

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
 - Aferio, a forensic utility for finding tool signatures

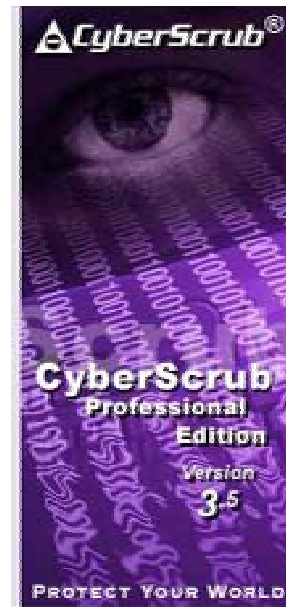
Counter-Forensic Landscape

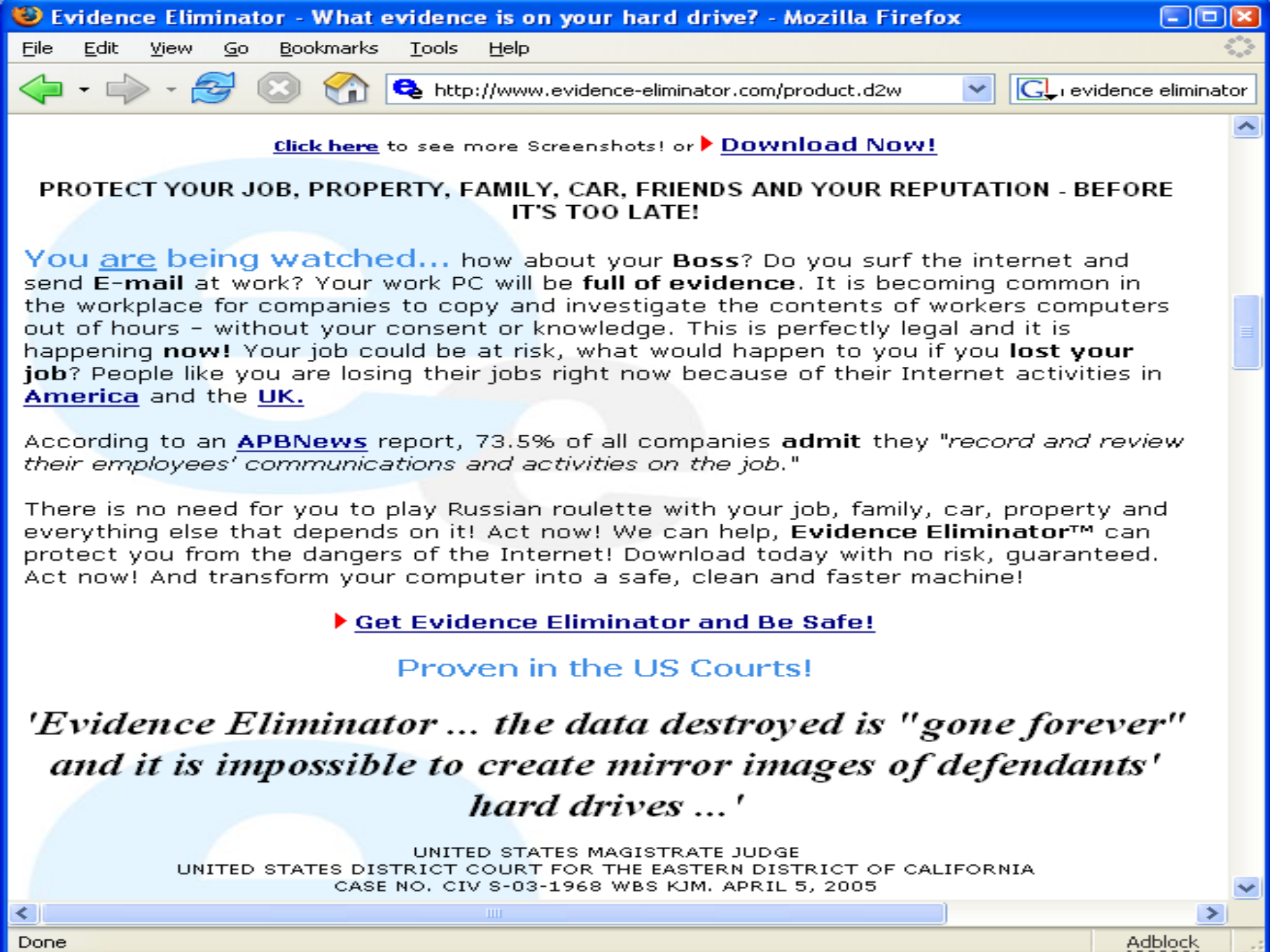
- More than twenty commercial software packages
- Designed to eliminate specific records and files but leave system otherwise functional
 - Overwrite deleted data to thwart recovery
 - Cope with system files, like the Registry
- Aimed at users that may not be proficient

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





[Click here](#) to see more Screenshots! or [Download Now!](#)

PROTECT YOUR JOB, PROPERTY, FAMILY, CAR, FRIENDS AND YOUR REPUTATION - BEFORE IT'S TOO LATE!

You are being watched... how about your **Boss**? Do you surf the internet and send **E-mail** at work? Your work PC will be **full of evidence**. It is becoming common in the workplace for companies to copy and investigate the contents of workers computers out of hours - without your consent or knowledge. This is perfectly legal and it is happening **now!** Your job could be at risk, what would happen to you if you **lost your job**? People like you are losing their jobs right now because of their Internet activities in [America](#) and the [UK](#).

According to an [APBNews](#) report, 73.5% of all companies **admit** they "*record and review their employees' communications and activities on the job.*"

There is no need for you to play Russian roulette with your job, family, car, property and everything else that depends on it! Act now! We can help, **Evidence Eliminator™** can protect you from the dangers of the Internet! Download today with no risk, guaranteed. Act now! And transform your computer into a safe, clean and faster machine!

[▶ Get Evidence Eliminator and Be Safe!](#)

[Proven in the US Courts!](#)

'Evidence Eliminator ... the data destroyed is "gone forever" and it is impossible to create mirror images of defendants' hard drives ...'

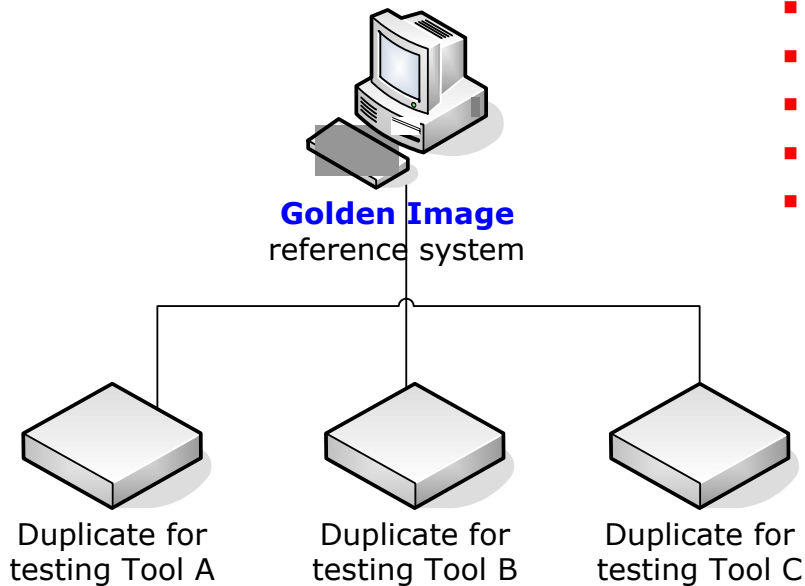
UNITED STATES MAGISTRATE JUDGE
UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF CALIFORNIA
CASE NO. CIV S-03-1968 WBS KJM, APRIL 5, 2005

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

View in Access Data's FTK of deleted – but not wiped – files in test system's Internet Explorer cache.

File Name	Full Path	Recycl...	E..	File Type	Category	Subject	Cr Date	Mod Date
Bk3pd0MSgWTeVIR3UkZpL...	window-washer\NODNAME-NTFS\Documents an...	!!!		JPEG/JIF File	Graphic		10/31/2004 2:46:36 ...	10/31/2004 6:28
btn7a_delete_up[1].gif	window-washer\NODNAME-NTFS\Documents an...		gif	GIF File	Graphic		10/27/2004 3:02:36 ...	10/27/2004 3:00
btn7a_rep[1].gif	window-washer\NODNAME-NTFS\Documents an...		gif	GIF File	Graphic		10/27/2004 3:02:36 ...	10/27/2004 3:00
business[2].gif	window-washer\NODNAME-NTFS\Documents an...		gif	GIF File	Graphic		10/27/2004 3:12:09 ...	10/27/2004 3:10
B2w/BQk_cP9m3z_q34TQK...	window-washer\NODNAME-NTFS\Documents an...	!!!		GIF File	Graphic		10/23/2004 2:42:30 ...	10/31/2004 6:28
C2TT54noTWpWtaw2A_8Nb...	window-washer\NODNAME-NTFS\Documents an...	!!!		GIF File	Graphic		10/23/2004 2:42:28 ...	10/31/2004 6:28
C4kHfVcv8wNAwshabSR0wT...	window-washer\NODNAME-NTFS\Documents an...	!!!		GIF File	Graphic		10/30/2004 10:01:02...	10/31/2004 6:28
CAFA08NP	window-washer\NODNAME-NTFS\Documents an...			GIF File	Graphic		10/30/2004 10:02:50...	10/30/2004 10:0
campaign_new_promo160[1].gif	window-washer\NODNAME-NTFS\Documents an...		gif	JPEG/Exif file	Graphic		10/30/2004 10:02:49...	10/30/2004 10:0
ch_GyN4Po_V8rvo_Fg0ncub...	window-washer\NODNAME-NTFS\Documents an...	!!!		JPEG/JIF File	Graphic		10/30/2004 9:52:52 ...	10/31/2004 6:28
Ch377v0wM...	...	!!!		GIF File	Graphic		10/31/2004 2:52:29 ...	10/31/2004 6:28

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

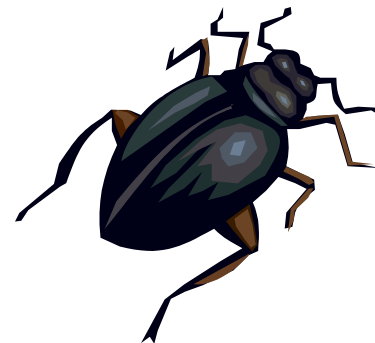
- Several tools failed to wipe:
 - Outlook Express e-mail selected for deletion
 - Scattered files in IE cache, or IE history / cache index
 - Third-party applications' usage data
- Some tools incompletely wiped unallocated space
- For about half the tested tools, document and web content was recoverable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

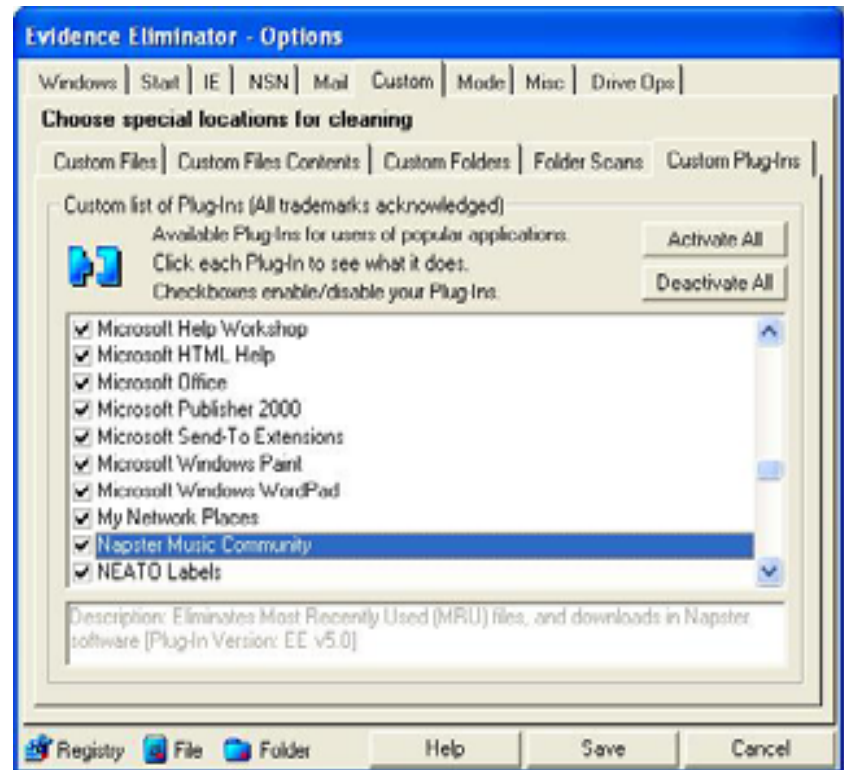
*Complexity = (# of applications) * (Δ / t of those applications)*

- 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.

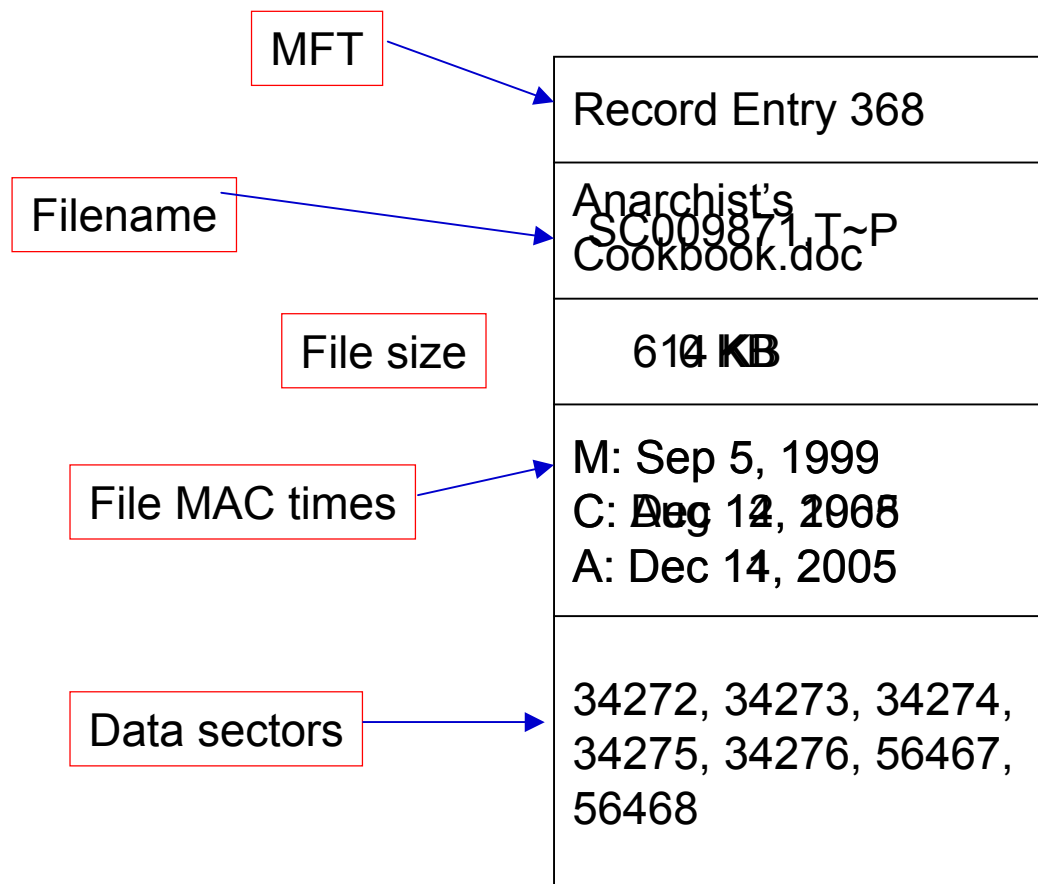
Note: These signatures exist even if a counter-forensic program was executed from another partition, or if its own files are eradicated

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	<p>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.</p> <p>Example: 0000002825wtkdvjiiugvwgveodruvlmdptxgpgfyrqnxpxyjajkqrienrnebnzhoshuyfzhdvzvsvveszlikswlhqpwbetowmznlvzquveyvhkrkcidsmpgpjrxjgpzaxcffvdxynlxiiikdnhgachijkuajmdfcdvxbupesrwdyykqfckndbqwittwnyfmtcesftoxyrnfdwwoblkpcvzwseokhydmcvtvodbrwyv vmewuoge</p>
Secure Clean	<p>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.</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

The screenshot shows a Mozilla Firefox browser window titled "Privacy Guardian 4.0 - Mozilla Firefox". The address bar contains the file path: file:///S:/Documents/Sites/counterforensics/tools/PrivacyGuardian_P2/PG_notes.html. The page content is as follows:

197100 Forensic

Privacy Guardian 4.0 testing notes

[Home](#)

[Tool Analysis](#)

- Absolute Shield 3
- Acronis Privacy Expert 7
- Acronis Privacy Expert 8
- CyberScrub 3.5
- CyberScrub 4
- Evidence-Blaster 2005
- Evidence Eliminator 5 b9
- Evidence Eliminator 5 b14
- HistoryKill 2005
- Privacy Eraser Pro 5.0
- Privacy Guardian 4.0
- Secure Clean 4 (XPSP1)
- Secure Clean 4 (XPSP2)
- TracksCleaner 3
- Window Washer 5.5.1.19
- Window Washer 5.5.1.240
- Window Washer 6
- Win & Internet Cleaner 3.6

[Tool Signatures](#)

[Published Research](#)

Installation 10/13/05

Installed licensed version of Privacy Guardian 4.0 from PC Tools Pty Ltd. (<http://www.pctools.com>). Reports version as 4.0.0.11. Plugins file version 4.0.0.4 (dated 2005-06-21). Verified that these are latest respective versions using Live Update tool.

Configuration

On Settings screen, set to globally clean IE tracks and delete all cookies. Under Clean menu, selected all options, including temp files, recycle bin, search, run and document history; IE cache, cookies, downloads, index.dat, auto-complete forms; MS Office recent file list; Windows media player; 3rd-party software including: Acrobat Reader 7, Yahoo Messenger, MS Paint. Although some P2P clients were listed, neither LimeWire nor eDonkey was. Also selected to "Bleach" free space on the partition. Separately, under Shredder menu, Anon Nym's My Documents folder and contents were selected. No variable overwrite pass selections were available.

Actions

Ran Clean functions first. All disk operations completed without errors. Then ran Shredder to wipe My Docs directory and subfolders, listed about 14MB of contents. Shred function completed extremely quickly -- about a second or two. Rebooted system and then shut it down cleanly.

Done AdBlock

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