

ANTI-FORENSICS

Or as I like to call it, Occult Computing

Adrian Crenshaw



About Adrian

- ▣ I run Irongeek.com
- ▣ I have an interest in InfoSec education
- ▣ I don't know everything - I'm just a geek with time on my hands



Why Occult Computing?

- ▣ Occult comes from the Latin word *occultus* (clandestine, hidden, secret), referring to "knowledge of the hidden".
- ▣ Forensic: Relating to the use of science and technology in the investigation and establishment of facts or evidence in a court of law.
- ▣ Since hiding activities is what we are doing, Occult Computing seems like a good name.
- ▣ Since people are not necessarily hiding their activities from a court of law, the term anti-forensics may not apply.
- ▣ Occult Computing sounds cooler than Anti-forensics ☺
Cthulhu fhtagn



What's this class about?

Why:

- ▣ Not about just hiding your stash from the Fuzz...
- ▣ Law/policy enforcement may find it useful to know how folks hide their computer activities
- ▣ Users may want to know how to hide their activities from invasive law/policy enforcement
- ▣ Companies may want to know how to clear boxes before donating them

What:

- ▣ Mostly Windows, but most ideas are applicable to other operating systems
- ▣ Not going to cover malware analysis, nor network anti-forensics (at least not much)
- ▣ Mostly we will cover hiding tracks left on storage media



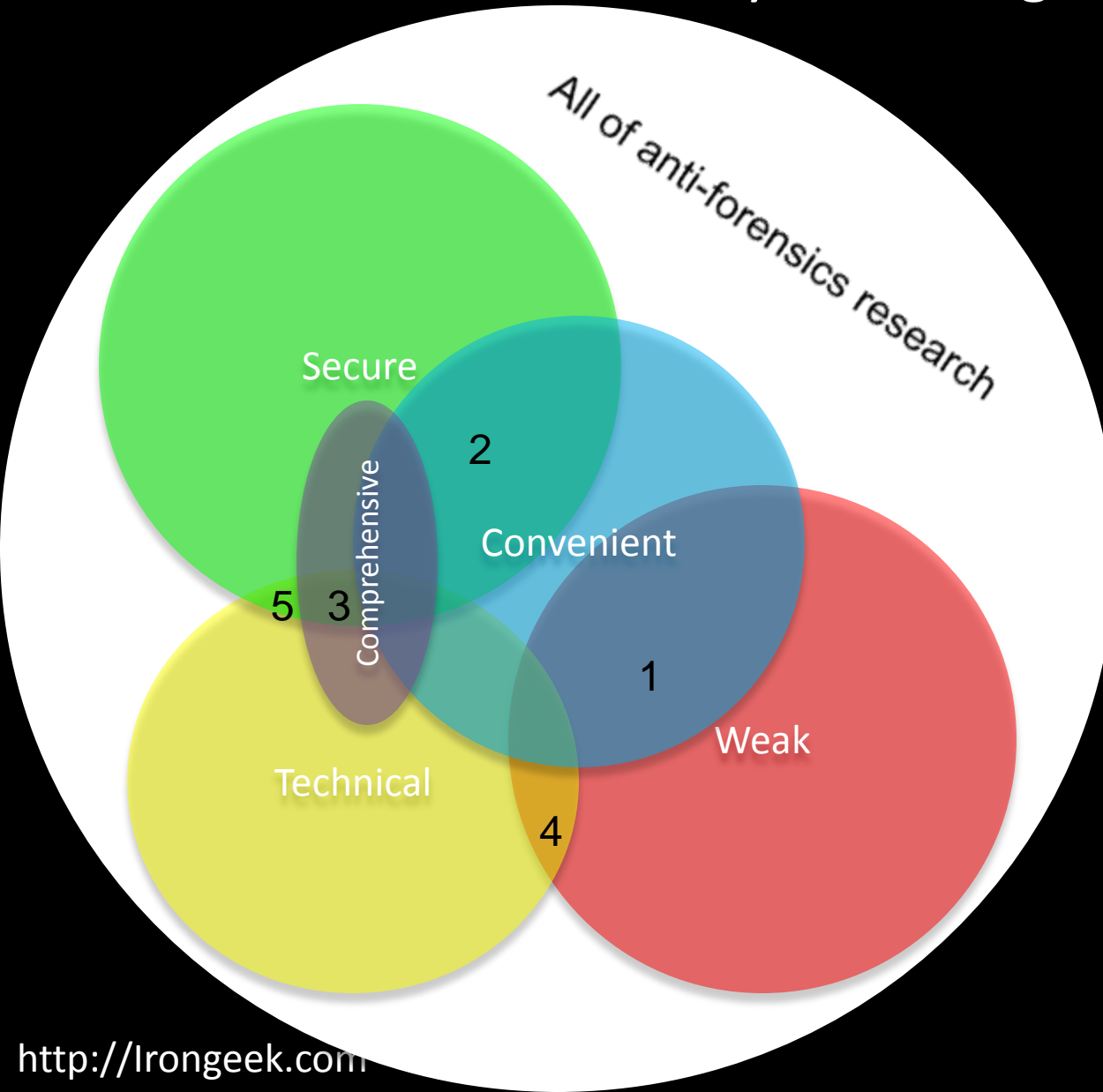
Four categories

1. Don't leave tracks in the first place
2. Selective file removal and encryption tools
3. Parlor Tricks
4. Nuke it from orbit, it's the only way to be sure



What anti-forensic techniques are likely to be seen?

▣ Bow down before my Venn diagram of doom!!!



If it's not easy, folks won't do it.
If it's not secure there's no point in doing it.

1. Just deleting a file
2. Selective file wiping and encryption
3. Full drive wiping and encryption
4. Hidden partitions
5. Stego



BACKGROUND INFO

Stuff that's useful to know



Interesting legal stuff

IANAL

- ▣ Julie Amero
http://en.wikipedia.org/wiki/State_of_Connecticut_v._Julie_Amero
<http://www.securityfocus.com/columnists/434/>
- ▣ Sebastien Boucher
http://en.wikipedia.org/wiki/United_States_v._Boucher
- ▣ The “Hacker Defense”
http://www.forensicswiki.org/wiki/Legal_issues
<http://exforensis.blogspot.com/2008/07/trojan-horse-defense.html>
- ▣ If the system is set to wipe data at regular intervals normally, that may be ok. Wiping data once an investigation is about to be underway will make things worse.
- ▣ Spoliation: Someone screwed up the evidence
- ▣ CSI effect
http://en.wikipedia.org/wiki/CSI_effect
- ▣ Plausible Deniability Tool Kit (PDTK)
<http://www.nmrc.org/pub/pdtk/>
<http://www.defcon.org/html/links/dc-archives/dc-14-archive.html#weasel>



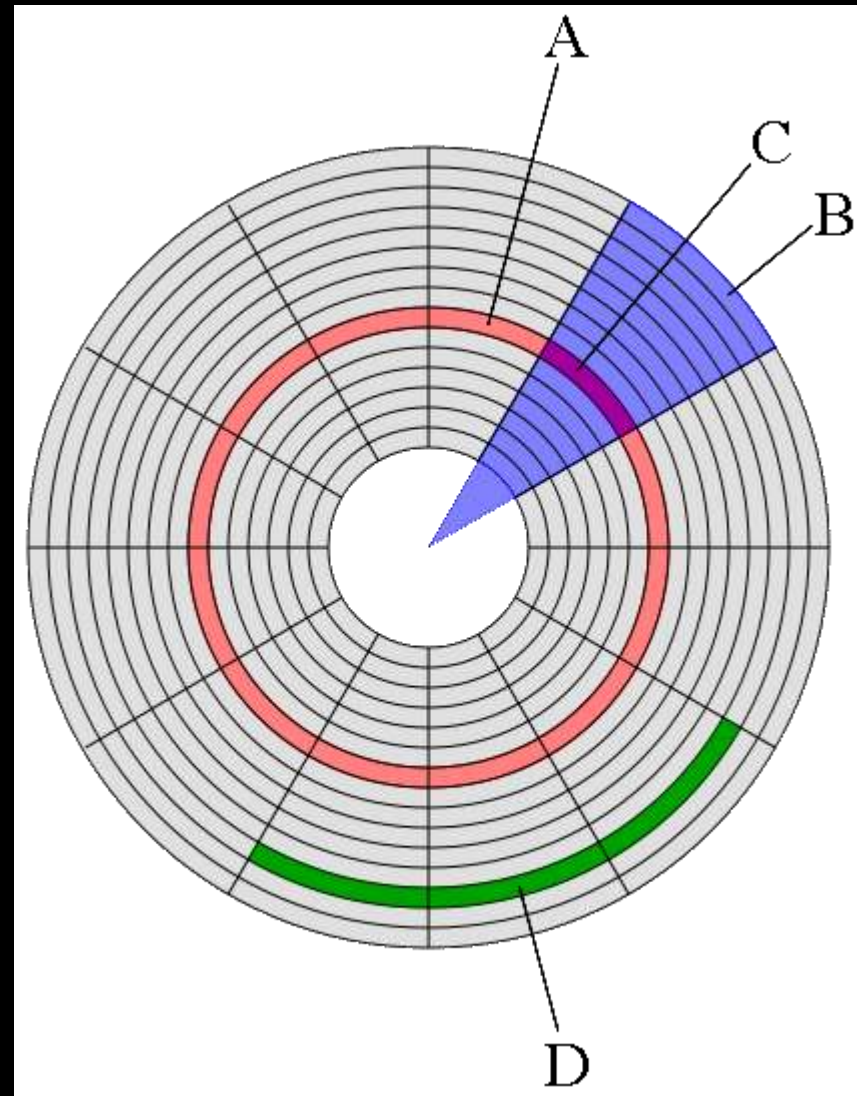
Tech Stuff

- ▣ It's hard to cover this in order.
- ▣ You need to understand some things before you understand others, but which you have to understand first is questionable.
- ▣ Windows jams data in all sorts of places, and there are tools to make this data fairly easy to recover.



Disks, Tracks, Sectors

- ▣ A. Track
- ▣ B. Geometric Sector
- ▣ C. Track Sector
- ▣ D. Cluster



Slack Space

▣ Yum...Leftovers!!!

▣ RAM slack (but name no longer really applies) and Residual slack

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
04049E70	32	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	2FILE2FILE2FILE2
04049E80	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	FILE2FILE2FILE2F
04049E90	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	49	ILE2FILE2FILE2FI
04049EA0	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	LE2FILE2FILE2FIL
04049EB0	45	32	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	E2FILE2FILE2FILE
04049EC0	32	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	2FILE2FILE2FILE2
04049ED0	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	FILE2FILE2FILE2F
04049EE0	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	49	ILE2FILE2FILE2FI
04049EF0	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	LE2FILE2FILE2FIL
04049F00	45	32	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	E2FILE2FILE2FILE
04049F10	32	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	2FILE2FILE2FILE2
04049F20	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	FILE2FILE2FILE2F
04049F30	49	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	49	ILE2FILE2FILE2FI
04049F40	4C	45	32	46	49	4C	45	32	46	49	4C	45	32	46	49	4C	LE2FILE2FILE2FIL
04049F50	45	32	46	49	4C	45	32	00	00	00	00	00	00	00	00	00	E2FILE2
04049F60	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049F70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049F80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049F90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049FA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049FB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049FC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049FD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049FE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
04049FF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0404A000	65	31	66	69	6C	65	31	66	69	6C	65	31	66	69	6C	65	e1file1file1file1
0404A010	31	66	69	6C	65	31	66	69	6C	65	31	66	69	6C	65	31	1file1file1file1



Hash

One way functions:

Easy:

```
md5("I am a string") =  
    "1710528bf976601a5d203cbc289e1a76"
```

Hard:

```
String("1710528bf976601a5d203cbc289e1a76") =  
("I am a string")
```

Can be used to fingerprint files, or see if they have
changed



Host-Protected Areas and Disk Configuration Overlay

- ▣ Parts of the drive that can be set aside that normal OS and BIOS functions can't see
- ▣ Possible to hide data there, but it's a pain
- ▣ Taft (he's one bad mother....)
<http://www.vidstrom.net/stools/taft/>
- ▣ More info
[http://www.forensicswiki.org/wiki/DCO and HPA](http://www.forensicswiki.org/wiki/DCO_and_HPA)



Forensically interesting areas in the Windows file system

- ▣ Way too many to list, but lets check some out:

<http://www.irongeek.com/i.php?page=security/windows-forensics-registry-and-file-system-spots>

- ▣ Nirsoft has a lot of tools for grabbing data:

<http://www.nirsoft.net/>

- ▣ Deft Linux

<http://www.deftlinux.net/>



DON'T LEAVE TRACKS IN THE FIRST PLACE

Pr0n mode and places data hides



Privacy mode (aka porn mode) in browsers



Firefox (Private Browsing)

- Keyboard shortcut: Ctrl+Shift+P
- Command line: No command line, but can be set on start via Tools>Options>Privacy "Use custom setting"



IE (InPrivate)

- Keyboard shortcut: Ctrl+Shift+P
- Command line: -private



Chrome (Incognito mode)

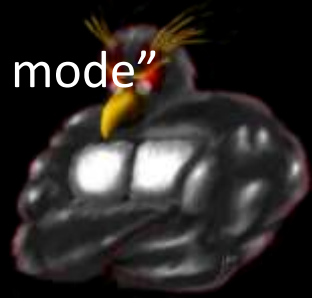
- Keyboard shortcut: Ctrl+Shift+N
- Command line: --incognito



Opera (kiosk mode)

- Ok, not quite the same thing, but maybe someone will email me a solution

- ☐ Do some research online to see how good your browser's "porn mode" really is.



Private portable browsers

- ▣ Portable Apps
<http://portableapps.com/apps/internet>
- ▣ Tor Browser Bundle
<http://www.torproject.org/easy-download.html.en>
Firefox based, comes with Tor and Pidgin
- ▣ OperaTor
<http://archetwist.com/opera/operator>
Opera based, comes with Tor
- ▣ Keep in mind, Tor != Secure



Boot media

Linux:

- ▣ Knoppix
<http://www.knoppix.net/>
- ▣ Ubuntu
<http://www.ubuntu.com/>
- ▣ Unetbootin
<http://unetbootin.sourceforge.net/>

And so many more... Look up the noswap option

Windows:

- ▣ Bart PE
<http://www.nu2.nu/pebuilder/>
- ▣ Ultimate Boot CD for Windows
<http://www.ubcd4win.com/>
- ▣ WinBuilder
<http://winbuilder.net/>



SELECTIVE FILE REMOVAL AND ENCRYPTION

For those that don't want to go all the way



Links to automated selective wiping tools

- ▣ Clean After Me

http://www.nirsoft.net/utils/clean_after_me.html

- ▣ CCleaner

<http://www.ccleaner.com/>

- ▣ And many more....



Tools for selective file wiping

- ▣ DD

`dd if=/dev/zero of=f:\Notes.docx bs=12940 count=1`

I like this Windows version:

<http://www.chrysocome.net/dd>

- ▣ Sdelete

<http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>

- ▣ Eraser

<http://eraser.heidi.ie/>

- ▣ *nix guys, look into Shred

[http://en.wikipedia.org/wiki/Shred %28Unix%29](http://en.wikipedia.org/wiki/Shred_%28Unix%29)



Just slack and unused space

- ▣ Eraser
- ▣ Cipher that comes with Windows as a command line EFS tool

Run once:

cipher /w:g:

Schedule script:

```
REM at 2:00 /every:m,t,w,th,f,s,su c:\defragandcipher.bat
```

```
defrag c: /f
```

```
defrag c: /f
```

```
defrag c: /f
```

```
cipher /w:c:\
```



Selective File Encryption

- ▣ EFS

- [http://en.wikipedia.org/wiki/Encrypting File System](http://en.wikipedia.org/wiki/Encrypting_File_System)

- Hash insertion does not help (Pnordahl)
 - Can read file names
 - Best to use a SYSKEY password or boot key

- ▣ TrueCrypt

- <http://www.truecrypt.org/>

- <http://sourceforge.net/projects/tcexplorer/>

- ▣ FreeOTFE

- <http://www.freeotfe.org/>

- ▣ Good encryption does not compress much



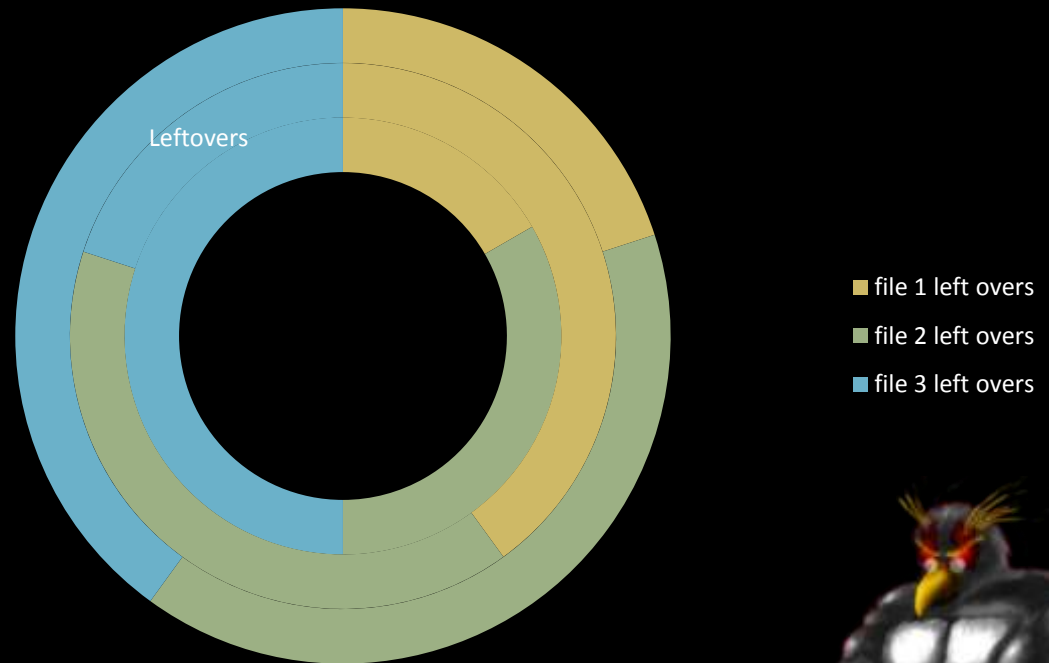
Reasons why relying on selective file wiping is not a good idea

- ▣ Windows jams data in all sorts of places, it's hard to get them all
- ▣ You got the main file, but what about the temp?
- ▣ Defrag, moving files and abandoned clusters
- ▣ USB device logs
- ▣ Page and hibernation files
- ▣ Data carving ☺



Defrag issues

- ▣ You defrag a drive
- ▣ You wipe a file on that drive
- ▣ What about the remnants of the file from before the defrag?



USB device log

- ▣ Ah, so the suspect has a camera/thumbdrive/iPod/etc
- ▣ USBDevice
http://www.nirsoft.net/utils/usb_devices_view.html
- ▣ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB
- ▣ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
- ▣ Search for “USBSTOR” in c:\windows\inf\setupapi.dev.log



Page file

- ▣ File used for swapping memory:
`pagefile.sys`

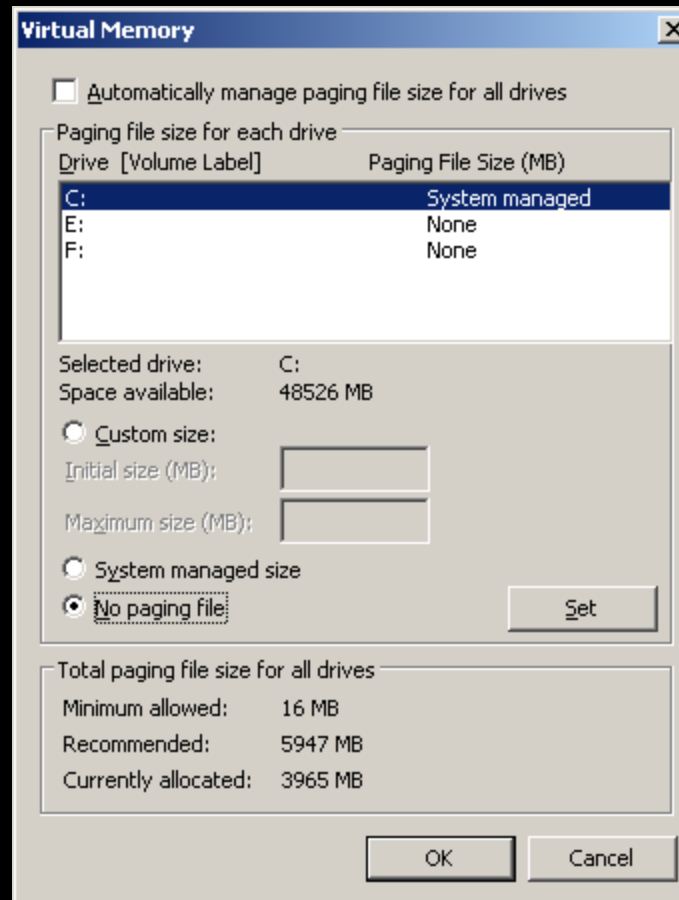
- ▣ Linux folks, investigate swap



Disable page file

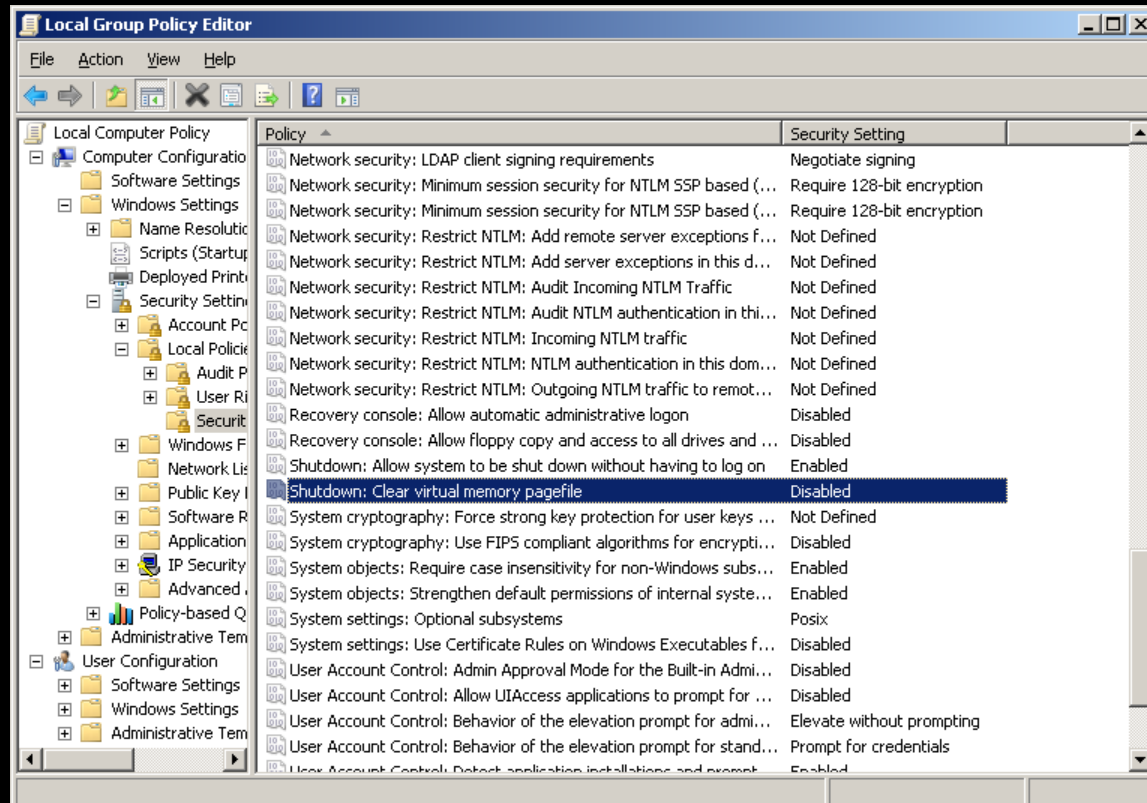
▣ Disable:

Control Panel->System and Security->System->Advanced System Settings->Performance->Advanced->Virtual Memory->Change



Wipe page file

- ▣ Set
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Control\Session Manager\Memory Management\
ClearPageFileAtShutdown to 1



Hibernation file

- ▣ File used for storing active memory when going into hibernation mode:

[hiberfil.sys](#)

Go into power setting to disable



Data carving

- Go down the drive bit by bit looking for file headers

```
C:\Users\adrian\Desktop\testdisk-6.11.3\win\photorec_win.exe
PhotoRec 6.11.3. Data Recovery Utility, May 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 160 GB / 149 GiB (RO) - ST3160815AS
Disk /dev/sdb - 160 GB / 149 GiB (RO) - WDC WD1600AAJS-75M0A0
Disk /dev/sdc - 129 MB / 123 MiB (RO) - LEXAR JUMPDRIVE

[Proceed ] [ Quit ]          Quit program

Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
```



- DiskDigger
<http://dmitrybrant.com/diskdigger>
- Photorec
<http://www.cgsecurity.org/wiki/PhotoRec>
- Other file carving tools
http://www.forensicswiki.org/wiki/Tools:Data_Recovery#Carving
- File system compression makes file carving far less reliable!



So, what is writing where?

What needs to be wiped? What is this tool doing?

- ▣ Process Monitor

<http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx>

- ▣ RegFromApp

http://www.nirsoft.net/utils/reg_file_from_application.html

- ▣ ProcessActivityView

http://www.nirsoft.net/utils/process_activity_view.html



PARLOR TRICKS

Maybe useful sometimes, but mostly fluff



Tool/Solution Kiddies

- ▣ Does the examiner understand the concepts, or just the tool?
- ▣ Think back to the Julie Amero case
- ▣ What is their case load like?



Timestomp

- ▣ Making the chain of events hard to manage

<http://www.metasploit.com/research/projects/antiforensics/>

- m <date> M, set the "last written" time of the file
- a <date> A, set the "last accessed" time of the file
- c <date> C, set the "created" time of the file
- e <date> E, set the "mft entry modified" time of the file
- z <date> set all four attributes (MACE) of the file
- v show the UTC (non-local time) MACE values for file
- b sets the MACE timestamps so that EnCase shows blanks -r does the same recursively ,
Know as the Craig option

- ▣ For setting an arbitrary time recursively:

Command:

for /R c:\users\ %i in (*) do timestomp.exe %i -z "Monday 3/12/2099 10:00:00PM"



AltDS

- ▣ Alternate data streams

type mypr0n.jpg disney.jpg:hide

mspaint disney.jpg:hide

- ▣ Hit or miss with file carving
- ▣ Practical Guide to Alternative Data Streams in NTFS

<http://www.irongeek.com/i.php?page=security/altds>



Steganography

(Hiding stuff in stuff so people don't find your stuff)

- ▣ **With encryption, most times people know that some data is there, just not what it is.**
- ▣ **With Stego, they hopeful will not even know it's there.**
- ▣ Tacked on
`copy /B image.jpg+putty.zip test.jpg`
- ▣ Insertion

Example: Putting a file inside of a DOCX, it's just a ZIP file with some XML, just add you inserted file name into [Content_Types].xml so the DOCX does not report as corrupted.

- ▣ Additive

LSB (Least Significant Bit), for example making imperceptible changes to a format that can take loss and still be useful (audio, images, video).

Vecna

<http://www.uni-koblenz.de/~strauss/vecna/>



Lemonwipe (rude and crude)

Not recommended from a legal standpoint, but funny.

Repeat script to feed into DD:

```
@Echo Off
```

```
:TOP
```

```
type %1
```

```
Goto TOP
```

Command:

```
repeat.bat adrianbeer.jpg | dd of=\\.\f:
```

Create one big file:

```
@Echo Off
```

```
:TOP
```

```
type %1 >>%2\%1
```

```
if not %errorlevel%==0 goto :error
```

```
Goto TOP
```

```
:error
```

```
echo Exiting and deleting %2\%1
```

```
del %2\%1
```

```
exit /B -1
```

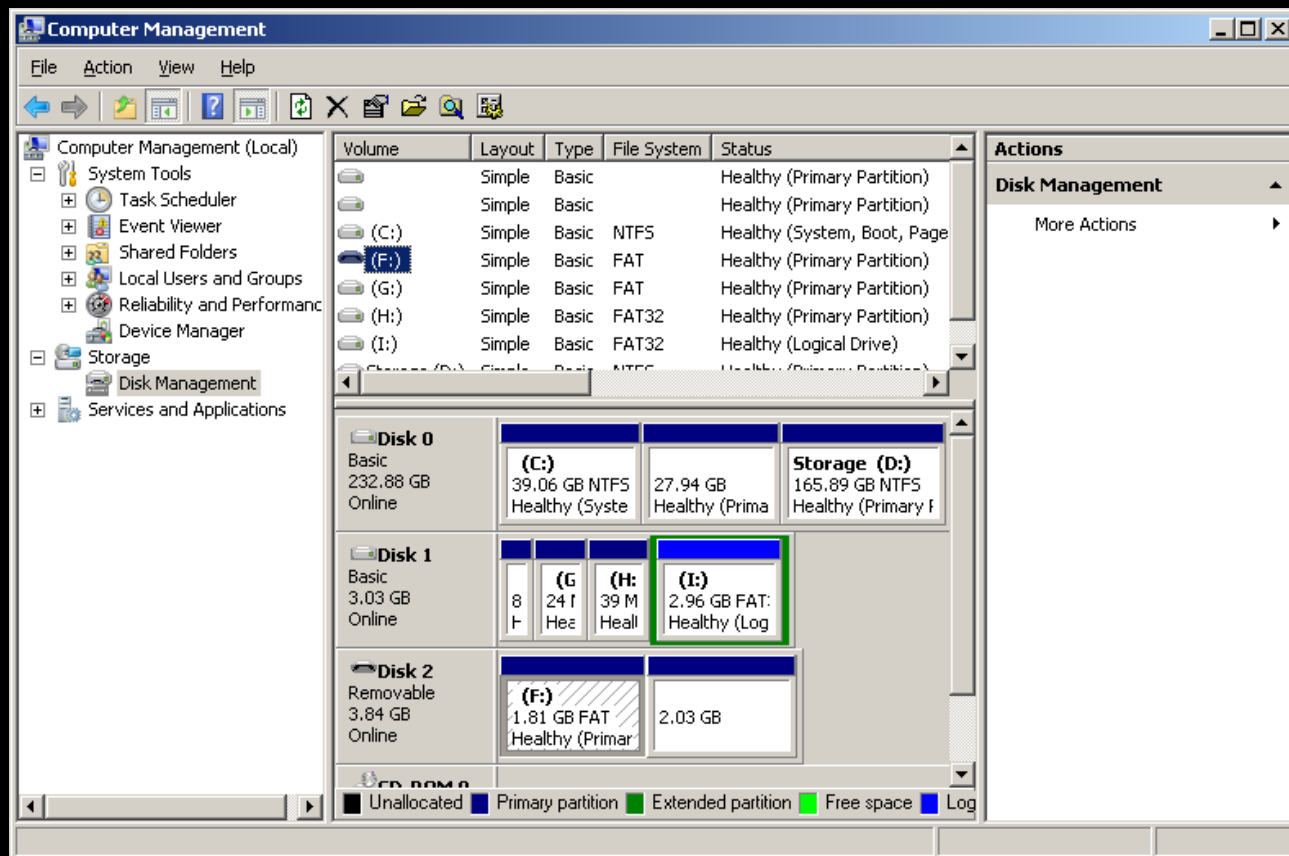
Command:

```
Smack.bat image.jpg f:
```



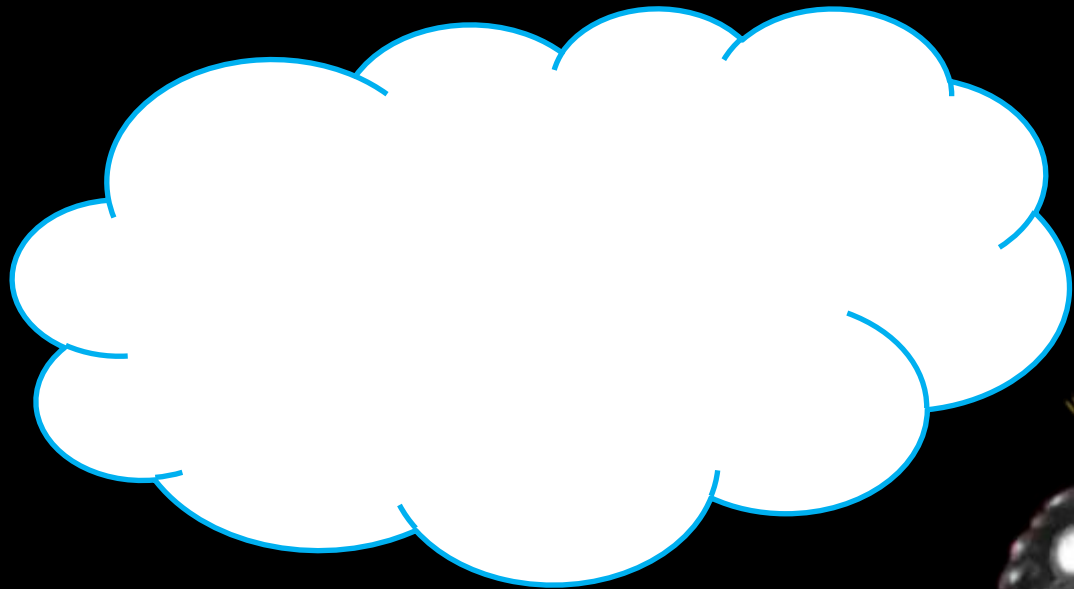
Two partitions on a thumbdrive

- Two partitions on a thumb drive? Windows sees one.



Cloud Computing?

- ▣ Use the browser's privacy mode, and SSL
- ▣ If it's not on the drive, they can't find it on the drive
- ▣ Less 4th amendment protection?
- ▣ Find a country that does not work well with US law enforcement



Attack the forensic software?

- ▣ XSS, not just for web forms anymore
<http://www.irongeek.com/i.php?page=security/xss-sql-and-command-inject-vectors>
- ▣ Breaking Forensics Software: Weaknesses in Critical Evidence Collection (Encase and Sleuth Kit)
ISEC Partners presentation at Defcon 15
<http://www.defcon.org/html/links/dc-archives/dc-15-archive.html#Palmer>
- ▣ 42.zip = 4.5 PetaBytes
<http://www.unforgettable.dk/>
http://en.wikipedia.org/wiki/Zip_bomb
- ▣ Two comments on these attacks:
 1. If the examiner sees the data attacking him, they will know something is up.
 2. Do you really think it's a good idea to piss off the forensic examiner?



Thermite

- ▣ <http://hackaday.com/2008/09/16/how-to-thermite-based-hard-drive-anti-forensic-destruction/>
- ▣ Uhm, just no.
- ▣ Destruction of evidence charges
- ▣ Fire hazard
- ▣ Just use full drive encryption
- ▣ While we are on that topic:
<http://www.youtube.com/watch?v=Bv5LHamqAsI>



A large, bright orange and yellow nuclear explosion with a prominent mushroom cloud, set against a dark, hazy background.

NUKE IT FROM ORBIT

It's the only way to be sure



Wipe Tools

- ▣ DD

```
dd if=/dev/zero of=\\.\f: --progress bs=1M
```

```
dd if=/dev/zero of=\\.\Volume{de891b6a-8432-11de-86d4-005056c00008} bs=1M --progress
```

- ▣ DBAN

<http://www.dban.org/>

- ▣ HDD Wipe Tool

<http://hddguru.com/content/en/software/2006.04.13-HDD-Wipe-Tool/>

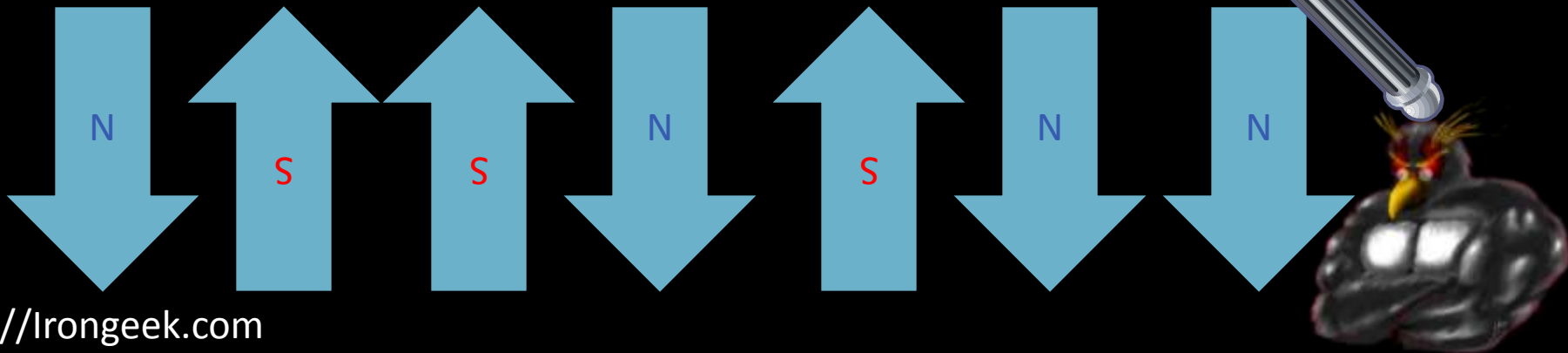


One wipe?

- ▣ Magnetic Force Microscopy

<http://sansforensics.wordpress.com/2009/01/15/overwriting-hard-drive-data/>

- ▣ On a pristine modern drive 92% chance to recover the correct previous bit , 56% on a used drive
- ▣ Probabilities multiply, so to get one byte:
 $.92^8 = 51\%$ (more or less)
- ▣ For 1 Kilobyte= $2.238e-297$



Enhanced Secure Erase

Not only is it faster, but it can wipe remapped blocks (bad sectors) from the G-LIST

- ▣ HDParm

http://ata.wiki.kernel.org/index.php/ATA_Secure_Erase

- ▣ MHDD

<http://hddguru.com/content/en/software/2005.10.02-MHDD/>

<http://hddguru.com/content/en/software/2006.02.10-Magic-Boot-Disk/>

- ▣ HDDEraser

<http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml>



Full System Drive Encryption

▣ BitLocker

<http://www.microsoft.com/windows/windows-vista/features/bitlocker.aspx>

- Built in to Windows Vista/7
- AES CBC
- Pain to setup in Vista
- Look into Bitlocker To Go to secure your USB drive
- To enable Bitlocker without TPM in Win 7, gpedit.msc > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Require Additional Authentication at Startup > Enable
- Bitlocker Modes:
 - TPM only
 - TPM + PIN
 - TPM + PIN + USB Key
 - TPM + USB Key
 - USB Key

▣ TrueCrypt

<http://www.truecrypt.org/>

- Open source
(for review of a lot of eyes)
- Read from other platforms
- Works on XP
- More cipher options
- Uses XTS which is better than CBC, but ask a cryptographer why

▣ Also, look into hardware based options

<http://www.enovatech.net/>



How about running a VM form an encrypted volume?

- ▣ Easy to do
- ▣ I have some concern about data leaking into swap/page file. This needs more testing.
- ▣ A few suggested tweaks:
MemAllowAutoScaleDown = "FALSE"
mainMem.useNamedFile = "FALSE"
- ▣ Use some of the page file wiping techniques mentioned before



Other tools

- ▣ Deft Linux
<http://www.deftlinux.net/>
- ▣ FTK Imager
<http://www.accessdata.com/downloads.html>
- ▣ WinHex
<http://www.x-ways.net/winhex/>



How do I know someone had ran anti-forensics software on a computer?

- ▣ No 100% positive way
- ▣ Look for files names I mentioned in this presentation
- ▣ Leftovers from the tool, for example:
HKCU\Software\Sysinternals\SDelete\EulaAccepted
- ▣ I need to work on some tools to do this sort of detection...
- ▣ Look at the drive for large sections of all zeros/random bytes, but this could be for other reasons (Vista & < after full format, Solid-state Drives)
- ▣ Hash search of know anti-forensics tools
HashMyFiles
http://www.nirsoft.net/utils/hash_my_files.html



Change the hash of the file 😊

- ▣ If it's just the hash, change a few bytes, preferably in strings
- ▣ Compile from source if you have it
- ▣ Use a packer

UPX

<http://upx.sourceforge.net/>

<http://sourceforge.net/projects/upxer/files/>

- ▣ Shikata Gai Nai from Metasploit

<http://www.metasploit.com>



Events

- ▣ Free ISSA classes
- ▣ ISSA Meeting
<http://issa-kentuckiana.org/>
- ▣ Louisville Infosec
<http://www.louisvilleinfosec.com/>
- ▣ Phreaknic/Notacon/Outerz0ne
<http://phreaknic.info>
<http://notacon.org/>
<http://www.outerz0ne.org/>



Helping with the free classes

- ▣ Got old hardware you would like to donate?
- ▣ Is there a subject you would like to teach?
- ▣ Let others know about upcoming classes, and the videos of previous classes.



Thanks

- ▣ Scott Moulton
<http://www.myharddrivedied.com/>
- ▣ Tyler “Trip” Pitchford
- ▣ Folks at Binrev and Pauidotcom
- ▣ Louisville ISSA
- ▣ John for the extra camera



QUESTIONS?

42

