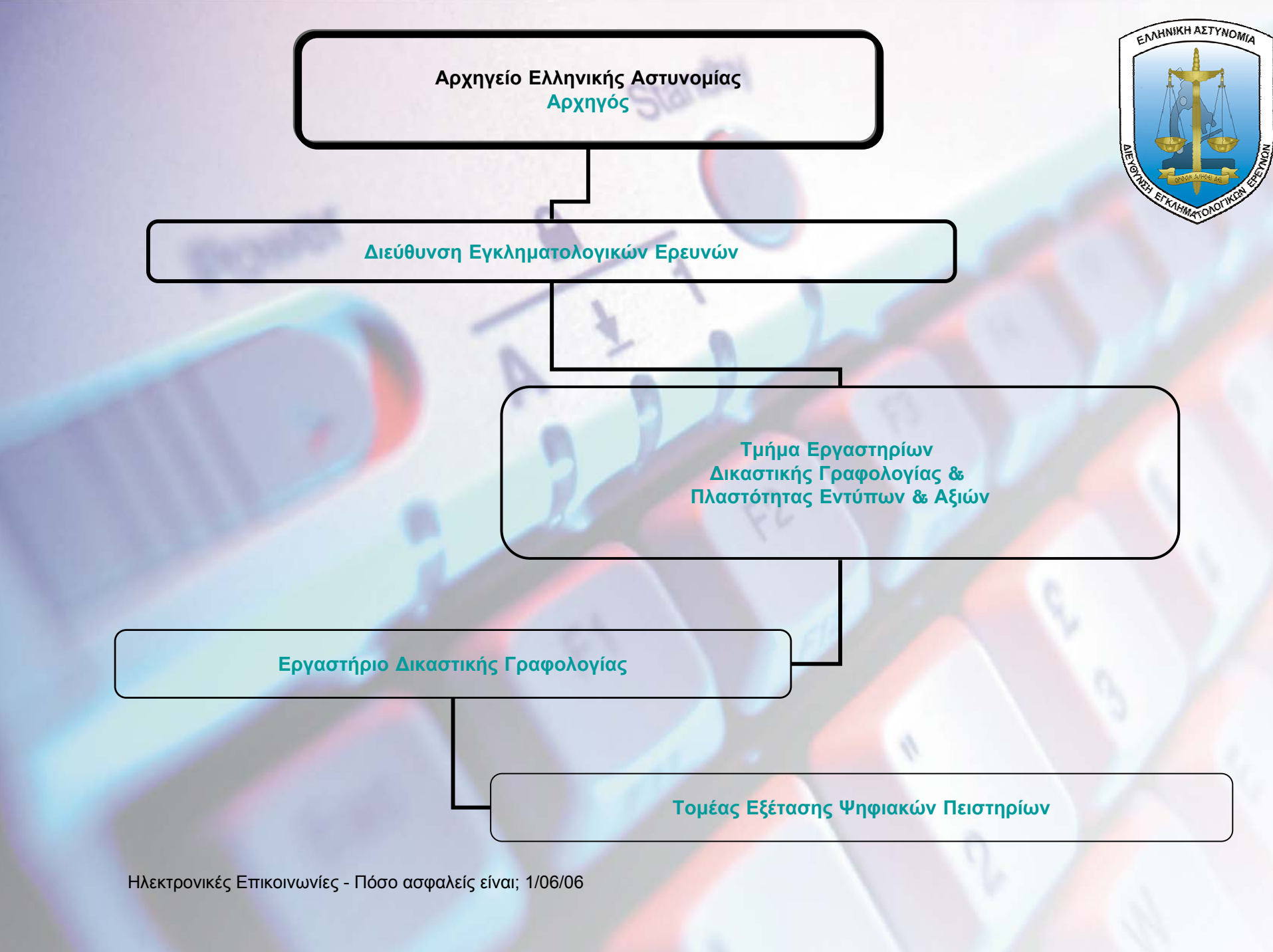
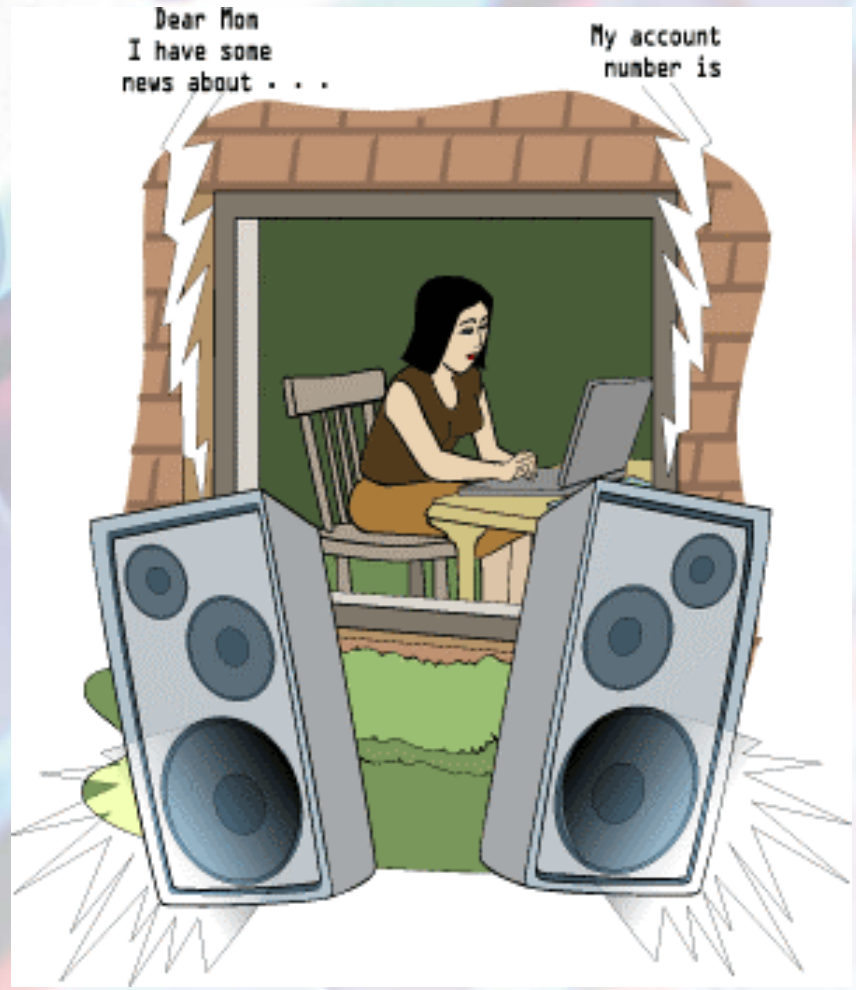

Αρχηγείο Ελληνικής Αστυνομίας
Αρχηγός
Διεύθυνση Εγκληματολογικών Ερευνών
Τμήμα Εργαστηρίων
Δικαστικής Γραφολογίας &
Πλαστότητας Εντύπων & Αξιών
Εργαστήριο Δικαστικής Γραφολογίας
Τομέας Εξέτασης Ψηφιακών Πειστηρίων

Ασφάλεια Η/Υ

- Επικοινωνία σήμερα σημαίνει Η/Υ.
- Οι Η/Υ είναι απαραίτητοι για τους περισσότερους τρόπους επικοινωνίας.
- Οι Η/Υ είναι τόσο ασφαλείς όσο όλοι γνωρίζουμε ότι είναι.



Επικοινωνία και Η/Υ

- Internet
- Εταιρικά κλπ κλειστά δίκτυα
- Δίκτυα τηλεπικοινωνιών

- Και όλα τα παραπάνω μπορεί να είναι ενσύρματα ή ασύρματα

Ασύρματα Δίκτυα

- Αναπτύσσονται Ταχύτατα
- Δεν ασφαλίζονται όπως θα πρέπει.
- Διασύνδεση μη ασφαλών ασύρματων δικτύων (Πχ δίκτυο σε χώρο στάθμευσης εταιρείας) με άλλα ασφαλή.
- Δύσκολος εντοπισμός του δράστη λόγω ασύρματης δυνατότητας σύνδεσης.

Wardriving

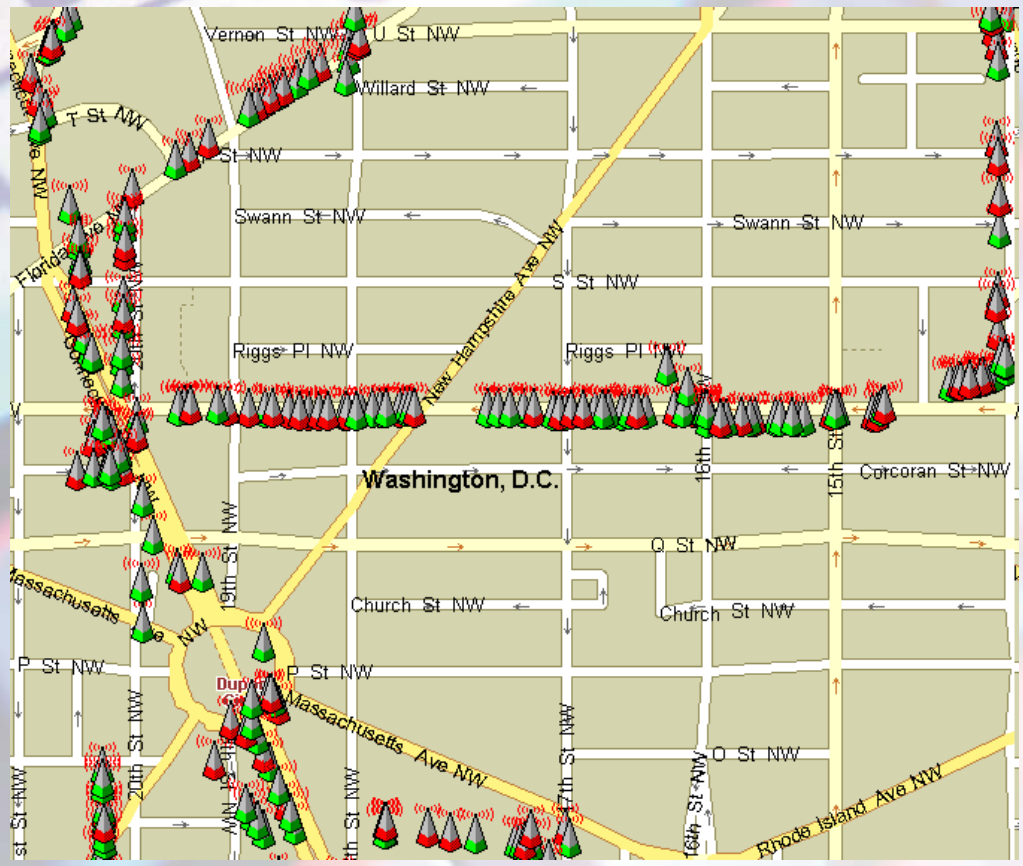
- Ο όρος που χρησιμοποιείται για να περιγράψουμε την ανεύρεση της θέσης και της κατάστασης ασύρματων δικτύων.
- Πραγματοποιείται με τη χρήση λογισμικού για τον εντοπισμό του δικτύου και μιας συσκευής GPS (όχι απαραίτητα), για την καταγραφή της ακριβούς θέσης.

Warbiking

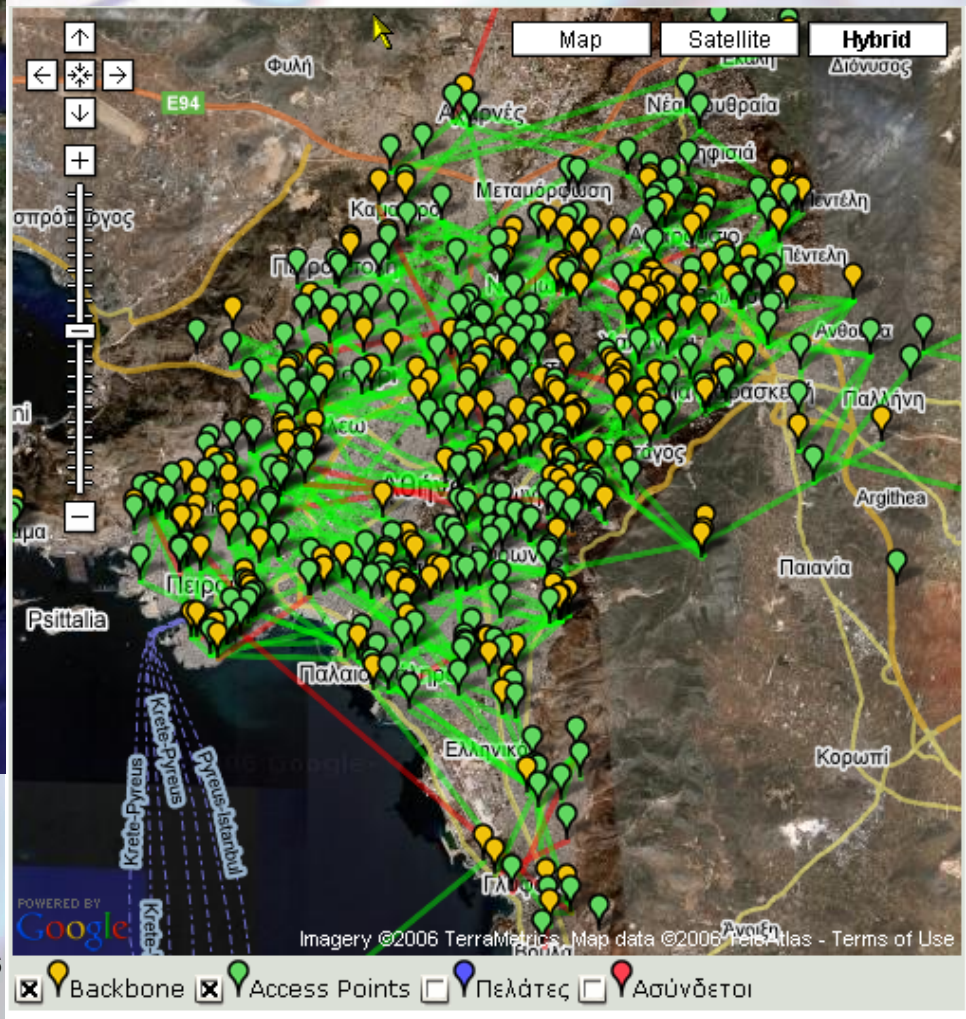

1630

+

=


Vernon St NW
U St NW
Willard St NW
T St NW
Swann St NW
Swann St NW
S St NW
Riggs Pl NW
Riggs Pl NW
New Hampshire Ave NW
16th St
15th St
Corcoran St NW
Washington, D.C.
Q St NW
19th St NW
Church St NW
Church St NW
P St NW
P St NW
Massachusetts Ave NW
20th St NW
17th St NW
O St NW
Rhode Island Ave NW

Ασύρματα Δίκτυα στην Ελλάδα – Αθήνα



Εργαλεία για το δράστη

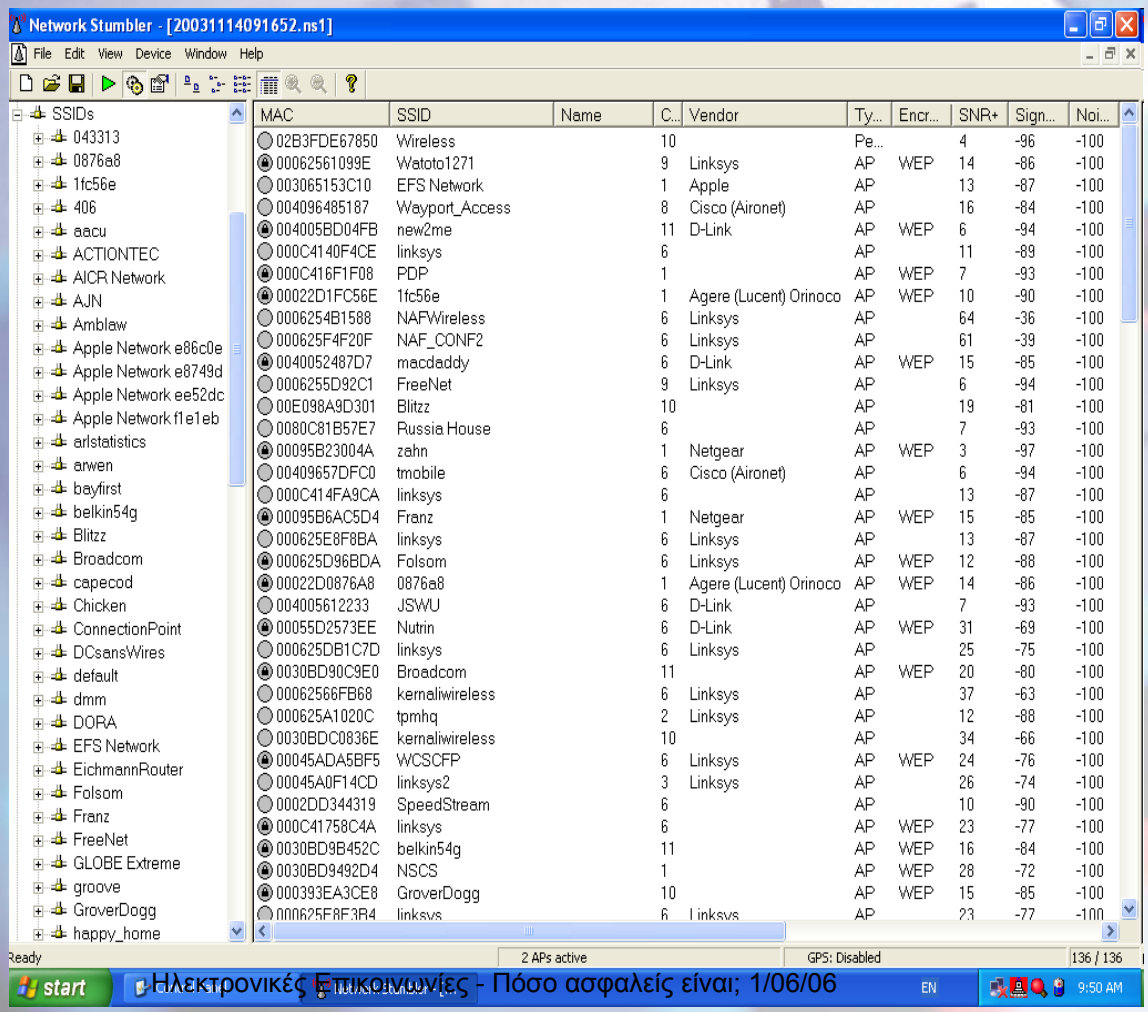
- Laptop

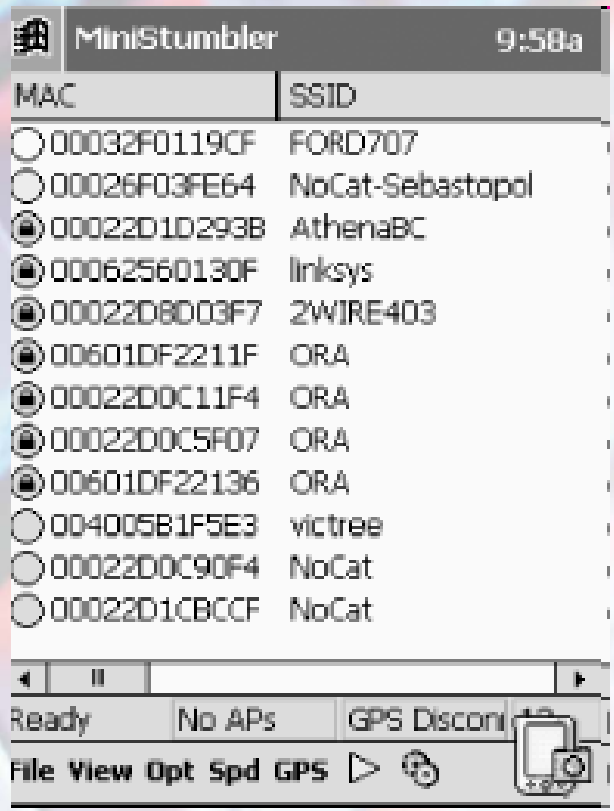
- PDA

- PSP

Εργαλεία για το δράστη

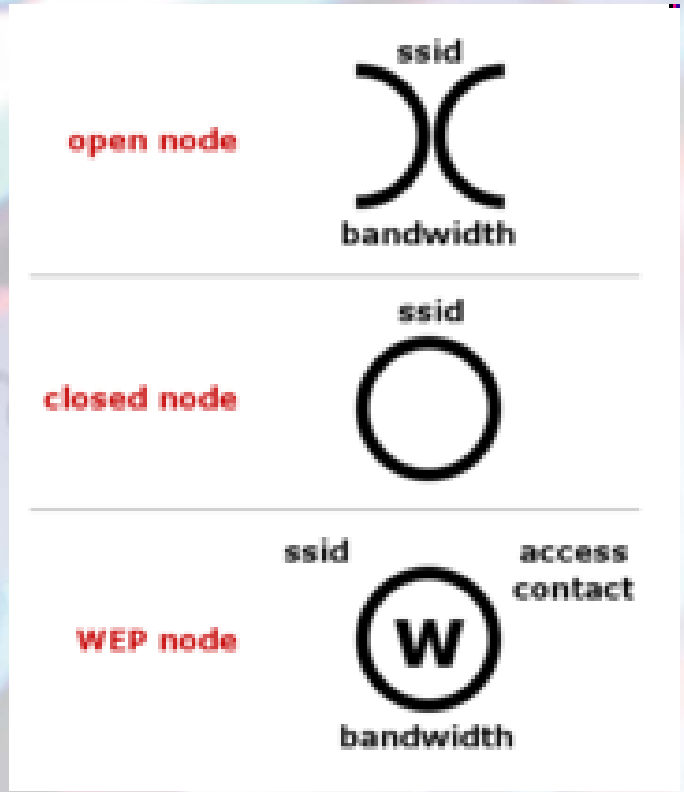
- Netstumbler Ministambler και 10άδες άλλα





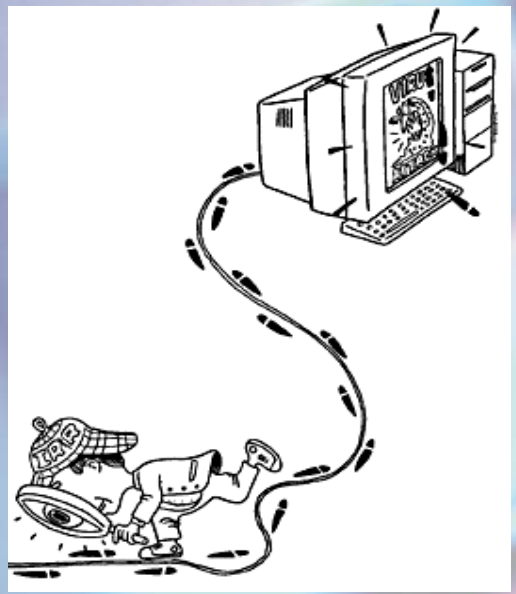
Warchalking

– Η σχεδίαση συμβόλων σε δημόσια μέρη, προκειμένου να δημοσιοποιηθεί η ύπαρξη ασύρματων δικτύων.



Warchalking

Forensics



- Όπως στο φυσικό επίπεδο, αφού συμβεί κάτι, προσπαθούμε να διακριβώσουμε τι και πως έγινε, προκειμένου να βρεθεί ο δράστης, ανάλογα πράττουμε και σε ψηφιακό επίπεδο.
- Η μεγάλη διαφορά: Στην πρώτη περίπτωση η ίδια η φύση φροντίζει να μένουν ίχνη. Εμείς απλά καλούμαστε να τα βρούμε. (αποτυπώματα κλπ)
- Στην άλλη περίπτωση εμείς είμαστε αυτοί που θα πρέπει να φροντίσουμε ούτως ώστε να μείνουν ίχνη. Και τα ίχνη αυτά στον ψηφιακό κόσμο είναι log files.

Log Files

- Να θυμάμαι: Πολύ συχνά το μέγεθος της ζημιάς που θα γίνει εξαρτάται και από την ποσότητα των log files που έχουν διατηρηθεί, δηλαδή από το αν υπάρχει υποδομή forensics στο όλο σύστημα. (Log files, IDS)
- Παράδειγμα. Αν από την ανάλυση όλων των στοιχείων που υπάρχουν στη διάθεσή μας διαπιστώσουμε τι ακριβώς συνέβη, ίσως χρειαστεί να διορθώσουμε μόνο αυτό χωρίς να είναι απαραίτητο να «ξαναχτίσουμε» το όλο σύστημα. Ελαχιστοποίηση downtime.

Log files

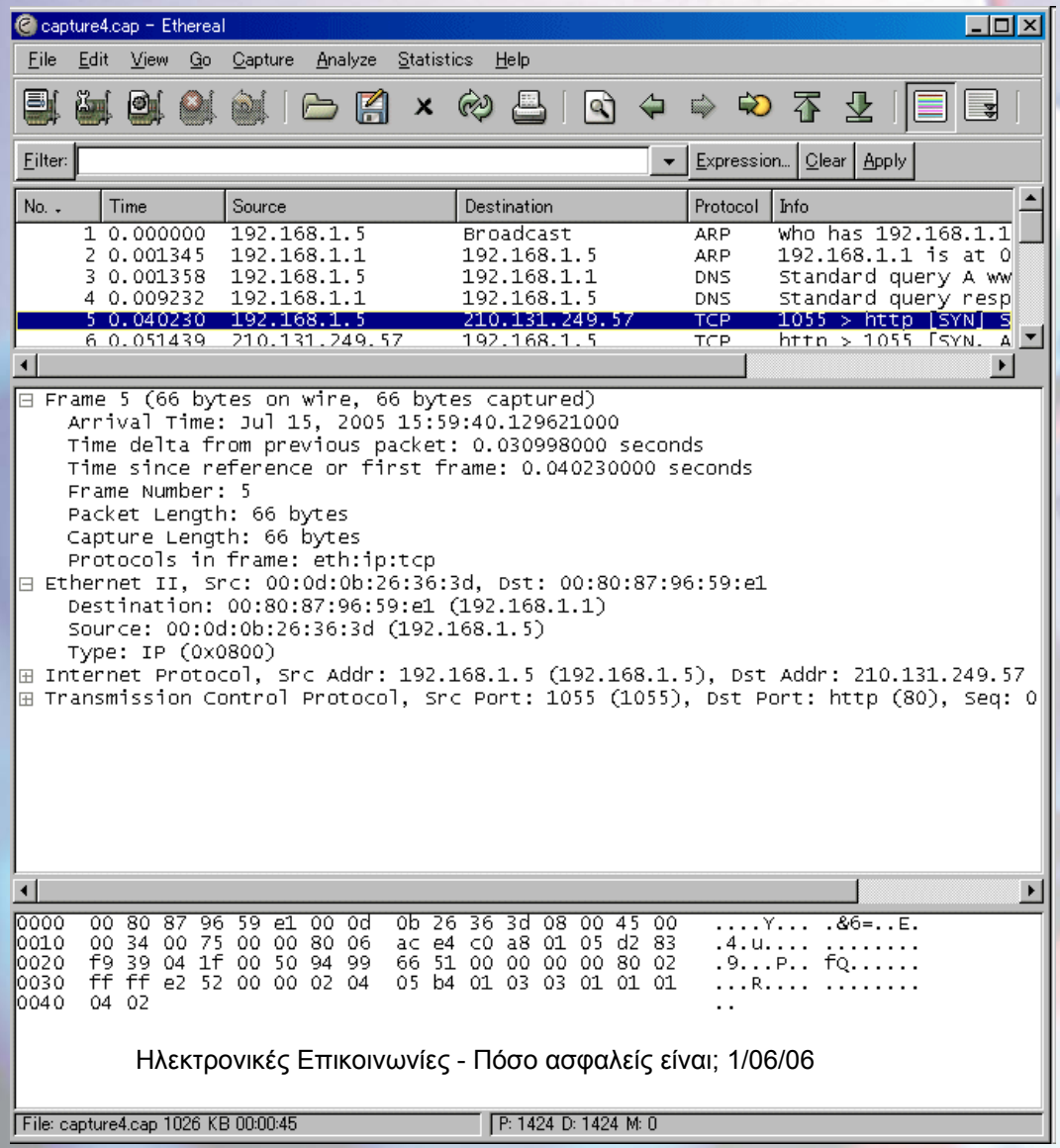
- Σε αντίθεση λοιπόν με το φυσικό κόσμο, στον ψηφιακό οι εγγραφές είναι αναλυτικές. Με την ανάγνωση των log αρχείων γνωρίζουμε τα πάντα για μια σύνδεση.
- Όμως μπορούν εύκολα να αλλοιωθούν απο τον δράστη για παραπλάνηση.
- Πρέπει να αλληλοεπιβεβαιώνονται σε διάφορα σημεία καταγραφής για να είναι αξιόπιστες.

- ΝΑ ΜΗΝ ΞΕΧΝΩ: Ποτέ δεν είμαι βέβαιος για το ποια δεδομένα διέρχονται του δικτύου μου….
- Με network sniffer, έχουν εντοπιστεί κωδικοί πρόσβασης θυρών «ασφαλείας». Χμμ.. λες να μεταδίδονται και ασύρματα στη γειτονιά?
- Ισως έχω ακούσει την λέξη κρυπτογράφηση?

Διασφάλιση ψηφιακών αρχείων

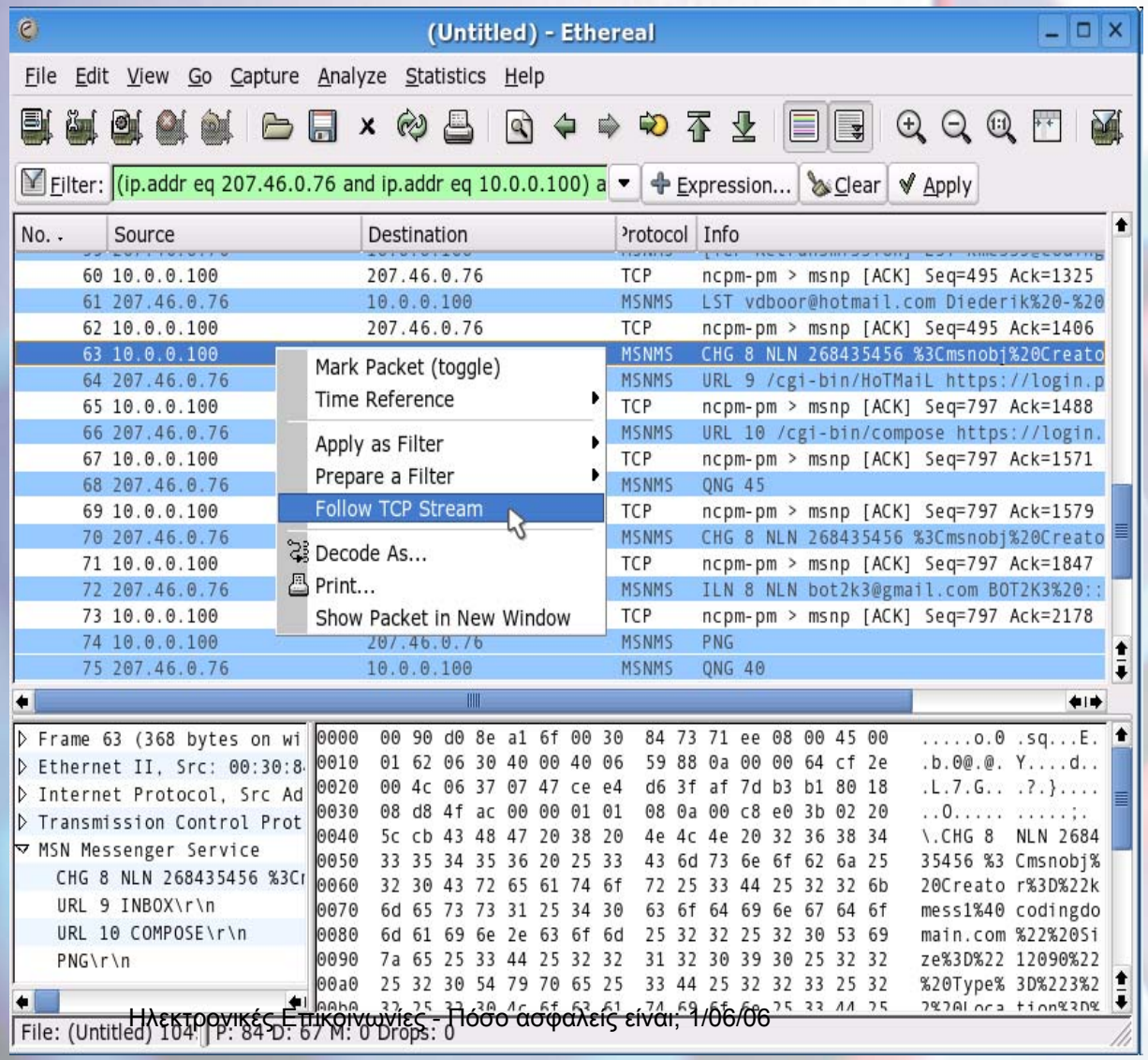
- Δεν αρκεί μόνο η συγκέντρωση των δεδομένων αλλά και η διατήρησή τους με τρόπο τέτοιο που να μπορεί να βεβαιωθεί η ακεραιότητά τους.
- Αποθήκευση δεδομένων (πειστήρια) κατά προτίμηση σε οπτικό δίσκο.
- Hash Value για κάθε αρχείο και για όλο το CD/DVD, για να διασφαλιστεί ότι δεν έχει αλλάξει τίποτα.

Raw data



- Η ανάλυση δεδομένων από log files είναι κουραστική, επίπονη και χρονοβόρα διαδικασία.

Ethereal



- Ευτυχώς υπάρχουν εργαλεία για να τη διευκολύνουν αλλά δυστυχώς δεν είναι αυτόματη.

Εγκληματολογική εξέταση - ίχνη

Όταν πληκτρολογούμε μία δ/νση στον browser

Και εφ'όσον τηρούνται logs.....

Καταγραφή γι' αυτή την ενέργεια μπορεί να βρεθεί στον Proxy server

```
1148851846.258     54 10.0.0.118 TCP_MISS/200 38300 GET http://sunny/phpinfo.php - DIRECT/10.0.0.200 text/html
1148851846.276      5 10.0.0.118 TCP_MISS/200 4905 GET http://sunny/phpinfo.php? - DIRECT/10.0.0.200 image/gif
1148851846.281      3 10.0.0.118 TCP_MISS/200 2407 GET http://sunny/phpinfo.php? - DIRECT/10.0.0.200 image/gif
```

Στον Web server, είτε σαν log file

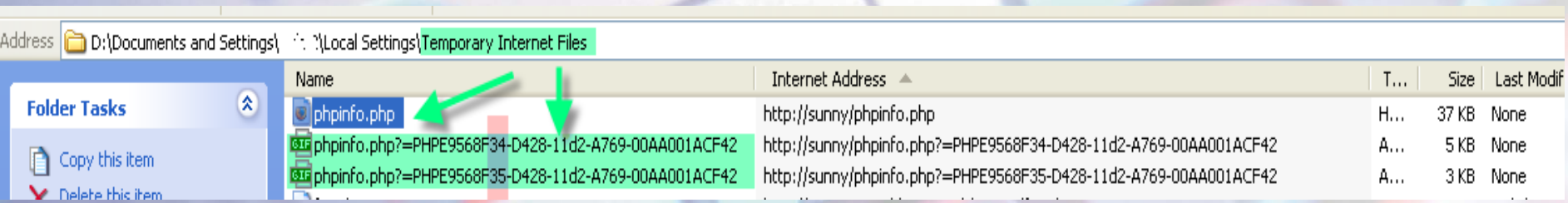
```
10.0.0.200 - - [29/May/2006:00:30:46 +0300] "GET /phpinfo.php HTTP/1.0" 200 38046
10.0.0.200 - - [29/May/2006:00:30:46 +0300] "GET /phpinfo.php?=PHPE9568F34-D428-11d2-A769-
10.0.0.200 - - [29/May/2006:00:30:46 +0300] "GET /phpinfo.php?=PHPE9568F35-D428-11d2-A769-
```

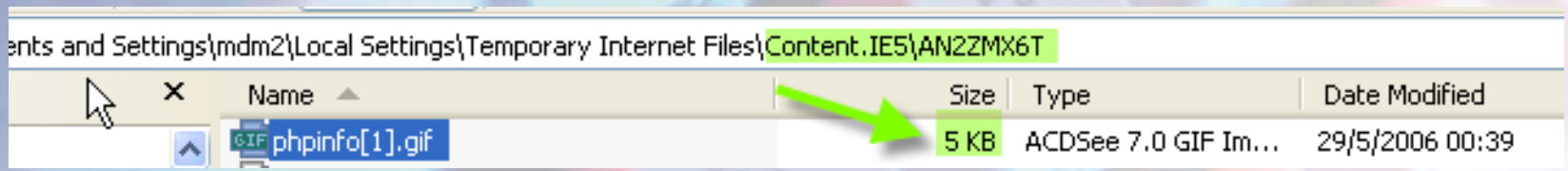
Είτε σαν πληροφορίες καταλόγου

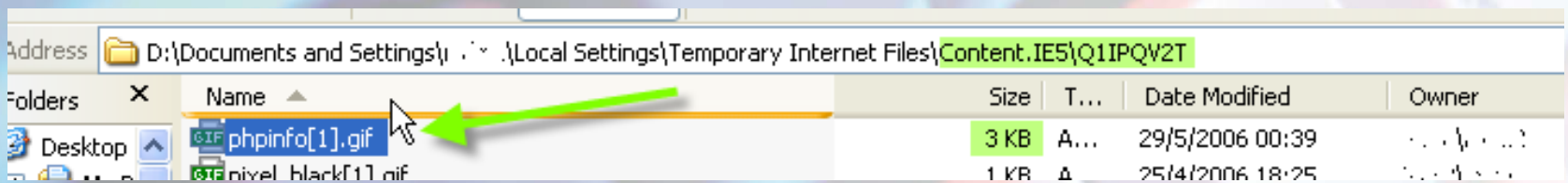
```
$ cat ls_--full-time_phpinfo.out
command:
ls --full-time /var/www/localhost/htdocs/phpinfo.php


output:
-rw-r--r--  1 root root 21 2006-05-29 00:02:14.000000000 +0300 /var/www/localhost/htdocs/phpinfo.php


explanation:
-rw-r--r--                                  file mode
1                                           Number of hard links
root                                        file user ownership
root                                        file group ownership
21                                          size in bytes
2006-05-29                                  date modified
00:02:14.000000000                          time
+0300                                       time zone
/var/www/localhost/htdocs/phpinfo.php       the file
```

Η/Υ δράστη

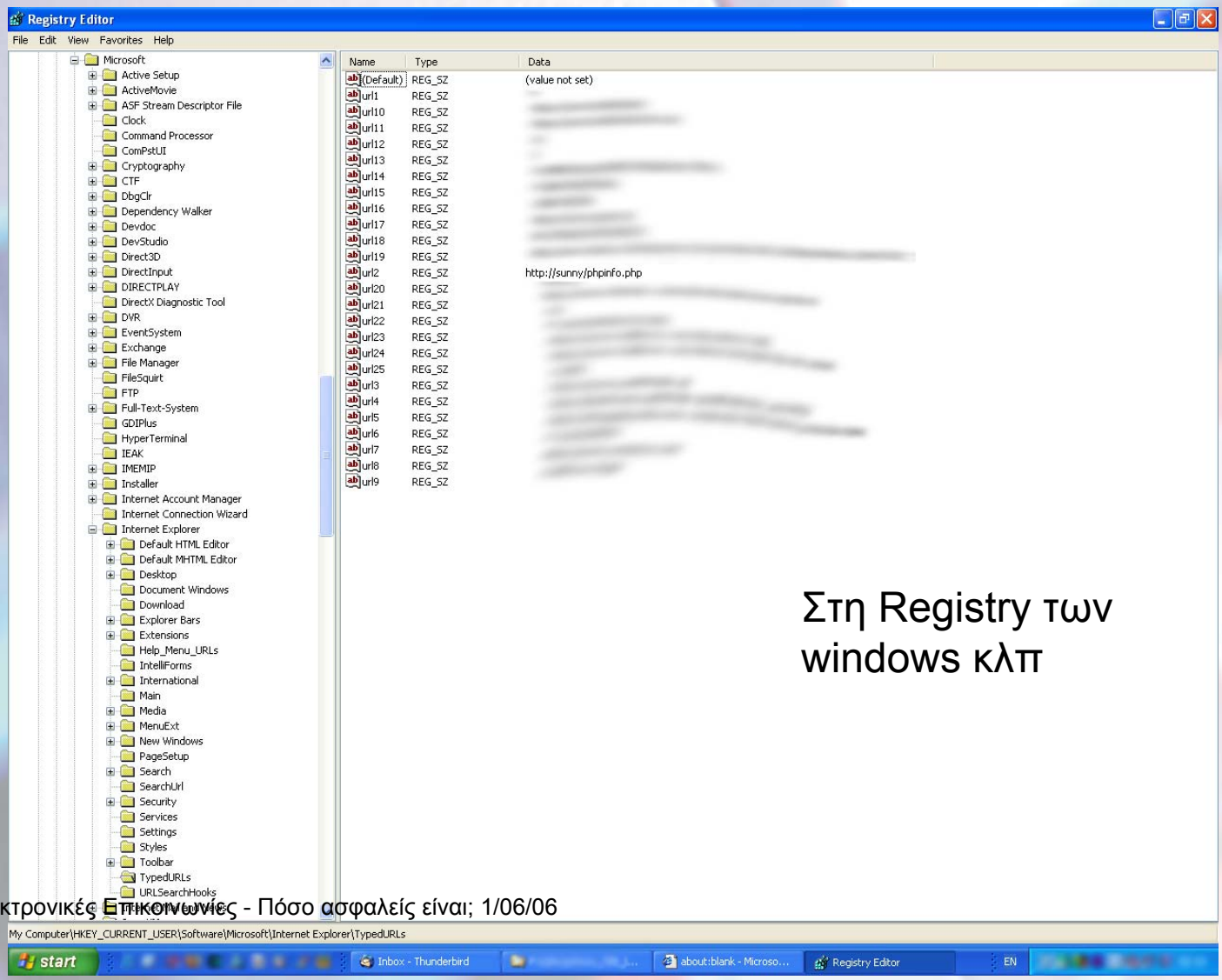
Στον κατάλογο Temp Internet files







Η/Υ δράστη



Στη Registry των windows κλπ

Να μην ξεχάσω

- **Να φροντίσω να υπάρχουν log files**

Τρέχουμε τώρα.... Ευχαριστώ

Ιωάννης Πάσχος – Υπαστυνόμος Α΄
Εξεταστής ψηφιακών πειστηρίων
ΔΙΕΥΘΥΝΣΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΕΡΕΥΝΩΝ
ΤΜΗΜΑ ΕΡΓΑΣΤΗΡΙΩΝ ΔΙΚΑΣΤΙΚΗΣ ΓΡΑΦΟΛΟΓΙΑΣ & ΠΛΑΣΤΟΤΗΤΑΣ ΕΝΤΥΠΩΝ & ΑΞΙΩΝ
ΕΡΓΑΣΤΗΡΙΟ ΔΙΚΑΣΤΙΚΗΣ ΓΡΑΦΟΛΟΓΙΑΣ
ΤΟΜΕΑΣ ΕΞΕΤΑΣΗΣ ΨΗΦΙΑΚΩΝ ΠΕΙΣΤΗΡΙΩΝ
Λ. ΑΛΕΞΑΝΔΡΑΣ 173 – Τ.Κ 115 22
ΤΗΛ.: 210 647 62 68 – FAX: 210 643 02 38
E-MAIL: forensix@mopo.gr
Cell: +30 6932 355 775