DEFC_®N

ACL Steganography: Permissions to Hide Your Porn by Michael Perklin

Michael Perklin

- Corporate Investigator
- Digital Forensic Examiner
- Security Professional
- eDiscovery Administrator
- Computer Geek + Legal Support hybrid

Michael Perklin

- Diploma in Computer Science Technology
- Bachelor's Degree in Information Systems Security
- Master's Degree in Information Assurance
- EnCase Certified Examiner (EnCE)
- AccessData Certified Examiner (ACE)
- Certified Information Systems Security Professional (CISSP)

In This Talk...

- What is Steganography?
 - Historical examples of physical and digital forms
 - How do they work?
- Identifying a "Lowest Common Denominator"
- ACL Steganography a new scheme

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 Example: Tattoo

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



Tattoos Are Permanent





Classical Example: Morse

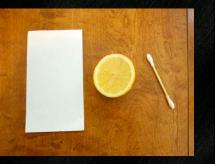
- Stitch morse code into a sweater/jacket worn by a messenger
- Messenger hand-delivers one message while actually delivering two





Classical Example: Invisible Ink

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



Decode With Heat



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

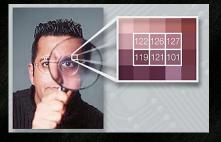


Photo Steganography

- 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

	Q	1	2	3	4	Ş	Ģ	7	ş	9		ç		ţ	_		
00000000h:			50													MZPÿÿ	DOS
																······6·····	
											 		 				HEADER
																°'.Í!,.LÍ!OO	
00000050h:																This program mus	DOS
00000060h:																t be run under W	STUB
																in32\$7	0100
															Ľ.		
											 		 		Ľ.		
															Ľ.		
															Ľ.		
																	PE
																PEL^B*	HEADER
																à.ŽD	HEADER
																.Þ	Signature
00000130h: 00000140h:																	- orginature
																	FileHeader
																.Đĝž	
																	OptionalHeader
																+	DATA
																	DIRECTORY
																	DIRECTORT
																CODE	
																^ ž	
											 		 				SECTION
																DATAô°	
											 		 		•		

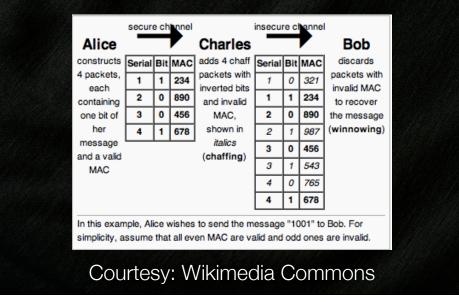
Digital Example: Chaffing and Winnowing

- 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 include a parity value
 - 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



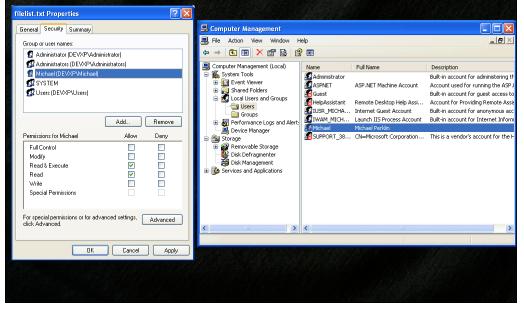
Steganography Breakdown

- 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 a 32-bit field
- Many more granular permissions exist than "Read, Write, Execute"

Name: Michael Perklin (DEVXP\Mic	hael)	Change
Apply onto: This object only		~
Permissions:	Allow	Deny
Full Control		~
Traverse Folder / Execute File	 Image: A start of the start of	
List Folder / Read Data		
Read Attributes		
Read Extended Attributes	~	
Create Files / Write Data		
Create Folders / Append Data		
Write Attributes Write Extended Attributes		
Write Extended Attributes Delete		
Bead Permissions	Image: A start of the start	
Change Permissions		
Take Ownership		
- Apply these permissions to objects a	and/or	Clear All
containers within this container only	1	
	ПК	Cancel

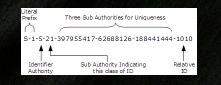
NTFS Permissions

- 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

elist.txt Properties		? 🛽
ieneral Security Summary		
Group or user names:		
🖗 Account Unknown(S-1-5-21-	839522115-7461	37067-68200
🙍 Administrator (DEVXP\Admin	istrator)	
🚮 Administrators (DEVXP\Admi	nistrators)	
🚮 SYSTEM		
🕵 Users (DEVXP\Users)		
Permissions for Account	Add	Remove
Unknown(S-1-5-21-839522115-7+	Allow	Deny
Full Control		
Modify		
Read & Execute	~	
Read	~	
Write		
Special Permissions		
For special permissions or for adva click Advanced.	nced settings, [Advanced
ПК	Cancel	Apply

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

ACL Steganography

- (photo of file with 60byte chunks)
- A file is split up into 60-byte chunks
- Each chunk becomes a SID
- ACEs are created with "Allow" permissions for each of these SIDs
- ACEs are added to the ACLs of multiple files

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

ACLEncoding Details

- Two bits are set for all ACLEncoded entries:
 - Synchronize + ReadPermissions
 - Synchronize cannot be set within the Windows UI
- The 9 least significant bits are used as a counter from 0-512
 - These bits correspond to the permissions: ReadData, CreateFile, AppendData, ReadExtendedAttribute, WriteExtendedAttribute, ExecuteFile, Traverse, DeleteSubdirectoriesAndFiles, ReadAttributes

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:
 - NumFilesInList * 512 * 60bytes
 - 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

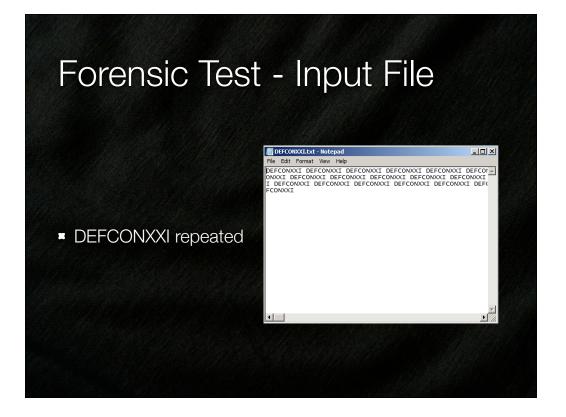
- NTFS does *NOT* remove old/unused SIDs from the \$SECURE file
- The \$SECURE file is designed only to grow in size and never shrink
- This means, every ACLEncoded chunk from every run of ACLEncode will persist here forever

A Forensic Review

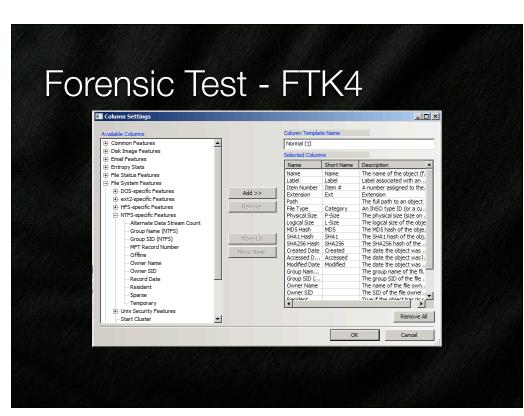
- I conducted a test:
 - 2GB USB Key, formatted as NTFS
 - AccessData FTK 4.0.2.33
 - Guidance EnCase Forensic 6.19.6

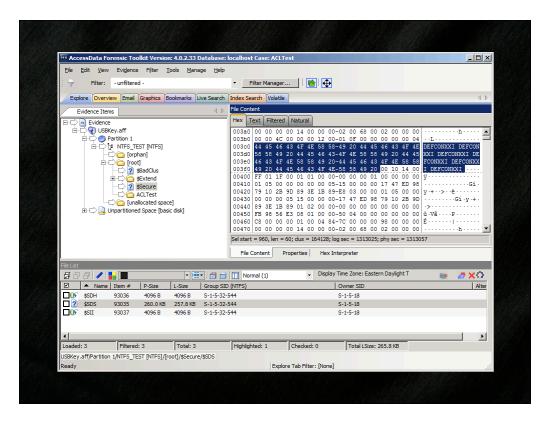
For	rens	ic Te	<u>- tec</u>	Ē	le List
			501		
ACLTest				_ 🗆 ×	
	EST (E:) 🔹 ACLTest	👻 🌆 Search	ACLTest	<u> </u>	
Irganize 👻 🗾 Open 🕙	▼ Print Burn Ne	ew folder		- 🗌 🔞	File Edit Format View Help E:\ACLTest\file01.txt
☆ Favorites	Name ^	Date modified	Type Size		E:\ACLTest\file02.txt E:\ACLTest\file03.txt
Desktop	file01.txt	7/5/2013 3:06 PM	Text Document	0 KB	E:\ACLTest\file04.txt E:\ACLTest\file05.txt
Downloads	file02.txt	7/5/2013 3:06 PM	Text Document	0 KB	E:\ACLTest\file06.txt
🔛 Recent Places	file03.txt	7/5/2013 3:06 PM	Text Document	0 KB	E:\ACLTest\file07.txt E:\ACLTest\file08.txt
	file04.txt	7/5/2013 3:06 PM	Text Document	0 KB	E:\ACLTest\file09.txt E:\ACLTest\file10.txt
Libraries Documents	file05.txt	7/5/2013 3:06 PM	Text Document	0 KB	E:\ACLTest\file11.txt E:\ACLTest\file12.txt
Music	file06.txt	7/5/2013 3:06 PM	Text Document	0 KB	E:\ACLTest\file13.txt E:\ACLTest\file14.txt
E Pictures	ile07.txt	7/5/2013 3:06 PM	Text Document	0 KB	E:\ACLTest\file15.txt
🛃 Videos	ile08.txt	7/5/2013 3:06 PM	Text Document	0 KB	E:\ACLTest\file16.txt
💷 Computer	ile09.txt	7/5/2013 3:06 PM	Text Document	0 KB	
Local Disk (C:)	file 10.txt	7/5/2013 3:06 PM	Text Document	0 KB	
NTFS_TEST (E:)	file 11. txt	7/5/2013 3:06 PM	Text Document	0 KB	
•	file 12. txt	7/5/2013 3:06 PM	Text Document	0 KB	4
📬 Network	file 13.txt	7/5/2013 3:06 PM	Text Document	0 KB	
	file 14. txt	7/5/2013 3:06 PM	Text Document	0 KB	
	file 15. txt	7/5/2013 3:06 PM	Text Document	0 KB	
	file 16. txt	7/5/2013 3:06 PM	Text Document	0 KB	
file01.txt	Date modified: 7/5/20	13 3:06 PM Date	created: 7/5/2013 3:39	РМ	

I created these files for the test I could have used any file already on the system



	essData Fo	orensic To	oolkit Versi	ion: 4.0.2.3	3 Database: local	host Case: ACLT	est		<u>_ ×</u>
Eile	<u>E</u> dit <u>V</u> iew	Evi <u>d</u> eno	ce Filter	<u>T</u> ools <u>M</u> a	anage <u>H</u> elp				
-	Filter:	- unfilter	red -		•	Filter Manager.	📄 🕂		
						a 1 1 1 1 1			4 Þ
Expl	ore Overvi	iew Email	I Graphics	Bookmarks	Live Search Inde	ex Search Volatile			N P
E	vidence Iten	ns		4 ⊳	Properties				
	Evidence				2 ↓				
🖻 🛱 😲 USBKey.aff					🗆 NTFS Info	^			
					MFT Recor	d Number	36		
⊡-C≻[‡ NTFS_TEST [NTFS] C≻[☐ [orphan] ⊡-C≻[☐ [root]					Record dat	te	7/5/2013 3:41:20) PM (2013-07-05 19:41:20 UTC)	
					Resident		True		
	1		\$BadClus		Offline		False		
		⊕ -⊂> <mark>`</mark>	\$Extend		Sparse		False		
			\$Secure		Temporary	,	False		
			ACLTest	1	Owner SID		S-1-5-21-256568	7063-2636845177-2300264073-1000	
			nallocated sp ned Space [b		Group SID		S-1-5-21-256568	7063-2636845177-2300264073-513	
	шц/ <u>тө</u> ч	Shiparadon	ica opace [o	conc chord					•
					File Content	Info			<u>.</u>
					File Content		Hex Interpreter		<u>·</u>
ile List							Hex Interpreter		<u>.</u>
	日 /		_	.	File Content	Properties		y Time Zone: Eastern Daylight Time (From I	<u>.</u> 84 / XO
7 -		Item #	P-Size	1 1	File Content	Properties Normal (1)			● <u>^</u> ×○
2 2	 Name 	Item #	P-Size	L-Size	File Content	Properties Normal (1) S)	 Display 	Owner SID	💓 🏄 🗙 🔇 Alterna 🔺
2 2			P-Size 0 B 0 B	1 1	File Content	Properties Normal (1) =S) 587063-263684517			🧼 🏄 X 🗘 Alterna 🔺 0
	▲ Name file01.txt	Item # 93042	0 B	L-Size 0 B	File Content	Properties Normal (1) =S) =S87063-263684517 587063-263684517	▼ Display 77-2300264073-513	Owner SID S-1-5-21-2565687063-2636845177-2300264073-100	Alterna •
	▲ Name file01.txt file02.txt	Item # 93042 93043	0 B 0 B	L-Size 0 B 0 B	File Content	Properties Normal (1) 	 Display 77-2300264073-513 77-2300264073-513 	Owner SID 5-15-21-2565687063-2636845177-2300264073-100 5-1-5-21-2565687063-2636845177-2300264073-100 5-1-5-21-2565687063-2636845177-2300264073-100	Alterna A
	Name file01.txt file02.txt file03.txt file04.txt file05.txt	Item # 93042 93043 93044 93045 93045	0 B 0 B 0 B 0 B 0 B	L-Size OB OB OB OB OB	File Content	Properties Normal (1) =S) =S7063-263684517 =S87063-263684517 =S87063-263684517 =S87063-263684517	 Display 7-2300264073-513 7-2300264073-513 7-2300264073-513 	Owner SID 5-15-21-2565687063-2636845177-2300264073-100 5-1-5-21-2565687063-2636845177-2300264073-100 5-1-5-21-2565687063-2636845177-2300264073-100	Alterna
	Name file01.txt file02.txt file03.txt file04.txt file05.txt file06.txt	Item # 93042 93043 93044 93045 93046 93047	0 B 0 B 0 B 0 B 0 B 0 B	L-Size OB OB OB OB OB OB	File Content	Properties Normal (1) 55) 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517	 Display 77-2300264073-513 77-2300264073-513 77-2300264073-513 77-2300264073-513 77-2300264073-513 77-2300264073-513 	Owner SID 5-1-5-21-2565687053-2258645177-2300264073-100 5-1-5-21-2555687053-2258645177-2300264073-100 5-1-5-21-2555687053-2258645177-2300264073-100 5-1-5-21-2555687053-2258645177-2300264073-100 5-1-5-21-2555687053-2258645177-2300264073-100 5-1-5-21-2555687053-2258645177-2300264073-100 5-1-5-21-2555687053-2258645177-2300264073-100 5-1-5-21-2555687053-2258645177-2300264073-100 5-1-5-21-2555687053-2258645177-2300264073-100	Alterna A
	Name file01.txt file02.txt file03.txt file04.txt file05.txt file06.txt file07.txt	Item # 93042 93043 93044 93045 93045 93046 93047 93048	0 B 0 B 0 B 0 B 0 B 0 B 0 B	L-Size 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	File Content	Properties Normal (1) 55) 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517	 Display 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 	Owner SID \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100	Alterna
	Name file01.txt file02.txt file03.txt file04.txt file05.txt file05.txt file07.txt file08.txt	Item # 93042 93043 93044 93045 93046 93047 93048 93049	0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	L-Size 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	File Content	Properties Normal (1) :5) :50 :50 :50 :50 :50 :50 :50 :50	 Display 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 7-2300264073-513 	Owner SID \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100	Alterna A 0 0 0 0 0 0 0 0 0 0 0 0 0
	Name file01.txt file02.txt file03.txt file04.txt file05.txt file05.txt file07.txt file08.txt file09.txt	Item # 93042 93043 93044 93045 93045 93046 93047 93048 93049 93050	0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	L-Size 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	Fle Content Group SID (NTF S-1-5-21-25658 S-1-5-21-25658 S-1-5-21-25658 S-1-5-21-25658 S-1-5-21-25658 S-1-5-21-25658 S-1-5-21-25658 S-1-5-21-25658 S-1-5-21-25658	Properties Normal (1) *5) 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517	 Display 7-2300264073-513 	Owner SID \$-1-5-21-2565687053-2636845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100 \$-1-5-21-2565687053-2536845177-2300264073-100	Alterna
	► Name file01.txt file02.txt file03.txt file04.txt file05.txt file05.txt file05.txt file08.txt file09.txt file09.txt	Item # 93042 93043 93044 93045 93046 93046 93047 93048 93049 93050 93051	0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	L-Size 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	File Content Group SID (MT S-1-5-21-25656 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657	Properties Normal (1) '5) 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517 587063-263684517	 Display 7-2300264073-513 	Owner SID \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100	Aterna Aterna A
	► Name file01.txt file02.txt file03.txt file04.txt file05.txt file05.txt file05.txt file05.txt file09.txt file09.txt file10.txt	Item # 93042 93043 93044 93045 93046 93047 93048 93049 93050 93051 93052	0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	L-Size 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	File Content Group SID (MT S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657 S-1-5-21-25657	Properties Normal (1) *5) \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517	Pisplay T-2300264073-513 7-230 7-230 7-230 7-230267 7-230 7-2	Owner SID 61-5-21-265687063-263645177-2300264073-100 51-5-21-265687063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-256587063-2636845177-2300264073-100 51-5-21-2565687063-2636845177-2300264073-100 51-5-21-2565687063-2636845177-2300264073-100 51-5-21-2565687063-2636845177-2300264073-100 51-5-21-2565687063-2636845177-2300264073-100	Alterna
	► Name file01.txt file02.txt file03.txt file04.txt file05.txt file05.txt file05.txt file08.txt file09.txt file09.txt	Item # 93042 93043 93044 93045 93046 93046 93047 93048 93049 93050 93051	0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	L-Size 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	File Content If an an analysis Group SID (WIT S-1-5-21-2565	Properties Normal (1) *5) \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517	 Display 7/2300264073-513 	Owner SID \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100	Atterna A 0 0 0 0 0 0 0 0 0 0 0 0 0
	▲ Name file01.txt file02.txt file03.txt file04.txt file05.txt file05.txt file05.txt file09.txt file09.txt file10.txt file10.txt file12.txt file13.txt	Item # 93042 93043 93044 93045 93046 93046 93047 93048 93049 93050 93051 93052 93053	0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	L-Size 0 B 0 B 0 B 0 B 0 B 0 B 0 B 0 B	File Content If m m Group SID (MT S-1-5-21-2565 S-1-5-21-2565	Properties Normal (1) *5) \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517 \$87063-263684517	 Display 7/2300264073-513 	Owner SID \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-2565687063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100 \$-1-5-21-256587063-2636845177-2300264073-100	Atema A Atema A 0 0 0 0 0 0 0 0 0 0 0 0 0





Forensic Test - EnCase 6

New 🧭 Open 🚽 Save 🚽 Print 🌤 Add Device 🔍 Search 📓 Refresh 🕽 Cases X 🔛 Table 🔄 Report 🖂 Gallery 📀 Timeline 💭 Disk 🔧 Code											
Home Fritries Dookmarks Q Se		Name	Filter	In Report	File Ext	File Type	File Category	Signature	Descrip	ot 🔦	
🔁 Home 👓 File Extents 🔒 Permissions	• 🗹 1	🗋 file01.txt		No	bat	Text	Document		File, Archive		
	2	🗋 file02.txt		No	bat	Text	Document		File, Archive		
	3	🗋 file03.txt		No	txt	Text	Document		File, Archive		
 ₽₽₩∞c	4	🗋 file04.txt		No	txt	Text	Document		File, Archive		
⊕-D⊡ ∰Extend	5	🗋 file05.txt		No	txt	Text	Document		File, Archive		
-D.	6	🗋 file06.txt		No	txt	Text	Document		File, Archive	-	
	7	🗋 file07.txt		No	bxt	Text	Document		File, Archive		
	28	🗋 file08.txt		No	txt	Text	Document		File, Archive		
	9	🗋 file09.txt		No	txt	Text	Document		File, Archive		
	10	🗋 file10.txt		No	txt	Text	Document		File, Archive		
	<	Pt Blatt NA		Ma	Full	Taut	Deciment		Eila Archiva		
🔹 💽 Text, 🖏 Hex, 🎧 Doc 🧐 Transcript 🔝 Picture 📑 Report 🖸 Console 🗟 👀 🥂 🔀 EnScript, 🔍 Hits 🍸 Filters (ﷺ Conditions 🏠 Display 🙂 Qu4											
					🐴 En					1	
					T - I	CF2 EnScripts					
Empty Fi		Enterprise Examples									
				1 <u>-</u> 0 LE 1)	• • •				1		

Forensic Test - EnCase 6

Cases	Print Add Device Q Searcl	Report 🐴 Code		
Home Entries	Bookmarks Q Se	Name sone 5-1-4-112 5-1-1-0 5-1-5-21- 5-1-5-21-	1d 28678724-1482182223-1162092617-1313817414 -2565687063-2636845177-2300264073-1000 -2565687063-2636845177-2300264073-513	541677656-1128
I Text & Hex Coc	Transcript 🖾 Picture 🗐 Repor	Console 201	②EnScript 了 Filters (ఓ= Conditions ఎ), Display	Z S Oueries A∢I

Forensic Test - EnCase 6

		Search 🔝 Refresh		_	-					
Cases 🗙 🔛 🔚 Table 🔄 Report 🕮 Gallery 🥑 Timeline 💭 Disk 松 Code										
🕒 Home 🍃 Entries 💭 Bookmarks 🔍 Se 🕕		Name	Filter	In Report	File Ext	File Type	File Category	Signature	C	
🗄 Home 🗠 File Extents 🔒 Permissions 🕕	13	🗐 \$Secure		No					File, Inte	
HD👿 📴 Entries	14	🗐 \$Secure \$SII		No					File, Inte	
	2 15	🗐 \$Secure \$SDH		No					File, Inte	
É₽₩∞⊆	2 16	Secure \$\$05		No					File, Inte	
E-D C Extend	17	🗐 \$UpCase	\sim	No					File, Inte	
LON ACLTest	18	I MFT Allocation		No	-				File, Bitm	
	2 19	📰 Volume Slack		No					File, Unal	
	<								>	
🔄 Text 😺 Hex 🎧 Doc 😪 Transcript 🖾 Pio	ture 🗐	Report 🖸 Console	9 1)	EnS	ript 🔍	Hits 🍸 Filter	rs ()= Condition	ıs 🆄 Displa	v 😨 Ourt	
00795·L·····		•••••••	• •		Scrint	-				
00848 ·GiOy·+OO>·Qè······					CF2 Eng	icripts				
00901DÈD D 00954DEFCONXXI DEFCONXXI DEF				C = Enterprise C = Enterprise C = C = C = C = C = C = C = C = C =						
01007XI DEFCONXXI ····ÿ······		·····GiBy·+	0							
01060 <mark>0≻•Dè•••••••••••••••••••••••••••••••••••</mark>										
01113 · · · · È · · · · □ · · · □ · · · · · · · · · ·		🗑 🧰 Include								
01219 RFCONXXI ·····				Main Source Processor						
01272è·····GiDy·+OD≻·O··										
01325 ···È·····D ···D························										
	SECORAL STATE	T DEPCORVET DEPC		0 LE 60)						

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 Q&A room for Track 1
- Thanks to Josh, Nick, Joel, Reesh, my family, my friends, my colleagues, and my employer for providing me the time for this research
- Thanks Eugene for seeding the thought in my mind of "How can you hide data on a drive without detection?"

ACLEncode

- Source code Available for download:
- http://www.perklin.ca/~defcon21/ACLEncode.zip



Latest version of Slides

- The latest version of these slides are available online:
- http://www.perklin.ca/~defcon21/aclsteganography.pdf



This latest version will be available on the DEFCON site soon

References

- http://msdn.microsoft.com/en-us/library/gg465313.aspx
- http://stackoverflow.com/questions/1140528/what-is-the-maximum-length-of-a-sid-in-sddlformat
- http://technet.microsoft.com/en-us/library/cc962011.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