ΣΤΕΓΑΝΑΛΥΣΗ

Είναι η διαδικασία ανίχνευσης της στεγανογραφίας, δλδ της αναγνώρισης ότι σε ένα *μέσο* έχει ενθεθεί κρυμμένη πληροφορία, χωρίς γνώση ούτε του μηχανισμού ούτε της κλείδας ένθεσης.

Κατ' ουσίαν η στεγανάλυση αφορά τη διάκριση ενός μέσου που έχει στεγανογραφηθεί, από άλλα που δεν έχουν.

σκοπός

Η ανίχνευση της ύπαρξης ενός κρυμμένου μηνύματος μέσα σε ένα μέσο.

Δεν απαιτείται η αναγνώριση-διάσπαση της κρυμμένης πληροφορίας, παρά απλά η ανίχνευσή της.

Στεγανάλυση ορισμός

Ορισμός

Αναγνώριση της ύπαρξης κρυμμένου μηνύματος

Όχι εξαγωγή του μηνύματος

Σημείωση: τεχνικά η στεγανογραφία έχει να κάνει με την κάλυψη ενός μηνύματος κι όχι την κρυπτογράφησή του.

Η στεγανάλυση κυρίως έχει να κάνει με την ανίχνευση κρυμμένου μηνύματος

Στεγανάλυση

Με την αναγνώριση ύπαρξης κρυμμένου μηνύματος, ίσως αναγνωρίσουμε και τα εργαλεία με τα οποία αυτό εντέθηκε.

Εάν αναγνωρίσουμε τα εργαλεία ένθεσης, ίσως να καταφέρουμε να εξάγουμε και το μήνυμα καθεαυτό.

Στεγανάλυση-Τεχνικές απόκρυψης

Συνήθεις τεχνικές απόκρυψης

- Πρόσθεση μετά το τέλος ενός αρχείου.
- Ένθεση στο αχρησιμοποίητο τμήμα της κεφαλίδας ενός αρχείου, πριν την έναρξη των περιεχομένων του.
- Χρήση αλγορίθμου διασποράς του κρυμμένου μηνύματος κατά μήκος ολόκληρου του αρχείου.
  - Τροποποίηση των LSB (Least Significant Bits)
  - άλλο

Στεγανάλυση-Μέθοδοι ανίχνευσης

Μέθοδοι ανίχνευσης στεγανογραφίας:

- Οπτική ανίχνευση (JPEG, BMP, GIF, etc.)
- Ακουστική ανίχνευση (WAV, MPEG, etc.)
- Στατιστική ανίχνευση (αλλαγές στα πρότυπα των pixels or LSB – Least Significant Bit) ή Ανάλυση ιστογράμματος
- Δομική ανίχνευση – Εποπτεία των ιδιοτήτων / περιεχομένων ενός αρχείου.
  - Διαφορά στο μέγεθος
  - Διαφορά σε ώρα/ημερομηνία
  - Τροποποίηση περιεχομένων
  - checksum

Στεγανάλυση μέθοδοι ανίχνευσης

- Κατηγορίες
  - Αλλοιώσεις
    - Ανάλυση ιστογράμματος
    - Αλλαγές στις ιδιότητες του αρχείου
    - Στατιστική επίθεση
    - Οπτικές
    - Ακουστικές
  - «Υπογραφές»
    - Εύρεση κάποιου προτύπου άμεσα συνδεδεμένου με το πρόγραμμα που χρησιμοποιήθηκε.

Στεγανάλυση-Μέθοδοι ανίχνευσης

Σκοπός

- Ακρίβεια
- Συνέπεια
- Ελαχιστοποίηση των ψευδοενδείξεων (false-positives)

Αλλοίωση – Οπτική ανίχνευση

Ανιχνεύοντας τη στεγανογραφία με οπτικό έλεγχο.

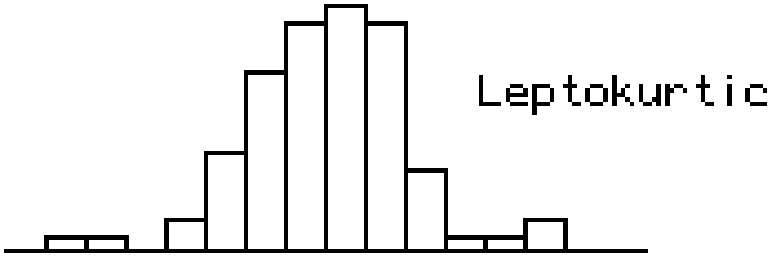
Μπορείτε να βρείτε διαφορά στις δύο εικόνες? (Προσωπικά εγώ δεν μπορώ!)

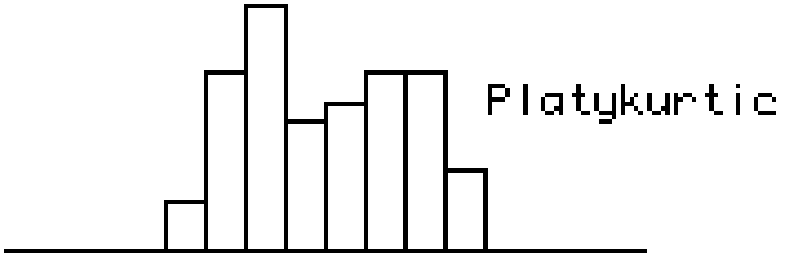
Αλλοίωση - Kurtosis

Kurtosis

The degree of flatness or peakedness of a curve desribing a frequency of distribution

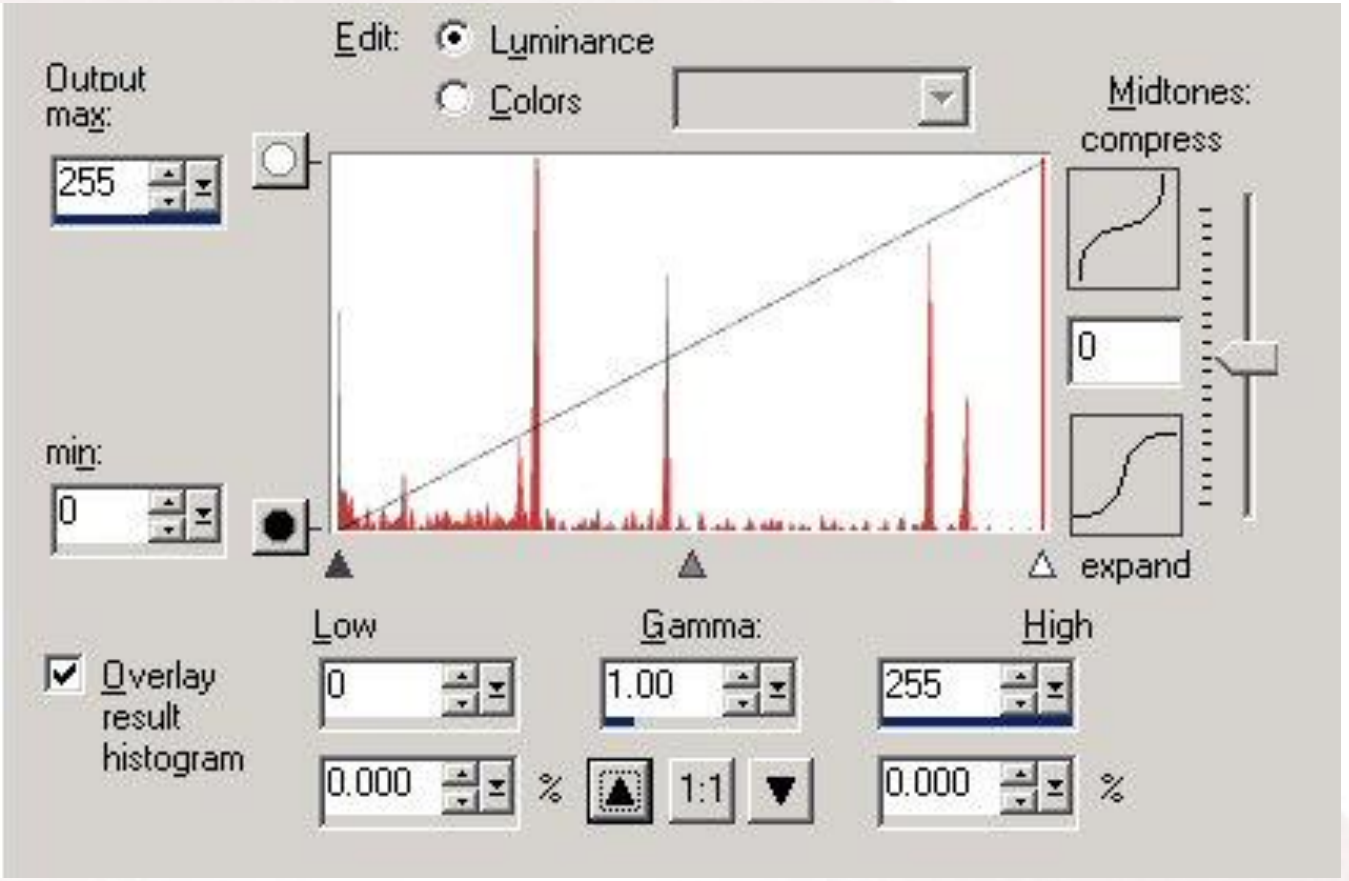
Random House Dictionary





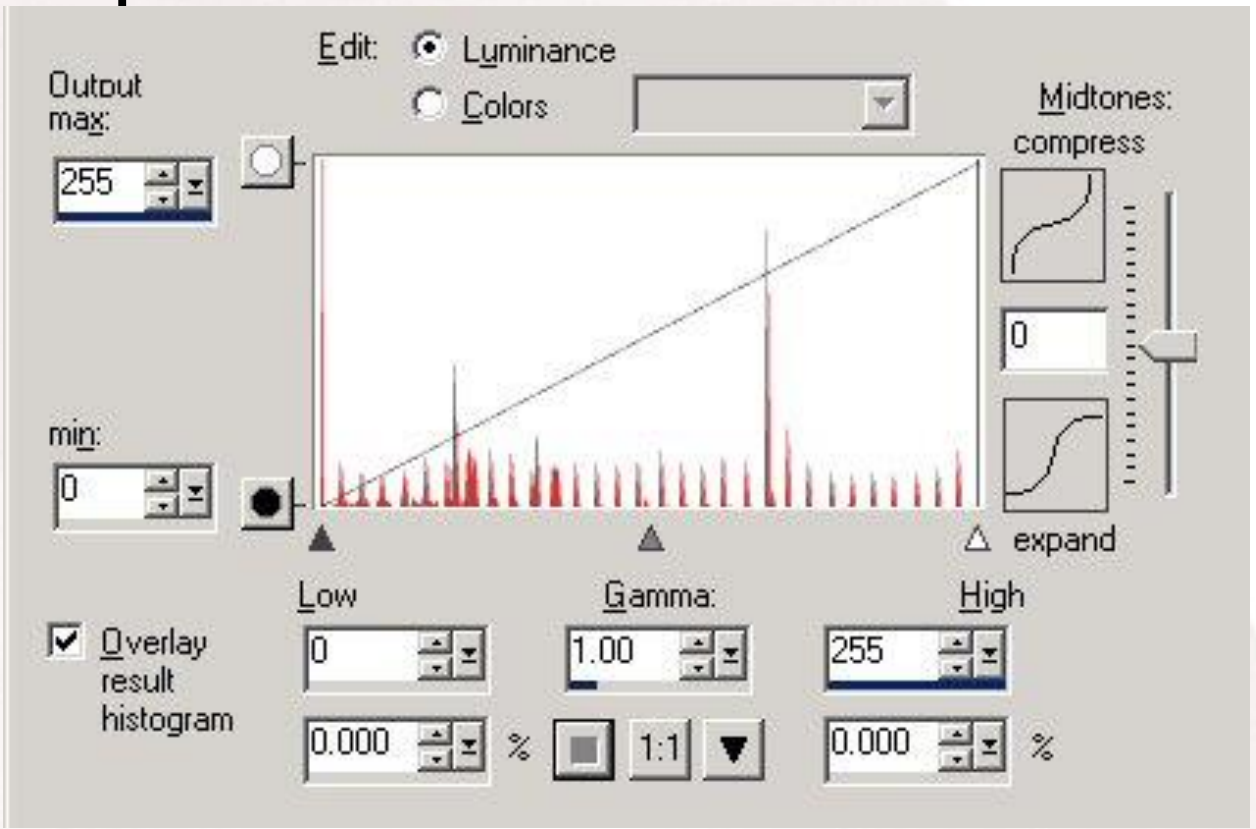
Αλλοίωση - Histogram Analysis

Η ανάλυση ιστογράμματος χρησιμοποιείται για την πιθανή ανίχνευση κρυμμένου μηνύματος



Αλλοίωση – Histogram Analysis

Μία σύγκριση ιστογράμματος μπορεί να αποδώσει μια επίμονη επαναληπτική τάση σε ένα από αυτά.



Ανάλυση Αλλοιώσεων – Σύγκριση ιδιοτήτων αρχείου

Σύγκριση ιδιοτήτων αρχείου

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

«Υπογραφές» Αρχείων

HEX Signature	File Extension	ASCII Signature
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

Στεγανάλυση – Αναλύοντας τα περιεχόμενα του αρχείου

Εάν υπάρχει το γνήσιο (παρθένο) αρχείο, μπορεί να συγκριθεί με το τροποποιημένο, ύποπτο για στεγανογραφία αρχείο.

Πολλά εργαλεία μπορούν να χρησιμοποιηθούν για να γίνει επισκόπηση και σύγκριση των περιεχομένων ενός αρχείου.

Από το Notepad μέχρι το Hex Editor, υπάρχει πληθώρα λογισμικού που θα μπορούσε να χρησιμοποιηθεί ώστε να ανιχνευθούν είτε πρότυπα είτε αλλοιώσεις.

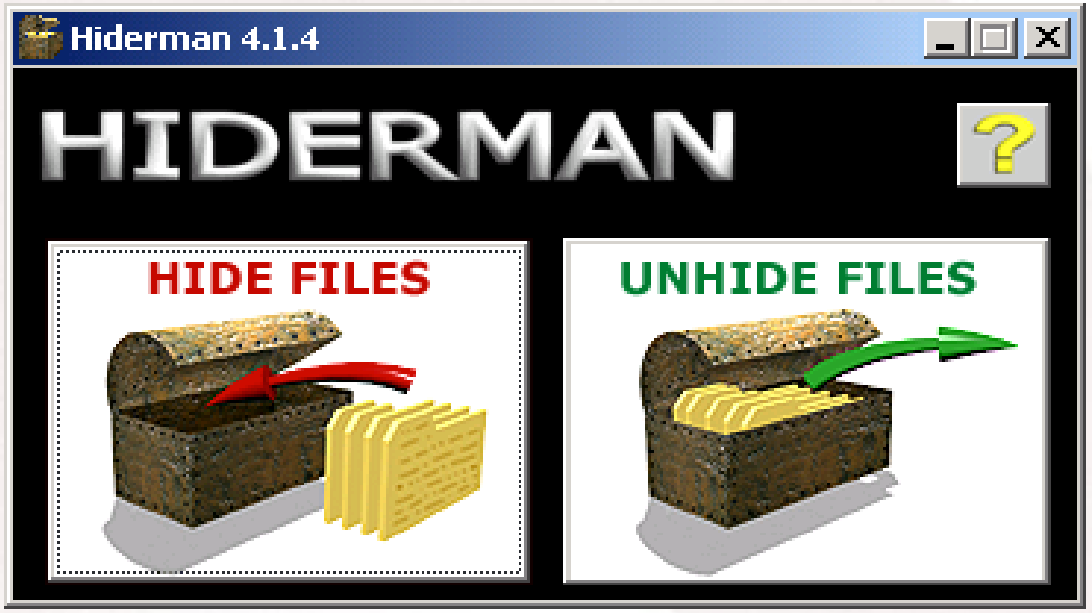
Η ανάλυση πολλών αρχείων, ίσως αναδείξει κάποιο πρότυπο-υπογραφή που σχετίζεται με συγκεκριμένο λογισμικό στεγανογραφίας.

Στεγανάλυση – Αναλύοντας τα περιεχόμενα του αρχείου

- Χρήσιμο λογισμικό ανάλυσης
  - WinHex – www.winhex.com
    - Δυνατότητα μετατροπής μεταξύ ASCII and Hex
    - Δυνατότητα σύγκρισης αρχείων
      - Σώζει τη σύγκριση ως αναφορά
      - Ερευνά για διαφορές ή ισότητες bytes
    - Δυνατότητα σήμανσης αρχείου
    - Δυνατότητα έρευνας για ακολουθία χαρακτήρων– είτε ASCII είτε Hex
    - Πολλές άλλες λειτουργίες

Hiderman – Υπόθεση Έρευνας

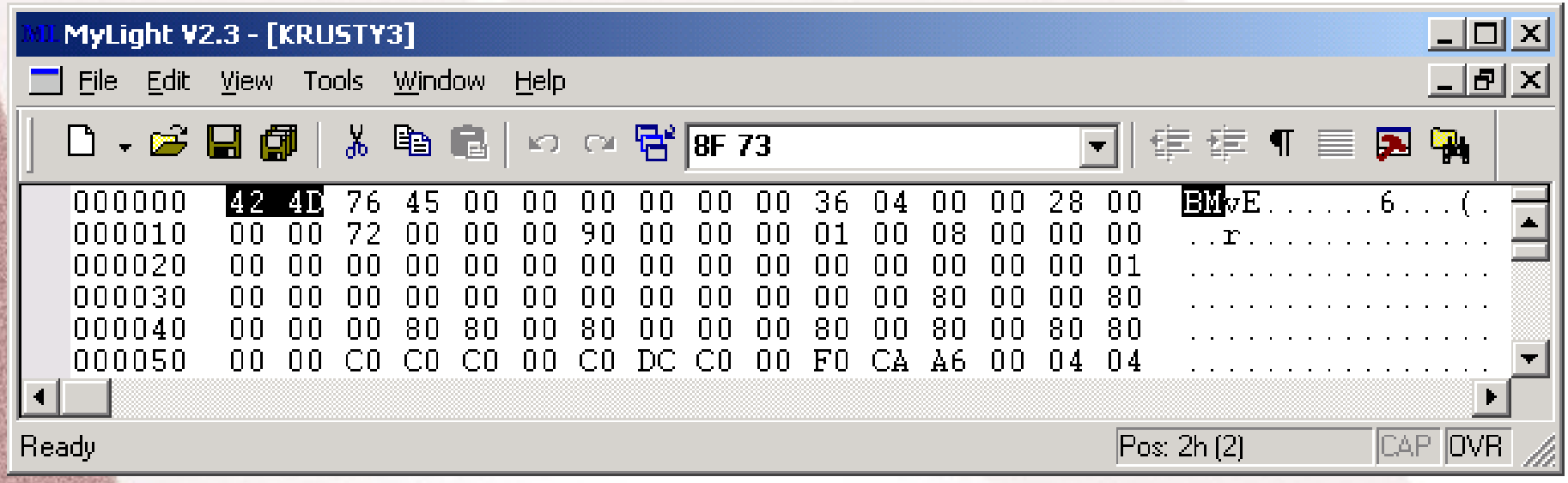
Ας δούμε το λογισμικό στεγανογραφίας – Hiderman



Hiderman – Υπόθεση Έρευνας

Κρύβοντας ένα μήνυμα με το Hiderman, κάνουμε επισκόπηση στο αρχείο με το Hex Tool.

Παρατηρώντας την κεφαλίδα (Αρχή του αρχείου) βλέπουμε ότι είναι ένα Bitmap καθώς φαίνεται από τη δήλωση "BM" του τύπου του αρχείου.

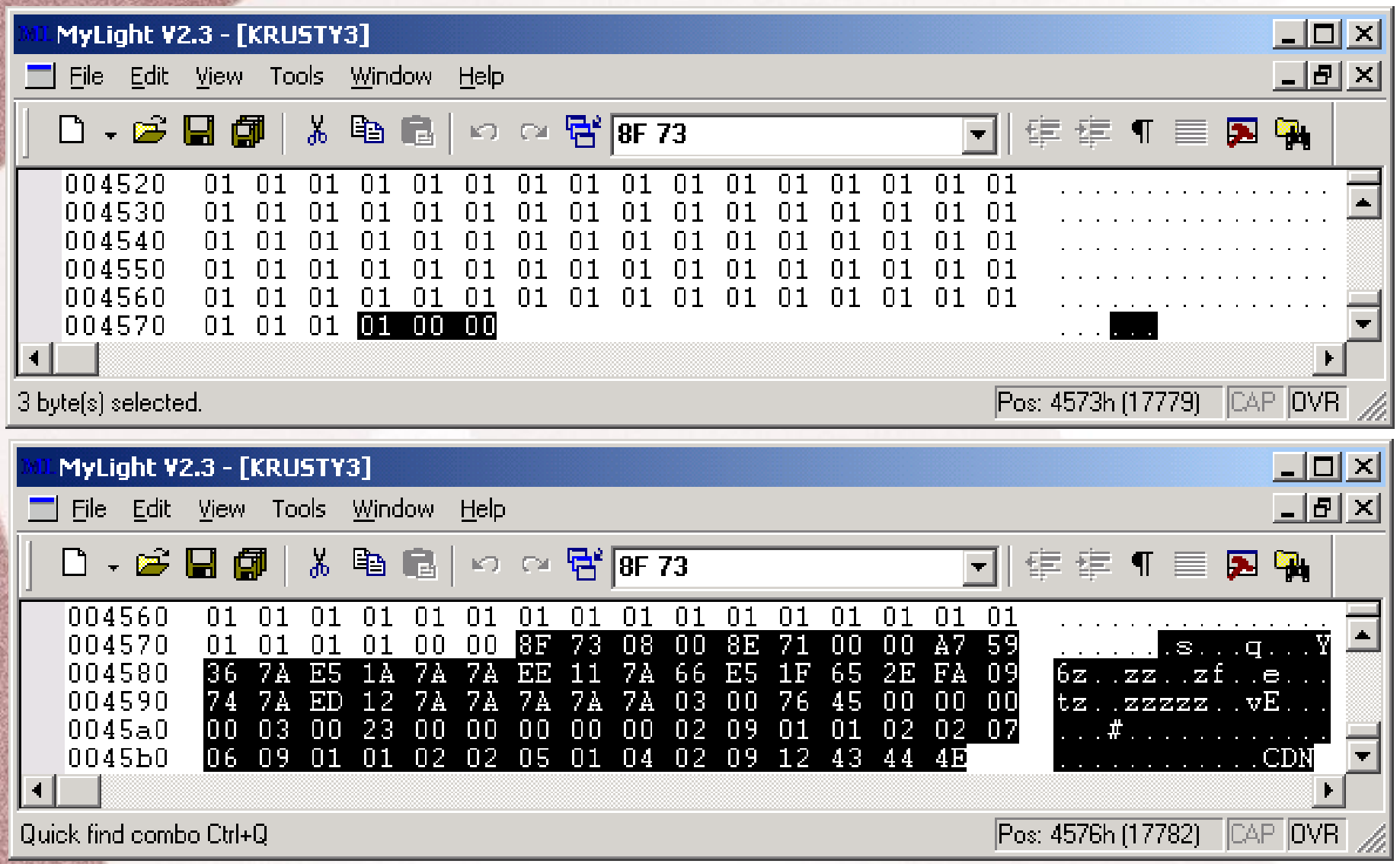


Hiderman – Υπόθεση Έρευνας

Στη συνέχεια παρατηρούμε το τέλος του αρχείου, συγκρίνοντας το γνήσιο με το αλλαγμένο.

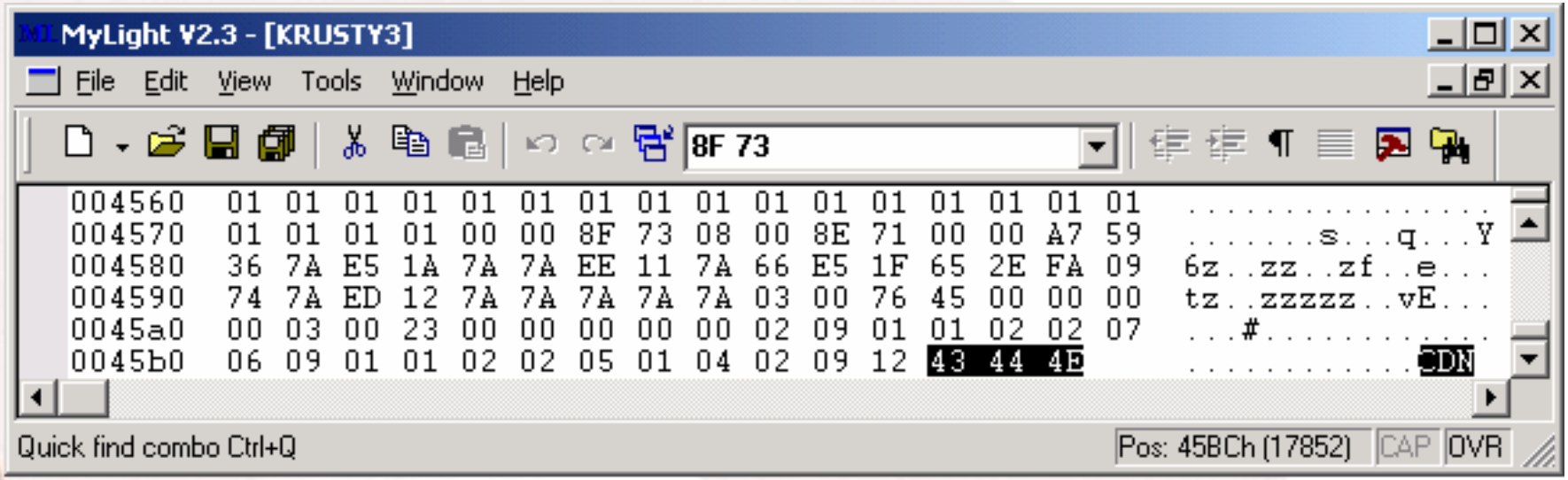
Υπάρχουν επιπρόσθετα δεδομένα στο αρχείο (στην επόμενη διαφάνεια)

Hiderman – Υπόθεση Έρευνας



Hiderman – Υπόθεση Έρευνας

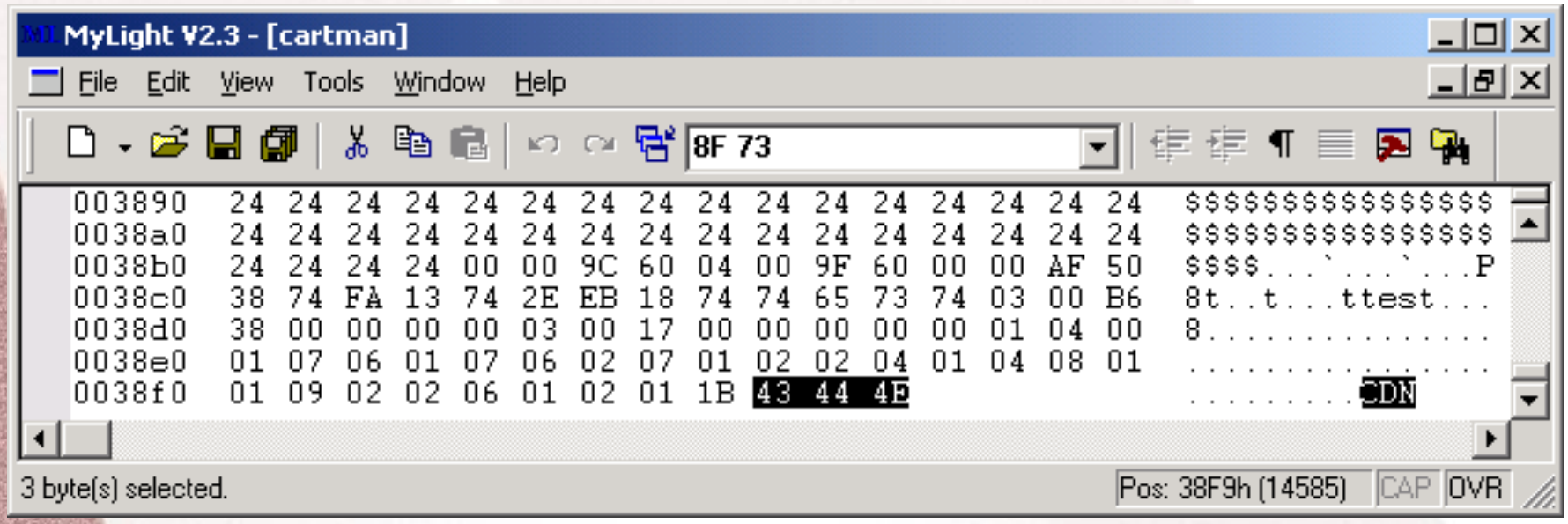
Επιπλέον, σημειώνονται οι τρεις τελευταίοι χαρακτήρες "CDN" που είναι οι 43 44 4E σε HEX.



Hiderman – Υπόθεση Έρευνας

Κρύβοντας διαφορετικά μηνύματα σε διαφορετικά αρχεία, παρατηρούμε τους ίδιους τρεις χαρακτήρες που προστίθενται στο τέλος του αρχείου (“CDN”).

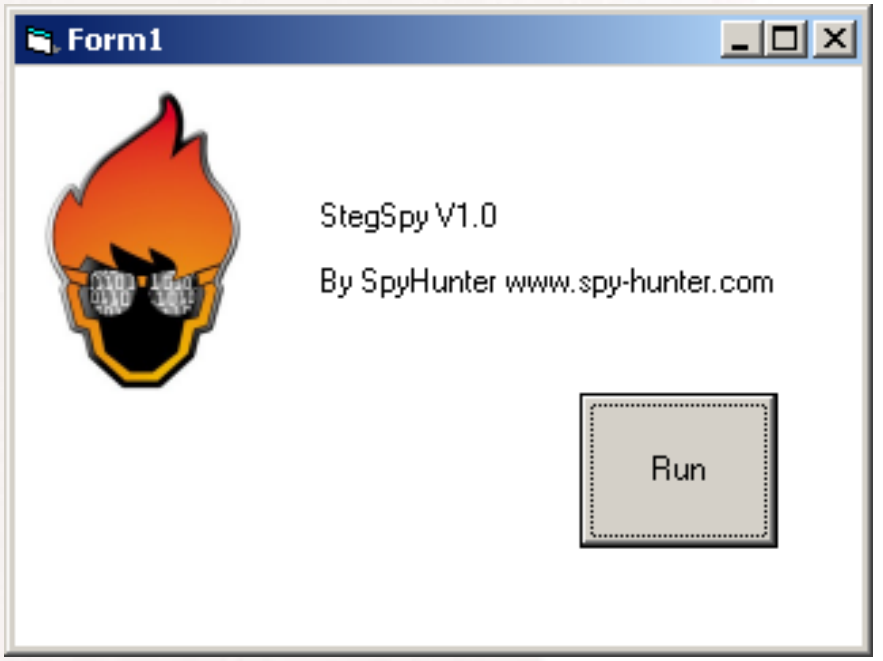
Εύρεση «υπογραφής»



Στεγανάλυση – Stegspy V2.0

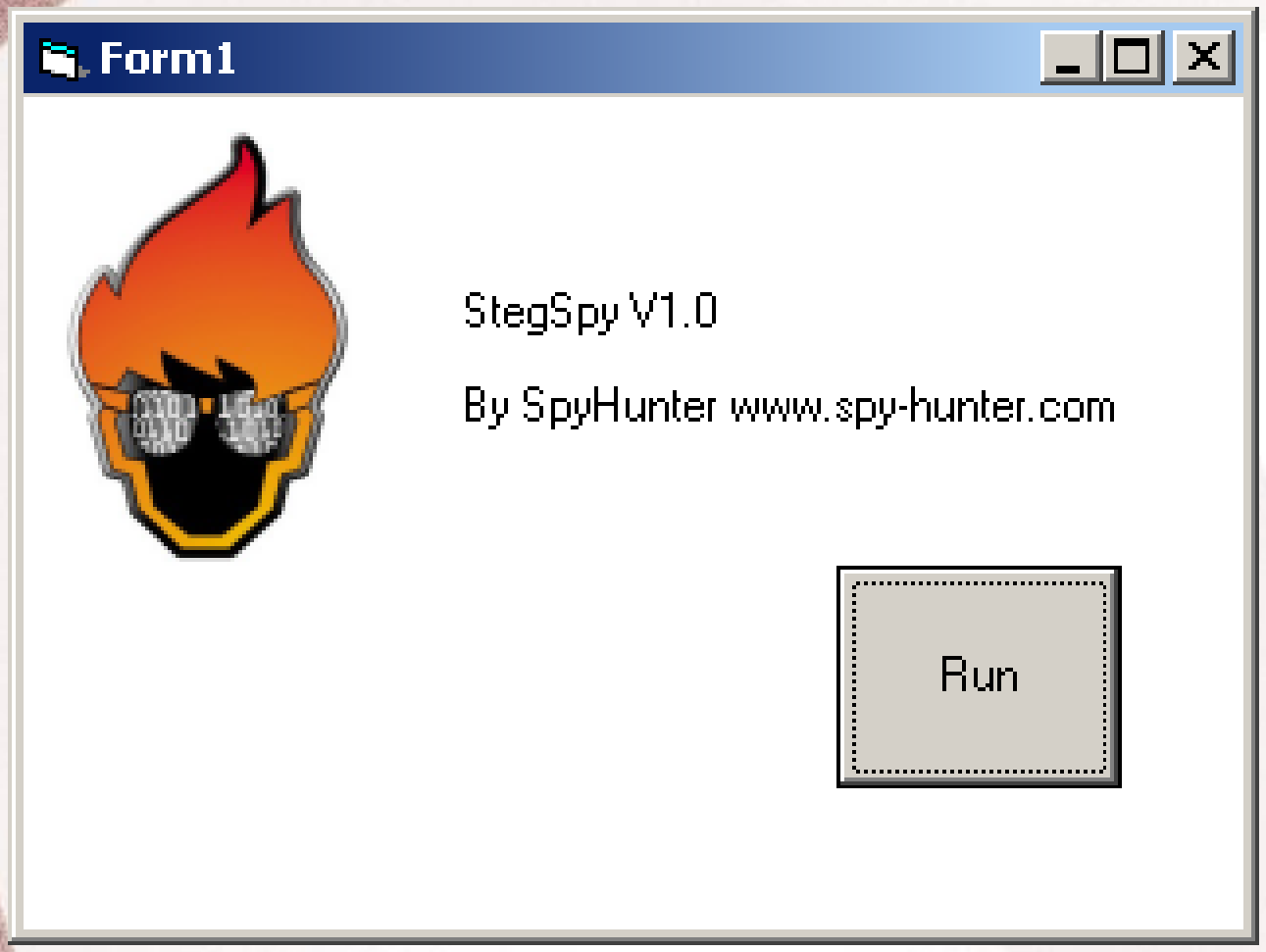
StegSpy V2.0

- **Λογισμικό αναγνώρισης «υπογραφής»**
- **Ερευνά για «υπογραφές» στεγανογραφίας και βρίσκει το πρόγραμμα που χρησιμοποιήθηκε για την ένθεση του μηνύματος.**
- **Έρευνα 13 διαφορετικά λογισμικά στεγανογραφίας**
- **Έυρεση της τοποθεσίας ένθεσης μηνύματος**



Στεγανάλυση – Stegspy V2.0

StegSpy - Demo

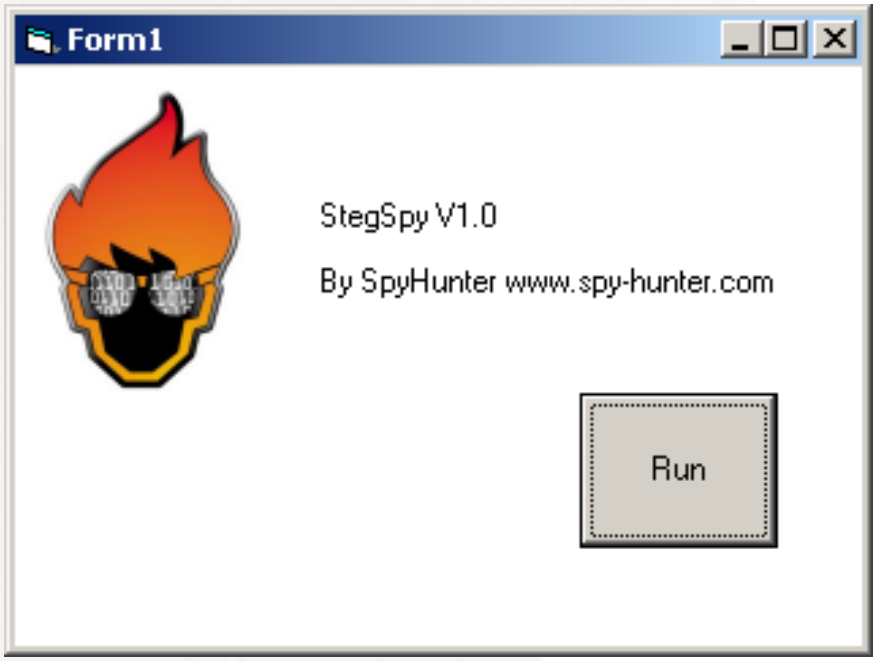


Στεγανάλυση – Stegspy V2.0

StegSpy V2.0

Διαθέσιμο από:

www.spy-hunter.com



Στεγανάλυση – Ανιχνεύοντας μια υπογραφή»

Η στεγανάλυση βασισμένη στην εύρεση «υπογραφής» χρησιμοποιήθηκε για την ανίχνευση υπογραφών μιας πληθώρας λογισμικών μεταξύ των οποίων και τα Invisible Secrets, JPHide, Hiderman, etc.

Στεγανάλυση – Ανιχνεύοντας μια υπογραφή»

Δεν είναι μια τυποποιημένη διαδικασία

Όταν δεν υπάρχει το γνήσιο αρχείο?

Έρευνα για εύρεση προτύπων-«υπογραφών» που θα μας υποψιάζουν για την ύπαρξη κρυμμένου μηνύματος.

Έρευνα για «υπογραφές – πρότυπα» που θα υποδηλώνουν το λογισμικό που χρησιμοποιήθηκε.

Στεγανάλυση και Κρυπτανάλυση

Κρυπτανάλυση

Στη Στεγανογραφία ο σκοπός είναι η απόκρυψη του μηνύματος κι όχι η κρυπτογράφησή του.

Για αυτό το σκοπό είναι η κρυπτογραφία.

Αποκάλυψη του κρυμμένου μηνύματος

Στεγανάλυση και Κρυπτανάλυση

- Η γνώση του προγράμματος στεγανογράφησης κάνει ευκολότερη την αποκάλυψη του πραγματικού κρυμμένου μηνύματος
- Αναγνωρίζοντας και σπάζοντας τον αλγόριθμο κρυπτογράφησης
  - Δυστυχώς κάποια προγράμματα χρησιμοποιούν 128-bit ή ακόμη ισχυρότερη κλείδα – Καλή Επιτυχία!
- Αποκάλυψη του συνθηματικού (password)
  - Πρακτικά, τα περισσότερα προγράμματα στεγανογραφίας, χρησιμοποιούν συνθηματικό.

Στεγανάλυση και Κρυπτανάλυση

Αναγνώριση του λογισμικού που χρησιμοποιήθηκε για την απόκρυψη του μηνύματος.

Αναγνώριση της θέσης της «υπογραφής» του λογισμικού στο αρχείο.

Αναγνώριση της θέσης του συνθηματικού στο αρχείο.

Αναγνώριση της θέσης του κρυμμένου μηνύματος στο αρχείο.

Αναγνώριση του αλγορίθμου κρυπτογράφησης του μηνύματος.

Στεγανάλυση-αποκάλυψη του συνθηματικού

Password Guessing/Dictionary Attacks

Λογισμικό για μάντεμα συνθηματικών:

Stegbreak by Niels Provos, www.outguess.org

J-Steg

Υπάρχει στο Knoppix Penguin Sleuth forensics CD

www.linux-forensics.com

Κρυπτανάλυση: Μέθοδος Εξαντλητικών Ελέγχων (Brute Force)

- Εξαντλητικοί έλεγχοι – Αντίστροφη Μηχανική
- Κοινές τεχνικές κρυπτογράφησης
  - Τροποποίηση του LSB (Least Significant Bit)
  - Το κρύψιμο του συνθηματικού ή των περιεχομένων με τη χρήση ενός αλγορίθμου.
    - Που βασίζεται σε μυστική κλείδα
    - Που βασίζεται σε συνθηματικό
    - Που βασίζεται σε τυχαίο seed κρυμμένο κάπου αλλού στο αρχείο.

Κρυπτανάλυση: Μέθοδος Εξαντλητικών Ελέγχων (Brute Force)

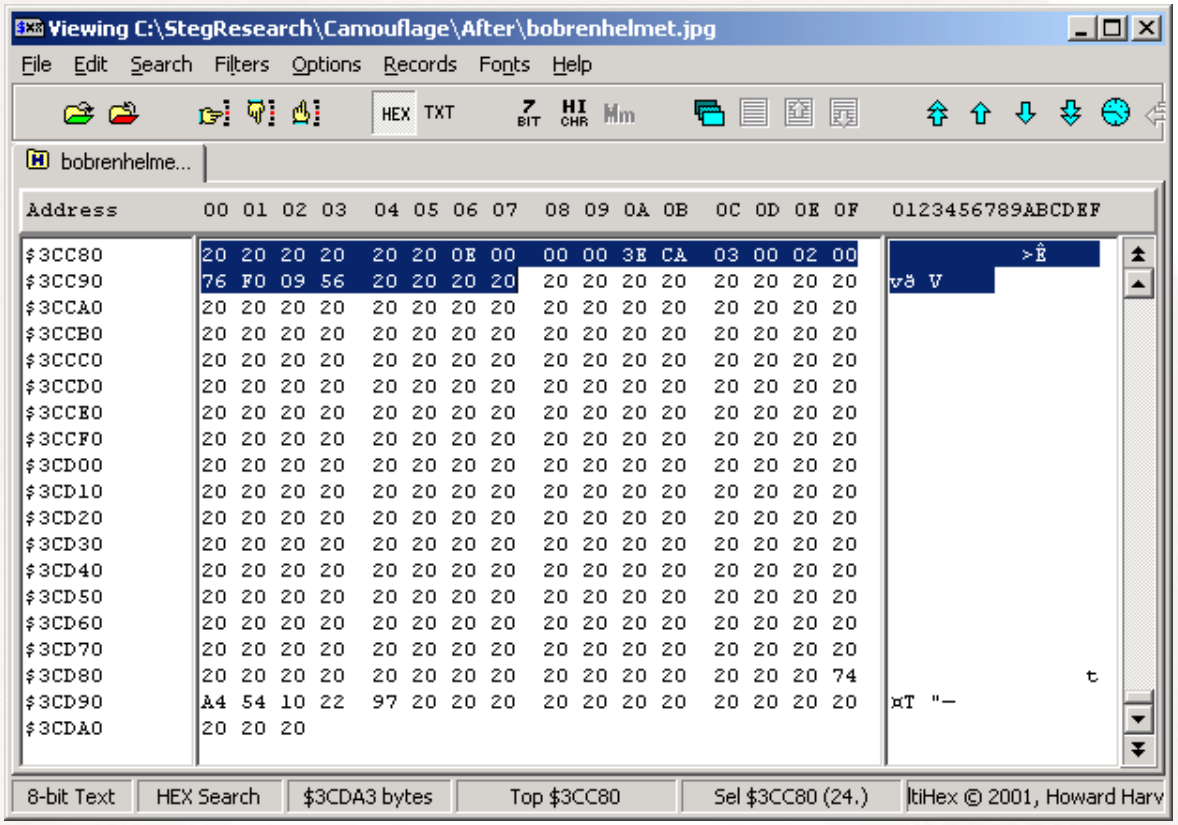
Χρήση συνηθισμένων αλγορίθμων κρυπτογράφησης στα λογισμικά στεγανογραφίας:

- XOR
- DES
- 3DES
- IDEA
- AES

Camouflage – Case Study

Ανιχνεύοντας το συνθηματικό του Camouflage

Η θέση του συνθηματικού ανιχνεύθηκε με το MultiHex που επιτρέπει έρευνα ακολουθίας Hex χαρακτήρων.



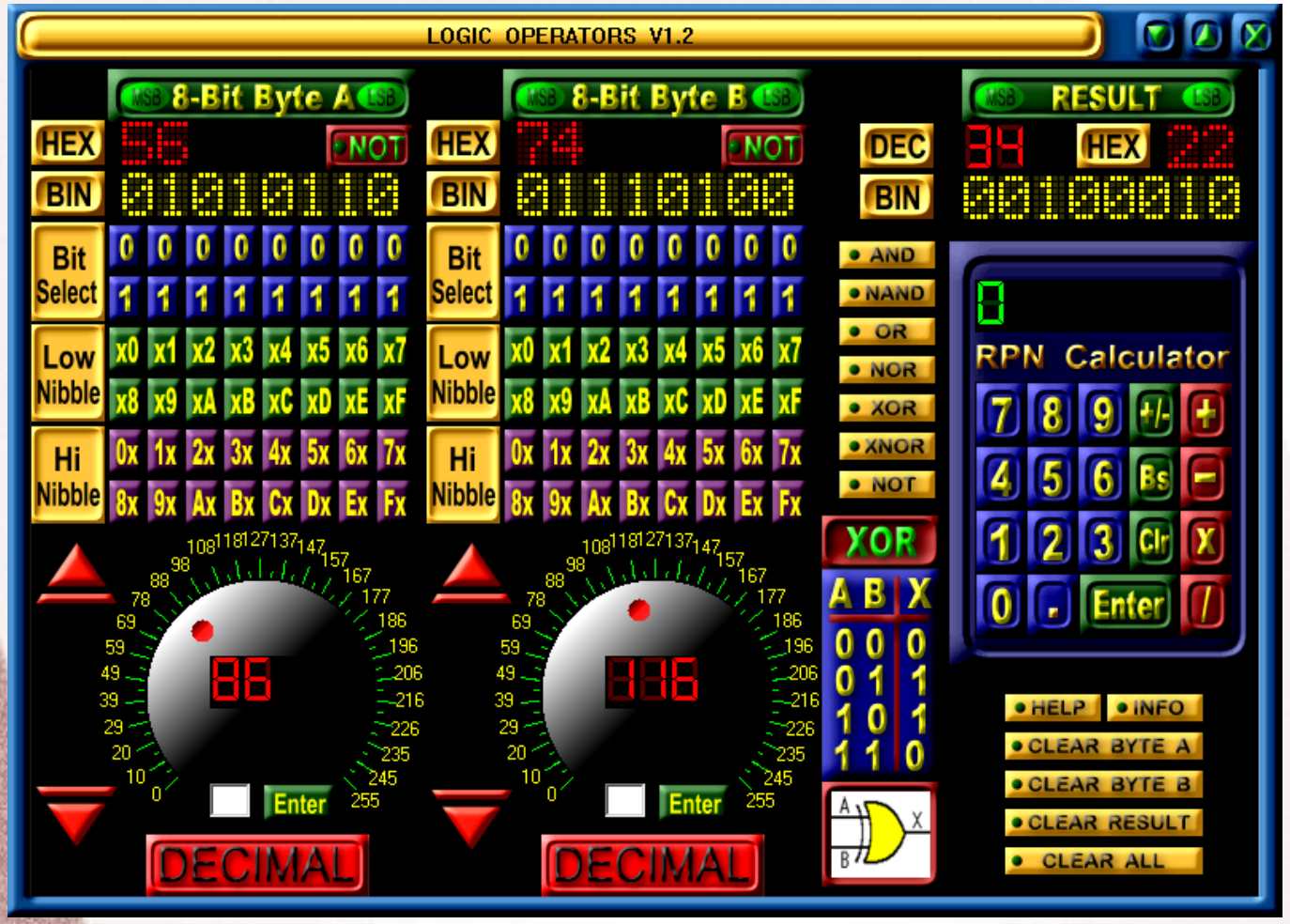
Camouflage

Η ακολουθία ήταν “76 F0 09 56”

Το συνθηματικό είναι γνωστό ότι είναι το “test” που μεταφράζεται σε “74 65 73 74” στο 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

Το πρώτο από τα 4 ψηφία της κλείδας είναι:
"02 95 7A 22"

Έτσι δοκιμάζουμε...

Camouflage

Κρύβουμε ένα άλλο μήνυμα χρησιμοποιώντας άλλο συνθηματικό

Το αρχείο δίνει Hex code of "63 F4 1B 43"

Κάνουμε XOR με το γνωστό κλειδί "02 95 7A 22"

Το αποτέλεσμα είναι "61 61 61 61" που είναι ο κωδικός "aaaa" σε ASCII

Έτσι αποκαλύψαμε το συνθηματικό!

Guillermito at www.guillermito2.net

Forensics/Anti-Forensics

Anti-Forensics

Καλές πρακτικές όταν χρησιμοποιούμε λογισμικό στεγανογραφίας:

- Χρήση διαφορετικού συνθηματικού από εκείνου που χρησιμοποιούμε στο λειτουργικό σύστημα
- Μετά τη δημιουργία της εικόνας με το κρυμμένο μήνυμα να γίνεται ασφαλής διαγραφή του μηνύματος.
- Αφαίρεση του λογισμικού στεγανογραφίας μετά την ένθεση του μηνύματος.
- Ή λειτουργία αυτού από φορητή συσκευή (portable) .
- Χρήση εναλλακτικών ροών δεδομένων

Anti-Forensics – Εναλλακτικές Ροές Δεδομένων

Εναλλακτικές Ροές Δεδομένων

(NTFS) New Technology File System επιτρέπει εναλλακτικές ροές.

Ένα αρχείο μπορεί να συνδέεται με διαφορετικά αρχεία που να αντιστοιχούν το κάθε ένα σε διαφορετική ροή δεδομένων οποιουδήποτε μεγέθους.

Σημαντικό! – Αυτές οι εναλλακτικές ροές δεδομένων είναι κρυφές

Επιτρέπει το κρύψιμο αρχείων ή και φακέλων!

Δυσκολία ανίχνευσης

Δεν εμφανίζονται με το c:\dir

Anti-Forensics – Εναλλακτικές Ροές Δεδομένων

Εναλλακτική ροή δεδομένων

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!

Anti-Forensics – Εναλλακτικές Ροές Δεδομένων

Οι εναλλακτικές ροές δεδομένων μπορούν να χρησιμοποιηθούν για την απόκρυψη ιδιωτικών αρχείων, viruses and trojans!

Anti-Virus/Anti-Trojan Test - Does your scanner pass the test?

Με το MakeStream, μπορούμε να συνδέσουμε έναν ιό ή έναν δούρειο ίππο με ένα κρυμμένο αρχείο που αποτελεί εναλλακτική ροή δεδομένων συνδεδεμένη σε ένα «αθώο» αρχείο κειμένου.

Παράδειγμα, αν τρέξει κανείς το **makestrm.exe c:\test.exe**, τα περιεχόμενα του αρχείου c:\test.exe μετακινούνται στο c:\test.exe:StreamTest (Μια εναλλακτική ροή δεδομένων αρχείου), ενώ τα περιεχόμενα του πρωτότυπου αρχείου, τροποποιούνται με ένα απλό μήνυμα που απλά υπενθυμίζει τη συνδεδεμένη ροή.

Αν πάρουμε ένα αρχείο ιού ή δούρειου ίππου που ανιχνεύθηκε με το αντιικό λογισμικό μας, και τρέξουμε το makestrm.exe σε αυτό ώστε να οδηγήσουμε το περιεχόμενο σε εναλλακτική ροή, εξακολουθεί το αντιικό μας λογισμικό να ανιχνεύει τον ιό ή τον δούρειο ίππο?

Πολλά εμπορικά αντιικά λογισμικά ***δεν*** ανιχνεύουν ιούς και δούρειους ίππους κρυμμένους σε ADS!

http://www.diamondcs.com.au/web/streams/streams.htm

Forensics

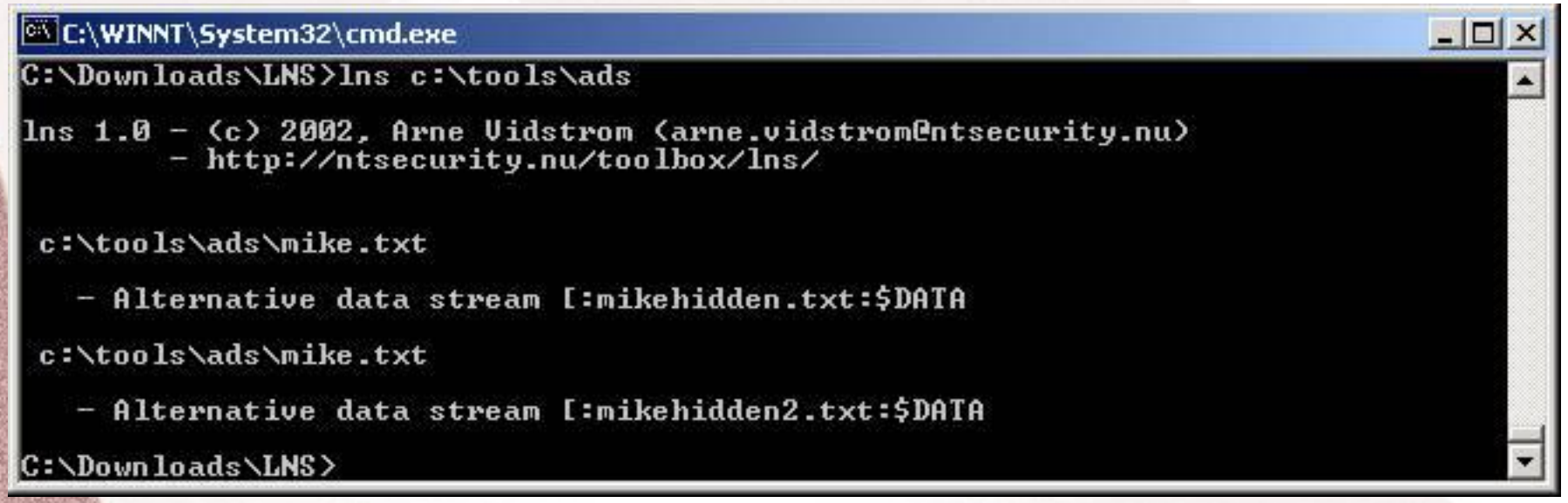
Εάν κάνοντας έρευνα ευρεθεί ένα πιθανώς στεγανογραφημένο αρχείο:

- Εξετάζουμε για ίχνη λογισμικού στεγανογραφίας στον Η/Υ
- Εκμεταλλευόμαστε συνθηματικά άλλων λειτουργικών συστημάτων και εφαρμογών που πιθανώς βρήκαμε καθώς ενδεχομένως αυτά μπορεί να χρησιμοποιήθηκαν για τη στεγανογραφία.
- "Electronic Crime Scene Investigation – A Guide for First Responders, U.S. Dept of Justice"

Forensics – Alternate Data Streams

Εργαλεία για ανίχνευση Alternate Data Streams

- LNS – www.ntsecurity.nu
- LADS - www.heysoft.de
- NTFS ADS Check - www.diamondcs.com.au



Το μέλλον της Στεγανάλυσης?

Εξέλιξη

Πληθώρα λογισμικών: πχ το StegSpy για την ώρα ανιχνεύει JPHide, Hiderman, and Invisible Secrets. Εμφάνιση και άλλων

Εμφάνιση Ανιχνευτών συνθηματικών (Το stegbreak ήδη διατείθεται)

Επέκταση της Στατιστικής Ανάλυσης για ανίχνευση στεγανογραφίας (histogram, LSB, etc).

Άλλα εργαλεία για Στεγανάλυση

Η Wetstone Technologies προσφέρει το Stego Watch

Ανιχνεύει τη στεγανογράφηση σε αρχείο μέσω στατιστικής και άλλου είδους ανάλυσης.

Ακριβές και εύχρηστο εργαλείο ($$$)

Δεν επιχειρεί την αποκάλυψη του κρυμμένου μηνύματος, απλά αναδεικνύει την ύπαρξή του.

Προσφέρει εκπαίδευση Steganography Investigator Training Course

See http://www.wetstonetech.com

Άλλα εργαλεία για Στεγανάλυση

Stegdetect by Niels Provos

Διαθέσιμο: http://www.outguess.org/detection.php

Ανιχνεύει:

- jsteg
- jphide (unix and windows)
- invisible secrets
- outguess 01.3b
- F5 (header analysis)
- appendX and camouflage

Για κάποιο λόγο η ιστοσελίδα δεν ήταν διαθέσιμη εξαιτίας της νομοθεσίας της πολιτείας του Michigan.

Αναφορές

Steganographica, Gaspari Schotti, 1665

Disappearing Cryptography, Peter Wayner, 2002

Hiding in Plain Sight, Eric Cole 2003

Steganography – presentation Chet Hosmer, Wetstone Technologies, TechnoSecurity 2003

Υπόβαθρο

Η ***στεγανογραφία*** είναι μια σχετικά νέα επιστήμη, που φυσικά βασίζεται στην πολύ καλή εξειδικευμένη γνώση των ψηφιακών πολυμέσων, της επιστήμης των Η/Υ και φυσικά επεξεργασία σήματος, αναγνώριση πρωτύπων, έμπειρα συστήματα κα
σε συνδυασμό με
πολύ καλή γνώση του σχετικών μαθηματικών εργαλείων που τη συνοδεύουν.

Η ***στεγανάλυση*** απαιτεί ακριβώς τα ανωτέρω σε συνδυασμό με μια καλή και εμπεριστατωμένη επιστημονική γνώση των νέων τεχνικών στεγανογραφίας που δημοσιεύονται και υλοποιούνται, σε συνδυασμό με καλή γνώση τόσο ως προς την εφαρμογή, όσο και στα όρια των υπαρχόντων σήμερα εργαλείων

Τεχνικές Στεγανάλυσης

- Τεχνικές Στεγανάλυσης που αφορούν αποκλειστικά συγκεκριμένο αλγόριθμο στεγανογραφίας
  - Παρέχουν ικανοποιητική ανίχνευση για τη συγκεκριμένη τεχνική
  - Δεν ενδείκνυνται για τις υπόλοιπες περιπτώσεις στεγανογραφίας

- Γενικευμένες Τεχνικές Στεγανάλυσης
  - Λιγότερο αποδοτικές σε ανίχνευση από τις εξατομικευμένες
  - Ενδείκνυνται ακόμη και για περιπτώσεις στεγανογραφίας που εφαρμόζεται τελείως νέα τεχνική

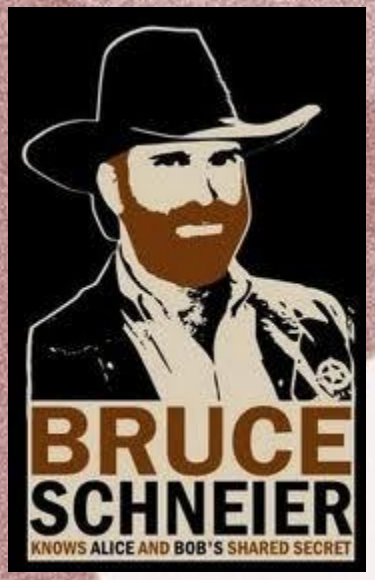
Τεχνικές Στεγανάλυσης

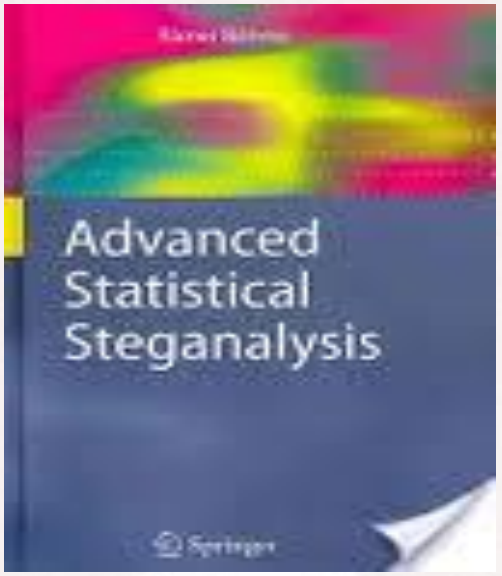
Stego-only attack	Επίθεση με γνωστό μόνο το στεγανογραφημένο μέσο
Chozen stego-attack	Ο αλγόριθμος στεγανογραφίας είναι γνωστός και είναι διαθέσιμο και το στεγανογραφημένο μέσο
Known cover attack	Είναι γνωστό το στεγανογραφημένο μέσο και το πρωτότυπο
Known stego-attack	Είναι γνωστός ο αλγόριθμος στεγανογραφίας, το πρωτότυπο και το στεγανογραφημένο μέσο
Message attack	Ο Στεγαναλυτής, γνωρίζει τόσο το μήνυμα, όσο και το στεγανογραφημένο μέσο
Chozen-message attack	Ο Στεγαναλυτής, γνωρίζει τον αλγόριθμο στεγανογραφίας και το επιλλεγμένο μήνυμα

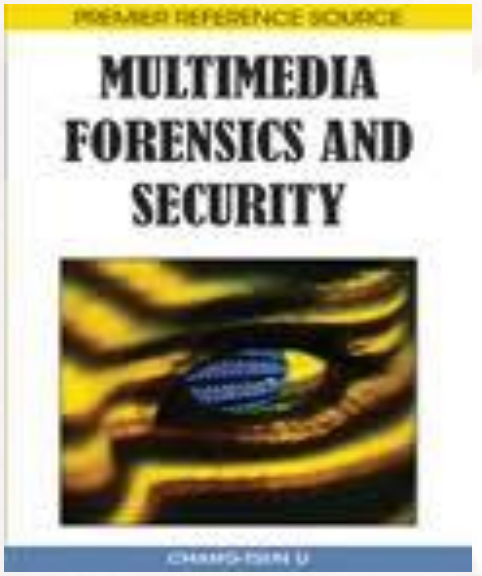
Τεχνικές Στεγανάλυσης

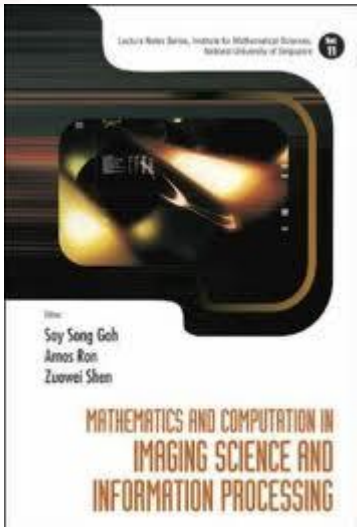
Είναι κατανοητό, πως η Στεγανάλυση είναι στην ουσία μια επιστήμη που βασίζεται σε υψηλού επιπέδου **ΑΝΑΓΝΩΡΙΣΗ ΠΡΩΤΥΠΩΝ**

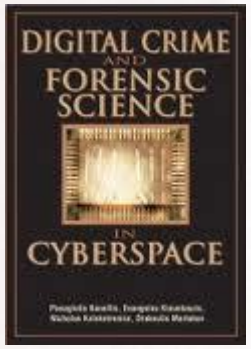
Στεγανάλυση Εικόνας

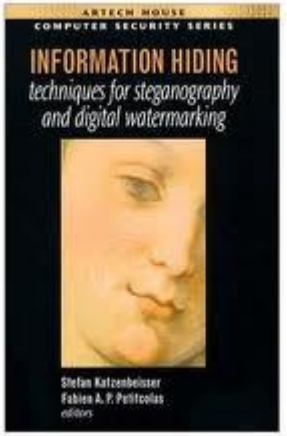


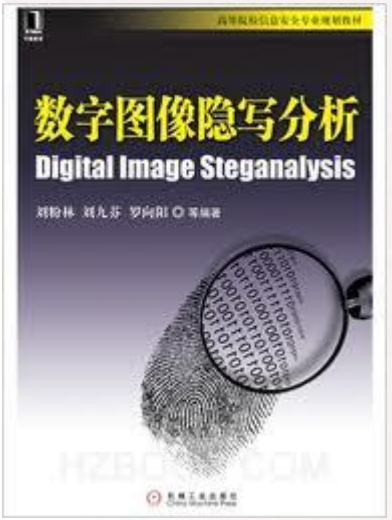












Στεγανάλυση Εικόνας

LENA

CAMERAMAN

Λίγη Ιστορία...

Το φεβρουάριο του 2001 ο Jack Kelly, έγραψε δύο άρθρα στην USA TODAY, που λίγο έως πολύ, ισχυριζόταν ότι ο Osama Bin Landen και αρκετά παρακλάδια της Al-Qaeda, επικοινωνούσαν μεταξύ τους με στεγανογραφία, αναρτώντας σε δημόσια sites όπως το e-bay, το Amazon, chat-rooms και φυσικά ιστοσελίδες πορνογραφίας.

...λίγη Ιστορία

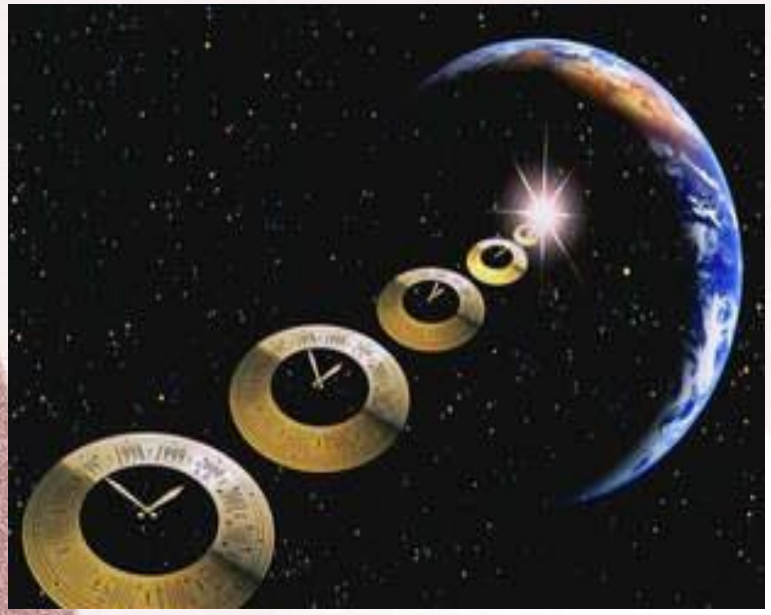
Το άρθρο του Jack Kelly ακολούθησαν και άλλα σε άλλες εκδόσεις, κανένα από τα οποία δεν έδινε σαφείς αναφορές ή αποδεικτικά στοιχεία, παρά κυρίως βασίζονταν σε εικασίες στελεχών μυστικών υπηρεσιών.

...λίγη Ιστορία...

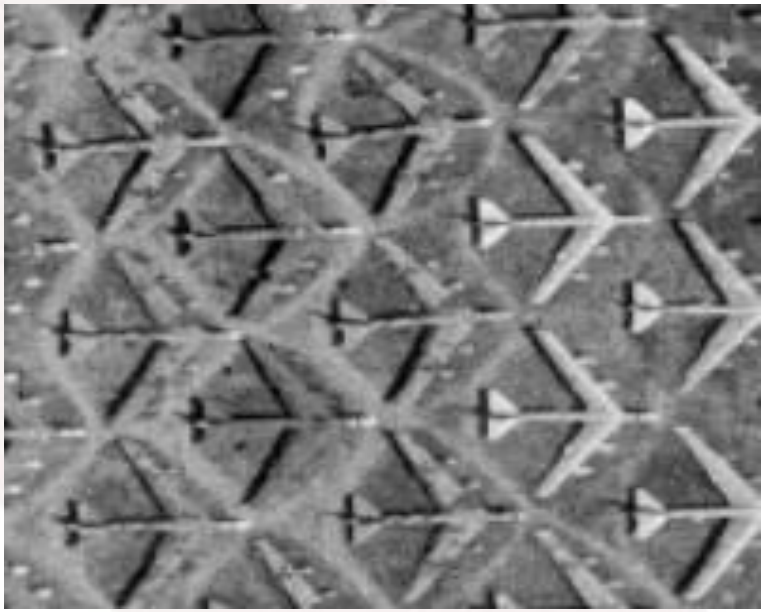
Βασισμένοι σε αυτές τις αναφορές, οι Niels Provos and Peter Honeyman, ερευνητές του University of Michigan, ξεκίνησαν ένα project, ώστε να διερευνήσουν την βαρύτητα αυτών των δημοσιευμάτων
Στις 31 Αυγούστου 2001, δημοσίευσαν μια εργασία παρουσιάζοντας τα εργαλεία στεγανάλυσης που είχαν αναπτύξει (Stegdetect, Stegbreak,
Crawl and Disconcert) ώστε να ερευνηθούν αυτόματα 2 εκατομύρια φωτογραφίες στην ιστοσελίδα e-bay.

...συνέχεια της ιστορίας

...μέχρι το τέλος του έτους 2001, μόνο μια φωτογραφία ανακαλύφθηκε η οποία περιείχε στεγανογραφημένη μια άλλη φωτογραφία. Ήταν σε μια καταχώρηση άρθρου της ABC συμβούλων του internet με θέμα ακριβώς τη στεγανογραφία!



sovereigntime.jpg



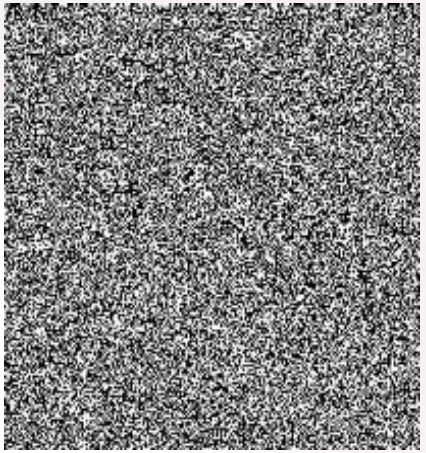
B-52 graveyard" at Davis-Monthan Air Force Base

LSB Embedding

Τεχνικές στεγανάλυσης εικόνας







Στεγανάλυση LSB Embedding

PoV Steganalysis: Westfeld and Pfitzmann
RS Steganalysis: Fridrich
LSB steganalysis with primary sets: Dumitrescu, Wu, Memon
Ανίχνευση τοπικών χαρακτηριστικών: πχ σε μια κανονική εικόνα μια αλλαγή σε έναν συντελεστή LSB δημιουργεί το πολύ 4 γειτονικά χρώματα, ενώ στα στεγανογραφημένα της τάξης του 20 και άνω...

Γενικές τεχνικές στεγανάλυσης εικόνων

Βασίζονται στην τεχνική του να βρει κάποιος ένα συγκεκριμένο χαρακτηριστικό στην εικόνα το οποίο είναι ευαίσθητο και η όποια αλλοίωσή του προδίδει την στεγανογραφία.
Πχ Ένα καλό σύνολο μέτρων ονομάζεται Image Quality Metrics (IQM)

Αντίμετρα

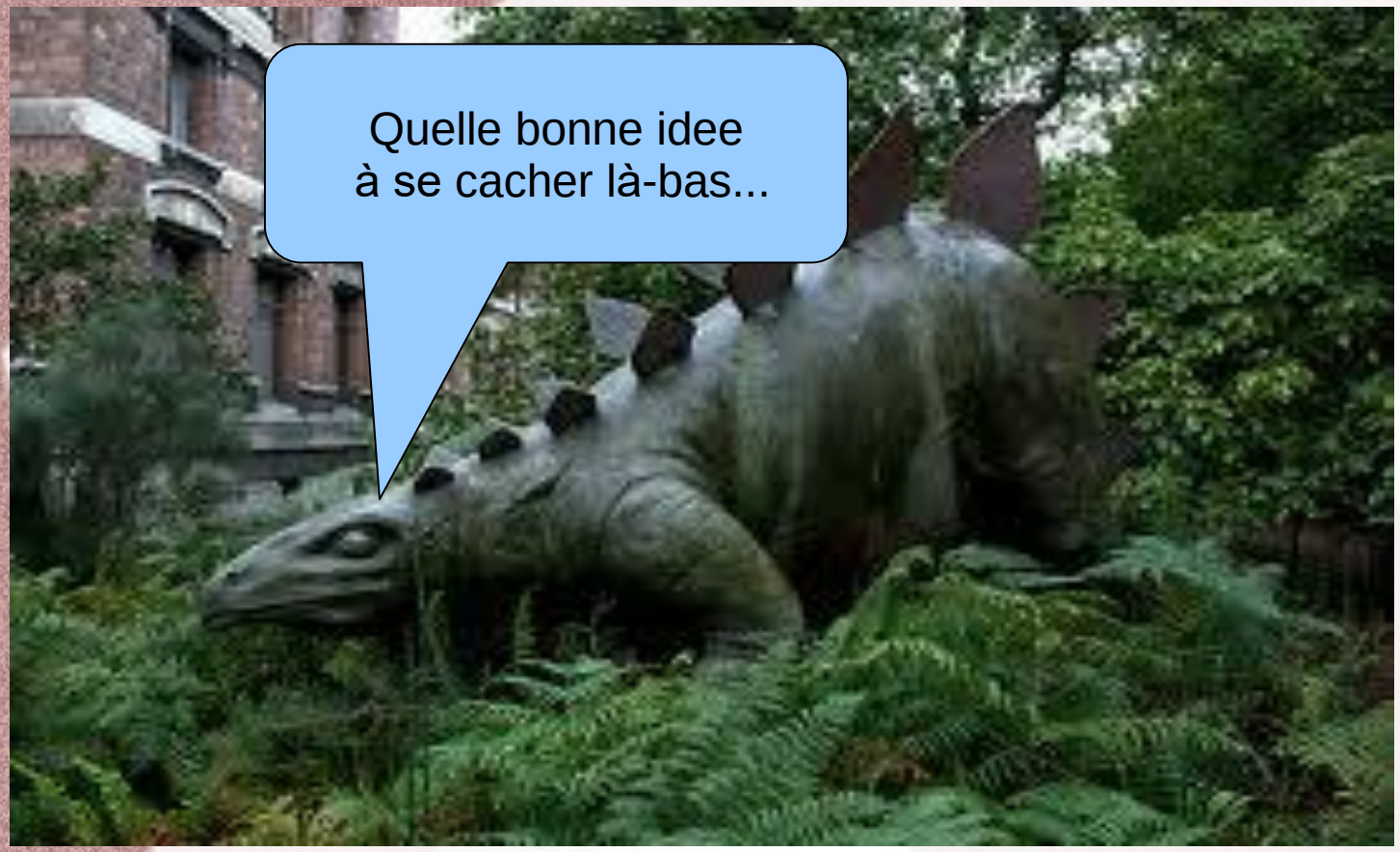
Στεγανογραφία:

- Εισαγωγή θορύβου στα μέσα-φορείς με χρήση διαφόρων ειδών προσαρμοστικού θορύβου.
- Στεγανάλυση

Στεγανάλυση:

- Χρήση λακωνικών μηνυμάτων
- Χρήση ένθεσης βασισμένης σε μοντέλα (Stochastic Modulation-Fridrich, προσαρμοστικά μοντέλα-Phil Salle)
- Adaptive embedding
- Active embedding (προσθήκη θορύβου μετά την ένθεση, προσθήκη ψευδού ίχνους)

ΣΤΕΓΑΝΟΣΑΥΡΟΣ



ΤΕΛΟΣ...