

# Testdisk - Hızlı Veri Kurtarma

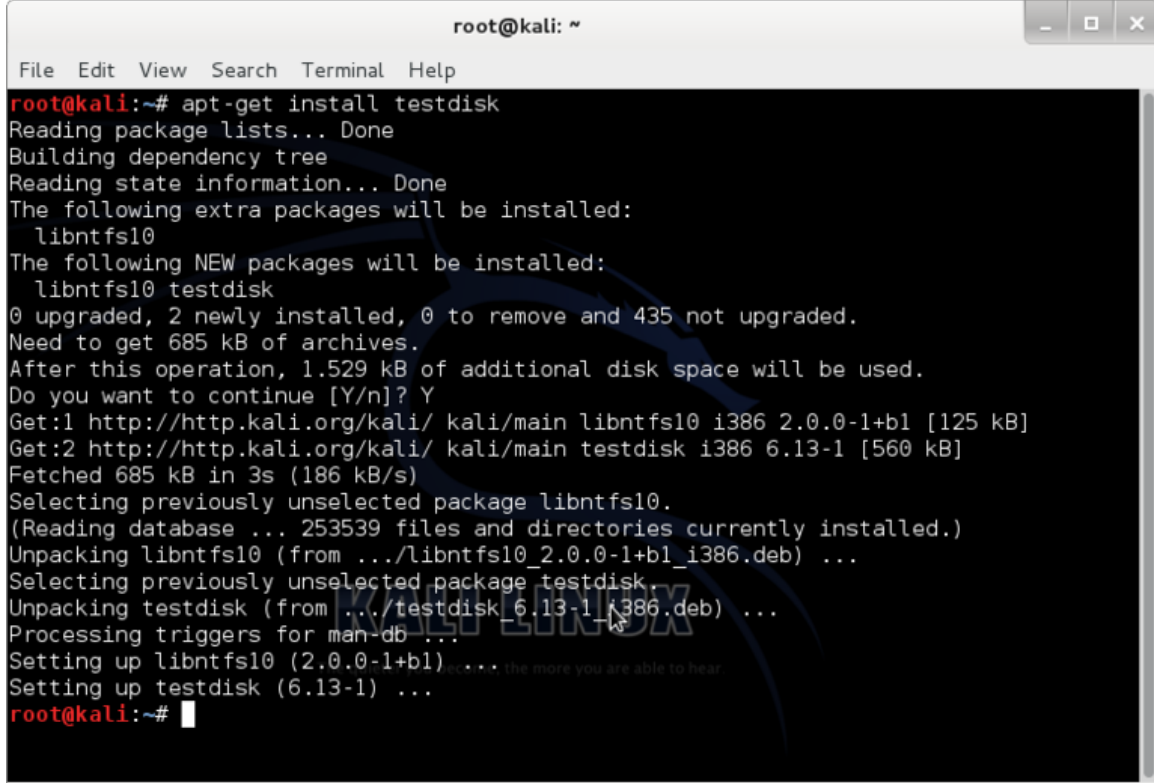
Barış Can

Eylül, 2013

Gerek günlük hayatımızda, gerekse kurumsal yaşantımızda veri depolama aygıtlarımız bir anda bozulabilir ve işlerimiz planladığımız gibi gitmeyebilir. Bu gibi durumlarda veri kurtarma araçlarını kullandığımızda, çoğu aracın sonucu saatler dahilinde verdiğini görürüz. Bu süreç, bilgisayarınızın donanımına da bağlı olabilir, programın kodlanış biçimine de. Gelelim, verilerimizi en hızlı şekilde nasıl kurtarabileceğimize. Yardımcımızın adı, testdisk.

Uçbirim aracılığı ile kolayca çalıştırılabilen bu program, basit bir şekilde hasar görmüş veri depolama aygıtındaki verileri kurtarmanıza ve sisteminize tekrar kopyalamanıza yardımcı olur.

Kullanımını Kali Linux üzerinde açıklayacağım bu programın kurulumunu, Debian işletim sistemi tabanlı tüm Linux dağıtımlarında aynı şekilde yapabilirsiniz.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get install testdisk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libntfs10
The following NEW packages will be installed:
  libntfs10 testdisk
0 upgraded, 2 newly installed, 0 to remove and 435 not upgraded.
Need to get 685 kB of archives.
After this operation, 1.529 kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://http.kali.org/kali/ kali/main libntfs10 i386 2.0.0-1+b1 [125 kB]
Get:2 http://http.kali.org/kali/ kali/main testdisk i386 6.13-1 [560 kB]
Fetched 685 kB in 3s (186 kB/s)
Selecting previously unselected package libntfs10.
(Reading database ... 253539 files and directories currently installed.)
Unpacking libntfs10 (from ../libntfs10_2.0.0-1+b1_i386.deb) ...
Selecting previously unselected package testdisk.
Unpacking testdisk (from ../testdisk_6.13-1_i386.deb) ...
Processing triggers for man-db ...
Setting up libntfs10 (2.0.0-1+b1) ... the more you are able to hear
Setting up testdisk (6.13-1) ...
root@kali:~#
```

Şekil 1:

Kurulum için uçbirim'e "**apt-get install testdisk**" yazıyoruz ve programımız kuruluyor.

Bu aşamadan sonra, uçbirim'e testdisk yazıp programımızı çalıştırıyoruz.

Program açılıştan itibaren yazısını sunuyor ve bize seçenekler sunuyor. Yeni bir veri kurtarma çalışması yapacağımızdan, "create" seçimini yapıp Enter'e basarak devam ediyoruz.

Ardından, bizden listelediği sürücü ya da aygıtlar arasından seçim yapmamızı istiyor. Burada biraz dikkatli olmamız gerekiyor zira yanlış sürücü ya da aygıt seçimleri yanlış şeylere neden olabiliyor. Hasar görmüş olan veri depolama aygıtımızı seçip, yolumuza Enter tuşu ile devam ediyoruz.

Bu bölüm biraz daha önem arz ediyor. Eğer, kurtarmaya çalıştığınız sadece harici bir veri depolama aygıtı ise "none" kısmı bu iş için uygundur; lakin, kurtarmaya çalıştığınız işletim sisteminize bağlı dahili depolama aygıtınız ise, buna göre seçim yapmalısınız. Örneğin, işletim sisteminiz (aygıtı bağlı) Linux ya da Windows ise "Intel" gibi...

Bu bölümü de atlayıp yolumuza devam ediyoruz.

Bu bölümde dahil, bu bölümden sonra atacağımız her adımda dikkatli olmamızda yarar var. Bilmediğimiz şeyleri yapmamakta da öyle. "Analyse" bizim için uygun olan seçenek.

```
root@kali: ~
File Edit View Search Terminal Help
TestDisk 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

TestDisk is free data recovery software designed to help recover lost
partitions and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.

Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
>[ Create ] Create a new log file
  [ Append ] Append information to log file
  [ No Log ] Don't record anything
```

Şekil 2:

Burada da, "Quick Search" diyerek devam ediyoruz zira başka bir seçenek yok.

Bize yapacağımız taramadan emin olup olmadığımız soruluyor ve "y" ya da "yes" yazarak yolumuza devam ediyoruz.

ve Tarama başlıyor. Tarama bittikten sonra kurtardığı verileri görmek için "P" harfini kullanıp, bulduğunuz verileri sisteminize kopyalamak için yön tuşları ile istediğiniz veri üzerine gelip "C" tuşunu kullanabilirsiniz.

Bu tür sorunlar yaşamamanız dileğiyle...

```
root@kali: ~
File Edit View Search Terminal Help
TestDisk 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 32 GB / 30 GiB - VMware, VMware Virtual S
>Disk /dev/sdb - 987 MB / 941 MiB - SAMSUNG GT-S5660 Card

>[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.
```

Şekil 3:

```
root@kali: ~
File Edit View Search Terminal Help
TestDisk 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 987 MB / 941 MiB - SAMSUNG GT-S5660 Card

Please select the partition table type, press Enter when done.
>[Intel ] Intel/PC partition
[EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
[Humax  ] Humax partition table
[Mac    ] Apple partition map
[None   ] Non partitioned media
[Sun    ] Sun Solaris partition
[XBox   ] Xbox partition
[Return ] Return to disk selection

Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a drive to be 'Non-partitioned'.
```

Şekil 4:

```
root@kali: ~
File Edit View Search Terminal Help
TestDisk 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 987 MB / 941 MiB - CHS 1020 31 61
>[ Analyse ] Analyse current partition structure and search for lost partitions
[ Advanced ] Filesystem Utils
[ Geometry ] Change disk geometry
[ Options ] Modify options
[ MBR Code ] Write TestDisk MBR code to first sector
[ Delete ] Delete all data in the partition table
[ Quit ] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

Şekil 5:

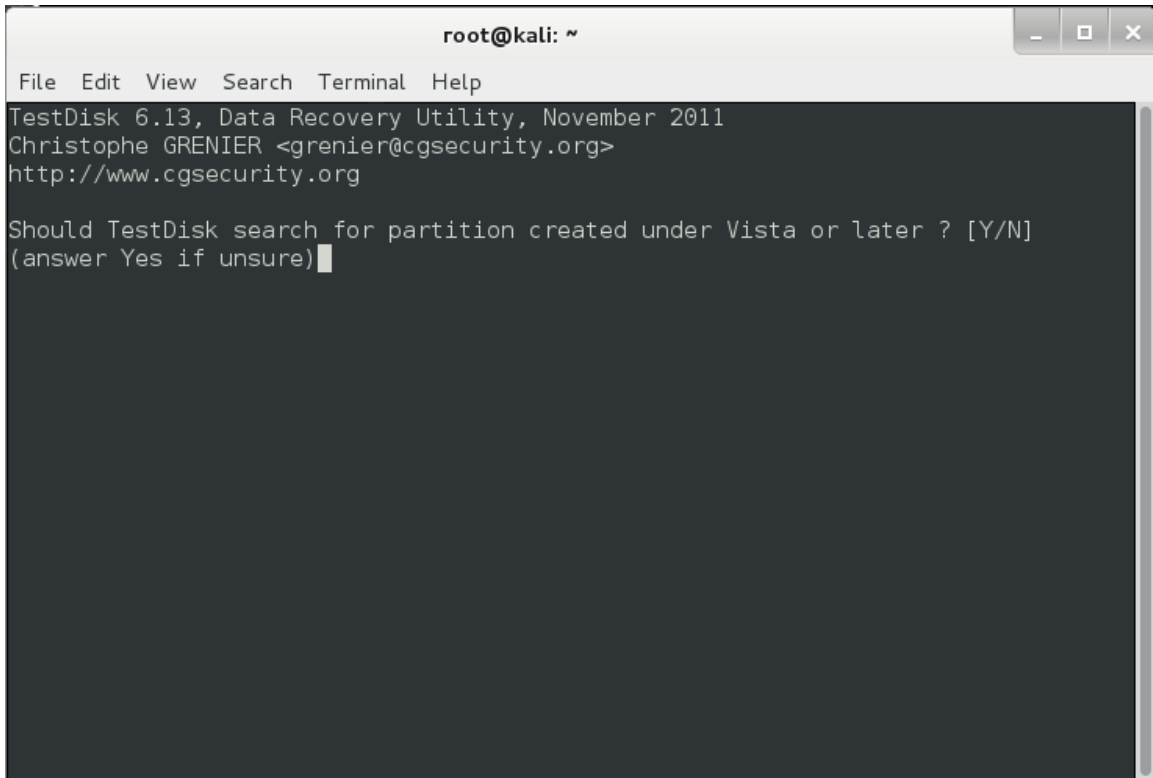
```
root@kali: ~
File Edit View Search Terminal Help
TestDisk 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdc - 987 MB / 941 MiB - CHS 1020 31 61
Current partition structure:
  Partition          Start          End      Size in sectors

No partition is bootable

*=Primary bootable P=Primary L=Logical E=Extended D=Deleted
>[Quick Search]
                        Try to locate partition
```

Şekil 6:



The image shows a terminal window titled "root@kali: ~". The window contains the following text:

```
File Edit View Search Terminal Help
TestDisk 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Should TestDisk search for partition created under Vista or later ? [Y/N]
(answer Yes if unsure) █
```

Şekil 7:



```
root@kali: ~
File Edit View Search Terminal Help
TestDisk 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdc - 988 MB / 942 MiB - CHS 1021 31 61
Analyse cylinder 101/1020: 09%

Stop
```

Şekil 8: