STACH&LIU

Defeating Forensic Analysis

CEIC 2006 – Technical Lecture 1

Thursday, May 4 – 10:30 am to 11:30 am

Presented by Vincent Liu and Patrick Stach

STACH&LIU

Welcome

- Vincent Liu
  - Managing Director, Stach & Liu
  - Researcher, Metasploit Project
  - Former Fortune 100, Big 4 consulting, and government intel
  - vliu@stachliu.com

- Patrick Stach
  - Director of Research and Development, Stach & Liu
  - Researcher & Developer, Metasploit Project
  - Former security industry developer and freelance consultant
  - pstach@stachliu.com

STACH&LIU

Agenda

- Weaknesses in current forensic analysis tools and techniques
- Metasploit Anti-Forensics Tools
- Specific recommendations on how to improve

STACH&LIU

Rapid History

- Basic Utilities
  - touch
  - mv and rename
  - rm and del
- Repurpose Existing Technologies
  - ADS, encryption, Gutmann secure deletion (Eraser)
- Targeted Research into Anti-Forensics
  - Metasploit Anti-Forensics Project
  - Deflier's Toolkit
  - Conferences: BlackHat, BlueHat, ToorCon, and now CEIC

Defeating Timestamps

- Technique
  - Examine timestamps for temporal locality
- Anti-technique
  - touch for UNIX & MAC in FAT
  - MACE in NTFS
    - timestomp.exe from the Metasploit Anti-Forensics Project
    - NtQueryInformationFile() and NtSetInformationFile()

STACH&LIU

Defeating 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**)*

Defeating EnCase

- **normal**

AUTOEXEC.BAT	06/30/05 11:57:13AM	12/02/04 09:43:29AM	12/02/04 09:43:29AM	12/02/04 09:43:29AM

- **after setting values (-z “Monday 05/05/2005 05:05:05 AM”)**

AUTOEXEC.BAT	05/05/05 05:05:05AM	05/05/05 05:05:05AM	05/05/05 05:05:05AM	05/05/05 05:05:05AM

- **example EnCase weakness (-b)**

AUTOEXEC.BAT				

STACH&LIU

Defeating EnCase

	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

STACH&LIU

Defeating EnCase

	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				

STACH&LIU

Defeating MS Antispyware

Microsoft AntiSpyware (Beta 1)

File Options Tools Help

Microsoft AntiSpyware Beta1

Spyware Scan | Real-time Protection | Advanced Tools

Advanced Tools | Advanced File Analyzer | Back to Advanced Tools

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.

Browse... 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
Create date: Wednesday June 29, 2005
Access date: Tuesday July 19, 2005
Modified date: Wednesday June 29, 2005

MD5: ae2b1fca515949e5d54fb22b8ed95575

Quick File Profile

testfile.txt
testfile.txt

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

Defeating MS Antispyware

Detailed File Analysis
Display name: testfile.txt
Name: testfile.txt
Publisher: Unspecified
Path: [illegible]
Size: 7 bytes
Create date: Wednesday June 29, 2005
Access date: Tuesday July 19, 2005
Modified date: Wednesday June 29, 2005

MD5: [illegible]

Detailed File Analysis
Display name: testfile.txt
Name: testfile.txt
Publisher: Unspecified
Path: [illegible]
Size: 7 bytes
Access date: Tuesday July 19, 2005

MD5: ae2b1fca515949e5d54fb22b8ed95575

Defeating Windows

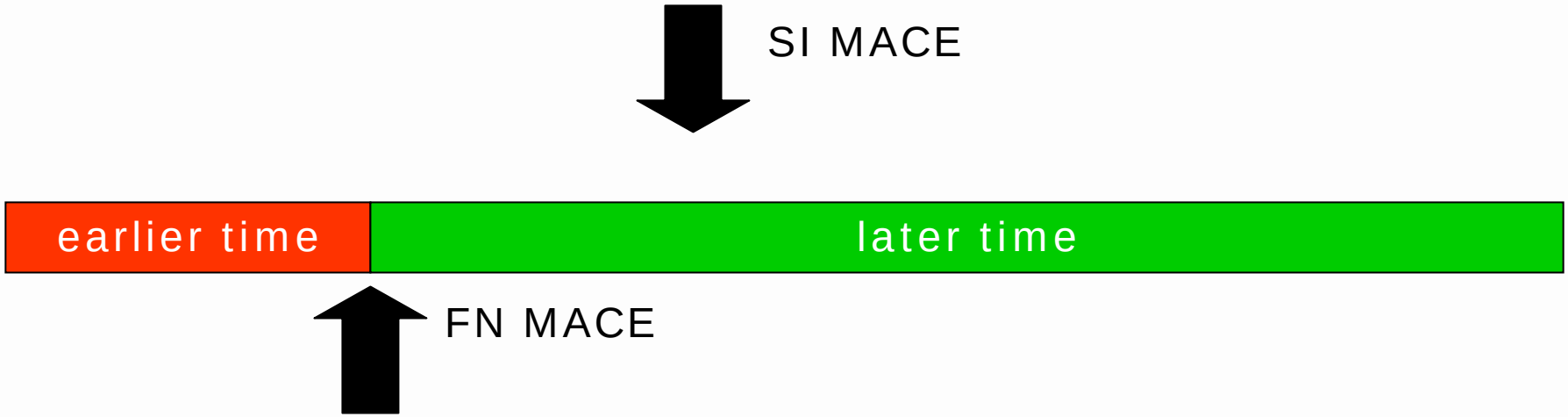
Live Windows Explorer Demo

Improving Timestamps

Entry Header	SI Attribute MACE	FN Attribute MACE	Other Attributes ...

- Every file stores MACE values in more than one attribute!
- Standard Information (SI)
  - Currently used by EnCase and other tools.
- Filename (FN)
  - Not used by EnCase or other tools.

Improving Timestamps



1. MACE values always updated in SI.
2. MACE values only updated in FN when a file is created and/or moved.
3. Therefore, MACE values from FN should always be older when compared to the SI values.

Anti-counter Anti-technique

Entry Header	SI Attribute	FN Attribute	Other ...
Entry Header	SI Attribute	FN Attribute	Other ...
...	...	...	...

- Modify the Filename (FN) attribute
  - Calculate the offsets
  - Modify via raw disk I/O.
- Modify the Data attribute
  - Swap out the data.
  - Timestomp it back.

Defeating Signature Analysis

- Two Detection Techniques
  - File extensions
  - File signatures
- Anti-detection Technique
  - Change the file extension
  - Change the file signature

STACH&LIU

Defeating Signature Analysis

Signature	Hash Value	Name	File Ext	File Type
Match	4e65745d42c70ac0a5f697e22b8bb033	sdelete.exe	exe	Windows Executable
Match	4e65745d42c70ac0a5f697e22b8bb033	sdelete-modified.exe	exe	Windows Executable

STACH&LIU

Defeating Signature Analysis

UltraEdit-32 - [C:\Documents and Settings\Administrator\Desktop\sdelete-modified.exe]

File Edit Search Project View Format Column Macro Advanced Window Help

sdelete-modified.exe

```
00000000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 ; MZ□.........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 ; .□....@.........
```

Pos: 0H, 0, C0 | DOS | Mod: 2/28/2005 10:51:41PM | File Size: 61440 | INS

STACH&LIU

Defeating 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

```
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 ; ..°..´.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 ; .□....@.........
```

For Help, press F1 | Pos: 0H, 0, C0 | DOS | Mod: 7/23/2005 5:16:52PM | File Size: 61440 | INS

STACH&LIU

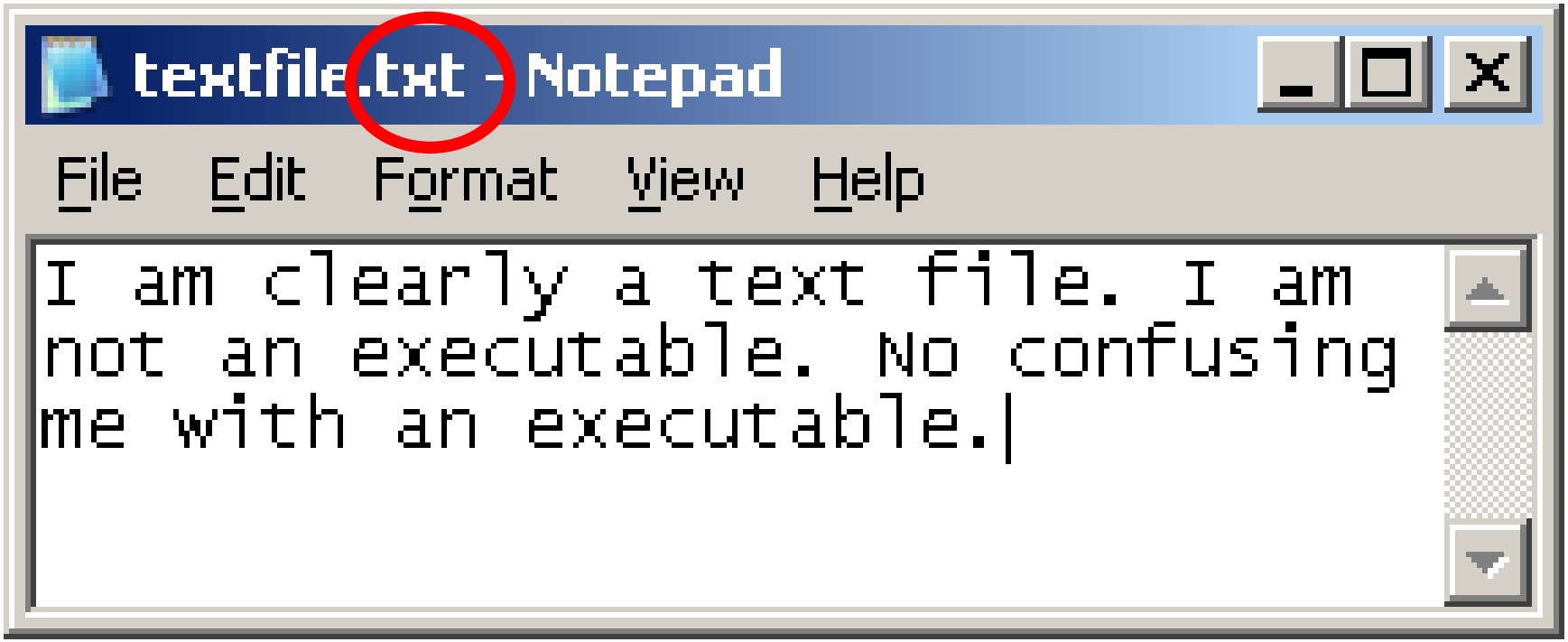
Defeating Signature Analysis

Signature	Hash Value	Name	File Ext	File Type
Match	4e65745d42c70ac0a5f697e22b8bb033	sdelete.exe	exe	Windows Executable
Match	4e65745d42c70ac0a5f697e22b8bb033	sdelete-modified.exe	exe	Windows Executable

- one byte modified

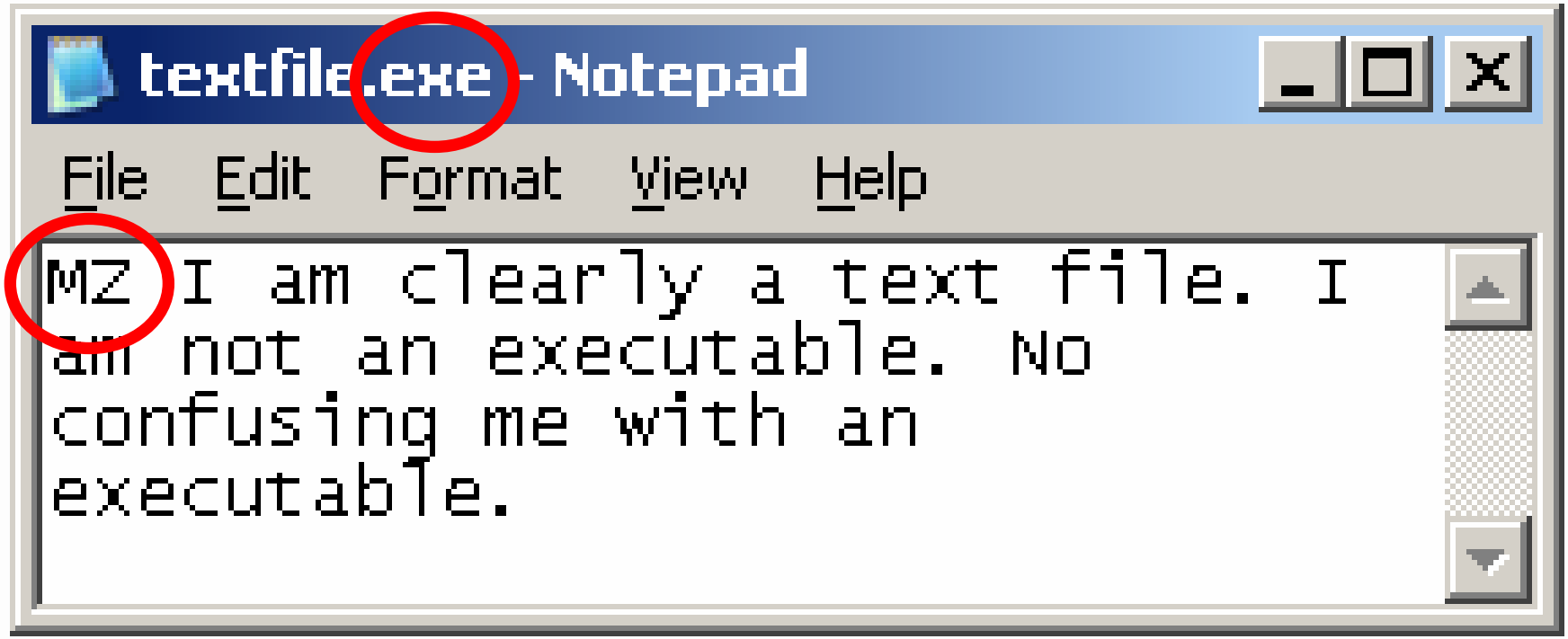
Signature	Hash Value	Name	File Ext	File Type
Match	4e65745d42c70ac0a5f697e22b8bb033	sdelete.exe	exe	Windows Executable
Unknown	a9fb4408297bb43ebc0a219d0d5a94f5	sdelete-modified		

Defeating Signature Analysis



	Name	File Ext	File Type	Signature
20	textfile.txt	txt	Text	Match

Defeating Signature Analysis

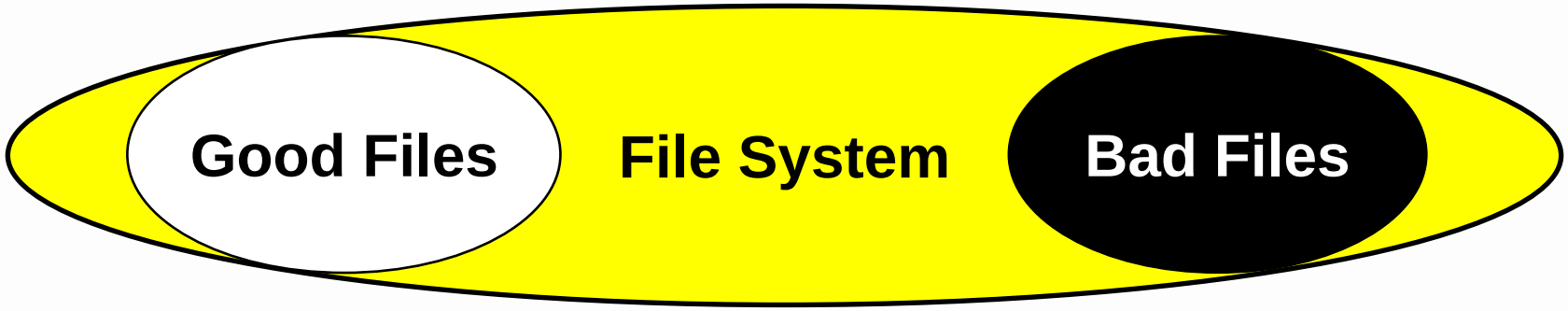


	Name	File Ext	File Type	Signature
21	textfile.exe	exe	Windows Executable	Match

Improving Signature Analysis

- Perform statistical analysis against headers & footers.
  - PE/ELF binary headers have a fixed format/structure.
  - Data for JPEG, GIF, and other have repeatable patterns.
- Perform file content analysis
  - Text files usually ASCII text.
- Open the file ☺

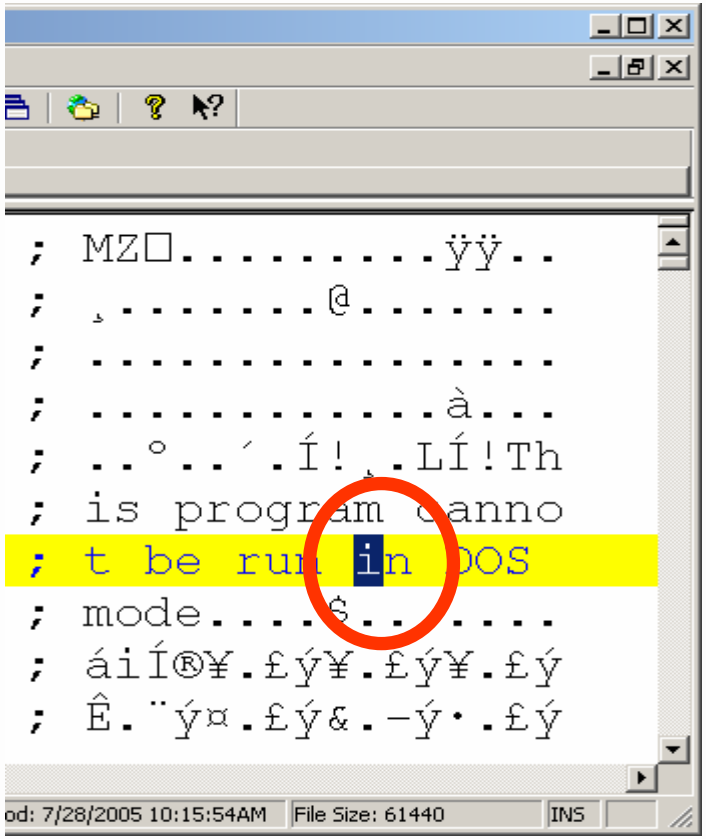
Defeating Hashing

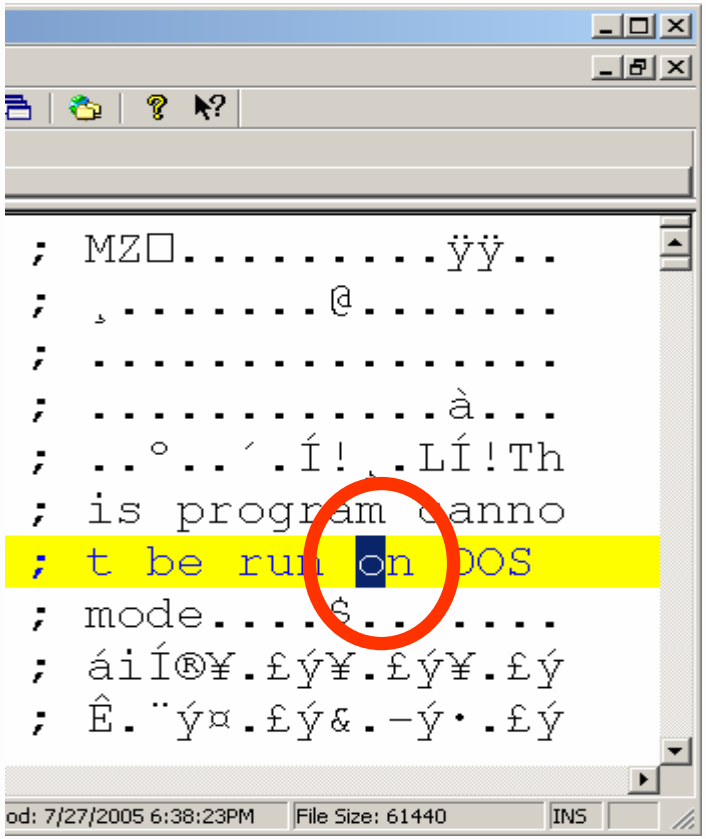


- Technique
  - Identify known good files with hashing white lists and known bad files with black lists
  - Identify known bad files with hashing black lists
  - Examine the remaining files
- Anti-technique
  - Get off of the black list
  - Get on the white list

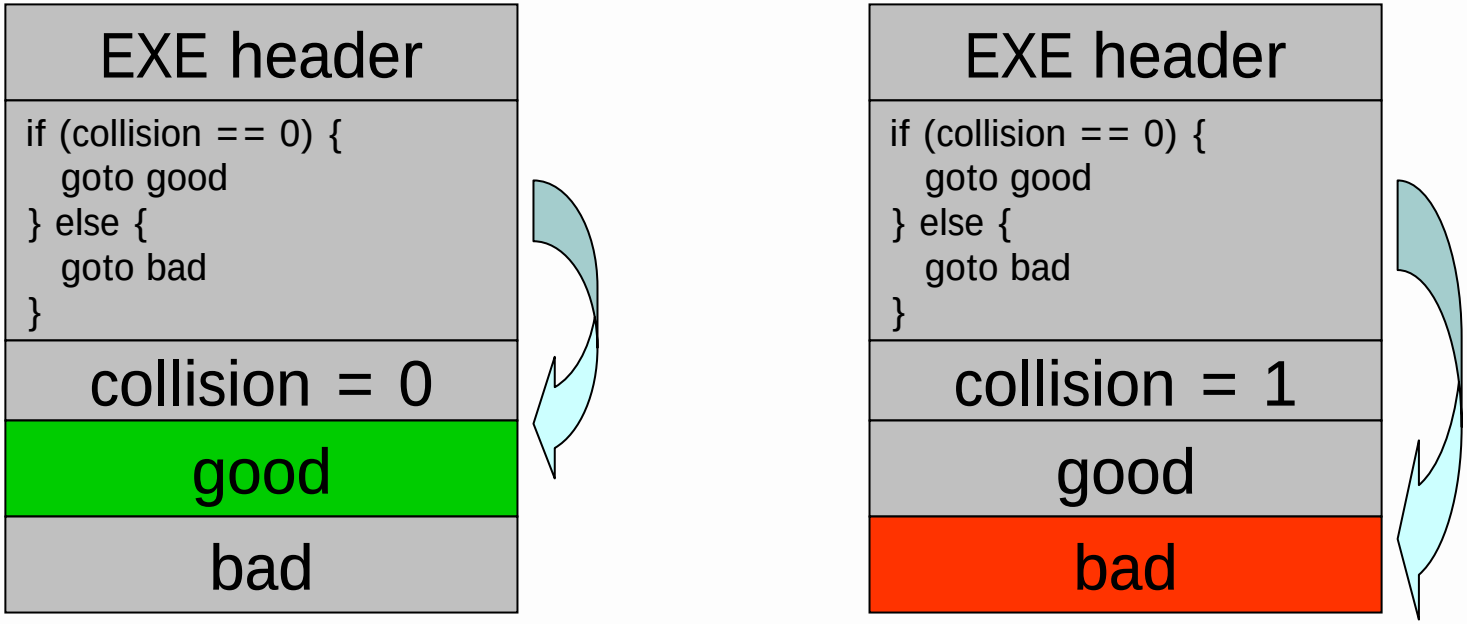
Defeating Hashing

4e65745d42c70ac0a5f697e22b8bb033
eafcc942c7960f921c64c1682792923c





Defeating Hashing



- **We can generate hash collisions in MD4, MD5 (public)**
- **We can generate hash collisions in SHA1 (not public)**

Defeating Hashing

Live Executable Collision Demo

STACH&LIU

Improving Hashing

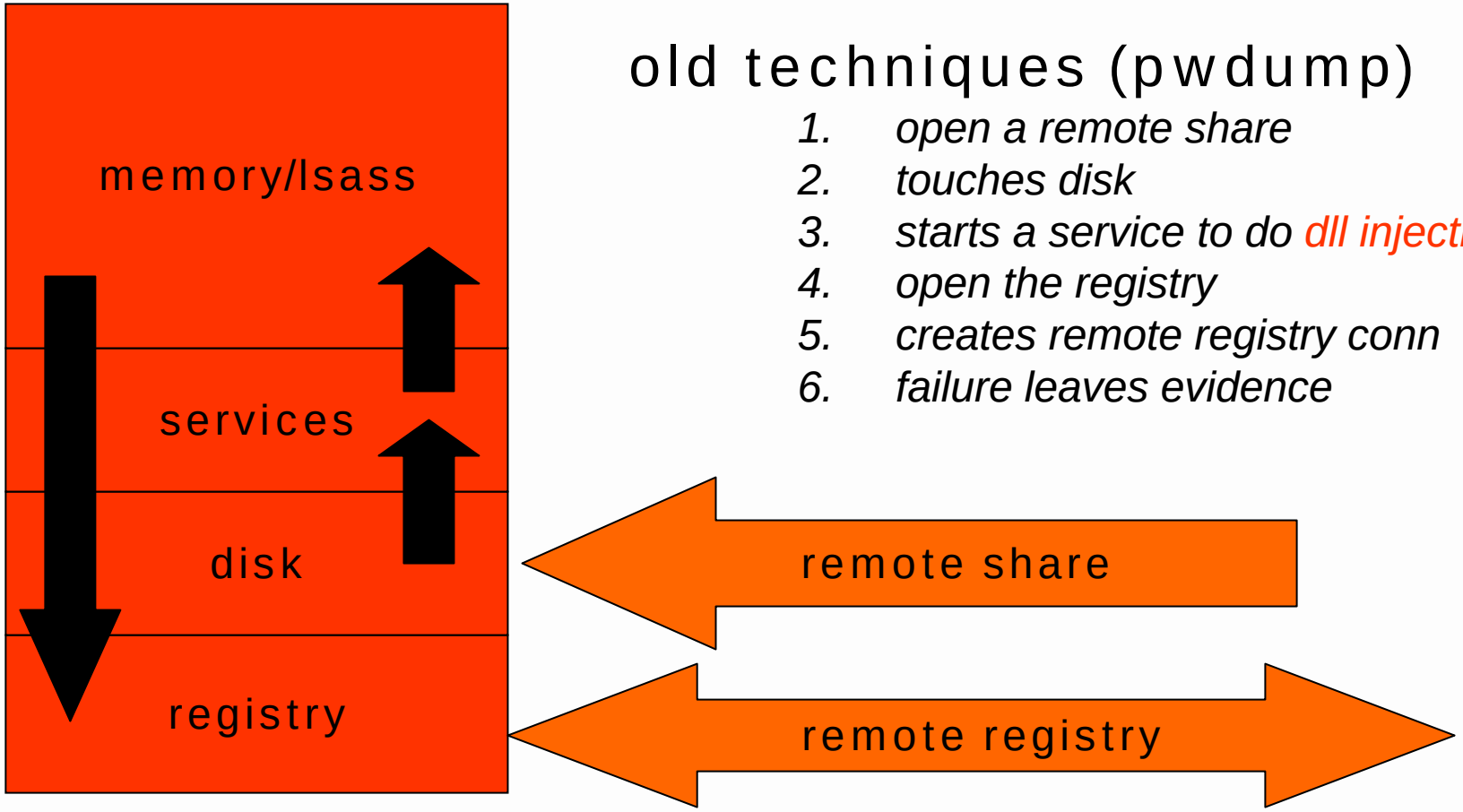
- Use only trusted hash white lists
- Don’t rely on black lists to find bad files
- Perform bit-by-bit file comparisons
- Stack multiple hashing algorithms

http://www.stachliu.com/collision.html

Defeating Disk Analysis

- Technique
  - Capture everything on disk and analyze
  - Capture list of active processes, open files, open ports, etc…
- Anti-technique
  - Never touch the disk,
  - Never open a new port
  - Never open a file
  - Never create a new process
  - And so on…

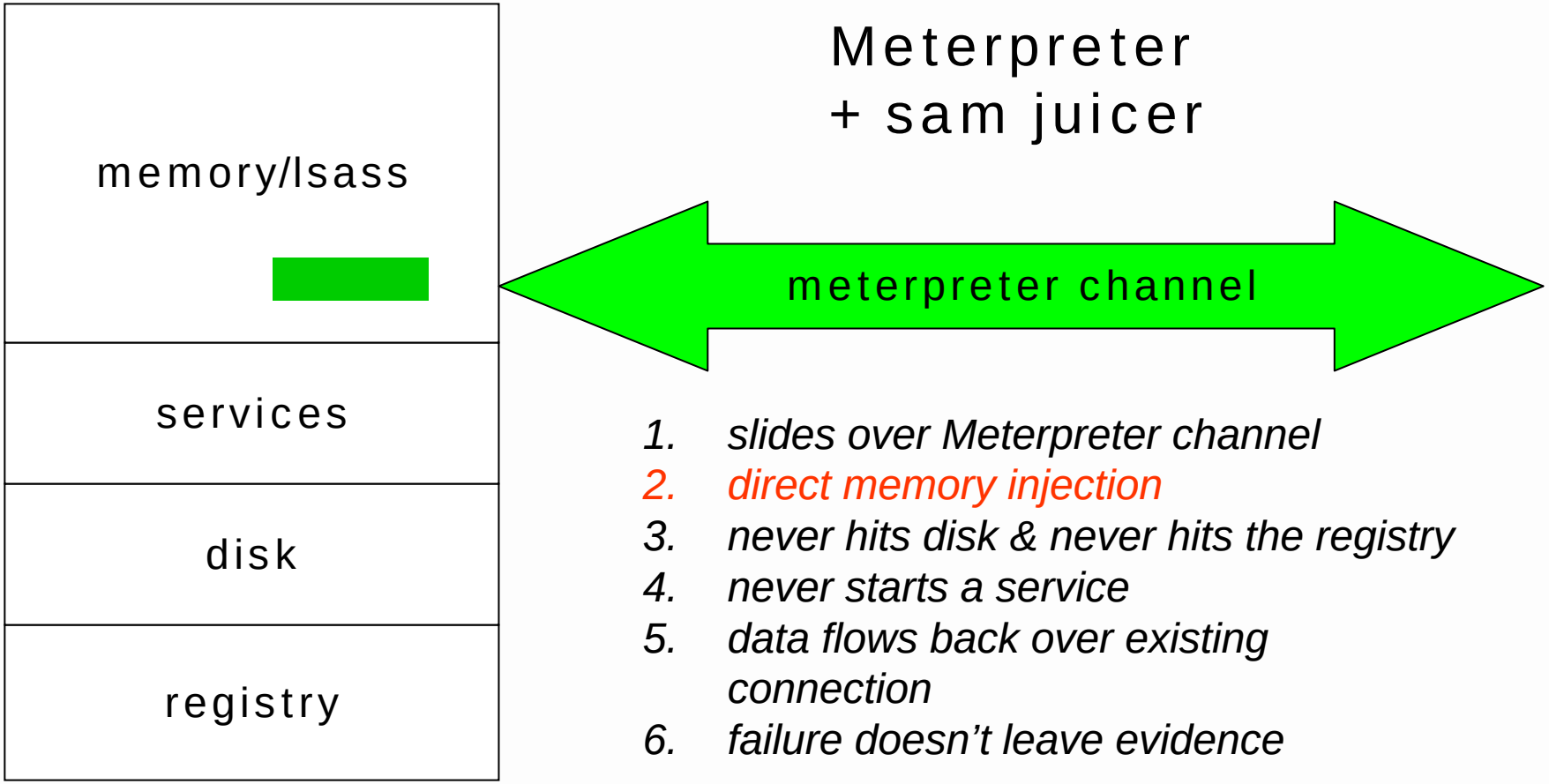
Defeating Disk Analysis



old techniques (pwdump)

1. *open a remote share*
2. *touches disk*
3. *starts a service to do dll injection*
4. *open the registry*
5. *creates remote registry conn*
6. *failure leaves evidence*

Defeating Disk Analysis



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*

STACH&LIU

Improving Disk Analysis

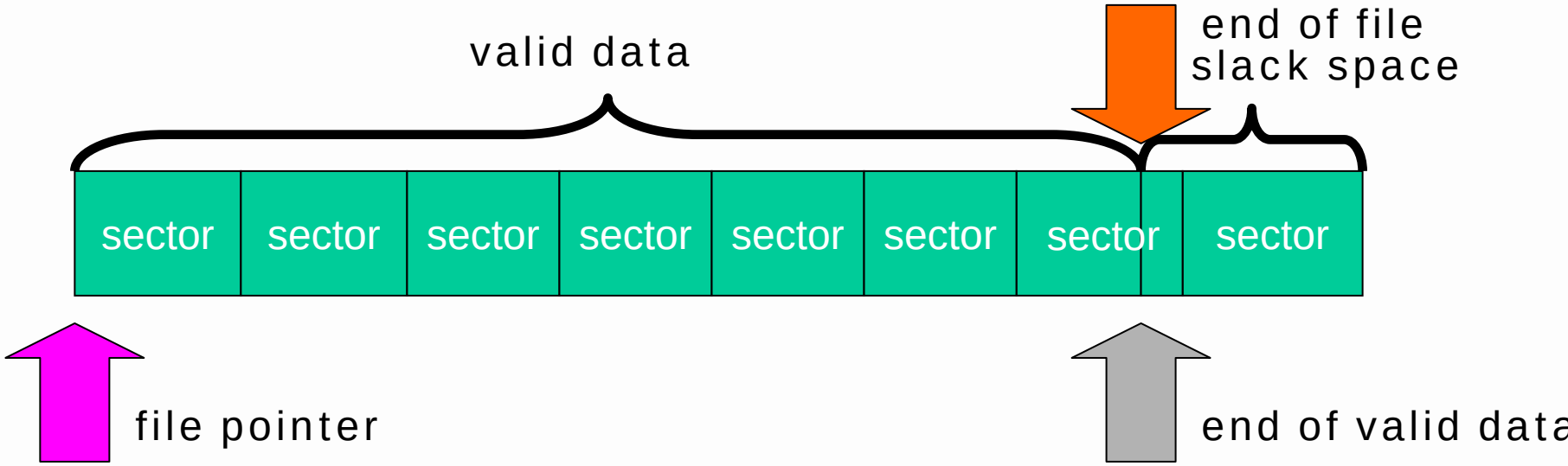
- Capture live system information
  - lsof, netstat, dd, ifconfig
- Capture live memory information
  - memparser, kntlist, Windows Memory Forensic Toolkit
  - Immature technologies that can be subverted
- Use trusted external hardware to verify
  - CoPilot – expensive, use on mission critical systems

Hiding in Slack Space

- Technique
  - Analyze the existing file system for information
  - Look for file fragments in slack space
- Anti-technique
  - Leverage an NTFS implementation oddity
  - Avoid NTFS zeroing your data
  - Store a larger file in smaller slack space areas

Hiding in Slack Space

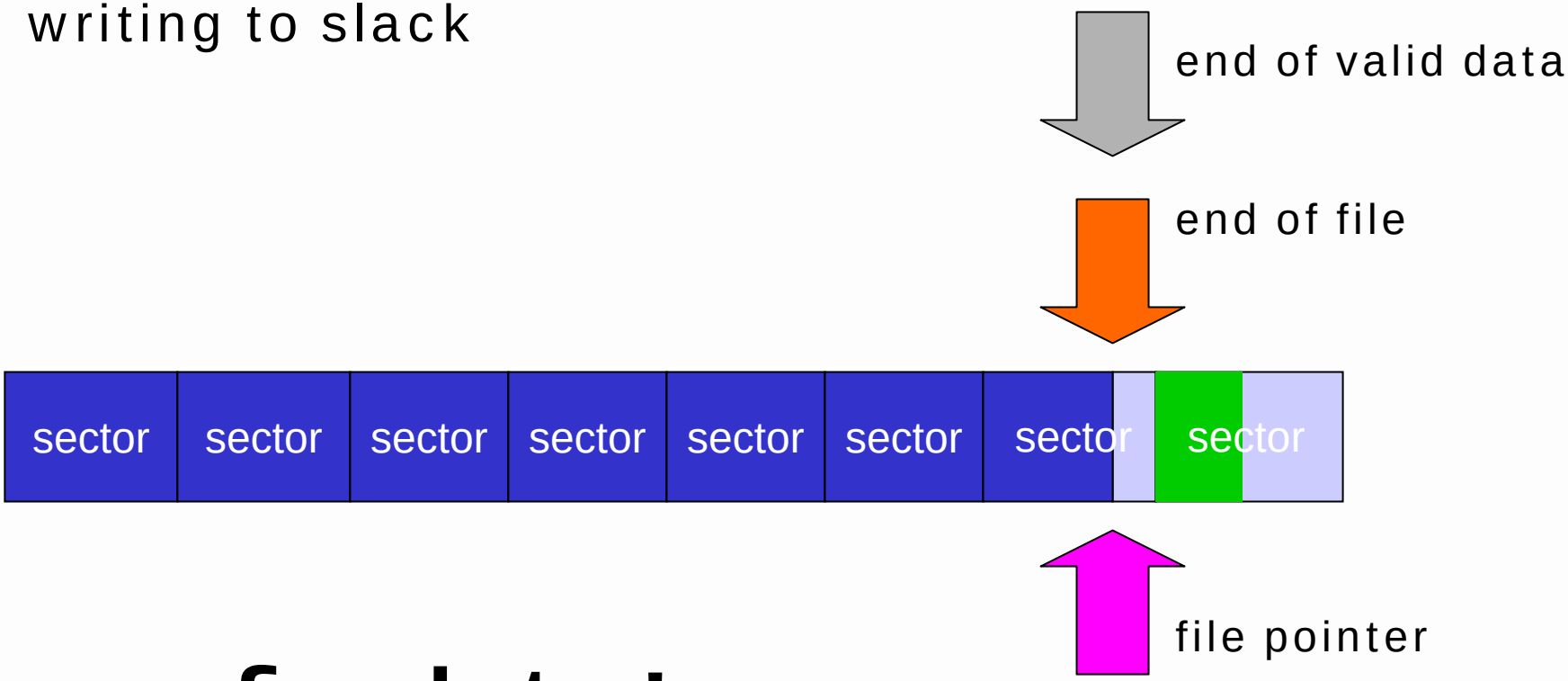
standard file setup



1 cluster = 8 sectors

Hiding in Slack Space

writing to slack

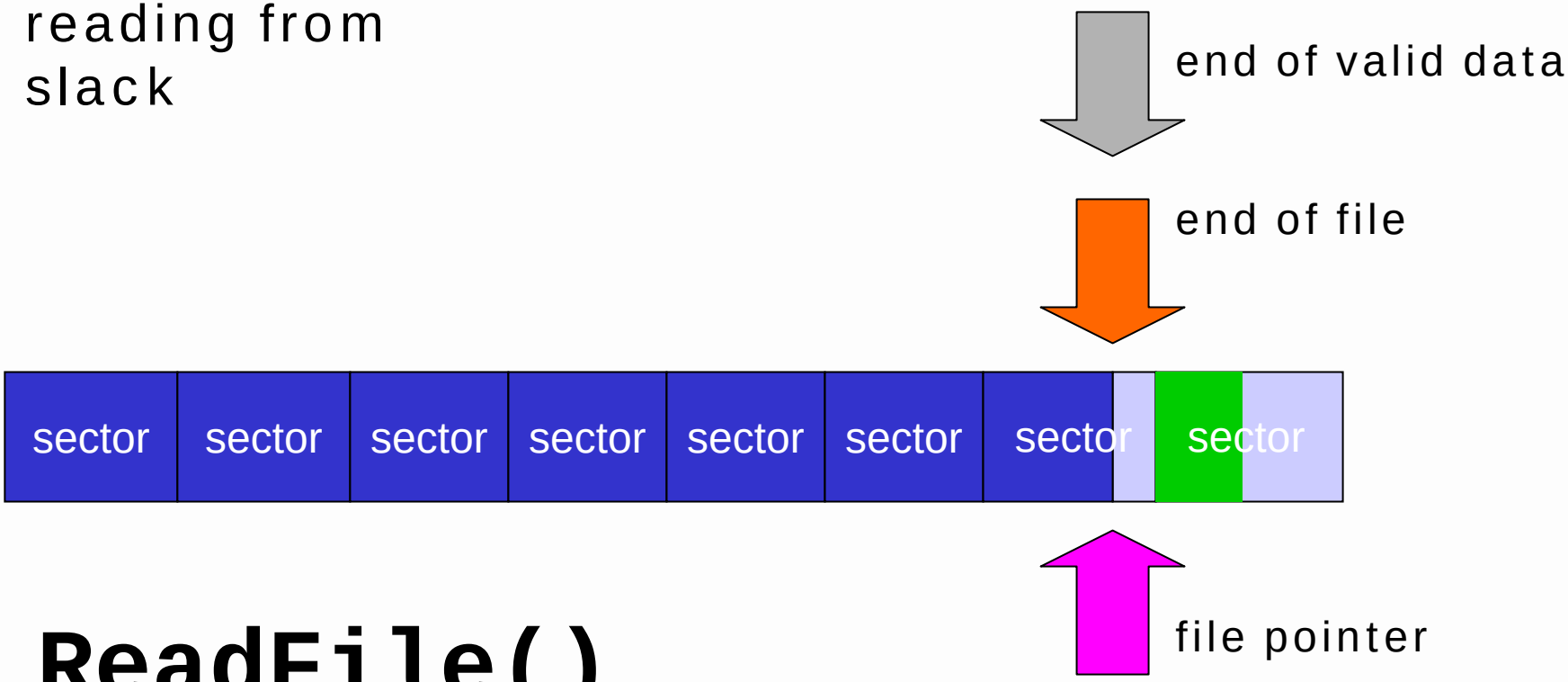


safe data!

1 cluster = 8 sectors

Hiding in Slack Space

reading from slack

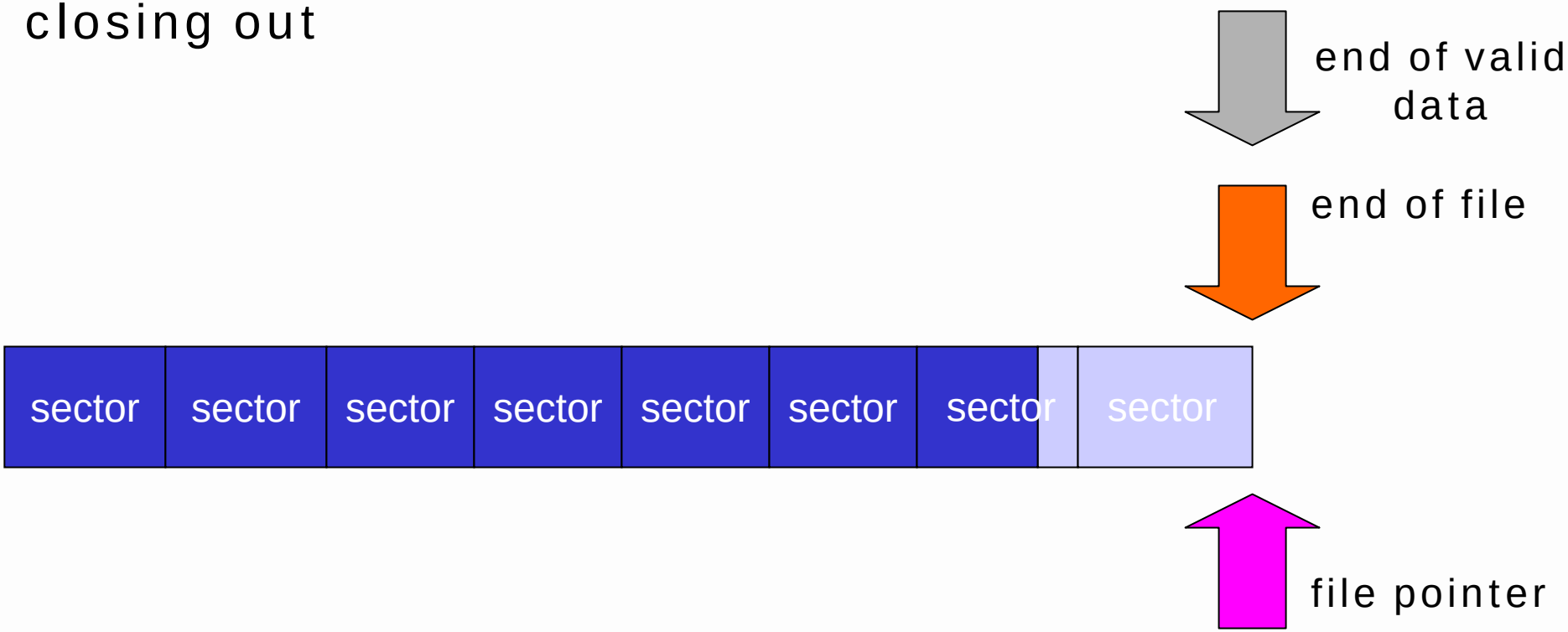


ReadFile()

1 cluster = 8 sectors

Hiding in Slack Space

closing out



1 cluster = 8 sectors

Hiding in Slack Space

- Proper selection of slack space
  - Dumb – first N files
  - Random – random selection of files
  - Safe – selects oldest (last modified) files

- Obfuscation
  - none - no obfuscation
  - XOR key – random 8 bit key
  - one-time pad – use a known fixed file

Message = 100 bits

XOR Key = 100 bits

Encrypted Message = 100 bits

STACH&LIU

Improving Slack Space

- Perform statistical analysis against slack space information to locate anomalous patterns.

- Routinely clear slack space
  - Eraser
  - PGP Disk Wipe

Future Directions

- Techniques
  - Cross-disciplinary tools
  - i.e. slacker, Meterpreter
- Availability
  - Actively researched, discussed, and distribution of tools
- Sophistication
  - Targeted research into anti-forensics
  - More brainpower is being directed this way

Thank you for your time.

Questions?

Slides available @

http://www.metasploit.com/projects/antiforensics/