Simple but Sound Tools for First Responders

Special Agent Jesse Kornblum
Air Force Office of Special Investigations

Overview

- Introduction
- The First Responder Dilemma
- What Law Enforcement Needs
- What Makes a Good Tool
- FRED
- ICE^3
- Humbert
- Questions

U.S. AIR FORCE

Introduction

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

U.S. AIR FORCE

The First Responder Dilemma

- System administrators are trying to keep the system running
  - May not care about who did what
  - Just want to keep things running
  - Resembles a herd of buffalo to a forensic analyst

- Not an issue with most other types of crime
  - The Dead Body Theorem

U.S. AIR FORCE

What Law Enforcement Needs

- We need <u>proof</u>!
- We must establish facts beyond all reasonable doubt
- We usually do not testify as experts
  - Our “opinions” don’t count
- There are only five questions we ask
  - Who
  - What
  - Where
  - When
  - How

U.S. AIR FORCE

What Makes a Good Tool

- Benefits the first responder
  - They have to want to run it
- Benefits law enforcement
  - Provides meaningful data
  - Results can be used to further investigation, in court
- Keeps all evidence handling away from user
  - Not all control, just evidence handling
- Snappy name

U.S. AIR FORCE

FRED - Background

- Air Force Computer Emergency Response Team (AFCERT)
  - Responsible for monitoring all Air Force computers
  - Manage system administrators
  - Investigate suspicious events
- When an event happens:
  - AFCERT, SysAdmin talk
  - Figure out what happened
  - If necessary, call AFOSI

U.S. AIR FORCE

FRED – The Problem

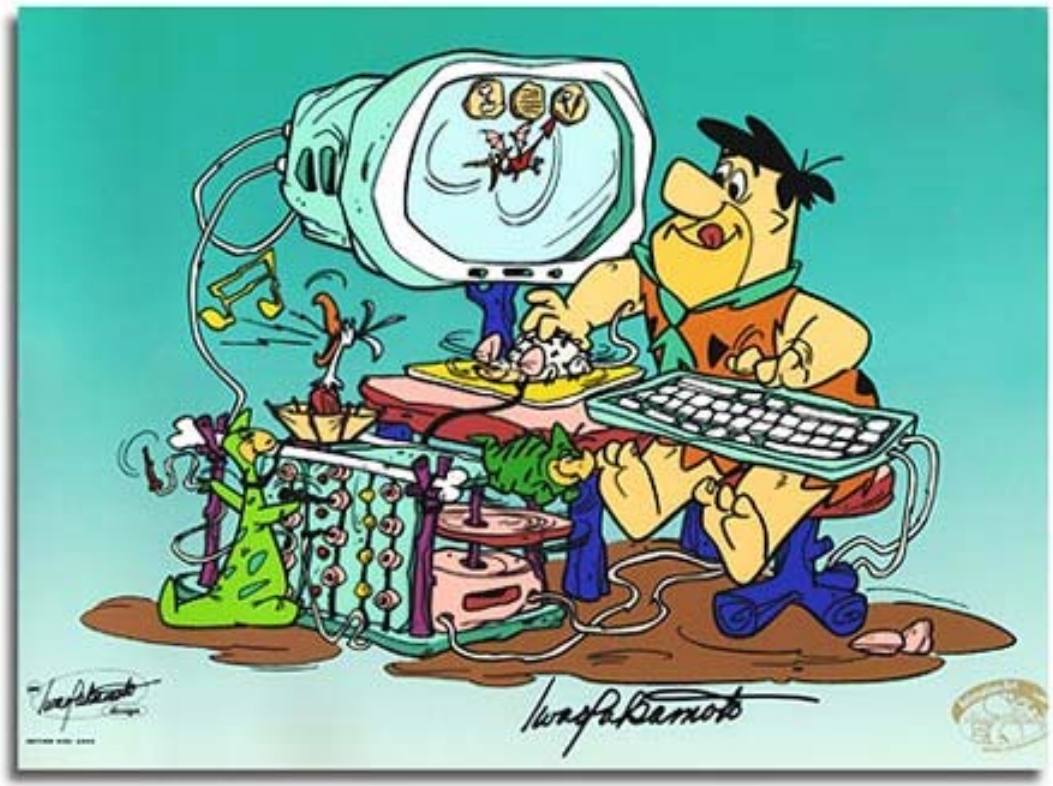
- Evidence lost during initial response
  - Files accessed, Programs executed (bad)
  - Victim rebooted, Files/Accounts deleted (very bad)
  - Victim wiped, rebuilt, or “reutilized” (go home)

- We need a tool to:
  - Gather data useful to first responder
  - Preserve that data for law enforcement
  - Begin a chain of custody for that data

U.S. AIR FORCE

FRED – The Solution

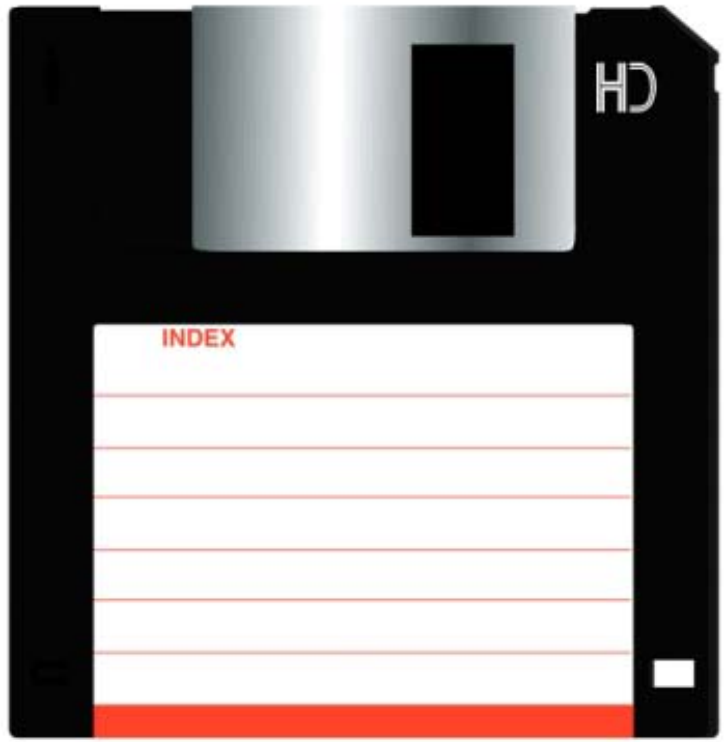
- The First Responder's Evidence Disk
- Single floppy disk with COTS tools for system analysis
- Records results back to same floppy
- Quick analysis to figure out what happened
- Determine if full analysis or investigation is warranted



U.S. AIR FORCE

FRED – Design Choices

- KISS principle in all things
- Fit on a floppy disk
  - Most Air Force computers have a floppy disk drive
  - Easy to transport
  - Easy to store securely
- Use COTS tools
  - Saves time, effort, money
- Write results back to floppy



U.S. AIR FORCE

FRED – Design Constraints

- Don't Trust the Victim System
  - Where possible, avoid using any system resources
  - Unavoidable for many low-level resources
  - Can't bring our own copy of kernel.dll
  - But can bring copies of all executables
- Don't Alter Anything on the Victim System
  - Unavoidable for some things
  - But record all data that is about to be destroyed first
- Full discussion in DFRWS paper
  - http://www.csa.syr.edu/Jesse_Kornblum.pdf

U.S. AIR FORCE

FRED – The Design

- Record the follow kinds of things
  - Date and time of exam start
  - OS name, version, patch level
  - Mounted filesystems
  - Who's logged on
  - Running processes
  - Network connections
  - Shared filesystems
  - ARP cache
  - Port to Process bindings
  - Hash of *:\WINNT*
  - Date and time of exam end

FRED – Behind the curtain

It's a batch file:

```
@echo FRED v1.1 is running...
@echo FRED v1.1 - 2 April 2002 > audit.txt
@echo. >> audit.txt
@echo START TIME >> audit.txt
@time /t >> audit.txt
@date /t >> audit.txt
@echo. >> audit.txt
```

U.S. AIR FORCE

FRED – Initial Response

- FRED v1.1 released on April 2nd 2002
- Good? It's grrrrrrreat!
- Version 1.2 coming soon
- New version will be released to the general public!

U.S. AIR FORCE

FRED – What's Next

- fred2html – Script to parse output file

Protocol	Port	Service	PID	Name
TCP	80	HTTP	104	httpd
TCP	5190	AOL	7219	aim.exe
TCP	1026		7091	iexplore
TCP	26531		2817	iexplore
UDP	31337	BackOrfice	2819	explorer

ICE3

- Investigator Controlled Evidence Extraction Engine
  - Pronounced “ice cube”
- Allows a non-computer person to image a computer
  - Bit for bit forensic copy

U.S. AIR FORCE

ICE3

- Linux boot CDROM
- DCFLdd http://prdownloads.sourceforge.net/biatchux/dcfldd-1.0.tar.gz
- USB hard drive(s)
- Custom program to glue it all together
  - About 2,000 lines of C
  - About two months to develop

U.S. AIR FORCE

ICE3 - Instructions

- Insert ICE3 CDROM into the computer
- Connect one or more USB hard drives
- Turn on computer
- Prompt: “Do you want to image this computer?”
  - Hit “y” for yes, “n” for no
  - Wait until done (~ 2 mins/GB)
- Turn off computer
- Remove CDROMs, USB drives
- Label evidence

U.S. AIR FORCE

ICE3 - Issues

- Last 512 bytes error on Linux
- Using Firewire instead of USB
- USB 1.1 versus USB 2.0

U.S. AIR FORCE

Humbert

- Automated child porn detection tool
  - Humbert is the protagonist from Nabakov's *Lolita*
- Based on MD5 message digest (RFC 1321) analysis
- Engine is md5deep http://md5deep.sourceforge.net/
  - Cross platform MD5 program
  - Can work recursively
  - Can work in matching mode
  - About 1,600 lines of C
- Hashes of child porn coming from past AFOSI cases, other LE agencies and government organizations
  - Identified child porn

U.S. AIR FORCE

Humbert Instructions

- Insert CDROM/floppy into computer
- If computer is off, turn it on
- If computer is on `a: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

U.S. AIR FORCE

Questions?

Ask me anything!

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