Open Source in Computer Forensics

Special Agent Jesse Kornblum
Air Force Office of Special Investigations

U.S. AIR FORCE

U.S. AIR FORCE

Overview

- Introduction
- The Complete Guide to Computer Forensics [abridged]
- dcfldd
- Foremost
- md5deep
- Humbert
- Questions

U.S. AIR FORCE

Introduction

- What is AFOSI?
- Who is this guy?
- Why is this guy here?

U.S. AIR FORCE

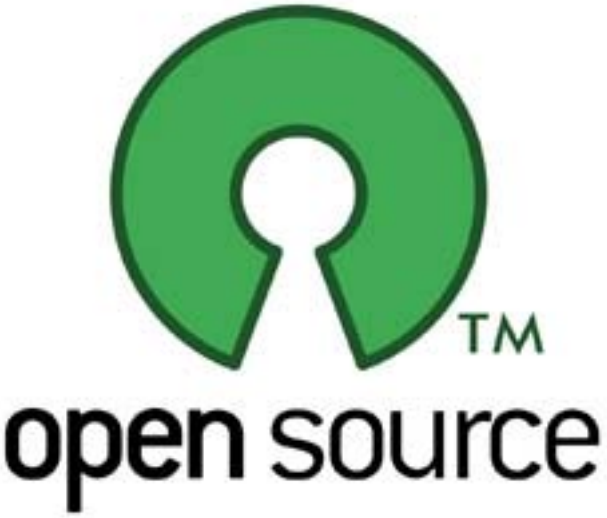
What is Computer Forensics

- Figure out what the heck happened
- Think of CSI, except with computers
- Must be able to show <u>proof</u>
  - Fact finders vs. expert testimony
- All tools and techniques must meet the Daubert standard
  - Tested
  - Reviewed by peers
  - Known error rates
  - Qualifications
  - Explainable

U.S. AIR FORCE

How Open Source Helps

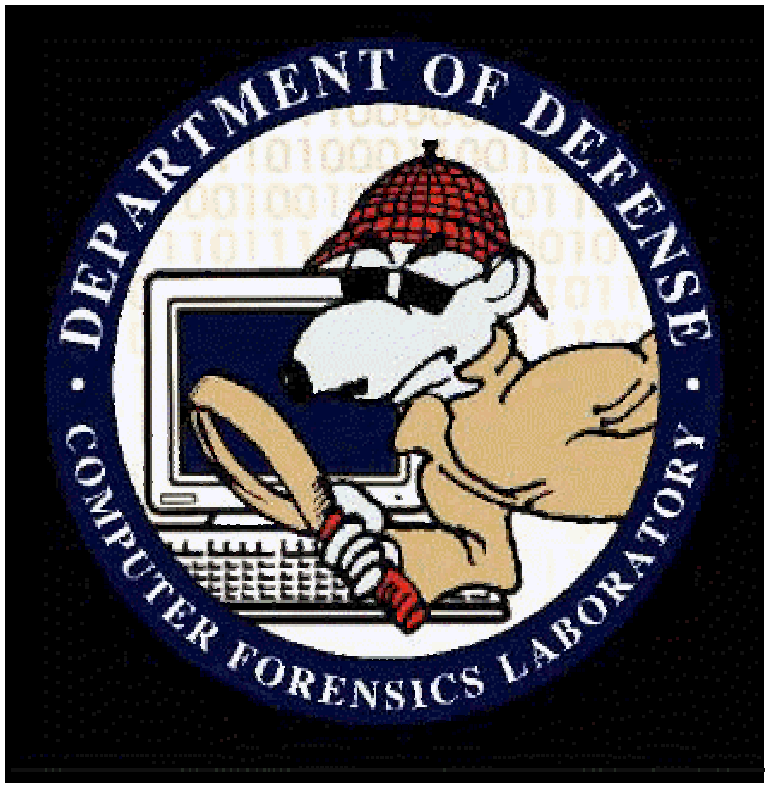
- Removes ambiguity of analysis
  - Clearly defines the methodology
  - Helps with testing and peer review
- Details how analysis was conducted
  - Not necessarily what happened
- Gives same toolset to both sides
- Saves money!
  - Tools can be written or modified by anybody
  - Gov't agent, defense attorney, contractors, etc



U.S. AIR FORCE

Success Stories - dcfldd

- DCFLdd
- Defense Computer Forensics Lab
- Modified GNU dd (CoreUtils)
- Added time estimation
- Added MD5 hashing
  - RFC 1321
  - Computes chunks as it goes
  - Computes for entire drive



- http://prdownloads.sf.net/biatchux/dcfldd-1.0.tar.gz

U.S. AIR FORCE

Success Stories - Foremost

- Linux program to recovers files based on headers and footers
  - Kind of like a complex grep operation
- Works on dd image files, live devices
- Headers and footers given in a configuration file
- Upshot: Given a person's hard drive, you can find all of the GIF, JPEG, Office and PST files in one step.
  - Even if they've been "deleted"
- Licensed as public domain
  - 17 USC 105 – "Copyright protection … is not available for any work of the United States Government."
- http://foremost.sf.net/

U.S. AIR FORCE

Success Stories - md5deep

- Like md5sum from GNU Coreutils, but more!
- Can work recursively
- Cross platform MD5 program
  - Windows, Linux, *BSD, Solaris, OS X
- Hashes can be in a variety of formats
  - Plain, NIST NSRL, iLook, Hashkeeper
- Can do positive and negative matching
- Estimates time remaining
- Again, public domain

- http://md5deep.sf.net/

U.S. AIR FORCE

md5deep

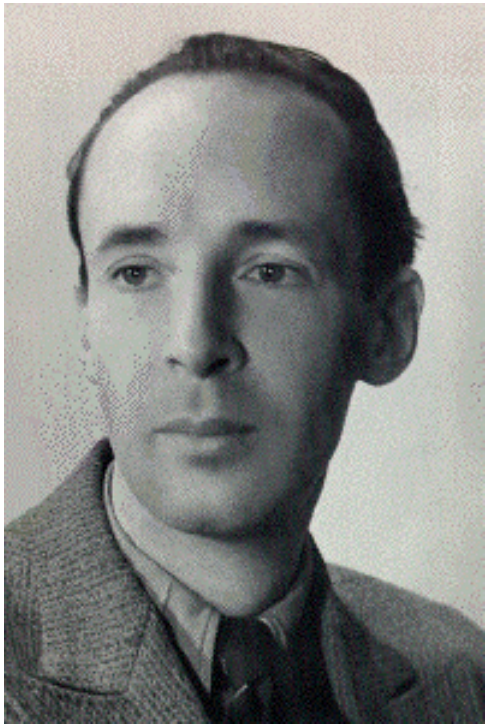
```
C:\> md5deep -r c:

a0ba48fec299daaa06eb713e2cf2f191 c:\arcldr.exe
09fd1a7152212579ca25b44d4b7a9993 c:\arcsetup.exe
d41d8cd98f00b204e9800998ecf8427e c:\AUTOEXEC.BAT
bec50a347a5fb2ff498be5022637180f c:\boot.ini
90d0f023a1913e0f4ef2b2d77ac731fb c:\Cabs\7508736\AREAEXT.DAT
9947ff7d1a9873b2ab491bbed617dae7 c:\Cabs\7508736\BEEP.COM
a8f7445c54064a38db1bb51d3c73c12a c:\Cabs\7508736\BIOS.REC
3efea3144abee232fda1719d2c1a4066 c:\Cabs\7508736\COMMAND.COM
```

U.S. AIR FORCE

Humbert

- Automated child abuse imagery detection tool
  - Humbert is the protagonist from Nabakov's *Lolita*
- Based on MD5 message digest comparison
- Used during command directed inspections
- Hashes of child porn coming from past AFOSI cases, other law enforcement agencies and government organizations
  - Identified imagery



U.S. AIR FORCE

Humbert Instructions

- Insert CDROM/floppy into computer
- (Can auto-run from CDROM on insecure Windows computers)
- If computer is off, turn it on
- If computer is on `d:humbert`
- Humbert turns screen green while processing
- If child porn is found…

THIS COMPUTER CONTAINS CHILD PORNOGRAPHY

c:\My Documents\Pics\k-12\000hot!!!.jpg

c:\My Documents\Pics\k-12\017ashley.jpg

c:\My Documents\Pics\k-12\2hot4u.jpg

SAVE

PRINT

Questions?

Ask me anything!

SA Jesse Kornblum - jesse.kornblum@ogn.af.mil - 240.857.1143