June 6, 2003

Steganography & Steganalysis

SpyHunter
www.spy-hunter.com
spyhunter@spy-hunter.com

Agenda

- Steganography
  - What is Steganography?
  - History
  - Steganography today
  - Steganography tools
- Steganalysis
  - What is Steganalysis?
  - Identification of Steganographic files
  - Cracking Steganographic files
  - What's in the future?

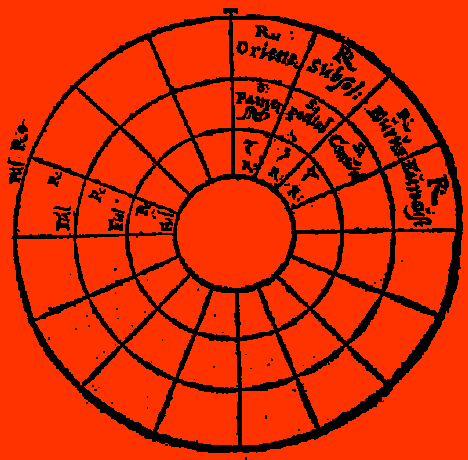
Steganography

Steganography - Definition

- Steganography
  - from the Greek word steganos meaning "covered"
  - and the Greek word graphie meaning "writing"
- Steganography is the process of hiding of a secret message within an ordinary message and extracting it at its destination
- Anyone else viewing the message will fail to know it contains hidden/encrypted data

Steganography - History

- Greek history – warning of invasion by scrawling it on the wood underneath a wax tablet. To casual observers, the tablet appeared blank.
- Pirate legends tell of the practice of tattooing secret information, such as a map, on the head of someone, so that the hair would conceal it.



Steganography

- Both Axis and Allied spies during World War II used such measures as invisible inks -- using milk, fruit juice or urine which darken when heated.
- Invisible Ink is also a form of steganography

Steganography

- The U.S. government is concerned about the use of Steganography.
- Common uses in include the disguising of corporate espionage.
- It's possible that terrorist cells may use it to secretly communicate information
- It's also a very good Anti-forensics mechanism to mitigate the effectiveness of a forensics investigation

Steganography

Terror groups hide behind Web encryption

By Jack Kelley, USA TODAY AP

WASHINGTON — Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies. It sounds farfetched, but U.S. officials and experts say it's the latest method of communication being used by Osama bin Laden and his associates to outfox law enforcement. Bin Laden, indicted in the bombing in 1998 of two U.S. embassies in East Africa, and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites, U.S. and foreign officials say.

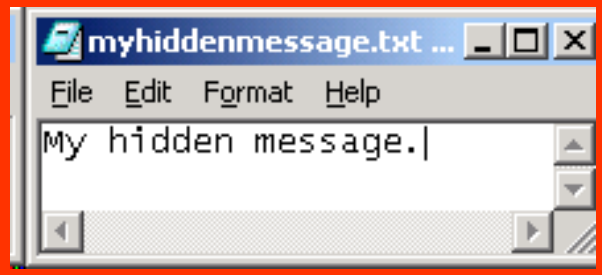
Steganography

- Steganography has also been popularized in movies
  - The Saint, Val Kilmer
  - Along Came a Spider, Morgan Freeman

Steganography

- **Modern digital steganography**
  - **data is encrypted**
  - **then inserted, using a special algorithm which may add and/or modify the contents of the file**
  - **Carefully crafted programs apply the encrypted data such that patterns appear normal.**

Steganography – Modern Day



Carrier File

Carrier File with Hidden Message

Steganography – Carrier Files

Steganography Carrier Files

- **bmp**
- **jpeg**
- **gif**
- **wav**
- **mp3**
- **Amongst others…**

Steganography - Tools

Steganography Tools

- **Steganos**
- **S-Tools (GIF, JPEG)**
- **StegHide (WAV, BMP)**
- **Invisible Secrets (JPEG)**
- **JPHide**
- **Camouflage**
- **Hiderman**
- **Many others…**

Steganography

- **Popular sites for Steganography information**
  - http://www.ise.gmu.edu/~njohnson/Steganography
  - http://www.rhetoric.umn.edu/Rhetoric/misc/dfrank/stegsoft.html
  - http://www.topology.org/crypto.html

Steganalysis

Identification of hidden files

Steganalysis - Definition

- **Definition**
  - Identifying the existence of a message
  - **Not** extracting the message
  - Note: Technically, Steganography deals with the concealment of a message, not the encryption of it

- **How is this meaningful???**

Steganalysis

- By identifying the existence of a hidden message, perhaps we can identify the tools used to hide it.
- If we identify the tool, perhaps we can use that tool to extract the original message.

Steganalysis – Methods of Detection

- **Methods of detecting the use of Steganography**
  - View it (JPEG, BMP, GIF, etc.)
  - Listen to it (WAV, MPEG, etc.)
  - Statistical Attack (changes in patterns of the pixels or LSB – Least Significant Bit) or Histogram Analysis
  - View file properties/contents
    - size difference
    - date/time difference
    - contents – modifications
    - checksum

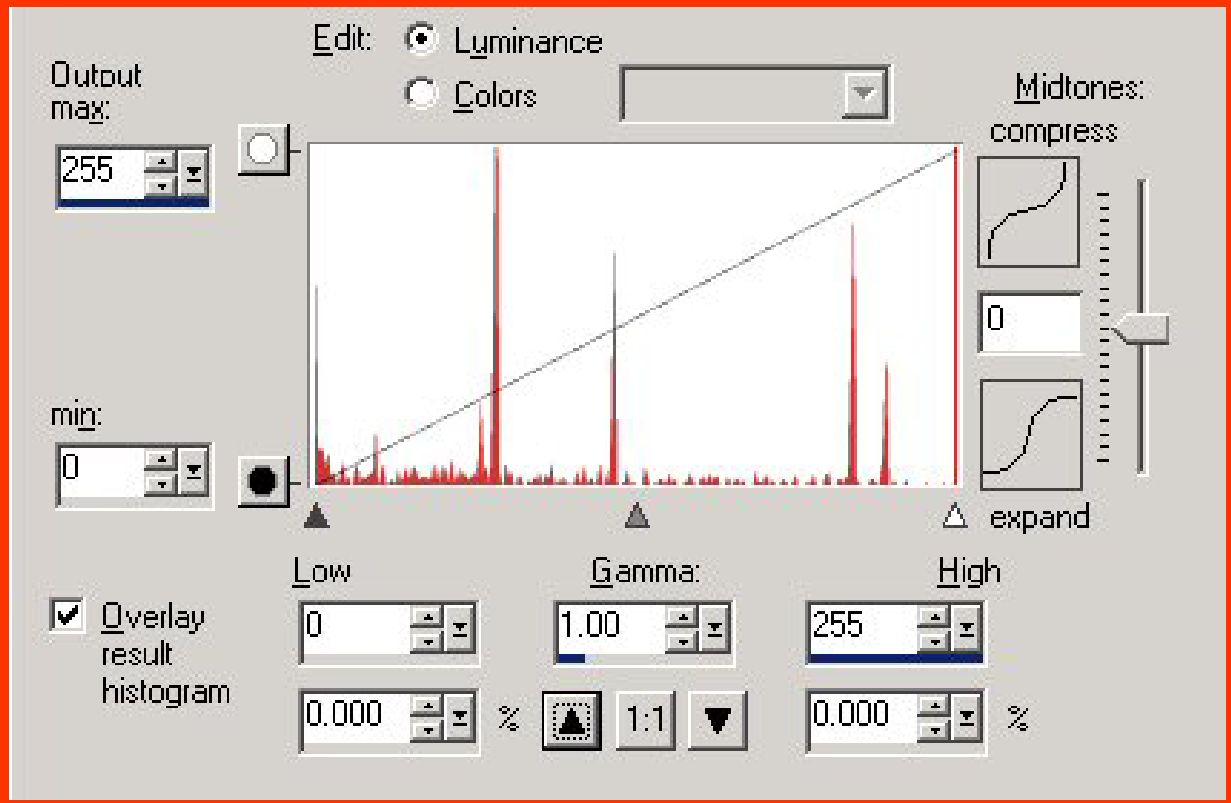
Steganalysis – Methods of Analysis

- **Detecting Steganography by viewing it**

- **Can you see a difference in these two pictures? (I can't!)**

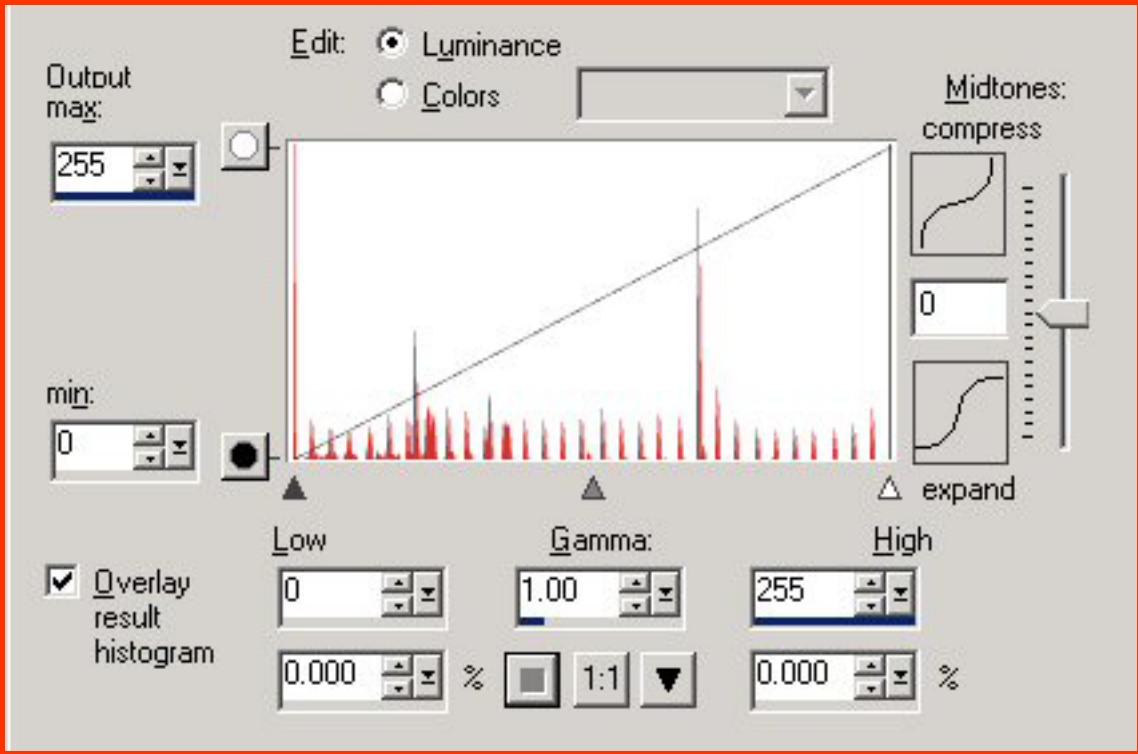
Steganalysis – Histogram Analysis

- **Histogram analysis can be used to possibly identify a file with a hidden message**



Steganalysis – Histogram Analysis

- **By comparing histograms, we can see this histogram has a very noticeable repetitive trend.**



Steganalysis – Compare properties

- Compare the properties of the files
- Properties
  - 04/04/2003 05:25p 240,759 helmetprototype.jpg
  - 04/04/2003 05:26p 235,750 helmetprototype.jpg
- Checksum
  - C:\GNUTools>cksum a:\helmetprototype.jpg
    3749290633 235750 a:\helmetprototype.jpg
  - C:\GNUTools>cksum a:\before\helmetprototype.jpg
    3241690497 240759 a:\before\helmetprototype.jpg

Steganalysis – Analyzing contents of file

- Viewing the contents of the file
  - If you have the copy of the original picture, it can be compared to the modified suspect file
  - Identify inconsistencies
  - Identify a signature pattern associated with a specific steganographic tool

Steganalysis – Analyzing contents of file

- Identifying the presence of a hidden message
- Many tools can be used for viewing and comparing the contents of a hidden file.
- Everything from Notepad to a Hex Editor can be used
- Reviewing mutiple files generated from the same program may reveal a signature!

Steganalysis – Analyzing contents of file

- **WinHex Analysis**

securitydaemonlogo.jpg

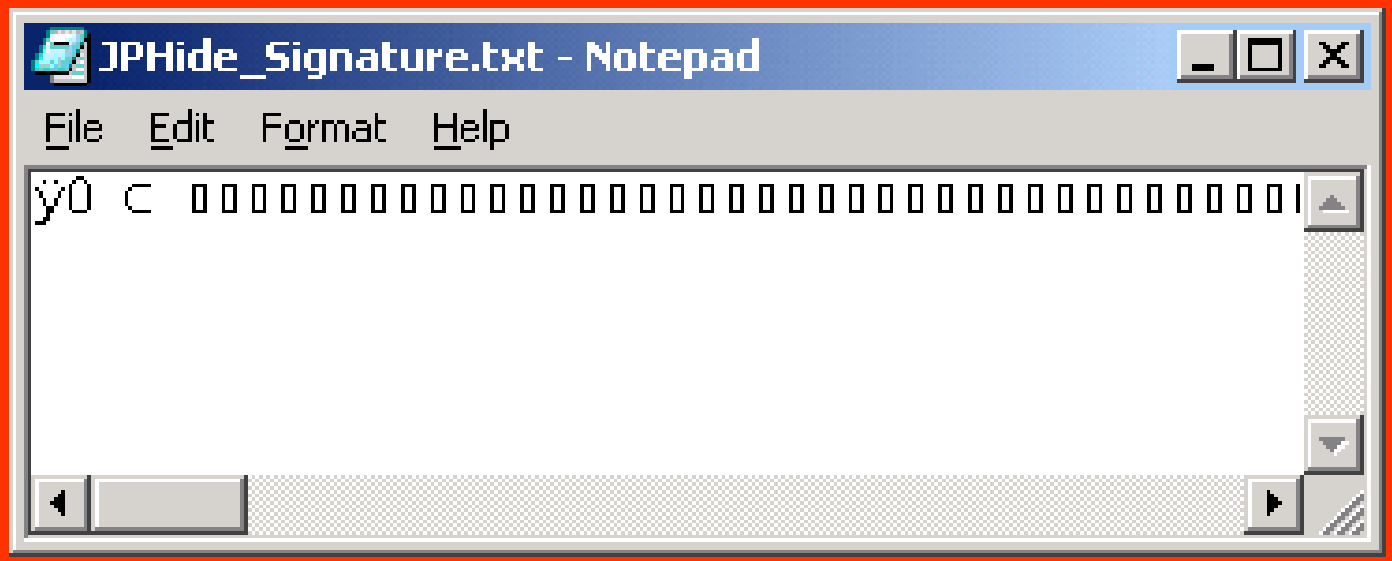
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	00	48	ÿØÿà..JFIF.....H
00000010	00	48	00	00	FF	ED	0C	E4	50	68	6F	74	6F	73	68	6F	.H..ÿí.äPhotosho
00000020	70	20	33	2E	30	00	38	42	49	4D	03	E9	00	00	00	00	p 3.0.8BIM.é....

securitydaemonlogo.jpg

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	00	48	ÿØÿà..JFIF.....H
00000010	00	48	00	00	FF	FE	00	4B	3B	88	CC	66	E5	68	09	6C	.H..ÿþ.K;ˆÌfåh.l
00000020	45	B4	BD	4E	0A	3D	62	66	F3	FB	4B	61	1F	CF	47	FE	E´½N.=bfóûKa.ÏGþ
00000030	03	62	4E	75	F6	82	EC	27	AE	D6	47	04	F7	39	E4	F9	.bNuö‚ì'®ÖG.÷9äù
00000040	63	2C	CC	09	FB	4E	42	FA	A0	11	C8	9C	B0	87	9F	E5	c,Ì.ûNBú .È‰°‡Ÿå
00000050	54	8C	28	B8	97	86	8A	10	42	E2	B9	A9	5C	08	00	00	TŒ(¸—†Š.Bâ¹©\...
00000060	00	FF	FE	00	0A	04	00	00	00	D2	BB	6D	93	FF	FF	ED	.ÿþ.....Ò»m“ÿÿí

Steganalysis – Identifying a signature

- **Identifying the signature**
  - WinHex is very helpful for identifying the differences between two files to determine what was modified and/or added.
  - Notepad can then utilized to reveal the signature string added to the file

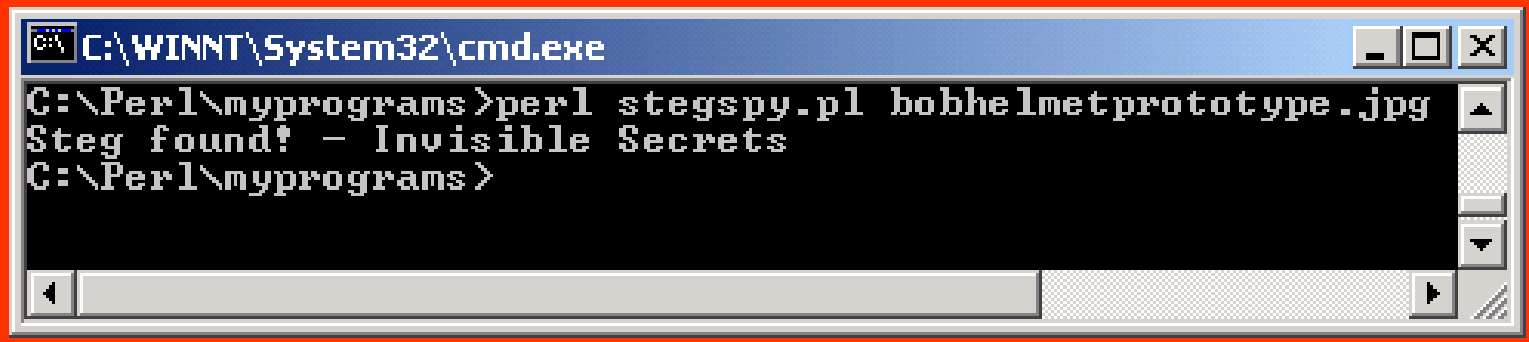


Steganalysis – Identifying a signature

- **Signature found!**
- **Signature-based steganalysis was used to identify signatures in many programs including Invisible Secrets, JPHide, Hiderman, etc.**

Steganalysis - Stegspy

- **Signature found!**
  - Stegspy.pl searches for stego signatures and determines the program used to hide the message
  - Will be available for download from my site
  - Example:



Steganalysis – Identifying a signature

- How is this handy?
- No original file to compare it to
- Search for the signature pattern to determine a presence of a hidden message
- Signature reveals program used to hide the message!

Steganalysis meets Cryptanalysis

Cryptanalysis

- **As stated previously, in Steganography the goal is to hide the message, NOT encrypt it**
- **Cryptography provides the means to encrypt the message.**
- **How do we reveal the hidden message?**

Steganalysis meets Cryptanalysis

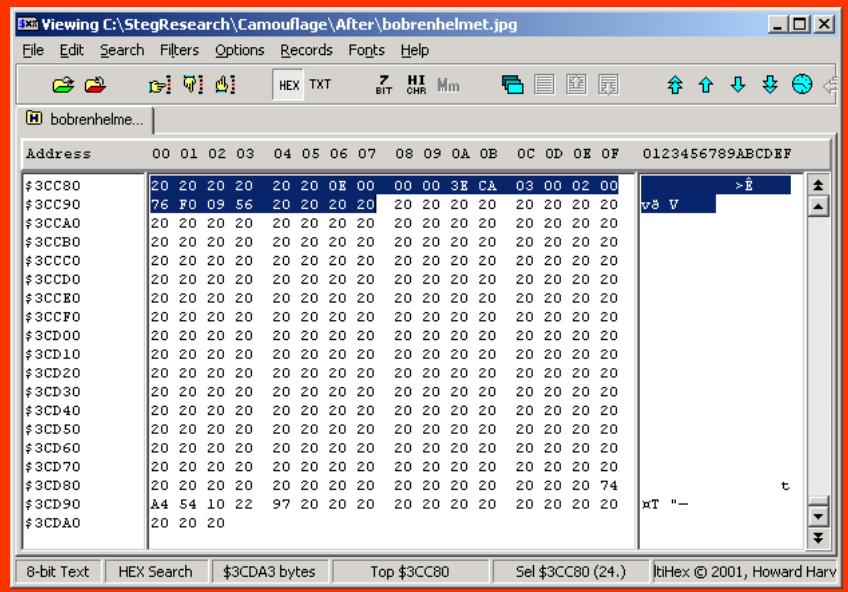
- Knowing the steganography program used to hide the message can be extremely handy when attempting to reveal the actual hidden message
- Unfortunately, some of these programs use strong encryption 128-bit or stronger – GOOD LUCK!
- The only thing we need is the PASSWORD!

Steganalysis meets Cryptanalysis

- **A few Brute Force password grinding programs have been created.**
- **Stegbreak by Niels Provos, www.outguess.org**
  - J-Steg

Camouflage – Case Study

- **Determining the password used with Camouflage**
- **The location of the password was determined by using MultiHex which allows searches for Hex strings**

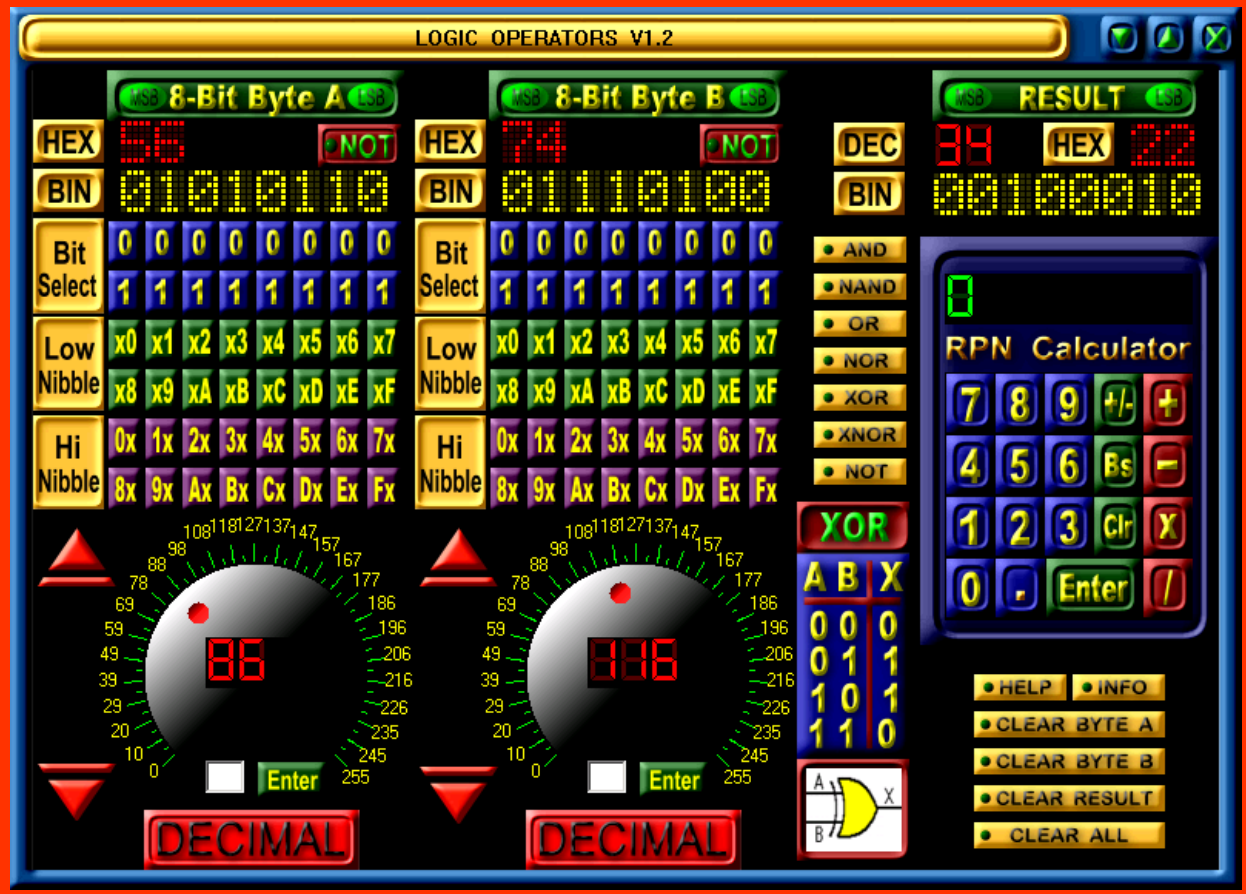


Camouflage

- The string was found to be “76 F0 09 56”
- The password is know to be “test” which is “74 65 73 74” in Hex

BDHTool

- Using BDHTool we can XOR the two to reveal the key



Camouflage

76 XOR 74 = 02

F0 XOR 65= 95

09 XOR 73 = 7A

56 XOR 74 = 22

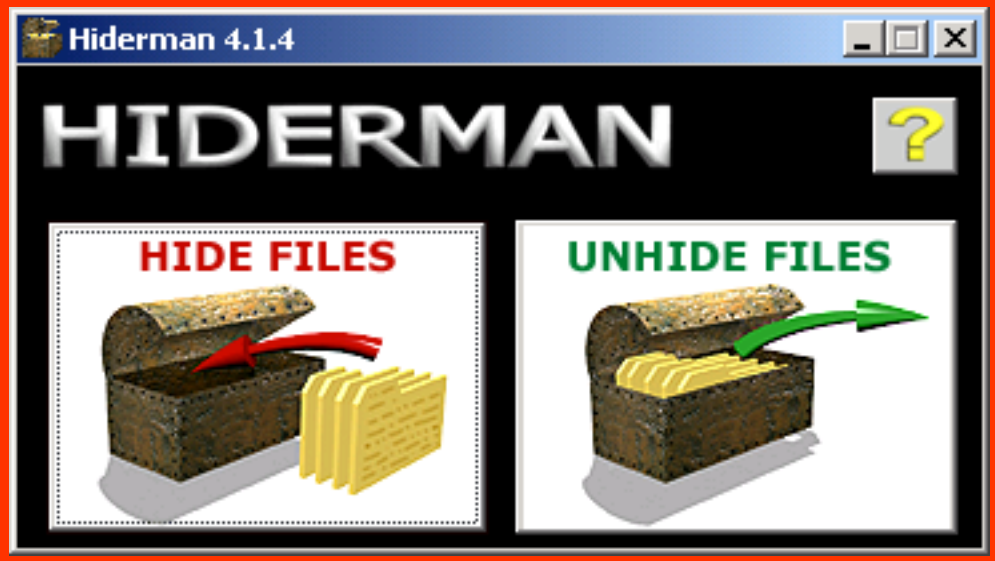
- **The 1st 4 digits of the key are "02 95 7A 22"**
- **So let's test our theory…**

Camouflage

- We store another message using a different password
- The file reveals a Hex code of "63 F4 1B 43"
- We XOR this with the known key "02 95 7A 22"
- The result is "61 61 61 61" which is a password of "aaaa" in ASCII
- We've revealed the hidden password to hide the message!
- This exploit discovered by Guillermito at www.guillermito2.net

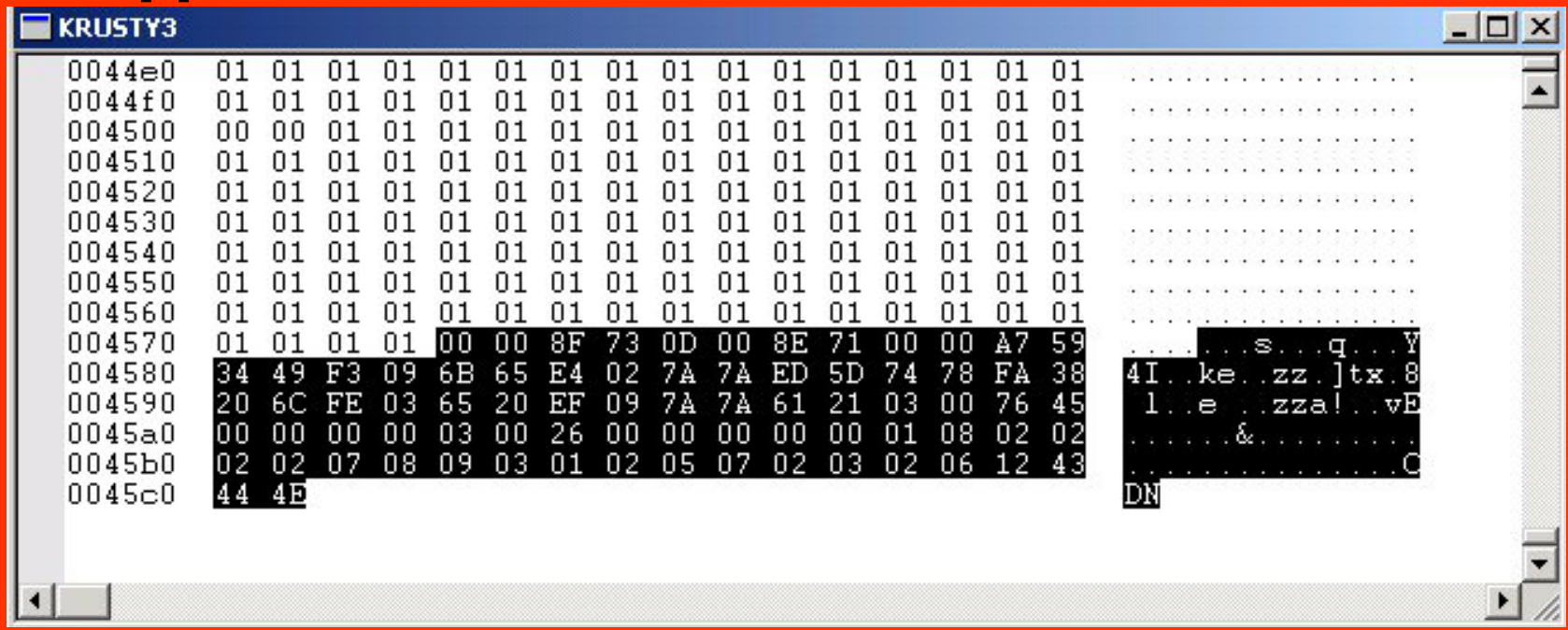
Hiderman – Case Study

- Let's examine a slightly more sophisticated stego program – Hiderman



Hiderman

- **After hiding a message with Hiderman, we can review the file with our favorite Hex Tool. This reveals that the message is encrypted and appended to the end of the file.**



Hiderman

- Extracting the hidden message we have

49 F3 09 6B 65 E4 02 7A 7A ED 5D 74 78 FA 38

20 6C FE 03 65 20 EF 09 7A 7A 61 21

In ASCII we have: I??ke??zz??tx??l??e ??zza!

Ever do a cryptogram???

Hiderman

- **Deciphering the code:**

The first part is the file name:

I??ke??zz??tx? = I??ke??zz?.txt

The second part is the message:

?l??e ??zza!

Hiderman

- Many keys are based on the password
- Assuming the file name is Ilikepizza.txt and the message is "I like pizza!", we can reverse engineer this
- We convert everything to it's actual ASCII equivalent:

49 6C 69 6B 65 70 69 7A 7A 61 2E 74 78 74 49

20 6C 69 6B 65 20 70 69 7A 7A 61 21

I l i k e p i z z a . t x t I

l i k e p i z z a !

Hiderman

- Original

49 F3 09 6B 65 E4 02 7A 7A ED 5D 74 78 FA 38

20 6C FE 03 65 20 EF 09 7A 7A 61 21

- Deciphered

49 6C 69 6B 65 70 69 7A 7A 61 2E 74 78 74 49

20 6C 69 6B 65 20 70 69 7A 7A 61 21

- If we take each ciphered character and XOR it with the actual result, we can reveal the key which in this case is the password
- F3 XOR 6C = 9F
- 09 XOR 69 = 69
- And perform the same for the remaining characters

Hiderman

- The resultant is the key

  9F 60 94 6B 8C 73 8E 71 97 68

- 60 is 01100000 in binary
- Running that through the NOT logic gives us 10011111 which is 9F in HEX
- So 9F NOT = 60, 94 NOT = 6B, and so forth
- Same is for the remaining characters

Hiderman

- Tossing aside the NOT transforms, that leaves us with 60 6B 73 71 68
- Adding 1 to each we have 61 6C 74 72 69
- We convert this to ASCII => altri
- And rotate the letters => trial
- We found the password!
- More information on my personal site www.spy-hunter.com

Steganalysis – Future?

- Where do we go from here?
- My program Stegspy currently identifies JPHide, Hiderman, and Invisible Secrets. More to come!
- Write a program to crack weak Stego programs
- Need a password grinder, may vary depending on the Stego program (stegbreak already available)
- Statistical analysis has been performed and is also capable of detecting Steganographic programs (histogram, LSB, etc)

Steganalysis – Other Tools

- **Wetstone Technologies offers Stego Watch**
- **Identifies the presence of steganography through special statistical and analytical programs.**
- **Accurate and comprehensive tool, also very expensive!**
- **Does not attempt to crack or reveal the hidden message, merely identifies it**
- **Offer a Steganography Investigator Training Course**
- **See http://www.wetstonetech.com**

Steganalysis – Other Tools

- **Stegdetect by Niels Provos**
- **Available at http://www.outguess.org/detection.php**
- **Detects**
  - jsteg
  - jphide (unix and windows)
  - invisible secrets
  - outguess 01.3b
  - F5 (header analysis)
  - appendX and camouflage
- **Site down due to State of Michigan law!**

References

- Steganographica, Gaspari Schotti, 1665
- Disappearing Cryptography, Peter Wayner, 2002
- Hiding in Plain Sight, Eric Cole 2003
- Steganography – presentation Chet Hosmer, Wetstone Technologies, TechnoSecurity 2003

Question and Answer with SpyHunter

www.spy-hunter.com
spyhunter@spy-hunter.com