

RE: [Full-disclosure] Forensic help?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-09/0314.html>

From: James Wicks (jjjwicks_at_gmail.com)

Date: 09/12/05

Date: Sun, 11 Sep 2005 18:49:48 -0400

To: full-disclosure@lists.grok.org.uk

Here is a way to do it on the cheap:

1. Ghost the hard drive with "Symantec Ghost" –
http://www.symantec.com/sabu/ghost/ghost_personal/
2. Take the original drive with you and put a new drive in the machine
3. Copy the Ghost image on the new drive, allowing the system to go back into production
4. Take the suspect drive and install it in another system with the same configuration as the original. Run "RecoverMyFiles"
<http://www.whitecanyon.com/rmf-hard-drive-data-recovery.php> or "File Recover 5.0"
http://www.pctools.com/file-recover/?ref=google_fr

The whole thing should cost you about \$140 in software cost and the cost of a replacement hard drive.

JJJ

-----Original Message-----

From: full-disclosure-bounces@lists.grok.org.uk [mailto:full-disclosure-bounces@lists.grok.org.uk] On Behalf Of Red Leg
Sent: Sunday, September 11, 2005 6:34 PM
To: full-disclosure@lists.grok.org.uk
Subject: [Full-disclosure] Forensic help?

Hi all.

I was wondering if anyone knows of a program/system that I can purchase, as a private individual, that will allow me to

- 1) mirror a hard drive on location and
- 2) take that mirror and restore it to another drive. And

RE: [Full-disclosure] Forensic help?

Full-Disclosure: RE: [Full-disclosure] Forensic help?

3) Find any CONVENTIONALLY erased files?

-- This would be either a Windows NTFS or FAT32 drive.

Anyone have first hand experience? Please let me know, if you do. In ANY case, please suggest whatever you might have learned even without first hand experience.

Thanks!

Redleg18

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>