

(Approx. 1,226 words)

Rescuing Windows with the Trinity Rescue Kit

By Dick Maybach, Member, Brookdale Computer Users' Group, NJ

May 2015 issue, BUG Bytes

www.bcug.com

n2nd (at) att.net

I've discussed several approaches to restoring a Windows PC in previous articles. Since these are all available on the BCUG Website, I'll just include their references here. As usual the most important rescue step is preparation (*Disaster Recovery and Error Correction in Windows 7* – February, 2012). For several years my favorite recovery tool has been PartedMagic (*PartedMagic* – April 2012). I also wrote a three-article series on recovering files (*File Recovery Strategies* – June 2012, *File Recovery Using Windows Graphical Tools* – July 2012, and *File Recovery Using Command-line Tools* – August 2012). Finally, I documented an example of recovery (*Disaster Recovery: A Case Study* – June 2013).

If you want to do everything using Windows, your options are limited. If the system won't boot and you've made the preparations discussed in the 2/12 article, follow the procedures discussed there. If this doesn't work, or if you haven't prepared, you will have to remove your hard disk and install it in a working Windows PC on which you've installed recovery tools as described in the 6/12 and 7/12 articles. Indeed, this may be your only option, since Microsoft has announced that it will approve PCs for Windows 10 on which the safe boot option cannot be disabled, and this may make it impossible to boot live media on such machines.

You will have more flexibility if you can use a rescue system on a live CD-ROM or live memory stick, which will allow you to work directly on the ailing PC without removing its hard disk. First the bad news – every useful rescue system I've found runs on Linux. I don't think this will change as both Microsoft and Apple require a separate license for each computer on which you use their operating systems. There are some DOS-based systems, but I haven't found one that has enough useful tools to make it worthwhile. As a result, if you want to be able to rescue a Windows system, you will have to learn enough about Linux to at least find your way around its file system, because when you use a Linux-based rescue disk, it mounts your Windows file system as a Linux one. As a result, you won't see a C: drive for example, instead it's probably something like *sda1* (disk a, partition 1), and there may also be an *sda2* if the first disk has a second partition. If you have a second disk, it will be *sdb*, and so on. Now the worse news – many of the tools run from the command line. This means you will have to do some reading before you begin, because you probably won't see a menu of choices; instead you'll have to type the command with some arguments. Your reading will allow you to compose a command that does what you need. The prudent user will practice on an old PC with the tools that appear useful; the bold user prefers “under the gun” learning, but bold users and their files are soon separated.

As I said above, my favorite rescue tool is PartedMagic, but you may prefer an alternative. Regardless of which tool or tools you choose, spend some time exploring, preferably on an old, completely backed-up PC, especially if you're not a Linux user. You will be using powerful software, where a minor mistake can wreak real havoc. In this article we'll take a brief look at the Trinity Rescue Kit,

http://www.trinityhome.org/Home/index.php?content=TRINITY_RESCUE_KIT_CPR_FOR

[YOUR COMPUTER&front_id=12&lang=en&locale=en](#). When first started, you see the screen below, which gives you several boot options. In almost all cases, the default is what you want.



Assuming you use the default boot, you'll see the main menu below.

```
Trinity Rescue Kit easy menu
| Welcome
| TRK Help -->
| Keyboard layout selection -->
| Windows password resetting -->
| Mount all local filesystems
| Unmount all local filesystems
| Virus scanning -->
| Windows junkfile cleaning -->
| Mclone: computer replication over the network -->
| Backup and restore utilities-->
| Run a windows fileserver -->
| Run an ssh server
| Set an ip-address on the first adapter
| TRK Network boot server
| Trinity Remote Support (contact us first)
| Ethernet packet sniffing -->
| Try detecting more harddisk controllers
| Try detecting more USB and PCMCIA network adapters
| Midnight Commander
| Go to a shell
| Go to a shell and save all output to /tmp/terminal.out
| Quit this menu
| Poweroff computer
| Reboot without ejecting CD / usb stick

Welcome to Trinity Rescue Kit 3.4 build 372
This simple menu allows you to perform simple actions that don't require any Linux knowledge and
gets things done in a quick and rather dirty way.
If you need a command line you can switch to the 5 other consoles by pressing ALT+<F2 to F6> or use
'Go to a shell' below
NOTD: your TRK has successfully connected to the Internet
```



Trinity Rescue Kit 3.4

You may recall this sort of menu from your DOS days. You use the cursor keys to select an item then <Enter> to run it. Note the second item, TRK Help, which makes available a detailed manual, the first page of which appears below (assuming you select “Offline web help” when it asks what format you want). Trinity has much better documentation than most other rescue disks, and unlike most others, you don't need Internet access to see it. Although a big disadvantage is that it's not available when you are using the tools. Take good notes as you read the manual.



Trinityhome

Trinity Rescue Kit | CPR for your computer

Getting started with TRK

0. Quick and dirty guide to using TRK

0.1 The easiest way to get it onto a CD: a self burning TRK

0.2 Burning TRK with Magiciso

0.3 Booting from TRK

0.4 Resetting passwords

1. TRK for Linux newbies

1.1 What is TRK? What 's a live distribution?

1.2 What is different between accessing your PC from Windows and accessing from TRK?

1.3 Getting around with common linux commands (cd, cp, mv, rm, more, grep, mount)

1.4 Reading information about your PC (dmesg, /proc/partitions)

2. TRK own commands and utils

2.1 Virusscan

2.2 Winpass and regedit

2.3 Mass Clone: a multicast disk cloning tool

2.4 Winclean

2.5 Mountallfs

2.6 Updatetrk

OK

Another important item on the main menu is number 5, Mount all local file systems. When TRK first boots, only the device where it resides (probably a CD-ROM or a memory stick) is mounted. If, for example, you are planning to copy files from your PC to a USB hard drive, you would plug in the USB drive and then select item 5, which would make all the PC's disks as well as the external one available to TRK. The screenshot below shows the Midnight Commander file manager (main menu item 19) display after mounting the local file systems.

```

Left File Command Options Right
< /sda2/Users/n2nd > < /sdb1 >
Name Size MTime Name Size MTime
UP--DIR UP--DIR
/.. 0 May 2 2014 /.. 0 Dec 10 2011
/.config 0 Feb 15 2013 /$RECYCLE.BIN 0 Dec 10 2011
/.swt 0 Dec 15 2012 /17_MIN7 0 Dec 10 2011
/AppData 0 Dec 15 2012 /Passport 4096 Aug 12 2009
~Application Data 144 Dec 14 2012 /System Volume Information 4096 Aug 14 2012
/Contacts 0 Aug 15 2014 /Windows ImageBackup 0 Jun 25 2012
/Cookies 248 Dec 14 2012 /Windows ImageBackup.dehlia 0 Dec 10 2011
/Desktop 4096 Dec 15 16:20 /Windows ImageBackup.i7 0 Dec 10 2011
/Documents 4096 Dec 11 02:36 /Windows ImageBackup.ian 0 Dec 10 2011
/Downloads 8192 Sep 13 22:03 /Windows ImageBackup.vbox 0 Dec 10 2011
/Favorites 4096 Aug 15 2014 *700n_Win.tib 22483M Aug 14 2012
/Finance 12288 Dec 8 17:48 *MediaID.bin 528 Dec 10 2011
/Garmin Maps 0 Apr 26 2014
/Links 4096 Jan 25 02:30
~Local Settings 136 Dec 14 2012
/Music 0 Aug 15 2014
~My Documents 120 Dec 14 2012
~NetHood 288 Dec 14 2012
~/Pictures 8192 Feb 27 00:09
~/PrintHood 288 Dec 14 2012
~Recent 244 Dec 14 2012
~/Saved Games 0 Aug 15 2014
~/Searches 4096 Aug 15 2014
~SendTo 244 Dec 14 2012
~/SkyDrive 4096 Feb 27 00:10
~Start Menu 260 Dec 14 2012
~/Sync 8192 Jan 1 19:07
~/TI-Nspire 8192 Dec 15 16:25
~Templates 256 Dec 14 2012
~/Tracing 0 Nov 17 2013
~/Videos 0 Aug 15 2014
*NTUSER.DAT{01~e3ec}.TM.blf 65536 Dec 15 2012
*NTUSER.DAT{01~.regtrans-ms 524288 Dec 15 2012
*NTUSER.DAT{01~.regtrans-ms 524288 Dec 15 2012
*NTUSER.DAT{b9~6288}.TM.blf 65536 Dec 22 2012
*NTUSER.DAT{b9~.regtrans-ms 524288 Dec 22 2012
*NTUSER.DAT{b9~.regtrans-ms 524288 Dec 22 2012
*Picturenaut.pdf 780939 Sep 10 2013
*SkyDrive Message.txt 396 Nov 14 2012
*Sti_Trace.log 2537 Dec 2 22:17
*ntuser.dat 3145728 Mar 4 02:19
/Downloads
/..

```

Hint: Tab changes your current panel.
trk n2nd #
1 Help 2 Menu 3 View 4 Edit 5 Copy 6 RenMov 7 Mkdir 8 Delete 9 PullDn 10 Quit

The left side displays my Windows home directory, which in Linux's view resides on partition 2 of drive sda or sda2 instead of C: as Windows would label it. The right side shows partition 1 of sdb, which is a USB hard disk. Midnight Commander is the program you would use to copy your files from a failing Windows disk to an external one.

A unique feature of TRK appears as main menu item 7, Virus scanning, where you can choose from five different scanners. When you select this, you see the top portion of the next screen. The portion below shows the result of activating "Scan with f-prot," which results in TRK downloading the latest version of that virus scanner and starting it.

```
Trinity Rescue Kit easy menu
| <-- Go back to main menu
| Set the scan destination (if not set: all local drives)
| Scan with Clam AV
| Scan with F-Prot
| Scan with BitDefender
| Scan with Vexira
| Scan with Avast (license key needed first)
| Help on virusscan


(command: virusscan -a fprot)

Downloading F-prot from http://files.f-prot.com/files/unix-trial/fp-Linux.x86.32-ws.tar.gz
--2015-03-02 20:24:33-- http://files.f-prot.com/files/unix-trial/fp-Linux.x86.32-ws.tar.gz
Resolving files.f-prot.com... 66.232.150.62, 84.40.30.92
Connecting to files.f-prot.com|66.232.150.62|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 30914110 (29M) [application/x-gzip]
Saving to: 'fp-Linux.x86.32-ws.tar.gz'

100%[=====>] 30,914,110 1.17M/s in 26s

2015-03-02 20:24:59 (1.15 MB/s) - 'fp-Linux.x86.32-ws.tar.gz' saved [30914110/30914110]

Started scanning with F-Prot
Scanning: /
```



F-prot not only detects viruses, but also removes them. Most Linux systems have only the Clam virus scanner, which only detects and quarantines infected files. If one of the Windows system files is infected, the result will be a virus-free, but broken system.

Another item you might find useful is number 4, Windows password resetting, most likely for a new user who has forgotten his or hers.

Finally, you can go to a shell and use one of the many command-line utilities for more difficult problems. Among the procedures covered in the documentation are

- rescuing files from a dying hard disk,
- recovering deleted files,
- recovering lost partitions,
- bootsector repair,
- cloning a Windows installation,
- hardware testing, and
- PC cleaning.

While the solutions to some common problems appear in the main menu, the Trinity Rescue Kit is capable of a lot more. Even though you must often work in a command-line environment, there is enough good help to make this possible, if perhaps a little uncomfortable, for most inhabitants of the graphic user interface world. It's well worth

spending some time with it, just in case disaster strikes. The man command can be a great help here; for example the screen shot below shows the result of typing “man testdisk” on a command line.

```
TESTDISK(1) Administration Tools TESTDISK(1)
NAME
  testdisk - Scan and repair disk partitions
SYNOPSIS
  testdisk [/log] [/debug] [/dump] [device|image.dd|image.e01]
  testdisk /version
  testdisk /list [/log]
DESCRIPTION
  TestDisk checks and recovers lost partitions
  It works with :
  - BeFS (BeOS)
  - BSD disklabel (FreeBSD/OpenBSD/NetBSD)
  - CramFS, Compressed File System
  - DOS/Windows FAT12, FAT16 and FAT32
  - HFS and HFS+, Hierarchical File System
  - JFS, IBM's Journaled File System
  - Linux Ext2 and Ext3
  - Linux Raid
  - RAID 1: mirroring
  - RAID 4: striped array with parity device
  - RAID 5: striped array with distributed parity information
  - RAID 6: striped array with distributed dual redundancy information
  - Linux Swap (versions 1 and 2)
  - LVM and LVM2, Linux Logical Volume Manager
  - Mac partition map
  - Novell Storage Services NSS
  - NTFS (Windows NT/2K/XP/2003/Vista)
  - ReiserFS 3.5, 3.6 and 4
  - Sun Solaris i386 disklabel
  - Unix File System UFS and UFS2 (Sun/BSD/...)
  - XFS, SGI's Journaled File System
OPTIONS
  /log create a testdisk.log file
  /debug add debug information
  /dump dump raw sectors
  /list display current partitions
SEE ALSO
  fdisk(1), photorec(1).
lines 1-51
```

The Trinity Rescue Kit can turn a disaster into an inconvenience, but only if you know how to use it, and this requires that you actually play with it first. If you're reading this, your friends and family probably look to you to solve their PC problems. Becoming familiar with some good repair tools and techniques could be a wise investment.