VeriSign®
The Value of Trust℠

Steganography, Steganalysis, & Cryptanalysis

Michael T. Raggo, CISSP
Principal Security Consultant
VeriSign

Agenda

- Steganography
  - What is Steganography?
  - History
  - Steganography today
  - Steganography tools
- Steganalysis
  - What is Steganalysis?
  - Types of analysis
  - Identification of Steganographic files
- Steganalysis meets Cryptanalysis
  - Password Guessing
  - Cracking Steganography programs
- Forensics/Anti-Forensics
- Conclusions
  - What's in the Future?
  - Other tools in the wild
  - References

VeriSign®

VeriSign®
The Value of Trust℠

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**

VeriSign®

Steganography - History

- Greek history – warning of invasion by scrawling it on the wood underneath a wax tablet. To casual observers, the tablet appeared blank.
- 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

VeriSign®

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.**
  - This is rumored to be a common technique used by Al-Qaeda. By posting the image on a website for download by another terrorist cell. Using the same Steganography program, the terrorist cell could then reveal the message with plans for a new attack.
- **It's also a very good Anti-forensics mechanism to mitigate the effectiveness of a forensics investigation**
  - Child pornography

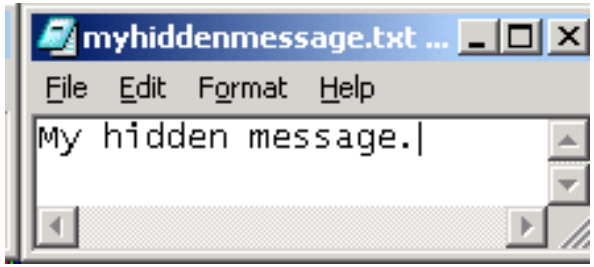
VeriSign®

Steganography

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

VeriSign®

Steganography – Modern Day



Carrier File

Carrier File with Hidden Message

VeriSign®

Steganography – Carrier Files

Steganography Carrier Files

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

VeriSign®

Steganography - Tools

Steganography Tools

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

VeriSign®

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

VeriSign®

VeriSign®
The Value of Trust℠

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
- **Steganalysis essentially deals with the *detection* of hidden content**
- **How is this meaningful???**

VeriSign®

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.

VeriSign®

Steganalysis – Hiding Techniques

- **Common hiding techniques**
  - Appended to a file
  - Hidden in the unused header portion of the file near the beginning of the file contents
  - An algorithm is used to disperse the hidden message throughout the file
    - Modification of LSB (Least Significant Bit)
    - Other

VeriSign®

Steganalysis – Methods of Detection

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

VeriSign®

Steganalysis – Methods of Detection

- **Categories**
  - Anomaly
    - Histogram analysis
    - Change in file properties
    - Statistical Attack
    - Visually
    - Audible
  - Signature
    - A pattern consistent with the program used

VeriSign®

Steganalysis – Methods of Detection

- **Goal**
  - Accuracy
  - Consistency
  - Minimize false-positives

VeriSign®

Anomaly – Visual Detection

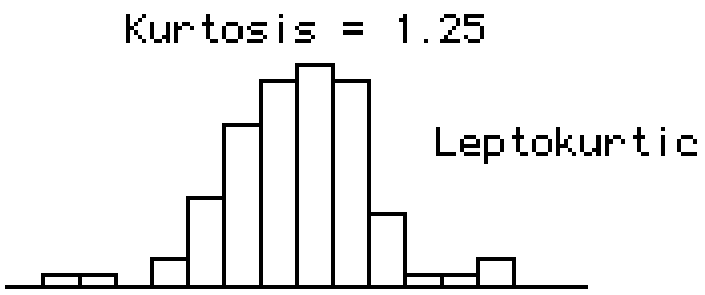
- **Detecting Steganography by viewing it**

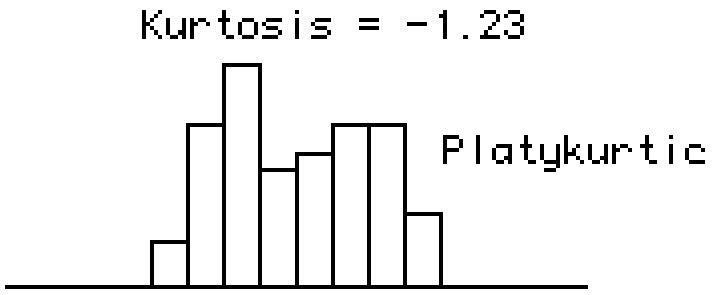
- **Can you see a difference in these two pictures? (I can't!)**

VeriSign®

Anomaly - Kurtosis

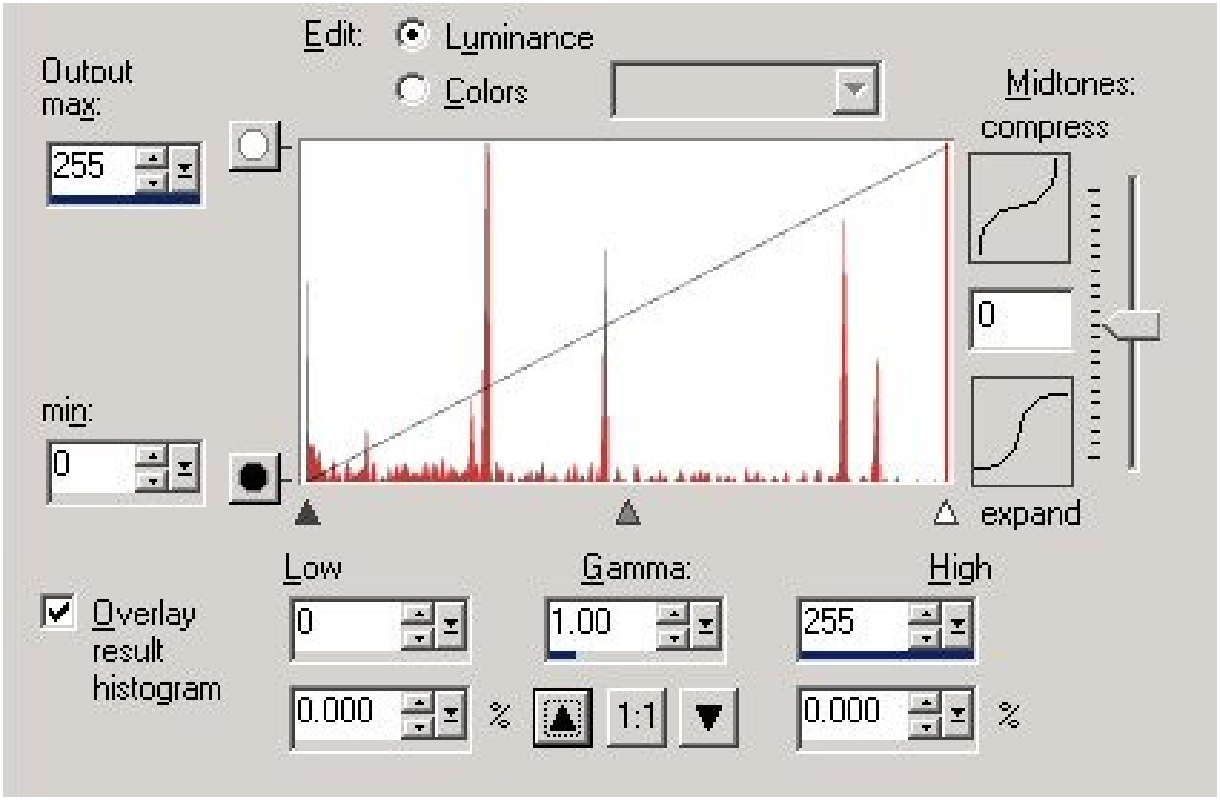
- **Kurtosis**
  - The degree of flatness or peakedness of a curve desribing a frequency of distribution
    - Random House Dictionary





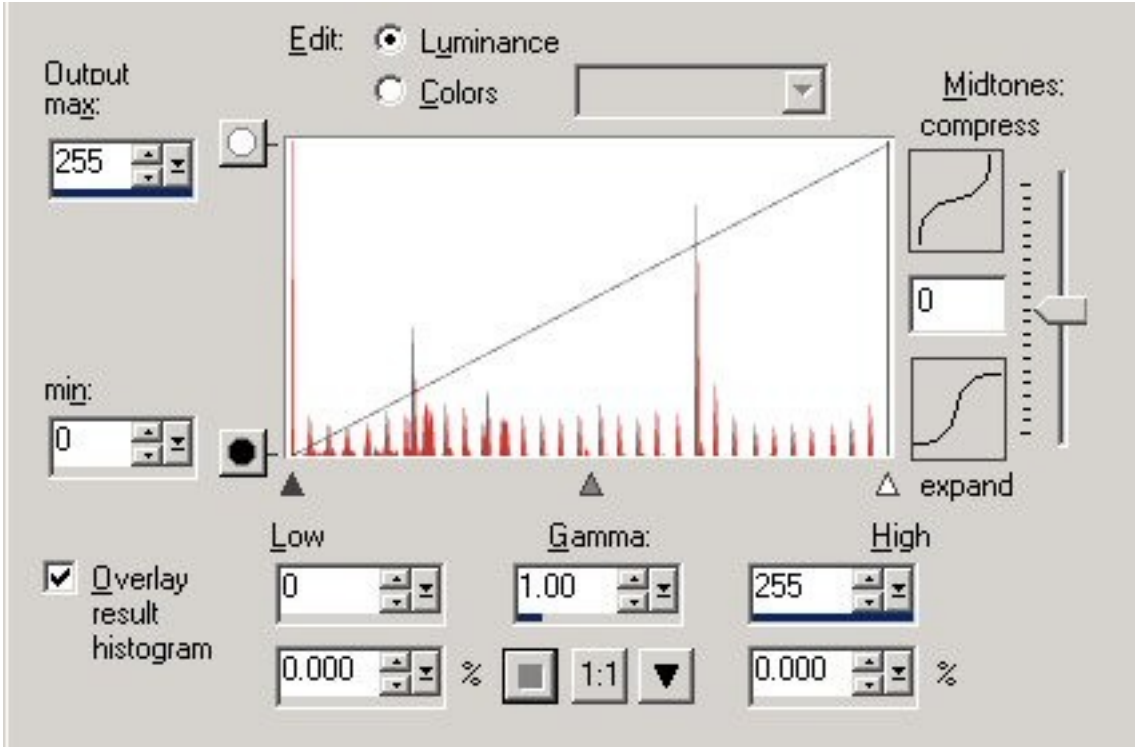
Anomaly - Histogram Analysis

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



Anomaly – Histogram Analysis

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



Anomaly Analysis - Compare file properties

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

VeriSign®

File Signatures

HEX Signature Signature	File Extension	ASCII
FF D8 FF E0 xx xx 4A 46 49 46 00	JPEG (JPEG, JFIF, JPE, JPG)	ÿØÿà..JFIF.
47 49 46 38 37 61 47 49 46 38 39 61	GIF	GIF87a GIF89a
42 4D	BMP	BM

- For a full list see:

  www.garykessler.net/library/file_sigs.html

Steganalysis – Analyzing contents of file

- If you have a copy of the original (virgin) file, it can be compared to the modified suspect/carrier file
- 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 to identify inconsistences and patterns
- Reviewing multiple files may identify a signature pattern related to the Steganography program

VeriSign®

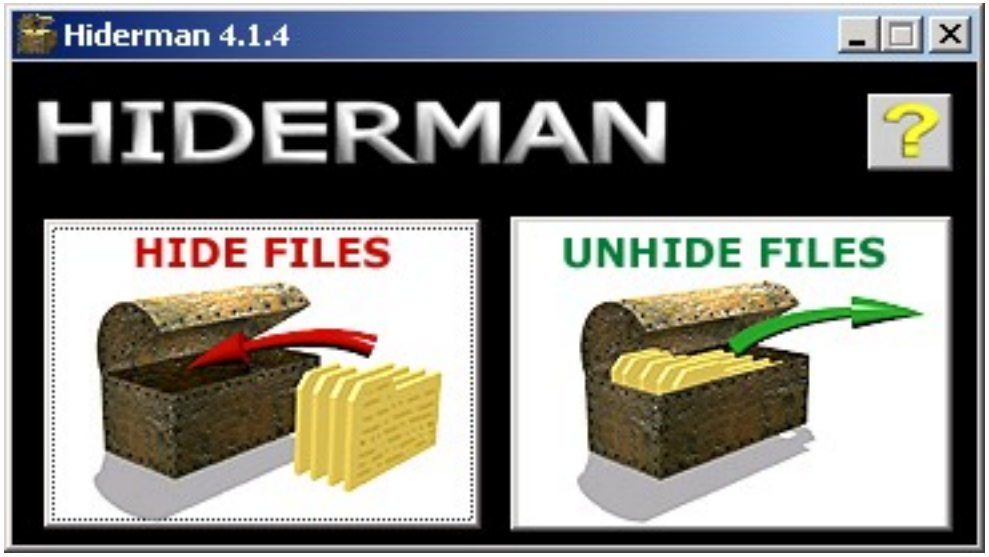
Steganalysis – Analyzing contents of file

- **Helpful analysis programs**
  - WinHex – www.winhex.com
    - Allows conversions between ASCII and Hex
    - Allows comparison of files
      - Save comparison as a report
      - Search differences or equal bytes
    - Contains file marker capabilities
    - Allows string searches – both ASCII and Hex
    - Many, many other features

VeriSign®

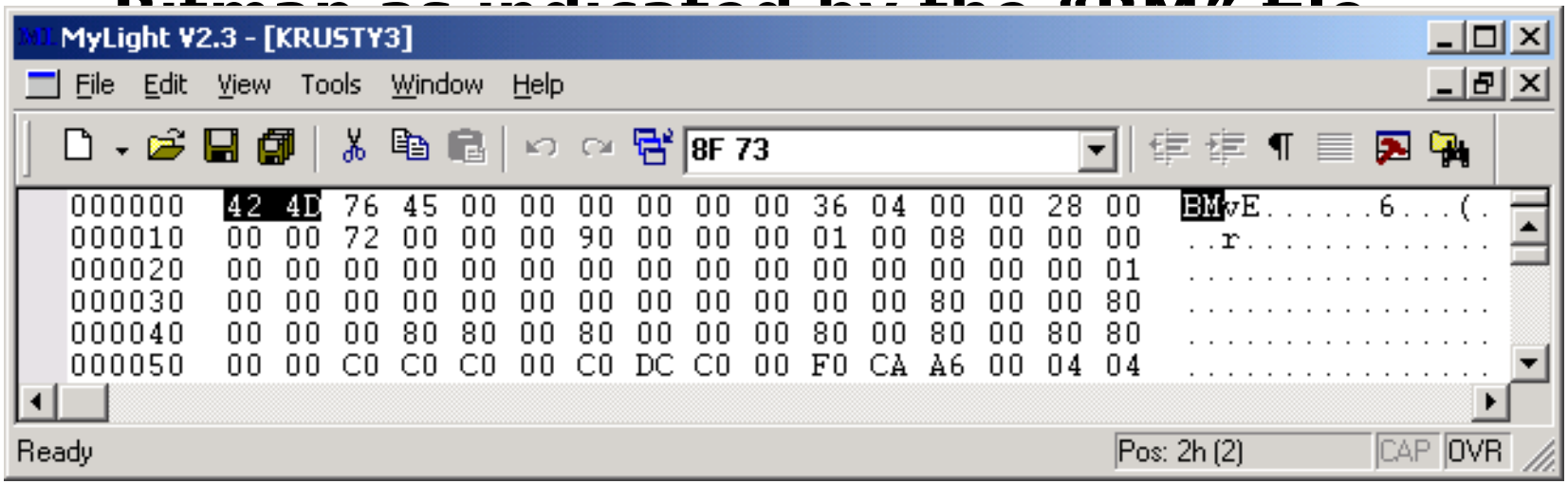
Hiderman – Case Study

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



Hiderman – Case Study

- **After hiding a message with Hiderman, we can review the file with our favorite Hex Tool.**
- **Viewing the Header information (beginning of the file) we see that it's a Bitman as indicated by the "BM" file**

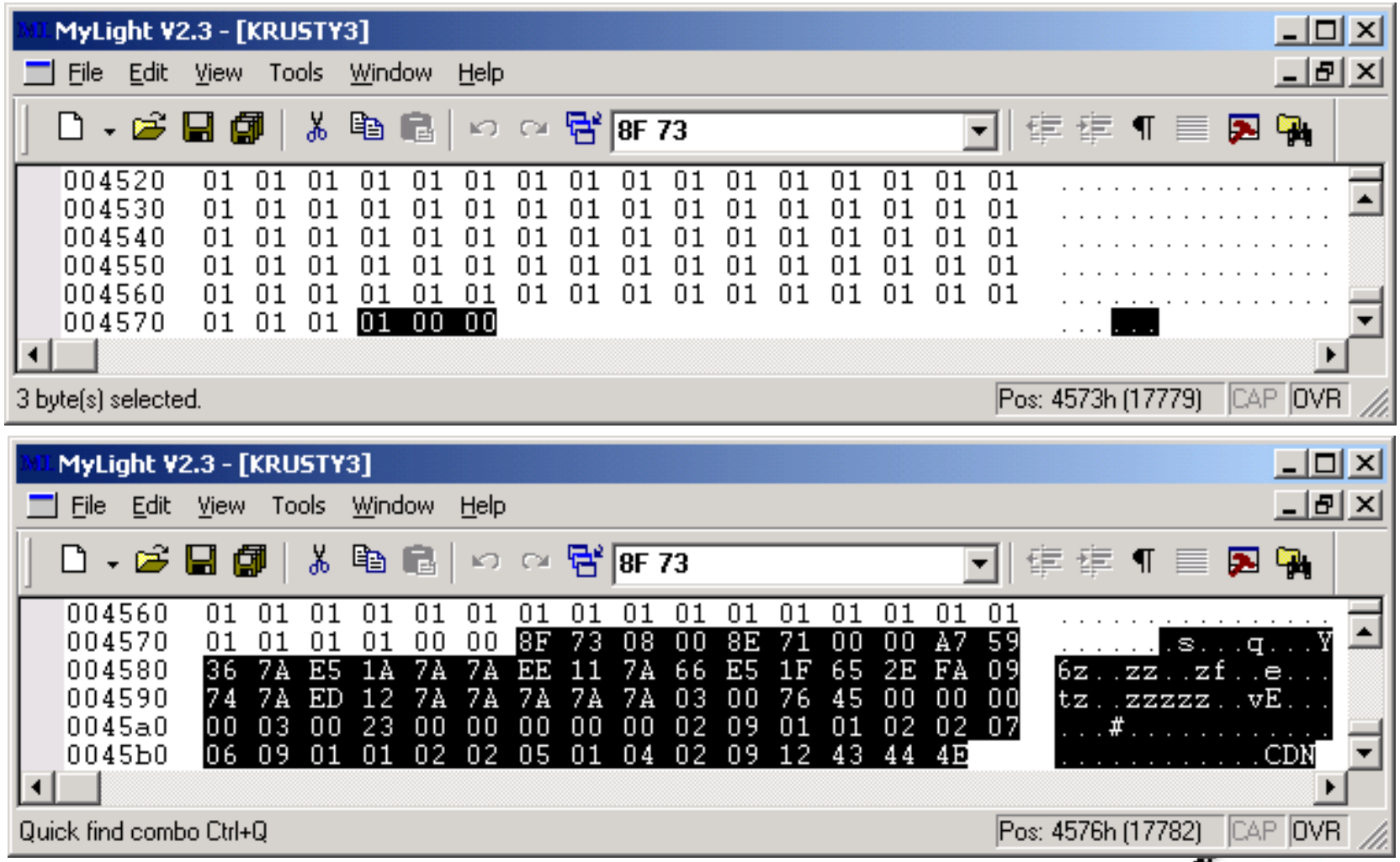


VeriSign®

Hiderman – Case Study

- We then view the end of the file, comparing the virgin file to the carrier file
- Note the data appended to the file (on the next slide)

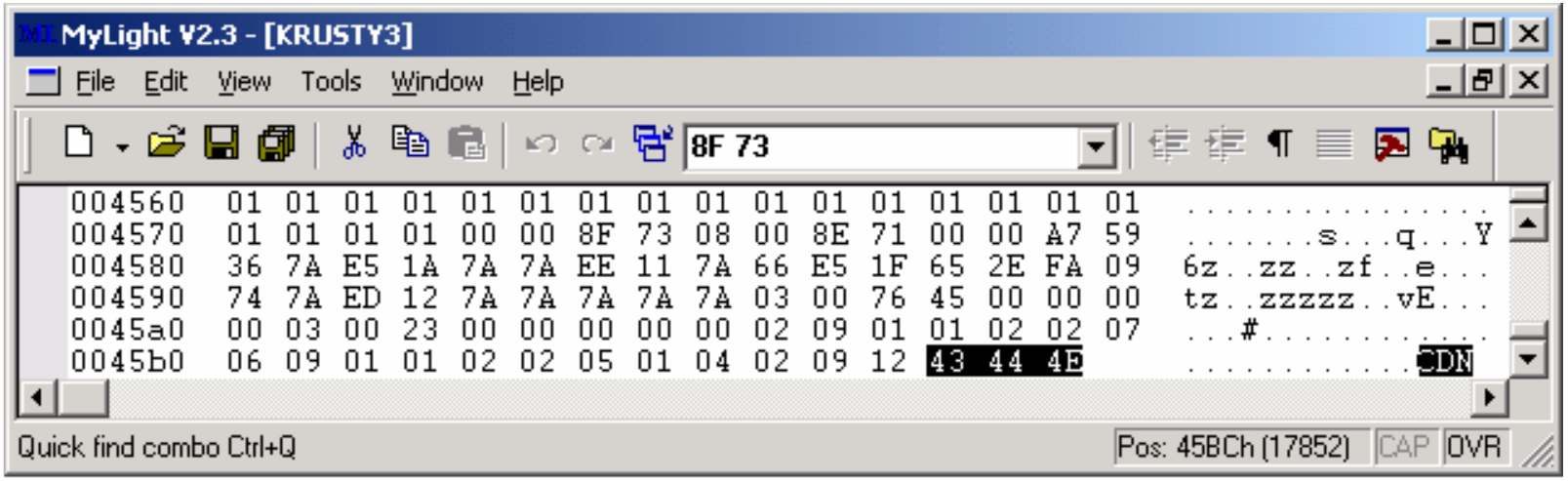
Hiderman – Case Study



VeriSign®

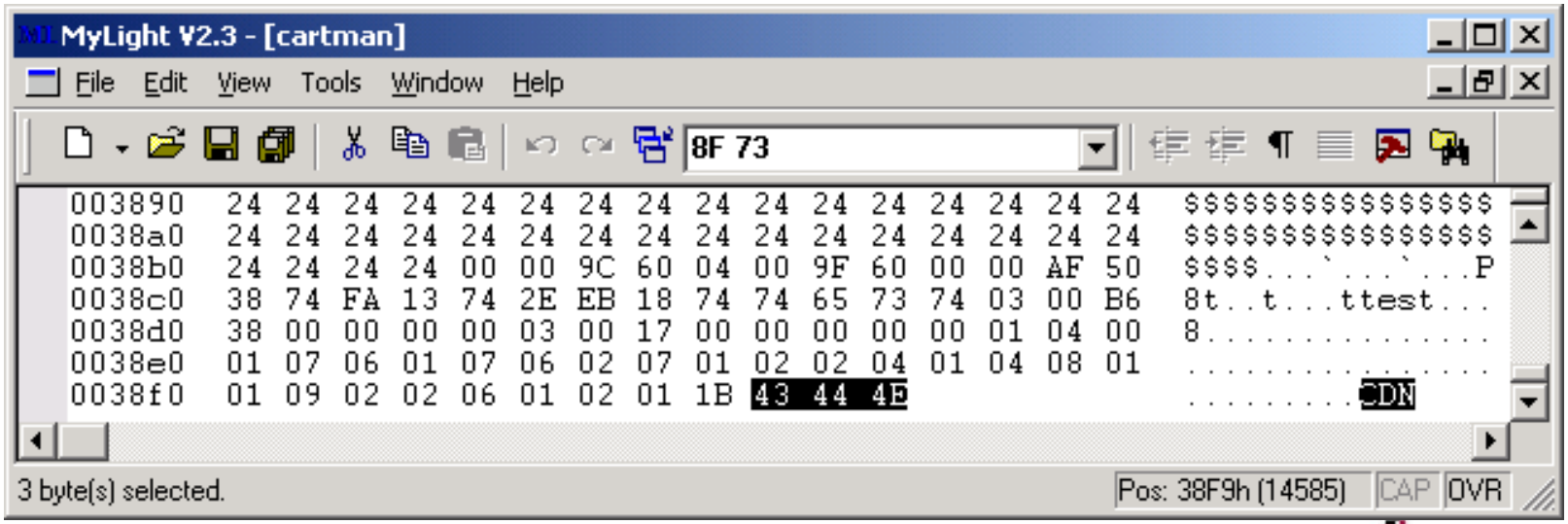
Hiderman – Case Study

- **In addition, note the last three characters “CDN” which is 43 44 4E in HEX.**



Hiderman – Case Study

- **Hiding different messages in different files with different passwords, we see that the same three characters (“CDN”) are appended to the end of the file.**
- **Signature found.**



VeriSign®

Steganalysis – Stegspy V2.0

- **StegSpy V2.0**
  - **Signature identification program**
  - **Searches for stego signatures and determines the program used to hide the message**
  - **Identifies 13 different steganography programs**
  - **Identifies location of hidden message**

Steganalysis - Stegspy

- **StegSpy - Demo**

Steganalysis – Stegspy V2.0

- **StegSpy V2.0**
  - **Will be available for download from my site**
    - **www.spy-hunter.com**

Steganalysis – Identifying a signature

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

VeriSign®

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!

VeriSign®

VeriSign®
The Value of Trust℠

Steganalysis meets Cryptanalysis

Revealing hidden files

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**
- **Identifying and cracking the algorithm**
  - Unfortunately, some of these programs use strong encryption 128-bit or stronger – GOOD LUCK!
- **Reveal or Crack the password, seed, or secret key**
  - Practically all Steganography programs use a password to hide the message

VeriSign®

Cryptanalysis

- Identify program used to hide message
- Identify the location of the program signature in the file
- Identify the location of the password in the file
- Identify location of the hidden message in the file
- Identify the algorithm used to encrypt the hidden message

VeriSign®

Steganalysis – Password Guessing

Password Guessing/Dictionary Attacks

- **A few password guessing programs have been created.**
- **Stegbreak by Niels Provos, www.outguess.org**
  - J-Steg
- **Can now be found on the Knoppix Penguin Sleuth forensics CD**
  - www.linux-forensics.com

VeriSign®

Cryptanalysis – Brute Force Method

Brute Force – Reverse Engineering

- **Common encryption techniques**
  - Modification of LSB (Least Significant Bit)
  - Password and/or contents masked using an algorithm
    - Algorithm based on a secret key
    - Algorithm based on the password
    - Algorithm based on a random seed hidden somewhere else in the file

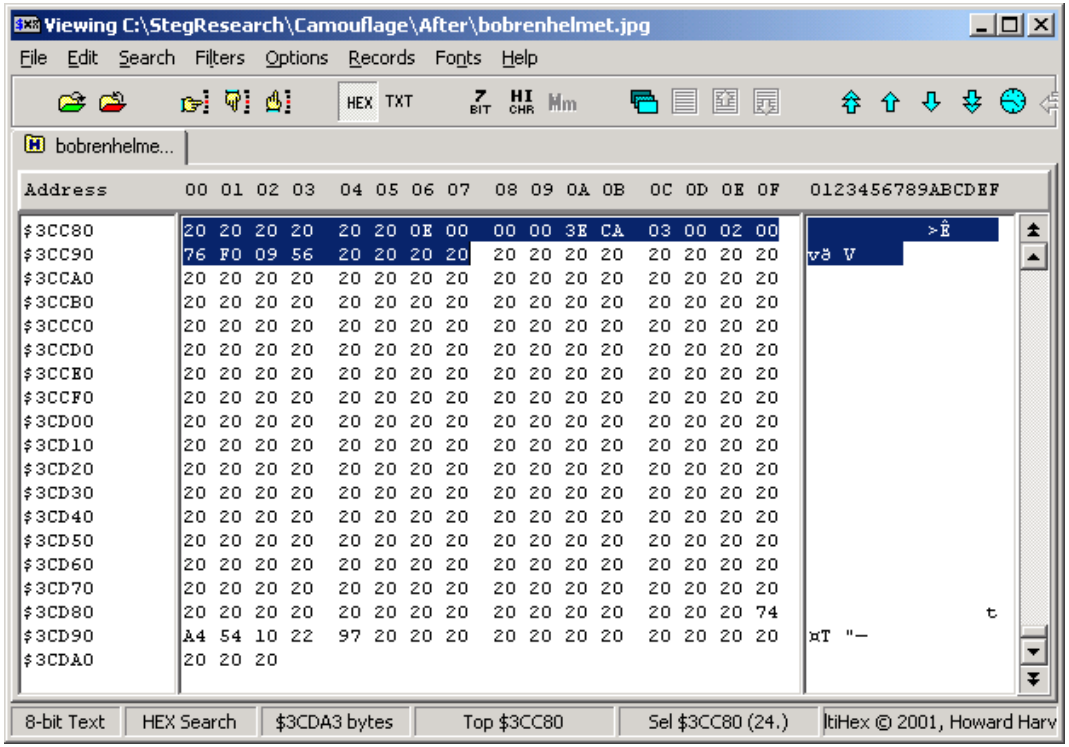
VeriSign®

Cryptanalysis – Brute Force Method

- **Common encryption algorithms used in steganography programs**
  - XOR
  - DES
  - 3DES
  - IDEA
  - AES

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**

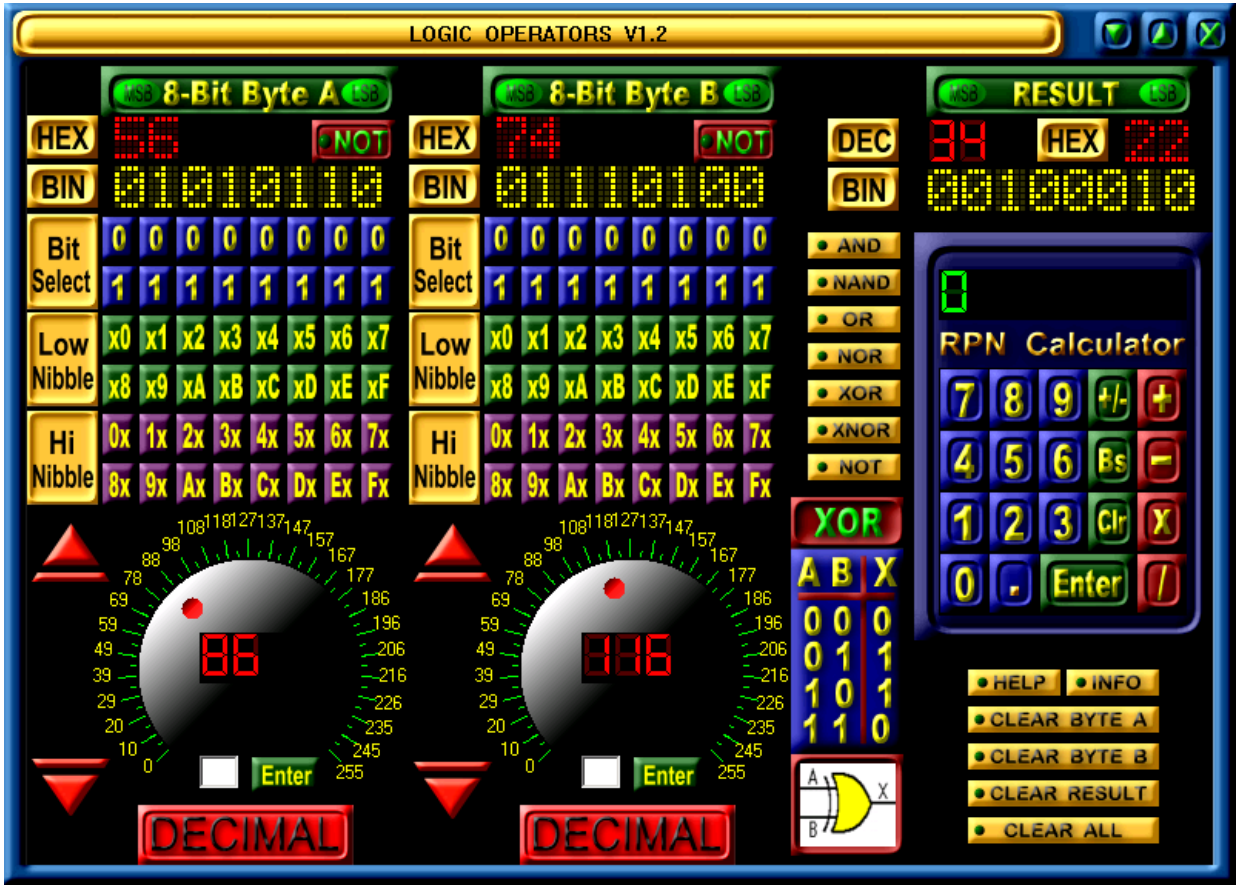


Camouflage

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

BDHTool

- **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

VeriSign®

VeriSign®
The Value of Trust℠

Forensics/Anti-Forensics

Anti-Forensics

- **Best Practices when using Steganography programs:**
  - Use a password different than your O/S password
  - Delete original message once you have created a new image with the hidden message
  - Remove the Steganography program after hiding the message
  - OR run the Steganography program from a CD if possible.
  - Use Alternate Data Streams…

VeriSign®

Anti-Forensics – Alternate Data Streams

Alternate Data Streams

- (NTFS) New Technology File System allows for Alternate Data Streams
- One file can be a link to multiple Alternate Data Streams of files of any size.
- Important Note! – These Alternate Data Streams are Hidden!
- Allows for hiding of files and even directories!
- Difficult to detect
  - Doesn’t show up when you run c:\dir

Anti-Forensics – Alternate Data Streams

- **Alternate Data Streams**
  - C:\notepad mike.txt:mikehidden.txt
  - This allows mikehidden.txt to be a hidden ADS
  - C:\dir
  - 02/26/2004 02:29p 0 mike.txt
  - Notice – no indication of mikehidden.txt
  - Although a message was saved in the mikehidden.txt, the mike.txt shows 0 bytes!

VeriSign®

Anti-Forensics – Alternate Data Streams

- Alternate Data Streams can be used to hide private files, viruses and trojans!
  - **Anti-Virus/Anti-Trojan Test - Does your scanner pass the test?**
  - There's a small utility MakeStream, that can be used to move a virus or trojan to a hidden Alternate Data Stream attached to an "innocent" text file!
  - For example, if you ran **makestrm.exe c:\test.exe**, the file contents of c:\test.exe would be moved into c:\test.exe:StreamTest (an Alternate Data Stream), and the original file contents are then over-written with a simple message reminding you about the linked stream.
  - Get any trojan or virus that is detected by your virus/trojan scanner, and run makestrm.exe on it to move its file contents into a hidden stream. Then, re-scan the file - is it still detected?
  - Many commercials scanners ***do not*** identify viruses and trojans hidden in ADS's!
  - http://www.diamondcs.com.au/web/streams/streams.htm

VeriSign®

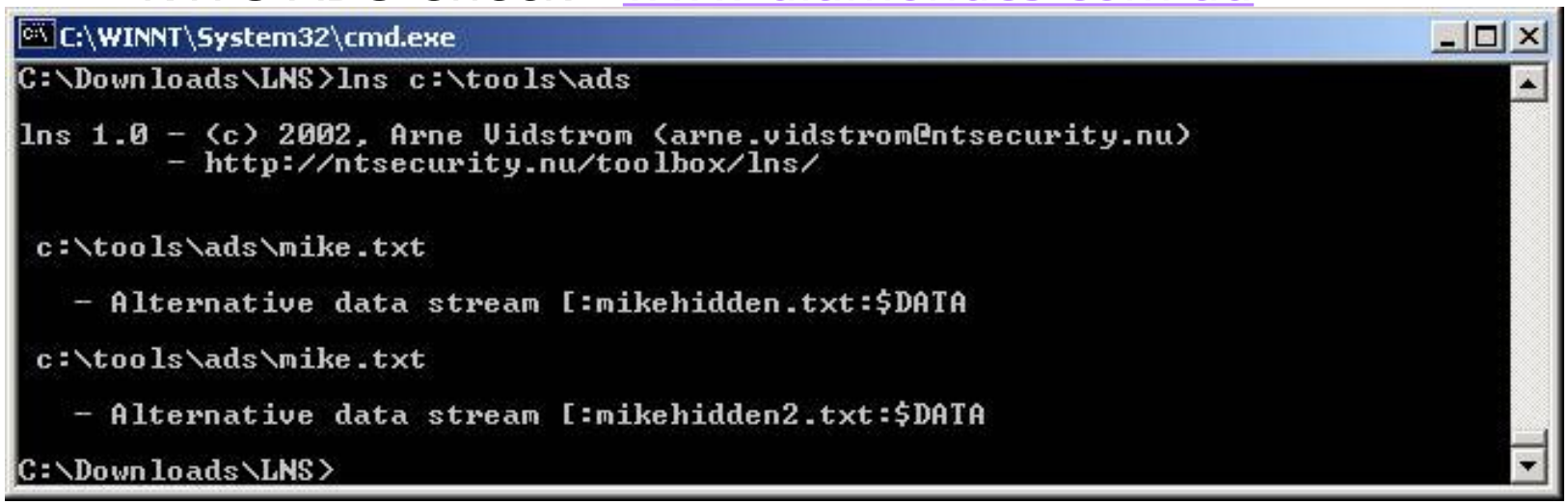
Forensics

- **If performing Forensics and discover a potentially "stega-nized" file:**
  - Look for evidence of steganography programs on the computer
  - Leverage other O/S and application passwords found on the machine, this may also be the password used to hide the message
  - Look for other hints such as a password written down on a note, letters, diaries, etc.
  - For more info – please see "Electronic Crime Scene Investigation – A Guide for First Responders, U.S. Dept of Justice"

VeriSign®

Forensics – Alternate Data Streams

- **Tools for Detecting Alternate Data Streams**
  - LNS – www.ntsecurity.nu
  - LADS - www.heysoft.de
  - NTFS ADS Check - www.diamondcs.com.au



VeriSign®
The Value of Trust℠

Conclusions

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)

VeriSign®

Steganalysis – Other Tools

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

VeriSign®

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!**

VeriSign®

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

VeriSign®

VeriSign®
The Value of Trust℠

Question and Answer