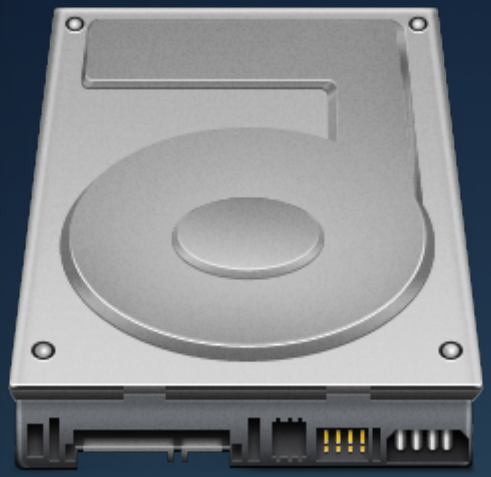
Recupero dati fai da te

Andrea Lazzarotto
http://andrealazzarotto.com

> More than half of people who toss computers in the garbage or sell them are leaving sensitive data on their hard drives.
>
> - Larry Greenemeier, Scientific American

Percorso

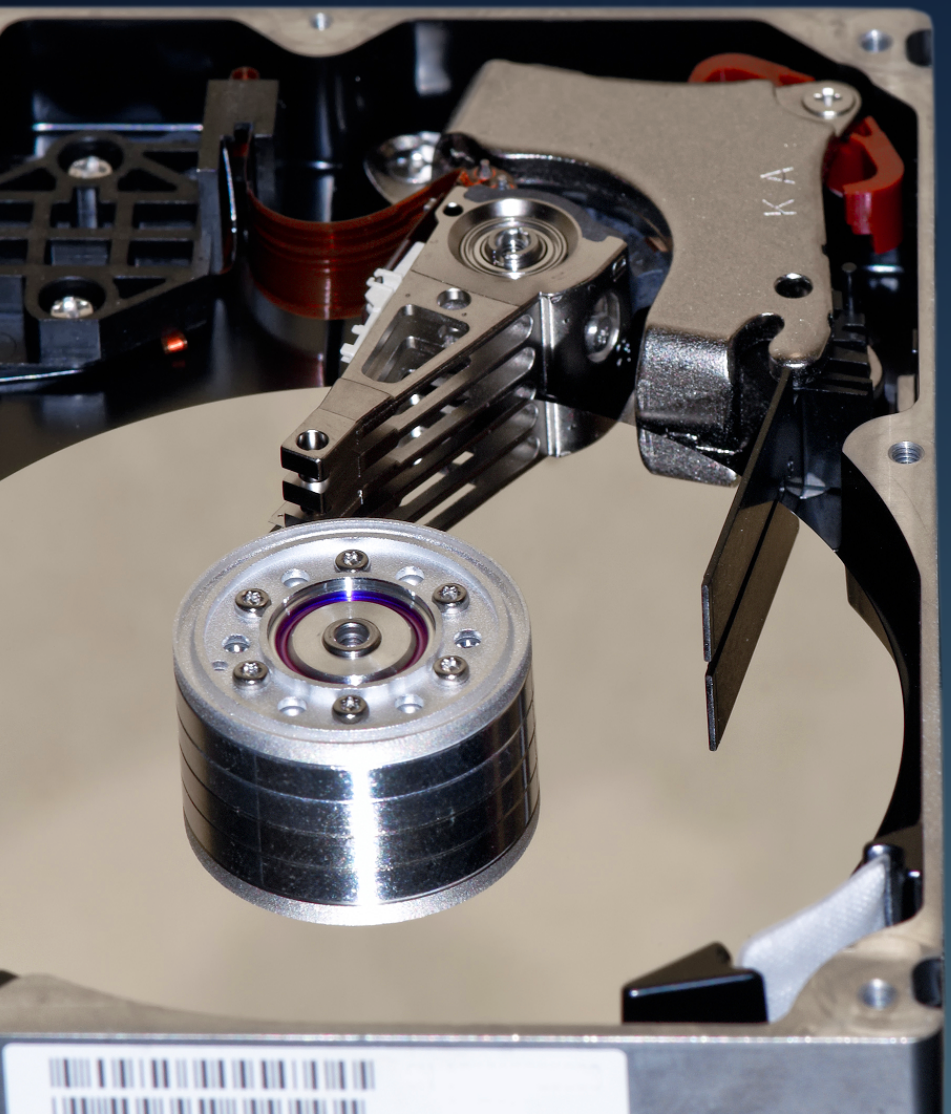


Le memorie

Come si fa?

Demo

Che memorie conosciamo?



Hard disk

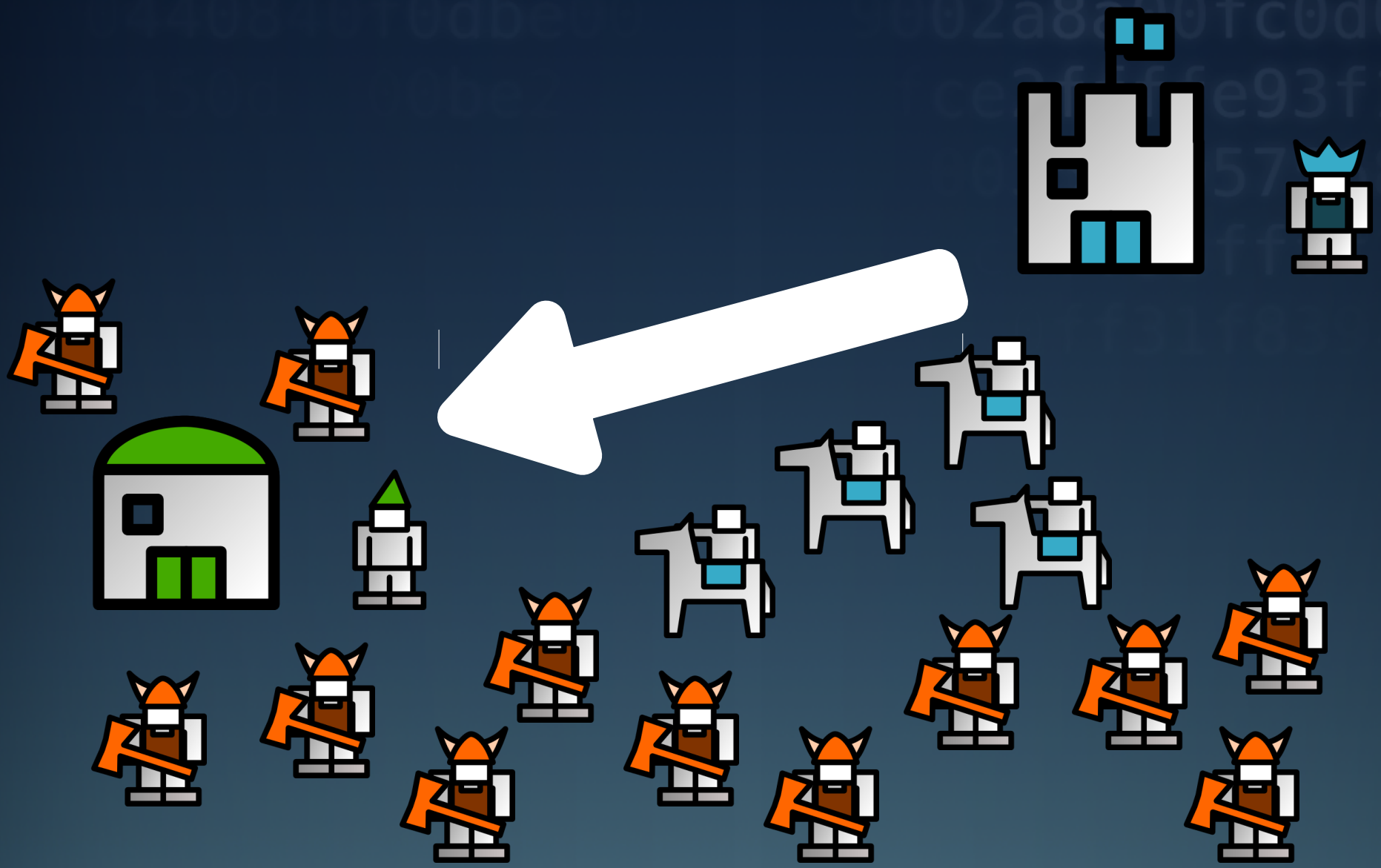
Pendrive

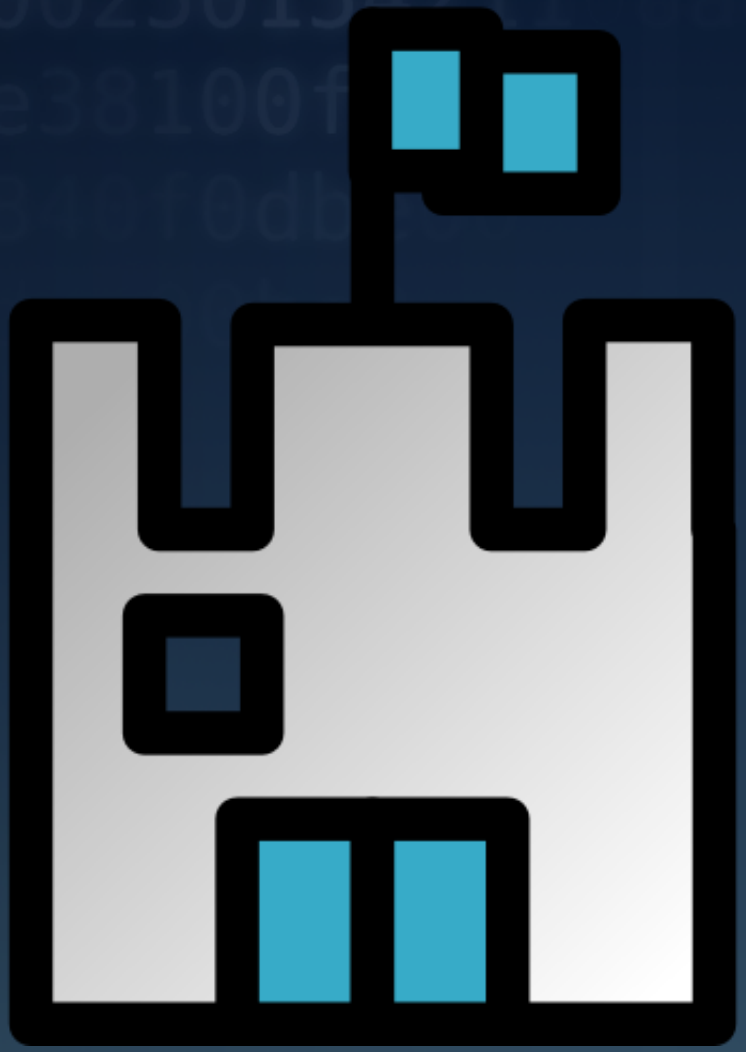
Schede SD

Compact flash

...

Storiella semi-seria





Utente ignaro

Sistema operativo

Filesystem

Software di recupero

Linux: tutto è un file

Come si fa?

Copia memoria

Analisi struttura

Carving

```
andrea@andrea-laptop:~$ dmesg | tail
[10129.333665] scsi 5:0:0:0: Direct-Access  PLEOMAX  m80 8GB  0000 PQ: 0 ANSI: 0 CCS
[10129.334198] sd 5:0:0:0: Attached scsi generic sg2 type 0
[10129.339258] sd 5:0:0:0: [sdb] 15663104 512-byte logical blocks: (8.01 GB/7.46 GiB)
[10129.340127] sd 5:0:0:0: [sdb] Write Protect is off
[10129.340130] sd 5:0:0:0: [sdb] Mode Sense: 43 00 00 00
[10129.340132] sd 5:0:0:0: [sdb] Assuming drive cache: write through
[10129.344755] sd 5:0:0:0: [sdb] Assuming drive cache: write through
[10129.344764]  sdb: sdb1
[10129.363746] sd 5:0:0:0: [sdb] Assuming drive cache: write through
[10129.363750] sd 5:0:0:0: [sdb] Attached SCSI removable disk
```

Identificare il dispositivo

```
andrea@andrea-laptop:~$ sudo fdisk -l /dev/sdb

Disco /dev/sdb: 8019 MB, 8019509248 byte
247 testine, 62 settori/tracce, 1022 cilindri
Unità = cilindri di 15314 * 512 = 7840768 byte
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Identificativo disco: 0x000a38f6

Dispositivo Boot      Start         End      Blocks   Id  System
/dev/sdb1   *             1        1022     7825423    c  W95 FAT32 (LBA)
```

Visualizzare le partizioni


dd

sudo dcfldd if=/dev/sdb of=chiavetta.img bs=4096

I tre “guerrieri”

Testdisk

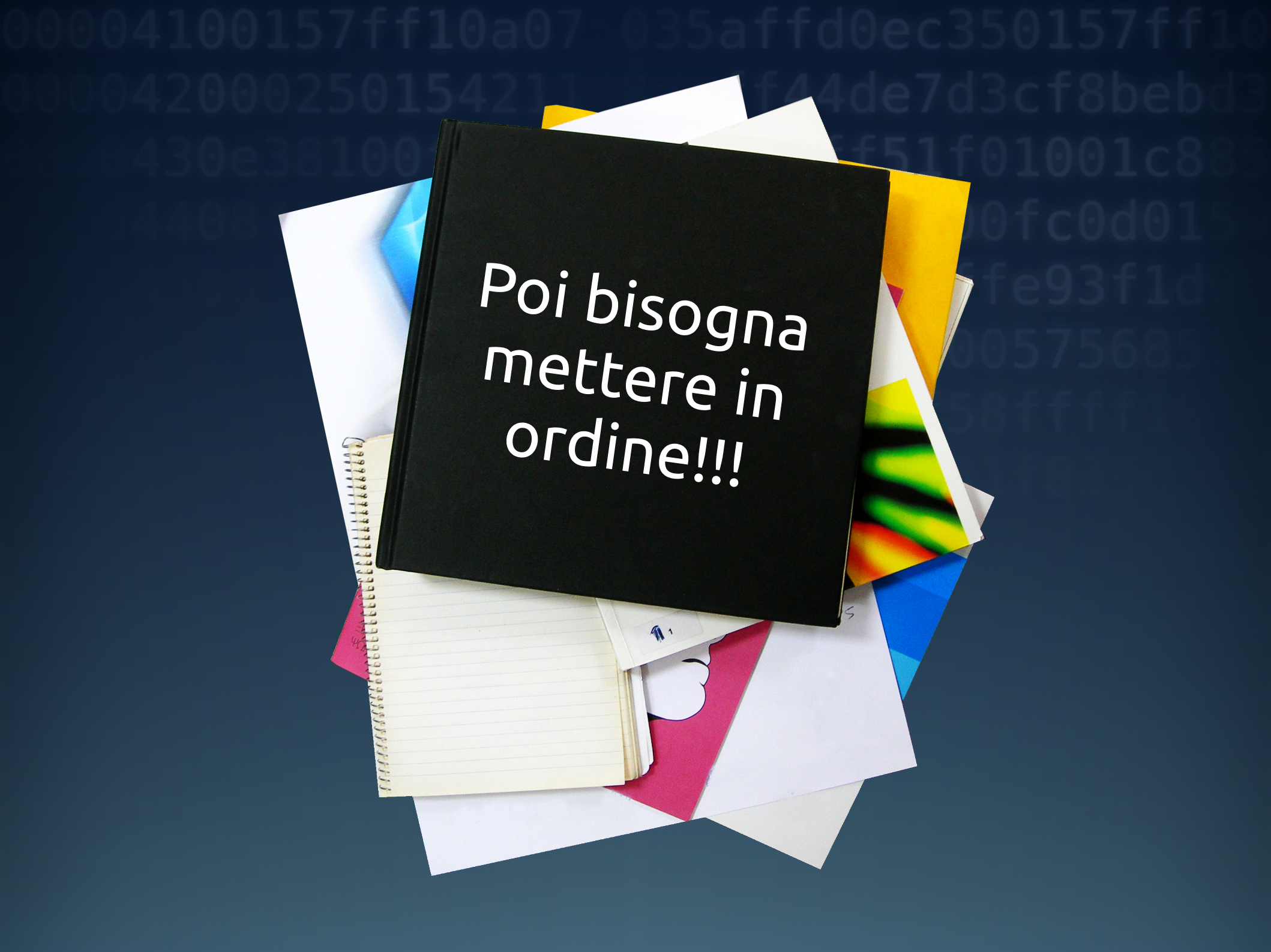
Photorec

Autopsy browser

Testdisk: recupero di partizioni

Photorec: bulk file carving

Autopsy browser: funzioni avanzate

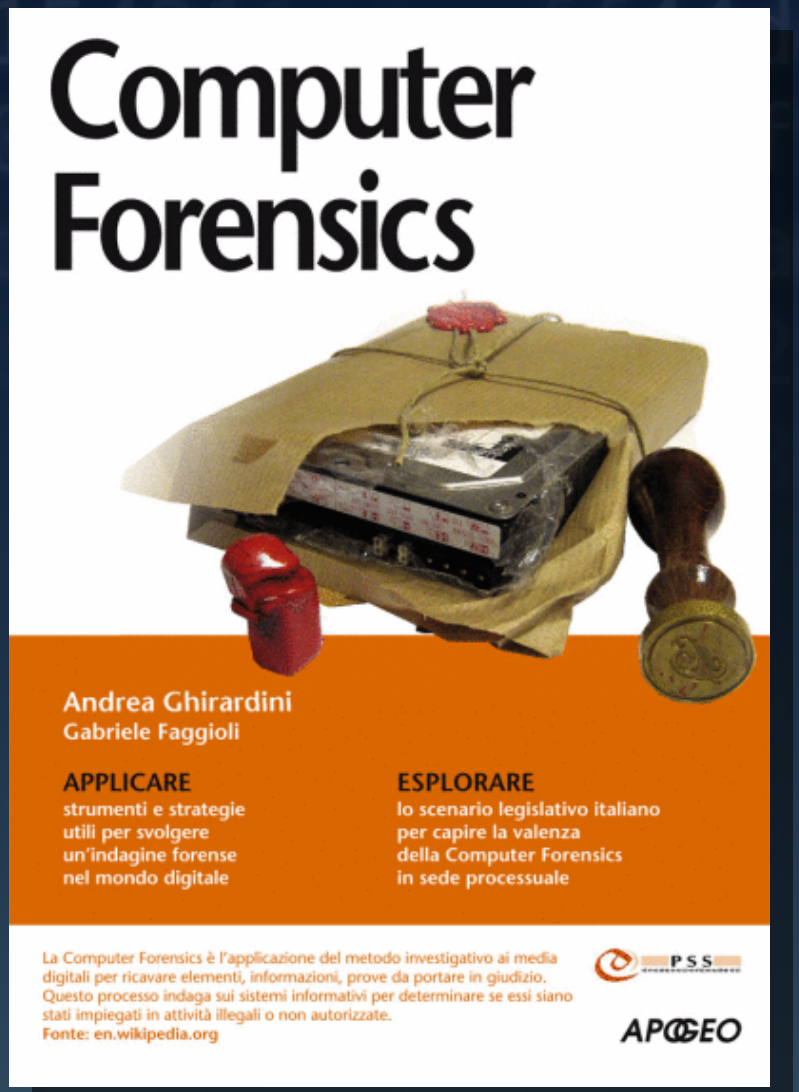

Poi bisogna
mettere in
ordine!!!

Dove trovo tutto?

Helix

Deft

Caine



http://bit.ly/libro-forensics

Demo