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*
  - cover_medium + hidden_data + stego_key = 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"

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

4

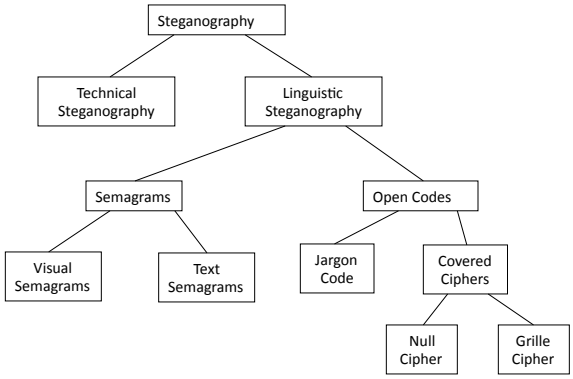
Is This Real?

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

5

A Taxonomy of Steganography



*

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...
    - $T_{DETECT} + T_{DECODE} > T_{CRITICAL}$

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.

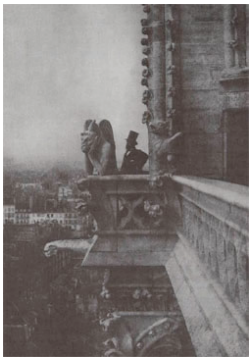
"Perhaps the mystery is a little too plain," said Dupin.

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

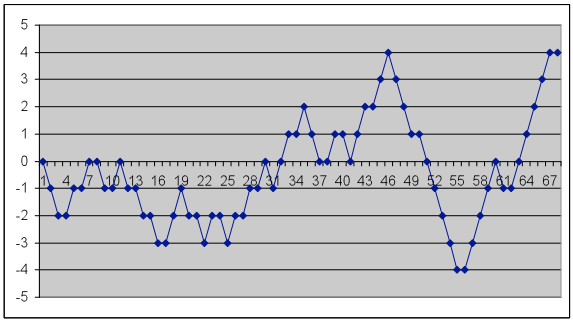
"A little too self-evident."

"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



A Side Issue

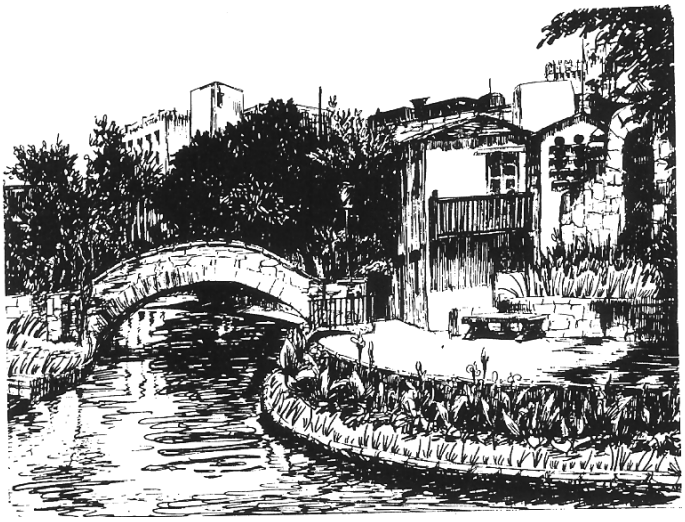


Accumulated heating degree-day units in Burlington, VT, 12/15/2005-2/21/2006... a bad winter for show shoeing

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

The San Antonio River



The Message in the Picture

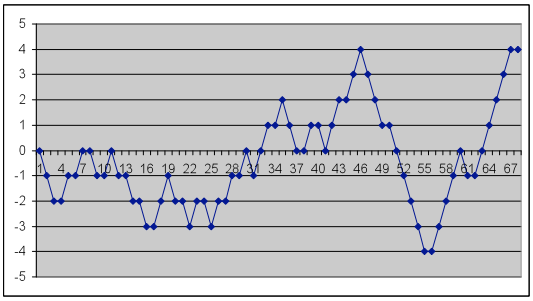
-.-. --- .-.. .... .- .-. --- .-.. -.. .-. ... .- .-- --- -- ....- .. ...

"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.)*

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.

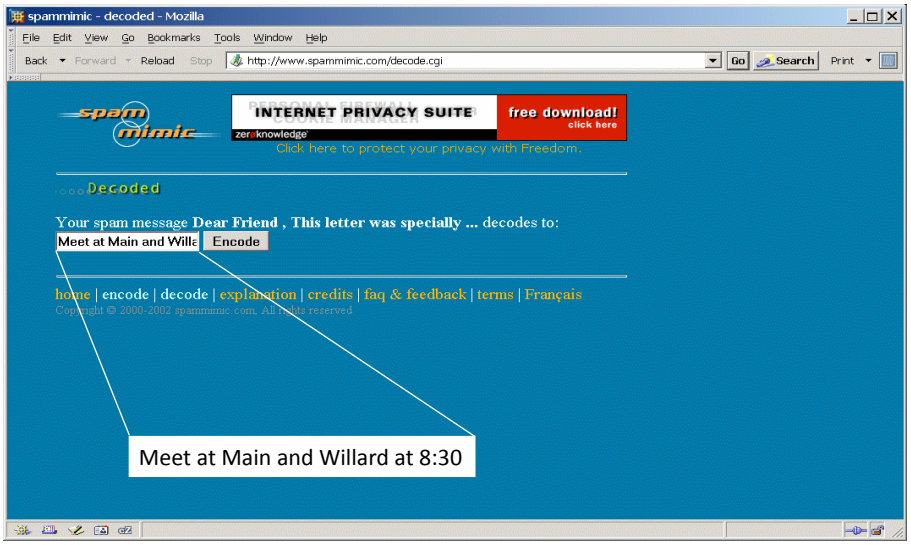
PERSHING SAILS FROM N.Y. JUNE 1

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 ligitimate 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 ligitimate 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)

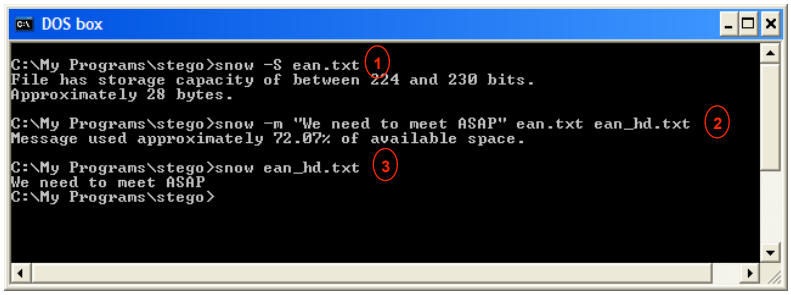
Dear Decision maker , This letter was specially selected to be sent to you ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 2416 ; Title 6 , Section 306 ! THIS IS NOT MULTI-LEVEL MARKETING . Why work for somebody else when you can become rich inside 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 .

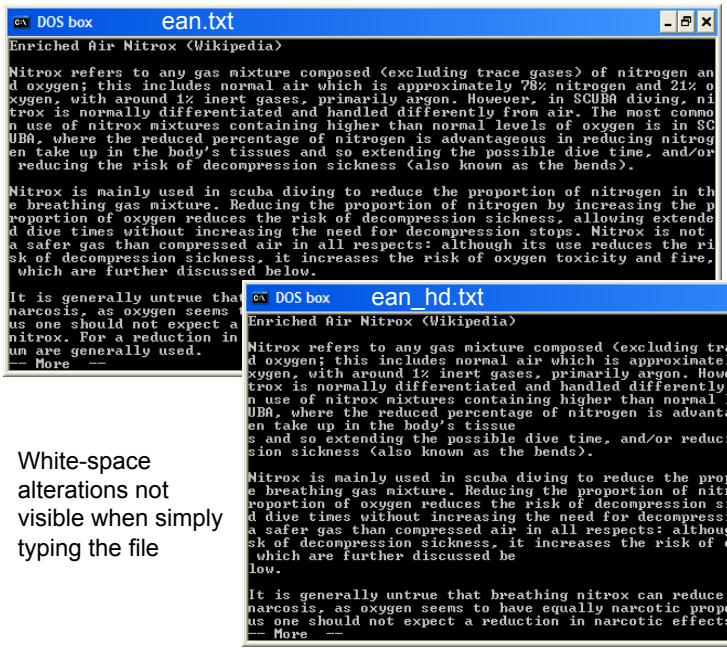
http://www.spammimic.com

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

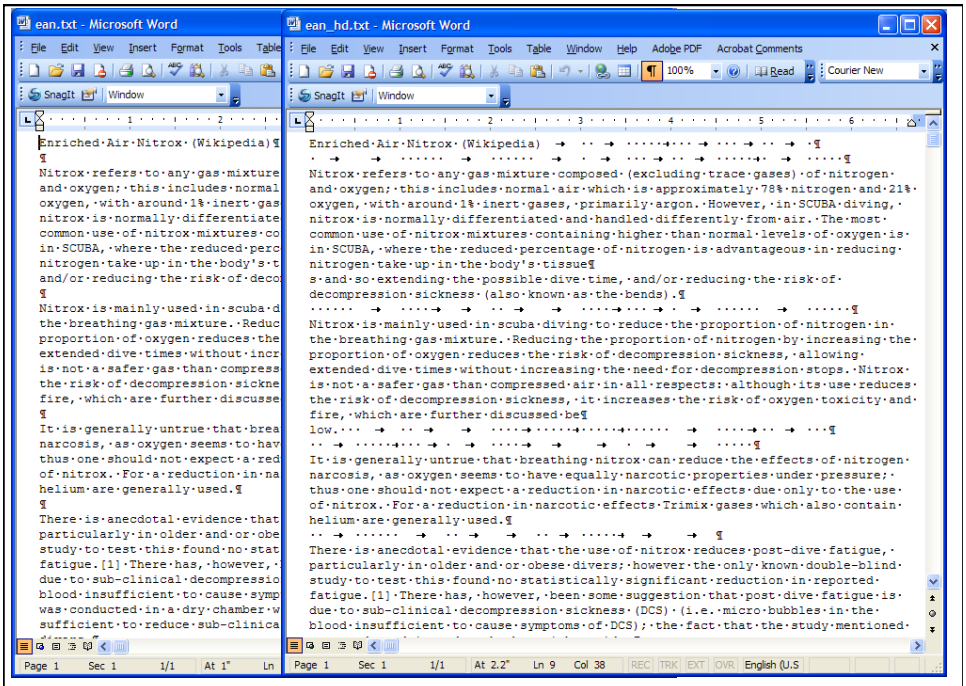
White-Space Stego

- 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





White-space alterations not visible when simply typing the file



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

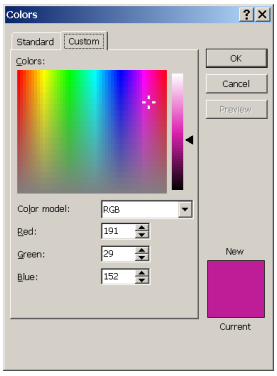
Inch, S. (2008, June). A simple image hiding technique: What you may be missing. *Journal of Digital Forensic Practice*, *2*(2), 83:94.

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/

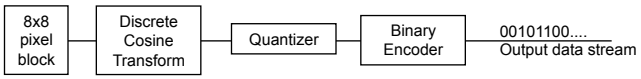
8-bit vs. 24-bit Color



- 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

JPEG

- JPEG saves DCT coefficients rather than pixel encoding

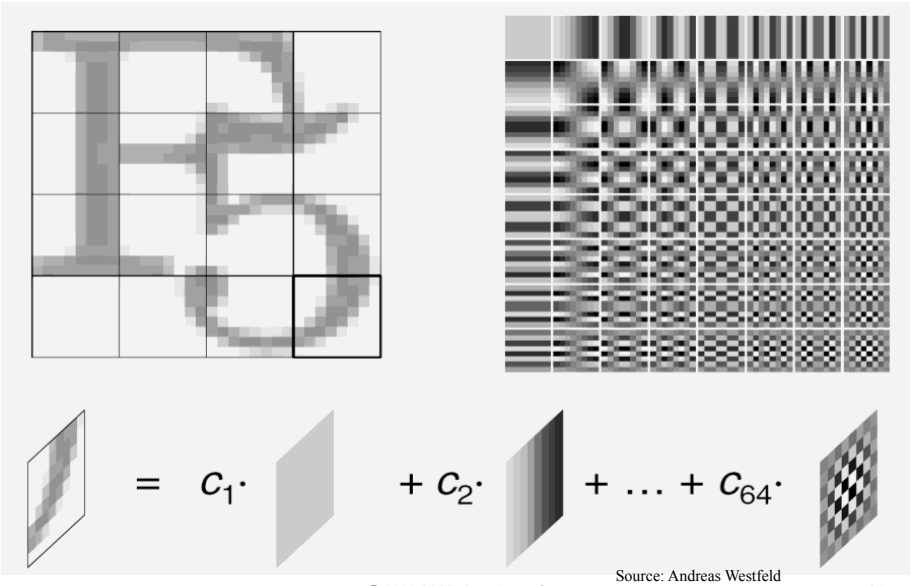


- DCT uses 8x8 pixel array (N_1=N_2=8), creates arrays of luminance (A) and chrominance (B)

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

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

JPEG Coefficients

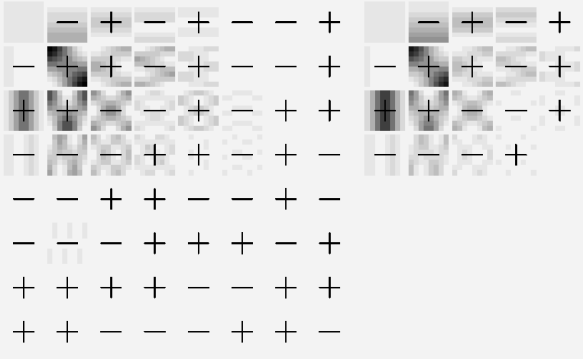


Source: Andreas Westfeld

Discrete Cosine Transformation

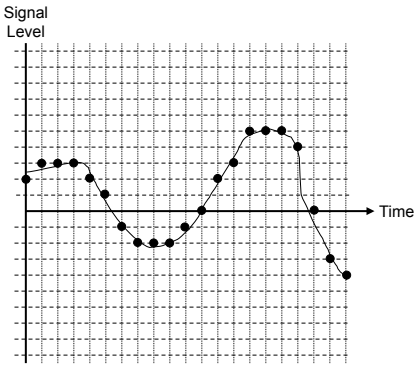
64 brightness values

➽ 19 nonzero JPEG coefficients



Source: Andreas Westfeld

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

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*0*   0000110*1*   1100100*0*
1001011*0*   0000111*0*   1100101*1*
1001111*1*   0001000*1*   11001011
```

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

Where Stego Works Best

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

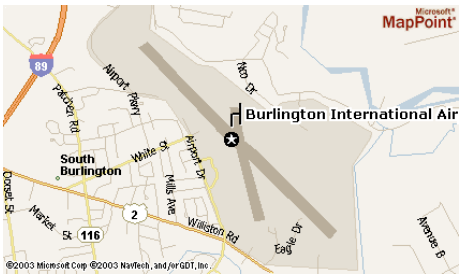
Steganography Methods and Tools

- 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

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

Examples



btv_map.gif [11,067 B]

Hide map in:

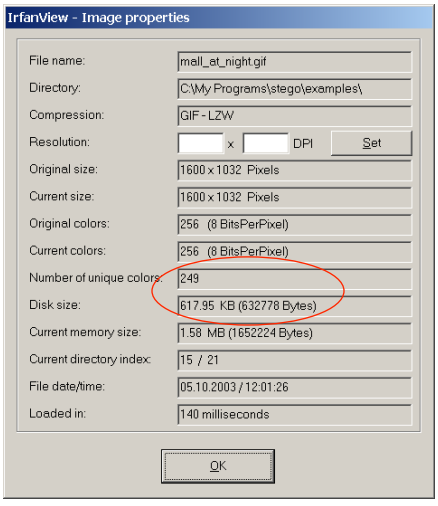
1. GIF file (Gif-It-Up)
2. JPEG file (JP Hide-&-Seek)
3. WAV file (S-Tools)
4. JPEG file (Camouflage)

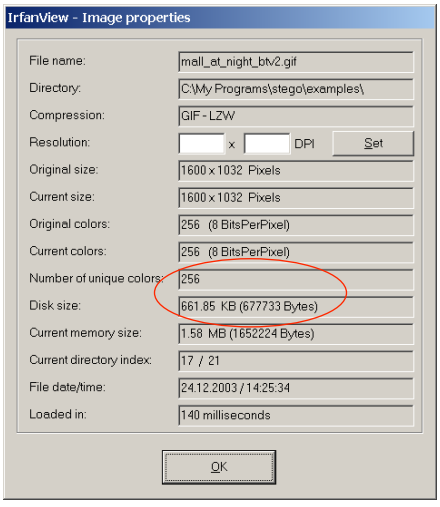
Example 1 - GIF File (Gif-It-Up)

mall_at_night.gif

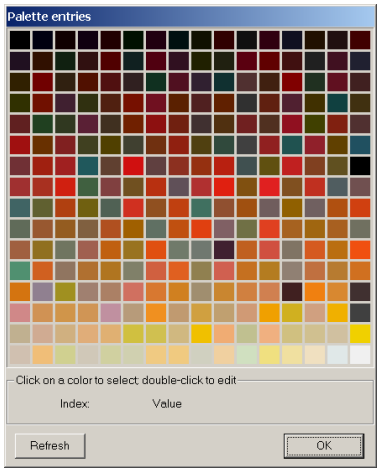
mall_at_night_btv2.gif

Example 1 - GIF File Properties





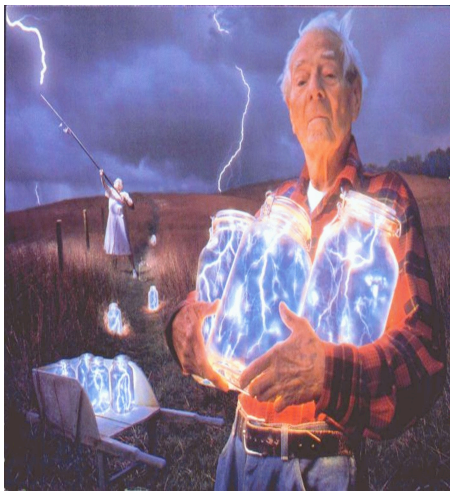
Example 1 - GIF File Palettes



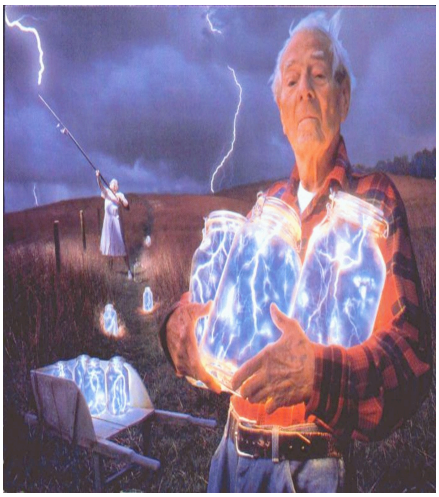
mall_at_night.gif

mall_at_night_btv2.gif

Example 2 - JPEG File (JPHS)

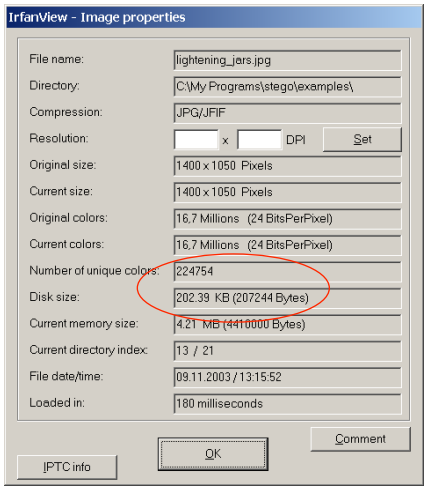


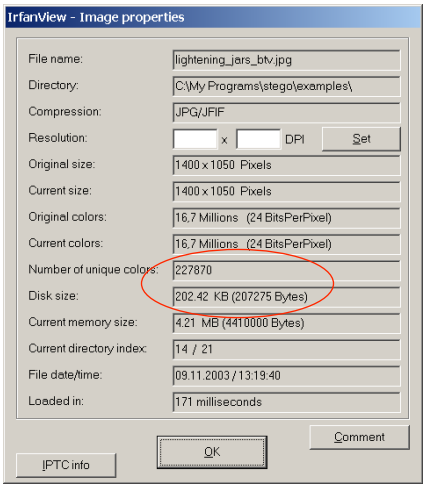
lightening_jars.jpg



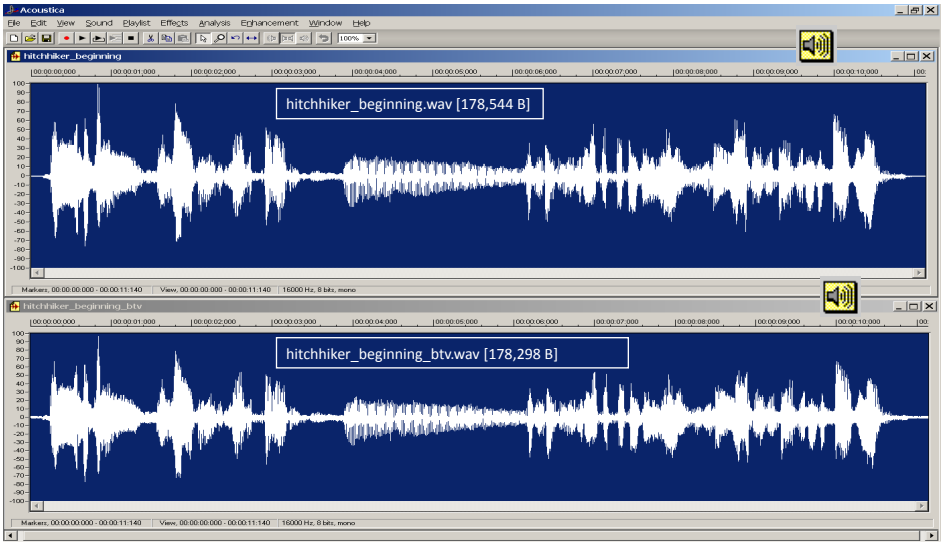
lightening_jars_btv.jpg

Example 2 - JPEG File Properties

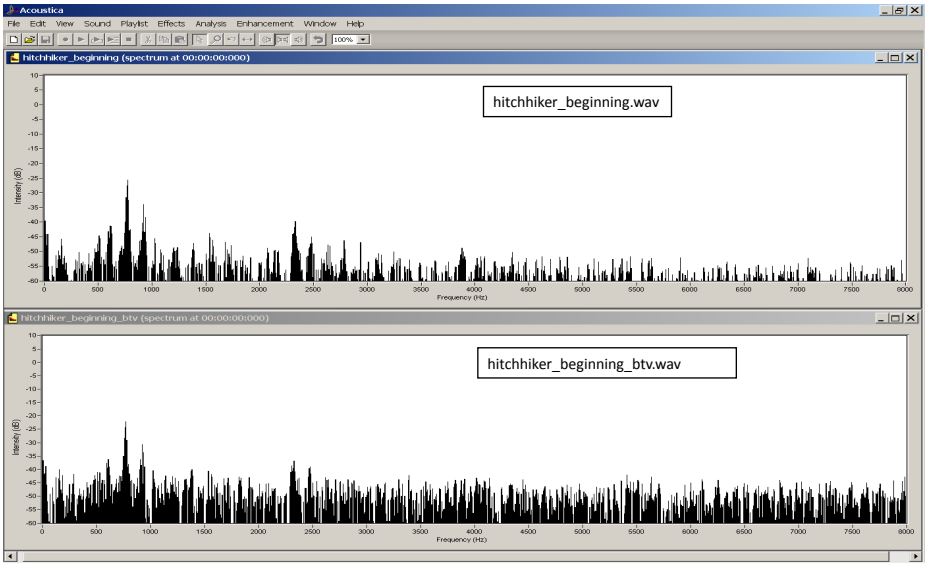




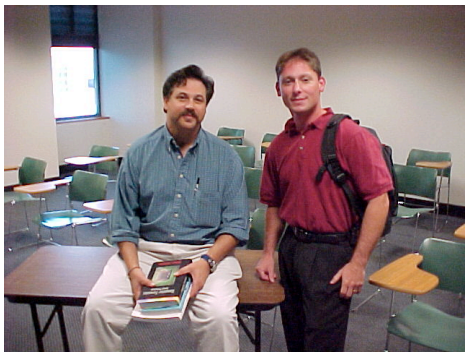
Example 3 - WAV File (S-Tools)



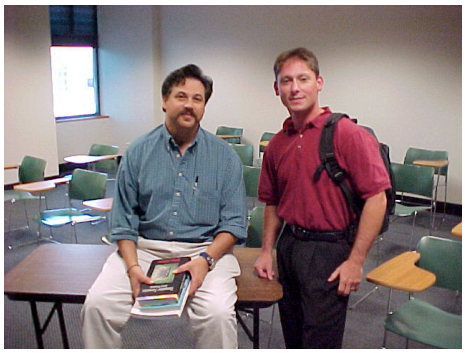
Example 3 - WAV Spectrum Analysis



Example 4 - JPEG File (Camouflage)

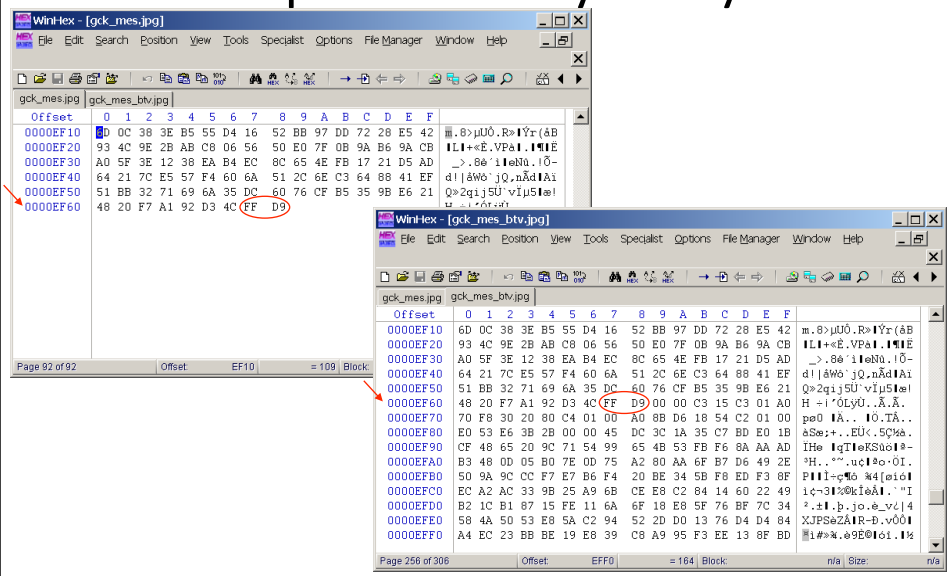


gck_mes.jpg
61,289 B



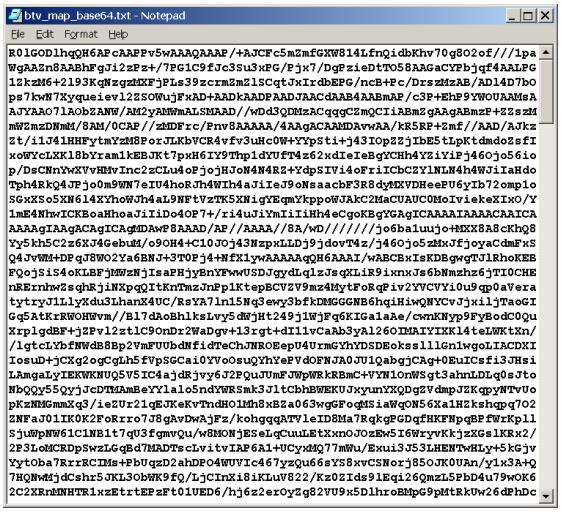
gck_mes_btv.jpg
73,211 B

Example 4 - Binary Analysis



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

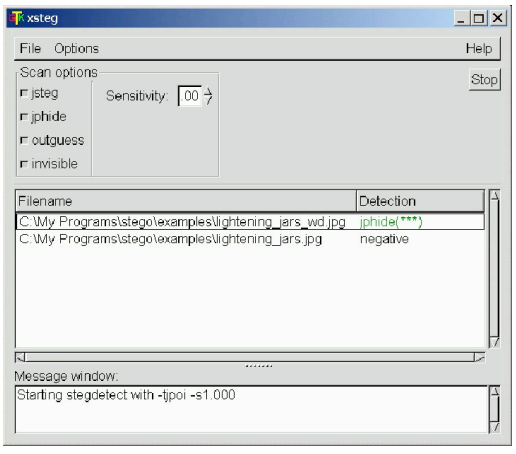


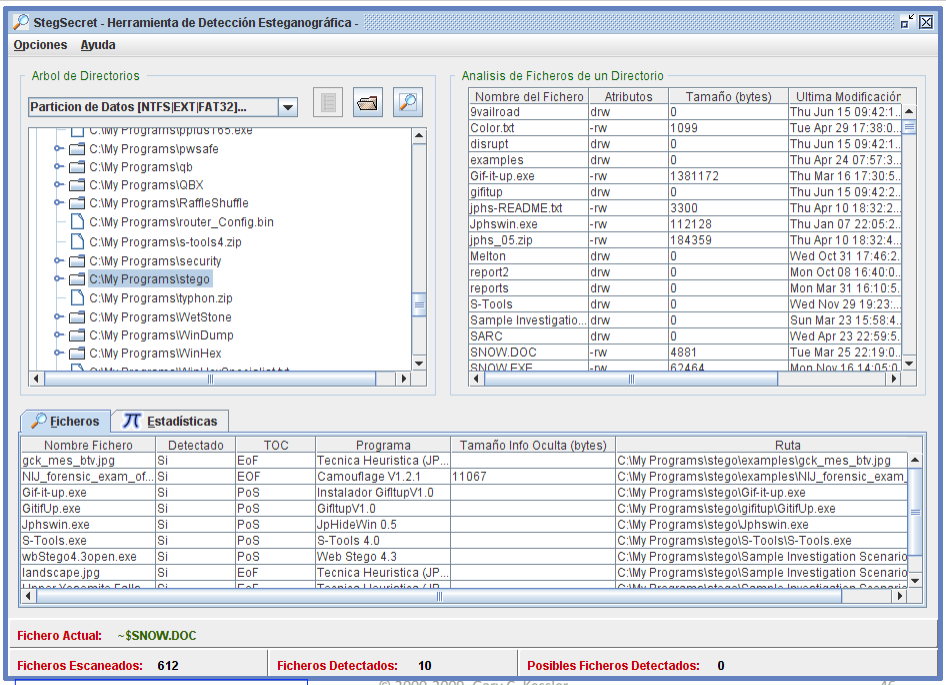
Steganalysis

- 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

stegdetect

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

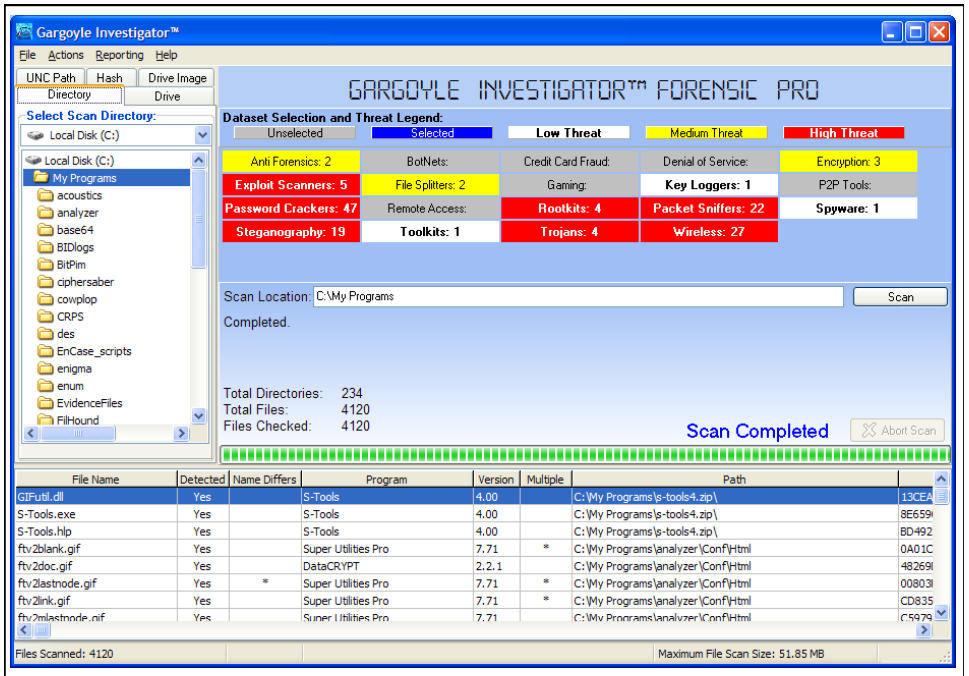




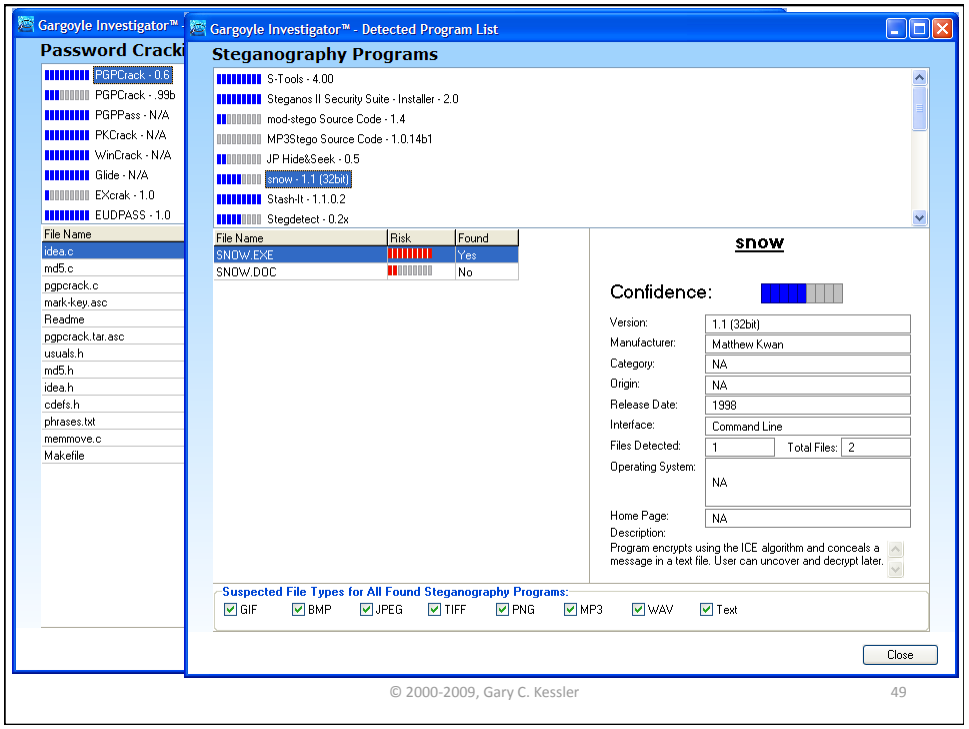
http://stegsecret.sourceforge.net/

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

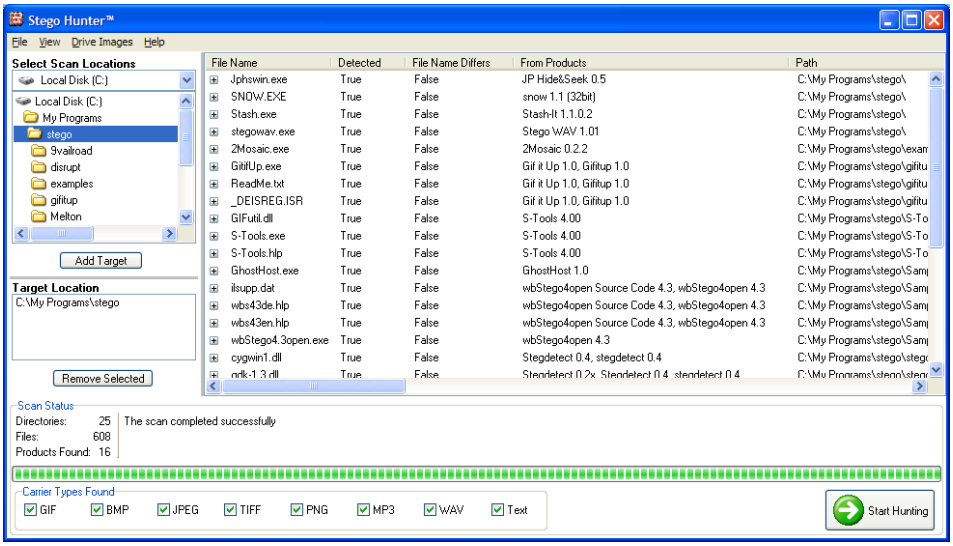


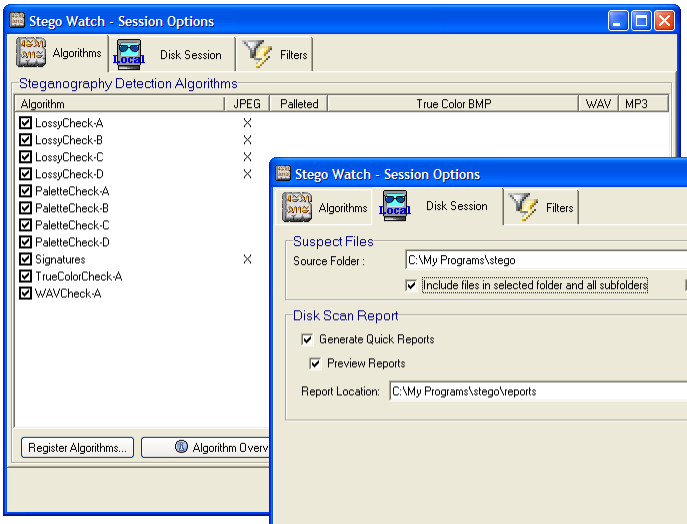
 48

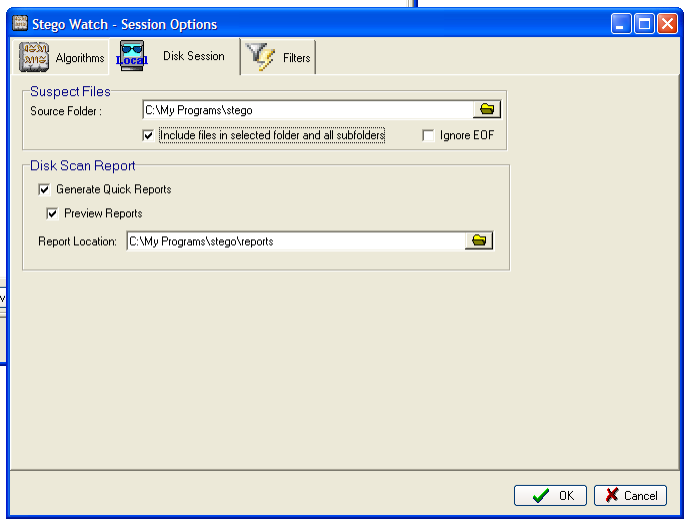


 49

Stego Hunter

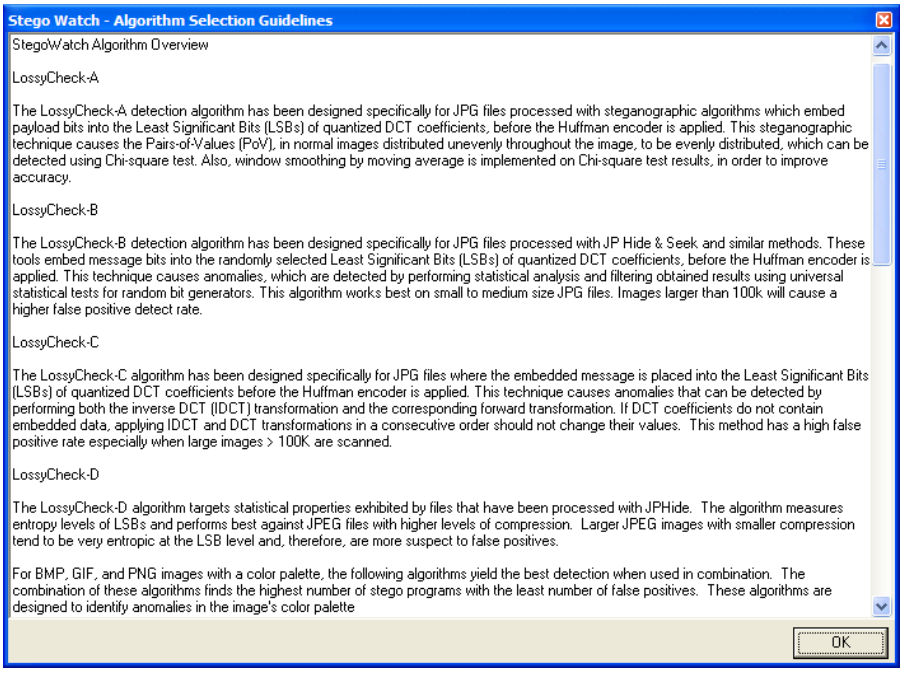




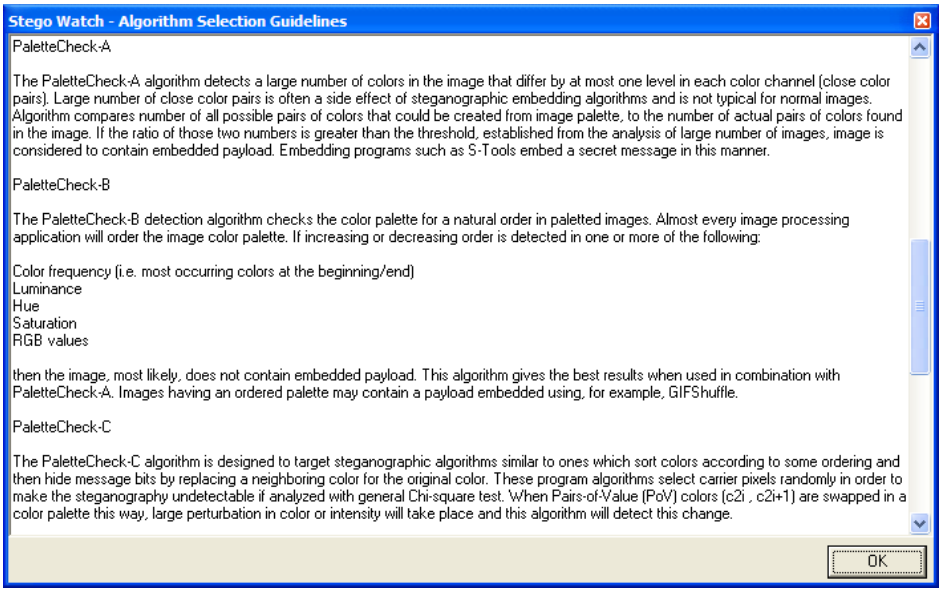


Stego Watch

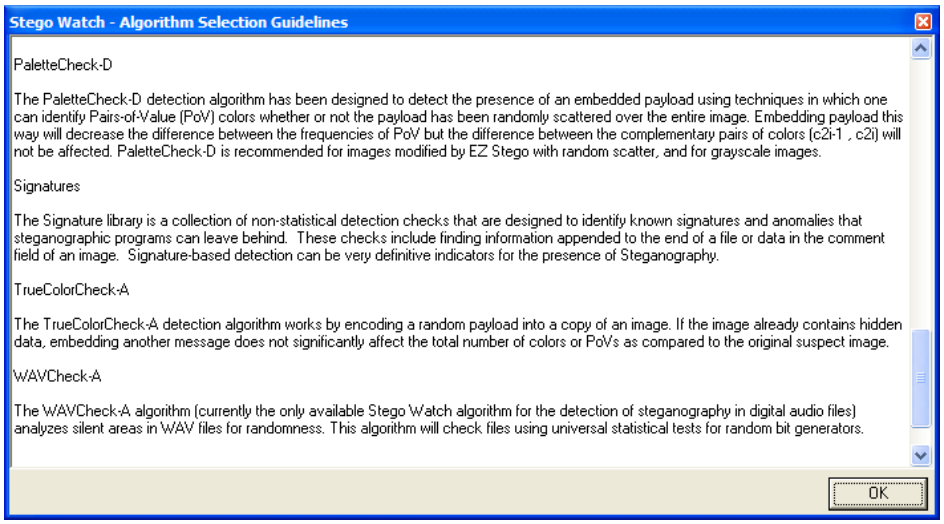
Session setup for examining files on a local drive

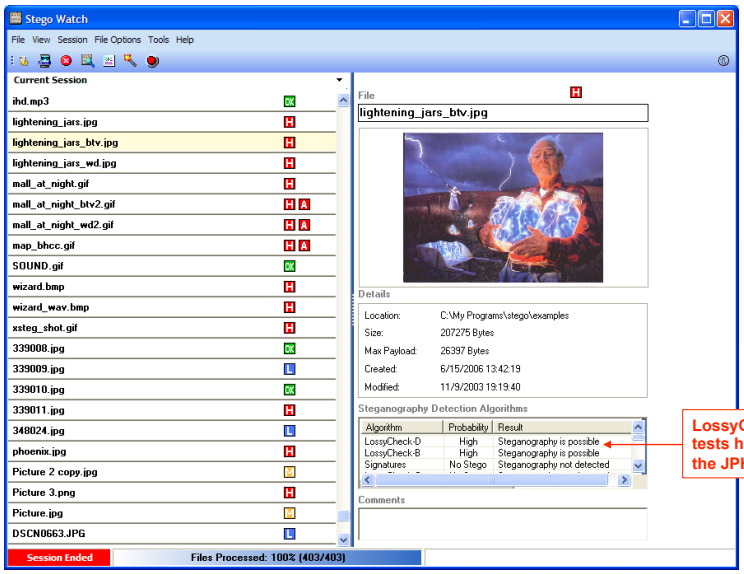


 52



 53





Stego Watch

File details

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

File Details :

File :	mall_at_night_btv2.gif
File Origin :	C:\My Programs\stego\examples
Disk Location :	C:\My Programs\stego\examples
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

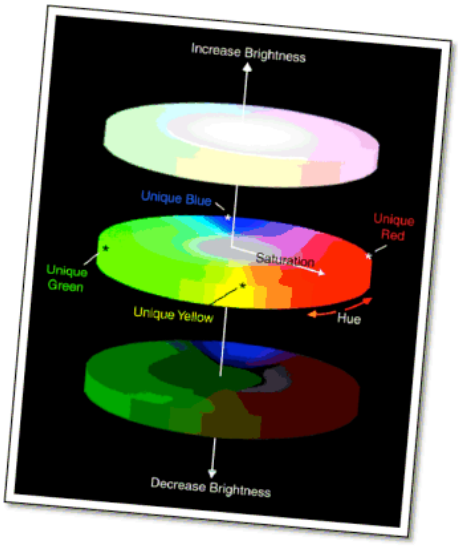
Report generated by Stego Watch from WetStone Technologies, Inc. on 10/08/2007 13:38:02

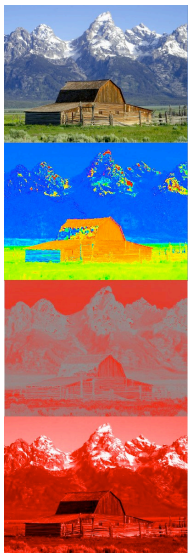
Algorithm :	Results :
LossyCheck-A	Invalid File for Algorithm
LossyCheck-B	Invalid File for Algorithm
LossyCheck-C	Invalid File for Algorithm
LossyCheck-D	Invalid File for Algorithm
PaletteCheck-A	Steganography not detected
PaletteCheck-B	Steganography is possible
PaletteCheck-C	Steganography not detected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

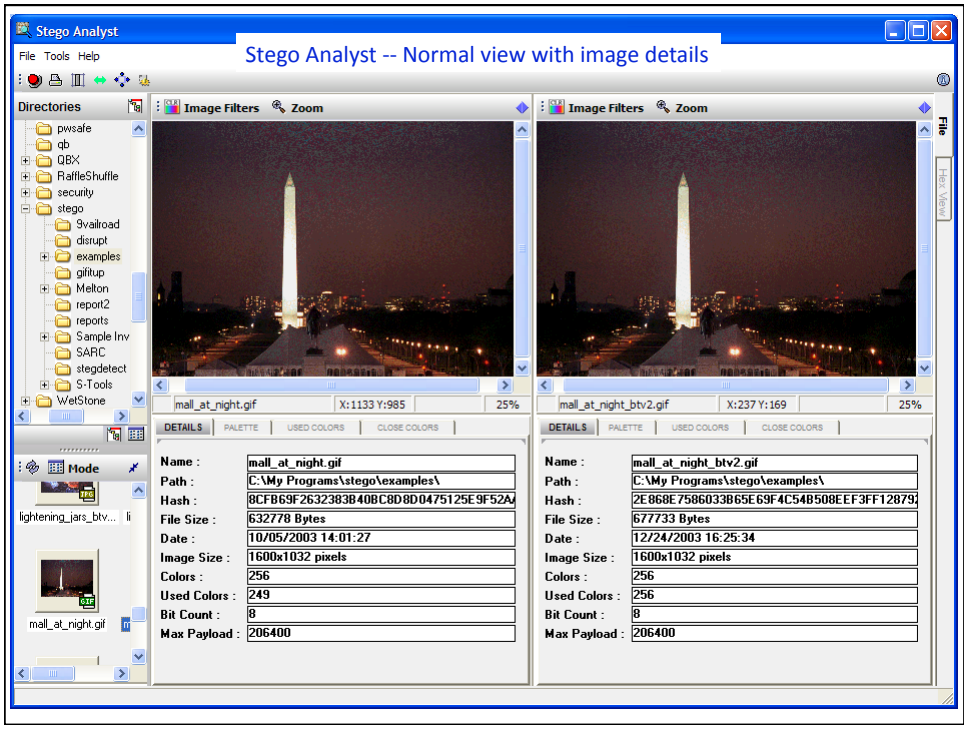
LossyCheck tests not applicable to JPEG files

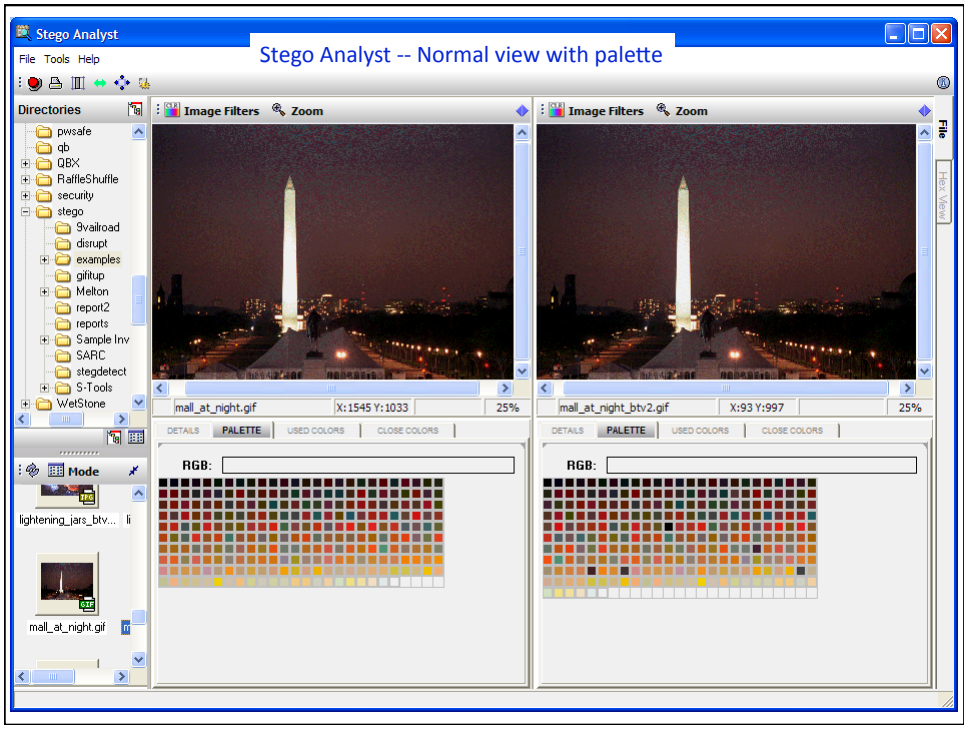
Palette check tests appropriate for GIF files

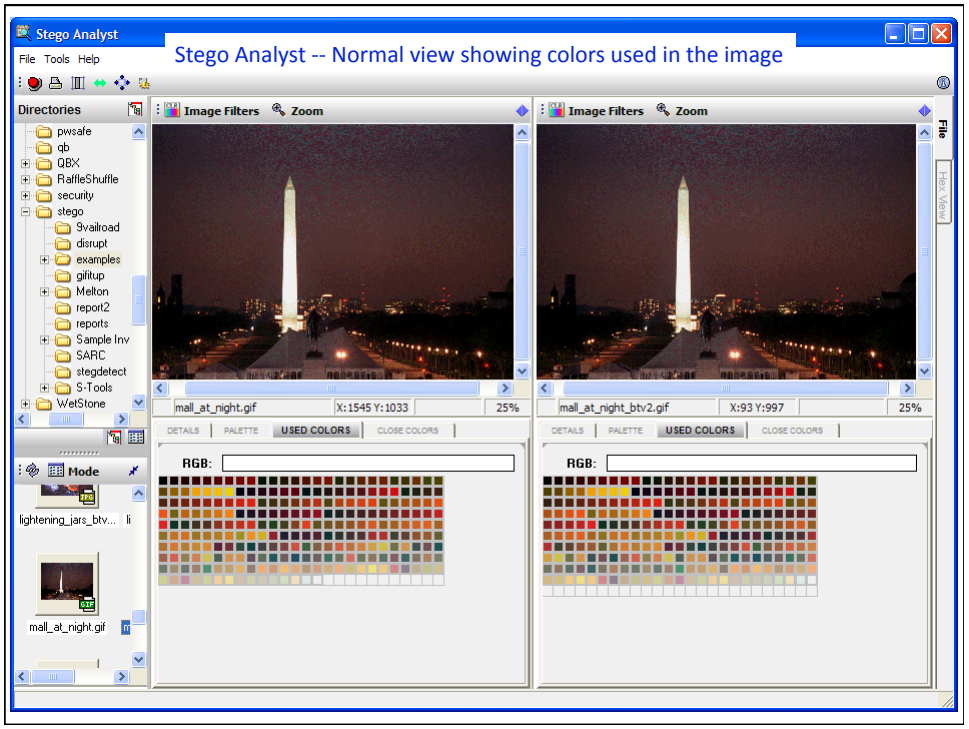
Hue, Intensity, and Saturation

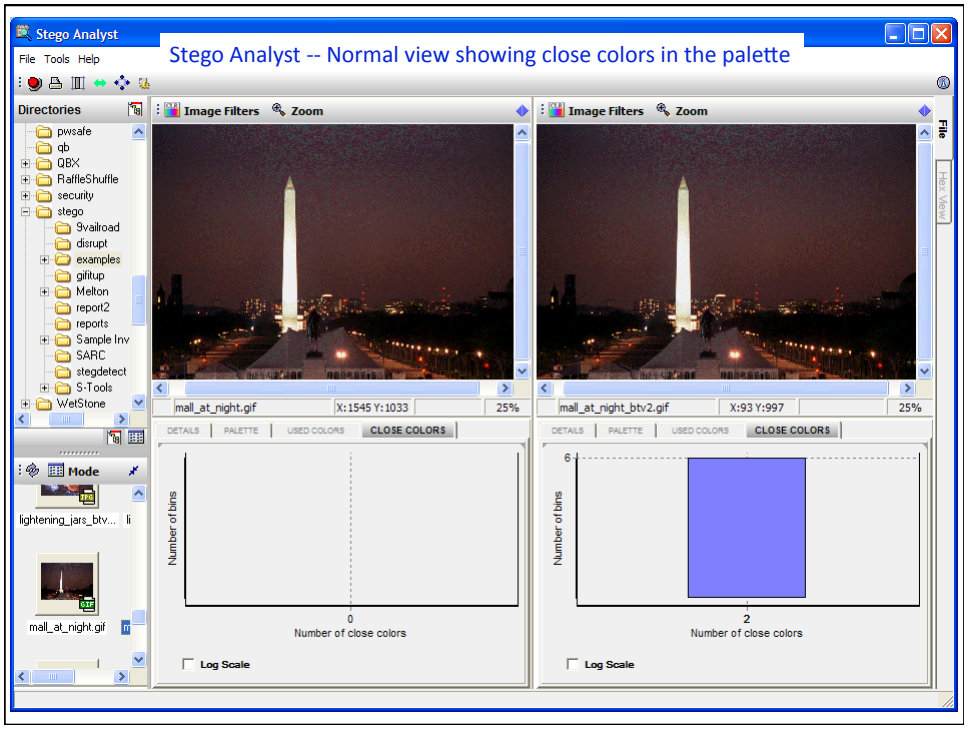


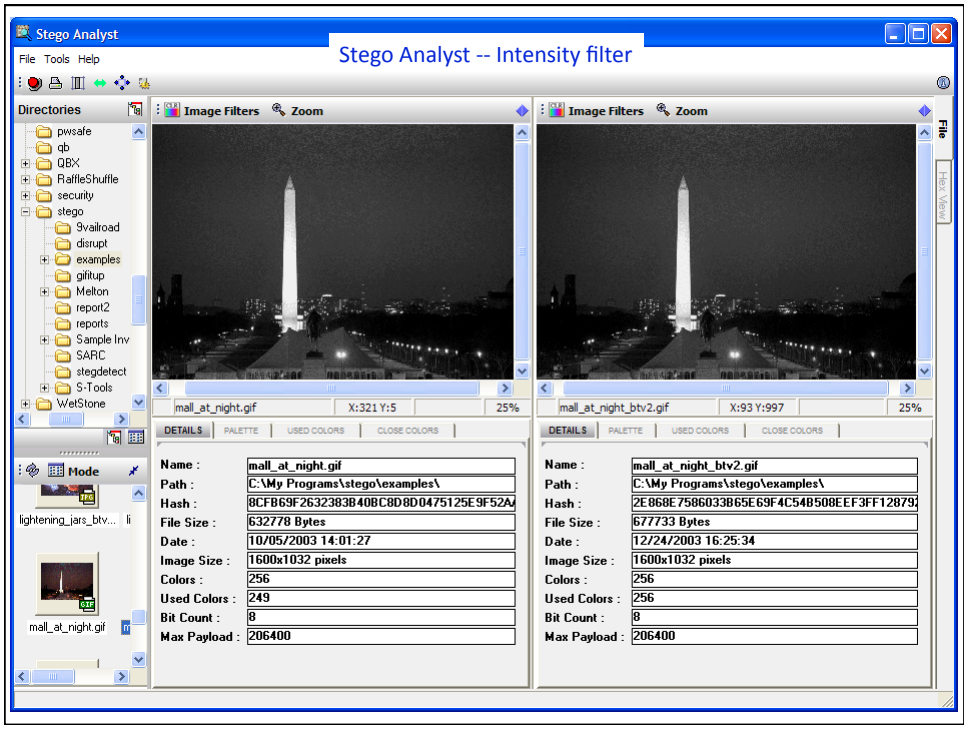



Stego Analyst -- Normal view with image details
Stego Analyst
File Tools Help
Directories
Image Filters
Zoom
mall_at_night.gif
mall_at_night_btv2.gif
DETAILS
PALETTE
USED COLORS
CLOSE COLORS
Name :
Path :
Hash :
File Size :
Date :
Image Size :
Colors :
Used Colors :
Bit Count :
Max Payload :
mall_at_night.gif
632778 Bytes
10/05/2003 14:01:27
1600x1032 pixels
256
249
8
206400
mall_at_night_btv2.gif
C:\My Programs\stego\examples\
677733 Bytes
12/24/2003 16:25:34
1600x1032 pixels
256
256
8
206400

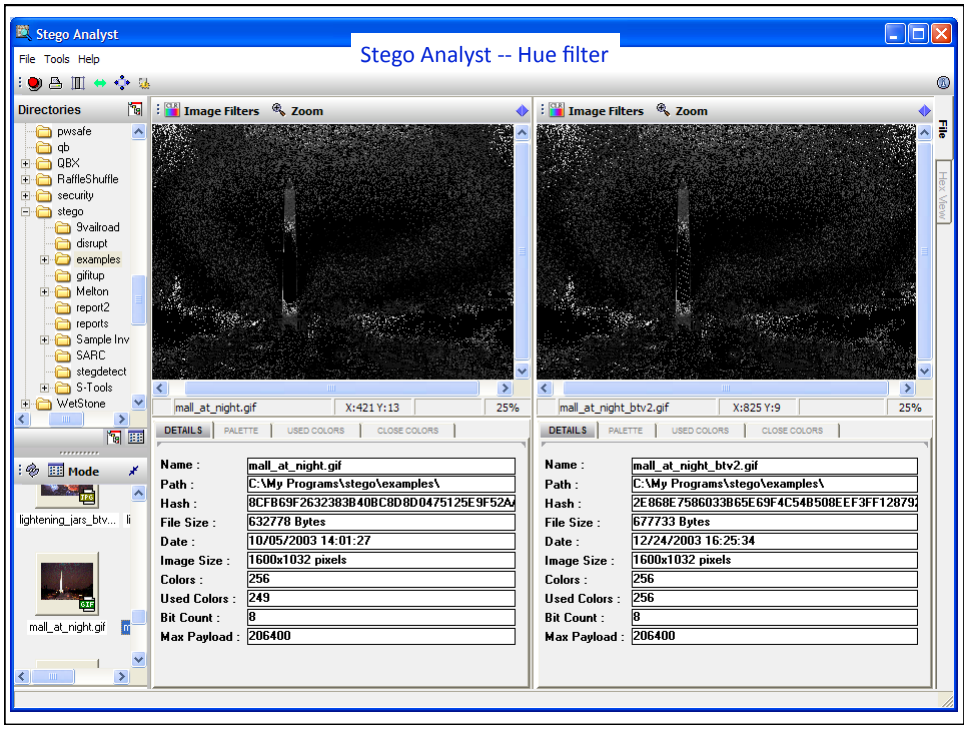

Stego Analyst -- Normal view with palette
Stego Analyst
File Tools Help
Directories
Image Filters
Zoom
mall_at_night.gif
mall_at_night_btv2.gif
DETAILS
PALETTE
USED COLORS
CLOSE COLORS
RGB:

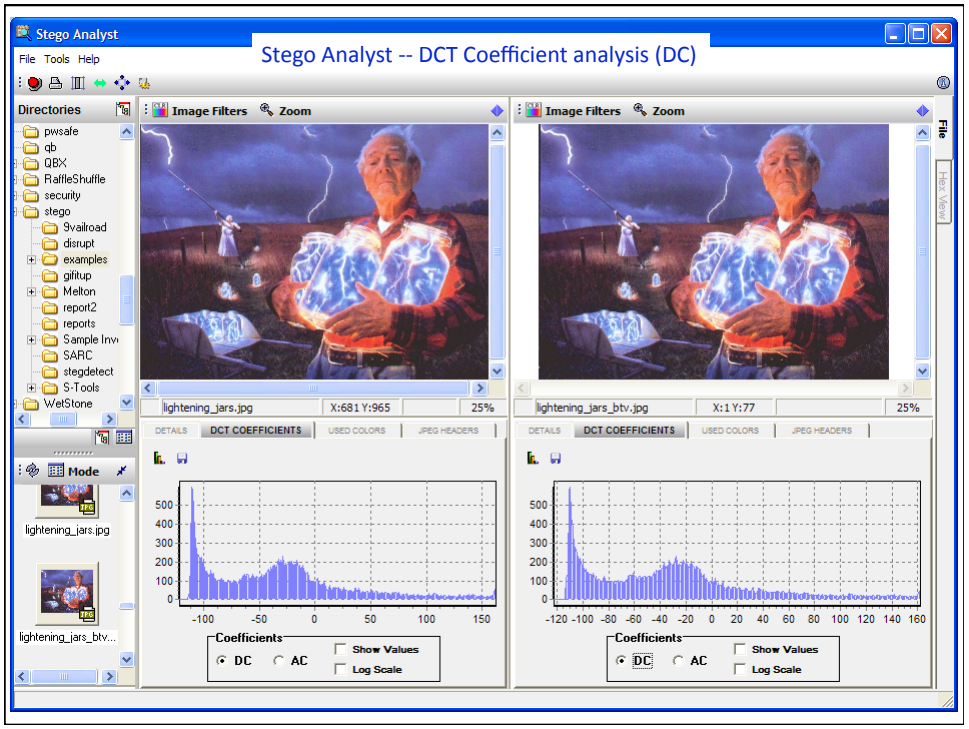

Stego Analyst
File Tools Help
Stego Analyst -- Normal view showing colors used in the image
Directories
Image Filters
Zoom
mall_at_night.gif
X:1545 Y:1033
25%
mall_at_night_btv2.gif
X:93 Y:997
DETAILS
PALETTE
USED COLORS
CLOSE COLORS
RGB:
Mode

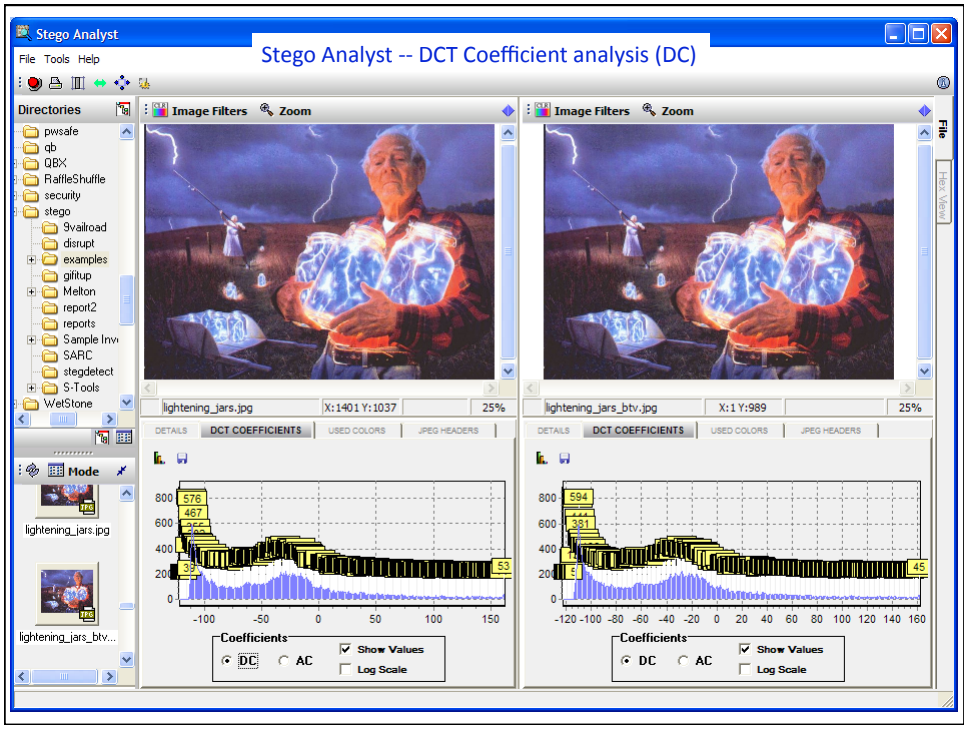

Stego Analyst
File Tools Help
Stego Analyst -- Normal view showing close colors in the palette
Directories
Image Filters
Zoom
mall_at_night.gif
X:1545 Y:1033
25%
mall_at_night_btv2.gif
X:93 Y:997
DETAILS
PALETTE
USED COLORS
CLOSE COLORS
Number of bins
Number of close colors
Log Scale
Mode

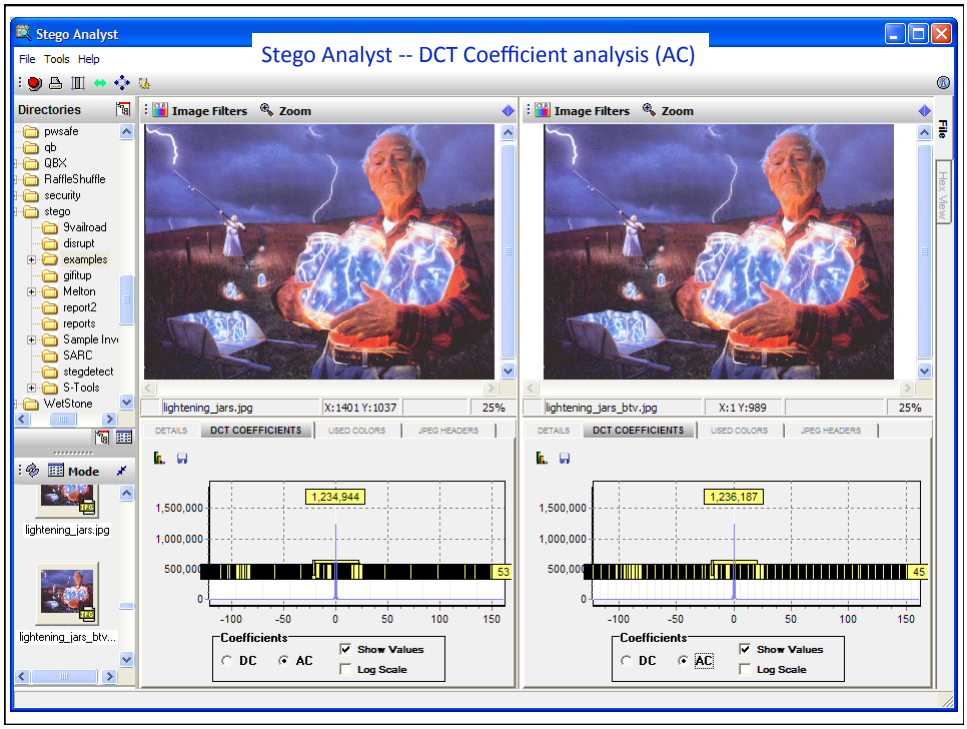

Stego Analyst -- Intensity filter
Stego Analyst
File Tools Help
Directories
Image Filters
Zoom
mall_at_night.gif
X:321 Y:5
25%
mall_at_night_btv2.gif
X:93 Y:997
25%
DETAILS
PALETTE
USED COLORS
CLOSE COLORS
Name : mall_at_night.gif
Path : C:\My Programs\stego\examples\
Hash : 8CFB69F2632383B40BC8D8D0475125E9F52A
File Size : 632778 Bytes
Date : 10/05/2003 14:01:27
Image Size : 1600x1032 pixels
Colors : 256
Used Colors : 249
Bit Count : 8
Max Payload : 206400
Name : mall_at_night_btv2.gif
Path : C:\My Programs\stego\examples\
Hash : 2E868E7586033B65E69F4C54B508EEF3FF12879
File Size : 677733 Bytes
Date : 12/24/2003 16:25:34
Image Size : 1600x1032 pixels
Colors : 256
Used Colors : 256
Bit Count : 8
Max Payload : 206400
Mode
lightening_jars_btv...
mall_at_night.gif


Stego Analyst -- Saturation filter
Stego Analyst
File Tools Help
Directories
Image Filters
Zoom
mall_at_night.gif
X:661 Y:5
25%
mall_at_night_btv2.gif
X:825 Y:9
25%
DETAILS
PALETTE
USED COLORS
CLOSE COLORS
Name : mall_at_night.gif
Path : C:\My Programs\stego\examples\
Hash : 8CFB69F2632383B40BC8D8D0475125E9F52A
File Size : 632778 Bytes
Date : 10/05/2003 14:01:27
Image Size : 1600x1032 pixels
Colors : 256
Used Colors : 249
Bit Count : 8
Max Payload : 206400
Name : mall_at_night_btv2.gif
Path : C:\My Programs\stego\examples\
Hash : 2E868E7586033B65E69F4C54B508EEF3FF12879
File Size : 677733 Bytes
Date : 12/24/2003 16:25:34
Image Size : 1600x1032 pixels
Colors : 256
Used Colors : 256
Bit Count : 8
Max Payload : 206400
Mode
lightening_jars_btv...
mall_at_night.gif


Stego Analyst -- Hue filter
Stego Analyst
File Tools Help
Directories
Image Filters
Zoom
mall_at_night.gif
mall_at_night_btv2.gif
Name :
Path :
Hash :
File Size :
Date :
Image Size :
Colors :
Used Colors :
Bit Count :
Max Payload :
632778 Bytes
677733 Bytes
10/05/2003 14:01:27
12/24/2003 16:25:34
1600x1032 pixels
256
249
8
206400


Stego Analyst -- DCT Coefficient analysis (DC)
Stego Analyst
File Tools Help
Directories
Image Filters
Zoom
lightening_jars.jpg
lightening_jars_btv.jpg
DETAILS
DCT COEFFICIENTS
USED COLORS
JPEG HEADERS
Coefficients
DC
AC
Show Values
Log Scale

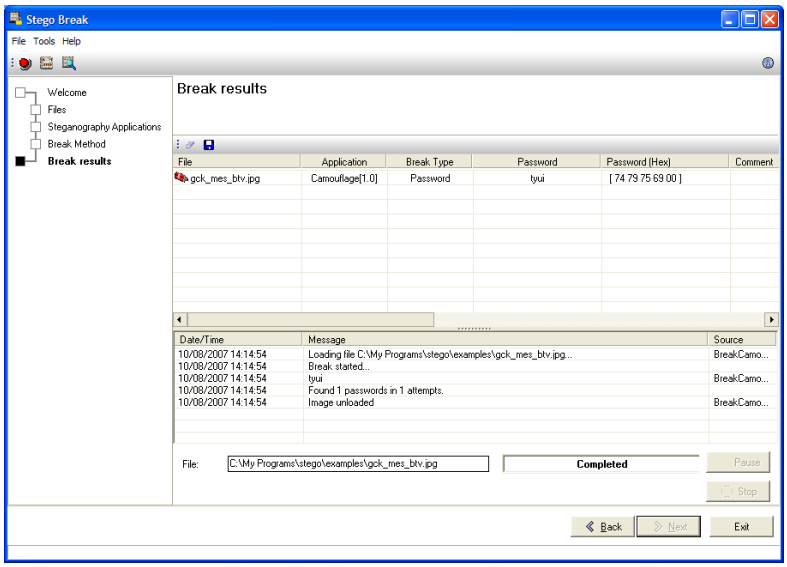

Stego Analyst -- DCT Coefficient analysis (DC)
Stego Analyst
File Tools Help
Directories
Image Filters
Zoom
lightening_jars.jpg
X:1401 Y:1037
25%
lightening_jars_btv.jpg
X:1 Y:989
25%
DETAILS
DCT COEFFICIENTS
USED COLORS
JPEG HEADERS
Coefficients
DC
AC
Show Values
Log Scale


Stego Analyst -- DCT Coefficient analysis (AC)
Stego Analyst
File Tools Help
Directories
Image Filters
Zoom
lightening_jars.jpg
X:1401 Y:1037
25%
lightening_jars_btv.jpg
X:1 Y:989
25%
DETAILS
DCT COEFFICIENTS
USED COLORS
JPEG HEADERS
1,234,944
1,236,187
Coefficients
DC
AC
Show Values
Log Scale

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....

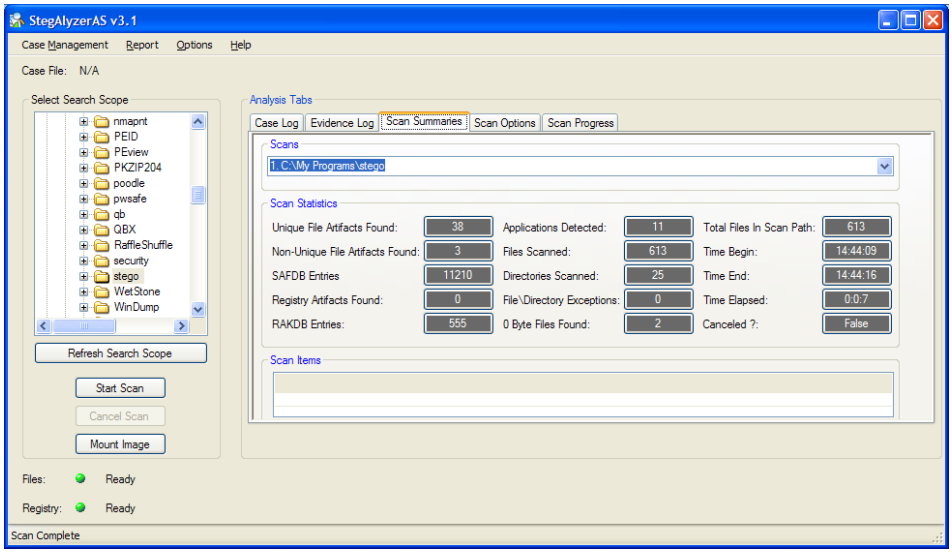
Stego Break



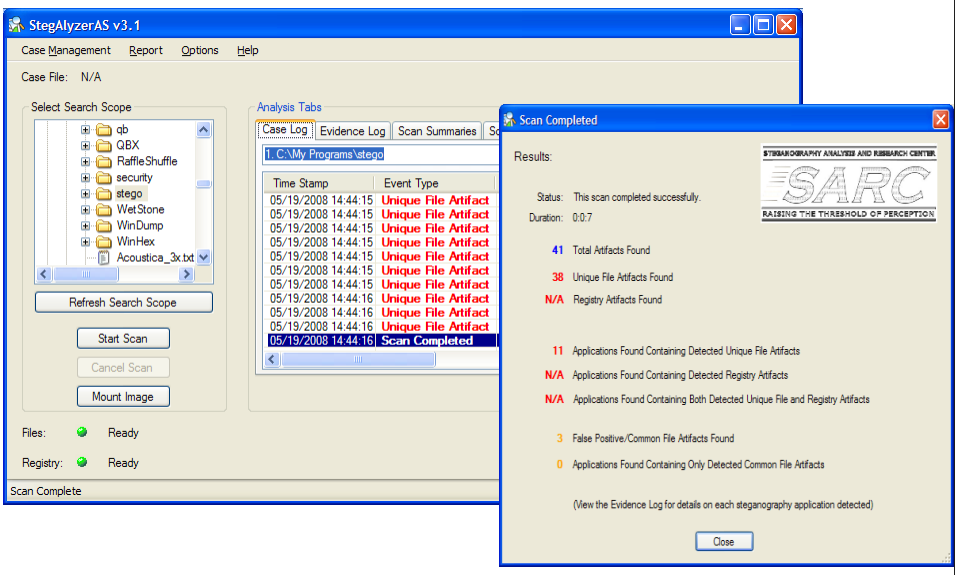
Steganography Analysis and Research Center (SARC)

- 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

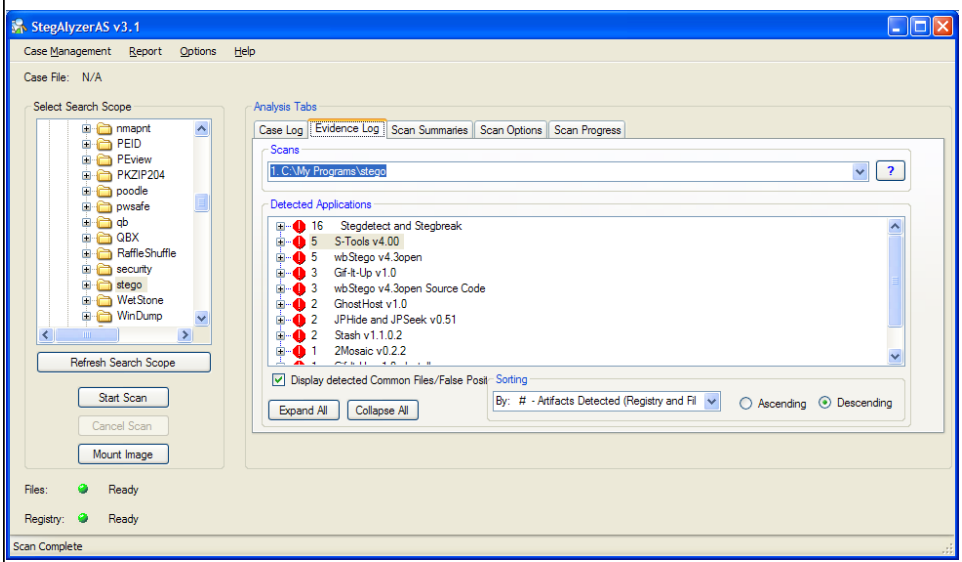
StegAlyzerAS - Scan Summary



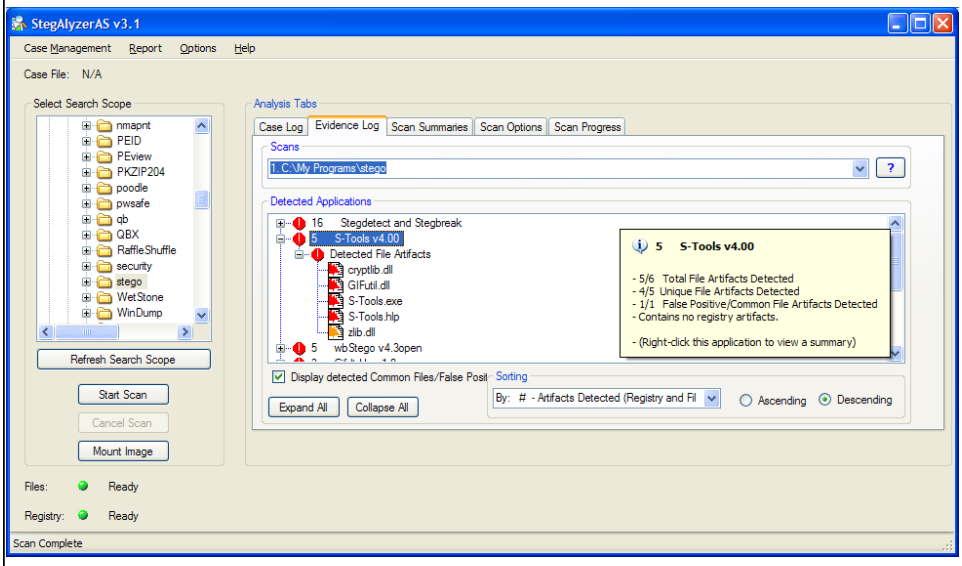
StegAlyzerAS - Case Log

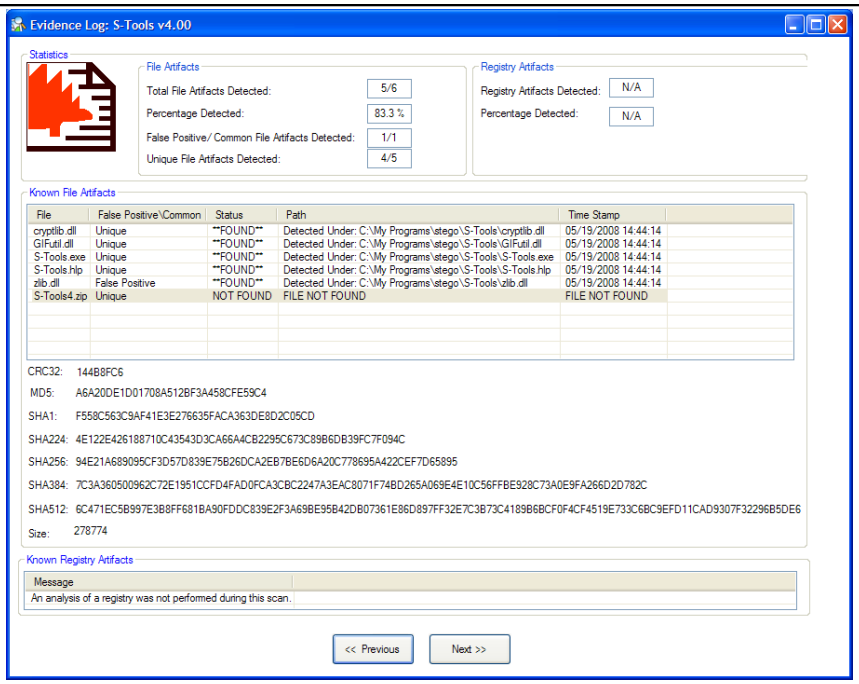


StegAlyzerAS - Evidence Log

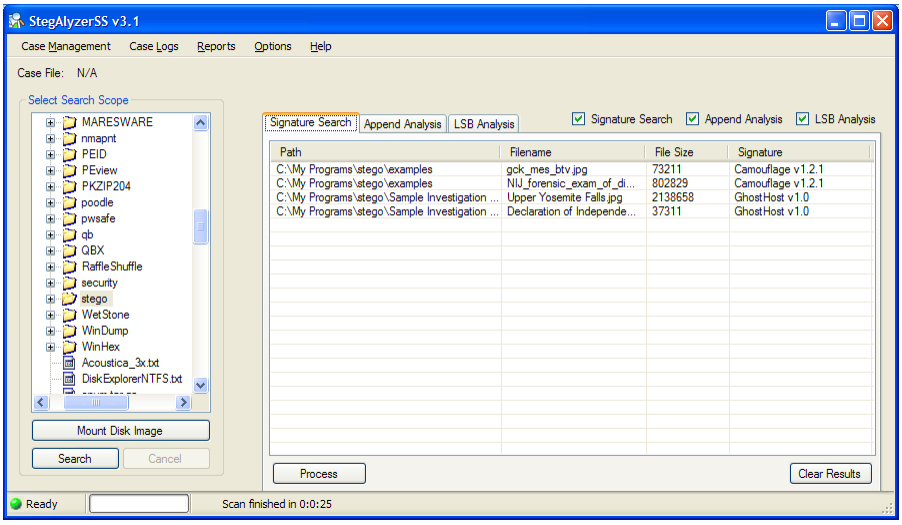


StegAlyzerAS - Application Info



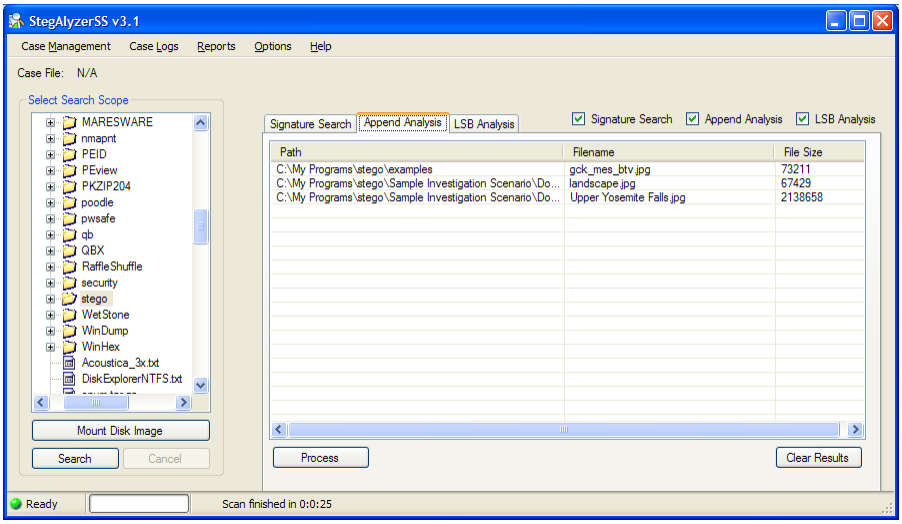


StegAlyzerSS - Signature Search



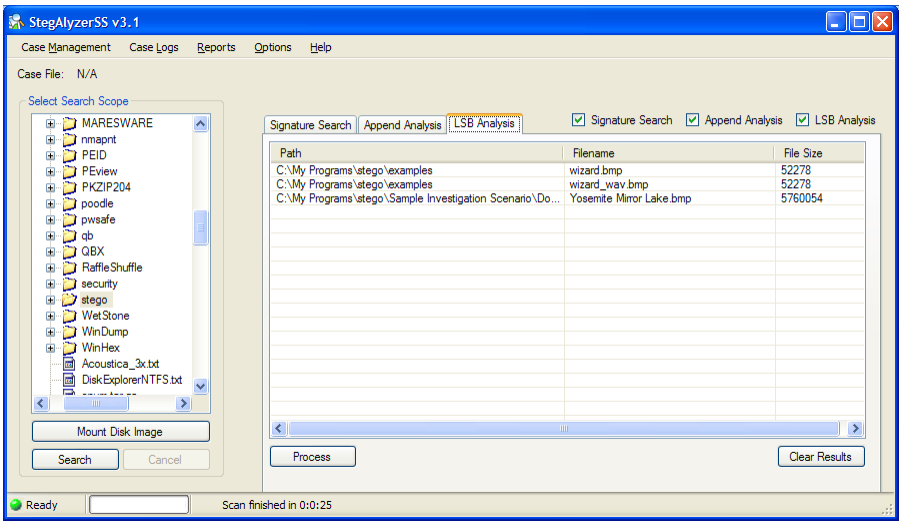
 76

StegAlyzerSS - Append Analysis



 77

StegAlyzerSS - LSB Analysis

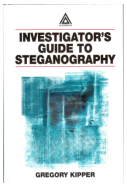


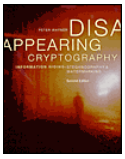
Some Final Words

- 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, Wayner





- 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/*)

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*

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

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*

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.

