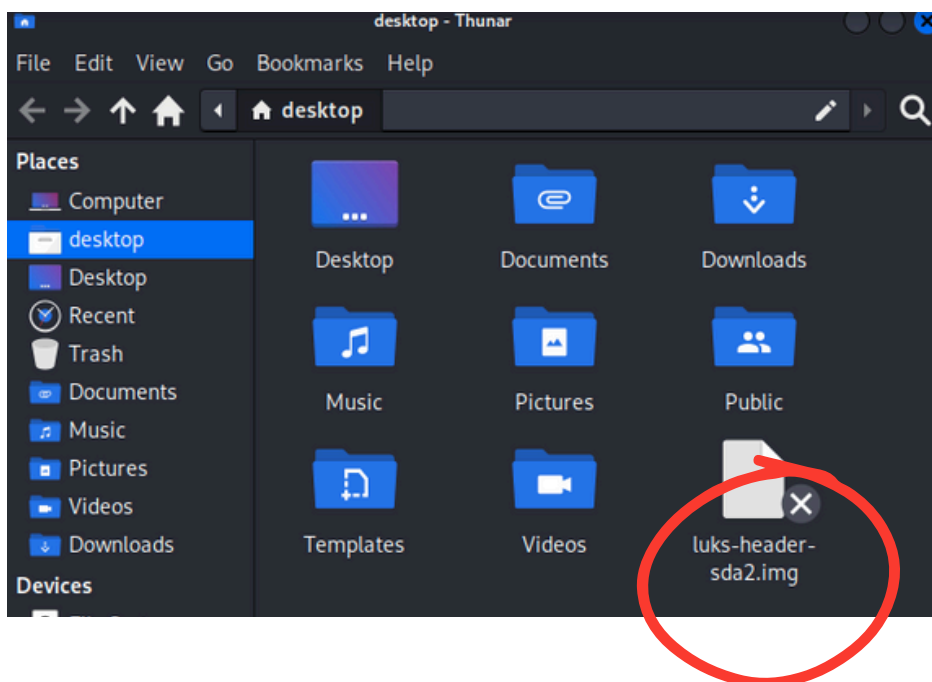
sudo cryptsetup luksHeaderBackup /dev/sda2 --header-backup-file ~/luks-header-sda2.img
crea file binario contenente header e l'area dei keyslot

```
(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
- Crittografia i backup



Generazione Ulteriore Password di Backup

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

sudo cryptsetup luksAddKey /dev/sda2

```
(desktop@HPLaserJet-400)-[~]  
$ sudo cryptsetup luksAddKey /dev/sda2  
Enter any existing passphrase: █
```

inserire password/passphrase del disco crittografato in LUKS

inserire la nuova **passphrase**

```
(desktop@HPLaserJet-400)-[~]  
$ sudo cryptsetup luksAddKey /dev/sda2  
Enter any existing passphrase:  
Enter new passphrase for key slot: █
```

digitiamo nuovamente per confermare

```
(desktop@HPLaserJet-400)-[~]  
$ sudo cryptsetup luksAddKey /dev/sda2  
Browse Network  
Enter any existing passphrase:  
Enter new passphrase for key slot:  
Verify passphrase: █
```

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

```
(desktop@HPLaserJet-400)-[~]  
$ sudo cryptsetup luksAddKey /dev/sda2  
Browse Network  
Enter any existing passphrase:  
Enter new passphrase for key slot:  
Verify passphrase:  
  
(desktop@HPLaserJet-400)-[~]  
$ █
```

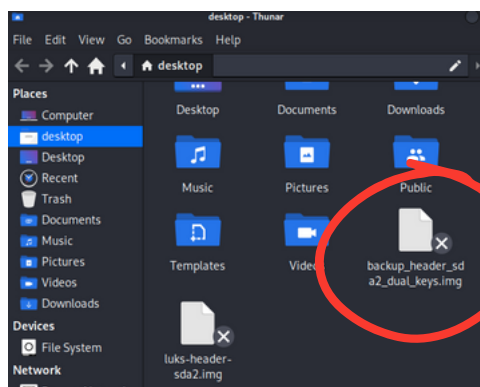
Con due chiavi attive, eseguiamo nuovamente il backup

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 all'aggiunta di **keylogger**, che rivelerebbero le passphrase quando le reinseriamo al nostro accesso o ad altri tipi di attacchi.

Prendere adeguate precauzioni preventivamente nel caso si preveda la possibilita' di lasciare il dispositivo incustodito.