https://www.cgsecurity.org/wiki/TestDisk: undelete file for FAT

cgsecurity.org

TestDisk: undelete file for FAT

This Recovery example guides you through <u>TestDisk</u> step by step to undelete files from the FAT (FAT12/FAT16/FAT32) and VFAT filesystem. FAT is mainly used on memory cards from digital cameras and on USB keys. VFAT can be found mainly on external harddisks formated under Windows. It's possible to recover your deleted files. When a file is deleted, the filename is marked as deleted and the data area as unallocated/free, but TestDisk can read the deleted directory entry and find where the file began. If the data area hasn't been overwritten by a new file, the file is recoverable.

Running TestDisk executable

If TestDisk is not yet installed, it can be downloaded from <u>TestDisk Download</u>. Extract the files from the archive including the sub-directories.

To recover a lost partition or repair the filesystem from hard disk, USB key, Smart Card, etc., you need enough rights to access a physical device.

To recover a partition from a media image or repair a filesystem image, run

- testdisk image.dd to carve a raw disk image
- testdisk image.E01 to recover files from an Encase EWF image
- testdisk 'image.???' if the Encase image is split into several files.

To repair a filesystem not listed by TestDisk, run testdisk device, i.e.

- testdisk /dev/mapper/truecrypt0 or testdisk /dev/loop0 to repair the NTFS or FAT32 boot sector files from a TrueCrypt partition. The same method works with a filesystem encrypted with cryptsetup/dm-crypt/LUKS.
- testdisk /dev/md0 to repair a filesystem on top of a Linux RAID device.

Log creation



- Choose Create unless you have a reason to append data to the log or if you execute TestDisk from read only media and must create it elsewhere.
- Press Enter to proceed.

Disk selection

All hard drives should be detected and listed with the correct size by TestDisk.

🔏 TestDisk	- X
TestDisk 6.10-WIP, Data Recovery Utility, February 2008 Christophe GRENIER <grenier@cgsecurity.org> http://www.cgsecurity.org</grenier@cgsecurity.org>	
TestDisk is free software, and comes with ABSOLUTELY NO WARRANTY.	
Select a media (use Arrow keys, then press Enter): Disk /dev/sda - 320 GB / 298 GiB - WDC WD3200KS-00PFB0 Disk /dev/sdb - 73 GB / 68 GiB - FUJITSU MAT3073NP Disk /dev/sdc - 36 GB / 34 GiB - IBM IC35L0360WD210-0 Disk /dev/sdd - 36 GB / 34 GiB - IBM DPSS-336950N Disk /dev/sdf - 36 GB / 34 GiB - IBM DPSS-336950N Disk /dev/sdf - 36 GB / 34 GiB - IBM DPSS-336950N	
[Proceed] [Quit]	
Note: Disk capacity must be correctly detected for a successful recovery. If a disk listed above has incorrect size, check HD jumper settings, BIOS detection, and install the latest OS patches and disk drivers.	
	-

- Use up/down arrow keys to select your hard drive with the lost partition/s.
- Press Enter to Proceed.

If available, use raw device /dev/rdisk* instead of /dev/disk* for faster data transfer.

Partition table type selection

TestDisk displays the partition table types.

- Select the partition table type usually the default value is the correct one as TestDisk auto-detects the partition table type.
- Press Enter to Proceed.

Start the undelete process

• Select Advanced



• Select the partition that was holding the lost files and choose **Undelete**



FAT file undelete

Deleted files and directories are displayed in red.

- To undelete a file, select the file to recover and press 'c' to copy the file.
- To recover a deleted directory, select the directory and press 'c' to undelete the directory and its content.



Select where recovered files should be written

Select the destination

	kmaster@adsl:~/src/testdisk _									
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	Ta <u>b</u> s <u>H</u>	<u>l</u> elp					
TestDisk 6.11-WIP, Data Recovery Utility, September 2008 Christophe GRENIER <grenier@cgsecurity.org> http://www.cgsecurity.org</grenier@cgsecurity.org>										
Are you sure you want to copy /_ULT1.DAT to the directory /home/kmaster/src/ /testdisk ? [Y/N]										
To se	lect a	another	directo	ory, use	the arrow ke	ys.				
drwxr	-xr-x	500	500	4096	22-Sep-2008	20:51				
drwxr	-XF-X	500	500	12288	20-Sep-2008	19:53 .				
drwxr	WXI-X	500	500	20480	20-Sep-2008	14:00 08:16 2005 08 06 Daric Blaco				
drwxr		500	500	4090	17-Apr-2005	15:23 AddressBook				
drwxr		500	500	4090	17-1ul-2007	18:58 BITLD				
drwxr	- 21-2	500	500	4096	25 - Jun - 2007	13:03 CVS				
drwxr	-xr-x	500	500	4096	16-Sen-2006	15:51 DCTM				
drwxr	-xr-x	500	500	4096	4-Aug-2008	07:55 System Volume Information				
drwxr	-xr-x	500	500	4096	26-Sep-2008	19:51 TMP				
drwxr	-xr-x	500	500	4096	14-Feb-2004	12:53 YSTEM~1				
drwxr	-xr-x	500	500	4096	10-Jul-2007	20:36 afflib-2.3.0				
drwxr	-xr-x	500	500	4096	12-Jun-2008	22:22 darwin				
drwxr	-xr-x	500	500	4096	25-Jun-2007	13:03 doc				
drwxr	-xr-x	500	500	4096	22-Sep-2008	20:35 doc src				
N	ext							\sim		

FAT file recovery is completed

When you get your files back, use Quit to exit.



For maximum security, TestDisk doesn't try to unerase files but lets you copy the deleted files onto another partition or disk. Remember, you must avoid writing anything on the filesystem that was holding the data. If you do, deleted files may be overwritten by new ones.

TestDisk can undelete

- files and directory from FAT12, FAT16 and FAT32 filesystem,
- <u>files from NTFS partition</u> since version <u>6.11</u>,
- <u>files from ext2 filesystem</u>.

If a lost file is still missing, give PhotoRec a try. <u>PhotoRec</u> is a signature based file recovery utility and may be able to recover your data where other methods have failed.