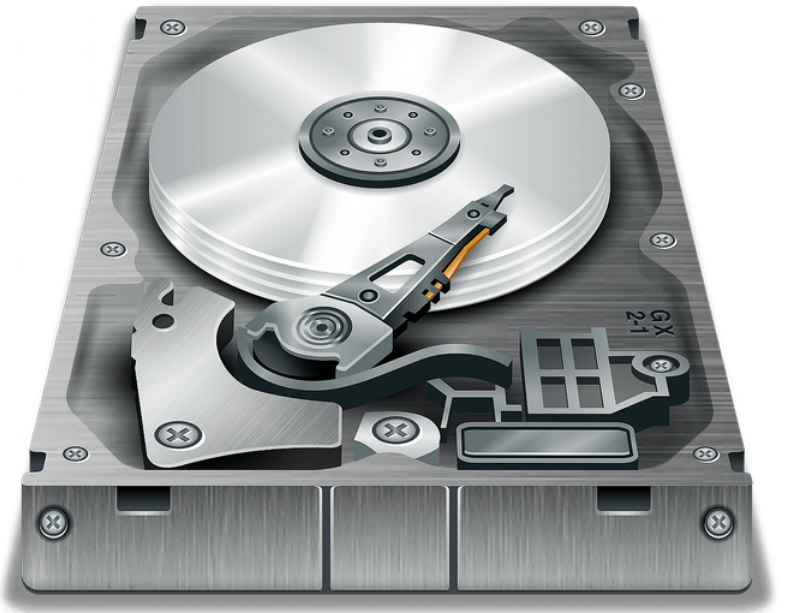
Lugvicenza

Recuperare dati da partizioni NTFS danneggiate



Andrea Lazzarotto — andrealazzarotto.com

Mi presento

Sviluppatore software e consulente informatico

Autore di script per il download da Rai, Mediaset, La7, RSI, BBC

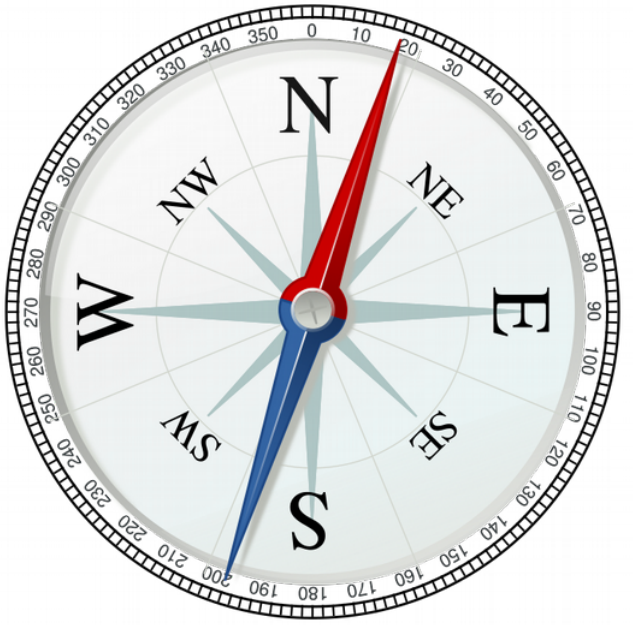
Creatore di RecuperaBit

Percorso

Descrizione del problema

Ricostruire NTFS

Il software



Descrizione del problema

Backup

> «Sono scioccato che un utente prenda le proprie cose più importanti (foto dei bambini, dati aziendali, ecc) e non le tenga al sicuro (backup). Ho un'azienda che fa soldi in **un settore che non dovrebbe nemmeno esistere,** francamente.»
> — Kevin Ripa in Let’s Talk About Data Recovery

Recupero dati

Motivazioni

Indagini

Danni o errori

Carving

Significa “scavare”

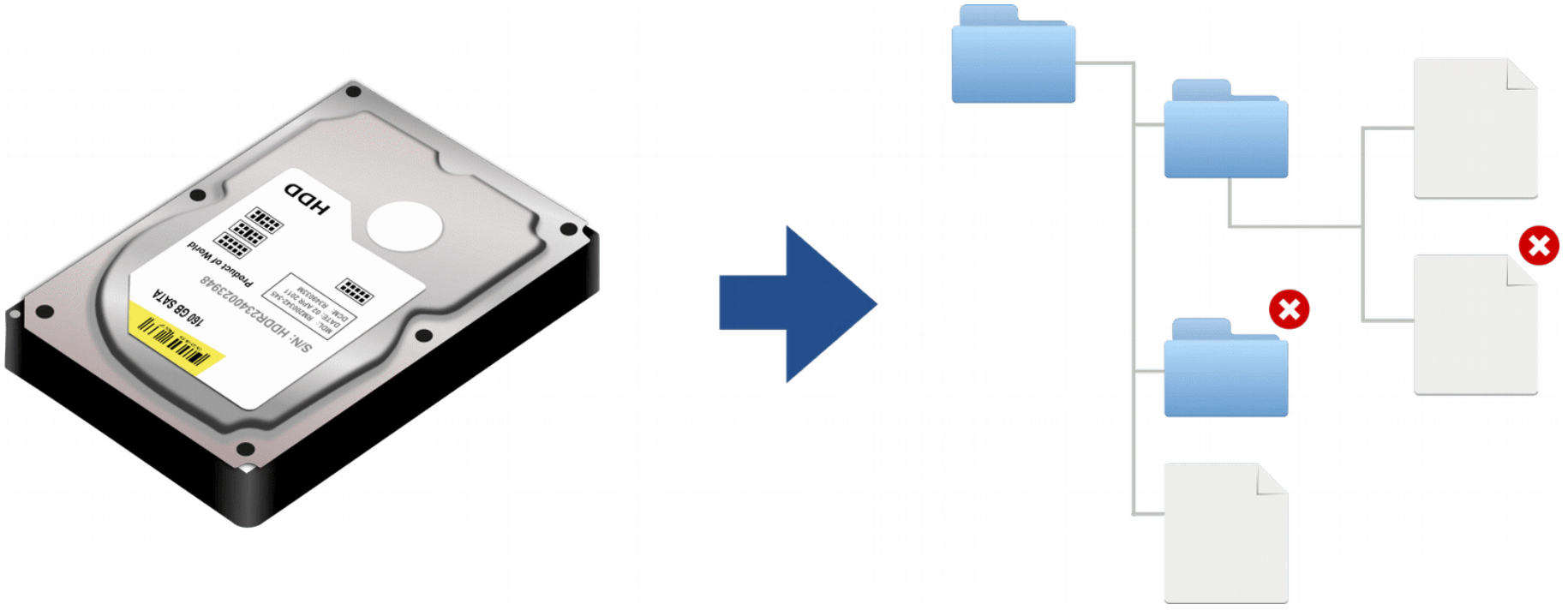
Nessuna struttura delle directory

L’esatto contrario di ciò che vogliamo

Problemi comuni

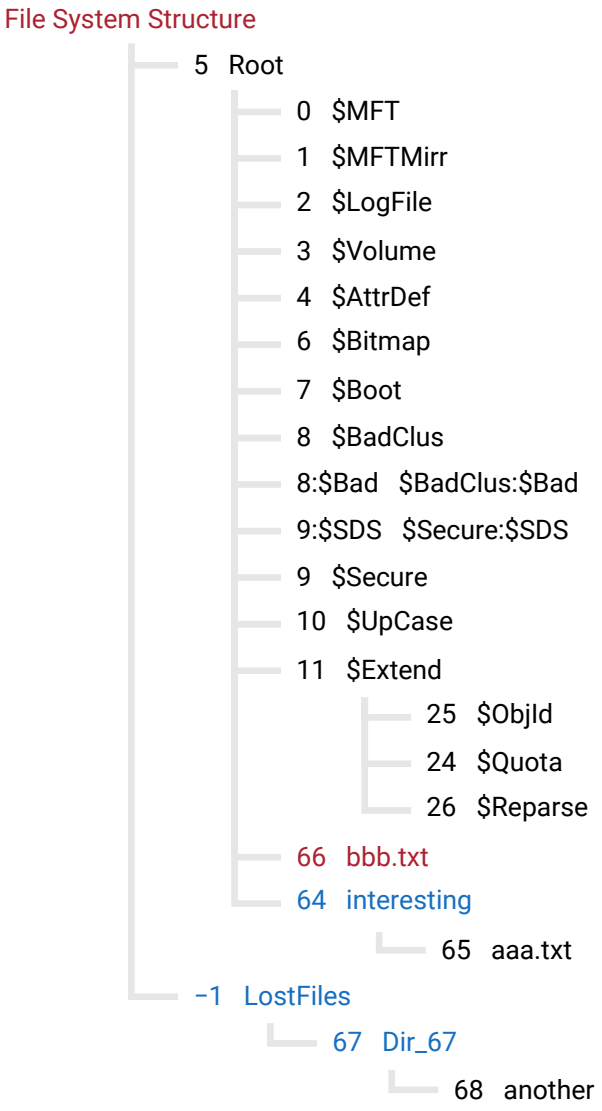
File cancellati

Partizione non trovata



Ricostruzione

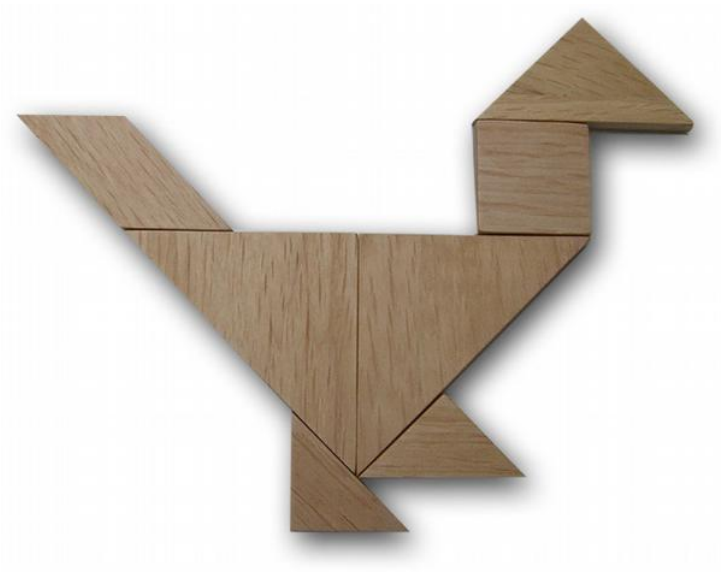
Risultato


File System Structure
5 Root
0 $MFT
1 $MFTMirr
2 $LogFile
3 $Volume
4 $AttrDef
6 $Bitmap
7 $Boot
8 $BadClus
8:$Bad $BadClus:$Bad
9:$SDS $Secure:$SDS
9 $Secure
10 $UpCase
11 $Extend
25 $ObjId
24 $Quota
26 $Reparse
66 bbb.txt
64 interesting
65 aaa.txt
-1 LostFiles
67 Dir_67
68 another

Ricostruire NTFS

NTFS

Molto diffuso



Struttura variabile

Cluster

Gruppi da 1, 2, 4, 8, 16… settori

Elementi principali

```
[…]
0x55 0xAA
```

(512 byte)

Boot sector

```
FILE
[…]
```

(1024 byte)

File record

```
INDX
[…]
```

(4096 byte)

Index record

> «[…] valori a 64-bit che rappresentano il numero di *centinaia di nanosecondi* dal 1° Gennaio 1601 UTC, che è utile se dovete analizzare **un computer che è stato usato nel diciottesimo secolo.**»
> — Brian Carrier in File System Forensic Analysis

Le date in NTFS

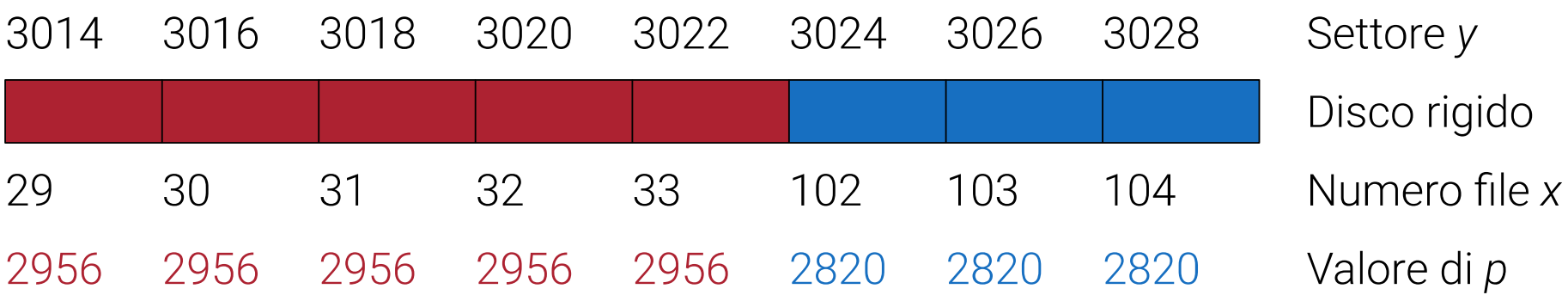
Algoritmo

Il disco viene **scansionato** (carving dei metadati)

I file vengono **partizionati** (clustering)

La struttura ad albero viene ricostruita

Clustering

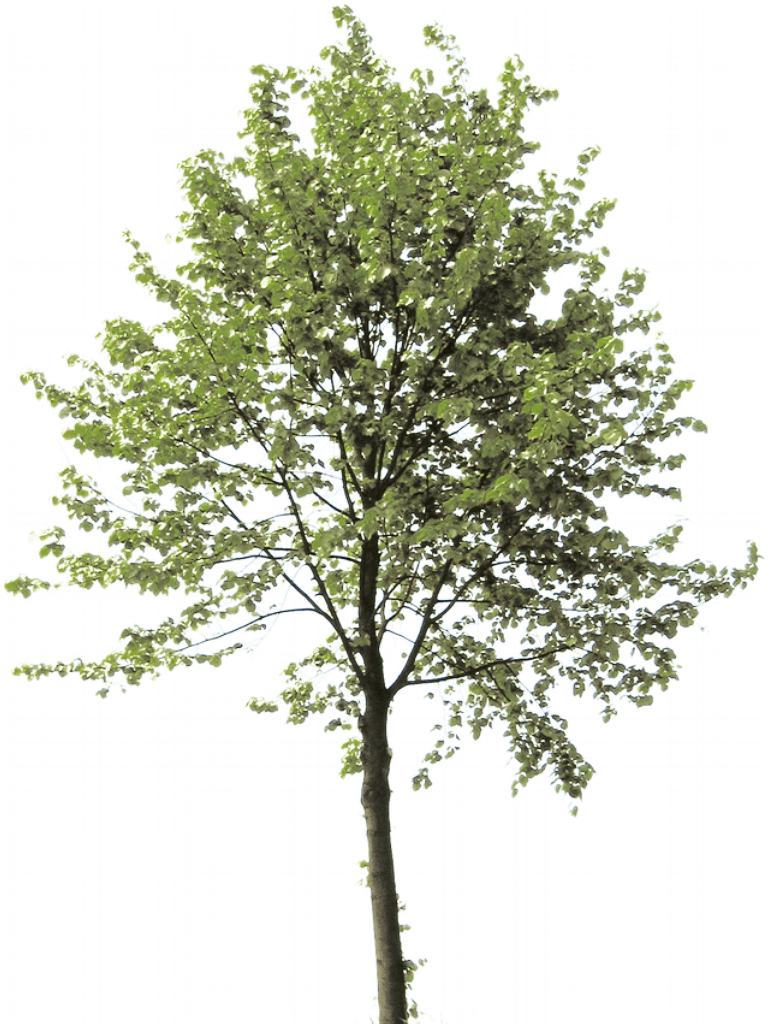


Posizione del **file numero 0:** $p = y - 2 \cdot x$

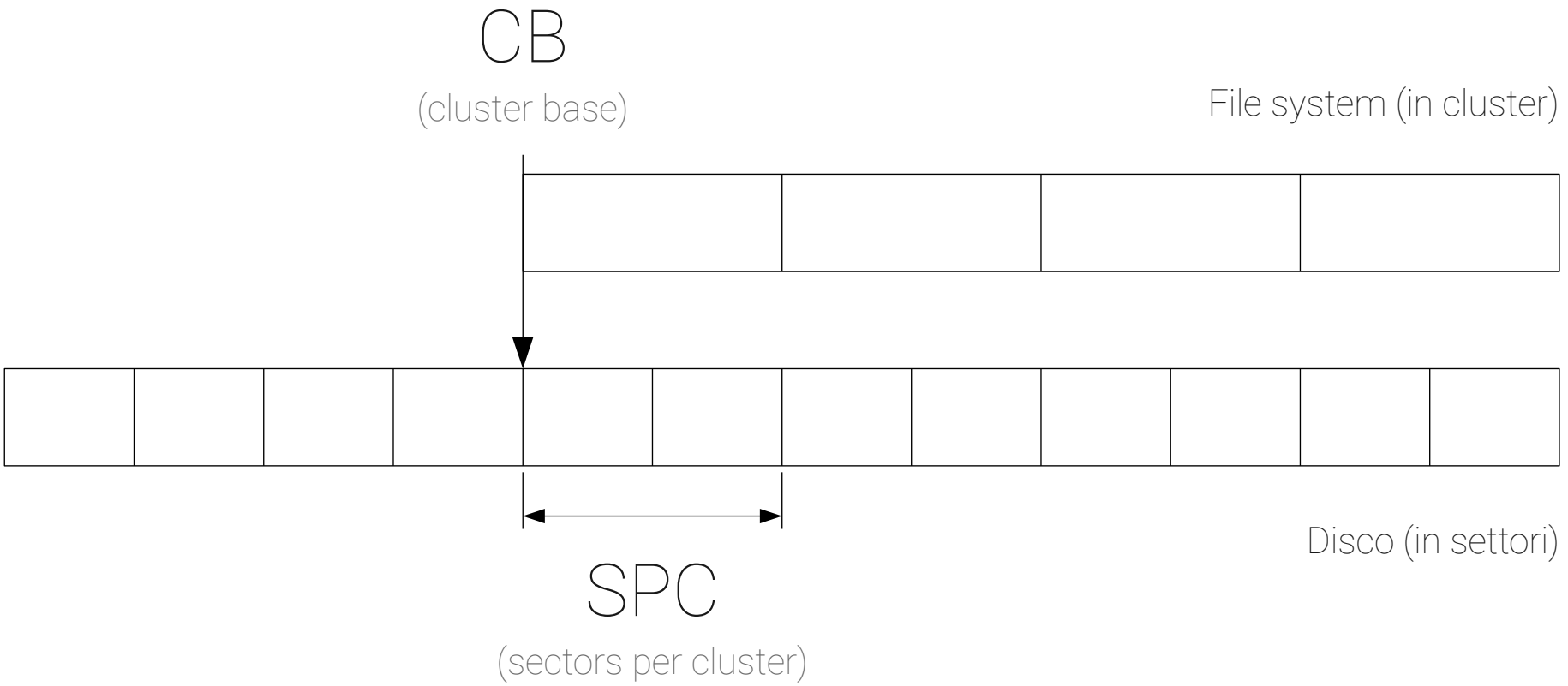
Albero delle directory

Ogni nodo è **collegato** a quello superiore

Se non esiste, viene messo sotto a *Lost Files*



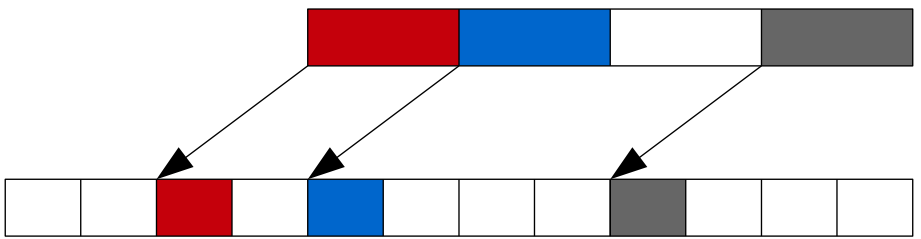
Geometria


CB
(cluster base)
File system (in cluster)
Disco (in settori)
SPC
(sectors per cluster)

Matching

CB e SPC ▸ **Necessari** per recuperare i file

Usiamo i riferimenti agli indici delle directory



Riferimenti relativi a index record

Index record presenti nel disco

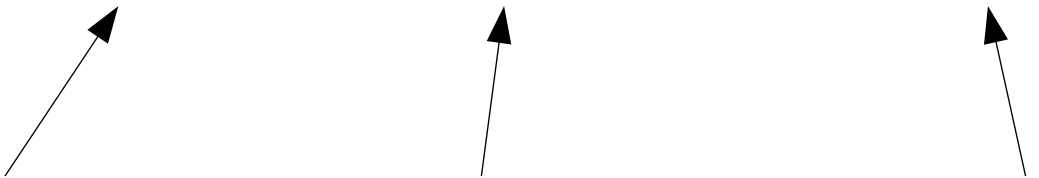
Il software

Copia bitstream

Motivo
Non tutti i restauri
riescono subito

Acquisizione

```
ddrescue /dev/sdb copia.img status.log
```



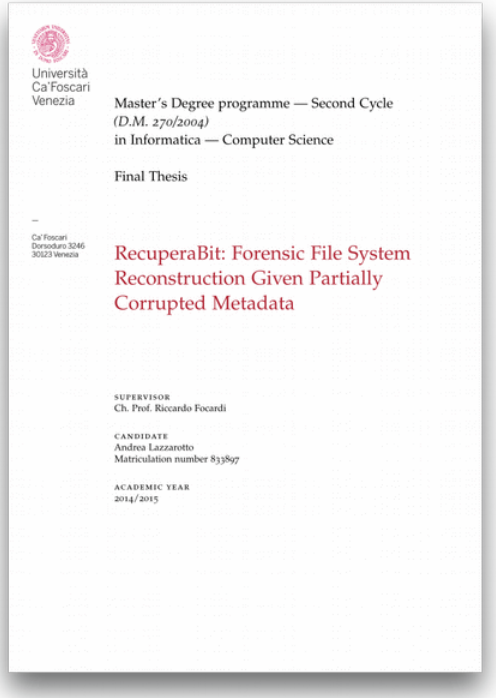
Dispositivo Destinazione File di log

RecuperaBit

Scritto in Python

Modulare e estendibile

Pieno supporto a NTFS



Università
Ca'Foscari
Venezia

Master's Degree programme — Second Cycle
(D.M. 270/2004)
in Informatica — Computer Science

Final Thesis

Ca'Foscari
Dorsoduro 3246
30123 Venezia

RecuperaBit: Forensic File System Reconstruction Given Partially Corrupted Metadata

SUPERVISOR
Ch. Prof. Riccardo Focardi

CANDIDATE
Andrea Lazzarotto
Matriculation number 833897

ACADEMIC YEAR
2014/2015

Riconoscimento file system

Software	#1	#2	#3	#4
Gpart	OK	OK	Niente	Parziale
TestDisk	OK	OK	Niente	OK
Autopsy	OK	Parziale	Niente	OK
Scrounge-NTFS	OK	OK	Niente	OK
Restorer Ultimate	OK	OK	OK	OK
DMDE	OK	OK	OK	OK
Recover It All Now	OK	Niente	Niente	OK
GetDataBack	OK	OK	Niente	OK
SalvageRecovery	OK	OK	Niente	OK
RecuperaBit	OK	OK	OK	OK

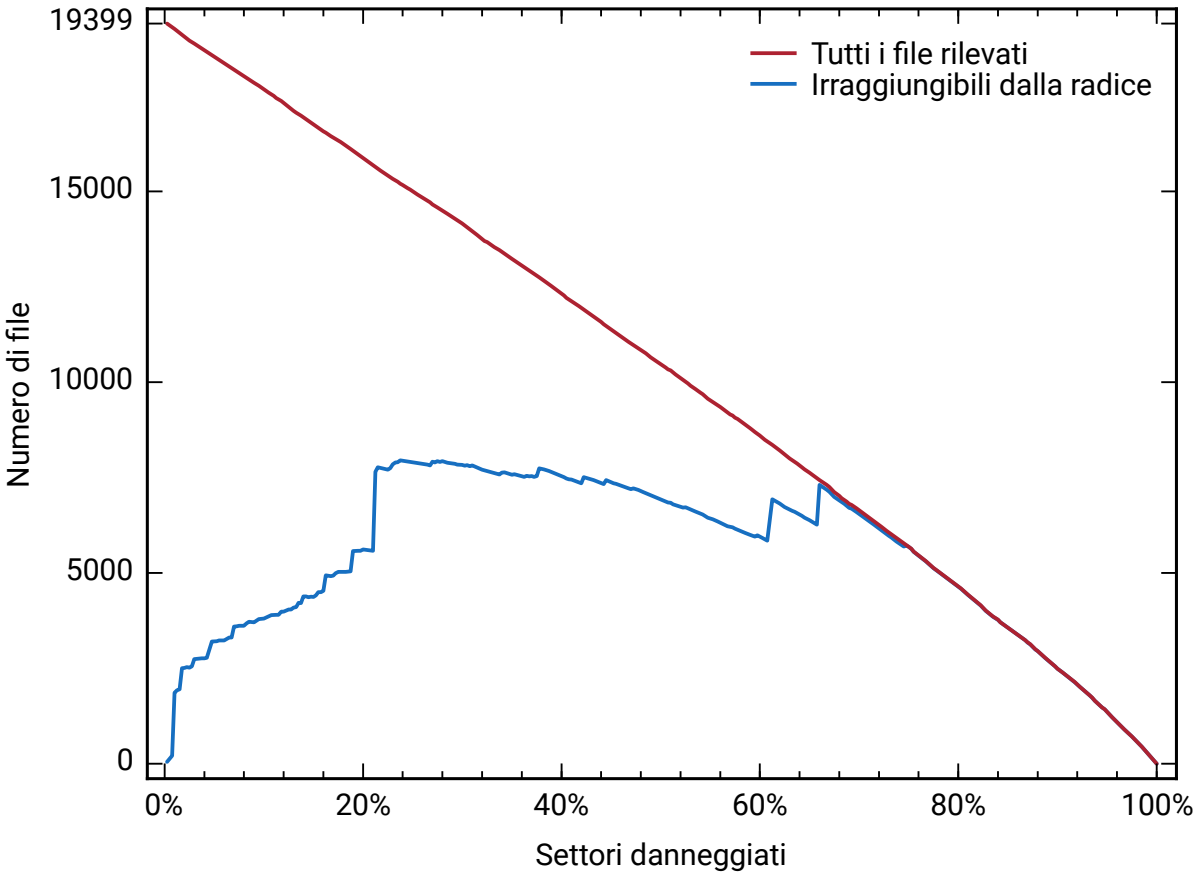
Accuratezza della ricostruzione

Software	#1	#2	#3	#4
TestDisk	Perfetta	Errore	—	Errore
Autopsy	Perfetta	Nessun file	—	Buona
Scrounge-NTFS	Parziale	Terribile	Terribile	Terribile
Restorer Ultimate	Perfetta	Parziale	Perfetta	Buona
DMDE	Perfetta	Errore	Perfetta	Buona
Recover It All Now	Terribile	—	—	Nessun file
GetDataBack	Perfetta	Buona	—	Buona
SalvageRecovery	Perfetta	Terribile	—	Perfetta
RecuperaBit	Perfetta	Perfetta	Perfetta	Perfetta

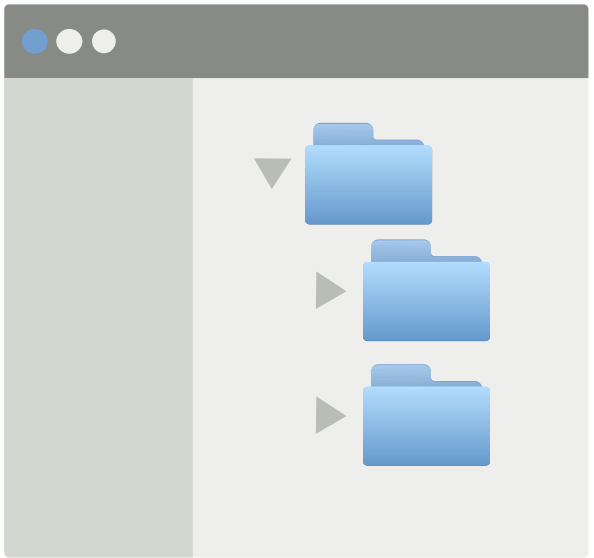
Contenuto dei file

Software	Sparsi	Compressi	Criptati
TestDisk	OK	OK	Vuoto
Autopsy	Vuoto	OK	OK
Scrounge-NTFS	OK	Non implementato	OK
Restorer Ultimate	OK	OK	OK
DMDE	OK	OK	Non implementato
Recover It All Now	OK	Errato	OK
GetDataBack	Vuoto	OK	OK
SalvageRecovery	Vuoto	Errato	OK
RecuperaBit	OK	Non implementato	OK

Danni vs file rilevati



In futuro...



FAT, EXT,
HFS+, ...

GUI

Altri moduli

CAINE

Domande