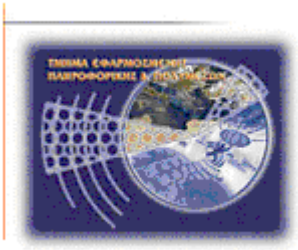
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Τίτλος: PASSWORD CRACKING

Θεοδωράκης Δημήτρης (ΑΜ: 1574)
epp1574@epp.teiher.gr

Ηράκλειο - Ημερομηνία

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

***Υπεύθυνη δήλωση**: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επόπτη καθηγητή της εργασίας μου κύριο Χαράλαμπο Μανιφάβα, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτή την εργασία, για την πολύτιμη βοήθεια και καθοδήγησή του καθ' όλη τη διάρκειά της και κυρίως για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα πολύ ενδιαφέρον αντικείμενο.

Ιστορικό εκδόσεων

Ημερομηνία	Έκδοση	Λεπτομέρειες
20/10/2009	1.1	
02/03/2010	2	
09/03/2010	2.1	
24/04/2010	2.2	
03/05/2010	3	

Πίνακας Περιεχομένων

ΚΕΦΆΛΑΙΟ 1 ΕΙΣΑΓΩΓΉ 1

1.1 Γενικά 1
1.2 Σκοπός 1
1.3 Συνοπτική Περιγραφή 2
1.4 Σχεδιάγραμμα Αναφοράς 2

ΚΕΦΆΛΑΙΟ 2 ΚΡΥΠΤΟΓΡΆΦΗΣΗ 3

2.1 Γενικά 3
2.2 TrueCrypt 4
2.2.1 Γενικά 4
2.2.2 Η λογική του TrueCrypt 4
2.2.3 Στην πράξη 5

ΚΕΦΆΛΑΙΟ 3 PASSWORD POLICY 29

3.1 Κύρια χαρακτηριστικά ενός Password Policy 29
3.2 Επιλέγοντας την κατάλληλη πολιτική 30
3.3 Εκτιμήσεις χρησιμότητας 30
3.4 Πολιτική facebook 32

ΚΕΦΑΛΑΙΟ 4 PASSWORD STRENGTH 35

4.1 Password meter 35
4.2 Δημιουργια δυνατου κωδικου στα Windows XP 38
4.3 Password Safe 40
4.4 KeePass 45
4.5 Firefox master password 49

ΚΕΦΆΛΑΙΟ 5 ΣΠΆΣΙΜΟ ΚΩΔΙΚΟΎ ADMINISTRATOR ΚΑΙ BIOS 57

5.1 Administrator ο εύκολος τρόπος (μέσω safe mode) 57
5.2 Administrator ο δύσκολος τρόπος 59
5.3 Bios password crack 62

ΚΕΦΆΛΑΙΟ 6 PHISHING 64

6.1 Ενδείξεις πως ένα ηλεκτρονικό μήνυμα είναι πιθανόν πλαστό 64
6.2 Τρόποι προφύλαξης από το Phishing 65

ΚΕΦΑΛΑΙΟ 7 ΧΡΗΣΗ ΠΡΟΓΡΑΜΜΑΤΩΝ ΑΝΑΚΤΗΣΗΣ ΚΩΔΙΚΩΝ 69

7.1 Πίσω από τα αστεράκια 69
7.2 Keyfinder 73

7.3 ΑΣΎΡΜΑΤΑ ΔΊΚΤΥΑ 76
7.4 ΚΩΔΙΚΟΊ ΔΙΚΤΥΑΚΏΝ ΠΡΟΓΡΑΜΜΆΤΩΝ 77
7.4.1 E-MAIL 77
7.4.2 INSTANT MESSAGING 78
7.4.3 ΑΝΆΚΤΗΣΗ ΚΩΔΙΚΏΝ ΣΎΝΔΕΣΗΣ INTERNET 80
7.5 BROWSER 81
7.5.1 INTERNET EXPLORER 81
7.5.2 MOZILLA FIREFOX, GOOGLE CHROME 82
7.6 RAR PASSWORD RECOVERY 84
7.7 JOHN THE RIPPER (JTR) 89
7.8 CAIN & ABEL 94

ΚΕΦΆΛΑΙΟ 8 PASSWORD STATISTICS 103

8.1 ΟΙ ΠΙΟ ΑΔΎΝΑΜΟΙ ΚΩΔΙΚΟΊ ΣΤΟ ΔΙΑΔΊΚΤΥΟ 103
8.2 ΧΡΌΝΟΙ ΑΝΆΚΤΗΣΗΣ ΚΩΔΙΚΏΝ 105

ΚΕΦΑΛΑΙΟ 9 ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ 110

ΒΙΒΛΙΟΓΡΑΦΙΑ 117

Πίνακας Εικόνων

Εικόνα 1: αρχικό παράθυρο TrueCrypt 5
Εικόνα 2: Truecrypt οδηγός δημιουργίας νέας μονάδας 6
Εικόνα 3: Truecrypt επιλογή κανονικού ή κρυφού volume 6
Εικόνα 4: Truecrypt τοποθεσία volume 7
Εικόνα 5: Truecrypt αποθήκευση volume 8
Εικόνα 6: Truecrypt επιλογή τοποθεσίας volume 8
Εικόνα 7: Truecrypt επιλογή αλγόριθμου κρυπτογράφησης 9
Εικόνα 8: Truecrypt μέγεθος εικονικής μονάδας 9
Εικόνα 9: Truecrypt επιλογή κωδικού για το volume 10
Εικόνα 10: Truecrypt προειδοποίηση ασφάλειας για κωδικό 10
Εικόνα 11: Truecrypt δημιουργία volume 11
Εικόνα 12: Truecrypt μήνυμα επιτυχίας δημιουργίας volume 11
Εικόνα 13: Truecrypt εικονική μονάδα έτοιμη για χρήση 12
Εικόνα 14: Truecrypt επιλογή γράμματος για εικονική μονάδα 12
Εικόνα 15: επιλογή Truecrypt volume 13
Εικόνα 16: Truecrypt mount volume 14
Εικόνα 17: Truecrypt εισαγωγή κωδικού για να γίνει mount 14
Εικόνα 18: Truecrypt εικονικός τόμος έτοιμος 15
Εικόνα 19: παράθυρο Ο Υπολογιστής μου 16
Εικόνα 20: Truecrypt dismount volume 16
Εικόνα 21: Truecrypt volume σε usb flash drive 17
Εικόνα 22: Truecrypt standard volume 18
Εικόνα 23: Truecrypt τοποθεσία volume 18
Εικόνα 24: Truecrypt επιλογή συσκευής 19
Εικόνα 25: Truecrypt ερώτηση επιβεβαίωσης κρυπτογράφησης 19
Εικόνα 26: Truecrypt volume creation mode 20
Εικόνα 27: Truecrypt επιλογή αλγορίθμου κρυπτογράφησης 20
Εικόνα 28: Truecrypt μέγεθος volume 21
Εικόνα 29: Truecrypt κωδικός volume 21
Εικόνα 30: Truecrypt διαμόρφωση volume 22
Εικόνα 31: Truecrypt επιβεβαίωση διαμόρφωσης 22
Εικόνα 32: Truecrypt επιτυχία δημιουργίας volume 22
Εικόνα 33: Truecrypt εισαγωγή κωδικού 23
Εικόνα 34: παράθυρο Ο υπολογιστής μου 23
Εικόνα 35: Truecrypt επιλογή για hidden volume 24
Εικόνα 36: Truecrypt επιλογή direct mode 25
Εικόνα 37: Truecrypt τοποθεσία volume 25
Εικόνα 38: Truecrypt κωδικός outer volume 26
Εικόνα 39: Truecrypt επιλογή αλγορίθμου κρυπτογράφησης 26
Εικόνα 40: Truecrypt μέγεθος hidden volume 27
Εικόνα 41: Truecrypt κωδικός hidden volume 27
Εικόνα 42: Truecrypt διαμόρφωση hidden volume 28
Εικόνα 43: facebook αρχική 32
Εικόνα 44: facebook αλλαγή κωδικού 32
Εικόνα 45: email αλλαγής κωδικού 33
Εικόνα 46: facebook επιβεβαίωση αλλαγής κωδικού 33
Εικόνα 47: facebook password meter 34

Εικόνα 48: password meter αρχική....35
Εικόνα 49: password meter εισαγωγή εύκολου κωδικού....35
Εικόνα 50: password meter υπολογισμός ασφαλείας κωδικού....36
Εικόνα 51: password meter εισαγωγή δυνατού κωδικού....36
Εικόνα 52: password meter υπολογισμός ασφαλείας κωδικού....37
Εικόνα 53: πατάμε έναρξη και εκτέλεση....38
Εικόνα 54: πληκτολογούμε cmd....39
Εικόνα 55: γραμμή εντολών....39
Εικόνα 56: cmd εντολή για δημιουργία κωδικού....39
Εικόνα 57: password safe αρχική....40
Εικόνα 58: password safe επιλογή δυνατού κωδικού....40
Εικόνα 59: περιβάλλον εργασίας passwordsafe....41
Εικόνα 60: password safe: edit και add entry....41
Εικόνα 61: επιλογές passwordsafe....42
Εικόνα 62: password safe δημιουργία νέου group....43
Εικόνα 63: password safe αποθηκευμένα group και κωδικοί....44
Εικόνα 64: αρχική του KeePass....45
Εικόνα 65: KeePass επιλογή κύριου κωδικού....45
Εικόνα 66: KeePass επιλογή ασφαλούς κύριου κωδικού....46
Εικόνα 67: παράθυρο KeePass....46
Εικόνα 68: KeePass επιλογές για τα group....47
Εικόνα 69: KeePass νέα καταχώρηση....47
Εικόνα 70: KeePass καταχωρήσεις στο group email....48
Εικόνα 71: Firefox επιλογές....49
Εικόνα 72: Firefox χρήση ενός κύριου κωδικού....50
Εικόνα 73: Firefox εισαγωγή κύριου κωδικού....50
Εικόνα 74: Firefox επιτυχής αλλαγή κύριου κωδικού....51
Εικόνα 75: Firefox εισαγωγή κύριου κωδικού....51
Εικόνα 76: Firefox διαγραφή κύριου κωδικού....52
Εικόνα 77: Firefox επιτυχής αλλαγή κωδικού....52
Εικόνα 78: ανοίγουμε ένα command prompt....54
Εικόνα 79: command prompt....54
Εικόνα 80: command prompt διαδρομή για Firemaster....54
Εικόνα 81: command prompt Firemaster....55
Εικόνα 82: command prompt Firemaster εντολή για crack....55
Εικόνα 83: command prompt Firemaster ανάκτηση κωδικού....56
Εικόνα 84: επιλογή safe mode....57
Εικόνα 85: Windows log in λογαριασμοί χρηστών....57
Εικόνα 86: εντολή control userpasswords2....58
Εικόνα 87: παράθυρο λογαριασμοί χρηστών....58
Εικόνα 88: ορισμός νέου κωδικού πρόσβασης....59
Εικόνα 89: πατάμε έναρξη εκτέλεση και πληκτρολογούμε cmd....59
Εικόνα 90: γραμμή εντολών....60
Εικόνα 91: αρχεία cmd.exe και logon.scr....60
Εικόνα 92: εντολές στο cmd....61
Εικόνα 93: default screensaver....61
Εικόνα 94: Bios password....62
Εικόνα 95:ανοίγουμε ενα command prompt....63
Εικόνα 96: command prompt εντολές για σβήσιμο cmos memory....63
Εικόνα 97: Firefox επιλογές....66

Εικόνα 98: Firefox επιλογές ασφαλείας 67
Εικόνα 99: Firefox Phishing protection 68
Εικόνα 100: πεδία τύπου password 69
Εικόνα 101: Asterisk Logger 70
Εικόνα 102: Asterisk Key 71
Εικόνα 103: Asterisk Key recover 71
Εικόνα 104: φάκελος keyfinder 73
Εικόνα 105: keyfinder κλειδί Windows XP 74
Εικόνα 106: keyfinder κλειδί office pro 2003 74
Εικόνα 107: keyfinder κλειδί FrontPage 2003 74
Εικόνα 108: keyfinder πληροφορίες σχετικά με τα windows 75
Εικόνα 109: keyfinder κλειδί power DVD 75
Εικόνα 110: φάκελος WirelessKeyView 76
Εικόνα 111: WirelessKeyView αποκάλυψη κωδικών 76
Εικόνα 112: φάκελος mailpv 77
Εικόνα 113: mailpv αποκάλυψη κωδικών 78
Εικόνα 114: φάκελος mspass 78
Εικόνα 115: MessenPass αποκάλυψη κωδικών 79
Εικόνα 116: φάκελος dialupass 80
Εικόνα 117: Dialupass αποκάλυψη κωδικών 80
Εικόνα 118: φάκελος iepv 81
Εικόνα 119: IE Passview αποκάλυψη κωδικών 82
Εικόνα 120: ChromePass αποκάλυψη κωδικών 82
Εικόνα 121: PasswordFox αποκάλυψη κωδικών 83
Εικόνα 122: δεξί κλικ και συμπίεση στο 84
Εικόνα 123: winrar κλείδωμα αρχείου 85
Εικόνα 124: winrar κωδικός πρόσβασης 85
Εικόνα 125: winrar συμπίεση αρχείου 86
Εικόνα 126: φάκελος και συμπιεσμένος 86
Εικόνα 127: Advanced Archive Password Recovery αρχική 87
Εικόνα 128: Advanced Archive Password Recovery εύρεση κωδικού 88
Εικόνα 129: Advanced Archive Password Recovery ανάκτηση κωδικού 88
Εικόνα 130: mock-unix-password-file.txt 89
Εικόνα 131: John The Ripper 90
Εικόνα 132: πατάμε έναρξη εκτέλεση και πληκτρολογούμε cmd 90
Εικόνα 133: command prompt 91
Εικόνα 134: cmd άνοιγμα φακέλου run 91
Εικόνα 135: JTR εύρεση κωδικών 92
Εικόνα 136: JTR αποτελέσματα κωδικών 92
Εικόνα 137: Cain αρχική 94
Εικόνα 138: Εγκατάσταση Abel 95
Εικόνα 139: Cain network 96
Εικόνα 140: Cain εισαγωγή IP 96
Εικόνα 141: Cain quick list 97
Εικόνα 142: Cain Users 97
Εικόνα 143: Cain Cracker 98
Εικόνα 144: Cain hashes 98
Εικόνα 145: Cain λογαριασμοί χρηστών 99
Εικόνα 146: Cain επιλογή επίθεσης 100
Εικόνα 147: Cain Brute Force Attack 101

Εικόνα 148: Cain Hash Cracked 101
Εικόνα 149: Cain εύρεση κωδικού 102

Πίνακας Πινάκων

Πίνακας 1: Χρόνοι ανάκτησης κωδικών περίπτωση 1 - Μόνο αριθμοί 105
Πίνακας 2: Χρόνοι ανάκτησης κωδικών περίπτωση 1 - παραδείγματα 106
Πίνακας 3: Χρόνοι ανάκτησης κωδικών περίπτωση 2 - Όλο το αλφάβητο (κεφαλαία ή μικρά) 106
Πίνακας 4: Χρόνοι ανάκτησης κωδικών περίπτωση 2- παραδείγματα 106
Πίνακας 5: Χρόνοι ανάκτησης κωδικών περίπτωση 3 - Όλο το αλφάβητο και αριθμοί 107
Πίνακας 6: Χρόνοι ανάκτησης κωδικών περίπτωση 3- παραδείγματα 107
Πίνακας 7: Χρόνοι ανάκτησης κωδικών περίπτωση 4 - Όλο το αλφάβητο (κεφαλαία και μικρά) 107
Πίνακας 8: Χρόνοι ανάκτησης κωδικών περίπτωση 4- παραδείγματα 107
Πίνακας 9: Χρόνοι ανάκτησης κωδικών περίπτωση 5 - Όλο το αλφάβητο και αριθμοί 108
Πίνακας 10: Χρόνοι ανάκτησης κωδικών περίπτωση 5- παραδείγματα 108
Πίνακας 11: Χρόνοι ανάκτησης κωδικών περίπτωση 6 - Όλο το αλφάβητο και σύμβολα 108
Πίνακας 12: Χρόνοι ανάκτησης κωδικών περίπτωση 6- Παραδείγματα 108
Πίνακας 13: Χρόνοι ανάκτησης κωδικών περίπτωση 7 - Όλο το αλφάβητο αριθμοί και σύμβολα 109
Πίνακας 14: Χρόνοι ανάκτησης κωδικών περίπτωση 7- παραδείγματα 109

Κεφάλαιο 1 Εισαγωγή

1.1 Γενικά

Ο κωδικός πρόσβασης είναι μια μυστική λέξη ή συμβολοσειρά χαρακτήρων που χρησιμοποιείται για έλεγχο ταυτότητας, για να αποδειχθεί η ταυτότητα ή για να αποκτηθεί πρόσβαση σε έναν λογαριασμό. Ο κωδικός πρόσβασης πρέπει να παραμένει απόρρητος από αυτούς στους οποίους δεν επιτρέπεται η πρόσβαση.

Ένας κωδικός πρόσβασης δεν είναι απαραίτητο να αποτελείται από πραγματικές λέξεις. Κωδικοί που δεν είναι πραγματικές λέξεις είναι πιο δύσκολο να τις μαντέψει κάποιος εισβολέας. Ορισμένοι κωδικοί σχηματίζονται από πολλές λέξεις. Ο κωδικός όρος μερικές φορές αποτελείται από ψηφία αριθμών, όταν υπάρχει ανάγκη οι μυστικές πληροφορίες να είναι αριθμοί, όπως ο προσωπικός αριθμός αναγνώρισης (PIN), που χρησιμοποιείται συνήθως για την πρόσβαση στα ATM. Οι κωδικοί πρόσβασης είναι γενικά αρκετά μικροί για να απομνημονεύονται εύκολα.

Το όνομα χρήστη και ο κωδικός είναι τα πιο σημαντικά στοιχεία που αποδεικνύουν την άδεια πρόσβασής μας σε ένα σύστημα. Κωδικούς χρειαζόμαστε και όταν δουλεύουμε σε ένα μεμονωμένο υπολογιστή αλλά κυρίως μέσα σε δίκτυα, όπως το ίντερνετ. Για να αποτρέψουμε επίδοξους εισβολείς ή απλά περίεργους να αποκτήσουν πρόσβαση στις δικές μας υπηρεσίες όπως email, forum κτλ, χρειαζόμαστε ένα ισχυρό κωδικό. Η ανάγκη αυτή γίνεται ακόμα πιο έντονη όταν οι κωδικοί μας είναι πολύτιμα κλειδιά σε υπηρεσίες φιλοξενίας ιστοσελίδων, σε διακομιστές, πίνακες ελέγχου φόρουμ, λογαριασμοί σε τράπεζες ή ακόμα και στο ίντρανετ της επιχείρησης μας.

1.2 Σκοπός

Η εργασία αυτή επικεντρώνεται στους κωδικούς πρόσβασης, την δύναμη τους και πως αυτοί μπορούν να παραβιαστούν από άλλο χρήστη. Επίσης συμπεριλαμβάνονται οδηγίες ασφαλείας και παραδείγματα ώστε να γίνει βαθύτερη κατανόηση του θέματος.

Πιο συγκεκριμένα αναλύονται τα παρακάτω θέματα:

- Κρυπτογράφηση δεδομένων
- Πολιτική κωδικών πρόσβασης
- Δύναμη κωδικών
- Ηλεκτρονικό ψάρεμα
- Σπάσιμο κωδικών (windows, αστεράκια, mail, messenger, browser, rar)
- Οδηγίες ασφάλειας

1.3 Συνοπτική Περιγραφή

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στην έννοια του κωδικού και στην χρησιμότητα των κωδικών πρόσβασης.
Το κεφάλαιο δύο αναφέρεται στην κρυπτογράφηση των δεδομένων. Γίνεται επεξήγηση της έννοιας και παρουσίαση κάποιων προγραμμάτων της κρυπτογράφησης.
Το τρίτο κεφάλαιο αναφέρεται στην πολιτική των κωδικών πρόσβασης. Συγκεκριμένα αναλύονται τα κύρια χαρακτηριστικά ενός password policy, επιλογή κατάλληλης πολιτικής και εκτιμήσεις χρησιμότητας. Επίσης γίνεται ένας έλεγχος στην πολιτική κωδικών που χρησιμοποιεί το facebook.
Στο κεφάλαιο τέσσερα αναλύεται η δύναμη ενός κωδικού και το πόσο ασφαλής μπορεί να είναι.
Στο πέμπτο κεφάλαιο παρουσιάζονται τρόποι σπασίματος του Administrator password και του Bios σε ένα PC.
Το έκτο κεφάλαιο είναι αφιερωμένο στο ηλεκτρονικό ψάρεμα γνωστό και ως phishing.
Στο κεφάλαιο επτά γίνεται παρουσίαση προγραμμάτων ανάκτησης κωδικών με παραδείγματα.
Στο κεφάλαιο οκτώ παρουσιάζονται κάποια στατιστικά στοιχεία σε σχέση με τους κωδικούς.
Τέλος το ένατο κεφάλαιο περιλαμβάνει κάποιες οδηγίες ασφάλειας για τη σωστή χρήση του διαδικτύου.

1.4 Σχεδιάγραμμα Αναφοράς

Αριθμός κεφαλαίου	Τίτλος
1	Εισαγωγή
2	Κρυπτογράφηση
3	Password policy
4	Password strength
5	Σπάσιμο κωδικού Administrator
6	Phishing
7	Χρήση προγραμμάτων ανάκτησης κωδικών
8	Password statistics
9	Οδηγίες ασφάλειας

Κεφάλαιο 2 Κρυπτογράφηση

2.1 Γενικά

Σχεδόν όλοι οι σύγχρονοι μηχανισμοί ασφάλειας βασίζονται στο γεγονός ότι ορισμένα μυστικά, κρατούνται ιδιωτικά σε ορισμένα άτομα. Τα συστήματα ασφάλειας χρησιμοποιούν κρυπτογράφηση για να κρατούν μυστικά και χρησιμοποιούν επαλήθευση για να αποδεικνύουν την ταυτότητα συγκεκριμένων ατόμων.
Κρυπτογράφηση (encryption) είναι η διαδικασία κωδικοποίησης ενός μηνύματος καθαρού κειμένου, έτσι ώστε να μην μπορεί να γίνει κατανοητό από ενδιάμεσα μέρη, που δεν γνωρίζουν το κλειδί για να το αποκρυπτογραφήσουν.
Ο κύριος σκοπός της κρυπτογράφησης είναι να κρατά μυστικά. Αρχικά χρησιμοποιήθηκε για να προστατεύει μηνύματα, έτσι ώστε μόνο το άτομο που γνώριζε το τέχνασμα αποκωδικοποίησης ενός μηνύματος να μπορεί να το διαβάσει. Σήμερα η κρυπτογράφηση επιτρέπει σε υπολογιστές να κρατούν μυστικά, μετασχηματίζοντας δεδομένα σε μια ακατάληπτη μορφή, χρησιμοποιώντας μια μαθηματική συνάρτηση. Όπως συμβαίνει και στην απλή αριθμητική, οι συναρτήσεις κρυπτογράφησης συνδυάζουν το μήνυμα και το κλειδί κρυπτογράφησης για να παράγουν ένα κρυπτογραφημένο αποτέλεσμα. Αν δεν γνωρίζει κάποιος το μυστικό κλειδί, το αποτέλεσμα δεν θα σημαίνει τίποτα.
Η πιο συνηθισμένη χρήση της κρυπτογράφησης με τους υπολογιστές είναι για προστασία των επικοινωνιών ανάμεσα σε χρήστες και σε συσκευές επικοινωνίας.
Τα περισσότερα σύγχρονα λειτουργικά συστήματα έχουν διαμορφωθεί έτσι ώστε να επιτρέπουν μόνο σε εξουσιοδοτημένους χρήστες να προσπελαύνουν αρχεία όταν λειτουργεί το λειτουργικό σύστημα, αλλά όταν σβήνουμε τον υπολογιστή, όλα αυτά τα χαρακτηριστικά ασφαλείας χάνονται και τα δεδομένα μας μένουν ανυπεράσπιστα. Ένας εισβολέας μπορεί να φορτώσει ένα άλλο λειτουργικό σύστημα στον υπολογιστή ή ακόμα να αφαιρέσει το σκληρό δίσκο και να τον τοποθετήσει σε έναν άλλο υπολογιστή, που δεν ακολουθεί τις ρυθμίσεις ασφάλειας του αρχικού υπολογιστή, οπότε τα δεδομένα μας θα είναι προσπελάσιμα. Η κρυπτογράφηση λύνει αυτό το πρόβλημα, σιγουρεύοντας ότι τα δεδομένα είναι ακατάληπτα, αν δεν δοθεί το σωστό κλειδί, ανεξάρτητα από το αν ο υπολογιστής συνεχίζει να λειτουργεί και να προστατεύει τα δεδομένα.

2.2 TrueCrypt

2.2.1 Γενικά

Όλοι μας έχουμε κάποια αρχεία στον υπολογιστή που θέλουμε να κρατήσουμε μακριά από τα αδιάκριτα βλέμματα και χέρια. Μπορεί το μόνο που μας νοιάζει να είναι η ασφάλεια τους, μπορεί όμως να θέλουμε οι άλλοι να μη γνωρίζουν καν την ύπαρξη τους. Σε κάθε περίπτωση πάντως η λύση είναι μία: να χρησιμοποιήσουμε ένα σύστημα ή πρόγραμμα κρυπτογράφησης. Ανάλογα με τις δυνατότητες του προγράμματος, μπορούμε είτε να κλειδώσουμε τα αρχεία μας, απαγορεύοντας ουσιαστικά την πρόσβαση στους ανεπιθύμητους, είτε να τα κλειδώσουμε και ταυτόχρονα να τα κρύψουμε ώστε να μην γνωρίζει την ύπαρξη τους ο πιθανός εισβολέας.
Ένα από τα προγράμματα που μπορούν να κλειδώνουν αλλά και να κρύβουν αρχεία είναι το TrueCrypt. Το πρόγραμμα διατίθεται δωρεάν (για την ακρίβεια αποτελεί ανοιχτό λογισμικό) και κυκλοφορεί για Windows 2000/ XP/ VISTA/ 7 και Linux.[1]
Τα σημαντικότερα χαρακτηριστικά του TrueCrypt είναι δύο: η μεγάλη ευκολία χρήσης του και η δυνατότητα του να κρύβει αρχεία. Δεν χρειάζεται να γνωρίζει κάποιος πολλά περί κρυπτογράφησης για να χρησιμοποιήσει το πρόγραμμα. Ο άπειρος χρήστης μπορεί να κάνει εύκολα και αποτελεσματικά τη δουλεία του χρησιμοποιώντας απλώς τις προεπιλεγμένες ρυθμίσεις. Επιπλέον διαθέτει wizards που αναλαμβάνουν να καθοδηγούν βήμα προς βήμα το χρήστη σε όλες τις διαδικασίες της κρυπτογράφησης.
Το δεύτερο σημαντικό χαρακτηριστικό του TrueCrypt είναι η δυνατότητα να κρύβει αρχεία. Τα προγράμματα κρυπτογράφησης συνήθως κλειδώνουν τα αρχεία ή τα partition, χωρίς όμως να κρύβουν το γεγονός αυτό. Έτσι ναι μεν ο αδιάκριτος δεν θα έχει πρόσβαση στα δεδομένα μας, αλλά θα γνωρίζει ότι υπάρχει απαγορευμένος καρπός. Με το TrueCrypt είναι εξαιρετικά δύσκολο (αν όχι αδύνατον) να διαπιστώσει κανείς ότι υπάρχουν κρυφά, κρυπτογραφημένα αρχεία. Δεδομένου ότι το απαγορευμένο προκαλεί μια ακαταμάχητη έλξη στον άνθρωπο, είναι μεγάλο πλεονέκτημα να μην υπάρχει πιθανότητα να γίνει γνωστή η ύπαρξη κρυφών αρχείων.

2.2.2 Η λογική του TrueCrypt

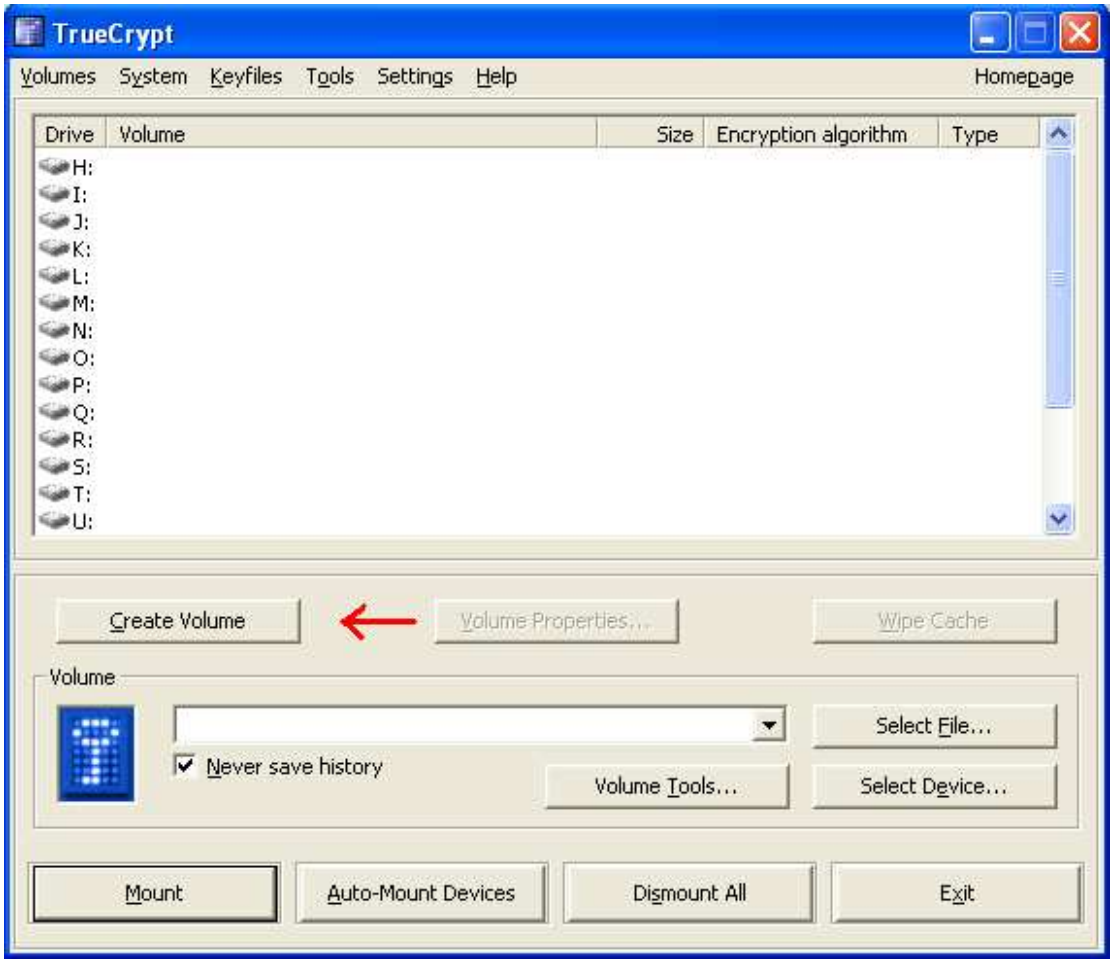
Ο τρόπος λειτουργίας του TrueCrypt είναι απλός και αποτελεσματικός. Το πρόγραμμα μπορεί να κρυπτογραφήσει μεμονωμένα αρχεία, φακέλους, κατατμήσεις, σκληρούς δίσκους αλλά και φορητές συσκευές όπως φλασάκια usb. Αν πρόκειται για μεμονωμένα αρχεία ή φακέλους, δημιουργεί ένα αρχείο, στο οποίο αποθηκεύει τα δεδομένα που θα του υποδείξουμε. Αν θέλουμε να γράψουμε, να σβήσουμε ή να αποκτήσουμε πρόσβαση στα δεδομένα που βρίσκονται μέσα στο κρυπτογραφημένο αρχείο, αρχικά το πρόγραμμα μας ζητάει τον κωδικό ασφάλειας και στη συνέχεια δημιουργεί μια εικονική συσκευή με βάση το αρχείο αυτό. Κάνει δηλαδή mount το αρχείο όπως συμβαίνει με το daemon tools των windows. Από κει και πέρα ο χρήστης μπορεί, εργαζόμενος με την εικονική συσκευή, να γράψει, να σβήσει, να διαβάσει και γενικότερα ότι θα έκανε αν είχε μια κανονική συσκευή αποθήκευσης. Κάθε φορά που γράφονται ή διαβάζονται δεδομένα στην εικονική συσκευή, το TrueCrypt φροντίζει

[1] www.truecrypt.org

να τα αποκρυπτογραφεί ή να τα κρυπτογραφεί αντίστοιχα. Η όλη διαδικασία γίνεται στην μνήμη του υπολογιστή.

2.2.3 Στην πράξη

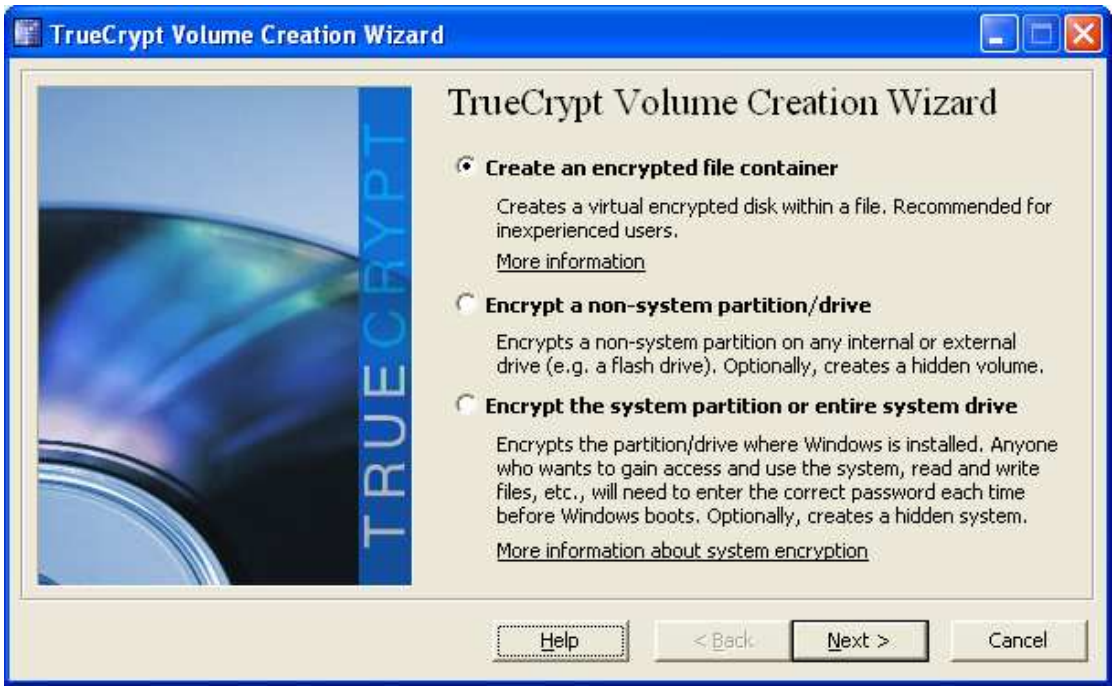
Αφού κάνουμε την εγκατάσταση του TrueCrypt, όπως μια τυπική εγκατάσταση προγράμματος των windows, το εκτελούμε και το πρώτο παράθυρο που βλέπουμε είναι το παρακάτω:



Εικόνα 1: αρχικό παράθυρο TrueCrypt

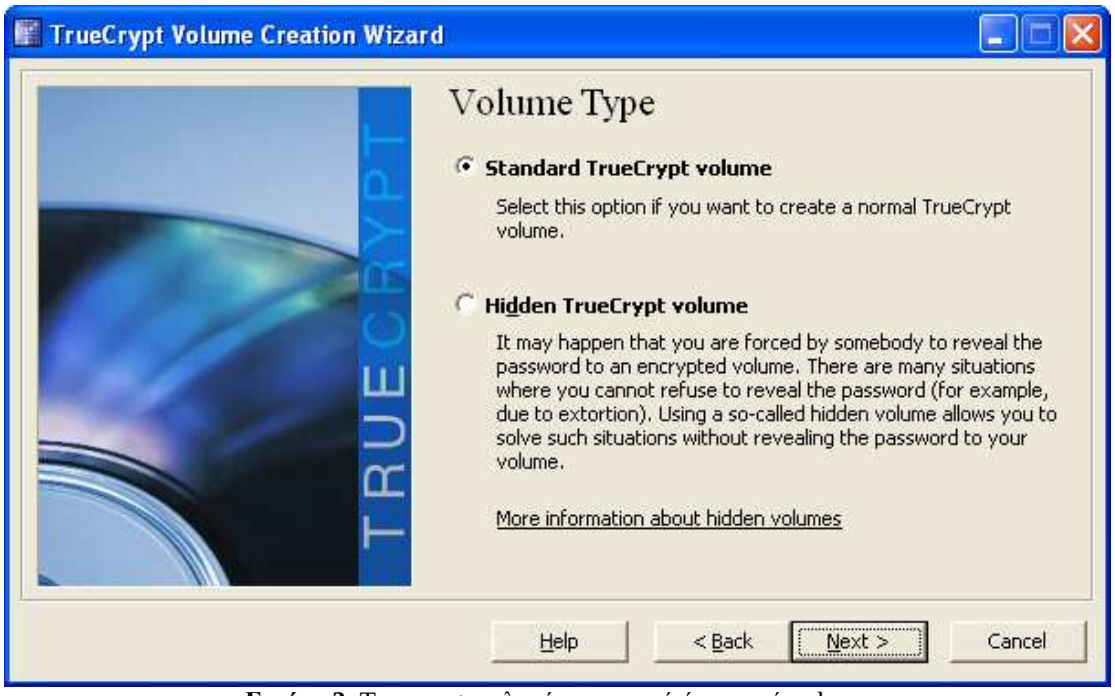
Πατάμε πάνω στο κουμπί Create Volume και εμφανίζεται το ακόλουθο παράθυρο.

Volume σε αρχείο



Εικόνα 2: Truecrypt οδηγός δημιουργίας νέας μονάδας

Μόλις ανοίξαμε τον οδηγό δημιουργίας νέας μονάδας. Σε αυτό το βήμα επιλέγουμε που θα δημιουργηθεί η εικονική μονάδα. Μπορούμε να επιλέξουμε ένα αρχείο, κάποιο διαμέρισμα δίσκου ή ακόμα και ολόκληρο τον δίσκο. Στη συγκεκριμένη περίπτωση επιλέγουμε ένα αρχείο (Create an encrypted file container) και πατάμε Next. Οι υπόλοιπες περιπτώσεις θα εξεταστούν παρακάτω.

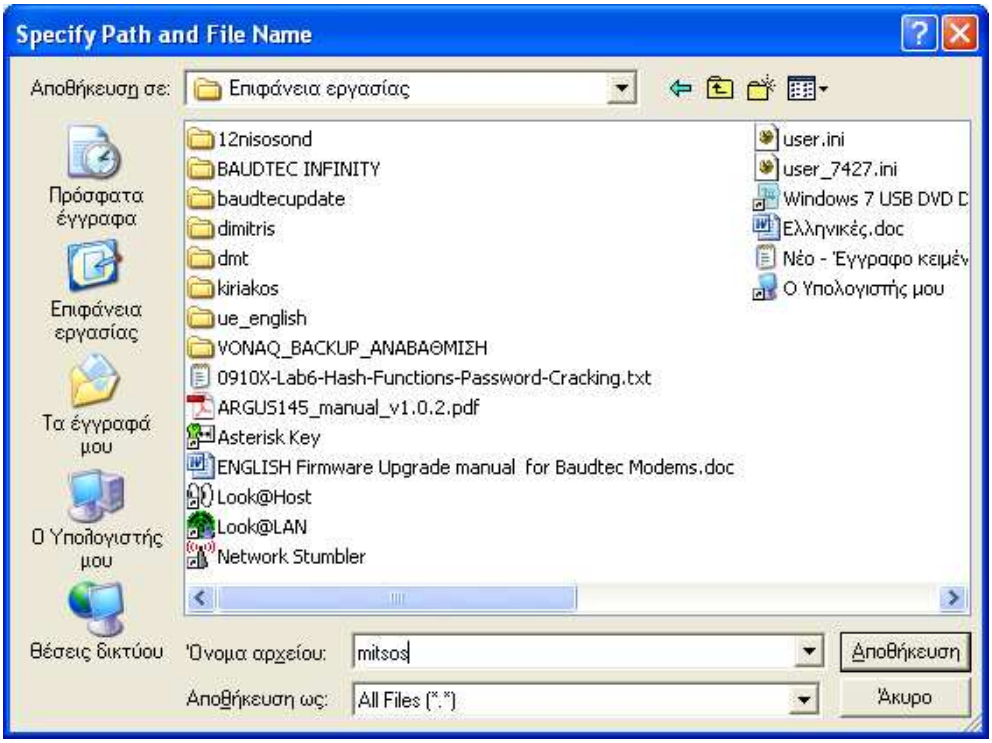


Εικόνα 3: Truecrypt επιλογή κανονικού ή κρυφού volume

Εδώ διαλέγουμε αν θα δημιουργήσουμε μία κανονική ή μια κρυφή μονάδα. Επιλέγουμε την κανονική (standard TrueCrypt volume) και πατάμε Next. Για να φτιάξουμε κρυφή μονάδα πρέπει πρώτα να δημιουργηθεί μια κανονική.

Εικόνα 4: Truecrypt τοποθεσία volume

Σε αυτό το βήμα καθορίζουμε την τοποθεσία στην οποία θα δημιουργηθεί το νέο volume. Να σημειώσουμε ότι το αρχείο που θα δημιουργηθεί είναι ακριβώς όπως ένα κανονικό αρχείο. Μπορεί να μετακινηθεί και να διαγραφεί οποιαδήποτε στιγμή. Επίσης χρειάζεται να δώσουμε και ένα όνομα στο αρχείο το οποίο θα χρησιμοποιήσουμε σε επόμενο βήμα. Πατάμε Select File…



Εικόνα 5: Truecrypt αποθήκευση volume

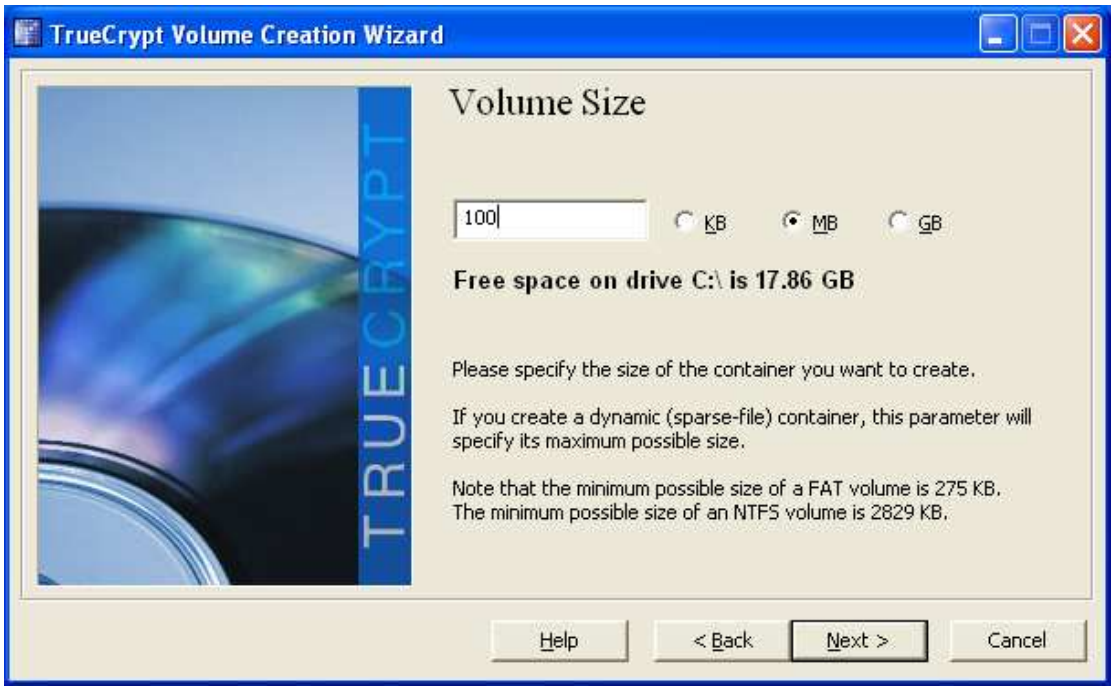
Έστω ότι ονομάζουμε το αρχείο mitsos και το αποθηκεύουμε στην επιφάνεια εργασίας.

Εικόνα 6: Truecrypt επιλογή τοποθεσίας volume

Συναντάμε πάλι το προηγούμενο παράθυρο και πατάμε Next.

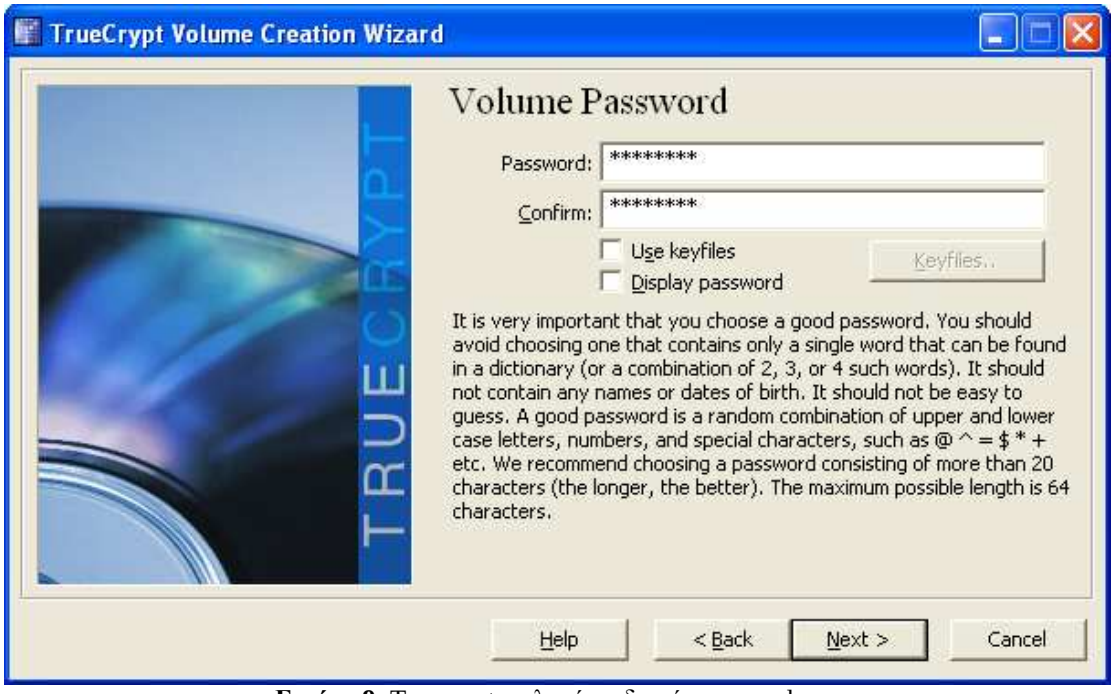
Εικόνα 7: Truecrypt επιλογή αλγόριθμου κρυπτογράφησης

Εδώ επιλέγουμε έναν αλγόριθμο κρυπτογράφησης και έναν αλγόριθμο για το volume. Στην συγκεκριμένη περίπτωση AES και πατάμε Next.



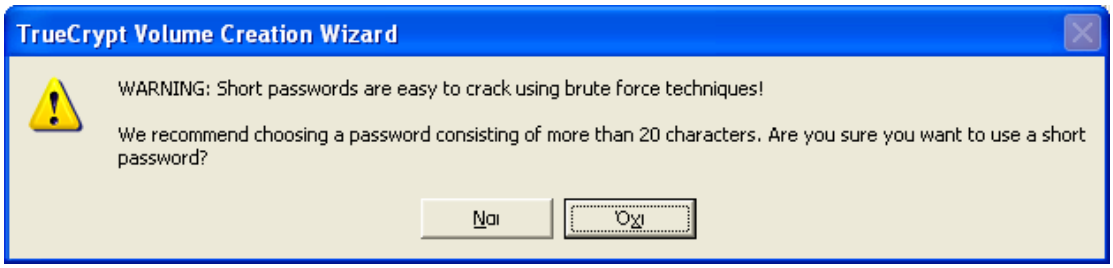
Εικόνα 8: Truecrypt μέγεθος εικονικής μονάδας

Στο επόμενο βήμα διαλέγουμε το μέγεθος που επιθυμούμε να έχει η νέα εικονική μονάδα. Εδώ 100 MegaByte και πατάμε Next.



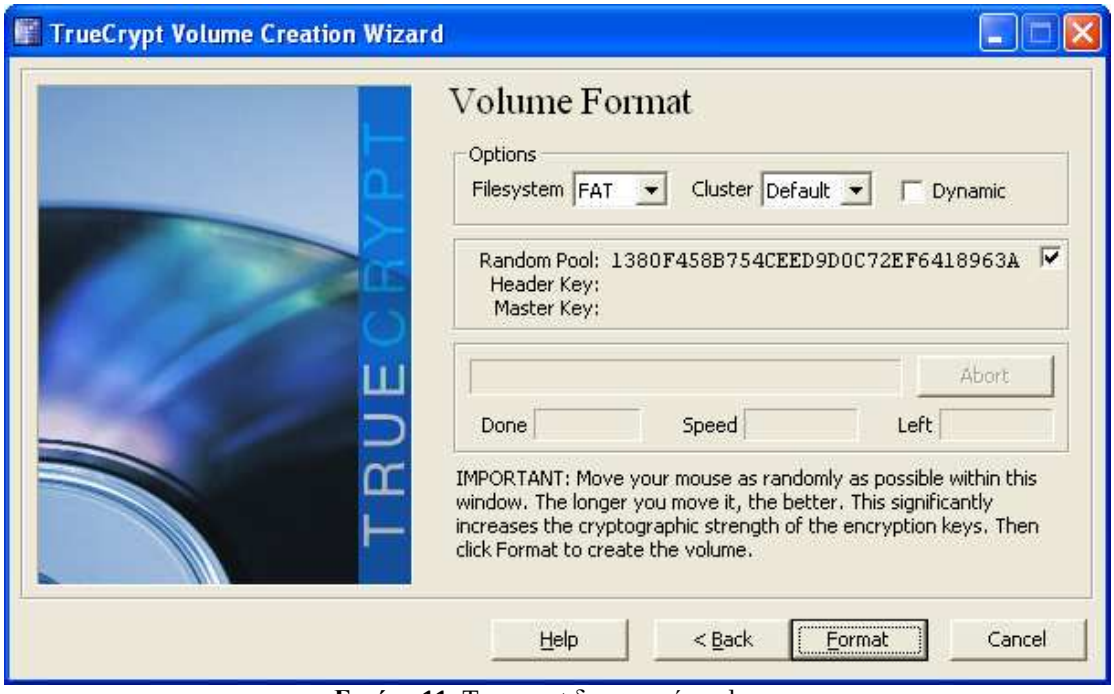
Εικόνα 9: Truecrypt επιλογή κωδικού για το volume

Στη συνέχεια ακολουθεί το πιο σημαντικό μέρος, η επιλογή ενός κωδικού δυνατού και ασφαλή. Από ότι παρατηρούμε το πρόγραμμα προτείνει μια πολιτική επιλογής δυνατού κωδικού. Να χρησιμοποιήσουμε πεζά, κεφαλαία γράμματα, αριθμούς και σύμβολα. Επίσης μας συνιστά ο κωδικός που θα βάλουμε να είναι μεγαλύτερος από είκοσι χαρακτήρες. Επιλέγουμε κωδικό και πατάμε Next.



Εικόνα 10: Truecrypt προειδοποίηση ασφάλειας για κωδικό

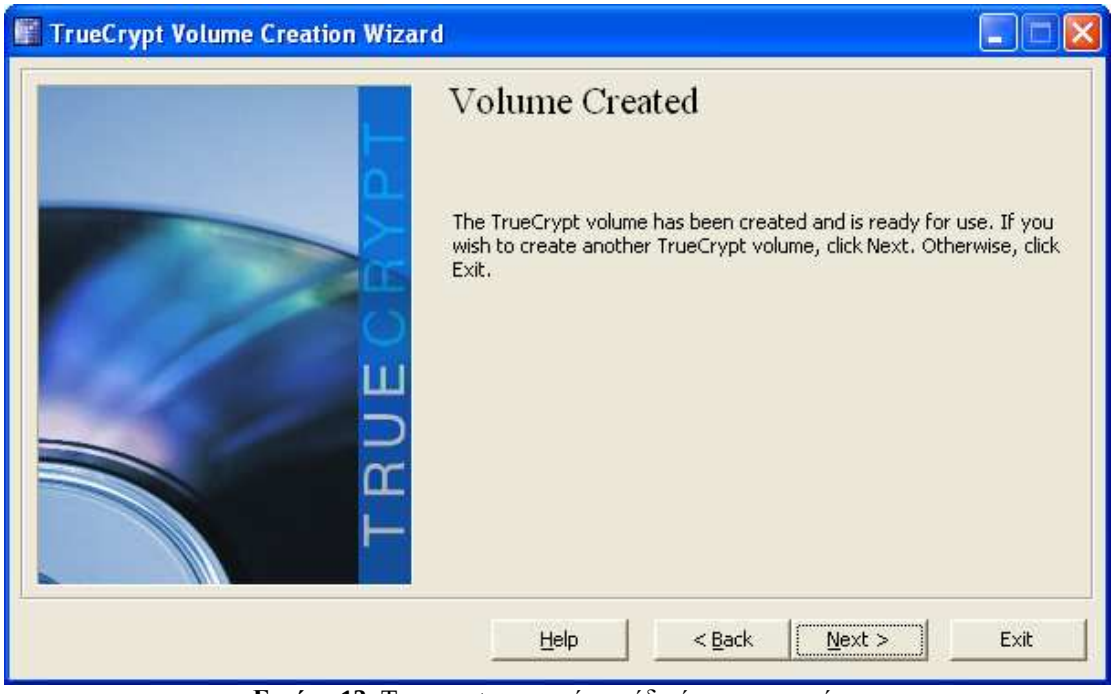
Επειδή ο κωδικός που χρησιμοποιήθηκε αποτελείται από 8 χαρακτήρες το TrueCrypt μας προειδοποιεί ότι δεν ακολουθεί την πολιτική του προγράμματος. Πατάμε ναι και συνεχίζουμε.



Εικόνα 11: Truecrypt δημιουργία volume

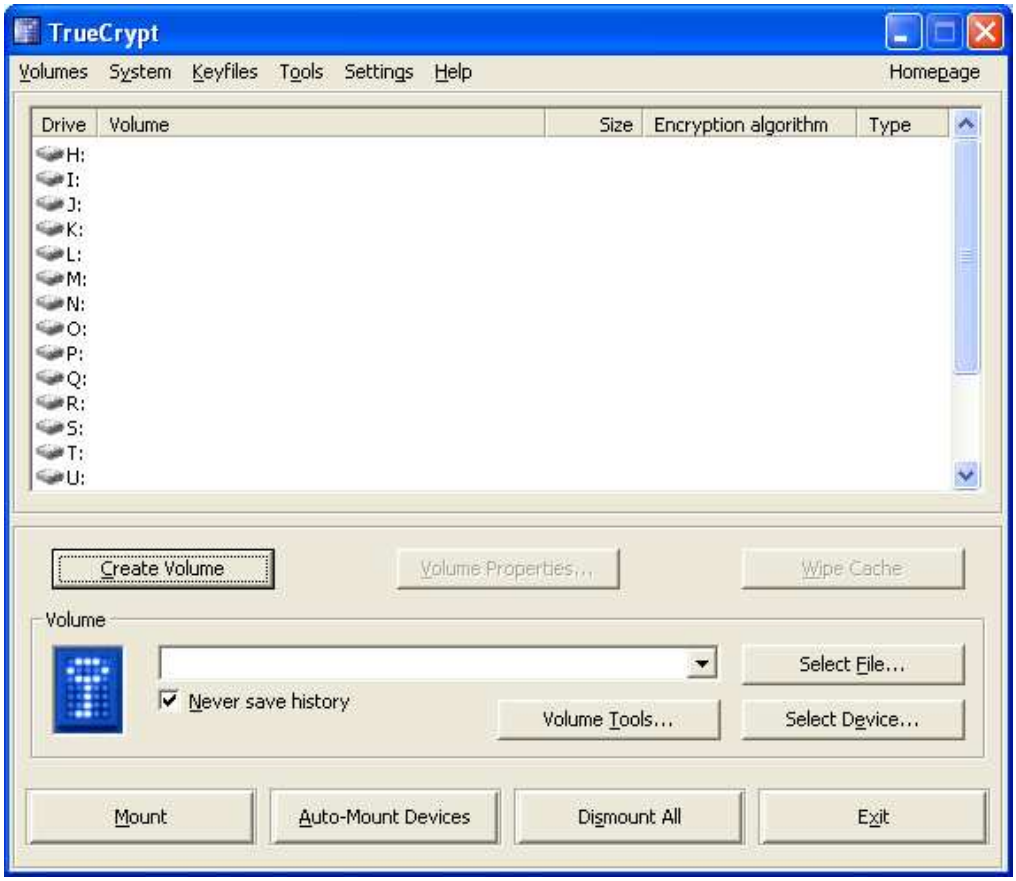
Τώρα πρέπει να μετακινήσουμε το ποντίκι μας όσο το δυνατόν τυχαία εντός του παραθύρου για τουλάχιστον 30 δευτερόλεπτα. Όσο περισσότερο μετακινήσουμε το ποντίκι τόσο το καλύτερο. Αυτό αυξάνει σημαντικά την κρυπτογραφική δύναμη των κλειδιών κρυπτογράφησης (η οποία αυξάνει την ασφάλεια). Έπειτα πατάμε Format και συνεχίζουμε παρακάτω.

Εικόνα 12: Truecrypt μήνυμα επιτυχίας δημιουργίας volume



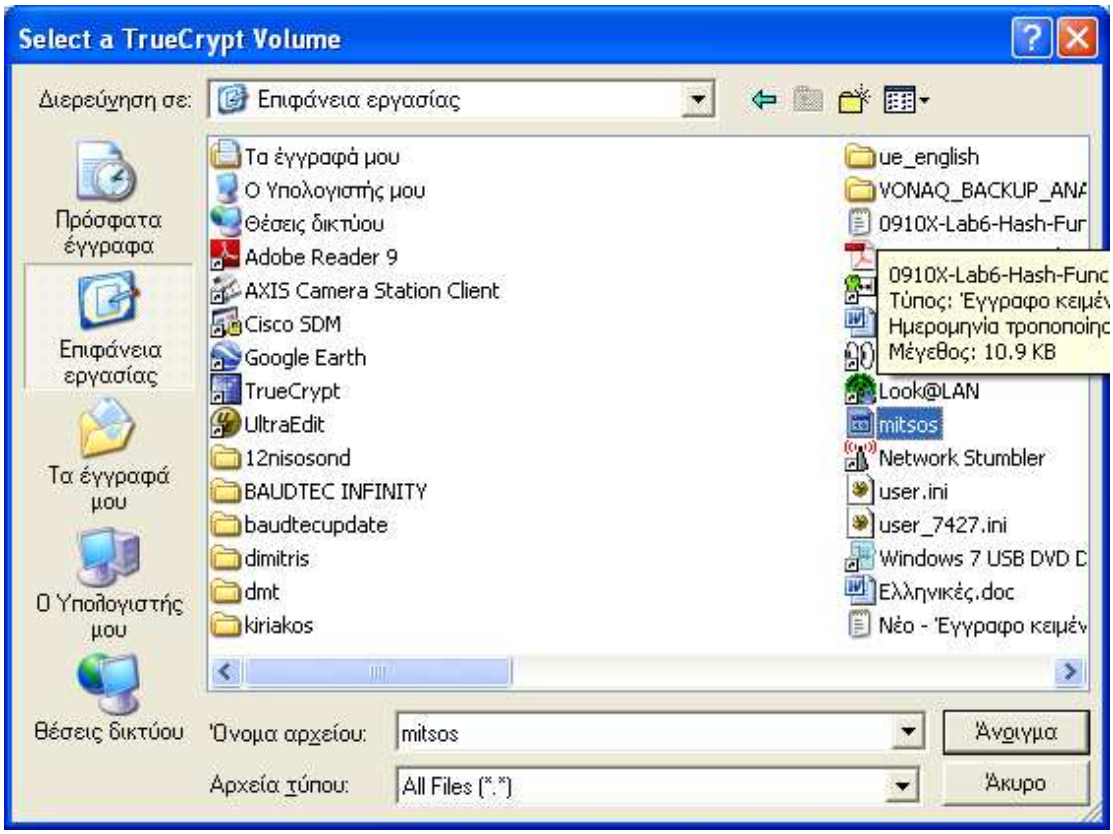
Εικόνα 13: Truecrypt εικονική μονάδα έτοιμη για χρήση

Δημιουργήσαμε τη νέα εικονική μονάδα και είναι έτοιμη για χρήση. Πατάμε Exit και επιστρέφουμε στο αρχικό παράθυρο του προγράμματος.



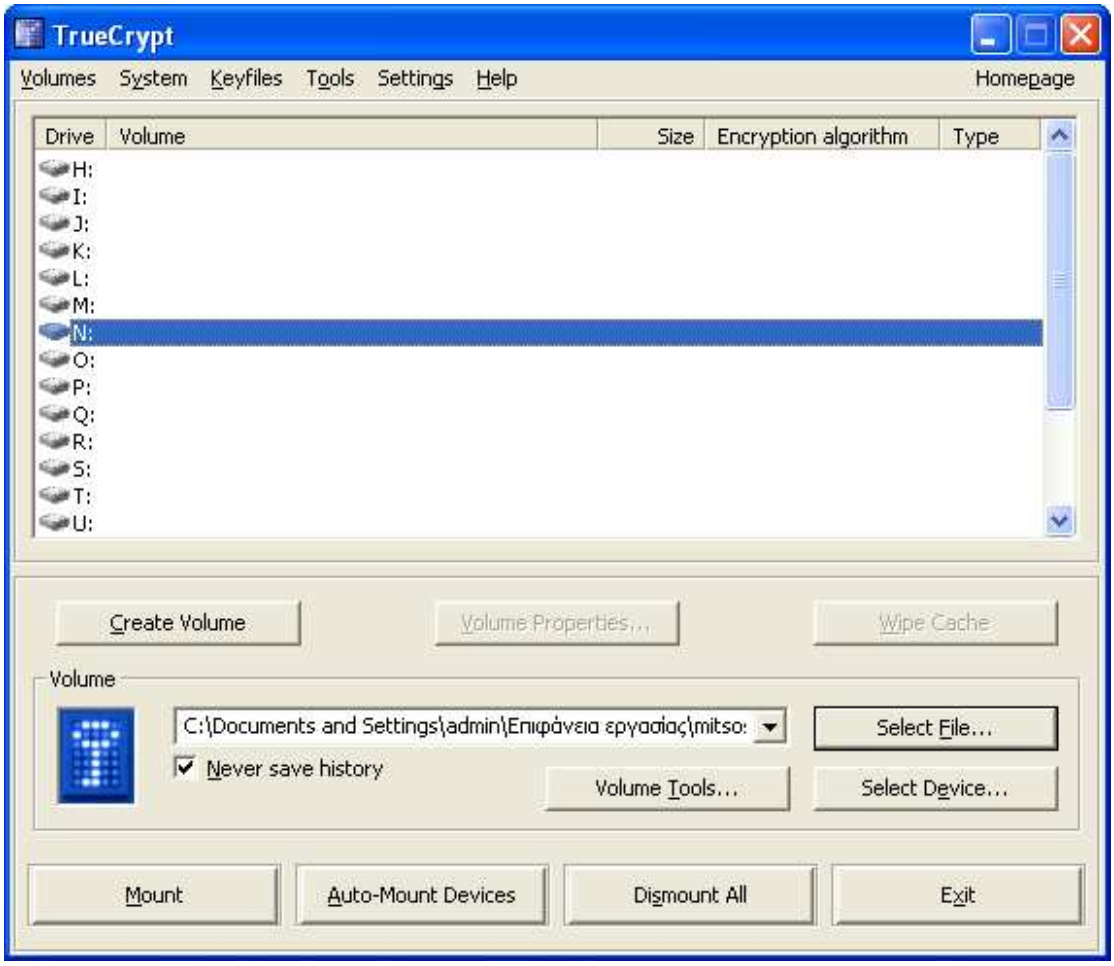
Εικόνα 14: Truecrypt επιλογή γράμματος για εικονική μονάδα

Σε αυτό το βήμα διαλέγουμε ποιό γράμμα θέλουμε να έχει ο νέος εικονικός μας τόμος. Επιλέγουμε τυχαία ένα (εδώ το N) και πατάμε Select file.



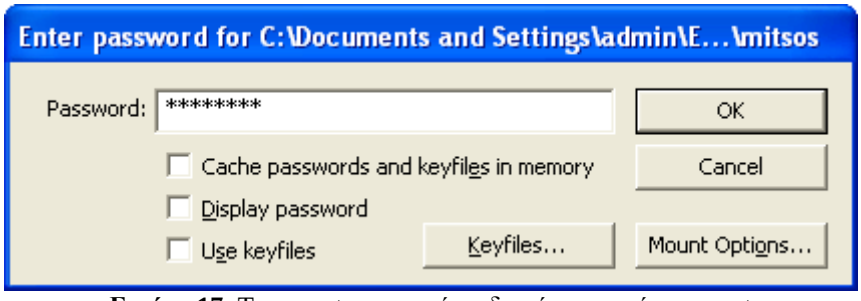
Εικόνα 15: επιλογή Truecrypt volume

Τώρα θα επιλέξουμε το αρχείο mitsos που δημιουργήσαμε σε προηγούμενο βήμα και θα πατήσουμε άνοιγμα.



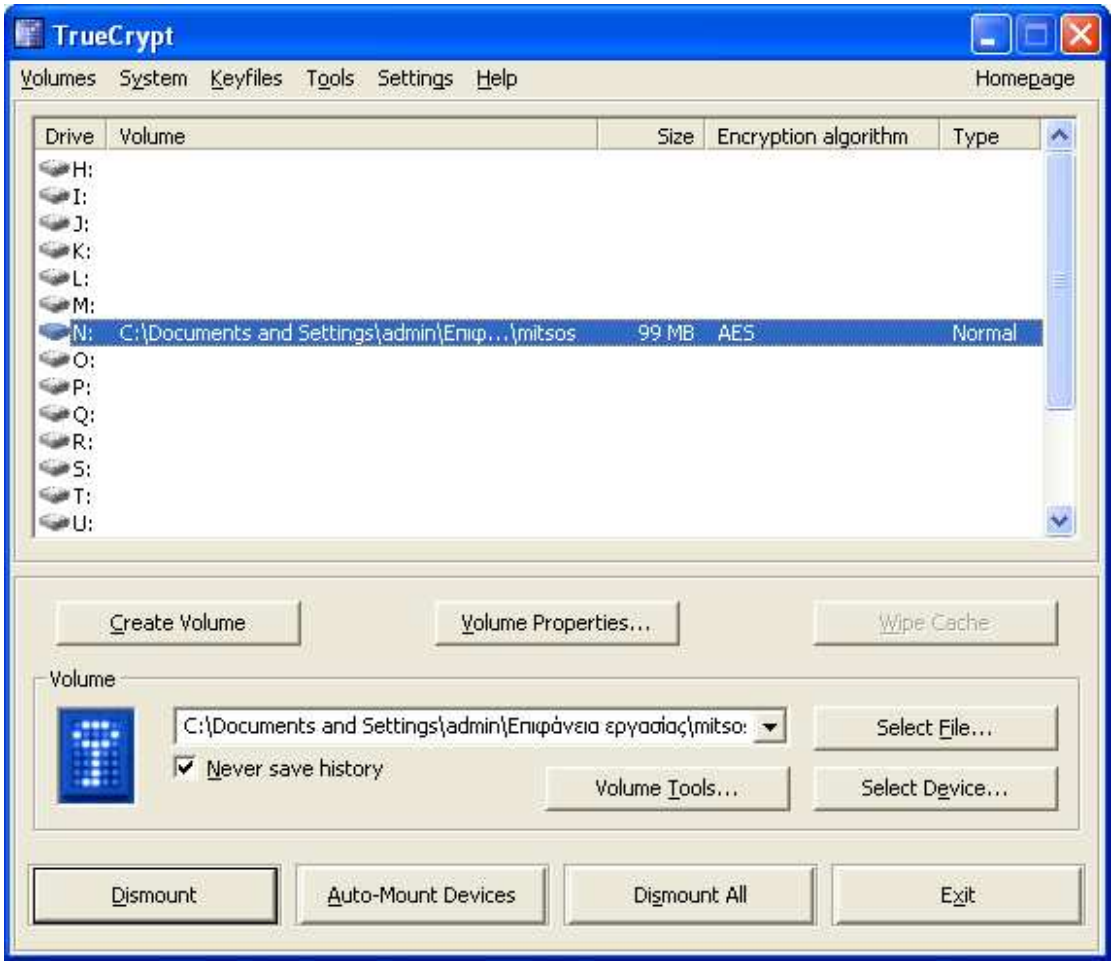
Εικόνα 16: Truecrypt mount volume

Πατάμε το κουμπί Mount και το πρόγραμμα μας ζητάει τον κωδικό που δώσαμε όταν δημιουργήσαμε το αρχείο mitsos.



Εικόνα 17: Truecrypt εισαγωγή κωδικού για να γίνει mount

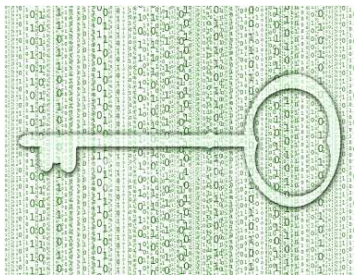
Δίνουμε τον κωδικό και πατάμε OK.

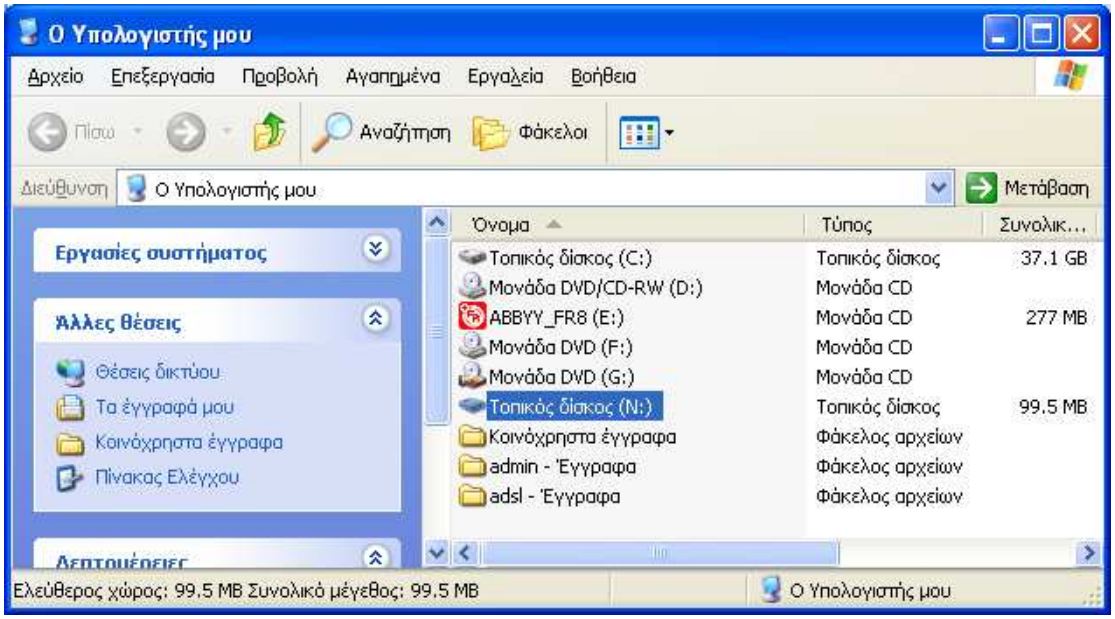


Εικόνα 18: Truecrypt εικονικός τόμος έτοιμος

Μόλις κάναμε mount τον εικονικό δίσκο N. Ο εικονικός αυτός δίσκος είναι εντελώς κωδικοποιημένος και συμπεριφέρεται σαν πραγματικός δίσκος. Μπορούμε να αποθηκεύσουμε και να μετακινήσουμε αρχεία στον εικονικό δίσκο και να γίνεται η κρυπτογράφηση καθώς αυτά μεταφέρονται ή αποθηκεύονται.

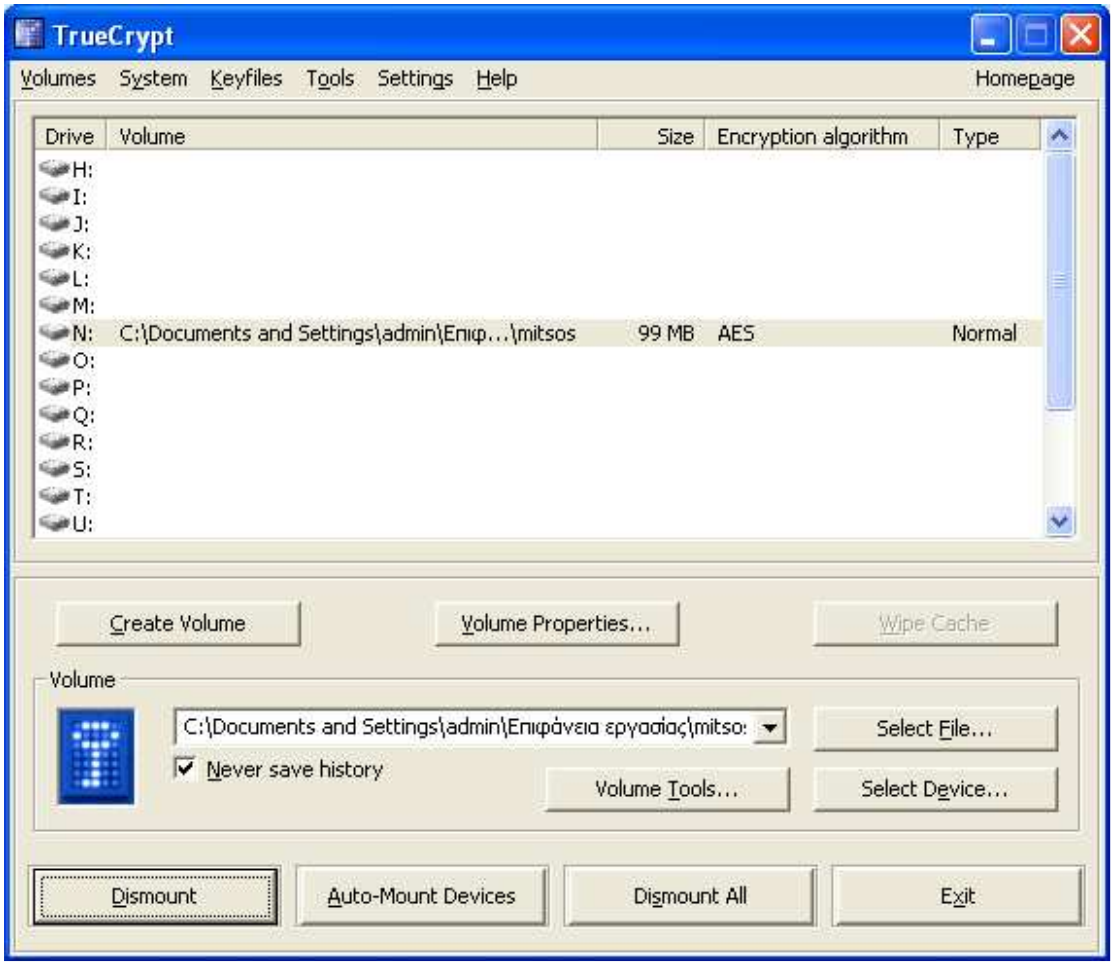
Αν ανοίξουμε το εικονίδιο *Ο Υπολογιστής μου*, θα δούμε ότι έχει προστεθεί μια μονάδα στους δίσκους με το γράμμα N και χωρητικότητα 100 MegaByte.





Εικόνα 19: παράθυρο Ο Υπολογιστής μου

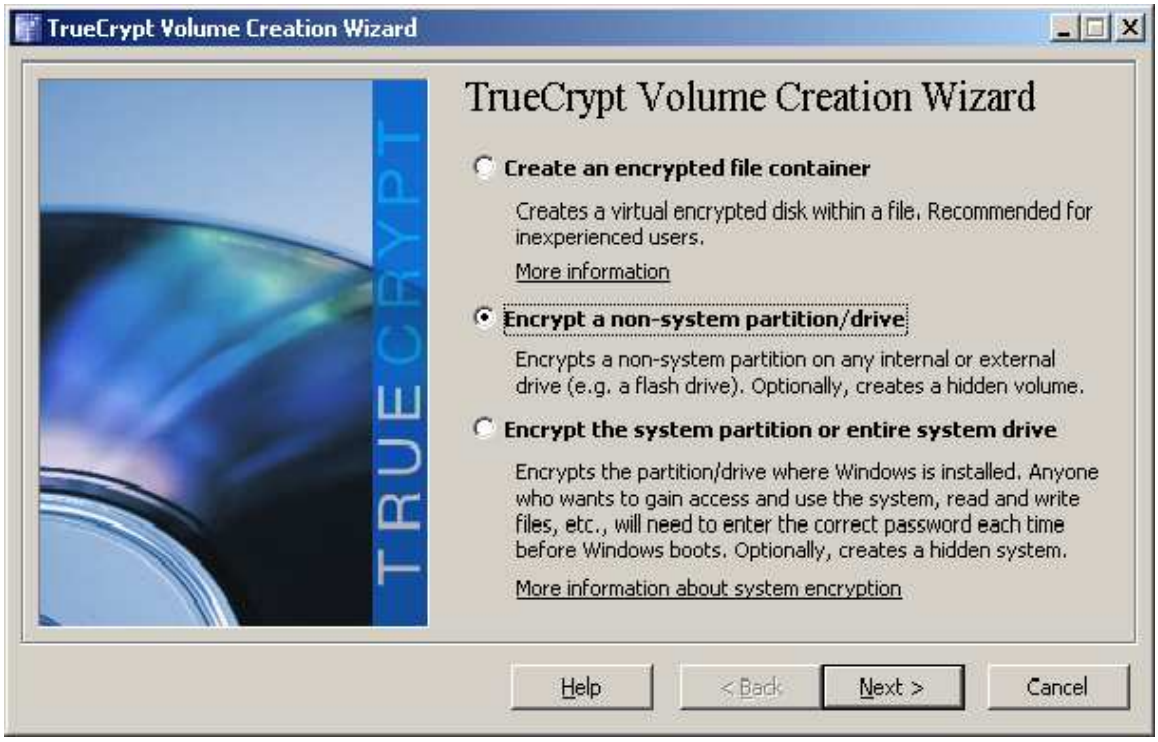
Αν τώρα κάνουμε Dismount το volume θα δούμε ότι ο τοπικός δίσκος N θα πάψει πλέον να υπάρχει.



Εικόνα 20: Truecrypt dismount volume

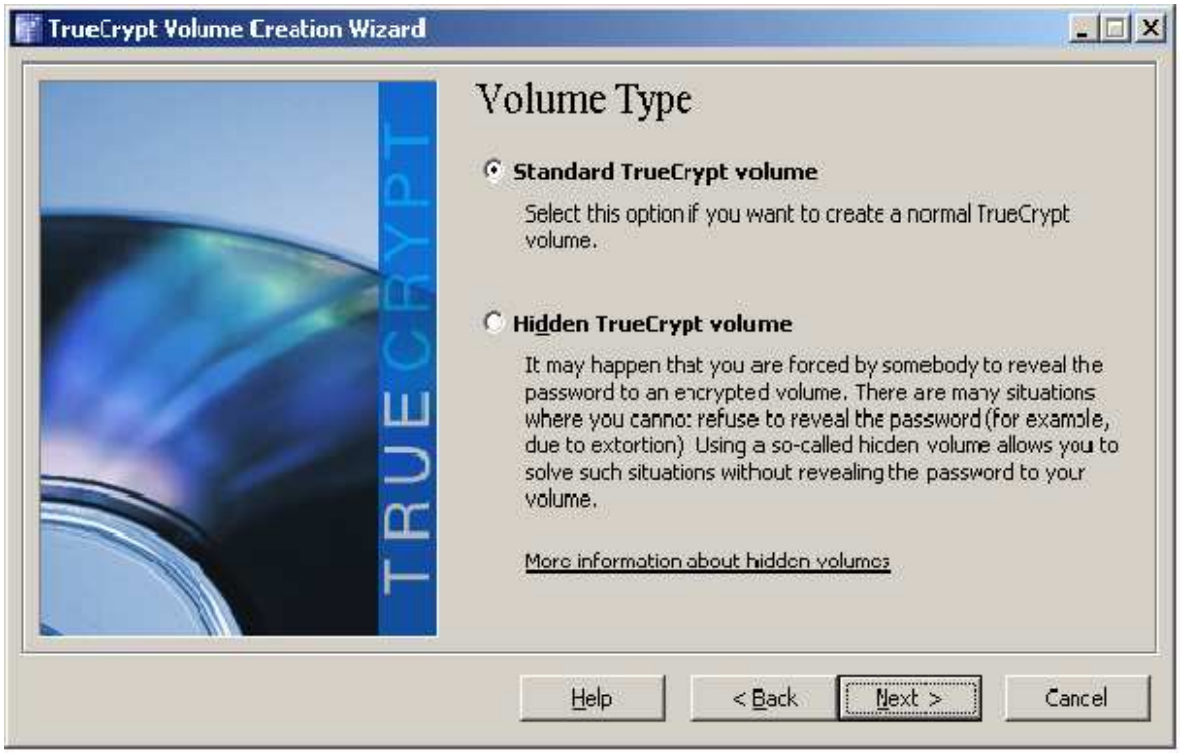
Volume σε usb flash

Τώρα θα εξεταστεί η περίπτωση κατά την οποία θέλουμε να δημιουργήσουμε την εικονική μονάδα σε ένα usb flash.
Ανοίγουμε το Truecrypt πατάμε create volume και στην οθόνη που εμφανίζεται επιλέγουμε Encrypt a non-system partition/drive όπως φαίνεται παρακάτω και πατάμε Next.



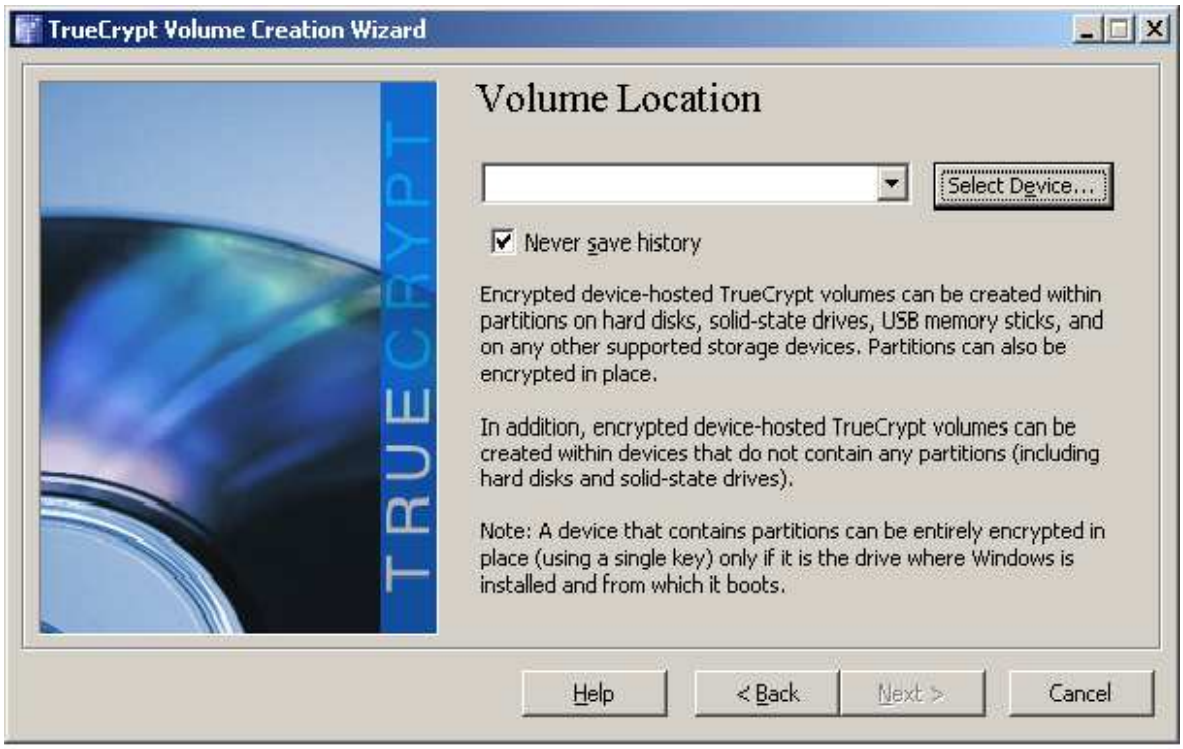
Εικόνα 21: Truecrypt volume σε usb flash drive

Στο επόμενο παράθυρο που εμφανίζεται επιλέγουμε αν η μονάδα που θα δημιουργηθεί θα είναι κανονική ή κρυφή. Διαλέγουμε Standard Truecrypt Volume και πατάμε Next.



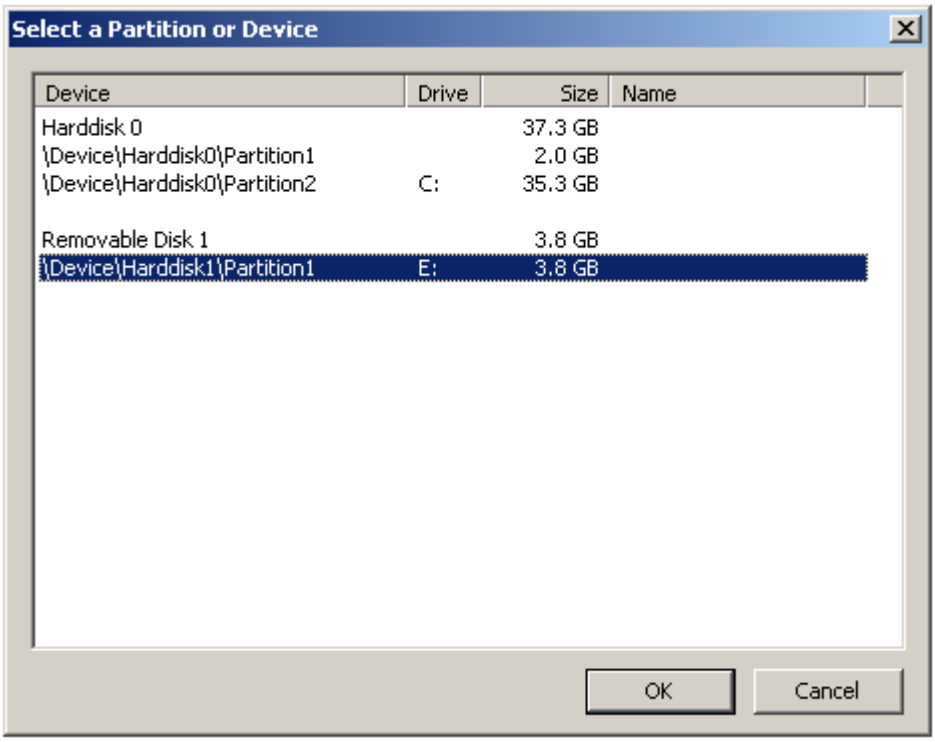
Εικόνα 22: Truecrypt standard volume

Στο επόμενο βήμα επιλέγουμε τη συσκευή (δίσκο) στην οποία θέλουμε να δημιουργήσουμε το volume. Πατάμε select device.



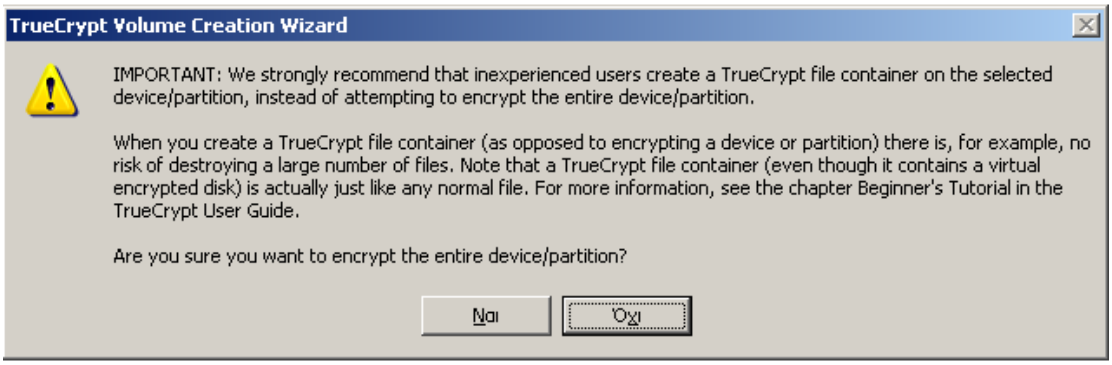
Εικόνα 23: Truecrypt τοποθεσία volume

Διαλέγουμε τον αφαιρούμενο δίσκο (removable disk 1) και πατάμε OK.



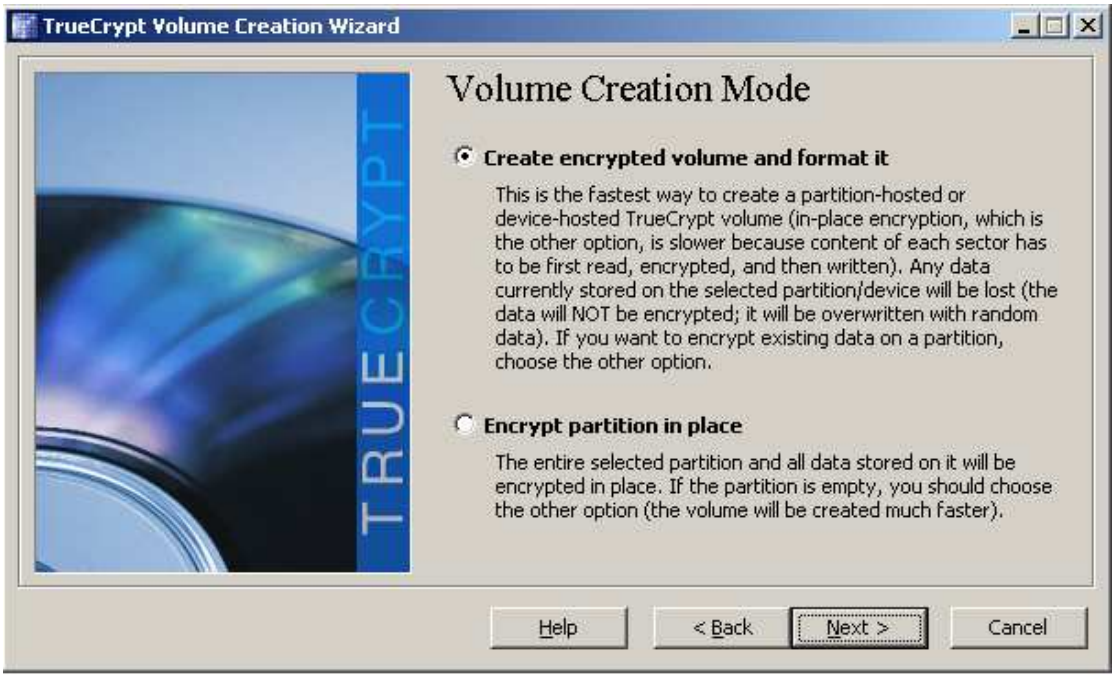
Εικόνα 24: Truecrypt επιλογή συσκευής

Εμφανίζεται ένα μήνυμα το οποίο μας ρωτάει αν είμαστε βέβαιοι ότι θέλουμε να κρυπτογραφήσουμε το δίσκο. Πατάμε Ναι και συνεχίζουμε παρακάτω.



Εικόνα 25: Truecrypt ερώτηση επιβεβαίωσης κρυπτογράφησης

Στο παράθυρο που εμφανίζεται επιλέγουμε αν θέλουμε να κρυπτογραφηθεί ολόκληρος ο δίσκος ή μέρος αυτού. Διαλέγουμε την πρώτη επιλογή και πατάμε Next.



Εικόνα 26: Truecrypt volume creation mode

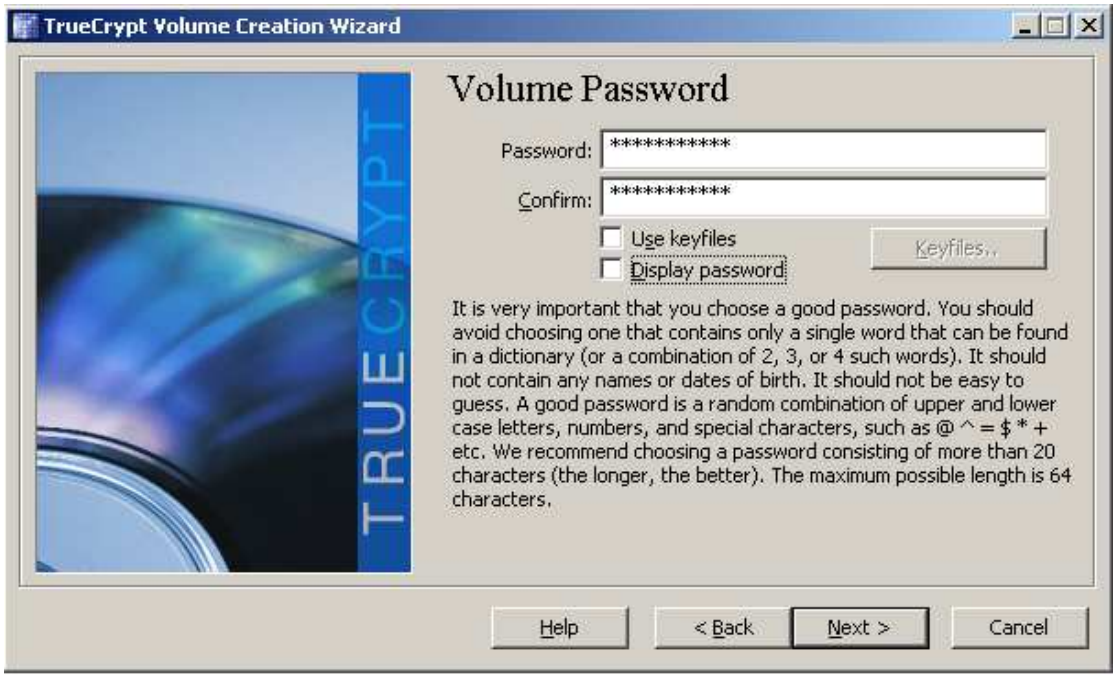
Στο επόμενο βήμα επιλέγουμε αλγόριθμο κρυπτογράφησης. Εδώ AES και πατάμε Next.

Εικόνα 27: Truecrypt επιλογή αλγορίθμου κρυπτογράφησης

Στη συνέχεια διαλέγουμε το μέγεθος του volume που θα δημιουργηθεί. Όπως παρατηρούμε το πρόγραμμα δεν μας αφήνει περιθώριο επιλογής καθώς σε προηγούμενο βήμα επιλέξαμε να κρυπτογραφηθεί ολόκληρος ο δίσκος.

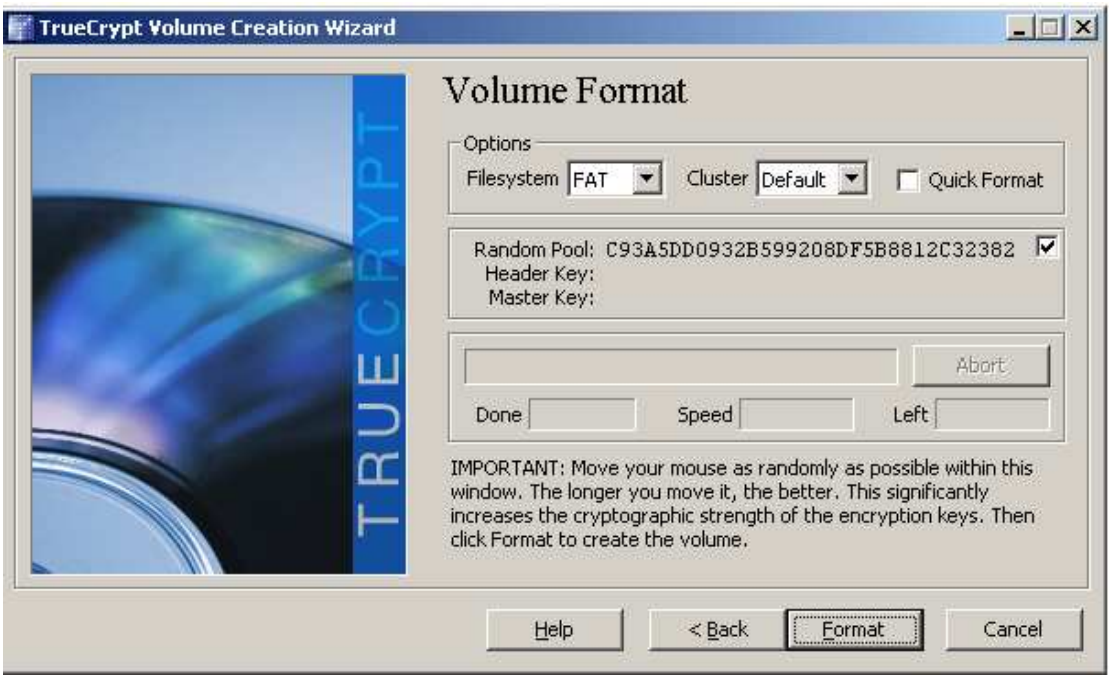
Εικόνα 28: Truecrypt μέγεθος volume

Έπειτα βάζουμε τον κωδικό του volume και πατάμε Next.



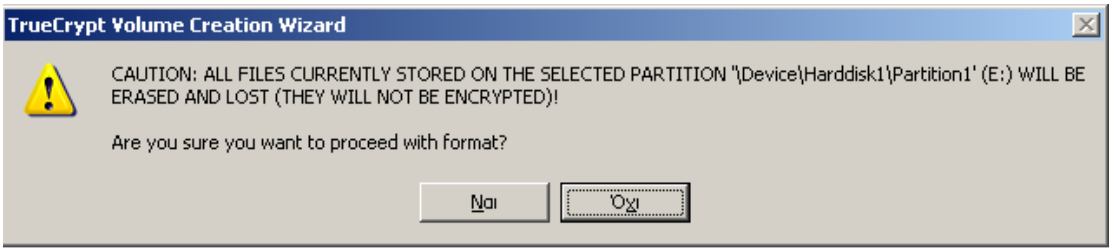
Εικόνα 29: Truecrypt κωδικός volume

Στο επόμενο βήμα πατάμε Format και περιμένουμε μέχρι να διαμορφωθεί ο δίσκος.



Εικόνα 30: Truecrypt διαμόρφωση volume

Μόλις πατήσουμε Format το Truecrypt μας προειδοποιεί πως τα δεδομένα του δίσκου θα διαγραφούν και ρωτάει αν είμαστε σίγουροι πως θέλουμε να προχωρήσουμε με τη διαμόρφωση του δίσκου.

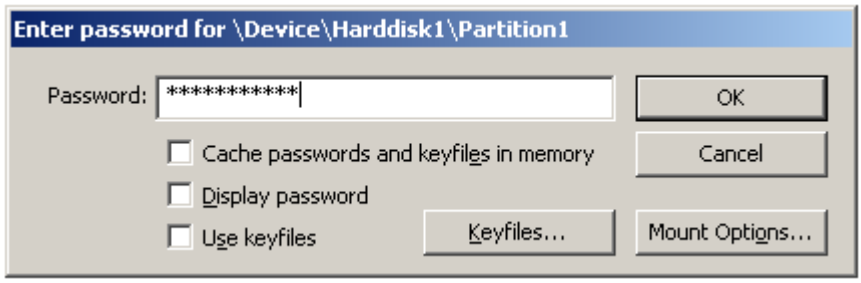


Εικόνα 31: Truecrypt επιβεβαίωση διαμόρφωσης

Πατάμε Ναι και μετά από μερικά λεπτά ο δίσκος μας είναι έτοιμος.

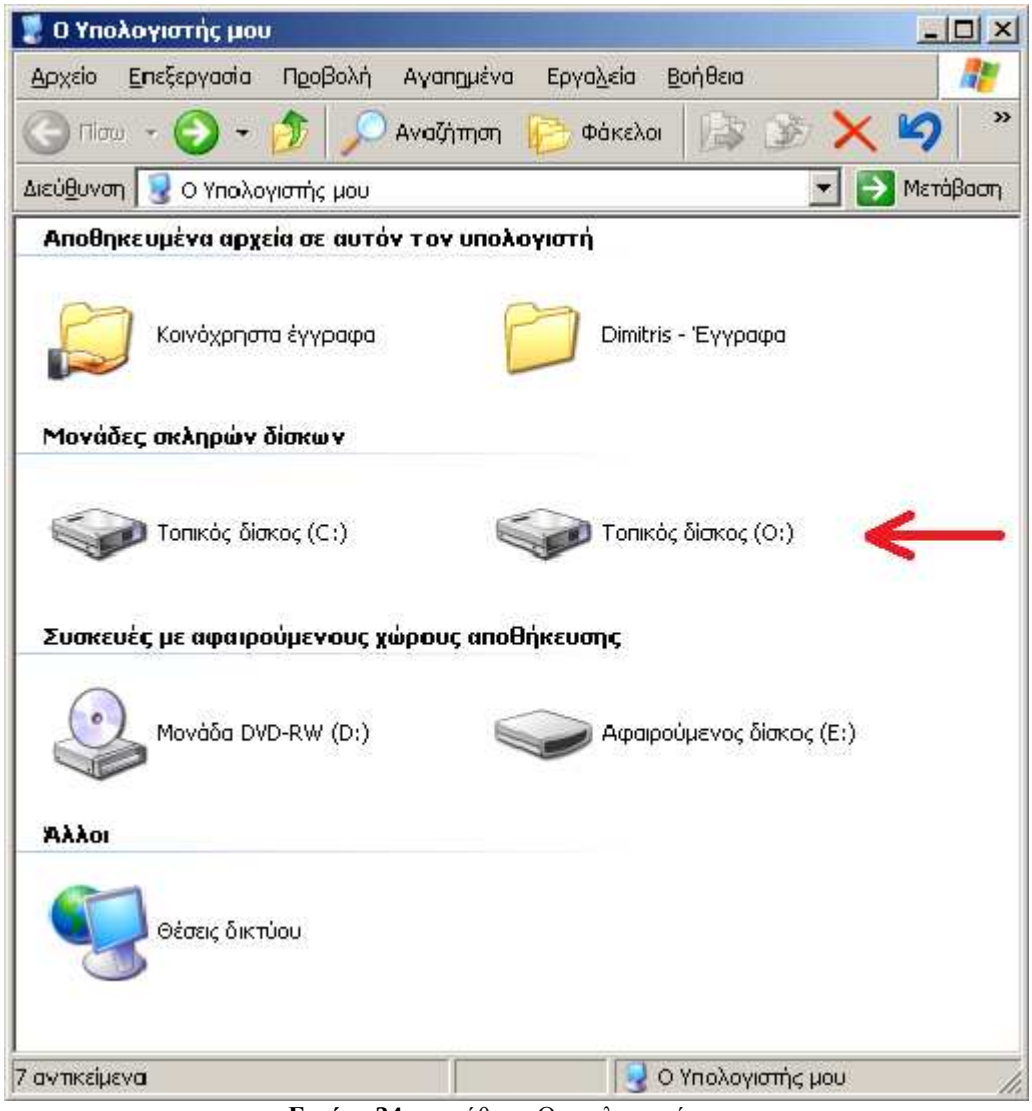
Εικόνα 32: Truecrypt επιτυχία δημιουργίας volume

Τώρα επιστρέφουμε στο αρχικό παράθυρο του Truecrypt και αντί για select file που επιλέξαμε στην προηγούμενη περίπτωση, διαλέγουμε select device. Θα επιλέξουμε την συσκευή που μόλις κρυπτογραφήσαμε και αφού βάλουμε τον κωδικό που θα ζητηθεί θα κάνουμε mount την συγκεκριμένη συσκευή.



Εικόνα 33: Truecrypt εισαγωγή κωδικού

Αφού κάνουμε mount ανοίγουμε το παράθυρο *Ο Υπολογιστής μου* και παρατηρούμε ότι έχει δημιουργηθεί μια νέα μονάδα σκληρού δίσκου η οποία δεν είναι άλλη από το κρυπτογραφημένο μας usb flash.

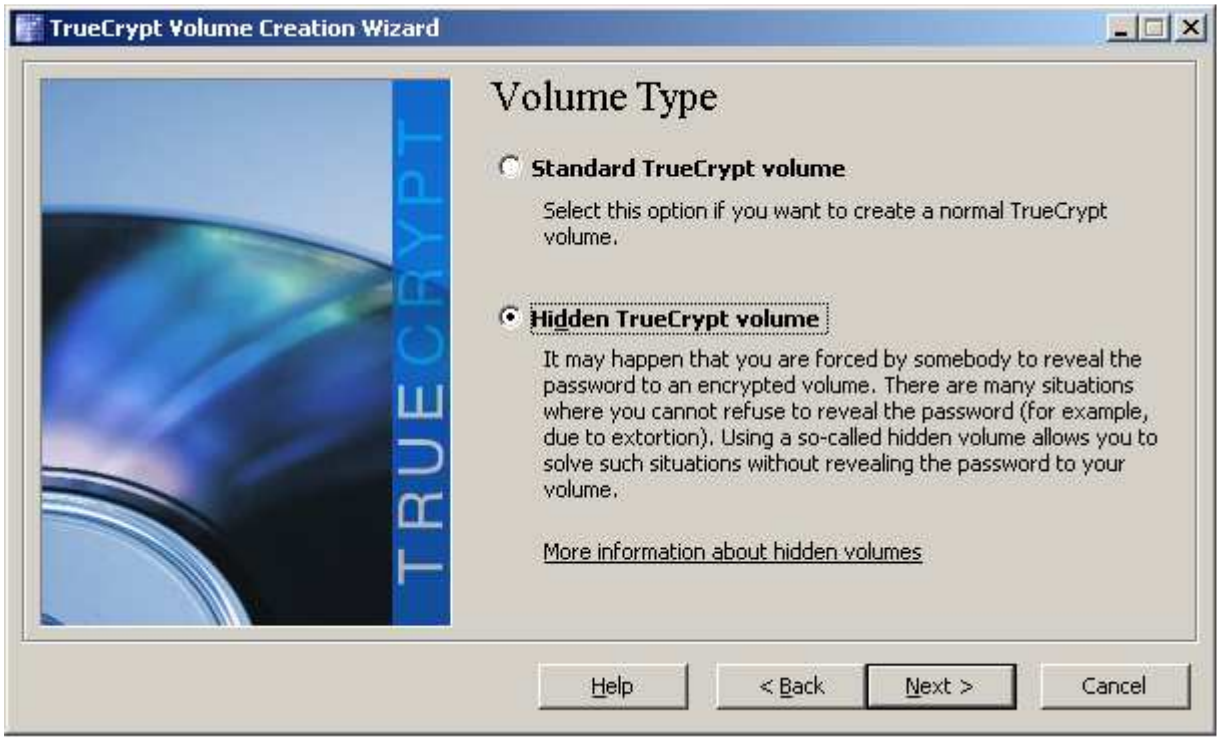


Εικόνα 34: παράθυρο Ο υπολογιστής μου

Σε περίπτωση που θέλουμε να επαναφέρουμε το flash drive στην αρχική του μη κρυπτογραφημένη κατάσταση δεν έχουμε παρά να πατήσουμε δεξί κλικ πάνω του και να επιλέξουμε διαμόρφωση (format) γνωρίζοντας βέβαια πως θα χαθούν τα δεδομένα τα οποία υπάρχουν στο δίσκο.

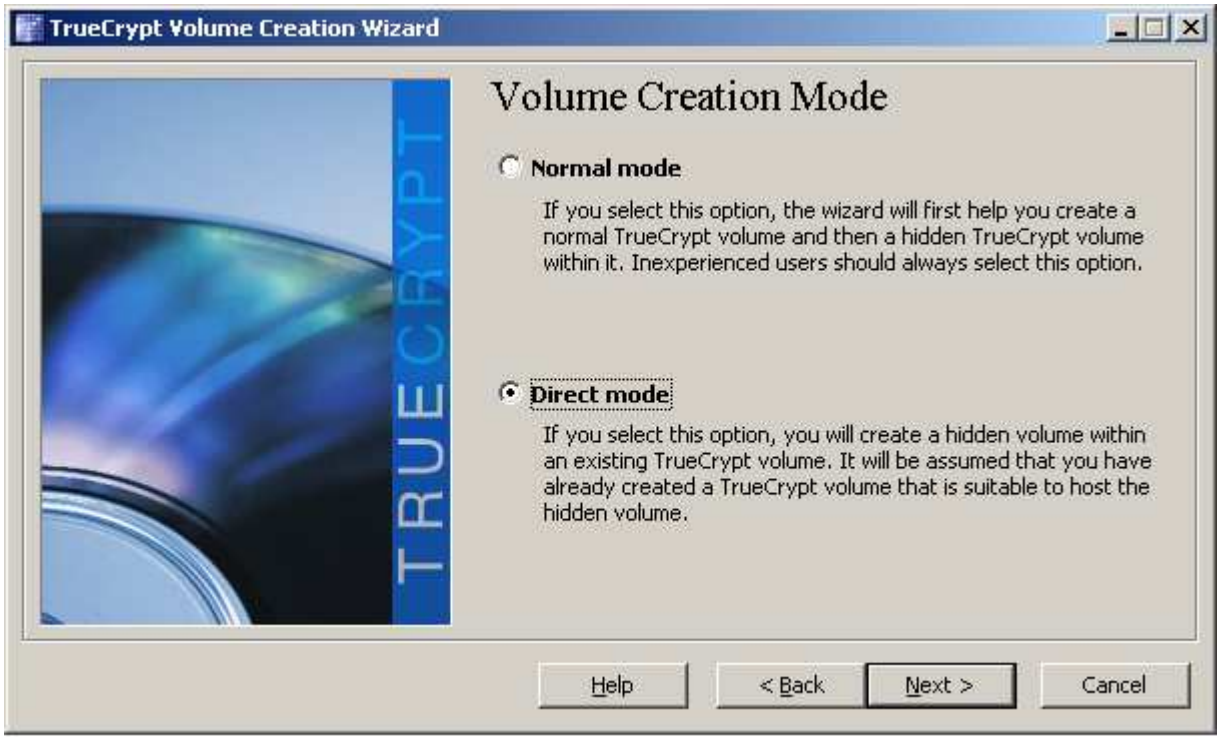
Hidden volume

Για ακόμα μεγαλύτερη ασφάλεια μπορούμε να δημιουργήσουμε ένα κρυφό αρχείο μέσα σε ένα άλλο (hidden volume). Το τεράστιο πλεονέκτημα σε αυτή την περίπτωση είναι ότι ακόμα και αν υποθέσουμε ότι ορισμένοι, με κάποιον τρόπο, σπάσουν το πρώτο κρυφό αρχείο (outer volume), δεν υπάρχει καμία περίπτωση να συμβεί το ίδιο και με το hidden volume, για τον απλούστατο λόγο ότι είναι εντελώς αόρατο. Ακόμα και αν ανοίξει κάποιος το ίδιο το truecrypt δεν θα μπορεί να δει το hidden volume εκτός αν γνωρίζει τον κωδικό του. Χρειάζεται, ωστόσο, να προσέξουμε πάρα πολύ το μέγεθος των δεδομένων, καθώς τα δύο αρχεία μοιράζονται στην πραγματικότητα τον ίδιο χώρο.
Πως όμως δημιουργούμε ένα hidden volume?
Ανοίγουμε το truecrypt επιλέγουμε create volume και στο επόμενο παράθυρο διαλέγουμε Hidden truecrypt volume.



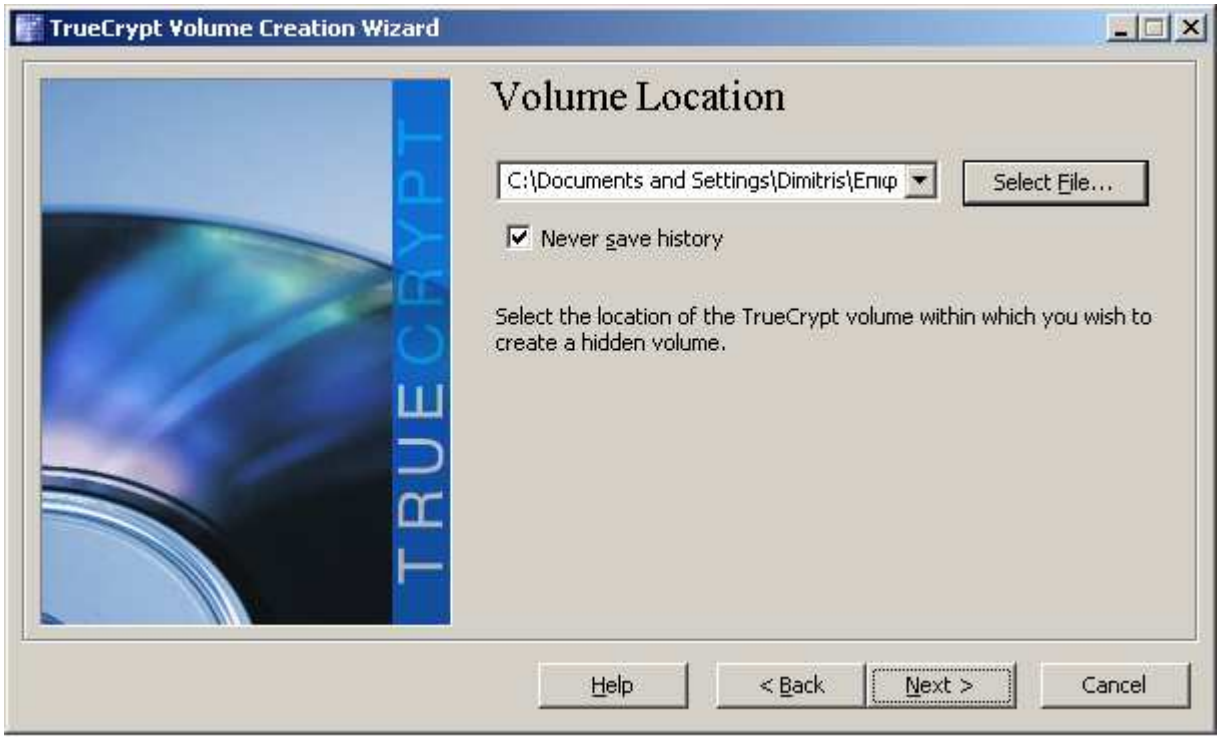
Εικόνα 35: Truecrypt επιλογή για hidden volume

Στο επόμενο παράθυρο επιλέγουμε Direct mode. Με την επιλογή αυτή διαλέγουμε να δημιουργήσουμε ένα νέο volume μέσα σε ένα ήδη υπάρχων. Το νέο volume που θα δημιουργηθεί θα είναι το κρυφό.



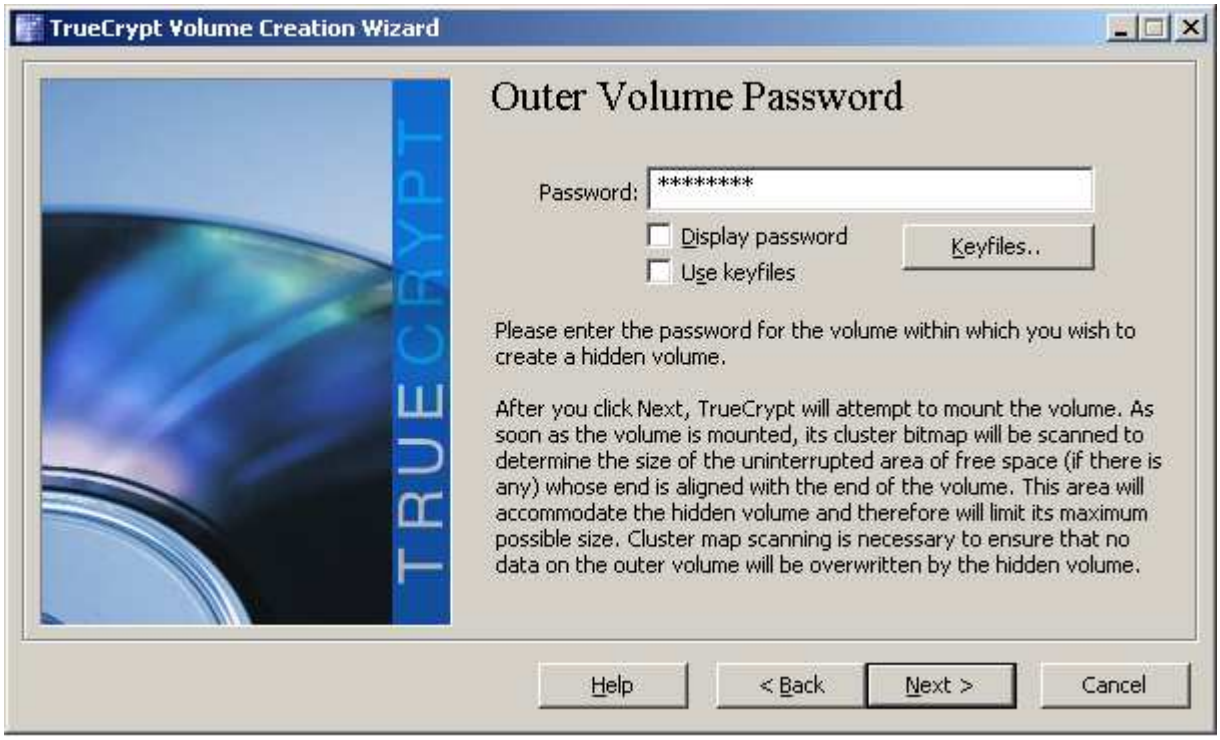
Εικόνα 36: Truecrypt επιλογή direct mode

Επιλέγουμε την τοποθεσία του outer volume και πατάμε Next.



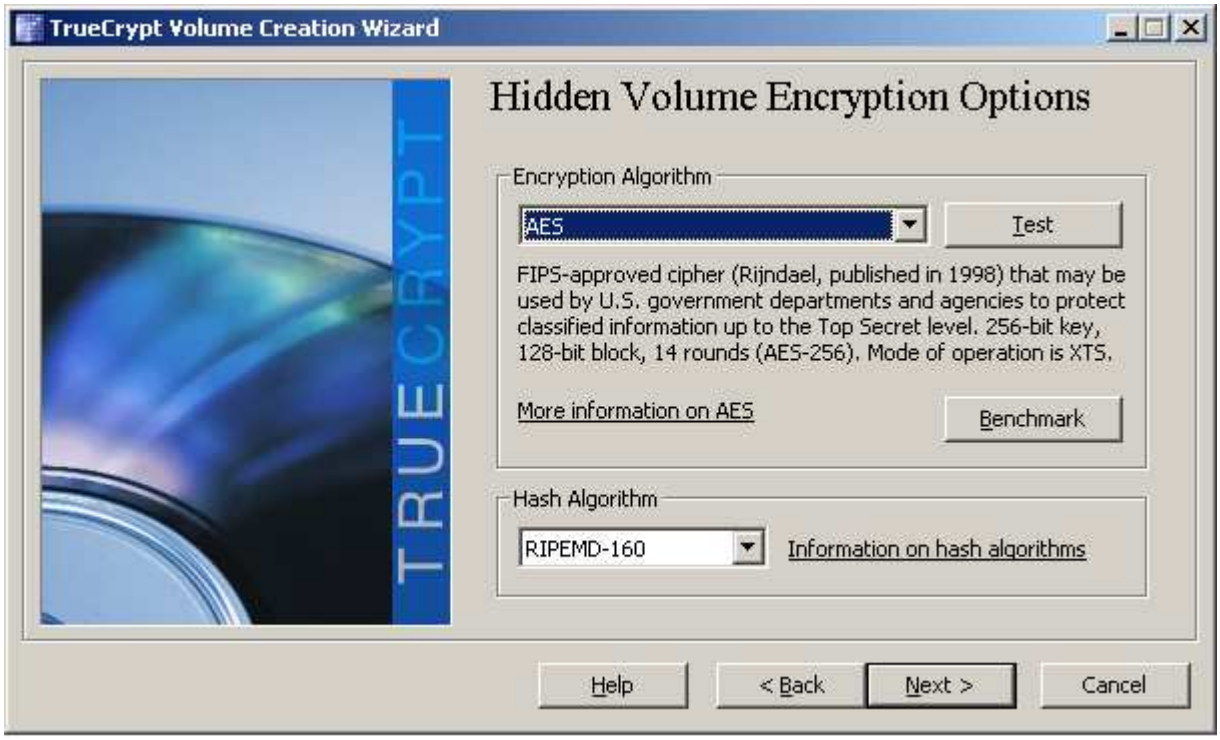
Εικόνα 37: Truecrypt τοποθεσία volume

Στο επόμενο βήμα δίνουμε τον κωδικό του outer volume.



Εικόνα 38: Truecrypt κωδικός outer volume

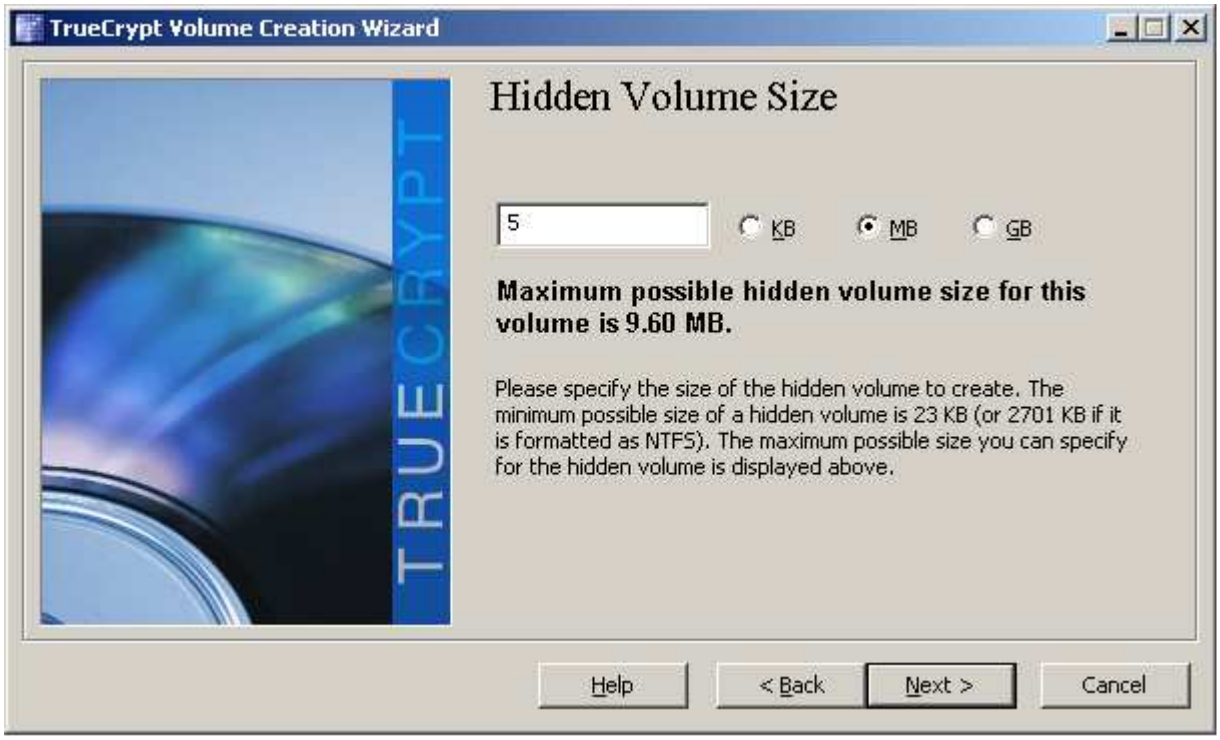
Επιλέγουμε αλγόριθμο κρυπτογράφησης για το νέο πια hidden volume.



Εικόνα 39: Truecrypt επιλογή αλγορίθμου κρυπτογράφησης

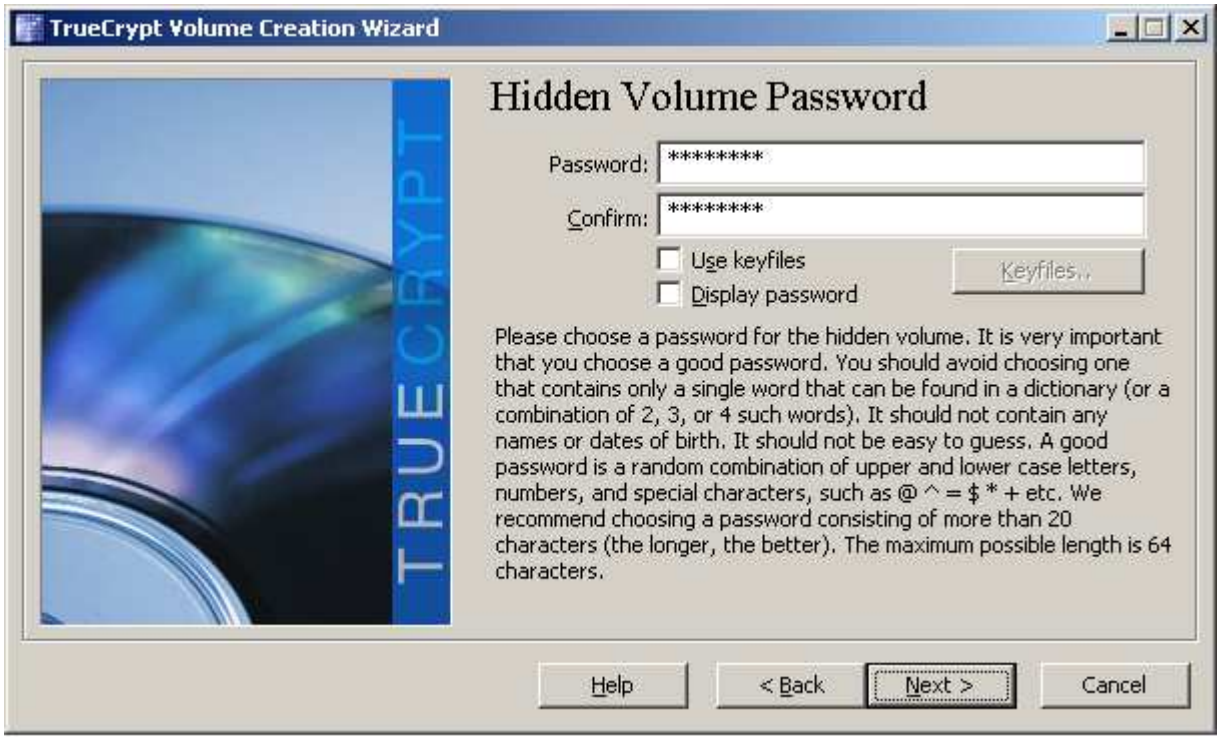
Μέτα διαλέγουμε το μέγεθος το οποίο θέλουμε να έχει το hidden volume. Βλέπουμε ότι το πρόγραμμα μας ενημερώνει για το μέγιστο δυνατό μέγεθος που μπορούμε να

επιλέξουμε καθώς αυτό δεν μπορεί να είναι μεγαλύτερο από το outer volume αφού μέσα σε αυτό θα δημιουργηθεί το κρυφό volume.



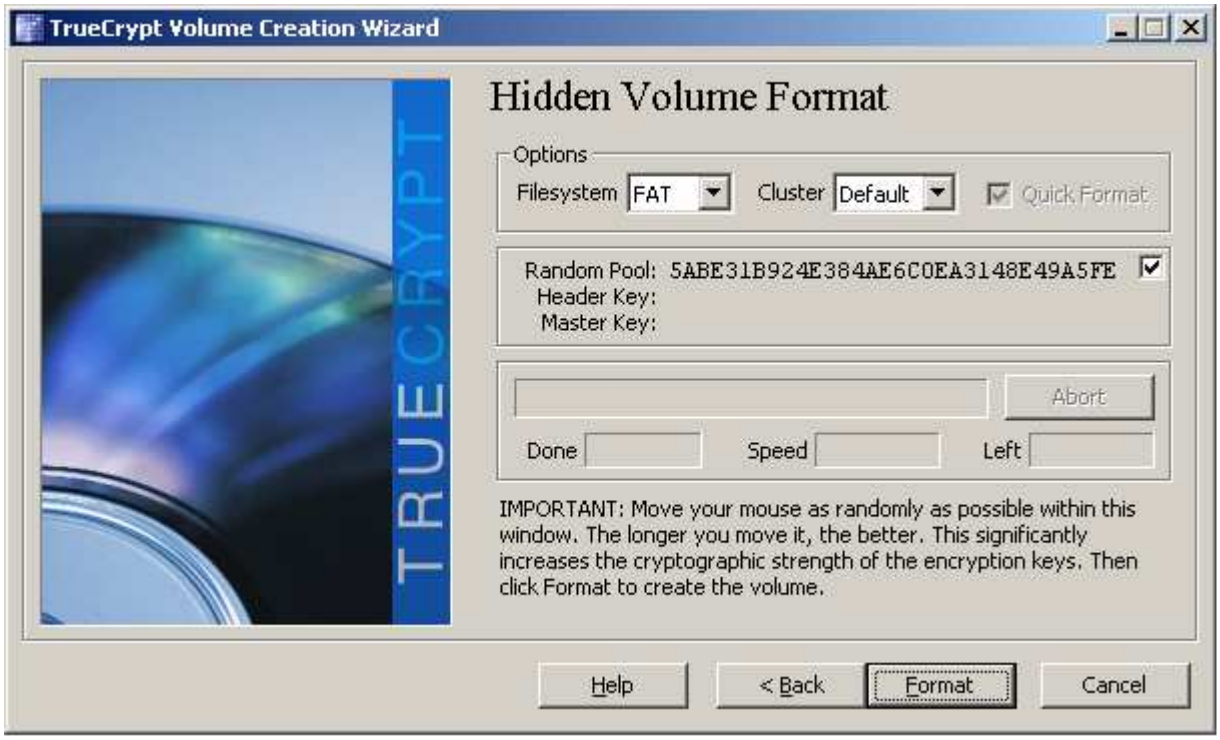
Εικόνα 40: Truecrypt μέγεθος hidden volume

Βάζουμε νέο κωδικό για το Hidden volume και πατάμε Next.



Εικόνα 41: Truecrypt κωδικός hidden volume

Τέλος στο επόμενο παράθυρο πατάμε Format ώστε να διαμορφωθεί το hidden volume.



Εικόνα 42: Truecrypt διαμόρφωση hidden volume

Στη συνέχεια επιστρέφουμε στο αρχικό παράθυρο του προγράμματος, επιλέγουμε αρχείο και πατάμε mount. Αυτό ουσιαστικά που καθορίζει αν θα γίνει mount το outer ή το hidden volume είναι ο κωδικός που θα δώσουμε.

Κεφάλαιο 3 Password Policy

Η πολιτική κωδικού πρόσβασης είναι ένα σύνολο κανόνων που έχουν σκοπό να ενισχύσουν την ασφάλεια των υπολογιστών με την ενθάρρυνση των χρηστών για να υιοθετούν ισχυρούς κωδικούς και να τους χρησιμοποιούν κατάλληλα.. Το Password Policy μπορεί να είναι είτε συμβουλευτικό είτε εξουσιοδοτημένο από τεχνικά μέσα.

3.1 Κύρια χαρακτηριστικά ενός Password Policy

Password length and formation

Πολλά policies απαιτούν ένα ελάχιστο μήκος κωδικού (6 με 8 χαρακτήρες). Μερικά συστήματα επιβάλουν κάποιο μέγιστο μήκος κωδικού ώστε να είναι συμβατά με άλλα συστήματα.

Ορισμένες πολιτικές συνιστούν ή επιβάλουν τον τύπο του κωδικού που μπορεί να επιλέξει ο χρήστης, όπως:

- Η χρήση πεζών και κεφαλαίων ταυτόχρονα
- Αναγραφή ενός ή περισσοτέρων αριθμητικών ψηφίων
- Ενσωμάτωση των ειδικών χαρακτήρων
- Απαγόρευση των λέξεων που βρέθηκαν σε λεξικό ή προσωπικά στοιχεία χρήστη
- Απαγόρευση των κωδικών πρόσβασης που ταιριάζουν με τη μορφή των ημερομηνιών ημερολογίου, αριθμούς πινακίδων ή άλλους κοινούς αριθμούς

Password duration

Κάποια policies απαιτούν από τους χρήστες να αλλάζουν περιοδικά τους κωδικούς τους, π.χ. κάθε 90 ή 180 ημέρες. Τα συστήματα που εφαρμόζουν τέτοιες πολιτικές αποτρέπουν τους χρήστες να επιλέξουν κάποιο κωδικό σχεδόν ίδιο με κάποια προηγούμενη επιλογή. Αυτή η πολιτική μπορεί συχνά να αποτύχει. Επειδή είναι δύσκολο να βρεθούν “καλοί” κωδικοί πρόσβασης τους οποίους να θυμάται ο χρήστης και να χρειάζεται να τους αλλάζει συχνά, η κατάληξη είναι η χρήση αδύναμων κωδικών πρόσβασης. Η χρήση ενός ισχυρού κωδικού και η μη αλλαγή του είναι προτιμότερη. Ωστόσο, έχει ένα σημαντικό μειονέκτημα: αν κάποιος αποκτήσει έναν κωδικό πρόσβασης, αν δεν αλλάξει, μπορεί να έχει μακροπρόθεσμη πρόσβαση.

Common password practice

Συχνά τα password policies συμπεριλαμβάνουν συμβουλές για την σωστή διαχείριση ενός κωδικού όπως:

1. Ποτέ να μην μοιράζεται ο κωδικός

2. Ποτέ να μην χρησιμοποιείται ο ίδιος κωδικός για περισσότερους από ένα λογαριασμούς χρηστών

3. Ποτέ να μην λέγεται ο κωδικός σε κανένα, συμπεριλαμβανομένου ανθρώπων που ισχυρίζονται ότι είναι από το τμήμα εξυπηρέτησης πελατών ή της ασφάλειας

4. Ποτέ να μη γράφεται ο κωδικός σε χαρτί

5. Ποτέ να μην δίνεται ο κωδικός μέσω τηλεφώνου, e-mail η instant messaging

6. Να γίνεται log off μετά την χρήση του υπολογιστή

7. Να αλλάζεται ο κωδικός σε περίπτωση που υπάρχουν υποψίες

8. Οι κωδικοί των λειτουργικών συστημάτων και των εφαρμογών τους να είναι διαφορετικοί

9. Οι κωδικοί να περιέχουν γράμματα και νούμερα ταυτόχρονα

10. Οι κωδικοί να φτιάχνονται απολύτως τυχαία αλλά να είναι εύκολο να τον θυμάται ο χρήστης.

Sanctions (κυρώσεις)

Τα password policies μπορούν να περιλαμβάνουν προοδευτικές κυρώσεις, ξεκινώντας από προειδοποιήσεις και καταλήγοντας σε πιθανή απώλεια των δικαιωμάτων ενός υπολογιστή ή τον τερματισμό της συνεργασίας. Όπου η εμπιστευτικότητα εξουσιοδοτείται από το νόμο μια παραβίαση ενός password policy μπορεί να είναι και ένα ποινικό αδίκημα. Μερικοί θεωρούν μια πειστική εξήγηση της σπουδαιότητας της ασφάλειας περισσότερο αποτελεσματική παρά τις απειλές των κυρώσεων.

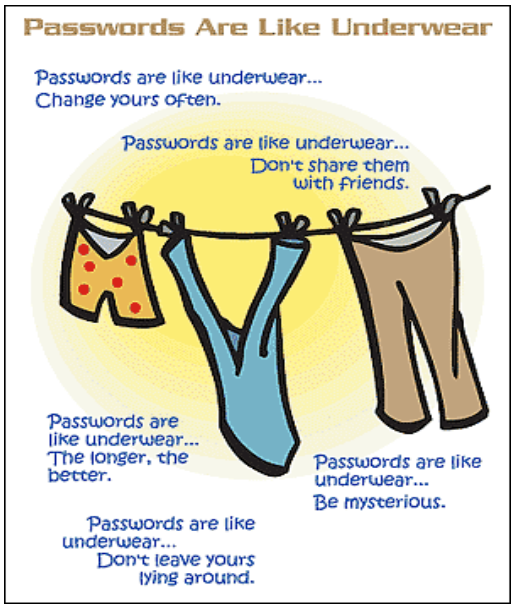
3.2 Επιλέγοντας την κατάλληλη πολιτική

Το επίπεδο της αντοχής που απαιτείται από τον κωδικό πρόσβασης εξαρτάται, εν μέρει, από το πόσο εύκολο είναι για έναν εισβολέα να υποβάλει πολλές εικασίες. Ορισμένα συστήματα περιορίζουν τον αριθμό των φορών που ο χρήστης μπορεί να εισαγάγει λανθασμένο κωδικό πρόσβασης πριν του επιβληθεί κάποια καθυστέρηση. Στο άλλο άκρο, σε ορισμένα συστήματα, ένας εισβολέας μπορεί να επιχειρήσει κωδικούς πολύ γρήγορα. Σε αυτή την περίπτωση πολύ πιο ισχυροί κωδικοί πρόσβασης είναι απαραίτητοι για τη λογική της ασφάλειας. Αυστηρότερες απαιτήσεις είναι επίσης κατάλληλες για τους λογαριασμούς με υψηλότερα προνόμια όπως ο λογαριασμός διαχειριστή του συστήματος.

3.3 Εκτιμήσεις χρησιμότητας

Τα password policies είναι συνήθως μια ανταλλαγή μεταξύ θεωρητικής ασφάλειας και πρακτικότητας της ανθρώπινης συμπεριφοράς. Για παράδειγμα:

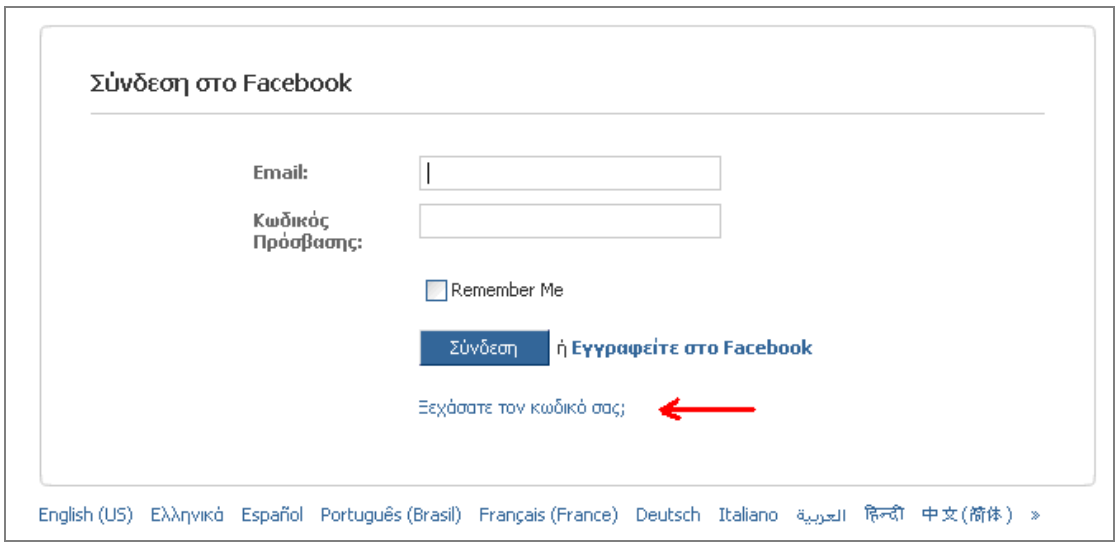
- Η απαίτηση των υπερβολικά σύνθετων passwords και ο καταναγκασμός να αλλάζονται συχνά αναγκάζουν τους χρήστες να γράφουν τους κωδικούς σε μέρη τα οποία είναι εύκολο για κάποιον ανεπιθύμητο να τα βρει, όπως για παράδειγμα δίπλα στον υπολογιστή.
- Οι χρήστες έχουν συχνά δεκάδες κωδικούς τους οποίους διαχειρίζονται. Θα ήταν πιο ρεαλιστικό να προτεινόταν ένας απλός κωδικός για όλες τις εφαρμογές χαμηλής ασφάλειας όπως για παράδειγμα το διάβασμα μιας on-line εφημερίδας ή την πρόσβαση σε ιστοχώρους ψυχαγωγίας.
- Παρομοίως, η απαίτηση να μην γράφουν οι χρήστες ποτέ τους κωδικούς τους μπορεί να μην είναι ρεαλιστικό και να ωθεί τους χρήστες να επιλέγουν αδύναμα passwords. Μια εναλλακτική λύση είναι να κρατάνε τους κωδικούς τους γραμμένους σε ένα ασφαλές μέρος όπως ένα χρηματοκιβώτιο ή ένα κρυπτογραφημένο αρχείο. Γράφοντας ένα κωδικό πρόσβασης μπορεί να είναι πρόβλημα εάν οι πιθανοί επιτιθέμενοι έχουν πρόσβαση στο ασφαλές σύστημα. Εάν η απειλή είναι μακρινοί επιτιθέμενοι που δεν έχουν πρόσβαση στο σύστημα τότε αυτό μπορεί να είναι μια πολύ ασφαλής μέθοδος.
- Ο συνυπολογισμός ειδικών χαρακτήρων μπορεί να είναι ένα πρόβλημα αν κάποιος χρήστης θέλει να συνδεθεί σε ένα υπολογιστή σε μια διαφορετική χώρα. Μερικοί ειδικοί χαρακτήρες μπορεί να είναι δύσκολοι ή αδύνατο να βρεθούν σε πληκτρολόγια σχεδιασμένα για άλλες γλώσσες.
- Μερικά συστήματα διαχείρισης ταυτότητας (identity management systems) επιτρέπουν το Self Service Password Reset κατά το οποίο ο χρήστης μπορεί να προσπεράσει την ασφάλεια απαντώντας σε μια η περισσότερες ερωτήσεις όπως "Που γεννήθηκες", "Ποια είναι η αγαπημένη σου ταινία" κτλ. Συχνά οι απαντήσεις σε αυτές τις ερωτήσεις μπορούν να βρεθούν εύκολα από μια απλή έρευνα είτε με phishing.



3.4 Πολιτική facebook

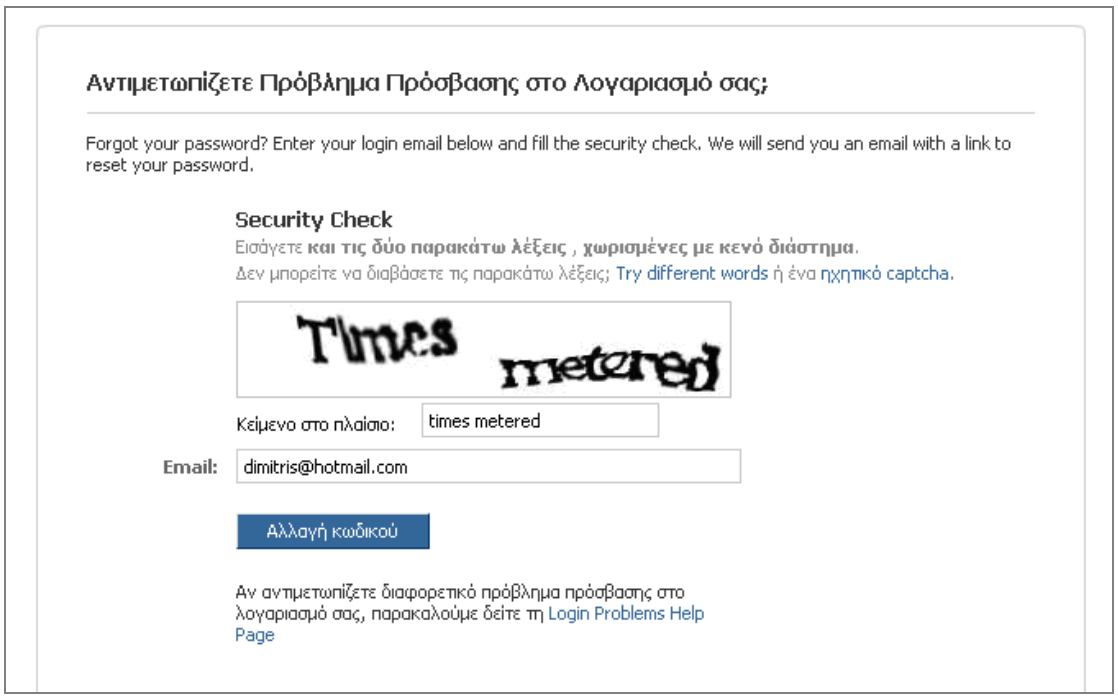
Στην ενότητα αυτή θα μελετήσουμε ποια είναι η πολιτική που χρησιμοποιεί το facebook σε περίπτωση που κάποιος χρήστης ξεχάσει τον κωδικό πρόσβασης του στη σελίδα.

Σε περίπτωση που κάποιος χρήστης ξεχάσει τον κωδικό του η απλά θέλει να τον αλλάξει δεν έχει παρά να πατήσει στο link "ξεχάσατε τον κωδικό σας ;" στην κύρια σελίδα του facebook.



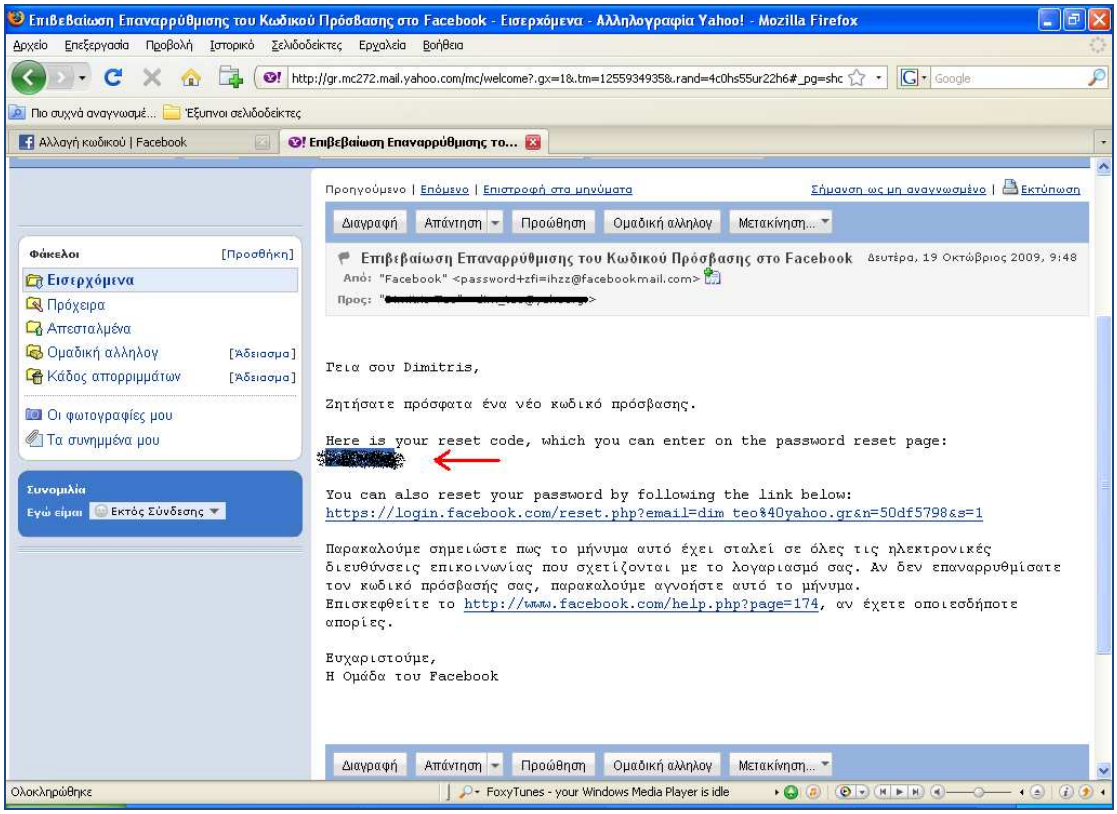
Εικόνα 43: facebook αρχική

Μας ζητάει ένα security check και το mail μας. Τα εισάγουμε και πατάμε "Αλλαγή κωδικού"



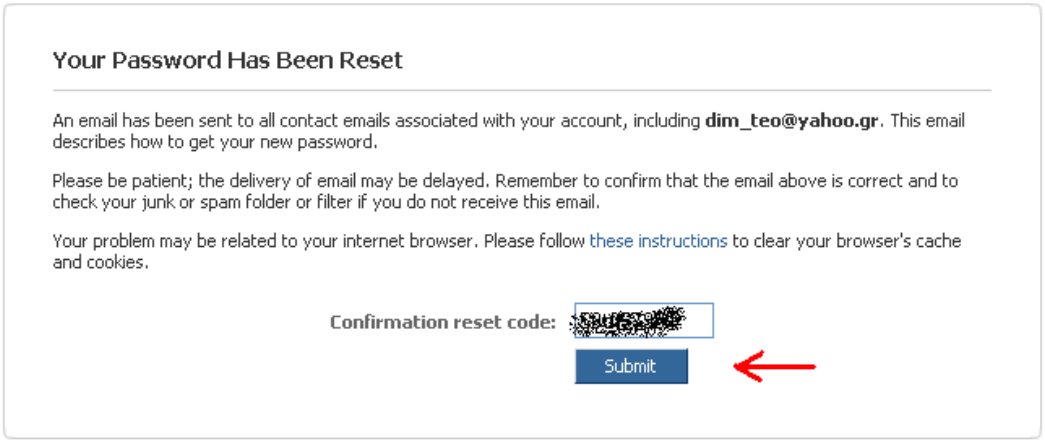
Εικόνα 44: facebook αλλαγή κωδικού

Μόλις πατήσουμε αλλαγή κωδικού μας έχει σταλεί ένα mail στη διεύθυνση που βάλαμε το οποίο περιέχει έναν κωδικό με τον οποίο μπορούμε να κάνουμε reset τον λογαριασμό μας.



Εικόνα 45: email αλλαγής κωδικού

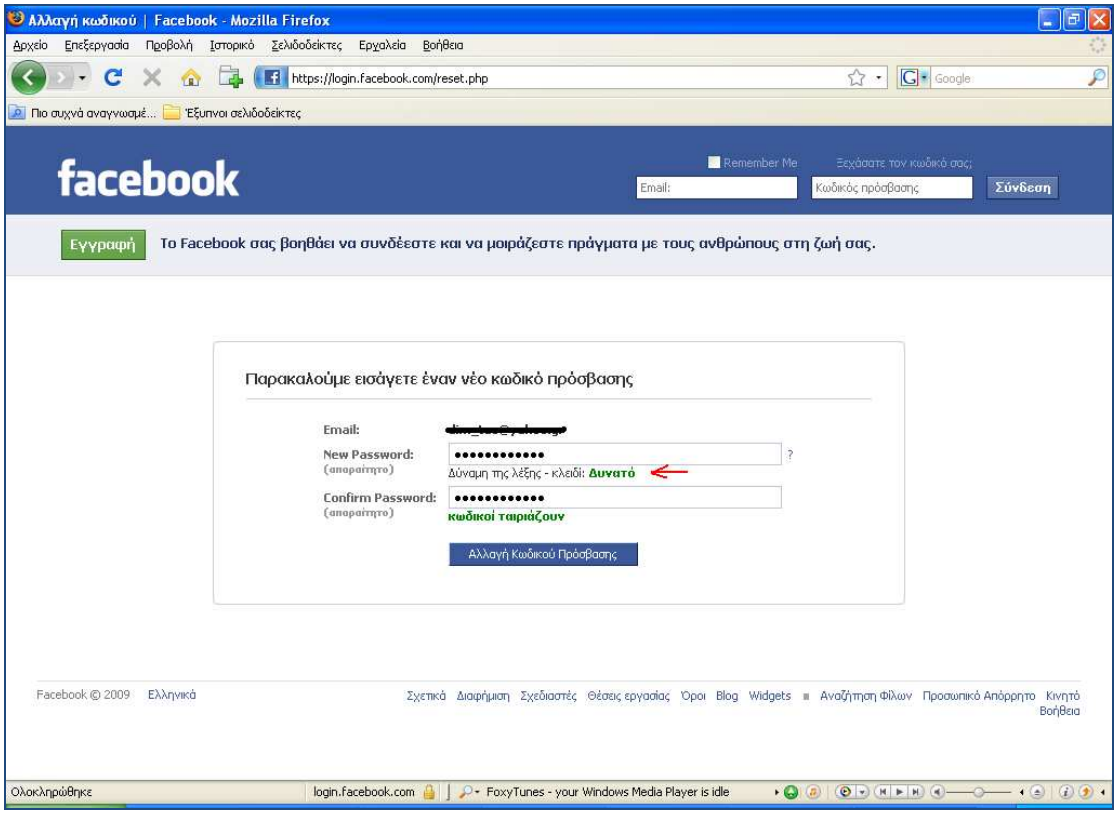
Επιστρέφουμε στο facebook βάζουμε τον κωδικό στο πεδίο που ζητείται και πατάμε *submit*.



Εικόνα 46: facebook επιβεβαίωση αλλαγής κωδικού

Στην επόμενη σελίδα βάζουμε καινούριο κωδικό πρόσβασης και πατάμε στο κουμπί *Αλλαγή κωδικού πρόσβασης*. Από ότι παρατηρούμε το facebook χρησιμοποιεί δικό του password meter με το οποίο μας ενημερώνει κατά πόσο είναι ασφαλής ο κωδικός που τοποθετήσαμε.

Η πολιτική λοιπόν του facebook απαιτεί μόνο να δώσουμε την σωστή διεύθυνση ηλεκτρονικού ταχυδρομείου από την οποία έχει ενεργοποιηθεί ο λογαριασμός. Αν δηλαδή έχουμε πρόσβαση στον λογαριασμό του e-mail μπορούμε να αλλάξουμε και τον κωδικό του facebook.

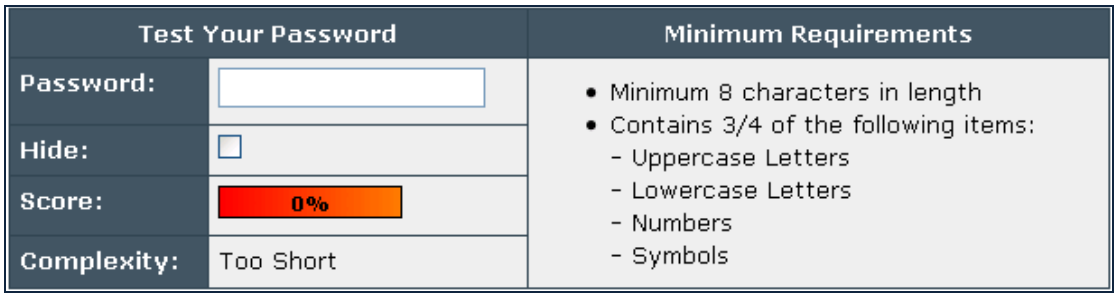


Εικόνα 47: facebook password meter

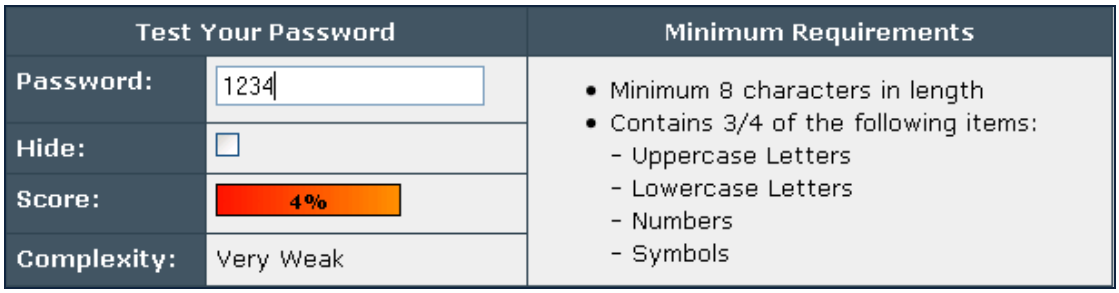
Κεφάλαιο 4 Password Strength

Η δύναμη κωδικού πρόσβασης είναι μια μέτρηση της αποτελεσματικότητας ενός κωδικού πρόσβασης. Συγκεκριμένα, υπολογίζει πόσες δοκιμές ένας επιτιθέμενος που δεν έχει άμεση πρόσβαση στον κωδικό πρόσβασης θα χρειαζόταν, κατά μέσον όρο, για να υποθέσει σωστά τον κωδικό. Υπάρχουν πολλά εργαλεία που ελέγχουν αν κάποιος κωδικός είναι ισχυρός ή όχι. Στην σελίδα http://www.passwordmeter.com/ [2] μπορούμε να βάλουμε κάποιο κωδικό και να μας δείξει το πρόγραμμα πόσο δυνατός είναι.

4.1 Password meter



Εικόνα 48: password meter αρχική



Εικόνα 49: password meter εισαγωγή εύκολου κωδικού

[2] http://www.passwordmeter.com/

✗	Number of Characters	Flat	+(n*4)	4	+ 16
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
✓	Numbers	Conc	+(n*4)	4	0
✗	Symbols	Flat	+(n*6)	0	0
✓	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
✗	Requirements	Flat	+(n*2)	1	0
Deductions					
✓	Letters Only	Flat	-n	0	0
!	Numbers Only	Flat	-n	4	- 4
✓	Repeat Characters (Case Insensitive)	Incr	-(n(n-1))	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
!	Consecutive Numbers	Flat	-(n*2)	3	- 6

Εικόνα 50: password meter υπολογισμός ασφαλείας κωδικού

Όπως βλέπουμε η ασφάλεια που μας παρέχει ένας απλός κωδικός π.χ. 1234 είναι πολύ μικρή. Της τάξης του 4%. Αν όμως χρησιμοποιήσουμε ένα password το οποίο περιέχει κεφαλαία , μικρά γράμματα, αριθμούς και σύμβολα βλέπουμε ότι είναι αρκετά ασφαλής.

Test Your Password		Minimum Requirements
Password:	DIM_teo*2009	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Εικόνα 51: password meter εισαγωγή δυνατού κωδικού

	Number of Characters	Flat	+(n*4)	12	+ 48
	Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 18
	Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 18
	Numbers	Cond	+(n*4)	4	+ 16
	Symbols	Flat	+(n*6)	1	+ 6
	Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
	Requirements	Flat	+(n*2)	5	+ 10
Deductions					
	Letters Only	Flat	-n	0	0
	Numbers Only	Flat	-n	0	0
	Repeat Characters (Case Insensitive)	Incr	-(n(n-1))	2	- 2
	Consecutive Uppercase Letters	Flat	-(n*2)	2	- 4
	Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
	Consecutive Numbers	Flat	-(n*2)	3	- 6

Legend

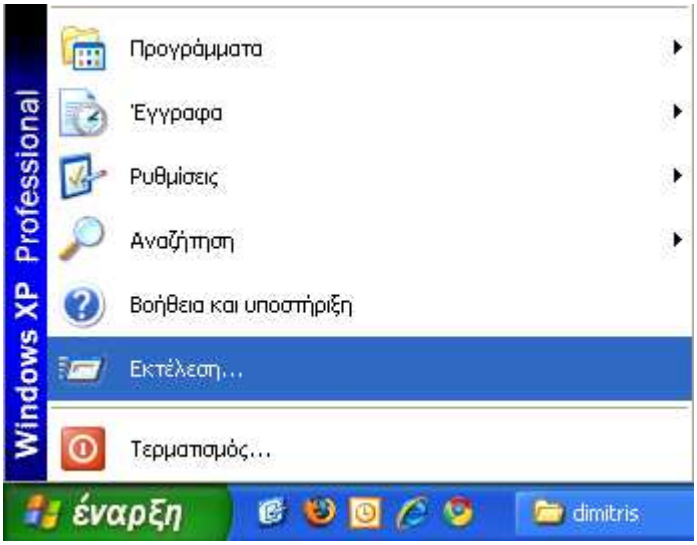
Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Εικόνα 52: password meter υπολογισμός ασφαλείας κωδικού

4.2 Δημιουργία δυνατού κωδικού στα Windows XP

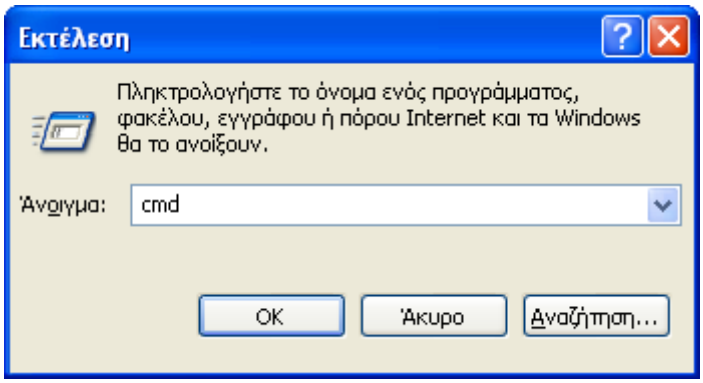
Για να κρατήσουμε το σύστημα μας ασφαλές, είναι σημαντικό να αλλάζουμε συχνά τα passwords μας. Αν κάποιος δυσκολεύεται στο να βρει έναν δυνατό κωδικό τα Windows XP μπορούν να δημιουργήσουν για εμάς.
Οι χρήστες ηλεκτρονικών υπολογιστών συχνά χρησιμοποιούν πολύ απλοϊκή λογική όταν δημιουργούν password. Για παράδειγμα πολλοί από μας διαλέγουν λέξεις που έχουν νόημα, προσωπικές ημερομηνίες ή μια λέξη που κάποιος μπορεί να βρει στο λεξικό γιατί αυτό κάνει το password πιο εύκολο για να το θυμάται κάνεις.
Αν δεν μπορείτε να σκεφτείτε ένα δυνατό password, αφήστε τα Windows να δημιουργήσουν και να ορίσουν ένα τυχαίο password για το account σας. Για να γίνει αυτό ακολουθούμε τα παρακάτω βήματα:

Πατάμε έναρξη→ εκτέλεση…



Εικόνα 53: πατάμε έναρξη και εκτέλεση

Στο παράθυρο που θα εμφανιστεί γράφουμε cmd και πατάμε OK.



Εικόνα 54: πληκτολογούμε cmd

Ανοίγει το παρακάτω παράθυρο.

Εικόνα 55: γραμμή εντολών

Πληκτρολογούμε net user [username] /random και τα Windows δημιουργούν αυτόματα έναν δυνατό και ασφαλή κωδικό για εμάς.

Εικόνα 56: cmd εντολή για δημιουργία κωδικού

Όπως βλέπουμε με την εντολή net user admin /random ο κωδικός πρόσβασης για τον λογαριασμό του χρήστη admin άλλαξε σε a3f7nrmU.

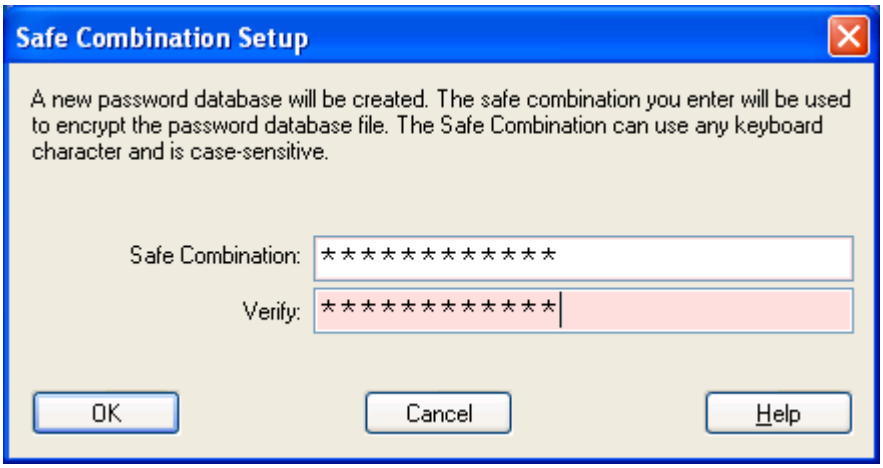
4.3 Password Safe

Για την προφύλαξη των passwords που έχει ο καθένας μας είναι δυνατό να χρησιμοποιηθεί το πρόγραμμα passwordsafe το οποίο αποθηκεύει τα passwords κρυπτογραφημένα σε database. [3]

Κατά την εκκίνηση του προγράμματος εμφανίζεται η παρακάτω οθόνη.

Εικόνα 57: password safe αρχική

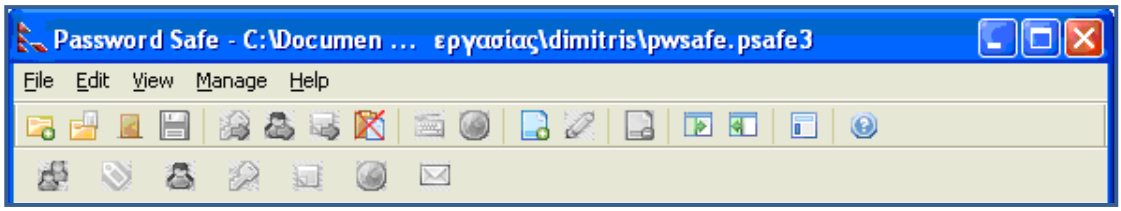
Επιλέγουμε *new database*



Εικόνα 58: password safe επιλογή δυνατού κωδικού

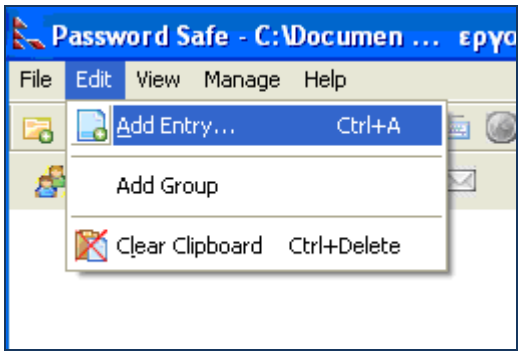
Βάζουμε έναν ασφαλή κωδικό (στη συγκεκριμένη περίπτωση DIM_teo*2009) πατάμε OK και εμφανίζεται το επόμενο παράθυρο.

[3] http://passwordsafe.sourceforge.net/



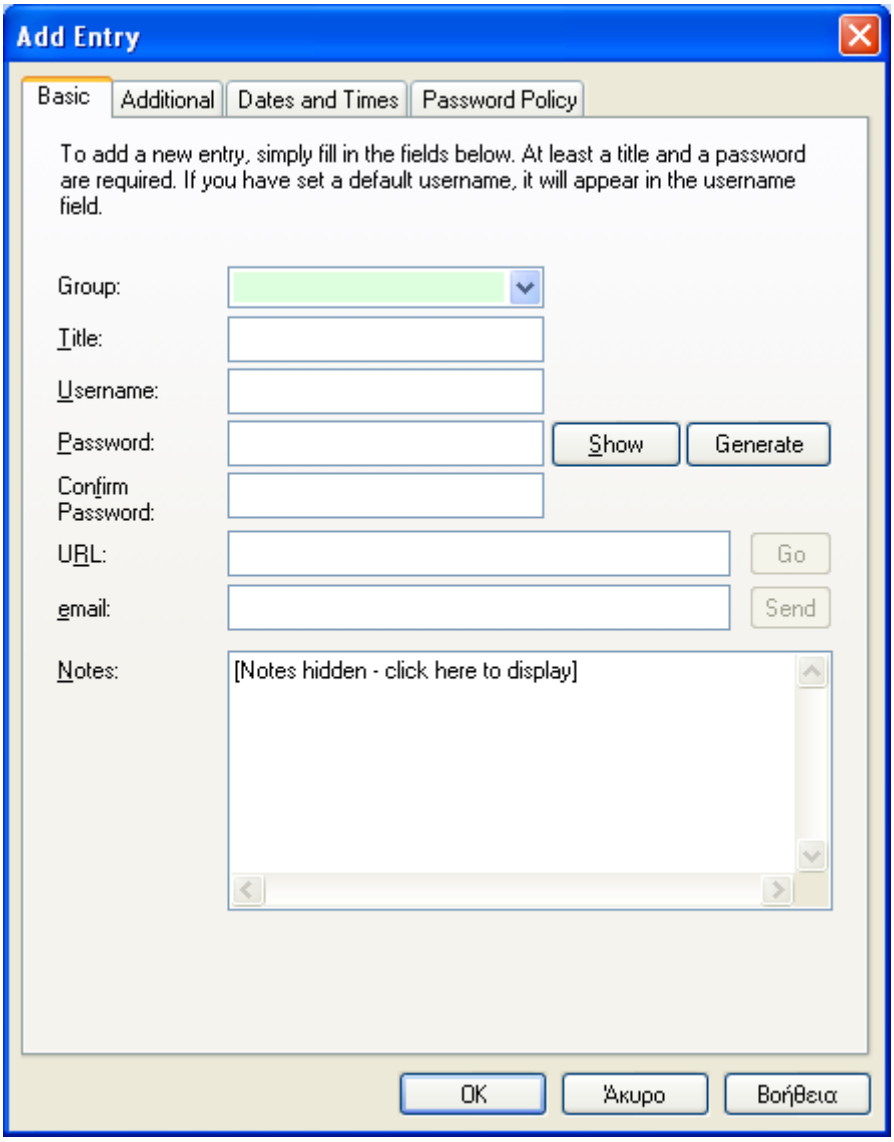
Εικόνα 59: περιβάλλον εργασίας passwordsafe

Πατάμε edit→ Add Entry, ή εναλλακτικά ctrl+A ως συντόμευση.



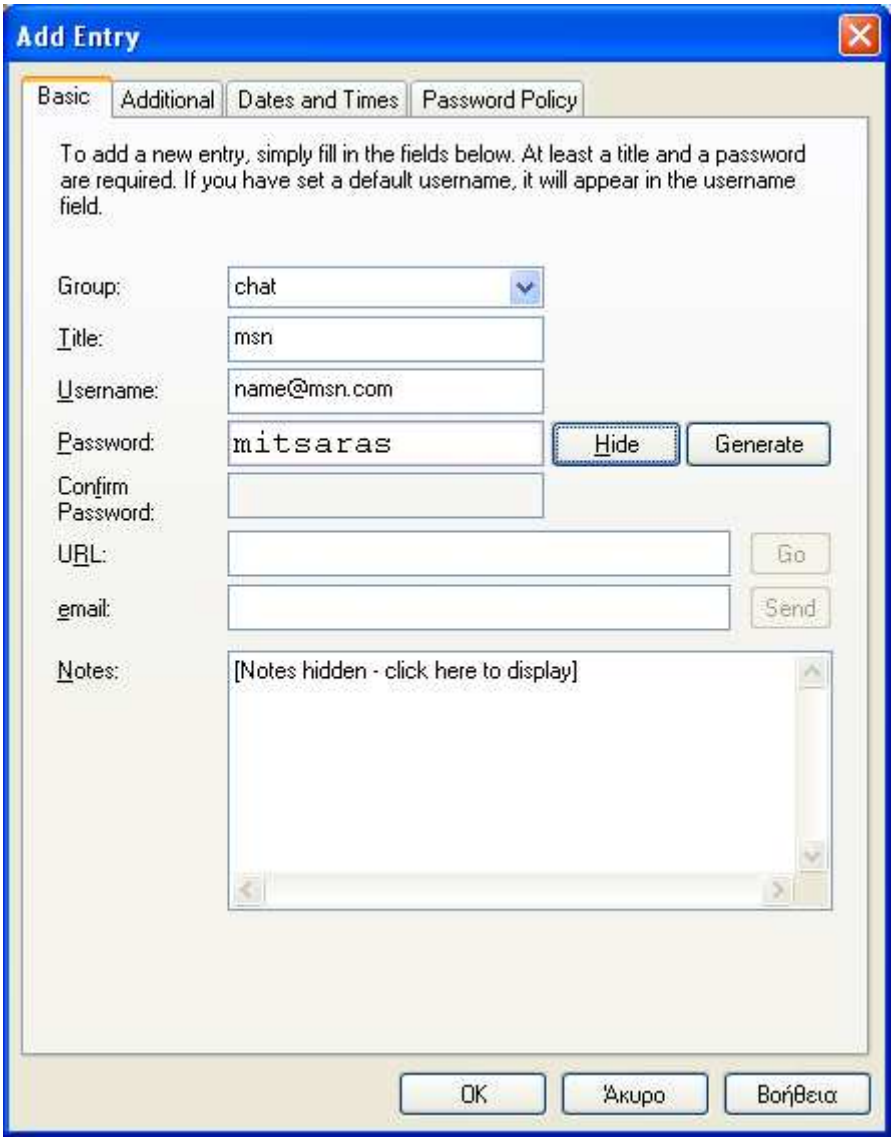
Εικόνα 60: password safe: edit και add entry

Και βλέπουμε το παρακάτω παράθυρο.



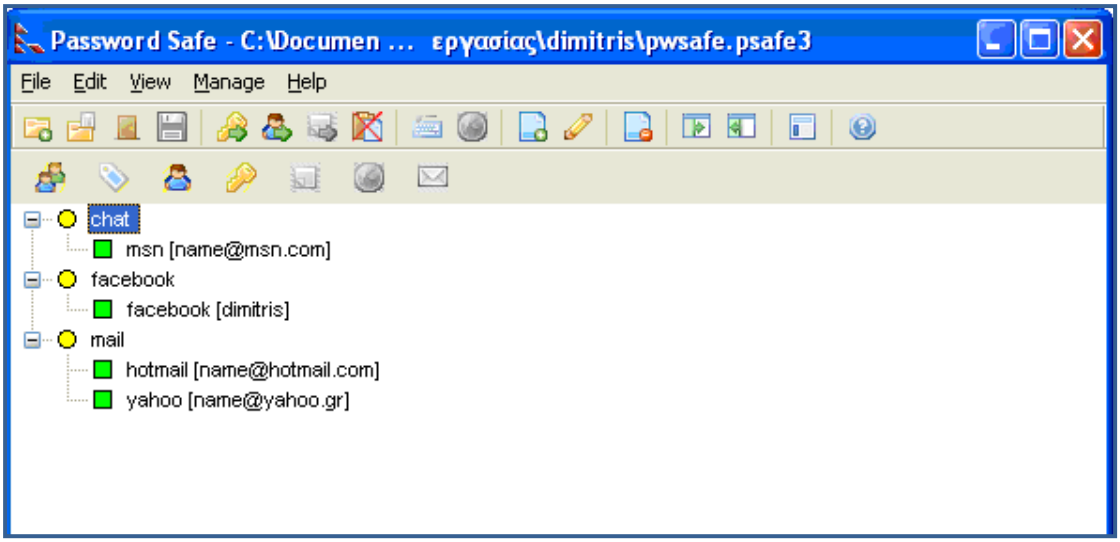
Εικόνα 61: επιλογές passwordsafe

Από εδώ μπορούμε να ομαδοποιήσουμε τους κωδικούς μας ανάλογα με τον τομέα στον οποίο τους χρησιμοποιούμε. Το πρόγραμμα μας δίνει τη δυνατότητα να φτιάξουμε δικά μας group και να προσθέσουμε όσους κωδικούς επιθυμούμε. Για παράδειγμα μπορούμε να ορίσουμε ένα group με το όνομα mail και να βάλουμε όλα μας τα mail μαζί με τους κωδικούς τους.



Εικόνα 62: password safe δημιουργία νέου group

Παρατηρούμε ότι το password safe μας δίνει τη δυνατότητα μαζί με το username και το password να αποθηκεύσουμε και κάποιες σημειώσεις σχετικά με τον συγκεκριμένο κωδικό. Μπορούμε να προσθέσουμε όσους κωδικούς θέλουμε. Το αποτέλεσμα φαίνεται παρακάτω.

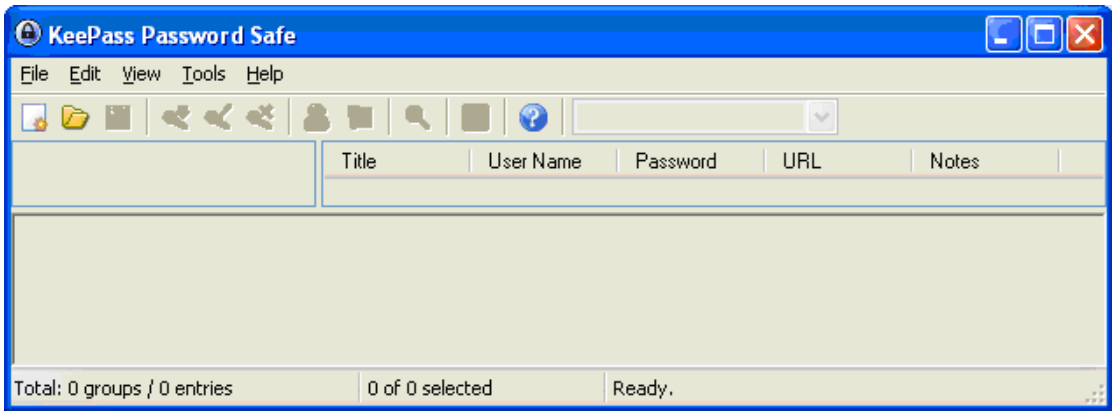


Εικόνα 63: password safe αποθηκευμένα group και κωδικοί

Αν θέλουμε να χρησιμοποιήσουμε κάποιον απ΄ τους κωδικούς κάνουμε διπλό κλικ πάνω και το πρόγραμμα αντιγράφει τον κωδικό στο clipboard. Μέτα μπορούμε να κάνουμε επικόλληση τον κωδικό όπου εμείς επιθυμούμε.

4.4 KeePass

Ένα εξίσου χρήσιμο και εύχρηστο προγραμματάκι για την φύλαξη των κωδικών μας είναι το KeePass [4]. Στην παρακάτω εικόνα βλέπουμε το αρχικό παράθυρο του προγράμματος.



Εικόνα 64: αρχική του KeePass

Επιλέγουμε File→New ή Ctrl + N σαν συντόμευση και εμφανίζεται το παρακάτω παράθυρο.

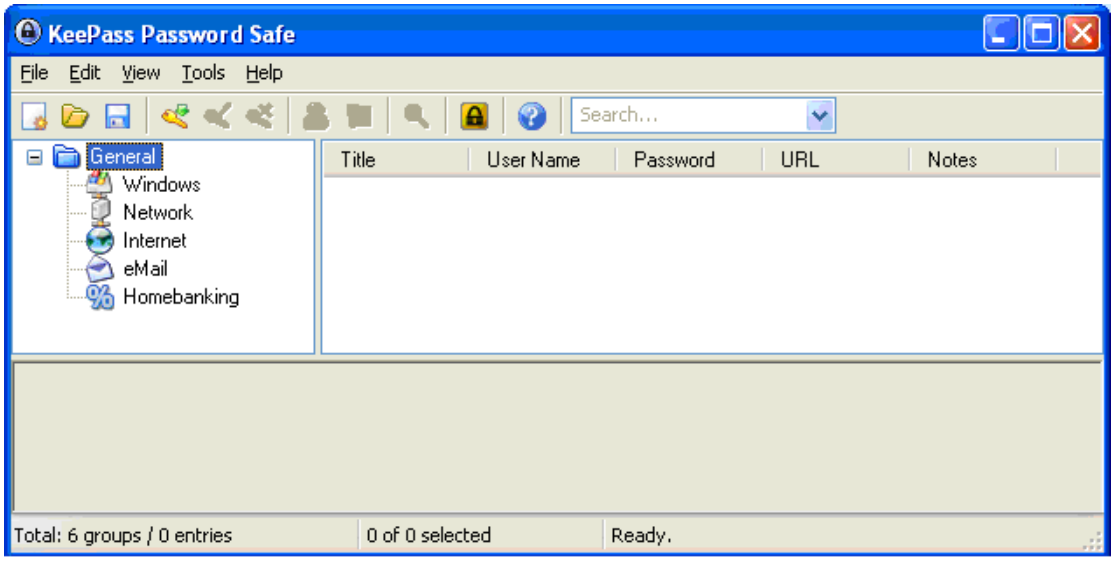
Εικόνα 65: KeePass επιλογή κύριου κωδικού

Βάζουμε έναν ασφαλή κωδικό και πατάμε OK.

[4] http://keepass.info/

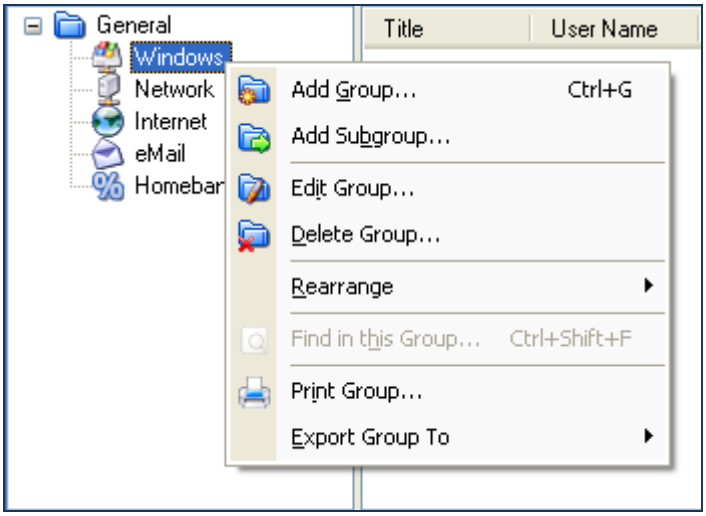
Εικόνα 66: KeePass επιλογή ασφαλούς κύριου κωδικού

Αφού βάλουμε τον κωδικό και δεύτερη φορά σαν επιβεβαίωση έχουμε δημιουργήσει μια νέα βάση δεδομένων στην οποία θα αποθηκεύονται οι κωδικοί.



Εικόνα 67: παράθυρο KeePass

Όπως βλέπουμε στο παράθυρο που εμφανίζεται το πρόγραμμα έχει χωρίσει από μόνο του σε group (windows, network, internet, email, home banking). Μπορούμε βέβαια να διαγράψουμε αυτά τα group και να φτιάξουμε δικά μας με τις ονομασίες που εμείς επιθυμούμε. Αυτό γίνεται με δεξί κλικ πάνω στο group και επιλέγοντας delete group αν θέλουμε να διαγράψουμε και add group αν θέλουμε να δημιουργήσουμε ένα νέο.

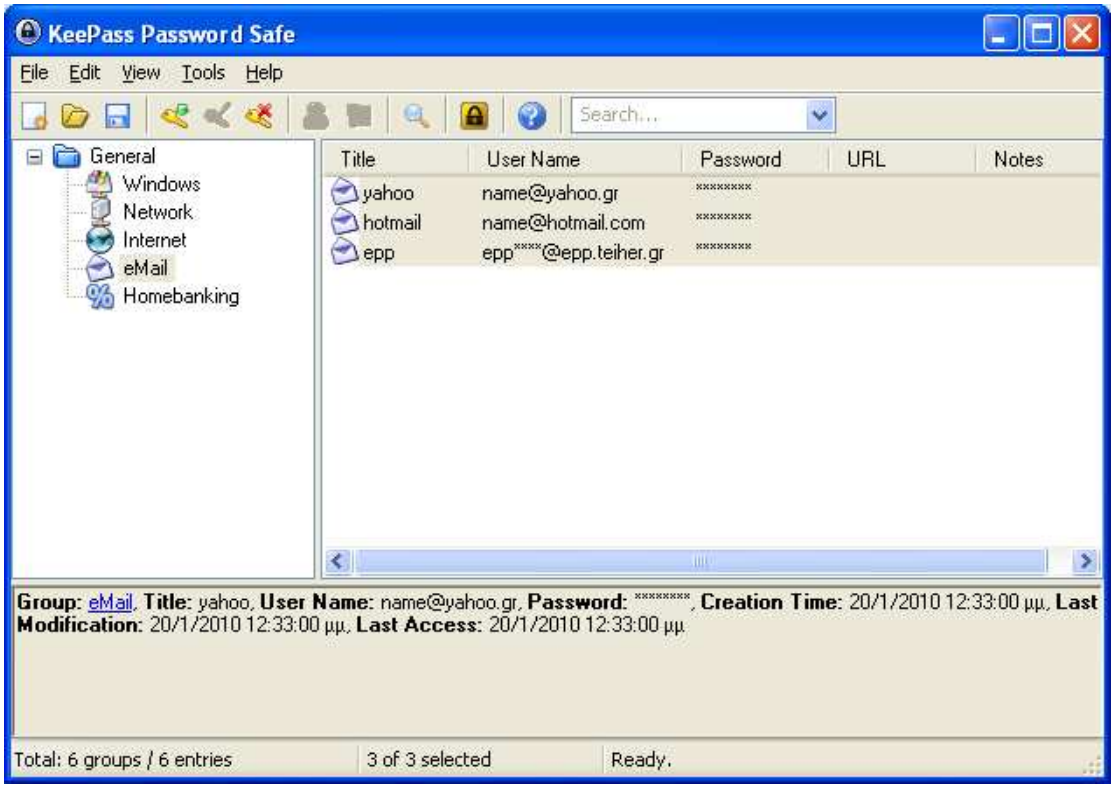


Εικόνα 68: KeePass επιλογές για τα group

Έχοντας επιλεγμένο ένα group και πατώντας edit→ add entry δημιουργούμε μια νέα καταχώρηση στο συγκεκριμένο group.

Εικόνα 69: KeePass νέα καταχώρηση

Γράφουμε τον τίτλο, το όνομα χρήστη, τον κωδικό πρόσβασης και ότι άλλες σημειώσεις θέλουμε και πατάμε OK. Το πρόγραμμα μετράει από μόνο του την ποιότητα του κωδικού που βάλαμε.



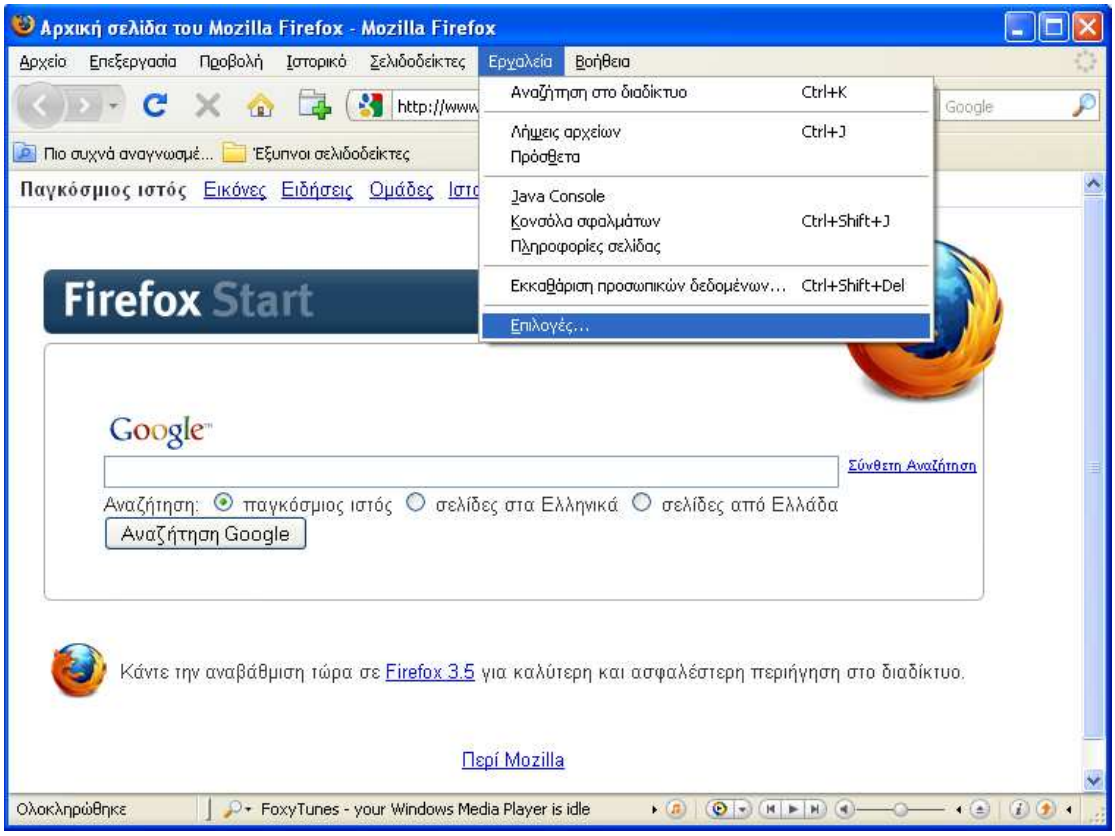
Εικόνα 70: KeePass καταχωρήσεις στο group email

Τώρα αν θέλουμε να χρησιμοποιήσουμε κάποιο από τους αποθηκευμένους κωδικούς δεν έχουμε παρά να κάνουμε διπλό κλικ πάνω στην συγκεκριμένη καταχώρηση, ή απλά δεξί κλικ και copy password. Ο κωδικός έχει αντιγραφεί στο clipboard και μπορούμε να τον κάνουμε επικόλληση.

4.5 Firefox master password

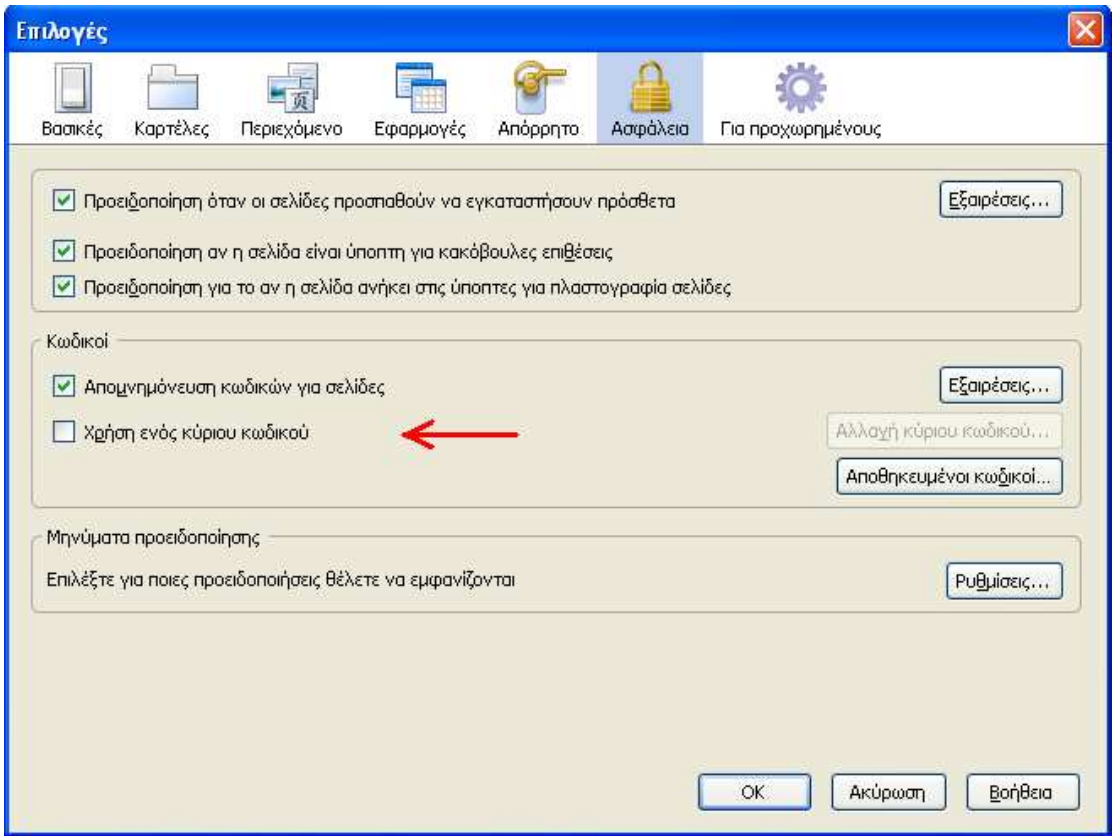
Ο Firefox έχει τη δυνατότητα να αποθηκεύει το όνομα χρήστη και τον κωδικό πρόσβασης σε διάφορες σελίδες που επισκεπτόμαστε (π.χ. forum, mail, facebook). Χρησιμοποιώντας έναν κύριο κωδικό (master password) μπορούμε να προστατέψουμε τους κωδικούς μας. Έτσι όταν κάποιος χρήστης μπει σε μια σελίδα στην οποία χρειάζεται να δώσει username και password θα ζητηθεί επιπλέον και ο κύριος κωδικός.

Ανοίγουμε ένα παράθυρο του Firefox και επιλέγουμε από την καρτέλα *Εργαλεία→ Επιλογές…*

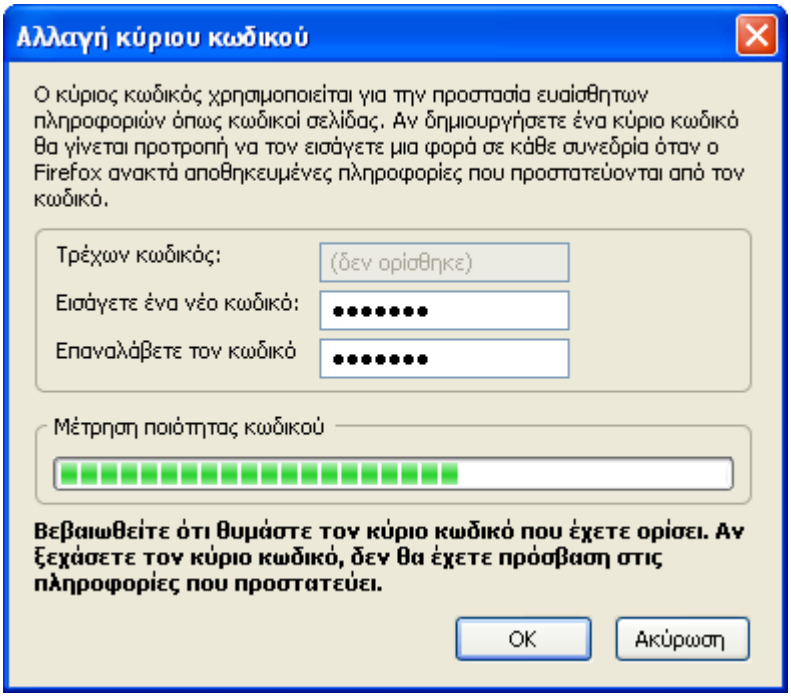


Εικόνα 71: Firefox επιλογές

Από το νέο παράθυρο που άνοιξε, πάμε στην καρτέλα *Ασφάλεια* και επιλέγουμε *Χρήση ενός κύριου κωδικού.*

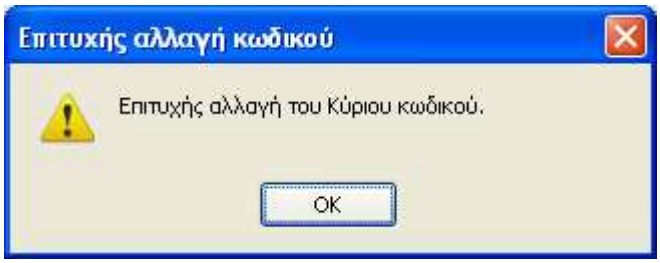


Εικόνα 72: Firefox χρήση ενός κύριου κωδικού



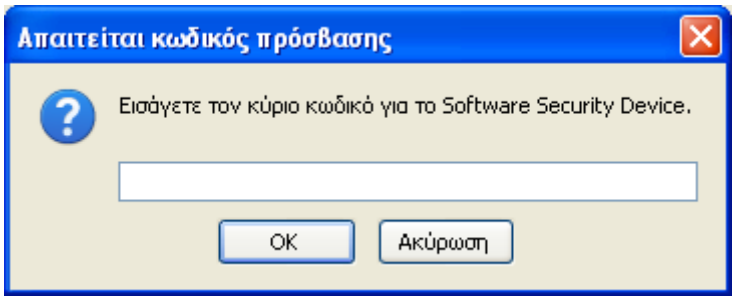
Εικόνα 73: Firefox εισαγωγή κύριου κωδικού

Βλέπουμε ότι η συγκεκριμένη επιλογή του Firefox χρησιμοποιεί δικό της ενσωματωμένο password meter ώστε να δούμε πόσο ισχυρός θα είναι ο κύριος κωδικός που χρησιμοποιούμε.



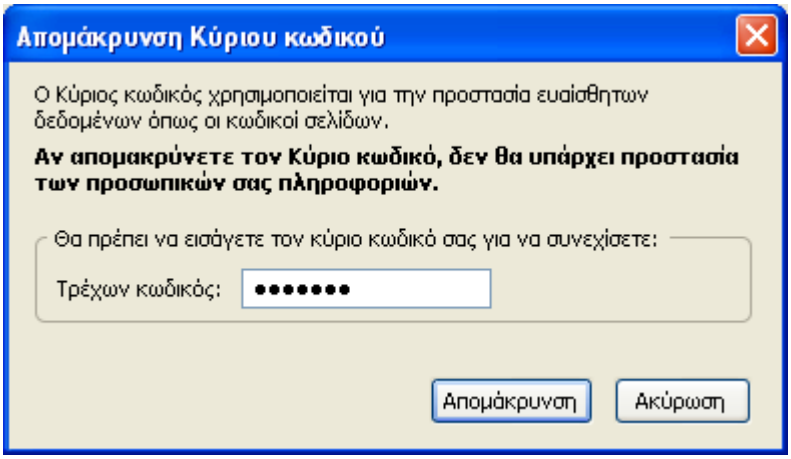
Εικόνα 74: Firefox επιτυχής αλλαγή κύριου κωδικού

Τώρα εκτός του password θα πρέπει να βάζουμε και τον κύριο κωδικό σε κάθε σελίδα που χρειάζεται login.

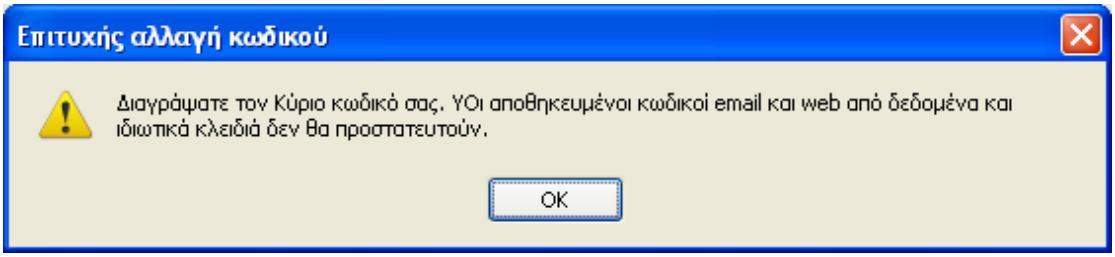


Εικόνα 75: Firefox εισαγωγή κύριου κωδικού

Αν θελήσουμε να απομακρύνουμε τον κύριο κωδικό ο Firefox μας προειδοποιεί ότι δεν θα έχουμε πλέον προστασία των προσωπικών μας δεδομένων. Πατάμε απομάκρυνση και ο κύριος κωδικός δεν θα χρειάζεται πλέον σε όποια σελίδα υπάρχει login name και password.



Εικόνα 76: Firefox διαγραφή κύριου κωδικού



Εικόνα 77: Firefox επιτυχής αλλαγή κωδικού

Firefox Master password crack

Αν κάποιος χρήστης ξεχάσει τον κύριο κωδικό μπορεί να χρησιμοποιήσει το δωρεάν εργαλείο FireMaster[5] για να τον ανακτήσει. Το πρόγραμμα χρησιμοποιεί ένα συνδυασμό τεχνικών όπως επιθέσεις λεξικού(dictionary) και ωμής βίας(brute force) για να ανακτήσει τον master password από το αρχείο βάσης δεδομένων του Firefox.

Η διαδικασία έχει ως εξής:

- Το FireMaster δημιουργεί κωδικούς πρόσβασης στη μνήμη του υπολογιστή.
- Στη συνέχεια υπολογίζει το hash του κωδικού πρόσβασης χρησιμοποιώντας γνωστούς αλγόριθμους.
- Μετά το hash του κωδικού χρησιμοποιείται για την αποκρυπτογράφηση των κρυπτογραφημένων δεδομένων.
- Τέλος αν το αποκρυπτογραφημένο string ταιριάζει με το plain text τότε το παραγόμενο password αποτελεί τον κύριο κωδικό.

Το FireMaster υποστηρίζει τις ακόλουθες μεθόδους ανάκτησης του κωδικού πρόσβασης.

1. Μέθοδος λεξικό

Σε αυτή τη λειτουργία το FireMaster χρησιμοποιεί αρχείο λεξικού έχοντας κάθε λέξη σε ξεχωριστή γραμμή για την εκτέλεση της διαδικασίας. Υπάρχουν πολλά έτοιμα λεξικά στο διαδίκτυο με διαφορετικά μεγέθη και να τα δώσουμε στο FireMaster. Η μέθοδος αυτή είναι γρήγορη και μπορεί να βρει κοινούς κωδικούς πρόσβασης.

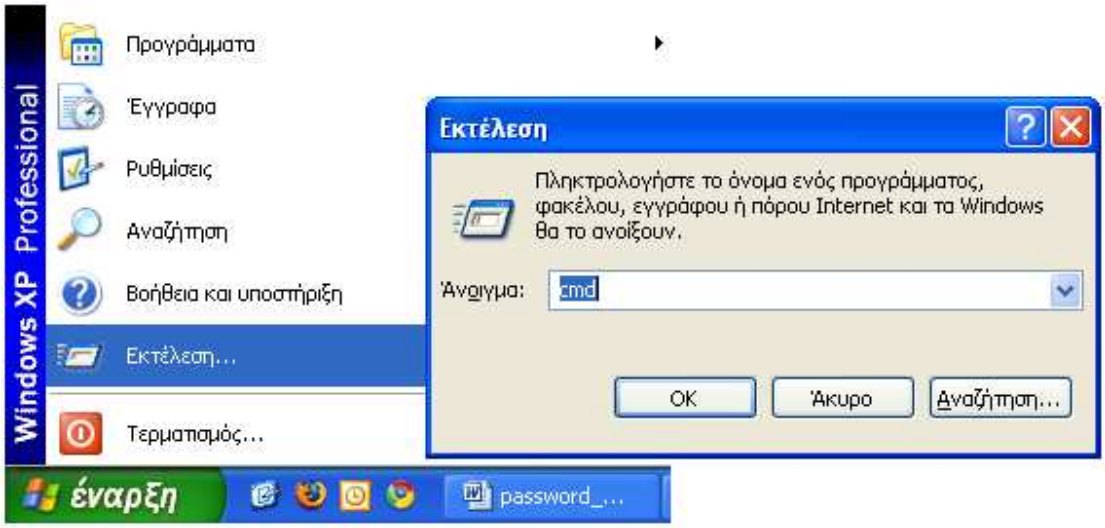
2. Μέθοδος ωμής βίας (brute force)

Σε αυτή την μέθοδο, παράγονται όλοι οι δυνατοί συνδυασμοί λέξεων από δεδομένο κατάλογο χαρακτήρων και υποβάλλονται στη διαδικασία του cracking. Αυτό μπορεί να διαρκέσει μεγάλο χρονικό διάστημα ανάλογα με τον αριθμό των χαρακτήρων τον οποίο αποτελείται ο κωδικός.

Ο Firefox αποθηκεύει τις λεπτομέρειες σχετικά με το κωδικοποιημένο string στο αρχείο βάσης δεδομένων key3.db. Το αρχείο αυτό βρίσκεται στο φάκελο του προφίλ του Firefox. Αν ακολουθήσουμε τη διαδρομή C:\Users\dimitrs\AppData \Roaming\Mozilla\Firefox\Profiles θα βρούμε το αρχείο αυτό. Για να δούμε όμως πως λειτουργεί το FireMaster.

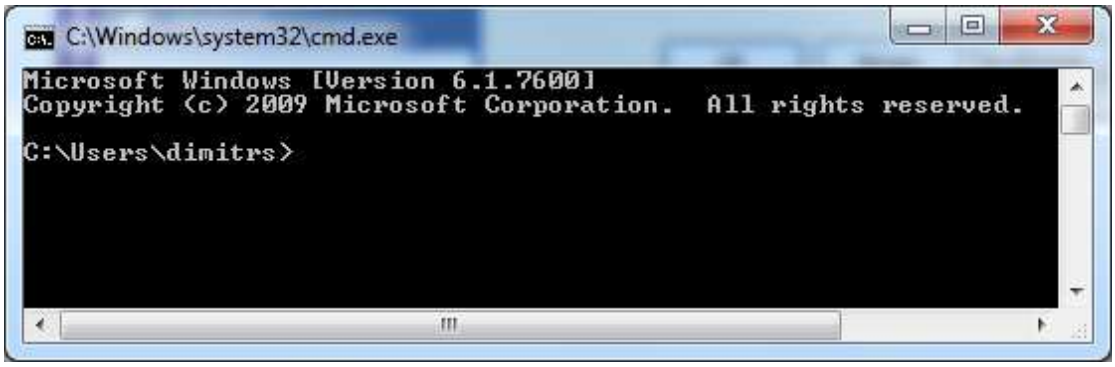
[5] http://securityxploded.com/firemaster.php

Πρώτα από όλα ανοίγουμε ένα command prompt. Πατάμε έναρξη → εκτέλεση και πληκτρολογούμε cmd.



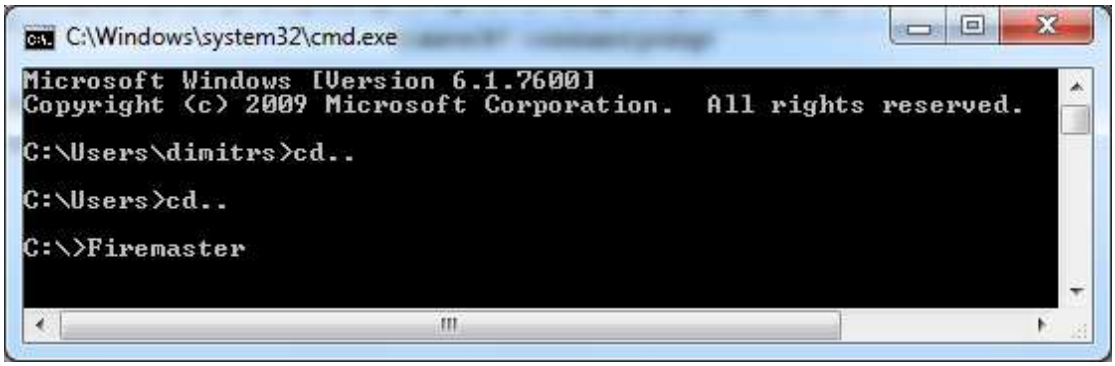
Εικόνα 78: ανοίγουμε ένα command prompt

Θα ανοίξει μια γραμμή εντολών.

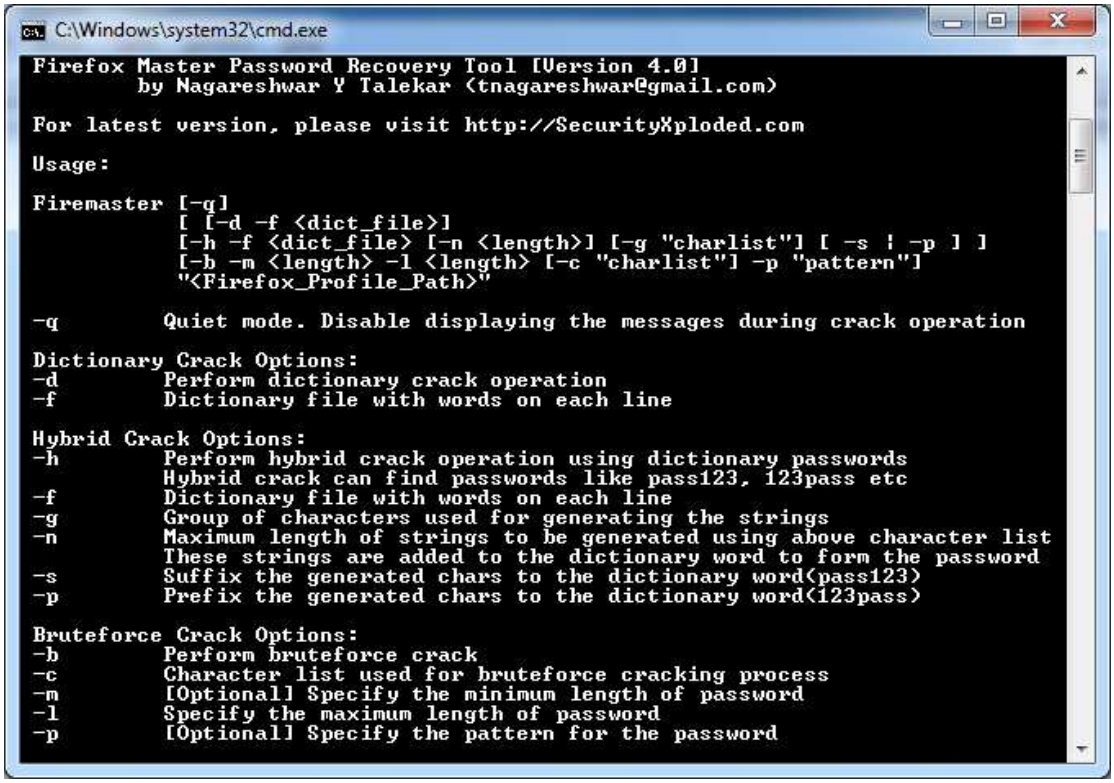


Εικόνα 79: command prompt

Ακολουθούμε τη διαδρομή για να φτάσουμε στο φάκελο όπου έχουμε αποθηκεύσει το πρόγραμμα.

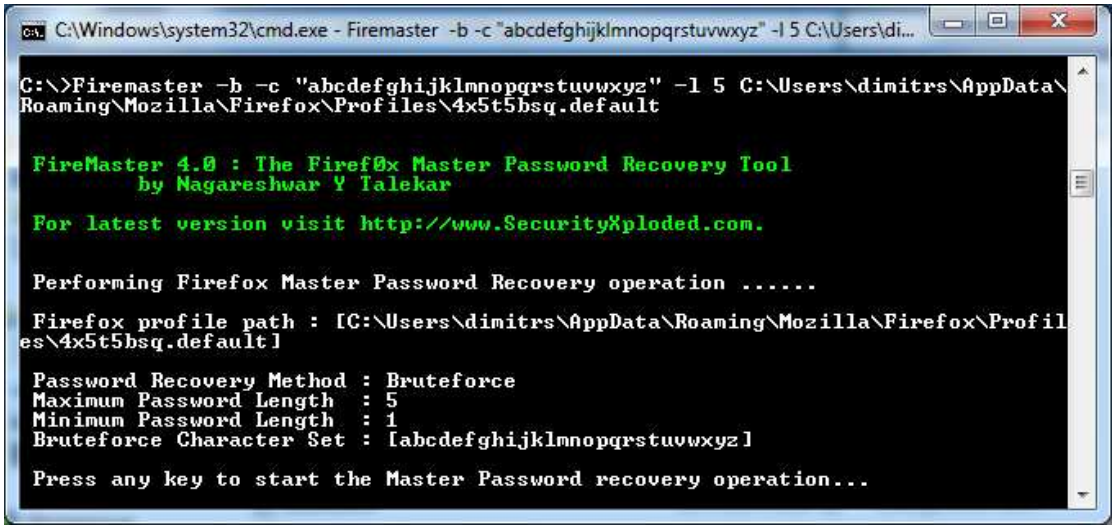


Εικόνα 80: command prompt διαδρομή για Firemaster



Εικόνα 81: command prompt Firemaster

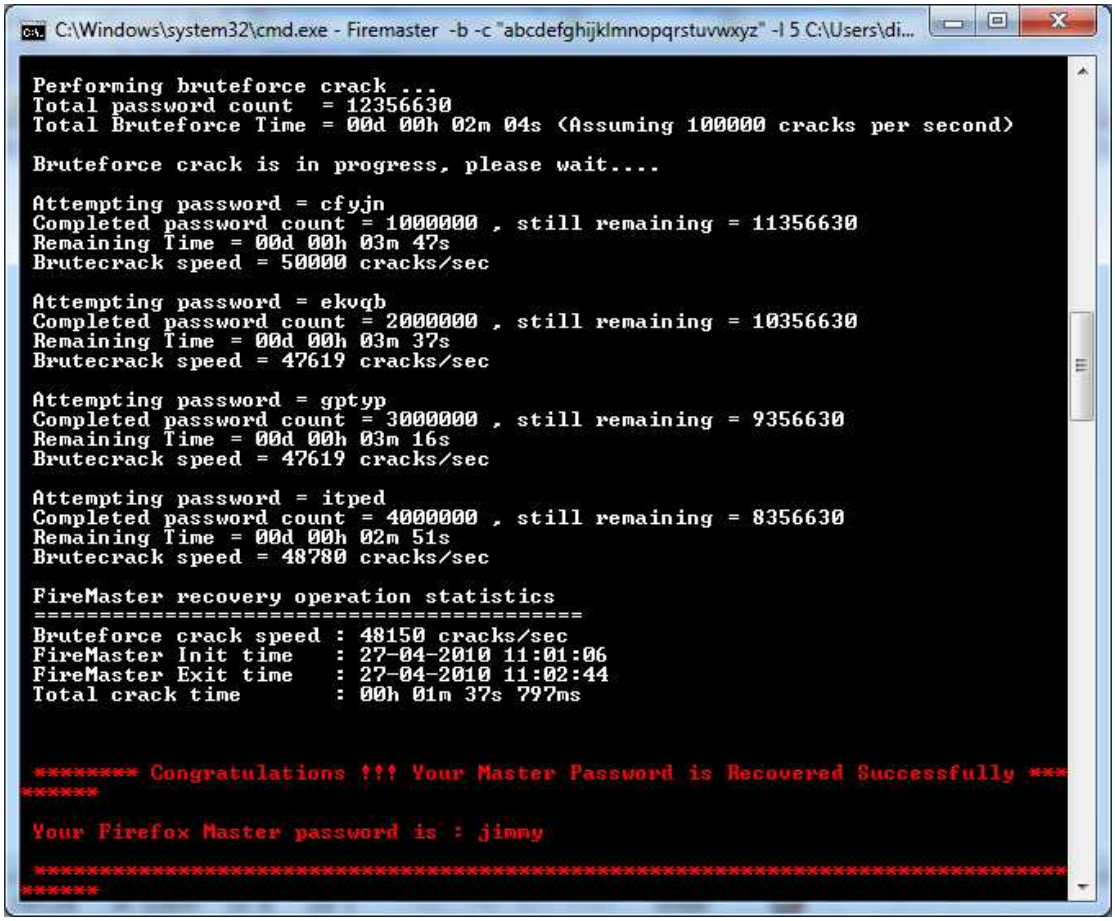
Όπως βλέπουμε το πρόγραμμα μας ενημερώνει για τις εντολές που πρέπει να πληκτρολογήσουμε ώστε να γίνει το crack και να ανακτήσουμε τον κύριο κωδικό του Firefox.



Εικόνα 82: command prompt Firemaster εντολή για crack

Δίνοντας την εντολή Firemaster –b –c “abcdefghijklmnopqrstuvwxyz” –l 5 C:\Users \dimitrs\AppData\Roaming\Mozilla\Firefox\Profiles\4x5t5bsq.default αρχίζει το cracking.

Με το –b δηλώνουμε στο Firemaster ότι η επίθεση που θα κάνει θα είναι Brute force. Το –c δηλώνει τη λίστα των χαρακτήρων που θα χρησιμοποιηθούν για την επίθεση. Με το –l δίνουμε το μέγιστο αριθμό χαρακτήρων από τους οποίους αποτελείται ο κωδικός. Και με τη διαδρομή C:\Users\dimitrs\AppData\Roaming\Mozilla\Firefox \Profiles\4x5t5bsq.default καθορίζουμε που βρίσκεται το key3.db αρχείο.



Εικόνα 83: command prompt Firemaster ανάκτηση κωδικού

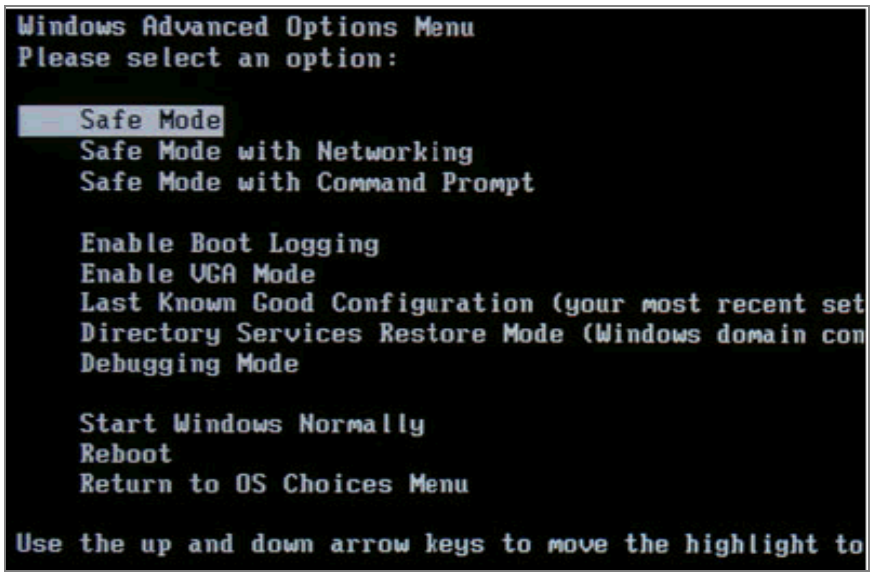
Βλέπουμε ότι το Firemaster κατά τη διάρκεια τη επίθεσης δοκίμαζε 48150 πιθανούς κωδικούς το δευτερόλεπτο και του πήρε 1 λεπτό και 37 δευτερόλεπτα για να ανακτήσει τον Maser password του Firefox.

Κεφάλαιο 5 Σπάσιμο κωδικού administrator και BIOS

Σε αρκετές περιπτώσεις ο χρήστης μπορεί να ξεχάσει τον κωδικό του λογαριασμού του με αποτέλεσμα να μην έχει πρόσβαση στα αρχεία του. Υπάρχουν διάφοροι τρόποι για να γίνει ανάκτηση του κωδικού. Δύο από αυτούς περιγράφονται παρακάτω.

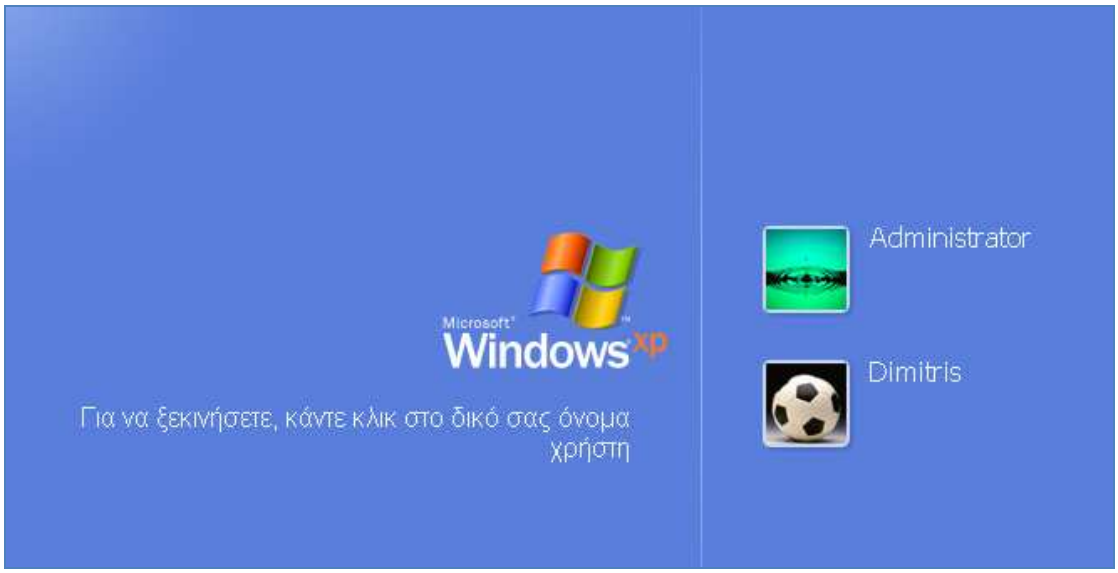
5.1 Administrator ο εύκολος τρόπος (μέσω safe mode)

Αρχικά κάνουμε επανεκκίνηση τον υπολογιστή. Κατά τη διαδικασία της εκκίνησης πατάμε F8 και περιμένουμε μέχρι να εμφανιστεί η παρακάτω εικόνα.



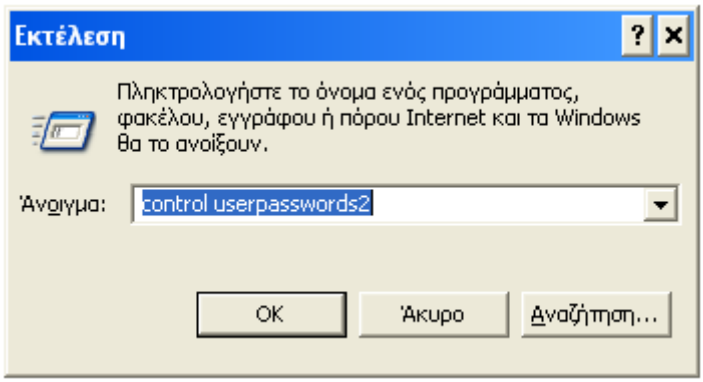
Εικόνα 84: επιλογή safe mode

Επιλέγουμε Safe Mode και πατάμε ENTER. Περιμένουμε λίγο και εμφανίζεται η αρχική εικόνα των Windows στην οποία επιλέγουμε σε ποιό λογαριασμό θέλουμε να συνδεθούμε.



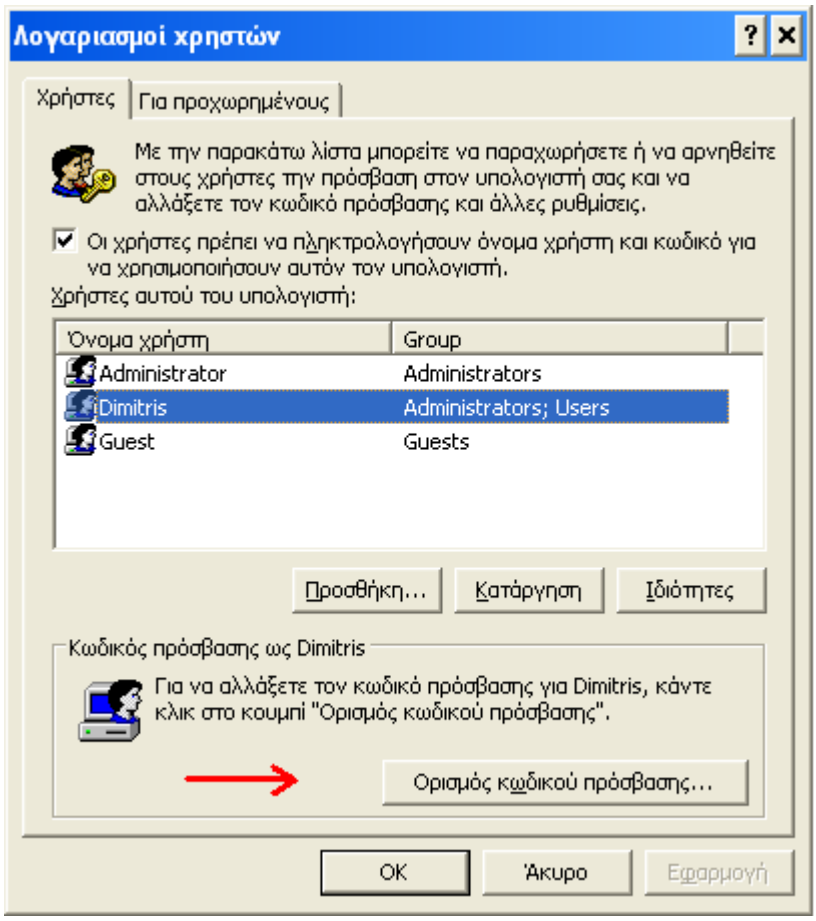
Εικόνα 85: Windows log in λογαριασμοί χρηστών

Επιλέγουμε τον λογαριασμό Administrator και παρατηρούμε ότι δεν μας ζητάει κάποιο κωδικό για την είσοδο στα windows. Τώρα πατάμε Έναρξη → εκτέλεση και δίνουμε την εντολή control userpasswords2.



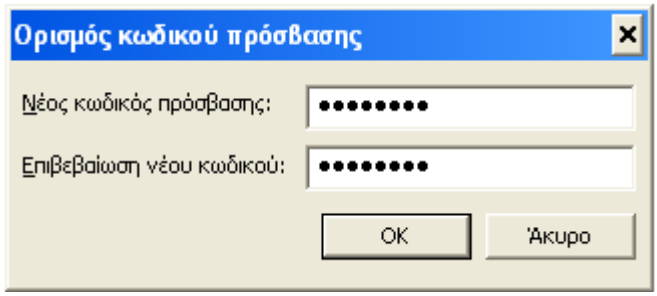
Εικόνα 86: εντολή control userpasswords2

Ανοίξαμε το παράθυρο λογαριασμοί χρηστών. Στην καρτέλα χρήστες βλέπουμε μια λίστα με όλα τα ονόματα χρηστών αυτού του υπολογιστή καθώς και το group στο οποίο ανήκουν. Επιλέγουμε τον λογαριασμό που θέλουμε και πατάμε το κουμπί ορισμός κωδικού πρόσβασης.



Εικόνα 87: παράθυρο λογαριασμοί χρηστών

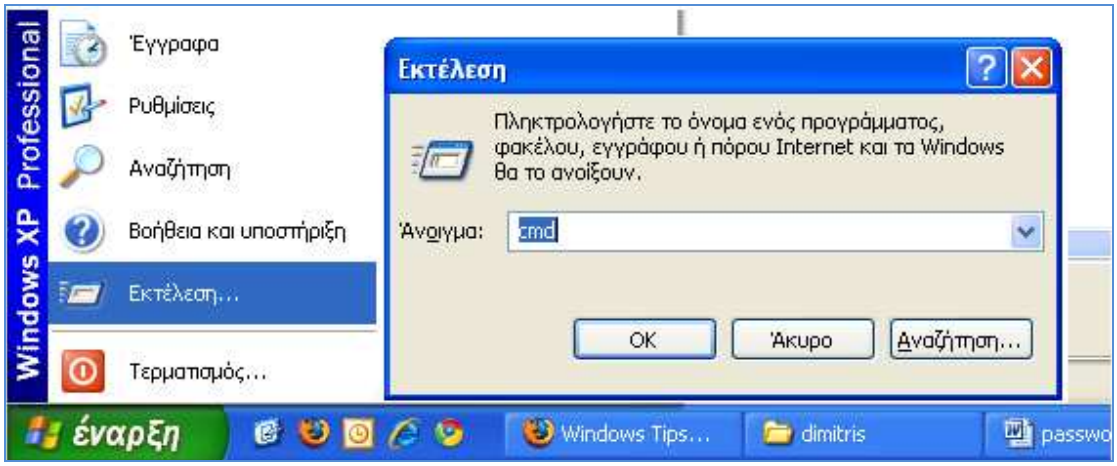
Ανοίγει ένα νέο παράθυρο και μας ζητάει να ορίσουμε νέο κωδικό για τον συγκεκριμένο λογαριασμό. Μπορούμε να βάλουμε ότι κωδικό θέλουμε και να τον χρησιμοποιήσουμε για να εισέλθουμε κανονικά στα Windows την επόμενη φορά που θα ξεκινήσουμε τον υπολογιστή.



Εικόνα 88: ορισμός νέου κωδικού πρόσβασης

5.2 Administrator ο δύσκολος τρόπος

Ο τρόπος αυτός απαιτεί να έχουμε πρόσβαση σε έναν οποιονδήποτε λογαριασμό του υπολογιστή. Ανοίγουμε ένα παράθυρο DOS. Κάνουμε κλικ Έναρξη → εκτέλεση και πληκτρολογούμε cmd.



Εικόνα 89: πατάμε έναρξη εκτέλεση και πληκτρολογούμε cmd

Ανοίξαμε μια γραμμή εντολών.

Εικόνα 90: γραμμή εντολών

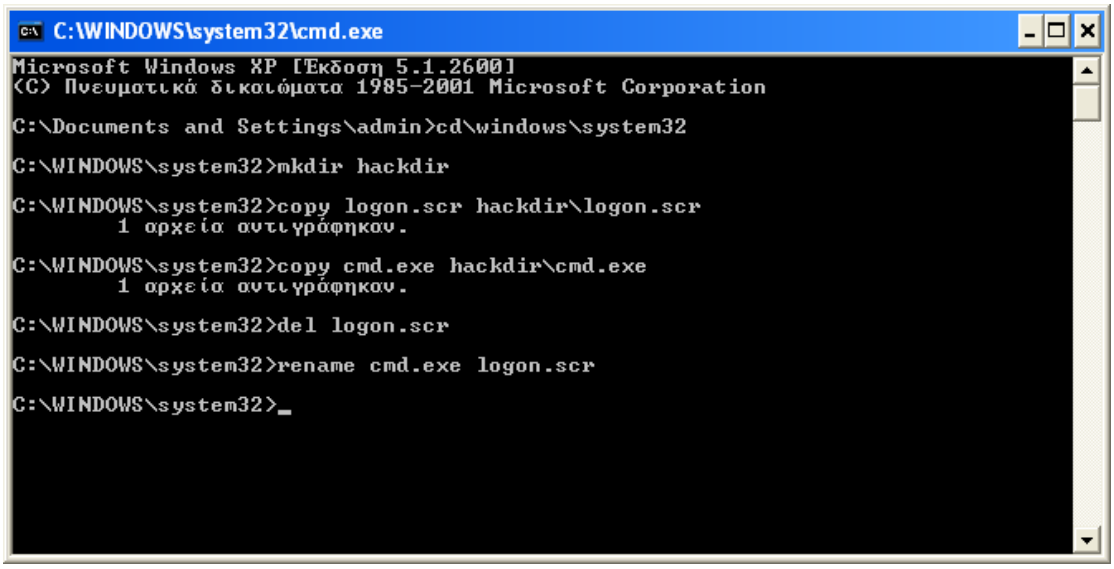
Γράφουμε τις εξής εντολές:

```
cd\windows\system32
mkdir hackdir
copy logon.scr hackdir\logon.scr
copy cmd.exe hackdir\cmd.exe
del logon.scr
rename cmd.exe logon.scr
exit
```

Αυτό που μόλις κάναμε είναι:

- Μπήκαμε στον φάκελο system32 των windows.
- Δημιουργήσαμε ένα νέο φάκελο με το όνομα hackdir.
- Αντιγράψαμε το αρχείο logon.scr μέσα στον φάκελο hackdir.
- Αντιγράψαμε το αρχείο cmd.exe στον φάκελο hackdir.
- Σβήσαμε το αρχείο logon.scr από το system32
- Κάναμε μετονομασία το αρχείο cmd.exe σε logon.scr.
- Κλείσαμε το παράθυρο του DOS.

Εικόνα 91: αρχεία cmd.exe και logon.scr



Εικόνα 92: εντολές στο cmd

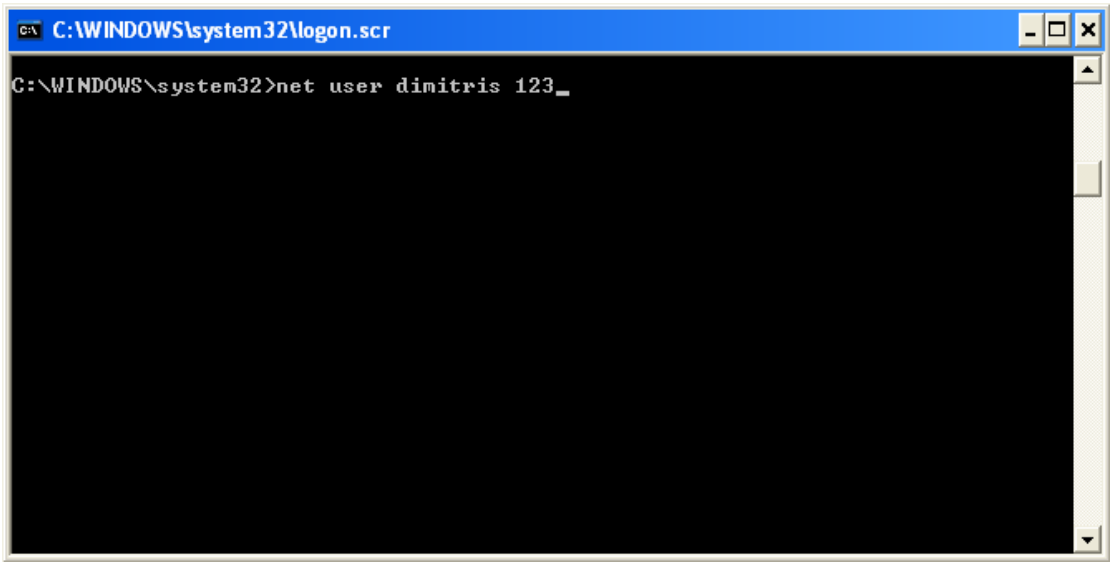
Αποτέλεσμα αυτών των εντολών είναι να αντικαταστήσουμε το default screensaver των Windows με το cmd.exe. Στην επόμενη εκκίνηση του υπολογιστή, στην οθόνη επιλογής χρήστη, θα περιμένουμε μέχρι να εμφανιστεί το Screensaver (περίπου 15 λεπτά), που δεν θα είναι άλλο από μια γραμμή εντολών του DOS, χωρίς καμιά απολύτως προστασία. Αφού ανοίξει το παράθυρο του DOS πληκτρολογούμε την παρακάτω εντολή:

net user <όνομα λογαριασμού Administrator> <νέο κωδικό>

Αν για παράδειγμα το όνομα του λογαριασμού του Admin είναι “Dimitris” και σαν κωδικό θέλουμε το “123” τότε γράφουμε:

net user Dimitris 123

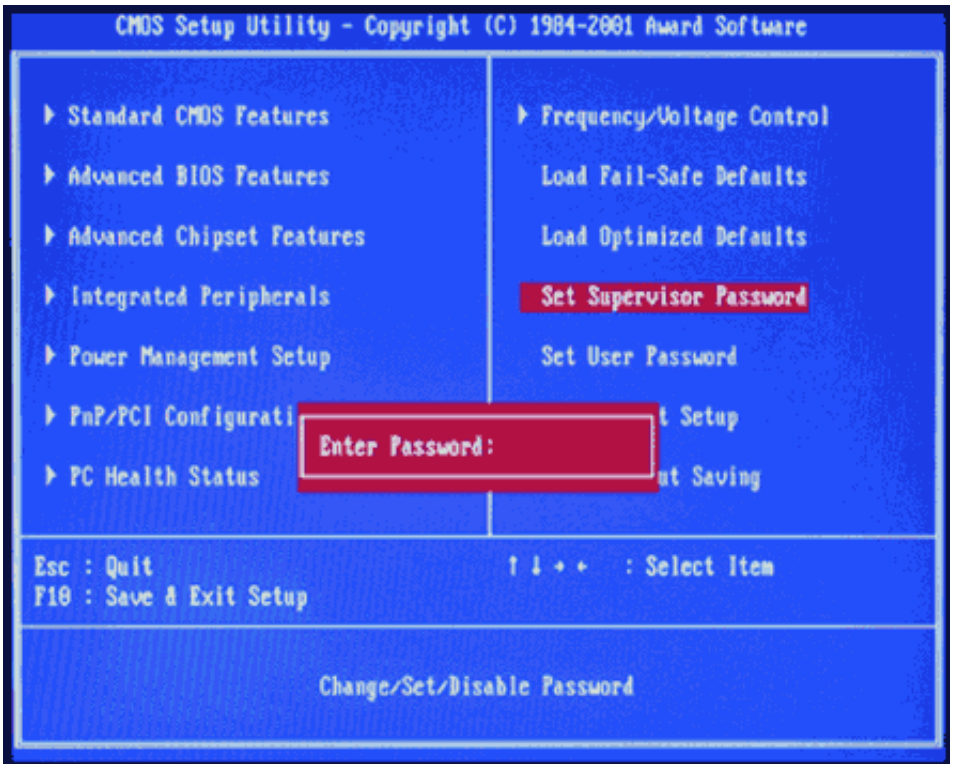
Μόλις αλλάξαμε τον κωδικό του Administrator από οτιδήποτε ήταν σε 123.



Εικόνα 93: default screensaver

5.3 Bios password crack

Οι ρυθμίσεις του Bios που χρησιμοποιούνται για τη λειτουργία του PC πρέπει να αποθηκεύονται σε μια ειδική μνήμη, ώστε να διατηρούνται ακόμα και όταν η συσκευή είναι απενεργοποιημένη. Αυτό είναι αντίθετο με τη μνήμη του συστήματος, η οποία εκκαθαρίζεται κάθε φορά που κλείνει το PC. Ένας ειδικός τύπος μνήμης, που ονομάζεται CMOS μνήμη, χρησιμοποιείται για την αποθήκευση των πληροφοριών αυτών. Η μνήμη CMOS περιέχει πολλές πληροφορίες, όπως ο χρόνος του συστήματος (άμεση πρόσβαση στο ρολόι πραγματικού χρόνου) και η ενημέρωση του Bios. Τι γίνεται όμως σε περίπτωση που κλειδώσουμε το Bios και έχουμε ξεχάσει τον κωδικό?

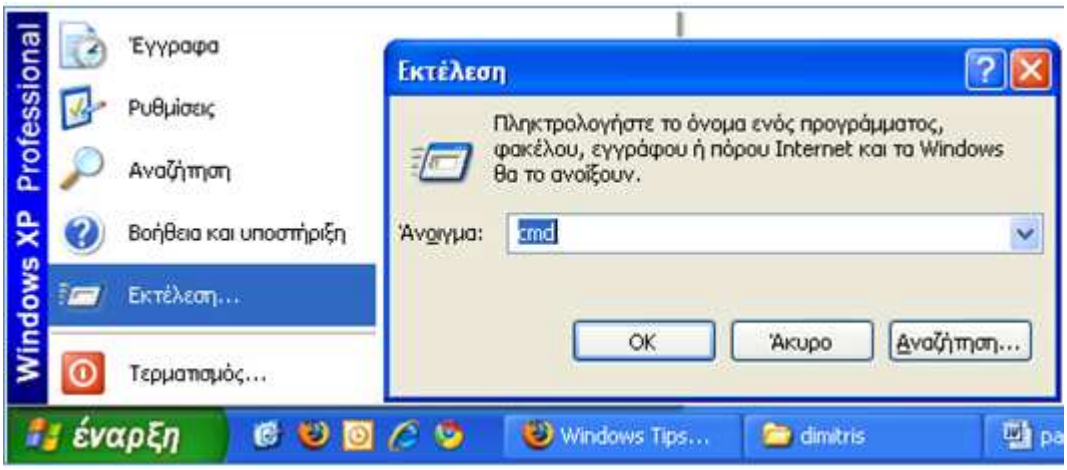


Εικόνα 94: Bios password

Αρκεί να έχουμε πρόσβαση σε λογαριασμό του υπολογιστή για να σβήσουμε την μνήμη CMOS και μαζί τον κωδικό για το Bios.

Αρχικά ανοίγουμε ένα παράθυρο cmd.

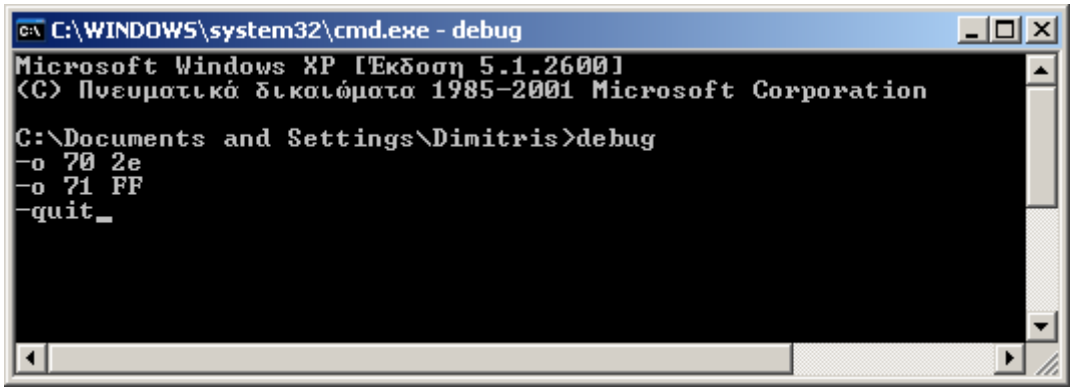
Πατάμε έναρξη →εκτέλεση και πληκτρολογούμε cmd.



Εικόνα 95:ανοίγουμε ένα command prompt

Αφού ανοίξει το command prompt πληκτολογούμε τις παρακάτω εντολές:

```
debug
-o 70 2E
-o 71 FF
-quit
```



Εικόνα 96: command prompt εντολές για σβήσιμο cmos memory

Αφού εκτελέσουμε τις εντολές κλείνουμε το command prompt και κάνουμε επανεκκίνηση τον υπολογιστή. Οι ρυθμίσεις που ήταν αποθηκευμένες στην CMOS μνήμη έχουν χαθεί, μαζί και ο κωδικός για το Bios.

Ας εξηγήσουμε όμως τις εντολές που μόλις εκτελέσαμε. Σε αυτή την μέθοδο χρησιμοποιούμε το debug εργαλείο του MS DOS. Η παρουσία του χαρακτήρα “o” στην αρχή των εντολών οδηγεί σε τιμές εισόδου εξόδου. Οι αριθμοί 70 και 71 είναι οι πόρτες που χρησιμοποιούνται για την είσοδο στην μνήμη CMOS. Με την τιμή FF ενημερώνουμε την CMOS ότι έχει άκυρο αποτέλεσμα και έτσι θα επαναφερθεί στις αρχικές της ρυθμίσεις, χωρίς κωδικό για το Bios.

Κεφάλαιο 6 Phishing

Όπως το ίδιο το όνομά του υπονοεί, παραλλαγή του αγγλικού «fishing» (ψάρεμα), το Phishing αναφέρεται στην προσπάθεια απόσπασης προσωπικών στοιχείων, οικονομικού συνήθως χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες, χρησιμοποιώντας ως δόλωμα κάποιο ψεύτικο πρόσχημα.

Το Phishing επιχειρείται συνήθως με τη αποστολή κάποιου spam e-mail, το οποίο ισχυρίζεται –ψευδώς- ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά θα χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση μη εξουσιοδοτημένων/παράνομων οικονομικών συναλλαγών.

Τα e-mail αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα, κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, και τον οδηγούν μέσω συνδέσμων σε πλαστά web sites, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών. Σε κάποιες περιπτώσεις η αντιγραφή είναι τόσο καλή που και ο ίδιος ο internet browser «ξεγελιέται» και δείχνει στην γραμμή θέματος την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας.

Σε μία προσπάθεια να μειώσουν τον χρόνο αντίδρασης του ανυποψίαστου παραλήπτη, ορισμένα μηνύματα απειλούν ότι εάν δεν προβεί στις απαιτούμενες ενέργειες (ενημέρωση, επαλήθευση στοιχείων) εντός του υποδεικνυόμενου -σύντομου- χρονικού διαστήματος, ο λογαριασμός του θα μπλοκαριστεί και δεν θα μπορεί να πραγματοποιήσει περαιτέρω συναλλαγές. Σκοπός τους είναι να εξαναγκάσουν τον παραλήπτη να αποκαλύψει τις πληροφορίες που του ζητείται χωρίς καν να προλάβει να εξετάσει την γνησιότητα του μηνύματος.
Χρειάζεται ιδιαίτερη προσοχή ώστε ο παραλήπτης ενός τέτοιου μηνύματος να αποφύγει την εξαπάτηση μέσω Phishing. Τα e-mail που αποστέλλονται μοιάζουν αρκετά επίσημα και οι πλαστές σελίδες είναι τις περισσότερες φορές πανομοιότυπες με τις πραγματικές, αφού δημιουργούνται με αντιγραφή του HTML κώδικά τους.

6.1 Ενδείξεις πως ένα ηλεκτρονικό μήνυμα είναι πιθανόν πλαστό

- Ως spam μηνύματα, χρησιμοποιούν συνήθως γενικές προσφωνήσεις, όπως "Αγαπητέ πελάτη", αντί για το πραγματικό όνομα του παραλήπτη.
- Η πλειοψηφία των Phishing μηνυμάτων επικαλείται κάποιο δήθεν πρόβλημα ή κάποια "μοναδική ευκαιρία" και, χρησιμοποιώντας φρασεολογία που δημιουργεί την αίσθηση του επείγοντος, ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.
- Συνήθως ζητούν την παραχώρηση απορρήτων προσωπικών στοιχείων οικονομικού χαρακτήρα που αφορούν τραπεζικούς λογαριασμούς και

πιστωτικές κάρτες, όπως το Όνομα Χρήστη (username) και τον Κωδικό Πρόσβασης (password).

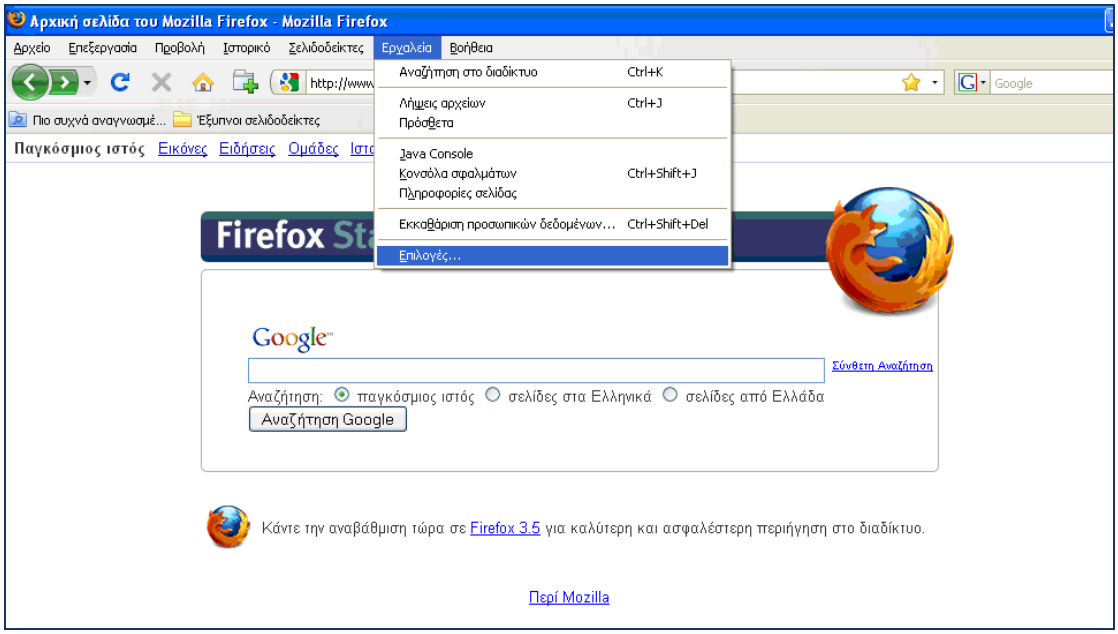
6.2 Τρόποι προφύλαξης από το Phishing

- Να είστε γενικά καχύποπτοι και να μην απαντάτε σε μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν να αποκαλύψετε αξιοποιήσιμα προσωπικά στοιχεία οικονομικού χαρακτήρα. Οι αξιόπιστες εταιρείες δεν συνηθίζουν να ζητούν από τους πελάτες τους να ενημερώσουν ή να επαληθεύσουν τέτοια απόρρητα στοιχεία με ένα απλό email.
- Ακόμη και σε περιπτώσεις που όλα δείχνουν ότι το μήνυμα είναι γνήσιο, είναι προτιμότερο να επικοινωνήσετε με την εταιρία που παρουσιάζεται ως αποστολέας, για να επιβεβαιώσετε ότι πράγματι αυτή σας έστειλε το μήνυμα και ότι δεν πρόκειται για περίπτωση απάτης.
- Φροντίστε, όμως, να επικοινωνήσετε με την εταιρεία αυτή με τον τρόπο που χρησιμοποιείτε συνήθως, και όχι σύμφωνα με τις οδηγίες που περιέχει το email ή απαντώντας σε αυτό.
- Πριν προβείτε στην παραχώρηση ευαίσθητων προσωπικών πληροφοριών μέσω του διαδικτύου προσέξτε την ηλεκτρονική διεύθυνση στην οποία βρίσκεστε. Αντί για το απλό «http://», θα πρέπει να αρχίζει με «https://». Έτσι διασφαλίζετε ότι χρησιμοποιείτε ασφαλή σύνδεση web (http secure).
- Γενικότερα, αγνοείτε ηλεκτρονικά μηνύματα που λαμβάνετε από άγνωστες πηγές και αποφεύγετε να συμπληρώνετε ηλεκτρονικές φόρμες που παραλαμβάνετε μέσω ηλεκτρονικού ταχυδρομείου.
- Ελέγχετε συχνά τους online λογαριασμούς σας, εξετάζοντας προσεκτικά τόσο την συνολική κίνησή τους όσο και κάθε συναλλαγή ξεχωριστά, ώστε να είστε βέβαιοι ότι εγκρίνετε όλα τα ποσά που έχει χρεωθεί.
- Χρησιμοποιείτε πάντα λογισμικό προστασίας από ιούς (antivirus). Παρόλο που τα antivirus δεν μπορούν να σας αποτρέψουν να ανοίξετε ένα πλαστό ηλεκτρονικό μήνυμα, μπορούν εντούτοις να σας προστατεύσουν από ιούς ή λογισμικά υποκλοπής (spyware) που θα προέλθουν από τέτοιες ενέργειες. Πολλά Phishing μηνύματα οδηγούν σε διαδικτυακές τοποθεσίες που εγκαθιστούν στον υπολογιστή σας spywares τα οποία συνεχίζουν να καταγράφουν κάθε πληροφορία που εισάγετε -πιθανότατα και αριθμούς λογαριασμών και πιστωτικών καρτών, και κωδικούς πρόσβασης- για πολύ καιρό μετά την αποχώρηση σας από τον συγκεκριμένο διαδικτυακό τόπο, ενώ μπορεί να περιέχει ακόμη και κάποιον ιό.
- Εγκαταστήστε ψηφιακό φίλτρο που μπλοκάρει τα spam emails (antispam).

6.3 Firefox phishing protection

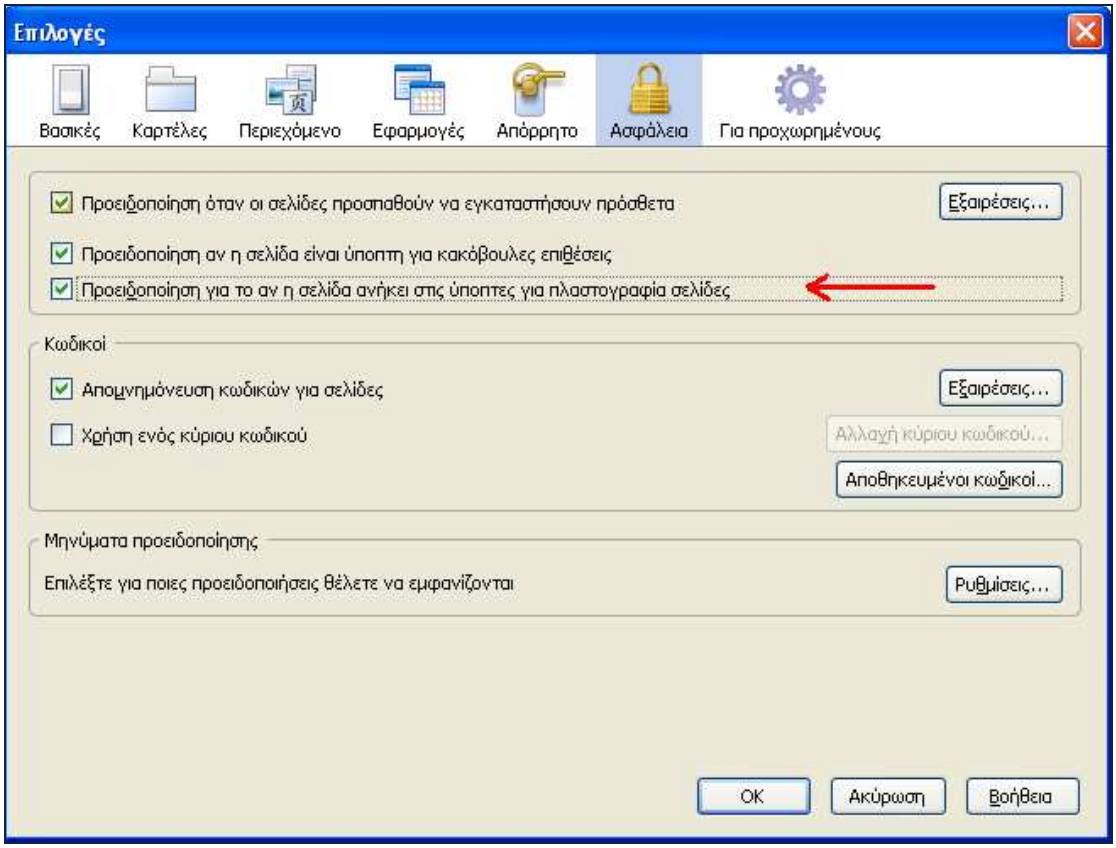
Ο Mozilla Firefox 3 και οι επόμενες εκδόσεις του, παρέχουν ενσωματωμένη προστασία phishing ώστε να βοηθάει την ασφάλεια μας σε απευθείας σύνδεση. Το χαρακτηριστικό αυτό μας προειδοποιεί όταν μια σελίδα που επισκεπτόμαστε είναι σελίδα phishing.

Η επιλογή ενεργοποιείται στον Firefox αν πάμε *Εργαλεία* → *Επιλογές*



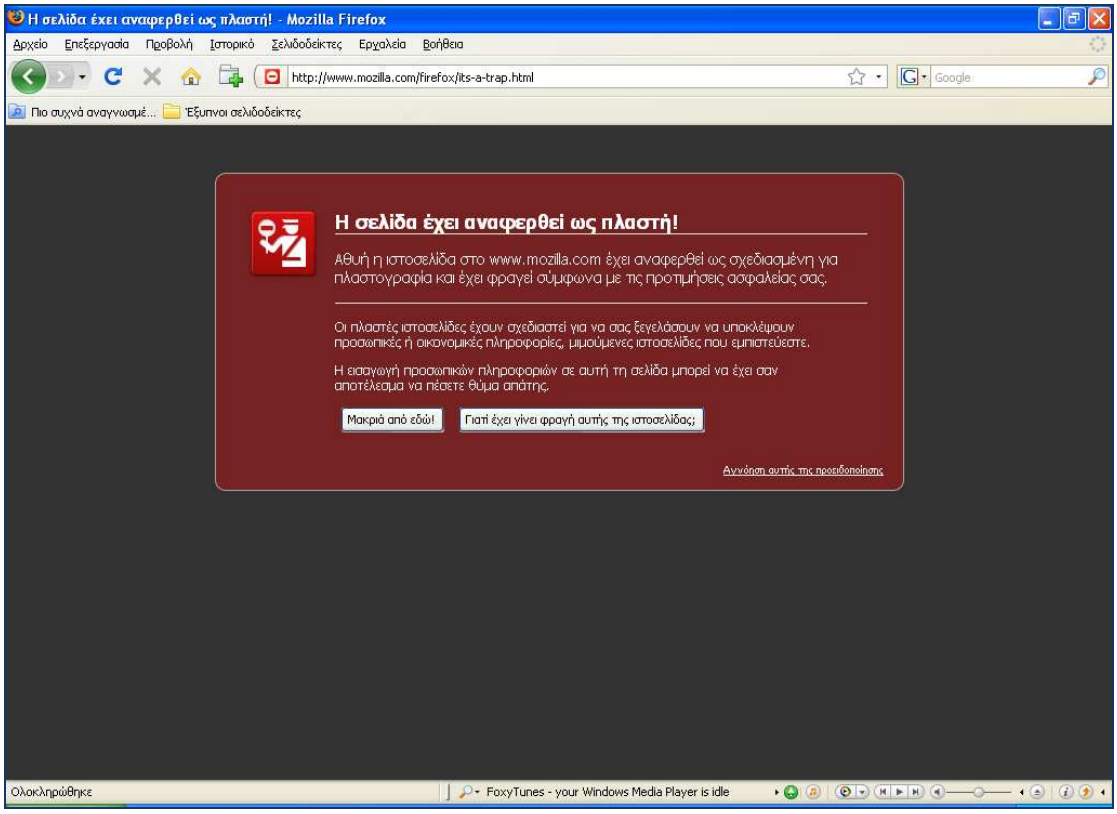
Εικόνα 97: Firefox επιλογές

Στην καρτέλα ασφάλεια τικάρουμε την επιλογή *Προειδοποίηση για το αν η σελίδα ανήκει στις ύποπτες για πλαστογραφία σελίδες* και έτσι έχουμε ενεργοποιήσει το φίλτρο ηλεκτρονικού ψαρέματος του Firefox.



Εικόνα 98: Firefox επιλογές ασφαλείας

Τώρα αν προσπαθήσουμε να μπούμε σε μια πλαστή σελίδα ο Firefox μας αποτρέπει. Θα δούμε την παρακάτω εικόνα.



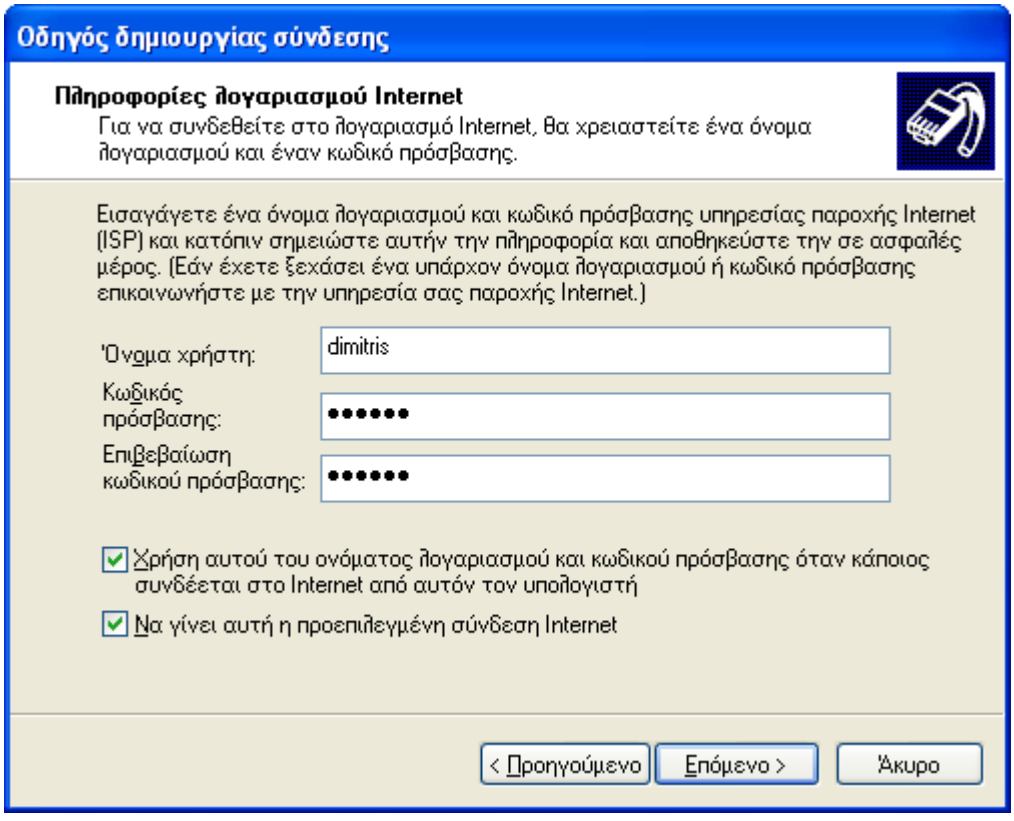
Εικόνα 99: Firefox Phishing protection

Κεφάλαιο 7 Χρήση προγραμμάτων ανάκτησης κωδικών

7.1 Πίσω από τα αστεράκια

Σε φόρμες των windows, όπου υπάρχουν πεδία με κωδικούς, τα πεδία αυτά είναι καλυμμένα με αστερίσκους (‘*’) και απαγορεύεται από το λειτουργικό σύστημα η αντιγραφή των περιεχομένων τους. Όσοι έχουν ασχοληθεί με τον προγραμματισμό, ήδη θα γνωρίζουν ότι τα πεδία αυτά είναι συνηθισμένα πεδία κειμένου, στα οποία ο τύπος, από normal , text ή plain (η ονομασία αλλάζει ανάλογα με την γλώσσα προγραμματισμού) έχει μετατραπεί σε password. Σε αυτές τις περιπτώσεις η registry δεν μας βοηθάει και πολύ αφού οι πληροφορίες των λογαριασμών δεν αποθηκεύονται συνήθως σε αυτήν, αλλά σε ειδικά αρχεία που βρίσκονται ‘‘θαμμένα’’ σε διάφορα μέρη του σκληρού δίσκου. Τότε χρειαζόμαστε άλλου τύπου προγράμματα στην εργαλειοθήκη μας, αυτά που αποκαλύπτουν και συλλέγουν τα περιεχόμενα των πεδίων.

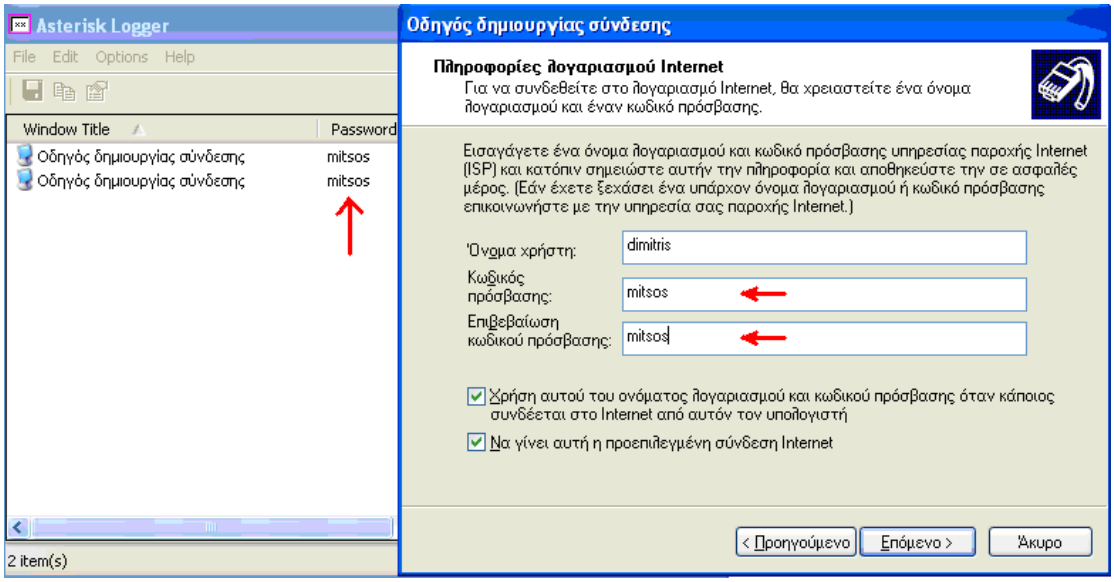
Το Asterisk Logger [6] είναι ένα μικρό και βολικό εργαλείο τέτοιου τύπου. Ανιχνεύει και συλλέγει αυτόματα από κάθε παράθυρο που ανοίγετε και κάθε εφαρμογή που εκτελείται, τα απαραίτητα πεδία.



Εικόνα 100: πεδία τύπου password

[6] http://www.nirsoft.net/utils/astlog.html

Στην παραπάνω εικόνα παρατηρούμε ότι δεν είναι ορατό το περιεχόμενο των πεδίων που είναι τύπου password. Αν όμως εκτελέσουμε το Asterisk Logger παρατηρούμε ότι στη θέση που πριν βρίσκονταν τα αστεράκια τώρα φαίνεται ο κωδικός. Οι κωδικοί επίσης εμφανίζονται και στο παράθυρο του προγράμματος.



Εικόνα 101: Asterisk Logger

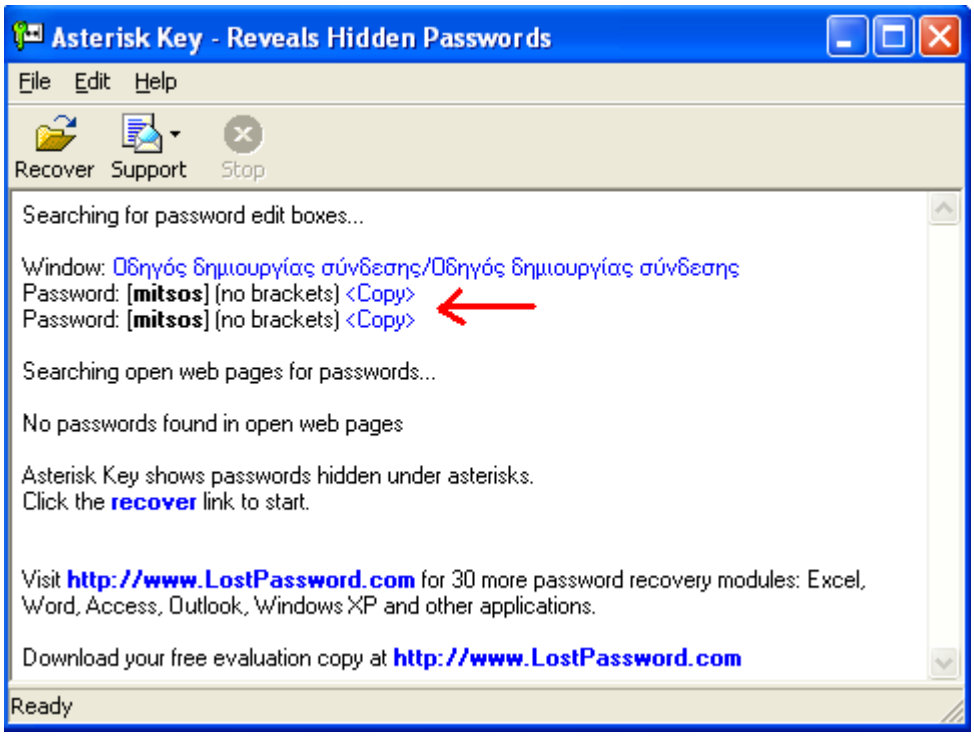
Όπως βλέπουμε το Asterisk Logger εν δράσει αποκαλύπτει και καταγράφει τον κωδικό της σύνδεσης στο Internet. Αφού εκτελέσουμε το πρόγραμμα, αυτό ανιχνεύει αυτόματα και αποκαλύπτει τα πεδία password καταγράφοντας μεθοδικά όλους τους κρυμμένους κωδικούς που περνούν από την οθόνη του υπολογιστή μας.

Ένα εξίσου καλό εργαλείο το οποίο λειτουργεί με παρόμοιο τρόπο με το Asterisk Logger είναι το Asterisk Key [7] το οποίο επίσης αναγνωρίζει και εμφανίζει τους κωδικούς που περνούν από την οθόνη του υπολογιστή μας.

[7] http://www.lostpassword.com/asterisk.htm

Εικόνα 102: Asterisk Key

Το Asterisk Key αναγνωρίζει και παρουσιάζει στο παράθυρο του, τους κωδικούς που κρύβονται κάτω από τα πεδία με τους αστερίσκους. Δεν έχουμε παρά να πατήσουμε το κουμπί recover και το πρόγραμμα βρίσκει από μόνο του τα παράθυρα στα οποία υπάρχουν πεδία τύπου password και τα εμφανίζει στην κεντρική του οθόνη.



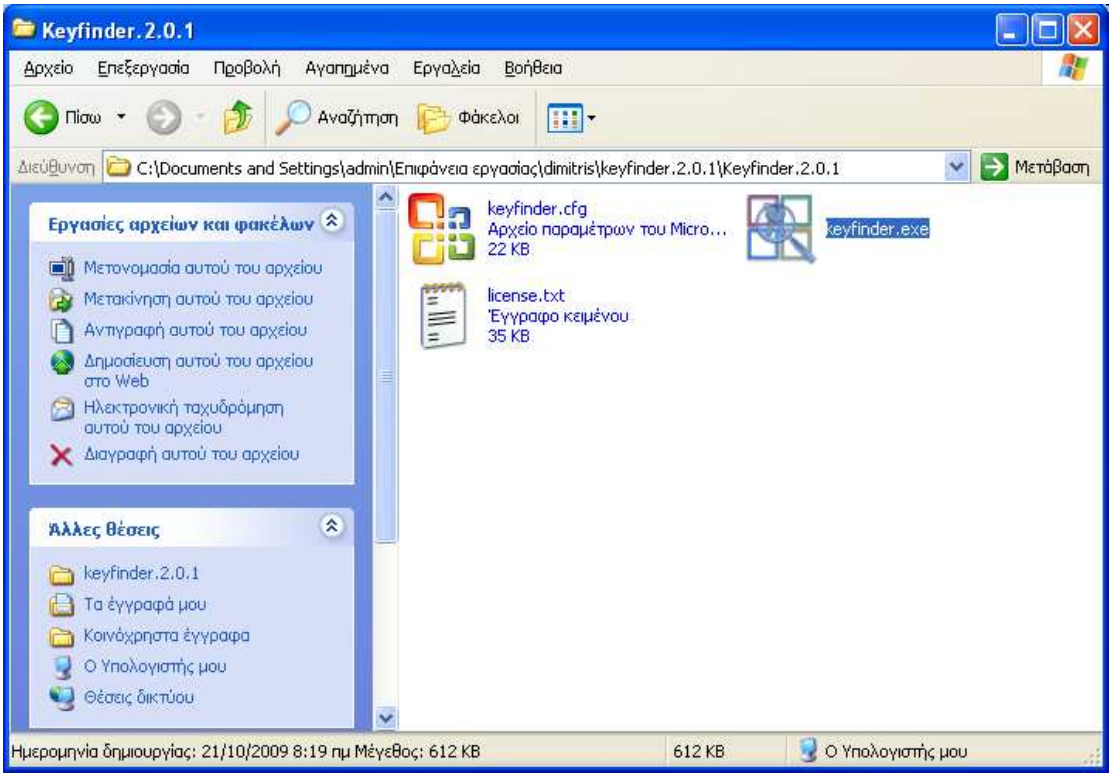
Εικόνα 103: Asterisk Key recover

Στη συγκεκριμένη περίπτωση από ότι βλέπουμε στην παραπάνω εικόνα το πρόγραμμα εντόπισε ένα πεδίο τύπου password. Το πεδίο αυτό βρίσκεται στο παράθυρο *Οδηγός δημιουργίας σύνδεσης* και ο κωδικός που βρίσκεται κάτω από τα αστεράκια είναι *mitsos.*

7.2 Keyfinder

Το Magical Jelly Bean Keyfinder [8] είναι ένα δωρεάν λογισμικό ανοικτού κώδικα του οποίου η χρησιμότητα είναι να ανακτά το κλειδί προϊόντος (cd key) που χρησιμοποιείται για την εγκατάσταση των Windows, από το μητρώο μας. Μας επιτρέπει να εκτυπώσουμε ή να αποθηκεύσουμε τα κλειδιά μας για φύλαξη. Λειτουργεί με Windows 95, 98, ME, 2000, XP, Vista, 7, Server 2003, Server 2008, Office XP, Office 2003 και Office 2007. Έχει επίσης ένα ενημερωμένο αρχείο διαμόρφωσης που ανακτά κλειδιά προϊόντος για πολλές άλλες εφαρμογές. Ένα ακόμα χαρακτηριστικό είναι η δυνατότητα να ανακτήσει τα κλειδιά προϊόντος από unbootable εγκαταστάσεις των Windows.

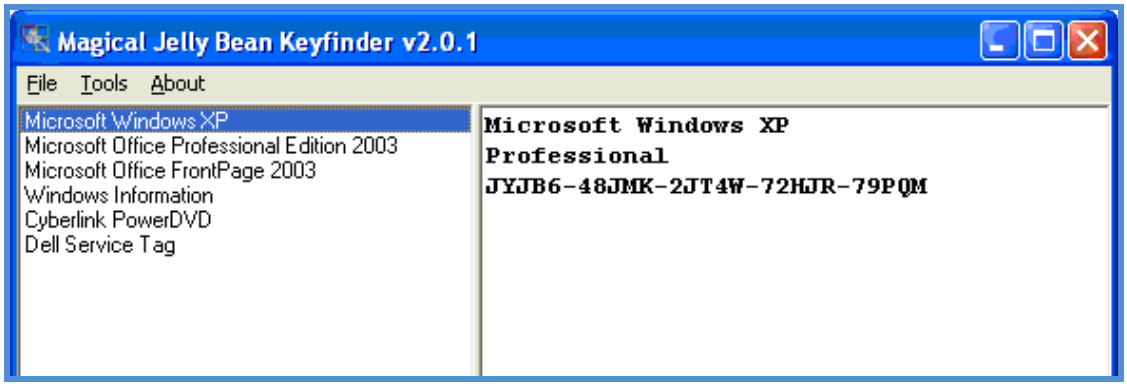
Η λειτουργία του προγράμματος είναι αρκετά απλή και αυτοματοποιημένη. Το μόνο που χρειάζεται να κάνουμε είναι να τρέξουμε το εκτελέσιμο αρχείο keyfinder.exe το οποίο βρίσκεται στο φάκελο του keyfinder.



Εικόνα 104: φάκελος keyfinder

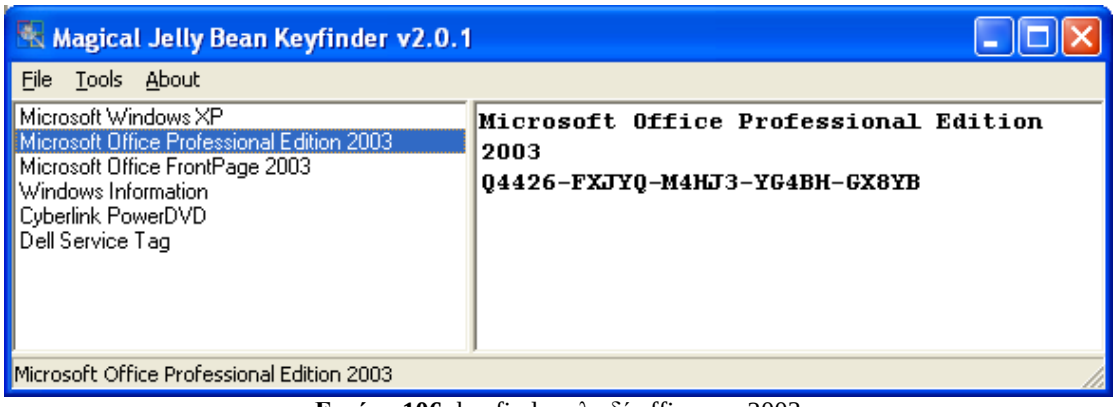
[8] http://www.magicaljellybean.com/keyfinder/

Αφού εκτελέσουμε το αρχείο θα εμφανιστεί το παρακάτω παράθυρο.

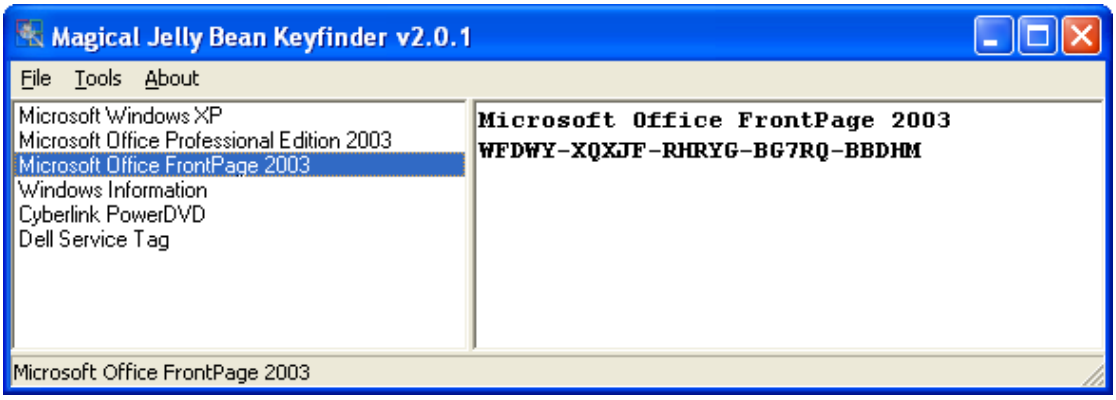


Εικόνα 105: keyfinder κλειδί Windows XP

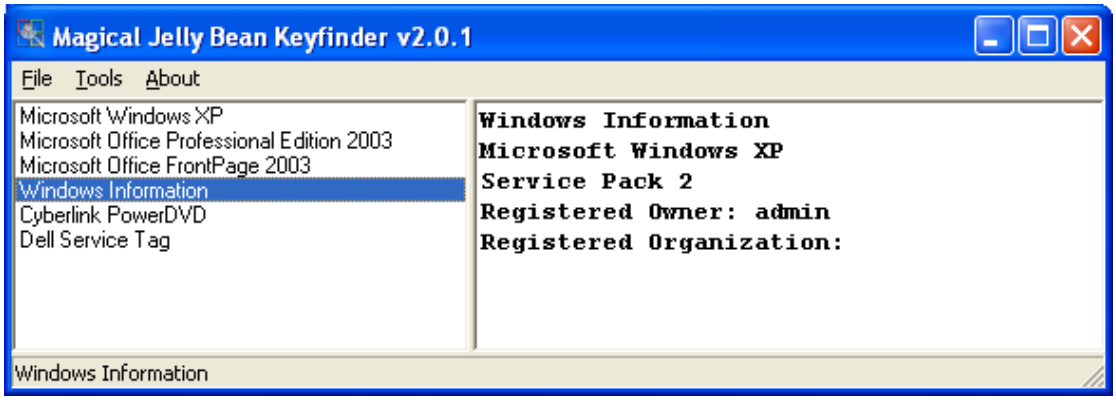
Όπως βλέπουμε, στην αριστερή στήλη το πρόγραμμα βρήκε κλειδιά για Windows Xp, office, FrontPage, Windows information, power DVD μέσα στο μητρώο του υπολογιστή μας. Τα κλειδιά αυτά φαίνονται στη δεξιά στήλη.



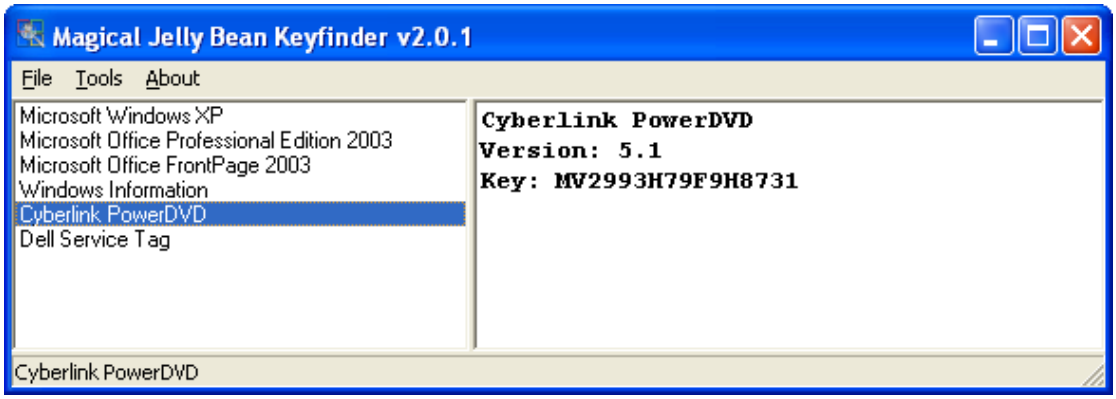
Εικόνα 106: keyfinder κλειδί office pro 2003



Εικόνα 107: keyfinder κλειδί FrontPage 2003



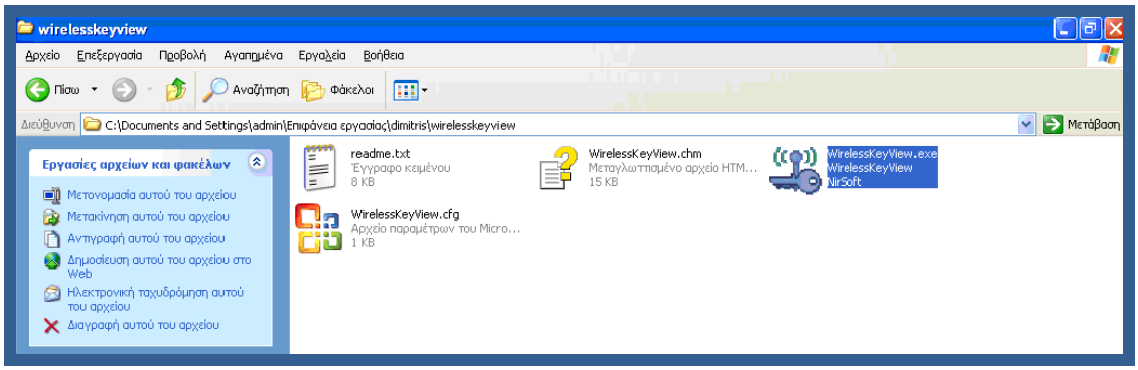
Εικόνα 108: keyfinder πληροφορίες σχετικά με τα Windows



Εικόνα 109: keyfinder κλειδί power DVD

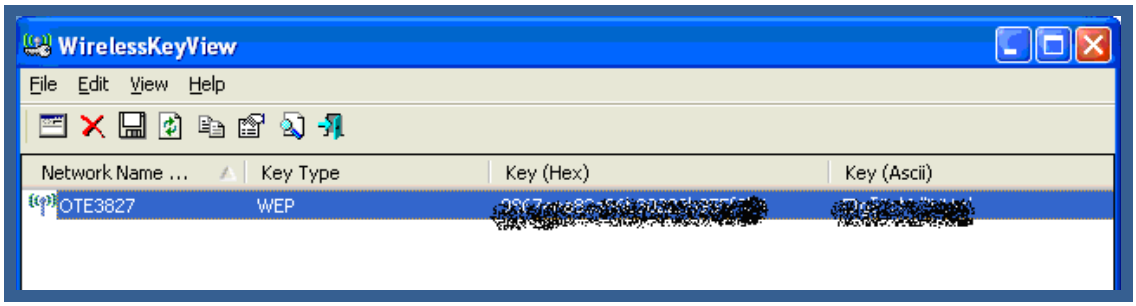
7.3 Ασύρματα δίκτυα

Όταν συνδέσουμε τον υπολογιστή μας σε κάποιο ασύρματο δίκτυο, συχνά χρησιμοποιούμε πρωτόκολλα σύνδεσης που απαιτούν κάποιο κωδικό. Έτσι εξασφαλίζεται ότι μόνο αδειοδοτημένοι χρήστες θα αποκτήσουν πρόσβαση στο ασύρματο αυτό δίκτυο. Τα κλειδιά του ασύρματου δικτύου διατηρούνται στον υπολογιστή, κρυμμένα σε διάφορα αρχεία από το Wireless Zero Configuration των Windows XP και το WLAN AutoConfig των Windows Vista. Χρησιμοποιώντας το WirelessKeyView [9] θα μπορέσουμε να εντοπίσουμε τα κλειδιά αυτά, μαζί με τις λοιπές πληροφορίες των ασυρμάτων δικτύων στα οποία ανήκουν, απλώς με την εκτέλεση του προγράμματος. Υποστηρίζεται αναγνώριση των κλειδιών που χρησιμοποιούνται τόσο από τον WEP όσο και από τον WPA αλγόριθμο.



Εικόνα 110: φάκελος WirelessKeyView

Το WirelessKeyView λειτουργεί αυτόματα. Αρκεί να ανοίξουμε το εκτελέσιμο αρχείο για να εντοπιστούν και να εμφανιστούν τα κλειδιά μαζί με τα ασύρματα δίκτυα στα οποία αναφέρονται.



Εικόνα 111: WirelessKeyView αποκάλυψη κωδικών

[9] http://www.nirsoft.net/utils/wireless_key.html

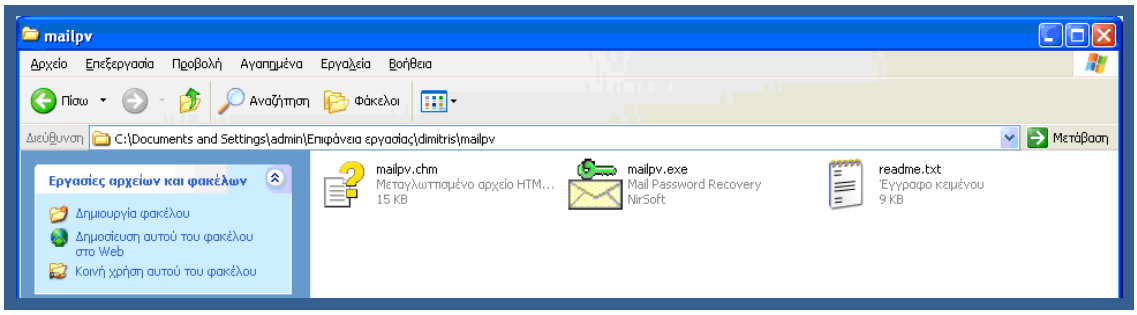
7.4 Κωδικοί δικτυακών προγραμμάτων

7.4.1 e-mail

Τα προγράμματα e-mail και instant messaging διατηρούν, το καθένα σε δικό του τόπο και με δικό του τρόπο, τις πληροφορίες για τους λογαριασμούς που χρησιμοποιούν στο σκληρό δίσκο. Αυτό συμβαίνει στην περίπτωση που έχουμε ενεργοποιήσει την επιλογή Remember password, save password ή Log me in automatically στους λογαριασμούς που δημιουργούμε. Για να επανακτήσουμε λοιπόν, τις πλήρεις πληροφορίες των λογαριασμών, θα πρέπει να χρησιμοποιήσουμε ένα εργαλείο που γνωρίζει τις ιδιοτροπίες κάθε προγράμματος και μπορεί να εντοπίσει που αποθηκεύονται οι κωδικοί.

Ένα τέτοιο εργαλείο για τα προγράμματα e-mail είναι το Mail PassView [10] της Nirsoft. Αν χρησιμοποιούμε Outlook Express, Microsoft Outlook, Netscape Mail, Mozilla Thunderbird, Eudora ή Windows Mail το Mail PassView θα μπορέσει να εντοπίσει τους λογαριασμούς που χρησιμοποιείται. Αν έχετε κλειδώσει τους λογαριασμούς με κάποιο master password τότε η αναζήτηση θα αποτύχει.

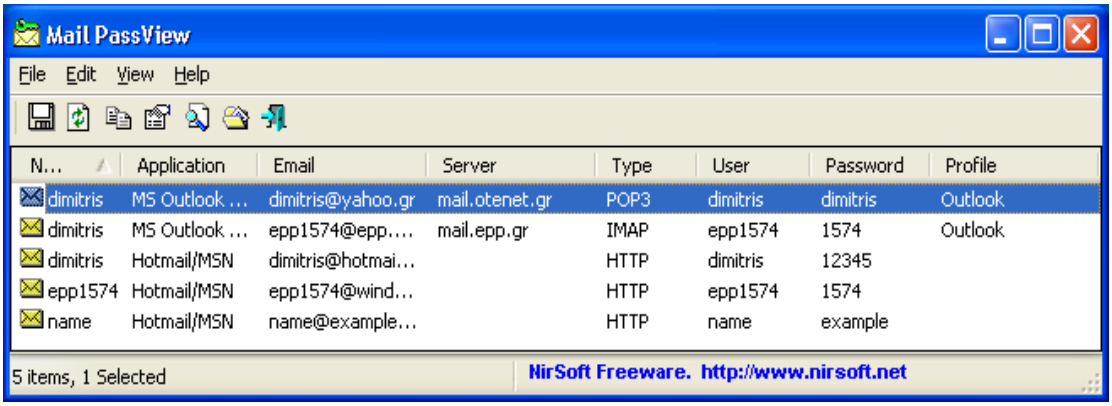
Το Mail PassView υποστηρίζει επίσης και τα βοηθητικά προγράμματα Webmail υπηρεσιών όπως το Gmail, Hotmail, MSN mail, Windows Live mail και το Yahoo mail.



Εικόνα 112: φάκελος mailpv

Η λειτουργία του προγράμματος είναι εξαιρετικά αυτοματοποιημένη, αφού αρκεί να το εκτελέσουμε (mailpv.exe) για να εντοπίσει τα εγκατεστημένα e-mail clients και να περισυλλέξει όλους τους λογαριασμούς και να τους εμφανίσει.

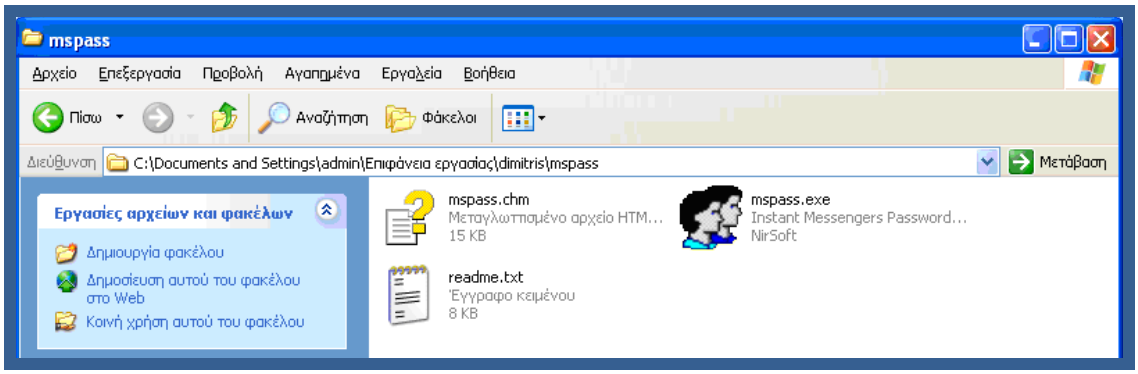
[10] http://www.nirsoft.net/utils/mailpv.html



Εικόνα 113: mailpv αποκάλυψη κωδικών

7.4.2 Instant messaging

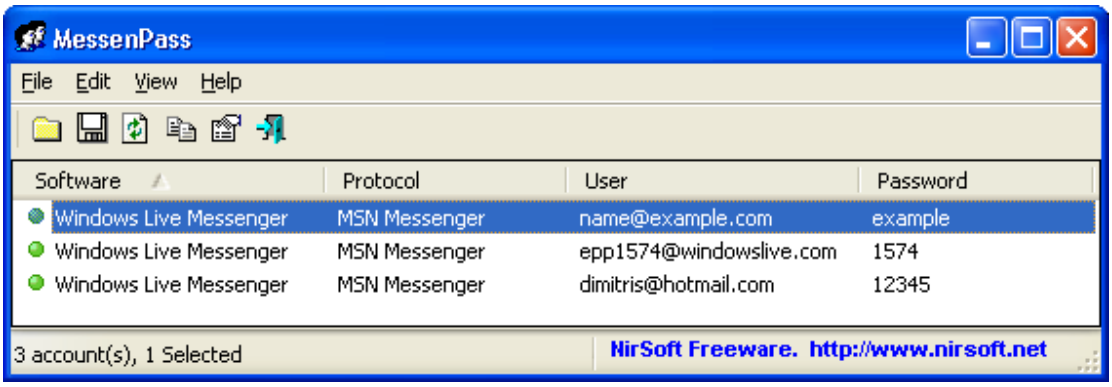
Τώρα για τα προγράμματα που χρησιμοποιούμε για instant messaging η λύση είναι παρόμοια. Μπορούμε να χρησιμοποιήσουμε το MessenPass της ίδιας εταιρίας[11]. Το πρόγραμμα υποστηρίζει τους ακόλουθους instant messaging clients: Google talk, MSN Messenger, Windows Messenger, Windows Live Messenger, Yahoo Messenger και διάφορα αλλά ακόμη. Εκτελώντας το πρόγραμμα θα περισυλλεχθούν όλοι οι κωδικοί που χρησιμοποιούνται από όλα τα προγράμματα instant messaging που έχουμε εγκατεστημένα στον υπολογιστή μας.



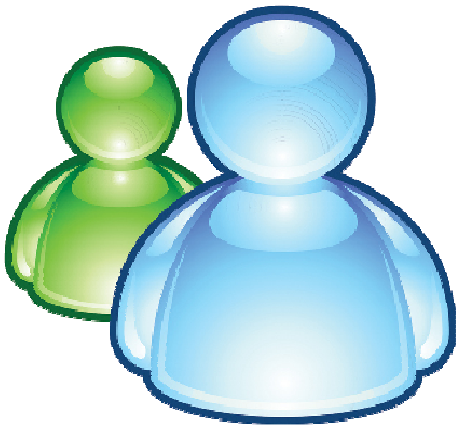
Εικόνα 114: φάκελος mspass

Ανοίγουμε το εκτελέσιμο αρχείο(mspass.exe) και αυτόματα εντοπίζει και μας εμφανίζει τα εγκατεστημένα instant messaging clients με τα username και τα password που έχουν εισέλθει στον συγκεκριμένο υπολογιστή.

[11] http://www.nirsoft.net/utils/mspass.html

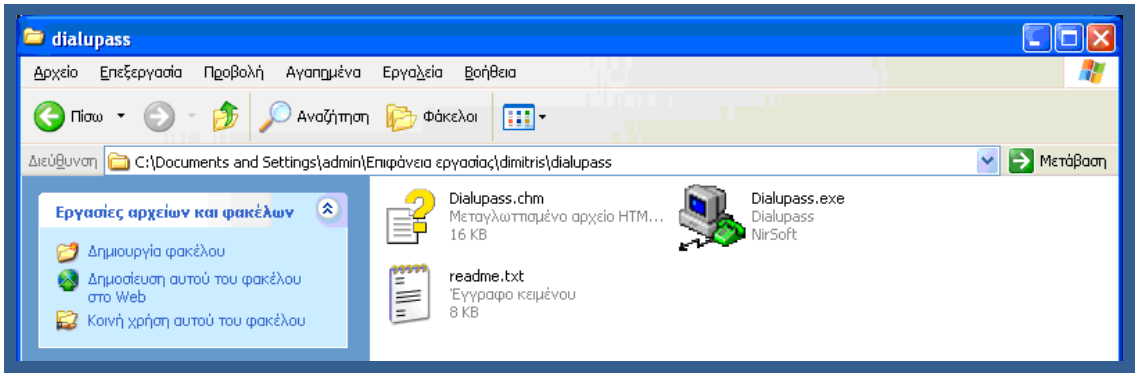


Εικόνα 115: MessenPass αποκάλυψη κωδικών



7.4.3 Ανάκτηση κωδικών σύνδεσης Internet

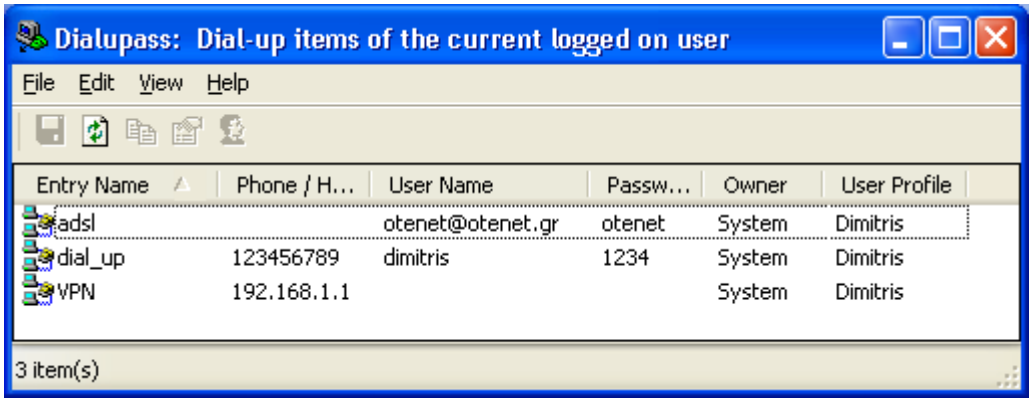
Αν ειδικότερα θέλουμε να ανακτήσουμε τους κωδικούς των dial-up συνδέσεων των windows(στις οποίες κατατάσσονται τόσο οι παλιές PSTN και ISDN dial-up συνδέσεις με modem όσο και οι on-demand ADSL συνδέσεις) θα πρέπει να χρησιμοποιήσουμε το Dialupass- Dialup Password Recovery [12] από την ίδια εταιρία.



Εικόνα 116: φάκελος dialupass

Το Dialupass εξειδικεύεται στην ανάκτηση των κωδικών των συνδέσεων τέτοιου τύπου και άμεσα θα περισυλλέξει και θα εμφανίσει τους κωδικούς μαζί με τις λοιπές συναφείς πληροφορίες που βρίσκονται στο σύστημα μας. Επειδή οι κωδικοί αποθηκεύονται σε μη κρυπτογραφημένη μορφή είναι πολύ απλό και άμεσο θέμα να ανευρεθούν και να εμφανιστούν.

Δεν έχουμε παρά να εκτελέσουμε το Dialupass.exe αρχείο και το πρόγραμμα θα εμφανίσει τις Dialup συνδέσεις που έχουν γίνει από τον συγκεκριμένο υπολογιστή μαζί με τους κωδικούς τους.



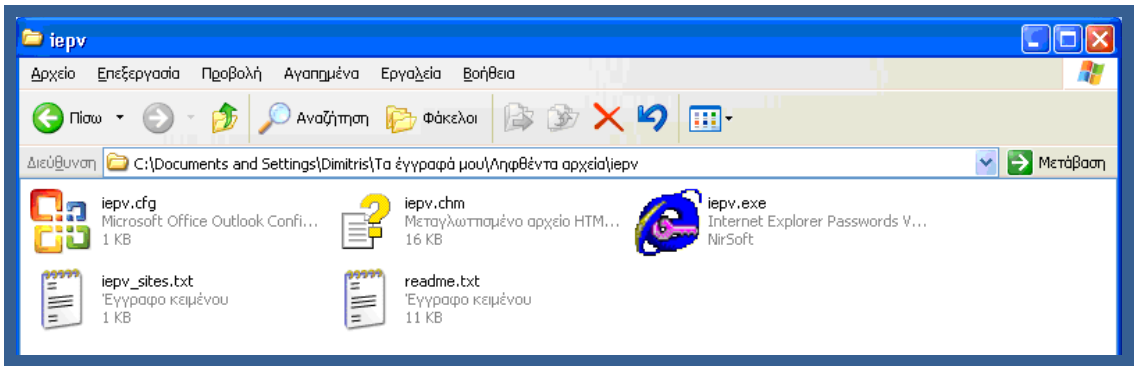
Εικόνα 117: Dialupass αποκάλυψη κωδικών

[12] http://www.nirsoft.net/utils/dialupass.html

7.5 Browser

7.5.1 Internet explorer

Το IE PassView είναι ένα μικρό πρόγραμμα που αποκαλύπτει τους κωδικούς πρόσβασης που αποθηκεύονται από τον Web browser Internet Explorer. Υποστηρίζει όλες τις εκδόσεις του Internet Explorer, από την έκδοση 4.0 και μέχρι 8.0. Για κάθε κωδικό πρόσβασης που αποθηκεύεται από τον Internet Explorer εμφανίζονται οι παρακάτω πληροφορίες: η διεύθυνση στο Web, ο τύπος του κωδικού (αυτόματη καταχώρηση, προστατεύεται με κωδικό πρόσβασης Web Site, ή FTP), τοποθεσία αποθήκευσης καθώς και το όνομα χρήστη / κωδικό πρόσβασης.



Εικόνα 118: φάκελος iepv

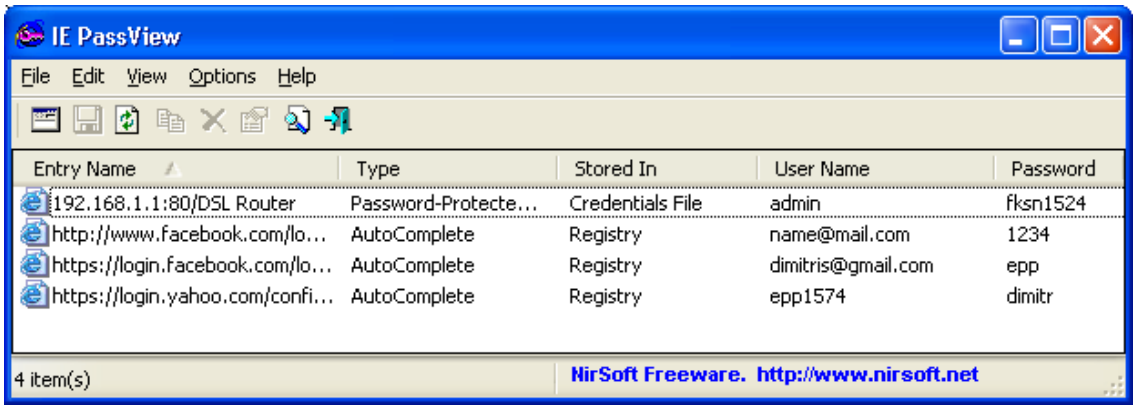
Το IE PassView δεν απαιτεί καμία διαδικασία εγκατάστασης ή πρόσθετα DLLs. Για να αρχίσουμε να το χρησιμοποιούμαι αντιγράφουμε μόνο το εκτελέσιμο αρχείο (iepv.exe) σε όποιο φάκελο θέλουμε και το εκτελούμε. Μετά την εκτέλεση του iepv.exe, το πρόγραμμα σαρώνει όλους τους κωδικούς πρόσβασης του Internet Explorer στο σύστημά μας και τους τοποθετεί στο κύριο παράθυρο του.

Το πρόγραμμα μπορεί να ανακτήσει 3 είδη κωδικών πρόσβασης:

1. Αυτόματη συμπλήρωση κωδικών πρόσβασης. Σε μια ιστοσελίδα που περιέχει φόρμα με το όνομα χρήστη, τον κωδικό και ένα κουμπί πρόσβασης ο Internet Explorer μπορεί να μας ρωτήσει εάν θέλουμε να αποθηκεύσουμε τον κωδικό πρόσβασης, μετά το πάτημα του login. Αν επιλέξουμε να αποθηκεύσουμε τον κωδικό, αυτός αποθηκεύεται ως αυτόματη συμπλήρωση κωδικού πρόσβασης. Μερικά sites (όπως το Yahoo) σκόπιμα απενεργοποιούν τη δυνατότητα αυτόματης καταχώρησης, προκειμένου να αποφευχθεί η κλοπή κωδικού από άλλους χρήστες.

2. HTTP Authentication κωδικών πρόσβασης: Ορισμένες τοποθεσίες Web επιτρέπουν στο χρήστη να εισέλθει μόνο μετά την πληκτρολόγηση του ονόματος χρήστη και κωδικού πρόσβασης σε ένα διαχωρισμένο κουτί διαλόγου. Εάν επιλέξουμε να αποθηκεύσουμε τον κωδικό πρόσβασης σε αυτό το πλαίσιο διαλόγου, ο κωδικός πρόσβασης αποθηκεύετε ως κωδικός HTTP αναγνώρισης.

3. Οι κωδικοί πρόσβασης FTP. Απλά οι κωδικοί πρόσβασης των ftp διευθύνσεων (ftp:// ...)



Εικόνα 119: IE Passview αποκάλυψη κωδικών

Από ότι βλέπουμε στην πρώτη στήλη αναφέρεται το όνομα της σελίδας(π.χ. dsl router, facebook,yahoo), στη δεύτερη ο τύπος του κωδικού που αποθηκεύτηκε, στην επόμενη η τοποθεσία που βρίσκεται ο κωδικός και στις δύο τελευταίες στήλες το όνομα χρήστη και ο κωδικός πρόσβασης.

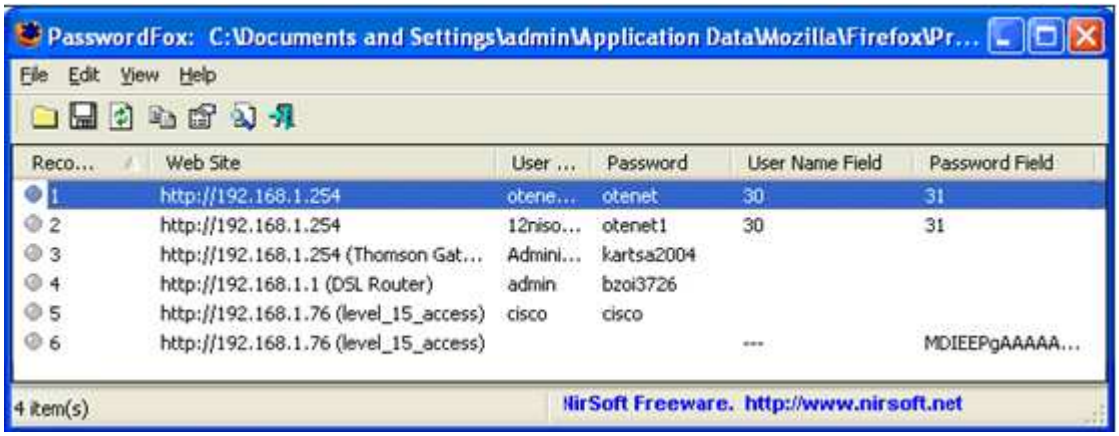
7.5.2 Mozilla Firefox, Google chrome

Με τον ίδιο ακριβώς τρόπο λειτουργούν άλλα δύο μικρά προγραμματάκια της ίδιας εταιρίας. Το ChromePass [13] με το οποίο ανακτούμε τους κωδικούς του browser Google Chrome και το PasswordFox [14] για το Mozilla Firefox.

Εικόνα 120: ChromePass αποκάλυψη κωδικών

[13] http://www.nirsoft.net/utils/chromepass.html
[14] http://www.nirsoft.net/utils/passwordfox.html

Στην παραπάνω εικόνα φαίνονται οι κωδικοί που έχουν αποθηκευτεί στο Google chrome.



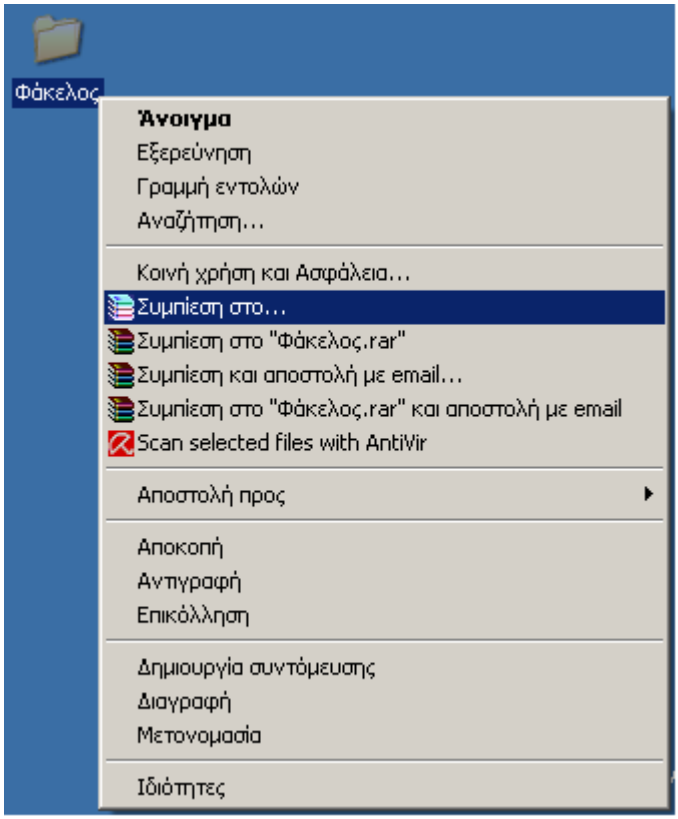
Εικόνα 121: PasswordFox αποκάλυψη κωδικών

Στην παραπάνω εικόνα φαίνονται οι κωδικοί που έχουν αποθηκευτεί στο Mozilla Firefox.

7.6 Rar Password Recovery

Πολλές φορές κάνουμε χρήση κωδικού σε συμπιεσμένα αρχεία, ώστε να τα προφυλάξουμε από τους καχύποπτους χρήστες. Για να δούμε πως πραγματοποιείται η συμπίεση ενός αρχείου με το πρόγραμμα WinRar[15].

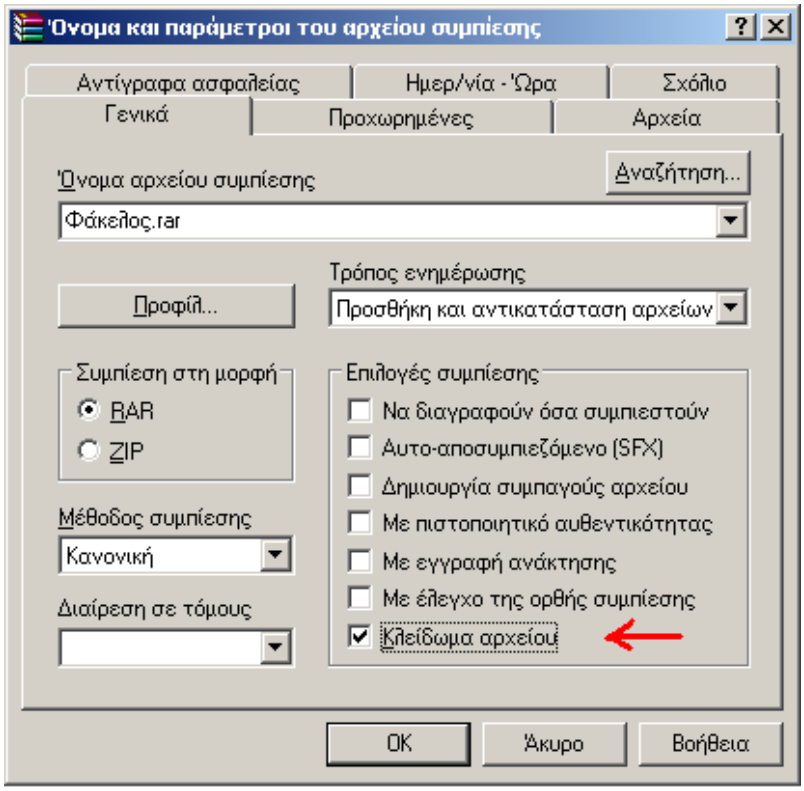
Κάνουμε δεξί κλικ στο φάκελο τον οποίο θέλουμε να συμπιέσουμε και πατάμε συμπίεση στο...



Εικόνα 122: δεξί κλικ και συμπίεση στο

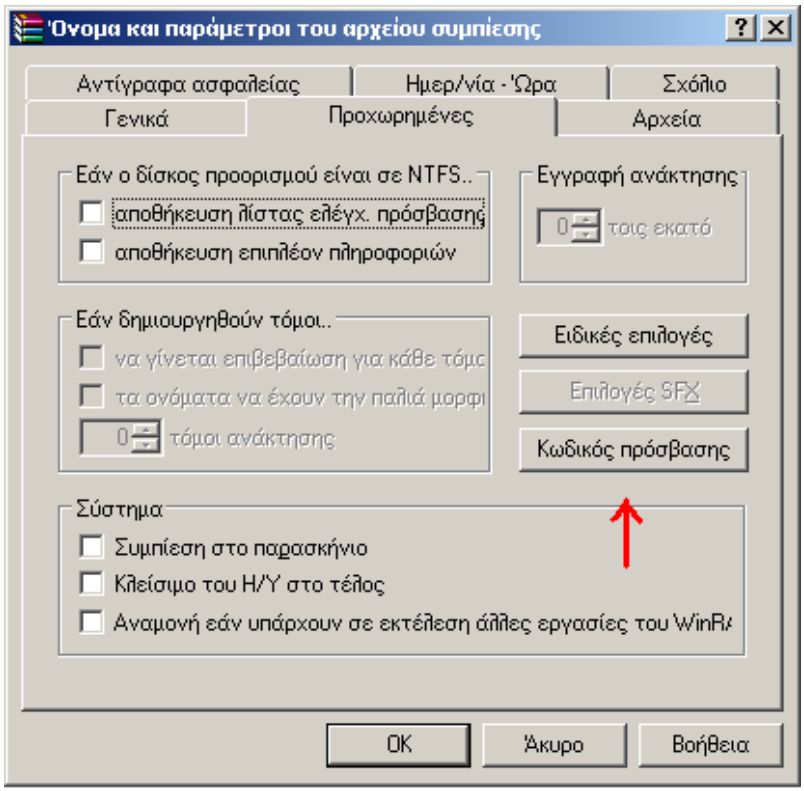
Ανοίγει το ακόλουθο παράθυρο στο οποίο κλικάρουμε την επιλογή κλείδωμα αρχείου στην καρτέλα γενικά.

[15] http://www.rarlab.com/download.htm



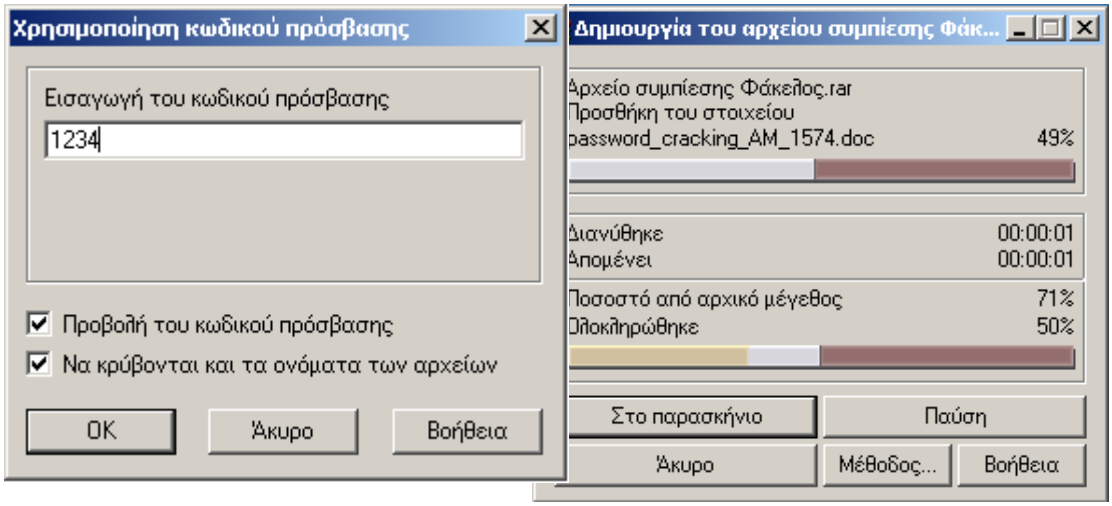
Εικόνα 123: winrar κλείδωμα αρχείου

Στη συνέχεια αλλάζουμε και πατάμε στην καρτέλα προχωρημένες. Εδώ πατάμε το κουτί που λέει κωδικός πρόσβασης όπως φαίνεται παρακάτω.



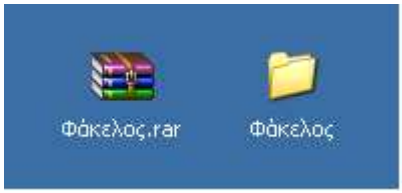
Εικόνα 124: winrar κωδικός πρόσβασης

Θα εμφανιστεί ένα νέο παράθυρο στο οποίο θα βάλουμε τον κωδικό που θέλουμε για να κλειδώσουμε το αρχείο.



Εικόνα 125: winrar συμπίεση αρχείου

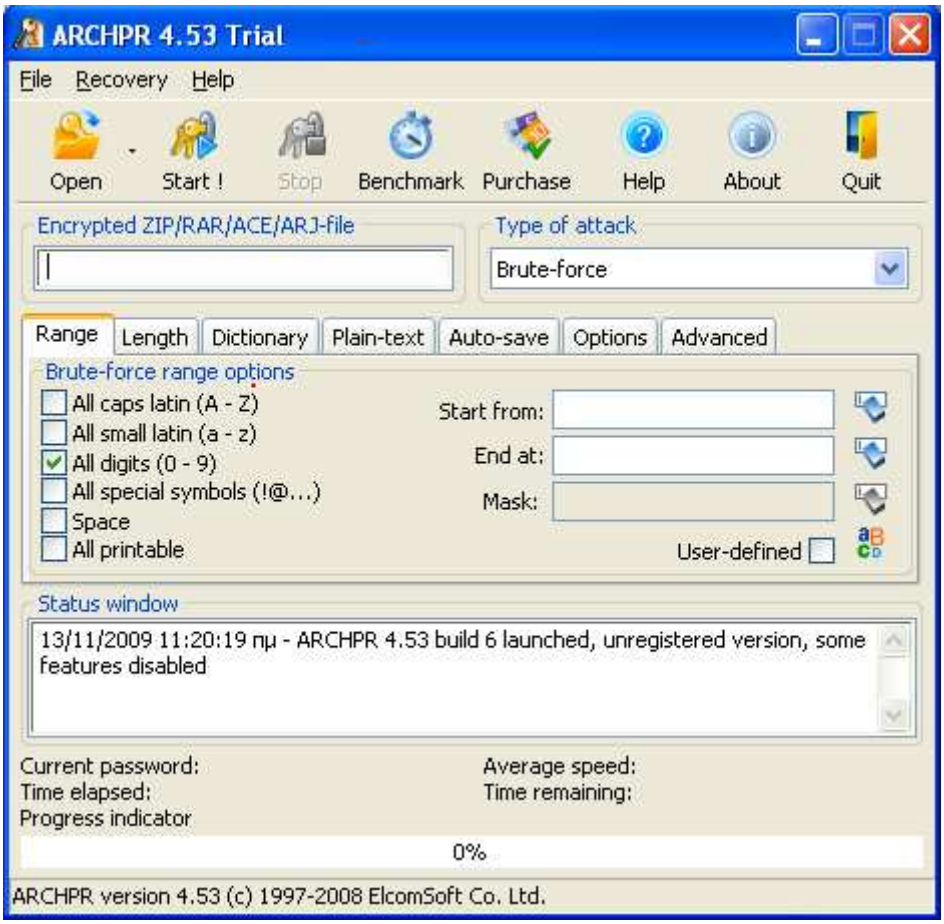
Πατάμε OK και το πρόγραμμα θα συμπιέσει το αρχείο. Έτσι λίγα απλά βήματα έχουμε συμπιέσει το φάκελο.



Εικόνα 126: φάκελος και συμπιεσμένος

Τι γίνεται όμως αν ξεχάσουμε τον κωδικό που είχαμε τοποθετήσει? Τη λύση μας δίνει ένα εύχρηστο και απλό εργαλείο της εταιρίας elcomsoft, το Advanced Archive Password Recovery[16].

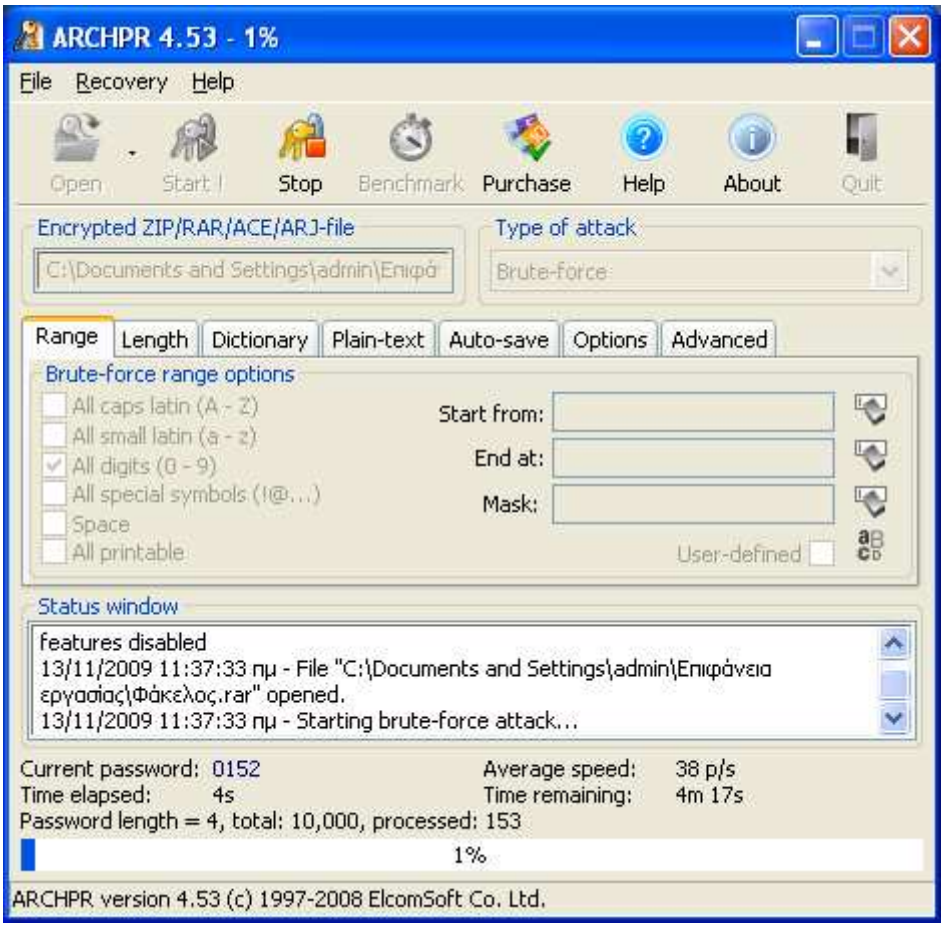
[16] http://www.elcomsoft.com/download.html



Εικόνα 127: Advanced Archive Password Recovery αρχική

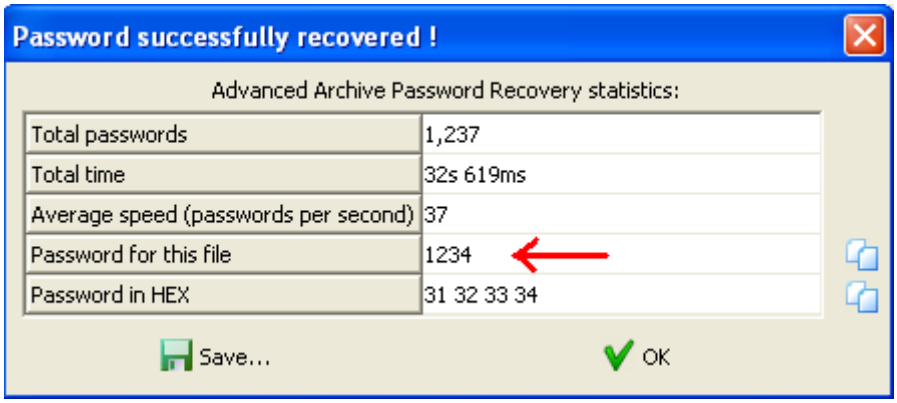
Από ότι βλέπουμε το πρόγραμμα μας δίνει μια πληθώρα επιλογών. Μπορούμε να επιλέξουμε το είδος της επίθεσης που θέλουμε να γίνει(brute force, dictionary, plain text), το είδος των χαρακτήρων που θα χρησιμοποιηθούν (κεφαλαία, πεζά, αριθμοί, σύμβολα) και τη λέξη κλειδί από την οποία επιθυμούμε να αρχίσει η αναζήτηση. Επίσης μπορούμε να καθορίζουμε το μήκος του κωδικού, τον ελάχιστο και τον μέγιστο αριθμό χαρακτήρων ώστε να γίνει πιο εξειδικευμένη η αναζήτηση.

Η χρήση του Advanced Archive Password Recovery είναι πολύ απλή και εύκολη. Δεν έχουμε παρά να πατήσουμε το κουμπί Open και να επιλέξουμε το αρχείο που θέλουμε να ξεκλειδώσουμε.



Εικόνα 128: Advanced Archive Password Recovery εύρεση κωδικού

Παρατηρούμε πως το πρόγραμμα μας δίνει κάποιες πληροφορίες όπως τον τρέχων κωδικό που δοκιμάζει, πόσους κωδικούς δοκιμάζει τον δευτερόλεπτο, πόσος χρόνος πέρασε και πόσος απομένει.



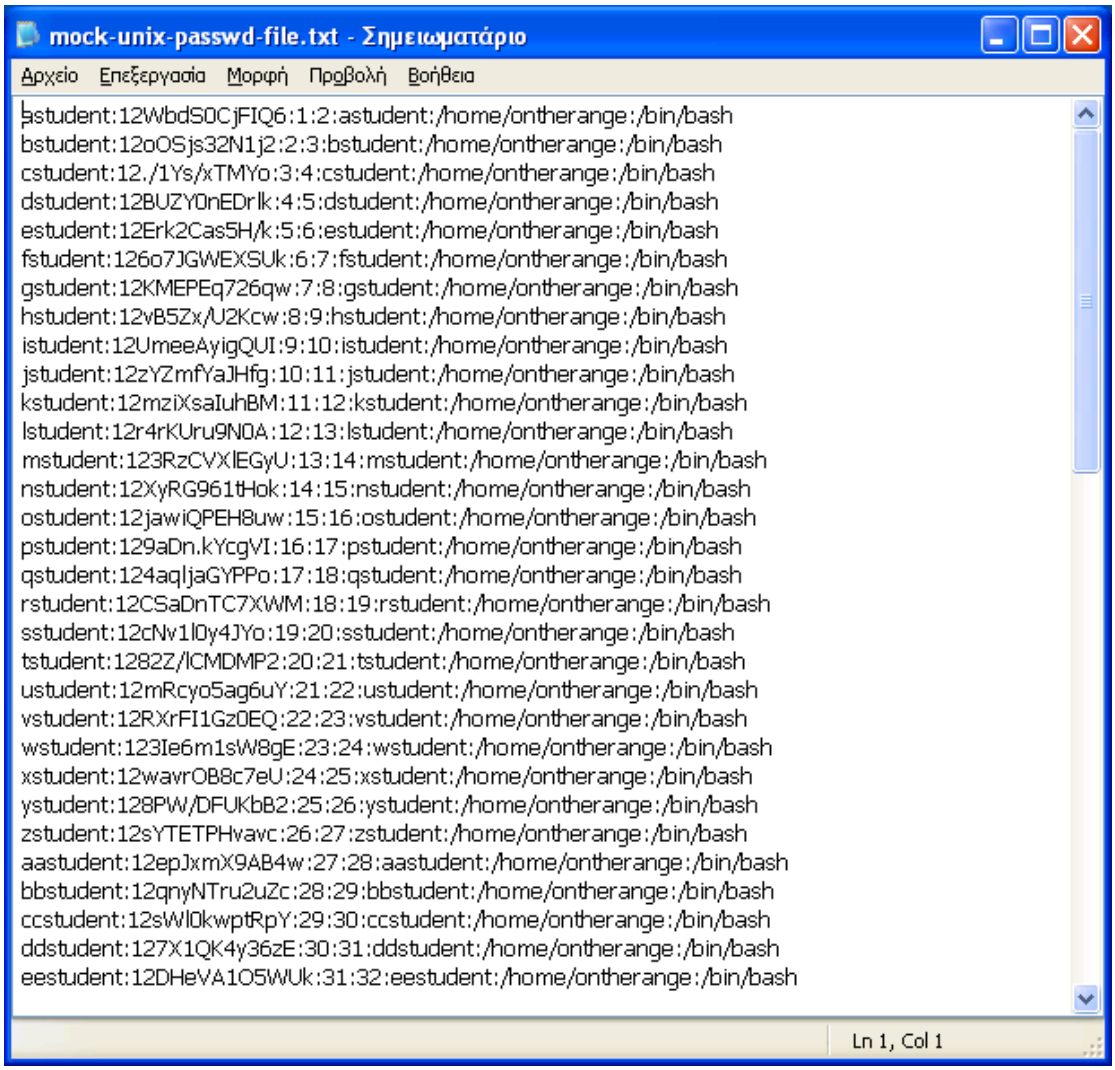
Εικόνα 129: Advanced Archive Password Recovery ανάκτηση κωδικού

Το πρόγραμμα ‘έσπασε’ τον κωδικό μέσα σε 32 δευτερόλεπτα.

7.7 John The Ripper (JTR)

Το πρόγραμμα John the Ripper [17] είναι ένα δωρεάν εργαλείο cracking. Αρχικά δημιουργήθηκε για το λειτουργικό σύστημα UNIX ενώ πλέον τρέχει σε δεκαπέντε διαφορετικές πλατφόρμες. (11 UNIX, DOS, Win32, BeOS, και OpenVMS). Είναι ένα από τα δημοφιλέστερα προγράμματα «σπασίματος» κωδικών και συνδυάζει ένα αριθμό από password crackers σε ένα πακέτο, εντοπίζει αυτόματα τύπους hash κωδικών και περιλαμβάνει ένα ειδικό cracker.

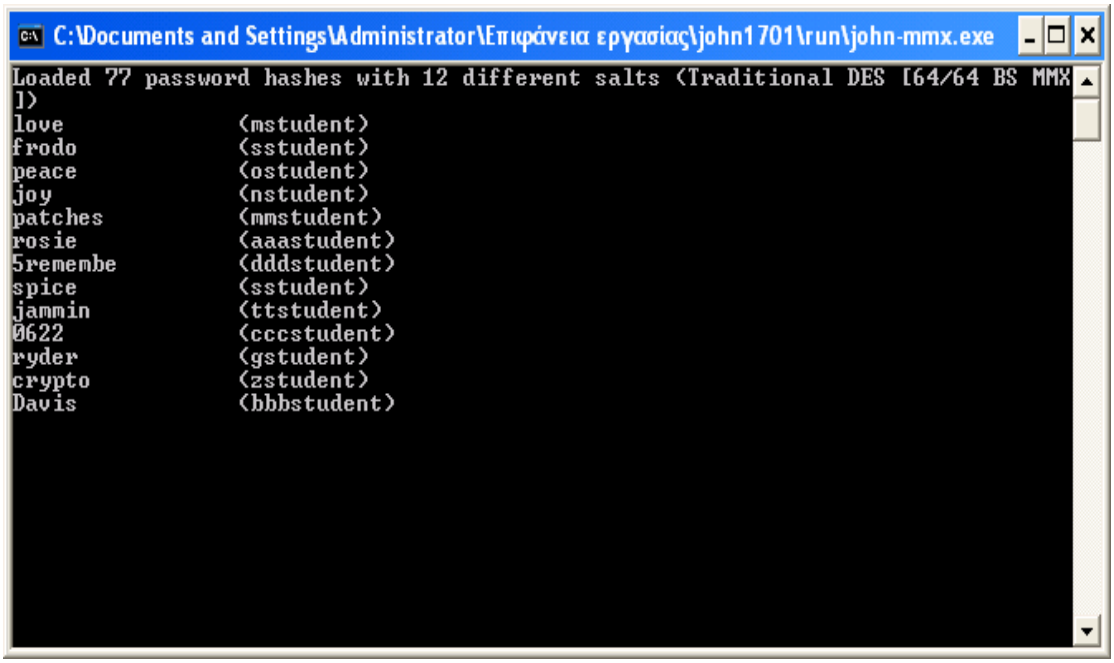
Οι πληροφορίες για τους λογαριασμούς και passwords στο UNIX βρίσκονται συνήθως στο /etc/passwd. Για να δούμε το αρχείο αυτό εκτελούμε σε UNIX μηχάνημα > cat /etc/passwd OR > ypcat passwd. Στην συγκεκριμένη περίπτωση έχουμε ένα υπόδειγμα τέτοιου αρχείου (mock-unix-password-file.txt).



Εικόνα 130: mock-unix-password-file.txt

[17] http://www.openwall.com/john/

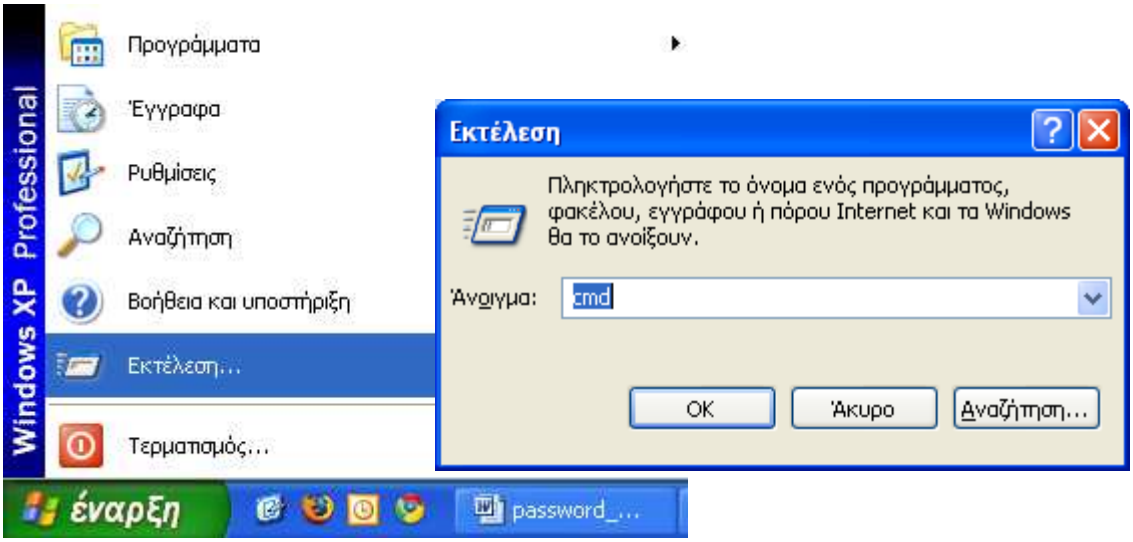
Το συγκεκριμένο πρόγραμμα λειτουργεί με δύο τρόπους. Στην πρώτη περίπτωση κάνουμε drop το mock-unix-password-file.txt στο john-mmx.exe του JTR. Αυτομάτως ανοίγει ένα νέο παράθυρο όπου αποκαλύπτονται οι κωδικοί.



Εικόνα 131: John The Ripper

Φορτώθηκαν 77 κωδικοί. Σε μια ώρα αποκαλύφθηκαν 13 κωδικοί από το JTR.

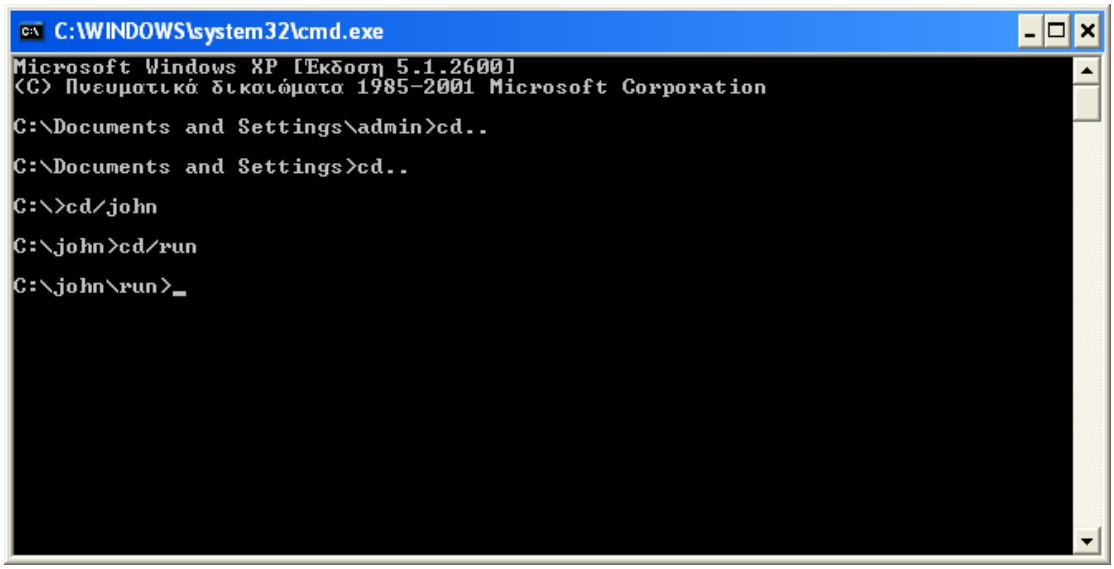
Στη δεύτερη περίπτωση θα τρέξουμε το πρόγραμμα μέσα από γραμμή εντολών MS-DOS. Επιλέγουμε έναρξη → εκτέλεση και πληκτρολογούμε cmd.



Εικόνα 132: πατάμε έναρξη εκτέλεση και πληκτρολογούμε cmd

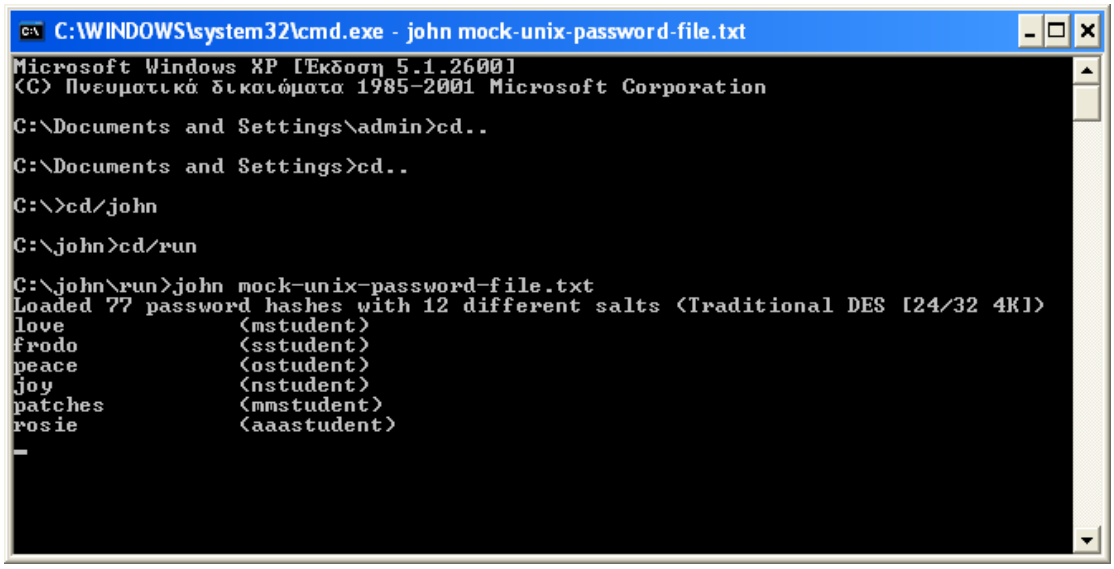
Εικόνα 133: command prompt

Για να τρέξουμε το πρόγραμμα πρέπει να μεταβούμε στο φάκελο στον οποίο βρίσκεται το john.exe και να το εκτελέσουμε από εκεί. Η διαδικασία φαίνεται στην παρακάτω εικόνα.



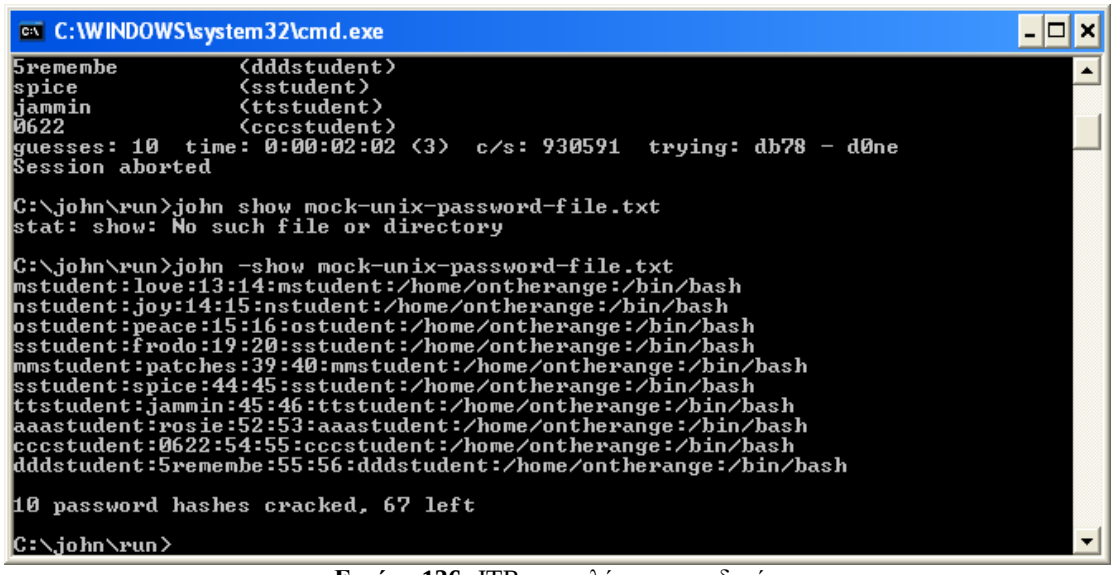
Εικόνα 134: cmd άνοιγμα φακέλου run

Τώρα βρισκόμαστε στον φάκελο run και το μόνο που απομένει είναι να πούμε στο πρόγραμμα που θα βρει το αρχείο με τους κωδικούς. Αυτό θα γίνει με την εντολή john mock-unix-password-file.txt



Εικόνα 135: JTR εύρεση κωδικών

Για να σταματήσει η διαδικασία πατάμε Ctrl+C και για να δούμε τα αποτελέσματα πληκτρολογούμε john –show mock-unix-password-file.txt



Εικόνα 136: JTR αποτελέσματα κωδικών

Το JTR υποστηρίζει 4 διαφορετικά είδη cracking modes:

Στο wordlist mode, ο οποίος είναι ο απλούστερος τρόπος εύρεσης κωδικού. Σ' αυτό δίνεται μια wordlist και κάποια password files.
Στο Single crack mode χρησιμοποιούνται login names, full names fields ή home directories names για τον υπολογισμό των passwords και είναι πιο γρήγορος από το wordlist mode.
Στο incremental mode, έχουμε να κάνουμε με το πιο ισχυρό εργαλείο για την εύρεση κωδικών κάτι σαν το brute force. Εδώ το πρόγραμμα θα δοκιμάσει να

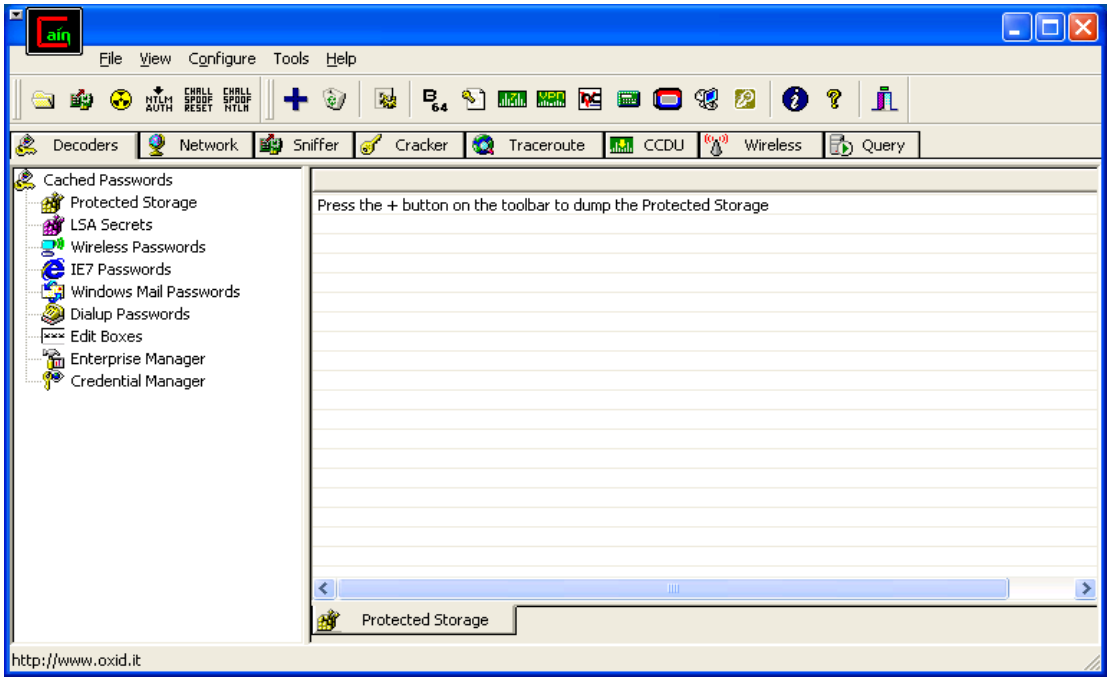
ανακαλύψει τον κωδικό δοκιμάζοντας όλους τους πιθανούς συνδυασμούς. Παρόλα αυτά υπάρχει ο κίνδυνος αν ο κωδικός είναι πολύ μεγάλος να μην τα καταφέρει.
Τέλος **στο external mode,** δοκιμάζεται ο συνδυασμός κάποιου εξωτερικού προγράμματος πάνω στο JTR για την ανακάλυψη των επιθυμητών κωδικών.

7.8 Cain & Abel

Το Cain & Abel είναι ένα εργαλείο αποκατάστασης κωδικού πρόσβασης για τα λειτουργικά συστήματα της Microsoft. Μπορεί να ανακτήσει πολλά είδη κωδικών πρόσβασης χρησιμοποιώντας μεθόδους όπως οι dictionary attacks, brute force και επιθέσεις κρυπτανάλυσης, καταγράφοντας συνομιλίες VOIP, ανάκτηση των κλειδιών ασύρματων δικτύων, αποκάλυψη των εναποθηκευμένων κωδικών πρόσβασης και ανάλυση των πρωτοκόλλων δρομολόγησης. Το Cain & Abel έχει αναπτυχθεί με την ελπίδα ότι θα είναι χρήσιμο για τους administrator δικτύων, τους δασκάλους, τους σύμβουλους ασφαλείας, τους προμηθευτές λογισμικού ασφάλειας και για οποιονδήποτε θέλει να το χρησιμοποιήσει για ηθικούς σκοπούς. Το πρόγραμμα προειδοποιεί ότι υπάρχει η δυνατότητα να προκαλέσει ζημίες ή απώλεια στοιχείων και ότι ο χρήστης είναι ο αποκλειστικός υπεύθυνος. [18]

Εγκατάσταση Cain

Η εγκατάσταση του Cain είναι απλή αρκεί να τρέξουμε το setup αρχείο που θα βρούμε στην περιοχή που το έχουμε αποθηκεύσει. Η εγκατάσταση του είναι απλή. Είναι σαν μια εγκατάσταση ενός τυπικού προγράμματος των Windows.

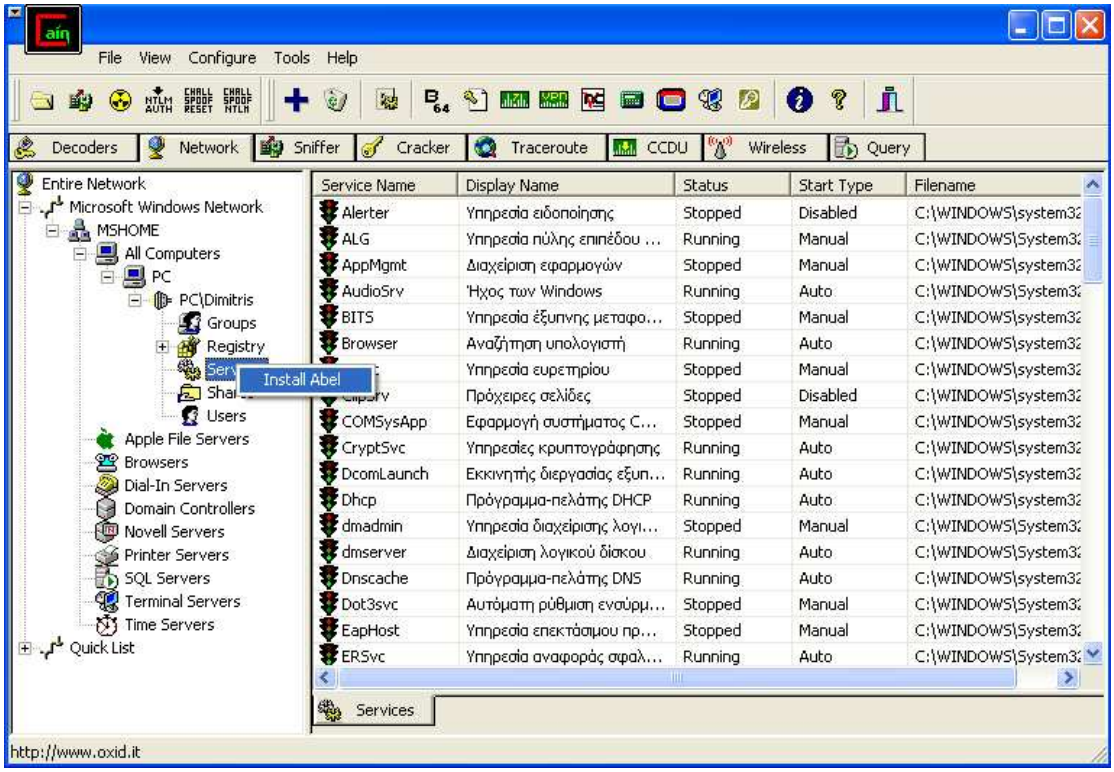


Εικόνα 137: Cain αρχική

Εγκατάσταση Abel

Η εγκατάσταση του Abel πραγματοποιείται μέσα από το Cain. Επιλέγουμε την καρτέλα *network* και στη συνέχεια διαδοχικά *MMicrosoft Windows Network→ MSHOME→ All computers→ PC→ PC\Dimitris→ services* δεξί κλικ κ πατάμε *install Abel.*

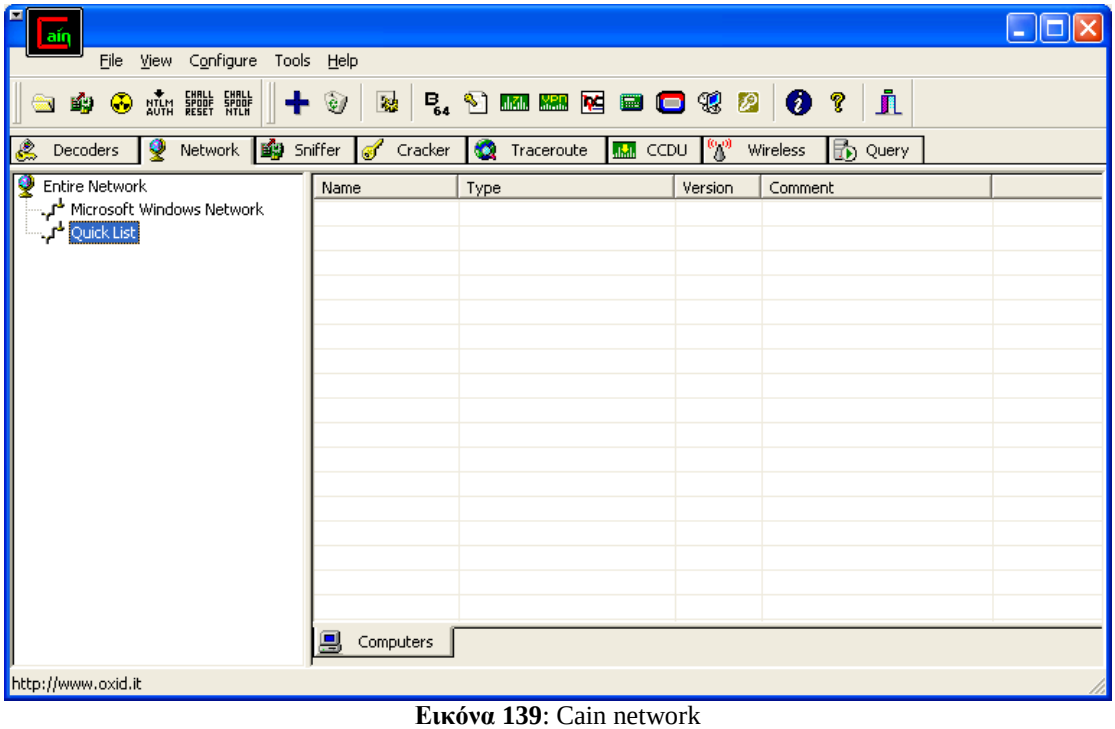
[18] http://www.oxid.it/cain.html



Εικόνα 138: Εγκατάσταση Abel

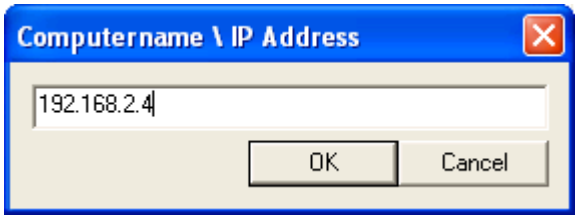
Θα προσπαθήσουμε με τη χρήση του συγκεκριμένου εργαλείου να “σπάσουμε” τον κωδικό που χρειάζεται για να εισέλθουμε στα windows.

Πατάμε *network* και αριστερά εμφανίζονται οι επιλογές “*Microsoft Windows network*” και “*quick list*”.



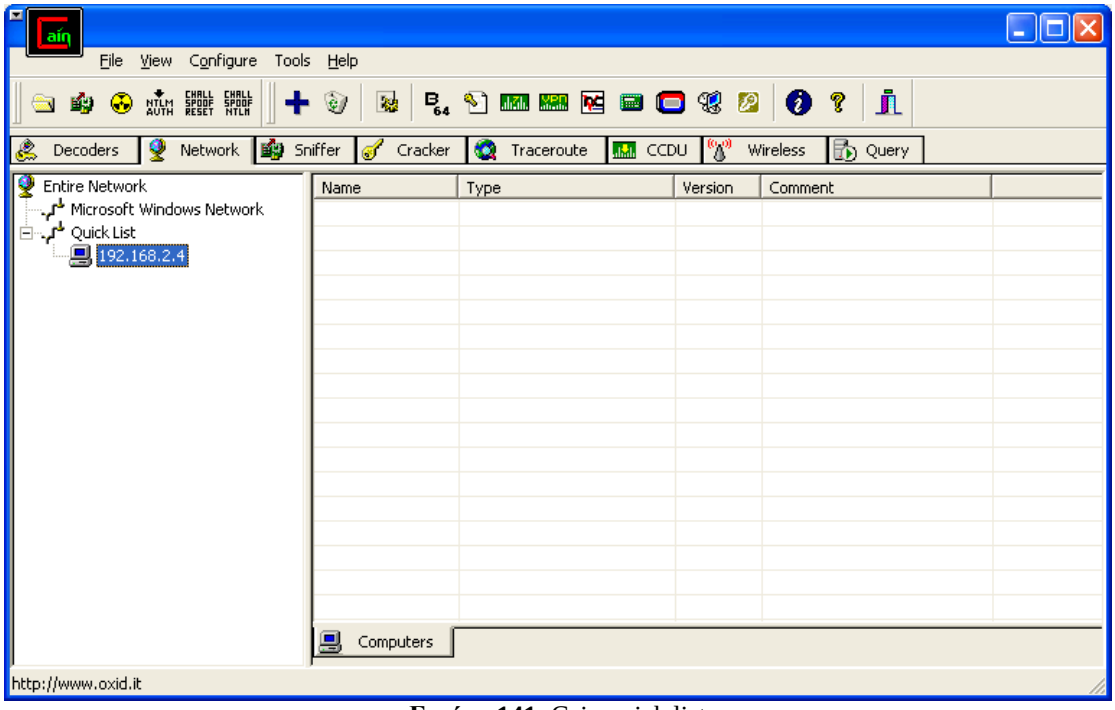
Εικόνα 139: Cain network

Κάνουμε δεξί κλικ στο *quick list* και επιλέγουμε "*add to quick list*". Εμφανίζεται ένα παράθυρο στο οποίο πρέπει να βάλουμε την IP στην οποία θέλουμε να επιτεθούμε. (εδώ θα βάλουμε την IP του συγκεκριμένου PC).



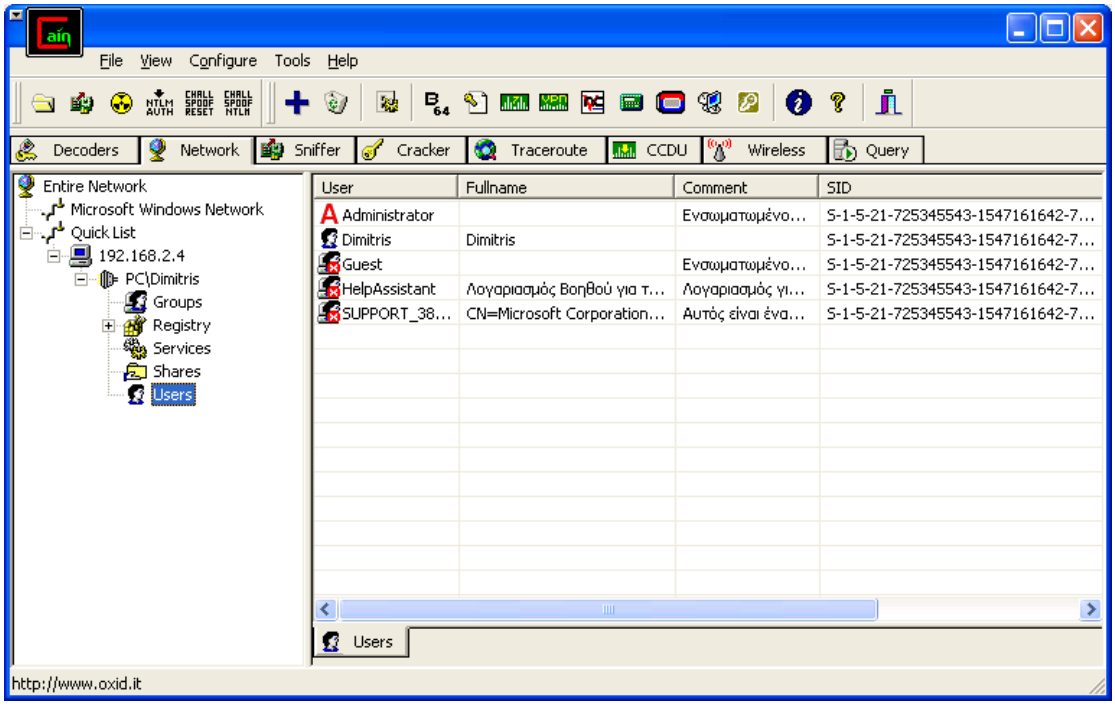
Εικόνα 140: Cain εισαγωγή IP

Από ότι βλέπουμε παρακάτω, ακριβώς κάτω απ το quick list εμφανίζεται η IP μας.



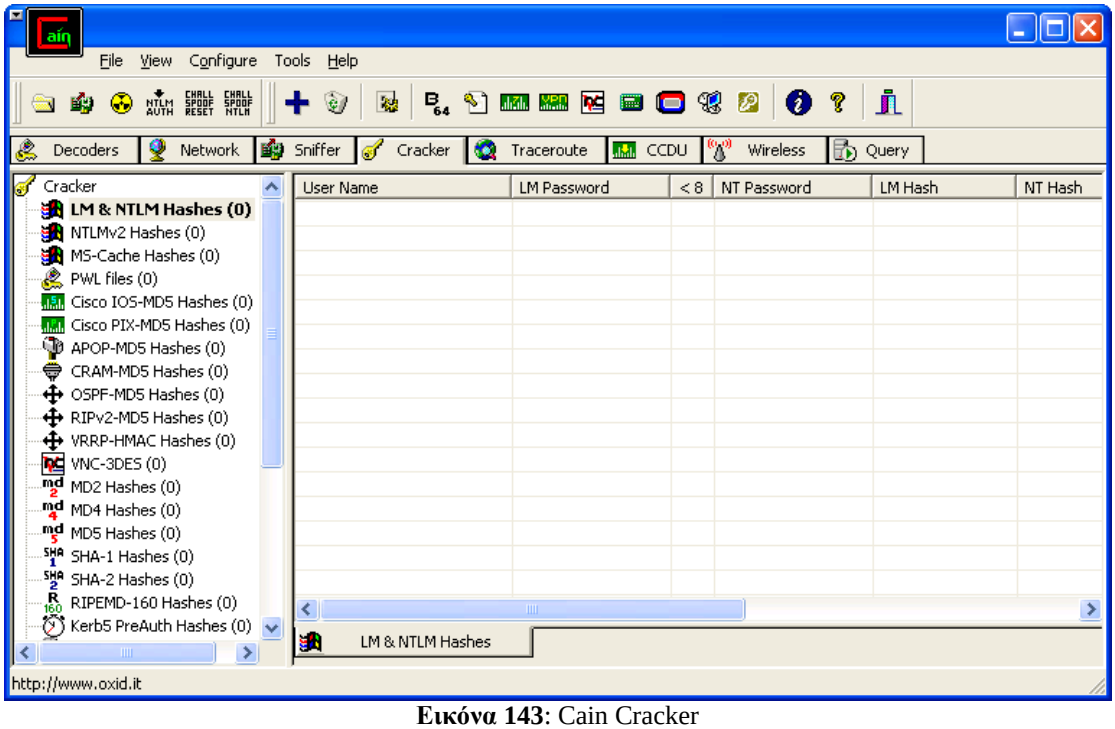
Εικόνα 141: Cain quick list

Κάνουμε διπλό κλικ στην IP κ έπειτα πατάμε την επιλογή *users.*



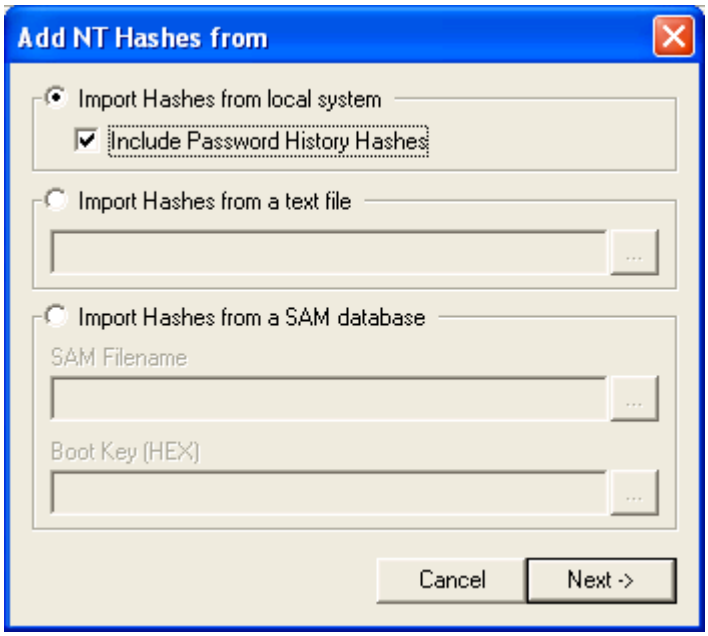
Εικόνα 142: Cain Users

Στη συνέχεια αλλάζουμε tab και πατάμε στο τέταρτο κατά σειρά (*cracker*).



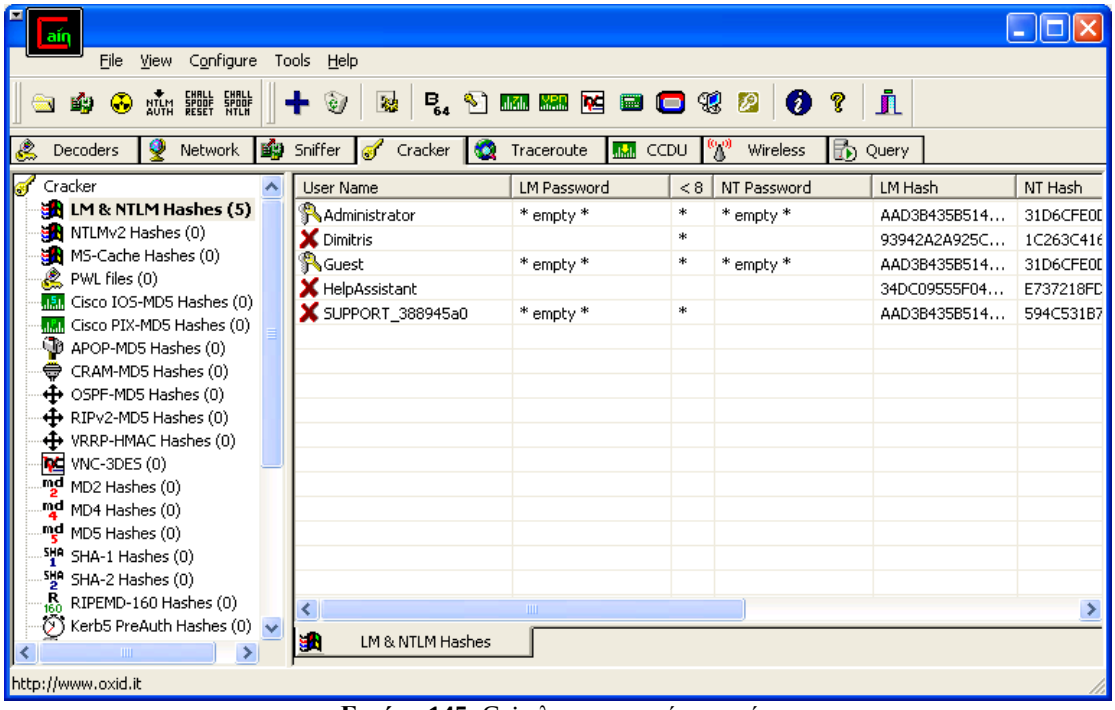
Εικόνα 143: Cain Cracker

Πατάμε τον μπλε σταυρό που βρίσκεται πάνω από την καρτέλα sniffer.



Εικόνα 144: Cain hashes

Πατάμε next και βλέπουμε ότι το Cain έχει εισάγει στο cracker τους λογαριασμούς που υπάρχουν στο PC.



Εικόνα 145: Cain λογαριασμοί χρηστών

Το username με το οποίο έχω μπει στα Windows είναι Dimitris. Κάνουμε δεξί κλικ πάνω του και επιλέγουμε τον τρόπο της επίθεσης την οποία επιθυμούμε. Το Cain προσφέρει 3 ειδών επιθέσεις (dictionary attack, brute force attack και cryptanalysis attack)

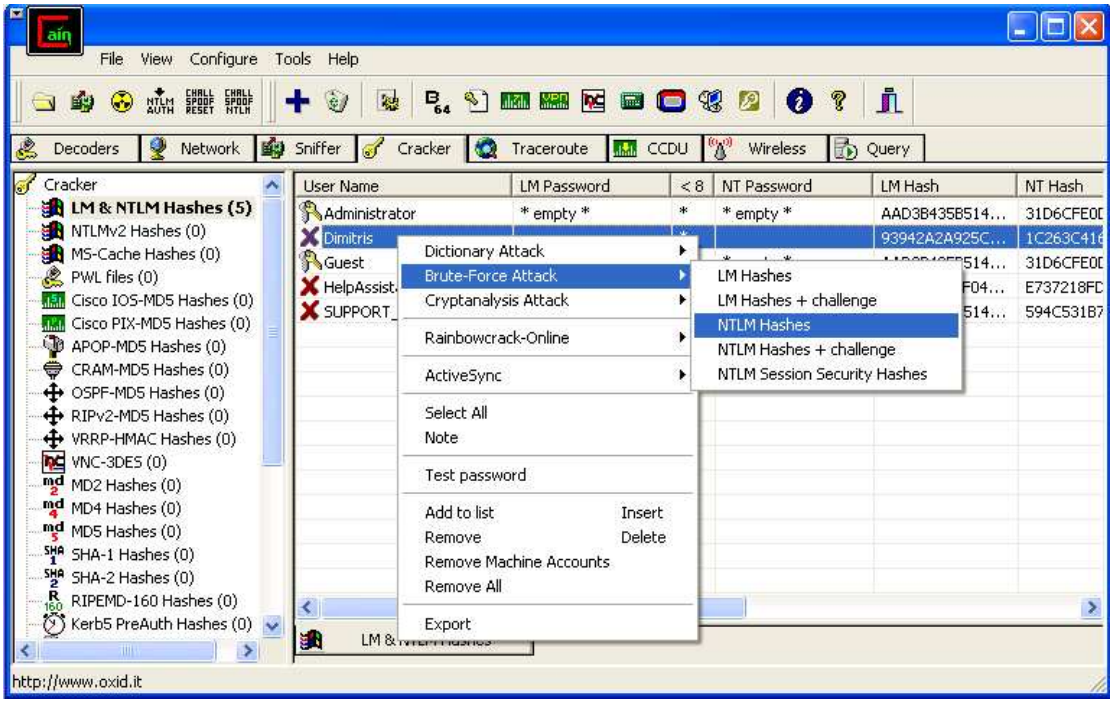
Είδη επιθέσεων

- **Brute force attack:** Η **brute-force attack** (*επίθεση ωμής βίας*) αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Τέτοιου είδους επιθέσεις, οι οποίες χρησιμοποιούν όλα τα δυνατά κλειδιά, μπορούν πάντοτε να πραγματοποιηθούν. Συχνά, όμως, ο επιτιθέμενος ξεκινά την επίθεση χρησιμοποιώντας πιο "πιθανά", κατά την άποψή, του κλειδιά, προσπαθώντας με αυτό τον τρόπο να βρει το κλειδί πιο γρήγορα. Πρακτικά, η αναζήτηση σταματά μόλις βρεθεί το κλειδί, χωρίς να χρειαστεί περαιτέρω ενημέρωση της λίστας κλειδιών.

- **Dictionary attack:** Η **dictionary attack** (επίθεση λεξικού) χρησιμοποιεί μια τεχνική ωμής βίας από διαδοχικές προσπάθειες όλων των λέξεων σε έναν εξαντλητικό κατάλογο (από προκαθορισμένη λίστα των τιμών). Σε αντίθεση με την επίθεση brute-force, η επίθεση λεξικού προσπαθεί μόνο τις δυνατότητες που έχουν τις περισσότερες πιθανότητες να πετύχουν. Σε γενικές γραμμές, οι επιθέσεις είναι επιτυχείς, διότι πολλοί άνθρωποι έχουν την τάση να επιλέγουν κωδικούς πρόσβασης που είναι μικροί (7 ή λιγότερους χαρακτήρες), και μόνο λέξεις που βρίσκονται σε λεξικά ή απλά, εύκολα-προβλεπόμενες παραλλαγές λέξεων.

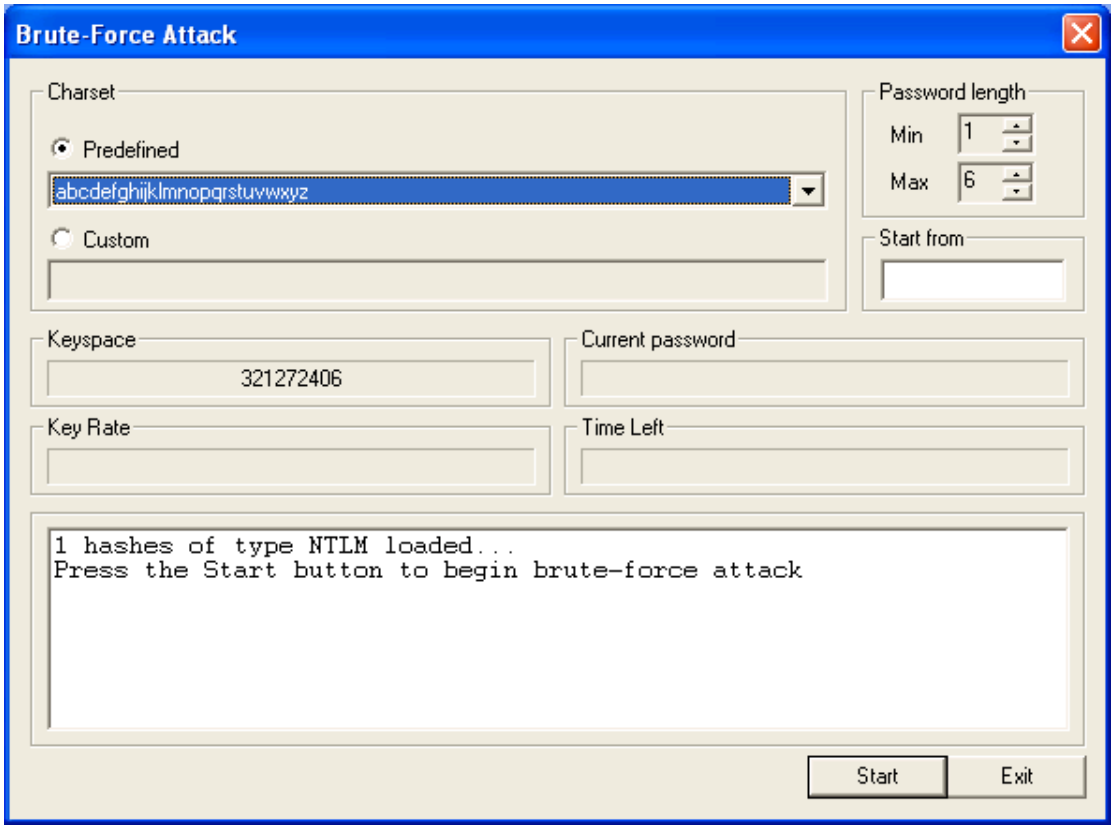
- **Cryptanalysis attack:** Η συγκεκριμένη τακτική είναι αρκετά γρήγορη όμως είναι χρήσιμη στο να σπάει μόνο μερικά είδη κρυπτογραφημένων κωδικών. Χρησιμοποιεί ένα σετ από μεγάλους πίνακες από προ-υπολογισμένους κρυπτογραφημένους κωδικούς (Rainbow Tables), ώστε να βελτιώσει τις μεθόδους ανταλλαγής οι οποίες είναι γνωστές σήμερα και για να ανακτήσει γρηγορότερα διάφορους κωδικούς.

Στη συγκεκριμένη περίπτωση χρησιμοποιήσαμε την επίθεση ωμής βίας (brute-force attack)



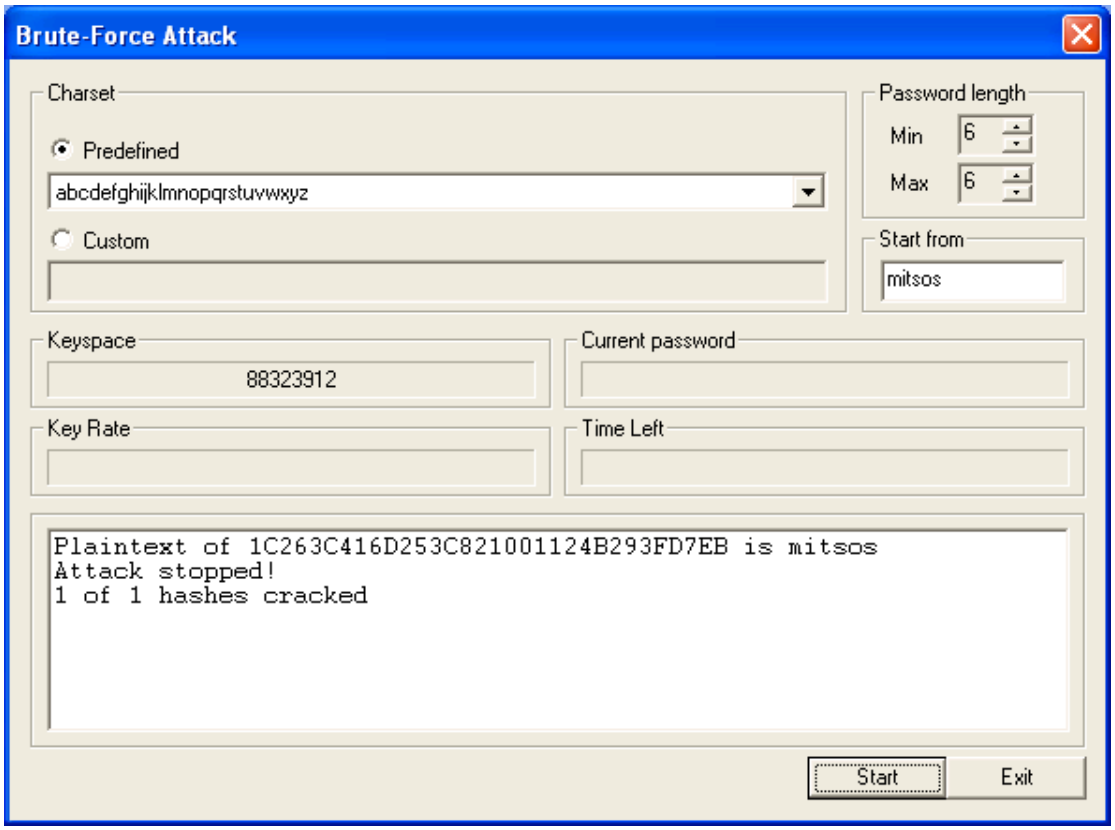
Εικόνα 146: Cain επιλογή επίθεσης

Εμφανίζεται ένα παράθυρο, στο οποίο μπορούμε να καθορίσουμε το μήκος του κωδικού ή το εύρος των χαρακτήρων που χρειάζεται για να σπάσει ο κωδικός και πατάμε start ώστε να ξεκινήσει η διαδικασία.

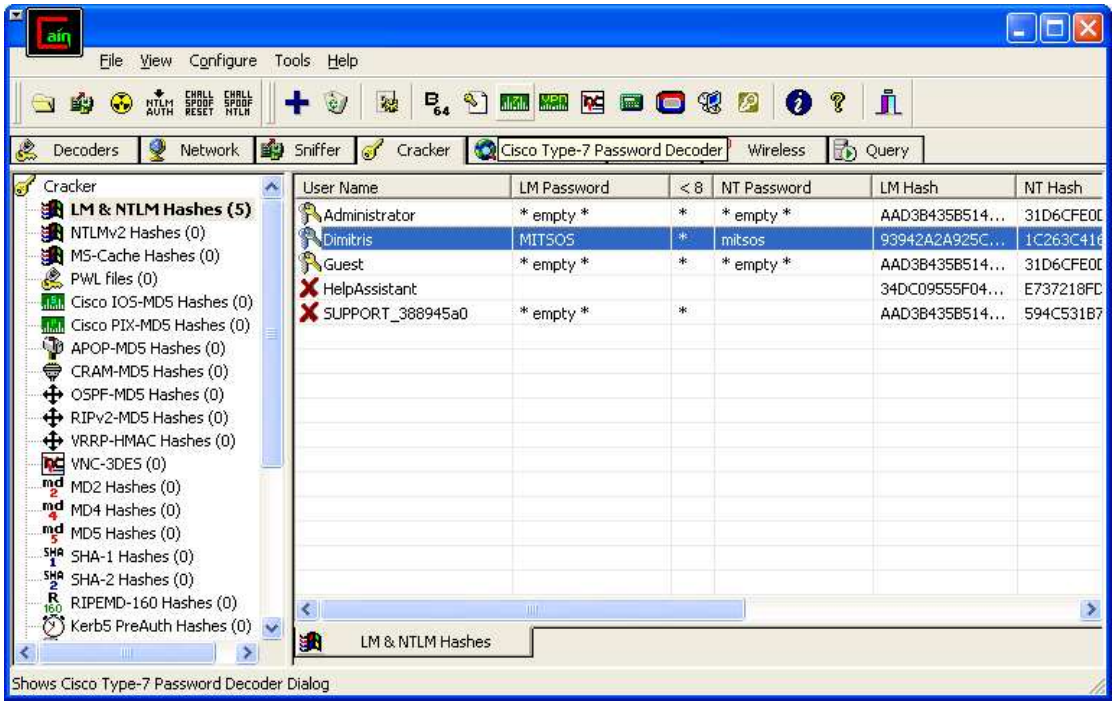


Εικόνα 147: Cain Brute Force Attack

Σε χρόνο λιγότερο του ενός λεπτού παρατηρούμε ότι το Cain έσπασε τον κωδικό.



Εικόνα 148: Cain Hash Cracked



Εικόνα 149: Cain εύρεση κωδικού

Βλέπουμε ότι το πεδίο NT Password που πριν ήταν κενό τώρα έχει συμπληρωθεί από τον κωδικό.

Username: Dimitris
Password: mitsos

Κεφάλαιο 8 Password statistics

8.1 Οι πιο αδύναμοι κωδικοί στο διαδίκτυο

Η εταιρεία Imperva διεξήγαγε έρευνα τον Ιανουάριο του 2010 για το ποιοι κωδικοί του διαδικτύου «σπάνε» πιο εύκολα, παίρνοντας ως δείγμα την παραβίαση 32 εκατ. λογαριασμών μέσω του RockYou.com. Σύμφωνα με την έρευνα περίπου οι μισοί από τους χρήστες του διαδικτύου χρησιμοποιούν για την είσοδό τους σε λογαριασμούς κοινωνικών δικτύων, ηλεκτρονικών ταχυδρομείων κ.α., τους ίδιους ή παρόμοιους κωδικούς.
Παρόμοιες έρευνες που έγιναν το 1990 και το 2000 είχαν τα ίδια περίπου αποτελέσματα. Οι χρηστές όταν τους επιτρέπεται, επιλέγουν πολύ μικρούς και αδύναμους κωδικούς ακόμη και για λογαριασμούς που περιέχουν ευαίσθητα προσωπικά δεδομένα. Όπως υπογραμμίζει, η Imperva οι παραβιάσεις στο διαδίκτυο από χάκερς ολοένα και αυξάνονται. Συγκεκριμένα, στο πλαίσιο των αυτοματοποιημένων επιθέσεων σε αδύναμους κωδικούς, μόλις σε 110 προσπάθειες, ένας χάκερ κερδίζει πρόσβαση σε έναν λογαριασμό κάθε δευτερόλεπτο. Χρειάζονται δηλαδή 17 λεπτά για να εισβάλει σε 1.000 λογαριασμούς.

Οι πιο συνηθισμένοι κωδικοί είναι:

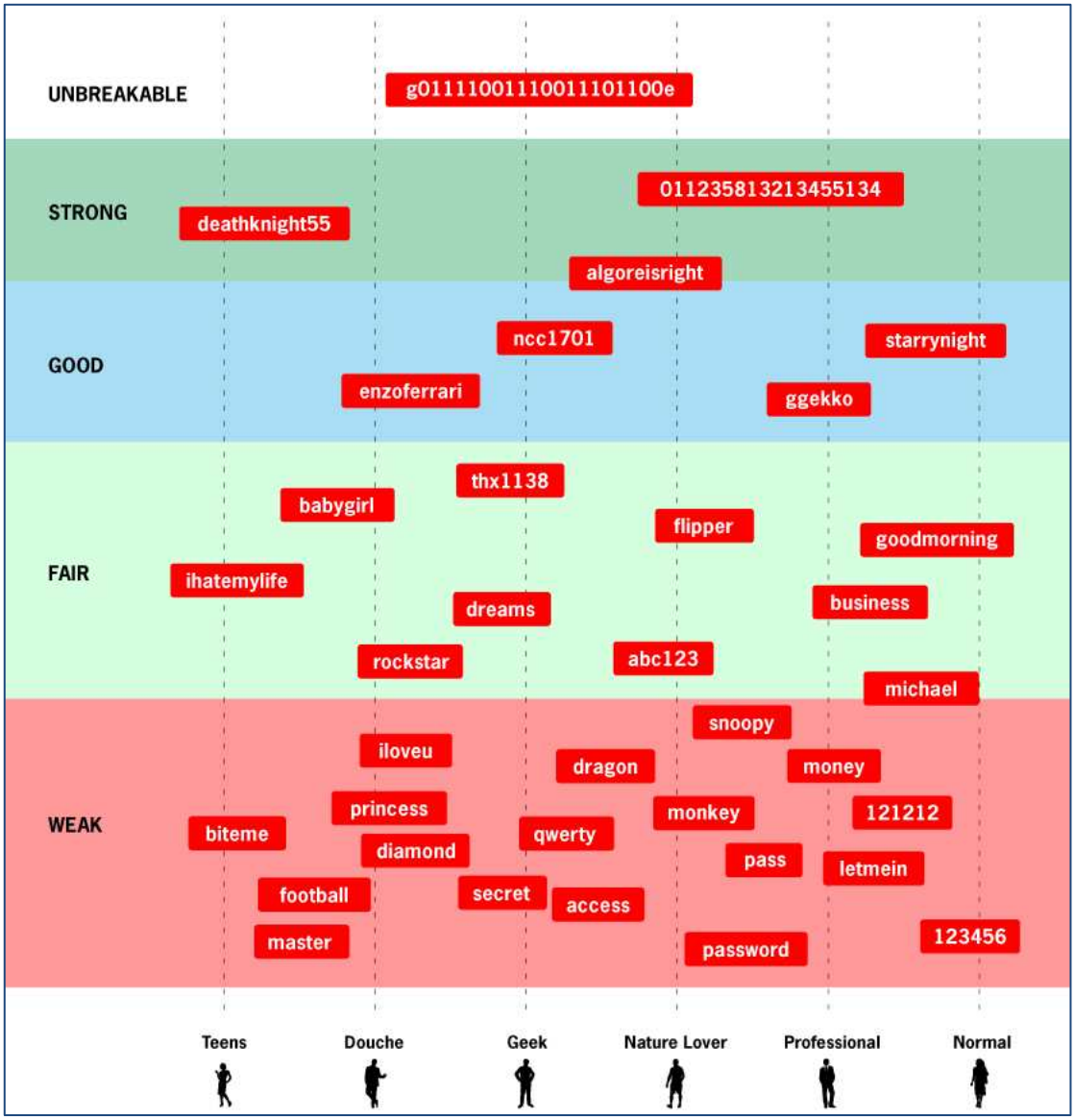
1. 123456
2. 12345
3. 123456789
4. Password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123

Τα αποτελέσματα της έρευνας υποδεικνύουν ότι περίπου το 30% των χρηστών επιλέγει κωδικούς με λιγότερους από έξι χαρακτήρες, ενώ το 60% επιλέγει κωδικούς μόνο από το λατινικό αλφάβητο ή σε συνδυασμό με αριθμούς. Επίσης το 50% χρησιμοποιεί ονόματα, λέξεις αργκό, του λεξικού ή τυχαίες (συνεχόμενους αριθμούς, συνεχόμενα γράμματα στο πληκτρολόγιο κ.τ.λ.).

Για έναν ασφαλή κωδικό, η N.A.S.A. προτείνει:

- Να περιέχει τουλάχιστον 8 χαρακτήρες.
- Να περιέχει διαφορετικών τύπων χαρακτήρες. Κεφαλαία και πεζά γράμματα και ειδικούς χαρακτήρες όπως !@#$%^&*,;". Αν υπάρχει μόνο ένα γράμμα στον κωδικό, αυτό δεν θα πρέπει να είναι ο πρώτος ή τελευταίος χαρακτήρας του κωδικού.
- Δεν πρέπει να είναι όνομα, αργκό ή οποιαδήποτε λέξη από το λεξικό. Δεν πρέπει να περιέχει κανένα γράμμα από το όνομα ή το e-mail του χρήστη.

Επομένως ο κωδικός πρέπει να δημιουργείται με σκοπό να είναι αδιάβλητος. Σύμφωνα με τον ειδικό στην ασφάλεια στο διαδίκτυο, Bruce Schneir, ένας εύκολος τρόπος είναι να επιλέξουμε μια πρόταση και να την μετατρέψουμε σε κωδικό. Το παράδειγμα που θέτει είναι: Η φράση “This little piggy went to market” να μετατραπεί σε "tlpWENT2m". Ο ίδιος προτείνει στους χρήστες να έχουν διαφορετικούς κωδικούς για κάθε λογαριασμό. Αν αντιμετωπίζουν δυσκολίες στο να τους θυμούνται, τότε μπορούν να τους σημειώσουν και να τους φυλάξουν στο πορτοφόλι τους.



8.2 Χρόνοι ανάκτησης κωδικών

Παρακάτω παρουσιάζεται κατά προσέγγιση ο χρόνος που απαιτείται για έναν υπολογιστή ή μια ομάδα υπολογιστών να μαντέψει διάφορους κωδικούς. Τα αριθμητικά στοιχεία που παρατίθενται είναι κατά προσέγγιση και είναι το μέγιστο χρονικό διάστημα που απαιτείται για να μαντέψει ένας υπολογιστής κάθε κωδικό πρόσβασης χρησιμοποιώντας μια brute force επίθεση.

ΚΛΑΣΕΙΣ 'ΕΠΙΘΕΣΗΣ'

Έχουμε έξι κλάσεις ανάλογα με την ταχύτητα σπασίματος των διαφόρων ειδών των κωδικών πρόσβασης με διάφορα hardware:

A. 10,000 Κωδικοί / δευτερόλεπτο
   Χαρακτηριστικό για την ανάκτηση των κωδικών πρόσβασης του Microsoft Office σε έναν Pentium 100
B. 100,000 Κωδικοί / δευτερόλεπτο
   Χαρακτηριστικό για την ανάκτηση των Windows Password Cache (. PWL Files) κωδικών πρόσβασης σε έναν Pentium 100
C. 1,000,000 Κωδικοί / δευτερόλεπτο
   Χαρακτηριστικό για την ανάκτηση των ZIP κωδικών πρόσβασης σε έναν Pentium 100
D. 10,000,000 Κωδικοί / δευτερόλεπτο
   Γρήγορος υπολογιστής με Dual core επεξεργαστή.
E. 100,000,000 Κωδικοί / δευτερόλεπτο
   Σταθμός εργασίας ή πολλοί υπολογιστές που εργάζονται μαζί.

Ακλουθούν όλοι οι πιθανοί συνδυασμοί για την 'δημιουργία' ενός κωδικού.

- ✧ Περίπτωση 1: Μόνο αριθμοί

Πλήθος χαρακτήρων: 10
Χαρακτήρες: 0123456789

Κωδικός		**Χρόνος**				
Μάκρος	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
2	100	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
3	1.000	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
4	10.000	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
5	100.000	10 δευτ.	Αμέσως	Αμέσως	Αμέσως	Αμέσως
6	1.000.000	1½ λεπτό	10 δευτ.	Αμέσως	Αμέσως	Αμέσως
7	10.000.000	17 λεπτά	1½ λεπτό	1½ λεπτό	Αμέσως	Αμέσως
8	100.000.000	2¾ ώρες	17 λεπτά	1½ λεπτό	10 δευτ.	Αμέσως

Πίνακας 1: Χρόνοι ανάκτησης κωδικών περίπτωση 1 - Μόνο αριθμοί

Παραδείγματα

		Χρόνος				
Κωδικός	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
1234	10.000	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
7654321	10.000.000	17 λεπτά	1½ λεπτό	1½ λεπτό	Αμέσως	Αμέσως

Πίνακας 2: Χρόνοι ανάκτησης κωδικών περίπτωση 1 - παραδείγματα

✧ Περίπτωση 2: Όλο το αλφάβητο (κεφαλαία ή μικρά, όχι συνδυασμός)

Πλήθος χαρακτήρων: 26
Χαρακτήρες: ABCDEFGHIJKLMNOPQRSTUVWXYZ ή
Abcdefghijklmnopqrstuvwxyz

Κωδικός		**Χρόνος**				
Μάκρος	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
2	676	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
3	17.576	< 2 δευτ.	Αμέσως	Αμέσως	Αμέσως	Αμέσως
4	456.976	46 δευτ.	5 δευτ.	Αμέσως	Αμέσως	Αμέσως
5	11.8 εκατ.	20 λεπτά	2 λεπτά	12 δευτ.	Αμέσως	Αμέσως
6	308.9 εκατ.	8½ ώρες	51½ λεπτά	5 λεπτά	30 δευτ.	3 δευτ.
7	8 δις.	9 μέρες	22 ώρες	2¼ ώρες	13 λεπτά	1¼ λεπτά
8	200 δις.	242 μέρες	24 μέρες	2½ μέρες	348 λεπτά	35 λεπτά

Πίνακας 3: Χρόνοι ανάκτησης κωδικών περίπτωση 2 - Όλο το αλφάβητο (κεφαλαία ή μικρά)

Παραδείγματα

		Χρόνος				
Κωδικός	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
jimmy	11.8 εκατ.	20 λεπτά	2 λεπτά	12 δευτ.	Αμέσως	Αμέσως
MITSARAS	200 δις.	242 μέρες	24 μέρες	2½ μέρες	348 λεπτά	35 λεπτά

Πίνακας 4: Χρόνοι ανάκτησης κωδικών περίπτωση 2- παραδείγματα

✧ Περίπτωση 3: Όλο το αλφάβητο (κεφαλαία ή μικρά, όχι συνδυασμός) και αριθμοί

Πλήθος χαρακτήρων: 36
Χαρακτήρες: ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ή
abcdefghijklmnopqrstuvwxyz0123456789

Κωδικός		**Χρόνος**				
Μάκρος	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
2	1.296	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
3	46.656	4 δευτ.	Αμέσως	Αμέσως	Αμέσως	Αμέσως
4	1.6 εκατ.	2½ λεπτά	16 δευτ.	1½ δευτ.	Αμέσως	Αμέσως
5	60.4 εκατ.	1½ ώρες	10 λεπτά	1 λεπτά	Αμέσως	Αμέσως

Πίνακας 5: Χρόνοι ανάκτησης κωδικών περίπτωση 3 - Όλο το αλφάβητο και αριθμοί

Παραδείγματα

		Χρόνος				
Κωδικός	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
jim1	1.6 εκατ.	2½ λεπτά	16 δευτ.	1½ δευτ.	Αμέσως	Αμέσως
DIM12	60.4 εκατ.	1½ ώρες	10 λεπτά	1 λεπτά	Αμέσως	Αμέσως

Πίνακας 6: Χρόνοι ανάκτησης κωδικών περίπτωση 3- παραδείγματα

✧ Περίπτωση 4: Όλο το αλφάβητο (κεφαλαία και μικρά)

Πλήθος χαρακτήρων: 52
Χαρακτήρες:
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz

Κωδικός		**Χρόνος**				
Μάκρος	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
2	2.704	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
3	140.608	14 δευτ.	< 2 δευτ.	Αμέσως	Αμέσως	Αμέσως
4	7.3 εκατ.	12½ λεπτά	1¼ λεπτά	8 δευτ.	Αμέσως	Αμέσως
5	380 εκατ.	10½ ώρες	1 ώρα	6 λεπτά	38 δευτ.	Αμέσως
6	19 δις.	23 μέρες	2¼ μέρες	5½ ώρες	33 λεπτά	19 δευτ.
7	1 τρις.	3¼ χρόνια	119 μέρες	12 μέρες	28½ ώρες	17 λεπτά
8	53 τρις.	169½ χρόνια	17 χρόνια	1½ χρόνια	62 μέρες	15 ώρες

Πίνακας 7: Χρόνοι ανάκτησης κωδικών περίπτωση 4 - Όλο το αλφάβητο (κεφαλαία και μικρά)

Παραδείγματα

		Χρόνος				
Κωδικός	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
DiMiTrIs	53 τρις.	169½ χρόνια	17 χρόνια	1½ χρόνια	62 μέρες	15 ώρες
Rodos	380 εκατ.	10½ ώρες	1 ώρα	6 λεπτά	38 δευτ.	Αμέσως

Πίνακας 8: Χρόνοι ανάκτησης κωδικών περίπτωση 4- παραδείγματα

✧ Περίπτωση 5: Όλο το αλφάβητο (κεφαλαία και μικρά) και αριθμοί

Πλήθος χαρακτήρων: 62
Χαρακτήρες:
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz0123456789

Κωδικός		**Χρόνος**				
Μάκρος	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
2	3.844	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
3	238.328	23 δευτ.	< 3 δευτ.	Αμέσως	Αμέσως	Αμέσως
4	15 εκατ.	24½ λεπτά	2½ λεπτά	15 δευτ.	< 2 δευτ.	Αμέσως
5	916 εκατ.	1 μέρα	2½ μέρες	15 λεπτά	1½ λεπτά	9 δευτ.
6	57 δις.	66 μέρες	6½ μέρες	16 μέρες	1½ μέρες	9½ λεπτά
7	3.5 τρις.	11 χρόνια	1 χρόνος	41 μέρες	4 μέρες	10 μέρες
8	218 τρις.	692 χρόνια	69¼ χρόνια	7 χρόνια	253 μέρες	25¼ μέρες

Πίνακας 9: Χρόνοι ανάκτησης κωδικών περίπτωση 5 - Όλο το αλφάβητο και αριθμοί

Παραδείγματα

		Χρόνος				
Κωδικός	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
Epp1574	3.5 τρις.	11 χρόνια	1 χρόνος	41 μέρες	4 μέρες	10 μέρες
dim123	57 δις.	66 μέρες	6½ μέρες	16 μέρες	1½ μέρες	9½ λεπτά

Πίνακας 10: Χρόνοι ανάκτησης κωδικών περίπτωση 5- παραδείγματα

✧ Περίπτωση 6: Όλο το αλφάβητο (κεφαλαία και μικρά) και σύμβολα

Πλήθος χαρακτήρων: 86
Χαρακτήρες:
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz
<SP>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Κωδικός		**Χρόνος**				
Μάκρος	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
2	7.396	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
8	2.9 τετράκις	9.488 χρόνια	948 χρόνια	94 χρόνια	57 χρόνια	346 μέρες

Πίνακας 11: Χρόνοι ανάκτησης κωδικών περίπτωση 6 - Όλο το αλφάβητο και σύμβολα

Παραδείγματα

		Χρόνος				
Κωδικός	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
A@	7.396	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
D!m!Tr!s	2.9 τετράκις	9.488 χρόνια	948 χρόνια	94 χρόνια	57 χρόνια	346 μέρες

Πίνακας 12: Χρόνοι ανάκτησης κωδικών περίπτωση 6- Παραδείγματα

✧ Περίπτωση 7: Όλο το αλφάβητο (κεφαλαία και μικρά) αριθμοί και σύμβολα

Πλήθος χαρακτήρων: 96
Χαρακτήρες:
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz0123456789
<SP>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Κωδικός		**Χρόνος**				
Μάκρος	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
2	9.216	Αμέσως	Αμέσως	Αμέσως	Αμέσως	Αμέσως
3	884.736	88½ δευτ.	9 δευτ.	Αμέσως	Αμέσως	Αμέσως
4	85 εκατ.	2¼ ώρες	14 λεπτά	1½ λεπτά	8½ δευτ.	Αμέσως
5	8 δις.	9½ μέρες	22½ ώρες	2¼ ώρες	13½ λεπτά	1¼ λεπτά
6	782 δις.	2½ χρόνια	90 μέρες	9 μέρες	22 ώρες	2 ώρες
7	75 τρις.	238 χρόνια	24 χρόνια	2½ χρόνια	87 μέρες	8½ μέρες
8	7.2 τετράκις	22.875 χρόνια	2.287 χρόνια	229 χρόνια	23 χρόνια	2¼ χρόνια

Πίνακας 13: Χρόνοι ανάκτησης κωδικών περίπτωση 7 - Όλο το αλφάβητο αριθμοί και σύμβολα

Παραδείγματα

		Χρόνος				
Κωδικός	**Συνδυασμοί**	**Κλάση A**	**Κλάση B**	**Κλάση C**	**Κλάση D**	**Κλάση E**
D!m12	8 δις.	9½ μέρες	22½ ώρες	2¼ ώρες	13½ λεπτά	1¼ λεπτά
1a!A	85 εκατ.	2¼ ώρες	14 λεπτά	1½ λεπτά	8½ δευτ.	Αμέσως

Πίνακας 14: Χρόνοι ανάκτησης κωδικών περίπτωση 7- παραδείγματα

[19] http://www.lockdown.co.uk/?pg=combi&s=articles

Κεφάλαιο 9 Οδηγίες Ασφάλειας

Πρόσβαση στο διαδίκτυο

Η πρόσβαση στο Διαδίκτυο με οποιοδήποτε τρόπο και αν πραγματοποιείται (dial-up, ADSL, WLAN, Κινητή Τηλεφωνία), συνδέει τον υπολογιστή ή και άλλες συσκευές (π.χ. κινητά τηλέφωνα, PDA, smartphones κ.α.) με το παγκόσμιο Διαδίκτυο και ως εκ τούτου τον κάνουν προσβάσιμο από όλους τους άλλους υπολογιστές που είναι επίσης διασυνδεμένοι στο δίκτυο αυτό. Για το λόγο αυτό υπάρχει επιτακτική ανάγκη να γνωρίζουμε τους κινδύνους κατά την χρήση των υπηρεσιών πρόσβασης στο Διαδίκτυο, έτσι ώστε να χρησιμοποιήσουμε κατάλληλα μέτρα προφύλαξης και να αποκομίσουμε το μέγιστο από την τεχνολογία αυτή, διευκολύνοντας τη ζωή μας. Όπως και με την τηλεφωνία, οποιαδήποτε χρήση ηλεκτρονικής επικοινωνίας του Διαδικτύου πραγματοποιείται μέσω διάφορων τεχνολογιών επικοινωνίας που συνδέουν τον αποστολέα με τον παραλήπτη (και αντίστροφα), είτε αυτοί βρίσκονται κοντά είτε σε αντιδιαμετρικά σημεία του κόσμου. Είναι σαφές πως η επικοινωνία αυτή μεταφέρεται από διάφορα σημεία και διαμέσου πολλαπλών τηλεπικοινωνιακών παρόχων και παρόχων υπηρεσιών, πολλές φορές σε διαφορετικές χώρες και με διαφορετικά μέσα επικοινωνίας (καλώδια χαλκού, οπτικές ίνες, ασύρματη και δορυφορική σύνδεση, κ.α.). Η χρήση των τηλεπικοινωνιακών υπηρεσιών αποσκοπούν στην πρόσβαση στο διαδίκτυο και στις υπηρεσίες του διαδικτύου όπως και στην επικοινωνία μεταξύ αποστολέα και παραλήπτη. Ο τρόπος χρήσης των υπηρεσιών αυτών θα πρέπει να είναι τέτοιος, ώστε το περιεχόμενο να γνωστοποιείται μόνο εκεί που απαιτείται για να διεκπεραιωθεί η συγκεκριμένη υπηρεσία και η πραγματοποίηση της επικοινωνίας αυτής, να μην εμπεριέχει κινδύνους απώλειας δεδομένων, οικονομικών στοιχείων ή άλλων μέσων που χρησιμοποιούνται κατά τη διάρκειά της. Για το λόγο αυτό θα πρέπει να λαμβάνουμε μέτρα ασφάλειας στο σπίτι μας, στις συσκευές που χρησιμοποιούμε για την επικοινωνία αυτή και στα δεδομένα (συμπεριλαμβανομένου της τηλεφωνίας) που ανταλλάσουμε.
Συγκεκριμένα:

1. **Φυσική Ασφάλεια στο σπίτι μας.** Όλη η επικοινωνία από το σπίτι μας συνήθως περνάει από ένα ή περισσότερα ζευγάρια από καλώδια όπου παλιότερα συνδέαμε το τηλέφωνό μας. Εκεί συνδέεται και το απλό dial up modem ή τώρα πια το ADSL modem ή router επιπλέον του απλού τηλεφώνου μας. Θα πρέπει να βεβαιωθούμε πως τα καλώδια αυτά δεν είναι εκτεθειμένα στην είσοδο του σπιτιού ή του διαμερίσματος και της πολυκατοικίας μας και ότι οι τυχόν διανεμητές της τηλεφωνίας στην είσοδο είναι κλειδωμένοι και δεν είναι προσβάσιμα τα καλώδια αυτά από άλλους ενοίκους ή τρίτους. Συνήθως οι κατανεμητές αυτοί είναι στην είσοδο σε κάθε πολυκατοικία και δυστυχώς τις περισσότερες φορές είναι εκτεθειμένοι**.** Ρωτήστε και ενημερώστε το διαχειριστή σας (εάν κατοικείτε σε πολυκατοικία), έτσι ώστε να διασφαλιστούν**.** Εφόσον κάποιος μπορεί να αποκτήσει φυσική πρόσβαση στα καλώδια αυτά είναι δυνατόν να υποκλέψει τα δεδομένα που διακινούνται. Εφόσον μάλιστα τα δεδομένα αυτά δεν είναι κρυπτογραφημένα μπορεί κανείς να συνδεθεί σε συσκευές που είναι συνδεμένες εκείνη τη στιγμή και να προκαλέσει απώλεια δεδομένων στον υπολογιστή μας. Για το σκοπό αυτό είναι ακόμα πιο επιτακτική η ανάγκη να χρησιμοποιείται κρυπτογράφηση.

2. **Ασύρματο Προσωπικό Δίκτυο στο σπίτι μας (WLAN) και ασύρματη τηλεφωνία (DECT).** Το ασύρματο δίκτυο στο σπίτι μας μέσω της τεχνολογίας WLAN που συνήθως διαθέτουν τα ADSL modem ή και τα ασύρματα τηλέφωνα τύπου DECT απλοποιούν την χρήση του Διαδικτύου και την διασύνδεση διάφορων υπολογιστών και συσκευών πρόσβασης (PSTN/ISDN/ADSL modem). Ωστόσο αποτελούν ταυτόχρονα και σημεία ανασφάλειας στην περίπτωση που δεν παραμετροποιηθούν κατάλληλα. Τα ασύρματα τοπικά δίκτυα θα πρέπει:
α) να ασφαλίζονται με κωδικούς ασφάλειας και κρυπτογράφηση και
β) να μην ανακοινώνεται το όνομα του συγκεκριμένου τοπικού μας δικτύου (SSID).
Η κρυπτογράφηση τύπου WEP θεωρείται ανασφαλής και για το λόγο αυτό πρέπει να χρησιμοποιείται WPA/WPA2. Για την κρυπτογράφηση τύπου WPA/WPA2 θα πρέπει να χρησιμοποιούνται κωδικοί ασφάλειας με τυχαίους χαρακτήρες (αριθμοί, πεζά και κεφαλαία γράμματα, ειδικοί χαρακτήρες) τουλάχιστον μεγέθους 20 χαρακτήρων, ενώ συνίσταται να είναι μεγέθους 63 χαρακτήρων για μέγιστη ασφάλεια.

Στην περίπτωση ελεύθερης πρόσβασης στο ασύρματο δίκτυο του σπιτιού μας, είναι δυνατόν κάποιος γείτονάς μας να αποκτήσει πρόσβαση στους δικούς μας υπολογιστές, τα δεδομένα και στο διαδίκτυο, λόγω της αλληλοεπικάλυψης των δικτύων αυτών. Σε δημόσια δίκτυα ασύρματης πρόσβασης, η πρόσβαση δεν μπορεί να προστατευτεί μέσω κρυπτογράφησης και για το λόγο αυτό οι χρήστες θα πρέπει να είναι προσεκτικοί και να χρησιμοποιούν πάντα κρυπτογραφημένες υπηρεσίες εφόσον μεταφέρουν κρίσιμα στοιχεία όπως κωδικούς ασφάλειας, προσωπικά και οικονομικά δεδομένα (π.χ. https, E-mail over SSL, τεχνολογίες VPN, κα).

Τα ασύρματα τηλέφωνα τύπου DECT, είναι ψηφιακά (τα αναλογικά τείνουν να εκλείψουν) και με τον τρόπο αυτό είναι πιο ασφαλή. Ωστόσο, τα τηλέφωνα αυτά δεν προσφέρουν απόλυτη προστασία επειδή πολλά από αυτά δεν υποστηρίζουν την κρυπτογράφηση κατά την διάρκεια της συνομιλίας. Για μεγαλύτερη ασφάλεια συνίσταται να επιλέγονται συσκευές που υποστηρίζουν κρυπτογράφηση του ακουστικού με τη συσκευή βάσης που συνδέεται στο τηλεφωνικό δίκτυο (τα οποία δυστυχώς είναι ελάχιστα). Η πρόσβαση συγκεκριμένου ακουστικού στο σταθμό βάσης πραγματοποιείται μέσω κάποιο κωδικού (PIN). Ο κωδικός αυτός θα πρέπει να αλλαχτεί αμέσως μετά την προμήθεια του εξοπλισμού για να μην είναι δυνατόν να χρησιμοποιηθεί η συγκεκριμένη συσκευή με άλλο ακουστικό που δεν βρίσκεται στην κυριότητά μας. Επίσης θα πρέπει να αποφεύγεται η χρήση των ακουστικών σε μεγάλη απόσταση από την βάση για να αποφεύγεται η τυχαία συνακρόαση από τρίτους.

3. **Επικαιροποίηση λειτουργικού συστήματος και λογισμικό υπολογιστών ή συσκευών σύνδεσης στο Διαδίκτυο (Modem, ADSL Router)**. Κάθε υπολογιστής ή συσκευή απαιτεί λογισμικό (software) για να λειτουργήσει. Ένα μέρος του λογισμικού αυτού χρησιμοποιείται από τον ίδιο τον υπολογιστή και για την σύνδεσή του στο Διαδίκτυο. Το λογισμικό αυτό εν γένει μπορεί να έχει λάθη από τον κατασκευαστή του τα οποία διορθώνονται με ειδικές προσθήκες (software updates, patches, κα). Είναι δυνατόν χρήστες του Διαδικτύου να εκμεταλλευτούν τα λάθη αυτά, για να αποκτήσουν πρόσβαση στον υπολογιστή ή τη συσκευή πρόσβασης και στα δεδομένα (αρχεία, εικόνες, κλπ.) του χρήστη και να εγκαταστήσουν κακόβουλο λογισμικό (trojans, virus), δημιουργώντας προβλήματα ή και διαγραφή των αρχείων αυτών. Επίσης μπορεί αυτός ο υπολογιστής να χρησιμοποιηθεί για την εκμετάλλευση ευπαθειών άλλων υπολογιστών και με τον τρόπο αυτό να αποτελέσει ο ίδιος απειλή

για τρίτους. Για το σκοπό αυτό θα πρέπει ο υπολογιστής να είναι πάντοτε ενημερωμένος με τις τελευταίες προσθήκες του κατασκευαστή. Το ίδιο ισχύει και για συσκευές πρόσβασης στο Διαδίκτυο όπως ADSL modems, routers, κ.α., στα οποία το λογισμικό αυτό αναφέρεται σαν firmware. Το ίδιο ισχύει και για άλλες συσκευές πρόσβασης όπως PDA, κινητά τηλέφωνα, smartphones, στα οποία είτε ο ίδιος χρήστης μπορεί να κάνει αναβάθμιση του λειτουργικού συστήματος και firmware ή θα πρέπει να επισκεφθεί κάποιο κέντρο τεχνικής υποστήριξης της συγκεκριμένης συσκευής.

4. **Εγκατάσταση Λογισμικού Ασφάλειας (Firewall, AntiVirus, AntiSpyware, κ.α.)**. Κάθε υπολογιστής θα πρέπει να έχει εγκατεστημένο λογισμικό ασφάλειας όπως firewall, antivirus, antispyware, κα. Σε πολλές περιπτώσεις ο ίδιος ο κατασκευαστής προμηθεύει μερικώς τέτοιο λογισμικό μαζί με το λειτουργικό σύστημα του υπολογιστή (π.χ. Microsoft Windows Firewall), το οποίο πρέπει να συμπληρωθεί με επιπλέον λογισμικό ασφάλειας όπως antivirus. Σε πολλές περιπτώσεις και σε μεγάλα δίκτυα χρηστών, ειδικές συσκευές τύπου firewall προστατεύουν τους υπολογιστές μη επιτρέποντας την πρόσβαση σε αυτούς από το Διαδίκτυο. Τέτοιες συσκευές firewall είναι ήδη ενσωματωμένες στις συσκευές πρόσβασης στο Διαδίκτυο μέσω ADSL (ADSL modem/router) και θα πρέπει να ενεργοποιούνται όπου είναι διαθέσιμες.

5. **Αλλαγή προσωρινών κωδικών ασφάλειας (default passwords) και χρήση προσωπικών κωδικών ασφάλειας**. Κάθε κωδικός ασφάλειας που υπάρχει είτε σε κάποιον υπολογιστή είτε σε κάποια άλλη συσκευή σύνδεσης (π.χ. ADSL modem/router) θα πρέπει να αλλάζεται από τον χρήστη αρχικά και περιοδικά, έτσι ώστε να είναι σίγουρος ο χρήστης πως μόνο αυτός έχει τη δυνατότητα πρόσβασης στη συσκευή αυτή. Επίσης κάθε κωδικός ασφάλειας που δίνεται από υπηρεσίες Διαδικτύου συνίσταται να αλλάζεται και αυτός την πρώτη φορά, έτσι ώστε η πρόσβαση με τους συγκεκριμένους κωδικούς να είναι δυνατή μόνο από τον ίδιο.

6. **Μη κοινοποίηση κωδικών ασφάλειας σε οποιονδήποτε**. Οι κωδικοί ασφάλειας (passwords) είναι προσωπικοί και δεν πρέπει σε καμία περίπτωση να τους καταγράφουμε σε χαρτί ή να τους μεταδίδουμε μέσω E-mail ή με άλλο τρόπο. Επίσης, οι κωδικοί αυτοί δεν πρέπει να κοινοποιούνται σε τρίτους ή σε υπηρεσίες του Διαδικτύου άλλες από αυτές για τις οποίες έχουν εκδοθεί. Σε κάθε περίπτωση που πρέπει να χρησιμοποιήσουμε κωδικούς ασφάλειας θα πρέπει να προτιμούμε να χρησιμοποιούμε κρυπτογραφημένες μεθόδους (https, SSL, κ.λπ.).

7. **Μη εκτέλεση και εγκατάσταση αγνώστου λογισμικού από οποιαδήποτε πηγή και εάν προέρχεται αυτό (Web, E-mail, download, κ.α.).** Η εγκατάσταση οποιουδήποτε λογισμικού από το Διαδίκτυο εμπεριέχει κινδύνους διότι είναι δυνατόν, μαζί με το λογισμικό αυτό να εγκατασταθεί και επιπλέον λογισμικό με ιούς, spyware, trojans κ.α., τα οποία μπορούν να υποκλέψουν ή να καταστρέψουν δεδομένα από τον υπολογιστή μας. Θα πρέπει κάθε τέτοιο λογισμικό να ελέγχεται πρώτα με λογισμικό ασφάλειας (antivirus, antispyware, κ.α.), και να εγκαθιστούμε μόνο λογισμικό από προμηθευτές που είναι αναγνωρισμένοι. Το ίδιο ισχύει και για οποιοδήποτε εκτελέσιμο πρόγραμμα και με οποιοδήποτε τρόπο αυτό έχει έρθει στην κυριότητάς μας (π.χ. με CD, USB Stick, κ.λπ.). Θα πρέπει απαραιτήτως πριν την χρήση του να ελεγχθεί με λογισμικό ασφάλειας.

8. **Χρήση κρυπτογράφησης (https, E-mail over SSL, E-mail Personal Certificates, κ.α.)**. Κάθε φορά που επικοινωνούμε κρίσιμες πληροφορίες (username/password, προσωπικά δεδομένα, οικονομικά δεδομένα, αριθμοί πιστωτικών καρτών) θα πρέπει να είμαστε βέβαιοι πως η επικοινωνία αυτή είναι κρυπτογραφημένη. Θα πρέπει να είμαστε πολύ προσεκτικοί και να αρνούμαστε να χρησιμοποιούμε ιστοσελίδες που μας ζητούν τέτοια στοιχεία χωρίς η ίδια η ιστοσελίδα να είναι κρυπτογραφημένη (που είναι γνωστό από την χρήση https αντί http στον browser). Όσο αφορά το ηλεκτρονικό ταχυδρομείο (e-mail), θα πρέπει εδώ να διαχωρίσουμε (α) την κρυπτογραφημένη επικοινωνία που λαμβάνει μέσω του πρωτοκόλλου SSL από (β) την κρυπτογράφηση και υπογραφή των ίδιων των δεδομένων που μεταδίδονται (π.χ. του ηλεκτρονικού ταχυδρομείου) μέσω των προσωπικών πιστοποιητικών. Η κρυπτογράφηση των δεδομένων (π.χ. e-mail) μέσω προσωπικών πιστοποιητικών διασφαλίζει τα δεδομένα από οποιοδήποτε τρίτο που μεσολαβεί για την μετάδοση των στοιχείων αυτών και μόνο ο τελικός παραλήπτης έχει την δυνατότητα ανάγνωσής τους.

Η χρήση https ή e-mail over SSL διασφαλίζει την κρυπτογραφημένη μετάδοση από τον υπολογιστή του χρήστη μέχρι τον web ή e-mail server και χρησιμοποιείται κυρίως για την διασφάλιση των κωδικών πρόσβασης που απαιτούνται για τις υπηρεσίες αυτές. Επειδή όμως η μετάδοση των ηλεκτρονικών μηνυμάτων (e-mail) πραγματοποιείται μέσω πολλαπλών συστημάτων και τα μηνύματα αυτά παραμένουν στη θυρίδα του παραλήπτη μέχρι ό ίδιος να τα παραλάβει, για την ασφάλεια των ίδιων των μηνυμάτων συνίσταται επιπλέον η χρήση κρυπτογράφησης με την χρήση πιστοποιητικών ασφάλειας.

Συγκεκριμένα θα πρέπει να χρησιμοποιούμε:

a) *Https* για επικοινωνία με ιστοσελίδες (Web sites) και με υπηρεσίες webmail όπως hotmail, yahoo, Gmail. Κατά την χρήση https θα πρέπει να είμαστε προσεκτικοί και να μην εμπιστευόμαστε πιστοποιητικά ιστοσελίδων που έχουν λήξη ή έχουν προβλήματα, μιας και αυτά αποτελούν ενδείξεις για παράνομες ιστοσελίδες τύπου Phishing .

b) *E-mail over SSL* για την επικοινωνία με τους εξυπηρετητές e-mail (e-mail servers) χρησιμοποιώντας POP3 over SSL και IMAP over SSL για την ανάγνωση των μηνυμάτων και SMTP over SSL για την αποστολή.

c) *κρυπτογράφηση* ηλεκτρονικών μηνυμάτων μέσω προσωπικών πιστοποιητικών

9. **Ηλεκτρονικό Ταχυδρομείο**. Η χρήση της υπηρεσίας ηλεκτρονικού ταχυδρομείου περιλαμβάνει τη σύνδεση με τους εξυπηρετητές (mail servers) της υπηρεσίας ηλεκτρονικού ταχυδρομείου, για την ανάγνωση ή την αποστολή ηλεκτρονικών μηνυμάτων συνήθως μέσω ειδικών προγραμμάτων ανάγνωσης (π.χ. Outlook, Outlook Express, Windows Mail, Windows Live Mail, Mozilla Thunderbird, κ.λπ.). Η σύνδεση συνήθως εμπεριέχει έναν έλεγχο πρόσβασης μέσω username και password και πραγματοποιείται μέσω των πρωτοκόλλων POP3 και IMAP για την ανάγνωση των μηνυμάτων και SMTP για την αποστολή.

Για την ασφάλεια των κωδικών αυτών θα πρέπει η σύνδεση να πραγματοποιείται μέσω τεχνολογίας SSL, που σημαίνει πως οι κωδικοί αυτοί μεταφέρονται κρυπτογραφημένοι μέχρι τους E-mail servers της εταιρείας. Η χρήση SSL

πραγματοποιείται με την κατάλληλη παραμετροποίηση των προγραμμάτων ανάγνωσης e-mail.
Η τεχνολογία αυτή διασφαλίζει το απόρρητο των κωδικών ασφαλείας και των ηλεκτρονικών μηνυμάτων από το σημείο παρουσίας του χρήστη (προσωπικός υπολογιστής). Τα ίδια τα ηλεκτρονικά μηνύματα όμως δεν είναι κρυπτογραφημένα. Για να είναι δυνατόν η κρυπτογράφηση των ηλεκτρονικών μηνυμάτων θα πρέπει να μας έχει γνωστοποιηθεί το πιστοποιητικό του παραλήπτη. Δηλαδή με το δικό μας πιστοποιητικό υπογράφουμε τα μηνύματα και ο παραλήπτης μπορεί να επιβεβαιώσει πως έχουν αποσταλεί από εμάς και με το πιστοποιητικό του παραλήπτη κρυπτογραφούμε τα μηνύματα που αποστέλλουμε προς αυτόν. Η κρυπτογράφηση δηλαδή των μηνυμάτων απαιτεί να υπάρχει κάποιο πιστοποιητικό του παραλήπτη. Τα προσωπικά πιστοποιητικά εκδίδονται από σχετικούς οργανισμούς, συνήθως κοστίζουν και θα πρέπει για να είναι δυνατή η ανταλλαγή κρυπτογραφημένων μηνυμάτων, να συμφωνήσουν και οι δύο εμπλεκόμενοι (αποστολές και παραλήπτης).

Σε κάθε περίπτωση συνίσταται η χρήση E-mail over SSL και https για την επικοινωνία με τις υπηρεσίες ηλεκτρονικού ταχυδρομείου ανεξάρτητα εάν ο χρήστης χρησιμοποιεί προσωπικά πιστοποιητικά (ή επιπλέον). Στην περίπτωση επικοινωνίας με υπηρεσίες ηλεκτρονικού ταχυδρομείου τύπου hotmail, yahoo, Gmail συνίσταται η χρήση https εάν αυτή είναι διαθέσιμη.

10. **Phishing**. Το phishing βασίζεται στην απόσπαση κυρίως οικονομικών στοιχείων (πιστωτικές κάρτες ή στοιχεία πρόσβασης username και password τραπεζικών λογαριασμών χρηστών), μέσω απάτης. Ο χρήστης δηλαδή προτρέπεται να εισάγει τα στοιχεία αυτά σε κάποια ιστοσελίδα που μοιάζει με την ιστοσελίδα που συνήθως χρησιμοποιεί. Με τον τρόπο αυτό αποσπώνται τα στοιχεία αυτά και κατόπιν χρησιμοποιούνται για την απόσπαση χρημάτων.

11. **Dialers**. Οι dialers είναι προγράμματα που έχουν εγκατασταθεί είτε μέσω κάποιου τρίτου προγράμματος που έχουμε χρησιμοποιήσει, εγκαταστήσει είτε μέσω συστημάτων που δεν έχουν επικαιροποιηθεί και για το λόγο αυτό είναι ευπαθή σε επιθέσεις. Τα προγράμματα αυτά συνδέονται εν αγνοία του χρήστη σε τηλεφωνικές γραμμές υψηλής χρέωσης διαμέσου του modem του χρήστη με σκοπό την οικονομική απάτη. Με την χρήση τεχνολογιών ADSL, η απειλή αυτή έχει ελαττωθεί εφόσον ο υπολογιστής δεν συνδέεται απευθείας σε τηλεφωνική σύνδεση.

12. **Προσεκτική Χρήση Οικονομικών και Προσωπικών Στοιχείων**. Η χρήση και μετάδοση οποιονδήποτε προσωπικών (όνομα, διεύθυνση, τηλέφωνο, E-mail) και οικονομικών στοιχείων (Τραπεζικοί Λογαριασμοί, Πιστωτικές Κάρτες) θα πρέπει να γίνεται προσεκτικά και θα πρέπει να είμαστε σίγουροι για την εταιρεία ή τον οργανισμό στον οποίο κοινοποιούμε τα στοιχεία αυτά. Είναι γνωστό ότι ακόμα και απλά στοιχεία όπως το e-mail που χρησιμοποιούμε σε κάποιες ιστοσελίδες ή Forums συλλέγονται από ειδικά προγράμματα και χρησιμοποιούνται κατόπιν για spam. Επίσης τα οικονομικά στοιχεία θα πρέπει να δίνονται με προσοχή και η επικοινωνία θα πρέπει να πραγματοποιείται κρυπτογραφημένα.
Για την προσωπική μας ασφάλεια περιορίζουμε τις προσωπικές πληροφορίες που δίνουμε σε ιστοσελίδες κοινωνικής δικτύωσης (π.χ. myspace, facebook, twitter, κ.α.) για να αποφύγουμε πιθανή κλοπή της ταυτότητάς μας (Identity theft), που μπορεί να έχει προσωπικές και οικονομικές συνέπειες. Στην περίπτωση που θέλουμε να χρησιμοποιήσουμε τις συγκεκριμένες υπηρεσίες, θα ήταν επιθυμητό να

εκμεταλλευτούμε τις δυνατότητες των συγκεκριμένων ιστοσελίδων για περιορισμό της πρόσβασης στις πληροφορίες που ανεβάζουμε και να ελέγχουμε ποιοι έχουν πρόσβαση.

Θα πρέπει εδώ να σημειώσουμε πως το διαδίκτυο είναι τεράστιο με μεγάλες δυνατότητες αποθήκευσης δεδομένων. Οποιαδήποτε στοιχεία ή δεδομένα, από τη στιγμή που δημοσιευτούν στο διαδίκτυο είναι εύκολο να αντιγραφούν και να αποθηκευτούν από οποιονδήποτε και οποιαδήποτε υπηρεσία. Η διαγραφή των στοιχείων αυτών από το αρχικό σημείο δημοσίευσης δεν σημαίνει πως τα στοιχεία αυτά θα διαγραφούν και από τις άλλες υπηρεσίες του διαδικτύου που τυχόν έχουν αντιγράψει τα δεδομένα αυτά. Είναι σαφές λοιπόν πως από τη στιγμή που δημοσιεύσουμε κάτι στο διαδίκτυο, ουσιαστικά έχουμε χάσει τον έλεγχο διαχείρισης της πληροφορίας αυτής ακόμα και εάν τα διαγράψουμε κατόπιν. Επειδή το κόστος της ψηφιακής πληροφορίας είναι πολύ χαμηλό είναι δυνατόν η μετάδοση και διατήρησή τους να είναι ουσιαστικά μόνιμη. Επιπλέον οι μηχανές αναζήτησης (π.χ. Google) διατηρούν τα δεδομένα αυτά σε δικές τους βάσεις δεδομένων (για ταχύτερη προσπέλαση) ακόμα και για μήνες από τι στιγμή που έχουν διαγραφεί από τις αρχικές ιστοσελίδες.

Η διεθνής ομάδα εργασίας για την προστασία των δεδομένων στις τηλεπικοινωνίες έχει εκδώσει πρόσφατα οδηγό με συστάσεις για την χρήση των υπηρεσιών κοινωνικής δικτύωσης. Είναι σημαντικό να εκμεταλλευόμαστε την δυνατότητα ανώνυμης χρήσης των υπηρεσιών αυτών (όπου αυτό είναι δυνατόν), γεγονός που ισχύει γενικότερα για όλες τις υπηρεσίες του διαδικτύου (π.χ. και για τις υπηρεσίες ηλεκτρονικού ταχυδρομείου hotmail, yahoo, Gmail), χρησιμοποιώντας ψευδώνυμα (nicknames) αντί των πραγματικών μας ονομάτων (π.χ. σαν username).

Συγκεντρωτικά για την ασφαλή χρήση του διαδικτύου συνίστανται τα παρακάτω:

1. Προστατεύουμε τα καλώδια της τηλεφωνικής σύνδεσης στο διαμέρισμα μας, την πολυκατοικία μας ή σε οποιοδήποτε χώρο έχουμε εγκαταστήσει εξοπλισμό πρόσβασης στο διαδίκτυο ή στις υπηρεσίες διαδικτύου.

2. Αλλάζουμε τον κωδικό PIN της ασύρματης τηλεφωνικής μας συσκευής (DECT) και δεν την χρησιμοποιούμε μακριά από τον σταθμό βάσης της.

3. Ενεργοποιούμε κωδικό πρόσβασης και κρυπτογράφηση στο ασύρματο δίκτυο μας (WLAN) χρησιμοποιώντας WPA/WPA2 μόνο (όχι WEP) και ο κωδικός ασφάλειας πρέπει να έχει τουλάχιστον μέγεθος 20 χαρακτήρων ενώ συνίσταται να έχει μέγεθος 63 τυχαίων χαρακτήρων συμπεριλαμβανομένων και των ειδικών (special characters).

4. Ενημερώνουμε τακτικά το firmware του ADSL modem για την πρόσβαση στο διαδίκτυο ή οποιασδήποτε άλλης συσκευής χρησιμοποιούμε για το σκοπό αυτό.

5. Αλλάζουμε τον κωδικό (password) διαχείρισης του ADSL modem ή router.

6. Εγκαθιστούμε λογισμικό ασφάλειας στον προσωπικό μας υπολογιστή (Antivirus, Firewall)

7. Δεν κοινοποιούμε σε κανέναν τους παραπάνω κωδικούς και τα PIN ασφάλειας του εξοπλισμού μας (ADSL modem, κωδικός σύνδεσης στο διαδίκτυο, κωδικός WLAN, DECT PIN)

8. Αλλάζουμε περιοδικά τους παραπάνω κωδικούς έτσι ώστε να τους γνωρίζουμε μόνο εμείς οι ίδιοι.

9. Χρησιμοποιούμε πάντοτε https για υπηρεσίες διαδικτύου (Web sites) όταν εισάγουμε κωδικούς ασφαλείας ή άλλα προσωπικά ή οικονομικά στοιχεία και αριθμοί πιστωτικών καρτών. Ελέγχουμε τυχόν μηνύματα σχετικά με προβληματικά πιστοποιητικά ασφάλειας των ιστοσελίδων αυτών.

10. Χρησιμοποιούμε E-mail over SSL για την αποστολή και λήψη των μηνυμάτων του ηλεκτρονικού ταχυδρομείου.

11. Κρυπτογραφούμε τα ηλεκτρονικά μας μηνύματα εφόσον αυτό είναι δυνατόν (π.χ. μέσω των προσωπικών πιστοποιητικών).

13. Βεβαιωνόμαστε πως η ιστοσελίδα που εισάγουμε στοιχεία κωδικών ή προσωπικά και οικονομικά στοιχεία είναι όντως η ιστοσελίδα της συγκεκριμένης εταιρίας της οποίας την υπηρεσία θέλουμε να χρησιμοποιήσουμε για να αποφύγουμε το phishing.

14. Δεν απαντάμε σε e-mail εσωκλείοντας προσωπικά στοιχεία και δεν χρησιμοποιούμε links μέσα σε e-mail που μας προτρέπουν να δώσουμε προσωπικά στοιχεία και κωδικούς ασφαλείας.

15. Πάντα εισάγουμε το URL απευθείας στον εκάστοτε browser και ελέγχουμε τυχόν μηνύματα σχετικά με προβληματικά πιστοποιητικά ασφάλειας.

16. Ενεργοποιούμε τις επιλογές ελέγχου των ιστοσελίδων για phishing από τους browsers.

17. Σε περίπτωση αμφιβολιών σχετικά με την ταυτότητα της ιστοσελίδας, του πιστοποιητικού της ή προειδοποιήσεις από τον browser, δεν προχωράμε με την εισαγωγή των στοιχείων μέχρι να είμαστε απόλυτα σίγουροι.

18. Περιορίζουμε τις προσωπικές πληροφορίες που δίνουμε σε ιστοσελίδες κοινωνικής δικτύωσης (myspace, facebook, twitter, κα) και ελέγχουμε την πρόσβαση σε αυτές από αγνώστους που είναι επίσης μέλη των υπηρεσιών αυτών, για να αποφύγουμε πιθανή κλοπή της ταυτότητάς μας (Identity theft) που μπορεί να έχει προσωπικές και οικονομικές συνέπειες. Θα πρέπει να γνωρίζουμε πως από τη στιγμή που μια πληροφορία έχει γίνει δημόσια έχουμε χάσει ουσιαστική την δυνατότητα ελέγχου της.

19. Αποφεύγουμε να χρησιμοποιούμε το πραγματικό μας όνομα και χρησιμοποιούμε κυρίως ψευδώνυμα.

Βιβλιογραφία

URL

http://www.truecrypt.org

http://www.passwordmeter.com/

http://passwordsafe.sourceforge.net/

http://keepass.info/

http://securityxploded.com/firemaster.php

http://www.nirsoft.net/utils/astlog.html

http://www.lostpassword.com/asterisk.htm

http://www.magicaljellybean.com/keyfinder/

http://www.nirsoft.net/utils/wireless_key.html

http://www.nirsoft.net/utils/mailpv.html

http://www.nirsoft.net/utils/mspass.html

http://www.nirsoft.net/utils/dialupass.html

http://www.nirsoft.net/utils/chromepass.html

http://www.nirsoft.net/utils/passwordfox.html

http://www.rarlab.com/download.htm

http://www.elcomsoft.com/download.html

http://www.openwall.com/john/

http://www.oxid.it/cain.html

http://www.lockdown.co.uk/?pg=combi&s=articles

http://www.insomnia.gr/

http://www.pcw.gr/

http://el.wikipedia.org/wiki/

Password Cracking

http://www.lockdown.co.uk/?pg=combi&s=articles
http://lifehacker.com/5505400/how-id-hack-your-weak-passwords?skyline=true&s=i

http://www.cxo.eu.com/news/password-protected/

http://www.securityxploded.com/firemaster.php

http://www.robertpeaslee.com/index.php/reset-bios-passwords-an-explanation-and-tool/

http://www.askvg.com/how-to-reset-remove-bypass-a-bios-or-cmos-password/

http://www.hackeruniversity.gr/forum/

http://www.happyhacker.org/

http://www.thelab.gr/

http://www.computeractive.gr/

http://www.adslgr.com/

ΒΙΒΛΙΑ

Strebe M. Ασφάλεια δικτύων- εισαγωγή στη σύγχρονη τεχνολογία. 2005. Εκδόσεις Γκιούρδα.

E-BOOKS

OReilly. Security Power Tools. Aug.2007

McClure S. Scambray J. Kurtz G. Hacking Exposed.

ΕΛΛΗΝΙΚΑ ΜΗΝΙΑΙΑ ΠΕΡΙΟΔΙΚΑ

Total Xaker

PC World

Computer Active

Computer για όλους

PC Magazine