Counter-Forensic Tools
Failures & Fingerprints

Matthew Geiger
mgeiger@cert.org

Roadmap

- What do these tools do? Who produces and sells them?
- Why do we care? Legal issues
- Summary of testing procedures & results
- Identifying fingerprints left by these tools
- Resources for forensic practitioners
  - Tool behavior guide for analysts
  - Aperio, a forensic utility for finding tool signatures

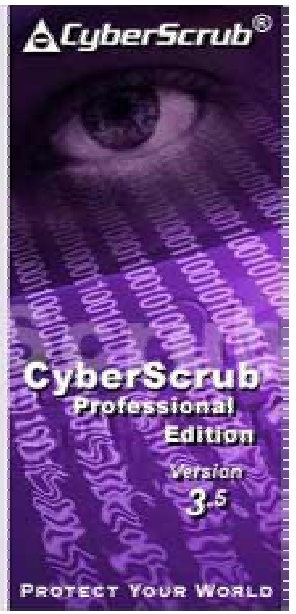
Counter-Forensic Landscape

- More than twenty commercial software packages
- Designed to eliminate specific records and files but leave system otherwise functional
  - Overwrite deleted data to thwart recovery
  - Cope with system files, like the Registry
- Aimed at users that may not be proficient

Who Produces Them?

The vendor marketplace:

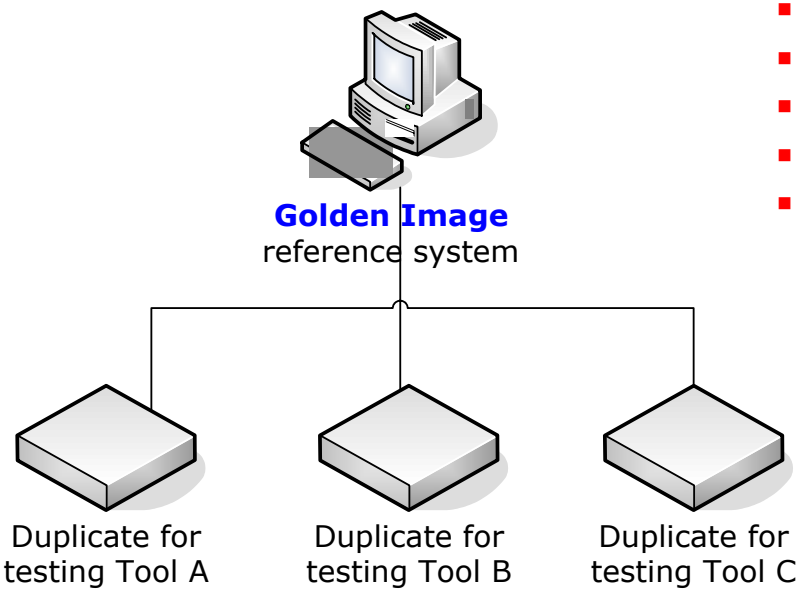
- Competitive
- Wide range of enterprises
  - Unincorporated entities
  - Well-financed companies
- Marketed as:
  - Safeguarding privacy
  - Protecting corporate data
  - Helping avoid consequences



Legal Trends

- Counter-forensic tools increasingly reported as factors in investigation, court
- Courts have grappled with how to treat the use of these tools:
  - US v. H. Marc Watzman, 2003
  - Kucala Enterprises v Auto Wax Co., 2003
  - UK v. Timothy Pickup, 2004
  - U.S. v. Robert Johnson, 2005
  - State of Missouri v. Zacheriah Tripp, 2005

Testing the Tools



- Twelve software packages:
  - Cyberscrub
  - Window Washer
  - SecureClean
  - Evidence Eliminator
  - Acronis Privacy Expert
  - RTT R-Wipe & Clean
  - Absolute Shield
  - Privacy Eraser Pro
  - Evidence Blaster
  - History Kill
  - Privacy Guardian
  - Tracks Cleaner

- Reference system created on Windows XP
- Typical user activity generated
- Bitstream image of test system duplicated as starting point for each tool test

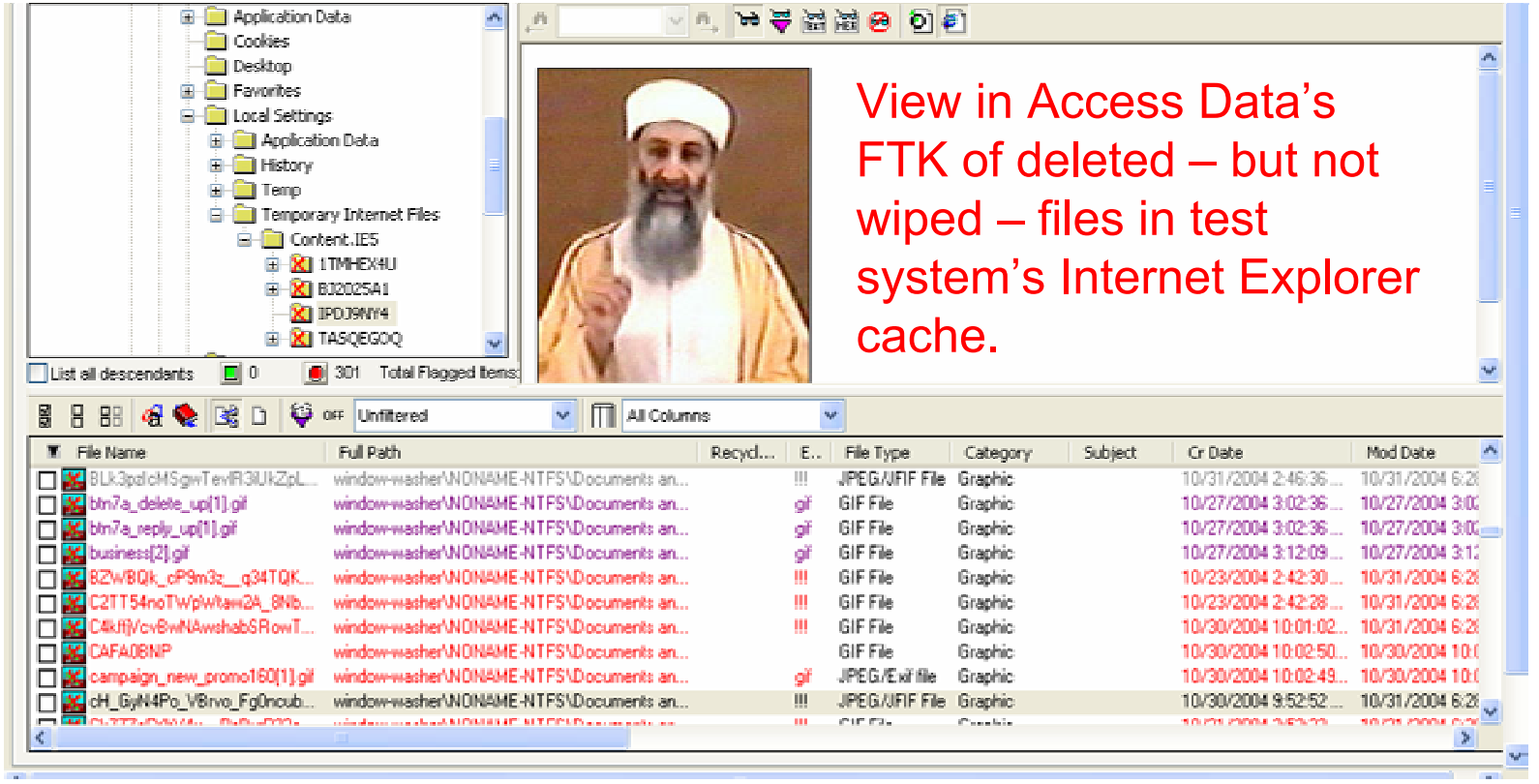
Design Goals

- **Technical**
  - Accepted forensic tools and practices
  - Readily reproducible and extensible
  - Evaluate each tool's performance in an identical environment
- **Strategic**
  - Common technical challenges = common practices?
  - Common practices = common flaws?
- **Not** an exhaustive catalog of tool performance

Results: Some Significant Flaws

- **All** the tested tools missed some degree of potential evidentiary data
- Three of the 12 exhibited wiping failures that allowed for extensive data recovery
- Two broad classes of failures:
  - Implementation flaws / bugs
  - Inability to keep up with evolving systems and applications – data targets changing

Window Washer



1st test version of Window Washer failed to wipe deleted files

Evidence Eliminator

- Evidence Eliminator created temp directory while processing locked files – but then neglected to purge its contents
- Files included IE history and cache index

URL	http://artists.iuma.com/site-bin/mp3gen/62398/IUMA/Bands/The_Cash_County_Survivors_Paper_Bottle_Brown_Live__the_Darkhorse.mp3
User name	Anon Nym
Page title	
Last Accessed (UTC)	9/30/2005 7:31:41 PM
Last Modified (UTC)	9/30/2005 7:31:41 PM
Last Checked (UTC)	9/30/2005 7:31:42 PM
Expires (UTC)	10/11/2005 7:24:32 PM
Hits	1
Use Count	0

Acronis Privacy Expert

Acronis Privacy Expert 8 purged Recycle Bin but overlooked INFO file listing its former contents

Filename	De5.doc
Original Name	E:\Documents and Settings\Anon Nym\My Documents\Private material\world domination topics\masterplan-secretstuff.doc
Date Recycled	10/3/2005 4:56:41 PM
Removed from Bin	Yes

Filename	De6.jpg
Original Name	E:\Documents and Settings\Anon Nym\My Documents\Private material\world domination topics\domination photos\land3.jpg
Date Recycled	10/3/2005 4:57:03 PM
Removed from Bin	Yes

Other Examples

- Several tools failed to wipe:
  - Outlook Express e-mail selected for deletion
  - Scattered files in IE cache, or IE history / cache index
  - Third-party applications' usage data
- Some tools incompletely wiped unallocated space
- For about half the tested tools, document and web content was recoverable from the pagefile

Examples of "Complexity" Failures

- Tools failed when the location and/or format of user data was changed
  - Most tools missed some Registry file usage data created by Office 2003
  - Many of the tools don't report the version of the application they have been designed to handle
- All but three tested tools missed copies of the registry preserved in Windows restore points, a feature new in XP

Buggy Software

- Several tools have *serious functional flaws*
- Shortfalls in QA and testing
  - Leads to both classes of flaws
  - Not limited to smaller companies

- *Many failures would not be noticeable to users*
  - May reduce pressure to fix, increase lifespan of bugs
  - Difficult for users to validate performance

Complexity Failures

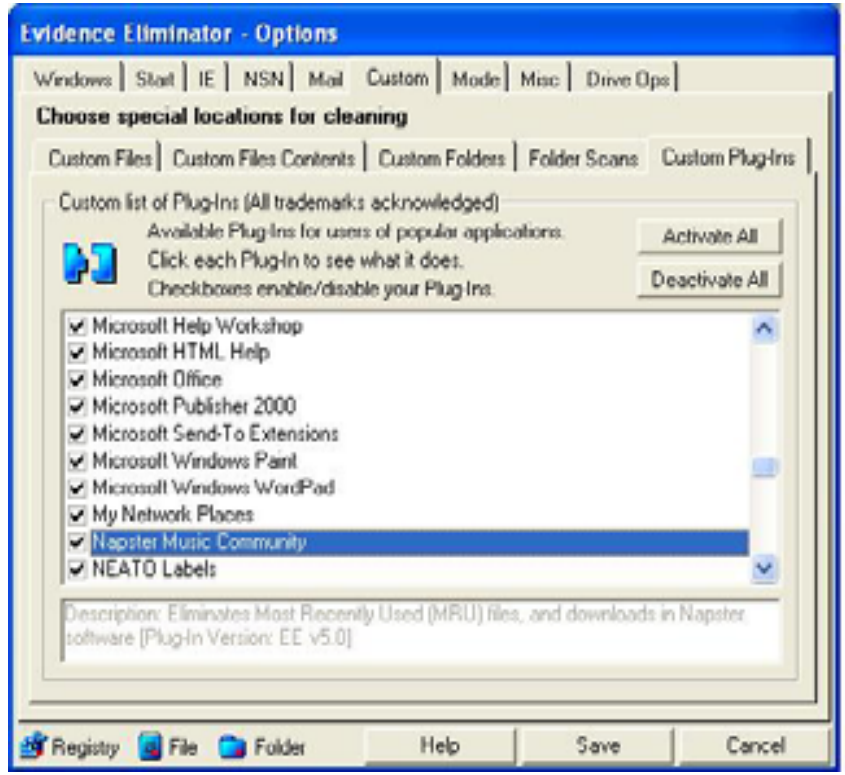
*Complexity = (# of applications) * (Δ/t of those applications)*

- Challenge of locating & deleting usage records rises with the number of applications covered
- What's more, programs and the underlying operating system are continually evolving
- Some of these changes affect their data storage – and how to eliminate it

Committed by Competition

- Yet, marketing & competition based on number of third-party programs handled

Some tools provide "plug-ins" to purge activity records for more than 100 separate applications



Operational Fingerprints

- Each tool creates a *distinct operational fingerprint* on filesystem, which may:
  - Identify the counter-forensic application used
  - Guide a search for residual data
  - Demonstrate the use of a tool in cases where use may have legal ramifications.

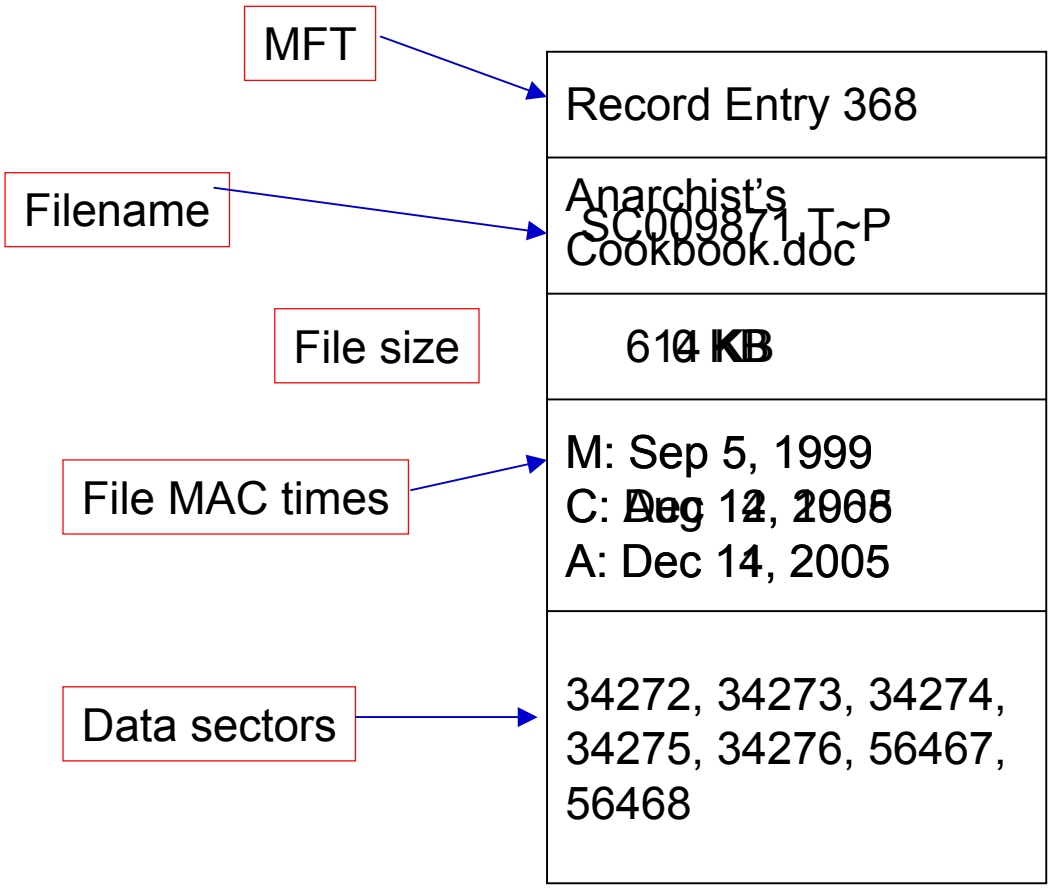
Note: These signatures exist even if a counter-forensic program was executed from another partition, or if its own files are eradicated

Tell-Tale Tracks

- Most obvious and common fingerprint is the way a tool tries to obscure file name, other metadata
- None of the tools tested duplicated another's

Evidence Eliminator	Wiped files were renamed with 243 characters with no filename extensions. All except the first 10 characters are pseudo-random combinations of lowercase letters. The first 10 characters are numbers that increment by one for every file wiped. Example: 0000002825wtkdvjiiugvwgveodruvlmdptxgpgfyrqnxpxyjajk qrienrnebnzhoshuyfzhdvzvvvveszlikswlhqpwbetowmznlvzquveyvhkrk cidsmpgpjrxjgpzaxcffvdxynlxiikdnhgachijkuajmdfdcvxbupesrwdyykqf ckndbqwittwnyfmtcesftoxtyrnfdwwoblkpcvzwseokhydmcvtvodbrwyv vmewuoge
Secure Clean	Targeted files renamed with a six-digit numerical sequence that appears to be incremented by one for every file wiped. The numbers are preceded by the initials SC. The extension assigned was consistently T~P. Example: SC000043.T~P.

Data-Scrubbing in Action



Aperio

- Forensic utility allows examiners to screen for the use of counter-forensic tools
- Uses Linux-NTFS libraries to address MFT, filesystem structures
- Configuration file specifies elements of tool signatures:

```
# Sample regex specification file for Aperio
# This file specifies terms, where applicable, for
# setting up Aperio searches. Fields are white-space separated.
#
#Name                Version    MFT Name Pattern          Mod Time    File Length    Data Pattern
Evidence Eliminator  5.508      [0-9]{6,10}[a-z]{210,245}  NA          0              NA
```

Aperio output

- Running Aperio version 0.4
- Started at Tue May 9 15:26:06 2006

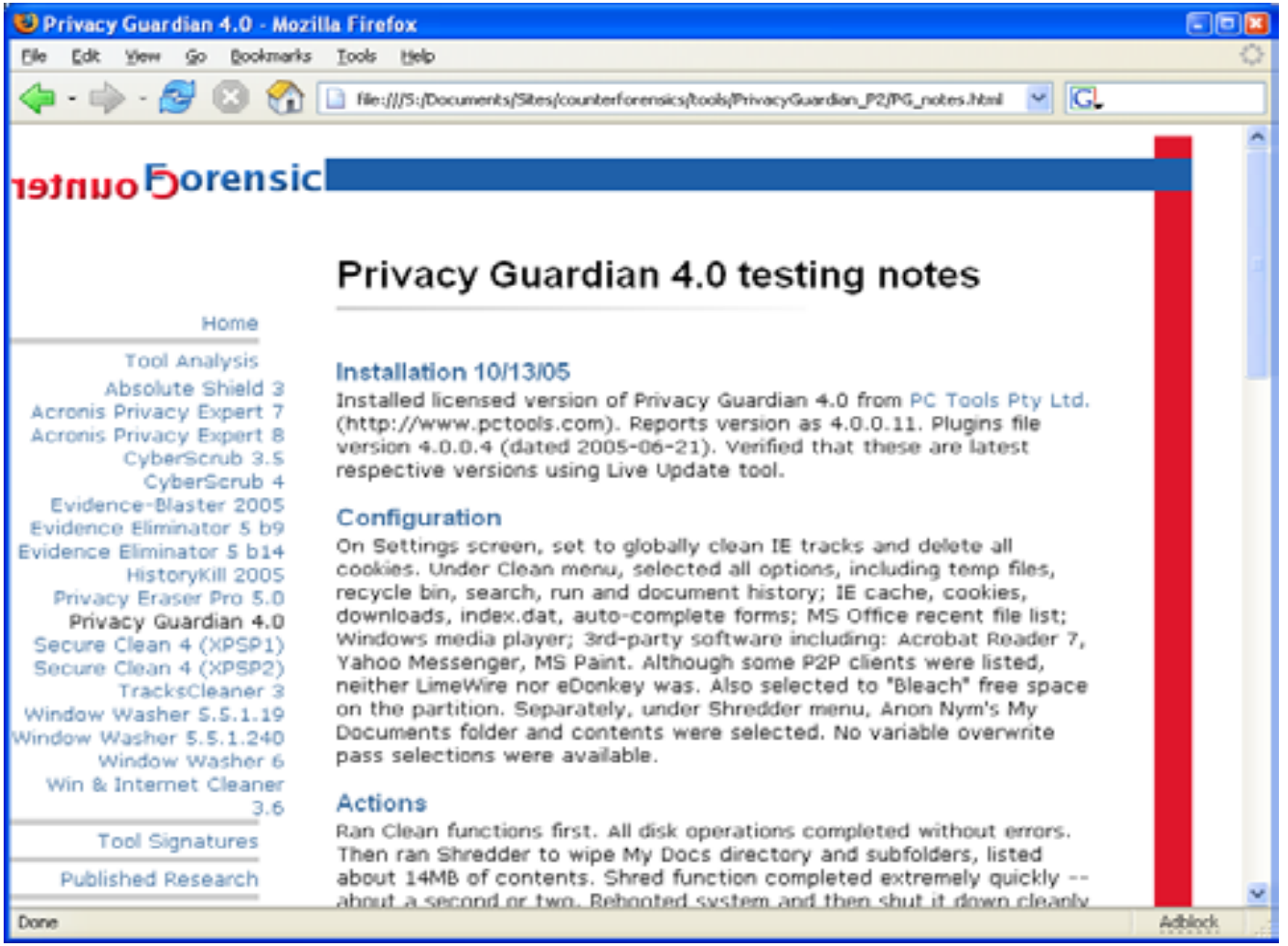
- Signature file used: ./aperio.conf

- Signatures loaded for:
- Evidence_Eliminator v. 5.0x
- Secure_Clean v. 4.0
- Absolute_Shield v. 3.x
- CyberScrub v. 3.5-4
- CyberScrub v. 3.5
- CyberScrub v. 4
- Privacy_Eraser(Win&Inet_Cleaner) v. 5.0(3.6)
- Window_Washer v. 5.5.0-1.19
- R-Wipe&Clean v. 6.0
-
- _____

•MFT pattern consistent with the use of Privacy_Eraser(Win&Inet_Cleaner) v. 5.0(3.6) detected.
•MFT Record 74641
•Type: File
•Date: 2006-04-27 19:03
•Filename: (2) SSCS52~1.TMP
•Filename: (1) SSCS52456C76-041C-49CA-BA64-125244E0D99A.tmp
•File Flags: <none>
•Size alloc: 0
•Size data: 0
•Date C: 2006-03-20 07:31
•Date A: 2006-03-20 07:31
•Date M: 2006-03-20 07:31
•Date R: 2006-03-20 07:31
•Data Streams:
•Name: <unnamed>
•Flags: Resident

•Size alloc: 0
•Size data: 10
•Size init: 0
•Size vcn: 0
•Data runs:
- None

Analyst Reference



Summary

- Most tested commercial counter-forensic tools leave potentially useful data

- Still, their ability to destroy data can also present a significant obstacle to analysts

- Research such as this can help:
  - understand the behavior of these tools
  - identify and interpret the records a tool misses
  - provide a foundation for demonstrating evidence of wiping activity

Thank you