Anti-forensics

Vincent Liu och Patrick Stach

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

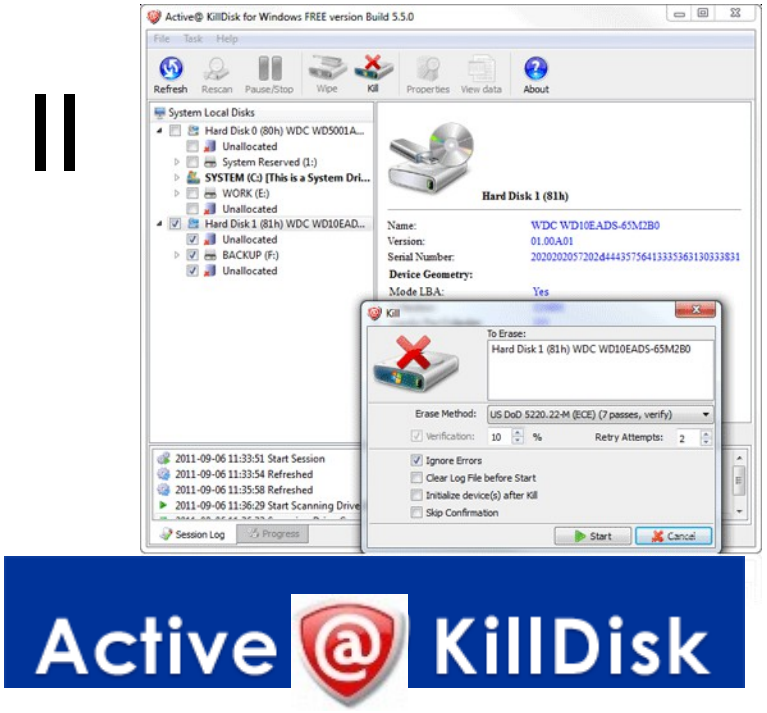
Forensics and the future

http://www.forensicswiki.org/wiki/Anti-forensic_techniques

Anti-forensics (AF) I

- Various definitions
  - Attempts to negatively effect the existence, amount and/or quality of evidence from a crime scene
  - Or make the analysis and examination of evidence difficult or impossible to conduct
- Who uses it?
  - Hackers, dodgy employees, Al Qaeda, pedophiles, …
- Attacks
  - The data, the tools, the analysts
- Forensic analysts have issues vs. criminals
  - Frequently short on time
  - Generally short on various skills as programming
  - Almost always slaves to their tools
  - Need to check *everything*

Anti-forensics (AF) II



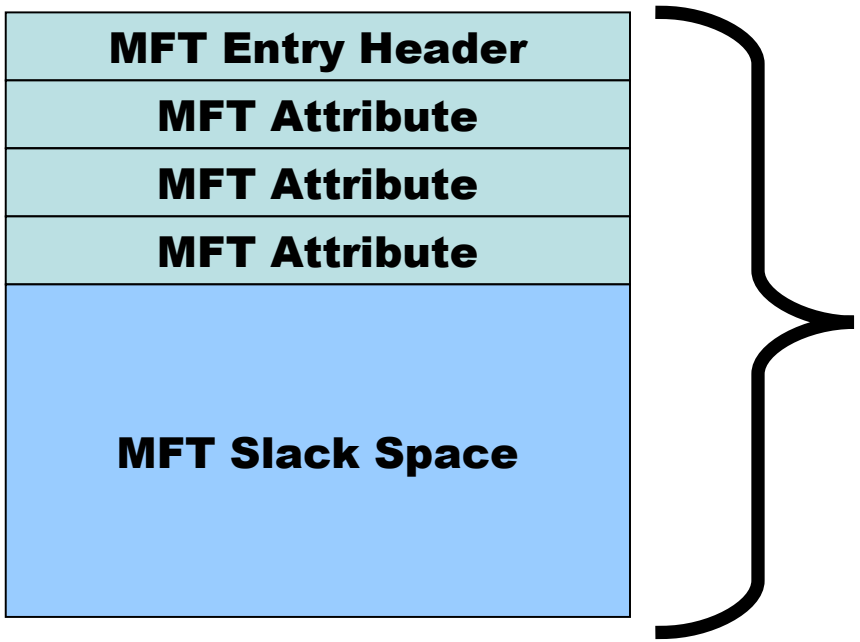
- Forensic tools attacks
  - Implementation bugs
  - Find gaps in tool coverage
  - Trick the tools analysis
  - Counter Technique
    - Use different set of tools
- Disk and data wiping
  - Darik's Boot and Nuke (Dban), Active Killdisk etc.
    - Gutmann's method (old), Secure Erase Standard (HDDerase)
  - Commercial Tools
    - PGP Wipe, Evidence Eliminator, and a lot more…
  - Free Tools
    - Eraser, sdelete.exe, The Defiler's Toolkit (TDT)
  - Anti Forensic Tools
    - http://www.forensicswiki.org/wiki/Category:Anti-forensics_tools
  - Counter Technique
    - Analyze missed pieces

Anti-forensics (AF) III

- Data hiding (nothing new here!)
  - Rootkits have been around for quite some time
  - Attempt to hide data in unusual places
    - Memory – never written to disk
    - Slack space
    - Hidden directories/files
    - Alternate Data Streams
    - Hidden partitions
  - Modify file name/suffix and file header
  - Mix or embed files together
  - Steganography
    - Mixed results on identifying stego

Anti-forensics (AF) IV

- Hiding in file system metadata
  - Journal file, bad blocks or other special place
  - FragFS
    - Hides data within records of the NTFS Master File Table
  - Counter Technique
    - Detailed analysis of the empty metadata areas
    - Closer examination and interpretation of metadata by forensic tools



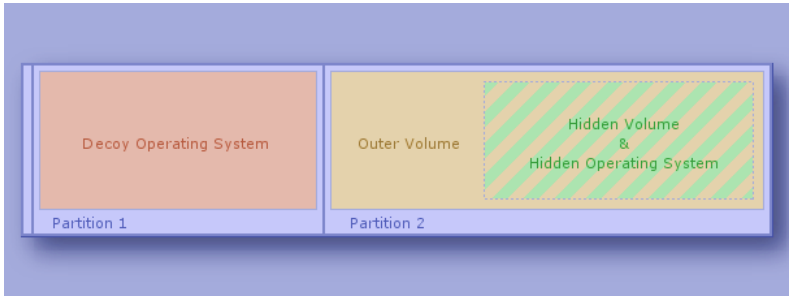
FragFS

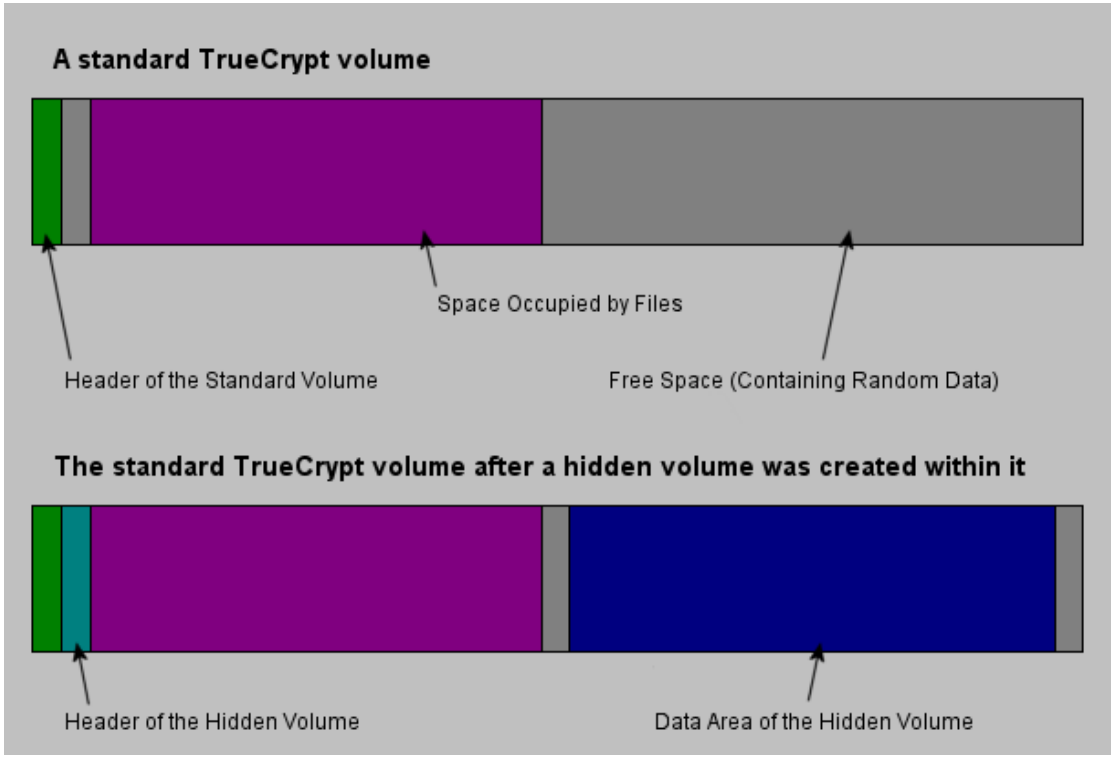
NTFS allocates 1024 bytes per MFT entry.

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

Anti-forensics (AF) V

- Data Encryption
  - Commerical quality free tools
    - TrueCrypt, GnuPG
  - Plausible deniability via hidden TrueCrypt volumes or hidden operating systems





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

Anti-forensics (AF) VI

- 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) – part of MAFIA
    - Encryption, intelligent space selection
  - Bmap (ext2fs)
  - Counter Technique
    - Strings slack space
    - Statistical analysis of slack

#1 timestamps

- Technique
  - Timestamps hint as to when an event occurred
  - Timestamps help an analyst timeline events and profiling attackers behavior
  - If an investigator finds a suspicious file, they will search for other files with similar MAC attributes
- Anti-technique
  - Modify file times, log file entries, and create bogus and misleading timestamps
  - UNIX
    - touch command
  - Windows
    - FAT has MAC
      - Many tools exist
    - NTFS has MACE
      - Timestomp.exe – part of MAFIA

#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 09:45:34AM	12/02/04 09:45:55AM	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) only NTFS

tool #1: timestomp

- TimeStomp <filename> [options]
  - <filename> the name of the file you wish to modify
  - -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
  - <date> "DayofWeek Month\Day\Year HH:MM:SS [AM|PM]"
- EnCase only uses the Standard Information Attribute (SI) (probably fixed by now?)
  - Given
    - The FileName Attribute (FN) MACE values are only updated when a file is created or moved
  - Therefore
    - FN MACE values must be older than SI MACE values

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

#2 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

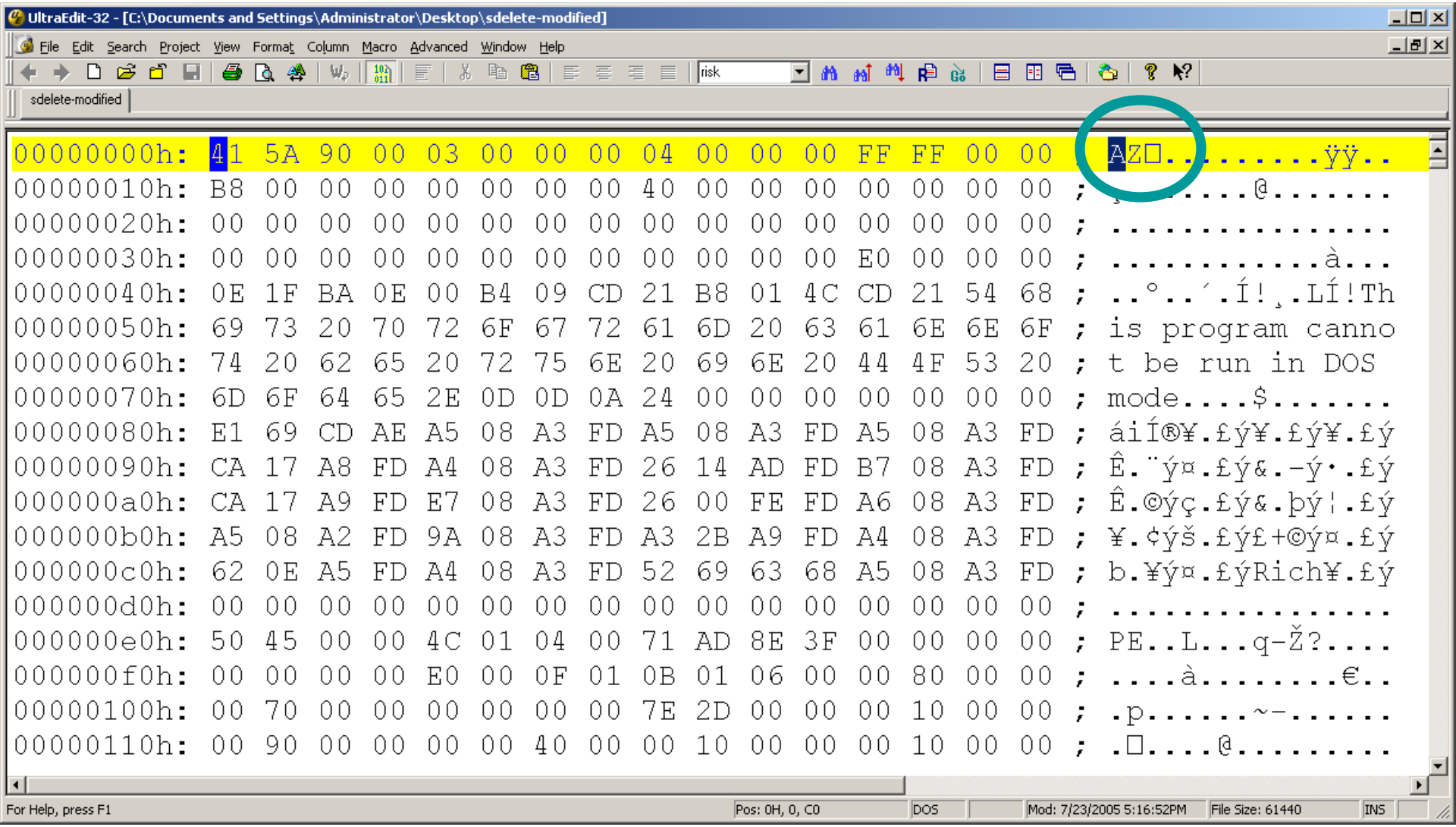
#3 undelete

- 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
- Tools
  - SysInternals – sdelete.exe
    - Doesn't clean file slack space
  - Eraser (Heidi Computers)
    - Does clean file slack space

#4 signature analysis

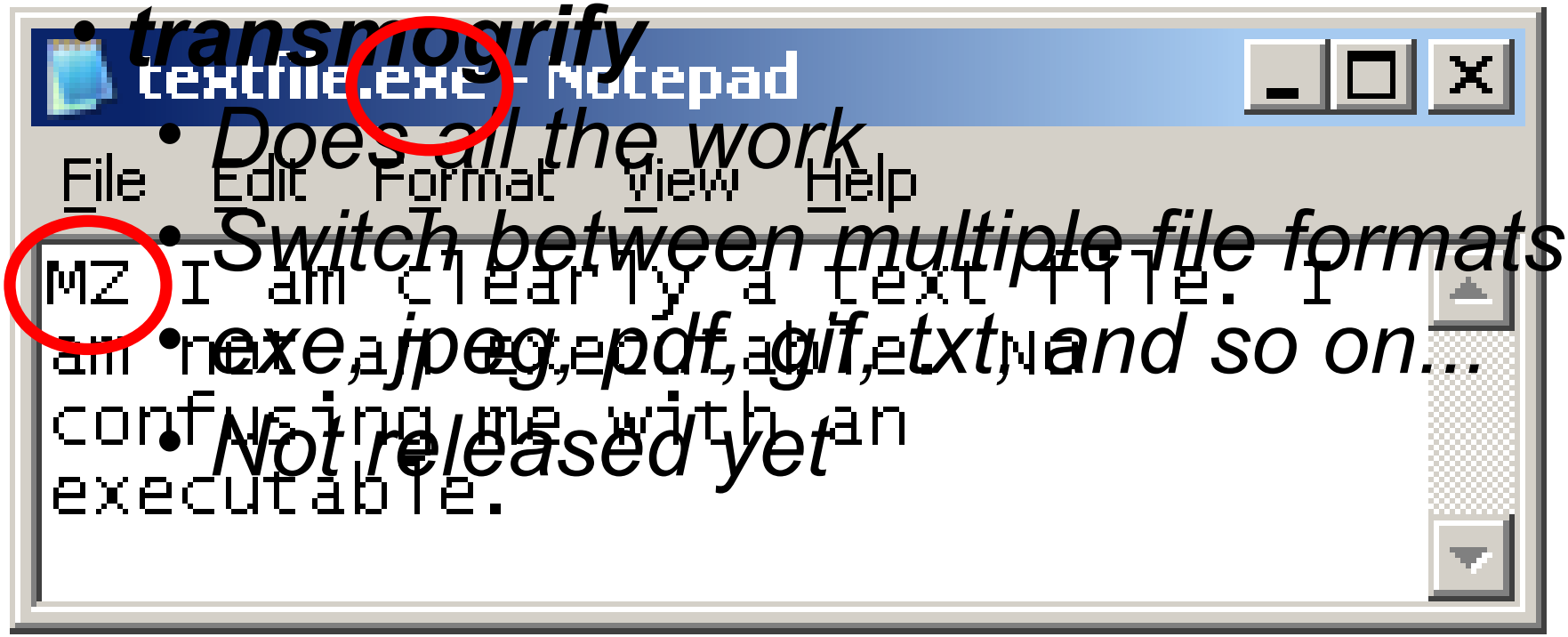
- Technique
  - EnCase has two methods for identifying file types
    - File extension
    - File signatures
- Anti-technique
  - Change the file extension
  - Changing file signatures to avoid EnCase analysis

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…*
    - *Not released yet*



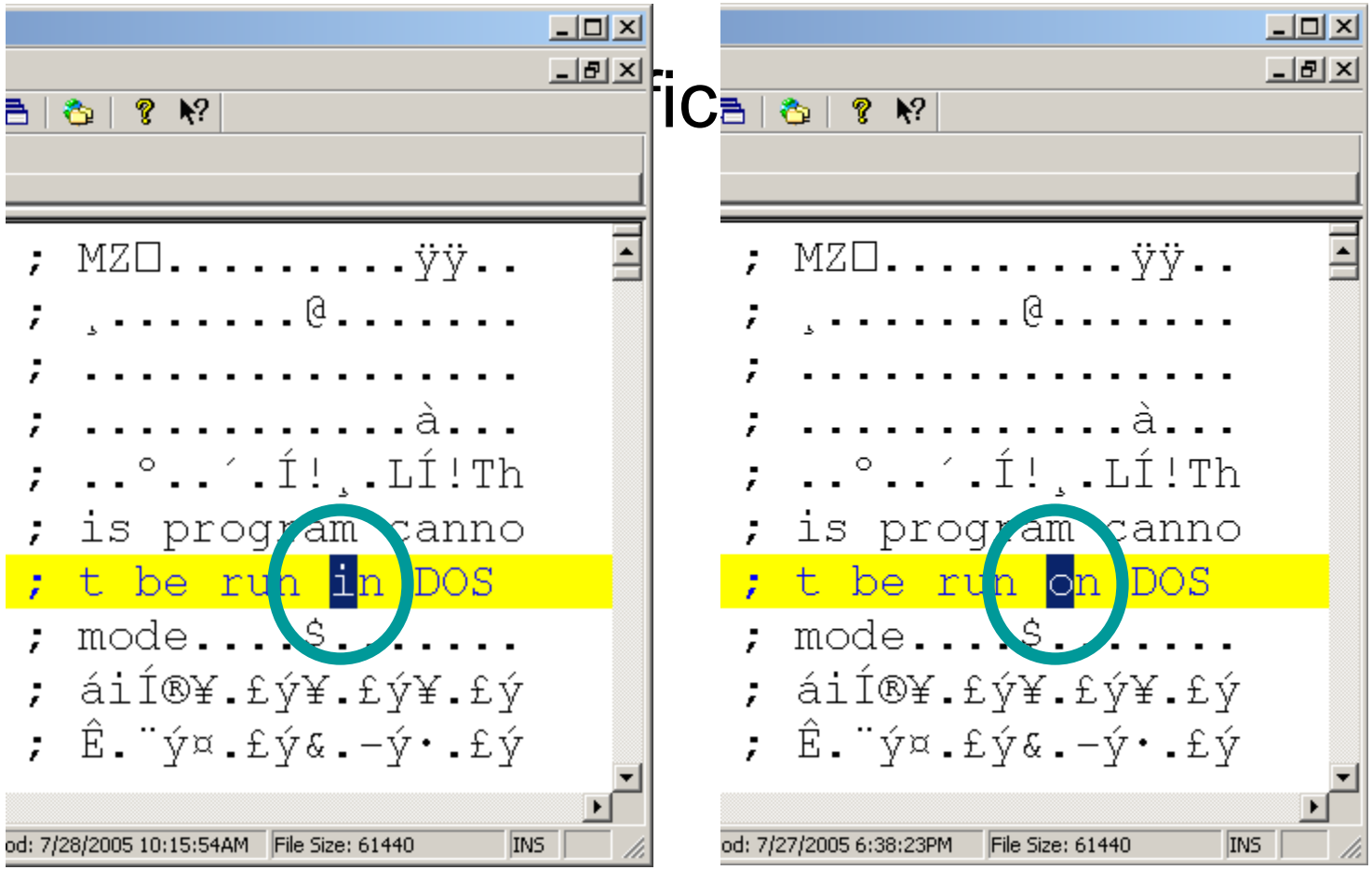
	Name	File Ext	File Type	Signature
21	textfile.exe	exe	Windows Executable	Match

#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** and **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

- fic



#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 (dynamic) analysis
- Anti-technique
  - Use uncommon packers or create a custom loader
  - PEC2 - http://www.bitsum.com/
  - 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 – time is money
  - Businesses will have to make a judgment call of when to stop analysis
  - No pulling-the-plug. Business data takes priority
- Anti-technique
  - Make the investigation cost as much as possible (large drives, RAID, leave a mess)
  - “Help” the investigators
- Opportunity for improvement
  - Prioritize systems analysis
  - Automate analysis as much as possible

#10 hiding in memory

- Technique
  - EnCase Enterprise allows the examiner to see current processes, open ports, file system, etc…
- Anti-technique
  - Metasploit's Meterpreter (Reflective) DLL injection (never hit the disk)
  - Exploit a running process and create threads
- Opportunity for improvement
  - Capture what's in memory

Next Generation Tools

- Summaries for digital video files
  - Extraction of key frames
- Better image classification
  - Beyond hashing - feature identification (FTK4 - EID)
- Searching audio files for voice prints
- Generation of searchable text from audio files using speech recognition
- Automatic detection of steganography, malware etc.
- Background digital evidence preprocessing… (FTK2 >)
  - Analysis of evidence during pre-processing phase
  - Means…investigatory phase can start right away
- Extremely fast searches == uninterrupted brainstorming

Kom ihåg och dagens sanning

- Dokumentera
  - Man kommer inte komma ihåg allt
  - Kanske flera som utreder
- Automatisera
  - Insamling och analys
- Överdriv inte brottslingens kompetens
  - Oftast den enklaste förklaringen
  - Slipper gräva efter något som inte finns
- **"I have no data yet. It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts."**

- Sherlock Holmes