



Steganography and Steganalysis

Creating and Detecting Hidden Messages

Gary C. Kessler
Digital Investigation Management program
Champlain College

Overview

- The role of steganography
- Low-tech stego methods
- Digital steganography
 - LSB substitution
- Stego examples
- Suspecting and investigating stego
- Steganalysis software

Steganography

- Steganography = *covered writing*
 - $\text{cover_medium} + \text{hidden_data} + \text{stego_key} = \text{stego_medium}$
- Uses...
 - Dates back several millennium: wax tablets, messages tattooed on scalps
 - Microdots, invisible ink, microfilm...
 - Could hide an image under another image in a PPT file or text in same color as background
 - Digital steganography can hide information in image, video, or audio files -- or just about any binary file
 - Primary legitimate use is "digital watermarking"

© 2000-2009, Gary C. Kessler

2

Digital Watermarking

- Digital watermarking is a subset of stego
 - Used to protect ownership of intellectual property
- Characteristics
 - Usually involves a small amount of repetitive data
 - Watermark not necessarily hidden
 - Watermark can be removed without disrupting integrity of original file

© 2000-2009, Gary C. Kessler

3



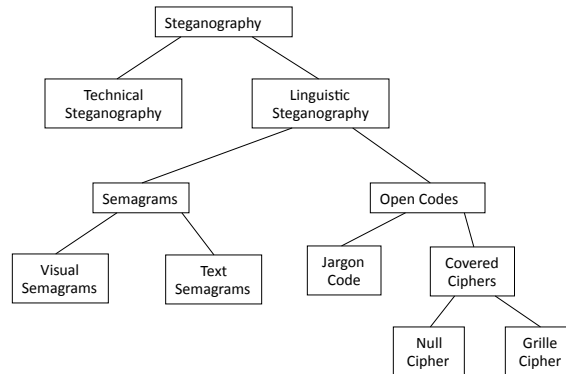
Is This Real?



ABC News
Prime Time Thursday
10/4/2001

- Stego can be used to hide information
 - In e-mail messages
 - On FTP or P2P sites
 - On auction, news, blog, or other sites

A Taxonomy of Steganography



*

© 2000-2009, Gary C. Kessler

6

Low-Tech Stego Methods

- There are many low-tech ways of hiding information
 - Hard to detect
 - Take advantage of fact that some information doesn't need to stay hidden forever
 - If the message can stay undetected or undeciphered until after some event...
 - $T_{\text{DETECT}} + T_{\text{DECODE}} > T_{\text{CRITICAL}}$

© 2000-2009, Gary C. Kessler

7

The Purloined Letter

"And what is the difficulty now?" I asked. "Nothing more in the assassination way, I hope?"

"Oh no; nothing of that nature. The fact is, the business is very simple indeed, and I make no doubt that we can manage it sufficiently well ourselves; but then I thought Dupin would like to hear the details of it, because it is so excessively odd."

"Simple and odd," said Dupin.

"Why, yes; and not exactly that, either. The fact is, we have all been a good deal puzzled because the affair is so simple, and yet baffles us altogether."

"Perhaps it is the very simplicity of the thing which puts you at fault," said my friend.

"What nonsense you do talk!" replied the Prefect, laughing heartily.

"Perhaps the mystery is a little too plain," said Dupin.

"Oh, good heavens! who ever heard of such an idea?"

"A little too self-evident."

"Ha! ha! ha! --ha! ha! ha! --ho! ho! ho!" --roared our visitor, profoundly amused, "oh, Dupin, you will be the death of me yet!"

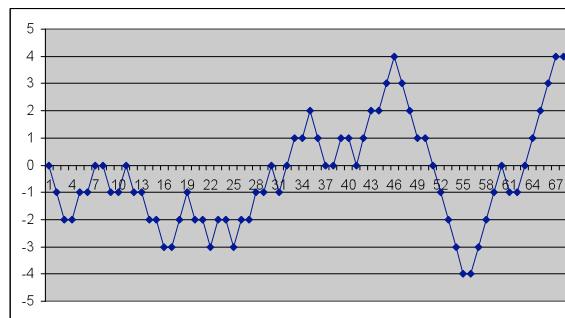
"The Purloined Letter," Edgar Allen Poe, 1845



© 2000-2009, Gary C. Kessler

8

A Side Issue



Accumulated heating degree-day units in Burlington, VT, 12/15/2005-2/21/2006... a bad winter for show shoeing

© 2000-2009, Gary C. Kessler

9

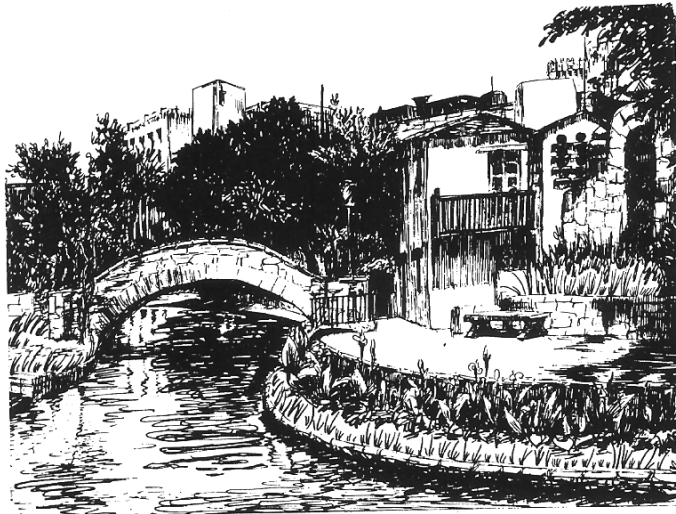
Semagrams

- Means "sign message"
- Use of everyday symbols to convey meaning
 - Arrangement of items on a desk or books on a bookshelf
 - Orientation of a picture
 - Choice of clothing
- Detection cannot (yet?) be automated!
 - Requires human eye and intelligence

© 2000-2009, Gary C. Kessler

10

The San Antonio River



© 2000-2009, Gary C. Kessler

11

The Message in the Picture



.....

"compliments of CPSA MA to our chief Col Harold R Shaw on his visit to San Antonio May 11th 1945"

Historical note: Col. Shaw was then the head of the Technical Operations Division of the U.S. government's censorship division.

From: Bauer, Decrypted Secrets (3rd. ed.)

© 2000-2009, Gary C. Kessler

12

Aljazeera.Net English - Home Page - Mozilla Firefox

http://english.aljazeera.net/HomePage

ALJAZEERA.NET

Updated on: Wednesday 01 February 2006, 17:13 Makka Time, 14:13 GMT

Abbas, Egypt tough on Hamas

Palestinian leader Mahmud Abbas and Egypt have taken a tough line with Hamas, setting a renunciation of violence and the recognition of Israel as conditions for the Islamist movement to form the next government. **FULL STORY**

- Annan urges Hamas to shun violence

TOP NEWS

- Violence erupts during West Bank pullout
- Iran vows to resist Western pressures
- Saddam boycotts trial
- French daily prints anti-Islam cartoons

madrid 3 TIMES A WEEK

QATAR AIRWAYS قطرية

3 FLIGHTS A WEEK

Palestinian Elections

AUDIENCE PANEL

ALJAZEERA INTERNATIONAL Click here to join

منتدى الجزيرة الثاني THE 2ND ALJAZEERA FORUM

Market Watch

Job Vacancies

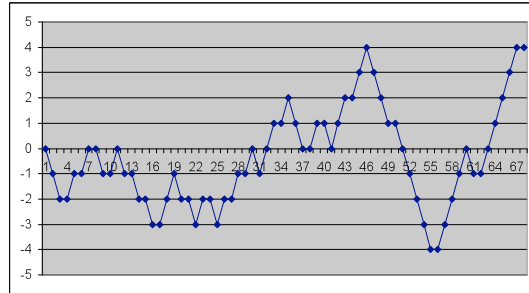
Interviews

"We are all Christians"

Done

7

Revisit The Graph...



Read as...
 1 = dot
 0 = space
 -1 = dash

-. . - / . - - / - - /
 . - . . . / . - - - -

Meet at tunnel Wed 2045

Null Cipher

- Null cipher hides message in the text of another message
- E.g., messages sent by Germans during WW I

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

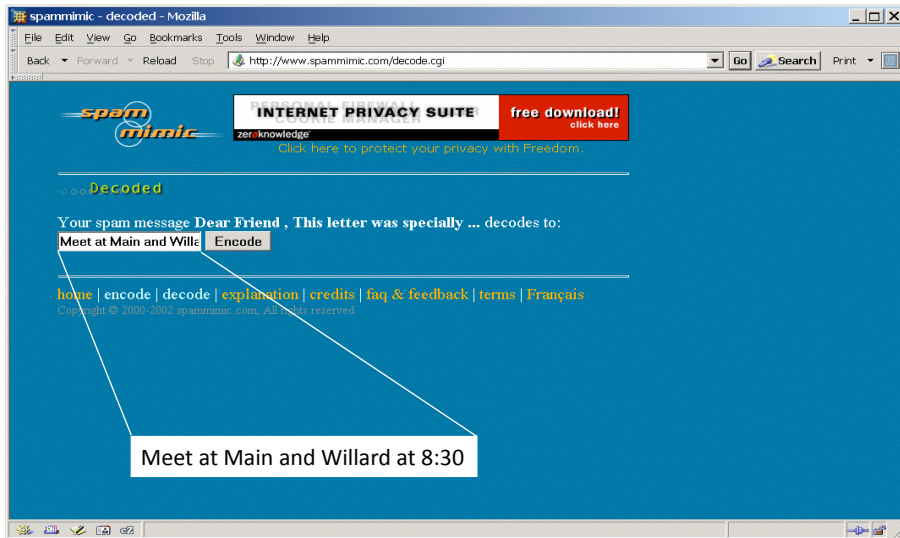
PERSHING SAILS FROM N.Y. JUNE 1

Spam as a Stego Medium

Dear Friend , This letter was specially selected to be sent to you ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1621 ; Title 5 ; Section 303 ! Do NOT confuse us with Internet scam artists . Why work for somebody else when you can become rich within 38 days ! Have you ever noticed the baby boomers are more demanding than their parents & more people than ever are surfing the web ! Well, now is your chance to capitalize on this ! WE will help YOU sell more & SELL MORE . You can begin at absolutely no cost to you ! But don't believe us ! Ms Anderson who resides in Missouri tried us and says "My only problem now is where to park all my cars" . This offer is 100% legal . You will blame yourself forever if you don't order now ! Sign up a friend and your friend will be rich too . Cheers ! Dear Salaryman , Especially for you - this amazing news . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate bill 2116 , Title 3 ; Section 306 ! This is a legitimate business proposal ! Why work for somebody else when you can become rich within 68 months ! Have you ever noticed more people than ever are surfing the web and nobody is getting any younger ! Well, now is your chance to capitalize on this . We will help you decrease perceived waiting time by 180% and SELL MORE . The best thing about our system is that it is absolutely risk free for you !

But don't believe us ! Mrs Ames of Alabama tried us and says "My only problem now is where to park all my cars" . We are licensed to operate in all states ! You will blame yourself forever if you don't order now ! Sign up a friend and you'll get a discount of 20% ! Thanks ! Dear Salaryman , Your email address has been submitted to us indicating your interest in our briefing ! If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our mailing list . This mail is being sent in compliance with Senate bill 1618 , Title 6 , Section 307 . THIS IS NOT A GET RICH SCHEME . Why work for somebody else when you can become rich within 17 DAYS ! Have you ever noticed more people than ever are surfing the web and more people than ever are surfing the web ! Well, now is your chance to capitalize on this ! WE will help YOU turn your business into an E-BUSINESS and deliver goods right to the customer's doorstep ! You are guaranteed to succeed because we take all the risk ! But don't believe us . Ms Simpson of Wyoming tried us and says "Now I'm rich, Rich, RICH" ! We assure you that we operate within all applicable laws . We implore you - act now ! Sign up a friend and you'll get a discount of 50% . Thank-you for your serious consideration of our offer .

spammimic.com



Grammar-Based Stego

Encoded message: K (01001011)

Dear Friend , Especially for you - this cutting-edge intelligence ! This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 2316 , Title 3 ; Section 307 . This is a legitimate business proposal ! Why work for somebody else when you can become rich as few as 98 DAYS . Have you ever noticed most everyone has a cellphone and more people than ever are surfing the web . Well, now is your chance to capitalize on this ! WE will help YOU decrease perceived waiting time by 200% and turn your business into an E-BUSINESS ! The best thing about our system is that it is absolutely risk free for you ! But don't believe us . Mr Ames of Massachusetts tried us and says "My only problem now is where to park all my cars" ! We are licensed to operate in all states ! We beseech you - act now . Sign up a friend and your friend will be rich too ! Thank-you for your serious consideration of our offer !

Encoded message: k (01101011)

Dear Decision maker , This letter was specially selected to be sent to you ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 2416 ; Title 6 , Section 306 ! THIS IS NOT MULTI-LEVEL MARKETING . Why work for somebody else when you can become rich inside 30 DAYS ! Have you ever noticed people love convenience & most everyone has a cellphone ! Well, now is your chance to capitalize on this . We will help you use credit cards on your website and decrease perceived waiting time by 200% . You can begin at absolutely no cost to you ! But don't believe us ! Prof Ames of Florida tried us and says "Now I'm rich many more things are possible" ! This offer is 100% legal ! We BESEECH you - act now ! Sign up a friend and you'll get a discount of 50% . Thanks .

<http://www.spammimic.com>

See also <http://www.delirandom.net/20070407/steganalysis-attack-against-spammimic/>

© 2000-2009, Gary C. Kessler

18

White-Space Stego

- Snow
 - Conceals messages by appending tabs and spaces on the end of lines
 - Data is concealed in a text file by appending strings of up to 7 spaces, interspersed with tabs
 - Allows 3 bits to be stored every 8 columns

```

DOS box
C:\My Programs\stego>snow -s ean.txt
File has storage capacity of between 224 and 230 bits.
Approximately 28 bytes.

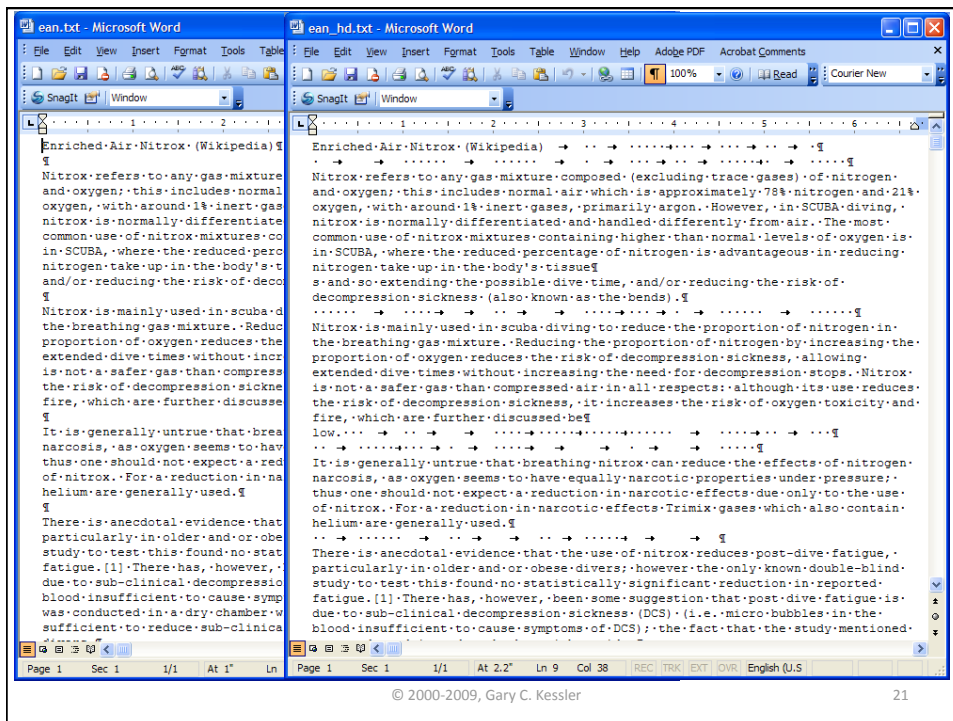
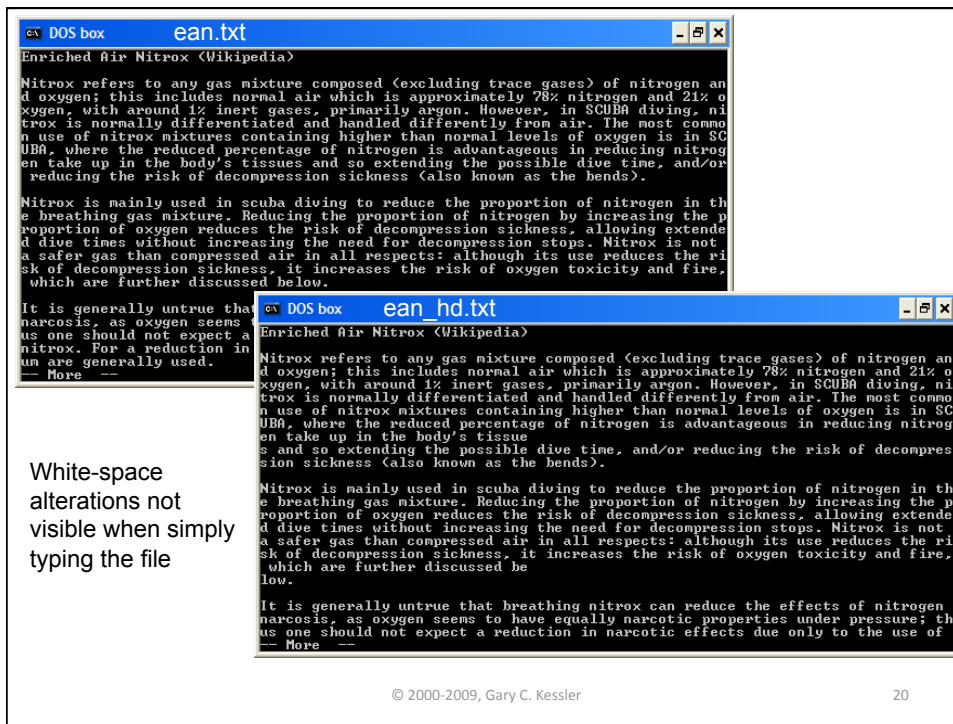
C:\My Programs\stego>snow -m "We need to meet ASAP" ean.txt ean_hd.txt
Message used approximately 72.07% of available space.

C:\My Programs\stego>snow ean_hd.txt
We need to meet ASAP
C:\My Programs\stego>

```

© 2000-2009, Gary C. Kessler

19



Stego on the Cheap

- Suppose you have an innocuous image (`gck.jpg`) and data to hide (`secret.xxx`)
 - Compress `secret.xxx` with WinZip or equivalent
 - Use the following DOS command:


```
copy /b gck.jpg+secret.zip newpic.jpg
```
 - `newpic.jpg` will display normally with no indication that anything follows the JPEG file trailer
- Try this and look at the resultant file with WinHex

Inch, S. (2008, June). A simple image hiding technique: What you may be missing. *Journal of Digital Forensic Practice*, 2(2), 83:94.

© 2000-2009, Gary C. Kessler

22

Hiding Data in Executable Files

- *hydan*
 - Hides data in a Windows or Linux binary file
 - Takes advantage of redundancies in i386 assembler
 - E.g., **A+B** vs. **A- (-B)**
 - Can hide one byte in ~110 instruction bytes
 - Maintains size of carrier file

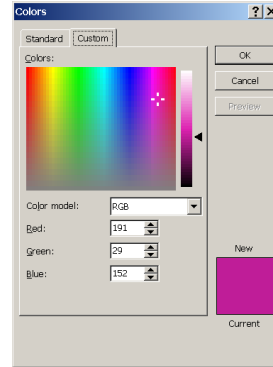
<http://www.crazyboy.com/hydan/>

© 2000-2009, Gary C. Kessler

23

8-bit vs. 24-bit Color

- 24-bit color is *True Color*
 - 1 pixel requires three bytes, each representing level of red/green/blue (RGB) color
 - Color of this line is denoted 0xbf-1d-98 [i.e., Red=191 (0xbf), Green=29 (0x1d), Blue=152 (0x98)]
 - 16,777,216 (2^{24}) possible colors/image
- 8-bit color is *also* True Color, but...
 - » Image contains a palette with up to 256 (2^8) unique colors, each of which is denoted by a 24-bit RGB value
 - » Each pixel requires 1 byte to point to palette entry

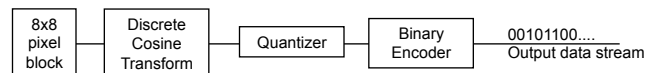


© 2000-2009, Gary C. Kessler

24

JPEG

- JPEG saves DCT coefficients rather than pixel encoding



- DCT uses 8x8 pixel array ($N_1=N_2=8$), creates arrays of luminance (A) and chrominance (B)


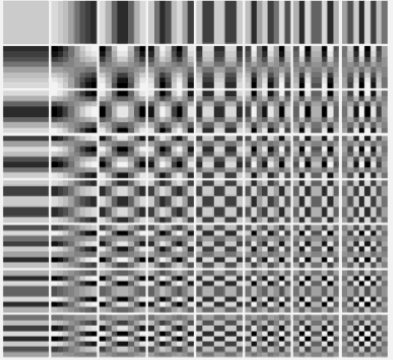
$$B(k_1, k_2) = \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} 4 \cdot A(i, j) \cdot \cos\left[\frac{\pi \cdot k_1}{2 \cdot N_1} \cdot (2i + 1)\right] \cdot \cos\left[\frac{\pi \cdot k_2}{2 \cdot N_2} \cdot (2j + 1)\right]$$

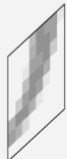



- *luminance* = brightness, darkness and contrast
- *chrominance* = colors to display

© 2000-2009, Gary C. Kessler

25


JPEG Coefficients


 $= C_1 \cdot$

 $+ C_2 \cdot$

 $+ \dots + C_{64} \cdot$



© 2000-2009, Gary C. Kessler Source: Andreas Westfeld 26

Discrete Cosine Transformation



64 brightness values

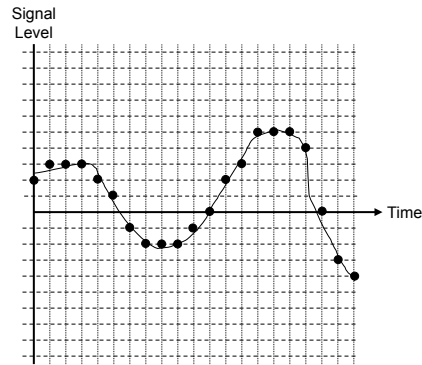
➔ 19 nonzero JPEG coefficients



	-	+	-	+	-	-	+		-	+	-	+	
-	+	+	+	+	-	-	+		-	+	+	-	+
+	+	-	-	+	-	+	+		+	+	-	+	
-	-	+	+	+	+	-	+		-	-	+		
-	-	-	+	+	+	+	-	+					
+	+	+	+	-	-	+	+						
+	+	-	-	-	+	+	-						

© 2000-2009, Gary C. Kessler Source: Andreas Westfeld 27

Encoding Voice



- Pulse Code Modulation
 - Human ear detects 20-20,000 Hz; sampling rate is twice highest frequency
 - Voice uses 2^8 quantization levels; music uses 2^{16} levels
 - Voice samples 8 kHz, music up to 44.1 kHz

© 2000-2009, Gary C. Kessler

28

LSB Substitution

- LSB substitution overwrites the least significant bit of target bytes
- Example: Hide "G" (01000111) in 3 pixels

– Original data

10010101	00001101	11001001
10010110	00001111	11001011
10011111	00010000	11001011

– Stego data

1001010 <u>0</u>	0000110 <u>1</u>	1100100 <u>0</u>
1001011 <u>0</u>	0000111 <u>0</u>	1100101 <u>1</u>
1001111 <u>1</u>	0001000 <u>1</u>	11001011

Note that only 50% of the stego bits actually change!

© 2000-2009, Gary C. Kessler

29

Where Stego Works Best

- Steganography works best in cover files with high energy...
 - Bright colors
 - High volume

© 2000-2009, Gary C. Kessler

30

Steganography Methods and Tools

- **LSB Encoding**
 - E.g., S-Tools
- **Grammar selection**
 - E.g., spammimic, hydan
- **Covert Channels**
 - E.g., Covert TCP
- **Data Appending**
 - E.g., Camouflage
- **Color Palette Modification (8-bit)**
 - E.g., S-Tools, Gif-It-Up
- **Format Modification**
 - E.g., Invisible Secrets, Snow
- **Encoding Algorithm Modification**
 - E.g., J-Steg, JP Hide-&-Seek, MP3 Steno

© 2000-2009, Gary C. Kessler

31

Sample Stego Tools

- **There are over 350 free and commercial stego tools**
 - Primary carrier files are image and audio formats
 - **Any** type of binary file can be hidden
- **Examples**
 - S-Tools
 - Designed for lossless compression; hides information inside BMP, GIF, or WAV files using LSB overwriting (password used for LSB randomization and encryption)
 - Gif-It-Up
 - Designed for lossless compression; hides information inside GIF files using LSB overwriting
 - JP Hide-&-Seek
 - Designed for lossy compression; hides information inside JPEG files using LSB overwriting of DCT coefficients
 - Camouflage
 - Append hidden file to carrier file

© 2000-2009, Gary C. Kessler

32

Examples



btv_map.gif [11,067 B]

Hide map in:

1. GIF file (Gif-It-Up)
2. JPEG file (JP Hide-&-Seek)
3. WAV file (S-Tools)
4. JPEG file (Camouflage)

© 2000-2009, Gary C. Kessler

33

Example 1 - GIF File (Gif-It-Up)



mall_at_night.gif



mall_at_night_btv2.gif

© 2000-2009, Gary C. Kessler

34

Example 1 - GIF File Properties

IrfanView - Image properties

File name:	mall_at_night.gif
Directory:	C:\My Programs\stego\examples\
Compression:	GIF - LZW
Resolution:	x DPI <input type="button" value="Set"/>
Original size:	1600 x 1032 Pixels
Current size:	1600 x 1032 Pixels
Original colors:	256 (8 BitsPerPixel)
Current colors:	256 (8 BitsPerPixel)
Number of unique colors:	249
Disk size:	617.95 KB (632778 Bytes)
Current memory size:	1.58 MB (1652224 Bytes)
Current directory index:	15 / 21
File date/time:	05.10.2003 / 12:01:26
Loaded in:	140 milliseconds

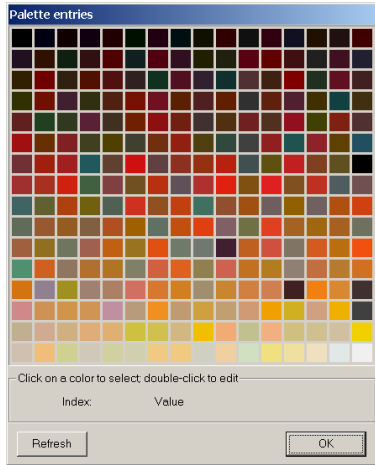
IrfanView - Image properties

File name:	mall_at_night_btv2.gif
Directory:	C:\My Programs\stego\examples\
Compression:	GIF - LZW
Resolution:	x DPI <input type="button" value="Set"/>
Original size:	1600 x 1032 Pixels
Current size:	1600 x 1032 Pixels
Original colors:	256 (8 BitsPerPixel)
Current colors:	256 (8 BitsPerPixel)
Number of unique colors:	256
Disk size:	661.85 KB (677733 Bytes)
Current memory size:	1.58 MB (1652224 Bytes)
Current directory index:	17 / 21
File date/time:	24.12.2003 / 14:25:34
Loaded in:	140 milliseconds

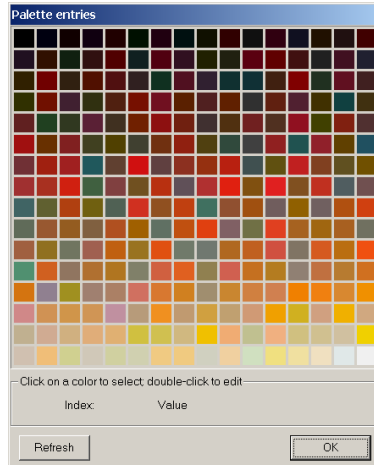
© 2000-2009, Gary C. Kessler

35

Example 1 - GIF File Palettes



mall_at_night.gif

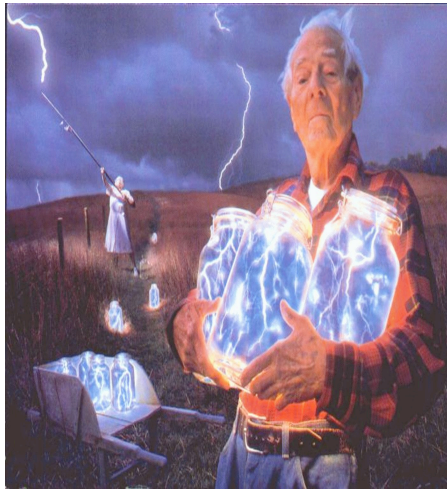


mall_at_night_btv2.gif

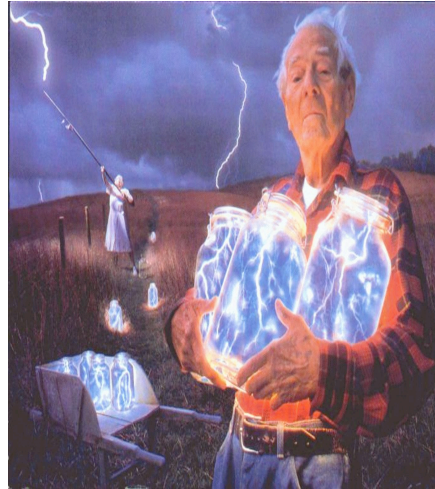
© 2000-2009, Gary C. Kessler

36

Example 2 - JPEG File (JPHS)



lightning_jars.jpg

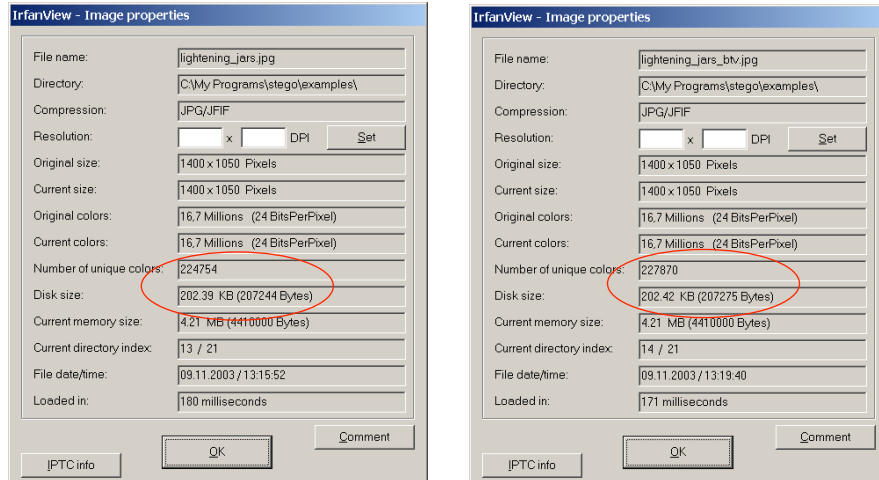


lightning_jars_btv.jpg

© 2000-2009, Gary C. Kessler

37

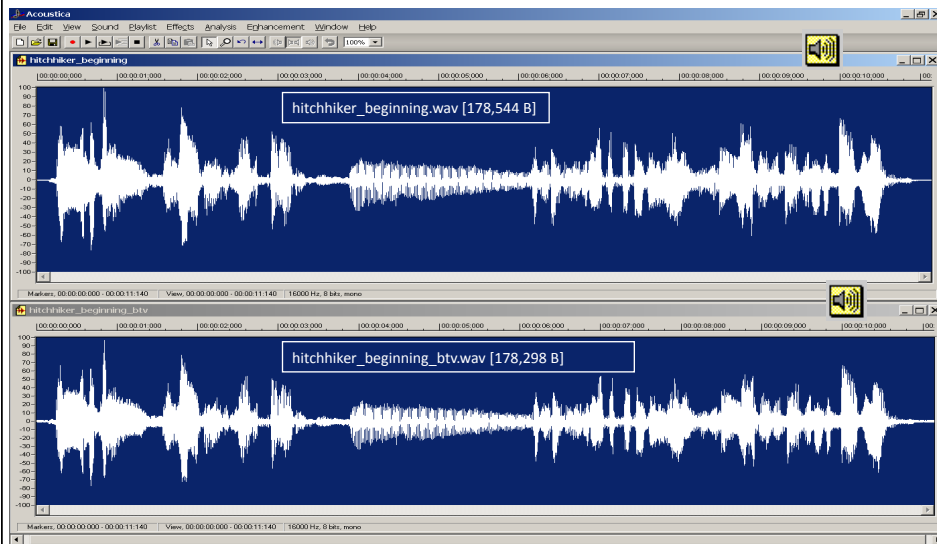
Example 2 - JPEG File Properties



© 2000-2009, Gary C. Kessler

38

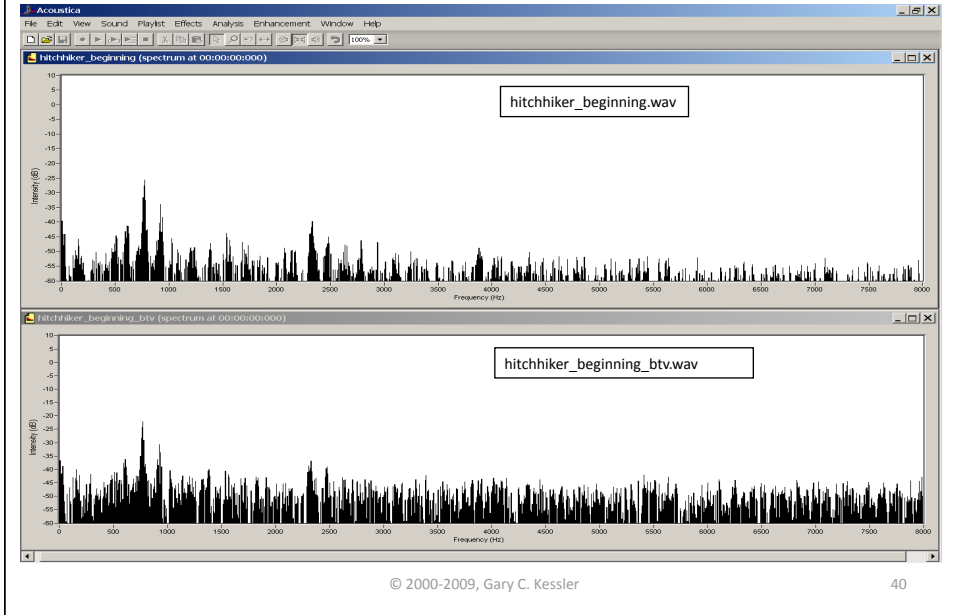
Example 3 - WAV File (S-Tools)



© 2000-2009, Gary C. Kessler

39

Example 3 - WAV Spectrum Analysis



Example 4 - JPEG File (Camouflage)



gck_mes.jpg
61,289 B

gck_mes_bt.jpg
73,211 B

Example 4 - Binary Analysis

© 2000-2009, Gary C. Kessler 42

Side Topic - BASE64

- Any file type can be converted to text
 - BASE64 is a 6-bit "alphabet" composed of a-zA-Z0-9/+
- BASE64 commonly used to transport encrypted files

```

btv_map_base64.txt - Notepad
R01G0DlhqG6APcAAPPv5wAAAQAAAP/+AJCFc5m2mFGXW814Lfnq1dbkHv70g802of///1pa
WgAA2n8AABHfgJ12zpz+/7PG1C9fJc3Su3xPG/Pjx7/DgpzieDTOS8AAGaCYBj4q4AALPG
12kz26+2193KqNzqz5XfJPLs39scrm2m2LSCqtJXiRdbEFG/nCB+Fc/DrzszizAB/AD14D7bo
ps7kwn7Xyqueiev122SOWuJFNAD+AADKAADFADJACdAAB4AABmAP/c3P+EH9YWOuAMMA
AJYAAO71Aob2AMW/AM2yAMmALSDAAD//vd45GmzaCqggc2mgC1IABm2gAAGBmzP+82szM
mWzABDMH/8AM/OCAP//zndFcc/Fm6AA3L/42zqCARMMdAvwAR/KRSR+Emf//AAD/Jtz
t/i1J41HfYtmYzHBPozJLkBVCR4vtv3uH0W+YySti+43Top22jIbESLpKtdm2o2sFI
koYcLXK18Yram1kEBJkT7pKH6IY9Thp1dYUFT4z62xndIeIeBgYCH4Y2iYIPj460j056io
p/DcNnyXVYHvIn2zCLa4oPojYHJonAN4R3+YdpsIVi4ofriICBc2YLN1N4H4WJ1IAHo
Tph4Rk4JFj0m9W7eIU4hoRjH4W1H4aJiIeJ9oMsaacB3R8dYEXDHeeP6y1b72omp1o
SGXs05XN614XXhoWJh4aL9NFtVzTK5XNigYemYkppoWJAKC2MaCUAUCOMoIviekeIXo/Y
1mE4NhwICKBoaHhoJiIiDo4OP7+ri4uYiYmIiLHh4eCqoBgYGAICAAAAIAAAACAIcA
AAAAGtIAGACAgICAgMDAwP8AAAD/8P/AAA//8A/wd/////j06ba1uujo+HEX828ckhQ8
Yy5khsC2z6KJ4Gebul/09H04+C10J0j43NzpxLLDj9j dovT4z/j460j05zntxJfj0yacdmsK
Q4JvWm+DFqj8W02Ya6BNJ+3TOPj4+HFK1yWAAAAQGH6AAAI/wABCXBsIKDBgwg7J1RhKWB
FQo3i1S4oKLFBJmWzNjIeafHjYBNYFw0SDJgydqlzJsgqLLR91kxkJs6Bmzh2657TTCHE
nRErmlhw2sghEjJmZpqgIKxTmasJmPpIKtepbCVZV9mz4htyEPORqFiv2YVCV1i0u9qp0afEza
kytYrY1L1Ykd3IhazX4UC/RgY71n1S83evy3kEKMDGGNB6hqiHwqYVcVjw1i1jmeoFI
Gq5tkRWOHvM//B17da0h1kLwY5dWjH249j1RjFq6IGAlaAe/cwnKXpY8Yp0e00Qu
XrplqdfP+j2Pv12ztLC90ndr2Wadgv+13rgt+d111vCaab3Yal260IMAIYIK141teWKTdx/
/1gtcLbYfNW8B2P2YmFUUBdfi4reChJNROepU4UrxmYhYSDDeoks11Lgn1wqoIACDXI
Ioeud+JcXg2ogCgtH5fVpSGCai0YVooSuYhYEPVdofNJA0JU1abgqCAG+0BICsfi3JhoI
LAAgalyIEKWKNUQ5V5IC4a1dRjYv6J2QJmUmfJwPwRkRbMc+YXNlonWSgt3ahnLDLq0sJto
NBQy55QyJcDMMAmbeYY1a1o5ndYVRSmk3J1tChhBWEKUJxyunYQDg2VdmpJ2KqpyNvto
pZkIM6mXkq3/ie2Ur21JkQKevTndh01Mh8x82a063vgFogBIS1aWQ0N56XalH2kshqpg702
2NFaJ01IK0K2F0zr07J8gavDwJfz/kohgqgATV1eID8Ma7RkqgdGqfHKFPpqbFwKp11
SjU9pW61C1NB1t7q3fgmvQu/w8MONJESelqCuULeLkXnoJ0zBw5I6WryvKjz2G61KRk2/
2F50uCRDpSwzLgqBd7MADTsClwitvIAP6Al+UCYm8q77mnu/Emu13J53LHFWmWLY+5K6Jv
YyYob7RzEXRkHwPbUgnd2ahBD04WUUIe467yqU66sTS8wCSWozjBS0J001Zs/YL3P+q
7HQWnt4j4Cehs5XK130bWk9Fq/LjCmK18IKUv822/Kz02Id91Eqi26gmL5PbdU179w6E
2CXZRNHNR1kxExtrtEPzFt01UED6/hj6z2er0y2g82VU9xS01hroEMpG9pmttkk2w26dhdc

```

Steganalysis

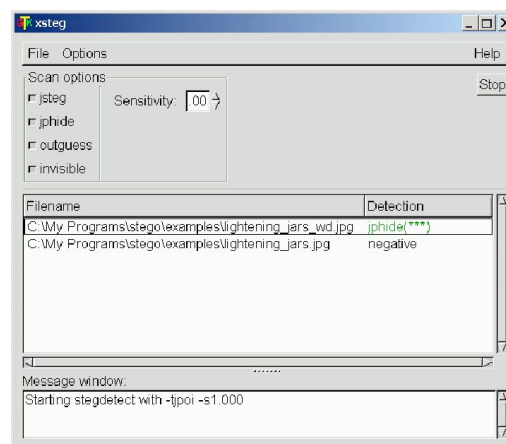
- Methods for detecting the use of steganography tools, detecting carrier files, and extracting hidden data
 - Each becomes increasingly difficult
- Several methods
 - Detecting stego software
 - Hash databases of known programs
 - Detecting carrier files
 - Comparison of "similar" files
 - Anomaly detection
 - Signature detection

© 2000-2009, Gary C. Kessler

44

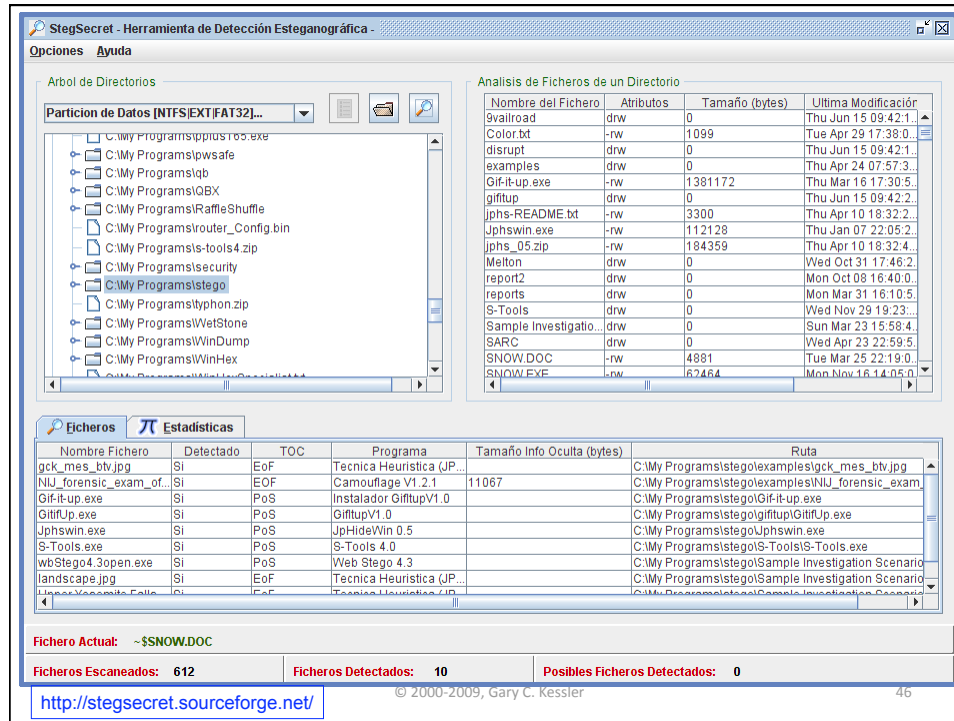
stegdetect

- Detects stego in JPEG images using several algorithms
- Neils Provo
 - Outguess.org



© 2000-2009, Gary C. Kessler

45



Wetstone Technologies

- Gargoyle (née StegoDetect)
 - Finds remnants of ~20 types of malware software, including stego, Trojans, and keyloggers
- Stego Suite
 - *Stego Hunter*: Detects remnants of steganography programs; can examine a local hard drive or mount and examine an E01 (EnCase), AD1 (AccessData), dd, ISO, or other image file
 - *Stego Watch*: Anomaly-based, blind stego detection software
 - *Stego Analyst*: Imaging and analysis tool, providing visual clues that steganography may have been used in both image and audio files
 - *Stego Break*: A password cracker for stego carrier files

Gargoyle Investigator™ FORENSIC PRO

Dataset Selection and Threat Legend:

Unselected	Selected	Low Threat	Medium Threat	High Threat
Anti Forensics: 2	BotNets:	Credit Card Fraud:	Denial of Service:	Encryption: 3
Exploit Scanners: 5	File Splitters: 2	Gaming:	Key Loggers: 1	P2P Tools:
Password Crackers: 47	Remote Access:	Rootkits: 4	Packet Sniffers: 22	Spyware: 1
Steganography: 19	Toolkits: 1	Trojans: 4	Wireless: 27	

Scan Location: C:\My Programs Scan

Completed.

Total Directories: 234
Total Files: 4120
Files Checked: 4120

Scan Completed Abort Scan

File Name	Detected	Name Differs	Program	Version	Multiple	Path
GIFutil.dll	Yes		S-Tools	4.00		C:\My Programs\g-tools4.zip\
S-Tools.exe	Yes		S-Tools	4.00		C:\My Programs\g-tools4.zip\
S-Tools.hlp	Yes		S-Tools	4.00		C:\My Programs\g-tools4.zip\
ftv2blank.gif	Yes		Super Utilities Pro	7.71	*	C:\My Programs\analyzer\Conf\html
ftv2doc.gif	Yes	*	DataCRYPT	2.2.1	*	C:\My Programs\analyzer\Conf\html
ftv2lastnode.gif	Yes	*	Super Utilities Pro	7.71	*	C:\My Programs\analyzer\Conf\html
ftv2link.gif	Yes		Super Utilities Pro	7.71	*	C:\My Programs\analyzer\Conf\html
ftv2lastnode.nif	Yes		Super Utilities Pro	7.71	*	C:\My Programs\analyzer\Conf\html

Files Scanned: 4120 Maximum File Scan Size: 51.85 MB

© 2000-2009, Gary C. Kessler 48

Gargoyle Investigator™ - Detected Program List

Password Crack

- PGPCrack - 0.6
- PGPCrack - .99b
- PGPPass - N/A
- PKCrack - N/A
- WinCrack - N/A
- Glide - N/A
- EXcrak - 1.0
- EUDPASS - 1.0

Steganography Programs

- S-Tools - 4.00
- Steganos II Security Suite - Installer - 2.0
- mod-stego Source Code - 1.4
- MP3Stego Source Code - 1.0.14b1
- JP Hide&Seek - 0.5
- show - 1.1 (32bit)
- Stash-It - 1.1.0.2
- Stegdetect - 0.2x

File Name	Risk	Found
SNOW.EXE	■■■■■■■■	Yes
SNOW.DOC	■■■■■■■■	No

Confidence: ■■■■■■

Version: 1.1 (32bit)
 Manufacturer: Matthew Kwan
 Category: NA
 Origin: NA
 Release Date: 1998
 Interface: Command Line
 Files Detected: 1 Total Files: 2
 Operating System: NA
 Home Page: NA
 Description: Program encrypts using the ICE algorithm and conceals a message in a text file. User can uncover and decrypt later.

Suspected File Types for All Found Steganography Programs:

GIF BMP JPEG TIFF PNG MP3 WAV Text

Close

© 2000-2009, Gary C. Kessler 49

Stego Hunter

The screenshot shows the Stego Hunter application window. On the left, there is a 'Select Scan Locations' tree view showing 'Local Disk (C:)' and 'My Programs' folders, with 'stego' selected. Below it is a 'Target Location' field set to 'C:\My Programs\stego'. The main area is a table with the following columns: File Name, Detected, File Name Differs, From Products, and Path. The table lists 16 files, including 'jphswin.exe', 'SNOW.EXE', 'Stash.exe', 'stegowav.exe', '2Mosaic.exe', 'GiftUp.exe', 'ReadMe.txt', '_DEISREG.ISR', 'GIFutil.dll', 'S-Tools.exe', 'S-Tools.hlp', 'GhostHost.exe', 'ilsupp.dat', 'wbs43de.hlp', 'wbs43en.hlp', 'wbStego4.3open.exe', 'cgvwin1.dll', and 'nrk-1.3.rll'. Each file is marked as 'Detected' and 'True'. The 'From Products' column lists various steganography products like 'JP Hide&Seek 0.5', 'snow 1.1 (32bit)', 'StashIt 1.1.0.2', 'Stego WAV 1.01', '2Mosaic 0.2.2', 'Gift Up 1.0, Giftup 1.0', 'S-Tools 4.00', 'wbStego4open Source Code 4.3, wbStego4open 4.3', and 'Stegdetect 0.4, stegdetect 0.4'. At the bottom, there is a 'Scan Status' section showing 'Directories: 25', 'Files: 608', and 'Products Found: 16'. A 'Carrier Types Found' section has checkboxes for GIF, BMP, JPEG, TIFF, PNG, MP3, WAV, and Text, all of which are checked. A 'Start Hunting' button is visible on the right.

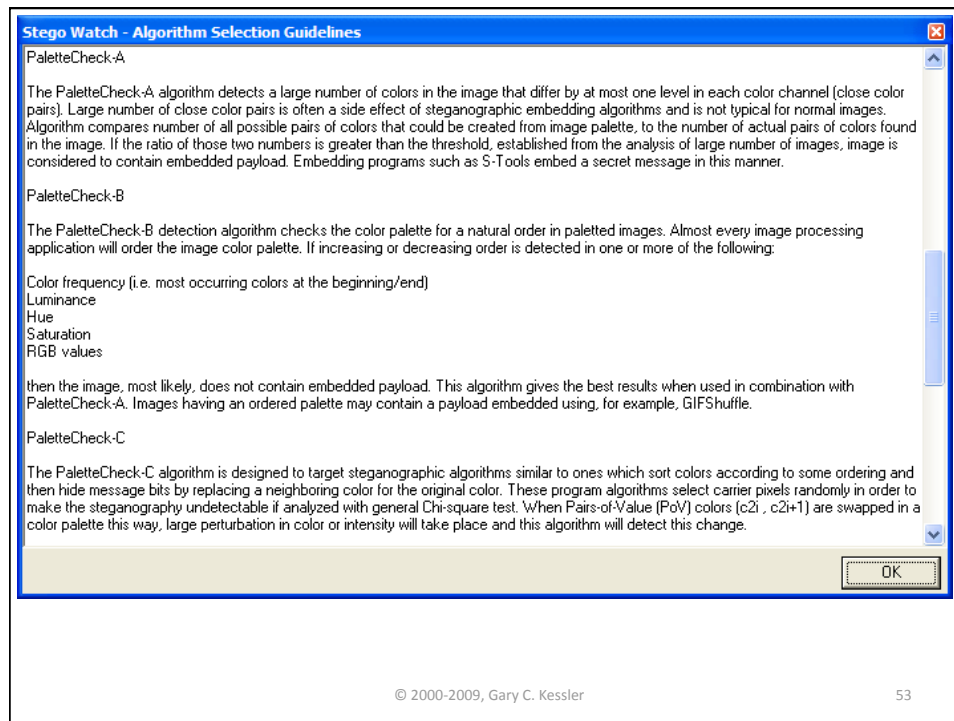
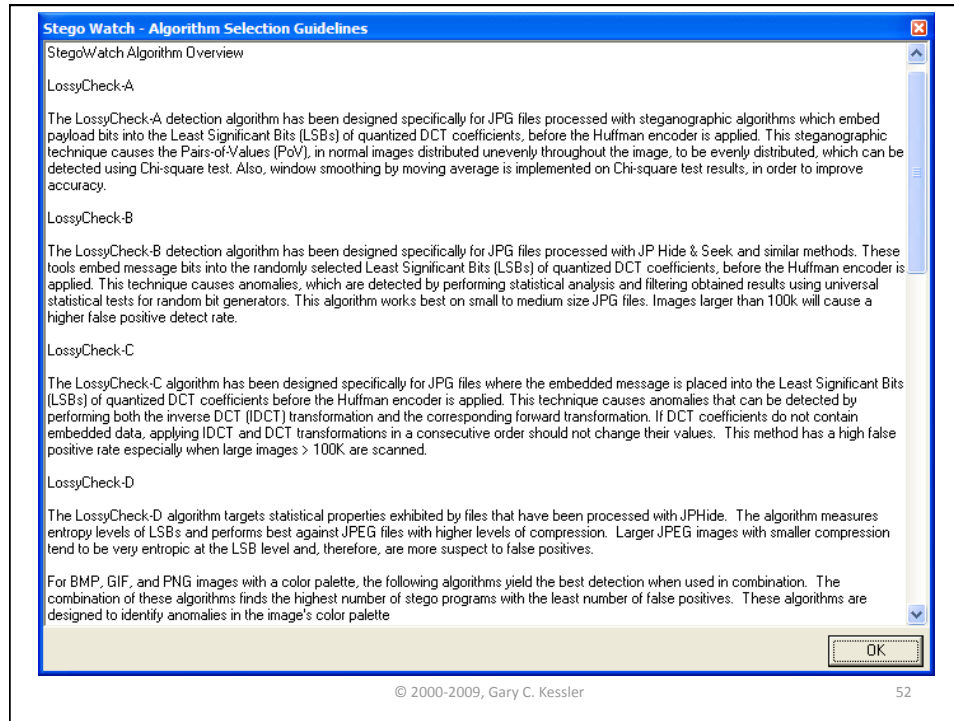
File Name	Detected	File Name Differs	From Products	Path
jphswin.exe	True	False	JP Hide&Seek 0.5	C:\My Programs\stego\
SNOW.EXE	True	False	snow 1.1 (32bit)	C:\My Programs\stego\
Stash.exe	True	False	StashIt 1.1.0.2	C:\My Programs\stego\
stegowav.exe	True	False	Stego WAV 1.01	C:\My Programs\stego\
2Mosaic.exe	True	False	2Mosaic 0.2.2	C:\My Programs\stego\exam
GiftUp.exe	True	False	Gift Up 1.0, Giftup 1.0	C:\My Programs\stego\giftu
ReadMe.txt	True	False	Gift Up 1.0, Giftup 1.0	C:\My Programs\stego\giftu
_DEISREG.ISR	True	False	Gift Up 1.0, Giftup 1.0	C:\My Programs\stego\giftu
GIFutil.dll	True	False	S-Tools 4.00	C:\My Programs\stego\S-To
S-Tools.exe	True	False	S-Tools 4.00	C:\My Programs\stego\S-To
S-Tools.hlp	True	False	S-Tools 4.00	C:\My Programs\stego\S-To
GhostHost.exe	True	False	GhostHost 1.0	C:\My Programs\stego\Samj
ilsupp.dat	True	False	wbStego4open Source Code 4.3, wbStego4open 4.3	C:\My Programs\stego\Samj
wbs43de.hlp	True	False	wbStego4open Source Code 4.3, wbStego4open 4.3	C:\My Programs\stego\Samj
wbs43en.hlp	True	False	wbStego4open Source Code 4.3, wbStego4open 4.3	C:\My Programs\stego\Samj
wbStego4.3open.exe	True	False	wbStego4open 4.3	C:\My Programs\stego\Samj
cgvwin1.dll	True	False	Stegdetect 0.4, stegdetect 0.4	C:\My Programs\stego\steg
nrk-1.3.rll	True	False	Stendetect 0.4, Stendetect 0.4, stendetect 0.4	C:\My Programs\stego\stend

Stego Watch

Session setup for examining files on a local drive

The screenshot shows the 'Stego Watch - Session Options' dialog box. It has three tabs: 'Algorithms', 'Disk Session', and 'Filters'. The 'Algorithms' tab is active, showing a list of steganography detection algorithms with checkboxes. The 'Disk Session' tab is also visible, showing 'Suspect Files' with a 'Source Folder' set to 'C:\My Programs\stego' and a 'Report Location' set to 'C:\My Programs\stego\reports'. The 'Generate Quick Reports' and 'Preview Reports' options are checked. At the bottom, there are 'OK' and 'Cancel' buttons.

Algorithm	JPEG	Palleted	True Color BMP	WAV	MP3
<input checked="" type="checkbox"/> LossyCheck-A	X				
<input checked="" type="checkbox"/> LossyCheck-B	X				
<input checked="" type="checkbox"/> LossyCheck-C	X				
<input checked="" type="checkbox"/> LossyCheck-D	X				
<input checked="" type="checkbox"/> PaletteCheck-A					
<input checked="" type="checkbox"/> PaletteCheck-B					
<input checked="" type="checkbox"/> PaletteCheck-C					
<input checked="" type="checkbox"/> PaletteCheck-D					
<input checked="" type="checkbox"/> Signatures	X				
<input checked="" type="checkbox"/> TrueColorCheck-A					
<input checked="" type="checkbox"/> WAVCheck-A					



Stego Watch - Algorithm Selection Guidelines

PaletteCheck-D

The PaletteCheck-D detection algorithm has been designed to detect the presence of an embedded payload using techniques in which one can identify Pairs-of-Value (PoV) colors whether or not the payload has been randomly scattered over the entire image. Embedding payload this way will decrease the difference between the frequencies of PoV but the difference between the complementary pairs of colors (c2i-1 , c2i) will not be affected. PaletteCheck-D is recommended for images modified by EZ Stego with random scatter, and for grayscale images.

Signatures

The Signature library is a collection of non-statistical detection checks that are designed to identify known signatures and anomalies that steganographic programs can leave behind. These checks include finding information appended to the end of a file or data in the comment field of an image. Signature-based detection can be very definitive indicators for the presence of Steganography.

TrueColorCheck-A

The TrueColorCheck-A detection algorithm works by encoding a random payload into a copy of an image. If the image already contains hidden data, embedding another message does not significantly affect the total number of colors or PoVs as compared to the original suspect image.

WAVCheck-A

The WAVCheck-A algorithm (currently the only available Stego Watch algorithm for the detection of steganography in digital audio files) analyzes silent areas in WAV files for randomness. This algorithm will check files using universal statistical tests for random bit generators.

OK

© 2000-2009, Gary C. Kessler 54

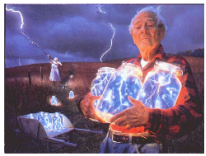
Stego Watch

File: View Session File Options Tools Help

Current Session

- ind.mp3 [OK]
- lightening_jars.jpg [H]
- lightening_jars_btv.jpg [H]
- lightening_jars_wd.jpg [H]
- mall_at_night.gif [H]
- mall_at_night_btv2.gif [H A]
- mall_at_night_wd2.gif [H A]
- map_bhcc.gif [H A]
- SOUND.gif [OK]
- wizard.bmp [H]
- wizard_wav.bmp [H]
- xsteg_shot.gif [H]
- 339008.jpg [OK]
- 339009.jpg [L]
- 339010.jpg [OK]
- 339011.jpg [H]
- 348024.jpg [L]
- phoenix.jpg [H]
- Picture 2 copy.jpg [H]
- Picture 3.png [H]
- Picture.jpg [H]
- DSCN0663.JPG [L]

File: lightening_jars_btv.jpg



Details

Location: C:\My Programs\stego\examples
 Size: 207276 Bytes
 Max Payload: 26397 Bytes
 Created: 6/15/2006 13:42:19
 Modified: 11/9/2003 19:19:40

Steganography Detection Algorithms

Algorithm	Probability	Result
LossyCheck-D	High	Steganography is possible
LossyCheck-B	High	Steganography is possible
Signatures	No Stego	Steganography not detected

Comments

LossyCheck-B and -D tests highly suggestive of the JPHide algorithm

© 2000-2009, Gary C. Kessler 55

File Details :	
File :	mall_at_night_bt2.gif
File Origin :	C:\My Programs\stegolexamples
Disk Location :	C:\My Programs\stegolexamples
File Size :	677733 Bytes
Content Size :	1600 x 1032 Pixels
Date Created :	6/15/2006 13:42:19
Last Modified :	12/24/2003 20:25:34
Compression :	LZ
Bit Count :	8
Used Colors :	256
Colors :	256
Hash :	2E868E7586033B65E69F4C54B508EEF3FF128792

Stego Analysis Details :	
Stego Detection Level :	H A
Analysis Date :	10/08/2007 13:32:56
Detection Status :	Quick
Maximum Possible Payload :	206400 Bytes

Comments :	
Close Colors - Close colors found	

Report generated by Stego Watch from WeiStone Technologies, Inc. on 10/08/2007 13:38:02

Algorithm :	Results :
LossyCheck-A	Invalid File for Algorithm
LossyCheck-B	Invalid File for Algorithm
LossyCheck-C	Invalid File for Algorithm
LossyCheck-D	Invalid File for Algorithm
PaletteCheck-A	Steganography not detected
PaletteCheck-B	Steganography is possible
PaletteCheck-C	Steganography not detected
PaletteCheck-D	Steganography not detected
Signatures	Steganography not detected
TrueColorCheck-A	Invalid File for Algorithm

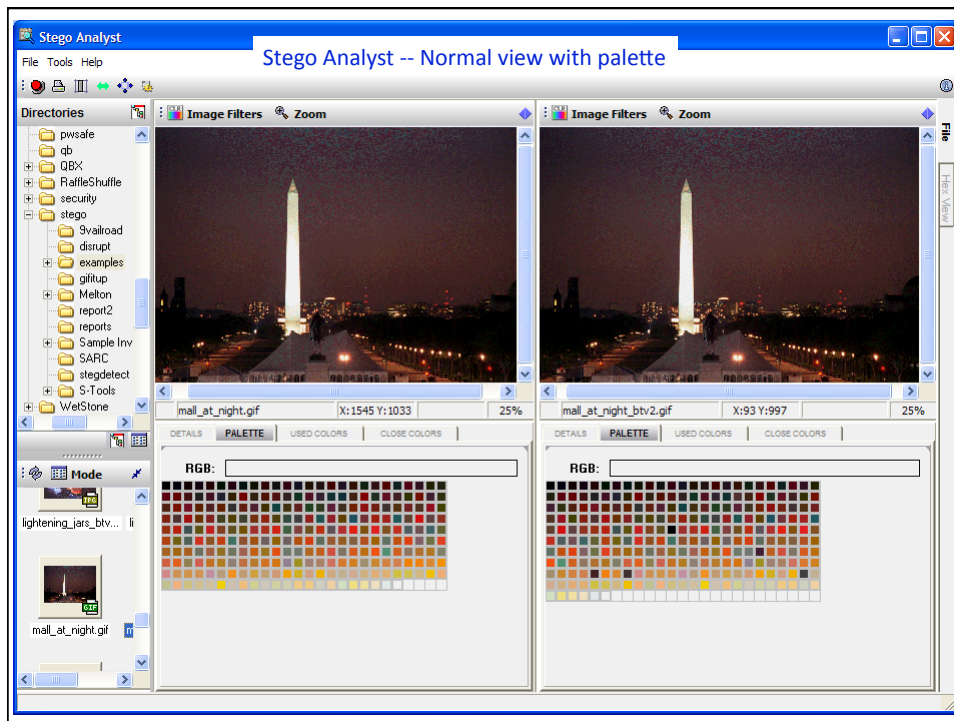
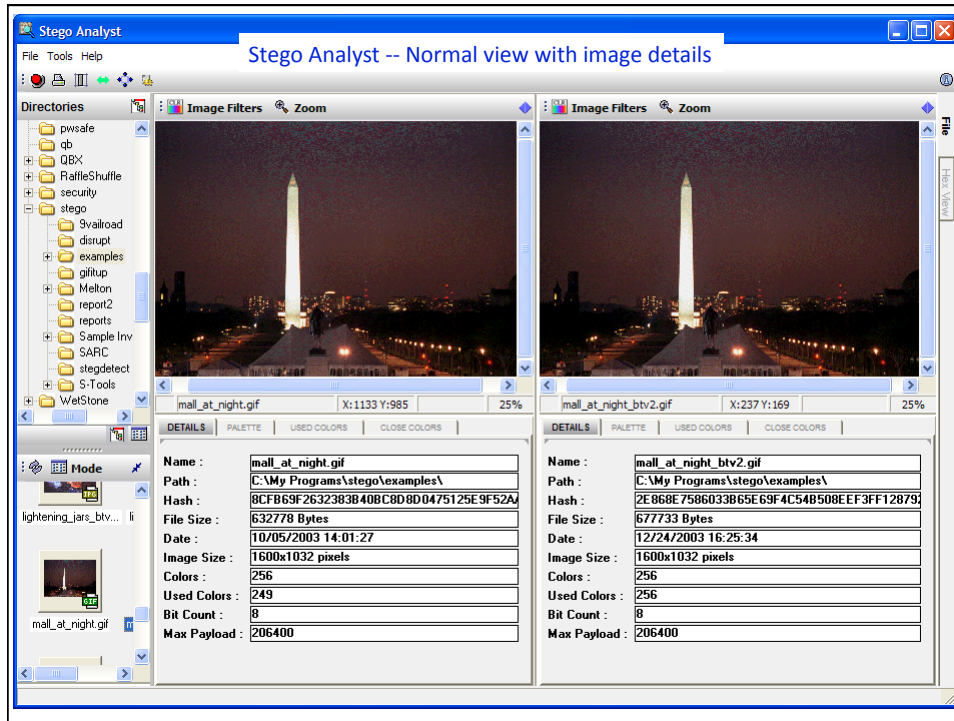
LossyCheck tests not applicable to JPEG files

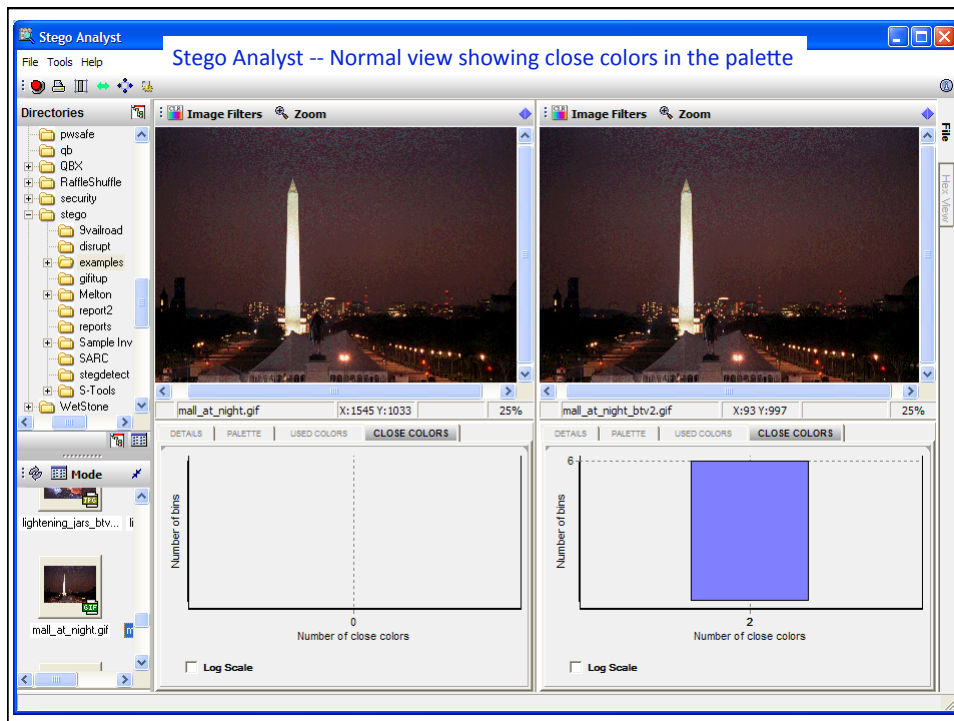
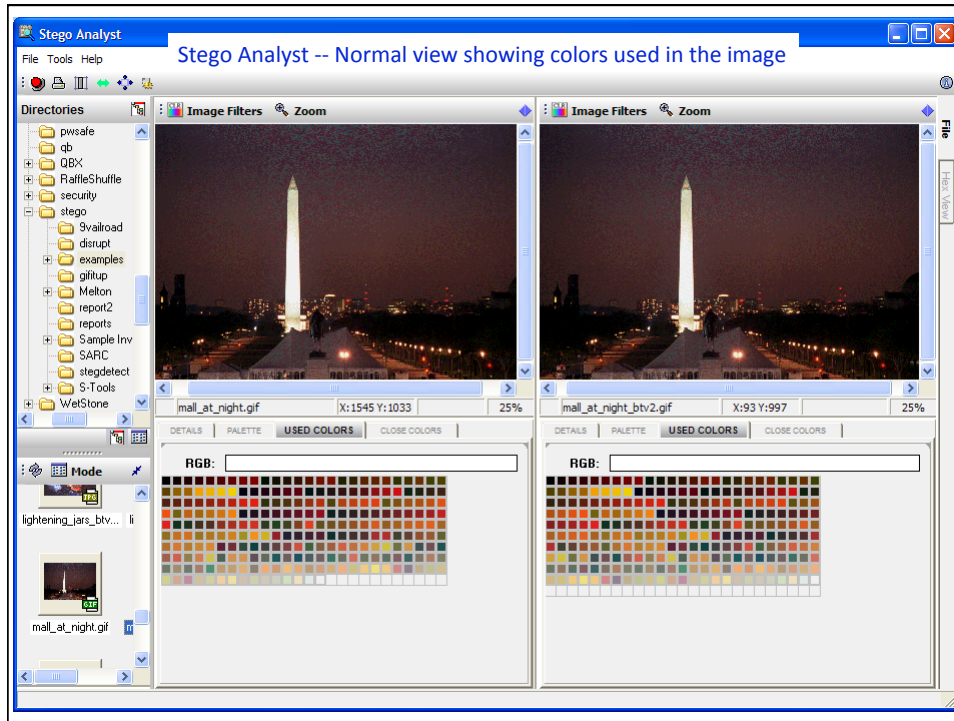
Palette check tests appropriate for GIF files

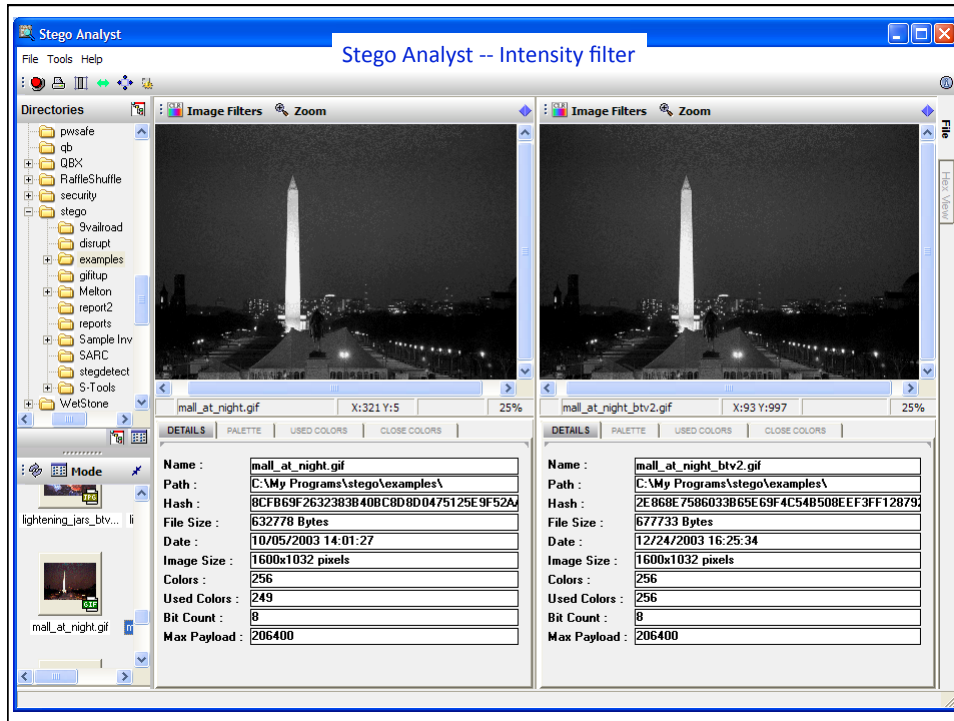
© 2000-2009, Gary C. Kessler 56

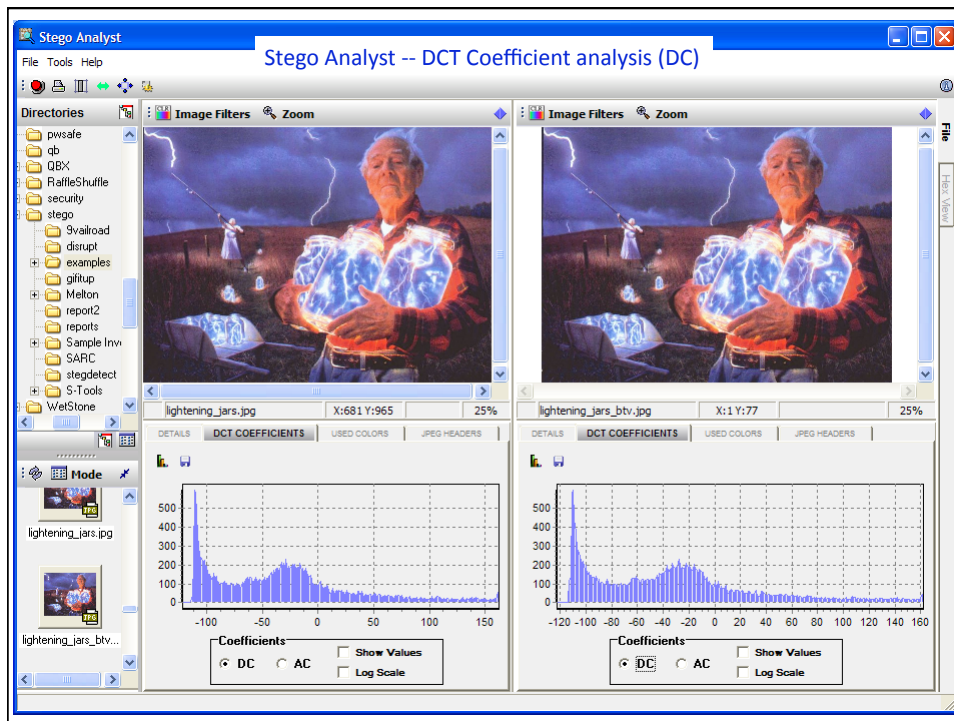
Hue, Intensity, and Saturation

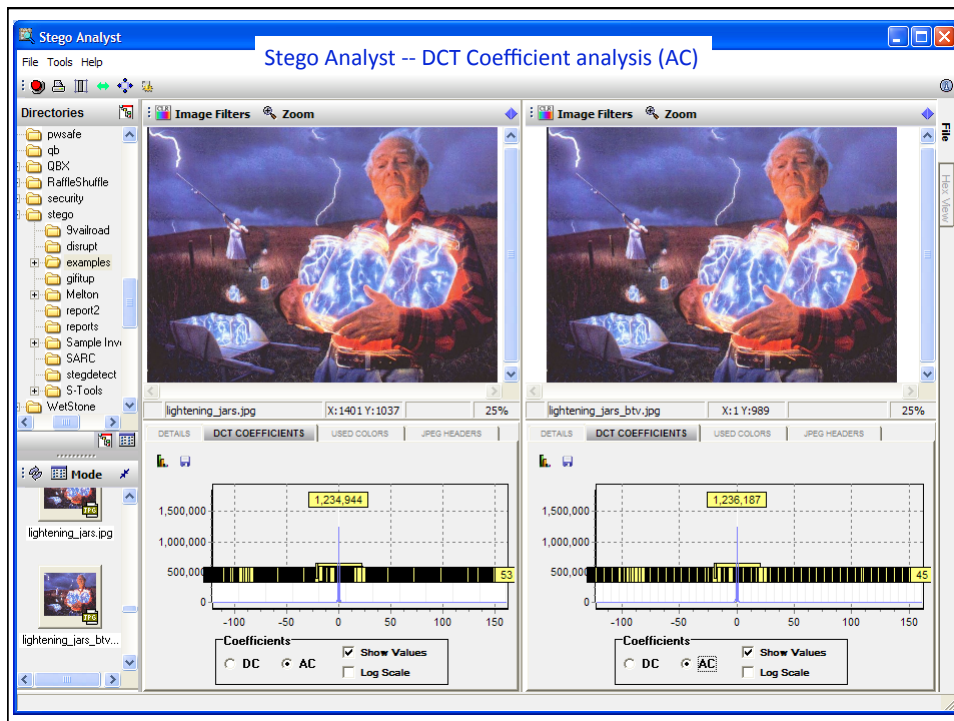
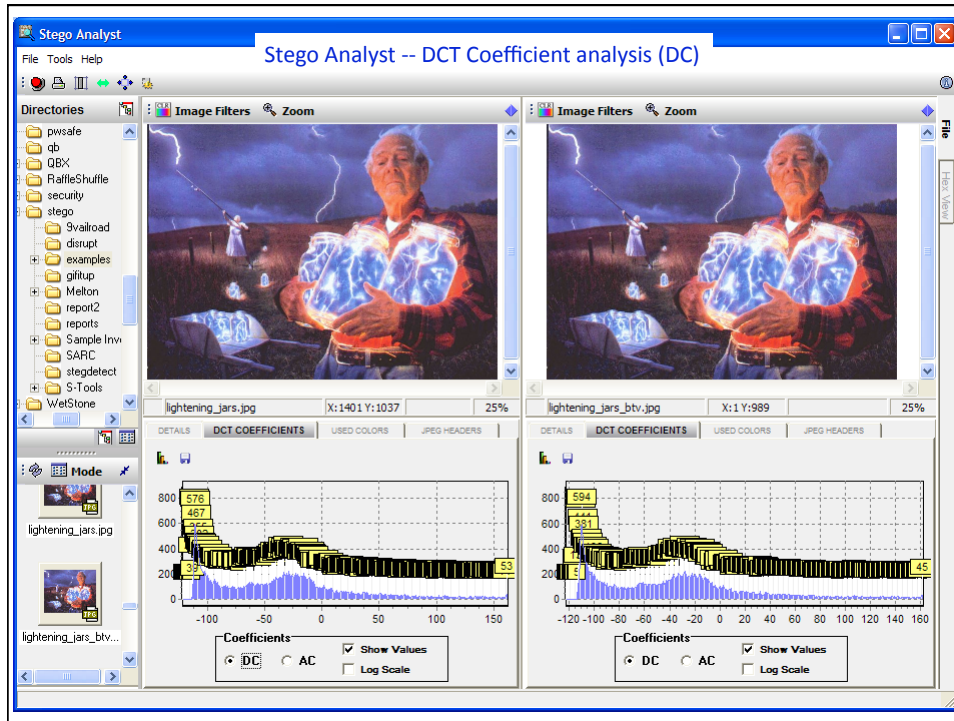
© 2000-2009, Gary C. Kessler 57











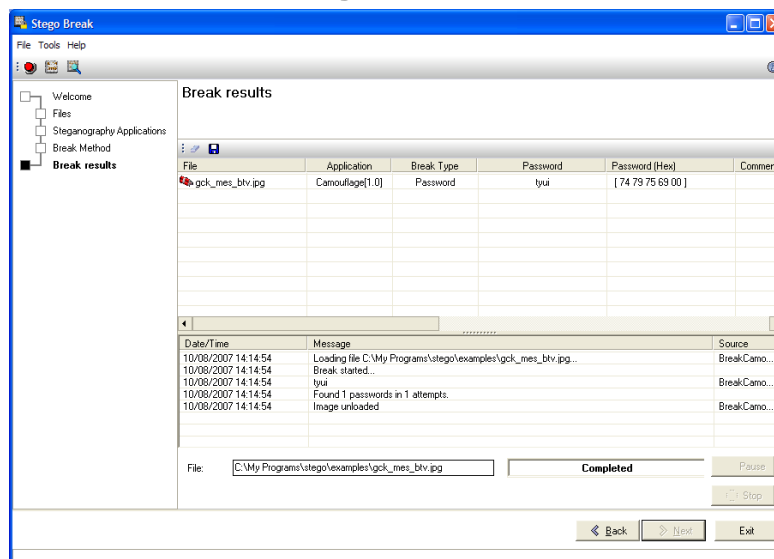
But We're Not Done Yet...

- So now what?
 - We've identified possible stego software and carrier files with hidden data
 - Without the password, we may still be out of luck....

© 2000-2009, Gary C. Kessler

68

Stego Break



© 2000-2009, Gary C. Kessler

69

Steganography Analysis and Research Center (SARC)

- Steganography Application Fingerprint Database (SAFDB)
 - Steganography and watermarking applications hashset
- Steganography Analyzer Artifact Scanner (StegAlyzerAS)
 - Scan media for the presence of steganography application artifacts
- Steganography Analyzer Signature Scanner (StegAlyzerSS)
 - Scan files for presence of hexadecimal byte patterns (signatures) of particular steganography applications

© 2000-2009, Gary C. Kessler

70

StegAlyzerAS - Scan Summary

The screenshot displays the StegAlyzerAS v3.1 application window. The interface includes a menu bar (Case Management, Report, Options, Help), a case file field (N/A), and a search scope selection pane on the left. The main area shows analysis tabs (Case Log, Evidence Log, Scan Summaries, Scan Options, Scan Progress) and a 'Scans' section with a dropdown menu. Below this is a 'Scan Statistics' table and a 'Scan Items' list.

Scan Statistics			
Unique File Artifacts Found:	38	Applications Detected:	11
Non-Unique File Artifacts Found:	3	Files Scanned:	613
SAFDB Entries:	11210	Directories Scanned:	25
Registry Artifacts Found:	0	File/Directory Exceptions:	0
RAKDB Entries:	555	0 Byte Files Found:	2
		Total Files in Scan Path:	613
		Time Begin:	14:44:09
		Time End:	14:44:16
		Time Elapsed:	0:0:7
		Canceled ?:	False

At the bottom of the window, the status shows 'Files: Ready' and 'Registry: Ready', with a 'Scan Complete' message at the very bottom.

© 2000-2009, Gary C. Kessler

71

StegAlyzerAS - Application Info

The screenshot shows the StegAlyzerAS v3.1 application window. The interface includes a menu bar (Case Management, Report, Options, Help), a Case File field (N/A), and a 'Select Search Scope' tree view on the left. The main area displays 'Analysis Tabs' with 'Scans' selected. A tree view shows detected applications, including 'S-Tools v4.00' which is expanded to show 'Detected File Artifacts' like cryptlib.dll, GIFutil.dll, S-Tools.exe, S-Tools.hlp, and zlib.dll. A summary box for 'S-Tools v4.00' provides statistics: 5/6 Total File Artifacts Detected, 4/5 Unique File Artifacts Detected, 1/1 False Positive/Common File Artifacts Detected, and no registry artifacts. At the bottom, there are status indicators for Files and Registry (both Ready) and a 'Scan Complete' message.

© 2000-2009, Gary C. Kessler

74

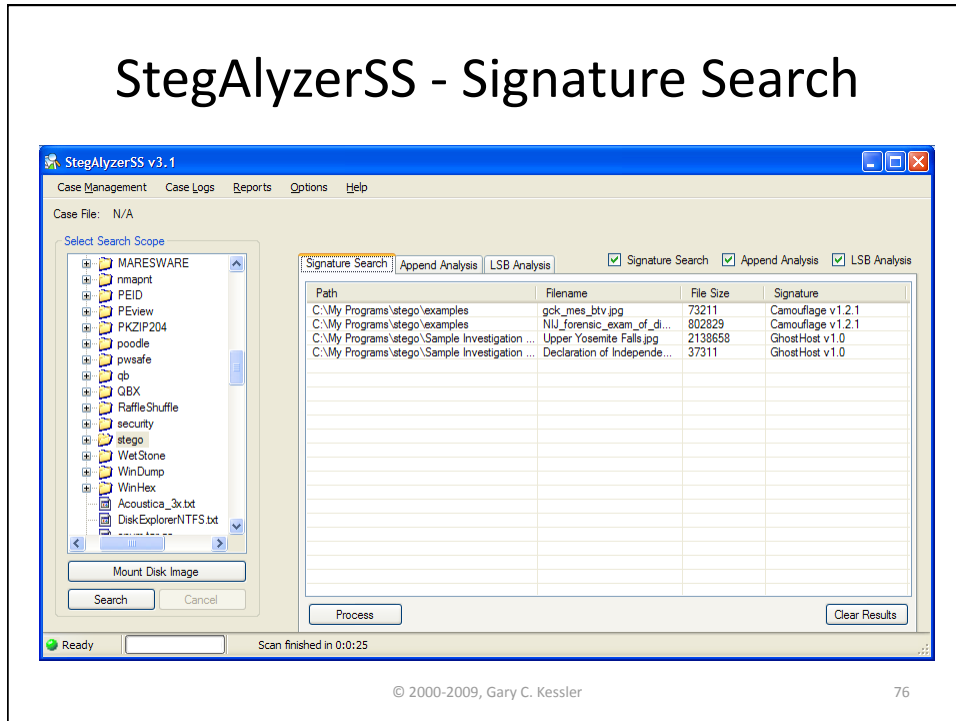
The screenshot shows the 'Evidence Log: S-Tools v4.00' window. It features a 'Statistics' section with a tree icon and a summary of file and registry artifacts. Below this is a table of 'Known File Artifacts' with columns for File, False Positive/Common, Status, Path, and Time Stamp. The table lists several files, including cryptlib.dll, GIFutil.dll, S-Tools.exe, S-Tools.hlp, and zlib.dll, with their respective detection status and paths. Below the table, there are sections for 'Known Registry Artifacts' (Message: An analysis of a registry was not performed during this scan.) and navigation buttons for '<< Previous' and 'Next >>'. The interface also displays various cryptographic hashes (CRC32, MD5, SHA1, SHA224, SHA256, SHA384, SHA512) and the file size (278774).

File	False Positive/Common	Status	Path	Time Stamp
cryptlib.dll	Unique	**FOUND**	Detected Under: C:\My Programs\stego\S-Tools\cryptlib.dll	05/19/2008 14:44:14
GIFutil.dll	Unique	**FOUND**	Detected Under: C:\My Programs\stego\S-Tools\GIFutil.dll	05/19/2008 14:44:14
S-Tools.exe	Unique	**FOUND**	Detected Under: C:\My Programs\stego\S-Tools\S-Tools.exe	05/19/2008 14:44:14
S-Tools.hlp	Unique	**FOUND**	Detected Under: C:\My Programs\stego\S-Tools\S-Tools.hlp	05/19/2008 14:44:14
zlib.dll	False Positive	**FOUND**	Detected Under: C:\My Programs\stego\S-Tools\zlib.dll	05/19/2008 14:44:14
S-Tools4.zip	Unique	NOT FOUND	FILE NOT FOUND	FILE NOT FOUND

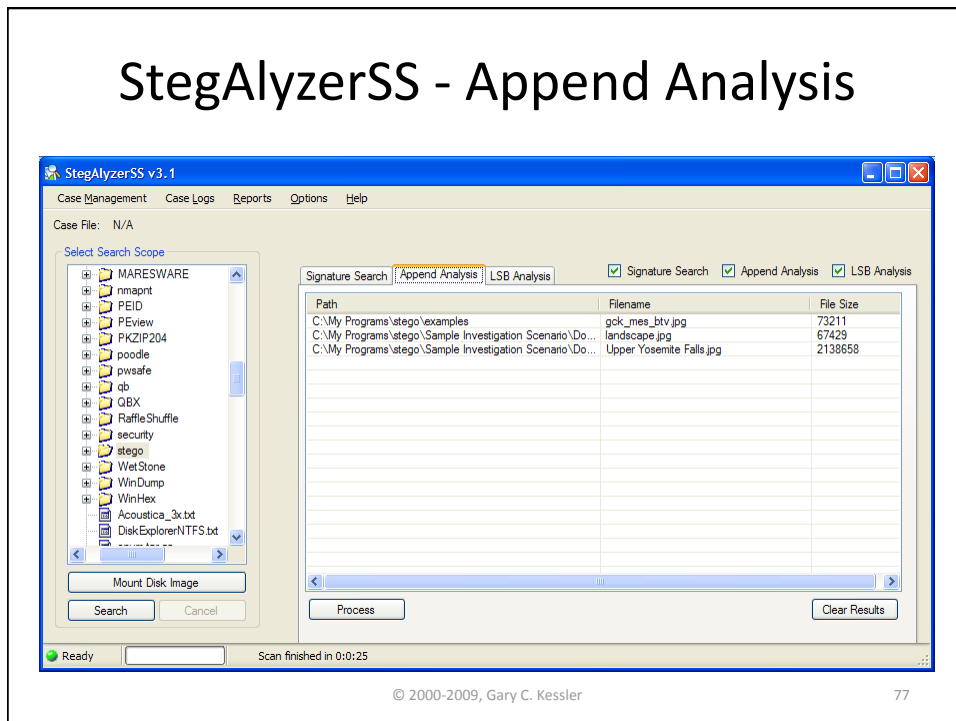
© 2000-2009, Gary C. Kessler

75

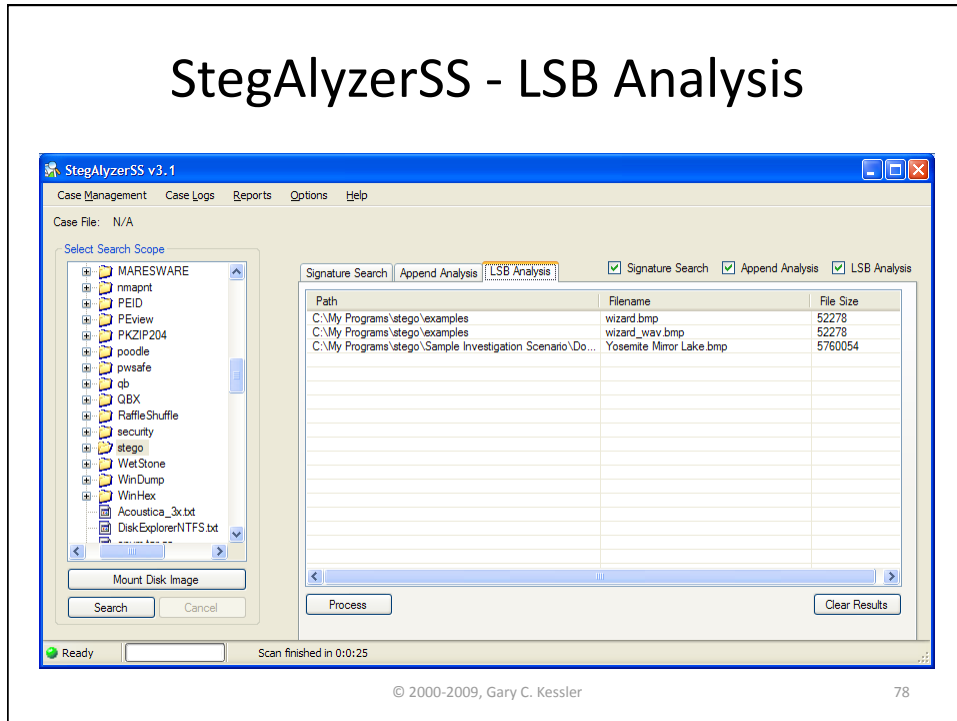
StegAlyzerSS - Signature Search



StegAlyzerSS - Append Analysis



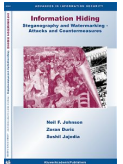
StegAlyzerSS - LSB Analysis



Some Final Words

- Use of steganography for nefarious purposes is very real!
 - Some examinations have found a large number of "suspicious" images at eBay and 2600.com
 - Terrorist organizations -- including Al Qaeda -- are known to use forms of stego
- Most law enforcement agencies don't believe that stego is being widely used -- yet!
 - But they don't know what they can't find
 - There are few standardized processes and few tools

Additional References



- *Techniques and Applications of Digital Watermarking and Content Protection*, Arnold, Schmucker, & Wolthusen
- *Information Hiding: Steganography and Watermarking - Attacks and Countermeasures*, Johnson, Duric, & Jajodia
- *Investigator's Guide to Steganography*, Kipper
- *Disappearing Cryptography*, 2/e, Wayne

- Neil Johnson's Steganography & Digital Watermarking page (<http://www.jjtc.com/Steganography/>)
- GCK's stego links (www.garykessler.net/library/securityurl.html#crypto)
- Stego Archive (<http://www.stegoarchive.com/>)

© 2000-2009, Gary C. Kessler

80

Downloads

- Software products
 - SARC (<http://www.sarc-wv.com/>)
 - WetStone Technologies (<http://www.wetstonetech.com>)
- Non-commercial stego software mirror at <http://msdim.champlain.edu/download/df/>
 - Camouflage (*Camou121.exe*)
 - Gif-It-Up (*Gif-it-up.exe*)
 - JPHS for Windows (*jphs_05.zip*)
 - S-Tools (*s-tools4.zip*)
 - Snow (*snowdos32.zip*)
 - Stegdetect (*stegdetect-0.4.zip*)
- All example GIF, JPEG, and WAV files can be downloaded at <http://msdim.champlain.edu/PD/fsc>
 - Use the password "tyui" to recover hidden information
- Presentation: <http://msdim.champlain.edu/PD/public>

© 2000-2009, Gary C. Kessler

81

Acronyms and Abbreviations

B	Byte
BMP	Bitmap image format
DCT	Discrete cosine transform
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
Hz	Hertz (cycles/second)
IM	Instant messaging
IRC	Internet Relay Chat
JPEG	Joint Photographic Experts Group
LSB	Least significant bit
OS	Operating system
PPT	PowerPoint
P2P	Peer-to-Peer
RAM	Random-access memory
WAV	Waveform audio

© 2000-2009, Gary C. Kessler

82

Author Contact Information

Gary C. Kessler, Ed.S., CCE, CISSP
 M.S. in Digital Investigation Management program
 Champlain College
 163 South Willard Street
 Burlington, VT 05401

office: +1 802-865-6460
 cell: +1 802-238-8913
 e-mail: gary.kessler@champlain.edu
 Skype: [gary.c.kessler](https://www.skype.com/user/gary.c.kessler)

<http://msdim.champlain.edu>
<http://c3di.champlain.edu>
<http://www.garykessler.net>



This work was partially supported by Grant No. 2006-DD-BX-0282 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United State Department of Justice.

© 2000-2009, Gary C. Kessler

83