Rescuing data on Linux and Windows machines

Rescue Center

Trinity Rescue Kit is driven by the practical requirements of the admin's daily work, integrating a full set of tools for maintaining and rescuing Linux and Windows PCs. *By Erik Bärwaldt*

When troubleshooting problems and reconstructing lost or damaged data on mixed Linux and Windows networks, you can be saddled with a number of programs – the result of working on two different operating systems, as well as the accumulation of applications over the years. Rapid innovation cycles for hardware aggravate the situation and make it even more difficult to keep track of your tools.

To make maintaining networks a more tranquil experience, introduce yourself to the Live Trinity Rescue Kit (TRK) distribution. Not only does it collaborate perfectly with Linux, it also helps you solve problems on other operating systems.

TRK is available as an ISO image, weighing in at around 135MB [1] for a Live CD. Alternatively, you can use a USB stick as a Live medium. However, be aware that although many older personal computers have USB ports, you often will not be able to boot from them. In this light, the Live CD gives you a more universal approach.

The Trinity Rescue Kit, primarily based on the Mandriva distribution, doesn't detract from its primary function by confusing the user with gimmicks. Instead, it comes up with what initially looks like a fairly anachronistic text-based screen. Under the hood, the new version of TRK, version 3.4, relies on the 2.6.35 kernel, which harmonizes perfectly with more recent hardware. The website for the distribution also provides comprehensive documentation of all the features [2].

Framework

Booting the Trinity Rescue Kit is a new experience. GRUB lists no fewer than 22 start options with custom configurations for a variety of application scenarios.

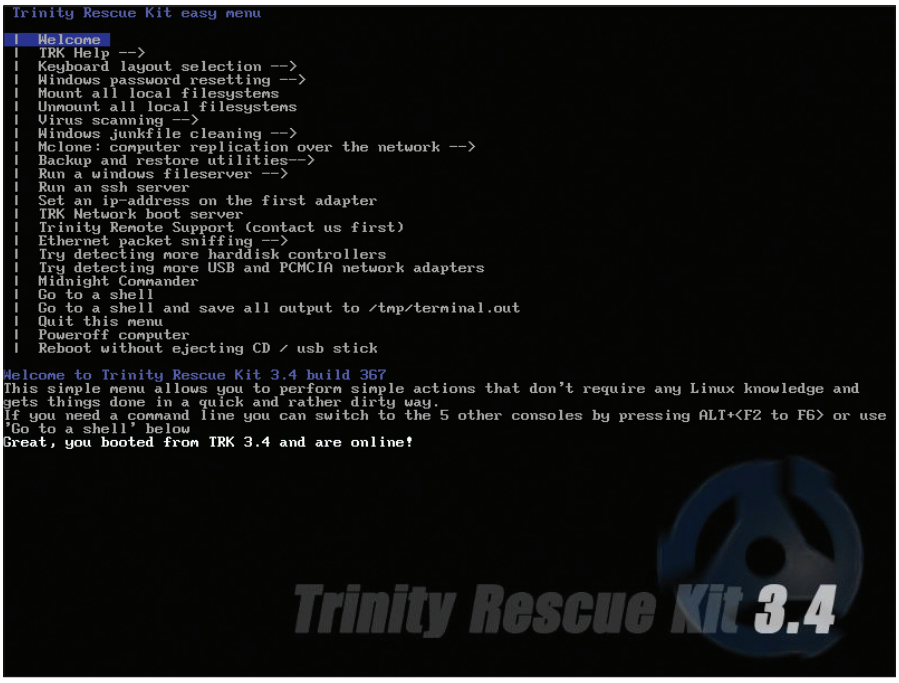

Figure 1: Technically impressive, but less so visually: The main Trinity Rescue Kit menu.

Some of these boot options are designed to help you run the system on computers with – shall we say – unusual, hardware. For example, you might have a computer with a SCSI host adapter and matching drives. If you experience compatibility issues when booting, you can just select the *Try more SCSI drivers (when disks not detected)* boot option to try to solve the problem. And, the system doesn't leave you in the lurch if you inadvertently use some kind of exotic network interface card or USB WLAN stick.

For legacy computers with slow, optical drives, you also have the option of running a complete system in RAM. If you have a less mature operating system than Linux, you might prefer to start your troubleshooting activities with a virus scan – another of TRK's tricks. If you select the default mode, TRK boots very quickly to a plain text-based screen that simply takes you to a feature-rich option menu (Figure 1).

If you check out the menu items, you will immediately notice that TRK is a perfect choice for dealing with the daily issues and tribulations that Windows users face. If Windows has once again collected too much ballast and is thus slowing down the whole system, you can get rid of the data garbage by selecting the *Windows junkfile cleaning* option. If a user has locked himself out, you can select the *Windows password resetting* feature.

Getting Rid of Vermin

If you suspect that viruses, Trojans, or worms have infiltrated the computer, it is a good idea to select *Virus scanning* to investigate the issue more closely. Doing so tells the Trinity Rescue Kit to check the medium in question with five different virus scanners.

To make sure the search for malware on the system is as reliable as possible, TRK starts by accessing the network to download the latest updates and virus patterns for each of the virus scanners it uses. In other words, a fast Internet connection is one prerequisite for using TRK. The only trouble with this procedure, which is actually quite clever, is that using the Avast virus scanner means having a valid license key (which you can pick up free of charge after registration) (Figure 2).

Even if you suspect that one of your Linux clients has been compromised by a rootkit, TRK will still help you. It includes two scanners for the free operating system, rkhunter and chkrootkit, which reliably put an end to these pests.

Trinity Rescue Kit doesn't give you a separate menu item for this fairly rare threat, but it does let you scan a disk and a console. Because the distribution gives you five additional consoles in addition to the menu screen – you can access them by pressing the keyboard shortcuts Alt + F2 through Alt + F6 – you can execute multiple commands at the same time.

To launch the rootkit scanner, you can just type `chkrootkit` or `rkhunter -c -sk` at the command line. Tools will check any drives that you have mounted for malware without the need for user interaction.

Backups and File Managers

On an intranet, the rescue system offers additional options for backup and restore tasks. The program Pi lets you create

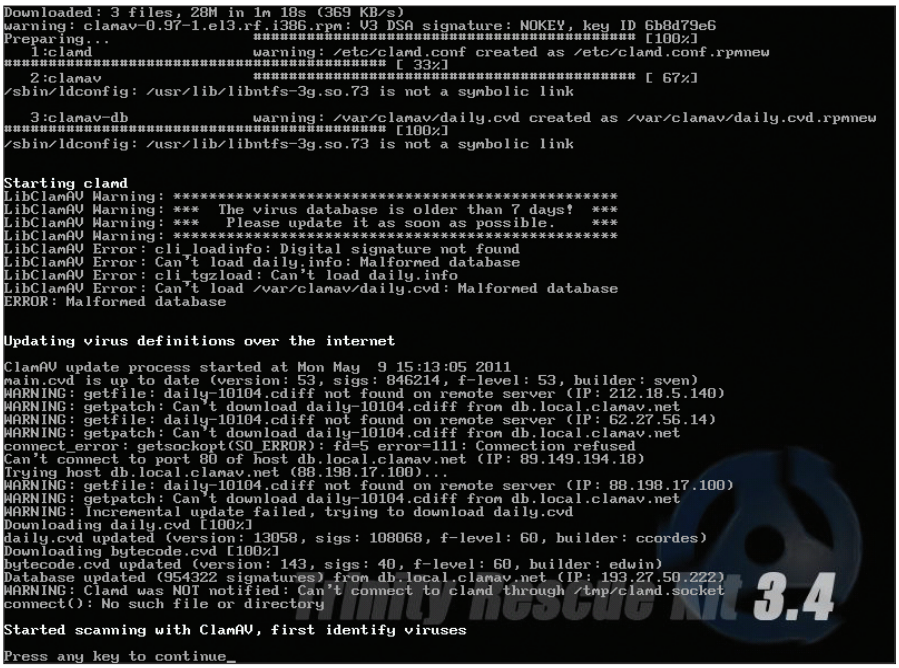

Figure 2: TRK removes malware from other operating systems.

full disk images automatically or images of individual partitions. This tool also shows you all the partitioning information at the press of a button, giving you at-a-glance information on whether the mass medium you are scanning has a consistent partition table.

Trinity Rescue Kit also lets you launch *Midnight Commander*, the tried and trusted file manager, at boot time as a convenient option for copying or backing up individual files or directories. If you run `mountallfs`, Midnight Commander easily handles file operations (Figure 3).

Multilingual Clones

TRK also supports unassisted computer installations across the network, thanks to the `mclone` program. To use this option, you need a computer on the network that serves up the required disk images. Then, launch TRK from a USB stick or CD-ROM on the computer to distribute the image to other systems that were booted with the TRK system.

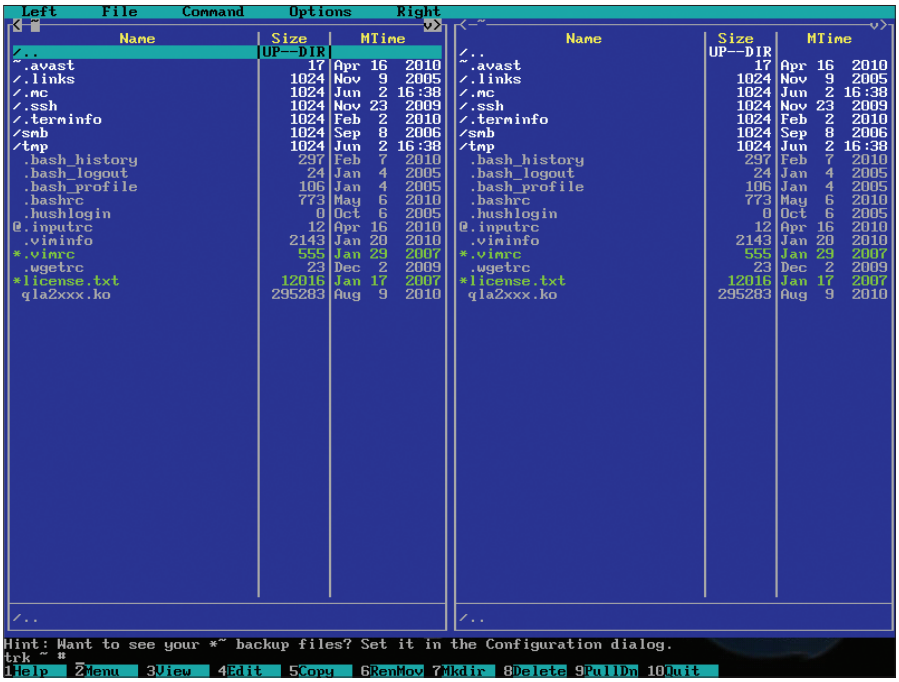

Figure 3: The versatile Midnight Commander is included with TRK.

Because TRK works independently of platform-specific restrictions, it doesn't matter which operating system you are copying. Your cloning speed will depend on your network bandwidth. On a typical Fast Ethernet LAN with a maximum bandwidth of 100Mbps, you can create a Linux clone that weighs in at around 4GB on a newish computer with a Core 2 Duo CPU within less than 10 minutes.

File Server

If you need to share the drives on a computer temporarily on a heterogeneous network – say, to serve up some files or directories to another workstation – you can select the *Run a windows fileserver* or *Run an ssh server* option. After typing a new password, you can start transferring files.

If you use an SSH server, the transfer will use a secure connection. Additionally, this method lets you access Linux clients, so you have virtually no limits to the operations.

Conclusions

Trinity Rescue Kit turns out to be a bona fide Swiss Army knife for anybody who needs to manage a mixed Linux/Windows environment. The distro understands the practical needs of the admin and integrates a full set of tools for maintaining and rescuing Linux and Windows PCs.

Also, it offers a backup function that helps you rescue important files and directories. Because it integrates the cloning routine for producing and distributing a hard disk image, you can provision a complete network in a very short time, assuming identical hardware.

Trinity Rescue Kit demonstrates that free software has a technological advantage, even on heterogeneous networks, and that you can troubleshoot quickly and reliably without investing in expensive proprietary software. ■■■

INFO

[1] Download: *http://trinityhome.org/Home/index.php?content=TRINITY_RESCUE_KIT_DOWNLOAD&front_id=12&lang=en&locale=en*

[2] Documentation: *http://trinityhome.org/Home/index.php?content=GETTING_STARTED_WITH_TRK&front_id=12&lang=en&locale=en*