Preliminary Slides

- These are rough rough drafts of my final slides
- The most up-to-date version that was used at DEFCON20 will be posted online

Anti-Forensics and Anti-Anti-Forensics

by Michael Perklin

(But not Anti-Anti-Anti-Forensics)

...or Uncle-Forensics...

Anti-Forensic Techniques and Countermeasures

by Michael Perklin

DEFCON 20 - Friday July 27

Outline

- Techniques that can complicate digital-forensic examinations
- Methodologies to mitigate these techniques
- Open discussion on digital complications

Michael Perklin

- Digital Forensic Examiner
- Corporate Investigator
- Computer Programmer
- eDiscovery Consultant

- Basically - A computer geek + legal support hybrid

Typical Methodologies:

- Copy First, Ask Questions Later; or
- Assess relevance first, copy if necessary; or
- Remote analysis of live system, copy targeted evidence only

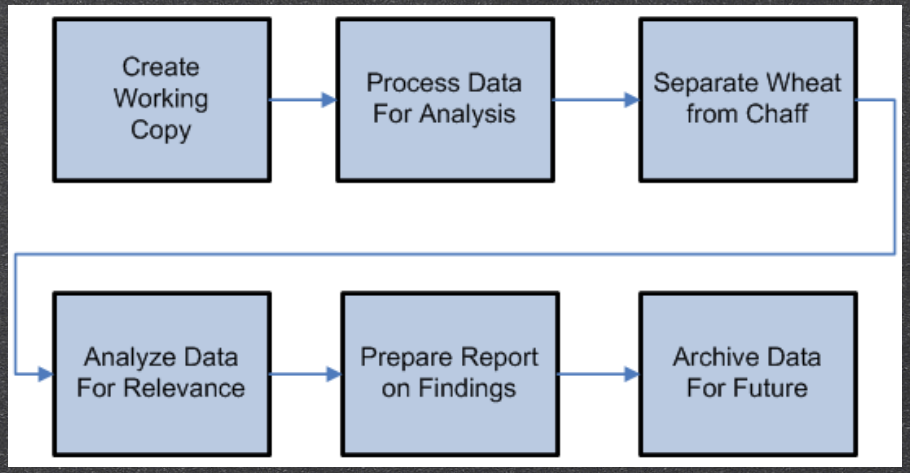
The approach of Private Firms

- Copy everything; leave originals with the client
  - (unless repossession is part of the job)
- Have to respect the property of custodians

The approach of Public Agencies

- “Gung Ho”
- Seize everything that may be relevant
- Copy everything when safely in their lab on their own time
- Less pressure to return items
- Typically longer turnaround times

Typical Workflow



Create Working Copy
- Image the HDD
- Copy files remotely for analysis

Process Data
- Hash files
- Analyze Signatures

Separate Wheat
- De-NIST or De-NSRL
- Known File Filter (KFF)
- Keyword Searches

Analyze For Relevance
- Good hits or false positives?
- Look at photos, read documents, analyze spreadsheets
- Export files for native analysis
- Bookmark, Flag, or otherwise list useful things

Prepare Report
- Include thumbnails, snapshots, or snippets
- Write-up procedures (Copy/Paste from similar case to speed up workload)
- Attach appendices, lists, etc

Archive Data
- Store images on central NAS
- Shelve HDDs for future use

#1. Create a Working Copy

Confounding the first stage of the process

AF Technique #1
Data Saturation

- Let's start simple
  - Own a LOT of media
  - Stop throwing out devices
  - Use each device/container for a small piece of your crimes
- Investigators will need to go through everything

Mitigating Data Saturation

- Parallelize the acquisition process
  - Multiple Acquisition machines (limit is your budget)
  - Write-Blocking Linux Boot Disks can use their hardware to your advantage.
    (limit is # of suspect devices, which could equal the #targets)

AF Technique #2
Non-Standard RAID

- Common RAIDs share stripe patterns, block sizes, and other parameters
- This hack is simple:
  Use uncommon settings!
- Use uncommon hardware RAID controllers (HP Smart Array P420)
- Use firmware with poor Linux support.
  Don’t flash that BIOS!

Non-standard RAID controllers sometimes allow you to choose arbitrary blocksizes (not 128 or 256, but how about 287?)
This can force an examiner to take a logical copy using seized hardware

Less damaging for Public sector, can be very expensive for Private sector

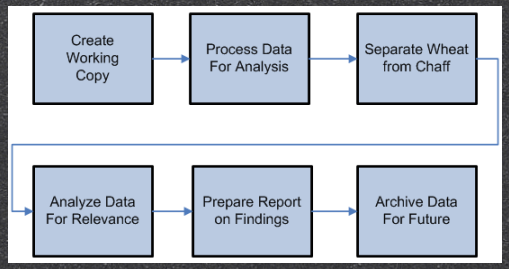
- [Diagram/screenshot of improperly-reassembled stripes]
- Odd or Even?
- 1, 2, 3, 4?
- 2, 4, 1, 3?
- Little Endian or Big Endian?

Mitigating Non-Standard RAIDs

- De-RAID volumes on their own system
  - Use boot discs
  - Their hardware reassembles it for you!
  - If it doesn't support Linux, use Windows! Windows-Live CD!
  - Image the volume, not the HDDs

#2. Process Data for Analysis

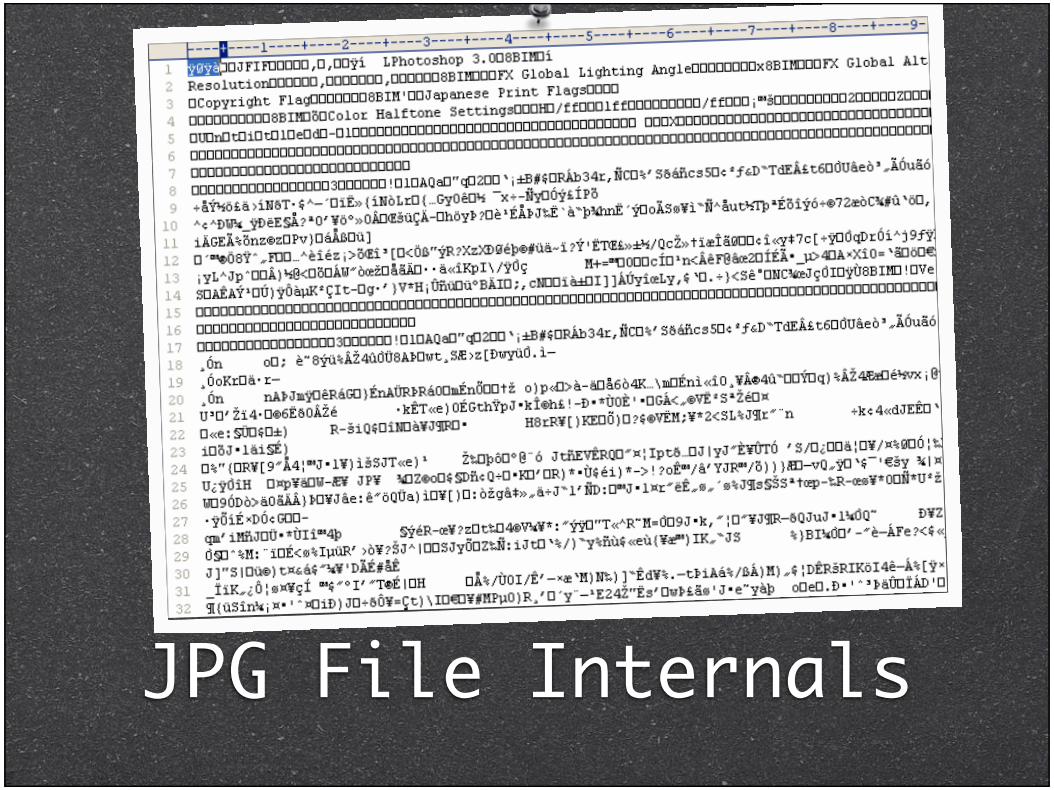
Confounding the processing stage



AF Technique #3
File Signature Masking

- File Signatures are identified by file headers/footers
- “Hollow Out” a file and store your crime inside
- Encode data and paste in middle of a binary file

MZ for EXEs
PDF for PDFs
PK for Zips

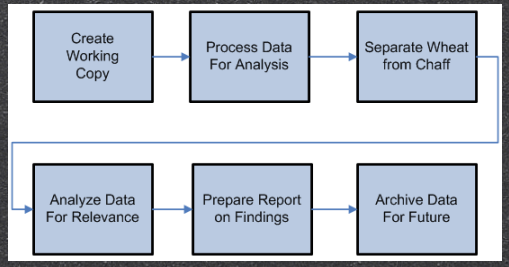

JPG File Internals

Mitigating File Signature Masking

- Use “Fuzzy Hashing” to identify potentially interesting files
  - FTK supports this out-of-the-box
- Analyze all “Recent” lists of common apps for curious entries

#3. Separate Wheat from Chaff

Confounding the sifting process



Talk about NRSL, date filtering, deduplication and other sifting/culling techniques

Background: NSRL

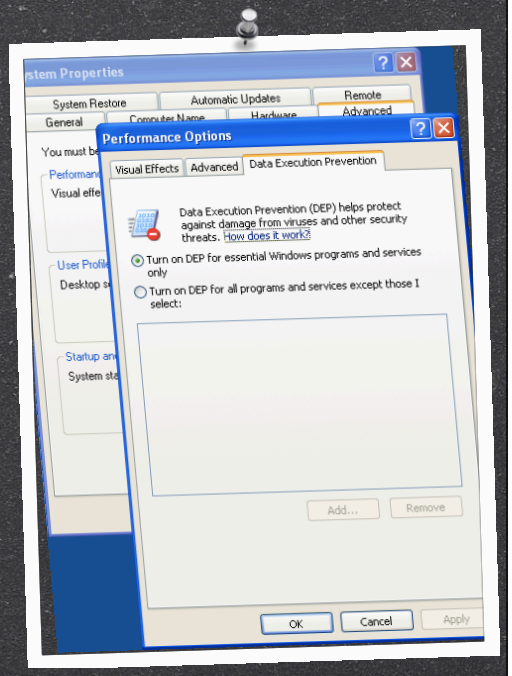
- National Software Reference Library
- Huge databases of hash values
- They strive for complete coverage of all commercially available software
- Every dll, exe, hlp, pdf, dat file installed by every commercial installer
- Used by investigators to filter “typical” stuff

AF Technique #4
Rendering NSRL Useless

- Modify all system and program files
  - Modify a string in the file
  - Recalculate and update the embedded CRCs
- Turn off Data Execution Prevention (DEP)
- NSRL will no longer match anything

Data Execution Prevention

Validates system files
Stops unsafe code
Protects integrity



Mitigating Rendering NSRL Useless

- Search, don't filter
- Identify useful files rather than eliminating useless files (i.e. Whitelist approach vs Blacklist)

AF Technique #5
Scrambled MAC Times

- All files store multiple timestamps
  - Modified - the last write
    Accessed - the last read
    Created - the file's birthday 
- Randomize every timestamp (ie Timestomp)
- Disable time updates in registry
- Randomize BIOS time regularly

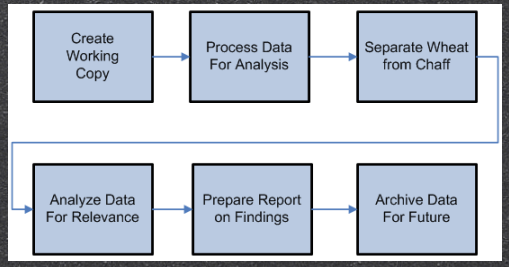
Mitigating Scrambled MAC Times

- Ignore dates on all metadata
- Look for dates within files themselves
- Identify sets of similar times
  - Infer mini timelines for each set
- Use deduction to order sets chronologically

- [Histogram]

#4. Analyze Data

Confounding file analysis



Sometimes files can't be analyzed completely inside FTK/Encase/tool
Files are commonly exported to a temporary folder for external analysis with other tools
Badguy files exist on the analysis machine natively instead of isolated within an image

This can cause problems, and not just the obvious problems with viruses...

AF Technique #6
Restricted Filenames

- Even Windows 7 still has holdovers from DOS days: Restricted filenames
  - CON
    PRN
    AUX
    NUL
    COM#
    LPT#
- Use these filenames liberally

Mitigating Restricted Filenames

- Never export files with native filenames
  - Always specify a different name
  - FTK does this by default (1.jpg)
- Export by FileID or autogen'd name

AF Technique #7
Circular References

- Folders in folders have typical limit of 255 characters on NTFS
- “Symbolic Links” or “Junctions” can point to a parent
- C:\Parent\Child\Parent\Child....
- Store criminal data in multiple nested files/folders

Circular References

- Many tools that recursively scan folders are affected by this attack
- Some tools don’t bat an eye (FTK4)

Mitigating Circular References

- Do not export folders for analysis
  - Only export files themselves
- “Flatten” the export of all nested files into one common folder

AF Technique #8
Use Lotus Notes

- NSF files and their .id files always give problems
- There are many tools to deal with NSFs
  - Every one of them has its own problems

Lotus Notes

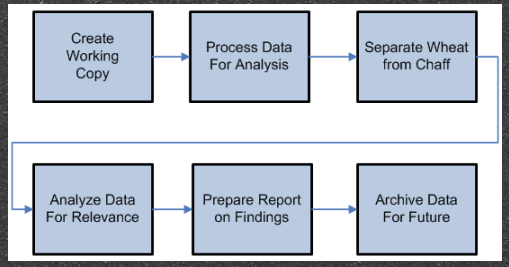
- [Diagram comparing notes dll use]
- Most apps that support .NSF files use the same IBM Lotus Notes dll
- If anyone knows how to use their API, it's IBM themselves

Mitigating Lotus Notes

- Train yourself on Lotus Notes itself
- Do not rely on NSF conversion tools
- Lotus Notes is the best NSF parser but has its quirks
- Once you know the quirks you can navigate around them

#5. Report Your Findings

Confounding the reporting process



AF Technique #9
HASH Collisions

- MD5 and SHA1 hashes are used to identify files in reports
- Add dummy data to your criminal files so its MD5 hash matches known good files
- Searches for files by hash will yield unexpected results

Hash Collisions

- Of course, this would only be useful in a select few cases:
  - i.e. you stole company data and stored on a volume they could seize/search

Mitigating HASH Collisions

- Use a hash function with fewer collisions (SHA1, SHA256, Whirlpool)
- Doublecheck your findings by opening each matched file to verify the search was REALLY a success
  - boy would your face be red!

AF Technique #10
Dummy HDD

- Have a PC with an HDD that isn't used
- USB-boot and ignore the HDD for everyday use
- Store work on cloud/remote machine
- Manually connect to address each day
- Automate dummy writes to local HDD to simulate regular usage

Mitigating Dummy HDDs

- Always check for USB drives
  They can be SMALL these days...
- Pagefile on USB drive may point to network locations (if the OS was paging at all...)
- If possible, monitor network traffic before seizure to detect remote drive location

Questions

- Have you encountered frustration in your examinations?
- How did you deal with it?
- I’d love to hear about it in the speaker room!

Thanks!

- Thanks DEFCON for letting me speak
- Thanks:
  - Forensic Friends (Josh, Joel, Nick)
  - Dad, Brother, Sister
  - Coworkers
  - You!