Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Πτυχιακή εργασία

ΑΝΩΝΥΜΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΤΟ ΙΝΤΕΡΝΕΤ

Δουλγεράκη Καλλιόπη (ΑΜ: 1382)
E-mail: p.doulgeraki@hotmail.com
Κάππα Βιργινία (ΑΜ: 1389)
E-mail: veraagg@hotmail.com

Ηράκλειο – 27/1/2010

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

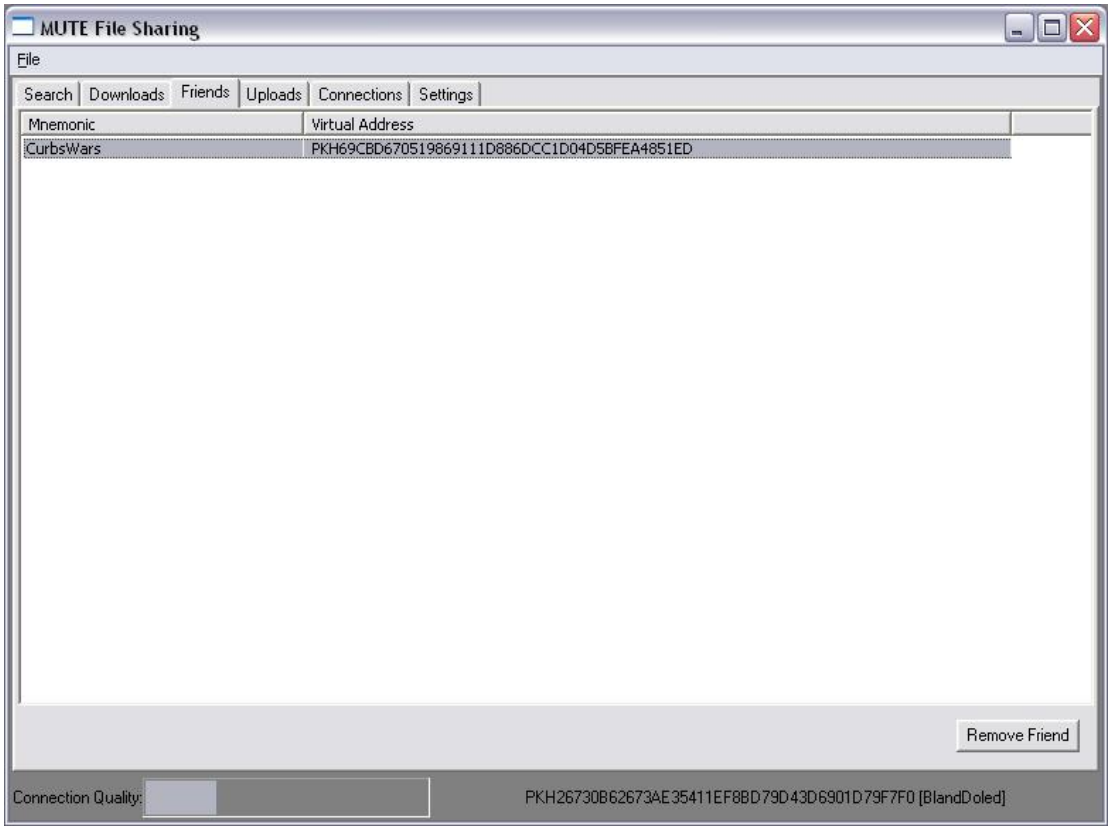
Υπεύθυνη Δήλωση*: Βεβαιώνουμε ότι είμαστε συγγραφείς αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχουμε αναφέρει τις όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνουμε ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμάς προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τον εισηγητή καθηγητή Δρ. Μανιφάβα Χαράλαμπο , ο οποίος μας επόπτευε στην πτυχιακή εργασία μας, τις οικογένειές μας για τη συμπαράστασή τους, και έναν καλό μας φίλο και συνάδελφο, τον Δανιηλίδη Ιωάννη για την πολύτιμη βοήθειά του.

Πίνακας Περιεχομένων

Πίνακας Εικόνων



Πίνακας Πινάκων

Κεφάλαιο 1 Εισαγωγή

1.1 Σκοπός

Ο σκοπός της ανωνυμίας είναι να προστατεύει την ιδιωτικότητά μας, την ελεύθερη έκφραση των απόψεών μας, την ηλεκτρονική μας ψήφο, την φαρμακευτική μας αγωγή, τα οικονομικά μας θέματα. Η ανωνυμία είναι ένας μηχανισμός που επιτρέπει στους ανθρώπους να εξερευνούν και να πειραματίζονται, να κινούνται μακριά από την κοινωνική αποδοκιμασία άσχετα αν οι πράξεις τους έχουν εγκληματικό χαρακτήρα ή όχι.

Πότε άλλοτε δεν υπήρξε μεγαλύτερη ανάγκη για ανωνυμία και προστασία ιδιωτικού απορρήτου στο Internet.[1] Κυβερνήσεις, οργανισμοί και πολυεθνικές εταιρείες επιχειρούν -καθένας για τους δικούς τους λόγους- να καταγράψουν, να ελέγξουν ή ακόμα και να περιορίσουν τις διαδικτυακές συνήθειες των κυβερνοπολιτών. Ποιες όμως είναι οι επιλογές που έχετε ώστε να διώξετε από πάνω σας τα αδιάκριτα μάτια;

Ξεκινώντας σχεδόν από το 1995 και φθάνοντας κατά την τελευταία πενταετία στην ολοκλήρωση, το Internet γνώρισε μια μετεξέλιξη που το μεταμόρφωσε από ένα άκρως δημοκρατικό forum σε ένα εμπορευματοποιημένο μέσο, που είναι στα χέρια κρατικών και ιδιωτικών φορέων. Φορέων, που στην πλειοψηφία τους επιχειρούν-και συνήθως κατορθώνουν να καταγράφουν και να περιορίζουν δραστηριότητες και συνήθειες των χρηστών του Internet για εμπορικούς αλλά και πολιτικούς λόγους.

Η ίδια η αρχιτεκτονική του Internet (κυρίως η server - client φιλοσοφία που διέπει το Διαδίκτυο και όλα τα χρησιμοποιούμενα πρωτόκολλά του) καθιστά εύκολη την καταγραφή της συμπεριφοράς των χρηστών, ενώ η ανάπτυξη ολοένα πιο "έξυπνων" μηχανισμών παρακολούθησης σε συνδυασμό με την γνωστοποίησή τους λειτουργούν ανασταλτικά στην εξάσκηση του αναφαίρετου δικαιώματος της ελευθερίας του λόγου.

Σε μια ακραία περιγραφή της υπάρχουσας κατάστασης, μπορούμε να πούμε ότι έχει διαμορφωθεί ένας νέος ψηφιακός άγραφος νόμος σε ορισμένες χώρες του πλανήτη που έχει ως εξής: "Είσαι ελεύθερος να πεις ό,τι θες, αρκεί να υποστείς τις συνέπειες". Οι κυριότερες απειλές που ενδέχεται να αντιμετωπίσετε ως χρήστες του Internet σήμερα, προέρχονται από κάποια επικοινωνία που ενδέχεται να έχουν είτε μέσω e-mail, σε chat rooms και message boards είτε μέσω instant messengers, είτε από άτομα που έχουν φυσική πρόσβαση στον υπολογιστή σας, είτε από διαχειριστές Web sites που επισκέπτεστε, είτε από ISPs και λοιπούς παροχείς δικτυακών υπηρεσιών είτε από Crackers, είτε από πολυεθνικές και διαφημιστικές εταιρείες, είτε ακόμα κι από κυβερνήσεις.

Η πτυχιακή αυτή εργασία μελετά και παρουσιάζει στην πράξη μια σειρά από εργαλεία που υποστηρίζουν την ανωνυμία στο διαδίκτυο. Πιο συγκεκριμένα, στην πτυχιακή αναλύονται τα παρακάτω:

- Ιστορική Αναδρομή

[1] http://www.inout.gr/showthread.php?t=19801

- Η ανωνυμία πριν από το Διαδίκτυο
- Ψευδωνυμία
- Παρουσίαση του Προβλήματος & Σημερινή Κατάσταση

- Η ανωνυμία στο Διαδίκτυο
  - E-cash
  - E-voting
  - Ανώνυμες IP

- Εφαρμογές που υποστηρίζουν την ανωνυμία
  - TOR (The Onion Router)
  - P2P (Peer to Peer system) anonymity
  - Ανώνυμοι remailers

και

- Ιδιωτική περιήγηση (Private Browsing)

Κεφάλαιο 2 Ιστορική Αναδρομή

2.1 Ιστορική αναδρομή της ανωνυμίας

2.1.1 Η ανωνυμία πριν από το Διαδίκτυο

Η λέξη «ανωνυμία» πρωτοεμφανίστηκε τον 16ο αιώνα, προέρχεται από την ελληνική γλώσσα και έχει δανειστεί στην αγγλική ως anonymity. [2] Σημαίνει χωρίς όνομα και συνήθως αναφέρεται σε άτομο του οποίου η ταυτότητα ή κάποια προσωπικά στοιχεία του είναι άγνωστα, ή οι «ανώνυμοι λίθοι», ή ο ανυπόγραφος όπως ένα «ανώνυμο έργο» ή μια «ανώνυμη επιστολή». Επίσης σημαίνει η δήλωση κάποιου ατόμου έτσι ώστε να μην είναι αναγνωρίσιμο εν μέσω κάποιου σετ στοιχείων ανωνυμίας, το οποίο σετ μπορεί να είναι ο λόγος που θέλει να διατηρήσει το άτομο την ανωνυμία του εκείνη την στιγμή.

Επιπλέον η ανωνυμία είναι ο μη προσδιορισμός χαρακτηριστικών (όπως ένα όνομα ή την περιγραφή της φυσικής εμφάνισης), ή ακόμα και το αποτέλεσμα απόρρητων χαρακτηριστικών. [3] Αυτό μπορεί να προκύψει από την έλλειψη ενδιαφέροντος για μάθηση της φύσης αυτών των χαρακτηριστικών, είτε από την προσπάθεια απόκρυψης των χαρακτηριστικά αυτών.

Ένα παράδειγμα για την πρώτη εκδοχή θα μπορούσε να είναι μια σύντομη συνάντηση με έναν άγνωστο, όταν η εκμάθηση των στοιχείων του δεν κρίνεται αναγκαία. Ένα παράδειγμα της τελευταίας εκδοχής θα μπορούσε να είναι η απόκρυψη των στοιχείων κάποιου, ο οποίος κρύβεται πίσω από την επιμέλεια των ειδών ένδυσης, όπως το χρώμα των μαλλιών, ουλές ή τατουάζ , για να αποφευχθεί η ταυτοποίηση.

Σε ορισμένες περιπτώσεις, η ανωνυμία επιτεύχθηκε και αθέλητα, όπως συμβαίνει συχνά με τα θύματα των εγκλημάτων ή πολέμου, όταν ένα σώμα ανακαλύπτεται και είναι σε μια τέτοια κατάσταση όπου τα φυσικά χαρακτηριστικά του χρησιμοποιούνται για τον προσδιορισμό του τα οποία δεν είναι πρόσφατα. Μια άλλη περίπτωση, όπου, ο νικητής της λαχειοφόρου αγοράς παραμένει ανώνυμος έως ότου γυρίσει στο πρακτορείο για την εξαργύρωσή της.

Όπως για παράδειγμα, η ιαπωνική αστυνομία το 2008 συνέλαβε έναν 51χρονο εφημεριδοπώλη με την κατηγορία ότι σκότωσε τη φίλη του, η οποία είχε κερδίσει 2 εκατομμύρια δολάρια στο λαχείο. Όπως μετέδωσε ένα από τα ιαπωνικά πρακτορεία, η σύλληψη έγινε ύστερα από τριετή έρευνα για την εξαφάνιση του θύματος το 2005, η οποία φαίνεται ότι είχε κρατήσει τα κέρδη της μυστικά από όλους, εκτός από τον φίλο της. Ο σύντροφός της ομολόγησε το έγκλημά του και παραδέχθηκε ότι

---

[2] http://en.wikipedia.org/wiki/Anonymity

[3] http://www.kazam.gr/online/node/128151

χρησιμοποίησε μέρος των κερδών για να εξοφλήσει οφειλές από την χρεοκοπημένη του επιχείρηση.

Η ανωνυμία, συνήθως, τον 16ο αιώνα αναφερόταν σε ιερές γραφές, εκκλησιαστικά ποιήματα και δημοτικά άσματα όλων των εθνών, των οποίων οι συγγραφείς ήταν άγνωστοι ή παρέμεναν κρυφοί. [4] Άλλωστε, αυτοί οι συγγραφείς ήταν κοινοί άνθρωποι και το όνομά τους ήταν πιο εύκολο να ξεχαστεί με την πάροδο του χρόνου.

Τα ανώνυμα βιβλία διακρίνονται ακόμη και σε αυτά που δεν ξέρουμε σε ποιον ανήκουν, όπως τα αποσπάσματα αγνώστου συγγραφέα, ή και των αγνώστων εκδοτών, και από τα αποσπάσματα των γνωστών συγγραφέων άγνωστων έργων. Το πλήθος αυτών είναι τέτοιο, ώστε, γύρω στα μέσα του 9ου αιώνα, υπολογίζονταν ότι το 1/3 των βιβλίων που υπήρχαν στις βιβλιοθήκες ανήκαν σε ανώνυμους.

Σε άλλα χάθηκε το όνομα του συγγραφέα, ή αναφέρονταν εσφαλμένα (έτσι σώθηκαν βίοι αρχαίων φιλοσόφων αναφερόμενοι συνήθως ως «ανωνύμου βίος Πλάτωνος - Αριστοτέλους»)κ.τ.λ. Άλλοι νεότεροι συγγραφείς τύπωσαν τα έργα τους χωρίς το όνομά τους ή το ψευδώνυμό τους σε εποχές τρομοκρατίας, χάρη στην ασφάλεια. Τα ονόματα των τελευταίων συγγραφέων, έχουν ήδη, κατά το πλείστον ανακαλυφθεί και έχουν αντικαταστήσει τα ψευδώνυμα.

Ένα αξιοσημείωτο ποσοστό της μεσαιωνικής λογοτεχνίας προέρχεται από ανώνυμους συγγραφείς. Το γεγονός αυτό οφείλεται στην έλλειψη γραπτών πηγών μιας συγκεκριμένης περιόδου, αλλά και στη διαφορετική ερμηνεία του συγγραφέα εκείνης της εποχής με τα σημερινά δεδομένα. Η συνηθέστερη λογοτεχνική μορφή των κειμένων που βρίσκονταν στις μεσαιωνικές βιβλιοθήκες ήταν τα εκκλησιαστικά κείμενα, καθώς οι καθολικοί ιερείς ήταν το πνευματικό κέντρο της κοινωνίας του Μεσαίωνα.

Θρησκευτικοί συγγραφείς και μελετητές, όπως ο Θωμάς Ακινάτης, συνέγραψαν θεολογικές και φιλοσοφικές πραγματείες, συχνά προσπαθώντας να συμβιβάσουν τις διδαχές των Ελλήνων και Ρωμαίων συγγραφέων και φιλοσόφων με τα εκκλησιαστικά δόγματα. Συνηθισμένο είδος γραφής αποτελούσαν κι οι "βίοι αγίων", που προσέφεραν ενθάρρυνση, αλλά και προειδοποίηση στους αναγνώστες. Οι μεσαιωνικοί συγγραφείς, συνήθως, αφηγούνταν ξανά και ωραιοποιούσαν ιστορίες που είχαν διαβάσει ή ακούσει παρά επινοούσαν νέες. Συνεπώς, η αναφορά του ονόματος ενός συγγραφέα δεν είχε ιδιαίτερη σημασία κι έτσι αγνοούμε τους συγγραφείς πολλών σημαντικών έργων.

2.1.2 Ψευδωνυμία

Η λέξη pseudonymity προέρχεται από το ψευδώνυμο, που σημαίνει 'ψεύτικο όνομα' , ενώ η ανωνυμία, σημαίνει την άγνωστη ή αδήλωτη πηγή, που περιγράφει μια κατάσταση της μπερδεμένης μεταμφιεσμένης ταυτότητας. Η διαφορά της ανωνυμίας

[4] http://en.wikipedia.org/wiki/Medieval_literature

και της ψευδωνυμίας στην τεχνολογία υπολογιστών είναι η εξής:[5] Η ανωνυμία διασφαλίζει την χρήση μιας υπηρεσίας από ένα χρήστη χωρίς να αποκαλύπτεται η ταυτότητά του, ενώ η ψευδωνυμία χρησιμοποιείται στις περιπτώσεις όπου η ανωνυμία δεν είναι εφικτή (on-line purchasing).

Η λέξη ψευδώνυμο σημαίνει το πλαστό όνομα με το οποίο εμφανίζεται κάποιος (συγγραφέας, καλλιτέχνης, επαναστάτης κτλ.), όταν θέλει να κρύψει την πραγματική του ταυτότητα.[6] Το ψευδώνυμο μπορεί να είναι καλλιτεχνικό, λογοτεχνικό, φιλολογικό, επαναστατικό ή συνωμοτικό.[7] Προσδιορίζει έναν κάτοχο, δηλ., ένα ή περισσότερα ανθρώπινα όντα που κατέχουν αλλά δεν αποκαλύπτουν τα αληθινά ονόματά τους.

Οι περισσότεροι κάτοχοι ψευδωνύμων χρησιμοποιούν τα ψευδώνυμα επειδή επιθυμούν να παραμείνουν ανώνυμοι, αλλά η ανωνυμία είναι δύσκολο να επιτευχθεί, και είναι συχνά γεμάτη με τα νομικά θέματα.[8] Πολλοί καλλιτέχνες, ηθοποιοί, τραγουδιστές, ποιητές, συγγραφείς, επιχειρηματίες, ποδοσφαιριστές, συνθέτες αλλά και αθλητικές ομάδες χρησιμοποιούν ψευδώνυμα. Ένα παράδειγμα ψευδωνύμου, είναι αυτό του James Bond, το οποίο είναι ψευδώνυμο του χαρακτήρα James St. John Smith.

Οι περισσότεροι ιστοχώροι που προσφέρουν ψευδωνυμία, διατηρούν τις πληροφορίες για τους χρήστες. Αυτές οι περιοχές είναι συχνά ευαίσθητες στις παράνομες διεισδύσεις τους σε μη δημόσια συστήματα βάσεων δεδομένων Παραδείγματος χάριν, το 2000, ένας Ουαλλός έφηβος έλαβε τις πληροφορίες για περισσότερους από 26.000 απολογισμούς πιστωτικών καρτών, συμπεριλαμβανομένης αυτής του Bill Gates. Το 2003, η VISA και MasterCard ανήγγειλαν ότι οι εισβολείς έλαβαν τις πληροφορίες για 5.6 εκατομμύρια πιστωτικές κάρτες. Περιοχές που προσφέρουν ψευδωνυμία, είναι επίσης τρωτές στις παραβιάσεις εμπιστευτικότητας.

Σε μια μελέτη για έναν διαδικτυακό τόπο, οι ερευνητές του Πανεπιστημίου Cambridge ανακάλυψαν ότι τα συστήματα που χρησιμοποιήθηκαν από αυτούς τους ιστοχώρους για να προστατεύσουν τα στοιχεία χρηστών θα μπορούσαν να συμβιβαστούν εύκολα, ακόμα κι αν το ψευδώνυμο κανάλι προστατεύεται από ισχυρή κρυπτογράφηση. Χαρακτηριστικά, το προστατευμένο ψευδώνυμο κανάλι υπάρχει μέσα σε ένα ευρύτερο πλαίσιο στο οποίο οι πολλαπλάσιες ευπάθειες υπάρχουν. Οι χρήστες ψευδωνύμων πρέπει να σημειώσουν ότι, λαμβάνοντας υπόψη τη τρέχουσα κατάσταση της εφαρμοσμένης μηχανικής ασφάλειας Ιστού, τα αληθινά ονόματά τους μπορούν να αποκαλυφθούν οποιαδήποτε στιγμή.

Η ανωνυμία ή η χρήση ψευδωνύμων στις επικοινωνίες μέσω υπολογιστών έχει ορισμένες φορές χρησιμοποιηθεί σε εκπαιδευτικές και εμπορικές εφαρμογές για να ενθαρρύνει ειλικρινείς απαντήσεις ή αμερόληπτες συναλλαγές.[9] Υπάρχουν όμως

---

[5] http://www.aegean.gr/culturaltec/economoud/modules/VM/Security%20&%20Privacy.pdf
[6] http://openitnow.blogspot.com/2007/06/blog-post_487.html
[7] http://en.wikipedia.org/wiki/Pseudonymity
[8] http://en.wikipedia.org/wiki/Pseudonym

[9] http://www.math.upatras.gr/~mboudour/articles/ktemy.html

δίκτυα επικοινωνιών, όπως, π.χ., το WELL, που δεν αποδέχονται την ανωνυμία. Είναι αλήθεια ότι έχει υποστηριχθεί η θετική αξία της ανωνυμίας σε περιπτώσεις που δημιουργούνται ευκαιρίες να πλασθούν εναλλακτικοί τύποι προσωπικότητας και να δοκιμασθούν καινούργιες μορφές σχέσεων. Σε επικοινωνιακά συστήματα μέσω υπολογιστών, στα οποία οι συνομιλητές παίζουν διάφορους ρόλους, η χρήση ψευδωνύμων πιστεύεται ότι "επιτρέπει τους ανθρώπους να είναι διαφορετικοί από τους 'εαυτούς τους' ή να υπερβούν τους εαυτούς τους και ότι άλλο κανονικά εκφράζουν".

Ακόμη, οι Matheson & Zanna (1990) υποστηρίζουν ότι οι ανώνυμοι ή οι ψευδώνυμοι συνομιλητές αισθάνονται πιο άνετα και είναι πρόθυμοι να αποκαλύψουν προσωπικές πληροφορίες, Έτσι, αναπτύσσονται μεταξύ τους σχέσεις κοινωνικής αλληλεξάρτησης και ίσως ακόμη και οικειότητας με την ελάττωση των περιορισμών των στερεοτύπων που προδιαγράφουν πρότυπα συμπεριφοράς μεγαλύτερης κοινωνικής ανεξαρτησίας. Αντιθέτως, συχνά συμβαίνει στις επικοινωνίες μέσω υπολογιστών η χρήση ανωνυμίας ή ψευδωνυμίας να κρύβει την προσωπική ταυτότητα με σκοπό να μειωθούν οι κοινωνικές απαγορεύσεις και να πραγματοποιηθούν κακεντρεχείς ή και υβριστικοί έντονοι διαξιφισμοί - flaming.

Μερικές φορές πάντως, η πρακτική της απόκρυψης ταυτοτήτων μπορεί να προστατεύσει τα μέλη ενός δημόσιου forum από εχθρικά προσκείμενες κοινωνικές αντιδράσεις, όταν τα μέλη αυτά εκφράζουν απόψεις που μπορούν να θεωρηθούν κοινωνικά αποκλίνουσες. Επιπλέον, τότε, θα μπορούσε να αποτραπεί η αναγνώριση εκείνων των μελών ενός τέτοιου φόρουμ επικοινωνίας, τα οποία η κοινή γνώμη θα μπορούσε να εκλάβει ως εκτρεπόμενα με κάποια έννοια.

Για παράδειγμα, η τελευταία περίπτωση αφορά κάποια από τα Νέα του USENET, στα οποία κυκλοφορεί πορνογραφικό υλικό. Το γεγονός όμως είναι ότι αργά ή γρήγορα ακόμη και οι ανώνυμοι συνομιλητές ενός επικοινωνιακού συστήματος μέσω υπολογιστών προχωρούν να κατασκευάσουν ταυτότητες για τους εαυτούς τους. Η γενική τάση σε τέτοιες επικοινωνιακές σχέσεις είναι ότι και οι ανώνυμοι και οι ψευδώνυμοι συνομιλητές δημιουργούν τις προσωπικές ταυτότητές τους με έναν ενεργό και συνεργατικό τρόπο μέσα από μια σειρά από διαδικασίες, όπως του κατονομασμού, της χρήσης υπογραφών, της δημιουργίας ρόλων και της αποκάλυψης προσωπικών στοιχείων.

Σύμφωνα με τον Myers, τα ονόματα των χρηστών επικοινωνιακών συστημάτων μέσω υπολογιστών "μετασχηματίζονται σε σήματα κατατεθέντα, χαρακτηριστικές προσωπικές οσμές, που χρησιμοποιούνται για να αναγνωρισθούν οι χρήστες είτε σαν φίλοι ή σαν εχθροί μέσα σε ένα κατά τα άλλα ασαφές και απρόσωπο επικοινωνιακό περιβάλλον." Με τον τρόπο αυτό, όχι μόνο μπορούν να δημιουργηθούν φανταστικές ταυτότητες, αλλά και να συμβεί κάποιοι ανώνυμοι χρήστες να αλλάξουν φύλο, τύπους εμφάνισης και διάφορες άλλες καθολικές όψεις της προσωπικότητάς τους.

Μια ακόμα πτυχή της ηλεκτρονικής αυτής “επανάστασης” είναι και η ανωνυμία την οποία έχουν το ελεύθερο να επιλέξουν οι χρήστες του διαδικτύου, χρησιμοποιώντας ψευδώνυμα.[10] Η δυνατότητα αυτή λειτουργεί συνήθως σαν ένα επιπλέον “κίνητρο”

[10] http://www.odigitis.gr/2008/12/07/blogs/

για την εμπέδωση αυτής της καινούριου τύπου "ελευθερίας έκφρασης". Το ένα βέβαια ζήτημα είναι το πόσο "ανώνυμη" είναι τελικά αυτή η ανωνυμία, αν λάβει κανείς υπ' όψιν το πλήθος ηλεκτρονικών ιχνών που αφήνει ο καθένας μας στο πέρασμά του από το διαδίκτυο.

Ωστόσο, ούτε αυτό είναι το μοναδικό ή το κύριο πρόβλημα. Πίσω από τα διάφορα ψευδώνυμα μπορεί να κρύβεται ο οποιοσδήποτε, ενώ δεν είναι λίγες οι φορές που χρήστες δημιουργούν μια σειρά από διαφορετικά ψευδώνυμα-"χαρακτήρες". Αυτό το γεγονός υποβαθμίζει την όποια επικοινωνία, αλλά ακόμα κι αν κάποιος τη χρησιμοποιεί καλοπροαίρετα, αφήνει να υπάρχουν γύρω από αυτόν και τους σκοπούς του, συγχύσεις και παρανοήσεις. Το περιεχόμενο της επικοινωνίας που υπάρχει έτσι, αλλοιώνεται και από αυτό το χαρακτηριστικό των blogs και όχι μόνο. Αποξενώνει τον χρήστη, περνάει την αντίληψη ότι δεν μπορούμε να λέμε τα πράγματα στο φως του ήλιου, παίρνοντας και την ευθύνη των όσων λέμε, αλλά πως είναι καλύτερα ή ίσως πιο ανώδυνα να τα λέμε κρυμμένοι πίσω από διάφορα προσωπεία.

Υπάρχουν πολλοί λόγοι για τους οποίους ένα άτομο μπορεί να επιλέξει να συσκοτίσει την ταυτότητά του και να γίνει ανώνυμο. Αρκετοί από αυτούς τους λόγους, είναι νόμιμοι και θεμιτοί, πολλές πράξεις φιλανθρωπίας πραγματοποιούνται ανώνυμα, γιατί οι ευεργέτες δεν επιθυμούν, για οποιοδήποτε λόγο, να αναγνωρίζονται για τη δράση τους. Επίσης, κάποιος που θεωρεί ότι απειλείται από κάποιον άλλο θα μπορούσε να προσπαθήσει να κρύψει τα στοιχεία του από την απειλή πίσω από διάφορα μέσα της ανωνυμίας, όπως ένας μάρτυρας σε ένα έγκλημα που μπορεί να επιδιώξει να αποφύγει την τιμωρία.

Ένα χαρακτηριστικό παράδειγμα, όπου αποκαλύφθηκε η ανωνυμία μετά από αρκετά χρόνια, είναι αυτό της υπόθεσης της πρώην Τουρκάλας πρωθυπουργού, Tansu Ciller, ήρθαν στο φως, στο πλαίσιο της εκδίκασης της υπόθεσης Ergenekon.[11] Σύμφωνα με έγγραφο - ντοκουμέντο των Μυστικών Υπηρεσιών της Τουρκίας, που παρουσιάστηκε στο δικαστήριο για την παρακρατική οργάνωση, η Ciller φέρεται να είναι πράκτορας της CIA με την κωδική ονομασία «Το Τριαντάφυλλο της Πόλης». Το ντοκουμέντο αυτό έφτασε στα χέρια της Μυστικής Υπηρεσίας το 2002.

Σύμφωνα με το ντοκουμέντο αυτό, η πρώην πρωθυπουργός στρατολογήθηκε το 1967, πέρασε από ειδική εκπαίδευση από τη μυστική υπηρεσία, ενώ έκανε διδακτορικό στο πανεπιστήμιο Yale. Οι πρώτες φήμες για την υπόθεση αυτή και τη δραστηριότητα της Ciller πρωτοκυκλοφόρησαν το 1999. Όταν πια εκλέχθηκε πρωθυπουργός το 1993 έως το 1996, η αντιπολίτευση απευθύνθηκε σε ένα αμερικανικό δικηγορικό γραφείο, ώστε να ερευνήσει τα περιουσιακά της στοιχεία. Η έρευνα του συγκεκριμένου γραφείου μεταφέρεται στην Πράγα, καθώς εκεί διαμένει ένας πρώην πράκτορας της CIA με την κωδική ονομασία Fish, ο οποίος έδωσε τα στοιχεία για την Ciller. Περιέργως, ο Fish πέθανε λίγο αργότερα σε πυρκαγιά που ξέσπασε στο σπίτι του.

Τέλος, το ονομαζόμενο "αρχείο υπογραφής," που επισυνάπτεται στο τέλος των μηνυμάτων ηλεκτρονικής επικοινωνίας, αποτελεί "ένα από τα αμεσότερα και

[11] http://www.zougla.gr/news.php?id=44994

παραστατικότερα χαρακτηριστικά σημάδια της ταυτότητας". Σε μια τέτοια υπογραφή, πέρα από το όνομα και την διεύθυνση του αποστολέα του ηλεκτρονικού μηνύματος, συνήθως συμπεριλαμβάνονται παρατιθέμενα χωρία, αποποιητικές δηλώσεις, είτε προσωπικές ή του εργοδότη, και σχέδια που κατασκευάζονται με χαρακτήρες ASCII (σημεία στίξεως και γράμματα).

Από τα παραπάνω, μπορεί κανείς να συμπεράνει ότι οι επικοινωνίες μέσω υπολογιστών αποτελούν στην πραγματικότητα μια σφαίρα κοινωνικών πρακτικών. Είναι μια κοινωνική σφαίρα, μέσα στην οποία και κατά την διάρκεια των επικοινωνιακών σχέσεων οι άνθρωποι αλληλεπιδρούν είτε πλάθοντας νέους τύπους προσωπικοτήτων ή αναδημιουργώντας τις δικές τους προσωπικότητες, καθώς βρίσκονται σε επικοινωνιακή αλληλεπίδραση με άλλους ανθρώπους, ή και τα δυο.

Μολονότι αυτές οι μορφές των διαδικασιών της διαχείρισης των ταυτοτήτων είναι κοινές σχεδόν σε όλες τις επικοινωνιακές πρακτικές των μέσων μαζικής επικοινωνίας, ο Mark Poster (1995) μας διαβεβαιώνει ότι στις επικοινωνίες μέσω υπολογιστών οι διαδικασίες αυτές είναι βαθύτερα ριζωμένες. Σύμφωνα με τον Poster, "η επικοινωνιακή απόδοση ενός ατόμου απαιτεί γλωσσικές ενέργειες αυτο-προσδιορισμού," με τις οποίες το άτομο αφενός είναι δέκτης επικοινωνίας, όταν διαβάζει και ερμηνεύει τα μηνύματα που δέχεται, και αφετέρου είναι πομπός, όταν απαντά συντάσσοντας μηνύματα και μεταδίδοντάς τα.

Θα μπορούσαμε να πούμε ότι ψευδώνυμη είναι η επικοινωνία εκείνη που αν και δεν περιέχει κανένα σαφές στοιχείο για την ταυτότητα του ενεργούντα αυτήν ως πραγματικού φυσικού ή νομικού προσώπου, ωστόσο περιέχει στοιχεία για τον προσδιορισμό και την αναγνωρισιμότητα κάποιας πλασματικής προσωπικότητας στην οποία αποδίδεται η επικοινωνία. [12] Αυτό συμβαίνει στην περίπτωση των συγγραφέων καθιερωμένων στην αγορά των αναγνωστών τους με το ψευδώνυμό τους.

Για παράδειγμα, η περίπτωση του μεγάλου Αμερικανού συγγραφέα Mark Twain. Η πρώτη νουβέλα που δημοσιεύθηκε από τον υπογράφοντα αυτήν Mark Twain, το ψευδώνυμο του μεγάλου Αμερικανού συγγραφέα Samuel Langhome Clemens, δεν δημιουργούσε στο αναγνωστικό κοινό καμία βεβαιότητα για την ταυτότητα του πραγματικού συγγραφέα. Ήταν δηλαδή ουσιαστικά ένα ανώνυμο κείμενο ενός άσημου—τότε—συγγραφέα που υπέγραφε με ψευδώνυμο που κανείς ή ελάχιστοι συμπολίτες του ήξεραν ότι αποδίδεται σε συγκεκριμένο φυσικό πρόσωπο.

Επίσης σε χώρες με απολυταρχικά καθεστώτα, οι συγγραφείς ήταν αναγκασμένοι να χρησιμοποιούν ψευδώνυμα ή να διατηρούν την ανωνυμία τους.[13] Παραδείγματος χάριν, ο συγγραφέας Μοχάμεντ Μουλεσεχούλ, ο οποίος χρησιμοποιεί το γυναικείο ψευδώνυμο Γιασμίνα Χάντρα. Γεννήθηκε το 1955 και σε ηλικία εννέα χρόνων μπήκε σε στρατιωτική σχολή. Αρχίζει να δημοσιεύει λογοτεχνικά κείμενα το 1984, ενώ έχει ήδη γίνει αξιωματικός. Η δυσπιστία με την οποία το στρατιωτικό κατεστημένο της χώρας του αντιμετωπίζει ένα στρατιωτικό λογοτέχνη, αλλά κυρίως ο εμφύλιος

[12] http://www.actionnemesis.com/v2/index.php?option=com_content&task=view&id=369&Itemid=53
[13] http://www.thessalonikibookfair.com/2006/html/docs/blackbook.pdf

πόλεμος στην Αλγερία τον αναγκάζει να περάσει, ως λογοτέχνης, στην πιο βαθιά παρανομία και να χρησιμοποιήσει ένα γυναικείο ψευδώνυμο.

Δημοσιεύοντας πλέον με το όνομα Γιασμίνα Χάντρα, θα γίνει πασίγνωστος πρώτα στη Γαλλία και ύστερα σε όλο τον κόσμο. Οι αστυνομικές του ιστορίες είναι πάντα συνδεδεμένες με την κοινωνικοπολιτική κατάσταση της χώρας του. Ο συνταγματάρχης -συγγραφέας διασφάλισε την ανωνυμία του πίσω από αυτό το γυναικείο ψευδώνυμο ως ένδειξη σεβασμού στις γυναίκες της χώρας του. Την αληθινή του ταυτότητα ο Μουλεσεχούλ αποκάλυψε στο γαλλικό τύπο τον Ιανουάριο του 2001, όταν παραιτήθηκε από τον αλγερινό στρατό. Σήμερα ζει στη Γαλλία.

Η ανωνυμία βοήθησε αρκετά και τις γυναίκες συγγραφείς οι οποίες μπορούσαν να κρύψουν το γένος τους.[14] Το 1967 μια γυναίκα πρώην πράκτορας, που την έλεγαν Alice Sheldon, θέλησε να γράψει ανώνυμα και άρχισε να συγγράφει διηγήματα με το όνομα James Tiptree Jr. Την πραγματική της ταυτότητα την κράτησε κρυφή από τους πάντες, εκτός από τον άνδρα της. Κρύφτηκε πίσω από το όνομα αυτό για δέκα χρόνια, ενώ τα ενδιαφέροντα διηγήματά της, της εξασφάλιζαν αναγνώριση και βραβεία. Αν ένας λάτρης της επιστημονικής φαντασίας δεν είχε διεξάγει μια κυριολεκτικά αστυνομική έρευνα γύρω από το άτομό της, θα εξακολουθούσε να μας είναι άγνωστη. Η ανωνυμία της, όσο κράτησε, ήταν μια μορφή αυτοσυντήρησης - αυτοπροστασίας από τις ατέλειωτα περίπλοκες και πιεστικές κοινωνικές απαιτήσεις.

Επίσης, η Σιμόν ντε Μπωβουάρ είναι μια ανώνυμη συγγραφέας.[15] Είναι φορέας ενός πνεύματος εξέγερσης αστικής προέλευσης, του λεγόμενου υπαρξισμού. Φορέας ιστορίας, πολιτικής, φιλοσοφίας και συγγραφικής δραστηριότητας. Η Σιμόν ντε Μπωβουάρ είναι εκδότρια μιας μεγάλης επιθεώρησης, των Νέων Καιρών, με μακρόχρονη παρουσία στην πνευματική ζωή της Γαλλίας. Διατηρεί σύνδεσμο με μια ομάδα γυναικών, που εκφράζονται από τις στήλες του περιοδικού της. Η στράτευση της Σιμόν ντε Μπωβουάρ έρχεται από πολύ μακριά.

Κατορθώνει να διατηρεί την παρουσία της χωρίς να γίνεται ακαδημαϊκή, έστω και συγκαλυμμένα. Χρησιμοποιώντας μια αυταρχική ανωνυμία, κατορθώνει να διαγράφει τον εαυτό της, χωρίς να τον εξαφανίζει. Μέσα από τη Μπωβουάρ μιλάνε οι γυναίκες, σε διάλογο ή μόνες. Γύρω της παίρνουν σάρκα κάθε λογής φωνές, καθημερινές, θεωρητικές, όλες αγωνιστικές. Δεν έχουν όλες κοινή ιδεολογική καταγωγή. Όμως, σε μια εποχή όπου ακόμα και τα προβλήματα των γυναικών διαφημίζονται και πουλιούνται στην αγορά, δεν βλάπτει καθόλου η ταύτιση σε ένα όνομα, όπως εκείνο της Σιμόν ντε Μπωβουάρ.

Φυσικά το ψευδώνυμο είναι πολύ συνηθισμένη υπόθεση. Μερικές φορές ένας συγγραφέας υιοθετεί ένα πιο εύηχο όνομα ή χρησιμοποιεί διαφορετικά ονόματα για διαφορετικά είδη γραφής. Και στις δυο περιπτώσεις πάντως δεν κρατιέται υπερβολική μυστικότητα. Ακόμη και οι συγγραφείς που αποφεύγουν τη δημοσιότητα δεν είναι πρόθυμοι να υποστούν την απόλυτη ανωνυμία.

---

[14] http://www.altfactor.ath.cx/magazine/aplanet/iss5/tiptree.html
[15] http://www.allbooks.gr/book.php?TitlesID=106499

Όσο περνούσαν τα χρόνια η ανωνυμία εξακολουθούσε να χρησιμοποιείται πιο συχνά σε συγγραφικές δουλειές. Στην φιλολογία κάθε έθνους, κάθε εποχής και κάθε κλάδου, υπάρχουν συγγραφείς που συνέγραψαν ανώνυμα. Πρόκειται για ένα φαινόμενο που παρουσιάζει πτυχές κοινωνικές, πολιτικές, ψυχολογικές, αισθητικές κ.λπ.

Όταν όμως εφευρέθηκε η τυπογραφία, τα βιβλία πολλαπλασιάστηκαν και όπως ήταν επόμενο πολλαπλασιάστηκε και ο αριθμός των ανώνυμων συγγραφέων. Σήμερα δημοσιεύονται ανώνυμα έργα μόνο λόγω μικρού ενδιαφέροντος, είτε γιατί η δημόσια θέση αποκλείει τον συγγραφέα τους, είτε η φύση του έργου είναι τέτοια ώστε η ανώνυμη έκδοσή του να εγγυάται μεγαλύτερη διάδοση. Αντίθετα η ψευδώνυμη συγγραφή εξακολουθεί να ακμάζει.

Δεν είναι λίγοι οι λογοτέχνες που κρύβονται πίσω από ένα ή πολλά διαφορετικά ονόματα. Η λογοτεχνία έχει βαλθεί να μας μπερδέψει. Κείμενα χαμένα ή άγνωστα έρχονται στην επιφάνεια και γνωρίζουν επιτυχία έπειτα από πολλά χρόνια. Ψευδώνυμα αναζητούν το πραγματικό πρόσωπο του συγγραφέα που κρύβεται πίσω τους, μελετητές ανακαλύπτουν, ταυτίζουν, αμφισβητούν ή ερίζουν. Το ψευδώνυμο είναι ένας σκεπασμένος αγώνας, είναι άδεια κυκλοφορίας σε αντιπνευματικές κοινωνίες και εκφράζει τη στάση του χρήστη απέναντι στα κυρίαρχα ιδεολογικά, αισθητικά, πνευματικά ρεύματα. Ο βιβλιογράφος και συγγραφέας Κυριάκος Ντελόπουλος ασχολείται εδώ και πολλά χρόνια με την αποδελτίωση των ψευδωνύμων.

Στο βιβλίο του «Ψευδώνυμα» καταγράφει 4.117 που αντιστοιχούν σε 2.261 συγγραφείς: λογοτέχνες, φιλολόγους, δοκιμιογράφους, χρονογράφους, δημοσιογράφους, μεταφραστές. Είναι η τρίτη προσπάθεια καταγραφής των λογοτεχνικών ψευδωνύμων. Η πρώτη έγινε το 1968 για τις ανάγκες της Βιβλιοθήκης του Κολλεγίου Αθηνών, πάλι από τον Κυριάκο Ντελόπουλο. Πρόκειται για ένα φαινόμενο που παρουσιάζει πτυχές κοινωνικές, πολιτικές, ψυχολογικές, αισθητικές κ.λπ. Συγγραφείς που διώκονταν από το εκάστοτε πολιτικό καθεστώς βιοπορίζονταν μεταφράζοντας ή δημοσιεύοντας με ψευδώνυμα· τα αυστηρά οικογενειακά ήθη, που αντιδρούσαν στην καλλιτεχνική τάση των κλώνων τους, ήταν μια δεύτερη αιτία για ψευδώνυμα, κυρίως σε γυναίκες συγγραφείς.

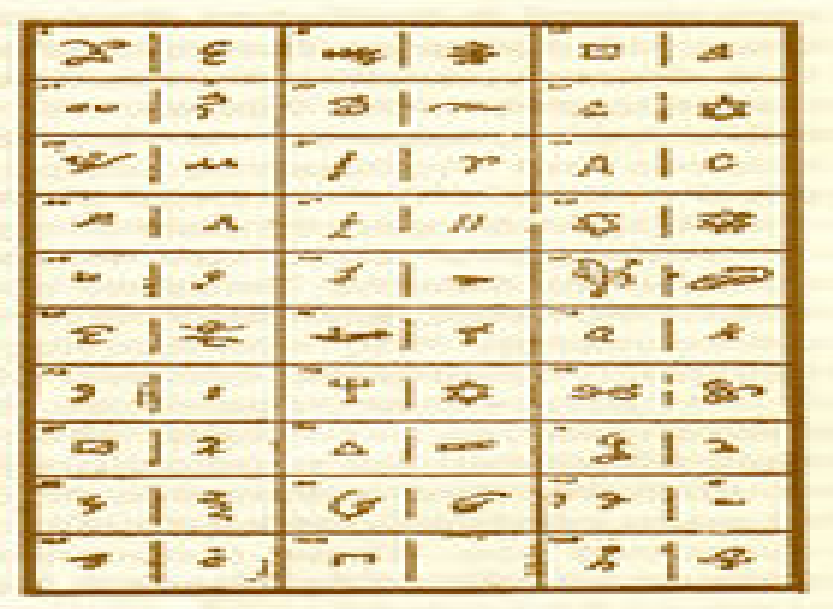
Τολμηρά κείμενα κρύβονταν πάντα κάτω από τα προσωπεία της ψευδωνυμίας. Η ψευδωνυμία δεν είναι όμως συνήθεια του 19ου αιώνα. Πολλοί από τους σύγχρονους συγγραφείς παίζουν αυτό το παιχνίδι: Μανόλης Αναγνωστάκης, Κώστας Βάρναλης, Νάσος Βαγενάς, Νίκος Καζαντζάκης, Δημήτριος Καμπούρογλου, Ανδρέας Καρκαβίτσας, Κώστας Καρυωτάκης, Ιωάννης Κονδυλάκης, Αλέξανδρος Κοτζιάς, Γιάννης Ρίτσος (με 17 ψευδώνυμα), Βασίλης Ρώτας, Γιάννης Σκαρίμπας κ. ά.

Κοινωνικές και πολιτικές ανάγκες, οικογενειακοί ή οικονομικοί λόγοι, αλλά και λογοτεχνικά παιχνίδια κρύβονται πίσω από τις επιλογές πολλών ψευδωνύμων, που επέλεξαν πασίγνωστοι Έλληνες λογοτέχνες.[16] Κάποιοι έγιναν γνωστοί μόνο με το ψευδώνυμό τους: Μ. Καραγάτσης, Οδυσσέας Ελύτης, Γιώργος Σεφέρης, Στρατής

[16] http://www.actionnemesis.com/v2/index.php?option=com_content&task=view&id=369&Itemid=53

Μυριβήλης, Στρατής Τσίρκας.[17] Κάποιοι άλλοι είχαν πάθος με το παιχνίδι της μάσκας και του ψευδώνυμου. Ο Εμμανουήλ Ροΐδης, για παράδειγμα, έχει υπογράψει με 33 διαφορετικά ψευδώνυμα! Αριθμός που είναι ελάχιστος μπροστά στα 160 ψευδώνυμα που αποδίδονται στον Βολτέρο! Ο Ρένος Αποστολίδης χρησιμοποίησε 34 ψευδώνυμα. Ο Ρίτσος πάλι είχε εμφανιστεί με 16 ψευδώνυμα, ενώ με 9 ο Αναγνωστάκης.

Στα τέλη του 18ου αιώνα και στις αρχές του 19ου ένας επαναστατικός πυρετός διακατέχει την Ευρώπη, κυρίως ενάντια στην ανθρώπινη εκμετάλλευση και τη μοναρχία. [18] Μια σημαντική περίπτωση ψευδωνυμίας δημιουργήθηκε στην Ελλάδα όπου το βάρος της προετοιμασίας της επανάστασης ανέλαβε η Φιλική Εταιρεία, που ιδρύθηκε το 1814. Η Φιλική Εταιρεία οργανώθηκε με μεγάλη μυστικότητα, και οι Φιλικοί μυούνταν στην Εταιρεία με μυστικό όρκο και επικοινωνούσαν με κώδικες, ψευδώνυμα και συνθηματικές λέξεις. Αυτή η δομή ήταν που διαφύλαξε μέχρι τέλους και διατήρησε αλώβητη τη Φιλική Εταιρεία.



Εικόνα 1 Σύμβολα της Φιλικής Εταιρίας

Η ανωνυμία και η ψευδωνυμία υπήρξε ιστορικά μέρος της ζωντανής και ζωηρής πολιτικής συζήτησης. [19] Υπήρχε στην αρχαία Ελλάδα και τη Ρώμη με τα graffiti στους δρόμους. Κάθε τεχνολογική εξέλιξη που διευκόλυνε τον λόγο, όπως το internet, διευκόλυνε και την παραγωγή ανώνυμου λόγου. Και όσο προχωράει η τεχνολογία τόσο πιο δύσκολη γίνεται η παρακολούθησή του και από τις αρχές, αλλά και από τους πολίτες.

---

[17] http://stavrochoros.pblogs.gr/2009/03/pisw-apo-ta-psefdwnyma-.html

[18] http://el.wikipedia.org/wiki/%CE%A6%CE%B9%CE%BB%CE%B9%CE%BA%CE%AE_%CE%95%CF%84%CE%B1%CE%B9%CF%81%CE%AF%CE%B1

[19] http://www.apologitis.com/gr/ancient/apologites.htm

Κεφάλαιο 3 Παρουσίαση του Προβλήματος & Σημερινή Κατάσταση

3.1 Η ανωνυμία στην καθημερινότητα

3.1.1 Ανωνυμία και κοινωνικές καταστάσεις

Εικόνα 2 Μάσκα καρναβαλιού

Η ανωνυμία μπορεί να μειώσει τη λογοδοσία των ανθρώπων που έχουν για τις πράξεις τους, και καταργεί τις επιπτώσεις αυτών των ενεργειών, που πιθανόν να έχουν στην φήμη τους.[20] Αυτό μπορεί να έχει δραματικές συνέπειες, τόσο χρήσιμο όσο και επιβλαβές. Στην καθημερινή ζωή η ανωνυμία μπορεί να επιτρέπει στα άτομα να αποκαλύψουν την ιστορία και τα προσωπικά συναισθήματα, χωρίς το φόβο της αμηχανίας αργότερα. Ηλεκτρονικές συζητήσεις μπορούν να παρέχουν φυσική απομόνωση, εκτός από την ανωνυμία. Αυτή η φυσική απομόνωση αποτρέπει από κάθε είδους αντίποινα για παρατηρήσεις, και εμποδίζει την αρνητική συμπεριφορά ή ταμπού ή συζητήσεις γύρω από τη φήμη του ομιλητή.

Αυτό μπορεί να είναι επωφελής όταν συζητάμε για πολύ προσωπικά θέματα ή θέματα ταμπού ή εκφράζοντας απόψεις ή την αποκάλυψη γεγονότων όπου μπορεί να θέσει κάποιος στη φυσική, οικονομική ή νομική πλευρά του κινδύνου (όπως η παράνομη δραστηριότητα, ή αντιδημοφιλείς πολιτικές απόψεις ή εκτός νόμου απόψεις). Με λίγες αντιληπτές αρνητικές συνέπειες, τα ανώνυμα ή ημι-ανώνυμα forum παρέχουν συχνά μια περιοχή συζητήσεων για την αποδιοργανωτική συνομιλητική συμπεριφορά. Ο όρος troll Internet χρησιμοποιείται συχνά για να αναφερθεί σε εκείνους που το κάνουν αυτό στο διαδίκτυο.

Η σχετική ανωνυμία εντοπίζεται συχνά σε μεγάλο αριθμό χρηστών. Οι διαφορετικοί άνθρωποι έχουν τις διαφορετικές ψυχολογικές και φιλοσοφικές αντιδράσεις σε αυτήν

---

[20] http://en.wikipedia.org/wiki/Anonymity

την ανάπτυξη, ειδικά ως σύγχρονο φαινόμενο. Αυτή η ανωνυμία είναι ένας σοβαρός παράγοντας στην ψυχολογία του πλήθους.

3.1.2 Ανωνυμία στη φιλανθρωπία

Υπάρχουν δύο πτυχές όσον αφόρα την ανωνυμία στην φιλανθρωπία. Η μια είναι, η δωρεά σε μια μεγάλη φιλανθρωπική οργάνωση. Στην άλλη η δωρεά δίνεται ανώνυμα με σκοπό να κρύψει τα στοιχεία του ευεργέτη από το δικαιούχο. Υπάρχουν πολλοί λόγοι που γίνεται αυτό. Η ανώνυμη φιλανθρωπία είναι από καιρό ένα διαδεδομένο και ανθεκτικό ηθικό ένταλμα πολλών ηθικών και θρησκευτικών συστημάτων, καθώς επίσης και μια διαδεδομένη ανθρώπινη δραστηριότητα. Ένας ευεργέτης δεν μπορεί να επιθυμήσει να καθιερώσει οποιαδήποτε σχέση με το δικαιούχο. Ένας ευεργέτης μπορεί να επιθυμήσει να βελτιώσει τον κόσμο, εφ' όσον δεν ξέρει κανένας ποιος το έκανε, από τη σεμνότητα, επιθυμώντας να αποφύγει τη δημοσιότητα

Για παράδειγμα, οι κυβερνήσεις της Σαουδικής Αραβίας και της Νορβηγίας, το Ίδρυμα Ντουμπάι, και οι επιχειρηματίες Μπιλ Γκέιτς, Στέφεν Μπινγκ, Χάιμ Σαμπάν και Ρόμπερτ Τζόνσον, είναι ορισμένοι από τους σημαντικότερους δωρητές του Ιδρύματος του πρώην προέδρου των ΗΠΑ, Μπιλ Κλίντον.[21] Τα ονόματά τους αναφέρονται στον πλήρη κατάλογο δωρητών, που δόθηκε στη δημοσιότητα πρόσφατα. Ο κ. Κλίντον αποκάλυψε τα ονόματα 200.000 και πλέον δωρητών του Ιδρύματός του, στο πλαίσιο συμφωνίας, την οποία είχε διαπραγματευτεί με τον Μπαράκ Ομπάμα.

Από τον κατάλογο των δωρητών, όπως εμφανίζεται στην ιστοσελίδα του Ιδρύματος Γουίλιαμ Τζ. Κλίντον -www.clintonfoundation.org- προκύπτει ότι η οργάνωση του πρώην προέδρου δέχθηκε δωρεές ύψους πολλών εκατομμυρίων δολαρίων από διάφορες ξένες κυβερνήσεις, εταιρείες και ιδιώτες, με άμεσο ενδιαφέρον ή και συμφέροντα συναφή με την εξωτερική πολιτική των Ηνωμένων Πολιτειών. Συνολικά, το Ίδρυμα συγκέντρωσε 500 εκατ. δολάρια στο διάστημα της τελευταίας δεκαετίας, ποσό που διοχετεύθηκε στην προεδρική βιβλιοθήκη και στις φιλανθρωπικές δραστηριότητες του κ. Κλίντον.

Κορυφαία θέση μεταξύ δωρητών μεγάλης γενναιοδωρίας, με ποσά άνω των 25 εκατ. δολαρίων, κατέχουν το Ίδρυμα Επενδύσεων για παιδιά, φιλανθρωπική οργάνωση με δράση κυρίως στην Αφρική. Επίσης η Unitaid, διεθνής συμμαχία με στόχο την καταπολέμηση του Aids. Έντεκα ακόμη δωρητές έχουν καταβάλει ποσά 10 έως 20 εκατ. δολαρίων, μεταξύ αυτών το Ίδρυμα Μπιλ Γκέιτς και η κυβέρνηση της Σαουδικής Αραβίας.

Υπάρχουν επίσης πολλοί παράνομοι λόγοι να κρύβεται ένα άτομο πίσω από την ανωνυμία. Οι εγκληματίες συνήθως προσπαθούν να διατηρήσουν την ανωνυμία τους, είτε για να συγκαλυφθεί το γεγονός ότι ένα έγκλημα έχει διαπραχθεί ή για να αποφεύγεται η σύλληψη όπως συμβαίνει με τους απαγωγείς. Επίσης άλλοι σημαντικοί λόγοι μπορεί να είναι η οργάνωση παράνομων δραστηριοτήτων, συζήτηση προσωπικών προβλημάτων με τρίτους, φάρσες, διαμαρτυρίες κατά

---

[21] http://news.kathimerini.gr/4dcgi/_w_articles_world_2_21/12/2008_296934

οποιασδήποτε αρχής, κοινωνικοί ή ερωτικοί πειραματισμοί όπως επίσης και τα εκλογικά καθήκοντα είναι κάποιοι από αυτούς.

Αν και η Ελλάδα δεν είναι χώρα με παράδοση στις απαγωγές, υπάρχει πλούσια προϊστορία.[22] Ένα παράδειγμα απαγωγής όπου αποκαλύφθηκε ποιος ήταν ο απαγωγέας, είναι αυτό με την 24χρονη καθηγήτρια ξένων γλωσσών Ζέτα Κουκέα. Η ίδια ισχυρίστηκε ότι την απήγαγαν καθώς επέστρεφε στο σπίτι της στο Ν. Ψυχικό. Μόλις πάρκαρε το αυτοκίνητό της, την απήγαγαν άγνωστοι με καλυμμένα τα πρόσωπά τους και την μετέφεραν σε ένα σπίτι.

Η ίδια δήλωσε ότι ήταν πολύ τρομοκρατημένη, και την κράτησαν τέσσερις ημέρες, ώσπου συμφώνησαν με τον πατέρα της, Π. Κουκέα οποίος ήταν έμπορος αυτοκινήτων, για την πληρωμή 49,4 εκατ. δραχμών ως λύτρα, ενώ αρχικά ζητούσαν 400 εκατομμύρια. Η παράδοση των χρημάτων έγινε στο τούνελ της Πανεπιστημιούπολης. Την απαγωγή είχε σχεδιάσει ο Πέτρος Καμπούρης που είχε επιχειρήσει να αγοράσει ταξί από τον πατέρα του θύματος.

Οι γόνοι ευκατάστατων οικογενειών είναι συχνότατα στόχος των κακοποιών, που δρουν με τη μέθοδο της απαγωγής για να βγάλουν λεφτά. Ξέρουν ότι προβάλλοντας τη δική τους συναισθηματική ψυχρότητα ενεργοποιούν την ψυχολογική πίεση των οικείων και τους μηχανισμούς σιωπής για να μην τους προδώσουν. Το μετά μιας απαγωγής τυραννά για καιρό τα θύματα και πόσο μάλλον όταν είναι σε τρυφερή ηλικία. Ο Δημήτρης Λουλάκης, πατέρας της εξάχρονης Ελένης που έπεσε θύμα απαγωγής τον Ιανουάριο του 1997 έξω από το ιδιωτικό σχολείο που πήγαινε στο Ηράκλειο Κρήτης, δήλωσε στο δικαστήριο, ότι η κόρη του είχε για αρκετό διάστημα ψυχολογικές διαταραχές.

Οι απαγωγείς τηλεφωνούν από το κρησφύγετό τους στον πατέρα της μικρής, ο οποίος ήταν διευθυντικό στέλεχος στην αντιπροσωπεία της Ford, και του ζήτησαν 120 εκ. δραχμές. Η αντίστροφη μέτρηση για τους απαγωγείς άρχισε, όταν ο οδηγός του σχολικού λεωφορείου ανέφερε ότι αντιλήφθηκε σε κοντινή απόσταση από το σχολείο μια γνωστή του, η οποία στο παρελθόν είχε δουλέψει ως οικιακή βοηθός στο σπίτι της μητέρας του ιδιοκτήτη του ιδιωτικού σχολείου. Τελικά, οι απαγωγείς ήταν η ιδιοκτήτρια βρεφονηπιακού σταθμού στο οποίο πήγαινε παλαιότερα η μικρή.

Όσον αφορά την υπόθεση Χαΐτογλου, τον Δεκέμβριο του 1995 απήχθη ο γνωστός βιομήχανος ενώ πήγαινε στο οικογενειακό εργοστάσιο που διατηρούσε στην Θεσσαλονίκη. Έπειτα από ογδόντα ώρες κράτησης ο απαχθείς εγκαταλείφθηκε στο ΚΤΕΛ υπεραστικών λεωφορείων της Καρδίτσας. Ο αδελφός του Κώστας, ήταν ο υπερτυχερός της κλήρωσης του ΛΟΤΤΟ με 160 εκατομμύρια δραχμές. Οι απαγωγείς όμως ζήτησαν πολύ περισσότερα. Η οικογένεια τελικά κατέβαλε σχεδόν τα μισά από τα τρία εκατομμύρια μάρκα που είχαν ζητήσει (260 εκατομμύρια δραχμές).

Στην υπόθεση απαγωγής του Γ. Μυλωνά οι δράστες του είχαν στήσει καρτέρι στο parking του σπιτιού του και αφού έβγαλαν από το αυτοκίνητο, με την απειλή όπλου τον επιχειρηματία και την γυναίκα του, την οποία άφησαν να φύγει, εξαφανίστηκαν

[22] http://www.tovima.gr/default.asp?pid=2&ct=34&artid=99815&dt=31/05/1998

προς άγνωστη κατεύθυνση. [23] Μετά από 13 μέρες οι απαγωγείς του τον άφησαν ελεύθερο και του υπέδειξαν πού βρίσκεται ένα αυτοκίνητο, ώστε να το πάρει και να γυρίσει μόνος του στο σπίτι του.

Τα προσημειωμένα χαρτονομίσματα που δόθηκαν ως λύτρα (πάνω από 10.000.000 ευρώ) βρέθηκαν στην Κρήτη όταν ένας 40χρονος άντρας προσπάθησε να αγοράσει ένα πολυτελές τζιπ με τα συγκεκριμένα χρήματα και δυο μήνες μετά συνελήφθη ο εγκέφαλος της απαγωγής, Βασίλης Παλαιοκώστας μαζί με άλλους τέσσερις συνεργούς, οι οποίοι ήταν υπεύθυνοι και για την απαγωγή του βιομήχανου Χαΐτογλου.

Στο σημείο αυτό έχει ενδιαφέρον να διαβάσει κανείς ένα απόσπασμα από τα αμερικανικά αστυνομικά εγχειρίδια, σχετικά με την αντιμετώπιση απαγωγών με κίνητρο τα λύτρα: «Σε τέτοιες περιπτώσεις την υπόθεση χειρίζονται οι οικείοι του απαχθέντος.[24] Η Αστυνομία καταβάλλει προσπάθεια να συνεργαστεί, χωρίς όμως να επιδιώκει την ανάληψη πρωτοβουλιών αν δεν το επιθυμεί η οικογένεια του θύματος. Στο μέρος της συνάντησης για την είσπραξη των λύτρων δεν λαμβάνονται αστυνομικά μέτρα. Δεν συμβαίνει το ίδιο με άλλες περιπτώσεις απαγωγών με διαφορετικά κίνητρα, όπως απελευθέρωση κρατουμένων ή φυλακισμένων, ικανοποίηση πολιτικών αιτημάτων, κρίση τρέλας, εκβίαση γενικά».

3.1.3 Η ανωνυμία και ο Τύπος

Με το πρόβλημα της ανωνυμίας στη δημοσιογραφική εργασία έχουν ασχοληθεί όλοι οι μελετητές της ιστορίας του Τύπου.[25] Ο σημαντικότερος Έλληνας ιστορικός του τύπου Γ.Δ. Ζιούτος (Γεώργιος Ζωιτόπουλος, δημοσιογράφος ο ίδιος), αναφέρει ότι η ανωνυμία του συντάκτη «είναι μία κατάκτηση του Τύπου, είναι η άλλη μορφή του "μυστικού της σύνταξης", είναι η κατοχύρωση του συντάκτη στις αυθαιρεσίες της εξουσίας» («Ο Τύπος στη Λαϊκή Δημοκρατία», Νέα Βιβλία, Αθήνα 1945).

Αναφέρεται στον Μαρξ και στη θέση του ότι «η ανωνυμία κάνει αμερόληπτο και ελεύθερο κι αυτόν που γράφει και το κοινό, που έτσι προσέχει στα γραφόμενα, στα πράγματα, στις ιδέες και όχι στο πρόσωπο του γράφοντος». Όμως αυτή η ειδυλλιακή μορφή των σχέσεων εφημερίδας-αναγνωστών δεν άντεξε όσο ο Τύπος άρχισε να παίρνει τη γνωστή μορφή της τέταρτης (και καθόλου έσχατης) εξουσίας.

Ο Μαρξ περιγράφει στο έργο του για τους «Ταξικούς Αγώνες στη Γαλλία 1848-1850» τη θέσπιση ενός καινούργιου νόμου για τον Τύπο, ο οποίος επέβαλε από τη μια μεριά υψηλές χρηματικές εγγυήσεις για τον εκδότη και από την άλλη την επωνυμία στους συντάκτες: «Όσο ο καθημερινός Τύπος ήταν ανώνυμος, παρουσιαζόταν σαν το όργανο της αναρίθμητης, ανώνυμης κοινής γνώμης. Ήταν η τρίτη δύναμη στο κράτος.

---

[23] http://www.cosmo.gr/News/Hellas/228165.html
[24] http://www.tovima.gr/default.asp?pid=2&ct=34&artid=99815&dt=31/05/1998
[25] http://www.enet.gr/online/online_fpage_text?dt=05/02/2005&id=49834608,55636976,63658352

Η υπογραφή κάθε άρθρου έκανε την εφημερίδα μια απλή συλλογή φιλολογικών διατριβών από περισσότερο ή λιγότερο γνωστά άτομα. Κάθε άρθρο ξέπεσε στο επίπεδο αγγελίας. Μέχρι τότε οι εφημερίδες κυκλοφορούσαν σαν χαρτονόμισμα της κοινής γνώμης. Τώρα μετατρέπονταν σε συναλλαγματικές που η αξία και η κυκλοφορία εξαρτιόταν από την πίστη όχι μόνο του εκδότη, αλλά και του οπισθογράφου».

Όμως η πραγματική υπονόμευση του παλιού είδους της ανώνυμης εφημερίδας ήταν έμμεση. Όπως εξηγεί ο Ζιούτος:
«Ο καπιταλισμός υπονόμευσε την ανωνυμία με δύο τρόπους:
α) Χρησιμοποιώντας την για λόγους κερδοσκοπικούς (ανώνυμες πληρωμένες διατριβές κ.λπ.).
β) Δημιουργώντας «δημοσιογραφικές βεντέτες" (όπως στον κινηματογράφο), δηλ. "ηχηρά ονόματα" δημοσιογράφων, συγγραφέων κ.λπ., χωρίς αρχές, που τα χρησιμοποιεί για ν' αυξάνει την κυκλοφορία και να συγκεντρώνει αγγελίες (σ.σ. διαφημίσεις)».

Αυτά τα δύο χαρακτηριστικά του σύγχρονου Τύπου που περιγράφει ο Ζιούτος πριν από 60 χρόνια, ισχύουν σήμερα στο πολλαπλάσιο. Οι εφημερίδες με τα ανυπόγραφα κείμενα έχουν πλήρως εξαφανιστεί ή βρίσκονται στο εκδοτικό περιθώριο. Οι πληρωμένες καταχωρήσεις έχουν αναχθεί σε επιστήμη. Και βέβαια η ηλεκτρονική δημοσιογραφία και η γιγάντωση των επιχειρήσεων ΜΜΕ ενίσχυσε τους δημοσιογράφους-βεντέτες και τους μετέτρεψε σε εργοδότες άλλων δημοσιογράφων.

Απ’ αυτή την άποψη η διεκδίκηση της ανωνυμίας στο δημοσιογραφικό επάγγελμα ισοδυναμεί με την αποδοχή της υπάρχουσας διάκρισης πατρικίων και πληβείων και οδηγεί στο συμβιβασμό με την ιδέα ότι «επώνυμοι» (δηλαδή ικανοί να έχουν προσωπική άποψη) είναι μόνο οι «σταρ», ενώ οι υπόλοιποι πρέπει να αρκεστούν στην τυφλή υπηρεσία του (δημόσιου ή ιδιωτικού) εργοδότη τους.

3.1.4 Ανωνυμία φορέων HIV

Η ανωνυμία και η ιδιωτικότητα είναι αυστηρώς απαραίτητες για εφαρμογές όπως το AIDS, ο αλκοολισμός, ο καρκίνος κλπ.[26] Η ιατρική φροντίδα και η περίθαλψη ασθενών και φορέων του ιού του HIV αποτελεί ένα πολυσύνθετο και συνεχώς εξελισσόμενο θέμα. Όπως είναι γνωστό, μέχρι τα τέλη της δεκαετίας του ’90 ο ιός HIV ήταν θανατηφόρος. Ο φορέας του ιού εμφάνιζε, μετά από λίγα χρόνια, το σύνδρομο επίκτητης ανοσολογικής ανεπάρκειας (AIDS), δηλαδή καταστροφή του ανοσοποιητικού συστήματος και ως αποτέλεσμα αυτού, διάφορες σοβαρές ασθένειες, όπως πνευμονίες, διαρροϊκά σύνδρομα και άλλες σοβαρότατες λοιμώξεις, τον οδηγούσαν στον θάνατο.

Μετά το 1998 και την εφαρμογή των πρώτων αποτελεσματικών θεραπειών για το AIDS, ο ιός άρχισε να ελέγχεται και να περιορίζεται. Η λοίμωξη με τον HIV πλέον έχει καταστεί χρόνιο νόσημα, συχνά μάλιστα ασυμπτωματικό για

[26] http://www.synigoros.gr/pdfs/porisma_HIV_27_8.pdf

πολλά χρόνια και ως εκ τούτου προκαλεί μικρότερη αναστάτωση στη φυσιολογική ζωή του ατόμου (φορέα). Ο φορέας, όμως, συνεχίζει να είναι μεταδοτικός και να μολύνει και άλλους σε περίπτωση απροφύλακτης σεξουαλικής επαφής ή με το αίμα του. Στην Ελλάδα, τα πρόσφατα επιδημιολογικά δεδομένα καταδεικνύουν τη σοβαρότητα του προβλήματος και τον αυξημένο κίνδυνο που διατρέχει ο πληθυσμός σε σχέση με άλλες ανεπτυγμένες χώρες της Ευρώπης. Συγκεκριμένα, ενώ το 2000 ο αριθμός των νέων μολύνσεων που δηλώθηκαν μειώθηκε (τάση που συνεχίστηκε μέχρι το 2002), το 2003 και το 2004 παρουσιάστηκε αύξηση.

Το 2005 μάλιστα παρατηρήθηκε μια ιδιαιτέρως σημαντική μεταβολή, καθώς ο αριθμός των νέων μολύνσεων που δηλώθηκαν ανά εκατομμύριο πληθυσμού ανέρχονταν σε 50,6 νέες μολύνσεις (αύξηση 23,7 % σε σχέση με το 2004 και σχεδόν 39% συγκριτικά με το 2002). Η αύξηση αφορά και τους άνδρες και τις γυναίκες. Η ποσοστιαία μάλιστα αναλογία των γυναικών το 2005 έφτασε το 24,8% και αποτελούσε την υψηλότερη τιμή από την αρχή της επιδημίας. Μέχρι τις αρχές του 2006 στην Ελλάδα είχαν καταγραφεί 7718 άτομα οροθετικών και ασθενών AIDS. Από αυτά 6166 (79,9%) ήταν άνδρες και 1503 (19,5%) ήταν γυναίκες. Για ένα μικρό ποσοστό δεν δηλώθηκε φύλο.

Οι κίνδυνοι για τη δημόσια υγεία, η συχνή παραβίαση του απορρήτου, το στίγμα και οι συνακόλουθες κοινωνικές διακρίσεις, οδηγούν συχνά τους πάσχοντες στην απομόνωση. Κρίσιμο ρόλο στην προστασία και αποφυγή της απομόνωσης των πασχόντων παίζουν οι επαγγελματίες υγείας, οι οποίοι πρέπει να είναι πλήρως ενήμεροι για τα καθήκοντα και τις υποχρεώσεις τους ως αρωγοί και συμπαραστάτες των πασχόντων. Για να συζητηθούν τα προβλήματα που αντιμετωπίζουν οι πάσχοντες και οι εν δυνάμει πάσχοντες, πρέπει να υπάρχει περιβάλλον απόλυτης ασφάλειας, εμπιστοσύνης και εχεμύθειας.

Η ποινικοποίηση των υποθέσεων (όπως για παράδειγμα η υπόθεση δίωξης νεαρού αιμοδότη που μετέδωσε ακούσια τον ιό, η οποία ήλθε τον περασμένο χρόνο στη δημοσιότητα) είναι αμφίβολο αν οδηγεί στα επιθυμητά αποτελέσματα, δηλαδή στη βελτίωση της ποιότητας ζωής των ασθενών, στη μείωση του ρυθμού εξάπλωσης του ιού HIV και πάνω από όλα στη προστασία της δημόσιας υγείας. Σκοπός του παρόντος πορίσματος είναι η ανάδειξη προβλημάτων που αντιμετωπίζουν οι ασθενείς και οι φορείς HIV AIDS, καθώς και η διατύπωση προτάσεων που διασφαλίζουν την αποτελεσματική άσκηση των δικαιωμάτων τους.

3.1.5 Ανωνυμία στους αλκοολικούς

Οι αλκοολικοί ανώνυμοι είναι μία αδελφότητα ανδρών και γυναικών που μοιράζονται μεταξύ τους τις εμπειρίες τους, τη δύναμη και την ελπίδα προς την επίλυση του κοινού τους προβλήματος και προς τη βοήθεια άλλων να αποθεραπεύονται από τον αλκοολισμό. [27] Η μοναδική προϋπόθεση εγγραφής ως μέλος είναι η επιθυμία να σταματήσει να πίνει. Τα μέλη δεν πληρώνουν εγγραφή ούτε άλλα χρήματα για τις υπηρεσίες που προσφέρονται - συντηρούμαστε με δικές μας συνεισφορές.

---

[27] http://www.aa-greece.gr/11.htm

Η αδελφότητα των Α.Α. δεν συνδέεται με κανένα δόγμα, πολιτικό κόμμα ή άλλο οργανισμό ή ίδρυμα. Δεν συμμετέχει σε διενέξεις και δεν υποστηρίζει ούτε εναντιώνεται σε οτιδήποτε σκοπούς. Ο κύριος σκοπός τους είναι να βρίσκονται σε κατάσταση νηφαλιότητας και να βοηθάνε άλλους αλκοολικούς να πετυχαίνουν κι αυτοί την νηφαλιότητα.

Ποιός είναι ο σκοπός της ανωνυμίας στους Αλκοολικούς Ανώνυμους; Γιατί συχνά αναφέρεται σαν η μεγαλύτερη και μοναδική προστασία που η Αδελφότητα έχει για να διασφαλίσει την συνεχιζόμενη ύπαρξή της και ανάπτυξη; Αν ανατρέξουμε στην ιστορία του Α.Α (Αλκοολικοί Ανώνυμοι), από το ξεκίνημά του το 1935 μέχρι σήμερα, είναι ξεκάθαρο πως η ανωνυμία εξυπηρετεί δύο διαφορετικές αλλά εξίσου ζωτικής σημασίας λειτουργίες:

- Σε προσωπικό επίπεδο, η ανωνυμία παρέχει προστασία σε όλα τα μέλη από το να αναγνωριστούν ως αλκοολικοί, μία προστασία με ιδιαίτερη συχνά σπουδαιότητα για τους νεοφερμένους.

- Σε επίπεδο τύπου, ραδιοφώνου, τηλεόρασης και ταινιών, η ανωνυμία ‘υπογραμμίζει’ την ισότητα όλων των μελών της Αδελφότητας βάζοντας φρένο σε εκείνους που διαφορετικά ίσως θα εκμεταλλευόταν τον δεσμό τους με το Α.Α. για να αποκτήσουν αναγνώριση, δύναμη ή προσωπικό όφελος.

Από την αρχή του, το Α.Α. έχει υποσχεθεί προσωπική ανωνυμία σε όλους όσους παρίστανται στις συγκεντρώσεις του. Επειδή οι ιδρυτές του καθώς και τα πρώτα μέλη του ήταν οι ίδιοι αλκοολικοί σε ανάρρωση, γνώριζαν από την εμπειρία τους πόσο ντρέπονται οι περισσότεροι αλκοολικοί για το πιόμα τους, και πόσο φοβισμένοι είναι μην γίνει δημόσια γνωστό αυτό. Το κοινωνικό στίγμα του αλκοολισμού ήταν μεγάλο, και εκείνοι, τα πρώτα μέλη των Α.Α., αναγνώρισαν πως μία ακλόνητη εγγύηση εχεμύθειας ήταν επιτακτική εάν θελαν να επιτύχουν στην προσέλκυση και βοήθεια άλλων αλκοολικών για να καταφέρουν την νηφαλιότητα.

Με το πέρασμα των χρόνων, η ανωνυμία έχει αποδειχθεί να είναι ένα από τα σημαντικότερα δώρα που το Α.Α. προσφέρει στον αλκοολικό που υποφέρει. Χωρίς αυτήν, αρκετοί δεν θα πήγαιναν ποτέ στην πρώτη τους συγκέντρωση. Παρ’ όλο που το στίγμα έχει μικραίνει σε κάποιο βαθμό, οι περισσότεροι νεοφερμένοι ακόμη βρίσκουν την παραδοχή του αλκοολισμού τους τόσο επίπονη που είναι εφικτή μόνο σε ένα προστατευμένο περιβάλλον. Η ανωνυμία είναι απαραίτητη για την δημιουργία αυτής της ατμόσφαιρας εμπιστοσύνης και ειλικρίνειας.

Καθώς η προσωπική ανωνυμία είναι πολύτιμη στα νέα μέλη, είναι αξιοσημείωτο ότι τα περισσότερα είναι πρόθυμα να μοιραστούν τα καλά νέα της ένταξής τους στο Α.Α. με τις οικογένειές τους. Μια τέτοια αποκάλυψη, ωστόσο, είναι πάντα δική τους επιλογή. Το Α.Α. σαν σύνολο ψάχνει να διασφαλίσει ότι το κάθε ένα μέλος μένει ανώνυμο και προστατευμένο στο βαθμό που εκείνο επιθυμεί, ή όσο ‘ανοιχτό’ όσο εκείνο επιθυμεί, σχετικά με το ότι ανήκει στην Αδελφότητα, αλλά πάντα με την κατανόηση ότι η ανωνυμία στο επίπεδο τύπου, ραδιοφώνου, τηλεόρασης και ταινιών είναι ζωτικής σημασίας για την συνεχιζόμενη νηφαλιότητα και ανάπτυξη- τόσο σε προσωπικό επίπεδο όσο και στο επίπεδο των ομάδων.

3.1.6 Ανώνυμα καρτοκινητά

Κυβερνήσεις, οργανισμοί και πολυεθνικές εταιρείες επιχειρούν -καθένας για τους δικούς τους λόγους- να καταγράψουν, να ελέγξουν ή ακόμα και να περιορίσουν τις διαδικτυακές συνήθειες των κυβερνο-πολιτών, για παράδειγμα η χρήση καρτοκινητών έγινε πλέον κι αυτή επώνυμη. [28]

Από 1/7/2009 τέθηκε σε δημόσια διαβούλευση το νομοσχέδιο για την ταυτοποίηση των καρτοκινητών και στην Ελλάδα.[29] Το ίδιο ζητούσε και η Ένωση Εταιριών Κινητής Τηλεφωνίας σε σχετική της ανακοίνωση, θεωρώντας ότι η εφαρμογή του συγκεκριμένου Νόμου θα επιφέρει πολλαπλές οικονομικές και κοινωνικές επιπτώσεις. Ο υπουργός Μεταφορών και Επικοινωνιών, Ευριπίδης Στυλιανίδης, σε συνέντευξη Τύπου που παραχώρησε δήλωσε ότι μέχρι τις 30 Ιουνίου του 2010 θα έχουν ταυτοποιηθεί όλα τα καρτοκινητά τηλέφωνα, τα οποία στο σύνολό τους υπολογίζεται ότι φθάνουν τα 13,5 εκατ., από τα οποία τα 9 εκατ. είναι "ενεργά".

Στόχος του μέτρου, σύμφωνα με τον υπουργό, είναι η καταπολέμηση της εγκληματικότητας. Εμπόδιο όμως αποτελούν ορισμένες "μαύρες τρύπες", όπως η προσκόμιση πλαστών πιστοποιητικών στις εταιρείες κινητής τηλεφωνίας. Σύμφωνα με τον κ. Στυλιανίδη το κόστος του νέου μέτρου θα αναλάβουν οι εταιρείες κινητής, και σε περίπτωση που αυτό μετακυλήσει στους καταναλωτές θα παρέμβει η ΕΕΤΤ. Πρόσθεσε δε ότι το κόστος του έργου δεν ανέρχεται σε αρκετά εκατομμύρια ευρώ -όπως ισχυρίζονται οι εταιρείες κινητής- με δεδομένο ότι οι εταιρείες διαθέτουν ήδη το λογισμικό.

Πλέον, τα καρτοκινητά θα πωλούνται μόνο στα καταστήματα των εταιρειών κινητής τηλεφωνίας και μονάχα οι κάρτες ανανέωσης χρόνου σε περίπτερα και mini markets. Η κάρτα θα ενεργοποιείται μόνο όταν υπάρξει η ταυτοποίηση, ενώ σε περίπτωση μεταβίβασης ή κλοπής τη κάρτα θα πρέπει να ενημερωθεί η εταιρεία, όπως συμβαίνει με τις πιστωτικές κάρτες. Αξίζει να σημειωθεί ότι το μέτρο της ταυτοποίησης των καρτοκινητών εφαρμόζεται ήδη σε Γαλλία, Ισπανία, Γερμανία, Ολλανδία, Ουκρανία και Σλοβενία, ενώ στη Μεγάλη Βρετανία βρίσκεται υπό εξέταση. Εκτός της ΕΕ, ισχύει στην Αλβανία, Ελβετία, Νορβηγία, Αυστραλία.

Με την ταυτοποίηση των καρτοκινητών, το ελληνικό Δημόσιο, σύμφωνα με το ΥΜΕ προσαρμόζεται στις ευρωπαϊκές κοινοτικές οδηγίες, καθώς πρόθεση της κοινότητας αποτελεί η εφαρμογή του μέτρου σε όλα τα κράτη – μέλη, σε μια προσπάθεια ενίσχυσης των προσπαθειών καταπολέμησης της εγκληματικότητας. Νωρίτερα, η ένωση εταιρειών Κινητής Τηλεφωνίας εξέδωσε σχετική ανακοίνωση στην οποία ζητούσε τη διενέργεια δημόσιας διαβούλευσης.

Σύμφωνα με την ΕΕΚΤ, την Πέμπτη 11 Ιουνίου 2009 εκλήθη στο ΥΜΕ για συνάντηση – συζήτηση, η οποία περιορίστηκε σε προφορική ενημέρωση για ορισμένες πτυχές του Σχεδίου Νόμου, εφόσον οι εκπρόσωποι του Υπουργείου δεν κοινοποίησαν γραπτά τις διατάξεις του. Η ΕΕΚΤ θεωρεί ότι η εφαρμογή του

---

[29] http://www.isotimia.gr/default.asp?pid=24&ct=6&artid=73802

συγκεκριμένου Νόμου θα επιφέρει πολλαπλές οικονομικές και κοινωνικές επιπτώσεις και για αυτό το λόγο προτείνει τη δημοσίευση του Σχέδιου Νόμου και - σύμφωνα με την ανειλημμένη δέσμευση του Υπουργείου - τη διενέργεια Δημόσιας Διαβούλευσης με υποβολή απόψεων και προτάσεων τόσο από τον κλάδο Κινητής Τηλεφωνίας όσο και από όλους τους εμπλεκόμενους φορείς, με συγκεκριμένο και επαρκές χρονοδιάγραμμα. «Η ΕΕΚΤ, λόγω της μη επαρκούς ενημέρωσης της, δυστυχώς δεν είναι σε θέση να τοποθετηθεί εγκαίρως ολοκληρωμένα επί του θέματος, ούτε να αξιολογήσει τεκμηριωμένα την αποτελεσματικότητα του και τις επιπτώσεις της εφαρμογής του Νόμου»,σημειώνει χαρακτηριστικά.

Επί της ουσίας, η ΕΕΚΤ, σε σχετική επιστολή που έστειλε από τις αρχές Μαΐου στο Υπουργείο ΜΕ, ανάμεσα σε άλλες κοινωνικές και οικονομικές παραμέτρους που θα πρέπει να ληφθούν υπόψη για κατάρτιση του Νομοσχεδίου, έχει επισημάνει:

- Ο νέος Νόμος δεν αναμένεται να επιφέρει τα προσδοκώμενα αποτελέσματα για την εξιχνίαση εγκλημάτων, αντιθέτως μπορεί να ενθαρρύνει την εγκληματικότητα και την παραοικονομία, ενώ δεν αποκλείεται η χρήση καρτοκινητών ξένων δικτύων για την υποστήριξη αξιόποινων πράξεων.

- Η αλλαγή του τρόπου διανομής της καρτοκινητής τηλεφωνίας θα έχει επιπτώσεις σε ευρύτερες επαγγελματικές ομάδες (χονδρέμποροι, διανομείς, περιπτερούχοι).

- Το συγκεκριμένο μέτρο αφενός θα είναι εις βάρος της ανάπτυξης των τηλεπικοινωνιών και αφετέρου θα επιβαρύνει το κόστος χρήσης για τους καταναλωτές.

Αξίζει να σημειωθεί ότι, οι λίγες χώρες οι οποίες εφαρμόζουν σήμερα κάποιο σύστημα ταυτοποίησης χρηστών κινητής τηλεφωνίας, κατέληξαν σε αυτό μετά από πολύμηνο διάλογο με τους φορείς της αγοράς και τις ανεξάρτητες αρχές, δίνοντας επαρκή χρόνο και για την εφαρμογή του. Είναι χαρακτηριστικό ότι στην Ισπανία μετά από το πέρας του διαλόγου, δόθηκε διετής προθεσμία για την εφαρμογή του νέου Νόμου. Στη Μεγάλη Βρετανία, μετά τη διαβούλευση, το Σχέδιο Νόμου ανακλήθηκε ως μη ρεαλιστικό και επαναπροσδιορίζεται σε νέα βάση. Η ταχύτητα με την οποία προωθείται το Σχέδιο Νόμου στη χώρα μας, εγκυμονεί προβλήματα για την ουσιαστική εφαρμογή του.

Σε κάθε περίπτωση η ΕΕΚΤ επισημαίνει ότι η υλοποίηση ενός τέτοιου μέτρου απαιτεί σωστό σχεδιασμό εκ μέρους της Πολιτείας και επαρκή χρόνο για την ορθή εφαρμογή του από τις εταιρίες κινητής τηλεφωνίας. Οι εταιρίες αν και δεν γνωρίζουν το ακριβές περιεχόμενου των διατάξεων του Σχεδίου Νόμου θεωρούν ότι:

- Θα πρέπει να υπάρξουν ειδικές ρυθμίσεις για την ταυτοποίηση τουριστών που θα θελήσουν να χρησιμοποιήσουν ελληνικό καρτοκινητό κατά την περιορισμένη παραμονή τους στην Ελλάδα.

- Θα πρέπει να βρεθεί τρόπος να μην αποκλειστούν από τη χρήση καρτοκινητής τηλεφωνίας ευαίσθητες κοινωνικές ομάδες (πχ. ηλικιωμένοι, κάτοικοι χωριών, απομονωμένων ή ακριτικών περιοχών, οικονομικοί μετανάστες, κλπ).

- Δεν εξυπηρετεί τους σκοπούς του Νόμου το να ζητούνται Δικαιολογητικά νομιμοποίησης (όπως πχ. άδειες παραμονής κλπ) τα οποία είναι αδύνατον να ελεγχθούν από τους πωλητές των καταστημάτων στα σημεία πώλησης Εταιριών Κινητής Τηλεφωνίας.

3.1.7 Ανωνυμία του εμπορίου και του εγκλήματος

Οι ανώνυμες εμπορικές συναλλαγές μπορούν να προστατεύσουν τη μυστικότητα των καταναλωτών.[30] Μερικοί καταναλωτές προτιμούν να χρησιμοποιήσουν τα μετρητά κατά την αγορά των καθημερινών αγαθών (όπως τα παντοπωλεία ή τα εργαλεία), να αποτρέψουν τους πωλητές από τη συνάθροιση των πληροφοριών ή την επιδίωξη τους στο μέλλον.

Η πιστωτική κάρτα συνδέεται με το όνομα του κατόχου της και μπορεί να χρησιμοποιηθεί για να ανακαλυφθούν άλλες πληροφορίες, όπως η ταχυδρομική διεύθυνση, ο αριθμός τηλεφώνου, κ.λπ. Το σύστημα e-cash αναπτύχθηκε για να επιτρέψει τις ασφαλείς ανώνυμες συναλλαγές. Κατά την αγορά των αγαθών ή των υπηρεσιών ταμπού, η ανωνυμία καθιστά πολλούς πιθανούς καταναλωτές πιο άνετους ή προθυμότερους να συμμετέχουν στη συναλλαγή.

Πολλά προγράμματα χρησιμοποιούν τις κάρτες που προσδιορίζουν προσωπικά τον καταναλωτή που συμμετέχει σε κάθε συναλλαγή (ενδεχομένως για την πιο πρόσφατη παράκληση, ή για λόγους εξαγοράς ή ασφάλειας), ή που ενεργούν ως αριθμητικό ψευδώνυμο, για τη χρήση στην ανάσυρση δεδομένων.

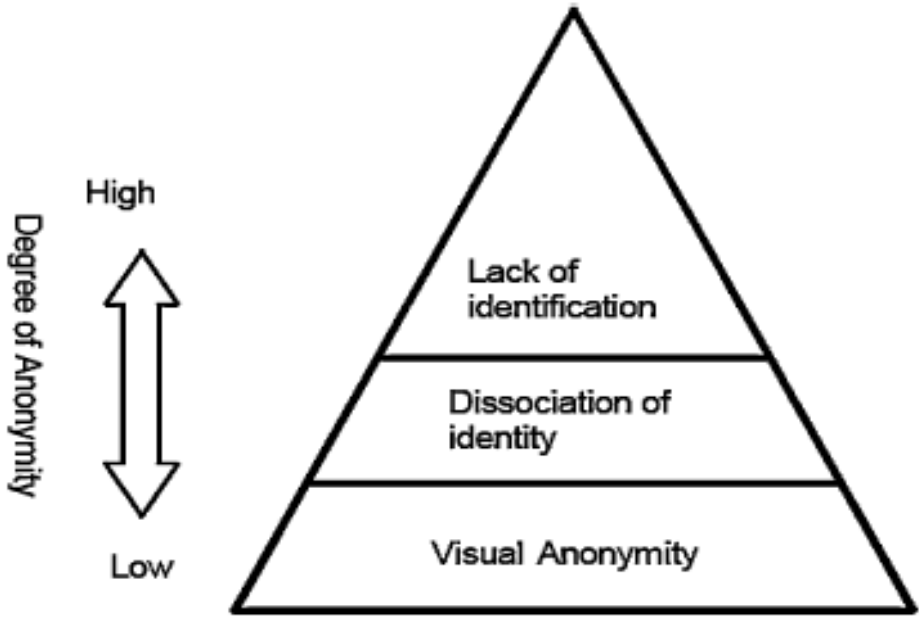
Η ανωνυμία μπορεί επίσης να χρησιμοποιηθεί ως προστασία ενάντια στη νομική συνέχιση. Παραδείγματος χάριν, κατά τη διάπραξη μιας ληστείας, πολλοί εγκληματίες θα κρύψουν τα πρόσωπά τους για να αποφύγουν τον προσδιορισμό. Στο οργανωμένο έγκλημα, οι ομάδες εγκληματιών μπορούν να συνεργαστούν σε ένα ορισμένο πρόγραμμα χωρίς να αποκαλύπτουν ο ένας στον άλλο τα ονόματά τους ή άλλες προσωπικές πληροφορίες.

Στον κινηματογράφο ο Thomas Crown Affair απεικόνισε μια πλασματική συνεργασία από ανθρώπους που δεν είχαν συναντηθεί προηγουμένως και δεν ήξεραν ποιος τους είχε στρατολογήσει. Η ανώνυμη αγορά ενός πυροβόλου όπλου ή ενός μαχαιριού που χρησιμοποιείται σε ένα έγκλημα βοηθά να αποτρέψει τη σύνδεση ενός εγκαταλειμμένου όπλου με την ταυτότητα του δράστη.

[30] http://en.wikipedia.org/wiki/Anonymity

3.2 Ανωνυμία στο Internet

3.2.1 Ιεραρχία της ανωνυμίας



Εικόνα 3 Ιεραρχία της ανωνυμίας

Η οπτική ανωνυμία (Visual Anonymity) βρίσκεται στο χαμηλότερο επίπεδο, όπως για παράδειγμα τα e-mail που δεν περιέχουν φωτογραφίες του αποστολέα ή οποιαδήποτε άλλα μη λεκτικά συνθηματικά.[31] Εντούτοις σε αυτό το επίπεδο ανωνυμίας, υπάρχει συχνά μια σχέση ανάμεσα στην ψεύτικη ταυτότητα κάποιου ο οποίος μπορεί με αυτή να δέχεται και να λαμβάνει e-mail.

Τα chat rooms είναι ένα πολύ καλό παράδειγμα για το επόμενο επίπεδο ανωνυμίας το οποίο είναι ο διαχωρισμός ανάμεσα στην αληθινή και online ταυτότητα (Dissociation of identity). Αυτό επιτυγχάνεται με το να χρησιμοποιεί ο χρήστης ψευδώνυμα ή διαστρεβλωμένα στοιχεία για να μπορέσει να έχει πρόσβαση και να επικοινωνήσει με άλλα άτομα σε αυτά τα chat rooms.

Στο υψηλότερο επίπεδο ανωνυμίας είναι η έλλειψη αναγνώρισης (Lack of identification), όπου οι χρήστες είναι απολύτως ανώνυμοι, όπως για παράδειγμα τα γνωστά blogs τα οποία είναι sites όπου οι χρήστες είναι όλοι ανώνυμοι και μπορούν να εκφέρουν τις απόψεις τους χωρίς να υπάρχει κάποιος κίνδυνος να αποκαλυφθούν.

---

[31] http://www.springerlink.com/content/m734u30244347706/fulltext.pdf

3.2.2 Η ανωνυμία στο Διαδίκτυο

Η έρευνα για τις ανώνυμες επικοινωνίες άρχισε το 1981 με το έγγραφο του Chaum «Untraceable electronic mail, return addresses, and digital pseudonyms» (Chaum (1981)). Από τότε, το σώμα της έρευνας έχει επικεντρωθεί στη κατασκευή, στην ανάλυση και στις επιθέσεις στα ανώνυμα συστήματα επικοινωνιών. Η χρήση δικτύων επικοινωνίας χρησιμοποιούν τη δρομολόγηση που είναι, καταρχήν, ορατή στον καθένα που παρατηρεί το δίκτυο.

Πότε άλλοτε δεν υπήρξε μεγαλύτερη ανάγκη για ανωνυμία και προστασία ιδιωτικού απορρήτου στο Internet.[32] Ξεκινώντας σχεδόν από το 1995 και φθάνοντας κατά την τελευταία πενταετία στην ολοκλήρωση, το Internet γνώρισε μια μετεξέλιξη που το μεταμόρφωσε από ένα άκρως δημοκρατικό forum σε ένα εμπορευματοποιημένο μέσο, που είναι στα χέρια κρατικών και ιδιωτικών φορέων. Φορέων, που στην πλειοψηφία τους επιχειρούν-και συνήθως κατορθώνουν να καταγράφουν και να περιορίζουν δραστηριότητες και συνήθειες των χρηστών του Internet για εμπορικούς αλλά και πολιτικούς λόγους.

Η ίδια η αρχιτεκτονική του Internet καθιστά εύκολη την καταγραφή της συμπεριφοράς των χρηστών, ενώ η ανάπτυξη ολοένα πιο "έξυπνων" μηχανισμών παρακολούθησης σε συνδυασμό με την γνωστοποίησή τους λειτουργούν ανασταλτικά στην εξάσκηση του αναφαίρετου δικαιώματος της ελευθερίας του λόγου. Σε μια ακραία περιγραφή της υπάρχουσας κατάστασης, μπορούμε να πούμε ότι έχει διαμορφωθεί ένας νέος ψηφιακός άγραφος νόμος σε ορισμένες χώρες του πλανήτη που έχει ως εξής: "Είσαι ελεύθερος να πεις ότι θες, αρκεί να υποστείς τις συνέπειες".

Από τη στιγμή που δημιουργήθηκε το διαδίκτυο, η ανωνυμία έχει γίνει καθημερινός σκοπός για πολλούς χρήστες. [33] Το internet παρέχει πολύ περισσότερες δυνατότητες για ανωνυμία από τον πραγματικό κόσμο. Δεν είναι σπάνιο φαινόμενο η ύπαρξη ολόκληρων ψηφιακών κοινοτήτων που βασίζονται ή και προωθούν την ανωνυμία μεταξύ των μελών τους, συνήθως με τη χρήση ψευδωνύμων, δίνοντας στο κάθε μέλος τη διακριτική ευχέρεια να επιλέγει αν και σε ποιους επιθυμεί να αποκαλύψει την πραγματική του ταυτότητα. Τέτοια είναι κυρίως τα newsgroups που αποτελούν ίσως τα πιο ζωντανά σημεία του Internet αφού εκεί συζητούνται χιλιάδες θέματα μεταξύ χρηστών απ' όλο τον κόσμο.

Ισχυρότερο όμως εργαλείο στην υπηρεσία της ανωνυμίας είναι η κρυπτογραφία.[34] Στη δεκαετία του 1990 έγινε μια ιδιότυπη όσο και άγνωστη επανάσταση. Μερικοί ιδεαλιστές χρήστες πληροφοριακών συστημάτων χρησιμοποίησαν την γνώση της κρυπτογραφίας για να φτιάξουν ισχυρά κρυπτογραφικά εργαλεία για τον κάθε πολίτη. Τα εργαλεία αυτά, προς έκπληξη και τρόμο όλων των διωκτικών αρχών του κόσμου μοιράστηκαν και μοιράζονται ευρέως μέσω του Διαδικτύου.

---

[32] http://www.go-online.gr/ebusiness/specials/article.html?article_id=417
[33] ftp://ftp.research.microsoft.com/pub/tr/TR-2008-35.pdf
[34] http://www.go-online.gr/ebusiness/specials/article.html?article_id=417

Τα στοιχεία τα οποία σχετίζονται με την ανωνυμία στο διαδίκτυο λέγονται προσωπικά στοιχεία (Personally Identifiable Information,PII) και χρησιμοποιούνται στην ασφάλεια των πληροφοριών. Αναφέρονται στις πληροφορίες που μπορούν να χρησιμοποιηθούν για την αποκλειστική αναγνώριση, την επαφή, ή τον εντοπισμό ενός μόνο προσώπου ή μπορεί να χρησιμοποιηθούν με άλλες πηγές που θα αναγνωρίζουν μοναδικά ένα και μόνο άτομο. Οι πληροφορίες αυτές μπορεί να είναι το ονοματεπώνυμο, αριθμό κοινωνικής ασφάλισης, τα βιομετρικά αρχεία, ή να συνδυάζονται με προσωπικές ή άλλες πληροφορίες ταυτότητας που συνδέονται ή συσχετίζονται με ένα συγκεκριμένο άτομο, όπως η ημερομηνία και τόπος γέννησης, το γένος της μητέρας, κλπ.

Ο όρος ανωνυμία εκτός από τα προσωπικά στοιχεία μπορεί να αναφέρεται σε ένα αυθαίρετο στοιχείο (π.χ. ένα ανθρώπινο, ένα αντικείμενο, έναν υπολογιστή), στο πλαίσιο ενός σαφώς καθορισμένου συνόλου. Η ανωνυμία του εν λόγω στοιχείου αναφέρεται στο ότι η ιδιοκτησία του εν λόγω στοιχείου δεν είναι αναγνωρίσιμη σε αυτό το σύνολο.

Ο όρος «ανώνυμο μήνυμα» συνήθως αναφέρεται σε μήνυμα (το οποίο είναι, για παράδειγμα, κάποια μορφή που μεταδίδονται μέσω του δικτύου), ότι δεν φέρει οποιαδήποτε πληροφορία σχετικά με τον αποστολέα στον αποδέκτη. [35] Ως εκ τούτου, είναι ασαφές εάν υπάρχουν περισσότερα τέτοια μηνύματα που έχουν σταλεί από τον ίδιο αποστολέα ή αν έχουν τον ίδιο αποδέκτη.

Οι τεχνολογίες ανωνυμίας χρησιμεύουν ως τα εργαλεία για την προστασία των ιδιωτικών ηλεκτρονικών συναλλαγών και προστατεύουν την μυστικότητα των χρηστών του Internet από το ένα άκρο της επικοινωνίας έως το άλλο. Αυτό επιτυγχάνεται με την απόκρυψη της σύνδεσης μεταξύ του αποστολέα και του παραλήπτη.

3.2.3 E-cash

Το ηλεκτρονικό χρήμα (επίσης γνωστό ως ηλεκτρονικό νόμισμα, ψηφιακό χρήμα ή ψηφιακό νόμισμα) αναφέρεται σε χρήματα ή πιστοποιητικά που ανταλλάσσονται μόνο ηλεκτρονικά. [36] Χαρακτηριστικά, αυτό περιλαμβάνει τη χρήση των δικτύων υπολογιστών, του Διαδικτύου και των ψηφιακών αποθηκευμένων συστημάτων αξίας. Η ηλεκτρονική μεταφορά Ταμείων (EFT) και η άμεση κατάθεση είναι παραδείγματα των ηλεκτρονικών χρημάτων. Επίσης, είναι ένας συλλογικός όρος για το οικονομικό σύστημα κρυπτογραφίας και τις τεχνολογίες που το επιτρέπουν.

Μέχρι σήμερα, η χρήση των ψηφιακών μετρητών έχει σχετικά χαμηλή κλίμακα. Μια σπάνια επιτυχία είναι το Octopus card system του Χονγκ Κονγκ , το οποίο άρχισε ως σύστημα πληρωμής διέλευσης και έχει μετατραπεί σε ένα ευρέως χρησιμοποιημένο ηλεκτρονικό σύστημα μετρητών. Η Σιγκαπούρη διαθέτει επίσης ένα ηλεκτρονικό χρήμα για την εφαρμογή μαζικής μεταφοράς (μετακινούμενα τρένα, λεωφορεία,

[35] http://en.wikipedia.org/wiki/Anonymity
[36] http://en.wikipedia.org/wiki/Electronic_money

κλπ.), το οποίο είναι παρόμοιο με του Χονγκ Κονγκ και του Octopus card system με βάση τον ίδιο τύπο κάρτας (FeliCa). Υπάρχει επίσης μία εφαρμογή στην Ολλανδία, που είναι γνωστή ως Chipknip.

Τι είναι όμως το e-cash; Ενώ πολλές διαφορετικές εταιρείες είναι πρόθυμες να προσφέρουν ηλεκτρονικό χρήμα, το e-cash, εκπροσωπείται από δύο μοντέλα. Το ένα είναι η on-line ηλεκτρονική μορφή μετρητών (που εισάγονται από DigiCash) η οποία επιτρέπει την ολοκλήρωση όλων των τύπων των συναλλαγών στο Διαδίκτυο. Η άλλη μορφή είναι η off-line. Ουσιαστικά χρησιμοποιείται μια κωδικοποιημένη κάρτα που θα μπορούσε να χρησιμοποιηθεί για πολλές από τις ίδιες συναλλαγές σαν μετρητά. Αυτή η off-line έκδοση (η οποία επίσης έχει on-line δυνατότητες) είναι υπό δοκιμή από Mondex σε συνεργασία με διάφορες τράπεζες.

Η πρωταρχική λειτουργία του e-cash είναι η διευκόλυνση των συναλλαγών στο Διαδίκτυο. Πολλές από τις συναλλαγές αυτές μπορεί να είναι μικρές σε μέγεθος και δεν θα είναι αποτελεσματικές από πλευράς κόστους σε σχέση με άλλα μέσα πληρωμής, όπως πιστωτικές κάρτες. Έτσι, οι WWW τοποθεσίες στο μέλλον μπορεί να χρεώσουν μια επίσκεψη $ 0,10, ή 0,25 δολάρια για να κατεβάσουμε ένα αρχείο γραφικών. Αυτά τα είδη των πληρωμών, μετατρέπουν το Διαδίκτυο σε μια συναλλαγή η οποία προσανατολίζεται σε φόρουμ, που απαιτούν μέσα που είναι εύκολα, φθηνά (από εμπόρους προοπτικών), εμπιστευτικά, και ασφαλές.

Το ηλεκτρονικό χρήμα είναι πλέον μια φυσική λύση, και οι εταιρείες που είναι πρωτοπόρες ισχυρίζονται ότι τα προϊόντα θα πληρούν τα κριτήρια που αναφέρει. Με την παροχή αυτού του είδους πληρωμής , τα κίνητρα για να παρέχουν αξιόλογες υπηρεσίες και προϊόντα μέσω του Διαδικτύου θα πρέπει να αυξηθούν. Για να ολοκληρωθεί η ψηφιακή επανάσταση χρήματος χωρίς σύνδεση είναι επίσης αναγκαίο περισσότεροι άνθρωποι να φέρουν μικρές συναλλαγές (π.χ. αγορά μιας εφημερίδας , αγορά ενός φλιτζανιού καφέ, κλπ.).

Η έννοια του ηλεκτρονικού χρήματος ξεκίνησε τουλάχιστον μια δεκαετία πριν. Όταν ένα άτομο γράφει μια επιταγή σχετικά με τον τραπεζικό λογαριασμό και την δίνει σε άλλο πρόσωπο με ένα λογαριασμό σε μια άλλη τράπεζα, οι τράπεζες δεν κάνουν μεταβίβαση των χρημάτων αυτών. Οι τράπεζες χρησιμοποιούν την ηλεκτρονική μεταφορά των χρημάτων. Το ηλεκτρονικό χρήμα, καταργεί την μεταφορά αυτή. Αντί να ζητούν οι τράπεζες τη μεταφορά των κεφαλαίων μέσω της επιταγής , το e-cash απλά μεταφέρει τα χρήματα από τον ένα τραπεζικό λογαριασμό στον άλλο.

Η πραγματικότητα του e-cash είναι λίγο πιο περίπλοκη, και αυτό είναι που κάνει τις συναλλαγές τόσο ασφαλείς και ιδιωτικές. Ο χρήστης κατεβάζει το ηλεκτρονικό χρήμα από τον τραπεζικό λογαριασμό με χρήση ειδικού λογισμικού και αποθηκεύει τα e-μετρητά στην τοπική μονάδα του σκληρού δίσκου. Για να πληρώσει έναν έμπορο WWW ηλεκτρονικά, ο E-cash χρήστης καταβάλει από το λογισμικό το επιθυμητό ποσό από το E-cash " wallet" στον τοπικό σκληρό δίσκο εμπόρων (" wallet") μετά από την συναλλαγή μέσω μιας E-cash τράπεζας για τον έλεγχο της γνησιότητας.

Ο έμπορος μπορεί να πληρώσει τους λογαριασμούς με αυτό το e-χρήμα ή να το ανεβάσει στο εμπορικό σκληρό νόμισμα του τραπεζικού λογαριασμού. Η E-cash επιχείρηση κάνει τα χρήματα σε κάθε συναλλαγή από τον έμπορο (αυτή η αμοιβή

είναι πολύ μικρή, εντούτοις) και από τα δικαιώματα που πληρώνονται από τις τράπεζες που παρέχουν στους πελάτες E-cash το λογισμικό/το υλικό έναντι μικρής μηνιαίας αμοιβής.

Οι συναλλαγές μεταξύ των ατόμων δεν θα υπόκειντο σε μια αμοιβή. Το E-cash διεθνοποιεί αληθινά την οικονομία, δεδομένου ότι ο χρήστης μπορεί να μεταφορτώσει τα χρήματα στο cyber-πορτοφόλι του σε οποιοδήποτε επιθυμητό νόμισμα. Ένας έμπορος μπορεί να δεχτεί οποιοδήποτε νόμισμα και να το μετατρέψει στο τοπικό νόμισμα όταν φορτώνεται το cybercash στον τραπεζικό λογαριασμό.

Στην έκταση που ένας χρήστης θέλει E-cash off-line, όλα αυτά είναι απαραίτητα στην τεχνολογία έξυπνων καρτών. Τα χρήματα φορτώνονται επάνω στην έξυπνη κάρτα, και τα πρόσθετα ηλεκτρονικά πορτοφόλια χρησιμοποιούνται για να ξεφορτώσουν τα χρήματα επάνω σε άλλες έξυπνες κάρτες ή άμεσα σε ένα σύστημα ανοικτής γραμμής. Οι έξυπνες κάρτες έχουν χρησιμοποιηθεί επιτυχώς σε άλλες χώρες για τέτοιες συναλλαγές. Τα χρήματα θα μπορούσαν επίσης να αφαιρεθούν από μια έξυπνη κάρτα και να μπουν σε έναν τραπεζικό λογαριασμό. Η Visa αναπτύσσει ένα σχετικό προϊόν, την αποθηκευμένη κάρτα αξίας. Αυτή η κάρτα έρχεται σε ποικίλες μετονομασίες, αλλά λειτουργεί περισσότερο σαν μια χρεωστική κάρτα από E-cash.

Στην ουσία, το E-cash συνδυάζει τα οφέλη άλλων μέσων συναλλαγής. Κατά συνέπεια, είναι παρόμοιο με τις χρεωστικές πιστωτικές κάρτες, αλλά το E-cash επιτρέπει στα άτομα να διεξάγουν συναλλαγές μεταξύ τους. Είναι παρόμοιο με τους προσωπικούς ελέγχους, αλλά είναι εφικτό για τις πολύ μικρές συναλλαγές.. Ενώ εμφανίζεται ανώτερο από άλλες μορφές, το E-cash δεν θα αντικαταστήσει εντελώς το νόμισμα εγγράφου. Η χρήση E-cash θα απαιτήσει το πρόσθετο υλικό, και οι περισσότεροι άνθρωποι θα έχουν πρόσβαση, αλλά όχι όλοι.

Εντούτοις, το E-cash παρουσιάζει τις πρόσθετες προκλήσεις για την ύπαρξη "μεσαζόντων" από την τρέχουσα κοινωνία νομίσματος εγγράφου. Όλο και περισσότερο, οι τράπεζες και άλλοι οικονομικοί μεσάζοντες θα χρησιμεύσουν απλά ως οι αποθήκες για τα χρήματα, τους δανειστές, και την επεξεργασία/την επαλήθευση των ηλεκτρονικών συναλλαγών. Η προσωπική αλληλεπίδραση με έναν αφηγητή, ή ακόμα και οι επισκέψεις σε μια τράπεζα ATM θα γίνουν ξεπερασμένες. Το μόνο που θα πρέπει να κάνει κανείς είναι να ανοίγει τον υπολογιστή του.

3.2.3.1 Οφέλη από τη χρήση των ηλεκτρονικών πληρωμών

- Ευκολία: Φυσικά, το πιο εμφανές όφελος από αυτό το μέσο πληρωμής είναι η ευκολία που μπορεί να μας προσφέρει. [37] Με τις ηλεκτρονικές πληρωμές η πληρωμή των λογαριασμών μπορεί να γίνει εύκολα, χωρίς τις συνήθεις μεγάλες γραμμές και ενοχλήσεις.

[37] http://el.tech-faq.com/what-are-electronic-payments.shtml&prev=hp

- Κάτω κόστος: λόγω αυτοματοποίησης των λειτουργιών, όπως η πιστωτική κάρτα επεξεργασίας και πληρωμής, οι ηλεκτρονικές πληρωμές μείωσαν το κόστος της επιχειρηματικής δραστηριότητας. Υπάρχει λιγότερο χαρτί που καταναλώνεται, καθώς και το προσωπικό, καθώς και οι πόροι που χρειάζονται, κι έτσι το κόστος είναι μικρότερο.

3.2.3.2 Ασφάλεια Ηλεκτρονικών πληρωμών

Τέθηκαν ερωτήματα σχετικά με την ασφάλεια των ηλεκτρονικών πληρωμών και τα περισσότερα από αυτά προέρχονται από το φόβο των εμπιστευτικών πληροφοριών και του ιδιωτικού κινδύνου. Η κλοπή ταυτότητας είναι μια έγκυρη ανησυχία, και αυτό έχει ρίξει κάποιες αμφιβολίες σχετικά με την ασφάλεια των ηλεκτρονικών πληρωμών.

Ωστόσο, υπάρχουν κάποια βασικά μέτρα ασφάλειας τα οποία μπορούν να ληφθούν για να ελαχιστοποιηθεί σε μεγάλο βαθμό ο κίνδυνος που ενέχεται. Ορισμένα από αυτά περιλαμβάνουν την εγκατάσταση και τη συνεχή ενημέρωση των ιών και anti-spyware προγραμμάτων. Η εγκατάσταση τείχους ασφαλείας, η ευαισθητοποίηση των νέων απειλών online και γνώσεων σχετικά με τον καλύτερο τρόπο για την αντιμετώπιση των απειλών αυτών θα βοηθήσει επίσης.

Η εξασφάλιση ότι η ηλεκτρονική συναλλαγή γίνεται μέσω ασφαλούς διακομιστή μπορεί επίσης σημαντικά να ελαχιστοποιήσει τον κίνδυνο αλλά και να θέσει σε κίνδυνο την πιστωτική μας κάρτα και τις οικονομικές μας πληροφορίες. Αυτό μπορεί να γίνει με την εξέταση για το βασικό εικονίδιο κλειδώματος ή του φυλλομετρητή μας και για "https" αντί για "http" στη γραμμή διευθύνσεων.

3.2.3.2 Συχνές απορίες για τη χρήση του e-cash στην διεθνή εταιρεία ECash Direct

1. Τι είναι ο λογαριασμός ECash Direct και πώς μπορώ να αποκτήσω έναν;

   Το ECash σημαίνει "ηλεκτρονικά μετρητά".[38] Το ECash είναι μια νομική μορφή νομίσματος που δημιουργείται μέσω του υπολογιστή η οποία μπορεί να αγοραστεί με πιστωτικές και χρεωστικές κάρτες, ηλεκτρονική επιταγή, επιταγή, έμβασμα, τραπεζική μεταφορά ή άλλες μορφές πληρωμής. Όταν ο χρήστης αγοράσει το ECash, μπορεί να το χρησιμοποιήσει σε εφαρμογές που χρησιμοποιούν το σύστημα ECash Direct. Ο λογαριασμός ECash Direct δημιουργείται αυτόματα όταν ο χρήστης καταχωρεί μια εφαρμογή που περιέχει ένα προϊόν ECash Direct. Κάθε λογαριασμός ECash Direct διαθέτει όνομα χρήστη και κωδικό πρόσβασης τα οποία επιλέγονται από τον χρήστη κατά την εγγραφή.

2. Πώς καταθέτω χρήματα στον λογαριασμό μου στο ECash Direct;

   Για να καταθέσετε κεφάλαια στον λογαριασμό σας στο ECash Direct, επιλέξτε Κατάθεση από την οθόνη ECash Direct και να επιλέξτε τη μέθοδο με

[38] http://gre.ecashdirect.net/faq/faq-ecash.html

την οποία θέλετε να προχωρήσετε σε κατάθεση και εισαγάγετε το ποσό που θέλετε να καταθέσετε. Στη συνέχεια, μπορείτε να κάνετε κλικ στο κουμπί Συνέχεια και η κατάθεσή σας θα επεξεργαστεί..

3. Ποια είναι τα τρέχοντα όρια καταθέσεων μέσω πιστωτικών καρτών σε λογαριασμούς ECash Direct;

   Τα τρέχοντα όρια καταθέσεων και αναλήψεων για όλες τις επιλογές πληρωμής βρίσκονται στη Σύνοψη όρων συναλλαγών στο Ταμείο.

4. Οι καταθέσεις μου στον λογαριασμό μου ECash Direct μέσω πιστωτικής κάρτας χρεώνονται ως αγορές ή ως ανάληψη μετρητών;

   Όλες οι καταθέσεις στον λογαριασμό σας ECash Direct μέσω πιστωτικών καρτών χρεώνονται ως αγορές. Όλες οι χρεώσεις από το ECash Direct λογίζονται ως αγορές. Ωστόσο, έχετε υπόψη σας ότι η Visa και/ή η MasterCard ενδέχεται να ταξινομήσουν αυτές τις χρεώσεις ως Ανάληψη μετρητών και θα σας χρεώσουν ανάλογα.

5. Πώς προχωρώ σε ανάληψη χρημάτων από τον λογαριασμό μου ECash Direct;

   Έχετε υπόψη σας ότι για να προχωρήσετε σε ανάληψη κεφαλαίων από τον λογαριασμό σας στο ECash Direct, ενδέχεται να απαιτηθούν συγκεκριμένες πληροφορίες.

   Επιλέξτε Ανάληψη από την οθόνη ECash Direct και κάντε κλικ στη μέθοδο με την οποία επιθυμείτε να προχωρήσετε σε ανάληψη - πιστωτική κάρτα ή επιταγή (έχετε υπόψη σας τους όρους μας που αναφέρονται παρακάτω). Στη συνέχεια, μπορείτε να κάνετε κλικ στο κουμπί Συνέχεια και η ανάληψή σας θα επεξεργαστεί.

6. Εάν προχωρήσω σε ανάληψη χρημάτων από τον λογαριασμό μου στο ECash Direct στην πιστωτική μου κάρτα, πόσος χρόνος χρειάζεται συνήθως για να εμφανιστούν στον λογαριασμό της πιστωτικής μου κάρτας;

   Κατά την ανάληψη χρημάτων από τον λογαριασμό σας στο ECash Direct στην πιστωτική σας κάρτα, απαιτούνται συνήθως 2-5 εργάσιμες ημέρες για να εμφανιστούν στον λογαριασμό της πιστωτικής σας κάρτας. Εάν έχουν περάσει 5 εργάσιμες ημέρες από τη στιγμή που προχωρήσατε στην ανάληψη των χρημάτων από τον λογαριασμό σας στο ECash Direct και δεν εμφανίζονται στον λογαριασμό σας, επικοινωνήστε με την τράπεζα που εξέδωσε την πιστωτική σας κάρτα και ζητήστε να μάθετε εάν υπάρχει κάποια εκκρεμής πίστωση από το ECash Direct. Εάν δεν υπάρχει, επικοινωνήστε με το ECash Direct.

7. Πόσο μεγάλη ανάληψη χρημάτων μπορώ να πραγματοποιήσω προς την πιστωτική μου κάρτα;

   Κατά την ανάληψη από τον λογαριασμό σας στο ECash Direct προς την πιστωτική σας κάρτα, μπορείτε να κάνετε ανάληψη χρημάτων έως του ποσού

που έχετε καταθέσει μέσω πιστωτικής κάρτας καθ' όλη τη διάρκεια ζωής των λογαριασμών σας στο ECash Direct. Όταν προχωρήσετε σε ανάληψη αυτού του ποσού, τυχόν υπόλοιπα κεφάλαια πρέπει να αναληφθούν με άλλες μεθόδους.

8. Μπορώ να ζητήσω ανάληψη μέσω επιταγής ή πιστωτικής κάρτας, ανάλογα με την προτίμησή μου;

   Όχι. Εάν έχετε προχωρήσει σε κατάθεση στον λογαριασμό σας στο ECash Direct ανά πάσα στιγμή με χρήση πιστωτικής κάρτας, θα πρέπει πρώτα να προχωρήσετε σε ανάληψη αυτού του ποσού προς την πιστωτική σας κάρτα. Μπορείτε να προχωρήσετε σε ανάληψη του επιπλέον υπολοίπου σας μέσω επιταγής. Οι πιστωτικές κάρτες έχουν προτεραιότητα. Δεν μπορείτε να ζητήσετε ανάληψη μέσω επιταγής εάν δεν έχετε πρώτα προχωρήσει σε ανάληψη του συνόλου των καταθέσεών σας που πραγματοποιήθηκαν μέσω πιστωτικής κάρτας. Δεν μπορείτε να προχωρήσετε σε ανάληψη προς την πιστωτική σας κάρτα ποσού μεγαλύτερου από αυτό που έχετε καταθέσει.

9. Έπρεπε να επανεγκαταστήσω ένα πρόγραμμα που περιείχε την εφαρμογή ECash Direct. Μπορώ να επιστρέψω στον παλιό μου λογαριασμό ECash Direct;

   Ναι, συγκεκριμένες εφαρμογές θα σας επιτρέψουν να ενεργοποιήσετε εκ νέου τον παλιό σας λογαριασμό ECash Direct. Όταν πραγματοποιήσετε είσοδο στην εφαρμογή για πρώτη φορά μετά την επανεγκατάσταση, θα πρέπει να επιλέξετε το κουμπί Ενεργοποίηση. Έχετε υπόψη σας ότι για να ενεργοποιήσετε εκ νέου τον παλιό σας λογαριασμό ECash Direct θα πρέπει να γνωρίζετε τον αριθμό του λογαριασμού, το όνομα χρήστη και τον κωδικό πρόσβασής σας.

10. Λαμβάνω ένα μήνυμα σφάλματος "Ο λογαριασμός είναι κλειδωμένος". Τι κάνω;

    Εάν λάβετε αυτό το μήνυμα, επικοινωνήστε με την ομάδα εξυπηρέτησης πελατών/τεχνικής υποστήριξης. Θα βοηθήσετε το τμήμα εξυπηρέτησης πελατών μας εάν γνωρίζετε τον αριθμό λογαριασμού σας προτού επικοινωνήσετε μαζί μας. Εάν δεν γνωρίζετε ποιος είναι ο αριθμός λογαριασμού σας, μπορείτε να τον βρείτε σε μία από τις ακόλουθες τρεις σελίδες (εάν ισχύει):

    1. στην αρχική σελίδα του Ταμείου,
    2. στο πεδίο "Σημαντική σημείωση" στη σελίδα Κατάθεση μέσω επιταγής ή
    3. στη σελίδα καταθέσεων μέσω Εμβάσματος.

11. Διαθέτω λογαριασμό ECash Direct αλλά δεν μπορώ να θυμηθώ το όνομα χρήστη και/ή τον κωδικό πρόσβασής μου. Τι πρέπει να κάνω;

Δυστυχώς, για λόγους ασφάλειας, δεν μπορούμε να σας στείλουμε μήνυμα ηλεκτρονικού ταχυδρομείου με το όνομα χρήστη και τον κωδικό πρόσβασής σας. Θα

πρέπει να επικοινωνήσετε μαζί μας μέσω μιας εκ των 24ωρων γραμμών ατελούς κλήσης για να λάβετε αυτά τα στοιχεία.

3.2.4 E-voting

Με τον όρο ηλεκτρονική ψηφοφορία (electronic voting, e-voting), εννοούμε την άσκηση του εκλογικού δικαιώματος, με τη χρήση ηλεκτρονικών μεθόδων.[39] Πραγματοποιείται μέσω της χρήσης είτε του Διαδικτύου (on line voting) είτε άλλων δικτύων, παρέχοντας στους ψηφοφόρους τη δυνατότητα να προβούν στην κατάθεση μίας ασφαλούς και μυστικής ψήφου, με τη βοήθεια υπολογιστικών συστημάτων.

Δυο είναι τα θεμελιώδη στοιχεία που συνθέτουν την ιδιαίτερη φύση της ηλεκτρονικής ψήφου και τη διαφοροποιούν σε μεγάλο βαθμό από τα υπάρχοντα συστήματα της εκλογικής διαδικασίας:

- Η δυνατότητα άσκησης του εκλογικού δικαιώματος από απόσταση, χωρίς την αυτοπρόσωπη, επομένως, παρουσία του ψηφοφόρου στο εκλογικό τμήμα

.

- Η χρήση υπολογιστικού συστήματος και κατά συνέπεια αυτοματοποιημένων μεθόδων, για την οργάνωση και διεξαγωγή της όλης εκλογικής διαδικασίας.

Η υιοθέτηση ενός συστήματος ηλεκτρονικής ψηφοφορίας πρέπει να πληροί τις εξής δύο προϋποθέσεις [40]

- να επιτρέπει την όσο το δυνατόν μεγαλύτερη συμμετοχή των πολιτών

- να αναβαθμίζει την ποιότητα επιτρέποντας την συμμετοχή καλύτερα ενημερωμένων πολιτών.

Ο κίνδυνος που ελλοχεύει συνίσταται στο ότι , η χρησιμοποίηση των νέων τεχνολογιών μπορεί να δημιουργήσει ανισότητες , εμποδίζοντας ένα τμήμα του πληθυσμού να συμμετάσχει. Το πρόβλημα γίνεται πιο πολύπλοκο εάν ληφθεί υπ' όψιν το ζήτημα της ασφάλειας της ηλεκτρονικής ψήφου σε συνδυασμό με την χρήση του κατάλληλου ψηφιακού πιστοποιητικού. Η χρήση των νέων τεχνολογιών μπορεί να οδηγήσει σε περιθωριοποίηση ομάδες του πληθυσμού από το πολιτικό γίγνεσθαι.

Επί πλέον υπάρχει ο κίνδυνος να αλλοιωθούν τα εκλογικά αποτελέσματα εάν δεν διασφαλιστεί η ασφαλής διαδρομή της ψήφου και η ελευθερία έκφρασης των πολιτών. Η συνταγματικότητα λοιπόν της ηλεκτρονικής ψήφου είναι άμεσα συναρτημένη με την ισότητα πρόσβασης , την μυστικότητα της ψήφου και την ελευθερία έκφρασης των πολιτικών ιδεών δια μέσω της ψήφου. Η ύπαρξη ψηφιακών εκλογικών κέντρων, ή σημείων (kiosks) με ελεύθερη πρόσβαση στο διαδίκτυο φαίνεται να λύνουν σε σημαντικό βαθμό το πρόβλημα της πρόσβασης.

---

[39] http://www.ebusiness-lab.gr/Portals/12/Ptyxiakes/Presentations/Mitsou_Kalogirou_

[40] http://www.infolaw.gr/articles.asp?ArticleID=602

Ένα άλλο στοιχείο που πρέπει να ληφθεί υπ΄ όψιν είναι το ότι τα συστήματα ηλεκτρονικής ψήφου πρέπει να είναι απλά και προσιτά στον πολίτη για να μπορούν να χρησιμοποιηθούν εύκολα από αυτόν . Το παράδειγμα της πολιτείας της Φλόριντα στις πρόσφατες αμερικανικές προεδρικές εκλογές αποτελεί παράδειγμα προς αποφυγή.

Το συνταγματικά κατοχυρωμένο πολιτικό δικαίωμα της ελεύθερης ψήφου εμπεριέχει δύο βασικές παραμέτρους : την ελεύθερη διαμόρφωση της συνείδησης των εκλογέων και την ελεύθερη έκφραση αυτής μέσω της ψήφου. Η χρήση της ηλεκτρονικής ψήφου μπορεί να έχει σημαντικές παραμέτρους όπως η γρηγορότερη και καλύτερη ενημέρωση των ψηφοφόρων με την χρήση των νέων τεχνολογιών.

Έχει ήδη προταθεί σε άλλες χώρες η δημιουργία ειδικών links στις ιστοσελίδες των πολιτικών κομμάτων για την ενημέρωση των εκλογέων. Βέβαια εάν υιοθετηθεί η ηλεκτρονική ψήφος είναι ευνόητο ότι οποιαδήποτε πολιτική διαφήμιση στην οθόνη του υπολογιστή την ώρα της ψηφοφορίας θα πρέπει να απαγορευθεί. Ένα ζήτημα που τίθεται είναι η δυνατότητα έκφρασης μέσω του άκυρου ψηφοδελτίου και ο τρόπος εξασφάλισης αυτής της δυνατότητας στην ηλεκτρονική ψηφοφορία.

Η μυστικότητα της ψήφου πρέπει να εξασφαλίζεται στην ηλεκτρονική ψηφοφορία. Αυτό σημαίνει ότι η έκφραση της βούλησης του ψηφοφόρου δεν πρέπει να αποτελεί αντικείμενο ελέγχου από οποιαδήποτε δημόσια αρχή και επίσης ότι ουδείς πρέπει να γνωρίζει τι ψήφισε ο πολίτης. Δεν πρέπει να υπάρχει δυνατότητα παραβίασης της μυστικότητας της ψήφου την στιγμή της έκφρασης, της αποστολής, της συγκέντρωσης και της κατανομής της ηλεκτρονικής ψήφου.

Η ανωνυμία πρέπει να εξασφαλίζεται καθ’ όλη την διάρκεια της ενέργειας της ψηφοφορίας. Η αξιοπιστία και πρωτίστως η συνταγματικότητα ενός συστήματος ηλεκτρονικής ψήφου εξασφαλίζεται από τη εξασφάλιση της μυστικότητας της ψήφου. Η διαβίβαση και η λήψη της ηλεκτρονικής ψήφου πρέπει να εξασφαλίζονται απολύτως. Η μυστικότητα είναι άμεσα συνυφασμένη και με την απουσία οποιασδήποτε εξωτερικής επίδρασης επί των πολιτών στον τόπο ηλεκτρονικής ψηφοφορίας.

Άμεση σχέση υπάρχει και με την συνταγματικά κατοχυρωμένη προστασία του ιδιωτικού βίου. Οποιαδήποτε στοιχεία, δεδομένα, συνδεδεμένα με τον ψηφοφόρο και την ψηφοφορία με ηλεκτρονικό τρόπο πρέπει να έχουν εμπιστευτικό χαρακτήρα. Είναι αδιανόητο για παράδειγμα να υπάρξει διαρροή ή ακόμα και πώληση στην αγορά στοιχείων των πολιτών που προέρχονται από τους εκλογικούς καταλόγους. Είναι ευνόητο ότι οποιαδήποτε πρόσβαση στα ανωτέρω στοιχεία πρέπει να είναι επιτρεπτή μόνο στα εξουσιοδοτημένα όργανα.

Οι εκλογές αποτελούν σημαντικό πολιτικό γεγονός και η ηλεκτρονική ψηφοφορία είναι ένας νέος τρόπος συμμετοχής στο πολιτικό γίγνεσθαι. Οποιεσδήποτε αλλαγές στον τρόπο ψηφοφορίας πρέπει να είναι συμβατές με τις αρχές τις νομιμότητας, της διαφάνειας , του πλουραλισμού, της ευχέρειας του δικαστικού ελέγχου.

Βασικό στοιχείο των ελεύθερων, δημοκρατικών ,εκλογών στα φιλελεύθερα πολιτεύματα είναι η εμπιστοσύνη στην διαφάνεια και νομιμότητα της διαδικασίας της

ψηφοφορίας και καταμέτρησης , που έχει αποκτηθεί με την πάροδο του χρόνου και τον ομαλό πολιτικό βίο. Στα κλασσικά συστήματα εκλογών υπάρχει η δυνατότητα άμεσης επαφής και ελέγχου μεταξύ ψηφοφόρων, εκπροσώπων των πολιτικών κομμάτων και των αρχών που έχουν επωμισθεί την διενέργεια των εκλογών.

Αντίθετα στην ηλεκτρονική ψηφοφορία αυτή η φυσική επαφή δεν υφίσταται το software και hardware που θα χρησιμοποιείται πρέπει να είναι απολύτως αξιόπιστο για να εξασφαλίζεται το αδιάβλητο των εκλογών. Η εμπιστοσύνη στο σύστημα που θα χρησιμοποιηθεί για την διενέργεια των εκλογών με ηλεκτρονικό τρόπο αποτελεί απαραίτητο στοιχείο για την διασφάλιση των συμμετεχόντων στην εκλογική διαδικασία. Στα κλασσικά συστήματα εκλογών λόγω του αποκεντρωτικού χαρακτήρα τους (πολλά εκλογικά κέντρα) περιορίζονται οι πιθανότητες αλλοίωσης του αποτελέσματος.

Στην ηλεκτρονική ψηφοφορία όμως καθώς το σύστημα είναι κεντρικό πρέπει να εξασφαλισθεί η διαφάνεια και η εμπιστοσύνη των πολιτών. Είναι απαραίτητη η συνεργασία τεχνικών, νομικών και πολιτικών για την λειτουργία του συστήματος με διαφάνεια και σύμφωνα με τις συνταγματικές επιταγές ‘ πολύ δε περισσότερο με την ηλεκτρονική ψηφοφορία όπου δεν έχουν όλοι οι άμεσα εμπλεκόμενοι τις απαραίτητες γνώσεις , για αυτό και το λογισμικό και το είδος του διαδικτύου που θα χρησιμοποιηθούν πρέπει να επιτρέπουν την διαφάνεια και την ευχέρεια ελέγχου.

Η αξιοπιστία των εκλογικών αποτελεσμάτων και η μυστικότητα της εκπεφρασμένης βούλησης των πολιτών αποτελούν συνταγματικές επιταγές. Το γεγονός ότι και τα κλασσικά συστήματα ψήφου δεν προσφέρουν απόλυτη ασφάλεια δεν αποτελεί επιχείρημα για την μείωση των υψηλών επιπέδων ασφαλείας που απαιτούνται για την ηλεκτρονική ψηφοφορία. Η εμπιστοσύνη των πολιτών στο σύστημα διενέργειας εκλογών είναι άμεσα συνυφασμένη με την εμπιστοσύνη τους στην αξιοπιστία του πολιτικού συστήματος όπως αυτό κατοχυρώνεται στο Σύνταγμα.

Όταν η ψηφοφορία που πραγματοποιείται από τον χώρο εργασίας του ψηφοφόρου, λόγω της εγγενούς ανισότητας που υπάρχει στη σχέση εργοδότη και υπαλλήλου, υπάρχει ο κίνδυνος ο τελευταίος να υποχρεωθεί να αποκαλύψει το περιεχόμενο της ψήφου του ή και να μεταβάλλει την επιλογή του. Ακόμη όμως και στις περιπτώσεις όπου η πίεση δεν είναι τόσο προφανής, η ύπαρξη εσωτερικού δικτύου στο χώρο της επιχείρησης, παρέχει τη δυνατότητα σε μέλη υψηλότερου διοικητικού επιπέδου να παρακολουθήσουν και να καταγράψουν τη δραστηριότητα σε κάθε σταθμό εργασίας, προκειμένου να λάβουν γνώση των πολιτικών πεποιθήσεων των εργαζομένων. Οι κίνδυνοι, επομένως, που απορρέουν από το περιβάλλον εργασίας για τη μυστικότητα της ψήφου, είναι πολλοί.

Ακόμη και στην περίπτωση όπου ο πολίτης επιλέγει να ψηφίσει από την οικία του, είναι ιδιαίτερα δύσκολο να φανταστεί κάποιος ένα ιδεατό περιβάλλον απόλυτης απομόνωσης, το οποίο θα μπορούσε να προσεγγίσει τα επιθυμητά επίπεδα ακεραιότητας της διαδικασίας, όμοιας με εκείνη που πραγματοποιείται στον προστατευμένο χώρο του εκλογικού τμήματος. [41] Η οικογένεια αποτελεί ένα χώρο όπου η έννοια της ιδιωτικότητας δεν μπορεί να οριοθετηθεί με την ίδια ακρίβεια,

[41] http://www.teg.cti.gr/Library/e-voting/Systimata%20Hlektronikis%20Psifoforias.rtf

όπως συμβαίνει στην περίπτωση διαχωρισμού μεταξύ δημόσιας σφαίρας και ιδιωτικής και οικογενειακής ζωής του ατόμου. Ως ιδιωτική, σε σύγκριση με την οικογενειακή ζωή, λογίζεται η ατομική ζωή, η ζωή δηλαδή του ατόμου καθ΄ εαυτό σε σύγκριση με την ζωή του ατόμου ως μέλος της οικογένειας.

Στο πλαίσιο της οικογενειακής εστίας, οι σχέσεις που αναπτύσσονται μεταξύ των μελών της, γνωρίζουν μεγαλύτερα επίπεδα αλληλεξάρτησης σε σύγκριση με τις κοινωνικές σχέσεις. Ο εκλογέας που ψηφίζει ηλεκτρονικά από το σπίτι του είναι πολύ πιθανό να μην θέλει ή να μην είναι σε θέση να διατηρήσει κρυφή την επιλογή του. Το φαινόμενο της λεγόμενης «οικογενειακής ψήφου» (family voting), η ομοιομορφία δηλαδή που παρουσιάζεται στις πολιτικές επιλογές μίας οικογένειας και η οποία είναι αποκαλυπτική της απουσίας αυτόνομης πολιτικής βούλησης από τα λιγότερο πλεονεκτούντα σε γνώσεις ή δύναμη, μέλη της, όσον αφορά την ηλεκτρονική ψηφοφορίας, μπορεί να εδράζεται σε πολλές αιτίες.

- το ψηφιακό χάσμα, τα διαφορετικά δηλαδή επίπεδα ή και η ανυπαρξία εξοικείωσης με τις νέες τεχνολογίες, αναμφισβήτητα λειτουργεί σε βάρος εκείνων που θα αναζητήσουν βοήθεια για να ασκήσουν το εκλογικό τους δικαίωμα,
- συσκευές όπως η ψηφιακή τηλεόραση ή οι υπολογιστές, θεωρούνται αντικείμενα κοινής κτήσης και χρήσης, γι' αυτό και βρίσκονται σε χώρους όπου συνήθως έχουν πρόσβαση όλα τα μέλη της οικογένειας, οπότε είναι αρκετά δύσκολο για ένα μέλος να επιτύχει την πλήρη απομόνωση του προκειμένου να αποφασίσει αυτόνομα τι θα ψηφίσει. Πέρα από τα παραπάνω, πολλές περιπτώσεις οικογενειακής ψήφου μπορεί να οφείλονται στην ανάρμοστη ή υπέρμετρη πίεση που υφίσταται κάποιος προκειμένου να ψηφίσει με συγκεκριμένο τρόπο.

Ανεξάρτητα από τις αιτίες που μπορούν να οδηγήσουν στην διακινδύνευση της μυστικότητας της ψηφοφορίας, η δημιουργία τέτοιων φαινομένων, είναι δυνατόν να λάβει μεγαλύτερες διαστάσεις, με την εισαγωγή της ηλεκτρονικής ψηφοφορίας, γεγονός που θα θέσει υπό αμφισβήτηση το εκλογικό αποτέλεσμα.

Στην αντίπερα όχθη της μυστικότητας, βρίσκεται η διαφάνεια που πρέπει να χαρακτηρίζει κάθε εκλογική διαδικασία. Η λειτουργία των ηλεκτρονικών συστημάτων δεν μπορεί να είναι σχεδιασμένη με τέτοιο τρόπο που να μην αφήνει περιθώριο για την άσκηση ελέγχου εκ μέρους των αρμόδιων αρχών. Οι δύο αυτές αρχές δεν αντιστρατεύονται η μία την άλλη, καθώς είναι δυνατόν οι ηλεκτρονικές ψήφοι να κωδικοποιούνται και να καταμετρούνται μετά τον έλεγχο και τον αποχωρισμό τους από τα στοιχεία που είναι διακριτικά της ταυτότητας του ψηφοφόρου.

Συμπερασματικά μπορούμε να πούμε ότι η εξέλιξη των εκλογικών συστημάτων συμπεριλαμβανομένου και του τρόπου ψηφοφορίας αντικατοπτρίζουν την εξέλιξη του πολιτικού συστήματος. Η τεχνολογία μπορεί να βοηθήσει σημαντικά και να ενισχύσει την συμμετοχή των πολιτών στα κοινά. Δεν μπορεί όμως από μόνη της να αναδομήσει το δημοκρατικό πολίτευμα. Το πάτημα ενός κουμπιού στο πληκτρολόγιο

του υπολογιστή δεν μπορεί να αντικαταστήσει την ανθρώπινη συμμετοχή στο κοινωνικό-πολιτικό γίγνεσθαι. [42]

3.2.5 Ανώνυμες IP

Συχνά οι διευθύνσεις (όπως οι διευθύνσεις IP, ή Ethernet MACs) είναι ένα μοναδικό προσδιοριστικό που εμφανίζονται καθ' όλη την διάρκεια επικοινωνίας ενός χρήστη. Επιπλέον αυτές οι επίμονες διευθύνσεις μπορεί να είναι συνδεδεμένες με φυσικά πρόσωπα, συμβιβάζοντας σοβαρά τη μυστικότητά τους. Με το να υπάρχει ανωνυμία στο στρώμα επικοινωνίας μπορεί να προστατευθεί η μυστικότητα των χρηστών, και να προστατευθούν τα συγκροτήματα ηλεκτρονικών υπολογιστών από την ανάλυση κυκλοφορίας.

Με τη συνεχώς αυξανόμενη ανταλλαγή πληροφοριών που διατίθενται στον Παγκόσμιο Ιστό, υπάρχει μια ολοένα αυξανόμενη απειλή των κινδύνων όπως η απάτη, κλοπή ταυτότητας, τη χειραγώγηση της ενημέρωσης, και η δολιοφθορά [43] Επιπλέον, τα δικαιώματα ενός ατόμου στην ιδιωτική ζωή είναι διαρκώς υπό αυξημένο έλεγχο στο χώρο εργασίας από τους εργοδότες οι οποίοι συχνά ελέγχουν τα email, τους web browsing, τους instant messenger και τις συνομιλίες.

Η IP διεύθυνση πρέπει να θεωρείται από εδώ και πέρα ως προσωπικό δεδομένο, σύμφωνα με την αρμόδια επιτροπή της Ευρωπαϊκής Ένωσης.[44] Ο Γερμανός επίτροπος για την προστασία των δεδομένων, Peter Scharr, ετοιμάζει μία αναφορά σχετικά με το πώς διαχειρίζονται ζητήματα ιδιωτικότητας οι μηχανές αναζήτησης όπως αυτές της Google, της Yahoo και της Microsoft. Ο Scharr υποστηρίζει πως όταν κάποιος αναγνωρίζεται στο διαδίκτυο από την διεύθυνση IP του υπολογιστή του τότε αυτό πρέπει να θεωρείται προσωπική πληροφορία.

Σε αντίθεση η Google, υποστηρίζει πως κάτι τέτοιο απλά καθορίζει την φυσική τοποθεσία του υπολογιστή και όχι το ποιος τον χειρίζεται. Φυσικά και οι δύο απόψεις έχουν την βάση και την πρακτική τους απόδειξη, ενώ από την πλευρά της η Google τονίζει πως αποθηκεύει στοιχεία για τις IPs όχι για να μάθει τα ονόματα των χρηστών που την επισκέπτονται αλλά κυρίως για να βελτιώσει τα αποτελέσματα της μηχανής της και φυσικά να δημιουργήσει ακόμα καλύτερες και στοχευμένες διαφημίσεις.

Φαίνεται λοιπόν ότι σύντομα θα έχουμε εξελίξεις στην πολιτική που ακολουθεί κάθε μεγάλη μηχανή αναζήτησης. Και αν αλλάξει το νομοθετικό πλαίσιο στην Ευρωπαϊκή ένωση, πολλά θα πρέπει να γίνουν από αυτές ώστε να αποφύγουν τις κυρώσεις που θα επιβάλει η ΕΕ σε όσους δεν συμμορφωθούν με τις υποδείξεις της.

Οι HTTP proxies μπορεί να χρησιμοποιηθούν από τους χρήστες του internet για να αποκρύψουν την IP (Internet Protocol) διεύθυνση. Οποιαδήποτε συσκευή ή υπολογιστής που συνδέεται στο Internet έχει έναν μοναδικό αριθμό που του

---

[42] http://www.infolaw.gr/articles.asp?ArticleID=602

[43] http://el.tech-faq.com/http-proxies.shtml&prev=hp&rurl=translate.google.com

[44] http://www.pcw.gr//Article/News-General-Latest/IP_address_private_data/179-2945.html

αποδίδεται και του επιτρέπει τον ακριβή προσδιορισμό και την επικοινωνία. Κλέφτες μπορούν να χρησιμοποιήσουν αυτή τη διεύθυνση ανυποψίαστων χρηστών του Διαδικτύου για να παρακολουθήσουν τις συνήθειες τους και να αποκτήσουν κρίσιμες πληροφορίες που μπορούν να τους επιτρέψουν να κλέψουν την ταυτότητα τους.

Οι εργοδότες χρησιμοποιούν την IP διεύθυνση της εταιρείας των ηλεκτρονικών υπολογιστών, σε συνδυασμό με άλλες μεθόδους, για την παρακολούθηση των εργαζομένων πάνω στις Internet συνήθειες τους ,κατά την εργασία τους. Υπάρχει μια διαρκής συζήτηση επί του δικαιώματος της ιδιωτικής ζωής ενός ατόμου, αλλά ο νόμος συνήθως υποστηρίζει την πλευρά του εργοδότη για το θέμα αυτό.

Ως αποτέλεσμα αυτών των ζητημάτων, όλο και περισσότεροι χρήστες χρησιμοποιούν HTTP proxies τους για την προστασία της ανωνυμίας στο web-surfing. Οι HTTP proxies επιτρέπουν σε έναν χρήστη να σερφάρει στο διαδίκτυο ανώνυμα. Οι χρήστες μπορούν να επισκεφθούν οποιοδήποτε δικτυακό τόπο που θέλουν με το πρόσχημα μιας εντελώς ανώνυμης IP διεύθυνση.

Ωστόσο, οι HTTP proxies δεν είναι πάντα ασφαλής. Ορισμένα από αυτά έχουν μείνει ανοικτά, είτε από πρόχειρης διαχείρισης ή επιλήψιμη κακόβουλη πρόθεση. Σε αυτές τις περιπτώσεις μπορεί να εκτεθεί ο χρήστης σε ακόμη περισσότερες απόπειρες πειρατείας και όλα τα ήθη της απάτης.

3.2.6 Απειλές στην ανωνυμία

Οι κυριότερες απειλές που ενδέχεται να αντιμετωπίσουμε ως χρήστες του Internet σήμερα, προέρχονται από:[45]

- ✓ Το x άτομο που επικοινωνεί, είτε μέσω e-mail, σε chat rooms και message boards είτε μέσω instant messengers. Αν δεν γνωρίζουμε το άτομο στην πραγματική ζωή, καλό θα ήταν να αποφύγουμε να του αποκαλύψουμε την πραγματική μας ταυτότητα. Είναι απίστευτο το μέγεθος των πληροφοριών που μπορεί να συγκεντρώσει κάποιος μύστης απλά και μόνο γνωρίζοντας το όνομά μας. Πρόκειται για μια μορφή social engineering/phreaking (απόσπαση πληροφοριών μέσω κοινωνικής εξαπάτησης π.χ. μέσω τηλεφώνου) πολύ δημοφιλή στην τάξη των hackers.

- ✓ Άτομα που έχουν φυσική πρόσβαση στον υπολογιστή μας. Φροντίζουμε όταν έχουμε κάποια δραστηριότητα που θέλουμε να αποκρύψουμε από το οικείο ή και το εταιρικό μας περιβάλλον: α) να μην έχουμε απρόσκλητη παρέα πάνω από το κεφάλι μας και β) εφόσον κάποιος άλλος χρησιμοποιεί τον υπολογιστή, τίποτα να μην αποκαλύπτει τις συνήθειές μας.

- ✓ Διαχειριστές Web sites που επισκεπτόμαστε. Οι περισσότεροι Web administrators (και όχι μόνο) έχουν ως χόμπι την ανάλυση των logs (αρχεία καταγραφής δραστηριότητας) του Web site που διαχειρίζονται. Μέσα από

[45] http://www.go-online.gr/ebusiness/specials/article.html?article_id=417

αυτά τα logs παίρνουν πληροφορίες όπως αριθμός επισκέψεων διεύθυνση και αριθμός αιτήσεων ανά IP, τύπος αιτήσεων (ποια αρχεία) κ.ο.κ. Το μόνο που χρειάζεται είναι ένα καλό πρόγραμμα ούτως ώστε να γίνει πλήρης ομαδοποίηση των "δραστηριοτήτων μας" και η ανάλυση των cookies που έχουμε στον υπολογιστή μας για να δημιουργηθεί το προφίλ μας (ως ένα βαθμό βέβαια ατελές).

- ✓ ISPs και λοιπούς παροχείς δικτυακών υπηρεσιών. Οποιοσδήποτε μας παρέχει σε κάποιο βαθμό πρόσβαση στο Internet και πρόσβαση σε συγκεκριμένες υπηρεσίες μπορεί να μας ελέγξει. Απλοί μηχανισμοί επιτρέπουν την καταγραφή όλων των εισερχόμενων/εξερχόμενων δεδομένων στον server που λειτουργεί ως προσωπική πύλη μας στο Internet.

- ✓ Crackers**.** Εκμεταλλευόμενοι κενά ασφάλειας του λειτουργικού συστήματος και του browser που χρησιμοποιούμε, οι crackers μπορούν να αποκτήσουν εύκολα πρόσβαση σε όλα τα αρχεία του υπολογιστή μας, συγκεντρώνοντας μεγάλο αριθμό πληροφοριών για τις δικτυακές μας συνήθειες αλλά και όποια ευαίσθητα προσωπικά δεδομένα συνηθίζουμε να διατηρούμε στον υπολογιστή μας.

- ✓ Πολυεθνικές και διαφημιστικές εταιρείες**.** Οι μεγάλες εταιρείες έχουν δύο λόγους για να ελέγχουν την αναπτυσσόμενη δικτυακή δραστηριότητα των χρηστών καθώς και τις δικτυακές του συνήθειες. Ο πρώτος είναι η συλλογή στατιστικών στοιχείων για επιτυχημένη έρευνα αγοράς, ο δεύτερος είναι ο ίδιος ο πόλεμος των πληροφοριών - εξάλλου το παιχνίδι της εξουσίας έχει να κάνει με τον έλεγχο της γνώσης.

- ✓ Κυβερνήσεις**.** Οι κυβερνήσεις και ιδίως αυτές των μεγάλων χώρων του πλανήτη μπορούν να ασκήσουν πιέσεις στους ίδιους τους παροχείς της δικτυακής υποδομής του Internet, των εταιρειών δηλαδή που ευθύνονται για την κεντρική λειτουργία του Διαδικτύου και να ελέγξουν όλη την αναπτυσσόμενη δικτυακή δραστηριότητα. Φημολογείται ότι τέτοια είδους παρακολούθηση ήδη υφίσταται ενώ ο αντίλογος ισχυρίζεται ότι είναι τέτοιος ο όγκος των πληροφοριών που είναι αδύνατη η επεξεργασία του- ωστόσο κανείς δεν μπορεί να είναι σίγουρος.

3.2.7 Ζητήματα που αντιμετωπίζουν οι ανώνυμοι

Οι προσπάθειες στην ανωνυμία δεν συναντιούνται πάντα με την υποστήριξη της κοινωνίας. [46] Υπάρχει μια τάση της κοινωνίας στη δυσπιστία κάποιου ο οποίος καταβάλλει προσπάθεια να διατηρήσει την ανωνυμία τους. Αυτό συνοψίζει συχνά στη δήλωση, " Εσείς δεν θα θέλατε να μείνετε ανώνυμοι εκτός αν είχατε κάτι να κρύψετε". Η επίπτωση είναι ότι δεν υπάρχει κανένας νόμιμος λόγος να κρύψει

[46] http://blogz.gr/search/google?cx=001811651856122118421%3Akclaghsbst0&cof=FORID%3A11&query=%CE%B1%CE%BD%CF%89%CE%BD%CF%85%CE%BC%CE%AF%CE%B1&form_id=google_cse_searchbox_form#1125

κάποιος την ταυτότητα του από τον κόσμο συνολικά. Η ανωνυμία διαφωνεί μερικές φορές με τις πολιτικές και τις διαδικασίες των κυβερνήσεων ή των ιδιωτικών οργανώσεων.

Στις Ηνωμένες Πολιτείες, η κοινοποίηση της ταυτότητας απαιτείται για να είναι σε θέση να ψηφίσει. Στους αερολιμένες στις περισσότερες χώρες, οι επιβάτες δεν έχουν την άδεια για να επιβιβαστούν στις πτήσεις εκτός αν έχουν προσδιοριστεί σε κάποιο είδος της αερογραμμής ή του προσωπικού ασφαλείας μεταφορών, χαρακτηριστικά υπό μορφή παρουσίασης μιας ταυτότητας. Αφ' ενός, μερικές πολιτικές και διαδικασίες απαιτούν την ανωνυμία.

Για παράδειγμα σύμφωνα με την καθολική Διακήρυξη των ανθρώπινων δικαιωμάτων, " … οι περιοδικές και γνήσιες εκλογές που θα είναι από την καθολική και ίση ψήφο… θα πραγματοποιηθούν από τη μυστική ψηφοφορία ή με την ισοδύναμη ελεύθερη ψηφοφορία ."

.

Κεφάλαιο 4 TOR (The Onion Router)

4.1 Δρομολόγηση Onion

4.1.1 Εισαγωγή

Η δρομολόγηση onion (Onion Routing), είναι μια τεχνική για την ανώνυμη επικοινωνία σε ένα δίκτυο υπολογιστών.[47] Το Onion Routing αποτελεί μία γενικού σκοπού υποδομή για ιδιωτικές συνδέσεις σε ένα δημόσιο δίκτυο μεταφοράς δεδομένων.[48] Παρέχει ανώνυμες συνδέσεις χρησιμοποιώντας διαφορετικά επίπεδα κρυπτογράφησης που είναι ιδιαίτερα ανθεκτικά σε επιθέσεις τύπου ωτακουστών και ανάλυσης κίνησης. Οι συνδέσεις είναι δικατευθυντήριες, σχεδόν πραγματικού χρόνου και μπορούν να χρησιμοποιηθούν είτε για κινήσεις προσανατολισμένες σε σύνδεση, είτε για κινήσεις άνευ εγκατάστασης σύνδεσης.

Το Onion Routing βασίζεται σχεδιαστικά στην ιδέα της ανάμιξης των συνδέσεων των χρηστών και των εφαρμογών, ώστε να επιτευχθεί η απόκρυψη της ταυτότητας του χρήστη σε μία επικοινωνία μέσω ενός δημόσιου δικτύου. Έτσι τελικά είναι δύσκολο να διακριθεί μία συγκεκριμένη σύνδεση. Το Onion Routing αποτρέπει εκείνους που έχουν πρόσβαση στο μέσο μετάδοσης να αναγνωρίσουν τις οντότητες που συμμετέχουν σε μία επικοινωνία, επιτρέποντάς τους μόνο να διαπιστώσουν απλώς ότι διεξάγεται κάποια επικοινωνία. Το Onion Routing παρέχει ανώνυμες συνδέσεις ανθεκτικές στην παρακολούθηση περιεχομένου της επικοινωνίας, αλλά και στην ανάλυση της κίνησης της πληροφορίας.
Το Onion routing αποτελείται από δύο κύρια μέρη:

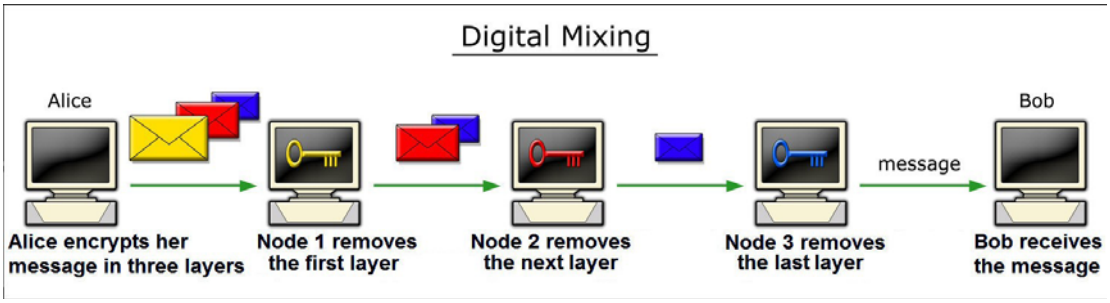
- τη δικτυακή υποδομή που εξυπηρετεί τις ανώνυμες συνδέσεις και περιλαμβάνει τους δρομολογητές Onion
- τους πληρεξούσιους που μεσολαβούν στις εφαρμογές του χρήστη και στις συνδέσεις στο Internet.

Η ιδέα της δρομολόγησης onion είναι να προστατεύσει την ιδιωτικότητα του αποστολέα και του παραλήπτη του μηνύματος και, επίσης να παρέχει την προστασία του περιεχομένου του μηνύματος καθώς δρομολογείται στο δίκτυο.[49] Η δρομολόγηση onion έχει στηριχτεί πάνω στην ιδέα των Mix Networks τα οποία δημιουργήθηκαν στις αρχές του 1980 από τον David Chaum. Ο D.Chaum είναι ο εφευρέτης πολλών κρυπτογραφικών πρωτοκόλλων στα οποία περιλαμβάνονται οι ψηφιακές υπογραφές (digital signature), η ηλεκτρονική ψηφοφορία (voting systems) και το ψηφιακό χρήμα (digital cash).

---

[47] http://en.wikipedia.org/wiki/Onion_routing
[48] www.ted.unipi.gr/Uploads/Files/Material/.../66_1206783724.doc
[49] http://en.wikipedia.org/wiki/David_Chaum

Τα mix networks δημιουργούν μια σκληρή ανιχνευσιμότητα της επικοινωνίας χρησιμοποιώντας proxy servers.[50] Κάθε μήνυμα κρυπτογραφείται σε κάθε proxy χρησιμοποιώντας ένα δημόσιο κλειδί κρυπτογραφίας. Το αποτέλεσμα της κρυπτογράφησης είναι επίπεδο κάτι σαν την Ρώσικη κούκλα, όπου η κάθε κούκλα είναι στο ίδιο μέγεθος, και το μήνυμα να βρίσκεται στο εσωτερικό επίπεδο. Κάθε proxy server «ξεγυμνώνει» το επίπεδο κρυπτογράφησης για να αποκαλύψει που θα στείλει μετά το μήνυμα. Βασική έννοια στα mixnets είναι ο MIX, ένας proxy που αποδέχεται τα κρυπτογραφημένα μηνύματα με το public key τους τα αποκωδικοποιεί τα ταξινομεί και τα προωθεί στον τελικό αποδέκτη τους διαγράφοντας όλες τις πληροφορίες για την πηγή τους.[51]



Εικόνα 4 Digital Mixing

Το πλεονέκτημα είναι, ότι, αν ένας από τους proxy servers είναι εκτεθειμένος, η ανώνυμη επικοινωνία μπορεί ακόμα να κατορθωθεί.[52] Αυτό συμβαίνει επειδή κάθε δρομολογητής στην δρομολόγηση onion δέχεται μηνύματα, τα επανακρυπτογραφεί και τα μεταφέρει στον επόμενο δρομολογητή onion. Ένας επιτιθέμενος που έχει την ικανότητα να ελέγχει κάθε δρομολογητή σε ένα δίκτυο μπορεί να εντοπίσει την πορεία ενός μηνύματος μέσα στο δίκτυο. Όμως ένας επιτιθέμενος με περιορισμένες ικανότητες θα έχει τη δυσκολία να ανακαλύψει το μονοπάτι του μηνύματος, ακόμα και αν ελέγχει έναν ή περισσότερους δρομολογητές onion.

Η δρομολόγηση onion δεν παρέχει τη τέλεια ανωνυμία του αποστολέα και του παραλήπτη ενάντια σε όλα τα πιθανά κρυφακούσματα σε ιδιωτικές συνομιλίες. Επιτρέπει έναν ισχυρό βαθμό διαχωρισιμότητας, με την ιδέα ότι ένας επιτιθέμενος δύσκολα θα ξεχωρίσει τον αποστολέα και τον παραλήπτη ενός δεδομένου μηνύματος. Ακόμη και μέσα σε αυτά τα όρια, η δρομολόγηση onion δεν παρέχει οποιαδήποτε απόλυτη εγγύηση της μυστικότητας.[53] Αντιθέτως, παρέχει μια συνέχεια στην οποία ο βαθμός μυστικότητας είναι γενικά μια λειτουργία του αριθμού των συμμετεχόντων δρομολογητών εναντίον του αριθμού των κακόβουλων δρομολογητών.

Οι δρομολογήσεις onion είναι δομές δεδομένων που χρησιμοποιούν μηνύματα για να δημιουργήσουν τις πορείες μέσω των οποίων πολλά από αυτά μπορούν να διαβιβαστούν.[54] Τα μηνύματα που δρομολογούνται, κρυπτογραφούνται επανειλημμένα και στέλνονται μέσω διαφόρων κόμβων του δικτύου, οι οποίοι

[50] http://en.wikipedia.org/wiki/Mix_network
[51] http://annaevi.freegr.net/afieromata/asfaleia_sto_surfing.htm
[52] http://en.wikipedia.org/wiki/Onion_routing
[53] http://en.wikipedia.org/wiki/Onion_routing
[54] www.ted.unipi.gr/Uploads/Files/Material/.../66_1206783724.doc

αποκαλούνται δρομολογητές onion. Οι Onion δρομολογητές συνδέονται στο δημόσιο δίκτυο, αλλά έχουν αποκαταστήσει μία και μοναδική σύνδεση με καθένα από τους γειτονικούς τους δρομολογητές Onion και μόνον έτσι μπορούν να επικοινωνούν. Σκοπός των πληρεξούσιων είναι να μεταφράζουν τα δεδομένα σε μορφή ανεξάρτητη της εκάστοτε εφαρμογής, η οποία θα γίνεται αποδεκτή και κατανοητή από το δίκτυο των δρομολογητών Onion.

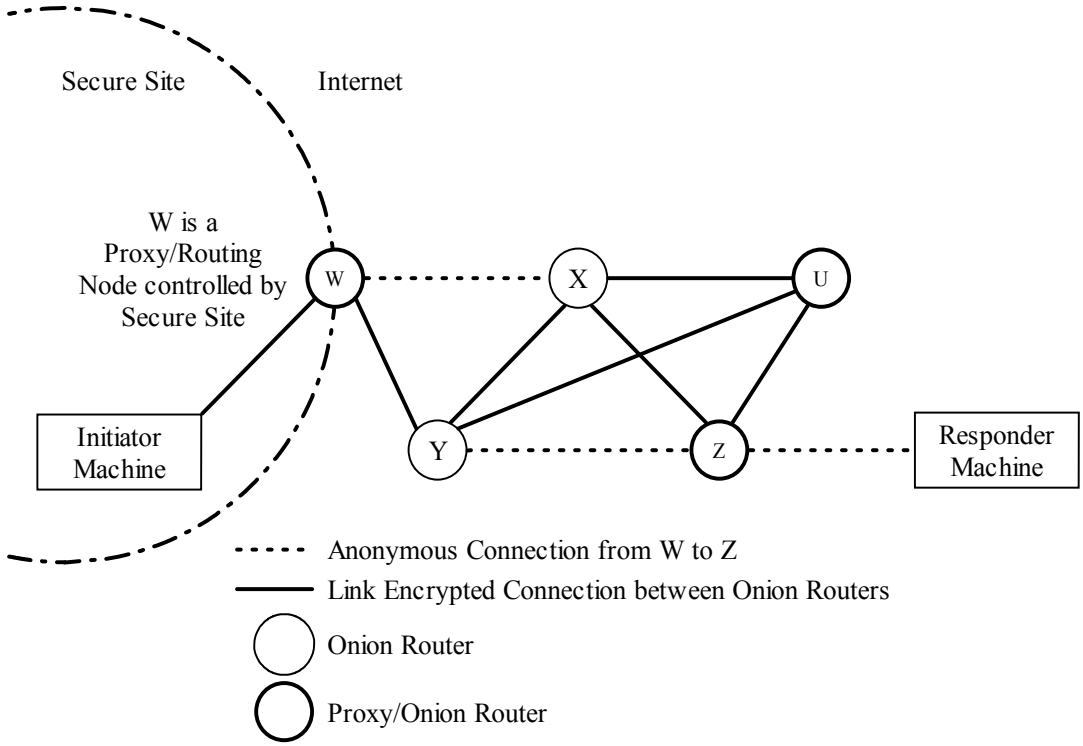
Κάθε δρομολογητής onion, ο οποίος γνωρίζει την ταυτότητα και τα δημόσια κλειδιά των υπόλοιπων δρομολογητών, αφαιρεί ένα στρώμα της κρυπτογράφησης για να αποκαλύψει τις οδηγίες δρομολόγησης και στέλνει το μήνυμα στον επόμενο δρομολογητή, όπου αυτό επαναλαμβάνεται έως ότου το μήνυμα φτάσει στον τελικό προορισμό του. Ο Onion πληρεξούσιος που βρίσκεται στην πλευρά του αποστολέα, επιλέγει ένα μονοπάτι από το οποίο θα φτάσει στον παραλήπτη. Αυτή η διαδικασία αποτρέπει τους ενδιάμεσους κόμβους να γνωρίζουν την προέλευση, τον προορισμό και το περιεχόμενο του μηνύματος.

Κατά μήκος του μονοπατιού υπάρχουν και άλλοι δρομολογητές. Για κάθε δρομολογητή, στο μονοπάτι που επιλέχτηκε, δημιουργείται ένα στρώμα με ένα πακέτο που περιλαμβάνει την IP διεύθυνση του επόμενου δρομολογητή και τις πληροφορίες που απαιτούνται για τη δημιουργία του κλειδιού κρυπτογράφησης. Αυτό το στρώμα με το πακέτο θα χρειαστεί ώστε να είναι σε θέση να επικοινωνήσει με τον επόμενο. Τα πακέτα αυτά, αντί να μεταφέρουν πληροφορία για την πηγή και τον προορισμό τους, περιέχουν πληροφορία μόνο για τον προηγούμενο και τον επόμενο σταθμό. Επομένως, στον αμέσως επόμενο από το χρήστη δρομολογητή δημιουργείται ένα Onion, το οποίο καθορίζει το μονοπάτι της σύνδεσης στο Internet.

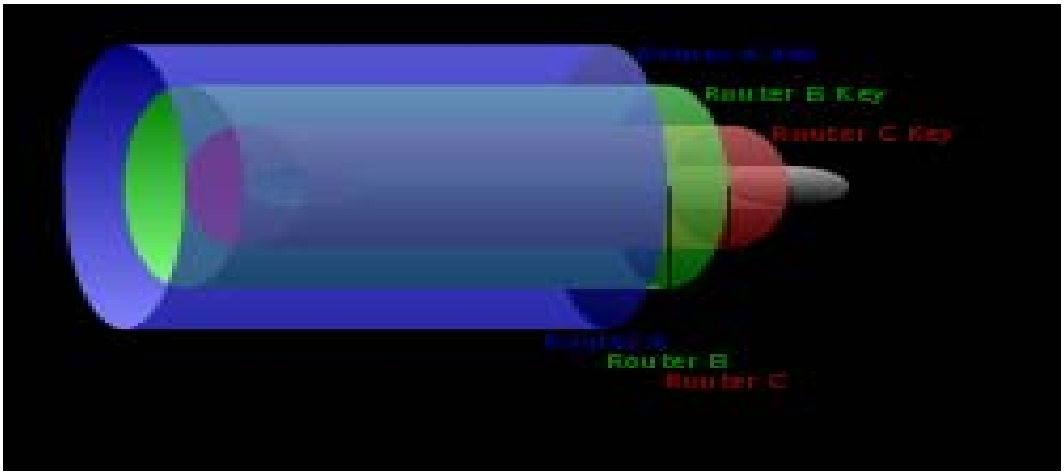
Κατά τη χρησιμοποίηση της δρομολόγησης onion η αλυσίδα των κόμβων διαμορφώνεται ως εξής: ο ιδρυτής κρυπτογραφεί τα στοιχεία που θέλει να επικοινωνήσει σε διάφορα layers με την ενίσχυση της βασικής κρυπτογράφησης δημόσιου κλειδιού και το στέλνει στον πρώτο κόμβο.[55] Ο κόμβος εισόδου θα αφαιρέσει το πρώτο στρώμα της κρυπτογράφησης και θα μεταλλάξει τα στοιχεία ο δεύτερος κόμβος. Εκείνος ο κόμβος θα αφαιρέσει επίσης ένα στρώμα της κρυπτογράφησης και θα στείλει στοιχεία στον τρίτο κόμβο. Κάθε διαδοχικός κόμβος θα κάνει επιπλέον αυτή τη διαδικασία μέχρι τον τελευταίο κόμβο, όπου ο κόμβος εξόδου θα αφαιρεί το υπόλοιπο στρώμα της κρυπτογράφησης και στέλνει το αποκρυπτογραφημένο μήνυμα στον προοριζόμενο παραλήπτη.

Κάθε μεμονωμένος κόμβος ξέρει μόνο την ταυτότητα και τη διεύθυνση IP του προηγούμενου και του διαδοχικού κόμβου. Και μόνο ο κόμβος εξόδου και εισόδου αντίστοιχα ξέρει τον ιδρυτή και τον προοριζόμενο παραλήπτη της επικοινωνίας. Αυτό σημαίνει ότι είναι πιθανό να συσχετίσουν την πλήρη επικοινωνία εφ' όσον υπάρχουν το λιγότερο τρεις κόμβοι. Εφ' όσον αλλάζει αυτή η αλυσίδα αρκετά συχνά, ή ο ιδρυτής είναι μέρος μιας αλυσίδας άλλου χρήστη, η δρομολόγηση onion παρέχει μια πολύ υψηλότερου επιπέδου ανωνυμία από ότι άλλες τεχνολογίες ιδιωτικότητας, επειδή ο βαθμός του εγκυρότητας ενός χρήστη μειώνεται σημαντικά

[55] http://www.rechtenforum.nl/files/Onion_routing.pdf



Εικόνα 5 Παράδειγμα δικτύου Onion Routing με μία ανώνυμη σύνδεση από έναν ιδρυτή σε ένα ανταποκριτή διαμέσου των δρομολογητών W, X, Y και Z.



Εικόνα 6 Δρομολογητής onion (Onion router)

Οι Onion rooters επιβάλλεται να λειτουργούν παράλληλα και ως μεσάζοντες δρομολογητές Onion για άλλες ανώνυμες συνδέσεις, ώστε να μην μπορούν να συναχθούν συμπεράσματα που αφορούν στην κίνηση των δεδομένων από και προς αυτούς.[56] Οι χρήστες πρέπει να προσπελάσουν πρώτα κάποιον Onion router, ο οποίος μπορεί να ανήκει στον ISP τους, σε κάποιον τρίτο ή ακόμη και να εκτελείται στον ίδιο τον υπολογιστή τους. Στην περίπτωση που ο rooter αυτός δεν εκτελείται τοπικά

[56] www.ted.unipi.gr/Uploads/Files/Material/.../66_1206783724.doc

και η σύνδεση είναι κρυπτογραφημένη, δε χρειάζεται εγκατάσταση λογισμικού και το υπολογιστικό κόστος είναι μηδενικό για το χρήστη. Σε περίπτωση που όλες οι λειτουργίες διεξάγονται στον υπολογιστή του, του παρέχεται η μεγαλύτερη προστασία για την ανωνυμία και ιδιωτικότητα, ακόμη και από αυτούς που συμμετέχουν στη σύνδεση, αλλά προφανώς υπάρχει σχετική επιβάρυνση.

Ένας Onion rooter δημιουργεί και διαχειρίζεται τις ανώνυμες συνδέσεις και επομένως είναι το πιο έμπιστο συστατικό τμήμα του συστήματος. Αποτελεί ουσιαστικά μία διεπαφή μεταξύ των εφαρμογών και του δικτύου, όπου οι συνδέσεις μπορεί να γίνονται με sockets, αλλά αντικαθιστούν τις κλασικές TCP/IP συνδέσεις. Ο onion rooter αποτελείται από τρία επίπεδα:

- ✓ Ένα μη απαραίτητο φίλτρο, εξειδικευμένο σε εφαρμογές, που ελέγχει και διαμορφώνει κατάλληλα τις ροές των δεδομένων.
- ✓ Ένα φίλτρο, εξειδικευμένο για εφαρμογές onion, το οποίο μεταφράζει τις ροές των δεδομένων σε μορφή ανεξάρτητη από την εκάστοτε εφαρμογή η οποία είναι αποδεκτή από το δίκτυο του Onion Routing.
- ✓ Έναν onion rooter, ο οποίος οικοδομεί και διευθύνει ανώνυμες συνδέσεις και αποτελεί το πιο αξιόπιστο τμήμα του συστήματος.

Για να δημιουργηθεί ένα onion, ο δρομολογητής στη κεφαλή της γραμμής μεταφοράς επιλέγει τυχαία ένα αριθμό δρομολογητών onion. [57] Στη συνέχεια παράγει ένα μήνυμα για τον καθένα, που προωθεί με συμμετρικά κλειδιά για την αποκρυπτογράφηση των μηνυμάτων και τον ενημερώνει ποιός δρομολογητής στο μονοπάτι θα είναι ο επόμενος. Κάθε ένα από αυτά τα μηνύματα και τα μηνύματα των διαδοχικών δρομολογητών, είναι κρυπτογραφημένα με το αντίστοιχο δημόσιο κλειδί του δρομολογητή. Αυτό διασφαλίζει μια επίπεδη δομή, στην οποία είναι απαραίτητο να αποκρυπτογραφηθούν όλα τα εξωτερικά στρώματα του onion προκειμένου να επιτευχθεί ένα εσωτερικό στρώμα.

Επίσης, για τη δημιουργία των Onions και τον καθορισμό διαδρομών, πρέπει ο Onion rooter να γνωρίζει την τοπολογία του δικτύου και την κατάσταση της διασυνδεσιμότητάς του.[58] Ακόμη, είναι αναγκαίο να έχει υπόψη του τα δημόσια πιστοποιητικά, καθώς και υπό ποιες συνθήκες μπορεί και πώς θα διαχειρισθεί μία έξοδο κόμβου από το Internet. Αυτές οι πληροφορίες διοχετεύονται κατάλληλα και με ασφάλεια στο Internet αυτομάτως, καθώς εισέρχονται νέοι κόμβοι ή προκύπτει κάποια αλλαγή.

Οι socket συνδέσεις βρίσκονται σε χαμηλότερο επίπεδο από αυτό της εφαρμογής του πρωτοκόλλου, συνεπώς είναι ανεξάρτητες εφαρμογής. Προκειμένου να χρησιμοποιηθεί η υποδομή των Onion δρομολογητών, αρκεί οι δικτυακές εφαρμογές του χρήστη να υποστηρίζουν onion. Οι συνδέσεις που δημιουργούνται είναι:

- ✓ Socket σύνδεση μεταξύ αποστολέα και Onion rooter.
- ✓ Ανώνυμη σύνδεση μεταξύ Onion rooter αποστολέα και παραλήπτη.

---

[57] http://en.wikipedia.org/wiki/Onion_routing
[58] www.ted.unipi.gr/Uploads/Files/Material/.../66_1206783724.doc

- ✓ Socket σύνδεση μεταξύ Onion rooter στην πλευρά του παραλήπτη και του ίδιου του παραλήπτη.

Οι συνδέσεις είναι αμφίδρομες, πλησιάζουν να γίνουν πραγματικού χρόνου και μπορούν να χρησιμοποιηθούν τόσο για τη διακίνηση πληροφορίας που είναι βασισμένη σε συνδέσεις όσο και για τη διακίνηση πληροφορίας που δε βασίζεται σε συνδέσεις. Το Onion Routing είναι εύκολο να ενταχθεί στα υπάρχοντα συστήματα, καθώς λειτουργεί μέσω εξειδικευμένων rooters. Πρωτότυπα (prototypes) του Onion εκτελούνται ήδη από το φθινόπωρο του 1997. Το πρωτότυπο δίκτυο επεξεργάζεται περισσότερες από ένα εκατομμύριο ηλεκτρονικές συνδέσεις ανά μήνα, από περισσότερες από έξι χιλιάδες διευθύνσεις IP σε είκοσι χώρες.

Η τεχνολογία Onion Routing δεν είναι απρόσβλητη σε επιθέσεις ανάλυσης κίνησης. Εάν υπάρχει κάποια εφαρμογή εκφραζόμενη από αιτήσεις δικτύου που απαιτεί σύνδεση πραγματικού χρόνου, είναι πιθανή η ανίχνευση της ταυτόχρονης εισόδου των πλησιέστερων συνδέσεων socket των Onion routing του ιδρυτή και του ανταποκριτή. Ωστόσο, αυτές οι μορφές επιθέσεων απαιτούν τη συλλογή και ανάλυση τεράστιων ποσών δεδομένων από εξωτερικούς παρατηρητές.

Τρόπο για βελτίωση του συστήματος για την αντιμετώπιση αυτού του είδους της ανάλυσης αποτελεί η διέλευση μη ουσιαστικής κίνησης διαμέσου του δικτύου, ώστε να επιτευχθεί η σταθερότητα του επιπέδου κίνησης. Βεβαίως, με τον τρόπο αυτό, υπάρχει σχετική επιβάρυνση με όφελος τη βελτίωση της συνολικής ασφάλειας του συστήματος. Δεν παρέχει ισχυρή άμυνα ενάντια στην ανάλυση συγχρονισμού. Εάν ένας επιτιθέμενος παρατηρήσει έναν σχετικά φορτωμένο δρομολογητή onion, μπορεί να ελέγξει τα εισερχόμενα και εξερχόμενα μηνύματά του και να παρατηρήσει πόσο κοντά χρονικά λαμβάνονται και αποστέλλονται.

4.1.2 Αρχές Λειτουργίας

Για την περιγραφή της λειτουργίας του Onion Routing θεωρείται ότι κάθε Onion δρομολογητής γνωρίζει τις ταυτότητες και τα δημόσια κλειδιά κάθε άλλου δρομολογητή Onion.[59] Ο ιδρυτής "Initiator" ξεκινά επιλέγοντας μία πορεία για τον ανταποκριτή "Responder". Για κάθε δρομολογητή Onion στο μονοπάτι, ο ιδρυτής δημιουργεί ένα πακέτο επίπεδου εγκατάστασης σύνδεσης που αποτελείται από την IP διεύθυνση του επόμενου δρομολογητή, το κρυπτογραφημένο κλειδί με το οποίο μπορεί να διαμοιράζεται μυστικές πληροφορίες ένας δρομολογητής με τον επόμενό του k, καθώς και το επόμενο επίπεδό του. Το πιο εσωτερικό επίπεδο του Onion περιέχει την ταυτότητα του ανταποκριτή και τα δεδομένα προς αποστολή.

Όπως προωθείται το πακέτο στο μονοπάτι των δρομολογητών Onion, τα επίπεδα ξετυλίγονται. Όταν το πακέτο φτάσει στον τελευταίο δρομολογητή του μονοπατιού, τα δεδομένα προωθούνται άμεσα στον αποδέκτη τους. Όλες οι αιτήσεις από τον ιδρυτή-αποστολέα αποστέλλονται από το ίδιο μονοπάτι των δρομολογητών Onion. Οι απαντήσεις αποστέλλονται από τον τελευταίο δρομολογητή Onion του μονοπατιού, ο οποίος επιστρέφει τα δεδομένα στον αποστολέα-ιδρυτή από το ίδιο μονοπάτι, αλλά με

[59] www.ted.unipi.gr/Uploads/Files/Material/.../66_1206783724.doc

την αντίστροφη πορεία. Η υλοποίηση του Onion Routing δεν αναπτύσσεται σε κάθε αιτούντα. Αντ' αυτού, είναι διαθέσιμος για χρήση ένας αριθμός αφιερωμένων Onion δρομολογητών. Ο ιδρυτής πρέπει να συνδεθεί σε έναν από αυτούς τους δρομολογητές για να επικοινωνήσει με τον παραλήπτη.

Η λειτουργία του Onion Routing συνίσταται στη δυναμική οικοδόμηση των ανώνυμων συνδέσεων μέσα σε ένα δίκτυο από πραγματικού χρόνου Chaum mixes. Αυτά τα mixes αποδέχονται σταθερού μεγέθους μηνύματα από ποικίλες πηγές, τα κρυπτογραφούν και στη συνέχεια τα προωθούν στον επόμενο προορισμό με τυχαία σειρά. Με τη δρομολόγηση μέσα από πολυάριθμα mixes στο Internet είναι δύσκολο να διευκρινισθεί ποιος επικοινωνεί με ποιόν. Το δίκτυο του Onion Routing είναι κατανεμημένο και παρουσιάζει ανοχή σε σφάλματα, ενώ βρίσκεται υπό τον έλεγχο πολλαπλών διαχειριστικών τμημάτων (domains). Με αυτό τον τρόπο, ένας μόνο δρομολογητής Onion δεν είναι δυνατό να καταρρίψει το δίκτυο, ούτε μπορεί να παραβιάσει την ανωνυμία ενός χρήστη.

Οι συνδέσεις του Onion Routing είναι ανεξάρτητες από το πρωτόκολλο που θα χρησιμοποιηθεί, ενώ περιλαμβάνουν τρεις φάσεις: τη διαδικασία ρύθμισης της σύνδεσης, τη διακίνηση των δεδομένων και τη διαδικασία τερματισμού της σύνδεσης. Η πρώτη φάση ξεκινά όταν ο χρήστης δημιουργήσει ένα Onion και τότε καθορίζεται το μονοπάτι του δικτύου που θα ακολουθήσει η σύνδεση. Το Onion είναι ακριβώς μία δομή δεδομένων που αποτελείται από στρώματα και καθορίζει τις ιδιότητες της σύνδεσης, όπως τις πληροφορίες κρυπτογραφικού ελέγχου δηλαδή τους συμμετρικούς κρυπτογραφικούς αλγόριθμους και τα μυστικά κλειδιά που θα χρησιμοποιηθούν κατά τη διάρκεια διακίνησης των δεδομένων.

Κάθε δρομολογητής Onion στο μονοπάτι χρησιμοποιεί το δημόσιο κλειδί του για να αποκρυπτογραφήσει ολόκληρο το Onion που παραλαμβάνει. Αυτή η διαδικασία εκθέτει τις πληροφορίες ελέγχου της κρυπτογράφησης, την ταυτότητα του επόμενου δρομολογητή Onion και το συνημμένο Onion. Εάν χρειαστεί, ο δρομολογητής Onion συμπληρώνει με στοιχεία το συνημμένο Onion και το στέλνει στον επόμενο δρομολογητή Onion.

Αφού πραγματοποιηθεί η σύνδεση, τα δεδομένα μπορούν να σταλούν και προς τις δύο κατευθύνσεις. Επαναλαμβανόμενα δεδομένα από τον ιδρυτή της σύνδεσης κρυπτογραφούνται με διάφορους αλγόριθμους και τα κλειδιά καθορίζονται μέσα στο Onion. Καθώς προχωρούν τα δεδομένα στην ανώνυμη σύνδεση, κάθε δρομολογητής του Onion αφαιρεί ένα επίπεδο κρυπτογράφησης και αποκαλύπτει τον επόμενο δρομολογητή, ενώ τελικά το μήνυμα φτάνει στον παραλήπτη σε αποκρυπτογραφημένη μορφή. Εάν ακολουθηθεί η αντίστροφη πορεία, η διαστρωμάτωση αυτή ακολουθείται στην αντίστροφη σειρά με διαφορετικούς αλγόριθμους και κλειδιά.

Η διαδικασία τερματισμού της σύνδεσης μπορεί να πραγματοποιηθεί είτε από τα δύο άκρα είτε και στη μέση αν έτσι απαιτηθεί. Μόλις τερματιστεί η σύνδεση, οι δρομολογητές Onion χάνουν όλη την πληροφορία σχετικά με τη σύνδεση. Για να μην μπορέσει κάποιος να συνάγει το μήκος του δρομολογίου, τα onions πρέπει να διατηρούν σταθερό μέγεθος κατά τη διάρκεια της δρομολόγησής τους. Για να

επιτευχθεί αυτό, κάθε δρομολογητής υποχρεούται να συμπληρώνει (padding) στο Onion που του αποκαλύπτεται το κενό που δημιούργησε η αφαίρεση του στρώματος από αυτό. Εάν το Onion δεν έχει το σωστό και αυστηρά καθορισμένο μέγεθος όταν σταλεί, απορρίπτεται από τον επόμενο δρομολογητή.

Η συνολική πληροφορία, η οποία αποτελείται από τα Onion, τα δεδομένα και τις πληροφορίες ελέγχου του δικτύου, αποστέλλεται μέσα στο δίκτυο του Onion Routing σε ομοιόμορφου μεγέθους κυψέλες. Οι κυψέλες φτάνουν σε ένα ορισμένο χρονικό διάστημα και αναμιγνύονται για να μη διαπιστωθούν τυχόν συσχετίσεις που θα διευκόλυναν την εργασία όσων θέλουν να παραβιάσουν την ανωνυμία του χρήστη. Κάτι ανάλογο είναι δυνατό να γίνει με τις συνδέσεις μεγάλης διάρκειας και αυτές του περιορισμένου εύρους ζώνης, οι οποίες γεμίζονται.

Κάθε Onion φαίνεται διαφορετικά σε κάθε δρομολογητή Onion, λόγω της διαστρωματοποιημένης κρυπτογράφησης δημοσίου κλειδιού. Ομοίως, κατά τη διάρκεια της μεταφοράς των δεδομένων κάθε Onion φαίνεται διαφορετικό λόγω της διαστρωματοποιημένης κρυπτογράφησης συμμετρικού κλειδιού. Αυτή η τεχνική αντιστέκεται στις επιθέσεις ανάλυσης κίνησης, περισσότερο από κάθε άλλη παρόμοια τεχνική στο Internet. Το προκύπτον κόστος για τη λειτουργία του Onion Routing είναι σχετικά μικρό.

4.2 TOR

Μια σημαντική εφαρμογή της δρομολόγησης onion είναι το Tor.[60] Το Tor είναι ένα πρόγραμμα λογισμικού που προστατεύει τις επικοινωνίες στο διαδίκτυο από την ανάλυση κίνησης, μια μορφή δικτυακής παρακολούθησης που απειλεί την προσωπική ελευθερία και την ιδιωτικότητα, τις εμπιστευτικές επαγγελματικές δραστηριότητες και σχέσεις, και την κρατική ασφάλεια. Το Tor προστατεύει την δικτυακή δραστηριότητα συνδέοντας τον χρήστη με τον υπολογιστή που θέλει μέσω ενός διανεμημένου δικτύου υπολογιστών που χρησιμοποιούν κρυπτογράφηση για να εγγυηθεί η μυστικότητα της προώθησης των πακέτων επικοινωνίας μεταξύ των δρομολογητών.

Δίνει την δυνατότητα στους χρήστες του να επικοινωνούν ανώνυμα στο διαδίκτυο. Αυτό υλοποιείται με το να χρησιμοποιεί proxy servers οι οποίοι ελέγχουν την κυκλοφορία του δικτύου και αποκρυπτογραφούν τα δεδομένα που διακινούνται σε αυτό. Με το να χρησιμοποιεί αυτήν την υπηρεσία ο κάθε χρήστης μπορεί να αποκρύψει το που έχει πρόσβαση στο Internet, είτε αυτές είναι διαδικτυακές εφαρμογές νόμιμες ή όχι.

Το Tor λειτουργεί με πολλές εφαρμογές που βασίζονται στο πρωτόκολλο TCP όπως προγράμματα άμεσων μηνυμάτων και φυλλομετρητές ιστοσελίδων εμποδίζοντας έτσι άλλα άτομα να μάθουν την φυσική τοποθεσία του χρήστη ή ποιες σελίδες επισκέπτεται. Εκατοντάδες άτομα ανά τον κόσμο χρησιμοποιούν το Tor για διάφορους λόγους: δημοσιογράφοι και ιστολόγοι, υπερασπιστές των ανθρωπίνων

[60] http://el.wikipedia.org/wiki/Tor

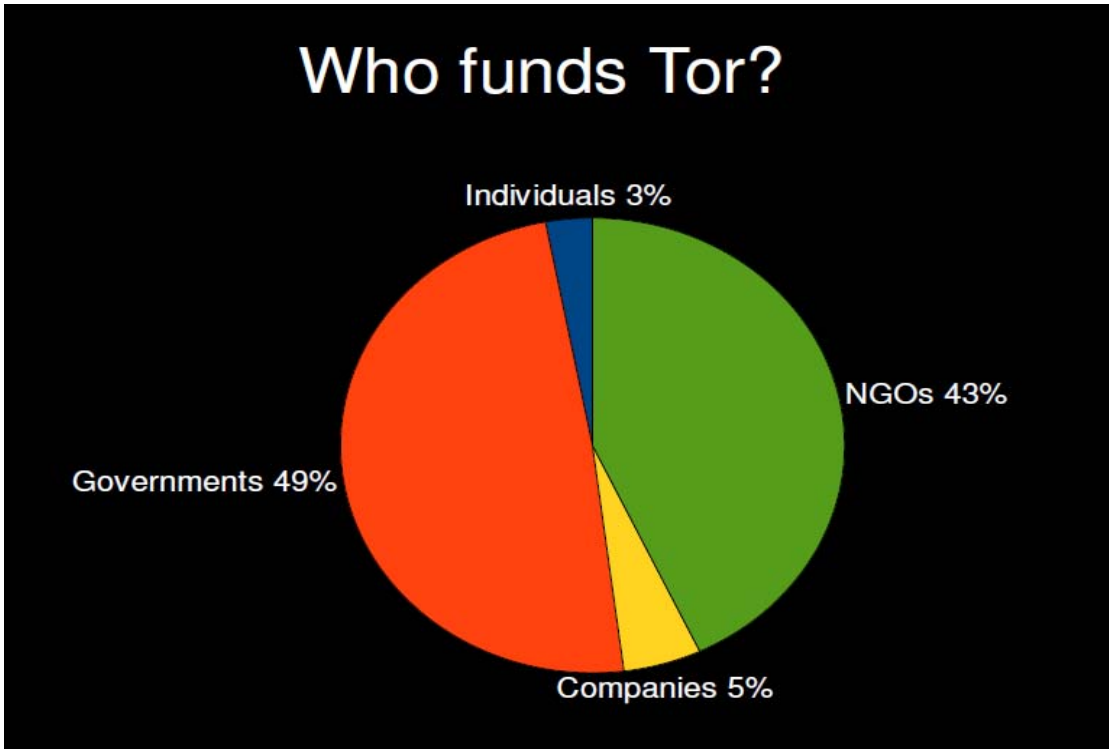
δικαιωμάτων, στρατιώτες, εταιρίες, πολίτες καταπιεστικών καθεστώτων και απλοί πολίτες. Το Tor δεν προστατεύει την ανωνυμία αν δεν χρησιμοποιηθεί σωστά. Ακόμα όμως και αν γίνει σωστά η παραμετροποίησή του και η χρήση του, υπάρχουν ακόμα πιθανές επιθέσεις που μπορούν να μειώσουν την δυνατότητα του να μας προστατεύει.

Πολλοί χρήστες αναγνωρίζουν την χρησιμότητα του TOR δικτύου, ειδικά σε περιπτώσεις όπου χρειάζεται απόλυτη ιδιωτικότητα για ύποπτους λόγους. Για παράδειγμα, κάποιοι επιτιθέμενοι μπορεί να χρησιμοποιούν αυτή την υπηρεσία για να κρύψουν την αληθινή πηγή ή τον προορισμό της σύνδεσής τους, ή ένας υπάλληλος να μπορέσει να έχει πρόσβαση σε παράνομα web sites την ώρα εργασίας του. Υπάρχουν όμως και περιπτώσεις, οι οποίες είναι πολλές, που χρησιμοποιείται και για καλή χρήση.

Το μεγαλύτερο group ανθρώπων που επωφελείται με τη χρήση του Tor δικτύου είναι κυρίως οι καθημερινοί άνθρωποι.[61] Η χρησιμοποίηση του Tor για αυτούς δεν έχει σκοπό την ανωνυμία. Για αυτούς το Tor είναι ένας πιο αποτελεσματικός τρόπος για να έχουν ασφαλή online μυστικότητα. Επίσης το δίκτυο Tor προσφέρει πολλά πλεονεκτήματα και για εταιρίες. Αν σε μια περίοδο 24 ωρών πολλοί χρήστες φορτώνουν τη σελίδα www.monster.com, η οποία ασχολείται με εύρεση εργασίας, και όλοι έχουν IP διευθύνσεις οι οποίες ανήκουν στην διεθνή εταιρία Oracle, τότε αυτό δίνει πολλές πληροφορίες για τους συγκεκριμένους χρήστες στους ανθρώπους της monster. Μπορεί, πιθανώς, να είναι σημαντικές πληροφορίες, και η Oracle να τις προωθήσει στο κοινό.

Ένα άλλο group ανθρώπων που για αυτούς είναι σημαντικό το Tor , είναι οι κυβερνήσεις. Για παράδειγμα, η κυβέρνηση της Μ. Βρετανίας θέλει ερευνήσει έναν αριθμό ατόμων οι οποίοι είναι ύποπτοι για παιδική πορνογραφία. Δεν θα είναι σωστό οι IP διευθύνσεις τους να είναι πχ της μορφής AC45B569.MI5.GOV.UK. Αν όμως χρησιμοποιούν λογικές IP, τότε θα είναι δύσκολο να τους αναγνωρίσουν. Οι κυβερνήσεις, παρόλα αυτά, θα πρέπει να χρησιμοποιούν μια δικιά τους έκδοση του Tor. Ο μόνος τρόπος για να ερευνούν ή για να προσεγγίσουν έναν αριθμό εγκληματιών ή κάποιο ηλεκτρονικό έγκλημα,, είναι να κοιτάξουν καλύτερα σε group "φυσιολογικών" χρηστών του internet.

[61] www.rechtenforum.nl/files/Onion_routing.pdf

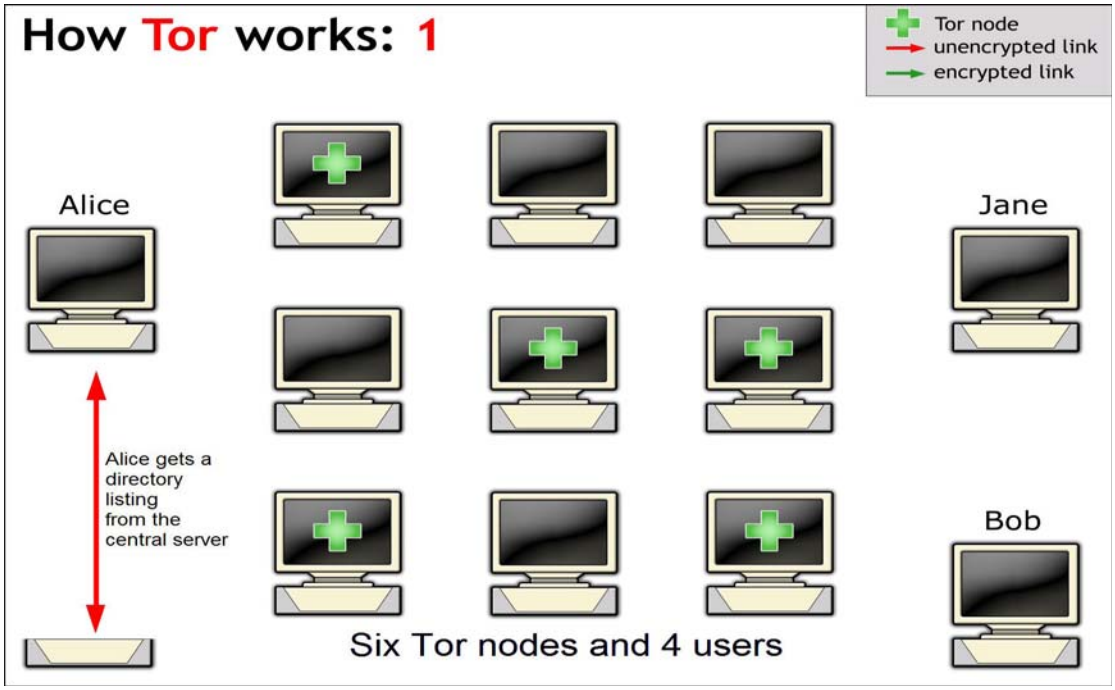


Εικόνα 7 Χρησιμότητα Tor

4.2.1 Λειτουργία Tor

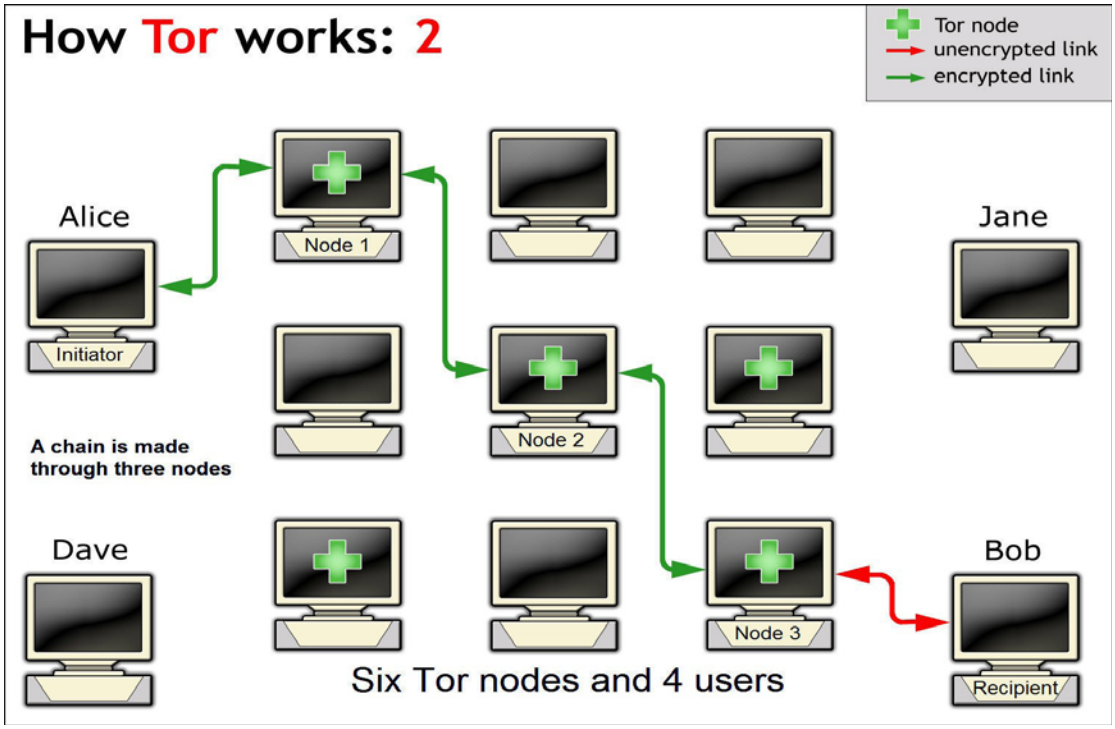
Πολύ απλά και συνοπτικά η λειτουργία του Tor είναι η εξής: Υπάρχει ένα δίκτυο, το λεγόμενο Tor network, που αποτελείται από διάφορους server (nodes).[62] Το πρόγραμμα συνδέεται στο δίκτυο αυτό και μεταφέρει τα πακέτα από node σε node, μέχρι αυτά να φτάσουν στην άλλη άκρη (πχ την ιστοσελίδα που θέλουμε). Το Tor βοηθά να μειώσει τους κινδύνους μιας απλής και περίπλοκης ανάλυσης κυκλοφορίας με τη διανομή των συναλλαγών μας από διαφορετικά μέρη στο internet, κι έτσι κανένα σημείο δεν μπορεί να μας συνδέσει με το προορισμό μας. Αντί για τη λήψη μιας άμεσης διαδρομής από την πηγή στον προορισμό, τα πακέτα δεδομένων στο Tor, παίρνουν μια τυχαία ροή μέσω διαφορετικών relays (αναμεταδότες), που καλύπτουν τις διαδρομές μας, με αποτέλεσμα κανένας παρατηρητής σε κανένα σημείο να μη μπορεί να ξεχωρίσει τα δεδομένα από πού προέρχονται και ποιος είναι ο προορισμός τους. **Όπως βλέπουμε και στην Εικόνα 8 How Tor works Step 1 και στην Εικόνα 9 How Tor works Step 2.**

[62] http://www.torproject.org/overview.html



Εικόνα 8 How Tor works Step 1

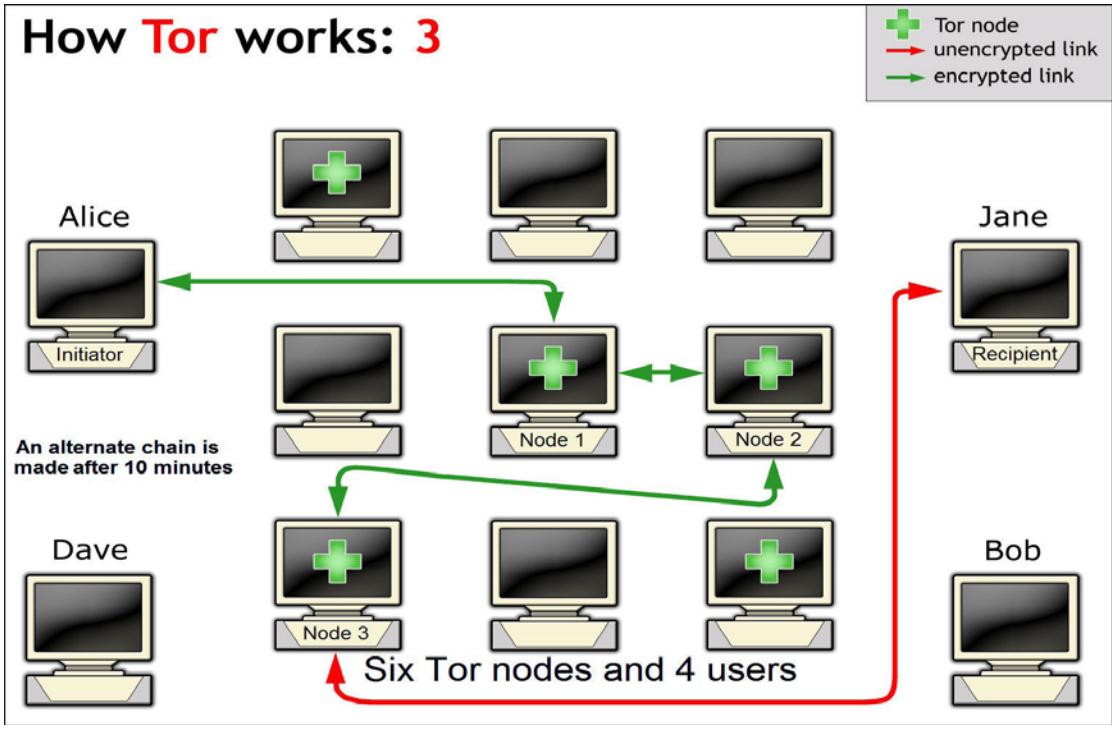
Για να δημιουργήσουμε ένα ιδιωτικό μονοπάτι στο Tor, το λογισμικό των χρηστών ή ο client δημιουργεί ένα κύκλωμα από κρυπτογραφημένες συνδέσεις μέσα από το δίκτυο. Το κύκλωμα επεκτείνεται ένα βήμα κάθε φορά, και κάθε relay κατά του μήκους ξέρει από πού παρέλαβε τα δεδομένα και πού πρέπει να τα παραδώσει. Κανένας μεμονωμένος relay δεν ξέρει πάντα τη πλήρη πορεία του πακέτου. Ο client διαπραγματεύεται ένα ξεχωριστό ζευγάρι κλειδιών για κάθε βήμα κατά μήκους του κυκλώματος, έτσι ώστε να σιγουρέψει ότι κάθε βήμα δεν μπορεί να εντοπιστεί όσο το πακέτο δρομολογείται στο κύκλωμα. **Όπως βλέπουμε και στην Εικόνα 10 How Tor works Step 3 και στην Εικόνα 11 How Tor works Step 4.**



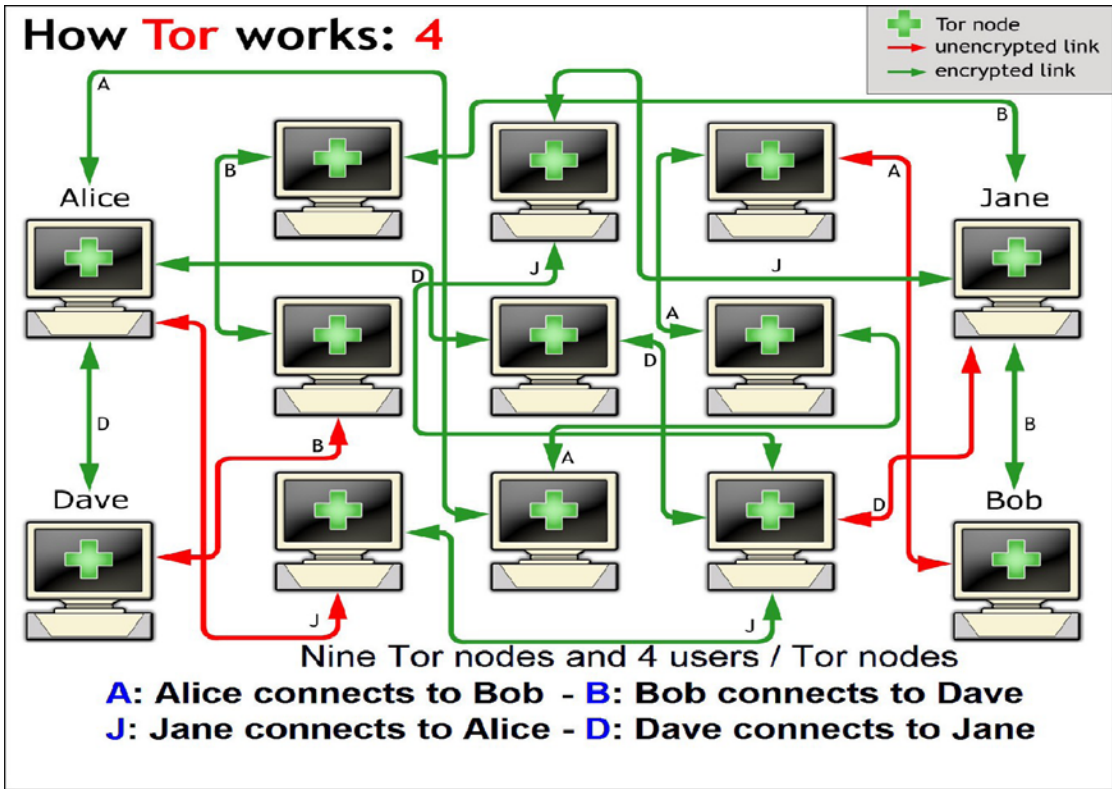
Εικόνα 9 How Tor works Step 2

Μόλις καθιερωθεί ένα κύκλωμα, πολλά είδη δεδομένων μπορούν να ανταλλαχτούν και διαφορετικά είδη εφαρμογών λογισμικού μπορούν να επεκταθούν πέρα από το δίκτυο Tor. Επειδή κάθε relay δεν βλέπει παρά μόνο ένα βήμα κάθε φορά στο κύκλωμα, ούτε ένας ωτακουστής, ούτε ένας συμβιβασμένος relay δεν μπορεί να χρησιμοποιήσει την ανάλυση κυκλοφορίας για να συνδέσει την πηγή της σύνδεσης με τον προορισμό.

Το Tor δουλεύει μόνο με TCP streams και μπορεί να χρησιμοποιηθεί από κάθε εφαρμογή που υποστηρίζει Socks. Για την αποδοτικότητα, το Tor λογισμικό χρησιμοποιεί το ίδιο κύκλωμα για συνδέσεις που πραγματοποιούνται μέσα σε 10 λεπτά το πολύ. Οι επόμενες αιτήσεις θα δίνονται σε νέο κύκλωμα, έτσι ώστε να κρατήσουν τους επιτιθέμενους μακριά από τις συνδέσεις που κάναμε νωρίτερα.



Εικόνα 10 How Tor works Step 3



Εικόνα 11 How Tor works Step 4

Ανώνυμες εξερχόμενες συνδέσεις (Anonymous outgoing connections)

Οι χρήστες του Tor δικτύου «τρέχουν» στον υπολογιστή τους έναν onion proxy server.[63] Αυτός ο server τους συνδέει διαπραγματεύοντας μέσω ενός εικονικού κυκλώματος μέσα στο Tor δίκτυο. Το Tor πραγματοποιεί την κρυπτογράφηση υψηλού επιπέδου, ασφαλίζοντας τέλεια μυστικότητα μετάδοσης ανάμεσα στους δρομολογητές. Την ίδια στιγμή, ο onion proxy server παρουσιάζει μια διεπαφή Socks στους χρήστες του. Οι εφαρμογές Socks είναι καθορισμένες στο Tor, οι οποίες μετά πολυπλέκουν την κυκλοφορία μέσω του εικονικού κυκλώματος.

Μέσα στο Tor δίκτυο, τα δεδομένα στέλνονται από router σε router, και εν τέλει φτάνουν σε έναν κόμβο εξόδου (exit node) ο οποίος είναι υπεύθυνος για την αποστολή των πακέτων στον σωστό προορισμό. Το Tor ξεχωρίζει από τα άλλα δίκτυα ανωνυμίας γιατί λειτουργεί στο TCP επίπεδο. Οι ανώνυμες εφαρμογές που περιλαμβάνει είναι το IRC (Internet Relay Chat), τα άμεσα μηνύματα και η πρόσβαση στο διαδίκτυο. Όταν κάποιος χρήστης έχει πρόσβαση στο internet, το Tor συνεργάζεται με το Privoxy – ένας proxy server που χρησιμοποιεί φίλτρα- όπου ως αποτέλεσμα έχουμε την πρόσθεση της ιδιωτικότητας στο επίπεδο εφαρμογών.

Ανώνυμες κρυμμένες υπηρεσίες (Anonymous hidden services)

Το πιο δημοφιλή χαρακτηριστικό του Tor δικτύου είναι η ανωνυμία που παρέχει στους servers του. Με το να χρησιμοποιούν το Tor είναι πολύ πιθανό να μην τους εντοπίζουν. Για να έχουν πρόσβαση σε μια κρυμμένη υπηρεσία, το Tor πρέπει να χρησιμοποιείται και από τους clients (χρήστες). Οι κρυμμένες υπηρεσίες προσεγγίζονται μέσω ενός συγκεκριμένου υψηλού επιπέδου ψευδο-τομέα ο οποίος ονομάζεται .onion. Το Tor καταλαβαίνει αυτόν τον top level domain και δρομολογεί τα δεδομένα ανώνυμα στην κρυμμένη υπηρεσία.

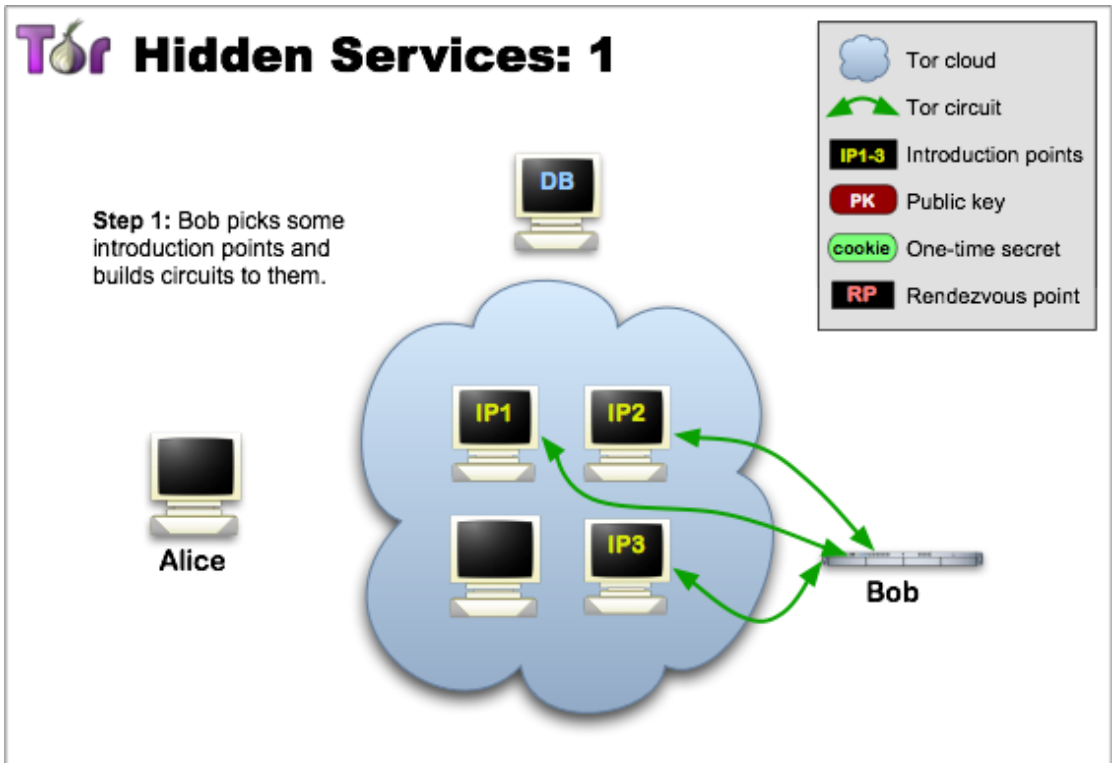
Οι χρήστες που χρησιμοποιούν το Tor μπορούν και συνδέονται σε αυτές τις κρυμμένες υπηρεσίες, χωρίς ο καθένας να γνωρίζει την δικτυακή ταυτότητα του άλλου. Αυτές οι κρυμμένες υπηρεσίες στην ουσία επιτρέπουν στους χρήστες να έχουν πρόσβαση σε κάποιο web site και να δημοσιοποιούν δεδομένα χωρίς να τους απασχολεί η λογοκρισία. Κανένας δεν είναι πρόθυμος να μάθει ποιος έχει πρόσβαση στο συγκεκριμένο site και κανένας που πρότεινε το site δεν μπορεί να μάθει ποιος το χρησιμοποιεί.

Οι κρυμμένες υπηρεσίες είναι κεντρικοί υπολογιστές εφικτοί μόνο από το Tor, οι οποίοι επιτρέπουν σε άλλους να συνδεθούν με αυτούς χωρίς την αποκάλυψη της θέσης των κεντρικών υπολογιστών.[64] Οι λόγοι για αυτό μπορούν να κυμανθούν με την παρεμπόδιση μιας επίθεσης DoS (Denial of Service) από το να γίνει εφικτή ή απλά να αποτρέψει την αποκάλυψη των στοιχείων αυτών των χρηστών που είναι συνδεδεμένοι. Για να δημιουργήσουν μια κρυμμένη υπηρεσία, ένας κεντρικός υπολογιστής επιλέγει διάφορους αναμεταδότες για να ενεργήσουν ως σημεία

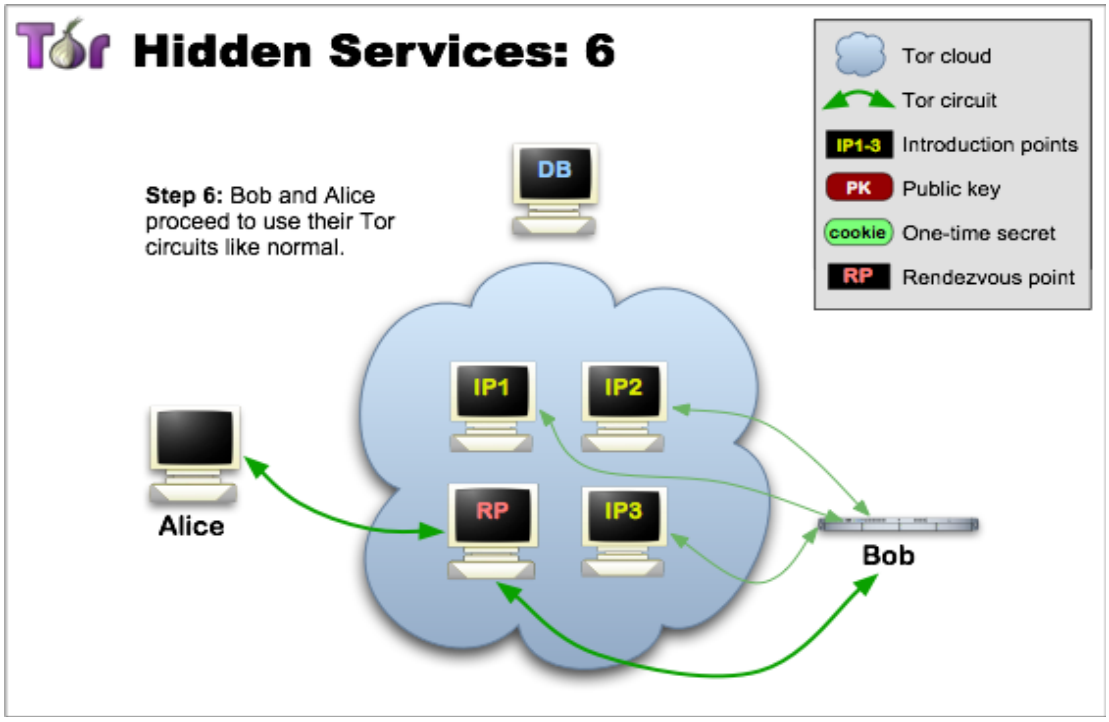
[63] http://el.wikipedia.org/wiki/Tor
[64] http://blag.cerebralmind.net/wp-content/uploads/2008/05/tor.pdf

εισαγωγής, όπου αυτές είναι οι μηχανές στις οποίες οι άλλες θα συνδεθούν κατευθείαν για να έχουν πρόσβαση στον κεντρικό υπολογιστή.

Ο κεντρικός υπολογιστής αρχίζει με τη δημιουργία ενός κυκλώματος στα σημεία εισαγωγής. Η υπηρεσία διαφημίζεται έπειτα με τους κεντρικούς υπολογιστές καταλόγου. Όταν ένας client επιθυμεί να συνδεθεί με μια κρυμμένη υπηρεσία, ρωτά αρχικά την υπηρεσία καταλόγου για τις ταυτότητες σημείων εισαγωγής. Ο server καταλόγου αποκρίνεται, σε αυτό το σημείο ο client στήνει ένα άλλο Tor κύκλωμα με έναν αναμεταδότη για να πράξει στο Rendezvous Point, δηλαδή ο κόμβος ο οποίος είναι γνωστός και στις 2 πλευρές. Ο client επικοινωνεί έπειτα ότι η ταυτότητα του Rendezvous Point δείχνει τον server μέσω του σημείου εισαγωγής. Ο server δημιουργεί τώρα ένα κύκλωμα στο Rendezvous Point, και η σύνδεση έχει ολοκληρωθεί.



Εικόνα 12 Tor hidden service



Εικόνα 13 Tor Connected Hidden Service

4.2.2 Αδυναμίες Tor δικτύου (weaknesses)

Διαρροή DNS (DNS leaks)

Η διαρροή DNS είναι ένα σύνηθες πρόβλημα του Tor δικτύου, όπου μπορούν να αποκαλυφθούν ποιοι χρήστες είναι συνδεδεμένοι σε αυτό.[65] Το Tor δεν μπορεί να κρύψει ποιος το χρησιμοποιεί αλλά μπορεί να κρύψει για ποιο λόγο το χρησιμοποιεί. Με το να παρακολουθούν κάποιοι επιτιθέμενοι τι πακέτα διακινούνται από έναν server, μπορούν να βρουν ποιοί είναι συνδεδεμένοι σε αυτό. Μια λύση είναι να χρησιμοποιήσουμε το Privoxy, το οποίο είναι ένα λογισμικό web proxy που περιέχει ιδιότητες φιλτραρίσματος για την προστασία ιδιωτικότητας, τροποποιεί δεδομένα διαδικτύου και διαχειρίζεται τα cookies.

Ανάλυση κυκλοφορίας (Traffic analysis)

Μερικοί επιτιθέμενοι κατασκοπεύουν σε πολλά μέρη του διαδικτύου και χρησιμοποιούν τεχνικές για να εντοπίσουν τα σχέδια πολλών οργανισμών και ατόμων. Η κρυπτογράφηση δεν βοηθά ενάντια σε αυτούς τους επιτιθέμενους, δεδομένου ότι κρύβει μόνο το περιεχόμενο της κίνησης του δικτύου και όχι τις κεφαλίδες των πακέτων που διακινούνται. Είναι λίγο δύσκολο το TOR να μπορεί να ελέγξει την ανάλυση κυκλοφορίας και στις 2 άκρες της σύνδεσης. Υπάρχουν τεχνικές ανάλυσης για την ασφάλεια και την ιδιωτικότητα μεταξύ όλων των κόμβων έτσι ώστε να βρεθεί αυτός που παρέχει λιγότερη μυστικότητα στο δίκτυο.

---

[65] http://en.wikipedia.org/wiki/Tor_(anonymity_network)

Επίθεση από ωτακουστές (Eavesdroppers)

Αν κάποιος κόμβος εξόδου δεν χρησιμοποιεί κρυπτογράφηση end to end, τότε είναι πολύ εύκολο να αποκρυπτογραφηθεί η ανάλυση κυκλοφορίας μεταξύ αυτού του κόμβου με τον server που επικοινωνεί. Ένας ωτακουστής είναι ένας επιτιθέμενος ικανός να παρακολουθεί όλες τις πληροφορίες που είτε αποστέλλονται, είτε λαμβάνονται από κάποιο συγκεκριμένο συμμετέχοντα, με σκοπό να ανιχνευθεί είτε ο ιδρυτής, είτε ο παραλήπτης για κάθε επικοινωνία.[66] Οι ωτακουστές αντιμετωπίζονται δύσκολα, ακριβώς επειδή μπορούν να καταγράφουν και να συγκρίνουν όλα τα εισερχόμενα και εξερχόμενα μηνύματα.

Etiquette

Υπάρχουν λίγες φορές που κάποιοι κόμβοι θέλουν να εκμεταλλευτούν συνδέσεις του δικτύου TOR λόγω της ήδη υπάρχουσας ανωνυμίας που διατηρεί.[67] Το TOR έχει κάποια χαρακτηριστικά επίλυσης αυτού του προβλήματος σε περίπτωση που προκύψει. Κάθε ένας κόμβος εξόδου διατηρεί μια πολιτική αστυνόμευσης στο ποια σύνδεση έχει πάρει άδεια να διακόψει την επικοινωνία και ποια όχι. Οι περισσότερες εκμεταλλεύσεις δικτύου έχουν χαρακτηριστικά όπως:

- ✓ Εκμετάλλευση εύρους ζώνης με μεταφορά μεγάλου όγκου δεδομένων.
- ✓ Λόγω της χρησιμοποίησης περισσότερου εύρους ζώνης δεν προτείνονται και μεταφορές Bit torrent.
- ✓ Αποστολή spam μηνυμάτων.
- ✓ Κάποιοι ανώνυμοι χρήστες δεν δέχονται τις διαφορετικές πολιτικές πρόσβασης σελίδων του web.

Παράνομες χρήσεις

Ανάμεσα στο μεγάλο ποσοστό χρηστών που χρησιμοποιούν το TOR δίκτυο, υπάρχουν και κάποιοι επιτήδειοι που το χρησιμοποιούν για εκμεταλλεύσιμους σκοπούς πχ, την παιδική πορνογραφία. Έχει παρατηρηθεί ότι το ποσοστό αυτών που το χρησιμοποιούν για παράνομες χρήσεις είναι μεγαλύτερο από αυτούς που το χρησιμοποιούν καθαρά για ανωνυμία και ιδιωτικότητα της επικοινωνίας τους.

4.2.3 Proxy server

Ένας διακομιστής μεσολάβησης (Proxy server) είναι μία εφαρμογή η οποία βρίσκεται ανάμεσα σε μία εφαρμογή πελάτη (πχ web browser) και έναν εξωτερικό εξυπηρετητή (εξυπηρετητής web).[68] Ο proxy server από τη μία πλευρά παραλαμβάνει αιτήσεις από το εσωτερικό του δικτύου και τις μεταφέρει στους κατάλληλους εξυπηρετητές στο

[66] www.ted.unipi.gr/Uploads/Files/Material/.../66_1206783724.doc
[67] http://en.wikipedia.org/wiki/Tor_(anonymity_network)
[68] www.conta.uom.gr/.../Comparison%20of%20Proxy%20Servers%20(1).pdf

διαδίκτυο, και από την άλλη παραλαμβάνει αρχεία από το διαδίκτυο και τα μεταφέρει στο εσωτερικό του δικτύου. Επομένως, ένας τέτοιος διακομιστής λειτουργεί και ως εξυπηρετητής και ως εφαρμογή πελάτης. Ένας Proxy server χαρακτηρίζεται από τρεις βασικές δυνατότητες: το φιλτράρισμα των αιτήσεων, την ταχύτερη λειτουργία («άνοιγμα» ιστοσελίδων) και το διαμερισμό των πόρων μίας σύνδεσης.

Με τον όρο «φιλτράρισμα των αιτήσεων» εννοείται η παρακολούθηση των εισερχόμενων και εξερχόμενων αιτήσεων με σκοπό τον αποκλεισμό των ανεπιθύμητων. Ένας Proxy server μπορεί να χρησιμοποιηθεί για να αποκλείσει την πρόσβαση όλων ή κάποιων χρηστών σε κάποιες υπηρεσίες (πχ την ανάγνωση ιστοσελίδων με συγκεκριμένο περιεχόμενο).

Ο proxy server δέχεται αιτήσεις για την παρουσίαση σελίδων του World Wide Web από το φυλλομετρητή (browser) ενός χρήστη και αναλαμβάνει να προσκομίσει σε αυτόν τις ζητούμενες σελίδες.[69] Ο proxy server, δηλαδή, παρεμβάλλεται μεταξύ του χρήστη και του WWW server από τον οποίο ζητά πληροφορίες ο χρήστης. Έτσι λοιπόν ο φυλλομετρητής (π.χ. Netscape Navigator, MS Explorer κλπ.) αντί να επικοινωνήσει απευθείας με τον server που επιθυμεί ο χρήστης ζητά από τον proxy server να του προσκομίσει τη σελίδα. Στη συνέχεια ο proxy server ζητά από τον server που ενδιαφέρει το χρήστη τις ζητούμενες σελίδες. Αφού ο server αποστέλλει τις σελίδες στον proxy server, ο proxy server με τη σειρά του στέλνει τις σελίδες που ζητήθηκαν στο φυλλομετρητή του χρήστη, ο οποίος και τις παρουσιάζει.

Τις περισσότερες φορές ένας proxy server είναι και cache server. Ένας cache server αποθηκεύει τις αιτήσεις των φυλλομετρητών και τις αντίστοιχες απαντήσεις των servers με σκοπό να διαχειριστεί νέες αιτήσεις. Έτσι, έχουμε ένα proxy-cache server. Η διαχείριση της μνήμης cache είναι ένα μεγάλο κομμάτι της λειτουργίας του proxy server. Ο κύριος στόχος είναι η μνήμη cache να είναι αποτελεσματική αλλά και να μην περιέχει αρχεία που δεν είναι ενημερωμένα.

Για παράδειγμα, αν έχουμε ένα σύνολο χρηστών που αξιοποιούν τη λειτουργία ενός proxy-cache server, όπως ο proxy server του CYTANET, τότε αν ένας από αυτούς ζητήσει μια συγκεκριμένη σελίδα από ένα server στην Αμερική ο proxy-cache server θα φέρει τη σελίδα και αφενός θα την παραδώσει στο πρόγραμμα πλοήγησης του χρήστη, αφετέρου θα την αποθηκεύσει για μελλοντική χρήση.

Αν τώρα ένας άλλος χρήστης ή και ο ίδιος ζητήσει την ίδια σελίδα τότε ο proxy-cache server θα του προσκομίσει το αντίγραφο που έχει κρατήσει και δε θα αναζητήσει τη σελίδα στην Αμερική. Επομένως, αν την ίδια σελίδα θέλουν να δουν 100 άτομα, με τη χρήση του proxy-cache server, μόνο ο πρώτος θα χρειαστεί να περιμένει να έρθει η σελίδα από τον αρχικό server, ενώ οι υπόλοιποι 99 θα δουν τη σελίδα να έρχεται ταχύτερα, αφού θα τους διατεθεί από τον proxy-cache server.

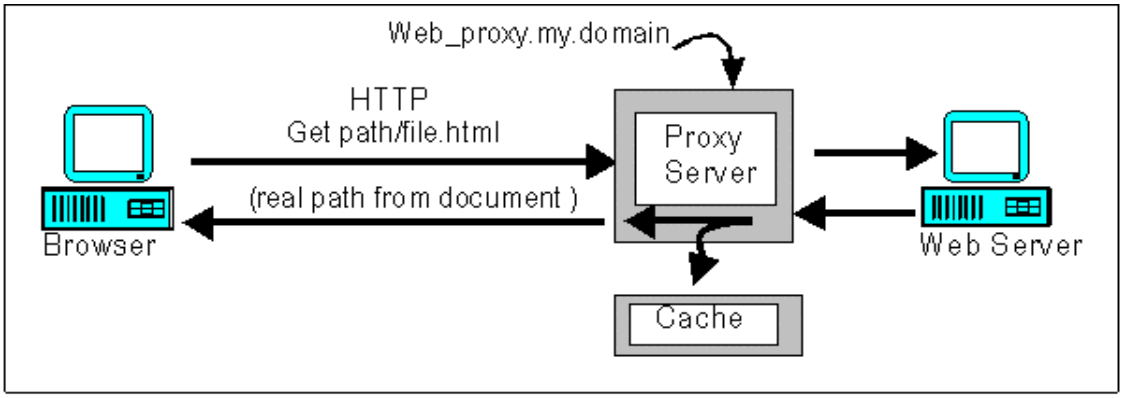
Το τρίτο σημαντικό μέρος της λειτουργίας ενός proxy server είναι ο διαμερισμός των πόρων μίας σύνδεσης διαδικτύου.[70] Αυτό είναι ένα χαρακτηριστικό το οποίο είναι ιδιαίτερα σημαντικό στην περίπτωση της σύνδεσης ενός οικιακού ή μικροεταιρικού

[69] http://www.call-centre.cyta.com.cy/techinfo.htm#PROXY%20SERVER
[70] *www*.conta.uom.gr/.../Comparison%20of%20Proxy%20Servers%20(1).pdf

δικτύου, αφού επιτρέπει τη σύνδεση πολλών υπολογιστών χρησιμοποιώντας μόνο ένα modem και μία σύνδεση μέσω τηλεφώνου. Οπωσδήποτε, μία τέτοια σύνδεση υπόκειται σε περιορισμούς σε ότι αφορά στην ταχύτητα της επικοινωνίας, ωστόσο μπορεί να είναι πρακτική στην εξυπηρέτηση κάποιων αναγκών όπως για παράδειγμα η διακίνηση του ηλεκτρονικού ταχυδρομείου ενός μικρού γραφείου.

Εκτός όμως από τους διακομιστές μεσολάβησης που χρησιμοποιούνται από ένα συγκεκριμένο τοπικό δίκτυο, υπάρχουν και κάποιοι οι οποίοι είναι κοινής χρήσης και δεν υπόκεινται στην ιδιοκτησία αυτού που τους χρησιμοποιεί. Για να χρησιμοποιήσει κάποιος έναν τέτοιο proxy server το μόνο που χρειάζεται είναι η ρύθμιση των παραμέτρων του browser του. Αυτό θα του επιτρέψει, κάθε φορά που μία αίτηση του προωθείται στο διαδίκτυο, να διέρχεται πρώτα από τον proxy server που έχει επιλέξει ο χρήστης.

Αυτού του είδους οι διακομιστές μεσολάβησης (3rd party proxy servers) χρησιμοποιούνται κυρίως για την προσφορά υπηρεσιών ανωνυμίας αλλά και για την βελτίωση των επιδόσεων της σύνδεσης. Το σημαντικότερο πρόβλημα με τέτοιου είδους διακομιστές είναι η μειωμένη αξιοπιστία τους, κάτι που αντισταθμίζεται από το μεγάλο πλήθος τους. Ένα μεγάλο πλήθος βοηθητικών εφαρμογών οι οποίες διευκολύνουν τη σύνδεση με απομακρυσμένους proxy servers είναι διαθέσιμο στο διαδίκτυο σε χαμηλές τιμές ή εντελώς δωρεάν.



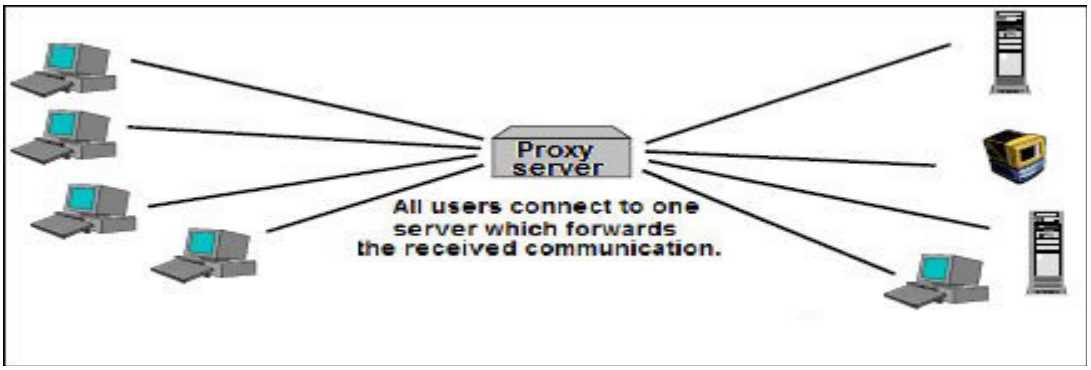
Εικόνα 14 Τυπική λειτουργία ενός Proxy server

Ένα παράδειγμα χρήσης proxy server είναι το εξής: υπάρχει ένας hacker στην Ελλάδα, ένας host στην Αγγλία κι ένας proxy στην Ιρλανδία. [71] Ο hacker στην Ελλάδα ρυθμίζει τον υπολογιστή του ώστε να διακινεί τις πληροφορίες του διαμέσου του proxy στην Ιρλανδία. Έτσι λοιπόν, τα "πακέτα" πληροφοριών διακινούνται από τον hacker στην Ελλάδα, στον proxy στην Ιρλανδία και μετά στον host στην Αγγλία. Ο client συνδέεται με τον proxy, προμηθεύει την διεύθυνση του server στον οποίο συνδεόμαστε, προμηθεύει την διεύθυνση της υπηρεσίας που θέλουμε να έχουμε πρόσβαση και "μπαίνει" σε αναμονή. Μετά ο proxy συνδέεται στην διεύθυνση του server που του ζητήσαμε, "καλεί" την υπηρεσία που επιθυμούμε και την επιστρέφει στον client.

Έτσι λοιπόν, ο server "καταγράφει" μόνο την διεύθυνση του host που πραγματοποιείται στην σύνδεση και την "κλήση" μας proxy. Σε γενικές γραμμές

[71] http://community.athens.indymedia.org/index.php/topic,458.0/prev_next,prev.html#new

περιγράψαμε τον τρόπο σύνδεσης και διακίνησης των πληροφοριών μας στο δίκτυο, διαμέσου proxy. Εύλογα κάποιος θα μπορούσε να αναρωτηθεί "γιατί, οι proxy είναι λιγότερο σίγουροι?". Απλά, γιατί δεν είμαστε οι διαχειριστές των proxy, επιπλέον 9 στις 10 φορές δεν γνωρίζουμε αν ο proxy που χρησιμοποιούμε είναι πραγματικά ελεύθερος και ανώνυμος, αν οι διαχειριστές καταγράφουν κάθε στοιχείο της πλοήγησης μας στο δίκτυο. Έτσι λοιπόν, η αστυνομία γνωρίζοντας τον proxy που χρησιμοποιούμε, θα μπορούσε από τους διαχειριστές του να "απαιτήσει" κάθε πληροφορία για εμάς.



Εικόνα 15 Proxy server

4.2.4 Τύποι Proxy servers

Catching Proxy Server

Ένας catching proxy server επιταχύνει τα αιτήματα υπηρεσιών με την ανάκτηση του περιεχομένου που έχει σωθεί από ένα προηγούμενο αίτημα που υποβάλλεται από τον ίδιο client ή ακόμα και άλλους clients.[72] Οι catching proxy servers κρατούν τα τοπικά αντίγραφα των συχνά ζητούμενων πόρων, όπου επιτρέπουν στις μεγάλες οργανώσεις να μειώσουν σημαντικά την χρήση και το κόστος του εύρους ζώνης, έτσι ώστε να αυξηθεί σημαντικά η απόδοση. Οι περισσότερες ISPs και μεγάλες επιχειρήσεις έχουν ένα catching proxy. Αυτές οι μηχανές χτίζονται για να παραδώσουν τη τέλεια απόδοση συστημάτων αρχείων και να περιέχουν επίσης ειδικές εκδόσεις του TCP. Οι catching proxy servers ήταν το πρώτο είδος κεντρικού proxy server.

Web proxy server

Ο Web proxy server εστιάζει στην κυκλοφορία του διαδικτύου και η κυρίως ενασχόλησή του είναι να διαχειρίζεται την μνήμη cache. Πολλά proxy προγράμματα πχ το Squid, παρέχουν τη μη πρόσβαση σε συγκεκριμένα URLs, δηλαδή επιτυγχάνεται το φιλτράρισμα του περιεχομένου. Αυτό χρησιμοποιείται συχνά σε εταιρικό, εκπαιδευτικό ή περιβάλλον βιβλιοθηκών, και οπουδήποτε αλλού όπου το φιλτράρισμα περιεχομένου επιδιώκεται. Μερικοί web proxies επαναμορφοποιούν τις ιστοσελίδες για ένα συγκεκριμένο σκοπό πχ τα cell phones και τα PDAs.

[72] http://en.wikipedia.org/wiki/Proxy_server

Content filtering web proxy

Ο content filtering web proxy παρέχει διοικητικό έλεγχο του περιεχομένου που αναμεταδίδεται μέσω του proxy server. Χρησιμοποιείται συνήθως σε εμπορικές και μη εμπορικές οργανώσεις (ειδικά στα σχολεία), για να εξασφαλίσει ότι η χρήση διαδικτύου προσαρμόζεται στην αποδεκτή πολιτική χρήσης. Σε μερικές περιπτώσεις οι χρήστες μπορούν να παρακάμψουν τον proxy, δεδομένου ότι υπάρχουν υπηρεσίες με σκοπό στις πληροφορίες proxy από έναν φιλτραρισμένο ιστοχώρο μέσω μιας μη φιλτραρισμένης περιοχής, να επιτρέψουν τη μετάδοσή του μέσω του proxy των χρηστών.

Μερικές κοινές μέθοδοι που χρησιμοποιούνται για τον content filtering web proxy περιλαμβάνουν: URL ή DNS, URL regex φιλτράρισμα, MIME φιλτράρισμα, ή φιλτράρισμα λέξης κλειδιού περιεχομένου. Μερικά προϊόντα ήταν γνωστά για να υιοθετούν τις τεχνικές ανάλυσης περιεχομένου για να βρίσκουν τα γνωρίσματα που χρησιμοποιούνται συνήθως από ορισμένους τύπους προμηθευτών. Ένας content filtering web proxy θα υποστηρίξει συχνά την αυθεντικότητα των χρηστών, για να ελέγξει την πρόσβαση στο διαδίκτυο. Επίσης, συνήθως παράγει logs (αρχεία server), είτε για να δώσει τις αναλυτικές πληροφορίες για τα URLs που έχουν πρόσβαση συγκεκριμένοι χρήστες, είτε για να ελέγξει το εύρος ζώνης.

Anonymizing proxy server

Ένας anonymizing proxy server (μερικές φορές καλείται web proxy), γενικά αναφέρεται στην ανώνυμη πρόσβαση. Μία από τις κοινές παραλλαγές είναι ο open proxy. Επειδή είναι δύσκολο να εντοπιστούν, οι open proxies είναι ειδικώς χρήσιμοι για αυτούς που επιδιώκουν την απευθείας online ανωνυμία, από τους πολιτικούς αποστάτες μέχρι και το ηλεκτρονικό έγκλημα. Μερικοί χρήστες ενδιαφέρονται μόνο για την ανωνυμία στην αρχή, για να διευκολύνουν τα δικαιώματα της ελευθερίας του λόγου για παράδειγμα. Ο server λαμβάνει τις αιτήσεις από τον anonymizing proxy server, και έτσι δεν λαμβάνει πληροφορίες για τις διευθύνσεις για τους τελικούς χρήστες. Παρόλα αυτά, οι αιτήσεις δεν είναι ανώνυμες, κι έτσι ένας βαθμός εμπιστοσύνης είναι παρών μεταξύ του server και του χρήστη.

Hostile proxy

Οι proxies μπορούν επίσης να εγκατασταθούν προκειμένου να πέσουν πάνω σε ένα «κρυφάκουσμα» μεταξύ μιας μηχανής client και του διαδικτύου. Όλες οι προσβάσιμες σελίδες μπορούν να προσεγγιστούν και να αναλυθούν από τον proxy operator. Για αυτόν το λόγο, οι κωδικοί σε online υπηρεσίες (όπως το e-mail ή το web banking), πρέπει πάντα να εξασφαλίζουν κρυπτογράφηση με ένα πρωτόκολλο κρυπτογράφησης, πχ το SSL.

Intercepting proxy server

Ο Intercepting proxy server, γνωστός και ως transparent proxy, συνδυάζει έναν proxy server και μια θύρα. Οι συνδέσεις γίνονται από τις μηχανές αναζήτησης των χρηστών μέσω των θυρών που περνούν απευθείας από τον proxy, χωρίς την αυθεντικοποίηση του client. Οι intercepting proxies servers συνήθως χρησιμοποιούνται σε επιχειρήσεις που θέλουν να αποτρέψουν την αποφυγή πολιτικής χρήσης. Είναι συχνά δυνατό να ανιχνευθεί η χρήση ενός τέτοιου proxy server, συγκρίνοντας την εξωτερική ip διεύθυνση με την διεύθυνση που βλέπει ένας web server ή με το να εξεταστούν οι HTTP επικεφαλίδες των μηνυμάτων του server.

Transparent and not transparent proxy server

Ο ορισμός Transparent proxy συνήθως χρησιμοποιείται για την έννοια του intercepting proxy. Ο Transparent proxy δεν τροποποιεί την αίτηση ή την απάντηση, πέρα από το να απαιτεί την αυθεντικότητα του proxy και την ταυτότητά του. Ενώ ο not transparent proxy server τροποποιεί τα μηνύματα αίτησης και απάντησης με σκοπό να παρασχεθεί μια επιπλέον υπηρεσία στον χρήστη, όπως πχ το φιλτράρισμα ανωνυμίας.

Socks proxy server

Το Socks είναι ένα πρωτόκολλο διαδικτύου το οποίο διαχειρίζεται τη δρομολόγηση των πακέτων μεταξύ του client και του server μέσω ενός proxy server.[73] Τα Socks λειτουργούν στο επίπεδο 5 του OSI μοντέλου και στο επίπεδο συνεδρίας (Session Layer, το επίπεδο που βρίσκεται μεταξύ του επιπέδου παρουσίασης και του επιπέδου μεταφοράς).

Επίσης, το Socks μπορεί να συνεργαστεί και με τα πρωτόκολλα HTTP, FTP, SMTP, POP3, NNTP, κλπ.[74] Το Socks μεταφέρει όλα τα δεδομένα από έναν client σε έναν server, χωρίς να προσθέτει κάτι σε αυτά, και από τη μεριά του web server ο socks proxy είναι ο client. Έτσι λοιπόν, η ανωνυμία αυτού του είδους proxy server είναι πλήρης. Υπάρχουν δύο εκδόσεις του πρωτοκόλλου Socks, η 4 και η 5. Η 4η έκδοση, η οποία εμφανίστηκε και πρόσφατα, είναι πιο διαδεδομένη. Ωστόσο η 5η έκδοση υποστηρίζεται από πολλά προγράμματα όπως το ICQ (το οποίο χρησιμοποιεί μόνο proxy servers), το Napster, το AudioGalaxy, το EeDoonkey2000 (για download mp3), κλπ.

Γενικώς, ένας socks proxy server μπορεί να λειτουργήσει με πρωτόκολλα όπως το TCP/UDP, και μπορεί να χρησιμοποιηθεί από προγράμματα για e-mails, όμως δεν το κάνουν. Για τέτοια προγράμματα, τα οποία δεν δουλεύουν με socks, έχει δημιουργηθεί ένα ειδικό λογισμικό το οποίο αυτόματα επιτρέπει τις εφαρμογές μεταξύ client και server που μεταφέρονται μέσω ενός socks server. Το πιο διαδεδομένο είναι το Sockscap, το οποίο επιτρέπει τον έλεγχο όλης της κίνησης και κάνει τη δρομολόγηση μέσω ενός socks proxy 4 ή 5.

---

[73] http://en.wikipedia.org/wiki/SOCKS
[74] http://www.freeproxy.ru/en/free_proxy/faq/what_is_socks_proxy.htm

4.3 Εργαλεία Tor

4.3.1 Privoxy

Ο οποιοσδήποτε που επιθυμεί ασφάλεια, ιδιωτικότητα και έλεγχο στην περιήγησή στο διαδίκτυο, μπορεί να χρησιμοποιεί το Privoxy.[75] Το συγκεκριμένο πρόγραμμα ειδικά, είναι μια καλή επιλογή για αυτούς που χρειάζονται περισσότερη ασφάλεια**.** Το Privoxy στηρίζεται πάνω στον web proxy server και χρησιμοποιείται σε συνδυασμό με το Tor. Και τα δύο μαζί δουλεύουν για να κρύψουν την ip διεύθυνση του υπολογιστή μας. Αυτό το καταφέρνουν με το να στέλνουν το σήμα μας σε ειδικούς servers του διαδικτύου, οι οποίοι αποκαλούνται onion routers.

Το Privoxy είναι ένας web proxy για HTTP συνδέσεις που μας δίνει πολλές δυνατότητες για προσαρμογές στα μέτρα μας και λειτουργικότητα.[76] Με τη χρήση του Privoxy θα μπορούμε να διαχειριστούμε τα HTTP cookies, να φιλτράρουμε το περιεχόμενο και διαφημίσεις στο διαδίκτυο κ.ά. Το Privoxy έχει το πλεονέκτημα ότι όλα τα υπάρχοντα αιτήματα HTTP μπορούν να προωθηθούν. Αυτό είναι το αδύναμο σημείο του Tor. Το Tor μπορεί μόνο να προωθήσει κίνηση, αλλά όλα τα αιτήματα DNS (που αντιστοιχούν το όνομα του διακομιστή στην IP του server) προσπερνιούνται. Αυτό σημαίνει ότι η ανωνυμία δεν είναι πια εγγυημένη, καθώς κάποιος θα μπορεί να αναγνωρίσει την πραγματική IP στα αρχεία καταγραφής του server.

Για παράδειγμα όπως γίνεται με τις ταινίες κατασκόπων του Hollywood, οι οποίες δείχνουν ένα τηλεφώνημα που εντοπίζεται σε δεκάδες λάθος περιοχές.[77] Έτσι γίνεται και με την IP μας όταν κρύβεται πίσω από αυτούς τους ειδικούς servers. Η πραγματική μας IP διεύθυνση όντως «εξαφανίζεται» όταν σερφάρουμε στο διαδίκτυο, ή στέλνουμε ένα e-mail ή «κατεβάζουμε» κάποια αρχεία μέσω του δικτύου Tor onion. [78] Ο web proxy είναι μια υπηρεσία η οποία είναι φτιαγμένη με το ίδιο λογισμικό όπως το Privoxy, δηλαδή, οι clients μπορούν να συνδέονται απευθείας με τους servers διαδικτύου (web servers ή proxy servers).

Χαρακτηριστικά Privoxy:

- ✓ Μπορεί να κρατά ενεργές τις εξερχόμενες συνδέσεις και να τις επαναχρησιμοποιήσει αργότερα.
- ✓ Υποστηρίζει την αλλαγή συμπεριφοράς η οποία αφορά τις επικεφαλίδες των client και servers.
- ✓ Μπορεί να «τρέχει» ως ενδιάμεσος proxy server, ο οποίος προλαμβάνει την ανάγκη να χωριστούν οι μηχανές αναζήτησης χωριστά.
- ✓ Περιέχει περίπλοκες ενέργειες και φίλτρα για να χειρίζεται τις επικεφαλίδες των server και client.
- ✓ Μπορεί να συνεργαστεί και με άλλους proxy servers.

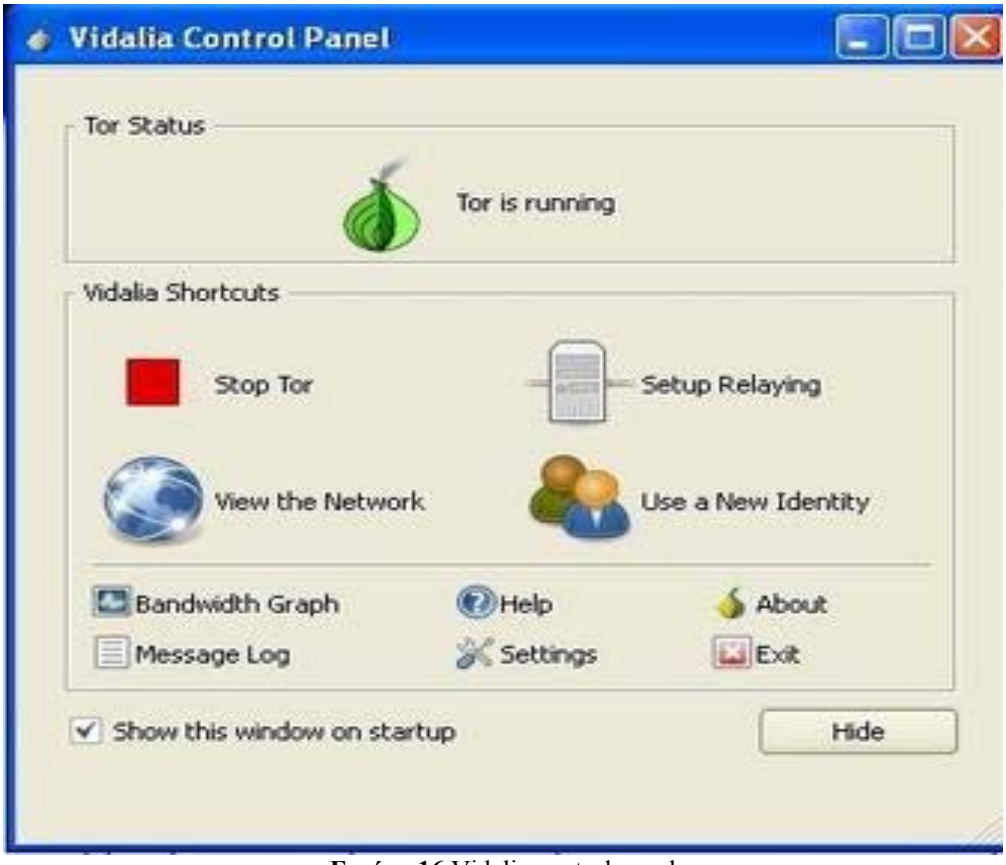
---

[75] http://en.wikipedia.org/wiki/Privoxy
[76] http://community.athens.indymedia.org/index.php?topic=427.0
[77] http://netforbeginners.about.com/od/internet101/f/anonymous_surf.htm
[78] http://en.wikipedia.org/wiki/Privoxy

- ✓ Μπορεί να φιλτράρει τις ιστοσελίδες, δηλαδή κάνει αντικατάσταση κειμένου, αφαιρεί τα bunner, διαθέτει ορατά εργαλεία για διαχείριση, αγνοεί τα επανεμφανιζόμενα παράθυρα και τα κομμάτια κώδικα javascript και html κλπ.
- ✓ Βελτιώνει τη διαχείριση των cookies.
- ✓ Υποστηρίζει πολυμέσα.

4.3.2 Vidalia

Το Vidalia είναι ένα πακέτο εφαρμογής το οποίο περιλαμβάνει το Tor, τον Privoxy proxy, όπως επίσης και το Vidalia GUI (Graphical User Interface) για διαχείριση του Tor.[79] Με την εγκατάσταση του Vidalia κατευθείαν φορτώνεται στον υπολογιστή μας ένας Privoxy proxy ο οποίος επιτυγχάνει τη σύνδεσή μας με το Tor δίκτυο. Το Vidalia στην ουσία αναλαμβάνει την εγκατάσταση του Tor και του privoxy και τον εύκολο χειρισμό τους.



Εικόνα 16 Vidalia control panel

Ο πίνακας ελέγχου του Vidalia μας δείχνει τη θέση σύνδεσής μας με το Tor και μας αφήνει να ξεκινάμε και να σταματάμε τη σύνδεση, όπως επίσης και να αλλάζουμε τους proxies με τη χρήση ενός κατάλληλου κουμπιού το οποίο καλείται New Identity

[79] http://www.tomsguide.com/us/security-online-privacy,review-1055-4.html

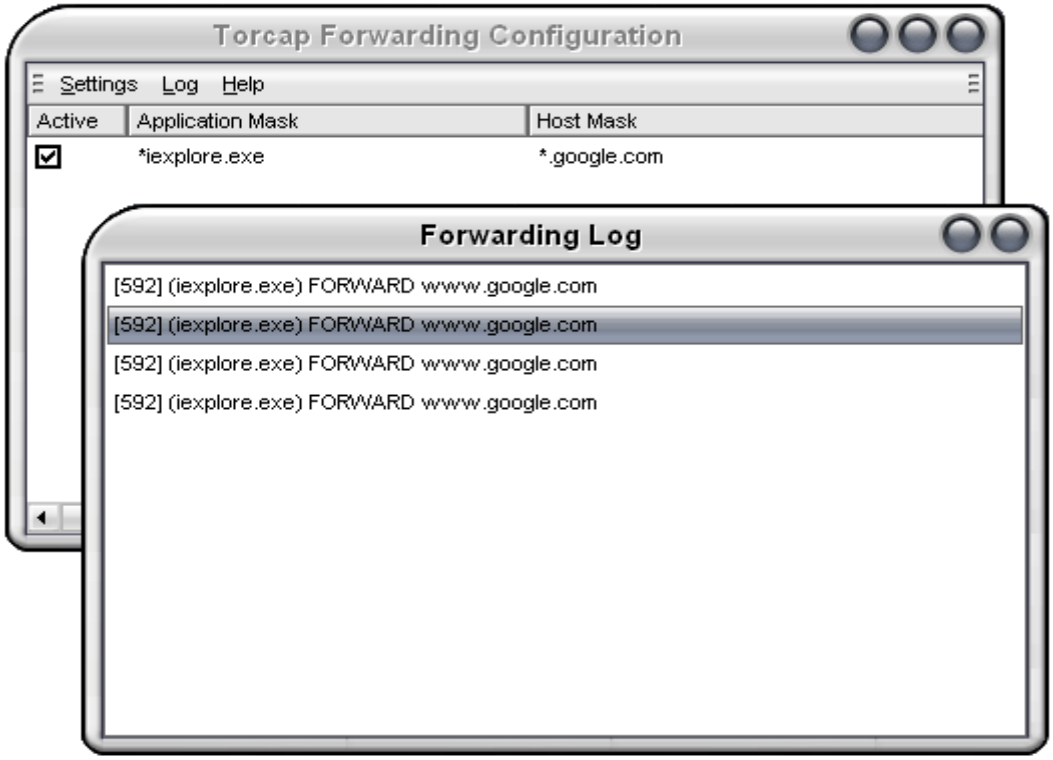
button. Το Vidalia επιπλέον προσφέρει μια γραφική αναπαράσταση του bandwidth, έτσι ώστε να μπορούμε να δούμε πόση κίνηση έχουμε στείλει μέσω του Tor.

Εικόνα 17 Vidalia Tor network map

4.3.3 Torcap

Το Torcap είναι ένα εργαλείο το οποίο επιτρέπει οποιαδήποτε δικτυακή εφαρμογή να συνδεθεί μέσω του Tor, ακόμα και αν αυτή η εφαρμογή δεν υποστηρίζει τα socks.[80] Λειτουργεί με το να εισάγει ένα DLL (Dynamic Link Library) σε κάθε διαδικασία που τρέχει στον υπολογιστή του χρήστη. Αυτό το DLL δουλεύει με το Winsock API (Winsock Application Programming Interface) το οποίο συνεργάζεται τη παροχή DNS (Domain Name System) και τις συνδέσεις TCP/IP. Η απόφαση για το πότε θα συνδέεται ο χρήστης μέσω του Tor ή απευθείας στο internet, εξαρτάται από την μάσκα της εφαρμογής (application mask) και τη μάσκα του εξυπηρετητή (host mask). Όταν αυτά τα δύο ταιριάξουν τότε η σύνδεση θα γίνει μέσω του Tor Socks server.

[80] http://www.freehaven.net/~aphex/torcap/



Εικόνα 18 Torcap Forwarding Configuration

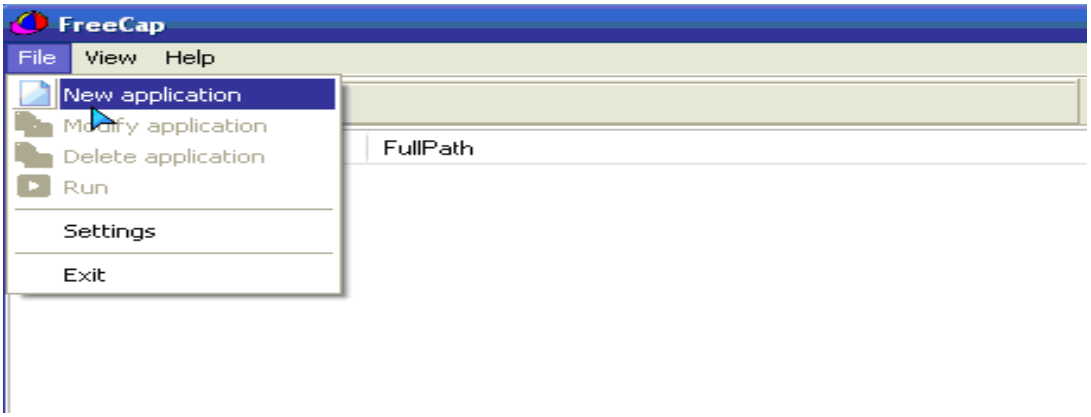
4.3.4 Torcap2

Το Torcap2 είναι ένα μικρό πρόγραμμα το οποίο βασίζεται πάνω στο Torcap και κάνει την ίδια λειτουργία, δηλαδή προσθέτει τα socks4a σε κάθε εφαρμογή που έχει πρόσβαση στο internet.[81] Η διαφορά των Torcap και Torcap2 είναι ότι, το Torcap είναι γραμμένο σε Delphi και έχει μέγεθος περίπου 200K, ενώ το Torcap2 είναι γραμμένο σε C και το μέγεθός του είναι 50K.

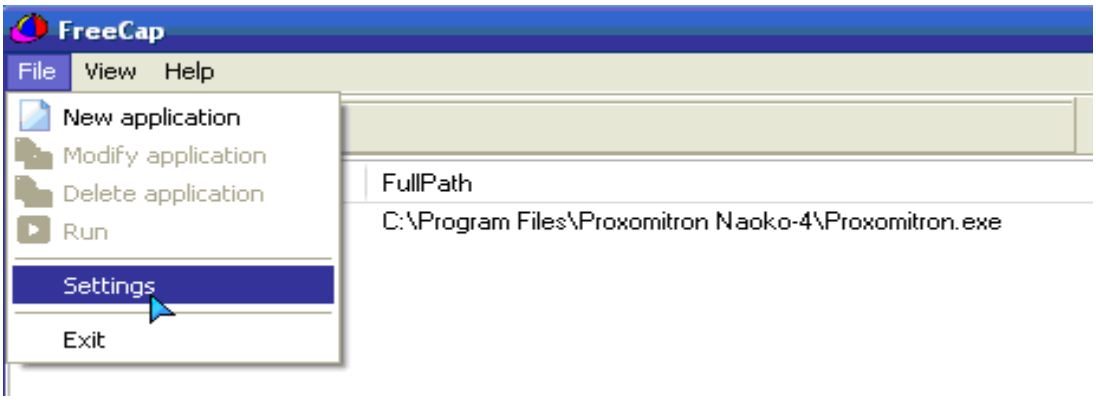
4.3.5 Freecap

Το Freecap είναι ένα πρόγραμμα το οποίο ασχολείται με τις απευθείας συνδέσεις μέσω των socks servers.[82] Αν κάποια προγράμματα δεν υποστηρίζουν τα socks πχ, ο internet explorer, τότε το Freecap είναι πολύ χρήσιμο σε αυτές τις περιπτώσεις γιατί αυτόματα περνάει όλες τις συνδέσεις μέσω του socks server.[83]

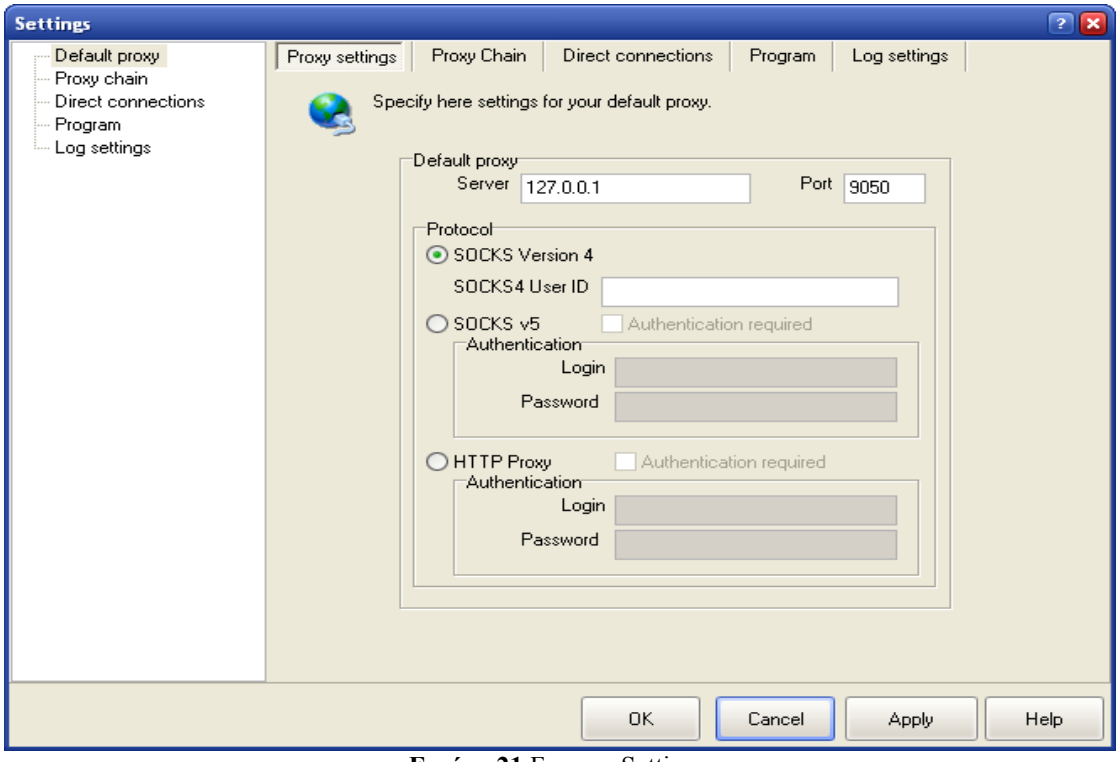
[81] http://www.virtualventures.ca/~cat/
[82] http://www.freecap.ru/eng/?p=whatis
[83] http://prxbx.com/forums/showthread.php?tid=639



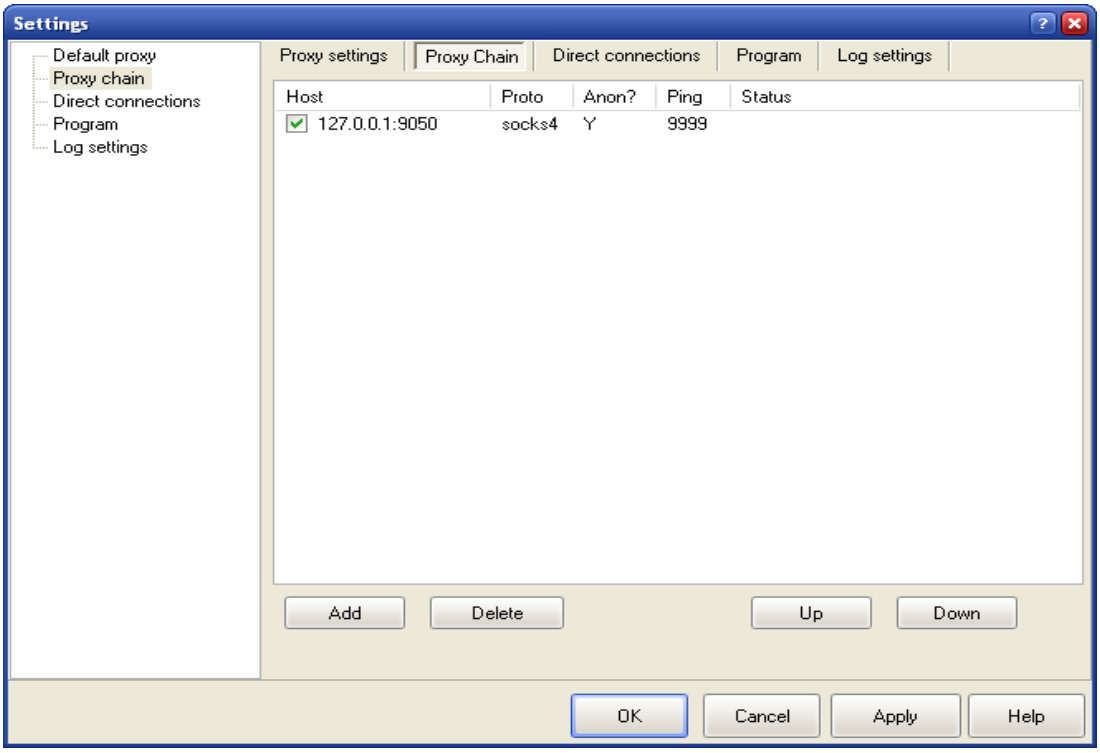
Εικόνα 19 Freecap New Application



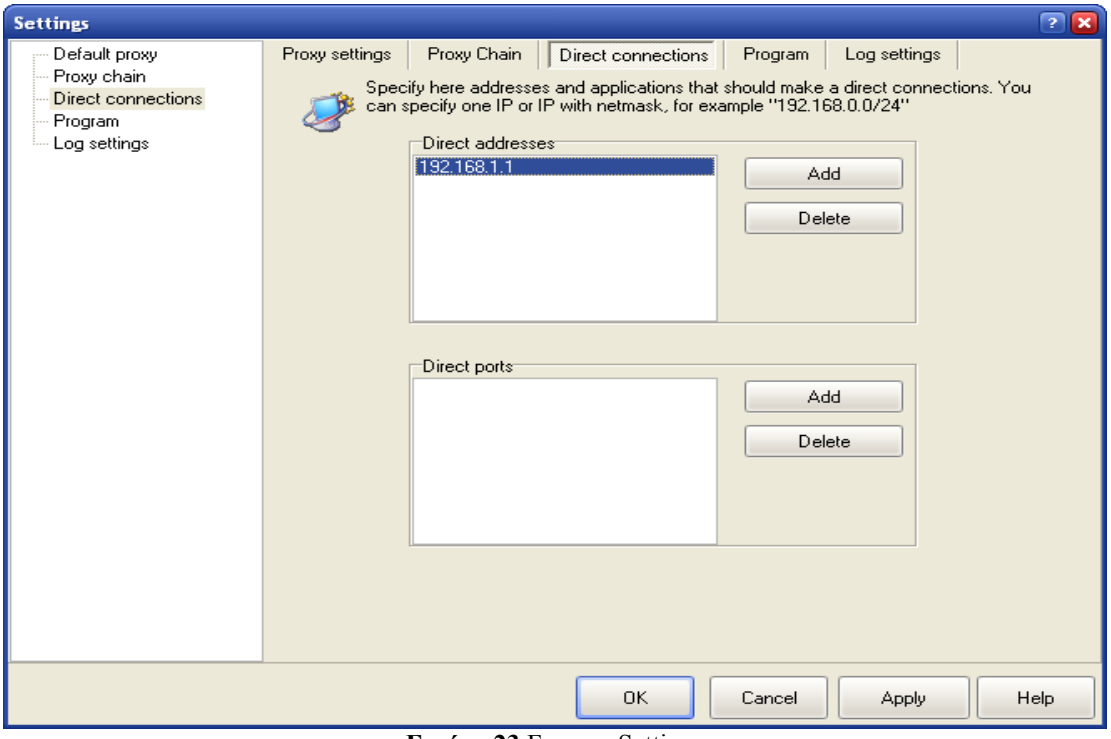
Εικόνα 20 Freecap Settings



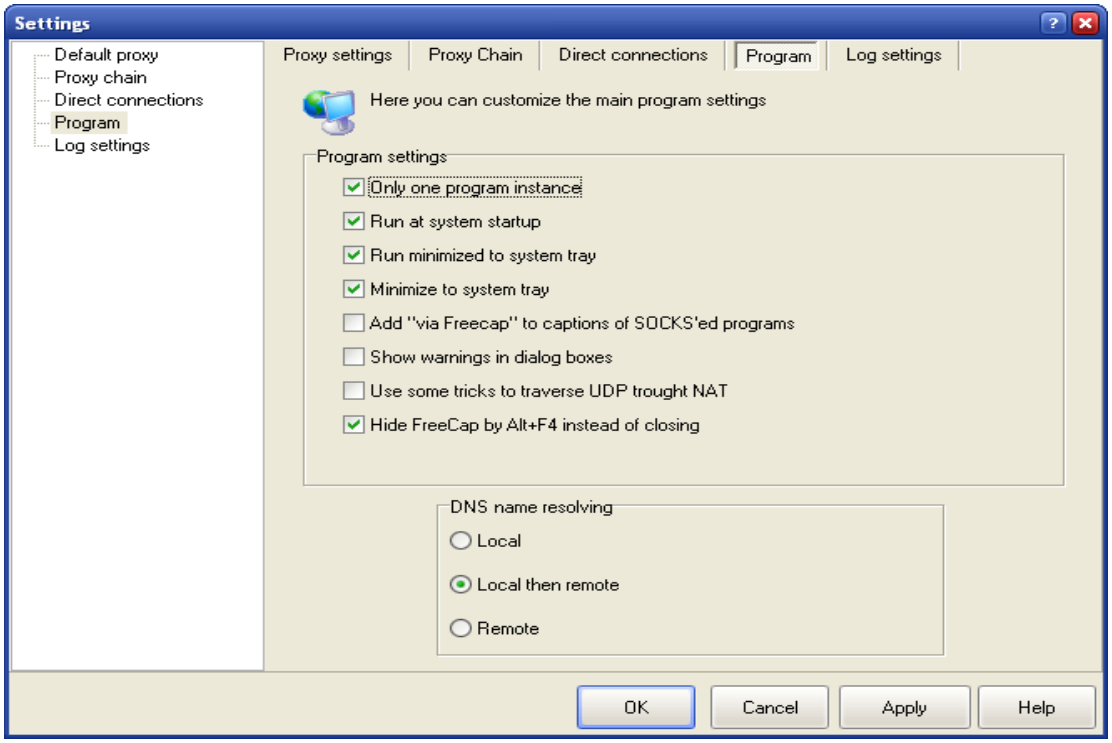
Εικόνα 21 Freecap Settings



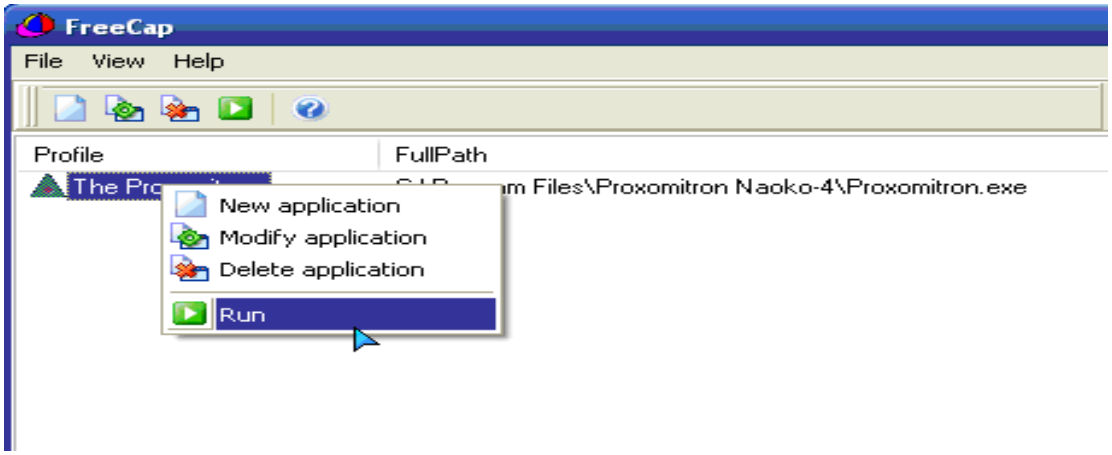
Εικόνα 22 Freecap Settings



Εικόνα 23 Freecap Settings



Εικόνα 24 Freecap Settings

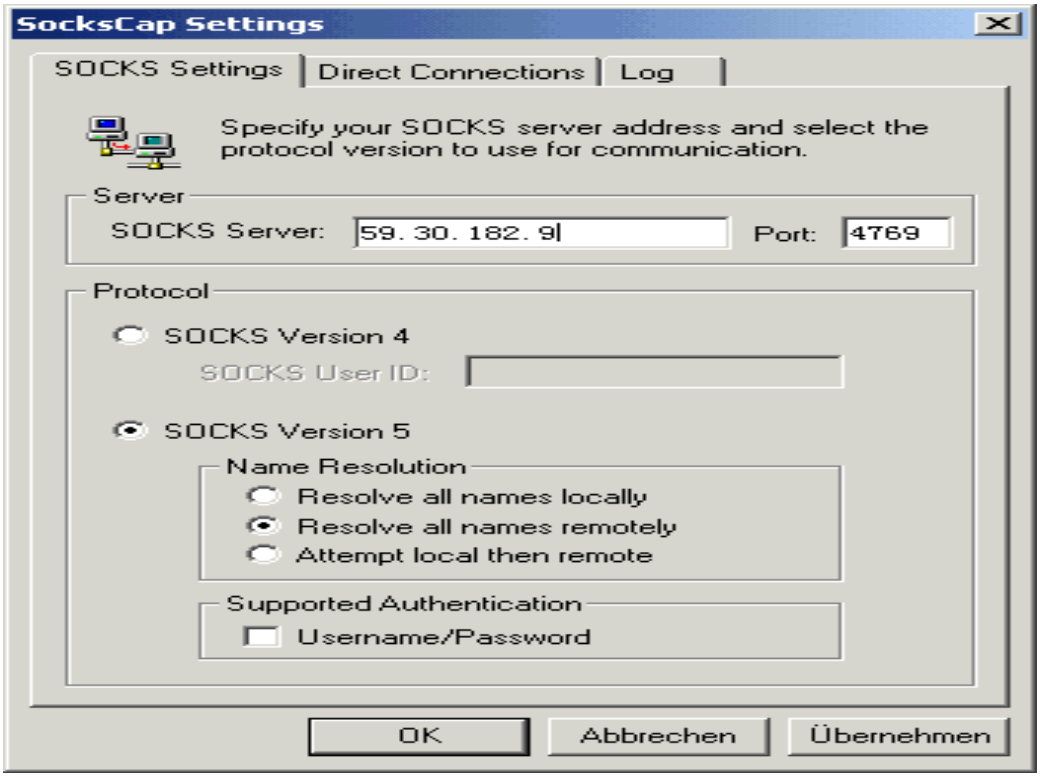


Εικόνα 25 Freecap Run

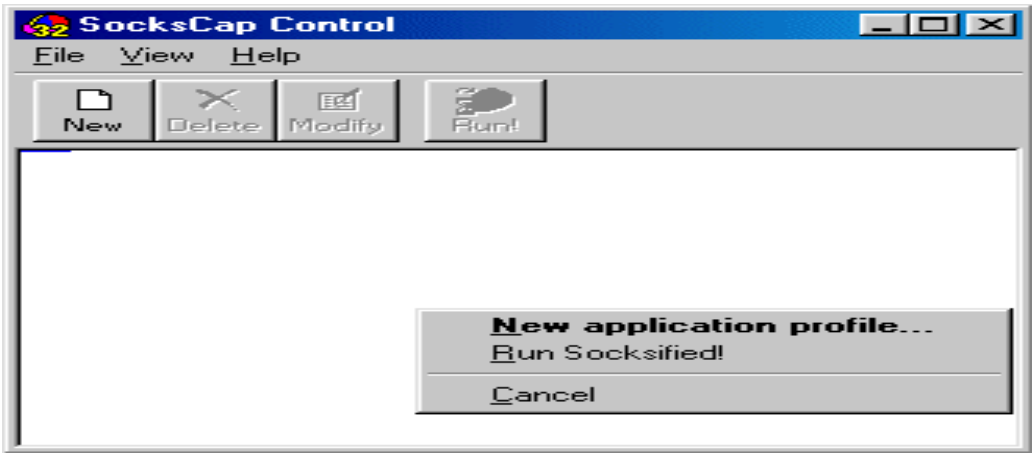
4.3.6 Sockscap

Το Sockscap είναι ένα πρόγραμμα το οποίο λειτουργεί μέσω ενός socks server έκδοσης 4 ή 5, με αποτέλεσμα ο server που βρίσκεται στην άκρη της σύνδεσης να μην μπορεί να γνωρίζει την αληθινή μας IP. [84]

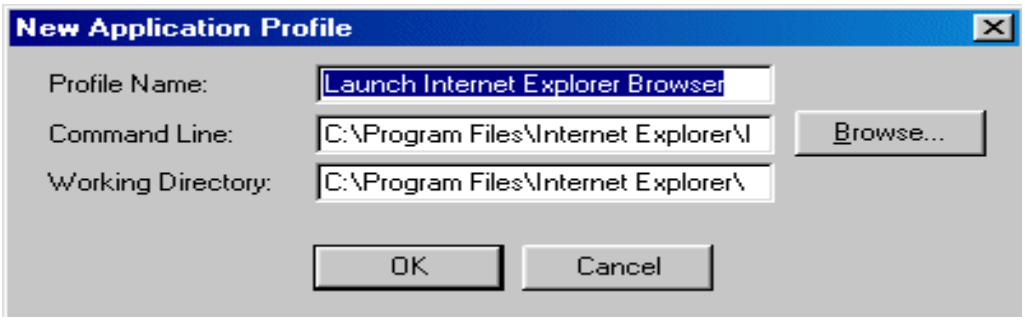
[84] http://www.my-proxy.com/content/Proxy%20Tools/SocksCap%20Full%20Tutorial%20with%20Pictures.html



Εικόνα 26 Sockscap Settings



Εικόνα 27 Sockscap Control



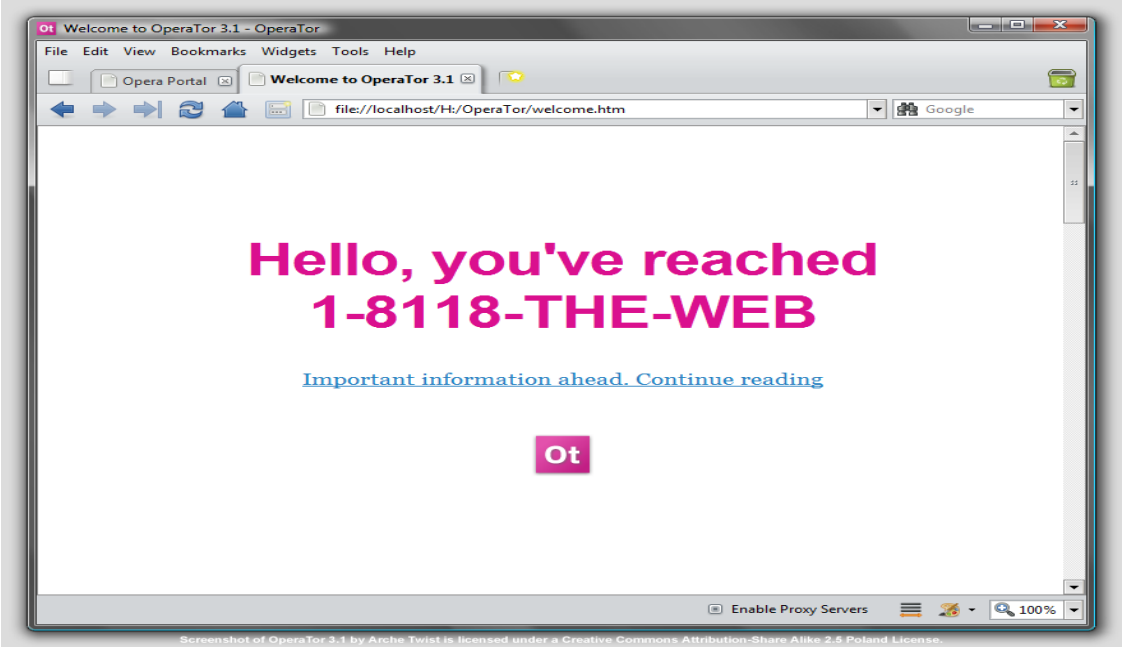
Εικόνα 28 New Application Proflile

Εικόνα 29 Sockscap Control

4.3.7OperaTor

Το OperaTor είναι ένα πακέτο που μπορεί εύκολα να εγκατασταθεί σε κάποια φορητή μνήμη (usb stick, pendrive, εξωτερικό σκληρό) και επιτρέπει ανώνυμο σερφάρισμα σε δημόσιους χώρους (net cafes, δημόσιες βιβλιοθήκες κοκ) και όχι μόνο.[85] Συνδυάζει τη δύναμη του Opera , του The Onion Router και του Privoxy. Με το OperaTor δεν θα αποθηκευτούν καθόλου πληροφορίες στο computer που έχουμε συνδέσει τη φορητή μνήμη. Μια σημαντική σημείωση είναι ότι οι ακόλουθες λειτουργίες δεν περνάνε ανώνυμες καθώς δεν χρησιμοποιούν τις proxy ρυθμίσει του Opera : Java, ενσωματωμένος διακομιστής Bittorrent, ενσωματωμένος διακομιστής e-mail και IRC.

[85] http://community.athens.indymedia.org/index.php?topic=427.0



Εικόνα 30 OperaTor

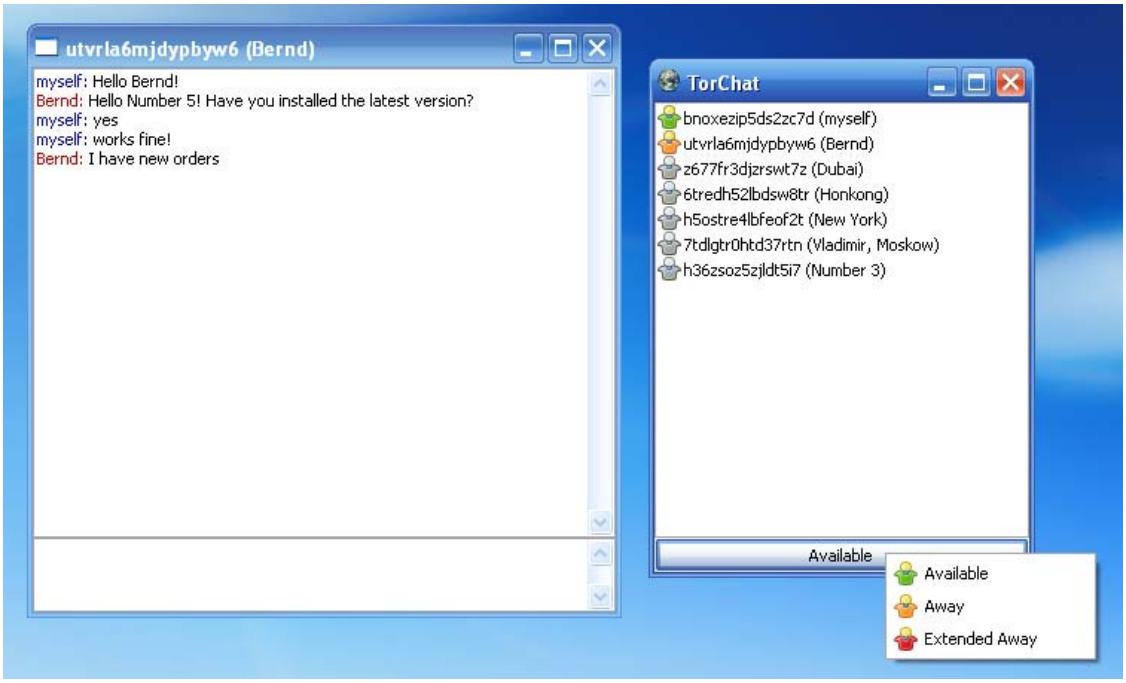
4.3.8 Xerobank browser

Το λογισμικό XeroBank μας δίνει τη δυνατότητα να «σερφάρουμε» ανώνυμα στο διαδίκτυο. Το XeroBank installer περιλαμβάνει το xB Browser, το xB Mail και το xB VPN.[86] Ο xB Browser χρησιμοποιείται για πρόσβαση στον web browser μέσω φορητής μνήμης και μπορεί να προσφέρει υψηλού επιπέδου ανωνυμία. Επίσης ο xB Browser κρυπτογραφεί τις δραστηριότητές μας και αποτρέπει τον εντοπισμό μας από κακόβουλους. Το xB Mail περιλαμβάνεται για τους Xerobank χρήστες, και χρησιμοποιείται για την πρόσβαση σε κρυπτογραφημένο e-mail. Το xB VPN χρησιμοποιείται για να δημιουργήσει μια VPN σύνδεση στο δίκτυο ανωνυμίας XeroBank. Έχει σχεδιαστεί για συνδέσεις OpenVPN και μπορεί να λειτουργήσει σε Windows 2k, NT, XP και Vista x64.

4.3.9 TorChat

Το TorChat είναι ένας peer to peer instant messenger και έχει σχεδιαστεί με βάση τις κρυμμένες υπηρεσίες του Tor.[87] Μας παρέχει ισχυρή ανωνυμία και είναι πολύ εύκολο στη χρήση του. Λειτουργεί μέσω ενός USB οδηγού σε οποιοδήποτε υπολογιστή που έχει λειτουργικό σύστημα τα windows.

[86] https://xerobank.com/download/
[87] http://code.google.com/p/torchat/

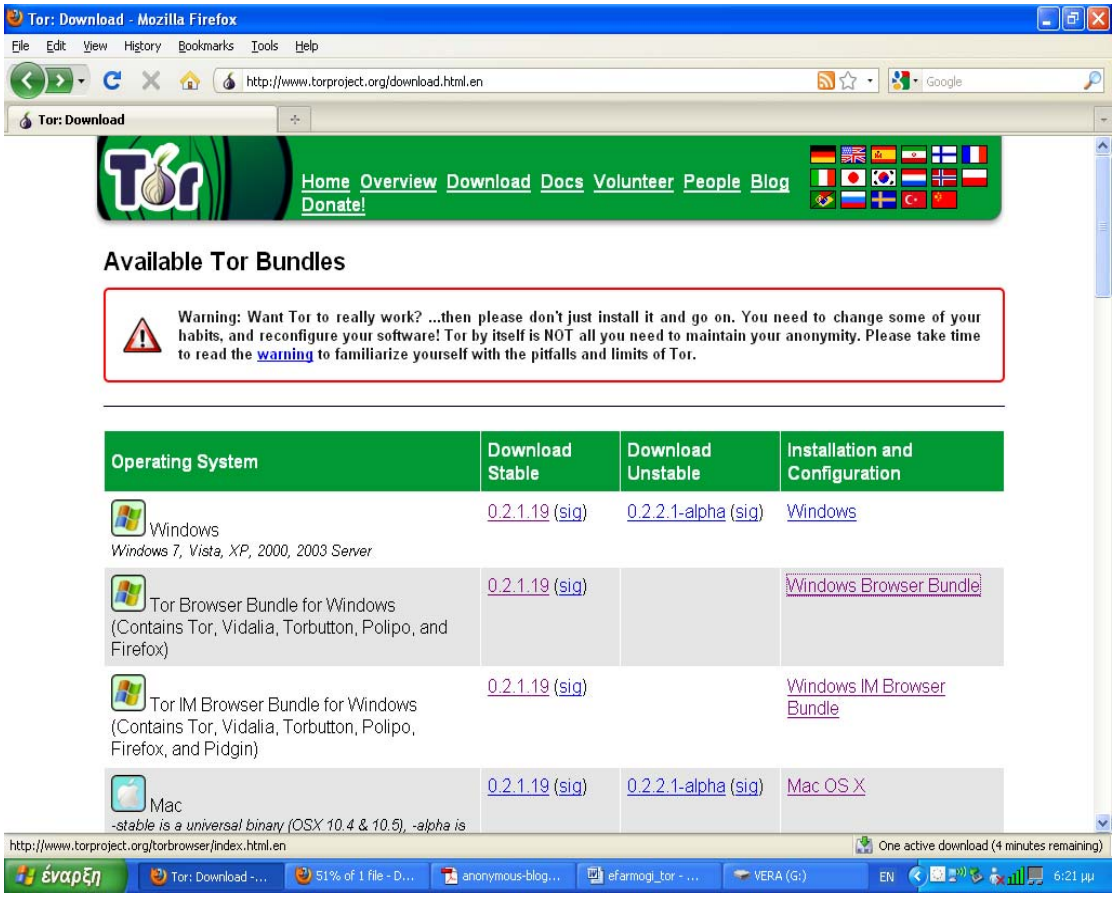


Εικόνα 31 Using TorChat

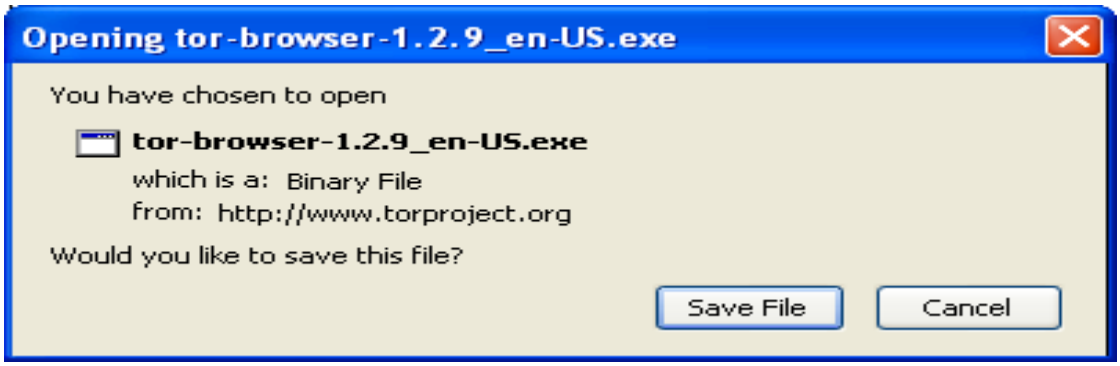
4.4 Εφαρμογή TOR

Για να εγκαταστήσουμε το Tor πηγαίνουμε στο site του Tor [88] και επιλέγουμε την δεύτερη επιλογή *Tor Browser Bundle for Windows*.

[88] http://www.torproject.org/download.html.en

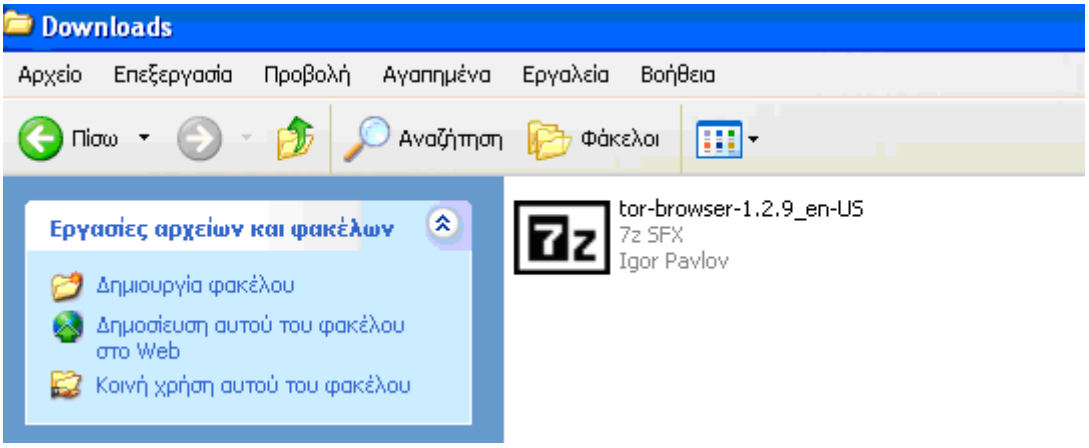


Εικόνα 32 Tor: Download



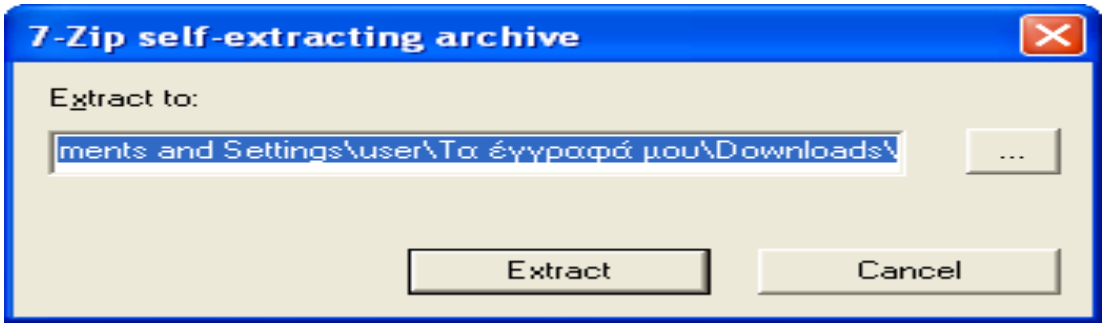
Εικόνα 33 Tor: Save

Αποθηκεύουμε το αρχείο και μας εμφανίζεται το αρχείο Tor-browser-1.2.9_en-US.

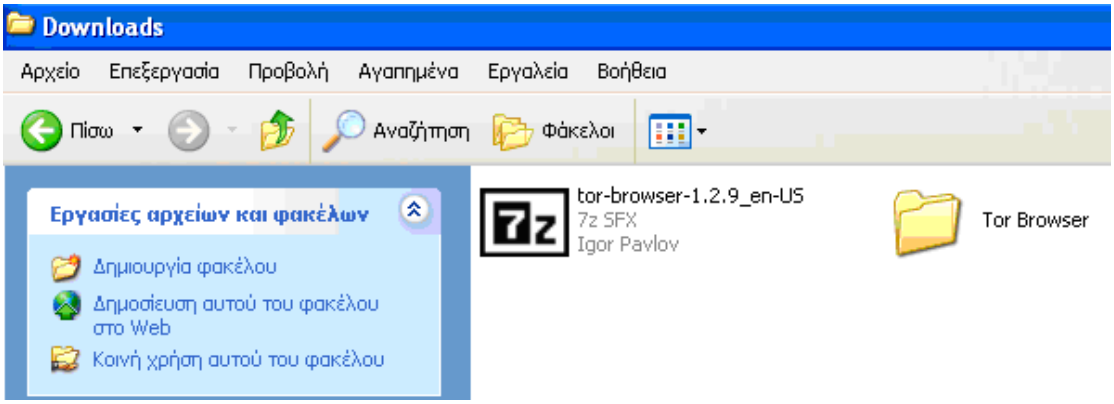


Εικόνα 34 Tor: Is downloaded

Στη συνέχεια το επιλέγουμε με διπλό κλικ για να κάνει extract τα αρχεία που περιέχει.

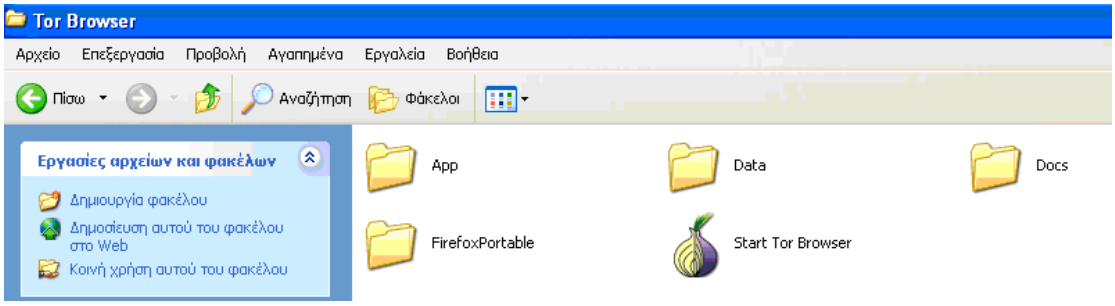


Εικόνα 35 Tor: Extract files



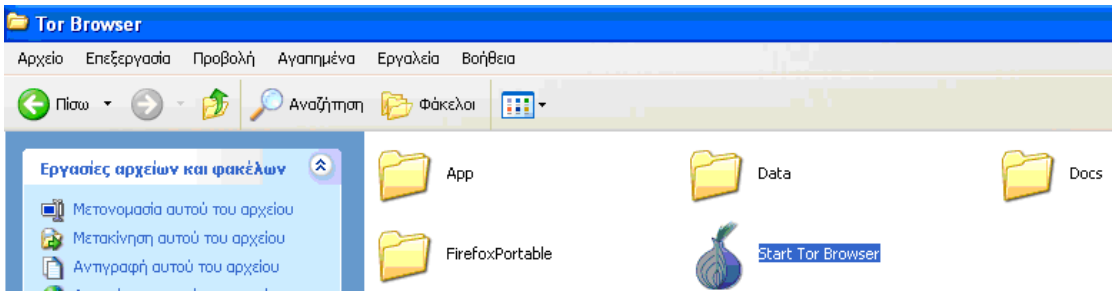
Εικόνα 36 Tor: Extracting files

Αφού ανοίξουμε τον φάκελο Tor Browser μας εμφανίζονται τα παρακάτω αρχεία.



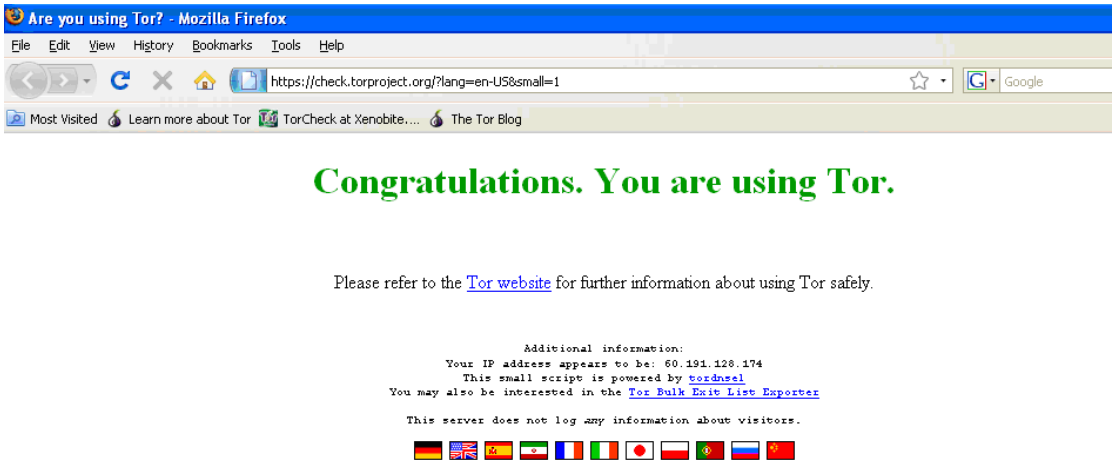
Εικόνα 37 Tor: Opening tor folder

Επιλέγουμε Start tor Browser, και ξεκινάει να φορτώνει το Tor.



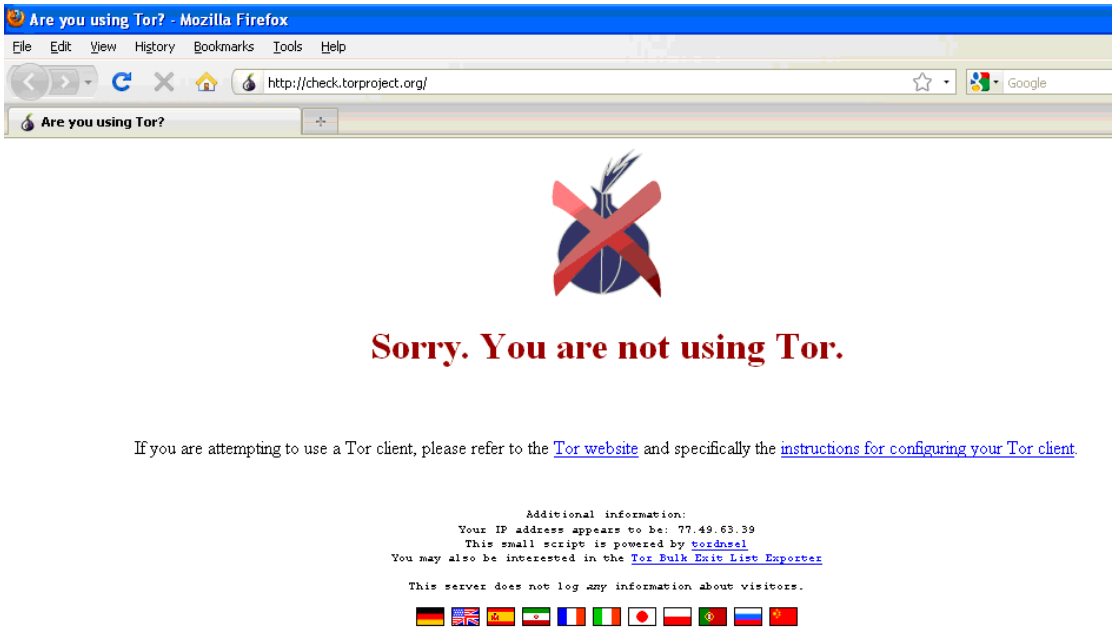
Εικόνα 38 Tor: Load tor browser

Αν μας εμφανιστεί το μήνυμα ότι έχουμε συνδεθεί στο Tor, τότε μας ανοίγει την παρακάτω σελίδα στον Firefox



Εικόνα 39 Tor: Opening firefox through tor

Αν δεν έχει γίνει σωστά η σύνδεση, τότε θα μας εμφανιστεί το παρακάτω μήνυμα στον Firefox.



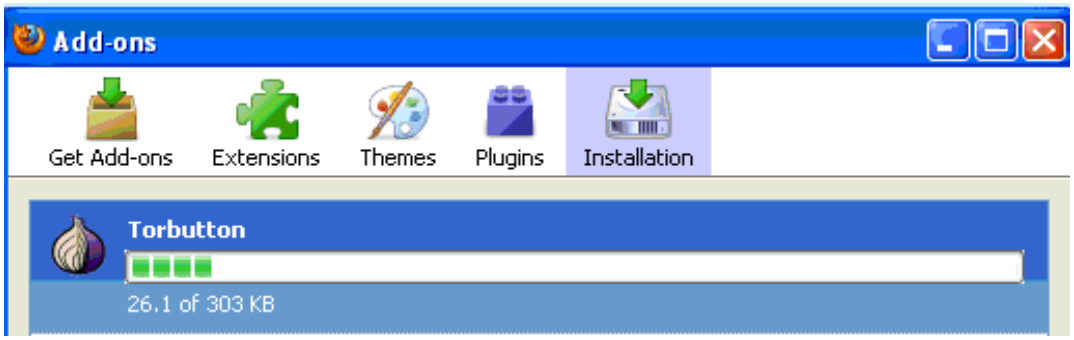
Εικόνα 40 Tor: Not connected

Από το site του Mozilla [89] μπορούμε να κατεβάσουμε το Tor button, το οποίο μας επιτρέπει να ενεργοποιούμε και να απενεργοποιούμε το Tor από τον Firefox.

Εικόνα 41 Tor: Download tor button

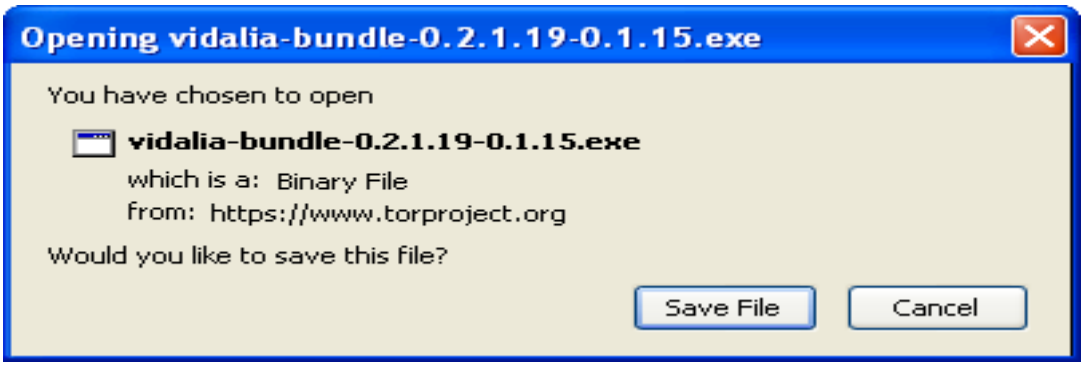
[89] https://addons.mozilla.org/en-US/firefox/addon/2275

Επιλέγουμε Add to Firefox και εκτελείται η εγκατάσταση.



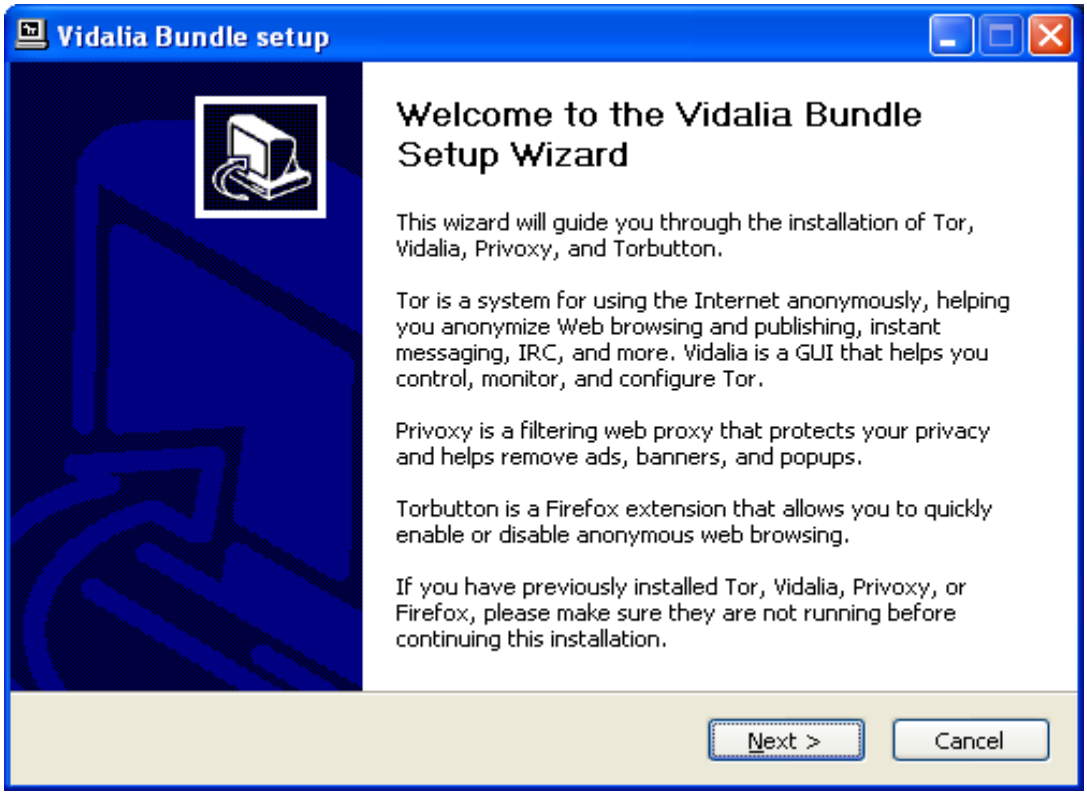
Εικόνα 42 Tor: Setup tor button

Για καλύτερη χρήση του Tor θα πρέπει να εγκαταστήσουμε και το παρακάτω αρχείο από το site του Tor [90] , και εκτελούμε τα παρακάτω βήματα.

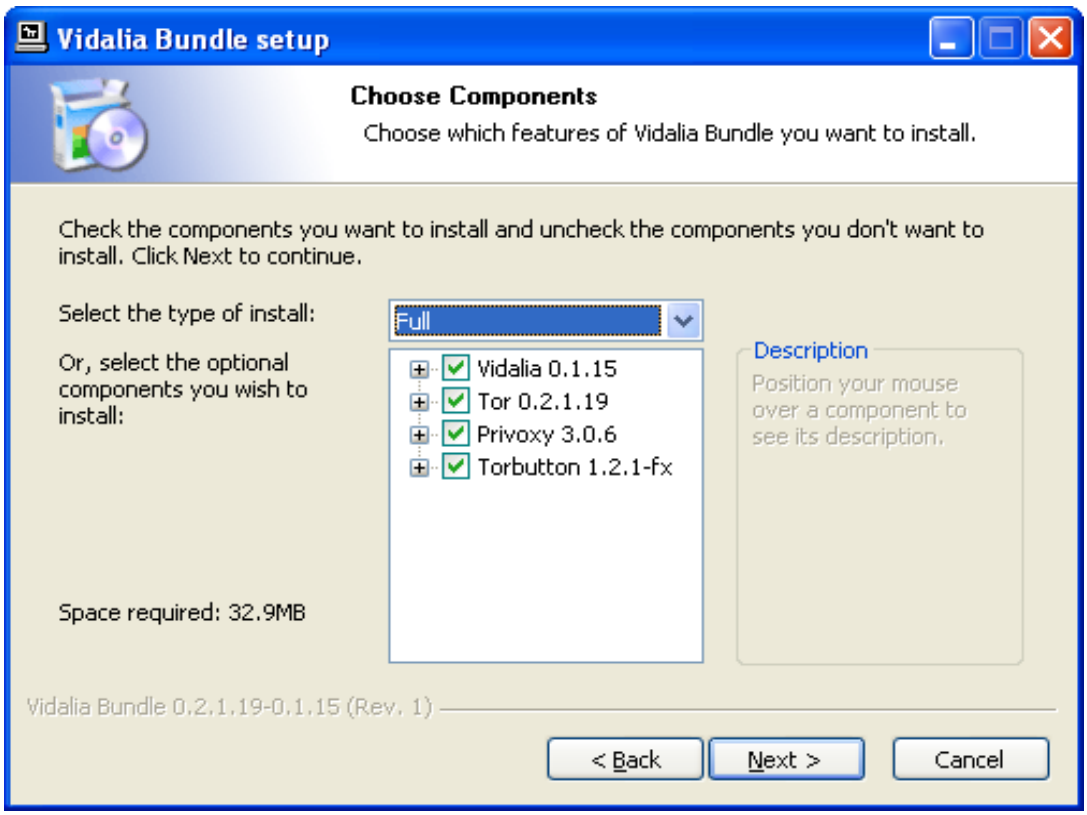


Εικόνα 43 Tor: Save vidalia tool

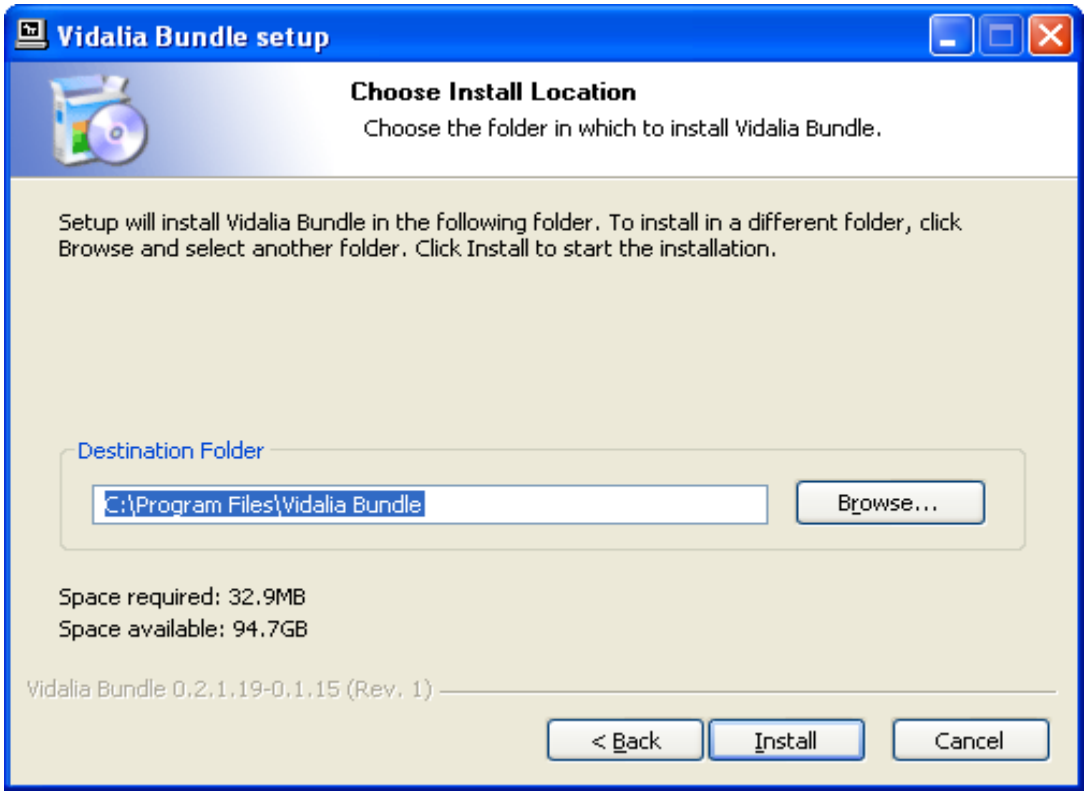
[90] http://www.torproject.org/easy-download.html.en



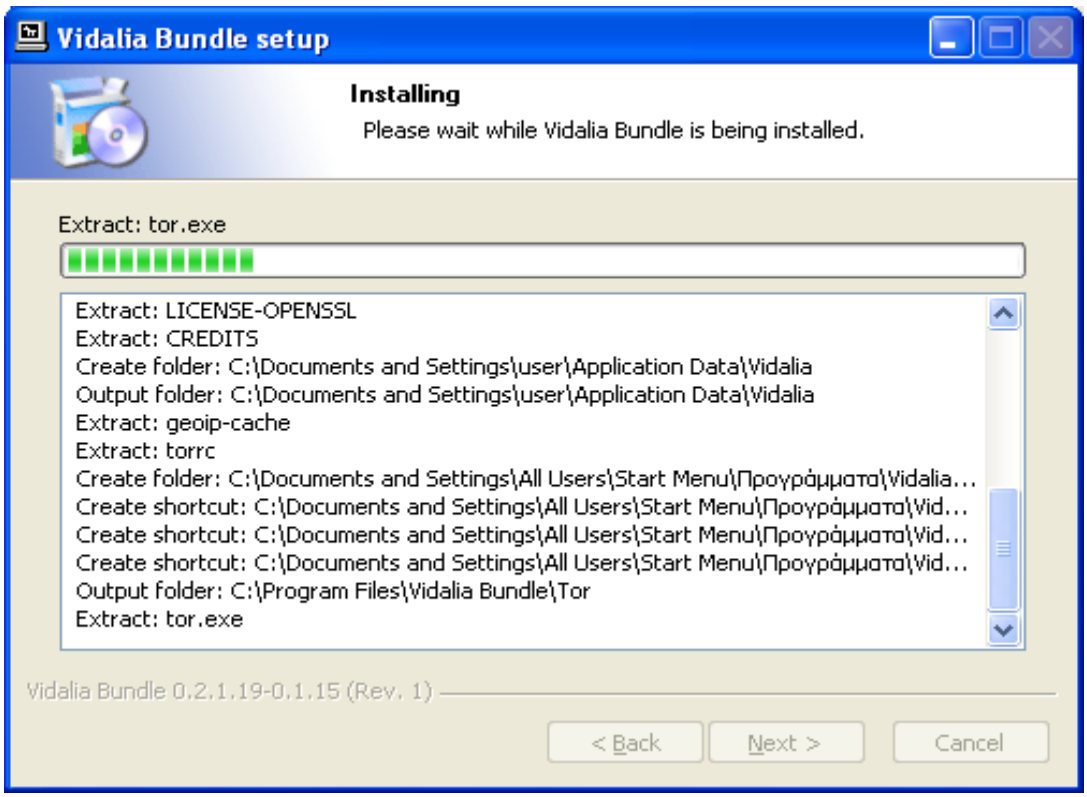
Εικόνα 44 Tor: Setup vidalia tool



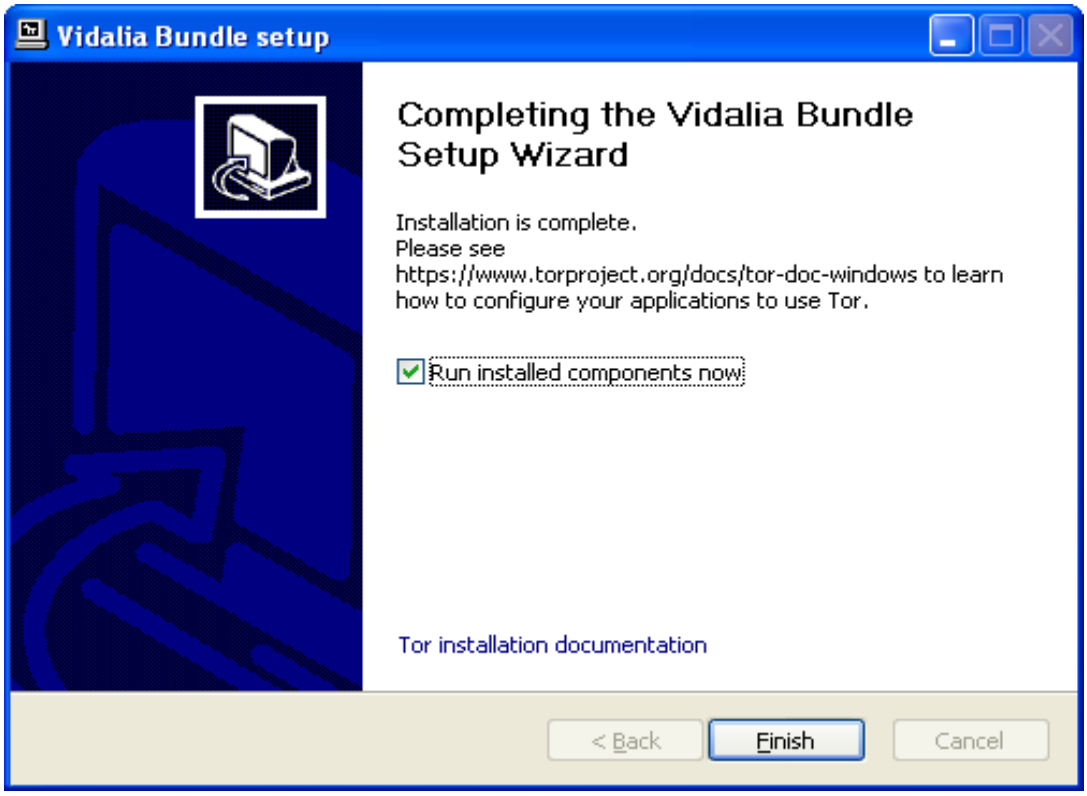
Εικόνα 45 Tor: Setup vidalia tool



Εικόνα 46 Tor: Setup vidalia tool

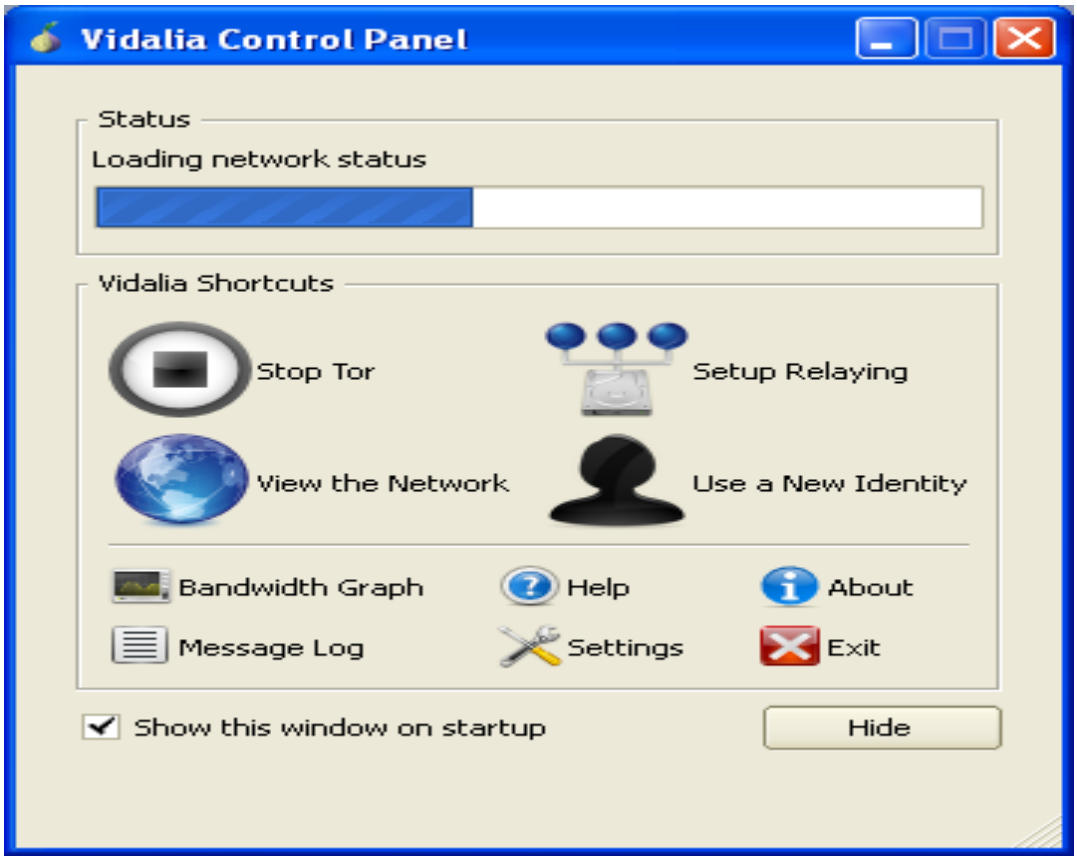


Εικόνα 47 Tor: Setup vidalia tool

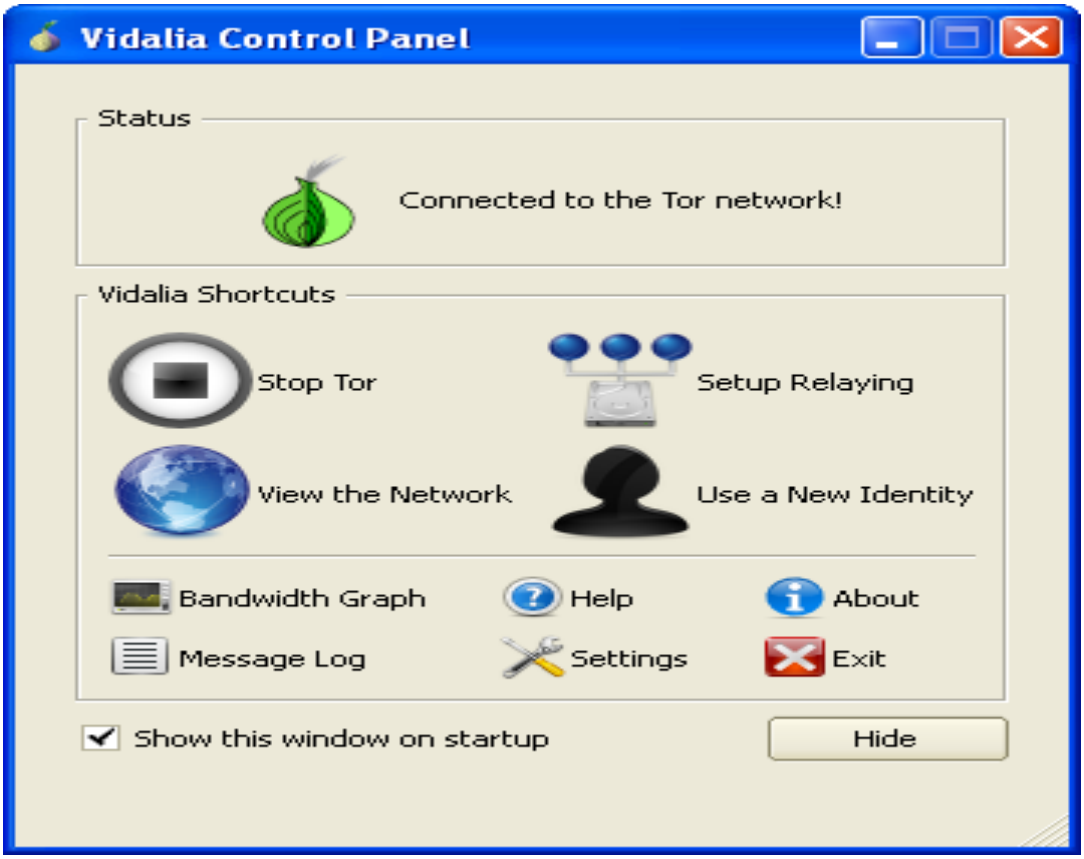


Εικόνα 48 Tor: Setup vidalia tool

Αφού τελειώσουμε με την εγκατάσταση ανοίγει ο πίνακας ελέγχου του Vidalia.



Εικόνα 49 Tor: Vidalia control panel



Εικόνα 50 Tor: Vidalia control panel - Connected

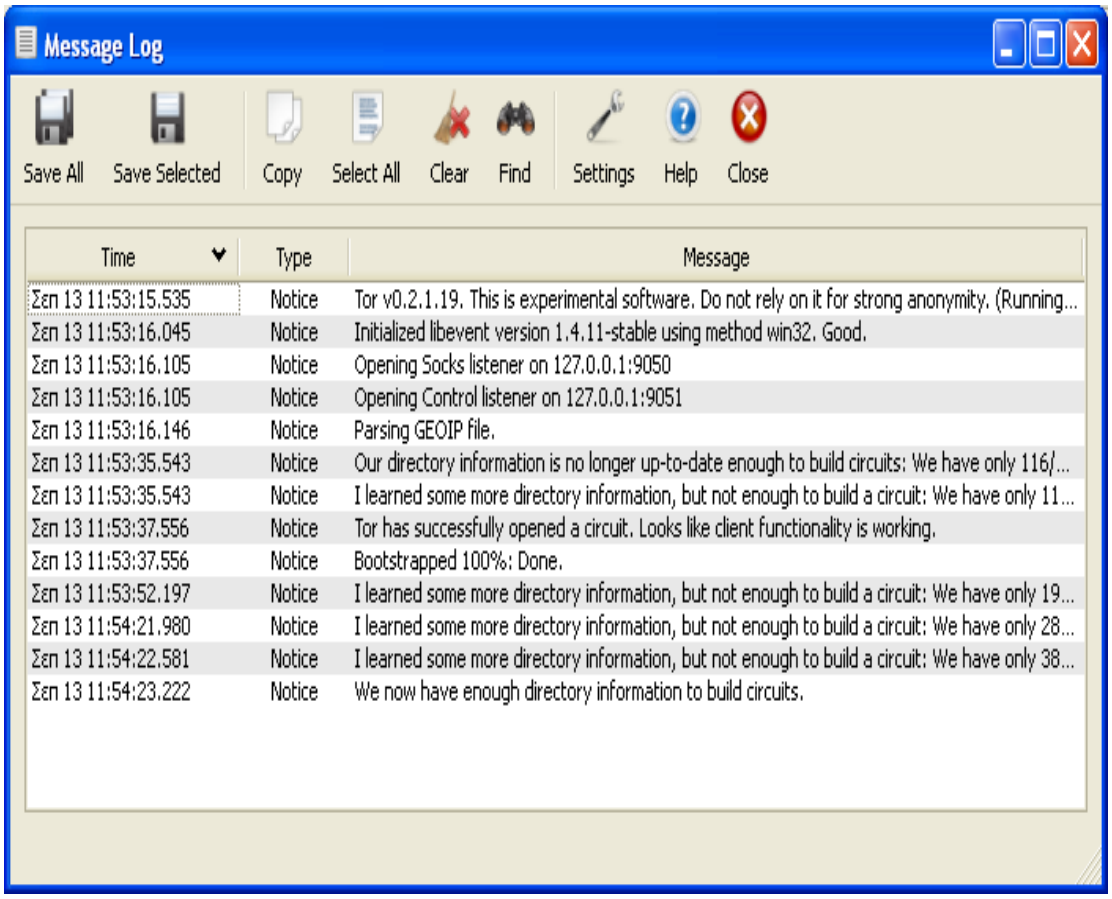
Αν έχει γίνει επιτυχώς η εγκατάσταση τότε στη γραμμή εργαλείων θα πρέπει να δούμε τα παρακάτω εικονίδια: P για Privoxy και onion για Tor.

Πρέπει να σημειώσουμε ότι για να δουλέψει το Tor πρέπει να έχουμε απενεργοποιήσει το firewall του υπολογιστή μας. Τα παρακάτω εικονίδια απεικονίζουν την κατάσταση που μπορεί να βρίσκεται το Tor.

 Αν μας εμφανιστεί αυτό το εικονίδιο τότε το Tor έχει σταματήσει. Για να ξεκινήσει πρέπει να επιλέξουμε *Start* από το Vidalia menu.
 Το Tor ξεκινάει.
 Το Tor είναι ενεργό. Αν θέλουμε να σταματήσει το Tor, τότε επιλέγουμε *Stop* από τοVidalia menu. Αν επιθυμούμε να δούμε τι κάνει το Tor, τότε μπορούμε να ανοίξουμε το *message log*, το οποίο αποθηκεύει πληροφορίες καθώς τρέχει το Tor.

Το Tor είναι στη διαδικασία απενεργοποίησης.

Πίνακας 1 Tor Status



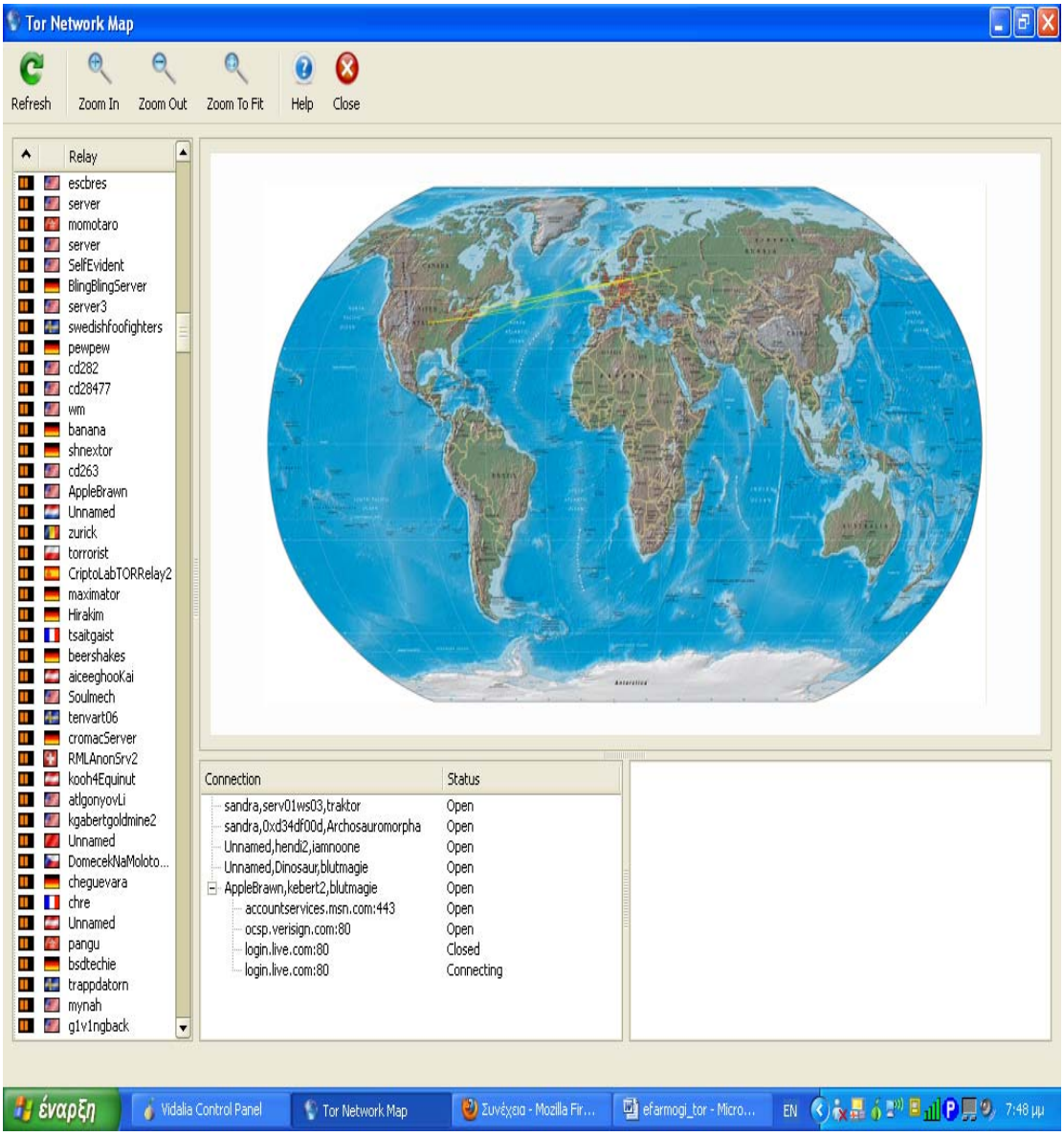
Εικόνα 51 Tor: Message Log

Network viewer

Όταν θέλουμε να επικοινωνήσουμε ανώνυμα μέσω του Tor, δηλαδή με το να συνδεθούμε σε ένα site, τότε το Tor δημιουργεί ένα κύκλωμα από κρυπτογραφημένες συνδέσεις μέσα από μια σειρά αναμεταδοτών στο δίκτυο. Η κίνηση των εφαρμογών μας στέλνεται σαν ένα stream μέσα από αυτό το κύκλωμα. Πολλά από αυτά τα streams μπορεί να μοιράζονται το ίδιο κύκλωμα.

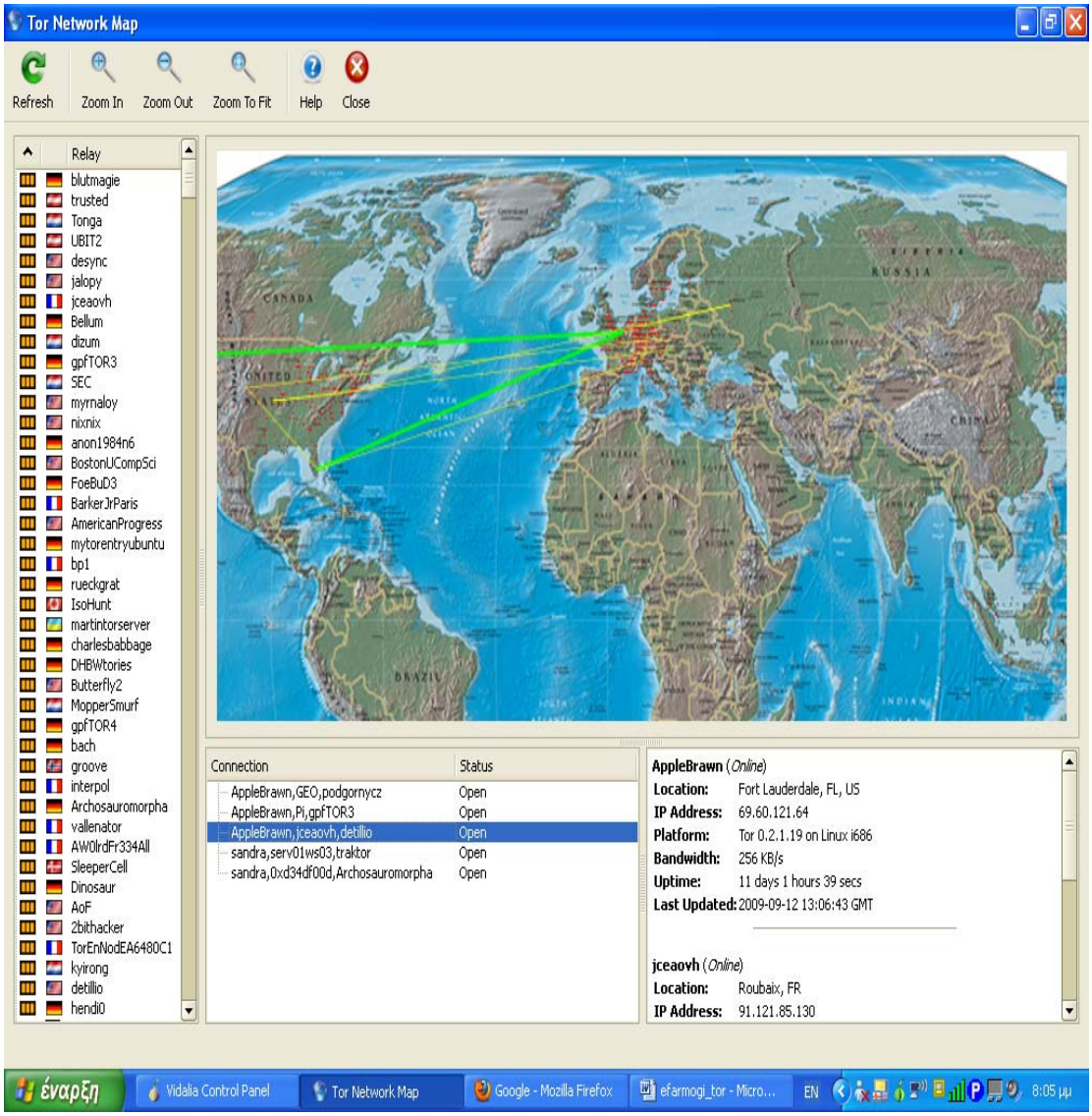
Network Map

Το network map περιέχει ένα παγκόσμιο χάρτη, με κόκκινες κουκίδες που δείχνουν τη γεωγραφική θέση των αναμεταδοτών (relays) στο δίκτυο Tor. Οι πράσινες γραμμές εμφανίζονται μεταξύ των relays που δείχνουν το μονοπάτι των κυκλωμάτων που δημιούργησε ο δικός μας Tor client στο δίκτυο Tor.

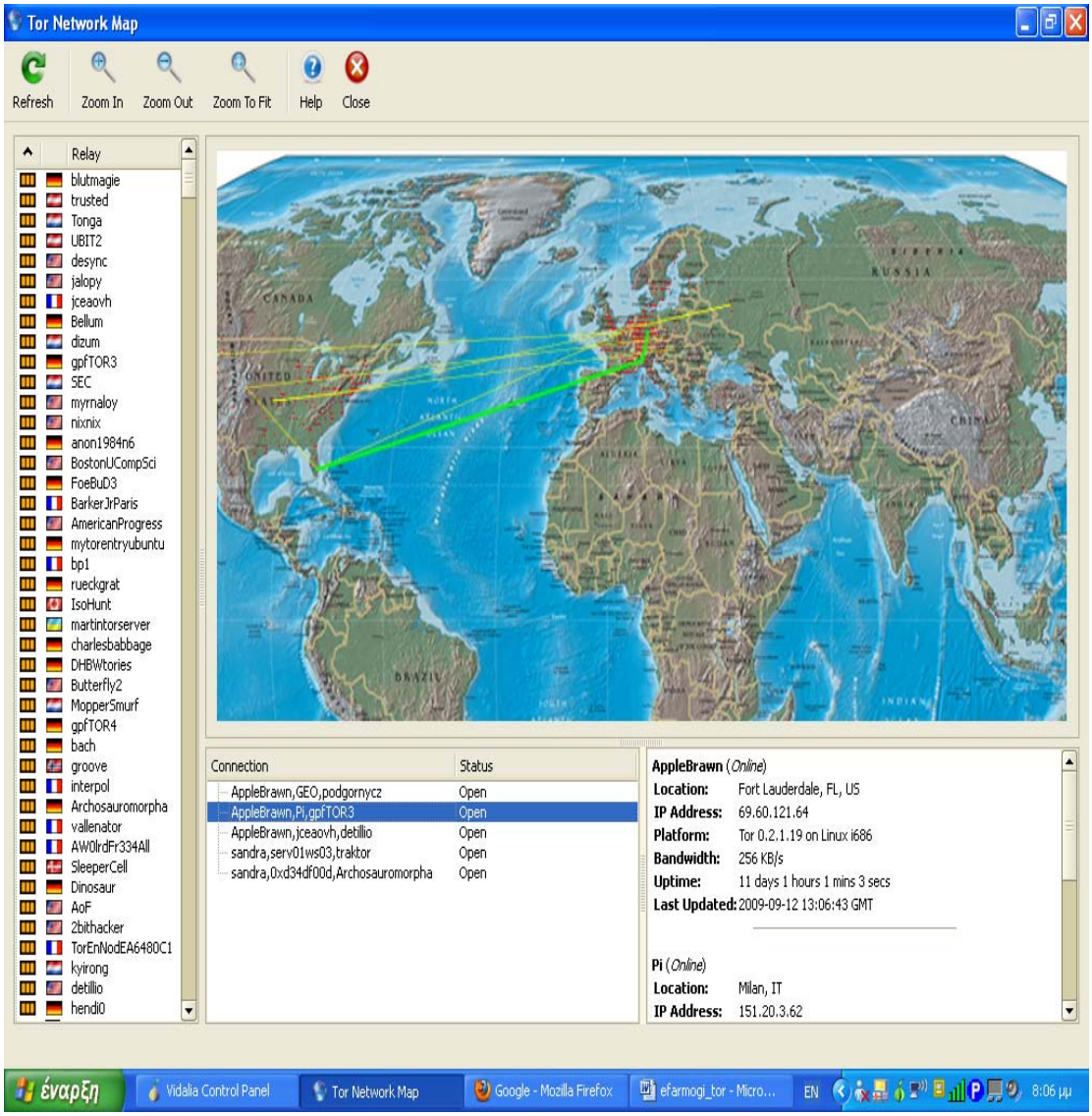


Εικόνα 52 Tor: Network Map

Εικόνα 53 Tor: Network Map



Εικόνα 54 Tor: Network Map



Εικόνα 55 Tor: Network Map

Κάτω από τον Network map, βλέπουμε μια λίστα των ενεργών κυκλωμάτων και τη κίνηση των εφαρμογών τους.

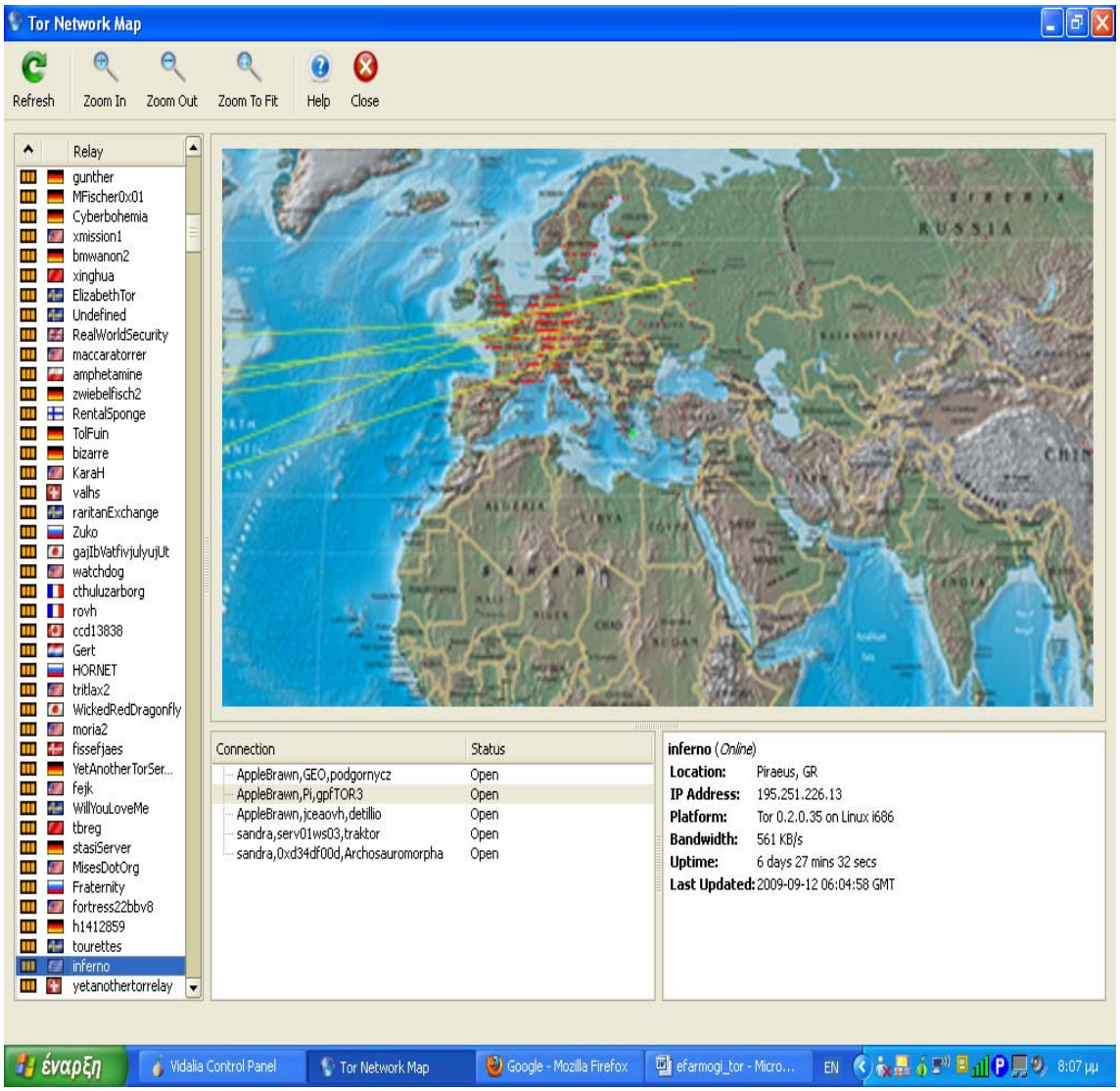
Location	Η γεωγραφική θέση του Tor relay.
IP Address	Η IP διεύθυνση στην οποία ο Tor relay μπορεί να συνδεθεί.
Platform	Πληροφορίες για το λειτουργικό σύστημα και η έκδοση του Tor που χρησιμοποιεί ο relay που «τρέχει» συγχρόνως.
Bandwidth	Ο φάκελος πληροφοριών των relays υπολογίζει το bandwidth που έχει δει πρόσφατα για αυτόν τον relay.
Uptime	Χρονική περίοδος όπου αυτός ο relay είναι διαθέσιμος.
Last Updated	Πληροφορίες ημερομηνίας τελευταίας ενημέρωσης του relay.

Πίνακας 2 Relay Details

Όταν εμφανίζεται αρχικά ο χάρτης, πιθανώς να δούμε ότι συνδέεται στο geoip.vidalia-project.net, το οποίο μας δείχνει τη γεωγραφικές πληροφορίες για τη λίστα των Tor relays. Στην αριστερή μεριά του network view, βλέπουμε μια λίστα από relays του Tor δικτύου. Δίπλα από κάθε relay εμφανίζεται ένα εικονίδιο που δείχνει τη κατάστασή του.

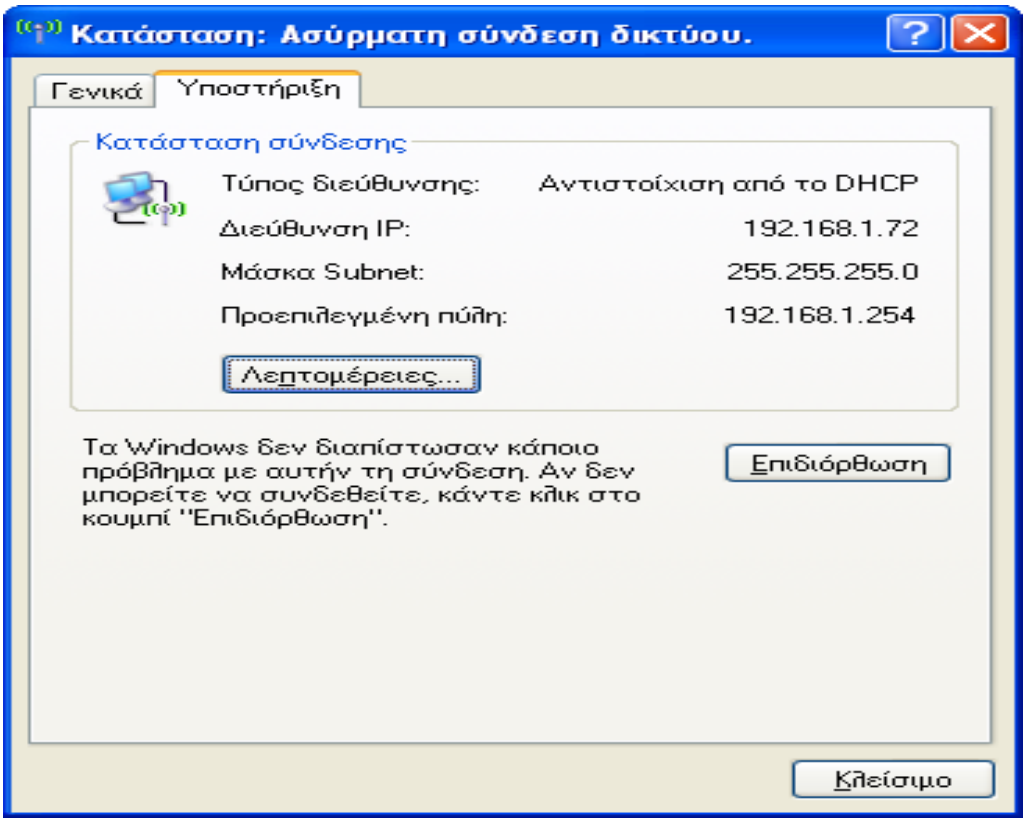
Ο relay είναι offline ή δεν ανταποκρίνεται.
Ο relay είναι *hibernating*, δηλαδή είναιonline, αλλά χρησιμοποιεί τόσο bandwidth όσο του δίνει ο operator για μια χρονική περίοδο.
Ο relay είναι online, αλλά δείχνει ελάχιστο throughput.
Ο relay είναι online και έχει throughput >= 20 KB/s.
Ο relay είναι online και έχει throughput >= 60 KB/s.
Ο relay είναι online και έχει throughput >= 400 KB/s.

Πίνακας 3 Relay Status



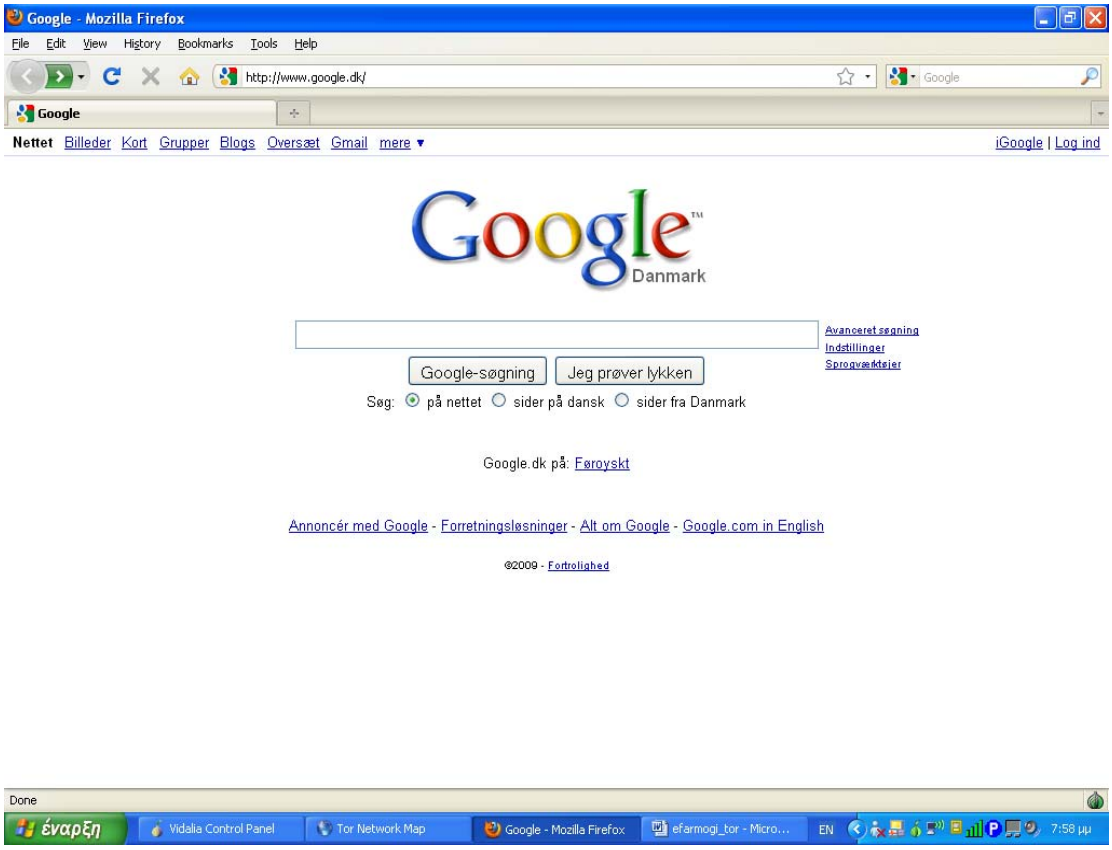
Εικόνα 56 Tor: Network Map

Μπορούμε επίσης να ελέγξουμε εάν έχει αλλάξει η IP διεύθυνση μας. Όπως βλέπουμε παρακάτω η IP μας είναι 192.168.1.72. Στη συνέχεια ανοίγουμε τον Firefox και πηγαίνουμε στο site της whatismyipaddress.com[91].



Εικόνα 57 Tor: IP address

[91] http://whatismyipaddress.com

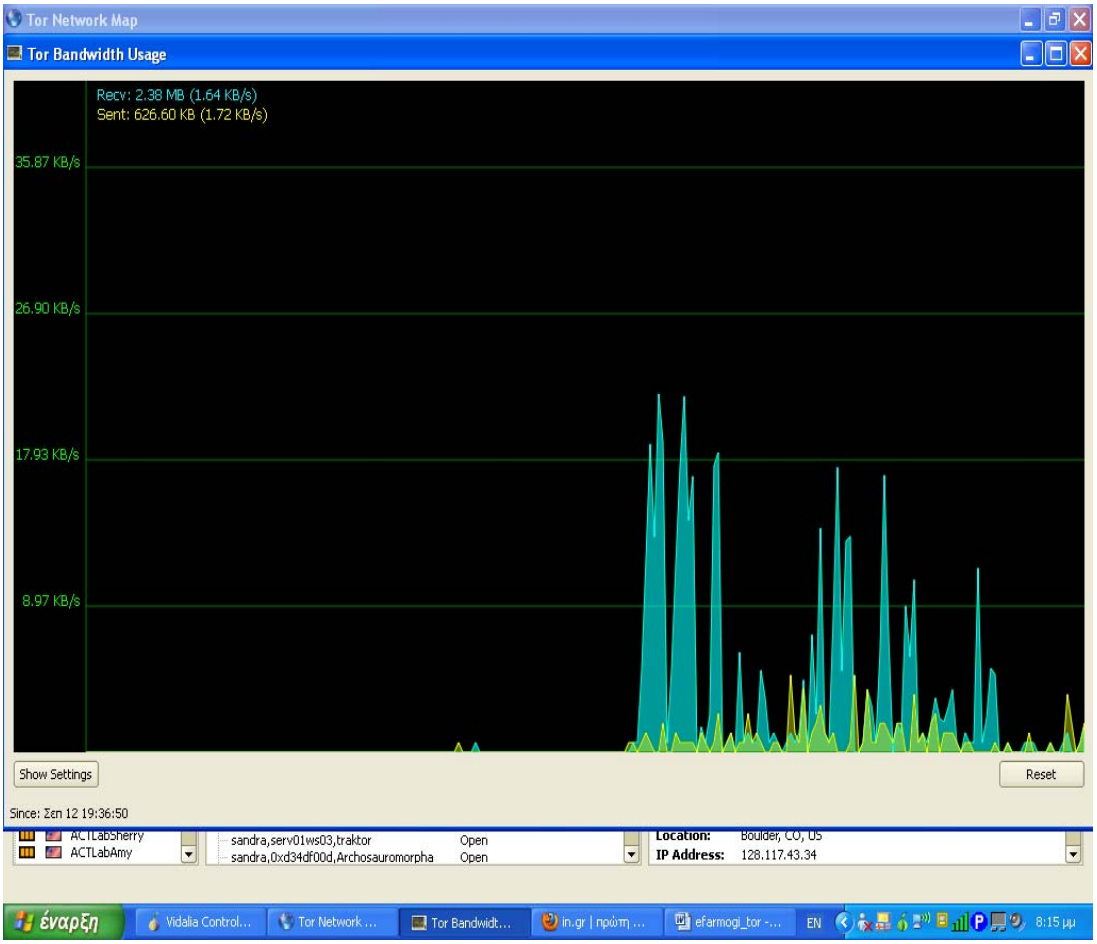


Εικόνα 58 Tor: www.google.dk

Παρατηρούμε ότι η IP διεύθυνσή μας έχει αλλάξει και έχει γίνει 192.251.226.206.

Εικόνα 59 Tor: http://whatismyipaddress.com

Παρακάτω βλέπουμε τη χρήση bandwidth του υπολογιστή μας από την επιλογή Tor Bandwidth Usage του Vidalia Control Panel.



Εικόνα 60 Tor: Bandwidth Usage

Κεφάλαιο 5 P2P (Peer to Peer system)

Ένα ανώνυμο P2P σύστημα επικοινωνιών είναι μια διανεμημένη εφαρμογή στην οποία οι κόμβοι ή οι συμμετέχοντες είναι ανώνυμοι ή ψευδώνυμοι.[92] Η ανωνυμία των συμμετεχόντων επιτυγχάνεται συνήθως από τα πρόσθετα δίκτυα επικαλύψεων δρομολόγησης που κρύβουν τη φυσική θέση κάθε κόμβου από άλλους συμμετέχοντες.

Το ενδιαφέρον για τα ανώνυμα P2P συστήματα έχει αυξηθεί τα τελευταία χρόνια για πολλούς λόγους, συμπεριλαμβανομένης της δυσπιστίας των κυβερνήσεων, της μαζικής επιτήρησης και της διατήρησης στοιχείων, και των δικών ενάντια στα bloggers. Τα δίκτυα αυτά μπορούν επίσης να απευθυνθούν σε εκείνους που επιθυμούν να μοιραστούν ενδεχομένως τα αρχεία - οργανώσεις όπως η ένωση βιομηχανίας καταγραφής της Αμερικής και της βρετανικής φωνογραφικής βιομηχανίας έχουν ακολουθήσει επιτυχώς και έχουν μηνύσει τους χρήστες στα μη-ανώνυμα P2P δίκτυα.

5.1 Κίνητρα για την ανωνυμία

Υπάρχουν πολλοί λόγοι να χρησιμοποιηθεί η ανώνυμη P2P τεχνολογία. Οι χρήστες P2P που επιθυμούν την ανωνυμία το κάνουν συνήθως διότι δεν επιθυμούν να προσδιοριστούν ως εκδότες (αποστολέας), ή αναγνώστες (δέκτης), των πληροφοριών.

Οι κοινοί λόγοι είναι οι παρακάτω:

- Το υλικό ή η διανομή του είναι παράνομο ή ενοχοποιητικά.
- Το υλικό είναι νομικό αλλά κοινωνικά ενοχλητικό ή προβληματικό στο κοινό (παραδείγματος χάριν, η ανωνυμία θεωρείται βασική απαίτηση για τις οργανώσεις όπως Αλκοολικούς)
- Ο φόβος της τιμωρίας
- Λογοκρισία στο τοπικό, οργανωτικό, ή εθνικό επίπεδο
- Προτιμήσεις προσωπικής μυστικότητας όπως της καταδίωξης παρεμπόδισης ή datamining δραστηριότητες.

Μια ιδιαίτερα ανοικτή άποψη σχετικά με το νομικό και παράνομο περιεχόμενο δίνεται στη φιλοσοφία πίσω από το ελεύθερο δίκτυο (freenet). Οι κυβερνήσεις ενδιαφέρονται επίσης για την ανώνυμη P2P τεχνολογία.

Το ναυτικό Ηνωμένου Βασιλείου χρηματοδότησε την αρχική έρευνα δρομολόγησης onion που οδήγησε στην ανάπτυξη του δικτύου Tor, το οποίο χρηματοδοτήθηκε αργότερα από το ηλεκτρονικό συνοριακό ίδρυμα και τώρα αναπτύσσεται από τη μη κερδοσκοπική οργάνωση Electronic Frontier Foundation.

---

[92] 5.1,5.2,5.3 και 5.4 από: http://en.wikipedia.org/wiki/Anonymous_P2P

5.2 Επιχειρήματα υπέρ και κατά του ανώνυμου P2P δικτύου επικοινωνίας

5.2.1 Γενικά

Ενώ τα ανώνυμα P2P συστήματα μπορούν να υποστηρίξουν την προστασία της μη δημοφιλούς ομιλίας, μπορούν επίσης να προστατεύσουν τις παράνομες δραστηριότητες που δεν προστατεύονται βάση μερικών ελεύθερων λεκτικών νόμων, όπως η απάτη, δυσφήμηση, η ανταλλαγή της παράνομης πορνογραφίας, η αναρμόδια αντιγραφή οι εργασίες, ή ο προγραμματισμός των ποινικών δραστηριοτήτων. Οι κριτικοί των ανώνυμων P2P συστημάτων υποστηρίζουν ότι τα πλεονεκτήματα που προσφέρονται από τέτοια συστήματα δεν ξεπερνούν τα μειονεκτήματα, και ότι άλλα κανάλια επικοινωνίας είναι ήδη ικανοποιητικά για τη μη δημοφιλή ομιλία.

Μερικοί υπερασπιστές των ανώνυμων P2P συστημάτων θεωρούν ότι όλοι οι περιορισμοί στην ελεύθερη ομιλία εξυπηρετούν τα αυταρχικά ενδιαφέροντα. Άλλοι υποστηρίζουν ότι οι πληροφορίες οι ίδιες είναι ηθικά ουδέτερες, και ότι οι άνθρωποι είναι που ενεργούν επάνω στις πληροφορίες οι οποίες μπορούν να είναι καλές ή κακές. Οι αντιλήψεις για το καλό και το κακό μπορούν επίσης να αλλάξουν παραδείγματος χάριν, εάν τα ανώνυμα P2P δίκτυα είχαν υπάρξει στη δεκαετία του '50 ή τη δεκαετία του '60, θα είχαν στοχεύσει τις πληροφορίες μεταφοράς τα αστικά δικαιώματα ή τον αναρχισμό.

Τα ευπρόσιτα ανώνυμα P2P δίκτυα φαίνονται από μερικούς ως εκδημοκρατισμός της τεχνολογίας της κρυπτογράφησης, που δίνει τη γενική πρόσβαση του λαού στα ασφαλή κανάλια επικοινωνιών που χρησιμοποιήθηκαν ήδη από τις κυβερνήσεις. Οι υποστηρικτές αυτής της άποψης υποστηρίζουν ότι οι τεχνολογίες αντί-επιτήρησης βοηθούν να εξισώσουν τη δύναμη μεταξύ των κυβερνήσεων και των ανθρώπων τους, η οποία είναι ο πραγματικός λόγος για αυτές.. Ορισμένοι πιστεύουν ότι η παρακολούθηση του λαού βοηθά στις απειλές για τη "συναινετική άποψη" των καθιερωμένων αρχών ή απειλών στη συνοχή της δομικής ισχύος και του προνομίου.

5.2.2 Η ελευθερία του λόγου

Μερικοί υποστηρίζουν ότι η αληθινή ελευθερία λόγου, ειδικά στα αμφισβητούμενα θέματα, είναι δύσκολη ή αδύνατη εκτός αν τα άτομα μπορούν να μιλήσουν ανώνυμα. Αν η ανωνυμία δεν είναι δυνατή, θα μπορούσε κάποιος να υποβληθεί στις απειλές ή τα αντίποινα για την έκφραση μιας μη δημοφιλούς άποψης. Αυτό είναι ένας λόγος για τον οποίο υπάρχει η μυστική ψηφοφορία σε πολλές δημοκρατίες. Τις αμφισβητούμενες πληροφορίες που ένα συμβαλλόμενο μέρος θέλει να κρατήσει κρυμμένες, όπως οι λεπτομέρειες για τη δωροδοκία, δημοσιεύονται συχνά ή διαρρέουν ανώνυμα.

5.2.2.1 Ανώνυμος blogging

Ανώνυμο blogging είναι μια διαδεδομένη χρήση των ανώνυμων δικτύων. Ενώ το ανώνυμο blogging είναι δυνατό στο μη-ανώνυμο διαδίκτυο μέχρι ενός ορισμένου βαθμού, ένας προμηθευτής που φιλοξενεί το εν λόγω blog θα μπορούσε να υποχρεωθεί να αποκαλύψει την διεύθυνση IP του blogger. Τα ανώνυμα δίκτυα παρέχουν έναν καλύτερο βαθμό ανωνυμίας. Το Flogs σε ελεύθερο δίκτυο, Syndie I2P και Osiris sps είναι μερικά παραδείγματα των ανώνυμων blogging τεχνολογιών.

Ένα επιχείρημα για ανωνυμία είναι μια λεπτή φύση της κατάστασης εργασίας. Μερικές φορές ένας blogger που γράφει από κάτω το πραγματικό όνομα του/της αντιμετωπίζει μια επιλογή μεταξύ είτε της σιωπής είτε της πρόκλησης μιας ζημιάς σε αυτόν, τους συναδέλφους του είτε στην επιχείρηση που εργάζεται. Ο κίνδυνος δικών είναι ένας άλλος λόγος. Μερικά bloggers έχουν αντιμετωπίσει τις multi-million δίκες δολαρίων που αργότερα παραγράφηκαν εντελώς ενώ τα ανώνυμα bloggers παρέχουν την προστασία ενάντια σε τέτοιους κινδύνους.

5.2.2.2 Λογοκρισία μέσω των ονομάτων περιοχών Διαδικτύου

Στο μη-ανώνυμο διαδίκτυο, ένα όνομα περιοχών όπως " mysite.com" είναι ένα κλειδί στην πρόσβαση των πληροφοριών. Η λογοκρισία του ιστοχώρου Wikileaks δείχνει ότι τα ονόματα περιοχών είναι εξαιρετικά τρωτά στη λογοκρισία. Ορισμένα domain registrars έχουν αναστείλει ονόματα περιοχών ακόμη και την ελλείψει μιας δικαστικής απόφασης.

Για τους πελάτες που επλήγησαν, καθώς και το κλείδωμα του ονόματος τομέα είναι ένα πολύ μεγαλύτερο πρόβλημα από τον γραμματέα (registrar), που αρνείται να παράσχει μια υπηρεσία. Χαρακτηριστικά, ο γραμματέας κρατά τον ολικό έλεγχο, πέρα από τα εν λόγω ονόματα περιοχών. Στην περίπτωση ενός ευρωπαϊκού ταξιδιωτικού γραφείου, περισσότεροι από 80 ιστοχώροι του .com διακόπηκαν χωρίς οποιαδήποτε διαδικασία δικαστηρίων και κρατούνται από το γραμματέα από τότε. Το ταξιδιωτικό γραφείο έπρεπε να επανοικοδομήσει τις περιοχές κάτω από την κορυφαία περιοχή του .net αντ' αυτού.

Τα ανώνυμα δίκτυα, αφ' ενός, δεν στηρίζονται στα ονόματα των περιοχών (domain name registrars). Παραδείγματος χάριν, το ελεύθερο δίκτυο (freenet) είναι ανθεκτικό στην λογοκρισία και τα URLs είναι βασισμένα στο δημόσιο βασικό σύστημα της κρυπτογραφίας : μόνο ένα πρόσωπο που έχει το σωστό ιδιωτικό κλειδί είναι σε θέση να ενημερώσει το URL ή να το πάρει.

5.2.3 Έλεγχος online εντοπισμού

Το ανώνυμο P2P έχει αξία και στην κανονική καθημερινή επικοινωνία. Όταν η επικοινωνία είναι ανώνυμη, η απόφαση να αποκαλυφθούν οι ταυτότητες των επικοινωνούντων συμβαλλόμενων μερών έχει αφεθεί στα ενδιαφερόμενα μέρη και δεν είναι διαθέσιμη σε τρίτους. Συχνά δεν υπάρχει καμία ανάγκη ή επιθυμία από τα επικοινωνούντα συμβαλλόμενα μέρη να αποκαλύψουν τις ταυτότητές τους. Σαν θέμα προσωπικής ελευθερίας, πολλοί άνθρωποι δεν θέλουν τις διαδικασίες σε ισχύ, που εξ

ορισμού παρέχουν περιττά στοιχεία. Σε μερικές περιπτώσεις τέτοια στοιχεία θα μπορούσαν να συνταχθούν στα ιστορικά των δραστηριοτήτων τους.

Παραδείγματος χάριν, το τρέχον τηλεφωνικό σύστημα διαβιβάζει τις πληροφορίες μεταδίδει πληροφορίες από προεπιλογή του καλούντα. Εάν κάποιος καλεί για να βρει μια έρευνα για ένα προϊόν ή το χρόνο μιας ταινίας , το πρόσωπο που καλείται έχει ένα αρχείο με τον αριθμού τηλεφώνου που κάλεσε, και μπορεί να λάβει το όνομα, τη διεύθυνση και άλλες πληροφορίες για τον καλούντα. Εάν ήταν να περπατήσει κάποιος σε ένα κατάστημα και να γίνει μια παρόμοια έρευνα, όλη αυτή η προσωπική πληροφορία δεν θα περιλαμβανόταν. Το ανώνυμο P2P απλά επιτρέπει για αυτήν την υπάρχουσα δραστηριότητα «meatspace» να εμφανιστεί ένα δίκτυο επικοινωνιών.

5.2.4 Αποτελέσματα της επιτήρησης στη νόμιμη δραστηριότητα

Η online επιτήρηση, όπως η καταγραφή και διατήρηση των λεπτομερειών του Ιστού και της κυκλοφορίας ηλεκτρονικού ταχυδρομείου, μπορεί να έχει αποτελέσματα στις νόμιμες δραστηριότητες. Οι άνθρωποι μπορούν να αποτραπούν από την πρόσβαση ή την μεταβίβαση των νομικών πληροφοριών επειδή ξέρουν για την πιθανή επιτήρηση και πιστεύουν ότι αυτή η ανακοίνωση μπορεί να θεωρηθεί ύποπτη. Σύμφωνα με το καθηγητή Νομικής Ντάνιελ J. Solove, τέτοια αποτελέσματα "βλάπτουν την κοινωνία, διότι, μεταξύ άλλων, θα μειώσουν το φάσμα των απόψεων που εκφράζετε και τον βαθμό ελευθερίας άσκησης της πολιτικής δραστηριότητας.".

5.2.5 Ανώνυμα online χρήματα

Με τα ανώνυμα χρήματα, είναι δυνατό να τακτοποιηθούν οι ανώνυμες αγορές όπου μπορεί κανείς να αγοράζει και να πουλάει τα πάντα ανώνυμα. Τα ανώνυμα χρήματα θα μπορούσαν να χρησιμοποιηθούν για να αποφευχθεί η είσπραξη των φόρων. Εντούτοις, οποιαδήποτε μεταφορά των φυσικών αγαθών μεταξύ δύο συμβαλλόμενων μερών θα μπορούσε να θέσει σε κίνδυνο την ανωνυμία.

Μερικοί υποστηρίζουν ότι τα μετρητά παρέχουν ένα παρόμοιο είδος ανωνυμίας, και ότι οι υφιστάμενοι νόμοι είναι επαρκείς να καταπολεμήσουν τα εγκλήματα όπως τη φοροδιαφυγή που προκύπτει από τη χρήση των ανώνυμων μετρητών, είτε on-line είτε off-line.

5.3 Λειτουργία του ανώνυμου P2P

5.3.1 Ανωνυμία και ψευδωνυμία

Μερικά από τα δίκτυα που κοινός ονομάζονται "ανώνυμα P2P" είναι πραγματικά ανώνυμα, υπό την έννοια ότι οι κόμβοι δικτύων δεν φέρνουν κανένα προσδιοριστικό. Άλλα είναι πραγματικά ψευδώνυμα. Αντί να προσδιορίζονται από τις διευθύνσεις IP,

οι κόμβοι προσδιορίζονται από τα ψευδώνυμα όπως τα κρυπτογραφικά κλειδιά. Παραδείγματος χάριν, κάθε κόμβος στο MUTE δίκτυο έχει μια διεύθυνση επικαλύψεων που προέρχεται από το δημόσιο κλειδί της. Αυτή η διεύθυνση επικαλύψεων λειτουργεί ως ψευδώνυμο για τον κόμβο, επιτρέποντας στα μηνύματα να απευθύνονται στη διεύθυνση αυτή. Στα Freenet δίκτυα τα μηνύματα καθοδηγούνται χρησιμοποιώντας τα κλειδιά που προσδιορίζουν τα συγκεκριμένα κομμάτια των στοιχείων και όχι τους συγκεκριμένους κόμβους. Οι κόμβοι από μόνοι τους είναι ανώνυμοι.

Ο όρος ανώνυμος χρησιμοποιείται για την περιγραφή των δύο ειδών υπηρεσιών δικτύου επειδή είναι δύσκολο - εάν όχι αδύνατο - να προσδιοριστεί εάν ένας κόμβος που στέλνει ένα μήνυμα, δημιούργησε το μήνυμα αυτό ή τον διαβιβάζει για λογαριασμό ενός άλλου κόμβου. Κάθε κόμβος σε ένα ανώνυμο P2P δίκτυο ενεργεί ως καθολικός αποστολέας και καθολικός δέκτης για να διατηρήσει την ανωνυμία του. Εάν ένας κόμβος ήταν μόνο ένας δέκτης και δεν έστειλε, τότε οι γειτονικοί κόμβοι θα πρέπει να γνωρίζουν ότι οι πληροφορίες που ζητούσε ήταν μόνο για τον εαυτό της, αφαιρώντας κάθε εύλογη δυνατότητα άρνησης ότι ήταν ο παραλήπτης (και καταναλωτής) των πληροφοριών. Κατά συνέπεια, προκειμένου να παραμείνουν ανώνυμοι οι κόμβοι αυτοί, θα πρέπει να φέρουν άλλες πληροφορίες σχετικά με το δίκτυο.

5.3.2 Spam και επιθέσεις DoS σε ανώνυμα δίκτυα

Αρχικά, τα ανώνυμα δίκτυα χρησιμοποιήθηκαν από τις μικρές και φιλικές κοινότητες των προγραμματιστών. Δεδομένου ότι το ενδιαφέρον για ανώνυμο P2P αυξήθηκε και η βάση χρηστών επίσης αυξήθηκε, οι κακόβουλοι χρήστες εμφανίστηκαν αναπόφευκτα και δοκίμασαν διάφορες επιθέσεις. Αυτό είναι παρόμοιο με το Διαδίκτυο, όπου έχει ευρεία χρήση, ακολουθούμενη από τα κύματα του spam και της διανεμημένης άρνησης παροχής υπηρεσιών.

Τέτοιες επιθέσεις μπορούν να απαιτήσουν διάφορες λύσεις στα ανώνυμα δίκτυα. Παραδείγματος χάριν, η καταχώρηση στη μαύρη λίστα των δημιουργών των διευθύνσεων των δικτύων, δεν λειτουργεί επειδή τα ανώνυμα δίκτυα κρύβουν αυτές τις πληροφορίες. Αυτά τα δίκτυα είναι πιο τρωτά στις επιθέσεις DOS που οφείλονται επίσης στο μικρότερο εύρος ζώνης,

5.4 Opennet και darknet τύποι δικτύων

Όπως τα συμβατικά P2P δίκτυα, τα ανώνυμα P2P δίκτυα μπορούν να εφαρμόσουν είτε opennet είτε darknet (συχνά ονομασμένος το φίλο σε φίλο) τύπους δικτύων. Αυτό περιγράφει πώς ένας κόμβος στο δίκτυο επιλέγει τους όμοιους κόμβους:

- Στο δίκτυο opennet, οι όμοιοι κόμβοι ανακαλύπτονται αυτόματα. Δεν υπάρχει καμία διαμόρφωση που απαιτείται, αλλά διατίθεται λίγος έλεγχος στους ομότιμους κόμβους
- Σε ένα δίκτυο darknet, οι χρήστες εγκαθιστούν με το χέρι τις συνδέσεις με τους κόμβους που οργανώνονται από τους ανθρώπους που ξέρουν. Το darknet

χρειάζεται χαρακτηριστικά περισσότερη προσπάθεια στην οργάνωση αλλά μόνο ένας κόμβος έχει εμπιστευθεί τους κόμβους.

Μερικά δίκτυα όπως το Freenet, υποστηρίζουν και τους δύο τύπους δικτύων ταυτόχρονα (ένας κόμβος μπορεί να έχει 5 με το χέρι προστιθέμενους darknet όμοιους κόμβους και 5 αυτόματα επιλεγμένους opennet).

Σε ένα δίκτυο F2F (friend-to-friend), οι χρήστες κάνουν μόνο άμεσες συνδέσεις με τους ανθρώπους που ξέρουν. Πολλά F2F δίκτυα υποστηρίζουν την έμμεση ανώνυμη ή ψευδόνυμη επικοινωνία μεταξύ των χρηστών που δεν ξέρουν ή δεν εμπιστεύονται ο ένας τον άλλον. Παραδείγματος χάριν, ένας κόμβος σε ένα δίκτυο F2F μπορεί αυτόματα να διαβιβάσει ένα αρχείο (ή ένα αίτημα για ένα αρχείο) ανώνυμα μεταξύ δύο φίλων, χωρίς να μεταφέρει σε κανέναν από τους δύο το όνομα ή την διεύθυνση IP του άλλου. Αυτοί οι φίλοι μπορούν στη συνέχεια να διαβιβάσουν το ίδιο αρχείο (ή το αίτημα) στους φίλους τους, και ούτω καθεξής. Οι χρήστες σε ένα δίκτυο F2F δεν μπορούν να ανακαλύψουν ποιος άλλος συμμετέχει πέρα από τον κύκλο των φίλων τους, έτσι τα F2F δίκτυα μπορούν να αυξηθούν στο μέγεθος χωρίς να θέτει σε κίνδυνο τους χρήστες της ανωνυμίας.

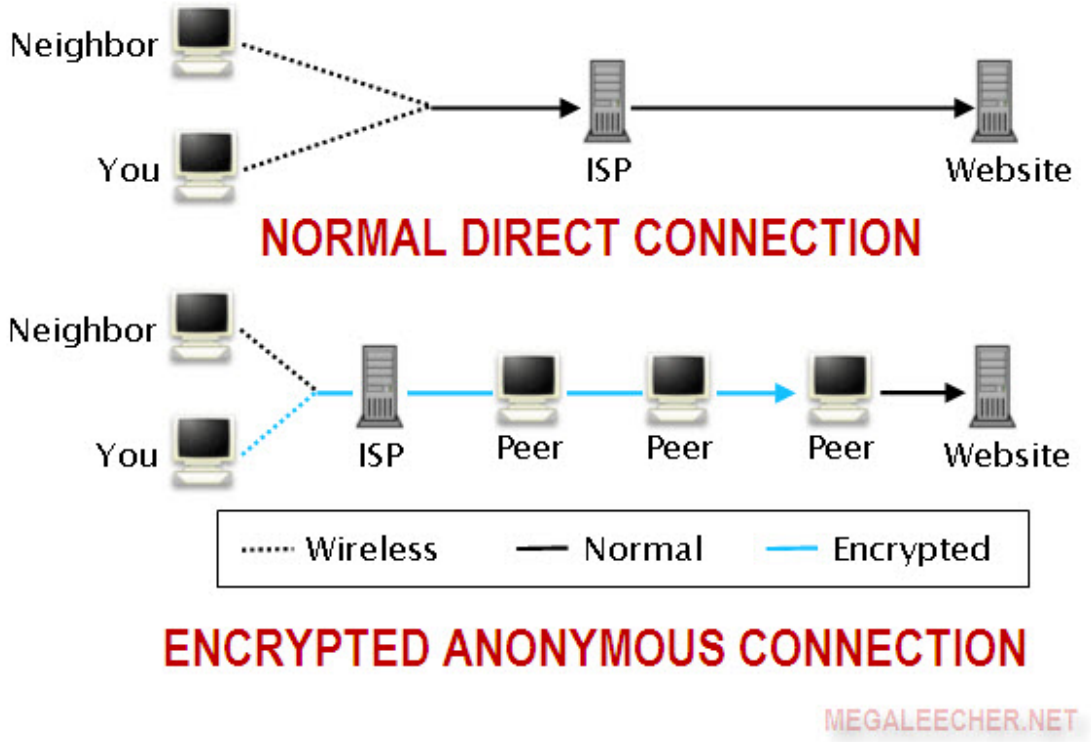
5.5 Κατάλογος ανώνυμων P2P δικτύων

Παρακάτω ακολουθούν τα χαρακτηρίστηκα μερικών εφαρμογών P2P δικτύων. Οι εφαρμογές είναι οι εξής :

- Bitblinder
- Entropy
- Freenet
- GNUnet
- I2P
- Phex
- Marabunta
- Nodezilla
- OFF System
- Omemo
- Osiris sps
- Perfect Dark
- StealthNet
- StegoShare Network
- Mute
- Ants

5.5.1 Bitblinder

Το Bitblinder είναι ένα αποκεντρωμένο P2P softwarer ανωνυμίας που περιλαμβάνει το Tor αλλά με αυξανόμενη ταχύτητα με την κρυπτογράφηση και επιτρέπει P2P browsing, email, voip, messenging.[93] Το Bitblinder είναι ένα πρόγραμμα λογισμικού ανοιχτού κώδικα που επιτρέπει στους χρήστες να μοιράζονται το εύρος ζώνης και την IP να κατεβάζουν ανώνυμα torrents και να κάνουν ανώνυμα περιήγηση στο Διαδίκτυο. Το λογισμικό είναι βασισμένο στις αρχές που το Tor χρησιμοποιήθηκε για να δημιουργήσει την ανωνυμία αλλά σχεδιάστηκε για να είναι γρηγορότερο και να ενθαρρύνει το μοίρασμα αρχείων, εκτός από την ανώνυμη περιήγηση. Σήμερα έρχεται με μια ανώνυμη μηχανή αναζήτησης βασισμένη σε Firefox και έναν ανώνυμο bit torrent client που βασίζονται στο BitTornado.



Εικόνα 61 Συνδεσμολογία

5.5.2 Entropy

Η Entropy είναι ένα " Freenet alternative" δίκτυο το οποίο διακοπεί στις 9 Ιουλίου 2004, λόγω της αβεβαιότητας σχετικά με την ασφάλεια της McEliece cryptosystem. [94] Η Entropy είναι ένα αποκεντρωμένο, P2P δίκτυο επικοινωνίας με σκοπό να είναι ανθεκτική στη λογοκρισία, σαν ελεύθερο δίκτυο. Η εντροπία είναι μια ανώνυμη βιβλιοθήκη δεδομένων που γράφεται στη γλώσσα προγραμματισμού C. Συγκεντρώνει το διάστημα εύρους ζώνης και αποθήκευσης των υπολογιστών μελών για να

[93] http://en.wikipedia.org/wiki/Bitblinder
[94] http://en.wikipedia.org/wiki/Anonymous_P2P&ei

επιτρέπει στους χρήστες να δημοσιεύουν ανώνυμα ή να ανακτήσουν τις πληροφορίες όλων των ειδών.

Η Entropy έχει ως σκοπό να είναι συμβατή με το παρόμοιο Freenet σύστημα δικτύου. Ωστόσο, σήμερα η Entropy και οι βιβλιοθήκες δεδομένων freenet δεν είναι συμβατές η μια με την άλλη και επομένως δεν μοιράζονται τα στοιχεία. Η Entropy χαρακτηρίζει επίσης μια διεπαφή ειδήσεων, για την ανάγνωση και την ταχυδρόμηση στις πιο τελευταίες επιτροπές frost message boards μηνυμάτων από μέσα από τον πελάτη.

5.5.3 Freenet

Το freenet είναι μια αποκεντρωμένη, ανθεκτική διανεμημένη βιβλιοθήκη δεδομένων που σχεδιάστηκε αρχικά από τον Ian Clarke. Στόχος του είναι η παροχή ελευθερίας λόγου μέσω ενός P2P δικτύου με ισχυρή προστασία της ανωνυμίας. Το Freenet. λειτουργεί με τη συγκέντρωση του διαστήματος του εύρους ζώνης και της αποθήκευσης των υπολογιστών μελών για να επιτρέπει στους χρήστες να δημοσιεύουν ανώνυμα ή να ανακτούν διάφορα είδη πληροφοριών. Από την πλευρά των χρηστών, μπορεί να θεωρηθεί απλώς ως μια μεγάλη συσκευή αποθήκευσης.

Το δίκτυο αποτελείται από έναν αριθμό κόμβων που μεταφέρουν μηνύματα μεταξύ τους. Συνήθως, ένας κεντρικός (host) υπολογιστής στο δίκτυο τρέχει το λογισμικό που ενεργεί ως κόμβος, και συνδέεται με άλλους κεντρικούς υπολογιστές που τρέχουν το ίδιο λογισμικό για να διαμορφώσουν ένα μεγάλο διανεμημένο δίκτυο των όμοιων κόμβων. Μερικοί κόμβοι είναι τελικοί κόμβοι χρηστών, από τους οποίους ζητούνται τα έγγραφα και παρουσιάζονται στους ανθρώπινους χρήστες. Άλλοι κόμβοι χρησιμεύουν μόνο για να δρομολογήσουν τα δεδομένα.

Όλοι οι κόμβοι επικοινωνούν ο ένας με τον άλλον όμοια - δεν υπάρχει κανένας client που να επικοινωνεί αποκλειστικά με έναν server. Δεν είναι δυνατό για έναν κόμβο να εκτιμήσει έναν άλλο κόμβο, εκτός από την ικανότητά του να παρεμβάλει και να προσκομίσει τα στοιχεία που συνδέονται με ένα κλειδί. Αυτό είναι αντίθετο από τα περισσότερα άλλα P2P δίκτυα όπου οι διοικητές κόμβων μπορούν να υιοθετήσουν μια αναλογία συστημάτων, όπου οι χρήστες πρέπει να μοιραστούν ένα συγκεκριμένο ποσό του περιεχομένου προτού να μπορέσουν να κάνουν download.

Το freenet μπορεί επίσης να θεωρηθεί σαν ένα μικρό παγκόσμιο δίκτυο. Το πρωτόκολλο αυτού του δικτύου προορίζεται για να χρησιμοποιηθεί σε ένα δίκτυο της σύνθετης τοπολογίας, όπως το Διαδίκτυο (πρωτόκολλο Διαδικτύου). Κάθε κόμβος ξέρει μόνο για κάποιο αριθμό άλλων κόμβων ότι μπορεί να φθάσει άμεσα, αλλά οποιοσδήποτε κόμβος μπορεί να είναι γείτονας σε οποιουσδήποτε άλλους. Καμία ιεραρχία ή άλλη δομή δεν προορίζεται.

Κάθε μήνυμα καθοδηγείται μέσω του δικτύου με τη διάβαση από το γείτονα στο γείτονα έως ότου φτάσει στον προορισμό του. Καθώς κάθε κόμβος περνά ένα μήνυμα σε έναν γείτονα, δεν ξέρει ή δεν τον ενδιαφέρει εάν ο γείτονας θα διαβιβάσει το μήνυμα σε έναν άλλο κόμβο, ή είναι ο τελικός προορισμός ή η αρχική πηγή του μηνύματος. Αυτό αποσκοπεί στην προστασία της ανωνυμίας των χρηστών και των εκδοτών. Κάθε κόμβος διατηρεί ένα χώρο αποθήκευσης δεδομένων που περιέχει τα έγγραφα που συνδέονται με τα κλειδιά,, και ένα πίνακα δρομολόγησης κόμβων

σύνδεσης με τα αρχεία της απόδοσής τους στην ανάκτηση των διαφορετικών κλειδιών.

5.5.4 GNUnet

Το GNUnet είναι ένα πλαίσιο ελεύθερου λογισμικού για την αποκεντρωμένη, P2P δικτύωση. [95] Το πλαίσιο προσφέρει κρυπτογράφηση συνδέσεων και όμοια κατανομή των πόρων. Ο αρχικός κώδικας είναι γραμμένος στη C, αλλά υπάρχει μια προσπάθεια να παραχθεί μια συμβατή έκδοση γραμμένη σε Java. Το GNUnet σήμερα τρέχει σε Linux, BSD, Mac OS X, Solaris και Windows.

Η κύρια εφαρμογή είναι ανώνυμη, ανθεκτική στην λογοκρισία με κοινή χρήση αρχείων, επιτρέποντας στους χρήστες να δημοσιεύουν ανώνυμα ή να ανακτούν τις πληροφορίες όλων των ειδών. Η κοινή χρήση αρχείων χρησιμοποιεί το πρωτόκολλο GNUnet's ανωνυμίας για τη δρομολόγηση των ερωτήσεων και των απαντήσεων. Τα μηνύματα ερώτησης που προωθούνται χρησιμοποιούνται στην αναζήτηση του περιεχομένου και του όγκου των δεδομένων. Ανάλογα με το φορτίο του κόμβου αποστολής, τα μηνύματα διαβιβάζονται σε 0 ή περισσότερους κόμβους. Όταν ένας κόμβος είναι υπό πίεση 'πετάει' τα αιτήματα από τους γειτονικούς, που έχουν τη χαμηλότερη εσωτερική αξία εμπιστοσύνης.

Το GNUnet προσφέρει μια επιλογή " F2F τοπολογία " για να επιτρέπει τις συνδέσεις μόνο στους έμπιστους φίλους. Στην συνέχεια οι φίλοι των φίλων σας (και ούτω καθεξής) μπορούν έμμεσα να ανταλλάξουν τα αρχεία με τον υπολογιστή σας, χωρίς να χρησιμοποιούν την IP τους διεύθυνση. Το GNUnet χρησιμοποιεί Uniform Resource Identifiers (URI) τα οποία όμως δεν εγκρίνονται από Java. Ο URI συμβολισμός έχει αλλάξει μαζί με τις νέες εκδόσεις GNUnet. Η ακόλουθη σημείωση χρησιμοποιείται από την έκδοση 0.7.0. Το GNUnet URIs αποτελείται από δύο σημαντικά μέρη: την ενότητα και το συγκεκριμένο προσδιοριστικό ενότητας. Ένα GNUnet URI είναι της μορφής : gnunet://module/identifier όπου η ενότητα είναι το όνομα και το προσδιοριστικό ενότητας είναι μια συγκεκριμένη σειρά ενότητας.

Η κοινή χρήση αρχείων με GNUnet είναι κωδικοποιημένη με ECRS (μια κωδικοποίηση που είναι ανθεκτική στην λογοκρισία). Το προσδιοριστικό της ενότητας ECRS αποτελείται είτε από chk ή sks ή ksk ή loc που ακολουθούνται από μια κάθετο και μια συγκεκριμένη αξία κατηγορίας. Το chk προσδιορίζει αρχεία συνήθως ως εξής: gnunet: //ecrs/chk/ [hash αρχείο, χρησιμοποιώντας 0-9A-V]. [ερώτημα hash, με 0-9A-V]. [μέγεθος αρχείου σε bytes].

Το sks προσδιορίζει τα αρχεία μέσα στα namespaces, συνήθως ως εξής :
gnunet: //ecrs/sks/NAMESPACE/IDENTIFIER. Το ksk προσδιορίζει τις ερωτήσεις αναζήτησης, συνήθως ως εξής :
gnunet: //ecrs/ksk/KEYWORD [+KEYWORD] *
τα loc προσδιορίζουν ένα στοιχείο όσον αφορά μια συγκεκριμένη μηχανή, συνήθως ως εξής : gnunet: //ecrs/loc/PEER/QUERY.TYPE.KEY.SIZE.

---

[95] http://en.wikipedia.org/wiki/GNUnet

5.5.5 I2P

Το I2P είναι ένα ελεύθερου και ανοικτού κώδικα σχέδιο οικοδόμησης ενός ανώνυμου δικτύου (ή, για την ακρίβεια, ένα ψευδώνυμο δίκτυο επικαλύψεων).[96] Το δίκτυο είναι ένα απλό στρώμα το οποίο οι εφαρμογές μπορούν να χρησιμοποιήσουν ανώνυμα και να στείλουν με ασφάλεια τα μηνύματα η μια στην άλλη. Οι πιθανές χρήσεις περιλαμβάνουν το ανώνυμο surfing, chatting, και μεταφορές αρχείων.

Το I2P σήμερα είναι ένα βήτα λογισμικό. Αυτό σημαίνει ότι έχει περάσει από το πρώτο δοκιμαστικό στάδιο ανάπτυξης και έχει απαλλαγεί από τους χρήστες για τις δοκιμές του λογισμικού πριν την επίσημη κυκλοφορία. Οι υπεύθυνοι για την ανάπτυξη υπογραμμίζουν ότι ενδέχεται να υπάρχουν σφάλματα στο λογισμικό και ότι έχει υπάρξει ανεπαρκής αξιολόγηση από τους ειδικούς μέχρι σήμερα. Εντούτοις, θεωρούν ότι ο κώδικας είναι τώρα αρκετά σταθερός και καλά ανεπτυγμένος, και η έκθεση μπορεί να βοηθήσει περισσότερο στην ανάπτυξή του. Οι άνθρωποι το χρησιμοποιούν συχνά για ινκόγκνιτο περιήγηση.

Το ίδιο το δίκτυο είναι αυστηρά βασισμένο στα μηνύματα (όπως την IP), αλλά υπάρχει μια βιβλιοθήκη διαθέσιμη για να επιτρέψει την αξιόπιστη ροή επικοινωνίας πάνω σε αυτό. Όλη η επικοινωνία γίνετε με end to end κρυπτογράφιση, έτσι ώστε ούτε ο αποστολέας ούτε ο παραλήπτης ενός μηνύματος να αποκαλύπτει τη διεύθυνση IP του στην άλλη πλευρά ή σε τρίτους παρατηρητές.

Αν και πολλοί από τους υπεύθυνους για την ανάπτυξη συμμετείχαν στην ανάπτυξη του I2P και freenet, υπάρχουν σημαντικές διαφορές μεταξύ των σχεδίων και των εννοιών τους. Το freenet είναι μια βιβλιοθήκη δεδομένων ανθεκτική στην λογοκρισία. Το I2P είναι ένα ανώνυμο P2P διανεμημένο στρώμα επικοινωνίας με σκοπό να ανατρέξουν σε οποιαδήποτε παραδοσιακή υπηρεσία Διαδικτύου (π.χ. USENET, ηλεκτρονικό ταχυδρομείο, IRC, μοίρασμα αρχείων, Web hosting και HTTP, Telnet), καθώς επίσης και παραδοσιακότερες διανεμημένες εφαρμογές (π.χ. ένα διανεμημένο κατάστημα στοιχείων, ένα web proxy Squid cache, και DNS).

Δεδομένου ότι το I2P είναι ένα ανώνυμο στρώμα δικτύου, σχεδιάζεται έτσι ώστε άλλα προγράμματα λογισμικού να μπορούν να το χρησιμοποιήσουν για την ανώνυμη επικοινωνία, το λεγόμενο επίπεδο εφαρμογών. Έτσι υπάρχει μια ποικιλία εργαλείων που διατίθενται σήμερα για I2P ή που βρίσκονται σε φάση ανάπτυξης.

I2PTunnel

Το I2PTunnel είναι μια εφαρμογή που ενσωματώνεται μέσο του I2P επιτρέποντας τις αυθαίρετες εφαρμογές TCP/IP να επικοινωνούν μέσω I2P με τη δημιουργία "σήραγγας" (tunnels).

---

[96] http://en.wikipedia.org/wiki/I2P

SAM

Το SAM είναι ένα πρωτόκολλο που επιτρέπει σε μια εφαρμογή πελατών (client) που γράφεται σε οποιαδήποτε γλώσσα να επικοινωνήσουν πέρα από τη χρήση του I2P, με τη χρήση μιας υποδοχής η οποία βασίζετε στον I2P δρομολογητή.

BitTorrent

Διάφορα προγράμματα παρέχουν τη λειτουργία BitTorrent για χρήση μέσα στο I2P δίκτυο. Κάθε ένας στηρίζεται στο χρήστη που είναι σε θέση να έχει πρόσβαση στο I2P δίκτυο με μια μηχανή αναζήτησης Ιστού για να κατεβάσει τα αρχεία .

eDonkey iMule

Φτιάχτηκε για ανώνυμη χρήση αρχείων (File sharing) με τη χρήση I2P δικτύου. Λόγω του συμπεριλαμβανόμενου δρομολογητή από την έκδοση 1.2.3 κανένα άλλο λογισμικό δεν απαιτείται για να συνδεθεί με το I2P-δίκτυο. Διαφορετικά, εάν θέλετε να χρησιμοποιήσετε όλα τα άλλα χαρακτηριστικά γνωρίσματα I2P (BitTorrent, Gnutella, ανώνυμοι ηλεκτρονικά ταχυδρομεία και ιστοχώροι…) πρέπει να εγκαταστήσετε το συνολικό πακέτο.

Susimail

Το I2P έχει μια ελεύθερη ψευδώνυμη υπηρεσία αποστολής ηλεκτρονικών μηνυμάτων, η οποία εκτελείτε από ένα άτομο αποκαλούμενο ' Postman'. Το Susimail δημιουργήθηκε για να εξετάσει τις ανησυχίες μυστικότητας αυτών των διακομιστών χρησιμοποιώντας άμεσα email με τη χρήση παραδοσιακών πελατών,, όπως η διαρροή του user' s hostname ενώ επικοινωνεί με τον κεντρικό υπολογιστή SMTP. Το Susimail είναι ένα Web-based email client που προορίζετε κυρίως για χρήση Postman's mail servers, που έχουν σχεδιαστεί με την ασφάλεια και την ανωνυμία τους. Σήμερα περιλαμβάνεται στην προεπιλεγμένη διανομή I2P, και μπορεί να προσεγγιστεί μέσω του I2P δρομολογητή σας . (Σημειώστε ότι αυτό χρησιμοποιείται μόνο για να διαβάσει και να στείλει το ηλεκτρονικό ταχυδρομείο, για να μην δημιουργήσει ή να μην διαχειριστεί τον απολογισμό του mail.I2P σας. Τα τελευταία πρέπει να γίνουν σε www.mail.I2P).

Syndie

Το Syndie είναι μια blogging εφαρμογή για I2P, το οποίο είναι επίσης χρησιμοποιήσιμο μέσω του δικτύου TOR.

5.5.6. Phex

Το Phex είναι ένα peer-to-peer file sharing client για το δίκτυο Gnutella. [97]To Phex είναι βασισμένο στην πλατφόρμα της Java και υποστηρίζει από J2SE 5.0 και έπειτα. Το Phex είναι ένα ελεύθερο λογισμικό.

---

[97] http://en.wikipedia.org/wiki/I2phex#Anonymous_Phex

Το Phex υποστηρίζει τα περισσότερα από τα τελευταία στοιχεία του δικτύου Gnutella. Επιπλέον επιτρέπει τη δημιουργία των ιδιωτικών δικτύων μέσω του Διαδικτύου, έχει ένα ισχυρό φίλτρο αποτελέσματος αναζήτησης, παρουσιάζει σημαίες χωρών πελατών, και μπορεί να εξαγάγει τον κατάλογο κοινών αρχείων στα πολλαπλάσια σχήματα, μερικά από τα οποία μπορούν επίσης να διαβαστούν έξω και να ληφθούν άμεσα από ένα άλλο Phex. Η έκδοση 3.2.0.102 υποστηρίζει επίσης Tiger Tree hashes για uploads και downloads, παρέχοντας πλήρη προστασία έναντι μολυσμένων λήψεων. Μαζί με το Swarming, το μερικό μοίρασμα αρχείων και το Download πλέγμα που κάνει, καθιστά τις λήψεις τόσο αποτελεσματικές και ασφαλή όσο με το BitTorrent downloads.

Από το 2006, μια ανώνυμη έκδοση Phex είναι διαθέσιμη, το I2Phex, το οποίο χρησιμοποιεί το I2P δίκτυο για να κρύψει τη διεύθυνση IP των χρηστών αυτού του Gnutella client. Ο μελλοντικός χάρτης (roadmap) πρόκειται να ενσωματώσει τον κώδικα I2Phex σε μια από τις επόμενες εκδόσεις Phex.

Αντί να χρησιμοποιηθεί το δημόσιο δίκτυο IP, το I2Phex χρησιμοποιεί τις κρυπτογραφημένες σήραγγες του I2P δικτύου (μυστικότητας/κρυπτογράφησης). Η κυκλοφορία αναμιγνύεται με άλλη κυκλοφορία δικτύων μέσω ενός συστήματος δρομολόγησης garlic routing, που καθιστά δύσκολο για τους εξωτερικούς παρατηρητές να προσδιορίσουν τους δημιουργούς ή τους παραλήπτες ενός αρχείου μέσω της ανάλυσης κυκλοφορίας.

Τα ανώνυμα δίκτυα έχουν αμελήσει να φιλοξενήσουν πρωτόκολλα για την κοινή χρήση αρχείων λόγω λάθους εκτίμησης του εύρους ζώνης. Συχνά μόνο η αναζήτηση (ή η ακολούθηση για BitTorrent) υποστηρίζεται. Οι κόμβοι μέσα στο σύστημα δρομολόγησης σκόρδου (garlic routing) θα μπορούσαν να αρνηθούν να καθοδηγήσουν την κυκλοφορία των κοινών αρχείων. Αυτό καθιστά τις εισερχόμενες και εξερχόμενες συνδέσεις ευκολότερο να εντοπίσουν. Η εξερχόμενο κίνηση γίνετε χωρίς κρυπτογράφηση, έτσι όταν συνδεθεί με τον εισερχόμενο κόμβο θα σπάσει η ανωνυμία του.

Το LimeWire, FrostWire, το gtk-gnutella, και Phex όλα υποστηρίζουν τη χρήση TLS για να κρυπτογραφήσουν την κυκλοφορία μεταξύ των κόμβων. Το TLS δεν είναι ανώνυμο όπως το I2P, εντούτοις, αυτό αποτρέπει τον ISPs από το φιλτράρισμα Gnutella του περιεχομένου και το καθιστά πιο δύσκολο στην ανίχνευση κίνησης.

5.5.7 Marabunta

Το Marabunta είναι μια πλήρως διανεμημένη εφαρμογή λογισμικού για ανώνυμο P2P. Ο κύριος στόχος του είναι η καταπολέμηση της λογοκρισίας στο internet και η διασφάλιση της ελευθερίας του λόγου. Είναι μια P2P πλατφόρμα για την ανταλλαγή πληροφοριών μεταξύ των κόμβων με έναν ανώνυμο τρόπο, βασισμένο σε διάφορους αλγορίθμους επικοινωνίας αποκαλούμενους " Order and Chaos ", ο όποιος μπορεί να βρεθεί σε μαζικές κοινωνικές οργανώσεις, όπως ant colonies.

Το πρόγραμμα ιδρύθηκε στο πανεπιστήμιο Σαραγόσα, της Ισπανίας , αναπτύχθηκε και προωθήθηκε από τους σπουδαστές της υπολογιστικής μηχανικής, αν και οι ομάδες και οι χρήστες ανάπτυξης από πολλές διαφορετικές θέσεις έχουν παρουσιάσει ενδιαφέρον, ίσως προσελκύονται από τους ιδεολογικούς στόχους του προγράμματος.. Το λογισμικό είναι διαθέσιμο μόνο στα ισπανικά, αλλά η ιστοσελίδα είναι επίσης διαθέσιμα στην αγγλική γλώσσα. Το Marabunta χρησιμοποιεί το Qt γραφικό κουτί εργαλείων widget, επιτρέποντας σε το για να χρησιμοποιηθεί και σε Linux και στο Microsoft Windows.

Υπάρχουν πολλές πιθανές υπηρεσίες που μπορούν να τρέχουν πάνω από Marabunta. Η ανταλλαγή μηνυμάτων κειμένων είναι η πρώτη υπηρεσία. Θα μπορούσε να ληφθεί ως πλατφόρμα για τη διανομή τηλεγραφημάτων, όπου κάθε υπολογιστής στις καθαρές εργασίες λειτουργεί ως οικοδεσπότης και ως κεντρικός υπολογιστής (server). Όταν λειτουργεί σαν οικοδεσπότης τα μηνύματα στέλνονται, οι ενεργοί κόμβοι επιδιώκονται, κ.λπ.. Όταν λειτουργεί σαν κεντρικός υπολογιστής : Τα μηνύματα και τα αιτήματα κειμένων για την αύξηση της συνδετικότητας μεταξύ των κόμβων καθοδηγούνται στο δίκτυο χρησιμοποιώντας μια ραδιοφωνική μετάδοση διαβιβάζοντας τη μέθοδο.

Υπάρχουν τέσσερις κατάλογοι διανομής μηνυμάτων, έτσι οι δέκτες λαμβάνουν μόνο τα μηνύματα που στέλνονται στον κατάλογο για τον οποίο ενδιαφέρονται: Γενικά, Τεχνολογία, Φιλοσοφία και Πολιτική.

Όλη η παραγόμενη κυκλοφορία χρησιμοποιεί τα πρωτόκολλα UDP/IP. Η αποφυγή της καθιέρωσης συνδέσεων μεταξύ των κόμβων αφήνει περισσότερη κυκλοφοριακή ροή στο δίκτυο και ο λειτουργικός πλεονασμός κάθε κόμβου μπορεί να χρησιμοποιηθεί. Επιπλέον, το πρωτόκολλο UDP θα μπορούσε να θεωρηθεί σαν τρόπος αύξησης την ανωνυμία στο δίχτυ επειδή δεν υπάρχει καμία ανάγκη να επικυρωθούν οι οικοδεσπότες πηγής για να λάβει ένα διάγραμμα δεδομένων (datagram).

5.5.8 Nodezilla

Το Nodezilla είναι ένα P2P δίκτυο που είναι γραμμένο σε C++ και Java.[98] Προσπαθεί να παρέχει ανωνυμία. Τεχνικά, το Nodezilla είναι ένα εξασφαλισμένο, διανεμημένο και ανεκτικό στα σφάλματα, σύστημα δρομολόγησης. Ο κύριος σκοπός του είναι να χρησιμεύσει ως μια σύνδεση για τις διανεμημένες υπηρεσίες που χτίζονται πάνω από σε αυτό (όπως chat, efficient video multicasting streaming, File Sharing, secured file store).

Το Nodezilla παρέχει χαρακτηριστικά γνωρίσματα. Οποιοσδήποτε κεντρικός υπολογιστής μπορεί να δημιουργήσει ένα τοπικό αντίγραφο οποιουδήποτε αντικειμένου στοιχείων. Αυτά τα τοπικά αντίγραφα παρέχουν γρηγορότερη πρόσβαση και την ευρωστία στα χωρίσματα δικτύων. Μειώνουν επίσης τη συμφόρηση δικτύων με τον εντοπισμό πρόσβασης της κυκλοφορίας.

---

[98] http://en.wikipedia.org/wiki/Nodezilla

Υποτίθεται ότι οποιοσδήποτε κεντρικός υπολογιστής στην υποδομή μπορεί να συντρίψει, να διαρρεύσει τις πληροφορίες, ή να γίνει συμβιβασμένος, επομένως προκειμένου να εξασφαλίσει προστασία δεδομένων, χρησιμοποιούνται ο πλεονασμός και η κρυπτογράφηση TLS. Δεδομένου ότι οι υπεύθυνοι για την ανάπτυξη δεν έχουν δημοσιεύσει το κωδικό πηγής του πράκτορα δικτύων ακόμα, καμία ανεξάρτητη επικύρωση του παρεχόμενου επιπέδου ανωνυμίας δεν έχει εκτελεσθεί.

Αυτή τη στιγμή προσφέρει τρεις υπηρεσίες:

- Κοινή χρήση αρχείων, ανώνυμα.
- Ιεραρχική ροή πολυμέσων (Hierarchical Multimedia Streaming).
- Ψηφιακή φωτογραφία που μοιράζεται με τους επιλεγμένους φίλους.

5.5.9 OFF System

Το Owner-Free File System (OFF System , or OFF) είναι ένα P2P διανεμημένο σύστημα αρχείων μέσω του οποίου όλα τα κοινά αρχεία αντιπροσωπεύονται από τους τυχαίους πολυ-χρησιμοποιημένους φραγμούς στοιχείων. [99] Το σύστημα αναφέρεται ως brightnet για να αντιπαραβάλει τη μέθοδο λειτουργίας του με αυτό των ιδιωτικών συστημάτων κοινών αρχείων που είναι γνωστών ως darknets. Το OFF δημιουργήθηκε με την εκδηλωθείσα πρόθεση " για να κόψει μερικά γάγγραινα-μολυσμένα κομμάτια των πνευματικών copyright industry."

Κατά την εισαγωγή αρχείων, το OFFSystem δημιουργεί τυχαίο πολυ-χρησιμοποιημένο " blocks" από τα στοιχεία, όπου το καθένα είναι 128Kb στο μέγεθος. Μετά από την εισαγωγή, ένα URL που έχει δημιουργηθεί μπορεί αργότερα να χρησιμοποιηθεί για την εκ νέου συναρμολόγηση των δεδομένων στην αρχική μορφή του. Ένα block των τυχαίων αριθμών συνδέεται σε ένα κρυπτογραφημένο κλειδί. Επειδή οι αριθμοί στο block των δεδομένων είναι τυχαίοι, μόνο το κλειδί τους δίνει νόημα. Αυτό επιτρέπει στο ίδιο block να χρησιμοποιηθεί με τα πολλαπλάσια κλειδιά για να αντιπροσωπεύσει τα διάφορα μέρη των διαφορετικών μηνυμάτων.

Ειδικότερα για την εύλογη δυνατότητα άρνησης, οποιοσδήποτε δεδομένος block μπορεί να χρησιμοποιηθεί για έναν άπειρο αριθμό αρχείων για λόγους αναδημιουργίας, καθιστώντας κατά συνέπεια αδύνατο για μια οντότητα να υποστηρίξει ότι οποιοσδήποτε block πρέπει να εμπέσει στα πνευματικά δικαιώματά τους. Κανένα στοιχείο που αποθηκεύεται στο σύστημα δεν κρυπτογραφείται, δεν συμπιέζετε, ή δεν χωρίζετε σε χοντρά κομμάτια επειδή δεν αντιπροσωπεύει τα αρχικά στοιχεία που παρεμβάλλονται για να αρχίσουν.

5.5.10 Omemo

Το Omemo είναι μια open source κοινωνική πλατφόρμα αποθήκευσης, στην οποία οι χρήστες μοιράζονται ανώνυμα τα αρχεία σε ένα μέρος των σκληρών τους δίσκων.[100] Έχει αναπτυχθεί από τον Pablo Soto, ο οποίος είναι επίσης ο δημιουργός του

[99] http://en.wikipedia.org/wiki/Owner_free_filing_system
[100] http://en.wikipedia.org/wiki/Omemo

Blubster. Το Omemo χρησιμοποιεί ένα ring-shaped DHT βασισμένο στη χορδή. Προορίζεται για να υποστηρίξει την "βασισμένη στο κλειδί" δρομολόγηση (Key based routing) διατηρώντας παράλληλα το ερώτημα της πηγής στην αφάνεια λόγω τυχαιοποίησης.

5.5.11 Osiris sps

Το Osiris Serverless Portal System είναι ένα πρόγραμμα δωρεάν λογισμικού που χρησιμοποιείται για να δημιουργήσει τις δικτυακές πύλες που διανέμονται μέσω P2P δικτύου και αυτόνομες από τους συγκεντρωμένους κεντρικούς υπολογιστές.[101] Είναι διαθέσιμο για το Microsoft Windows και το λειτουργικό σύστημα GNU/Linux.

Αντίθετα από τα κοινά εργαλεία που χρησιμοποιούνται για να "δημοσιεύει πληροφορίες" στο διαδίκτυο π.χ. CMS, φόρουμ ή Blogs που είναι βασισμένα σε ένα συγκεντρωμένο σύστημα, τα στοιχεία μιας πύλης που δημιουργούνται από το Osiris μοιράζονται μέσω P2P μεταξύ όλων των συμμετεχόντων του.

Χάρη σε αυτήν την αρχιτεκτονική στην οποία όλο το περιεχόμενο είναι απαραίτητο για την πλοήγηση αναδιπλώνεται σε κάθε μηχανή που μπορεί η πύλη να χρησιμοποιηθεί χωρίς έναν κεντρικό εξυπηρετητή (serverless). Αυτό αποτρέπει το ενδεχόμενο ότι η πύλη δεν είναι προσβάσιμη λόγω DDoS επιθέσεων , Internet Service Provider περιορισμών ή κάποια βλάβη υλικού.

Το Osiris έχει πολλά χαρακτηριστικά γνωρίσματα που το κάνουν ένα μοναδικό προϊόν αυτή τη στιγμή. Είναι το αποτέλεσμα μιας ένωσης μεταξύ του P2P και των δικτυακών πυλών (web portals).

- Επιτρέπει σε καθέναν να δημιουργήσει μια δικτυακή πύλη δωρεάν, χωρίς να εξαρτάται από κανέναν ή να έχει ειδικές τεχνικές γνώσεις.
- Σας επιτρέπει να δημιουργήσετε περιεχόμενο ανώνυμα, επιτρέποντάς σας να συμβάλετε στην ελευθερία της έκφρασης και του λόγου.
- Το Osiris προσφέρει μια ολοκληρωμένου κειμένου μηχανή αναζήτησης που επιτρέπει να ψάξει σε όλες τις πύλες του ψηφιακού περιεχομένου.
- Χαμηλή χρησιμοποίηση των πόρων. Με την αύξηση των χρηστών σε μια πύλη υπάρχει μια μείωση του φόρτου εργασίας στους ενιαίους κόμβους, καθώς η εργασία διανέμεται μεταξύ όλου του δικτύου.
- Χρησιμοποιείται μια P2P υποδομή (βασισμένη σε Kademlia) για τη διανομή πυλών, ένας τομέας όπου υπάρχουν λίγες και είναι δύσκολο να χρησιμοποιηθούν εναλλακτικές λύσεις.
- Η διοίκηση βασίζετε στο σύστημα της φήμης, σε έναν νέο τρόπο να διαχειριστεί το χρήστη σε ένα διανεμημένο σύστημα χωρίς τη χρήση των κεντρικών υπολογιστών.

5.5.12 Perfect Dark

[101] http://en.wikipedia.org/wiki/Osiris_(Serverless_Portal_System)

Το perfect Dark είναι μια ιαπωνική εφαρμογή δικτύου P2P που σχεδιάζεται για να χρησιμοποιηθεί με τα Microsoft Windows.[102] Ο συντάκτης του είναι γνωστός με το ψευδώνυμο Kaichō (☐☐; , λιτ. " Ο πρόεδρος"). Το perfect Dark αναπτύχθηκε με την πρόθεση να είναι ο διάδοχος τόσο του Winny όσο και των μετόχων του. Από την πιο πρόσφατη έκδοση (v1.02 "STAND ALONE COMPLEX") υπάρχει οικονομική ενίσχυση για το πρόγραμμα για να τρέξει και στη αγγλική γλώσσα, μια επιλογή που μπορεί να επιλεχτεί όταν εγκαθίσταται το πρόγραμμα.

Όπως και άλλο λογισμικό για τη μετοχή, το Perfect Dark έχει το δικό της P2P δίκτυο δεδομένων, τα οποία μετατρέπονται και ονομάζονται ενότητα. Ένα από τα μεγαλύτερα χαρακτηριστικά του Perfect Dark είναι η ισχυρή δυνατότητα αναζήτησης. Με τη βοήθεια του dht (distributed hash table), μπορεί να κρατήσει την απόδοσή του στην έρευνα ανεξάρτητη από την επέκταση του δικτύου.

Έτσι ελευθερώνει τους χρήστες από την εισαγωγή ή την αλλαγή του συμπλέγματος των λέξεων-κλειδιά, αλλά συγχρόνως επιτρέπουν στους χρήστες να ψάξουν τα αρχεία των διαφορετικών υφών. Όσον αφορά τον Winny και τους μετόχους του, έχουν προβλήματα όπου το σύμπλεγμα των λέξεων-κλειδιά τα οποία εγκαθίστανται για τα στοχοθετημένα αρχεία, θα πρέπει να διαμορφωθούν εκ των προτέρων, καθώς επίσης θα πρέπει να ρυθμιστούν και οι λέξεις κλειδιά προτού να εφαρμοστούν.

5.5.13 StealthNet

Το StealthNet είναι ένα δωρεάν λογισμικό ανοικτό λογισμικό κοινών αρχείων πηγής P2P, για το ανώνυμο διομότιμο δίκτυο RShare.[103] Το πρόγραμμα απαιτεί .net Framework package για να λειτουργήσει σωστά, και τον κωδικό που έχει αδειοδοτηθεί από την GPL. Μερικά από τα χαρακτηριστικά του είναι τα ακόλουθα:

- Swarming
- Επιτρέπει την επανάληψη των λήψεων που διακόπηκαν
- Επιτρέπει την προσθήκη και την αφαίρεση των αρχείων και των καταλόγων σε πραγματικό χρόνο.
- Multi-language (Multi-γλώσσα) διεπαφής χρήστη.
- Αναζήτηση φίλτρου για τους τύπους αρχείων.
- Point-to-Point κυκλοφορίας με κρυπτογράφηση Advanced Encryption Standard (AES).
- Ισχυρά hashes αρχεία με βάση τον αλγόριθμο SHA-512.
- Εύκολο στη χρήση, ακόμη και για αρχάριους.
- Multi-source downloads.
- Anti-flodding μέτρα έχουν τεθεί σε εφαρμογή για να αποτραπεί η υπονόμευση του RShare δικτύου όπως οι πλημμύρες με άχρηστα πακέτα.

[102] http://en.wikipedia.org/wiki/Perfect_Dark_(P2P)

[103] http://en.wikipedia.org/wiki/StealthNet

5.5.14 StegoShare Network

Το StegoShare είναι ένα εργαλείο στενογραφίας (steganography), το οποίο επιτρέπει να ενσωματώσει τα μεγάλα αρχεία στις πολλαπλάσιες εικόνες. [104]Μπορεί να χρησιμοποιηθεί για την ανώνυμη κοινή χρήση αρχείων. Μερικά από τα χαρακτηριστικά του είναι τα ακόλουθα:

- Υποστηρίζει διάφορους τύπους εικόνων (png, jpg, bmp, gif, tiff κλπ)
- Το μέγιστο υποστηριζόμενο κρυφό αρχείο έχει μεγέθους 2GB, αριθμός που καλύπτει εικόνες μέχρι 65.536.
- Ο μέσος όρος της ικανότητα είναι 40% (σε 250Mb εικόνας μπορούν να ενσωματωθούν 100MB αρχείου).
- 128-bit κρυπτογράφησης.
- Καλή ποιότητα παραγωγής εικόνων (αλλαγές ανιχνεύσιμες από το ανθρώπινο μάτι)

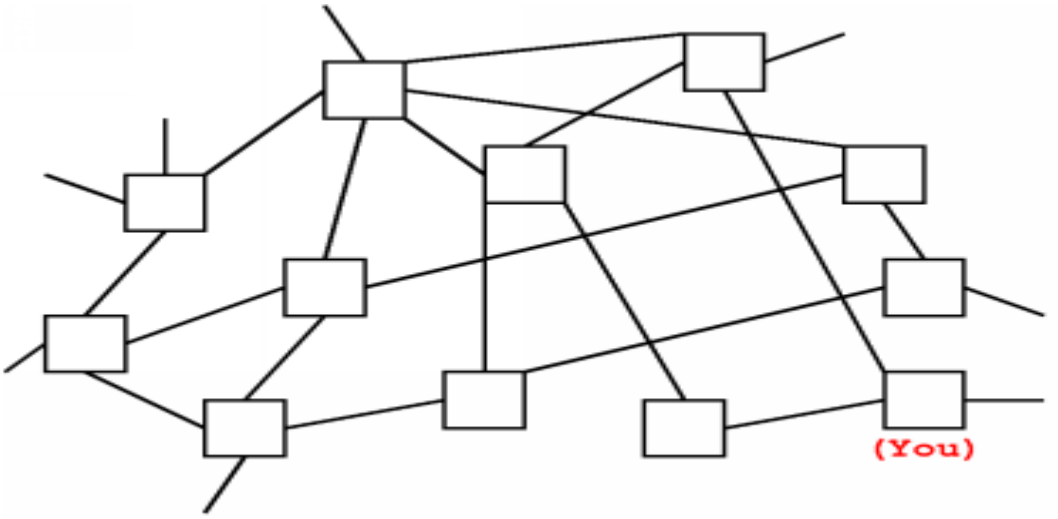
MUTE Network

5.5.15.1 Εισαγωγή

Μετά από το «θάνατο» του δικτύου Napster, όλα τα κοινής χρήσης αρχεία που ανήλθαν στην επικρατούσα δημοτικότητα, αποκεντρώθηκαν.[105] Η διοικητική αποκέντρωση παρέχει τη νομική προστασία για τις επιχειρήσεις που διανέμουν το λογισμικό, δεδομένου ότι δεν είναι απαραίτητο να τρέξουν οποιοδήποτε συστατικό του δικτύου οι ίδιοι: μόλις πάρετε το λογισμικό, γίνεστε μέρος του δικτύου, και το δίκτυο θα μπορούσε να επιζήσει ακόμα κι αν η μητρική εταιρεία εξαφανιστεί.

Όλα αυτά τα δίκτυα λειτουργούν ως Ιστός ή πλέγμα των κόμβων των γειτονικών συνδέσεων. Ο κόμβος σας συνδέεται με μερικούς άλλους κόμβους στο δίκτυο, και εκείνοι οι κόμβοι συνδέονται με μερικούς άλλους κόμβους, που συνδέονται στη συνέχεια με μερικούς άλλους κόμβους, και ούτω καθεξής. Αυτό το σχεδιάγραμμα είναι παρόμοιο με ένα πραγματικό κοινωνικό δίκτυο: ξέρετε κάποιους ανθρώπους, και εκείνοι οι άνθρωποι ξέρουν άλλους ανθρώπους, που ξέρουν στη συνέχεια άλλους ανθρώπους, και ούτω καθεξής. Ένα τμήμα ενός τέτοιου δικτύου μπορεί να μοιάζει κάπως έτσι:

[104] http://en.wikipedia.org/wiki/StegoShare
[105] http://mute-net.sourceforge.net/howPrivacy.shtml



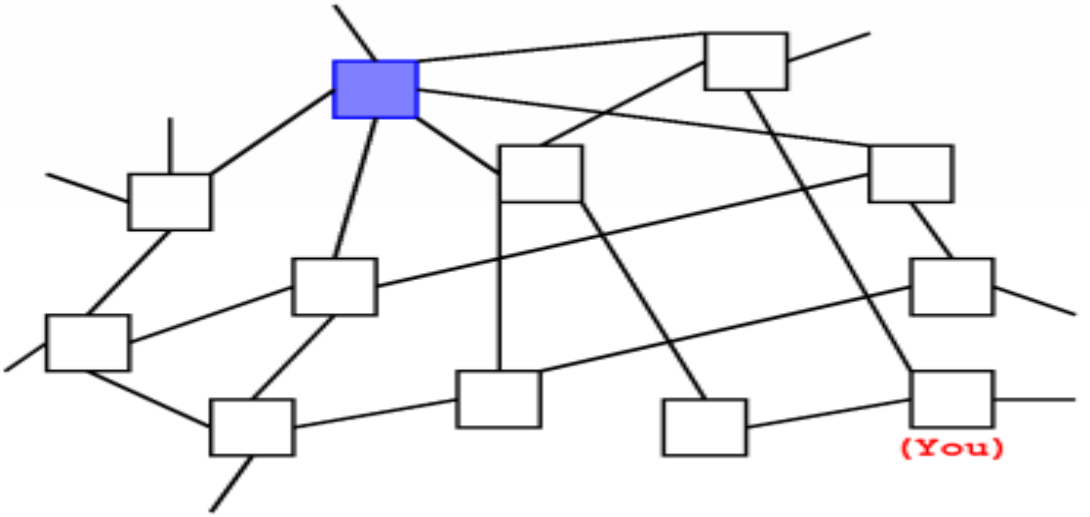
Εικόνα 62 Mute:Τμήμα δικτύου

Όταν ψάχνετε για αρχεία στο δίκτυο, στέλνετε ένα αίτημα αναζήτησης στους γείτονές σας, αυτοί στέλνουν το αίτημα προς τους γείτονές τους, και ούτω καθεξής. Τελικά, το αίτημά σας φθάνει σε πολλούς κόμβους στο δίκτυο. Παραδείγματος χάριν, στείλετε μια αναζήτηση metallica mp3. Τα μέρη των κόμβων λαμβάνουν το αίτημά σας, αλλά μόνο μερικοί από αυτούς μοιράζονται πραγματικά οποιαδήποτε μουσική metallica. Εκείνοι που έχουν τις αντιστοιχίες στέλνουν τα αποτελέσματά τους πίσω στον κόμβο σας. Τα αποτελέσματα αυτά είναι κάπως έτσι:

My Address: **128.223.12.122** **128.223.12.122**	My File: **Metallica__Enter_Sandman.mp3** **Metallica__Enter_Sandman.mp3**
My Address: **128.223.12.122** **128.223.12.122**	My File: **Metallica__Unforgiven.mp3** **Metallica__Unforgiven.mp3**
My Address: **128.223.12.122** **128.223.12.122**	My File: **Metallica__Everywhere_I_Roam.mp3** **Metallica__Everywhere_I_Roam.mp3**

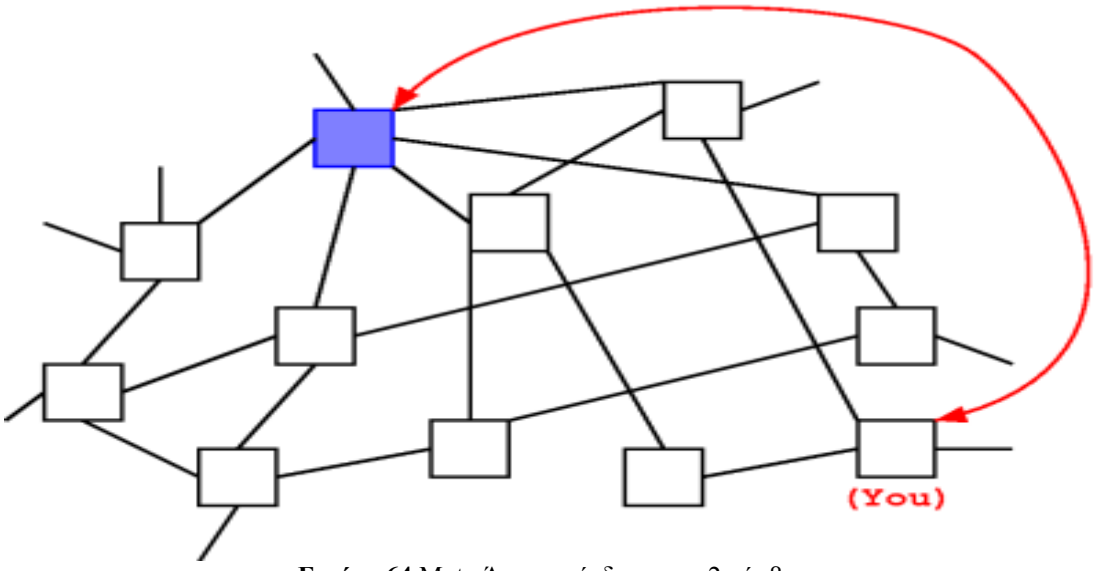
Πίνακας 4 Mute:Αποτελέσματα έρευνας

Παρατηρήστε το "My Address" αυτών των απαντήσεων. Η διεύθυνση που απαριθμείται είναι η διεύθυνση Διαδικτύου του υπολογιστή που έχει το αρχείο. Εάν δεν είστε εξοικειωμένοι με τις διευθύνσεις Διαδικτύου (συνήθως αποκαλούμενες διευθύνσεις IP), είναι όπως ένα " αριθμό τηλεφώνου" για έναν υπολογιστή στο διαδίκτυο. Οι υπολογιστές χρησιμοποιούν αυτές τις διευθύνσεις για να κάνουν τις συνδέσεις ο ένας στον άλλο μέσω του Διαδικτύου, και ο κόμβος σας μπορεί να χρησιμοποιήσει αυτήν την διεύθυνση για να κάνει μια σύνδεση στον κόμβο που μοιράζεται τα τρία αρχεία Metallica που παρουσιάζονται παραπάνω. Επίσης όπως τους αριθμούς τηλεφώνου, οι διευθύνσεις Διαδικτύου μπορούν να επισημανθούν για να ανακαλύψουν ποιος τους είναι ο κάτοχός της. Υποθέστε ότι ο μπλε κόμβος είναι ο κόμβος στο 128.223.12.122 που επέστρεψε τα τρία αποτελέσματα Metallica:



Εικόνα 63 Mute:Σύνδεση με τον μπλε κόμβο που περιέχει το ζητούμενο αρχείο

Για να κατεβάσετε ένα αρχείο από τον μπλε κόμβο, ο κόμβος σας κάνει μια άμεση σύνδεση στον μπλε χρησιμοποιώντας τη διεύθυνση 128.223.12.122. Αφότου συνδεθεί ο κόμβος σας με τον μπλε κόμβο, ο μπλε κόμβος ξέρει την IP σας διεύθυνση, για παράδειγμα 113.18.92.15 (σε αναλογία με την τηλεφωνία, είναι σαν να χρησιμοποιεί αναγνώριση κλήσεων ο μπλε κόμβος). Ο μπλε κόμβος σας στέλνει το αρχείο Metallica, και έπειτα κλείνετε τη σύνδεση. Αυτή η σύνδεση, η οποία είναι ξεχωριστή από τις άλλες συνδέσεις στο γειτονικό δίκτυο, θα είναι κάπως έτσι:



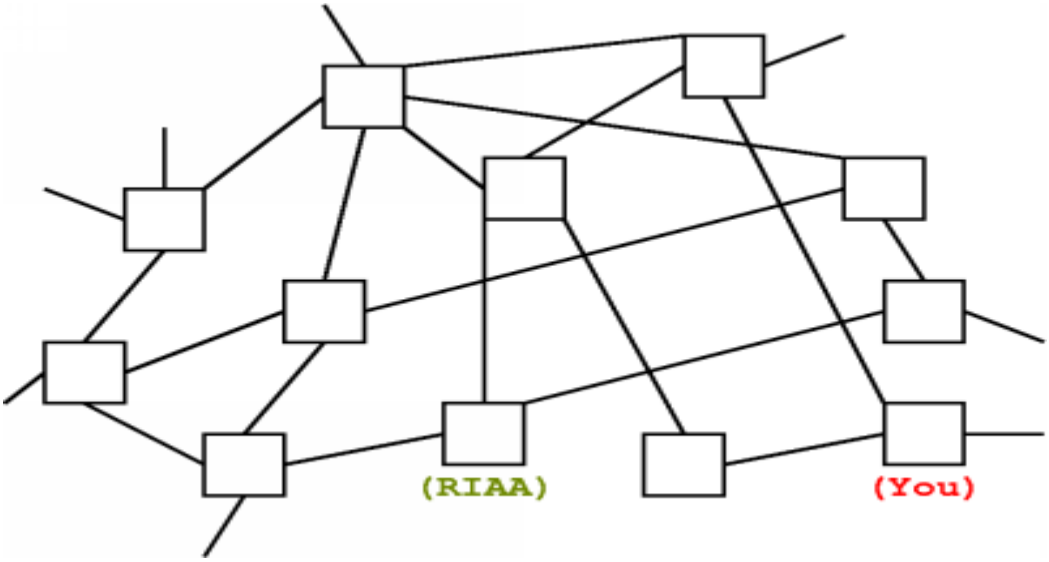
Εικόνα 64 Mute:Άμεση σύνδεση των 2 κόμβων

Με την εκτέλεση μιας αναζήτησης, παίρνετε την IP διεύθυνση όσων μοιράζονται Metallica. Όταν κατεβάζετε ένα αρχείο από εκείνο το πρόσωπο, τότε αυτός παίρνει και την δική σας IP διεύθυνση επίσης. Λοιπόν, είναι μόνο μια διεύθυνση στο Internet, έτσι;

Ο Πάροχος Υπηρεσιών Ίντερνετ, ή ο ISP, σας παρέχει την IP διεύθυνση σας, με τον ίδιο τρόπο που η τηλεφωνική εταιρεία σας παρέχει τον αριθμό του τηλεφώνου σας. Και, όπως μια τηλεφωνική εταιρεία, έτσι και ο ISP ξέρει ποιος χρησιμοποιεί κάθε

διεύθυνση Διαδικτύου που χρησιμοποιείτε . Γενικά, ο ISP σας θα κρατήσει την ταυτότητά σας ιδιωτική. Έτσι, αν το πρόσωπο με το οποίο μοιράζεστε το Metallica έρθει σε επαφή με τον ISP σας και ρωτήσει, " ποίος χρησιμοποιεί το 113.18.92.15; " , ο ISP σας θα κρατήσει πιθανώς τα χείλια του σφραγισμένα. εκτός αν είναι φοβισμένο. Τίποτα δεν φοβίζει τον ISP περισσότερο από το RIAA (εκτός από ίσως το FBI και το NSA).

Υποθέστε ότι μοιράζεστε μια μεγάλη συλλογή της αγαπημένης μουσικής σας, και υποθέστε ότι η συλλογή σας περιέχει περισσότερα από 1000 τραγούδια. Επίσης, υποθέστε ότι τα περισσότερα από τα τραγούδια σε αυτήν την συλλογή είναι "ιδιοκτησίας" από δισκογραφικές που εκπροσωπούνται από την RIAA. Όταν κάποιος ψάχνει για " mp3" στο δίκτυο κοινής χρήσης αρχείων σας, ο κόμβος σας επιστρέφει πολλά αποτελέσματα. Τώρα υποθέστε ότι ένας από τους κόμβους στο δίκτυο, τυγχάνει να είναι ιδιοκτησία της RIAA:



Εικόνα 65 Mute: Ύπαρξη RIAA κόμβου στο δίκτυο

Το RIAA εκτελεί μια αναζήτηση στο δίκτυο των τραγουδιών για τα οποία φροντίζει. Από τότε που το RIAA ονομάζει " δικιά της " τη μεγάλη πλειοψηφία της μουσικής που δημοσιεύεται μέσα σε όλο τον κόσμο, μπορούμε να απλοποιήσουμε τα πράγματα με το να υποθέσουμε ότι η RIAA φροντίζει για τα περισσότερα τραγούδια. Κατά συνέπεια, το RIAA εκτελεί μια αναζήτηση " mp3" , και ο κόμβος σας επιστρέφει πάνω από 1000 αποτελέσματα, τα οποία είναι κάπως έτσι:

My Address: **113.18.92.15** **113.18.92.15**	My File: **Madonna__Holiday.mp3** **Madonna__Holiday.mp3**
My Address: **113.18.92.15** **113.18.92.15**	My File: **Fleetwood_Mac__Dreams.mp3** **Fleetwood_Mac__Dreams.mp3**
My Address: **113.18.92.15**	My File: **Journey__Faithfully.mp3**

113.18.92.15	**Journey__Faithfully.mp3**
. . . . . .	
My Address: **113.18.92.15** **113.18.92.15**	My File: **Bonnie_Raitt__Something_To_Talk_About.mp3** **Bonnie_Raitt__Something_To_Talk_About.mp3**
My Address: **113.18.92.15** **113.18.92.15**	My File: **Poison__Unskinny_Bop.mp3** **Poison__Unskinny_Bop.mp3**

Πίνακας 5 Mute: Αποτελέσματα αναζήτησης

Αν και ένας μέσος χρήστης κοινών αρχείων θα άρχιζε συνήθως να κατεβάζει σε απάντηση σε αυτό το ορυχείο χρυσού των αποτελεσμάτων αναζήτησης, το RIAA έχει όλες τις πληροφορίες που χρειάζεται, και έτσι σταματά εδώ. Με τον κατάλογο των 1000+ των τραγουδιών που παραβιάζονται, αρχειοθετεί μια κλήση ενάντια στον ISP σας (" Ποιος χρησιμοποιεί το 113.18.92.15; ") και ζητάει από την υπηρεσία παροχής Internet τα προσωπικά σας στοιχεία. Μόλις η RIAA έχει τα προσωπικά σας στοιχεία, είναι έτοιμη να καταθέσει αγωγή εναντίον σας για την παραβίαση πνευματικών δικαιωμάτων.

Με πρότυπο την κοινή χρήση αρχείων δικτύων, η βασική αδυναμία είναι ότι διευθύνσεις στο Διαδίκτυο για όλους όσους μοιράζονται αρχεία είναι άμεσα διαθέσιμα. Επιμερίζοντας τα copyrighted αρχεία χωρίς άδεια, θα μπορούν να παραβιάζουν τη νομοθεσία, ως έχει. Επιστρέφοντας στην τηλεφωνική αναλογία, η κοινή χρήση αρχείων τυποποιημένων δικτύων που χρησιμοποιούν είναι παρόμοια με τα τηλεφωνήματα φάρσας σε κάποιον που έχει την αναγνώριση κλήσεων---είναι επικίνδυνο και ηλίθιο Με την ευρεία χρήση της αναγνώρισης κλήσεων, ο καθένας που κάνει πλέον τηλεφωνήματα φάρσας ξέρει αυτές τις μέρες να τοποθετεί το " #31#" πριν από κάθε κλήση για να κρύψει την ταυτότητά του/της από το συμβαλλόμενο μέρος που καλείται.

Ο λόγος που οι διευθύνσεις IP είναι διαθέσιμες στα τυποποιημένα δίκτυα κοινής χρήσης αρχείων είναι επειδή δεν πρέπει να υπάρχει κανένας τρόπος να γίνει μια άμεση σύνδεση σε έναν κόμβο χωρίς να γνωρίζετε την IP του διεύθυνση. Επιπλέον, δεν υπάρχει κανένας τρόπος για έναν κόμβο να δεχτεί να κάνετε σύνδεση χωρίς επίσης να γνωρίζει την IP σας διεύθυνση. Η μετάδοση στοιχείων στο διαδίκτυο λειτουργεί απλά με αυτόν τον τρόπο, και δεν υπάρχει κάτι όπως το " blocking αναγνώρισης κλήσεων" βασισμένο πάνω στο Διαδίκτυο. Ο μόνος τρόπος να προστατευθούν οι ταυτότητες είναι να χτιστεί κάτι πάνω από το Διαδίκτυο για να αποφύγει τις άμεσες συνδέσεις μεταξύ των downloaders και των uploaders, και να αποφύγει έτσι την αναγκαιότητα της κατανομής διευθύνσεων στο Internet.

Ο κύριος τρόπος για να προστατευτεί τη μυστικότητά σας από το MUTE είναι με την αποφυγή των άμεσων συνδέσεων μεταξύ των downloaders και των uploaders. Νωρίτερα, περιγράψαμε πώς τα αιτήματα αναζήτησης στέλνονται γύρω από τα τυποποιημένα δίκτυα: στέλνετε μια αναζήτηση στους γείτονές σας, και την στέλνουν

στους γείτονές τους, που την στέλνουν στη συνέχεια στους γείτονές τους, και ούτω καθεξής. Με τη χρησιμοποίηση του δικτύου στα αιτήματα αναζήτησης διαδρομών, αυτά τα δίκτυα παραδίδουν ένα ιδιαίτερο αίτημα σε πολλούς κόμβους χωρίς παραγωγή των άμεσων συνδέσεων σε οποιοιδήποτε από αυτούς. Φυσικά, όταν έρχεται η ώρα να μεταφερθεί ένα αρχείο, αυτά τα δίκτυα χρησιμοποιούν τις άμεσες συνδέσεις.

Το MUTE δρομολογεί όλα τα μηνύματα, συμπεριλαμβανομένης της αναζήτησης, τα αποτελέσματα αναζήτησης, και τις μεταφορές αρχείων, μέσω του δικτύου των συνδέσεων των γειτόνων. Κατά συνέπεια, αν και ξέρετε τις IP διευθύνσεις των γειτόνων σας, δεν ξέρετε την IP διεύθυνση του κόμβου από τον οποίο κατεβάζετε τα αρχεία.

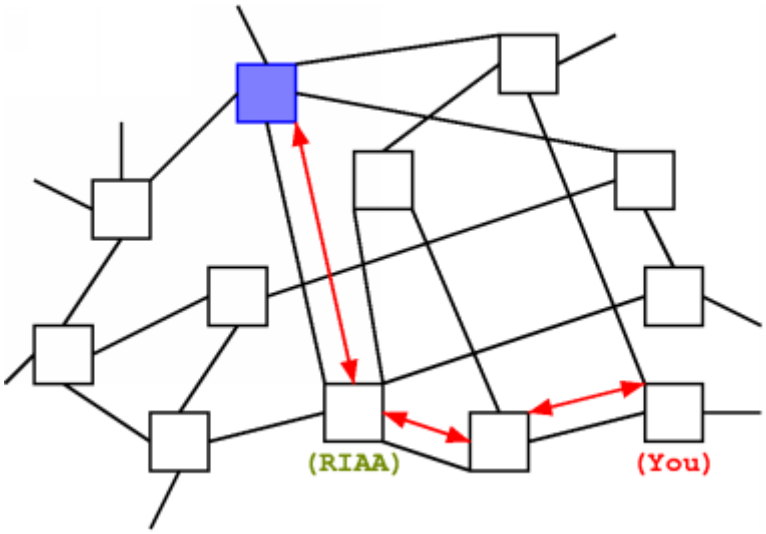
Ένας χάρτης ενός MUTE δικτύου φαίνεται ίδιος με τους χάρτες των τυποποιημένων δικτύων που παρουσιάζονται νωρίτερα. Εάν εκτελείτε μια αναζήτηση " metallica mp3" , θα λάβετε πίσω ακόμα τρία αποτελέσματα, αλλά αυτά τα αποτελέσματα φαίνονται λίγο διαφορετικά:

My Address: **7213D...2DCA5**	My File: **Metallica__Enter_Sandman.mp3**
My Address: **7213D...2DCA5**	My File: **Metallica__Unforgiven.mp3**
My Address: **7213D...2DCA5**	My File: **Metallica__Everywhere_I_Roam.mp3**

Πίνακας 6 Mute: Αποτελέσματα αναζήτησης

Ας σημειωθεί ότι το "My address" τμήμα από τις απαντήσεις αυτές δεν περιέχει πλέον μια διεύθυνση στο Internet. Η διεύθυνση, η οποία αποτελεί συντομογραφία με "..." ώστε να προσαρμοστεί στον πίνακα, είναι η 7213D29781593840CF00CDD1E9A7A425AE16DCA5. Αυτή είναι μια "εικονική" διεύθυνση του MUTE. Κάθε κόμβος στο δίκτυο MUTE έχει μια εικονική διεύθυνση που δημιουργείτε τυχαία κάθε φορά που ξεκινάει. Οι γείτονες σας στο δίκτυο (οι κόμβοι εκείνοι που πραγματικά θα μάθω τις διεύθυνση στο Internet) δεν γνωρίζουν ποια είναι η εικονική σας διεύθυνση, ώστε κανείς από το δίκτυο να μην μπορεί να συνδεθεί με την εικονική σας διεύθυνση στο Internet, και έτσι κανείς δεν μπορεί να αποκτήσει την ταυτότητα του πραγματικού κόσμου.

Το MUTE χρησιμοποιεί εικονικές διευθύνσεις και δρομολογεί τα μηνύματα μέσω του δικτύου χρησιμοποιώντας μια ant-inspired τεχνική. Κατά συνέπεια, για να κατεβάσει ένα αρχείο metallica, ο κόμβος σας θα έστελνε ένα αίτημα μέσω του δικτύου στο 7213D… 2DCA5, και κόμβος σας θα σηματοδοτούσε το αίτημα αυτό με την δική σας εικονική διεύθυνση, D1E9A59380CD425AE16D40CF0CA57A7213D29781. Ο κόμβος που μοιράζεται το αρχείο metallica θα έστελνε το ζητούμενο αρχείο πίσω σε σας χρησιμοποιώντας την εικονική σας διεύθυνση. Ολόκληρη η μεταφορά που δρομολογείτε μέσω του δικτύου, θα είναι κάπως έτσι:



Εικόνα 66 Mute: Δρομολόγηση μεταφοράς αρχείου

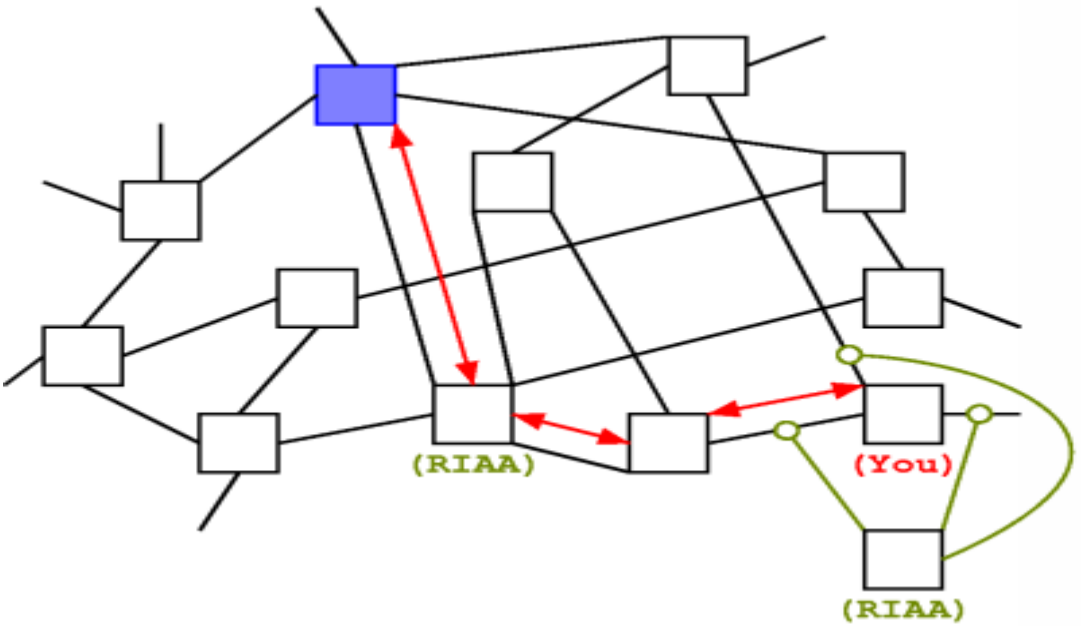
Αν και η μεταφορά καθοδηγείται μέσω ενός κόμβου που ανήκει στο RIAA, όλος ο κόμβος βλέπει ποιες είναι οι εικονικές διευθύνσεις σας και του συνεργάτη χρήσης κοινών αρχείων σας. Το RIAA μπορεί να στείλει μια αναζήτηση " mp3" , και θα πάρει ακόμα πίσω 1000 αποτελέσματα από σας, αλλά αυτά τα αποτελέσματα θα έμοιαζαν με αυτό:

My Address: **D1E9A...29781 D1E9A ... 29781**	My File: **Madonna__Holiday.mp3 Madonna__Holiday.mp3**
My Address: **D1E9A...29781 D1E9A ... 29781**	My File: **Fleetwood_Mac__Dreams.mp3 Fleetwood_Mac__Dreams.mp3**
My Address: **D1E9A...29781 D1E9A ... 29781**	My File: **Journey__Faithfully.mp3 Journey__Faithfully.mp3**
. . . . . .	
My Address: **D1E9A...29781 D1E9A ... 29781**	My File: **Bonnie_Raitt__Something_To_Talk_About.mp3**
My Address: **D1E9A...29781 D1E9A ... 29781**	My File: **Poison__Unskinny_Bop.mp3 Poison__Unskinny_Bop.mp3**

Πίνακας 4 Mute:Αποτελέσματα αναζήτησης

Το RIAA μπορεί να κλητεύσει τον ISP σας χρησιμοποιώντας την εικονική σας διεύθυνση, αλλά ο ISP σας δεν ξέρει ποιος χρησιμοποιεί αυτήν την διεύθυνση. Έτσι, το πρότυπο της RIAA είναι άχρηστη στο δίκτυο MUTE.

Δεδομένου ότι η τυποποιημένη τακτική αναζήτησης -και-κλήσης δεν λειτουργεί σε ένα δίκτυο MUTE , το RIAA ίσως να προσπαθήσει να στοχεύσει στους μεμονωμένους κόμβους με τον εντονότερο έλεγχο. Παραδείγματος χάριν, το RIAA μπορεί να οργανώσει έναν υπολογιστή στο τοπικό σας δίκτυο που θα άκουγε την όλη κίνηση του δικτύου σας (αυτό είναι παρόμοιο με το FBI που τρυπά τη τηλεφωνική γραμμή σας). Εάν το RIAA άκουγε την όλη κυκλοφορία σας, θα έβλεπε όλα τα δεδομένα που στείλατε σε κάθε έναν από τους γείτονές σας στο δίκτυο MUTE, και η κυκλοφορία θα είναι κάπως έτσι :



Εικόνα 67 Mute: Προσπάθεια του RIAA να ελέγξει τους κόμβους του δικτύου

Παρατηρήστε ότι το RIAA τώρα σας στριμώχνει: μπορεί να δει ότι υπάρχουν αιτήσεις που θα κατεβάσετε από τον κόμβο σας, αλλά κανένα αντίστοιχο αίτημα που μπαίνει στον κόμβο σας. Με άλλα λόγια, θα πρέπει να δημιουργείτε τις αιτήσεις και απλώς να βλέπετε τις αιτήσεις που έχετε λάβει από γείτονες σας.. Χρησιμοποιώντας αυτήν την τακτική, το RIAA θα μπορούσε να καθορίσει την IP διεύθυνση που συνδέθηκε με την εικονική διεύθυνσή σας και να αρχειοθετήσει έπειτα μια κλήση. Πώς όμως το MUTE εμποδίζει αυτήν την τακτική;

Το MUTE προστατεύει το περιεχόμενο κάθε σύνδεσης γειτόνων στο δίκτυό σας χρησιμοποιώντας την κρυπτογράφηση military-grade. Αν και το RIAA μπορεί να τρυπήσει το δίκτυό σας και να δει την όλη κίνηση του δικτύου σας, όλα τα MUTE μηνύματα δεν θα μπορούν να διαβαστούν. Κατά συνέπεια, το RIAA δεν θα ήταν σε θέση να σας στριμώξει στο δίκτυο ή να λάβει μια IP διεύθυνση σχετικά με την εικονική σας διεύθυνσή.

Φυσικά, οι γείτονές σας είναι σε θέση να αποκρυπτογραφήσουν τα μηνύματα που στέλνετε μέσω αυτών. Κατά συνέπεια, εάν το RIAA ήταν σε θέση να πειρατέψει κάθε

έναν από τους γειτονικούς σας κόμβους, θα μπορούσε πάλι να σας στριμώξει και να συνδέσει τη διεύθυνση Διαδικτύου σας με την εικονική σας διεύθυνση. Εντούτοις, είναι απίθανο ότι το RIAA θα ήταν σε θέση να πάρει έναν μεγάλο αριθμό κόμβων στο δίκτυο, και δεδομένου ότι ανακαλύπτετε τους γείτονές σας με έναν κάπως τυχαίο τρόπο, είναι απίθανο ότι κάθε ένας από τους γείτονές σας θα ήταν ένας κόμβος RIAA.

5.5.15.2 Εγκατάσταση του MUTE

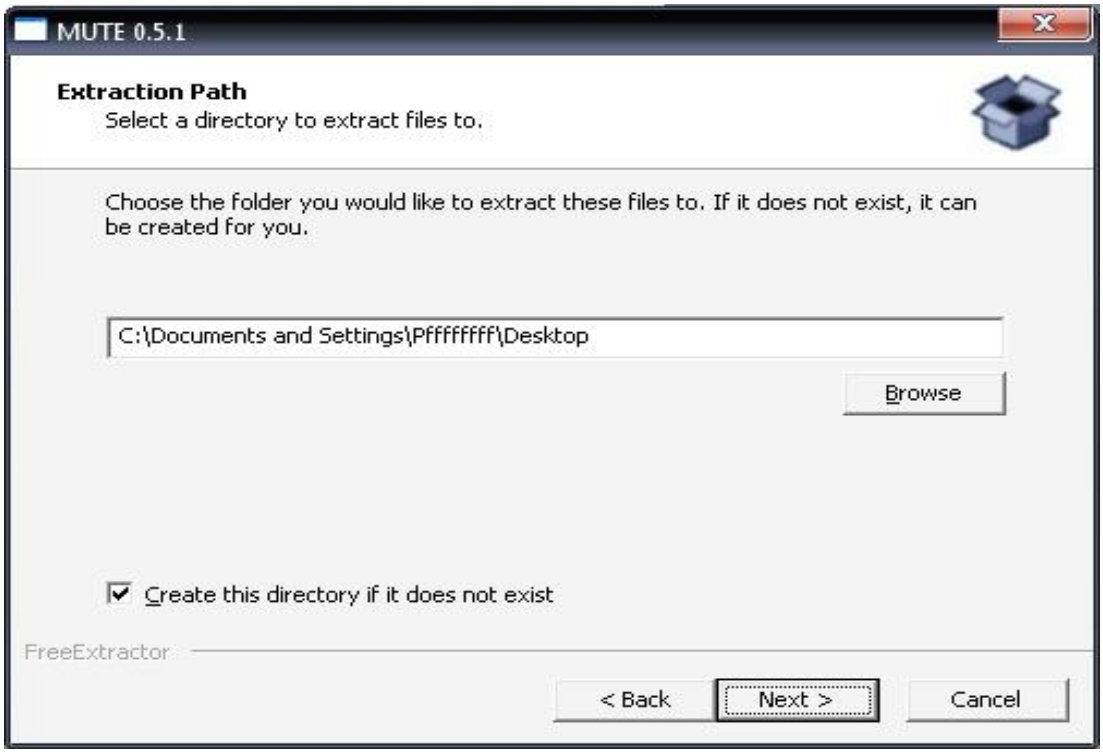
Αρχικά κατεβάζουμε την εφαρμογή.[106] Μόλις το κατεβάσουμε εμφανίζετε στον οθόνη του υπολογιστή μας το παρακάτω εικονίδιο:

Εικόνα 68 Mute:Εμφάνιση συντόμευσης της εφαρμογής

Έπειτα αποσυμπιέζουμε το αρχείο αυτό:

[106] http://sourceforge.net/projects/mute-net/

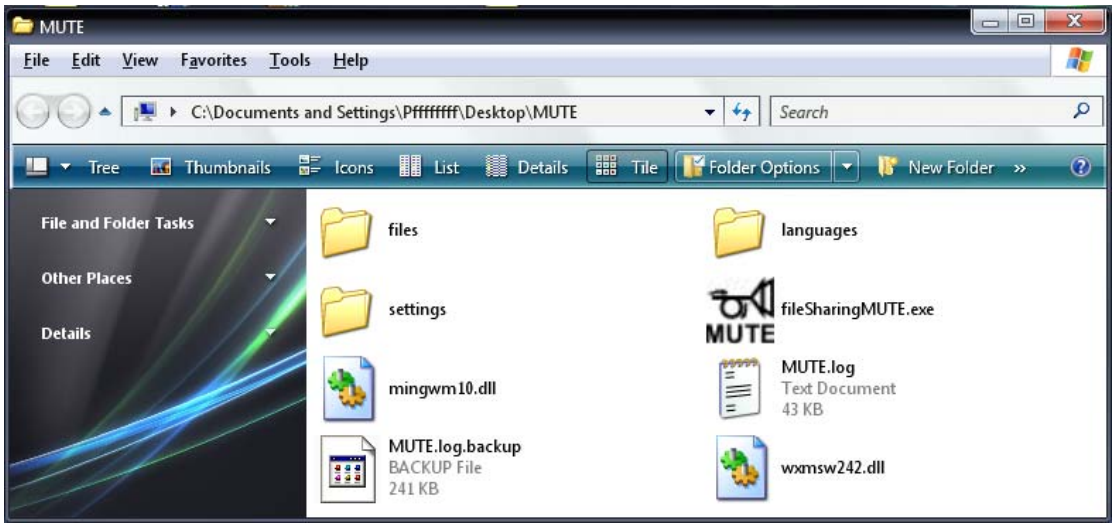
Εικόνα 69 Mute:Αποσυμπίεση αρχείου



Εικόνα 70 Mute:Επιλογή τοποθεσίας για την αποθήκευση του αρχείου της εφαρμογής

Έπειτα εμφανίζεται στην οθόνη μας ένας φάκελος με το όνομα MUTE, με το αρχείο της εφαρμογής στην τοποθεσία που έχουμε επιλέξει παραπάνω (στην περίπτωση μας στην επιφάνεια εργασίας) όπως φαίνεται και παρακάτω:

Εικόνα 71 Mute:Εμφάνιση του φακέλου με το αρχείο της εφαρμογής



Εικόνα 72 Mute:Περιεχόμενα του φακέλου

Για να τρέξουμε την εφαρμογή πατάμε διπλό κλικ πάνω στο fileSharingMUTE. Για να τρέξει η εφαρμογή θα πρέπει να έχουμε διαθέσιμες πόρτες, για αυτό το λόγο μας εμφανίζει τον παρακάτω διάλογο:

Εικόνα 73 Mute:Ενημέρωση για τυχών χρήση firewall

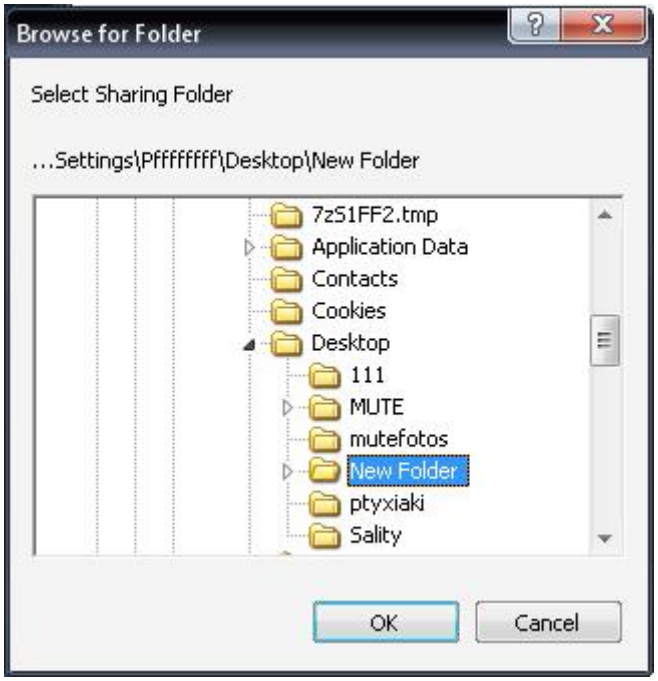
Έπειτα ζητάει να γράψουμε μια αλφαριθμητική ακολουθία με την οποία θα κρυπτογραφεί τα μηνύματα.

Εικόνα 74 Mute: Εισαγωγή αλφαριθμητικής ακολουθίας

Αφού εισάγουμε την αλφαριθμητική ακολουθία ζητάει να επιλέξεις το μέγεθος του κλειδιού:

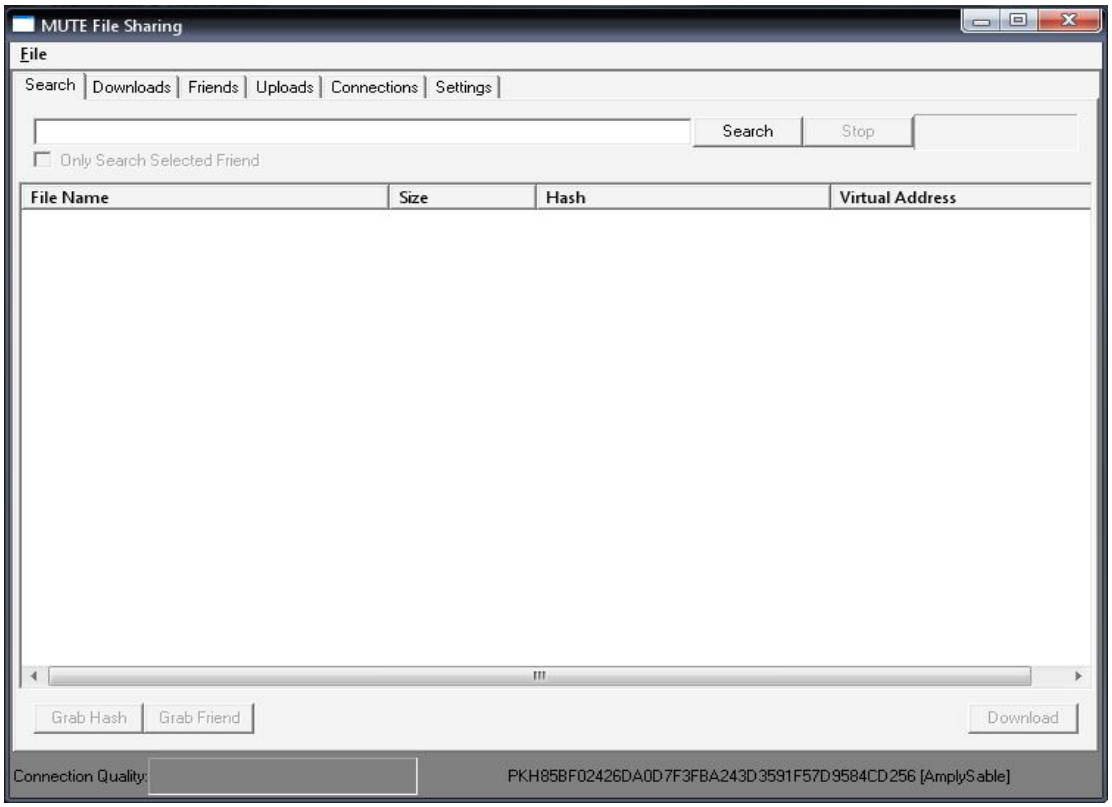
Εικόνα 75 Mute: Επιλογή μεγέθους κλειδιού

Στο επόμενο βήμα ζητάει να επιλέξουμε τα αρχεία που επιθυμούμε να μοιραστούμε:



Εικόνα 76 Mute: Επιλογή μοιραζόμενων αρχείων

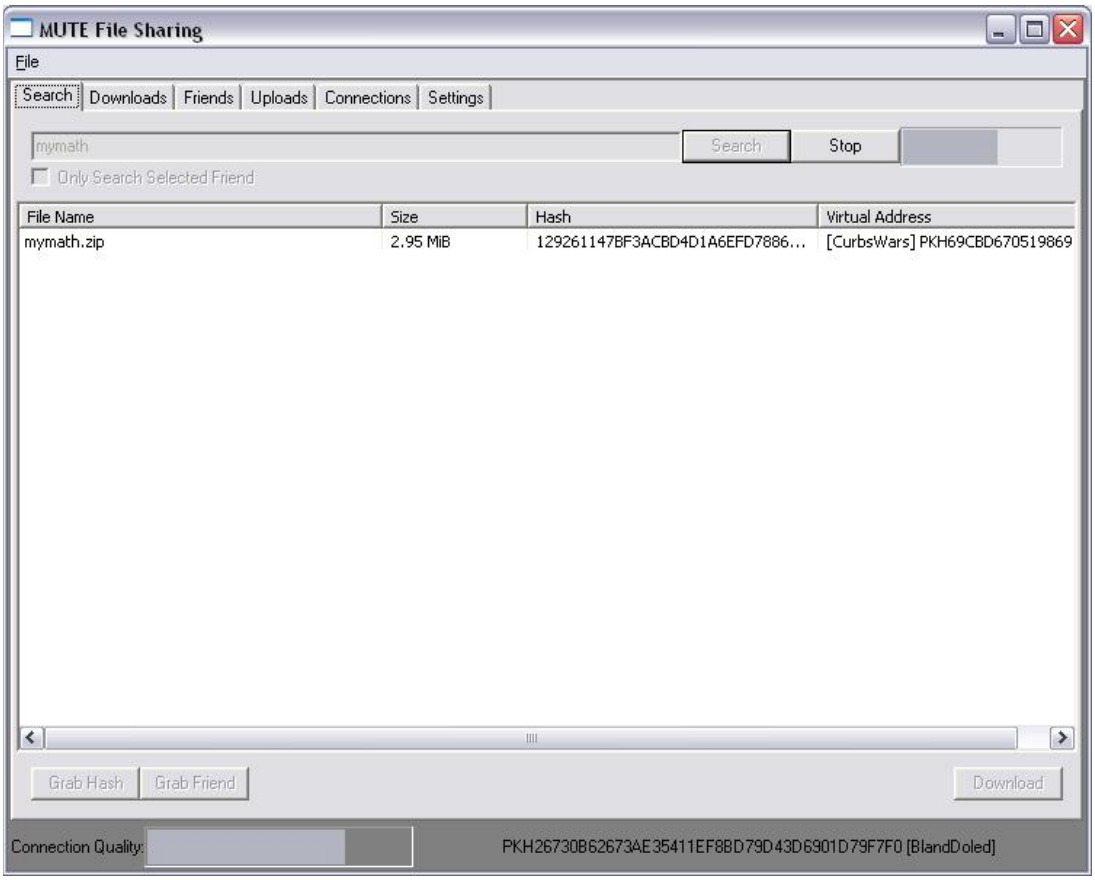
Από το σημείο αυτό και μετά μπορούμε να τρέξουμε την εφαρμογή και να αναζητήσουμε αρχεία.



Εικόνα 77 Mute: Αρχική σελίδα

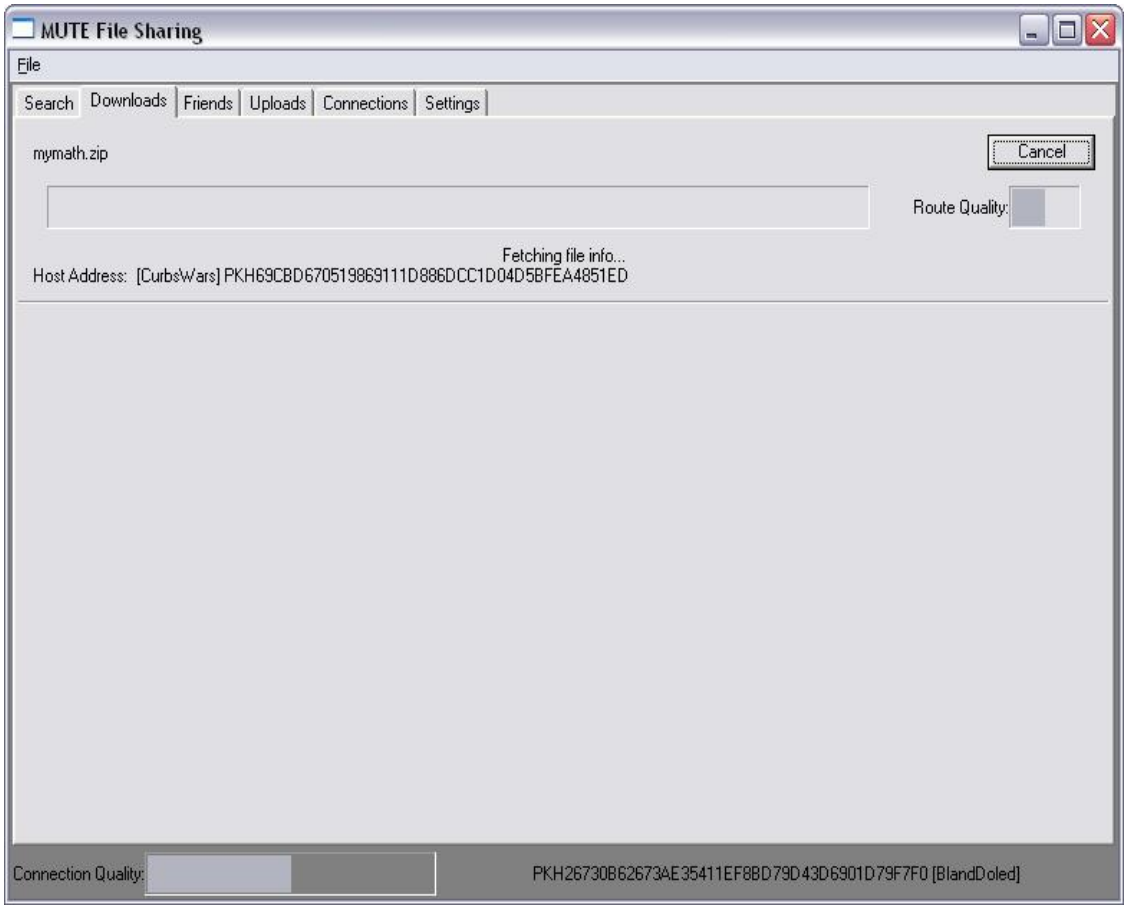
Στο πεδίο κάτω από το μενού της εφαρμογής γράφουμε το όνομα του αρχείου που επιθυμούμε να αναζητήσουμε ή αν δεν ξέρουμε ακριβώς ονομασία γράφουμε μια λέξη κλειδί. Όπως για παράδειγμα γίνεται παρακάτω.

Στο PC1 αναζητάμε το αρχείο mymath. Αφού πληκτρολογήσουμε το ζητούμενο όνομα αρχείου κάνουμε κλικ στο Search και ξεκινάει η αναζήτηση. Αφού βρει το αρχείο που ψάχνει εμφανίζει το όνομα του αρχείου που βρήκε, το μέγεθός του καθώς και την εικονική του διεύθυνση όπως και το ψευδώνυμο του κόμβου από τον οποίο θα πάρει το αρχείο.



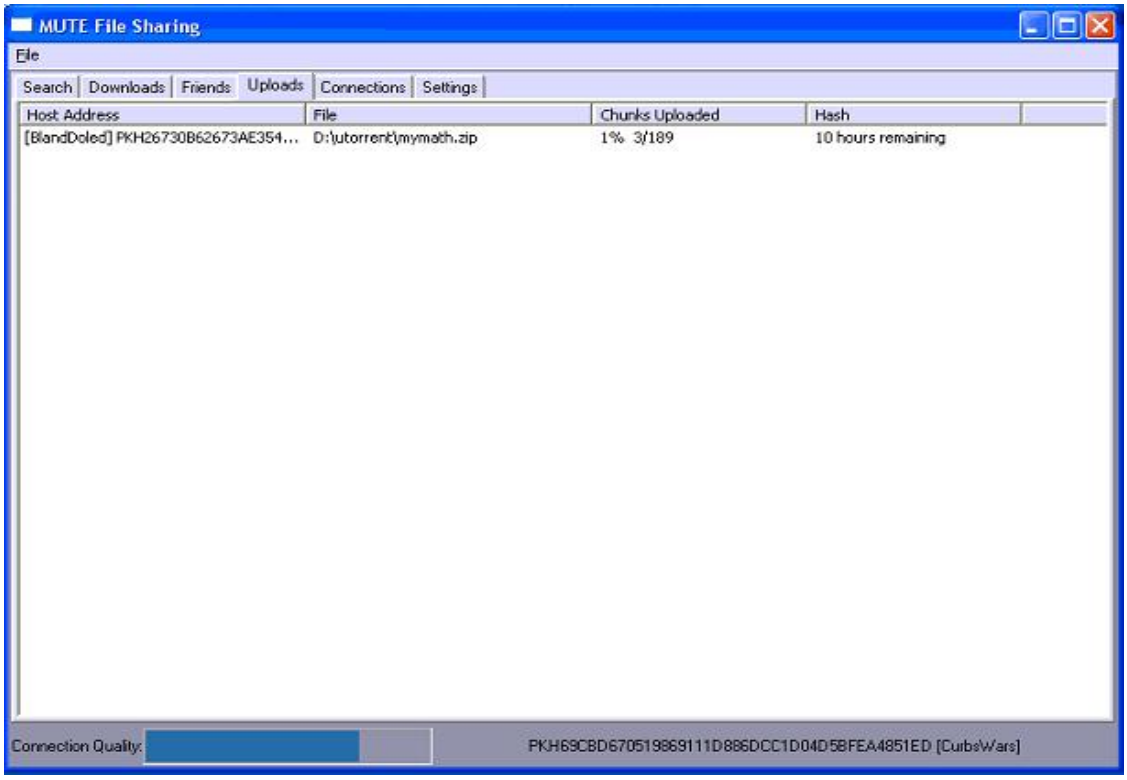
Εικόνα 78 Mute:Εισάγουμε όνομα αρχείου για αναζήτηση

Στο πεδίο Connection Quality μας δείχνει την ποιότητα της σύνδεσής μας. Και ακριβώς δίπλα είναι η κρυπτογραφημένη IP μας διεύθυνση με το ψευδώνυμο μας δίπλα από αυτό. Στη συνέχεια το PC1 κατεβάζει το αρχείο.



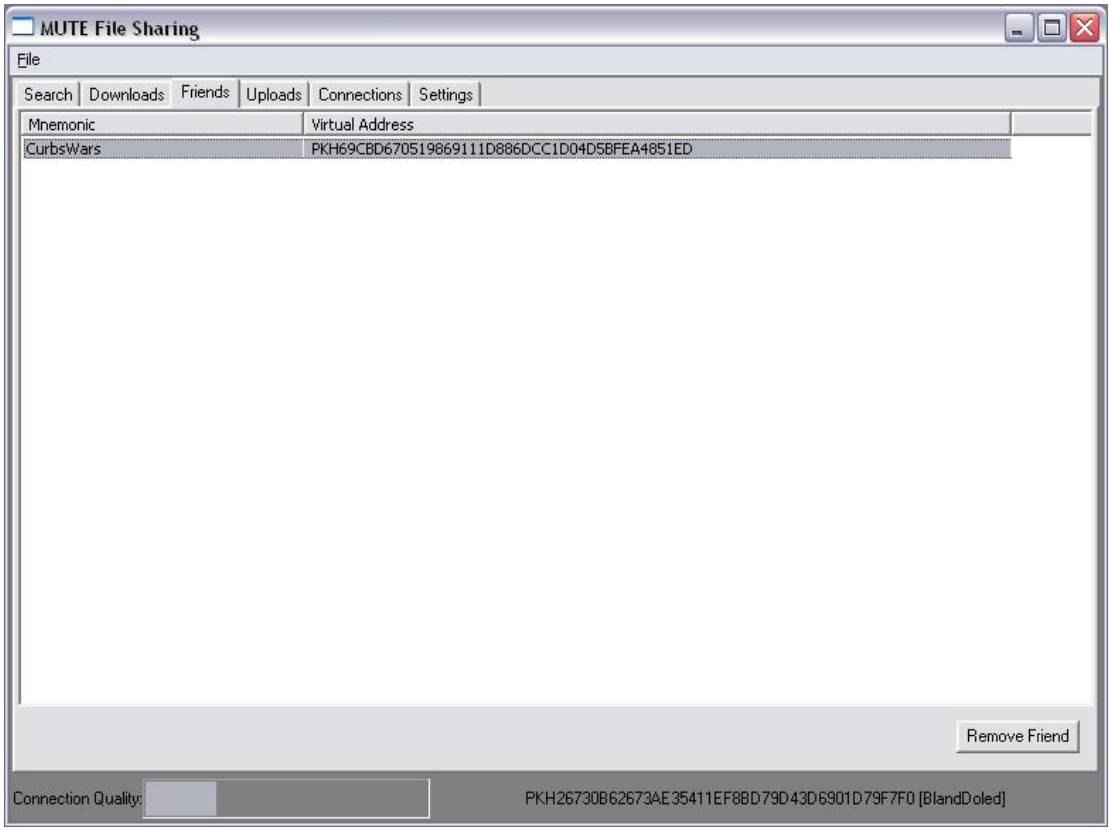
Εικόνα 79 Mute:Κάνουμε download το αρχείο

Ενώ στο PC2,στο οποίο βρήκαμε το αρχείο mymath, βλέπουμε το αρχείο που ανεβάζει την τοποθεσία που βρίσκετε και τον κόμβο που το ζητάει.



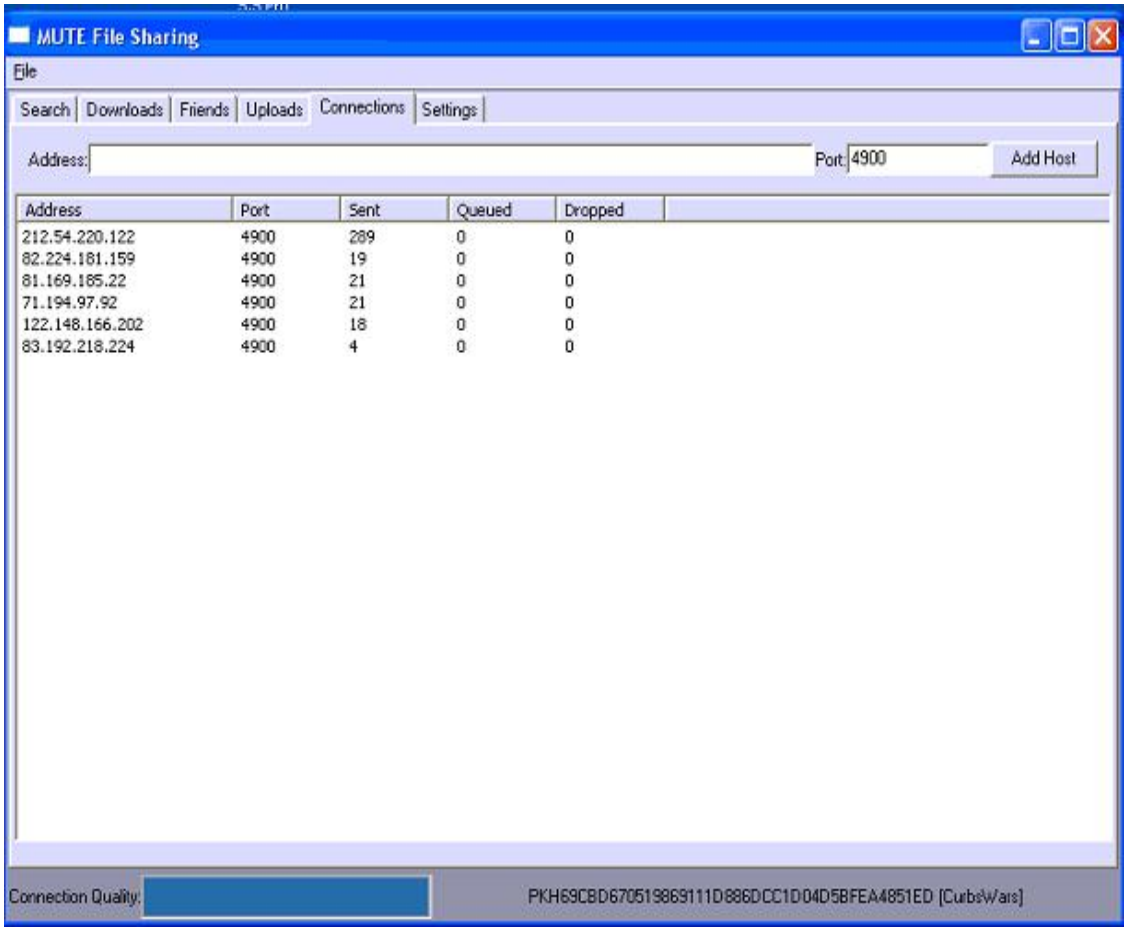
Εικόνα 80 Mute:Upload του αρχείου.

Στο πεδίοFriends μπορούμε να προσθέσουμε άτομα που γνωρίζουμε και θέλουμε να μοιραστούμε αρχεία. Γράφουμε δηλαδή το ψευδώνυμο και την εικονική του διεύθυνση κι έτσι μπορεί να υπάρξει μια άμεση σύνδεση με τον κόμβο αυτό.



Εικόνα 81 Mute: Προσθήκη φίλου στο πεδίο Friends

Στο πεδίο Connections φαίνονται οι κόμβοι με τους οποίους έχουμε συνδεθεί.



Εικόνα 82 Mute:Εμφάνιση κόμβων με τους οποίους έχουμε συνδεθεί

Το Mute προστατεύει την ιδιωτικότητά των χρηστών και τους καθιστά μη ανιχνεύσιμους, αντικαθιστώντας την ταυτότητά τους με μια "εικονική" διεύθυνση και κρυπτογραφώντας όσα αρχεία στέλνονται ή λαμβάνονται. Η εφαρμογή είναι αργή στο να συνδέσει, να βρει και να ανεβάσει ή να κατεβάσει αρχεία, αλλά αυτό είναι το 'τίμημα' για να πετύχει την ανωνυμία.

5.5.16 ANts P2P

5.5.16.1 Γενικά

Το ANts P2P είναι ένα δίκτυο τρίτης γενιάς,. ανοικτού κώδικα λογισμικό γραμμένο σε Java.[107] Προστατεύει την ιδιωτικότητά μας ενώ συνδεόμαστε σε αυτό, κρύβοντας την IP μας διεύθυνση και κρυπτογραφώντας τα αρχεία αυτά που στέλνουμε ή λαμβάνουμε από άλλους. Χαρακτηριστικό γνώρισμα του δικτύου αυτού είναι η διπλή κρυπτογράφηση η οποία επιτυγχάνεται point-to-point and endpoint-to-endpoint κρυπτογράφηση, όπου ενισχύουν την ιδιωτικότητά μας επειδή οι proxies που

[107] http://www.zeropaid.com/antsp2p/

καθοδηγούν το μήνυμά μας δεν θα είναι σε θέση να το αποκρυπτογραφήσουν. Το πρόγραμμα προωθήθηκε το 2004, και ο κώδικας είναι χορηγημένος από το GPL (General Public License**)**.[108]

Χαρακτηριστικά:

Τα ANts P2P κρυπτογραφούν όλη την κυκλοφορία δεδομένων [που ακολουθείτε] που στέλνεται ή που παραλαμβάνεται, και την κυκλοφορία των proxies που συμμετέχουν σε ένα δίκτυο, ώστε να είναι πιο δύσκολο να προσδιοριστεί η προέλευση των διευθύνσεων IP. Μερικά από τα χαρακτηριστικά γνωρίσματά του περιλαμβάνουν είναι τα παρακάτω:

- Αυτόματη αναπροσαρμογή του λογισμικού.
- Point-to-point κρυπτογράφηση
- End to end κρυπτογράφηση
- Πολλαπλών διαδρομών δρομολόγηση (Multipath routing) για τα πακέτα.
- Προνομιακές συνδέσεις για να δώσει στο δίκτυο ένα γρήγορο κορμό.
- Υποστήριξη για μερικές λήψεις.
- Υποστήριξη για το σχήμα συνδέσεων eDonkey.
- Αυτόματες πηγές για την ενεργοποίηση και την διακοπή λήψεων.
- Εύρεση τμημάτων των αρχείων μέσω κανονικών ερωτήσεων ή απορίων από hash.
- Μη ανώνυμο Internet Relay Chat.
- Οι ερωτήσεις κρυπτογραφούνται ασυμμετρικά. Αυτό σημαίνει ότι μόνο ο δημιουργός μπορεί να διαβάσει τα αποτελέσματα μιας αναζήτησης. Ο καθένας μπορεί να διαβάσει τη σειρά ερώτησης αλλά αυτή η ασύμμετρη προσέγγιση μειώνει τη δυνατότητα ενός κόμβου να κάνει ανάλυση διέλευσης μιας ερώτησης.

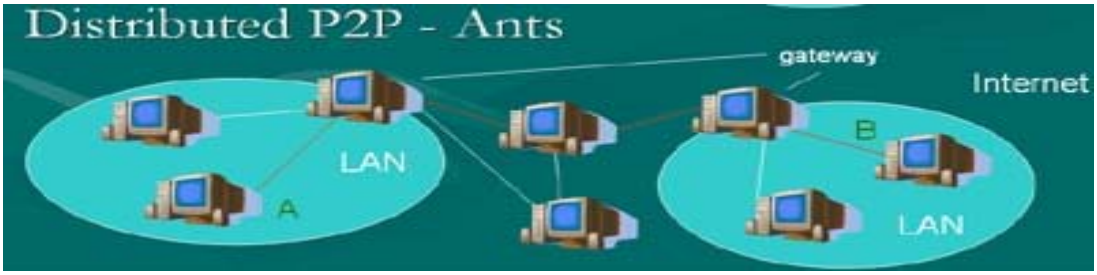
Το ANts P2P επίσης επιτρέπει στους χρήστες να χρησιμοποιούν ανώνυμους web servers (διακομιστές). Αυτό είναι εφικτό μόνο μέσα από το δίκτυο ANts P2P. Το ANts P2P εντούτοις, δεν είναι ένα outproxy δίκτυο που αφήνει τις υπηρεσίες προσιτότητας χρηστών στο συμβατικό διαδίκτυο. Για αυτό, μια υπηρεσία outproxy όπως το Tor μπορεί να χρησιμοποιηθεί χωριστά.

Οι μεταφορές δεδομένων τρέχουν πέρα από τις έμμεσες συνδέσεις: Οι αποστολείς και οι δέκτες ενός αρχείου δεν κρατούν μια άμεση σύνδεση ο ένας με τον άλλον, αλλά η σύνδεση πέφτει απότομα πέρα από διάφορους κόμβους, έτσι ώστε κανένα συμβαλλόμενο μέρος να μην μπορεί κοινότοπα να καθορίσει την ταυτότητα του άλλου. Η κυκλοφορία μεταξύ των κόμβων κρυπτογραφείται με AES, το οποίο αποτρέπει το ρουθούνισμα (sniffing) και από τους ξένους και από τους κόμβους διέλευσης. Η βασική ανταλλαγή κρυπτογράφησης χρησιμοποιεί τον αλγόριθμο diffie-Hellman.

[108] http://en.wikipedia.org/wiki/ANts_P2P

5.5.16.2 Λειτουργία του ANts P2P

Τα ANts P2P δεν είναι ένα κοινό P2P λογισμικό. Το δίκτυο αυτό είναι ένα AD-HOC δίκτυο. Στα κλασικά P2P δίκτυα τα αρχεία ανταλλάσσονται με τη βοήθεια των άμεσων συνδέσεων μεταξύ των χρηστών που θέλουν να μοιραστούν ένα αρχείο. Στα AD-HOC δίκτυα δύο κόμβοι (πέστε το A και το B) δεν χρειάζεται να κάνουν μια άμεση σύνδεση για να επικοινωνήσουν μεταξύ τους, αφού η επικοινωνία πραγματοποιείται από τα κανάλια που περνούν μέσω άλλων κόμβων:



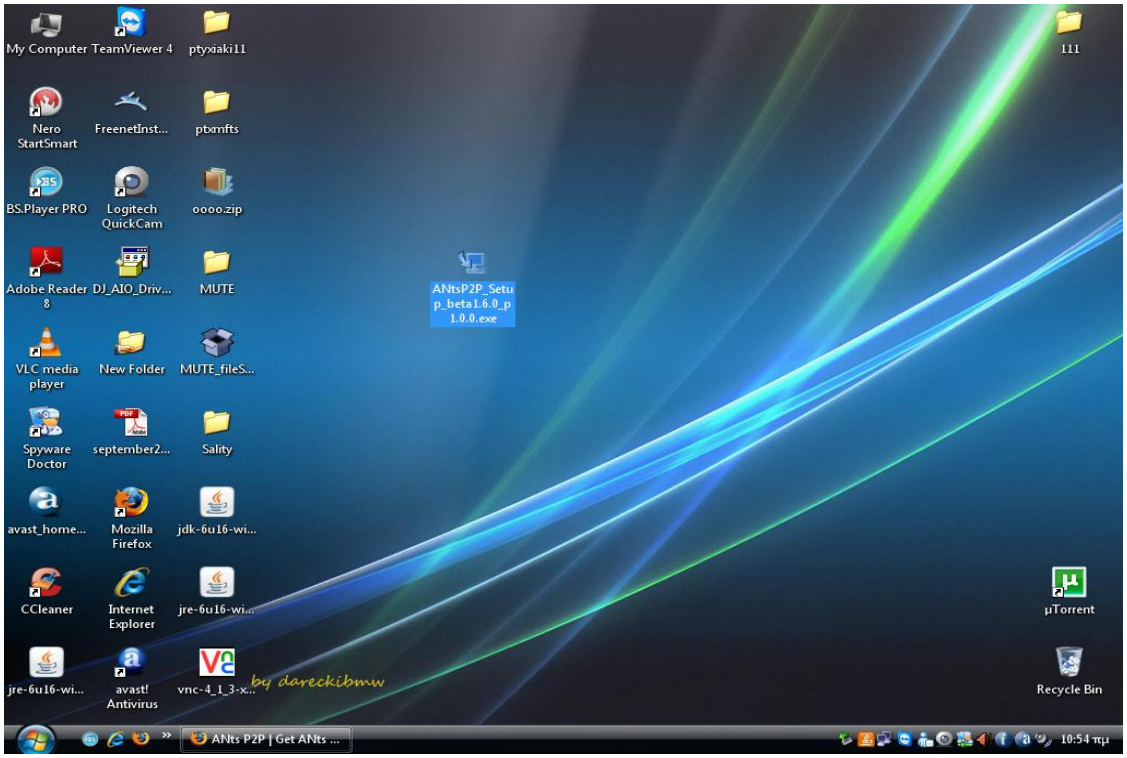
Εικόνα 83 ANts: Λειτουργία δικτύου.

Τα ANts P2P χρησιμοποιούν αυτό το χαρακτηριστικό γνώρισμα των AD-HOC δικτύων προκειμένου να επιτευχθεί η ανωνυμία και οι ιδιωτικές επικοινωνίες (private communications).

5.5.16.3 Εγκατάσταση του ANts P2P

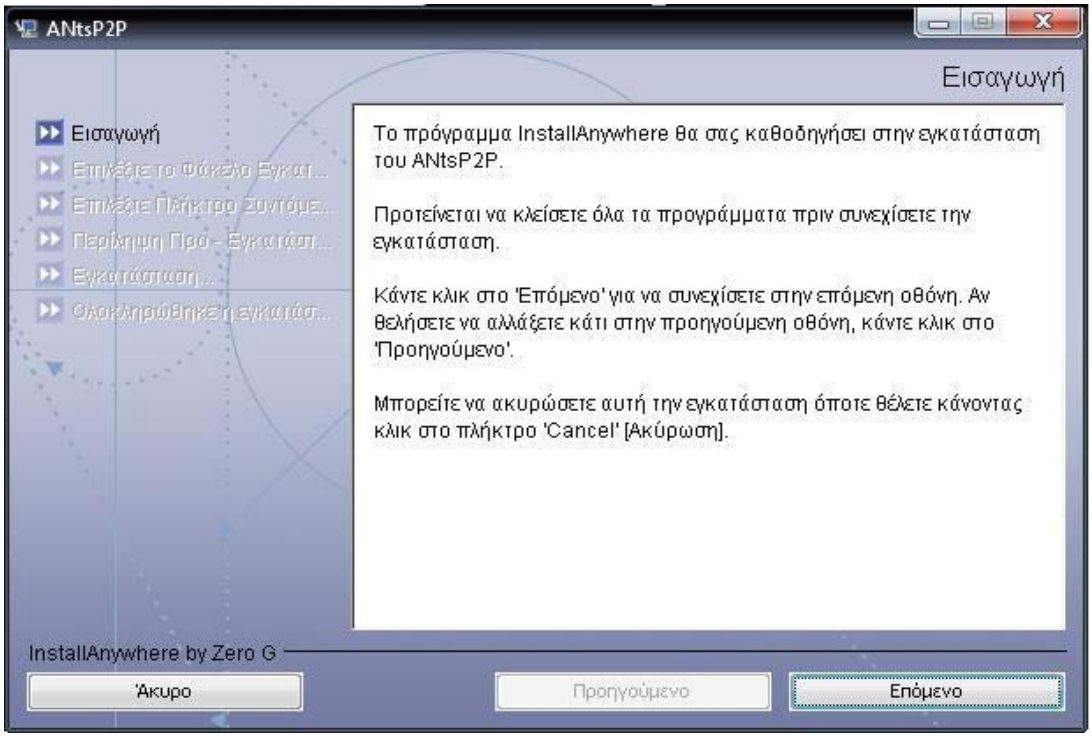
Αρχικά κατεβάζουμε την εφαρμογή.[109] Μόλις το κατεβάσουμε εμφανίζεται στον οθόνη του υπολογιστή μας το παρακάτω εικονίδιο:

[109] http://sourceforge.net/projects/antsp2p/



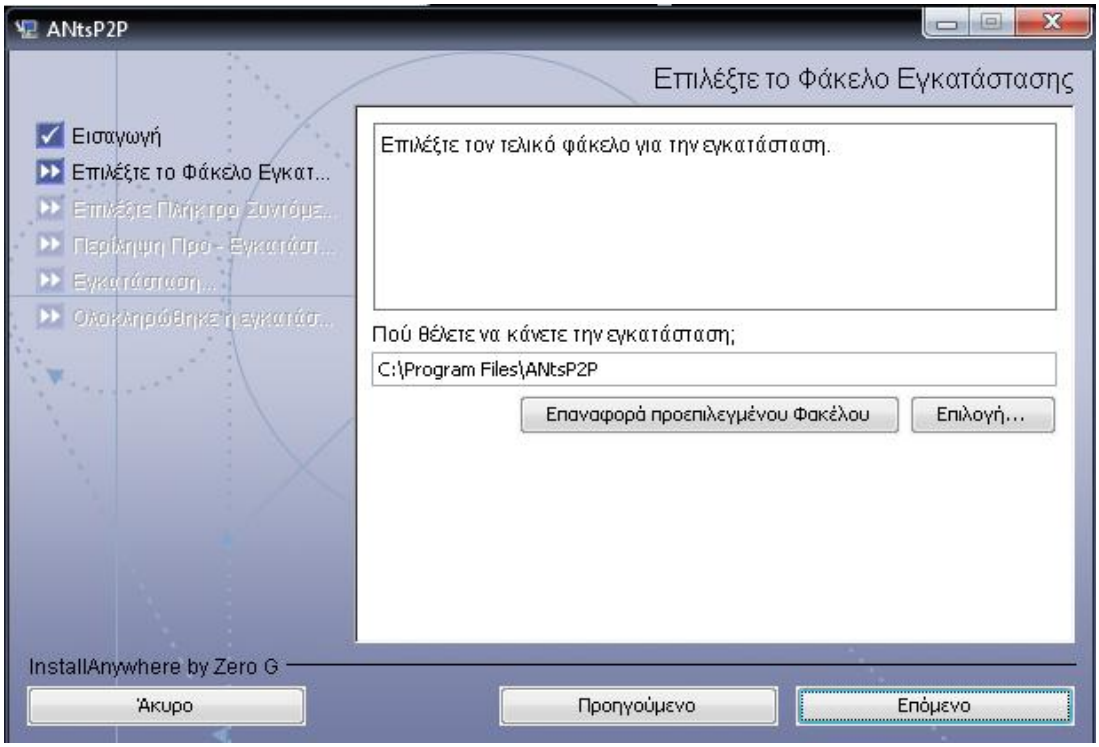
Εικόνα 84 ANts: Εμφάνιση συντόμευσης της εφαρμογής

Πατώντας διπλό κλικ πάνω στο εικονίδιο αυτό ξεκινάει η εγκατάσταση του προγράμματος:



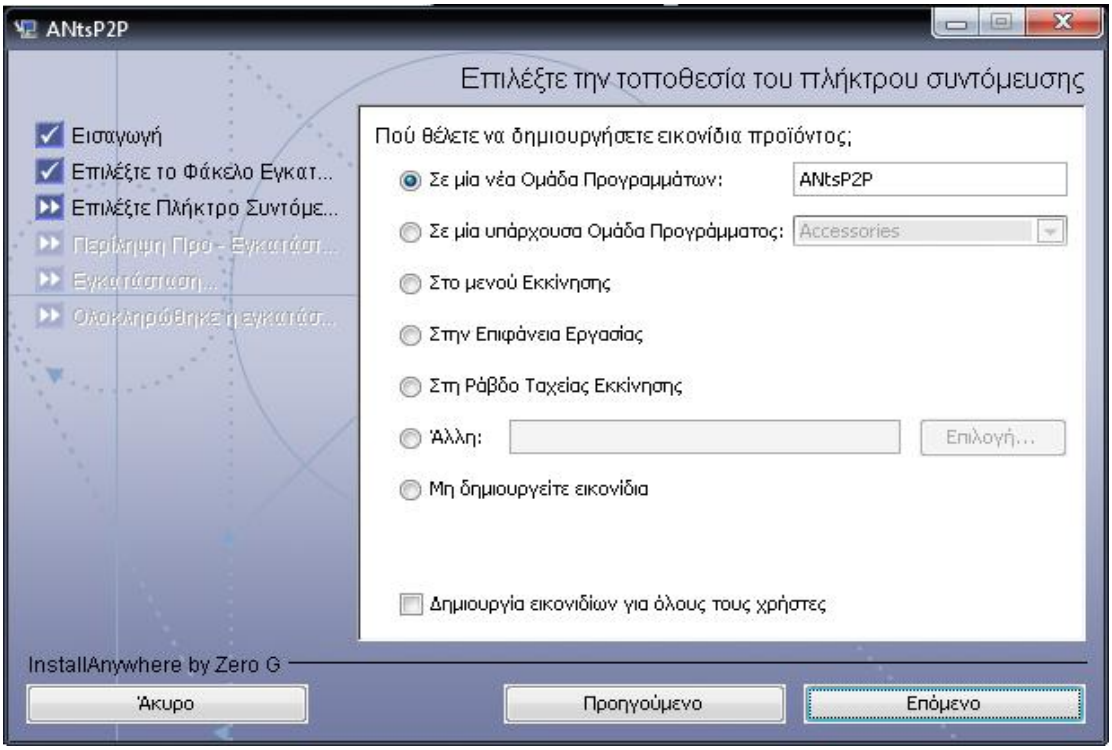
Εικόνα 85 AntsP2P: Εισαγωγή

Πατώντας ‘Επόμενο’ επιλέγουμε φάκελο εγκατάστασης του προγράμματος.



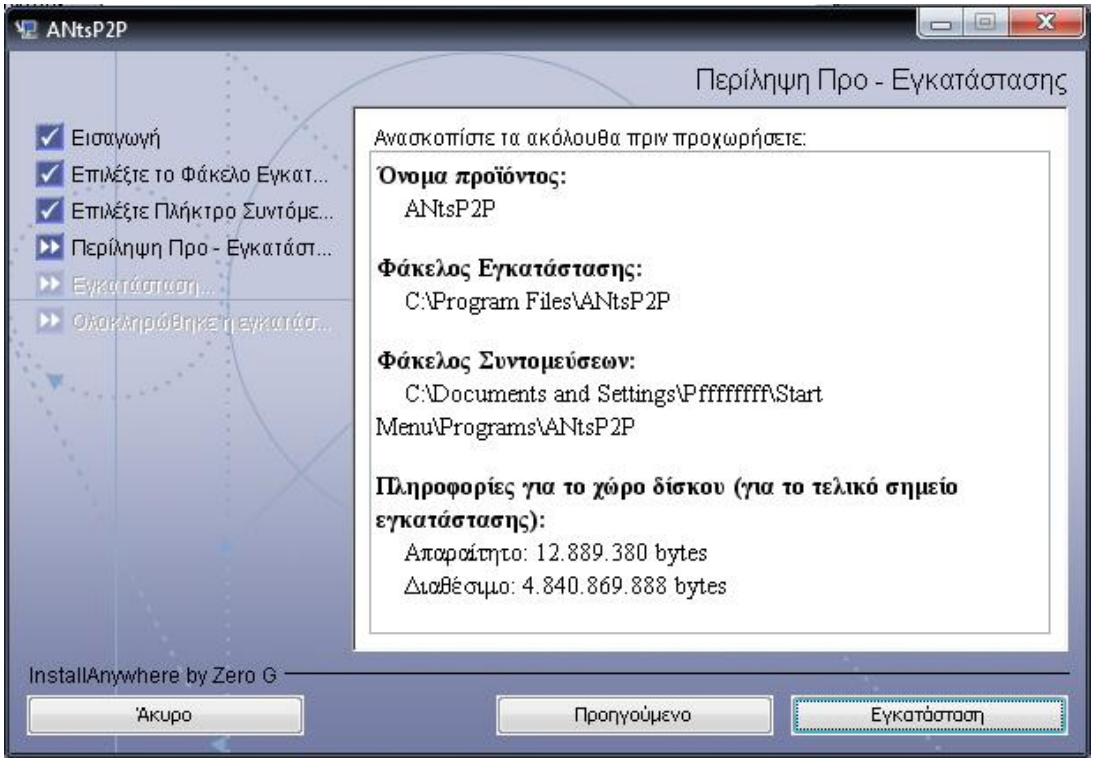
Εικόνα 86 AntsP2P: Επιλογή φακέλου εγκατάστασης

Προχωρώντας παρακάτω επιλέγουμε πλήκτρο συντόμευσης για το πρόγραμμα.

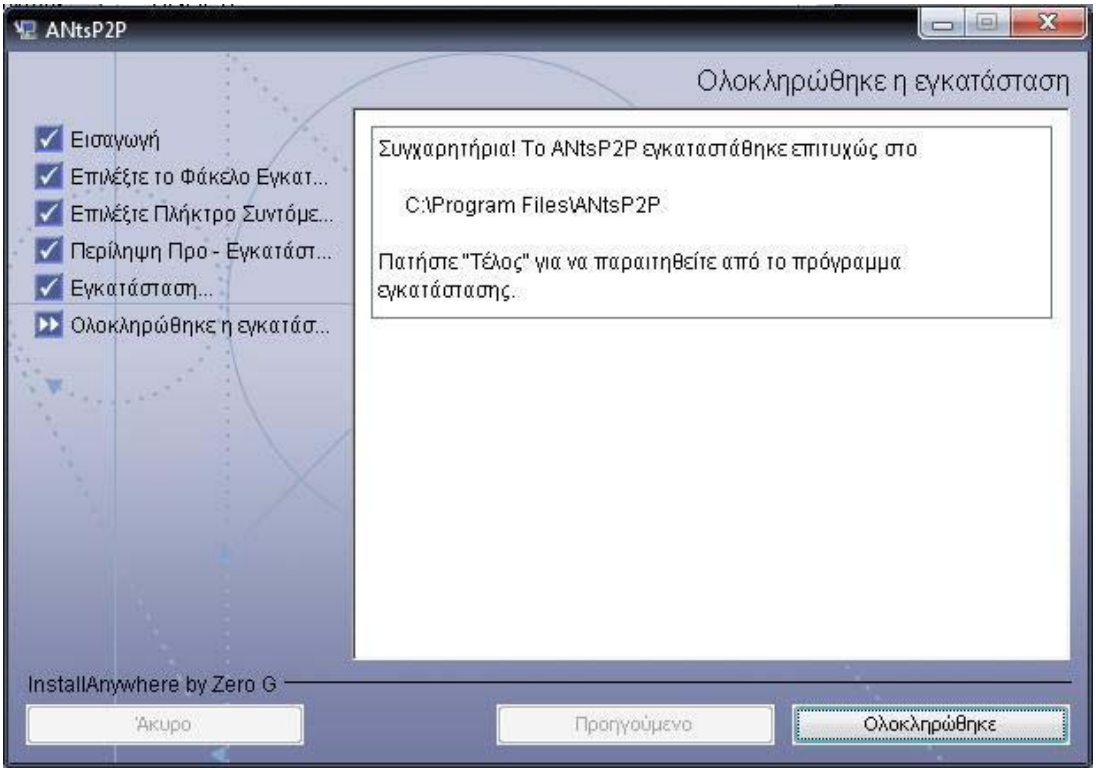


Εικόνα 87 AntsP2P: Επιλογή πλήκτρου συντόμευσης

Στο επόμενο βήμα εμφανίζει μια περίληψη της εγκατάστασης του προγράμματος δίνοντας μας την ευκαιρία να κάνουμε κάποια αλλαγή αν επιθυμούμε.



Εικόνα 88 AntsP2P: Περίληψη Προ-Εγκατάστασης



Εικόνα 89 AntsP2P: Ολοκλήρωση εγκατάστασης

Εικόνα 90 AntsP2P: Επιλογή γλώσσας

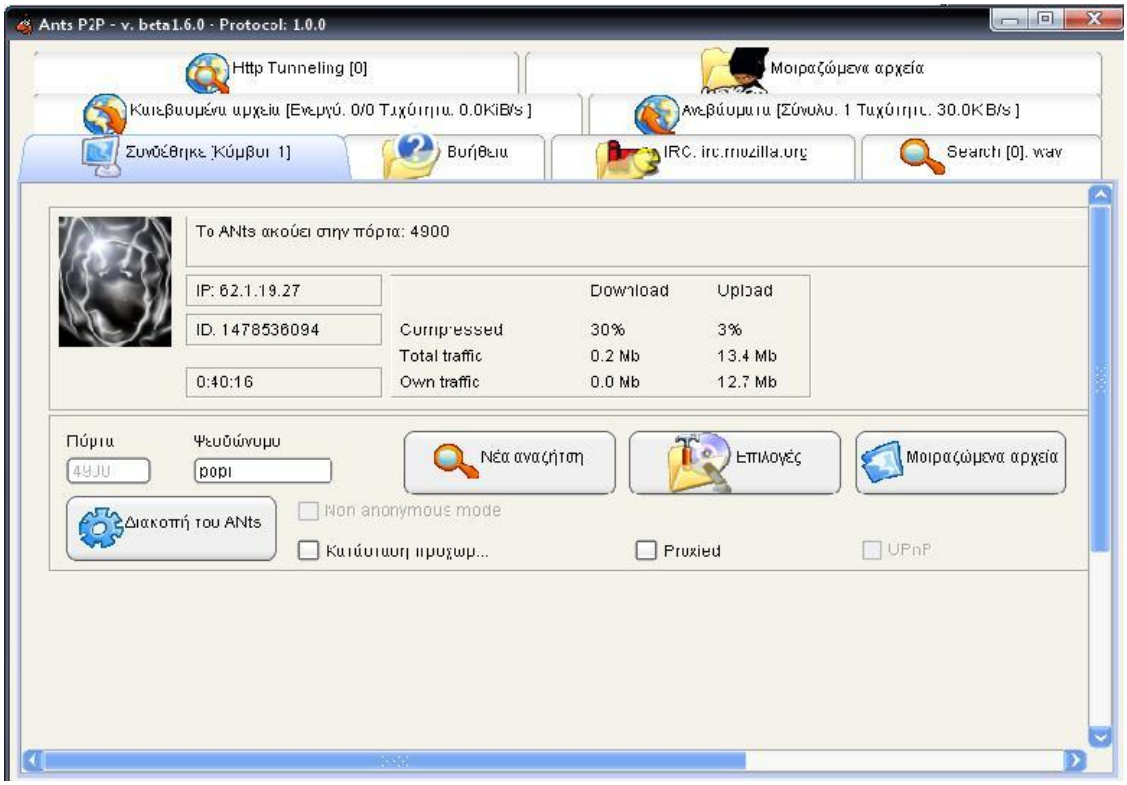
Εικόνα 91 AntsP2P: Έλεγχος IP address

Στο σημείο αυτό έχει γίνει εγκατάσταση του προγράμματος έχουμε επιλέξει γλώσσα εμφάνισης του προγράμματος καθώς έχει γίνει και έλεγχος της IP.

5.5.16.4 Εκτέλεση

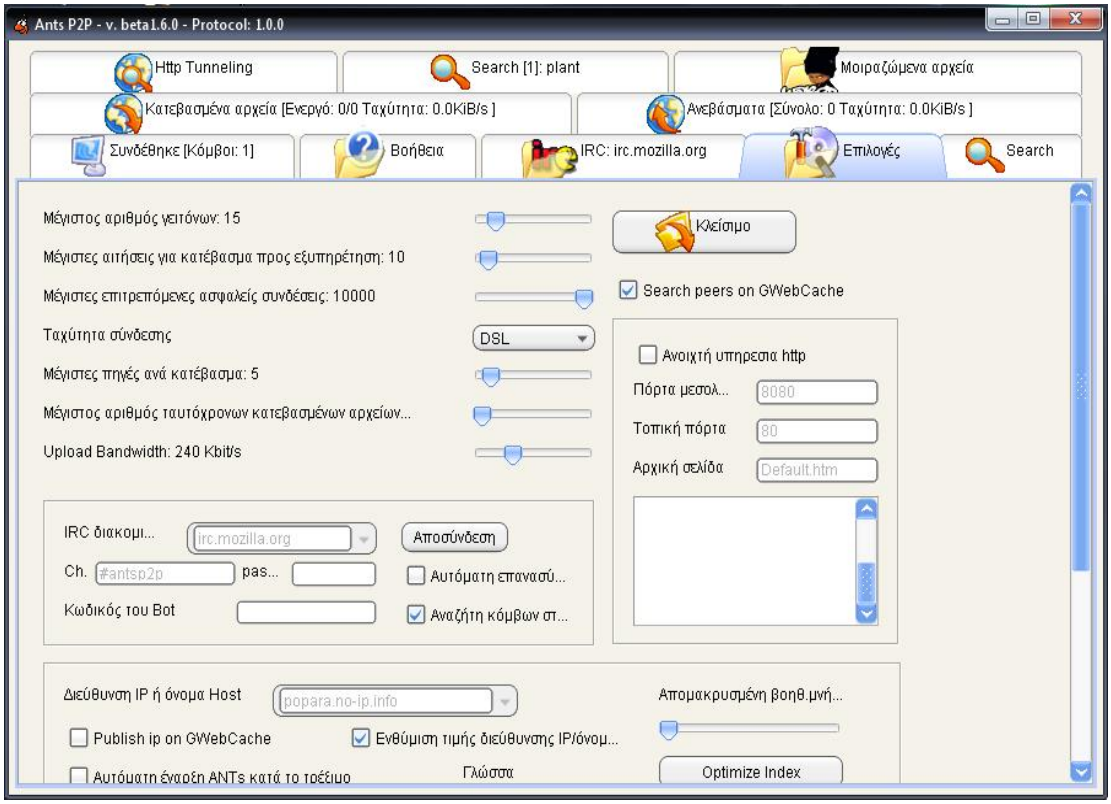
Από το σημείο αυτό και μετά μπορούμε να τρέξουμε την εφαρμογή και να αναζητήσουμε αρχεία.

Παρακάτω βλέπουμε το αρχικό παράθυρο της εφαρμογής όπου φαίνεται το ψευδώνυμο και η IP που χρησιμοποιείτε καθώς και η πόρτα στην οποία ακούει. Επίσης φαίνεται το ποσοστό των αρχείων που ανεβάζει και κατεβάζει. Από εδώ γίνεται και η διακοπή και έξοδος της εφαρμογής.



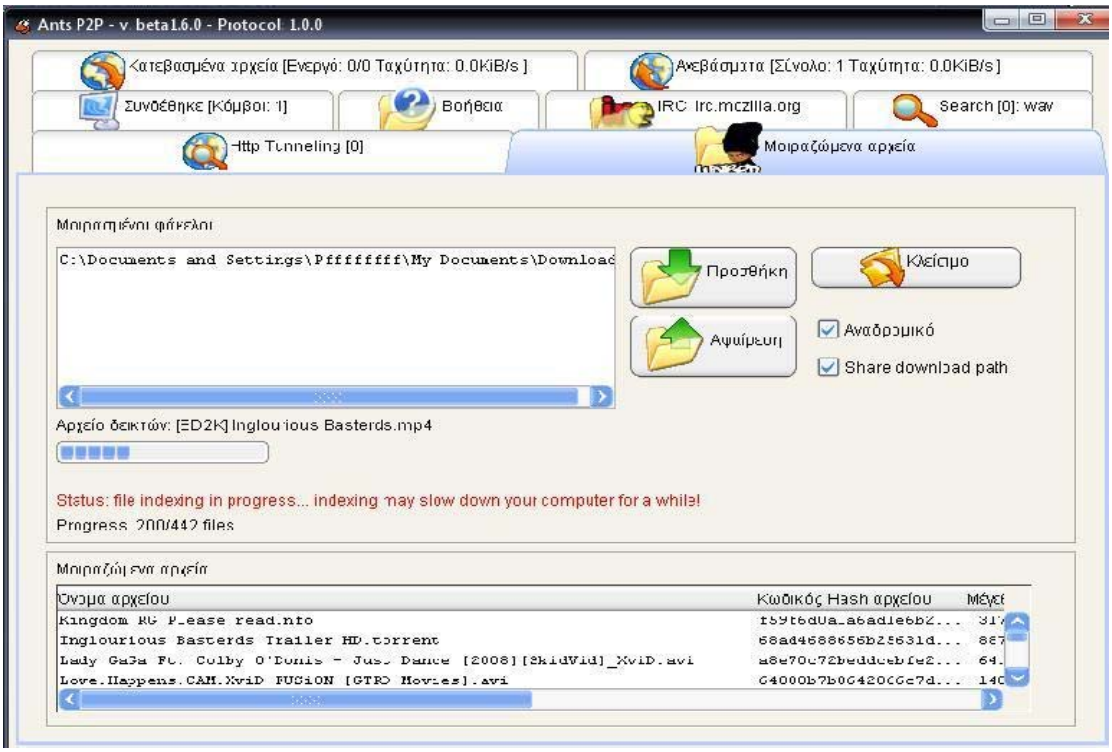
Εικόνα 92 AntsP2P: Σύνδεση κόμβου

Αν πατήσουμε πάνω στο κουμπί 'Επιλογές' εμφανίζεται το παρακάτω παράθυρο όπου εδώ μπορούμε να κάνουμε κάποιες αλλαγές στις ρυθμίσεις πάνω στο δίκτυό μας.



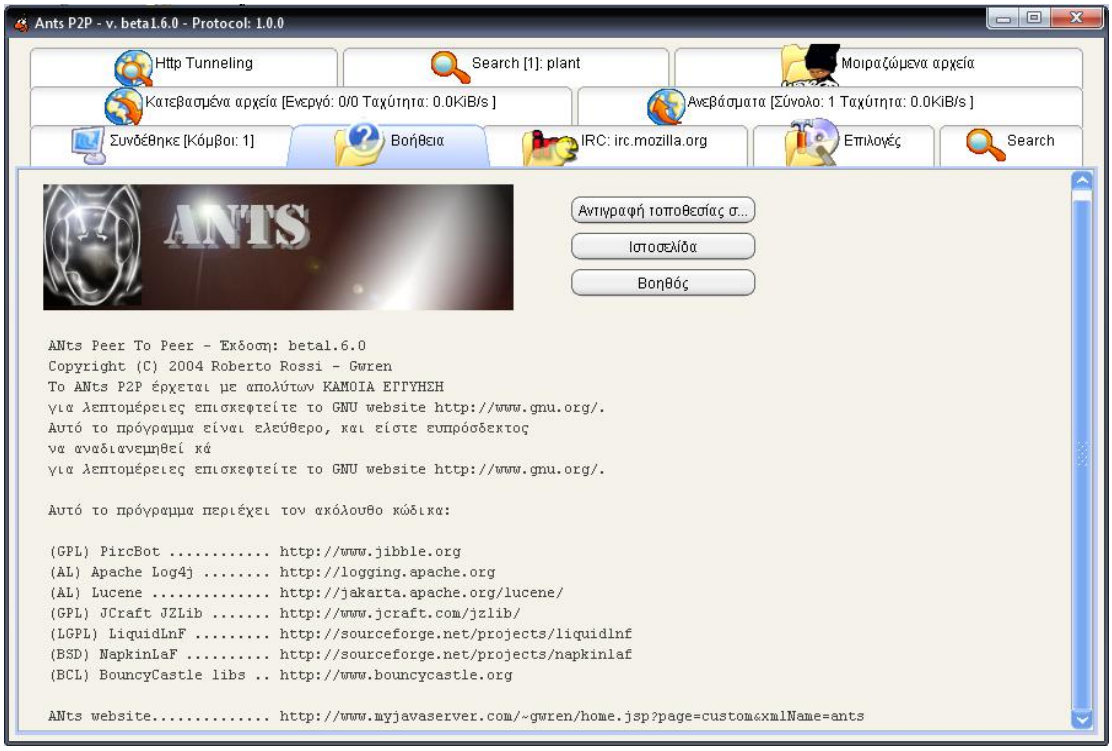
Εικόνα 93 AntsP2P: Επιλογές

Στο παράθυρο ‘Μοιραζόμενα αρχεία’ έχουμε την δυνατότητα να προσθέσουμε ή να αφαιρέσουμε αρχεία που θέλουμε να μοιραστούμε.



Εικόνα 94 AntsP2P: Μοιραζόμενα αρχεία

Σε περίπτωση που συναντήσουμε κάποια δυσκολία κατά την εκτέλεση της εφαρμογής μπορούμε ανοίξουμε το παράθυρο ‘Βοήθεια’ το οποίο μας παραπέμπει στο internet.



Εικόνα 95 AntsP2P: Βοήθεια

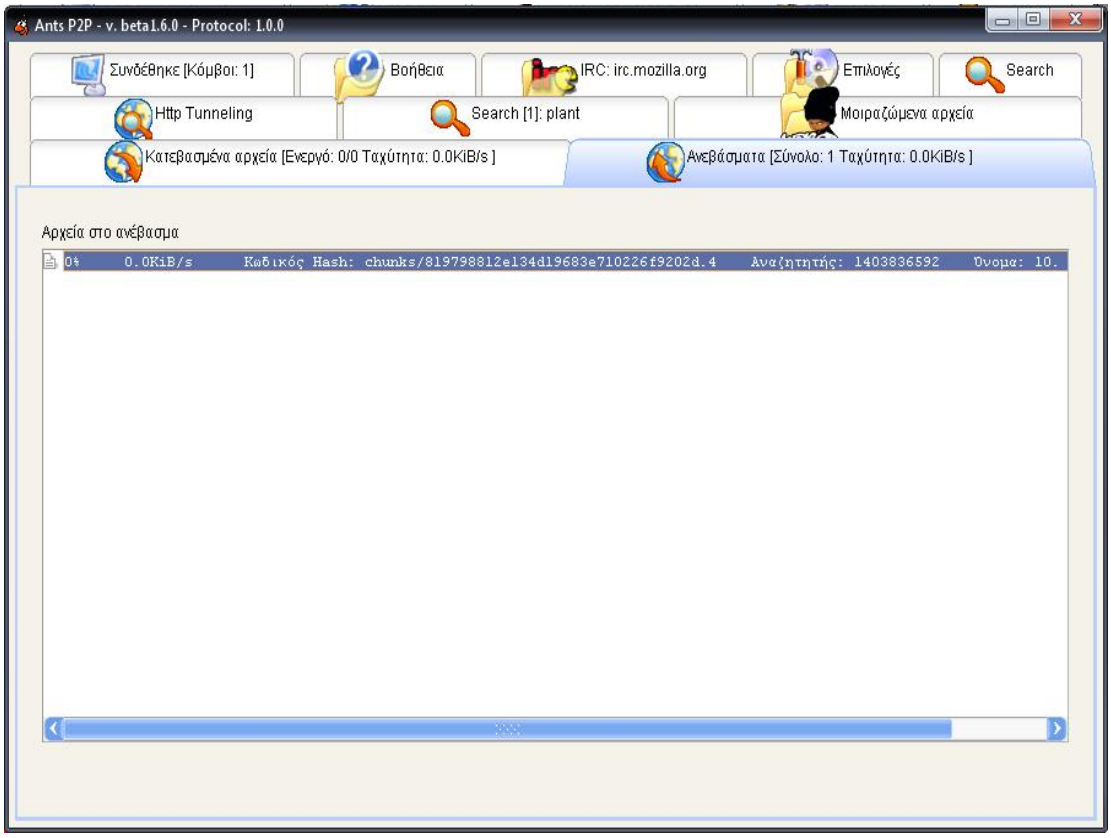
Παρακάτω αναζητάμε το αρχείο mp3. Αφού πληκτρολογήσουμε το ζητούμενο όνομα αρχείου κάνουμε κλικ στο 'Αναζήτηση με λέξη' και ξεκινάει η αναζήτηση. Αφού βρει αρχεία που εμπεριέχουν την λέξη που πληκτρολογήσαμε εμφανίζει τα ονόματα των αρχείων που βρήκε και το μέγεθός τους.

Εικόνα 96 AntsP2P: Search

Στο παράθυρο 'Κατεβασμένα αρχεία' βλέπουμε τα αρχεία που κατεβάσαμε από την παραπάνω αναζήτηση.

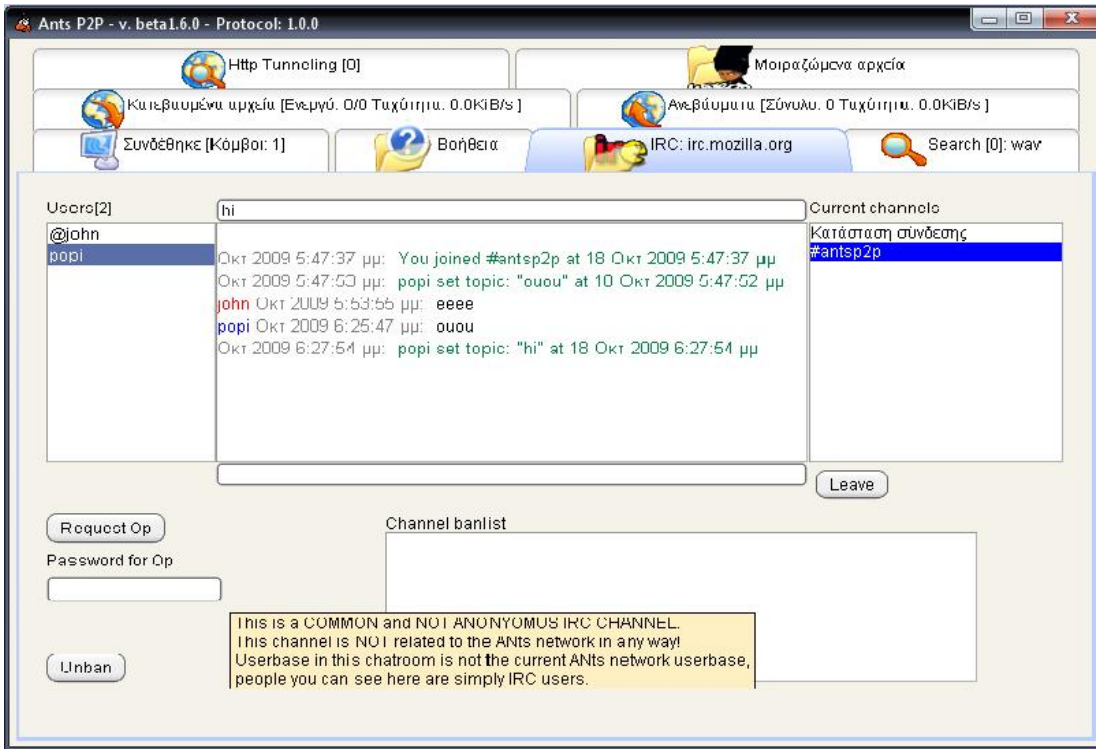
Εικόνα 97 AntsP2P: Κατεβασμένα αρχεία

Στο παράθυρο 'Ανεβάσματα' βλέπουμε τα αρχεία που έχουν πάρει από εμάς.



Εικόνα 98 AntsP2P: Ανέβασμα αρχείων

Το IRC είναι ένα δωμάτιο συνομιλίας όπου μπορείς να ανταλλάξεις μηνύματα με κάποιο χρήστη ενός κόμβου με τον οποίο έχουμε συνδεθεί.



Εικόνα 99 AntsP2P: Δωμάτιο συνομιλίας

Το ANts P2P προστατεύει την ιδιωτικότητά των χρηστών και τους καθιστά μη ανιχνεύσιμους, κρύβοντας την ταυτότητά τους και κρυπτογραφώντας όσα αρχεία στέλνονται ή λαμβάνονται.[110]

Το ANts P2P είναι:

- Ένα μικρό, υπό ανάπτυξη, δίκτυο.
- Είναι αργό στο να συνδέσει, να βρει και να ανεβάσει ή να κατεβάσει αρχεία, αλλά αυτό είναι το 'τίμημα' για να πετύχει την ανωνυμία.
- Υπάρχουν λίγα αρχεία διαθέσιμα.
- Τα αρχεία έχουν μόνο λίγες πηγές, μερικές φορές μόνο μια.
- Υπάρχει πιθανότητα να μην βρούμε αυτό που ψάχνουμε.

[110] http://antsp2p.altervista.org/

Κεφάλαιο 6 Ανώνυμοι remailers

6.1 Anonymous remailers

6.1.1 Λειτουργία anonymous remailers

Ένας τρόπος μέσω του οποίου επιτυγχάνεται η ανωνυμία στο δίκτυο είναι οι ανώνυμοι remailers. Οι ανώνυμοι remailers είναι υπηρεσίες προώθησης και δρομολόγησης ηλεκτρονικού ταχυδρομείου με μία ουσιώδη ωστόσο διαφορά από τους κλασσικούς mail servers.[111] Ο ανώνυμος remailer στέλνει το μήνυμα αυτούσιο, αφαιρώντας όμως πρώτα όλες τις επικεφαλίδες που σχετίζονται με την ταυτότητα του αποστολέα.

Στη συνέχεια, ο παραλήπτης, είτε πρόκειται για άτομο, είτε για newsgroup, όπως συνήθως συμβαίνει, διαβάζει το μήνυμα, και πολλές φορές μπορεί να απαντήσει απευθείας στον αποστολέα, χωρίς όμως να γνωρίζει ή να μπορεί να μάθει κάτι για την ταυτότητά του. Ο ιδιοκτήτης του ανώνυμου remailer συνήθως τα γνωρίζει αυτά, τουλάχιστον την πραγματική e-mail διεύθυνση του αποστολέα, και τα διατηρεί σε μια μεγάλη βάση δεδομένων.

Αυτή χρησιμεύει κυρίως στο να δίνεται η δυνατότητα στον παραλήπτη να απαντά απευθείας στον αποστολέα, χωρίς πάντα να παραβιάζεται η ανωνυμία του τελευταίου. Το γεγονός της ύπαρξης μιας τέτοιας βάσης δεδομένων λογικά θα έπρεπε να αποθαρρύνει τους επίδοξους χρήστες της υπηρεσίας, η τεράστια επιτυχία όμως του anon.penet.fi, του πιο διάσημου ανώνυμου remailer στην ιστορία, πλέον του Internet απέδειξε το ακριβώς αντίθετο. Επίσης, σχεδόν κάθε ISP (Internet Service Provider) μπορεί να ελέγξει και να σώσει κάθε e-mail χωρίς να το γνωρίζουν οι χρήστες.

Σε πολλές χώρες οι ISPs ελέγχονται κυρίως από πράκτορες της κυβέρνησης.[112] Το 1980 ο Karl Kleinpaste ίδρυσε έναν pseydonymous server για το Usenet. Το 1992 εγκαθιδρύθηκε ο πλέον πιο γνωστός pseydonymous server, ο anon.penet.fi από τον Johan "Julf" Helsingius. Επίσης το 1992 μια ομάδα από κρυπτογράφους, η οποία αποκαλούνταν Cypherpunks, και μέλη της ήταν ο Eric Hughes και ο Hal Finney, δημιούργησαν ένα ανώνυμο σύστημα για e-mails, τον γνωστό Cypherpunk remailer. Στη συνέχεια ο Lance Cottrell προσπάθησε να βελτιώσει τον Cypherpunk και δημιούργησε τον Mixmaster.

Μέχρι τα τέλη της δεκαετίας του '90, ένας remailer μας επέτρεπε να στείλουμε e-mails σε μια ομάδα του Usenet ή σε κάποιον που δεν θα έπρεπε να αποκαλύψουμε το αληθινό μας όνομα ή την διεύθυνση του ηλεκτρονικού μας ταχυδρομείου.[113] Σήμερα, οι web based remailers μας επιτρέπουν να στείλουμε e-mail χρησιμοποιώντας την

---

[111] http://www.it.uom.gr/project/MultimediaTechnologyNotes/extra/append10.htm
[112] www.cosy.sbg.ac.at/~held/teaching/wiss.../Remailer_Slides.pdf
[113] http://www.andrebacard.com/remail.html

αληθινή μας ταυτότητα, εάν θέλουμε, όπως επίσης μας προστατεύουν από τους τυχόν κατασκόπους που παρακολουθούν τις διαδικτυακές μας συναλλαγές.

6.1.2 Τύποι remailers

Υπάρχουν πολλές στρατηγικές που συμβάλλουν στο να φτιαχτεί ένα e-mail περισσότερο ή λιγότερο ανώνυμα.[114] Σε γενικές γραμμές, διάφορες κατηγορίες ανώνυμων remailers διαφέρουν όσον αφορά τις επιλογές που έχουν κάνει οι σχεδιαστές τους. Οι επιλογές αυτές μπορούν να επηρεαστούν από τις νομικές επιπτώσεις της λειτουργίας των συγκεκριμένων τύπων remailers.

Θα πρέπει να γίνει κατανοητό, ότι κάθε πακέτο δεδομένων που δρομολογείται στο internet περιέχει τη διεύθυνση του κόμβου, δηλαδή μια ροή bit της IP, όπως επίσης και τις διευθύνσεις τόσο του αποστολέα όσο και του αποδέκτη, κι έτσι κανένα πακέτο δεδομένων δεν μπορεί να είναι πάντα ανώνυμο σε αυτό το επίπεδο. Παρόλα αυτά, αν η IP είναι λάθος, τότε δεν υπάρχει τρόπος ώστε να εντοπιστεί εύκολα ο πραγματικός κόμβος ή ακόμα και η αυθεντικότητα του μηνύματος.

Επιπλέον, όλες ο προδιαγραφές με βάση τα μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν τα πεδία που ορίζονται στις κεφαλίδες τους, κατά τα οποία η πηγή και οι διαβιβαστές φορέων του internet, είναι υποχρεωτικό να συμπεριληφθούν. Ωστόσο επειδή οι περισσότεροι χρήστες του ηλεκτρονικού ταχυδρομείου δεν έχουν πολύ τεχνική εμπειρογνωμοσύνη, οι πλήρης κεφαλίδες των μηνυμάτων συνήθως αποσιωπούνται από λογισμικό ανάγνωσης mail. Και για αυτό το λόγο πολλοί χρήστες δεν έχουν δει ούτε ένα.

Ορισμένοι remailers αλλάζουν και τους δύο τύπους της διεύθυνσης του μηνύματος που προωθούν, καθώς και τη λίστα των κόμβων διαβίβασης όσο το μήνυμα προωθείται. Η IP διεύθυνση της πηγής για το πακέτο μπορεί να προέρχεται από τον ίδιο τον remailer μέσα σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο αποτελείται από διαφορετικά πακέτα, κι έτσι μετονομάζει τον χρήστη στον server που διέρχεται. Κάποιοι remailers μπορούν και προωθούν τα ανώνυμα e-mails σε άλλους remailers, και μόνο μετά από αρκετά τέτοια βήματα το e-mail έχει παραδοθεί στην προοριζόμενη διεύθυνση.

Υπάρχουν 4 είδη remailers:

- Nym servers ή αλλιώς Pseydonymous remailers, όπου απλά στερούν την ηλεκτρονική διεύθυνση του αποστολέα δίνοντας ένα ψευδώνυμο σε αυτόν και στέλνουν το μήνυμα προς τον αποδέκτη.

- Cypherpunk anonymous remailers οι οποίοι αποκαλούνται τύπου 1. Στέλνουν το μήνυμα κατευθείαν στον προοριζόμενο παραλήπτη και δεν μπορούμε να απαντήσουμε στο μήνυμα που αποστέλλεται μέσω αυτού του remailer. Συνήθως μπορούμε να αποκρυπτογραφήσουμε το μήνυμα που στάλθηκε προς τον remailer, και ο remailer να αποκρυπτογραφήσει και να αποστείλει το μήνυμα στην διεύθυνση που κρύβεται στο κρυπτογραφημένο μήνυμα.

[114] http://en.wikipedia.org/wiki/Anonymous_remailer

Χρησιμοποιούν τα δοσμένα public keys για να κρυπτογραφήσουν τα εισερχόμενα μηνύματα, ενώ παρέχουν anonymous e-mail μέσα από την χρήση των reply blocks. Η κρυπτογράφηση γίνεται με PGP (Pretty Good Encryption) ή GPG (GNU Privacy Guard), ή μερικές φορές το μήνυμα προωθείται με το να αφαιρούνται οποιεσδήποτε πληροφορίες από τις κεφαλίδες. [115]

- Mixmaster anonymous remailers, οι οποίοι αποκαλούνται τύπου 2. Διακρίνονται από όλα τα χαρακτηριστικά των Cypherpunks σε συνδυασμό με:

  - το καθορισμένο σταθερό μέγεθος των μηνυμάτων.
  - την ανακατανομή τους.
  - τη μη σταθερή καθυστέρηση κατά την μεταφορά τους από hop σε hop.

Απαιτούν την χρήση ενός προγράμματος για να γράψουμε τα μηνύματά μας. Τέτοια προγράμματα δεν παρέχονται ως πρότυπο για τα περισσότερα λειτουργικά συστήματα ή τα συστήματα διαχείρισης mail. Επίσης στέλνουν τα μηνύματα σε καθορισμένα πακέτα έτσι ώστε να είναι δύσκολος ο εντοπισμός τους. [116]

- Mixminion remailers, οι οποίοι αποκαλούνται και τύπου 3. Ένας τέτοιος remailer προσπαθεί να εντοπίσει τις ακόλουθες προκλήσεις στον Mixmaster remailer: απαντήσεις, προώθηση ανωνυμίας, πρόληψη απάντησης και εναλλαγή κλειδιού, ολοκληρωμένο κατάλογο servers, exit policies και εικονική κίνηση .

Καθένας από αυτούς τους τύπους απευθύνεται σε ξεχωριστό κοινό.[117] Συγκεκριμένα, ο πρώτος απευθύνεται κυρίως σε αρχάριους χρήστες που επιθυμούν μία μέθοδο επικοινωνίας ασφαλέστερη εκείνης που προσφέρει ο mail server του ISP τους (ή οι παροχείς Web mail), ο δεύτερος σε κοινό με μεγαλύτερες απαιτήσεις σε θέματα ασφαλείας και ο τρίτος στους σκληροπυρηνικούς θιασώτες της ασφάλειας και της ανωνυμίας στο Internet.

Message format για Cypherpunk anonymous remailer [118]

::
[Remailer directives]
##
[Hash headers]
[Message text]

Παράδειγμα μηνύματος:

::
ANON-TO: final@recipient.com
Latent-Time: +1:00

---

[115] http://en.wikipedia.org/wiki/Cypherpunk_anonymous_remailer
[116] http://en.wikipedia.org/wiki/Mixmaster_anonymous_remailer
[117] http://www.go-online.gr/ebusiness/specials/article.html?article_id=420
[118] www.cosy.sbg.ac.at/~held/teaching/wiss.../Remailer_Slides.pdf

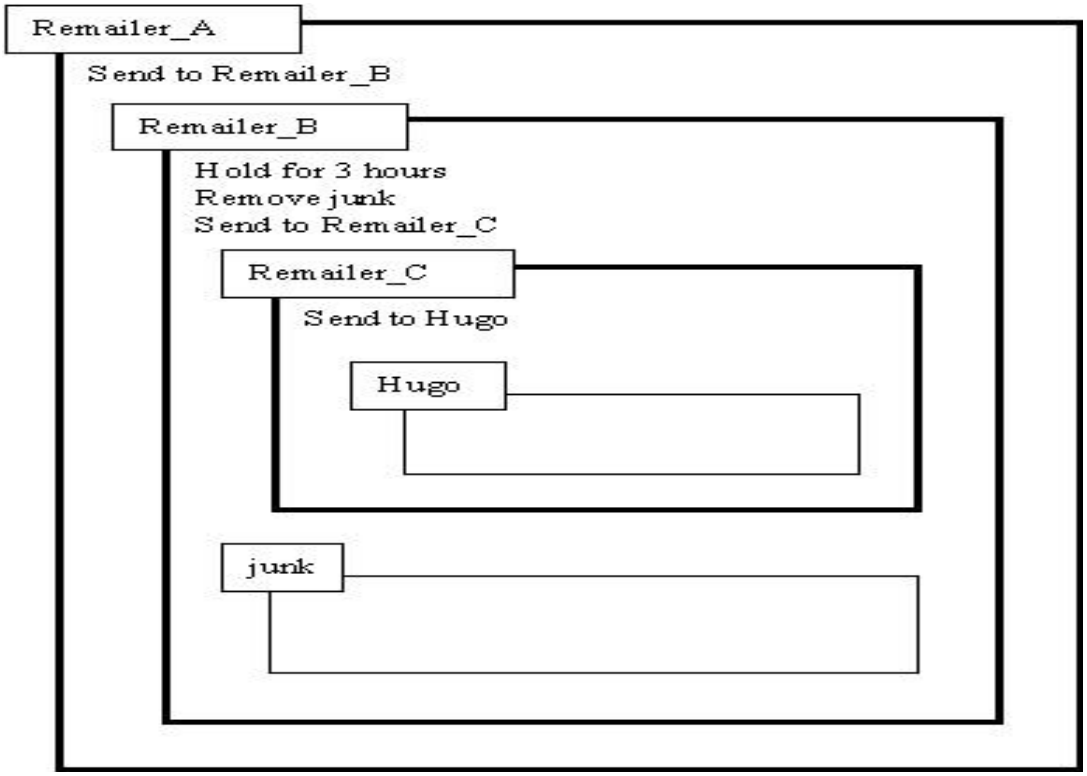
##
Subject: This is an anonymous message example
This ist the text of the

Είναι σημαντικό στο πεδίο ANON-TO να βάλουμε τη διεύθυνση του remailer και να αφήσουμε το πεδίο subject κενό.

Επίσης είναι σημαντικό να χρησιμοποιήσουμε PGP κρυπτογράφηση εάν ο remailer την υποστηρίζει.

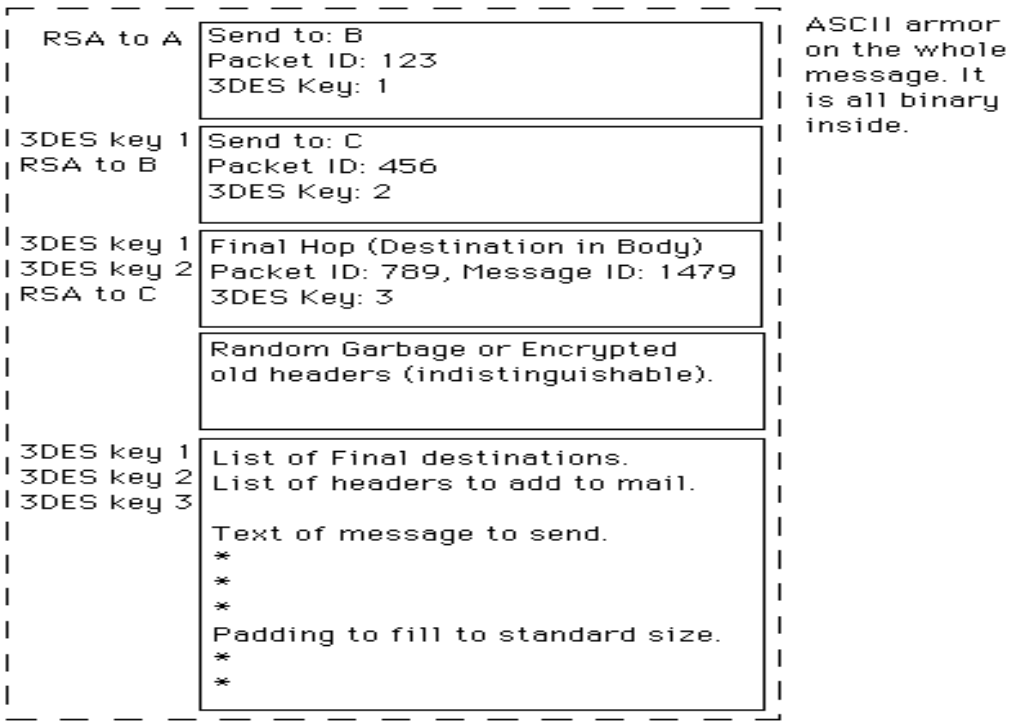
Παράδειγμα κρυπτογραφημένου μηνύματος:
::
Encrypted: PGP
—BEGIN PGP MESSAGE—
Version: 2.6.2
ahfjkadhflakhfjadf. . .
—END PGP MESSAGE——

Η μαύρη γραμμή μετά το πεδίο Encrypted: PGP είναι απολύτως απαραίτητη.



Εικόνα 100 Message

Όσον αφορά τα μηνύματα του Mixmaster remailer, είναι κρυπτογραφημένα με αλγορίθμους RSA και 3DES, και χρησιμοποιείται ένα κλειδί για κάθε remailer.



Εικόνα 101 Mixmaster message format

6.1.3 Ανιχνεύσιμοι remailers

Ορισμένοι remailers δημιουργούν μια εσωτερική λίστα από ενεργούς αποστολείς και εφεύρουν ονόματα έτσι ώστε ο παραλήπτης να μπορέσει να στείλει mail στο invented name AT some_remailer.net.[119] Όταν λαμβάνει την κίνηση σε αυτόν τον χρήστη, ο server λογισμικού συμβουλεύεται αυτόν τον κατάλογο, και προωθεί το mail στον προοριζόμενο παραλήπτη, επιτρέποντας έτσι την ανωνυμία, αν και με ανιχνεύσιμη πρόσβαση στο κατάλογο, και έτσι επιτυγχάνεται αμφίδρομη επικοινωνία. Ο γνωστός penet.fi remailer στη Φιλανδία το έκανε αυτό για αρκετά χρόνια και τον αναλύουμε παρακάτω.

Οι πιο πρόσφατοι σχεδιασμοί remailers χρησιμοποιούν την κρυπτογραφία με σκοπό να παρέχουν περισσότερο ή λιγότερο την ίδια υπηρεσία, όμως χωρίς τόσο μεγάλο κίνδυνο να χάσουν την εμπιστευτικότητα του χρήστη. Πρόκειται γενικά για τους nym remailers ή pseydonymous remailers. Ο βαθμός στον οποίο εξακολουθούν να είναι ευάλωτοι στο να εντοπιστούν από την αστυνομία, είναι και παραμένει ασαφή, δεδομένου ότι οι νέες εξελίξεις κρυπτανάλυσης προχωρούν με γρήγορους ρυθμούς.

6.1.4 Μη ανιχνεύσιμοι remailers

Αν οι χρήστες έχουν δεχθεί την απώλεια της αμφίδρομης επικοινωνίας, η ανωνυμία μπορεί να επιτευχτεί πιο σίγουρα. Με το να μη κρατούν καμία λίστα από χρήστες και τις αντίστοιχες κεφαλίδες, ο remailer μπορεί να μας διαβεβαιώσει ότι κανένα μήνυμα δεν αφήνει καμία εσωτερική πληροφορία να διαρρεύσει κατά την προώθησή του, και

[119] http://en.wikipedia.org/wiki/Anonymous_remailer

να έχει ως αποτέλεσμα αργότερα τον τερματισμό του απορρήτου. Ωστόσο, τα μηνύματα καθ' όλη τη διάρκεια της μεταφοράς τους ανάμεσα στους servers, παραμένουν ευπαθή. Όπως και η σύγκριση της ανάλυσης κυκλοφορίας προς και από έναν τέτοιο server, μπορεί να δείχνει πολύ παραπάνω από ότι είναι στη πραγματικότητα.

Η στρατηγική των Mixmaster έχει σχεδιαστεί έτσι ώστε να αποτρέπει τέτοιες επιθέσεις. Αν κάθε μήνυμα περνά από διαφορετικούς servers, πχ σε διαφορετικές νομικές και πολιτικές δικαιοδοσίες, τότε οι επιθέσεις βασίζονται σε νομικά συστήματα και γίνονται πιο δύσκολες, έστω και μόνο από την προστριβή Clausewitzian ανάμεσα σε δικηγόρους, δικαστήρια, διαφορετικά καταστατικά, οργανωτικές αντιπαλότητες, νομικά συστήματα κλπ. Και από τότε που η κατάσταση περιπλέκεται με πολλούς servers, γίνεται περισσότερο αποτελεσματική δεδομένου κανένας δεν είναι διατεθειμένος να σπάσει μια ολόκληρη αλυσίδα από remailers.

Το τυχαίο padding, δηλαδή ο αριθμός των κρυπτογραφήσεων που έχει δεχθεί ένα μήνυμα, τυχαία καθυστερεί την προώθησή του, και η κρυπτογράφηση μεταξύ των remailers που προωθούν το μήνυμα, αυξάνει ραγδαία το βαθμό δυσκολίας ώστε να εντοπιστεί το μήνυμα από επιτιθέμενους, και την ίδια χρονική στιγμή μπορούν να εξαλειφθούν όλες οι πληροφορίες ένδειξης της κίνησης, με αποτέλεσμα η έλλειψη ανάγνωσης της διαβίβασης των πληροφοριών να κατορθώνεται από τους αλγορίθμους ανάλυσης κυκλοφορίας.

6.1.5 Διαφορά anonymous και pseydo anonymous remailer

Οι περισσότεροι άνθρωποι χρησιμοποιούν την έκφραση «anonymous remailer» σαν μια σύντομη περιγραφή δύο διαφορετικών τύπων remailer.[120] Ένας pseydo anonymous remailer βασίζεται στην σχέση εμπιστοσύνης. Ο remailer SecretBacard.com είναι ένας pseydo anonymous remailer. Πρέπει να εμπιστευτούμε ότι αυτός ο remailer προστατεύει όλα τα αρχεία μας. Επιπλέον, θα πρέπει να συνειδητοποιήσουμε ότι όλες οι συναλλαγές μας με το SecretBacard.com μπορούν να είναι:

- Καταγραφή από δεκάδες servers του internet μεταξύ του υπολογιστή μας και του SecretBacard.com.
- Καταγραφή από τον υπολογιστή του SecretBacard.com.
- Σύνδεση με το τηλεφωνικό νούμερο που χρησιμοποιούμε για να έχουμε πρόσβαση στο internet.

Πρακτικά, υπάρχουν λογικά όρια που θα πρέπει να φτάνει η εμπιστοσύνη μας. Μπορεί κάποιος να πάρει μια δικαστική απόφαση και να μπορέσει να βρει την αληθινή μας ταυτότητα μέσω του pseydo anonymous remailer. Η φιλανδική αστυνομία ανάγκασε τον Julf Helsingius, ο οποίος είναι δημιουργός remailer, να αποκαλύψει τουλάχιστον ενός ατόμου την αληθινή ταυτότητά του. Αυτή η νόμιμη πράξη ανάγκασε τον Julf να κλείσει τον remailer του. Το πλεονέκτημα των περισσοτέρων pseydo anonymous remailers είναι ότι έχουν εύκολη χρήση ως προς

[120] http://www.andrebacard.com/remail.html

τον χρήστη. Αν μπορούμε να στείλουμε ένα e-mail, τότε πιθανώς θα μπορούμε να καταλάβουμε και τους pseydo anonymous remailers.

Οι αληθινοί anonymous remailers είναι ένα διαφορετικό κομμάτι. Αν χρησιμοποιούνται σωστά, μπορούν να παρέχουν καλύτερη ιδιωτικότητα από ότι ένας pseydo anonymous remailer. Γενικά, είναι πιο δύσκολοι σε χρήση. Οι anonymous remailers χρησιμοποιούνται κυρίως από προγραμματιστές και αυτούς που αγαπούν το τεχνικό μέρος του internet. Οι άνθρωποι τείνουν να χρησιμοποιήσουν αυτούς τους remailers για να στείλουν αμφισβητούμενα μηνύματα σε αμφισβητούμενες ομάδες του Usenet.

Αυτοί που θέλουν την μέγιστη δυνατή μυστικότητα στέλνουν το e-mail τους μέσω 3 ή περισσοτέρων remailers. Αυτό σημαίνει ότι, κανένας χειριστής remailer, κανένας χειριστής internet υπολογιστών και κανένας που κατασκοπεύει, δεν θα μπορέσει να διαβάσει την προέλευση του ηλεκτρονικού μας ταχυδρομείου και τον προορισμό. Επιπλέον, πολλοί remailers έχουν και επιλογές χρονικής καθυστέρησης (time delays). Για παράδειγμα, μπορούμε να πούμε στον remailer να κρατήσει το μήνυμά μας για μια ώρα πριν πάει στον επόμενο remailer. Πρακτικά, κανείς δεν μπορεί να αναγκάσει τον χειριστή του anonymous remailer να αποκαλύψει την ταυτότητά μας, γιατί ο χειριστής δεν έχει ιδέα ποιος είμαστε. Επίσης όλα τα e-mail μηνύματα που δρομολογούνται κρυπτογραφούνται.

6.1.6 Web based mailer

Υπάρχουν επίσης υπηρεσίες του διαδικτύου που μας αφήνουν να στέλνουμε ανώνυμα e-mail.[121] Αυτές οι υπηρεσίες δεν παρέχουν ανωνυμία αληθινών remailers, αλλά είναι εύκολες σε χρήση. Όταν χρησιμοποιούμε ένα web based ανώνυμο e-mail ή μια υπηρεσία ενός ανώνυμου remailer, θα πρέπει πρώτα να ελέγξουμε την εγκυρότητα αυτής της υπηρεσίας, πριν αποφασίσουμε να κάνουμε αποστολή του e-mail.

6.1.7 Χρησιμοποιώντας έναν remailer

Αν το αντικείμενο είναι η ταυτότητα της ανωνυμίας, τίποτα που στέλνεται μέσω ενός remailer δεν περιλαμβάνει πληροφορίες αναγνώρισης από έναν εξωτερικό παρατηρητή. Έτσι λοιπόν, αν κάποιος στείλει ένα μήνυμα πχ. Από: anon(At)remailer.net ‘Γεια σου φίλε, στείλε μου το καινούργιο τεύχος του comic στην διεύθυνση Καλοκαιρινού 158 Ηράκλειο Κρήτης Σε ευχαριστώ’, είναι προφανές εντελώς μη ασφαλές.

Κάποιο λογισμικό, πχ η πρόσφατη έκδοση του Microsoft office, περιλαμβάνει πληροφορίες αναγνώρισης σε κάθε αρχείο που αποθηκεύει. Αυτές οι πληροφορίες μπορούν να είναι το όνομα, η διεύθυνση ηλεκτρονικού ταχυδρομείου, το serial number του προϊόντος, ή η Mac διεύθυνση του υπολογιστή. Ένα πρόγραμμα λογισμικού μπορεί να ισχυρίζεται ότι μπορεί να αφαιρέσει τέτοιες πληροφορίες, όμως πρέπει να σημειώσουμε ότι υπάρχουν περίπου 30 διαφορετικά είδη format αρχείων στο Word.

---

[121] http://en.wikipedia.org/wiki/Anonymous_remailer

Αυτοί που ενδιαφέρονται για ανωνυμία, θα πρέπει να περιορίζονται σε μηνύματα απλού κειμένου, με χαρακτήρες ASCII μόνο, που προέρχονται από επεξεργασία απλών προγραμμάτων, όπως το Notepad, το οποίο δεν περιλαμβάνει τέτοιες κρυφές πληροφορίες. Διαφορετικά, οι χρήστες θα πρέπει να είναι ιδιαίτερα προσεκτικοί με αρχεία όπως κειμένου, εικόνων και ήχου, προκειμένου να σιγουρευτούν ότι δεν περιέχουν πληροφορίες αναγνώρισης. Πρέπει να σημειώσουμε ότι, ακόμα και να γίνεται έλεγχος byte by byte, δεν είναι απαραίτητο ότι αυτές οι πληροφορίες θα αποκαλυφθούν, δεδομένου ότι μπορούν εύκολα να κρυπτογραφηθούν, ή να αποκρυπτογραφηθούν με στεγανογραφία.

Η ανωνυμία, σχεδόν ποτέ δεν μπόρεσε να ξανακερδίσει αυτούς που ενδιαφέρονται για την παραβίαση του απορρήτου, γιατί υπάρχουν αρχεία με τέτοιες ανακαλύψεις. Αυτά τα αρχεία τυπικά είναι πολύ παλιά, ειδικά αν τα κρατούν αυτοί που ασχολούνται με την κυβέρνηση ή αυτοί που έχουν κοινωνικά και πολιτικά ενδιαφέροντα. Αυτό, για μερικές απόψεις, μπορεί να έχει σοβαρές συνέπειες.

6.1.8 Επιλέγοντας έναν remailer

Δεν είναι όλοι οι ανώνυμοι remailers το ίδιο, ακόμα και αν υπάρχουν διαδικασίες που πρέπει να γίνουν στο μέλλον. Πρέπει να δώσουμε ιδιαίτερη προσοχή στα επιχειρησιακά πρότυπα και στους στόχους που έχουμε, στην τοποθεσία και την αξιοπιστία αρχείων πριν επιλέξουμε κάποιον. Μερικά από τα κριτήρια που πρέπει να εξεταστούν είναι:

- Η κατηγορία τους, πχ αν διαθέτουν μονόδρομη ή αμφίδρομη δρομολόγηση, αν το περιεχόμενο του μηνύματος είναι κρυπτογραφημένο ή όχι και αν υποστηρίζει Mixmaster ή one hope προώθηση.
- Το ιστορικό τους, πχ σε κάποιους το υλικό και το λογισμικό τους είναι σε καλύτερες συνθήκες από άλλους, ειδικότερα σε θέματα ασφάλειας.
- Η ασφάλεια, πχ κάποια λειτουργικά συστήματα έχουν χειρότερο ιστορικό ασφάλειας.
- Ο διαχειριστής.
- Η ιδιωτικότητα και αρχές λειτουργίας.
- Το λογισμικό που χρησιμοποιεί.
- Η καταγραφή και η φήμη που έχει.

Οι remailers όπως αναφέραμε παραπάνω είναι προηγμένες υπηρεσίες, οι οποίες θα απογυμνώσουν κάθε αναγνωριστική λεπτομέρεια από ένα γράμμα και μετά θα το προάγουν, ανώνυμα και κάτω από ένα ψευδώνυμο, στο προορισμένο αποδέκτη ή στην ομάδα νέων.[122] Η διεύθυνση με ψευδώνυμο που προστίθεται από πολλούς, αλλά όχι όλους, τους ανταποστολείς (remailers), δείχνει ξεκάθαρα ότι το μήνυμα είναι ανώνυμο: ένας remailer [123] και ένας anon- remailer[124] είναι χαρακτηριστικά. Καθώς οι remailers μπορούν να χρησιμοποιηθούν μοχθηρά, η πρωταρχική τους χρήση είναι να προμηθεύουν μυστικότητα.

---

[122] http://hyperion.math.upatras.gr/courses/newcommmedia99-00/papers99-00/donath.html
[123] 12321@anon.penet.fi
[124] remailer@utopia.hacktic.nl

Τα ανώνυμα ταχυδρομεία είναι συχνά σε ομάδες όπου οι συμμετέχοντες αποκαλύπτουν πολύ προσωπικές πληροφορίες και πολλές από τις ομάδες υποστήριξης (π.χ.alt.support.depression) προμηθεύουν περιοδικά οδηγίες για το πως να χρησιμοποιηθεί ένας ανώνυμος ανταποστολέας (remailer). Η χρήση ενός τέτοιου (remailer) μπορεί επίσης να είναι πολιτική έκθεση, μια επιβεβαίωση ότι κάποιος υποστηρίζει το δικαίωμα του πολίτη για μυστικότητα (το οποίο περικλείει ανωνυμία, πρόσβαση σε δυνατά εν-κρυμμένα εργαλεία κλπ.) και αντιτίθεται στην κυβερνητική επιτήρηση και στην επιτήρηση των σωματίων

6.1.9 Remailer penet.fi

Κάποιος που επιθυμεί διακαώς να παραμείνει στην ανωνυμία, δύσκολα θα εμπιστευτεί κάποιον remailer που ανήκει στην κυβέρνηση ή κάποια άλλη έκφραση εξουσίας.[125] Το ίδιο δύσκολα θα εμπιστευτεί κάποιον εμπορικό πάροχο της υπηρεσίας αυτής γνωρίζοντας ότι βασικό του κίνητρο είναι το κέρδος, που μολονότι ως πρακτική είναι γενικά αποδεκτή, δεν αποτελεί και εγγύηση ακεραιότητας.

Στην περίπτωση των ανωνύμων remailers, ο χρήστης ενδιαφέρεται περισσότερο για την προσωπική του ασφάλεια και λιγότερο για την τεχνική αρτιότητα της υπηρεσίας. Τι θα ήταν λοιπόν περισσότερο άξιο εμπιστοσύνης από ένα τέτοιο σύστημα, του οποίου ο ιδιοκτήτης είναι ένας γνωστός ιδεαλιστής που προσφέρει την υπηρεσία χωρίς προσωπικό κέρδος, με έδρα μάλιστα μια από τις πλέον ασφαλείς σε θέματα προστασίας του ιδιωτικού βίου χώρες, τη Φινλανδία, που εκτός των άλλων είναι και μία πραγματικά "ιντερνετική" χώρα αφού το 12% του πληθυσμού της έχει πρόσβαση στο διαδίκτυο.

Σε μια εποχή λοιπόν που οι πιο προχωρημένες και ασφαλείς μορφές ανώνυμης συμμετοχής στο "παζάρι" του κυβερνοχώρου ήταν διαθέσιμες μόνο στους hackers, ο anon.penet.fi, ο ανώνυμος remailer που δημιούργησε το 1992 ο Φιλανδός Julf Helsingius, έκανε θραύση. Οι χρήστες του κάλυπταν όλο το φάσμα των δραστηριοτήτων και αναγκών ανωνυμίας, από φορείς του AIDS που έβρισκαν την ευκαιρία να συζητήσουν με ομοιοπαθείς τους και αντικαθεστωτικούς σε χώρες με ολοκληρωτικά καθεστώτα όπως η Κίνα, μέχρι βέβαια εμπόρους όπλων και παιδικής πορνείας αλλά και προβοκάτορες.

Όπως ήταν αναμενόμενο όμως, πολλοί θα ήταν αυτοί που ενοχλημένοι από κάποια προσωπικά ανώνυμα e-mail ή θιγμένοι από ανώνυμα άρθρα στα newsgroups θα έτρεχαν στον Helsingius πιέζοντάς τον να παραδώσει τα στοιχεία των αποστολέων. Οι φινλανδικές αρχές μάλιστα, τις οποίες ο Helsingius υπολόγιζε ως συμμάχους στο εγχείρημά του δεν τον δικαίωσαν. Ο νόμος περί προστασίας της ιδιωτικής ζωής στη Φινλανδία δεν αναφερόταν πουθενά στο e-mail και συνεπώς αυτό δεν υπόκειται σε προστασία.

Όταν λοιπόν το FBI ζήτησε τη συνεργασία της φινλανδικής αστυνομίας για τον εντοπισμό ενός χρήστη του penet ο οποίος είχε δημοσιεύσει σε newsgroups απόρρητα στοιχεία για την εκκλησία της Σαϊεντολογίας, πίεσε τον Helsingius,

---

[125] http://www.it.uom.gr/project/MultimediaTechnologyNotes/extra/append10.htm

απειλώντας μάλιστα να κατασχέσει τον εξοπλισμό του, πράγμα που θα καθιστούσε ιδιαίτερα επισφαλή τη θέση των περίπου 600.000 χρηστών του.

Έτσι, ο Helsingius παρέδωσε στις αρχές το όνομα του παραβάτη. Όταν το ίδιο σενάριο επανελήφθη ένα χρόνο αργότερα, ο Helsingius αρνήθηκε με αποτέλεσμα να καταλήξει στα δικαστήρια. Αντιλαμβανόμενος όμως την αδυναμία του να εγγυηθεί πλέον την ανωνυμία των χρηστών του, αναγκάστηκε να κλείσει το penet το 1996. Η υπόθεση προκάλεσε σάλο στη φιλελεύθερη φινλανδική κοινή γνώμη. Πέρα από τη φυσιολογική απορία για το πώς μπορούσε μια οργάνωση που λειτουργεί με καθεστώς φοροαπαλλαγής να επικαλείται χρήση "εμπορικά απορρήτων" στοιχείων, το πλήγμα στην ελευθερία του λόγου και το σεβασμό της προσωπικής ζωής ήταν βαρύ. Και προέκυπτε και το παράδοξο ένας Ιάπωνας λόγου χάρη να κρίνεται βάσει της Φινλανδικής νομοθεσίας.

Ο Julf δεν εγκατέλειψε τις προσπάθειες του για τη διασφάλιση των προσωπικών δεδομένων στο Internet και σήμερα, από το Amsterdam που είναι πλέον η μόνιμη κατοικία του, εργάζεται σε συνεργασία με τη φινλανδική κυβέρνηση και την Ευρωπαϊκή Ένωση πάνω σε ένα νομοθετικό πλαίσιο που θα αναγνωρίζει τα δικαιώματα των κυβερνοπολιτών στην "ιδιωτικότητα" και την ανωνυμία, προβλέποντας παράλληλα περιορισμούς αλλά και κυρώσεις για τις περιπτώσεις που οι νόμοι αυτοί θα παραβιάζονται.

6.2 Εργαλεία ανώνυμων remailers

Ο χρήστης ενός απλού, ανώνυμου remailer, όπως ήταν το anon.penet.fi γνωρίζει ότι τα στοιχεία του υπάρχουν σε κάποιο αρχείο στο remailer και πιθανόν να αποκτήσουν πρόσβαση σε αυτά υπηρεσίες ασφαλείας ή και ιδιώτες, ειδικά αν ο χειριστής του συστήματος δεν είναι κάποιος σαν τον Helsingius ή αν τα συστήματα ασφαλείας του remailer δεν είναι ιδιαίτερα αξιόπιστα. Ένας "καλός" hacker ποτέ δεν θα χρησιμοποιούσε έναν ανώνυμο remailer για να καμουφλαριστεί. Φτάνουμε έτσι στην "ισχυρή" ανωνυμία που επιτυγχάνεται με τη χρήση πολλαπλών τέτοιων remailers σε συνδυασμό με ισχυρή κρυπτογράφηση.

Ο κάθε remailer αφαιρεί όλα τα στοιχεία της ταυτότητας του τελευταίου αποστολέα που μπορεί να είναι ο πραγματικός αποστολέας ή ένας άλλος ανώνυμος remailer. Η διαδικασία αυτή επαναλαμβάνεται καθώς το μήνυμα περνάει από remailer σε remailer μέχρι να φτάσει στον τελικό του προορισμό πλήρως "καθαρισμένο". Το μήνυμα είναι κρυπτογραφημένο, όπως και οι διευθύνσεις που αποκρυπτογραφούνται διαδοχικά καθώς περνάει από τους remailers.

Για να ανακαλυφθεί ο πραγματικός αποστολέας θα πρέπει να γίνει μεγάλης κλίμακας έρευνα με συλλογή στοιχείων από όλους του remailers που πήραν μέρος στη μεταγωγή. Αυτό είναι πρακτικά αδύνατο να επιτευχθεί, ειδικά αν ο συγκεκριμένος αποστολέας δεν ακολουθεί συχνά την ίδια "διαδρομή". Εξ' άλλου πολλοί remailers περιμένουν ένα τυχαίο χρονικό διάστημα προτού στείλουν τα μηνύματά τους, ώστε να μην μπορεί να γίνει εύκολα η διασταύρωση των αρχείων καταγραφών που διατηρούνται στον καθένα από αυτούς.

Όλα αυτά βέβαια στερούν τη δυνατότητα να σταλεί απάντηση απ' τον παραλήπτη απ' ευθείας στον αποστολέα, οπότε η χρησιμότητα της μεθόδου περιορίζεται σε

μονόδρομη επικοινωνία ή newsgroups. Τονίζεται ιδιαίτερα η σημασία της ισχυρής κρυπτογράφησης του μηνύματος στην πηγή του αφού μπορεί αυτό να διαβαστεί από κάποιον πριν ακόμη φτάσει στον πρώτο remailer.

Σήμερα υπάρχει μια αρκετά μεγάλη λίστα ανώνυμων ή "ψευδώνυμων" (όπως ο anon.penet.fi) remailers που είναι διαθέσιμοι για αποστολή μηνυμάτων με την παραπάνω μέθοδο. Έχουν αναπτυχθεί μέχρι και πακέτα λογισμικού που κάνουν αυτή τη δουλειά αυτόματα, φέρνοντας έτσι την "ισχυρή" ανωνυμία πιο κοντά στο μέσο χρήστη. Τα γνωστότερα τέτοια προγράμματα είναι το Private Idaho και το John Doe.

Τον τελευταίο καιρό έχουν δημιουργηθεί ακόμα πιο φιλικοί στο χρήστη τρόποι για να στείλει ανώνυμα μηνύματα και μάλιστα μέσω του web (π.χ.στο site ozemail)[126]. Το site προσφέρει κρυπτογραφημένα sessions σε μια προσπάθεια να μειώσει κάπως το ρίσκο που πάντως παραμένει αρκετά μεγάλο για την ανωνυμία του αποστολέα. Όπως επίσης, και το site hoaxmail[127] το οποίο και αυτό παρέχει εργαλεία για να στείλουμε ανώνυμα emails και sms.

Επιπλέον μια άλλη ιστοσελίδα που μπορούμε μέσω αυτής να στείλουμε ανώνυμα emails είναι η hushmail.com[128]. Τα άτομα αυτής της εταιρίας έχουν φέρει την τεχνολογία των remailer σε ένα πιο υψηλό επίπεδο. Η Hushmail δημιουργήθηκε από τον Julf Helsingius στην Φιλανδία το 1993, και έγινε η πρώτη εταιρία που χρησιμοποίησε web based remailer, πλήρη κρυπτογράφηση και φιλικό προς τον χρήστη σύστημα e-mail. Επίσης το site sendfakemail.com[129] προσφέρει πολλές υπηρεσίες όπως anonymous e-mail, secured e-mail, web proxy server, anonymous proxy server, anonymous surfing κλπ.

Όλα αυτά είναι χωρίς αμφιβολία ισχυρά εργαλεία στα χέρια του χρήστη που θέλει να κινείται ελεύθερα στον κυβερνοχώρο, αποφεύγοντας, στο μέτρο του δυνατού, όσους περίεργους επιθυμούν να μπλέκονται στα πόδια του, ανεξάρτητα από το αν έχει κάτι να κρύψει ή όχι.[130] Προκαλεί ωστόσο κάποια ανησυχία η δυνατότητα που δίνεται στα άτομα να κινούνται ανώνυμα στην ψηφιακή κοινωνία. Η υπερβολή στη χρήση της είναι χωρίς αμφιβολία κάθε άλλο παρά υγιής κατάσταση και κανείς δεν γνωρίζει τι αλλαγές μπορεί να επιφέρει στην κοινωνική συμπεριφορά του ατόμου η πλήρης ανωνυμία.

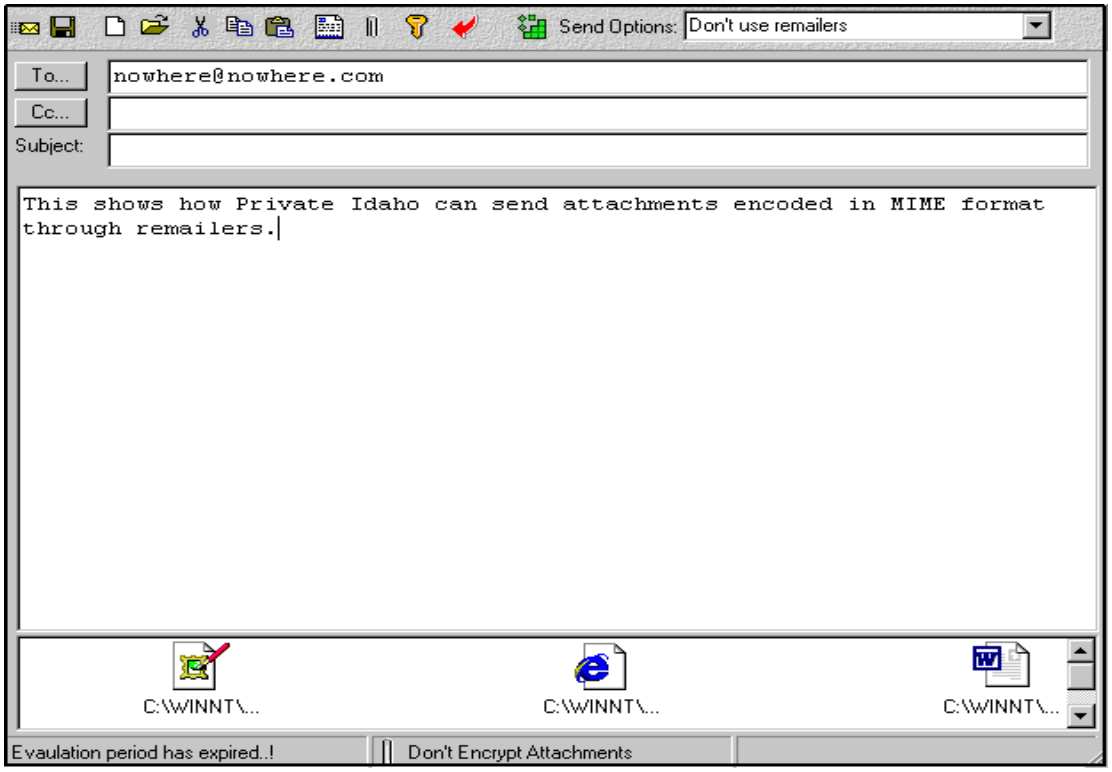
Ποτέ ως τώρα δεν είχε ο άνθρωπος τη δυνατότητα να ενεργεί χωρίς συνέπειες, και έννοιες όπως η καλή έξωθεν μαρτυρία και η διατήρησή της, που αναμφίβολα λειτουργούν ενισχυτικά στην προσαρμογή της ανθρώπινης συμπεριφοράς στις κοινωνικές νόρμες, καταργούνται σε μια ανώνυμη κοινωνία. Η διευκόλυνση που παρέχει η ανωνυμία σε παράνομες δραστηριότητες δεν μπορεί να αγνοηθεί, όπως δεν μπορεί να αγνοηθεί και το γεγονός ότι δύσκολα μπορεί να χτιστεί μια σχέση εμπιστοσύνης μέσα απ' την ανωνυμία και η ελεύθερη αγορά φυσικά δεν είναι δυνατόν να λειτουργήσει και να αναπτυχθεί χωρίς σχέσεις εμπιστοσύνης.

---

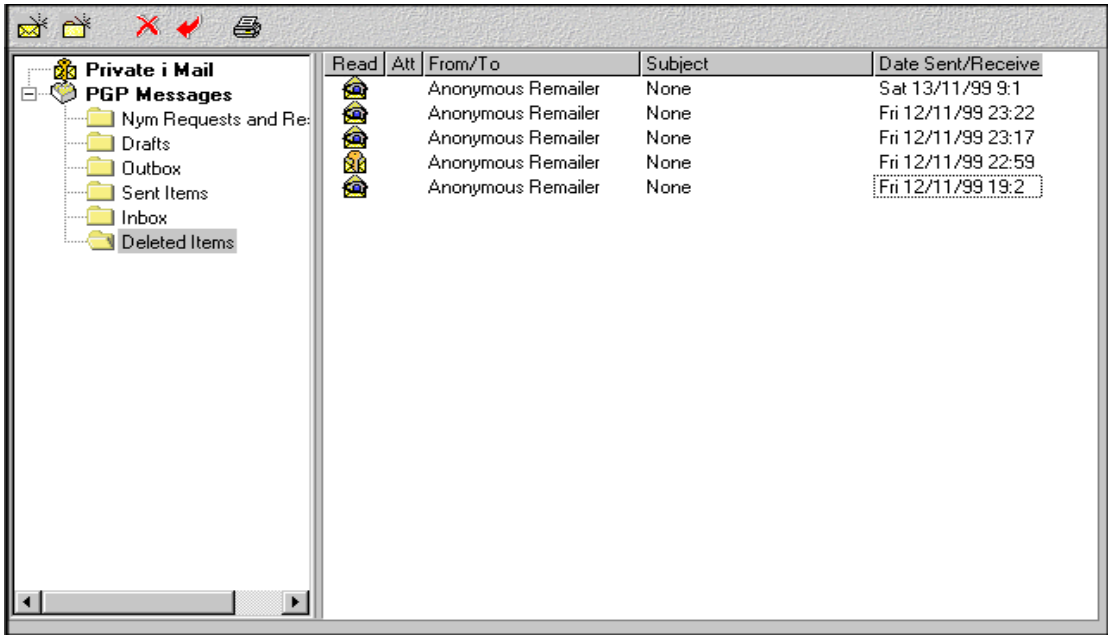
[126] http://www.ozemail.com.au/~geoffk/anon/anon.html
[127] http://www.hoaxmail.co.uk/
[128] www.hushmails.com
[129] http://www.sendfakemail.com/
[130] http://hyperion.math.upatras.gr/courses/newcommmedia99-00/papers99-00/donath.html

6.2.1 Private Idaho

Το πρόγραμμα Private Idaho χρησιμοποιεί PGP κρυπτογράφηση για ισχυρή ανωνυμία και μας δίνει τη δυνατότητα να κάνουμε και χρήση των remailers. [131]

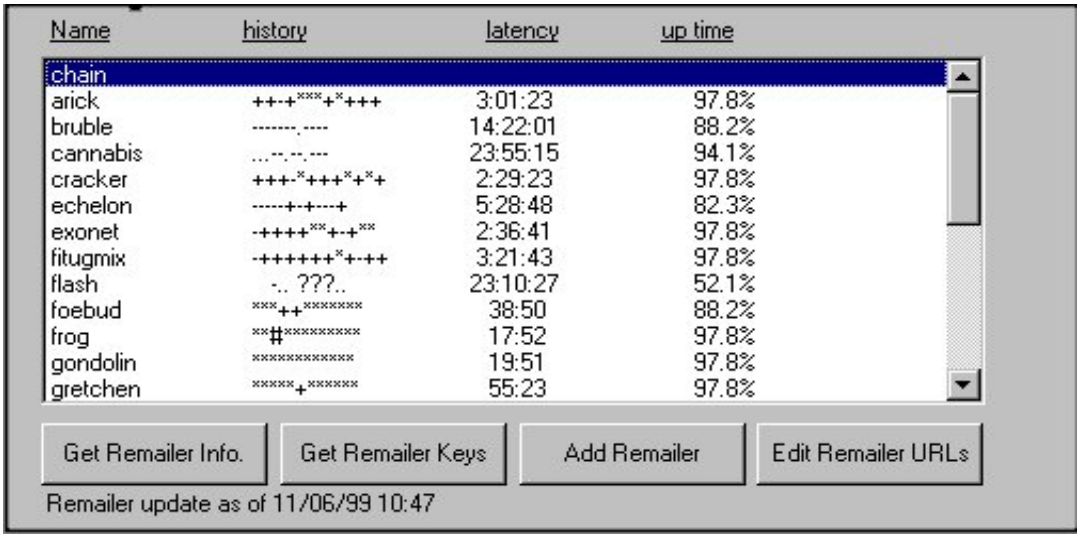


Εικόνα 102 Drag and Drop an attachment into the message area



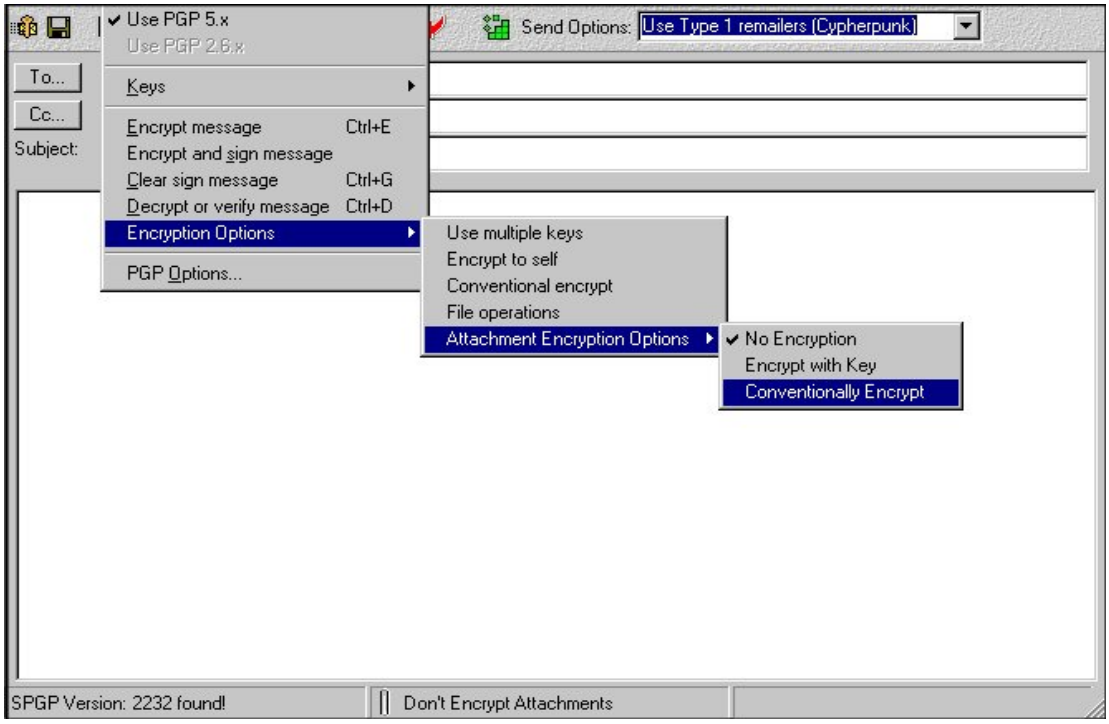
Εικόνα 103 Private Idaho now uses Folder to manage your emails

[131] http://www.itech.net.au/pi/

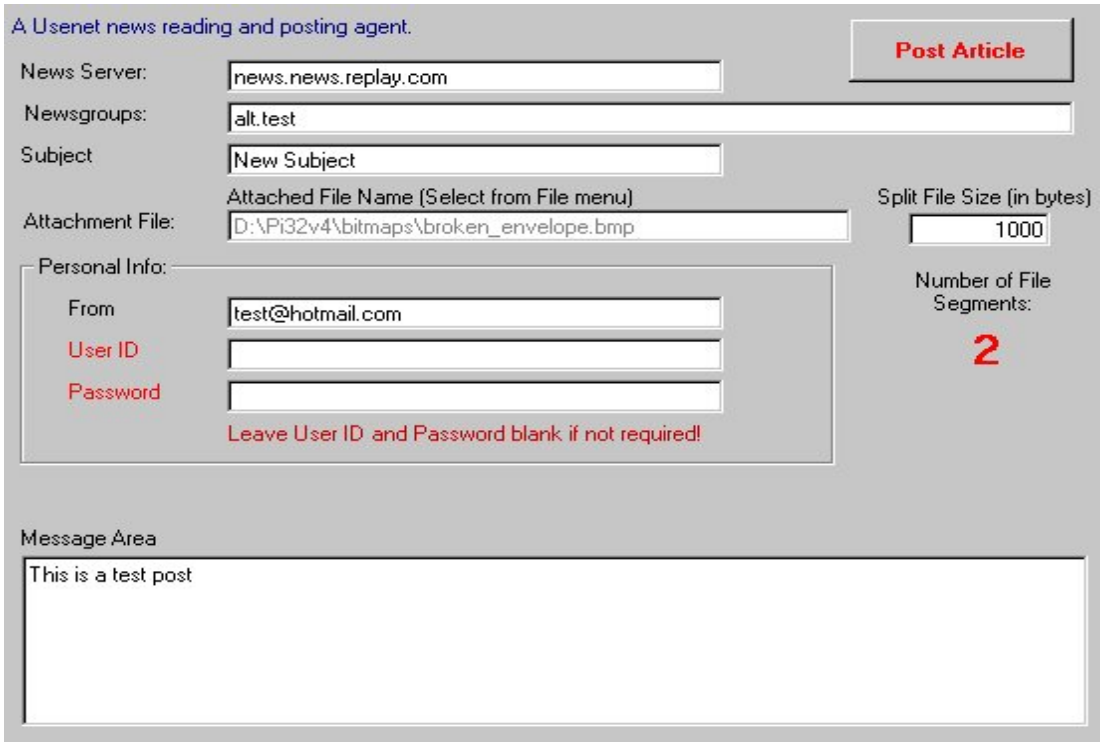


Εικόνα 104 Remailers are now better organised

Εικόνα 105 More option for accessing the POP Mailer Server



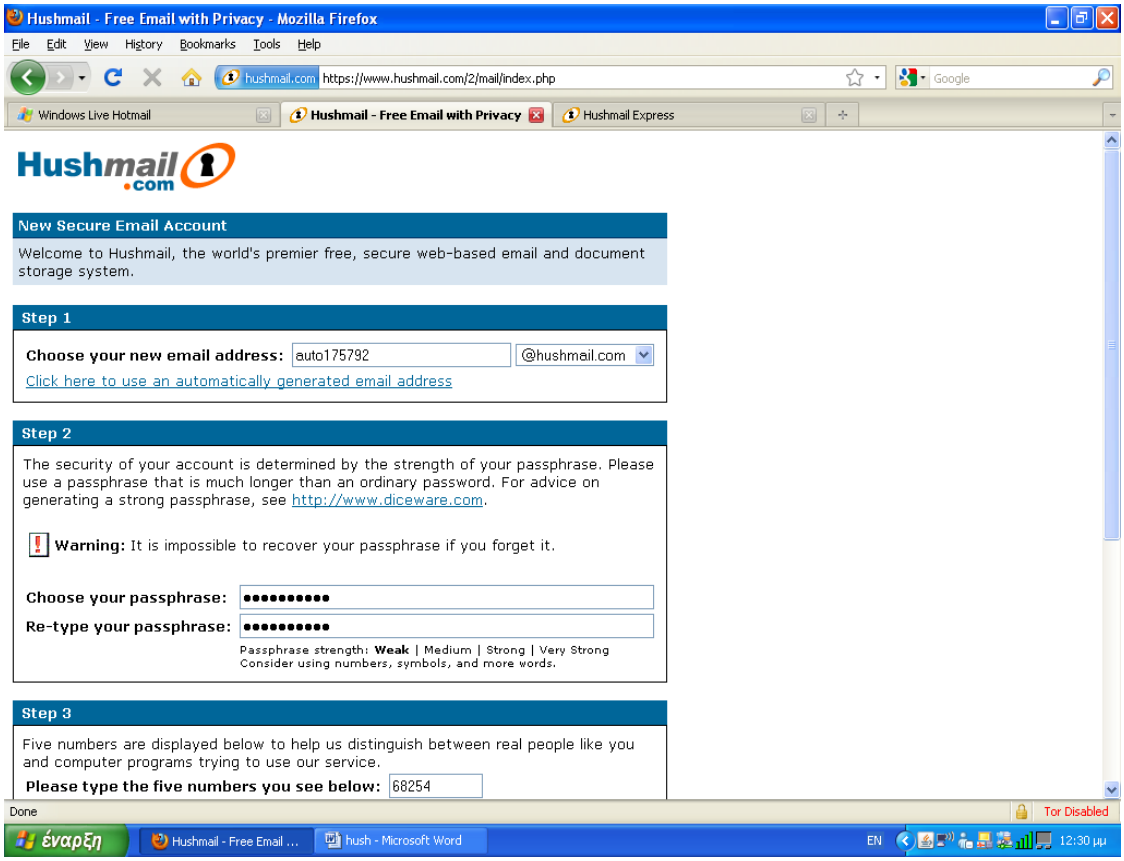
Εικόνα 106 More option to encrypt attachments



Εικόνα 107 Posting to Newsgroups with automatic file splitting on large files

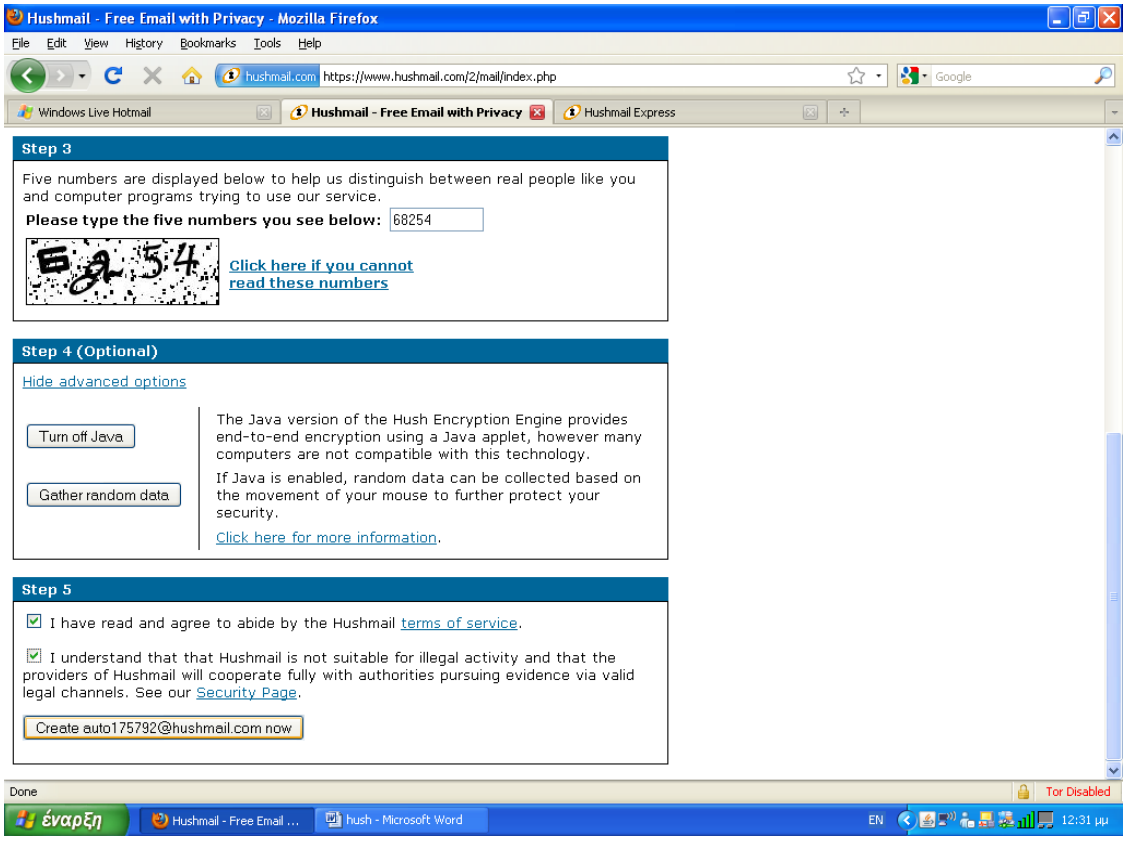
6.3 Εφαρμογή remailer

Για να δούμε πως λειτουργεί μια εφαρμογή με χρήση remailer, επιλέξαμε την σελίδα hushmail[132] όπου μέσω αυτής μπορούμε να στείλουμε ανώνυμα e-mails. Αρχικά δημιουργήσαμε ένα λογαριασμό στη συγκεκριμένη ιστοσελίδα.[133]



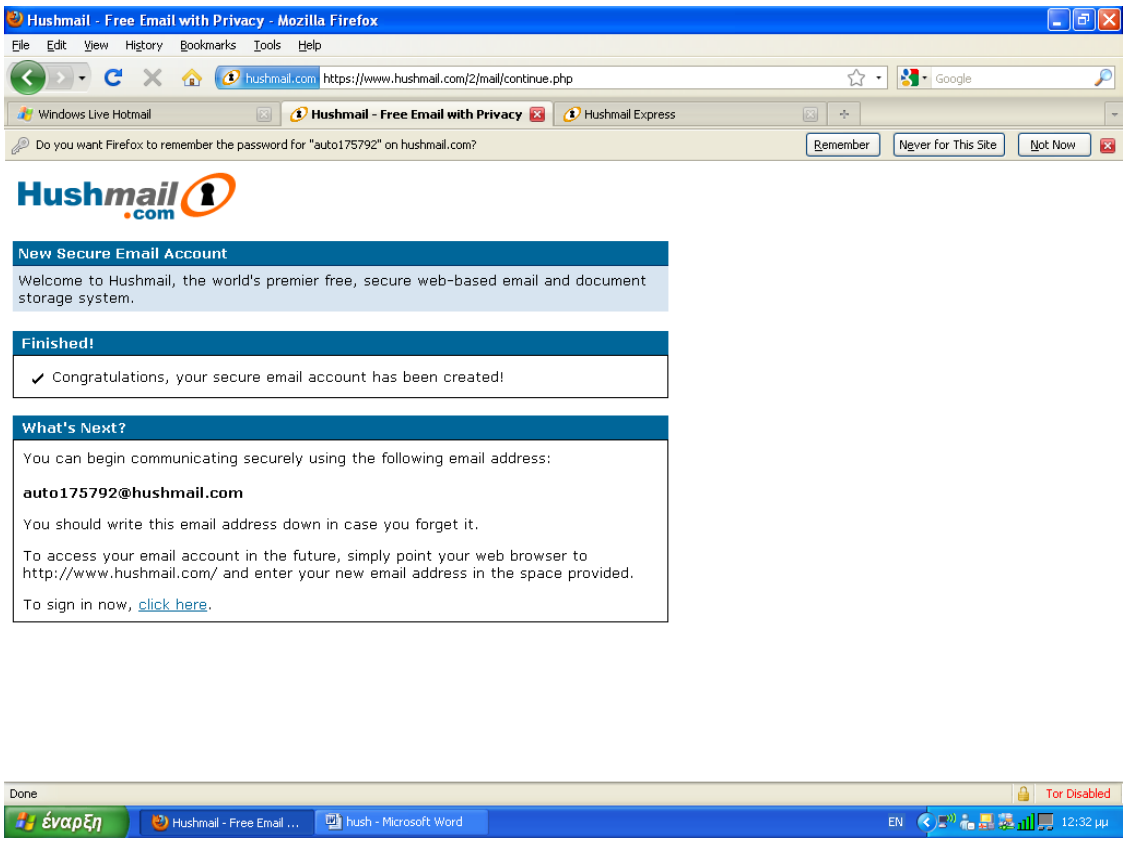
Εικόνα 108 Hushmail: New hushmail account

[132] www.hushmail.com
[133] https://www.hushmail.com/2/mail/index.php



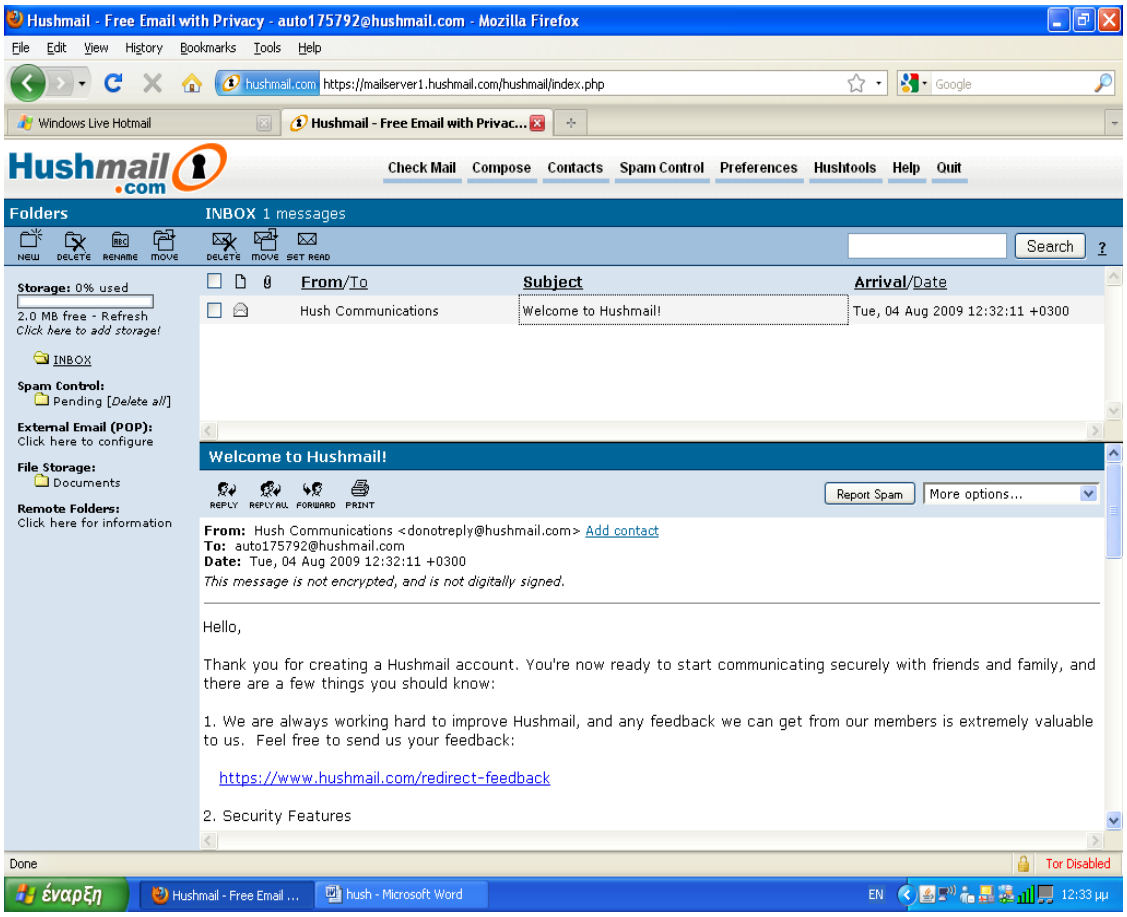
Εικόνα 109 Hushmail: New hushmail account

Όπως παρατηρούμε η νέα διεύθυνσή μας e-mail είναι auto175792@hushmail.com.



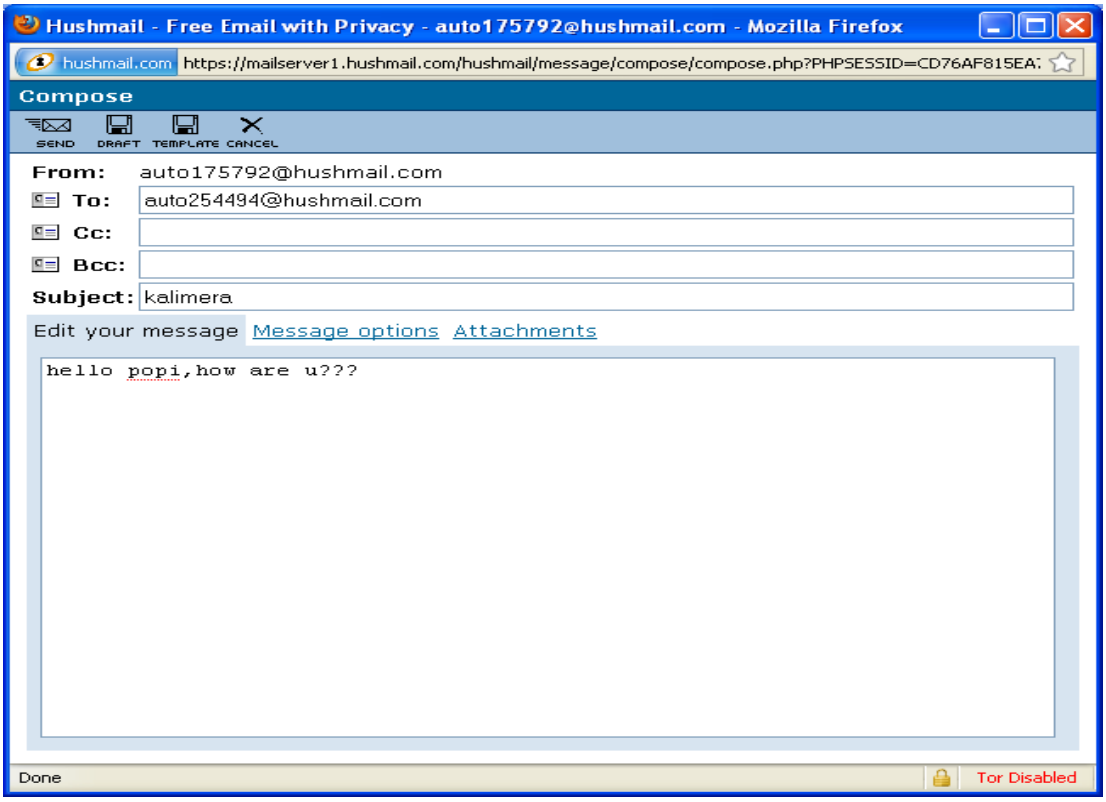
Εικόνα 110 Hushmail: Hushmail account is ready

Στη συνέχεια ανοίγουμε το λογαριασμό και δημιουργούμε ένα ανώνυμο e-mail. Ο παραλήπτης έχει και αυτός λογαριασμό στην hushmail.com με διεύθυνση auto254494@hushmail.com.



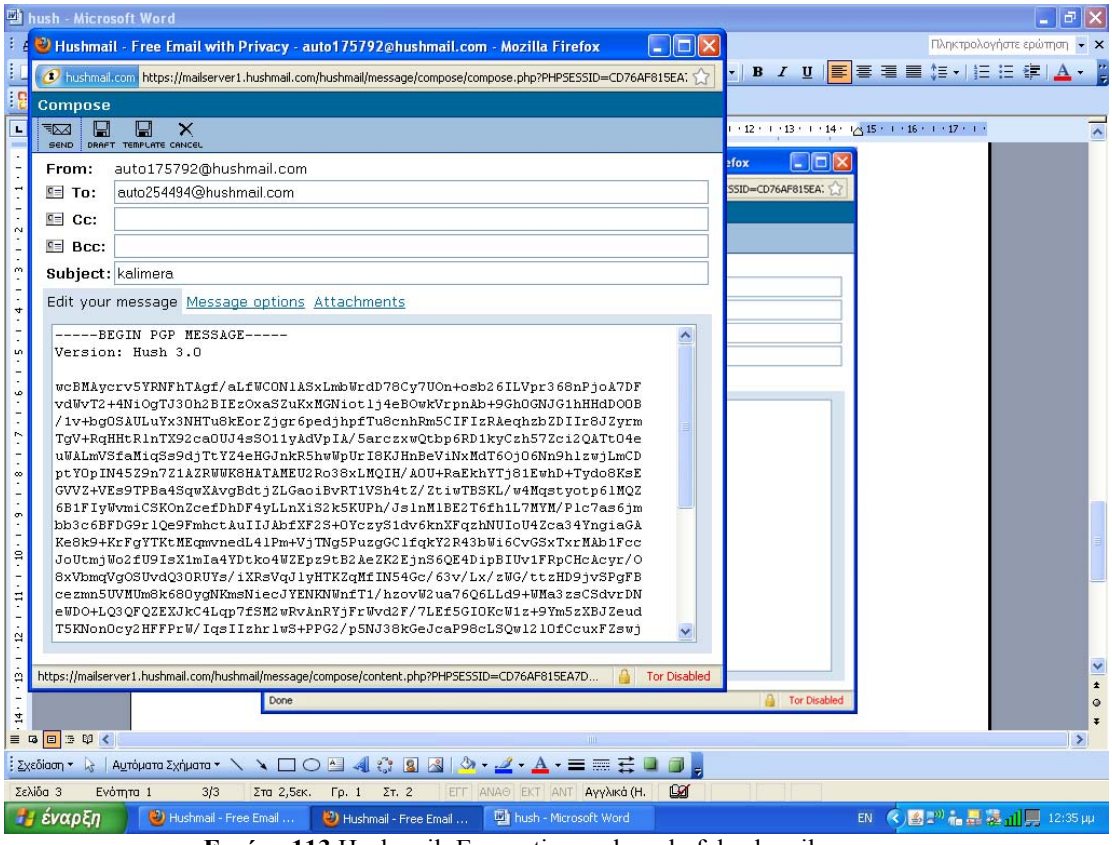
Εικόνα 111 Hushmail: Edit hushmail mailbox

Γράφουμε το κείμενό μας και προσθέτουμε τον παραλήπτη.



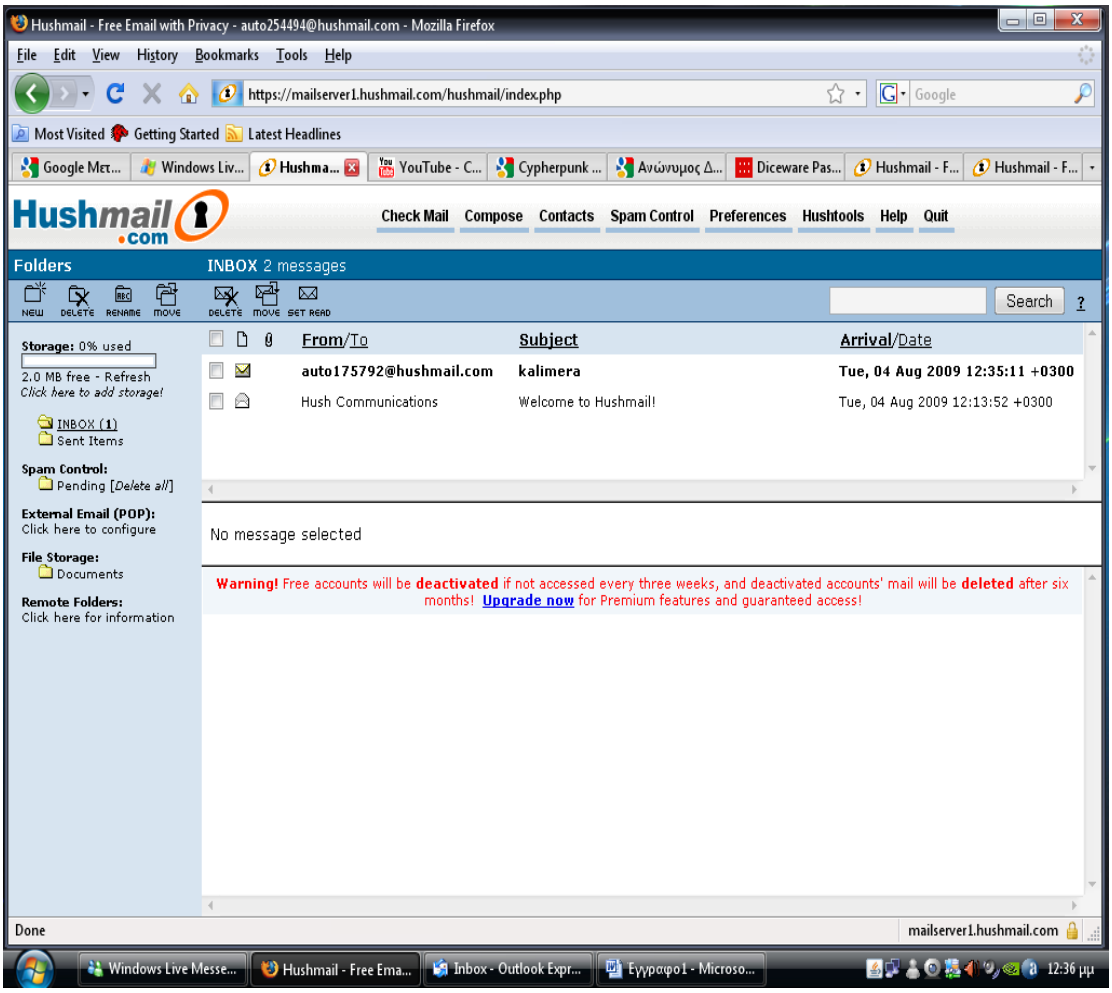
Εικόνα 112 Hushmail: New hushmail message

Μόλις επιλέξουμε send παρατηρούμε ότι το μήνυμά μας κρυπτογραφείται με κρυπτογράφηση PGP και περιέχει ψηφιακή υπογραφή (hush).



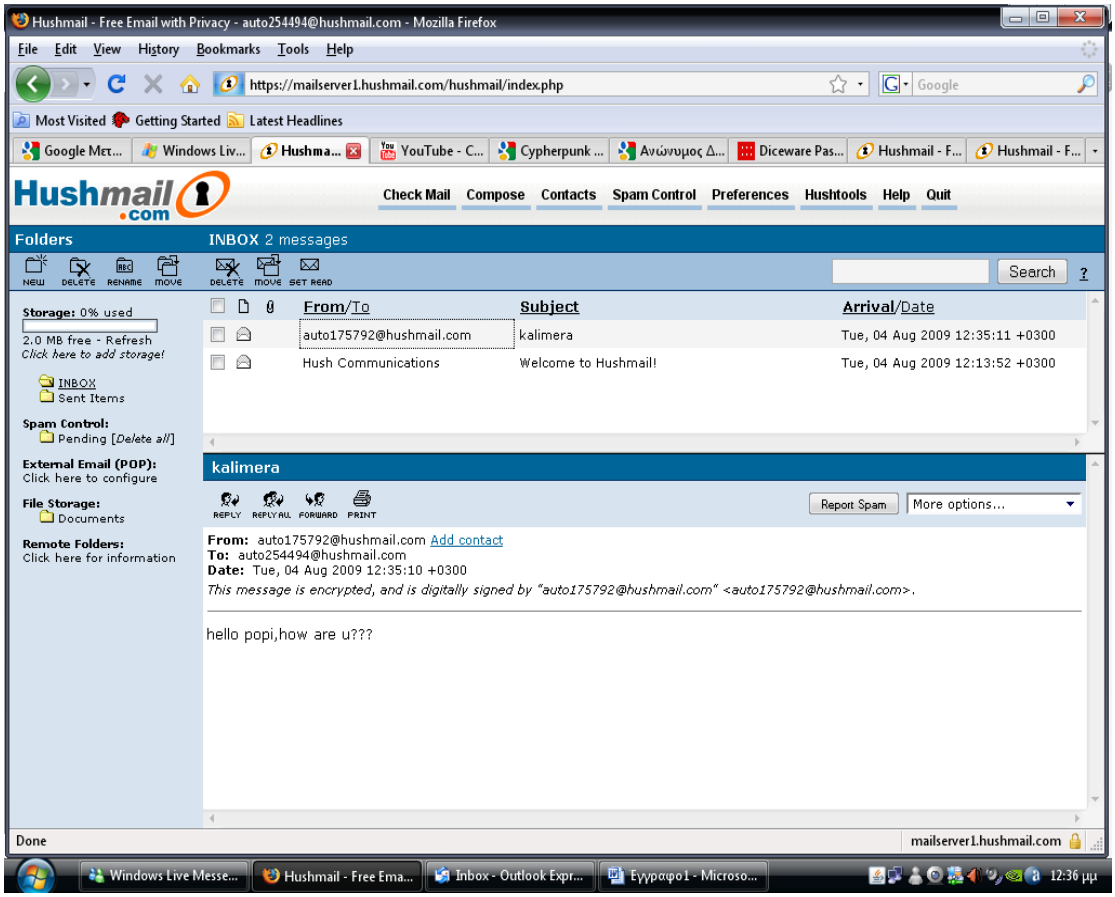
Εικόνα 113 Hushmail: Encryption and send of hushmail message

Και τώρα μπορούμε να δούμε τι έλαβε ο παραλήπτης.



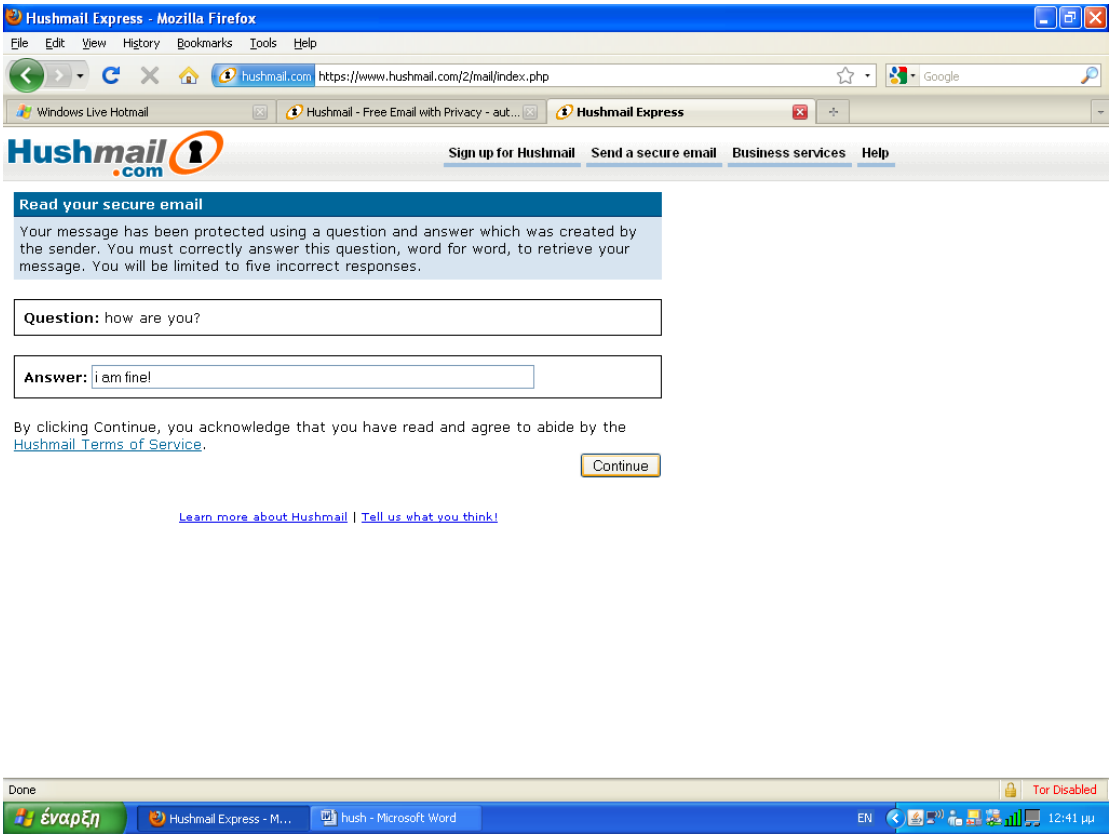
Εικόνα 114 Hushmail: Inbox messages of hushmail

Επιλέγουμε να ανοίξουμε το μήνυμα από τον αποστολέα auto@hushmail.com. Αφού βλέπουμε τι περιέχει το μήνυμα, μπορούμε να παρατηρήσουμε κάτω από την ημερομηνία που στάλθηκε το e-mail, ότι το μήνυμα είναι κρυπτογραφημένο και ψηφιακά υπογεγραμμένο και από τον αποστολέα και από τον παραλήπτη.



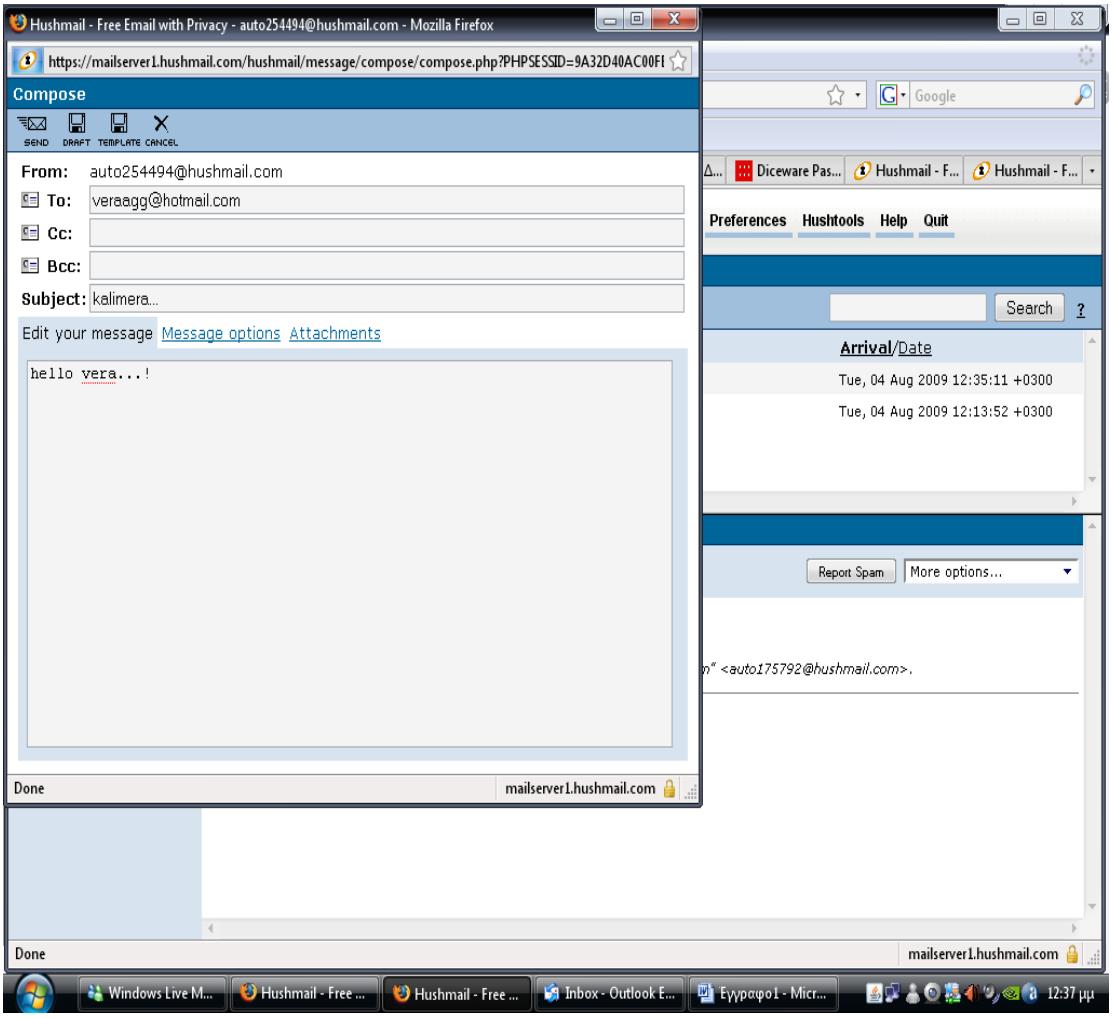
Εικόνα 115 Hushmail: Opening hushmail message

Αν τώρα ο παραλήπτης δεν διαθέτει λογαριασμό στην συγκεκριμένη σελίδα του web, τότε η hushmail ζητάει μια ερώτηση και μια απάντηση κλειδί που θα χρησιμοποιηθεί για να ανοίξει ο παραλήπτης το μήνυμα. Στην περίπτωσή μας η ερώτηση είναι «how are you?» και η απάντηση «I am fine!». Πρέπει να σημειώσουμε ότι ο αποστολέας έχει ενημερώσει τον αποστολέα για την συγκεκριμένη απάντηση κλειδί.



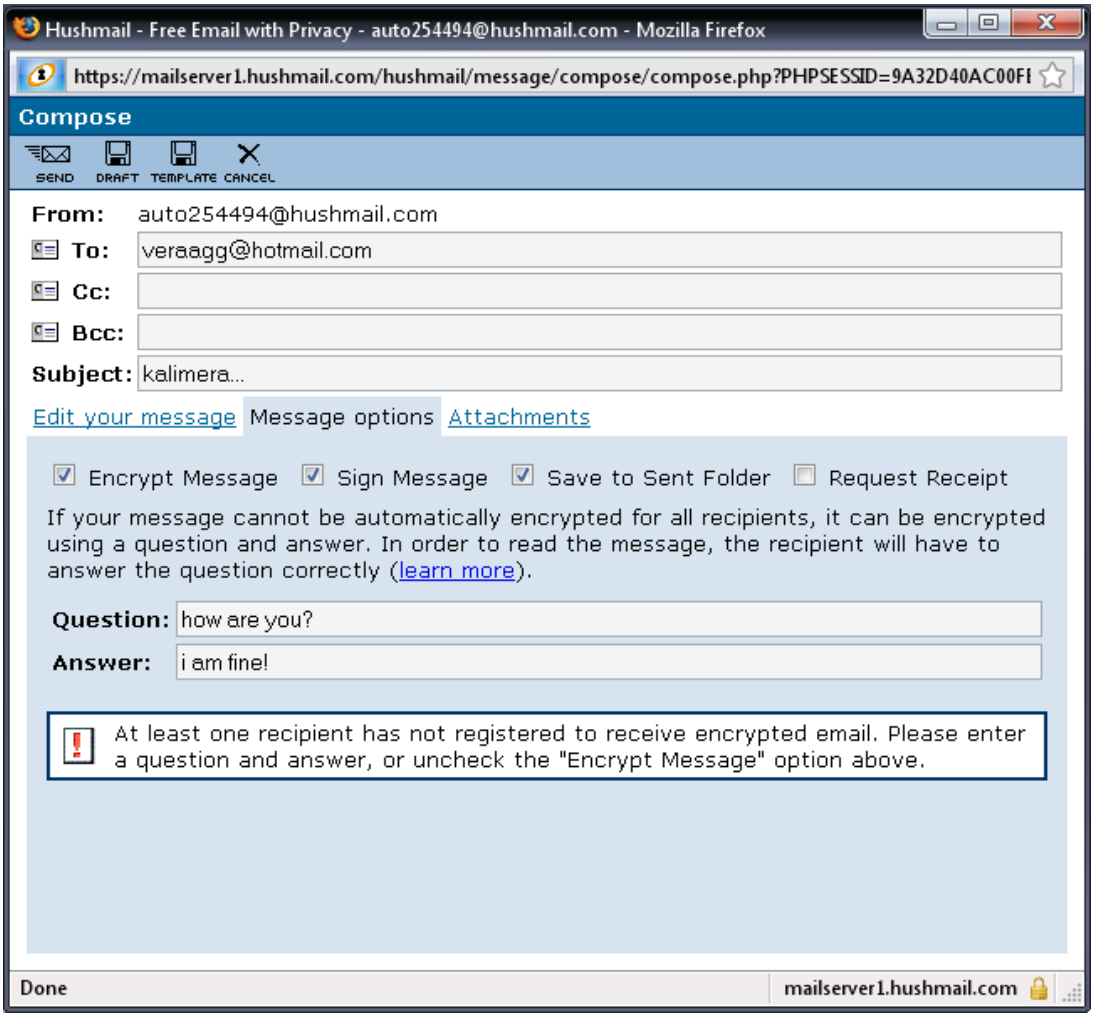
Εικόνα 116 Hushmail: Send a secure message to hotmail recipient

Αφού έχουμε επιλέξει την ερώτηση και την απάντηση, δημιουργούμε το μήνυμά μας και προσθέτουμε τον παραλήπτη, ο οποίος διαθέτει λογαριασμό hotmail.



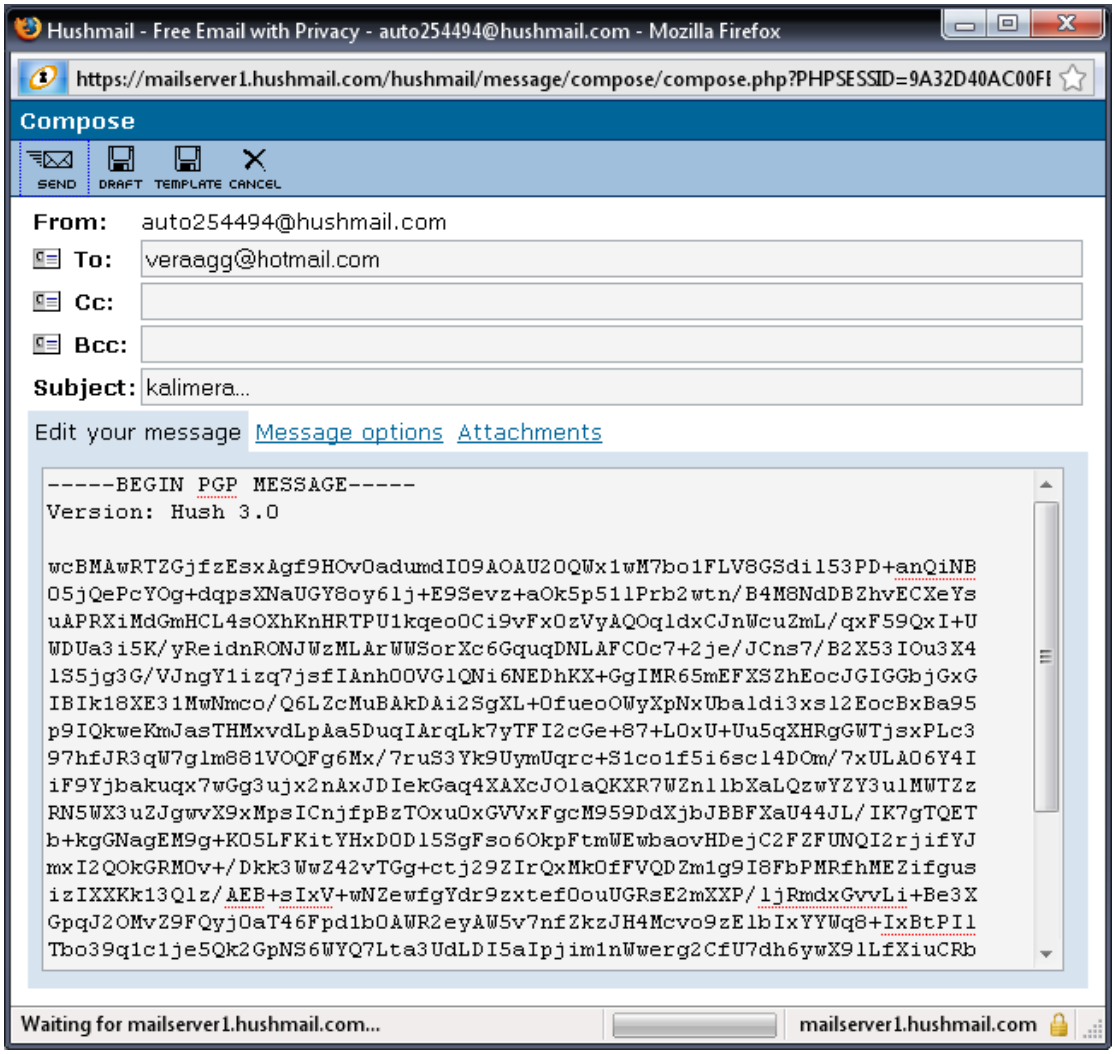
Εικόνα 117 Hushmail: Edit a secure message to hotmail recipient

Στη συνέχεια, στο δεύτερο πεδίο Message options, πληκτρολογούμε και πάλι την ερώτηση και την απάντηση που δώσαμε προηγουμένως για επιβεβαίωση.



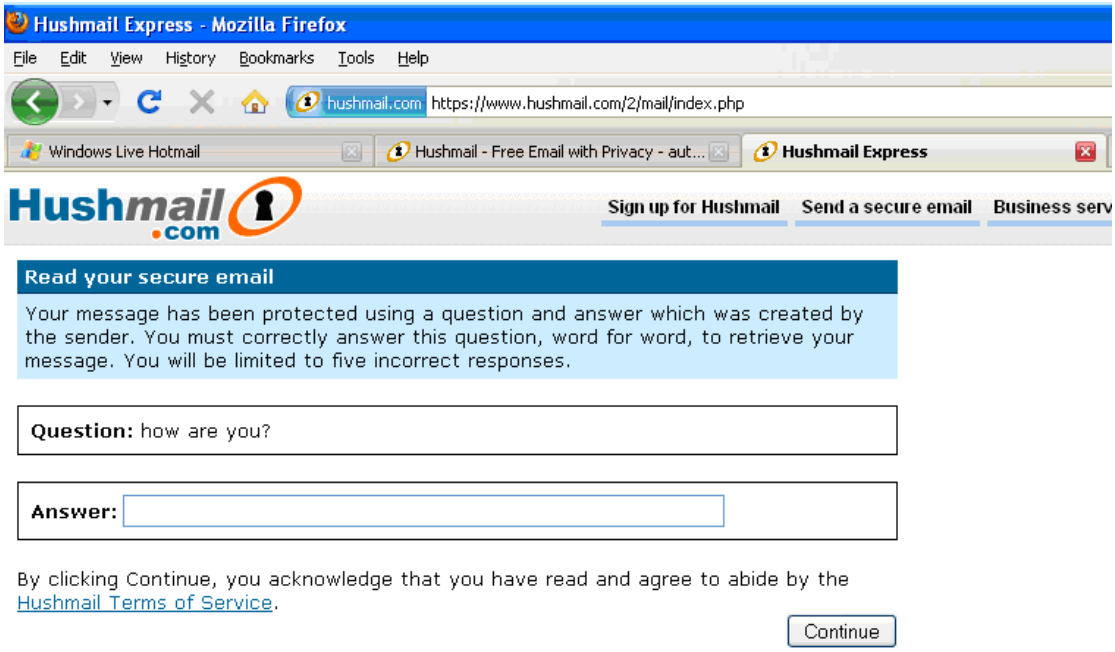
Εικόνα 118 Hushmail: Hushmail message options

Αφού επιλέξουμε send βλέπουμε και πάλι ότι το μήνυμά μας κρυπτογραφείται με κρυπτογράφηση PGP και επίσης ότι περιέχει ψηφιακή υπογραφή (hush).



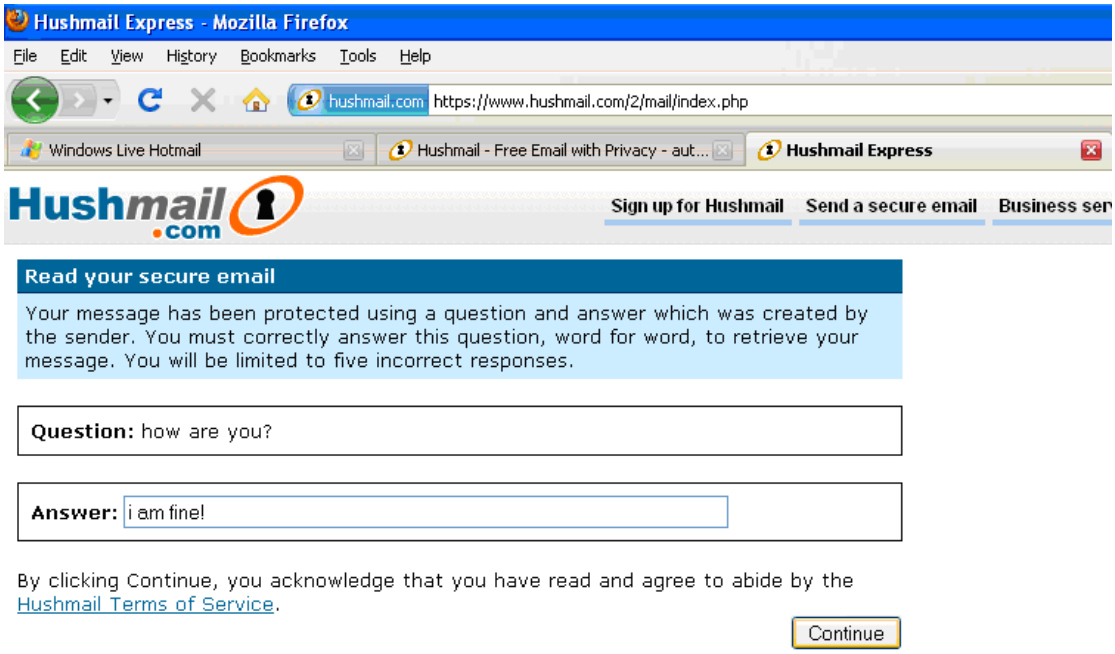
Εικόνα 119 Hushmail: Encryption and send of hushmail message

Αυτό που λαμβάνει αρχικά ο παραλήπτης είναι ένα παράθυρο με την ερώτηση κλειδί του αποστολέα.



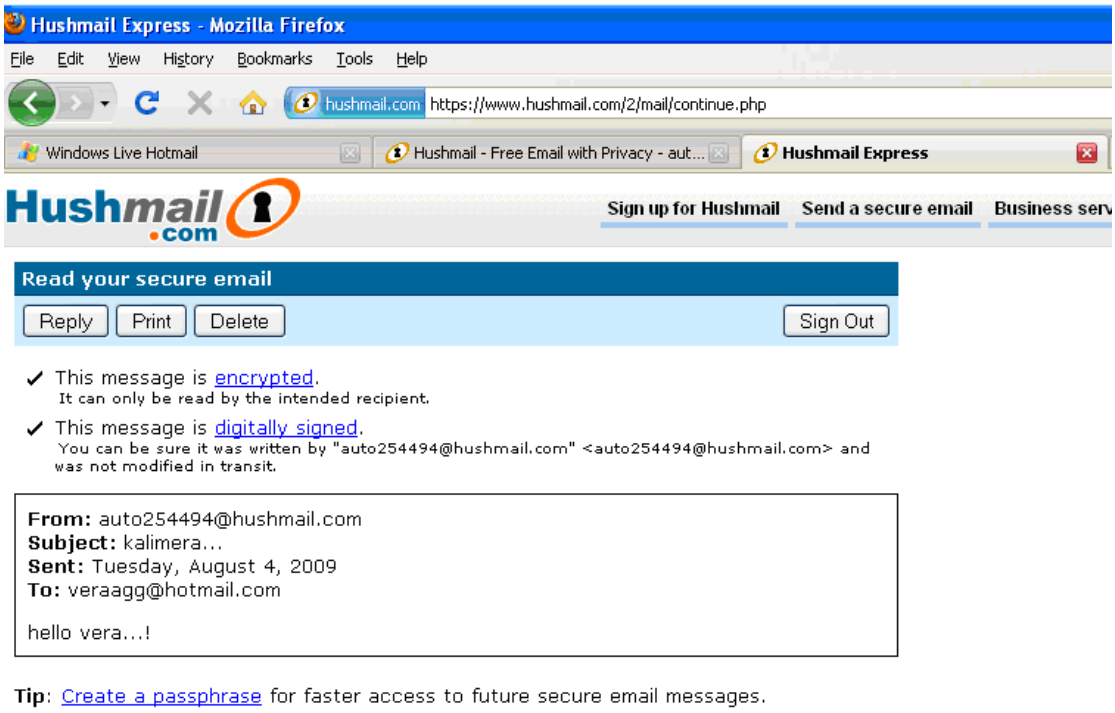
Εικόνα 120 Hushmail: Receiving a secure e-mail step 1

Ο παραλήπτης πληκτρολογεί την απάντηση κλειδί για να ανοίξει το μήνυμα.



Εικόνα 121 Hushmail: Receiving a secure e-mail step 2

Μετά από αυτή τη διαδικασία εμφανίζεται το κείμενο που περιέχει το e-mail, κι ένα μήνυμα διαβεβαίωσης ότι το μήνυμα είναι κρυπτογραφημένο και ψηφιακά υπογεγραμμένο από τον αποστολέα που περιμέναμε e-mail.



Εικόνα 122 Hushmail: Opening e secure e-mail

Κεφάλαιο 7 Ιδιωτική περιήγηση (Private Browsing)

7.1 Ιδιωτική περιήγηση

7.1.1 Private Browsing (Porn Mode)

Η ιδιωτική περιήγηση (private mode), καλείται αλλιώς και porn mode, είναι ένας όρος που αναφέρεται στην προστασία της ιδιωτικής ζωής σε κάποιους web browsers.[134] Οι web browsers αποθηκεύουν πληροφορίες όπως το ιστορικό περιήγησης, εικόνες, βίντεο, και κείμενα στην μνήμη cache. Αντιθέτως, η ιδιωτική ζωή μπορεί να λειτουργήσει εάν ο browser δεν αποθηκεύει αυτές τις πληροφορίες για επιλεγμένες περιηγήσεις μας. Αυτό επιτρέπει σε κάποιον χρήστη να περιηγηθεί στο internet χωρίς να αποθηκεύονται τα δεδομένα που μπορούν να ανακτηθούν σε μεταγενέστερη στιγμή με σκοπό να τον ενοχοποιήσουν.

Η πρώτη αναφορά του όρου ήταν το Μάιο του 2005 και χρησιμοποιήθηκε για την συζήτηση των χαρακτηριστικών της ιδιωτικότητας στον browser Safari, οποίος λειτουργούσε με το Mac OS X Tiger. Το χαρακτηριστικό αυτό είχε ήδη διαδοθεί στους άλλους browsers, και οδήγησε στην εκλαΐκευση του όρου το 2008 από τον internet explorer 8. Παρ' όλα αυτά, ο τρόπος λειτουργίας της ιδιωτικότητας λειτουργούσε ως ασπίδα, καθώς οι browsers, τυπικά, δεν αφαιρούν όλα τα δεδομένα από τη μνήμη cache μετά από κάθε συνεδρία (session).

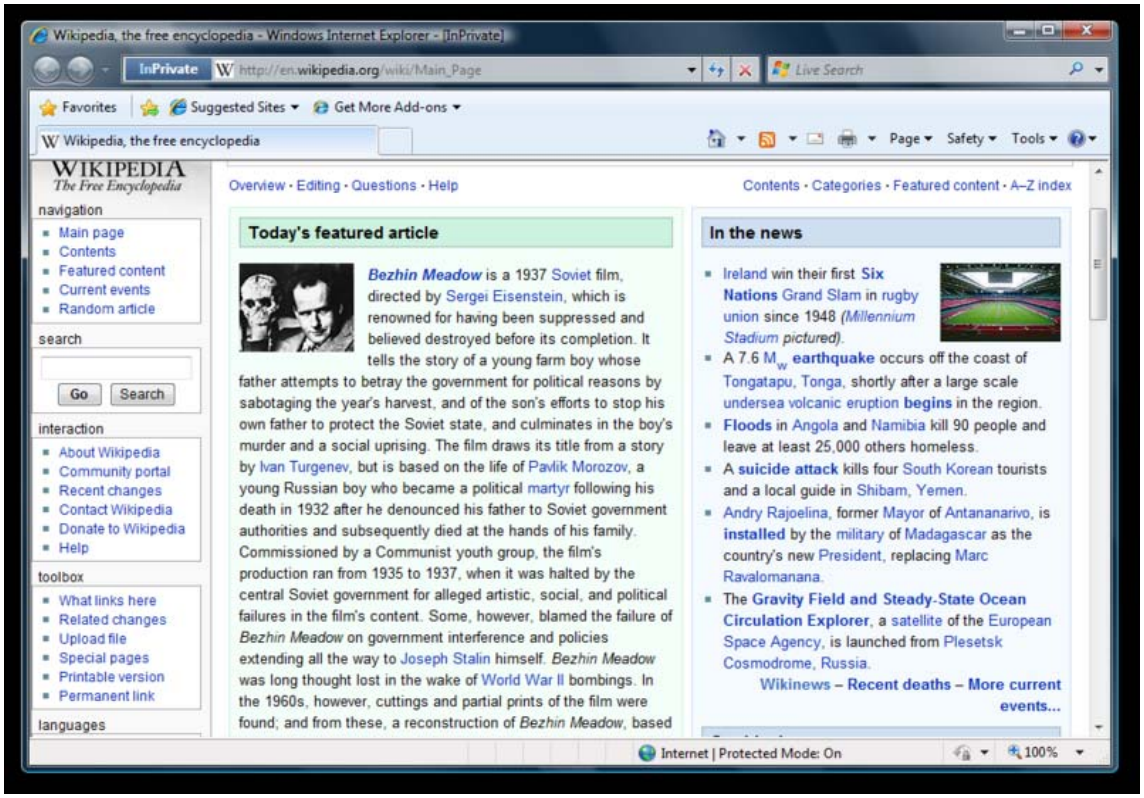
Κάποια προγράμματα, όπως το Adobe Flash, είναι ικανά να ενεργοποιήσουν τα cookies που δεν αφαιρέθηκαν μετά από τη σύνοδο. Η Adobe πρόσφατα, δημοσίευσε ένα έγγραφο που εξηγεί πώς να απενεργοποιούμε και να αφαιρούμε τα δεδομένα. Ο Internet Explorer 8 επίσης περιέχει ένα χαρακτηριστικό που καλείται InPrivate Subscriptions, το οποίο βοηθά στη χρήση της ιδιωτικής περιήγησης.

Η ιδιωτική περιήγηση ή αλλιώς Private mode, είναι γνωστή με διαφορετικά ονόματα σε διαφορετικούς browsers. Στο παρακάτω πίνακα φαίνονται πότε ο κάθε browser χρησιμοποίησε για πρώτη φορά την ιδιωτική περιήγηση.

Ημερ/νία	*Browser*	*Ονομασία*	*Τελευταία έκδοση*
29 Απριλίου 2005	Safari 2.0	Private Browsing	4.0.2
11 Δεκεμβρίου 2008	Google Chrome 1.0	Incognito	2.0.172.37
19 Μαρτίου 2009	Internet Explorer 8	InPrivate	8.0
30 Ιουνίου 2009	Mozilla Firefox 3.5	Private Browsing	3.5.1

Πίνακας 8 Supported Browsers

[134] http://en.wikipedia.org/wiki/Private_browsing



Εικόνα 123 Internet Explorer 8 in InPrivate mode

Εικόνα 124 Google Chrome in Incognito mode

Μερικές φορές είναι ωραία να περνάμε απαρατήρητοι.[135] Όταν ενεργοποιηθεί αυτό το χαρακτηριστικό, δεν μένει κανένα αποτύπωμα της περιήγησης μας για να το ανακαλύψει κάποιος. Μπορούμε να βγούμε και να μπούμε σε κατάσταση ιδιωτικής περιήγησης γρήγορα, οπότε είναι εύκολο να επιστρέψουμε σ' αυτό που κάναμε πριν σαν να μη συνέβηκε τίποτα (ή να χρησιμοποιούμε πάντα την ιδιωτική περιήγηση).

Όπως ήδη ξέρουμε, καθώς «σερφάρουμε» στο διαδίκτυο, ο browser μας καταγράφει συνήθως όλα τα δεδομένα τα οποία αργότερα μπορούν να χρησιμοποιηθούν για να βελτιώσουν την εμπειρία της περιήγησής μας.[136] Για παράδειγμα, καταγράφεται το ιστορικό από όλες τις σελίδες που έχουμε επισκεφτεί, έτσι ώστε αργότερα αν χρειαστούμε βοήθεια για να θυμηθούμε ένα site, μπορεί να μας βοηθήσει να το βρούμε εκείνη τη στιγμή. Αυτό από τη μία είναι πολύ χρήσιμο, αλλά από την άλλη όλα αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για τον εντοπισμό των δραστηριοτήτων μας στο Internet. Πχ, αν ένας συνάδελφός μας χρησιμοποιήσει τον υπολογιστή μας, τότε θα μπορέσει να δει όλο το ιστορικό περιήγησής μας, κάτι το οποίο μπορεί να μην θέλουμε.

Ας υποθέσουμε ότι κάνουμε κάτι online,και δεν θέλουμε να το ξέρουν οι συνάδελφοί μας. Πχ να ψάχνουμε για νέα δουλειά. Από τη μία, μπορούμε να βρούμε αυτό που θέλουμε και στη συνέχεια να διαγράψουμε όλα τα δεδομένα τα οποία έχουν αποθηκευτεί στον Firefox, όπως το ιστορικό, τα cookies, κλπ. Όμως με αυτή την ενέργεια θα διαγραφούν όλες μας οι δραστηριότητες, ακόμα και αυτές που δεν θέλουμε να κρύψουμε. Σε αυτό το σημείο η λειτουργία Private Browsing του Firefox μας βοηθάει.

Όλα ξεκίνησαν με το porn mode του Internet Explorer 8 ή αλλιώς InPrivate Browsing.[137] Ακολούθησε ο Chrome και φυσικά ο Firefox. Η ιδέα είναι απλή και πρακτικά σημαίνει ότι ο browser και ο χρήστης θυσιάζουν λίγη ευκολία προς όφελος της ανωνυμίας. Ο browser δεν συγκρατεί ιστορικό, ούτε cookies, ούτε περιεχόμενο στη cache. Ο χρήστης δεν έχει την δυνατότητα να ανατρέξει στο παρελθόν αλλά ξέρει ότι τα sites που βλέπει, δεν αποθηκεύουν τίποτα στον υπολογιστή και ο browser δεν θυμάται τίποτα για αυτή την επίσκεψη. Εύκολα αντιλαμβανόμαστε γιατί αρχικά η λειτουργία ονομάστηκε porn mode.

Χρήσιμο για ορισμένες καταστάσεις και ανά περίπτωση, το Private Browsing μπορεί να δυσκολέψει σημαντικά τα πράγματα αν επιλεγεί ως μόνιμη λύση. Πολλά sites χρησιμοποιούν cookies για να αποθηκεύουν login sessions και ρυθμίσεις του χρήστη που διαφορετικά δεν είναι διαθέσιμες. Το Private Browsing ίσως φανεί χρήσιμο σε internet cafe ή σε υπολογιστές που δεν εμπιστευόμαστε.

Το Private Browsing στοχεύει στο να σιγουρέψει ότι οι διαδικτυακές μας δραστηριότητες δεν θα αφήσουν κανένα ίχνος στον υπολογιστή μας.[138] Είναι πολύ σημαντικό να σημειώσουμε ότι το Private Browsing δεν είναι ένα εργαλείο που μας κρατά ανώνυμους από τα sites που επισκεπτόμαστε ή από τους ISPs, ή για

---

[135] http://www.mozilla-europe.org/el/firefox/features/#private-browsing
[136] http://ehsanakhgari.org/blog/2008-11-04/dont-leave-trace-private-browsing-firefox
[137] http://www.pestaola.gr/firefox-private-browsing/
[138] http://ehsanakhgari.org/blog/2008-11-04/dont-leave-trace-private-browsing-firefox

παράδειγμα να μας προστατεύει από όλα τα είδη εφαρμογών που χρησιμοποιούνται για να μας εντοπίσουν. Το Private Browsing φροντίζει μόνο ότι ο Firefox δεν αποθηκεύει κανένα δεδομένο το οποίο στο μέλλον μπορεί να χρησιμοποιηθεί για να αποκαλυφθούν οι κινήσεις μας στο διαδίκτυο.

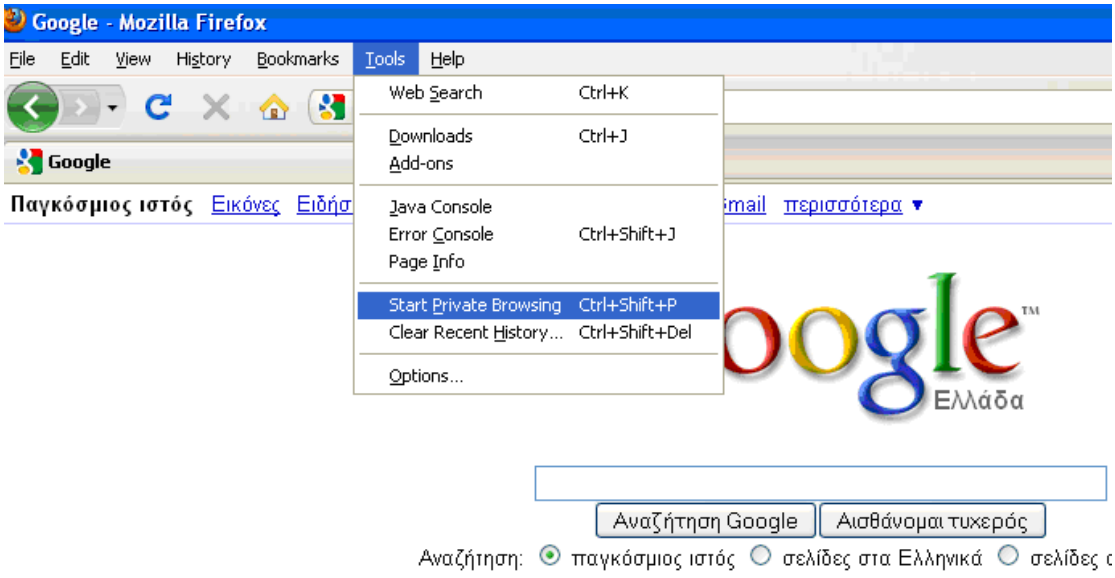
Τι δεν περιλαμβάνει το private browsing:

- Σελίδες που έχουμε επισκεφτεί.[139] Καμία από τις σελίδες δεν θα περιλαμβάνονται στη λίστα ιστορικού του μενού.
- Εισαγωγή χαρακτήρων σε φόρμες και μπάρες αναζήτησης. Τίποτα από ότι πληκτρολογούμε σε text boxes ή στην μπάρα αναζήτησης δεν θα περιλαμβάνονται στην λίστα εισαγωγής για την Form autocomplete.
- Κωδικοί. Κανένας κωδικός δεν θα τοποθετείται αυτόματα σε πεδία, και ούτε κανένας από τους νέους κωδικούς δεν θα αποθηκεύονται.
- Λίστα αρχείων. Κανένα αρχείο που «κατεβάσαμε» από το Internet δεν θα παραμένει στο φάκελο Downloads window αφού απενεργοποιήσουμε την λειτουργία Private Browsing.
- Cookies. Τα αρχεία που δημιουργούνται από σελίδες που έχουμε επισκεφτεί και κρατούν πληροφορίες για αυτές στον υπολογιστή μας, τα λεγόμενα cookies, δεν θα αποθηκεύονται.
- Αρχεία web cashe. Κανένα από τα προσωρινά αρχεία του Internet ή cashed αρχεία από σελίδες του web δεν θα αποθηκεύονται αφού απενεργοποιήσουμε τη λειτουργία Private Browsing.

7.1.2 Starting Private Browsing session

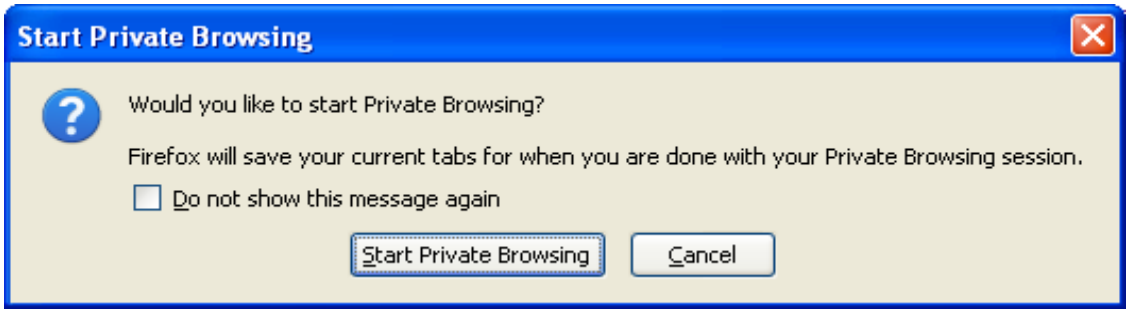
Για να ξεκινήσουμε ένα Private Browsing session η διαδικασία είναι η εξής: Πηγαίνουμε στο πεδίο Tools από το μενού και επιλέγουμε την λειτουργία Start Private Browsing.

[139] http://support.mozilla.com/en-US/kb/Private+Browsing#What_Private_Browsing_will_not_retain



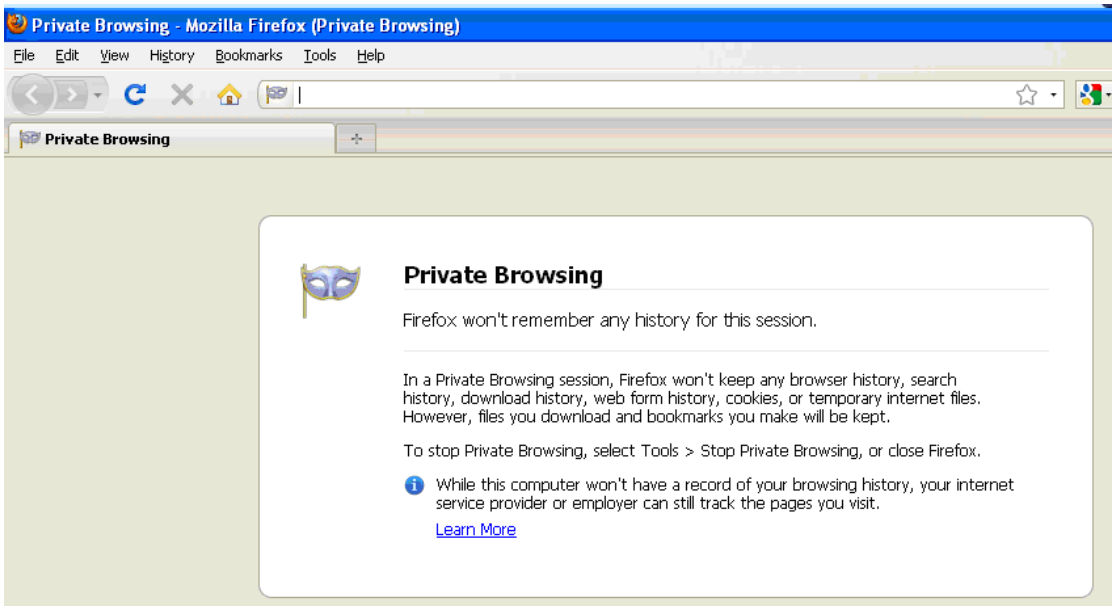
Εικόνα 125 Starting private browsing

Αμέσως μας εμφανίζεται ένα μήνυμα που μας ρωτάει εάν θέλουμε αν ξεκινήσουμε την ιδιωτική μας περιήγηση και ότι ο Firefox θα αποθηκεύσει το ιστορικό μας έτσι ώστε να το χρησιμοποιήσουμε αφού τελειώσουμε με το Private Browsing. Εάν λοιπόν επιθυμούμε να λειτουργήσει αυτή η ιδιότητα του Firefox στον browser μας πατάμε Start Private Browsing.



Εικόνα 126 Accept private browsing session

Αφού επιλέξουμε Start Private Browsing, αυτόματα μας εμφανίζεται ένα νέο παράθυρο που μας πληροφορεί ότι από αυτό το σημείο και μετά, ο Firefox δεν θα αποθηκεύει κανένα από τα δεδομένα της ιδιωτικής μας περιήγησης στο internet. Άρα από εδώ και πέρα μπορούμε να επισκεφτούμε όποια σελίδα του web, θέλουμε χωρίς να υπάρχει καμία διαφορά με πριν όσον αφορά τον τρόπο περιήγησης.

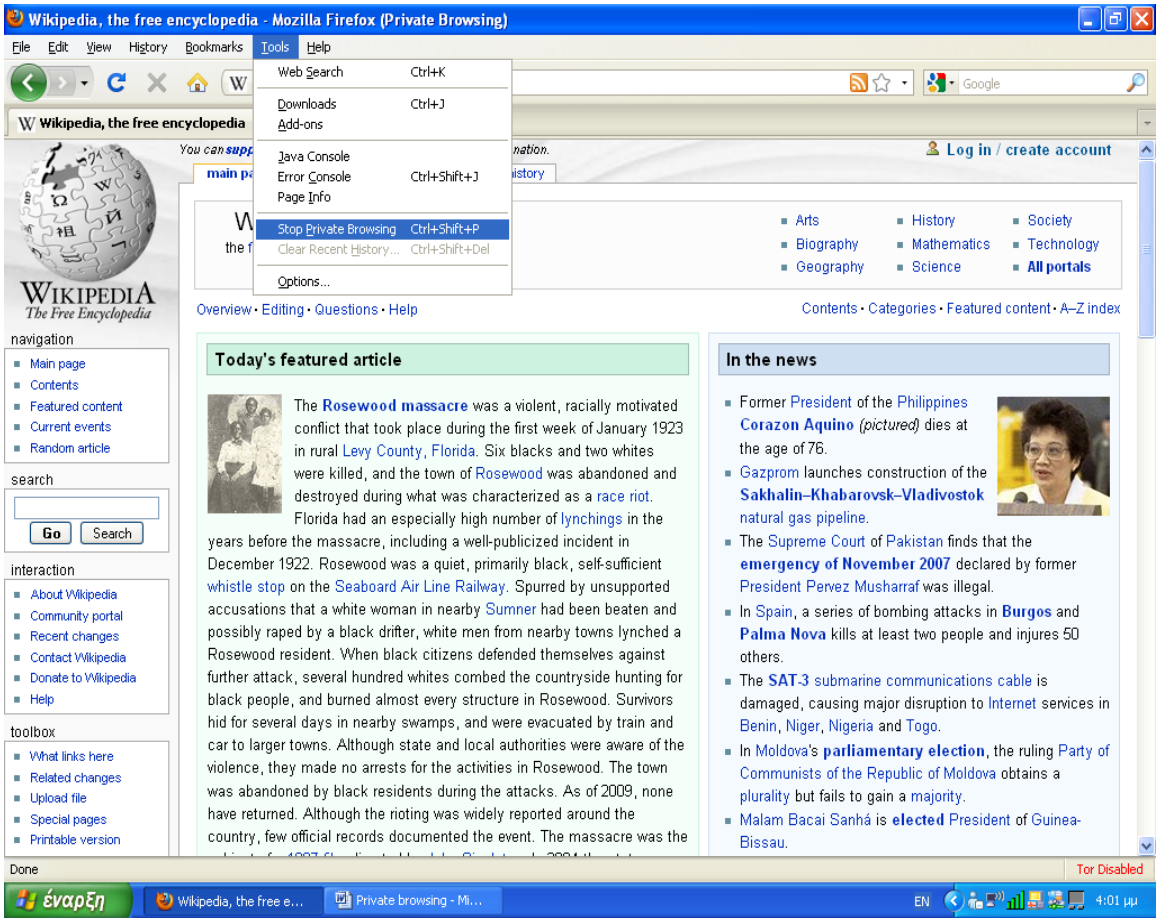


Εικόνα 127 Private browsing is ready

Για παράδειγμα μπορούμε να επισκεφτούμε τη σελίδα www.wikipedia.com. Αφού φορτωθεί, βλέπουμε στο πάνω μέρος ότι η ιδιότητα Private Browsing είναι ενεργοποιημένη.

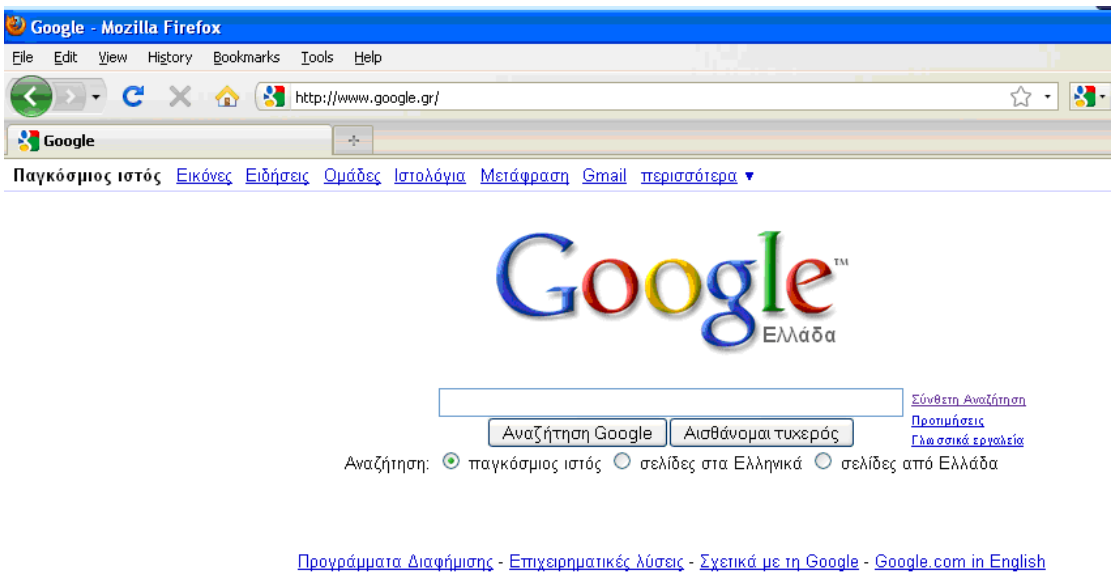
Εικόνα 128 www.wikipedia.org

Εάν λοιπόν θέλουμε να διακόψουμε την ιδιωτική περιήγηση, μπορούμε να πάμε από το μενού στο πεδίο Tools και να επιλέξουμε Stop Private Browsing.



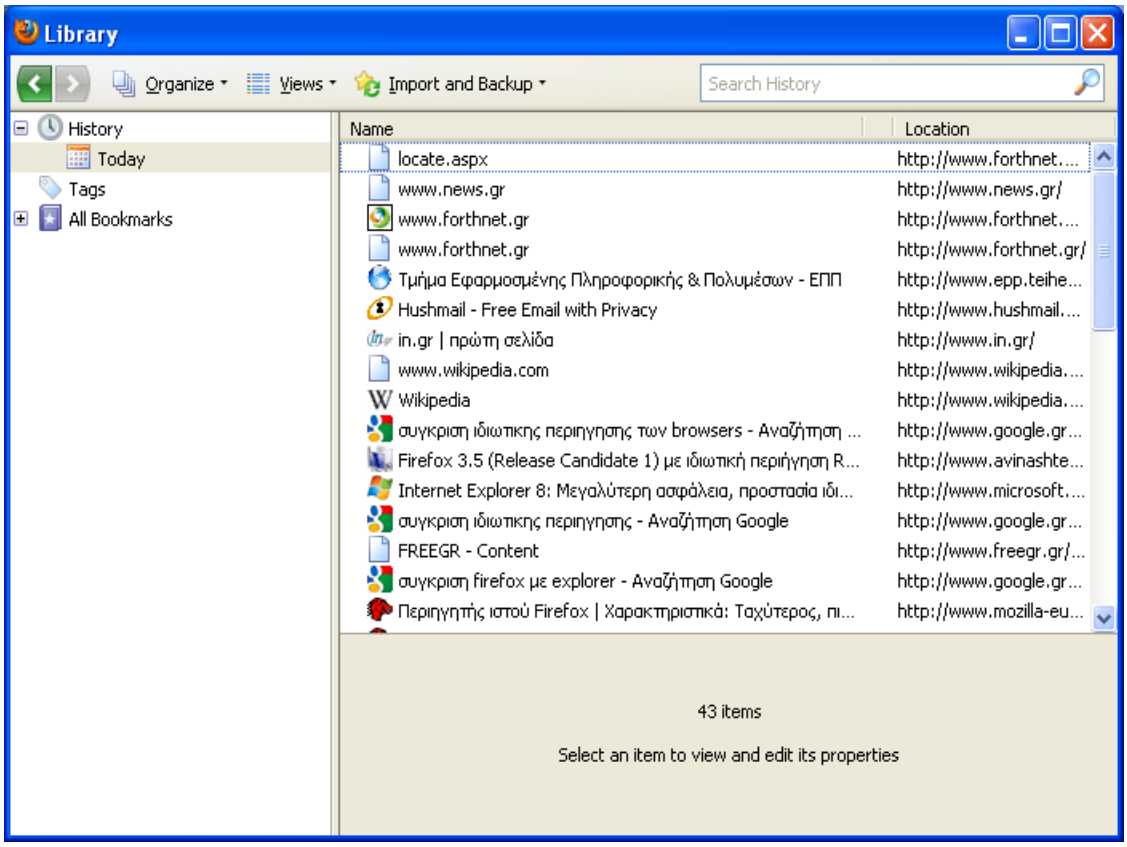
Εικόνα 129 Stop private browsing

Αφού το επιλέξουμε, αυτόματα ο Firefox μας γυρνά στην σελίδα που ήμασταν πριν ξεκινήσουμε την ιδιωτική περιήγησή μας στο διαδίκτυο.



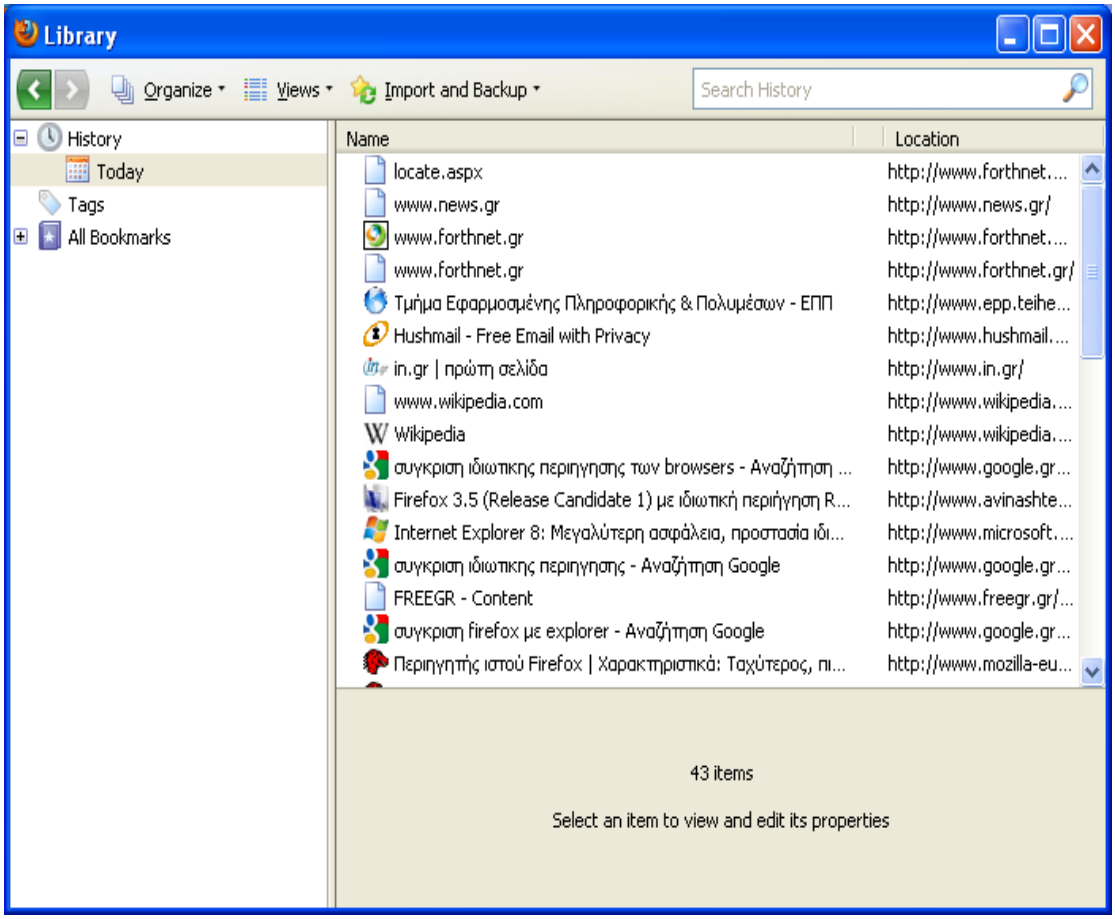
Εικόνα 130 www.google.com

Στο επόμενο screen shot φαίνεται το ιστορικό μας κατά την περιήγησή μας πριν χρησιμοποιήσουμε την ιδιότητα Private Browsing.



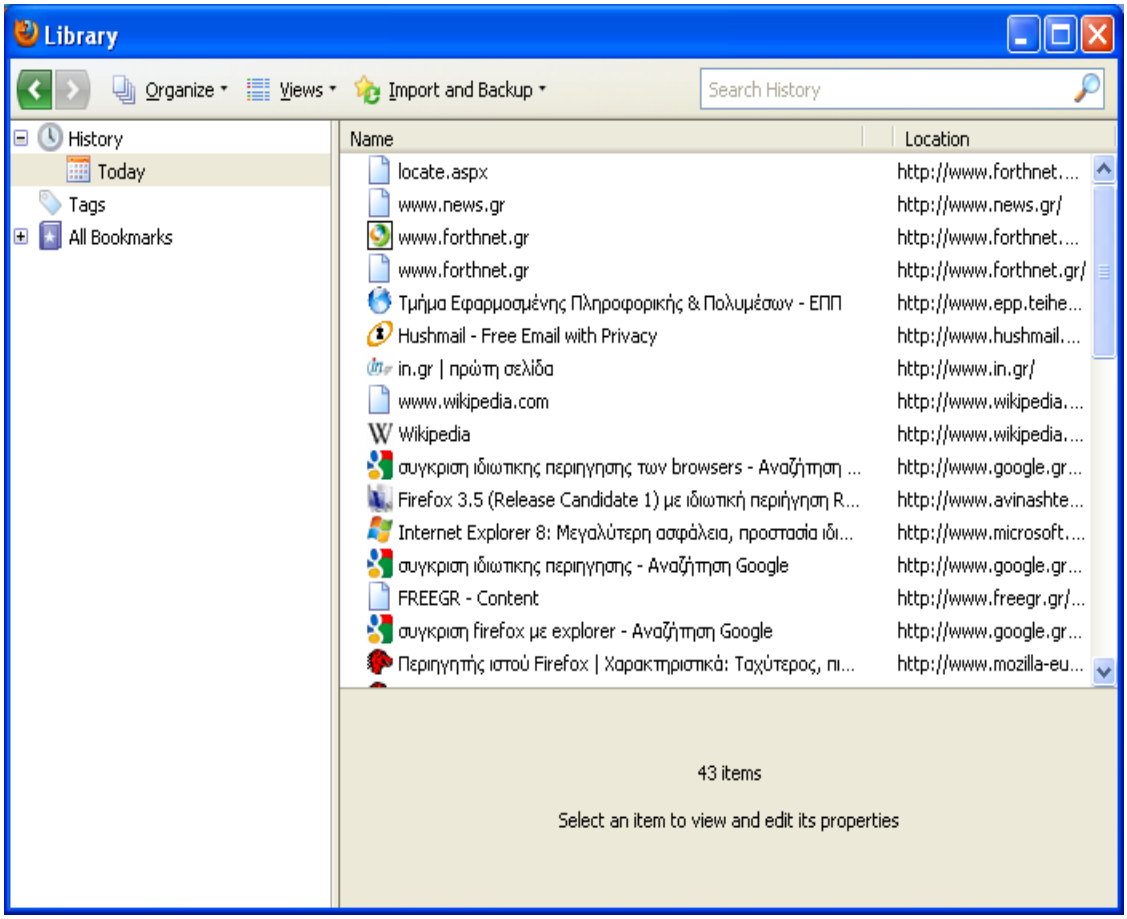
Εικόνα 131 History before private browsing

Στο παρακάτω screen shot φαίνεται το ιστορικό μας κατά τη διάρκεια της περιήγησής μας με τη χρήση του Private Browsing.



Εικόνα 132 History during private browsing

Όπως παρατηρούμε στο επόμενο screen shot το ιστορικό μας δεν άλλαξε καθόλου. Άρα επιβεβαιώνεται ότι ο Firefox κατά τη διάρκεια του Private Browsing δεν αποθηκεύει καμία σελίδα που έχουμε επισκεφθεί στο web.



Εικόνα 133 History after private browsing

Κεφάλαιο 8 Συμπεράσματα

Οι χρήστες του Internet μπορεί να θέλουν να μείνουν ανώνυμοι είτε εξαιτίας αυτών που παρέχουν κάποια υπηρεσία (να αποφύγουν πολύ μεγάλα μεγέθη πληροφορίας, να παρακάμψουν κάποιους περιορισμούς της χώρας τους), είτε εξαιτίας άγνωστων αντιπαλοτήτων (να προστατευθεί κάποιος από μυστικές υπηρεσίες, να προστατευθεί ένα θύμα από εγκληματική επίθεση).[140] Στην ουσία η έννοια της ανωνυμίας είναι το αντίθετο της υπευθυνότητας (accountability), αφού στόχος είναι οι ενέργειές μας να μην μπορούν να 'επιστρέψουν σε εμάς' (be tracked back to you), θα μπορούν βέβαια να επιστρέψουν στο σύνολο της ανωνυμίας μας (anonymity set).

Το πρόβλημα όμως που προκύπτει είναι όταν θέλουμε να μπορούμε να λάβουμε αντίστροφη επικοινωνία. Αυτό λύνεται από τη βασική ιδέα η οποία είναι η εξής: Ένας χρήστης μιλάει σε ένα ενδιάμεσο, ο ενδιάμεσος μιλάει στον άλλο χρήστη και έτσι ο πρώτος χρήστης 'κρύβεται' πίσω από τον ενδιάμεσο. Βέβαια υπάρχουν διάφορα θέματα που καθυστερούν την ανάπτυξή του. Κατ' αρχάς η ανωνυμία δε μπορεί να δημιουργηθεί από τον αποστολέα ή από τον παραλήπτη, επομένως κάποιος άλλος πρέπει να παράγει κυκλοφορία (traffic) και να καλύψει τον 'ανώνυμο αποστολέα'. Έτσι προκύπτουν θέματα χρηστικότητας, αποτελεσματικότητας και κόστους.

Το "κυνήγι" της ανωνυμίας στο διαδίκτυο ξεκινά από το ότι δεν ξέρουμε ποιος είναι απέναντι μας, ποια εταιρεία κρύβεται πίσω από το κάθε site/υπηρεσία καθώς και πως θα χρησιμοποιηθούν τα στοιχεία που δίνουμε. Είναι τέτοια η δομή του Internet που αν δίνουμε ελεύθερα όλα τα προσωπικά μας δεδομένα, είναι πολύ εύκολο μετά για τον καθένα να δημιουργήσει έναν ψηφιακό "φάκελο" για εμάς.

Αν δεν έχουμε κάτι να κρύψουμε, πιθανότατα να μην μας ενοχλεί ιδιαίτερα αυτό (σαν άτομο, αν και μπορεί να καταπατά τα προσωπικά μας δικαιώματα). Ένα μεγάλο κομμάτι όμως αυτών που θέλουν ανωνυμία, είναι και αυτοί που κάνουν την "παρανομία" τους, συνεχώς ή σπανιότερα. Πχ, πόσοι θέλουν να δίνουν το όνομα τους όταν κατεβάζουν ένα τραγούδι, μια ταινία ή κάτι παρόμοιο από το Rapidshare ή από κάποιο torrent?

Υπάρχουν πολλοί που θέλουν να αγοράσουν ένα λογαριασμό (premium account) στο Rapidshare, και ψάχνουν τρόπο για να μην δώσουν τα στοιχεία τους ή κάποια πιστωτική κάρτα, στοιχεία τα οποία θα μπορούσαν να τους συσχετίσουν με αυτά που κατέβασαν. Φυσικά δεν έχουν το ίδιο πρόβλημα όταν δίνουν τα στοιχεία τους με φυσικό τρόπο (χέρι με χέρι ή μέσα ταχυδρομείου για παράδειγμα) σε κάποια εταιρεία, σε έναν διαγωνισμό ή σε κάτι παρόμοιο. Άρα το πρόβλημα εκεί δεν είναι τόσο στο ότι θεωρούν τα στοιχεία τους προσωπικό δεδομένο, όσο στο ότι φοβούνται μην φτάσουν εκεί που δεν πρέπει.

Συνοψίζοντας, η ανωνυμία και το προσωπικό δεδομένα είναι δικαίωμα που δεν πρέπει να το καταπατά και να έχει πρόσβαση σε αυτό κανένας, όταν δεν έχει την συγκατάθεση μας. Το πρόβλημα στο internet ξεκινά από το ότι δεν μπορούμε να

---

[140] http://ru6.cti.gr/bouras/ergasies/foithtes/206_KASTANHS_DHHTRIOS_3871_KABOURGIAS_GEORGIOS_3659.pdf

ελέγξουμε εύκολα που θα φτάσουν τα δεδομένα μας, πόσο θα τα κρατήσουν, ποιος θα τα δει, με τι άλλο θα συσχετιστούν κτλ. Από την άλλη, κανείς δεν απαγορεύει σε κανέναν να δώσει όλα του τα στοιχεία, οπουδήποτε.

8.1 Αποτελέσματα Πτυχιακής Εργασίας

Η ανωνυμία και η ψευδωνυμία υπήρξε ιστορικά μέρος της ζωντανής και ζωηρής πολιτικής συζήτησης. [141] Υπήρχε στην αρχαία Ελλάδα και τη Ρώμη με τα graffiti στους δρόμους, φούντωσε την πρώτη περίοδο της τυπογραφίας με ανώνυμες παμφλέτες για να γίνει εκρηκτική με τη διάχυση του Διαδικτύου. Κάθε τεχνολογική εξέλιξη που ευκόλυνε τον λόγο, διευκόλυνε και την παραγωγή ανώνυμου λόγου. Και όσο προχωράει η τεχνολογία τόσο πιο δύσκολη γίνεται η παρακολούθησή του και από τις αρχές, αλλά και από τους πολίτες. Οι πρώτες δεν μπορούν να επιβάλλουν την «τάξη» (όση, τέλος πάντων, μπορούσαν στην εποχή των μονόδρομων Μέσων) και οι πολίτες δεν μπορούν να τον παρακολουθήσουν λόγω της πληθώρας του. Αν κάποιος έχει διαβάσει δέκα υβριστικά ή συκοφαντικά ανώνυμα σχόλια, τα 'χει διαβάσει όλα.

Το πρόβλημα εντείνεται με την εξέλιξη της τεχνολογίας. Σήμερα, ακόμη κι αν μπορούσαν να ταυτοποιηθούν ποιοι υπολογιστές δημοσιεύουν κάποια πράγματα, η ανωνυμία μπορεί να εξασφαλιστεί από δημοσιεύσεις που θα γίνονται μέσω internet cafe, αλλά και από την πλατεία Συντάγματος! Με την έλευση των ελεύθερων ασύρματων δικτύων μπορεί να πάει κάποιος απέναντι από το υπουργείο Οικονομικών, να ανοίξει τον φορητό του υπολογιστή και να εξαπολύσει κατά του υπουργού όσες ύβρεις ή συκοφαντίες επιθυμεί. Και οι ασύρματες επικοινωνίες είναι το μέλλον του Διαδικτύου.

Υπάρχουν όμως κι άλλα εργαλεία για να εξασφαλιστεί η ανωνυμία. Ένα είναι οι «anonymous remailers». Αυτοί είναι υπολογιστές διάσπαρτοι σε ολόκληρο τον κόσμο οι οποίοι σβήνουν από τα μηνύματα τα ηλεκτρονικά ίχνη του αποστολέα. Άρα, ακόμη κι αν μπορούσαν να βρεθούν τα ίχνη εκείνων που ανωνύμως χυδαιολογούσαν σε σχόλια, θα ήταν αδύνατο αν αυτά περνούσαν από κάποιους «anonymous» ή «pseudonymous remailers».

Ισχυρότερο όμως εργαλείο στην υπηρεσία της ανωνυμίας είναι η κρυπτογραφία. Στη δεκαετία του 1990 έγινε μια ιδιότυπη όσο και άγνωστη επανάσταση. Μερικοί ιδεαλιστές που ασχολούντο με την πληροφορική χρησιμοποίησαν την γνώση της κρυπτογραφίας (που σημειωτέον υπήρχε και υπάρχει στις βιβλιοθήκες των μαθηματικών τμημάτων των πανεπιστημίων) για να φτιάξουν ισχυρά κρυπτογραφικά εργαλεία για τον κάθε πολίτη. Τα εργαλεία αυτά, προς έκπληξη και τρόμο όλων των διωκτικών αρχών του κόσμου μοιράστηκαν και μοιράζονται ευρέως μέσω του Διαδικτύου.

Όπως γίνεται συνολικά με την παγκοσμιοποίηση, το Διαδίκτυο (που είναι μέρος της) αλλάζει ραγδαία τους κανόνες του παιγνιδιού. Η αντιμετώπιση των ζητημάτων που

---

[141] http://www.inout.gr/showthread.php?t=43778

ανακύπτουν προϋποθέτει νέα προσέγγιση. Η παλαιά αντίληψη του κράτους «όλα τα σφάζω, όλα τα μαχαιρώνω» ή περνώ νόμους που θα λύσουν προβλήματα που έχουν χαρακτήρα παγκοσμιότητας, το μόνο που επιτυγχάνει είναι να γελοιοποιεί τη χώρα διεθνώς. Έτσι κι αλλιώς ο έλεγχος 40.000 blogs στην Ελλάδα (100 εκατ. παγκοσμίως) είναι δύσκολος.

Το θέμα της ανωνυμίας στα μπλοκ τίθεται εντελώς διαφορετικά.[142] Καταρχήν δεν είναι βέβαια η Ελλάδα η μόνη χώρα που αντιμετωπίζει το ζήτημα. Όπως μπορεί να φανταστεί κανείς, παρόμοια φαινόμενα κατάχρησης της ελευθερίας γραφής στο διαδίκτυο είναι συνηθισμένα σε όλο τον κόσμο. Η κατάργηση, όμως, της ανωνυμίας στα μπλοκ εξαιτίας των κρουσμάτων συκοφαντικών ή ακόμα και εκβιαστικών σχολίων θα ισοδυναμούσε με την απόφαση να στερηθούμε την ηλεκτρονική αλληλογραφία μόνο και μόνο επειδή γεμίζει κάθε τόσο ο υπολογιστής μας από τα ανεπιθύμητα spam, τα ηλεκτρονικά σκουπίδια που μεταδίδονται αυτόματα σε χιλιάδες αποδέκτες.

Υπάρχει στις ΗΠΑ μια εξαιρετική απόφαση του Ανώτατου Δικαστηρίου της πολιτείας Ντέλαγουερ, με την οποία ανατρέπεται πρωτόδικη απόφαση που διέτασσε να αποκαλυφθεί η ταυτότητα κάποιου σχολιογράφου σε μπλοκ, ο οποίος αναφερόταν με υποτιμητικούς και συκοφαντικούς χαρακτηρισμούς σε δημοτικό σύμβουλο κάποιας πόλης. Η απόφαση του Ανώτατου Δικαστηρίου στηρίζεται στην άποψη ότι δεν μπορεί να εξισωθεί το μπλοκ με τον Τύπο και να υποβληθεί στους ίδιους νομοθετικούς περιορισμούς:

«Τα μπλοκ και οι δικτυακοί χώροι συζητήσεων (chat rooms) είναι χώροι έκφρασης απόψεων. Από τη φύση τους δεν αποτελούν πηγές γεγονότων ή δεδομένων, πάνω στα οποία θα στηριζόταν ένας εχέφρων άνθρωπος. Τουλάχιστον τρία δικαστήρια έχουν πρόσφατα καταλήξει σ' αυτή την παρατήρηση και διαπίστωσαν ότι τα μηνύματα στα μπλοκ είχαν συνήθως γραμματικά και συντακτικά λάθη, ενώ οι περισσότεροι σχολιαστές δεν χρησιμοποιούν καν κεφαλαία γράμματα. Πολλά από τα μηνύματα είναι χυδαία, επιθετικά και γεμάτα υπερβολές. Μ' αυτά τα δεδομένα, οι αναγνώστες είναι απίθανο να αντιμετωπίζουν αυτά τα ανώνυμα μηνύματα ως αληθείς ισχυρισμούς».

Οι παρατηρήσεις αυτές έχουν σημασία, διότι παίρνουν υπόψη τα ιδιαίτερα χαρακτηριστικά αυτού του νέου «μέσου ενημέρωσης», με τα οποία διαφοροποιείται από τον συμβατικό Τύπο (έντυπο και ηλεκτρονικό). Κανείς δεν διαβάζει (και δεν πιστεύει) ό,τι συναντάει στο Internet με την ίδια ευπιστία που διαβάζει την εφημερίδα του. Ακόμα και ο πιο ανίδεος χρήστης που έχει προλάβει να σερφάρει λίγα μόλις λεπτά, διαπιστώνει ότι ο βαθμός αξιοπιστίας των δημοσιεύσεων στο διαδίκτυο ξεκινά από το μηδέν.

Με την ίδια, λοιπόν, επιφυλακτικότητα θα δεχτεί και κάθε εξυβριστική ή συκοφαντική αναφορά σε πρόσωπα από κάποιον ανώνυμο σχολιογράφο. Αλλά δεν υπάρχει ούτε ένας ιστότοπος ελεύθερων συζητήσεων στον παγκόσμιο ιστό που να μην δέχεται επισκέψεις από παρόμοιους υβριστές, συκοφάντες ή απλά

---

[142] http://www.neagenia.com/gr/?p=65

φαντασιόπληκτους. Κανείς δεν τους δίνει ιδιαίτερη σημασία. Και όσο μεγαλώνει το ποσοστό τέτοιου είδους σχολίων σε κάποιο μπλοκ, τόσο μειώνεται η αξιοπιστία και φυσικά η επισκεψιμότητά του.

Από κει και πέρα, είναι ζήτημα του κάθε διαχειριστή ιστολογίου πώς θα αντιμετωπίσει το ενδεχόμενο υβριστικών, συκοφαντικών ή απλώς άσχετων κειμένων, τα οποία προσθέτει ως «σχόλια» (comments ή posts) οποιοσδήποτε επισκέπτης. Ένας από τους παλιότερους έλληνες blogger, ο Νίκος Δήμου, έχει περιγράψει σε παλιότερο κείμενό του πώς υποχρεώθηκε να κλείσει για μια περίοδο το ιστολόγιό του, όταν διαπίστωσε ότι χρειαζόταν ατέλειωτο χρόνο για να διαβάζει, να απαντά και κυρίως να απομακρύνει τα υβριστικά και χυδαία σχόλια ορισμένων αναγνωστών του. Αυτή είναι η μια λύση.

Δεν είναι η πιο πρακτική ούτε η πιο δημοφιλής στις τάξεις των blogger, εφόσον κάθε παρέμβαση του διαχειριστή στα σχόλια των επισκεπτών του μπορεί να θεωρηθεί λογοκριτική. Αλλά όποιος διεκδικεί για τον ιστότοπο ή το ιστολόγιό του τεκμήριο αξιοπιστίας δεν μπορεί να προβάλει –στο όνομα της αλογόκριτης διάδοσης των ιδεών- τα σκουπίδια που προσφέρονται αφειδώς από υβριστές και συκοφάντες ή απλά κακόβουλους επισκέπτες.

Περίληψη Πτυχιακής Εργασίας

Ο σκοπός της ανωνυμίας είναι να προστατεύει την ιδιωτικότητά μας, την ελεύθερη έκφραση των απόψεών μας, την ηλεκτρονική μας ψήφο, την φαρμακευτική μας αγωγή, τα οικονομικά μας θέματα. Η ανωνυμία είναι ένας μηχανισμός που επιτρέπει στους ανθρώπους να εξερευνούν και να πειραματίζονται, να κινούνται μακριά από την κοινωνική αποδοκιμασία άσχετα αν οι πράξεις τους έχουν εγκληματικό χαρακτήρα ή όχι.

Πότε άλλοτε δεν υπήρξε μεγαλύτερη ανάγκη για ανωνυμία και προστασία ιδιωτικού απορρήτου στο Internet. Κυβερνήσεις, οργανισμοί και πολυεθνικές εταιρείες επιχειρούν -καθένας για τους δικούς τους λόγους- να καταγράψουν, να ελέγξουν ή ακόμα και να περιορίσουν τις διαδικτυακές συνήθειες των κυβερνοπολιτών.

Η λέξη «ανωνυμία» πρωτοεμφανίστηκε τον 16^{ο} αιώνα, προέρχεται από την ελληνική γλώσσα και έχει δανειστεί στην αγγλική ως anonymity. Η χρήση της ανωνυμίας μπορεί να προκύψει από την έλλειψη ενδιαφέροντος για μάθηση της φύσης κάποιων χαρακτηριστικών, είτε από την προσπάθεια απόκρυψης τους. Σε όμως ορισμένες περιπτώσεις, η ανωνυμία επιτεύχθηκε και αθέλητα.

Αντί για την ανωνυμία όμως πολλοί επιλέγου να χρησιμοποιούν ψευδώνυμα για την απόκρυψη της αληθινής τους ταυτότητας (π.χ. συγγραφέας, καλλιτέχνης, επαναστάτης κτλ.). Η λέξη ψευδώνυμο σημαίνει πλαστό όνομα. Το ψευδώνυμο μπορεί να είναι καλλιτεχνικό, λογοτεχνικό, φιλολογικό, επαναστατικό ή συνωμοτικό. Προσδιορίζει έναν κάτοχο, δηλ., ένα ή περισσότερα ανθρώπινα όντα που κατέχουν αλλά δεν αποκαλύπτουν τα αληθινά τους ονόματα.

Υπάρχουν πολλοί λόγοι για τους οποίους ένα άτομο μπορεί να επιλέξει να συσκοτίσει την ταυτότητά του και να γίνει ανώνυμο. Αρκετοί από αυτούς τους λόγους, είναι νόμιμοι και θεμιτοί, πολλές πράξεις φιλανθρωπίας πραγματοποιούνται ανώνυμα, γιατί οι ευεργέτες δεν επιθυμούν, για οποιοδήποτε λόγο, να αναγνωρίζονται για τη δράση τους. Επίσης, κάποιος που θεωρεί ότι απειλείται από κάποιον άλλο θα μπορούσε να προσπαθήσει να κρύψει τα στοιχεία του από την απειλή πίσω από διάφορα μέσα της ανωνυμίας, όπως ένας μάρτυρας σε ένα έγκλημα που μπορεί να επιδιώξει να αποφύγει την τιμωρία.

Κάθε τεχνολογική εξέλιξη που διευκόλυνε τον λόγο, όπως το internet, διευκόλυνε και την παραγωγή ανώνυμου λόγου. Και όσο προχωράει η τεχνολογία τόσο πιο δύσκολη γίνεται η παρακολούθησή του και από τις αρχές, αλλά και από τους πολίτες. Την ανωνυμία στην καθημερινή μας ζωή, περά από το ιντερνέτ, την συναντάμε σε διάφορους τομείς, όπως στην φιλανθρωπία, σε καθημερινά κοινωνικά ζητήματα, στον τύπο, στους φορείς HIV, σε οργανώσεις όπως οι Ανώνυμοι Αλκοολικοί, στα καρτοκινητά, σε εμπορικές συναλλαγές και στην εγκληματικότητα. Στο Διαδίκτυο τώρα συναντάμε την ανωνυμία στο ηλεκτρονικό χρήμα (E-cash), την ηλεκτρονική ψηφοφορία (E-voting) και τις Ανώνυμες IP , με τους HTTP proxies.

Από τη στιγμή που δημιουργήθηκε το διαδίκτυο, η ανωνυμία έχει γίνει καθημερινός σκοπός για πολλούς χρήστες. Το internet παρέχει πολύ περισσότερες δυνατότητες για ανωνυμία από τον πραγματικό κόσμο. Δεν είναι σπάνιο φαινόμενο η ύπαρξη ολόκληρων ψηφιακών κοινοτήτων που βασίζονται ή και προωθούν την ανωνυμία

μεταξύ των μελών τους, συνήθως με τη χρήση ψευδωνύμων, δίνοντας στο κάθε μέλος τη διακριτική ευχέρεια να επιλέγει αν και σε ποιους επιθυμεί να αποκαλύψει την πραγματική του ταυτότητα. Τέτοια είναι κυρίως τα newsgroups που αποτελούν ίσως τα πιο ζωντανά σημεία του Internet αφού εκεί συζητούνται χιλιάδες θέματα μεταξύ χρηστών απ' όλο τον κόσμο.

Ισχυρότερο όμως εργαλείο στην υπηρεσία της ανωνυμίας είναι η κρυπτογραφία. Μερικοί ιδεαλιστές που ασχολούντο με την πληροφορική χρησιμοποίησαν την γνώση της κρυπτογραφίας για να φτιάξουν ισχυρά κρυπτογραφικά εργαλεία για τον κάθε πολίτη. Τα εργαλεία αυτά, προς έκπληξη και τρόμο όλων των διωκτικών αρχών του κόσμου μοιράστηκαν και μοιράζονται ευρέως μέσω του Διαδικτύου. Οι τεχνολογίες ανωνυμίας χρησιμεύουν ως τα εργαλεία για την προστασία των ιδιωτικών ηλεκτρονικών συναλλαγών και προστατεύουν την μυστικότητα των χρηστών του Internet από το ένα άκρο της επικοινωνίας έως το άλλο.

Μια τεχνική για την ανώνυμη επικοινωνία σε ένα δίκτυο υπολογιστών είναι η δρομολόγηση onion (Onion Routing). Η ιδέα της δρομολόγησης onion είναι να προστατεύσει την ιδιωτικότητα του αποστολέα και του παραλήπτη του μηνύματος και, επίσης να παρέχει την προστασία του περιεχομένου του μηνύματος καθώς δρομολογείται στο δίκτυο. Το πλεονέκτημα είναι, ότι, αν ένας από τους proxy servers, που χρησιμοποιούνται κατά την δρομολόγηση των μηνυμάτων είναι εκτεθειμένος, η ανώνυμη επικοινωνία μπορεί ακόμα να επιτευχθεί. Μια σημαντική εφαρμογή της δρομολόγησης onion είναι το Tor. Το Tor λειτουργεί με πολλές εφαρμογές που βασίζονται στο πρωτόκολλο TCP όπως προγράμματα άμεσων μηνυμάτων και φυλλομετρητές ιστοσελίδων εμποδίζοντας έτσι άλλα άτομα να μάθουν την φυσική τοποθεσία του χρήστη ή ποιες σελίδες επισκέπτεται.

Ένα άλλο εργαλείο για την επίτευξη της ανωνυμίας είναι η χρήση P2P δικτύων. Μερικά από τα δίκτυα που κοινός ονομάζονται "ανώνυμα P2P" είναι πραγματικά ανώνυμα, υπό την έννοια ότι οι κόμβοι δικτύων δεν φέρνουν κανένα προσδιοριστικό. Άλλα όμως είναι πραγματικά ψευδώνυμα. Αντί να προσδιορίζονται από τις διευθύνσεις IP, οι κόμβοι προσδιορίζονται από τα ψευδώνυμα όπως τα κρυπτογραφικά κλειδιά. Τα δίκτυα αυτά μπορούν να υποστηρίξουν την προστασία της μη δημοφιλούς ομιλίας, μπορούν επίσης να προστατεύσουν τις παράνομες δραστηριότητες που δεν προστατεύονται βάση μερικών ελεύθερων λεκτικών νόμων, όπως η απάτη, δυσφήμηση, η ανταλλαγή της παράνομης πορνογραφίας, η αναρμόδια αντιγραφή οι εργασίες, ή ο προγραμματισμός των ποινικών δραστηριοτήτων. Ακόμα μπορούν να απευθυνθούν σε εκείνους που επιθυμούν να μοιραστούν ενδεχομένως κάποια από τα αρχεία τους.

Ακόμα μια τεχνική για ανώνυμη επικοινωνία είναι η χρήση ανώνυμων remailers. Οι ανώνυμοι remailers είναι υπηρεσίες προώθησης και δρομολόγησης ηλεκτρονικού ταχυδρομείου, όπως και οι κλασσικοί mail servers, με την διαφορά ότι αφαιρούν πρώτα όλες τις επικεφαλίδες που σχετίζονται με την ταυτότητα του αποστολέα. Υπάρχουν 4 είδη remailers: οι Nym servers ή αλλιώς Pseydonymous remailers, οι Cypherpunk anonymous remailers, οι Mixmaster anonymous remailers και οι Mixminion remailers. Καθένας από αυτούς τους τύπους απευθύνεται σε ξεχωριστό κοινό. Πρέπει να δώσουμε ιδιαίτερη προσοχή στα επιχειρησιακά πρότυπα και στους στόχους που έχουμε, στην τοποθεσία και την αξιοπιστία αρχείων πριν επιλέξουμε κάποιον.

Τέλος υπάρχουν web browsers (όπως ο Mozilla firefox), οι οποίοι επιτρέπουν την Ιδιωτική περιήγηση (Private Browsing). Οι web browsers αυτοί δεν αποθηκεύουν πληροφορίες όπως το ιστορικό περιήγησης, εικόνες, βίντεο, Cookies και κείμενα στην μνήμη cache. Αυτό επιτρέπει σε κάποιον χρήστη να περιηγηθεί στο internet χωρίς να αποθηκεύονται τα δεδομένα που μπορούν να ανακτηθούν σε μεταγενέστερη στιγμή με σκοπό να τον ενοχοποιήσουν. Το Private Browsing στοχεύει στο να σιγουρέψει ότι οι διαδικτυακές μας δραστηριότητες δεν θα αφήσουν κανένα ίχνος στον υπολογιστή μας.

Η ανωνυμία και το προσωπικό δεδομένα είναι δικαίωμα που δεν πρέπει να το καταπατά και να έχει πρόσβαση σε αυτό κανένας, όταν δεν έχει την συγκατάθεση μας. Γι' αυτό το λόγο τα παραπάνω είναι απαραίτητη η χρήση των παραπάνω εφαρμογών για πολλούς χρήστες του ιντερνέτ. Παρόλα αυτά όμως οι προσπάθειες στην ανωνυμία δεν συναντιούνται πάντα με την υποστήριξη της κοινωνίας. Υπάρχει μια τάση της κοινωνίας στη δυσπιστία κάποιου ο οποίος καταβάλλει προσπάθεια να διατηρήσει την ανωνυμία τους.

Links

- Anonymity - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Anonymity
- InOut RSS Feed
  http://www.inout.gr/showthread.php?t=19801
- Medieval literature - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Medieval_literature
- Περί ανωνυμίας και λογοκρισίας διευκρινίσεις - Ψευδωνυμία
  http://openitnow.blogspot.com/2007/06/blog-post_487.html
- Pseudonymity - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Pseudonymity
- Pseudonym - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Pseudonym
- M.A. Boudourides: Κοινωνικά θέματα των επικοινωνιών μέσω υπολογιστή
  http://www.math.upatras.gr/~mboudour/articles/ktemy.html
- Εφημερίδα Οδηγητής
  http://www.odigitis.gr/2008/12/07/blogs/
- «Πράκτορας της CIA» η Tansu Ciller από το 1967
  http://www.zougla.gr/news.php?id=44994
- ActionNemesis - Ψευδώνυμα: μάσκες για συγγραφείς
  http://www.actionnemesis.com/v2/index.php?option=com_content&task=view&id=369&Itemid=53
- Alice Sheldon σε James Tiptree
  http://www.altfactor.ath.cx/magazine/aplanet/iss5/tiptree.html
- Το άβατο της Σιμόν ντε Μπωβουάρ (Ανώνυμη γυναίκα)
  http://www.allbooks.gr/book.php?TitlesID=106499
- Πίσω από τα ψευδώνυμα
  http://stavrochoros.pblogs.gr/2009/03/pisw-apo-ta-psefdwnyma-.html
- Filiki Eteria - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Filiki_Eteria
- Απολογητές και ανωνυμία
  http://www.apologitis.com/gr/ancient/apologites.htm
- kathimerini.gr | Ολοι οι δωρητές του πρώην προέδρου
  http://news.kathimerini.gr/4dcgi/_w_articles_world_2_21/12/2008_296934

- Το σκοτεινό πρόσωπο του σύγχρονου απαγωγέα - ΤΟ ΒΗΜΑ
  http://www.tovima.gr/default.asp?pid=2&ct=34&artid=99815&dt=31/05/1998

- Cosmo.gr - Δεκατέσσερις απαγωγές στην Ελλάδα από το 1990
  http://www.cosmo.gr/News/Hellas/228165.html

- Ελευθεροτυπία - Το παρελθόν της επωνυμίας
  http://www.enet.gr/online/online_fpage_text?dt=05/02/2005&id=49834608,55636976,63658352

- Καταλαβαίνοντας την Ανωνυμία
  http://www.aa-greece.gr/11.htm

- isotimia.gr - Παρελθόν τα ανώνυμα καρτοκινητά
  http://www.isotimia.gr/default.asp?pid=24&ct=6&artid=73802

- η-Επιχειρείν: Ανωνυμία στο Internet: "Ταξιδιώτες" χωρίς όνομα
  http://www.go-online.gr/ebusiness/specials/article.html?article_id=417

- Electronic money - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Electronic_money

- Electronic Payments
  http://el.tech-faq.com/what-are-electronic-payments.shtml&prev=hp

- ECash Direct - Συχνές ερωτήσεις λογαριασμού ECash
  http://gre.ecashdirect.net/faq/faq-ecash.html

- E-VOTING: Συνταγματικές προυποθέσεις
  http://www.infolaw.gr/articles.asp?ArticleID=602

- HTTP Proxies
  http://el.tech-faq.com/http-proxies.shtml&prev=hp&rurl=translate.google.com

- Προσωπικό δεδομένο η διεύθυνση IP
  http://www.pcw.gr//Article/News-General-Latest/IP_address_private_data/179-2945.html

- Onion routing - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Onion_routing

- David Chaum - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/David_Chaum

- Mix network - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Mix_network

- Tor (anonymity network) - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Tor

- Tor: Overview
  http://www.torproject.org/overview.html

- Techinfo- Proxy Server
  http://www.call-centre.cyta.com.cy/techinfo.htm#PROXY%20SERVER

- Ασφάλεια των υπολογιστών
  http://community.athens.indymedia.org/index.php/topic,458.0/prev_next,prev.html#new

- Proxy server - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Proxy_server

- SOCKS - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/SOCKS

- What is a SOCKS proxy server? (FAQ proxy)
  http://www.freeproxy.ru/en/free_proxy/faq/what_is_socks_proxy.htm

- Privoxy - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Privoxy

- Εγκατάσταση/Ρύθμιση για Tor, Privoxy και Tsocks (ανωνυμία στο net)
  http://community.athens.indymedia.org/index.php?topic=427.0

- Anonymous Surfing: How to Conceal Your Digital Identity While Online
  http://netforbeginners.about.com/od/internet101/f/anonymous_surf.htm

- Vidalia (Tor/Privoxy) : Protecting Your Privacy Online, Anonymously
  http://www.tomsguide.com/us/security-online-privacy,review-1055-4.html

- Torcap
  http://www.freehaven.net/~aphex/torcap/

- Cat's Page - electronics projects
  http://www.virtualventures.ca/~cat/

- FreeCap Homepage - What is FreeCap?
  http://www.freecap.ru/eng/?p=whatis

- Setting up Tor with Freecap and Proxomitron
  http://prxbx.com/forums/showthread.php?tid=639

- Internet Privacy Software - XeroBank
  https://xerobank.com/download/

- Torchat - Project Hosting on Google Code
  http://code.google.com/p/torchat/

- Anonymous P2P - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Anonymous_P2P
- Bitblinder - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Bitblinder
- GNUnet - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/GNUnet
- I2P - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/I2P
- Phex - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/I2phex#Anonymous_Phex
- Nodezilla - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Nodezilla
- OFFSystem - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Owner_free_filing_system
- Omemo - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Omemo
- Osiris (Serverless Portal System) - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Osiris_(Serverless_Portal_System)
- Perfect Dark (P2P) - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Perfect_Dark_(P2P)
- StealthNet - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/StealthNet
- StegoShare - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/StegoShare
- MUTE: Simple, Anonymous File Sharing
  http://mute-net.sourceforge.net/howPrivacy.shtml
- MUTE: Get MUTE at SourceForge.net
  http://sourceforge.net/projects/mute-net/
- Ants P2P
  http://www.zeropaid.com/antsp2p/
- ANts P2P - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/ANts_P2P
- Ants P2P Guide
  http://antsp2p.altervista.org/

- Privacy - Κρυπτογράφηση
  http://www.it.uom.gr/project/MultimediaTechnologyNotes/extra/append10.htm

- Andr&eacute Bacard's "Anonymous Remailer F.A.Q.
  http://www.andrebacard.com/remail.html

- Anonymous remailer - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Anonymous_remailer

- Cypherpunk anonymous remailer - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Cypherpunk_anonymous_remailer

- Mixmaster anonymous remailer - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Mixmaster_anonymous_remailer

- η-Επιχειρείν: Remailers
  http://www.go-online.gr/ebusiness/specials/article.html?article_id=420

- Judith S. Donath: Ταυτότητα και εξαπάτηση
  http://hyperion.math.upatras.gr/courses/newcommmedia99-00/papers99-00/donath.html

- Hushmail - Free Email with Privacy
  www.hushmails.com

- Send fake email
  http://www.sendfakemail.com/

- Private Idaho Email Version 5 Supports PGP 5 and PGP 6
  http://www.itech.net.au/pi/

- Privacy mode - Wikipedia, the free encyclopedia
  http://en.wikipedia.org/wiki/Private_browsing

- Mozilla Europe
  http://www.mozilla-europe.org/el/firefox/features/#private-browsing

- Private Browsing in Firefox
  http://ehsanakhgari.org/blog/2008-11-04/dont-leave-trace-private-browsing-firefox

- Firefox Private Browsing, ένα click μακρυά
  http://www.pestaola.gr/firefox-private-browsing/

- Private Browsing
  http://support.mozilla.com/en-US/kb/Private+Browsing#What_Private_Browsing_will_not_retain

- Ανωνυμία και αξιοπιστία στον τύπο και το Internet - Νέα Γενιά
  http://www.neagenia.com/gr/?p=65