Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Μελέτη και αποτίμηση των ανώνυμων κοινωνικών δικτύων

Βασίλειος Χατζηστεφάνου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2017

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Μελέτη και αποτίμηση των ανώνυμων κοινωνικών δικτύων

Βασίλειος Χατζηστεφάνου

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση
των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά και Επικοινωνιακά Συστήματα
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2017

Περίληψη

Αντικείμενο της παρούσας διατριβής είναι η αποτίμηση της ανωμυμοποίησης που παρέχουν τα ανώνυμα κοινωνικά δίκτυα. Η αύξηση των δικτύων αυτών τα τελευταία χρόνια οφείλεται στην ανάγκη των χρηστών για ιδιωτικότητα και προστασία των προσωπικών τους δεδομένων, ειδικά σε μια εποχή όπου ενημερωνόμαστε συνεχώς για περιστατικά διαρροής προσωπικών δεδομένων των χρηστών. Για να επιτευχθεί αυτό, τα εν λόγω δίκτυα «διαφημίζουν» ότι δεν αντλούν στοιχεία από τους χρήστες τα οποία θα μπορούσαν να οδηγήσουν στην ταυτοποίησή τους, επομένως η μελέτη ως προς το αν πράγματι παρέχεται ανωνυμία στους χρήστες αυτών των δικτύων αποτελεί ένα σημαντικό ερευνητικό ερώτημα που θα πρέπει να απαντηθεί.

Η παρούσα διατριβή αναλύει πέντε δημοφιλή ανώνυμα κοινωνικά δίκτυα - συγκεκριμένα, τα Social Number, Anomo, Whisper, Candid, και Yik Yak - στο λειτουργικό σύστημα Android για «έξυπνες» κινητές ή φορητές συσκευές και εξετάζει τα δεδομένα που αντλούν οι εφαρμογές αυτές από το κινητό του χρήστη με χρήση δυναμικής ανάλυσής τους.

Τα αποτελέσματα καταδεικνύουν ότι αν και τα δίκτυα αυτά προσπαθούν να προστατέψουν τα προσωπικά δεδομένα των χρηστών τους, ο τρόπος λειτουργίας των εφαρμογών αυτών υπό περιπτώσεις θα μπορούσε να οδηγήσει στην παύση της ανωμυμοποίησης των δεδομένων αυτών και, ως εκ τούτου, δεν θα πρέπει να εκλαμβάνεται ότι παρέχουν πλήρη ανωνυμία.

Λέξεις-Κλειδιά:

Ανωμυμοποίηση, προσωπικά δεδομένα, ανώνυμα κοινωνικά δίκτυα, δυναμική ανάλυση, «έξυπνες» συσκευές

Summary

This thesis studies and evaluates the anonymity provided by anonymous social networks. The growth of these networks over the past few years is strongly contingent on the users' need for privacy and protection of their personal data, which is further accentuated by the fact that we are continually informed of personal data breaches. Therefore, these networks advertise that they do not collect data from users that could reveal their identity; hence, focusing on whether there are ways – and if so, up to that extent - to end the anonymity of these network users is a major research question to be answered.

This thesis analyzes five popular anonymous social networks – namely, Social Number, Anomo, Whisper. Candid, Yik Yak on the Android operating system and examines through dynamic analysis the data that these applications obtain from the user's smart device. The results show that although these networks are trying to protect the personal data of their users, there are cases where anonymity cannot be ensured. Therefore, we should not take the anonymity of these networks for granted.

Key-words

Anonymity, Personal data, anonymous social networks, dynamic analysis, «smart» devices

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή μου Κωνσταντίνο Λιμνιώτη για την πολύτιμη βοήθεια , καθοδήγηση αλλά και υπομονή του, σε όλη την πορεία ανάπτυξης και συγγραφής της υπάρχουσας εργασίας.

Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου για την στήριξη και υπομονή που έδειξε καθ' όλη την διάρκεια των σπουδών μου.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Ζούμε σε μια εποχή όπου η συνεχής εξέλιξη της τεχνολογίας έχει επιφέρει σημαντικά οφέλη για τον άνθρωπο και αποτελεί αναπόσπαστο κομμάτι της κοινωνίας. Με αυτή έχουμε την δυνατότητα να αποκτούμε πρόσβαση σε πληροφορίες που μερικά χρόνια πριν δεν θεωρούσαμε καν εφικτό. Όλη αυτή η εξέλιξη έχει επηρεάσει όπως είναι φυσικό και τον τομέα της τηλεπικοινωνίας με την είσοδο κινητών τηλεφώνων νέας γενιάς, τηλέφωνα με την χρήση των οποίων ένας χρήστης μπορεί να κάνει πολύ περισσότερα πράγματα από τα να επικοινωνήσει με κάποιον άλλο. Τα «έξυπνα» κινητά τηλέφωνα ή αλλιώς smartphones αποτελούν πλέον κανονικούς υπολογιστές και είναι ικανά για να εκτελέσουν πολλαπλές σύνθετες λειτουργίες καθιστώντας τα ένα πολύ χρήσιμο εργαλείο στα χέρια ενός ανθρώπου. Σε αυτά έχουν αναπτυχθεί διάφορα λειτουργικά συστήματα όπως είναι το Android και το iPhone OS, τα οποία δίνουν τη δυνατότητα στους χρήστες των κινητών να «κατεβάσουν» εφαρμογές με τις οποίες μπορούν να ενημερωθούν, να παίξουν, αλλά και να επικοινωνήσουν ποικιλοτρόπως με άλλους χρήστες.

Ως συνέπεια αυτού του φαινομένου, τα τελευταία χρόνια έχουμε την εμφάνιση των κοινωνικών δικτύων όπως το facebook και το twitter. Τα κοινωνικά δίκτυα αποτελούν δίκτυα στα οποία ένας χρήστης, αφού κάνει εγγραφή, μοιράζεται πληροφορίες της προσωπικής του ζωής με ένα σύνολο άλλων ατόμων («φίλων» του) και αλληλεπιδρά μαζί τους. Τα δίκτυα αυτά, τα οποία μπορεί να τα αξιοποιήσει κανείς είτε μέσα από τον υπολογιστή του είτε μέσω του κινητού του τηλεφώνου ή άλλης «έξυπνης» φορητής ηλεκτρονικής συσκευής, αντλούν και ενίοτε διαμοιράζουν σε τρίτους ένα μεγάλο σύνολο από προσωπικές πληροφορίες του χρήστη. Στα πλεονεκτήματα αυτών των δικτύων

συγκαταλέγεται η δυνατότητα που δίνουν στους χρήστες τους να εκφέρουν την άποψή τους για όποιο θέμα επιθυμούν, το να σχολιάσουν τις απόψεις άλλων και, γενικότερα, να ενισχυθούν οι δυνατότητες ηλεκτρονικής επικοινωνίας μεταξύ προσώπων. Τα ανωτέρω συνιστούν μία μεγάλη συγκέντρωση και κοινοποίηση προσωπικών δεδομένων των χρηστών των κοινωνικών δικτύων, αφού προσωπικά τους στοιχεία όπως ονοματεπώνυμα, προτιμήσεις, φιλίες, απόψεις κ.α. δημοσιεύονται στα κοινωνικά δίκτυα και, κατά συνέπεια, δεν είναι πάντα εύκολα ελέγξιμη η περαιτέρω χρήση τους. Αυτή η μεγάλη συγκέντρωση προσωπικών πληροφοριών μπορεί αναμφίβολα να επιφέρει και αρνητικά αποτελέσματα: για παράδειγμα, δεν είναι λίγες οι φορές όπου η γνώμη κάποιου μπορεί να έχει αρνητικές για τον ίδιο επιπτώσεις στην πραγματική του ζωή λόγω ακριβώς του ότι η γνώμη αυτή αναρτήθηκε σε κάποιο μέσο κοινωνικής δικτύωσης.

Σε μια προσπάθεια εξέλιξης των κοινωνικών δικτύων και με γνώμονα την προστασία της ιδιωτικότητας των χρηστών άρχισαν τα τελευταία χρόνια να εμφανίζονται τα λεγόμενα ανώνυμα κοινωνικά δίκτυα: πρόκειται για κοινωνικά δίκτυα τα οποία επιτρέπουν στους χρήστες τους να τα χρησιμοποιούν χωρίς να αποκαλύπτουν την ταυτότητά τους, παρέχοντας με αυτόν τον τρόπο ένα είδος ανωνυμίας σε αυτούς. Η συγκεκριμένη διατριβή έρχεται να μελετήσει ακριβώς τη συμπεριφορά των εφαρμογών των ανώνυμων κοινωνικών δικτύων, αναλύοντας τα δεδομένα που συλλέγουν από ένα «έξυπνο» κινητό τηλέφωνο προκειμένου να αξιολογηθεί ο βαθμός ανωνυμίας των χρηστών που επιτυγχάνεται. Προς τούτο, πρέπει να σημειωθεί ότι – όπως αναλύεται στο Κεφάλαιο 2 - η Ευρωπαϊκή νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων ορίζει ότι, προκειμένου κάποια δεδομένα να είναι ανώνυμα, δεν πρέπει να υπάρχει κανένας τρόπος, λαμβάνοντας υπόψη κάθε πρόσφορο μέσο που μπορεί ενδεχομένως να χρησιμοποιηθεί, να αποκαλυφθεί η ταυτότητα των χρηστών στους οποίους τα δεδομένα αυτά αναφέρονται. Συνεπώς, δεδομένου ότι τα εν λόγω δίκτυα επικαλούνται την ανωνυμία των χρηστών ως σημαντικό πλεονέκτημά τους, καθίσταται ιδιαίτερα σημαντικό το να διερευνηθεί αν πράγματι η ανωνυμία αυτή διασφαλίζεται.

Στο πλαίσιο αυτό, η παρούσα διατριβή μελετά τα δεδομένα που συλλέγουν οι πιο γνωστές εφαρμογές ανώνυμων κοινωνικών δικτύων, προκειμένου να διερευνηθεί αν από τα δεδομένα αυτά καθίσταται εφικτή, έστω και υπό προϋποθέσεις, η αναγνώριση των χρηστών τους. Τα δίκτυα που θα μελετηθούν είναι το Whisper,Candid,Anomo,YikYak και SocialNumber και ο λόγος που επιλέχθηκαν τα συγκεκριμένα 5 ανώνυμα κοινωνικά δίκτυα είναι καθώς είναι ιδιαίτερα δημοφιλή αλλά επίσης και λόγω του ότι παρουσιάζουν διαφορετικό τρόπο λειτουργίας καθώς κάποια από αυτά απαιτούν από τον χρήστη να δημιουργήσει ένα προφίλ ενώ κάποια άλλα όχι. Τον Απρίλιο του 2017 – και ενώ ήδη είχε ολοκληρωθεί η έρευνα στο πλαίσιο της παρούσας διατριβής - το YikYak ανακοίνωσε την διακοπή της λειτουργίας του: παρόλα αυτά, η έρευνα που έγινε στο δίκτυο αυτό και προηγήθηκε του Απριλίου 2017 δείχνει την λειτουργία ενός τυπικού ανώνυμου κοινωνικού δικτύου.

Για τους ανωτέρω ερευνητητικούς σκοπούς, αναπτύχθηκε κατάλληλο πειραματικό περιβάλλον στο οποίο χρησιμοποιείται το λειτουργικό σύστημα Android, προκειμένου να αναλυθούν - με την χρήση εφαρμογών ελεύθερου λογισμικού - τα δεδομένα που συλλέγουν αυτές οι εφαρμογές από το κινητό κάποιου χρήστη. Όπως καταδεικνύει η έρευνά μας, δεν μπορεί να επιτευχθεί απόλυτη ανωνυμία από τις εν λόγω εφαρμογές και συνεπώς εξαλουθεί να χρήζει ιδιαίτερης προσοχής η χρήση των εφαρμογών αυτών.

1.1 Δομή της διατριβής

Όπως προαναφέρθηκε, αντικείμενο της παρούσας διατριβής είναι η μελέτη των πλέον γνωστών εφαρμογών ανώνυμων κοινωνικών δικτύων ως προς το βαθμό της ανωνυμίας που πράγματι παρέχουν στους χρήστες τους. Ειδικότερα, η δομή της διατριβής είναι η εξής:

Στο κεφάλαιο 2 γίνεται μια εισαγωγή στην έννοια των προσωπικών δεδομένων, με έμφαση και στο σχετικό νομοθετικό πλαίσιο. Στο κεφάλαιο αυτό γίνεται ουσιαστικά η διάκριση μεταξύ των εννοιών προσωπικά δεδομένα, ψευδωνυμοποιημένα δεδομένα και ανώνυμα δεδομένα.

Το κεφάλαιο 3 παρουσιάζει το λειτουργικό σύστημα Android και τον τρόπο με τον οποίο λειτουργούν οι εφαρμογές σε αυτό, προκειμένου να γίνει κατανοητή η λογική που διέπει τις εφαρμογές των ανώνυμων κοινωνικών δικτύων στο συγκεκριμένο λειτουργικό σύστημα. Επίσης γίνεται αναφορά σε προγενέστερες σχετικές έρευνες, ενώ περιγράφεται και ο διαχωρισμός ανάμεσα στους διαφορετικούς τρόπους ανάλυσης των εφαρμογών.

Το κεφάλαιο 4 αποτελεί ουσιαστικά τον κεντρικό άξονα της διατριβής, περιγράφοντας την ανάλυση που πραγματοποιήθηκε για την αντιμετώπιση των ερευνητικών ζητημάτων αλλά και τα αποτελέσματά της. Ειδικότερα, το κεφάλαιο αυτό αποτυπώνει τόσο την διαδικασία που ακολουθήθηκε για την δημιουργία του περιβάλλοντος εργασίας της διατριβής όσο και περιγραφή της ακριβούς μεθοδολογίας που ακολουθήθηκε για την ανάλυση της λειτουργίας των εφαρμογών των ανώνυμων δικτύων.

Στο κεφάλαιο 5 περιγράφεται με ποιον τρόπο θα μπορούσε κανείς να συνδυάσει δεδομένα που συλλέγουν οι ανώνυμες εφαρμογές κοινωνικών δικτύων με άλλα, δημόσια προσβάσιμα, δεδομένα – όπως είναι τα δεδομένα του κοινωνικού δικτύου Twitter - προκειμένου να οδηγηθεί σε επιτυχή ταυτοποίηση ενός χρήστη ανώνυμου κοινωνικού δικτύου.

Τέλος, στο Κεφάλαιο 6 γίνεται μία σύνοψη των ερευνητικών αποτελεσμάτων της διατριβής, με καταγραφή των συμπερασμάτων αλλά των ενδεχόμενων μελλοντικών ερευνητικών βημάτων.

Κεφάλαιο 2

Προσωπικά και ανώνυμα δεδομένα: ορισμοί

Τα προσωπικά δεδομένα – ή δεδομένα προσωπικού χαρακτήρα - είναι, σύμφωνα με την Οδηγία 95/46/ΕΚ [08] κάθε πληροφορία, είτε είναι άμεση είτε έμμεση που αναφέρεται σε φυσικό πρόσωπο και χαρακτηρίζει το υποκείμενο από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη. Για παράδειγμα, προσωπικά δεδομένα μπορεί να θεωρηθεί κάθε πληροφορία που μας χαρακτηρίζει ως άτομα όπως το όνομά μας, η διεύθυνσή μας είτε ταχυδρομική είτε ηλεκτρονική (e-mail), το τηλέφωνό μας ,τα ενδιαφέροντά μας, οι απόψεις μας, η εικόνα μας κ.α. Ωστόσο, πρέπει να σημειωθεί ότι ως προσωπικά δεδομένα νοούνται και άλλες πληροφορίες ακόμα και αν σε αυτές δεν είναι προφανές σε ποιο άτομο αναφέρονται αλλά θα μπορούσε υπό προϋποθέσεις αυτό να ταυτοποιηθεί. Για παράδειγμα, το ψευδώνυμό μας (nickname) σε μια δικτυακή υπηρεσία, ακόμα και αν δεν παραπέμπει στο πραγματικό μας ονοματεπώνυμο, όπως επίσης και η IP διεύθυνση του υπολογιστή μας από τον οποίο εισερχόμαστε στο διαδίκτυο, θεωρούνται επίσης προσωπικά δεδομένα.

Με το θεσμικό πλαίσιο της προστασίας προσωπικών δεδομένων, τίθενται προϋποθέσεις νομιμότητας της επεξεργασίας προσωπικών δεδομένων, καθώς επίσης αναγνωρίζονται συναφή δικαιώματα και υποχρεώσεις, στο πλαίσιο προστασίας του θεμελιώδους αγαθού της ιδιωτικότητας. Η σχετική προαναφερθείσα οδηγία 95/46/ΕΚ έχει κατάλληλα ενσωματωθεί στα Κράτη-Μέλη (π.χ. στην Ελλάδα είναι σε ισχύ ο σχετικός νόμος 2472/1997) και πρόκειται να αντικατασταθεί το Μάιο του 2018 από το νέο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων 2016/679 [17]. Ο νέος Γενικός Κανονισμός θα έχει άμεση ισχύ σε όλα τα Κράτη – Μέλη ενιαία, καταργώντας την Οδηγία 95/46/ΕΚ, θέτοντας πιο αυστηρούς κανόνες και ενισχύοντας την προστασία των δεδομένων των φυσικών προσώπων. Σύμφωνα με το νέο Κανονισμό, ως δεδομένα προσωπικού χαρακτήρα νοείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»), όπου το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό («online») αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

2.1 Ανώνυμα δεδομένα και αναγνωριστικά

Δεδομένα που δεν μπορούν να οδηγήσουν σε αναγνώριση (ταυτοποίηση) κάποιου προσώπου, αποκαλούνται ανώνυμα δεδομένα. Τα ανώνυμα δεδομένα δεν θεωρούνται προσωπικά δεδομένα. Τόσο στην οδηγία 95/46/ΕΚ όσο και στο νέο Γενικό Κανονισμό 679/2016 αναφέρεται ρητώς ότι οι αρχές της προστασίας των δεδομένων δεν εφαρμόζονται σε δεδομένα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε να μην μπορεί να εξακριβωθεί πλέον η ταυτότητα του προσώπου στο οποίο ανφέρονται. Με άλλα λόγια, το αυστηρό νομικό πλαίσιο που διέπει την προστασία των προσωπικών δεδομένων δεν εφαρμόζεται σε ανώνυμα δεδομένα.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι για να εκτιμηθεί αν τα δεδομένα μπορούν να οδηγήσουν σε αναγνώριση (δηλαδή αν είναι πράγματι ανώνυμα ή όχι), θα πρέπει να ληφθεί υπόψη κάθε δυνατό μέσο που μπορεί να διαθέτει ένας ο οποίος θέλει να άρει την ανωνυμία: αυτό σημαίνει ότι είναι, δυστυχώς , εύκολο να θεωρούμε κάποια δεδομένα ανώνυμα χωρίς πραγματικά να είναι, γιατί δεν έχουμε σκεφτεί όλους τους πιθανούς τρόπους και μέσα που μπορεί να χρησιμοποιήσει κάποιος για να αναγνωρίσει κάποιο πρόσωπο από τα ανωμυμοποιημένα δεδομένα.

Ειδικότερα, στη Σκέψη 26 στο Προοίμιο της Οδηγίας 95/46/ΕΚ αναφέρεται ότι «για να διαπιστωθεί αν η ταυτότητα ενός προσώπου μπορεί να εξακριβωθεί, πρέπει να λαμβάνεται υπόψη το σύνολο των μέσων που μπορούν ευλόγως να χρησιμοποιηθούν, είτε από τον υπεύθυνο της επεξεργασίας, είτε από τρίτο, για να εξακριβωθεί η ταυτότητα του εν λόγω προσώπου». Περαιτέρω, στη Σκέψη 26 στο Προοίμιο του Γενικού Κανονισμού αναφέρεται ακόμα ειδικότερα το εξής: «Οι αρχές της προστασίας δεδομένων θα πρέπει να εφαρμόζονται σε κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο. Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου. Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας».

Δηλαδή, στο Γενικό Κανονισμό αναφέρεται ρητώς ότι αφενός η ψευδωνυμοποίηση δεν συνιστά κατά κανόνα ανωνυμοποίηση, καθώς επίσης και

ότι πρέπει να συνυπολογίζεται κάθε τρέχουσα τεχνολογική εξέλιξη που μπορεί να αξιοποιηθεί για την αναγνώριση ενός προσώπου, προκειμένου να αποφανθεί κανείς αν πράγματι υπάρχει ανωνυμία.

Δυο τρόποι με τους οποίους κάποιος θα μπορούσε να αναγνωρίσει ένα πρόσωπο μέσα από ανωμυμοποιημένα δεδομένα είναι με την ανίχνευση κάποιου αναγνωριστικού ή κάποιου ψευδο-αναγνωριστικού.

Με τον όρο αναγνωριστικό (identifiers) αναφερόμαστε σε κάποιο στοιχείο το οποίο μπορεί να αποκαλύψει απ' ευθείας κάποιο άτομο (π.χ. αριθμός ταυτότητας, ΑΦΜ, αριθμός κοινωνικής ασφάλισης), ενώ με τον όρο ψευδο-ανωμυμοποίηση (Quasi-identifier) αναφερόμαστε σε στοιχεία τα οποία κατ' αρχάς δεν ταυτοποιούν απ' ευθείας το άτομο αλλά αν συνδυαστούν με κάποιες εξωτερικές πληροφορίες μπορούν να προσδιορίσουν μοναδικά ένα άτομο (ταχυδρομικός κώδικας, ημερομηνία γέννησης, φύλο). Προφανώς, η απαλοιφή των αναγνωριστικών είναι αναγκαία προϋπόθεση για την επίτευξη της ανωνυμίας, αλλά δεν αρκεί πάντα: εξάλλου, η αντικατάσταση ενός αναγνωριστικού με ένα άλλο, χωρίς νόημα, κωδικό που αναφέρεται πάντα στο άτομο αυτό αποτελεί ψευδωνυμοποίηση η οποία, όπως ρητώς επισημαίνει και ο νέος Κανονισμός, δεν συνιστά από μόνη της ανωνυμοποίηση.

2.2 Κοινωνικά δίκτυα

Με τον όρο κοινωνικά δίκτυα αναφερόμαστε σε web-based υπηρεσίες οι οποίες επιτρέπουν σε ανθρώπους να δημιουργήσουν ένα δημόσιο προφίλ μέσα σε ένα σύστημα και να δημιουργήσουν μια λίστα από άλλους χρήστες με τους οποίους θα μοιράζονται μια σύνδεση. Το είδος και η φύση της κάθε σύνδεσης διαφέρει ανάλογα με την πλατφόρμα κοινωνικής δικτύωσης που επιλέγει ο κάθε χρήστης.

Κατά κανόνα στα κοινωνικά δίκτυα οι χρήστες έχουν την δυνατότητα να δημοσιοποιήσουν ένα σύνολο από προσωπικές τους πληροφορίες όπως την τοποθεσία τους , τις φωτογραφίες τους, να ανεβάσουν προσωπικά τους βίντεο όπως επίσης και να συνομιλήσουν με ένα σύνολο από άλλους χρήστες στους οποίους δίνεται μια ονομασία «φίλοι» ή «επαφές».

Τα μέσα κοινωνικής δικτύωσης θα μπορούσαν να κατηγοριοποιηθούν στις παρακάτω ενότητες [21]:

1. Βασισμένα στην κοινωνική δικτύωση
    - Κοινωνικά Δίκτυα (Facebook, MySpace, Linkedin)
    - Ιστολόγια (Blogs) (Blogger, WordPress)
    - Microblogging (Twitter, Tumblr)
    - Wikis (Wikipedia, Wikinews)

2. Βασισμένα στο περιεχόμενο
    - Φωτογραφίες και εικόνες (flickr, deviantArt, Photobucket)
    - Βίντεο (YouTube, Dailymotion, Vimeo)
    - Μουσική (Last.fm, MySpace Music, SoundCloud)
    - Παρουσιάσεις και αρχεία κειμένων (SlideShare, Scribd)

3. Βασισμένα σε μία λειτουργία
    - Live broadcast (Skype, Ustream, justin.tv)
    - Bookmark Links (Delicious, Diigo)
    - Events (Eventful)
    - Τοποθεσίες (Foursquare)
4. Βασισμένα στα ενδιαφέροντα
    - Ειδήσεις (Digg)
    - Reviews (flixter, goodreads, Yelp)

- Αγορές (Blippy)

Τα μέσα κοινωνικής δικτύωσης αποτελούν μία κατ' εξοχήν περίπτωση διαρκούς επεξεργασίας προσωπικών δεδομένων, μεγάλης έκτασης.

2.3 Ανώνυμα κοινωνικά δίκτυα

Τα ανώνυμα κοινωνικά δίκτυα αποτελούν μια υποκατηγορία των κοινωνικών δικτύων. Ο αριθμός των χρηστών που χρησιμοποιεί αυτά τα δίκτυα αυξάνεται σταδιακά τα τελευταία χρόνια, γεγονός που οφείλεται σε μεγάλο βαθμό στην δυνατότητα που προσφέρουν στους χρήστες τους να επικοινωνούν «ανώνυμα».

Ο τρόπος με τον οποίο τα δίκτυα επιτυγχάνουν την ανωνυμία ποικίλλει: σε άλλα δεν χρειάζεται να εισάγει κανείς κάποιο όνομα χρήστη και κατά την σύνδεση γίνεται αυτόνομα η απόδοση κάποιου ψευδωνύμου, ενώ σε άλλα ζητείται από τον χρήστη να συνδεθεί με την βοήθεια κάποιου άλλου επώνυμου δικτύου (π.χ. Facebook) και με αυτό τον τρόπο το ανώνυμο δίκτυο «προτείνει» στον χρήστη άτομα και θέματα συζήτησης.

Η ανωνυμία των δικτυών αυτών έχει επιδράσεις και στο περιεχόμενο των δημοσιεύσεων ενός χρήστη. Τα ανώνυμα κοινωνικά δίκτυα χρησιμοποιούνται σε μεγάλο βαθμό από χρήστες που θέλουν να εκφράσουν αρνητικά συναισθήματα όπως θλίψη και τύψεις [07]. Το μεγάλο πλήθος αρνητικών δημοσιεύσεων στα ανώνυμα δίκτυα και η αύξηση του διαδικτυακού εκφοβισμού (cyberbulling) που δέχονται κάποιοι χρήστες έχει ωθήσει τα δίκτυα αυτά να δομήσουν αυστηρές πολιτικές χρήσης για να προστατέψουν τους χρήστες τους. Χαρακτηριστικό παράδειγμα είναι το ανώνυμο κοινωνικό δίκτυο Secret το οποίο λόγω του ότι δεν κατάφερε να περιορίσει αυτό το αρνητικό φαινόμενο αναγκάστηκε να σταματήσει τη λειτουργία του. Για την αποφυγή παρόμοιων καταστάσεων, πολλά από τα υπόλοιπα ανώνυμα κοινωνικά δίκτυα λαμβάνουν ειδικά μέτρα προστασίας των χρηστών τους. Τα μέτρα αυτά περιλαμβάνουν εξέταση του περιεχομένου των δημοσιεύσεων ενός χρήστη και χαρακτηρισμού του βάσει αυτών των δημοσιεύσεων. Με αυτό τον τρόπο προσπαθούν να διακρίνουν τους χρήστες με βάση τις δημοσιεύσεις τους: χαρακτηριστικό παράδειγμα είναι το ανώνυμο δίκτυο Candid.

Κεφάλαιο 3

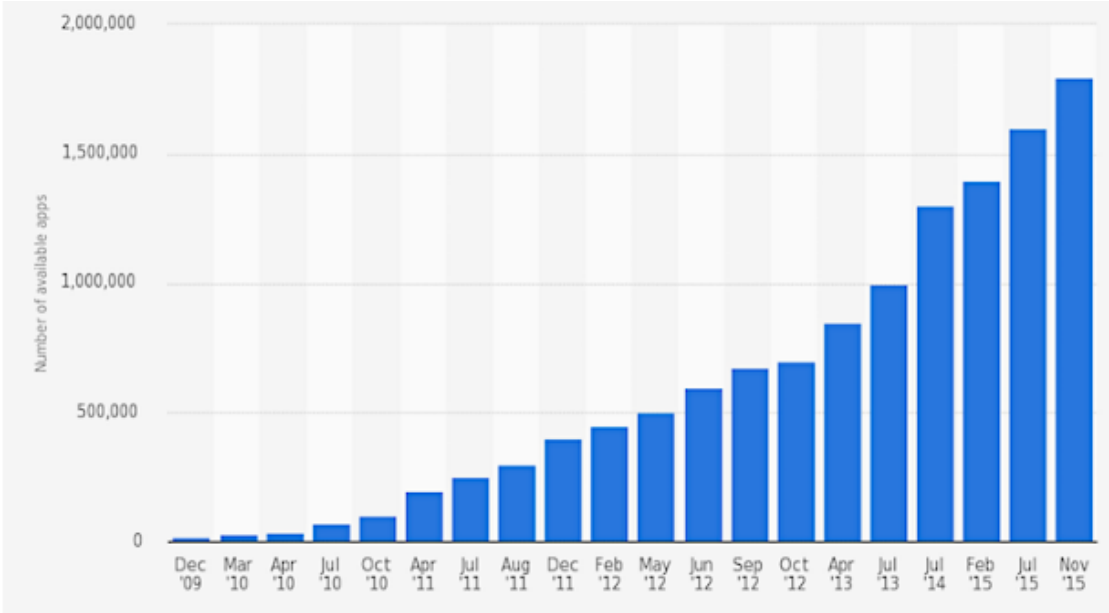
Λειτουργικό σύστημα Android: Εφαρμογές και α-ναγνωριστικά "έξυπνων" συσκευών

Το λειτουργικό σύστημα Android έχει καταφέρει να αποτελεί το κυρίαρχο λειτουργικό σύστημα για φορητές συσκευές καταλαμβάνοντας περίπου το 52,3% της αγοράς των κινητών τηλεφώνων στην Αμερική στα τέλη του 2013 και το 47,7% της αγοράς των tablet [11]. Χαρακτηριστικό είναι ότι, σύμφωνα με έρευνες, κάθε μέρα ενεργοποιούνται περισσότερα από 1,3 εκατομμύρια συσκευές με λειτουργικό σύστημα Android.

Υπάρχουν διάφορες εκδόσεις του λειτουργικού συστήματος Android, όπου κάθε μια έρχεται για να δώσει περισσότερες δυνατότητες τόσο στους χρήστες όσο και στους προγραμματιστές που δημιουργούν εφαρμογές για το συγκεκριμένο λειτουργικό. Οι εκδόσεις του λειτουργικού που χρησιμοποιούνται από το μεγαλύτερο ποσοστό των χρηστών είναι η έκδοση KitKat η οποία κατέχει το 20,8% του συνολικού αριθμού των συσκευών: η έκδοση αυτή ξεκίνησε να χρησιμοποιείται τον Οκτώβριο του 2013. Στην συνέχεια η Google δημοσίευσε την έκδοση Lollipop τον Οκτώβριο του 2014, όπου η έκδοση αυτή χρησιμοποιείται ακόμη από το 23,1% των χρηστών. Επόμενη έκδοση είναι η Marshmallow η οποία ξεκίνησε να χρησιμοποιείται τον Οκτώβριο του 2015 και

οι χρήστες που έχουν σήμερα εγκατεστημένη αυτήν την έκδοση κατέχουν το 31,3%. Η πιο πρόσφατη έκδοση του Android είναι η έκδοση Nougat στην οποία η Google έχει προσθέσει σημαντικές βελτιώσεις τόσο στα γραφικά όσο και σε ταχύτητα [02].

Οι εφαρμογές για ένα κινητό με λειτουργικό σύστημα Android είναι διαθέσιμες στους χρήστες μέσω του Google Play Store, από όπου ένας χρήστης μπορεί να μεταφορτώσει («κατεβάσει») εφαρμογές και να τις εγκαταστήσει στο κινητό του. Η παρακάτω εικόνα δείχνει την αύξηση στον αριθμό των εφαρμογών που είναι διαθέσιμες στο Google Play Store από το 2009 έως το 2015.

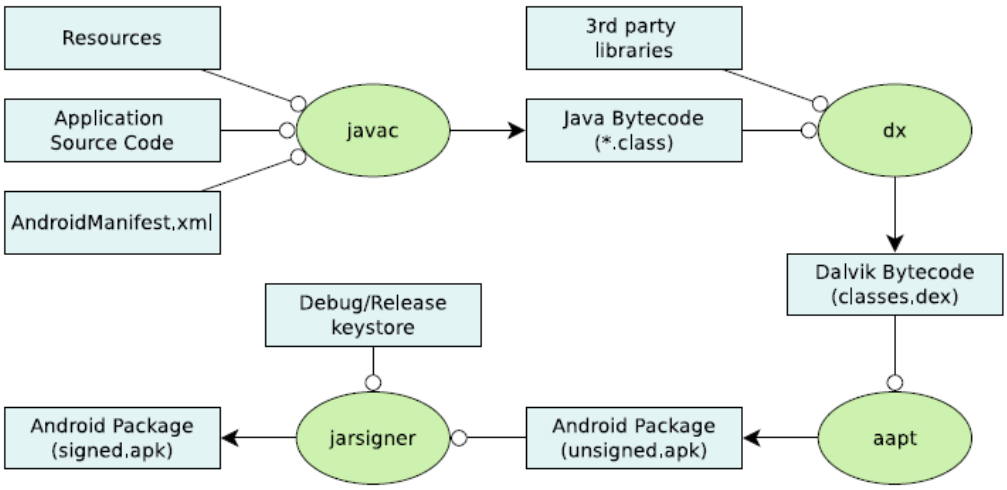


Πίνακας 3.1 : Μεταβολή του πλήθους των εφαρμογών που είναι διαθέσιμες στο Google Play Store από το 2009 έως το 2015 [11].

Στο κεφάλαιο αυτό, δεδομένου ότι το πειραματικό περιβάλλον που αναπτύχθηκε στο πλαίσιο της διατριβής βασίζεται στο Android, παρουσιάζεται η γενική λειτουργία των εφαρμογών στο περιβάλλον του Android.

3.1 Λειτουργία των εφαρμογών στο περιβάλλον Android

Οι εφαρμογές Android είναι εφαρμογές γραμμένες στη γλώσσα προγραμματισμού Java και διανέμονται σαν Android Package (APK) αρχεία. Τα αρχεία αυτά είναι ψηφιακά υπογεγραμμένα αρχεία τύπου .zip τα οποία περιέχουν τον κώδικα της εφαρμογής μαζί με όλα τα δεδομένα της: περιέχουν επίσης και βιβλιοθήκες τρίτων μελών (third-party) καθώς και ένα αρχείο «manifest» το οποίο περιγράφει τις δυνατότητες της εκάστοτε εφαρμογής. Η επόμενη εικόνα δείχνει, με απλοποιημένο τρόπο, τη διαδικασία με την οποία ο πηγαίος κώδικας γραμμένος σε Java μεταγλωττίζεται σε αρχείο APK.



Εικόνα 3.2: Διαδικασία μεταγλώττισης πηγαίου κώδικα μιας εφαρμογής σε αρχείο apk.

Για την ενίσχυση της ασφάλειας οι εφαρμογές εκτελούνται μέσα σε ένα απομονωμένο (sandbox) περιβάλλον. Κατά την διάρκεια της εγκατάστασης οι εφαρμογές λαμβάνουν ένα μοναδικό αναγνωριστικό (Linux user id) από το λειτουργικό σύστημα. Τα δικαιώματα για τα αρχεία της εφαρμογής ορίζονται κατά τρόπο τέτοιο ώστε μόνο η εφαρμογή να μπορεί να τα προσπελάσει. Επισπρόσθετα, όταν μια εφαρμογή εκκινείται, της παρέχεται ένα δικό της

εικονικό περιβάλλον (VM): αυτό σημαίνει ότι ο κώδικας της εφαρμογής είναι απομονωμένος από τις άλλες εφαρμογές που βρίσκονται στο κινητό. Το Android εφαρμόζει την αρχή των ελάχιστων προνομίων, κάτι που σημαίνει ότι κάθε εφαρμογή έχει πρόσβαση μόνο στους πόρους που χρειάζεται για να λειτουργήσει. Η επόμενη εικόνα δείχνει τα διαφορετικά μέρη του λειτουργικού συστήματος Android. Συγκεκριμένα, στο κατώτερο επίπεδο έχουμε τον πυρήνα (Linux Kernel) ο οποίος περιέχει τους οδηγούς για τις θύρες USB, το πληκτρολόγιο, τον ήχο και άλλα.

Ένα επίπεδο πάνω από τον πυρήνα συναντάμε τις βιβλιοθήκες SSL, libc, SGL, SQLite και άλλα. Ένα επίπεδο πάνω από τις βιβλιοθήκες βρίσκεται το λεγόμενο Πλαίσιο Εφαρμογών (Application Framework), το οποίο περιέχει ένα σύνολο από προγράμματα διαχείρισης (Managers) όπως τον Package Manager, τον Activity Manager, τον Resource Manager και άλλους.

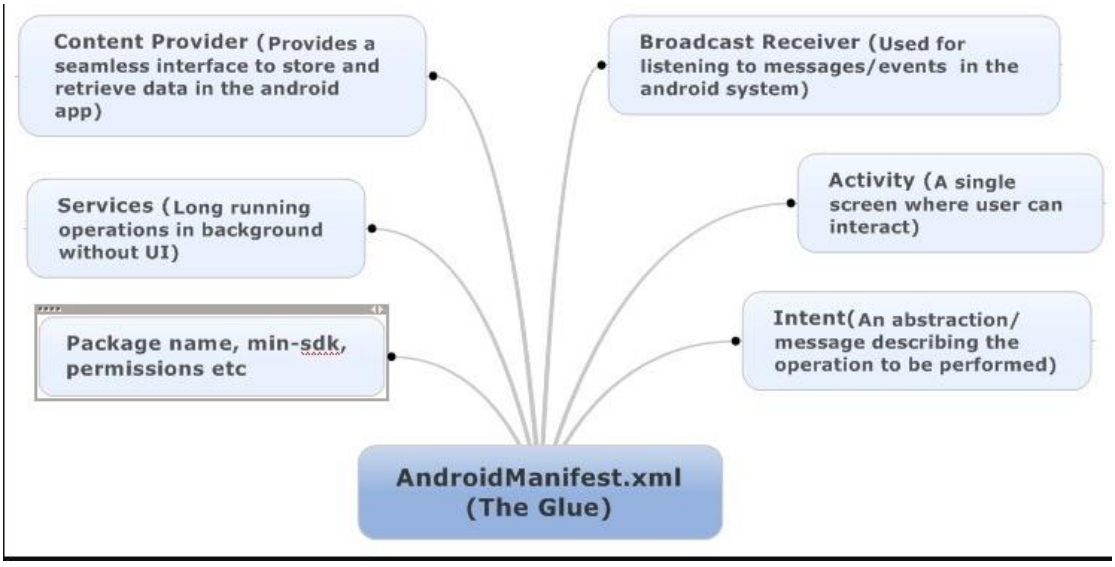
Τέλος στο επίπεδο που είναι ορατό από ένα χρήστη έχουμε τις επαφές, τις κλήσεις, τα μηνύματα και άλλα.

Εικόνα 3.3: Τα διαφορετικά επίπεδα του λειτουργικού συστήματος Android [18].

3.2 Το αρχείο Manifest

Κάθε Android εφαρμογή περιέχει ένα αρχείο το ***AndroidManifest.xml*** το οποίο ενημερώνει το σύστημα για τα περιεχόμενα της εφαρμογής. Οι υπηρεσίες (services) και οι διαδικασίες που δεν περιγράφονται στο manifest δεν μπορούν να εκτελεστούν. Στο manifest επίσης ορίζονται και οι απαιτήσεις της εφαρμογής, όπως τυχόν ειδικό υλικό που είναι απαραίτητο για τη λειτουργία της εφαρμογής (π.χ. να υπάρχει κάμερα στο κινητό ή η ελάχιστη έκδοση του λειτουργικού που απαιτείται για να λειτουργήσει η εφαρμογή).

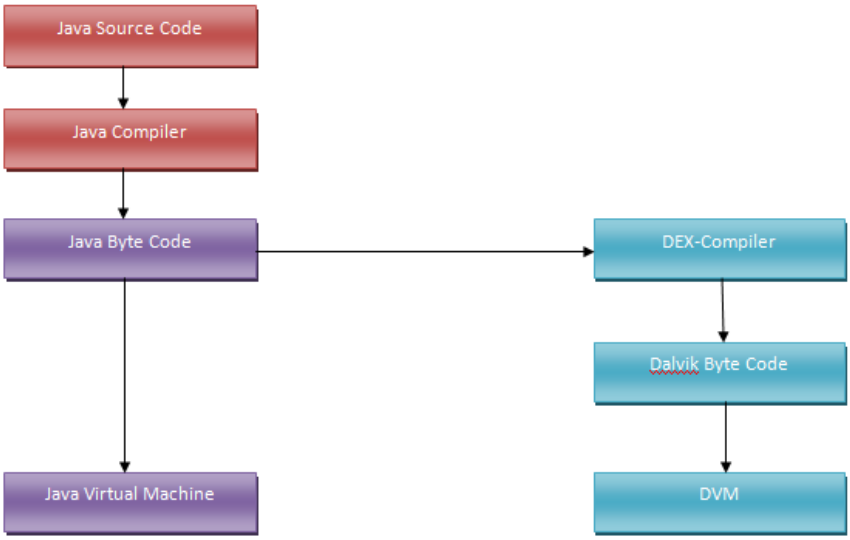
Για να μπορέσει μια εφαρμογή να έχει πρόσβαση σε προστατευμένα στοιχεία του κινητού όπως στις επαφές ή στα μηνύματα χρειάζεται να της δοθεί σχετικό δικαίωμα πρόσβασης. Οι προσβάσεις αυτές περιγράφονται στο αρχείο manifest και απονέμονται στην εφαρμογή κατά την εγκατάστασή της, όπου ο χρήστης ρωτάται αν επιθυμεί η εφαρμογή να έχει τα δικαιώματα αυτά.



Εικόνα 3.4: Σχηματική αναπαράσταση των εργασιών που εκτελεί το αρχείο Manifest στο λειτουργικό σύστημα Android [01].

3.3 Dalvik VM

Το Dalvik VM (DVM) είναι μια εικονική μηχανή όπου εκτελούνται όλες οι εφαρμογές στο λειτουργικό σύστημα Android. Μέσω αυτής, η συσκευή είναι είναι σε θέση να εκτελέσει πολλαπλά εικονικά μηχανήματα για αποδοτικότερη διαχείριση της ενέργειάς της. Κάθε εφαρμογή εκτελείται με την δική της διαδικασία καταλαμβάνοντας διαφορετική εικόνα του Dalvik VM. Αρχικά, αρχεία τύπου Java μετατρέπονται σε αρχεία τύπου .class μέσω του java compiler και στην συνέχεια αυτά τα αρχεία μετατρέπονται σε αρχεία τύπου .dex. Τα αρχεία τύπου .dex καταλήγουν στο DVM έτσι ώστε να παραχθεί ο κώδικας μηχανής και να εκτελεστεί από την CPU. Τα αρχεία .apk περιέχουν αρχεία τύπου .dex τα οποία μπορούν να εκτελεστούν στο Dalvik VM. Το DVM δημιουργήθηκε για καλύτερη διαχείριση τόσο της μπαταρίας στα κινητά τηλέφωνα, όσο και της επεξεργαστικής τους ισχύος – ενώ,τέλος, είναι δωρεάν, σε αντίθεση με το JVM (Java Virtual Machine) το οποίο δεν είναι. Η επόμενη εικόνα δείχνει σχηματικά τον τρόπο με τον οποίο ένα αρχείο Java μετατρέπεται σε μορφή αναγνωρίσιμη από το DVM.

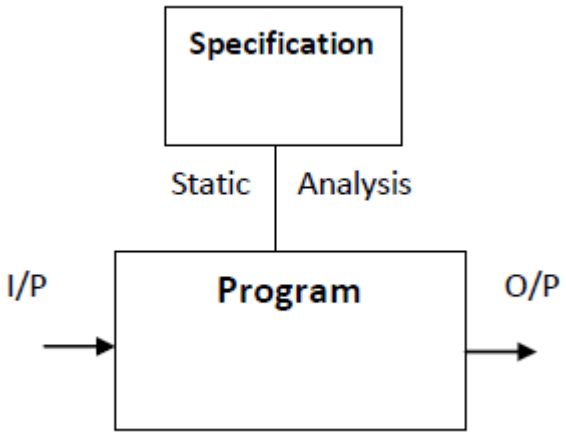


Εικόνα 3.5: Σχηματική αναπαράσταση μετατροπής του κώδικα ενός αρχείου σε μορφή αναγνωρίσιμη από το DVM.

3.4 Τρόποι ανάλυσης εφαρμογών

Η ανάλυση των εφαρμογών μπορεί να επιτευχθεί με δύο τρόπους: είτε μέσω στατικής ανάλυσης είτε μέσω δυναμικής. Κάθε μια από τις δύο τεχνικές παρουσιάζει τα πλεονηκτήματα και τα μειονεκτήματά της [12].

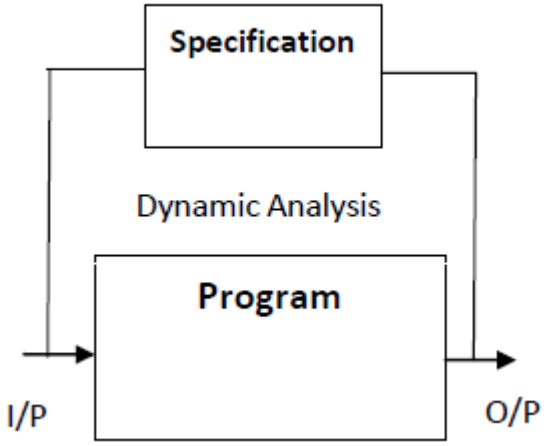
- Στατική ανάλυση. Στην στατική ανάλυση εξετάζεται ο κώδικας μιας εφαρμογής και οι λόγοι που μπορεί να οδηγούν μια εφαρμογή να λειτουργεί με ένα συγκεκριμένο τρόπο. Χαρακτηριστικό αυτής της μεθόδου είναι ότι η ανάλυση γίνεται πριν την εκτέλεση της εφαρμογής καθώς εξετάζονται όλα τα μονοπάτια εκτέλεσης του κώδικα. Βέβαια, η τεχνική αυτή έχει ως μειονέκτημα ότι δεν μπορεί να εντοπίσει τμήματα του κώδικα τα οποία έχουν κρυφτεί - πιθανόν από κάποιον κακόβουλο - και επομένως, σε ορισμένες περιπτώσεις, η τεχνική αυτή δεν επαρκεί για την ολοκληρωμένη ανάλυση μιας εφαρμογής.



Εικόνα 3.6 : Σχηματική αναπαράσταση στατικής ανάλυσης εφαρμογής.

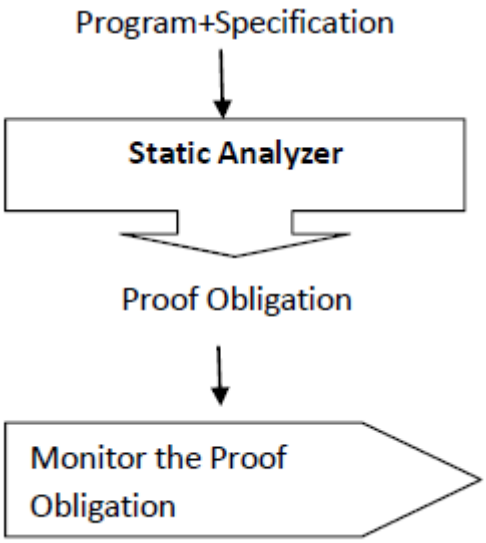
- Δυναμική ανάλυση. Η δυναμική ανάλυση λειτουργεί με το να εκτελεί μια εφαρμογή και να παρακολουθεί την εκτέλεσή της. Η μέθοδος αυτή θεωρείται ότι είναι μια τεχνική ακριβής και για να το επιτύχει αυτό εκτελεί δοκιμές και δημιουργεί «προφίλ» (profiling) της εφαρμογής έτσι ώστε να καταδείξει την συμπεριφορά της. Η δυναμική ανάλυση είναι σε

θέση να αναλύσει την ακριβή συμπεριφορά μιας εφαρμογής κατά την εκτέλεσή της και μπορεί να είναι τόσο γρήγορη όσο είναι και η εκτέλεση της εφαρμογής. Ένα μειονέκτημα της δυναμικής ανάλυσης είναι ότι τα αποτελέσματά της ενδέχεται να μην είναι εφαρμόσιμα σε μελλοντική εκτέλεσή της [12].



Εικόνα 3.7: Σχηματική αναπαράσταση δυναμικής ανάλυσης εφαρμογής.

- Συνδυασμός στατικής και δυναμικής ανάλυσης [12]. Μια ακόμη προσέγγιση που μπορεί να ακολουθηθεί είναι ο συνδυασμός των δυο προαναφερθεισών τεχνικών, σε μια προσπάθεια να αξιοποιήσουμε τα πλεονεκτήματα που προσφέρει η καθεμία. Σε αυτήν την περίπτωση προηγείται η στατική ανάλυση, η οποία διεξάγεται πριν την εκτέλεση της εφαρμογής, και ακολουθεί η δυναμική. Η επόμενη εικόνα δείχνει τον τρόπο με τον οποίο οι δύο τεχνικές μπορούν να συνδυαστούν.



Εικόνα 3.8: Σχηματική αναπαράσταση συνδυασμού στατικής και δυναμικής ανάλυσης

3.5 Προγενέστερες προσεγγίσεις στον τομέα της ασφάλειας των εφαρμογών Android

Δεδομένου ότι στην παρούσα διατριβή θα μελετηθούν εφαρμογές σε περιβάλλον Android ως προς το είδος των προσωπικών δεδομένων που επεξεργάζονται, στην παρούσα ενότητα περιγράφονται διάφορες προσεγγίσεις που έχουν ακολουθηθεί ως προς το συγκεκριμένο ζήτημα.

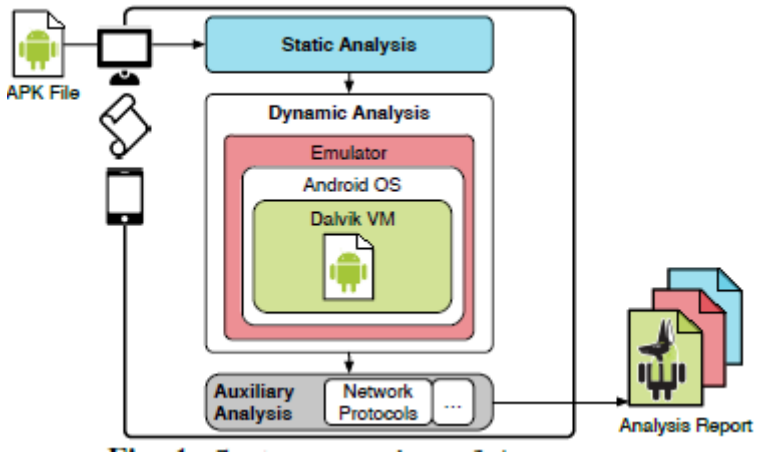
I. Taintdroid. Το 2010 παρουσιάστηκε το Taintdroid το οποίο αποτελεί μια τροποποιημένη έκδοση Android. Το Taintdroid παρακολουθεί τα δεδομένα που αντλούνται από ένα κινητό και ενημερώνει τον χρήστη σε περίπτωση που αποστέλλεται κάποιο προσωπικό δεδομένο [10].
II. DroidBox. Το DroidBox αναπτύχθηκε από τον Πάτρικ Λάντζ κατά την διάρκεια του Google Summer of Code το 2011. Η ιδιαιτερότητά του είναι ότι συνδυάζει το Taintdroid με μερικές τροποποιήσεις σε βιβλιοθήκες του πυρήνα του Android. Το τροποποιημένο λειτουργικό καταγράφει διαδικασίες ανάγνωσης και εγγραφής αρχείων, ανοίγματος συνδέσεων δικτύου και εξερχόμενης δικτυακής κίνησης [09].
III. Andrubis. Το Andrubis [13] εμφανίστηκε το 2012 από την International Secure Systems Lab και είναι ένα εργαλείο που συνδυάζει στατική και

δυναμική ανάλυση Android εφαρμογών. Τα αποτελέσματα της στατικής ανάλυσης χρησιμοποιούνται από την δυναμική για την επίτευξη καλύτερων αποτελεσμάτων. Τα επίπεδα της ανάλυσης του Andrubis διακρίνονται σε τρία επίπεδα και είναι τα εξής:

Στατική ανάλυση όπου εξάγονται πληροφορίες από το αρχείο manifest της εφαρμογής και των κώδικά της.

Δυναμική ανάλυση: σε αυτό το στάδιο εκτελείται η εφαρμογή σε ένα περιβάλλον Android και παρακολουθούνται οι ενέργειές της τόσο στο επίπεδο του συστήματος όσο και στο επίπεδο του Dalvki VM.

Post-Processing : Μετά τα κύρια επίπεδα ανάλυσης το Andrubis εκτελεί πρόσθετους ελέγχους στα αποτελέσματα. Οι έλεγχοι αυτοί περιλαμβάνουν ανάλυση της δικτυακής κίνησης της εφαρμογής.



Εικόνα 3.9: Σχηματική αναπαράσταση της ανάλυσης ενός αρχείου apk από το Andrubis.

IV. Tracedroid. Το Tracedroid είναι ένα ακόμη εργαλείο δυναμικής ανάλυσης εφαρμογών. Το εργαλείο αυτό καταγράφει την συμπεριφορά της εφαρμογής που εξετάζει, πιο συγκεκριμένα εξετάζει τις δικτυακές επικοινωνίες όπως και τις εσωτερικές κλήσεις συναρτήσεων αλλά και τα τμήματα κώδικα Java. Για να αναγκάσει την εφαρμογή να εκτελέσει όλα τα χαρακτηριστικά της το Tracedroid προσομειώνει μερικές πράξεις όπως διεπαφές χρήστη, εισερχόμενες κλήσεις και SMS μηνύματα [20].

3.6 Αναγνωριστικά κινητού

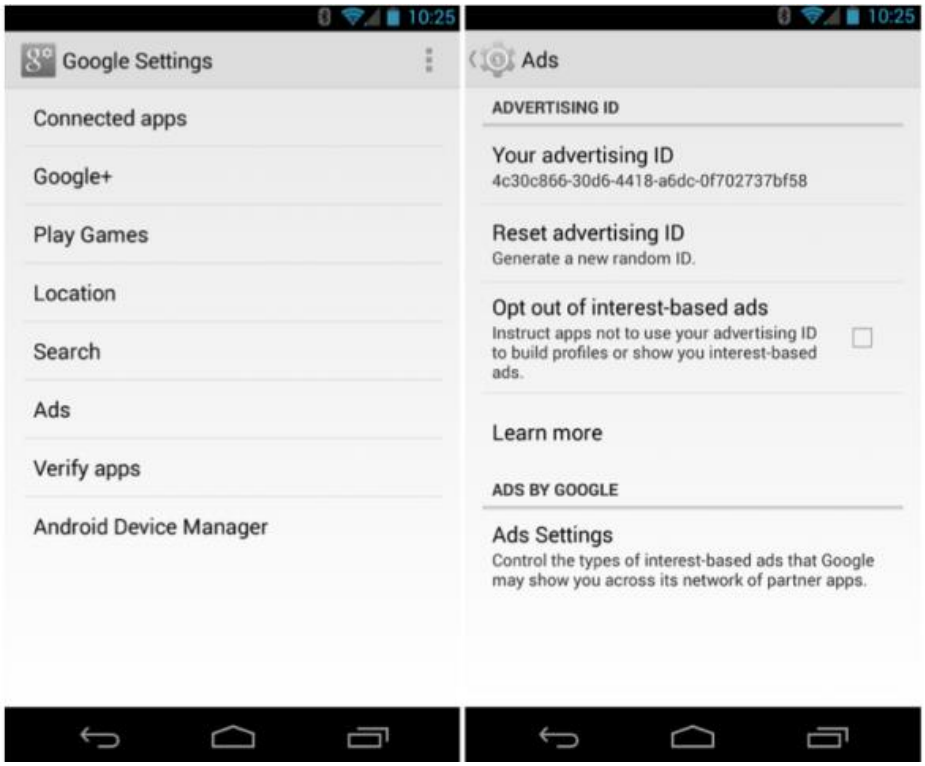
Τα αναγνωριστικά (identifiers) κινητών τηλεφώνων ή αλλιώς Mobile Device Identifiers είναι μοναδικοί αριθμοί (κωδικοί) οι οποίοι μπορεί να χρησιμοποιηθούν από διάφορες εφαρμογές για να αναγνωριστεί ένα κινητό τηλέφωνο. Για παράδειγμα, οι διαφημιστές χρησιμοποιούν αυτούς τους identifiers για να εξακριβώσουν αν έχουν ήδη προωθήσει μια διαφήμιση προς ένα συγκεκριμένο χρήστη [19]. Ο παρακάτω πίνακας αποτυπώνει κάποια αναγνωριστικά μιας έξυπνης κινητής συσκευής, το μέγεθος του καθενός και την ιδιότητά τους σε σχέση με το αν μπορούν να μεταβληθούν με παρέμβαση του χρήστη ή όχι.

Identifier	Description	Attribute
GAID	User-resettable 32-digit alphanumeric identifier	Pseudonymous
Android ID	64-bit number randomly generated when device is set up for the first time [5]	Semi-permanent
IMEI	15-digit decimal identifier representing GSM or LTE device	Permanent
IMSI	15-digit decimal identifier representing mobile subscriber identity	Permanent
MAC address	48-bit number assigned to the device's Wi-Fi network interface	Permanent

Πίνακας 3.10 :Οι identifiers ενός κινητού με λειτουργικό σύστημα Android **[**14]

Από τον πίνακα 3.10, το GAID (Google Advertising Id) είναι ένας μοναδικός αριθμός μεγέθους 32-bit ο οποίος αντικατέστησε το Android Id και το συναντάμε σε όλα τα κινητά με λειτουργικό Android που έχουν εγκαταστήσει το Google Play Store. Σε περίπτωση που αυτό δεν έχει εγκατασταθεί, το κινητό αυτό παραμένει ανιχνεύσιμο μέσο άλλου αναγνωριστικού όπως το Android ID. Ο λόγος χρησιμοποίησης του GAID είναι ότι δίνει την δυνατότητα στους χρήστες

να ορίζουν το επίπεδο της ασφάλειας που επιθυμούν. Επίσης έχουν την δυνατότητα να επανεκκινήσουν το αναγνωριστικό αυτό (δηλαδή να του αναθέσουν νέα τιμή) όποτε επιθυμούν. Το GAID, όπως θα δούμε στο Κεφάλαιο 4, έχει σημαντικό ρόλο στις εφαρμογές των ανώνυμων κοινωνικών δικτύων.



Εικόνα 3.11: Μέσω του Google Settings είναι ορατό το GAID ενός κινητού και μας δίνεται η επιλογή να το επανεκκινήσουμε.

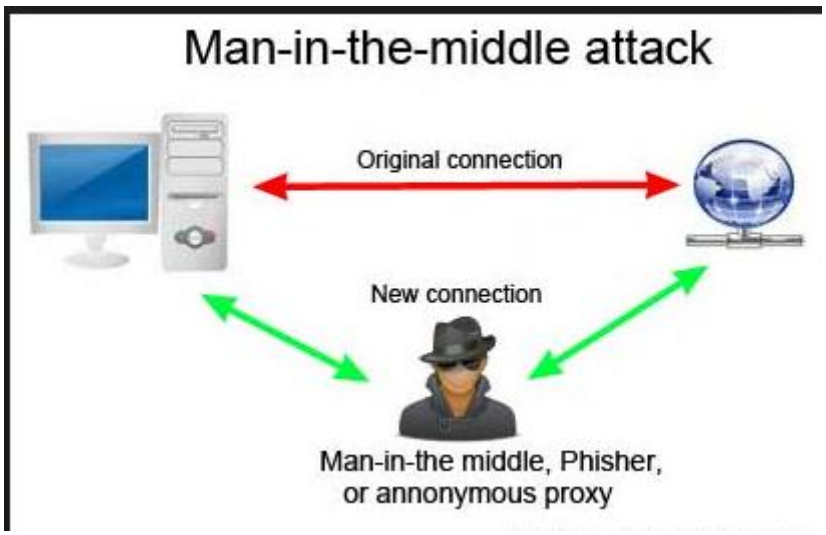
Κεφάλαιο 4

Ανάλυση των ανώνυμων εφαρμογών

Οι εφαρμογές που επεξεργάζονται «σημαντικά» δεδομένα θα πρέπει να κρυπτογραφούν αυτά τα δεδομένα πριν τα αποστείλλουν μέσω του διαδικτύου – διαφορετικά, οποιοσδήποτε έχει πρόσβαση στο κανάλι μετάδοσης θα είναι σε θέση να τα διαβάσει, πλήττοντας έτσι την εμπιστευτικότητα της μετάδοσης. Ο τυπικός τρόπος για να το πράξουν αυτό είναι με την χρησιμοποίηση του HTTPS (HyperText Transport Protocol Secure) το οποίο βρίσκεται πάνω από το SSL/TLS (Secure Socket Layer/Transport Layer Security). Το TLS (διάδοχος του πρωτοκόλλου SSL, αν και είθισται ακόμα να χρησιμοποιούμε τον όρο SSL) παρέχει εμπιστευτικότητα, ακεραιότητα δεδομένων και αυθεντικοποίηση χρηστών στο επίπεδο μεταφοράς (transport layer): για την αυθεντικοποίηση γίνεται χρήση ψηφιακών πιστοποιητικών, υπογεγραμμένα από έμπιστη τρίτη οντότητα για να διασφαλίζεται η εγκυρότητά τους. Όταν το γνωστό πρωτόκολλο HTTP δομείται πάνω από το SSL/TLS "υιοθετεί» όλες τις υποκείμενες υπηρεσίες ασφαλείας και μιλάμε πλέον για το ασφαλές πρωτόκολλο HTTPS.

Μια εφαρμογή, για να είναι ασφαλής, θα πρέπει να είναι ανθεκτική απέναντι σε επιθέσεις τύπου «*Man In The Middle Attack»* (κάτι που το HTTPS διασφαλίζει, στο βαθμό που λειτουργεί σωστά η πιστοποίηση της ταυτότητας του εξυπηρετητή μέσω ελέγχου εγκυρότητας του ψηφιακού πιστοποιητικού του). Αυτό πρακτικά σημαίνει ότι αν κάποιος παρακολουθεί την κίνηση του δικτύου μεταξύ της εφαρμογής και των servers της δεν θα μπορεί να αποκτήσει («διαβάσει») τα δεδομένα αυτά. Πρόβλημα όμως ως προς τη συγκεκριμένη

επίθεση εντοπίζεται στο γεγονός ότι υπάρχει μεγάλος αριθμός εφαρμογών στο Android οι οποίες αποτυγχάνουν να επαληθεύσουν την εγκυρότητα των πιστοποιητικών του SSL/TLS, γεγονός που τις καθιστά ευάλωτες στις επιθέσεις αυτές – αφού η μη επιβεβαίωση πιστοποίησης της εγκυρότητας ενός πιστοποιητικού θέτει εν αμφιβόλω την ταυτότητα του εξυπηρετητή. Το εν λόγω πρόβλημα των εφαρμογών σε περιβάλλον Android, έχει γίνει γνωστό από το ερευνητές του CERT (CERT Coordination Center at Carnegie Mellon University (CERT/CC)) οι οποίο έχουν δημοσιεύσει λίστα με τις εφαρμογές που είναι ευάλωτες σε αυτή την ευπάθεια [06]. Από την στιγμή που μια εφαρμογή θα θεωρεί κάθε εξυπηρετητή ως έγκυρο, η κρυπτογραφημένη επικοινωνία θα μπορεί να ανακτηθεί από κάποιον κακόβουλο εκτελώντας μια επίθεση τύπου «*Man In The Middle Attack*».



Εικόνα 4.1 :Γραφική απεικόνιση μιας Man In The Middle Attack. [16]

4.1 Δημιουργία περιβάλλοντος δοκιμών

Για την ανάλυση των ανώνυμων εφαρμογών αναπτύχθηκαν, στο πλαίσιο της διατριβής, δύο διαφορετικά περιβάλλοντα εργασίας. Ως proxy επιλέχθηκε το πρόγραμμα Burp Suite [04] το οποίο εκτελείται σε ένα υπολογιστή του τοπικού δικτύου, ενώ το Xposed framework [22] εγκαταστάθηκε τόσο σε ένα πραγματικό τηλέφωνο όσο και σε ένα εικονικό μηχάνημα όπου με την χρήση του VirtualBox έγινε εγκατάσταση μιας έκδοσης του Android με δικαιώματα διαχειριστή (root). Ο λόγος εγκατάστασης του Xposed framework σε δυο περιβάλλοντα είναι ότι με αυτό τον τρόπο θα μπορούμε να πιστοποιήσουμε την εγκυρότητα των ερυνητικών μας ευρημάτων. Κατά τις δοκιμές που θα πραγματοποιήσουμε, τόσο το πραγματικό κινητό όσο και το εικονικό μηχάνημα θα συνδέονται στις εφαρμογές: η εξερχόμενη κίνηση ωστόσο θα ανακατευθύνεται πρώτα μέσω του Proxy.

Το περιβάλλον που έχουμε δημιουργήσει μέχρι στιγμής, εσκεμμένα ακολουθεί τη λογική «*Man In The Middle Attack*» προκειμένου να καταγράψουμε, για τους ερευνητικούς μας σκοπούς, την εξερχόμενη κίνηση από την εφαρμογή μας, είναι σε θέση - όπως θα δούμε - να συλλέξει δεδομένα από κάποιον browser που θα χρησιμοποιήσει κάποιος χρήστης, αλλά θα αποτύχει να συλλέξει δεδομένα από εφαρμογές. Για να προσπεραστεί αυτό το πρόβλημα θα πρέπει να παραχθεί ένα πιστοποιητικό από το Burp Suite και να εγκατασταθεί στο κινητό του οποίου την λειτουργία θα αναλύσουμε. Το πιστοποιητικό αυτό θα πρέπει να το εγκαταστήσουμε στα Trusted Certificates του κινητού και αυτό θα χρησιμοποηθεί για να πιστοποιήσει την εγκυρότητα των ενεργειών μας με την εφαρμογή.

Η τεχνική αυτή θα έχει ως αποτέλεσμα την επιτυχή ανάλυση ανώνυμων εφαρμογών όπως το SocialNumber, αλλά θα αποτύχει στην ανάλυση των υπόλοιπων εφαρμογών. Ο λόγος είναι ότι πολλές εφαρμογές για λόγους ασφαλείας χρησιμοποιούν μια τεχνική αυθεντικοποίησης που ονομάζετε ssl pinning με την οποία στον κώδικα της εφαρμογής ορίζεται συγκεκριμένα ποιο πιστοποιητικό θα χρησιμοποιηθεί για την επικοινωνία του κινητού με την

εφαρμογή [15]. Η τεχνική αυτή έχει την ικανότητα να αποτρέπει επιθέσεις τύπου «Man In The Middle».

Η παράκαμψη του ssl pinning, για το σκοπό της έρευνάς μας, μπορεί να γίνει με δυο τρόπους: είτε θα πρέπει να κάνουμε decompile την εφαρμογή, να βρούμε το σημείο στο κώδικα που το πιστοποιητικό γίνεται “pinned” να το αφαιρέσουμε και, ακολούθως, να κάνουμε πάλι compile την εφαρμογή και να την εκτελέσουμε, είτε να εγκαταστήσουμε το Xposed Framework και μέσω των διάφορων Module που προσφέρει να αφαιρέσουμε το πιστοποιητικό. [03,05,15].

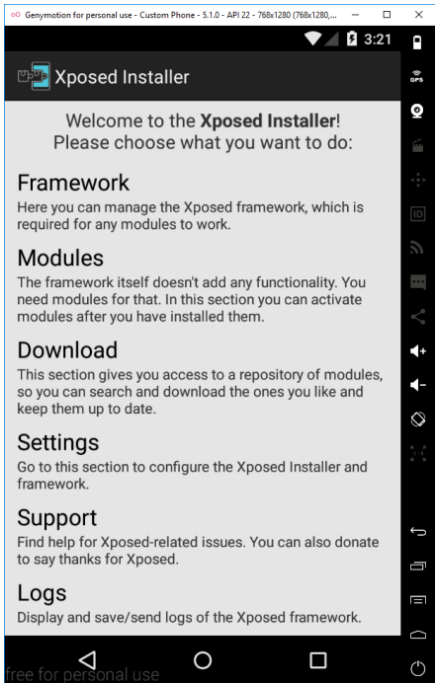
4.1.1 Burp Suite

Το Burp Suite [04] είναι ένα από τα καλύτερα εργαλεία για δοκιμή εφαρμογών στο web. Το γεγονός ότι διαθέτει μεγάλο πλήθος εργαλείων το καθιστά ικανό να εκτελεί πολλές εργασίες οι οποίες εκτείνονται από το να καταγράφει ένα αίτημα και να το τροποποιεί μέχρι να σκανάρει μια web εφαρμογή για ευπάθειες. Οι βασικές του λειτουργίες είναι οι εξής:

- Proxy-Burp Suite: Περιλαμβάνει ένα Proxy ο οποίος είναι διαθέσιμος στην πόρτα 8080 από προεπιλογή. Με την χρήση αυτού του Proxy μπορούμε να καταγράφουμε και να τροποποιούμε κίνηση που προέρχεται από το σύστημα κάποιου χρήστη και οδεύει προς την εφαρμογή που χρησιμοποιεί. Για να είμαστε σε θέση να χρησιμοποιήσουμε αυτό τον Proxy μέσα από το κινητό τηλέφωνο θα πρέπει να επιλέξουμε το ασύρματο δίκτυο στο οποίο είμαστε συνδεδεμένοι, να επιλέξουμε Modify Network και να ορίσουμε σαν proxy την ip διεύθυνση του μηχανήματος στο οποίο έχουμε εγκαταστήσει το Burp Suite.
- Scanner: Χρησιμοποιείται για να αναζητά ευπάθειες σε εφαρμογές web. Το είδος της αναζήτησης μπορεί να είναι παθητικό, ενεργό, ή να ορίζεται από τον χρήστη.

- Intruder: Το χαρακτηριστικό αυτό μπορεί να χρησιμοποιηθεί με πολλούς τρόπους, όπως για την εκμετάλλευση αδυναμιών που έχουμε βρεί πριν στο Scanner.
- Repeater: Το χαρακτηριστικό αυτό χρησιμοποιείται για να τροποποιεί και να αποστέλλει τα ίδια αιτήματα πολλές φορές και να αναλύει τις απαντήσεις που δέχεται από την εφαρμογή.

4.1.2 Xposed framework

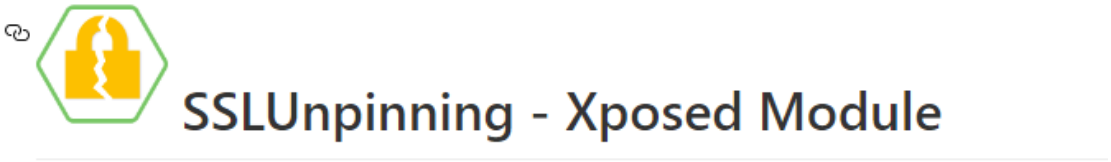


Εικόνα 4.2 : Η αρχική οθόνη του Xposed framework

Το Xposed framework απαιτεί δικαιώματα διαχειριστή (root) στο κινητό για να αποκτήσει πρόσβαση σε πόρους του πυρήνα του Android και ακολούθως τους χρησιμοποιεί για να εκτελέσει διάφορα modules στην συσκευή. Τα διαθέσιμα modules που υπάρχουν είναι πάρα πολλά και δίνουν την δυνατότητα σε κάποιον χρήστη να αλλάξει πολύ την λειτουργία του τηλεφώνου. Η εγκατάσταση του framework είναι διαφορετική για κάθε έκδοση Android και δεν αποτελεί αντικείμενο αυτής της διατριβής. Μέσω λοιπόν του framework θα

εγκαταστήσουμε δυο modules που θα μας βοηθήσουν στην ανάλυση των δεδομένων των εφαρμογών. Τα modules είναι:

- SSL Unpinnig: είναι ένα module το οποίο τροποποιεί διάφορα τμήματα κώδικα στις κλάσεις του ssl έτσι ώστε να προσπεραστούν οι έλεγχοι πιστοποιητικού για μια συγκεκριμένη εφαρμογή, καθιστώντας μετά εφικτή την ανάλυση των δεδομένων της εφαρμογής.

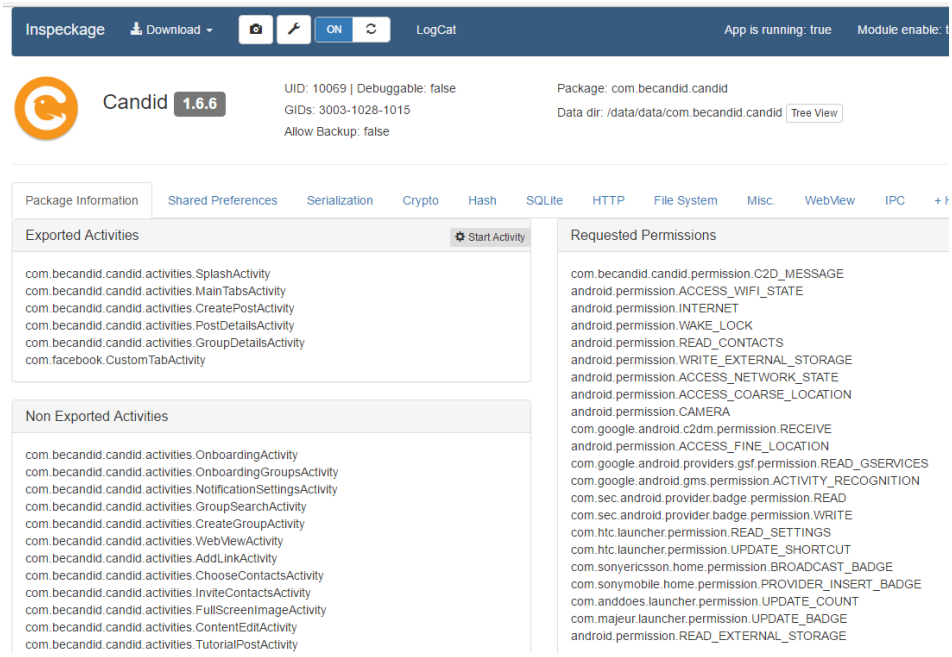


Εικόνα 4.3 : Το module SSLUnpinning το οποίο είναι διαθέσιμο μέσω του Xposed Framework.

- Το Inspeckage είναι ένα εργαλείο που παρέχει δυναμική ανάλυση εφαρμογών Android. Πιο συγκεκριμένα το Inspeckage παρέχει hooks σε κάποιες functions του API. Το module αυτό δίνει την δυνατότητα ανάλυσης της εφαρμογής και των διαδικασιών που λαμβάνουν χώρα κατά την εκκίνησή της.

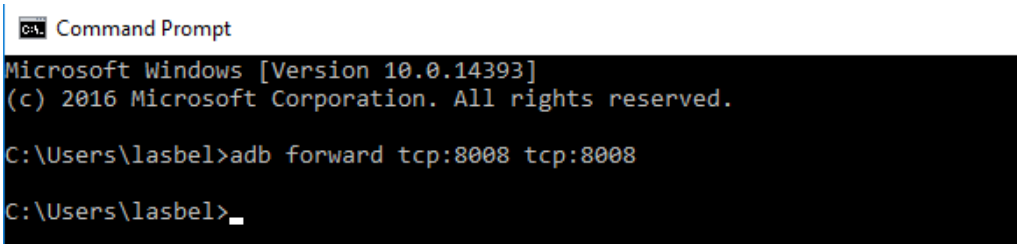
Εικόνα 4.4 : Το module του Inspeckage το οποίο είναι διαθέσιμο μέσω του Xposed Framework και θα χρησιμοποιηθεί για την εκτέλεση της δυναμικής ανάλυσης.

Πέρα από αυτό, το συγκεκριμένο module παρέχει και ένα GUI interface το οποίο επιτρέπει την ανάλυση των δεδομένων της εφαρμογής.



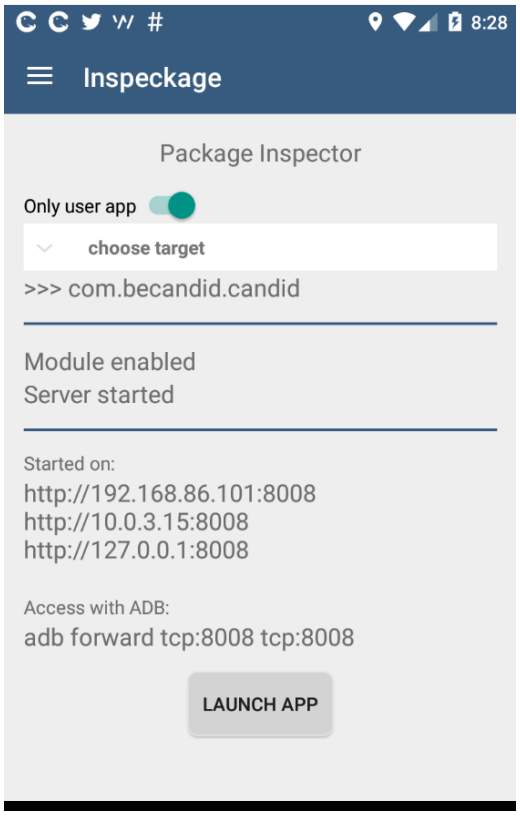
Εικόνα 4.5: Παρουσίαση του γραφικού περιβάλλοντος του Inspeckage.

Για να ενεργοποιηθεί το interface θα πρέπει κάποιος χρήστης είτε να συνδέσει το κινητό του με usb με τον υπολογιστή και να πληκτρολογήσει την εντολή adb forward tcp:8008 tcp:8008 (βλ. εικόνα 4.6).



Εικόνα 4.6: Εντολή που πρέπει να πληκτρολογήσουμε στην γραμμή εντολών για να είναι ορατό το γραφικό περιβάλλον της εφαρμογής.

Εναλλακτικά, όπως δείχνει και η εικόνα 4.7, μπορεί κανείς να πληκτρολογήσει την εσωτερική ip διεύθυνση του κινητού στο browser ενός υπολογιστή που βρίσκεται στο ίδιο δίκτυο έτσι ώστε να εμφανιστεί το GUI. Η επιλογή της εφαρμογής που θα αναλυθεί γίνεται μέσα από το μενού της παρακάτω εικόνας.



Εικόνα 4.7: Το κεντρικό menu του Inspeckage όπου η εφαρμογή μας δίνει την δυνατότητα να επιλέξουμε την εφαρμογή που θα αναλύσουμε και μας πληροφορεί για τις ip διευθύνσεις όπου θα είναι προσβάσιμο το γραφικό περιβάλλον της.

4.2 Ανάλυση των ανώνυμων εφαρμογών

Έχοντας περιγράψει τα εργαλεία που θα αξιοποιηθούν στη μεθοδολογία μας, θα περιγράψουμε στη συνέχεια την ανάλυση που επιχειρήθηκε για κάθε εφαρμογή ανώνυμου κοινωνικού δικτύου. Στην παρούσα διατριβή εστιάσαμε στα πιο γνωστά μέχρι σήμερα ανώνυμα κοινωνικά δίκτυα, τα οποία είναι τα εξής:

α) Social Number

β) Anomo

γ) Whisper

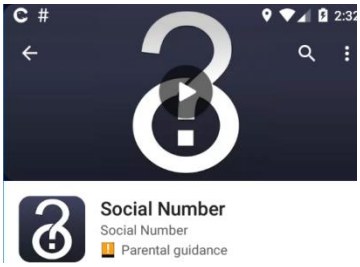
δ) Candid

ε) Yik Yak

Η ανάλυση των ανώνυμων εφαρμογών θα γίνει με χρήση δυο μεθόδων: αρχικά θα εξετάσουμε τις εφαρμογές SocialNumber και Anomo με την χρήση του προγράμματος Burp Suite, ενώ στην συνέχεια με το Inspeckage θα προχωρήσουμε σε δυναμική ανάλυση των τριών άλλων ανώνυμων εφαρμογών που εξετάζουμε. Ο λόγος που διακρίνουμε τις εφαρμογές σε δυο κατηγορίες έχει να κάνει με το γεγονός ότι το Socialnumber είναι μια εφαρμογή που δεν χρησιμοποιεί ssl pinning και, επομένως, μια προσέγγιση τύπου «Man in the Middle attack» για το σκοπό της έρευνάς μας είναι αρκετή για να μας δώσει τα δεδομένα που αποστέλλει κάποιος χρήστης. Την ίδια μεθοδολογία θα χρησιμοποιήσουμε και για το Anomo, το οποίο - λόγω του γεγονότος ότι ένας χρήστης μπορεί να συνδεθεί σε αυτό μέσω του λογαριασμού facebook που ενδεχομένως έχει - μας δίνει την δυνατότητα με μια ανάλογη επίθεση να καταγράψουμετα δεδομένα που αποστέλλει.

Οι τρεις άλλες εφαρμογές θα αναλυθούν μέσω του Inspeckage που είναι, όπως προαναφέρθηκε, ένα module του Xposed Framework.

4.2.1. SocialNumber



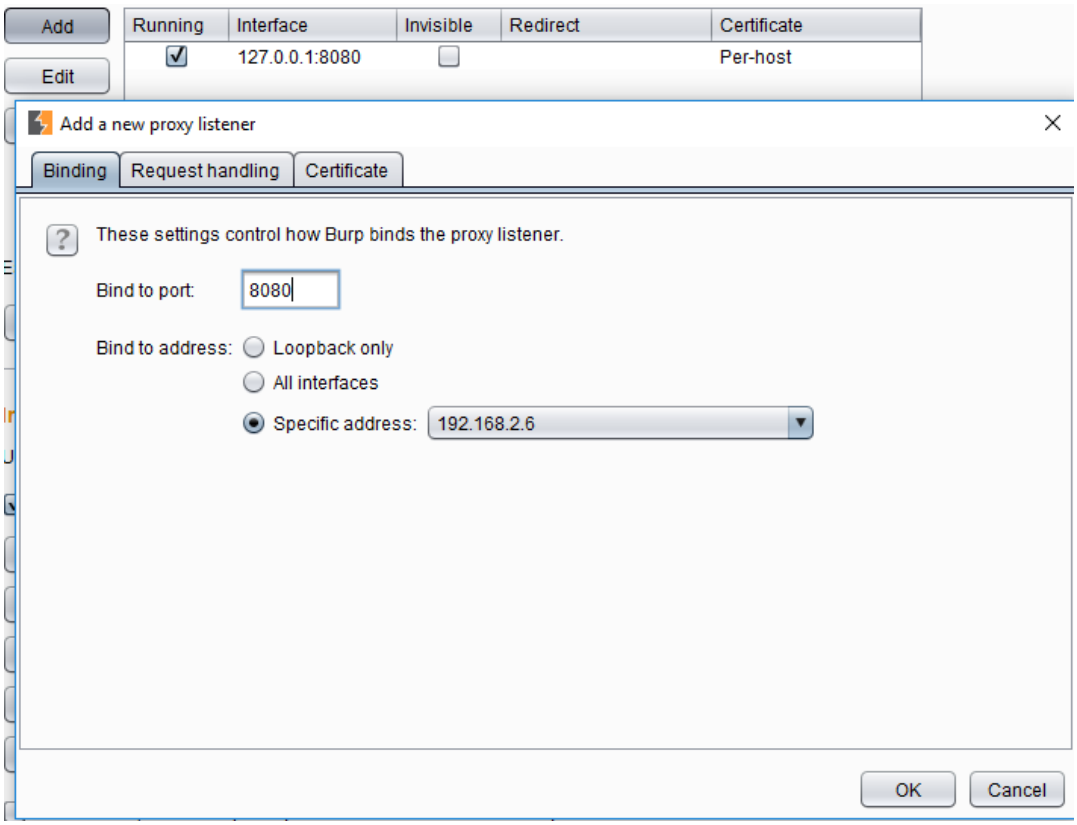
Εικόνα 4.8: Η εφαρμογή SocialNumber η οποία είναι διαθέσιμη μέσω του Google Play store

Η λογική της συγκεκριμένης εφαρμογής είναι πολύ απλή: σε κάθε χρήστη ανατίθεται ένας μεγάλος μοναδικός αριθμός ο οποίος θα είναι και το όνομα χρήστη που θα τον ακολουθεί κατά την περιήγηση του. Για την επιβεβαίωση της εγ-

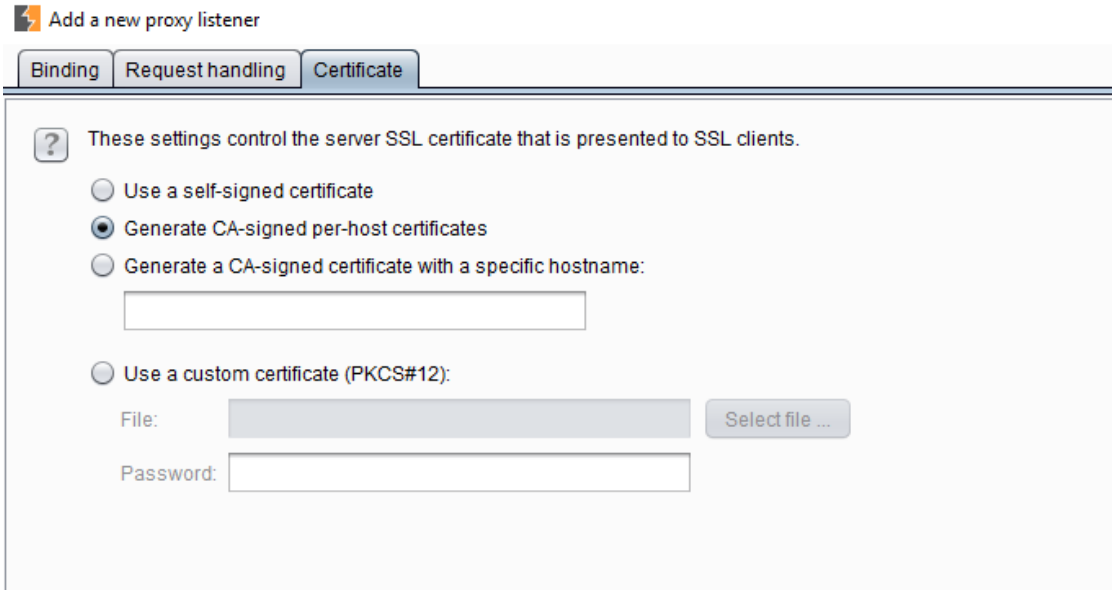
γραφής από τον χρήστη ζητείται να δώσει και μία διεύθυνση ηλεκτρονικού ταχυδρομείου email (γεγονός το οποίο από μόνο του καταδεικνύει εξ αρχής ότι η ο χαρακτηρισμός της εν λόγω εφαρμογής ως ανώνυμης είναι μη ακριβής, παρόλο που η ίδια η εφαρμογή στο διαδικτυακό της τόπο https://socialnumber.com/ αναφέρει ότι παρέχει ανωνυμία).

Με την χρήση του Burp Suite το οποίο θα εκτελείται σε ένα υπολογιστή του εσωτερικού δικτύου ανακατευθύνουμε όλη την δικτυακή κίνηση του κινητού τηλεφώνου να διέρχεται πρώτα μέσω του Burp και να παράγεται αυτόματα και το κατάλληλο πιστοποιητικό για προσπέραση των ελέγχων ασφαλείας.

Οι επόμενες εικόνες δείχνουν την παραμετροποίηση μέσα στο Burp.

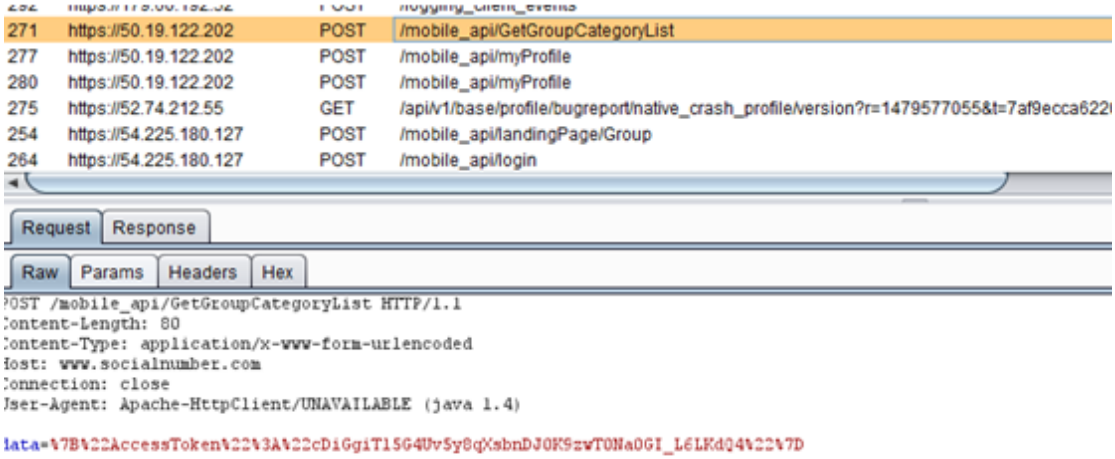


Εικόνα 4.9: Παραμετροποίηση του Burp Suite όπου ορίζουμε την ip του μηχανήματος και την πόρτα που θα δέχεται την δικτυακή κίνηση.

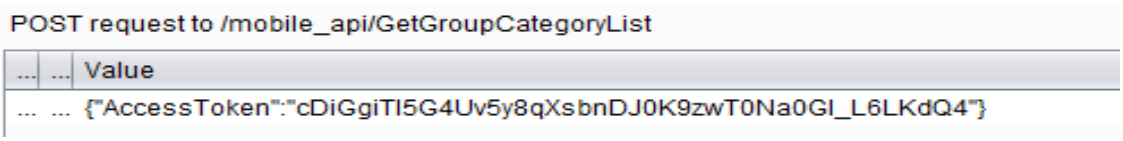


Εικόνα 4.10: Μέσω του tab «Certificate» στο Burp Suite επιλέγουμε να παράγει αυτόματα πιστοποιητικά για κάθε Host που συνδεόμαστε.

Το πρώτο μήνυμα που λαμβάνουμε από την εφαρμογή είναι αυτό που φαίνεται στην παρακάτω εικόνα. Βλέπουμε ότι κατά την είσοδο μας έχει ανατεθεί ένα random access Token το οποίο σε κάθε νέα σύνδεση (Login) είναι διαφορετικό. Αυτό το token θα είναι ίδιο όσο ο χρήστης διατηρεί την ίδια συνεδρία. Στο πεδίο Host φαίνεται ότι το πακέτο πηγαίνει προς www.socialnumber.com.

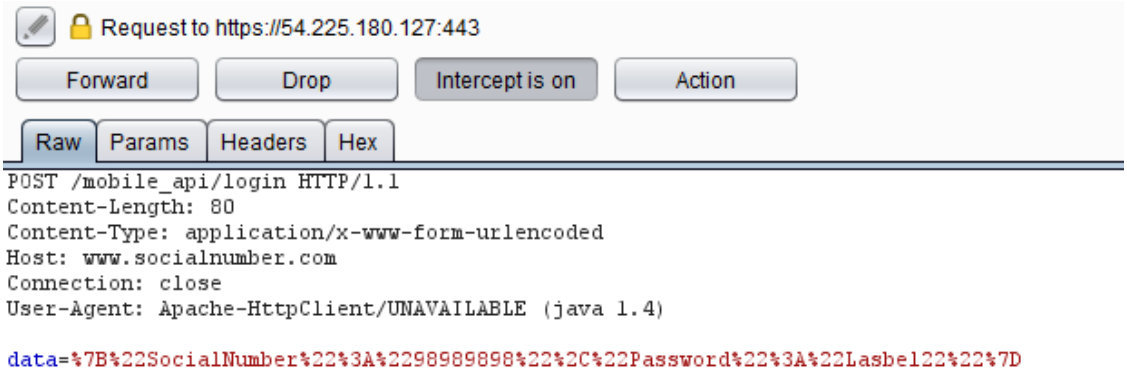


Εικόνα 4.11: Παρουσίαση ενός μηνύματος post που στέλνεται από ένα κινητό του δικτύου προς την ανώνυμη εφαρμογή SocialNumber.

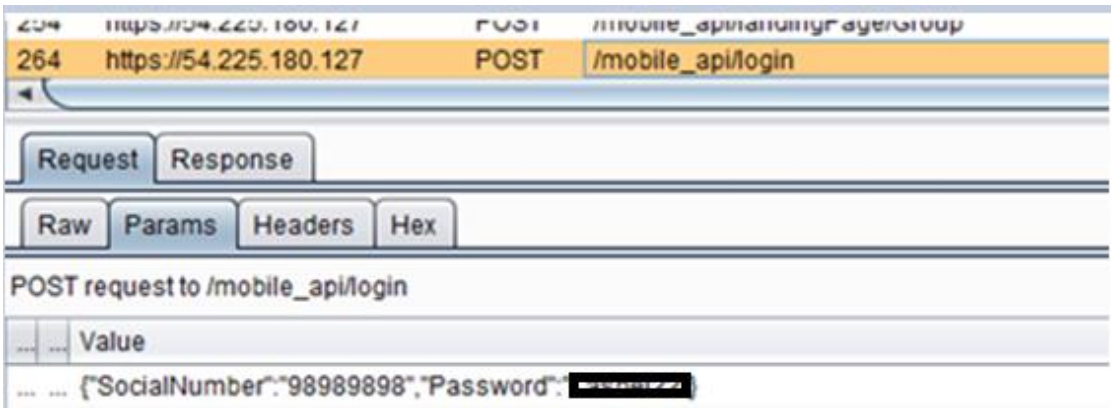


Εικόνα 4.12 : Παρουσίαση του τυχαίου Access Token που αναθέτει η εφαρμογή σε ένα χρήστη που εισέρχεται στην εφαρμογή.

Στην συνέχεια έχουμε άλλο ένα **post** μήνυμα στο οποίο μπορούμε να δούμε ότι στην μεταβλητή data στο tab Raw αποθηκεύεται τόσο το username όσο και το password – ως «καθαρό» κείμενο - που χρησιμοποιήθηκε για την είσοδο στην εφαρμογή. Τα διαπιστευτήρια αυτά είναι αναμεμειγμένα και με άλλους χαρακτήρες όμως αν επιλέξουμε το επόμενο tab με όνομα Params θα μπορούμε να διακρίνουμε καθαρά τόσο το username όσο και το password. Οι επόμενες δυο εικόνες δείχνουν τα διαπιστευτήρια που χρησιμοποιήθηκαν κατά την είσοδο στην εφαρμογή.



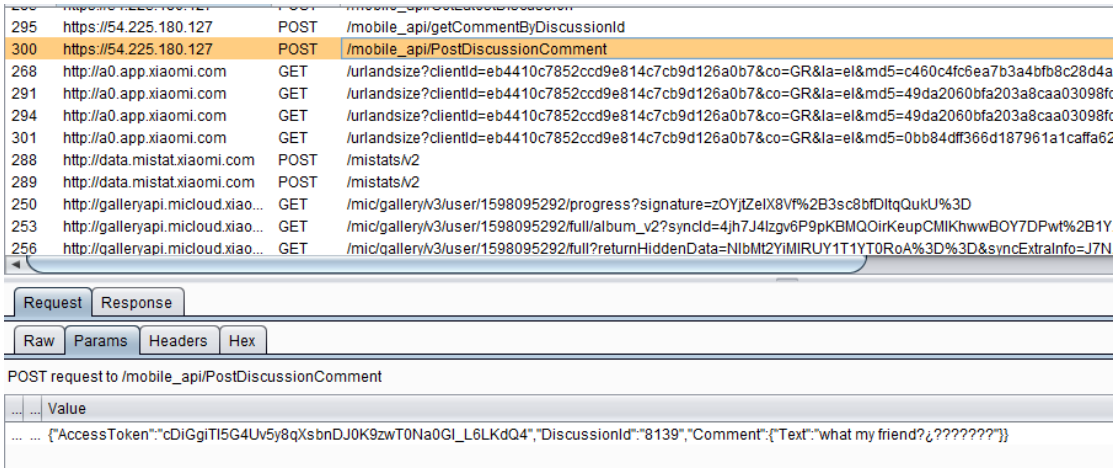
Εικόνα 4.13: Μέσω του Burp Suite βλέπουμε το όνομα χρήστη και τον κωδικό πρόσβασης που έχει χρησιμοποιήσει ένας χρήστης για την είσοδο του στην εφαρμογή.



Εικόνα 4.14 : Μέσω της καρτέλας Params είναι ορατά το όνομα χρήστη και ο κωδικός πρόσβασης που πληκτρολόγησε για την είσοδο του στην εφαρμογή SocialNumber.

Κατα την περιήγηση μέσα στην εφαρμογή μπορούμε να δούμε ότι κάθε φορά που επιλέγουμε κάποιο tab έχουμε ένα Post μήνυμα στο url /mobile_api/..... όπου οι τελείες αντικαθιστώνται κάθε φορά με το directory το οποίο επιλέγουμε: όταν παραδείγματος χάρη εισέρχομαστε στο discussionComment, τότε το αντίστοιχο url γίνεται το ακόλουθο: /mobile_api/PostDiscussionComment.

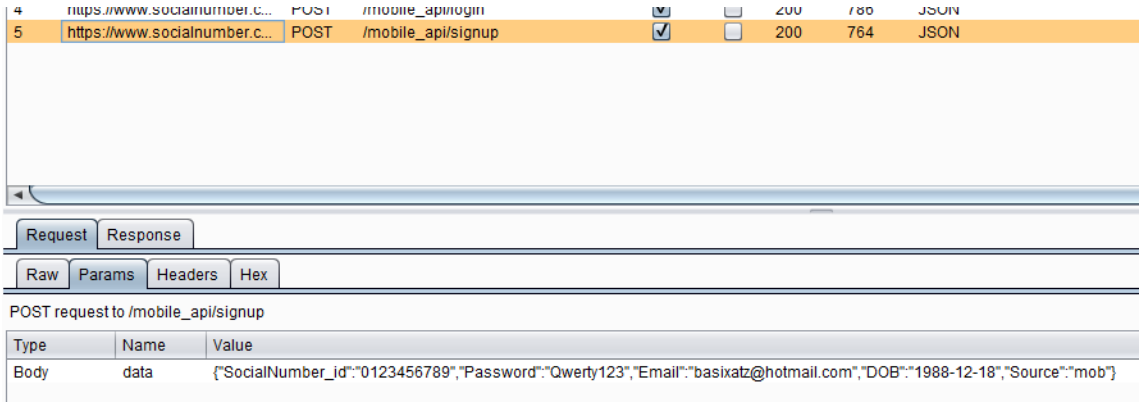
Τέλος, δημοσιεύοντας ένα comment μέσα στην εφαρμογή μπορούμε να δούμε στην παρακάτω εικόνα ότι έχει δημιουργηθεί ένα post πακέτο το οποίο περιέχει



Εικόνα 4.15 : Post μήνυμα όπου με την χρήση του Burp Suite είμαστε σε θέση να ανακτήσουμε μια δημοσίευση που γίνεται στην εφαρμογή SocialNumber.

το Access Token που μας έχει ανατεθεί, το discussion id όπως και το περιεχόμενο του μηνύματος.

Κατά την διαδικασία εγγραφής ενός νέου χρήστη στην εφαρμογή ζητείται να πληκτρολογήσουμε ένα λογαριασμό email τον οποίο μπορεί κάποιος να χρησιμοποιήσει για να κάνει ανάκτηση του κωδικού του σε περίπτωση που τον ξεχάσει. Σε αυτήν την περίπτωση λοιπόν με την τεχνική που αναλύσαμε καταφέραμε να ανακτήσουμε το προσωπικό δεδομένο της ηλεκτρονικής διεύθυνσης (email) όπως και φαίνεται στην παρακάτω εικόνα.



Εικόνα 4.16 : Το post μήνυμα όπου μέσω του Burp Suite μπορούμε να δούμε τα διαπιστευτήρια της σύνδεσης , το email επανάκτησης του κωδικού και η ημερομηνία γέννησης που δηλώσαμε μέσα στην εφαρμογή.

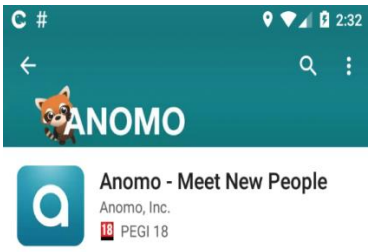
Στην εικόνα αυτή βλέπουμε τόσο το id που έχουμε επιλέξει για την εφαρμογή όσο και το password. Σημαντικό επίσης στοιχείο είναι το email, καθώς αυτό θα μπορούσε να συνδυαστεί με email που θα μπορούσε να δώσει ο χρήστης και σε άλλη επώνυμη εφαρμογή καθιστώντας την περιήγησή του στην «ανώνυμη» εφαρμογή ως τελικά καθόλου ανώνυμη καθώς το email και μόνο σε περίπτωση που έχει χρησιμοποιήσει το ίδιο και σε άλλο δίκτυο αρκεί για την ταυτοποίηση του.

Τα συμπεράσματα λοιπόν είναι τα εξής:

1) Η εν λόγω εφαρμογή δεν τηρεί ανωνυμία των χρηστών της, αφού απαιτείται για τη χρήση της να εισαχθεί η ηλεκτρονική διεύθυνση του χρήστη. Το γεγονός ότι ο χρήστης μπορεί να δημιουργήσει μία ηλεκτρονική διεύθυνση ειδικά για την εν λόγω εφαρμογή και να μην τη χρησιμοποιεί αλλού δεν την καθιστά ανώνυμη ως εφαρμογή (βλ. Κεφάλαιο 2)
2) Η εν λόγω εφαρμογή δεν παρέχει ασφάλεια ως προς τα προσωπικά δεδομένα των χρηστών της, αφού τόσο η διεύθυνση ηλεκτρονικού ταχυδρομείου όσο και το συνθηματικό (password) του χρήστη μπορούν σχετικά εύκολα να υποκλαπούν από οποιονδήποτε επίδοξο υποκλοπέα λόγω μη επαρκούς ελέγχου εγκυρότητας του ψηφιακού πιστοποιητικού (ο οποίος, με τη σειρά του, επίσης ενδέχεται να είναι σε θέση να ταυτοποιήσει το χρήστη).

Από τα παραπάνω προκύπτει ότι η χρήση της εφαρμογής μπορεί ενδεχομένως να επιφέρει πολύ δυσμενείς συνέπειες στο χρήστη (αν π.χ. αναγνωριστεί ο χρήστης από κάποιον τρίτο που κατέχει τα δεδομένα του και ταυτόχρονα ο χρήστης χρησιμοποιεί το ίδιο συνθηματικό και σε άλλες υπηρεσίες).

4.2.2. Λειτουργία της εφαρμογής Anomo



Εικόνα 4.17 : Το εικονίδιο της εφαρμογής όπως αυτή είναι διαθέσιμη μέσω του Google Play store.

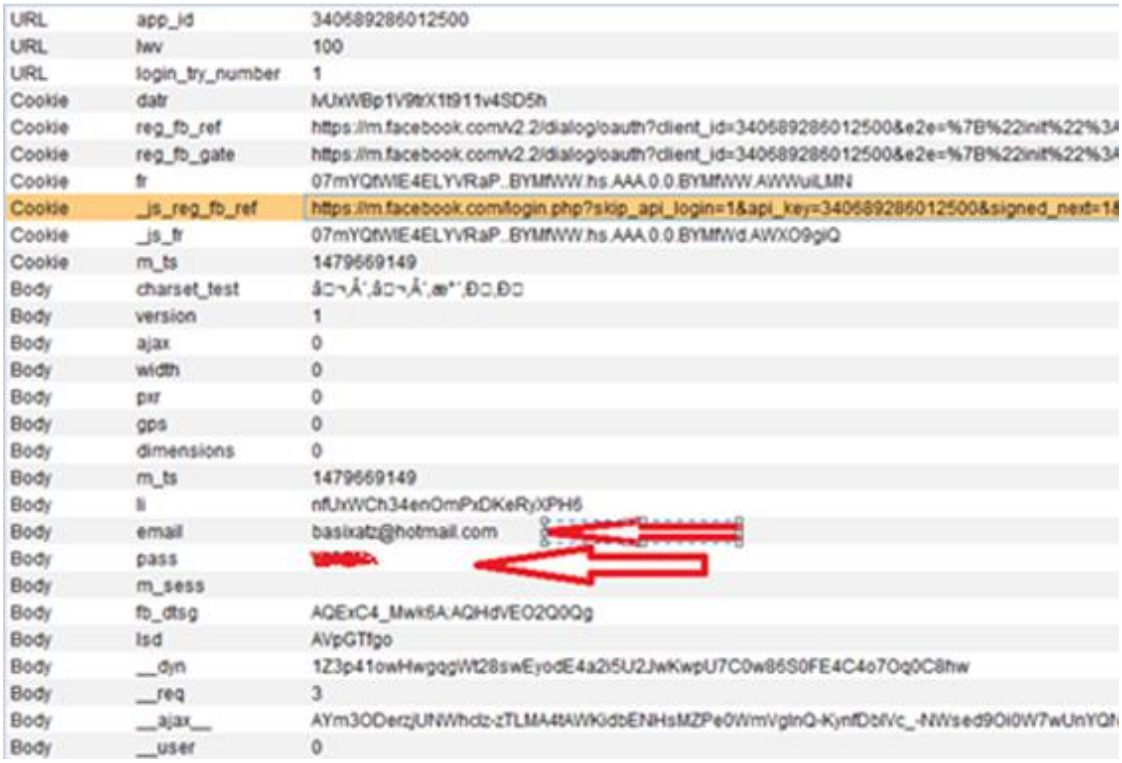
Η ανώνυμη εφαρμογή Anomo (http://www.anomo.com/) αποτελεί στην πραγματικότητα μια εφαρμογή γνωριμιών. Η διαφορετικότητα αυτής της εφαρμογής είναι ότι ένας χρήστης ξεκινάει ως ανώνυμος και στην συνέχεια έχει την δυνατότητα να ορίσει το βαθμό της ανωνυμίας του. Ο χρήστης κατά την είσοδό του στην εφαρμογή έχει την δυνατότητα είτε να κάνει απευθείας σύνδεση (sign in) είτε να εισέλθει σε αυτήν μέσω του Facebook λογαριασμού του. Μετά την πρώτη είσοδο στην εφαρμογή ο χρήστης επιλέγει avatar καθώς και τα θέματα που τον ενδιαφέρουν και βάσει των επιλογών του η εφαρμογή του προτείνει θέματα αλλά και άτομα για να συνομιλήσει.

Με τη χρήση της ίδιας μεθοδολογίας όπως και στην προηγούμενη εφαρμογή (δηλαδή μέσω του Burp Suite) αναλύουμε το Anomo. Το πρώτο ενδιαφέρον στοιχείο είναι ότι, όπως προαναφέραμε, κατά την είσοδο σε αυτή έχουμε την επιλογή να συνδεθούμε είτε κάνοντας sign in, είτε μέσω του λογαριασμού μας στο Facebook. Για τους σκοπούς της ανάλυσης μας θα εξετάσουμε και τις δυο περιπτώσεις για να δούμε ποια είναι τα δεδομένα που μπορούν αντληθούν από την χρήση της εφαρμογής.

Ξεκινώντας με την σύνδεση μέσω Facebook λαμβάνουμε ένα post μήνυμα μέσω του οποίου γίνεται η αυθεντικοποίηση του χρήστη με τα στοιχεία πρόσβασης στο Facebook. Μόνο από αυτό το γεγονός εξάγουμε το συμπέρασμα ότι η ανωμυμοποίηση στην συγκεκριμένη εφαρμογή δεν υφίσταται καθώς έχουμε ανακτήσει πολύ εύκολα το email του «ανώνυμου χρήστη», το οποίο μάλιστα είναι

συσχετισμένο με ένα μεγάλο επώνυμο κοινωνικό δίκτυο όπως το Facebook. Περαιτέρω, βλέπουμε ότι το Post μήνυμα που αποστέλλεται προς το Facebook περιέχει το όνομα χρήστη αλλά και τον κωδικό πρόσβασης σε μη κρυπτογραφημένη μορφή. Από το μήνυμα αυτό δεν είμαστε σε θέση να γνωρίζουμε αν το περιεχόμενο του μηνύματος αυτού γίνεται γνωστό και στην εφαρμογή Anomo, αν δηλαδή η εφαρμογή «μαθαίνει» με αυτόν τον τρόπο και όλους τους κωδικούς πρόσβασης των χρηστών στο Facebook.

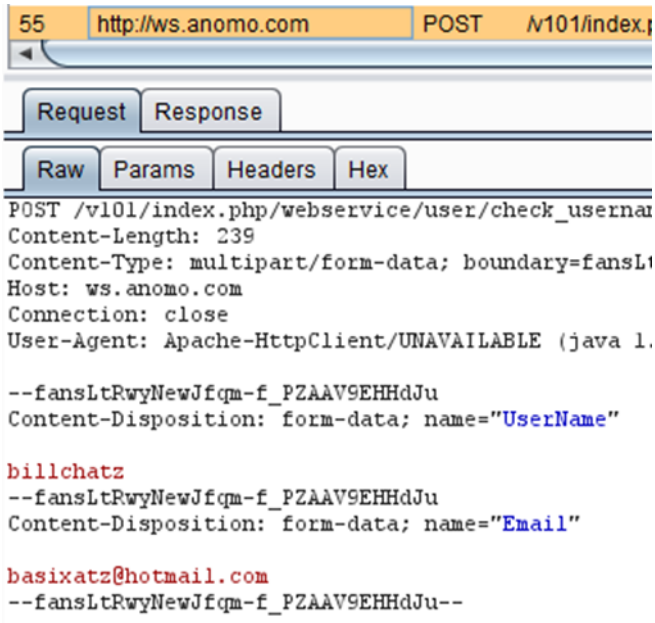
Εικόνα 4.18 : Μήνυμα που αποστέλλεται προς το Facebook κατά τη σύνδεση στην εφαρμογή Anomo (τα διαπιστευτήρια εμφανίζονται στην τελευταία γραμμή).



URL	app_id	340689286012500
URL	lwv	100
URL	login_try_number	1
Cookie	datr	MJxWBp1V9tX1t911v4SD5h
Cookie	reg_fb_ref	https://m.facebook.com/v2.2/dialog/oauth?client_id=340689286012500&e2e=%7B%22init%22%3A
Cookie	reg_fb_gate	https://m.facebook.com/v2.2/dialog/oauth?client_id=340689286012500&e2e=%7B%22init%22%3A
Cookie	fr	07mYQtWIE4ELYVRaP..BYMfWW.hs.AAA.0.0.BYMfWW.AWWuiLMN
Cookie	_js_reg_fb_ref	https://m.facebook.com/login.php?skip_api_login=1&api_key=340689286012500&signed_next=1&
Cookie	_js_fr	07mYQtWIE4ELYVRaP..BYMfWW.hs.AAA.0.0.BYMfWd.AWXO9giQ
Cookie	m_ts	1479669149
Body	charset_test	â□¬Å',â□¬Å',æ*',Ð□,Ð□
Body	version	1
Body	ajax	0
Body	width	0
Body	pxr	0
Body	gps	0
Body	dimensions	0
Body	m_ts	1479669149
Body	li	nfUxWCh34enOmPxDKeRyXPH6
Body	email	basixatz@hotmail.com
Body	pass	[redacted]
Body	m_sess	
Body	fb_dtsg	AQExC4_Mwk6A:AQHdVEO2Q0Qg
Body	lsd	AVpGTfgo
Body	__dyn	1Z3p41owHwgqgWt28swEyodE4a2i5U2JwKwpU7C0w86S0FE4C4o7Oq0C8hw
Body	__req	3
Body	__ajax__	AYm3ODerzjUfNWhdz-zTLMA4tAWKdbENHsMZPe0WmVginQ-KynfDbfVc_-NWsed9Oi0W7wUnYQ
Body	__user	0

Εικόνα 4.19: Τα διαπιστευτήρια της σύνδεσης στην εφαρμογή Anomo μέσω του Facebook είναι ορατά σε αυτή την εικόνα.

Στην συνέχεια επαναλαμβάνουμε την εγγραφή μας στην εφαρμογή αλλά τώρα ως τρόπο σύνδεσης επιλέγουμε να κάνουμε εγγραφή μέσω ειδικής φόρμας. Αυτό που παρατηρούμε είναι ότι τα στοιχεία που πληκτρολογούμε είναι και αυτά ανακτήσιμα μέσω του Burp Suite με ακριβώς τον ίδιο τρόπο όπως και στην σύνδεση μέσω Facebook. Στην παρακάτω εικόνα μπορούμε να δούμε το όνομα χρήστη αλλά και το email που δηλώθηκε κατά την εγγραφή.



Εικόνα 4.20: Μήνυμα από το Burp Suite που περιέχει τα διαπιστευτήρια που πληκτρολόγησε ο χρήστης κατά την εγγραφή του στην εφαρμογή.

Πέρα από τα στοιχεία εισόδου στην εφαρμογή, τα οποία και καταφέραμε να ανακτήσουμε, ενδιαφέρον παρουσιάζει το ερώτημα αν είμαστε σε θέση να ανακτήσουμε και τα διάφορα μηνύματα που θα αποστείλει ένας ανώνυμος χρήστης μέσω της συγκεκριμένης εφαρμογής. Για τον λόγο αυτό πραγματοποιήσαμε κάποια posts όπου και πάλι μέσω του Burp Suite μπορούμε να παρατηρήσουμε την συμπεριφορά της εφαρμογής. Αυτό που είναι εμφανές μέσω των επόμενων εικόνων είναι ότι η εφαρμογή όσο εκτελείται αποστέλλει διάφορα δεδομένα του κινητού του χρήστη. Για παράδειγμα στην επόμενη εικόνα έχουμε ένα Post μήνυμα προς το com.viasource.anomoinc.anomo, από το οποίο μπορούμε να δούμε ότι αποστέλλεται τόσο ένας κωδικός αποστολέα (sender) όσο και ένας κωδικός συσκευής (device). Οι κωδικοί αυτοί μπορεί να μην αντιστοιχούν κατ' αρχάς σε κάποιο εκ των αναγνωριστικών της συσκευής όπως αυτοί προσδιορίζονται στον Πίνακα 3.10, αλλά δείχνουν την γενική λειτουργία της εφαρμογής (εξάλλου, δεν μπορεί να αποκλειστεί το ενδεχόμενο από αυτούς τους κωδικούς, δεδομένου ότι δεν είναι γνωστός ο τρόπος παραγωγής τους, να μπορεί να υπολογιστεί κάποιο από τα αναγνωριστικά της συσκευής).

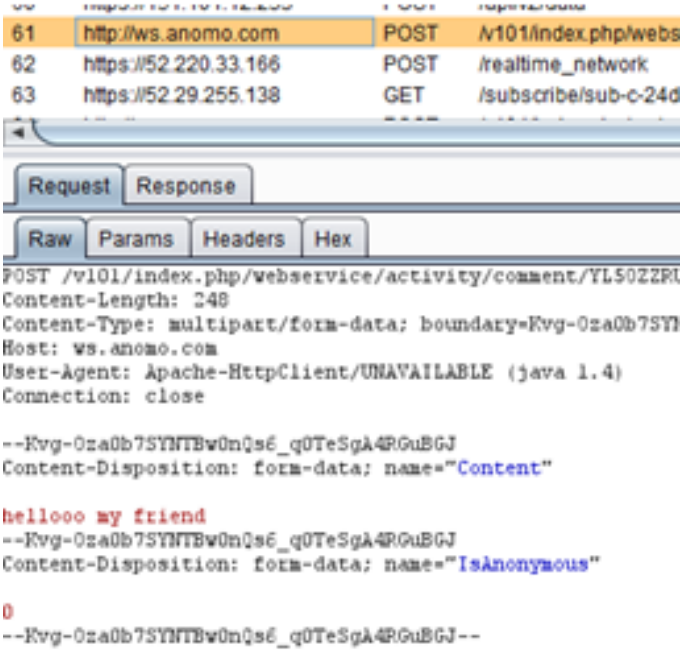
Εικόνα 4.21 : Post μήνυμα που λαμβάνουμε μέσω του Burp Suite και δείχνει την αποστολή κωδικών από το κινητό του χρήστη στους servers της εφαρμογής.

Στην επόμενη εικόνα έχουμε ένα άλλο post μήνυμα στο οποίο φαίνεται να αποστέλλεται το Google Advertising Id (GAID) του κινητού προς τους servers του ανώνυμου κοινωνικού δικτύου Anomo. Στο μήνυμα αυτό μπορούμε να διακρίνουμε ότι το πεδίο advertiser_tracking_enabled έχει τιμή true επομένως αντλείται από το κινητό το αναγνωριστικό το οποίο θα μπορούσε να παύσει την ανωμυμοποίηση ενός χρήστη και δείχνει με ακόμη ένα τρόπο ότι η συγκεκριμένη εφαρμογή προσφέρει ψευδωανυμοποίηση στους χρήστες της.

```
["al","com.vinasource.anomoinc.anomo",79,"2.11.9"]
--3i2ndDfv2rTHiSisAbouNdArYf0RhtTPEefj3q2f
Content-Disposition: form-data; name="advertiser_tracking_enabled"

true
--3i2ndDfv2rTHiSisAbouNdArYf0RhtTPEefj3q2f
Content-Disposition: form-data; name="anon_id"

XZ1cf2f50a-47b6-4604-b0fe-04f5036daf5e
--3i2ndDfv2rTHiSisAbouNdArYf0RhtTPEefj3q2f
Content-Disposition: form-data; name="advertiser_id"

4bff420f-2285-408b-a5e8-f6b06cb8c892
--3i2ndDfv2rTHiSisAbouNdArYf0RhtTPEefj3q2f
Content-Disposition: form-data; name="application_package_name"

com.vinasource.anomoinc.anomo
--3i2ndDfv2rTHiSisAbouNdArYf0RhtTPEefj3q2f
Content-Disposition: form-data; name="event"

CUSTOM_APP_EVENTS
--3i2ndDfv2rTHiSisAbouNdArYf0RhtTPEefj3q2f
Content-Disposition: form-data; name="application_tracking_enabled"

true
--3i2ndDfv2rTHiSisAbouNdArYf0RhtTPEefj3q2f
```

Εικόνα 4.22 : Post μήνυμα που λαμβάνουμε μέσω του Burp Suite και δείχνει την άντληση του αναγνωριστικού GAID από το κινητό του χρήστη και την αποστολή του προς τους servers της εφαρμογής.

Πέρα όμως από τα δεδομένα που αποστέλλονται αυτόματα από την εφαρμογή και έχουν να κάνουν με την λειτουργία της, στην επόμενη εικόνα μπορούμε να δούμε την ανάκτηση του περιεχομένου μιας δημοσίευσης στην εφαρμογή με την χρήση του Burp Suite. Το μήνυμα ήταν «**helooo my friend» .**



Εικόνα 4.23 : Ανάκτηση του περιεχομένου μιας δημοσίευσης στο ανώνυμο δίκτυο Anomo με την χρήση του Burp Suite.

Τα συμπεράσματα λοιπόν είναι τα εξής:

1. Η εφαρμογή είναι ευάλωτη σε επίθεση τύπου «Man In The Middle Attack». Με σχετικά εύκολο τρόπο καταφέραμε να καταδείξουμε ότι ενώ τα δεδομένα της εφαρμογής είναι κρυπτογραφημένα το γεγονός ότι δεν πιστοποιείτε το SSL chain και ότι το πιστοποιητικό έχει εκδοθεί από μια έμπιστη root certificate authority (CA), μπορεί να οδηγήσει σε επιτυχημένες επιθέσεις κατά της εφαρμογής. Συνεπώς, η εν λόγω εφαρμογή δεν παρέχει ασφάλεια ως προς τα προσωπικά δεδομένα των χρηστών της, αφού τόσο η διεύθυνση ηλεκτρονικού ταχυδρομείου όσο και το συνθηματικό (password) του χρήστη μπορούν σχετικά εύκολα να

υποκλαπούν από οποιονδήποτε επίδοξο υποκλοπέα (ο οποίος, με τη σειρά του, επίσης ενδέχεται να είναι σε θέση να ταυτοποιήσει το χρήστη).

2. Τα δεδομένα ενός ανώνυμου χρήστη της εφαρμογής μπορούν να συνδυαστούν με τα δεδομένα ενός επώνυμου δικτύου όπως το Facebook , καθώς η γνώση των διαπιστευτηρίων του Facebook μπορεί να οδηγήσει στην ταυτοποίηση του.
3. Η εφαρμογή συλλέγει το μοναδικό αναγνωριστικό GAID της συσκευής.

Από τα παραπάνω προκύπτει ότι η χρήση της εφαρμογής μπορεί ενδεχομένως να επιφέρει πολύ δυσμενείς συνέπειες στο χρήστη (αν π.χ. αναγνωριστεί ο χρήστης από κάποιον τρίτο που κατέχει τα δεδομένα του και ταυτόχρονα ο χρήστης χρησιμοποιεί το ίδιο συνθηματικό και σε άλλες υπηρεσίες). Εξάλλου, και το μοναδικό GAID της συσκευής θεωρείται προσωπικό δεδομένο του χρήστη της συσκευής, το οποίο πιθανότατα επεξεργάζονται πολλές άλλες εφαρμογές «έξυπνων» συσκευών. Είναι σωστό λοιπόν να θεωρήσουμε ότι τα δεδομένα των χρηστών αυτού του δικτύου είναι ψευδωνυμοποιημένα και όχι ανώνυμα.

4.2.3. Λειτουργία της εφαρμογής Whisper

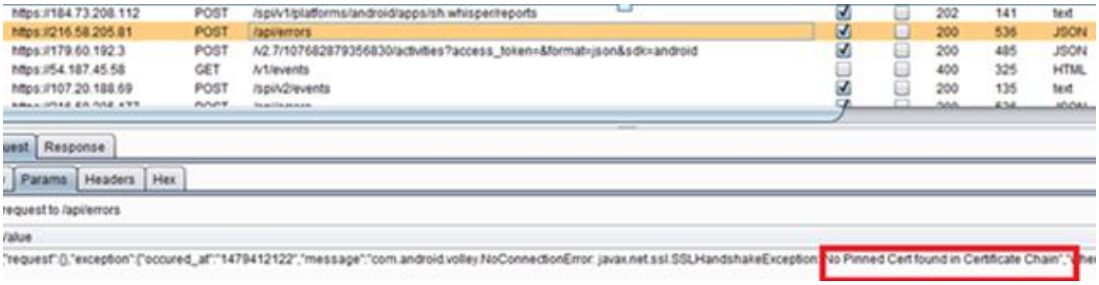
Εικόνα 4.24 : Το εικονίδιο της εφαρμογή Whisper όπως αυτή είναι διαθέσιμη μέσω του Google Play store.

Το Whisper (http://whisper.sh/) είναι μια εφαρμογή όπου ο χρήστης δεν δημιουργεί προφίλ και δεν απαιτείται είσοδος. Ουσιαστικά ένας χρήστης βλέπει posts άλλων χρηστών και μπορεί να σχολιάσει όποιο επιθυμεί. Κατά την είσοδό του παράγεται ένα μοναδικό αναγνωριστικό χρήστη (unique user_id) και με αυτό συνδέεται το κινητό με την εφαρμογή: αν ο χρήστης εισέλθει στην εφαρμογή από άλλο κινητό θα δημιουργηθεί άλλο user_id. Τα user_id των χρηστών αποθηκεύονται κεντρικά από την εφαρμογή έτσι ώστε όταν απαντάει κάποιος σε ένα post να μπορεί η εφαρμογή να στείλει μια ειδοποίηση στη συσκευή που συνδέεται με αυτό το user_id.

Η εφαρμογή μέσω του κεντρικού μενού διαθέτει τέσσερις (4) κατηγορίες οι οποίες είναι οι εξής:

- Οι ομάδες (Groups). Μέσα από αυτή την επιλογή ο χρήστης μπορεί να εισέλθει σε κάποιο group ή να δημιουργήσει κάποιο καινούργιο.
- Τα δημοφιλή. Μέσα από αυτή την επιλογή ο χρήστης έχει την δυνατότητα να δει τις δημοσιεύσεις με τη μεγαλύτερη απήχηση.
- Τα εγγύτερα (Nearby). Δίνεται η δυνατότητα στον χρήστη να δει δημοσιεύσεις από χρήστες σε μικρή γεωγραφική απόσταση από τον ίδιο.
- Τα πιο πρόσφατα. Τέλος ο χρήστης έχει την δυνατότητα να δει τις πιο πρόσφατες δημοσιεύσεις.

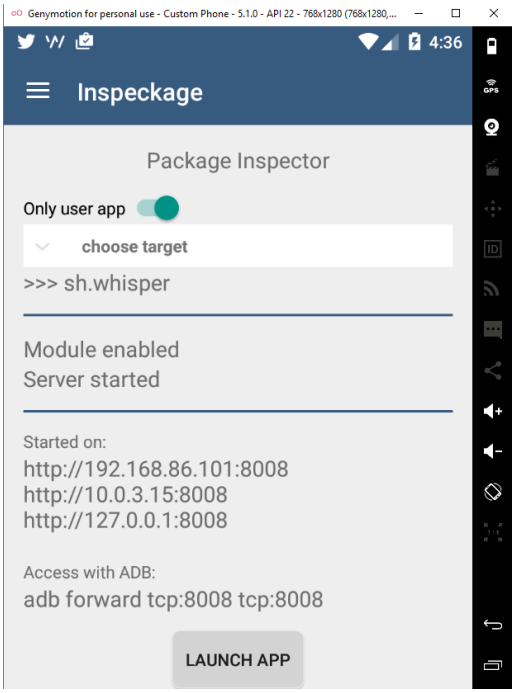
Χρησιμοποιήσαμε κατ' αρχάς, και στην εφαρμογή Whisper, την ίδια τεχνική όπου με την βοήθεια του Burp Suite σε ένα κινητό προσπαθήσαμε να ανακατευθύνουμε όλη την κίνηση της εφαρμογής στον Proxy. Η συγκεκριμένη τεχνική όμως δεν είχε αποτέλεσμα σε αυτήν την εφαρμογή, και όπως φαίνεται και στην παρακάτω εικόνα, λαμβάνουμε μήνυμα λάθους στο burp suite με αιτιολογία το ότι το πιστοποιητικό δεν είναι pinned, καθώς όπως φαίνεται η συγκεκριμένη εφαρμογή χρησιμοποιεί ssl pinning (Pinning είναι η διαδικασία συσχέτισης μιας εφαρμογής με το απαιτούμενο πιστοποιητικό ή δημόσιο κλειδί) έτσι ώστε να αποτρέψει επιθέσεις σαν αυτές που εκμεταλλευτήκαμε στις προηγούμενες εφαρμογές.



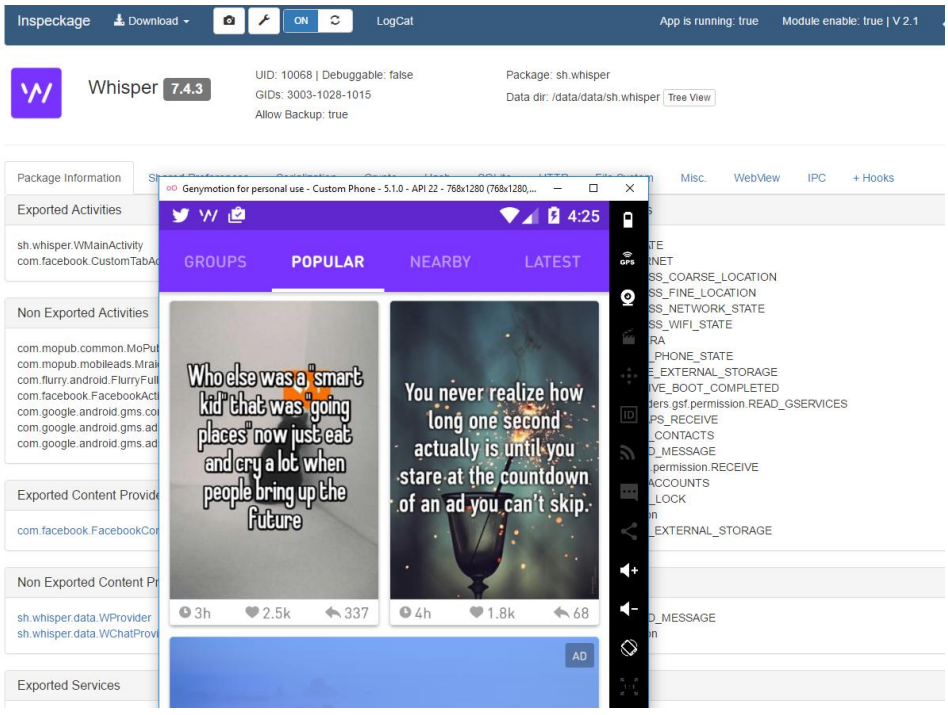
Εικόνα 4.25 : Μήνυμα λάθους που λαμβάνουμε από το Burp Suite που μας ενημερώνει ότι το πιστοποιητικό που χρησιμοποιείται για την σύνδεση μας δεν είναι έγκυρο.

Για να ξεπεράσουμε αυτό το μέτρο ασφαλείας για τους σκοπούς της έρευνάς μας θα πρέπει, όπως έχουμε δει στο προηγούμενο κεφάλαιο, να εγκαταστήσουμε το Xposed framework σε ένα κινητό με δικαιώματα root και να κατεβάσουμε και να εγκαταστήσουμε τα Modules SSLUnpinning και Inspeckage. Μέσα από το SSLUnpinning θα επιλέξουμε να κάνουμε unpin τα πιστοποιητικά στις εφαρμογές που θέλουμε να αναλύσουμε, ενώ μέσω του Inspeckage όπως δείχνει και η επόμενη εικόνα θα επιλέξουμε την εφαρμογή Whisper και μέσω του GUI interface που μας παρέχει θα εκτελέσουμε δυναμική ανάλυση της εφαρμογής.

Πρώτα, όπως δείχνει η παρακάτω εικόνα, επιλέγουμε και εκτελούμε την εφαρμογή Whisper, κάτι που μας οδηγεί στην επόμενη εικόνα όπου βλέπουμε την εκτέλεση της εφαρμογής, καθώς επίσης και τη δυναμική ανάλυσή της μέσω του Inspeckage.

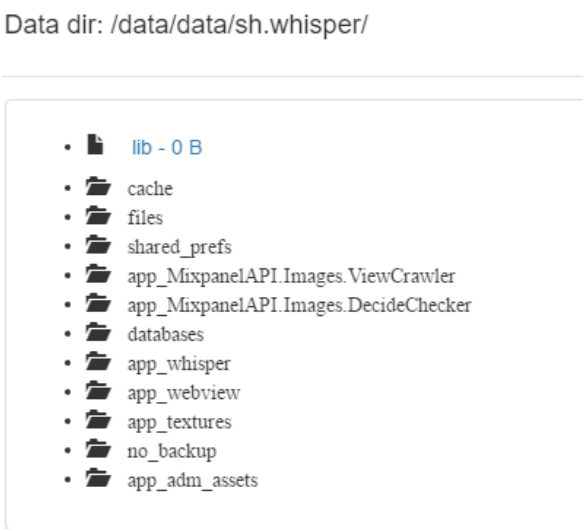


Εικόνα 4.26 :Το κεντρικό menu του module Inspeckage κατά την επιλογή της εφαρμογής Whisper.



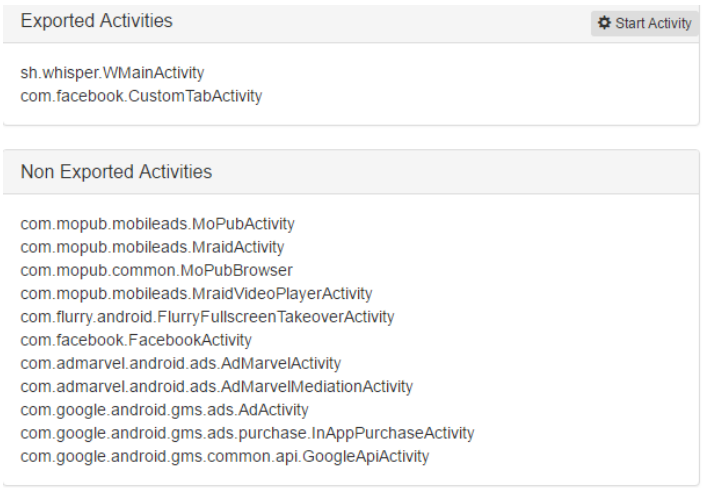
Εικόνα 4.27: Το γραφικό περιβάλλον του Inspeckage κατά την εκτέλεση της εφαρμογής Whisper.

Μέσω του Inspeckage μπορούμε να δούμε ποια δεδομένα «φορτώνονται» κατά την εκκίνηση της εφαρμογής. Τα δεδομένα αυτά είναι ορατά μέσω αρχείων τύπου xml. Από την επιλογή «Tree View» μπορούμε να δούμε μια λίστα με τα directories της εφαρμογής.



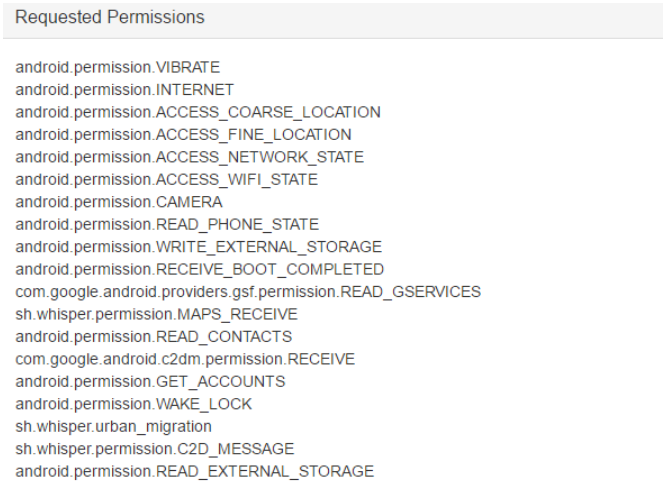
Εικόνα 4.28: Συνοπτική ανάλυση των αρχείων της εφαρμογής Whisper μέσω του Inspeckage.

Η επόμενη εικόνα μας δείχνει τις Exported και τις μη Exported διεργασίες της εφαρμογής και από το κουμπί Start Activity μπορούμε να ενεργοποιήσουμε όποια επιθυμούμε και να δούμε πώς θα συμπεριφερθεί η εφαρμογή.



Εικόνα 4.29: Παρουσίαση των εξερχόμενων και των μη εξερχόμενων δραστηριοτήτων της εφαρμογής Whisper μέσω του γραφικού περιβάλλοντος του Inspeckage.

Επιπλέον μέσω του Inspeckage μπορούμε να παρακολουθήσουμε τα δικαιώματα που χρησιμοποιεί η εφαρμογή όπως δείχνει η παρακάτω εικόνα.



Εικόνα 4.30: Παρουσίαση των δικαιωμάτων που χρησιμοποιεί η εφαρμογή Whisper για την εκτέλεσή της.

Μέσω του SQLite βλέπουμε αν η εφαρμογή εκτελεί κάποιο ερώτημα (query) αλλά και τα δεδομένα που περιέχει αυτό. Στην παρακάτω εικόνα μπορούμε να παρατηρήσουμε ότι κατά την εκτέλεση της εφαρμογής εκτελούνται διάφορα query's που κάνουν εισαγωγή δεδομένων (Insert) στους πίνακες με όνομα people και events και τα χαρακτηριστικά που αποθηκεύονται σε αυτούς τους πίνακες είναι τα χαρακτηριστικά του κινητού από το οποίο εκτελούμε δυναμική ανάλυση.

Εικόνα 4.31: Παρουσίαση των SQL statements που εκτελούνται κατά την εκτέλεση της εφαρμογής Whisper μέσα σε αυτά φαίνεται να αποθηκεύονται πληροφορίες από το κινητό του χρήστη όπως ο κατασκευαστής και το μοντέλο του κινητού.

Ένα ενδιαφέρον στοιχείο που μπορούμε να παρατηρήσουμε μέσω του Inspeckage είναι ότι το Whisper αντλεί το GAID (Google Advertising Id) από το κινητό του χρήστη - ένα στοιχείο που μπορεί να θεωρηθεί ως μοναδικό χαρακτηριστικό μιας συσκευής. Το αναγνωριστικό είναι ορατό μέσω του tab Shared Preferences.

TwitterAdvertisingInfoPreferences.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="limit_ad_tracking_enabled" value="false" ></boolean>
    <string name="advertising_id">4bff420f-2285-408b-a5e8-f6b06cb8c892</string>
</map>
```

Εικόνα 4.32: Στο xml με όνομα TwitterAdvertisingInfoPreferences.xml αποθηκεύει η εφαρμογή Whisper το Google Advertising Id του κινητού του χρήστη.

Επίσης βλέπουμε ότι κατά την εκτέλεση της εφαρμογής αποθηκεύονται και οι gps συντεταγμένες του κινητού: οι συντεταγμένες αυτές είναι ορατές μέσω του tab «Shared Preferences.»

```
<long name="last_successful_ad_timestamp" value="1485718287461" ></lor
<float name="longitude_prefs_key" value="25.876919" ></float>
<float name="lattitude_prefs_key" value="40.85136" ></float>
<string name="nickname">Coffee Knight</string>
```

Εικόνα 4.33: Στην καρτέλα Preferences του Inspeckage μπορούμε να δούμε την άντληση των gps συντεταγμένων από την εφαρμογή Whisper.

Το χαρακτηριστικό αυτό στο Whisper γίνεται διότι μέσω του tab NEARBY δίνεται η δυνατότητα σε γειτονικούς χρήστες να δουν αυτές τις αναρτήσεις. Ένα επίσης πολύ σημαντικό χαρακτηριστικό είναι ότι μέσω της δυναμικής ανάλυσης έχουμε την δυνατότητα να δούμε και το περιεχόμενο των δημοσιεύσεων που κάνουμε στο Whisper.

Για λόγους δοκιμής δημοσιεύσαμε το post που φαίνεται στην παρακάτω εικόνα

Εικόνα 4.34:Παρουσίαση μιας τυπικής ανάρτησης μέσω της εφαρμογής Whisper. Η εικόνα στο υπόβαθρο έχει προταθεί αυτόματα από την εφαρμογή.

1062 UPDATE w SET create_image_number=0,lon=25.880425,internal_id=1529270644,place_source=null,to_place_display_
ages.net/054be3e6f93531df75e7e6c4624c2225ff3853-v5.jpg,create_search_term=null,from_place_id=null,place_type=null,pla
17083942,to_place_image_url_home=null,retry=0,is_client_rendered=0,display_value=null,create_image_url=http://repo.wima
_crossed_paths=0,remote_attachment_url=null,_id=054be3e6f93531df75e7e6c4624c2225ff3853,to_place_image_url_browse
_source=suggest,wide_thumbnail=null,to_place_image_url_list=null,cell_type=1,create_font=Upright.otf,card_json_string=null,
pe=null,place_id=null,m=1,create_text_y_offset=0,parent=null,location=null,puid=null,text=Helloo evros,sort=0,lat=40.8463033,

Εικόνα 4.35: Ανάκτηση τόσο του περιεχομένου μιας δημοσίευσης στο δίκτυο Whisper με την χρήση του Inspeckage όσο και της γεωγραφικής θέσης από το οποίο έγινε η δημοσίευση (το περιεχόμενο της είναι ορατό στην τελευταία γραμμή) .

Το ενδιαφέρον είναι ότι στην παραπάνω εικόνα μπορούμε να δούμε τόσο το μήνυμα που κάναμε post δηλαδή το **Helloo evros** όσο και τις ακριβείς γεωγραφικές συντεταγμένες από όπου έγινε η δημοσίευση αυτή.

Τα συμπεράσματα λοιπόν είναι τα εξής:

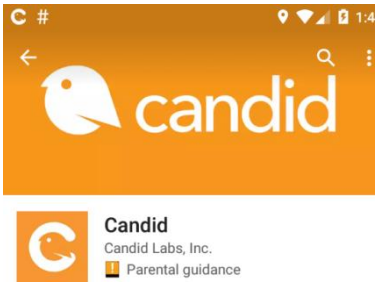
1) Το γεγονός ότι οι χρήστες συνδέονται στο Whisper χωρίς να δημιουργούν προφίλ είναι σίγουρα ένα χαρακτηριστικό που προσδίδει ασφάλεια στο δίκτυο αυτό μιας και δεν υπάρχουν καταχωρημένα προσωπικά δεδομένα των χρηστών. Επίσης, σε αντίθεση με τις προηγούμενες δύο εφαρμογές, δεν είναι εύκολα εφικτή η πραγματοποίηση επίθεσης τύπου «man-in-the-middle» attack λόγω της τεχνικής ssl pinning που έχει υιοθετηθεί.

2) Το Inspeckage έδειξε ότι η εφαρμογή αντλεί από το κινητό του χρήστη το GAID (Google Advertising ID). Η εύρεση του αναγνωριστικού σημαίνει ότι στο κινητό υπάρχει εγκατεστημένο το Google Play Store και ο λόγος που χρησιμοποιείται είναι η μοναδικοποίηση του κινητού έτσι ώστε να του παρουσιάζονται στοχευμένες διαφημίσεις.

3) Δείξαμε ότι μέσω του Inspeckage είναι δυνατή η άντληση τόσο του περιεχομένου των δημοσιεύσεων ενός χρήστη όσο και η άντληση της ακριβής γεωγραφικής του θέσης την στιγμή της δημοσίευσης ενός μηνύματος.

Από τα παραπάνω προκύπτει ότι ενώ η εφαρμογή χρησιμοποιεί τρόπους να προστατεύσει την ανωνυμία των χρηστών της, υπάρχουν τρόποι με τους οποίους η ανωνυμία αυτή μπορεί να αναιρεθεί γεγονός που ενδεχομένως να επιφέρει πολύ δυσμενείς συνέπειες στον χρήστη. Εξάλλου, το μοναδικό GAID της συσκευής θεωρείται προσωπικό δεδομένο του χρήστη της συσκευής, το οποίο πιθανότατα επεξεργάζονται πολλές άλλες εφαρμογές «έξυπνων» συσκευών. Είναι σωστό λοιπόν να θεωρήσουμε ότι τα δεδομένα των χρηστών αυτού του δικτύου είναι ψευδωνυμοποιημένα και όχι ανώνυμα.

4.2.4. Λειτουργία της εφαρμογής Candid



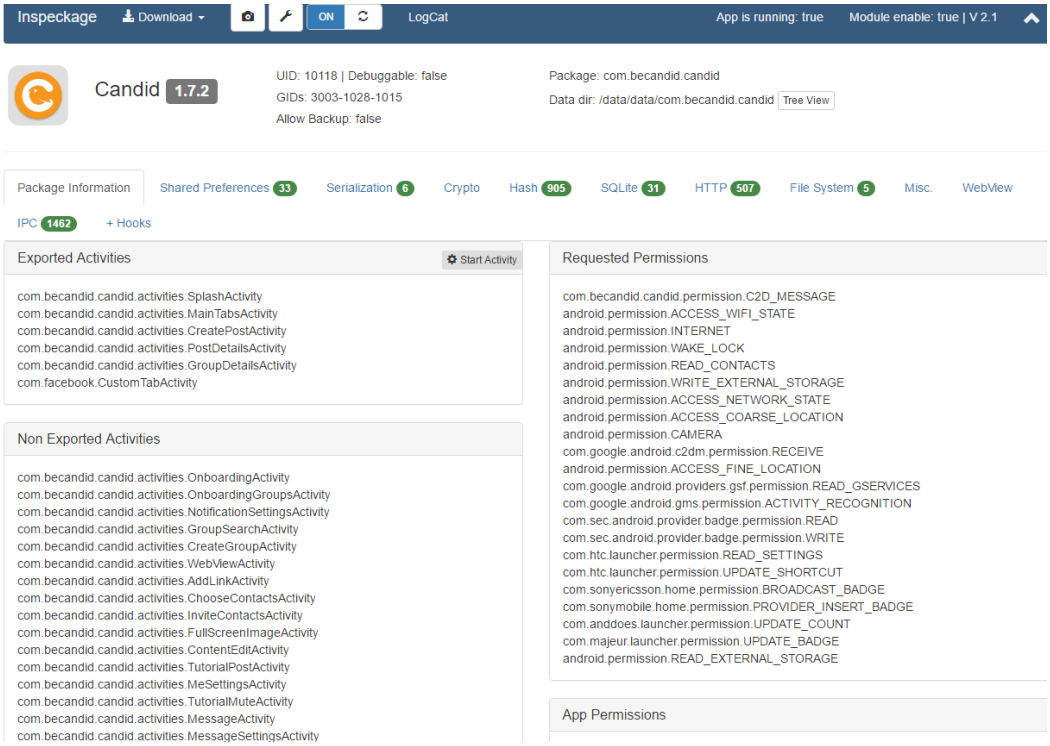
Εικόνα 4.36: Το εικονίδιο της εφαρμογή Candid όπως αυτή είναι διαθέσιμη μέσω του Google Play store.

Το Candid (https://becandid.com/) έχει αναπτύξει ένα σύστημα το οποίο αναλύει όλα τα δημοσιευμένα σχόλια στην εφαρμογή και σημειώνει προς διαγραφή δημοσιεύσεις που περιέχουν εκφράσεις όπως μίσος και απειλές. Η εγγραφή στην εφαρμογή μπορεί να γίνει με την χρήση του λογαριασμού Facebook, ενώ όλα τα προσωπικά δεδομένα των χρηστών όπως η ip διεύθυνση αλλά και η τοποθεσία του χρήστη κρυπτογραφούνται με one-way hash πριν φτάσουν στους servers της εταιρίας. Η εφαρμογή απαιτεί από τους χρήστες να πληκτρολογήσουν τον αριθμό του τηλεφώνου τους κατά την διάρκεια της αρχικής εγγραφής – όπως διαπιστώθηκε κατά τη χρήση της εφαρμογής - και χρησιμοποιεί αυθεντικοποίηση δυο επιπέδων για να πιστοποιήσει ότι ο αριθμός είναι πραγματικός.

Μετά την αρχική εγγραφή το Candid προσφέρει ένα σύνολο από μηχανισμούς ασφάλειας έτσι ώστε να εξασφαλίσει την ασφάλεια του χρήστη. Πιο συγκεκριμένα η εφαρμογή εφαρμόζει ένα νέο, συνεχώς τυχαίο σύστημα απόδοσης ονομάτων στους χρήστες με ονόματα όπως «Curious Rabbit» ή «Creative Lemur». Επίσης η εφαρμογή "αναγκάζει" ευγενικά τους χρήστες της να είναι ευγενικοί, για αυτό αποδίδει διάφορα σήματα όπως «Explorer», «Giver» or «Gossip» για θετικά σχόλια και «Hater» σε χρήστες οι οποίο είναι μονίμως αρνητικοί. Η διαδικασία αυτή είναι πλήρως αυτοματοποιημένη και γίνεται σε μια προσπάθεια περιορισμού του φαινομένου του cyber bulling.

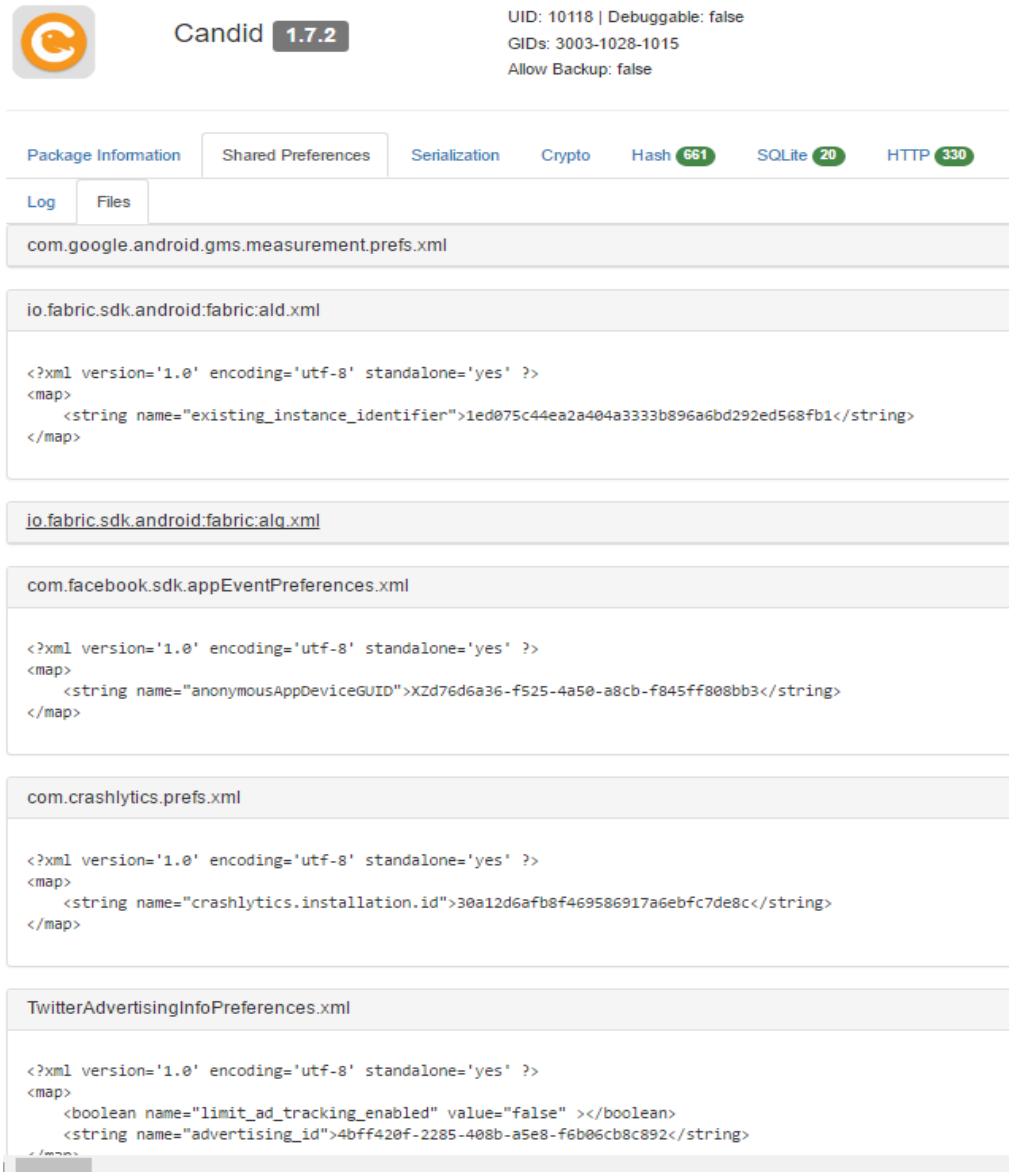
Μέσω του Inspeckage επιλέγουμε την εφαρμογή Candid για ανάλυση όπου, όπως φαίνεται και στην παρακάτω εικόνα, μπορούμε να δούμε πάλι τις Export-

ed Activities τις Non Exported Activities τα Requested Permissions και άλλες πληροφορίες.



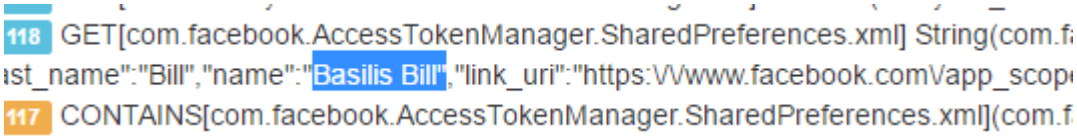
Εικόνα 4.37: Γενική απεικόνιση όλων των λειτουργιών που εκτελούνται κατά την εκτέλεση της εφαρμογής Candid.

Μέσω της καρτέλας “Shared Preferences” και στην επιλογή “Files” βλέπουμε τα διάφορα xml αρχεία όπου στο τέλος της επόμενης εικόνας μπορούμε να δούμε ότι στο xml με όνομα TwitterAdvertisingInfoPreferences.xml αποθηκεύεται το Advertising id του κινητού. Το id αυτό έχει την ίδια τιμή με το id που ανακτήσαμε και από το Anomo.



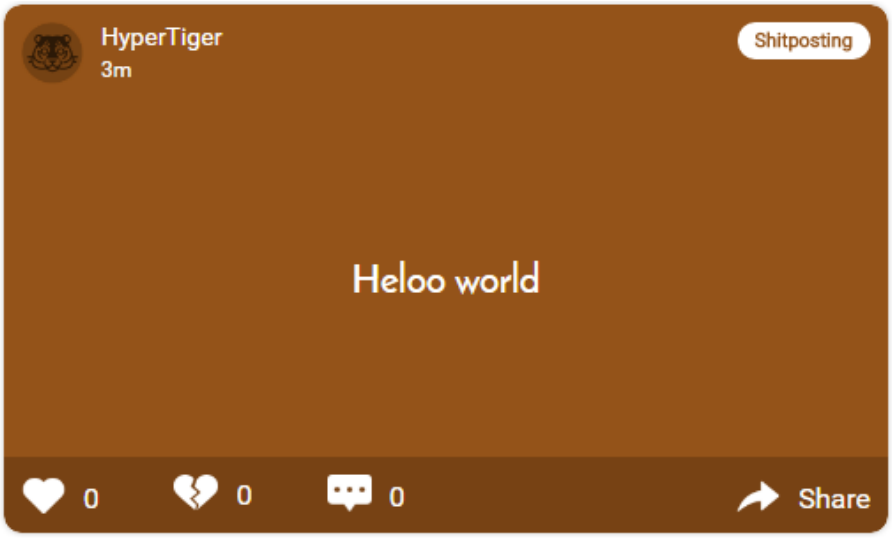
Εικόνα 4.38: Ανάλυση της εφαρμογής Candid όπου στο Shared Preferences και συγκεκριμένα στο xml με τίτλο TwitterAdvertisingInfoPreferences.xml αποθηκεύετε το Advertising Id του κινητού.

Όπως έχουμε ήδη αναφέρει η σύνδεση στην εφαρμογή μπορεί να γίνει με την βοήθεια του Facebook και η επόμενη εικόνα μας δείχνει ότι το όνομα χρήστη στο Facebook που πληκτρολογήθηκε από τον χρήστη ανακτάται μέσω του Inspeckage.



Εικόνα 4.39: Μέσω της καρτέλας Preferences του Inspeckage έχουμε την δυνατότητα να ανακτήσουμε το username ενός χρήστη στην εφαρμογή του Facebook.

Τέλος προσπαθήσαμε να ερευνήσουμε αν έχουμε την δυνατότητα να ανακτήσουμε μια δημοσίευση ενός μηνύματος στο Candid. Για τον λόγο αυτό δημοσιεύσαμε το μήνυμα που φαίνεται στην παρακάτω εικόνα.



Εικόνα 4.40: Τυπική δημοσίευση μηνύματος μέσω της εφαρμογής Candid.

Το μήνυμα αυτό δεν έχουμε την δυνατότητα να το ανακτήσουμε μέσω του Inspeckage όπως επίσης θα πρέπει να σημειώσουμε ότι το Candid δεν φαίνεται να αποθηκεύει και τις γεωγραφικές συντεταγμένες της θέσης μας.

Τα συμπεράσματα λοιπόν είναι τα εξής:

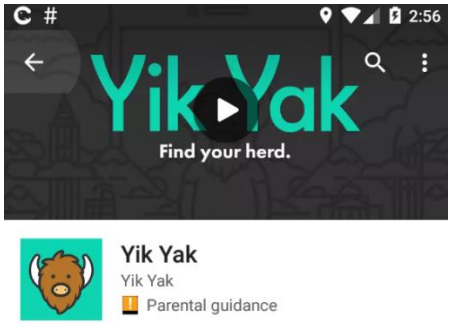
1) Η εφαρμογή χρησιμοποιεί ssl pinning, κάτι που σημαίνει ότι δεν είναι ευάλωτη σε επιθέσεις «Man In The Middle» όπως οι Social Number και Anomo.

2) Το Inspeckage έδειξε ότι η εφαρμογή αντλεί από το κινητό του χρήστη το GAID (Google Advertising ID). Η εύρεση του αναγνωριστικού σημαίνει ότι στο κινητό υπάρχει εγκατεστημένο το Google Play Store και ο λόγος που χρησιμοποιείται είναι η μοναδικοποίηση του κινητού έτσι ώστε να του παρουσιάζονται στοχευμένες διαφημίσεις.

3) Δείξαμε ότι μέσω του Inspeckage δεν είναι δυνατή η άντληση τόσο του περιεχομένου των δημοσιεύσεων ενός χρήστη όσο και η άντληση της ακριβής γεωγραφικής του θέσης την στιγμή της δημοσίευσης ενός μηνύματος.

Από τα παραπάνω προκύπτει ότι η εφαρμογή προσφέρει κατ' αρχάς καλούς μηχανισμούς ασφάλειας στους χρήστες της. Τα περιεχόμενα των δημοσιεύσεων δεν ήταν δυνατό να ανακτηθούν όπως και η γεωγραφική θέση του χρήστη. Η εφαρμογή αντλεί ωστόσο το αναγνωριστικό GAID όπως και το Whisper οπότε, παρόλο που ο χρήστης μπορεί να ταυτοποιηθεί μόνο σε περίπτωση που το δεδομένο αυτό συνδυαστεί με δεδομένα κάποιας άλλης εφαρμογής, η εφαρμογή επιτελεί ψευδωνυμοποίηση και όχι ανωνυμοποίηση του χρήστη.

4.2.5. Λειτουργία της εφαρμογής Yik Yak

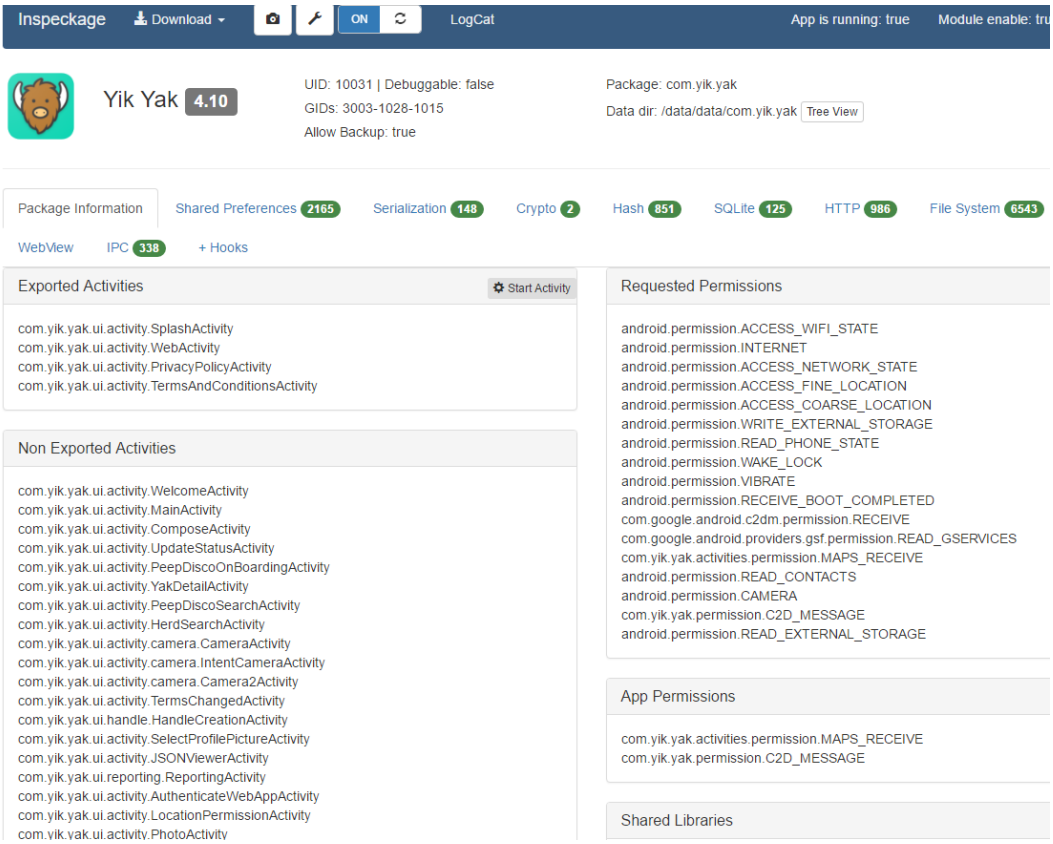


Εικόνα 4.41 : Το εικονίδιο της εφαρμογή YikYak όπως αυτή είναι διαθέσιμη μέσω του Google Play store.

Το Yik Yak (https://www.yikyak.com/home) ξεκίνησε να λειτουργεί το 2013 και σταμάτησε την λειτουργία του, όπως έχουμε αναφέρει στο κεφάλαιο 1, τον Απρίλιο του 2017.Η ανάλυση του δικτύου έγινε όταν αυτό λειτουργούσε ακόμη και δείχνει τον τρόπο λειτουργίας του και τα δεδομένα που αντλεί από τον χρήστη. Το YikYak είναι ένα δωρεάν τοπικό κοινωνικό δίκτυο το οποίο επιτρέπει στους χρήστες του να δημοσιεύουν «τα πάντα» ανώνυμα. Οι χρήστες της εφαρμογής δημοσιεύουν σύντομα μηνύματα - όπως και στο Twitter - αλλά και φωτογραφίες οι οποίες είναι διαθέσιμες στον οποιοδήποτε βρίσκεται στην ίδια γεωγραφική περιοχή. Λειτουργεί μέσω του GPS για να αναγνωρίσει πού βρίσκεται ο χρήστης κάθε χρονική στιγμή. Οι υπόλοιποι χρήστες έχουν την δυνατότητα να δώσουν είτε θετική είτε αρνητική ψήφο στις δημοσιεύσεις άλλων χρηστών. Τα μηνύματα εντός της εφαρμογής ποικίλουν από γενικές ερωτήσεις σε προσωπικές απόψεις για κάποιο θέμα αλλά και σε αρνητικά μηνύματα για κάποιον άλλο. Το 2015 η εφαρμογή ξεκίνησε να επιτρέπει μηνύματα με φωτογραφίες και το 2016 η εφαρμογή ξεκίνησε να απαιτεί από τους χρήστες της να πληκτρολογήσουν ένα όνομα χρήστη. Σύμφωνα με τους όρους χρήσης της εφαρμογής, κάθε χρήστης που την χρησιμοποιεί θα πρέπει να είναι μεγαλύτερος από 17 χρονών - αν και η εφαρμογή δεν ζητάει από τους χρήστες να το επιβεβαιώσουν αυτό

Χρησιμοποιώντας για ακόμη μια φορά το Inspeckage και επιλέγοντας μέσω του πλαισίου επιλογής την εφαρμογή Yik Yak προχωράμε στην δυναμική ανάλυσή

της. Η παρακάτω εικόνα δείχνει τα Exported Activities Non Exported Activities, Requested Permissions και App permissions τις εφαρμογής.



Εικόνα 4.42: Γενική απεικόνιση των λειτουργιών που εκτελούνται κατά την εκκίνηση της εφαρμογής YikYak.

Πάλι μέσω του tab «Shared Preferences» και στην επιλογή «Files» μπορούμε να δούμε ότι και σε αυτήν την εφαρμογή αποθηκεύεται το GAID του κινητού μέσα στο xml TwitterAdvertisingInfoPrefereces.xml

TwitterAdvertisingInfoPreferences.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="limit_ad_tracking_enabled" value="false" ></boolean>
    <string name="advertising_id">4bff420f-2285-408b-a5e8-f6b06cb8c892</string>
</map>
```

Εικόνα 4.43: Η εφαρμογή YikYak αποθηκεύει το Google Advertising id του κινητού στο xml με τίτλο TwitterAdvertisingInfoPreferences.xml

Επίσης το Yik Yak έχει μια παρόμοια λειτουργία με το Whisper καθώς αποθηκεύει τις gps συντεταγμένες του χρήστη που συνδέεται. Αυτό είναι ορατό μέσω του tab SQLite όπου σε διάφορα queries που φαίνονται να πραγματοποιούνται από την εφαρμογή αποστέλλονται προς την εφαρμογή σημαντικές πληροφορίες του κινητού.

Device manufacturer: Xiaomi

Device model:Redmi Note 3

Carrier:Vodafone

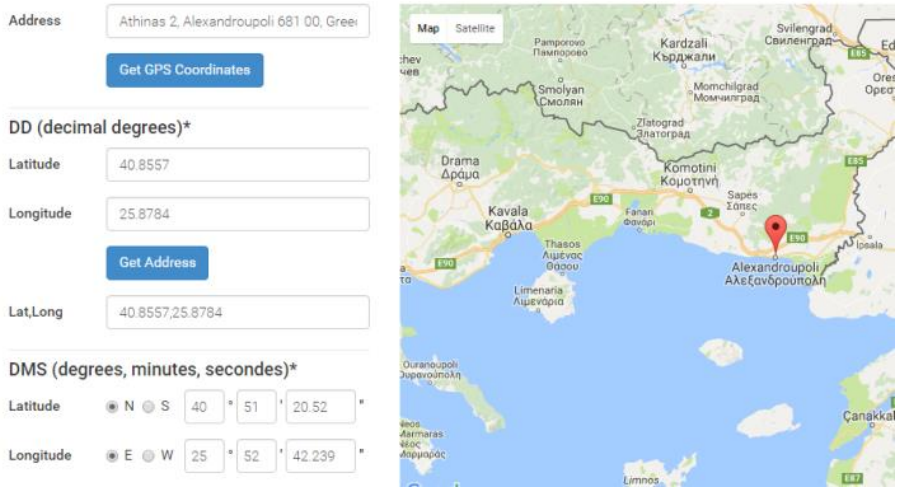
AndroidADID: 4bff420f-2285-408b-a5e8-f6b06cb8c892

Location: lat:40.8557 και lng: 25.878490000000003

'device_manufacturer":"Xiaomi","device_model":"Redmi Note 3","carrier":"vodafone GR","country":"GR","language":"el","platform":"Android","u
'sequence_number":217,"library":{"name":"amplitude-android","version":"2.7.1"},"api_properties":{"androidADID":"992a3c8c-5d12-4c00-8b6c-
abled":true},"event_properties":{},"user_properties":{"$set":{"Yakarma":106}},"groups":{}} id=130,event={"event_type":"$identify","timestamp":
4B5F06A5A471D5E07","device_id":"3190d47e-c11f-4131-89c3-958c391e8e9dR","session_id":1482075835393,"version_name":"4.7","os_na
":"Xiaomi","device_manufacturer":"Xiaomi","device_model":"Redmi Note 3","carrier":"vodafone GR","country":"GR","language":"el","platfor
d032b60a81f8","sequence_number":218,"library":{"name":"amplitude-android","version":"2.7.1"},"api_properties":{"androidADID":"992a3c8c-5
g":false,"gps_enabled":true},"event_properties":{},"user_properties":{"$set":{"HasEverSetProfilePic":false}},"groups":{}} id=131,event={"event_
ser_id":"6ABE83EDDD03B1B4B5F06A5A471D5E07","device_id":"3190d47e-c11f-4131-89c3-958c391e8e9dR","session_id":148207583539
_version":"5.0.2","device_brand":"Xiaomi","device_manufacturer":"Xiaomi","device_model":"Redmi Note 3","carrier":"vodafone GR","countr
":"d3d5dc0e-30bb-47b1-a54f-e89792f298ce","sequence_number":220,"library":{"name":"amplitude-android","version":"2.7.1"},"api_propertie
52d88b688f9","limit_ad_tracking":false,"gps_enabled":true},"event_properties":{},"user_properties":{"$set":{"HasBio":true}},"groups":{}} id=13
85361565327,"user_id":"6ABE83EDDD03B1B4B5F06A5A471D5E07","device_id":"3190d47e-c11f-4131-89c3-958c391e8e9dR","session_id":
e":"android","os_version":"5.0.2","device_brand":"Xiaomi","device_manufacturer":"Xiaomi","device_model":"Redmi Note 3","carrier":"vodafon
Android","uuid":"7ea40062-ac27-4efb-9a9d-b1bdc70224e8","sequence_number":225,"library":{"name":"amplitude-android","version":"2.7.
":25.878490000000003},"androidADID":"4bff420f-2285-408b-a5e8-f6b06cb8c892","limit_ad_tracking":false,"gps_enabled":true},"event_prop
6}},"groups":{}} id=133,event={"event_type":"$identify","timestamp":1485361565419,"user_id":"6ABE83EDDD03B1B4B5F06A5A471D5E0
91e8e9dR","session_id":1485361562247,"version_name":"4.10","os_name":"android","os_version":"5.0.2","device_brand":"Xiaomi","device_
Note 3","carrier":"vodafone GR","country":"GR","language":"el","platform":"Android","uuid":"eef89075-33bd-4085-943f-02f79168b10e","sequen
droid","version":"2.7.1"},"api_properties":{"location":{"lat":40.8557,"lng":25.878490000000003},"androidADID":"4bff420f-2285-408b-a5e8-f6b0
d":true},"event_properties":{},"user_properties":{"$set":{"HasEverSetProfilePic":false}},"groups":{}} id=134,event={"event_type":"$identify","tim
)D03B1B4B5F06A5A471D5E07","device_id":"3190d47e-c11f-4131-89c3-958c391e8e9dR","session_id":1485361562247,"version_name":"4.1
rice_brand":"Xiaomi","device_manufacturer":"Xiaomi","device_model":"Redmi Note 3","carrier":"vodafone GR","country":"GR","language":"e
15-883b-ec8d3693e8d1","sequence_number":227,"library":{"name":"amplitude-android","version":"2.7.1"},"api_properties":{"location":{"lat":4
D":"4bff420f-2285-408b-a5e8-f6b06cb8c892","limit_ad_tracking":false,"gps_enabled":true},"event_properties":{},"user_properties":{"$set":{"H
vent={"event_type":"$identify","timestamp":1485361687167,"user_id":"6ABE83EDDD03B1B4B5F06A5A471D5E07","device_id":"3190d47e-c1
5361562247,"version_name":"4.10","os_name":"android","os_version":"5.0.2","device_brand":"Xiaomi","device_manufacturer":"Xiaomi","devi
R","country":"GR","language":"el","platform":"Android","uuid":"feb725ae-2ffc-4222-a806-178adcf0b5a2","sequence_number":228,"library":{"na
roperties":{"location":{"lat":40.8557,"lng":25.878490000000003},"androidADID":"4bff420f-2285-408b-a5e8-f6b06cb8c892","limit_ad_trackin

Εικόνα 4.44: Απεικόνιση των SQL statements που εκτελούνται κατά την λειτουργία της εφαρμογής YikYak, με μπλε χρώμα βλέπουμε τις gps συντεταγμένες του κινητού που χρησιμοποιήθηκε για την σύνδεση.

Αν τοποθετήσουμε στο Google map τις gps συντεταγμένες που καταφέραμε να ανακτήσουμε από την εφαρμογή, θα μας δείξουν την τοποθεσία του κινητού ό-ταν ο χρήστης χρησιμοποίησε την εφαρμογή YikYak. Όπως είναι ορατό από την παρακάτω εικόνα, η σύνδεση πραγματοποιήθηκε από την πόλη της Αλεξαν-δρούπολης.



Εικόνα 4.45: Εντοπισμός των gps συντεταγμένων που βρέθηκαν μέσω του Inspeck-age, οι συντεταγμένες τοποθετήθηκαν στο Google maps για επιβεβαίωση και δεί-χνουν την τοποθεσία της σύνδεσης.

Τα συμπεράσματα λοιπόν είναι τα εξής:

Η εν λόγω εφαρμογή αντλεί τις γεωγραφικές συντεταγμένες των χρηστών καθώς αυτό το στοιχείο αποτελεί πολύ σημαντικό για την λειτουργία της. Επίσης αντλεί και το αναγνωριστικό GAID πιθανώς για επικοινωνία με τρίτου μέρους εξυπηρετητές.

Με βάση τα συμπεράσματα αυτά μπορούμε να πούμε ότι, κατ' αναλογία με την εφαρμογή Whisper, η άντληση ενός αναγνωριστικού του τηλεφώνου (του GAID) αλλά και η άντληση των γεωγραφικών συντεταγμένων ενός χρήστη την στιγμή της δημοσίευσης ενός μηνύματος μπορούν να οδηγήσουν στην παύση της ανωμυμοποίησης που προσφέρει το δίκτυο. Συνεπώς, και εδώ πρόκειται για ψευδωνυμοποίηση και όχι για ανωνυμοποίηση.

4.3 Πίνακας ευρημάτων

Στην ενότητα αυτή παρουσιάζονται συγκεντρωτικά, σε μορφή συνολικού πίνακα, τα ευρήματα της ανάλυσης των ανώνυμων εφαρμογών.

Δεδομένα Ανώνυμων εφαρμογών		
Whisper		
	GAID(Google Advertising Id)	4bff420f-2285-408b-a5e8-f6b06cb8c892
	Γεωγραφικές Συντεταγμένες	latitude:40.85136;longtitude:25.876919
	Μοντέλο Κινητού	Redmi Note 3
	Κατασκευαστής	Xiaomi
	Φορέας	vodafone
	Χώρα	GR
	Γλώσσα	GR
	Περιεχόμενο Δημοσιεύσεων	Έχει ανακτηθεί
YikYak	Λειτουργικό	Android
	GAID(Google Advertising Id)	4bff420f-2285-408b-a5e8-f6b06cb8c892
	Γεωγραφικές Συντεταγμένες	latitude:40.8557;longtitude:25.878490000000003
	Μοντέλο Κινητού	Redmi Note 3
	Κατασκευαστής	Xiaomi
	Φορέας	vodafone
	Λειτουργικό	Android
Anomo		
	GAID(Google Advertising Id)	4bff420f-2285-408b-a5e8-f6b06cb8c892
	Όνομα Χρήστη στο Facebook	Basilis Bill
	Email Σύνδεσης	basixatz@hotmail.com
	Φορέας	vodafone
	Μοντέλο Κινητού	Redmi Note 3
	Κατασκευαστής	Xiaomi
	Περιεχόμενο Δημοσιεύσεων	Έχει ανακτηθεί
Candid		
	GAID(Google Advertising Id)	4bff420f-2285-408b-a5e8-f6b06cb8c892
	Όνομα Χρήστη στο Facebook	Basilis Bill
SocialNumber		
	Email Σύνδεσης	basixatz@hotmail.com
	Όνομα χρήστη και κωδικός πρόσβασης	Έχουν ανακτηθεί
	Περιεχόμενο Δημοσιεύσεων	Έχει ανακτηθεί

Εικόνα 4.46: Πίνακας ευρημάτων που προέκυψαν από την ανάλυση των πέντε ανώνυμων εφαρμογών με την χρήση των προγραμμάτων Burp Suite και Inspeckage.

Κεφάλαιο 5

Σύνδεση ανώνυμων κοινωνικών δικτύων με επώνυμα δίκτυα

Όπως είδαμε στο προηγούμενο κεφάλαιο, τέσσερα από τα πέντε ανώνυμα κοινωνικά δίκτυα που εξετάσαμε (όλα πλην του SocialNumber[1]) συλλέγουν το GAID. Είδαμε επίσης ότι τα ανώνυμα κοινωνικά δίκτυα Whisper και YikYak χρησιμοποιούν για την λειτουργία τους τις gps συντεταγμένες των χρηστών τους, προκειμένου να παρέχουν την υπηρεσία του να προτείνουν στους χρήστες τους άλλους χρήστες που βρίσκονται γεωγραφικά σε κοντινή απόσταση.

Τα δύο αυτά ευρήματα της λειτουργίας των ανώνυμων κοινωνικών δικτύων - δηλαδή τόσο η άντληση ενός μοναδικού identifier όπως είναι το GAID όσο και η άντληση των gps συντεταγμένων των χρηστών – οδηγούν στο συμπέρασμα ότι οι εφαρμογές επεξεργάζονται προσωπικά και όχι ανώνυμα δεδομένα, έστω και σε ψευδωνυμοποιημένη μορφή. Στο παρόν κεφάλαιο, για να αποτιμήσουμε το βαθμό στον οποίο είναι εύκολο από την εν λόγω ψευδωνυμοποίηση να οδηγηθούμε σε ταυτοποίηση των χρηστών, θα διερευνήσουμε το αν τα δεδομένα αυτά συλλέγονται και σε επώνυμα κοινωνικά δίκτυα αλλά και κατά την απλή πλοήγηση με προγράμματα φυλλομετρητή (browsers).

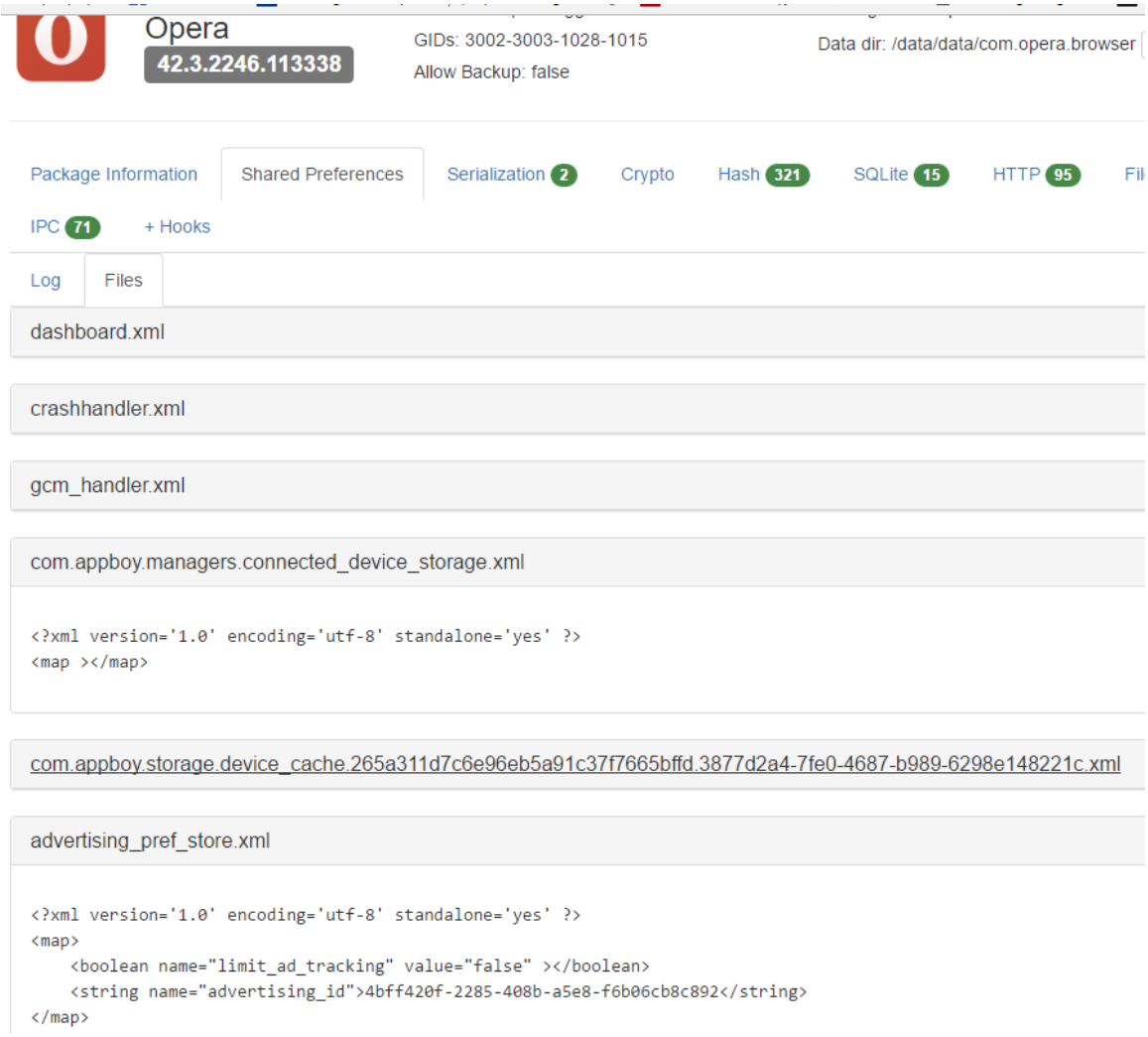
[1]Το SocialNumber βέβαια εμφανίζει, όπως είδαμε, άλλα σπουδαιότερα προβλήματα ως προς την τήρηση της ανωνυμίας των χρηστών του

Για τον λόγο αυτό στην ενότητα 5.1 θα γίνει μια ανάλυση των δεδομένων που αντλούν οι διάφοροι browsers όταν ένας χρήστης τους χρησιμοποιεί για την περιήγησή του στο διαδίκτυο. Η ανάλυση αυτή θα γίνει στον Chrome, στον Mozilla αλλά και στον Opera, ως οι πιο δημοφιλείς browsers. Στην ενότητα 5.2 θα γίνει μια ανάλυση μερικών επώνυμων κοινωνικών δικτύων: συγκεκριμένα, με χρήση δυναμικής ανάλυσης θα εξετάσουμε τα δεδομένα που αντλούνται από τις εφαρμογές Twitter Instagram αλλά και Facebook. Στην ενότητα 5.3 θα καταδείξουμε την πιθανότητα ένας χρήστης να αναγνωριστεί συνδυάζοντας την άντληση των gps συντεταγμένων του από τα ανώνυμα κοινωνικά δίκτυα σε συνδυασμό με data mining από την εφαρμογή Twitter.

5.1 Ανάλυση δεδομένων φυλλομετρητών

Οι φυλλομετρητές ή προγράμματα πλοήγησης (browsers) είναι προγράμματα που δίνουν την δυνατότητα σε ένα χρήστη να περιηγηθεί στο διαδίκτυο. Κατά την περιήγηση αυτή ο κάθε ένας αντλεί κάποια δεδομένα από το κινητό του χρήστη με σκοπό να του παρέχει όσο το δυνατόν πιο ποιοτικές υπηρεσίες.

Σε τρεις από τους πιο γνωστούς φυλλομετρητές, τον Chrome, τον Mozilla και τον Opera, αφού πρώτα τους εγκαταστήσαμε στο περιβάλλον εργασίας μας, εκτελέσαμε δυναμική ανάλυση με την βοήθεια του Inspeckage έτσι ώστε να εξετάσουμε τα δεδομένα που επεξεργάζονται και τον τρόπο με τον οποίο λειτουργούν. Χαρακτηριστικό είναι ότι από τους τρεις browser Chrome, Mozilla και Opera, καταφέραμε να συλλέξουμε το GAID μόνο από τον Opera, ενώ οι άλλοι δυο δείχνουν να μην το αντλούν κατά την περιήγηση του χρήστη. Η επόμενη εικόνα δείχνει το GAID του κινητού που αντλείται και όπως είναι φανερό ο identifier αυτός είναι ο ίδιος με αυτόν που είχε αντληθεί και από τα ανώνυμα δίκτυα.



Εικόνα 5.1 :Ανάλυση με το Inspeckage του browser Opera όπου στο advertising _pref_store.xml μπορούμε να δούμε να αποθηκεύετε το advertising id του κινητού.

Το ενδιαφέρον στοιχείο είναι ότι η περιήγηση ενός χρήστη μέσω ενός browser μπορεί να γίνει είτε μέσω του http πρωτοκόλλου είτε μέσω του https με την διαφορά των δυο να βρίσκεται στο γεγονός ότι η επικοινωνία μέσω https είναι κρυπτογραφημένη ενώ μέσω http όχι. Το γεγονός αυτό σημαίνει ότι σε περίπτωση που κάποιος χρήστης χρησιμοποιεί μια ανώνυμη εφαρμογή και χρησιμοποιεί επίσης και τον browser Opera για την περιήγησή του στο διαδίκτυο αυτός θα μπορούσε να οδηγήσει στην αναγνώριση του καθώς και οι δύο εφαρμογές αντλούν το ίδιο Identifier από το κινητό του χρήστη. Πέρα από αυτό η ανάλυση του Opera μας δείχνει ότι ο συγκεκριμένος browser όχι μόνο αντλεί ένα ανα-

γνωριστικό του κινητού του χρήστη αλλά το αποστέλλει και προς τους διάφορους web servers που επισκεπτόμαστε καθώς με αυτό τον τρόπο μπορεί να παρουσιάσει στοχευμένο περιεχόμενο περιήγησης στον χρήστη.

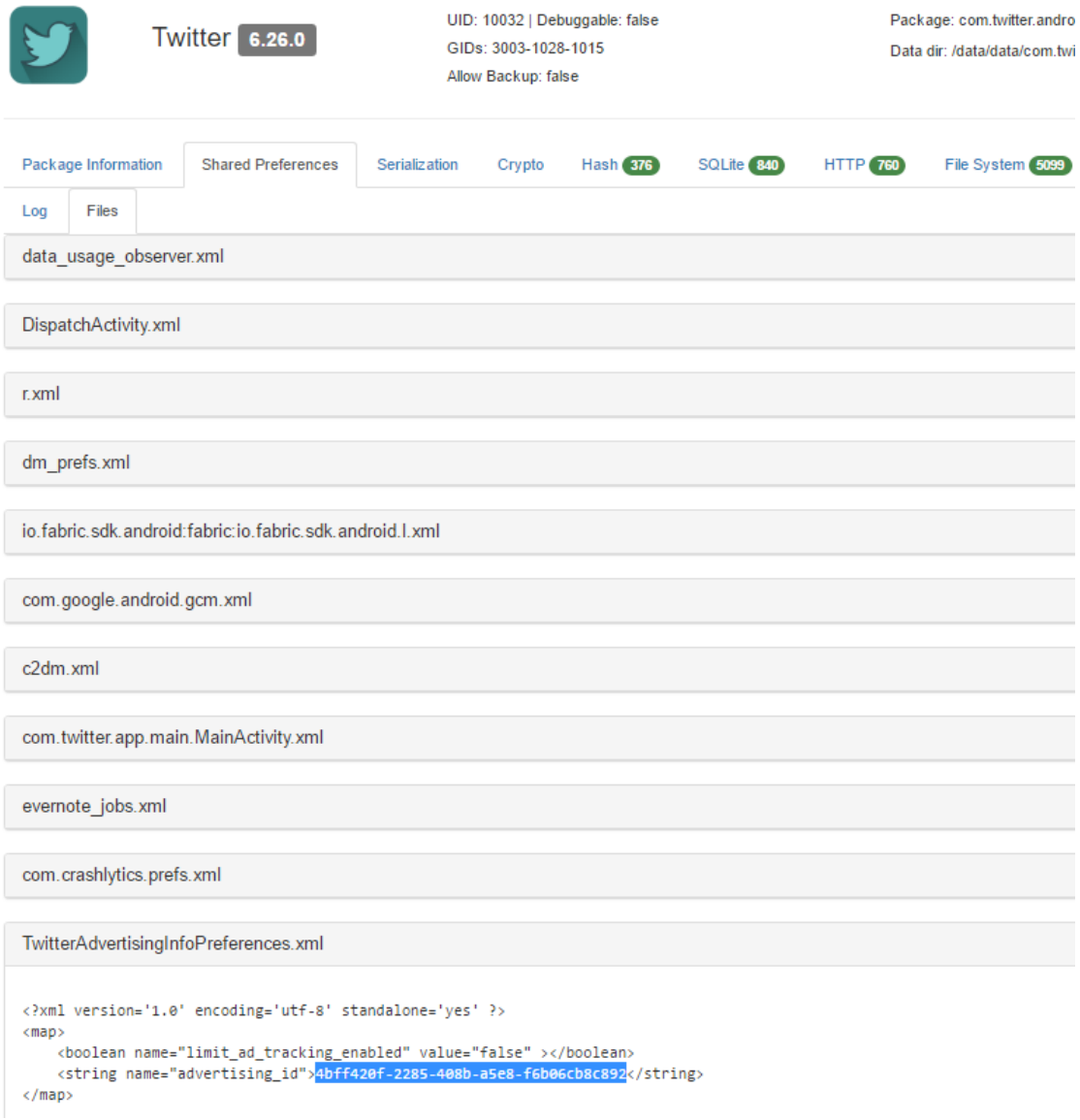
5.2 Επώνυμα κοινωνικά δίκτυα

Πέρα από τα προγράμματα πλοήγησης, με την χρήση του Inspeckage θα αναλύσουμε και επώνυμα κοινωνικά δίκτυα όπως είναι το Twitter το Instagram και το Facebook. Ο σκοπός είναι να δούμε τα δεδομένα που αντλούν οι συγκεκριμένες εφαρμογές από τα κινητά των χρηστών και αν υπό περίπτωση τα δεδομένα αυτά μπορούν να συνδυαστούν με τα δεδομένα από τα ανώνυμα κοινωνικά δίκτυα.

5.2.1 Twitter

Το Twitter είναι ένα ελεύθερο κοινωνικό δίκτυο και μια micro blogging υπηρεσία η οποία επιτρέπει στα εγγεγραμμένα μέλη της να δημοσιεύουν αλλά και να διαβάζουν σύντομα μηνύματα (tweets) άλλων χρηστών. Το Twitter μπορεί να χαρακτηριστεί σαν ένα δίκτυο ενημέρωσης πραγματικού χρόνου.

Μέσω του Inspeckage επιλέγουμε το Twitter και από το γραφικό περιβάλλον της εφαρμογής μπορούμε να δούμε τα δεδομένα που αντλεί η εφαρμογή. Από αυτά μπορούμε να δούμε μέσα από την καρτέλα Shared Preferences ότι το Twitter αποθηκεύει το GAID του κινητού μέσω του xml TwitterAdvertisingInfoPreferences.xml. Η επόμενη εικόνα μας δείχνει την ανάλυση με την χρήση του Inspeckage του Twitter ενώ στην εικόνα 5.3 μπορούμε να δούμε τόσο την αποθήκευση του GAID από το κινητό του χρήστη όσο και το όνομα χρήστη στην εφαρμογή Twitter.



Εικόνα 5.2: Ανάλυση με το Inspeckage της εφαρμογής Twitter όπου κατά την εκτέλεση της αποθηκεύετε στο xml με τίτλο TwitterAdvertisingInfoPreferences.xml το Google Advertising Id του κινητού.

TwitterAdvertisingInfoPreferences.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="limit_ad_tracking_enabled" value="false" ></boolean>
    <string name="advertising_id">4bff420f-2285-408b-a5e8-f6b06cb8c892</string>
</map>
```

com.twitter.android_preferences.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <long name="log_last_flush_request" value="1485707880143" ></long>
    <string name="client_uuid">e2b08d32-99b8-4abf-9c6c-e0adaf7e4b1e</string>
    <long name="become_inactive_timestamp" value="1485707882215" ></long>
    <boolean name="phone_verified" value="true" ></boolean>
    <string name="current_account">BillChatzistef1</string>
    <long name="pref_ref_src_date" value="1481476257124" ></long>
```

Εικόνα 5.3: Ανάλυση με το Inspeckage της εφαρμογής Twitter όπου διακρίνουμε την αποθήκευση τόσο του ονόματος χρήστη στην εφαρμογή όσο και του advertising id.

5.2.2 Instagram

Το Instagram είναι μια δωρεάν εφαρμογή διαμοιρασμού φωτογραφιών και μέσο κοινωνικής δικτύωσης. Το Instagram επιτρέπει στους χρήστες του να "ανεβάσουν", επεξεργαστούν, και να μοιραστούν φωτογραφίες με άλλα μέλη και άλλα δίκτυα όπως το Facebook, το Twitter, το Tumblr και το Flickr.

Εκτελώντας τοInspeckage θα επιλέξουμε την εφαρμογή Instagram όπου μέσω του γραφικού περιβάλλοντος θα δούμε τις κλήσεις συστήματος, τους πόρους και τα δεδομένα που αντλεί κατά την εκτέλεσή της. Αυτό που μπορούμε να δούμε από την επόμενη εικόνα είναι ότι και αυτή η εφαρμογή αποθηκεύει το GAID του κινητού μέσω του xml με ονομασία com.Instagram.android_preferences.xml

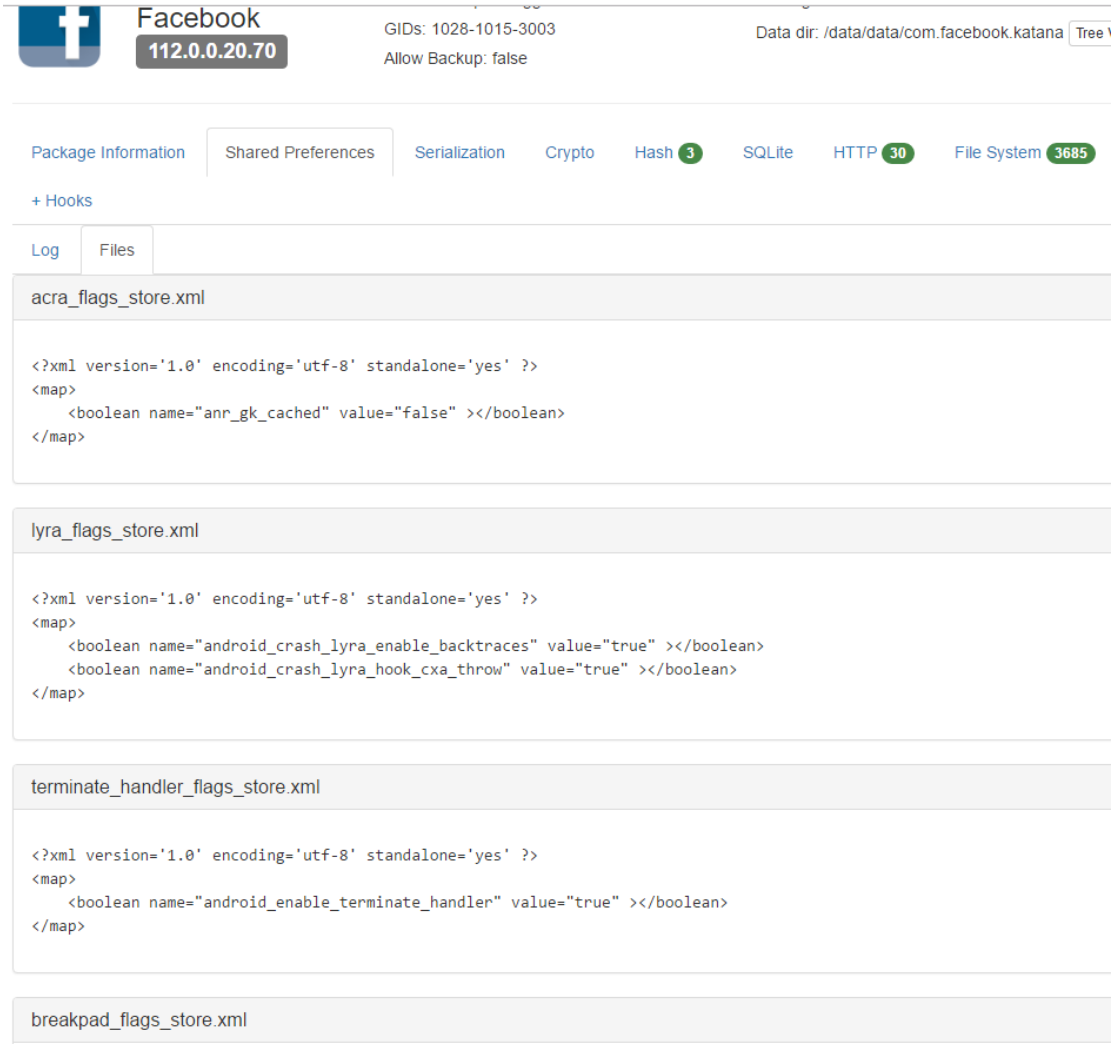
com.instagram.android_preferences.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="google_ad_id">4bff420f-2285-408b-a5e8-f6b06cb8c892</string>
    <boolean name="opt_out_ads" value="false" ></boolean>
    <string name="current">{&quot;id&quot;:&quot;1495233222&quot;,&quot;biography&quot;:&quot;&quot;,&quot;blocking&
    <boolean name="has_seen_direct_story_from_instagram_nux" value="true" ></boolean>
    <boolean name="has_seen_layout_button_nux" value="true" ></boolean>
    <boolean name="bgsync_launch_next_online" value="false" ></boolean>
    <string name="user_access_map">[{&quot;user_info&quot;:{&quot;id&quot;:&quot;1495233222&quot;,&quot;biography&qu
    <long name="push_reg_dateandroid_mqtt" value="1482156936901" ></long>
    <int name="used_double_tap_hint_impressions" value="1" ></int>
    <boolean name="show_tos" value="false" ></boolean>
    <boolean name="used_double_tap" value="true" ></boolean>
    <boolean name="com.facebook.sdk.appInstallEvent" value="true" ></boolean>
</map>
```

Εικόνα 5.4: Ανάλυση της εφαρμογής Instagram με το Inspeckage όπου στο xml με τίτλο com.instagram.android_preferences.xml αποθηκεύετε το Google Advertising Id του κινητού.

5.2.3 Facebook

Το Facebook αποτελεί το πιο δημοφιλές μέσο κοινωνικής δικτύωσης, με την χρήση του οποίου ένας χρήστης μπορεί να εκτελέσει πληθώρα ενεργειών: αυτές περιλαμβάνουν συζητήσεις με γραπτά μηνύματα, βιντεοκλήσεις, παιχνίδια και άλλα. Πέρα όμως από τις δυνατότητες που προσφέρει η εφαρμογή, μέσω δυναμικής ανάλυσης θα εξετάσουμε τα δεδομένα που αντλεί από το κινητό ενός χρήστη. Όπως φαίνεται και στην παρακάτω εικόνα, το Facebook δεν αντλεί το GAIDτου κινητού ούτε και κάποιο άλλο identifier.



Εικόνα 5.5 : Ανάλυση της εφαρμογής Facebook με την χρήση του Inspeckage.

5.3 Αποτίμηση

Πολλές εφαρμογές κατά την εγκατάστασή τους αιτούνται από τον χρήστη το δικαίωμα να μπορούν να αναγνωρίσουν την γεωγραφική του θέση. Το χαρακτηριστικό αυτό το είδαμε και στο κεφάλαιο 4 κατά την ανάλυση των ανώνυμων εφαρμογών αλλά συναντάται επίσης και σε πλήθος άλλων εφαρμογών. Ο λόγος που ζητάται αυτό είναι ότι δίνει τη δυνατότητα στους δημιουργούς της εκάστοτε εφαρμογής να παρέχουν στους χρήστες τους

υπηρεσίες στοχευμένες σύμφωνα με τα ενδιαφέροντα και τις συνήθειες κάθε γεωγραφικής περιοχής, ενώ επίσης πολλές από αυτές τις εφαρμογές χρησιμοποιούν αυτό το χαρακτηριστικό έτσι ώστε να βελτιώνουν την εμπειρία του χρήστη καθώς δημιουργείται μια αίσθηση πιο οικεία κατά την χρησιμοποίηση μιας εφαρμογής αν ο χρήστης βλέπει ότι χρησιμοποιείται επίσης από άτομα που βρίσκονται γεωγραφικά κοντά του.

Από την άλλη όμως, όπως καταδείξαμε στο κεφάλαιο 4, η γνώση της γεωγραφικής θέσης ενός χρήστη μπορεί να έχει αρνητικές συνέπειες για τον ίδιο καθώς σε περίπτωση που θέλει να διατηρήσει την ανωνυμία υπάρχουν τρόποι με τους οποίους η γνώση της γεωγραφικής του θέσης θα μπορούσε να παύσει την ανωμυμοποίησή του. Τέτοιο παράδειγμα μπορούμε να αναζητήσουμε στο δίκτυο Twitter το οποίο μέσω του API του δίνει την δυνατότητα σε όποιον το επιθυμεί να αντλήσει δεδομένα από το δίκτυό του μέσω τεχνικών εξόρυξης δεδομένων (“data mining”). Σε ένα σενάριο λοιπόν που κάποιος χρήστης θα αναρτούσε δημοσιεύσεις στο δίκτυο Twitter και ταυτόχρονα θα χρησιμοποιούσε κάποιο από τα ανώνυμα δίκτυα που αναλύσαμε σε προηγούμενο κεφάλαιο, ο συνδυασμός των γεωγραφικών του θέσεων όπως συλλέγονται από την εφαρμογή του ανώνυμου κοινωνικού δικτύου θα μπορούσε να καταδείξει την ταυτότητά του και να παύσει την ανωμυμοποίηση του (ιδίως δε αν αυτό επαναληφθεί περισσότερες φορές για τις συντεταγμένες του ίδιου GAID): συγκεκριμένα, το ανώνυμο δίκτυο γνωρίζει τις συντεταγμένες του χρήστη του και μπορεί να αναζητήσει να δει αν κάποιος χρήστης του Twitter, μέσω των δημόσια προσβάσιμων δεδομένων, βρίσκεται στις ίδιες συντεταγμένες σε κοντινή χρονική στιγμή – οπότε και, σε καταφατική περίπτωση, υπάρχει μία πιθανότητα να πρόκειται για τον ίδιο χρήστη. Το σενάριο αυτό, αν και βασίζεται στην υπόθεση χρησιμοποίησης διαφορετικών δικτύων από το ίδιο κινητό, εν τούτοις καταδεικνύει τη σημασία που έχει το συγκεκριμένο χαρακτηριστικό – εξάλλου, είναι συνήθης τακτική των χρηστών να είναι ταυτόχρονα συνδεδεμένοι σε πλέον του ενός δίκτυα.

Κεφάλαιο 6

Επίλογος

Η παρούσα μεταπτυχιακή διατριβή ασχολήθηκε με το θέμα της αποτίμησης της ανωμυμοποίησης που επιτυγχάνουν τα ανώνυμα κοινωνικά δίκτυα. Παρουσίασε τις έννοιες των προσωπικών και των ανώνυμων δεδομένων καθώς επίσης και τον τρόπο λειτουργίας μιας εφαρμογής στο λειτουργικό σύστημα Android. Τα ανωτέρω αποτελούν τη βάση για την υλοποίηση του κατάλληλου περιβάλλοντος εργασίας για την έρευνά μας. Σε αυτήν την κατεύθυνση, η διατριβή εξέτασε τη λειτουργία πέντε δημοφιλών ανώνυμων κοινωνικών δικτύων και προσπάθησε να αναλύσει τα δεδομένα που αντλούνται από ένα κινητό τηλέφωνο με λειτουργικό σύστημα Android που χρησιμοποιεί μια από αυτές τις εφαρμογές.

Η ανάλυση των δεδομένων μας έδειξε ότι αν και οι εν λόγω εφαρμογές λαμβάνουν κάποια σημαντικά μέτρα για την προστασία της ιδιωτικότητας των χρηστών, τα δεδομένα που συλλέγουν δεν μπορούν να θεωρηθούν ανώνυμα καθώς υπάρχουν τρόποι με τους οποίους τα δεδομένα αυτά θα μπορούσαν να καταδείξουν την πραγματική ταυτότητα κάποιου χρήστη. Το εύρημα αυτό επιβεβαιώνεται από την άντληση τόσο του αναγνωριστικού GAID το οποίο βρέθηκε να αντλείται στις τέσσερις από τις πέντε εφαρμογές όσο και στο γεγονός ότι με το περιβάλλον δοκιμών που δημιουργήσαμε είμασταν σε θέση στο ανώνυμο δίκτυο Whisper να αντλούμε τόσο το περιεχόμενο των δημοσιεύσεων ενός χρήστη όσο και την ακριβή του γεωγραφική θέση. Στη δε περίπτωση της εφαρμογής Social Number – η μόνη για την οποία δεν φαίνεται να συλλέγεται το GAID – η απουσία ανωνυμοποίησης είναι ακόμα πιο έκδηλη αφού συλλέγεται ηλεκτρονική διεύθυνση του χρήστη.

Περαιτέρω, για δύο περιπτώσεις (SocialNumber και Anomo) καταδείξαμε ότι δεν λαμβάνονται τα κατάλληλα μέτρα ασφάλειας για την αντιμετώπιση επιθέσεων τύπου «man-in-the-middle» οι οποίες μπορούν να οδηγήσουν σε υποκλοπή της μεταδιδόμενης πληροφορίας και, άρα, σε παραβίαση της εμπιστευτικότητας της μετάδοσης.

Τα ευρήματα αυτά δείχνουν ότι η ανωμυμοποίηση των δεδομένων είναι μια πολυσύνθετη διαδικασία και δεν είναι εύκολο να επιτευχθεί – απόρροια του γεγονότος ότι πολλοί είναι αυτοί που εκλαμβάνουν, λανθασμένα, την ψευδωνυμοποίηση ως ανωνυμοποίηση. Ως εκ τούτου, η χρήση αυτών των δικτύων δεν μπορεί να θεωρηθεί ως ανώνυμη αλλά μάλλον ως ψευδώνυμη, δηλαδή είναι δύσκολο, αλλά σίγουρα όχι αδύνατο, να αναγνωριστεί ο χρήστης τους. Με άλλα λόγια, το νομικό πλαίσιο για την προστασία προσωπικών δεδομένων έχει εφαρμογή στις συγκεκριμένες περιπτώσεις και αυτό είναι κάτι που θα πρέπει να γνωρίζουν τόσο οι πάροχοι των εν λόγω υπηρεσιών όσο και οι χρήστες. Το γεγονός ότι πολλοί χρήστες τα χρησιμοποιούν θεωρώντας ως δεδομένο ότι είναι πλήρως ανώνυμοι καθιστά τα εν λόγω κοινωνικά δίκτυα ως ένα μη απόλυτα ασφαλές περιβάλλον όσον αφορά την προστασία των προσωπικών δεδομένων των χρηστών.

Εν κατακλείδι, η παρούσα εργασία αναδεικνύει ένα εγγενές πρόβλημα που αντιμετωπίζει κάθε εφαρμογή η οποία εκλαμβάνεται ως ανώνυμη αλλά στην ουσία δεν είναι. Πέραν της σαφούς διαφοροποίησης που πρέπει να γίνεται μεταξύ ανώνυμων και ψευδώνυμων δεδομένων, είναι σημαντικό να διερευνηθούν οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technologies) που μπορούν να ενσωματωθούν σε τέτοιου τύπου εφαρμογές, προκειμένου να καθίσταται, αν όχι αδύνατη, εξαιρετικά δυσχερής η αναγνώριση της ταυτότητας των χρηστών αυτών. Εξάλλου, μία τέτοια προσέγγιση είναι σε άμεση συνάφεια με την αρχή της «προστασίας των δεδομένων κατά το σχεδιασμό» (data protection by design principle), η οποία ρητώς προβλέπεται και στο νέο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων και, ως εκ τούτου, μελλοντική έρευνα θα πρέπει να στραφεί προς σε αυτήν την κατεύθυνση.

Βιβλιογραφία

[01] Android Manifest http://gurushya.com/android-manifest/ [Πρόσβαση : 25. Μαρτίου. 2017]

[02] Android Versions http://socialcompare.com/en/comparison/android-versions-comparison [Πρόσβαση: 25. Μαρτίου. 2017]

[03] Denis Andzakovic – Security-Assessment.com. Bypassing SSL Pinning on Android via Reverse Engineering, 15 May 2014 [Πρόσβαση: 10. Φεβρουαρίου. 2017]

[04] Burp Suite https://portswigger.net/burp/ [Πρόσβαση: 14. Νοεμβρίου. 2016]

[05] Bypassing-ssl-pinning-in-android-applications https://serializethoughts.com/2016/08/18/bypassing-ssl-pinning-in-android-applications/ [Πρόσβαση: 20. Νοεμβρίου. 2016]

[06] Cert Vulnerabilities Notes Database http://www.kb.cert.org/vuls/id/582497 [Πρόσβαση: 31. Μαρτίου. 2017]

[07] D. Correa, L. Araújo Silva, M. Mondal, F. Benevenuto και K. Gummad, «The Many Shades of Anonymity: Characterizing Anonymous Social Media Content,» ICWSM, 2015. [Πρόσβαση: 10.Νοεμβρίου. 2016]

[08] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal

data and on the free movement of such data. Official Journal L. 1995;281:31–50 [Πρόσβαση :2. Νοεμβρίου. 2016]

[09] DroidBox (2014) https://github.com/pjlantz/droidbox/releases [Πρόσβαση: 20. Ιανουαρίου. 2017]

[10] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick D. McDaniel, Anmol Sheth, «TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones» Commun. ACM 57(3): 99-106 (2014)

[11] Growth of available apps through Google Play Store http://www.businessofapps.com/app-store-statistics-roundup/ [Πρόσβαση: 25. Μαρτίου. 2017]

[12] Mohd. Ishrat1, Manish Saxena2 and Dr. Mohd. Alamgir3, «Comparison of Static and Dynamic Analysis for Runtime Monitoring» Mohd.Ishrat et al , International Journal of Computer Science & Communication Networks,Vol 2(5), 615-617

[13] Martina Lindorfer, Matthias Neugschwandtner, Lukas Weichselbaum, Yanick Fratantonio ,Victor van der Veeny, Christian Platzer, « ANDRUBIS - 1,000,000 Apps Later: A View on Current Android Malware Behaviors » Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS) 2014/9/11

[14] Mobile Device Identifiers https://www.aerserv.com/mobile-device-identifiers/ [Πρόσβαση: 11.Νοεμβρίου. 2016]

[15] Veelasha Moonsamy and Lynn Batten. Mitigating Man-in-The-Middle Attacks on Smartphones - a Discussion of SSL Pinning and DNSSec, Proceedings of the 12th Australian Information Security Management Conference (AISM), pages 5-13, Perth, Australia, [Πρόσβαση: Δεκέμβριος. 2014]

[16] Pushpendra Kumar Pateriya and Srijith S Kumar. Analysis on Man in the Middle Attack on SSL. International Journal of Computer Applications in Technology.[Πρόσβαση Μάιος 2012]

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)Official Journal L. 2016;119(1). [Πρόσβαση : 5 Νοεμβρίου 2016]

[18] Aijaz Ahmad Sheikh, Prince Tehseen Ganai, Nisar Ahmad Malik & Khursheed Ahmad Dar «Smartphone: Android Vs IOS» The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 4, September-October 2013

[19] Sooel Son, Daehyeok Kim, Vitaly Shmatikov « What Mobile Ads Know About Mobile Users» NDSS 2016: San Diego, California, USA, Session 6: Privacy in Mobile

[20] TraceDroid (2013) http://tracedroid.few.vu.nl/ [Πρόσβαση: 21. Ιανουαρίου. 2017]

[21] Αργύρης Τζικόπουλος, Ηλεκτρονικά μέσα κοινωνικής δικτύωσης (social media), [Πρόσβαση: 10. Νοεμβρίου. 2016]

[22] Xposed Framework http://repo.xposed.info/module/de.robv.android.xposed.installer [Πρόσβαση: 17. Νοεμβρίου. 2016].