



# TrueBack

**TrueBack** is a cyber forensic software tool for digital evidence seizure and acquisition developed by Resource Centre for Cyber Forensics, Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram.

TrueBack is available on DOS, Windows and Linux and distributed on a Boot Floppy/CD.

The investigating officer will boot the suspect's system from the boot Floppy/CD supplied to him.

TrueBack allows investigators to preview the storage media before seizure. It enables investigators to electronically seize or acquire the digital evidence and create the report of the seizure with all details.

## TrueBack

### Digital Evidence Seizure and Acquisition Tool

- TB** Developed for Indian Law Enforcement Agencies
- TB** Available on DOS, LINUX and Windows
- TB** National Institute of Standards and Technology (NIST), USA, disk imaging tool specification compliant
- TB** Uses MD5 Hash for authentication
- TB** Preview of suspect media in Windows and Linux Versions
- TB** Creation of block hashes to prevent loss of evidence
- TB** Supports IDE, SCSI, SATA, CD, DVD, Floppy, USB and Firewire devices.
- TB** Disk Imaging facility with compression for any media
- TB** Facility for Seizure, Acquisition Or Seizure & Acquisition
- TB** Local, Parallel Port or Network Acquisition
- TB** Acquisition of partition or whole media to Hard disk, USB or Firewire devices
- TB** Detailed Report generation to floppy, USB or CD