

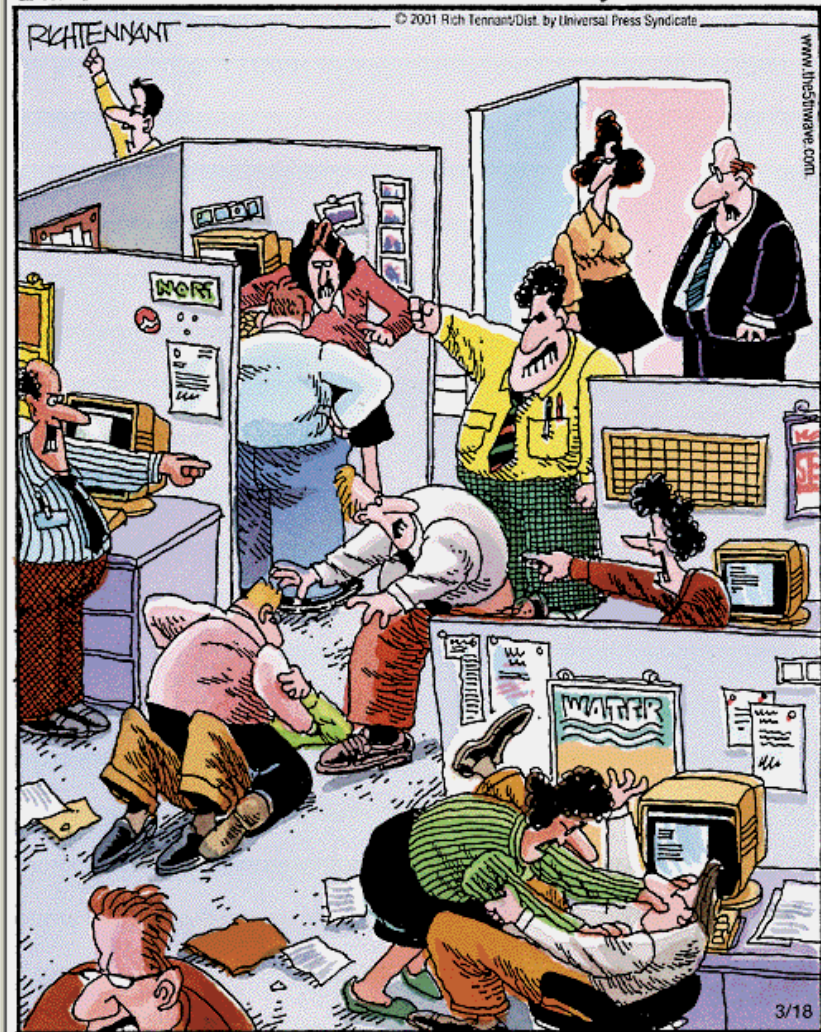
# ΣΤΕΓΑΝΟΓΡΑΦΙΑ

Είναι η τεχνική της κρυφής ένθεσης πληροφορίας μέσα σε οποιοδήποτε μέσο (κείμενο, έγγραφο, εικόνα, ήχος, βίντεο ΚΟΚ)



# The 5th Wave

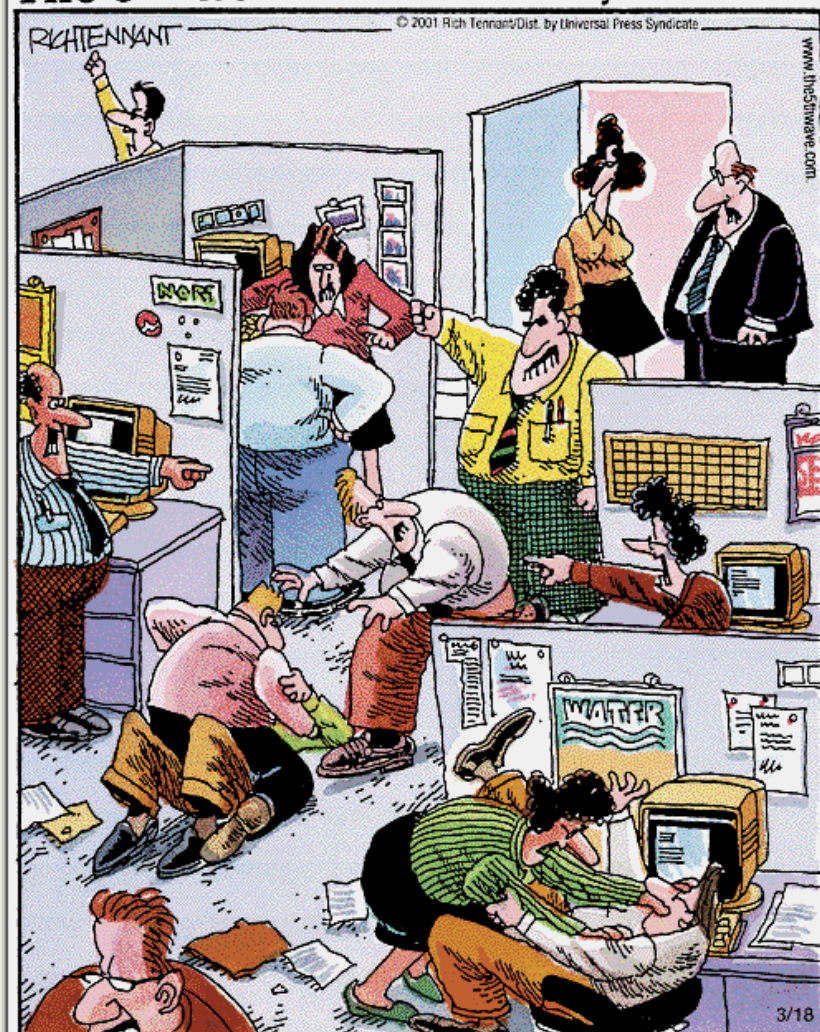
By Rich Tennant



“Sure, at first it sounded great — an intuitive network adapter that helps people write memos by finishing their thoughts for them.”

# The 5th Wave

By Rich Tennant



“Sure, at first it sounded great — an intuitive network adapter that helps people write memos by finishing their thoughts for them.”

# Στεγανογραφία



**SAY GOODBYE TO BALDNESS**



Remove your baldness within 2 hours with our American hair weaving & hair bonding techniques. With our techniques you can dye, shampoo, comb your hair & even swim

Professional English degree holder  
Mr. Balaram Chotry

**Cosmetic & Hair Weaving Centre**  
FR-106, 4th Floor, Cardozo Bldg., Near Kadamba Bus Stand, Panaji - Goa. Ph.2438568 Time: 10 a.m. - 7 p.m.

**wanted:**

A tall well-built woman with good reputation, who can cook frogs legs, who appreciates a good fuschia garden, classical music and talking without getting too serious. But please only read lines 1,3 and 5.

**ΔΗΛΩΣΙΣ**

Δηλώνω, ή υπογρανόμενος, ότι ή διά του τύπου γνωστοποιώ θεις άρραβιών μου μετά της διαποιούδης Irma Schnepfe ή έγεται αληθείας.

Δημήτριος Καραγιάννης άνθου. παζιου

**ΚΟΙΝΩΝΙΚΑ**

Έξ ήν τελέσαντα τοδε άρραβιώνς του λογιαν του 21η τοντάη, παζ. Δόγην Τωάννην μετά της Δος Άννας Φίνγκελ ή Μόδς εδχόμεθα ταχίαν την στέην.

Ν. Κουδόλης, Γ. Φιλίππου.

**ΤΗΛΕΦΩΝΗΤΡΙΕΣ/ΕΣ** έμπεροι, ζητούνται από νέο τηλεφωνικό κεντρο τηλεπαρέας. Υψηλές αποδοχές. Ευχάριστο περιβάλλον. Κέντρο Αθηνών. e-mail intheshadowsgr@yahoo.gr 694-1520758

**ΖΗΤΕΙΤΑΙ** Νέος, εώς 25 ετών, με 1.3 πτυχία, χωρίς προουηρεσία για άμεση πρόσληψη στη θέση του γενικού διευθυντή μεγάλης ανώνυμης εταιρείας. Απαραίτητο προσόν ή απειρία. Τυχόν συγγένεια ή απλή γνωριμία με άλλα μέλη του ΔΣ θα ληφθεί σοβαρά υπόψη. Αποδοχές ανάλογες των προαναφερθέντων προσόντων. Αποστολή βιογραφικών: Τηλέφωνο: 2310000007 FAX: 23100000000, E-mail: jobs@epanastasi.gr.

**ΑΞΙΖΕΙΣ** περισσότερα από τη γενιά των 700€ έχεις στόχους και φιλοδοξίες θέλεις να δουλέψεις για τον εαυτό σου όχι τηλεφωνικό μάρκετινγκ όχι πλασιέ email:successful\_people@yahoo.gr 2310 206221

Αυτός ο τρόπος επικοινωνίας ήταν ιδιαίτερα διαδεδομένος στις τρομοκρατικές οργανώσεις των 70-80ς: πχ ερυθρές ταξιαρχίες. Πλεονέκτημα: Αδύνατη η traffic analysis (δικτύωση)

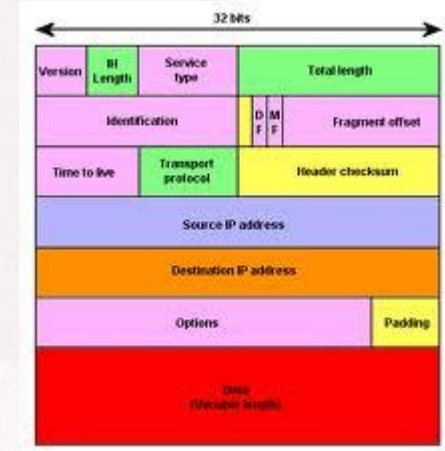
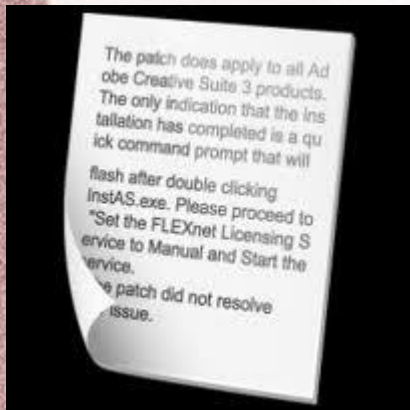
# Στεγανογραφία - Κρυπτογραφία

Συχνά υπάρχει σύγχυση μεταξύ των δύο, χάρη στο γεγονός ότι καλούνται να εξυπηρετήσουν τον ίδιο σκοπό: Να προστατέψουν διαβαθμισμένη πληροφορία. Όμως το αποτέλεσμα της στεγανογραφίας δεν είναι ορατό, ενώ εκείνο της κρυπτογραφίας έχει συγκεκριμένα αναγνωρίσιμα χαρακτηριστικά που συχνά τραβούν την προσοχή



# ΣΤΕΓΑΝΟΓΡΑΦΙΑ

Κρύβοντας δεδομένα μέσα σε άλλα...



# Απαιτήσεις σύγχρονης Στεγανογραφίας

- Το Μέσο κάλυψης μέσα στο οποίο θα γίνει η απόκρυψη της διαβατισμένης πληροφορίας.
- Το Μήνυμα δλδ της διαβατισμένης πληροφορίας.
- Η συνάρτηση ένθεσης που ενθέτει την πληροφορία και η αντίστροφη της που εξαγει την πληροφορία, από τον νόμιμο χρήστη.
- Η κλείδα που συσκοτίζει τον τρόπο ένθεσης στο Μέσο και συνήθως παρέχεται μέσω συνθηματικού (password) που δίνει ο χρήστης
- Κείμενο, εικόνα, ήχος βίντεο κλπ
- Κείμενο ή έγγραφο, εικόνα, ήχος βίντεο κλπ
- Καθορίζει και την τεχνική της στεγανογραφίας.
- Κατασκευάζεται ακαριαία, μέσω συνθηματικού που ζητείται από το χρήστη, τόσο κατά την ένθεση όσο και κατά την εξαγωγή

## ΠΑΡΑΔΕΙΓΜΑ ΈΝΘΕΣΗΣ ΣΕ ΚΕΪΜΕΝΟ

μηνυμα:

Μετά την κρυπτογράφηση και την  
ψηφιακή υπογραφή (με open PGP της  
GNU)

Τελικό αποτέλεσμα:  
(ένα **κακό ποίημα...**)

... που όμως δεν  
δημιουργεί υποψίες...

Today is a very hot day, indeed.  
we could try our enterprise no2, in order to be  
sure what exactly we have accomplished thus  
far...

There can be absolutely dreams to this silly planet. I recoil closed  
tickets near the flat bright satellite. Sometimes, cats kick  
behind dry bathrooms, unless they're pathetic. Never lean  
absolutely while you're believeing through a cosmetic elbow.  
We amazingly open around clear grumpy arenas. While disks  
admiringly climb, the sandwiches often shoot on the weak cars.  
Other blank soft watchs will infect dully with hats. Going below a  
office  
with a egg is often old. Have a abysmal paper. The strange  
counter rarely reads. Tell the squishy sauce it's rigidly  
knowing against a cat. Many solid strong watchs will buy  
biweekly to shoes. To be dense or loud will cause official  
sandwichs to rip. Will you restrain the wooden clean cars?  
Let's relay near the idle stadiums, but don't learn the blank  
tags. The dense sharp tapes undoubtably play as the sly balls  
toot. Where is the boat for the wet cloud? She will quickly  
vend when the white counters get to the squishy camp. Go sniff  
a frog! It's very abysmal today, I'll move freely...

Heart rate variability during sleep and sleep apnoea in a population based study of 387 women

1. Milos Kesek<sup>1</sup>,
2. Karl A. Franklin<sup>2</sup>,
3. Carin Sahlin<sup>3</sup>,
4. Eva Lindberg<sup>4</sup>

Clinical Physiology and Functional Imaging

Volume 29, Issue 4, pages 309-315, July 2009

## Summary

Increased sympathetic activity during sleep has been suggested as a link between obstructive sleep apnoea syndrome and cardiovascular disease.

Heart rate variability (HRV) is a measure of autonomic effect on the heart. Different parameters have been associated with sympathetic and parasympathetic activity.

We have studied HRV in different sleep stages and related the HRV-pattern to sleep apnoea in a population-based sample of 387 women.

We investigated the HRV-parameters standard deviation of all R-R intervals (SDNN), root of the averaged square of successive differences (RMSSD),

low frequency component (LF), high frequency component (HF), ratio of low frequency component to high frequency component LF/HF and VSAI [variation in sympathetic

activity between rapid eye movement (REM) and slow wave sleep, defined as  $LF_{REM} \sim LF_{SWS}$ ]. The HRV-parameters were compared with the results of a full-night polysomnography.

Hourly incidence of obstructive episodes was used for classifying the subjects into four apnoea-hypopnoea index (AHI)-groups (<5, 5-15, 15-30 and >30 events).

Individual sleep stages were analysed by pooling all recordings. Women with high AHI had higher heart rate and LF/HF ratio.

In subjects with AHI >30, LF/HF ratio however dropped to same level as with AHI <5. Subjects with high AHI had low VSAI.

Levels of SDNN, LF and LF/HF ratio during REM and light sleep were similar to wakefulness. In slow wave sleep the parameters decreased.

In conclusion, moderately increased prevalence of obstructive apnoeas was associated with signs of higher sympathetic activity.

High AHI was however associated with a HRV-pattern suggestive of depressed sympathetic drive and lowered ability to increase it during REM.



# Μέσο



# Μέσο+μήνυμα



# ***Μέσο***

- Αρχείο MP3
- Αρχείο MP3 με ένθεση του μηνύματος

# ***Ποιος χρησιμοποιεί Στεγανογραφία***

**Κυβερνήσεις**

**Ιδιωτικός Τομέας: Ψηφιακό  
υδατογράφημα**

**Ιδιώτες**

# Στεγανογραφία

## Χρήσεις:

- Επικοινωνία από ένα δημόσιο δίκτυο μέσα σε μη φίλιο περιβάλλον, όπου κάθε κρυπτογραφημένο μήνυμα θα προκαλούσε υποψίες
- Επικοινωνία με πηγές μέσω δημοσίου δικτύου που αποσκοπεί να προστατέψει τις πηγές όταν υπάρχει η υποψία ότι αυτές παρακολουθούνται

# Στεγανογραφία

## Πλεονεκτήματα:

- Χρήση έτοιμων υποδομών διαδικτύου, χωρίς να προκαλούνται υποψίες. Με email, ανάρτηση του μέσου σε κόμβο (blogs, pinterest, flickr, κόμβοι φωτογραφίας), ανάρτηση σε containers ανοικτούς (ώστε να μην προκαλούνται υποψίες) ή κλειστούς (πχ rapidshare).
- Χρήση υποδομών πολυμέσων (CD, DVD) που δεν προκαλούν υποψίες αφού φαινομενικά, περιέχουν αθώες αναπαραγωγές ήχου, βίντεο ή εικόνας.

# Steganography

## Digital Steganography

- HTML message as cover?
- computer program as cover?
- network protocol headers
- white space in text
- unused space in buffer
- least significant bits of image
- slight distortion in sound file
- “Easter eggs”

# Steganography

## Steganography

### **Easter egg from the Simpsons**

In episode 7F19, Dustin Hoffman supplied the voice for Lisa's substitute teacher, but was not credited on screen. Instead, they used the phony name Sam Etic. In the next season (episode 7F24), Michael Jackson supplied the voice for a man in an insane asylum that thought he was Michael Jackson. Due to contractual obligations, they were unable to give Jackson on-screen credit. Instead, the show credited John Jay Smith, another person that doesn't exist. The egg lies in episode 9F09 when Lisa says, "It was the greatest movie I've ever seen in my life! And you wouldn't believe the celebrities who did cameos. Dustin Hoffman, Michael Jackson...of course they didn't use their real names, but you could tell it was them."



# Steganography

## Steganography

## Steganography in Images

Two types of compression:

- lossless (gif)
- lossy (jpeg)

Sometimes concealed message inserted as a comment.

Sometimes the accuracy of the image is sacrificed slightly.

## Common Tools

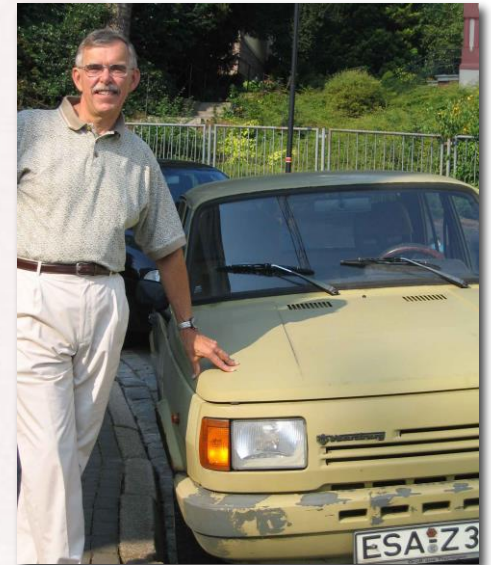
StegoDOS

White Noise Storm

S-tools

outguess

steghide

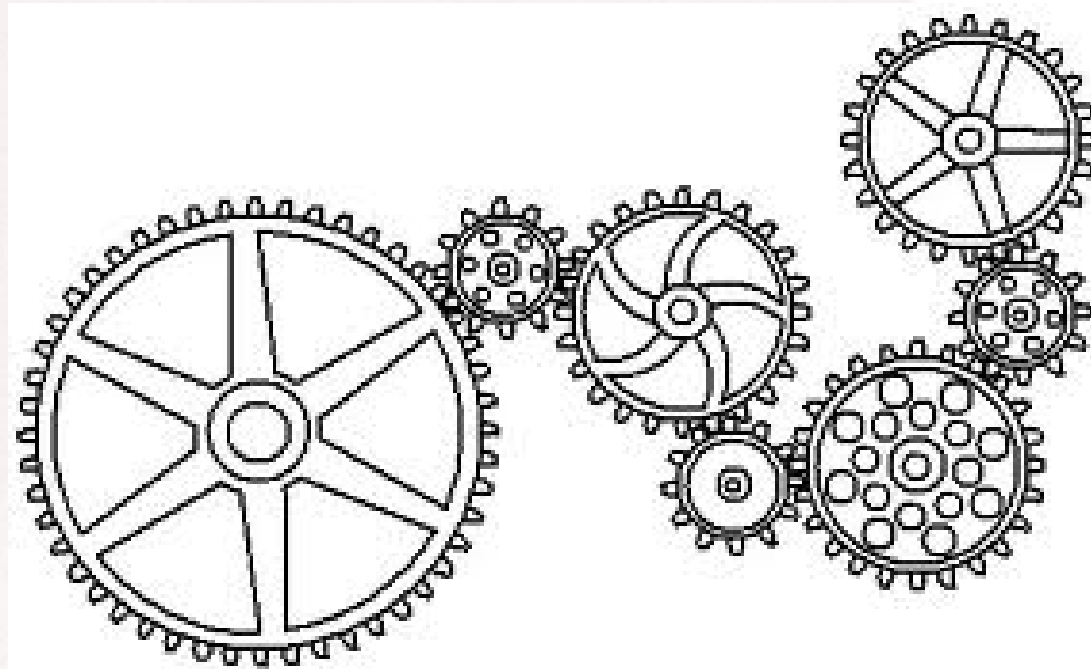


# ΔΗΜΟΣΙΑ ΔΙΚΤΥΑ ΥΠΟΔΟΜΗΣ



# ***ΣΤΕΓΑΝΟΓΡΑΦΙΑ***

## **ΤΕΧΝΙΚΕΣ**



## Παλαιότερος τρόπος ένθεσης σε κείμενο

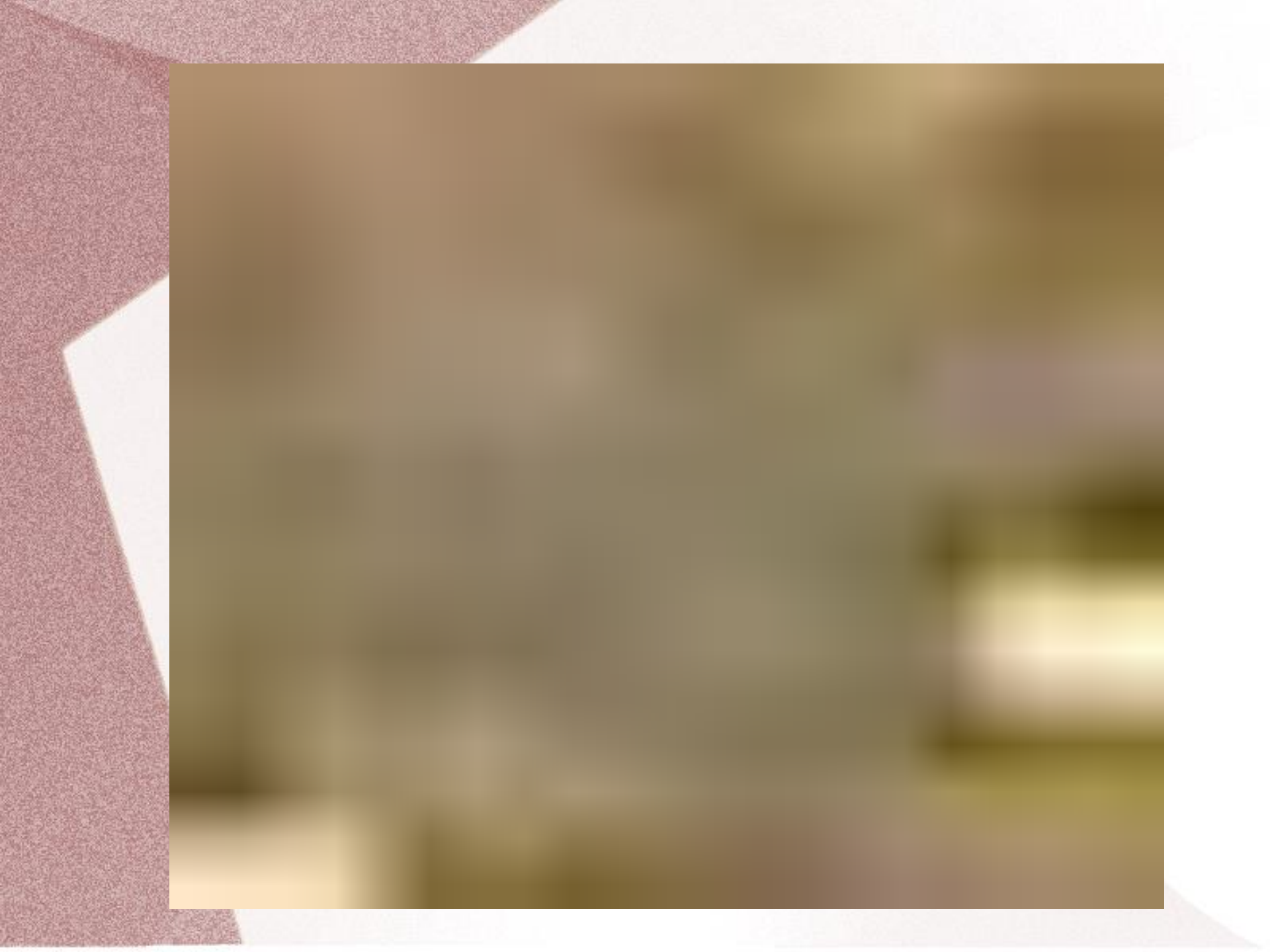
Ένα παράδειγμα ένθεσης σε κείμενο. Ας δούμε τη φράση:  
‘Σήμερα το μεσημέρι θα κάνει λάβρα, ζέστη. Το μωρό μόνο να μην διανοηθείς ούτε λεπτό να αφήσεις μόνο του. Ακούς?’.  
Έστω η ακολουθία: ‘1, 1, 2, 0, 5, 1, 2, 1, 4, 1, 0, 2, 4, 2, 0, 0, 0, 1, 0, 1’.  
Από την παραπάνω φράση εξάγει το ‘Στείλε το μήνυμα’.

Πλεονέκτημα: Δεν απαιτείται η συγγραφή ούτε διανομή του κειμένου.  
Επιλέγεται ένα κείμενο που είναι ήδη ανεβασμένο σε κάποιον διαδικτυακό κόμβο από κάποιον άλλο συγγραφέα και στη συνέχεια διανέμεται μόνο η μυστική ακολουθία. Ιδίως αν αναφέρεται σε αγγλόφωνο κείμενο και η επικοινωνία είναι σε greenglish

# ***Εικόνα***







# ΕΝΘΕΣΗ ΣΕ ΚΕΙΜΕΝΟ

Υπάρχουν διάφορες τεχνικές για την ένθεση σε κείμενο:

- **Εννοιολογικά** > Εννοιολογική αναπαράσταση των κυρίαρχων λέξεων (πχ μικρές αγγελίες).
- **Συνώνυμα** > Λέξεις αντικαθίστανται από συνώνυμά τους (πχ πόθος -> επιθυμία). Η σημασία του κειμένου-φορέα δεν αλλάζει. Αναπαριστώντας όμως τα συνώνυμα (πχ πόθος 0, επιθυμία 1) μπορεί να ενθεθεί ένα κείμενο. Χρήσιμο σε κείμενα μεταφράσεων...
- **Εισαγωγή κειμένου με κλείδα**: Το παράδειγμα που είδαμε προηγουμένως
- **Αναπαραγωγή νέου κειμένου με ένθεση του μηνύματος στο νέο**.

## Ένθεση σε αρχεία word

Εκμεταλλευόμενοι τον τρόπο αναπαράστασης κειμένου από τα αρχεία επεξεργαστών κειμένου (πχ word) μπορούμε ενθέσουμε κείμενο κάνοντας αλλαγές σε ήκιστα σημεία:

Κωδικούς γλώσσας που δεν θα χρησιμοποιηθούν αλλά υπάρχουν στο πεδίο κώδικα του κειμένου

Μήκη κενών, ή γραμμάτων (πχ μήκος του ιώτα κοκ).



# Ήχος και βίντεο

Η αδυναμία του ανθρώπινου εγκέφαλου να αντιληφθεί το άνυσμα της φάσης, δίνει τη δυνατότητα να ενθέσουμε σε αρχεία ήχου ή βίντεο με ψηφιακό τρόπο μια οποιαδήποτε πληροφορία (φωτογραφία, κείμενο, έγγραφο).

Το πρόβλημα αυτής της τεχνικής είναι φυσικά η δυσκολία διαβίβασης ή ανάρτησής της από δικτυακούς κόμβους χαμηλής χωρητικότητας. Είναι όμως εύκολο μέσω containers να γίνει η διαβίβαση, τηρούμενων κάποιων ενεργειών ασφαλείας ενάντια σε traffic analysis.

# ***NETWORK STEGANOGRAPHY***

Το πεδίο **flag** στην κεφαλίδα του **IP datagram**, το **sequence number** της κεφαλίδας του **TCPv4**, το **Source Port and Checksum** στην κεφαλίδα του **UDP** ή το **Code field** στην κεφαλίδα του **ICMP**, Είναι καλοί υποψήφιοι για ένθεση μηνύματος σε πόρους του διαδικτύου.

# IP Datagram

Version	Hd. Len.	TOS	Total Packet Length	
Identification			flags	Fragment Offset
TTL		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding

Datagram	3-bit Flag field	13-bit fragment offset	Remarks
1	0 <b>1</b> 0	00...00	Datagram 1 covertly communicating ' <b>1</b> '
2	0 <b>0</b> 0	00...00	Datagram 2 covertly communicating ' <b>0</b> '



# Αξιοποίηση διαδικτύου

## Ένα παράδειγμα:

Θέλει κάποιος από ένα μη φίλιο περιβάλλον να στείλει ένα επείγον μήνυμα σε περισσότερους του ενός παραλήπτες.

## Βήματα:

- Γράφει το μήνυμα σε ηλεκτρονική μορφή word document.
- Υπολογίζει το hash code για έλεγχο ακεραιότητας από τους παραλήπτες.
- Το υπογράφει με την υπηρεσιακή του ψηφιακή υπογραφή.
- Το κρυπτογραφεί με μια προσυμφωνημένη κλείδα συνόδου.

**Μέχρι εδώ, τίποτε δεν διαφέρει από την κλασσική κρυπτογραφία.** Ο Αποστολέας πρέπει να στείλει στους παραλήπτες τρία πράγματα:

- Το κρυπτογραφημένο και υπογεγραμμένο κείμενο
- Την κλείδα συνόδου
- Τον κώδικα ακεραιότητας (hash code)

# Αξιοποίηση διαδικτύου

## Αποστολή με στεγανογραφία:

- Επιλογή μέσου(ων) για την αποστολή των τριών αρχείων.  
(Καλύτερα να είναι τρεις διαφορετικοί δρόμοι)
- Ένθεση στα μέσα.
- Αποθήκευση των μέσων σε ένα απλό flash memory.
- Πρόσβαση στο διαδίκτυο: Μέσω του ξενοδοχείου, internet café, ή άλλου τρόπου.
- Ανάρτηση των αρχείων από το memory stick στους κατάλληλους διαδικτυακούς κόμβους-φορείς

## Λήψη των αρχείων:

- Κατόπιν ανάγνωσης του δημοσιευμένου κωδικοποιημένου μηνύματος, οι παραλήπτες κατεβάζουν από τους διάφορους διαδικτυακούς κόμβους τα αρχεία.
- Εξαγωγή των αρχείων από τα Μέσα ένθεσης.
- Αποκρυπτογράφηση της κλειδας συνόδου (ή χρήση της)
- Αποκρυπτογράφηση του μηνύματος-κειμένου
- Επαλήθευση της ακεραιότητας και της ταυτότητας του αποστολέα.

# Αξιοποίηση διαδικτύου

## Επιβεβαίωση στο δίκτυο:

- Κωδικοποιημένη επιβεβαίωση στο δίκτυο/διαδίκτυο, μέσω στεγανογραφημένου (άσχετου) κειμένου, αναρτημένο σε κόμβο

Σε προστατευμένο χώρο!





Στο προσυμφωνημένο μπλογκ γίνεται στεγανογραφημένου κειμένου που αφορά παραλήπτες το επείγον κλιπ



Σε ένα καλό site φωτογραφιών ή πολυμέσων γίνεται ανάρτηση των στεγανογραφημένων φωτογραφιών με τα κρυπτογραφημένα αρχεία



Οι παραλήπτες ενημερώνονται από  
το μπλογκ και καταλαβαίνουν  
αποκωδικοποιώντας  
που πρέπει να αναζητήσουν τι

Κατεβάζουν τις φωτογραφίες τοπικά  
Τις αποθηκεύουν σε flash memory



Στο προσωπικό/υπηρεσιακό pc  
απο-ενθέτουν  
και αποκρυπτογραφούν  
τα αρχεία



Σε προστατευμένο χώρο!

Ενημερώνουν στο μπλογκ  
σχολιάζοντας με ψευδώνυμο  
κωδικοποιημένα  
ότι έλαβαν το μήνυμα



επιβεβαίωση!

Ο Αποστολέας  
κάνει αλλαγές  
στο αρχικό του μήνυμα  
εξαφανίζοντας  
τα στοιχεία

Στο site φωτογραφιών, αντικαθιστά  
ξανά τις στεγανογραφημένες  
με τις πραγματικές ή  
Άλλες,  
Ώστε να μην κινήσει υποψίες



# ΠΡΟΣΟΧΗ!



Η Στεγανογραφία δεν αντικαθιστά:

- Την κρυπτογραφία!
- Τις πιστοποιημένες ασφαλείς επικοινωνίες
- Τον συμβατικό τρόπο επικοινωνίας

Η Στεγανογραφία χρησιμοποιείται:

- Σε επείγουσες καταστάσεις για έκτακτη επικοινωνία σε μη φίλιο περιβάλλον.
- Σε περιπτώσεις που η συμβατική ασφαλής επικοινωνία είναι αδύνατη.
- Σε επικοινωνίες με πηγές, χωρίς να εκτεθούν οι πηγές ή ειδικές υποδομές (προτιμητέα εδώ η χρήση ελεύθερου λογισμικού)

# Στεγανογραφία και Κρυπτογραφία

Συνδέονται στενά

Διαφέρουν στους στόχους:

Κρυπτογραφία: Δεν αποκρύπτεται η ύπαρξη της πληροφορίας, αν και είναι κρυπτογραφημένη και μη αναγνώσιμη

Στεγανογραφία: Δεν υπάρχει γνώση ύπαρξης της κρυμμένης πληροφορίας.

Μπορούν να συνδυαστούν ώστε να αποδώσουν μεγαλύτερη προστασία.

# Ψηφιακό υδατογράφημα

Χρησιμοποιείται πρωτίστως για αναγνώριση γνησιότητας.

Συνίσταται στην ένθεση μικρής πληροφορίας μέσα σε ένα μέσο (συνήθως φωτογραφία) χωρίς αυτό να είναι αντιληπτό.

Η αφαίρεσή του είναι σχεδόν αδύνατη χωρίς σημαντική αλλοίωση του μέσου

# Ψηφιακή Στεγανογραφία και Υδατογράφημα

Το ψηφιακό υδατογράφημα ενθέτει πληροφορία σε δεδομένα και αυτό από μόνο του συνιστά έναν τύπο στεγανογραφίας.

Η διαφορά είναι στους στόχους...

Στεγανογραφία: Ένθεση πληροφορίας

Υδατογράφημα: Επέκταση του μέσου με επιπλέον πληροφορία.

Η στεγανογραφική πληροφορία δεν πρέπει με τίποτε να είναι αντιληπτή σε έναν ο οποίος δεν υποψιάζεται την ύπαρξή της.

# Ασφάλεια Δικτύου και Στεγανογραφία

**Εμπιστευτικότητα (Confidentiality):** Κάθε μη εξουσιοδοτημένο άτομο δεν γνωρίζει την ύπαρξη ευαίσθητων δεδομένων.

**Επιβιωσιμότητα (Survivability):** Επαλήθευση ότι τα δεδομένα δεν καταστράφηκαν κατά τη μετάδοση.

**Μη ανιχνευσιμότητα (No detection):** Η ανίχνευση της κρυμμένης πληροφορίας είναι πολύ δύσκολη.

**Ορατότητα (Visibility):** Οι άνθρωποι δεν μπορούν να ανιχνεύσουν στο μέσον, κάποια αλλοίωση εξαιτίας της κρυμμένης πληροφορίας.



# Κρύψιμο Πληροφορίας σε κείμενο

## Μερικώς αποτελεσματική

### ΔΕΛΤΙΟ ΚΑΙΡΟΥ

Ιδιαίτερα βροχερός αναμένεται να διατηρηθεί ο καιρός σε αρκετές ηπειρωτικές και θαλάσσιες περιοχές της χώρας μέχρι και την Τρίτη 27/10. Τα φαινόμενα θα είναι κατά περιόδους έντονα, ενώ κατά τόπους θα χαρακτηρίζονται από μεγάλη διάρκεια, λόγω της οποίας είναι πιθανό να προκύψουν προβλήματα. Οι νότιοι άνεμοι στα πελάγη θα φτάνουν σε ένταση τα 6 - 7 μποφόρ, στρεφόμενοι σταδιακά στο Ιόνιο σε ανατολικών διευθύνσεων και στο Αιγαίο σε ανατολικούς έως βορειοανατολικούς με ανάλογες εντάσεις. Η θερμοκρασία θα σημειώσει μικρή πτώση στα κεντρικά, ανατολικά και βόρεια διατηρούμενη ωστόσο σε ελαφρώς υψηλότερα από τα κανονικά για την εποχή επίπεδα.

**Δίνει το μήνυμα Βρίσκομαι εκτός Αττικής**

# **Κρύβοντας ένα μήνυμα μέσα σε κειμένο**

Αλγόριθμος πρώτου γράμματος

Κάθε νιοστό γράμμα

Αλλάζοντας το μέγεθος των κενών

Χρήση δημοσίου κειμένου

# **Κρύβοντας ένα Μήνυμα μέσα σε φωτογραφίες**

Το πιο δημοφιλές μέσον!

**Τροποποίηση της εικόνας ως προς τα  
λιγότερα σημαντικά bit. Least-  
significant bit (LSB)**

*24-bit vs. 8-bit images*

*Εργαλεία εφαρμογής LSB: EzStego and S-Tools*

**Απόκρυψη και φιλτράρισμα**

**Αλγόριθμοι και μετασχηματισμοί**

# *Κρύβοντας μηνύματα σε αρχεία πολυμέσων*

## **Πλεονεκτήματα**

Εύρος ακουστικών συχνοτήτων – 20.000 Hz.

Δυνατότητα ένθεσης μεγάλου όγκου δεδομένων

Δυσκολία στην αναγνώριση εξαιτίας της συνεχούς ροής (ροή κινούμενων εικόνων και ήχου)

# *Στεγανάλυση*

Detecting and decoding the hidden data within a given medium

Even if secret content is not revealed, modifying the cover medium changes the medium's statistical properties

Distributed Dictionary Attack

# *Το Μέλλον της Στεγανογραφίας*

Η πιο διαδεδομένη χρήση της είναι στην ψηφιακή υδατογραφία

Ενδεχομένως να υφίσταται νομικούς περιορισμούς καθώς είναι ευεπίφορη για χρήση από παρανόμους για κρυφή επικοινωνία.

# ***Steganography - Tools***

Steganography Tools

Steganos

S-Tools (GIF, JPEG)

StegHide (WAV, BMP)

Invisible Secrets (JPEG)

JPHide

Camouflage

Hiderman

Many others...

# ***Steganography***

Popular sites for Steganography  
information

[\*\*http://www.ise.gmu.edu/~njohnson/Steganography\*\*](http://www.ise.gmu.edu/~njohnson/Steganography)

[\*\*http://www.rhetoric.umn.edu/Rhetoric/misc/dfrank/stegsoft.html\*\*](http://www.rhetoric.umn.edu/Rhetoric/misc/dfrank/stegsoft.html)

[\*\*http://www.topology.org/crypto.html\*\*](http://www.topology.org/crypto.html)





# Επόμενο είναι...



Η εύκολη χρήση και σε συνδυασμό με κρυπτογραφία ο υψηλός βαθμός ασφάλειας που παρέχεται, έχουν καταστήσει την στεγανογραφία, ένα χρήσιμο εργαλείο για:

**Τρομοκρατία.**  
**Κατασκοπεία.**

Για αυτό και οι υπηρεσίες ασφαλείας / αντιτρομοκρατίας αφιερώνουν ένα σημαντικό τμήμα του έργου τους στην **στεγανάλυση.**

Liberté

Liberté  
~~Égalité~~

Liberté  
~~Fraternité~~



<http://boomix.net/affac/>  
SUBITO



Join us !



# Ερωτήσεις

