Computer Based Forensics
- A Case Study -
U.S Support To The U.N.

Capt Kevin J. Ziese

AF Information Warfare Center

ziese@mailcenter.cmet.af.mil

Overview

- Presentation Strategy
- Working Definitions
- Problem Description
- Field Prototypes
- Major Shortfalls
- Top Five Christmas Gifts

Presentation Strategy

- Describe A, Serious, Real-World Problem
- Present The Low-Level Technical Issues
- Identify The Relevant Solution Criteria
- Generate, Focused, Expert Discussion
- Synthesize Potential R&D Directions
- Generate Potential COTS Opportunities
- Improve Overall Forensics Process

Computer Forensics

VALID TOOLS AND TECHNIQUES APPLIED AGAINST COMPUTER NETWORKS, SYSTEMS, PERIPHERALS, SOFTWARE, DATA, AND/OR USERS -- TO IDENTIFY ACTORS, ACTIONS, AND/OR STATES OF INTEREST

RELATED TO TRADITIONAL BIOLOGICAL, CHEMICAL, AND PHYSICAL SCIENCES

Valid Tools & Techniques

TOOLS AND TECHNIQUES THAT CAN BE APPLIED AS REQUIRED AND DO NOT REQUIRE RECASTING THE PROBLEM TO BE USED EFFECTIVELY

ARE CONFIGURATION DRIVEN WHICH MEANS THEY ARE, WHERE POSSIBLE, NOT COUNTRY OR OPERATING SYSTEM CENTRIC

Problem Description

- International Problems
  - Defines, And Complicates, The Solution Space
- Operational Problems
  - There Are Deltas Between “The Lab” & “Reality”
- Technical Problems
  - Effectiveness Always Comes Before Efficiency
- Legal Issues
  - Just Because It’s Legal Doesn’t Mean It’s Right

International Problems

- Is Iraq Violating U.N. Sanctions?
- Are Computers Supporting That Activity?
- Is Iraqi Compliance Real Or Feigned?
- How Reliable Are The Team's Findings?
- Did We Protect Iraq's Right?
- Did We Act As Good International Citizens?
- Where Are The 16 (?) Missing SCUDs?

Operational Problems

- How Did Computers Support NBC Activity?
- How Do You Protect Search Methods?
- How Do You Search Ancient Hardware?
- How Do You Search Hostile Systems Safely?
- How Do You Protect Tools & Data?
- When Should You Confiscate Hardware?
- How Long Can You Search ‘In Situ?’

Technical Problems

- Non-English Search Terms
- Non-Symmetric Language(s)
- Binary Application Interfaces
- Proprietary Storage Techniques
- Semantic Representation Of Data
- Information Hiding Techniques
- Search Tools Can Aggravate A Tense Situation

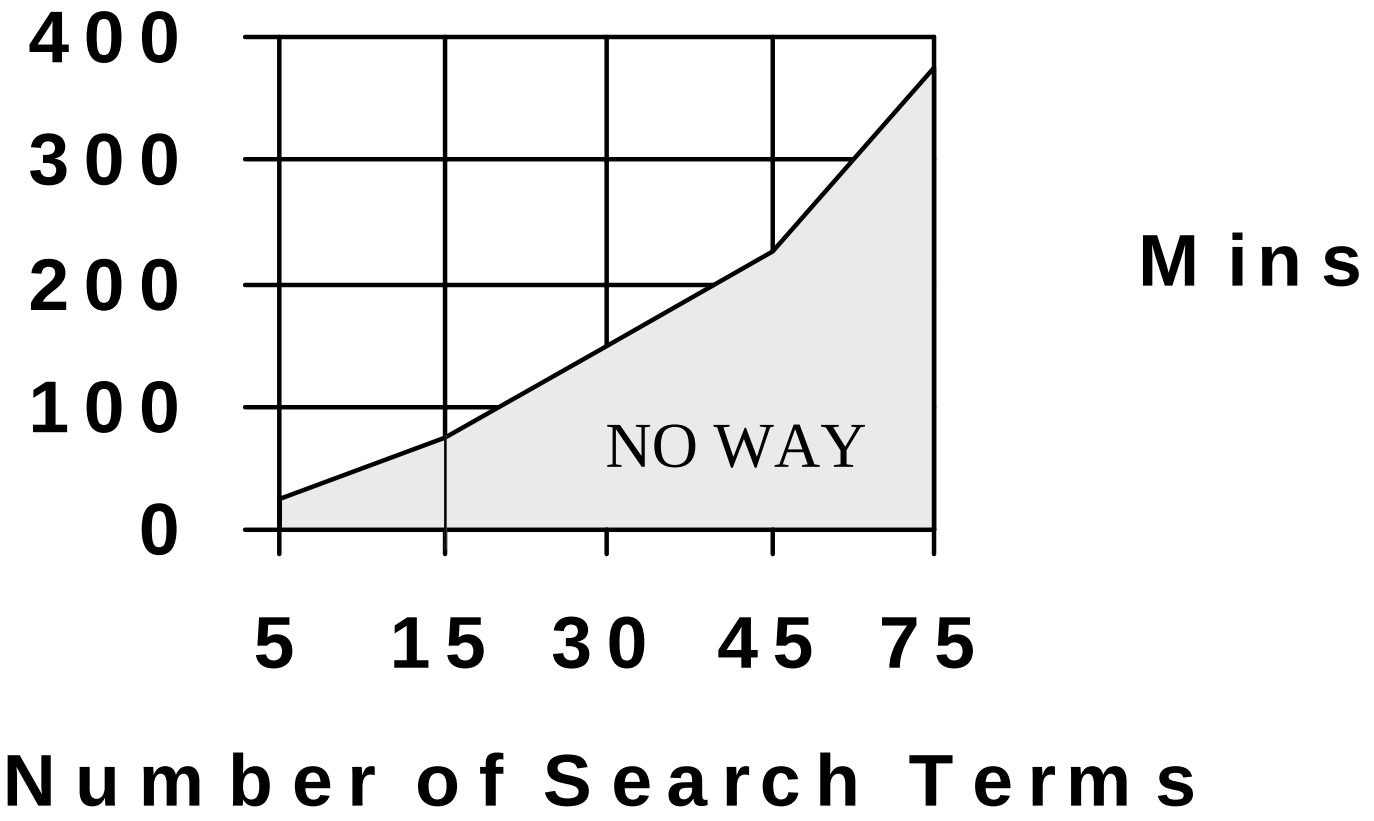
Non-English Search Terms

- Strings Are Not Easily Visualized
  - CONTRACT = UR]
  - CREDIT = HUJLA]
- Strings Change On Context
  - “HUJLA]” OR “MDXM” OR “HGU;”
- Often Mimic Binary Code Stubs
  - High False Positive Rate
  - Defies Many US-Centric Tools (STRINGS)

Non-Symmetric Languages

- Language Order Is Right -> Left
  - “ESUOH” vs “HOUSE”
- There Can Be Holes In The Language
  - “ESUxyOH” + “ESUxxyyzOH”
- Expressed Words Vary
  - “HOUSE” or “ABODE” ???
- Non-REGEX Searches Increased In Step-Linear Time
  - Time =(terms*3 mins) + (int(terms/5))* 10 mins
  - Best “Device” Tool Didn’t Support REGEX Searches

Search Times vs Search Terms



Binary Application Interfaces

- One Application Processes Data
- One Application Displays Data
- Common In Non-English Computers
- Data Was Stored As Huffman Encoded Trees

Semantic Data Representation

- Search Term Representation
  - MISSILE
- Context Representation

  “...MISSILE IN YOUR PATH...”
- Semantic Meaning
  - AUTOEXEC.BAT
  - REM Put Missile In Your Path
  - REM To Play Missile Commander Vers 2.1.3

Legal Issues

- People, And Countries, Have Rights!
- How Long, And Hard, Can You Search?
- What If Your Results Are Indeterminate?
- How Reproduceable Are Your Findings?
- Is Privacy Violated When Data Is Held?
- Is Freedom Violated When Data Is Held?

Operational Issues Today

- Do Manual Searches Endanger Privacy?
- Searches Are Long; Often Involve Confiscation
- Tools Are Not Standardized Or Validated
- Examiners Are Not Standardized Or Validated
- Good Forensics Can Enhance Personal Freedom
- Poor Forensics Can Erode Personal Freedom
- Today’s Forensics Need *LOTS* Of Work

Generic Search Shortfalls

- Tools/Data Must Be Secure In Transit
  - No Tool To Install Encrypted Payloads
- Findings Must Be Secure In Transit
  - No “Encrypt While Copying” Function
- Tools Require Positive Control
  - No “Permissive Action Link” Function(s)
- Tools Are OS Dependent

Prototyped Solutions

- Secure Delivery Tools
- Permissive Action Links
- Device Driven Tools

Secure Delivery

- Tools, And Terms, Encrypted On Floppy
- Floppy Is Mastered With Serial Number
- Decryption Requires
  - Decryption Key
  - Valid Serial Number
  - Operator Authorization
- Only Then Can Search Begin

Permissive Action Links

- Two-Passwords To Execute
- Aperiodic “Attributes” Check
- Destroy On Failed Test Return

Device Driven Tools

- Search Files, Slack Space, Erased/Swap
- Search Logical, Network, Devices
- Search Logical Filesystem Partitions
- Search Raw Device Filesystems

Major Shortfalls

- Technical Shortfalls
- Privacy Shortfalls
- Tomorrow’s Shortfalls

Technical Shortfalls

- Tools Tend To Be Time Inefficient
- Tools Tend To Be US-Centric
- Tools Tend To Be OS-Centric
- What About Information Hiding Techniques?
- We Need ‘dd’ For Every OS

Tools vs Time Efficiency

- Overfocus On Graphic Interfaces
- No Focus On Efficiency/Performance Impact
- Too Little Focus On Semantic Representation
- Don’t Scale Well To Disjoint Text Patterns
- Very High False Positive Rates
- Still Very Much “Caveat Emptor”

US-Centric Tools

- Strings & Egrep Are Efficient -- Not Effective
- Filtering Templates Would Be Better
  - Allow Users To Define “Strings”
  - Allow Users To Define “Operators”
- Other “Languages” Problem Mimics Encryption
  - What About Encryption…
  - Was Encryption Used? What Types?

OS-Centric Tools

- We Need Device Oriented Searches
- We Need User Definable Data Views
  - User Specifies Disk Geometry
  - User Specifies /etc/magic Relations
  - User Specifies User Views
- We Don’t Need “UNIX” Solutions…
- We Do Need “Cross-Platform” Solutions...

Information Hiding Techniques

- Painfully Slow
  - Good Graphics, Limited Functionality
- Few Choices And Limited Envrionments
  - Sound Files And Graphics In DOS primarily
  - What About .AU files What About JPEG?
- More Anecdotal & Notional
  - A Smart “Attacker” Will Use Them…
  - …We Don’t Usually Catch The Smart Ones

One ‘DD’ For Unix, DOS, Mac

- No Less Than 5 Backup Methods
- No Less Than 15 Reload Procedures
- One Source Tree With One Makefile
- Low-Level, Configurable, Disk Backup
- Ability To “Model” One System On Another
  - Simulation Environment To Analyze X on Y
  - Ability To Model One Executable X on OS Y
  - Backups/Reloads, Static, and Dynamic Analysis

Top Five Christmas Gifts

- Encrypted File Systems For Unix, DOS, Win95
- /etc/magic For All Unix, DOS, Mac, Etc
- Fast, CLI, Search Tool For Unix, DOS
- To Be Home For The Holidays
- The 16 Remaining SCUD Missiles