Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ανάλυση Εφαρμογών Και Ψηφιακών Πειστηρίων Σε "Έξυπνες" Κινητές Συσκευές

Στυλιανή Χειλιώτη

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

ΜΑΙΟΣ 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ανάλυση Εφαρμογών Και Ψηφιακών Πειστηρίων Σε "Έξυπνες" Κινητές Συσκευές

Στυλιανή Χειλιώτη

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

ΜΑΙΟΣ 2018

Περίληψη

Η ζήτηση των «έξυπνων» κινητών συσκευών ολοένα και αυξάνεται. Κάθε χρόνο οι αλλαγές που γίνονται είναι δραστικές. Οι περισσότεροι άνθρωποι στις μέρες μας είναι εθισμένοι με τις «έξυπνες» κινητές συσκευές με αποτέλεσμα να αποτελούν σημαντικό κομμάτι του εαυτού μας. Οι καθημερινές μας υποχρεώσεις πλέον γίνονται μέσω διαδικτύου όπως οικονομικές συναλλαγές, επικοινωνία κλπ. Πληθώρα ευαίσθητων προσωπικών δεδομένων υπάρχουν στα smartphones/tablets και αποτελούν πληροφορίες σημαντικού ενδιαφέροντος τόσο για τους εγκληματίες (κυβερνο-εγκληματίες ή μη) όσο και για τους ψηφιακούς εγκληματολόγους.

Στην παρούσα μεταπτυχιακή διατριβή αναλύονται, μέσω ενός τεχνητού «εργαστηρίου» που δημιουργήσαμε, εγκληματολογικά εργαλεία και εφαρμογές τις οποίες χρησιμοποιεί ένας ψηφιακός εγκληματολόγος για να εξάγει και να ανακτήσει δεδομένα από μια «έξυπνη» κινητή συσκευή με λειτουργικό σύστημα Android.

Συγκεκριμένα, μελετώνται 5 ελεύθερα διαθέσιμα εγκληματολογικά εργαλεία εφαρμόζοντάς τα σε ένα εικονικό κινητό τηλέφωνο, εξετάζοντας τα αρχεία που ανακτά το κάθε ένα εξ' αυτών από τη συσκευή. Επίσης, εξετάζεται, μέσω δυναμικής ανάλυσης των προγραμμάτων, εάν η χρήση και μόνο αυτών των εργαλείων έχει ως αποτέλεσμα τυχόν «διαρροή» προσωπικών δεδομένων της συσκευής σε τρίτους. Περαιτέρω, έμφαση δίνεται σε κάποιες ειδικές περιπτώσεις εγκληματολογικού ενδιαφέροντος οι οποίες θα πρέπει να αντιμετωπιστούν με ειδικό τρόπο, όπως για παράδειγμα όταν η συσκευή είναι «κλειδωμένη» με PIN ή τα δεδομένα της είναι κρυπτογραφημένα ώστε η συσκευή μας να είναι προσβάσιμη από τον ερευνητή.

Η συγκεκριμένη μεταπτυχιακή διατριβή αποσκοπεί στην διατύπωση μιας κατά το δυνατόν ολοκληρωμένης εικόνας αναφορικά με τα ελεύθερα διαθέσιμα λογισμικά που ανήκουν στον χώρο της ψηφιακής εγκληματολογίας για «έξυπνες» κινητές συσκευές Android, με απώτερο σκοπό να μπορεί να χρησιμοποιηθεί ως οδηγός σε τέτοιες περιπτώσεις

Summary

The demand for “smart” mobile devices is rising rapidly. Every year the changes which are made are drastic. Most people, in our era, are somehow addicted to “smart” mobile devices, making them an important part their lives. Several routine tasks, such as financial transactions or communications, are being executed through smart devices, whereas large amount of personal data being processed in them; these data are of great interest for digital forensics, as well as for criminals.

In this thesis, several forensics tools and application are being analyzed, though a testing environment that has been appropriately built, towards examining which type of personal data can be extracted and retrieved from Android devices.

More precisely, we describe 5 free forensics tools by using them onto a virtual mobile phone, with the aim to identity their behavior – namely, to investigate the device’s files that can be collected by each of these tools. Moreover, a dynamic analysis of these applications is performed, in order to investigate whether the usage of such tools may result in personal data breaches to third parties. Finally, we examine some specific cases of forensics analysis that rest with the fact the device is “locked” such as via PIN or via encrypting the data; in such cases, special procedures are needed to allow access to an investigator.

This thesis provides an integrated and comprehensive view of digital forensics for Android “smart” mobile devices, with the ultimate goal to serve as a guide to such approaches.

Ευχαριστίες

Πρώτα από όλα, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της μεταπτυχιακής διατριβής μου, τον κ. Κωνσταντίνο Λιμνιώτη για την πολύτιμη βοήθεια και καθοδήγηση του κατά τη διάρκεια της δουλειάς μου. Πάνω από όλα θα ήθελα να ευχαριστήσω ολόψυχα τους γονείς μου και την αδερφή μου για την κατανόηση καθ' όλη την διάρκεια του μεταπτυχιακού και για την ηθική υποστήριξη τους, Επίσης, θα ήθελα να ευχαριστήσω τον Γρηγόριο Ποζιό και την Ειρήνη Ποζιού για την κατανόηση τους όλα αυτά τα χρόνια και ιδιαίτερα κατά την διάρκεια των τελευταίων μηνών της προσπάθειας μου. Αφιερώνω αυτή την μεταπτυχιακή διατριβή σε όλους όσους με βοήθησαν να την υλοποιήσω.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

1.1 Ανάλυση ψηφιακών πειστηρίων σε «έξυπνες» συσκευές

Ζούμε σε μια εποχή όπου οι τεχνολογικές ανάγκες αυξάνονται με ιλιγγιώδεις ρυθμούς. Κάθε μέρα ανακοινώνονται καινοτόμες τεχνολογίες οι οποίες πλέον αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας των ανθρώπων. Η συνεχόμενη εξέλιξη της τεχνολογίας, οδηγεί τους χρήστες σε έναν αγώνα απόκτησης όλων και περισσότερων καινούργιων τεχνολογικών συσκευών.

Πλέον δεν χρειάζεται κάποιος να έχει υπολογιστή για να μπορέσει να διαχειριστεί όλες τις καθημερινές εργασίες που πρέπει να πραγματοποιήσει. Οι κινητές συσκευές έχουν μετατραπεί σε κινητούς ηλεκτρονικούς υπολογιστές εφόσον έχουν εφάμιλλες δυνατότητες με αυτούς. Είναι απαραίτητο και αναπόσπαστο μέρος στην καθημερινότητα των ανθρώπων εφόσον με αυτές υλοποιούνται τα εξής: κλήσεις, μηνύματα, ηλεκτρονική αλληλογραφία, συντεταγμένες τοποθεσίας, κοινωνικά δίκτυα, παιχνίδια, οικονομικές συναλλαγές, ιστορικό φυλλομετρητή, εικόνες, βίντεο, ημερολόγιο, barcode reader κ.λπ.

Αν αναλογιστούμε ότι ο πληθυσμός της Γης είναι 7.467.500.000 [1], ο αριθμός των συνδέσεων των κινητών συσκευών είναι 8.504.356.000 [2] και οι μοναδικές συνδέσεις είναι 5.058.410.000 [2], αντιλαμβανόμαστε ότι ο αριθμός των κινητών συνδέσεων ξεπερνάει κατά πολύ τον πληθυσμό της Γης. Έχοντας ως δεδομένα τον συνολικό πληθυσμό της Γης και τις μοναδικές συνδέσεις μπορούμε να υπολογίσουμε ότι το 68% [1,2] του συνολικού πληθυσμού χρησιμοποιεί κινητές συσκευές.

Οι «έξυπνες» κινητές συσκευές, όπως έχουν καθιερωθεί να ονομάζονται, ενώ από τη μια πλευρά αποτελούν αναπόσπαστο κομμάτι της καθημερινότητάς μας, από την άλλη αποτελούν ένα από τα πιο χρήσιμα εργαλεία για παράνομες ή/και εγκληματικές

ενέργειες. Πλέον τα δεδομένα που αποθηκεύονται στις κινητές συσκευές υπολογίζονται σε δεκάδες GB σε κάθε μία από αυτές. Συνεπώς, η συλλογή και η ανάλυση τέτοιων δεδομένων απαιτεί μεγάλο όγκο εργασίας. Κατά συνέπεια, η κλασική έννοια των ψηφιακών πειστηρίων έχει πλέον διευρυνθεί σημαντικά έτσι ώστε να εντάσσονται σε αυτά, ως κύρια μέρη της ψηφιακής εγκληματολογίας, και τα ψηφιακά πειστήρια που συλλέγονται από «έξυπνες» συσκευές. Οι εγκληματίες χρησιμοποιούν τις κινητές τους συσκευές για να διαπράξουν εγκλήματα όπως το να ενεργοποιήσουν έναν εκρηκτικό μηχανισμό εξ αποστάσεως.

Η ανάλυση ψηφιακών πειστηρίων αποτελούσε ανέκαθεν ένα σημαντικό τμήμα της εγκληματολογίας και όχι μόνο, ακριβώς λόγω της εμφάνισης παράνομων ενεργειών οι οποίες αξιοποιούν, για την πραγμάτωσή τους, νέες τεχνολογίες – με πλέον χαρακτηριστικό παράδειγμα τις κυβερνοεπιθέσεις. Ακριβώς λόγω της προαναφερθείσας τεχνολογικής μετάβασης σε μικρού μεγέθους «έξυπνες» συσκευές, η χρήση αυτών σε παράνομες ή/και εγκληματικές ενέργειες καθίστανται πλέον ως πολύ διαδεδομένη αφού παίζουν σημαντικό ρόλο πλέον στην διευκόλυνση των υποθέσεων. Οι περισσότεροι εγκληματίες χρησιμοποιούν την συσκευή τους σε τέτοιο βαθμό ώστε μπορούν να κατηγορηθούν μόνο από τα ψηφιακά πειστήρια που θα συλλεχθούν από αυτές, για παράδειγμα από τις γεωγραφικές συντεταγμένες που βρίσκεται ο ύποπτος κάθε ώρα.

Ως εκ τούτου τα ψηφιακά πειστήρια που συλλέγονται από «έξυπνες» κινητές συσκευές αποτελούν κύρια μέρη της ψηφιακής εγκληματολογίας. Παρατηρώντας τον μεγάλο όγκο των δεδομένων που εξάγονται από αυτές, έσω των διαφόρων εφαρμογών, τίθεται το ερώτημα τι είδους δεδομένα συλλέγονται από τις έξυπνες κινητές συσκευές και τι περαιτέρω επεξεργασία υφίστανται;

1.2 Σκοπός της έρευνας

Υπάρχουν ποικίλες εφαρμογές και προγράμματα για την συλλογή και την εξέταση των ψηφιακών πειστηρίων σε «έξυπνες» κινητές συσκευές: μερικά είναι επί-πληρωμή και άλλα δωρεάν. Είναι υψίστης σημασίας να γνωρίζουμε αν αυτά τα προγράμματα και οι εφαρμογές είναι αποτελεσματικά και πόσο μάλλον αν τα δεδομένα που συλλέγουν και επεξεργάζονται οι διάφορες εφαρμογές από τις έξυπνες κινητές συσκευές παραμένουν εμπιστευτικά και γίνεται νόμιμη επεξεργασία επ’ αυτών. Συναφώς με αυτό το ερώτημα,

το οποίο άπτεται του τι ακριβώς «διεργασία» πραγματοποιεί μία «έξυπνη» εφαρμογή, ανακύπτει το ζήτημα ως προς το ποια είναι τα κύρια μέρη συλλογής ψηφιακών πειστηρίων καθώς επίσης και ποια είναι τα εμπόδια που μπορούν να συναντήσουν οι εγκληματολόγοι για την συλλογή πειστηρίων.

Στόχος της παρούσας μεταπτυχιακής διατριβής είναι η εφαρμογή και η ανάλυση προγραμμάτων και εφαρμογών της ψηφιακής εγκληματολογίας για συσκευές του διαδομένου λειτουργικού συστήματος Android καθώς και η ανάλυση των δεδομένων που συλλέγονται μέσω αυτών. Πέραν της τυπικής χρήσης των εργαλείων, η οποία καταδεικνύει τι δεδομένα συλλέγουν από μια «έξυπνη» κινητή συσκευή στο πλαίσιο συλλογής ψηφιακών πειστηρίων, πραγματοποιήσαμε ενδελεχή δυναμική ανάλυση των ίδιων των εφαρμογών συλλογής πειστηρίων, προκειμένου να διαπιστώσουμε αν, πέραν αυτής της συλλογής για την οποία σχεδιάστηκαν, πραγματοποιούν και κάποια άλλη «κρυμμένη» επεξεργασία επί των δεδομένων της συσκευής. Δεδομένου ότι εστιάσαμε σε δωρεάν διαθέσιμα λογισμικά, ελεύθερα διαθέσιμα στον οποιοδήποτε, τα οποία πραγματοποιούν ανάλυση ψηφιακών πειστηρίων, ο σκοπός της έρευνας μας είναι διττός: πέραν της αποτίμησης των δυνατοτήτων που έχουν από πλευράς ψηφιακής εγκληματολογίας, έχει ενδιαφέρον να καταγραφούν οι δυνατότητές τους και από την σκοπιά κατά πόσον μπορούν να αξιοποιηθούν από άτομα εκτός του χώρου της ψηφιακής εγκληματολογίας, προκειμένου να γίνει συλλογή προσωπικών δεδομένων από μια κινητή συσκευή. Για την επίτευξη των ανωτέρω πραγματοποιήθηκαν τα εξής:

- Έρευνα επάνω στην τρέχουσα βιβλιογραφία για τα ψηφιακά πειστήρια σε κινητά τηλέφωνα με λειτουργικό Android
- Εντοπισμός των κατάλληλων προγραμμάτων και εφαρμογών που θα χρησιμοποιήσουμε για να τις αξιολογήσουμε
- Καθορισμός των ποιοτικών κριτήριων για την αξιολόγηση των εργαλείων
- Εξαγωγή κατάλληλων αποτελεσμάτων μετά την αξιολόγηση των εργαλείων.

1.3 Διάρθρωση Διατριβής

Η δομή της παρούσας διατριβής περιγράφεται στη συνέχεια.

Στο δεύτερο κεφάλαιο της διατριβής γίνεται παρουσίαση του λειτουργικού συστήματος Android, των εκδόσεων και της αρχιτεκτονικής του. Σκοπός του συγκεκριμένου

κεφαλαίου είναι να παρέχει απαραίτητο υπόβαθρο στον αναγνώστη ώστε να αντιληφθεί την δομή του λειτουργικού συστήματος και με ποιον τρόπο τα δεδομένα αποθηκεύονται και υφίστανται επεξεργασία σε αυτό.

Στο τρίτο κεφάλαιο εξετάζεται ο χώρος των ψηφιακών πειστηρίων. Κατ' αρχάς παρατίθεται ο ορισμός των ψηφιακών πειστηρίων. Επίσης, προσδιορίζονται τα δεδομένα τα οποία εντάσσονται σε αυτή την κατηγορία και ταξινομούνται αναλόγως. Επιπλέον, περιγράφεται η διαδικασία ή αλλιώς οι φάσεις της εγκληματολογικής εξέτασης ψηφιακών πειστηρίων ώστε να θεωρηθεί η συλλογή και η ανάλυση τους έγκυρη από την πλευρά του δικαστηρίου.

Στο τέταρτο κεφάλαιο περιγράφουμε το περιβάλλον δοκιμών το οποίο αναπτύχθηκε στο πλαίσιο της παρούσας διατριβής, προκειμένου να μελετηθούν τα εργαλεία ανάλυσης ψηφιακών πειστηρίων. Συγκεκριμένα, γίνεται αναφορά στο περιβάλλον προσομοίωσης της εικονικής συσκευής μας, καθώς και στα χαρακτηριστικά της. Επίσης, περιγράφουμε τις ιδιότητες του λειτουργικού Android που εγκαταστήσαμε καθώς και τα κατάλληλα προγράμματα που αξιοποιήσαμε ώστε το περιβάλλον μας να είναι έτοιμο για τις δοκιμές μας.

Στο πέμπτο κεφάλαιο περιγράφουμε τα εγκληματολογικά εργαλεία τα οποία θα χρησιμοποιήσουμε και θα μελετήσουμε το πλαίσιο της έρευνάς μας, την δομή τους καθώς και τον τρόπο που τα εγκαταστήσαμε. Επίσης, παρατίθενται τα πλεονεκτήματα και τα μειονεκτήματα κάθε εργαλείου. Επιπλέον, αναλύονται τα αποτελέσματα της μελέτης κάθε εργαλείου ξεχωριστά είτε από τον proxy (Burp Suite) είτε από το Inspeckage.

Στο έκτο κεφάλαιο περιγράφονται ειδικές περιπτώσεις που θα μπορούσαν να δυσκολέψουν το έργο των ψηφιακών εγκληματολόγων στις «έξυπνες» κινητές συσκευές όπως για παράδειγμα το PIN της συσκευής και η κρυπτογράφηση των δεδομένων.

Στο έβδομο κεφάλαιο γίνεται η σύνοψη της μεταπτυχιακής διατριβής και η συνολική αναφορά των αποτελεσμάτων. Ειδικότερα, παραθέτουμε τα συμπεράσματα που ανακύπτουν από την εφαρμογή και την ανάλυση των εγκληματολογικών εφαρμογών/εργαλείων.

Κεφάλαιο 2
Το Λειτουργικό Σύστημα Android

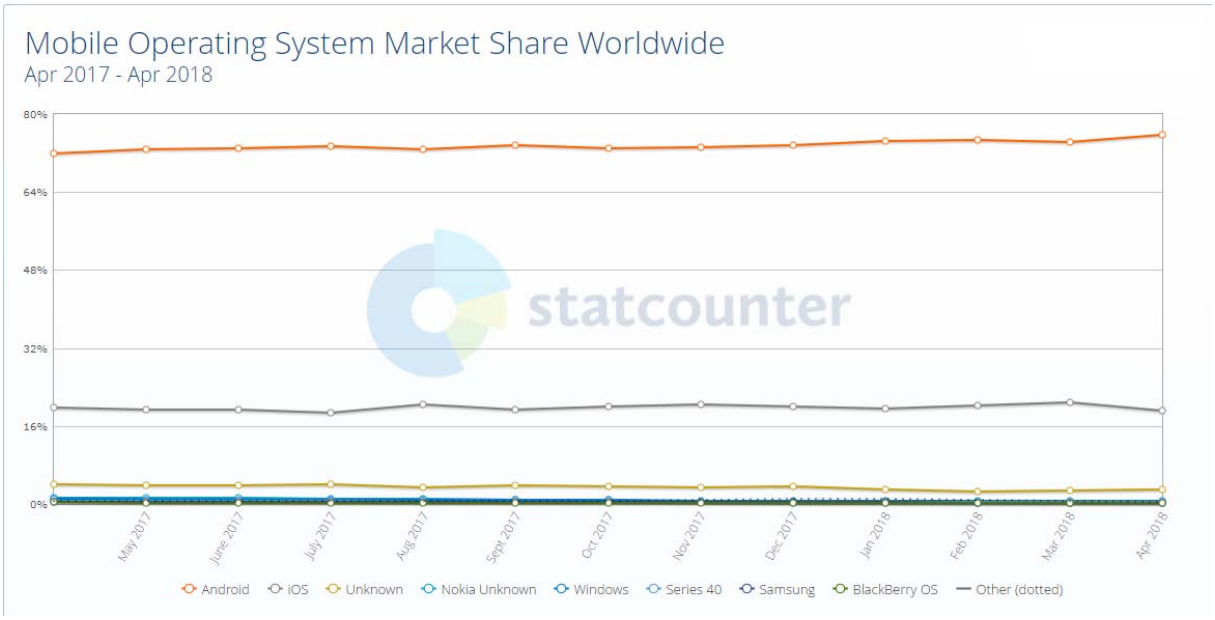
2.1 Λογισμικό Android

Το Android είναι ένα λειτουργικό σύστημα σχεδιασμένο από την Google. Η πρώτη παρουσίαση της πλατφόρμας Android έγινε στις 5 Νοεμβρίου του 2007 καθώς ανακοινώθηκε και η ίδρυση του οργανισμού Open Handset Alliance μιας κοινοπραξίας 48 τηλεπικοινωνιακών εταιριών λογισμικού οι οποίες έχουν ως σκοπό τους την ανάπτυξη και την εξέλιξη των ανοιχτών προτύπων για τις συσκευές κινητής τηλεφωνίας. Η πρώτη έκδοση του Android κυκλοφόρησε στις 23 Σεπτεμβρίου του 2008 [3]. Το λογότυπο για το λειτουργικό σύστημα Android είναι ένα ρομπότ σε χρώμα πράσινο μήλου που σχεδιάστηκε από τη γραφίστρια Ιρίνα Μπλοκ [4].

Εικόνα 2.1 Λογότυπο Android [5]

Το Android είναι από τα πιο δημοφιλέστερα λειτουργικά συστήματα για συσκευές κινητής τηλεφωνίας και ταμπλέτες (tablets), σχεδιασμένο ως επί το πλείστον για οθόνη αφής. Χρησιμοποιείται βέβαια σε τηλεοράσεις, αυτοκίνητα και ρολόγια χειρός με τελείως διαφορετικό περιβάλλον από αυτό των κινητών και των tablets.

Οι κινητές συσκευές διαθέτουν διαφορετικά λογισμικά συστήματα, αλλά το μεγαλύτερο ποσοστό αυτών διαθέτουν από αυτές να έχουν λειτουργικό Android. Σύμφωνα με έρευνα που έγινε από την εταιρία *StatCounterGlobalStats* από τον Απρίλιο του 2017 έως τον Απρίλιο του 2018, το λειτουργικό Android καταλαμβάνει το 75,66% των κινητών συσκευών, ενώ ακολουθεί το iOS με 19,23% [6].



Εικόνα2.2 Mobile Operating System Market Share Worldwide, April 2017- April 2018 [6]

Ο πυρήνας του Android είναι βασισμένος στον πυρήνα του Linux. Το Android καθώς και το Linux είναι και τα δυο ανοιχτού κώδικα λειτουργικά συστήματα με αποτέλεσμα να επιτρέπει στους προγραμματιστές ή γενικότερα στους χρήστες που έχουν κάποια εμπειρία σε κώδικα, να μπορούν να το προσαρμόσουν στις δικές τους ανάγκες χρησιμοποιώντας κώδικα Java επεμβαίνοντας με αυτό τον τρόπο στο εσωτερικό των ανωτέρων επιπέδων του λειτουργικού συστήματος.

Για την ανάπτυξη εφαρμογών Android διατίθεται ένας μεγάλος αριθμός εργαλείων ανάπτυξης που είτε είναι ανοιχτού κώδικα είτε είναι δωρεάν. Οι προγραμματιστές μπορούν να διανέμουν τις εφαρμογές τους χάρη στο Google Play Store και ο καθένας μπορεί να έχει πρόσβαση ώστε να τις κατεβάσει στην έξυπνη κινητή συσκευή του.

Σύμφωνα με έρευνα που διενεργήθηκε τον Μάρτιο του 2017 ο αριθμός των εφαρμογών που είναι διαθέσιμες στον Google Play Store έφτασε τις 2.800.000 [7].

2.2 Εκδόσεις του Android

Όπως αναφέραμε και προγενέστερα η πρώτη δοκιμαστική έκδοση Android ξεκίνησε στις 5 Νοεμβρίου του 2007. Η πρώτη έκδοση που ονομάστηκε alpha κυκλοφόρησε στις 23 Σεπτεμβρίου του 2008. Από τότε έχουν κυκλοφορήσει πολλές εκδόσεις επιφέροντας ποικίλες αλλαγές στις λειτουργίες του και διορθώνοντας αρκετά σφάλματα.

Έκδοση	Κωδική Ονομασία	Ημερομηνία Αρχικής Κυκλοφορίας
8.0	Oreo	21 Αυγούστου 2017
7.1	Nougat	4 Οκτωβρίου 2016
7.0	Nougat	22 Αυγούστου 2016
6.0 – 6.0.1	Marshmallow	5 Οκτωβρίου 2015
5.1	Lollipop	9 Μαρτίου 2015
5.0	Lollipop	3 Νοεμβρίου 2014
4.4 – 4.4.4	KitKat	31 Οκτωβρίου 2013
4.3	JellyBean	24 Ιουλίου 2013
4.2	JellyBean	13 Νοεμβρίου 2012
4.1	JellyBean	9 Ιουλίου 2012
4.0 – 4.0.4	IceCreamSandwich	16 Δεκεμβρίου 2011
3.0 – 3.2.6	Honeycomb	15 Ιουλίου 2011
2.3 -2.3.7	Gingerbread	9 Φεβρουαρίου 2011
2.2 - 2.23	Froyo	20 Μαΐου 2010
2.0 - 2.1	Eclair	26 Οκτωβρίου 2009
1.6	Donut	15 Σεπτεμβρίου 2009
1.5	Cupcake	27 Απριλίου 2009
1.1	Beta	9 Φεβρουάριου 2009
1.0	Alpha	23 Σεπτεμβρίου 2008

Πίνακας 2.1 Ονομασίες Εκδόσεων Android & Ημερομηνίες Αρχικής Κυκλοφορίας [8]

Ένα από τα μειονεκτήματα του λογισμικού Android είναι οι πολλαπλές εκδόσεις που έχουν δημιουργηθεί. Οι προγραμματιστές είναι υποχρεωμένοι να υλοποιούν και να δοκιμάζουν τις εφαρμογές τους σχεδόν σε όλες τις εμπορικές εκδόσεις του Android. Για αυτό το λόγο θα πρέπει να έχουνε μια εκτίμηση για τις εκδόσεις που χρησιμοποιούν το

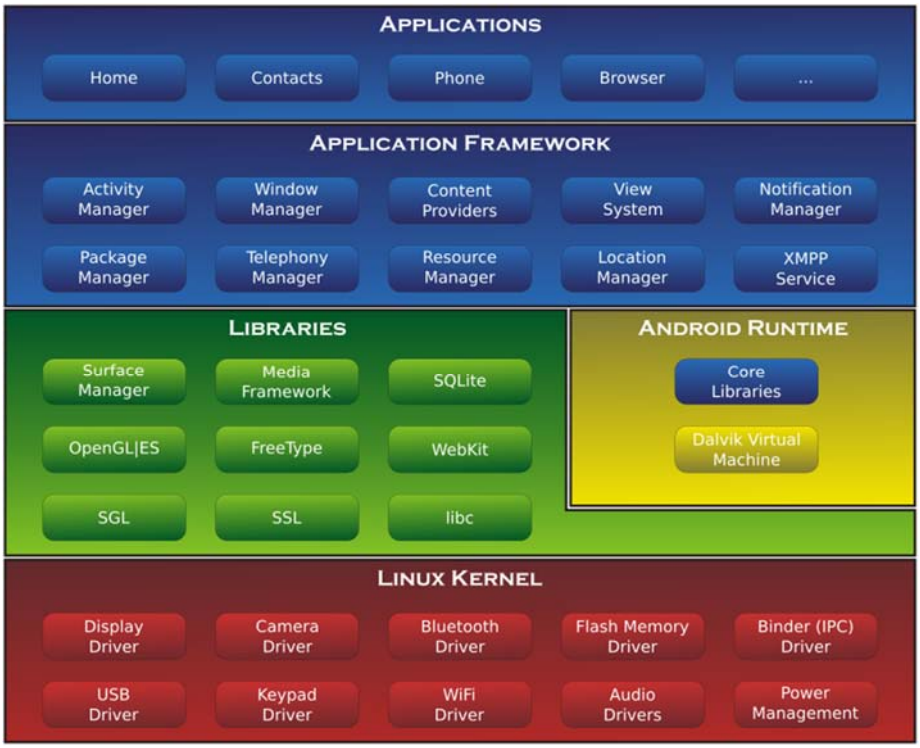
μεγαλύτερος μέρος των smartphones. Στην εικόνα 2.2 βλέπουμε μια ανασκόπηση από τις διάφορες εκδόσεις του λειτουργικού συστήματος Android που χρησιμοποιούνται.

Εικόνα 2.3 Εκδόσεις του λειτουργικού Android [6]

Όπως παρατηρούμε, το μεγαλύτερος μέρος των εκδόσεων λογισμικού Android το κατέχει η έκδοση Marshmallow 6.0 με ποσοστό 27.21% και τη δεύτερη θέση κατέχει η έκδοση Nougat 7.0 με ποσοστό 25.35%. Οι εκδόσεις που δεν εμφανίζονται έχουν ποσοστό χρήσης χαμηλότερο από 0,1%.

2.3 Αρχιτεκτονική του Android

Ο σκοπός ενός λειτουργικού συστήματος είναι να προσφέρει στο χρήστη τη δυνατότητα να αξιοποιεί κατάλληλα τους πόρους τους συστήματος προς όφελός του με την καλύτερη δυνατή διεπαφή. Για να είναι εφικτό αυτό θα πρέπει το λειτουργικό σύστημα να είναι δομημένο έτσι ώστε το κάθε τμήμα να έχει ξεκάθαρους ρόλους.



Εικόνα 2.4 Αρχιτεκτονική Android [9]

Η Αρχιτεκτονική Android περιλαμβάνει τον πυρήνα Linux, τις βιβλιοθήκες, το Android Runtime, το επίπεδο Application Framework και το επίπεδο των εφαρμογών.

2.3.1 Πυρήνας του Linux

Το Android βασίζεται στο λειτουργικό σύστημα Linux για βασικές υπηρεσίες συστήματος όπως ασφάλεια, διαχείριση μνήμης, διαχείριση διεργασιών, στοίβα και οδηγού συσκευών. Ο πυρήνας είναι το τμήμα ενός λειτουργικού το οποίο αναλαμβάνει την διασύνδεση μεταξύ εφαρμογών και υλικού (hardware).

Ο πυρήνας του Android μπορεί να βασίζεται στον πυρήνα του Linux, αλλά διαφέρει αρκετά από αυτόν. Αυτό οφείλεται στις αλλαγές στην αρχιτεκτονική που έχει κάνει η Google για να είναι ελαφρύτερος και βελτιστοποιημένος για χρήση σε κινητές συσκευές.

2.3.2 Επίπεδο Βιβλιοθηκών

Σε αυτό το επίπεδο, το οποίο είναι ακριβώς ένα επίπεδο πάνω από τον πυρήνα, συναντάμε τις βασικές βιβλιοθήκες του συστήματος. Το Android περιλαμβάνει ένα σύνολο βιβλιοθηκών C/C++ που χρησιμοποιούνται από διάφορα στοιχεία του συστήματος. Αυτές οι λειτουργίες είναι προσβάσιμες από τους προγραμματιστές μέσω της εφαρμογής ανάπτυξης του Android. Ορισμένες από αυτές είναι η τυπική βιβλιοθήκη της C, βιβλιοθήκη για τα πολυμέσα, η βιβλιοθήκη Media Framework η οποία περιέχει τους αποκωδικοποιητές για την αναπαραγωγή των πολυμέσων (MP3, MPEG), η βιβλιοθήκη SQLite για τις Βάσεις Δεδομένων, βιβλιοθήκη Surface Manager για τα γραφικά, η βιβλιοθήκη Web Kit για τους φυλλομετρητές κ.λπ.

2.3.3 Επίπεδο Android Runtime

Το επίπεδο Android Runtime περιλαμβάνει τις βασικές βιβλιοθήκες για την διεπαφή εφαρμογών Java που προσφέρονται στον προγραμματιστή για την υλοποίηση δικών του εφαρμογών καθώς και την Dalvik Virtual Machine η οποία είναι ο ειδικός διερμηνευτής του Android για την γλώσσα προγραμματισμού Java.

Κάθε εφαρμογή του Android είναι γραμμένη σε Java την οποία το σύστημα δεν την αναγνωρίζει απευθείας. Η Dalvik Virtual Machine αναλαμβάνει να μεταφράσει τα

αρχεία java σε εκτελέσιμα αρχεία *.dex (Dalvik Executable) τα οποία εκτελούνται κανονικά από το λειτουργικό σύστημα. Η Dalvik Virtual Machine έχει την δυνατότητα να εκτελεί πολλά αρχεία ταυτόχρονα διασφαλίζοντας έτσι την ευστάθεια και την ασφάλεια του λειτουργικού συστήματος.

2.3.4 Επίπεδο Application Framework

Το επίπεδο αυτό ενδιαφέρει περισσότερο τους προγραμματιστές γιατί τους δίνει πλήρη πρόσβαση. Το επίπεδο αυτό προσφέρει ένα μεγάλο αριθμό API τα οποία δίνουν στον προγραμματιστή την δυνατότητα να τα ενσωματώνει στις εφαρμογές του. Μερικές από τις βασικές οντότητες που παρέχονται από το συγκεκριμένο επίπεδο είναι:

- Activity Manager: Διαχειρίζεται τον κύκλο ζωής των εφαρμογών και παρέχει την δυνατότητα των εφαρμογών σε προηγούμενες καταστάσεις
- Resource Manager: Παρέχει την πρόσβαση σε πόρους του συστήματος,
- Notification Manager: Διαχειρίζεται τα μηνύματα των εφαρμογών που εμφανίζονται στην status bar
- View System: Επιτρέπει την χρήση λιστών, πλαισίων, πεδίων κειμένου, κουμπιών κλπ.

2.3.5 Επίπεδο εφαρμογών

Στο ανώτερο επίπεδο βρίσκονται οι εφαρμογές του συστήματος με τις οποίες αλληλοεπιδρούν οι χρήστες. Μερικές από τις πιο γνωστές εφαρμογές είναι ο φυλλομετρητής, το ημερολόγιο, τα SMS, το e-mail, διαχείριση επαφών, παιχνίδια, οι φωτογραφίες, η μουσική και πολλά άλλα. Οι παραπάνω εφαρμογές είναι γραμμένες σε Java και μπορούν να εκτελούνται πολλές ταυτόχρονα χωρίς να επηρεάζει η μία την άλλη.

2.4 Android Partitions

Η κατανόηση της δομής των αρχείων μιας «έξυπνης» κινητής συσκευής αποτελεί ακρογωνιαίο λίθο και συμβάλλει σημαντικά στην επιτυχή εξέταση μιας υπόθεσης από

τον ερευνητή. Ο ψηφιακός εγκληματολόγος θα πρέπει να κατέχει γνώση για το πως οργανώνονται, αποθηκεύονται και ανακτώνται τα δεδομένα από τις συσκευές.

Εικόνα 2.5 Android Partitions [10]

Κάθε «διαμέρισμα δίσκου» (partition) θεωρείται ξεχωριστή λογική μονάδα δεδομένων. Κάθε μονάδα περιέχει διαφορετικά δεδομένα και για αυτό το λόγο έχουν χωριστεί από τους κατασκευαστές. Παρακάτω θα αναλύσουμε εν συντομία τις λογικές μονάδες καθώς και τι δεδομένα περιλαμβάνει η καθεμία αντίστοιχα.

2.4.1 Boot Partition

Το Boot Partition είναι υπεύθυνο για την εκκίνηση της «έξυπνης» κινητής συσκευής εφόσον περιέχει όλα τα απαραίτητα δεδομένα. Επίσης περιλαμβάνει το kernel, τη ram, το download mode, την αναβάθμιση του πυρήνα kernel, το recovery mode κλπ. Θεωρείται το κατώτατο επίπεδο λειτουργικότητας της συσκευής.

2.4.2 System Partition

Το System Partition περιέχει όλο το λειτουργικό σύστημα της συσκευής και στη συγκεκριμένη περίπτωση το λειτουργικό σύστημα Android. Επιπλέον, περιλαμβάνει το interface του χρήστη και τις εφαρμογές που είναι προ-εγκατεστημένες με το λειτουργικό σύστημα.

2.4.3 Recovery Partition

Το Recovery Partition περιέχει τα δεδομένα για μπορέσει η συσκευή να μπει στο recovery console. Μέσω αυτής της κονσόλας ο χρήστης είναι σε θέσει να πραγματοποιήσει αναβάθμιση, λήψη backup των δεδομένων του κλπ.

2.4.4 Data Partition

Σε αυτή την λογική μονάδα είναι αποθηκευμένο το σύνολο των δεδομένων του χρήστη. Όπως συμπεραίνουμε είναι το partition με την μεγαλύτερη προτεραιότητα από την πλευρά του ερευνητή εφόσον περιέχει όλα τα προσωπικά δεδομένα του χρήστη καθώς και όλες τις εφαρμογές που έχουν εγκατασταθεί στη συσκευή όπως μηνύματα, κλήσεις, γεωγραφικές συντεταγμένες, εικόνες, βίντεο, μουσική, δεδομένα επικοινωνίας κλπ.

2.4.5 Cache Partition

Αυτό το Cache Partition θεωρείται η μνήμη της συσκευής εφόσον αποθηκεύει προσωρινά τα δεδομένα που χρησιμοποιούνται πιο συχνά από τις εφαρμογές για να είναι εύκολα προσπελάσιμα με αποτέλεσμα να εξοικονομείται χρόνος και πόροι του συστήματος

2.4.6 Misc Partition

Στο Misc Partition περιέχονται δεδομένα από διάφορες ρυθμίσεις του συστήματος όπως CID (Carries ID), ρυθμίσεις για τις USB συνδέσεις (USB configuration), αρχεία καταγραφής (logs) που αφορούν το wifi, το Bluetooth κλπ. Θεωρείται και αυτό σημαντικό από την πλευρά του ερευνητή εφόσον μπορεί να τοποθετήσει τον χρήστη σε κάποια περιοχή είτε από τα logs του wifi είτε από τα logs του gps.

Κεφάλαιο 3
Ψηφιακά Πειστήρια

3.1 Ορισμός

Η ψηφιακή εγκληματολογία κινητών τηλεφώνων (mobile forensics) είναι ένας κλάδος της ψηφιακής εγκληματολογίας που αφορά την ανάκτηση ψηφιακών πειστηρίων ή δεδομένων από μια κινητή συσκευή κάτω από εγκληματολογικές συνθήκες. Ο κλάδος των mobile forensics δεν αφορά μόνο τα κινητά τηλέφωνα αλλά και συσκευές που έχουν εσωτερική μνήμη και επικοινωνιακή ικανότητα όπως τα tablets, τις GPS συσκευές κλπ.

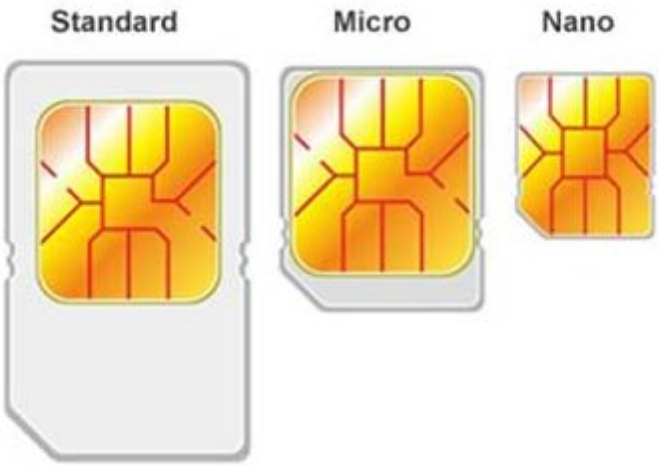
Η εξέταση και η ανάλυση των κινητών τηλεφώνων/συσκευών στο έγκλημα ξεκίνησε τέλη της δεκαετίας του 1990 με αρχές της δεκαετίας του 2000 [11]. Η μεγάλη αύξηση ωστόσο των «έξυπνων» τηλεφώνων / συσκευών δεν μπορούσε να καλυφθεί υπό τις υπάρχουσες τεχνολογικές μεθοδολογίες εφόσον οι υπολογιστές δεν έχουν τις ίδιες λειτουργίες με τις κινητές συσκευές όπως για παράδειγμα το GPS, κλήσεις κλπ. και για αυτό το λόγο υπήρχε ανάγκη για καινούργιες τεχνικές. Τα ψηφιακά στοιχεία στις συσκευές είναι ευαίσθητα και ευπαθή καθώς τα δεδομένα μπορούν εύκολα να αντικατασταθούν.

Ως ψηφιακό πειστήριο ορίζεται ένα κομμάτι πληροφορίας, σχετικό με την υπόθεση που διερευνάται, το οποίο είναι σε ψηφιακή μορφή [11]. Μπορεί να είναι ηλεκτρονικό αρχείο, φωτογραφία, πολυμέσο, ιστορικό φυλλομετρητή, βάση δεδομένων, αρχείο log, εκτελέσιμο αρχείο κλπ.

Καθώς η τεχνολογία εξελίσσεται ραγδαία, αυξάνεται συνεχώς η ποσότητα και οι τύποι των δεδομένων σε μια κινητή συσκευή. Τα αποδεικτικά ψηφιακά στοιχεία που μπορούν να ανακτηθούν από ένα τηλέφωνο ενδέχεται να προέρχονται από 4 διαφορετικές πηγές: από την εσωτερική μνήμη (internal memory), από την SIM, από την εξωτερική κάρτα μνήμης (memory card) και από το Cloud.

Κάρτα SIM

Η κάρτα SIM (Subscriber Identity Module) χρησιμοποιείται για την ταυτοποίηση του κατόχου. Κάθε κάρτα SIM προστατεύεται από έναν 4ψήφιο κωδικό PIN ο οποίος γνωστοποιείται στο χρήστη από τον πάροχο. Σε κάθε χρήστη δίνεται η δυνατότητα για αλλαγή του PIN εφόσον δεν επιθυμεί το προκαθορισμένο. Η κάρτα SIM παρέχει ασφάλεια αφού σε 3 αποτυχημένες προσπάθειες του PIN το τηλέφωνο κλειδώνει κατευθείαν και χρειάζεται ένα άλλον αριθμό που ονομάζεται PUK. Σε περίπτωση 10 λανθασμένων προσπαθειών εισαγωγής του αριθμού PUK η κάρτα καταστρέφεται και δεν γίνεται να χρησιμοποιηθεί ξανά.



Εικόνα 3.1 Κάρτα SIM [12]

Η κάρτα SIM έχει περιορισμένη μνήμη αποθήκευσης. Κάποια από τα αρχεία που αποθηκεύονται στη SIM είναι τα εξής:

- Ο σειριακός αριθμός της κάρτας
- Το δίκτυο που συνδέεται πιο συχνά
- Η γλώσσα του τηλεφώνου
- Περιορισμένος κατάλογος επαφών
- Περιορισμένα εισερχόμενα και εξερχόμενα μηνύματα
- Η προσωρινή ταυτότητα συνδρομητή δικτύου (IMSI-TMSI)
- Αναγνωριστικό ολοκληρωμένου κυκλώματος (ICCID)

Εσωτερική κάρτα μνήμης (Internal Memory)

Η εσωτερική μνήμη είναι αναπόσπαστο κομμάτι του κινητού τηλεφώνου. Όλα τα αρχεία που εισάγονται στο κινητό τηλέφωνο αποθηκεύονται στην εσωτερική μνήμη αφού είναι προεπιλεγμένο από τον κατασκευαστή του τηλεφώνου. Στη εσωτερική μνήμη του τηλεφώνου αποθηκεύονται οι επαφές, οι κλήσεις, τα μηνύματα, οι γεωγραφικές συντεταγμένες, τα γεγονότα του ημερολογίου, οι φωτογραφίες, η μουσική, τα video, προσωπικά αρχεία, ιστορικό πλοήγησης στο διαδίκτυο, τα cookies, κ.λπ. Επίσης, αποθηκεύονται και πληροφορίες από κάρτες που έχουν εισαχθεί κατά καιρούς.

Εξωτερική κάρτα μνήμης (MemoryCard)

Πλέον ο όγκος των δεδομένων που αποθηκεύονται στις έξυπνες κινητές συσκευές αυξάνεται με ραγδαίο ρυθμό, με αποτέλεσμα στις περισσότερες φορές ο προκαθορισμένος χώρος της μνήμης που έχει ο κατασκευαστής να μην επαρκεί. Η εξωτερική κάρτα μνήμης (Memory Card) προσφέρει επιπρόσθετο χώρο μνήμης στις κινητές συσκευές έτσι ώστε οι χρήστες να είναι σε θέση να αποθηκεύουν περισσότερα δεδομένα από ότι προσφέρει η συσκευή.

Εικόνα 3.2 Memory Card [13]

Cloud

Όπως είπαμε και προηγουμένως πλέον στους χρήστες δεν αρκεί ο αποθηκευτικός χώρος που έχει το κινητό από τον κατασκευαστή του εφόσον η απαίτηση τους σε χώρο συνέχεια αυξάνεται. Η μία λύση όπως είπαμε είναι η εξωτερική μνήμη (memory card) και η άλλη το Cloud. Το Cloud είναι μια υπηρεσία αποθήκευσης και συγχρονισμού αρχείων στο διαδίκτυο που ο χρήστης μπορεί να χρησιμοποιήσει αποθηκεύοντας

δεδομένα. Μια τέτοια υπηρεσία παρέχει η Google και ονομάζεται Google Drive στην οποία ο χρήστης μπορεί να αποθηκεύσει δεδομένα δωρεάν μέχρι 15GB.

3.2 Μεθοδολογία Ψηφιακής Έρευνας

Η μεθοδολογία της ψηφιακής εγκληματολογίας υπολογιστών διαφέρει από αυτήν των κινητών συσκευών. Η διαφορά τους έγκειται στην δομή των αρχείων του καθενός, καθώς και στο ότι στις έξυπνες κινητές συσκευές παρέχεται και η δυνατότητα της τηλεπικοινωνίας. Το ίδιο συμβαίνει και με τα εργαλεία της εγκληματολογίας.

Για να θεωρηθεί μια εγκληματολογική έρευνα νόμιμη είτε στους υπολογιστές είτε στις κινητές συσκευές θα πρέπει να τηρούνται 3 στάδια γνωστά ως 3Α τα οποία είναι τα εξής:

Acquire

Σε αυτό το στάδιο γίνεται η απόκτηση των ψηφιακών τεκμηρίων χωρίς τροποποίηση ή αλλοίωση των δεδομένων.

Αρχικά, ο πραγματογνώμονας μόλις πάει στον «τόπο του εγκλήματος» θα πρέπει να φωτογραφίσει την σκηνή του εγκλήματος πριν αφαιρέσει οποιαδήποτε ηλεκτρονική συσκευή και ύστερα να αφαιρέσει τα τεκμήρια προσεκτικά χρησιμοποιώντας γάντια για να μην αλλοιωθούν τυχόν δακτυλικά αποτυπώματα.

Από την στιγμή που ο πραγματογνώμονας αποκτήσει τα τεκμήρια στα χέρια του θα πρέπει να διαφυλάξει τα δεδομένα με την «αλυσίδα επιτήρησης» (Chain of Custody). Η αλυσίδα επιτήρησης περιγράφει ανά πάσα στιγμή που βρίσκεται το τεκμήριο, που φυλάσσεται, από ποιον συλλέχθηκε, τι ώρα, πως προστατεύονται, ποιος το επεξεργάστηκε, πως κλπ.

Οι ειδικοί συλλέγουν στοιχεία όπως: κλήσεις, μηνύματα, ηλεκτρονικά μηνύματα (e-mails), συντεταγμένες τοποθεσίας, κοινωνικά δίκτυα, ηλεκτρονική τράπεζα, ιστορικό φυλλομετρητή, εικόνες, βίντεο, ημερολόγιο, επαφές κλπ.

Authenticate

Σε αυτό το στάδιο γίνεται η πιστοποίηση της αυθεντικότητας των ανακτημένων αποδεικτικών στοιχείων και η επιβεβαίωση της συνάφειάς τους με τα πρωτότυπά κατασχεμένα δεδομένα.

Για καθένα από τα αποδεικτικά στοιχεία που συλλέχθηκαν υπολογίζουν το ψηφιακό αποτύπωμα (hash value) αυτού, για διασφάλιση της ακεραιότητάς του έτσι ώστε να είναι σε θέση να αποδείξουν ότι είναι το ίδιο με το αρχικό και δεν έχει αλλοιωθεί. Για καθένα ψηφιακό πειστήριο που συλλέχθηκε οι πραγματογνώμονες θα πρέπει να καταγράψουν τι ώρα συλλέχθηκε, από ποιον, ποια ημερομηνία, τι ψηφιακό αποτύπωμα έχει, ποιο εργαλείο χρησιμοποίησαν για να το βρουν κλπ.

Μια από τις πιο σημαντικές διαδικασίες που θα πρέπει να υλοποιηθούν είναι δημιουργία πολλαπλών αντιγράφων τα οποία θα φυλάσσονται σε διαφορετικά μέρη σε περίπτωση κάποιας ζημιάς.

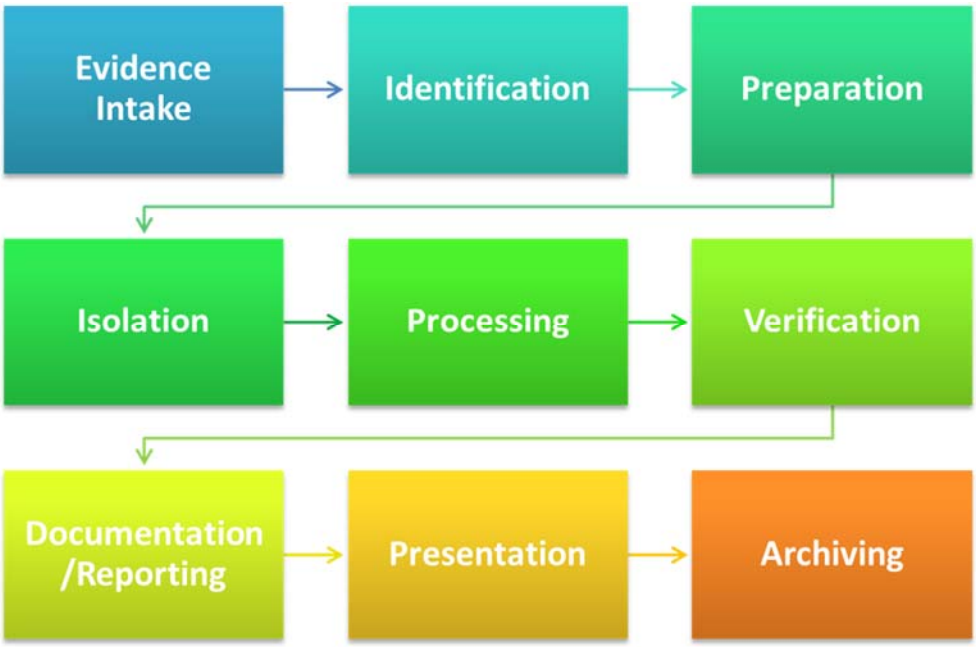
Analyze

Σε αυτό το στάδιο γίνεται η ανάλυση των δεδομένων που συλλέχθηκαν χωρίς οποιεσδήποτε τροποποιήσεις ή παραποιήσεις.

Η πρώτη τους προτεραιότητα είναι η κλωνοποίηση των κινητών τηλεφώνων ώστε να μην επηρεαστούν τα πρωτότυπα δεδομένα. Ύστερα, γίνεται η ανάλυση των δεδομένων με πιστοποιημένα προγράμματα κατάλληλα για εξαγωγή ψηφιακών τεκμηρίων.

Στο τέλος, ο πραγματογνώμονας γράφει την αναφορά του η οποία θα χρησιμοποιηθεί/αξιοποιηθεί καταλλήλως περαιτέρω (π.χ. στο δικαστήριο).

Η ηλεκτρονική έρευνα ενός εγκλήματος είναι μια διαδικασία που διαφέρει αρκετά από την τυπική έρευνα που κάνουν οι αστυνομικοί σε ένα τόπο εγκλήματος. Ο ηλεκτρονικός αναλυτής δεν αναζητά στοιχεία σε κάποιο φυσικό χώρο αλλά σε ηλεκτρονικούς φακέλους, αρχεία και υπολογιστικά συστήματα. Οπότε για να εξασφαλιστεί η εγκυρότητα της διαδικασία θα πρέπει να τηρηθούν τα στάδια της εγκληματολογικής έρευνας.



Εικόνα 3.3 Stages of Mobile Forensics - Analysis Process [14]

3.2.1 Προσδιορισμός του εγκλήματος

Στο πρώτο στάδιο της έρευνας ο ερευνητής της ψηφιακής εγκληματολογίας θα πρέπει να ενημερωθεί σχετικά με την υπόθεση, για παράδειγμα, για ποιο λόγο κατηγορείται ο ύποπτος, αν έχει συλληφθεί κλπ. Αυτές οι πληροφορίες είναι απαραίτητες για τον ερευνητή για να ξέρει προς τα ποια κατεύθυνση θα πρέπει να κινηθεί για να ερευνήσει. Για παράδειγμα, σε περίπτωση που ο ψηφιακός εγκληματολόγος δεν έχει άφθονο χρόνο για να ερευνήσει τις συσκευές τότε θα πρέπει να κάνει διαλογή ψηφιακών πειστηρίων εισάγοντας λέξεις κλειδιά π.χ. ναρκωτικά, φορτίο, ληστεία κλπ. ψάχνοντας για συγκεκριμένα δεδομένα. Η μέθοδος αυτή ονομάζεται triage.

3.2.2 Συλλογή αποδεικτικών στοιχείων

Σε αυτό το στάδιο της έρευνας ο ερευνητής της ψηφιακής εγκληματολογίας είναι υποχρεωμένος για την γραφειοκρατική διαδικασία που είναι μείζονος σημασίας για την καταγραφή της διαδικασίας και όλων των ενεργειών που περιλαμβάνει η ψηφιακή εγκληματολογία. Ο ψηφιακός ερευνητής θα συλλέξει τα αποδεικτικά στοιχεία και θα αξιολογήσει την κατάστασή τους.

Η πρώτη φάση είναι η ενημέρωση του ερευνητή για την υπόθεση που θα αναλάβει έτσι ώστε να έχει μια πλήρη εικόνα της υπόθεσης και για το τι πρέπει να αναζητήσει.

Δεύτερον, θα πρέπει να κάνει αυτοψία στον τόπο του εγκλήματος ώστε να συλλέξει τα ψηφιακά τεκμήρια της υπόθεσης.

Ο τρόπος που θα χειριστεί ο ψηφιακός εγκληματολόγος τις συσκευές που θα κατάσχει αποτελούν ένα μεγάλο μέρος μιας επιτυχημένης διαδικασίας. Πριν κάνει οποιαδήποτε ενέργεια και αλλαγή στα ψηφιακά συστήματα που θα βρει, θα πρέπει πρώτα να τα φωτογραφίσει έτσι ώστε να γνωρίζουν την αρχή τους τοποθεσία, την κατάσταση τους όταν τα βρήκε καθώς την ώρα και την ημερομηνία της κατάσχεσης.

Όλα τα ψηφιακά τεκμήρια που θα βρει ο ερευνητής όπως υπολογιστές, router, laptop, USB sticks, κινητά τηλέφωνα, κινητές συσκευές, ψηφιακές μηχανές, κάμερα, memory sticks κ.λπ. θα πρέπει να μεταφερθούν μέσα σε σακούλες τεκμηρίων στο εργαστήριο ώστε να εξετασθούν εξονυχιστικά από την ομάδα του ερευνητή.

3.2.3 Προσδιορισμός των ψηφιακών συσκευών

Μέρος της έρευνας είναι ο προσδιορισμός των ψηφιακών συσκευών που συλλέχθηκαν από τον τόπο του εγκλήματος καθώς και η καταγραφή τους. Επίσης, θα πρέπει να προσδιοριστούν τα λειτουργικά τους συστήματα, οι εκδόσεις και τα χαρακτηριστικά τους (hardware). Σε αυτό το στάδιο γίνεται η επιλογή και η προετοιμασία των κατάλληλων εργαλείων που θα χρησιμοποιηθούν για την ανάλυση των ψηφιακών πειστηρίων και θα προσδιοριστούν οι τεχνικές ανάλυσης των δεδομένων.

3.2.4 Απομόνωση ψηφιακών συσκευών

Στο συγκεκριμένο στάδιο γίνεται η απομόνωση των ψηφιακών συσκευών. Η συλλογή των ψηφιακών συσκευών θα πρέπει να γίνει προσεκτικά. Θα πρέπει να τοποθετηθούν με γάντια μέσα σε anti-static bags, οι οποίες προστατεύουν τα ηλεκτρονικά εξαρτήματα από τον στατικό ηλεκτρισμό έτσι ώστε να μην αλλοιωθούν τα δεδομένα και τυχόν δαχτυλικά αποτυπώματα πάνω στις συσκευές.

Επίσης, οι συσκευές τοποθετούνται μέσα σε Faraday bags ή isolation box για να απομονωθούν σε τυχόν προσπάθεια του χρήση για σύνδεση με απομακρυσμένη πρόσβαση. Η απομόνωση εμποδίζει την προσθήκη νέων δεδομένων μέσω εισερχόμενων κλήσεων και μηνυμάτων τα οποία έχουν ως σκοπό τους την καταστροφή των δεδομένων από απομακρυσμένη πρόσβαση [14]. Οποιαδήποτε επικοινωνία της

συσκευής με εξωτερικούς παράγοντας θα πρέπει να αποτραπεί έτσι ώστε ο χρήστης να μην μπορεί μέσω του λογαριασμού του να διαγράψει τα δεδομένα της συσκευής.

Οι ενέργειες του ερευνητή θα πρέπει να είναι προσεκτικές ώστε να μην χαθούν τα δεδομένα που μπορούν να αποδείξουν την ενοχή ή την αθωότητα του κατηγορούμενου.

3.4 Faraday bags [15]

3.2.5 Δημιουργία μας αλυσίδας φύλαξης (Chain of Custody)

Εφόσον ο ψηφιακός εγκληματολόγος πάρει στα χέρια του τα ψηφιακά τεκμήρια είναι υπεύθυνος γι' αυτά και θα πρέπει να τα διαφυλάξει σε ένα ασφαλές μέρος έτσι ώστε να μην μπορούν να τροποποιηθούν. Επιπλέον, είναι απαραίτητο ο ερευνητής να κρατήσει μερικά αντίγραφα των στοιχείων έτσι ώστε μην τυχόν χαθούν ή καταστραφούν από λάθος.

Το πιο σημαντικό βέβαια σε αυτό το στάδιο είναι να τηρηθεί μια αλυσίδα φύλαξης των ψηφιακών τεκμηρίων. Πιο συγκεκριμένα, θα πρέπει να καταγράφονται τα ψηφιακά αποτυπώματα των δεδομένων, οι ημερομηνίες, οι ώρες επεξεργασίας των δεδομένων, ποιος τα επεξεργάζεται, με ποιές διαδικασίες, ποιά προγράμματα χρησιμοποίησε, πού αποθηκεύονται και γενικά να καταγράφονται τα πάντα γύρω από τα δεδομένα ώστε να εξασφαλιστεί η ακεραιότητα αυτών.

3.2.6 Ανάλυση των αποδεικτικών στοιχείων – χρήση πιστού αντιγράφου

Πρώτα από όλα δημιουργούνται πιστά αντίγραφα των δεδομένων έτσι ώστε να εξασφαλιστεί η ασφάλεια τους. Σε αυτό το στάδιο γίνεται η ανάλυση των δεδομένων με κατάλληλα εργαλεία και τεχνικές που προσδιορίσαμε σε προηγούμενο στάδιο.

Ταυτόχρονα με την ανάλυση των δεδομένων συντάσσονται οι αναφορές από τους ερευνητές για τα ψηφιακά ευρήματα τηρώντας και καταγράφοντας και την αλυσίδα φύλαξης.

3.2.7 Παρουσίαση των αποδεικτικών στοιχείων/τεκμηρίων

Στο συγκεκριμένο στάδιο παρουσιάζονται όλα τα αρχεία που βρέθηκαν από τις «έξυπνες» ψηφιακές συσκευές. Δίνεται περισσότερη έμφαση στα ευρήματα που αφορούν την υπόθεση καθώς και σε λοιπά ευρήματα που θεωρούνται άξια λόγου.

Όλα τα δεδομένα που ανακτήθηκαν αρχικά από το τηλέφωνο ή το tablet, η ανάλυσή τους, τα αντίγραφα των δεδομένων, οι φωτογραφίες από την αρχική θέση των ψηφιακών συσκευών στον τόπο του εγκλήματος και όλες οι αναφορές που γράφτηκαν αρχειοθετούνται και φυλάσσονται σε ειδικά μέρη έτσι ώστε χρησιμοποιηθούν σε ενδεχόμενη μελλοντική χρήση.

3.2.8 Μαρτυρία / Κατάθεση

Σε αυτό το στάδιο ο ερευνητής αν θεωρηθεί απαραίτητο θα κληθεί να παραστεί στην αίθουσα του δικαστηρίου έτσι ώστε να καταθέσει σύμφωνα με τα ευρήματα που βρήκε στην ψηφιακή του έρευνα. Θα πρέπει να είναι απόλυτα προετοιμασμένος για την αξιοπιστία των ψηφιακών τεκμηρίων καθώς και για τα αποτελέσματα που προέκυψαν. Ο ερευνητής θα συντάξει μια αναφορά για τα στοιχεία που πήρε από τις «έξυπνες» κινητές συσκευές που εξέτασε, τις φωτογραφίες που έβγαλε και τα συμπεράσματα που πάρθηκαν από όλη την εξέταση των πειστηρίων.

3.2.9 Ποινική δίωξη

Ο ψηφιακός εγκληματολόγος ενεργεί και ως πραγματογνώμονας. Ο πραγματογνώμονας διαθέτει ειδικές επιστημονικές ή τεχνικές γνώσεις πάνω στην Ψηφιακή Εγκληματολογία και καλείται να εξετάσει την κατάσταση, να δώσει τη γνώμη του καθώς και να εκτιμήσει την έκταση της ζημιάς και το κόστος της αποκατάστασης της.

Η έκθεση που συντάσσει ο πραγματογνώμονας αποτελεί αυτοτελές αποδεικτικό μέσο, το οποίο και εκτιμάται ελεύθερα από το δικαστήριο. Ο πραγματογνώμονας απαντά

εμπεριστατωμένα σχετικά με τους υπάρχοντες ή πιθανούς κινδύνους καθώς και με την πρόληψη ή την ανάληψή τους.

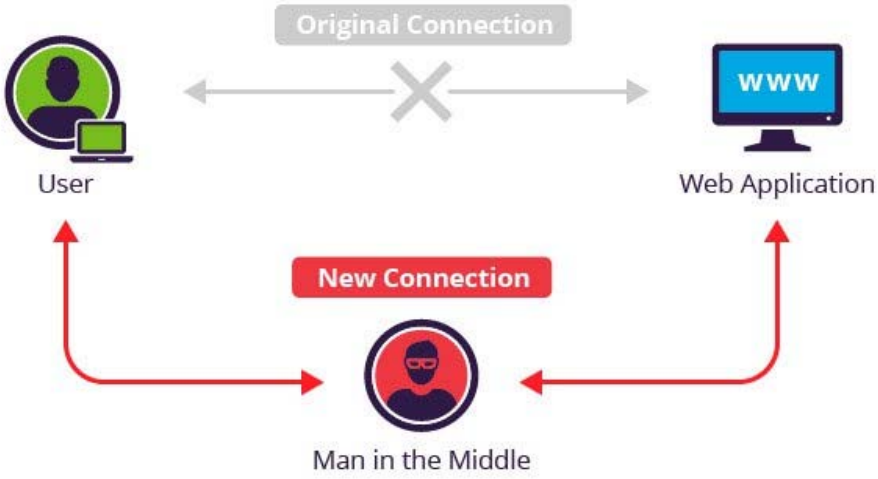
Κεφάλαιο 4
Περιβάλλον Δοκιμών

Οι άνθρωποι χρησιμοποιούν όλο και περισσότερο την τεχνολογία με αποτέλεσμα πλέον οι περισσότερες ψηφιακές τους «εκκρεμότητες» να γίνονται από τις «έξυπνες» κινητές συσκευές τους, είτε αυτό αφορά μια συναλλαγή με την τράπεζα, είτε αφορά την ψυχαγωγία τους με τα κοινωνικά δίκτυα ή ακόμα και ηλεκτρονικές αγορές. Στα δεδομένα τα οποία υφίστανται επεξεργασία μέσω «έξυπνων» κινητών συσκευών συγκαταλέγονται και κρίσιμα προσωπικά δεδομένα όπως δεδομένα πιστωτικών καρτών, κωδικοί πρόσβασης κλπ. , τα οποία πρέπει να μείνουν ασφαλή.

Ένα από τα πιο σημαντικά ζητήματα της ασφάλειας στις «έξυπνες» κινητές συσκευές είναι η κρυπτογράφηση των δεδομένων πριν αποσταλούν μέσω του διαδικτύου. Αυτό θα επιτευχθεί, όπως και σε κάθε άλλη διαδικτυακή επικοινωνία, μέσω πρωτοκόλλου HTTPS (Hypertext Transfer Protocol Secure). Το πρωτόκολλο HTTPS είναι ο συνδυασμός του πρωτοκόλλου HTTP με το πρωτόκολλο κρυπτογράφησης SSL/TLS (Secure Sockets Layer/Transport Layer Security).

Ο συνδυασμός των HTTP και SSL/TLS πρωτοκόλλων παρέχουν την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Για την αυθεντικοποίηση των δεδομένων θα πρέπει να γίνει χρήση ψηφιακών πιστοποιητικών υπογεγραμμένα από έμπιστη τρίτη ανεξάρτητη οντότητα.

Για να θεωρηθεί μια σύνδεση ασφαλής θα πρέπει να μην μπορεί κάποια ενδιάμεση οντότητα να «διαβάσει» τα δεδομένα που αποστέλλονται μέσω διαδικτύου. Τέτοιες επιθέσεις είναι γνωστές και ως “Man in the middle”. Αυτή η επίθεση επιτυγχάνεται εφόσον χρησιμοποιηθεί ένα ψεύτικο ψηφιακό πιστοποιητικό από την ενδιάμεση οντότητα το οποίο θα εκληφθεί, λανθασμένα, ως έγκυρο από τον αποστολέα των μηνυμάτων. Οι περισσότερες εφαρμογές δεν μπορούν να ξεχωρίσουν ή να επαληθεύσουν ένα πιστοποιητικό αν είναι έγκυρο ή όχι.



Εικόνα 4.1 Man in the Middle Attack [16]

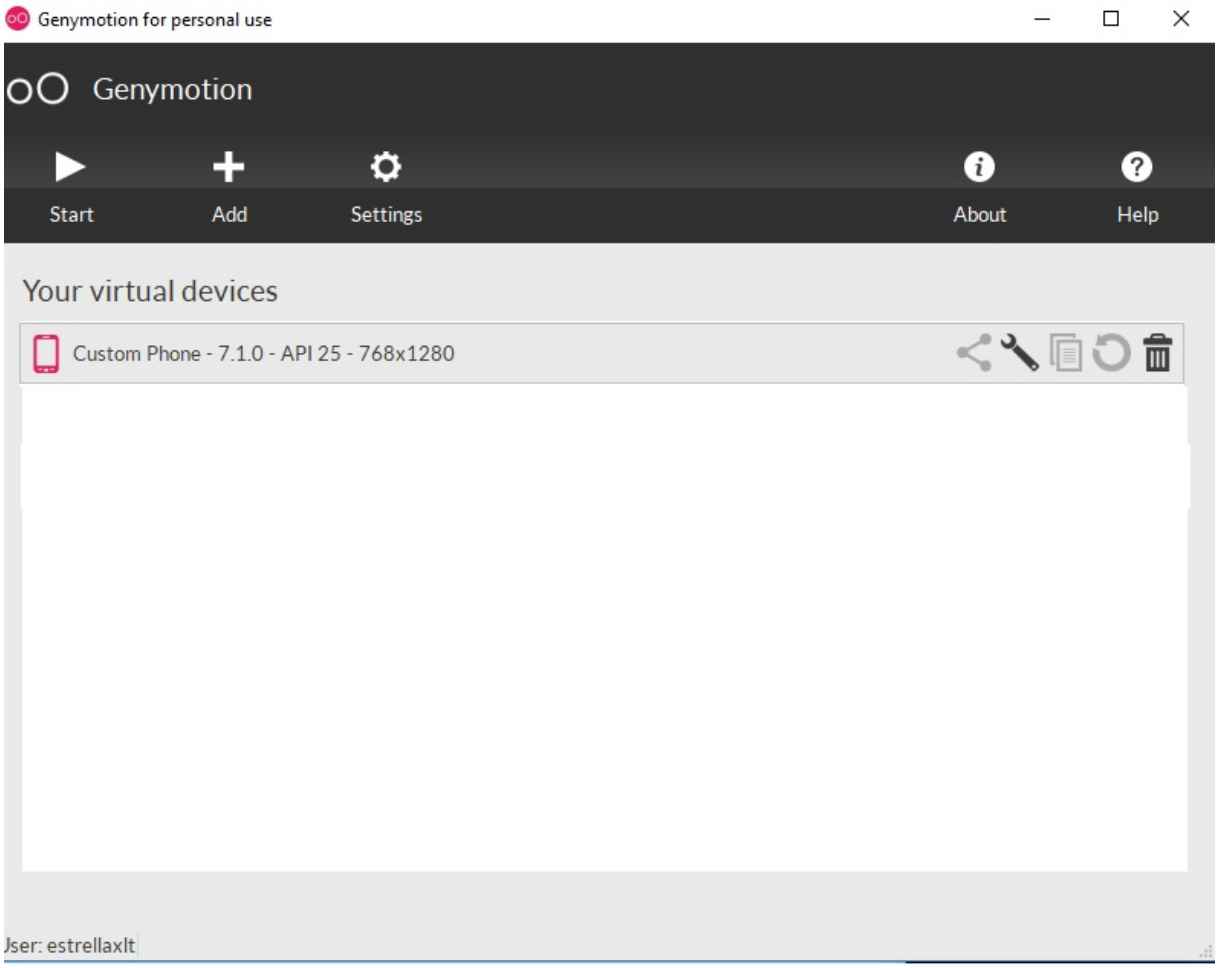
Βασικό τμήμα της ανάλυσης ψηφιακών πειστηρίων είναι η εξέταση του τι «κάνουν» εγκατεστημένες «έξυπνες» εφαρμογές σε πραγματικό χρόνο. Σε περιπτώσεις ωστόσο όπου τα εξερχόμενα από τις εφαρμογές δεδομένα είναι κρυπτογραφημένα μέσω του πρωτοκόλλου SLL/TLS, δεν είναι άμεσα εφικτή η ανάγνωσή τους. Σε αυτές τις περιπτώσεις, η ανάλυση των εφαρμογών μπορεί να γίνει μόνο αν «ανακατευθύνουμε» την εξερχόμενη κίνηση σε HTPS εξυπηρετητή που είναι υπό τον έλεγχο μας, έτσι ώστε να μπορούμε να αποκρυπτογραφήσουμε τα δεδομένα - δηλαδή, με άλλα λόγια, να ακολουθήσουμε μια τεχνική επίθεσης «Man in the Middle». Ως εκ τούτου για το πρακτικό τμήμα της παρούσας διατριβής, θα προσομοιώσουμε την επίθεση «Man in the Middle» για να μπορέσουμε να «διαβάζουμε» τα εξερχόμενα κρυπτογραφημένα δεδομένα μας πριν κρυπτογραφηθούν.

Δημιουργία περιβάλλοντος δοκιμών

Σε αυτό το στάδιο της μεταπτυχιακής διατριβής θα δημιουργήσουμε το περιβάλλον το οποίο θα θεωρηθεί η βάση της πρακτικής διαδικασίας όπου θα γίνουν οι δοκιμές. Το εργαστήριο μας αποτελείται από ένα φορητό υπολογιστή (laptop) κατασκευής Acer με λειτουργικό σύστημα Windows 10, ένα εικονικό κινητό τηλέφωνο (Virtual Machine) με λειτουργικό Android 7.1.1 Nougat rooted, έναν Proxy ο οποίος εκτελείται στον φορητό υπολογιστή και μια ασύρματη σύνδεση στο διαδίκτυο Wi-Fi.

4.1 Genymotion

Για να πραγματοποιήσουμε το πρακτικό κομμάτι της μεταπτυχιακής διατριβής θα χρησιμοποιήσουμε μια εικονική «έξυπνη» κινητή συσκευή. Το περιβάλλον προσομοίωσης Android ονομάζεται Genymotion [17] το οποίο είναι εγκαταστημένο στον υπολογιστή μας.

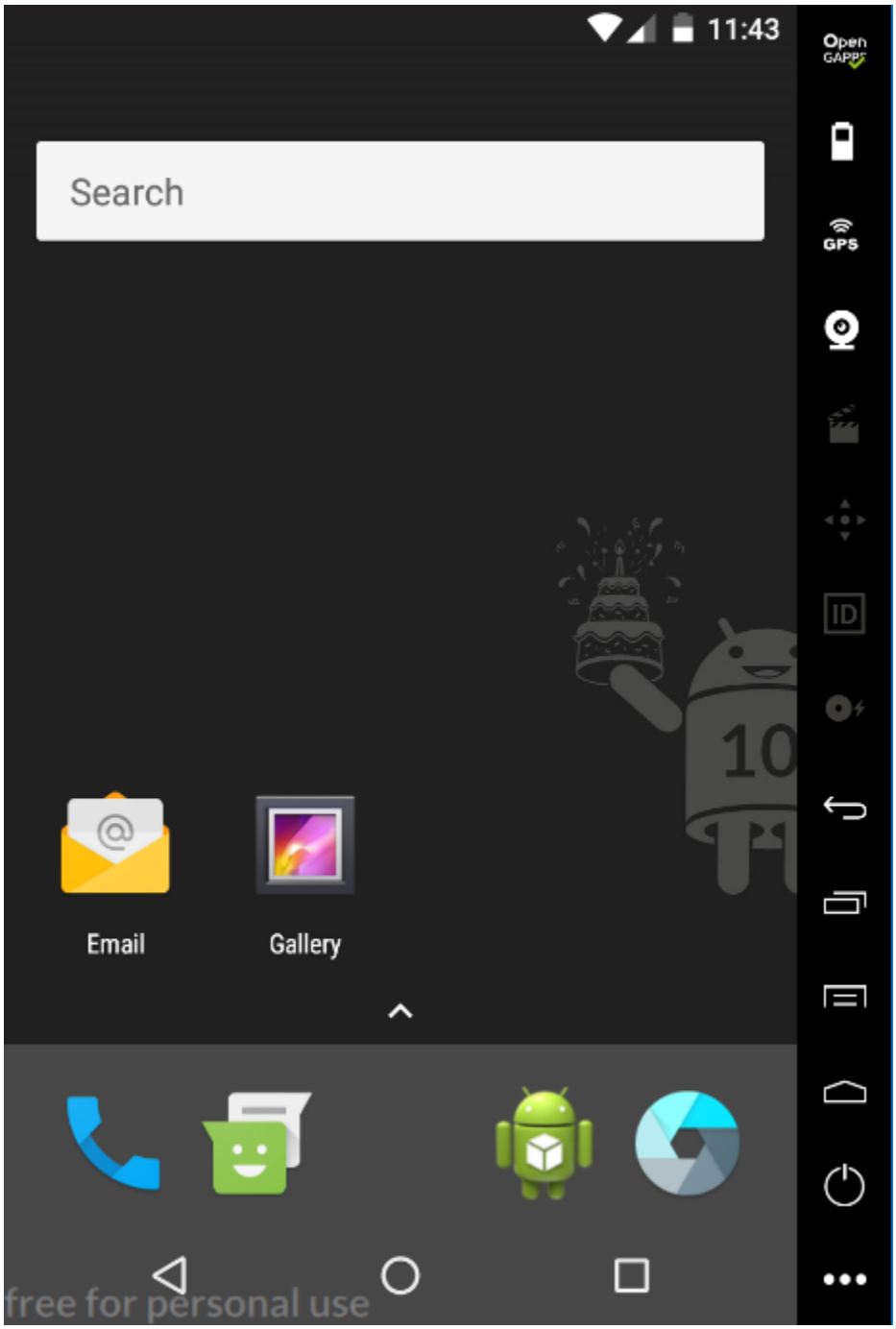


Εικόνα 4.2 Γραφικό Περιβάλλον Genymotion

Το εικονικό τηλέφωνο που θα χρησιμοποιήσουμε έχει λειτουργικό σύστημα Android 7.1.1 Nougat.

Εικόνα 4.3 Λειτουργικό Android

Δυο από τα μειονεκτήματα του Genymotion είναι πρώτον, ότι η αρχιτεκτονική του επεξεργαστή του είναι x86 και δεύτερον, ότι δεν έχει ενσωματωμένα τα Google Apps. Για να εγκαταστήσουμε τα Google Apps θα πρέπει να «αλλάξουμε» την αρχιτεκτονική του επεξεργαστή από x86 σε ARM. Για αυτό το λόγο θα εγκαταστήσουμε το Genymotion ARM Translation [18]. Το επόμενο βήμα θα είναι να ενσωματώσουμε τα Google Apps [18].

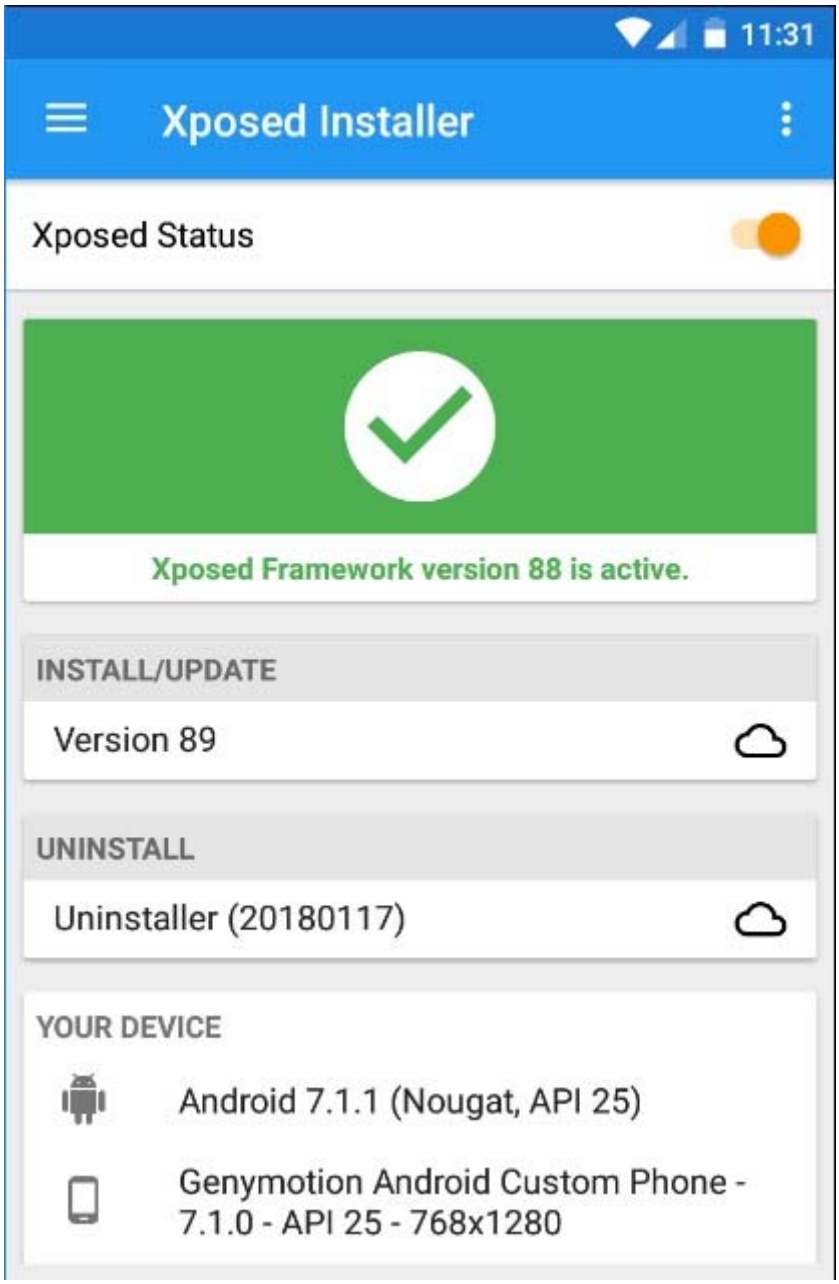


Εικόνα 4.4 Android 7.1.1 Nougat

Θα πρέπει στο λειτουργικό μας σύστημα να δώσουμε δικαιώματα υπερ-χρήστη έτσι ώστε να μπορέσει να εκτελέσει εφαρμογές που το απαιτούν. Rooting είναι η διαδικασία όπου επιτρέπει σε συσκευές Android να παρακάμψουν τα όρια που έχουν βάλει οι κατασκευαστές και οι διανομείς του υλικού και του λογισμικού της «έξυπνης» κινητής συσκευής.

4.2 Xposed Framework

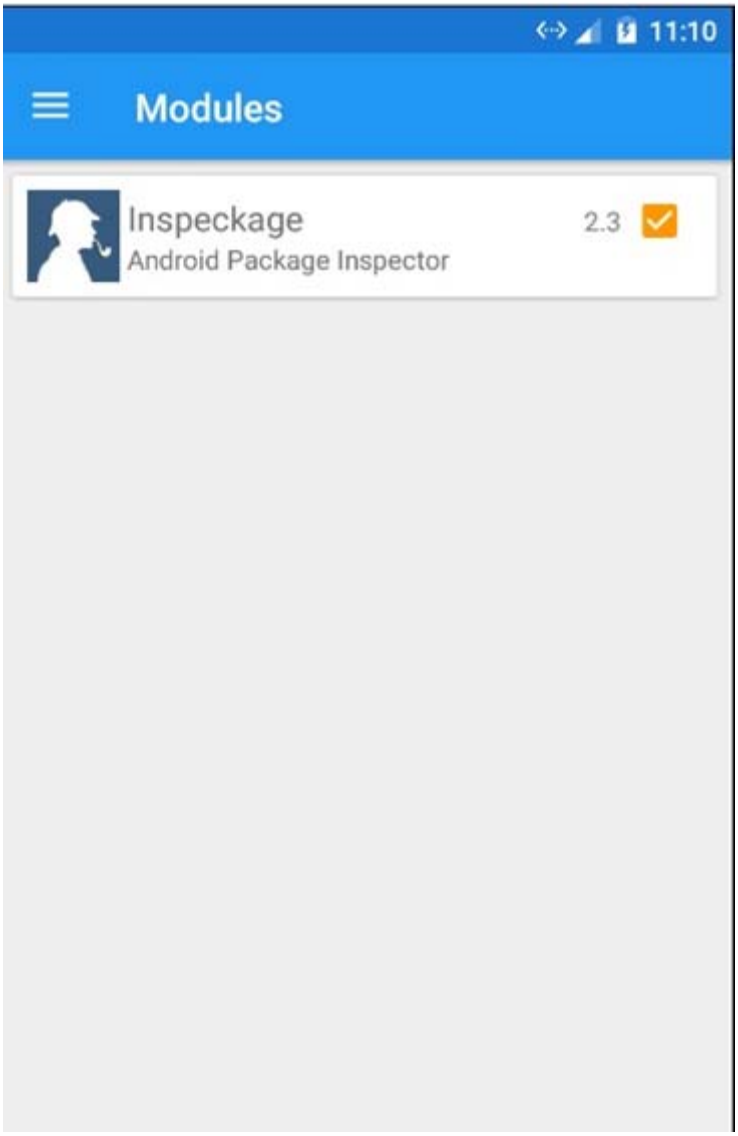
Το επόμενο μας βήμα είναι να εγκαθιστούμε το Xposed Framework [19] στην εικονική μας συσκευή το οποίο μας βοηθάει να κάνουμε αλλαγές στο σύστημά μας χωρίς να κάνουμε compile και recompile τα .apk και το Xposed Installer [20].



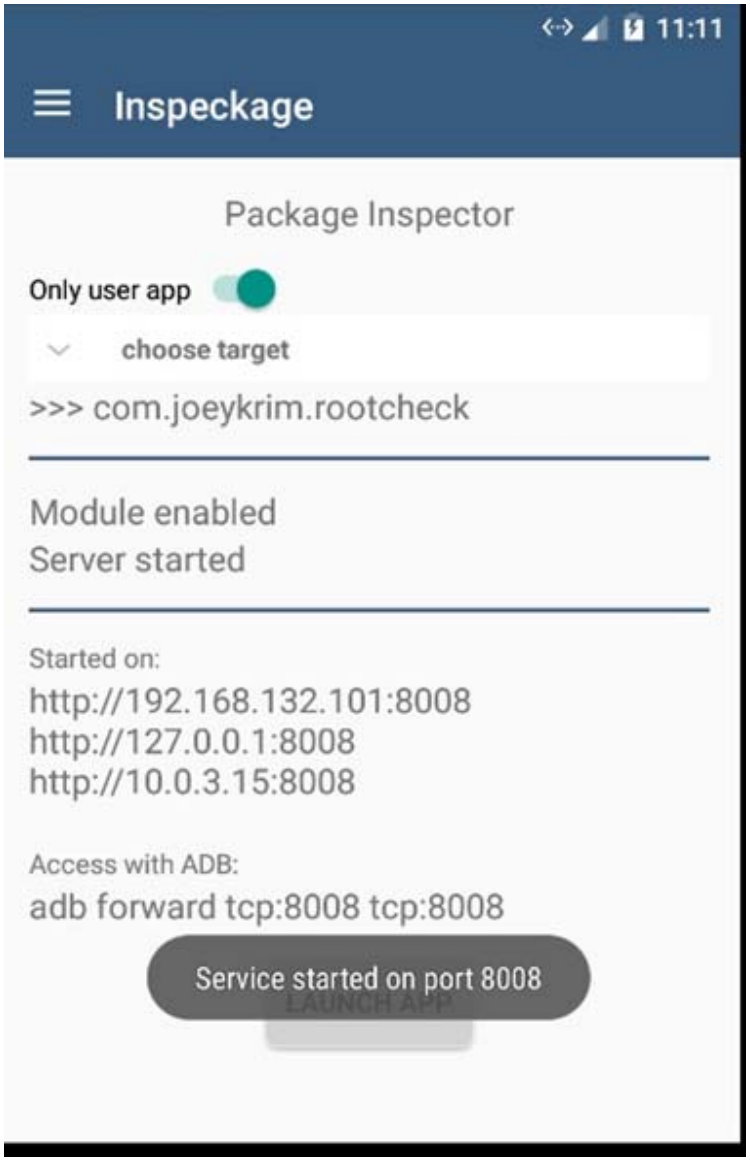
Εικόνα 4.5 Xposed Installer

4.3 Inspeckage

Οι επόμενες εφαρμογές που θα προσθέσουμε είναι το Inspeckage [21] η οποία κάνει δυναμική ανάλυση των εφαρμογών.



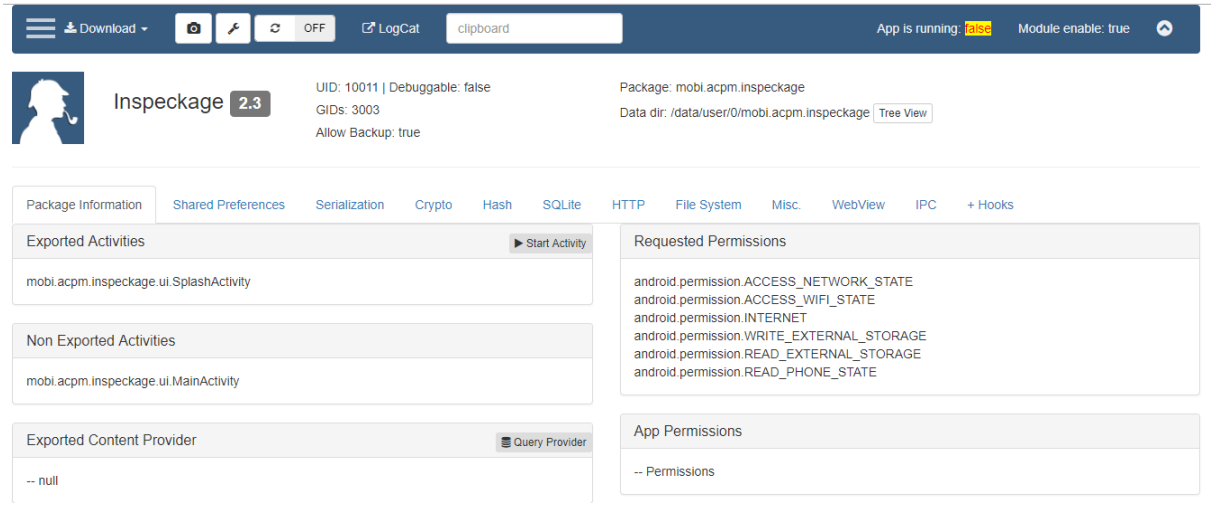
Εικόνα 4.6 Inspeckage Module



Εικόνα 4.7 Inspeckage - Package Inspector

Εφόσον πληκτρολογήσουμε στο ADB την εντολή «a*db forward tcp:8008 tcp:8008*» τότε θα μπορέσουμε να δούμε το interface του Inspeckage. Πληκτρολογούμε στο browser μας το url 127.0.0.1:8008.

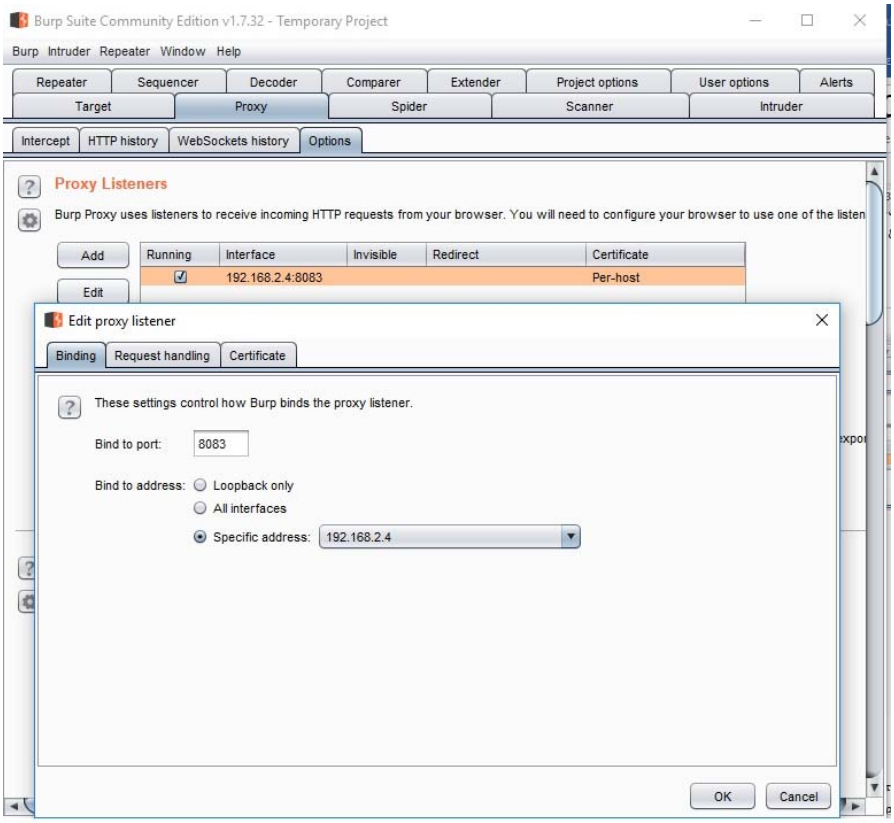
Στην παρακάτω εικόνα εμφανίζεται το interface της εφαρμογής Inspeckage.



Εικόνα 4.8 Interface of Inspeckage

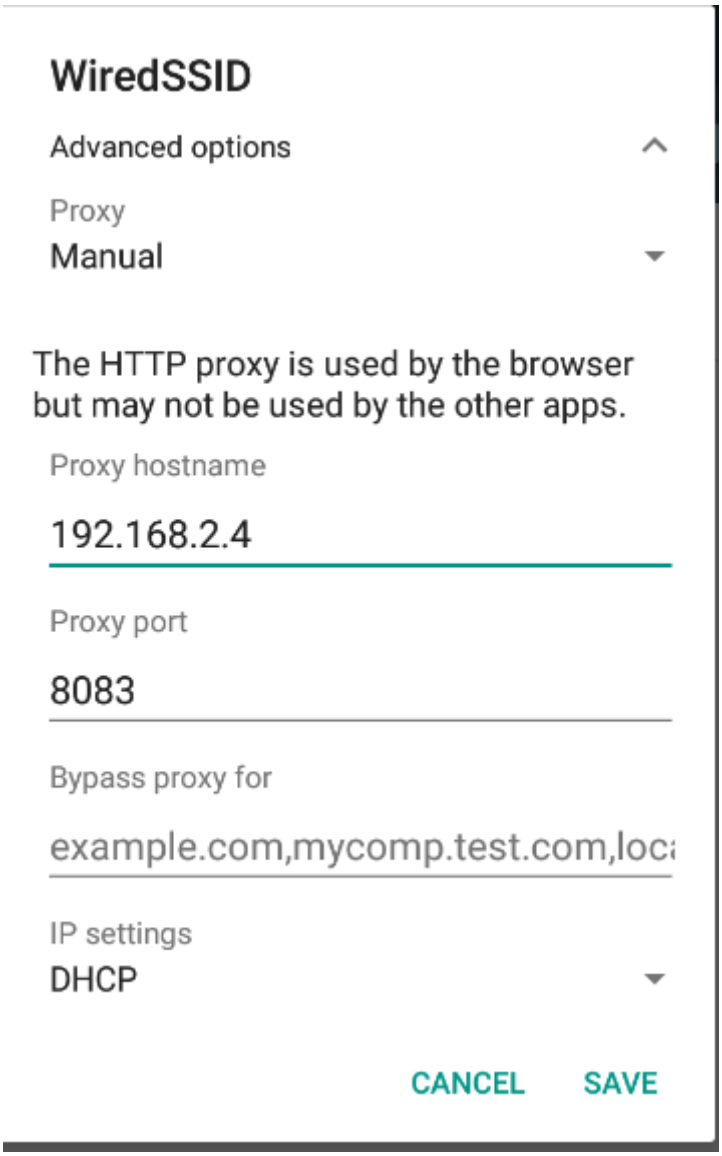
4.4 Burp Suite

Ως Proxy θα χρησιμοποιήσουμε το Burp Suite από το οποίο θα περνάνε όλα τα δεδομένα που εξέρχονται από το κινητό μας για να μπορέσουμε να τα «διαβάσουμε». Το έχουμε εγκαταστήσει στον υπολογιστή (laptop). Θα πρέπει να δώσουμε ως IP διεύθυνση, την IP του υπολογιστή που τρέχει τον proxy.



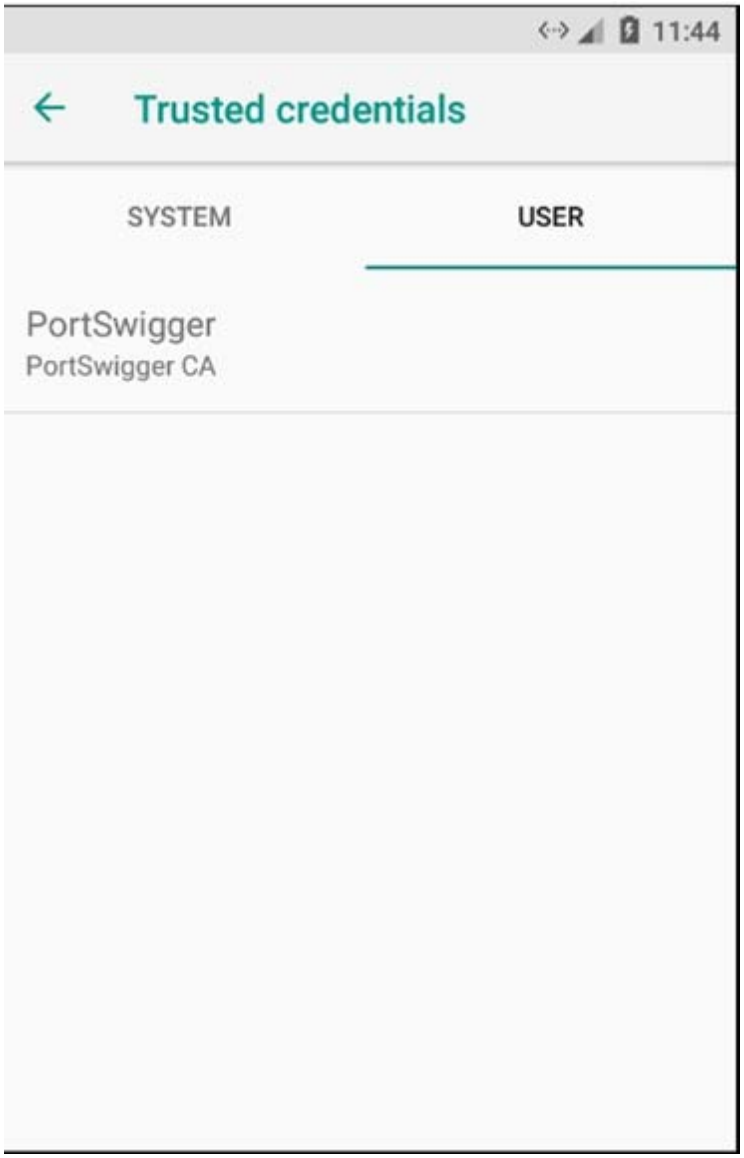
Εικόνα 4.9 Burp Suite- Proxy Listerners

Στην εικονική «έξυπνη» συσκευή θα αλλάξουμε τις ρυθμίσεις του δικτύου μας και θα δώσουμε ως όνομα proxy την διεύθυνση του IP του υπολογιστή που «τρέχει» τον proxy και ως θύρα (port) την 8083.



Εικόνα 4.10 Smartphone - Proxy's Settings

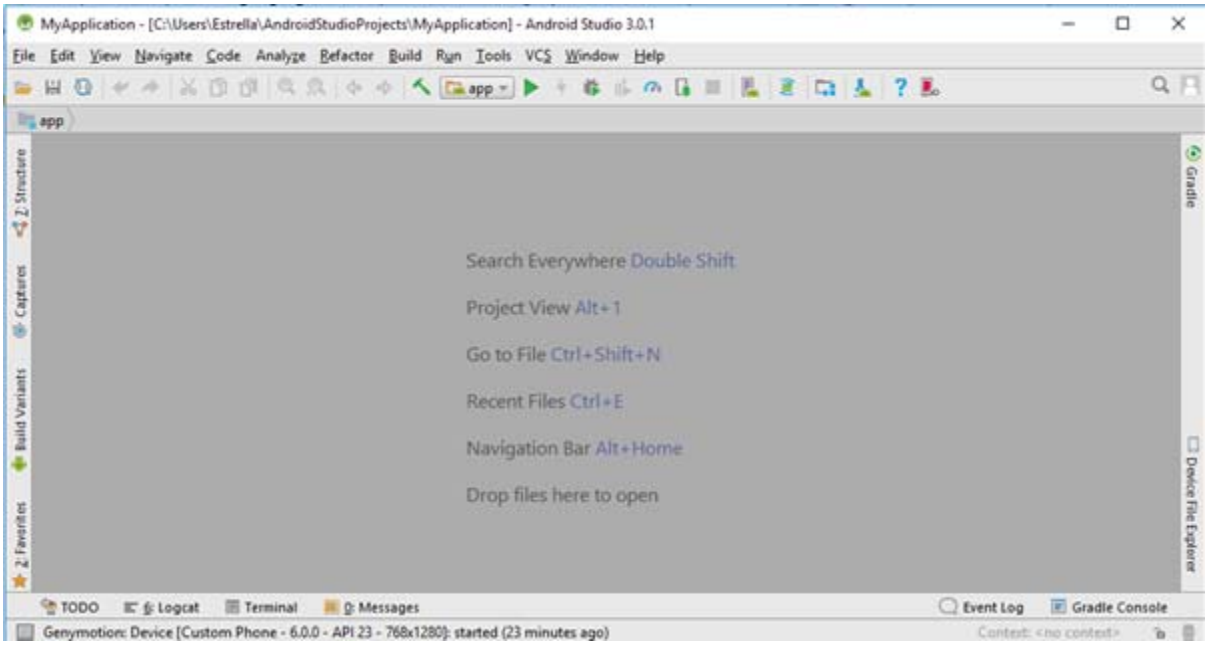
Το τελευταίο μας βήμα είναι να κατεβάσουμε το ψηφιακό πιστοποιητικό του Burp Suite και να το εγκαταστήσουμε στο κινητό μας.



Εικόνα 4.11 Εγκατάσταση ψηφιακού πιστοποιητικού από Burp Suite στην εικονική συσκευή

4.5 Android Studio & SDK Tools

Για να μπορέσουμε να έχουμε πρόσβαση στην εικονική έξυπνη συσκευή μας θα χρησιμοποιήσουμε το Android Studio και το SDK Tools [22] τα οποία είναι και αυτά εγκαταστημένα στον προσωπικό υπολογιστή μας. Η παρουσία του συγκεκριμένου εργαλείου θεωρείται απαραίτητη εφόσον λειτουργεί ως client-server και παρέχει επικοινωνία μεταξύ του ερευνητή και της συσκευής. Η επικοινωνία γίνεται μέσω command lines.



Εικόνα 4.12 Android Studio

Κεφάλαιο 5
Εγκληματολογικά Εργαλεία-Ανάλυση

Εξ' αιτίας του γεγονότος ότι οι «έξυπνες» κινητές συσκευές γίνονται όλο και περισσότερο ποικίλες και πολύπλοκες, ο τομέας των mobile forensics είναι συνεχώς εξελισσόμενος με αναπτυσσόμενες μεθόδους, εργαλεία και συσκευές.

Υπάρχουν πολλά εγκληματολογικά εργαλεία για τις «έξυπνες» κινητές συσκευές όπως για παράδειγμα NowSecureForensics, AcceessData'sMP3+, CellebriteUFED, EnCaseForensics, MicroSystemationXRY, FINALDATA, FINALMobileForensics, Latern 3, LogicubeCellXtract, MOBILeditForensic, OxygenForensicSuite, ParabenDeviceSeizure, PhoneForensicsExpress, RadioTacticsAthena, SecureView [23].

Σε αυτό το κεφάλαιο θα δοκιμάσουμε 5 εγκληματολογικά εργαλεία για «έξυπνες» κινητές συσκευές και θα πραγματοποιήσουμε δυναμική ανάλυση αυτών έτσι ώστε να δούμε τα δεδομένα που λήφθηκαν από αυτές, καθώς επίσης και αν υπάρχουν ευαίσθητα προσωπικά δεδομένα τα οποία αποστέλλονται σε μη εξουσιοδοτημένα άτομα. Τα εργαλεία που θα εξετάσουμε είναι τα εξής: AFLogical – OSE, Foroboto, το Dumpsys, το DiskDigger και το Google Takeout. Τα συγκεκριμένα εργαλεία επιλέχθηκαν για δύο λόγους: πρώτον, γιατί είναι δωρεάν και δεύτερον, γιατί αποτελούν βασικά εργαλεία της εγκληματολογίας [24,25,26,27,28]. Το γεγονός ότι τα εν λόγω εργαλεία διατίθενται δωρεάν προσδίδει και μια πρόσθετη διάσταση στην εν λόγω έρευνα, διότι καθίσταται σαφές ότι μπορούν εύκολα να χρησιμοποιηθούν και από άτομα εκτός του χώρου της ψηφιακής εγκληματολογίας, προκειμένου να συλλέξουν προσωπικά δεδομένα από μια «έξυπνη» κινητή συσκευή (όχι μόνο για νόμιμο αλλά – δυστυχώς – και για παράνομο σκοπό).

5.1 AFLogical – OSE

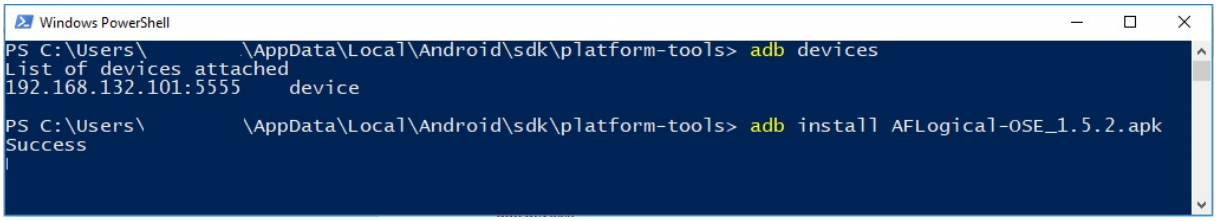
Εικόνα 5.1 Via Forensics [29]

Το AFLogical-OSE κυκλοφόρησε τον Δεκέμβριο του 2011 και τώρα διανέμεται από την GitHub [10]. Η έκδοση ανοιχτού κώδικα δημιουργήθηκε για άτομα με την δικαιοδοσία της επιβολής του νόμου και για ψηφιακούς εγκληματολόγους. Επιτρέπει σε έναν εξεταστή να εξάγει κλήσεις (Call Logs), επαφές (Contacts Phones), εικονομηνύματα (MMS) και μηνύματα (SMS).

Από τον υπολογιστή θα εγκαταστήσουμε την εφαρμογή στην «έξυπνη» κινητή συσκευή μας με την βοήθεια του ADB πληκτρολογώντας τις παρακάτω εντολές:

adb devices

adb install AFLogical-OSE_1.5.2.apk



Εικόνα 5.2 Εγκατάσταση της εφαρμογής AFLogical στην "έξυπνη" κινητή συσκευή μέσω εντολών του ADB

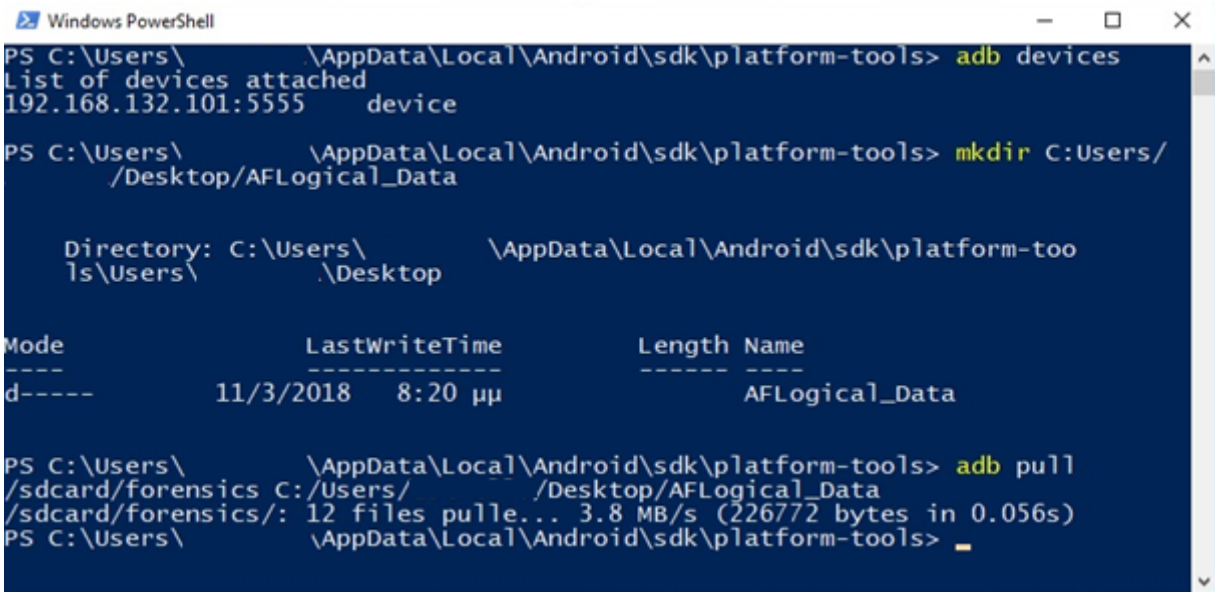
Στην παρακάτω εικόνα φαίνεται ότι η εφαρμογή έχει εγκατασταθεί στην «έξυπνη» εικονική συσκευή μας.

Εικόνα 5.3 Γραφικό περιβάλλον AFlogical

Πατώντας την Επιλογή Capture η εφαρμογή αποθηκεύει τα δεδομένα που θέλουμε στη διαδρομή /sdcard/forensics. Τώρα θα πρέπει να μεταφέρουμε τα δεδομένα που λήφθηκαν από την εφαρμογή στον υπολογιστή μας.

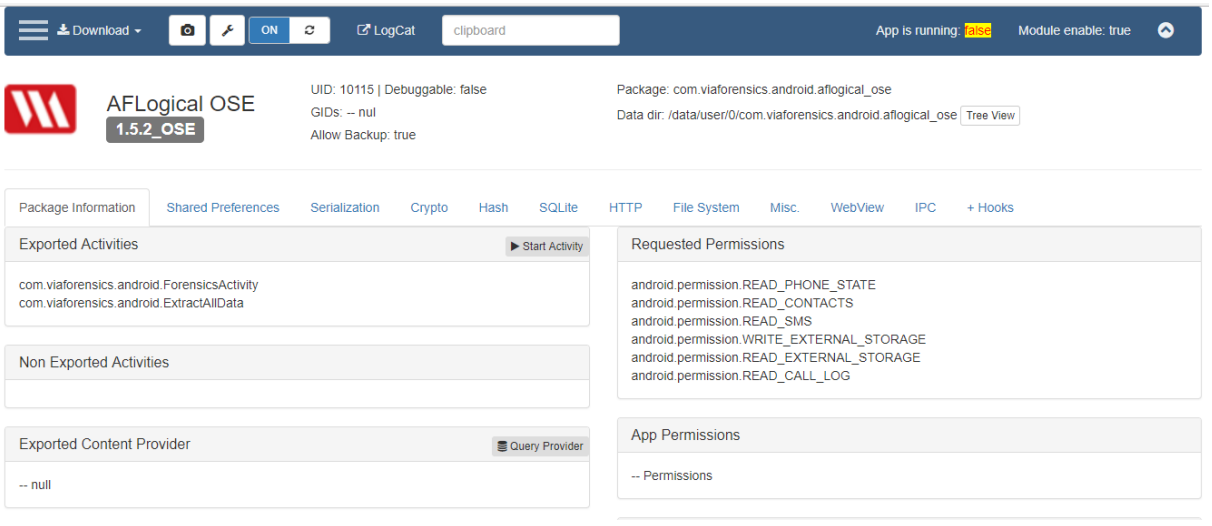
mkdir C:/Users/…/Desktop/AFLogical_Data

adb pull /sdcard/forensics C: /Users/…/Desktop/AFLogical_Data



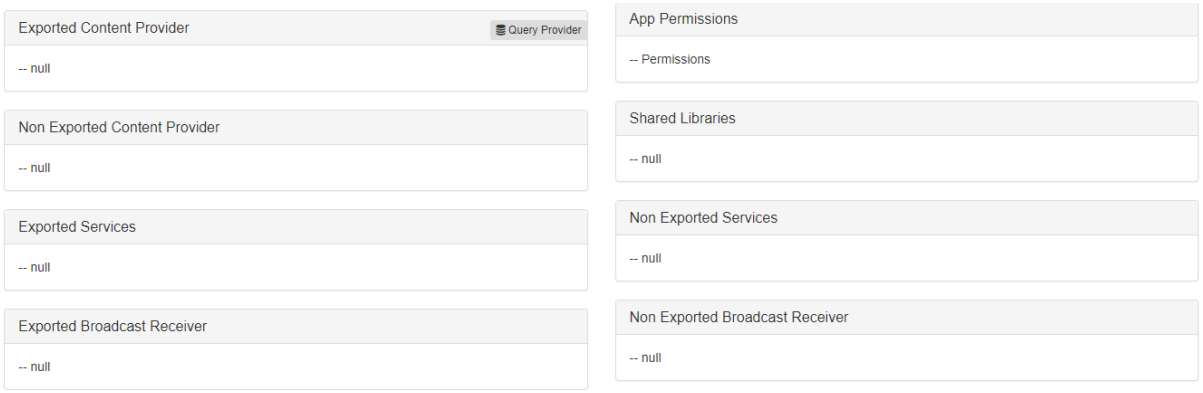
Εικόνα 5.4 Δημιουργία Φακέλου "AFLogical_Data" και αντιγραφή αρχείων από τον Φάκελο Forensics της SDCard στον φάκελο του υπολογιστή μας "AFLogical_Data"

Η δυναμική ανάλυση της εφαρμογής AFLogical – OSE θα γίνει με τη βοήθεια της εφαρμογής Inspeckage. Η εφαρμογή αποθηκεύει τα δεδομένα που εξάγει από το κινητό στον φάκελο /sdcard/forensics.

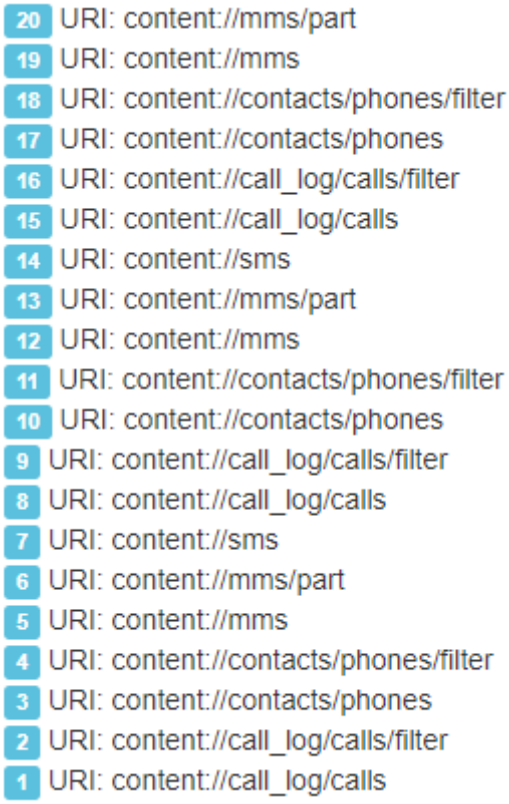


Εικόνα 5.5 Δυναμική Ανάλυση της εφαρμογής AFLogical μέσω Inspeckage I

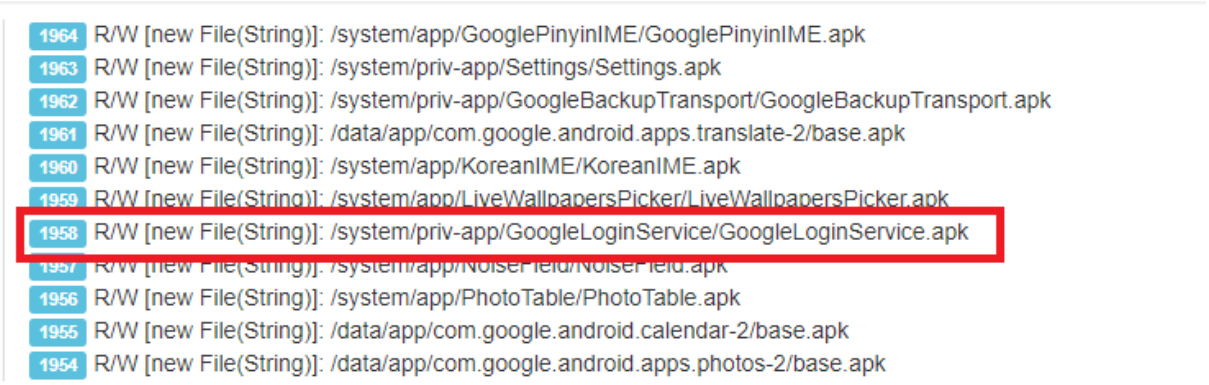
Όπως βλέπουμε στην παραπάνω εικόνα η εφαρμογή εξάγει από την «έξυπνη» κινητή συσκευή τις επαφές, τα sms και τις κλήσεις. Επίσης, ζητάει να αποκτήσει δικαιώματα στο να γράψει στην sdcard και να διαβάσει τα δεδομένα από αυτήν.



Εικόνα 5.6 Δυναμική Ανάλυση της εφαρμογής AFLogical μέσω Inspeckage II



Εικόνα 5.7 Λίστα με URI

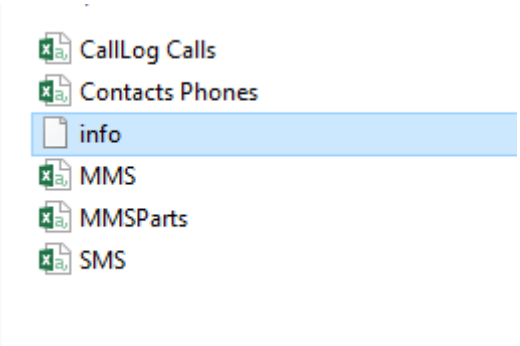


Εικόνα 5.8 Πρόσβαση της εφαρμογής "AFLogical" σε διάφορα αρχεία

Η εφαρμογή εκτός από τα δεδομένα που σκοπεύει να εξάγει αποκτά πρόσβαση και στα αρχεία που αφορούν τα Logins στις υπηρεσίες της Google και στο Captive Portal.

Εικόνα 5.9 Πρόσβαση της εφαρμογής AFLogical σε αρχείο "Captive Portal Login"

Τα αρχεία που συνέλλεξε η εφαρμογή από την «έξυπνη» κινητή συσκευή είναι τα παρακάτω:



Εικόνα 5.10 Αρχεία που ανακτήθηκαν από το AFLogical

Το αρχείο με όνομα info περιέχει στοιχεία της «έξυπνης» κινητής συσκευής που την περιγράφουν.

```
<android-forensics>
<date-time>20180312.1944</date-time>
<IMSI>310270000000000</IMSI>
<IMEI-MEID>000000000000000</IMEI-MEID>
<phone-type>1</phone-type>
<MSISDN-MDN>15555218135</MSISDN-MDN>
<ICCID>89014103211118510720</ICCID>
<build>
      <version.release>7.1.1</version.release>
      <version.sdk>25</version.sdk>
      <version.incremental>25</version.incremental>
      <board>unknown</board>
      <brand>Android</brand>
      <device>vbox86p</device>
      <display>vbox86p-userdebug 7.1.1 NMF26Q 25 test-
keys</display>
      <fingerprint>
```

Εικόνα 5.11 Πληροφορίες αρχείου Info

Αναφέρει την ημερομηνία διεξαγωγής της διαδικασίας 12/03/2018 και ώρα 19:44, τον αριθμό IMSI 310270000000000, τον αριθμό IMEI ο οποίος είναι μηδενικός επειδή η συσκευή είναι εικονική, το ICCID 89014103211118510720 και το λειτουργικό σύστημα της συσκευής Android έκδοση 7.1.1.

5.2 Foroboto

Το συγκεκριμένο εγκληματολογικό εργαλείο αυτοματοποιεί την ανάκτηση των δεδομένων από Android συσκευές μέσω ADB. Η ανάλυση γίνεται σε 5 διαφορετικά επίπεδα (levels), με το 1 να είναι το χαμηλότερο επίπεδο και το 5 το υψηλότερο. Κάθε επόμενο level εκτελεί και τις διεργασίες του προηγούμενου επιπέδου. Για παράδειγμα το level 3 εκτός από τις δικές του διεργασίες θα κάνει και αυτές των level 1 και level 2 [28]. Το εργαλείο έχει 5 στάδια τα οποία είναι τα εξής:

1. *Collect live information (Dumpstate + Logcat)*
   Η επιλογή αυτή ανακτά τα περισσότερα δυνατά δεδομένα στον συντομότερο δυνατό χρόνο. Παρέχει πληροφορίες για τους προγραμματιστές και λεπτομέρειες για την συσκευή που είναι προς εξέταση.

2. *Level 1 + System information*

   Περιέχει πληροφορίες για τις συνδέσεις δικτύου, ημερομηνία και ώρα, πληροφορίες για τον αποθηκευτικό χώρο, λίστα με ανοιγμένα αρχεία καθώς και τον χρόνο εκτέλεσης τους.

3. *Level 2 + Logical acquisition of the SD Card*

   Παρέχει αντιγραφή δεδομένων από την κάρτα SD. Θα ανακτήσει δεδομένα στα οποία έχει τα κατάλληλα δικαιώματα.

4. *Level 3 + Logical acquisition of the Data directory*

   Ανακτά τα δεδομένα του καταλόγου /data/. Ο κατάλογος αυτός αποτελείται από configuration αρχεία και αρχεία εφαρμογών.

5. *Level 4 + Full logical acquisition (Common local directories)*

   Η τελευταία επιλογή δίνει την δυνατότητα στον χρήστη να ανακτήσει αρχεία από τους πιο κοινούς καταλόγους της συσκευής.

   - /cache
   - /charger
   - /config
   - /d
   - /etc
   - /mnt
   - /res
   - /root
   - /sbin
   - /sys
   - /system
   - /tombstones

Το Foroboto θα εγκατασταθεί στον υπολογιστή (laptop) και με την βοήθεια του προγράμματος ADB θα ανακτήσουμε τα δεδομένα από την «έξυπνη» κινητή συσκευή

Τα αρχεία εγκατάστασης του Foroboto θα πρέπει να βρίσκονται στον φάκελο platform-tools του SDK. Για να έχουμε πρόσβαση στο Foroboto μέσω ADB θα πρέπει το αρχείο foroboto.bat να βρίσκεται στον ίδιο φάκελο με τα εξής αρχεία του ADB: adb.exe, AdbWinApi.dll και το AdbWinUsbApi.dll.

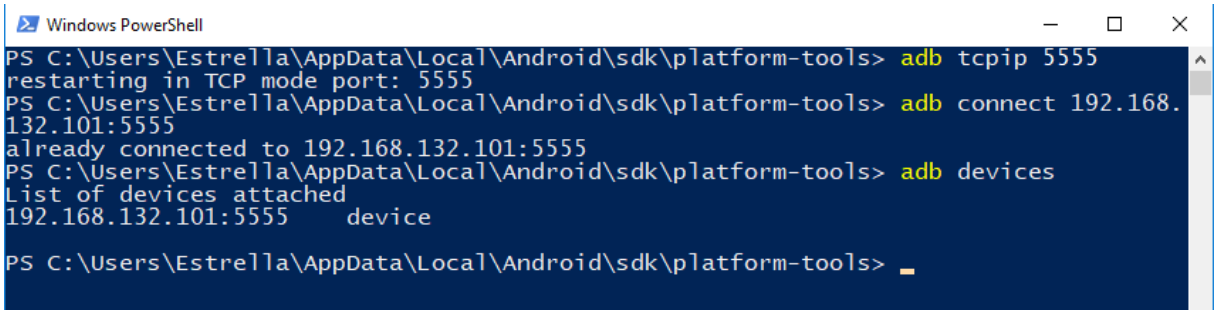
Ύστερα θα πληκτρολογήσουμε τις εξής εντολές :

adb root

adb tcpip 5555

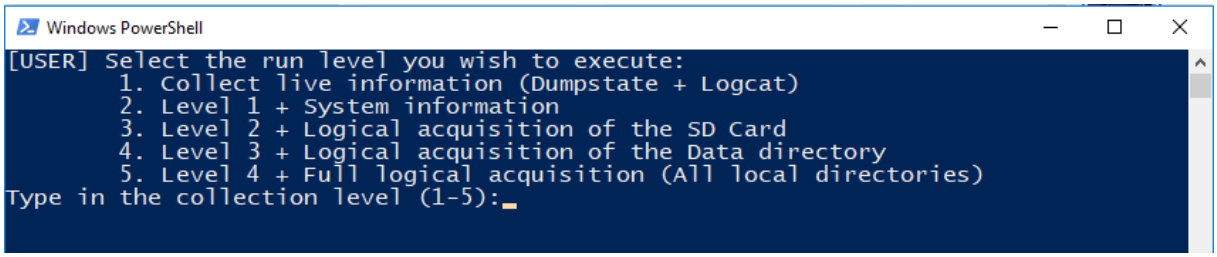
adb connect 192.168.132.101:5555

adb devices



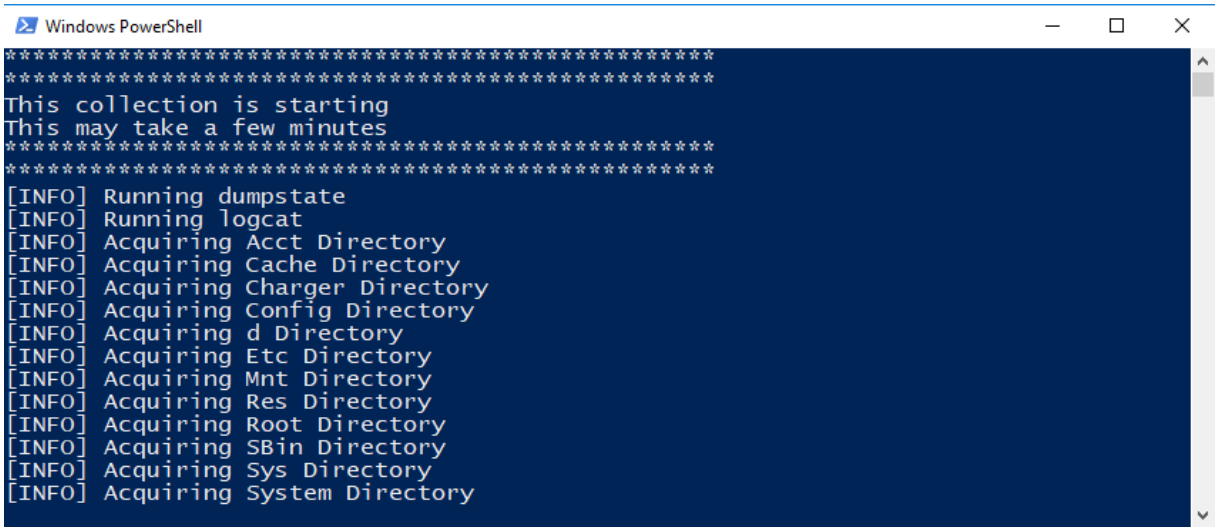
Εικόνα 5.12 Σύνδεση ADB με την "έξυπνη" κινητή συσκευή

Δίνοντας την εντολή ./foroboto.bat μας εμφανίζει το μενού του προγράμματος.

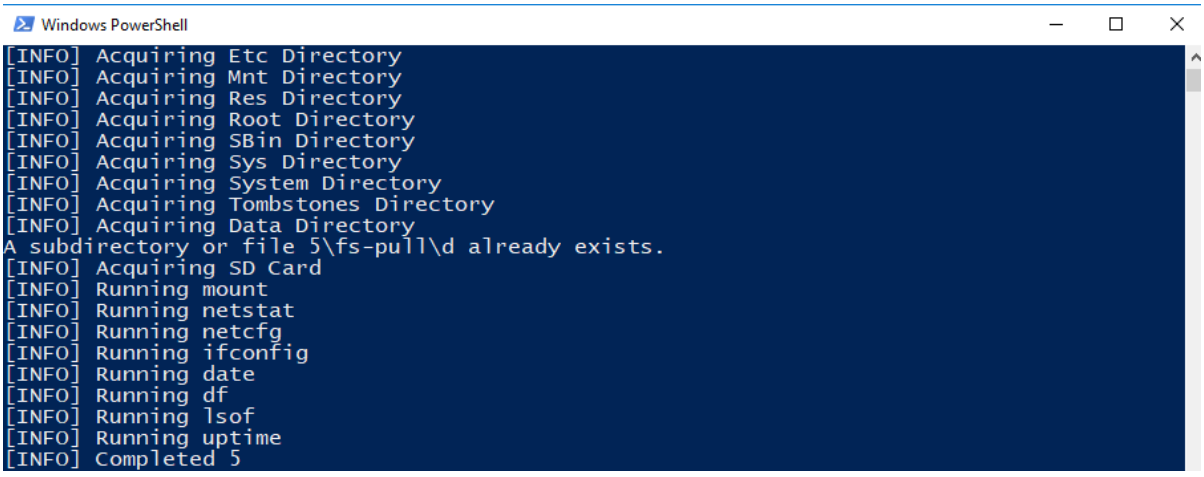


Εικόνα 5.13 Μενού του Foroboto

Επιλέγοντας το επίπεδο 5 θα ανακτήσουμε πλήρη πρόσβαση και πλήρη ανάκτηση των δεδομένων.

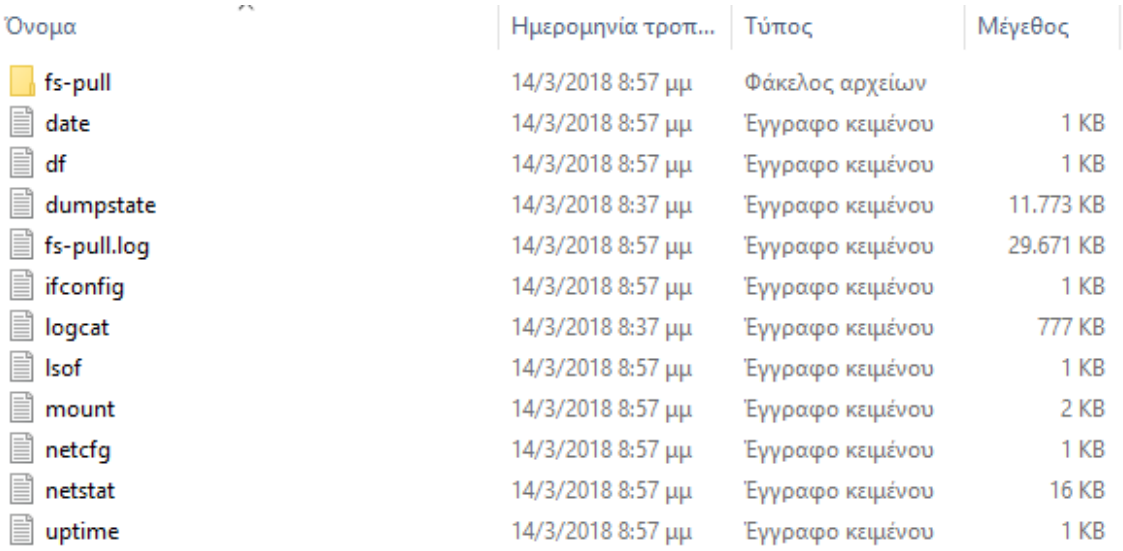


Εικόνα 5.14 Διαδικασία ανάκτησης δεδομένων Foroboto



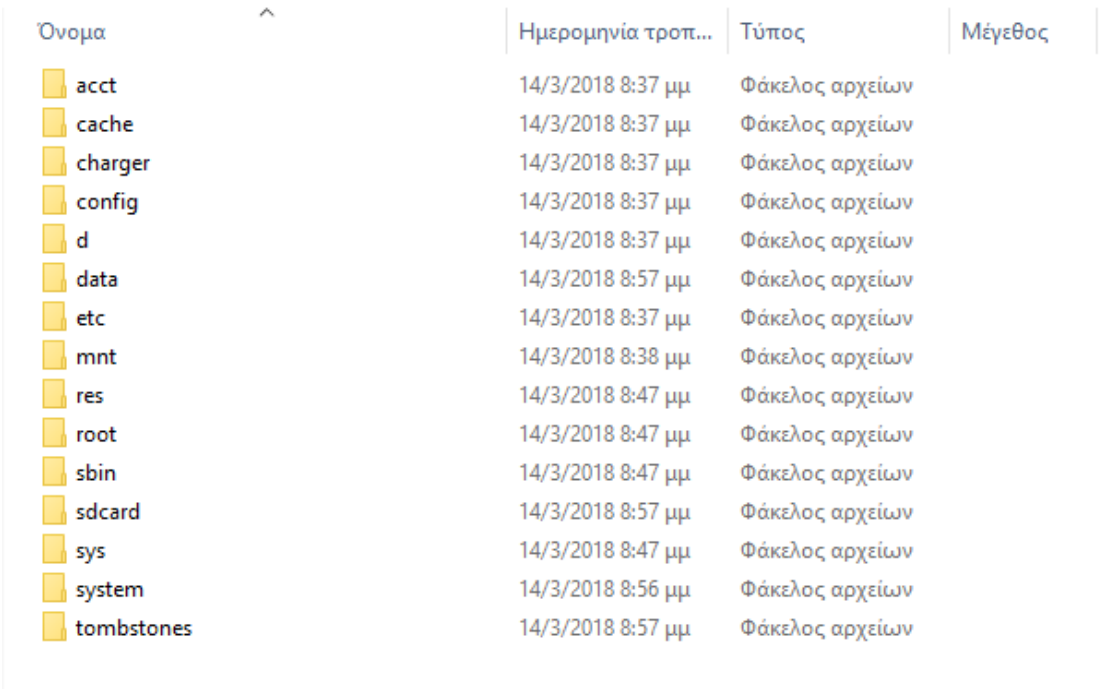
Εικόνα 5.15 Ολοκλήρωση ανάκτησης δεδομένων μέσω Foroboto

Έχει τελειώσει η ανάκτηση των αρχείων με μέγεθος 11,9GB. Τα αρχεία φαίνονται παρακάτω. Στον φάκελο fs-pll βρίσκονται όλα τα αρχεία του συστήματος και της SDCard.



Όνομα	Ημερομηνία τροπ...	Τύπος	Μέγεθος
fs-pull	14/3/2018 8:57 μμ	Φάκελος αρχείων	
date	14/3/2018 8:57 μμ	Έγγραφο κειμένου	1 KB
df	14/3/2018 8:57 μμ	Έγγραφο κειμένου	1 KB
dumpstate	14/3/2018 8:37 μμ	Έγγραφο κειμένου	11.773 KB
fs-pull.log	14/3/2018 8:57 μμ	Έγγραφο κειμένου	29.671 KB
ifconfig	14/3/2018 8:57 μμ	Έγγραφο κειμένου	1 KB
logcat	14/3/2018 8:37 μμ	Έγγραφο κειμένου	777 KB
lsof	14/3/2018 8:57 μμ	Έγγραφο κειμένου	1 KB
mount	14/3/2018 8:57 μμ	Έγγραφο κειμένου	2 KB
netcfg	14/3/2018 8:57 μμ	Έγγραφο κειμένου	1 KB
netstat	14/3/2018 8:57 μμ	Έγγραφο κειμένου	16 KB
uptime	14/3/2018 8:57 μμ	Έγγραφο κειμένου	1 KB

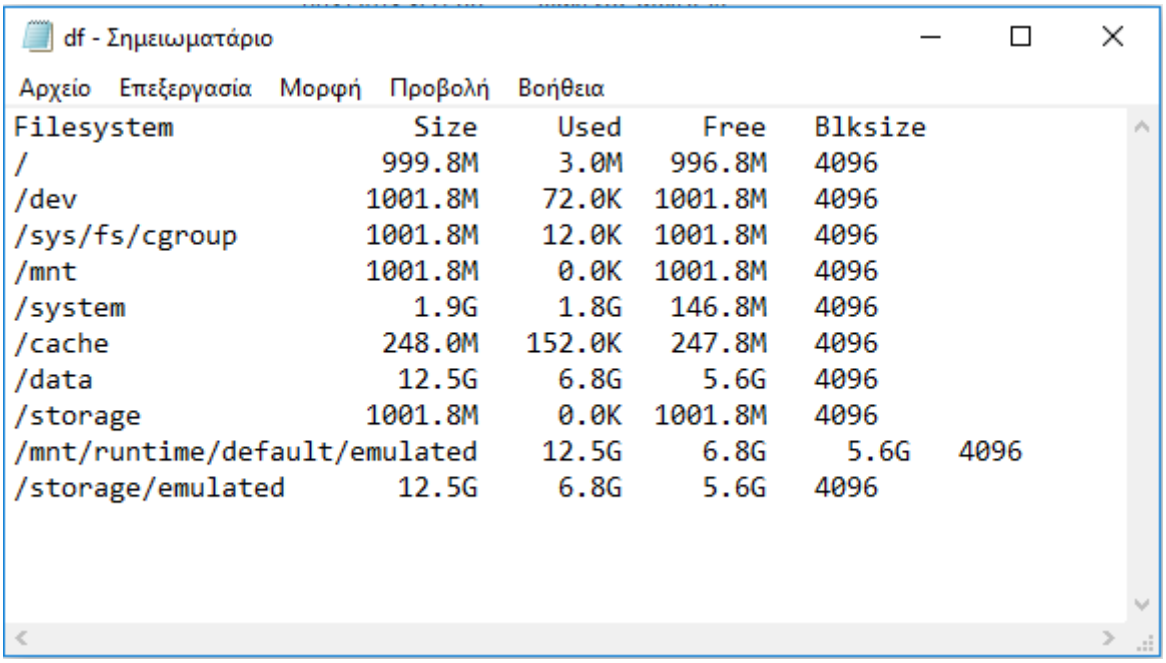
Εικόνα 5.16 Λίστα Αρχείων που ανακτήθηκαν από την συσκευή μας μέσω Foroboto



Όνομα	Ημερομηνία τροπ...	Τύπος	Μέγεθος
acct	14/3/2018 8:37 μμ	Φάκελος αρχείων	
cache	14/3/2018 8:37 μμ	Φάκελος αρχείων	
charger	14/3/2018 8:37 μμ	Φάκελος αρχείων	
config	14/3/2018 8:37 μμ	Φάκελος αρχείων	
d	14/3/2018 8:37 μμ	Φάκελος αρχείων	
data	14/3/2018 8:57 μμ	Φάκελος αρχείων	
etc	14/3/2018 8:37 μμ	Φάκελος αρχείων	
mnt	14/3/2018 8:38 μμ	Φάκελος αρχείων	
res	14/3/2018 8:47 μμ	Φάκελος αρχείων	
root	14/3/2018 8:47 μμ	Φάκελος αρχείων	
sbin	14/3/2018 8:47 μμ	Φάκελος αρχείων	
sdcard	14/3/2018 8:57 μμ	Φάκελος αρχείων	
sys	14/3/2018 8:47 μμ	Φάκελος αρχείων	
system	14/3/2018 8:56 μμ	Φάκελος αρχείων	
tombstones	14/3/2018 8:57 μμ	Φάκελος αρχείων	

Εικόνα 5.17 Τα αρχεία του λειτουργικού συστήματος και της SDcard

- ***df file***

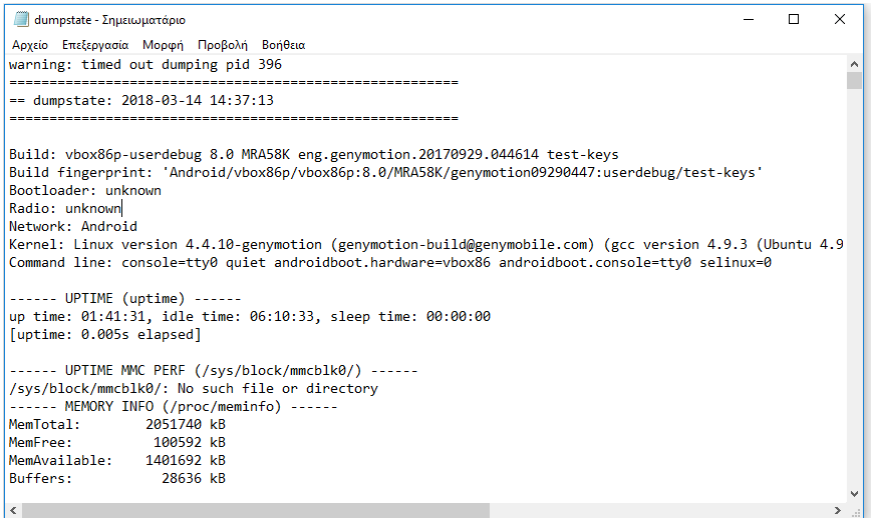


Εικόνα 5.18 Αρχείο «df file»

Στο αρχείο αναφέρεται ο κάθε φάκελος πόσο μέγεθος έχει, τον χρησιμοποιούμενο χώρο καθώς και τον ελεύθερο χώρο.

- ***dumpstate***

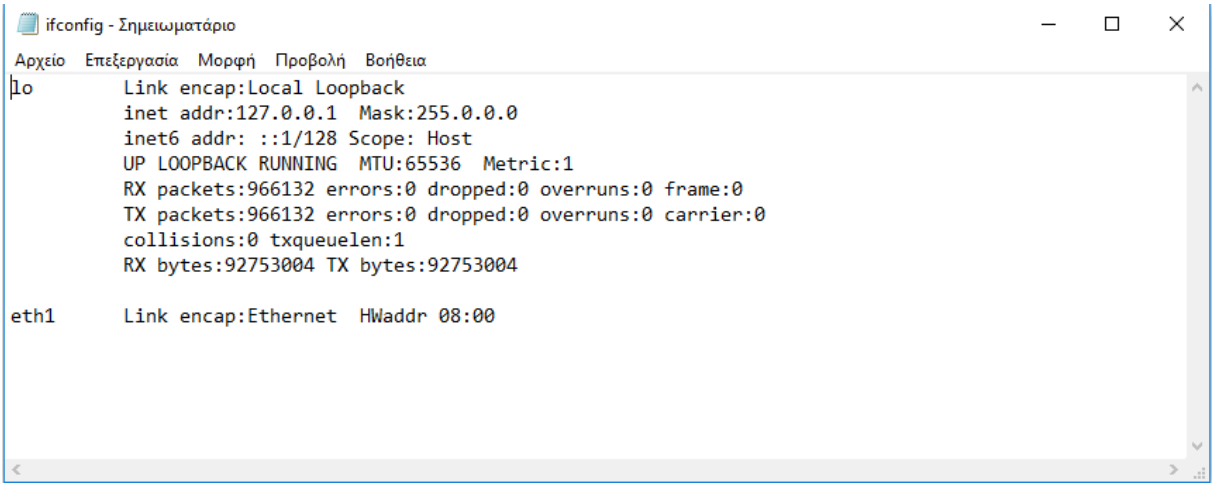
Στο αρχείο αναφέρονται ειδικές πληροφορίες για το hardware της «έξυπνη» κινητής συσκευής (π.χ. Memory info, CPUINFO, Virtual Memory Stats) καθώς και λεπτομερείς πληροφορίες για το λειτουργικό σύστημα.



Εικόνα 5.19 Αρχείο «Dumpstate»

- ***ipconfig***

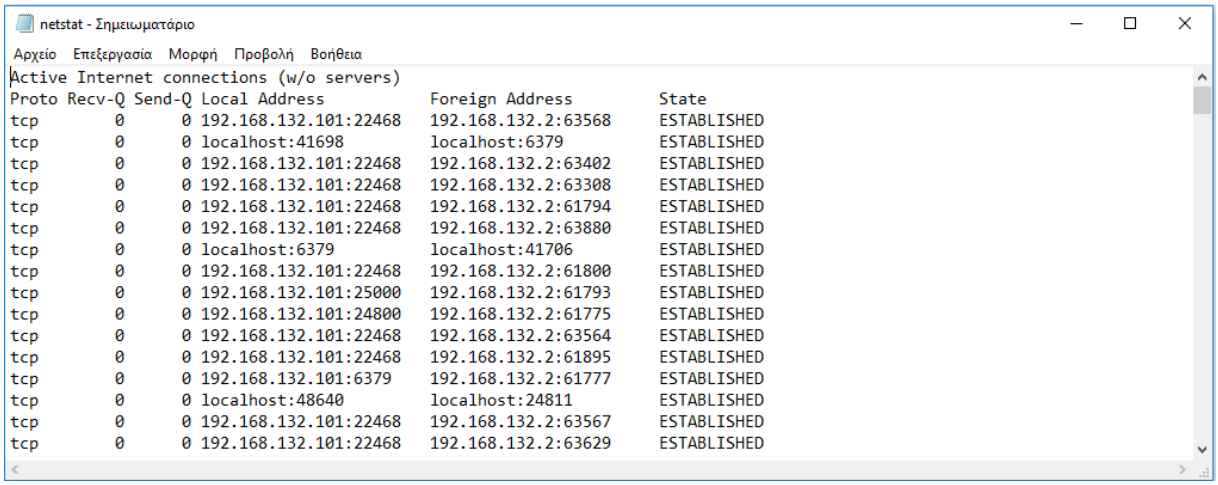
Εμφανίζει όλες τις τρέχουσες δικτυακές ρυθμίσεις της «έξυπνης» κινητής συσκευής για κάθε δικτυακό interface του συστήματος.



Εικόνα 5.20 Αρχείο «ipconfig»

- ***Netstat***

Σε αυτό το αρχείο φαίνονται οι ενεργές συνδέσεις της συσκευής σε ένα δίκτυο.



Εικόνα 5.21 Αρχείο «Netstat»

Εκτός από τα αρχεία που ανακτήθηκαν από την «έξυπνη» κινητή συσκευή στον υπολογιστή, μέσω proxy δεν λάβαμε κάτι περαιτέρω. Η συσκευή δεν αλληλοεπίδρασε κατά την ώρα της ανάκτησης.

5.3 Dumpsys

Το Dympsys είναι ένα εργαλείο που εκτελείται σε συσκευές Android και παρέχει πληροφορίες σχετικά με τις υπηρεσίες του συστήματος. Χρησιμοποιώντας το Android Debug Bridge (ADB), εφόσον το εργαλείο “dumpsys” είναι ενσωματωμένο στο ADB, λαμβάνουμε πληροφορίες για όλες τις υπηρεσίες του συστήματος που εκτελούνται στην «έξυπνη» κινητή συσκευή. Περιέχει εντολές τόσο για την εμφάνιση των εργασιών που εκτελούνται, πληροφορίες για την Ram, την μπαταρία και διαγνωστικά δικτύου.

Για να έχουμε μια πλήρη εικόνα των υπηρεσιών που μπορούμε να ανακτήσουμε από την συσκευή γράφουμε την εντολή “*adb shell dumpsys -l”* παραθέτοντάς τα σε έναν πίνακα.

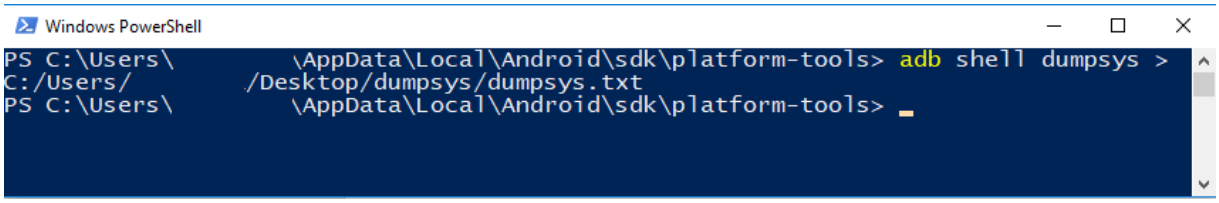
DockOdserver	Genyd	SurfaceFlinger	acceddibility
activity	alarm	Android.security.keystore	Android.service.gatekeeper.IGatekeeperService
appwidget	assetatlas	audio	backup
batteryproperties	batterystats	Carrier_config	clipboard
connectivity	Consumer_ir	content	Country_detector
Device_policy	devicestats	deviceidle	Devicestoragemonitor
display	dreams	Drm.drmManager	Dropbox
fingerprint	gfxinfo	graphicsctats	Imms
Input_method	iphonesubinfo	isms	Isub
launcherapps	location	Lock_settings	Media.audio_flinger
account	appops	battery	Cpmmpntime_management
cpuinfo	diskstats	ethernet	Jobscheduler
Input	Media.audio_policy	Media.camera	Media.camera.proxy
Media.player	Media.radio	Media.resource.manager	Media.sound_trigger_hw
Media_projection	Media_router	Media_session	Meminfo
mount	metpolicy	netstats	Network_management
Network_scire	notification	package	Permission
phone	power	print	Processinfo
procstats	restrictions	rttmanager	Samplingprofiler
Scheduling_policy	search	sensorservice	Serial
servicediscovery	simphonebook	sip	Statusbar
telecom	Telephony.registry	textservices	Trust
uimode	updatelock	usagestats	Ubs
user	vibrator	voiceinteraction	Wallpaper

webviewupdate	wifi	Wifip2p	Wifiscanner
window			

Πίνακας 5.1 Υπηρεσίες προγράμματος Dumpsys

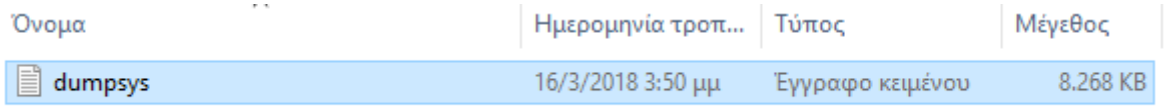
Με την εντολή *adb shell dumpsys* εμφανίζονται όλες οι υπηρεσίες στις οποίες αναφερθήκαμε παραπάνω με κάθε λεπτομέρεια. Βέβαια δεν γίνεται να αναλύσουμε όλες τις υπηρεσίες του προγράμματος αλλά τα πιο σημαντικά αποτελέσματα που προέκυψαν.

Adb shell dumpsys > C:\Users\...\Desktop\dumpsys\dumpsys.txt



Εικόνα 5.22 Εγγραφή των πληροφοριών που ανακτήθηκαν από το dumpsys σε ένα αρχείο στον υπολογιστή μας με όνομα "dumpsys.txt"

Αποθηκεύσαμε τα δεδομένα σε ένα αρχείο txt ώστε να αναλύσουμε.



Εικόνα 5.23 Αρχείο «Dumpsys.txt»

Στην παρακάτω εικόνα εμφανίζονται όλοι οι λογαριασμοί της «έξυπνης» κινητής συσκευής. Στην εικονική μας συσκευή έχουμε εισάγει μόνο έναν λογαριασμό της Google. Σε περίπτωση που υπήρχαν και άλλοι θα εμφανιζόταν σε αυτό το σημείο της αναφοράς.

```
DUMP OF SERVICE account:
User UserInfo{0:Owner:13}:
  Accounts: 1
    Account {name=s          gmail.com, type=com.google}

  AccountId, Action_Type, timestamp, UID, TableName, Key
  Accounts History
  -1,action_called_account_add,2018-01-28 17:16:56,10060,accounts,0
  -1,action_called_account_add,2018-01-28 17:20:51,10060,accounts,1
  1,action_account_add,2018-01-28 17:23:03,10063,accounts,2
  1,action_set_password,2018-01-28 17:23:03,10063,accounts,3
```

Εικόνα 5.24 Dumpsys - Accounts

Στην παρακάτω εικόνα αναφέρεται το συνολικό μέγεθος της μνήμης σε KB, η ελεύθερη μνήμη και η χρησιμοποιούμενη μνήμη.

```
Total RAM: 2051740 kB (status normal)
 Free RAM: 1270641 kB (443833 cached pss + 770700 cached kernel + 56108 free)
 Used RAM: 814556 kB (689048 used pss + 125508 kernel)
 Lost RAM: -33457 kB
   Tuning: 96 (large 256), oom 184320 kB, restore limit 61440 kB (high-end-gfx)
------------------------------------------------------------------------------
```

Εικόνα 5.25 Πληροφορίες του Dumpsys για την RAM

Στην επόμενη φωτογραφία εμφανίζονται πληροφορίες για την CPU. Αναφέρεται το ποσοστό εκμετάλλευσης του επεξεργαστή από κάθε υπηρεσία καθώς και το ποσοστό χρησιμοποίησης του Kernel αντίστοιχα.

```
CPU usage from 392768ms to 306571ms ago:
  2.2% 1261/com.google.android.googlequicksearchbox:search: 0.9% user + 1.2% kernel / faults: 295 minor
  2.1% 135/adbd: 0% user + 2% kernel / faults: 5099 minor
  1.7% 249/mediaserver: 0.1% user + 1.6% kernel
  1.4% 588/system_server: 0.3% user + 1.1% kernel / faults: 1699 minor
  0.9% 1288/com.google.android.gms.persistent: 0.3% user + 0.5% kernel / faults: 2222 minor
  0.8% 913/com.google.android.googlequicksearchbox: 0.6% user + 0.2% kernel / faults: 27 minor
  0.7% 114/logd: 0.1% user + 0.6% kernel / faults: 8 minor
  0.4% 132/redis: 0% user + 0.3% kernel
  0.3% 584/logcat: 0% user + 0.2% kernel
  0.2% 7/rcu_preempt: 0% user + 0.2% kernel
  0.1% 1338/com.google.android.gms: 0% user + 0% kernel / faults: 6929 minor
  0.1% 236/local_opengl: 0% user + 0.1% kernel
  0.1% 587/surfaceflinger: 0% user + 0.1% kernel / faults: 1 minor
  0.1% 1424/com.estrongs.android.pop: 0% user + 0.1% kernel / faults: 311 minor
  0.1% 8173/kworker/u8:1: 0% user + 0.1% kernel
  0.1% 379/logcat: 0% user + 0.1% kernel
  0% 262/healthd: 0% user + 0% kernel
```

Εικόνα 5.26 Πληροφορίες του Dumpsys για την CPU

Παρακάτω εμφανίζονται οι πληροφορίες σχετικά με την IP Address της συσκευής, την gateway, τον DNS Server, το Domains DHSP server, την DNS Addresses και το Http Proxy.

```
IP address 10.0.3.15/24 Gateway 10.0.3.2  DNS servers: [ 192.168.2.1 ] Domains DHCP server /10.0.3.2

DnsAddresses: [192.168.2.1,] Domains: null MTU: 0 TcpBufferSizes: 524288,1048576,2097152,262144,524288,1048576 HttpProxy: [192.168.2.4] 8083
```

Εκτός από τα παραπάνω δεδομένα και την αναφορά που ανακτήσαμε από το dumpsys δεν έχουμε κάποια περαιτέρω αλληλεπίδραση της συσκευής μέσω Proxy.

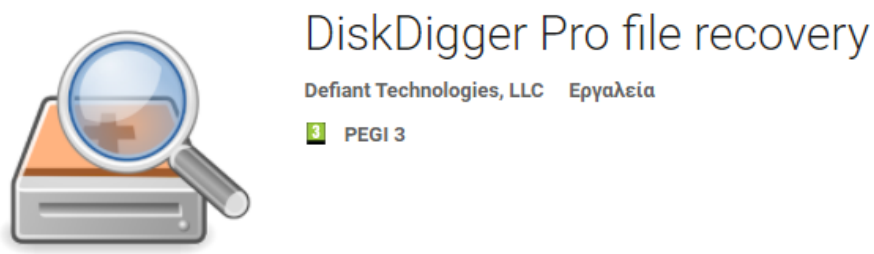
5.4 DiskDigger

Το DiskDigger είναι ένα εργαλείο ανάκτησης δεδομένων. Το συγκεκριμένο εργαλείο είναι κατάλληλο για λειτουργικά συστήματα Windows, Linux και Android. Όπως αναφέρεται και στην επίσημη ιστοσελίδα του εργαλείου ενδείκνυται για επαγγελματική χρήση από ψηφιακούς εγκληματολόγους [30].

Η εκδοχή του εργαλείου για Android βρίσκεται στο Google Play Store. Υπάρχουν δυο εκδοχές του εργαλείου, η μία είναι επί πληρωμή (DiskDigger Pro File Recover) [31] και η άλλη δωρεάν (DiskDigger Photo Recovery) [32].

Η εκδοχή επί πληρωμή μπορεί να ανακτήσει όλα τα είδη των αρχείων και υποστηρίζει μεταφορά αρχείων μέσω FTP. Επιπλέον, χρειάζεται πρόσβαση root για να μπορέσει να επαναφέρει άλλα αρχεία εκτός φωτογραφιών.

Η δωρεάν εκδοχή ανακτά μόνο φωτογραφίες και video δηλαδή τα πιο συνηθισμένα διαγραμμένα αρχεία. Επίσης, χρειάζεται root πρόσβαση για να ανακτηθούν τα video.



Εικόνα 5.27 DiskDigger Pro File Recovery [31]

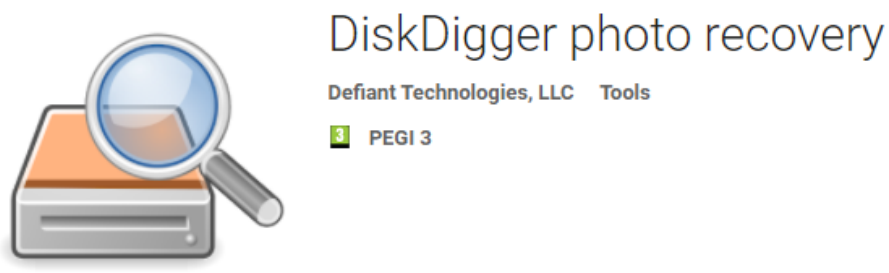
Στον παρακάτω πίνακα αναφέρουμε τα αρχεία που ανακτούν οι δυο εκδόσεις.

	DiskDigger Pro File Recovery	**DiskDigger Photo Recovery**
JPG	X	X
MP4	X	X
PNG	X	X
MP3	X	
GIF	X	

WAV	x	
AMR	x	
TIF	x	
CR2	x	
SR2	x	
NEF	x	
DCR	x	
PEF	x	
DNG	x	
ORF	x	
DOC	x	
XLS	x	
PPT	x	
PDF	x	
ZIP	x	
DOCX	x	
XLSX	x	
PPTX	x	
XPS	x	
ODT	x	
ODS	x	
ODP	x	
ODG	x	
APK	x	
EPUB	x	
SNB	x	
RAR	x	
VCF	x	
SQLITE	x	

Πίνακας 5.2 Σύγκριση DiskDigger Pro File Recovery με DiskDigger Photo Recovery

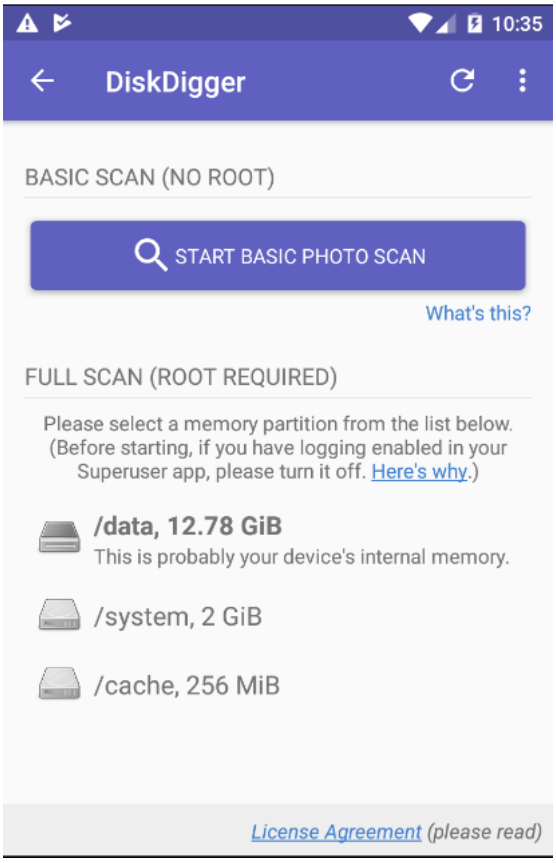
Στο πρακτικό μέρος της μεταπτυχιακής διατριβής εμείς θα χρησιμοποιήσουμε την δωρεάν εκδοχή του εργαλείου, η οποία βέβαια έχει περιορισμένες δυνατότητες ανάκτησης αρχείων.



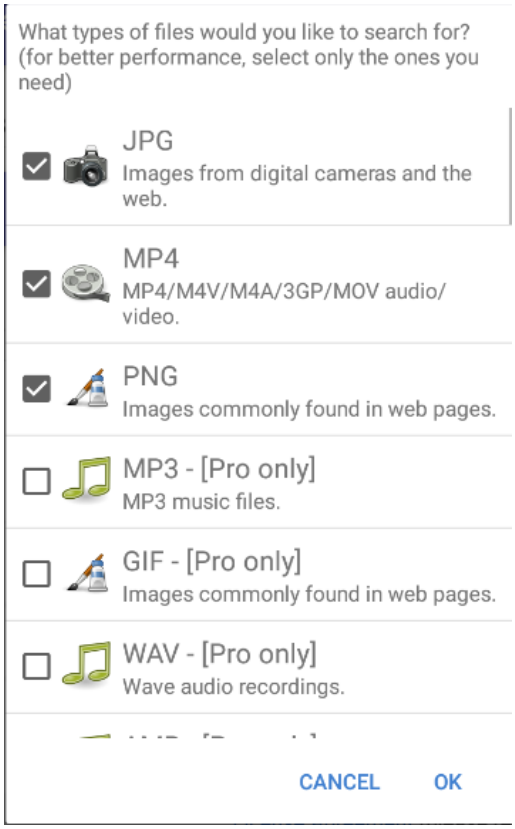
Εικόνα 5.28 DiskDigger Photo Recovery [32]

Ο αλγόριθμος του DiskDigger προσφέρει δύο ειδών αναζητήσεις για διαγραμμένα αρχεία:

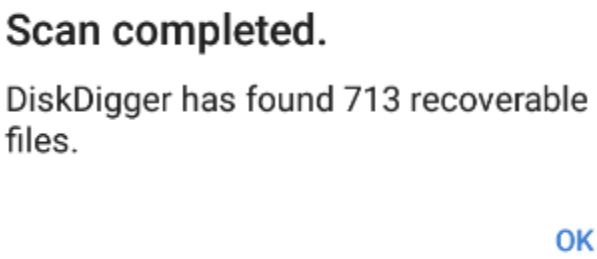
- **Basic**: Προσφέρει ανάκτηση αρχείων χωρίς η συσκευή να έχει root privileges
- **Full**: Προσφέρει ανάκτηση αρχείων (φωτογραφίες και βίντεο) σε root συσκευή



Εικόνα 5.29 DiskDigger Scan

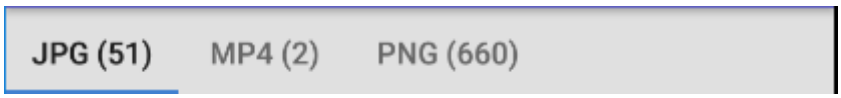


Εικόνα 5.30 Επιλογή αρχείων που θα ανακτηθούν από το DiskDigger



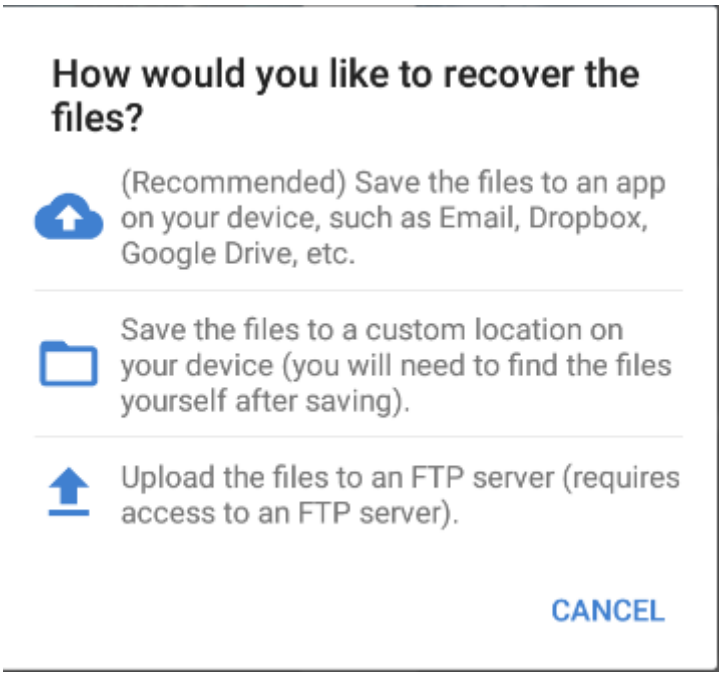
Εικόνα 5.31 Ολοκλήρωση της ανάκτησης αρχείων

Η αναζήτηση των αρχείων μόλις τελείωσε και το εργαλείο βρήκε 713 αρχεία που έχουν διαγραφεί.



Εικόνα 5.32 Εύρεση αρχείων στην "έξυπνη" κινητή συσκευή

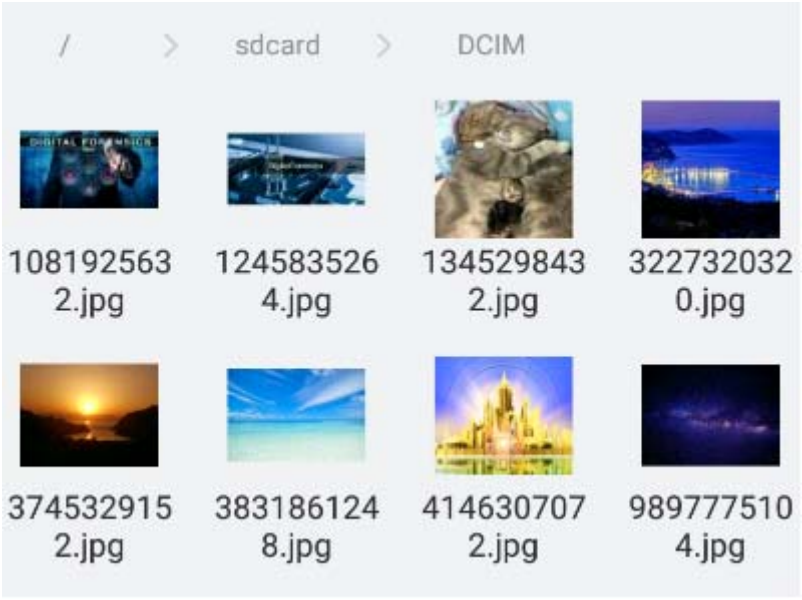
Πιο συγκεκριμένα ευρέθησαν 51 εικόνες JPEG, 660 εικόνες PNG και 2 αρχεία video με κατάληξη MP4.



Εικόνα 5.33 Επιλογές για το που θα αποθηκευτούν τα αρχεία

Σε αυτό το σημείο θα πρέπει να γίνει η ανάκτηση των αρχείων. Η εφαρμογή μας ζητάει να επιλέξουμε πού θέλουμε να αποθηκεύσουμε τα αρχεία που θα ανακτήσει το εργαλείο. Υπάρχουν 3 επιλογές: σε cloud (Email, Dropbox, Google Drive), σε μια τοποθεσία στη συσκευή μας και σε FTP Server. Εμείς θα επιλέξουμε να αποθηκεύσουμε τα αρχεία στην συσκευή μας και συγκεκριμένα στη διαδρομή /sdcard/DCIM.

Επιλέξαμε να ανακτήσουμε 8 φωτογραφίες JPEG και να τις αποθηκεύσουμε στην τοποθεσία της συσκευής μας με διαδρομή /sdcard/DCIM/.

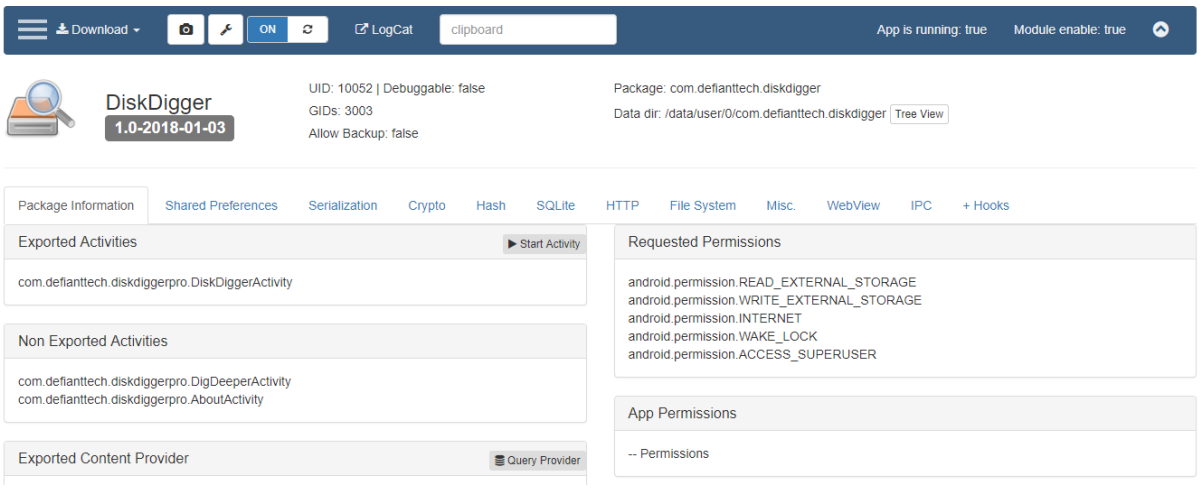


Εικόνα 5.34 Τα αρχεία που επιλέξαμε να ανακτήσουμε μέσω DiskDigger

Καθ' όλη την διάρκεια της αναζήτησης των αρχείων και της ανάκτησής τους γίνεται δυναμική ανάλυση της εφαρμογής μέσω Inspeckage καθώς και όλα τα δεδομένα του τηλεφώνου εισέρχονται στον Proxy (Burp Suite).

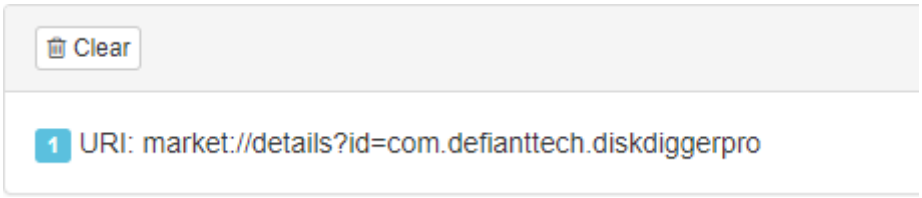
Ο Proxy δεν μας έδωσε κάποιο αποτέλεσμα, όποτε συμπεραίνουμε ότι δεν εξήλθαν δεδομένα από την «έξυπνη» κινητή μας συσκευή προς κάποια τρίτη οντότητα.

Από την δυναμική ανάλυση του Inspeckage θα παραθέσουμε τα αποτελέσματα που πήραμε παρακάτω:



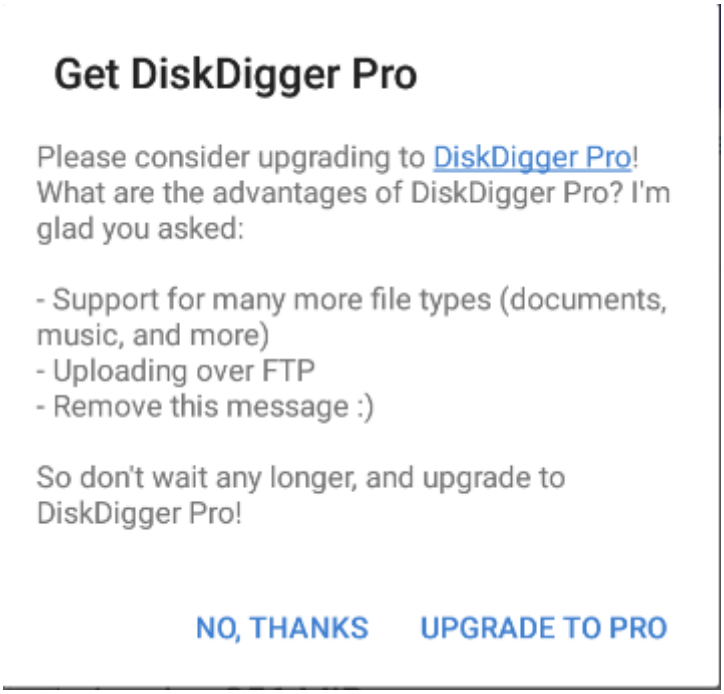
Εικόνα 5.35 Δυναμική Ανάλυση του DiskDigger μέσω Inspeckage

Η εφαρμογή ζητάει δικαιώματα για να διαβάσει και να γράψει στο external storage, να αποκτήσει δικαιώματα στο INTERNET, στο WAKELOCK και δικαιώματα υπερ-χρήστη (το οποίο όπως προ-είπαμε είναι απαραίτητο μόνο σε ανάκτηση video).



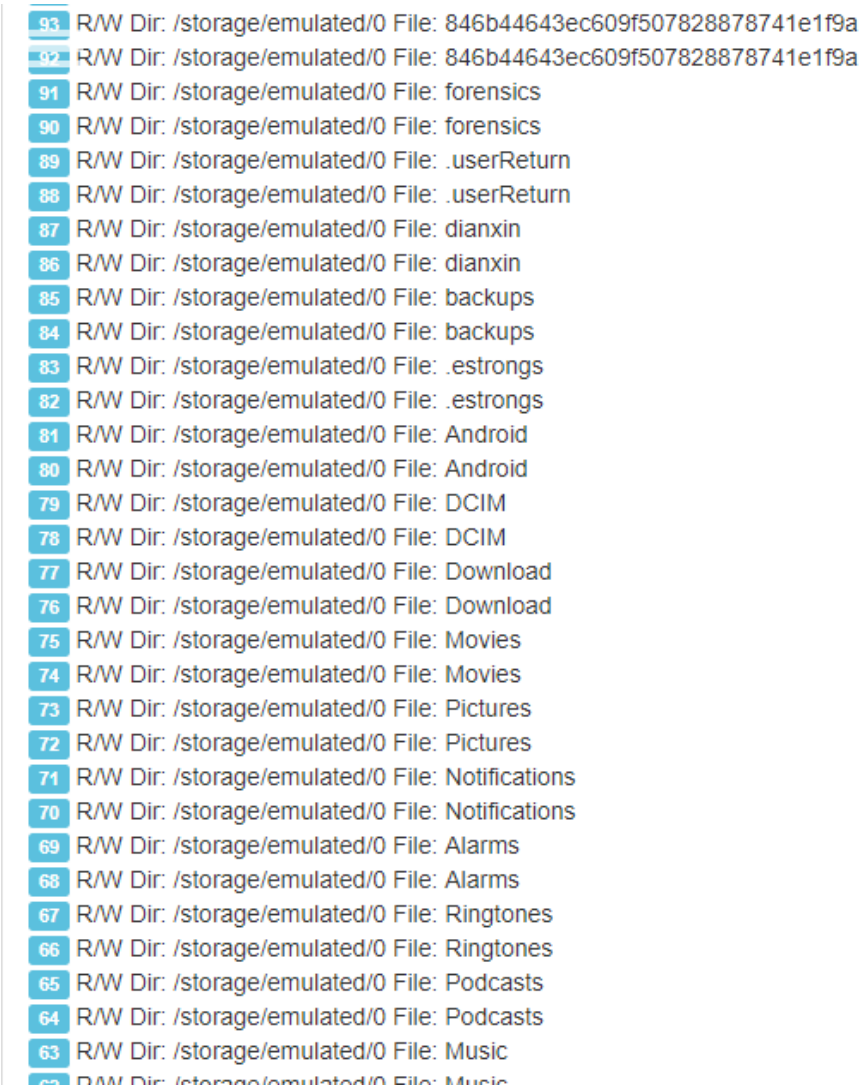
Εικόνα 5.36 Εμφάνιση επιλογής αναβάθμισης της εφαρμογής σε PRO

Όπως παρατηρούμε στο Inspeckage η εφαρμογή εμφανίζει επιλογή στο χρήστη να αποκτήσει την PRO έκδοση της.



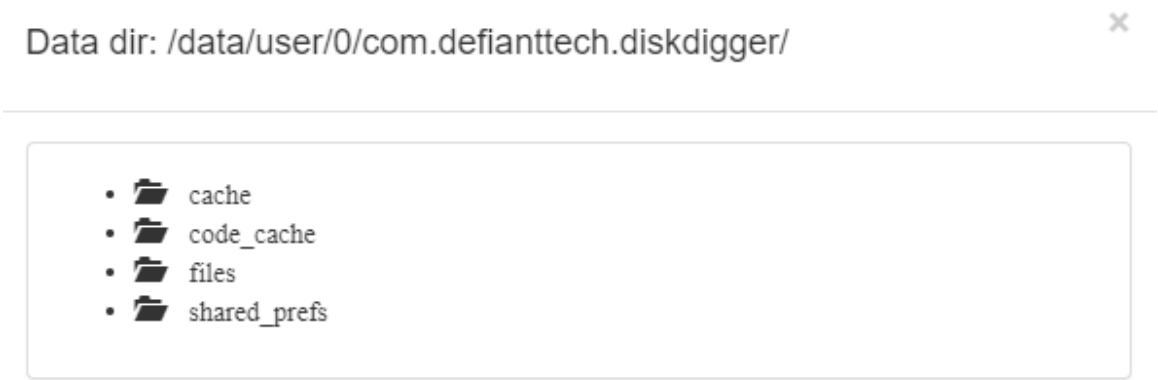
Εικόνα 5.37 Εμφάνιση Παραθύρου αναβάθμισης της εφαρμογής σε PRO έκδοση

Όπως βλέπουμε στην παρακάτω εικόνα η εφαρμογή έχει πρόσβαση σε αρχεία και φακέλους στην sdcard ώστε να μπορέσει να αναζητήσει τα αρχεία που θέλουμε ανακτήσουμε.



Εικόνα 5.38 Πρόσβαση της εφαρμογής DiskDigger στα αρχεία της συσκευής

Οι υπόλοιπες προσβάσεις στο File System είναι στα αρχεία της εφαρμογής.



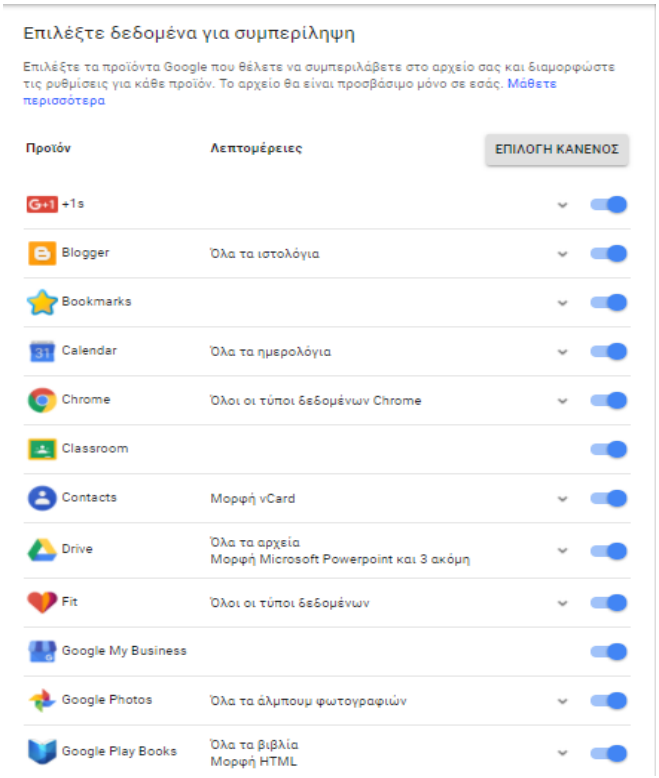
Εικόνα 5.39 Tree of DiskDigger

5.5 Google Takeout

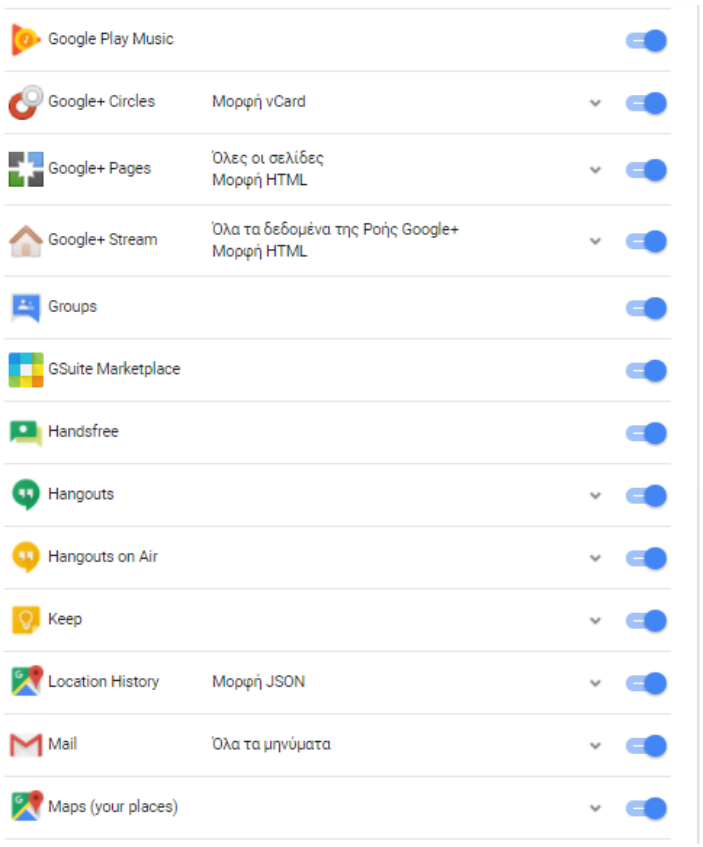
Εκτός από τα εγκληματολογικά εργαλεία που υπάρχουν ένα από τα πιο δυνατά «χαρτιά» της ψηφιακής εγκληματολογίας είναι η εταιρεία Google. Η Google συλλέγει τεράστιο όγκο δεδομένων για κάθε χρήστη. Η απόκτηση πρόσβασης σε αυτά τα δεδομένα είναι απαραίτητη για την επίλυση πολλών τύπων εγκλημάτων. Η εκμάθηση του τι γνωρίζει η Google για τον ύποπτο μπορεί να είναι θέμα ύψιστης σημασίας για τους ανακριτές και τους ειδικούς της εγκληματολογίας.

Η Google Takeout δημιουργήθηκε από την Google Data Front Liberation Front στις 28 Ιουνίου του 2011 για να επιτρέψει στους χρήστες να εξάγουν τα δεδομένα τους [33].

Στις μέρες μας οι περισσότεροι που χρησιμοποιούν λειτουργικό σύστημα Android έχουνε διεύθυνση ηλεκτρονικού ταχυδρομείου Gmail ώστε να έχουν πρόσβαση στις υπηρεσίες και στις εφαρμογές του Google Play Store. Το λειτουργικό σύστημα Android από την έκδοση 5.0 Lollipop και μετά προσφέρει την δυνατότητα μαζί με την Google να αποθηκεύει σε backup τα δεδομένα μιας «έξυπνης» κινητής συσκευής στην πλατφόρμα Google Drive. Το εργαλείο της Google για εξαγωγή αρχείων ονομάζεται Takeout και υπάρχει εδώ: https://takeout.google.com/settings/takeout.



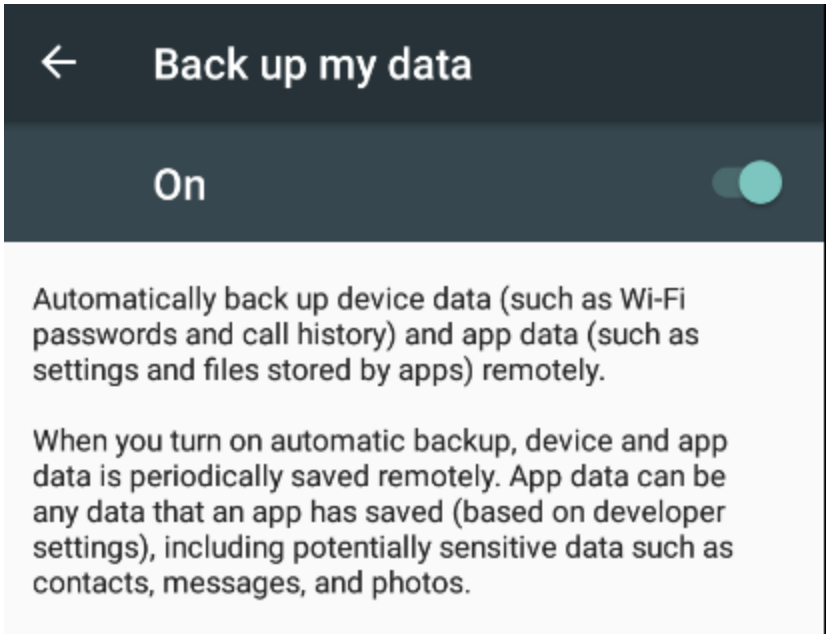
Εικόνα 5.40 Επιλογές Ανάκτησης Δεδομένων Google Takeout I



Εικόνα 5.41 Επιλογές Ανάκτησης Δεδομένων από το Google Takeout II

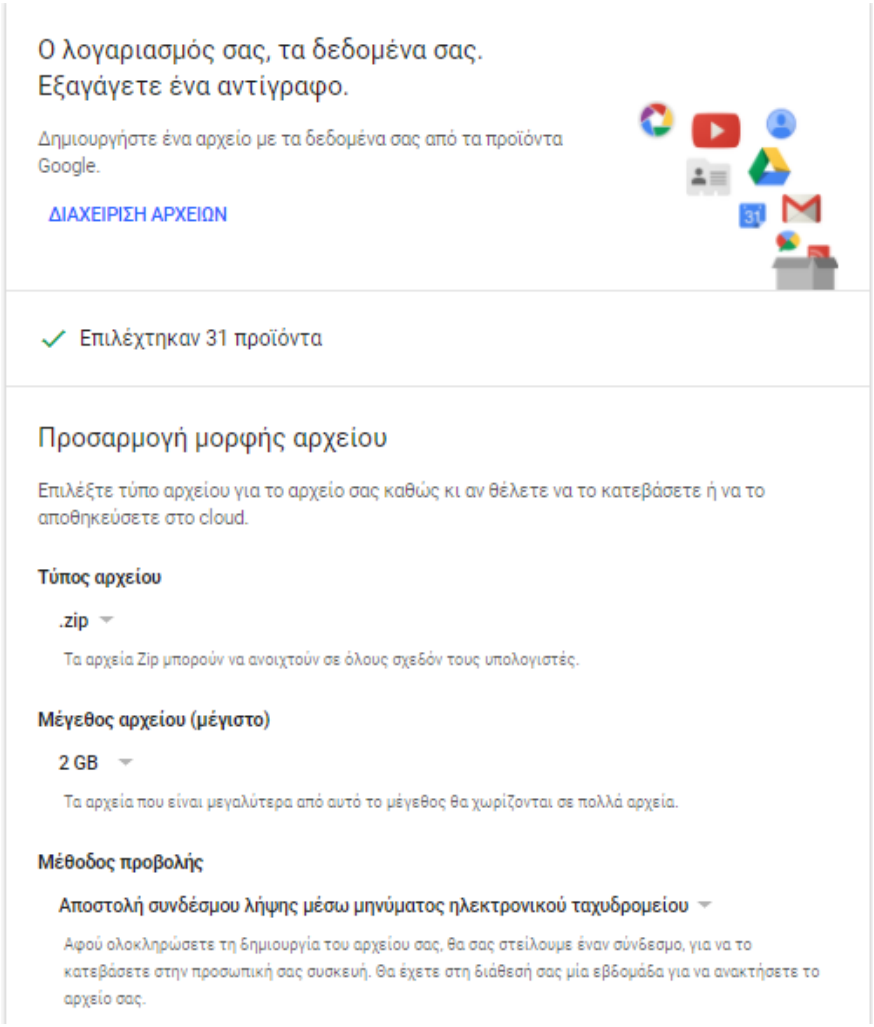
Εικόνα 5.42 Επιλογές Ανάκτησης Δεδομένων από το Google Takeout III

Πριν συνεχίσουμε στο επόμενο βήμα θα πρέπει να ενεργοποιήσουμε στο κινητό μας την επιλογή Back up my data η οποία βρίσκεται στις Ρυθμίσεις → Backup & Reset → Back up my data → on.



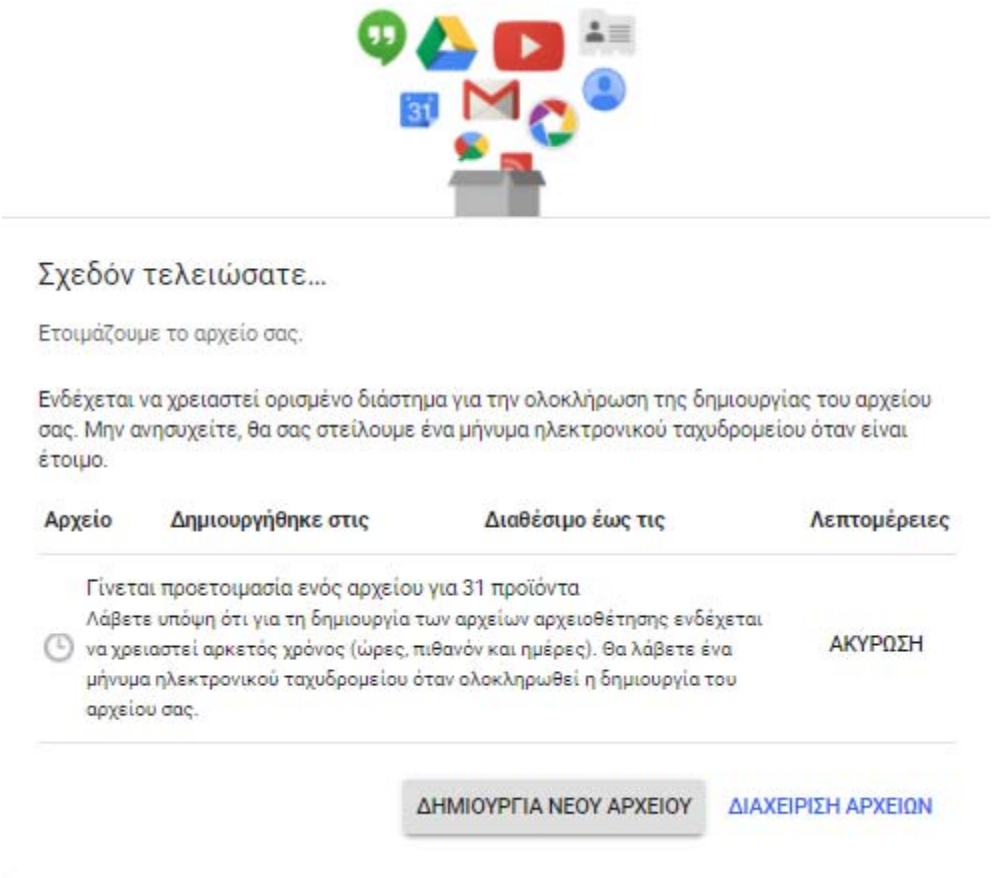
Εικόνα 5.43 Ενεργοποίηση επιλογής "Back up my data" στην "έξυπνη" κινητή συσκευή μας

Πατώντας στο Takeout στο επόμενο βήμα μας ζητείται να επιλέξουμε σε ποιον τύπο συμπιεσμένη μορφής zip ή tgz θα θέλαμε να δημιουργηθεί το αρχείο καθώς και το μέγιστο μέγεθος του αρχείου που θέλουμε να δημιουργηθεί.



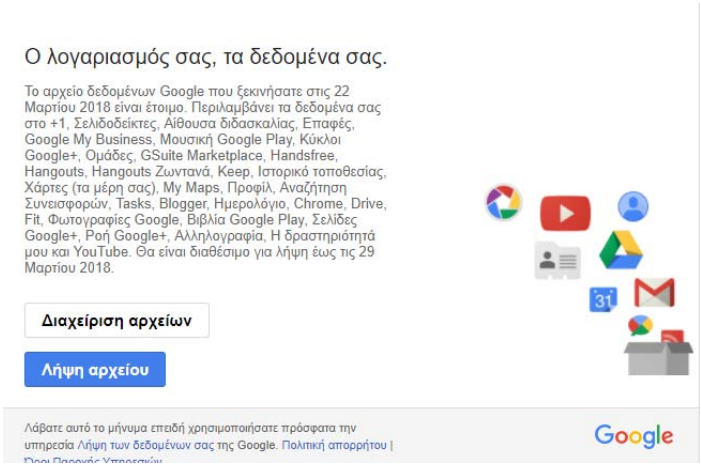
Εικόνα 5.44 Επιλογές δημιουργία αρχείου

Το τελευταίο βήμα είναι να επιλέξουμε την δημιουργία αρχείου.



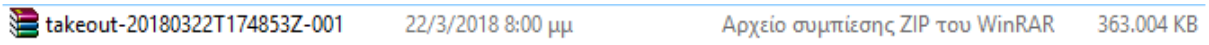
Εικόνα 5.45 Δημιουργία αρχείου των δεδομένων

Η δημιουργία του αρχείου έγινε, ενημερώνοντάς μας για αυτό η Google με Email και μας δίνεται η δυνατότητα για λήψη του αρχείου.



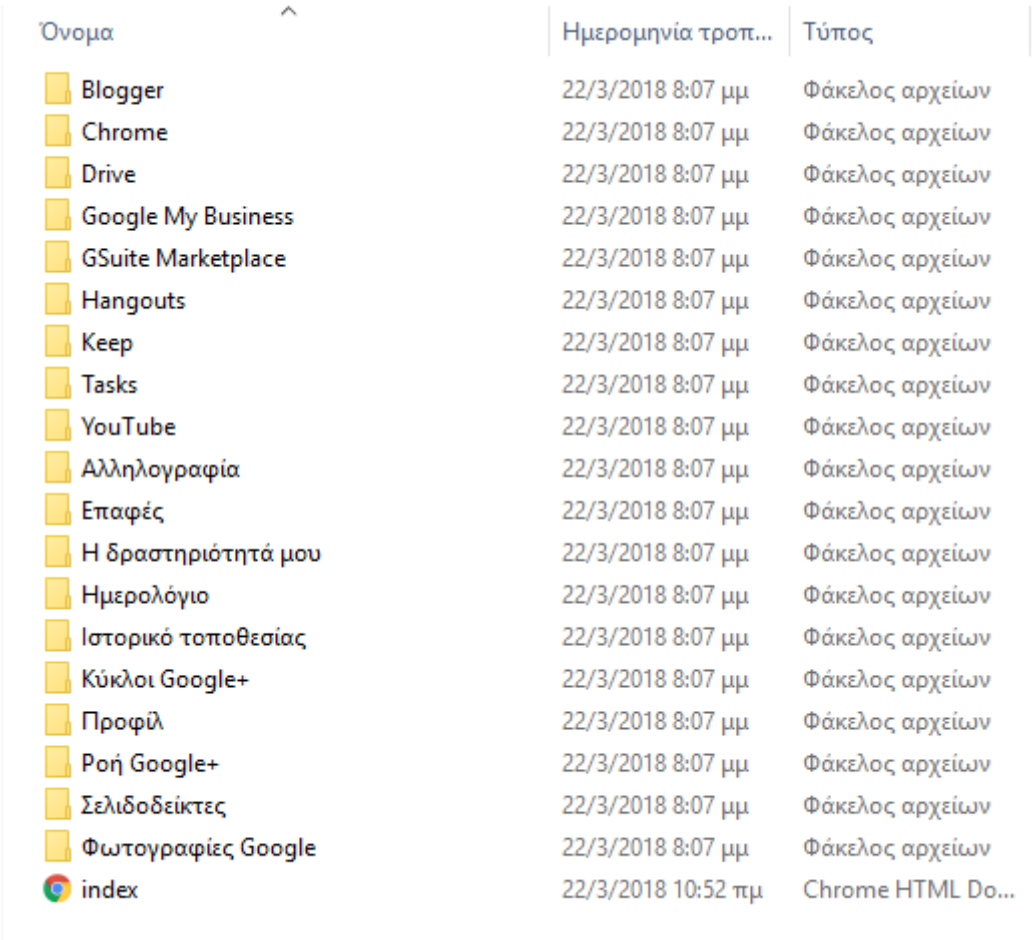
Εικόνα 5.46 Λήψη του αρχείου της Google μέσω του υπερσυνδέσμου που μας στάλθηκε στον email

Για να γίνει όλη αυτή η διαδικασία θα πρέπει ο ψηφιακός εγκληματολόγος να γνωρίζει το email και τον κωδικό του χρήστη καθώς και να είναι ενεργοποιημένη η επιλογή του Backup στην «έξυπνη» κινητή συσκευή.



Εικόνα 5.47 Το αρχείου του Takeout.zip

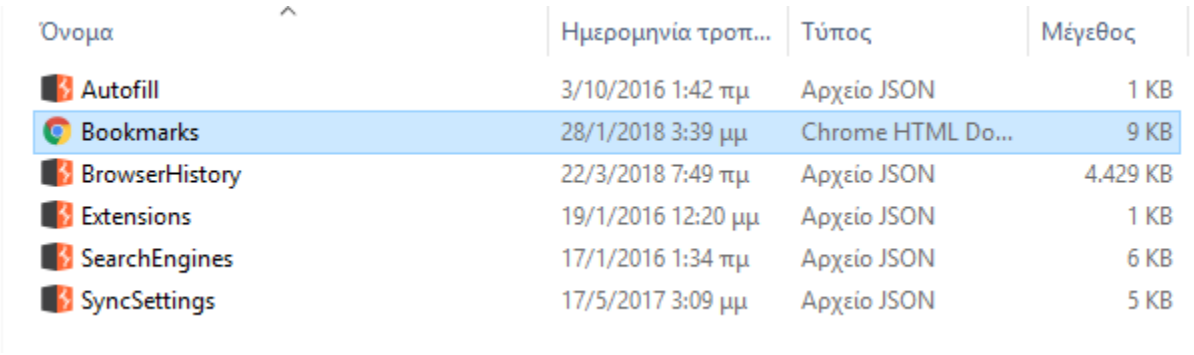
Το αρχείο μας κατέβηκε στον υπολογιστή μας με κατάληξη .zip και έχει μέγεθος 363 MB. Κάνοντας extract τα δεδομένα μας παίρνουμε τα παρακάτω αρχεία:



Εικόνα 5.48 Αρχεία του Takeout μετά την αποσυμπίεση του αρχείου

Επειδή τα αρχεία που ανακτήθηκαν είναι πάρα πολλά θα αναφερθούμε στα πιο σημαντικά.

- ***Chrome***

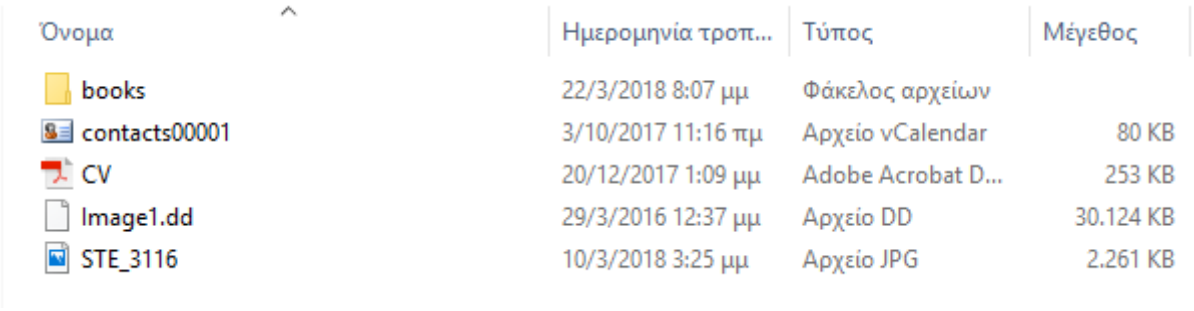


Όνομα	Ημερομηνία τροπ...	Τύπος	Μέγεθος
Autofill	3/10/2016 1:42 πμ	Αρχείο JSON	1 KB
Bookmarks	28/1/2018 3:39 μμ	Chrome HTML Do...	9 KB
BrowserHistory	22/3/2018 7:49 πμ	Αρχείο JSON	4.429 KB
Extensions	19/1/2016 12:20 μμ	Αρχείο JSON	1 KB
SearchEngines	17/1/2016 1:34 πμ	Αρχείο JSON	6 KB
SyncSettings	17/5/2017 3:09 μμ	Αρχείο JSON	5 KB

Εικόνα 5.49 Αρχεία Ανάκτησης του Chrome

Σε αυτά τα αρχεία αναφέρονται οι σελιδοδείκτες, το ιστορικό του browser και τα extensions που έχει ο φυλλομετρητής.

- ***Drive***

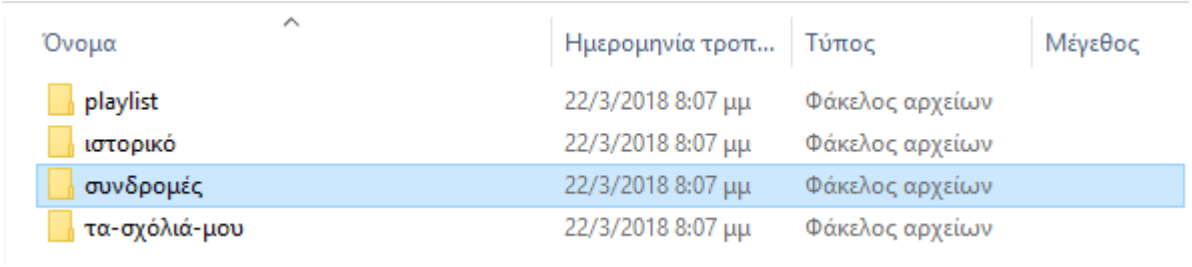


Όνομα	Ημερομηνία τροπ...	Τύπος	Μέγεθος
books	22/3/2018 8:07 μμ	Φάκελος αρχείων	
contacts00001	3/10/2017 11:16 πμ	Αρχείο vCalendar	80 KB
CV	20/12/2017 1:09 μμ	Adobe Acrobat D...	253 KB
Image1.dd	29/3/2016 12:37 μμ	Αρχείο DD	30.124 KB
STE_3116	10/3/2018 3:25 μμ	Αρχείο JPG	2.261 KB

Εικόνα 5.50 Αρχεία ανάκτησης από το Google Drive

Στο φάκελο «Drive» αναφέρονται όλα τα αρχεία που έχουν ανέβει από το χρήστη στην υπηρεσία του Google Drive.

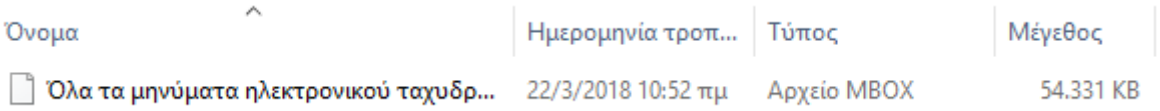
- ***Youtube***



Εικόνα 5.51 Αρχεία ανάκτησης από Youtube

Στο φάκελο «Youtube» αναφέρονται οι playlist που έχει κάνει ο χρήστης, το ιστορικό των video που είδε και τα σχόλια που έχει κάνει.

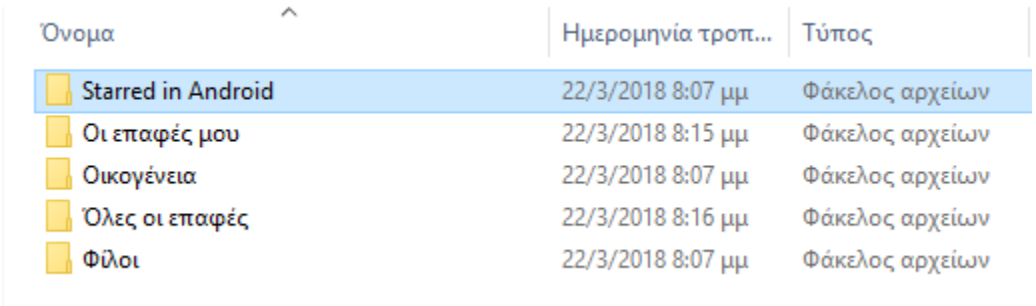
- ***Αλληλογραφία***



Εικόνα 5.52 Αρχείο ανάκτησης ηλεκτρονικής αλληλογραφίας

Στο φάκελο «αλληλογραφία» είναι όλα τα email που έχει στο λογαριασμό του Gmail ο χρήστης. Τα emails είναι κρυπτογραφημένα και δεν μπορούν, κατ' αρχήν, να αναγνωστούν.

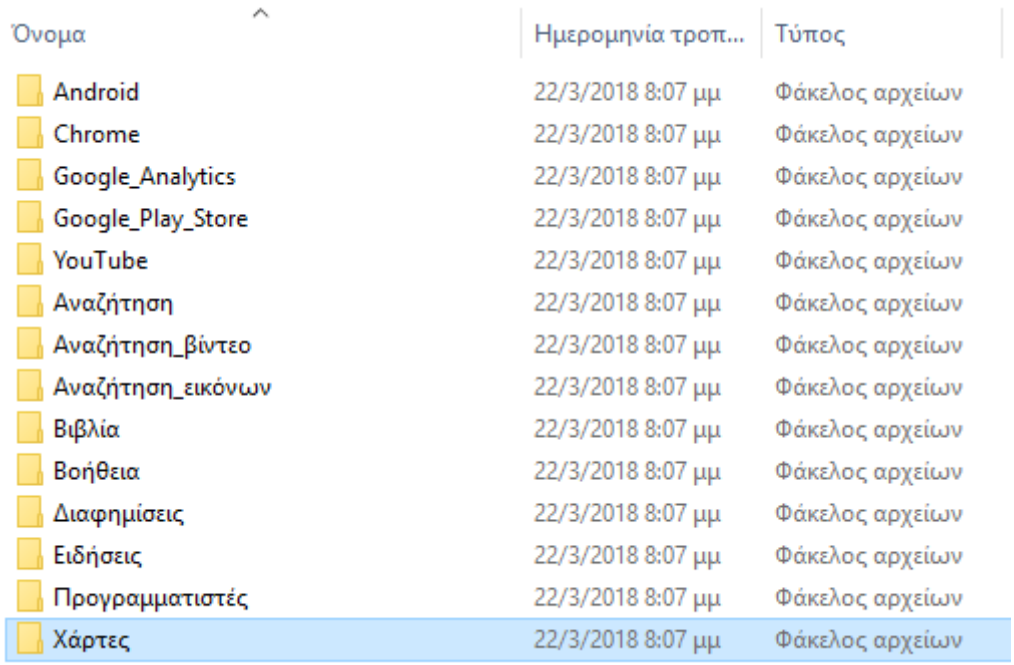
- ***Επαφές***



Εικόνα 5.53 Αρχεία ανάκτησης επαφών

Στο φάκελο «επαφές» αναφέρονται όλες οι επαφές σε αρχεία. Βέβαια εφόσον είναι χωρισμένες οι επαφές στο κινητό ανά ομάδα είναι χωρισμένες και στο backup.

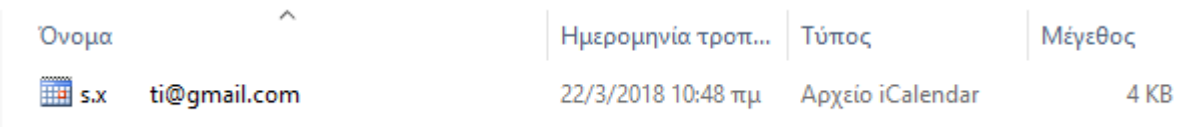
- ***Η δραστηριότητά μου***



Εικόνα 5.54 Αρχεία ανάκτησης της δραστηριότητας

Στο φάκελο «η δραστηριότητά μου» περιέχονται πολύ κρίσιμα αρχεία για τον ψηφιακό εγκληματολόγο αφού σχετίζονται με τις περιηγήσεις του χρήστη, την αναζήτηση του χρήστη σε video, εικόνες, youtube, βιβλία, διαφημίσεις που έχει δει ο χρήστης, ειδήσεις, τις εφαρμογές της «έξυπνης» κινητής συσκευής, τους χάρτες και τις τοποθεσίες που έχουν αναζητηθεί.

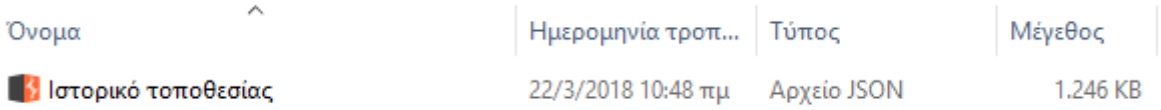
- ***Ημερολόγιο***



Εικόνα 5.55 Αρχείο Ημερολογίου

Σε αυτό το αρχείο αναφέρονται όλα τα γεγονότα που έχουν αποθηκευτεί στο ημερολόγιο του χρήστη.

- ***Ιστορικό Τοποθεσίας***



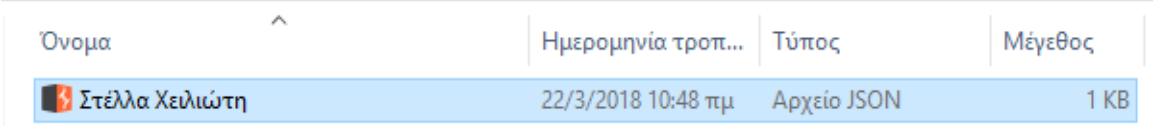
Εικόνα 5.56 Αρχείο Ιστορικού Τοποθεσίας

Σε αρχείο «Ιστορικό Τοποθεσίας» αναφέρονται όλες οι γεωγραφικές τοποθεσίας που έχει εντοπίσει το GPS για την τοποθεσίες του χρήστη. Όπως για παράδειγμα το παρακάτω:


```
{
  "locations" : [ {
    "timestampMs" : "1520800619000",
    "latitudeE7" : 659667000,
    "longitudeE7" : -185333000,
    "accuracy" : 11,
    "altitude" : 15,
    "verticalAccuracy" : 22
  }, {
    "timestampMs" : "1520800603000",
    "latitudeE7" : 659667000,
    "longitudeE7" : -185333000,
    "accuracy" : 10,
    "heading" : 0,
    "altitude" : 15,
    "verticalAccuracy" : 20
  }, {
```


Εικόνα 5.57 Αρχείο Συντεταγμένων

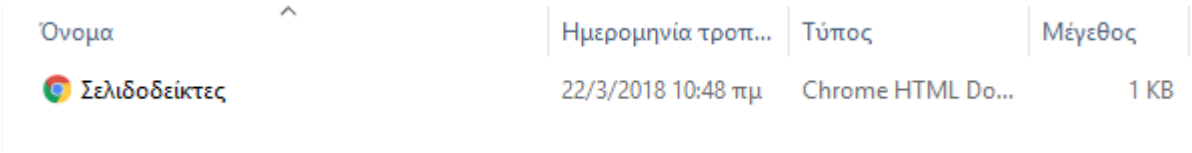
- ***Προφίλ***



Εικόνα 5.58 Προφίλ της Google

Σε αυτό το φάκελο αναφέρεται το προφίλ του χρήστη στη Google.

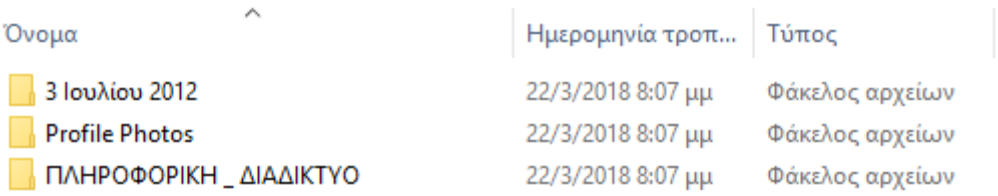
- ***Σελιδοδείκτες***



Εικόνα 5.59 Αρχείο σελιδοδεικτών του φυλλομετρητή

Εδώ υπάρχουν όλοι οι σελιδοδείκτες που έχει ο χρήστης.

- ***Φωτογραφίες της Google***



Εικόνα 5.60 Αρχεία από φωτογραφίες της Google

Σε αυτό το φάκελο εμφανίζονται όλες οι φωτογραφίες που έχει ο χρήστης.

Τα αποτελέσματα που πήραμε από το Takeout της Google είναι εξαιρετικά. Έχει γίνει εις βάθος ανάλυση των δεδομένων που υπάρχει στην «έξυπνη» κινητή συσκευή μας. Μια σημαντική παρατήρηση που ανέκυψε κατά την έρευνά μας είναι ότι το εργαλείο δεν εξάγει δεδομένα μόνο από την συγκεκριμένη «έξυπνη» κινητή συσκευή αλλά από όλες τις συσκευές που χρησιμοποιούν την ίδια ηλεκτρονική διεύθυνση.

Αποτίμηση

Σε αυτό το σημείο θα κάνουμε αποτίμηση της πρακτικής διαδικασίας. Πρώτα από όλα θα συγκρίνουμε τα εγκληματολογικά εργαλεία που χρησιμοποιήσαμε καθώς και θα περιγράψουμε συνοπτικά τα αποτελέσματα που λάβαμε από τις δοκιμές μας.

Τα εργαλεία που χρησιμοποιήσαμε είναι το AFLogical -OSE, το Foroboto, το Dumpsys, το DiskDigger και το Google TakeOut. Θα αναφέρουμε συνοπτικά τα μειονεκτήματα και τα πλεονεκτήματα κάθε εργαλείου.

Το εργαλείο ***AFLogical*** κάνει λογική ανάκτηση δεδομένων, δηλαδή ανακτά τα δεδομένα τα οποία υπάρχουν και όχι διαγραμμένα αρχεία. Είναι περιορισμένες οι μορφές αρχείων που ανακτά όπως κλήσεις, επαφές, εικονομηνύματα και μηνύματα. Δεν ανακτά ιστορικό browser ούτε συντεταγμένες ούτε εικόνες ούτε βίντεο. Τα αποτελέσματα που πήραμε ήταν τα αναμενόμενα. Εκτός από το email και το IMEI της «έξυπνης» κινητής συσκευής δεν εντοπίσαμε κάποιο άλλο προσωπικό δεδομένο που να έχει ανακτήσει χωρίς να υπάρχει στην περιγραφή του εργαλείου. Η ανάλυση μέσω του Proxy (Burp Suite) δεν κατέδειξε κάποια άλλη εξερχόμενη πληροφορία.

Το εργαλείο ***Foroboto*** κάνει επίσης λογική ανάκτηση των δεδομένων όπως και το AFLogical. Στα πλεονεκτήματά του είναι ότι ανακτά όλο το λειτουργικό σύστημα της συσκευής καθώς και τα δεδομένα της sdcard. Επίσης, κάνει ανάλυση δικτύου με αποτέλεσμα να παρέχει πληροφορίες και για το δίκτυο. Επιπλέον, αναλύει την μνήμη, την cpu, την ip, τις ενεργές συνδέσεις της συσκευής και το interface. Η ανάλυση μέσω του Proxy (Burp Suite) δεν έδειξε κάποια άλλη εξερχόμενη πληροφορία.

Το εργαλείο ***Dumpsys*** δεν κάνει λογική ανάκτηση δεδομένων απλώς παρέχει τη δυνατότητα στο χρήστη του προγράμματος να εξάγει δεδομένα για τις υπηρεσίες του συστήματος για παράδειγμα πόση μνήμη χρησιμοποιείται, πληροφορίες για την CPU, για την μπαταρία της συσκευής, πληροφορίες για το δίκτυο της συσκευής (IP Address, gateway, DNS Server, Domains DHSP server, Dns Address, Http Proxy). Δεν ανακτά δεδομένα όπως μηνύματα, κλήσεις, ιστορικό, τοποθεσία κλπ. Η ανάλυση μέσω του Proxy (Burp Suite) δεν έδειξε κάποια άλλη εξερχόμενη πληροφορία.

Η εφαρμογή ***DiskDigger*** παρέχει φυσική ανάκτηση των δεδομένων, δηλαδή ο χρήστης έχει την δυνατότητα να ανακτήσει δεδομένα που έχουν διαγραφεί. Στην δωρεάν έκδοση παρέχει την δυνατότητα ανάκτησης μόνο για φωτογραφίες (JPEG & PNG) και για video

(mp4). Στην έκδοση PRO οι δυνατότητες του εργαλείου είναι περισσότερες όπως αναφέραμε και σε προηγούμενο κεφάλαιο. Η δυναμική ανάλυση της εφαρμογής δεν έδειξε κάτι περαιτέρω ως προς τυχόν άλλη επεξεργασία δεδομένων.

Το εργαλείο της ***Google Takeout*** παρέχει λογική ανάκτηση δεδομένων μέσω του backup. Παρέχει στον ψηφιακό εγκληματολόγο πληροφορίες που είναι υψίστης σημασίας για την έκβαση της υπόθεσης. Παρέχει δεδομένα GPS, αναζήτηση σε χάρτες, ιστορικό browser, επαφές, σελιδοδείκτες, σχόλια, ιστορικό youtube, ειδήσεις που έχει δει ο χρήστης, αναζητήσεις για εικόνες και βίντεο, emails κλπ. Το μεγαλύτερο πλεονέκτημά του βέβαια είναι ότι αυτά τα δεδομένα που έχει ανακτήσει δεν είναι μόνο από την συγκεκριμένη συσκευή αλλά από όλες τις «έξυπνες» κινητές συσκευές που έχει τοποθετηθεί η συγκεκριμένη ηλεκτρονική διεύθυνση Gmail. Για τον ψηφιακό εγκληματολόγο αυτό είναι από τα δυνατά του «χαρτιά» εφόσον ακόμα και αν άλλες συσκευές δεν είναι στην κατοχή του μπορεί να αποκτήσει τα συγκεκριμένα αρχεία. Τα μειονεκτήματά του βέβαια είναι πρώτον, ότι ο ψηφιακός εγκληματολόγος θα πρέπει να γνωρίζει το gmail και το password του χρήστη ώστε να έχει πρόσβαση στο αρχείο zip εφόσον το link θα σταλθεί μέσω email και δεύτερον, ο χρήστης θα πρέπει να έχει ενεργοποιημένη την επιλογή back up στη συσκευή του.

Συνοψίζοντας, αντιλαμβανόμαστε ότι κανένα εργαλείο/εφαρμογή από αυτά που εφαρμόσαμε στο πρακτικό κομμάτι δεν αποτελεί ολοκληρωμένη λύση για την εγκληματολογική εξέταση μιας «έξυπνης» κινητής συσκευής αλλά φαίνεται ότι θα πρέπει να χρησιμοποιούνται συνδυαστικά.

Κεφάλαιο 6
Ειδικές Περιπτώσεις

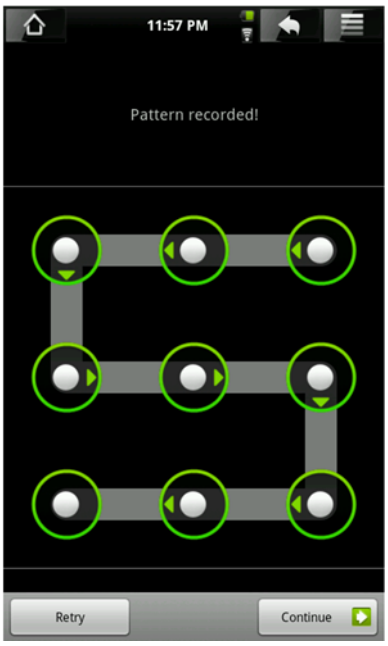
Σε αυτό το κεφάλαιο θα αναλυθούν περιπτώσεις των «έξυπνων» κινητών συσκευών στις οποίες η πρόσβαση και η ανάκτηση δεδομένων από αυτές είναι δύσκολη για τους λόγους που θα εξηγηθούν στη συνέχεια - και ως εκ τούτου θα πρέπει να ακολουθηθεί διαφορετική διαδικασία.

6.1 Κλειδωμένη Συσκευή

Η δυνατότητα των «έξυπνων» κινητών συσκευών να προστατεύεται από κάποιον «κωδικό» πρόσβασης είναι όλο και πιο συχνό φαινόμενο στις μέρες μας. Οι άνθρωποι θέλουν να έχουν την αίσθηση ότι τα ευαίσθητα προσωπικά τους δεδομένα προστατεύονται από μη εξουσιοδοτημένα άτομα. Υπάρχουν τέσσερις τύποι προστασίας σε συσκευές Androidοι οποίοι είναι οι εξής

Pattern

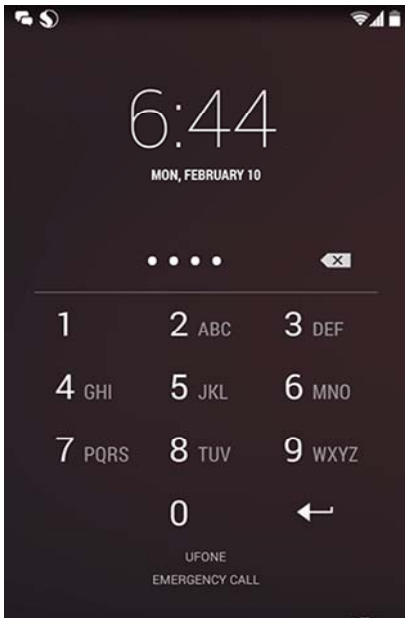
Το μοτίβο ήταν η προεπιλεγμένη μορφή προστασίας σε παλιές συσκευές. Ο χρήστης σχεδιάζει ένα μοτίβο επιλέγοντας μια διαδρομή ανάμεσα στα 9 σημεία του μοτίβου. Σε περίπτωση που ο χρήστης κάνει 5 φορές λάθος το μοτίβο θα πρέπει να περιμένει 30 δευτερόλεπτα ώστε να έχει ξανά την δυνατότητα να μπορέσει να το σχεδιάσει ξανά.



Εικόνα 6.1 Pattern [34]

PIN

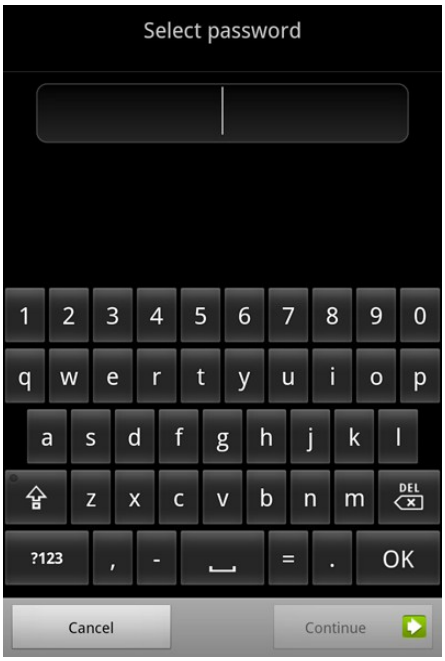
Ο πιο κοινός κωδικός προστασίας είναι το PIN. Το PIN αποτελείται από 4 ψηφία από το 0-9.



Εικόνα 6.2 PIN [35]

Password

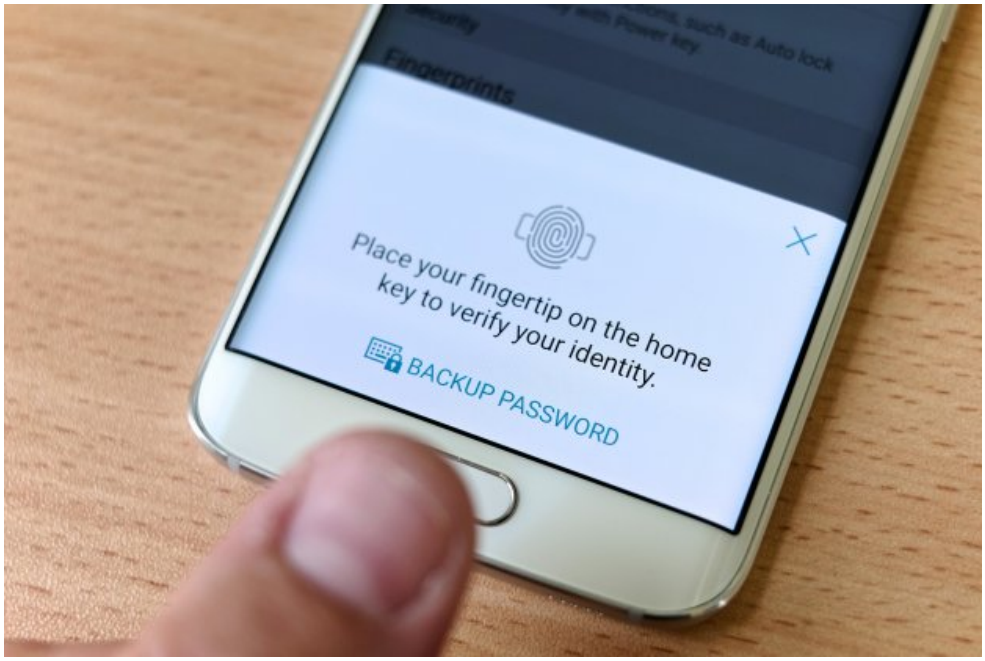
Ο τρίτος τρόπος προστασίας των δεδομένων είναι το password ή αλλιώς κωδικός. Αποτελείται από γράμματα (κεφαλαία, μικρά) και νούμερα. Ο κωδικός πρόσβασης μπορεί να απαρτίζεται μέχρι 16 χαρακτήρες, γεγονός που τον ισχυροποιεί έναντι επιθέσεων brute force attack ή dictionary attack.



Εικόνα 6.3 Password [36]

Fingerprint

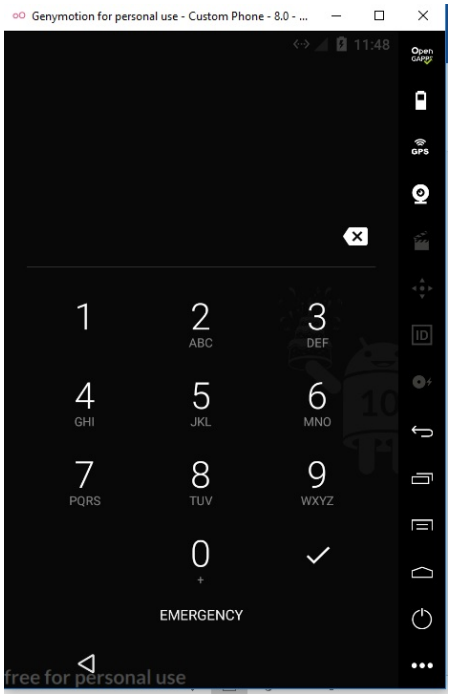
Οι καινούργιες «έξυπνες» κινητές συσκευές έχουν ένα νέο τρόπο προστασίας, το δαχτυλικό αποτύπωμα. Οι χρήστες σκανάρουν τα δαχτυλικά αποτυπώματα τους ένα-ένα και τα προσθέτουνε στη βάση δεδομένων του κινητού. Κάθε φορά που ο χρήστης θέλει να ξεκλειδώσει την συσκευή του θα πρέπει να ακουμπήσει το δάχτυλό του στην κατάλληλη υποδοχή του τηλεφώνου. Με αυτό τον τρόπο η συσκευή θα ξεκλειδώσει κατευθείαν. Είναι ο πιο εύκολος τρόπος ξεκλειδώματος εφόσον ο χρήστης δεν έχει να θυμηθεί τον κωδικό πρόσβασής του, δεν υπάρχει περίπτωση να τον ξεχάσει. Σε περίπτωση που κολλήσει ή χαλάσει η υποδοχή του δαχτυλικού αποτυπώματος της συσκευής υπάρχει εναλλακτικός κωδικός πρόσβασης όπως για παράδειγμα το μοτίβο που προ-είπαμε.



Εικόνα 6.4 Fingerprint [37]

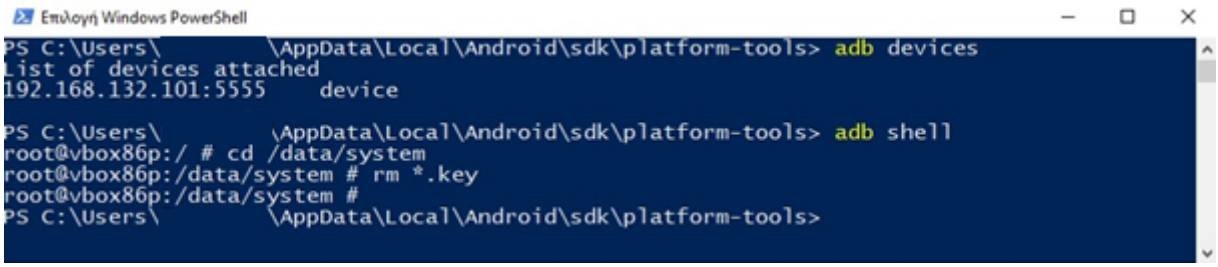
Στις περισσότερες «έξυπνες» κινητές συσκευές η πρόσβαση σε αυτές είναι εύκολη αν ξέρουμε το Gmail του χρήστη και τον κωδικό πρόσβασης σε αυτό. Μετά από πλήθος αποτυχημένων προσπαθειών στον κωδικό πρόσβασης εμφανίζεται μια οθόνη που ζητάει στον χρήστη να εισάγει το Gmail του και τον κωδικό πρόσβασης του σε περίπτωση που έχει ξεχάσει topin/password/pattern του.

Ας υποθέσουμε ότι η «έξυπνη» κινητή συσκευή μας έχει PIN ή κάποιο μοτίβο έτσι ώστε να προστατεύονται τα δεδομένα. Για να αποκτήσει ο ψηφιακός εγκληματολόγος πρόσβαση στο κινητό τηλέφωνο θα πρέπει να απενεργοποιήσει το PIN, το μοτίβο ή τον αλφαριθμητικό κωδικό.



Εικόνα 6.5 Κωδικός PIN στη συσκευή

Θα απενεργοποιήσουμε τον κωδικό πρόσβασης χρησιμοποιώντας το ADB.



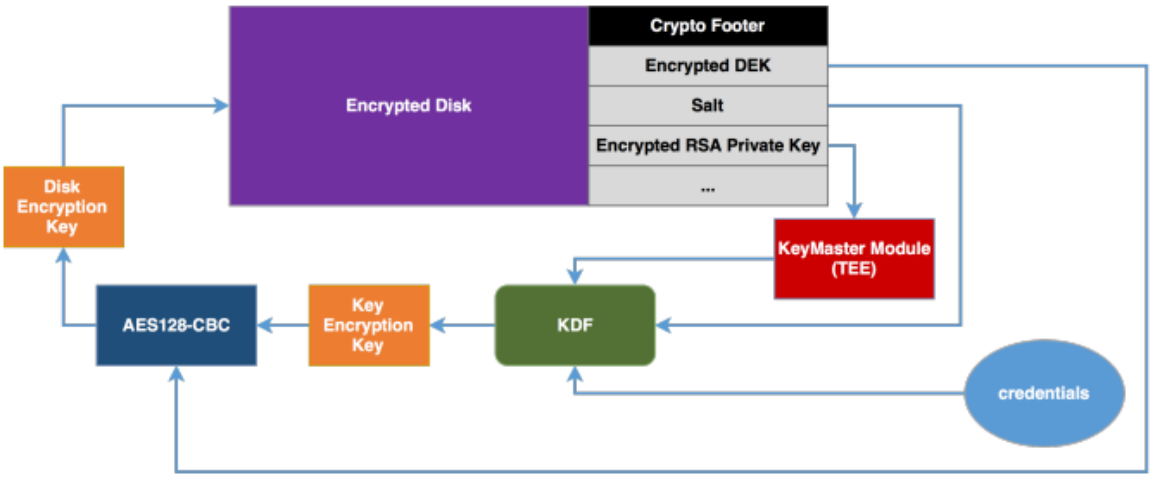
Εικόνα 6.6 Διαγραφή αρχείου στην «έξυπνη» κινητή συσκευή με κατάληξη .key το οποίο βρίσκεται στο φάκελο /data/system/

Διαγράψαμε το αρχείο **.key* που περιέχει τον κωδικό πρόσβασης και το οποίο βρίσκεται στην διαδρομή */data/system.* Κάνοντας επανεκκίνηση την «έξυπνη» κινητή συσκευή ο κωδικός πρόσβασης δεν υπάρχει και έχουμε πλέον πλήρη πρόσβαση στα δεδομένα.

6.2 Κρυπτογράφηση Δεδομένων

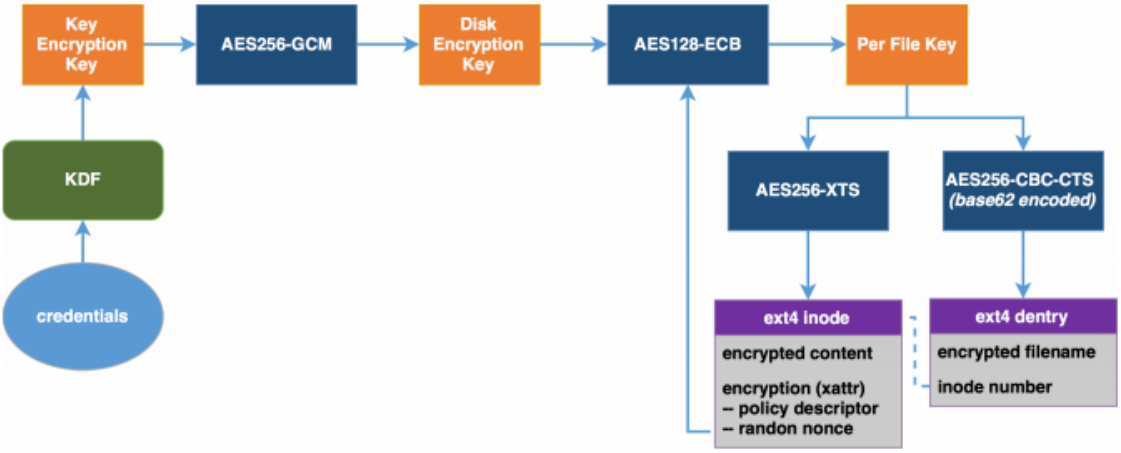
Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να «μετατρέψει» όλα τα δεδομένα σε μια μορφή έτσι ώστε να μην είναι προσβάσιμα σε μη εξουσιοδοτημένο άτομο αν δεν έχει το κλειδί αποκρυπτογράφησης. Η συγκεκριμένη διαδικασία διασφαλίζει ότι ακόμα κι αν κάποιος αποκτήσει πρόσβαση σε αυτά δεν είναι σε θέση να τα διαβάσει. Το λειτουργικό σύστημα Android έχει δύο μεθόδους κρυπτογράφησης των δεδομένων την κρυπτογράφηση full-disk και την file-based.

Η Full-disk κρυπτογράφηση αναφέρεται σε εκδόσεις λειτουργικού συστήματος από 5.0 και κάτω. Η κρυπτογράφηση όλου του δίσκου βασίζεται σε ένα μοναδικό κλειδί, ο κωδικός της συσκευής, ο οποίος κρυπτογραφεί και τα δεδομένα. Τα δεδομένα κρυπτογραφούνται πριν αποθηκευτούν στη συσκευή και αποκρυπτογραφούνται αφού ανακτηθούν από αυτή.



Εικόνα 6.7 FDE Decryption Process [38]

Η File-based κρυπτογράφηση αναφέρεται σε εκδόσεις λειτουργικού συστήματος από 6.0 και πάνω. Η κρυπτογράφηση βασισμένη σε αρχεία επιτρέπει την ξεχωριστή κρυπτογράφηση κάθε αρχείου μεμονωμένα και με διαφορετικά κλειδιά το καθένα.



Εικόνα 6.8 FBE Decryption Process [38]

Η διαφορά μεταξύ των δυο είναι ότι στην κρυπτογράφηση των δεδομένων με full-disk τα δεδομένα είναι ασφαλή όταν η συσκευή είναι απενεργοποιημένη. Όταν η συσκευή κάνει εκκίνηση τότε αυτόματα τα δεδομένα αποκρυπτογραφούνται αλλιώς δεν μπορεί να ξεκινήσει το λειτουργικό σύστημα. Για αυτόν τον λόγο αν η συσκευή συνδεθεί σε έναν υπολογιστή με καλώδιο τα δεδομένα μπορούν να διαβαστούν κανονικά. Αντιθέτως, στην κρυπτογράφηση με File-based αυτό δεν συμβαίνει. Η κρυπτογράφηση των δεδομένων είναι ενεργή καθ' όλη την διάρκεια που η συσκευή είναι ενεργοποιημένη.

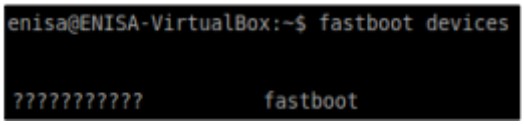
Το κλειδί της αποκρυπτογράφησης μπορεί να αποκτηθεί με τις κατάλληλες επιθέσεις όπως για παράδειγμα Brute Force Attack η οποία προσπαθεί να βρει το κλειδί δοκιμάζοντας όλα τα πιθανά κλειδιά απευθείας στη συσκευή. Η συγκεκριμένη διαδικασία περιγράφεται στο εγχειρίδιο Mobile Threats Incident Handling (Part II) του Ευρωπαϊκού Οργανισμού European Union Agency For Network And Information Security (ENISA) [23] και παρατίθεται στη συνέχεια για λόγους πληρότητας.

Αρχικά, τοποθετούμε την συσκευή μας σε recovery mode για να μπορέσουμε να την ξεκινήσουμε με recovery image. Αν η συσκευή μας είναι συνδεδεμένη με το ADB εργαλείο τότε δίνουμε την παρακάτω εντολή.

```
enisa@ENISA-VirtualBox:~$ adb reboot bootloader
```

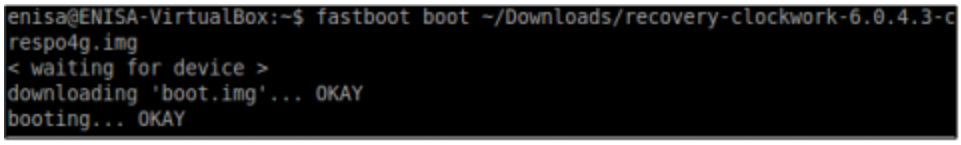
Εικόνα 6.9 Recovery Image [23]

Ύστερα ξεκινάμε την συσκευή μας με μια rooted recovery image από την συσκευή μας. Έπειτα, θα πρέπει να εκτελέσουμε την εξής εντολή.



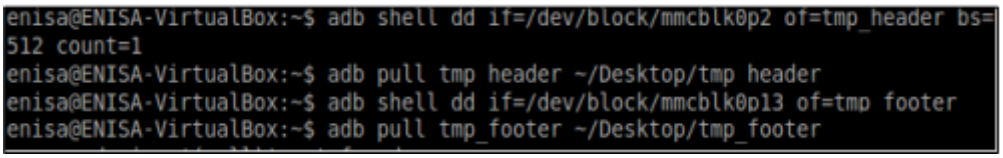
Εικόνα 6.10 Fastboot [23]

Εφόσον ελέγξαμε ότι η συσκευή μας επικοινωνεί με το fastboot κάνουμε επανεκκίνηση της συσκευή μας «φορτώνοντας» την recovery image.



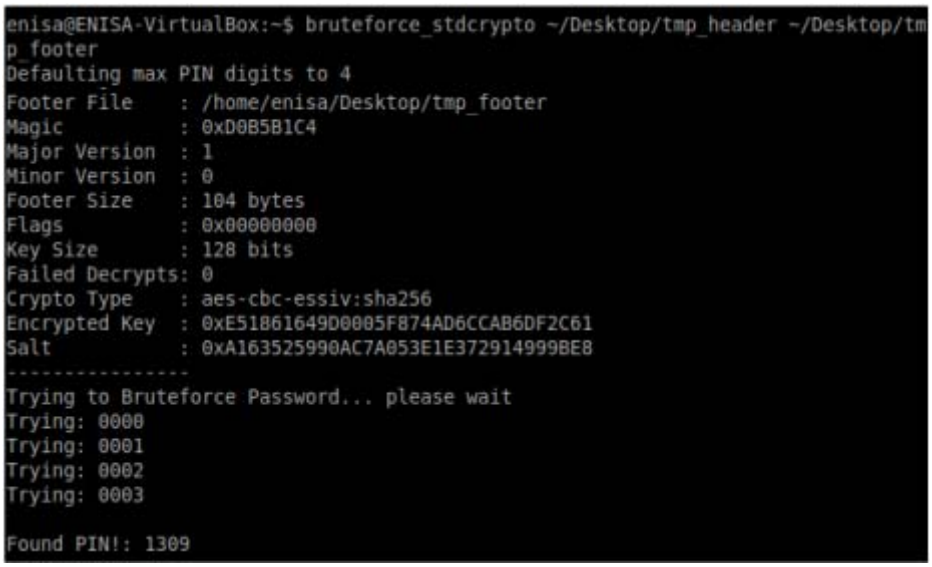
Εικόνα 6.11 Fastboot & Recovery Image [23]

Σε αυτό το σημείο η συσκευή μας είναι σε recovery mode. Λαμβάνοντας υπόψη ότι για να βρούμε το PIN της κρυπτογράφησης θα πρέπει να έχουμε το header και το footer της εικόνας (image) του αρχείου /system/, αντιγράφονται στον υπολογιστή.



Εικόνα 6.12 Header and Footer [23]

Το επόμενο και τελευταίο μας βήμα είναι να χρησιμοποιήσουμε ένα πρόγραμμα που δοκιμάζει όλους τους πιθανούς κωδικούς όπως το Android Brute Force Encryption.



Εικόνα 6.13 Android Brute Force Encryption[23]

Ύστερα από λίγο το πρόγραμμα θα εμφανίσει τον κωδικό της κρυπτογράφησης. Σε περίπτωση που περιγράψαμε ο κωδικός, όπως φαίνεται στη Εικόνα 6.13, ήταν 1309.

Κεφάλαιο 7
Επίλογος

Στην παρούσα μεταπτυχιακή διατριβή ασχοληθήκαμε με την ανάλυση εφαρμογών και ψηφιακών πειστηρίων σε «έξυπνες» κινητές συσκευές. Σκοπός της μεταπτυχιακής διατριβής ήταν να δημιουργήσουμε ένα «εργαστήριο» στο οποίο θα δοκιμάσουμε διάφορα εγκληματολογικά εργαλεία και εφαρμογές σε πραγματικό χρόνο σε μια «έξυπνη» κινητή συσκευή έτσι ώστε να αναλύσουμε τα χαρακτηριστικά των εν λόγω εργαλείων και τα δεδομένα που ανακτήσαμε μέσω αυτών. Έμφαση δόθηκε σε δωρεάν εργαλεία, τα οποία μπορούν προφανώς να χρησιμοποιηθούν από τον οποιοδήποτε – ακόμα και από άτομο εκτός του χώρου της εγκληματολογίας.

Αρχικά αναφέραμε κάποιες γενικές πληροφορίες για το λειτουργικό σύστημα Android, τις εκδόσεις στις οποίες υπάρχει, την αρχιτεκτονική του καθώς και πως δομούνται, οργανώνονται και αποθηκεύονται τα αρχεία στα αντίστοιχα Partitions στις «έξυπνες» κινητές συσκευές ώστε να υπάρχει το θεωρητικό υπόβαθρο για αυτά που έπονται.

Έπειτα, αναφερθήκαμε στους ορισμούς των ψηφιακών πειστηρίων και περιγράψαμε αναλυτικά την μεθοδολογία της ψηφιακής έρευνας. Η μεθοδολογία της ψηφιακής έρευνας είναι από τα σημαντικότερα κομμάτια εφόσον μας εξασφαλίζει μια αδιαμφισβήτητη έρευνα που ευσταθεί ενώπιον δικαστηρίου. Ο ψηφιακός εγκληματολόγος θα πρέπει να τηρήσει την διαδικασία σε όλα τα στάδια της ώστε να έχει μια επιτυχή έκβαση της υπόθεσης.

Εν συνεχεία, περιγράψαμε το «εργαστήριο» που εφαρμόσαμε το πρακτικό κομμάτι της μεταπτυχιακής διατριβής. Αναφέραμε τα χαρακτηριστικά της «έξυπνης» εικονικής συσκευής που δημιουργήσαμε καθώς και τα προγράμματα που εγκαταστήσαμε σε αυτό έτσι ώστε η κίνηση του τηλεφώνου να εξέρχεται διαμέσου ενός Proxy (Burp Suite) για να μπορέσουμε να δούμε τα δεδομένα που εξέρχονται πριν αυτά κρυπτογραφηθούν.

Επιπλέον, δοκιμάσαμε 5 εγκληματολογικά εργαλεία (AFLogical-OSE, Foroboto, Dumpsys, DiskDigger, Google Takeout) υλοποιώντας τόσο λογική όσο και φυσική

ανάκτηση δεδομένων σε ένα εικονικό τηλέφωνο με λειτουργικό σύστημα Android 7.1.1 Nougat. Αναφέραμε όλα τα ψηφιακά πειστήρια που κρίναμε ότι είναι άξια λόγου καθώς και τα αποτελέσματα που λάβαμε από την δυναμική ανάλυση των εργαλείων/εφαρμογών. Τα εν λόγω εργαλεία μελετήθηκαν και από τη σκοπιά του εάν η λειτουργίας τους έχει ως αποτέλεσμα την αποστολή δεδομένων της συσκευής σε τρίτο (είτε στις κατασκευάστριες εταιρίες των λογισμικών αυτών είτε σε άλλον), χωρίς όμως να παρατηρηθεί, τελικά, κάτι τέτοιο. Επίσης, συγκρίναμε τα εργαλεία μεταξύ τους και αναφέραμε τα μειονεκτήματα και τα πλεονεκτήματά τους. Όπως είπαμε και παραπάνω, κανένα εργαλείο από αυτά που μελετήθηκαν δεν μπορεί να θεωρηθεί ως πλήρες και να χρησιμοποιηθεί μεμονωμένα αλλά φαίνεται ότι μια βέλτιστη ανάλυση θα απαιτούσε συνδυαστική χρήση αυτών.

Επιπροσθέτως, περιγράψαμε κάποιες ειδικές περιπτώσεις, όπως το PIN και η κρυπτογράφηση του κινητού τηλεφώνου, που επιφέρουν κάποια δυσκολία στον ψηφιακό εγκληματολόγο να αποκτήσει πρόσβαση στα δεδομένα της «έξυπνης» κινητής συσκευής δίνοντας λύση.

Συνοψίζοντας, συμπεραίνουμε ότι τα συγκεκριμένα ενδεικτικά εργαλεία της ψηφιακής εγκληματολογίας εκτός από τα δεδομένα που αναφέρουν ότι εξάγουν (μηνύματα, εικονομηνύματα, συντεταγμένες, τοποθεσίες, ιστορικό περιηγητή, εικόνες, video, πληροφορίες για το δίκτυο) από την «έξυπνη» κινητή συσκευή, δεν φαίνεται ότι εξάγουν άλλα προσωπικά δεδομένα τα οποία να στέλνουν σε κάποιον «τρίτο» πρόσωπο. Αυτό το αντιληφθήκαμε μέσω της δυναμικής ανάλυσης των εργαλείων.

Τα αποτελέσματα που πήραμε χαρακτηρίζονται μάλλον ως αναμενόμενα και όχι ανησυχητικά. Ως εργαλεία της ψηφιακής εγκληματολογίας δεν θα έπρεπε να ανακτούν πληροφορίες που δεν αναφέρουν ή που δεν συμφωνήσαμε να έχουν πρόσβαση.

Η συγκεκριμένη μεταπτυχιακή διατριβή μπορεί να αποτελέσει πρακτικό οδηγό σε ερευνητές της εγκληματολογίας ή ακόμη και σε άτομα που τους ενδιαφέρει να ασχοληθούν στο μέλλον. Επίσης, η γνώση των δυνατοτήτων που παρέχουν τα εν λόγω, δωρεάν και ευκόλως διαθέσιμα εργαλεία, είναι εξαιρετικά σημαντική ακόμα και για απλούς χρήστες.

Βιβλιογραφία

[1] United States Census Bureau – World Population, https://www.census.gov/popclock/ [Πρόσβαση: 15 Οκτωβρίου 2017]

[2] GSMA Intelligence, https://www.gsmaintelligence.com/ [Πρόσβαση: 15 Οκτωβρίου 2017]

[3] Open Handset Alliance, Indrustry Leaders Announce Open Platform for Mobile Devices, 5 November, 2007 http://www.openhandsetalliance.com/press_110507.html

[4] Irina Blok, http://www.irinablok.com/android [Πρόσβαση: 10 Οκτωβρίου 2017]

[5] Dreamstime, https://www.dreamstime.com/editorial-photo-phitsanulok-thailand-october-vector-android-logo-image80056921 [Πρόσβαση: 10 Οκτωβρίου 2017]

[6] Statcounter GlobalStats, http://gs.statcounter.com/os-market-share/mobile/worldwide [Πρόσβαση: 10 Οκτωβρίου 2017]

[7] The Statistics Portal, https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ [Πρόσβαση: 10 Οκτωβρίου 2017]

[8] Android Version History, https://en.wikipedia.org/wiki/Android_version_history [Πρόσβαση: 10 Οκτωβρίου 2017]

[9] Android Operating System, https://en.wikipedia.org/wiki/Android_(operating_system) [Πρόσβαση: 10 Οκτωβρίου 2017]

[10] Android Boot Process, https://jiafei427.wordpress.com/2016/11/09/android-boot-process/ [Πρόσβαση: 10 Οκτωβρίου 2017]

[11] Mobile Device Forensics, https://en.wikipedia.org/wiki/Mobile_device_forensics [Πρόσβαση: 15 Οκτωβρίου 2017]

[12] SIM Card Forensics: An Introduction, http://resources.infosecinstitute.com/sim-card-forensics-introduction/#gref [Πρόσβαση: 15 Οκτωβρίου 2017]

[13] Memory Card, https://n1.sdlcdn.com/imgs/c/2/k/SanDisk-Ultra-32-GB-Micro-SDL128364209-5-1148f.jpg [Πρόσβαση: 15 Οκτωβρίου 2017]

[14] Mobile Forensics – Analysis Methology, http://4n6xplorer.com/forensics/mobile-device-forensic-process/ [Πρόσβαση: 15 Οκτωβρίου 2017]

[15] Faraday Bags, https://images-na.ssl-images-amazon.com/images/I/616Anprb1ZL._SL1200_.jpg [Πρόσβαση: 18 Οκτωβρίου 2017]

[16] Man in the Middle Attack, https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html [Πρόσβαση: 18 Οκτωβρίου 2017]

[17] Genymotion, https://www.genymotion.com/ [Πρόσβαση: 20 Οκτωβρίου 2017]

[18] Genymotion ARM Translation, https://gist.github.com/wbroek/9321145 [Πρόσβαση: 20 Οκτωβρίου 2017]

[19] Xposed Framework, https://www.xda-developers.com/official-xposed-framework-android-nougat/ [Πρόσβαση: 21 Οκτωβρίου 2017]

[20] Xposed Installer, http://repo.xposed.info/module/de.robv.android.xposed.installer [Πρόσβαση: 21 Οκτωβρίου 2017]

[21] Inspeckage, https://github.com/ac-pm/Inspeckage [Πρόσβαση: 21 Οκτωβρίου 2017]

[22] Android Studio & SDK Tools, https://developer.android.com/studio/index.html [Πρόσβαση: 22 Οκτωβρίου 2017]

[23] European Union Agency For Network And Information Security - «Mobile Threats Incident Handling (Part II) Handbook, Document for teachers», September 2015, pages 37-38

[24] Abdalazim Abdallah Mohammed Alamin – Dr. Amin Babiker A/Nabi Mustafa, «A Survey on Mobile Forensic for Android Smartphones,» *IOSR Journal of Computer Engineering (IOSR-JCE),* τόμ. 17, αρ. 2, pp. 15-19, Μάρτιος-Απρίλιος 2015

[25] Donnie Tindall - Rohit Tamma, «Learning Android Forensics», Packt, 2015.

[26] Kim_Kwang Raymond Choo - Ali Dehghantanha, «Contemporary Digital Forensic Investigations of Cloud and Mobile Applications», Syngress, 2017.

[27] Vladimir Katalov - Oleg Afonin, «Mobile Forensics - Advanced Investigative Strategies», Packt, 2016.

[28] Foroboto, https://el.wikibooks.org/wiki/%CE%91%CE%BD%CE%AC%CE%BB%CF%85%CF%83

%CE%B7_%CE%B5%CE%BD%CF%8C%CF%82_%CE%B5%CF%81%CE%B3%CE%B1%CE%BB%CE%B5%CE%AF%CE%BF%CF%85_forensic.

[29] Logo Via Forensics, https://www.featuredcustomers.com/customer/viaforensics/reviews [Πρόσβαση: 01 Νοεμβρίου 2017]

[30] Disk Digger https://diskdigger.org/ [Πρόσβαση: 01 Νοεμβρίου 2017]

[31] Disk Pro File Recover, https://play.google.com/store/apps/details?id=com.defianttech.diskdiggerpro&hl=el [Πρόσβαση: 03 Φεβρουαριου 2018]

[32] DiskDigger Photo Recovery, https://play.google.com/store/apps/details?id=com.defianttech.diskdigger&hl=en [Πρόσβαση: 03 Φεβρουαρίου 2018]

[33] Google Takeout, https://en.wikipedia.org/wiki/Google_Takeout [Πρόσβαση: 03 Φεβρουαρίου 2018]

[34] Android Pattern, https://playingwithmodels.wordpress.com/2010/04/14/andorid_unlock_patterns/

[Πρόσβαση: 10 Μαρτίου 2018]

[35] Android PIN, https://www.addictivetips.com/android/timepin-auto-change-android-lock-screen-pin-by-current-time/ [Πρόσβαση: 10 Μαρτίου 2018]

[36] Android Password, https://www.gottabemobile.com/how-to-android-lock-security/ [Πρόσβαση: 10 Μαρτίου 2018]

[37] Android Fingerprint, https://www.spaceotechnologies.com/integrate-android-fingerprint-api-tutorial/ [Πρόσβαση: 10 Μαρτίου 2018]

[38] R. Loftus και M. Baumann, «Android 7 File Based Encryption and the Attacks Against It», http://www.delaat.net/rp/2016-2017/p45/report.pdf , Ιανουάριους 2017 [Πρόσβαση: 10 Μαρτίου 2018]