# F.B.I. Forensic Field Kit

By *srlinuxx*
Created *10/10/2009 - 1:42pm*
Submitted by srlinuxx on Saturday 10th of October 2009 01:42:17 PM Filed under Gentoo [1] Software [2]

This is the ultimate bootable Disk for power user, or wannabe agent. Basically, the FBI Forensic Field Kit is a AIO Toolkit with compiled applications and ebooks designed to investigate and coordinate the user to look for buried files, and information logged inside your computers hard drive.

Forensics Tools:

Sleuth Kit -Forensics Kit
Py-Flag - Forensics Browser
Autopsy - Forensics Browser for Sleuth Kit
dcfldd - DD Imaging Tool command line tool and also works with AIR
foremost - Data Carver command line tool
Air - Forensics Imaging GUI
md5deep - MD5 Hashing Program
netcat - Command Line
cryptcat - Command Line
NTFS-Tools
qtparted - GUI Partitioning Tool
regviewer - Windows Registry Viewer

Field Kit Manuals:

Incident response - Computer Forensics
Computer Crime investigation
Forensic Pathology

Additional programs on Boot DVD:

Gentoo Linux 2.6 Kernel - Opyimized for Forensics Use
XFCE - GUI
Apache2 - Server

Mysql PHP4
Open Office
Gimp - Graphics Program
KSnapshot - Screen Capture Program
Mozilla
Internet Forensics

More here [3]

(Not associated with the Federal Bureau of Investigation.)

---

Gentoo Software

---

**Source URL:** http://www.tuxmachines.org/node/40223

**Links:**
[1] http://www.tuxmachines.org/taxonomy/term/109
[2] http://www.tuxmachines.org/taxonomy/term/38
[3] http://www.ddlhere.com/pc-applications/18829-f-b-i-forensic-field-kit.html