

DEFCON 

# ACL Steganography:

*Permissions to Hide Your Porn*

by Michael Perklin

# Michael Perklin

BaSc, MSIA, CISSP, EnCE, ACE

- Security Professional
- Corporate Investigator (Cyber-Crime)
- Digital Forensic Examiner
  
- Computer Geek + Legal Support hybrid

# In This Talk...

- ✦ What is Steganography?
  - ✦ Historical examples of physical and digital forms
  - ✦ How do they work?
- ✦ ACL Steganography - a new scheme
  - ✦ Demo
  - ✦ How It Works

# What Is Steganography?

- ✦ Greek origin and means "concealed writing"
  - ✦ *steganos* (στεγανός) meaning "covered or protected"
  - ✦ *graphei* (γραφή) meaning "writing"
  - ✦ The term was first coined in 1499, but there are many earlier examples
- ✦ Basically, hiding something in plain sight

# Classical Examples

# Classical Example: Tattoo

- ✦ Tattoo under hair
  - ✦ Encoder tattoos a slave's scalp
  - ✦ Decoder shaves the messenger's hair
- ✦ Problem: The message must be delayed to allow time for hair regrowth
  - ✦ Also...



# Tattoos Are Permanent

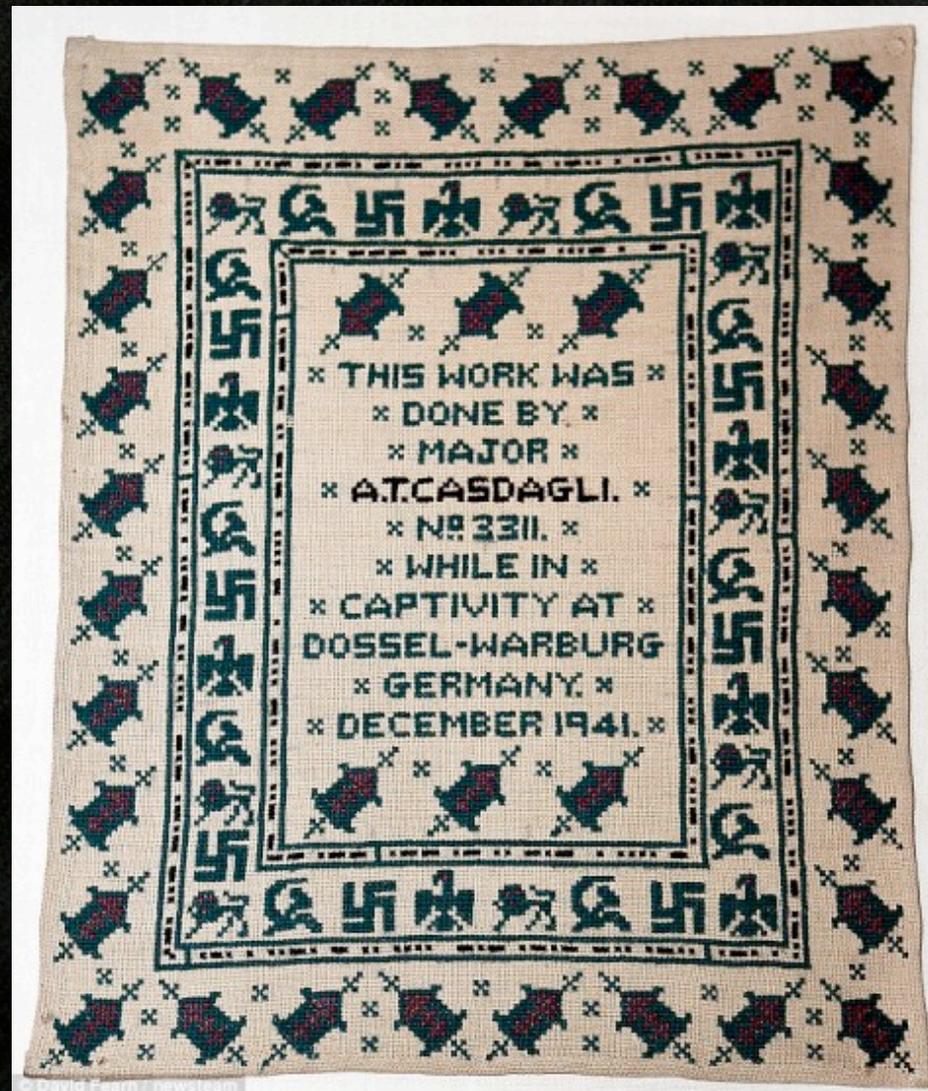
- Oops



# Classical Example: Morse

- Stitch morse code into a sweater/jacket worn by a messenger
- Messenger hand-delivers one message while actually delivering two

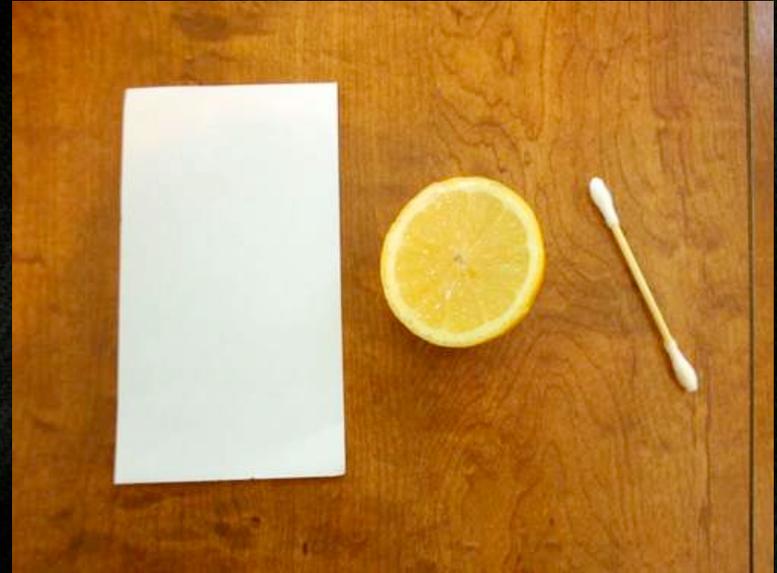




× THIS WORK WAS ×  
× DONE BY ×  
× MAJOR ×  
× A.T. CASDAGLI. ×  
× No 3311. ×  
× WHILE IN ×  
× CAPTIVITY AT ×  
× DOSSEL-WARBURG ×  
× GERMANY. ×  
× DECEMBER 1941. ×

# Classical Example: Invisible Ink

- ✦ Write secrets with lemon juice
- ✦ Allow to dry
- ✦ Decode with heat  
(candle, match, hair dryer, iron)



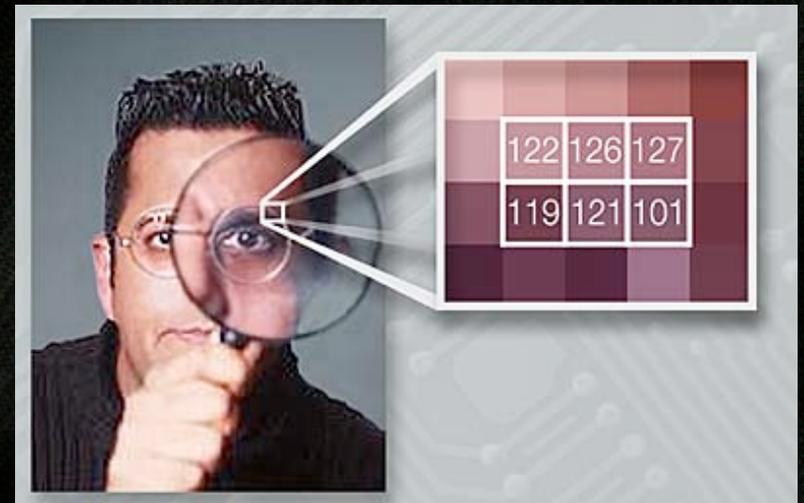
# Decode With Heat



# Digital Steganographic Methods

# Digital Example: Photos

- Files can be encoded as colour information embedded in a photo
- Most common type of digital steganography
- Based on the fact that only super-humans can tell the difference between **Chartreuse** and **Lemon**



# Photo Steganography

- Each pixel is assigned a colour with an RGB colour code
- The last bit of this 8-bit code is overwritten with encoded data
- `#DFFF00` is chartreuse
- `#DFFF01` is.... one of the yellows
- 8 adjacent pixels with 8 slightly-adjusted colours allows 1 byte of encoded information

# Audio Steganography

- ✦ Same principle as photographic steganography, but with audio
- ✦ Humans can't easily tell the difference between 400hz and 401hz, especially if the note isn't sustained
- ✦ Alter each frame of audio with 1 bit of encoded information

# Digital Example: x86 Ops

- Information can be encoded in x86 op codes
  - **NOP** - No Operation
  - **ADD / SUB** - Addition and Subtraction
- PE files (standard .exe programs) have many other areas that can hold arbitrary data

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f			
00000000h:	4D	5A	50	00	02	00	00	00	04	00	0F	00	FF	FF	00	00	; MZP.....ýý..	DOS HEADER	
00000010h:	B8	00	00	00	00	00	00	00	40	00	1A	00	00	00	00	00	; .....ø.....		
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	00	01	00	00	; .....		
00000040h:	BA	10	00	0E	1F	B4	09	CD	21	B8	01	4C	CD	21	90	90	; °....'í!„Lí!□□	DOS STUB	
00000050h:	54	68	69	73	20	70	72	6F	67	72	61	6D	20	6D	75	73	; This program mus		
00000060h:	74	20	62	65	20	72	75	6E	20	75	6E	64	65	72	20	57	; t be run under W		
00000070h:	69	6E	33	32	0D	0A	24	37	00	00	00	00	00	00	00	00	; in32..\$7.....		
00000080h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
00000090h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000000a0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000000b0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000000c0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000000d0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000000e0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000000f0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
00000100h:	50	45	00	00	4C	01	08	00	19	5E	42	2A	00	00	00	00	; PE..L....^B*....		PE HEADER
00000110h:	00	00	00	00	E0	00	8E	81	0B	01	02	19	00	A0	02	00	; ....à.ž□.....		
00000120h:	00	DE	00	00	00	00	00	00	B4	AD	02	00	00	10	00	00	; .P.....'.....		
00000130h:	00	B0	02	00	00	00	40	00	00	10	00	00	00	02	00	00	; °....ø.....		
00000140h:	01	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	; .....		
00000150h:	00	D0	03	00	00	04	00	00	00	00	00	00	02	00	00	00	; .D.....		
00000160h:	00	00	10	00	00	40	00	00	00	00	10	00	00	10	00	00	; .....ø.....		
00000170h:	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	; .....		
00000180h:	00	D0	02	00	1E	18	00	00	00	40	03	00	00	8E	00	00	; .D.....ø...ž..		
00000190h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000001a0h:	00	10	03	00	04	2B	00	00	00	00	00	00	00	00	00	00	; .....+.....		
000001b0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000001c0h:	00	00	03	00	18	00	00	00	00	00	00	00	00	00	00	00	; .....		
000001d0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000001e0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	; .....		
000001f0h:	00	00	00	00	00	00	00	00	43	4F	44	45	00	00	00	00	; .....CODE....		
00000200h:	88	9E	02	00	00	10	00	00	00	A0	02	00	00	04	00	00	; ^ž.....		
00000210h:	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	; .....		
00000220h:	44	41	54	41	00	00	00	00	D4	06	00	00	00	B0	02	00	; DATA....ô.....°..		
																		SECTION TABLE	

- Signature
- FileHeader
- OptionalHeader

DATA  
DIRECTORY

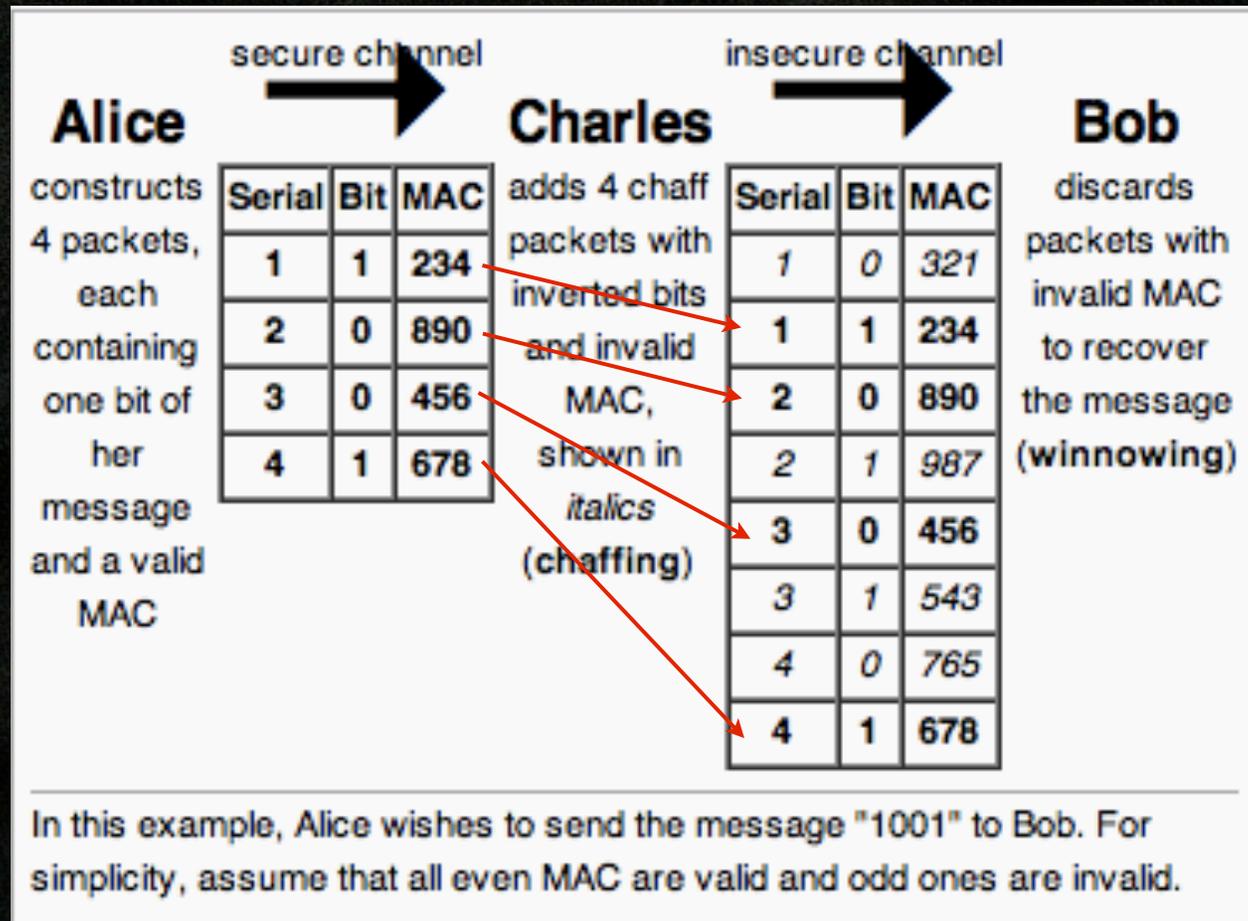
# Digital Example: Chaffing and Winnowing

- ✦ Conceived by Ron Rivest in 1998 (the **R** in **RSA**, as well as **RC4** and others)
- ✦ Not quite steganography
- ✦ Not quite encryption
- ✦ Has properties of both stego and encryption

# Chaffing and Winnowing

- ✦ Sender issues 'real' messages and 'chaff' messages
- ✦ Listeners don't know which messages are real
- ✦ Real chunks of the message pass a parity check
  - ✦ Message Authentication Code (MAC)
- ✦ Receiver calculates MACs on every packet
  - ✦ Discards packets whose MACs aren't valid
  - ✦ Reassembles all packets with valid MACs

# Chaffing and Winnowing



Courtesy: Wikimedia Commons

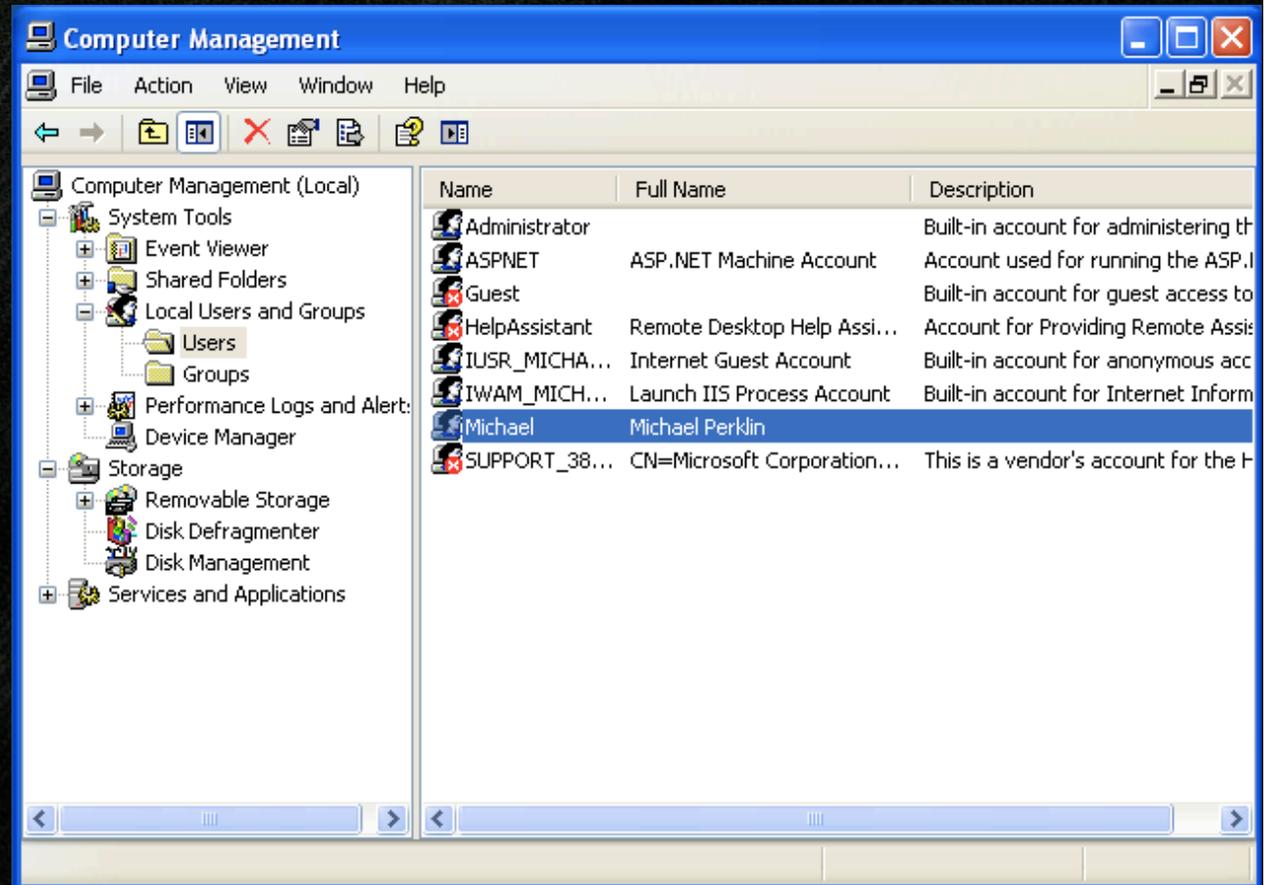
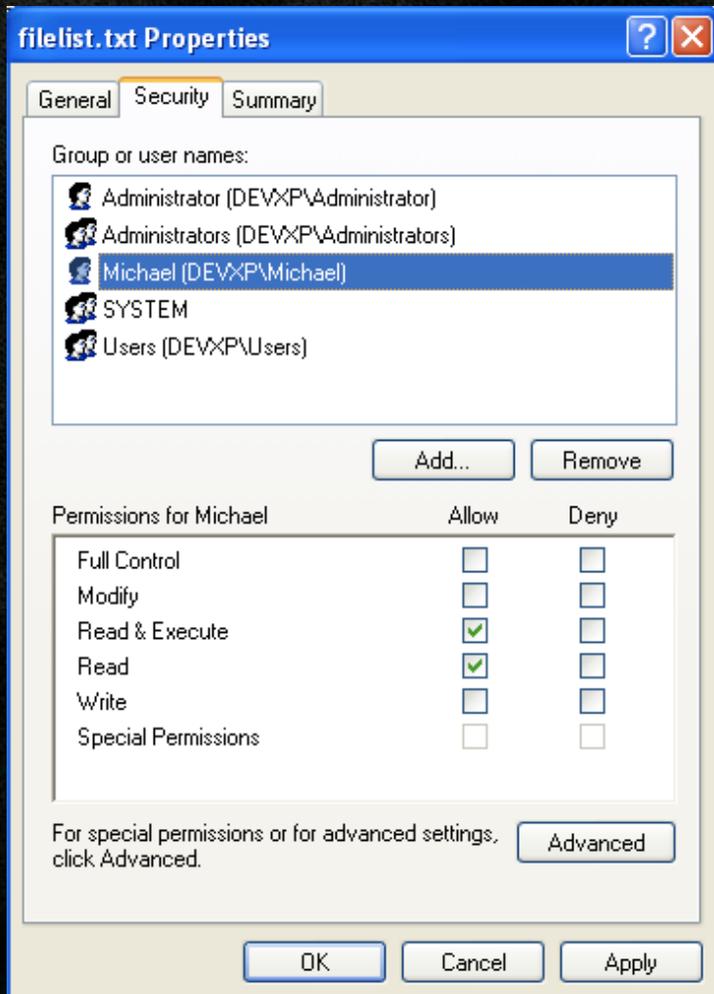
# Steganography Breakdown

- ✦ All types of steganography require three things:
  - ✦ A **medium** of arbitrary information
  - ✦ A **key** or legend for encoding information
  - ✦ A way to **differentiate** 'encoded' and 'medium' info

# ACL Steganography

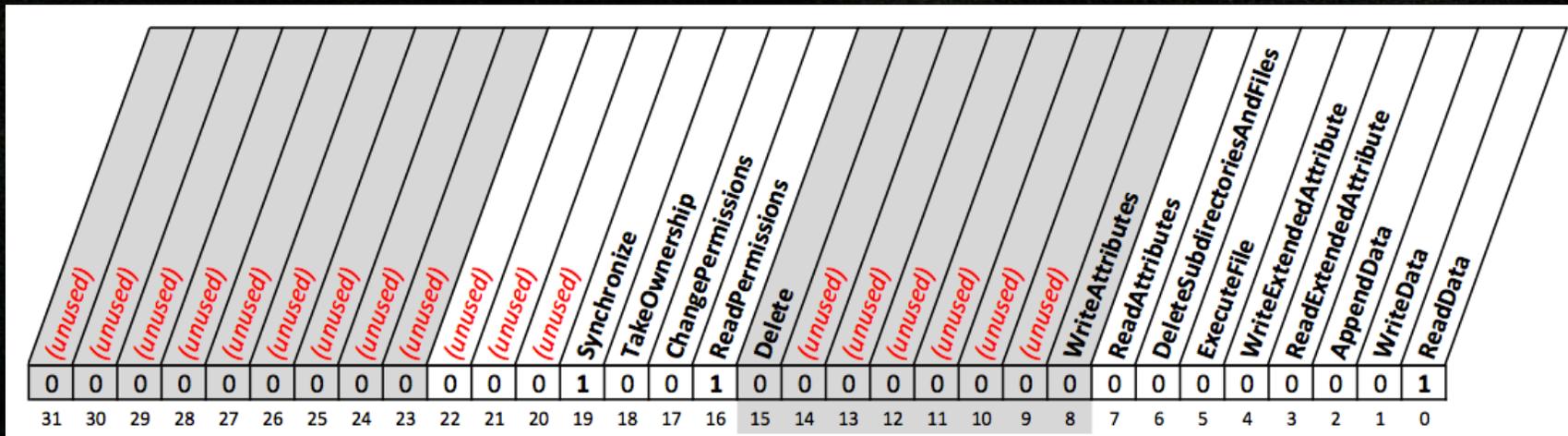
- ✦ A way to encode files as **Access Control Entries** within **Access Control Lists** of files stored on an NTFS volume
  - ✦ Medium: All files on an NTFS volume
  - ✦ Key: Security Identifiers in **ACEs**
  - ✦ Differentiator: **ACEs** with an unlikely combination of permissions

# Background: NTFS Security

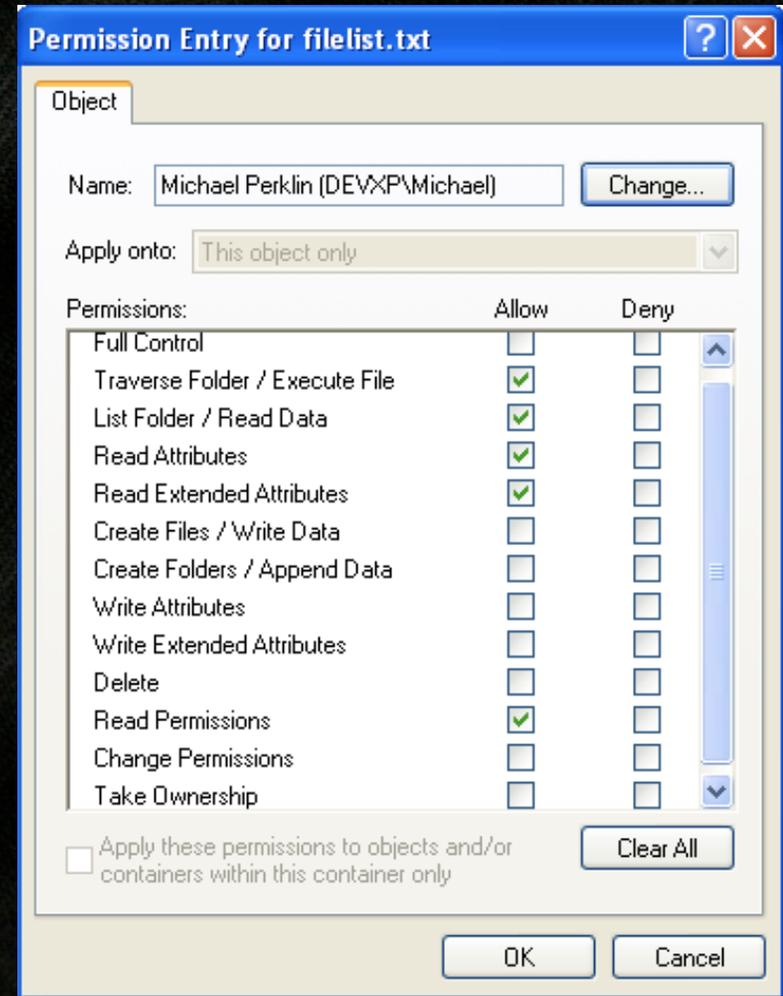
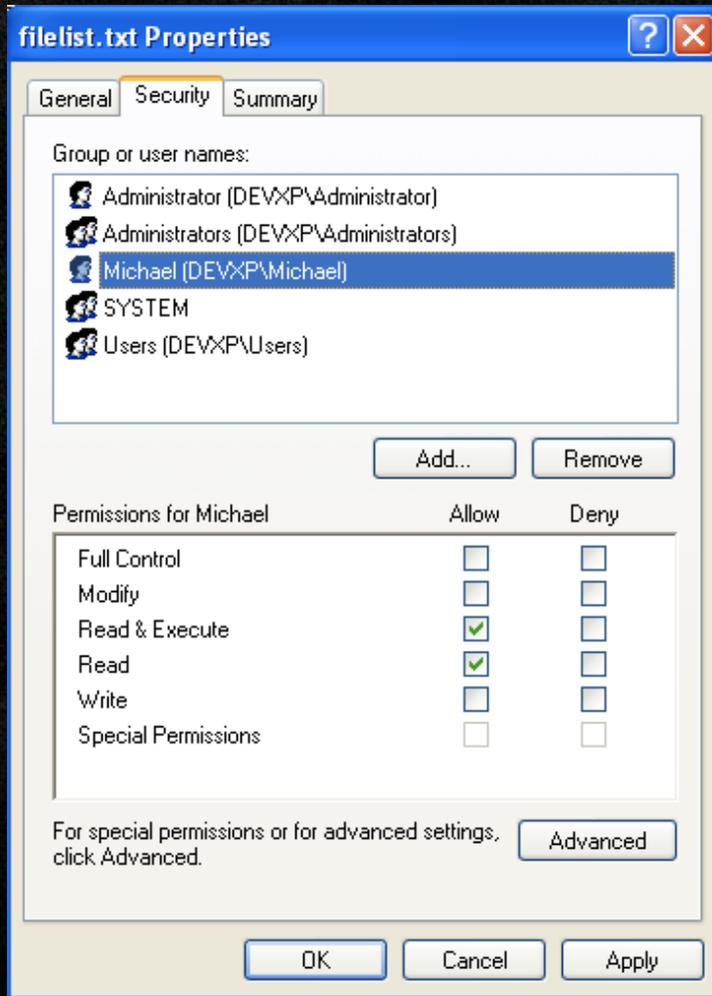


# NTFS Permissions

- ✦ Entries correspond to system users
- ✦ There are 22 unique permissions available, stored in 14 bits of a 32-bit field
- ✦ Many more granular permissions exist than “Read, Write, Execute”

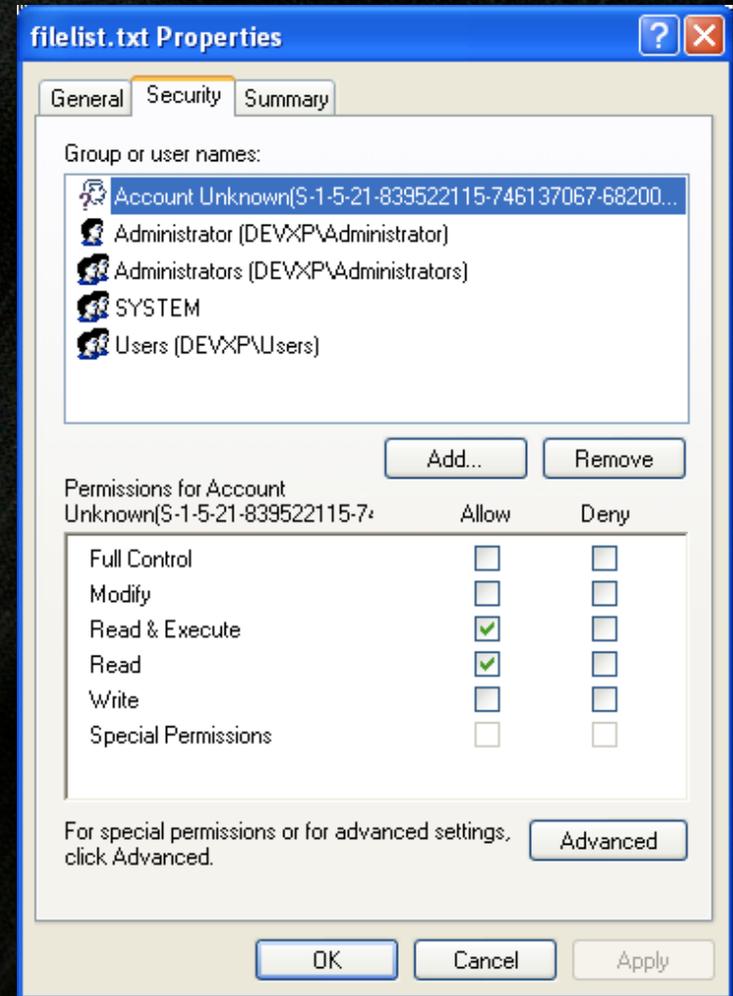


# Simple and Advanced Views



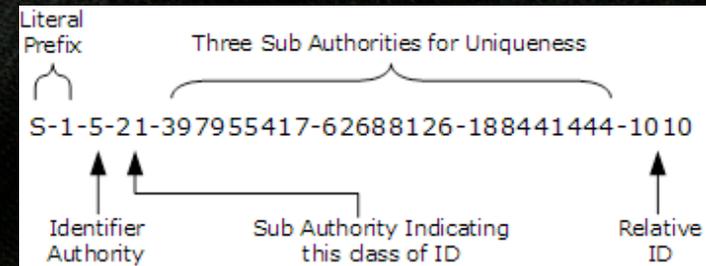
# NTFS Permissions

- ❖ Permission entries are stored using **Security Identifier (S-ID)**
- ❖ If the user is removed, the OS can't look up the friendly name
- ❖ Photo shows same file after "Michael" is removed from OS



# NTFS Security Identifiers

- Maximum Size: 68-bytes
- 1st byte is the revision  
(Always 1)
- 2nd byte is the count of SubAuthorities in this SID  
(Maximum 15 SubAuthorities per SID)
- 6 bytes used for the Identifier Authority  
(Always 000004)
- 60 bytes store the content of the SubAuthorities and the Relative ID



# Acronym Review (AR)

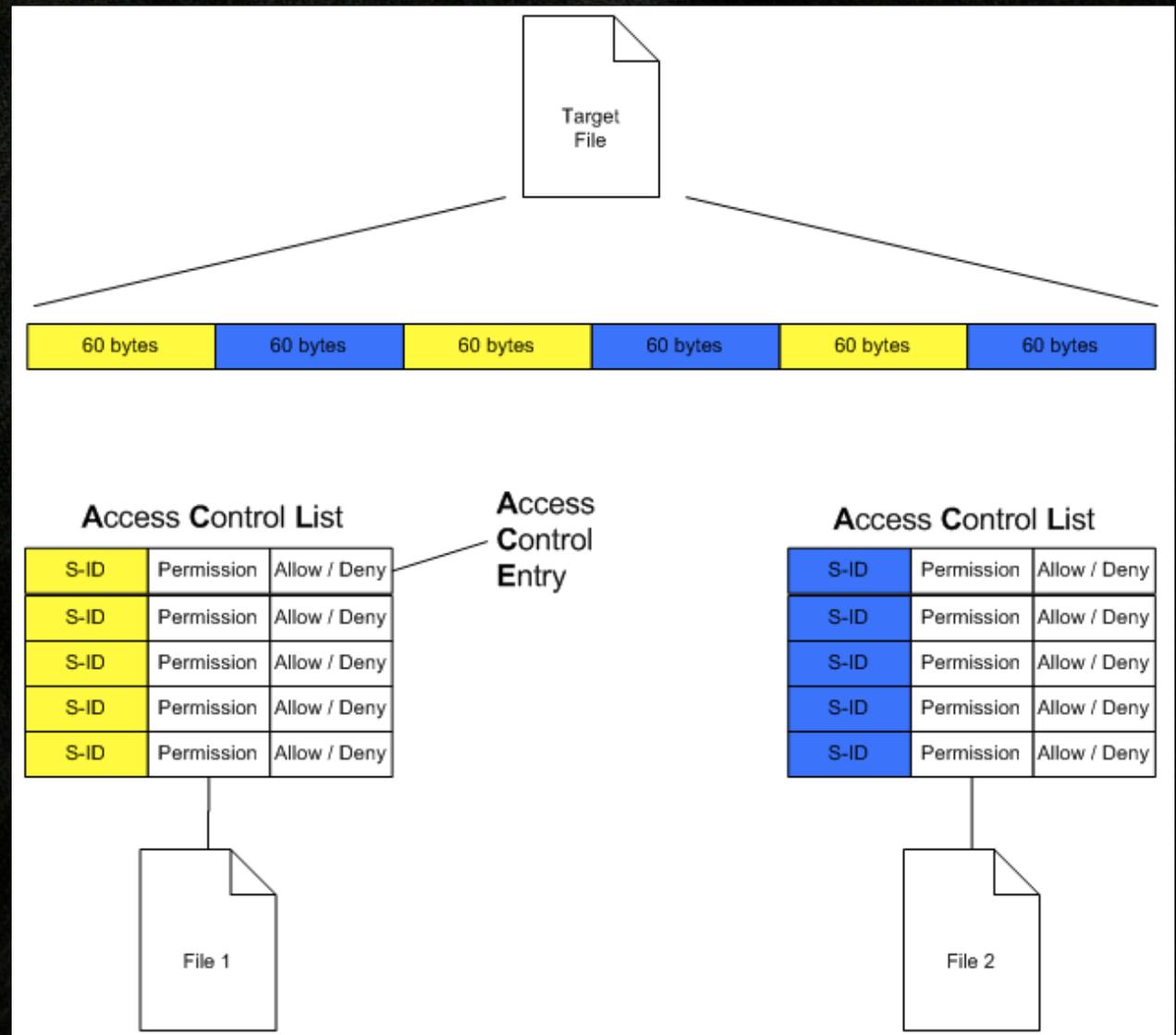
- Access Control List (ACL)
  - A list of Access Control Entries
- Access Control Entry (ACE)
  - A permission rule (allow or deny) pertaining to a SID
- Security Identifier (SID)
  - A unique identifier for a user or group of a Windows system

# Demonstration

- ✦ A folder full of files
- ✦ A filelist.txt with these files
- ✦ A .tc volume with cool stuff in it
- ✦ Encoding the volume
- ✦ Showing the [ACEs](#) on the files
- ✦ Decoding the volume

# ACL Steganography

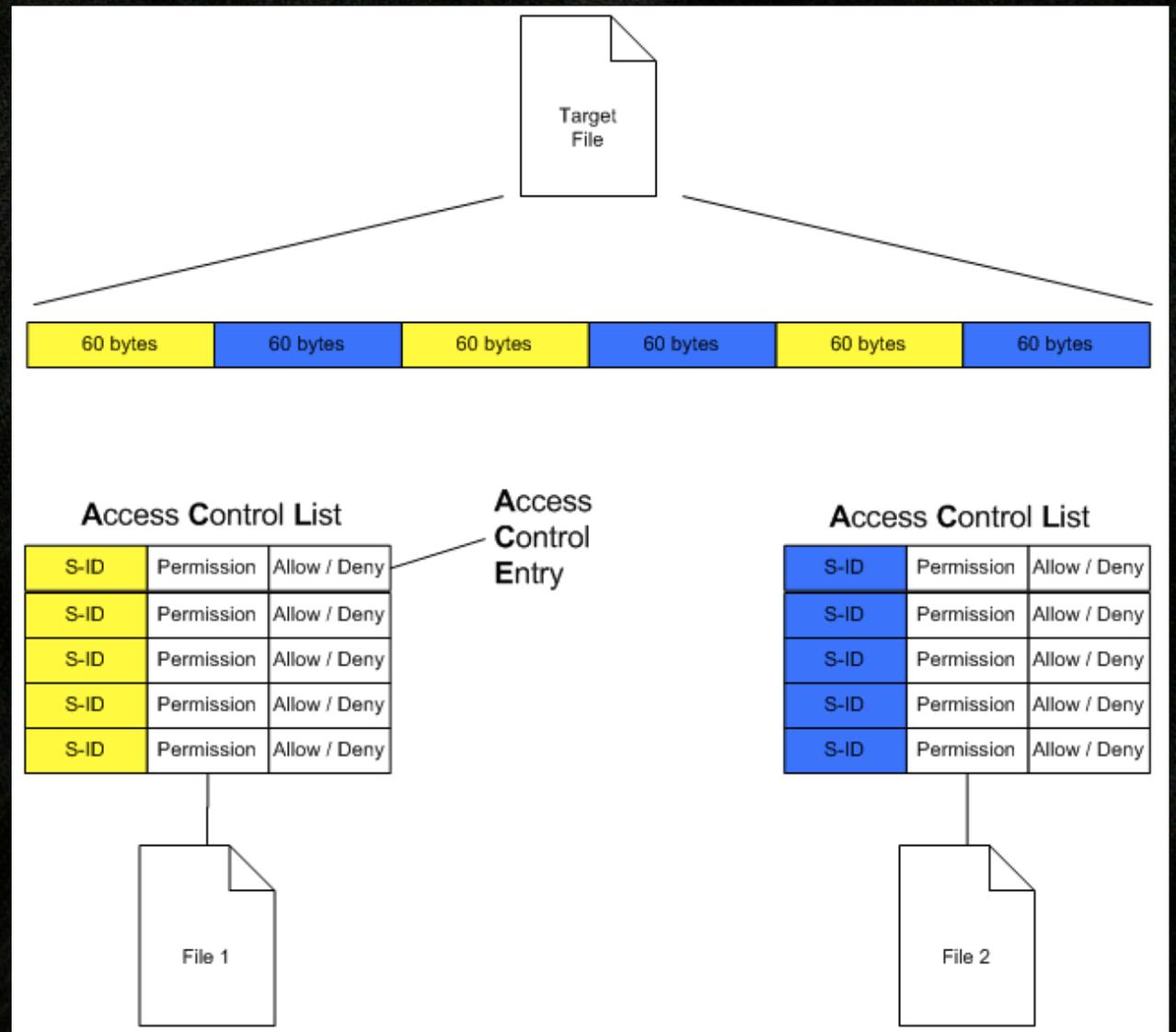
- ✦ A file is split up into 60-byte chunks
- ✦ Each chunk becomes a **SID**



Two files in the FileList.txt

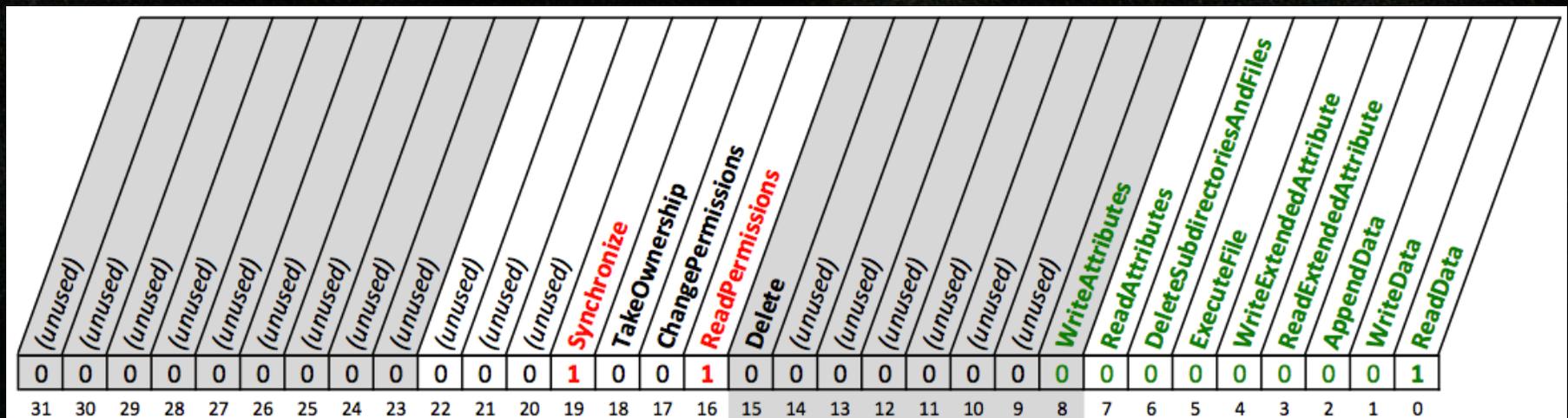
# ACL Steganography

- ❖ ACEs are created with “Allow” permissions for each of these SIDs
- ❖ ACEs are added to the ACLs of multiple files



# ACL Encoding Details

- Two bits are set for all ACL Encoded entries:
  - Synchronize + ReadPermissions
  - Synchronize cannot be set within the Windows UI
- The 9 least significant bits are used as a counter from 0-512



# ACLEncode Details

- ✦ The FileList becomes a kind of symmetric key between the encoder and decoder
- ✦ The list identifies:
  - ✦ Which files have ACLEncoded entries
  - ✦ The order in which those entries are encoded

# Limitations

- An **ACL** can be no bigger than 64kB per file
- Maximum **ACE** size is 76 bytes (68 for **SID** + 8 byte header)
- This produces a theoretical maximum of 862 **ACEs** per file
  - I've imposed a limit of 512 entries per file
  - This leaves room for legitimate permissions

# Limitations

- ✦ The largest possible file to be encoded:
  - ✦  $\text{NumFilesInList} * 512 * 60\text{bytes}$
  - ✦ or about 30KB per file
- ✦ Need to store a larger file? Use a longer file list.

# \$SECURE File Limitation

- ✦ The `$SECURE` file is a hidden file on every NTFS volume
- ✦ All `ACLs` for all files are stored in this one file
- ✦ Each time a new `SID` is encountered, it's added to this file
  - ✦ This way, future permission operations for that user can use the existing reference without duplicating it

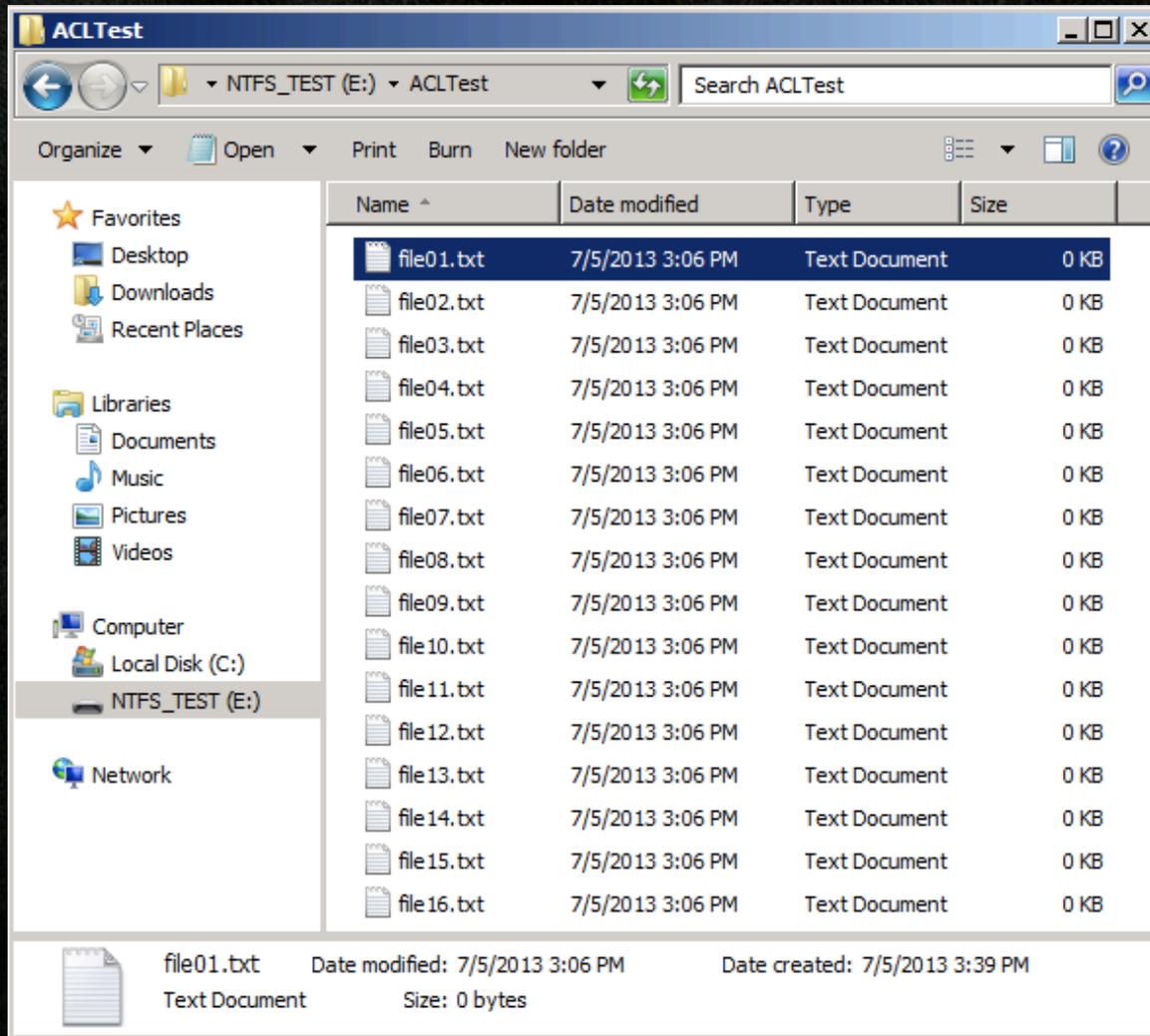
# \$SECURE File Limitation

- NTFS does \*NOT\* remove old/unused **SIDs** from the **\$SECURE** file
- The **\$SECURE** file is designed only to grow in size and never shrink
- This means, every ACLEncoded chunk from every run of ACLEncode will persist here **forever**

# A Forensic Review

- ✦ I conducted a test:
  - ✦ 2GB USB Key, formatted as NTFS
  - ✦ AccessData FTK 4.0.2.33
  - ✦ Guidance EnCase Forensic 6.19.6

# Forensic Test - File List



ACLTest

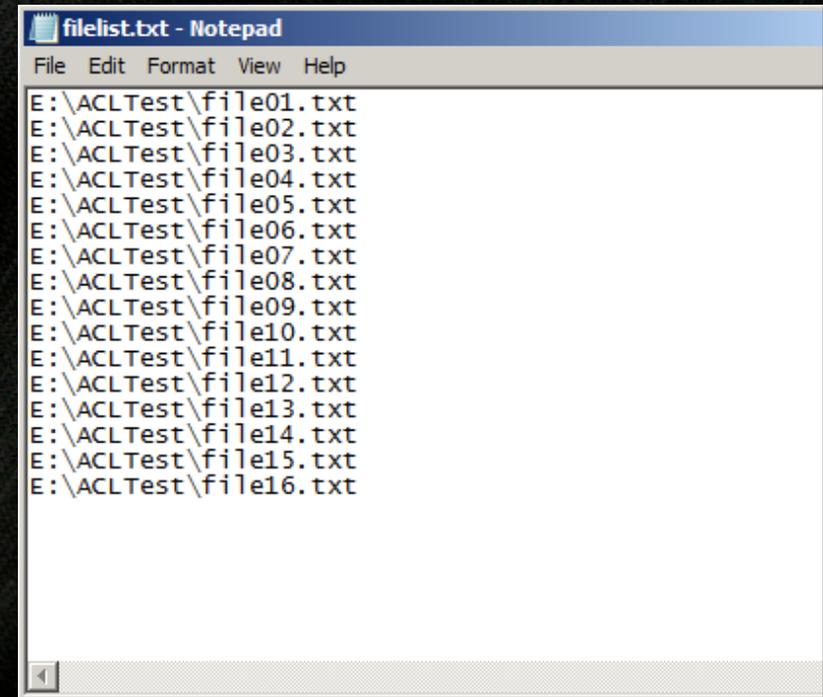
NTFS\_TEST (E:) > ACLTest

Search ACLTest

Organize Open Print Burn New folder

Name	Date modified	Type	Size
file01.txt	7/5/2013 3:06 PM	Text Document	0 KB
file02.txt	7/5/2013 3:06 PM	Text Document	0 KB
file03.txt	7/5/2013 3:06 PM	Text Document	0 KB
file04.txt	7/5/2013 3:06 PM	Text Document	0 KB
file05.txt	7/5/2013 3:06 PM	Text Document	0 KB
file06.txt	7/5/2013 3:06 PM	Text Document	0 KB
file07.txt	7/5/2013 3:06 PM	Text Document	0 KB
file08.txt	7/5/2013 3:06 PM	Text Document	0 KB
file09.txt	7/5/2013 3:06 PM	Text Document	0 KB
file10.txt	7/5/2013 3:06 PM	Text Document	0 KB
file11.txt	7/5/2013 3:06 PM	Text Document	0 KB
file12.txt	7/5/2013 3:06 PM	Text Document	0 KB
file13.txt	7/5/2013 3:06 PM	Text Document	0 KB
file14.txt	7/5/2013 3:06 PM	Text Document	0 KB
file15.txt	7/5/2013 3:06 PM	Text Document	0 KB
file16.txt	7/5/2013 3:06 PM	Text Document	0 KB

file01.txt Date modified: 7/5/2013 3:06 PM Date created: 7/5/2013 3:39 PM  
Text Document Size: 0 bytes



filelist.txt - Notepad

File Edit Format View Help

```
E:\ACLTest\file01.txt  
E:\ACLTest\file02.txt  
E:\ACLTest\file03.txt  
E:\ACLTest\file04.txt  
E:\ACLTest\file05.txt  
E:\ACLTest\file06.txt  
E:\ACLTest\file07.txt  
E:\ACLTest\file08.txt  
E:\ACLTest\file09.txt  
E:\ACLTest\file10.txt  
E:\ACLTest\file11.txt  
E:\ACLTest\file12.txt  
E:\ACLTest\file13.txt  
E:\ACLTest\file14.txt  
E:\ACLTest\file15.txt  
E:\ACLTest\file16.txt
```



AccessData FTK 4

Evidence Items

- Evidence
  - USBKey.aff
    - Partition 1
      - NTFS\_TEST [NTFS]
        - [orphan]
        - [root]
          - \$BadClus
          - \$Extend
          - \$Secure
          - ACLTest
          - [unallocated space]
        - Unpartitioned Space [basic disk]

Properties

**NTFS Information**

MFT Record Number	36
Record date	7/5/2013 3:41:20 PM (2013-07-05 19:41:20 UTC)
Resident	True
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-2565687063-2636845177-2300264073-1000
Group SID	S-1-5-21-2565687063-2636845177-2300264073-513

**File Content Info**

File Content Properties Hex Interpreter

File List

Item #	Name	P-Size	L-Size	Group SID (NTFS)	Owner SID	Alterna...
93042	file01.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93043	file02.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93044	file03.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93045	file04.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93046	file05.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93047	file06.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93048	file07.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93049	file08.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93050	file09.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93051	file10.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93052	file11.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93053	file12.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	
93054	file13.txt	0 B	0 B	S-1-5-21-2565687063-2636845177-2300264073-513	S-1-5-21-2565687063-2636845177-2300264073-1000	

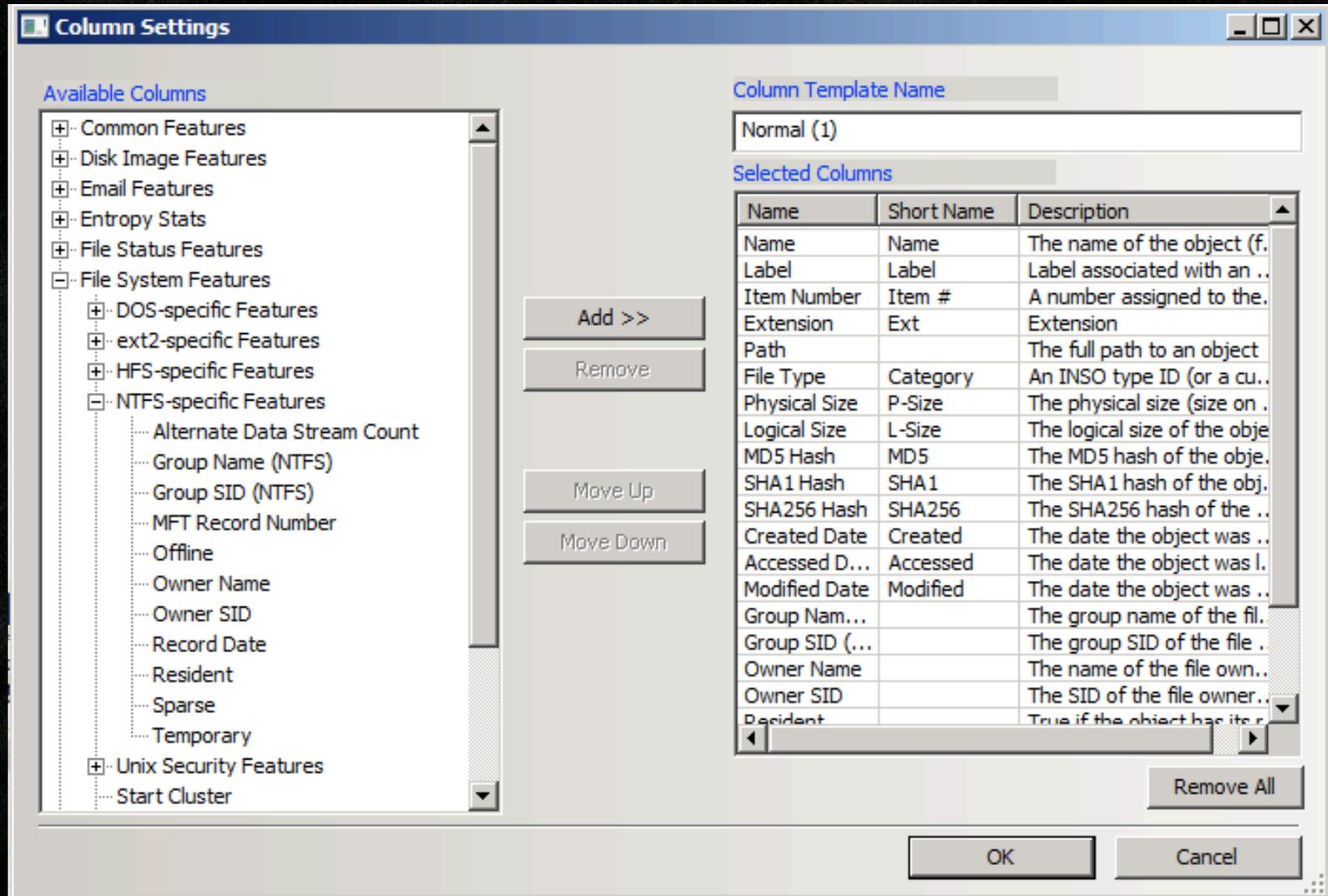
Loaded: 17 Filtered: 17 Total: 17 Highlighted: 1 Checked: 0 Total LSize: 4096 B

USBKey.aff/Partition 1/NTFS\_TEST [NTFS]/[root]/ACLTest/file01.txt

Ready

Explore Tab Filter: [None]

# Forensic Test - FTK4



# Forensic Test - FTK4

- ✦ FTK4 has no way to show [Access Control Lists](#) of files
  - ✦ Contacted their tech support
  - ✦ Discussed on their user forum
  - ✦ “Use another tool”

AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: ACLTest

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Evidence Items

Evidence

- USBKey.aff
  - Partition 1
    - NTFS\_TEST [NTFS]
      - [orphan]
      - [root]
        - \$BadClus
        - \$Extend
        - \$Secure
        - ACLTest
        - [unallocated space]
  - Unpartitioned Space [basic disk]

File Content

Hex	Text	Filtered	Natural
003a0	00 00 00 00 14 00 00 00-02 00 68 00 02 00 00 00		.....h.....
003b0	00 00 4C 00 00 00 12 00-01 0F 00 00 00 00 00 04		..L.....
003c0	44 45 46 43 4F 4E 58 58-49 20 44 45 46 43 4F 4E		DEFCONXXI DEFCON
003d0	58 58 49 20 44 45 46 43-4F 4E 58 58 49 20 44 45		XXI DEFCONXXI DE
003e0	46 43 4F 4E 58 58 49 20-44 45 46 43 4F 4E 58 58		FCONXXI DEFCONXX
003f0	49 20 44 45 46 43 4F 4E-58 58 49 20 00 10 14 00		I DEFCONXXI .....
00400	FF 01 1F 00 01 01 00 00-00 00 00 01 00 00 00 00		ÿ.....
00410	01 05 00 00 00 00 00 00-15 00 00 00 17 47 ED 98		.....Gí.
00420	79 10 2B 9D 89 3E 1B 89-E8 03 00 00 01 05 00 00		y+...>..è.....
00430	00 00 00 05 15 00 00 00-17 47 ED 98 79 10 2B 9D		.....Gí.y+.
00440	89 3E 1B 89 01 02 00 00-00 00 00 00 00 00 00 00		->.....
00450	FB 98 56 E3 08 01 00 00-50 04 00 00 00 00 00 00		û.Vã....P.....
00460	C8 00 00 00 01 00 04 84-7C 00 00 00 98 00 00 00		È..... .....
00470	00 00 00 00 14 00 00 00-02 00 68 00 02 00 00 00		.....h.....

Sel start = 960, len = 60; clus = 164128; log sec = 1313025; phy sec = 1313057

File Content Properties Hex Interpreter

File List

Item #	Name	P-Size	L-Size	Group SID (NTFS)	Owner SID	Alter
93036	\$SDH	4096 B	4096 B	S-1-5-32-544	S-1-5-18	
93035	\$SDS	260.0 KB	257.8 KB	S-1-5-32-544	S-1-5-18	
93037	\$SII	4096 B	4096 B	S-1-5-32-544	S-1-5-18	

Loaded: 3 Filtered: 3 Total: 3 Highlighted: 1 Checked: 0 Total LSize: 265.8 KB

USBKey.aff/Partition 1/NTFS\_TEST [NTFS]/[root]/\$Secure/\$SDS

Ready Explore Tab Filter: [None]

# Guidance EnCase Forensic 6

# Forensic Test - EnCase 6

The screenshot displays the EnCase Forensic software interface. The main window is titled "EnCase Forensic" and contains a menu bar (File, Edit, View, Tools, Help) and a toolbar with icons for New, Open, Save, Print, Add Device, Search, and Refresh. Below the toolbar is a "Cases" pane with a tree view showing a hierarchy: Home, Entries, Bookmarks, and Search. Under "Home", there are sub-items for "File Extents" and "Permissions". The "Entries" folder is expanded, showing a "USBKEY" folder, which is further expanded to show a "C" drive, containing "\$Extend" and "ACLTest" folders. Two red arrows point from the left side of the screen to the "Home" and "Permissions" sub-items in the tree view.

The main area of the interface is a table with the following columns: Name, Filter, In Report, File Ext, File Type, File Category, Signature, and Description. The table contains 11 rows of data, all representing text files named file01.txt through file11.txt. The first row is selected.

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description
<input checked="" type="checkbox"/>	1	file01.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	2	file02.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	3	file03.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	4	file04.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	5	file05.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	6	file06.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	7	file07.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	8	file08.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	9	file09.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	10	file10.txt	No	txt	Text	Document		File, Archive
<input type="checkbox"/>	11	file11.txt	No	txt	Text	Document		File, Archive

At the bottom of the interface, there is a "Text" pane showing the content of the selected file, which is "Empty File". To the right of the text pane is a "Console" pane with a tree view showing a hierarchy of folders: EnScript, CF2 EnScripts, Enterprise, Examples, and Forensic.

The status bar at the bottom of the window displays the file path: ACLTEST\USBKEY\C\ACLTest\file01.txt (PS 1337432 LS 1337400 CL 167175 SO 288 FO 0 LE 1)

# Forensic Test - EnCase 6

The screenshot displays the EnCase Forensic application window. The main area shows a table with the following data:

	Name	Id	
1		S-1-4-1128678724-1482182223-1162092617-1313817414-541677656-1128...	Al
2	Everyone	S-1-1-0	Al
3		S-1-5-21-2565687063-2636845177-2300264073-1000	Or
4	Domain Users	S-1-5-21-2565687063-2636845177-2300264073-513	Gr

A red arrow points from the left side of the interface towards the first row of the table. The bottom of the window shows a toolbar with options like Text, Hex, Doc, Transcript, Picture, Report, Console, EnScript, Filters, Conditions, Display, and Queries. The status bar at the bottom indicates the current file path: ACLTEST\USBKEY\C\ACLTest\file01.txt (PS 1337432 LS 1337400 CL 167175 SO 288 FO 0 LE 1).

# Forensic Test - EnCase 6

The screenshot displays the EnCase Forensic application window. The interface includes a menu bar (File, Edit, View, Tools, Help), a toolbar with icons for New, Open, Save, Print, Add Device, Search, Refresh, and Find, and a main workspace divided into several panes.

**File List Table:**

	Name	Filter	In Report	File Ext	File Type	File Category	Signature
<input type="checkbox"/>	13	\$Secure	No				File, Inte
<input type="checkbox"/>	14	\$Secure:\$SII	No				File, Inte
<input type="checkbox"/>	15	\$Secure:\$SDH	No				File, Inte
<input type="checkbox"/>	16	\$Secure:\$SDS	No				File, Inte
<input type="checkbox"/>	17	\$UpCase	No				File, Inte
<input type="checkbox"/>	18	MFT Allocation ...	No				File, Bitm
<input type="checkbox"/>	19	Volume Slack	No				File, Unal

**Hex Dump:**

```
000795 L .....ÿ.....  
000848 Gi0y +00>·0è.....Gi0y +00>·0.....û0Vã·  
000901 ····0|···0···h····L····  
000954 ····DEFCOXXI DEFCOXXI DEFCOXXI DEFCOXXI DEFCOXXI  
001007XI DEFCOXXI ····ÿ.....Gi0y +0  
0010600>·0è.....û0Vã····P  
001113 ····0|···0···h····L····  
001166 ····DEFCOXXI DEFCOXXI DEFCOXXI DEFCOXXI DEFCOXXI D  
001219EFCOXXI ····ÿ.....Gi0y +00>·0  
001272è.....Gi0y +00>·0.....û,Vã ····  
001325 ····0|···0···h····L····DE  
001328FCOXXI DEFCOXXI DEFCOXXI DEFCOXXI DEFCOXXI DEFCO  
ACLTEST\USBKEY\C\Secure:$SDS (P5 1313057 LS 1313025 CL 164128 SO 448 FO 960 LE 60)
```

**EnScript Panel:**

- EnScript
  - CF2 EnScripts
  - Enterprise
  - Examples
  - Forensic
  - Include
  - Main
  - Source Processor

# Forensic Detection of ACLEncoding

- Detection of ACLEncoded entries is a manual process
  - (using the most popular forensic tools)
- Detection can be automated with the creation of EnScripts (EnCase's scripting language) and other purpose-built tools
- Unfortunately not enough time to go over these today

# Questions and Answers

- If you have questions, see me in the Speaker Q&A room
- Thanks to Josh, Nick, Joel, Reesh, Kyle for their help with testing
- Thanks to my family, my friends, my colleagues, and my employer for providing me the time for this research
- Thanks to Eugene Filipowicz for seeding the thought in my mind:  
*“How can you hide data on a drive without detection?”*

# ACLEncode

**Source Code**



DEFCON 21  
Michael Perklin

**Latest Slides**



<http://www.perklin.ca/~defcon21/ACLEncode.zip>

<http://www.perklin.ca/~defcon21/aclsteganography.pdf>

# References

- <http://msdn.microsoft.com/en-us/library/gg465313.aspx>
- <http://stackoverflow.com/questions/1140528/what-is-the-maximum-length-of-a-sid-in-sddl-format>
- <http://technet.microsoft.com/en-us/library/cc962011.aspx>
- [http://msdn.microsoft.com/en-CA/library/ms229078\(v=vs.85\).aspx](http://msdn.microsoft.com/en-CA/library/ms229078(v=vs.85).aspx)
- <https://github.com/mosa/Mono-Class-Libraries/blob/master/mcs/class/corlib/System.Security.AccessControl/FileSystemRights.cs>
- <http://msdn.microsoft.com/en-us/library/system.security.accesscontrol.filesystemrights.aspx>
- <http://www.ntfs.com/ntfs-permissions-access-entries.htm>
- <http://www.ntfs.com/ntfs-permissions-security-descriptor.htm>
- <http://support.microsoft.com/kb/279682>