introducing the...

metasploit antiforensics project

vinnie liu, bluehat

speaker

- *vinnie*
  - *anti-forensics researcher*
  - *framework contributor*
  - *vinnie@metasploit.com*

coverage

- ***weaknesses in current forensic techniques***
- ***break industry tools***
  - *Guidance EnCase, PGP Desktop, NTFS, MS AntiSpyware, Windows Explorer*
- ***Metasploit AF Tools***
  - *timestomp, slacker, transmogrify, sam juicer*
- ***identify opportunities for improvement***

why

- *airing the forensic dirty laundry.*
- *no pressure to innovate in the forensics community.*
- ***too much dependence on forensic tools***

talk format

- *technique*
- *anti-technique*
- *opportunity for improvement, weaknesses, tools, etc...*

#1 timestamps

- *technique*
  - *timestamps hint as to when an event occurred.*
  - *timestamps help an analyst timeline events and profiling hacker behavior.*
  - *if an investigator finds a suspicious file, they will search for other files with similar MAC attributes.*

#1 timestamps

- *anti-technique*
  - *modify file times, log file entries, and create bogus and misleading timestamps*

- *we need better tools…*
  - *most tools only modify the MAC*
  - *ok for FAT, but not for NTFS…*

#1 timestamps

	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

A C M E

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

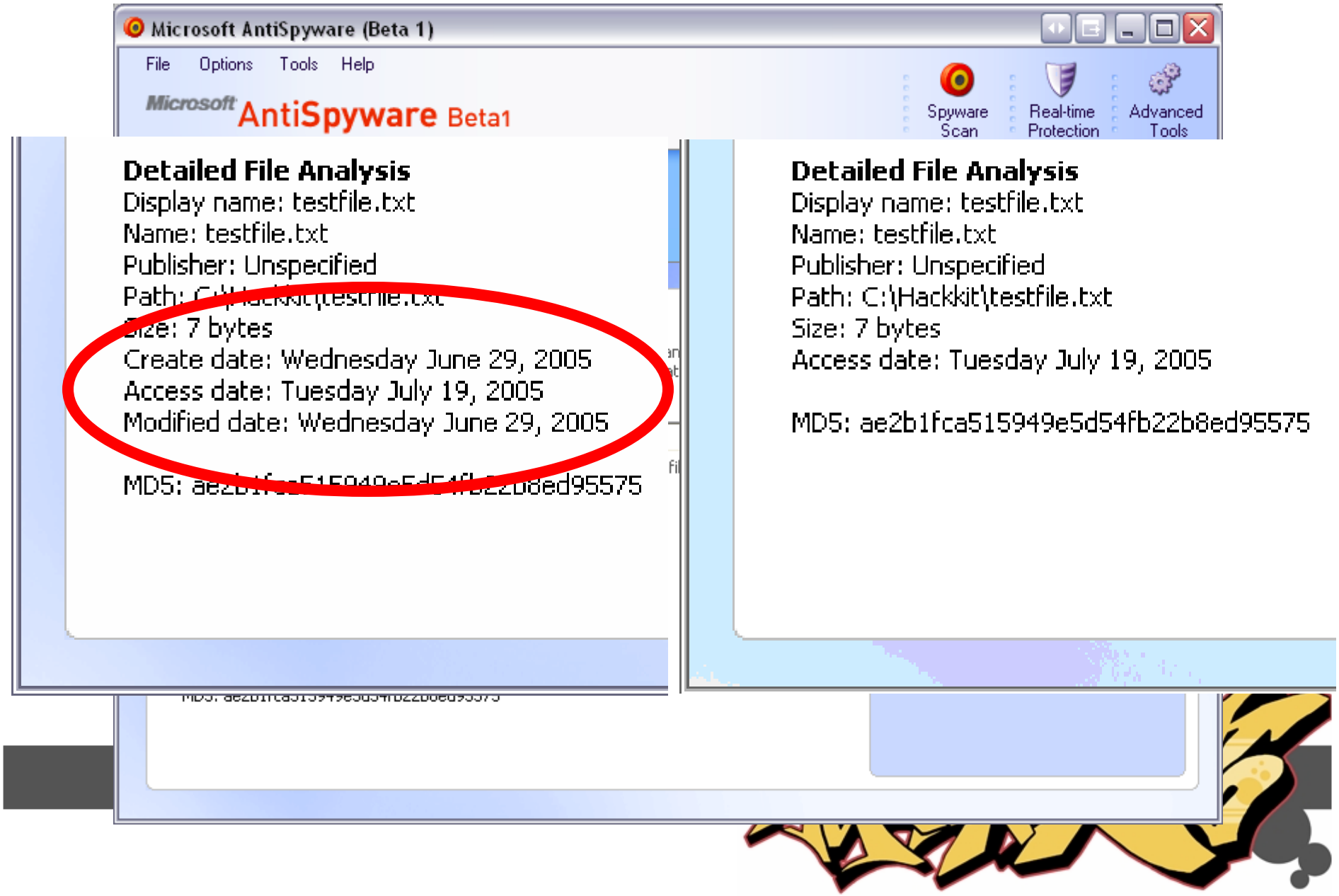
tool #1: timestomp

- ***timestomp***
  - *uses the following Windows system calls:*
    - *NtQueryInformationFile()*
    - *NtSetInformationFile()*
  - *doesn't use*
    - *SetFileTime()*
  - *features:*
    - *display & set MACE attributes*
    - *mess with **EnCase** and **MS Anti-Spyware***

timestomp @ work

	Name	Last Accessed	File Created	Last Written	Entry Modified
62	ODBCINST.INI				
63	iis5.log				
64	comsetup.log				
65	imsins.log				
66	ockodak.log				
67	ocgen.log				
68	mmdet.log				
69	ModemDet.txt				
70	Blue Lace 16.bmp				
71	Soap Bubbles.bmp				
72	Coffee Bean.bmp				
73	FeatherTexture.bmp				
74	Gone Fishing.bmp				
75	Greenstone.bmp				
76	Prairie Wind.bmp				
77	Rhododendron.bmp				
78	River Sumida.bmp				
79	Santa Fe Stucco.bmp				
80	Zapotec.bmp				
81	vb.ini				
82	vbaddin.ini				
83	COM+.log				
84	folder.htt				
85	desktop.ini				

timestomp @ work



timestomp @ work

- *Windows Explorer Demo*

opportunity for improvement

- *current state*
  - *EnCase only uses the Standard Information Attribute (SIA)*

MFT Entry Header	SIA Attribute MACE	FN Attribute MACE	Remaining Attributes…

- *opportunity for improvement*
  - *use the Filename (FN) attribute*

opportunity for improvement

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

...but we can bypass that too

- *anti-validation technique*
  - *system files and archives are false positives*
  - *use raw disk i/o to change the FN MACE values*
    - *$MFT is a file*
    - *calculate offsets from the start of the MFT to a file's FN MACE values*
    - ***may cause file system instability***

...but we can bypass that too

- *anti-validation technique*
  - *use a file that's not been used in a while, delete the $data attribute and fill it with your own data*
    - *no creating, no moving means no FN updates*
    - *only the SIA changes & SIA is controllable*

MFT Entry Header	SIA Attribute MACE	FN Attribute MACE	Data Attribute

#2 location, location, location

- *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, browser temp, AV/spyware*

#3 undelete

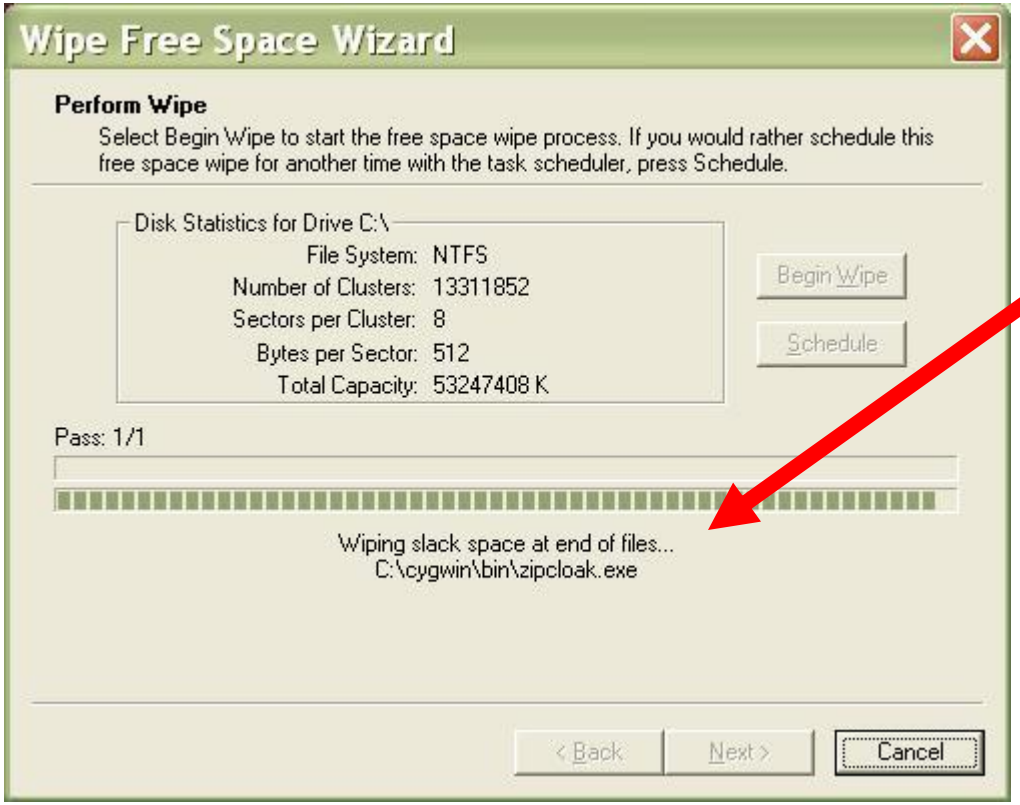
- *technique*
  - *forensics tools will make a best effort to reconstruct deleted data*

- *anti-technique*
  - *secure file deletion*
    - *filename, file data, MFT record entry*
  - *wipe all slack space*
  - *wipe all unallocated space*

#3 undelete

- *tools*
  - *Sys Internals – sdelete.exe*
    - *doesn't clean file slack space*
  - *Eraser (heide)*
    - *does clean file slack space*
  - *PGP Desktop's Disk Wipe*
    - *privacy concerns*
- *vulnerabilities*
  - *PGP Desktop's Disk Wipe*

snake oil



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

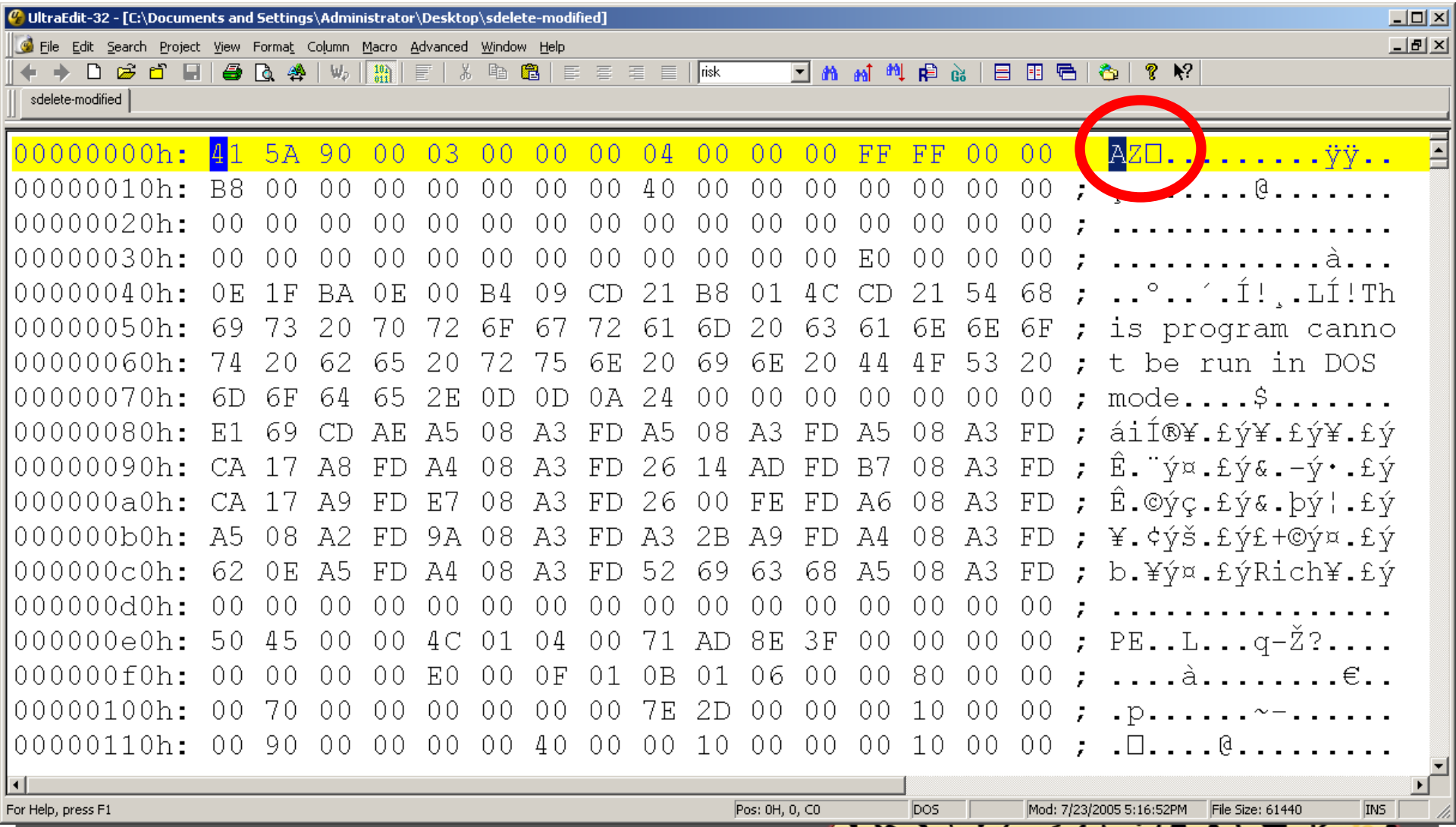
not so private...

#4 signature analysis

- *technique*
  - *EnCase has two methods for identifying file types*
    - *file extension*
    - *file signatures*

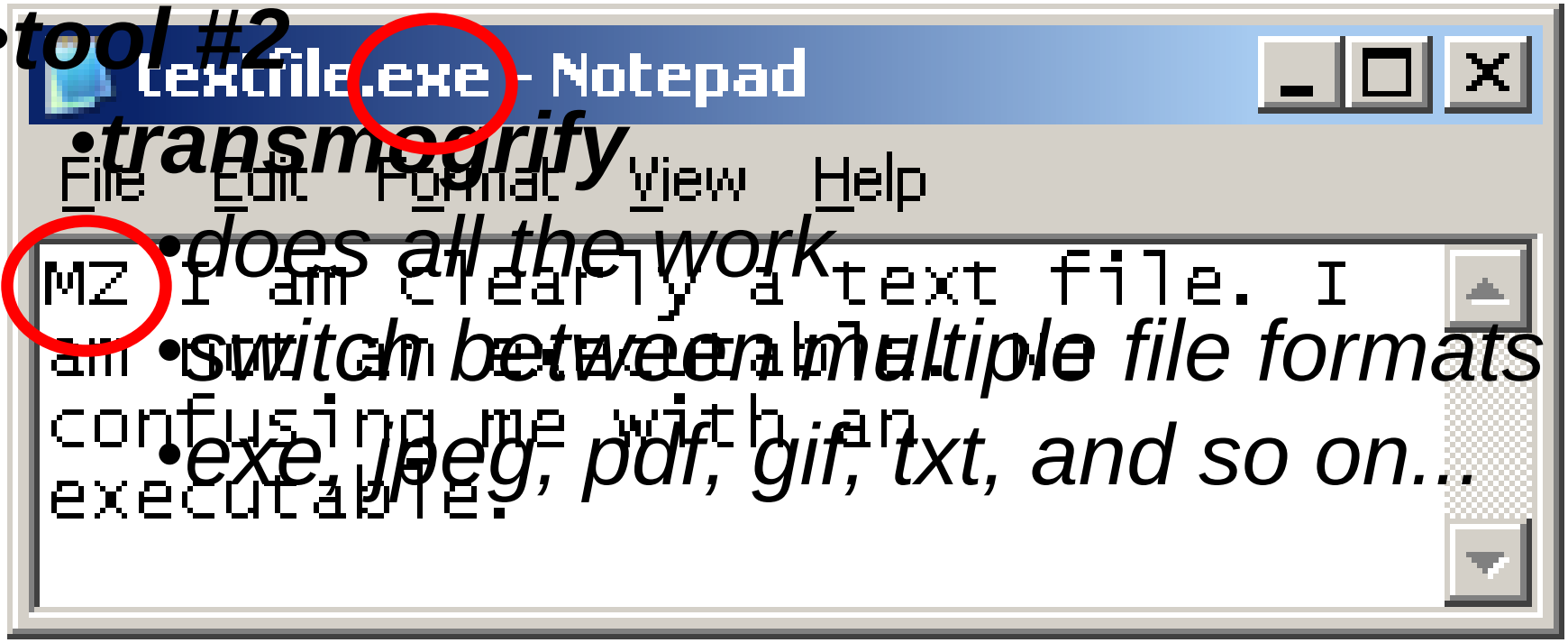
- *anti-technique*
  - *change the file extension*
  - *changing file signatures to avoid EnCase analysis*

foiling signature analysis



...flip it and reverse it

- *tool #2*
  - *transmogrify*
    - *does all the work*
    - *switch between multiple file formats*
      - *exe, jpeg, pdf, gif, txt, and so on...*



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

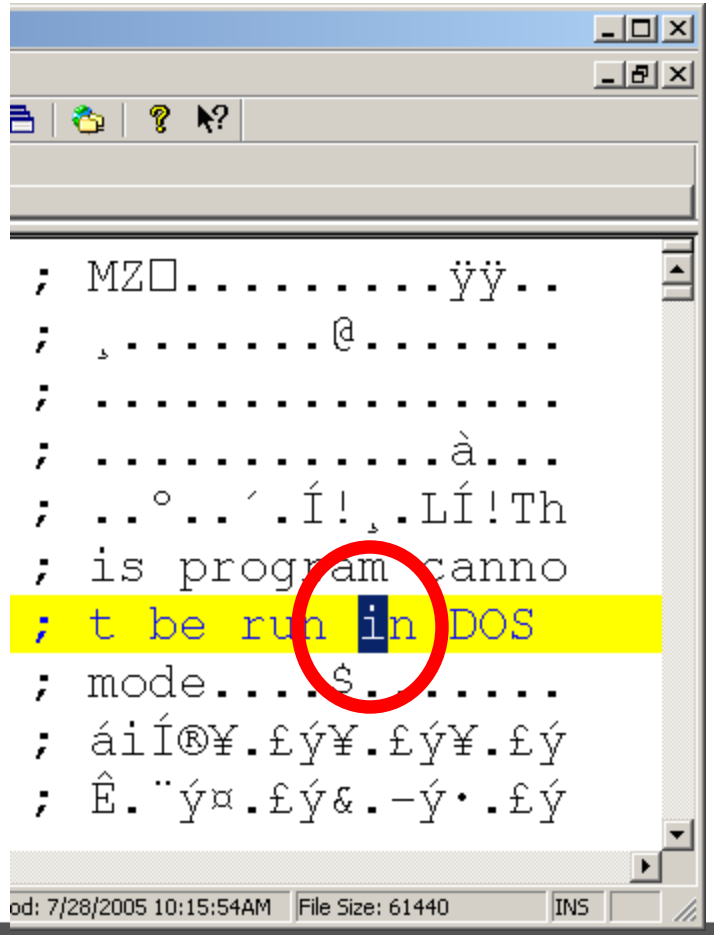
#5 hashing

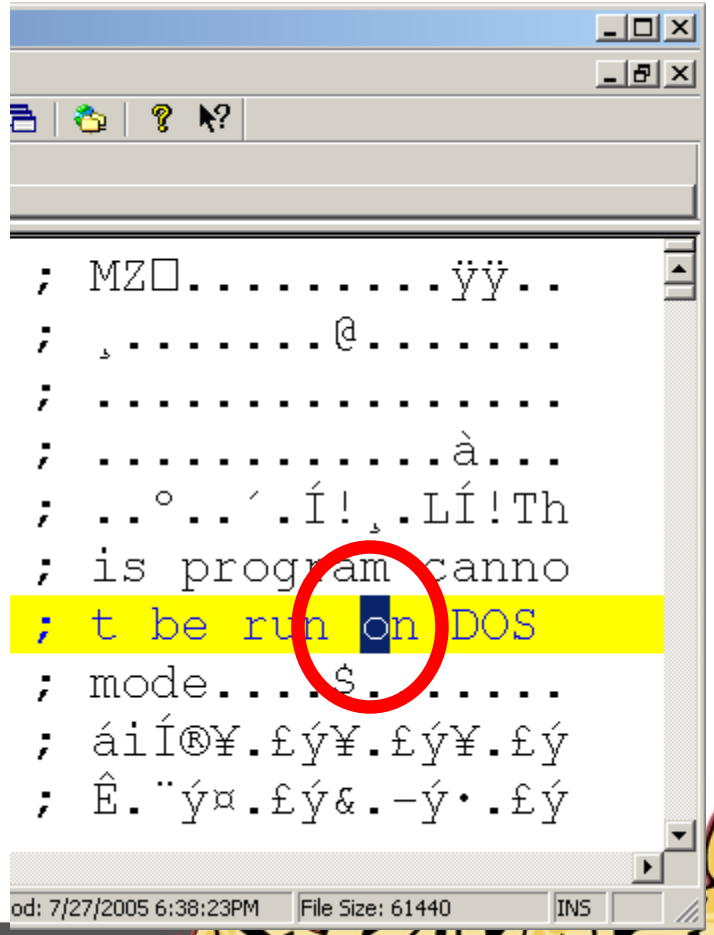
- *technique*
  - *to minimize search scope and analysis time*
  - *create an MD5 fingerprint of all files on a system*
  - *compare to lists of **known good** & **known bad** file hashes*

- *anti-technique*
  - *modify and recompile*
    - *remove usage information*
  - *stego works on non-executables as well as executables*
  - *direct binary modification*

#5 hashing

- [illegible]


; MZ□.....ÿÿ..
; ¸.....@.....
; ....
; .....à...
; ..°..´.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...
; ..°..´.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

#6 keyword searching

- *technique*
  - *analysts build lists of keywords and search through files, slack space, unallocated space, and pagefiles*
- *anti-technique*
  - *exploit the examiner's **lack of language skill***
- *opportunity for improvement*
  - *predefined keyword lists in different languages*

#7 reverse engineering

- *technique*
  - *99% of examiners can't code*
  - *possess rudimentary malware analysis skills if any*
    - *binary compression (packer) identification*
    - *commonly available unpackers*
    - *run strings*
    - *behavioral analysis*
- *anti-technique*
  - *use uncommon packers or create a custom loader*
    - *PEC2*
  - *packing strategy*

#8 profiling

- *technique*
  - *analysts find commonalities between: tools, toolkits, packers, language, location, timestamps, usage info, etc…*

- *anti-technique*
  - *use what's already in your environment*

#9 information overload

- *technique*
  - *forensics takes time, and time costs money*
  - *businesses must make business decisions, again this means money*
  - *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*

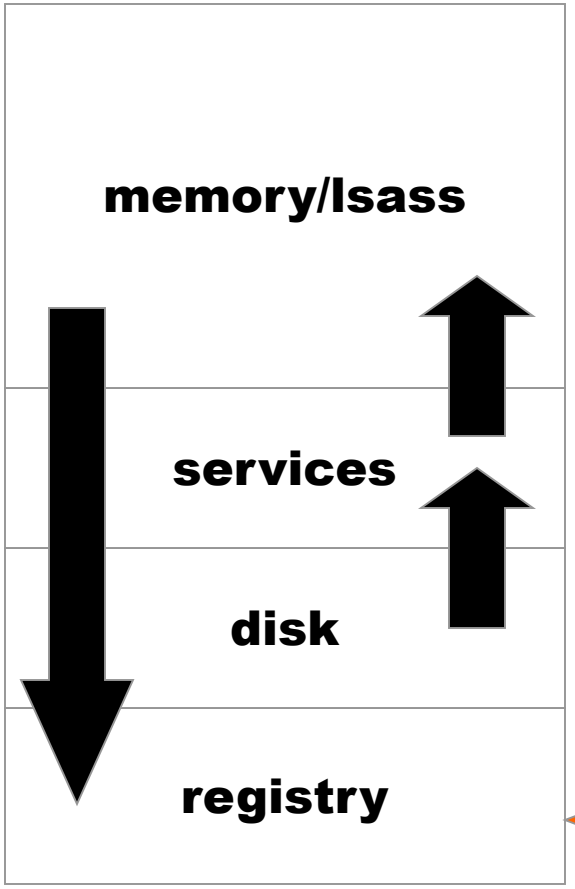
#10 hiding in memory

- *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*

tool #3: sam juicer

- ***sam juicer***
  - *grab the password hashes from the SAM*
  - *built from the ground up, real-world implementation*
  - *oooooohhh, stealthy!*
  - *tool name sucks*

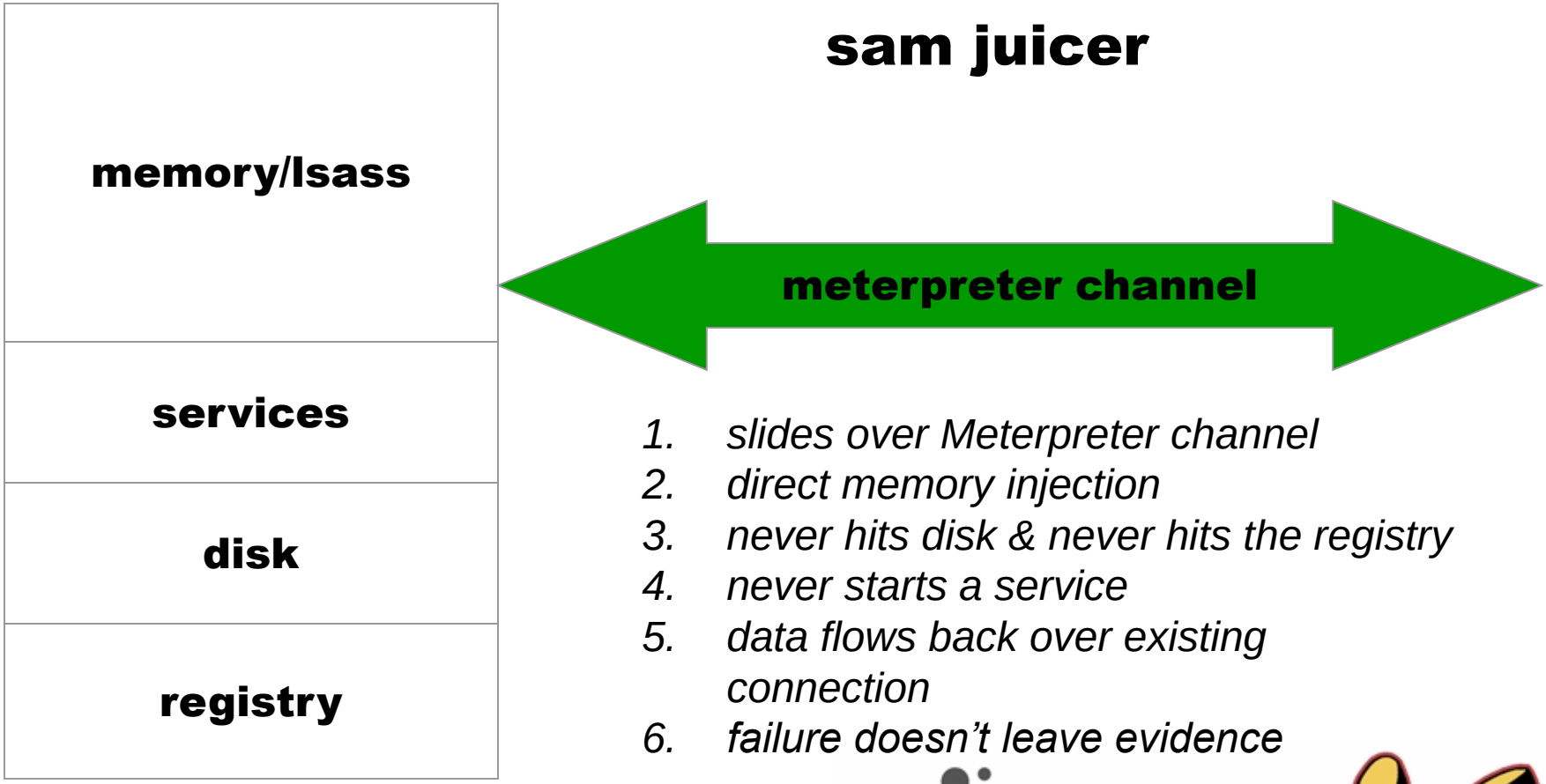
tool #3: pwdump is no good



current state of tools

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*

tool #3: the juice is good



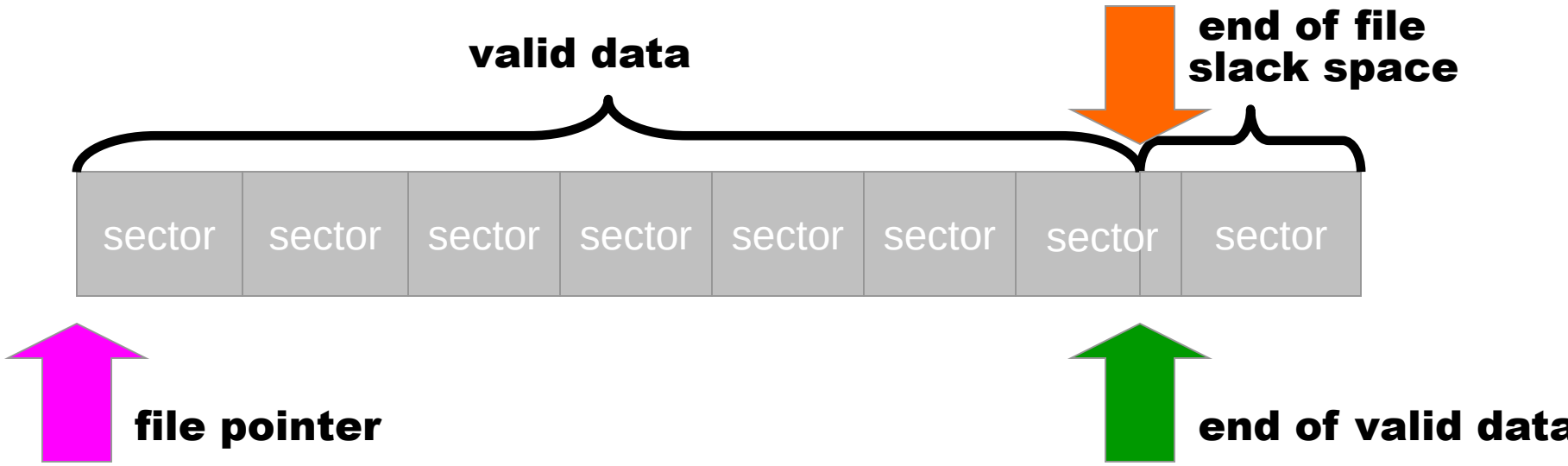
1. *slides over Meterpreter channel*
2. *direct memory injection*
3. *never hits disk & never hits the registry*
4. *never starts a service*
5. *data flows back over existing connection*
6. *failure doesn't leave evidence*

tool #4: 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 splitting*
    - *multiple selection techniques*
    - *obfuscation*

tool #4: slacker

standard file setup



1 cluster = 8 sectors

tool #4: slacker

writing to slack

1 cluster = 8 sectors

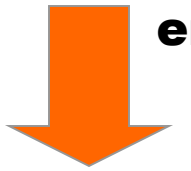
tool #4: slacker

reading from slack

`SetEndOfFile()`

`SetFilePointer()`

end of valid data

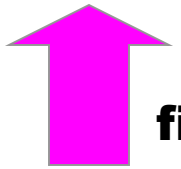


end of file

`ReadFile()`

`SetFilePointer()`

`SetFileValidData()`

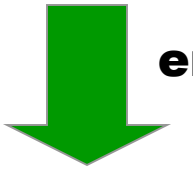


file pointer

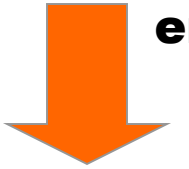
1 cluster = 8 sectors

tool #4: slacker

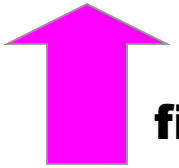
closing out



end of valid data



end of file



file pointer

SetEndOfFile()

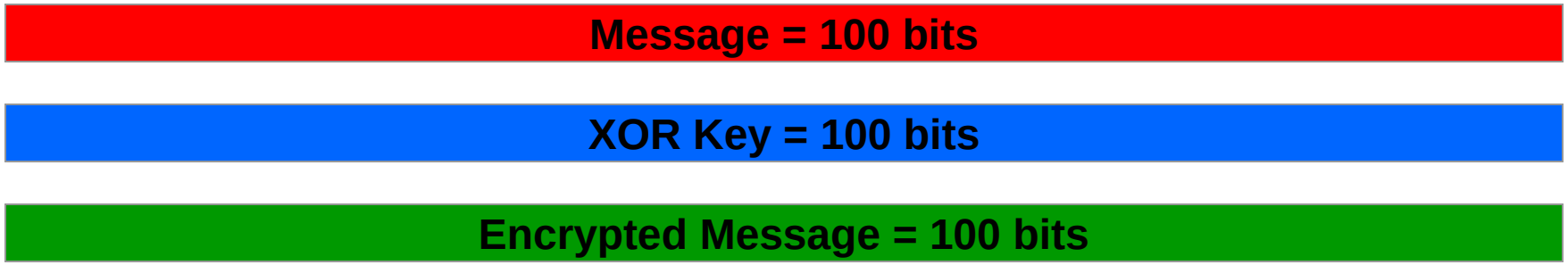
1 cluster = 8 sectors

tool #4: slacker

- *selection*
  - *dumb*
    - *first N files that have enough combined slack space*
  - *random*
    - *random selection of files in a directory*
  - *intelligent*
    - *selects the oldest files in a directory*
  - *each flavor also available with recursion*

tool #4: slacker

- *obfuscation*
  - *none*
  - *xor key*
    - *random 8 bit key repeated over all data*
  - *one-time pad*



tool #4: slacker

- *one-time pad (sort of...)*
  - *strength relies on a truly random xor key of equal length to the message*
  - *by using a file...*
    - *we avoid generating a an xor key*
    - *we avoid having to store it anywhere*
    - *because its already on the system*
  - *BUT, it's not truly random*
  - *EVEN SO, good luck trying to figure out which series of 1s and 0s on your hard drive I chose.*

tool #4: slacker

- *Normally, this is where I demo slacker.*
- *but my $20k USB dongle for EnCase was “reposessed”.*

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*

more information

- *what?*
  - *slide decks*
  - *Metasploit Anti-Forensic Investigation Arsenal (MAFIA)*

- *where?*
  - *www.metasploit.com/projects/antiforensics/*

thanks microsoft

questions

comments

suggestions

vinnie@metasploit.com