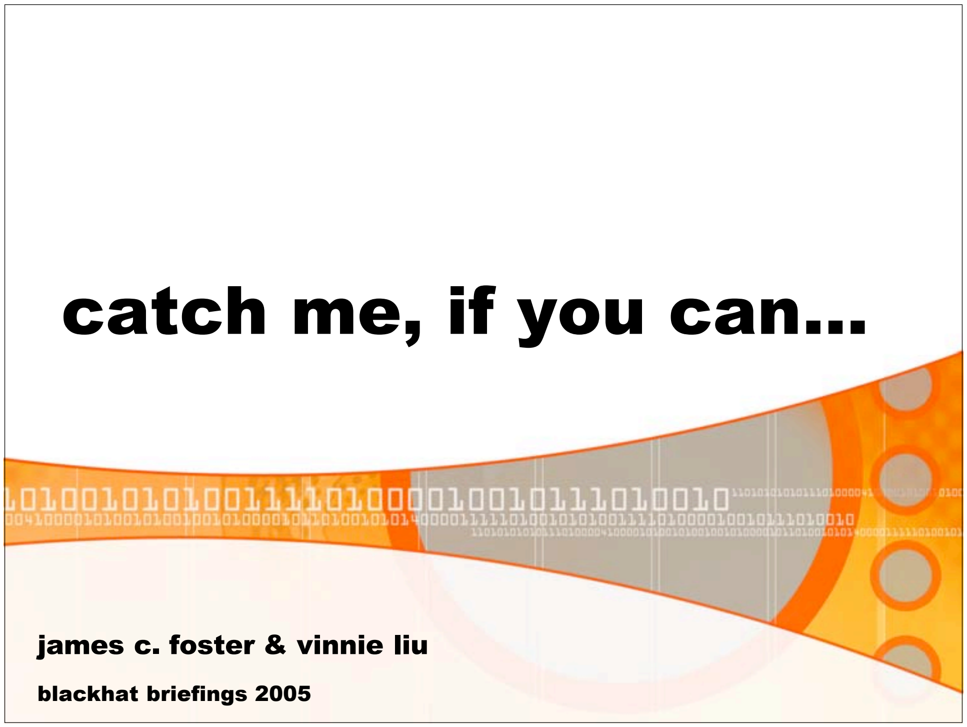


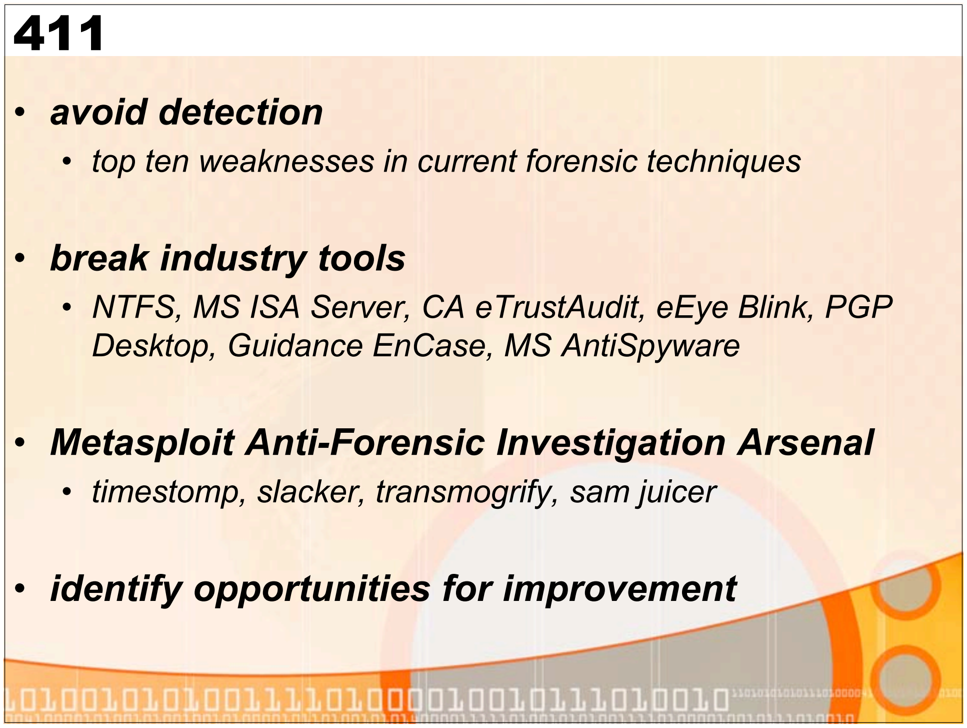
# catch me, if you can…

james c. foster & vinnie liu

blackhat briefings 2005

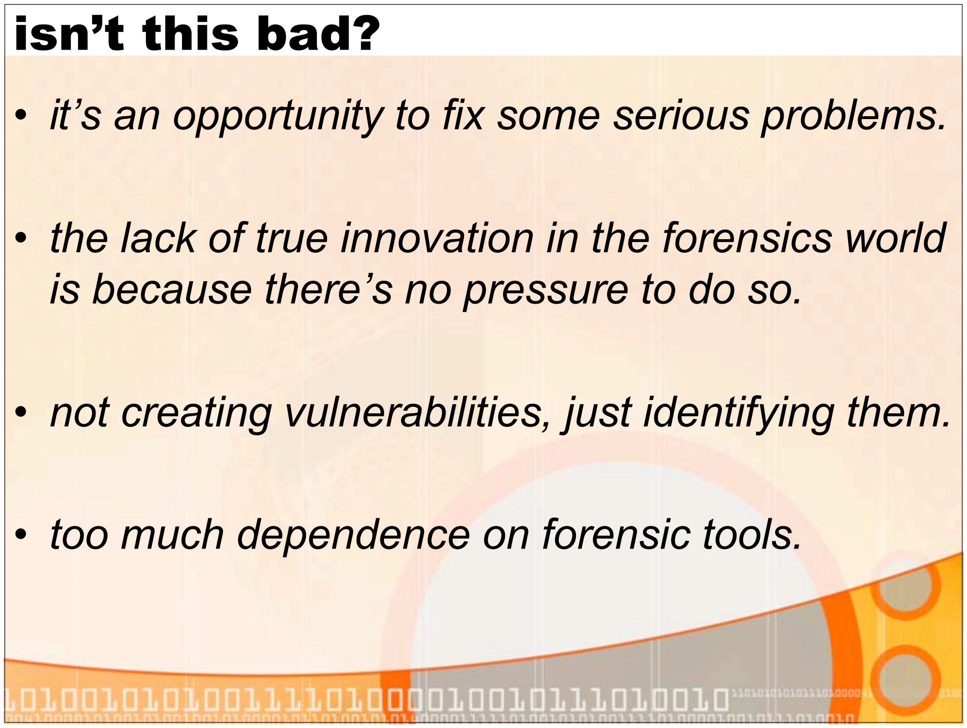
## speaker bios

- *Vinnie*
  - *researcher*
  - *vinnie@metasploit.com*
- *Foster*
  - *researcher*
  - *jamescfoster@gmail.com*



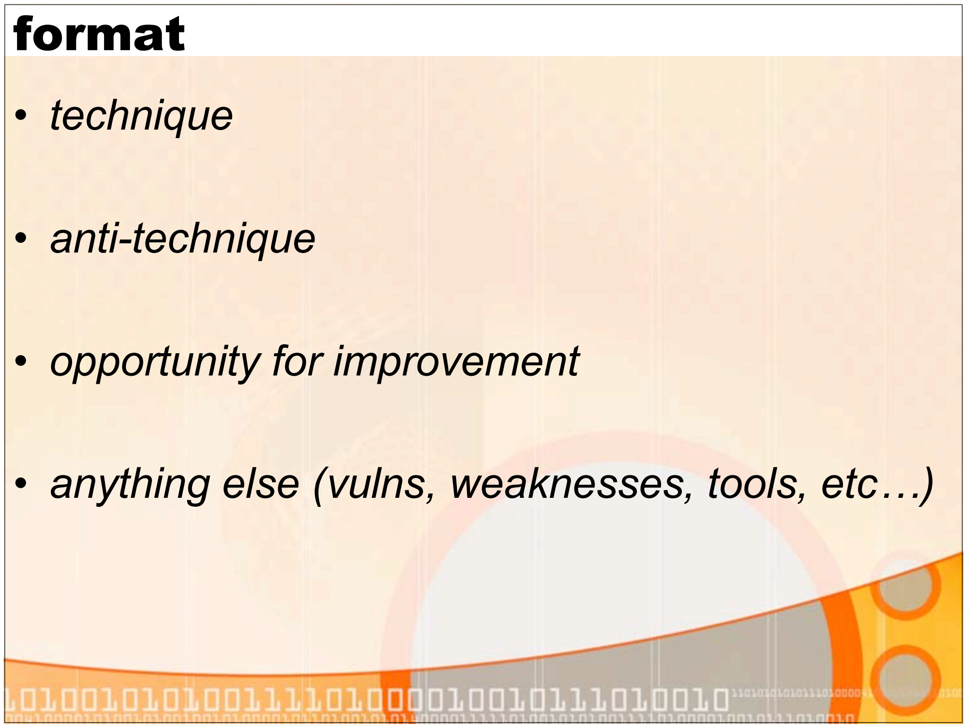
## 411

- ***avoid detection***
  - *top ten weaknesses in current forensic techniques*
- ***break industry tools***
  - *NTFS, MS ISA Server, CA eTrustAudit, eEye Blink, PGP Desktop, Guidance EnCase, MS AntiSpyware*
- ***Metasploit Anti-Forensic Investigation Arsenal***
  - *timestomp, slacker, transmogrify, sam juicer*
- ***identify opportunities for improvement***



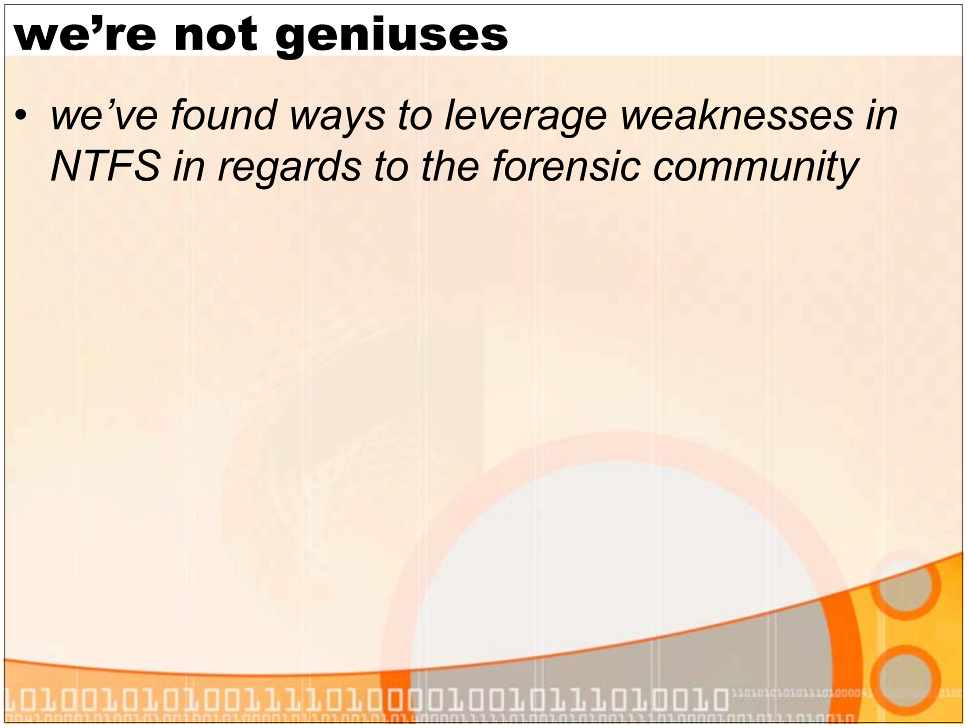
## isn’t this bad?

- *it’s an opportunity to fix some serious problems.*
- *the lack of true innovation in the forensics world is because there’s no pressure to do so.*
- *not creating vulnerabilities, just identifying them.*
- *too much dependence on forensic tools.*



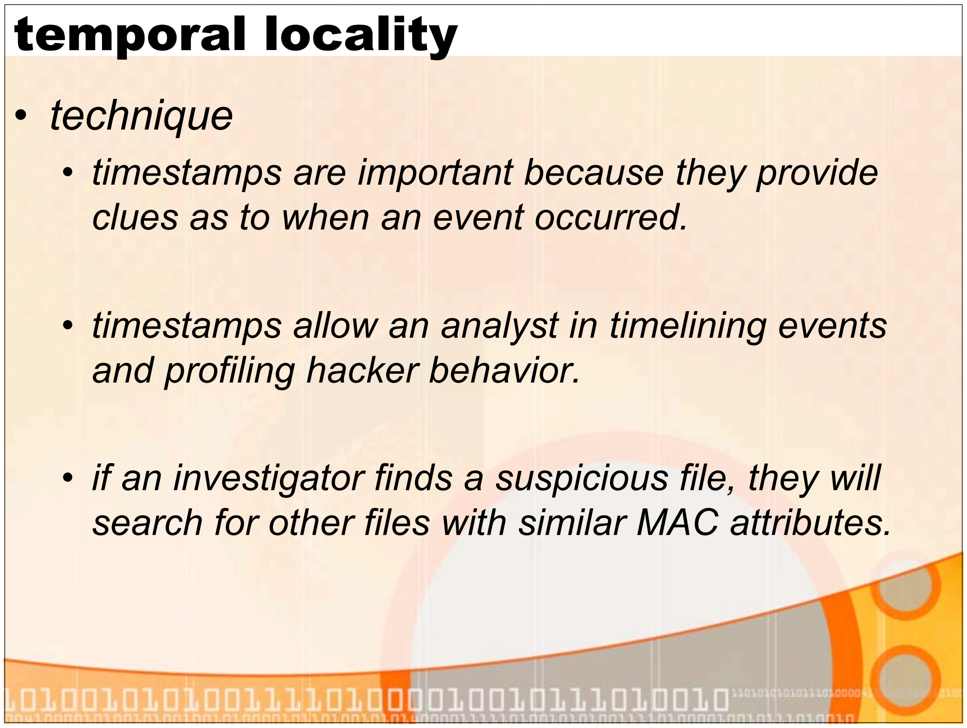
## format

- *technique*
- *anti-technique*
- *opportunity for improvement*
- *anything else (vulns, weaknesses, tools, etc…)*



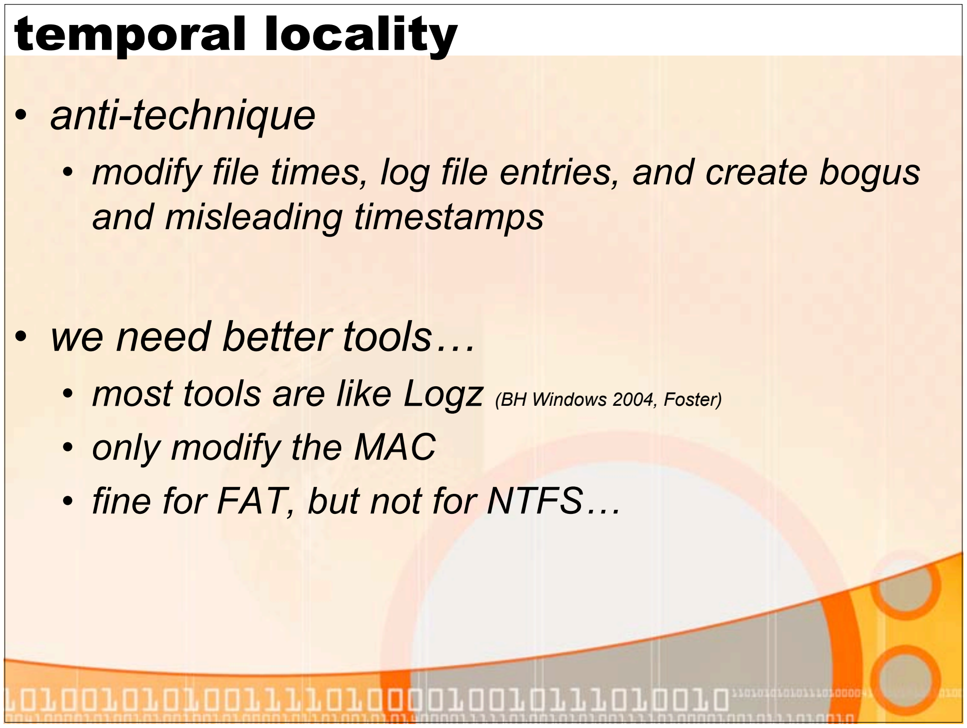
## we’re not geniuses

- *we’ve found ways to leverage weaknesses in NTFS in regards to the forensic community*



## temporal locality

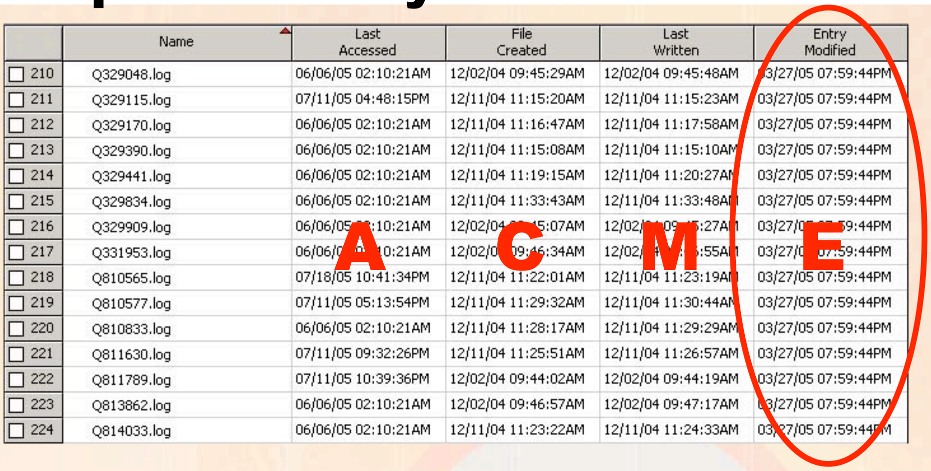
- *technique*
  - *timestamps are important because they provide clues as to when an event occurred.*
  - *timestamps allow an analyst in timelining events and profiling hacker behavior.*
  - *if an investigator finds a suspicious file, they will search for other files with similar MAC attributes.*



## temporal locality

- *anti-technique*
  - *modify file times, log file entries, and create bogus and misleading timestamps*
- *we need better tools…*
  - *most tools are like Logz (BH Windows 2004, Foster)*
  - *only modify the MAC*
  - *fine for FAT, but not for NTFS…*

# temporal locality



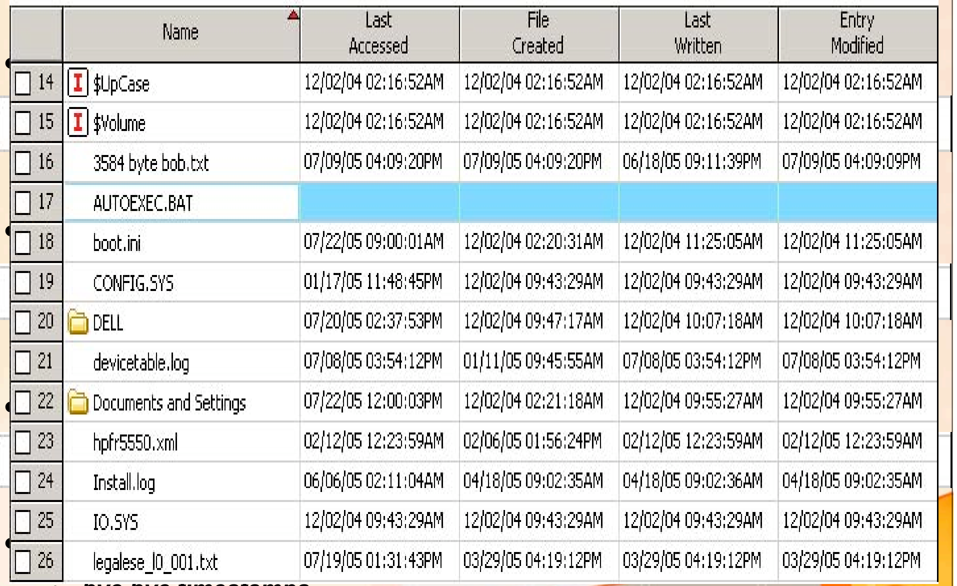
|  | Name | Last Accessed | File Created | Last Written | Entry Modified |
|---|---|---|---|---|---|
| □ 210 | Q329048.log | 06/06/05 02:10:21AM | 12/02/04 09:45:29AM | 12/02/04 09:45:48AM | 03/27/05 07:59:44PM |
| □ 211 | Q329115.log | 07/11/05 04:48:15PM | 12/11/04 11:15:20AM | 12/11/04 11:15:23AM | 03/27/05 07:59:44PM |
| □ 212 | Q329170.log | 06/06/05 02:10:21AM | 12/11/04 11:16:47AM | 12/11/04 11:17:58AM | 03/27/05 07:59:44PM |
| □ 213 | Q329390.log | 06/06/05 02:10:21AM | 12/11/04 11:15:08AM | 12/11/04 11:15:10AM | 03/27/05 07:59:44PM |
| □ 214 | Q329441.log | 06/06/05 02:10:21AM | 12/11/04 11:19:15AM | 12/11/04 11:20:27AM | 03/27/05 07:59:44PM |
| □ 215 | Q329834.log | 06/06/05 02:10:21AM | 12/11/04 11:33:43AM | 12/11/04 11:33:48AM | 03/27/05 07:59:44PM |
| □ 216 | Q329909.log | 06/06/05 02:10:21AM | 12/02/04 09:45:07AM | 12/02/04 09:45:27AM | 03/27/05 07:59:44PM |
| □ 217 | Q331953.log | 06/06/05 02:10:21AM | 12/02/04 09:46:34AM | 12/02/04 09:46:55AM | 03/27/05 07:59:44PM |
| □ 218 | Q810565.log | 07/18/05 10:41:34PM | 12/11/04 11:22:01AM | 12/11/04 11:23:19AM | 03/27/05 07:59:44PM |
| □ 219 | Q810577.log | 07/11/05 05:13:54PM | 12/11/04 11:29:32AM | 12/11/04 11:30:44AM | 03/27/05 07:59:44PM |
| □ 220 | Q810833.log | 06/06/05 02:10:21AM | 12/11/04 11:28:17AM | 12/11/04 11:29:29AM | 03/27/05 07:59:44PM |
| □ 221 | Q811630.log | 07/11/05 09:32:26PM | 12/11/04 11:25:51AM | 12/11/04 11:26:57AM | 03/27/05 07:59:44PM |
| □ 222 | Q811789.log | 07/11/05 10:39:36PM | 12/02/04 09:44:02AM | 12/02/04 09:44:19AM | 03/27/05 07:59:44PM |
| □ 223 | Q813862.log | 06/06/05 02:10:21AM | 12/02/04 09:46:57AM | 12/02/04 09:47:17AM | 03/27/05 07:59:44PM |
| □ 224 | Q814033.log | 06/06/05 02:10:21AM | 12/11/04 11:23:22AM | 12/11/04 11:24:33AM | 03/27/05 07:59:44PM |

- *modified (**M**), accessed (**A**), created (**C**)*
- *entry modified (E)*

# we have the technology…

- ***timestomp***
  - *uses the following Windows system calls:*
    - *NtQueryInformationFile()*
    - *NtSetInformationFile()*
  - *features:*
    - *display current MACE attributes*
    - *set MACE attributes*
    - *mess with **EnCase** and **MS Anti-Spyware***

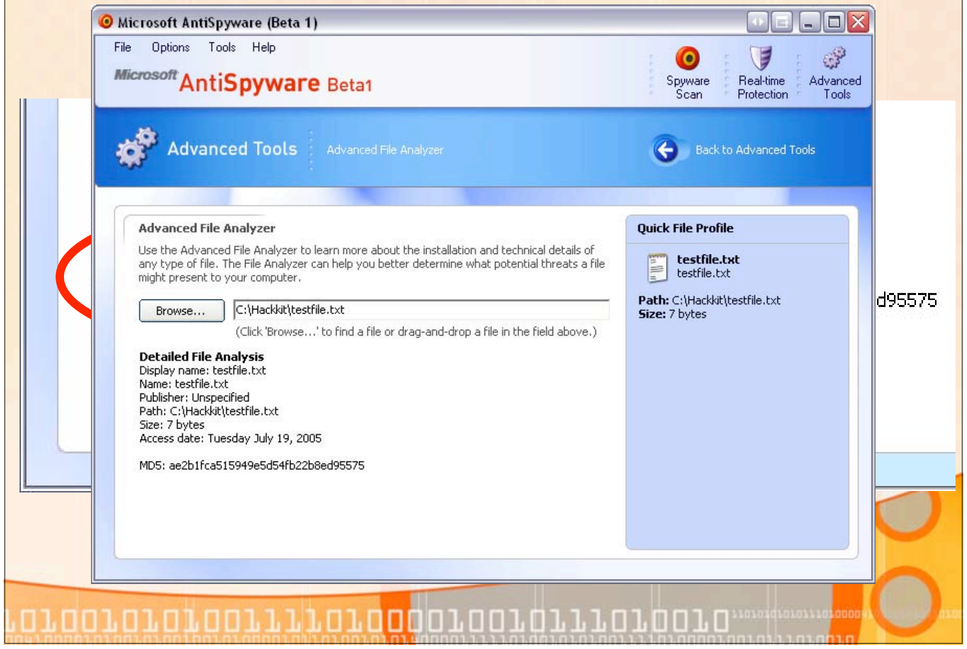
# timestomp doing its thing



|  | Name | Last Accessed | File Created | Last Written | Entry Modified |
|---|---|---|---|---|---|
| □ 14 | $UpCase | 12/02/04 02:16:52AM | 12/02/04 02:16:52AM | 12/02/04 02:16:52AM | 12/02/04 02:16:52AM |
| □ 15 | $Volume | 12/02/04 02:16:52AM | 12/02/04 02:16:52AM | 12/02/04 02:16:52AM | 12/02/04 02:16:52AM |
| □ 16 | 3584 byte bob.txt | 07/09/05 04:09:20PM | 07/09/05 04:09:20PM | 06/18/05 09:11:39PM | 07/09/05 04:09:09PM |
| □ 17 | AUTOEXEC.BAT |  |  |  |  |
| □ 18 | boot.ini | 07/22/05 09:00:01AM | 12/02/04 02:20:31AM | 12/02/04 11:25:05AM | 12/02/04 11:25:05AM |
| □ 19 | CONFIG.SYS | 01/17/05 11:48:45PM | 12/02/04 09:43:29AM | 12/02/04 09:43:29AM | 12/02/04 09:43:29AM |
| □ 20 | DELL | 07/20/05 02:37:53PM | 12/02/04 09:47:17AM | 12/02/04 10:07:18AM | 12/02/04 10:07:18AM |
| □ 21 | devicetable.log | 07/08/05 03:54:12PM | 01/11/05 09:45:55AM | 07/08/05 03:54:12PM | 07/08/05 03:54:12PM |
| □ 22 | Documents and Settings | 07/22/05 12:00:03PM | 12/02/04 02:21:18AM | 12/02/04 09:55:27AM | 12/02/04 09:55:27AM |
| □ 23 | hpfr5550.xml | 02/12/05 12:23:59AM | 02/06/05 01:56:24PM | 02/12/05 12:23:59AM | 02/12/05 12:23:59AM |
| □ 24 | Install.log | 06/06/05 02:11:04AM | 04/18/05 09:02:35AM | 04/18/05 09:02:36AM | 04/18/05 09:02:35AM |
| □ 25 | IO.SYS | 12/02/04 09:43:29AM | 12/02/04 09:43:29AM | 12/02/04 09:43:29AM | 12/02/04 09:43:29AM |
| □ 26 | legalese_l0_001.txt | 07/19/05 01:31:43PM | 03/29/05 04:19:12PM | 03/29/05 04:19:12PM | 03/29/05 04:19:12PM |

- *bye bye timestamps*

# timestomp doing its thing



**Advanced File Analyzer**

Use the Advanced File Analyzer to learn more about the installation and technical details of any type of file. The File Analyzer can help you better determine what potential threats a file might present to your computer.

C:\Hackkit\testfile.txt

(Click 'Browse...' to find a file or drag-and-drop a file in the field above.)

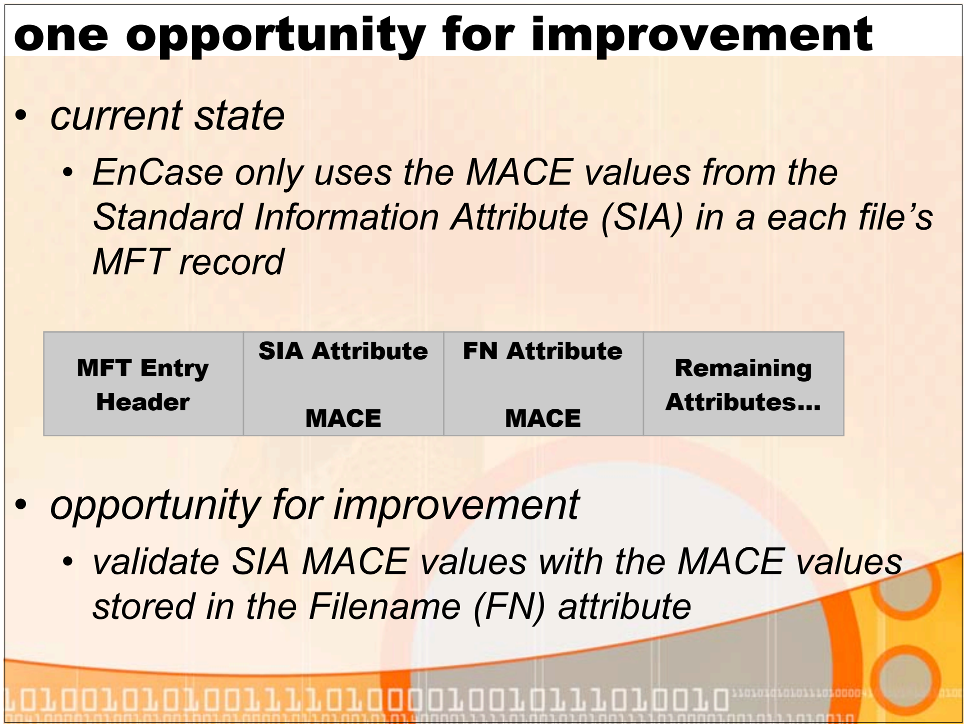
**Detailed File Analysis**
Display name: testfile.txt
Name: testfile.txt
Publisher: Unspecified
Path: C:\Hackkit\testfile.txt
Size: 7 bytes
Access date: Tuesday July 19, 2005

MD5: ae2b1fca515949e5d54fb22b8ed95575

**Quick File Profile**

**testfile.txt**
testfile.txt

**Path:** C:\Hackkit\testfile.txt
**Size:** 7 bytes

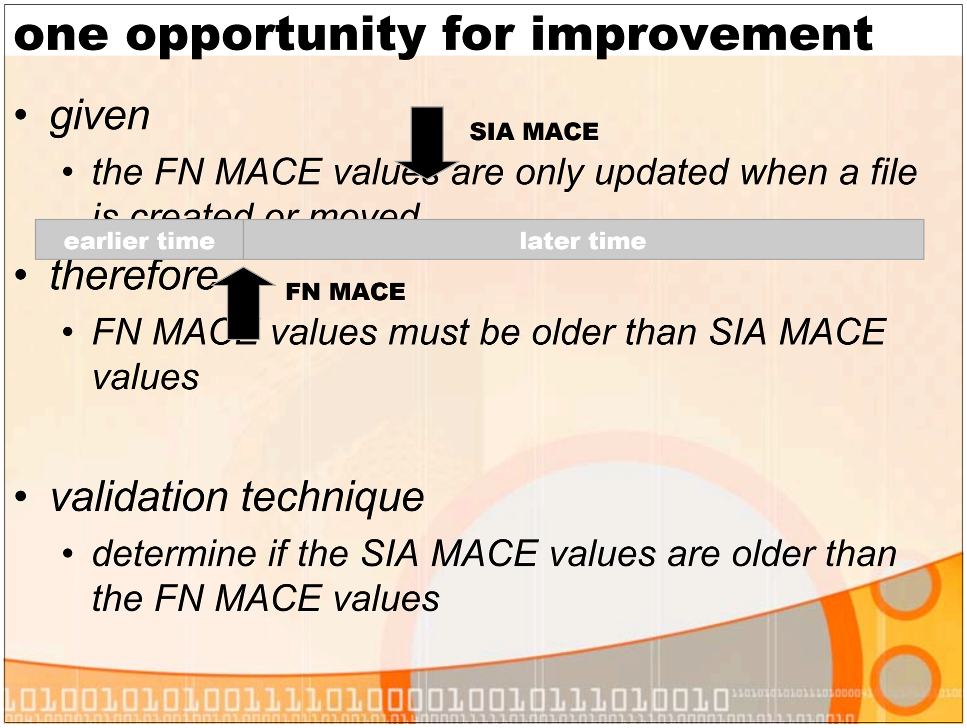


# one opportunity for improvement

- *current state*
  - *EnCase only uses the MACE values from the Standard Information Attribute (SIA) in a each file's MFT record*

| MFT Entry Header | SIA Attribute<br>MACE | FN Attribute<br>MACE | Remaining Attributes... |
|---|---|---|---|

- *opportunity for improvement*
  - *validate SIA MACE values with the MACE values stored in the Filename (FN) attribute*



# one opportunity for improvement

- *given*
  - *the FN MACE values are only updated when a file is created or moved*

SIA MACE

| earlier time | later time |
|---|---|

FN MACE

- *therefore*
  - *FN MACE values must be older than SIA MACE values*
- *validation technique*
  - *determine if the SIA MACE values are older than the FN MACE values*

## ...more like one-half

- *anti-validation technique*
  - *calculate offsets from the start of the MFT to a file's FN MACE values*
  - *use raw disk i/o to change the FN MACE values*
  - *us ete the $d*

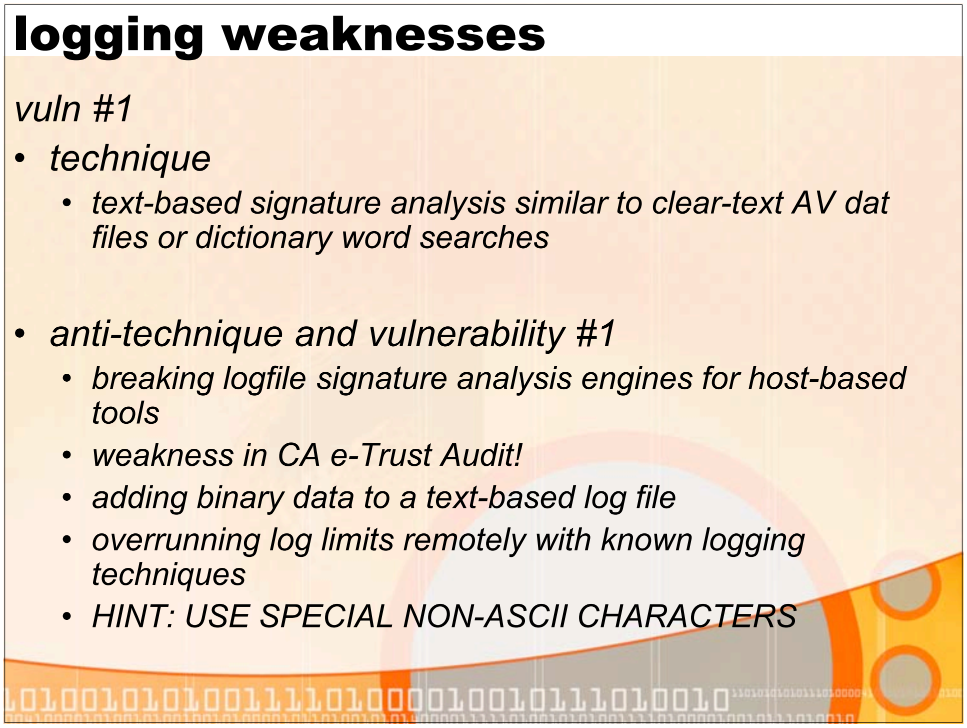
BlackHat
USA • EUROPE • ASIA
Japan 2005

- *timestomp*
  - *its definitely dicey to perform live changes to the MFT, but look for it in future versions*

## more goodies...

- *weaknesses in what?*
  - *all computer logging applications*
- *think STICK for logging systems*
  - *specifically: CA e-Trust Suite has issues reading numerous types of log file, especially if they have been modified*

***Hopefully new STICK-like host-based anti-forensics tool to be released at BlackHat Japan 2005!*



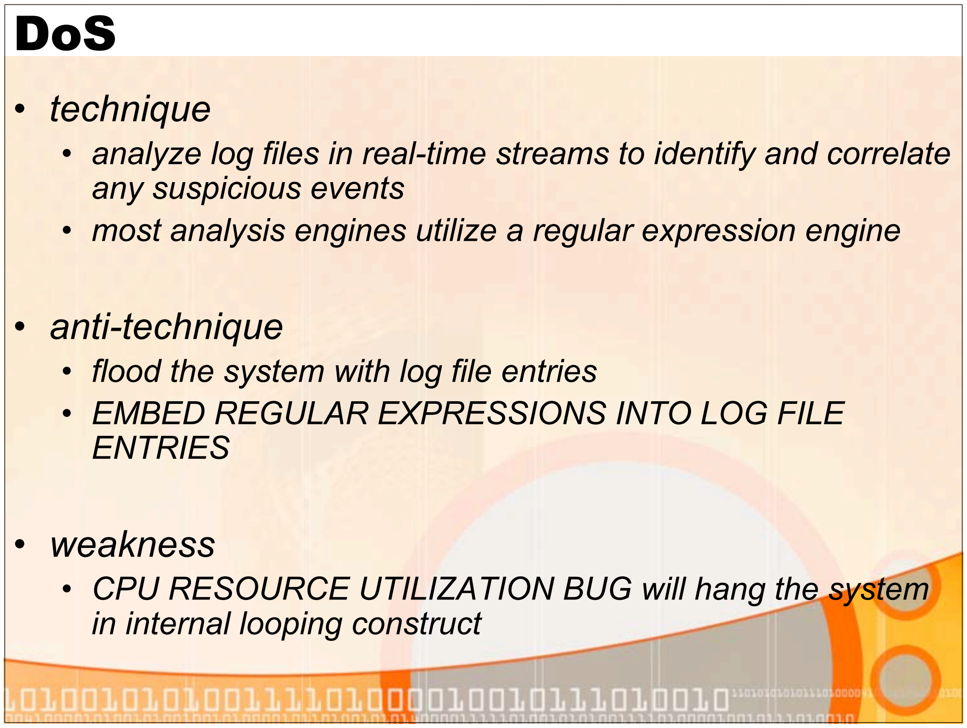
## logging weaknesses

*vuln #1*

- *technique*
  - *text-based signature analysis similar to clear-text AV dat files or dictionary word searches*
- *anti-technique and vulnerability #1*
  - *breaking logfile signature analysis engines for host-based tools*
  - *weakness in CA e-Trust Audit!*
  - *adding binary data to a text-based log file*
  - *overrunning log limits remotely with known logging techniques*
  - *HINT: USE SPECIAL NON-ASCII CHARACTERS*

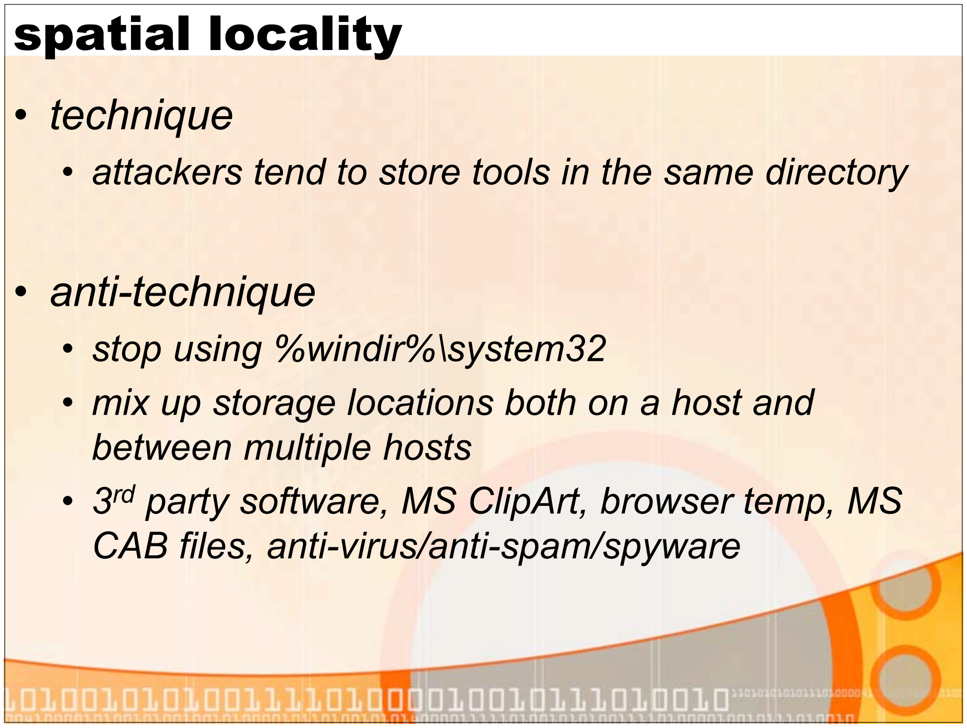
## fooling MSFT logging techniques

- *anti-techniques continued*
  - *leveraging Windows system calls and logging schemes that are default-enabled in MSFT*
    - *Ex: MsiInstaller Event (11707)*



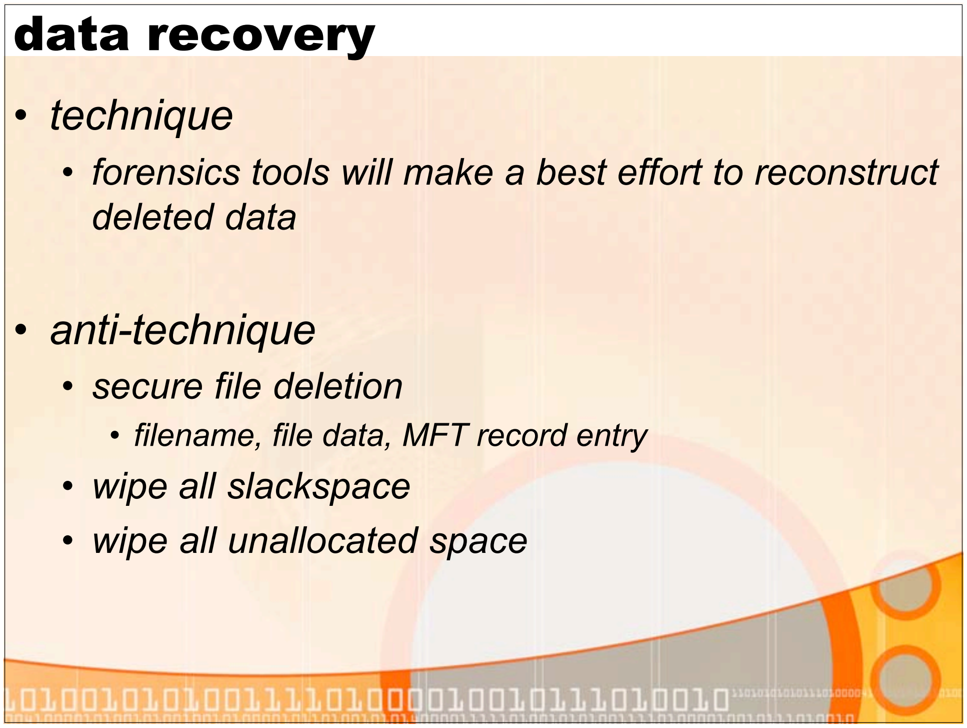
## DoS

- *technique*
  - *analyze log files in real-time streams to identify and correlate any suspicious events*
  - *most analysis engines utilize a regular expression engine*
- *anti-technique*
  - *flood the system with log file entries*
  - *EMBED REGULAR EXPRESSIONS INTO LOG FILE ENTRIES*
- *weakness*
  - *CPU RESOURCE UTILIZATION BUG will hang the system in internal looping construct*



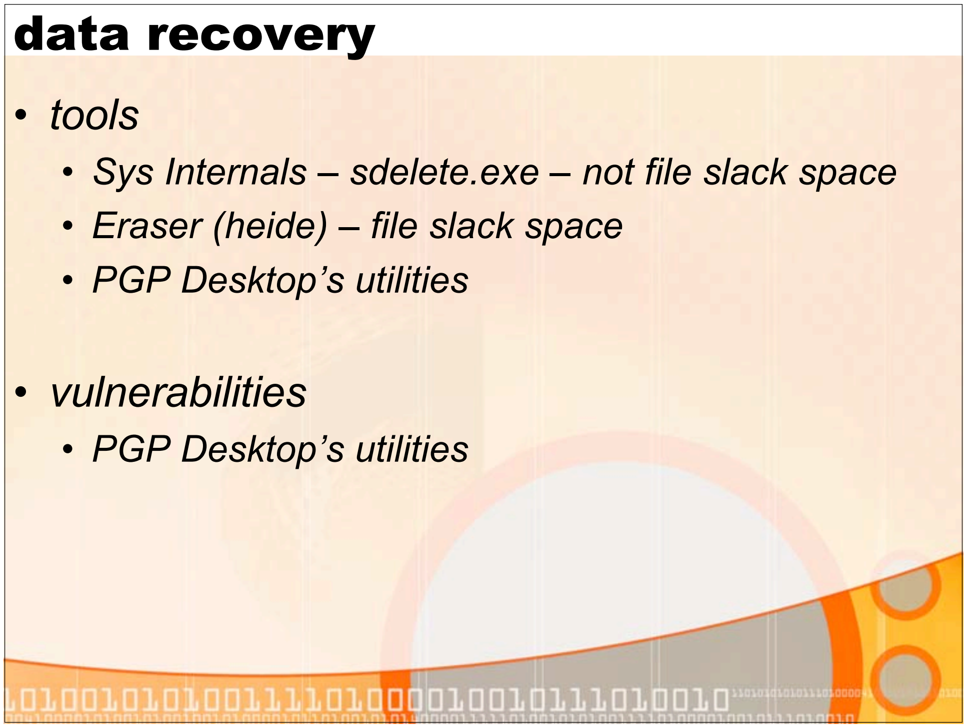
## spatial locality

- *technique*
  - *attackers tend to store tools in the same directory*
- *anti-technique*
  - *stop using %windir%\system32*
  - *mix up storage locations both on a host and between multiple hosts*
  - *3rd party software, MS ClipArt, browser temp, MS CAB files, anti-virus/anti-spam/spyware*



## data recovery

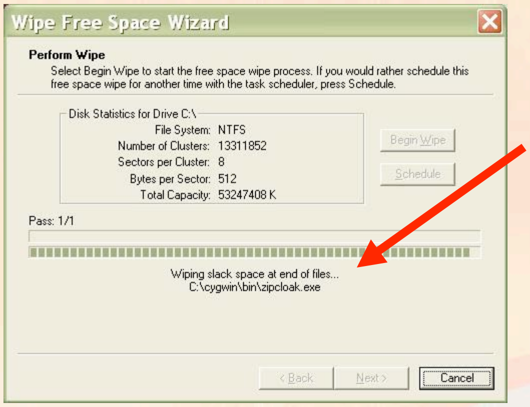
- *technique*
  - *forensics tools will make a best effort to reconstruct deleted data*
- *anti-technique*
  - *secure file deletion*
    - *filename, file data, MFT record entry*
  - *wipe all slackspace*
  - *wipe all unallocated space*



## data recovery

- *tools*
  - *Sys Internals – sdelete.exe – not file slack space*
  - *Eraser (heide) – file slack space*
  - *PGP Desktop's utilities*
- *vulnerabilities*
  - *PGP Desktop's utilities*

## selling snake oil



**Perform Wipe**

Select Begin Wipe to start the free space wipe process. If you would rather schedule this free space wipe for another time with the task scheduler, press Schedule.

Disk Statistics for Drive C:\

| | |
|---|---|
| File System: | NTFS |
| Number of Clusters: | 13311852 |
| Sectors per Cluster: | 8 |
| Bytes per Sector: | 512 |
| Total Capacity: | 53247408 K |

Pass: 1/1

Wiping slack space at end of files...
C:\cygwin\bin\zipcloak.exe

**PGP 8.x and 9.1 - "wiping slack space at end of files…"**

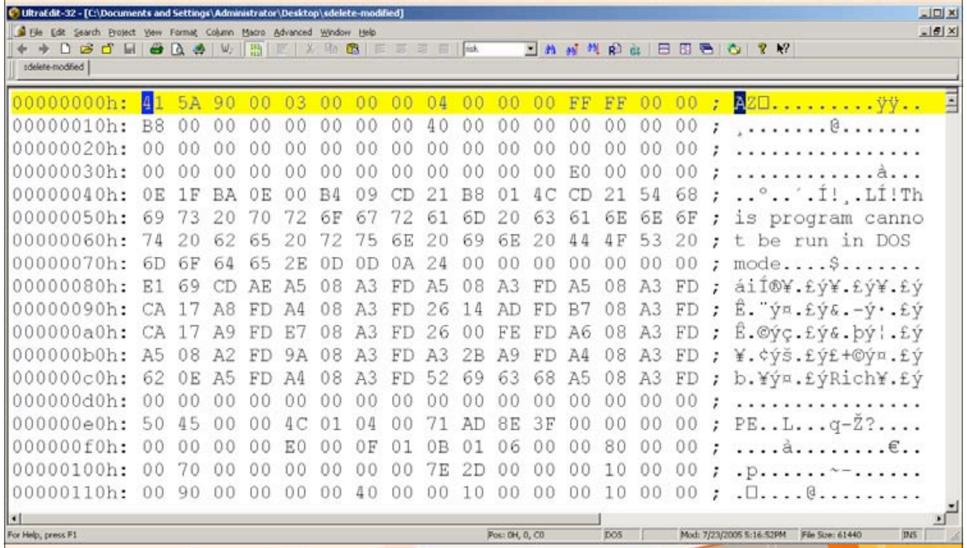
**think of it as an opportunity for improvement…**

**well, it doesn't.**

## signature analysis

- *technique*
  - *EnCase has two methods for identifying file types*
    - *file extension*
    - *file signatures*
- *anti-technique*
  - *change the file extension*
    - ***Special note – this lame technique will also work on nearly every perimeter-based file sweeping product (prime ex: gmail)*
  - *changing file signatures to avoid EnCase analysis*
    - *one-byte modification*

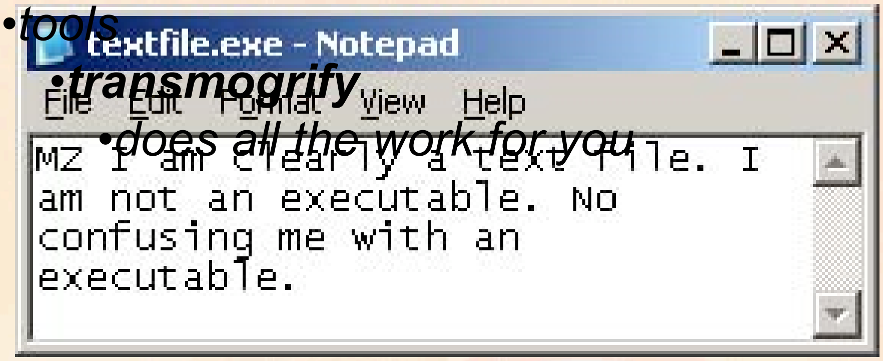
# fooling signature analysis


UltraEdit-32 - [C:\Documents and Settings\Administrator\Desktop\sdelete-modified]
File Edit Search Project View Format Column Macro Advanced Window Help
sdelete-modified
For Help, press F1
Pos: 0H, 0, C0
DOS
Mod: 7/23/2005 5:16:52PM
File Size: 61440
INS

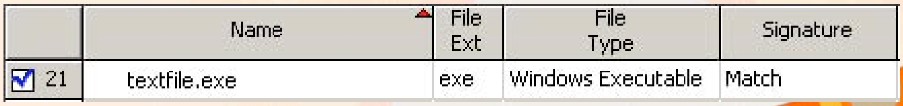
```
00000000h: 41 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 ; AZ□.........ÿÿ..
00000010h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ; ¸.......@.......
00000020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000030h: 00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00 ; ............à...
00000040h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ; ..º..´.Í!¸.LÍ!Th
00000050h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F ; is program canno
00000060h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 ; t be run in DOS 
00000070h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 ; mode....$.......
00000080h: E1 69 CD AE A5 08 A3 FD A5 08 A3 FD A5 08 A3 FD ; áiÍ®¥.£ý¥.£ý¥.£ý
00000090h: CA 17 A8 FD A4 08 A3 FD 26 14 AD FD B7 08 A3 FD ; Ê.¨ý¤.£ý&.-ý·.£ý
000000a0h: CA 17 A9 FD E7 08 A3 FD 26 00 FE FD A6 08 A3 FD ; Ê.©ýç.£ý&.þý¦.£ý
000000b0h: A5 08 A2 FD 9A 08 A3 FD A3 2B A9 FD A4 08 A3 FD ; ¥.¢ýš.£ý£+©ý¤.£ý
000000c0h: 62 0E A5 FD A4 08 A3 FD 52 69 63 68 A5 08 A3 FD ; b.¥ý¤.£ýRich¥.£ý
000000d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000e0h: 50 45 00 00 4C 01 04 00 71 AD 8E 3F 00 00 00 00 ; PE..L...q-Ž?....
000000f0h: 00 00 00 00 E0 00 0F 01 0B 01 06 00 00 80 00 00 ; ....à.......€..
00000100h: 00 70 00 00 00 00 00 00 7E 2D 00 00 00 10 00 00 ; .p......~-......
00000110h: 00 90 00 00 00 00 40 00 00 10 00 00 00 10 00 00 ; .□....@.........
```

# ...and again

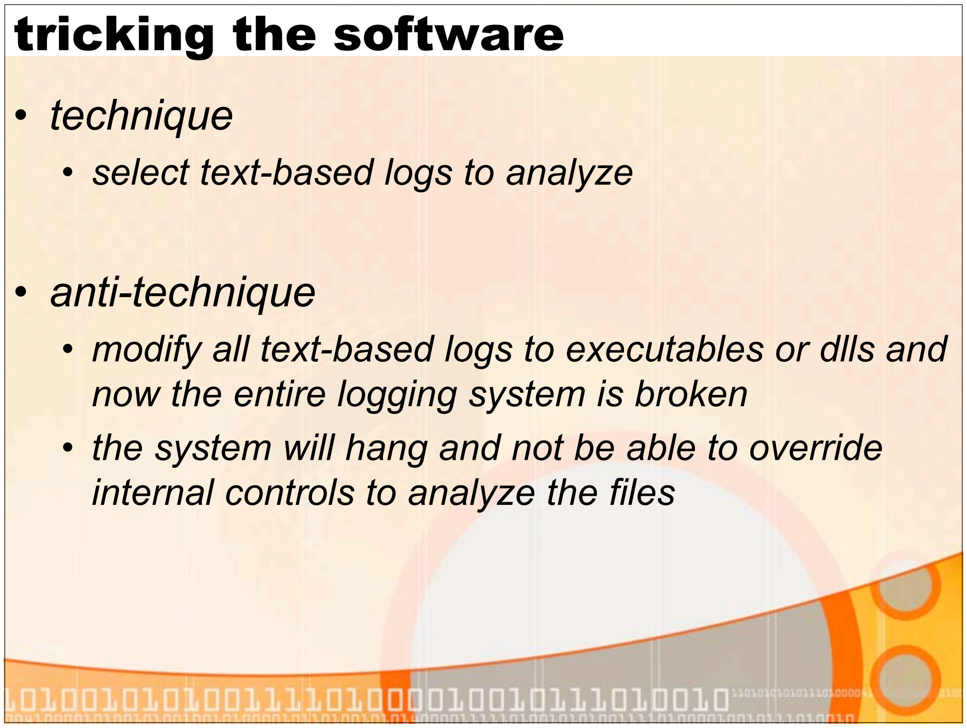
- *tools*
  - *transmogrify*
    - *does all the work for you*



MZ I am clearly a text file. I am not an executable. No confusing me with an executable.

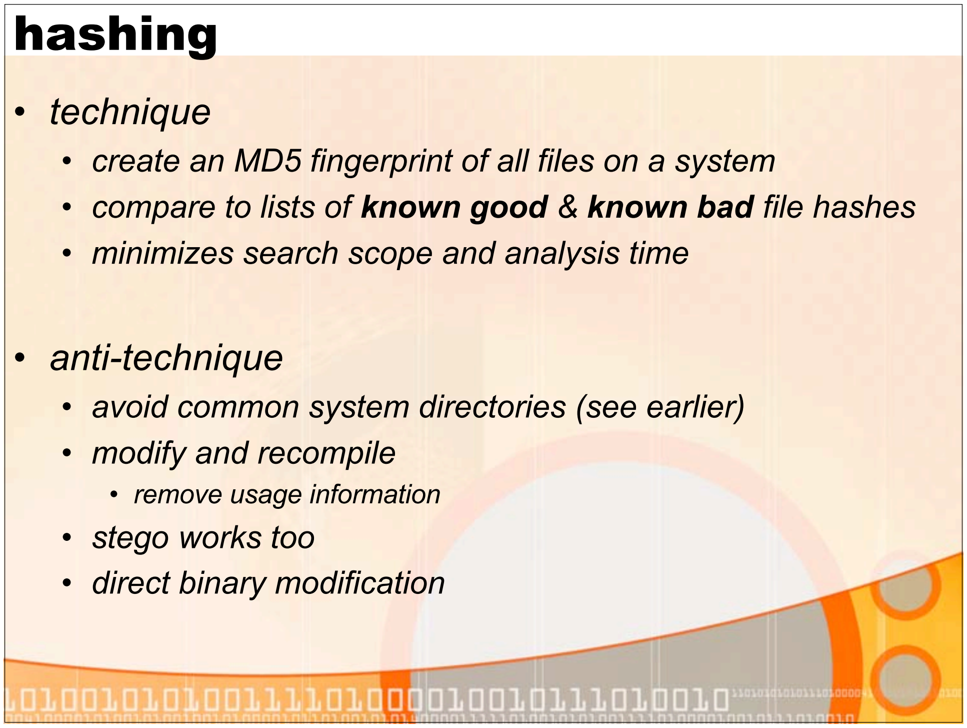


| | Name | File Ext | File Type | Signature |
|---|---|---|---|---|
| ☑ 21 | textfile.exe | exe | Windows Executable | Match |



## tricking the software

- *technique*
  - *select text-based logs to analyze*
- *anti-technique*
  - *modify all text-based logs to executables or dlls and now the entire logging system is broken*
  - *the system will hang and not be able to override internal controls to analyze the files*

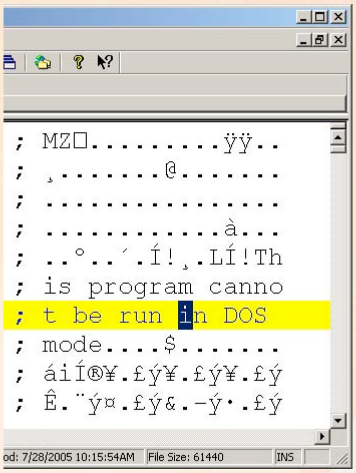


## hashing

- *technique*
  - *create an MD5 fingerprint of all files on a system*
  - *compare to lists of **known good** & **known bad** file hashes*
  - *minimizes search scope and analysis time*
- *anti-technique*
  - *avoid common system directories (see earlier)*
  - *modify and recompile*
    - *remove usage information*
  - *stego works too*
  - *direct binary modification*

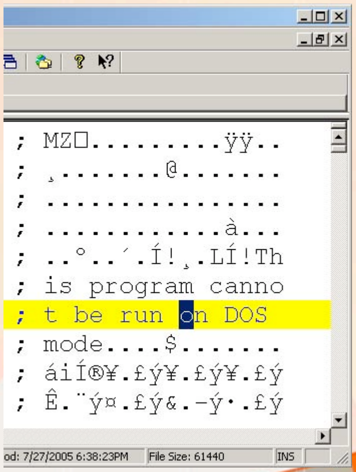
# hashing

- *direct binary modification (one-byte)*



```
; MZ□.........ÿÿ..
; ¸.......@.......
; ................
; ............à...
; ..º..´.Í!¸.LÍ!Th
; is program canno
; t be run in DOS
; mode....$.......
; áiÍ®¥.£ý¥.£ý¥.£ý
; Ê.¨ý¤.£ý&.–ý·.£ý
```

od: 7/28/2005 10:15:54AM | File Size: 61440 | INS



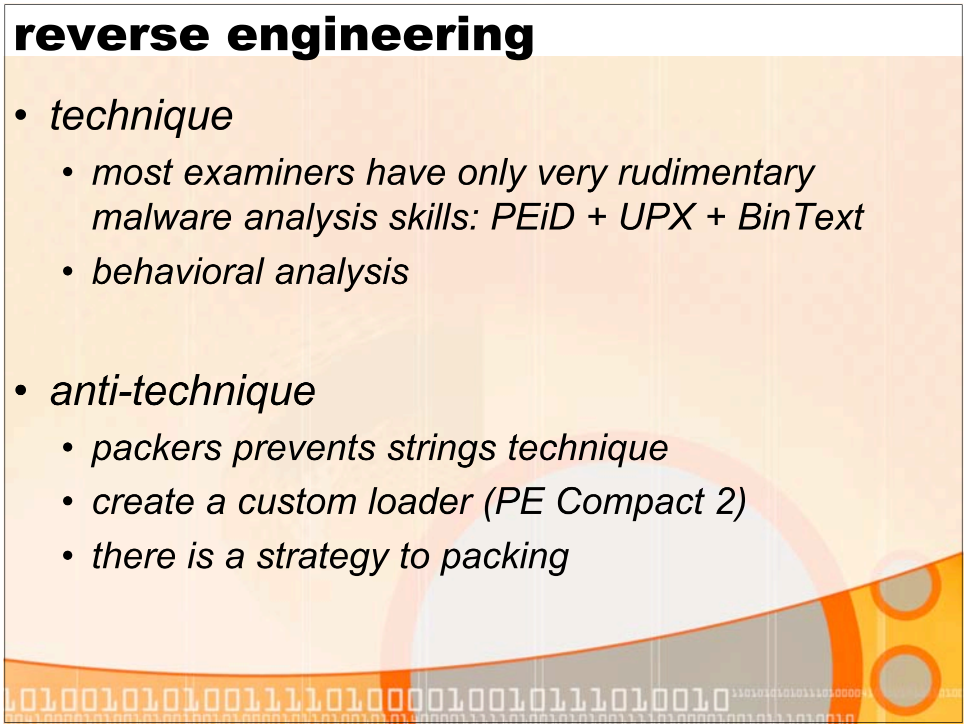
```
; MZ□.........ÿÿ..
; ¸.......@.......
; ................
; ............à...
; ..º..´.Í!¸.LÍ!Th
; is program canno
; t be run on DOS
; mode....$.......
; áiÍ®¥.£ý¥.£ý¥.£ý
; Ê.¨ý¤.£ý&.–ý·.£ý
```

od: 7/27/2005 6:38:23PM | File Size: 61440 | INS

[illegible]

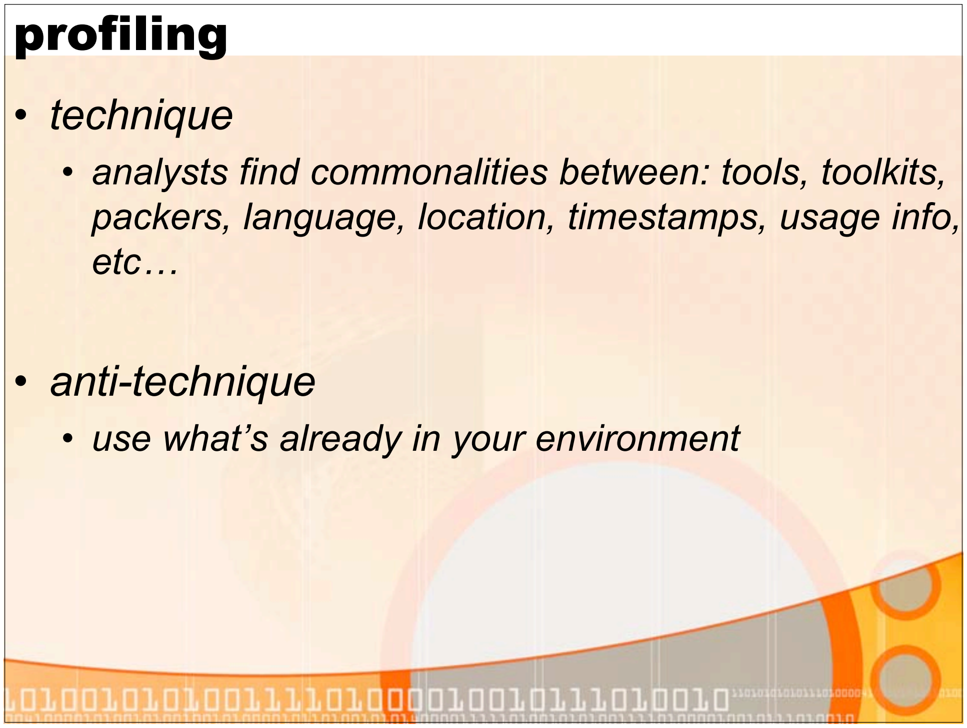
# keyword searching

- *technique*
  - *analysts build lists of keywords and search through files, slack space, unallocated space, and memory*
- *anti-technique*
  - *exploit the examiner’s lack of language skill*
  - *great and nearly impossible to catch*
- *opportunity for improvement*
  - *predefined keyword lists in different languages*



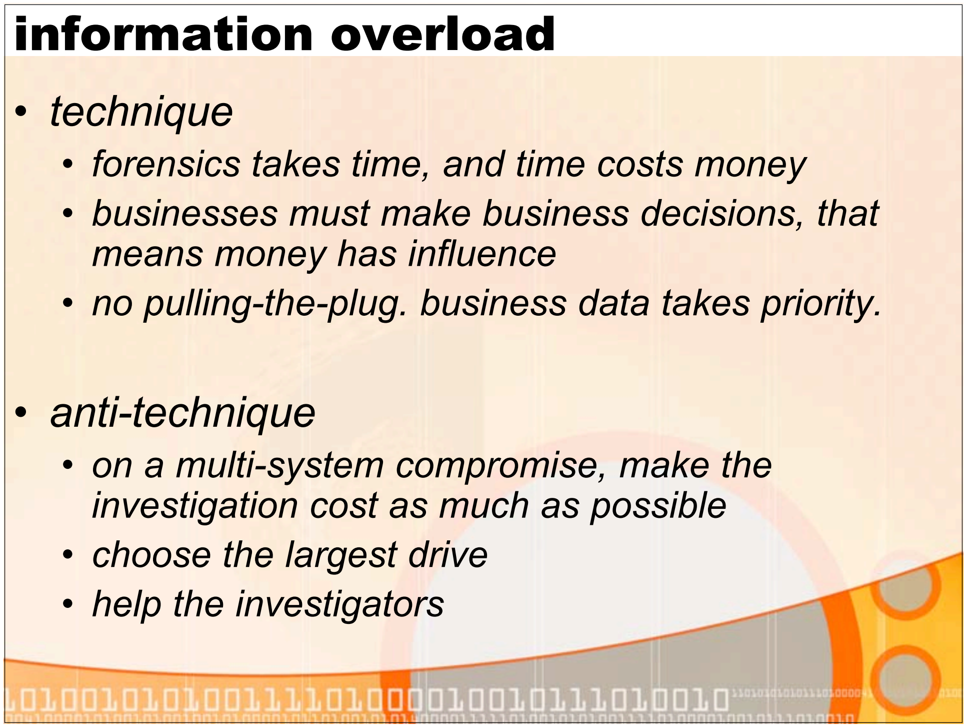
## reverse engineering

- *technique*
  - *most examiners have only very rudimentary malware analysis skills: PEiD + UPX + BinText*
  - *behavioral analysis*
- *anti-technique*
  - *packers prevents strings technique*
  - *create a custom loader (PE Compact 2)*
  - *there is a strategy to packing*



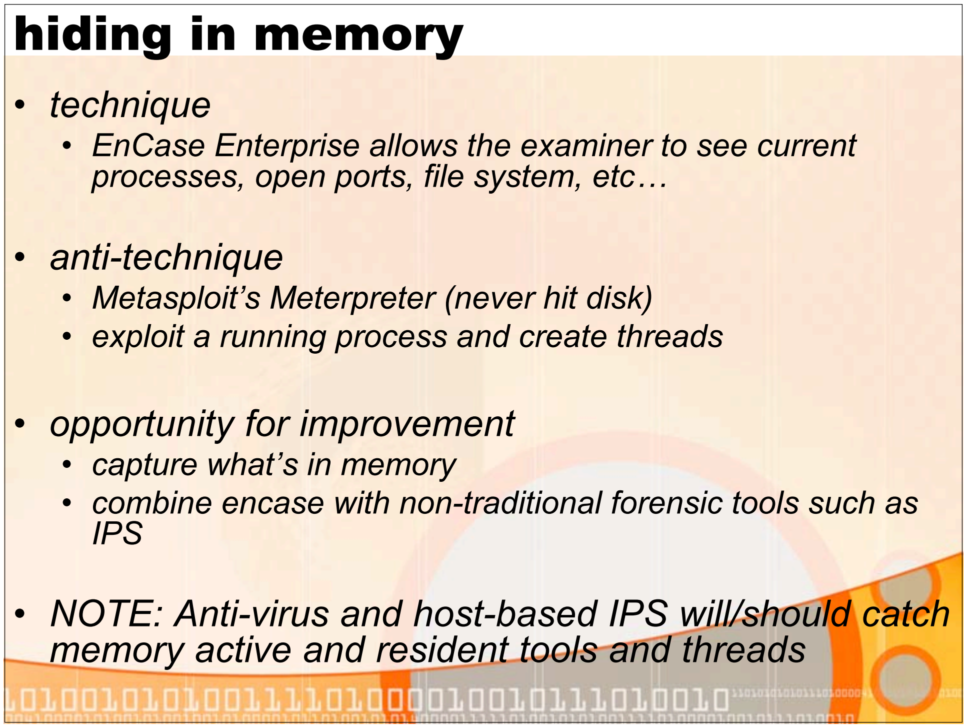
## profiling

- *technique*
  - *analysts find commonalities between: tools, toolkits, packers, language, location, timestamps, usage info, etc…*
- *anti-technique*
  - *use what's already in your environment*



## information overload

- *technique*
  - *forensics takes time, and time costs money*
  - *businesses must make business decisions, that means money has influence*
  - *no pulling-the-plug. business data takes priority.*
- *anti-technique*
  - *on a multi-system compromise, make the investigation cost as much as possible*
  - *choose the largest drive*
  - *help the investigators*



## hiding in memory

- *technique*
  - *EnCase Enterprise allows the examiner to see current processes, open ports, file system, etc…*
- *anti-technique*
  - *Metasploit's Meterpreter (never hit disk)*
  - *exploit a running process and create threads*
- *opportunity for improvement*
  - *capture what's in memory*
  - *combine encase with non-traditional forensic tools such as IPS*
- *NOTE: Anti-virus and host-based IPS will/should catch memory active and resident tools and threads*

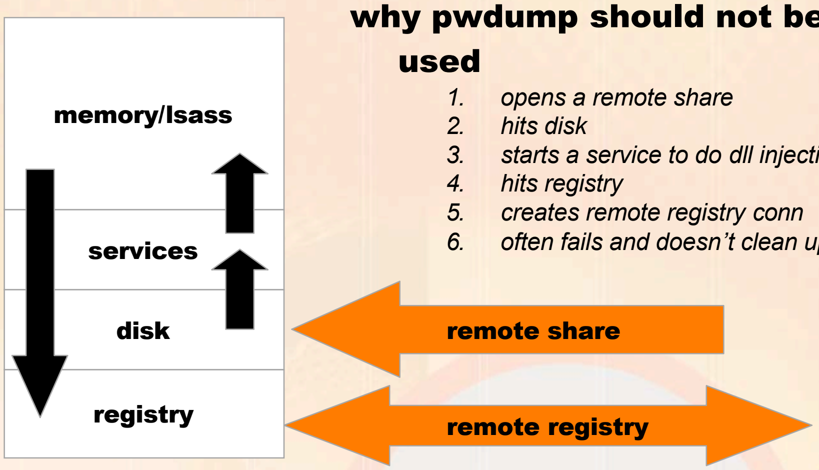
## hiding in memory

- *tools*
  - ***sam juicer***
    - *think: pwdump on crack*
    - *built from the ground up*
    - *stealthy!*

## hiding in memory

**why pwdump should not be used**

1. *opens a remote share*
2. *hits disk*
3. *starts a service to do dll injection*
4. *hits registry*
5. *creates remote registry conn*
6. *often fails and doesn't clean up*



**memory/lsass**

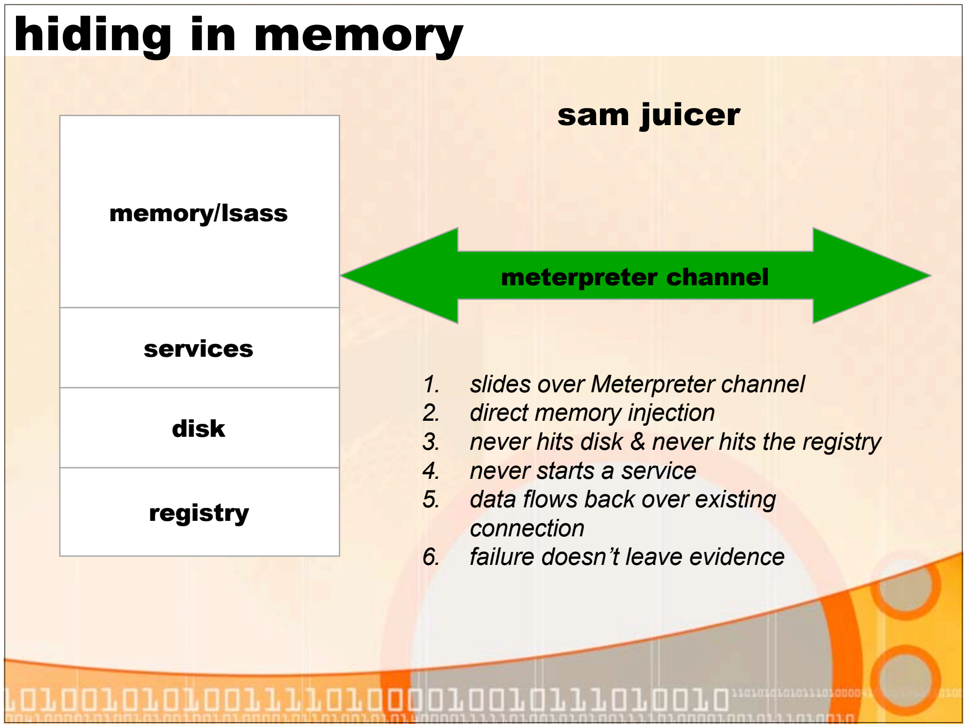
**services**

**disk**

**registry**

**remote share**

**remote registry**



## hiding in memory

### sam juicer

memory/lsass

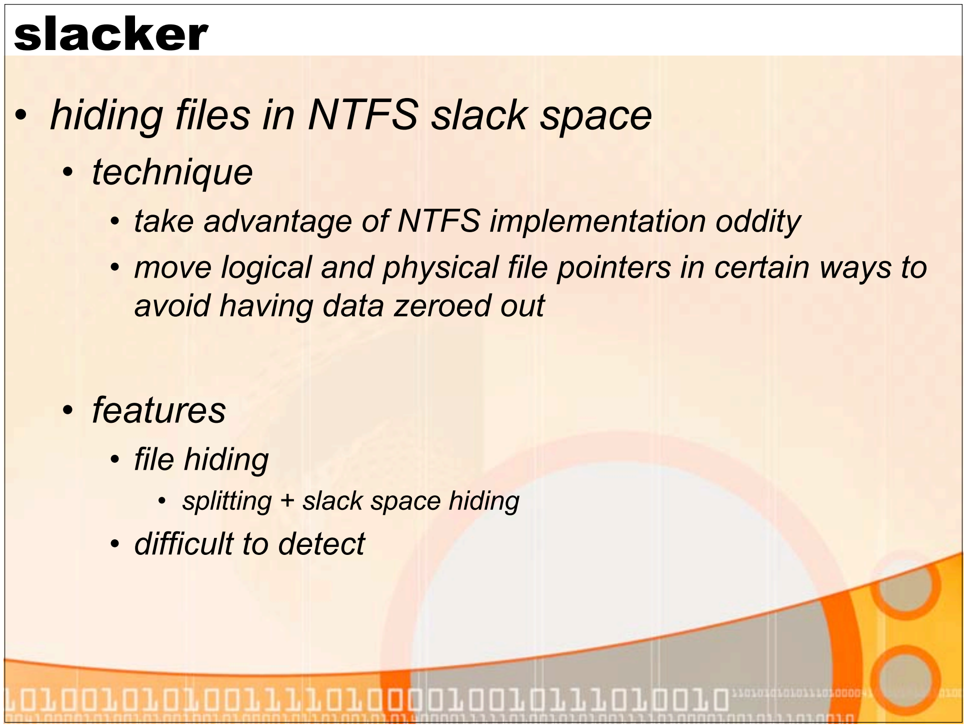
services

disk

registry

meterpreter channel

1. slides over Meterpreter channel
2. direct memory injection
3. never hits disk & never hits the registry
4. never starts a service
5. data flows back over existing connection
6. failure doesn’t leave evidence

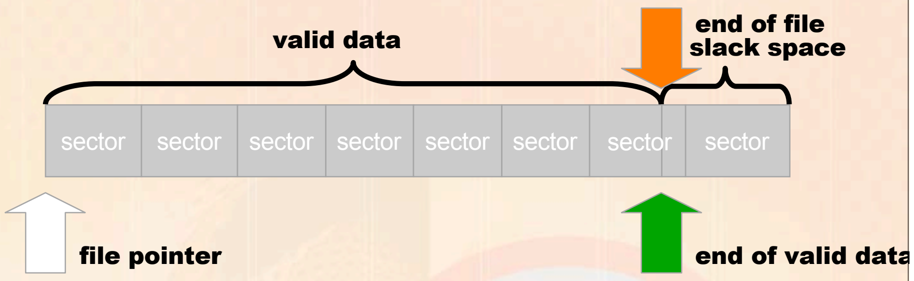


## slacker

- *hiding files in NTFS slack space*
  - *technique*
    - *take advantage of NTFS implementation oddity*
    - *move logical and physical file pointers in certain ways to avoid having data zeroed out*
  - *features*
    - *file hiding*
      - *splitting + slack space hiding*
    - *difficult to detect*

# slacker vs NTFS

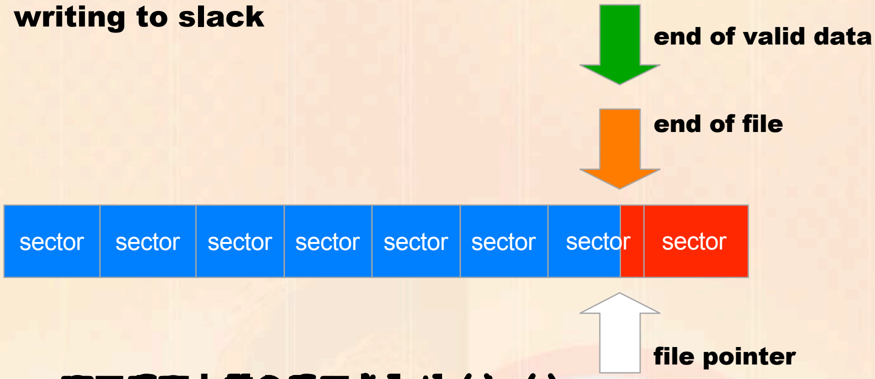
standard file setup



1 cluster (4096b) = 8 sectors (512b)

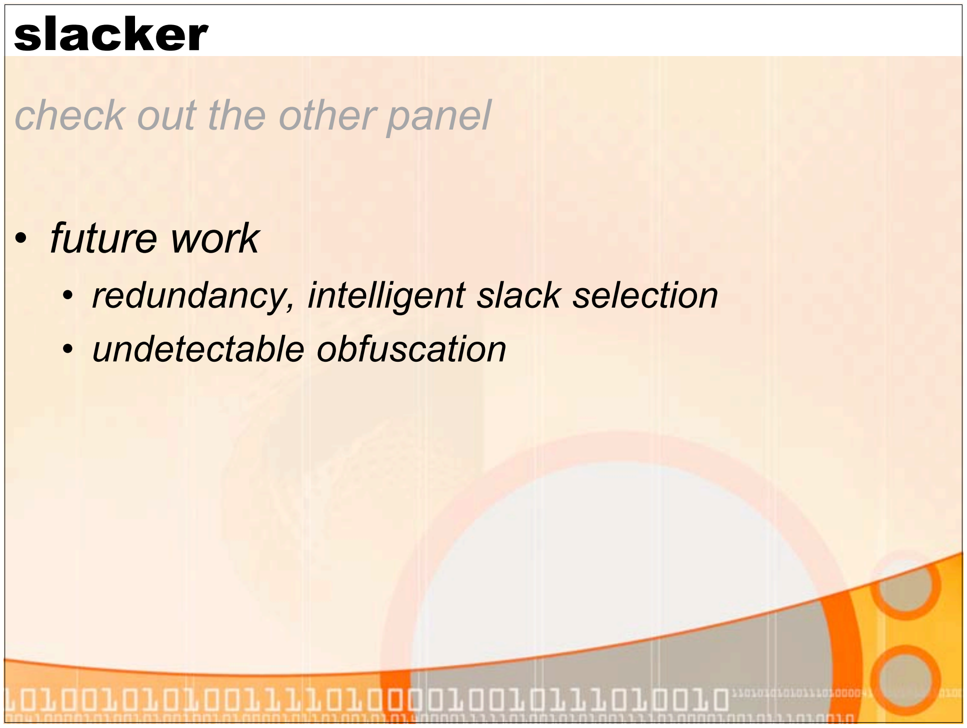
# slacker vs NTFS

writing to slack



[illegible]

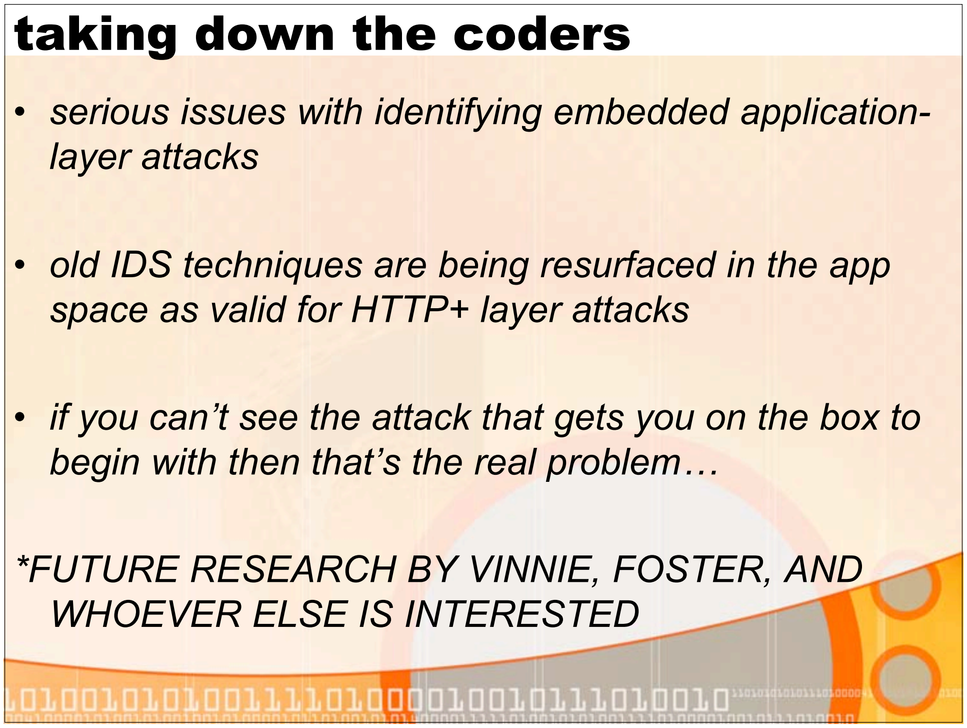
1 cluster (4096b) = 8 sectors (512b)



## slacker

*check out the other panel*

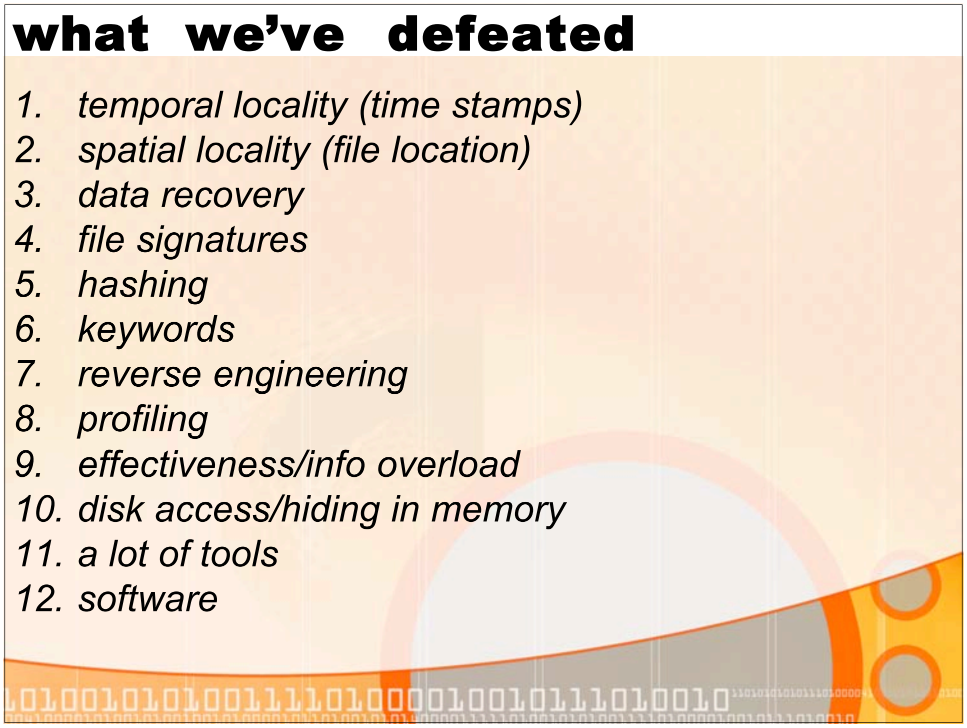
- *future work*
  - *redundancy, intelligent slack selection*
  - *undetectable obfuscation*



## taking down the coders

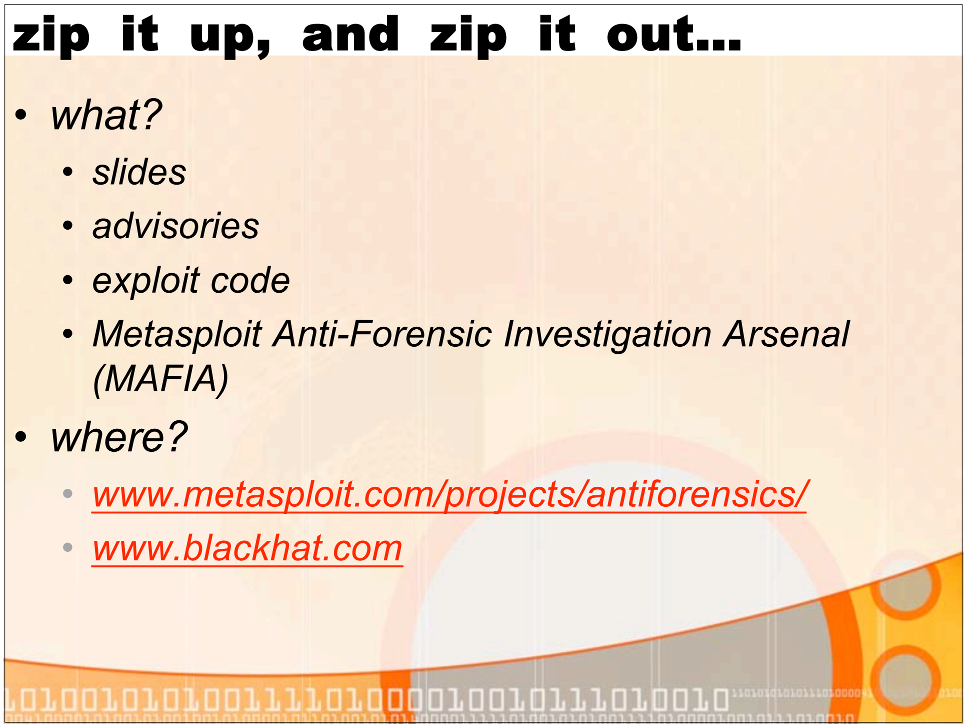
- *serious issues with identifying embedded application-layer attacks*
- *old IDS techniques are being resurfaced in the app space as valid for HTTP+ layer attacks*
- *if you can’t see the attack that gets you on the box to begin with then that’s the real problem…*

**FUTURE RESEARCH BY VINNIE, FOSTER, AND WHOEVER ELSE IS INTERESTED*



## what we've defeated

1. temporal locality (time stamps)
2. spatial locality (file location)
3. data recovery
4. file signatures
5. hashing
6. keywords
7. reverse engineering
8. profiling
9. effectiveness/info overload
10. disk access/hiding in memory
11. a lot of tools
12. software



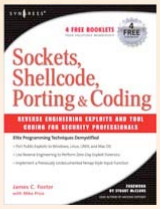
## zip it up, and zip it out…

- what?
  - slides
  - advisories
  - exploit code
  - Metasploit Anti-Forensic Investigation Arsenal (MAFIA)
- where?
  - www.metasploit.com/projects/antiforensics/
  - www.blackhat.com

## ...all questions to be answered at the nearest watering hole

*shoutouts and thanks*

- *muirnin, skape, hdm, optyx, spoonm, thief, ecam, senorpence, tastic, #vax, arimus, oblique, tony B, burnett, asc, j0hnny*


SYNGRESS
4 FREE BOOKLETS
4 FREE
Sockets, Shellcode, Porting & Coding
REVERSE ENGINEERING EXPLOITS AND TOOL CODING FOR SECURITY PROFESSIONALS
Elite Programming Techniques Demystified
James C. Foster
with Mike Price
FOREWORD BY STUART McCLURE

"Shameless plug for Foster and Vinnie's new book"