

---

# Voľne šíriteľné nástroje na obnovu zmazaných súborov

Norbert Matuška

Princípy Informačnej Bezpečnosti

Streda 10:00

---

---

# Obsah

## Súborové systémy

- Základné informácie
- Proces mazania dát
- Proces obnovy dát

## Nástroje

- Testdisk
- Recuva
- Photorec

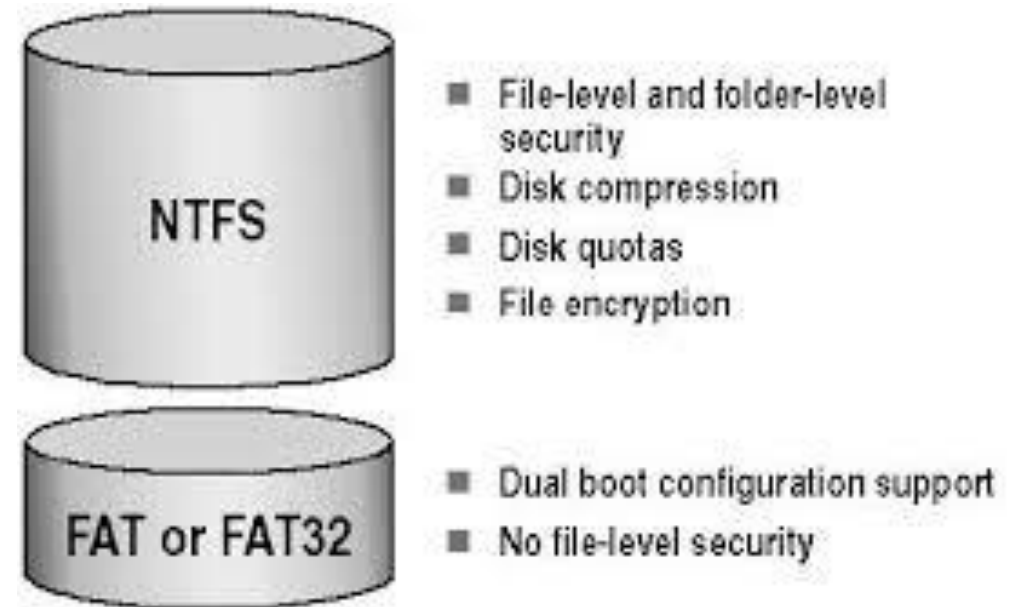
## Budúce plány

---

---

# Súborové systémy

- FAT32
  - Starší, obmedzenia
- NTFS
  - Moderný, podpora šifrovania, pokročilejšie možnosti
- EXT4
  - Linux, menšia fragmentácia, zložitejšia obnova



---

## Proces mazania dát

### Mazanie vo FAT32

- Maže sa iba odkaz v tabuľke

### Mazanie v NTFS

- Záznam je označený ako nepoužitý

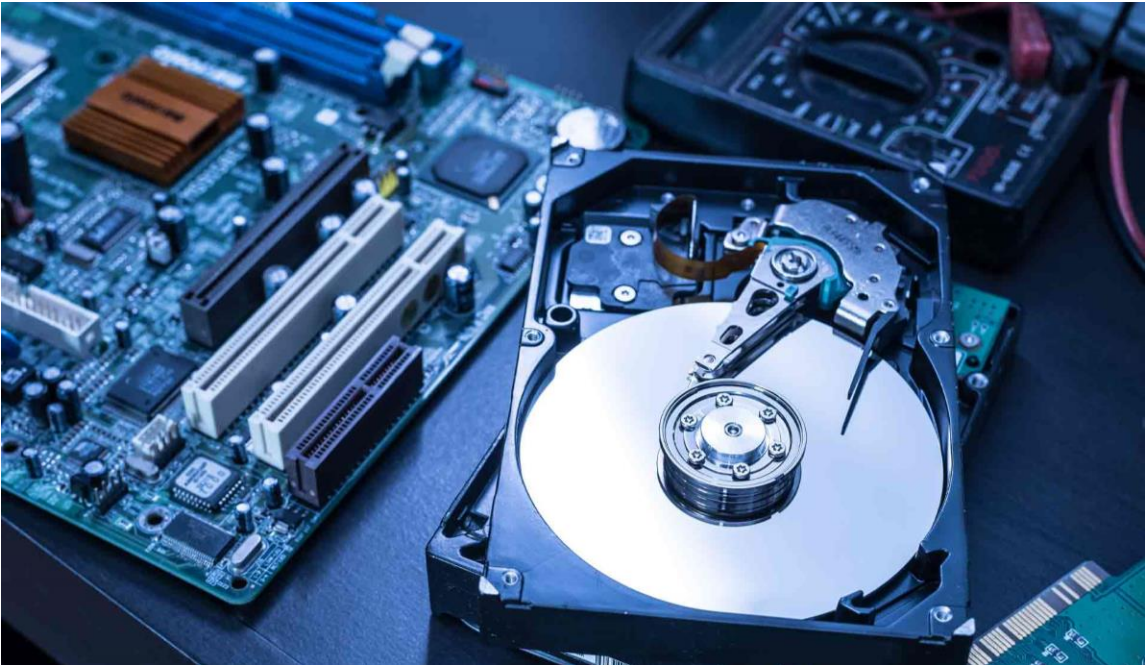
### Mazanie v EXT4

- Bloky sa označia ako voľné
-

---

# Obnova dát

- FAT32
  - Jednoduchá
- NTFS
  - MFT, denníkovanie pomáha
- EXT4
  - zložitejšia



# TestDisk

- Open-source nástroj na obnovu partícií a souborů z viacerých systémů (FAT32, NTFS, EXT4). Môže opraviť bootovacie sektory a prepisovať zálohy.
- Postup obnovy:
  - Skenuje, hľadá záznamy v tabulke, neporušené časti
- Podporuje viacero súborových systémů

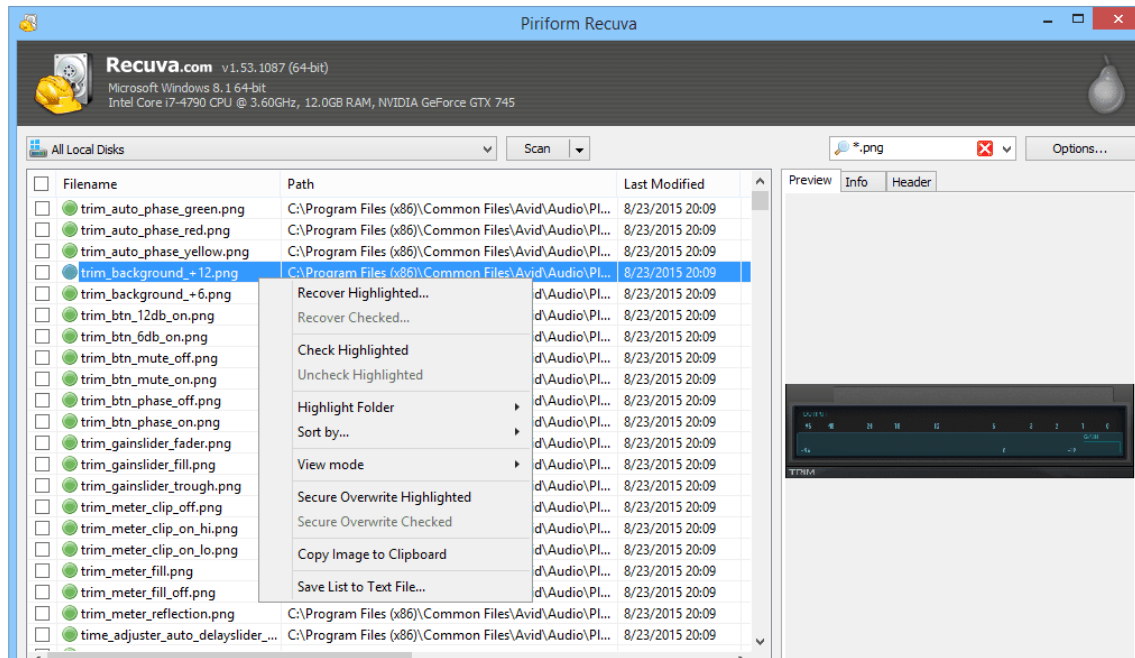
```
TestDisk 6.9, Data Recovery Utility, February 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 20 GB / 18 GiB - CHS 2432 255 63
Partition      Start      End      Size in sectors
* HPFS - NTFS   0 1 1 636 254 63 10233342 [Win2k]
D HPFS - NTFS   636 254 63 1273 254 63 10233406
D HPFS - NTFS   637 0 1 2430 254 63 28820610 [Data]
P HPFS - NTFS   1274 0 1 2426 254 63 18522845 [Data]
D FAT32 LBA     2304 1 1 2431 254 63 2056257 [NO NAME]
L FAT32 LBA     2427 1 1 2431 254 63 80262 [ACRONIS SZ]

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
Keys A: add partition, L: load backup, T: change type, P: list files,
Enter: to continue
FAT32, 41 MB / 39 MiB
```

# Recuva

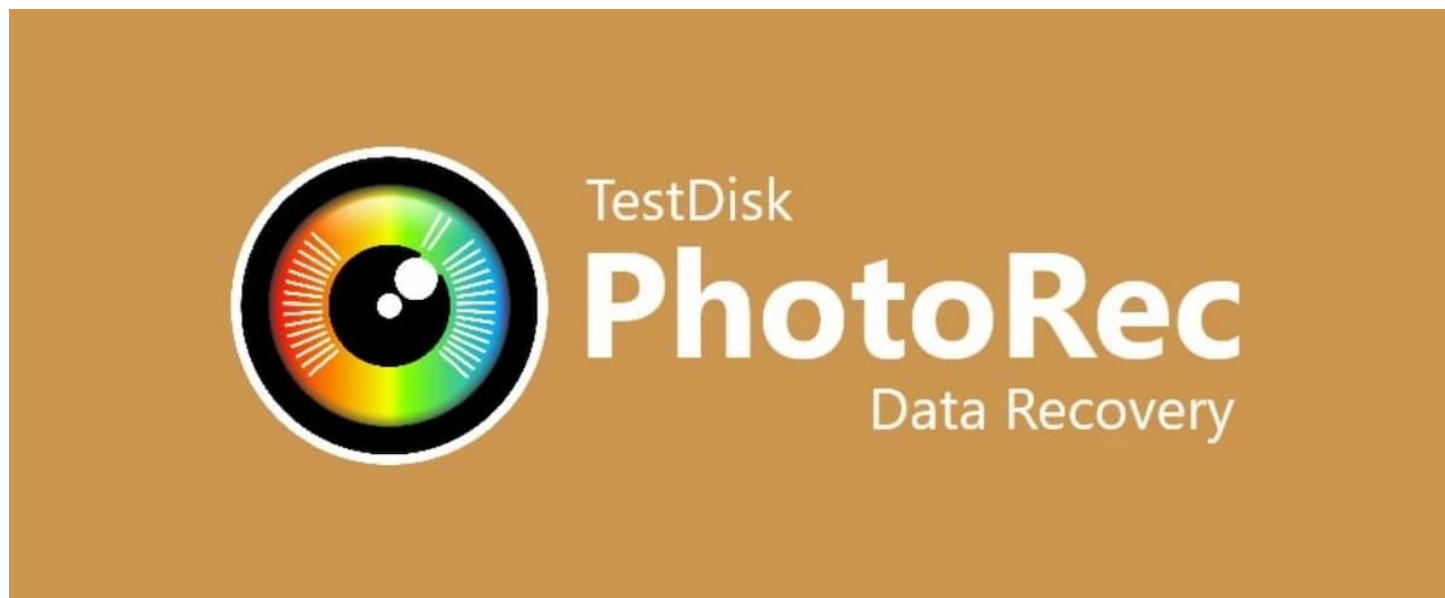
- Používateľsky priateľský nástroj na Windows, umožňuje rýchlu obnovu súborov z rôznych médií.
- Deep Scan - prehľadáva disk sektor po sektore.
  - Zobrazuje stav súborov (zmazané, poškodené, dostupné na obnovu).



---

# Photorec

- Nástroj na obnovu založený na signatúrach súborov, umožňuje obnovu z poškodených súborových systémov.
- Vyvíjaný najprv na obnovu multimediálnych súborov
  - Dnes odporuje širokú škálu súborových formátov





---

## Do budúcnosti

### **TestDisk:**

Najuniverzálnejší,  
vhodný pre obnovu  
súborov aj partícií

**Recuva:** Najjednoduchší  
na použitie pre bežných  
používateľov, rýchla  
obnova z Windows  
zariadení

**PhotoRec:** Silný nástroj  
na obnovu  
multimediálnych  
súborov, najlepší na  
poškodené disky

---

---

# Otázky?

---

---

# Zdroje

---

<https://answers.microsoft.com/en-us/windows/forum/all/what-is-the-maximum-file-size-fat-fat32-ntfs-file/1663db6b-490e-4021-9e36-f7a6976ac0c0>

---

[https://en.wikipedia.org/wiki/File\\_Allocation\\_Table](https://en.wikipedia.org/wiki/File_Allocation_Table)

---

<https://www.file-recovery.com/recovery-NTFS-data-recoverability-and-integrity.htm>

---

<https://en.wikipedia.org/wiki/NTFS>

---

<https://wiki.archlinux.org/title/Ext4>

---

[https://docs.redhat.com/en/documentation/red\\_hat\\_enterprise\\_linux/6/html/storage\\_administration\\_guide/ch-ext4#ext4creating](https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/6/html/storage_administration_guide/ch-ext4#ext4creating)

---

<https://en.wikipedia.org/wiki/TestDisk>

---

<https://www.cgsecurity.org/wiki/TestDisk>

---

<https://en.wikipedia.org/wiki/Recuva>

---

[https://support.ccleaner.com/s/article/how-does-recuva-works?language=en\\_US](https://support.ccleaner.com/s/article/how-does-recuva-works?language=en_US)

---

<https://en.wikipedia.org/wiki/PhotoRec>

---

<https://superuser.com/questions/1193468/how-the-photorec-works-internally-and-how-to-use-it-in-ubuntu14-04>

---