
Digital Forensic and E- Discovery Countermeasures

David Jesse Coker

Google is your friend...everything in
this presentation can be found by
using Google.

Introduction

- “None of your business.” – A uniquely American phrase.
 - Criminal Considerations
 - Civil Considerations
 - Learning Objectives:
 - Avoiding exploitation or compromise associated with overbroad discovery.
 - Provide attendees with links to tools (preferably cost-free) to aid them in the protection of their data.
-

Protection from Government

■ Fourth Amendment

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

- Drafted in response to the British magistrates issuing “general warrants” without probable cause or reasonable specificity.

■ Fifth Amendment

“No person...shall be compelled in any criminal case to be a witness against himself...”

- Applies only to spoken statements, generally will not apply to writings, contents of hard drives, etc. (very few exceptions: diaries, etc.)
-

Protection from Private Entities

- **Codified/Statutory Privacy Law**
 - Duty to Destroy
 - Duty to Report
 - Duty to Protect/Secure/Encrypt
 - **Prosser's Four Torts – Civil Right to Privacy**
 - Identity Theft
 - False Light
 - Public Disclosure of Private Facts
 - Unreasonable Intrusion Upon Seclusion or Solitude
-

Electronic Evidence

- **Birth of “Digital Forensics”**
 - Overview
 - Current Trends
 - Issues
 - **Growth of Electronic Discovery**
 - Overview
 - Deals with any “electronically stored” information.
 - Amendments to the Federal Rules of Civil Procedure
 - Issues
-

Digital Discovery and E-Discovery Issues

- Abuse and Misunderstanding
 - *In Re Honza*, 242 S.W.3d 578 (Tex. App. Waco 2008) In *Honza*, the court makes it clear that a firm's *entire* hard drive can be imaged/cloned by an expert as the first part of the electronic discovery process, even when the scope pertains to a very limited amount of information contained on the computer.
 - Sounds a lot like a "general warrant" solution to the problem of judicial ignorance of technical issues.
 - Public Response: Law
-

Digital Forensic Methodology

- Five Step Process:
 - Preparation/Training
 - Data Collection
 - Examination
 - Analysis
 - Reporting
-

Things to Think About...

- Cost - \$\$\$\$\$\$\$\$\$\$
 - Training/Background of the Investigator
 - Tools Used
 - Chain of Custody
 - Data Recovery/File Carving
 - Data Mining
 - Network/Email Tracking
 - Logs
 - Cruft (Browsing History, Cookies, etc.)
-

Some Forensic Tool Examples

- *dd and dcfldd (underlying tool of many GUI acquisition tools)
 - *Helix (Suite of OpenSourceTools)
 - Sleuth Kit
 - Autopsy
 - Adepto (dcfldd GUI)
 - pyflag
 - Many more...
 - EnCase
 - GUI tool that reduces training and technical knowledge requirements
 - *WinHex
 - Tool allowing manual review of raw data
 - *Scalpel
 - File Carving Tool
 - SMART
 - *The List goes on and on...and on...salesman's dream.*
 - Exhaustive list is available at: <http://www.forensicswiki.org>
-

*Coker preferred.

Defeating and Frustrating the Investigator or Opposing Counsel

- Policies, Habit, Good Business Practice
 - Data Segregation
 - Security by Obscurity
 - Removing Cruft
 - Data Encryption
 - Data Destruction
 - Slack Space and Free Space Wiping
 - Plausible Deniability/Deniable Encryption
 - Online Anonymity
-

Policies, Habit, and Good Business Practice

- Create business policies that allow for ongoing destruction and removal of unused data.
 - Comply with all relevant laws, regulations, and accepted practice within industry.
 - Distribute throughout company.
 - Training.
 - Goal of ensuring that non-relevant, discoverable data is destroyed as a matter of "...regularly conducted business..." or "...habit or ritual...".
 - **NEVER DESTROY IN ANTICIPATION OF LITIGATION!!!**
-

Data Segregation

- Explained
 - Methodology
 - Create separate drives, folders, or similar logically separated areas for each client, business area, subject, department.
 - Avoid lumping all client data in one place.
 - Habit and Best Practices
 - This must become standard practice.
 - Avoids perception of impropriety or bad faith.
-

Security by Obscurity

- Alternative File Systems
 - Alternative Operating Systems
 - Strange, “evolved”, systems that have grown over time.
 - Proprietary applications.
 - Generally, any non-standard configuration will aid in delaying, confusing, or confounding the typical investigator.
-

Logs

- Explained
 - Clearing them
 - Cost-Free Tools
 - Logmaid – Automatically clears your blackberry log every hour.
 - Log files are very vendor specific, therefore, the list of tools is as long as the list of all software applications.
 - CCCleaner - <http://www.ccleaner.com/>
-

Cruft

- Explained
 - Getting rid of it
 - Some Cost-Free Tools
 - CCCleaner - <http://www.ccleaner.com/>
 - My approach:
 - Run CCCleaner
 - Follow up with a full free space wipe using Eraser - <http://sourceforge.net/projects/eraser/>
-

Data Encryption

- Explained
- “Encryption at Rest”
- “Encryption in Transit”
- Cost-Free Tools
 - PGP - <http://www.pgp.com/>
 - Not free, but very intuitive and reasonably priced.
 - GnuPG - <http://www.gnupg.org/>
 - Requires experience working with PGP or similar public/private key encryption.
 - TrueCrypt - <http://www.truecrypt.org/>

Data Destruction

- Explained
- Cost-Free Tools
 - DBAN (Darik’s Boot and Nuke) - <http://www.dban.org/>
 - Eraser - <http://sourceforge.net/projects/eraser/>
- Device Wiping (PDAs, Blackberries, iPods, etc.)
 - Generally vendor specific
 - E.g., on a blackberry:
 - App Menu →
 - Options →
 - Security Options →
 - General Settings →
 - <menu button> →
 - “Wipe Handheld”

Metadata Removal

- Explained
 - Some Cost-Free Tools
 - Office 2003/XP Add-In: Remove Hidden Data
 - <http://www.microsoft.com/downloads/>
 - DocScrubber - <http://www.javacoolsoftware.com/docscrubber.html>
-

Slack Space and Free Space Wiping

- Explained
 - Some Cost-Free Tools
 - Eraser - <http://sourceforge.net/projects/eraser/>
-

Plausible Deniability – Deniable Encryption

- Explained
 - Rubber-hose cryptanalysis
 - “Hidden” volumes
 - Ethical Considerations
 - Some Cost-Free Tools
 - TrueCrypt - <http://www.truecrypt.org/>
 - FreeOTFE - <http://www.freeotfe.org/>
 - Great for PDAs
 - Does not require any installation
-

Online Anonymity

- Explained
 - Ethical Considerations
 - Some Cost-Free Tools
 - Anonymous Emailers – *Won't go here...go google.*
 - TOR - <http://www.torproject.org/>
 - Privoxy - <http://www.privoxy.org/>
-

Dealing with Malware

- Explained
 - Avoidance
 - Use *any* browser besides Microsoft IE
 - Google Chrome - <http://www.google.com/chrome>
 - Mozilla - <http://www.mozilla.org/>
 - Opera - <http://www.opera.com/>
 - Alternative Operating Systems (Security by Obscurity)
 - Some Cost-Free Removal Tools
 - MalwareBytes - <http://www.malwarebytes.org/>
 - Clamwin Antivirus - <http://www.clamwin.com/>
 - AdAware - <http://www.lavasoft.com/>
-

Web 2.0 and Privacy

Web 2.0



Source: "Austin Powers in Goldmember" MGM Studios

Web 1.0



Source: Honda, USA

If you want privacy, which one would you drive?

What Lies Ahead?

- Continued erosion of the U.S. Citizen's privacy and protection from unreasonable searches.
 - Reemergence of the "General Warrant" in the context of computer searches:
 - Increasingly frustrated and confused courts, legislative bodies, and lawyers will likely continue to take a "let it all in" approach, thus, turning back the clock to 1750 in the context of computer searches.
 - *In Re Honza* already smells like a "general warrant" solution.
-

Conclusion

- Current trends paint a rather bleak picture.
- Hard cases make bad law.
- The importance of knowing how to protect yourself cannot be emphasized enough.

"In skating over thin ice, our safety is our speed." --Ralph Waldo Emerson

Questions