Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Μελέτη Εφαρμογών Μηνυμάτων και Τηλεδιασκέψεων ως Προς την Προστασία Προσωπικών Δεδομένων

Γιώργος Αχιλλέως

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια*

Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Μελέτη Εφαρμογών Μηνυμάτων και Τηλεδιασκέψεων ως Προς την Προστασία Προσωπικών Δεδομένων

Γιώργος Αχιλλέως

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2022

Περίληψη

Το ξέσπασμα της πανδημίας του COVID-19 στα τέλη του 2019, ο φόβος και οι αναπόφευκτες απαγορεύσεις κυκλοφορίας σε πολλές χώρες του πλανήτη ώθησαν τους ανθρώπους στο να βρούνε εναλλακτικούς τρόπους επικοινωνίας και εργασίας μένοντας σπίτι. Τη λύση έδωσε η τεχνολογία και οι εφαρμογές τηλεπικοινωνιών με τη χρήση τους να αυξάνεται κατακόρυφα. Αυτή η ραγδαία αύξηση χρηστών οδήγησε στα εύλογα ερωτήματα εκ μέρους των χρηστών για την ιδιωτικότητα και την ασφάλεια των προσωπικών δεδομένων τους με τη χρήση των συγκεκριμένων εφαρμογών.

Στόχος της παρούσας μεταπτυχιακής διατριβής είναι η διερεύνηση διαφόρων δημοφιλών εφαρμογών τηλεπικοινωνίας / συνομιλιών ως προς τα θέματα ασφάλειας και ιδιωτικότητας των δεδομένων των χρηστών τους. Στο πλαίσιο αυτό, εξετάζεται και το κατά πόσο υπάρχουν διαρροές προσωπικών δεδομένων σε τρίτους λόγω χρήσης διαφόρων βιβλιοθηκών τρίτων μελών (ιχνηλάτες – trackers) για διαφημιστικούς ή άλλους σκοπούς χωρίς τη συγκατάθεση των χρηστών. Με βάση το ισχύον νομικό στην Ευρωπαϊκή Ένωση όσο αφορά τα προσωπικά δεδομένα υποχρεούνται οι εφαρμογές να παρέχουν διαφάνεια και ασφάλεια κατά τη συλλογή και επεξεργασία προσωπικών δεδομένων των χρηστών.

Για την επίτευξη των στόχων οι οποίοι τέθηκαν δημιουργήθηκε κατάλληλο περιβάλλον δοκιμών με διάφορα εργαλεία τα οποία προσφέρουν μεταξύ άλλων ανάλυση της κίνησης δικτύου των εφαρμογών, ενώ επίσης έγινε και ανάλυση των πολιτικών ιδιωτικότητας. Μέσω του περιβάλλοντος οι εφαρμογές τηλεπικοινωνιών / συνομιλιών αναλύθηκαν σε πραγματικό χρόνο ελέγχοντας εάν ισχύουν τα όσα αναφέρονται στις πολιτικές ασφάλειάς τους και για το κατά πόσο υπάρχει ιδιωτικότητα και ασφάλεια στα προσωπικά δεδομένα των χρηστών.

Τα αποτελέσματα δίνουν μία ικανοποιητική πρώτη αποτίμηση για την ασφάλεια των προσωπικών δεδομένων των χρηστών χωρίς να διαφαίνεται κάποια κρυφή διαρροή δεδομένων προς τρίτα μέλη. Ωστόσο διαφαίνονται κάποιες επεξεργασίες δεδομένων για τις οποίες, αν και θα μπορούσαν να είναι δικαιολογημένες, δεν προκύπτει με σαφήνεια για ποιους ακριβώς σκοπούς πραγματοποιούνται. Σε κάθε περίπτωση, λόγω των εγγενών περιορισμών που υπάρχουν αναφορικά με τα ευρήματα που καταδεικνύουν τα εργαλεία ανάλυσης, η παρούσα διατριβή καταδεικνύει την ανάγκη περαιτέρω έρευνας, αφού δεν είμαστε σε θέση να αποκλείσουμε εντελώς το ενδεχόμενο να γίνεται κάποια διαρροή δεδομένων από τις εφαρμογές συνομιλιών / τηλεπικοινωνιών ερήμην των χρηστών.

Summary

The outbreak of the COVID-19 pandemic in late 2019, fear and the inevitable traffic bans in many countries around the world pushed people to find alternative ways to communicate and work while staying home. The solution was provided by the technology and applications of telecommunications with their use increase vertically. This rapid increase in users has led to reasonable questions from users about the privacy and security of their personal data through the use of these applications.

The aim of this master's thesis is to investigate various popular telecommunications / chat applications regarding the security and privacy issues of their users' data. In addition, it examines whether there are leaks of personal data in various data in various third parties due to the use of third-party libraries (trackers) for advertising or other purposes without the consent of users. According to the current legal in the European Union regarding the personal data, the applications are obliged to provide transparency and security in the collection and processing of personal data of the users.

In order to achieve the research goals, an appropriate test environment was developed with various tools that offer, among other things, analysis of the network traffic of the applications, whereas analysis of their privacy policies has been also performed. Through the environment, telecommunications / chat applications were analyzed in real time, checking whether what is stated in their security policies is indeed the case, as well as whether there exist privacy and security issues. .

The results provide a satisfactory first evaluation for the security of users' personal data, without revealing any hidden data leakage to third parties. However, there exist cases for which the privacy policies are not very clear, whereas some detected personal data processes, although they seem to be logical, they do not have a clearly defined purpose. In any case, due to the inherent limitations on the effectiveness of the tools used, this thesis illustrated the importance of further research in the field, since we are not able to completely rule out the possibility of data leakage from chat / telecommunications applications without the users being aware of it.

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Κωνσταντίνο Λιμνιώτη για την αμέριστη βοήθεια και καθοδήγηση του στην εκπόνηση της παρούσας μεταπτυχιακής διατριβής. Οι συμβουλές και τα σχόλια του έπαιξαν καταλυτικό ρόλο στην επιτυχής μελέτη και συγγραφή της παρούσας εργασίας.

Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου για τη στήριξη και υπομονή τους καθ' όλη τη διάρκεια των σπουδών μου και κυρίως κατά το χρόνο συγγραφής της παρούσας διατριβής.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η συνεχής εξέλιξη της τεχνολογίας σε όλους τους τομείς επηρέασε σε μεγάλο βαθμό και τον χώρο των τηλεπικοινωνιών. Πενήντα χρόνια πριν ο Martin Cooper δεν θα μπορούσε να φανταστεί ότι η εξέλιξη του, η πρώτη κινητή τηλεφωνική συσκευή, θα εξελισσόταν σε μία «έξυπνη» συσκευή αναγκαία στη ζωή κάθε ανθρώπου. Η έλευση του διαδικτύου δημιούργησε μία νέα ανάγκη για τους ανθρώπους – καταναλωτές, την ανάγκη σύνδεσης στο διαδίκτυο από φορητές και ελαφριές συσκευές στο μέγεθος ενός χεριού. Αυτή η ανάγκη οδήγησε στο πρώτο «έξυπνο» κινητό τηλέφωνο ή αλλιώς smartphone τριάντα χρόνια πριν. Την τελευταία δεκαπενταετία οι έξυπνες κινητές συσκευές έφεραν μία επανάσταση στην κοινωνία. Η ανάπτυξη των «έξυπνων» κινητών συσκευών έφθασε σε σημείο όπου μπορούν να ανταγωνιστούν κανονικό υπολογιστή και κάποιες φορές να κάνουν κάποια πράγματα καλύτερα. Έχουν τη δυνατότητα πολλαπλών διεργασιών ταυτόχρονα λύνοντας αρκετά προβλήματα στην όλο και πιο απαιτητική καθημερινότητα. Οι χρήστες όμως έχουν διαφορετικές ανάγκες μεταξύ τους και αυτό οδήγησε στην ανάπτυξη διαφόρων λειτουργικών συστημάτων με πιο γνωστά το Android και το iOS. Μέσω των λειτουργικών συστημάτων οι χρήστες έχουν τη δυνατότητα να «κατεβάσουν» εφαρμογές στις συσκευές τους ανάλογα με τις ανάγκες τους. Αυτό οδήγησε σε επανάσταση στην κύρια χρήση του κινητού τηλεφώνου, την επικοινωνία με κάποιον άλλον.

Η πληθώρα εφαρμογών έδωσε τη δυνατότητα για πρόσβαση σε παιχνίδια, ενημέρωση, διασκέδαση και νέους τρόπους επικοινωνίας. Οι εφαρμογές ανταλλαγής μηνυμάτων ή αλλιώς messaging apps έγιναν όλο και πιο διαδεδομένες και προτιμώνται πολλές φορές από τον παραδοσιακό τρόπο επικοινωνίας. Για να τις χρησιμοποιήσει κάποιος χρειάζεται σύνδεση στο Διαδίκτυο και αυτό κάνει την επικοινωνία με κάποιον να έχει μηδαμινό κόστος σε σχέση με την ανταλλαγή μηνυμάτων SMS. Οι εφαρμογές ανταλλαγής μηνυμάτων δεν έμειναν μόνο στην αποστολή άμεσων απλών μηνυμάτων αλλά προχώρησαν ένα βήμα παραπέρα με την προσθήκη δωρεάν κλήσεων και ανταλλαγής πολυμέσων μέσω μηνυμάτων.

Για την εγκατάσταση μίας εφαρμογής απαιτείται συγκατάθεση του χρήστη σε κάποιους όρους χρήσης (πολιτικές απορρήτου). Αυτό γίνεται μέσω ενός παραθύρου το οποίο εμφανίζεται στο χρήστη την πρώτη φορά που θα ανοίξει την εφαρμογή και ονομάζεται Privacy Policy. Οι περισσότεροι χρήστες αποδέχονται τους όρους χωρίς να τους έχουν διαβάσει λόγω του ότι είναι αρκετές σελίδες ή δεν έχουν τις απαραίτητες γνώσεις να κατανοήσουν στο τι αναφέρονται. Επίσης, σε πολλές περιπτώσεις ο χρήστης ουσιαστικά δεν έχει δυνατότητα επιλογής, υπό την έννοια ότι αν δεν αποδεχτεί όλους τους όρους η εφαρμογή δεν εγκαθίσταται. Με αυτό τον τρόπο οι εφαρμογές αποκτούν πρόσβαση σε δεδομένα που ίσως να είναι ευαίσθητα χωρίς να είσαι εις γνώση των χρηστών και εδώ δημιουργείται ένα θέμα με τη διαφάνεια την οποία πρέπει να έχουν οι εφαρμογές ως προς το τι δεδομένα συλλέγουν.

Με το ξέσπασμα της πανδημίας του COVID-19 στα τέλη του 2019 και τις αναπόφευκτες απαγορεύσεις κυκλοφορίας σε πολλές χώρες του πλανήτη η χρήση εφαρμογών τηλεπικοινωνίας αυξήθηκε κατακόρυφα. Μέχρι το τέλος του 2021 οι χρήστες των εφαρμογών ανταλλαγής μηνυμάτων ξεπέρασαν τα τρία δισεκατομμύρια **Error! Reference source not found.**. Αυτό οδήγησε σε αλυσιδωτές εξελίξεις στον κόσμο των τηλεπικοινωνιών και στα δικαιώματα τα οποία δίνουμε σε τέτοιου είδους εφαρμογές, στο πόσα και ποια δεδομένα χρησιμοποιούν, το λόγο πίσω από τη συλλογή συγκεκριμένων δεδομένων αλλά και το αν υπάρχουν τα αναγκαία μέτρα ασφάλειας – κρυπτογραφίας κατά τη χρήση των εφαρμογών τηλεπικοινωνίας – ανταλλαγής μηνυμάτων. Πιο πρόσφατο το παράδειγμα της εφαρμογής Zoom όπου ο τριπλασιασμός των καθημερινών χρηστών σε λίγους μήνες ξεγύμνωσε τα προβλήματα σε θέματα ασφάλειας και ιδιωτικότητας της εφαρμογής [01].

Η συνεχιζόμενη αύξηση της χρήσης εφαρμογών τηλεπικοινωνίας παρακίνησε την ανάγκη εκπόνησης της παρούσας διατριβής όπου μέσω θεωρητικής και πρακτικής έρευνας έχει γίνει προσπάθεια κατανόησης του τρόπου με τον οποίο γνωστές εφαρμογές τηλεπικοινωνίας

διαχειρίζονται προσωπικά δεδομένα και αν αυτό γίνεται νόμιμα κάτω από το νέο νομικό πλαίσιο του GDPR.

1.1 Βασικά Ερευνητικά Ερωτήματα

Η παρούσα διατριβή έχει ως στόχο να μελετήσει τις εφαρμογές ανταλλαγής μηνυμάτων – εφαρμογές τηλεπικοινωνιών οι οποίες χρησιμοποιούνται περισσότερο στον κόσμο ως προς τα θέματα ασφάλειας και ιδιωτικότητας των δεδομένων των χρηστών τους. Οι απαιτήσεις για ασφάλεια και προστασία προσωπικών δεδομένων (η οποία είναι συνυφασμένη και με την ιδιωτικότητα των χρηστών) προκύπτουν και από νομικές διατάξεις, ως απόρροια της ανάγκης προάσπισης θεμελιωδών ατομικών δικαιωμάτων: συνεπώς, κάθε επεξεργασία προσωπικών δεδομένων πρέπει να διέπεται από σύνολο προϋποθέσεων για να είναι νόμιμη – και οι προϋποθέσεις αυτές φαίνεται ότι δύσκολα πληρούνται σε περιβάλλον «έξυπνων» εφαρμογών. Με αυτό ως γνώμονα, η διατριβή εστιάζει στις ως άνω εφαρμογές, προκειμένου να μελετηθεί αν οι εφαρμογές – τις οποίες πλέον χρησιμοποιούν αναπόφευκτα σχεδόν όλοι – ικανοποιούν τις αντίστοιχες απαιτήσεις.

Ειδικότερα,, με βάση τα ανωτέρω, η διατριβή εστιάζει στα ακόλουθα ερευνητικά ερωτήματα: :

- Υπάρχει ξεκάθαρη πληροφόρηση για την επεξεργασία προσωπικών δεδομένων από τις εφαρμογές μηνυμάτων και τηλεδιασκέψεων;
- Μπορεί να γίνει διαρροή προσωπικών δεδομένων προς τρίτα μέλη στα οποία στέλνονται δεδομένα;
- Οι εφαρμογές συλλέγουν μόνο τα απαραίτητα δεδομένα τα οποία χρειάζονται για την επεξεργασία την οποία κάνουν;
- Υιοθετούνται ισχυρά πρωτόκολλα και τεχνικές ασφάλειας για την αποτροπή υποκλοπής των δεδομένων;

1.2 Μεθοδολογία

Για την εκπόνηση της παρούσας διατριβής αποφασίστηκε αρχικά μία θεωρητική έρευνα για το λειτουργικό σύστημα το οποίο θα χρησιμοποιηθεί για να κάνουμε εγκατάσταση τις εφαρμογές τηλεπικοινωνιών. Καταλήξαμε στο λειτουργικό σύστημα Android λόγω του ότι είναι το πιο

διαδεδομένο σύστημα αλλά και το πιο εύχρηστο σε σχέση με τους ανταγωνιστές του κάτι το οποίο θα αναλυθεί αργότερα. Ακολούθως διατρέξαμε τα χαρακτηριστικά του Android περιβάλλοντος και κυρίως το permission model βλέποντας τα διάφορα επίπεδα αδειών (permissions) τα οποία μπορεί να ζητήσει μία εφαρμογή κατά την εγκατάσταση της.

Μετέπειτα έγινε μελέτη των γενικών θεμάτων ιδιωτικότητας και ασφάλειας σε εφαρμογές οι οποίες εγκαθίστανται σε κινητές συσκευές αλλά και μία μελέτη των νομικών απαιτήσεων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ - GDPR) και της e-Privacy οδηγίας ως προς το σκέλος της διαφάνειας και της επεξεργασίας. Η μελέτη του ΓΚΠΔ και της e-Privacy οδηγίας θεωρήθηκε επιβεβλημένη λόγω του ότι αν η επεξεργασία δεδομένων των οποίων συλλέγουν οι εφαρμογές γίνεται στην ΕΕ – δηλαδή αν αφορά πολίτες που βρίσκονται στην ΕΕ - θα πρέπει να γίνεται κάτω από τα νομικά πλαίσια του Κανονισμού και της Οδηγίας.

Ολοκληρώνοντας την βιβλιογραφική έρευνα προχωρήσαμε σε πειραματική έρευνα έτσι ώστε να μελετηθούν οι εφαρμογές σε πραγματικό χρόνο σε κατάλληλο περιβάλλον προσομοίωσης. Με αυτό τον τρόπο μας δόθηκε η δυνατότητα να δούμε, μεταξύ άλλων αν οι άδειες (permissions) και οι πολιτικές απορρήτου (privacy policies) ισχύουν και αν γίνεται με διαφάνεια η επεξεργασία δεδομένων χωρίς να αποστέλνονται σε τρίτα μη εξουσιοδοτημένα μέρη. Για να το επιτύχουμε αυτό χρησιμοποιήσαμε πέντε εργαλεία προκειμένου να συνδυαστούν τα αποτελέσματά τους και να ξεπεράσουμε τους όποιους περιορισμούς θέτει ενδεχομένως το καθένα. Τα εργαλεία αυτά είναι το εικονικό περιβάλλον «Privacy International's data interception environment», και τα εργαλεία Exodus, Lumen Privacy Monitor, Inspeckage, SSLUnpinning.

1.3 Δομή της Διατριβής

Η παρούσα μεταπτυχιακή διατριβή αποτελείται από επτά κεφάλαια στα οποία περιγράφεται η ανάγκη της διατριβής, η μεθοδολογία έρευνας και τα αποτελέσματα της. Πιο συγκεκριμένα, στο 2ο Κεφάλαιο περιγράφεται το λειτουργικό σύστημα Android, η αρχιτεκτονική του και το μοντέλο δικαιωμάτων του. Επιπλέον, γίνεται αναφορά και στη χρήση third-party libraries από τους προγραμματιστές στις εφαρμογές οι οποίες σχεδιάζονται για το Android.

Το 3ο Κεφάλαιο αναφέρεται στην προστασία προσωπικών δεδομένων και το νομικό πλαίσιο πίσω από αυτό. Ξεχωρίζει την έννοια της ιδιωτικότητας από αυτή των προσωπικών δεδομένων και γίνεται αναφορά στην εισαγωγή του Γενικού Κανονισμού Προσωπικών Δεδομένων (ΓΚΠΔ) και

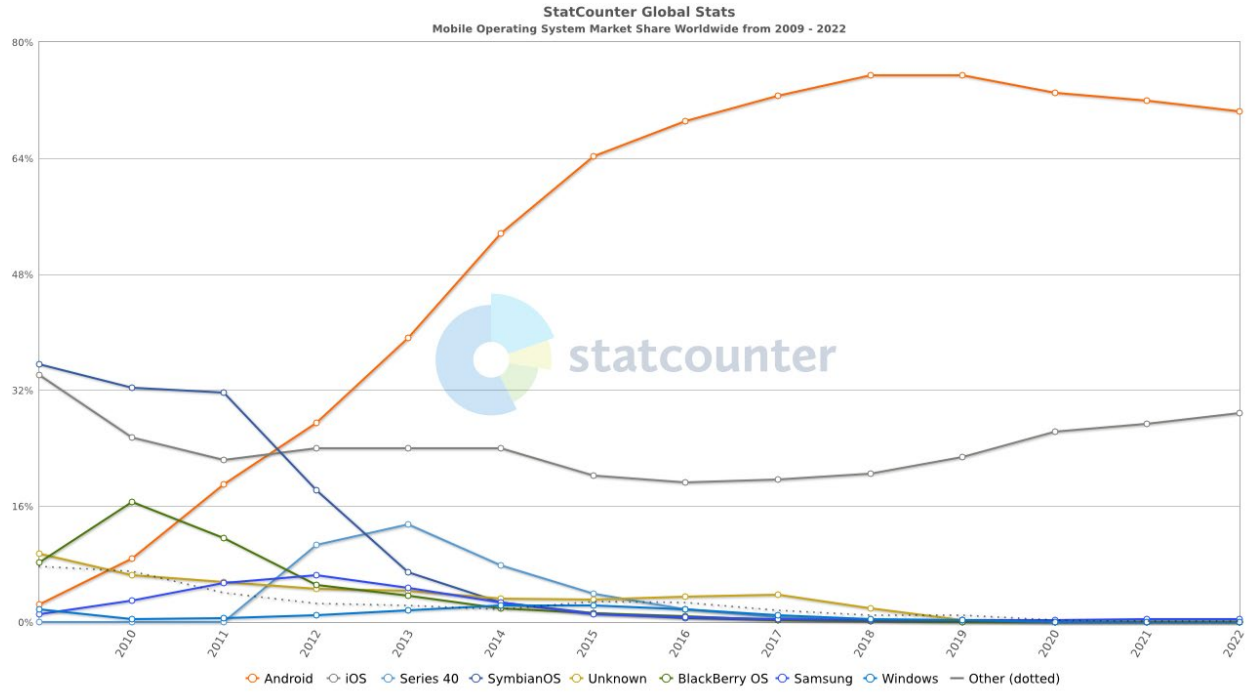
της e-privacy Οδηγίας για τις ηλεκτρονικές επικοινωνίες. Το Κεφάλαιο κλείνει με αναφορές στην επεξεργασία προσωπικών δεδομένων από κινητές συσκευές.

Στο 4ο Κεφάλαιο γίνεται παρουσίαση και αναφορά στα βασικά χαρακτηριστικά των δεκαοκτώ εφαρμογών συνομιλιών / τηλεπικοινωνιών οι οποίες επιλέχθηκαν και μελετήθηκαν στο πλαίσιο της παρούσας διατριβής. Το 5ο Κεφάλαιο είναι ένα από τα σημαντικότερα της διατριβής μιας και εκεί παρουσιάζεται το Περιβάλλον δοκιμών και ο τρόπος με τον οποίο δημιουργήθηκε με τη χρήση κατάλληλων εργαλείων για τη μελέτη των εφαρμογών συνομιλιών / τηλεπικοινωνιών. Τα αποτελέσματα από τη μελέτη των εφαρμογών παρουσιάζονται στο Κεφάλαιο 6 και συγκρίνοντας τα μαζί με τα privacy policies των εφαρμογών.

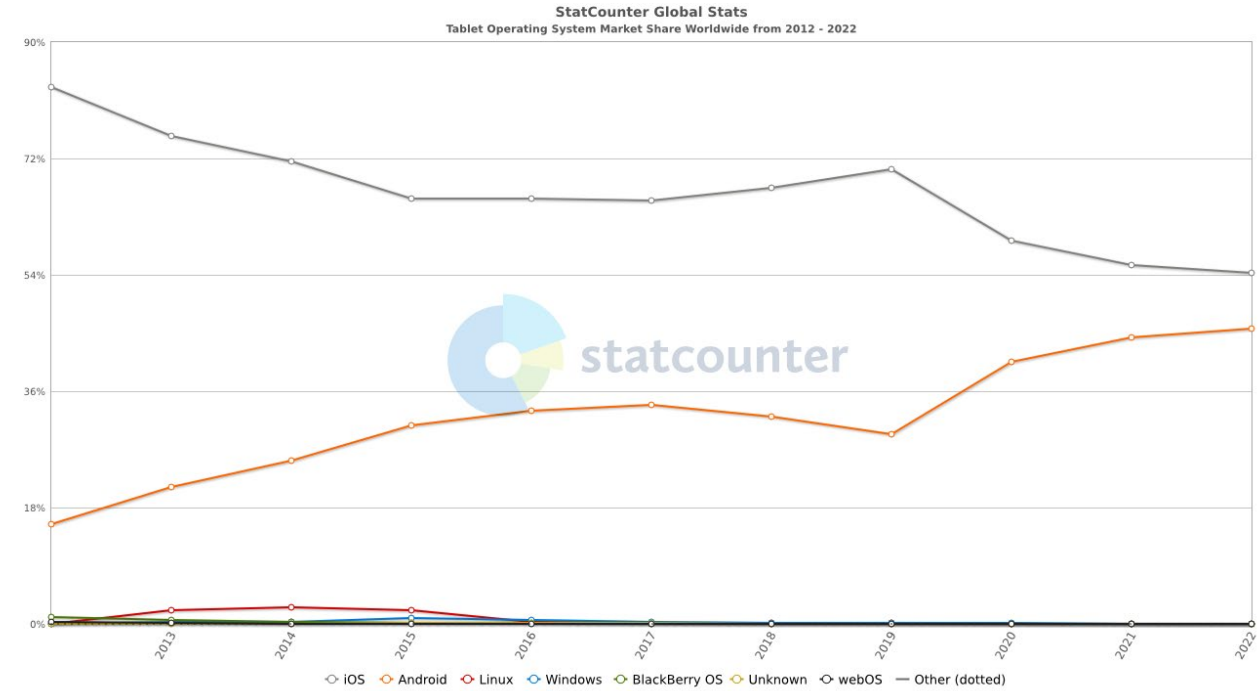
Τέλος, στο 7ο Κεφάλαιο παρουσιάζεται μία σύνοψη των αποτελεσμάτων της μελέτης και της σύγκρισης μας για τις εφαρμογές και τη διαρροή δεδομένων σε τρίτους. Το κεφάλαιο κλείνει με αναφορές σε ενδεχόμενες μελλοντικές έρευνες.

Κεφάλαιο 2
Λειτουργικό σύστημα Android

Το λειτουργικό σύστημα Android κυκλοφόρησε στα τέλη Σεπτεμβρίου του 2008 βασισμένο στον πυρήνα του Linux και άλλα ανοικτού κώδικα λογισμικά. Έφερε την επανάσταση στα λειτουργικά συστήματα των κινητών συσκευών με οθόνη αφής δίνοντας στον κόσμο – και στους κατασκευαστές τηλεφώνων – ένα ανοιχτού κώδικα λογισμικού όπου ο κάθε χρήστης και κατασκευαστής είχε και έχει την ευχέρεια να το τροποποιήσει στις δικές του ανάγκες. Χρειάστηκαν μόλις τρία χρόνια για να φθάσει και να ξεπεράσει σε μερίδιο αγοράς στα κινητά τηλέφωνα το μέχρι τότε κυρίαρχο λειτουργικό σύστημα iOS (Πίνακας 2.1). Δεν ισχύει όμως το ίδιο και με το μερίδιο αγοράς στις κινητές συσκευές – tablets όπου συνεχώς μειώνεται η διαφορά μεταξύ Android και iOS με το δεύτερο να διατηρεί την πρωτιά (Πίνακας 2.2).



Πίνακας 2.1: Μερίδιο αγοράς λειτουργικών συστημάτων κινητών τηλεφώνων από το 2009 μέχρι το 2022 [03]

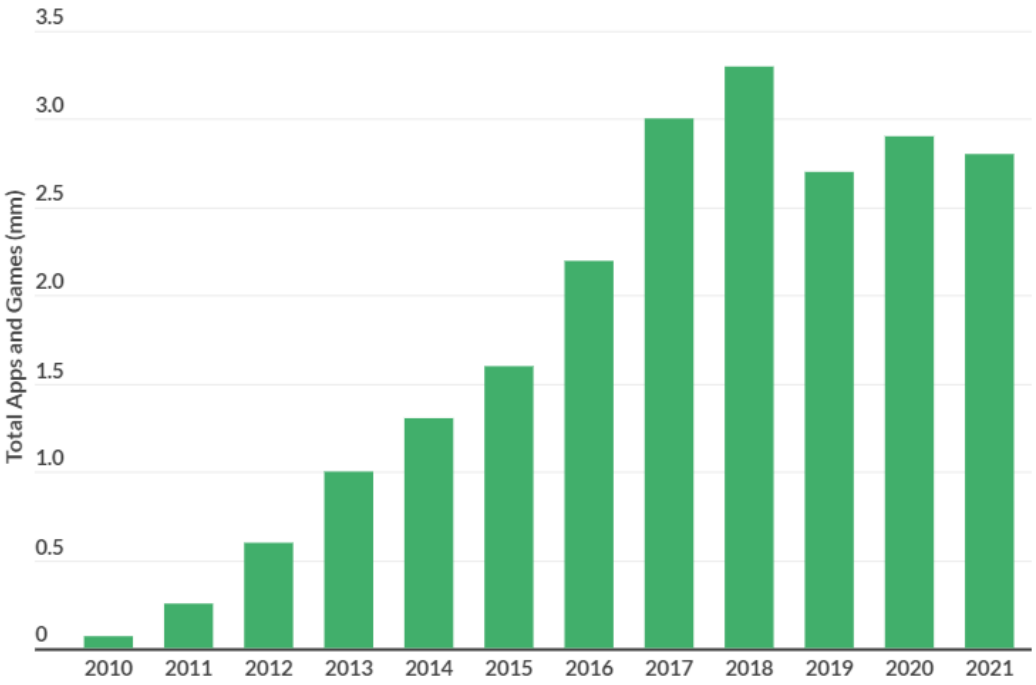


Πίνακας 2.2: Μερίδιο αγοράς λειτουργικών συστημάτων κινητών συσκευών – tablets από το 2012 μέχρι το 2022 [04]

Η πρώτη έκδοση του λειτουργικού συστήματος Android ονομάστηκε Android 1.0 Apple Pie για να φθάσουμε σήμερα στην έκδοση Android 12 Snow Cone. Μέσα από αυτές τις εκδόσεις κάποιες ξεχώρισαν αποκτώντας μεγάλο μερίδιο αγοράς στο χώρο των κινητών συσκευών με λειτουργικό σύστημα Android. Την αρχή έκανε η έκδοση Android 4.4 KitKat με μερίδιο αγοράς στο 6.9% τον

Οκτώβριο του 2013. Θα έπρεπε να περάσουν σχεδόν δύο χρόνια για να υπάρξει αντάξια έκδοση με την έκδοση Android 5.1 Lollipop η οποία είχε μερίδιο αγοράς 11.5%. Το υψηλότερο μερίδιο αγοράς το κατέχει η έκδοση Android 6 με 16.9% η οποία κυκλοφόρησε λίγους μήνες μετά την έκδοση 5.1 **[05]** .

Με κάθε νέα έκδοση προσθέτονται νέα χαρακτηριστικά, λειτουργίες και δυνατότητες για χρήστες και προγραμματιστές. Λόγω του ότι όπως προαναφέρθηκε το λειτουργικό σύστημα Android είναι ανοικτού κώδικα είναι και πιο εύκολη η δημιουργία νέων εφαρμογών σε σχέση με άλλα λειτουργικά συστήματα. Οι εφαρμογές είναι διαθέσιμες μέσω του Google Play Store για εγκατάσταση από τους χρήστες και το μόνο που απαιτείται είναι λογαριασμός Google. Ο πιο κάτω πίνακας παρουσιάζει τις συνολικές εφαρμογές μέχρι σήμερα στο Google Play Store αλλά και την τεράστια αύξηση τους από το 2010.

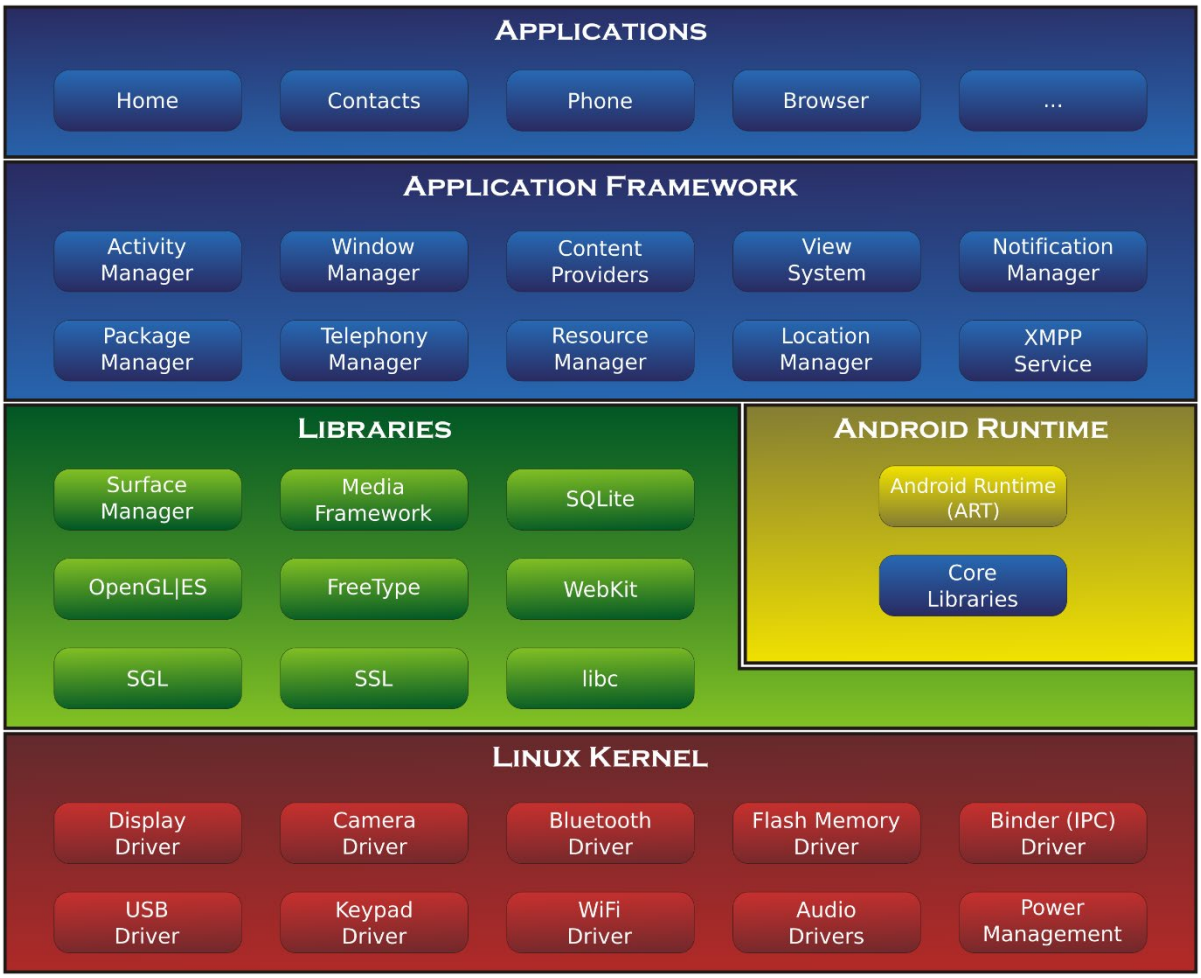


Πίνακας 2.3: Αριθμός διαθέσιμων εφαρμογών στο Google Play Store ανά χρονολογία από το 2010 μέχρι το 2021 [06]

Στο κεφάλαιο αυτό παρουσιάζεται η βασική αρχιτεκτονική του λειτουργικού συστήματος Android, το μοντέλο δικαιωμάτων (permissions model) το οποίο χρησιμοποιούν οι εφαρμογές και η ύπαρξη third-party libraries.

2.1 Αρχιτεκτονική λειτουργικού συστήματος Android

Η αρχιτεκτονική του λειτουργικού συστήματος Android αποτελείται από τέσσερα επίπεδα όπως φαίνεται στην Εικόνα 2.4. Το επίπεδο Εφαρμογών (Applications), το επίπεδο Πλαισίου Εφαρμογών (Application Framework), το επίπεδο Android Βιβλιοθηκών (Android Runtime & Libraries) και τέλος ο Πυρήνας Linux (Linux Kernel).

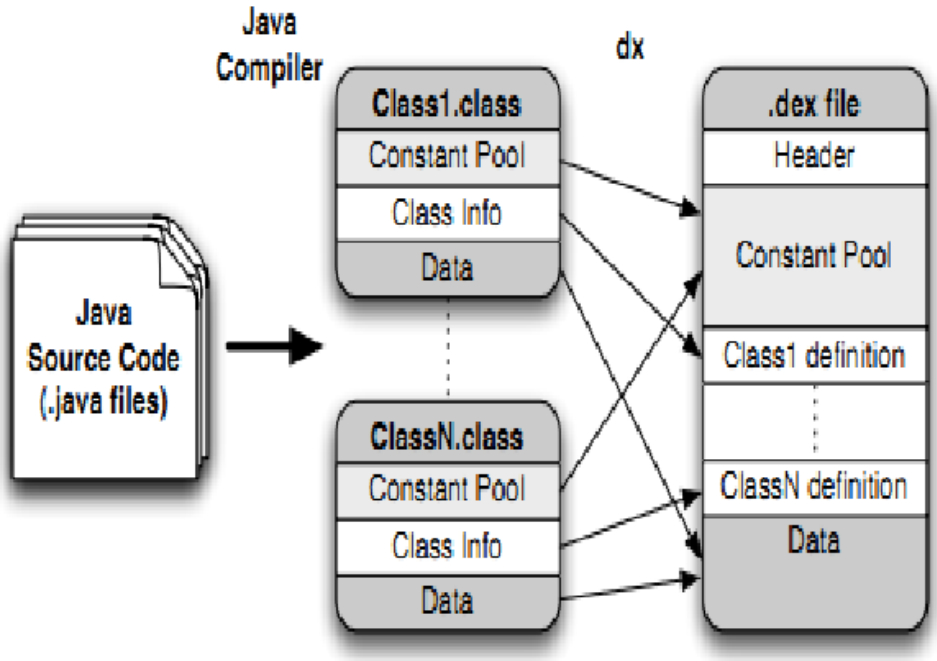


Εικόνα 2.4: Τα τέσσερα επίπεδα της αρχιτεκτονικής του λειτουργικού συστήματος Android [07]

Αρχίζοντας από το χαμηλότερο επίπεδο βλέπουμε τον Πυρήνα Linux (Linux Kernel) ο οποίος είναι και η βάση της όλης αρχιτεκτονικής. Δίνει στο λειτουργικό σύστημα την απαιτούμενη σταθερότητα μιας και προσφέρει υπηρεσίες για διαχείριση μνήμης (Memory Management), Ασφάλειας (Security), διαχείριση μπαταρίας (Power Management. Σε αυτό το επίπεδο βλέπουμε ότι γίνεται και η ένωση μεταξύ λογισμικού και εξοπλισμού (hardware) μέσω των κατάλληλων οδηγών (drivers). [08]

Προχωρώντας στο επίπεδο Βιβλιοθηκών (Libraries) και Android Runtime συναντάμε μία βασική λειτουργία στο Android. Το Android Runtime είναι υπεύθυνο για την εκτέλεση όλων των

εφαρμογών και για να το πετύχει αυτό χρησιμοποιεί μία Εικονική Μηχανή (Virtual Machine), την DVM (Dalvik Virtual Machine). Η συγκεκριμένη μηχανή εκτελεί τα αρχεία σε μορφή ".dex" και έχει τη δυνατότητα εκτέλεσης πολλαπλών εφαρμογών ταυτόχρονα. Πέραν από το VM αυτό το επίπεδο περιλαμβάνει και μία πληθώρα βιβλιοθηκών γραμμένες σε C και C++ γλώσσα προγραμματισμού οι οποίες χρησιμοποιούνται από πολλά συστατικά του λειτουργικού συστήματος. Η πρόσβαση στις βιβλιοθήκες γίνεται με τη βοήθεια του δεύτερου επιπέδου, του επιπέδου Πλαισίου Εφαρμογών.



Εικόνα 2.5: Ο τρόπος λειτουργίας της εικονικής Μηχανής Dalvik [08]

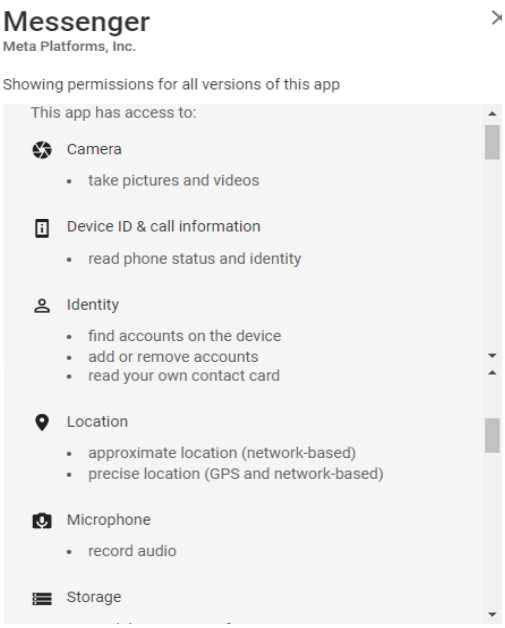
Στο επίπεδο Πλαισίου Εφαρμογών (Android Framework) προσφέρονται οι κλάσεις (classes) και οι υπηρεσίες (services) τα οποία απαιτούνται για τη δημιουργία Android Εφαρμογών. [08] Οι εφαρμογές Android είναι γραμμένες στη γλώσσα προγραμματισμού Java και οι προγραμματιστές έχουν πρόσβαση στο Framework API. Τα APIs αποτελούν τα βασικά δομικά στοιχεία στη δημιουργία μίας Android εφαρμογής λόγω του ότι δίνουν τη δυνατότητα στον προγραμματιστή να επαναχρησιμοποιήσει βασικά και δομικά συστατικά (modular system components) και υπηρεσίες. Κάποια από αυτά περιλαμβάνουν τον Activity Manager, τον Resource Manager, τον Content Provider κ.α. (βλ. Εικόνα 2.4).

Το τελευταίο επίπεδο, το επίπεδο Εφαρμογών (Applications) περιλαμβάνει τις βασικές και προκαθορισμένες εφαρμογές όπως SMS, Email, Internet Browsing, Contacts κ.α. Δεν αφαιρεί όμως τη δυνατότητα από το χρήστη να επιλέξει εφαρμογές τρίτων (third – party app) για προκαθορισμένες. Τέλος, τις δυνατότητες των βασικών εφαρμογών μπορεί ένας προγραμματιστής να τις ενσωματώσει στην εφαρμογή του αν αυτό απαιτείται.

2.2 Μοντέλο δικαιωμάτων στις εφαρμογές Android

Όλες οι εφαρμογές Android πρέπει να έχουν ένα αρχείο AndroidManifest.xml το οποίο λειτουργεί ως η βάση της εφαρμογής. Μεταξύ άλλων στο συγκεκριμένο αρχείο δηλώνονται τα στοιχεία (components), οι διαδικασίες, οι υπηρεσίες της εφαρμογής, οι απαιτήσεις σε εξοπλισμό (hardware) και λογισμικό (software) για να εγκατασταθεί η εφαρμογή και ίσως το πιο σημαντικό για το πλαίσιο της παρούσας διατριβής, τα δικαιώματα (permissions) τα οποία δίνουν στην εφαρμογή δυνατότητα πρόσβασης σε συγκεκριμένα δεδομένα, προστατευμένα σημεία ή άλλες εφαρμογές.

Κατά την εγκατάσταση μίας εφαρμογής μέσω του Google Play Store ο χρήστης έχει τη δυνατότητα να διαβάσει τα δικαιώματα τα οποία ζητάει η εφαρμογή κατά την εγκατάσταση της και ίσως να μην προχωρήσει σε εγκατάσταση της εφαρμογής. Μέσω της έκδοσης Android 6.0 Marshmallow το λειτουργικό σύστημα Android έδωσε τη δυνατότητα στους χρήστες να έχουν τον έλεγχο στο ποια δικαιώματα μπορούν να έχουν πρόσβαση σε πληροφορίες κατά την έναρξη της εφαρμογής.



Εικόνα 2.6: Μέρος των δικαιωμάτων των οποίων απαιτεί η εφαρμογή Messenger μέσω του Google Play Store κατά την εγκατάσταση της

Τα δικαιώματα εφαρμογών κατηγοριοποιούνται σε τρεις διαφορετικούς τύπους. Τα δικαιώματα χρόνου εγκατάστασης (install-time permissions), τα δικαιώματα χρόνου εκτέλεσης (runtime permissions) και τα ειδικά δικαιώματα (special permissions). [09]

Τα δικαιώματα χρόνου εγκατάστασης δίνουν περιορισμένη πρόσβαση σε ευαίσθητα δεδομένα και επιτρέπουν στην εφαρμογή να εκτελέσει ενέργειες οι οποίες δεν επηρεάζουν το σύστημα ή άλλες εφαρμογές. Ο χρήστης δεν ερωτάται για το αν δέχεται τα συγκεκριμένα δικαιώματα αλλά το σύστημα τα αποδέχεται αυτόματα κατά την εγκατάσταση μίας εφαρμογής και ο χρήστης οφείλει να τα διαβάσει πριν προχωρήσει με την εγκατάσταση της. Σε αυτό τον τύπο δικαιωμάτων συναντάμε δικαιώματα όπως "ACCESS_NETWORK_STATE", "ACCESS_WIFI_STATE", "BLUETOOTH", "INTERNET", "VIBRATE" κ.α. [10]

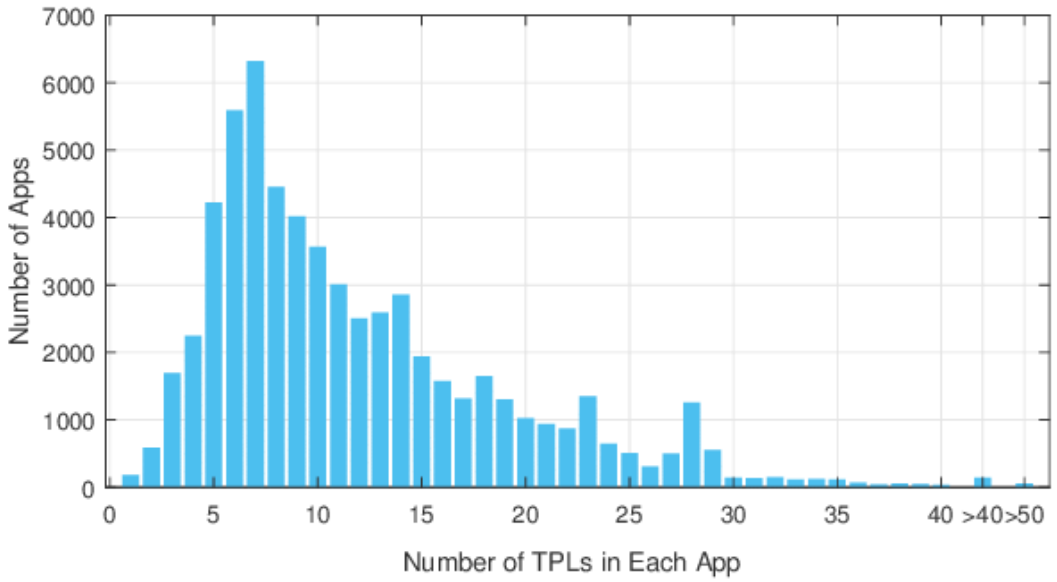
Τα δικαιώματα χρόνου εκτέλεσης δίνουν τη δυνατότητα σε μία εφαρμογή να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα και να προχωρήσει σε περιορισμένες ενέργειες οι οποίες μπορεί να επηρεάσουν το σύστημα ή άλλες εφαρμογές. Πολλά δικαιώματα αυτού του τύπου αποκτούν πρόσβαση σε προσωπικά δεδομένα χρηστών ή σε άλλες ευαίσθητες πληροφορίες. Για αυτό το λόγο έχουν γίνει γνωστά και ως Επικίνδυνα Δικαιώματα (Dangerous Permissions). Στη διάρκεια έναρξης της εφαρμογής εάν απαιτείται να τρέξει ένα δικαίωμα χρόνου εκτέλεσης ο χρήστης ερωτάται αν επιτρέπει στο δικαίωμα να τρέξει και να αποκτήσει πρόσβαση σε συγκεκριμένα δεδομένα ή ενέργειες. Μεταξύ άλλων Επικίνδυνα Δικαιώματα θεωρούνται τα "READ_CONTACTS", "WRITE_CONTACTS", "CAMERA", "ACCESS_FINE_LOCATION", "ANSWER_PHONE_CALLS" κ.α. [10]

Τέλος, τα ειδικά δικαιώματα αντιστοιχούν σε συγκεκριμένες λειτουργίες μίας εφαρμογής και μόνο η πλατφόρμα και οι κατασκευαστές κινητών συσκευών έχουν τη δυνατότητα να τα ορίσουν. Αυτό γίνεται όταν θέλουν να προστατεύσουν την πρόσβαση σε συγκεκριμένες δυνατές ενέργειες όπως η σχεδίασης εφαρμογών πάνω από άλλες εφαρμογές. Παραδείγματα ειδικών δικαιωμάτων αποτελούν τα "SYSTEM_ALERT_WINDOW", "WRITE_SETTINGS". [10]

2.3 Third-Party Libraries

Η χρήση third-party λογισμικού είναι αρκετά διαδεδομένη μεταξύ των προγραμματιστών. Στη δημιουργία εφαρμογών Android χρησιμοποιούνται third-party libraries. Οι βιβλιοθήκες αυτές έχουν τη δυνατότητα επαναχρησιμοποίησης αρκετές φορές και προσθέτουν πληθώρα

δυνατοτήτων στις εφαρμογές. Μαζί τους φέρνουν και προβλήματα ασφάλειας και ιδιωτικότητας κατά τη χρήση μίας εφαρμογής.

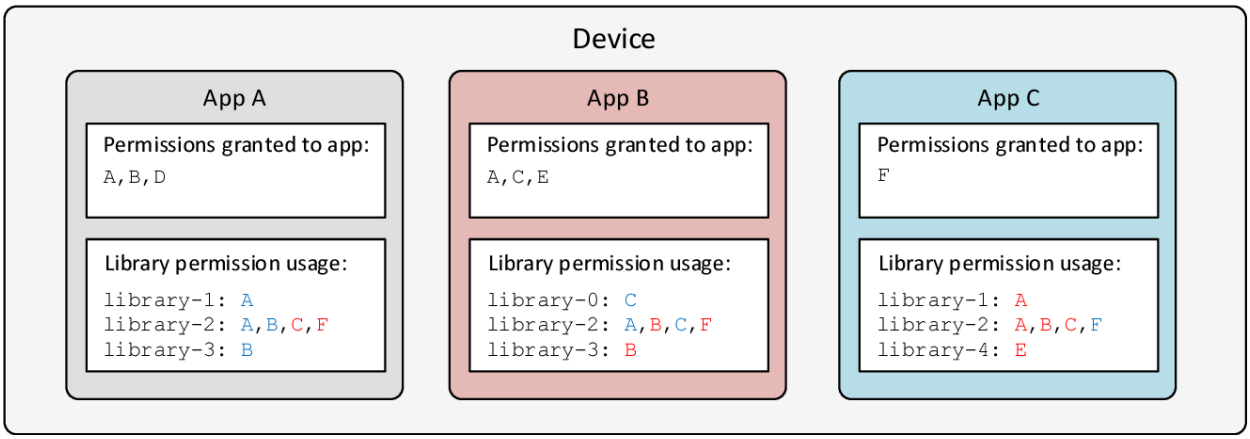


Πίνακας 2.7: Αριθμός third-party libraries οι οποίοι εντοπίστηκαν σε εφαρμογές του Google Play Store [11]

Με την όλο και αυξανόμενη χρήση third-party libraries προέκυψαν ερωτήματα για το αν είναι ασφαλείς η χρήση τους σε εφαρμογές Android ως προς την ασφάλεια και ιδιωτικότητα. Ενώ εκτελείται μία εφαρμογή οι third-party libraries τρέχουν στην ίδια διεργασία με την εφαρμογή και απολαμβάνουν τα ίδια δικαιώματα με τις εφαρμογές χωρίς όρια. Από πολλούς αυτό θεωρείται παραβίαση των δικαιωμάτων των οποίων έδωσε ο χρήστης στην εφαρμογή. Με βάση τις πολιτικές απορρήτου των third-party libraries χρειάζονται πρόσβαση σε συγκεκριμένες πληροφορίες μίας Android συσκευής (IMEI, MAC κ.α.) για να δημιουργήσουν το αναγνωριστικό συσκευής Android (Android-device identifier), να διαβάσουν γεωγραφικές πληροφορίες και να δημιουργήσουν σύνδεση δικτύου. Οι συγκεκριμένες ενέργειες μαζί με την απουσία ενημέρωσης της ύπαρξης third-party library σε μία εφαρμογή θέτει τους χρήστες και τα δεδομένα τους μπροστά σε σοβαρά θέματα ασφάλειας, με το χειρότερο να είναι η διαρροή δεδομένων εν αγνοία τους. [12]

Ένα έξυπνο κινητό τηλέφωνο έχει εγκατεστημένες κατά μέσο όρο εικοσιπέντε εφαρμογές με την κάθε μία να έχει διαφορετική πρόσβαση στη συσκευή ανάλογα με τα δικαιώματα τα οποία της έχουν δοθεί. Όπως προαναφέρθηκε τα δικαιώματα αυτά έχουν το προνόμιο να τα αποκτούν και οι third-party libraries. Αυτό, μαζί με το ότι είναι πιθανό δημοφιλής βιβλιοθήκες (third-party libraries) να χρησιμοποιούνται σε περισσότερες από μία εγκαταστημένες εφαρμογές δημιουργεί ένα πρωτοεμφανιζόμενο είδος επίθεσης, το Intra-Library Collusion (ILC). Η επίθεση συμβαίνει

όταν μία βιβλιοθήκη ενσωματωμένη σε περισσότερες από μία εφαρμογές εκμεταλλεύεται το σύνολο των δικαιωμάτων τα οποία της δόθηκαν και υποκλέπτει ευαίσθητα προσωπικά δεδομένα. [13]



Εικόνα 2.8: Παράδειγμα επίθεσης intra-library collusion (ILC) όπου η βιβλιοθήκη 2 (library-2) αποκτά τέσσερα δικαιώματα στη συσκευή λόγω του ότι εντοπίζεται σε τρεις διαφορετικές εφαρμογές και της έχει δοθεί πρόσβαση. [13]

Από την επίθεση ILC μπορεί να υποψιαστεί κανείς ότι το μεγαλύτερο όφελος το έχουν οι βιβλιοθήκες διαφημίσεων (ad libraries) χωρίς να εξαιρούνται άλλες δημοφιλής βιβλιοθήκες. Οι συγκεκριμένες βιβλιοθήκες χρησιμοποιούνται ως μέσο σύνδεσης μεταξύ διαφημιστή και προγραμματιστή δίνοντας τη δυνατότητα προσθήκης διαφημίσεων στην εφαρμογή. Εάν επιτευχθεί η επίθεση ILC οι βιβλιοθήκες έχουν πρόσβαση σε περισσότερα δεδομένα του χρήστη και γίνεται ευκολότερη η προβολή διαφημίσεων που να αφορούν έμμεσα ή άμεσα το χρήστη αυξάνοντας και το κέρδος των διαφημιστών. [13]

Οι εφαρμογές θα πρέπει να είναι ξεκάθαρες τόσο στο γιατί και ποια δικαιώματα ζητάνε όσο και στη χρήση και διαφάνεια των third-party libraries ώστε να μην ξεφύγουν από τις νομικές απαιτήσεις του νέου Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) και της e-privacy Οδηγίας, όπως περιγράφονται στο επόμενο κεφάλαιο.

Κεφάλαιο 3
Προστασία προσωπικών δεδομένων – Νομικό Πλαίσιο

Όπως προαναφέρθηκε σε μία κινητή συσκευή ο χρήστης, γνωρίζοντάς το ή όχι, πολλές φορές δίνει πρόσβαση σε ευαίσθητες πληροφορίες και προσωπικά του δεδομένα. Από τη νομική σκοπιά, για την περίπτωση χρηστών της Ευρωπαϊκής Ένωσης, η πρόσβαση αυτή των δικαιωμάτων (Permissions) και των third-party libraries θα πρέπει να καλύπτεται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) αλλά και από την e-Privacy Οδηγία. Τόσο ο Κανονισμός όσο και η Οδηγία δρουν μόνο όταν τα δεδομένα τα οποία συλλέγονται θεωρούνται προσωπικά δεδομένα και δεν είναι ανώνυμα (αν και η οδηγία αναφέρεται σε κάθε είδους πληροφορία που αποθηκεύεται στον τερματικό εξοπλισμό του χρήστη, χωρίς να εξειδικεύει στο αν αυτή η πληροφορία πρέπει να εκλαμβάνεται ως προσωπικό δεδομένο). Στο παρόν κεφάλαιο παρατίθενται βασικές έννοιες όπως η έννοια της ιδιωτικότητας και των προσωπικών δεδομένων, λίγα λόγια για τον ΓΚΠΔ και την e-Privacy Οδηγία και την επεξεργασία δεδομένων από εφαρμογές.

3.1 Η έννοια της ιδιωτικότητας

Η έννοια της ιδιωτικότητας (privacy) πηγάζει από τις φιλοσοφικές συζητήσεις των αρχαίων Ελλήνων προσπαθώντας να διαχωρίσουν την «πόλις» από τον «οίκο» και την ανάγκη του ανθρώπου να βρίσκεται μόνος. Το 1776 ο John Adams είχε πει ότι η Αμερικανική επανάσταση άρχισε λόγω του δικαιώματος των Βρετανών να ψάχνουν σπίτια χωρίς δικαιολογία. Καταπατώντας με αυτό τον τρόπο την ιδιωτικότητα των πολιτών και δίνοντας τη σπίθα για την επανάσταση. [14] Οι πρώτοι ορισμοί της ιδιωτικότητας εμφανίστηκαν με τη θεσμοθέτηση του ιδιωτικού δικαίου (privacy law) στην Αμερική από τη δεκαετία του 1890 και μετά. [15] Οι νομικοί Samuel D. Warren Και Louis D. Brandels έγραψαν πρώτοι για την ιδιωτικότητα ορίζοντας την ως «το δικαίωμα να αφήνεσαι μόνος» και την ανάγκη της κοινωνίας να εξελιχθεί προστατεύοντας τα άτομα από παραβιάσεις στην οικιακή και προσωπική ζωή τους. [16]

Την δική του έννοια στην ιδιωτικότητα έδωσε και ο Alan Westin, γνωστός και ως ο πατέρας του ιδιωτικού δικαίου, ορίζοντας την ιδιωτικότητα ως την «ικανότητα των ατόμων να προσδιορίσουν οι ίδιοι πότε, πως και σε ποιο βαθμό οι πληροφορίες τους κοινοποιούνται στους υπόλοιπους με τους οποίος επικοινωνούν».

Το 1981 το Συμβούλιο της Ευρώπης με τη «Σύμβαση 108», δηλαδή τη Σύμβαση για την Προστασία των Ατόμων σε σχέση με την Αυτόματη Επεξεργασία Προσωπικών Δεδομένων, υιοθετεί την πρώτη διεθνή συνθήκη για να αντιμετωπίσει το δικαίωμα των ατόμων στην προστασία των προσωπικών τους δεδομένων και συνάμα την ιδιωτικότητα τους. Λόγω του τεχνολογικά ουδέτερου στυλ με το οποίο συντάχθηκε η Σύμβαση και των συνεχόμενων συστάσεων από το Συμβούλιο της Ευρώπης η Σύμβαση βρίσκει εφαρμογή σε διάφορους τομείς της κοινωνίας για την επεξεργασία προσωπικών δεδομένων είτε αυτό γίνεται σε μία τράπεζα είτε γίνεται στο Διαδίκτυο ακολουθώντας τις τεχνολογικές εξελίξεις. [17]

Τέλος, στην ιδιωτικότητα αναφέρεται και ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης ο οποίος ανακηρύχθηκε επίσημα τον Δεκέμβριο 2000. Στο Άρθρο 7 περιγράφεται ο σεβασμός της ιδιωτικής και οικογενειακής ζωής αναφέροντας ρητά ότι «Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του». Η αναφορά στην επικοινωνία είναι στενά συνυφασμένη με τα προσωπικά δεδομένα τα οποία αποστέλνονται καθημερινά πλέον μέσω της επικοινωνίας μας με διάφορους τρόπους και στο Άρθρο 8 περιγράφεται η προστασία των δεδομένων προσωπικού χαρακτήρα. Στο άρθρο αυτό αναφέρεται το ότι:

- Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

- Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερόμενου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωση τους.

- Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής. [18]

3.2 Η έννοια των προσωπικών δεδομένων

Ως προσωπικά δεδομένα (ή δεδομένα προσωπικού χαρακτήρα) ορίζονται οι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Εάν μέσα από διαφορετικές πληροφορίες υπάρχει η δυνατότητα ταυτοποίησης ενός συγκεκριμένου ατόμου αποτελούν δεδομένα προσωπικού χαρακτήρα. Παραδείγματα δεδομένων προσωπικού χαρακτήρα αποτελούν το όνομα, το επώνυμο, η διεύθυνση κατοικίας, αναγνωριστικός αριθμός κάρτας κ.α. [19]

Η εξέλιξη της τεχνολογίας έφερε και την ψηφιοποίηση των προσωπικών δεδομένων. Σε μία κινητή συσκευή υπάρχει πληθώρα προσωπικών δεδομένων. Πιο γνωστά παραδείγματα αποτελούν οι φωτογραφίες και βίντεο, τα βιομετρικά όπως δαχτυλικό αποτύπωμα, οι επαφές (Contacts) και τα στοιχεία σύνδεσης (Login Credentials) σε διάφορους λογαριασμούς. Πέραν από αυτά, σε μία κινητή συσκευή υπάρχουν και τα δεδομένα τα οποία υπό προϋποθέσεις μπορούν να ταυτοποιήσουν ένα άτομο. Ως εκ τούτου, το αναγνωριστικό συσκευής (IMEI Number), ο αριθμός τηλεφώνου, η διεύθυνση δικτύου συσκευής (IP Address) αποτελούν προσωπικά δεδομένα και πρέπει να τυγχάνουν της ίδιας προσοχής. Επιπλέον, λόγω των δικαιωμάτων τα οποία δίνονται στις εφαρμογές, όπως έχουμε δει στο προηγούμενο κεφάλαιο, οι εφαρμογές έχουν τη δυνατότητα να ενεργοποιήσουμε κάποιες δυνατότητες της συσκευής, όπως η κάμερα ή το μικρόφωνο και να μαζέψουν επιπλέον προσωπικά δεδομένα.

Η ευρεία χρήση του διαδικτύου την τελευταία τριανταετία και η πρόσβαση σε αυτό από δισεκατομμύρια ανθρώπους οδήγησε αναπόφευκτα σε αντίστοιχο αριθμό δεδομένων να διακινούνται στο διαδίκτυο. Τα δεδομένα πρέπει να μεταφέρονται και να ανταλλάσσονται με

ασφάλεια, κάτι το οποίο δεν συμβαίνει πάντα. Περαιτέρω, ακόμα και αν λαμβάνονται μέτρα για την ασφαλή μετάδοση των δεδομένων όπως η κρυπτογράφηση, αυτό δεν σημαίνει ότι μέσω άλλων δεδομένων δεν μπορεί να υπάρξει ταυτοποίηση ατόμου και συνάμα παραβίαση της ιδιωτικότητας και των προσωπικών δεδομένων. Η ανάγκη για προστασία της ιδιωτικότητας και των προσωπικών δεδομένων έφερε την Οδηγία 95/46/ΕΚ από το Ευρωπαϊκό Συμβούλιο και Κοινοβούλιο. Η συγκεκριμένη οδηγία συντάχθηκε έτσι ώστε να προστατέψει τα φυσικά πρόσωπα από την επεξεργασία των προσωπικών δεδομένων τους και την ελεύθερη διακίνηση δεδομένων. Λίγα χρόνια αργότερα συντάχθηκε η νέα Οδηγία 2002/58/ΕΚ, γνωστή και ως ePrivacy Directive, αυτή την φορά για την προστασία των φυσικών προσώπων από την επεξεργασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Η ePrivacy Οδηγία αποτέλεσε ειδικότερη νομοθεσία της γενικότερης Οδηγίας 95/46/ΕΚ.

Οι εξελίξεις στη χρήση του διαδικτύου και το όλο και μεγαλύτερο ποσοστό ψηφιοποίησης ανάγκασε το Ευρωπαϊκό Κοινοβούλιο στη σύνταξη του Νέου Κανονισμού 2016/679 σε θέματα προστασίας των ατόμων για την επεξεργασία προσωπικών δεδομένων, γνωστός ως Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ). Ο ΓΚΠΔ αντικατάστησε την Οδηγία 95/46/ΕΚ και ήρθε για να ενισχύσει την προστασία προσωπικών δεδομένων σε ένα γρήγορα αναπτυσσόμενο κόσμο. Η ePrivacy Οδηγία, ως ειδικότερη νομοθεσία του ΓΚΠΔ, εξακολουθεί να παραμένει σε ισχύ.

3.3 Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) 2016/679 είναι ένας κανονισμός του Ευρωπαϊκού Κοινοβουλίου για της προστασία των προσωπικών δεδομένων και της ιδιωτικότητας στην Ευρωπαϊκή Ένωση (ΕΕ) με ισχύ από τις 25 Μαΐου 2018. Με την άμεση εφαρμογή του σε όλα τα Κράτη Μέλη της ΕΕ το Μάιο του 2018 καταργήθηκε η Οδηγία 95/46/ΕΚ και οι εθνικές νομοθεσίες.

Ο νέος κανονισμός θεωρήθηκε αναγκαίος αρχικά για να ενισχύσει την προστασία προσωπικών δεδομένων και των δικαιωμάτων των πολιτών αλλά και για την εναρμόνιση βασικών κανόνων. Επιπλέον έφερε νέες υποχρεώσεις για τους υπεύθυνους επεξεργασίας δεδομένων μαζί με τις κυρώσεις που μπορούν να επιβληθούν (π.χ. ύψη προστίμου) για τις παραβιάσεις προσωπικών δεδομένων κάτι το οποίο δεν συνέβαινε με την Οδηγία 95/46/ΕΚ.

3.3.1 Προσωπικά Δεδομένα σύμφωνα με τον ΓΚΠΔ

Προσωπικά δεδομένα (ή Δεδομένα προσωπικού χαρακτήρα) θεωρείται κάθε πληροφορία (άμεση ή έμμεση) που αναφέρεται σε φυσικό πρόσωπο και χαρακτηρίζει το υποκείμενο από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη (άρ. 2 του ν. 2472/1997) και παραμένει ο ίδιος ορισμός και στον ΓΚΠΔ. Στην πράξη μπορούμε να πούμε ότι είναι τα δεδομένα που αφορούν ένα πρόσωπο και συνδέονται με την ταυτότητα του όπως για παράδειγμα το όνομα, το τηλέφωνο, οι απόψεις κ.α.

3.3.2 Έννοιες - Ορισμοί

Ο ΓΚΠΔ προκειμένου να καλύψει όλο το φάσμα της επεξεργασίας δεδομένων και να είναι ξεκάθαρος είναι ένα αρκετά μεγάλο κείμενο με πληθώρα εννοιών. Πιο κάτω παρουσιάζονται κάποιες έννοιες του Κανονισμού, όπως αυτές καταγράφονται στο Άρθρο 4, οι οποίες είναι απαραίτητες να δοθούν στο πλαίσιο της παρούσας μεταπτυχιακής διατριβής.

- Επεξεργασία δεδομένων: Κάθε πράξη που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα όπως η συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, τροποποίηση, ανάκτηση, αναζήτηση, ανακοίνωση, χρήση, διαβίβαση, διασύνδεση, δέσμευση, διαγραφή, καταστροφή, ο περιορισμός

- Υποκείμενο δεδομένων (Data Subject): Είναι το φυσικό πρόσωπο το οποίο αφορούν τα δεδομένα

- Υπεύθυνος επεξεργασίας (Data Controller): Το φυσικό ή νομικό πρόσωπο που καθορίζει, μόνος του ή από κοινού με άλλου, το σκοπό και τον τρόπο επεξεργασίας. Για την περίπτωση «έξυπνων» εφαρμογών οι οποίες μελετώνται στην παρούσα διατριβή, οι πάροχοί τους είναι κατά κανόνα υπεύθυνοι επεξεργασίας.

- Εκτελών την επεξεργασία (Data Processor): Το φυσικό ή νομικό πρόσωπο που δρα για λογαριασμό του υπεύθυνου επεξεργασίας. Εφόσον ένας υπεύθυνος επεξεργασίας, για την ανάπτυξη μιας «έξυπνης» εφαρμογής, αναθέτει σε τρίτο τμήματα της επεξεργασίας για λογαριασμό του (π.χ. αναθέτει σε μία εταιρεία στατιστικής ανάλυσης τη διεκπεραίωση στατιστικών μετρήσεων επί της χρήσης της εφαρμογής), τότε αυτός ο τρίτος έχει το ρόλο του εκτελούντος την επεξεργασία. Αν όμως αυτός ο τρίτος πραγματοποιεί επεξεργασία

και για δικούς του αποκλειστικά σκοπούς, τότε καθίσταται και ο ίδιος υπεύθυνος επεξεργασίας για τους δικούς του σκοπούς.

- Ευαίσθητα προσωπικά δεδομένα: Προσωπικά δεδομένα τα οποία χρήζουν ακόμα μεγαλύτερης προστασίας γιατί εμπίπτουν στο σκληρό πυρήνα της ιδιωτικότητας. Είναι τα δεδομένα τα οποία αφορούν σε:

    - Φυλετική ή εθνική προέλευση,
    - Πολιτικά Φρονήματα,
    - Θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
    - Συμμετοχή σε συνδικαλιστική οργάνωση,
    - Υγεία,
    - Ερωτική ζωή,
    - Ποινικές διώξεις ή καταδίκες,
    - στη συμμετοχή σε συναφείς με τα παραπάνω ενώσεις.

    Τα ανωτέρω ευαίσθητα δεδομένα, ή διαφορετικά δεδομένα ειδικών κατηγοριών, είχαν την ίδια έννοια και με το προηγούμενο νομικό πλαίσιο της Οδηγίας 95/46/ΕΚ. Στο Άρθρο 9 του ΓΚΠΔ, όπου ορίζονται οι προϋποθέσεις υπό τις οποίες είναι επιτρεπτή η επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, προσθέτονται δύο νέες κατηγορίες ευαίσθητων προσωπικών δεδομένων οι οποίες δεν υπήρχαν στην Οδηγία 95/46/ΕΚ, τα Γενετικά και Βιομετρικά δεδομένα.

- Γενετικά δεδομένα: Δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου (π.χ. δεδομένα από ανάλυση DNA, RNA κτλ.).

- Βιομετρικά δεδομένα: Δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα (π.χ. facial recognition, fingerprint κ.α.).

- Ανώνυμα δεδομένα: Τα δεδομένα τα οποία δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο ή δεδομένα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου να μην μπορεί να εξακριβωθεί. Για να θεωρηθούν τα δεδομένα ανώνυμα θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν από τον υπεύθυνο επεξεργασίας είτε από τρίτο για άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου. Εάν είναι πρακτικά αδύνατο να ταυτοποιηθεί το φυσικό πρόσωπο τότε αυτό καθιστά τα δεδομένα ανώνυμα. Η νομοθεσία και δη ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν εφαρμόζονται σε δεδομένα τα οποία έχουν καταστεί ανώνυμα.

- Ψευδωνυμοποιημένα δεδομένα: Τα προσωπικά δεδομένα τα οποία έχουν τύχει επεξεργασίας κατά τρόπο ώστε να μην μπορούν να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Στον Κανονισμό αναφέρεται ρητώς ότι τα ψευδωνυμοποιημένα δεδομένα δεν πρέπει να θεωρούνται ανώνυμα αλλά πληροφορίες σχετικά με ταυτοποιήσιμο λόγω του ότι τα δεδομένα αυτά θα μπορούσαν να αποδοθούν σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών.

- Συγκατάθεση (Consent): Κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

- Παραβίαση δεδομένων προσωπικού χαρακτήρα (Personal Data Breach): Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

3.3.3 Νομιμότητα της επεξεργασίας προσωπικών δεδομένων

Στο Άρθρο 5 του ΓΚΠΔ ορίζονται οι βασικές αρχές που πρέπει να διέπουν κάθε επεξεργασία προσωπικών δεδομένων και αυτές είναι:

- Νομιμότητα, αντικειμενικότητα και διαφάνεια (lawfulness, fairness and transparency)
- Περιορισμός του σκοπού (purpose limitation)
- Ελαχιστοποίηση των δεδομένων (data minimization)
- Ακρίβεια (accuracy)
- Περιορισμός της περιόδου αποθήκευσης (storage limitation)
- Ακεραιότητα και εμπιστευτικότητα (integrity and confidentiality)
- Λογοδοσία (accountability)

Πιο ειδικά, αρχίζοντας με την πρώτη βασική αρχή τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Ο περιορισμός του σκοπού εξειδικεύει το σκοπό για τον οποίο συλλέγονται τα δεδομένα και αυτό γίνεται μόνο για καθορισμένος, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς. Οι επόμενες δύο αρχές ελαχιστοποιούν τα δεδομένα σε κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους επιβάλλονται σε επεξεργασία. Επιπλέον πρέπει να είναι ακριβή και όταν είναι αναγκαίο να επικαιροποιούνται όσο το δυνατό πιο γρήγορα. Τα δεδομένα θα πρέπει να διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται. Σημαντικό ρόλο παίζει και η απαίτηση εγγύηση για την ενδεδειγμένη ασφάλεια των δεδομένων από σειρά κινδύνων, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων. Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση με τις νομικές υποχρεώσεις, δηλαδή να λογοδοτήσει.

Με βάση τα πιο πάνω γίνεται εύκολα κατανοητό ότι τα δεδομένα τα οποία συλλέγονται και επεξεργάζονται θα πρέπει να είναι τα ελάχιστα δυνατά και μόνο τα απαραίτητα για το σκοπό ή σκοπούς τους οποίους υποβάλλονται σε επεξεργασία.

Περαιτέρω, για να επιτραπεί η επεξεργασία προσωπικών δεδομένων κάποιου, θα πρέπει να συντρέχει μία από τις προϋποθέσεις («νομικές βάσεις») του άρθρου 6 του ΓΚΠΔ. Η πιο χαρακτηριστική ίσως – αν και όχι η μόνη – νομική βάση είναι η συγκατάθεση του ατόμου, δηλαδή για να γίνει η επεξεργασία θα πρέπει το «υποκείμενο των δεδομένων» να έχει δώσει τη συγκατάθεσή (consent) του. Η συγκατάθεση χρειάζεται να είναι ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει και δίνεται με δήλωση ή με σαφή θετική ενέργεια. Υπάρχουν όμως και άλλες περιπτώσεις, όπου επιτρέπεται η επεξεργασία προσωπικών δεδομένων χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων, οι οποίες ορίζονται στο Άρθρο 6 του ΓΚΠΔ. Για παράδειγμα, επιτρέπεται η επεξεργασία εάν είναι αναγκαία στο πλαίσιο σύμβασης ή επιβάλλεται από το νόμο. Εάν ισχύει το δεύτερο τότε ο υπεύθυνος επεξεργασίας υποχρεούται να επεξεργαστεί τα δεδομένα βάσει του νόμου. Εξαίρεση επίσης αποτελεί και η αναγκαία επεξεργασία για τη διαφύλαξη ζωτικών συμφερόντων του υποκειμένου των δεδομένων αλλά και η αναγκαία για την εκπλήρωση καθήκοντος προς το δημόσιο συμφέρον. Τέλος, είναι νόμιμη η επεξεργασία χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων εάν είναι απαραίτητη για την ικανοποίηση έννομου συμφέροντος του υπεύθυνου της επεξεργασίας ή τρίτου, στον οποίο ανακοινώνονται τα δεδομένα και το συμφέρον υπερέχει των δικαιωμάτων και συμφερόντων του υποκειμένου (των δεδομένων).

3.3.4 Διαφάνεια και ασφάλεια στη συλλογή και επεξεργασία δεδομένων

Η διαφάνεια στη συλλογή δεδομένων από το υποκείμενο των δεδομένων αναγράφεται στο Άρθρο 13 του ΓΚΠΔ. Ο υπεύθυνος επεξεργασίας υποχρεούται κατά τη λήψη δεδομένων προσωπικού χαρακτήρα από το υποκείμενο των δεδομένων να το ενημερώσει δίνοντας του την ταυτότητα και τα στοιχεία επικοινωνίας του, τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία όπως επίσης τους αποδέκτες των δεδομένων εάν υπάρχουν. Επιπρόσθετα, για να εξασφαλιστεί θεμιτή και διαφανής επεξεργασία ο υπεύθυνος επεξεργασίας επιβάλλεται από τον Κανονισμό να παρέχει στο υποκείμενο των δεδομένων το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα, την ύπαρξη δικαιώματος υποβολής αιτήματος για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας

τους. Επίσης, το υποκείμενο των δεδομένων πρέπει να ενημερωθεί τόσο για το δικαίωμα του να ανακαλέσει τη συγκατάθεσή του στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα όποτε επιθυμεί όσο και για το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή. Επίσης, σε περίπτωση για την οποία η επεξεργασία ενέχει την αυτοματοποιημένη δημιουργία «προφίλ» των χρηστών για την εξαγωγή συμπερασμάτων για αυτό, τότε θα πρέπει να παρέχεται ενημέρωση και ως προς αυτό.

Η ασφάλεια στην επεξεργασία των δεδομένων και οι υποχρεώσεις του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία αναφέρονται στο Άρθρο 32 του ΓΚΠΔ. Οι δύο τους έχουν την ευθύνη να εφαρμόσουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων που απειλούν τα προσωπικά δεδομένα. Λαμβάνοντας υπόψη το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, τις συνέπειες που θα υπάρξουν για τα υποκείμενα των δεδομένων σε περίπτωση παραβίασης ασφαλείας των δεδομένων, τα μέτρα τα οποία πρέπει να εφαρμόσουν, μεταξύ άλλων, είναι:

- Ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα.

- Δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση.

- Δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος.

- Διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Ο ΓΚΠΔ ουσιαστικά «επιβάλλει» μία διαχείριση κινδύνων ασφάλειας, προκειμένου να υιοθετηθούν, κατάλληλα τεκμηριωμένα, τα βέλτιστα μέτρα ασφάλειας σε σχέση με τους υπάρχοντες κινδύνους, οι οποίοι πρέπει να έχουν αναγνωριστεί εξ αρχής.

3.4 Εφαρμογή της e-Privacy Οδηγίας στις ηλεκτρονικές επικοινωνίες

Η Ευρωπαϊκή Ένωση βλέποντας τις ραγδαίες τεχνολογικές εξελίξεις στον τομέα των τηλεπικοινωνιών και του διαδικτύου και για να προστατέψει τα δεδομένα προσωπικού χαρακτήρα εξέδωσε ήδη από το 2002 την Οδηγία 2002/58/ΕΚ για την προστασία των φυσικών προσώπων από την επεξεργασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, γνωστή και ως e-Privacy Directive. Η Οδηγία τροποποιήθηκε δύο φορές σε ορισμένα σημεία με τις νέες οδηγίες 2006/24/ΕΚ και 2009/136/ΕΚ του Ευρωπαϊκού Συμβουλίου και Κοινοβουλίου. Φυσικά, οι τεχνολογικές εξελίξεις έχουν υπερβεί την εν λόγω Οδηγία και ήδη είναι υπό κατάρτιση σχέδιο Κανονισμού e-Privacy που θα την αντικαταστήσει – όμως ακόμα, τη στιγμή που γράφονται οι εν λόγω γραμμές, είναι σε εφαρμογή η Οδηγία e-privacy.

Η Οδηγία είναι σε ισχύ παράλληλα με τον Γενικό Κανονισμό Προστασίας Δεδομένων συμπληρώνοντας τον και εφαρμόζεται σε όλα τα θέματα που δεν καλύπτονται από αυτόν. Η e-Privacy Οδηγία αποτελείται από δύο βασικές υποχρεώσεις οι οποίες είναι η παροχή ασφάλειας των υπηρεσιών από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και η τήρηση του απορρήτου των πληροφοριών από τα Κράτη Μέλη της Ε.Ε. Βάση αυτών των υποχρεώσεων η Οδηγία αρχικά ρυθμίζει τη διατήρηση δεδομένων από τους παρόχους υπηρεσιών και αναφέρεται ρητά στην υποχρέωση τους να διαγράφουν ή ανωνυμοποιούν τα δεδομένα κίνησης (traffic data) που υποβάλλονται σε επεξεργασία με το τέλος της χρήσης. Επιπρόσθετα ρυθμίζει τόσο τη λήψη ανεπιθύμητων μηνυμάτων με διάφορα μέσα, π.χ. e-mail, SMS κ.α., όσο και την αποθήκευση πληροφοριών ή απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στη συσκευή μέσω κάποιου μέσου, π.χ. HTTP Cookies, Permissions κ.α. Η ρύθμιση της αποθήκευσης πληροφοριών ή απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στη συσκευή αναγράφεται στο Άρθρο 5, Παράγραφος 3 της Οδηγίας και αποτελεί ένα από τα μεγαλύτερα θέματα ιδιωτικότητας και επεξεργασίας προσωπικών δεδομένων στις εφαρμογές ανταλλαγής μηνυμάτων όπου καθημερινά οι χρήστες αποστέλλουν μεγάλο όγκο προσωπικών δεδομένων χωρίς να γνωρίζουν - πολλές φορές - για το ποιος έχει πρόσβαση στη συλλογή και επεξεργασία τους.

3.5 Επεξεργασία προσωπικών δεδομένων από κινητές συσκευές

Οι κινητές συσκευές έχουν πρόσβαση σε πληθώρα προσωπικών και ευαίσθητων δεδομένων διαφόρων τύπων τα οποία δίνονται από τους χρήστες στις εφαρμογές τις οποίες εγκαθιστούν. Πέραν των δικαιωμάτων τα οποία δίνονται από τους χρήστες στις εφαρμογές, οι σύγχρονες κινητές συσκευές έχουν και αρκετούς αισθητήρες (sensors), όπως μικρόφωνο, κάμερα, GPS, Wi-Fi

κ.α., οι οποίοι παράγουν και επεξεργάζονται δικά τους δεδομένα και μεταδεδομένα (metadata). Μέσω συγκεκριμένων αισθητήρων οι χρήστες είναι εύκολο να αναγνωριστούν και να εντοπιστεί η ακριβής θέση τους. Ανάλογα και με το λειτουργικό σύστημα που τρέχουν, π.χ. Android ή iOS, περιέχουν πολλούς διαφορετικούς τύπους αναγνωριστικών. Αυτά μπορεί να είναι αναγνωριστικά κινητού (Device Hardware ID), αποθηκευμένα αρχεία, δαχτυλικά αποτυπώματα κ.α.

Πέραν των πιο πάνω οι χρήστες κινητών τηλεφώνων εγκαθιστούν καθημερινά εφαρμογές μέσω του αντίστοιχου με το λειτουργικό σύστημα τους καταστήματος (App Store, Play Store). Οι εφαρμογές αναπτύσσονται από διαφορετικές εταιρείες χρησιμοποιώντας η κάθε μία δικές της βιβλιοθήκες. Οι βιβλιοθήκες αυτές βοηθάνε τους προγραμματιστές στο να ενσωματώσουν διαφημίσεις, για αύξηση εσόδων, ιχνηλάτες (trackers) για καταγραφή της χρήσης της εφαρμογής από τους χρήστες, δυνατότητα ένωσης με κοινωνικά δίκτυα κ.α. Αυτό, όπως είδαμε στο προηγούμενο κεφάλαιο οδηγεί σε προβλήματα ιδιωτικότητας και πιθανής παραβίασης προσωπικών δεδομένων λόγω των δικαιωμάτων τα οποία αποκτούν οι βιβλιοθήκες χωρίς να είναι σε πλήρη επίγνωση των χρηστών. Κάποιες εφαρμογές αποθηκεύουν και προσωπικά δεδομένα των χρηστών στο Cloud και εάν αυτή η διαδικασία δεν γίνεται με ασφάλεια υπάρχει θέμα με διαρροή προσωπικών δεδομένων.

Με βάση το Ευρωπαϊκό νομικό δίκαιο οι πάροχοι εφαρμογών από τη στιγμή που επεξεργάζονται προσωπικά δεδομένα μέσω των εφαρμογών τους τότε θεωρούνται οι υπεύθυνοι επεξεργασίας (data controllers). Εάν τα δεδομένα του χρήστη καταλήξουν στα χέρια του προγραμματιστή, ο οποίος ίσως αργότερα τα επεξεργαστεί αναλόγως, και θεωρηθούν προσωπικά δεδομένα, όπως αυτά ορίζονται στον ΓΚΠΔ, τότε ενεργοποιούνται αυτόματα οι νομικές ρυθμίσεις του Κανονισμού. Η συλλογή αυτών των δεδομένων εννοείται ότι πρέπει πάντα να γίνεται με τη συγκατάθεση του χρήστη, όπως αυτή ορίζεται στο Άρθρο 6 του Κανονισμού και ο υπεύθυνος επεξεργασίας να είναι σε θέση να το αποδείξει με βάση το Άρθρο 7 του Κανονισμού. [20]

Κεφάλαιο 4
Εφαρμογές συνομιλιών/τηλεδιασκέψεων

Η δυνατότητα εγκατάστασης εφαρμογών στο λειτουργικό σύστημα Android δίνεται μέσω του ψηφιακού καταστήματος της Google, ενσωματωμένο σε όλες τις κινητές συσκευές οι οποίες τρέχουν Android, το Google Play Store. Μέσω του καταστήματος οι χρήστες έχουν τη δυνατότητα εγκατάστασης εκατομμύρια εφαρμογών, δωρεάν και επί πληρωμή, αλλά και αγοράς ψηφιακού περιεχομένου όπως ταινίες, βιβλία, ακουστικά βιβλία (audiobooks). Οι εφαρμογές στο κατάστημα χωρίζονται ανά κατηγορίες ανάλογα με το περιεχόμενο τους. Πιο δημοφιλής κατηγορία αποτελούν τα παιχνίδια και ακολουθούν οι εκπαιδευτικές εφαρμογές και οι εφαρμογές που προορίζονται για επιχειρήσεις (business).

Σημαντική άνοδο στον αριθμό εγκαταστάσεων (install) σημείωσαν οι εφαρμογές τηλεπικοινωνιών από τα τέλη του 2019 λόγω και του ξεσπάσματος της πανδημίας του COVID-19. Το δεύτερο τρίμηνο του 2020 άρχισε με περίπου τον μισό πληθυσμό της Γης να βρίσκεται κάτω

από κάποιας μορφής απαγορευτικά (lockdown), γενικά ή μερικά. Εξ' αυτού οι άνθρωποι αναγκαστικά παρέμειναν στο σπίτι για προστασία της υγείας τους και της δημόσιας υγείας και χρειάστηκε να ανακαλύψουν νέους τρόπους επικοινωνίας με τα αγαπημένα τους πρόσωπα αλλά και εργασίας εξ' αποστάσεως. Όπως αναμενόταν οι πλείστοι στράφηκαν στις εφαρμογές τηλεπικοινωνιών αυξάνοντας τον αριθμό εγκαταστάσεων και βγάζοντας κάποιες από αυτές από την αφάνεια χρόνων, π.χ. Zoom.

Στο παρόν κεφάλαιο περιγράφονται οι εφαρμογές τηλεπικοινωνιών οι οποίες έχουν μελετηθεί σε θεωρητικό και πρακτικό επίπεδο στην παρούσα διπλωματική και είναι αρκετά δημοφιλής σε πολλές χώρες του κόσμου. Οι συγκεκριμένες εφαρμογές προσφέρονται δωρεάν μέσω του Google Play Store και η επιλογή τους έγινε με βάση τη χρήση τους (downloads) από το κατάστημα και για να απευθύνονται σε διάφορες γεωγραφικές περιοχές (π.χ. KakaoTalk στη Νότια Κορέα).

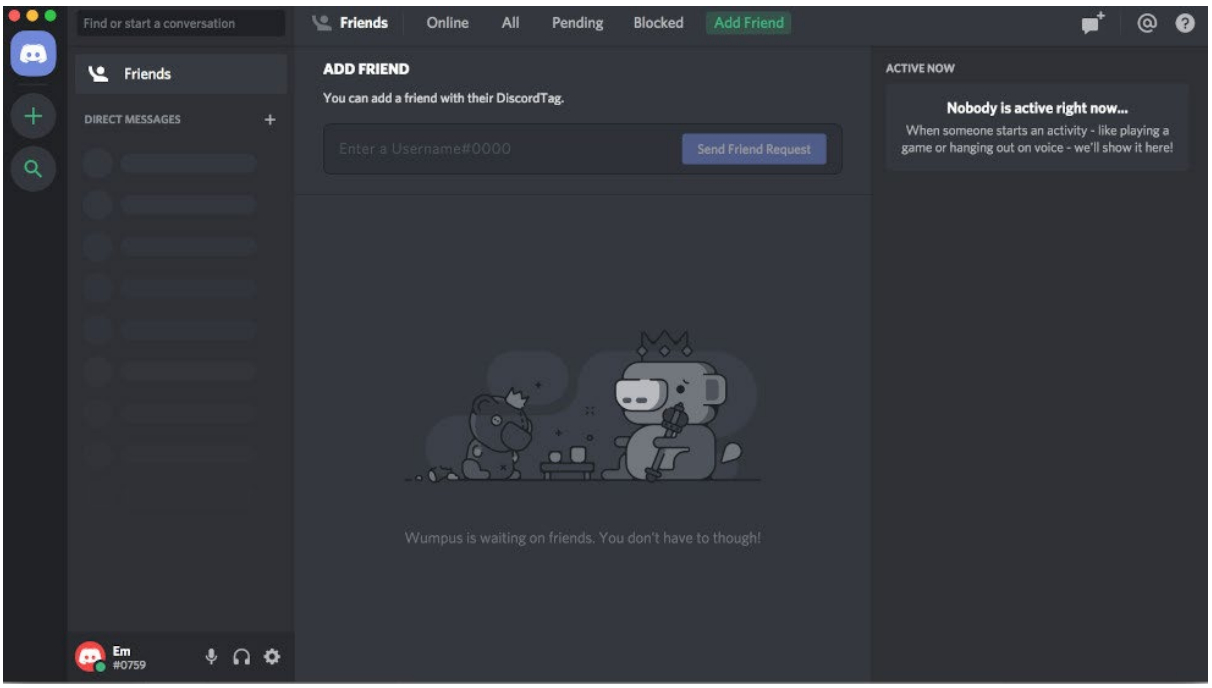
4.1 Discord

Το Discord είναι μία πλατφόρμα Voice over IP (VoIP) με δυνατότητα ανταλλαγής άμεσων μηνυμάτων (instant messaging) και ψηφιακού περιεχομένου όπως εικόνες, βίντεο, gif κ.α. Οι χρήστες επικοινωνούν μέσω φωνητικών κλήσεων, βιντεοκλήσεων και μηνυμάτων με δυνατότητα αποστολής πολυμέσων. Αυτό μπορεί να γίνει είτε μέσω προσωπικού μηνύματος σε άλλο χρήστη ή ως μέρος μίας κοινότητας η οποία λέγεται "server". Σε ένα server υπάρχει πληθώρα καναλιών φωνητικής κλήσης ή ανταλλαγής μηνυμάτων και πρόσβαση σε αυτόν δίνεται μέσω πρόσκλησης. Το Discord μπορεί να το χρησιμοποιήσει κάποιος σε υπολογιστή, κινητό τηλέφωνο, tablet ή μέσω του περιηγητή ιστού (web browser).

Η δημιουργία προφίλ στο Discord γίνεται μέσω ηλεκτρονικής διεύθυνσης (email address) και ο χρήστης επιλέγει ένα ψευδώνυμο (username). Υπάρχει η δυνατότητα πολλοί χρήστες να έχουν το ίδιο ψευδώνυμο μιας και σε κάθε χρήστη δίνεται ένας τετραψήφιος αριθμός ο οποίος αρχίζει με «#», γνωστό ως Discord tag και προσθέτετε στο τέλος του ψευδώνυμου του. Οι χρήστες έχουν τη δυνατότητα να ενώσουν στο λογαριασμό τους άλλες εξωτερικές πλατφόρμες όπως το Steam, Twitch, Spotify, PlayStation κ.α.

Το Discord δημιουργήθηκε αρχικά ως ένα εργαλείο για επικοινωνία μεταξύ παικτών κατά τη διάρκεια ηλεκτρονικών παιχνιδιών. Λόγω της μεγάλης απήχησης της οποίας απέκτησε πρόσθεσε

και άλλες λειτουργίες όπως αναφέρθηκαν πιο πάνω αλλά κατά τη μεταφορά δεδομένων υπάρχει απλή κρυπτογράφηση (standard encryption) και όχι κρυπτογράφηση end-to-end.



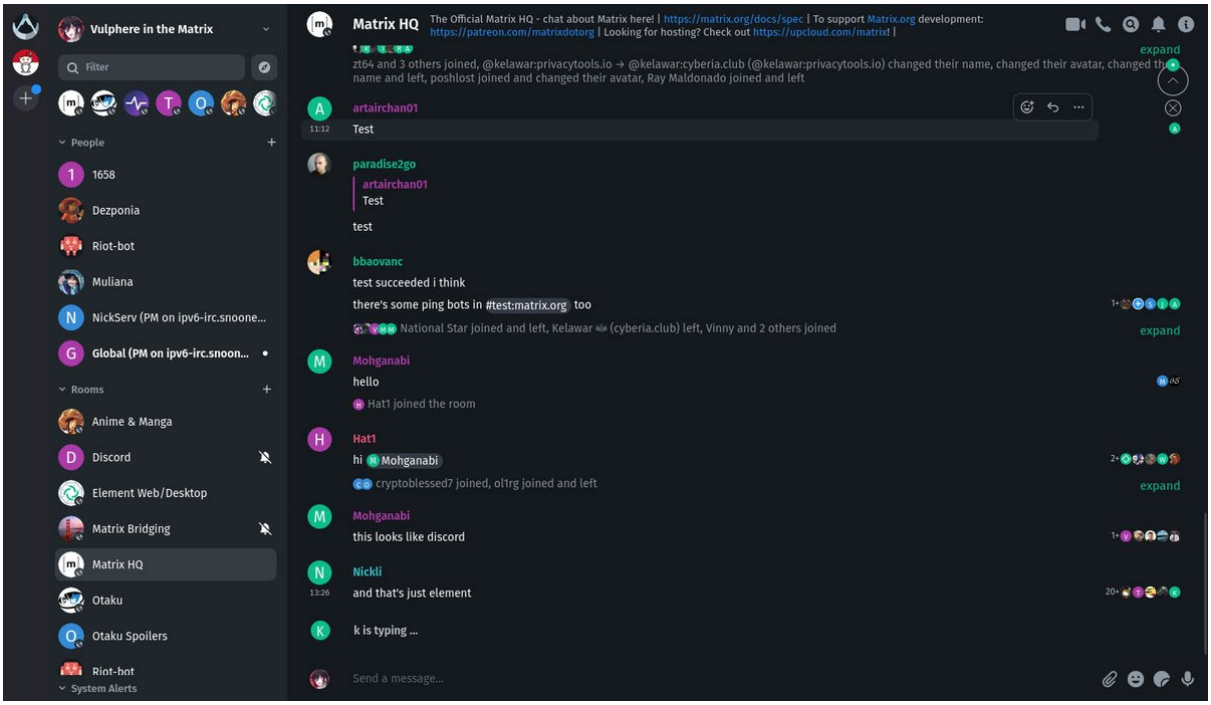
Εικόνα 4.1: Στιγμιότυπο από την αρχική οθόνη του Discord. Πάνω αριστερά διακρίνεται το λογότυπο του. [21]

4.2 Element

Το Element είναι μία ανοιχτού κώδικα εφαρμογή ανταλλαγής άμεσων μηνυμάτων η οποία ενσωματώνει το πρωτόκολλο Matrix. Το συγκεκριμένο πρωτόκολλο είναι ανοικτού κώδικα πρωτόκολλο το οποίο επιτρέπει άμεση επικοινωνία. Οι χρήστες επικοινωνούν μέσω φωνητικών κλήσεων, βιντεοκλήσεων και μηνυμάτων με δυνατότητα αποστολής πολυμέσων. Η επικοινωνία μπορεί να γίνει μεταξύ δύο χρηστών ή περισσότερων και υπάρχει η δυνατότητα συμμετοχής σε ομάδες, τα Rooms όπως τα ονομάζει το Element. Τα Rooms αποτελούν κύριο χαρακτηριστικό της χρήσης του Element μιας και χρησιμοποιείται ως ένα εργαλείο συνεργασίας (collaboration tool) είτε αυτό είναι στον τομέα της τεχνολογίας είτε σε ένα παιχνίδι. Ο χρήστης έχει τη δυνατότητα αναζήτησης δημόσιων (public) Rooms ή συμμετοχής σε κλειστά (private) Roomsμέσω πρόσκλησης ή να δημιουργήσει δικό του Room. Η πρόσβαση στο Element γίνεται μέσω εφαρμογής στον υπολογιστή ή στην κινητή συσκευή ή μέσω του περιηγητή ιστού από την

διαδικτυακή εφαρμογή (web application). Η δημιουργία λογαριασμού είναι αρκετά εύκολη και γίνεται είτε μέσω ηλεκτρονικής διεύθυνσης (email address), αριθμό τηλεφώνου, ψευδώνυμου (username) ή με τη χρήση άλλων λογαριασμών όπως Google, Facebook, Github κ.α.

Η εφαρμογή υποστηρίζει την κρυπτογραφία end-to-end κατά την ανταλλαγή δεδομένων μεταξύ χρηστών και επίσης χρησιμοποιεί το TLS/Noise πρωτόκολλο για κρυπτογραφία της κίνησης δικτύου (network traffic). Η κρυπτογραφία είναι ενεργοποιημένη από προεπιλογή και χρησιμοποιούνται οι κρυπτογραφικοί αλγόριθμοι Curve25519 / AES-256 / HMAC-SHA256. Τέλος υπάρχει η δυνατότητα αποθήκευσης δεδομένων στο σύννεφο (cloud) και τα δεδομένα είναι κρυπτογραφημένα. [22]



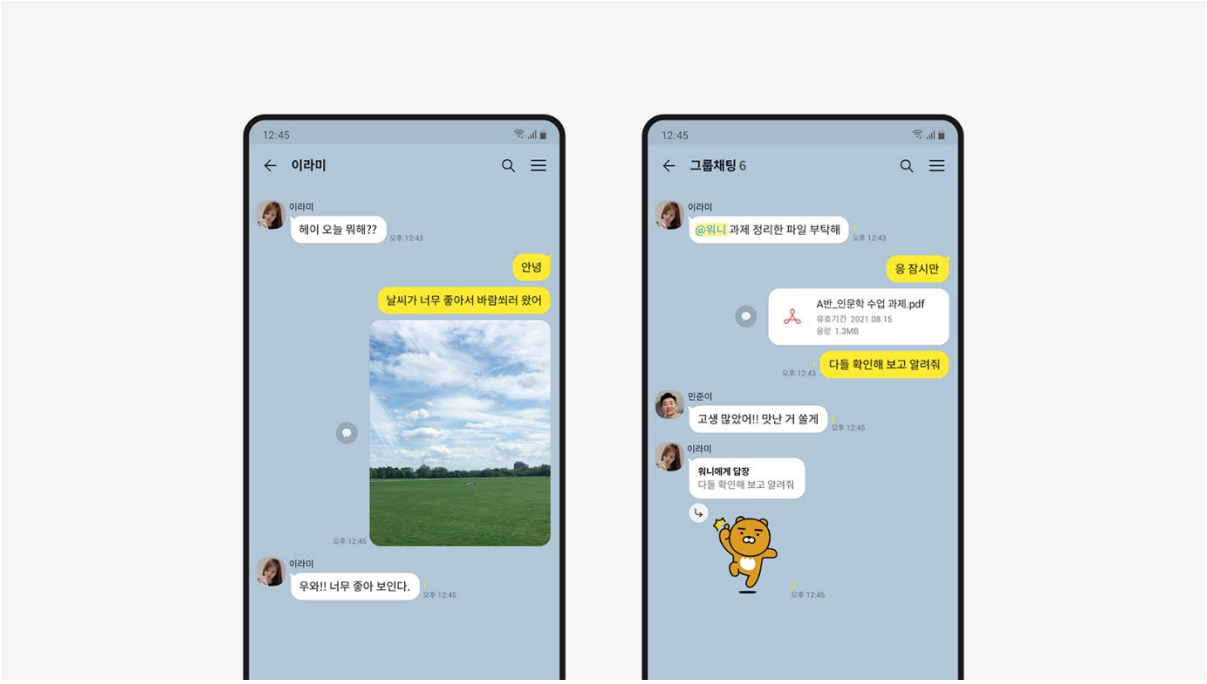
Εικόνα 4.2: Στιγμιότυπο από το Element. Μπορούμε να δούμε τα Rooms και τις δυνατότητες επικοινωνίας της εφαρμογής. [23]

4.3 KakaoTalk

Η εφαρμογή KakaoTalk είναι εφαρμογή ανταλλαγής μηνυμάτων από την εταιρεία Kakao της Νοτίου Κορέας. Δεν είναι τόσο διαδομένη στο δυτικό κόσμο αλλά με βάση έρευνα το 2020 το 97.5% των χρηστών στην Νότια Κορέα χρησιμοποιεί την εφαρμογή. [24] Για τη δημιουργία λογαριασμού χρειάζεται ηλεκτρονική διεύθυνση (email address) ή αριθμός τηλεφώνου. Το KakaoTalk είναι προσβάσιμο από κινητή συσκευή ή ηλεκτρονικό υπολογιστή και προσφέρει τις ίδιες υπηρεσίες με άλλες παρόμοιες εφαρμογές και ακόμη περισσότερα. Μέσω της εφαρμογής πέραν από ανταλλαγή μηνυμάτων, φωνητικές κλήσεις, βιντεοκλήσεις, ανταλλαγή πολυμέσων, οι

χρήστες έχουν τη δυνατότητα να κατεβάσουν και να παίξουν παιχνίδια με φίλους τους απευθείας (από την εφαρμογή). Επιπλέον η εφαρμογή δίνει τη δυνατότητα αναζήτησης δημοφιλών μάρκων (brands) και καλλιτεχνών και συζήτησης μεταξύ τους αλλά και τη δυνατότητα απόκτησης εκπτωτικών κουπονιών και αγοράς αγαθών μέσω της πλατφόρμας "Gifting".

Δυστυχώς δεν είναι γνωστά πολλά πράγματα για την ασφάλεια της εφαρμογής αλλά γνωρίζουμε ότι προσφέρεται η κρυπτογράφηση end-to-end κατά την ανταλλαγή μηνυμάτων. Η επιλογή αυτή δεν είναι ενεργοποιημένη και χρειάζεται να την ενεργοποιήσει ο χρήστης χειροκίνητα.



Εικόνα 4.3: Στιγμιότυπο από ανταλλαγή μηνυμάτων με την εφαρμογή KakaoTalk. [25]

4.4 Line

Το Line είναι δωρεάν εφαρμογή ανταλλαγής μηνυμάτων και πολυμέσων, VoIP κλήσεων και τηλεδιασκέψεων από την Νοτιοκορεάτικη εταιρεία Naver Corporation. Αρχικά δημιουργήθηκε ως εφαρμογή αντιμετώπισης καταστροφών την περίοδο του καταστροφικού σεισμού και τσουνάμι το 2011 στο Tohoku αλλά σύντομα προστέθηκαν περισσότερες δυνατότητες και σήμερα είναι η δημοφιλέστερη εφαρμογή ανταλλαγής μηνυμάτων σε Ιαπωνία, Ταϊβάν και Ταϊλάνδη. Η δημιουργία λογαριασμού γίνεται μέσω αριθμού τηλεφώνου και η πρόσβαση σε αυτή γίνεται είτε μέσω κινητής συσκευής είτε μέσω ηλεκτρονικού υπολογιστή. Πέραν από τις βασικές δυνατότης κλήσεων και ανταλλαγής μηνυμάτων και πολυμέσων η εφαρμογή πάει ένα βήμα πιο πέρα με την εισαγωγή περισσότερων υπηρεσιών για τους χρήστες.

Μεταξύ άλλων οι χρήστες του Line μπορούν να αναρτήσουν κάτι το οποίο θα εμφανιστεί στο Timeline της εφαρμογής, να διαβάσουν ειδήσεις μέσω του Line Today, να πληρώσουν μέσω του Line Pay, να παίξουν παιχνίδια τα οποία προσφέρονται από το Line Games, να αγοράσουν αγαθά, να δούνε ταινίες κ.α. Επιπλέον δίνει τη δυνατότητα εταιρικού λογαριασμού στις εταιρείες για προσέλκυση νέων πελατών αλλά και εμφάνισης στοχευμένων διαφημίσεων επί πληρωμή. [26]

Η ασφάλεια της εφαρμογής πέρασε από χίλια μύρια κύματα μιας και το 2013 ήταν εύκολο να γίνει υποκλοπή στην ανταλλαγή μηνυμάτων χρησιμοποιώντας εργαλεία τα οποία συλλέγουν τα πακέτα δεδομένων (packet capture). Τα μηνύματα αποστέλνονταν σε απλό κείμενο προς το server της εφαρμογής (Line) κατά τη χρήση των δεδομένων κινητού (cellular data) αλλά κρυπτογραφημένα κατά τη χρήση Wi-Fi. Τρία χρόνια αργότερα η εταιρεία έθεσε ως προεπιλογή την κρυπτογραφία end-to-end χρησιμοποιώντας το κρυπτογραφικό πρωτόκολλο ECDH (Elliptic-curve Diffie-Hellman) για όλους τους χρήστες. Η end-to-end κρυπτογραφία της εφαρμογής έχει πάρει την ονομασία Letter Sealing . [27]

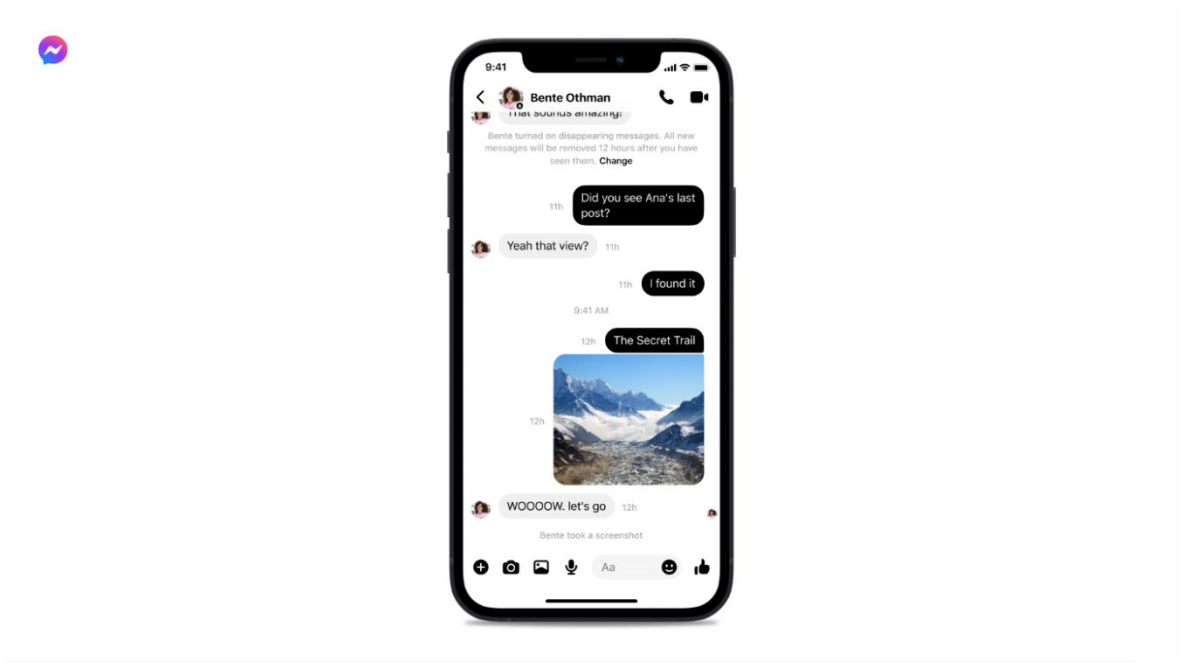
Εικόνα 4.4: Στιγμιότυπο από τη χρήση αυτοκόλλητων (stickers) μέσω της εφαρμογής Line. [28]

4.5 Messenger

Το Messenger είναι πλατφόρμα ανταλλαγής άμεσων μηνυμάτων της εταιρείας Meta. Άρχισε ως μέρος του κοινωνικού δικτύου Facebook αλλά πλέον υπάρχει και ως ανεξάρτητη εφαρμογή. Οι

χρήστες έχουν τη δυνατότητα δημιουργίας λογαριασμού σε αυτήν είτε μέσω του Facebook λογαριασμού τους είτε μέσω ηλεκτρονικής διεύθυνσης είτε μέσω αριθμού τηλεφώνου. Μπορεί να χρησιμοποιηθεί μέσω κινητής συσκευής, ηλεκτρονικού υπολογιστή ή μέσω της διαδικτυακής εφαρμογής του Facebook. Η εφαρμογή προσφέρει άμεση ανταλλαγή μηνυμάτων και ψηφιακού περιεχομένου με τη δυνατότητα αντίδρασης (react) μέσω εικονιδίων (emojis), φωνητικές κλήσεις, βιντεοκλήσεις. Επιπλέον προσφέρεται η δημιουργία ψηφιακής απάντησης με τη χρήση Chatbots αλλά και ψυχαγωγικό περιεχόμενο όπως παιχνίδια.

Κατά την αποστολή δεδομένων χρησιμοποιείται κρυπτογραφία end-to-end αλλά και TLS/Noise πρωτόκολλο για κρυπτογραφία της κίνησης δικτύου (network traffic). Η κρυπτογραφία δεν είναι ενεργοποιημένη από προεπιλογή αλλά πρέπει να ενεργοποιηθεί από το χρήστη. Οι αλγόριθμοι οι οποίοι χρησιμοποιούνται είναι οι Curve25519 / AES-256/ HMAC-SHA256. [22]



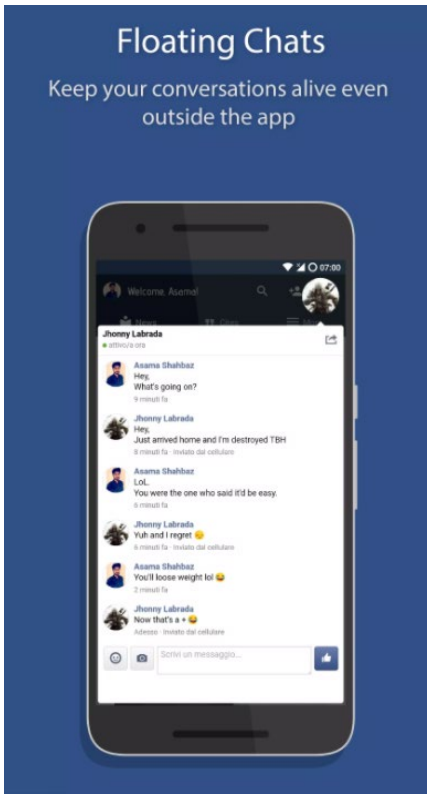
Εικόνα 4.5: Στιγμιότυπο από την αποστολή κρυπτογραφημένων μηνυμάτων μέσω του Messenger. [29]

4.6 Phoenix

Η εφαρμογή Phoenix της εταιρείας Unimania είναι εφαρμογή στην οποία μπορείς να ενσωματώσεις σε αυτήν το Facebook και το Messenger και με βάση την περιγραφή της χρειάζεται λιγότερη ενέργεια (μπαταρία) και δεδομένα για να τρέξει τις εφαρμογές και το κάνει γρηγορότερα.

Στην ουσία σου δίνει τη δυνατότητα να εξοικονομήσεις μπαταρία και δεδομένα τρέχοντας πιο γρήγορα το Facebook & Messenger δίνοντας σου όλα τα πλεονεκτήματα των δύο εφαρμογών. Οι δυνατότητες του Messenger αναφέρονται πιο πάνω (4.5 Messenger).

Δυστυχώς δεν είναι γνωστά πολλά για την ασφάλεια της εφαρμογής αλλά το ότι ο χρήστης δίνει στην εφαρμογή πρόσβαση στους λογαριασμούς του αυτό χρίζει περαιτέρω έρευνας και είναι ενδιαφέρον το πως επεξεργάζονται μετέπειτα τα δεδομένα αυτής της πρόσβασης.

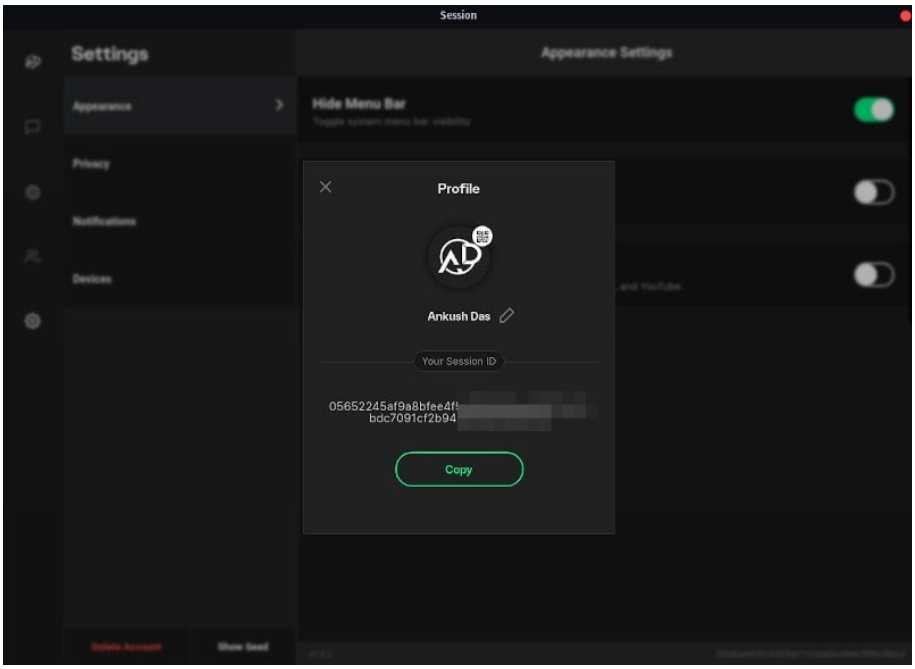


Εικόνα 4.6: Χρήση της δυνατότητας αναδυόμενου παραθύρου σε μήνυμα μέσω της εφαρμογής Phoenix. [30]

4.7 Session

Το Session messenger είναι μία ανοιχτή αποκεντρωμένη εφαρμογή ανταλλαγής άμεσων μηνυμάτων βασισμένη στο εικοσύστημα (ecosystem) Oxen (blockchain). Το συγκεκριμένο εικοσύστημα υποστηρίζει κρυπτογραφία end-to-end χρησιμοποιώντας το Signal protocol και διαγράφει κάποια μεταδεδομένα (metadata). Η εφαρμογή έχει τη δυνατότητα μόνο ανταλλαγής μηνυμάτων και πολυμέσων με τα λιγότερα δυνατόν μεταδεδομένα. Η δυνατότητα φωνητικής κλήσης και βιντεοκλήσης μέσω της εφαρμογής βρίσκεται ακόμη σε δοκιμαστική φάση.

Ιδιαίτερο ενδιαφέρον έχει η ασφάλεια της εφαρμογής. Για αρχή, δεν χρειάζεται ηλεκτρονική διεύθυνση (email address) ή αριθμός τηλεφώνου για εγγραφή αλλά στον κάθε χρήστη δίνεται ένα τυχαίο μοναδικό αναγνωριστικό (unique ID) του τύπου «05652245af9a8bfee4f5a8138fd5c…» και με αυτό μόνο μπορείς να προσθέσεις φίλους ή να βρεις άλλους χρήστες της εφαρμογής. Χρησιμοποιώντας το Oxen blockchain και το onion routing πρωτόκολλο υπάρχουν δεκάδες



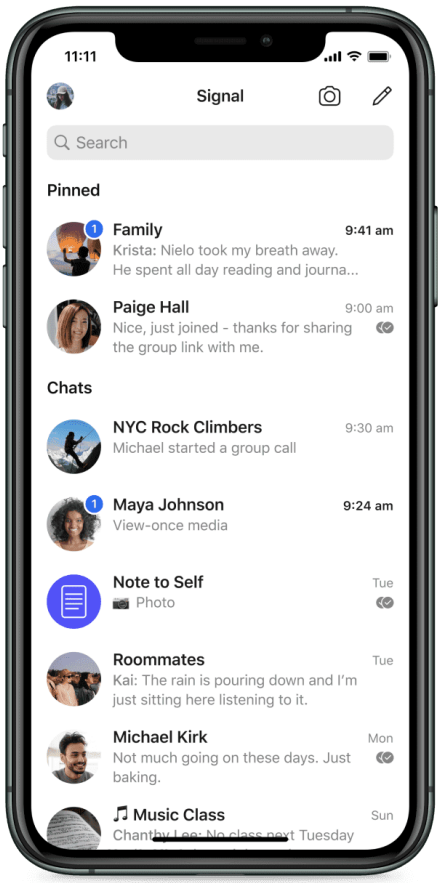
αποκεντρωμένοι διακομιστές (servers) και πετυχαίνετε κρύψιμο της διεύθυνσης IP των χρηστών. Εκτός αυτών, γίνεται και χρήση του Signal protocol το οποίο επιτρέπει την αποστολή ασύγχρονων μηνυμάτων με χρήση μεγάλης διάρκειας κλειδιών ασφάλειας. Χρησιμοποιούνται τα κρυπτογραφικά πρωτόκολλα X25519 / XSalsa20 256 / Poly1305. Από πολλούς θεωρείται η πιο ασφαλής εφαρμογή ανταλλαγής μηνυμάτων χωρίς διαρροή δεδομένων.

4.8 Signal

Εικόνα 4.7: Επεξεργασία προφίλ χρήστη στο Session όπου εμφανίζεται το μοναδικό αναγνωριστικό χρήστη (random unique ID). [31]

Το Signal είναι κεντρικοποιημένη κρυπτογραφημένη εφαρμογή ανταλλαγής άμεσων μηνυμάτων διαθέσιμη σε κινητές συσκευές και ηλεκτρονικούς υπολογιστές. Πέραν της βασικής λειτουργίας υπάρχει η δυνατότητα ανταλλαγής ψηφιακού περιεχομένου, φωνητικών κλήσεων, βιντεοκλήσεων και ομαδικών κλήσεων. Σε κινητές συσκευές οι οποίες τρέχουν λειτουργικό σύστημα Android το Signal μπορεί να χρησιμοποιηθεί ως η προκαθορισμένη εφαρμογή αποστολής SMS/MMS χωρίς τα μηνύματα αυτά να είναι κρυπτογραφημένα. Η δημιουργία λογαριασμού γίνεται με τη χρήση αριθμού τηλεφώνου.

Η κρυπτογραφία των μηνυμάτων και των κλήσεων στην εφαρμογή είναι end-to-end και δίνεται από το πρωτόκολλο Signal Protocol το οποίο δημιουργήθηκε αρχικά για το Signal αλλά χρησιμοποιείται και από άλλες εφαρμογές της ίδιας κατηγορίας π.χ. Session. Τα κρυπτογραφικά πρωτόκολλα τα οποία χρησιμοποιούνται είναι τα Curve25519 / AES-256 / HMAC-SHA256.

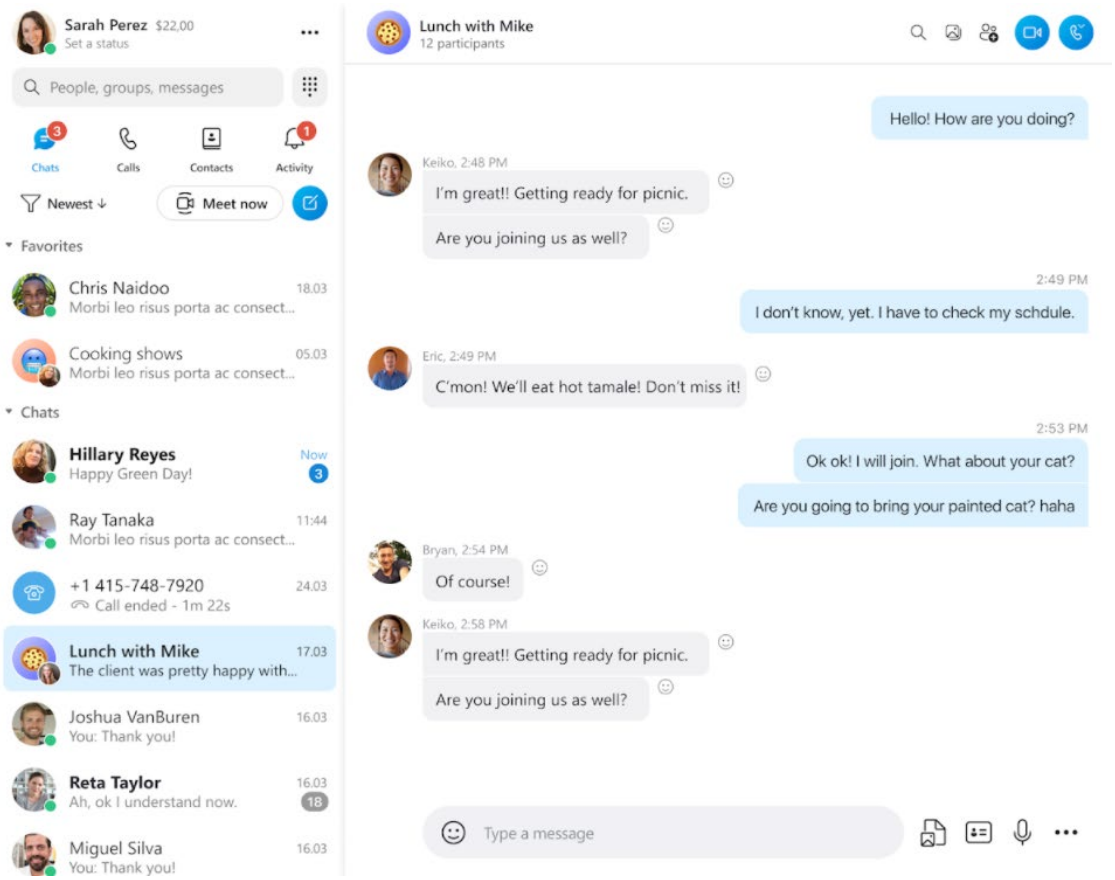


Εικόνα 4.8: Στιγμιότυπο από την αρχική οθόνη της εφαρμογής Signal(random unique ID). [32]

4.9 Skype

Το Skype αποτελεί ίσως την πιο γνωστή εφαρμογή τηλεφωνίας μέσω διαδικτύου (Voice over IP) με δυνατότητα τηλεδιασκέψεων, φωνητικών κλήσεων και βιντεοκλήσεων. Υπάρχει επίσης δυνατότητα ανταλλαγής μηνυμάτων, αρχείων αλλά και κλήσεων με χρήση του παραδοσιακού τρόπου τηλεφωνίας επί πληρωμή. Είναι διαθέσιμο σε ηλεκτρονικούς υπολογιστές, κινητές συσκευές αλλά και σε κονσόλες παιχνιδιών. Δημιουργία λογαριασμού μπορεί να γίνει με χρήση λογαριασμού Microsoft, ηλεκτρονική διεύθυνση (email address) και αριθμό τηλεφώνου.

Η εφαρμογή από τον Αύγουστο του 2018 υποστηρίζει κρυπτογραφία end-to-end και χρησιμοποιεί τα πρωτόκολλα RSA-1536 & 2048 / AES256 / SHA- 1 τα οποία ίσως πρέπει να μελετηθούν ξανά από την εταιρεία λόγω της ευκολίας τους στο να αποκρυπτογραφηθούν. Επιπλέον το Skype χρησιμοποιεί το TLS/Noise πρωτόκολλο για κρυπτογραφία της κίνησης δικτύου.



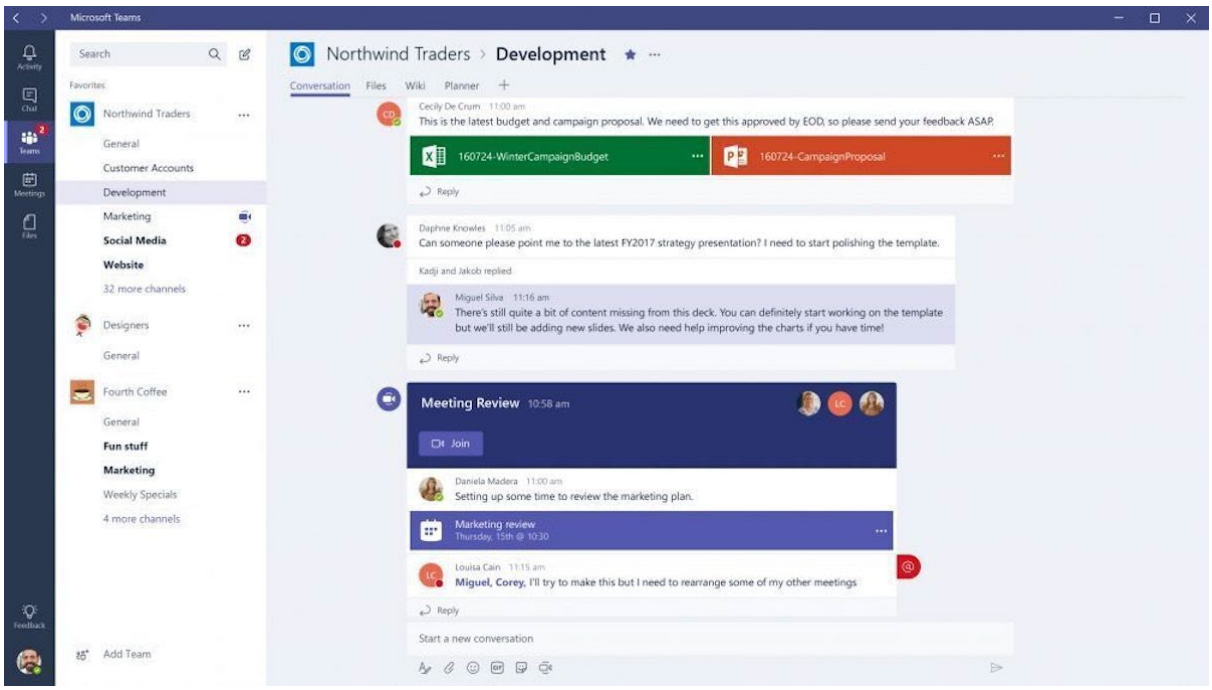
Εικόνα 4.9: Στιγμιότυπο από την εφαρμογή Skype σε κινητή συσκευή. [33]

4.10 Teams

Το Teams είναι πλατφόρμα επικοινωνίας της εταιρείας Microsoft και προσφέρεται κυρίως για επικοινωνία στον επαγγελματικό ή εργασιακό χώρο. Προσφέρει στο χρήστη τη δυνατότητα ανταλλαγής μηνυμάτων, τηλεδιασκέψεων, αποθήκευσης αρχείων είτε σε ιδιωτικά δωμάτια είτε σε δωμάτια σχεδιασμένα για εργασία. Η εφαρμογή είναι προσβάσιμη και από κινητή συσκευή πέραν από τον ηλεκτρονικό υπολογιστή και για τη δημιουργία λογαριασμού απαιτείται λογαριασμός Microsoft. Από τις αρχές της πανδημίας και λόγων των απαγορευτικών οι συναντήσεις αναγκαστικά γίνονταν διαδικτυακά και το Teams ήταν ένα από τα πιο διάσημα εργαλεία για αυτό.

Η πλατφόρμα κρυπτογραφεί τα δεδομένα τα οποία μεταφέρονται στο δίκτυο χρησιμοποιώντας end-to-end κρυπτογραφία αλλά επιτρέπει σε εξουσιοδοτημένες υπηρεσίες να τα αποκρυπτογραφήσουν για σκοπούς καταγραφής και διατήρησης των δεδομένων. Η

κρυπτογραφία end-to-end δεν είναι ενεργοποιημένη από προεπιλογή αλλά πρέπει να ενεργοποιηθεί από τον χρήστη.



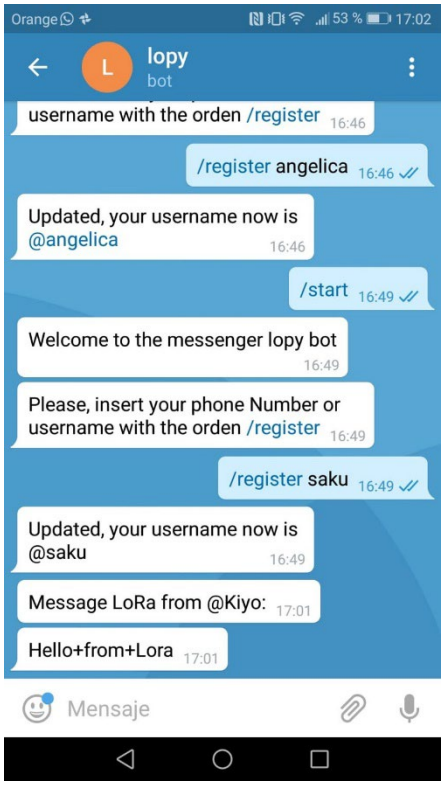
Εικόνα 4.10: Στιγμιότυπο από την εφαρμογή Teams και την αποστολή μηνυμάτων σε ομάδα. [34]

4.11 Telegram

Το Telegram είναι cloud-based εφαρμογή ανταλλαγής άμεσων μηνυμάτων. Οι διακομιστές της εφαρμογής είναι σκόρπιοι ανά το παγκόσμιο για να πετυχαίνετε μείωση στην υπερφόρτωση δεδομένων. Με τον όρο cloud-based εννοούμε ότι τα μηνύματα βρίσκονται στο σύννεφο δικτυακά και είναι προσβάσιμα σε πέραν από μία συσκευές. Οι χρήστες έχουν δυνατότητα ανταλλαγής μηνυμάτων και πολυμέσων, βιντεοκλήσεων και φωνητικών κλήσεων. Αυτό που κάνει την εφαρμογή να ξεχωρίζει είναι η διαδραστικότητα χρήστη με Chatbot τα οποία τρέχουν προγράμματα από πίσω και η υπηρεσία Channels όπου μόνο ο διαχειριστής μπορεί να γράψει και οι χρήστες μπορούν μόνο να το ακολουθήσουν (follow). Η εφαρμογή είναι προσβάσιμη και από κινητή συσκευή και από υπολογιστή αλλά με λιγότερες δυνατότητες.

Χρησιμοποιώντας το Telegram ο χρήστης έχει end-to-end κρυπτογραφία στις φωνητικές κλήσεις και βιντεοκλήσεις. Τα μηνύματα λόγω του ότι συγχρονίζονται στο σύννεφο (cloud)

προστατεύονται με το πρωτόκολλο MTProto το οποίο δημιουργήθηκε από προγραμματιστές της εταιρείας και είναι βασισμένο σε AES256 / RSA2048 / SHA-256.



Εικόνα 4.11: Παράδειγμα διαδραστικότητας χρήστη με Bot στο Telegram. [35]

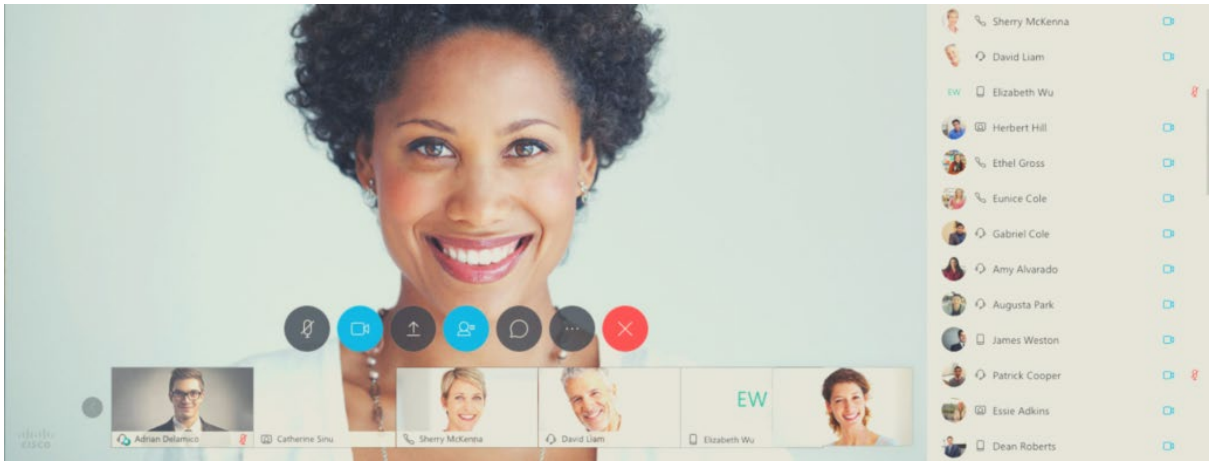
4.12 Viber

Το Viber είναι δωρεάν εφαρμογή Voice over IP κλήσεων και ανταλλαγής άμεσων μηνυμάτων. Ανήκει στην Γιαπωνέζικη εταιρεία Rakuten και είναι προσβάσιμο τόσο από ηλεκτρονικό υπολογιστή όσο και από κινητή συσκευή. Για τη δημιουργία λογαριασμού απαιτείται αριθμός τηλεφώνου χωρίς οποιαδήποτε άλλη εναλλακτική μέθοδο. Οι χρήστες έχουν τη δυνατότητα ανταλλαγής μηνυμάτων και ψηφιακού περιεχομένου, φωνητικών κλήσεων και βιντεοκλήσεων. Εκτός των πιο πάνω, υπάρχει η δυνατότητα τηλεφωνίας μέσω παραδοσιακής γραμμής τηλεφώνου επί πληρωμή.

Η εφαρμογή από το 2016 υποστηρίζει κρυπτογραφία end-to-end αλλά μόνο στις ένας με ένας και ομαδικές συνομιλίες και υπό την προϋπόθεση ότι όλοι χρησιμοποιούν την τελευταία έκδοση. Η κρυπτογραφία της (εφαρμογής) βασίζεται σε Curve25519 256 / Salsa20 128 / HMAC-SHA256.

4.13 Webex Meet

Το Webex Meet είναι μία cloud-based εφαρμογή της εταιρείας Cisco η οποία προσφέρει υπηρεσίες τηλεδιασκέψεων, βιντεοκλήσεων, φωνητικών κλήσεων και διαδικτυακών συναντήσεων. Επιπλέον η εφαρμογή προσφέρει ανταλλαγή μηνυμάτων και ψηφιακού περιεχομένου πριν και κατά τη διάρκεια μίας κλήσης. Δυστυχώς δεν γνωρίζουμε πολλά για την ασφάλεια της εφαρμογής αλλά το ότι υποστηρίζει κρυπτογραφία end-to-end είναι θετικό.



Εικόνα 4.1: Παράδειγμα διαδικτυακής συνάντησης με χρήση της εφαρμογής Webex Meet. [36]

4.14 WeChat

Το WeChat είναι εφαρμογή με πολλές δυνατότητες από την κινέζικη εταιρεία Tencent. Λόγω των πολλών δυνατοτήτων της πολλοί την θεωρούν ως «app for everything», δηλαδή εφαρμογή για τα πάντα. Αρχικά, προσφέρει στο χρήστη δυνατότητα ανταλλαγής άμεσων μηνυμάτων και ψηφιακού περιεχομένου, φωνητικών κλήσεων και βιντεοκλήσεων. Επιπλέον λειτουργεί και ως κοινωνικό δίκτυο με παιχνίδια, κοινοποίηση φωτογραφιών και βίντεο και δίνει και τη δυνατότητα διαδικτυακών πληρωμών. Η εφαρμογή είναι προσβάσιμη από ηλεκτρονικό υπολογιστή και κινητή συσκευή. Δημιουργία λογαριασμού επιτρέπεται με αριθμό κινητού τηλεφώνου μετά από πρόσκληση από υφιστάμενο χρήστη της εφαρμογής ή μέσω λογαριασμού Facebook.

Η εφαρμογή δεν υποστηρίζει κρυπτογραφία end-to-end και τρέχει κάτω από το κινέζικο δίκαιο. Με βάση το δίκαιο της Κίνας επιτρέπεται η ανάλυση, καταγραφή και δημοσιοποίηση στις κινέζικες αρχές της δραστηριότητας των χρηστών στην εφαρμογή ως μέρος της μαζικής επιτήρησης που υπάρχει στη χώρα.

4.15 WhatsApp

Το WhatsApp είναι κεντρικοποιημένη εφαρμογή ανταλλαγής άμεσων μηνυμάτων και Voice over IP (VoIP) υπηρεσιών. Είναι προσβάσιμη από κινητή συσκευή και ηλεκτρονικό υπολογιστή και για την εγγραφή απαιτείται αριθμός τηλεφώνου. Παρέχει στο χρήστη δυνατότητα ανταλλαγής μηνυμάτων και πολυμέσων – ψηφιακού περιεχομένου, διεξαγωγής φωνητικών κλήσεων και βιντεοκλήσεων. Επιπλέον υπάρχει η έκδοση WhatsApp Business μέσω της οποίας οι εταιρείες μπορούν να επικοινωνούν με τους πελάτες τους οι οποίοι χρησιμοποιούν την απλή εφαρμογή. Είναι μία από τις πιο δημοφιλής εφαρμογές του είδους της με πέραν των δύο δισεκατομμυρίων χρηστών το 2020.

Η εφαρμογή παρέχει κρυπτογραφία end-to-end κατά την ανταλλαγή μηνυμάτων βασισμένη στο Signal protocol το οποίο βασίζεται στα κρυπτογραφικά πρωτόκολλα Curve25519 / AES-256 / HMAC-SHA256. Οι φωνητικές κλήσεις κρυπτογραφούνται χρησιμοποιώντας το Secure Real-time Transport Protocol (SRTP) και από το 2021 η εφαρμογή προσφέρει κρυπτογραφία end-to-end και στα αντίγραφα ασφαλείας σε κινητές συσκευές με λειτουργικό σύστημα Android ή iOS εάν το επιθυμεί ο χρήστης.

4.16 Wire

Το Wire είναι εφαρμογή ανταλλαγής μηνυμάτων και συνεργασίας (collaboration) διαθέσιμη σε κινητές συσκευές, υπολογιστές και μέσω περιηγητών ιστού (web browsers). Η εφαρμογή προσφέρει τη δυνατότητα ανταλλαγής μηνυμάτων και ψηφιακού περιεχομένου, φωνητικών κλήσεων, βιντεοκλήσεων και τηλεδιασκέψεων.

Από το σχεδιασμό της εφαρμογής καθορίστηκαν η ασφάλεια και η ιδιωτικότητα ως βασικές αξίες. Παρέχεται κρυπτογραφία end-to-end στην αποστολή μηνυμάτων χρησιμοποιώντας το δικό τους πρωτόκολλο με όνομα Proteus βασισμένο στα πρωτόκολλα X25519 / XSalsa20 256 / Poly1305 και στο Signal Protocol. Στις φωνητικές κλήσεις η κρυπτογραφία γίνεται με τη χρήση του Datagram Transport Layer Security (DTLS) και του Secure Real-time Transport Protocol (SRTP). Επιπλέον η εφαρμογή χρησιμοποιεί το πρωτόκολλο TLS/Noise για κρυπτογραφία της κίνησης δικτύου (network traffic).

4.17 Zalo

Το Zalo είναι εφαρμογή ανταλλαγής μηνυμάτων και φωνητικών κλήσεων από την βιετναμέζικη εταιρεία VNG Corporation. Η εφαρμογή δεν είναι πολύ γνωστή στο δυτικό κόσμο αλλά είναι στις πρώτες προτιμήσεις στο Βιετνάμ και διατίθεται σε κινητή συσκευή και σε ηλεκτρονικό υπολογιστή. Η δημιουργία λογαριασμού στην εφαρμογή γίνεται μόνο με τη χρήση αριθμού τηλεφώνου. Δυστυχώς δεν έχουν γίνει γνωστά πολλά πράγματα για την ασφάλεια στην ανταλλαγή μηνυμάτων μέσω της εφαρμογής.

4.18 Zoom

Το Zoom (Meetings) είναι εφαρμογή τηλεδιασκέψεων από την εταιρεία Zoom Video Communications. Παρέχει τη δυνατότητα ανταλλαγής άμεσων μηνυμάτων και διεξαγωγής τηλεδιασκέψεων και κλήσεων Voice over IP (VoIP) μέσω δωρεάν και επί πληρωμή προγράμματος. Η δημιουργία λογαριασμού είναι απλή και γρήγορη με τη χρήση ηλεκτρονικής διεύθυνσης (email address) ή χρήση υφιστάμενου λογαριασμού π.χ. Google account ή Facebook account και η εφαρμογή τρέχει τόσο σε κινητή συσκευή όσο και σε ηλεκτρονικό υπολογιστή. Κατά τη διάρκεια της πανδημίας του COVID-19 οι χρήστες της εφαρμογής σημείωσαν ραγδαία αύξηση μιας και ήταν εύκολη η χρήση της για δουλειά από το σπίτι, τηλεκπαίδευση και επικοινωνία μεταξύ φίλων και συγγενών.

Η ραγδαία αύξηση χρηστών εμφάνισε και προβλήματα στην ασφάλεια και ιδιωτικότητα της εφαρμογής με την εταιρεία να τρέχει να τα μπαλώσει. Τα προβλήματα στην ιδιωτικότητα εμφανίστηκαν με τη δημοσίευση ενός άρθρου όπου σε αυτόν αναφερόταν ότι η εφαρμογή σε συσκευή με iOS λειτουργικό σύστημα σύλλεγε πληροφορίες για τη συσκευή και τις απόστελλε στο Facebook χωρίς να ενημερώνει το χρήστη. Ένα μήνα μετά γίνεται γνωστό ότι μία λειτουργία συλλογής πληροφοριών της εφαρμογής απόστελλε ονόματα χρηστών και ηλεκτρονικές διευθύνεις στο LinkedIn με την εταιρεία να το απενεργοποιεί άμεσα και πριν προλάβει να καταλαγιάσει το συγκεκριμένο θέμα έρχεται η είδηση ότι η εφαρμογή δεν προσφέρει κρυπτογραφία end-to-end. Μέσα στον πανικό των πιο πάνω ζητημάτων οι χρήστες κατάφεραν να βρούνε τρόπο να εισέρχονται σε συναντήσεις άλλων ατόμων λόγω μίας ευπάθειας και να προκαλούν προβλήματα στην ομαλή διεξαγωγή τους. Εξ αυτών, η εταιρεία προχώρησε σε εφαρμογή κρυπτογραφίας end-to-end, εισαγωγή των πρωτοκόλλων TLS 1.2 (Transport Layer

Security) και SRTP (Secure Real-time Transport Protocol) και κρυπτογραφία στις συναντήσεις πραγματικού χρόνου χρησιμοποιώντας τον 256-bit AES-GCM.

Κεφάλαιο 5
Πρακτική/ερευνητική μελέτη εφαρμογών

Μετά την επιλογή των εφαρμογών και την παρουσίαση τους στο προηγούμενο κεφάλαιο σειρά έχει η μελέτη η οποία έγινε σε περιβάλλον δοκιμών με χρήση κατάλληλων εργαλείων. Σκοπός της μελέτης σε περιβάλλον δοκιμών είναι η διερεύνηση των εφαρμογών συνομιλιών/τηλεδιασκέψεων ως προς την επεξεργασία προσωπικών δεδομένων την οποία πραγματοποιούν. Τα εργαλεία τα οποία επιλέχθηκαν προσφέρουν μεταξύ άλλων ανάλυση της κίνησης δικτύου (network traffic) των εφαρμογών αλλά και ανάλυση των πολιτικών ασφάλειας τους.

5.1 Περιβάλλον δοκιμών

Για τη διεξαγωγή της μελέτης των εφαρμογών συνομιλιών/τηλεδιασκέψεων δημιουργήθηκε το κατάλληλο περιβάλλον δοκιμών αποτελούμενο τόσο από διαδικτυακά εργαλεία όσο και από εργαλεία τα οποία χρειάζονταν εγκατάσταση σε κατάλληλο εξοπλισμό. Επελέγησαν εργαλεία τα οποία έχουν αξιοποιηθεί σε αντίστοιχες έρευνες.

Αρχικά ο εξοπλισμός αποτελείτο από ένα κινητό τηλέφωνο Samsung Galaxy S6 με εγκατεστημένο το λειτουργικό σύστημα Android 7 και για τις ανάγκες μας χρειάστηκε να γίνει Root, αποκτώντας περαιτέρω προνόμια και δυνατότητες στη συσκευή. Περαιτέρω, χρησιμοποιήθηκε ένας σταθερός ηλεκτρονικός υπολογιστής με λειτουργικό σύστημα Windows 10 και Wireless USB Adapter με Main Chipset Ralink RT5370.

Όσο αφορά τα εργαλεία τα οποία χρησιμοποιήθηκαν, αυτά είναι, με τη σειρά που παρουσιάζονται πιο κάτω, τα εξής: η διαδικτυακή εφαρμογή (web application) Exodus Privacy και οι εφαρμογές κινητών συσκευών Lumen privacy monitoring app και Inspeckage. Η παρουσίαση των εν λόγω εργαλείων θα γίνει με βάση τις δοκιμές που εκτελέστηκαν σε μία εκ των εφαρμογών που μελετήθηκαν – και, συγκεκριμένα, της Discord. Τέλος, χρησιμοποιήθηκε το εικονικό περιβάλλον που έχει αναπτύξει ο οργανισμός Privacy International για παρακολούθηση των δεδομένων των εφαρμογών τα οποία μεταδίδουν σε πραγματικό χρόνο. Το περιβάλλον αυτό εγκαταστάθηκε στο σταθερό ηλεκτρονικό υπολογιστή.

Ο λόγος για τον οποίο επελέγησαν πολλά διαφορετικά εργαλεία για την ανάλυση της κάθε εφαρμογής έγκειται στο ότι το κάθε ένα εξ αυτών των εργαλείων έχει κάποιους περιορισμούς – για παράδειγμα, κάποια εκ των εργαλείων δεν είναι σε θέση να καταγράψουν ολόκληρη την εξερχόμενη από τις εφαρμογές κίνηση εφόσον είναι κρυπτογραφημένη.

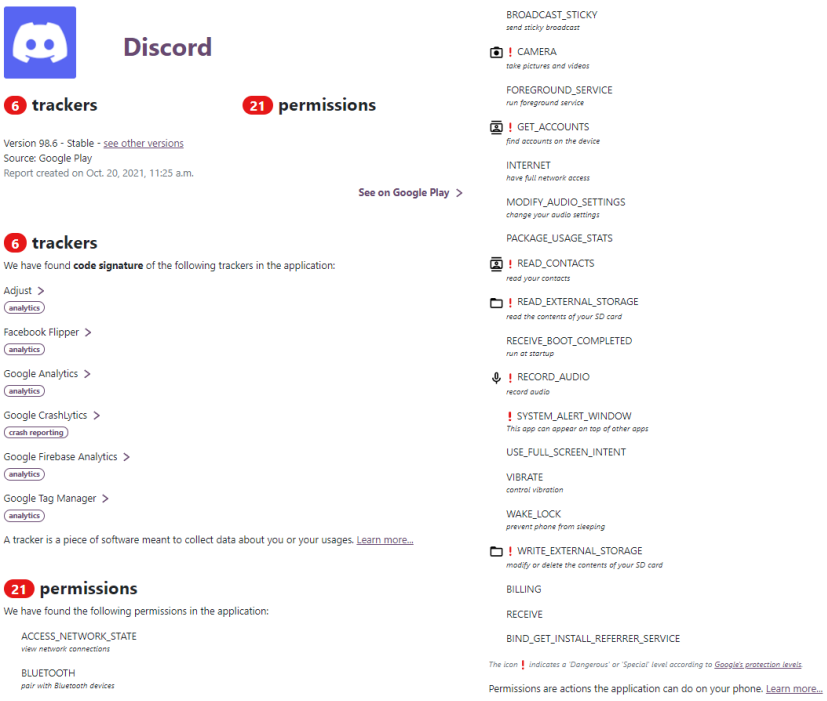
5.1.1 Exodus Privacy

Το Exodus Privacy είναι ένας γαλλικός μη κερδοσκοπικός οργανισμός τον οποίο διαχειρίζονται ακτιβιστές οι οποίοι είναι υπέρμαχοι της ιδιωτικότητας. Σκοπός του οργανισμού, όπως αυτός αναφέρεται στη σελίδα του, είναι να ευαισθητοποιήσουν τον κόσμο, με τη βοήθεια εργαλείων ανάλυσης και διδακτικού υλικού ,σχετικά με την παρακολούθηση η οποία γίνεται από εφαρμογές Android. [37]

Με πιο απλά λόγια, το exodus αναλύει εφαρμογές Android ψάχνοντας για ενσωματωμένους ιχνηλάτες (embedded trackers) παραθέτοντας λίστα με αυτούς εάν εντοπιστούν. Ως ιχνηλάτη (tracker) θεωρούμε ένα κομμάτι κώδικα το οποίο συλλέγει δεδομένα για το χρήστη και τη χρήση της εφαρμογής από αυτόν. Επιπλέον, η εφαρμογή Exodus, στη λίστα την οποία παραθέτει, παρουσιάζει και τα δικαιώματα (permissions) κάθε εφαρμογής, επισημαίνοντας ειδικώς (με κόκκινο θαυμαστικό) εάν ένα δικαίωμα ανήκει στην κατηγορία των Επικίνδυνων δικαιωμάτων (Dangerous permissions). [38]

Η χρήση του εργαλείου για τους σκοπούς της παρούσας διπλωματικής έγινε τον Οκτώβριο του 2021 και μελετήθηκαν και οι δεκαοχτώ εφαρμογές οι οποίες παρουσιάστηκαν στο προηγούμενο κεφάλαιο. Ενδεικτικά, παρατίθεται η μελέτη του Discord στο παρόν κεφάλαιο ενώ όλες οι σχετικές εικόνες από την ανάλυση των εφαρμογών παρατίθενται στο Παράρτημα Α.

Στην εφαρμογή Discord εντοπίστηκαν έξι ιχνηλάτες, οι οποίοι αποτελούνται από το Adjust, το Facebook Flipper και τα Google Analytics, Crashlytics, Firebase Analytics και Tag Manager. Αξιοσημείωτο ότι οι τέσσερις από τους έξι είναι από την εταιρεία Google. Όσο αφορά τα δικαιώματα (permissions) της εφαρμογής εντοπίστηκαν εικοσιένα με επτά από αυτά να ανήκουν στην κατηγορία των επικίνδυνων δικαιωμάτων (dangerous permissions) όπως αυτά καταγράφονται στον Πίνακα . Στην πιο κάτω εικόνα, στο στιγμιότυπο από την εφαρμογή Exodus παρουσιάζονται οι ιχνηλάτες και τα permissions της εφαρμογής Discord.



Εικόνα 5.1: Στιγμιότυπο από την ανάλυση της εφαρμογής Discord με τη χρήση του εργαλείου Exodus privacy.

CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	RECORD_AUDIO	SYSTEM_ALERT_WINDOW
WRITE_EXTERNAL_STORAGE		

Πίνακας 5.2: Τα επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν από την ανάλυση της εφαρμογής Discord με τη χρήση του εργαλείου Exodus Privacy.

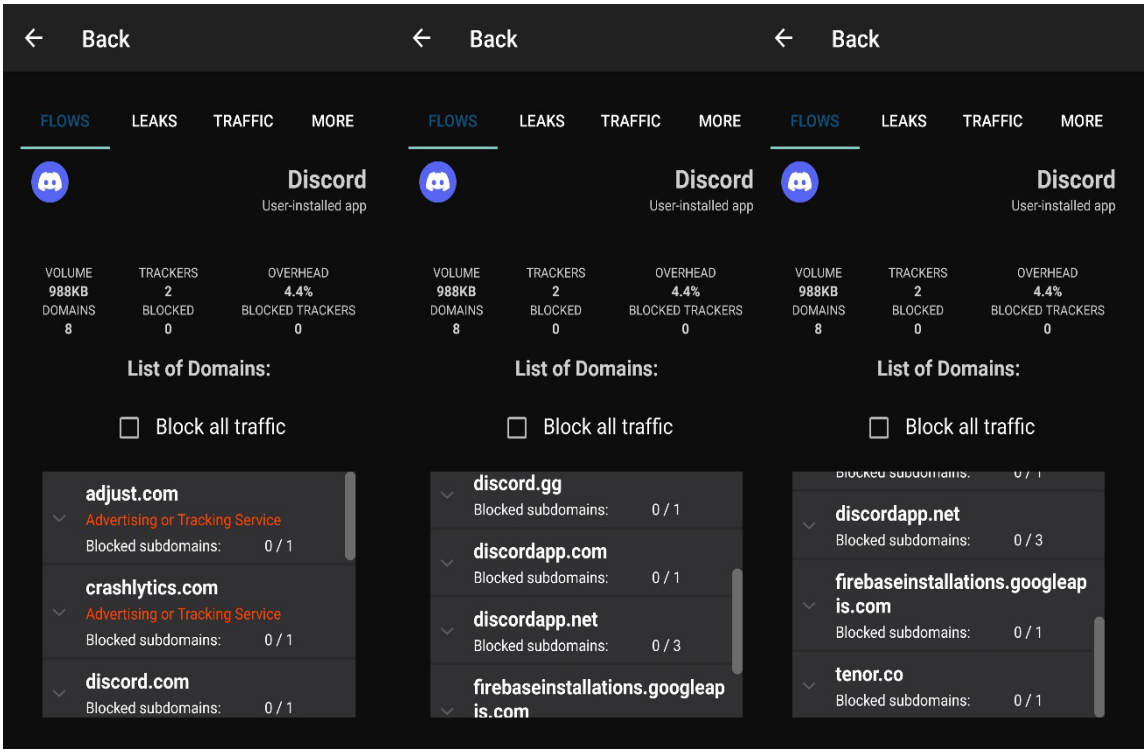
5.1.2 Lumen privacy monitoring app

Το Lumen app αποτελεί βασικό άξονα του ερευνητικού έργου Haystack Project, ακαδημαϊκής πρωτοβουλίας από ανεξάρτητους ακαδημαϊκούς ερευνητές του Διεθνές Ινστιτούτου Επιστήμης Υπολογιστών (ICSI), του University of California, Berkeley (UC Berkeley) και του IMDEA Networks. Το έργο χρηματοδοτείται από το Εθνικό Ίδρυμα Επιστήμης (National Science Foundation – NSF) και το Εργαστήριο Διαφάνειας Δεδομένων (DataTransparencyLabs – DTL).

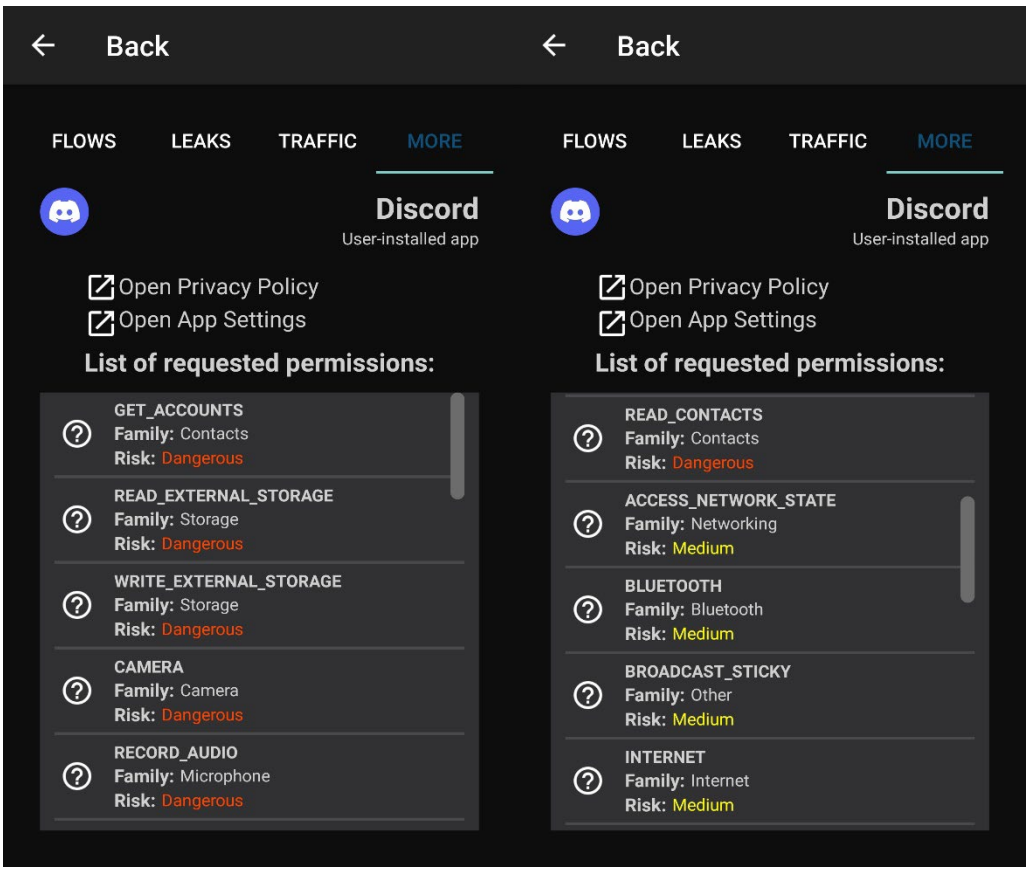
Η εφαρμογή εγκαθίσταται σε κινητές συσκευές μέσω του Google Play store ή μέσω apk αρχείου. Με την εγκατάστασή της η εφαρμογή χρησιμοποιεί τα δικαιώματα εγκαθίδρυσης VPN στο Android για να αναλύσει την κίνηση (traffic) των εφαρμογών που είναι εγκατεστημένες στη συσκευή. Το VPN εκτελείται στη συσκευή (local) και λειτουργεί ως ενδιάμεσος σταθμός (middleware) μεταξύ των εφαρμογών και των πακέτων των οποίων αποστέλλουν αναγνωρίζοντας τον τελικό τους σταθμό (endpoints). Για να μπορέσει η εφαρμογή να διαβάσει και να αναλύσει την κρυπτογραφημένη κίνηση (encrypted traffic) των εφαρμογών η οποία εξέρχεται μέσω του πρωτοκόλλου TLS απαιτείται η εγκατάσταση ενός πιστοποιητικού TLS (TLS certificate). Μέσω της ανάλυσης ο χρήστης μπορεί να δει τα προσωπικά δεδομένα τα οποία συλλέγει μία εφαρμογή, να αποκλείσει ανεπιθύμητες ροές και να διαμορφώσει τις άδειες τις εφαρμογής έτσι ώστε να έχει καλύτερο έλεγχο της ιδιωτικότητας και των προσωπικών δεδομένων του.

Με την εγκατάσταση της εν λόγω εφαρμογής στην κινητή συσκευή Samsung Galaxy S6 (Android 7) εξετάστηκαν οι εφαρμογές οι οποίες παρουσιάστηκαν στο Κεφάλαιο 4 με κάποιες να μην εντοπίζονται και να αναλύονται από την εφαρμογή. Ενδεικτικά, παρατίθεται η μελέτη του Discord στο παρόν κεφάλαιο ενώ όλες οι εικόνες από την ανάλυση των εφαρμογών με τη χρήση του εργαλείου Lumen παρατίθενται στο Παράρτημα Α.

Η εφαρμογή Discord αποστέλλει δεδομένα σε οχτώ διαφορετικά domains με τα τέσσερα από αυτά να ανήκουν στην Discord (discord.com, discord.gg, discordapp.com, discordapp.net) και τα δύο να χαρακτηρίζονται ως Advertising or Tracking Service (adjust.com, crashlytics.com) όπως φαίνεται στην Εικόνα 5.3. Το Lumen δεν εντόπισε διαρροές προσωπικών δεδομένων σε τρίτους, όπως προκύπτει εξετάζοντας την ενότητα Leaks που διαθέτει η διεπαφη (interface) του εργαλείου. Όσο αφορά τα δικαιώματα τα οποία δόθηκαν στην εφαρμογή εντοπίστηκαν εικοσιένα όπως και στην ανάλυση με το εργαλείο Exodus αλλά έξι κατηγοριοποιήθηκαν ως επικίνδυνα (dangerous) σε αντίθεση με τα επτά από την ανάλυση με το εργαλείο Exodus.



Εικόνα 5.3: Στιγμιότυπο από την ανάλυση της εφαρμογής Discord με τη χρήση του εργαλείου Lumen και τις ροές της εφαρμογής προς servers.



Εικόνα 5.4: Στιγμιότυπο από την ανάλυση της εφαρμογής Discord με τη χρήση του εργαλείου Lumen και τα επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν.

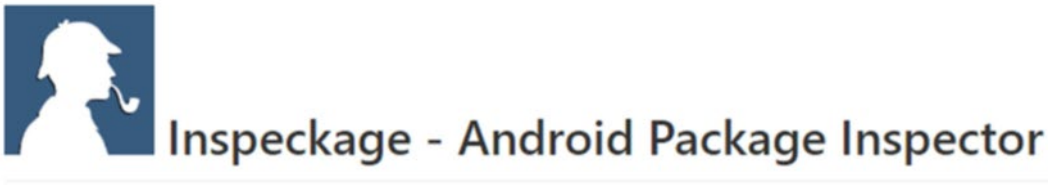
5.1.3 Xposed Framework

Το Xposed Framework είναι πλατφόρμα η οποία επιτρέπει την εγκατάσταση διαφόρων modules σε συσκευές με λειτουργικό σύστημα Android δίνοντας τη δυνατότητα στο χρήστη να αλλάξει τη λειτουργία και την εμφάνισή τους. Η εγκατάσταση γίνεται μέσω του Xposed Installer και η πλατφόρμα απαιτεί δικαιώματα διαχειριστή (root) στη συσκευή για να αποκτήσει πρόσβαση σε πόρους του πυρήνα του Android και μέσω αυτού να εκτελεστούν τα διάφορα modules.

Για τις ανάγκες της παρούσας διπλωματικής έγινε η εγκατάσταση δύο modules τα οποία βοήθησαν στην ανάλυση των δεδομένων των εφαρμογών συνομιλιών/τηλεπικοινωνιών. Τα modules είναι:

- Inspeckage: Είναι ένα εργαλείο το οποίο προσφέρει δυναμική ανάλυση εφαρμογών Android παρέχοντας hooks σε κάποια functions του Android API. Μέσω του συγκεκριμένου module γίνονται κατανοητές οι διαδικασίες των εφαρμογών Android οι

οποίες λαμβάνουν χώρα κατά την εκκίνηση τους. Ανοίγοντας την εφαρμογή ενεργοποιείται ένας εσωτερικός HTTP Server σε συγκεκριμένη IP διεύθυνση προσβάσιμη μέσω συσκευής ενωμένης στο ίδιο δίκτυο παρέχοντας στο χρήστη ένα φιλικό γραφικό περιβάλλον. Μέσω του μενού του Inspeckage επιλέγεται και η εφαρμογή η οποία θα αναλυθεί.



Εικόνα 5.5: Το λογότυπο του εργαλείου Inspeckage [39]

Ενδεικτικά στην πιο κάτω εικόνα φαίνονται τα εικοσιένα Permissions τα οποία εντόπισε η ανάλυση με τη χρήση του εργαλείου Inspeckage στην εφαρμογή Discord ενώ όλες οι εικόνες από την ανάλυση όλων των εφαρμογών με το συγκεκριμένο εργαλείο βρίσκονται στο Παράρτημα Α.

Requested Permissions

com.android.vending.BILLING
android.permission.ACCESS_NETWORK_STATE
android.permission.BLUETOOTH
android.permission.BROADCAST_STICKY
android.permission.INTERNET
android.permission.GET_ACCOUNTS
android.permission.READ_EXTERNAL_STORAGE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.CAMERA
android.permission.FOREGROUND_SERVICE
android.permission.RECORD_AUDIO
android.permission.MODIFY_AUDIO_SETTINGS
android.permission.PACKAGE_USAGE_STATS
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.USE_FULL_SCREEN_INTENT
android.permission.SYSTEM_ALERT_WINDOW
android.permission.READ_CONTACTS
com.google.android.c2dm.permission.RECEIVE
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
android.permission.RECEIVE_BOOT_COMPLETED

Εικόνα 5.6: Τα δικαιώματα (permissions) τα οποία εντοπίστηκαν κατά την ανάλυση του Discord με τη χρήση του εργαλείου Inspeckage.

- SSLUnpinning: Module το οποίο τροποποιεί διάφορα κομμάτια κώδικα στις κλάσεις του SSL (SSL Classes) έτσι ώστε να παρακαμφθούν οι έλεγχοι πιστοποιητικού (certificate verifications) μίας συγκεκριμένης εφαρμογής. Αυτό καθιστά εφικτή την ανάλυση της κίνησης (traffic) και των δεδομένων τα οποία απέστειλε η εφαρμογή, ακόμα και αν είναι κρυπτογραφημένα

Εικόνα 5.7: Το λογότυπο του εργαλείου SSLUnpinning [40]

5.1.4 Privacy International's data interception environment

Ο φιλανθρωπικός οργανισμός Privacy International (PI) με έδρα το Ηνωμένο Βασίλειο και στόχο την υπεράσπιση του δικαιώματος στην ιδιωτικότητα σε όλο τον κόσμο, διέθεσε το Φεβρουάριο του 2019 το δικό του περιβάλλον παρακολούθησης δεδομένων για τη διερεύνηση εφαρμογών και τον έλεγχο της λειτουργίας τους. Η χρήση του περιβάλλοντος είναι δωρεάν και βρίσκεται στη διεύθυνση https://privacyinternational.org/node/2732#privacy-internationals-data-interception-environment μαζί με οδηγίες εγκατάστασης, τα προ απαιτούμενα και το αρχείο για τη δημιουργία της εικονικής μηχανής.

Για την εγκατάσταση και χρήση του εικονικού περιβάλλοντος χρειαζόμαστε:

- Ηλεκτρονικό υπολογιστή με τουλάχιστον 2GB RAM και dual-core processor
- Oracle VM VirtualBox 6.x
- Το αρχείο του εικονικού περιβάλλοντος από τη σελίδα του οργανισμού "Privacy-International-data-interception-environment-stable-2.1.2.ova"
- Wi-Fi USB Dongle με Ralink 5370 Chipset

- Κινητή συσκευή Android με δικαιώματα διαχειριστή (rooted) και ADB enabled. Στην περίπτωση μας το Samsung Galaxy S6 με Android 7.

Πριν προχωρήσουμε στην εγκατάσταση του εικονικού περιβάλλοντος περιγράφονται κάποια στοιχεία του τα οποία εργάζονται μαζί για να επιτρέψουν την υποκλοπή δεδομένων στις εφαρμογές κατά τη μεταφορά στο δίκτυο(while in transit), όπως αυτά περιγράφονται στη σελίδα του Privacy International.. Αυτά είναι:

Virtualbox (6.x)

Το Virtualbox είναι ένας δωρεάν διαχειριστής εικονικής μηχανής πολλαπλών πλατφορμών. Με πιο απλά λόγια, επιτρέπει την εκτέλεση ενός λειτουργικού συστήματος μέσα σε ένα άλλο προσομοιώνοντας εικονικά τα χαρακτηριστικά ενός φυσικού ηλεκτρονικού υπολογιστή. Το λειτουργικό σύστημα μέσα σε μία εικονική μηχανή τρέχει με τη χρήση πόρων της φυσικής μηχανής και έχει το πλεονέκτημα του ότι μπορεί να μετακινηθεί και να χρησιμοποιηθεί σε μία άλλη μηχανή. Επιπλέον οποιαδήποτε δραστηριότητα γίνεται μέσα στην εικονική μηχανή περιορίζεται εκεί χωρίς να επηρεάζει το κυρίως λειτουργικό σύστημα του υπολογιστή.

Debian10 (Buster)

Το Debian είναι μία διανομή του GNU / Linux, αρχιτεκτονικής πυρήνα και λειτουργικού συστήματος τύπου UNIX.

mitmproxy (4.0.4)

Το mitmproxy είναι ένας ανοιχτού κώδικα διακομιστής μεσολάβησης (proxy) γραμμένος σε Python. Πιο συγκεκριμένα, λαμβάνει συνδέσεις στη μία πλευρά, τις ανοίγει και τις αναλύει και στη συνέχεια τις προωθεί στην άλλη πλευρά. Το βασικό χαρακτηριστικό του είναι ότι δημιουργεί όλα τα απαιτούμενα πιστοποιητικά σε πραγματικό χρόνο. Αυτό του το χαρακτηριστικό διασφαλίζει ότι η εισερχόμενη σύνδεση (από τον πελάτη – client), πιστεύει ότι ο διακομιστής μεσολάβησης είναι ο πραγματικός προορισμός. Σε αυτό το προ διαμορφωμένο περιβάλλον το mitmproxy έχει ρυθμιστεί σε «διαφανή (transparent)» λειτουργία. Αυτό σημαίνει ότι δεν χρειάζονται οποιεσδήποτε αλλαγές στις ρυθμίσεις του πελάτη (client) πέραν της εγκατάστασης του πιστοποιητικού (certificate) του mitmproxy.

dnsmasq (2.80) (Ενεργοποιημένο)

Το dnsmasq είναι ένας «ελαφρύς» (lightweight) διακομιστής DNS (Domain Name System) και DHCP (Dynamic Host Configuration Protocol) server. Εξυπηρετεί δύο σκοπούς:

1. Δίνει διευθύνσεις IP, επιτρέποντας στις συσκευές να προσχωρήσουν σε ένα υπάρχον δίκτυο χωρίς να χρειάζεται να διαμορφώσουν χειροκίνητα ρυθμίσεις για το συγκεκριμένο δίκτυο όπως διακομιστή DNS.

2. Εξυπηρετεί αιτήματα DNS. Περιλαμβάνει κυρίως τη μετατροπή ονομάτων τομέα (domain names) όπως το privacyinternational.org σε διευθύνσεις IP όπως το 144.76.205.68.

hostapd (2.6) (Απενεργοποιημένο)

Το hostapd είναι ένα διαμορφώσιμο δίκτυο 802.11 (Wireless LAN) το οποίο επιτρέπει τη διαμόρφωση ασύρματων συσκευών με πολλούς τρόπους. Είναι απενεργοποιημένο στο συγκεκριμένο περιβάλλον σε περίπτωση που δεν χρησιμοποιηθεί κατάλληλο WLAN controller αλλά μπορεί εύκολα να ενεργοποιηθεί.

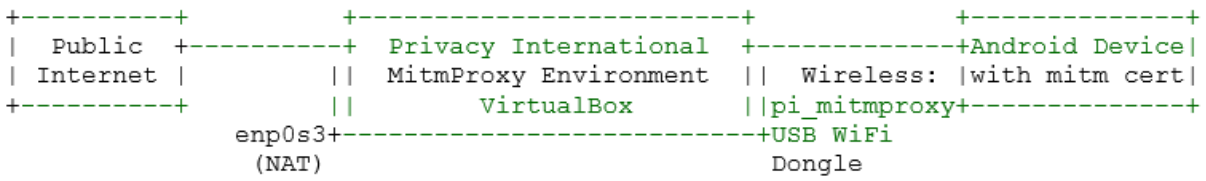
iptables (1.8.2)

Το iptables είναι το τυπικό σύστημα τείχους προστασίας (firewall system) σε πολλά λειτουργικά συστήματα βασισμένα σε Linux. Χρησιμοποιεί έναν πίνακα κανόνων, ο οποίος είναι αναγνώσιμος από τους ανθρώπους, για να κατηγοριοποιήσει και να χειριστεί την κίνηση (traffic) μέσω ενός συνόλου γνωστών καταστάσεων δικτύωσης (known networking states). Στο συγκεκριμένο σύνολο εργαλείων εξυπηρετεί δύο σκοπούς:

1. Τροφοδοτεί την κίνηση (traffic) από τις θύρες (ports) 80 (http) και 443 (https) στο mitmproxy.

2. Επιτρέπει σε άλλες συνδέσεις να «μεταμφιεστούν» έτσι ώστε το VM να λειτουργεί σαν δρομολογητής (router).

Διάταξη στοιχείων (Component Layout)



Εικόνα 5.8: Διάταξη στοιχείων του εικονικού περιβάλλοντος και σύνδεση με το διαδίκτυο [41]

Το πιο πάνω διάγραμμα περιγράφεται ως εξής:

- Το Διαδίκτυο (Internet) μπορεί να είναι ο οποιοσδήποτε τρόπος σύνδεσης στο διαδίκτυο.

- Ο προσαρμογέας 1 (Adapter) στο εικονικό περιβάλλον (enp0s3 μέσα στο VM) πρέπει να οριστεί ως συσκευή NAT. Αυτό σημαίνει ότι η VM θα χρησιμοποιήσει τη σύνδεση δικτύου του κεντρικού υπολογιστή (host) για να αποκτήσει πρόσβαση στο Διαδίκτυο χωρίς να απαιτούνται άλλες ρυθμίσεις εντός της εικονικής μηχανής (guest).

- Το Virtualbox VM θα πρέπει να εκκινήσει (boot) και το mitmproxy να εκτελείται πριν γίνει προσπάθεια να συνδεθούν οποιεσδήποτε συσκευές.

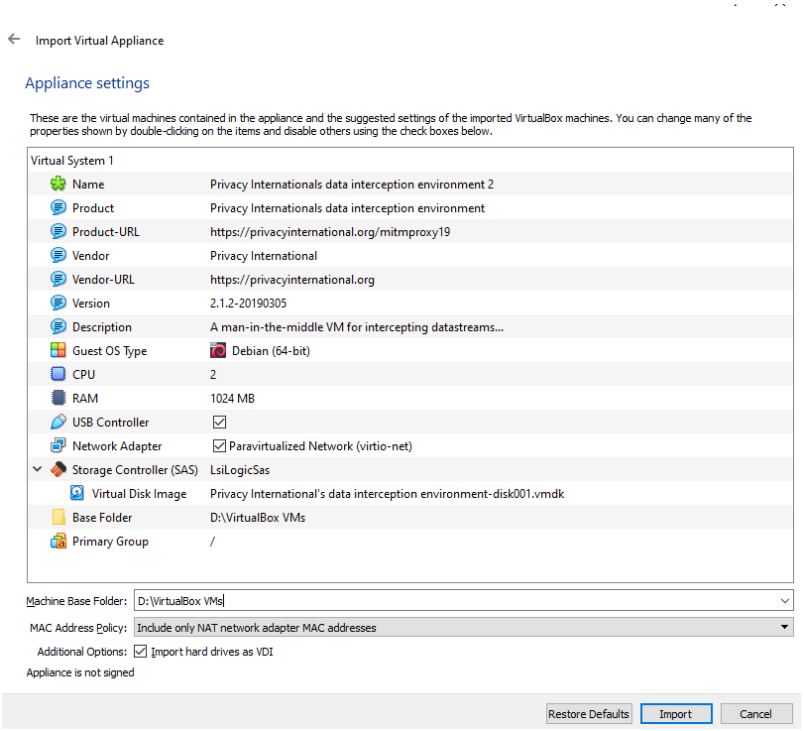
- Στα δεξιά του VM βρίσκεται ένα ασύρματο NIC (Network Interface Card), πιθανόν USB Dongle. Αυτό πρέπει να είναι απενεργοποιημένο και πρέπει να ρυθμιστεί προτού επιχειρήσει κάποιος να εκτελέσει το mitmproxy. Σε αυτό θα «φιλοξενηθεί» το ασύρματο δίκτυο pi_mitmproxy.

- Τέλος, στο άκρο δεξιά υπάρχει η συσκευή Android η οποία θα τύχει ανάλυσης. Για να δουλέψει θα πρέπει να συνδεθεί στο δίκτυο το οποίο παρέχεται από το ασύρματο NIC (pi_mitmproxy) και να γίνει εγκατάσταση του πιστοποιητικού mitmproxy.

5.1.5 Εγκατάσταση Εικονικού Περιβάλλοντος

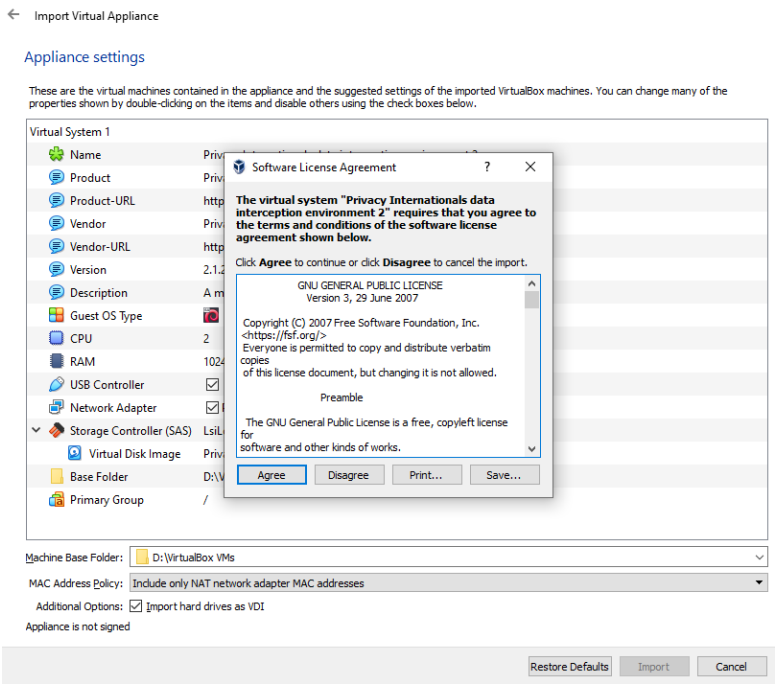
Η εγκατάσταση του εικονικού περιβάλλοντος του Privacy International απαιτεί τη χρήση του Oracle VM VirtualBox το οποίο βρίσκεται στη διεύθυνση https://www.virtualbox.org/wiki/Downloads. Μετά την εγκατάσταση της έκδοσης για υπολογιστή με λειτουργικό σύστημα Windows 10 κατεβάζουμε το αρχείο εικονικού περιβάλλοντος (Privacy-International-data-interception-environment-stable-2.1.2.ova) από τη

σελίδα του Οργανισμού. «Πατώντας» πάνω στο αρχείο .ova ανοίγει αυτόματα το VirtualBox για και ο οδηγός εγκατάστασης.



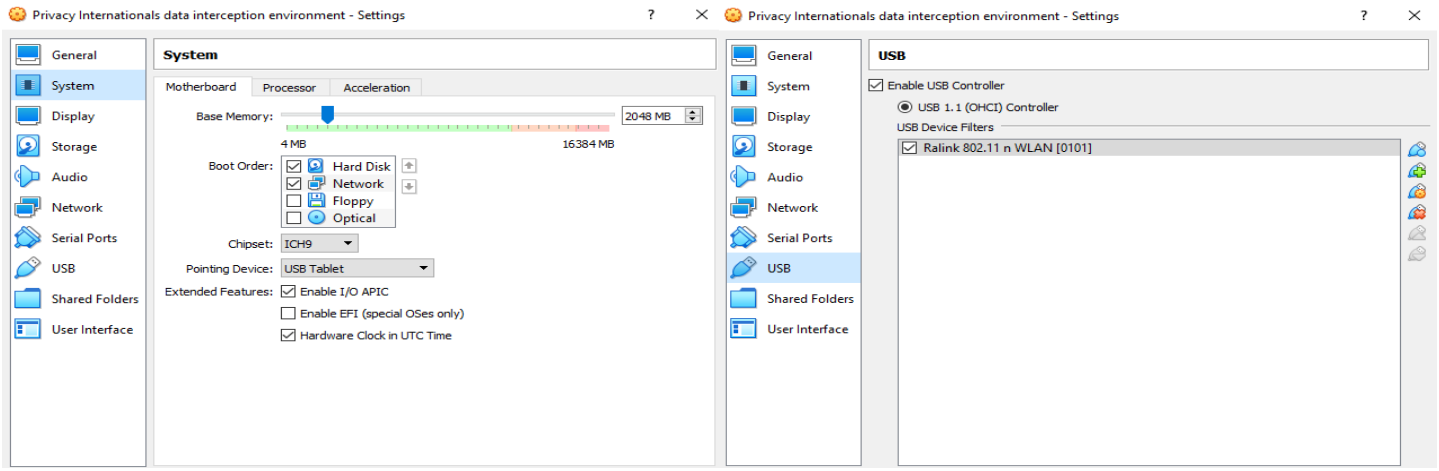
Εικόνα 5.9: Το παράθυρο του οδηγού εγκατάστασης του εικονικού περιβάλλοντος

Αφού επιλέξουμε το φάκελο στον οποίο θα γίνει η εγκατάσταση προχωράμε επιλέγοντας "Import" και "Agree", όπως φαίνεται πιο κάτω, και αφήνουμε την εγκατάσταση της εικονικής μηχανής να τελειώσει.



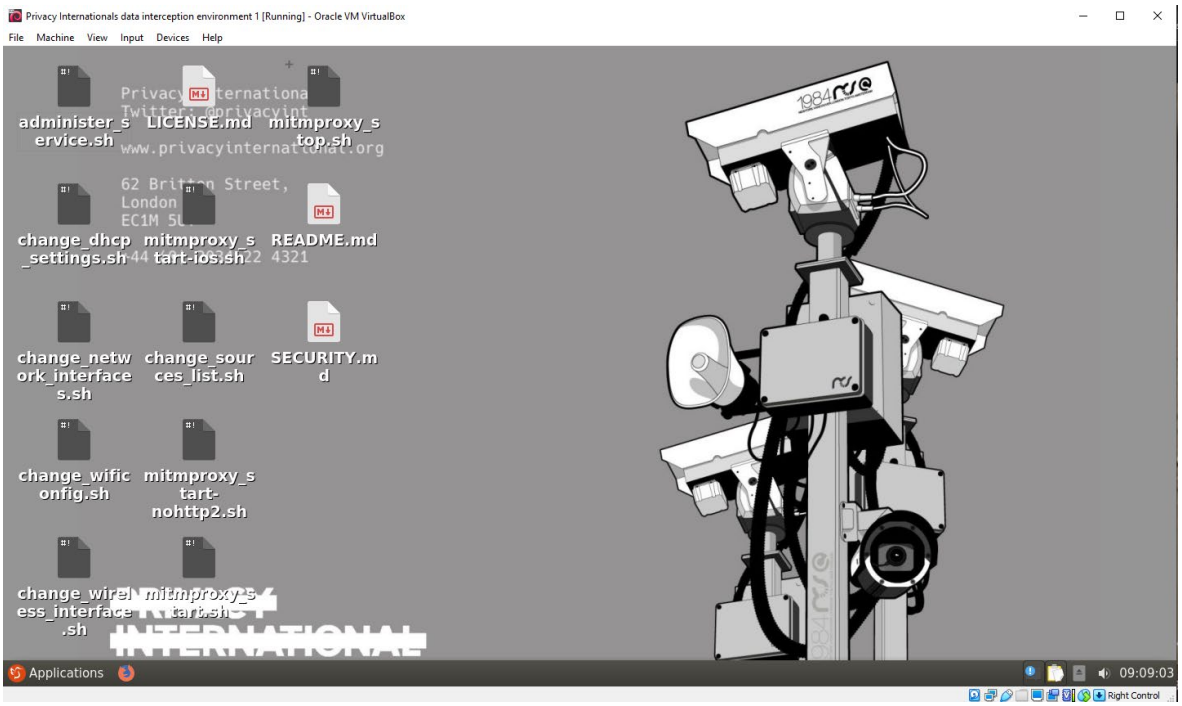
Εικόνα 5.10: Τα κουμπιά τα οποία επιλέγουμε για να προχωρήσει η εγκατάσταση του εικονικού περιβάλλοντος.

Με την ολοκλήρωση της εγκατάστασης και πριν την εκκίνηση της μηχανής κάνουμε τις απαραίτητες ρυθμίσεις δίνοντας στη μηχανή τουλάχιστον 2GB RAM (2048MB), τουλάχιστον δύο επεξεργαστές (CPUs) και βεβαιωνόμαστε ότι το Wireless NIC, στην περίπτωση μας το USB Wi-Fi adapter με Chipset Ralink5370, είναι συνδεδεμένο στο USB και διαβάζεται από την εικονική μηχανή.



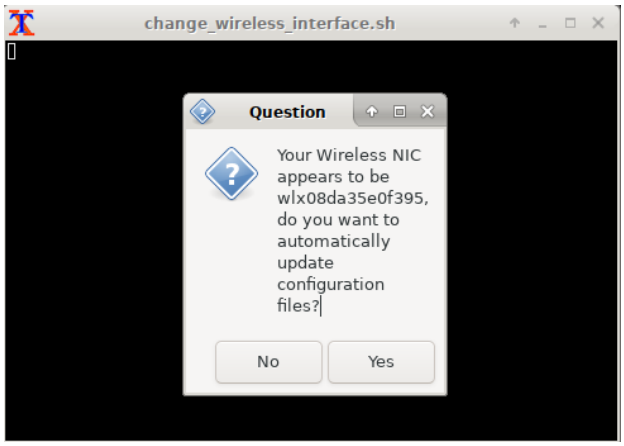
Εικόνα 5.11: Οι ρυθμίσεις οι οποίες χρειάζονται να γίνουν πριν την εκκίνηση του εικονικού περιβάλλοντος.

Με την ολοκλήρωση των ρυθμίσεων πατάμε το κουμπί Start και αρχίζει να «τρέχει» το εικονικό περιβάλλον.



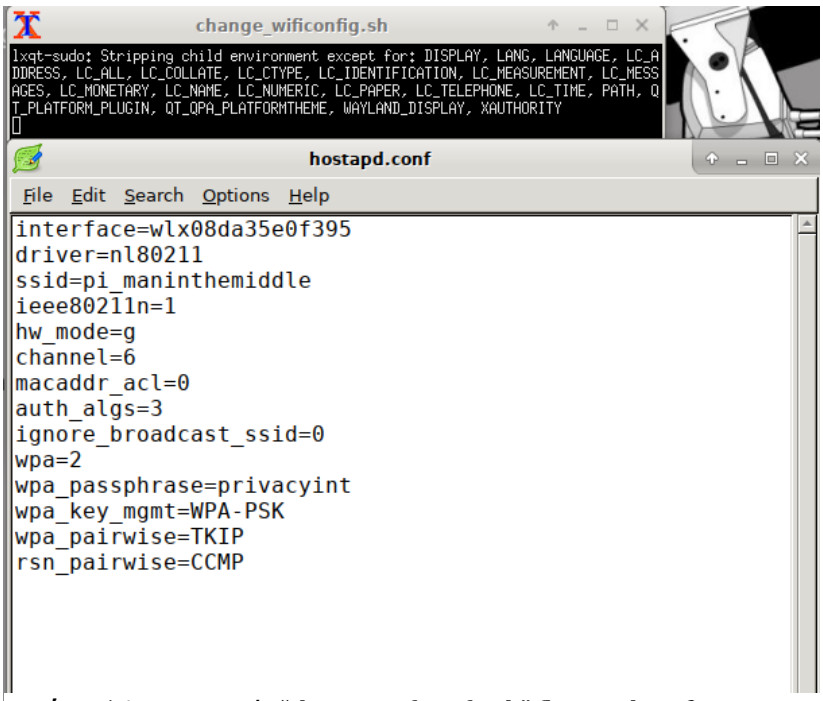
Εικόνα 5.12: Η αρχική οθόνη του εικονικού περιβάλλοντος.

Με βάση τις οδηγίες από τη σελίδα του οργανισμού Privacy International θα πρέπει να επεξεργαστούμε κάποια αρχεία. Αρχικά πατώντας πάνω στο αρχείο "change_wireless_interface.sh" μας δίνει την επιλογή "Execute in Terminal". Επιλέγοντας το ανοίγει το Terminal και το παράθυρο το οποίο μας ενημερώνει με το αναγνωριστικό συσκευής (device identifier) του Wireless NIC το οποίο χρησιμοποιούμε και θα χρειαστούμε αργότερα σε άλλο αρχείο. Το Wireless NIC μας έχει ID "wlx08da35e0f395" και πατώντας "Yes" στην επιλογή η οποία εμφανίστηκε ενημερώνονται αυτόματα τα configuration αρχεία και κλείνει το παράθυρο.



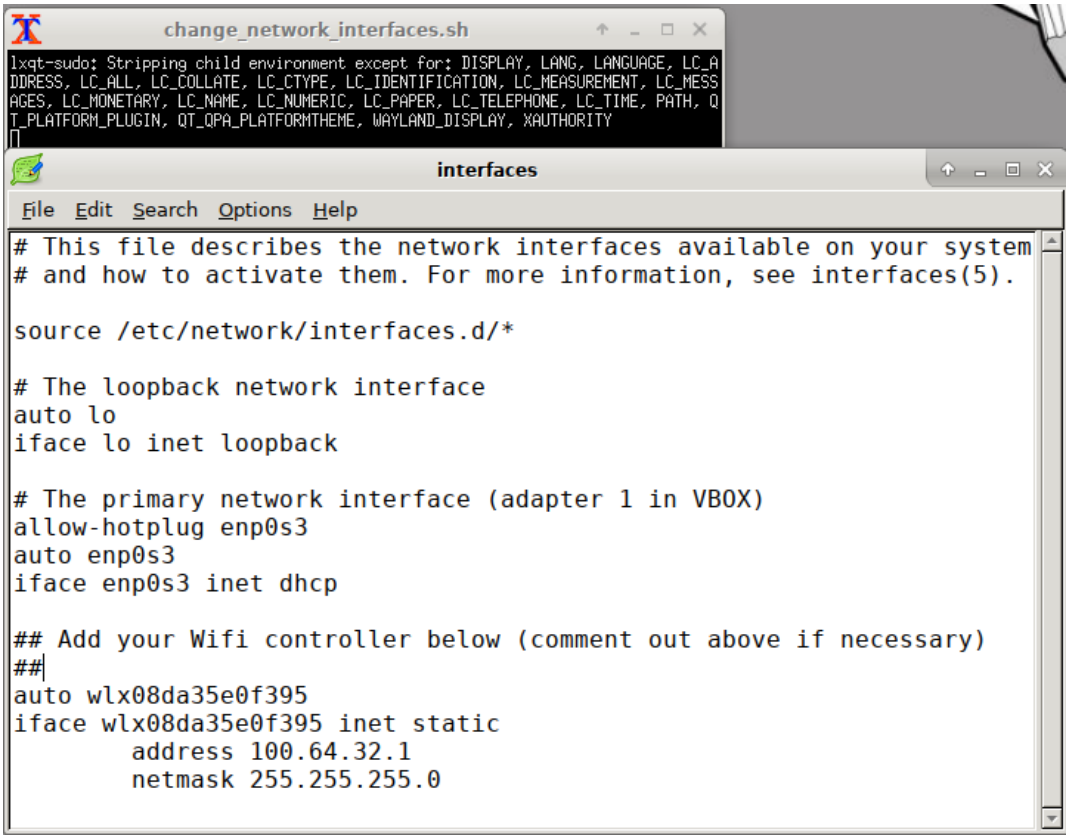
Εικόνα 5.13: Το αρχείο "change_wireless_interface.sh".

Με τον ίδιο τρόπο (Execute in Terminal) ανοίγουμε το αρχείο "change_wificonfig.sh" το οποίο είναι το hostapd αρχείο και χρειάζεται να κάνουμε τις απαραίτητες ρυθμίσεις για να συνδεθούμε στο δίκτυο του εικονικού περιβάλλοντος. Ως πρώτο βήμα αλλάζουμε το Interface βάζοντας του δικού μας NIC (το οποίο βρήκαμε από το προηγούμενο αρχείο). Ακολούθως αλλάζουμε τον Driver σε nl80211 και προσθέτουμε το ieee80211n=1 λόγω του ότι το NIC χρησιμοποιεί αυτό το standard. Μας δίνεται η επιλογή να αλλάξουμε το SSID και wpa_passphrase (password) του δικτύου αλλά επιλέξαμε να τα αφήσουμε ως έχουν. Αποθηκεύουμε και κλείνουμε το αρχείο.



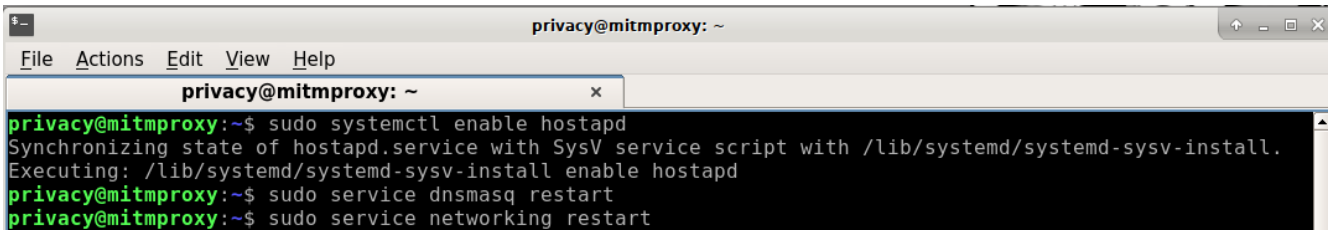
Εικόνα 5.14: Το αρχείο "change_wificonfig.sh" (hostapd.conf) με τις κατάλληλες αλλαγές .

Επιπλέον θα πρέπει να γίνουν αλλαγές και στο αρχείο "change_network_interface.sh" το οποίο περιέχει πληροφορίες για το interface του Wireless NIC το οποίο χρησιμοποιούμε. Ανοίγοντας το και πάλι με τον ίδιο τρόπο (Execute in Terminal) βγάζουμε από σχόλια όσα αφορούν το Wi-Fi controller (βλ. Εικόνα 5.15) και προσθέτουμε στο auto το δικό μας interface το οποίο βρήκαμε από το πρώτο αρχείο το οποίο τρέξαμε. Το interface μας πρέπει να το γράψουμε και από κάτω αντικαθιστώντας το προκαθορισμένο του περιβάλλοντος και τέλος επιλέγουμε τη διεύθυνση (IP address) στην οποία «ακούει» το Wireless NIC (100.64.32.1) μας και μάσκα δικτύου (netmask) (255.255.255.0).



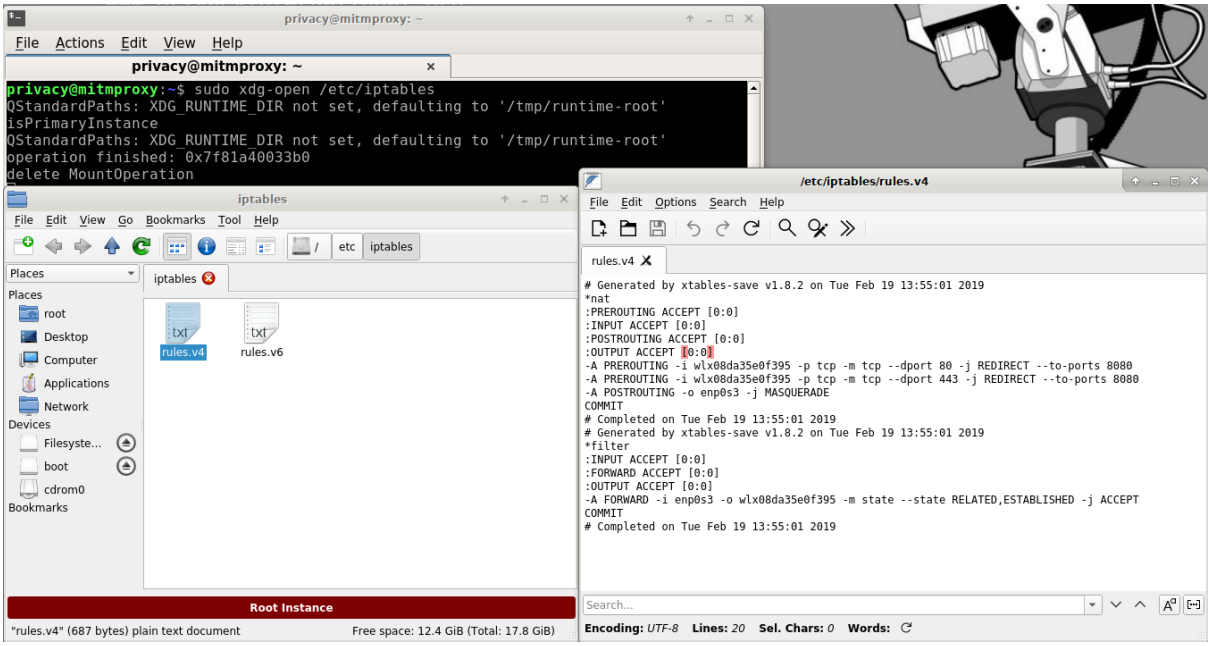
Εικόνα 5.15: Το αρχείο "change_network_interfaces.sh" με τις κατάλληλες αλλαγές.

Για να αποκτήσουν νόημα οι αλλαγές μας στα πιο πάνω αρχεία χρειάζεται να ενεργοποιηθεί το hostapd και να κάνουμε επανεκκίνηση το dnsmasq και τα networking services. Για να το πετύχουμε αυτό ανοίγουμε από το Applications → System Tools → QTerminal και τρέχουμε αρχικά την εντολή η οποία ενεργοποιεί το hostapd "sudo systemctl enable hostapd". Ακολούθως με την εντολή "sudo service dnsmasq restart" γίνεται επανεκκίνηση του dnsmasq και με την εντολή "sudo service networking restart" γίνεται επανεκκίνηση του δικτύου με τις σωστές ρυθμίσεις.



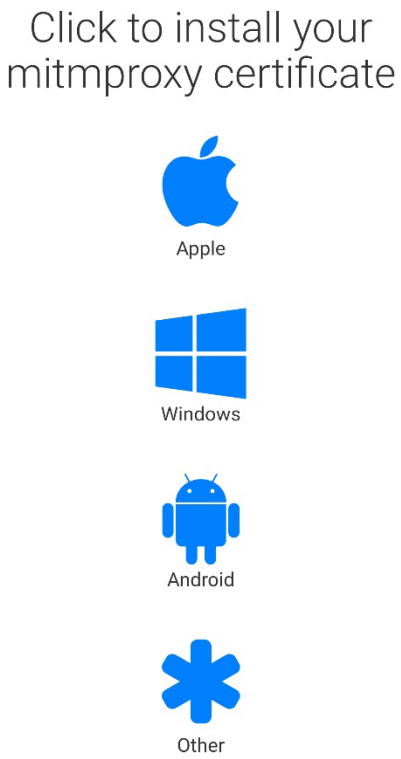
Εικόνα 5.16: Οι εντολές οι οποίες πρέπει να τρέξουν μετά τις μετατροπές στα αρχεία.

Πριν προχωρήσουμε στην εγκατάσταση του πιστοποιητικού mitmproxy στην κινητή συσκευή μας πρέπει να σιγουρευτούμε ότι στο αρχείο με τους κανόνες rules.v4 το interface έχει το interface του δικού μας NIC το οποίο γράφει και στο αρχείο hostapd.conf και όχι του προεπιλεγμένου. Το αρχείο βρίσκεται στο /etc/iptables/rules.v4 και η πρόσβαση σε αυτό απαιτεί δικαιώματα διαχειριστή. Για να αποκτήσουμε πρόσβαση ανοίγουμε το QTerminal και πληκτρολογώντας την εντολή "sudo xdg-open /etc/iptables/" ανοίγει ο φάκελος με τα αρχεία "rules.v4" και "rules.v6" όπου επεξεργαζόμαστε κατάλληλα το πρώτο και προσθέτουμε το δικό μας interface.



Εικόνα 5.17: Πρόσβαση στο αρχείο "rules.v4" και κατάλληλη τροποποίηση του με το interface του NIC μας.

Μετά την επανεκκίνηση των services και ενεργοποίηση του hostapd τρέχουμε το αρχείο "mitmproxy_start.sh" με το Execute in Terminal για να ενεργοποιηθεί το Proxy του εικονικού περιβάλλοντος. Έπειτα συνδεόμαστε στο δίκτυο "pi_maninthemiddle" από την κινητή συσκευή μας με κωδικό "privacyint". Από τον browser μεταβαίνουμε στη διεύθυνση http://mitm.it όπου κατεβάζουμε το mitmproxy πιστοποιητικό για Android συσκευές. Για την εγκατάσταση του πιστοποιητικού χρειάζεται η συσκευή μας να είναι rooted, δηλαδή να έχουμε δικαιώματα διαχειριστή.



Εικόνα 5.18: Η δυνατότητα εγκατάστασης του mitmproxy πιστοποιητικού μέσω της σελίδας http://mitm.it

5.1.6 Ανάλυση εφαρμογής μέσω του εικονικού περιβάλλοντος

Με την ολοκλήρωση της πιο πάνω διαδικασίας και την εγκατάσταση των εφαρμογών συνομιλιών/τηλεπικοινωνιών μελετήθηκαν οι εφαρμογές με τη χρήση του εικονικού περιβάλλοντος. Για να μελετηθούν οι εφαρμογές χρειάζεται να τρέξει το αρχείο ““mitmproxy_start.sh” και η εφαρμογή να αποδεχτεί το πιστοποιητικό. Κάποιες εφαρμογές δεν το αποδέχτηκαν (π.χ. Messenger) και αυτό δείχνει το καλό επίπεδο ασφάλειάς τους.

Ενδεικτικά παρατίθεται η ανάλυση της εφαρμογής Discord με τη χρήση του εικονικού περιβάλλοντος. Οι εικόνες από την ανάλυση όλων των εφαρμογών παρατίθενται στο Παράρτημα Α. Για την ανάλυση τόσο του Discord όσο και των άλλων εφαρμογών δημιουργήθηκε λογαριασμός (ξεχωριστός σε κάθε εφαρμογή) και έγινε ανταλλαγή μηνυμάτων και πολυμέσων μέσα σε ομαδικές συνομιλίες τις οποίες παρέχουν οι πλείστες εφαρμογές. Με αυτό τον τρόπο ελέγχθηκε η κίνηση δικτύου των δεδομένων κατά την αποστολή ή λήψη μηνυμάτων/πολυμέσων. Όπως φαίνεται και στις πιο κάτω εικόνες, στην ανάλυση του Discord τόσο στα GET όσο και στα Post requests δεν εντοπίστηκε κάποιο κενό ασφάλειας ή αποστολή δεδομένων σε τρίτους.

Εικόνα 5.19: Στιγμιότυπα από την ανάλυση των GET και POST Requests της εφαρμογής Discord μέσω του εικονικού περιβάλλοντος του PI

5.2 Προβλήματα κατά τη διεξαγωγή της πρακτικής / ερευνητικής μελέτης

Κατά τη διεξαγωγή της έρευνας και την εγκατάσταση τόσο των εφαρμογών συνομιλιών/επικοινωνιών όσο και των εργαλείων για το περιβάλλον δοκιμών αντιμετωπίστηκαν κάποια προβλήματα τα οποία επιλύθηκαν άμεσα. Τα προβλήματα αναφέρονται πιο κάτω και είναι τα εξής:

- Κατά την πρώτη χρήση των εφαρμογών τηλεπικοινωνιών/εφαρμογών κάποιες εξ αυτών απαιτούσαν αριθμό τηλεφώνου (χρησιμοποιήθηκε ο προσωπικός), ενώ κάποιες άλλες τη χρήση ηλεκτρονικής διεύθυνσης και κωδικού πρόσβασης ενώ κάποιες εφαρμογές δεν απαιτούσαν τίποτα από τα δύο καθιστώντας τες ανώνυμες (π.χ. Session). Στην περίπτωση όπου απαιτείτο ηλεκτρονική διεύθυνση για τη δημιουργία λογαριασμού δημιουργήθηκε λογαριασμός Gmail αποκλειστικά για χρήση στην πρακτική μελέτη της παρούσας διπλωματικής.

- Ο οργανισμός Privacy International προτείνει τη χρήση USB Wi-Fi adapter με ενσωματωμένο Ralink5370 Chipset για να υπάρχει σύνδεση με το εικονικό περιβάλλον. Δυστυχώς αυτό δεν ήταν εύκολο να βρεθεί εγχώρια και παραγγέλθηκε από το εξωτερικό (Ελλάδα) και πήρε αρκετές ημέρες μέχρι να παραληφθεί. Ευτυχώς παρά την καθυστέρηση το USB Wi-Fi Adapter δούλευε χωρίς κάποιο πρόβλημα

- Παρά τις απαραίτητες αλλαγές στα αρχεία όπως αυτές καταγράφηκαν πιο πάνω η κινητή συσκευή δεν είχε πρόσβαση στη σελίδα http://mitm.it. Για την επίλυση του προβλήματος έγινε επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου (emails) με τον οργανισμό Privacy International. Μέσω αυτής της επικοινωνίας έγινε αντιληπτό ότι δεν άλλαξε το interface στο αρχείο rules.v4 με το interface του δικού μας NIC (USB Wi-Fi Adapter) και χρειάστηκε να αλλαχθεί χειροκίνητα.

- Όταν κλείσει η εικονική μηχανή και την ανοίξουμε ξανά η σύνδεση με το δίκτυο "pi_maninthemiddle" μπορεί να μην είναι εφικτή. Η κινητή συσκευή μπορεί να μην βλέπει το δίκτυο ή να αδυνατεί να συνδεθεί σε αυτό (looping). Για να επιλυθεί αυτό χρειάζεται κατά την ενεργοποίηση της μηχανής να τρέξουμε τις εντολές "sudo service networking restart; sudo service hostapd restart; sudo service dnsmasq restart" από το QTerminal.

Κεφάλαιο 6
Αποτελέσματα μελέτης εφαρμογών

Στο παρόν κεφάλαιο παρουσιάζονται τα αποτελέσματα της πρακτικής/ερευνητικής μελέτης των εφαρμογών μηνυμάτων / τηλεπικοινωνιών στο περιβάλλον δοκιμών το οποίο παρουσιάστηκε στο προηγούμενο κεφάλαιο. Τα αποτελέσματα παρουσιάζονται ανά εργαλείο που χρησιμοποιήθηκε λόγω του ότι κάθε εργαλείο έχει διαφορετικές δυνατότητες.

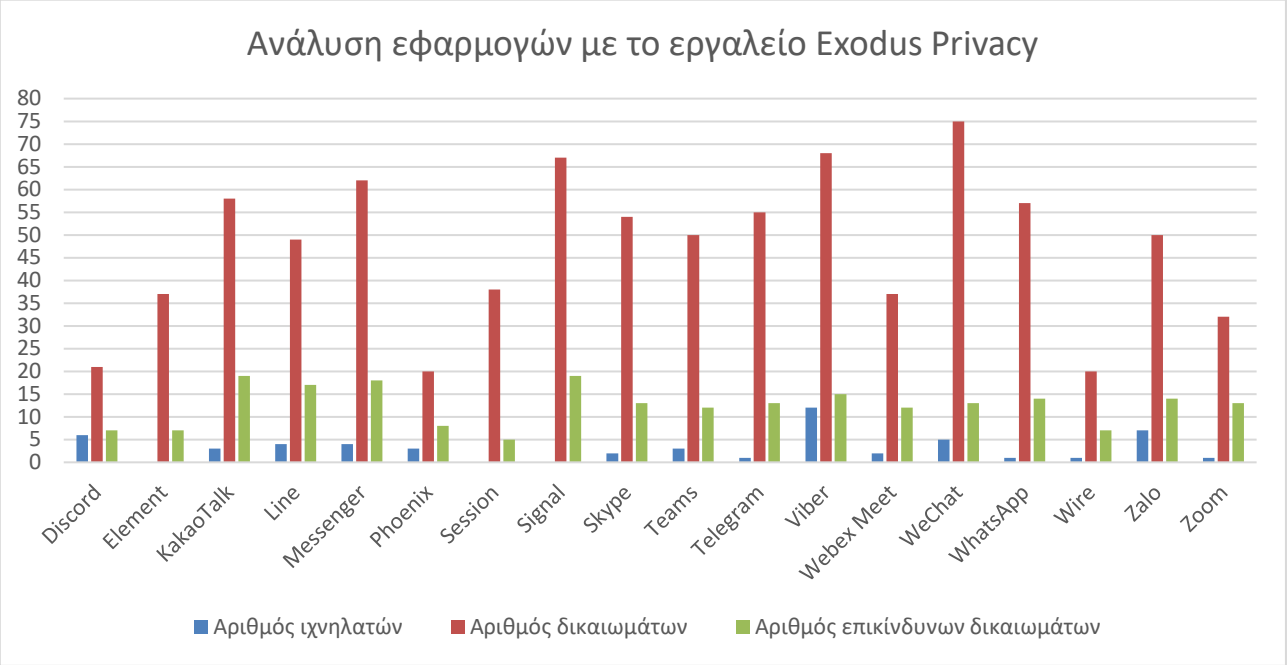
6.1 Αποτελέσματα της ανάλυσης με το Exodus Privacy

Με το διαδικτυακό εργαλείο Exodus Privacy έγινε μελέτη και των δεκαοχτώ εφαρμογών οι οποίες παρουσιάστηκαν στο Κεφάλαιο 5. Στον πιο κάτω πίνακα αναγράφεται ο αριθμός δικαιωμάτων (permissions), επικίνδυνων δικαιωμάτων (dangerous permissions) και ιχνηλατών (trackers) τα οποία έχει εντοπίσει το εργαλείο σε κάθε εφαρμογή.

Εφαρμογή	Αριθμός ιχνηλατών	Αριθμός δικαιωμάτων	Αριθμός επικίνδυνων δικαιωμάτων
Discord	6	21	7
Element	0	37	7
KakaoTalk	3	58	19
Line	4	49	17
Messenger	4	62	18
Phoenix	3	20	8
Session	0	38	5
Signal	0	67	19
Skype	2	54	13
Teams	3	50	12
Telegram	1	55	13
Viber	12	68	15
Webex Meet	2	37	12
WeChat	5	75	13
WhatsApp	1	57	14
Wire	1	20	7
Zalo	7	50	14

Zoom	1	32	13

Πίνακας 6.1: Συνολικός αριθμός ιχνηλατών, δικαιωμάτων και επικίνδυνων δικαιωμάτων στις εφαρμογές με τη χρήση του εργαλείου Exodus.



Εικόνα 6.2: Διάγραμμα σύγκρισης συνολικού αριθμού ιχνηλατών, δικαιωμάτων και επικίνδυνων δικαιωμάτων στις εφαρμογές με τη χρήση του εργαλείου Exodus.

Από τον πιο πάνω πίνακα (Πίνακας 6.1) γίνεται εύκολα αντιληπτό ότι όλες οι εφαρμογές οι οποίες μελετήθηκαν απαιτούν δικαιώματα στη συσκευή του χρήστη και απαιτούν τουλάχιστον επτά επικίνδυνα δικαιώματα για να λειτουργήσουν. Σε ότι αφορά τον αριθμό ιχνηλατών τους οποίους χρησιμοποιούν, δύο εφαρμογές (Signal, Session) δεν χρησιμοποιούν κανέναν με το Viber να κρατάει τα ηνία με το μεγαλύτερο αριθμό ιχνηλατών, ίσου με δώδεκα.

Αρχίζοντας με την ανάλυση των ιχνηλατών οι οποίοι εντοπίστηκαν, μόνο μία εφαρμογή (Wire) δεν χρησιμοποιεί ιχνηλάτη της Google με τις υπόλοιπες να χρησιμοποιούν τουλάχιστον έναν. Οι έντεκα από τις δεκαέξι εφαρμογές (στις οποίες εντοπίστηκαν ιχνηλάτες) κάνουν χρήση του Google Firebase Analytics με πέντε εξ αυτών να χρησιμοποιούν και το Google Crashlytics. Επιπλέον τρεις εφαρμογές κάνουν χρήση διαφορετικού ιχνηλάτη της Google, του Google Analytics. Στον πιο κάτω πίνακα παρουσιάζονται αναλυτικά οι ιχνηλάτες οι οποίοι εντοπίστηκαν στις εφαρμογές.

Discord

Adjust	Facebook Flipper	Google Analytics
Google CrashLytics	Google Firebase Analytics	Google Tag Manager

Element

-

KakaoTalk

AdFit (Daum)	Google CrashLytics	Google Firebase Analytics

Line

Facebook Login	Facebook Share	Google AdMob
Google Analytics		

Messenger

Facebook Notifications	Facebook Share	Google Analytics
Mapbox		

Phoenix

AppsFlyer	Google CrashLytics	Google Firebase Analytics

Session

-

Signal

-

Skype

Google Firebase Analytics	Microsoft Visual Studio App Center Crashes

Teams

Bugsnag	Google Firebase Analytics	Microsoft Visual Studio App Center Crashes

Telegram

Google Firebase Analytics

Viber

Adjust	AppMetrica	Braze (formerly Appboy)
Google AdMob	Google CrashLytics	Google Firebase Analytics
Huawei Mobile Services (HMS) Core	MixPanel	myTarger
Twitter MoPub	VKontakte SDK	Yandex Ad

Webex Meet

Amplitude	Google Firebase Analytics

WeChat

Facebook Analytics	Facebook Login	Facebook Share

Google Firebase Analytics	WeChat Location

WhatsApp

Google Analytics

Wire

Countly

Zalo

AdColony	Criteo	Facebook Ads
Google AdMob	Google Analytics	Google CrashLytics
Google Firebase Analytics		

Zoom

Google Firebase Analytics

Πίνακας 6.1: Οι ιχνηλάτες οι οποίοι εντοπίστηκαν με τη χρήση του εργαλείου Exodus Privacy.

Η ανάλυση των δικαιωμάτων των οποίων απαιτούν οι εφαρμογές επικεντρώθηκε κυρίως στα επικίνδυνα δικαιώματα μιας και μπορούν να επέμβουν σε λειτουργίες της συσκευής του χρήστη. Στον πιο κάτω πίνακα παρουσιάζονται τα επικίνδυνα δικαιώματα των δεκαοκτώ εφαρμογών που μελετήθηκαν. Η εφαρμογή η οποία απαιτεί τα λιγότερα επικίνδυνα δικαιώματα είναι το Session με πέντε ενώ στο άλλο άκρο βρίσκονται οι εφαρμογές Signal και KakaoTalk με δεκαεννέα. Απρόσμενο το ότι η εφαρμογή Signal ενώ δεν έχουν εντοπιστεί καθόλου ιχνηλάτες να ζητάει τόσα πολλά επικίνδυνα δικαιώματα.

Όσο αφορά στο πια επικίνδυνα δικαιώματα απαιτούνται πιο συχνά αυτά είναι η CAMERA (το οποίο αναμένεται βεβαίως για εφαρμογές τηλεδιασκέψεων), το READ_EXTERNAL_STORAGE, RECORD_AUDIO και το WRITE_EXTERNAL_STORAGE τα οποία ζητούνται και από τις δεκαοκτώ εφαρμογές. Μεγάλος αριθμός εφαρμογών απαιτεί τα δικαιώματα WRITE_SETTINGS και READ_CONTACTS (16 εφαρμογές) και το ACCESS_FINE_LOCATION (15 εφαρμογές) ενώ τα υπόλοιπα επικίνδυνα δικαιώματα απαιτούνται από λιγότερες εφαρμογές. Είναι αναγκαίο να ειπωθεί ότι «επικίνδυνο» δικαίωμα δεν σημαίνει και απαραίτητα ότι είναι κακό για το χρήστη και τα δεδομένα του. Αυτό γιατί είναι απόλυτα λογικό π.χ. εφαρμογές τηλεδιασκέψεων να απαιτούν πρόσβαση στην κάμερα και το μικρόφωνο. Το σημαντικό είναι αν τα επικίνδυνα δικαιώματα προκύπτουν ως απολύτως απαραίτητα για τις υπηρεσίες που παρέχει η κάθε εφαρμογή, καθώς και αν τεκμηριώνονται στις πολιτικές προστασίας δεδομένων. Αυτό παρουσιάζεται στο τελευταίο τμήμα του κεφαλαίου όπου γίνεται σύγκριση των δικαιωμάτων που απαιτούν οι εφαρμογές σε σχέση με το τι αναφέρεται στις πολιτικές προστασίας δεδομένων (privacy policies) τους.

Discord

CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	RECORD_AUDIO	SYSTEM_ALERT_WINDOW
WRITE_EXTERNAL_STORAGE		

Element

CAMERA	READ_CONTACTS	READ_EXTERNAL_STORAGE
RECORD_AUDIO	SYSTEM_ALERT_WINDOW	WRITE_EXTERNAL_STORAGE
WRITE_SETTINGS		

KakaoTalk

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALENDAR
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS
READ_PHONE_STATE	READ_SMS	RECEIVE_MMS
RECEIVE_SMS	RECORD_AUDIO	SEND_SMS
SYSTEM_ALERT_WINDOW	WRITE_CALENDAR	WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE		

Line

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS	READ_PHONE_STATE
READ_SMS	RECEIVE_MMS	RECEIVE_SMS
RECORD_AUDIO	SYSTEM_ALERT_WINDOW	WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE	WRITE_SETTINGS	

Messenger

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALENDAR
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS
READ_PHONE_STATE	READ_SMS	RECEIVE_MMS
RECEIVE_SMS	RECORD_AUDIO	SEND_SMS
SYSTEM_ALERT_WINDOW	WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE

Phoenix

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CAMERA
READ_EXTERNAL_STORAGE	READ_PHONE_STATE	RECORD_AUDIO
SYSTEM_ALERT_WINDOW	WRITE_EXTERNAL_STORAGE	

Session

CAMERA	READ_EXTERNAL_STORAGE	RECORD_AUDIO
WRITE_EXTERNAL_STORAGE	WRITE_SETTINGS	

Signal

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALENDAR
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS

READ_PHONE_STATE	READ_SMS	RECEIVE_MMS
RECEIVE_SMS	RECORD_AUDIO	SEND_SMS
WRITE_CALENDAR	WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE
WRITE_SETTINGS		

Skype

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_STATE	RECORD_AUDIO
SYSTEM_ALERT_WINDOW	WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE
WRITE_SETTINGS		

Teams

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	RECORD_AUDIO	SYSTEM_ALERT_WINDOW
WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE	WRITE_SETTINGS

Telegram

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALL_LOG
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_STATE
RECORD_AUDIO	SYSTEM_ALERT_WINDOW	WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE		

Viber

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALL_LOG
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS
READ_PHONE_STATE	RECORD_AUDIO	SYSTEM_ALERT_WINDOW
WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE	WRITE_SETTINGS

Webex Meet

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	READ_CALENDAR	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS	READ_PHONE_STATE
RECORD_AUDIO	SYSTEM_ALERT_WINDOW	WRITE_EXTERNAL_STORAGE

WeChat

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	BODY_SENSORS
CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_STATE	RECORD_AUDIO
SYSTEM_ALERT_WINDOW	WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE
WRITE_SETTINGS		

WhatsApp

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CAMERA
GET_ACCOUNTS	READ_CONTACTS	READ_EXTERNAL_STORAGE
READ_PHONE_NUMBERS	READ_PHONE_STATE	RECEIVE_SMS
RECORD_AUDIO	SEND_SMS	WRITE_CONTACTS

WRITE_EXTERNAL_STORAGE	WRITE_SETTINGS	

Wire

ACCESS_FINE_LOCATION	CAMERA	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_STATE	RECORD_AUDIO
WRITE_EXTERNAL_STORAGE		

Zalo

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	ANSWER_PHONE_CALLS
CALL_PHONE	CAMERA	GET_ACCOUNTS
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_STATE
RECORD_AUDIO	SYSTEM_ALERT_WINDOW	WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE		

Zoom

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	READ_CALENDAR	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS	READ_PHONE_STATE
RECORD_AUDIO	SYSTEM_ALERT_WINDOW	WRITE_CALENDAR
WRITE_EXTERNAL_STORAGE		

Πίνακας 6.2:Τα επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν με τη χρήση του εργαλείου Exodus Privacy.

6.2 Αποτελέσματα της ανάλυσης με το Lumen privacy monitor

Με το εργαλείο Lumen privacy monitor έγινε μελέτη δεκαπέντε εφαρμογών από τις δεκαοκτώ λόγω του ότι δεν εντόπισε στη συσκευή τις εφαρμογές Session, Telegram και WeChat. Το εργαλείο εντόπισε διαρροές δεδομένων (Leaks) σε έξι εφαρμογές με τις πιο σοβαρές (High Risk) να είναι το Android Serial και το facebook-messenger account τα οποία διαρρέονται από την εφαρμογή Skype και το BSSID το οποίο διαρρέεται από την εφαρμογή Viber. Πιο συγκεκριμένα, το BSSID (Basic Service Set Identifier) είναι το MAC address του Access point στο δίκτυο μας και στη δική μας περίπτωση μας δίνει το IP Address του router στο οποίο είναι απευθείας (Wi-Fi) ενωμένη η συσκευή μας κάτι το οποίο είναι επικίνδυνο αν πέσει σε λάθος χέρια. Στον πιο κάτω πίνακα παρουσιάζονται αναλυτικά οι διαρροές ανά εφαρμογή που εντοπίστηκαν. Ως επίπεδο επικινδυνότητας αναγράφεται αυτό που η εφαρμογή Lumen έχει αποτιμήσει.

Εφαρμογή	Leaks (Διαρροές)	Επίπεδο Επικινδυνότητας
Phoenix	Build Fingerprint	Low Risk
Skype	Android Serial	High Risk
	Account (com.facebook.messenger)	High Risk

	Time-zone	Mid Risk
Teams	Build Fingerprint	Low Risk
Viber	BSSID	High Risk
	Build Fingerprint	Low Risk
Webex Meet	Private IP	Mid Risk
	Time-zone	Mid Risk
	Build Fingerprint	Low Risk
WhatsApp	Build Fingerprint	Low Risk

Πίνακας 6.3: Οι διαρροές προσωπικών δεδομένων οι οποίες εντοπίστηκαν από εφαρμογές οι οποίες εντοπίστηκαν με το εργαλείο Lumen.

Επιπλέον το εργαλείο Lumen έχει τη δυνατότητα να εντοπίσει ιχνηλάτες στις εφαρμογές, δικαιώματα τα οποία απαιτούν χωρίζοντας τα σε κατηγορίες Dangerous (επικίνδυνα), Medium Risk και Low Risk αλλά και το αν αποστέλλουν δεδομένα σε κάποια domains και αν ναι ποια είναι αυτά. Ο πιο κάτω πίνακας δείχνει τον αριθμό ιχνηλατών, δικαιωμάτων, επικίνδυνων δικαιωμάτων και domains τα οποία εντοπίστηκαν στις εφαρμογές οι οποίες μελετήθηκαν.

Συγκρίνοντας τον αριθμό ιχνηλατών οι οποίοι εντοπίστηκαν με το εργαλείο Exodus βλέπουμε ότι εντοπίστηκαν περισσότεροι παρά με το εργαλείο Lumen κάτι το οποίο ίσως να έχει να κάνει με τον τρόπο τον οποίο τα δύο εργαλεία αναλύουν τις εφαρμογές. Επίσης στα δικαιώματα τα οποία απαιτούν οι εφαρμογές βλέπουμε κάποιες διαφορές με κάποιες εφαρμογές να έχουν μεγαλύτερο αριθμό και κάποιες μικρότερο σε σχέση με πριν. Το ίδιο συμβαίνει και στα επικίνδυνα δικαιώματα μιας και όπως διαφάνηκε η εφαρμογή Lumen δεν εντοπίζει και δεν κατηγοριοποιεί ως επικίνδυνα τα δικαιώματα SYSTEM_ALERT_WINDOW και WRITE_SETTINGS. Τα επικίνδυνα δικαιώματα καταγράφονται στον Πίνακα 6.6 και με πράσινο χρώμα είναι τα δικαιώματα τα οποία εντόπισαν και τα δύο εργαλεία.

Το εργαλείο εντόπισε μεγάλο αριθμό domains (third-party και της εταιρείας της εφαρμογής) όπου οι εφαρμογές αποστέλλουν δεδομένα με το Skype να αποστέλλει σε έντεκα διαφορετικά και τα Wire και Zoom σε μόλις ένα. Στον πιο κάτω πίνακα αναφέρεται ο αριθμός domains που εντοπίστηκε σε κάθε εφαρμογή και στο Παράρτημα Α υπάρχουν αναλυτικές εικόνες με τα ονόματα των domains.

Εφαρμογή	Αριθμός ιχνηλατών	Αριθμός domains (third-party και μη)	Αριθμός δικαιωμάτων	Αριθμός επικίνδυνων δικαιωμάτων
Discord	2	8	21	6
Element	0	3	37	5
KakaoTalk	1	6	62	18
Line	1	6	49	12
Messenger	0	2	64	17
Phoenix	5	10	20	7
Signal	0	2	67	18
Skype	0	11	54	11
Teams	0	8	47	10
Viber	2	5	75	13
Webex Meet	0	4	38	11
WhatsApp	0	2	59	15
Wire	0	1	20	7
Zalo	0	4	57	14
Zoom	0	1	32	12

Πίνακας 6.4: Συνολικός αριθμός ιχνηλατών, δικαιωμάτων, επικίνδυνων δικαιωμάτων και domains (για αποστολή δεδομένων) στις εφαρμογές με τη χρήση του εργαλείου Lumen Privacy.

Discord

CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	RECORD_AUDIO	WRITE_EXTERNAL_STORAGE

Element

CAMERA	READ_CONTACTS	READ_EXTERNAL_STORAGE
RECORD_AUDIO	SYSTEM_ALERT_WINDOW	

KakaoTalk

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALENDAR
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS
READ_PHONE_STATE	READ_SMS	RECEIVE_MMS
RECEIVE_SMS	RECORD_AUDIO	SEND_SMS
WRITE_CALENDAR	WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE

Line

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS	READ_PHONE_STATE
RECORD_AUDIO	WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE

Messenger

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALENDAR
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS
READ_PHONE_STATE	READ_SMS	RECEIVE_MMS
RECEIVE_SMS	RECORD_AUDIO	SEND_SMS
WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE	

Phoenix

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CAMERA
READ_EXTERNAL_STORAGE	READ_PHONE_STATE	RECORD_AUDIO
WRITE_EXTERNAL_STORAGE		

Signal

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALENDAR
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS
READ_PHONE_STATE	READ_SMS	RECEIVE_MMS
RECEIVE_SMS	RECORD_AUDIO	SEND_SMS
WRITE_CALENDAR	WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE

Skype

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_STATE	RECORD_AUDIO
WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE	

Teams

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CONTACTS
READ_EXTERNAL_STORAGE	RECORD_AUDIO	WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE		

Viber

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	GET_ACCOUNTS	READ_CALL_LOG
READ_CONTACTS	READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS
READ_PHONE_STATE	RECORD_AUDIO	WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE		

Webex Meet

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	READ_CALENDAR	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS	READ_PHONE_STATE
RECORD_AUDIO	WRITE_EXTERNAL_STORAGE	

WhatsApp

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CAMERA
GET_ACCOUNTS	READ_CONTACTS	READ_EXTERNAL_STORAGE
READ_PHONE_NUMBERS	READ_PHONE_STATE	RECEIVE_SMS
RECORD_AUDIO	SEND_SMS	WRITE_CONTACTS
WRITE_EXTERNAL_STORAGE		

Wire

ACCESS_FINE_LOCATION	CAMERA	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_STATE	RECORD_AUDIO
WRITE_EXTERNAL_STORAGE		

Zalo

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	ANSWER_PHONE_CALLS
CALL_PHONE	CAMERA	GET_ACCOUNTS
READ_CALL_LOG	READ_CONTACTS	READ_EXTERNAL_STORAGE
READ_PHONE_NUMBERS	READ_PHONE_STATE	RECORD_AUDIO
WRITE_CONTACTS	WRITE_EXTERNAL_STORAGE	

Zoom

ACCESS_COARSE_LOCATION	ACCESS_FINE_LOCATION	CALL_PHONE
CAMERA	READ_CALENDAR	READ_CONTACTS
READ_EXTERNAL_STORAGE	READ_PHONE_NUMBERS	READ_PHONE_STATE
RECORD_AUDIO	WRITE_CALENDAR	WRITE_EXTERNAL_STORAGE

Πίνακας 6.5: Τα επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν με τη χρήση του εργαλείου Lumen Privacy.

6.3 Αποτελέσματα της ανάλυσης με το Inspeckage

Η χρήση του συγκεκριμένου εργαλείου έγινε αρχικά για να εντοπιστούν διαρροές αναγνωριστικών των συσκευών (π.χ. Google Advertising ID) από τις εφαρμογές μέσω των .xml αρχείων τους χωρίς να εντοπίζεται κάτι. Όμως όπως φαίνεται και από τις εικόνες στο Παράρτημα Α το εργαλείο μας έδωσε και τις Exported και τις μη Exported διεργασίες (activities) των εφαρμογών και πάλι χωρίς να εντοπίζεται κάτι το μεμπτό. Επιπλέον μέσω του εργαλείου παρακολουθήσαμε τα δικαιώματα τα οποία χρησιμοποιεί η κάθε εφαρμογή και ο αριθμός τους παρουσιάζεται στον πιο κάτω πίνακα. Δυστυχώς λόγω του ότι οι εφαρμογές ανοίγουν μέσω του εργαλείου υπήρχαν κάποια θέματα με το Skype και το WeChat και δεν ανταποκρίνονταν κατά τη χρήση τους και δεν παρείχαν δεδομένα στο γραφικό περιβάλλον του Inspeckage.

Εφαρμογή	Αριθμός δικαιωμάτων
Discord	21
Element	38
KakaoTalk	62
Line	46
Messenger	64
Phoenix	20
Session	38
Signal	67
Teams	50
Telegram	56
Viber	68

Webex Meet	38
WhatsApp	60
Wire	20
Zalo	57
Zoom	32

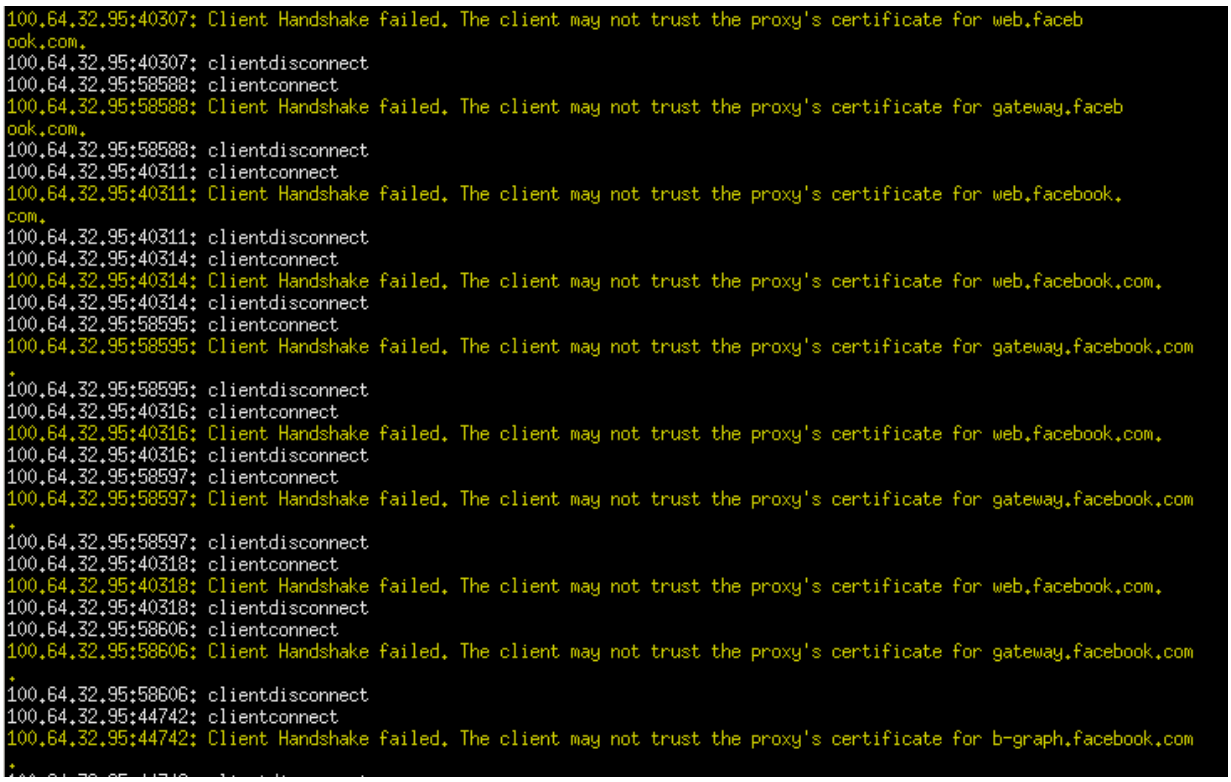
Πίνακας 6.6: Συνολικός αριθμός δικαιωμάτων στις εφαρμογές με τη χρήση του εργαλείου Inspeckage

Τέλος το εργαλείο Inspeckage μας παρουσίασε τα Exported & Non Exported Services, Shared Libraries (εάν υπήρχαν) αλλά και τους Exported & Non Exported Content Provider. Αναλυτικές εικόνες παρουσιάζονται στο Παράρτημα Α.

Στη συγκεκριμένη περίπτωση το Inspeckage δεν βοήθησε σε σχέση με τα άλλα εργαλεία και δεν μας πρόσφερε κάτι το οποίο δεν μάθαμε από τα άλλα εργαλεία για τις εφαρμογές οι οποίες μελετήθηκαν.

6.4 Αποτελέσματα της ανάλυσης με το PI's data interception environment

Στο συγκεκριμένο εικονικό περιβάλλον έγινε ανάλυση των εφαρμογών για να εντοπιστούν οι όποιες διαρροές προσωπικών δεδομένων σε τρίτους χωρίς να εντοπίζεται κάτι το μεμπτό. Πιο κάτω θα παρουσιαστούν οι έντεκα εφαρμογές οι οποίες «εμπιστεύτηκαν» το πιστοποιητικό mitmproxy και επιτράπηκε το Client Handshake. Κάποιες εφαρμογές δεν το εμπιστεύτηκαν και χρειάστηκε η χρήση του εργαλείου SSL Unpinning σε αυτές για να παρακαμφθούν οι έλεγχοι πιστοποιητικού. Όμως, παρά τη χρήση και του SSL Unpinning κάποιες εφαρμογές, π.χ. Messenger, δεν αποδέχθηκαν το πιστοποιητικό mitmproxy και δεν έγινε ανάλυση τους με το συγκεκριμένο εργαλείο. Αυτό, παρά το γεγονός ότι για τους ερευνητικούς μας σκοπούς αποτελεί περιορισμό στο να διεξαχθεί η έρευνα πλήρως, αποτελεί σαφώς θετικό στοιχείο για την ασφάλεια των συγκεκριμένων εφαρμογών μιας και μας δείχνει ότι παρέχουν ένα επιπλέον επίπεδο ασφαλείας σε επιθέσεις τύπου man-in-the middle.

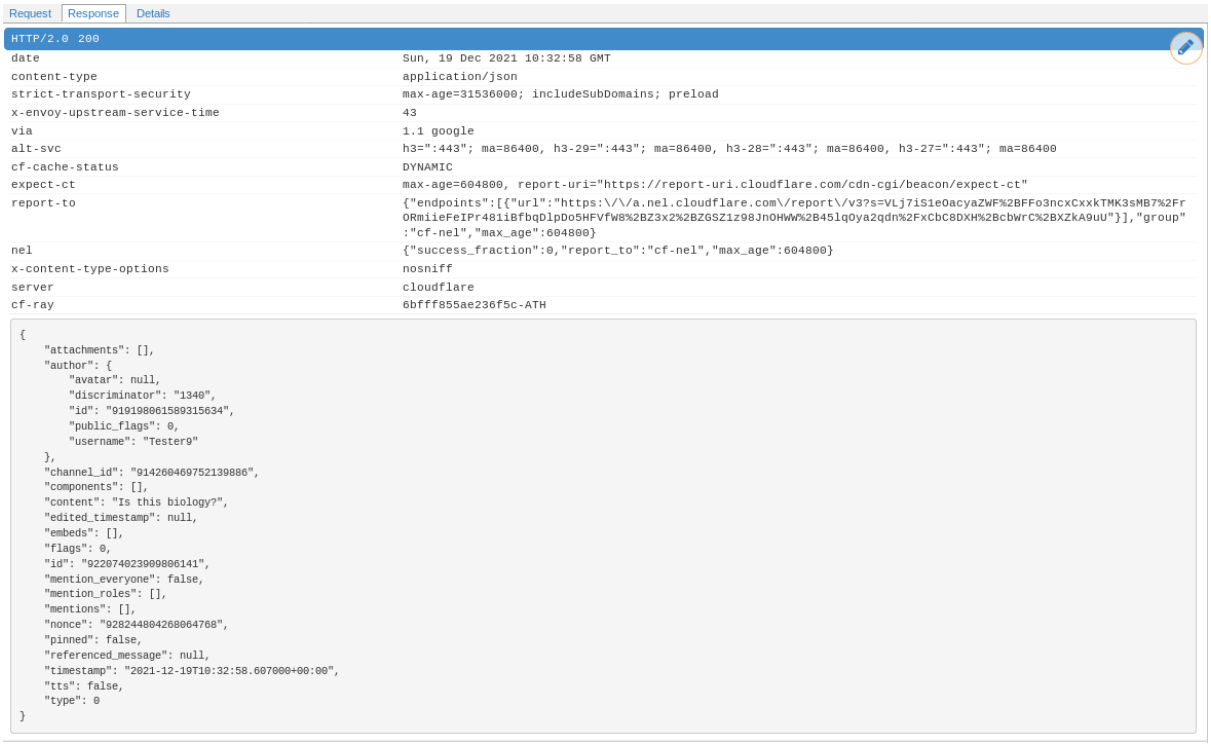


Εικόνα 6.9: Παράδειγμα μη εμπιστευτικότητας του mitmproxy certificate από την εφαρμογή Messenger και αδυναμία Client Handshake.

Για τη σωστή ανάλυση των εφαρμογών μέσω του εικονικού περιβάλλοντος έγινε αποστολή και λήψη μηνυμάτων, βιντεοκλήσεις και φωνητικές κλήσεις σε ατομικούς χρήστες ή ομαδικές συνομιλίες. Με αυτόν τον τρόπο μας δόθηκε η ευχέρεια να ελέγξουμε τόσο τα POS T όσο και τα GET requests των εφαρμογών συνομιλιών / τηλεδιασκέψεων.

6.4.1 Discord

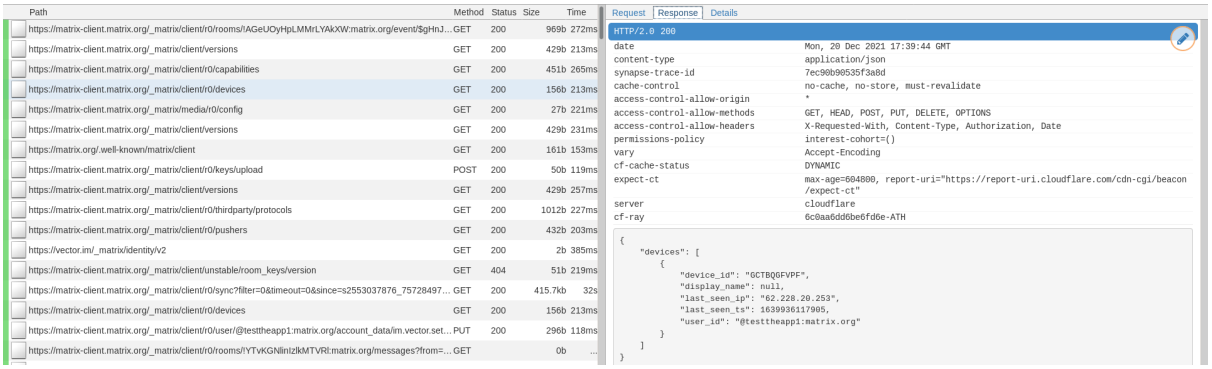
Η ανάλυση της εφαρμογής Discord δεν έδειξε οποιαδήποτε διαρροή προσωπικών δεδομένων ή αναγνωριστικών για ταυτοποίηση σε τρίτους. Η έναρξη της εφαρμογής αρχίζει με αίτημα GET για επικοινωνία με το https://dl.discordapp.net/apps/android/versions.json και χρησιμοποιείται CRC32 αλγόριθμος και κατακερματισμός με MD5 αλγόριθμο, ο οποίος δεν θεωρείται ασφαλής κρυπτογραφικός αλγόριθμος κατακερματισμού. Κατά την αποστολή δεδομένων (βλ. Εικόνα 6.10) δίνεται ένα "ID" στον author μαζί με το Username του και το channel_id και η ώρα αποστολής του μηνύματος (timestamp) χωρίς να αναγράφεται κάτι άλλο το οποίο πέραν του username που μπορεί να οδηγήσει σε άμεση ταυτοποίηση του χρήστη.



Εικόνα 6.10: Η ανάλυση της αποστολής μηνύματος μέσω της εφαρμογής Discord με το εικονικό περιβάλλον του Privacy International.

6.4.2 Element

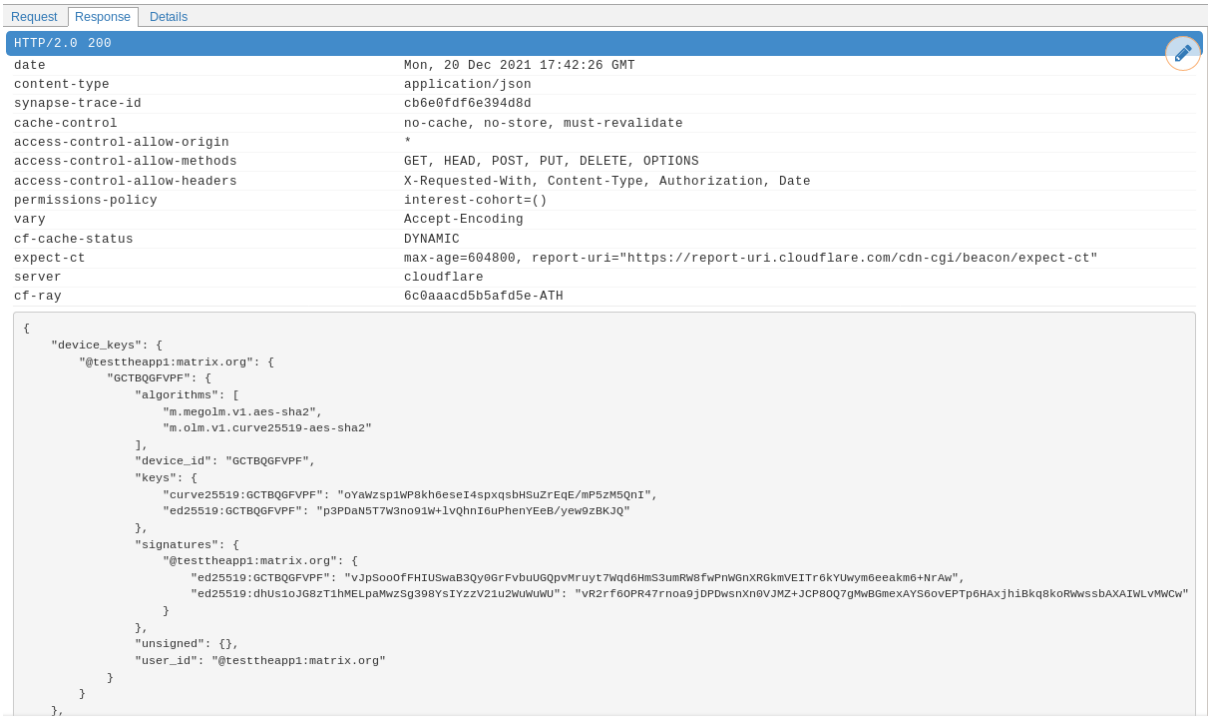
Η ανάλυση της εφαρμογής Element έδειξε ότι στη συσκευή την οποία χρησιμοποιήσαμε έδωσε ένα μοναδικό device_id και ένα διαφορετικό IP από εκείνο της συσκευής μας και τα σύνδεσε με το user_id μας στην εφαρμογή αλλά αυτά τα τρία δεν μπορούν να μας ταυτοποιήσουν άμεσα ή δεν δόθηκαν σε τρίτους.



Εικόνα 6.11: Τα χαρακτηριστικά της συσκευής μας με βάση την εφαρμογή Element.

Η κρυπτογραφία της εφαρμογής βασίζεται σε κλειδιά και end-to-end encryption όπως φαίνεται και στην πιο κάτω εικόνα. Αρχικά έχουμε τον αλγόριθμο Ed25519 ο οποίος είναι ένας αλγόριθμος δημοσίου κλειδιού ελλειπτικής καμπύλης για υπογραφή μηνυμάτων αλλά στις εφαρμογές οι οποίες χρησιμοποιούν το Matrix client χρησιμοποιείται το ζευγάρι κλειδιών για να αναγνωρίζεται

η συσκευή. Το ιδιωτικό κλειδί δεν πρέπει να φεύγει από τη συσκευή ενώ το δημόσιο δημοσιεύεται στο Matrix δίκτυο. Επιπλέον χρησιμοποιείται και ο αλγόριθμος δημοσίου κλειδιού Curve25519 σε δύο περιπτώσεις στην εφαρμογή, ως αναγνωριστικό συσκευής στη δημιουργία Olm sessions και στη δημιουργία Olm sessions πέραν της πρώτης φοράς. Πέραν των πιο πάνω έχουμε τη χρήση των Megolm encryption keys για την κρυπτογραφία των μηνυμάτων στα groups και είναι βασισμένα σε AES-256 key και HMAC-SHA256 key. Πιο συγκεκριμένα βλέπουμε τους m.olm.v1.curve25519-aes-sha2 και m.megolm.v1.aes-sha2.



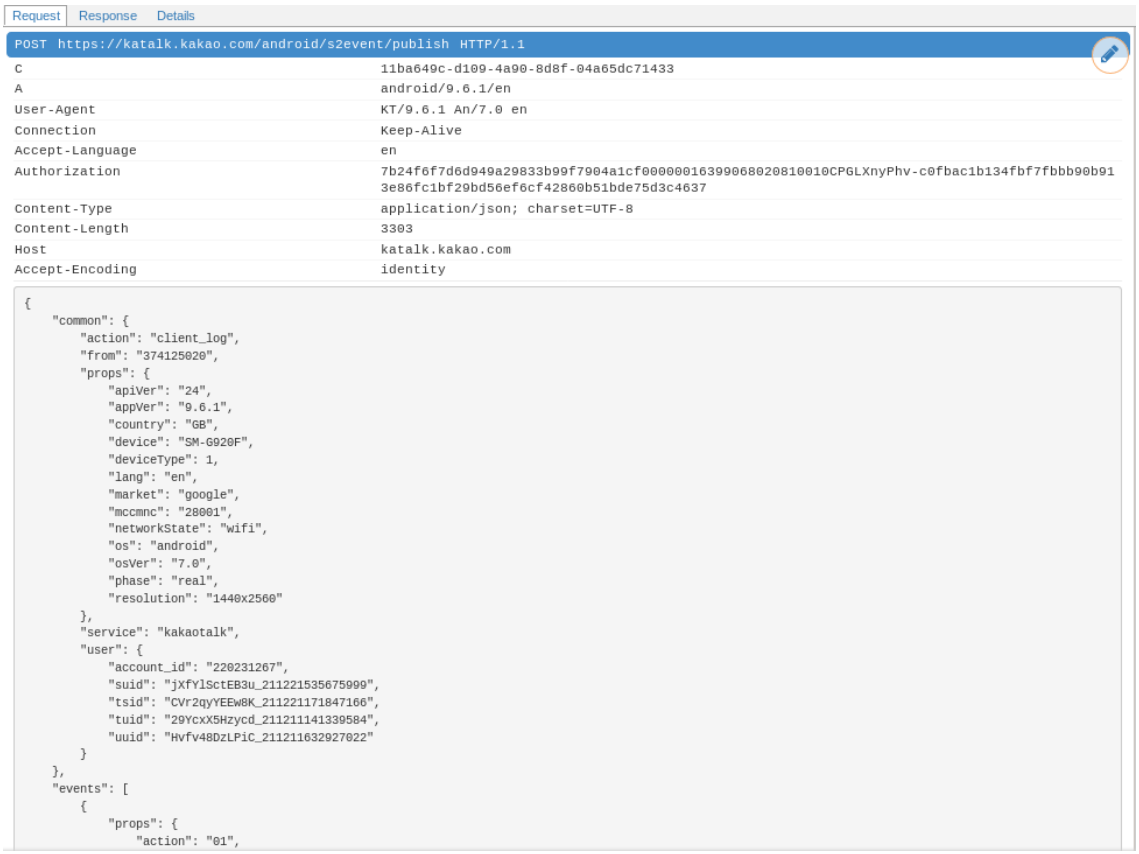
Εικόνα 6.12: Τα κρυπτογραφικά κλειδιά τα οποία αναφέρεται ότι χρησιμοποιεί η εφαρμογή Element και επιβεβαιώνονται μέσω της ανάλυσης.

Με βάση και τα πιο πάνω μπορούμε να ισχυριστούμε ότι η εφαρμογή Element υλοποιεί ασφαλείς αλγορίθμους κρυπτογράφησης, παρέχει κρυπτογραφία κατά την αποστολή μηνυμάτων και δεν υπάρχει οποιαδήποτε διαρροή δεδομένων προς τρίτους.

6.4.3 KakaoTalk

Η εφαρμογή KakaoTalk ζητά να επικοινωνήσει κατά την εκκίνηση της με τη διεύθυνση https://talk-pilsner.kakao.com/ping και καθορίζει ότι τη γλώσσα του χρήστη, στην περίπτωση μας τα αγγλικά. Όταν ο χρήστης προσπαθήσει να κάνει δημοσιοποίηση αυτό καταγράφεται ως client log και εκεί αναγράφονται πληροφορίες όπως το μοντέλο της συσκευής, η κατάσταση δικτύου της (αν υπάρχει σύνδεση Wi-Fi) , έκδοση λειτουργικού συστήματος κ.α. όπως αυτά

εμφανίζονται στην εικόνα πιο κάτω. Επιπλέον ο χρήστης έχει ένα μοναδικό αριθμό Account ID και αυτό χρησιμοποιείται όταν θα λάβει κάποιο μήνυμα. Από τις πληροφορίες που αναγράφονται στην ενέργεια του client log δεν προκύπτει, κατ' αρχάς, ότι είναι όλες αναγκαίες όπως π.χ. το resolution της συσκευής ή το μοντέλο της. Δεν εντοπίστηκε οτιδήποτε άλλο μεμπτό ή οποιαδήποτε διαρροή δεδομένων προς τρίτους.

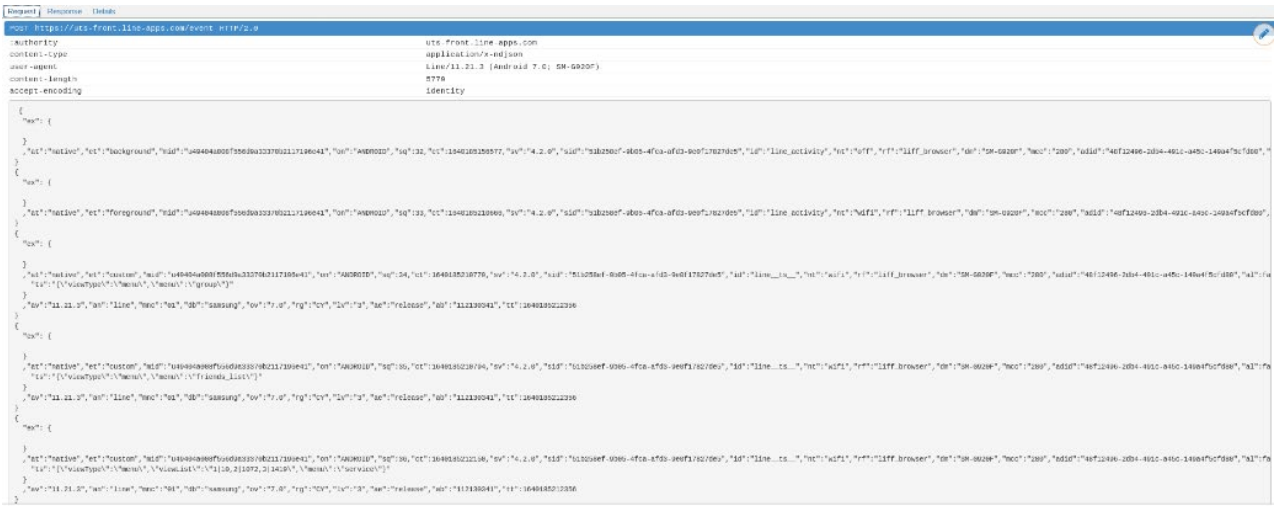


Εικόνα 6.13: Η ενέργεια η οποία καταγράφεται ως client_log από την εφαρμογή KakaoTalk.

6.4.4 Line

Η εφαρμογή κατά την έναρξη της ζητάει να φέρει δεδομένα από τη διεύθυνση https://gwg.line.naver.jp και καταγράφεται το timestamp και το start time της ενέργειας αυτής. Όταν ο χρήστης επιχειρεί να κάνει POST κάτι τότε εκεί δηλώνεται το μοντέλο της συσκευής του, το λειτουργικό σύστημα το οποίο χρησιμοποιεί και δευτερεύουσες πληροφορίες όπως network type της συσκευής (π.χ. Wi-Fi) και ένα adid. Το adid αποτελείται από 32 δεκαεξαδικούς χαρακτήρες και, συνεπώς, φαίνεται ότι είναι το advertising id της συσκευής. Αυτό χρησιμοποιείται έτσι ώστε οι διαφημίσεις να είναι σχετικές με τις προτιμήσεις του χρήστη και να έτσι να αυξηθούν τα έσοδα των εταιρειών από αυτές (τις διαφημίσεις). Το advertising ID είναι μοναδικό αναγνωριστικό της συσκευής – αν και οι χρήστες μπορούν να το αλλάζουν. Πέραν από

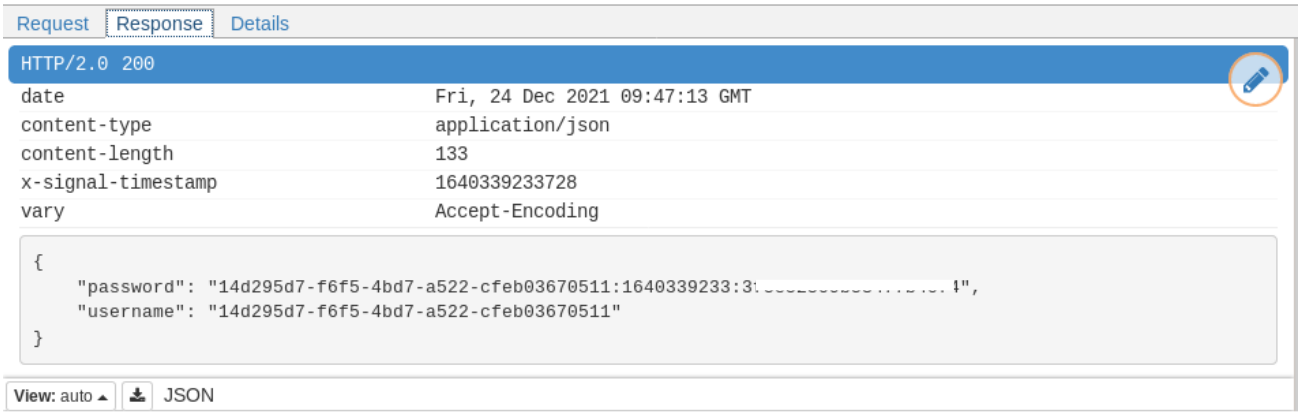
το advertising ID δεν εντοπίστηκε κάτι άλλο το οποίο να διαρρέει δεδομένα του χρήστη και ούτε εμφανίστηκε κάπου η IP διεύθυνση της συσκευής μας.



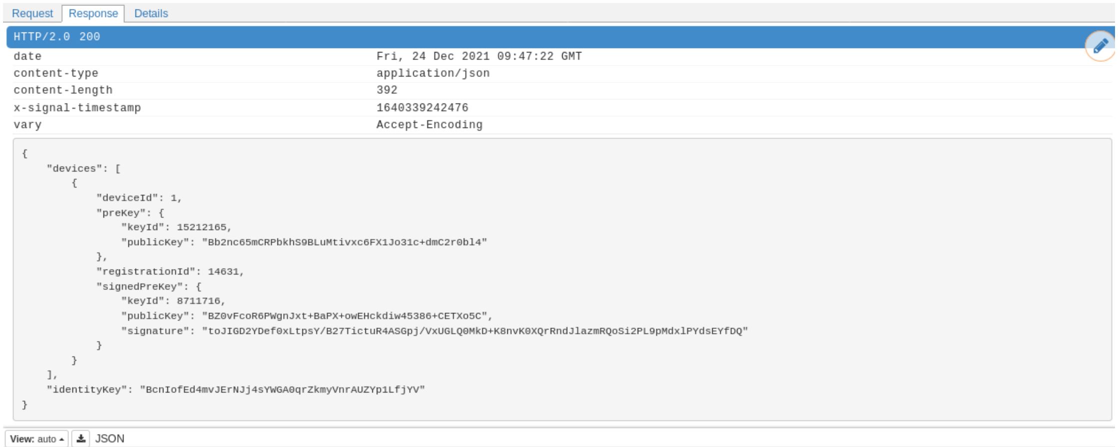
Εικόνα 6.14: Δεδομένα κατά την ενέργεια POST από το χρήστη στην εφαρμογή Line.

6.4.5 Signal

Εκκινώντας της εφαρμογή Signal ζητάει δικαιώματα από το storage.signal.org και ακολούθως μπαίνοντας στα μηνύματα από το chat.signal.org. Το username και password δεν εμφανίζονται ως κείμενο αλλά ως μοναδικό key (το κάθε ένα διαφορετικό) κρυπτογραφημένα με το Signal protocol. Στη συσκευή δίνονται δύο κλειδιά το preKey το οποίο συμπεριλαμβάνει το key ID και ένα public key και το signedPrekey το οποίο συμπεριλαμβάνει διαφορετικό key ID, το public key και μία υπογραφή (όλα κρυπτογραφημένα). Επιπλέον υπάρχει και ένα κρυπτογραφημένο identity key για αναγνώριση του χρήστη. Κατά την αποστολή μηνυμάτων δεν εντοπίστηκε οποιαδήποτε διαρροή δεδομένων σε τρίτους λόγω της κρυπτογραφίας και του Signal protocol.



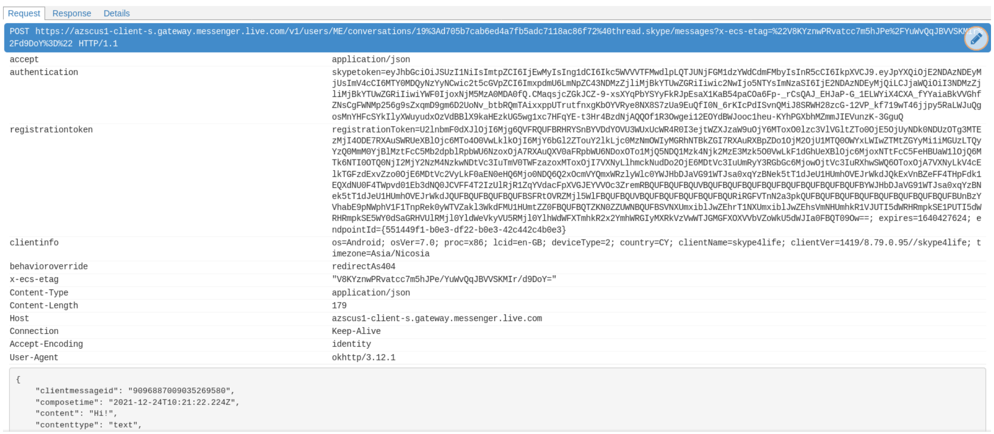
Εικόνα 6.15: Κρυπτογραφημένα το password και username μας στην εφαρμογή Signal



Εικόνα 6.16: Τα κλειδιά τα οποία αναθέτει σε κάθε συσκευή και χρήστη η εφαρμογή Signal

6.4.6 Skype

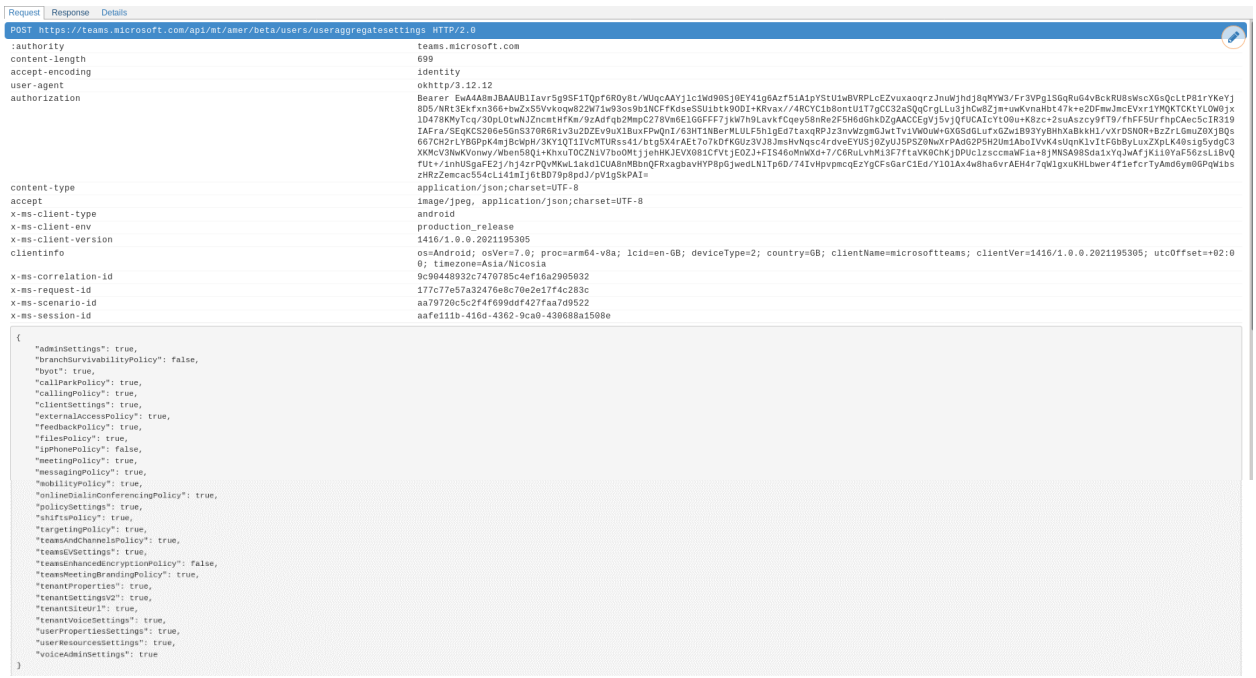
Το Skype με το που αρχίζει να εκτελείται κάνει POST στο https://prod.registrat.skype.com/v2/registrations και έπειτα βρίσκει την πλατφόρμα – λειτουργικό σύστημα μας και δίνει στον κάθε χρήστη ένα registrationId. Επιπλέον η εφαρμογή ελέγχει και το Skype Token κάθε χρήστη μέσω της σελίδας της στο /skypetokenauth χρησιμοποιώντας δύο άλλα id, το correlation id και το request id. Κατά την αποστολή μηνύματος από το χρήστη όπως φαίνεται και στην Εικόνα 6.17 αναγράφεται ένα client message id και το compose time (ώρα συγγραφής) του μηνύματος χωρίς οποιεσδήποτε πληροφορίες οι οποίες μπορούν να οδηγήσουν άμεσα σε ταυτοποίηση του αποστολέα. Παρά τις διαρροές δεδομένων τις οποίες εντόπισε το εργαλείο Lumen με τη χρήση του εικονικού περιβάλλοντος αυτές δεν εντοπίστηκαν κατά την αποστολή και λήψη μηνυμάτων – γεγονός που καταδεικνύει τόσο την εγγενή δυσκολία εντοπισμού όλων των διαρροών όσο και την αξία που αποκτά η χρήση περισσότερων του ενός εργαλείων.



Εικόνα 6.17: Καταγραφή της αποστολής μηνύματος στο Skype μέσω του εικονικού περιβάλλοντος του PI.

6.4.7 Teams

Στη δεύτερη εφαρμογή συνομιλιών της Microsoft, το Teams, δεν εντοπίστηκε η οποιαδήποτε διαρροή προσωπικών δεδομένων ή δεδομένων που να ταυτοποιούν το χρήστη. Η εφαρμογή φάνηκε ότι χρησιμοποιεί το api του Skype για τη διεκπεραίωση βιντεοκλήσεων χρησιμοποιώντας υπάρχον Skype ID αν ο χρήστης έχει κοινό λογαριασμό και στις δύο εφαρμογές (Microsoft Account). Κατά τη διεκπεραίωση μίας ενέργειας καταγράφεται η ενέργεια μαζί με το μοντέλο και το λειτουργικό σύστημα της συσκευής. Τέλος, όπως διαφάνηκε από τη μελέτη (θεωρητική / πρακτική) και φαίνεται και στην πιο κάτω φωτογραφία η κρυπτογραφία end-to-end είναι απενεργοποιημένη από προεπιλογή μιας και η ρύθμιση teamsEnhancedEncryptionPolicy έχει τιμή false (disabled). Άρα εναπόκειται στο χρήστη εάν θέλει να την ενεργοποιήσει από τις ρυθμίσεις της εφαρμογής.



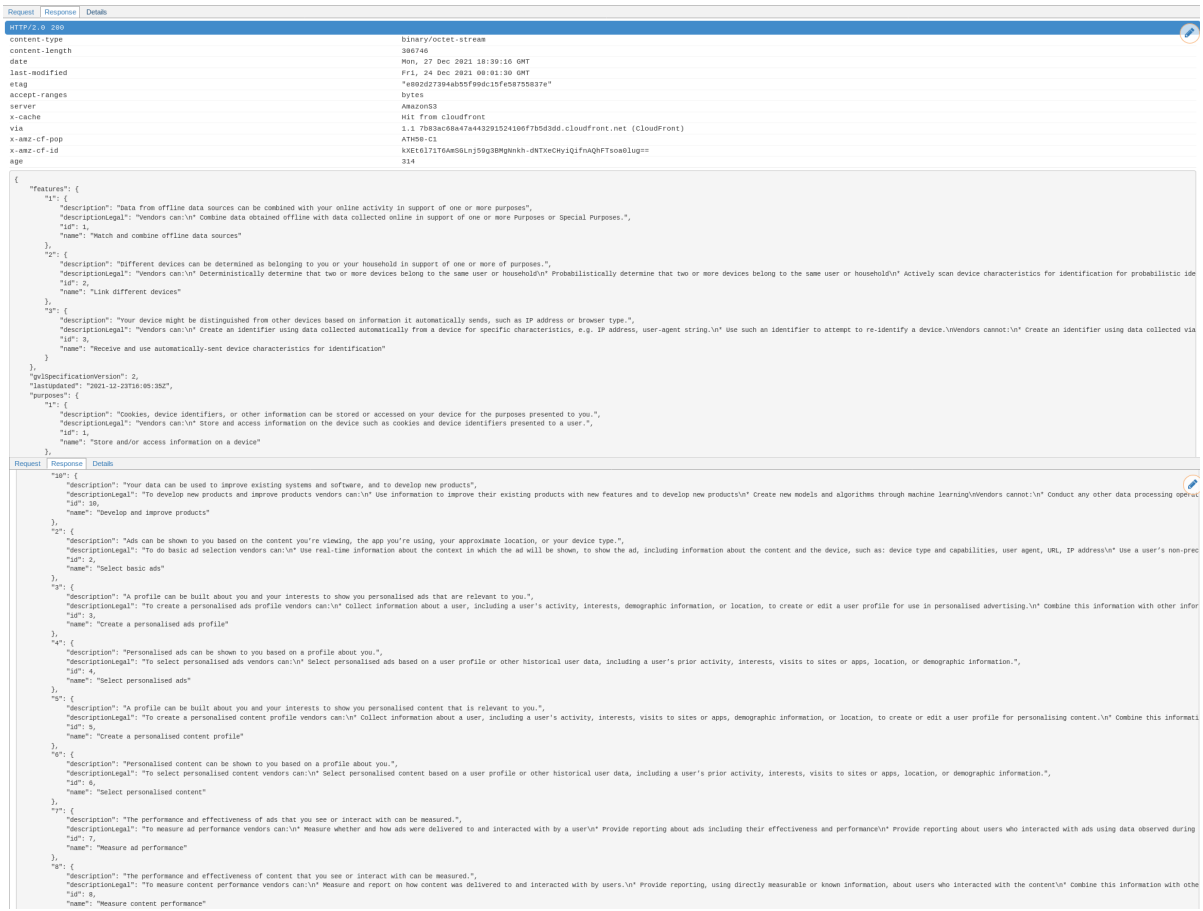
Εικόνα 6.18: Οι προεπιλεγμένες ρυθμίσεις της εφαρμογής Skype.

6.4.8 Viber

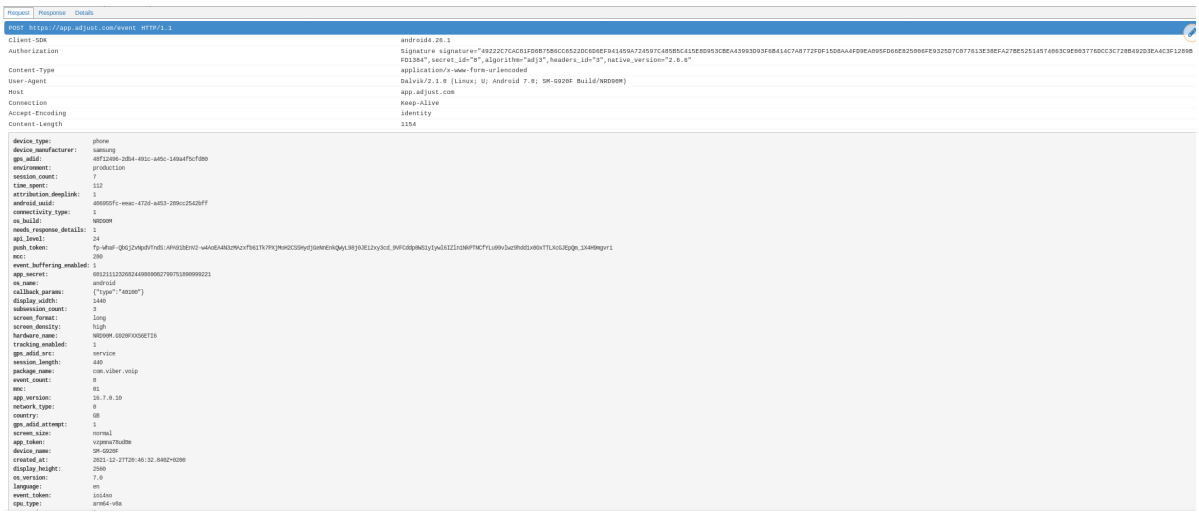
Η ανάλυση της εφαρμογής Viber έδειξε ότι κατά την εκκίνηση της έχει κάποια features και purposes μέρος των οποίων φαίνεται στην πιο κάτω εικόνα. Στα features μεταξύ άλλων υπάρχει το “Receive and use automatically-sent device characteristics for identification” ενώ μερικά από τα purposes είναι τα Cookies τα οποία έχουν όνομα “Store and/or access information on a device” και το “Develop and improve products” το οποίο αναφέρεται στη συλλογή και επεξεργασία

δεδομένων. Μέσα από αυτά τα οποία είναι ξεκάθαρα η εφαρμογή είναι «καλυμμένη» ως προς το τι προσφέρει στο χρήστη και για το πως επεξεργάζεται τα δεδομένα του αλλά και τα κριτήρια εμφάνισης διαφημίσεων. Επίσης η επιλογή “Store and/or access information on a device” εγείρει ερωτηματικά ως προς το αν πρόκειται για πληροφορία που είναι συμβατή με όσα προβλέπονται στην Οδηγία e-Privacy

Το Viber είναι η εφαρμογή η οποία συλλέγει τις περισσότερες πληροφορίες για τη συσκευή μας με πληροφορίες όπως gps_adid, android_uuid, κατασκευαστής, λειτουργικό σύστημα κ.α. (βλ. Εικόνα 6.20). Παρά τη συλλογή αυτών των δεδομένων δεν φάνηκε να αποστέλλεται το οτιδήποτε σε τρίτους ή κάποια άλλη συλλογή δεδομένων.



Εικόνα 6:19: Τα features και purposes τα οποία αναφέρει η εφαρμογή Viber



Εικόνα 6.20: Συλλογή δεδομένων της συσκευής μας από την εφαρμογή Viber

6.4.9 Webex Meet

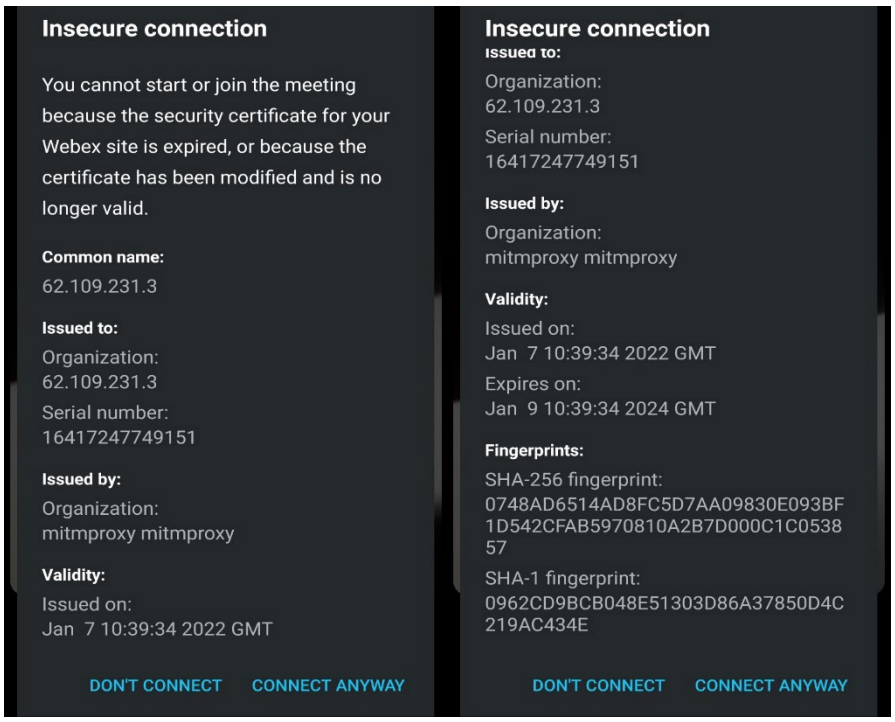
Η είσοδος στην εφαρμογή γίνεται δίνοντας στο χρήστη ένα access token και ένα authentication id. Στους υπόλοιπους χρήστες εμφανίζεται το αρχικό όνομα και ηλεκτρονική διεύθυνση τα οποία χρησιμοποιούνται για δημιουργία λογαριασμού. Ο κάθε χρήστης έχει το δικό του User ID. Για τη διεξαγωγή τηλεδιάσκεψης υπάρχει το client_id και ένας μυστικός κωδικός ο client secret. Κατά την τηλεδιάσκεψη δεν εντοπίστηκε οποιαδήποτε διαρροή δεδομένων προς τρίτους.

6.4.10 WhatsApp

Μέσω του εικονικού περιβάλλοντος δεν εντοπίστηκε οποιαδήποτε διαρροή δεδομένων προσωπικού χαρακτήρα ή κάτι άλλο το μεμπτό προς τρίτους για την εφαρμογή του WhatsApp.

6.4.11 Zoom

Η εφαρμογή Zoom θεώρησε ότι το mitmproxy πιστοποιητικό είχε λήξει και κατέστησε insecure τη σύνδεση και δεν μας επέτρεψε να κάνουμε βιντεοκλήσεις για έλεγχο της εφαρμογής μέσω του εικονικού περιβάλλοντος. Αυτό είναι ένα αρκετά καλό μέτρο ασφάλειας για την εφαρμογή.



Εικόνα 6.21: Αδυναμία χρήσης του Zoom με το πιστοποιητικό mitmproxy

6.5 Σύγκριση αποτελεσμάτων με την πολιτική προστασίας των εφαρμογών

Τα αποτελέσματα τα οποία συλλέχθηκαν από το Περιβάλλον δοκιμών για τις εφαρμογές χρειάζεται να γίνουν σύγκριση με την πολιτική προστασίας κάθε εφαρμογής για να διαφανεί κατά πόσο ζητάνε περισσότερα δικαιώματα από αυτά που αναγράφονται και αν η γίνεται διαφανής επεξεργασία προσωπικών δεδομένων. Με πιο απλά λόγια πιο κάτω θα δούμε ανά εφαρμογή εάν είναι συμβατή με την πολιτική προστασίας της και αυτό που κάνει δικαιολογεί τη λειτουργικότητα της.

6.5.1 Discord

Η πολιτική προστασίας δεδομένων βρίσκεται στη διεύθυνση https://discord.com/privacy και είναι χωρισμένη σε δεκαπέντε κεφάλαια. Για τους σκοπούς μας θα χρησιμοποιήσουμε τα κεφάλαια στα οποία γίνεται αναφορά στα δεδομένα του χρήστη, ποια δεδομένα δίνει ο ίδιος, ποια

δεδομένα συλλέγονται αυτόματα και ποιος ο τρόπος επεξεργασίας και προστασίας αυτών των δεδομένων.

Η εφαρμογή συλλέγει δεδομένα τα οποία δίνει ο χρήστης όπως το όνομα χρήστη και ο κωδικός τα οποία απαιτούνται για τη δημιουργία λογαριασμού, τρόπο επικοινωνίας (ηλεκτρονική διεύθυνση ή αριθμός τηλεφώνου), ηλικία, τρόπο πληρωμής (π.χ. αριθμό κάρτας και διεύθυνση χρέωσης) κ.α.. Ο χρήστης εάν χρειαστεί μπορεί να δώσει πρόσβαση στις Επαφές του για να συγχρονιστούν και να χρησιμοποιήσει συγκεκριμένες λειτουργίες της εφαρμογής (Read_Contacts permission) αλλά και σε τρίτους (third-party services) με τη σύνδεση π.χ. υπηρεσίας μουσικής αλλά με το τίμημα ότι το Discord συλλέγει τα δεδομένα αυτά.

Παρά τα δεδομένα τα οποία δίνει ο χρήστης η εφαρμογή συλλέγει αυτόματα δεδομένα για τη συσκευή (IP address, λειτουργικό σύστημα, μικρόφωνο, κάμερα) κάτι το οποίο δικαιολογεί δικαιώματα όπως Camera, Record Audio μιας και είναι εφαρμογή ανταλλαγής μηνυμάτων με τη δυνατότητα βιντεοκλήσεων και τηλεφωνικών κλήσεων. Επιπλέον η εφαρμογή συλλέγει δεδομένα για τη χρήση της εφαρμογής από τον χρήστη (σελίδες που επισκέπτεται, servers και channels που χρησιμοποιεί) και αν αυτός (ο χρήστης) πατήσει πάνω σε μία διαφήμιση ενημερώνεται η εφαρμογή εξού και η χρήση διαφημιστικών ιχνηλατών όπως το Adjust. Τέλος, όσο αφορά τα δεδομένα τα οποία συλλέγονται αυτόματα περιλαμβάνονται και τα Cookies τα οποία μπορεί να είναι της εταιρείας (first-party) ή από τρίτους (third-party) και χωρίζονται σε τρεις κατηγορίες, Strictly Necessary, Functional και Performance. Η εφαρμογή αναφέρει ότι η χρήση τους απαιτείται για να επιτραπεί στο χρήστη η χρήση των υπηρεσιών της και για να τη βοηθήσει να κάνει ανάλυση και βελτίωση της εμπειρίας του χρήστη και των υπηρεσιών της.

Τα πιο πάνω δεδομένα αρχικά χρησιμοποιούνται για να προσφερθούν οι υπηρεσίες της εφαρμογής στο χρήστη όπως για παράδειγμα κατά τη διάρκεια μιας βιντεοκλήσης οι φωτογραφίες και ο ήχος τυγχάνουν επεξεργασίας για τη σωστή διεκπεραίωση της (βιντεοκλήσης). Για να είναι ένας ασφαλής χώρος ανταλλαγής μηνυμάτων (χωρίς ύβρεις, ρατσισμό, malware κ.τ.λ.) χρησιμοποιούνται τα πιο πάνω συλλεγόμενα δεδομένα αλλά και για να παρέχεται στο χρήστη ένα πιο προσωπικό προϊόν και ότι εμφανίζεται να είναι σχετικό με το τι του αρέσει. Επιπλέον τα δεδομένα χρησιμοποιούνται για την επικοινωνία χρήστη – εφαρμογής και για μία καλύτερη εξυπηρέτηση πελατών (customer service) σε τυχόν απορίες ή άλλα προβλήματα. Τέλος, τα δεδομένα μπορεί να χρησιμοποιηθούν και για επαγγελματικούς σκοπούς της εφαρμογής όπως η διαφήμιση της σε άλλες πλατφόρμες για προσέλκυση νέων χρηστών και για βελτίωση των υπηρεσιών της εφαρμογής.

Τα δεδομένα αναφέρεται ότι είναι κρυπτογραφημένα όπως διαφάνηκε και από τη μελέτη μας και η εταιρεία αναφέρει ότι οι υπάλληλοι της έχουν περιορισμένη πρόσβαση σε μη δημόσιες προσωπικές πληροφορίες. Η εφαρμογή δίνει τη δυνατότητα στο χρήστη να ελέγξει τα δεδομένα και την ιδιωτικότητα του επιλέγοντας ο ίδιος τους Discord servers στους οποίους θα συμμετάσχει, από τις ρυθμίσεις όπου μεταξύ άλλων δίνεται η δυνατότητα να απενεργοποιήσει τα "Use data to improve Discord" και "Use data to customize my Discord experience", αλλά και να διαχειριστεί τα Cookies και τα δεδομένα τα οποία αυτά συλλέγουν.

Κλείνοντας, για την εφαρμογή Discord μπορούμε να ισχυριστούμε ότι είναι συμβατή με την προστασία προσωπικών δεδομένων, η πολιτική προστασίας της είναι σαφής και αυτό που κάνει δικαιολογεί τη διαλειτουργικότητα της. Μεταξύ των ιχνηλατών οι οποίοι εντοπίστηκαν υπήρχαν ιχνηλάτες για διαφημιστικούς σκοπούς και ιχνηλάτες τρίτων εταιρειών κάτι το οποίο αναφέρεται στην πολιτική προστασίας της εφαρμογής. Δικαιολογημένα είναι και τα «επικίνδυνα» δικαιώματα τα οποία εντοπίστηκαν καθώς αρχικά είναι εφαρμογή η οποία τα χρειάζεται για τη λειτουργία της (π.χ. Camera) και άλλα δίνονται μόνο εάν το αποδεχτεί ο χρήστης για συγκεκριμένες υπηρεσίες της εφαρμογής.

6.5.2 Element

Η πολιτική προστασίας δεδομένων της εφαρμογής είναι αρκετά απλοποιημένη και όπως αναφέρεται σε αυτή "we decided to use plain English as much as possible" και βρίσκεται στη διεύθυνση https://element.io/privacy . Το κείμενο αναφέρεται και στις υπόλοιπες εφαρμογές της εταιρείας, όπως το Gitter, αλλά εμείς θα επικεντρωθούμε στα δεδομένα που συλλέγονται από τους Element χρήστες (users).

Αρχικά η εφαρμογή συλλέγει την IP address του χρήστη όταν αυτός ζητήσει πρόσβαση στον client του Element από τον web server τους και αυτό το κάνει για την υποστήριξη της λειτουργικής συντήρησης της εφαρμογής και προστασία από κακόβουλες ενέργειες κατά της υποδομής της εφαρμογής. Η πολιτική προστασίας αναφέρει ξεκάθαρα τα δικαιώματα του υποκειμένου δεδομένων κάτω από τον GDPR όπου μεταξύ άλλων είναι τα δικαιώματα της πληροφόρησης, της πρόσβασης και της διαγραφής. Ο σκοπός συλλογής δεδομένων είναι ο ίδιος με το σκοπό συλλογής της IP Address κατά την πρώτη σύνδεση με την εφαρμογή και ο χρήστης δίνει κάποια δεδομένα στην εφαρμογή με τη δημιουργία λογαριασμού. Αυτά τα δεδομένα χρησιμοποιούνται με φειδώ στο ελάχιστο και είναι η ηλεκτρονική διεύθυνση και ένα αναγνωριστικό ταυτοποίησης (authentication identifier) το οποίο μπορεί να είναι ένα εκ των ηλεκτρονική διεύθυνση και

κωδικός, Twitter id ή Google id. Το αναγνωριστικό χρησιμοποιείται για να ταυτοποιηθεί ο χρήστης ως μοναδικός (unique) και να αποκτήσει πρόσβαση στο Element Matrix Services. Εάν ο χρήστης προχωρήσει σε αγορές στην εφαρμογή αυτό γίνεται με τον επεξεργαστή πληρωμών (payment processor) της εταιρείας, το Stripe, αλλά δεν αποθηκεύονται ούτε χρησιμοποιούνται τα δεδομένα όπως τα πλήρης στοιχεία πιστωτικής κάρτας (full credit card information).

Η εφαρμογή μπορεί να συλλέξει πληροφορίες από διαφημίσεις της σε τρίτους όπως π.χ. LinkedIn, Twitter ή Google εάν ο χρήστης της πατήσει και να πάρει δεδομένα όπως ηλεκτρονική διεύθυνση, τόπος εργασίας και θέση εργασίας. Ενημερώνοντας βεβαίως το χρήστη για το νομικό πλαίσιο επεξεργασίας αυτών των δεδομένων του. Πέραν από την IP address η οποία συλλέγεται αυτόματα η εφαρμογή συλλέγει και δεδομένα για τη χρήση της από το χρήστη (usage data) για να κατανοήσει το πως χρησιμοποιείται η εφαρμογή και παράλληλα να βελτιωθεί. Η επεξεργασία αυτών των δεδομένων γίνεται με την ανοικτού κώδικα πλατφόρμα Matomo πάνω στο δίκτυο του Element και τα δεδομένα (analytics) δεν δίνονται σε τρίτους. Ο χρήστης έχει τη δυνατότητα αν θέλει να μην συμμετάσχει σε αυτή τη διαδικασία και τη συλλογή ανώνυμων δεδομένων για βελτίωση της εφαρμογής.

Ολοκληρώνοντας. η εφαρμογή έχει μία ξεκάθαρη και σαφή πολιτική και τα επικίνδυνα δικαιώματα τα οποία ζητάει κρίνεται ότι είναι αναγκαία για τη λειτουργικότητα της. Τα δικαιώματα αυτά δίνονται μόνο εάν το επιτρέψει ο χρήστης και είναι τα απολύτως αναγκαία για τη χρήση της εφαρμογής ως μέσο ανταλλαγής μηνυμάτων και επικοινωνίας (βιντεοκλήσεις και φωνητικές κλήσεις).

6.5.3 KakaoTalk

Η εφαρμογή KakaoTalk προσφέρει την πολιτική προστασίας δεδομένων της σε τρεις γλώσσες, Κορεάτικα, Αγγλικά και Γιαπωνέζικα και μπορεί κανείς να τη βρει στη διεύθυνση https://www.kakao.com/policy/privacy . Είναι ένα σχετικά ευανάγνωστο κείμενο αναφερόμενο κυρίως στη συλλογή και επεξεργασία προσωπικών δεδομένων. Αρχίζει λέγοντας ότι η συλλογή δεδομένων γίνεται μόνο με τη συγκατάθεση του χρήστη και έχει δικαίωμα ο ίδιος σε αυτά και στον έλεγχο τους.

Το Kakao συλλέγει τα λιγότερα δυνατά δεδομένα για να προσφέρει τις υπηρεσίες του και χωρίζονται σε διάφορες κατηγορίες. Τα υποχρεωτικά που είναι ο λογαριασμός στην εφαρμογή (ηλεκτρονική διεύθυνση, κωδικός, ψευδώνυμο (nickname), κα.), τα προαιρετικά όπως η

ημερομηνία γέννησης και το φύλο, τα δεδομένα για ταυτοποίηση όπως αριθμός τηλεφώνου, και τα απαιτούμενα για την εξυπηρέτηση πελατών που είναι ο αριθμός τηλεφώνου και η ηλεκτρονική διεύθυνση. Κατά τη συλλογή προσωπικών δεδομένων η εφαρμογή ενημερώνει το χρήστη για αυτό και προχωράει μόνο με τη συγκατάθεση του. Επιπλέον προσωπικά δεδομένα μπορεί να συλλεχθούν όπως πληροφορίες για τη συσκευή σαν αυτές που εντοπίστηκαν μέσω του εικονικού περιβάλλοντος (screen resolution, λειτουργικό σύστημα, device ID), IP address, cookies κα.

Τα δεδομένα τα οποία συλλέγονται χρησιμοποιούνται μεταξύ άλλων για ταυτοποίηση του συνδρομητή και της ηλικίας του για σωστή και νόμιμη χρήση της εφαρμογής , για τη δυνατότητα χρήσης των υπηρεσιών της εφαρμογής όπως η αποστολή μηνυμάτων, ψηφιακού περιεχομένου, λήψη ειδοποιήσεων κ.α.. Επιπλέον χρησιμοποιούνται για εμπορικούς και διαφημιστικούς σκοπούς και για στατιστική ανάλυση της χρήσης της εφαρμογής. Όλα τα δεδομένα αναφέρεται ότι είναι κρυπτογραφημένα και μεταφέρονται μέσω κρυπτογραφημένων καναλιών.

Η πολιτική προστασίας αναφέρει ρητά ότι προσωπικά δεδομένα δεν αποστέλλονται σε τρίτους χωρίς τη συγκατάθεση του χρήστη ή την απαίτηση από τον νόμο. Το δεύτερο κομμάτι εφαρμόζεται με κάποια δεδομένα να αποστέλλονται σε έμπιστα τρίτα μέρη τα οποία προσφέρουν υπηρεσίες όπως η πιστοποίηση της ηλικίας του χρήστη για υπηρεσίες που απαιτείται. Τα προσωπικά δεδομένα του χρήστη καταστρέφονται μόλις ολοκληρωθεί ο σκοπός της συλλογής τους με συγκεκριμένα δεδομένα όπως ηλεκτρονική διεύθυνση να καταστρέφονται ένα χρόνο μετά την αίτηση διαγραφής του λογαριασμού. Ο χρήστης επιπλέον, έχει τη δυνατότητα να ρωτήσει και να επεξεργαστεί τα δεδομένα του ανά πάσα στιγμή και να αποσύρει τη συγκατάθεση του για συλλογή δεδομένων του εάν το επιθυμεί.

Καταλήγοντας, μπορούμε να ισχυριστούμε ότι η εφαρμογή KakaoTalk έχει μία σαφή πολιτική προστασίας δεδομένων αναφέροντας ξεκάθαρα στο ότι η χρήση της συνεπάγεται και συλλογή προσωπικών δεδομένων άλλα από τα αναμενόμενα π.χ. μέγεθος οθόνης συσκευής. Άρα τα όσα εντοπίστηκαν μέσω του περιβάλλοντος δοκιμών δικαιολογούνται, τόσο οι ιχνηλάτες όσο και τα επικίνδυνα δικαιώματα.

6.5.4 Line

Η πολιτική προστασίας δεδομένων της εταιρείας LINE αρχίζει αναφέροντας ότι συλλέγει δεδομένα ατόμων για να μπορέσει να προσφέρει την εφαρμογή της και τις υπόλοιπες υπηρεσίες της αλλά με γνώμονα την ασφάλεια των προσωπικών δεδομένων και με συμμόρφωση στους

σχετικούς νόμους και οδηγίες. Η πολιτική βρίσκεται στη διεύθυνση https://line.me/en/terms/policy/ .

Η εφαρμογή συλλέγει προσωπικά δεδομένα τόσο από αυτά που δίνονται από το χρήστη όσο και αυτόματα κατά τη χρήση των υπηρεσιών της εφαρμογής. Στην πρώτη κατηγορία ανήκουν δεδομένα όπως ο αριθμός τηλεφώνου κατά τη δημιουργία λογαριασμού ή δεδομένα από άλλο κοινωνικό δίκτυο αν αυτό χρησιμοποιηθεί για τη δημιουργία λογαριασμού π.χ. Facebook. Στη δεύτερη κατηγορία εμπίπτουν δεδομένα σχετικά με τη χρήση της εφαρμογής από το χρήστη όπως κείμενα, φωτογραφίες ή βίντεο που κοινοποιεί αλλά και δεδομένα σχετικά με το χρήστη τα οποία κοινοποιούν άλλοι χρήστες – φίλοι. Κατά τη μελέτη μας εντοπίστηκε η εφαρμογή να ζητάει το δικαίωμα Read_Contacts και αυτό δικαιολογείται μιας και υπάρχει η επιλογή "Auto Add Friends" και μπορεί να προσθέσει άλλους Users από τις Επαφές του χρήστη ως φίλους στην εφαρμογή αλλά μόνο αν ο ίδιος ο χρήστης το ενεργοποιήσει. Το ίδιο ισχύει και με τα δικαιώματα για την τοποθεσία μιας και ο χρήστης μπορεί να θέλει να μοιραστεί την τοποθεσία του με τους φίλους του και η εφαρμογή έχει τη δυνατότητα να συλλέξει αυτή την πληροφορία. Εάν ο χρήστης δεν αποδεχτεί την πρόσβαση στην τοποθεσία του αναφέρεται ξεκάθαρα ότι μπορεί η εφαρμογή να υπολογίσει την πιθανή του τοποθεσία με βάση το IP address του.

Κάτι το οποίο εντοπίστηκε μέσω του περιβάλλοντος δοκιμών ήταν ένα ad identifier το οποίο όπως δηλώνεται στην πολιτική προστασίας της εφαρμογής αυτό συλλέγεται ως δεδομένο σχετικό με τη συσκευή και την εφαρμογή μαζί με ένα Cookie ID και τον τύπο της εφαρμογής, το λειτουργικό σύστημα, την γλώσσα και τη ζώνη ώρας. Επιπλέον συλλέγονται πληροφορίες για το δίκτυο όπως IP address, πάροχος τηλεφωνίας κ.α. Η εφαρμογή μπορεί να συλλέξει και δεδομένα από υπηρεσίες τρίτων εάν υπάρχει plug-in για χρήση του Line αλλά και από δημόσιες πληροφορίες σχετικά με ένα χρήστη όπως π.χ. ειδήσεις στο διαδίκτυο.

Ο σκοπός αυτών των δεδομένων χωρίζεται σε τέσσερα μέρη. Τα τέσσερα αυτά μέρη είναι η παροχή και συντήρηση των υπηρεσιών, η ανάπτυξη και βελτίωση των υπηρεσιών και του περιεχομένου, η αποτροπή μη εξουσιοδοτημένης χρήσης ή πρόσβασης και τέλος παροχή βελτιστοποιημένου περιεχομένου για το χρήστη (π.χ. διαφημίσεις) . Η εφαρμογή δεν θα παρέχει ποτέ τα προσωπικά δεδομένα σε τρίτους χωρίς τη συγκατάθεση του χρήστη ή χωρίς να υποχρεούται από το νόμο. Τα δεδομένα τα οποία συλλέγονται είναι κρυπτογραφημένα και παρέχεται συνεχής παρακολούθησης της ασφάλειας τους με το χρήστη να έχει τη δυνατότητα επιλογών πάνω στα δεδομένα του. Μέσα από την πολιτική ασφαλείας αναφέρεται ξεκάθαρα η

χρήση third-party modules (ιχνηλάτες) και Cookies για σκοπούς ανάλυσης της χρήσης της εφαρμογής και για διαφημιστικούς σκοπούς.

Τελειώνοντας, θεωρούμε ότι η εφαρμογή παρέχει μία ξεκάθαρη πολιτική προστασίας δεδομένων όπου αναφέρονται και δικαιολογούνται όλα όσα εντοπίστηκαν στη μελέτη μας (π.χ. ad identifier). Τα δικαιώματα τα οποία ζητάει η εφαρμογή είναι τα αναγκαία για τη διαλειτουργικότητα της. Ωστόσο, γεννώνται κάποια ερωτηματικά για κάποια δεδομένα που συλλέγονται, όπως ο πάροχος της τηλεφωνίας του χρήστη.

6.5.5 Messenger

Η πολιτική προστασίας δεδομένων της εφαρμογής Messenger είναι κοινή για όλα τα προϊόντα και υπηρεσίες της εταιρείας Meta, όπως το Facebook και το Instagram και είναι προσβάσιμη από τη διεύθυνση https://www.facebook.com/policy.php. Αυτό βέβαια αποτελεί ένα σημείο που χρήζει βελτίωσης, γιατί έτσι ένας χρήστης μόνο μίας εφαρμογής της εταιρείας δεν μπορεί να είναι απόλυτα σίγουρος, μελετώντας την ενιαία πολιτική προστασίας δεδομένων, ποια/ποιες επεξεργασία/ες που περιγράφονται εκεί αφορούν τη συγκεκριμένη εφαρμογή.

Η εταιρεία Meta για να είναι σε θέση να προσφέρει τα προϊόντα της χρειάζεται να επεξεργαστεί τα δεδομένα των χρηστών. Αρχίζοντας συλλέγονται δεδομένα από το τι κοινοποιεί ο χρήστης τόσο κατά την εγγραφή του στην εφαρμογή (π.χ. ηλεκτρονική διεύθυνση) όσο και κατά τη χρήση της όπως μηνύματα, φωτογραφίες κ.α.. Από τη δεύτερη κατηγορία δεδομένων συχνά συλλέγονται μεταδεδομένα (metadata) όπως η τοποθεσία μίας φωτογραφίας αλλά και το τι βλέπει ο χρήστης χρησιμοποιώντας την Κάμερα μέσω του Messenger, εξού και το δικαίωμα στην Camera το οποίο απαιτείται. Επιπλέον συλλέγονται δεδομένα για τη χρήση της εφαρμογής από τους χρήστες όπως τα χαρακτηριστικά τα οποία χρησιμοποιούν περισσότερο αλλά και δεδομένα επαφών, τηλεφωνικών κλήσεων ή μηνυμάτων εάν ο χρήστης αποδεχτεί τα αντίστοιχα δικαιώματα. Τέλος, όσον αφορά τα δεδομένα τα οποία συλλέγονται από το χρήστη αυτά μπορεί να είναι και από τις αγορές του με δεδομένα όπως ο αριθμός πιστωτικής / χρεωστικής κάρτας είτε από πράγματα που κοινοποιούν άλλοι για το χρήστη όπως π.χ. εικόνες με φίλους. Για ολοκλήρωση της αγοράς μέσω ηλεκτρονικής πληρωμής θα πρέπει η εφαρμογή να παραπέμπει το χρήστη σε ασφαλές ιστοσελίδα Τράπεζας για να μην της είναι γνωστά τα δεδομένα πιστωτικών καρτών.

Τα δεδομένα συλλέγονται και από τις συσκευές όπου γίνεται χρήση της εφαρμογής και αυτά μπορεί να είναι πληροφορίες για το λειτουργικό σύστημα, τον αποθηκευτικό χώρο, το Bluetooth,

τη δύναμη στη σύνδεση Wi-Fi, την τοποθεσία, την IP Address κ.α.. Επιπλέον μπορεί να είναι μοναδικά χαρακτηριστικά (unique identifiers), χαρακτηριστικά συσκευής (device IDs) ή κάποιο άλλο χαρακτηριστικό από άλλη εφαρμογή της εταιρείας Meta πέραν του Messenger. Εννοείται ότι και η εφαρμογή Messenger κάνει χρήση των Cookies τα οποία αποθηκεύονται στη συσκευή και περιέχουν πληροφορίες για ρυθμίσεις και cookies ids. Υπάρχουν και τα δεδομένα από τις διαφημίσεις και άλλους συνεργάτες της εταιρείας Meta τα οποία αποστέλνονται στην εταιρεία σε συνεχή βάση.

Σκοπός της συλλογής των δεδομένων είναι αρχικά να προσφέρει η εταιρεία ένα βελτιωμένο προϊόν βασισμένο στο χρήστη (personalize). Υπάρχουν όμως και άλλοι μικρότεροι σκοποί οι οποίοι είναι η προώθηση της ασφάλειας και της ακεραιότητας κατά τη χρήση της εφαρμογής, η επικοινωνία με την εταιρεία (customer support), η έρευνα και καινοτομία για το κοινό καλό και η βοήθεια στις εταιρείες διαφημίσεων για το πόσο επιτυχημένες είναι οι διαφημίσεις τους μέσα από αναλυτικά στοιχεία. Η επεξεργασία των δεδομένων γίνεται κάτω από το υφιστάμενο νομικό πλαίσιο και επεξεργάζονται μόνο τα αναγκαία δεδομένα.

Κλείνοντας, η πολιτική προστασίας δεδομένων του Messenger – Meta Products είναι αρκετά ξεκάθαρη και ενημερώνει το χρήστη για την κάθε ενέργεια της εταιρείας σε ότι αφορά τα προσωπικά δεδομένα. Τα επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν ότι ζητάει η εφαρμογή είναι αναγκαία για τη διαλειτουργικότητα της και οι ιχνηλάτες οι οποίοι χρησιμοποιούν δεν κρίνεται ότι διαρρέουν υπέρμετρα δεδομένα χρηστών.

6.5.6 Phoenix

Η εταιρεία Unimania, η οποία δημιούργησε το Phoenix έχει από τα τέλη Μαρτίου 2020 να ανανεώσει την πολιτική ασφάλειας της και βρίσκεται σε μία μη ασφαλής διεύθυνση την http://privacy.unimania.xyz/privacy_policy_pnx.html. Η πολιτική της αρχίζει λέγοντας ότι τα δεδομένα τα οποία συλλέγονται από την εφαρμογή (Phoenix) επεξεργάζονται ανώνυμα και μη προσωπικά και δεν συλλέγονται ή αποθηκεύονται προσωπικά δεδομένα χωρίς τη συγκατάθεση του χρήστη. Ακόμη δεν παρακολουθείται η δραστηριότητα στην εφαρμογή εκτός και εάν ο χρήστης πατήσει πάνω σε μία διαφήμιση.

Τα δεδομένα τα οποία συλλέγονται είναι το πλήρες όνομα του χρήστη (full name), η ηλεκτρονική διεύθυνση και οποιαδήποτε άλλη πληροφορία παρέχει ο χρήστης και ο σκοπός τους είναι για να μπορεί να απαντήσει αργότερα η εταιρεία σε ερωτήσεις ή να επικοινωνήσει με το χρήστη. Τα

δεδομένα αυτά μοιράζονται και με το Gmail Business το οποίο χρησιμοποιείται για επικοινωνία με το χρήστη. Επιπλέον συλλέγονται μη προσωπικά και στατιστικά δεδομένα εάν ο χρήστης πατήσει πάνω σε μία διαφήμιση και επεξεργάζονται αυτά τα δεδομένα ανώνυμα με το user ID του κάθε χρήστη. Η εφαρμογή δημιουργεί Log files για πιθανά σφάλματα (errors) και σε αυτά τα αρχεία περιλαμβάνονται πληροφορίες όπως IP address, internet service provider (ISP) κα.

Κατά τη μελέτη μας εντοπίστηκαν τρεις ιχνηλάτες στην εφαρμογή Phoenix οι Google Crashlytics, Google Firebase Analytics και Apps Flyer με τους δύο τελευταίους να περιγράφονται στην πολιτική προστασίας μαζί με τον ιχνηλάτη Google Analytics ο οποίος δεν εντοπίστηκε από το περιβάλλον δοκιμών. Η τοποθεσία του χρήστη εντοπίζεται με τη χρήση του εργαλείου MaxMind του οποίου δίνεται η πολιτική προστασίας εάν θέλει κάποιος να τη μελετήσει. Τα πιο πάνω δεδομένα συλλέγονται για ανάλυση του πως οι εταιρείες διαφημίζουν το προϊόν τους στα μέσα κοινωνικής δικτύωσης και σε ποιο κοινό απευθύνονται. Αυτά τα δεδομένα, όπως η εταιρεία αναφέρει, δεν είναι σε θέση να ταυτοποιήσουν τον κάθε χρήστη μιας και είναι ανώνυμα και μη προσωπικά και διαγράφονται με το πέρας της επεξεργασίας τους.

Ολοκληρώνοντας μπορούμε να ισχυριστούμε ότι η πολιτική προστασίας δεδομένων για την εφαρμογή Phoenix χρήζει βελτίωσης. Κατ' αρχάς η πολιτική αναφέρεται σε ανώνυμα δεδομένα, ενώ κάνει σαφώς επεξεργασία προσωπικών δεδομένων. Η επίσκεψη σε μία σελίδα μη ασφαλής (http αντί https) εγείρει ερωτήματα και η πολιτική δεν έχει ανανεωθεί από το Μάρτιο του 2020. Τα όσα εντοπίστηκαν από το περιβάλλον δοκιμών μας δικαιολογούνται και περιγράφονται στην πολιτική προστασίας και αυτό αποτελεί θετικό στοιχείο για την εφαρμογή.

6.5.7 Session

Το Session θεωρείται από πολλούς η πιο ασφαλής εφαρμογή για ανταλλαγή μηνυμάτων. Η πολιτική προστασίας τους είναι διαθέσιμη μέσω της διεύθυνσης https://getsession.org/privacy-policy. Η πολιτική αρχίζει λέγοντας ότι το Session δεν γνωρίζει ποιος είναι ο χρήστης, σε ποιον μιλά ή ποιο είναι το περιεχόμενο των μηνυμάτων του και συνεχίζει λέγοντας μας ότι δεν συλλέγει ή κοινοποιεί δεδομένα του χρήστη.

Η εφαρμογή είναι σχεδιασμένη με τέτοιο τρόπο ώστε να μην αποθηκεύει δεδομένα τα οποία να οδηγήσουν σε ταυτοποίηση του χρήστη. Δεν αποθηκεύει πληροφορίες για τη συσκευή, την IP address, τον αριθμό τηλεφώνου ή την ηλεκτρονική διεύθυνση τα οποία χρησιμοποιούνται για δημιουργία λογαριασμού.

Αυτά τα λίγα περιγράφονται στην πολιτική προστασίας της εφαρμογής και αυτό φαίνεται και από το ότι δεν εντοπίστηκαν ιχνηλάτες μέσα από το περιβάλλον δοκιμών και τα επικίνδυνα δικαιώματα τα οποία ζητάει η εφαρμογή είναι τα λιγότερο δυνατά για να εξυπηρετήσουν τη διαλειτουργικότητα της. Φαίνεται πράγματι ότι συλλέγει, βάσει και της ανάλυσής μας, τα λιγότερα δεδομένα από όλες τις εφαρμογές.

6.5.8 Signal

«Το Signal είναι σχεδιασμένο να μην συλλέγει ή να αποθηκεύει προσωπικά δεδομένα». Με αυτή τη φράση αρχίζει η πολιτική ασφάλειας της εφαρμογής Signal η οποία βρίσκεται στη διεύθυνση https://signal.org/legal/#privacy-policy. Συνεχίζει λέγοντας ότι τα μηνύματα και οι κλήσεις που διεξάγονται μέσω της εφαρμογής δεν είναι προσβάσιμα από τους ίδιους ή τρίτους (third-parties) λόγω της ύπαρξης end-to-end κρυπτογραφίας, ιδιωτικότητας και ασφάλειας.

Ο χρήστης χρησιμοποιώντας την εφαρμογή παρέχει κάποια δεδομένα του. Για τη δημιουργία λογαριασμού γίνεται χρήση του αριθμού τηλεφώνου και αν θέλει ο ίδιος προσθέτει επιπλέον πληροφορίες όπως profile name ή φωτογραφία. Στη συσκευή του χρήστη αποθηκεύεται το ιστορικό μηνυμάτων του και υπάρχει η προαιρετική επιλογή μέσα από τις Επαφές του χρήστη να ανακαλύψει η εφαρμογή άλλους Signal users, εξού και το δικαίωμα Read_Contacts το οποίο εντοπίστηκε. Εάν ο χρήστης χρειαστεί να επικοινωνήσει με την εξυπηρέτηση πελατών ίσως χρειαστεί να δώσει επιπλέον πληροφορίες οι οποίες θα κρατηθούν μόνο για επικοινωνία και εξιχνίαση του περιστατικού. Τέλος, όσο αφορά τα δεδομένα του ο χρήστης μπορεί να τα ελέγξει όπως αυτός επιθυμεί μέσα από τις ρυθμίσεις της εφαρμογής.

Η εφαρμογή για να παρέχει κάποιες υπηρεσίες της χρησιμοποιεί τρίτους προμηθευτές (third-party providers) με τους οποίους ίσως μοιραστεί κάποια δεδομένα του χρήστη όπως π.χ. αριθμό τηλεφώνου για αποστολή κωδικού επιβεβαίωσης. Υπάρχουν βεβαίως ακόμη τέσσερις περιπτώσεις όπου η εφαρμογή μπορεί να κοινοποιήσει δεδομένα του χρήστη και αυτές είναι:

- Για την ικανοποίηση ισχύοντος νόμου, κανονισμού, νομικής διαδικασίας ή εκτελεστού κρατικού αιτήματος

- Για την επιβολή των ισχυόντων όρων, συμπεριλαμβανομένης της διερεύνησης πιθανών παραβιάσεων.

- Για τον εντοπισμό, την πρόληψη ή με άλλο τρόπο αντιμετώπιση απάτης, ασφάλειας ή τεχνικών ζητημάτων.

- Για την προστασία των δικαιωμάτων, της ιδιοκτησίας ή της ασφάλειας του Signal, των χρηστών ή του κοινού, όπως απαιτείται ή επιτρέπεται από τη νομοθεσία.

Κλείνοντας, φαίνεται ότι είναι μια αρκετά καλά γραμμένη πολιτική προστασίας αν και η τελευταία φορά που ανανεώθηκε ήταν το Μάιο του 2018 με την εφαρμογή του ΓΚΠΔ. Εάν και δεν εντοπίστηκαν ιχνηλάτες κατά τη μελέτη μας η εφαρμογή είναι ξεκάθαρη στο ότι χρησιμοποιεί υπηρεσίες από τρίτους για κάποιες υπηρεσίες και αυτό που κάνει δικαιολογεί τη διαλειτουργικότητα της και τα επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν να απαιτεί.

6.5.9 Skype & Teams

Οι εφαρμογές Skype και Teams ανήκουν στην εταιρεία Microsoft και για αυτό το λόγο αν και έχουν διαφορετική χρήση (συνομιλία με φίλους έναντι δουλειάς / εκπαίδευσης από το σπίτι) η πολιτική προστασίας δεδομένων τους είναι κοινή. Αυτό βέβαια αποτελεί ένα σημείο που χρήζει βελτίωσης, γιατί έτσι ένας χρήστης της μίας εκ των δύο εφαρμογών δεν μπορεί να είναι απόλυτα σίγουρος, μελετώντας την ενιαία πολιτική προστασίας δεδομένων, ποια/ποιες επεξεργασία/ες που περιγράφονται εκεί αφορούν τη συγκεκριμένη εφαρμογή. Η Microsoft λέει ότι η ιδιωτικότητα είναι σημαντική για αυτή και μέσα από την πολιτική προστασίας της παρουσιάζεται ο τρόπος επεξεργασίας και ο σκοπός των δεδομένων των οποίων συλλέγει μέσα από τις εφαρμογές και τα προϊόντα της. Εμείς θα επικεντρωθούμε στα προσωπικά δεδομένα τα οποία συλλέγει από τους χρήστες, το πως τα χρησιμοποιεί και για πιο σκοπό.

Η συλλογή δεδομένων αρχίζει από την αλληλεπίδραση του χρήστη με τις εφαρμογές και τα δεδομένα τα οποία ο ίδιος κοινοποιεί κατά τη χρήση των εφαρμογών. Μεταξύ αυτών των δεδομένων είναι τα προϊόντα της Microsoft τα οποία χρησιμοποιεί ο χρήστης, ρυθμίσεις ασφάλειας, προσωπικά δεδομένα (π.χ. όνομα, επίθετο, ηλεκτρονική διεύθυνση κ.α.). Δίνεται στο χρήστη η δυνατότητα να αρνηθεί να παρέχει τα προσωπικά του δεδομένα στην εταιρεία αλλά αυτό ίσως να μην του επιτρέψει τη χρήση προϊόντων της (εταιρείας) και τη δημιουργία λογαριασμού σε αυτά.

Τα δεδομένα τα οποία συλλέγει η Microsoft μέσα από τις εφαρμογές της χρησιμοποιούνται για να:

- Παρέχει στα προϊόντα της ενημέρωση, ασφάλεια και αντιμετώπιση προβλημάτων, καθώς και παροχή υποστήριξης. Περιλαμβάνει επίσης κοινή χρήση δεδομένων, όταν απαιτείται για την παροχή της υπηρεσίας ή την πραγματοποίηση των συναλλαγών που ζητάνε οι χρήστες.

- Βελτιώσει και να αναπτύξει τα προϊόντα της.

- Εξατομικεύσει τα προϊόντα της και να προτείνει κάτι που ίσως αρέσει στο χρήστη.

- Διαφήμιση και προώθηση προς τους χρήστες, κάτι το οποίο συμπεριλαμβάνει την αποστολή διαφημιστικών, τη στόχευση διαφημίσεων και την παρουσίασή σχετικών προσφορών.

Ο χρήστης έχει τη δυνατότητα της πρόσβασης και του ελέγχου των δεδομένων του ασκώντας τα δικαιώματα του για την προστασία δεδομένων με τη χρήση εργαλείων από την εταιρεία ή επικοινωνώντας απευθείας μαζί της. Η χρήση Cookies είναι και εδώ σημαντική μιας και αποθηκεύουν προτιμήσεις και ρυθμίσεις του χρήστη επιτρέποντας του πιο εύκολη σύνδεση στις εφαρμογές, παρέχοντας του διαφημίσεις που τον ενδιαφέρουν και ανάλυση της χρήσης του στις εφαρμογές. Επιπρόσθετα χρησιμοποιούνται και αναγνωριστικά όπως το Advertising ID, μοναδικό για κάθε χρήστη για παροχή εξατομικευμένων διαφημίσεων.

Κλείνοντας μέσα από την πολιτική προστασίας δεδομένων διαφαίνεται ότι η χρήση των ιχνηλατών που εντοπίστηκαν στις δύο εφαρμογές είναι αναγκαίες για την ανάλυση των δεδομένων τα οποία συλλέγουν οι εφαρμογές της Microsoft. Όσο αφορά στα δικαιώματα τα οποία εντοπίστηκαν και κυρίως στα επικίνδυνα δικαιώματα αυτά φαίνεται να είναι αναγκαία για τη διαλειτουργικότητα των εφαρμογών, ακόμη και η πρόσβαση σε Coarse ή Fine Location εάν χρειάζεται να μοιραστεί τη θέση του ο χρήστης. Δεν φαίνεται όμως να διαχωρίζονται οι επεξεργασίες δεδομένων ανά σκοπό και αυτό αποτελεί αρνητικό στοιχείο.

6.5.10 Telegram

Η πολιτική προστασίας του Telegram αρχίζει με τις δύο θεμελιώδεις αρχές της εφαρμογής στη συλλογή και επεξεργασίας δεδομένων, ότι δεν χρησιμοποιούνται - τα δεδομένα - για προβολή διαφημίσεων και αποθηκεύονται μόνο αυτά που χρειάζεται το Telegram για να λειτουργήσει. Μπορεί κανείς να την βρει στη διεύθυνση https://telegram.org/privacy.

Στα προσωπικά δεδομένα τα οποία χρησιμοποιεί η εφαρμογή συγκαταλέγονται τα βασικά στοιχεία λογαριασμού (αριθμός, τηλεφώνου, ηλεκτρονική διεύθυνση, profile name κα), τα μηνύματα τα οποία λόγω του ότι η εφαρμογή είναι υπηρεσία cloud αποθηκεύονται σε servers της και είναι κρυπτογραφημένα με τα κρυπτογραφικά κλειδιά αποθηκευμένα σε ξεχωριστά data centers και οι επαφές του χρήστη (Read Contacts) όπου ζητείται η συγκατάθεση του πριν το συγχρονισμό. Επιπλέον εάν ο χρήστης επιλέξει να μοιραστεί την τοποθεσία του σε μία συνομιλία, εξού και ζητούνται τα δικαιώματα για τοποθεσία, αυτή αντιμετωπίζεται ως μήνυμα και τέλος χρησιμοποιούνται Cookies (στο Web) για να λειτουργήσει και να παρέχει τις υπηρεσίες του το Telegram.

Τα δεδομένα αυτά είναι αποθηκευμένα σε data centers τα οποία ανήκουν στο Telegram και χρησιμοποιείται κρυπτογραφία end-to-end. Η επεξεργασία η οποία τυγχάνουν είναι για να μπορέσει η εφαρμογή να παρέχει τις cloud υπηρεσίες της (π.χ. μηνύματα, πολυμέσα και αρχεία) και λειτουργικότητα μεταξύ συσκευών (cross-device functionality), να υπάρχει ασφάλεια κατά τη χρήση της εφαρμογής μειώνοντας το spam και την κατάχρηση, να παρέχει προηγμένες δυνατότητες και τέλος να μην προβάλει διαφημίσεις με βάση τα δεδομένα του χρήστη. Ο χρήστης έχει το κάθε δικαίωμα να διαγράψει αυτά τα δεδομένα ή να δει πως αυτά επεξεργάζονται από την εφαρμογή.

Συνοψίζοντας, κρίνουμε ότι η πολιτική προστασίας της εφαρμογής είναι αρκετά απλή και εύκολα κατανοητή παρουσιάζοντας τις αναγκαίες πληροφορίες για την ενημέρωση του χρήστη. Δεν γίνεται κάπου αναφορά για τη χρήση ιχνηλατών ενώ εντοπίστηκε ένας (Google Firebase Analytics) κατά τη μελέτη μας – γεγονός που εγείρει ερωτηματικά. Σχετικά με τα επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν και λαμβάνοντας υπόψη ότι είναι εφαρμογή ανταλλαγής μηνυμάτων με δυνατότητα φωνητικών κλήσεων και βιντεοκλήσεων κρίνονται αναγκαία για τη λειτουργικότητα της.

6.5.11 Viber

Η μακροσκελής πολιτική προστασίας δεδομένων της εφαρμογής είναι διαθέσιμη στο κοινό μέσω της διεύθυνσης https://www.viber.com/en/terms/viber-privacy-policy/. Οι ενότητες της περιγράφουν αρκετά πράγματα αλλά εμείς θα επικεντρωθούμε στα δεδομένα τα οποία συλλέγει η εφαρμογή, τη χρήση τους και εάν γίνεται κοινοποίηση τους σε τρίτους.

Αρχίζοντας τα δεδομένα τα οποία συλλέγει η εφαρμογή απαιτούνται υποχρεωτικά για τις υπηρεσίες της ενώ υπάρχουν και κάποια τα οποία δεν συλλέγονται εάν δεν γίνει χρήση συγκεκριμένων υπηρεσιών ή χαρακτηριστικών. Τα δεδομένα τα οποία συλλέγονται είναι χωρισμένα σε κατηγορίες και αυτές είναι οι εξής:

- Δεδομένα τα οποία παρέχονται ή συλλέγονται μέσω εγγραφής στην εφαρμογή ή κατά τη συμμετοχή σε δραστηριότητες της. Αυτά είναι αναγνωριστικά όπως αριθμός κινητού, όνομα, ηλεκτρονική διεύθυνση κ.α., φωτογραφία προφίλ (εάν υπάρχει), ενδιαφέροντα και επαφές από το κινητό εάν δοθεί η συγκατάθεση (read contacts).

- Δεδομένα τοποθεσίας από IP address ή μέσω συντεταγμένων GPS όπου χρειάζεται η συγκατάθεση του χρήστη.

- Δεδομένα πληρωμών / αγορών εάν προχωρήσει ο χρήστης σε αγορά συνδρομής ή άλλων υπηρεσιών.

- Δεδομένα τα οποία συλλέγονται αυτόματα με τη χρήση cookies ή άλλων τεχνολογιών. Σε αυτά τα δεδομένα έχουμε αναγνωριστικά συσκευής, χρήση της εφαρμογής (activity data), πιθανόν προβλήματα (αποθηκευμένα σε log files) και άλλες πληροφορίες της συσκευής όπως το λειτουργικό σύστημα.

- Δεδομένα από άλλες πηγές όπως μέσα κοινωνικής δικτύωσης (εάν γίνει σύνδεση με αυτά), όνομα χρήστη από επαφές άλλων χρηστών (εάν είναι συγχρονισμένες), συμπεράσματα από ενδιαφέροντα, φωτογραφία προφίλ ή αλληλεπίδραση με διαφημίσεις.

- Δεδομένα από τη συμμετοχή του χρήστη σε δραστηριότητες της εφαρμογής.

- Δεδομένα από την επικοινωνία με την εφαρμογή για σκοπούς εξυπηρέτησης πελατών ή κάποιο άλλο λόγο.

- Δεδομένα από μη χρήστες της εφαρμογής όπως τηλέφωνο και όνομα τα οποία εντοπίστηκαν με το συγχρονισμό των επαφών χρήστη της εφαρμογής και χρησιμοποιούνται για να φαίνεται ποιοι από τις επαφές του είναι και ποιοι δεν είναι χρήστες της εφαρμογής.

- Δεδομένα για εταιρικούς σκοπούς (π.χ. συνεργασία)

Τα συλλεχθέντα δεδομένα χρησιμοποιούνται έχοντας απώτερο σκοπό την καλύτερη εμπειρία του χρήστη μέσω των υπηρεσιών της εφαρμογής. Αρχικά η χρήση τους γίνεται για αυθεντικοποίηση και επαλήθευση του λογαριασμού του χρήστη δίνοντας του έτσι τη δυνατότητα ελέγχου των ρυθμίσεων και πρόσβαση σε επιπλέον υπηρεσίες της εφαρμογής. Μετέπειτα, μέσα από δεδομένα όπως η τοποθεσία παρουσιάζονται στο χρήστη διαφημίσεις βάσει τοποθεσίας, ενώ μέσα από την ηλεκτρονική διεύθυνση και τα συμπεράσματα για την ηλικία ή το φύλο του χρήστη παρουσιάζονται διαφημίσεις για προϊόντα που ίσως να τον ενδιαφέρουν. Επιπλέον, τα δεδομένα χρησιμοποιούνται για σκοπούς ασφάλειας της εφαρμογής και πρόληψη οποιασδήποτε απάτης. Μέσα από το περιβάλλον δοκιμών και πιο συγκεκριμένα μέσω του εικονικού περιβάλλοντος PI εντοπίστηκαν οι πιο πάνω σκοποί και διαφαίνεται ότι η εφαρμογή τους αναφέρει στην πολιτική προστασίας της διαχωρίζοντας το σκοπό της κάθε επεξεργασίας.

Η κοινοποίηση των δεδομένων μπορεί να γίνει μεταξύ εφαρμογών της θυγατρικής εταιρείας (Rakuten), σε παρόχους υπηρεσιών στην εφαρμογή, σε τρίτους οι οποίοι παρέχουν υπηρεσίες μέσω του Viber, σε διαφημιστικούς συνεργάτες και τέλος για νομικούς λόγους και επιβολής του νόμου. Δεν αναγράφεται στην πολιτική εάν για την κοινοποίηση χρειάζεται η συγκατάθεση του χρήστη παρά μόνο το ότι ο χρήστης δίνει συγκατάθεση για τη συλλογή δεδομένων του.

Κλείνοντας, η πολιτική προστασίας δεδομένων της εφαρμογής Viber φαίνεται να περιγράφει ξεκάθαρα τα όσα εντοπίστηκαν κατά τη διεξαγωγή της μελέτης μας. Η θυγατρική της εταιρεία ανανεώνει την πολιτική κάθε χρόνο όπως αναγράφεται στην αρχή της έτσι ώστε να συμβαδίζει με πιθανόν νέους κανονισμούς και τη συνεχής εξέλιξη της τεχνολογίας.

6.5.12 Webex Meet

Η εφαρμογή Webex Meet δεν έχει δική της πολιτική προστασίας δεδομένων αλλά αυτή της Cisco και μπορεί να τη βρει κανείς στη διεύθυνση https://www.cisco.com/c/en/us/about/legal/privacy.html. Η εταιρεία δεν περιγράφει κάπου τα δεδομένα τα οποία συλλέγει παρά μόνο το σκοπό για τον οποίο γίνεται η συλλογή και ποιες επιλογές δίνονται στο χρήστη για τη διαχείριση των δεδομένων του – αυτό εγείρει σαφώς ερωτηματικά.

Τα προσωπικά δεδομένα συλλέγονται για πολλούς λόγους από τα προϊόντα της Cisco όπως η εξατομίκευση της εμπειρίας, η διαχείριση θέσεων εργασίας κ.α. Ο χρήστης ενημερώνεται για το λόγο που συλλέγονται προσωπικά δεδομένα του κατά τη διάρκεια της συλλογής και τα δεδομένα αυτά κρατούνται μέχρι να εξυπηρετήσουν το σκοπό της συλλογής τους. Η εταιρεία επίσης μπορεί να συνδυάσει δεδομένα ενός χρήστη από άλλες πηγές για να την βοηθήσουν να βελτιωθεί και να προσαρμοστεί καλύτερα κατά τις αλληλεπιδράσεις της με το χρήστη. Η χρήση προϊόντων της Cisco συνεπάγεται και αποδοχή των cookies τα οποία χρησιμοποιούνται για συλλογή πληροφοριών για τη χρήση των προϊόντων.

Τα προσωπικά δεδομένα χρησιμοποιούνται μόνο για το λόγο τον οποίο έγινε η συλλογή τους και δεν θα χρησιμοποιηθούν για διαφορετικό σκοπό χωρίς τη συγκατάθεση του χρήστη ή αν δεν υπάρχει νομική απαίτηση. Ο χρήστης ερωτάται για τη συγκατάθεση του εάν θα κοινοποιηθούν προσωπικά του δεδομένα σε τρίτους για λόγους άλλους από αυτούς τους οποίους είχε ήδη συμφωνήσει. Τέλος ο χρήστης μπορεί να τροποποιήσει τα προσωπικά του δεδομένα και τον τρόπο επικοινωνίας που προτιμάει μέσω των ρυθμίσεων της εφαρμογής.

Ολοκληρώνοντας, το Webex Meet κρίνουμε ότι χρειάζεται τη δική του ξεχωριστή πολιτική προστασίας χώρια από αυτή της Cisco. Αυτό, λόγω του ότι είναι ένα διαφορετικό προϊόν από μία μεγάλη εταιρεία και η χρήση του είναι αρκετά μεγάλη τόσο στον εργασιακό χώρο όσο και στην εκπαίδευση. Θα πρέπει επίσης η πολιτική να παρέχει αναλυτική πληροφόρηση και για το είδος των προσωπικών δεδομένων τα οποία υφίστανται επεξεργασία για τον κάθε σκοπό. Περαιτέρω, η ύπαρξη ιχνηλατών σε κάποια προϊόντα καλό θα ήταν να αναφέρεται στην πολιτική προστασίας από την εταιρεία για να είναι και εις γνώση των χρηστών πριν χρησιμοποιήσουν ένα προϊόν – εφαρμογή.

6.5.13 WeChat

Το WeChat διαθέτει δύο πολιτικές απορρήτου μία για χρήστες WeChat οι οποίοι είναι όσοι έχουν αριθμό με διεθνή τηλεφωνικό κωδικό διάφορο του κινέζικου +86, και μία για τους Weixin χρήστες οι οποίοι είναι όσοι έχουν αριθμό με τηλεφωνικό κωδικό +86 ή έχουν συμβόλαιο με την εταιρεία Tencent. Στην παρούσα διατριβή θα ασχοληθούμε με την πρώτη πολιτική απορρήτου μιας και χρησιμοποιήσαμε διεθνή αριθμό για τη δημιουργία λογαριασμού. Η πολιτική είναι διαθέσιμη στη διεύθυνση https://www.wechat.com/mobile/htdocs/en/privacy_policy.html#pp_how.

Ο χρήστης με τη δημιουργία λογαριασμού πρέπει να δώσει τον αριθμό τηλεφώνου του και ένα ψευδώνυμο (alias) και εάν θέλει προσθέτει επιπλέον πληροφορίες, δεδομένα τα οποία συλλέγονται από την εφαρμογή. Συλλογή δεδομένων έχουμε και για πληροφορίες ασφάλειας του λογαριασμού όπως κωδικός, άτομα επικοινωνίας σε έκτακτη ανάγκη, ηλεκτρονική διεύθυνση κα. Τα δεδομένα από τα μηνύματα τα οποία αποστέλλονται περνάνε από τους servers της εφαρμογής κατά την αποστολή τους και φυλάγονται εκεί μέχρι να φθάσουν στον παραλήπτη και να παραμείνουν στη συσκευή τόσο του ίδιου όσο και του αποστολέα. Εάν ο χρήστης δώσει τη συγκατάθεση του η εφαρμογή αποκτά πρόσβαση στις επαφές (Read Contacts) της συσκευής του και αυτές συγχρονίζονται με το WeChat. Για να μπορέσει το WeChat να παρέχει υπηρεσίες βασισμένες στην τοποθεσία του χρήστη αυτός χρειάζεται να δώσει τα δεδομένα τοποθεσίας του. Τα δεδομένα αυτά ορίζονται ως δεδομένα τα οποία συμπληρώνονται με τη χρήση συντεταγμένων GPS, του Wi-Fi, της IP address ή ακόμη και της τοποθεσίας μέσω των δημοσιεύσεων του χρήστη (location geo-tag). Τέλος, η εφαρμογή συλλέγει και log data αυτόματα τα οποία ορίζει χωρίζοντας τα σε τέσσερις κατηγορίες. Η πρώτη κατηγορία αφορά χαρακτηριστικά συσκευής, η δεύτερη πληροφορίες για το τι βλέπει ο χρήστης στην εφαρμογή, η τρίτη γενικές πληροφορίες για τις επικοινωνίες του χρήστη στην εφαρμογή και η τέταρτη μεταδεδομένα (metadata) τα οποία εξάγονται από φωτογραφίες ή βίντεο του χρήστη.

Ο τρόπος και ο σκοπός της επεξεργασίας δεδομένων περιγράφεται σε έναν αναλυτικό πίνακα με ποιο κύριο σκοπό την παροχή υπηρεσιών της εφαρμογής στο χρήστη κάτω από το νομικό πλαίσιο και τη σύμβαση χρήστη – εφαρμογής. Η εφαρμογή αν και έχει έδρα την Κίνα έχει και κέντρα επεξεργασίας δεδομένων και στην ΕΕ (Ολλανδία) τα οποία επεξεργάζονται τα δεδομένα με βάση τον ΓΚΠΔ.

Τελειώνοντας, η πολιτική προστασίας της εφαρμογής φαίνεται να περιέχει όλα τα στοιχεία που απαιτούνται από τη σχετική νομοθεσία στην ΕΕ. Οι ιχνηλάτες οι οποίοι εντοπίστηκαν θεωρούνται αναγκαίοι μιας και επιτρέπεται η δημιουργία λογαριασμού με την εφαρμογή Facebook, συλλέγονται δεδομένα για ανάλυση (Google Firebase Analytics) και καταγράφεται η τοποθεσία του χρήστη (WeChat Location) όπως αναφέρεται στην πολιτική προστασίας δεδομένων.

6.5.14 WhatsApp

«Εάν ο χρήστης επιθυμεί να χρησιμοποιήσει προαιρετικά χαρακτηριστικά της εφαρμογής τότε η εφαρμογή θα πρέπει να συλλέξει περισσότερα δεδομένα για να μπορέσει να του τα παρέχει». Με αυτόν τον τρόπο αρχίζει η πολιτική προστασίας δεδομένων του WhatsApp αναφερόμενη στη

συλλογή δεδομένων του χρήστη και βρίσκεται στη διεύθυνση https://www.whatsapp.com/legal/privacy-policy-eea.

Η εφαρμογή συλλέγει δεδομένα τα οποία δίνει ο χρήστης αρχίζοντας με τα στοιχεία λογαριασμού (αριθμός τηλεφώνου, όνομα προφίλ) τα οποία είναι υποχρεωτικά αλλιώς δεν μπορεί να δημιουργήσει λογαριασμό. Συλλέγεται επίσης το περιεχόμενο το οποίο αποστέλλει ο χρήστης όπως μηνύματα, ψηφιακό περιεχόμενο και κλήσεις. Πιο συγκεκριμένα, υπάρχει η κρυπτογραφία end-to-end και κατά την αποστολή μηνυμάτων αυτά αποθηκεύονται προσωρινά με κρυπτογράφηση σε servers της εταιρείας μέχρι να παραδοθούν (delivered) και να διαγραφούν άμεσα. Εάν δεν παραδοθεί παραμένει στους servers κρυπτογραφημένο για τριάντα ημέρες και έπειτα διαγράφεται. Επιπλέον, ο χρήστης μπορεί να κοινοποιήσει την κατάσταση του στην εφαρμογή (Status) αλλά και την ακριβής διεύθυνση του αποδεχόμενος το αντίστοιχο δικαίωμα. Όπως και στις περισσότερες εφαρμογές επικοινωνίας ο χρήστης μπορεί να συγχρονίσει τις επαφές του με την εφαρμογή εάν το επιθυμεί και να δημιουργήσει δικές του ομαδικές συνομιλίες πληροφορίες τις οποίες συλλέγει η εφαρμογή. Τέλος, η εφαρμογή συλλέγει δεδομένα κατά την επικοινωνία με την τεχνική υποστήριξη αλλά και για την πρόσβαση στην εφαρμογή όταν για παράδειγμα χρειάζεται να σταλεί SMS για επιβεβαίωση του αριθμού του χρήστη.

Συλλογή δεδομένων γίνεται και αυτόματα από την εφαρμογή με δεδομένα όπως τη χρήση της εφαρμογής, logs και πιθανά προβλήματα στην εφαρμογή, τον τρόπο σύνδεσης της συσκευής και άλλα γενικά δεδομένα συσκευής (μοντέλο, λειτουργικό σύστημα, ISP κα). Εκτός αυτών, εάν ο χρήστης δεν αποδεχτεί το δικαίωμα πρόσβασης στην εφαρμογή μπορεί να υπολογιστεί η πιθανή του τοποθεσία μέσω της IP address και του ταχυδρομικού κώδικα του. Επιπρόσθετα η εφαρμογή χρησιμοποιεί Cookies για συλλογή πληροφοριών για να λειτουργήσει και να προσφέρει τις διαδικτυακές της υπηρεσίες. Οι επιλογές και οι ρυθμίσεις του χρήστη στην εφαρμογή συλλέγονται με τη δυνατότητα να αλλάξει ρυθμίσεις ιδιωτικότητας μέσω της εφαρμογής.

Οι λόγοι και ο τρόπος επεξεργασίας των εφαρμογών είναι οι εκτενέστεροι από τις πολιτικές προστασίας των εφαρμογών που μελετήθηκαν στην παρούσα διατριβή και με λίγα λόγια αυτή η επεξεργασία γίνεται για την εκπλήρωση των όρων χρήσης της εφαρμογής, την εκτέλεση της σύμβασης χρήστη – εφαρμογής και για νομικούς σκοπούς. Η επεξεργασία γίνεται με τη συγκατάθεση του χρήστη και έχει όλα τα νόμιμα δικαιώματα να επέμβει σε αυτήν.

Εν κατακλείδι, η πολιτική προστασίας δεδομένωντου WhatsApp είναι η μεγαλύτερη και πιο λεπτομερής από όλες όσες μελετήθηκαν και φαίνεται να έχει όλα τα στοιχεία που απαιτούνται

από τη σχετική νομοθεσία. Μέσα από αυτήν αναλύεται ενδελεχώς η συλλογή και επεξεργασία προσωπικών δεδομένων και διαφαίνεται ο λόγος που απαιτούνται τα επικίνδυνα δικαιώματα τα οποία εντοπίσαμε κατά την μελέτη μας.

6.5.15 Wire

Η πολιτική προστασίας δεδομένων της εφαρμογής Wire βρίσκεται στη διεύθυνση https://wire.com/en/legal/. Ο χρήστης δίνει κάποια δεδομένα του στην εφαρμογή κατά τη δημιουργία λογαριασμού όπως το όνομα, ο αριθμός τηλεφώνου και η ηλεκτρονική διεύθυνση του. Αυτά χρησιμοποιούνται για να μπορεί η εφαρμογή να προσφέρει τις υπηρεσίες της και να παρουσιάζει το προφίλ του χρήστη σε άλλους χρήστες. Τα δεδομένα αυτά αποθηκεύονται μόνο κατά τη διάρκεια χρήσης του λογαριασμού και διαγράφονται αμέσως με τη διαγραφή του.

Εάν ο χρήστης αποστείλει αίτημα για επικοινωνία με την εξυπηρέτηση πελατών και συμπεριλάβει σε αυτό δεδομένα του αυτά συλλέγονται και επεξεργάζονται μόνο για σκοπούς απάντησης στο αίτημα. Επιπλέον, η εφαρμογή αποθηκεύει τεχνικά δεδομένα της συσκευής με τη συγκατάθεση του χρήστη για να είναι σε θέση να μεταφέρει δεδομένα μεταξύ συσκευών και αν ο χρήστης επιθυμεί μπορεί να δώσει και πρόσβαση στις επαφές του για να επικοινωνεί με τους φίλους του μέσω της εφαρμογής. Για τη δημιουργία ανώνυμων στατιστικών στοιχείων και crash logs της εφαρμογής εάν δώσει τη συγκατάθεση του ο χρήστης συλλέγονται επιπλέον δεδομένα. Η πολιτική προστασίας της εφαρμογής αναφέρεται και σε τρίτους παρόχους (third-party providers) οι οποίοι της παρέχουν υπηρεσίες για να μπορεί με αυτή με τη σειρά της να παρέχει υπηρεσίες.

Τελειώνοντας, η πολιτική προστασίας δεδομένων της εφαρμογής Wire φαίνεται να έχει όλα τα στοιχεία που απαιτούνται από τη σχετική νομοθεσία και σε κάθε της σημείο αναφέρεται σε άρθρο του ΓΚΠΔ. Θετικό στοιχείο αποτελεί το ότι εξηγείται η απαίτηση κάποιων δικαιωμάτων και γίνεται αναφορά στους τρίτους παρόχους οι οποίοι προσφέρουν τις υπηρεσίες τους στην εφαρμογή.

6.5.16 Zalo

Η εφαρμογή Zalo έχει τη μικρότερη πολιτική προστασίας δεδομένων από όλες τις εφαρμογές οι οποίες μελετήθηκαν και είναι διαθέσιμη στη διεύθυνση https://zalo.me/zalo/policy/. Αποτελείται από τρεις ενότητες με την πρώτη να αναφέρεται στα δεδομένα τα οποία συλλέγει η εφαρμογή, τη

δεύτερη στο πως χρησιμοποιούνται αυτά τα δεδομένα και την τρίτη στο πως κοινοποιούνται αυτά τα δεδομένα.

Τα δεδομένα τα οποία συλλέγει η εφαρμογή χωρίζονται σε τέσσερις τύπους. Ο πρώτος αφορά τα προσωπικά δεδομένα όπως το όνομα, ο αριθμός τηλεφώνου, η ημερομηνία γέννησης τα οποία απαιτούνται για τη δημιουργία λογαριασμού. Ο δεύτερος τύπος αφορά δεδομένα συσκευής όπως το μοντέλο και η έκδοση της εφαρμογής για να παρέχει (η εφαρμογή) καλύτερη υποστήριξη. Ο τρίτος τύπος αφορά την τοποθεσία (Access Coarse / Fine Location) του χρήστη η οποία αποθηκεύεται σε server της εφαρμογής για να βοηθήσει το χρήστη στην εύκολη κοινοποίηση της τοποθεσίας του και να του παρέχεται καλύτερη εμπειρία. Τέλος, ο τέταρτος τύπος είναι τα δεδομένα επικοινωνίας του χρήστη όπως οι επαφές (read contacts) του για να είναι ευκολότερο να βρει και να συνομιλήσει με φίλους του μέσω της εφαρμογής.

Τα συλλεχθέντα δεδομένα χρησιμοποιούνται έτσι ώστε να παρέχονται και να υποστηρίζονται οι υπηρεσίες της εφαρμογής και πιο συγκεκριμένα με αυτά:

- Αναπτύσσονται, λειτουργούν, βελτιώνονται, παραδίδονται, συντηρούνται και προστατεύονται τα προϊόντα και υπηρεσίες του Zalo.

- Γίνεται επικοινωνία με το χρήστη για τις υπηρεσίες της εφαρμογής και όταν χρειαστεί βοήθεια από την υποστήριξη πελατών.

- Ενισχύεται η ασφάλεια των προϊόντων και υπηρεσιών της εφαρμογής

- Πιστοποιείται η ταυτότητα του χρήστη και αποτρέπεται οποιαδήποτε απάτη ή άλλη μη εξουσιοδοτημένη παράνομη δραστηριότητα

- Επιβάλλονται οι Όροι Παροχής Υπηρεσιών της εφαρμογής και άλλες πολιτικές χρήσης.

Όσο αφορά την ασφάλεια των δεδομένων αναφέρεται ότι μεταφέρονται με ασφαλή τρόπο μέσω του πρωτοκόλλου https και δεν κοινοποιούνται σε τρίτους (third-parties). Καταλήγοντας, η πολιτική προστασίας δεδομένων είναι ξεκάθαρη με τη συλλογή και επεξεργασία δεδομένων αλλά δεν μας αφήνει ικανοποιημένους η παρουσία μεγάλου αριθμού ιχνηλατών (επτά) οι οποίοι εντοπίστηκαν κατά τη μελέτη μας και δεν αναφέρεται κάπου στο κείμενο η ύπαρξη τους. Τα

επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν δικαιολογούνται ως ένα βαθμό μιας και απαιτούνται για τις λειτουργίες τις οποίες προσφέρει η εφαρμογή.

6.5.17 Zoom

Η εφαρμογή μέσα από την πολιτική προστασίας της περιγράφει τα προσωπικά δεδομένα τα οποία συλλέγει και τον τρόπο τον οποίο τα επεξεργάζεται. Η πολιτική βρίσκεται στη διεύθυνση https://explore.zoom.us/en/privacy/.

Η εφαρμογή συλλέγει αρκετά προσωπικά δεδομένα του χρήστη χωρισμένα σε κατηγορίες. Οι κατηγορίες αυτές είναι οι εξής:

- Δεδομένα λογαριασμού (δεδομένα επικοινωνίας, account ID κα)
- Δεδομένα προφίλ και συμμετεχόντων σε διαδικτυακές συναντήσεις (meetings)
- Δεδομένα επαφών ή ημερολογίου τα οποία συγχρονίζει ο χρήστης με την εφαρμογή
- Δεδομένα ρυθμίσεων και προτιμήσεων στην εφαρμογή
- Δεδομένα εγγραφής για συμμετοχή σε διαδικτυακή συνάντηση στην εφαρμογή
- Δεδομένα συσκευής (λειτουργικό σύστημα, μικρόφωνο, ακουστικά, IP address κα.)
- Περιεχόμενο το οποίο κοινοποιείται κατά τη διεξαγωγή διαδικτυακής συνάντησης, ανταλλαγής μηνυμάτων ή διαδικτυακού σεμιναρίου.
- Δεδομένα χρήσης προϊόντων και σελίδας της εταιρείας Zoom
- Δεδομένα επικοινωνίας μέσω της εφαρμογής Zoom
- Δεδομένα από συνεργάτες ή third-party companies

Τα πιο πάνω συλλεχθέντα δεδομένα η εταιρεία (Zoom) τα χρησιμοποιεί για πολλούς σκοπούς χωρίς να είναι σαφές για κάθε σκοπό τι επεξεργασία γίνεται . Αρχικά για να προσφέρει τα προϊόντα και υπηρεσίες της στους χρήστες με τον καλύτερο δυνατό τρόπο και να είναι σε θέση να

επικοινωνήσει μαζί τους. Κατά δεύτερον, χρησιμοποιούνται για έρευνα και ανάπτυξη των προϊόντων της εταιρείας αλλά και για να έχει τη δυνατότητα η ίδια να προσφέρει marketing, προσφορές και διαφημίσεις από τρίτους στους χρήστες με βάση τη χρήση των προϊόντων της Zoom. Τέλος η επεξεργασία των δεδομένων γίνεται για νομικούς σκοπούς και για τον έλεγχο ταυτότητας χρηστών, την ασφαλής χρήση της εφαρμογής χωρίς οποιοδήποτε κίνδυνο ασφάλειας. Με τη χρήση της εφαρμογής δεδομένα του χρήστη μπορούν να τα δουν άλλα άτομα, οργανισμοί και τρίτοι εκτός της εφαρμογής. Αυτό γιατί ο χρήστης μπορεί να λάβει μέρος σε διάφορα σεμινάρια τα οποία διοργανώνει ένας οργανισμός ή μια εταιρεία και εκεί να εμφανίζεται το όνομα του ή η φωτογραφία προφίλ του.

Η εταιρεία Zoom κοινοποιεί τα προσωπικά δεδομένα κάτω από κάποιες προϋποθέσεις. Αρχικά, εάν αυτό απαιτείται από το νόμο ή αν η εταιρεία προχωρήσει σε πώληση τότε τα δεδομένα ίσως χρησιμοποιηθούν κατά τις διαπραγματεύσεις. Επιπρόσθετα, στα δεδομένα μπορούν να αποκτήσουν πρόσβαση μεταπωλητές ή προμηθευτές της εταιρείας οι οποίοι τις προσφέρουν υπηρεσίες ή προϊόντα αναγκαία για τη λειτουργία του Zoom. Τέλος τα δεδομένα μπορεί να παρουσιαστούν σε εταιρικούς συνεργάτες της εταιρείας ή να δοθούν σε προμηθευτές οι οποίοι προσφέρουν ανάλυση δεδομένων για σκοπούς marketing και διαφημίσεων και μόνο όπου απαιτείται από τον νόμο ζητείτε πρώτα η συγκατάθεση του χρήστη.

Καταλήγοντας, διαφαίνεται μέσα από την πολιτική προστασίας δεδομένων του Zoom ότι πολλά προσωπικά δεδομένα επεξεργάζονται για διαφημιστικούς σκοπούς και αυτό είναι αρνητικό. Επιπλέον, αν και η πολιτική είναι ξεκάθαρη με το ποια δεδομένα συλλέγονται είναι μεγάλος ο αριθμός τους και είναι στην ευχέρεια του ατόμου εάν επιθυμεί να χρησιμοποιήσει την εφαρμογή. Τα επικίνδυνα δικαιώματα τα οποία εντοπίστηκαν κρίνονται απαραίτητα για τη διαλειτουργικότητα της εφαρμογής.

Κεφάλαιο 7
Επίλογος

Κατά τη διάρκεια της πανδημίας COVID-19 η μόνη εναλλακτική λύση για προσωπικές και επαγγελματικές συναντήσεις ήταν οι εφαρμογές συνομιλιών/τηλεδιασκέψεων βλέποντας τη ζήτηση τους να αυξάνεται σημαντικά. Εφαρμογές όπως το Microsoft Teams και το Zoom αν και είχαν εμφανιστεί χρόνια πριν την πανδημία βγήκαν από την αφάνεια και απέκτησαν σημαντικό ρόλο. Για να είναι σε θέση να υποστηρίξουν τη λειτουργικότητα τους οι εφαρμογές απαιτούν από τους χρήστες να αποδεχτούν κάποια δικαιώματα, γνωστά και ως επικίνδυνα δικαιώματα, τα οποία με την αποδοχή αποκτούν πρόσβαση σε προσωπικά δεδομένα ή άλλες ευαίσθητες περιοχές. Τα δικαιώματα τα οποία απαιτεί κάθε εφαρμογή, η χρήση ιχνηλατών (trackers), η χρήση υπηρεσιών από τρίτους για διεξαγωγή συγκεκριμένων υπηρεσιών, ο τρόπος και ο σκοπός συλλογής δεδομένων περιγράφονται στις πολιτικές προστασίας (privacy policy) των εφαρμογών. Διαφαίνεται όμως, ότι το μεγαλύτερο ποσοστό των χρηστών δεν διαβάζουν τις πολιτικές αυτές και προχωράνε σε εγκατάσταση μίας εφαρμογής είτε αυτή είναι συνομιλιών ή κάποιο παιχνίδι μη γνωρίζοντας την κατάληξη ή την ασφάλεια των δεδομένων τα οποία θα παρέχουν. Περαιτέρω, οι πολιτικές προστασίας ενδέχεται να περιέχουν ασάφειες ή και να είναι ελλιπείς.

Η χρήση των εφαρμογών συνομιλιών/τηλεδιασκέψεων παρά τις χαλαρώσεις σχετικά με την πανδημία COVID-19 παραμένει υψηλή και σε συνδυασμό με την άγνοια των χρηστών για τα προσωπικά δεδομένα τους κρίθηκε αναγκαία η εκπόνηση της παρούσας μεταπτυχιακής διατριβής.

Μέσα από την ερευνητική και πρακτική μελέτη δεκαοχτώ εφαρμογών συνομιλιών/τηλεδιασκέψεων και τη σύγκριση των αποτελεσμάτων μας με την πολιτική προστασίας τους δεν διαφάνηκε κάποια διαρροή προσωπικών δεδομένων σε τρίτους η οποία να είναι αδιαφανής προς το χρήστη και όλες οι εφαρμογές παρείχαν μία αρκετά καλή και ευανάγνωστη πολιτική εύκολα προσβάσιμη στο χρήστη. Όμως, μέσα από την μελέτη και των πολιτικών προστασίας των εφαρμογών εντοπίστηκαν περιπτώσεις εφαρμογών οι οποίες αποστέλλουν δεδομένα σε διαφημιστές χωρίς να ζητείται η συγκατάθεση του χρήστη και περιπτώσεις όπου δεν είναι ξεκάθαρο τι επεξεργασία γίνεται ακριβώς για κάθε σκοπό επεξεργασίας. Στον πιο κάτω πίνακα συνοψίζονται τα αποτελέσματα της μελέτης των πολιτικών προστασίας των εφαρμογών συνομιλιών/τηλεπικοινωνιών που μελετήθηκαν.

Εφαρμογή	Σχόλιο για την πολιτική προστασίας
Discord	Δεν εντοπίστηκε ευπαθές σημείο
Element	Δεν εντοπίστηκε ευπαθές σημείο
KakaoTalk	Όχι σαφής ενημέρωση
Line	Δεν εντοπίστηκε ευπαθές σημείο
Messenger	Όχι σαφής ενημέρωση
Phoenix	Όχι σαφής ενημέρωση
Session	Δεν εντοπίστηκε ευπαθές σημείο
Signal	Δεν εντοπίστηκε ευπαθές σημείο

Skype	Όχι σαφής ενημέρωση
Teams	Όχι σαφής ενημέρωση
Telegram	Δεν εντοπίστηκε ευπαθές σημείο
Viber	Όχι σαφής ενημέρωση
Webex Meet	Όχι σαφής ενημέρωση
WeChat	Δεν εντοπίστηκε ευπαθές σημείο
WhatsApp	Δεν εντοπίστηκε ευπαθές σημείο
Wire	Δεν εντοπίστηκε ευπαθές σημείο
Zalo	Όχι σαφής ενημέρωση
Zoom	Όχι σαφής ενημέρωση

Πίνακας 7.1: Σχόλιο για την πολιτική προστασίας των εφαρμογών οι οποίες μελετήθηκαν

Βεβαίως δεν μπορεί να αποκλειστεί το ενδεχόμενο διαρροής δεδομένων σε τρίτους χωρίς να είναι εις γνώση του χρήστη και αυτό γιατί υπήρξαν κάποιοι περιορισμοί στην έρευνα μας. Κανένα από τα εργαλεία τα οποία χρησιμοποιήσαμε δεν μας παρείχε 100% αποκωδικοποίηση (decoding) των εφαρμογών και για αυτό το έγινε χρήση συνδυασμού εργαλείων με τα αποτελέσματα να είναι σαφώς καλύτερα και πιο ξεκάθαρα. Η αδυναμία πρόσβασης στο αρχείο AndroidManifest.xml για να διαφανεί εάν οι εφαρμογές χρησιμοποιούν το επιπλέον χαρακτηριστικό ασφάλειας Network security configuration αποτελεί τον δεύτερο περιορισμό στην έρευνα μας.

Παρά τους περιορισμούς τα αποτελέσματα της διατριβής έχουν εξαιρετικό ενδιαφέρον όχι μόνο για την ερευνητική κοινότητα αλλά και για όλο τον κόσμο μιας και έγινε μελέτη και σύγκριση μεταξύ δεκαοχτώ από τις πιο δημοφιλείς εφαρμογές συνομιλιών/τηλεπικοινωνιών σε ότι αφορά τη διαρροή προσωπικών δεδομένων.

7.1 Μελλοντική έρευνα

Η παρούσα μεταπτυχιακή διατριβή εξέτασε τις εφαρμογές σε συσκευή με λειτουργικό σύστημα Android 7 έκδοση η οποία κυκλοφόρησε πριν την εφαρμογή του ΓΚΠΔ και δεν υποστηρίζεται πλέον από την Google. Καλό θα ήταν για εμπλουτισμό της διατριβής οι εφαρμογές να εξεταστούν και σε συσκευή με νεότερη έκδοση του Android και μέσα από τη σύγκριση των δύο να διαφανεί κατά πόσο παίζει ρόλο στην προστασία προσωπικών δεδομένων και η έκδοση του λειτουργικού συστήματος Android.

Οι εκδόσεις των εφαρμογών συνεχώς αναβαθμίζονται προσφέροντας καινούργια χαρακτηριστικά και υπηρεσίες στους χρήστες χωρίς όμως να το προσθέσουν στην πολιτική προστασίας τους για πιθανή συλλογή δεδομένων. Οι πολιτικές προστασίας πρέπει ανά τακτά χρονικά διαστήματα να αναθεωρούνται έτσι ώστε να προσθέτονται τα πιθανόν νέα χαρακτηριστικά των εφαρμογών τους και να ανταποκρίνονται περισσότερο στην εκάστοτε νομοθεσία. Οι δύο αυτοί λόγοι μας οδηγούν στην ανάγκη για διεξαγωγή της μελέτης ξανά μετά από ένα εύλογο χρονικό διάστημα. Μέσα από τη νέα μελέτη θα διαφανεί εάν υπάρχει διαρροή δεδομένων, αν άλλαξε ο αριθμός στα δικαιώματα τα οποία απαιτούνται και αν η χρήση ιχνηλατών αυξήθηκε από τις εφαρμογές.

Πρόσφατα, μελετήθηκε το κατά πόσο ο χρήστης στις εφαρμογές τηλεδιασκέψεων πατώντας το κουμπί σίγασης είναι πραγματικά σε σίγαση. Πραγματικά ενδιαφέρουσα μελέτη η οποία ανοίγει το έδαφος και για άλλες παρόμοιες έρευνες. Ο χρήστης κλείνοντας την κάμερα του κατά τη διεξαγωγή τηλεδιάσκεψης όντως δεν φαίνεται από τους υπόλοιπους χρήστες ή την εφαρμογή; Η πρόσβαση για κοινοποίηση υλικού κατά τη διεξαγωγή τηλεδιάσκεψης πως χρησιμοποιείται αργότερα από την εφαρμογή, ίσως χρησιμοποιηθεί κακόβουλα; Οι εφαρμογές ανταλλαγής μηνυμάτων οι οποίες δίνουν τη δυνατότητα διαγραφής μηνύματος στο χρήστη όντως διαγράφουν το μήνυμα ή παραμένει αποθηκευμένο για κάποιο χρονικό διάστημα εν αγνοία του χρήστη; Αυτές είναι κάποιες από τις μελλοντικές έρευνες που θα μπορούσαν να διεξαχθούν μιας και με την εισαγωγή του ΓΚΠΔ ο κόσμος ευαισθητοποιήθηκε περισσότερο με την έννοια τόσο της ιδιωτικότητας όσο και των προσωπικών δεδομένων και απαιτεί όλο και περισσότερο διαφάνεια από τις εφαρμογές τις οποίες χρησιμοποιεί καθημερινά.

Βιβλιογραφία

[01] *Number of messaging app users to rise 6% to 3 billion in 2021*. (2021, September 14). Business of Apps. https://www.businessofapps.com/news/number-of-messaging-app-users-to-rise-6-to-3-billion-in-2021/

[02] Wagenseil, P. (2022, March 18). *Zoom security issues: What's gone wrong and what's been fixed*. Tom's Guide. https://www.tomsguide.com/news/zoom-security-privacy-woes#:%7E:text=Nov.,-10%3A%20FTC%20says&text=The%20Federal%20Trade%20Commission%20announced,authorization%20in%202018%20and%202019.

[03] *Mobile Operating System Market Share Worldwide | Statcounter Global Stats*. (2022). StatCounter Global Stats. https://gs.statcounter.com/os-market-share/mobile/worldwide/#yearly-2009-2022

[04] *Tablet Operating System Market Share Worldwide | Statcounter Global Stats*. (2022). StatCounter Global Stats. https://gs.statcounter.com/os-market-share/tablet/worldwide/#yearly-2012-2022

[05] *Android versions comparison | Comparison tables - SocialCompare*. (2021, December 29). SocialCompare. https://socialcompare.com/en/comparison/android-versions-comparison

[06] *App Store Data (2022)*. (2022, May 4). Business of Apps. https://www.businessofapps.com/data/app-stores/

[07] Developers, A. (2011). What is android?. *Dosegljivo: http://www. academia. edu/download/30551848/andoid--tech. pdf*.

[08] Kaur, P., & Sharma, S. (2014). Google Android a mobile platform: A review. *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*. https://doi.org/10.1109/raecs.2014.6799598

[09] *Permissions on Android |*. (n.d.). Android Developers. https://developer.android.com/guide/topics/permissions/overview?hl=en

[10] *Android Runtime Permissions Tutorial and Example*. (2021, May 23). Camposha Info. https://camposha.info/android-examples/android-runtime-permissions/#gsc.tab=0

[11] He, Q., Li, B., Chen, F., Grundy, J., Xia, X., & Yang, Y. (2022). Diversified Third-Party Library Prediction for Mobile App Development. *IEEE Transactions on Software Engineering*, *48*(1), 150–165. https://doi.org/10.1109/tse.2020.2982154

[12] He, Y., Yang, X., Hu, B., & Wang, W. (2019). Dynamic privacy leakage analysis of Android third-party libraries. *Journal of Information Security and Applications*, *46*, 259–270. https://doi.org/10.1016/j.jisa.2019.03.014

[13] Taylor, V. F., Beresford, A. R., & Martinovic, I. (2017). Intra-library collusion: A potential privacy nightmare on smartphones. *arXiv preprint arXiv:1708.03520*.

[14] *The evolution of the concept of privacy*. (2020, August 21). European Digital Rights (EDRi). https://edri.org/our-work/evolution-concept-privacy/

[15] *Privacy (Stanford Encyclopedia of Philosophy)*. (2018, January 18). Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/privacy/

[16] Abdul, T. (2020). The Concept of Privacy: Is Privacy Still a Useful Concept?. *Available at SSRN 3668520*.

[17] Council of Europe. (n.d.). *Protection of personal data and privacy*. https://www.coe.int/en/web/portal/personal-data-protection-and-privacy

[18] European Union. (2010). Charter of Fundamental Rights of the European Union. In *Official Journal of the European Union C83* (Vol. 53, p. 380). European Union.

[19] *What is personal data?* (2018, August 1). European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

[20] European Union Agency for Cybersecurity, (2018). *Privacy and data protection in mobile applications : a study on the app development ecosystem and the technical implementation of GDPR*, European Network and Information Security Agency. **https://data.europa.eu/doi/10.2824/114584**

[21] Tucker, J. (2020, March 24). *Discord 101: How to set up the chat app so you can live your best isolation life*. Curated. https://dailyhive.com/vancouver/set-up-discord

[22] Secure Messaging Apps Comparison. (2021, November 17). *Secure Messaging Apps Comparison | Privacy Matters*. https://www.securemessagingapps.com/

[23] *Software:Element - HandWiki*. (n.d.). HandWiki. https://handwiki.org/wiki/Software:Element

[24] Lebow, S. (2021, May 13). *KakaoTalk is the most popular messaging app in South Korea by a massive margin*. Insider Intelligence. https://www.emarketer.com/content/kakaotalk-most-popular-messaging-app-south-korea-by-massive-margin

[25] Kakao Corp. (n.d.). *KakaoTalk, where people and the world come to get connected*. Kakaocorp.Com. https://www.kakaocorp.com/page/service/service/KakaoTalk?lang=en

[26] DMFA Marketing Team. (2021, November 17). *Why LINE is the most popular social media app in Japan*. DIGITAL MARKETING FOR ASIA. https://www.digitalmarketingforasia.com/why-line-is-the-most-popular-social-media-app-in-japan/

[27] *LINE Transparency Report*. (n.d.). LINE Corporation. Retrieved November 13, 2019, from https://linecorp.com/en/security/encryption/2019h1#:%7E:text=LINE%20employs%20various%20encryption%20technologies,and%20supported%20voice%2Fvideo%20calls.

[28] *LINE Announces Message Stickers: Write Self-Introductions, Birthday Messages and More | LINE Corporation | News*. (2020, March 30). LINE Corporation. https://linecorp.com/en/pr/news/en/2020/3157

[29] Buck, T. (2022, January 27). *Express Yourself in Messenger's End-to-End Encrypted Chats*. Messenger News. https://messengernews.fb.com/2022/01/27/express-yourself-in-messengers-end-to-end-encrypted-chats/

[30] *Phoenix - Facebook & Messenger - Apps on Google Play*. (n.d.). Google Play. https://play.google.com/store/apps/details?id=com.jesture.phoenix&hl=en&gl=US

[31] Das, A. (2020, March 2). Session: An Open Source Private Messenger That Doesn't Need Your Phone Number. It's FOSS. https://itsfoss.com/session-messenger/

[32] *Signal Messenger: Speak Freely*. (n.d.). Signal Messenger. https://signal.org/

[33] *Skype - Apps on Google Play*. (n.d.). Google Play. https://play.google.com/store/apps/details?id=com.skype.raider&hl=en_US&gl=US

[34] Finnegan, M. (2020, December 21). *Microsoft Teams: How to use it, and how it stacks up to Slack and Zoom*. Computerworld. https://www.computerworld.com/article/3276276/microsoft-teams-its-features-how-it-compares-to-slack-and-other-rivals.html

[35] Figure 7: An example of interaction with the telegram bot. (n.d.). Retrieved May 4, 2022, from https://www.researchgate.net/figure/An-example-of-interaction-with-the-Telegram-Bot_fig7_330243030

[36] Reyes, S. (2021, August 13). *Cisco Webex Meetings Guide*. Greyson Technologies. https://www.greyson.com/getting-started-with-webex-meetings/

[37] *Who*. (n.d.). Exodus Privacy. https://exodus-privacy.eu.org/en/page/who/

[38] *What*. (n.d.). Exodus Privacy. https://exodus-privacy.eu.org/en/page/what/

[39] A. (n.d.). *Inspeckage/README.md at master · ac-pm/Inspeckage*. GitHub. https://github.com/ac-pm/Inspeckage/blob/master/README.md#-inspeckage---android-package-inspector

[40] A. (n.d.-a). *GitHub - ac-pm/SSLUnpinning_Xposed: Android Xposed Module to bypass SSL certificate validation (Certificate Pinning).* GitHub. https://github.com/ac-pm/SSLUnpinning_Xposed

[41] *Privacy International's data interception environment*. (2019, February 17). Privacy International. https://privacyinternational.org/node/2732#component-layout

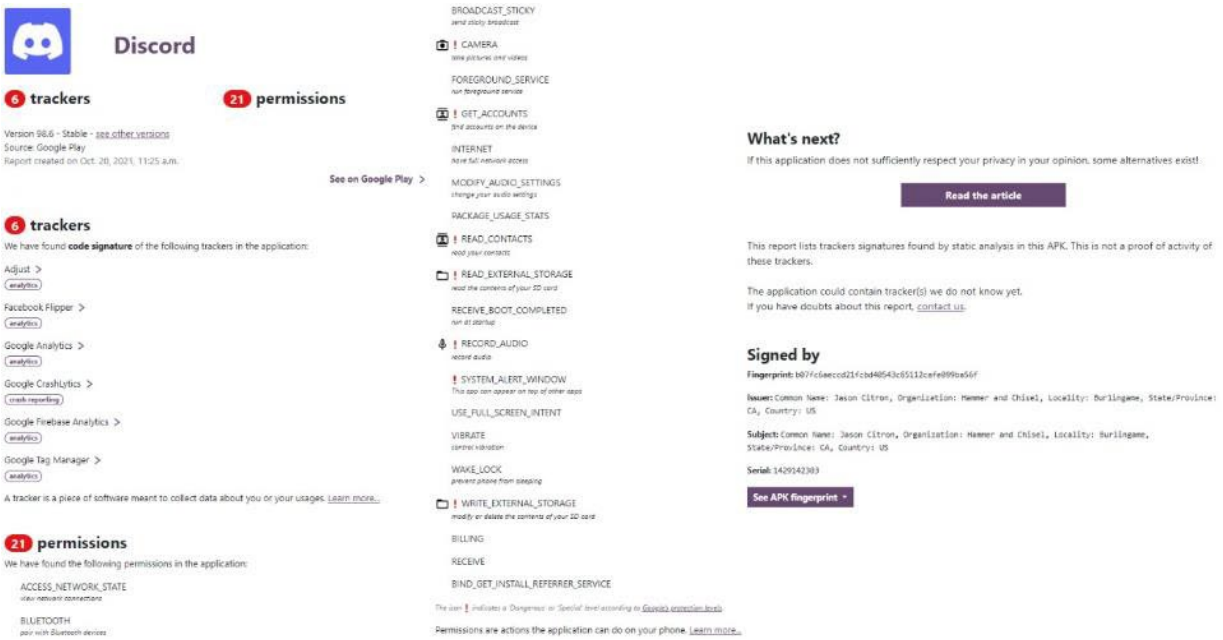
[42] Yang, Y., West, J., Thiruvathukal, G. K., Klingensmith, N., & Fawaz, K. (2022). Are You Really Muted?: A Privacy Analysis of Mute Buttons in Video Conferencing Apps. *arXiv preprint arXiv:2204.06128*.

Παράρτημα Α
Αποτελέσματα της ανάλυσης των εφαρμογών μέσω των εργαλείων λογισμικού

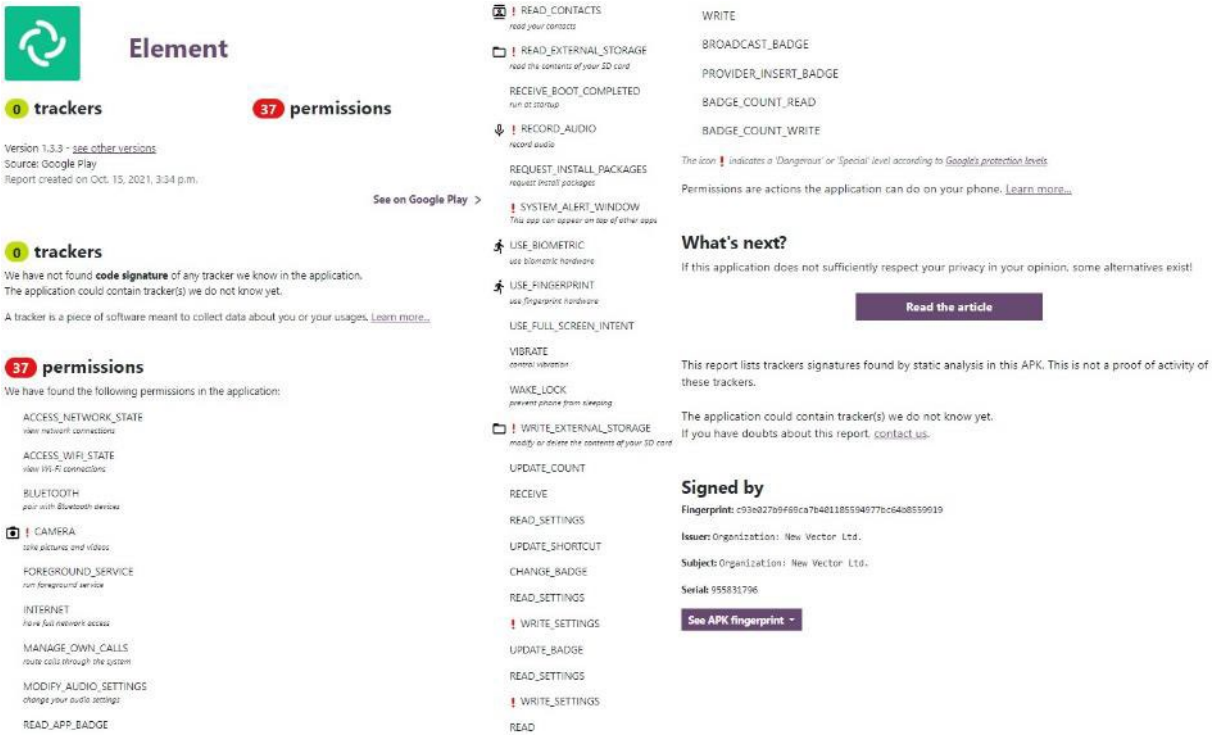
Στο παρόν παράρτημα παρουσιάζονται τα στιγμιότυπα από τη μελέτη των εφαρμογών με τη χρήση τεσσάρων διαφορετικών εργαλείων.

Α.1 Exodus Privacy

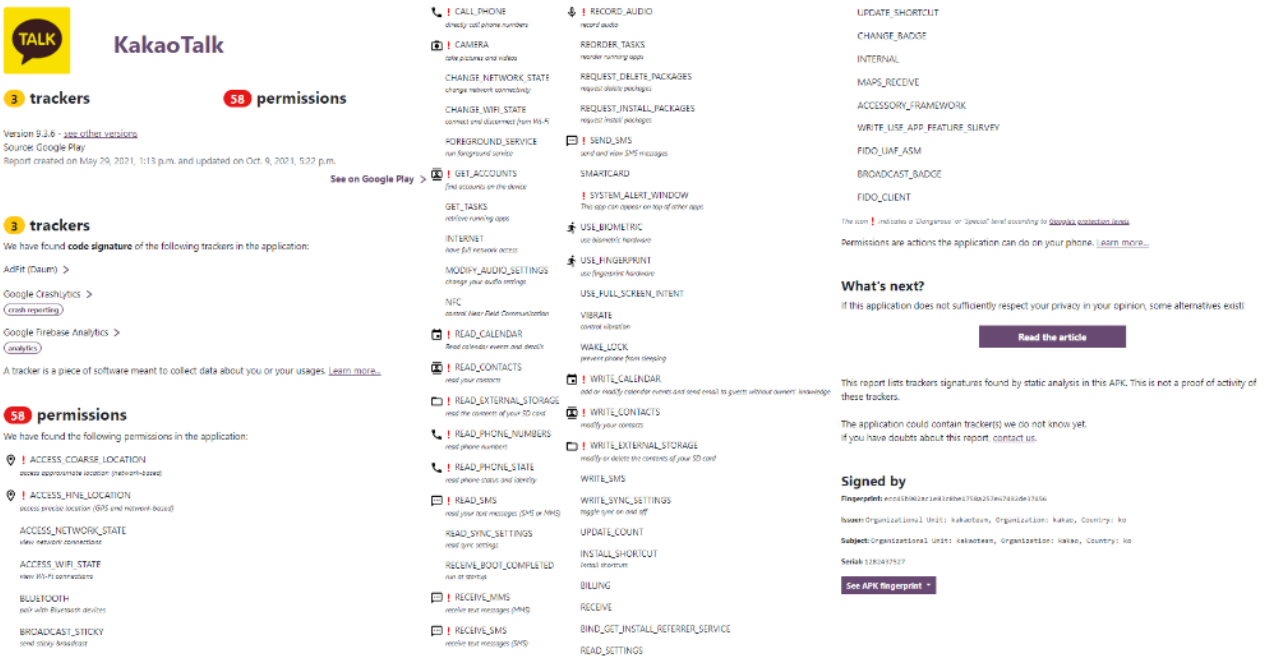
Πιο κάτω θα παρουσιαστούν στιγμιότυπα από τη μελέτη των εφαρμογών συνομιλιών/τηλεπικοινωνιών με τη χρήση του διαδικτυακού εργαλείου Exodus Privacy.



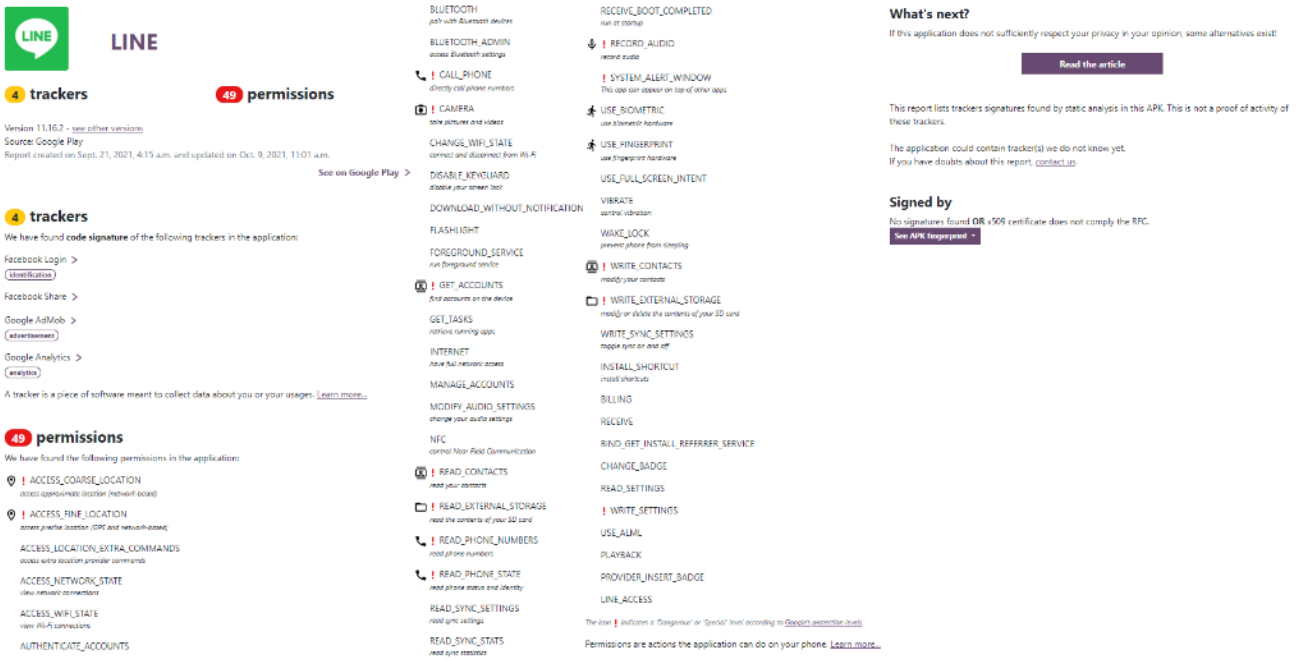
Εικόνα Α.1: Στιγμιότυπο της ανάλυσης της εφαρμογής Discord



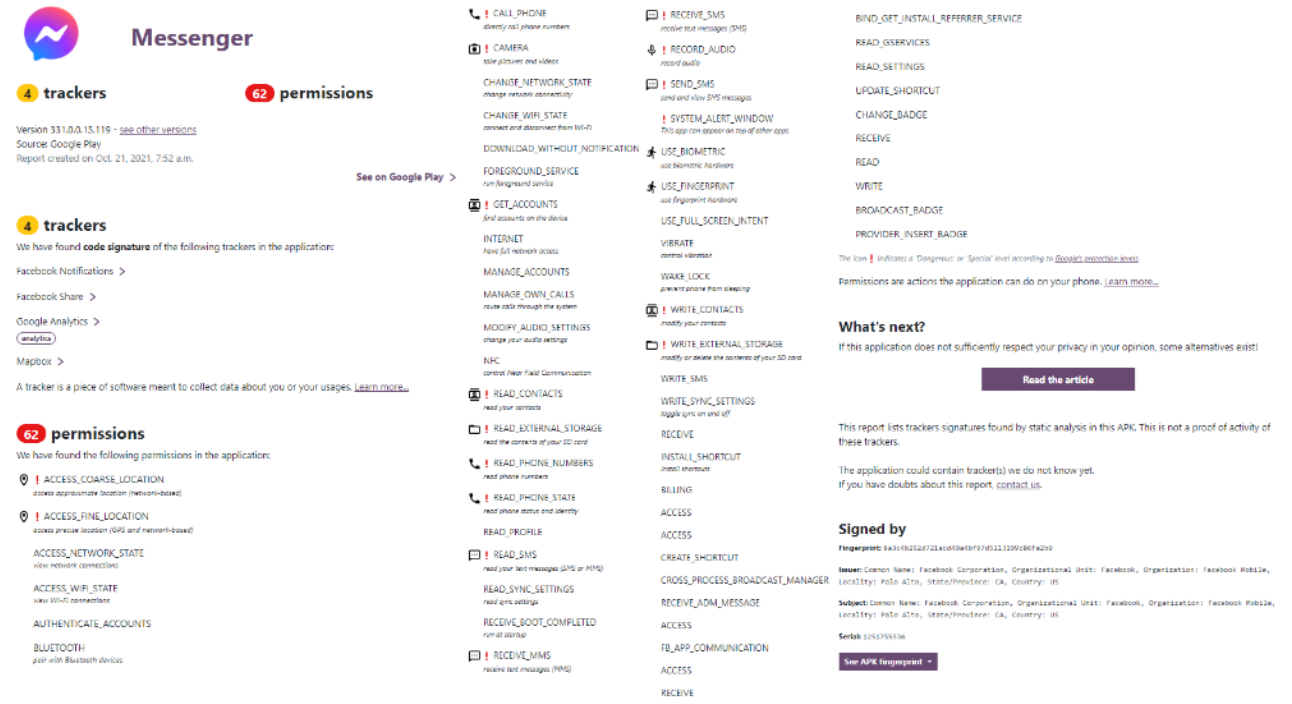
Εικόνα Α.2: Στιγμιότυπο της ανάλυσης της εφαρμογής Element



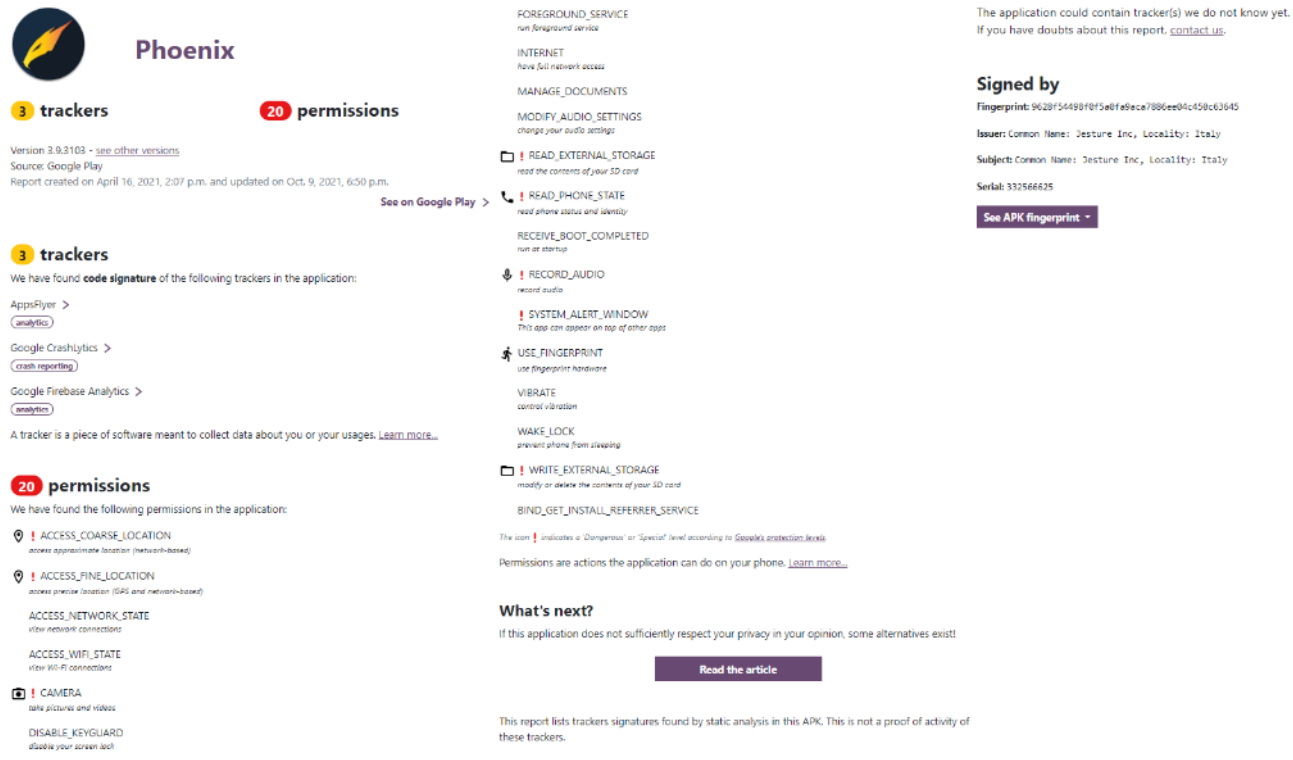
Εικόνα Α.3: Στιγμιότυπο της ανάλυσης της εφαρμογής KakaoTalk



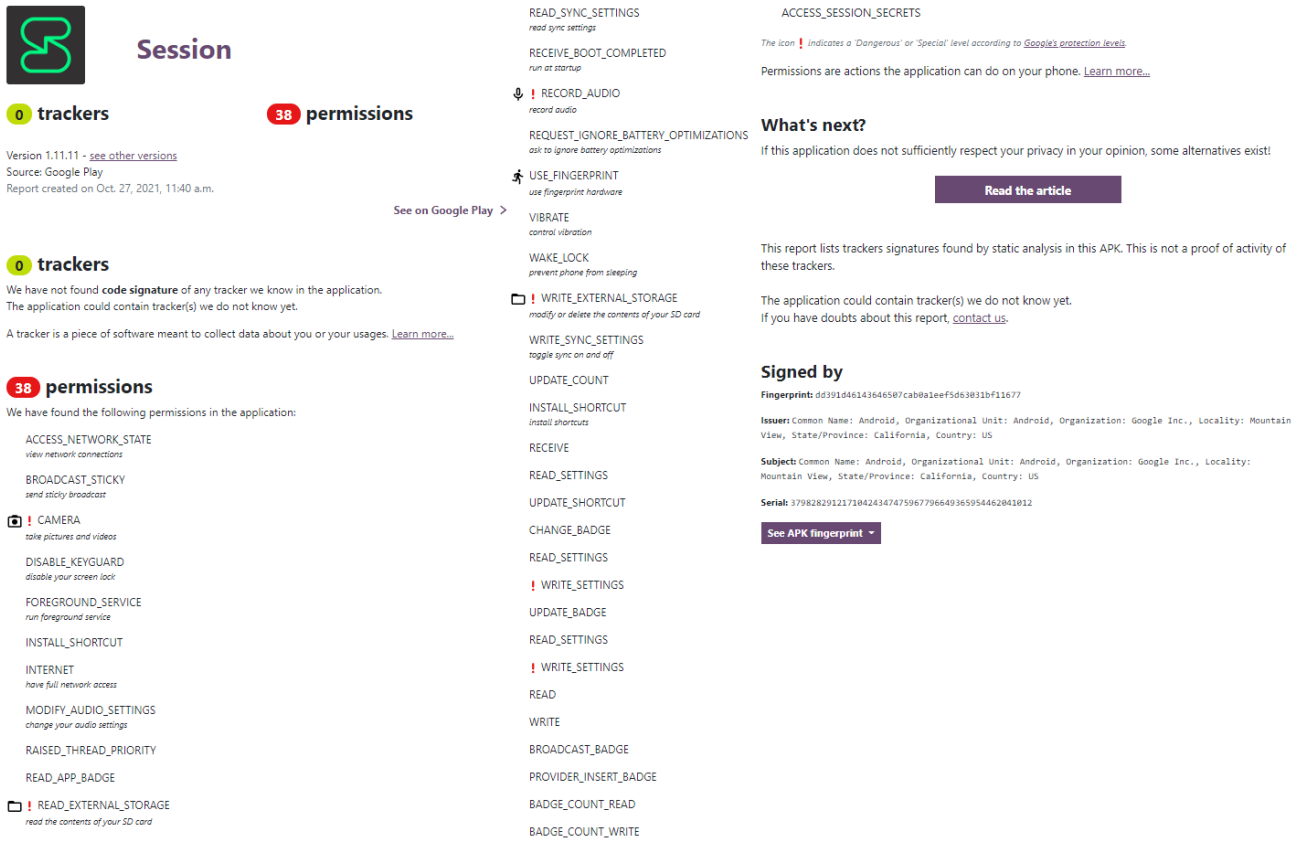
Εικόνα Α.4: Στιγμιότυπο της ανάλυσης της εφαρμογής Line



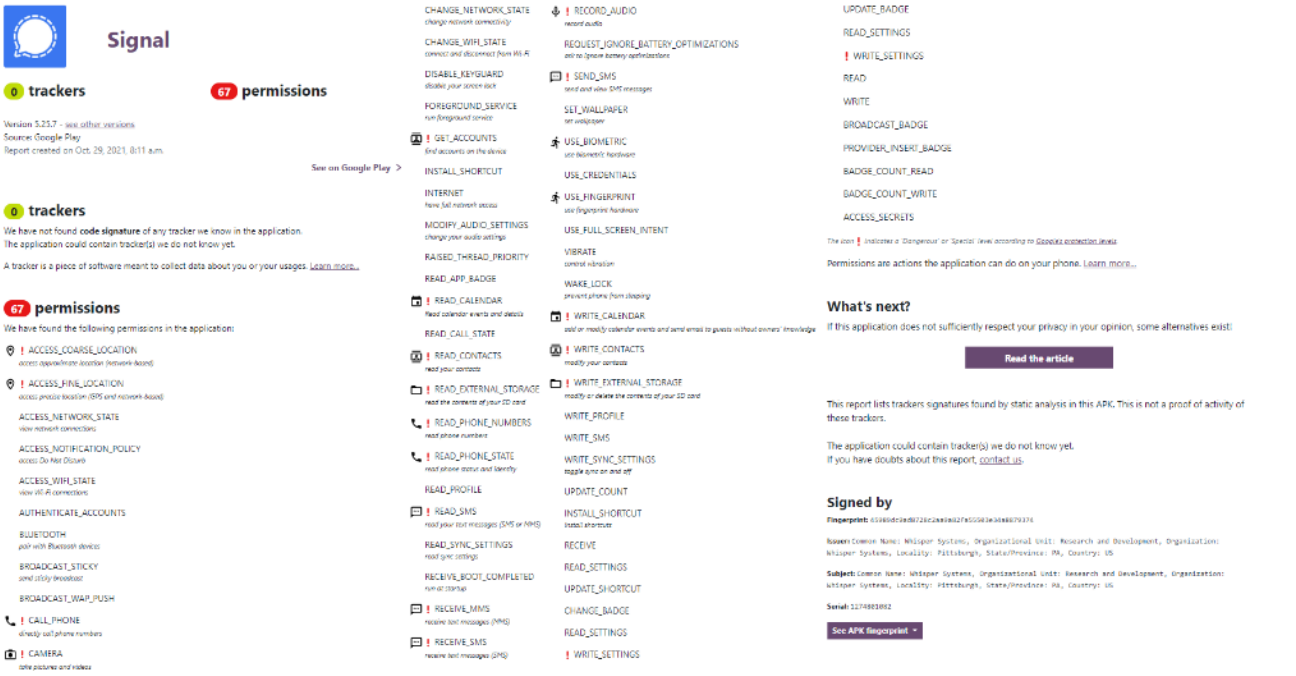
Εικόνα Α.5: Στιγμιότυπο της ανάλυσης της εφαρμογής Messenger



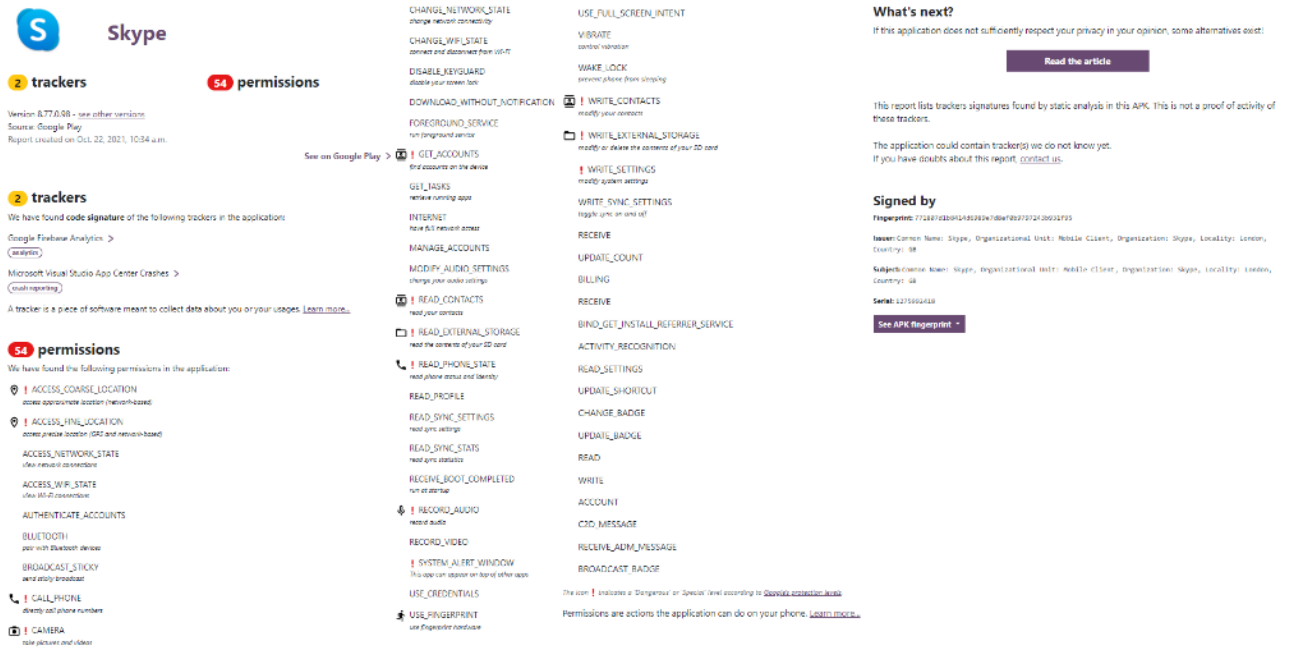
Εικόνα Α.6: Στιγμιότυπο της ανάλυσης της εφαρμογής Phoenix



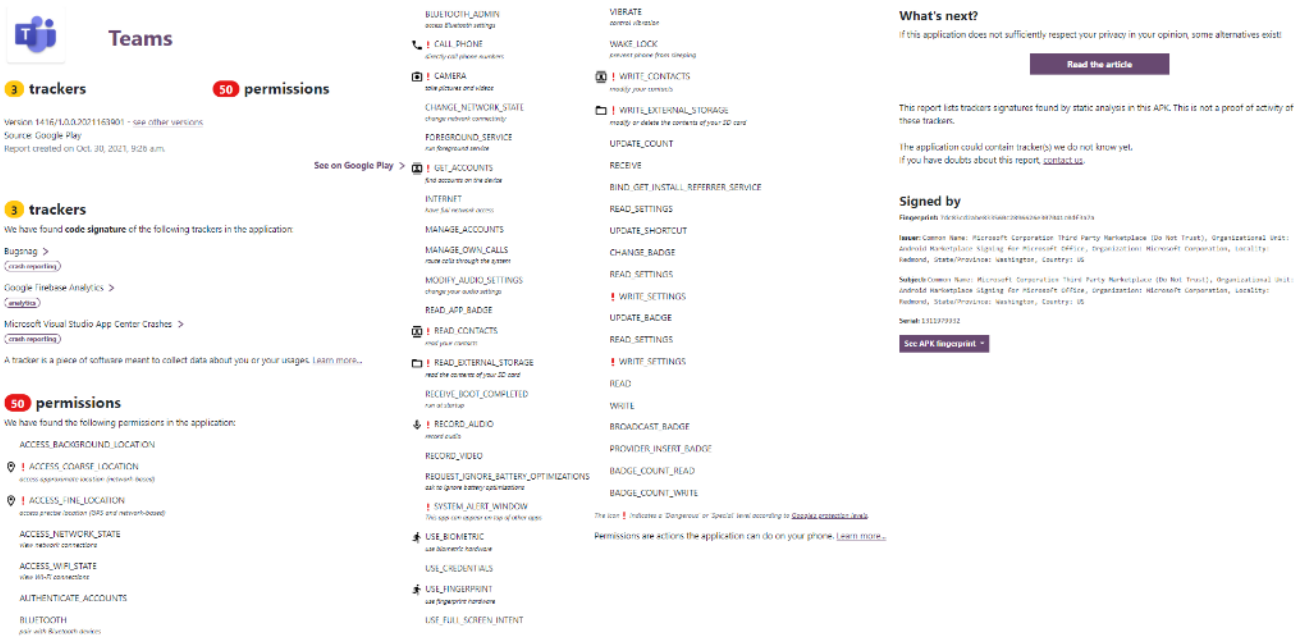
Εικόνα Α.7: Στιγμιότυπο της ανάλυσης της εφαρμογής Session



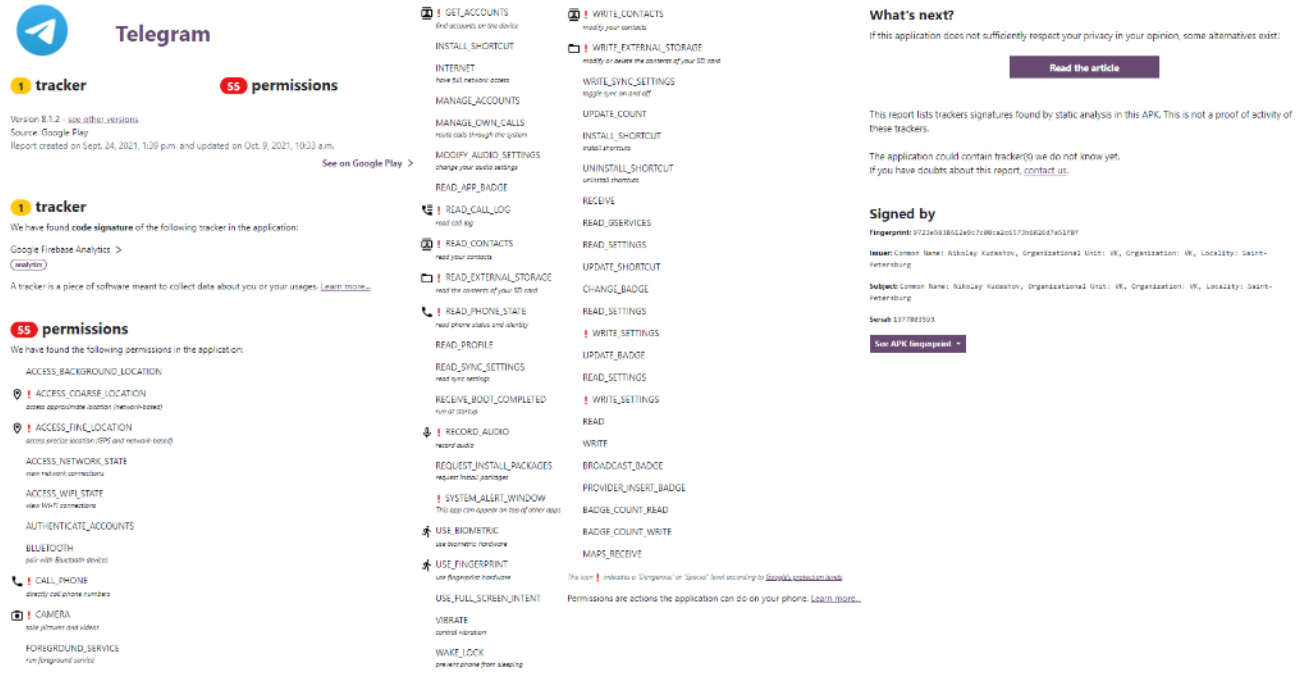
Εικόνα Α.8: Στιγμιότυπο της ανάλυσης της εφαρμογής Signal



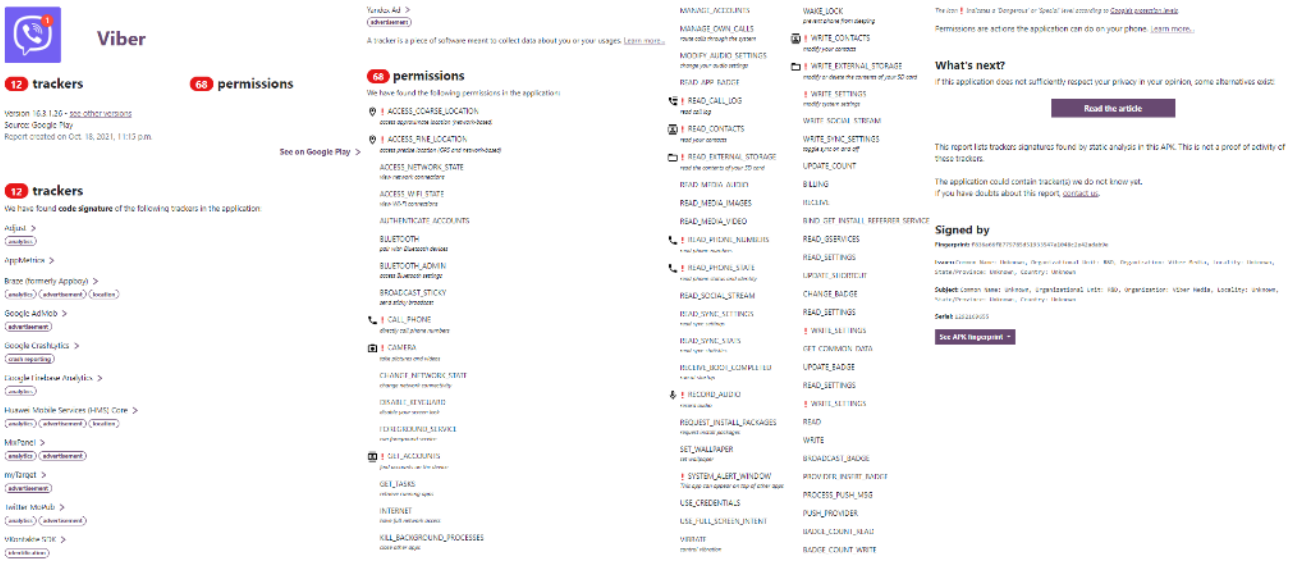
Εικόνα Α.9: Στιγμιότυπο της ανάλυσης της εφαρμογής Skype



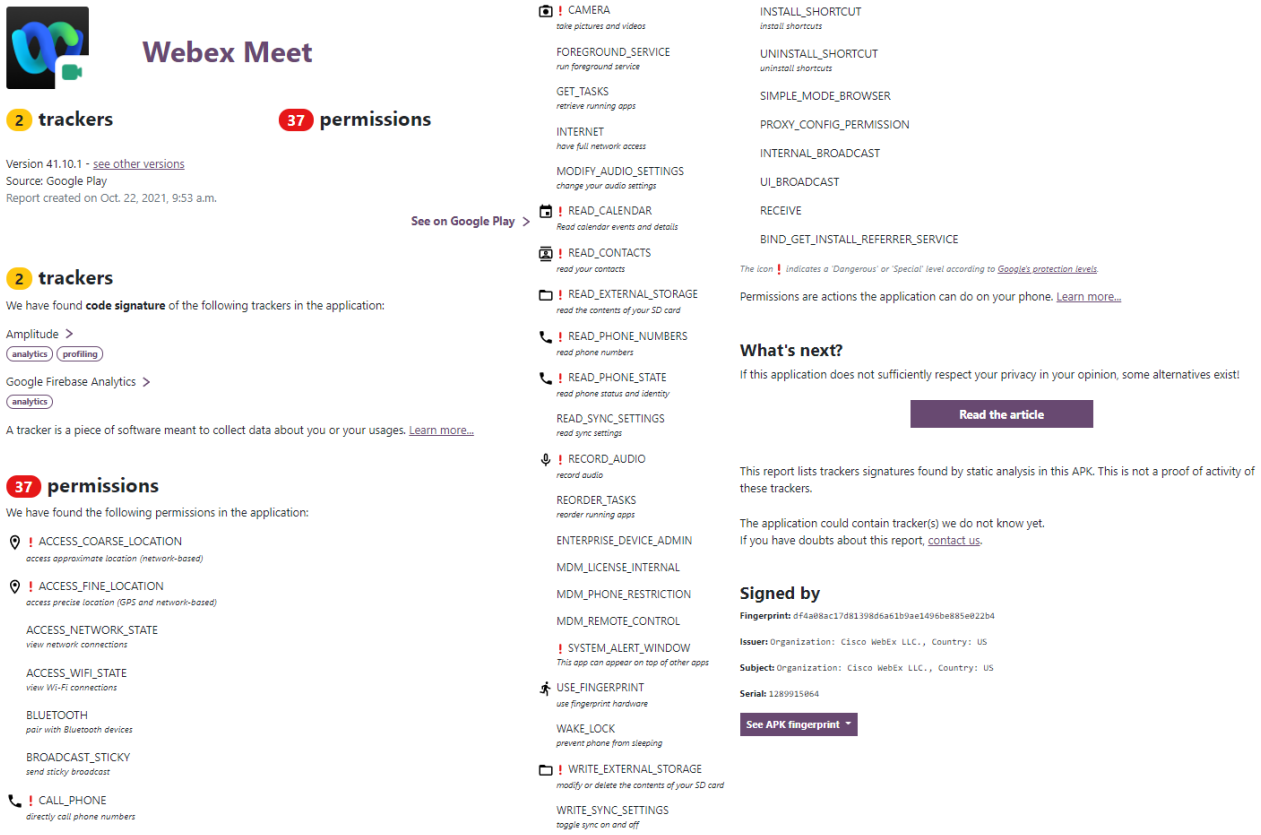
Εικόνα Α.10: Στιγμιότυπο της ανάλυσης της εφαρμογής Teams



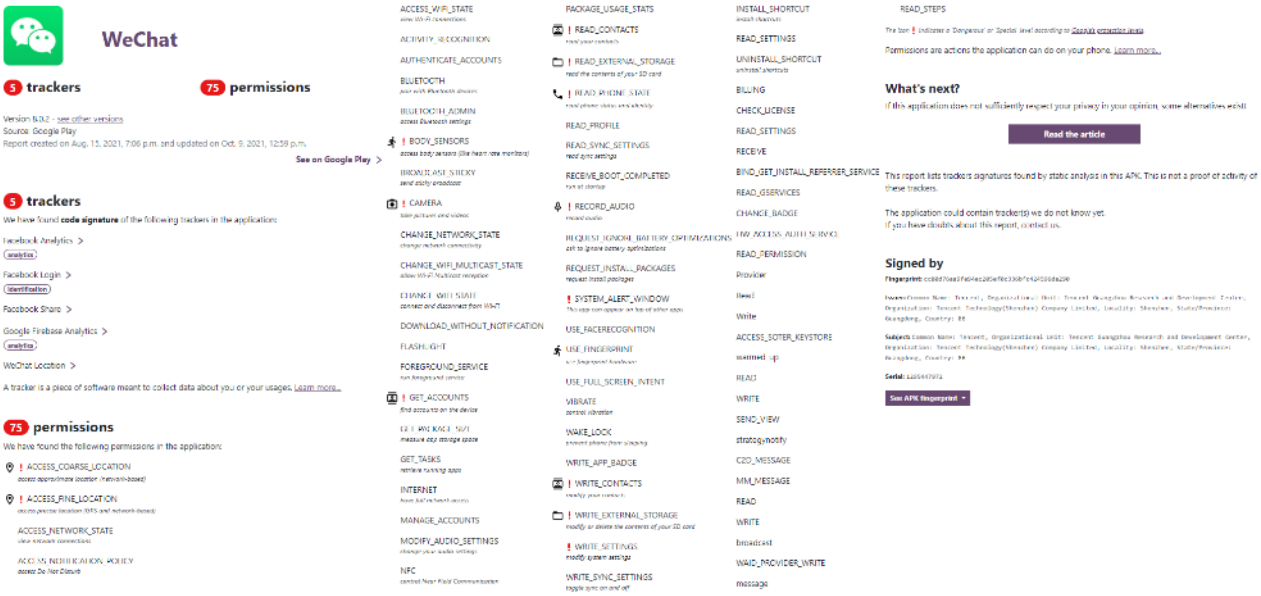
Εικόνα Α.11: Στιγμιότυπο της ανάλυσης της εφαρμογής Telegram



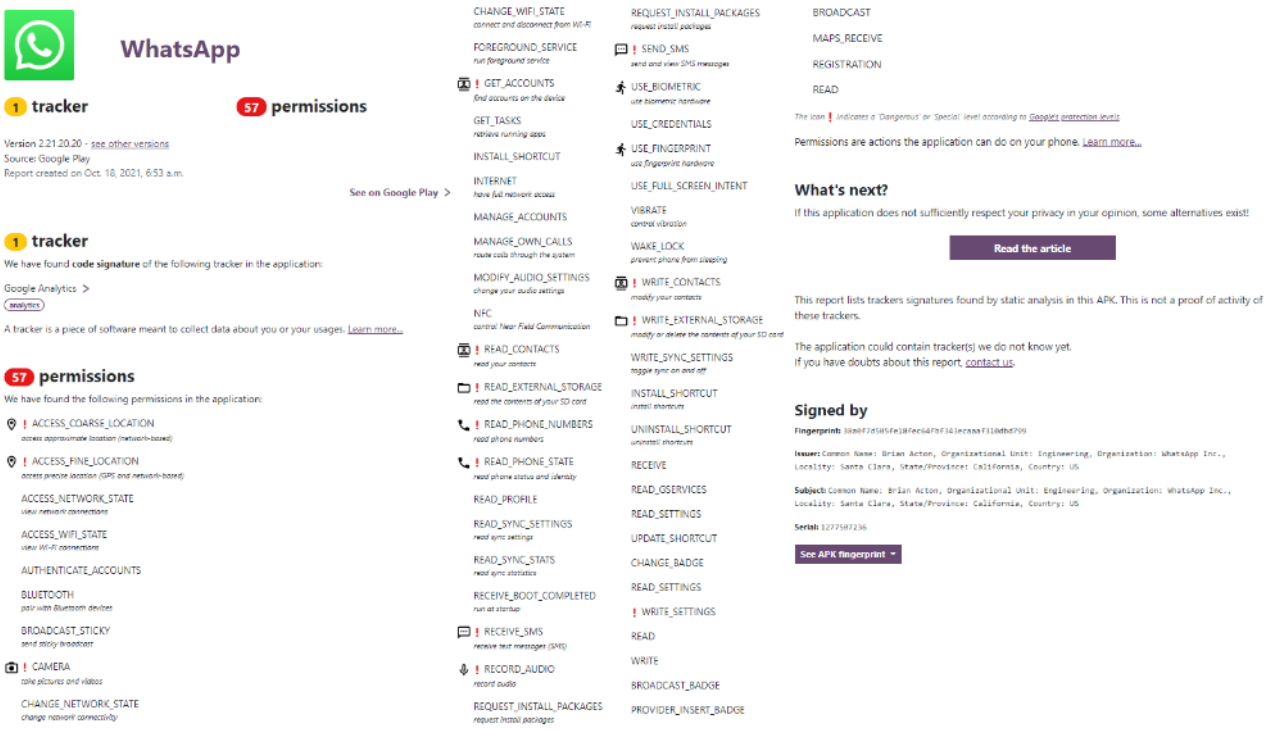
Εικόνα Α.12: Στιγμιότυπο της ανάλυσης της εφαρμογής Viber



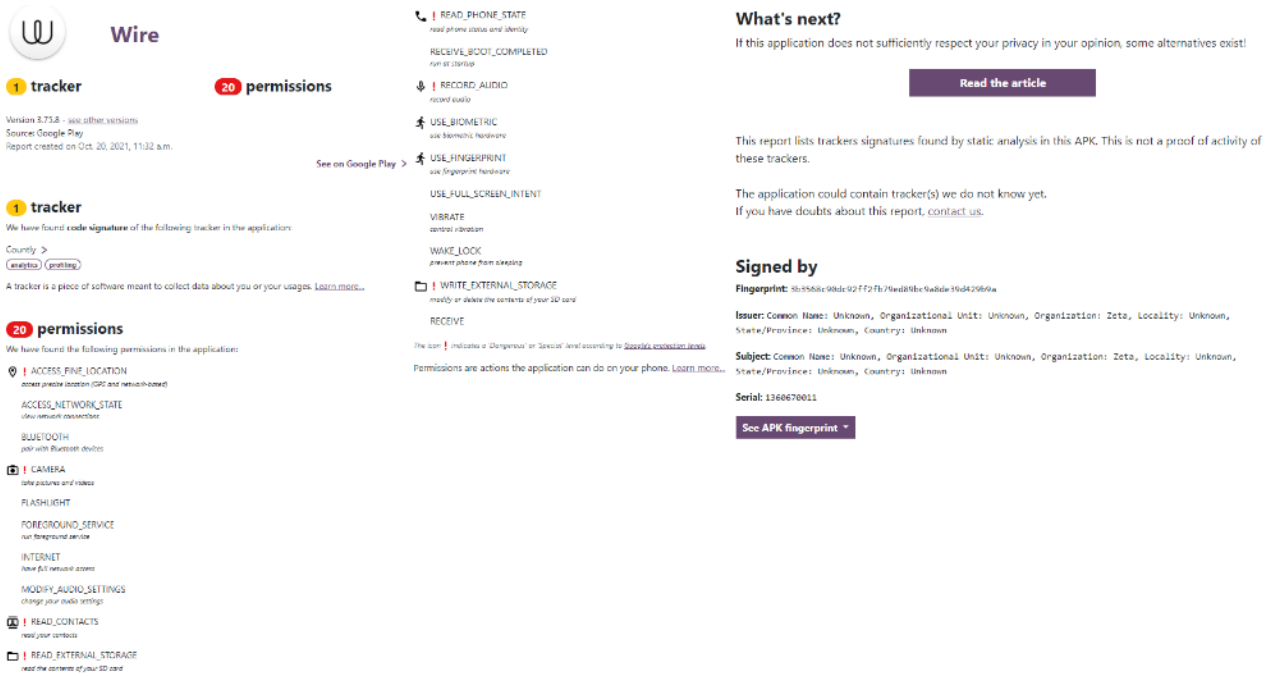
Εικόνα Α.13: Στιγμιότυπο της ανάλυσης της εφαρμογής Webex Meet



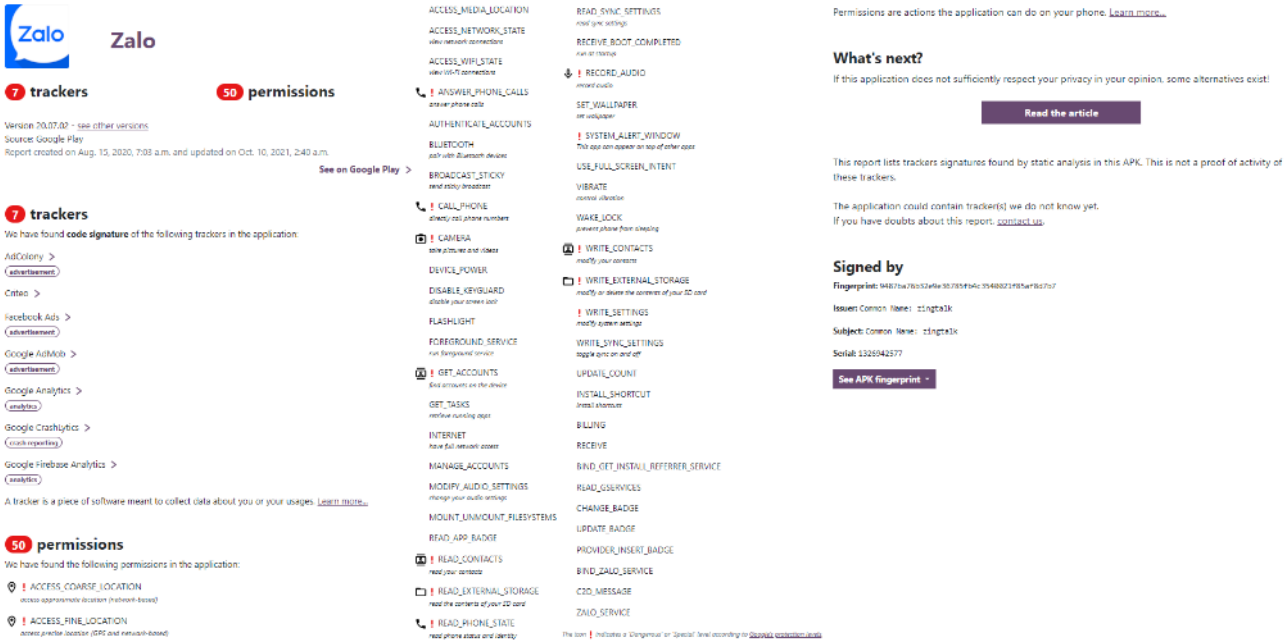
Εικόνα Α.14: Στιγμιότυπο της ανάλυσης της εφαρμογής WeChat



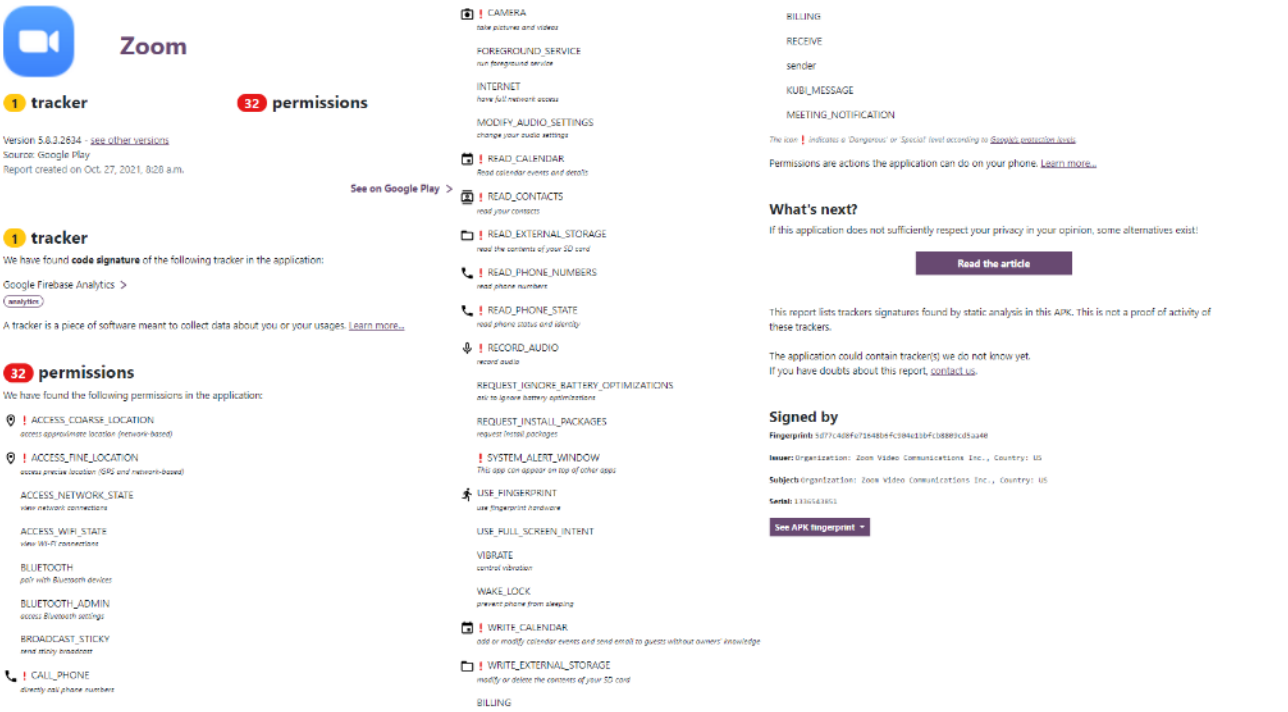
Εικόνα Α.15: Στιγμιότυπο της ανάλυσης της εφαρμογής WhatsApp



Εικόνα Α.16: Στιγμιότυπο της ανάλυσης της εφαρμογής Wire



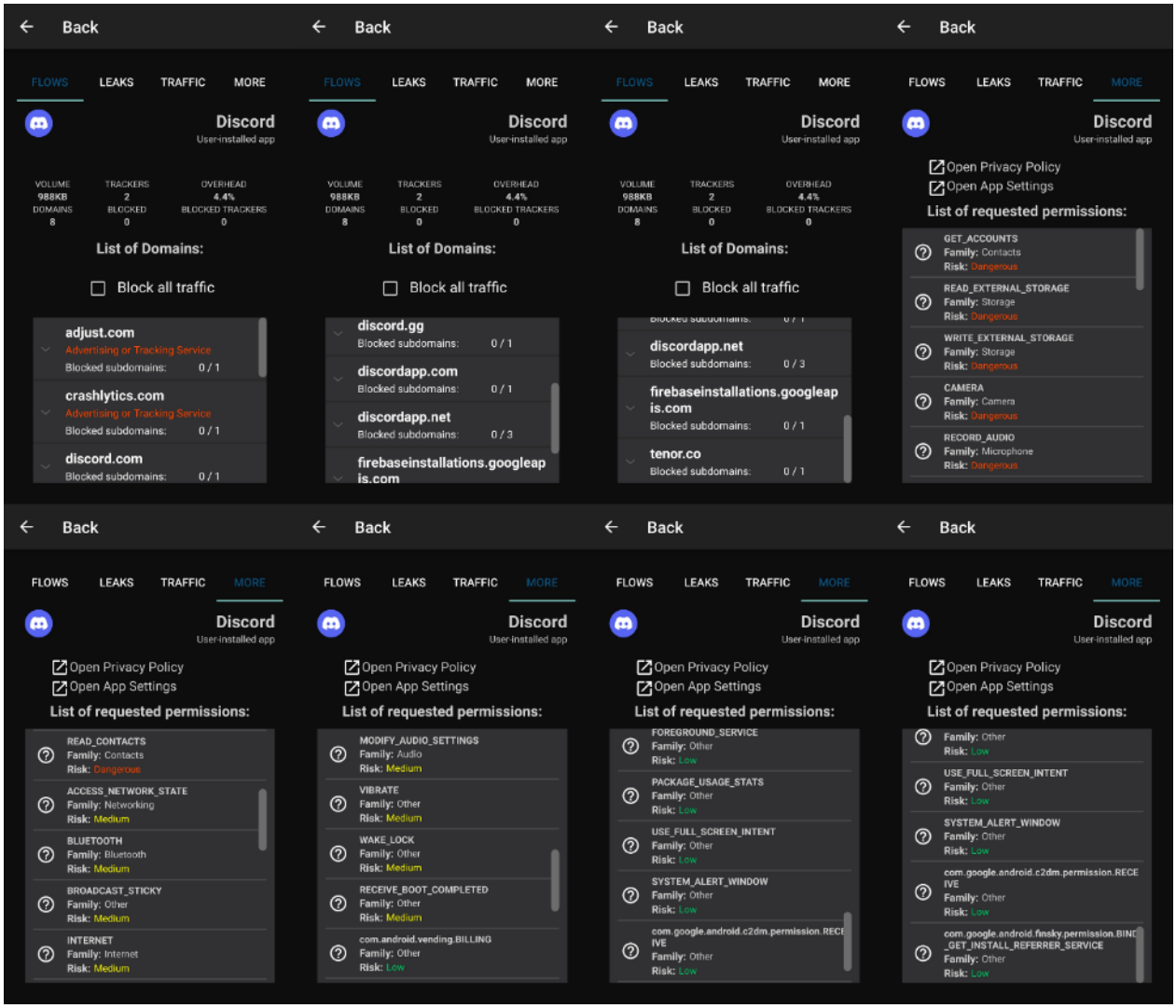
Εικόνα Α.17: Στιγμιότυπο της ανάλυσης της εφαρμογής Zalo



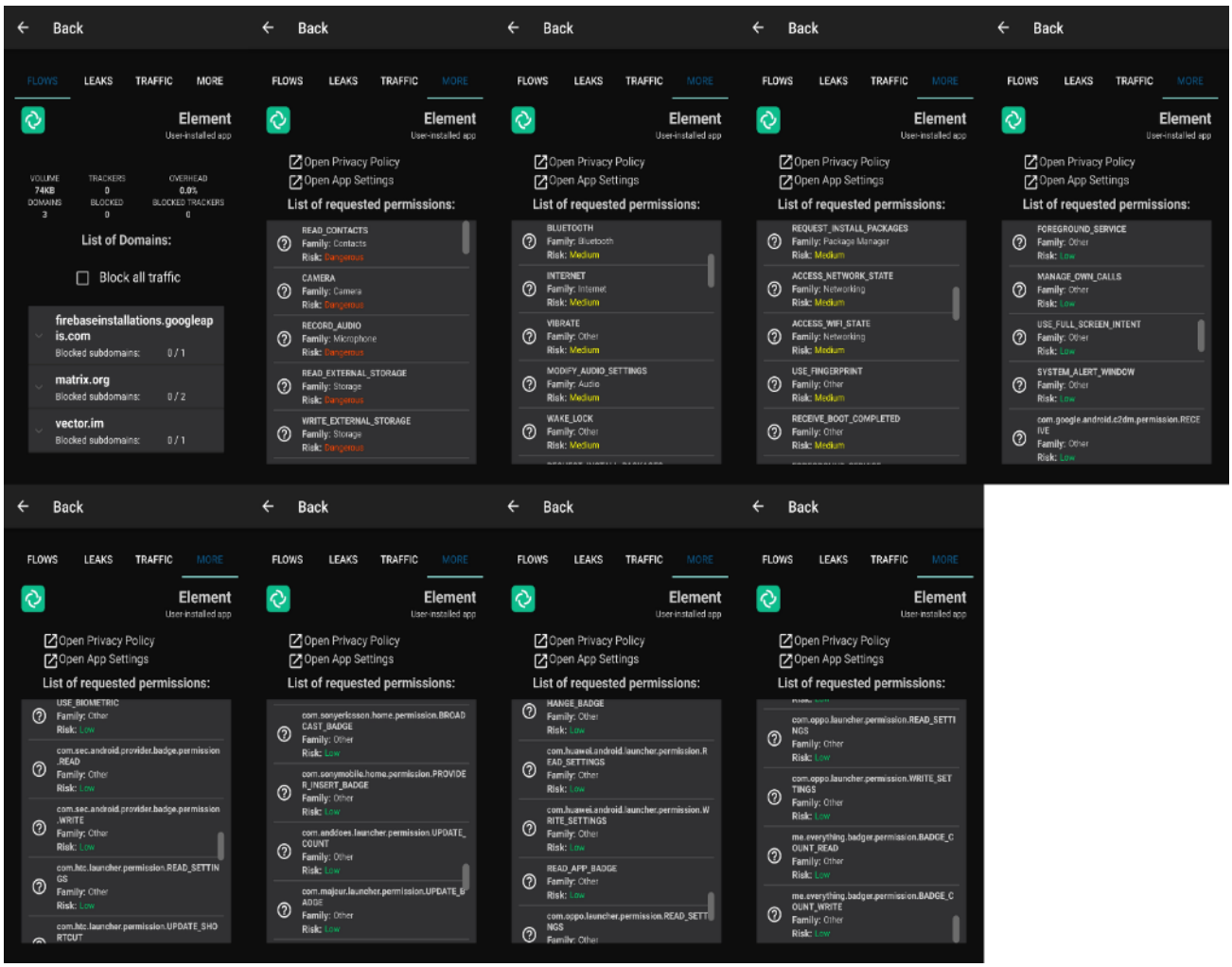
Εικόνα Α.18: Στιγμιότυπο της ανάλυσης της εφαρμογής Zoom

A.2 Lumen Privacy Monitor

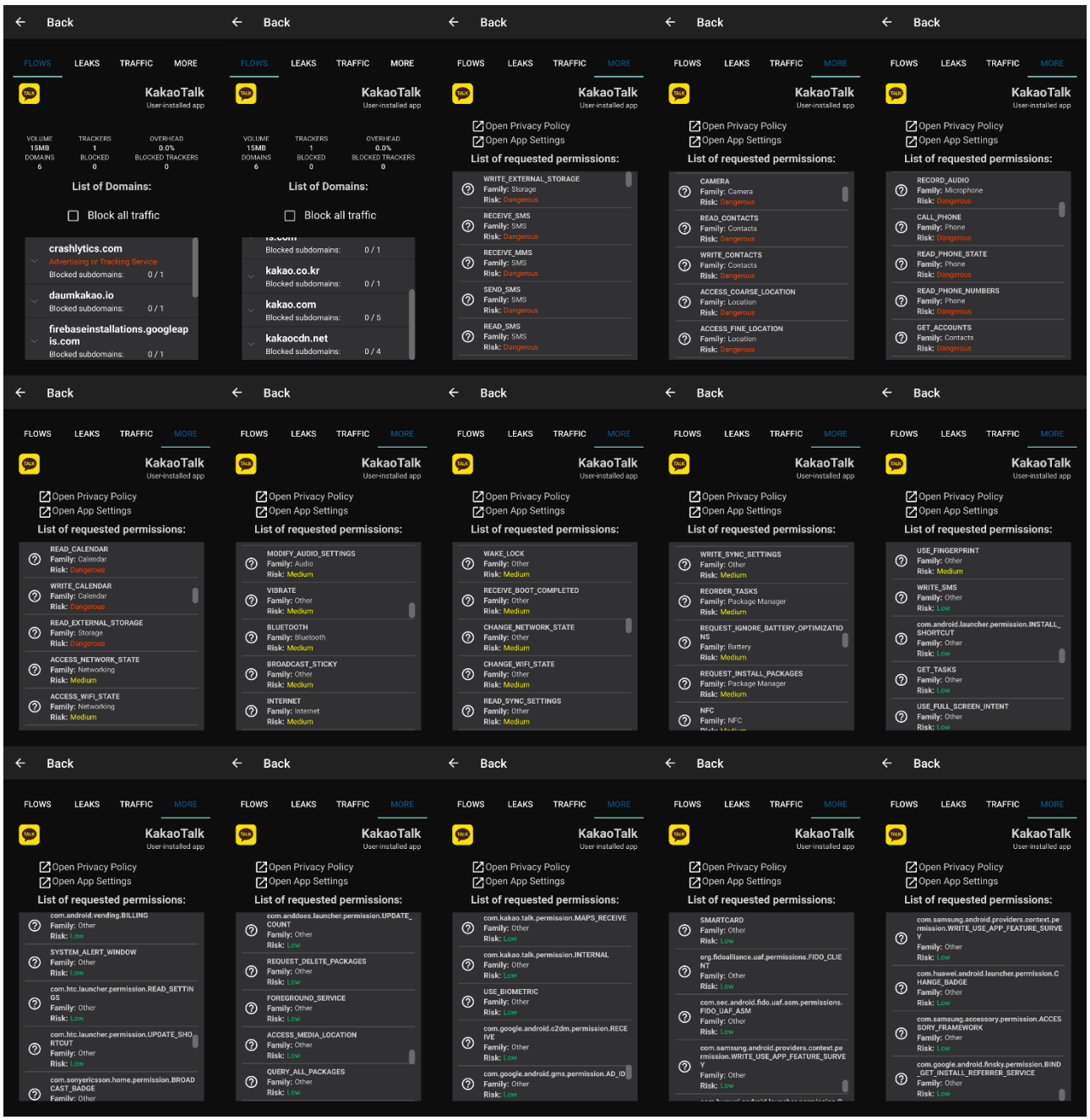
Πιο κάτω θα παρουσιαστούν στιγμιότυπα από τη μελέτη των εφαρμογών συνομιλιών/τηλεπικοινωνιών με τη χρήση του εργαλείου Lumen Privacy Monitor.



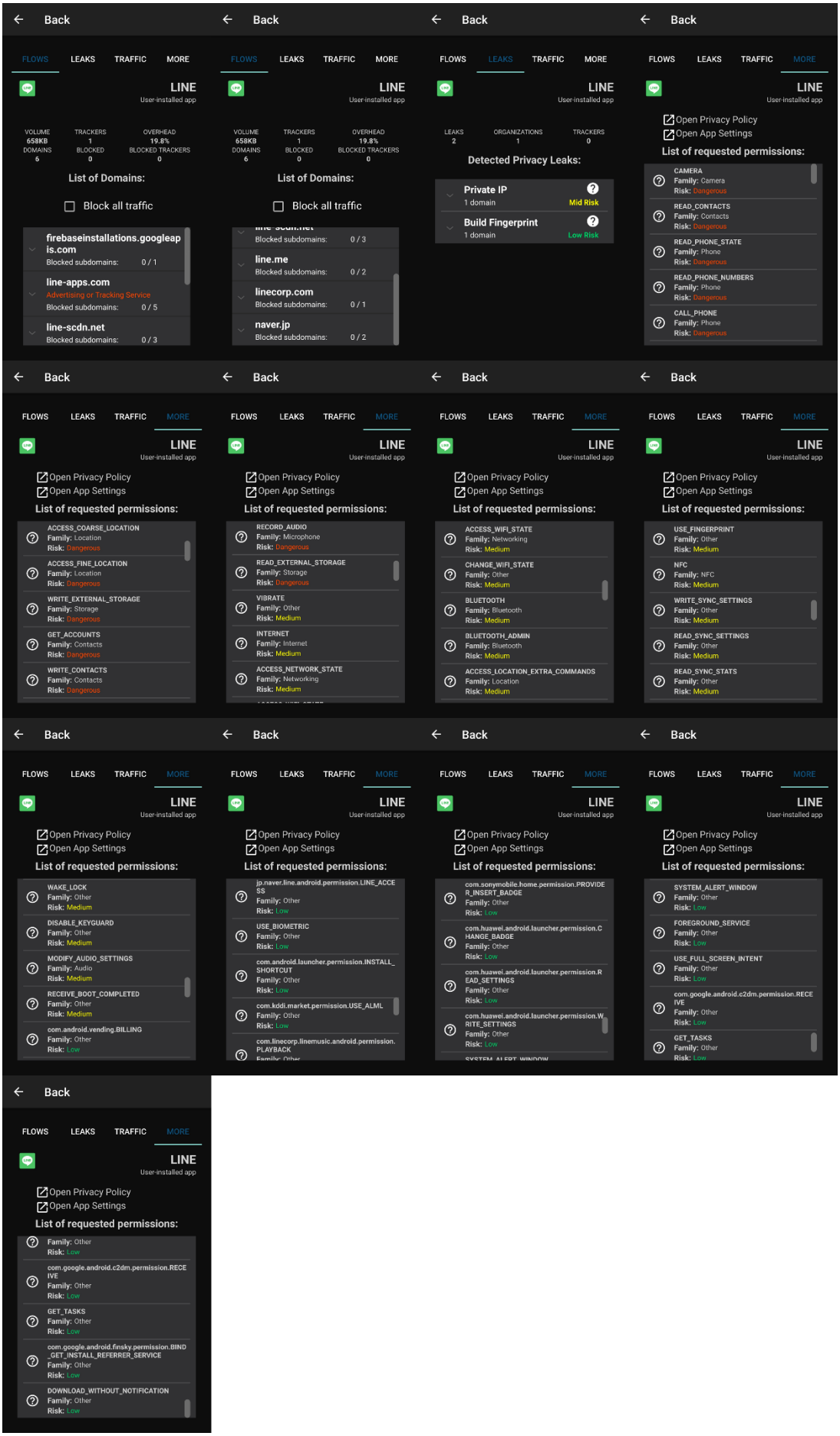
Εικόνα Α.19: Στιγμιότυπο της ανάλυσης της εφαρμογής Discord



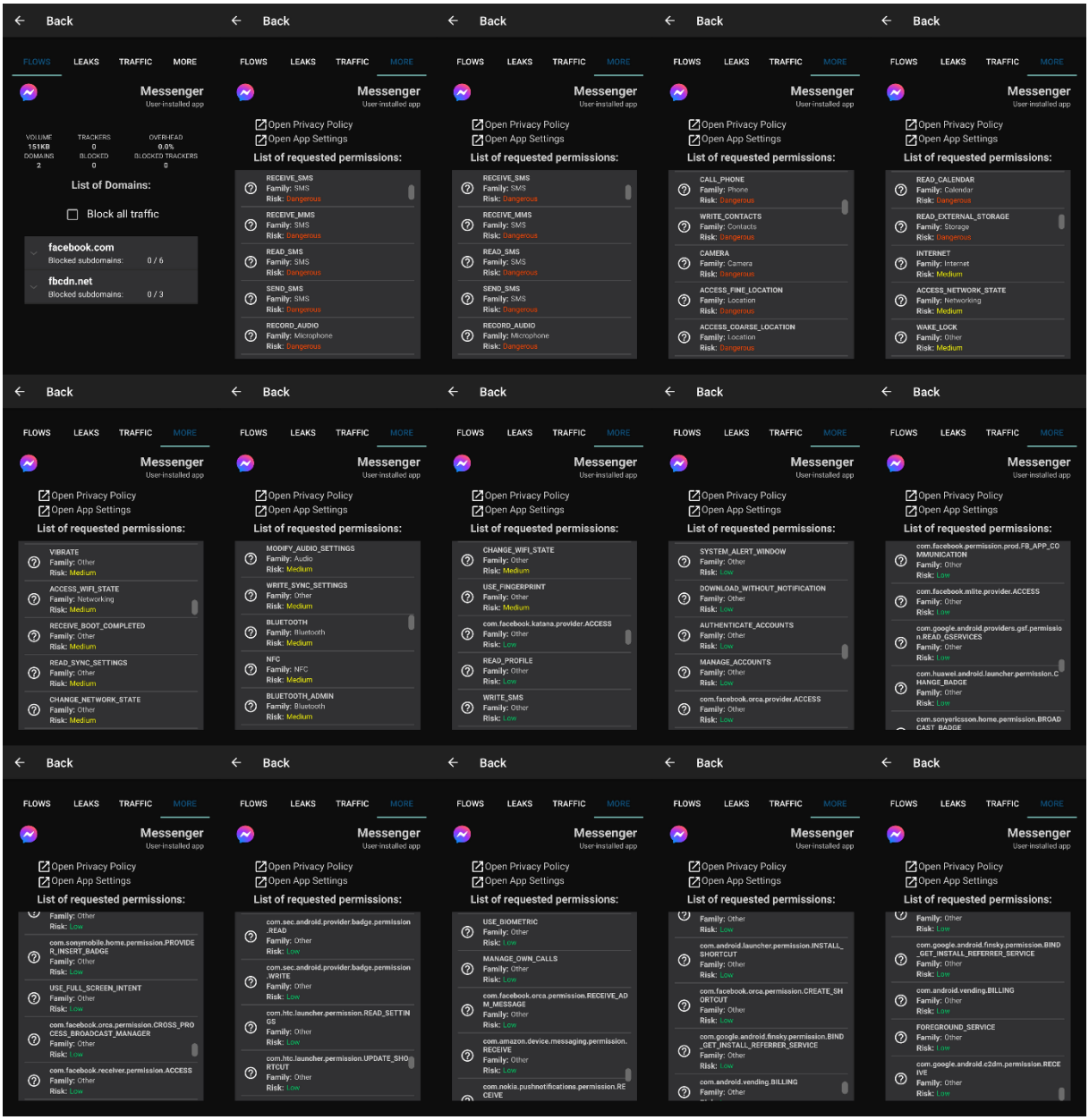
Εικόνα Α.20: Στιγμιότυπο της ανάλυσης της εφαρμογής Element



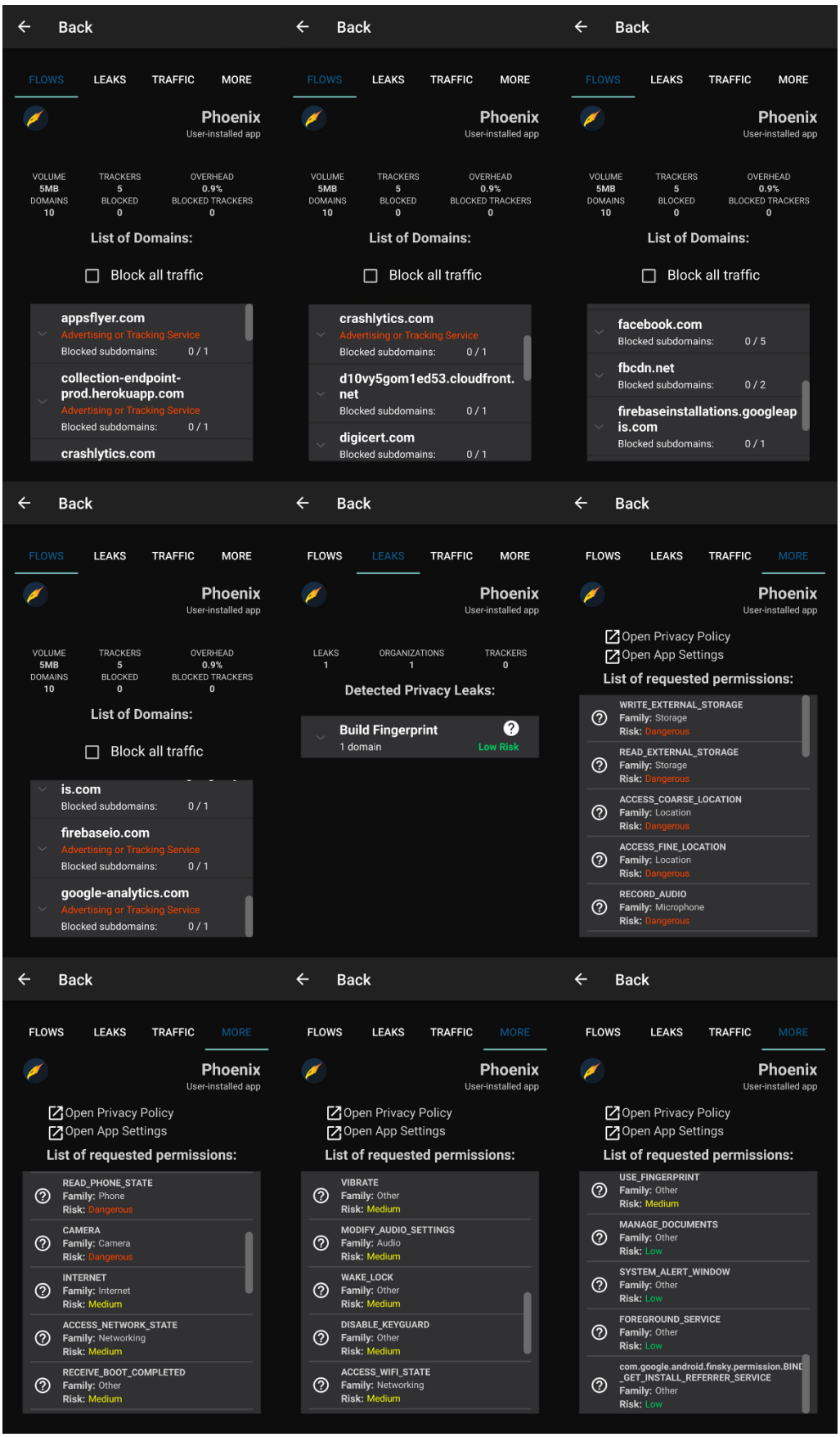
Εικόνα Α.21: Στιγμιότυπο της ανάλυσης της εφαρμογής KakaoTalk



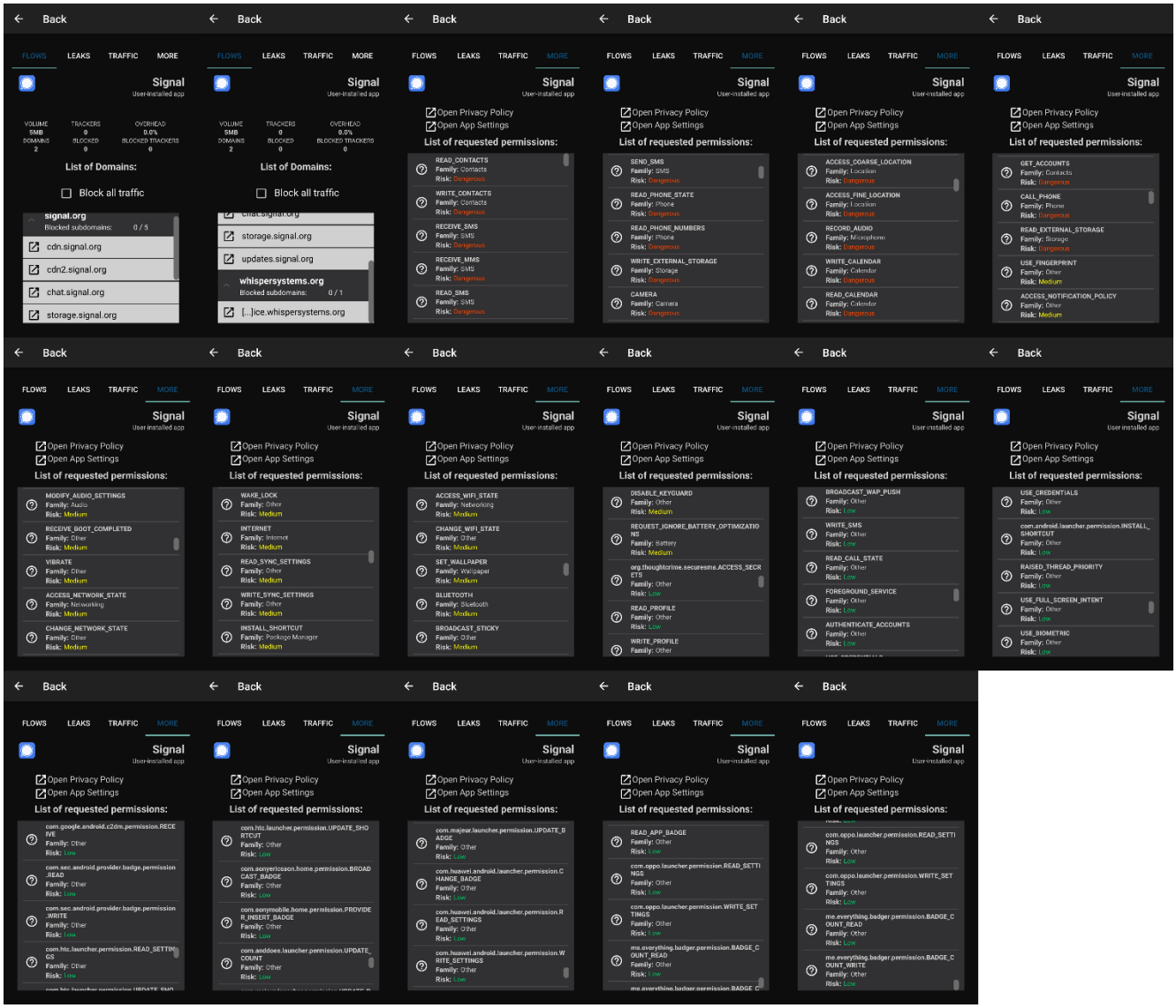
Εικόνα Α.22: Στιγμιότυπο της ανάλυσης της εφαρμογής Line



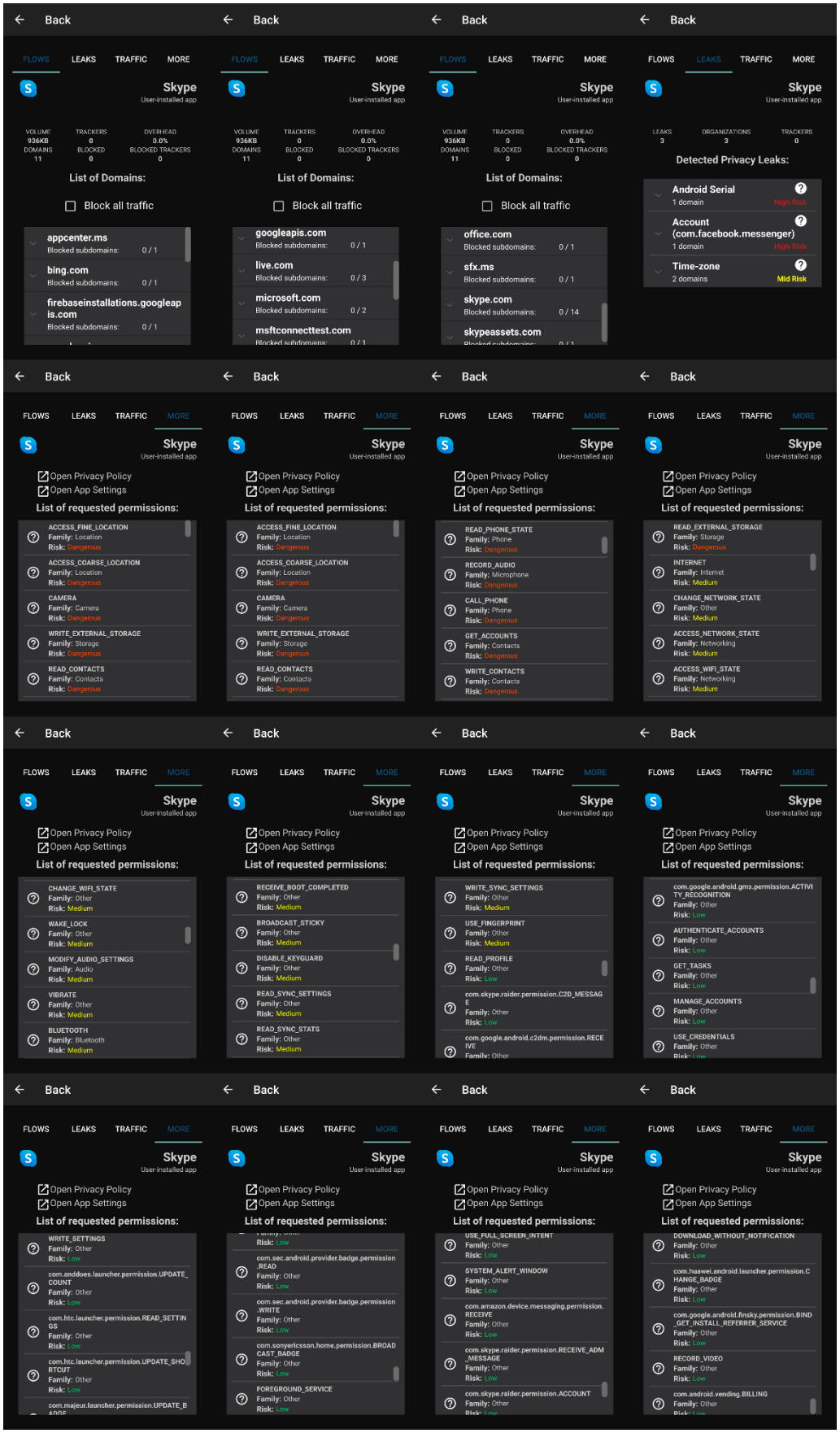
Εικόνα Α.23: Στιγμιότυπο της ανάλυσης της εφαρμογής Messenger



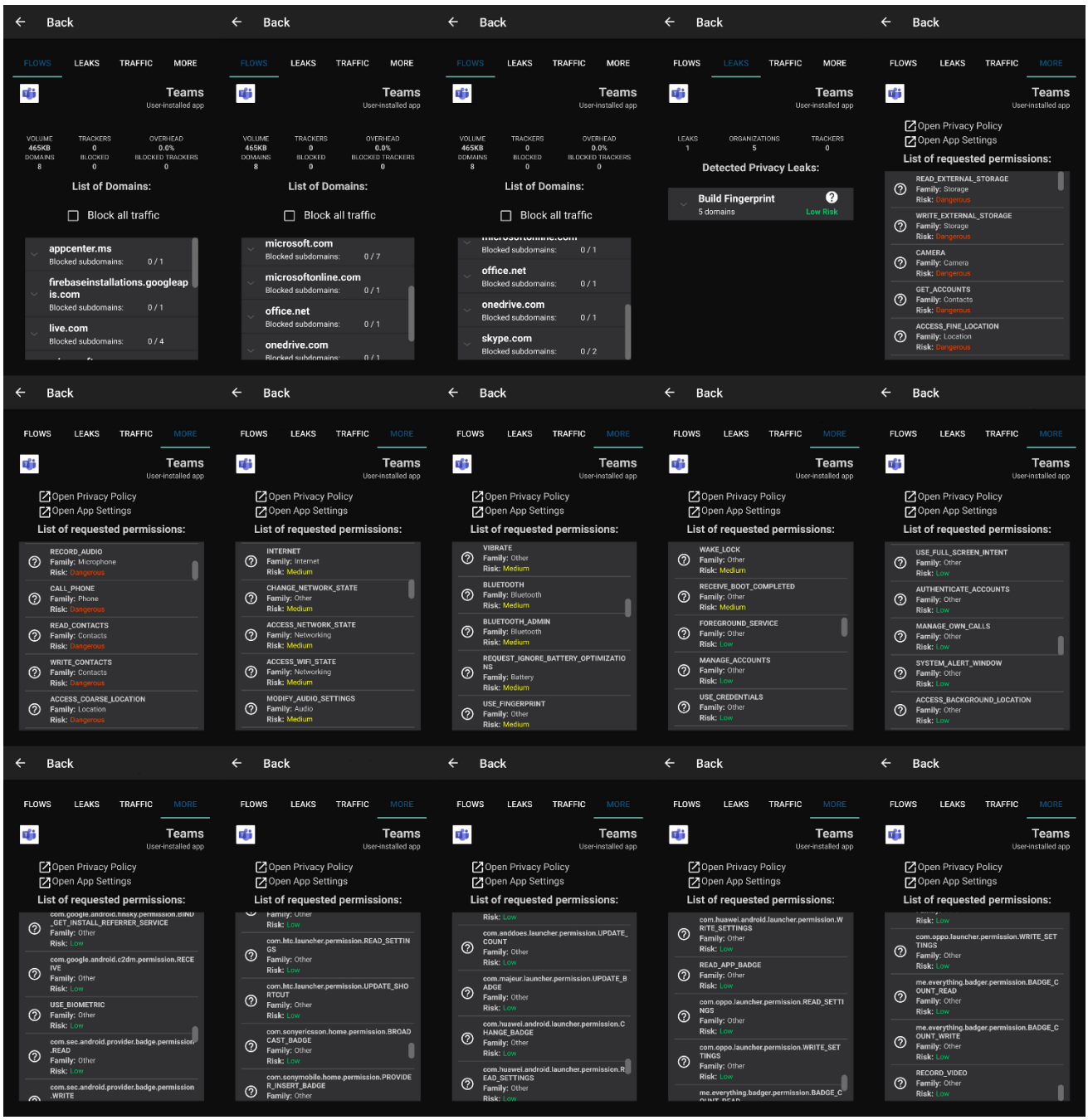
Εικόνα Α.24: Στιγμιότυπο της ανάλυσης της εφαρμογής Phoenix



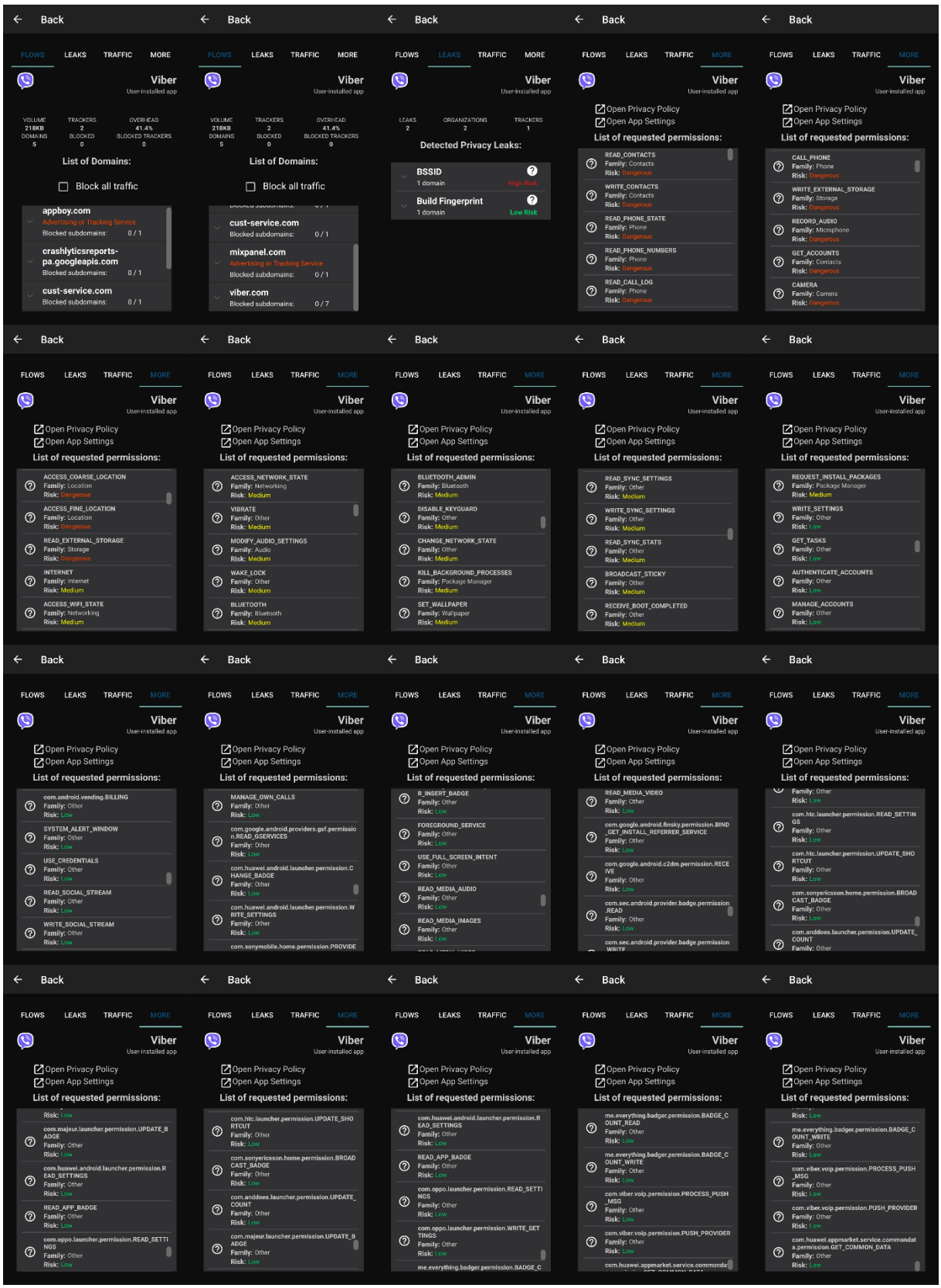
Εικόνα Α.25: Στιγμιότυπο της ανάλυσης της εφαρμογής Signal



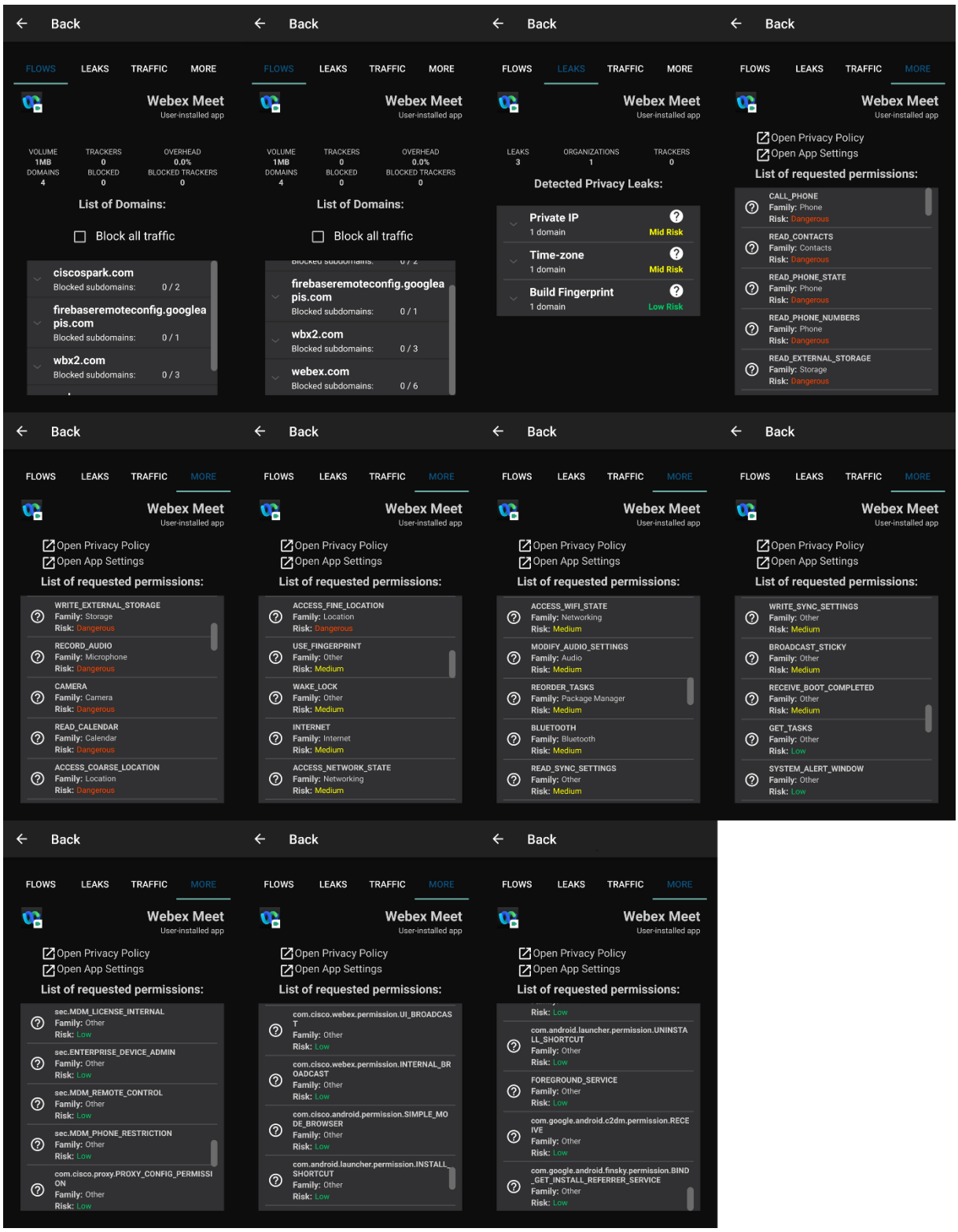
Εικόνα Α.26: Στιγμιότυπο της ανάλυσης της εφαρμογής Skype



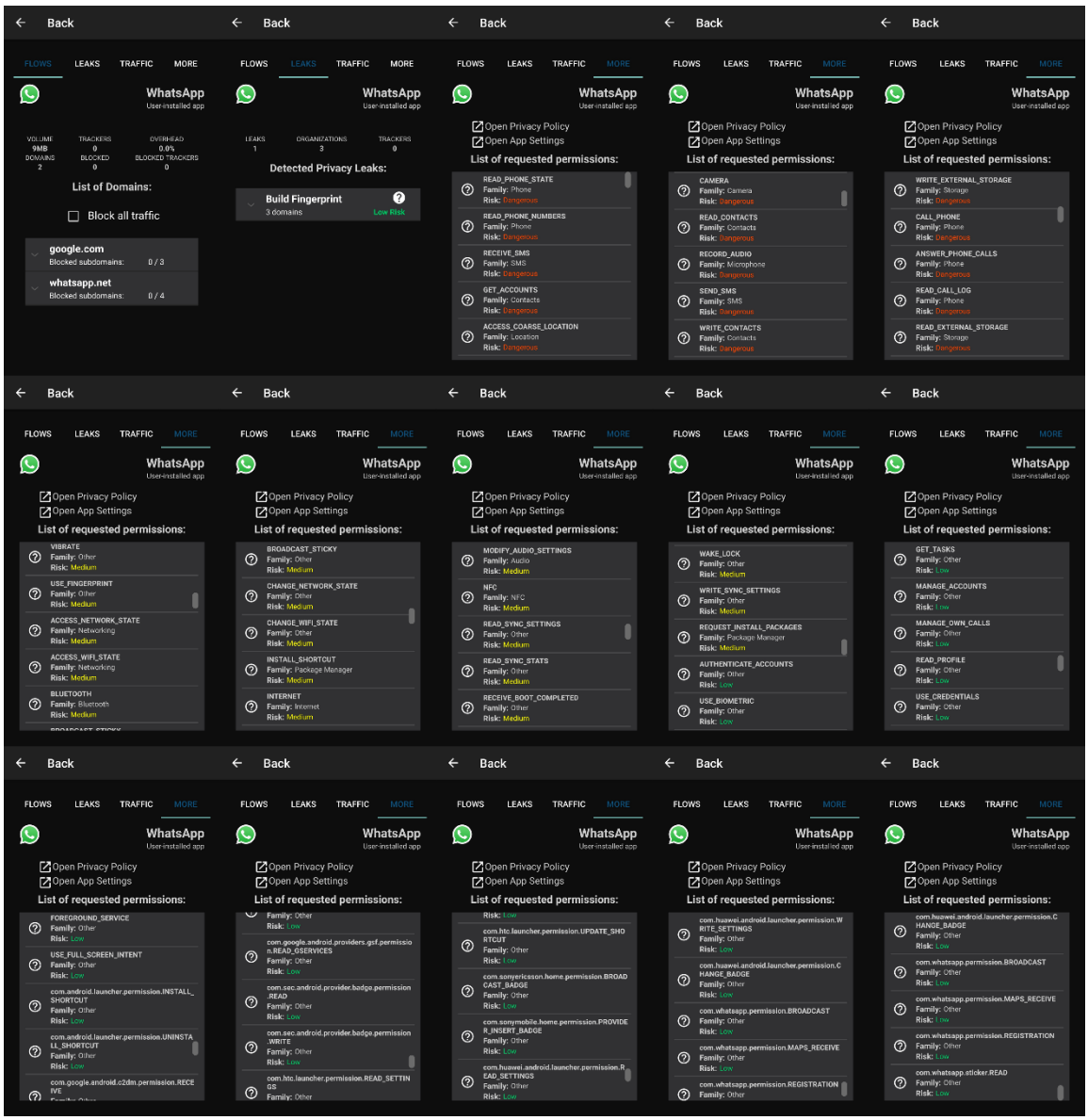
Εικόνα Α.27: Στιγμιότυπο της ανάλυσης της εφαρμογής Teams



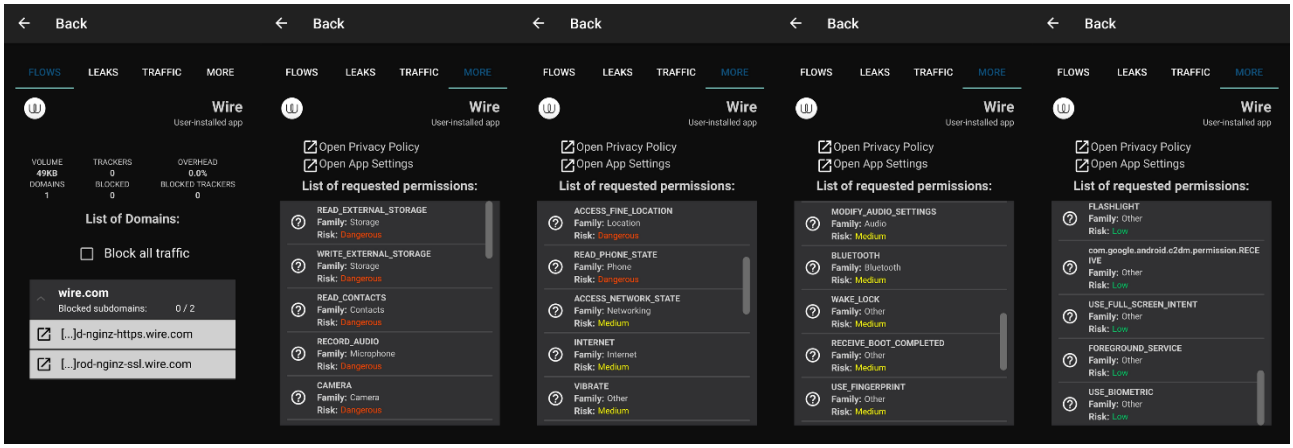
Εικόνα Α.28: Στιγμιότυπο της ανάλυσης της εφαρμογής Viber



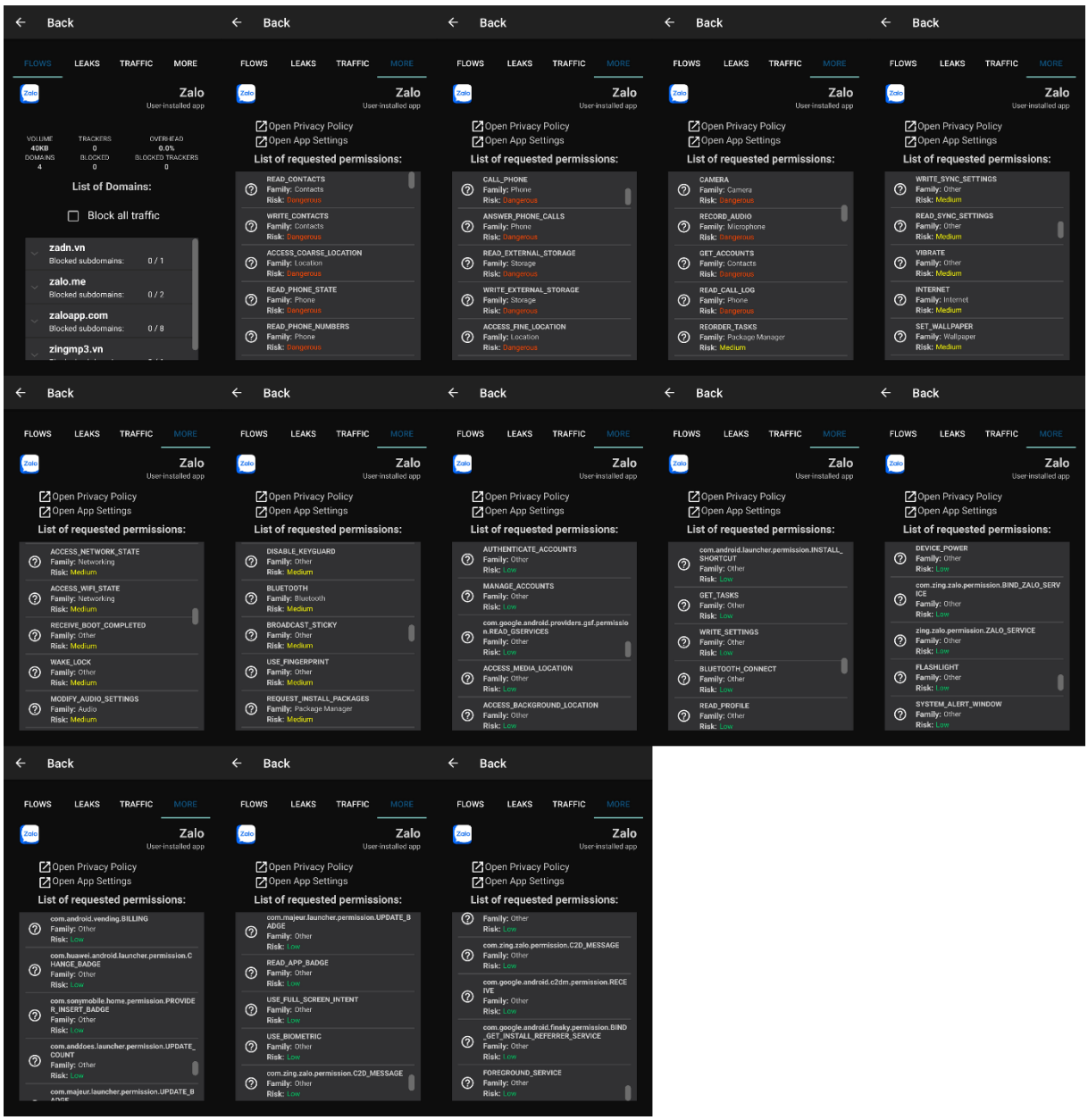
Εικόνα Α.29: Στιγμιότυπο της ανάλυσης της εφαρμογής Webex Meet



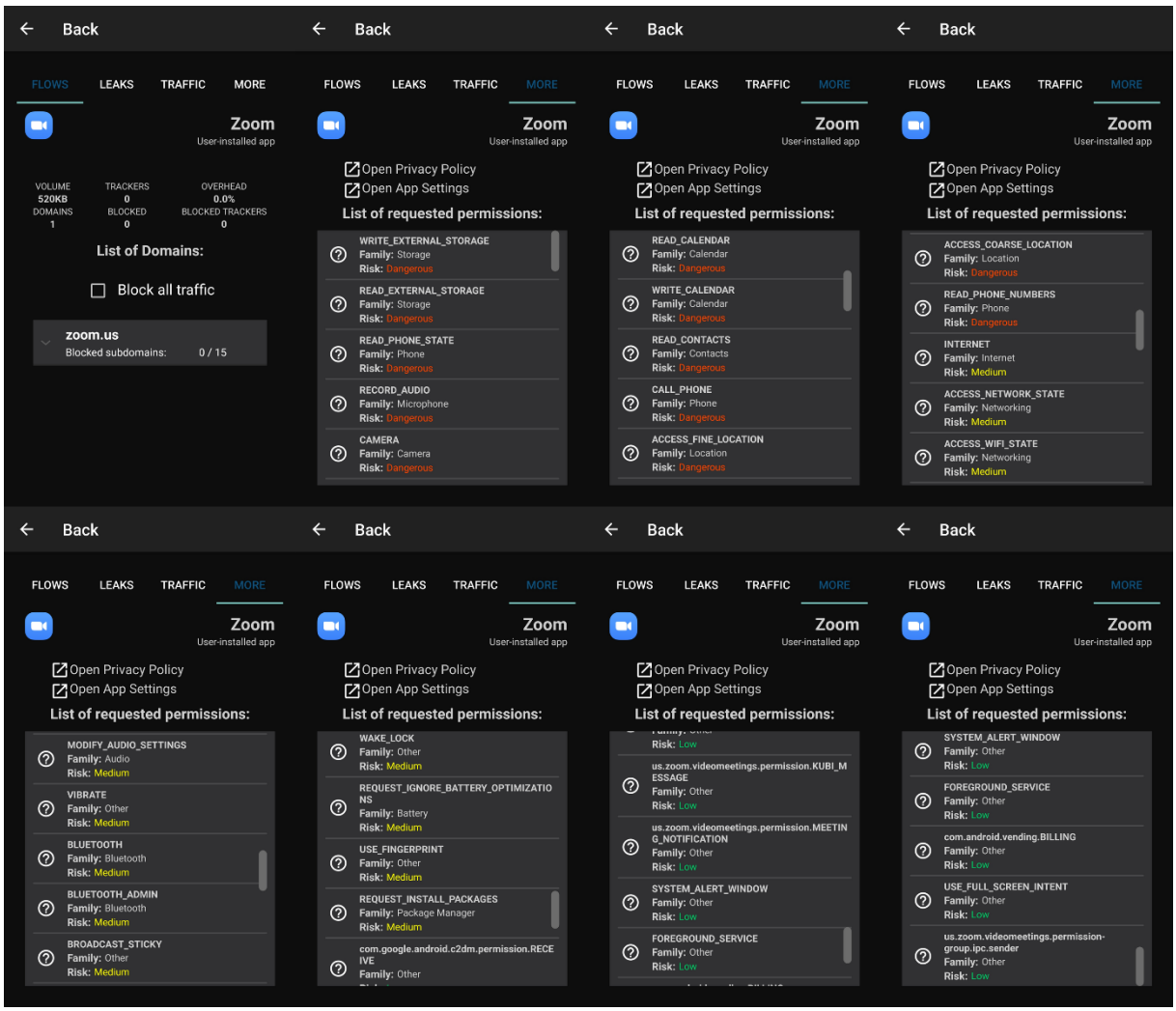
Εικόνα Α.30: Στιγμιότυπο της ανάλυσης της εφαρμογής WhatsApp



Εικόνα Α.31: Στιγμιότυπο της ανάλυσης της εφαρμογής Wire



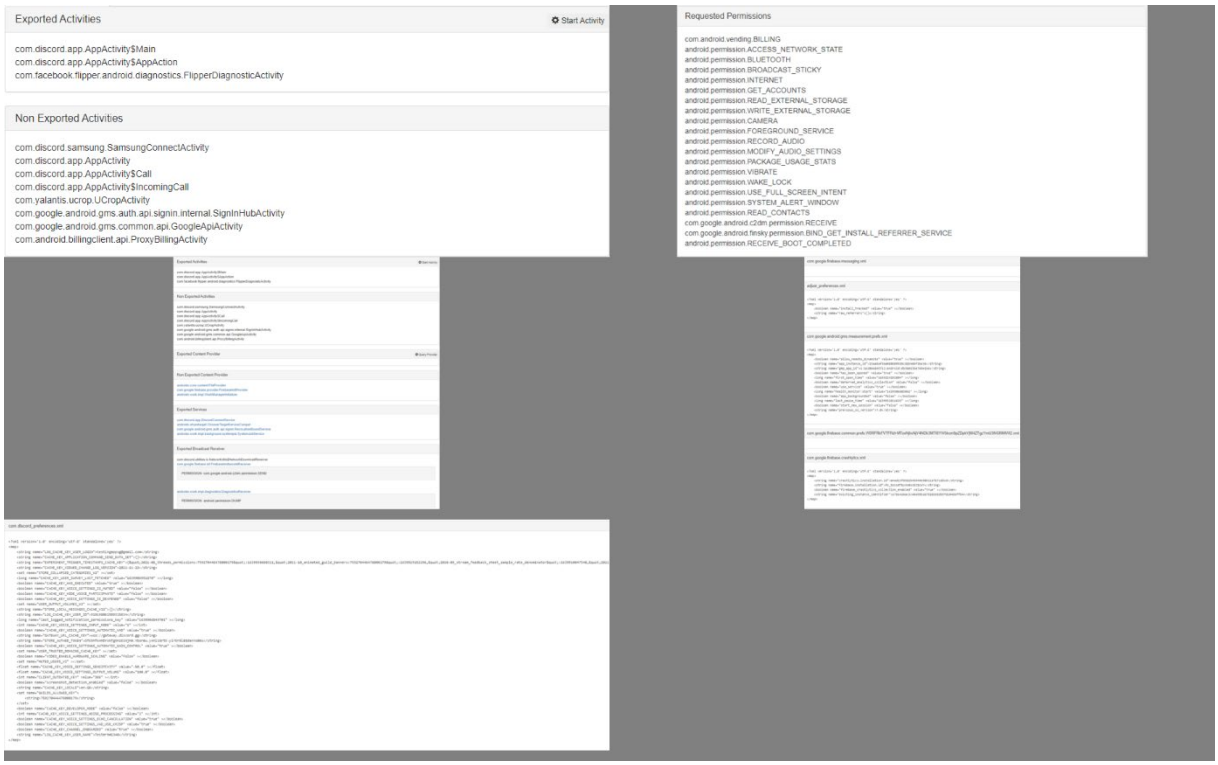
Εικόνα Α.32: Στιγμιότυπο της ανάλυσης της εφαρμογής Zalo



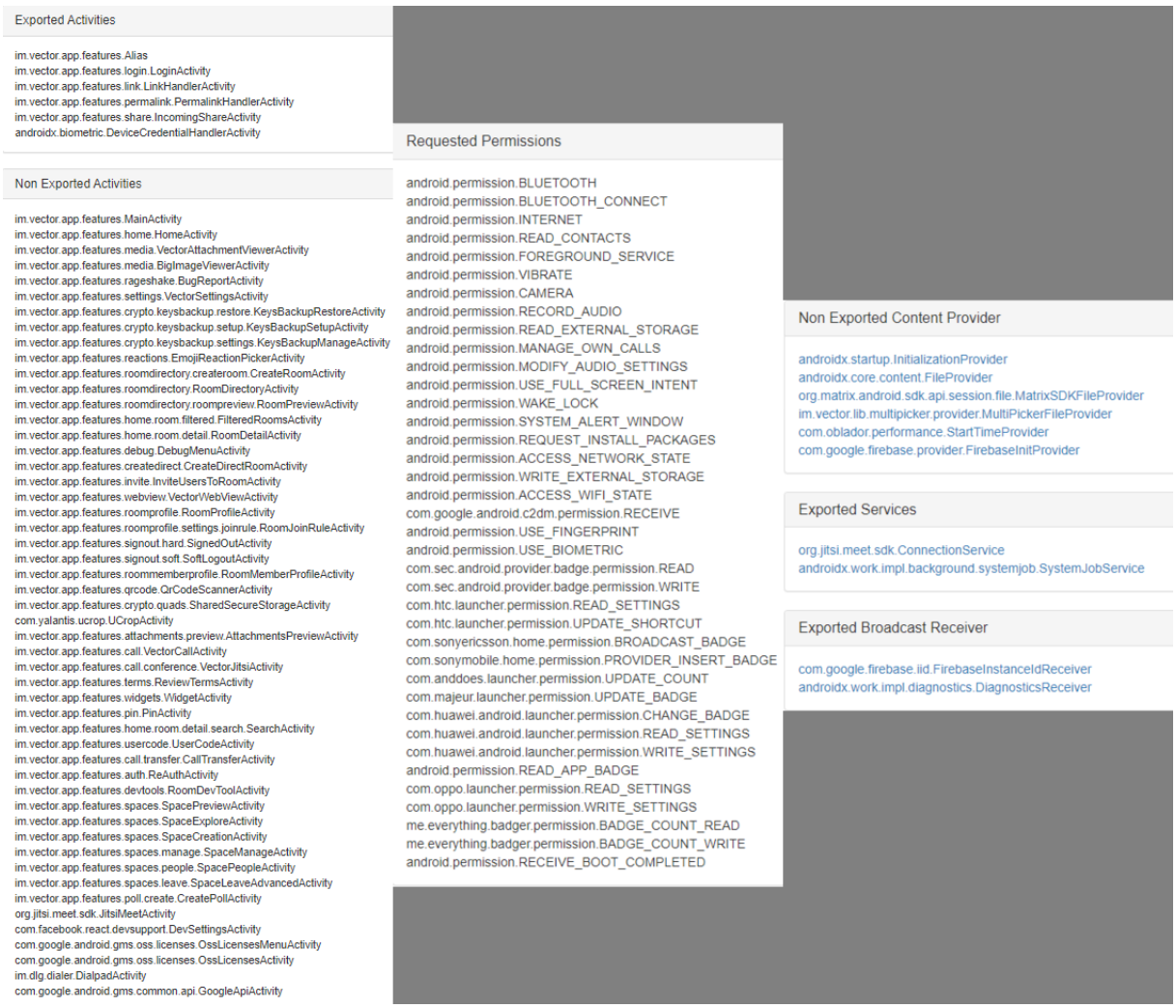
Εικόνα Α.33: Στιγμιότυπο της ανάλυσης της εφαρμογής Zoom

A.3 Inspeckage

Πιο κάτω θα παρουσιαστούν στιγμιότυπα από τη μελέτη των εφαρμογών συνομιλιών/τηλεπικοινωνιών με τη χρήση του εργαλείου Inspeckage.

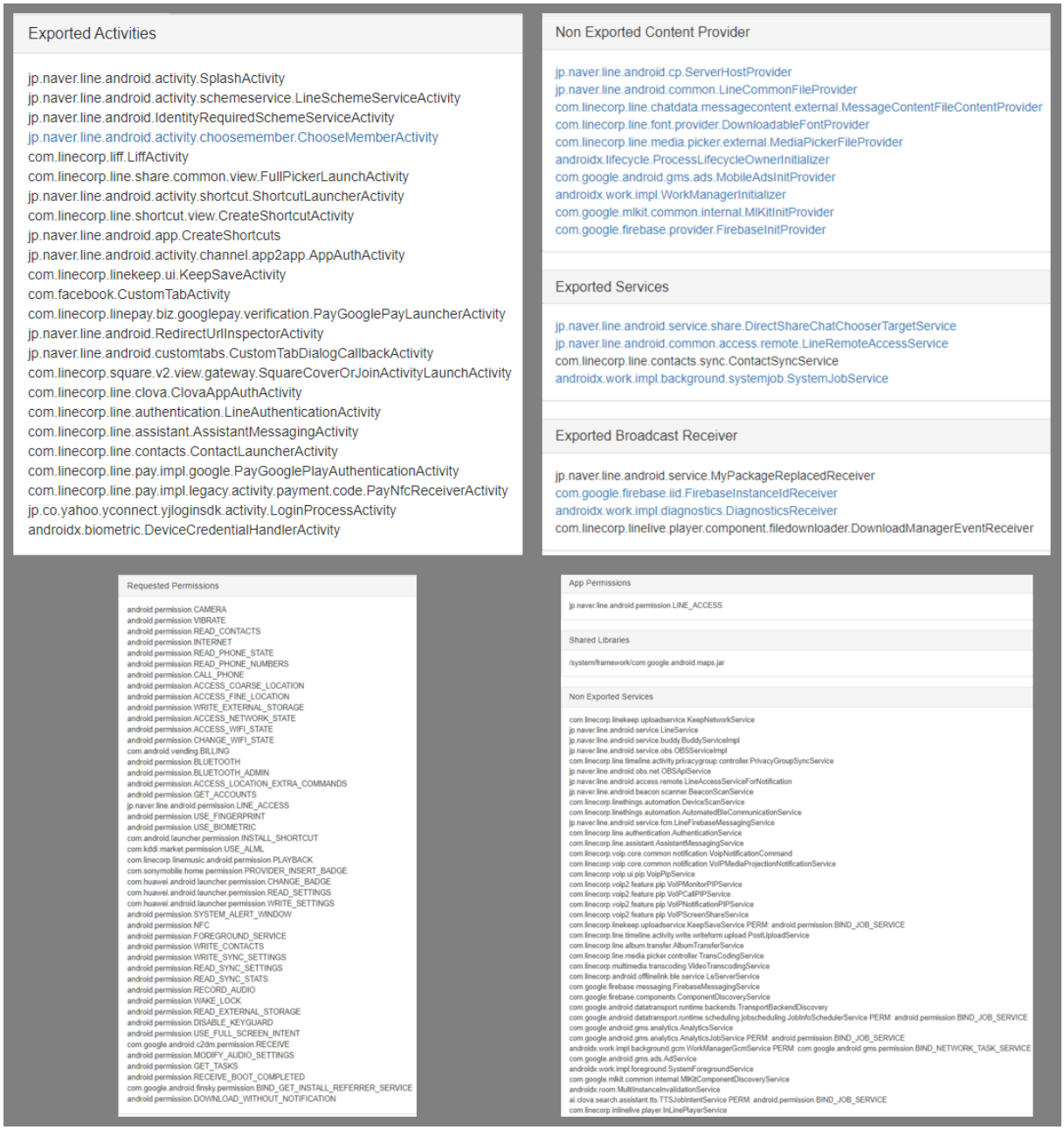


Εικόνα Α.34: Στιγμιότυπο της ανάλυσης της εφαρμογής Discord



Εικόνα Α.35: Στιγμιότυπο της ανάλυσης της εφαρμογής Element

Εικόνα Α.36: Στιγμιότυπο της ανάλυσης της εφαρμογής KakaoTalk



Exported Activities

jp.naver.line.android.activity.SplashActivity
jp.naver.line.android.activity.schemeservice.LineSchemeServiceActivity
jp.naver.line.android.IdentityRequiredSchemeServiceActivity
jp.naver.line.android.activity.choosemember.ChooseMemberActivity
com.linecorp.liff.LiffActivity
com.linecorp.line.share.common.view.FullPickerLaunchActivity
jp.naver.line.android.activity.shortcut.ShortcutLauncherActivity
com.linecorp.line.shortcut.view.CreateShortcutActivity
jp.naver.line.android.app.CreateShortcuts
jp.naver.line.android.activity.channel.app2app.AppAuthActivity
com.linecorp.linekeep.ui.KeepSaveActivity
com.facebook.CustomTabActivity
com.linecorp.linepay.biz.googlepay.verification.PayGooglePayLauncherActivity
jp.naver.line.android.RedirectUrlInspectorActivity
jp.naver.line.android.customtabs.CustomTabDialogCallbackActivity
com.linecorp.square.v2.view.gateway.SquareCoverOrJoinActivityLaunchActivity
com.linecorp.line.clova.ClovaAppAuthActivity
com.linecorp.line.authentication.LineAuthenticationActivity
com.linecorp.line.assistant.AssistantMessagingActivity
com.linecorp.line.contacts.ContactLauncherActivity
com.linecorp.line.pay.impl.google.PayGooglePlayAuthenticationActivity
com.linecorp.line.pay.impl.legacy.activity.payment.code.PayNfcReceiverActivity
jp.co.yahoo.yconnect.yjloginsdk.activity.LoginProcessActivity
androidx.biometric.DeviceCredentialHandlerActivity

Non Exported Content Provider

jp.naver.line.android.cp.ServerHostProvider
jp.naver.line.android.common.LineCommonFileProvider
com.linecorp.line.chatdata.messagecontent.external.MessageContentFileContentProvider
com.linecorp.line.font.provider.DownloadableFontProvider
com.linecorp.line.media.picker.external.MediaPickerFileProvider
androidx.lifecycle.ProcessLifecycleOwnerInitializer
com.google.android.gms.ads.MobileAdsInitProvider
androidx.work.impl.WorkManagerInitializer
com.google.mlkit.common.internal.MlKitInitProvider
com.google.firebase.provider.FirebaseInitProvider

Exported Services

jp.naver.line.android.service.share.DirectShareChatChooserTargetService
jp.naver.line.android.common.access.remote.LineRemoteAccessService
com.linecorp.line.contacts.sync.ContactSyncService
androidx.work.impl.background.systemjob.SystemJobService

Exported Broadcast Receiver

jp.naver.line.android.service.MyPackageReplacedReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver
com.linecorp.linelive.player.component.filedownloader.DownloadManagerEventReceiver

Requested Permissions

android.permission.CAMERA
android.permission.VIBRATE
android.permission.READ_CONTACTS
android.permission.INTERNET
android.permission.READ_PHONE_STATE
android.permission.READ_PHONE_NUMBERS
android.permission.CALL_PHONE
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.CHANGE_WIFI_STATE
com.android.vending.BILLING
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS
android.permission.GET_ACCOUNTS
jp.naver.line.android.permission.LINE_ACCESS
android.permission.USE_FINGERPRINT
android.permission.USE_BIOMETRIC
com.android.launcher.permission.INSTALL_SHORTCUT
com.kddi.market.permission.USE_ALML
com.linecorp.linemusic.android.permission.PLAYBACK
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE
com.huawei.android.launcher.permission.CHANGE_BADGE
com.huawei.android.launcher.permission.READ_SETTINGS
com.huawei.android.launcher.permission.WRITE_SETTINGS
android.permission.SYSTEM_ALERT_WINDOW
android.permission.NFC
android.permission.FOREGROUND_SERVICE
android.permission.WRITE_CONTACTS
android.permission.WRITE_SYNC_SETTINGS
android.permission.READ_SYNC_SETTINGS
android.permission.READ_SYNC_STATS
android.permission.RECORD_AUDIO
android.permission.WAKE_LOCK
android.permission.READ_EXTERNAL_STORAGE
android.permission.DISABLE_KEYGUARD
android.permission.USE_FULL_SCREEN_INTENT
com.google.android.c2dm.permission.RECEIVE
android.permission.MODIFY_AUDIO_SETTINGS
android.permission.GET_TASKS
android.permission.RECEIVE_BOOT_COMPLETED
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION

App Permissions

jp.naver.line.android.permission.LINE_ACCESS

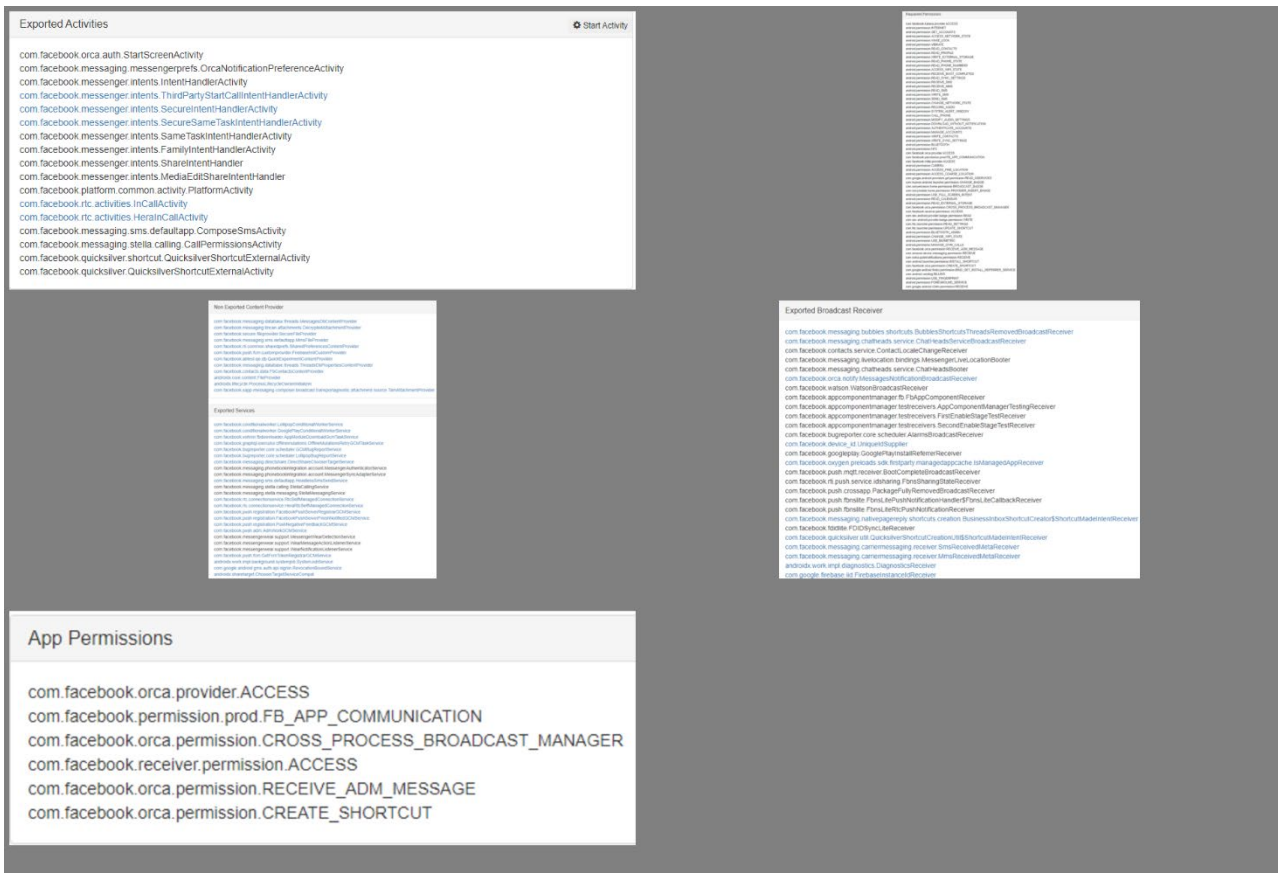
Shared Libraries

/system/framework/com.google.android.maps.jar

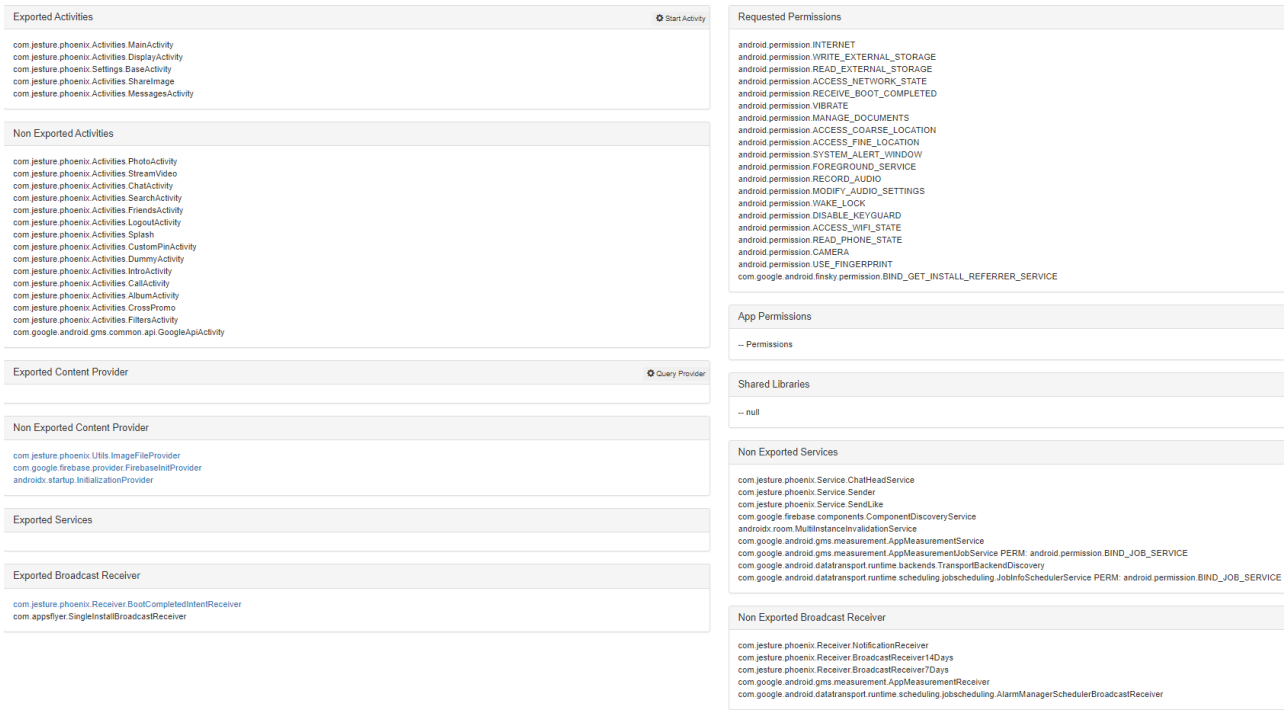
Non Exported Services

com.linecorp.linekeep.uploadservice.KeepNetworkService
jp.naver.line.android.service.LineService
jp.naver.line.android.service.buddy.BuddyServiceImpl
jp.naver.line.android.service.obs.OBSServiceImpl
com.linecorp.line.timeline.activity.privacygroup.controller.PrivacyGroupSyncService
jp.naver.line.android.obs.net.OBSApiService
jp.naver.line.android.access.remote.LineAccessServiceForNotification
jp.naver.line.android.beacon.scanner.BeaconScanService
com.linecorp.linethings.automation.DeviceScanService
com.linecorp.linethings.automation.AutomatedBleCommunicationService
jp.naver.line.android.service.fcm.LineFirebaseMessagingService
com.linecorp.line.authentication.AuthenticationService
com.linecorp.line.assistant.AssistantMessagingService
com.linecorp.voip.core.common.notification.VoipNotificationCommand
com.linecorp.voip.core.common.notification.VoIPMediaProjectionNotificationService
com.linecorp.voip.ui.pip.VoipPipService
com.linecorp.voip2.feature.pip.VoIPMonitorPIPService
com.linecorp.voip2.feature.pip.VoIPCallPIPService
com.linecorp.voip2.feature.pip.VoIPNotificationPIPService
com.linecorp.voip2.feature.pip.VoIPScreenShareService
com.linecorp.linekeep.uploadservice.KeepSaveService PERM: android.permission.BIND_JOB_SERVICE
com.linecorp.line.timeline.activity.write.writeform.upload.PostUploadService
com.linecorp.line.album.transfer.AlbumTransferService
com.linecorp.line.media.picker.controller.TransCodingService
com.linecorp.multimedia.transcoding.VideoTranscodingService
com.linecorp.android.offlinelink.ble.service.LeServerService
com.google.firebase.messaging.FirebaseMessagingService
com.google.firebase.components.ComponentDiscoveryService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService PERM: android.permission.BIND_JOB_SERVICE
com.google.android.gms.analytics.AnalyticsService
com.google.android.gms.analytics.AnalyticsJobService PERM: android.permission.BIND_JOB_SERVICE
androidx.work.impl.background.gcm.WorkManagerGcmService PERM: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE
com.google.android.gms.ads.AdService
androidx.work.impl.foreground.SystemForegroundService
com.google.mlkit.common.internal.MlKitComponentDiscoveryService
androidx.room.MultiInstanceInvalidationService
ai.clova.search.assistant.tts.TTSJobIntentService PERM: android.permission.BIND_JOB_SERVICE
com.linecorp.linelive.player.InLinePlayerService

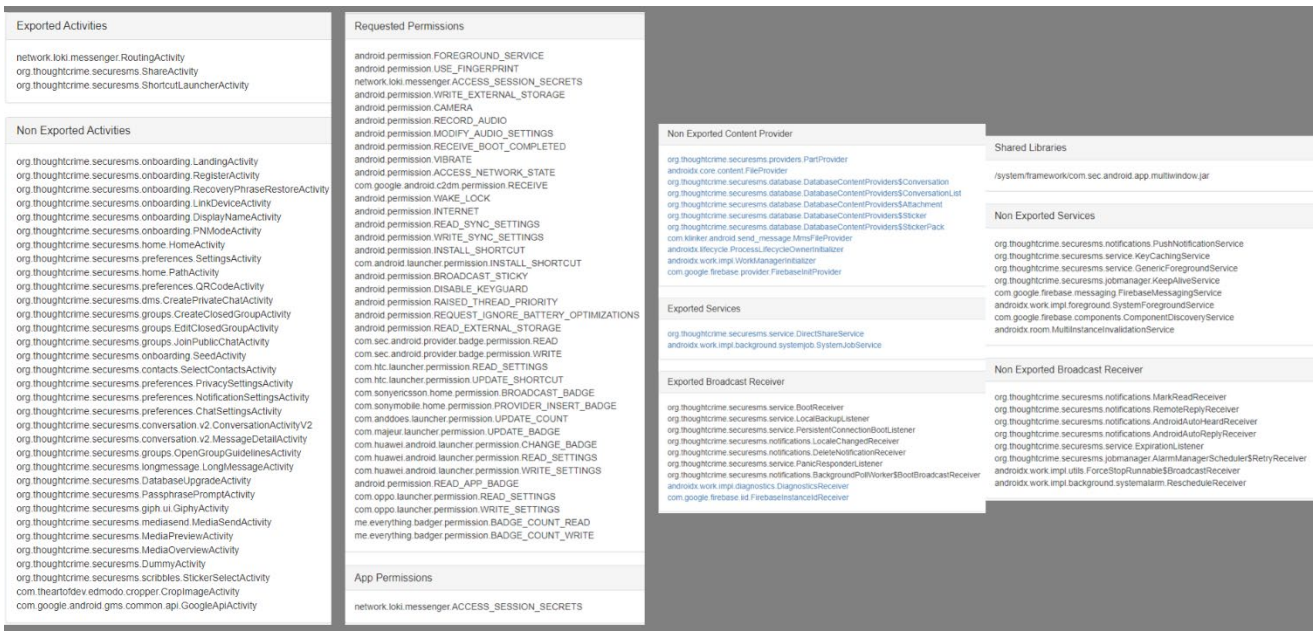
Εικόνα Α.37: Στιγμιότυπο της ανάλυσης της εφαρμογής Line



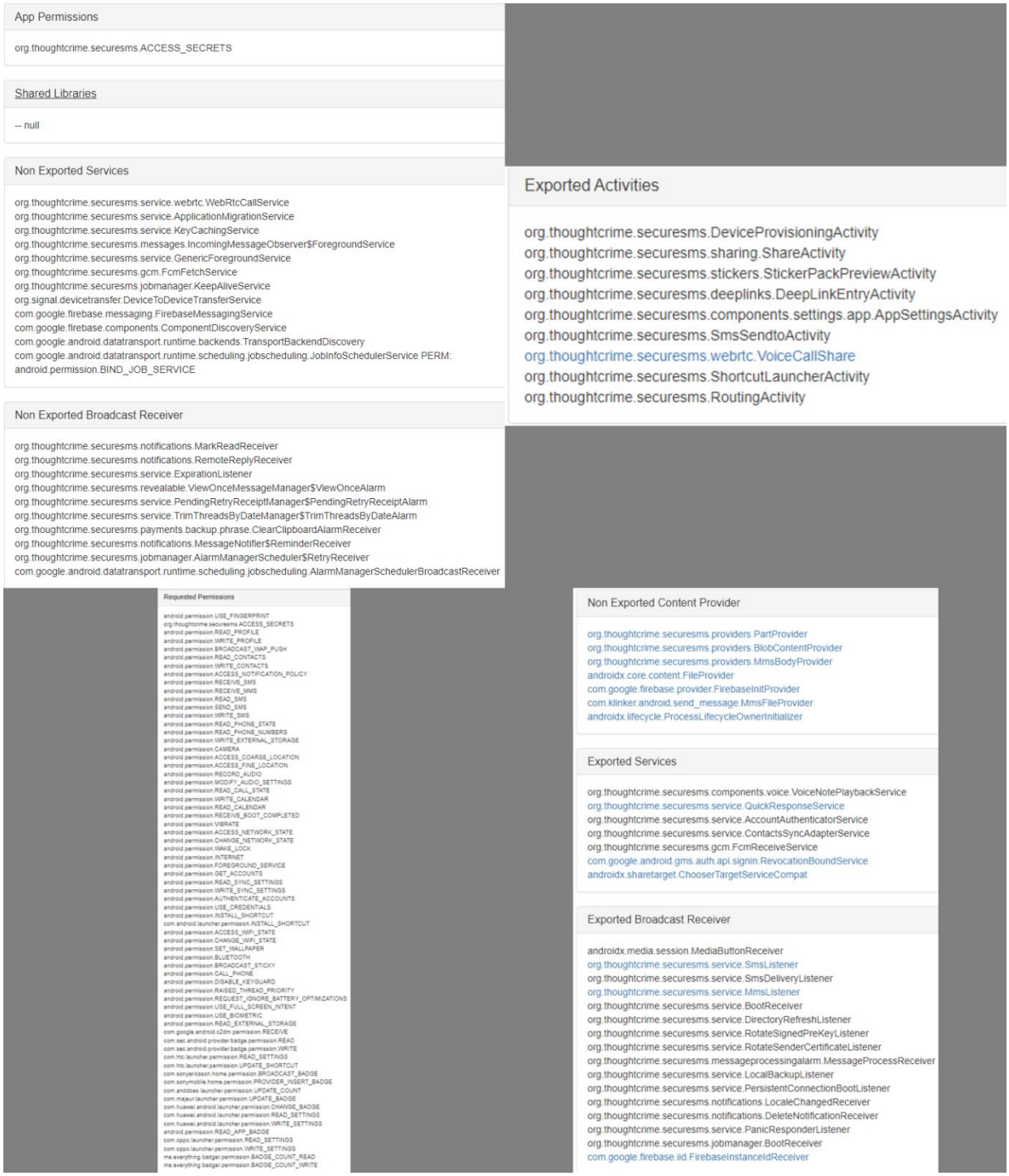
Εικόνα Α.38: Στιγμιότυπο της ανάλυσης της εφαρμογής Messenger



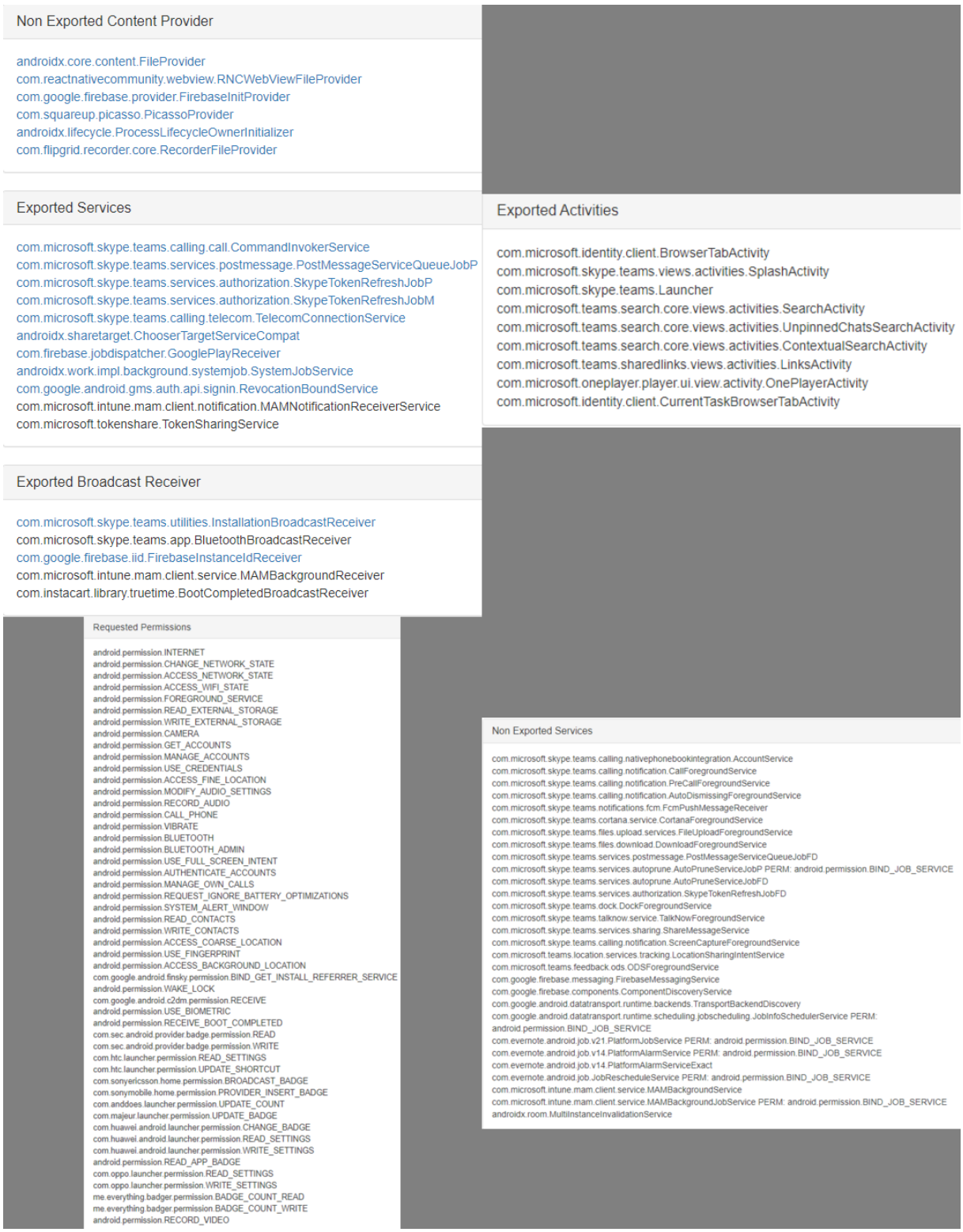
Εικόνα Α.39: Στιγμιότυπο της ανάλυσης της εφαρμογής Phoenix



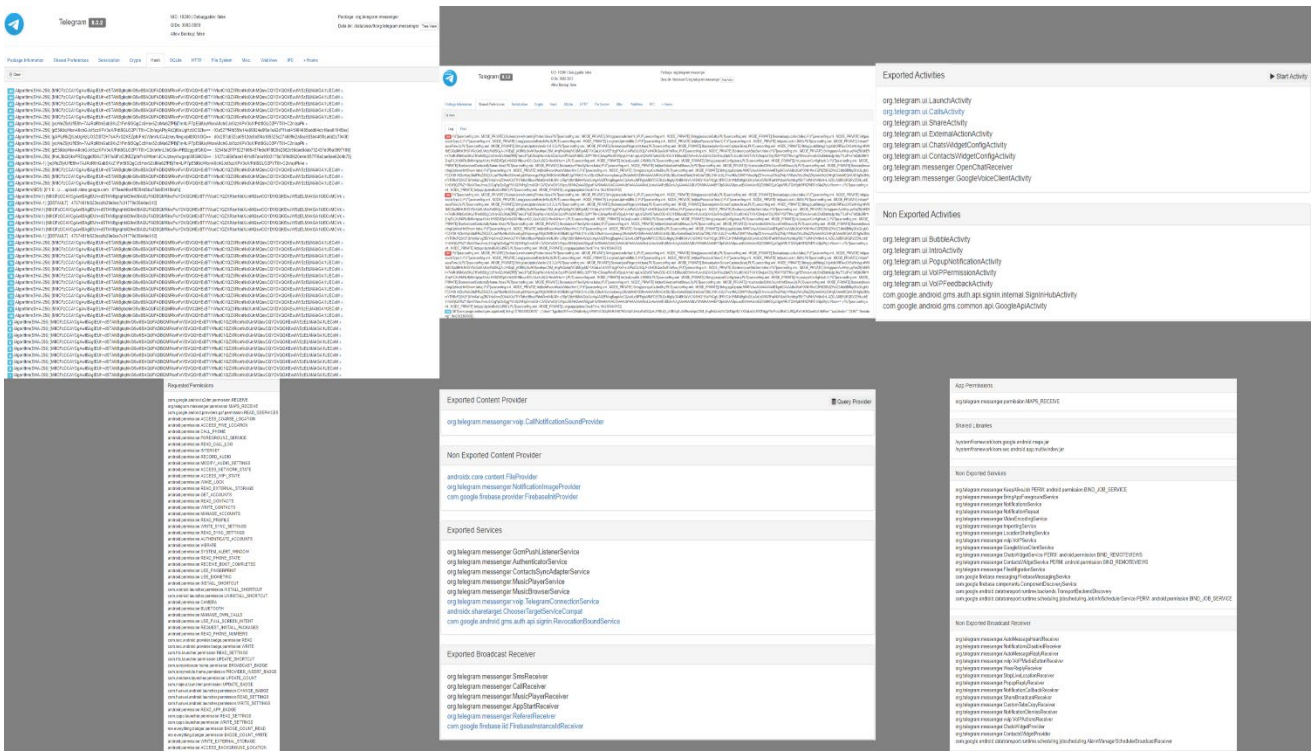
Εικόνα Α.40: Στιγμιότυπο της ανάλυσης της εφαρμογής Session



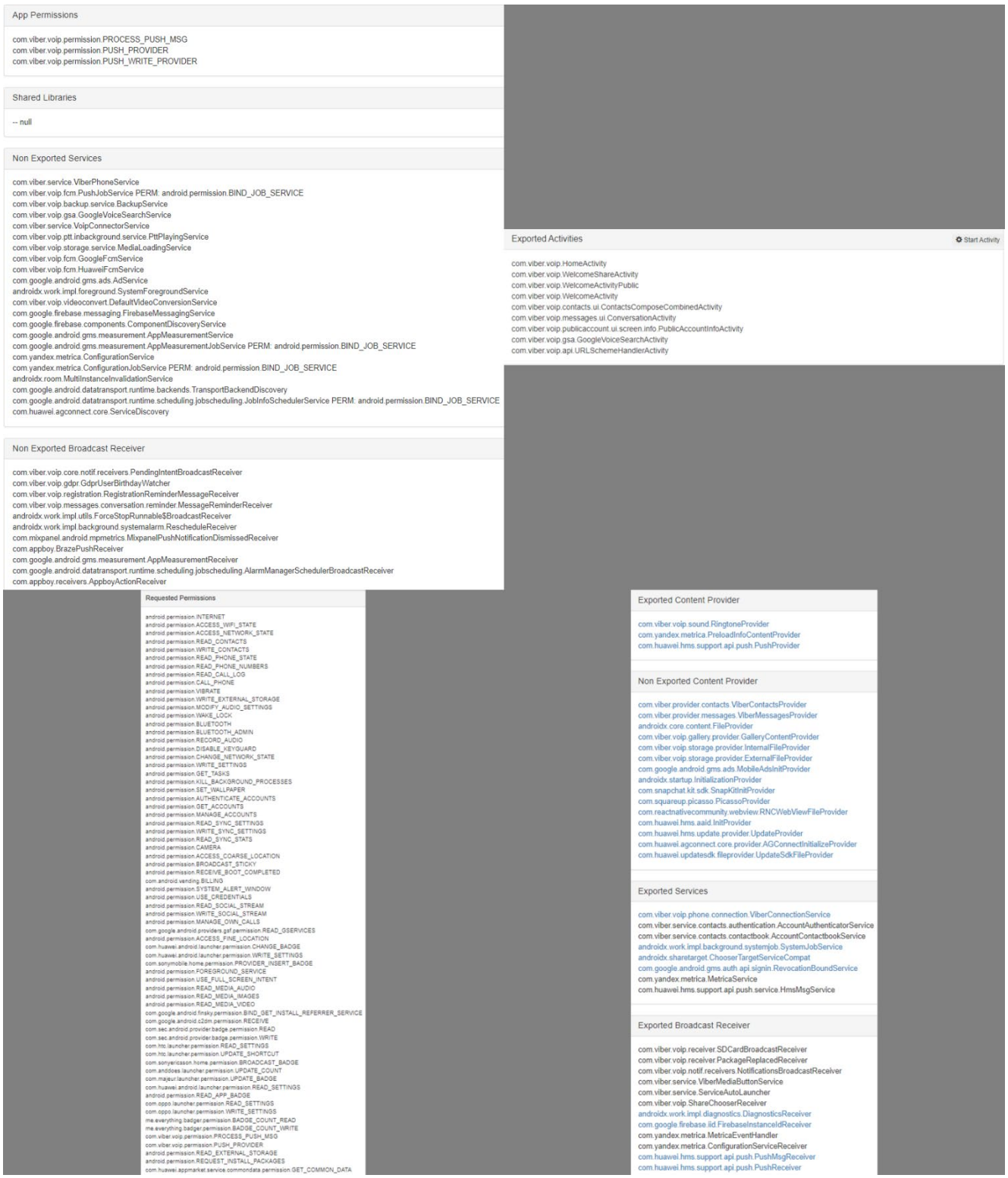
Εικόνα Α.41: Στιγμιότυπο της ανάλυσης της εφαρμογής Signal



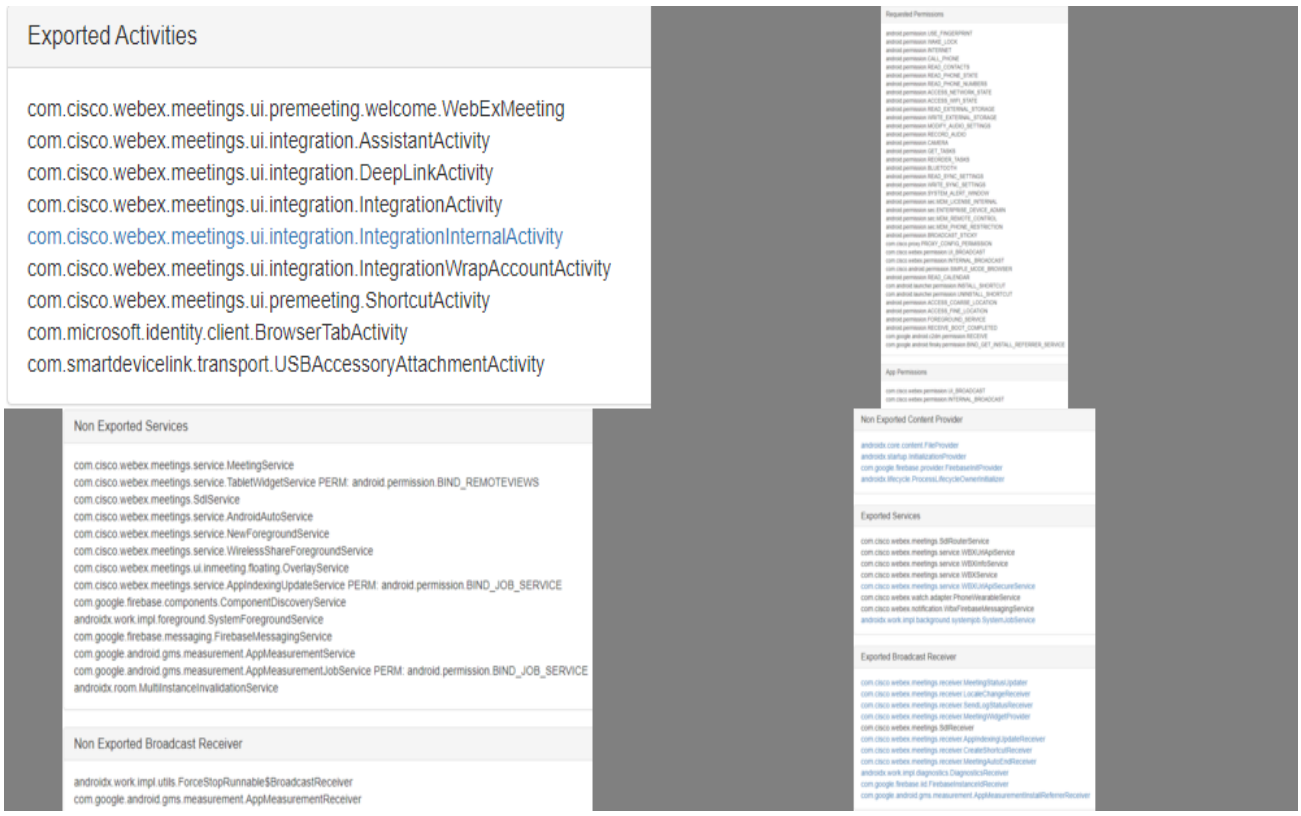
Εικόνα Α.42: Στιγμιότυπο της ανάλυσης της εφαρμογής Teams



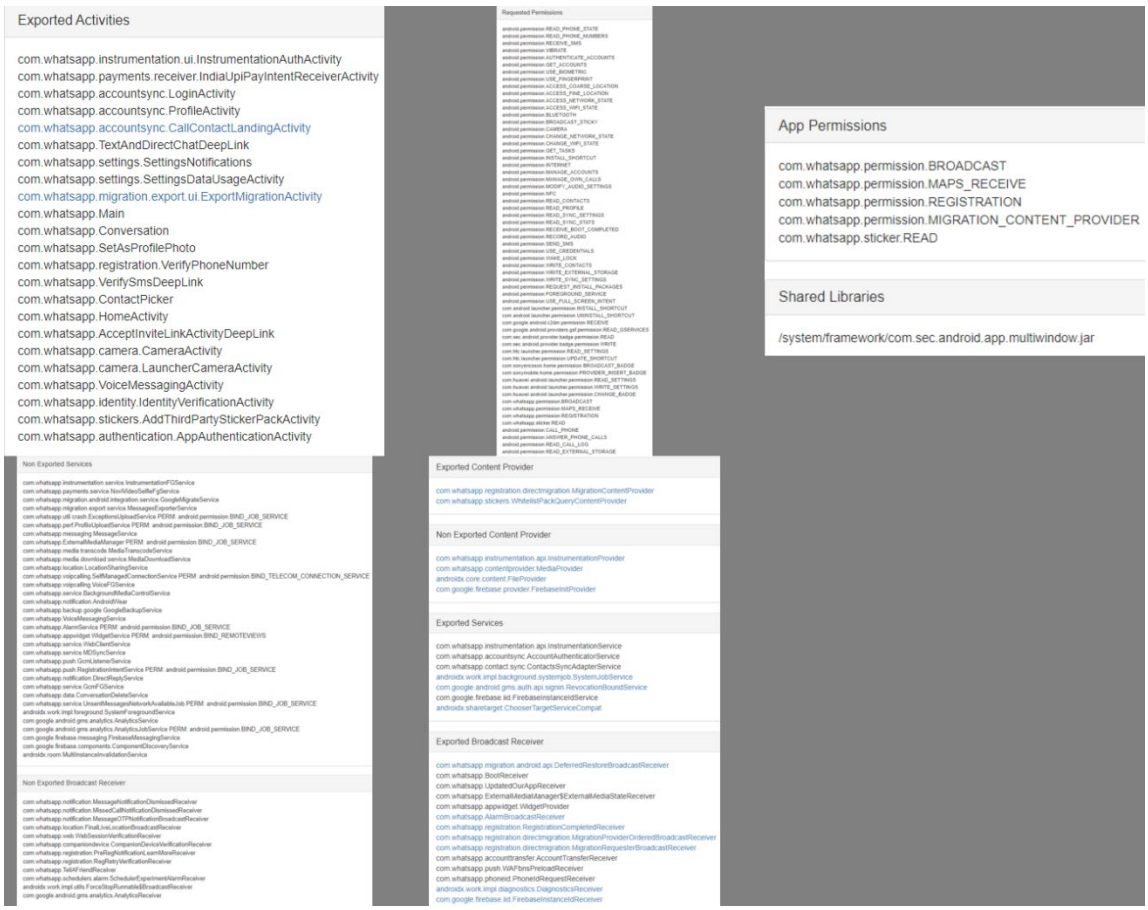
Εικόνα Α.43: Στιγμιότυπο της ανάλυσης της εφαρμογής Telegram



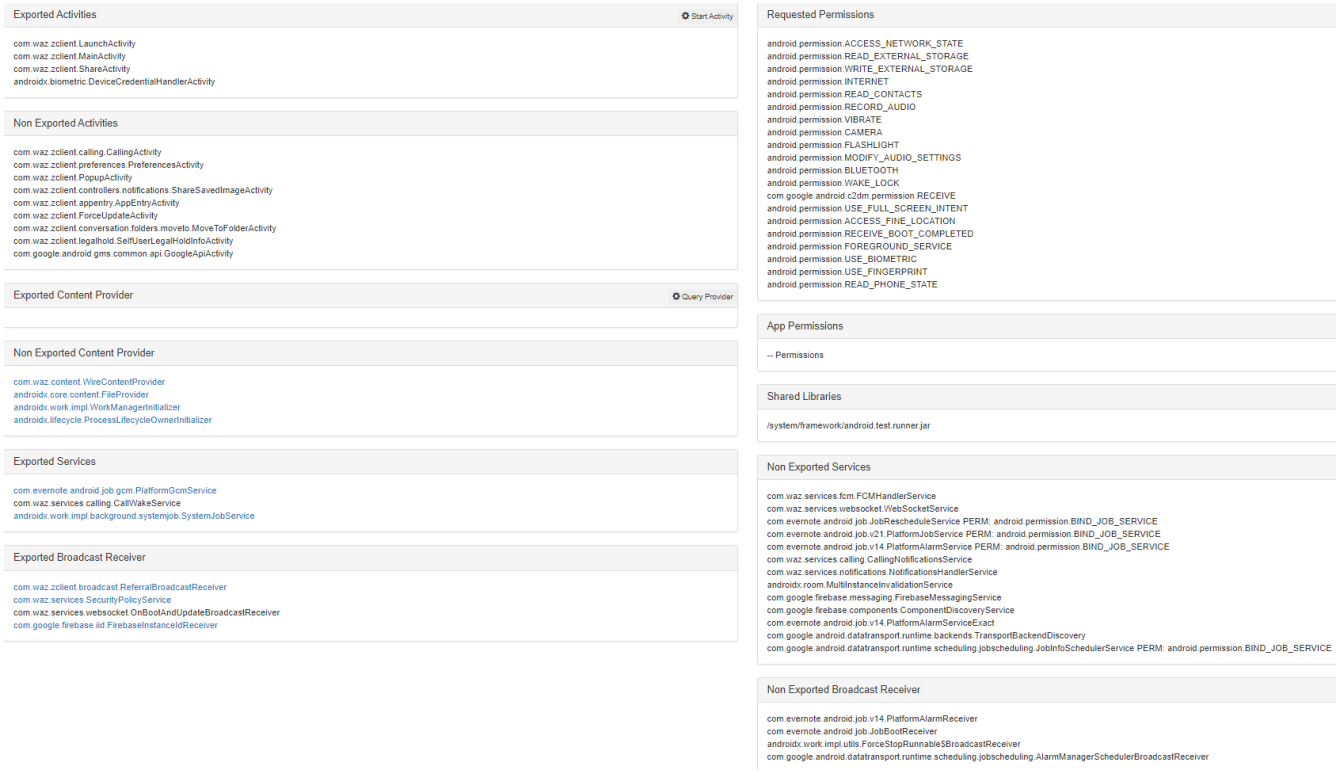
Εικόνα Α.44: Στιγμιότυπο της ανάλυσης της εφαρμογής Viber



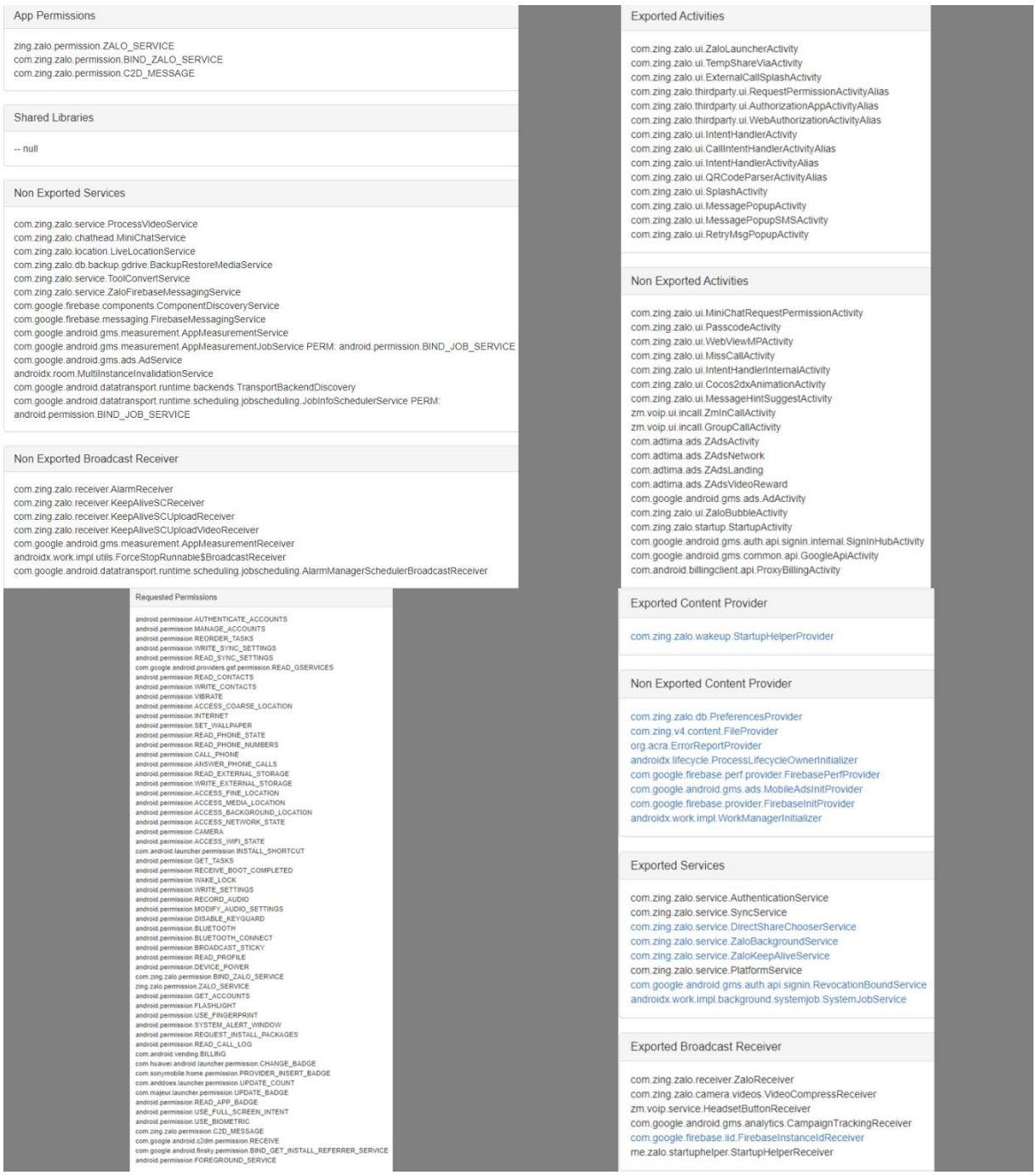
Εικόνα Α.45: Στιγμιότυπο της ανάλυσης της εφαρμογής Webex Meet



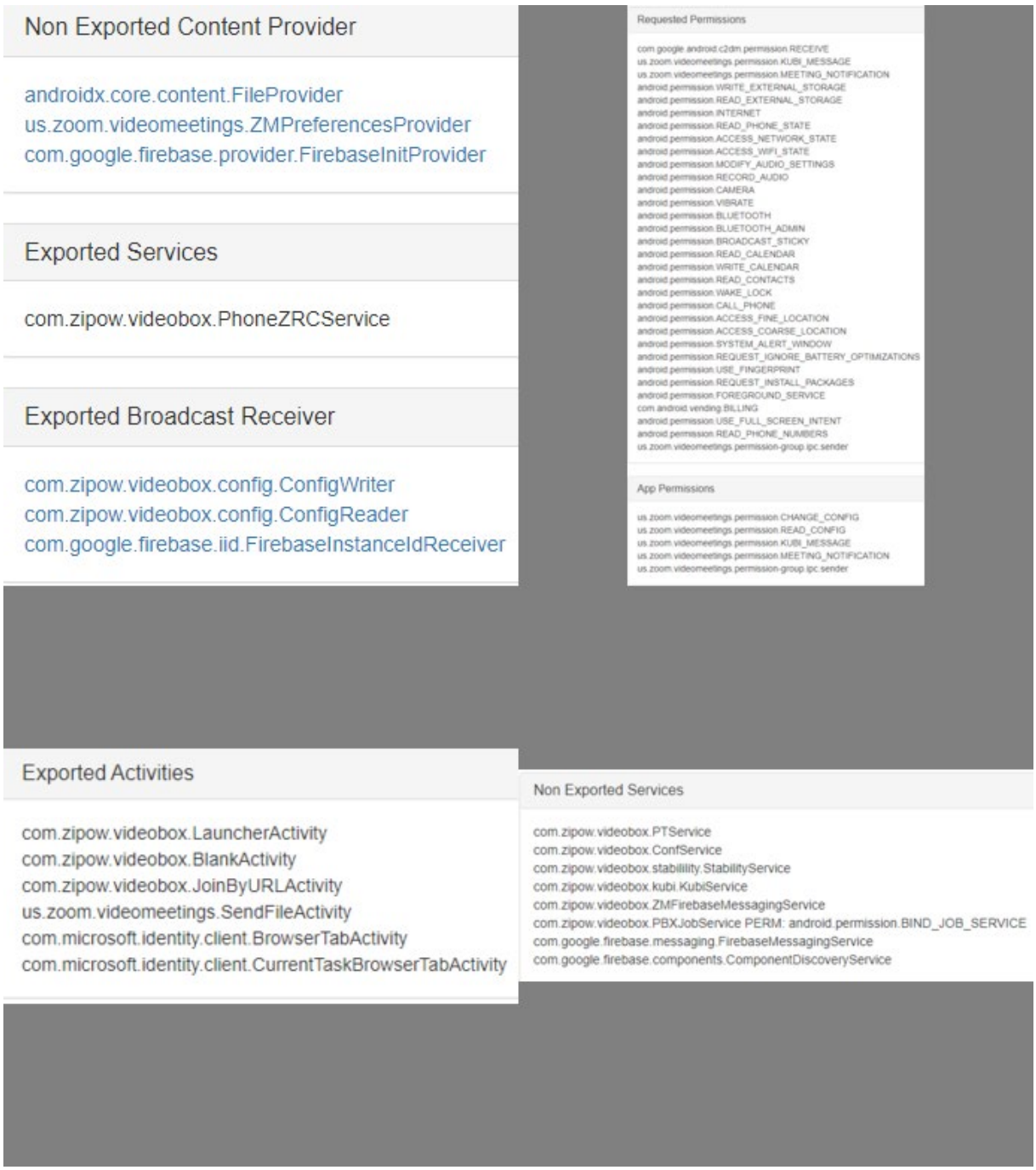
Εικόνα Α.46: Στιγμιότυπο της ανάλυσης της εφαρμογής WhatsApp



Εικόνα Α.47: Στιγμιότυπο της ανάλυσης της εφαρμογής Wire



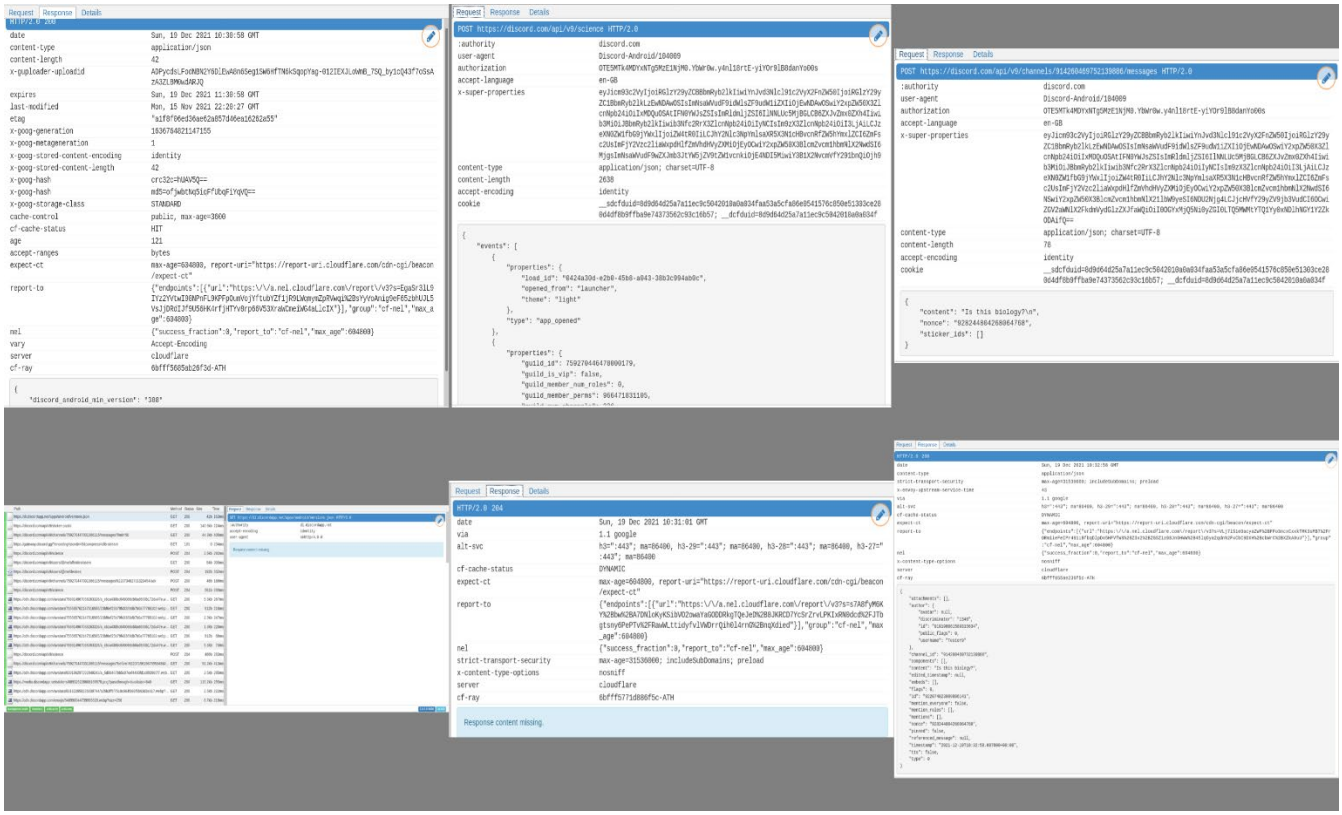
Εικόνα Α.48: Στιγμιότυπο της ανάλυσης της εφαρμογής Zalo



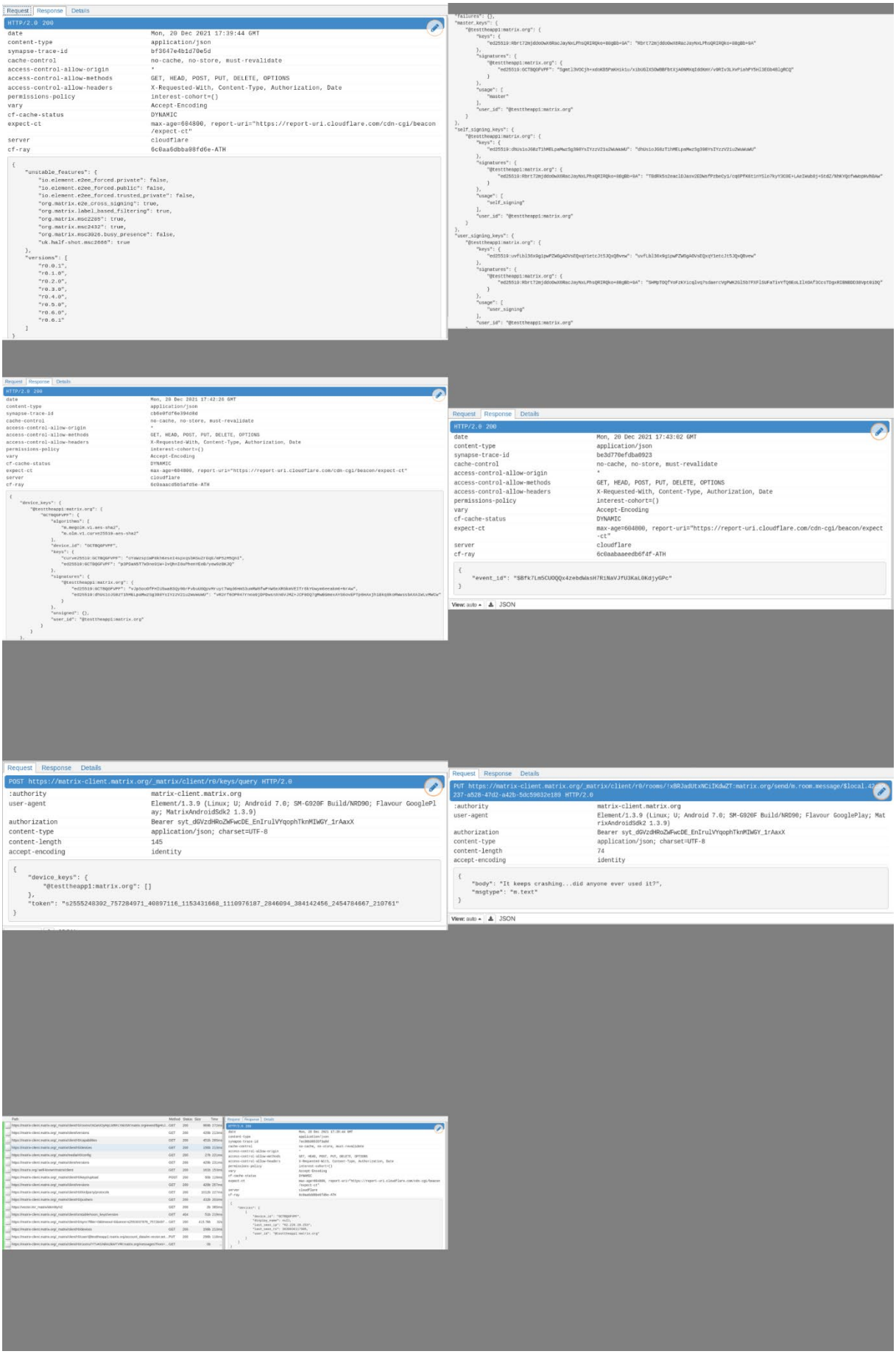
Εικόνα Α.49: Στιγμιότυπο της ανάλυσης της εφαρμογής Zoom

A.4 Privacy International's data interception environment

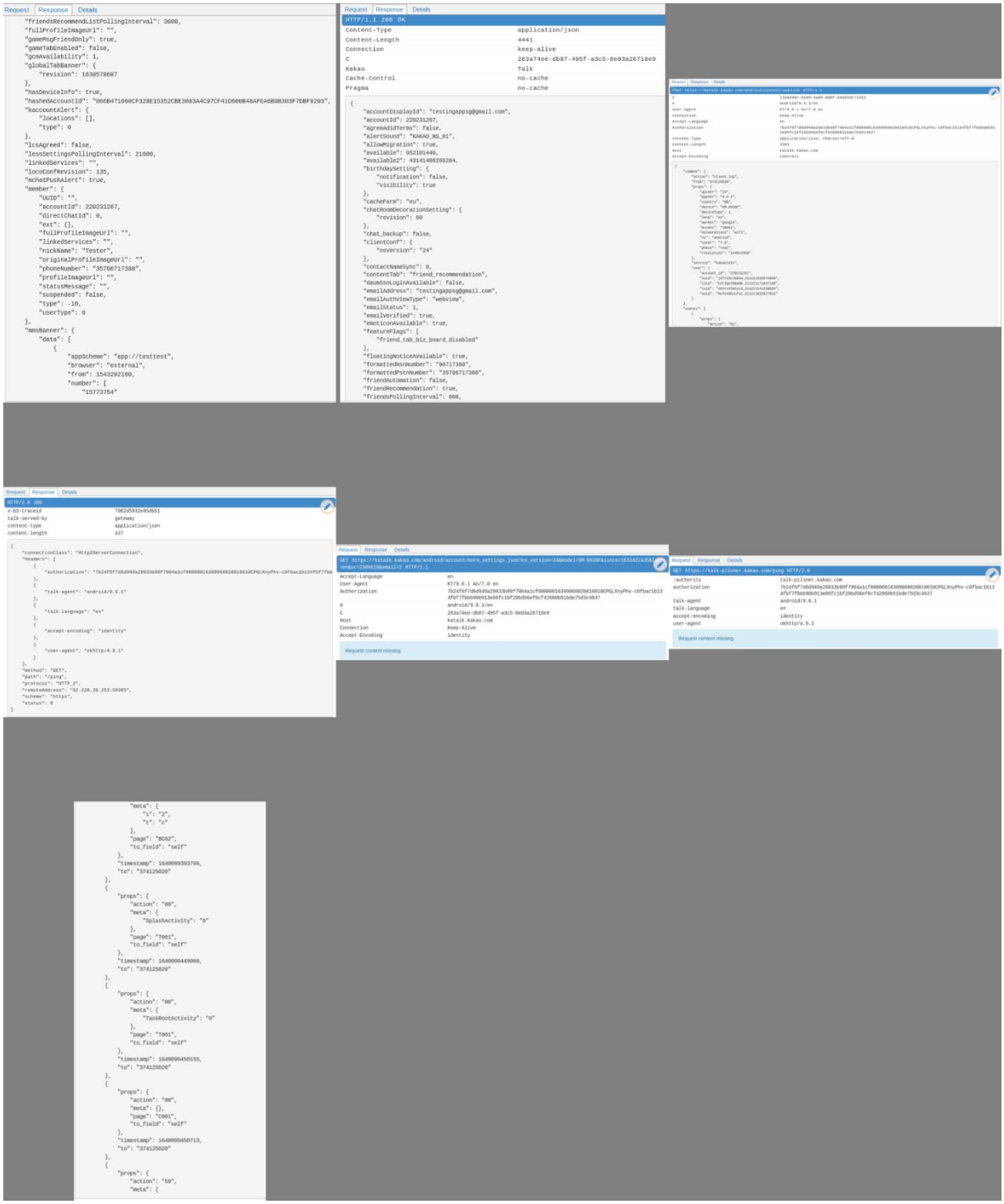
Πιο κάτω θα παρουσιαστούν στιγμιότυπα από τη μελέτη των εφαρμογών συνομιλιών/τηλεπικοινωνιών με τη χρήση του εικονικού περιβάλλοντος του οργανισμού PI.



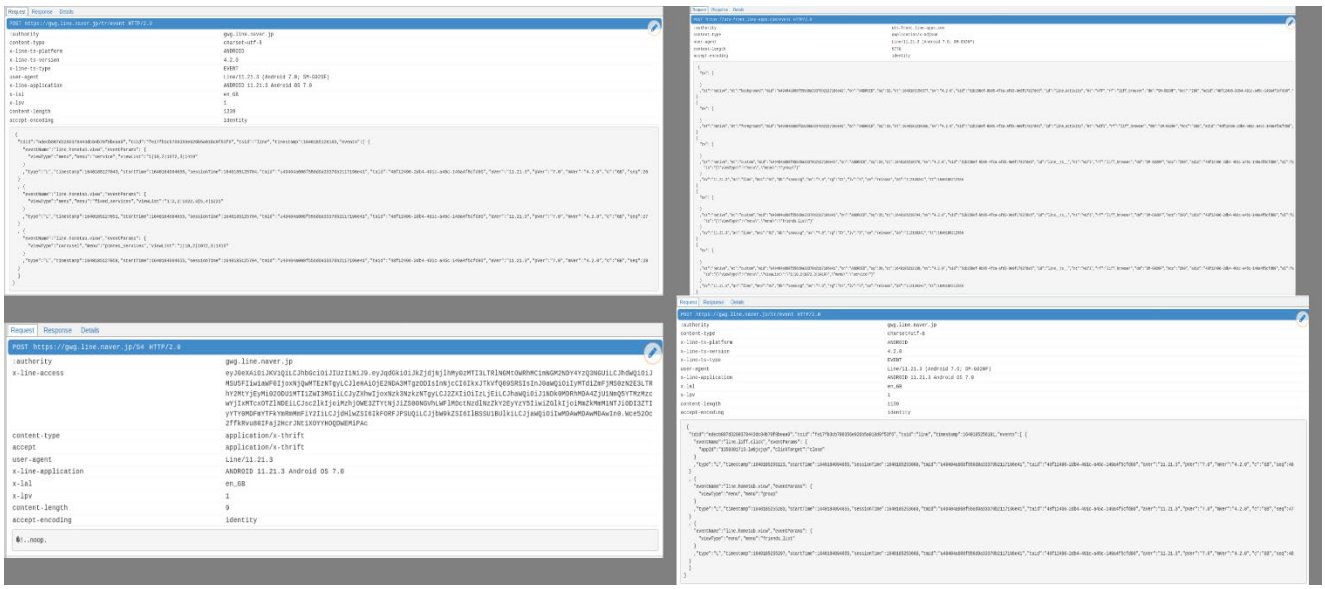
Εικόνα Α.50: Στιγμιότυπο της ανάλυσης της εφαρμογής Discord



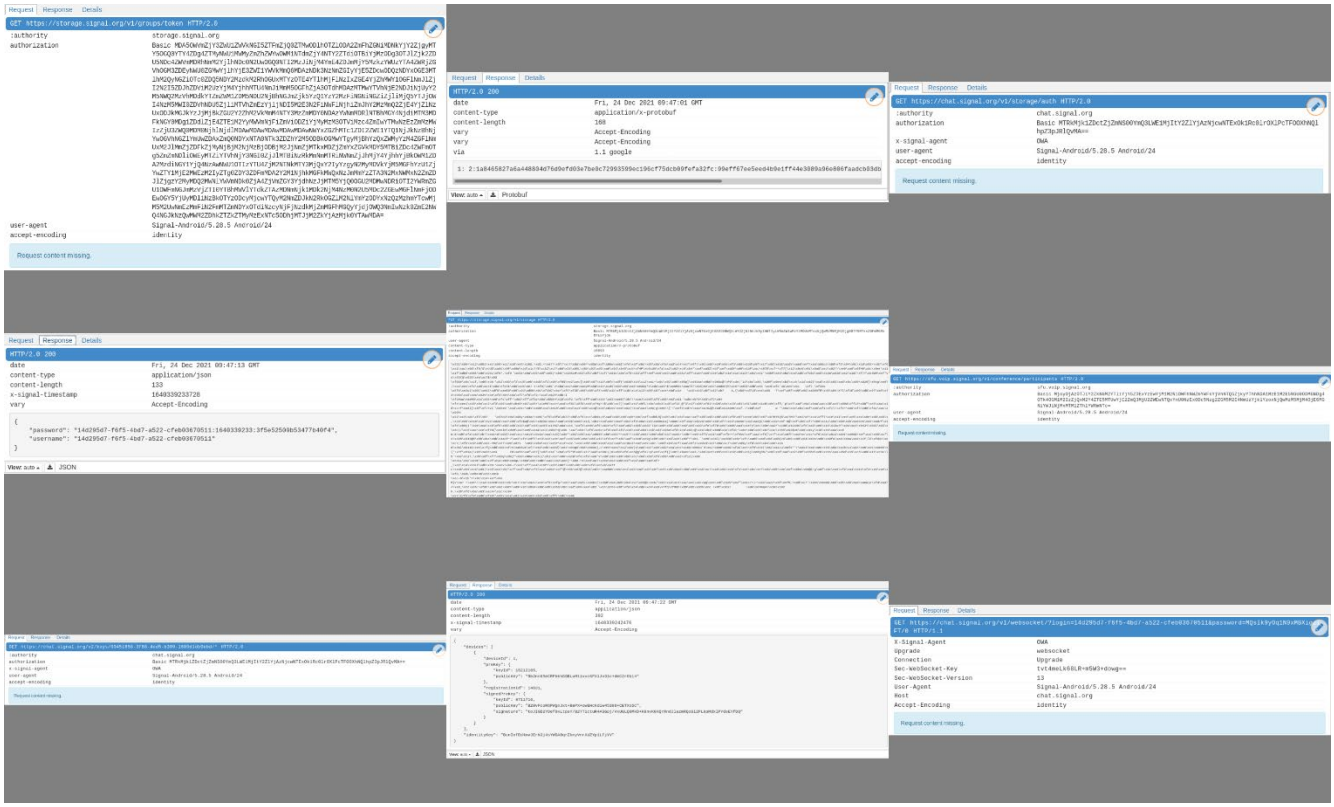
Εικόνα Α.51: Στιγμιότυπο της ανάλυσης της εφαρμογής Element



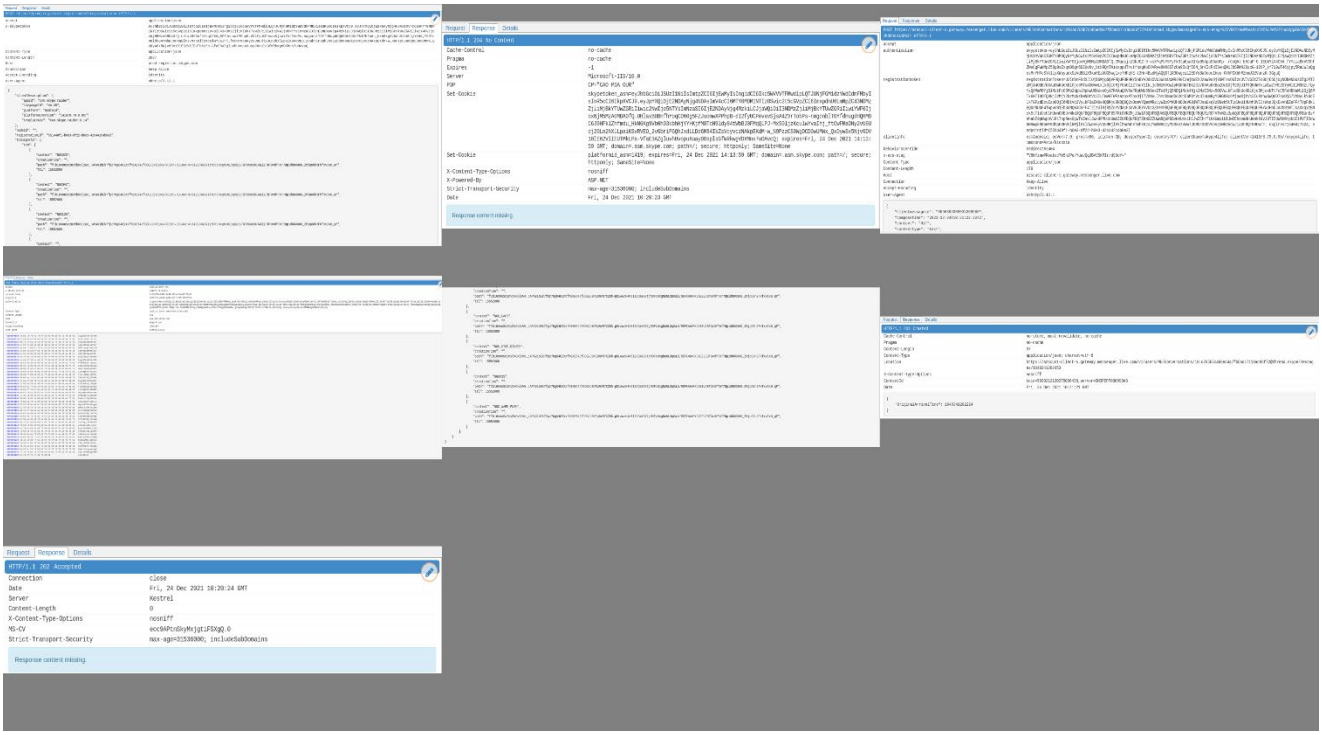
Εικόνα Α.52: Στιγμιότυπο της ανάλυσης της εφαρμογής KakaoTalk



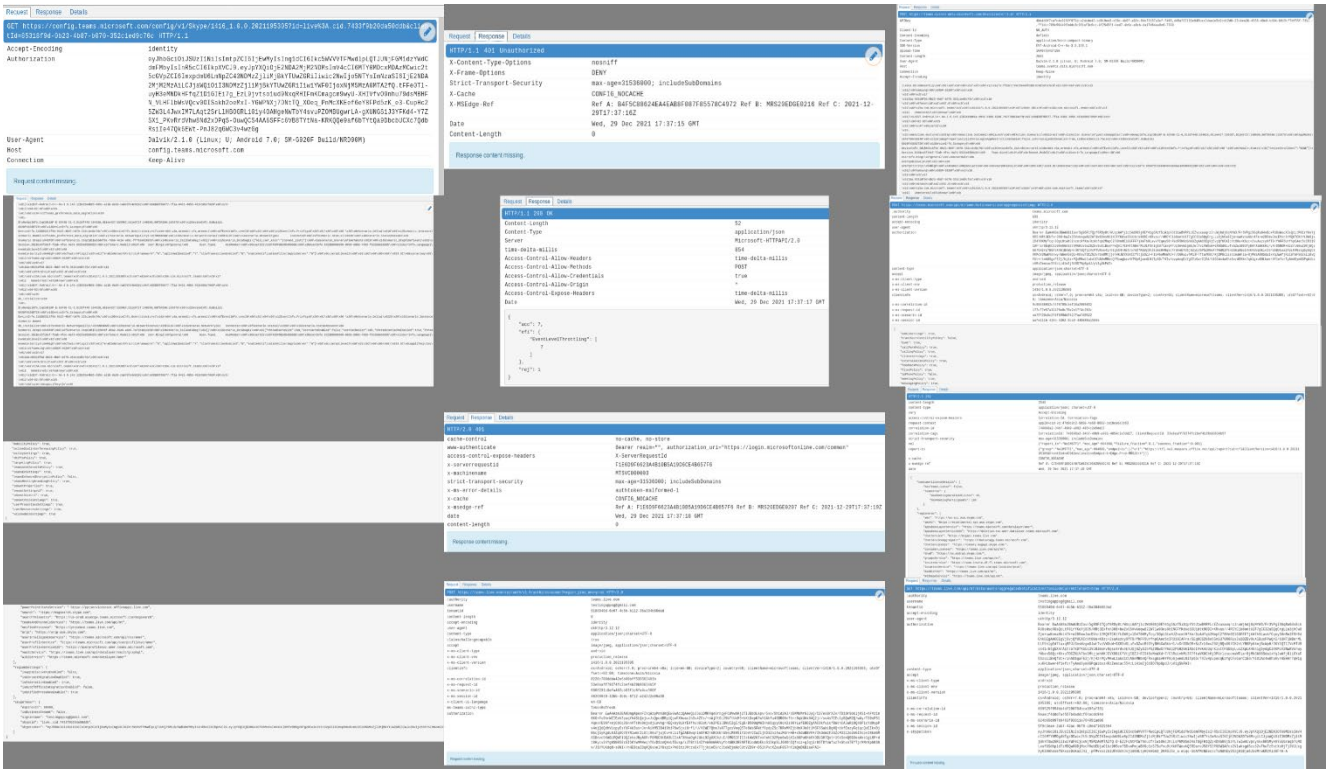
Εικόνα Α.53: Στιγμιότυπο της ανάλυσης της εφαρμογής Line



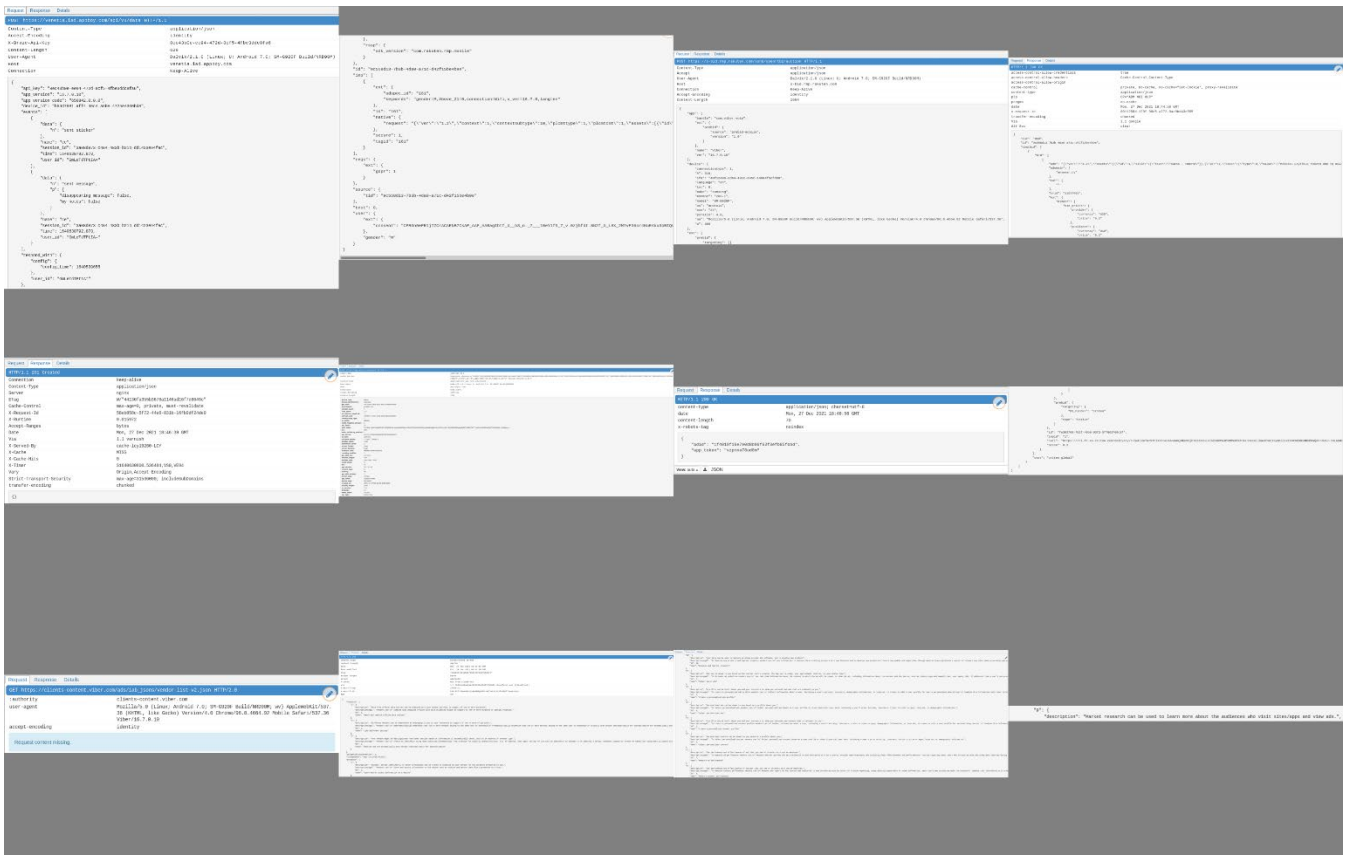
Εικόνα Α.54: Στιγμιότυπο της ανάλυσης της εφαρμογής Signal



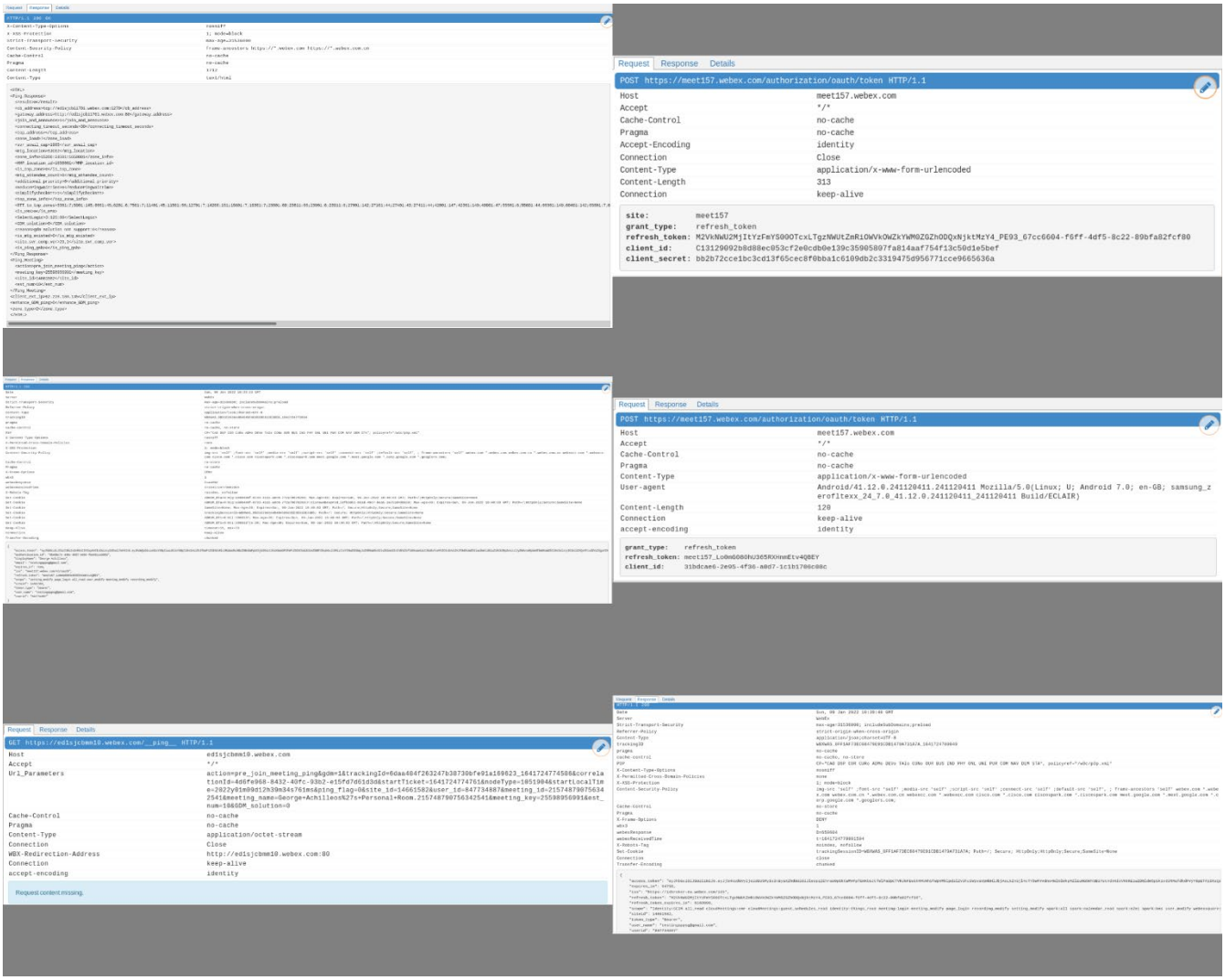
Εικόνα Α.55: Στιγμιότυπο της ανάλυσης της εφαρμογής Skype



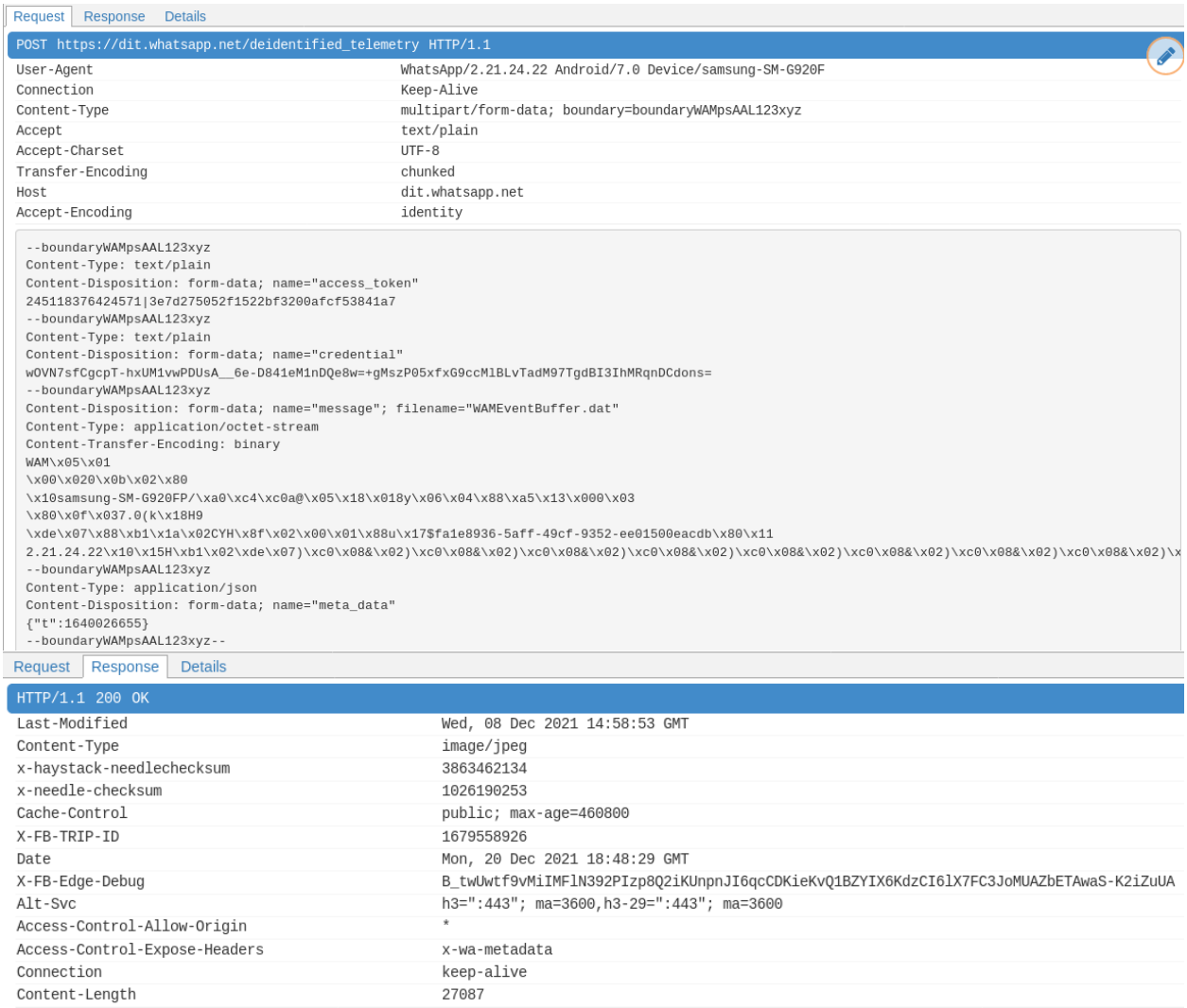
Εικόνα Α.56: Στιγμιότυπο της ανάλυσης της εφαρμογής Teams



Εικόνα Α.57: Στιγμιότυπο της ανάλυσης της εφαρμογής Viber



Εικόνα Α.58: Στιγμιότυπο της ανάλυσης της εφαρμογής Webex Meet



Request Response Details

POST https://dit.whatsapp.net/deidentified_telemetry HTTP/1.1

User-Agent	WhatsApp/2.21.24.22 Android/7.0 Device/samsung-SM-G920F
Connection	Keep-Alive
Content-Type	multipart/form-data; boundary=boundaryWAMpsAAL123xyz
Accept	text/plain
Accept-Charset	UTF-8
Transfer-Encoding	chunked
Host	dit.whatsapp.net
Accept-Encoding	identity

```
--boundaryWAMpsAAL123xyz
Content-Type: text/plain
Content-Disposition: form-data; name="access_token"
245118376424571|3e7d275052f1522bf3200afcf53841a7
--boundaryWAMpsAAL123xyz
Content-Type: text/plain
Content-Disposition: form-data; name="credential"
wOVN7sfCgcpT-hxUM1vwPDUsA__6e-D841eM1nDQe8w=+gMszP05xfxG9ccMlBLvTadM97TgdBI3IhMRqnDCdons=
--boundaryWAMpsAAL123xyz
Content-Disposition: form-data; name="message"; filename="WAMEventBuffer.dat"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
WAM\x05\x01
\x00\x020\x0b\x02\x80
\x10samsung-SM-G920FP/\xa0\xc4\xc0a@\x05\x18\x018y\x06\x04\x88\xa5\x13\x000\x03
\x80\x0f\x037.0(k\x18H9
\xde\x07\x88\xb1\x1a\x02CYH\x8f\x02\x00\x01\x88u\x17$fa1e8936-5aff-49cf-9352-ee01500eacdb\x80\x11
2.21.24.22\x10\x15H\xb1\x02\xde\x07)\xc0\x08&\x02)\xc0\x08&\x02)\xc0\x08&\x02)\xc0\x08&\x02)\xc0\x08&\x02)\xc0\x08&\x02)\xc0\x08&\x02)\x
--boundaryWAMpsAAL123xyz
Content-Type: application/json
Content-Disposition: form-data; name="meta_data"
{"t":1640026655}
--boundaryWAMpsAAL123xyz--
```

Request Response Details

HTTP/1.1 200 OK

Last-Modified	Wed, 08 Dec 2021 14:58:53 GMT
Content-Type	image/jpeg
x-haystack-needlechecksum	3863462134
x-needle-checksum	1026190253
Cache-Control	public; max-age=460800
X-FB-TRIP-ID	1679558926
Date	Mon, 20 Dec 2021 18:48:29 GMT
X-FB-Edge-Debug	B_twUwtf9vMiIMFlN392PIzp8Q2iKUnpnJI6qcCDKieKvQ1BZYIX6KdzCI6lX7FC3JoMUAZbETAwaS-K2iZuUA
Alt-Svc	h3=":443"; ma=3600,h3-29=":443"; ma=3600
Access-Control-Allow-Origin	*
Access-Control-Expose-Headers	x-wa-metadata
Connection	keep-alive
Content-Length	27087

Εικόνα Α.59: Στιγμιότυπο της ανάλυσης της εφαρμογής WhatsApp