

## Re: Rooted system

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-02/0102.html>

---

**From:** Brian Keefer (*chort\_at\_amaunetsgothique.com*)

**Date:** 02/19/04

To: [freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org)

Date: 18 Feb 2004 23:34:10 -0800

On Mon, 2004-02-16 at 12:20, Clifton Royston wrote:

> > *And now what? [ You are unclear to me ]*

> >

> > *Well, you could use a Security Toolkit Distribution from Knoppix, called*

> > *knoppix-std*

> > *And do some research with that.*

>

> *More generic forensic help (less Linux-specific) might come from the*

> *"Coroner's Toolkit" from the team of Wietse Venema and Dan Farmer*

> *(SATAN et al., and also TCPwrap and Postfix in the case of Wietse.)*

> *It's supposed to be pretty cross-platform with BSD support.*

>

> <<http://www.porcupine.org/forensics/tct.html>>

>

FYI the Knoppix-STD live-CD does have an extended version of Coroner's Toolkit. Have a look:

<http://www.knoppix-std.org/tools.html>

Also, although it's a Linux distribution, it's *\*not\** expressly for Linux forensics. It has NTFS rw support (limited) and Windows password reset functions, etc... In other words, it's a multi-OS generic forensics kit. I'm fairly certain that it does have support for mount -t ufs, but I haven't confirmed that.

--

Brian Keefer, CISSP

Systems Engineer

CipherTrust Inc, [www.CipherTrust.com](http://www.CipherTrust.com)

---

[freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org) mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "[freebsd-security-unsubscribe@freebsd.org](mailto:freebsd-security-unsubscribe@freebsd.org)"