A Brief, Completely Inadequate Forensic Tools Overview

CS 585-002
Cybercrime and Digital Investigations
Fall 2009
Major Digital Forensic Tool Providers

- **AccessData Corporation**
  - Makers of FTK (Forensic Tool Kit®)

- **Guidance Software**
  - Makers of EnCase®

- **X-Ways Software Technology AG**
  - Makers of X-Ways Forensics®
AccessData® Products

- Forensic Tool Kit (FTK) 3.0 – Integrated Forensic tool
  - Acquisition, analysis, decryption, password-cracking, case management
  - “Built for speed”
  - “Explicit image detection” – identifies images likely to be pornography
  - Distributed processing: use up to 3 add’l computers for parallel analysis (cloud, anyone?)
    • “True multi-processor and multi-threading support”
AccessData® Products

• AccessData® Enterprise
  – Designed for investigations on a corporate network
  – Incident response console, live analysis of Windows systems running on the network

• AccessData® eDiscovery
  – “the only true custodian-based, end-to-end eDiscovery solution on the market today”
  – “Maps to EDRM”
    • Electronic Discovery Reference Model
    • Interesting: they make Enron email files available
  – Extensive logging and reporting of all discovery activity for chain of custody and auditing purposes
Guidance Software

• EnCase® Forensic
  – “Recognized worldwide as the de facto standard for computer forensics”
  – Acquisition, Case management, analysis, search
  – Customizable filters via EnScript® language
  – Decryption suite (add-on)
  – “Uses the EnCase evidence file format (LEF or E01), a digital evidence container validated and approved by courts worldwide.”
  – Requires a USB fob to be inserted for analysis
    • Acquisition does not require fob ➞ acquire on many machines, but analyze on only one
Guidance Software

• **EnCase® Portable**
  – “A Data Collection Solution that Anyone Can Use”
  – “Search and collect forensically sound data with a pocket-sized toolkit that can be used by anyone, anywhere, anytime.” (!)

• **EnCase® Enterprise**
  – Provides “investigative infrastructure”
  – “Investigate any incident across the network”
    • “…HR matters, allegations of fraud, suspicious network activity, and more with a forensically sound solution operated from a central location with no disruption to business”
X-Ways Software

• X-Ways Forensics 15.4
  – “An advanced work environment for computer forensic examiners.”
  – Acquisition, analysis, case management, deleted file recovery, search, ...
  – Based on WinHex (!)
  – Skin-color detection
    • “A gallery view sorted by skin color percentage greatly accelerates a search for traces of child pornography”

• X-Ways Investigator
  – Subset of Forensics for investigators
NIST’s Computer Forensics Tool Testing Project (CFTT)

• Idea: provide law enforcement (LE) with independent testing of forensic tools --- do they do what they say they do?

• Developed jointly with LE
NIST’s Computer Forensics Tool Testing Project (CFTT)

Methodology:

1. Decide on categories, and tools to test
2. Work with LE to develop a Tool Specification
   = Requirements, assertions and test cases
   Covers options supported by tools in category
   Example: “If the tool creates a multi-file image of a requested size, then all the individual files shall be of the requested size, except that one file may be smaller.”
3. Acquire a tool, RTFM, develop testing strategy
4. Select relevant test cases for the options supported by the tool
NIST’s Computer Forensics Tool Testing Project (CFTT)

Methodology:

5. Execute tests.
6. Produce test report.
7. Steering Committee reviews test report.
8. Vendor reviews test report.
9. Post support software to web
10. Post report to the web
Tool Categories

- Imaging/Acquisition
- Forensic Media Preparation
- Write block (software)
- Write block (hardware)
- Deleted File recovery
- Mobile devices (smart phones)
- String Searching
Disk Imaging Tool Reports

- **BlackBag MacQuisition 2.2** (September 2009)
- **EnCase 6.5** (September 2009)
- **EnCase LinEn 6.01** (October 2008)
- **EnCase 5.05f** (June 2008)
- **FTK Imager 2.5.3.14** (June 2008)
- **DCCldd (Version 2.0, June 1 2007)** (January 2008)
- **EnCase 4.22a** (January 2008)
- **Encase Linen 5.05f** (January 2008)
- **IXimager (Version 2.0, Feb-01 2006)** (April 2007)
- **dd FreeBSD** (January 2004)
- **Encase 3.20** (June 2003)
- **Safeback 2.18** (June 2003)
- **dd GNU fileutils 4.0.36, Provided with Red Hat Linux 7.1** (August 2002)
Software Write Blocker Tool Reports

• Writeblocker Windows XP V6.10 (Jan 2008)
• PDBlock (June 2005)
• RCMP HDL (Feb 2004)