INFOSEC WORLD™

CONFERENCE & EXPO 2006

K2
Bleeding-Edge Anti-Forensics

MIS® TRAINING INSTITUTE

STACH&LIU

Bleeding-Edge Anti-Forensics

K2

Vincent Liu & Francis Brown

Monday - April 3, 2006

1:30PM to 3:30PM

INFOSEC WORLD CONFERENCE & EXPO 2006

STACH&LIU

MIS TRAINING INSTITUTE

Welcome

STACH&LIU

Vincent Liu
Managing Director
Stach & Liu, LLC
vliu@stachliu.com

Francis Brown
Dir of Assessment
Stach & Liu, LLC
fbrown@stachliu.com

INFOSEC WORLD CONFERENCE & EXPO 2006

STACH&LIU

MIS TRAINING INSTITUTE

Agenda

- Anti-forensics (AF) Background
- AF Attacks & Defenses
  - On-going Q & A
  - Metasploit AF vs. EnCase
- Future Directions

Anti-forensics Background

AF Background

- Computer Forensics
  - "application of the scientific method to digital media in order to **establish** factual information for judicial review" [1]

- Computer Anti-forensics (AF)
  - application of the scientific method to digital media in order to **invalidate** factual information for judicial review

AF Background

- Forensics Process
  - Data Collection
    - Chain of custody, documentation, evidence preservation
  - Data Analysis
    - Automated analysis with tools
    - Manual analysis with experience and training
  - Findings Presentation
    - Oral or written presentation

AF Background

- Forensics Process Weaknesses
  - Data Collection
    - Incomplete data collection, chain-of-custody
  - Data Analysis
    - Inadequate tools, methodology, training
  - Findings Presentation
    - Easy to cast doubt on submitted findings
- Locate & exploit issues in all phases.

AF Quick History

- In the beginning…
  - touch, encryption, renaming
- Then there was…
  - ADS, sdelete, Gutmann delete, Eraser
- Now we're seeing…
  - MAFIA, Defiler's toolkit, FragFS
  - Discussions @ BH, Bellua, HITB, HTCIA, CEIC, and more

Why AF?

- Good
  - Validation of forensic tools and techniques
    - Gutmann Method [2]
    - Improve tools (i.e. PGP) [3]
    - Improve process (i.e. JDFP) [4]
      - "Challenging the Presumption of Reliability"
      - Journal of Digital Forensic Practice, 2006
- Bad
  - Exonerate a guilty party by *deleting* or *modifying* data
- Ugly
  - Implicate an innocent party by *planting* data

AF Fundamentals

- **Assumptions**
  - (i) Data is evidence, (ii) We trust our tools, and (iii) Our analysts will find everything.
- **Process**
  - Understand the process better than the good guys. Theorize about weaknesses. Test the theory.
- **Attack**
  - Attack the (i) data, (ii) the tools, and (ii) the analysts.

AF Fundamentals

- **Attack the Data**
  - Contraception, Hiding, Destruction
  - Manipulation, Fabrication
- **Attack the Tools**
  - Findings gaps in tool coverage.
  - Tricking the tool analysis.
- **Attack the Analyst**
  - Information is power, and attackers leverage knowledge.
  - Attackers need only one place to hide, analysts have to check them all.

Attacks & Defenses

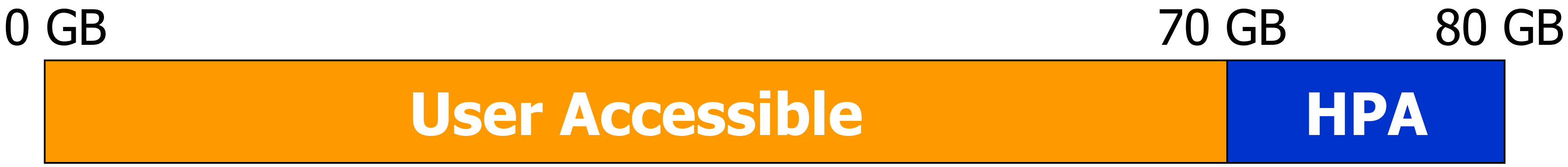
Attacks & Defenses: Type

- **AF Technique**
  - Discussion and application of the AF technique.

- **Counter Technique**
  - Discussion and application of one or more defenses to the AF technique.

Attacks & Defenses: Data Acquisition

- **Host Protected Areas (HPA)**
  - OS inaccessible areas on ATA disks for vendors to store data/information.
  - Not visible through BIOS.
  - Can be abused to hide data.



0 GB

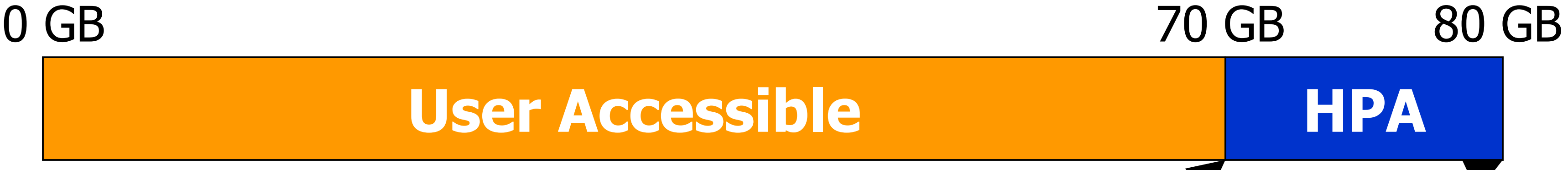
70 GB

80 GB

User Accessible

HPA

Attacks & Defenses: Data Acquisition

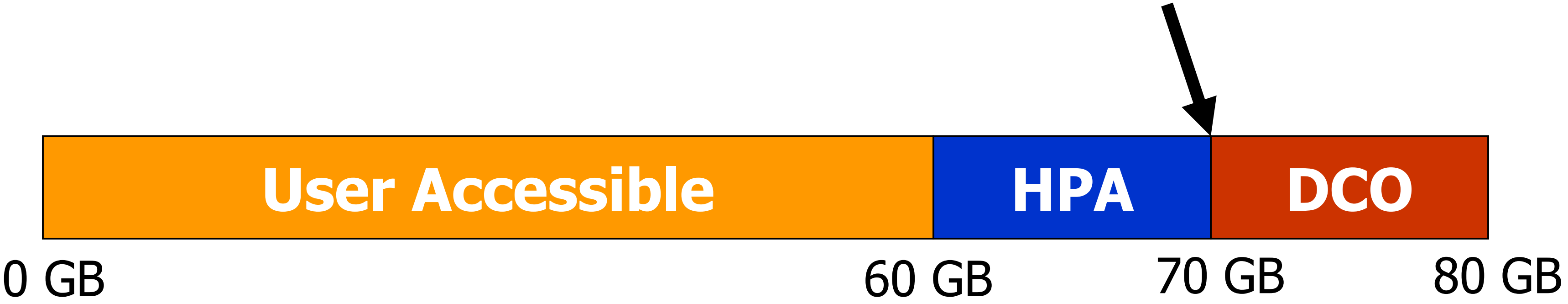


- **Counter Technique**
  - Compare IDENTIFY_ADDRESS & READ_NATIVE_MAX_ADDRESS
  - Use a tool that detects and acquires the HPA [5]

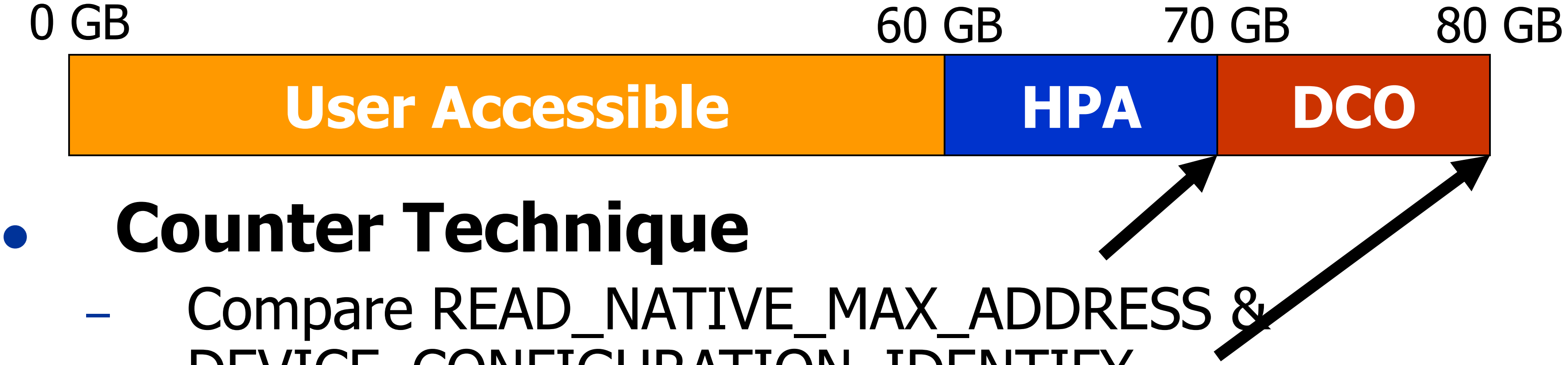
Use	Don’t Use
EnCase DOS mode w/”Direct ATA”	EnCase in DOS mode w/”BIOS”
	EnCase Enterprise Edition, EnCase in Windows

Attacks & Defenses: Data Acquisition

- **Disk Configuration Overlay (DCO)**
  - Can be abused like HPA to hide data.
  - Limits the visible maximum size from READ_NATIVE_MAX_ADDRESS.



Attacks & Defenses: Data Acquisition



- **Counter Technique**
  - Compare READ_NATIVE_MAX_ADDRESS & DEVICE_CONFIGURATION_IDENTIFY
  - Use a tool that detects and acquires the DCO [6]

Use	Don't Use
TAFT http://www.vidstrom.net/stools/taft/	Any version of EnCase.
Image MASSter Solo2 http://www.icsforensic.com	

Attacks & Defenses: Data Acquisition

- **Self-Monitoring, Analysis and Reporting Tool (SMART)**
  - Allows a hard drive to perform self-tests and collect statistical information.
    - Power_On_Hours
    - Power_On_Minutes
    - Power_Cycle_Count
  - Information can be used by an attacker to determine if the system has been powered down to be forensically duplicated [7]
  - Provides an attacker with advanced intelligence.

Attacks & Defenses: Data Acquisition

- **Counter Technique**
  - No foolproof technique because drive vendors don't follow SMART specifications
  - Make a best attempt to minimize changes to the SMART values [7]

Attacks & Defenses: Data Acquisition

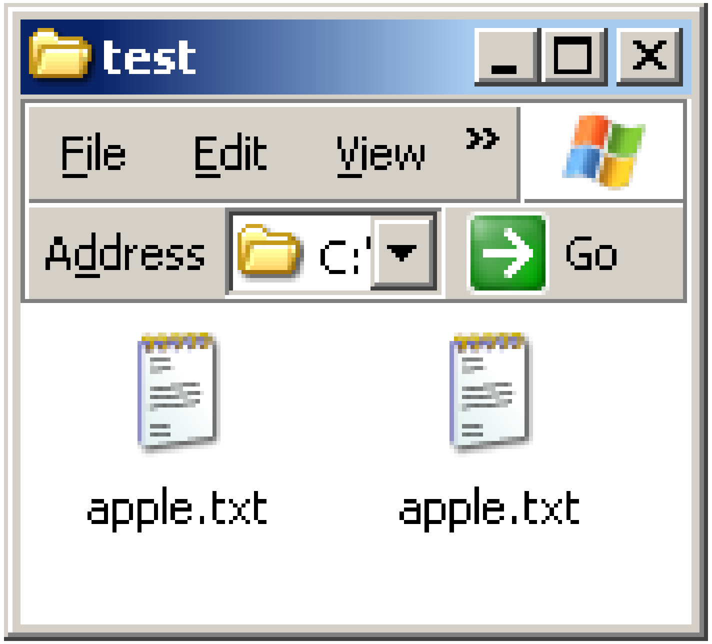
- **Information Overload**
  - Forensics takes time. Time is money.
  - Make the investigation cost as much as possible (i.e. pick the largest drives, RAID, leave a mess on as many systems as possible)
  - Businesses will have to make a judgment call of when to stop analysis and just image and rebuild

Attacks & Defenses: Data Acquisition

- **Counter Technique**
  - Prioritize systems analysis
  - Automate analysis as much as possible

Attacks & Defenses: Hiding Data

- **Homographic Attacks [8]**
  - Substitution of non-Latin letters
  - Displayed as a result of Unicode support
  - Cyrillic letters a, e, p, y are indistinguishable from the Western counterpart.



Attacks & Defenses: Hiding Data

- Are Russian (Cyrillic) apples different?

```
apple.txt

\x0061 \x0070 \x0070 \x006c \x0065
```

```
apple.txt

\x0430 \x0440 \x0440 \x006c \x0435
```

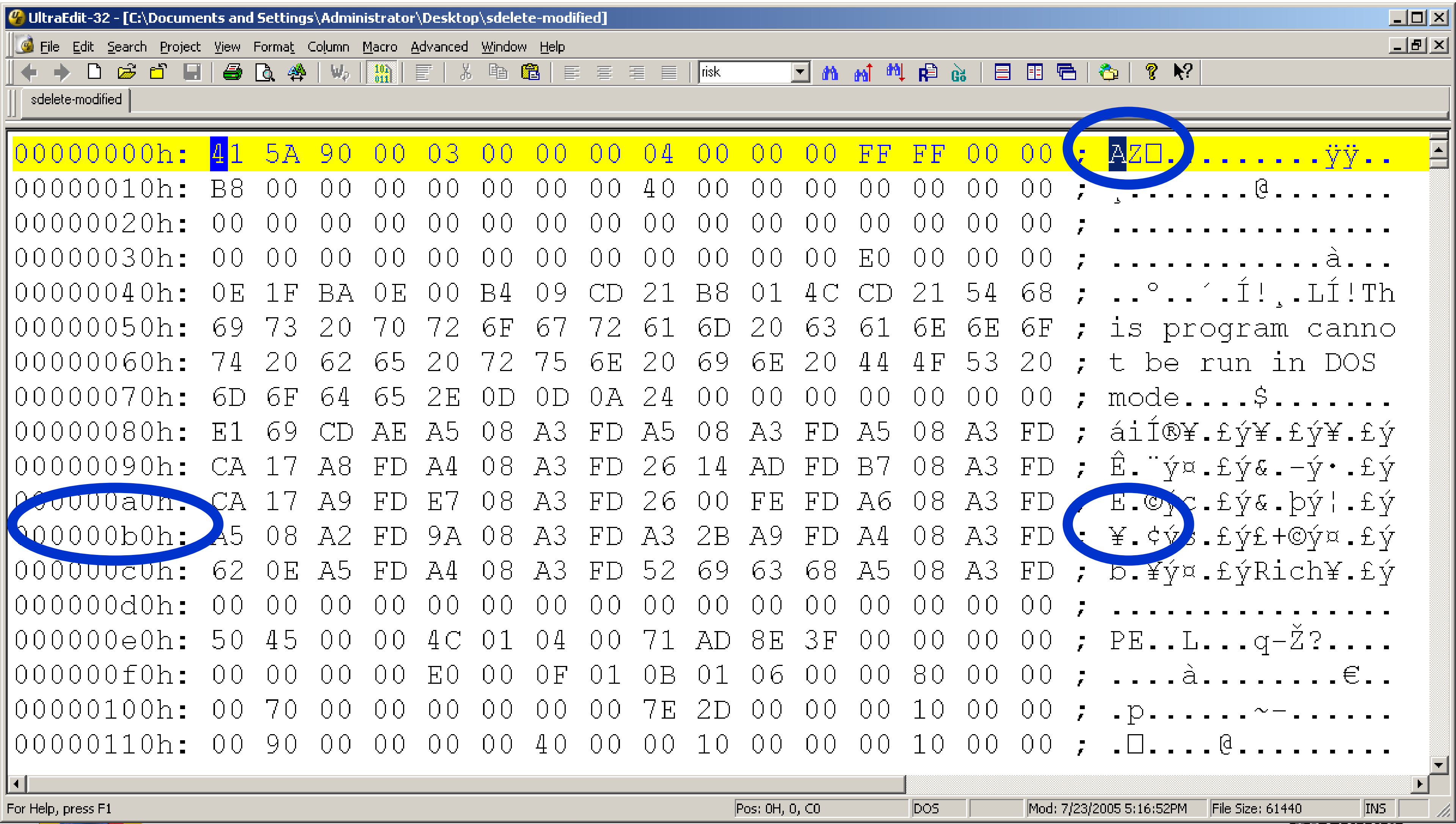
Attacks & Defenses: Hiding Data

- **Counter Technique**
  - File signature analysis
  - Tools improvements
    - right file (hash)
    - right place (directory)
    - right time (time stamp)
    - highlight characters from different character sets

Attacks & Defenses: Hiding Data

- **File name modification**
  - Change file name and extension
    - **passwords.txt → avscan.exe**
  - Most tools use two (2) techniques
    - File extension
    - File signature
  - If we know what the tools are looking for, we can change the file signature to meet those requirements
    - Manual method using notepad.exe
    - Automated method using transmogrify.exe

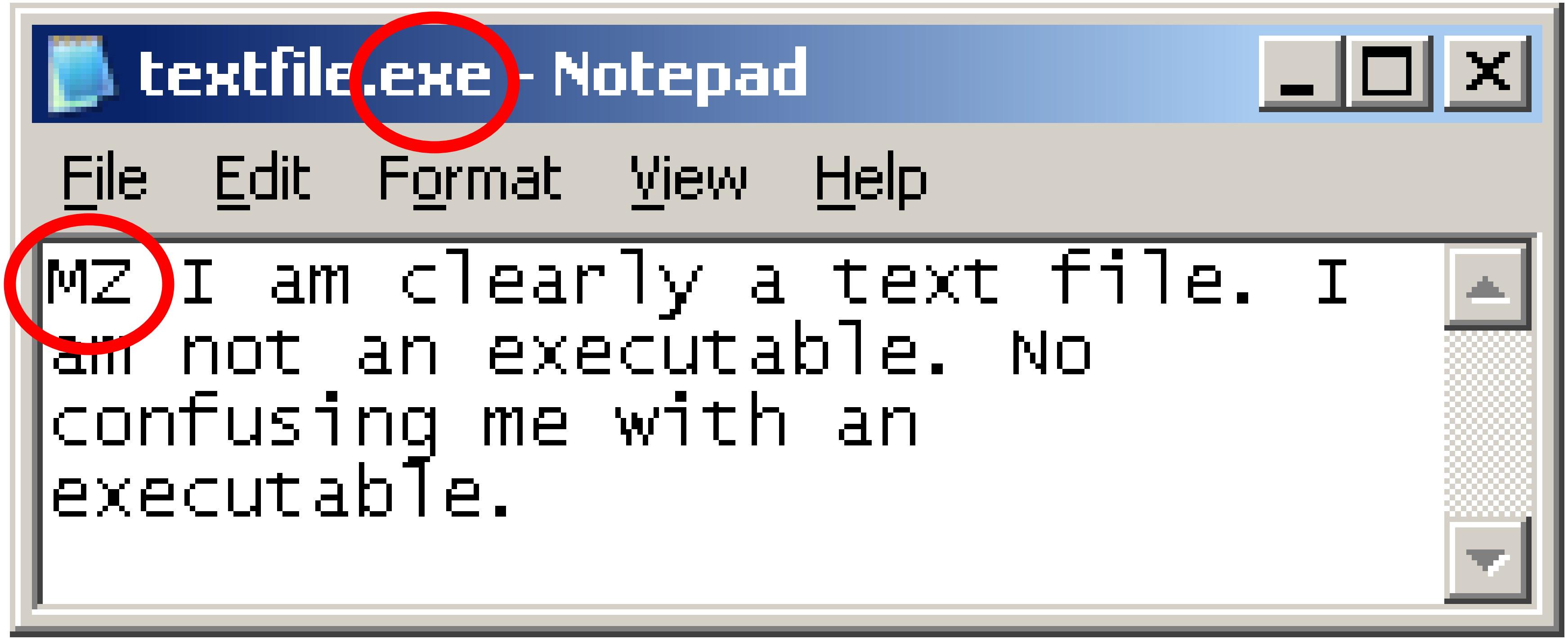
Attacks & Defenses: Hiding Data


UltraEdit-32 - [C:\Documents and Settings\Administrator\Desktop\sdelete-modified]
File
Edit
Search
Project
View
Format
Column
Macro
Advanced
Window
Help
risk
sdelete-modified

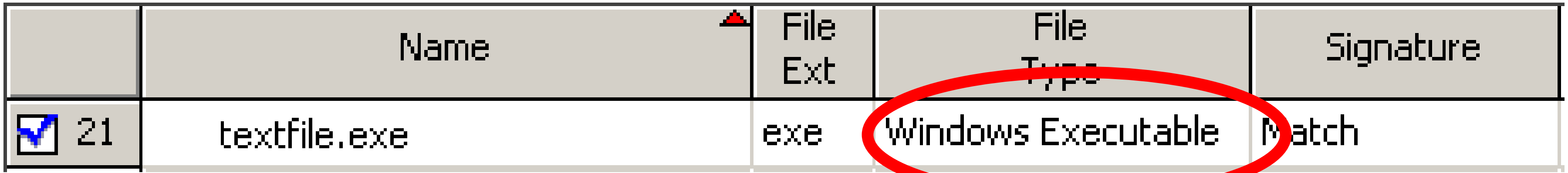
```
00000000h: 41 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 ; AZ□.........ÿÿ..
00000010h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ; ¸.......@.......
00000020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000030h: 00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00 ; ............à...
00000040h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ; ..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 ; .□....@.........
```

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

Attacks & Defenses: Hiding Data



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



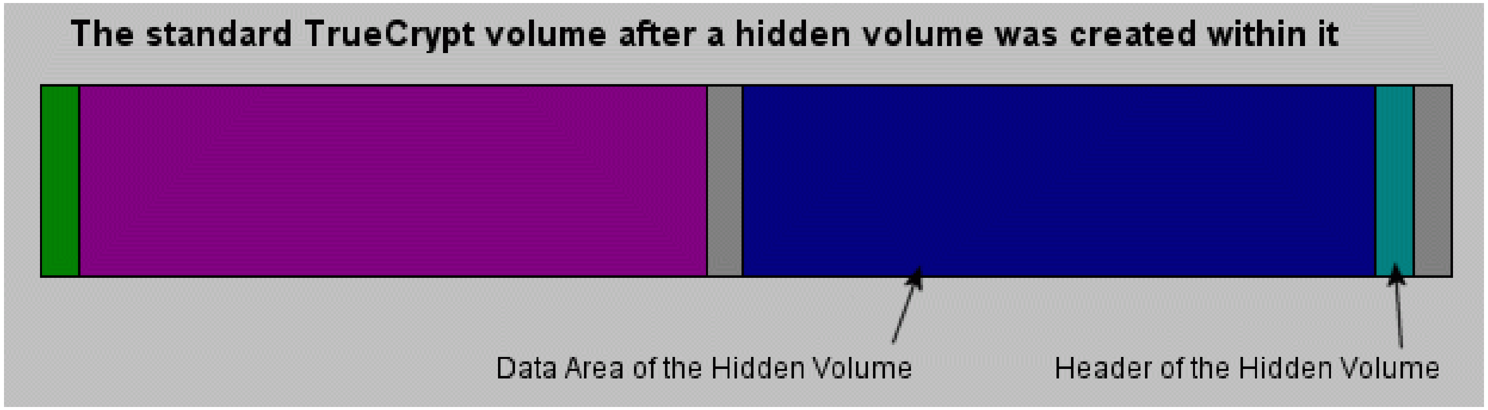
	Name	File Ext	File Type	Signature
☑ 21	textfile.exe	exe	Windows Executable	Match

Attacks & Defenses: Hiding Data

- **Counter Technique**
  - File contents should be analyzed more closely.
  - Statistical header analysis.
  - Just open the file.

Attacks & Defenses: Hiding Data

- **Encrypting Data**
  - When used correctly, encryption will prevent an examiner from reading your data.
  - Protect e-mail, files, folders, volumes, and entire drives
  - Commerical quality free tools:
    - TrueCrypt, GnuPG
  - Plausible deniability via hidden TrueCrypt volumes [9]


The standard TrueCrypt volume after a hidden volume was created within it
Data Area of the Hidden Volume
Header of the Hidden Volume

Attacks & Defenses: Hiding Data

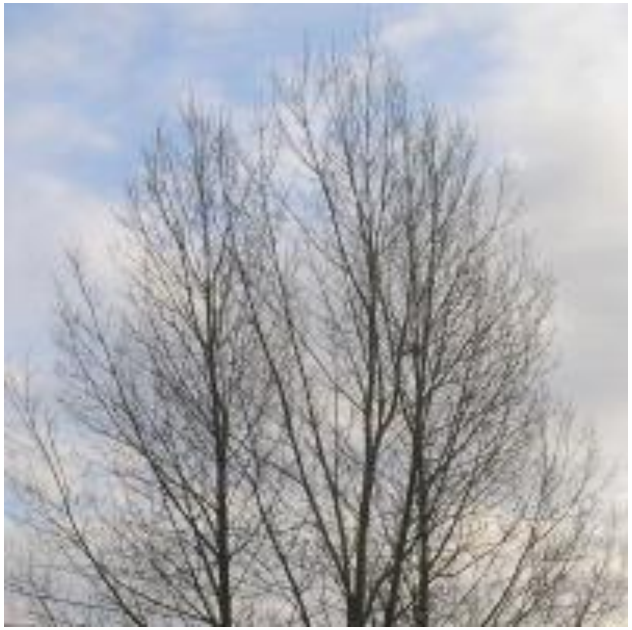
- **Counter Technique**
  - Brute-force the encryption
  - Look for stored passwords elsewhere
  - Key logging
  - Physical coercion to retrieve key

Attacks & Defenses: Hiding Data

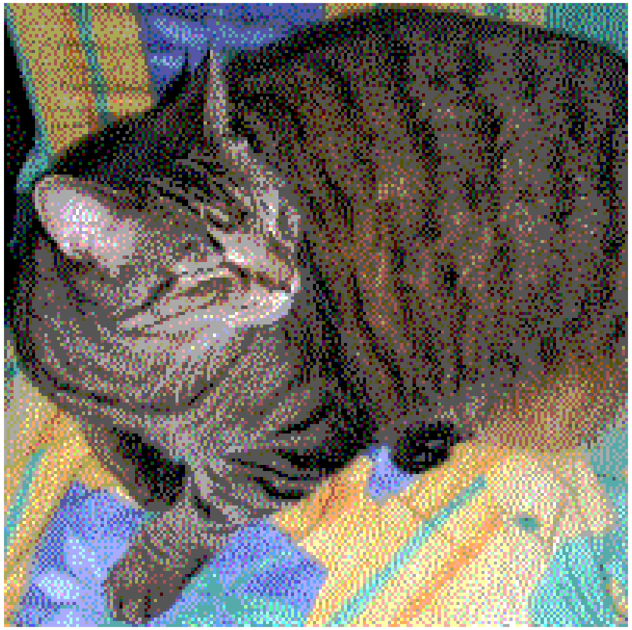
- **Steganography**
  - Hiding information within a file without visibly changing its contents or behavior
  - Steghide [10]
    - compression, encryption, checksum
    - JPEG, BMP, mp3, WAV, AU
  - Hydan [11]
    - Replaces executable instructions with functional equivalents that encode information
    - encrypted data, file size is unchanged
    - 1 to 110 byte encoding ratio

Attacks & Defenses: Hiding Data

Original [12]



Extracted



STACH&LIU

Attacks & Defenses: Hiding Data

- **Counter Technique**
  - Stegdetect [13]
    - jsteg, jphide, invisible secrets, outguess, F5, appendX, camouflage
    - Free
  - Gargoyle
    - Commercial

Attacks & Defenses: Hiding Data

- **Rootkits**
  - Hide presence on a system and allow for future access
  - User-mode & Kernel-mode
    - Kernel mode allows access to all system resources
  - Hooking & DKOM
    - Hacker Defender
    - FU
  - Persistent & Memory-only
  - Advanced Hiding Techniques
    - Hide their own code as well as modifications they make in memory
    - Shadow Walker will intercept memory accesses
  - BIOS rootkits
    - ACPI
    - Anywhere there is memory

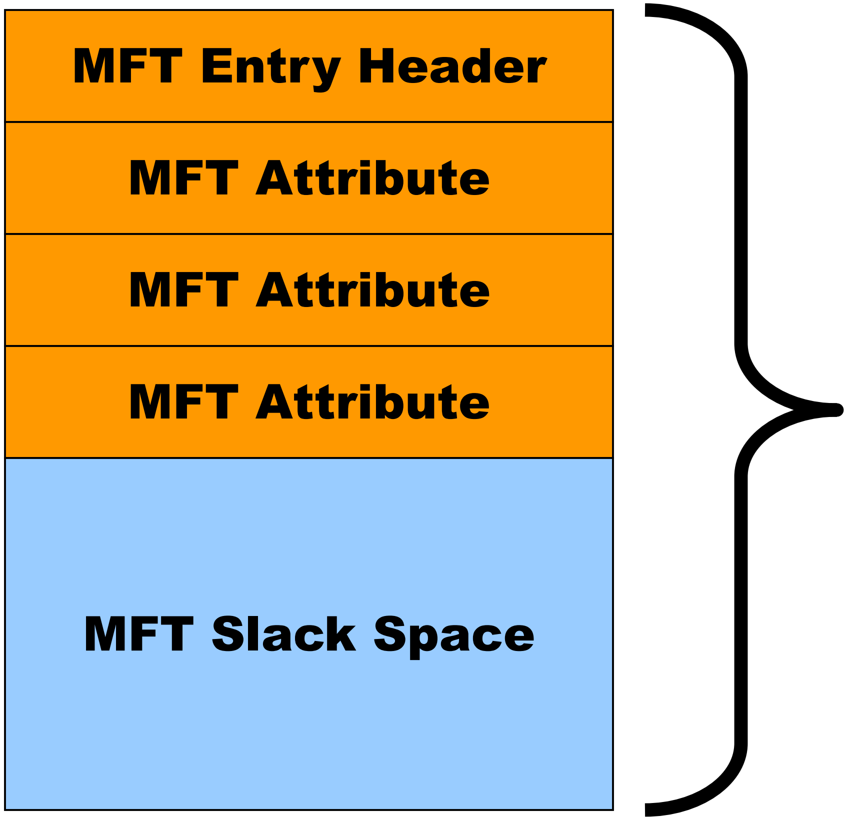
Attacks & Defenses: Hiding Data

- **Counter Technique [14]**
  - AV Scanning
    - Signature-based detection of known rootkits
  - VICE
    - Detects most of today's hooking rookits
    - High false-positive rate
  - Klister
    - Leverages redundancy in OS process structures to identify hidden processes via DKOM.
  - Rootkit Revealer / Strider GhostBuster
    - Cross-view detection for persistent rootkits based on file system differences.
    - Registry Entries, Processes, Loaded modules (GB)
  - SVV
    - Like VICE but compares loaded modules with their disk counterparts
  - CoPilot
    - Hardware based solution for high assurance

Attacks & Defenses: Hiding Data

- **Hiding in Metadata**
  - Take advantage of the fact that tools only analyze what they believe contain content. A lot of metadata isn't even visible in tools except in their raw format. Lots of small spaces can add up to a large collective area to store data if it can be managed.
  - FragFS [15]
    - Hides data within records of the NTFS Master File Table
  - Journaling File Systems [16]
    - Exploits inadequate checking by journaling file systems
  - the grugq Research [17]
    - Rune FS – stores data in bad blocks
    - Waffen FS – stores data in the ext3 journal file
    - KY FS – stores data in directory files
    - Data Mule FS – stores data in inode reserved space

Attacks & Defenses: Hiding Data



FragFS

NTFS allocates 1024 bytes per MFT entry.

Usually only a portion is used, leaving plenty of space for storage.

Attacks & Defenses: Hiding Data

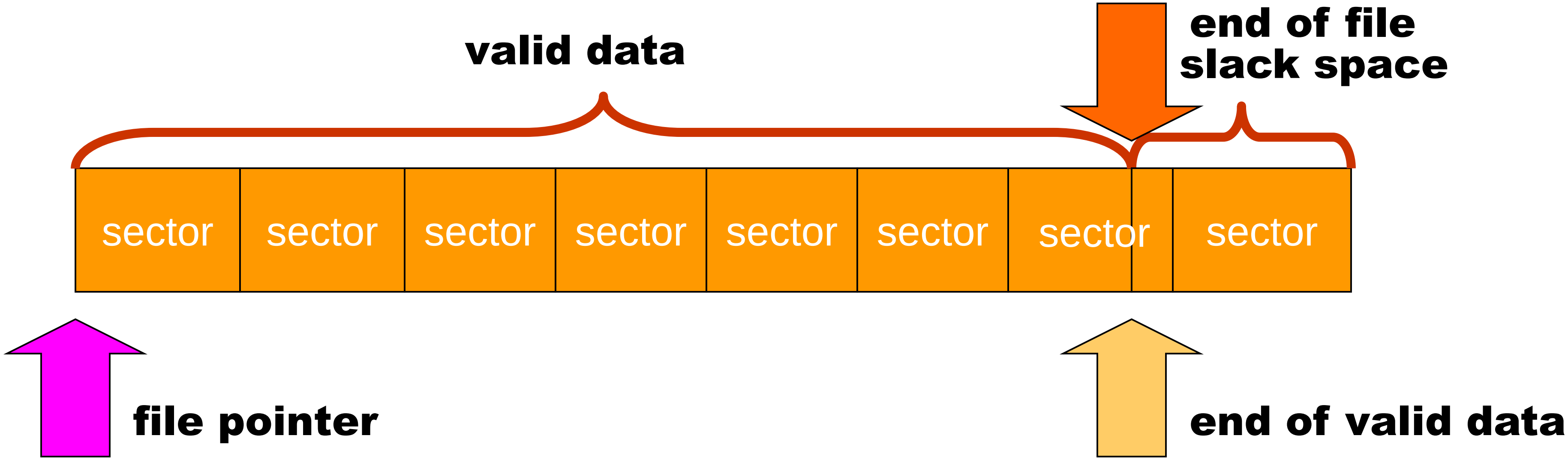
- **Counter Technique**
  - Detailed analysis of the empty metadata areas as well as the standard content locations
  - Closer examination and interpretation of metadata by forensic tools

Attacks & Defenses: Hiding Data

- **Hiding in File Slack Space**
  - Hiding data in the space between allocated and actual bytes in a file
  - Hidden data usually indistinguishable from old, overwritten files in slack
  - Slacker (NTFS/FAT)
    - encryption, intelligent space selection
  - Bmap (ext2fs)

Attacks & Defenses: Hiding Data

standard file setup



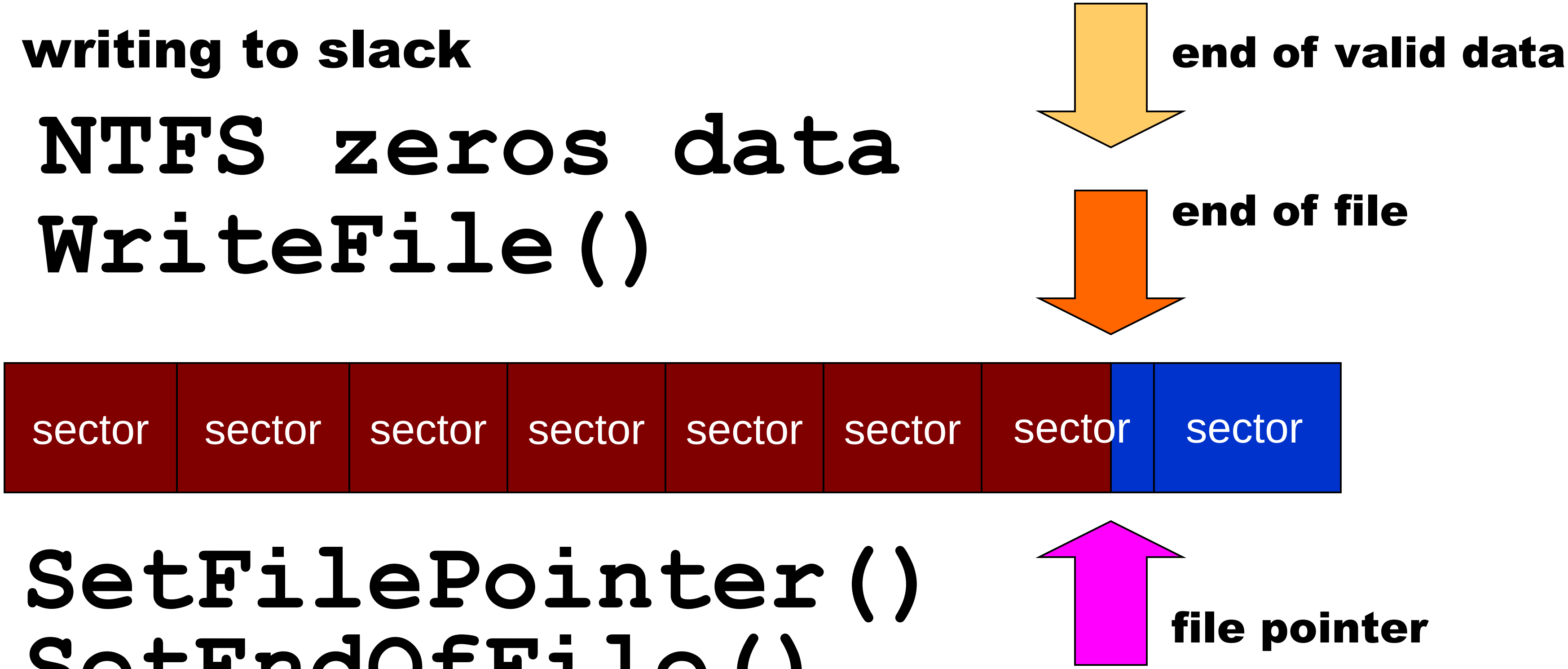
1 cluster = 8 sectors

Attacks & Defenses: Hiding Data

writing to slack

`NTFS zeros data`

`WriteFile()`



`SetFilePointer()`

`SetEndOfFile()`

`safe data!`

1 cluster = 8 sectors

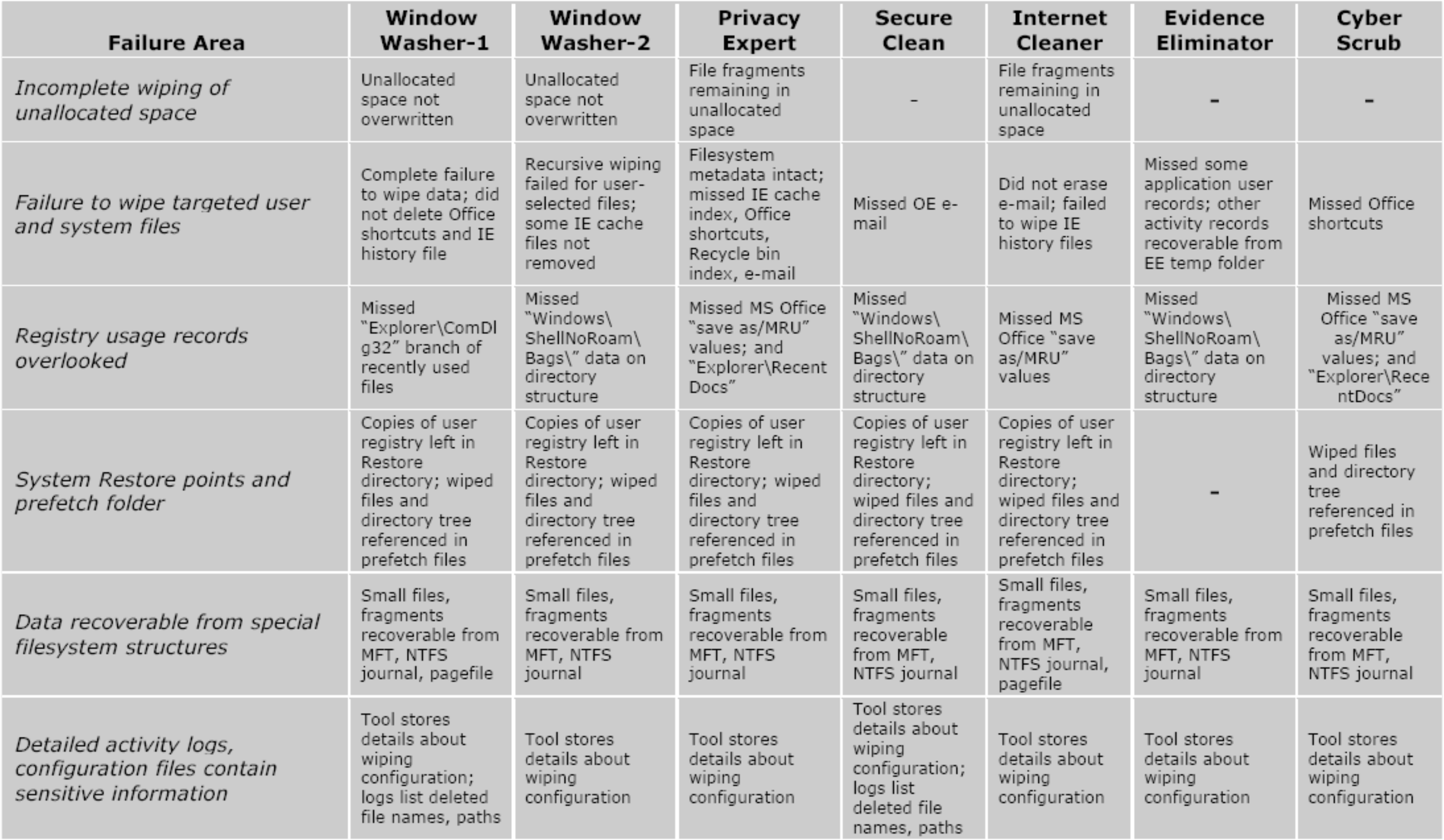
Attacks & Defenses: Hiding Data

- **Counter Technique**
  - Strings slack space
  - Statistical analysis of slack
  - Routinely clear slack space
    - Eraser (heide.ie), PGP Wipe

Attacks & Defenses: Destroy Data

- **Wiping Tools**
  - Darik's Boot and Nuke (dban)
    - Gutmann method (1996)
  - Commercial Tools
    - PGP Wipe, Evidence Eliminator, and more…
  - Free Tools
    - Eraser, sdelete.exe, the defiler's toolkit (TDT)
  - Default Features
    - MS Anti-spyware (Track Eraser)

Attacks & Defenses: Destroy Data



Failure Area	Window Washer-1	Window Washer-2	Privacy Expert	Secure Clean	Internet Cleaner	Evidence Eliminator	Cyber Scrub
Incomplete wiping of unallocated space	Unallocated space not overwritten	Unallocated space not overwritten	File fragments remaining in unallocated space	-	File fragments remaining in unallocated space	-	-
Failure to wipe targeted user and system files	Complete failure to wipe data; did not delete Office shortcuts and IE history file	Recursive wiping failed for user-selected files; some IE cache files not removed	Filesystem metadata intact; missed IE cache index, Office shortcuts, Recycle bin index, e-mail	Missed OE e-mail	Did not erase e-mail; failed to wipe IE history files	Missed some application user records; other activity records recoverable from EE temp folder	Missed Office shortcuts
Registry usage records overlooked	Missed “Explorer\ComDlg32” branch of recently used files	Missed “Windows\ShellNoRoam\Bags\” data on directory structure	Missed MS Office “save as/MRU” values; and “Explorer\RecentDocs”	Missed “Windows\ShellNoRoam\Bags\” data on directory structure	Missed MS Office “save as/MRU” values	Missed “Windows\ShellNoRoam\Bags\” data on directory structure	Missed MS Office “save as/MRU” values; and “Explorer\RecentDocs”
System Restore points and prefetch folder	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	Copies of user registry left in Restore directory; wiped files and directory tree referenced in prefetch files	-	Wiped files and directory tree referenced in prefetch files
Data recoverable from special filesystem structures	Small files, fragments recoverable from MFT, NTFS journal, pagefile	Small files, fragments recoverable from MFT, NTFS journal	Small files, fragments recoverable from MFT, NTFS journal	Small files, fragments recoverable from MFT, NTFS journal	Small files, fragments recoverable from MFT, NTFS journal, pagefile	Small files, fragments recoverable from MFT, NTFS journal	Small files, fragments recoverable from MFT, NTFS journal
Detailed activity logs, configuration files contain sensitive information	Tool stores details about wiping configuration; logs list deleted file names, paths	Tool stores details about wiping configuration	Tool stores details about wiping configuration	Tool stores details about wiping configuration; logs list deleted file names, paths	Tool stores details about wiping configuration	Tool stores details about wiping configuration	Tool stores details about wiping configuration

Evaluating Commercial Counter-Forensic Tools, Matthew Geiger [18]

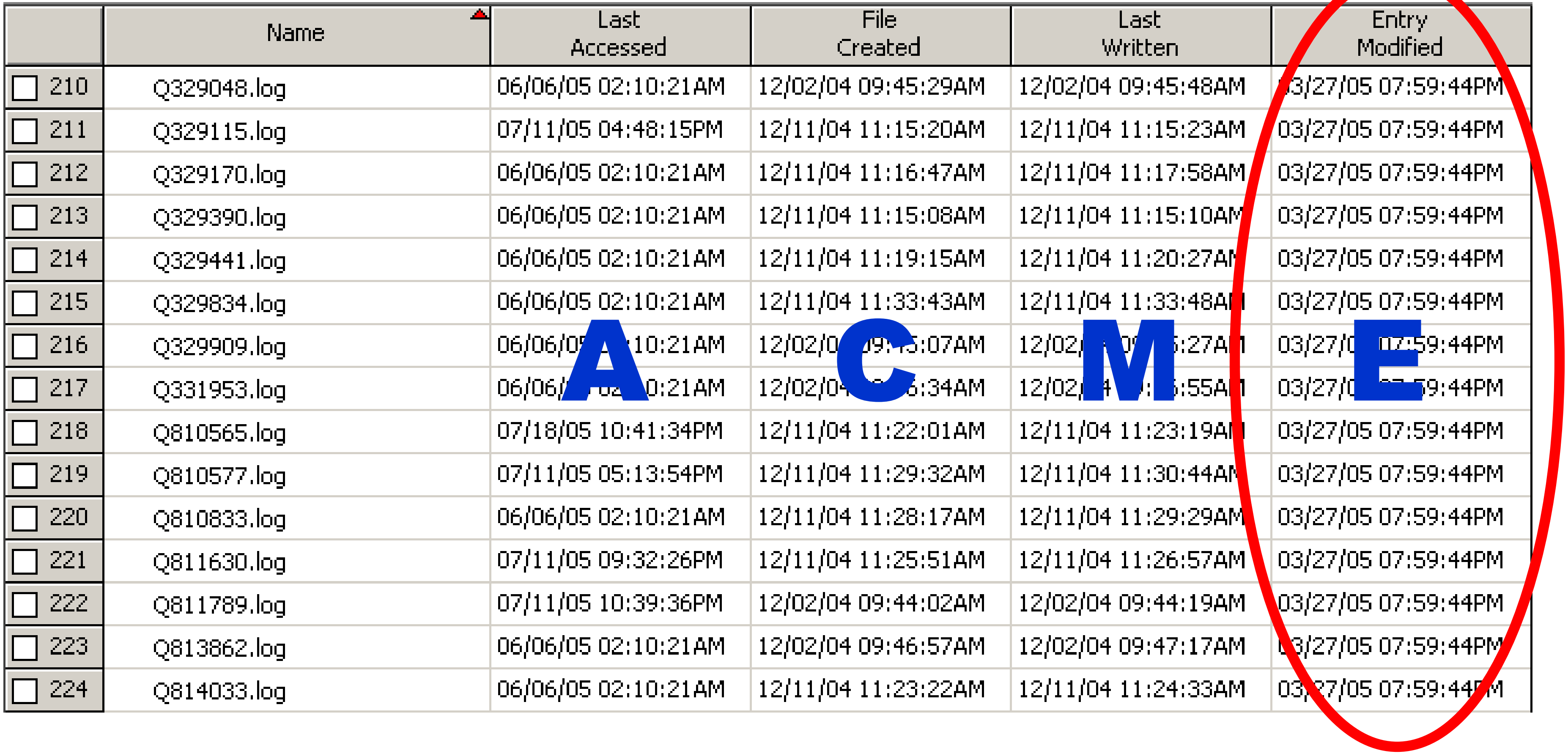
Attacks & Defenses: Destroy Data

- **Counter Technique**
  - Enable journaling on NTFS
  - Extract NTFS small files
  - Analyze missed pieces
  - Electron scanning microscope

Attacks & Defenses: Manipulate Data

- **Time stamp modification**
  - UNIX
    - touch
  - Windows
    - FAT has MAC
      - Many tools exist
    - NTFS has MACE [19]
      - timestomp.exe

Attacks & Defenses: Manipulate Data



	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 [illegible]10:21AM	12/02/0[illegible]9:[illegible]5:07AM	12/02/[illegible]:27AM	03/27/0[illegible]07:59:44PM
□ 217	Q331953.log	06/06/[illegible]0:21AM	12/02/04[illegible]6:34AM	12/02/[illegible]4[illegible]:55AM	03/27/0[illegible]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**)*

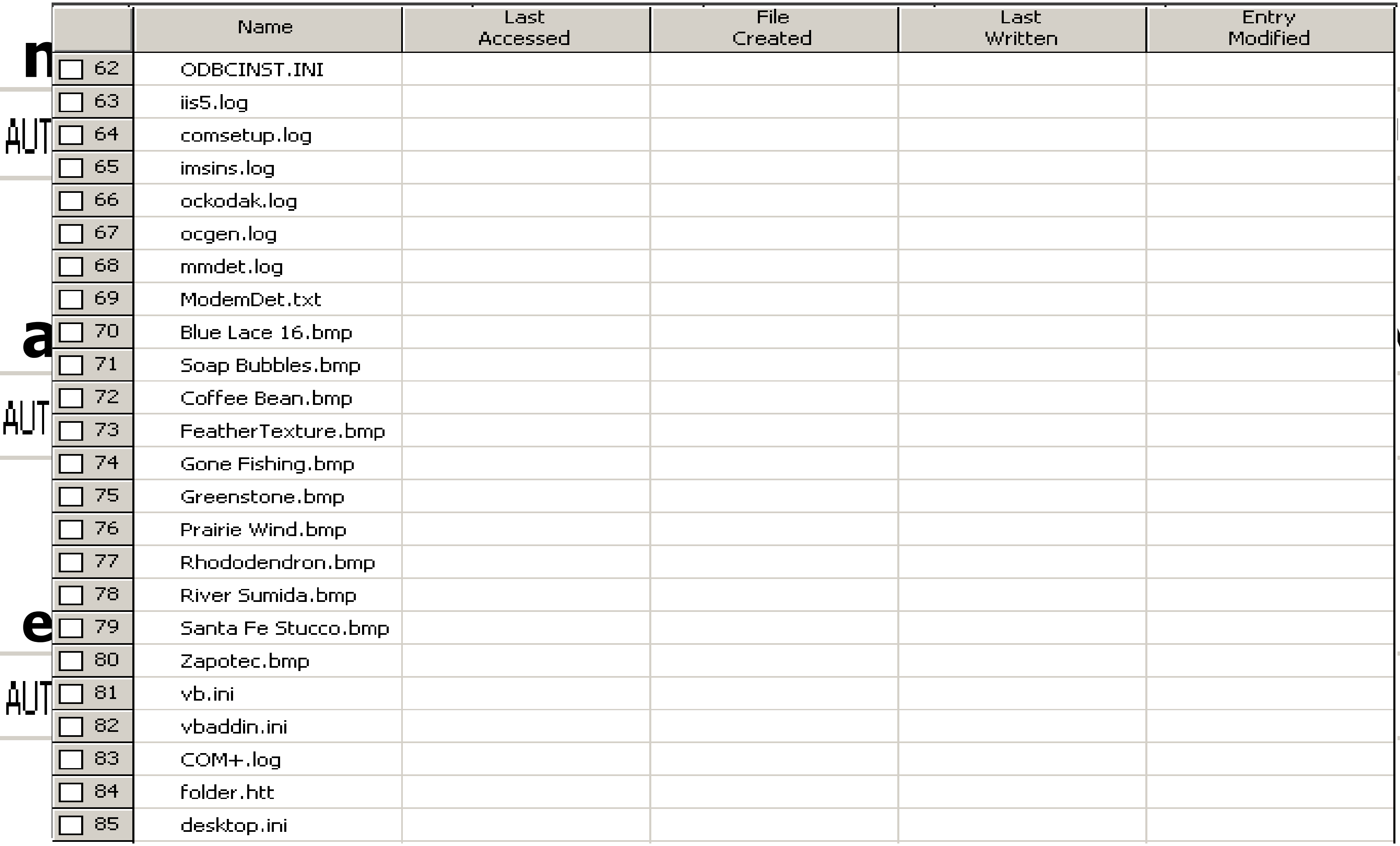
Attacks & Defenses: Manipulate Data

EnCase

Vs

timestomp.exe

Attacks & Defenses: Manipulate Data



	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				

- n

AUT :43:29AM

- a M”)

AUT :05:05AM

- e

AUT

Attacks & Defenses: Manipulate Data

Windows Explorer

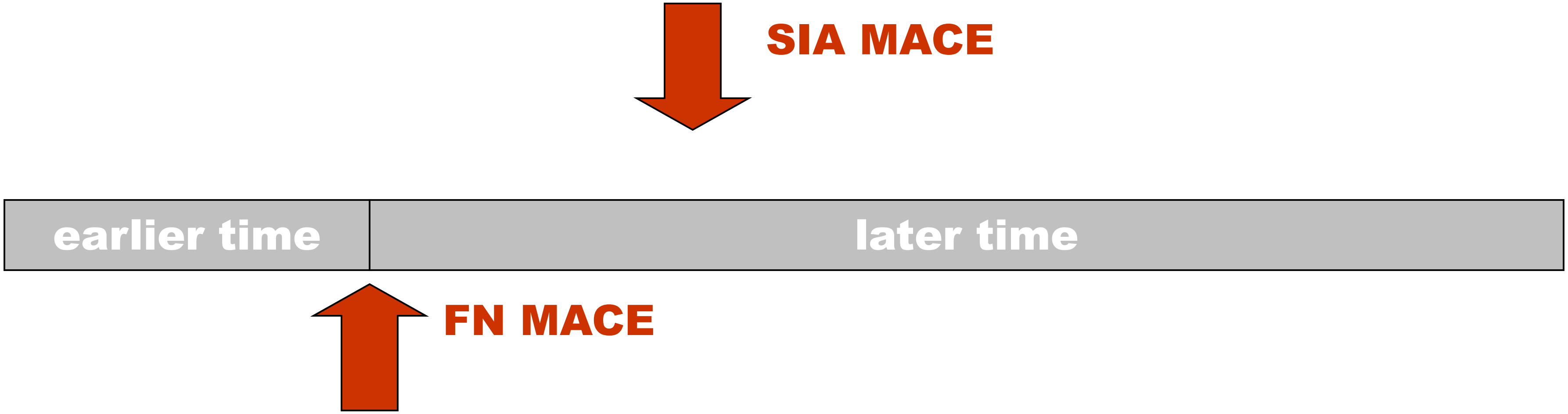
Vs

timestomp.exe

(Demo)

Attacks & Defenses: Manipulate Data

- **Counter Technique**
  - Use the secondary MACE values stored in the $filename (FN) attribute to validate standard MACE values [19]



SIA MACE

earlier time

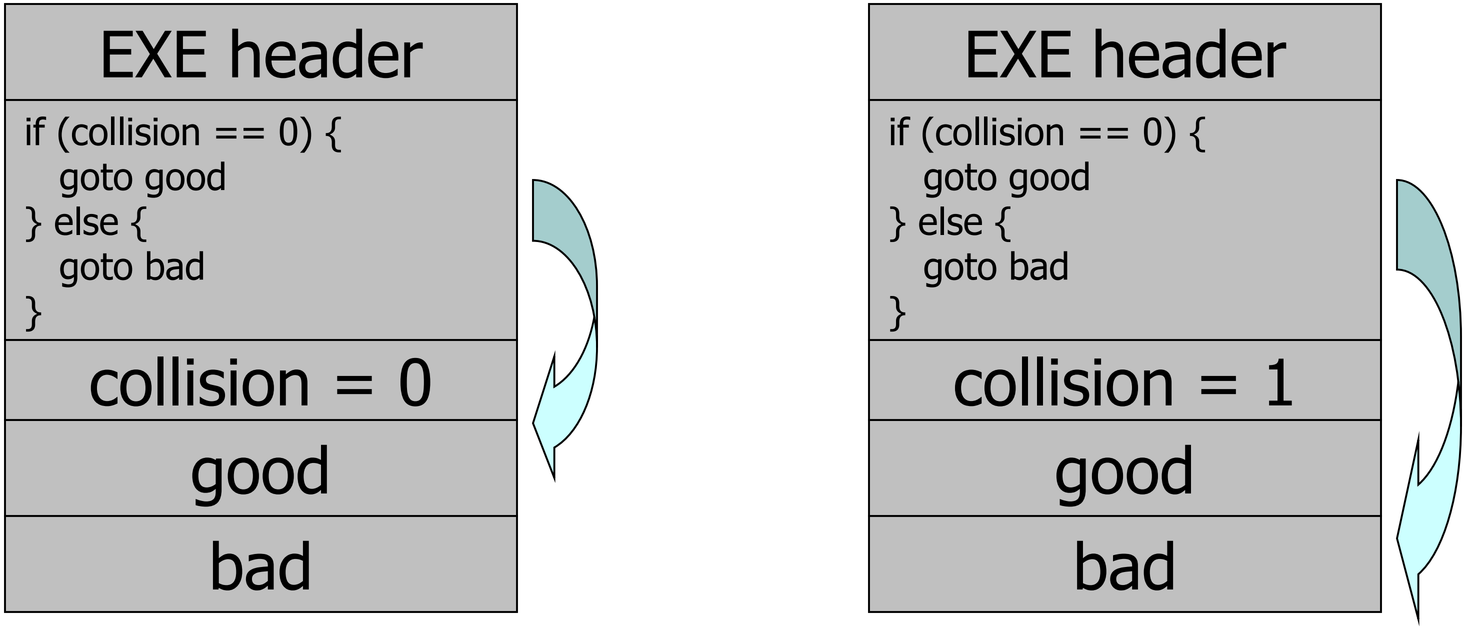
later time

FN MACE

Attacks & Defenses: Manipulate Data

- **Hash Collisions**
  - Generating MD4 and MD5 collisions is now in the realm of the personal computer [20]
  - What can we make look the same?
    - web pages, executables, etc…
  - Can we make a malicious executable hash to the same value as an innocuous executable?

Attacks & Defenses: Manipulate Data



EXE header

```
if (collision == 0) {
   goto good
} else {
   goto bad
}
```

collision = 0

good

bad

EXE header

```
if (collision == 0) {
   goto good
} else {
   goto bad
}
```

collision = 1

good

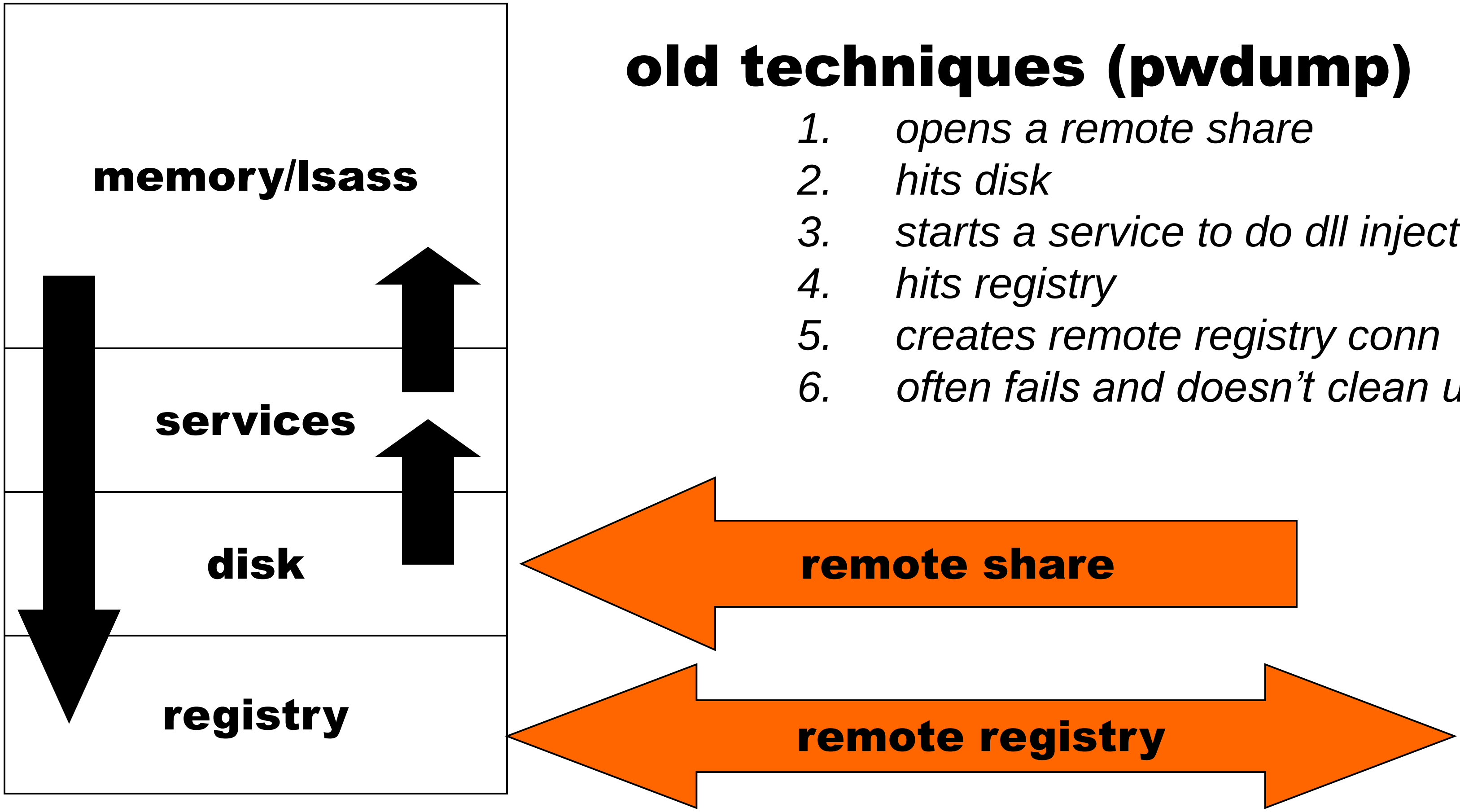
bad

- **Counter Technique**
  - Bit-by-bit file comparison
  - Use trusted hash lists

Attacks & Defenses: No Data

- **In-memory Execution**
  - Prevents data from being written to any persistent storage by executing directly from memory
  - *Syscall Proxying* (Core Impact)
    - Client contains the application logic, but passes system calls to the exploited machine (server)
  - *MOSDEF* (Immunity CANVAS)
    - "Compile" code on the client to send over to the server to arbitrary code can be run
  - *Meterpreter* (Metasploit Framework)
    - Allows loading of arbitrary DLLs to be executed

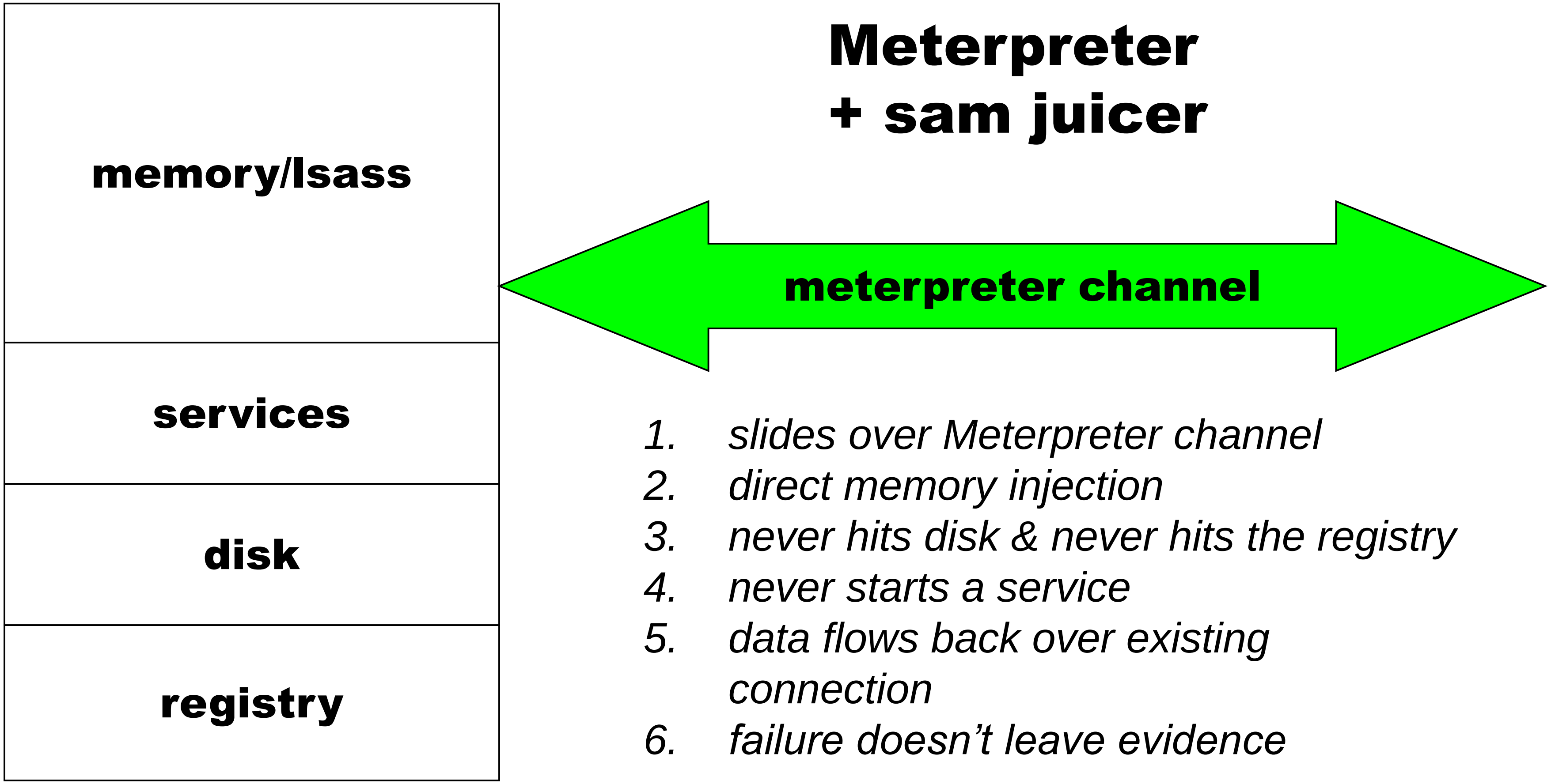
Attacks & Defenses: No Data



old techniques (pwdump)

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*

Attacks & Defenses: No Data



Meterpreter
+ sam juicer

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*

Attacks & Defenses: No Data

- **Counter Technique**
  - Active Processes
    - lsof, netstat, dd, ifconfig
  - CoPilot
    - Hardware based solution that is installed before system runs
  - Memparser, Kntlist, and Windows Memory Forensic Toolkit [21]
    - Processes, strings, environment, list of DLLs, etc…
  - IDETECT & gdb
    - Examine collected memory of Linux system
  - Use hardware to collect memory instead of software which can be subverted.

Attacks & Defenses: Analyst

- **Leave a false trail**
  - Two questions:
    - How did they get in?
    - How far did they get?
  - Answer the question for them.
    - Leave fake evidence.
    - Reduce level of sophistication.

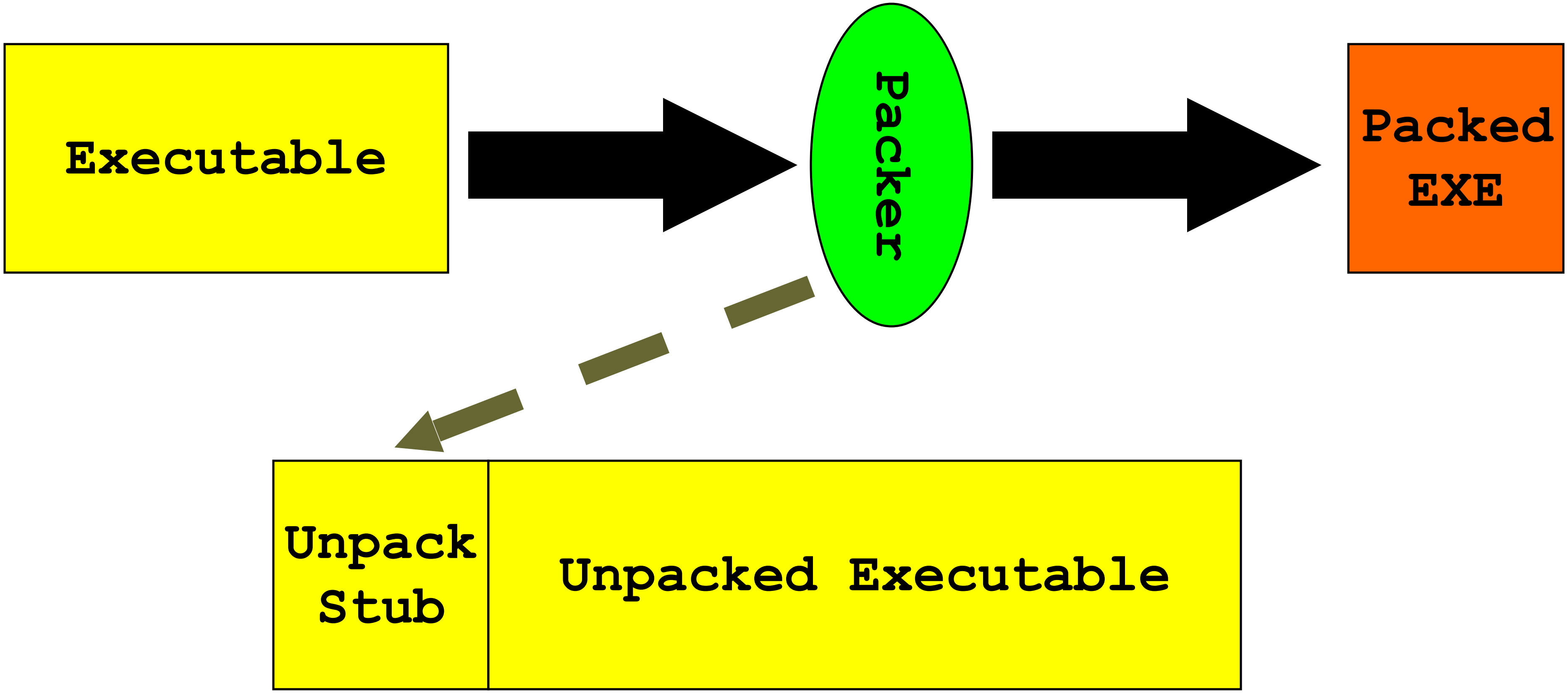
Attacks & Defenses: Analyst

- **Counter Technique**
  - Follow through the entire investigation
  - Utilize as much automation as possible
  - Identify inconsistencies within toolkits and skill level.

Attacks & Defenses: Analyst

- **Packers**
  - Packers compress and obfuscate executables so they must be reverse engineering.
  - Reverse engineering is a highly specialized skill.
  - Using a packers isn't.

Attacks & Defenses: Analyst



Executable

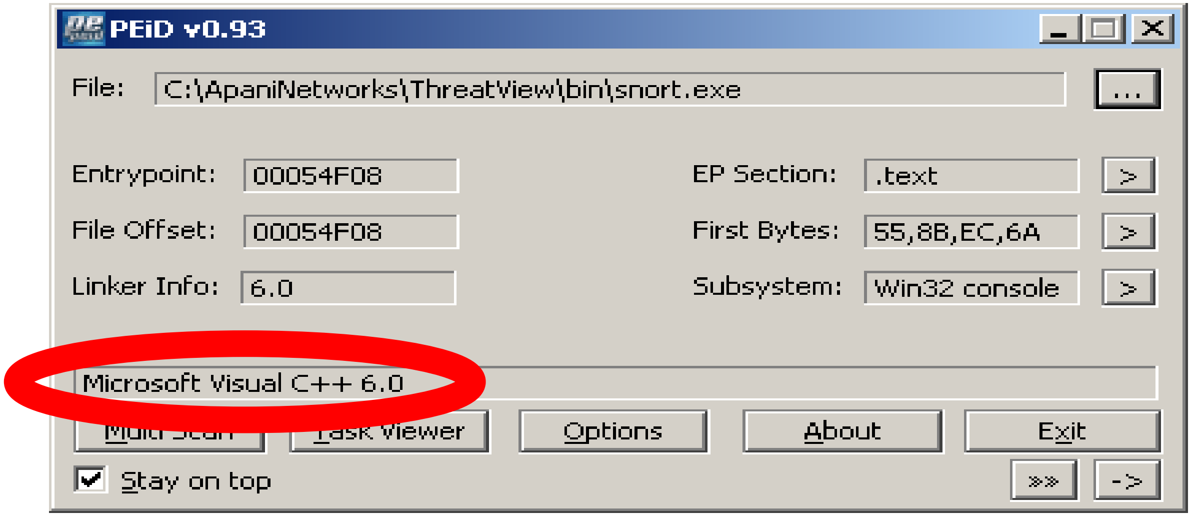
Packer

Packed EXE

Unpack Stub

Unpacked Executable

Attacks & Defenses: Analyst



File: C:\ApaniNetworks\ThreatView\bin\snort.exe

Entrypoint: 00054F08

EP Section: .text

File Offset: 00054F08

First Bytes: 55,8B,EC,6A

Linker Info: 6.0

Subsystem: Win32 console

Microsoft Visual C++ 6.0

- **Counter Technique**
  - Identify with PEiD or RoyalTS
  - Common packers have freely available unpackers
  - Debugging (OllyDbg with OllyScripts, IDA Pro)
  - Dump the process memory and strings

Future Directions

- **Techniques**
  - Seeing a combination of techniques especially encryption (i.e. slacker.exe)
  - Actively discussing and looking for places to hide, no longer serendipitous.
- **Availability**
  - It’s no longer the preserve of the expert.
  - Everyone’s doing it for pennies a day.
- **Sophistication**
  - Getting more and more difficult to detect and prevent with current technology.
  - Vendors need to improve their tools and techniques.

Thank you for your time.

Questions?

Slides can be found @

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

Image Citations

- Tree steganography image courtesy of Cyp from Wikimedia Commons
- Cat steganography image courtesy of Cyp from Wikimedia Commons