



Αρχηγείο Ελληνικής Αστυνομίας  
Αρχηγός

Διεύθυνση Εγκληματολογικών Ερευνών

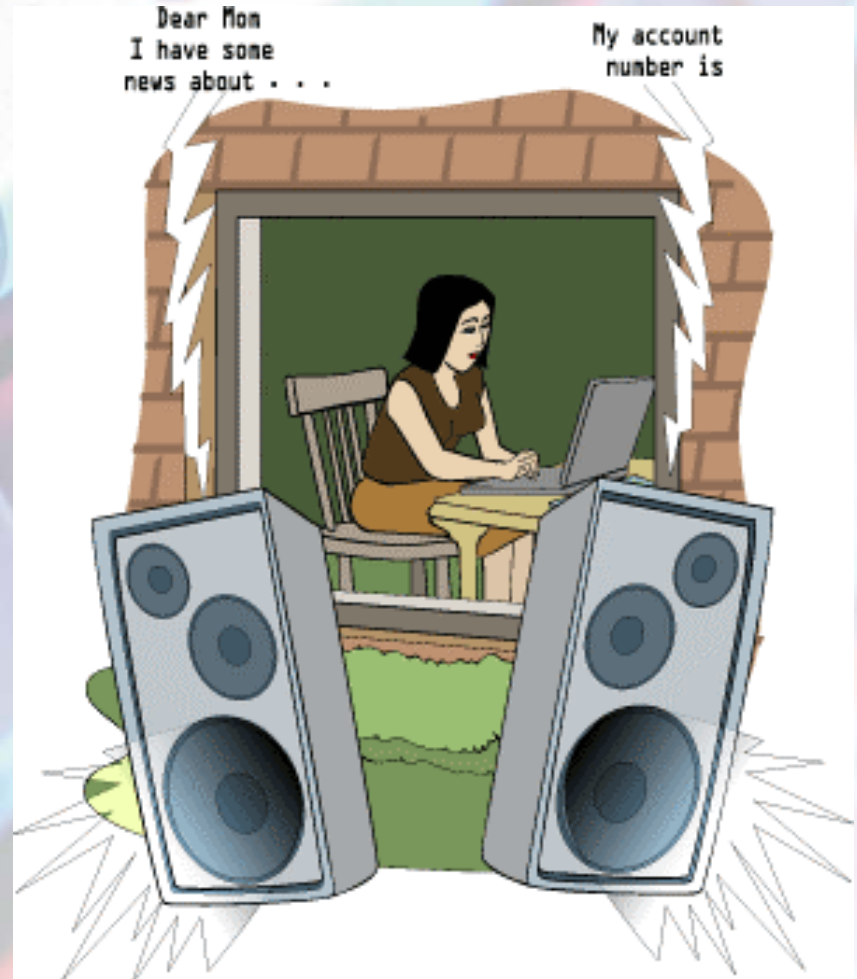
Τμήμα Εργαστηρίων  
Δικαστικής Γραφολογίας &  
Πλαστότητας Εντύπων & Αξιών

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.



# ΕΠΙΚΟΙΝΩΝΙΑ 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 ασφαρίζονται 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

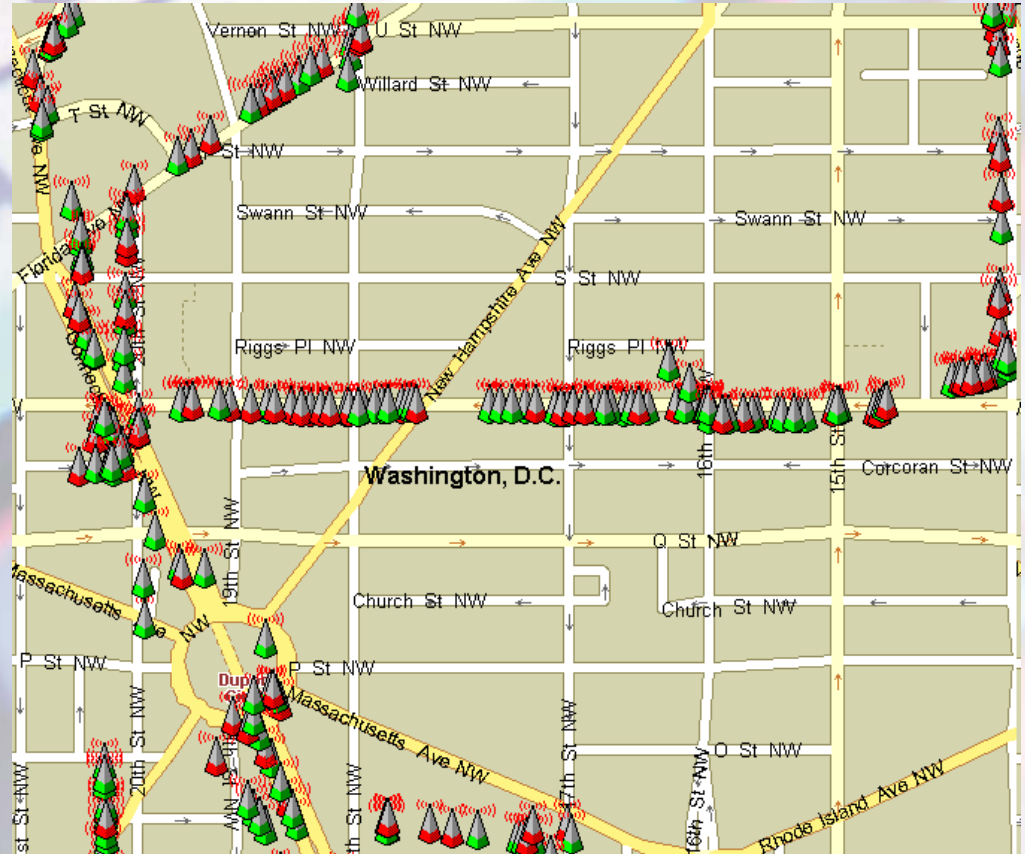
- Ο όρος που χρησιμοποιείται για να περιγράψουμε την ανεύρεση της θέσης και της κατάστασης ασύρματων δικτύων.
- Πραγματοποιείται με τη χρήση λογισμικού για τον εντοπισμό του δικτύου και μιας συσκευής GPS (όχι απαραίτητα), για την καταγραφή της ακριβούς θέσης.

# Warbiking



+

=







# Εργαλεία για το δράστη



- Laptop



- PDA



- PSP





# Εργαλεία για το δράστη

- Netstumbler Ministumbler και 10άδες άλλα

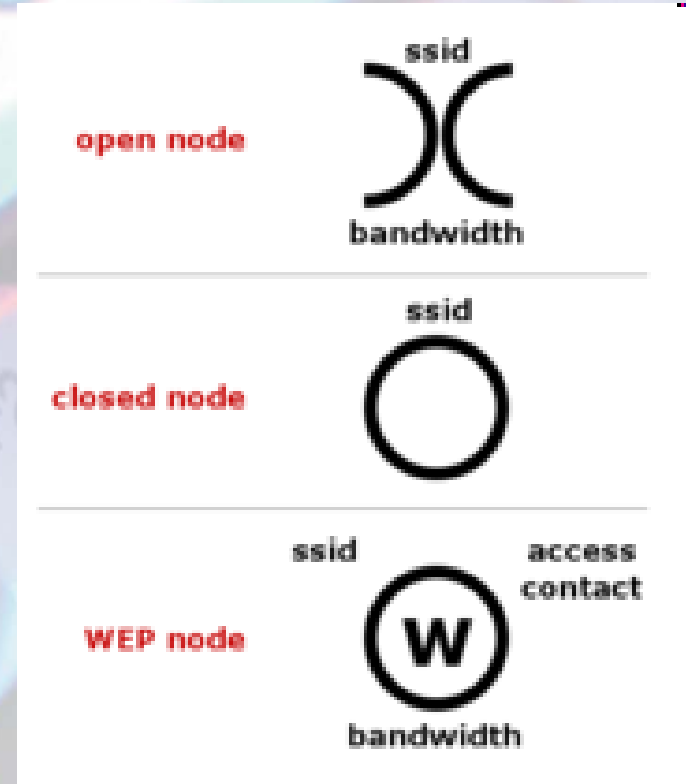
MAC	SSID	Name	C...	Vendor	Ty...	Encr...	SNR+	Sign...	Noi...
02B3FDE67850	Wireless		10		Pe...		4	-96	-100
00062561099E	Watoto1271		9	Linksys	AP	WEP	14	-86	-100
003065153C10	EFS Network		1	Apple	AP		13	-87	-100
004096485187	Wayport_Access		8	Cisco (Aironet)	AP		16	-84	-100
004005BD04FB	new2me		11	D-Link	AP	WEP	6	-94	-100
000C4140F4CE	linksys		6		AP		11	-89	-100
000C416F1F08	PDP		1		AP	WEP	7	-93	-100
00022D1FC56E	1fc56e		1	Agere (Lucent) Orinoco	AP	WEP	10	-90	-100
0006254B1588	NAFWireless		6	Linksys	AP		64	-36	-100
000625F4F20F	NAF_CONF2		6	Linksys	AP		61	-39	-100
0040052487D7	macdaddy		6	D-Link	AP	WEP	15	-85	-100
0006255D92C1	FreeNet		9	Linksys	AP		6	-94	-100
00E098A9D301	Blitz		10		AP		19	-81	-100
0080C81B57E7	Russia.House		6		AP		7	-93	-100
00095B23004A	zahn		1	Netgear	AP	WEP	3	-97	-100
00409657DFC0	tmobile		6	Cisco (Aironet)	AP		6	-94	-100
000C414FA9CA	linksys		6		AP		13	-87	-100
00095B6AC5D4	Franz		1	Netgear	AP	WEP	15	-85	-100
000625E8F8BA	linksys		6	Linksys	AP		13	-87	-100
000625D96BDA	Folsom		6	Linksys	AP	WEP	12	-88	-100
00022D0876A8	0876a8		1	Agere (Lucent) Orinoco	AP	WEP	14	-86	-100
004005612233	JSWU		6	D-Link	AP		7	-93	-100
00055D2573EE	Nutrin		6	D-Link	AP	WEP	31	-69	-100
000625DB1C7D	linksys		6	Linksys	AP		25	-75	-100
0030BD90C9E0	Broadcom		11		AP	WEP	20	-80	-100
00062566FB68	kemaliwireless		6	Linksys	AP		37	-63	-100
000625A1020C	tpmhc		2	Linksys	AP		12	-88	-100
0030BDC0836E	kemaliwireless		10		AP		34	-66	-100
00045ADA5BF5	WCSCFP		6	Linksys	AP	WEP	24	-76	-100
00045A0F14CD	linksys2		3	Linksys	AP		26	-74	-100
0002DD344319	SpeedStream		6		AP		10	-90	-100
000C41758C4A	linksys		6		AP	WEP	23	-77	-100
0030BD9B452C	belkin54g		11		AP	WEP	16	-84	-100
0030BD9492D4	NSCS		1		AP	WEP	28	-72	-100
000393EA3CE8	GroverDogg		10		AP	WEP	15	-85	-100
000625F8F3R4	linksys		6	Linksys	AP		23	-77	-100

MAC	SSID
00032F0119CF	FORD707
00026F03FE64	NoCat-Sebastopol
00022D1D293B	AthenaBC
00062560130F	linksys
00022D08D03F7	ZWIRE403
00601DF2211F	ORA
00022D0C11F4	ORA
00022D0C5F07	ORA
00601DF22136	ORA
004005B1F5E3	victree
00022D0C90F4	NoCat
00022D1CBCCF	NoCat

# Warchalking



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

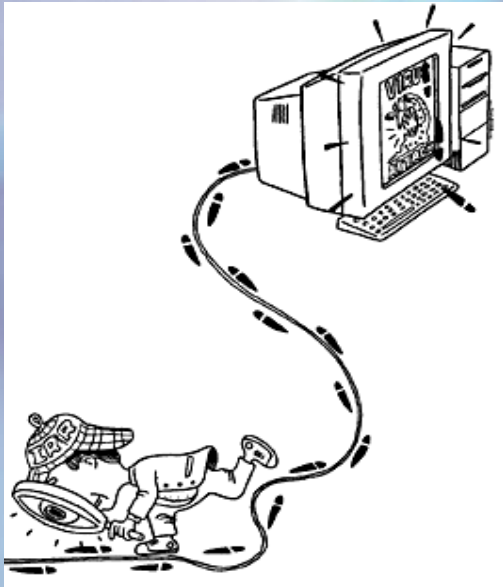


# Warchalking





# 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?
- Ίσως 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

capture4.cap - Ethereal

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.5	Broadcast	ARP	who has 192.168.1.1
2	0.001345	192.168.1.1	192.168.1.5	ARP	192.168.1.1 is at 0
3	0.001358	192.168.1.5	192.168.1.1	DNS	Standard query A ww
4	0.009232	192.168.1.1	192.168.1.5	DNS	Standard query resp
5	0.040230	192.168.1.5	210.131.249.57	TCP	1055 > http [SYN] S
6	0.051439	210.131.249.57	192.168.1.5	TCP	http > 1055 [SYN. A

Frame 5 (66 bytes on wire, 66 bytes captured)  
Arrival Time: Jul 15, 2005 15:59:40.129621000  
Time delta from previous packet: 0.030998000 seconds  
Time since reference or first frame: 0.040230000 seconds  
Frame Number: 5  
Packet Length: 66 bytes  
Capture Length: 66 bytes  
Protocols in frame: eth:ip:tcp

Ethernet II, Src: 00:0d:0b:26:36:3d, Dst: 00:80:87:96:59:e1  
Destination: 00:80:87:96:59:e1 (192.168.1.1)  
Source: 00:0d:0b:26:36:3d (192.168.1.5)  
Type: IP (0x0800)

Internet Protocol, Src Addr: 192.168.1.5 (192.168.1.5), Dst Addr: 210.131.249.57

Transmission Control Protocol, Src Port: 1055 (1055), Dst Port: http (80), Seq: 0

```
0000 00 80 87 96 59 e1 00 0d 0b 26 36 3d 08 00 45 00  ....Y... .&6=..E.
0010 00 34 00 75 00 00 80 06 ac e4 c0 a8 01 05 d2 83  .4.u.... ..
0020 f9 39 04 1f 00 50 94 99 66 51 00 00 00 00 80 02  .9...P.. fQ.....
0030 ff ff e2 52 00 00 02 04 05 b4 01 03 03 01 01 01  ...R.... ..
0040 04 02
```

Ηλεκτρονικές Επικοινωνίες - Πόσο ασφαλείς είναι; 1/06/06

File: capture4.cap 1026 KB 00:00:45 | P: 1424 D: 1424 M: 0

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





# Ethereal

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 207.46.0.76 and ip.addr eq 10.0.0.100) a + Expression... Clear Apply

No.	Source	Destination	Protocol	Info
60	10.0.0.100	207.46.0.76	TCP	ncpm-pm > msnp [ACK] Seq=495 Ack=1325
61	207.46.0.76	10.0.0.100	MSNMS	LST vdboor@hotmail.com Diederik%20-%20
62	10.0.0.100	207.46.0.76	TCP	ncpm-pm > msnp [ACK] Seq=495 Ack=1406
63	10.0.0.100	207.46.0.76	MSNMS	CHG 8 NLN 268435456 %3Cmsnobj%20Creato
64	207.46.0.76	10.0.0.100	MSNMS	URL 9 /cgi-bin/HotMail https://login.p
65	10.0.0.100	207.46.0.76	TCP	ncpm-pm > msnp [ACK] Seq=797 Ack=1488
66	207.46.0.76	10.0.0.100	MSNMS	URL 10 /cgi-bin/compose https://login.
67	10.0.0.100	207.46.0.76	TCP	ncpm-pm > msnp [ACK] Seq=797 Ack=1571
68	207.46.0.76	10.0.0.100	MSNMS	QNG 45
69	10.0.0.100	207.46.0.76	TCP	ncpm-pm > msnp [ACK] Seq=797 Ack=1579
70	207.46.0.76	10.0.0.100	MSNMS	CHG 8 NLN 268435456 %3Cmsnobj%20Creato
71	10.0.0.100	207.46.0.76	TCP	ncpm-pm > msnp [ACK] Seq=797 Ack=1847
72	207.46.0.76	10.0.0.100	MSNMS	ILN 8 NLN bot2k3@gmail.com BOT2K3%20:
73	10.0.0.100	207.46.0.76	TCP	ncpm-pm > msnp [ACK] Seq=797 Ack=2178
74	10.0.0.100	207.46.0.76	MSNMS	PNG
75	207.46.0.76	10.0.0.100	MSNMS	QNG 40

Mark Packet (toggle)  
Time Reference  
Apply as Filter  
Prepare a Filter  
Follow TCP Stream  
Decode As...  
Print...  
Show Packet in New Window

Frame 63 (368 bytes on wire) (Captured on interface eth0)  
Ethernet II, Src: 00:30:8c:00:00:00, Dst: 08:00:00:08:00:00  
Internet Protocol, Src Address: 10.0.0.100, Destination: 207.46.0.76  
Transmission Control Protocol, Src Port: 495, Destination Port: 1325  
MSN Messenger Service  
CHG 8 NLN 268435456 %3Cmsnobj%20Creato r%3D%22k  
URL 9 INBOX\r\n  
URL 10 COMPOSE\r\n  
PNG\r\n

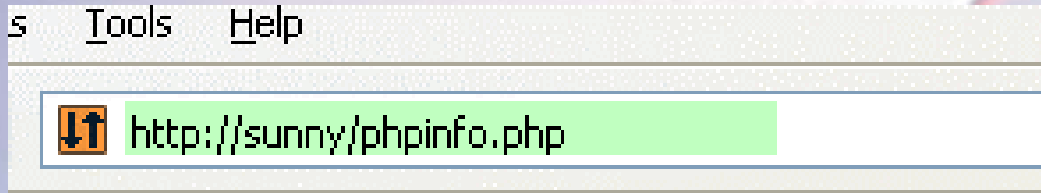
File: (Untitled) 104 | P: 84 | D: 67 | M: 0 | Drops: 0

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

# Εγκληματολογική εξέταση - ίχνη



Όταν πληκτρολογούμε μία δ/υση 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



Address  D:\Documents and Settings\... \Local Settings\Temporary Internet Files

Name	Internet Address	T...	Size	Last Modif
 phpinfo.php	http://sunny/phpinfo.php	H...	37 KB	None
 phpinfo.php?PHPE9568F34-D428-11d2-A769-00AA001ACF42	http://sunny/phpinfo.php?PHPE9568F34-D428-11d2-A769-00AA001ACF42	A...	5 KB	None
 phpinfo.php?PHPE9568F35-D428-11d2-A769-00AA001ACF42	http://sunny/phpinfo.php?PHPE9568F35-D428-11d2-A769-00AA001ACF42	A...	3 KB	None

Documents and Settings\mdm2\Local Settings\Temporary Internet Files\Content.IE5\AN2ZMX6T

Name	Size	Type	Date Modified
 phpinfo[1].gif	5 KB	ACDSee 7.0 GIF Im...	29/5/2006 00:39

Address  D:\Documents and Settings\... \Local Settings\Temporary Internet Files\Content.IE5\Q1IPQV2T

Name	Size	T...	Date Modified	Owner
 phpinfo[1].gif	3 KB	A...	29/5/2006 00:39	...
 pixel_black[1].gif	1 KB	A...	25/4/2006 18:25	...



# Η/Υ δράστη

Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	
url10	REG_SZ	
url11	REG_SZ	
url12	REG_SZ	
url13	REG_SZ	http://sunny.phpinfo.php
url14	REG_SZ	
url15	REG_SZ	
url16	REG_SZ	
url17	REG_SZ	
url18	REG_SZ	
url19	REG_SZ	
url2	REG_SZ	
url20	REG_SZ	
url21	REG_SZ	
url22	REG_SZ	
url23	REG_SZ	
url24	REG_SZ	
url25	REG_SZ	
url3	REG_SZ	
url4	REG_SZ	
url5	REG_SZ	
url6	REG_SZ	
url7	REG_SZ	
url8	REG_SZ	
url9	REG_SZ	

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](mailto:forensix@mopo.gr)**  
**Cell: +30 6932 355 775**