Evaluating Commercial Counter-Forensic Tools

By

Matthew Geiger

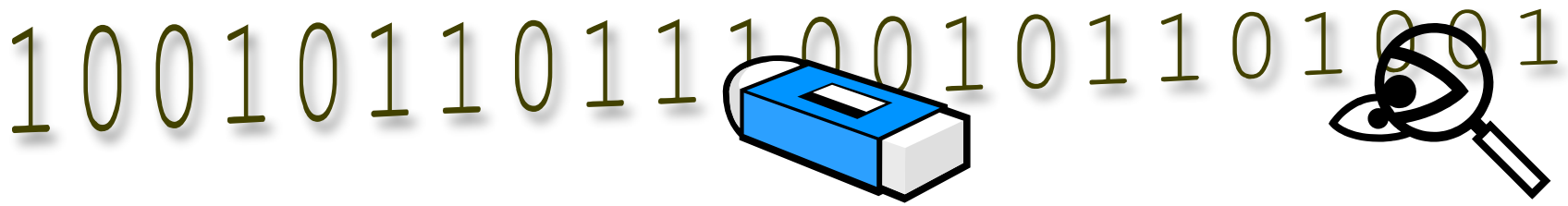
Presented At

The Digital Forensic Research Conference

DFRWS 2005 USA New Orleans, LA (Aug 17th - 19th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org



Evaluating Commercial Counter-Forensic Software

Matthew Geiger

Carnegie Mellon University

Roadmap

- What do these tools do and why do they exist?
- Why are they important to us? Legal significance
- Who produces and sells them?
- Outline of testing procedures
- Summary of results, examples
- Implications for forensic practitioners

Counter-Forensic Landscape

- More than a dozen 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

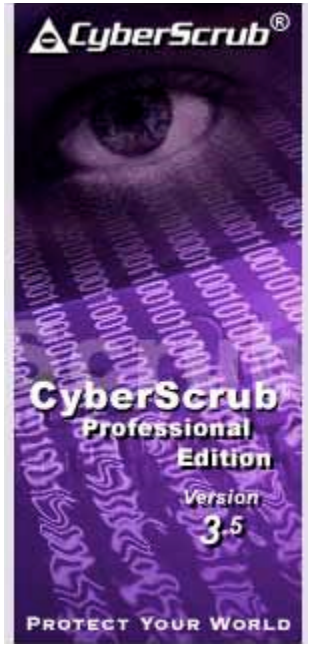
Who Produces Them?

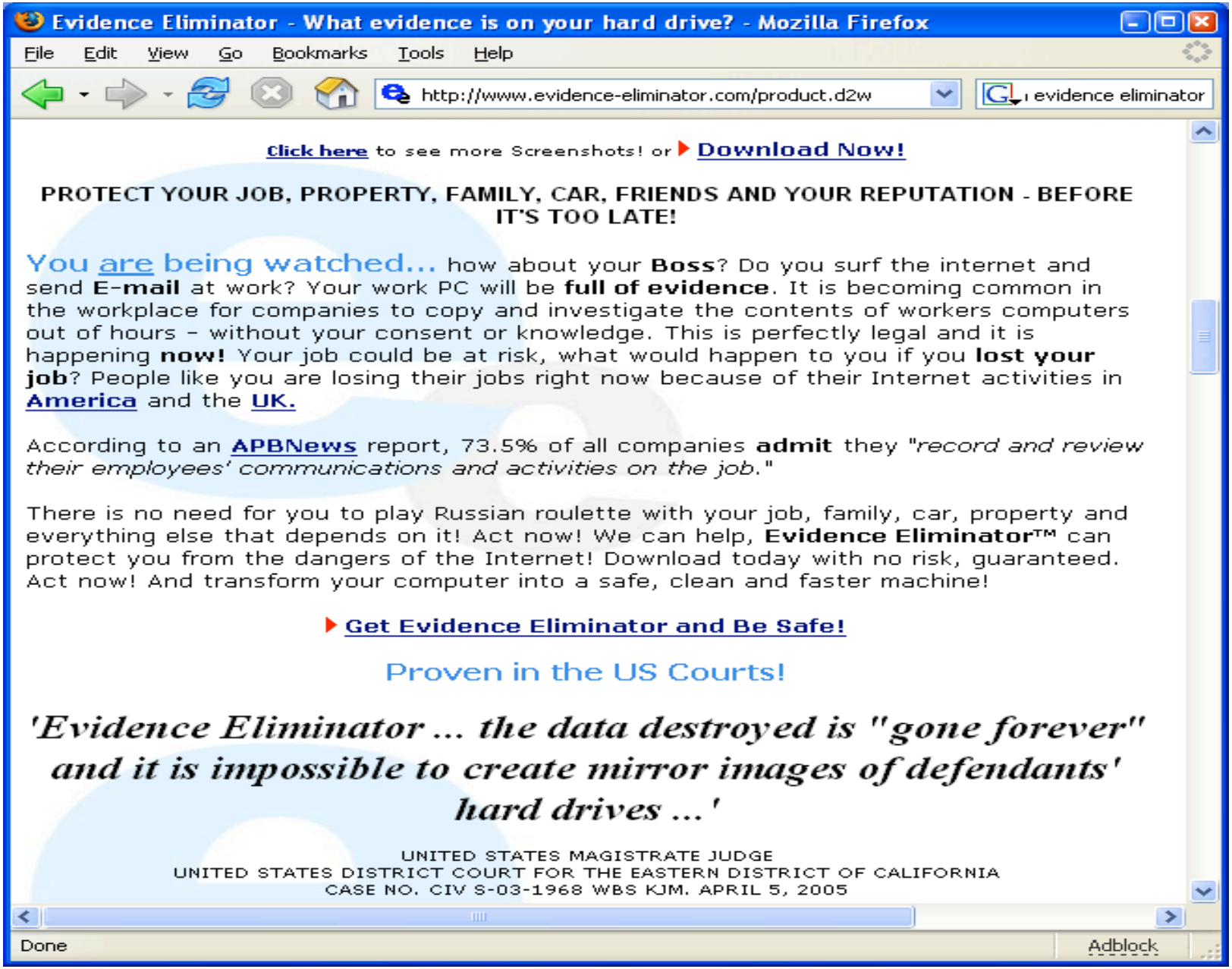
The vendor marketplace:

- Competitive

- Wide range of enterprises
  - Unincorporated entities
  - Well-financed companies

- Marketed as:
  - Safeguarding privacy
  - Protecting corporate data
  - Helping avoid consequences

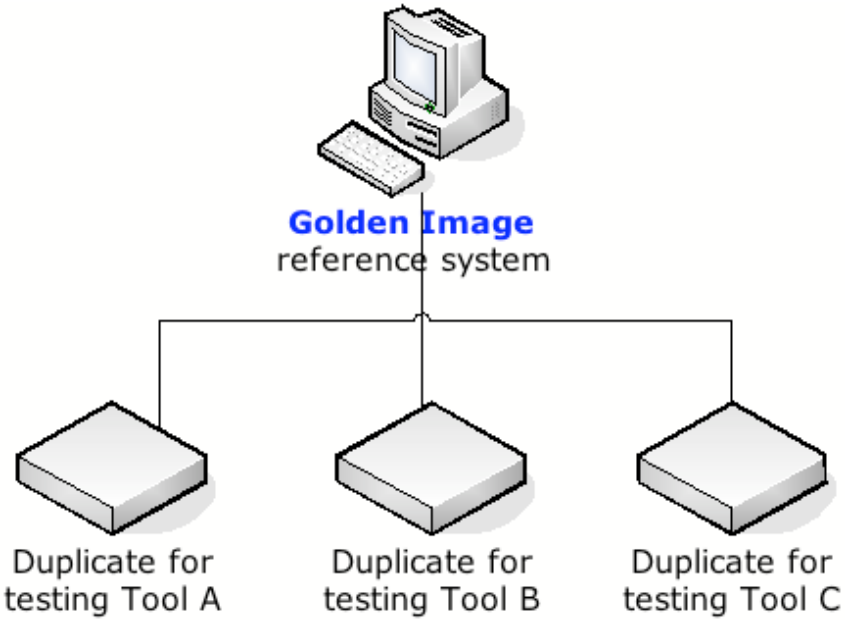



Evidence Eliminator - What evidence is on your hard drive? - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.evidence-eliminator.com/product.d2w
evidence eliminator
Click here to see more Screenshots! or Download Now!
PROTECT YOUR JOB, PROPERTY, FAMILY, CAR, FRIENDS AND YOUR REPUTATION - 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
Done
Adblock

Legal Trends

- Counter-forensic tools increasingly reported as factors in legal action
- 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



- Six software packages:
  - **Cyberscrub**
  - **Window Washer**
  - **SecureClean**
  - **Evidence Eliminator**
  - **Windows & Internet Cleaner**
  - **Acronis Privacy Expert**
- Reference system created – Windows XP Pro
- Typical user activity generated
- Bitstream image of test system duplicated as starting point for each tool test

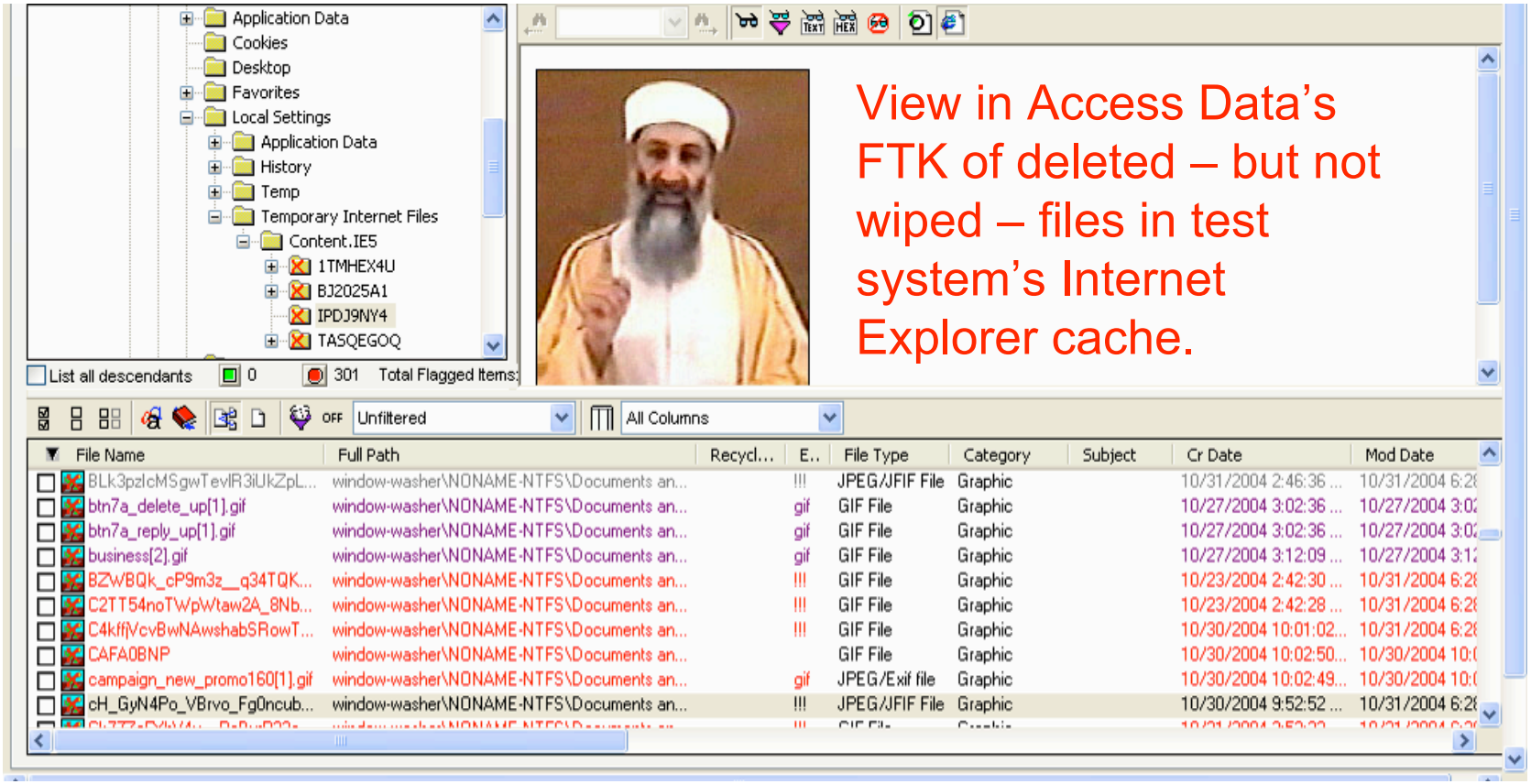
Design Goals

- **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
- First test version of *Window Washer* left almost everything recoverable
- 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://www.washingtonpost.com/wp-dyn/articles/A9659-2004Oct29_2.html
User name	Anon Nym
Page title	Bin Laden Warns U.S. Voters (washingtonpost.com)
Last Accessed (UTC)	10/30/2004 7:05:26 PM
Last Modified (UTC)	10/30/2004 7:05:26 PM
Last Checked (UTC)	10/30/2004 7:05:28 PM
Expires (UTC)	11/8/2004 7:05:28 PM
Hits	2
Use Count	0

Acronis Privacy Expert

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

Filename	Dc17.txt
Original Name	C:\Documents and Settings\Anon Nym\My Documents\Copy (27) of secret.txt
Date Recycled	10/23/2004 2:31:40 PM
Removed from Bin	Yes

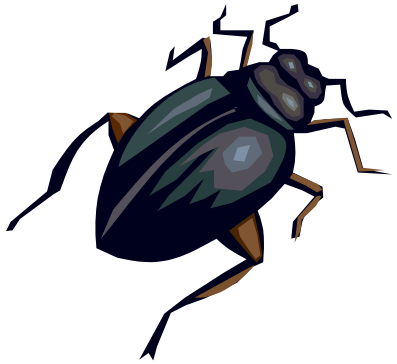
Filename	Dc18.doc
Original Name	C:\Documents and Settings\Anon Nym\My Documents\Copy (2) of secret document.doc
Date Recycled	10/26/2004 3:31:25 PM
Removed from Bin	Yes

Other Examples

- Several tools missed:
  - Outlook Express e-mail selected for deletion
  - Scattered files in IE cache, or IE history / cache index
- Two tools incompletely wiped unallocated space
- Test user data was left in pagefile by a few tools

Buggy Software

- Several tools have *serious functional flaws*
- Shortfalls in QA and testing
  - Relevant to the next class 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

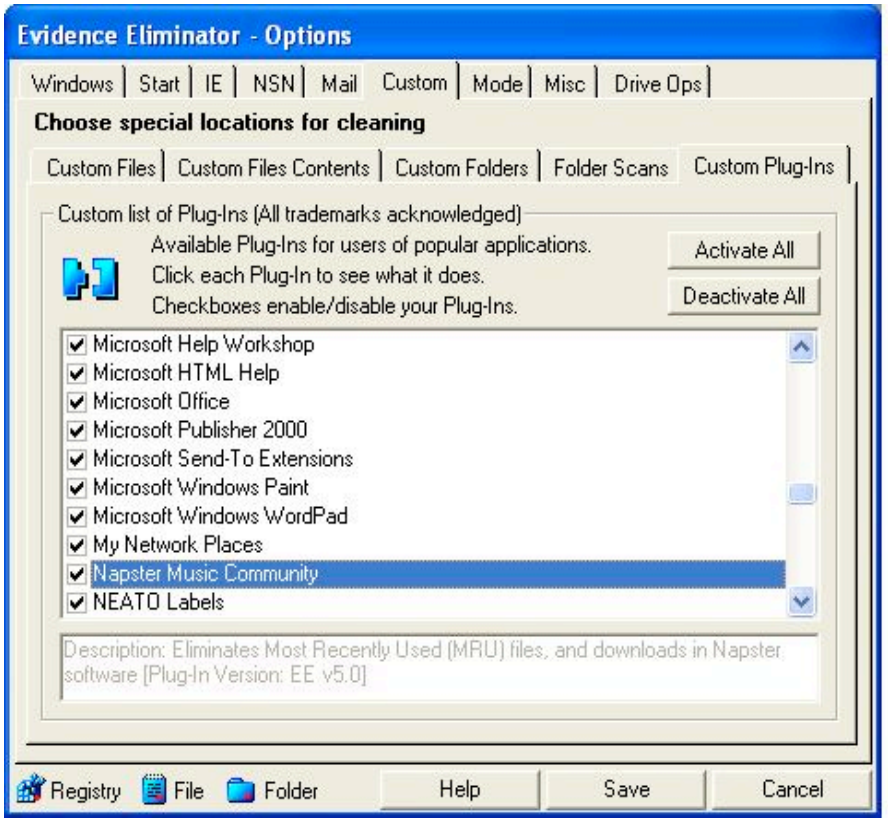
Complexity Failures

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

- Challenge of locating & deleting usage records rises with the number of applications covered
- But programs, including operating systems, are continually evolving
- And 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



Examples of "Complexity" Failures

- Tools failed when the location and/or format of user data was changed
  - For example, Evidence Eliminator's Napster plug-in missed activity files created by Napster Light
  - Many of the tools don't report the version of the application they have been designed to handle
- All but two tested tools missed copies of the registry preserved in Windows restore points, a feature new in XP

More Examples: Prefetch Folder

- Windows prefetch folder was also commonly overlooked – only Evidence Eliminator wiped this area
- Layout.ini and/or NTOSBOOT-BOODFAAD.pf files disclosed path structure, file names of deleted material

From Layout.ini file:

C:\WINDOWS\SYSTEM32\DRIVERS\PARVDM.SYSC:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTSC:\WINDOWS\FONTS\FRAMD.TTF
C:\DOCUMENTS AND SETTINGS\ANON NYM\RECENT\WORLD DOMINATION DATABASE.LNK
C:\DOCUMENTS AND SETTINGS\ANON NYM\RECENT\SECRET DOCUMENT.LNK
C:\DOCUMENTS AND SETTINGS\ANON NYM\RECENT\SUPER PRIVATE.LNK
C:\DOCUMENTS AND SETTINGS\ANON NYM\RECENT\PARTIAL SECRETS.LNK
C:\DOCUMENTS AND SETTINGS\ANON NYM\RECENT\PRIVACY REPORT.LNK
C:\DOCUMENTS AND SETTINGS\ANON NYM\RECENT\300X250_1.LNK
C:\DOCUMENTS AND SETTINGS\ANON NYM\RECENT\WIRED 12_05 THE KINGMAKER.LNK

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 common fingerprint is the way a tool renames files
- Action designed to replace file name, other metadata
- None of the tools tested duplicated another's scheme

Window Washer 1	Targeted files renamed with scrambled characters. But all assigned the same 3-character file extension of exclamation marks. Example: 8wVia7S2B39_nX_Xl9Xfw1DhrhS_Da_j.!!!
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.

Implications

- The tested commercial counter-forensic tools leave potentially useful data
- Don’t underestimate their ability to destroy data and present a significant obstacle
- Research such as this can help:
  - understand the behavior of these tools
  - identify and interpret the records a tool misses

Future Work

- Extend testing to similar counter-forensic tools and other versions of tested tools
- Expand the catalog of operational signatures and functional weaknesses
- How about a tool to automate the signature discovery process ?

Thanks