Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

με κατεύθυνση στις

«Τεχνολογίες Διαχείρισης Ασφάλειας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ψηφιακή Εγκληματολογία σε έξυπνες συσκευές Android** **Forensics in Android Smart Devices**
Ονοματεπώνυμο Φοιτητή	**Αλέξανδρος Βασιλαράς**
Πατρώνυμο	**Κωνσταντίνος**
Αριθμός Μητρώου	**ΜΠΣΠ/13014**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου** **Επίκουρος Καθηγητής**
Συνεπιβλέπων Ερευνητής	**Παπαγεωργίου Σπυρίδων**

Ημερομηνία Παράδοσης **Μάρτιος 2016**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Παναγιώτης Κοτζανικολάου Επίκουρος Καθηγητής	Χρήστος Δουληγέρης Καθηγητής	Κωνσταντίνος Πατσάκης Λέκτορας

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον διευθυντή της Διεύθυνσης Κυβερνοάμυνας (ΔΙΚΥΒ) και καθηγητή μου στο μάθημα «Ανάλυση πειστηρίων & κακόβουλου λογισμικού» κ. Παπαγεωργίου Σπυρίδων & τον επιβλέποντα επίκουρο καθηγητή κ. Παναγιώτη Κοτζανικολάου για την σημαντική βοήθεια τους στην ολοκλήρωση αυτής της μεταπτυχιακής εργασίας. Θεωρώ την εμπειρία που αποκόμισα όχι μόνο χρήσιμη, αλλά απαραίτητη σε μελλοντική μου σταδιοδρομία. Λυπάμαι, όμως, γιατί ξέρω ότι δεν θα έχω πάντα την τύχη να συνεργάζομαι με τόσο αξιόλογους και αληθινούς ανθρώπους μελλοντικά.

Τέλος θα ήθελα να ευχαριστήσω την σύζυγο και την κόρη μου που είναι πάντα δίπλα μου και με στηρίζουν.

Περίληψη

Στην παρούσα μεταπτυχιακή διατριβή παρουσιάζονται τόσο θεωρητικά όσο και τεχνικά στοιχεία που απαρτίζουν την επιστήμη της “Ψηφιακής Εγκληματολογίας σε κινητές συσκευές Android”. Αρχικά, γίνεται αναφορά στην ραγδαία εξέλιξη των κινητών συσκευών καθώς και στο πόσο δημοφιλές είναι το λειτουργικό σύστημα Android. Στη συνέχεια, παρουσιάζονται βασικές έννοιες σχετικά με το λειτουργικό σύστημα Android όπως η αρχιτεκτονική, οι εκδόσεις και η δομή των δεδομένων του, ενώ ακολουθεί μια σύντομη περιγραφή ως προς τα βήματα και τους μεθόδους εγκληματολογικής εξέτασης μιας κινητής συσκευής Android, καθώς και στα εργαλεία που χρησιμοποιούνται για την εξέταση των συσκευών. Τέλος, πραγματοποιείται πειραματική υλοποίηση εξέτασης μιας πραγματικής συσκευής τηλεφώνου Android, χρησιμοποιώντας εμπορικά και ελεύθερα λογισμικά. Αξίζει να σημειωθεί ότι η εξέταση χωρίζεται σε δύο (2) κατηγορίες: α) κλειδωμένη κινητή συσκευή και β) ξεκλείδωτη.

Λέξεις Κλειδιά: ψηφιακή εγκληματολογία, έξυπνες κινητές συσκευές, android, φυσική και λογική εξαγωγή, στάδια εγκληματολογικής εξέτασης κινητών συσκευών

Abstract

This thesis describes the theoretical, as well as the technical aspect of the Digital Forensics on Android mobile devices. Firstly, an extent reference has been made to the rapid development of the mobile devices, as well as to the popularity of the Android operating system. Subsequently, the basic concepts on the Android operating system, such as its architecture, its edition and its data structure have been set out, before referring briefly to the steps, the methods and the tools of the forensic examination of a mobile Android device. Finally, a pilot test of a real Android phone device has been implemented, using both software (either commercial or free one) and manual analysis. It is to be noted that the afore–mentioned test is implemented on a locked mobile device, on the one hand, and on an unlocked one, on the other hand.

Keywords: Android forensics, physical and logical acquisition, mobile forensic examination process

Πίνακας Περιεχομένων

1 Εισαγωγή 10

1.1 Τεχνολογική Εξέλιξη κινητών συσκευών 10

1.2 Ορισμοί και έννοιες της ψηφιακής εγκληματολογίας 10

1.3 Εγκληματολογική Εξέταση κινητών συσκευών vs Ηλεκτρονικών υπολογιστών 11

1.4 Οι κινητές συσκευές τύπου Android 11

1.5 Διάρθρωση της Μελέτης 12

2 Λειτουργικό σύστημα Android 14

2.1 Η αρχιτεκτονική του Android 14

2.1.1 Πυρήνας του Linux (Linux kernel) 14

2.1.2 Βασικές Βιβλιοθήκες (Libraries) 15

2.1.3 Το επίπεδο εκτέλεσης (Android Runtime) 15

2.1.4 Το πλαίσιο εφαρμογής (Application Framework) 15

2.1.5 Επίπεδο Εφαρμογών (Applications) 16

2.2 Εκδόσεις Android 16

2.3 Το σύστημα Αρχείων (Filesystem) 16

3 Δομή Δεδομένων σε κινητές συσκευές Android 17

3.1 Εισαγωγή 17

3.2 Τι αναζητάμε 18

3.3 Μέσα αποθήκευσης 18

3.3.1 Κάρτα SIM 19

3.3.2 Εσωτερικός χώρος Συσκευής 20

3.3.3 Κάρτα μνήμης 20

3.3.4 Σύννεφο (Cloud) 21

4 Εργαλεία και μέθοδοι εξαγωγής ψηφιακών πειστηρίων σε κινητές συσκευές Android. 22

4.1 Εισαγωγικά 22

4.2 Εργαλεία εξαγωγής ψηφιακών πειστηρίων σε κινητές συσκευές Android 22

4.2.1 Cellebrite UFED 22

4.2.2 Micro systemation XRY 22

4.2.3 OXYGEN Forensic Suite 23

4.2.4 Ελεύθερο Λογισμικό - ViaExtract 23

4.3 Μέθοδοι Ανάλυσης εσωτερικού χώρου της κινητής συσκευής Android 23

4.4 Μέθοδος Ανάλυσης κάρτα μνήμης (android micro sd card Acquisition types) 26

4.5 Ανάλυση κάρτας SIM (Analysis SIM card) 26

5 Εγκληματολογική εξέταση κινητών συσκευών Android 28

5.1 Εισαγωγικά 28

5.2 Οι φάσεις της εξέτασης 29

5.2.1 Φάση 1η: Παραλαβή / Έναρξη της εξέτασης (Intake) 29

5.2.2 Φάση 2η: Αναγνώριση (Identification) 29

5.2.3 Φάση 3η: Προετοιμασία (Preparation) 29

5.2.4 Φάση 4η: Απομόνωση (Isolation) 29

5.2.5 Φάση 5η: Επεξεργασία (Processing) 30

5.2.5.1 Χειροκίνητη Επεξεργασία (χρήση του Adb) 31

5.2.5.1.1 Εισαγωγικά 31

5.2.5.1.2 Android Adb ... 31
5.2.5.1.3 Adb και USB Debugging ... 32
5.2.5.1.4 Δικαιώματα Διαχειριστή (Root) ... 33
5.2.5.1.5 Φάση 6η: Επαλήθευση (Verification) ... 34
5.2.5.1.6 Φάση 7η: Σύνταξη Αναφοράς (Documenting / Reporting) ... 34
5.2.5.1.7 Φάση 8η: Παρουσίαση (Presentation) ... 34
5.2.5.1.8 Φάση 9η: Αρχειοθέτηση (Archiving) ... 35
6 Πρακτικός οδηγός εξέταση κινητής συσκευής Android ... 36
6.1 Εισαγωγικά ... 36
6.2 Εξέταση Συσκευής - Πρώτη Περίπτωση [το κινητό να είναι κλειδωμένο (μοτίβο), USB debugging ON & no root access] ... 38
6.2.1 Το εμπορικό εργαλείο Celebrite ... 38
6.2.1 Το εργαλείο Cellebrite ... 38
6.2.1.1 Φυσική Εξαγωγή (Physical extraction) ... 38
6.2.1 Λογική Εξαγωγή (Logical extraction) ... 49
6.2.2 Το εργαλείο Oxygen ... 53
6.2.2.1 Φυσική Εξαγωγή (Physical extraction) ... 54
6.2.2.2 Λογική Εξαγωγή (Logical extraction) ... 58
6.2.3 Το ελεύθερο λογισμικό AFlogical viaExtract ... 61
6.2.3.1 Φυσική Εξαγωγή (Physical extraction) ... 62
6.2.3.1 Λογική Εξαγωγή (Logical extraction) ... 62
6.3 Εξέταση Συσκευής - Δεύτερη Περίπτωση [το κινητό δεν είναι κλειδωμένο & δεν υπάρχουν δικαιώματα διαχειριστή (no root)] ... 65
6.3.1 Το εργαλείο Celebrite ... 65
6.3.1.1 Φυσική Εξαγωγή (Physical extraction) ... 65
6.3.1.2 Λογική Εξαγωγή (Logical extraction) ... 65
6.3.2 Το εργαλείο Oxygen ... 69
6.3.2.1 Φυσική Εξαγωγή (Physical extraction) ... 70
6.3.2.2 Λογική Εξαγωγή (Logical extraction) ... 70
6.3.3 Το ελεύθερο λογισμικό AFlogical viaExtract ... 70
6.3.3.1 Φυσική Εξαγωγή (Physical extraction) ... 70
6.3.3.2 Λογική Εξαγωγή (Logical extraction) ... 70
6.4 Εξέταση Συσκευής - Χειροκίνητη ανάλυση της συσκευής ... 73
6.4.1 Εισαγωγικά ... 73
6.4.2 Το κινητό δεν είναι κλειδωμένο & δεν υπάρχουν δικαιώματα διαχειριστή (no root)] ... 73
6.4.2.1 Λογική Εξαγωγή (Logical extraction) και Ανάλυση των δεδομένων ... 73
6.4.2.1.1 Λογική Εξαγωγή (Logical extraction) ... 73
6.4.2.1.2 Ανάλυση των δεδομένων από τα αντίγραφα ασφαλείας (Backup) ... 76
6.4.2.2 Φυσική Εξαγωγή (physical Extraction) και Ανάλυση των δεδομένων με το εργαλείο Autopsy ... 80
6.4.2.2.1 Φυσική Εξαγωγή (physical Extraction) ... 80
6.4.2.2.2 Ανάλυση των δεδομένων με το εργαλείο Autopsy ... 84
6.4.3 Το κινητό είναι κλειδωμένο & δεν υπάρχουν δικαιώματα διαχειριστή (no root)] ... 93
6.4.3.1 Λογική Εξαγωγή (Logical extraction) ... 93
6.4.3.2 Φυσική Εξαγωγή (Physical extraction) ... 93
6.4.3.3 Ξεκλείδωμα της συσκευής μέσω της διαδικασίας της φυσικής εξαγωγής (Physical extraction) ... 93
6.5 Εξέταση Κάρτας SIM ... 94
6.6 Εξέταση εξωτερικής κάρτας μνήμης (SD) ... 99
7 Επίλογος ... 104
7.1 Σύνοψη ... 104

7.2 Συμπεράσματα 104
8 Βιβλιογραφικές Πηγές 106

1 Εισαγωγή

1.1 Τεχνολογική Εξέλιξη κινητών συσκευών

Σήμερα, οι κινητές συσκευές έχουν μετατραπεί από ένα (1) απλό μέσο επικοινωνίας σε κινητούς Ηλεκτρονικούς Υπολογιστές (Η/Υ) με δυνατότητες εφάμιλλες των υπολογιστών. Η ραγδαία τεχνολογική εξέλιξη έχει οδηγήσει στη δημιουργία νέων έξυπνων κινητών με διαφορετικά λειτουργικά συστήματα. Ως τέτοια χαρακτηρίζονται και τα έξυπνα κινητά λειτουργικού συστήματος Android. Το Android είναι μία πλατφόρμα για κινητές συσκευές και όχι μόνο, ανοιχτού κώδικα, που διαχειρίζεται η Open Handset Alliance (OHA). Η OHA είναι μία κοινοπραξία με επικεφαλείς την Google και άλλες κορυφαίες εταιρίες του κλάδου (48 τηλεπικοινωνιακών εταιριών), για την ανάπτυξη ανοικτών προτύπων της κινητής τηλεφωνίας. Τα έξυπνα κινητά τηλέφωνα Android είναι τα από τα πιο δημοφιλή κινητά και σε σύντομο χρονικό διάστημα έχουν καταφέρει να κατέχουν το μεγαλύτερο μερίδιο της αγοράς των λειτουργικών συστημάτων για κινητά.

Οι έξυπνες κινητές συσκευές ενώ από τη μία μεριά αποτελούν μία πολύ χρήσιμη συσκευή για τον καθένα μας, από την άλλη αποτελούν χρήσιμα εργαλεία για εγκληματικές ενέργειες. Η εμπλοκή των κινητών τηλεφώνων με τα εγκλήματα ποικίλει ανάλογα με τον τρόπο που ο εγκληματίας επιθυμεί να χρησιμοποιήσει προς όφελος και διευκόλυνση του την συσκευή. Συνεπώς, ως τέτοιου είδους εγκληματικών ενεργειών θα μπορούσαμε να αναφέρουμε κάθε είδους οργανωμένων εγκληματικών ενεργειών όπως απάτες, ληστείες, ναρκωτικά, κ.α.. Ακόμα, μία έξυπνη κινητή συσκευή μπορεί να χρησιμοποιηθεί και σε τρομοκρατικές ενέργειες. Χαρακτηριστικό παράδειγμα ήταν η επίθεση στο μετρό της Μαδρίτης όπου οι εκρηκτικοί μηχανισμοί ενεργοποιήθηκαν με την χρήση του ξυπνητηριού κινητών τηλεφώνων.

1.2 Ορισμοί και έννοιες της ψηφιακής εγκληματολογίας

Γενικά, τα ψηφιακά πειστήρια[1] είναι πληροφορίες και δεδομένα ικανά και χρήσιμα για εξέταση, οι οποίες βρίσκονται αποθηκευμένες ή έχουν μεταβιβαστεί σε οποιασδήποτε μορφής αποθηκευτικό μέσο, μέσω υπολογιστικού συστήματος.

Η φύση των ψηφιακών πειστηρίων είναι τέτοια που θέτουν ειδικές προκλήσεις για την παραδοχή τους κυρίως από τα δικαστήρια. Για να αντιμετωπιστούν αυτές οι προκλήσεις ακολουθούνται κατάλληλες και διεθνώς αναγνωρισμένες εγκληματολογικές διαδικασίες. Αυτές οι διαδικασίες περιλαμβάνουν, (χωρίς να υπάρχει περιορισμός), σε τέσσερις (4) βασικές φάσεις :

- Την συλλογή.
- Την εξέταση.
- Την ανάλυση και
- Την σύνταξη της αναφοράς (ή αλλιώς έκθεση πραγματογνωμοσύνης όταν πρόκειται για δικαστήρια).

Ειδικότερα, η φάση της συλλογής περιλαμβάνει την αναζήτηση, αναγνώριση, συγκέντρωση και τεκμηρίωση των ψηφιακών πειστηρίων. Σε αυτή τη φάση μπορεί να περιληφθεί και η αποθήκευση των πληροφοριών αυτών.

Η διαδικασία εξέτασης βοηθά στο να καταστήσει τα πειστήρια ορατά και να εξηγήσει την προέλευση και τη σημασία τους. Αυτή η διαδικασία πρέπει να τεκμηριώσει το περιεχόμενο και την κατάσταση των στοιχείων στο σύνολό τους. Στη φάση αυτή συμπεριλαμβάνεται η διαδικασία αναζήτησης των πληροφοριών που μπορούν να είναι κρυμμένες ή χαμένες ή διαγεγραμμένες. Μόλις όλες οι πληροφορίες είναι ορατές, η διαδικασία διαλογής των δεδομένων αρχίζει. Απομονώνονται οι χρήσιμες πληροφορίες (έχουσες εγκληματολογικό ενδιαφέρον) από τις άχρηστες. Λαμβάνοντας υπόψη τον τεράστιο όγκο πληροφοριών που μπορεί να είναι αποθηκευμένος στα μέσα αποθήκευσης που χρησιμοποιούν οι υπολογιστές, γίνεται αντιληπτό ότι αυτό το σημείο της εξέτασης είναι πολύ κρίσιμο.

[1] http://www.elesme.gr/elesmegr/periodika/t16/t16_5.htm, πρόσβαση την 13/07/2015

Η φάση της ανάλυσης διαφέρει από την εξέταση, δεδομένου ότι εξετάζεται το προϊόν προκειμένου να ανακαλυφθούν συγκεκριμένα αποδεικτικά στοιχεία ή να ανακτηθούν δεδομένα.

Η εγκληματολογική εξέταση ολοκληρώνεται με την σύνταξη της αναφοράς στην οποία περιγράφεται με λεπτομέρεια όλη η διαδικασία της εξέτασης. Εδώ, θα πρέπει η αναφορά να συνοδεύεται και από παραρτήματα όπου θα παρουσιάζονται τα ευρήματα με τέτοιο τρόπο ώστε να γίνονται αντιληπτά και από μη εξειδικευμένα άτομα καθώς και φωτογραφικό υλικό με τα αποτελέσματα.

1.3 Εγκληματολογική Εξέταση κινητών συσκευών vs Ηλεκτρονικών υπολογιστών

Οι Αρχές επιβολής του Νόμου και γενικότερα οι εξεταστές ψηφιακών πειστηρίων αντιμετωπίζουν αρκετά προβλήματα ως προς την εγκληματολογική εξέταση των κινητών συσκευών (smartphone, tablet, κ.α.) σε σχέση με τους Ηλεκτρονικούς Υπολογιστές. Για παράδειγμα θα αναφέραμε τους εξής λόγους:

- Οι κινητές συσκευές απαιτούν εξειδικευμένη διεπαφή (interface), αποθηκευτικά μέσα και υλικοτεχνικό εξοπλισμό.
- Το σύστημα αρχείων των κινητών συσκευών απαιτούν την μνήμη υπολογιστή (volatile memory), η οποία χρειάζεται ενέργεια (power) προκειμένου να διατηρήσει αποθηκευμένες πληροφορίες, εν αντιθέσει με τους αυτόνομους σκληρούς δίσκους.
- Η ποικιλομορφία των λειτουργικών συστημάτων των κινητών συσκευών και ο σύντομος κύκλος ζωής τους, έχει αποτέλεσμα να καθιστά δύσκολη την παρακολούθηση των τεχνολογιών.
- Η δυσκολία να πραγματοποιηθεί φυσική ανάλυση της μνήμης των κινητών συσκευών εν αντιθέσει με τα αποθηκευτικά μέσα (σκληροί δίσκοι) των ηλεκτρονικών υπολογιστών.

1.4 Οι κινητές συσκευές τύπου Android

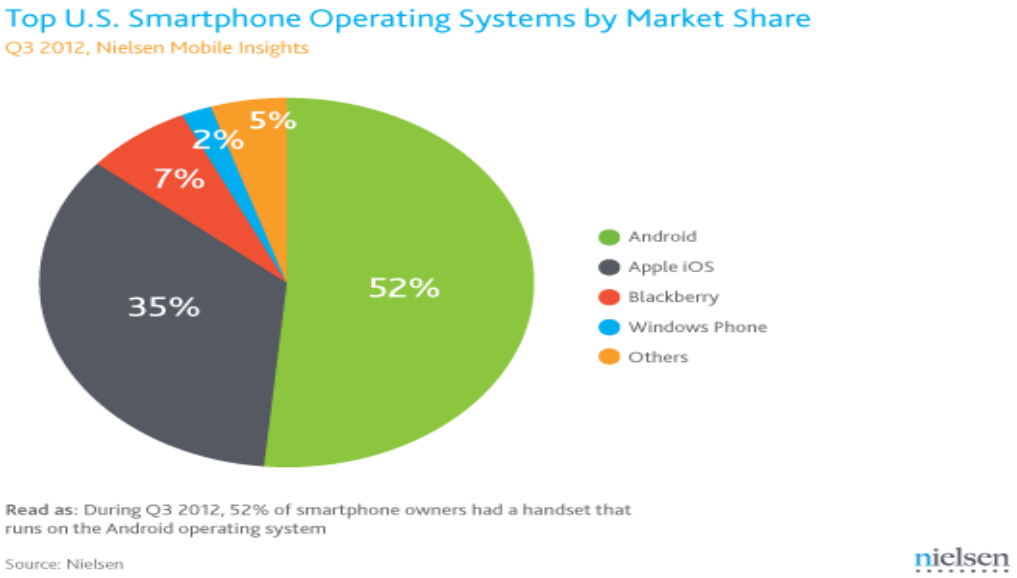
Το Android αποτελεί ένα από τα δημοφιλέστερα λειτουργικά σύστηματα για συσκευές κινητής τηλεφωνίας το οποίο τρέχει τον πυρήνα του λειτουργικού Linux. Αρχικά αναπτύχθηκε από την Google και αργότερα από την [Handset Alliance|Open Handset Alliance]. Επιτρέπει στους κατασκευαστές λογισμικού να συνθέτουν κώδικα με την χρήση της γλώσσας προγραμματισμού Java, ελέγχοντας την συσκευή μέσω βιβλιοθηκών λογισμικού ανεπτυγμένων από την Google. Το Android είναι κατά κύριο λόγο σχεδιασμένο για συσκευές με οθόνη αφής, όπως τα έξυπνα τηλέφωνα και τα τάμπλετ, με διαφορετικό περιβάλλον χρήσης για τηλεοράσεις (Android TV), αυτοκίνητα (Android Auto) και ρολόγια χειρός (Android Wear). Παρόλο που έχει αναπτυχθεί για συσκευές με οθόνη αφής, έχει χρησιμοποιηθεί σε κονσόλες παιχνιδιών, ψηφιακές φυτογραφικές μηχανές, συνηθισμένους Η/Υ (π.χ. το HP Slate 21) και σε άλλες ηλεκτρονικές συσκευές[2].

Η πρώτη παρουσίαση της πλατφόρμας Android έγινε στις 5 Νοεμβρίου 2007, παράλληλα με την ανακοίνωση της ίδρυσης του οργανισμού Open Handset Alliance, μιας κοινοπραξίας 48 τηλεπικοινωνιακών εταιριών, εταιριών λογισμικού καθώς και κατασκευής hardware, οι οποίες είναι αφιερωμένες στην ανάπτυξη και εξέλιξη ανοιχτών προτύπων στις συσκευές κινητής τηλεφωνίας. Η Google δημοσίευσε το μεγαλύτερο μέρος του κώδικα του Android υπό τους όρους της Apache License, μιας ελεύθερης άδειας λογισμικού. Το λογότυπο για το λειτουργικό σύστημα

[2] https://el.wikipedia.org/wiki/Android, πρόσβαση την 12/08/2015

Android είναι ένα ρομπότ σε χρώμα πράσινου μήλου και σχεδιάστηκε από τη γραφίστρια Ιρίνα Μπλόκ[3].

Το Android είναι το πιο ευρέως διαδεδομένο λογισμικό στον κόσμο. Οι συσκευές με Android έχουν περισσότερες πωλήσεις από όλες τις συσκευές Windows, iOS και Mac OS X μαζί όπως φαίνεται και στο γράφημα που παρουσιάζεται παρακάτω (βλ. Εικόνα 1).



Εικόνα 1. Γράφημα Πίτας σχετικά με το δημοφιλέστερο λειτουργικό σύστημα το τελευταίο τετράμηνο του 2012.

1.5 Διάρθρωση της Μελέτης

Η διπλωματική αυτή εργασία αναλύεται σε επτά (7) κεφάλαια. Παρακάτω ακολουθεί σύντομη περιγραφή του κάθε κεφαλαίου.

Στο πρώτο και δεύτερο κεφάλαιο περιγράφεται το λειτουργικό σύστημα Android, το οποίο αποτελεί ένα βασικό υπόβαθρο για τον αναγνώστη, ώστε να κατανοήσει τη δομή του λειτουργικού συστήματος. Εν συνεχεία, ακολουθεί μία αναλυτική περιγραφή της αρχιτεκτονικής του Android με αναφορές στα πέντε βασικά επίπεδα που αποτελείται, των εκδόσεων καθώς και τη δομή των αρχείων του συστήματος.

Στο τρίτο κεφάλαιο γίνεται αναφορά στη δομή των δεδομένων των κινητών συσκευών Android. Τα δεδομένα αυτά αναπτύσσονται ανάλογα με την κατηγορία στην οποία ανήκουν, όπως δεδομένα κάρτας SIM, δεδομένα εσωτερικής μνήμης κινητού και δεδομένα εξωτερικής μνήμης SD. Στο τέλος αυτού του κεφαλαίου παρουσιάζονται και οι βασικές αρχές για την ανάλυση των κινητών τηλεφώνων Android.

Το τέταρτο κεφάλαιο αναφέρουμε τις μεθοδολογίες που έχουν αναπτυχτεί ως σήμερα για τον τρόπο που εξάγονται τα δεδομένα από τα κινητά τηλέφωνα. Έτσι γίνεται μία αναλυτική περιγραφή της βασικής μεθοδολογίας ως προς την ανάλυση της εξωτερικής μνήμης SD, της λογικής ανάλυσης, της τεχνικής ανάλυσης και της ανάλυσης του κυκλώματος του κινητού. Στο παρόν κεφάλαιο παρουσιάζονται επίσης τα βασικότερα εργαλεία εξέτασης ψηφιακών πειστηρίων που κυκλοφορούν σήμερα.

Στο πέμπτο κεφάλαιο αναπτύσσονται με λεπτομέρεια τα στάδια της εγκληματολογικής εξέτασης των κινητών συσκευών και στα επόμενα κεφάλαια παρουσιάζεται ένας πρακτικός οδηγός εγκληματολογικής εξέτασης του κινητού τηλεφώνου Samsung Galaxy S III. Εδώ,

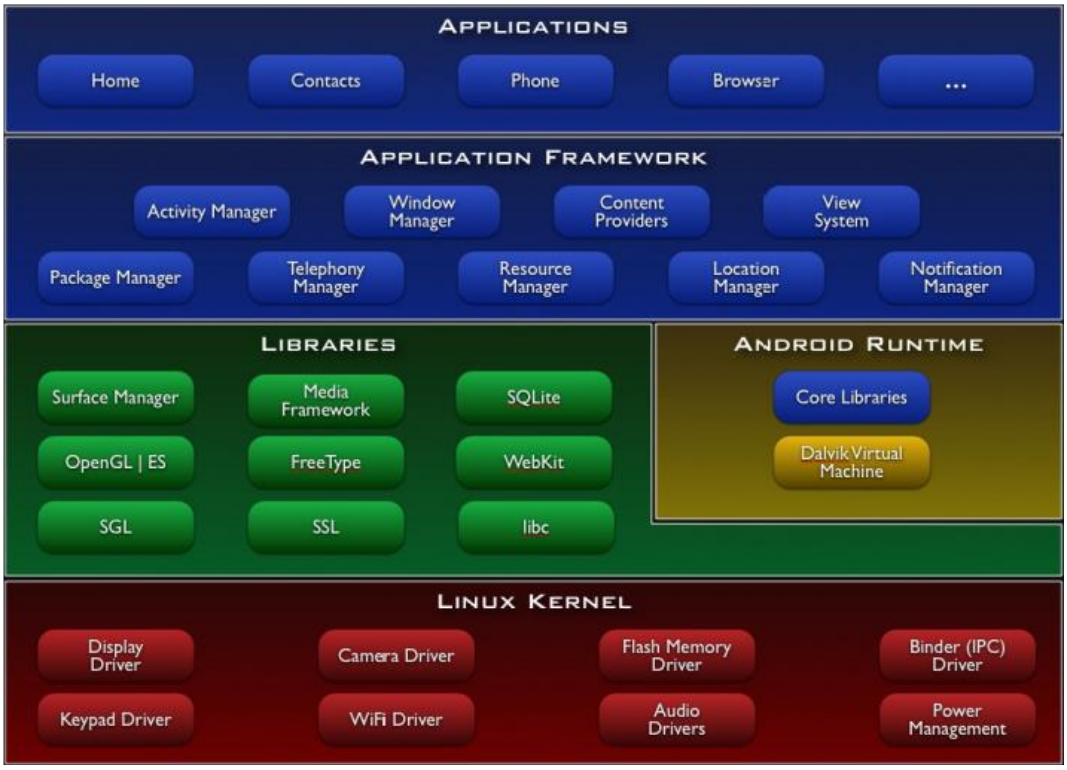
[3] https://el.wikipedia.org/wiki/Android, πρόσβαση την 12/08/2015

πραγματοποιείται η εξέταση με τη χρήση δύο (2) εκ των κορυφαίων εμπορικών λογισμικών, ενός ελεύθερου λογισμικού, καθώς και γίνεται χειροκίνητη εξαγωγή μέσω Adb Shell. Τελειώνοντας, παρουσιάζονται τα αποτελέσματα και τα τυχόν προβλήματα που ανακύπτουν.

2 Λειτουργικό σύστημα Android

2.1 Η αρχιτεκτονική του Android

Το Android είναι ένα λειτουργικό σύστημα. Σαν λειτουργικό σύστημα σκοπός του είναι να παρέχει ένα επίπεδο αφαιρετικότητας ανάμεσα στο υλικό και τον χρήστη. Με λίγα λόγια ο ρόλος ενός λειτουργικού συστήματος είναι να δίνει την δυνατότητα στον χρήστη να χρησιμοποιεί τους πόρους του συστήματος προς όφελος του με μια διεπαφή περισσότερο κατανοητή προς τον άνθρωπο. Για να το καταφέρει αυτό, το Android, αποτελείται από μία στοίβα λογισμικών τμημάτων (software stack) με ξεκάθαρους και καθορισμένους ρόλους. Παρακάτω ακολουθεί μια περιγραφή των επιπέδων της αρχιτεκτονικής του Android[4,5], ξεκινώντας από το χαμηλότερο στο υψηλότερο καθώς και γραφική αναπαράσταση (βλ. Εικόνα 2).



Εικόνα 2. Η αρχιτεκτονική του Android.
(Πηγή: http://elinux.org/Android_Architecture)

2.1.1 Πυρήνας του Linux (Linux kernel)

Το Android βασίζεται στον πυρήνα Linux έκδοση 2.6 για βασικές υπηρεσίες συστήματος όπως ασφάλεια, διαχείριση μνήμης, διαχείριση διεργασιών, στοίβα δικτύου, και οδηγούς συσκευών. Ο πυρήνας λειτουργεί επίσης ως ένα ενδιάμεσο επίπεδο αφαίρεσης μεταξύ της στοίβας λογισμικού και του υλικού.

Ο πυρήνας του Linux είναι γνωστός για την μεγάλη ποικιλία αρχιτεκτονικών επεξεργαστών με τις οποίες είναι συμβατός. Χτίζοντας, λοιπόν, τα υπόλοιπα τμήματα του Android

[4] Hoog, A. (2011). Android Forensics. Investigation, Analysis, and Mobile Security for Google Android. USA: Elsevier, p. 95
[5] Καλλέργης, Γ., (2013). Ανάπτυξη εφαρμογών σε περιβάλλον Android, Διπλωματική εργασία του τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών, p. 16

πάνω από τον πυρήνα του Linux επιτυγχάνουμε την συμβατότητα του με μια ευρεία γκάμα αρχιτεκτονικών και άρα συσκευών που μπορούν να το υποστηρίξουν.

2.1.2 Βασικές Βιβλιοθήκες (Libraries)

Ένα (1) επίπεδο πιο πάνω από τον πυρήνα του Linux βρίσκονται οι βασικές βιβλιοθήκες του συστήματος. Εδώ βρίσκονται ένα (1) σύνολο από βιβλιοθήκες γραμμένες σε C/C++, οι οποίες χρησιμοποιούνται από διάφορα στοιχεία του συστήματος. Όλες αυτές οι βιβλιοθήκες "τρέχουν" στον πυρήνα του Linux και οι δυνατότητες τους είναι προσβάσιμες στους προγραμματιστές μέσω του επιπέδου πλαισίου εφαρμογής.

2.1.3 Το επίπεδο εκτέλεσης (Android Runtime)

Αποτελείται από ένα (1) σύνολο βασικών βιβλιοθηκών (core libraries) της Java και την εικονική μηχανή (Dalvik virtual Machine). Οι εφαρμογές του περιβάλλοντος Android καθώς και πολλές από τις βιβλιοθήκες υψηλού επιπέδου (στο επίπεδο του Application Framework) είναι γραμμένες στην γλώσσα προγραμματισμού Java. Το android όμως δεν χρησιμοποιεί ένα (1) τυπικό διερμηνευτή Java για την εκτέλεση του αλλά έναν ειδικά διαμορφωμένο διερμηνευτή, ο οποίος είναι βελτιστοποιημένος για μικρά ενσωματωμένα συστήματα με περιορισμένους πόρους. Το γεγονός αυτό το διαφοροποιεί από τα ανταγωνιστικά λειτουργικά συστήματα κινητών συσκευών που χρησιμοποιούν γλώσσες όπως C, C++ και Objective C.

2.1.4 Το πλαίσιο εφαρμογής (Application Framework)

Πιο πάνω από το επίπεδο των βιβλιοθηκών και του επιπέδου εκτέλεσης βρίσκεται το πλαίσιο εφαρμογής. Το συγκεκριμένο επίπεδο παρέχει υψηλού επιπέδου δομικές μονάδες (API) τις οποίες μπορούμε να χρησιμοποιούμε για τη συγγραφή των εφαρμογών μας. Όλες οι βιβλιοθήκες του επιπέδου αυτού είναι γραμμένες στην γλώσσα προγραμματισμού Java και αξιοποιούν τις δυνατότητες που προσφέρει το Android Runtime και οι βασικές βιβλιοθήκες του λειτουργικού συστήματος. Ο τρόπος που είναι οργανωμένα τα API στο επίπεδο αυτό ακολουθεί την λογική του διαχειριστή (manager). Για κάθε υπηρεσία που προσφέρει το επίπεδο αυτό υπάρχουν διαχειριστές που οι εφαρμογές μπορούν να καλέσουν για να τους παρασχεθεί η αντίστοιχη υπηρεσία. Οι εφαρμογές πρέπει να χρησιμοποιούν αυτό τον τρόπο για να επικοινωνήσουν με τις βιβλιοθήκες του συστήματος και όχι απευθείας με τις βασικές βιβλιοθήκες. Επομένως, το Android έχει την δυνατότητα να βάζει περιορισμούς σε ποιες λειτουργίες μπορεί κάθε εφαρμογή να εκτελεί. Τα σημαντικότερα δομικά στοιχεία του πλαισίου αυτού είναι:

- View System: Επιτρέπει τη χρήση λιστών, πλαισίων, πεδίων κειμένου, κουμπιών κλπ.
- Content Providers - Πάροχος Περιεχομένου: Επιτρέπει στις εφαρμογές να έχουν πρόσβαση σε δεδομένα άλλων εφαρμογών (όπως οι Επαφές) ή το διαμοιρασμό των δικών τους δεδομένων.
- Resource Manager - Διαχειριστής Πόρων: Παρέχει πρόσβαση σε πόρους, οι οποίοι είναι οτιδήποτε υπάρχει σε ένα πρόγραμμα και δεν είναι κώδικας π.χ. κωδικοί χρωμάτων, σχεδιαγράμματα, γραφικά κλπ.
- Notification Manager - Διαχειριστής Κοινοποιήσεων: Επιτρέπει σε όλες τις εφαρμογές να εμφανίσουν μηνύματα για να ενημερώσουν το χρήστη για τα γεγονότα που συμβαίνουν.
- Location Manager - Διαχειριστής τοποθεσίας: Διαχειρίζεται πληροφορίες σχετικές με την τοποθεσία.
- Activity Manager - Διαχειριστής Δραστηριοτήτων: Διαχειρίζεται τον κύκλο ζωής μιας εφαρμογής και παρέχει τη δυνατότητα μετάβασης σε προηγούμενες καταστάσεις τους.
- Package Manager - Διαχειριστής Εφαρμογών: Υπεύθυνο για τον έλεγχο του χρόνου ζωής των εφαρμογών και για τη διατήρηση μιας στοίβας που επιτρέπει την πλοήγηση του χρήστη σε προηγούμενες οθόνες.

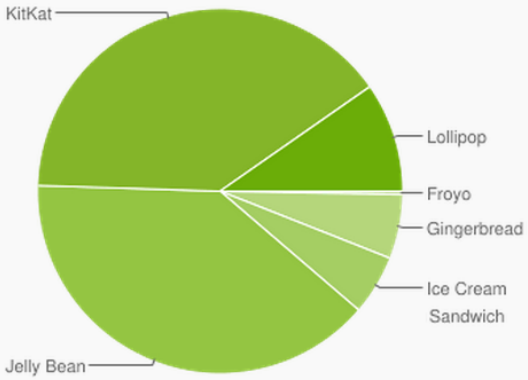
2.1.5 Επίπεδο Εφαρμογών (Applications)

Το Android αποτελείται από ένα σύνολο βασικών εφαρμογών που περιλαμβάνουν συνήθως, μία (1) εφαρμογή ηλεκτρονικού ταχυδρομείου, μία (1) εφαρμογή για μηνύματα (SMS), μία (1) εφαρμογή για ημερολόγιο, καθώς και εφαρμογές για χάρτες (Google Maps), περιηγητή ιστού, πρόγραμμα για δομημένη αποθήκευση των επαφών και άλλα. Όλες οι εφαρμογές του είναι γραμμένες στην γλώσσα προγραμματισμού Java.

2.2 Εκδόσεις Android

Η πρώτη έκδοση του Android SDK παρουσιάστηκε το Νοέμβριο του 2007 με την πρώτη δοκιμαστική (beta) έκδοσή του. Η πρώτη εμπορική έκδοση του Android κυκλοφόρησε έναν χρόνο αργότερα, τον Σεπτέμβριο του 2008. Από τότε, πολλές εκδόσεις έχουν δημιουργηθεί καθώς και έχουν προστεθεί αρκετά χαρακτηριστικά. Στην παρακάτω εικόνα βλέπουμε μια σύντομη ανασκόπηση των εμπορικών εκδόσεων του Android.

Version	Codename	API	Distribution
2.2	Froyo	8	0.3%
2.3.3 - 2.3.7	Gingerbread	10	5.7%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	5.3%
4.1.x	Jelly Bean	16	15.6%
4.2.x		17	18.1%
4.3		18	5.5%
4.4	KitKat	19	39.8%
5.0	Lollipop	21	9.0%
5.1		22	0.7%



Data collected during a 7-day period ending on May 4, 2015.
Any versions with less than 0.1% distribution are not shown.

Εικόνα 3. Οι εκδόσεις του Android μέχρι τις 4 Μαΐου του 2015 (Πηγή:http://www.phonearena.com/news/Android-Lollipop-market-share-closing-in-on-the-10-mark-latest-Google-numbers-show_id68977)

2.3 Το σύστημα Αρχείων (Filesystem)

Τα αρχεία συστήματος[6] περιγράφουν τον τρόπο με τον οποίο τα δεδομένα αποθηκεύονται και οργανώνονται. Υπάρχουν διαφορετικά αρχεία συστήματος για υπολογιστές και για κινητά. Όπως αντιλαμβανόμαστε, το να καταλάβουμε το σύστημα αρχείων του Android είναι πολύ σημαντικό για την εγκληματολογική εξέταση των Android συσκευών, γιατί μας βοηθάει να γνωρίσουμε το πώς τα δεδομένα αποθηκεύονται και πως μπορούμε να τα ανακτήσουμε. Γενικότερα, το Android βασίζεται στα αρχεία του συστήματος Linux και πολλά από αυτά χρησιμοποιούνται για να ξεκινήσουν και να τρέξουν τη συσκευή. Χρησιμοποιεί τύπους αρχείων EXT, FAT32 και YAFFS2 για την εκκίνηση αλλά και την καταχώρηση των δεδομένων. Τα αρχεία συστήματος FAT και

[6] Hoog, A. (2011). Android Forensics. Investigation, Analysis, and Mobile Security *for Google Android.* USA: Elsevier, p. 113

FAT32 είναι γνωστά από το λειτουργικό σύστημα των Windows. Ειδικότερα, θα λέγαμε ότι το σύστημα αρχείων που παρουσιάζεται στις Android συσκευές χωρίζεται σε τρεις κατηγορίες (Flash memory filesystems, Media-based filesystems & Pseudo filesystems), όπου η καθεμία υποστηρίζει διαφορετικούς τύπους αρχείων. Για να δούμε το σύστημα αρχείων που υποστηρίζει μία (1) συσκευή Android εξετάζουμε το φάκελο (../proc/filesytem), όπως φαίνεται παρακάτω:
//……

shell@Android:/ $ cat /proc/filesystems
cat /proc/filesystems
nodev sysfs
nodev rootfs
nodev bdev
nodev proc
nodev cgroup
nodev tmpfs
nodev binfmt_misc
nodev debugfs
nodev sockfs
nodev usbfs
nodev pipefs
nodev anon_inodefs
nodev devpts
ext2
ext3
ext4
nodev ramfs
vfat
msdos
nodev ecryptfs
nodev fuse
fuseblk
nodev fusectl
exfat

……..//

Τα στοιχεία που έχουν το πρόθεμα nodev είναι εικονικά (Pseudo filesystems) και δεν έχουν γραφτεί για φυσική συσκευή (Nand flash or sd cards).

3 Δομή Δεδομένων σε κινητές συσκευές Android

3.1 Εισαγωγή

Όπως έχουμε ήδη αναφέρει η εγκληματολογική εξέταση κινητών συσκευών σε σχέση με την εξέταση των Η/Υ παρουσιάζει αρκετές ιδιαιτερότητες. Ο ερευνητής προκειμένου να προβεί σε μια αποτελεσματική εξέταση των κινητών συσκευών Android, πρέπει πρώτα να κατανοήσει μια σειρά από άλλα θέματα, όπως ποιοι τύποι δεδομένων αποθηκεύονται, που και πως αυτά αποθηκεύονται, κ.α.. Οι παράγοντες αυτοί καταδεικνύουν για το τι δεδομένα μπορεί να

αναζητηθούν, να ανακτηθούν και τελικά να αναλυθούν. Στις επόμενες παραγράφους ακολουθεί περιγραφή των ως άνω παραγόντων.

3.2 Τι αναζητάμε

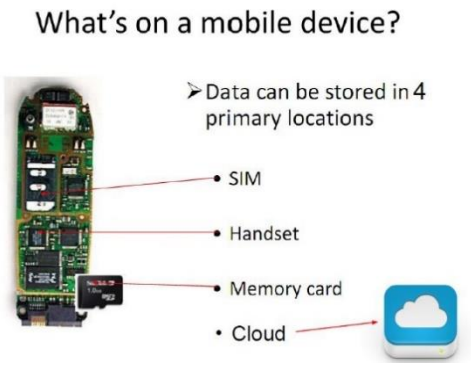
Οι συσκευές Android αποθηκεύουν αρκετά ευαίσθητα δεδομένα μέσω των εφαρμογών που διαθέτουν. Εκτός από τις βασικές εφαρμογές όπως μηνύματα (sms), μηνύματα ηλεκτρονικού ταχυδρομείου (email), ημερολόγιο (calendar), χάρτες (maps), κ.α., υπάρχουν και οι εφαρμογές που ο ίδιος χρήστης κατεβάζει και εγκαθιστά. Γενικότερα, θα αναφέραμε ότι εφαρμογές κατηγοριοποιούνται στις εξής κατηγορίες:

- βασικές εφαρμογές που προέρχονται από το Android,
- εφαρμογές που προέρχονται από την κατασκευάστρια εταιρία και
- εφαρμογές που εγκαθιστά ο χρήστης είτε από το play store είτε από κάπου αλλού.

Τα στοιχεία δεδομένων που αναζητά ο ερευνητής λοιπόν, θα μπορούσανε, μεταξύ άλλων να είναι τα εξής[7]:

- τηλεφωνικός κατάλογος με τις επαφές
- τελευταίες εισερχόμενες / εξερχόμενες / αναπάντητες κλήσεις
- εισερχόμενα και εξερχόμενα γραπτά μηνύματα και MMS
- ηχογραφήσεις / φωνητικές σημειώσεις / ήχοι κλήσης
- φωτογραφίες & video
- ημερολόγιο, ξυπνητήρια / υπενθυμίσεις, κατάλογος εκκρεμοτήτων
- γραπτές σημειώσεις
- ηλεκτρονικό ταχυδρομείο
- επισκεψιμότητα & αναζητήσεις στο διαδίκτυο (search & history web)
- έγγραφα και αρχεία κάθε τύπου
- αναγνωριστικά χρήστη (όπως PIN) και συσκευής (όπως IMEI)
- γεωγραφικά δεδομένα (GPS coordinates)
- αρχεία διαμοιρασμού
- δεδομένα από μέσα κοινωνικής δικτύωσης
- αρχεία αποθηκευμένα στο cloud

3.3 Μέσα αποθήκευσης



Τα δεδομένα που ανήκουν σε διαφορετικές εφαρμογές μπορούν να αποθηκευτούν είτε εσωτερικά είτε εξωτερικά. Στην περίπτωση της εξωτερικής αποθήκευσης (κάρτα SD), τα δεδομένα μπορούν να αποθηκευτούν σε οποιαδήποτε θέση. Ωστόσο, στην περίπτωση της εσωτερικής αποθήκευση, η τοποθεσία είναι προκαθορισμένη. Πιο συγκεκριμένα, εσωτερικά δεδομένα όλων των εφαρμογών που υπάρχουν στη συσκευή (είτε εφαρμογές του συστήματος ή είτε εγκατεστημένες εφαρμογές από το χρήστη) αποθηκεύονται αυτόματα στον υποκατάλογο (../data/data). Για παράδειγμα, η προεπιλεγμένη εφαρμογή του e-mail έχει ένα πακέτο που ονομάζεται com.android.email και τα δεδομένα αυτής αποθηκεύονται στο υποκατάλογο /data/data/com.android.email. Το Android παρέχει στους προγραμματιστές ορισμένες επιλογές για την αποθήκευση των δεδομένων στη συσκευή. Η επιλογή που μπορεί να χρησιμοποιείται εξαρτάται από το χρήστη και από τον τύπο της συσκευής. Γενικά, τα δεδομένα μπορούν να αποθηκεύονται σε μία από τις ακόλουθες θέσεις:

- Κάρτα Sim

[7] Turnbull, E. C. (2011). *Digital Evidence on Mobile Devices*. Academic Press

- Εσωτερικός χώρος (Internal storage / handset)
- Κάρτα μνήμης (Memory card)
- Σύννεφο (Cloud)

Παρακάτω παρέχουμε μια πιο σαφή εξήγηση για κάθε μία από αυτές τις επιλογές.

3.3.1 Κάρτα SIM

Η κάρτα SIM[8] (Subscriber Identity Module), είναι μία έξυπνη κάρτα (smart card), με την οποία πιστοποιείται η ταυτότητα του κατόχου. Κάθε κάρτα SIM προστατεύεται από ένα κωδικό PIN (4-8 αριθμητικά ψηφία). Ο αριθμός PIN ορίζεται από τον κατασκευαστή ή τον πάροχο, αλλά μπορεί να αλλάξει από τον κάτοχο του κινητού. Προκειμένου η κάρτα να προστατευτεί από επιθέσεις τύπου brute force, επιτρέπεται μόνο η χρήση δύο (2) λανθασμένων προσπαθειών, ενώ στην τρίτη λανθασμένη προσπάθεια η κάρτα κλειδώνει. Για να ξεκλειδώσει αυτή απαιτείται η χρήση των αριθμών PUK. Σε περίπτωση δέκα ανεπιτυχών προσπαθειών εισαγωγή αριθμού PUK, η κάρτα καταστρέφεται και τότε ο κάτοχος του πρέπει να ζητήσει από τον πάροχο νέα κάρτα. Τέλος, υπάρχει και ο κωδικός ADM, ο οποίος δίνει την δυνατότητα πλήρους πρόσβασης (προσθήκη, τροποποίηση ή διαγραφή τους, έστω και απομακρυσμένα) στα περιεχόμενα της κάρτας.

Η δομή της κάρτας SIM οργανώνεται σε καταλόγους και αρχεία, όπου μέσα στους καταλόγους βρίσκονται αρχεία-θέσεις μνήμης και αποθηκεύονται διάφορες πληροφορίες. Σε κάθε ένα από αυτά τα αρχεία υπάρχει διαφορετικά δικαιώματα πρόσβασης (ανάγνωση, εγγραφή, τροποποίηση ή διαγραφή κ.α), δηλαδή ορισμένα μπορούν να αναγνωσθούν χωρίς καν να έχει πληκτρολογηθεί το PIN, άλλα απαιτούν την πιστοποίηση του PIN, ενώ στα πιο σημαντικά έχει πρόσβαση μόνον ο πάροχος μέσω του κατάλληλου κωδικού ADM. Στην SIM υπάρχουν περίπου 100 αρχεία σύμφωνα με το πρότυπο και κάποια επιπρόσθετα που διατηρεί ο κάθε πάροχος[9]. Ενδεικτικά κάποια αρχεία βάση του προτύπου περιέχουν:

- τις δυνατότητες του κινητού,
- το σειριακό αριθμό της κάρτας,
- τον κατάλογο παρόχων και ονομάτων τους,
- το κατά προτίμηση δίκτυο,
- τις κατά προτίμηση γλώσσες,
- τον κατάλογο επαφών,
- τα εισερχόμενα και εξερχόμενα μηνύματα,
- τις ρυθμίσεις για την αποστολή μηνυμάτων,
- τον κατάλογο τελευταίων εξερχόμενων κλήσεων.
- την προσωρινή ταυτότητα συνδρομητή δικτύου (IMSI-TMSI), για τη θέση του συνδρομητή (LAI), για τα κανάλια ελέγχου (BCCH), για το τρέχον κλειδί κρυπτογράφησης (Kc).

Πολλά από τα αρχεία αυτά, αποτελούν πολύ καλή πηγή πληροφοριών για τους εξεταστές ψηφιακών πειστηρίων, καθόσον ο κάτοχος τους δεν έχει άμεση πρόσβαση σε αυτά και επομένως δεν γνωρίζει την ύπαρξη τους προκειμένου να τα τροποποιήσει. Γενικότερα, οι κάρτες SIM παραδοσιακά περιείχαν στοιχεία του χρήστη, όπως επαφές, μηνύματα και κλήσεις, καθώς και δεδομένα δικτύου[10] όπως:

- **Αρχείο ICCID** (Integrated Circuit Card Identifier): είναι ο σειριακός αριθμός της κάρτας SIM (βρίσκεται και τυπωμένος στο πλαστικό περίβλημα της κάρτας).
- **Αρχείο IMSI** (International Mobile Subscriber Identify): είναι ένας μοναδικός παγκοσμίως 15ψήφιος αριθμός που χρησιμοποιείται για την αναγνώριση του συνδρομητή από το σύστημα και αποτελεί το μυστικό κλειδί για την πιστοποίηση. Μέσω του αριθμού IMSI

[8] Καρατάσιου, Ε., (2012). Δικανική υπολογιστική: Μέθοδοι, εργαλεία και προοπτικές, Διπλωματική εργασία του τμήματος Πληροφορικής, Πανεπιστήμιο Πειραιώς, p. 88

[9] Fabio Casadei, A. S. (2005). Forensics and SIM cards: an Overview. International Journal of Digital Evidence

[10] Μήττα Μ., (2014). Ψηφιακά Πειστήρια σε έξυπνα τηλέφωνα Android, Διπλωματική εργασία του τμήματος Εφαρμοσμένης Πληροφορικής, Πανεπιστήμιο Μακεδονίας, p. 27

μπορεί να ταυτοποιηθεί ο αριθμός τηλεφώνου, ακόμα και αν η κάρτα έχει λήξει και δεν είναι πλέον δυνατή η χρήση της στο δίκτυο.

- **Αρχείο Location Information και αρχείο Broadcast Control Channel**. Στο αρχείο πληροφοριών περιοχής (Location Information) βρίσκεται η προσωρινή ταυτότητα του κινητού, που πρόκειται για αριθμό παρόμοιο με τον IMSI και χρησιμοποιείται για λόγους ασφάλειας προκειμένου να μην εκπέμπεται στο δίκτυο η μόνιμη ταυτότητα του χρήστη και ο αριθμός περιοχής που αντιστοιχεί στη χώρα, στο δίκτυο και σε μία ευρύτερη περιοχή, η οποία περιλαμβάνει δεκάδες ή ακόμα και εκατοντάδες κυψέλες. Στο αρχείο πληροφοριών καναλιών ελέγχου εκπομπής αποθηκεύεται η ταυτότητα του τρέχοντος καναλιού ελέγχου επικοινωνίας αλλά και των έξι γειτονικών καναλιών. Από το συνδυασμό των στοιχείων LAI Και BCCH μπορεί να εξαχθεί η τελευταία περιοχή στην οποία λειτουργούσε το κινητό. Τα δεδομένα αυτά παραμένουν στην SIM και μετά την απενεργοποίηση της συσκευής και ανανεώνονται καθώς αυτή αλλάζει περιοχές. Συνεπώς εκτός από τη χώρα προέλευσης της κάρτας είναι δυνατή και η εύρεση της τοποθεσίας στην οποία χρησιμοποιήθηκε τελευταία φορά η κάρτα.
- **Αρχείο αποθήκευσης SMS**. Οι σύγχρονες SIM διαθέτουν 35 θέσεις αποθήκευσης μηνυμάτων. Συνεπώς σε περίπτωση που ο κατασκευαστής του κινητού δεν έχει προεπιλέξει τη μνήμη του κινητού ως πρωτεύουσα μνήμη αποθήκευσης, μπορεί να βρεθούν γραπτά μηνύματα. Σαφώς όμως όταν συμπληρωθεί όλος ο διαθέσιμος χώρος αποθηκεύονται και στη μνήμη του κινητού. Όπως προαναφέρθηκε η απλή διαγραφή ενός SMS δεν οδηγεί σε άμεση διαγραφή του αλλά σε σήμανση της συγκεκριμένης περιοχής μνήμης ως ελεύθερης για περαιτέρω αποθήκευση.
- **Αρχείο AND** (Abbreviated Dialing Numbers). Οι σύγχρονες SIM διαθέτουν 250 θέσεις για το αρχείο όπου φυλάσσεται ο κατάλογος επαφών. Στην περίπτωση του καταλόγου επαφών κατά τη διαγραφή μιας επαφής ισχύει το γέμισμα της περιοχής με δυαδικά ‘1’, συνεπώς η ανάκτηση είναι και εδώ ανέφικτη. Το μόνο συμπέρασμα που μπορεί ένας πραγματογνώμονας να εξάγει είναι να επιβεβαιώσει την διαδικασία της διαγραφής, καθόσον οι θέσεις μνήμης στο αρχείο αυτό καταλαμβάνονται με τη σειρά και σε περίπτωση διαγραφής η θέση παραμένει κενή.

3.3.2 Εσωτερικός χώρος Συσκευής

Ορισμένα δεδομένα όπως ο αριθμός IMEI, οι ρυθμίσεις ώρας, ήχων, έντασης, τα μηνύματα SMS, το ημερολόγιο-ξυπνητήρι, οι αναπάντητες και απαντημένες κλήσεις, εκτελέσιμα αρχεία και εφαρμογές ή παιχνίδια και δεδομένα πολυμέσων όπως εικόνες, video, ηχογραφήσεις κ.α., αποθηκεύονται στη μνήμη του κινητού, εάν έχει οριστεί από τον κατασκευαστή του. Επιπρόσθετα, σε περίπτωση που πρόκειται για κινητό που έχει δυνατότητα να συνδεθεί με το διαδίκτυο, αποθηκεύονται στοιχεία όπως ηλεκτρονικές διευθύνσεις που επισκέφθηκε ο χρήστης, αγαπημένες ιστοσελίδες, ονόματα από Wi-Fi access spots κ.λπ.. Στην συσκευή μπορούν επίσης να βρεθούν δεδομένα από παλαιότερες SIM που είχαν συνδεθεί στο κινητό (π.χ. IMSI) ή και να ανακτηθούν διαγραμμένα αρχεία (μερικώς ή ολικώς).

Η εξέταση των δεδομένων μπορεί να γίνει από ένα πραγματογνώμονα με την χρήση ειδικών εργαλείων λογισμικού που αποτυπώνουν την μνήμη του τηλεφώνου σε μορφή κλώνου. Η όλη διαδικασία από τεχνικής άποψης είναι ιδιαίτερα πολύπλοκη, καθώς τα δεδομένα είναι αδόμητα και πρέπει να μεταφρασθούν στο συγκεκριμένο σύστημα αρχείων. Υπάρχουν διάφορα τέτοια διαθέσιμα εργαλεία, τα οποία μπορούν να εξάγουν δεδομένα ακόμη και αν το κινητό είναι σβηστό, κλειδωμένο, χαλασμένο κ.ο.κ.

3.3.3 Κάρτα μνήμης

Οι εξωτερικές κάρτες μνήμης παρέχουν επιπρόσθετο χώρο αποθήκευσης ο οποίος είναι χρήσιμος αν σκεφτούμε τις απαιτήσεις των σύγχρονων κινητών τηλεφώνων (δεδομένα μεγάλου όγκου από videos, φωτογραφίες, μουσική και άλλα είδη αρχείων). Εκτός, όμως από τα αρχεία που μπορεί να αποθηκεύει ο κάθε χρήστης σ’ αυτή (π.χ. μεταφορά από Η/Υ), υπάρχουν και τα δεδομένα από τις εφαρμογές. Οι κάρτες αυτές συνήθως είναι FAT32, εάν και τελευταία

παρατηρούμε ότι χρησιμοποιούνται και άλλα συστήματα αρχείων όπως ext3 & ext4. Αντίθετα, όμως με το εσωτερικό χώρο, ο εξωτερικός χώρος δεν παρέχει κανένα είδος προστασίας, καθόσον τα δεδομένα τους μπορούν να προσπελαστούν πολύ εύκολα.

3.3.4 Σύννεφο (Cloud)

Όπως και στους Ηλεκτρονικούς Υπολογιστές και εδώ ο χρήστης έχει την δυνατότητα να χρησιμοποιήσει το σύννεφο (cloud) ως επιπρόσθετο χώρο για να αποθηκεύσει τα δεδομένα του (δεδομένα μεγάλου όγκου από videos, φωτογραφίες, μουσική και άλλα είδη αρχείων). Στην περίπτωση μας όλες οι κινητές συσκευές Android παρέχουν το γνωστό σε όλους μας, google drive, το οποίο παρέχει εντελώς δωρεάν 15GB χώρο. Ωστόσο υπάρχουν και άλλες εφαρμογές που μπορεί ο χρήστης να κατεβάσει και οι οποίες παρέχουν αντίστοιχες δυνατότητες.

4 Εργαλεία και μέθοδοι εξαγωγής ψηφιακών πειστηρίων σε κινητές συσκευές Android.

4.1 Εισαγωγικά

Τα ψηφιακά πειστήρια σε κινητά τηλέφωνα θεωρείται σχετικά καινούργιος τομέας στην ψηφιακή εγκληματολογία. Το λογισμικό και τα εργαλεία που απαιτούνται για την ανίχνευση στοιχείων είναι ακόμα σε αρχικό στάδιο. Επιπρόσθετα, με την εξέλιξη που παρατηρείται στις κινητές συσκευές, τα εργαλεία είναι σχεδόν αδύνατο να μπορούν άμεσα να εξυπηρετήσουν όλες τις συσκευές. Υπάρχουν αρκετά εργαλεία που κυκλοφορούν στις μέρες μας και υπόσχονται θεαματικά αποτελέσματα, εκ των οποίων αυτά που προσφέρουν φυσική εξαγωγή/ανάλυση δεδομένων έχουν πολύ υψηλό κόστος.

4.2 Εργαλεία εξαγωγής ψηφιακών πειστηρίων σε κινητές συσκευές Android

Εδώ, θα πρέπει να αναφέρουμε ορισμένα από τα πιο γνωστά και διεθνώς αναγνωρισμένα τόσο εμπορικά όσο και ελεύθερα λογισμικά. Συγκεκριμένα, κάποια από τα πιο γνωστά εμπορικά, είναι:

- Cellebrite UFED
- Micro systemation XRY
- OXYGEN Forensic Suite

4.2.1 Cellebrite UFED

Το cellebrite προσφέρει για τους εξεταστές ψηφιακών πειστηρίων σε κινητές συσκευές τον συνδυασμό υλικού και λογισμικού (hardware & software) για την αποτελεσματικότερη εξαγωγή των δεδομένων, την ανάλυση τους καθώς και εργαλεία για τη σύνταξη της αναφοράς των αποτελεσμάτων. Το cellebrite προσφέρεται κυρίως σε δύο εκδόσεις:

- την απλή UFED Touch Logical μαζί με UFED Logical Analyzer
  [σχεδιασμένο για απλή και γρήγορη λογική και σύστημα αρχείων εξαγωγή (logical & file system extraction), ανάλυση και σύνταξη αναφοράς]
- την απλή UFED Touch Ultimate μαζί με UFED Physical Analyzer
  (σχεδιασμένο για πιο εξιδικευμένους χρήστες, αφού προσφέρει εξαγωγή δεδομένων, αποδικοποίηση, ανάλυση και σύνταξη αναφοράς λογική και σύστημα αρχείων εξαγωγή (logical & file system extraction)

Συνοψίζοντας, τα κυριότερα χαρακτηριστικά του είναι ότι:

- υποστηρίζει λογική και φυσική ανάλυση (Logical & Physical Analysis),
- υποστηρίζει την φυσική ανάλυση κινητών κινέζικης κατασκευής (*UFED CHINEX),*
- *υποστηρίζει ανάλυση του σύννεφου (Cloud)*
- *δυνατότητα εξαγωγής κωδικών πρόσβασης*

4.2.2 Micro systemation XRY

Το XRY έρχεται πλήρης ως ένα πακέτο που παρέχει τόσο λογική όσο και φυσική ανάλυση (Logical & Physical Analysis) δεδομένων της συσκευής. Το λογισμικό μπορεί να εξάγει

πληροφορίες τηλεφωνικού καταλόγου, SMS και άλλα μηνύματα κειμένου, MMS, λίστες κλήσεων, των καταχωρίσεων ημερολογίου, εργασιών αντικείμενα, εικόνες, αρχεία πολυμέσων, καθώς και τα στοιχεία της κάρτας SIM. XRY ανακτά επίσης πολλές πληροφορίες για το ίδιο το τηλέφωνο, όπως IMEI / ESN, IMSI, το μοντέλο, κ.α.. Η τελευταία έκδοση περιλαμβάνει υποστήριξη για ορισμένες εφαρμογές smartphone, όπως το Facebook, Myspace, το Skype και το Gmail. Επίσης, παρέχει το λογισμικό XRY viewer, όπου δίνεται η δυνατότητα να διαβάσεις τα .XRY αρχεία και να κάνεις εκ νέου αναζητήσεις ή να εξάγεις αναφορές αποτελεσμάτων.

Ως κυριότερα χαρακτηριστικά του θα λέγαμε ότι:

- *υποστηρίζει λογική και φυσική ανάλυση (Logical & Physical Analysis),*
- *υποστηρίζει την φυσική ανάλυση κινητών κινέζικης κατασκευής (XRY PINPOINT),*
- *υποστηρίζει την ταυτόχρονη ανάλυση τριών (3) συσκευών*
- *υποστηρίζει περίπου 15,330 συσκευές και 675 εφαρμογές κινητών (Smartphone Apps)*
- *XRY viewer*

4.2.3 OXYGEN Forensic Suite

Το εργαλείο Oxygen Forensic είναι ένα από τα κορυφαία εργαλεία στον τομέα των ψηφιακών πειστηρίων με πολύ μεγάλο εύρος υποστηριζόμενων κινητών. Το Oxygen Forensic εξάγει τις περισσότερες πληροφορίες με τον πιο αποτελεσματικό τρόπο. Παρέχει ένα πολύ καλό καθορισμένο σύστημα αναφοράς, ώστε ο ερευνητής να μπορεί να διαβάσει και να επαληθεύσει λεπτομερείς στοιχεία από τα δεδομένα που συλλέχθηκαν.

Τα κυριότερα χαρακτηριστικά του είναι ότι:

- υποστηρίζει **10350+ μοναδικές συσκευές**,
- *υποστηρίζει ανάλυση του σύννεφου (Cloud)*
- διαθέτει δυνατότητα ανάκτησης κωδικών

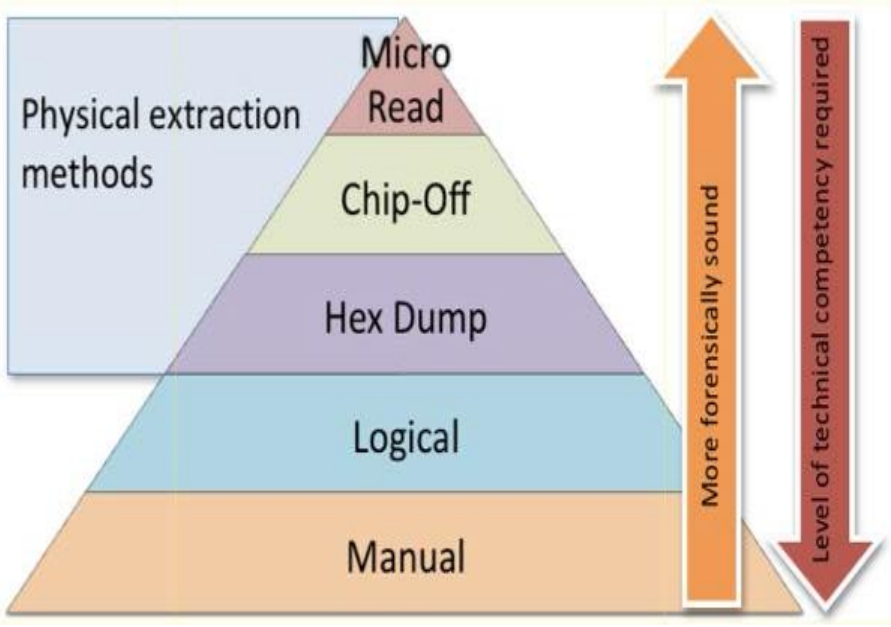
4.2.4 Ελεύθερο Λογισμικό - ViaExtract

Το ViaExtract είναι ένα εργαλείο λογικής και φυσικής ανάλυσης (logical and physical analysis tool) της εταιρείας NowSecure (γνωστή και ως ViaForensics). Η λογική ανάλυση (καθώς και τα αντίγραφα ασφαλείας) είναι διαθέσιμα χωρίς κόστος, σε αντίθεση με την φυσική ανάλυση που απαιτεί κόστος. Προσφέρεται μέσω διανομής Linux και συγκεκριμένα της NowSecure's Santoku διανομής.

4.3 Μέθοδοι Ανάλυσης εσωτερικού χώρου της κινητής συσκευής Android

Στις κινητές συσκευές Android υπάρχουν τέσσερις (4) τρόποι ώστε να ανιχνευθούν και να διασφαλιστούν τα δεδομένα, τρόποι οι οποίοι όσο πιο τεχνικοί γίνονται τόσο πιο ακριβά είναι τα εργαλεία όσο και πιο χρονοβόρα είναι η διαδικασία της εξέτασης. Αυτοί οι τρόποι είναι οι εξής

(Data acquisition types), όπως φαίνονται και στην εικόνα 4. Ακολουθεί, μία (1) συνοπτική ανάλυση των μεθόδων.



Εικόνα 4. Μέθοδοι ανάλυσης κινητών συσκευών Android

- **Χειροκίνητη Ανάλυση (Manual acquisition Analysis)**

Ο εξεταστής χρησιμοποιεί το μενού της συσκευής για να εξερευνήσει το περιεχόμενο του. Ως εκ τούτου η συσκευή χρησιμοποιείται κανονικά από τον εξεταστή, οποίος φωτογραφίζει τα ευρήματα και κρατάει σημειώσεις για να συντάξει την τελική του αναφορά. Αυτή, η μέθοδος μπορεί να χρησιμοποιηθεί σε όλες τις συσκευές, οι οποίες είτε δεν είναι κλειδωμένες είτε δεν είναι κατεστραμμένες.

- **Λογική ανάλυση (logical acquisition analysis)**

Εδώ, ο εξεταστής αποκτά ένα (1) προς ένα (1) (bit-for-bit copy) αντίγραφο του λογικού χώρου (διαμέρισμα συστήματος – filesystem partition) και στη συνέχεια, το αναλύει για τον εντοπισμό των ευρημάτων. Υποστηρίζεται από την πλειονότητα των συσκευών και εξαρτάται όπως και η προηγούμενη μέθοδος από το εάν η συσκευή είναι κλειδωμένη ή κατεστραμμένη.

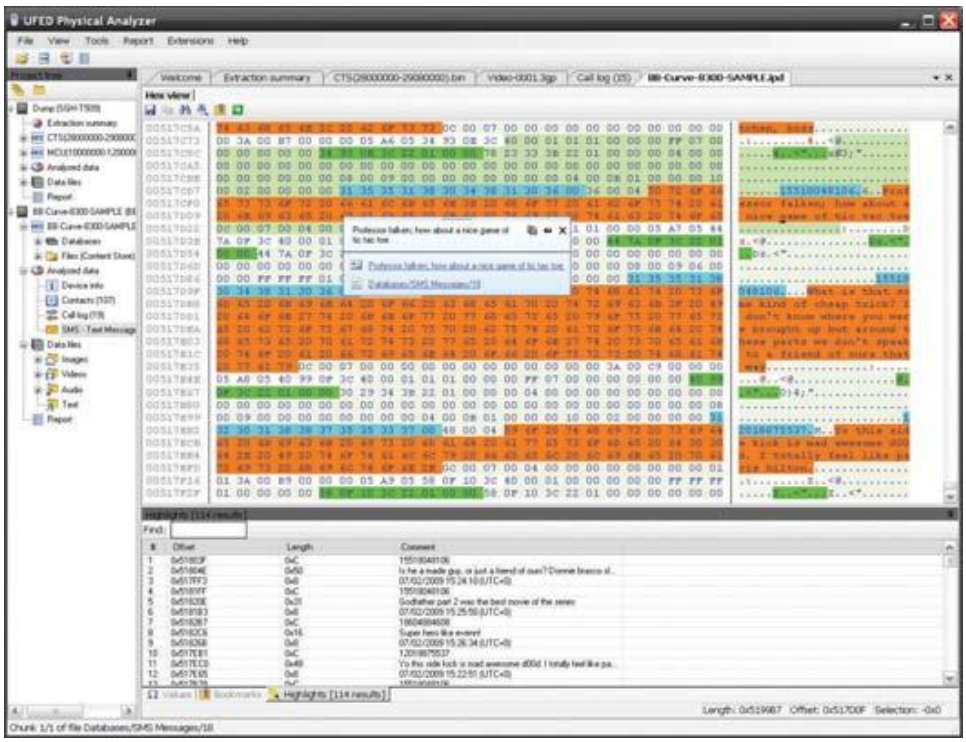
- **Ανάλυση του συστήματος Αρχείων (File system acquisition analysis)**

Εδώ, ο εξεταστής απόκτα πρόσβαση σε όλο το σύστημα των αρχείων (Full File System) περιλαμβάνοντας αρχεία και φακέλους.

- **Φυσική Ανάλυση (Physical acquisition Analysis)**

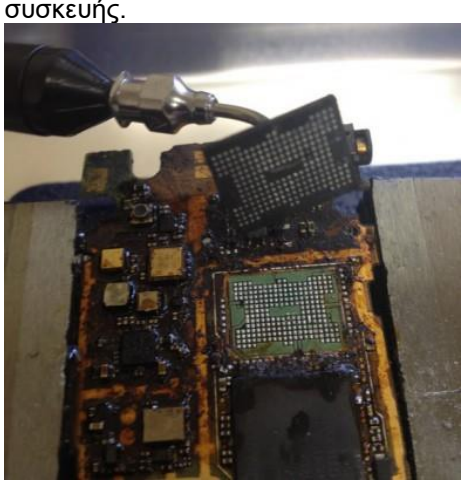
Σ' αυτή τη μέθοδο ο εξεταστής αποκτά ένα (1) ακριβές αντίγραφο (bit-for-bit copy) της μνήμης της συσκευής. Επομένως, αποτελεί και την πιο παρόμοια μέθοδο που ακολουθείται στους Ηλεκτρονικούς Υπολογιστές. Θεωρείται ως η πιο βέλτιστη μέθοδο εξέτασης μιας κινητής συσκευής καθώς ο εξεταστής έχει πρόσβαση και σε διαγεγραμμένα αρχεία. Για λόγους ασφαλείας οι περισσότερες συσκευές δεν επιτρέπουν την αυθαίρετη ανάγνωση της μνήμης και για το λόγο αυτό απαιτούνται εξειδικευμένα εργαλεία (βλ. παρ. 4.2) για την εφαρμογή της. Η μέθοδος αυτή επιτυγχάνεται με έναν από τους εξής τρείς τρόπους, ανάλογα με το είδος της συσκευής και με το τυχόν μέγεθος της καταστροφής.

- Physical Analysis (Hex Dump) – Αλλαγή του προκαθορισμένου αρχείου εκκίνησης (boot loader) με ένα παραμετροποιημένο προκειμένου να είναι δυνατή η προσπέλαση και η απόκτηση της μνήμης (Dump memory).



Εικόνα 5. Απεικόνιση από το εργαλείο UFED Physical Analyzer

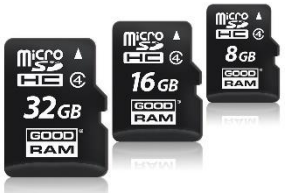
- Physical Analysis (Chip-Off and Jtag techniques) – Εδώ, στην περίπτωση της Chip-off τεχνικής απομακρύνεται η μνήμη από την συσκευή και τοποθετείται σε ειδική συσκευή για την ανάγνωσή της, ενώ στην άλλη περίπτωση εφαρμόζεται ειδικός εξοπλισμός στην μνήμη και εν συνεχεία γίνεται εξαγωγή των δεδομένων. Σημειώνεται, ότι στην πρώτη περίπτωση έχουμε μη αναστρέψιμη καταστροφή της συσκευής.



Εικόνα 6 & 7. Απεικονίσεις τεχνικών ανάλυσης (Chip-Off and Jtag techniques) (Πηγή:http://www.phonearena.com/news/Android-Lollipop-market-share-closing-in-on-the-10-mark-latest-Google-numbers-show_id68977 & http://joojooj.blogspot.gr/2014/09/nokia-lumia-610-unlock-with-atf-jtag-12.html

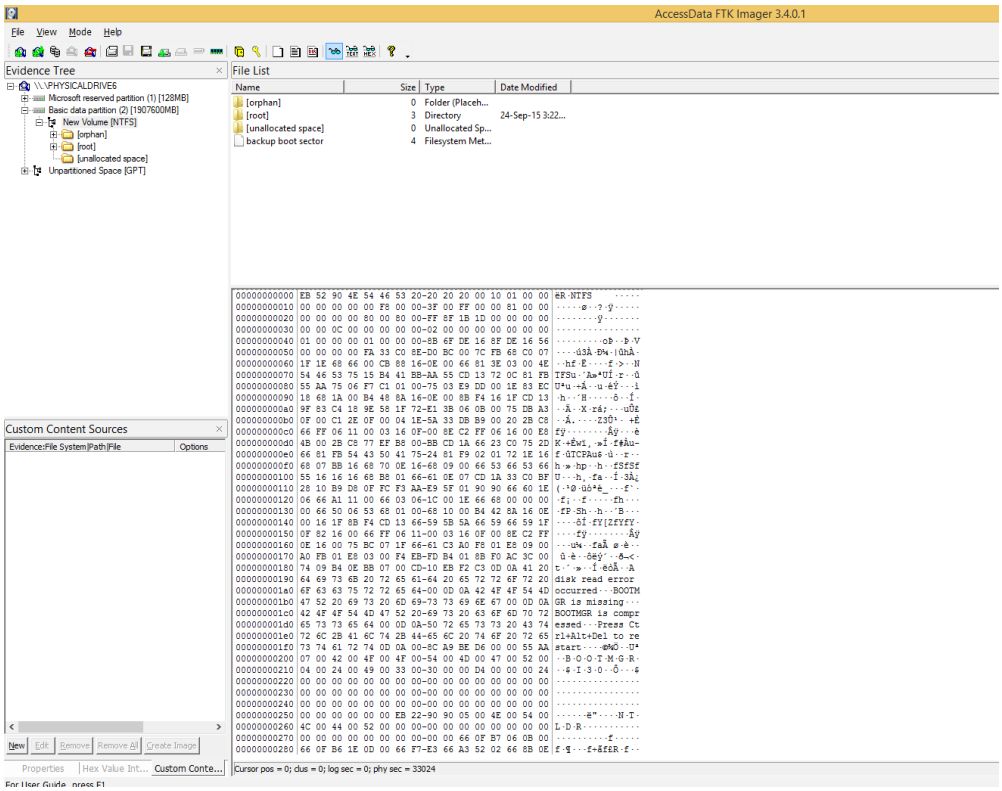
- Physical Analysis (Micro Read) – Τη χρησιμοποίηση ενός ηλεκτρονικού μικροσκοπίου προκειμένου να δούμε το επίπεδο της μνήμης. Αυτή η μέθοδος είναι η πιο δαπανηρή, χρονοβόρα και τεχνικά απαιτητική για να εφαρμοστεί.

Τέλος, αξίζει να σημειωθεί ότι ανάλογα με την περίπτωση, ο εξεταστής μπορεί να συνδυάσει τους μεθόδους προκειμένου να επιτύχει το βέλτιστο αποτέλεσμα.



4.4 Μέθοδος Ανάλυσης κάρτα μνήμης (android micro sd card Acquisition types)

Η κάρτα sd μπορεί να αναλυθεί με τα τυπικά εργαλεία εγκληματολογίας που χρησιμοποιούμε και στους Ηλεκτρονικούς Υπολογιστές. Αφού αφαιρεθεί από την συσκευή είτε τοποθετείται σ' ένα μηχάνημα write blocker (hardware write blocker) είτε τοποθετείται απευθείας σε θύρα του Υπολογιστή (στην περίπτωση αυτή χρησιμοποιούμε software write blocker). Ακολούθως, χρησιμοποιούμε ένα από τα πολλά εργαλεία (εμπορικά ή μη) που υπάρχουν για την ανάλυση τους (όπως Encase, Autopsy, Ftk Imager, Winhex κ.α.).



Εικόνα 8. Απεικόνιση εργαλείου FTK Imager

4.5 Ανάλυση κάρτας SIM (Analysis SIM card)

Η κάρτα SIM θα πρέπει πάντα να αφαιρείται από τη συσκευή και να εξετάζεται ξεχωριστά. Κάποια εργαλεία ισχυρίζονται ότι μπορούν να εξάγουν τα δεδομένα της κάρτας ενώ είναι τοποθετημένη στη συσκευή, το οποίο όμως δεν συνίσταται γιατί ίσως δεν ανακτηθούν όλα τα δεδομένα της κάρτας. Ακολούθως, η SIM μέσω ενός ανεξάρτητου αναγνώστη καρτών (συνήθως συνοδεύεται στις εμπορικές εκδόσεις των εργαλείων) αναλύεται για την εξαγωγή των δεδομένων.

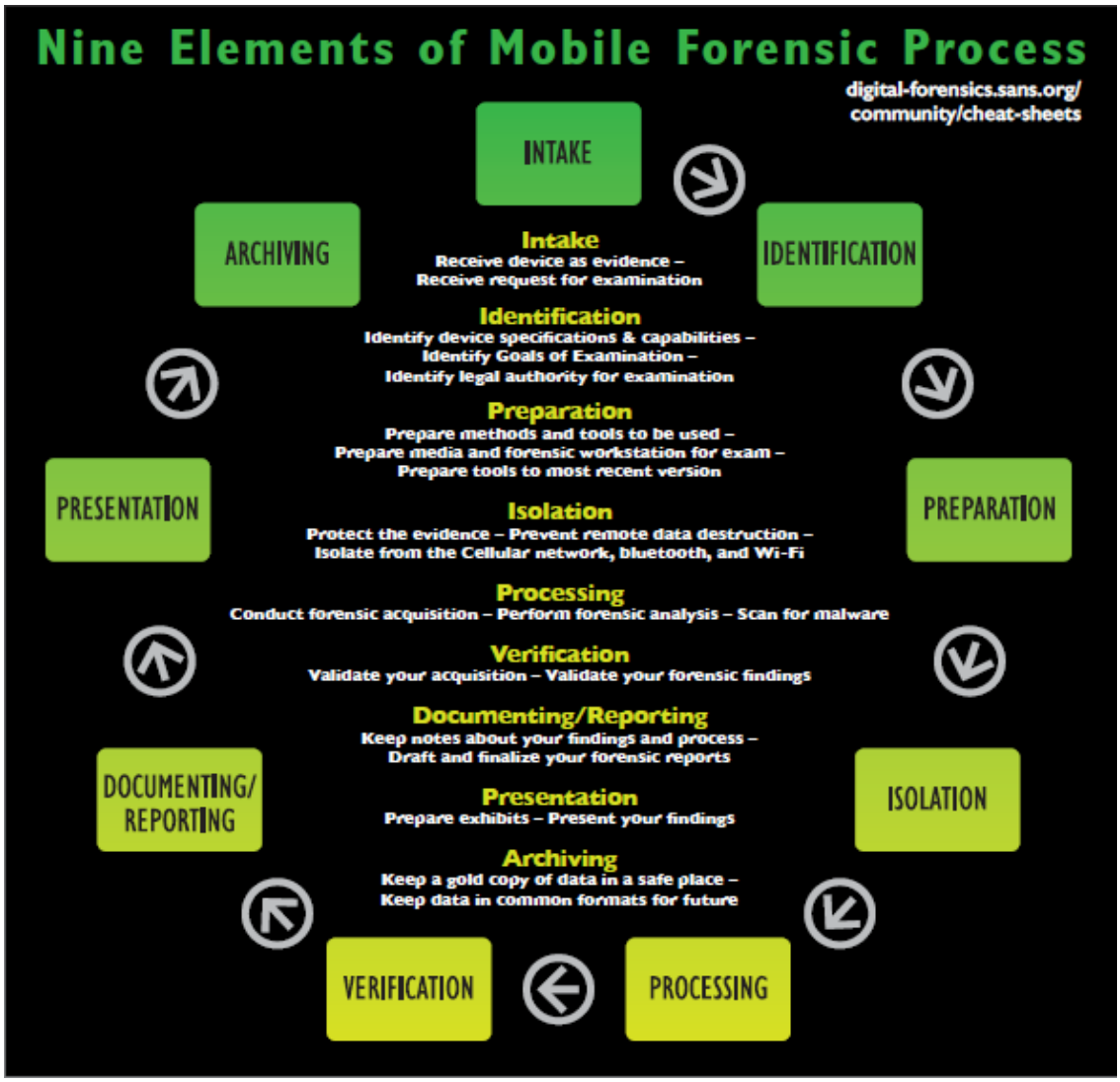
Τονίζεται, ότι η κάρτα SIM μπορεί να προστατεύεται από κωδικό (Pin code), ο οποίος λόγω του γεγονότος ότι οι κάρτες SIM θα πρέπει να είναι σύμφωνες με τους καθιερωμένους

διεθνείς κανόνες, προσφέρει την ίδια λειτουργία: 4 έως 6 ψηφία κωδικό PIN. Μετά την πάροδο τριών λανθασμένων προσπαθειών εισαγωγής του PIN απαιτείται ο κωδικός PUK. Τελειώνοντας, θα αναφέραμε ότι ο εξεταστής εφόσον η SIM είναι κλειδωμένη: είτε ζητάει από τον κάτοχο της το κωδικό είτε σε διαφορετική περίπτωση ζητάει από την εταιρία κινητής τηλεφωνίας των αριθμό PUK, παρέχοντας σ' αυτές το ICCID ή το σειριακό αριθμό της κάρτας SIM.

5 Εγκληματολογική εξέταση κινητών συσκευών Android

5.1 Εισαγωγικά

Όπως ήδη έχουμε προαναφέρει η εγκληματολογική εξέταση των ψηφιακών πειστηρίων με βάση διεθνώς αναγνωρισμένες μεθόδους χωρίζεται σε τέσσερις (4) γενικές φάσεις: α) τη συλλογή, β) την εξέταση, γ) την ανάλυση και την υποβολή της αναφοράς των αποτελεσμάτων. Οι φάσεις αυτές κατά την εξέταση των κινητών συσκευών με βάση το ινστιτούτου της εταιρίας “SANS”, μπορούν να επιμεριστούν σε εννέα (9) (βλ. Εικόνα 9).



Εικόνα 9. Τα εννέα (9) στάδια της εγκληματολογικής εξέτασης των Android συσκευών (Πηγή:https://digital-forensics.sans.org/blog/2014/06/24/getting-the-most-out-of-smartphone-forensic-exams-sans-advanced-smartphone-forensics-poster-release)

5.2 Οι φάσεις της εξέτασης

5.2.1 Φάση 1η: Παραλαβή / Έναρξη της εξέτασης (Intake)

Στη φάση αυτή ξεκινάει η εγκληματολογική διαδικασία με την παραλαβή της πειστήριας(-ων) συσκευής(-ων) και του εγγράφου με τα τιθέντα ερωτήματα (π.χ. αναζήτηση επαφών, εισερχόμενες/εξερχόμενες κλήσεις, αναζήτηση και ανεύρεση τυχών διαγεγραμμένων εικόνων ή βίντεο, κ.α.).

5.2.2 Φάση 2η: Αναγνώριση (Identification)

Εδώ, αναγνωρίζεται το είδος της κινητής συσκευής (π.χ. κινητό, φορητός κινητός Η/Υ τύπου tablet, κ.α.), η εταιρία κατασκευής, το μοντέλο, τα αλφαριθμητικά χαρακτηριστικά αυτής. Τα στοιχεία αυτά καταγράφονται για το κάθε πειστήριο, σημαίνεται και εν συνεχεία φωτογραφίζεται προκειμένου να μοναδικοποιηθεί.

Συνηθίζεται, ανάλογα με το είδος του πειστηρίου να σημαίνεται με βάση τον κανόνα «EX-MEDIA», όπου X=αύξων αριθμός του πειστηρίου και όπου MEDIA=mob, sd, sim, tab, κ.α.. Για παράδειγμα, μία (1) κινητή συσκευή τηλεφώνου, στο οποίο περιέχεται μία (1) κάρτα SIM και μία (1) κάρτα SD, θα σημανθούν ως: E1-MOB, E2-SIM & E3-SD.

Στο σημείο αυτό και πριν ξεκινήσει η κυρίως διαδικασία, θα πρέπει ο εξεταστής (εφόσον ανήκει σε Υπηρεσία επιβολής του Νόμου), να είναι ιδιαίτερα προσεκτικός προκειμένου να εξάγει στοιχεία που δεν αντιβαίνουν στην εκάστοτε Νομοθεσία, (π.χ. στην χώρας μας την νομοθεσία «περί προστασίας των επικοινωνιών και δεδομένων προσωπικού χαρακτήρα»). Αξίζει να σημειωθεί, ότι στην Ελλάδα το περιεχόμενο των επικοινωνιών διασφαλίζεται πλήρως πλην των ρητά περιγραφόμενων στην περί άρση των απορρήτου των επικοινωνιών (Ν.2225/1994, Ν.3115/2003, Ν.3674/2008, Ν.3917/2011 & ΠΔ47/2005).

5.2.3 Φάση 3η: Προετοιμασία (Preparation)

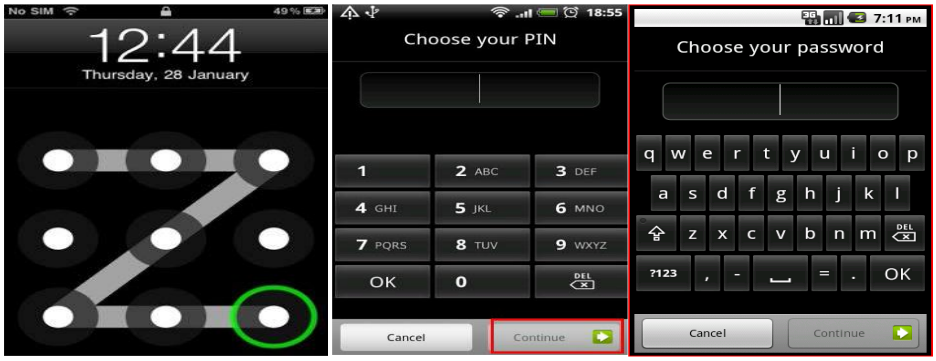
Στη φάση αυτή χρησιμοποιώντας τα στοιχεία της προηγούμενης φάσης, προσδιορίζουμε ποια από τα εργαλεία που διαθέτουμε ως εξεταστές (εμπορικά ή ελεύθερα λογισμικά – commercial or open source mobile forensics tools) υποστηρίζουν την εν λόγω συσκευή(-ες), καθώς και το είδος της ανάλυσης που προσφέρουν. Για παράδειγμα, την λογική, την φυσική ή την σύστημα αρχείων εξαγωγή των δεδομένων (βλ. παρ. 4.2).

5.2.4 Φάση 4η: Απομόνωση (Isolation)

Στη φάση αυτή θα πρέπει ο εξεταστής με κάποιο τρόπο να απομονώσει τη συσκευή από οποιαδήποτε επικοινωνία με το δίκτυο (cellular network, Bluetooth, wifi). Παλαιότερα, στην εγκληματολογική εξέταση των κινητών συσκευών έπρεπε η συσκευή να απενεργοποιείται άμεσα προκειμένου να διατηρηθούν τα δεδομένα της ακέραια. Στις μέρες μας, εφαρμόζεται ο κανόνας που λέει:

- αν το τηλέφωνο είναι κλειστό το αφήνεις κλειστό (if the phone is off, leave it off)
- αν είναι ανοικτό, το αφήνεις ανοικτό (if the phone is on, leave it on).

Πλεονεκτήματα αυτής της μεθόδου είναι, στις περιπτώσεις που το τηλέφωνο είναι ανοικτό και δεν το κλείσεις άμεσα, η προσπέλαση της μνήμης καθώς και η μη ενεργοποίηση των κλειδωμάτων του κινητού (μοτίβο, pin ή αλφαριθμητικό) (βλ. Εικόνες 10 έως 12) έπειτα από το σβήσιμό του.



(α) (β) (γ)

Εικόνες 10, 11 & 12. Κλειδώματα κινητών συσκευών Android
[(α) Κλείδωμα με μοτίβο, (β) Κλείδωμα με κωδικό PIN, (γ) Κλείδωμα με αλφαριθμητικό κωδικό]

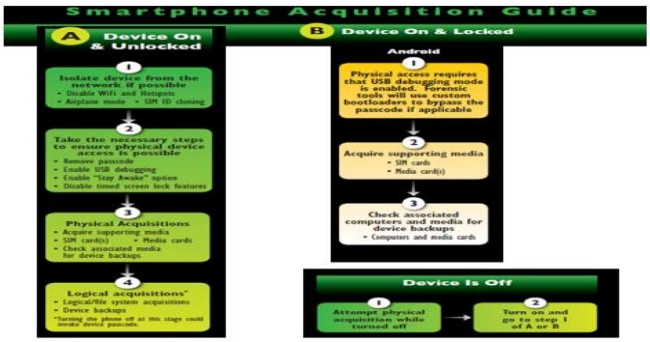
Για το λόγο αυτό και προκειμένου να διασφαλίσουμε από την μία την ακεραιότητα των δεδομένων (overwritten sms, call logs, κ.α.) ή ακόμα απομακρυσμένη διαγραφή των δεδομένων (remote wipe) και από την άλλη να μπορέσουμε να έχουμε πρόσβαση στην συσκευή όσο είναι ανοικτή, χρησιμοποιούνται οι εξής τεχνικές για απομόνωση από το δίκτυο:

- Faraday cage / bag
- SIM Clone
- Signal jamming device
- Airplane mode

Με την πιο αποτελεσματική την λειτουργία πτήσης (Airplane mode), την οποία όλες οι σημερινές κινητές συσκευές διαθέτουν.

5.2.5 Φάση 5η: Επεξεργασία (Processing)

Μόλις το τηλέφωνο έχει απομονωθεί από το όλα τα δίκτυα επικοινωνιών, ξεκινά η κύρια εξέταση του, με την εξαγωγή/ανάλυση της συσκευής, της κάρτας μνήμης και της SIM. Τα κατάλληλα εργαλεία για να επιτευχθεί αυτό περιγράφονται παραπάνω (βλ. παρ. 4.2). Οι κάρτες μνήμης και οι κάρτες SIM πρέπει να υποβάλλονται σε επεξεργασία χωριστά από το τηλέφωνο όταν αυτό είναι δυνατό, χρησιμοποιώντας τις παροδοσιακές τεχνικές της εγκληματολογικής εξέτασης όπως και στους Ηλεκτρονικούς Υπολογιστές. Υπάρχουν περιπτώσεις, που δεν είναι δυνατόν να επεξεργαστούμε την κάρτα μνήμης χωριστά από την κινητή συσκευή, όπως στην περίπτωση που είναι κλειδωμένη από το τηλέφωνο ή κρυπτογραφημένη. Σε αυτές τις περιπτώσεις εξετάζεται μέσω της συσκευής. Η διαδικασία που ακολουθείται για την κύρια εξέταση περιγράφεται παρακάτω σύμφωνα με το πρότυπο του ινστιτούτου της εταιρίας “SANS” (βλ. Εικόνα 13).



Εικόνα 13. Μέθοδοι εγκληματολογικής ανάλυσης Android (ανάλογα με την κατάσταση της συσκευής)
(Πηγή:https://digital-forensics.sans.org/blog/2014/06/24/getting-the-most-out-of-smartphone-forensic-exams-sans-advanced-smartphone-forensics-poster-release)

Από την εικόνα αυτή καταλαβαίνουμε ότι σημαντικό ρόλο για την εξέταση μιας κινητής συσκευής Android παίζουν το εάν η συσκευή είναι ανοικτή, εάν είναι κλειδωμένη, εάν έχει δικαιώματα διαχειριστή (rooted) και εάν έχει ενεργοποιημένη την επιλογή USB debugging. Ανάλογα, με το τι ισχύει κάθε φορά εφαρμόζεται και διαφορετική διαδρομή. Επί των πλείστων, τα εργαλεία που αναφέραμε δίνουν την δυνατότητα προσπέλασης των ανωτέρω, περιγράφοντας αναλυτικά τα βήματα που πρέπει ο εξεταστής να ακολουθήσει. Η προσπέλαση αυτών, χωρίς εξειδικευμένα εργαλεία, θεωρείται αρκετά δύσκολη, επίπονη και χρονοβόρα διαδικασία.

5.2.5.1 Χειροκίνητη Επεξεργασία (χρήση του Adb)

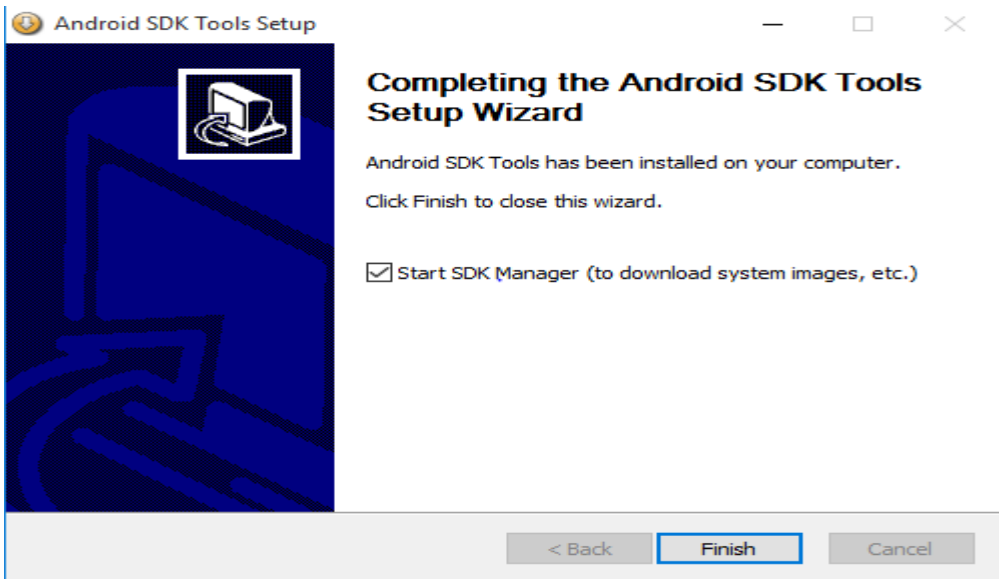
5.2.5.1.1 Εισαγωγικά

Στη περίπτωση που θέλουμε να εξετάσουμε μια (1) Android συσκευή, χωρίς την χρησιμοποίηση είτε εμπορικών είτε ελεύθερων λογισμικών, θα σημειώναμε ότι τα πράγματα είναι αρκετά δύσκολα και εξαρτάται από παράγοντες που έχουμε ήδη προαναφέρει όπως κλείδωμα συσκευής, ενεργοποίηση του USB Debugging, δικαιώματα διαχειριστή.

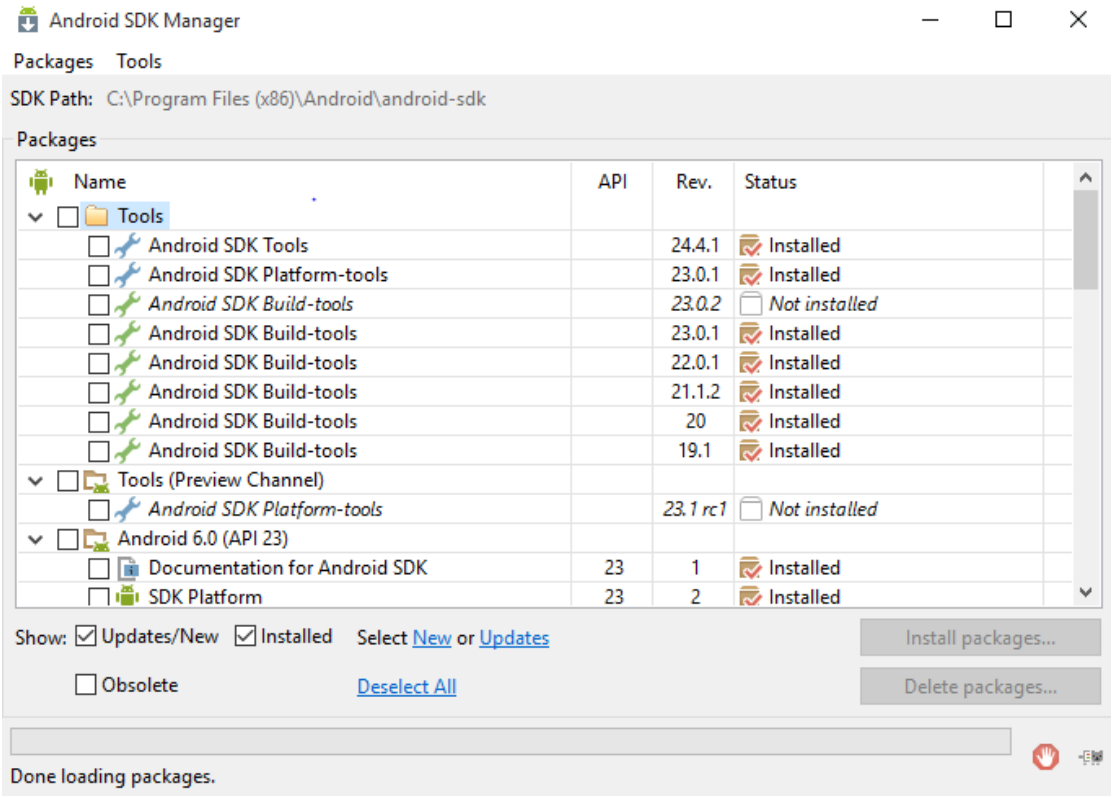
5.2.5.1.2 Android Adb

Για την χειροκίνητη ανάλυση θα χρησιμοποιήσουμε έναν (1) Η/Υ με αρκετές δυνατότητες (επεξεργαστή Intel i5, Windows 7 Professional, 6GB Μνήμη RAM και σκληρό δίσκο ssd). Στον συγκεκριμένο υπολογιστή έχει εγκατασταθεί το Android SDK, στο οποίο παρέχεται και το Android ADB, ένα ισχυρό εργαλείο που δίνει αρκετές δυνατότητες στον εξεταστή ψηφιακών πειστηρίων (βλ. Εικόνες 14 έως 16).

Εικόνα 14. Απεικόνιση από την διαδικασία εγκατάστασης του SDK Android



Εικόνα 15. Απεικόνιση από την διαδικασία εγκατάστασης του SDK Android



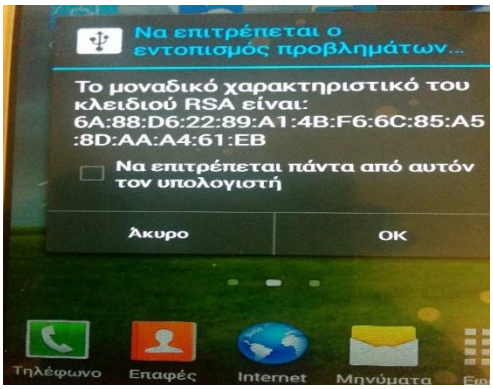
Εικόνα 16. Απεικόνιση του εργαλείου SDK Manager

5.2.5.1.3 Adb και USB Debugging

Αφού προηγουμένως, δείξαμε πως κάποιος μπορεί να εγκαταστήσει το περιβάλλον ADB, τώρα θα δούμε κάποια πράγματα σχετικά με το USB Debugging. Γενικά, το USB debugging είναι η μέθοδος εκείνη που επιτρέπει στο κινητό να συνδεθεί με το Η/Υ. Παλαιότερα, η επιλογή αυτή

δινόταν κάτω από επιλογές του Προγραμματιστή, τώρα όμως από την έκδοση του Android 4.2, η επιλογή αυτή είναι κρυμμένη και θα πρέπει για να ενεργοποιηθεί να επιλέξουμε την επιλογή <σχετικά με το τηλέφωνο>, εκεί να πατήσουμε επτά (7) φορές την επιλογή <αριθμός κατασκευής> και εν συνεχεία να ενεργοποιήσουμε το USB Debugging.

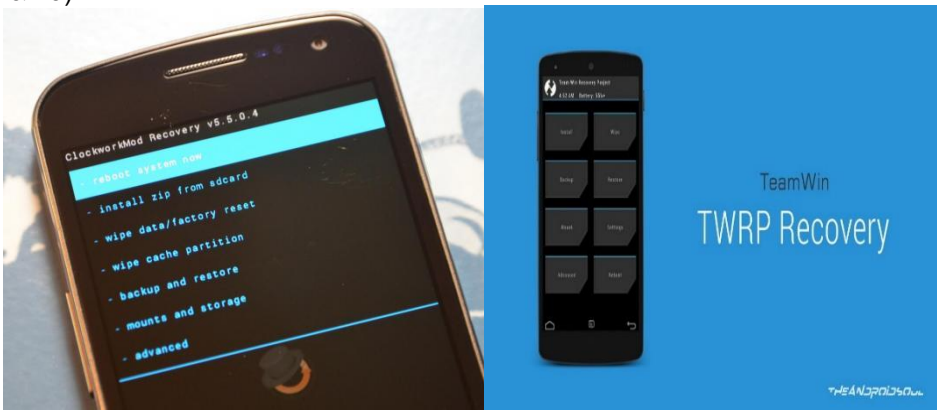
Ακόμα, από την έκδοση του Android 4.2.2 και μετά, απαιτείται επιπλέον να γίνει authorized ο Η/Υ από την συσκευή (βλ. Εικόνα 17). Εάν δεν υπήρχε αυτή η επιλογή θα μπορούσε να γίνει λογική ανάλυση της συσκευής και στην περίπτωση που ήταν κλειδωμένη.



Εικόνα 17. Authorized συσκευής

5.2.5.1.4 Δικαιώματα Διαχειριστή (Root)

Το επόμενο πρόβλημα που υπάρχει αφορά κυρίως την φυσική εξαγωγή, την λογική εξαγωγή (όταν είναι κλειδωμένο) καθώς και κάποιες αναλύσεις όπως την File System, όπου δεν υπάρχουν δικαιώματα διαχειριστή. Εδώ, θα πρέπει ο εξεταστής προκειμένου να προβεί στις αναλύσεις με κάποιο τρόπο να αποκτήσει δικαιώματα διαχειριστή. Δικαιώματα διαχειριστή μπορεί κάποιος να αποκτήσει με διαφορετικούς τρόπους εξαρτάται όμως με το εάν η συσκευή είναι κλειδωμένη ή όχι. Καταρχάς, θα λέγαμε ότι δεν υπάρχει μία (1) συγκεκριμένη μέθοδος για να αποκτήσεις δικαιώματα διαχειριστή σε κάθε συσκευή. Αρκετές, πληροφορίες για τον τρόπο που μπορούμε να το επιτύχουμε μπορούμε να βρούμε στην σελίδα: http://www.xda-developers.com/. Εδώ, αξίζει να σημειώσουμε ότι στην περίπτωση που η συσκευή δεν είναι κλειδωμένη, εφαρμογές όπως το Kingo Root και Towelroot έχουν επιτυχημένα αποτελέσματα σε μεγάλο αριθμό συσκευών. Στις περιπτώσεις κλειδωμένων συσκευών ο εξεταστής πρέπει να χρησιμοποιήσει (εάν δεν υπάρχει), μια διαμορφωμένη έκδοση επαναφοράς (custom recovery image) και όχι την stock, οι οποίες προσφέρουν δικαιώματα διαχειριστή. Ως τέτοιες θεωρούνται οι ClockworkMod and TWRP (βλ. Εικόνες 18 & 19).



Εικόνες 18 & 19. Απεικονίσεις των εργαλείου ClockworkMod and TWRP (πηγή: http://www.xda-developers.com/)

5.2.5.1.5 Φάση 6η: Επαλήθευση (Verification)

Μετά την εξέταση της συσκευής ακολουθεί η διαδικασία της επαλήθευσης[11] της ακεραιότητας των δεδομένων που εξήχθησαν. Η διαδικασία αυτή θεωρείται πολύ σημαντική ειδικά στις περιπτώσεις που τα δεδομένα αυτά χρησιμοποιηθούν στο δικαστήριο, προκειμένου να μην υπάρχουν αμφισβητήσεις. Συγκεκριμένα, με κάποιους τρόπους που θα περιγράψουμε παρακάτω θα πρέπει ο εξεταστής να συγκρίνει ότι τα δεδομένα που εξήχθησαν από την συσκευή είναι τα ίδια-ταιριάζουν με τα δεδομένα που βρίσκονται στην συσκευή. Ως τέτοιους τρόπους θα αναφέραμε τους εξής:

- Έλεγχος της δεκαεξαδικής μορφής (Hex)
  Στις περιπτώσεις της φυσικής ή της συστήματος αρχείων ανάλυσης, τα συνήθης εργαλεία προσφέρουν την δυνατότητα να ελέξεις την ακεραιότητα μέσω της ανάλυσης του Hex. Αυτή η μέθοδος όμως απαιτεί καλή τεχνική κατάρτιση και εμπειρία.
- Χρησιμοποιήσιμη περισσότερων του ενός εργαλείων και σύγκριση των αποτελεσμάτων
- Χρησιμοποίηση των ειδικών αριθμών Hash Values (md5, sha1, κ.α.)
  Εδώ ο εξεταστής αφού εξάγει τα δεδομένα και τους δώσει τον ειδικό αλφαριθμητικό κωδικό, έπειτα τα συγκρίνει με τα πρωτότυπα. Συνήθως υπολογίζεται αυτός ο αριθμός με τον αλγόριθμο MD-5, αλλά πολλές φορές μπορεί να προκύψουν προβλήματα κατά την διαδικασία του δικαστηρίου, διότι ο αλγόριθμος MD5 είναι δυνατόν για δύο διαφορετικά αρχεία με διαφορετικό περιεχόμενο να δώσει ίδιο hash value αυτό είναι το λεγόμενο «MD5 – collision» και γι΄ αυτό συνήθως χρησιμοποιείται το SHA1.

5.2.5.1.6 Φάση 7η: Σύνταξη Αναφοράς (Documenting / Reporting)

Σημειώσεις σχετικά με τα βήματα της εξέτασης και τα ευρήματα θα πρέπει να κρατούνται κατά την διάρκεια της. Αυτές, θα πρέπει να περιλαμβάνουν στοιχεία όπως:

- Ημερομηνία και ώρα που ξεκίνησε η εξέταση.
- Κατάσταση του τηλεφώνου (π.χ. λειτουργικότητα, φθορές)
- Αν το τηλέφωνο ήταν ανοικτό ή κλειστό και με τι συνοδεύεται (κάρτα SIM και κάρτα μνήμης).
- Εταιρία κατασκευής, μοντέλο και λειτουργικό σύστημα.
- Φωτογραφίες από την συσκευή και τα παρελκόμενα της.
- Τα εργαλεία που χρησιμοποιήθηκαν για την εξέταση.
- Τι δεδομένα εξήχθησαν

Τα περισσότερα εργαλεία κινητών τηλεφώνων περιλαμβάνουν λειτουργίες αναφοράς, αλλά τις περισσότερες φορές δεν είναι επαρκείς. Τέλος, ιδιαίτερη προσοχή πρέπει να δίνεται και στον τρόπο που τα δεδομένα αυτά καταγράφονται στην αναφορά, ώστε να μην υπάρχουν ασάφειες. Ειδικά, σε περιπτώσεις που η αναφορά αφορά δικαστικούς σκοπούς είναι επιθυμητό τα ευρήματα που περιγράφονται στην αναφορά να συνοδεύονται και από αντίστοιχες φωτογραφίες.

5.2.5.1.7 Φάση 8η: Παρουσίαση (Presentation)

Στη φάση αυτή θα πρέπει ο εξεταστής να δώσει ιδιαίτερη σημασία, ειδικά εάν στην υπόθεση υπάρχουν περισσότερες από μία συσκευές. Η αναφορά για κάθε εξέταση συσκευής στις περισσότερες φορές, από μόνη της, μπερδεύει τους τελικούς αναγνώστες. Επιθυμητό, λοιπόν, είναι να γίνεται μία παρουσίαση η οποία θα συνοδεύεται από φωτογραφικό υλικό ως προς την διαδικασία, τα ευρήματα, καθώς και τον συσχετισμό των αποτελεσμάτων.

[11] Murphy, Det. Cynthia A. Developing Process for Mobile Device Forensics_v3, Sans Press, p. 7

5.2.5.1.8 Φάση 9η: Αρχειοθέτηση (Archiving)

Τελειώνοντας, θα πρέπει να επισημανθεί ότι η διατήρηση των στοιχείων που εξάγονται και αναφορές που συντάσσονται είναι ένα σημαντικό μέρος της συνολικής διαδικασία. Είναι απαραίτητο να διατηρηθούν τα δεδομένα σε μια χρησιμοποιήσιμη μορφή για την εν εξελίξει δικαστική διαδικασία καθώς και για μελλοντική αναφορά. Για το λόγο αυτό και μην γνωρίζοντας το χρονικό διάστημα για να τελεσιδικήσει μια υπόθεση, θα πρέπει να χρησιμοποιούνται εργαλεία τα οποία θα δίνουν τη δυνατότητα μελλοντικής προσπέλασης ακόμα και στην περίπτωση που το συγκεκριμένο εργαλείο δεν είναι διαθέσιμο.

6 Πρακτικός οδηγός εξέταση κινητής συσκευής Android

6.1 Εισαγωγικά

Σε αυτό το κεφάλαιο θα κάνουμε πρακτική εξέταση μιας (1) κινητής συσκευής/τηλέφωνο, η οποία συνοδεύεται από μία (1) κάρτα SIM καθώς και μία (1) εξωτερική κάρτα μνήμης SD. Για την εξέταση της συσκευής θα χρησιμοποιήσουμε δύο (2) εμπορικά λογισμικά και ένα (1) ελεύθερο λογισμικό, καθώς και τέλος θα κάνουμε χειροκίνητη εξέταση. Για την κάρτα SIM θα χρησιμοποιήσουμε ένα (1) από τα εμπορικά λογισμικά, ενώ για την εξωτερική κάρτα μνήμης SD θα χρησιμοποιήσουμε το λογισμικό FTK Imager, το οποίο προσφέρεται δωρεάν.

Η κινητή συσκευή που έχουμε επιλέξει για εξέταση είναι ένα κινητό τηλέφωνο Samsung Galaxy S III (βλ. Εικόνα 20), με τα κυριότερα χαρακτηριστικά του να περιγράφονται στον Πίνακα 1, ενώ στο Πίνακα 2 δίνουμε ένα (1) παράδειγμα αναφοράς εξέτασης (πρότυπο αναφοράς).

Εικόνα 20. Το κινητό τηλέφωνο Samsung Galaxy SIII(GT-I9300)

Μοντέλο	Samsung Galaxy SIII(GT-I9300)
Λειτουργικό Σύστημα:	Android 4.3
Επεξεργαστής:	Quad-core 1.4 GHz Cortex-A9
Μνήμη:	1GB

Πίνακας 1. Χαρακτηριστικά του Samsung Galaxy SIII

Τίτλος: Καρτέλα Εξέτασης Υπόθεσης (ΚΙΝΗΤΟ/SIM)

Πρωτόκολλο Υπόθεσης: 13/1234.....
Πρωτόκολλο Αιτούντος: -
Εμπλεκόμενοι \ Διεύθυνση: Ιδιώτης
Πειστήρια: Ένα (1) κινητό τηλέφωνο Samsung SIII
Ερωτήματα: Πλήρης Εξέταση
Εξεταστής: Βασιλαράς Αλέξανδρος

Εξέταση Υπόθεσης

Ανάγνωση ΟΛΩΝ των εγγράφων ■	Αναγνώριση ΟΛΩΝ των Πειστηρίων ■	Φωτογράφιση ■	Περιγραφή ■

Αρχικές Ενέργειες

Βούλευμα για την άρση του απορρήτου	Όχι ☐ Ναι ■ (Για όλα τα πειστήρια ☐)
Record date & time of examination	Έλεγχος ■
Φυσική Κατάσταση Συσκευής	Normal ■ Cracked ☐ Damaged ☐ Other ☐
Κατάσταση Λειτουργίας	ON ■ OFF ☐
Αναγνώριση Μοντέλου και Μάρκας	Έλεγχος ■
Χαρακτηριστικά Συσκευής (GSMArena.com)	Έλεγχος ■
Ανάγκη χρήσης Faraday bag (Μεταφορά εξέτασης στο υπόγειο) για αποτροπή σύνδεσης στο Δίκτυο.	Έλεγχος ☐

Εξέταση Συσκευής

ΠΡΟΣΟΧΗ ΕΑΝ Η ΣΥΣΚΕΥΗ ΕΙΝΑΙ ΑΝΟΙΧΤΗ

Φωτογράφιση ■	Έλεγχος ■ Ημερομηνία ■
Ενεργοποίηση Λειτουργίας Flight Mode	Έλεγχος ☐
Προστασία από PIN ή Security Lock;	Όχι ☐ Ναι ■
Ανάκτηση Security Lock;	Όχι ☐ Ναι☐
Έλεγχος IMEI (*#06#)	Όχι ■ Ναι☐ IMEI:
Μεταφορά Χώρο Αποθήκευσης	Έλεγχος ☐
Απενεργοποίηση Συσκευής	Ημερομηνία : 22/12/2015.....

Κοινές Ενέργειες (ΑΝΟΙΧΤΗ/ ΚΛΕΙΣΤΗ Συσκευή)

Εξέταση SIM Χρήση PUK	Όχι ☐ Ναι ■ Όχι ☐ Ναι ■ NEO PIN: 1234.....		
Δημιουργία Κλώνου SIM	Όχι ■ Ναι☐		
Αφαίρεση και Εξέταση Κάρτας Μνήμης	Έλεγχος ■		
Επαλήθευση IMEI	Έλεγχος ☐		
Εγκληματολογικό Λογισμικό	UFED	■	Version:
	XRY	☐	Version:
	Oxygen	■	Version:
	Άλλο	■	Version:
Τύπος Εξαγωγής	Physical ■ Logical ■ Άλλη ■		
Εξέταση Συσκευής με Φωτογραφική Μηχανή	Έλεγχος ☐		
Συγκριτική Εξέταση Timestamp	Έλεγχος ■		

Σημειώσεις: Η συσκευή ήταν κλειδωμένη και απαιτήθηκε χειροκίνητη εξέταση προκειμένου να προσπελαστεί ο κωδικός πρόσβασης (Pattern Lock).

Ο Εξεταστής

Πίνακας 2. Παράδειγμα προτύπου Αναφοράς για την διαδικασία της Εξέτασης

Η εξέταση του κινητού θα χωριστεί σε δύο (2) περιπτώσεις: i) το κινητό να είναι κλειδωμένο (μοτίβο) και ii) το κινητό να είναι ξεκλείδωτο. Ακόμα, θα πρέπει να τονιστεί ότι δεν υπάρχουν δικαιώματα διαχειριστή και ότι η λειτουργία USB Debugging είναι ενεργοποιημένη (θα

δείξουμε και περιπτώσεις που δεν είναι ενεργοποιημένη). Όπως ήδη έχουμε αναφέρει το βασικό πρόβλημα είναι εάν το κινητό είναι κλειδωμένο και αν στο κινητό υπάρχουν δικαιώματα διαχειριστή (root access). Πριν όμως ξεκινήσουμε και περιγράψουμε τα εργαλεία για την εξέταση του, θα πρέπει αρχικά να το σημάνουμε και έπειτα να το φωτογραφίσουμε.

6.2 Εξέταση Συσκευής - Πρώτη Περίπτωση [το κινητό να είναι κλειδωμένο (μοτίβο), USB debugging ON & no root access]

6.2.1 Το εμπορικό εργαλείο Celebrite

Στην περίπτωση αυτή το κινητό που καλούμαστε να εξετάσουμε είναι ανοικτό αλλά κλειδωμένο με μοτίβο και ο επομένως ο εξεταστής δεν έχει άμεση πρόσβαση.

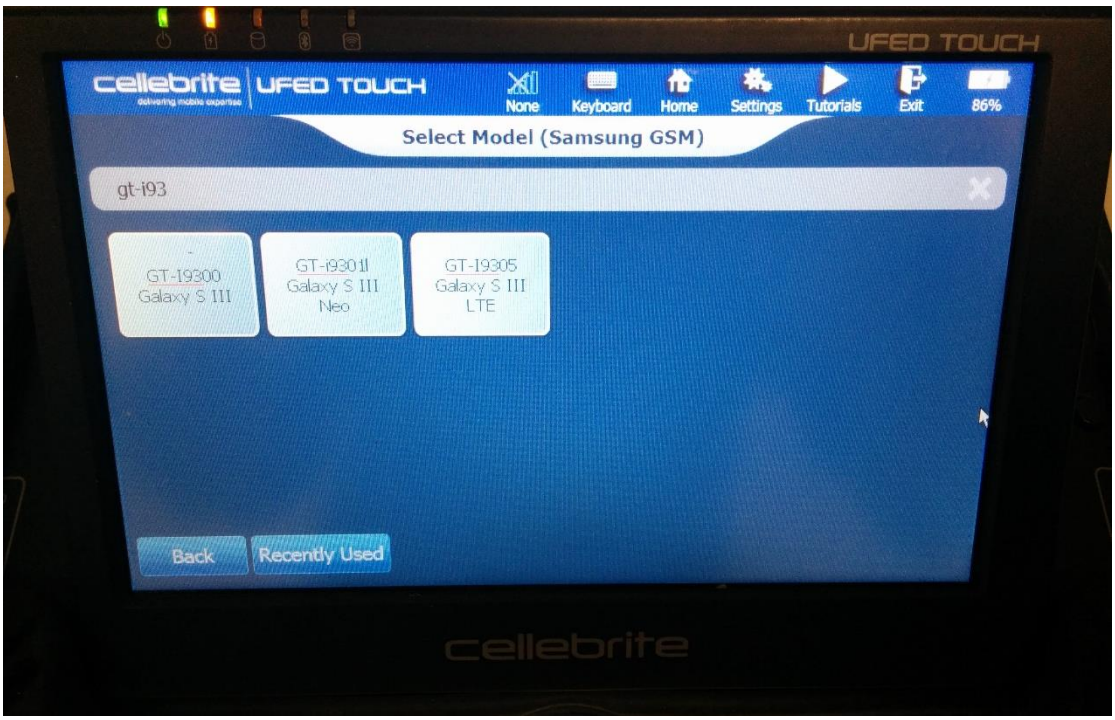
Εικόνες 21. Μέθοδοι εγκληματολογικής ανάλυσης Android (ανάλογα με την κατάσταση της συσκευής)

6.2.1 Το εργαλείο Cellebrite

Εδώ θα χρησιμοποιήσουμε το εμπορικό εργαλείο Cellebrite και θα δείξουμε όλα τα στάδια που απαιτούνται για την εξέταση του (Physical & Logical extraction).

6.2.1.1 Φυσική Εξαγωγή (Physical extraction)

Αρχικά, ψάχνουμε το μοντέλο του κινητού προκειμένου να δούμε εάν το συγκεκριμένο εργαλείο το υποστηρίζει (βλ. Εικόνες 22 & 23).

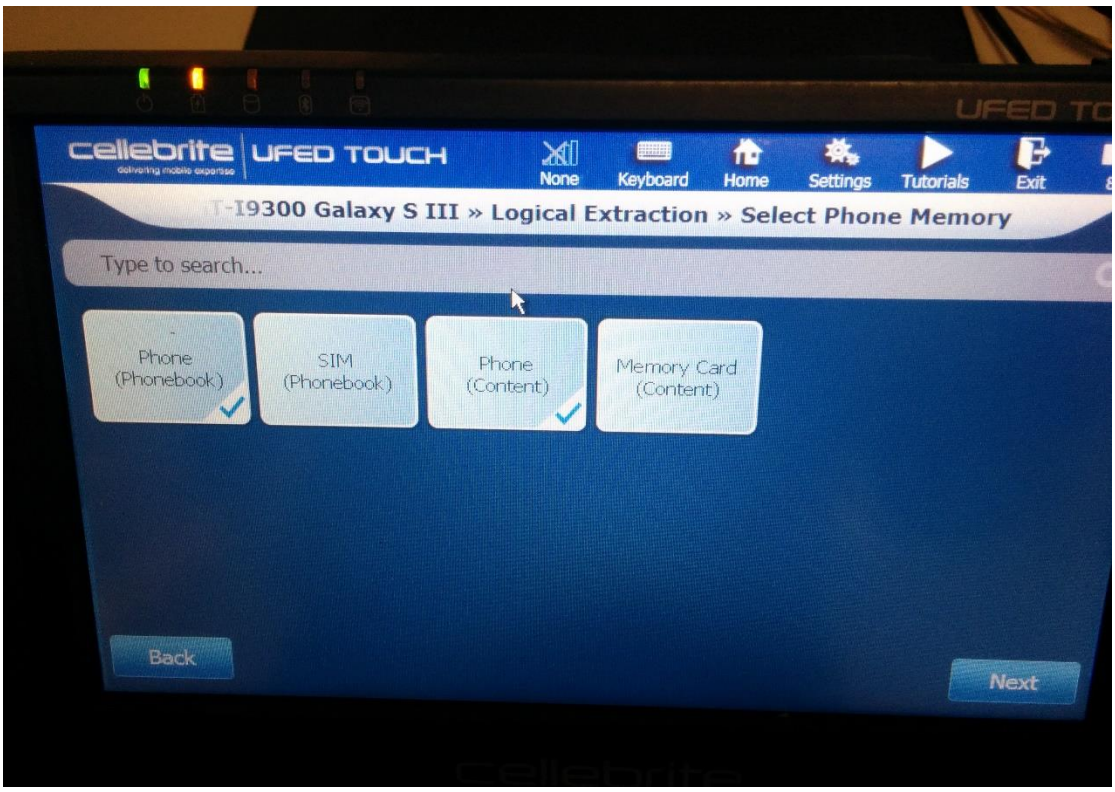


Εικόνα 22. Απεικόνιση του εργαλείου Cellebrite

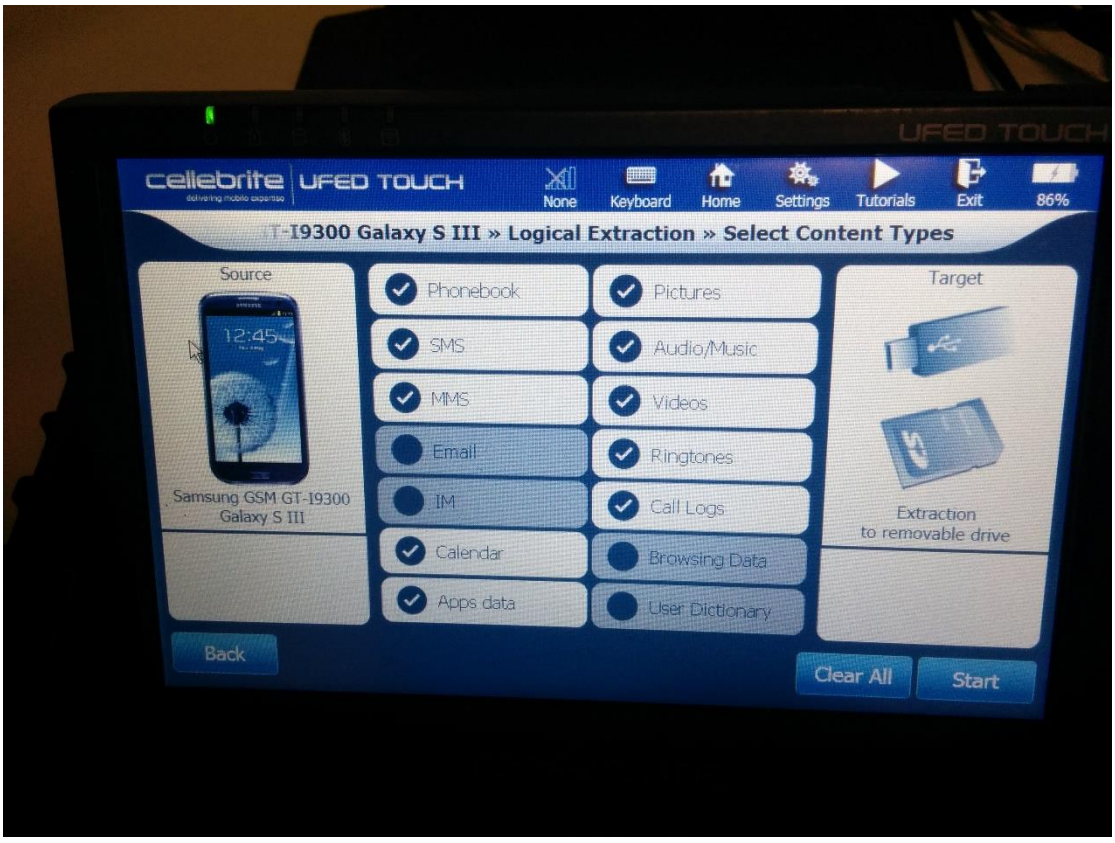
Εν συνεχεία, βλέπουμε ποιες από τις εξαγωγές/αναλύσεις υποστηρίζει (π.χ. φυσική, λογική ανάλυση κ.α.).

Εικόνα 23. Απεικόνιση του εργαλείου Cellebrite (τύποι εξαγωγής)

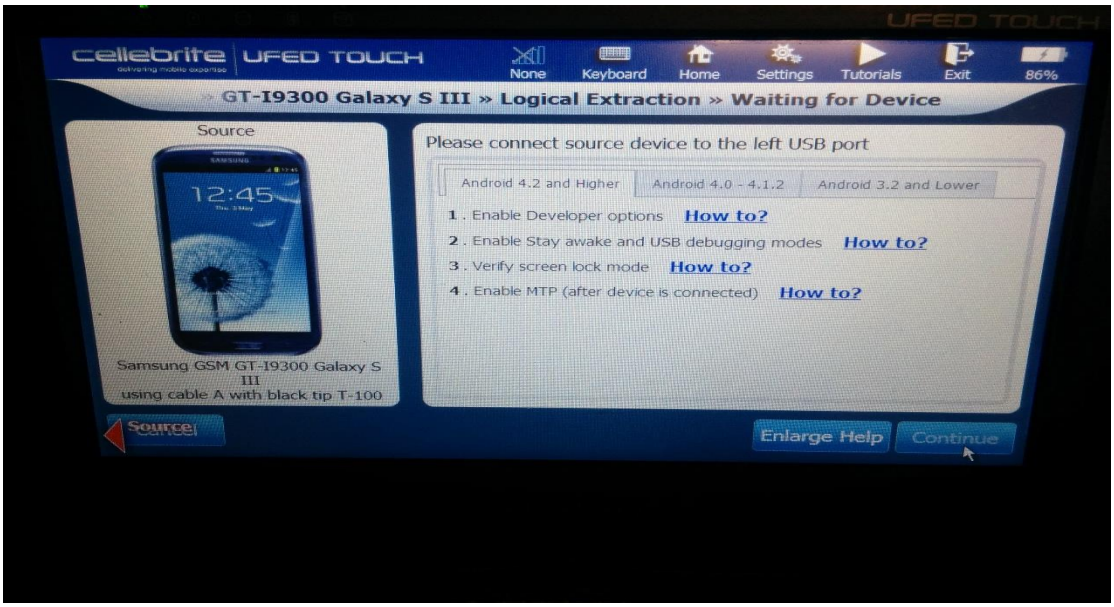
Αρχικά, δοκιμάζουμε την λογική ανάλυση αλλά διαπιστώνουμε ότι δεν είναι εφικτή στην περίπτωση που η συσκευή είναι κλειδωμένη (βλ. εικόνες 24 έως 28).



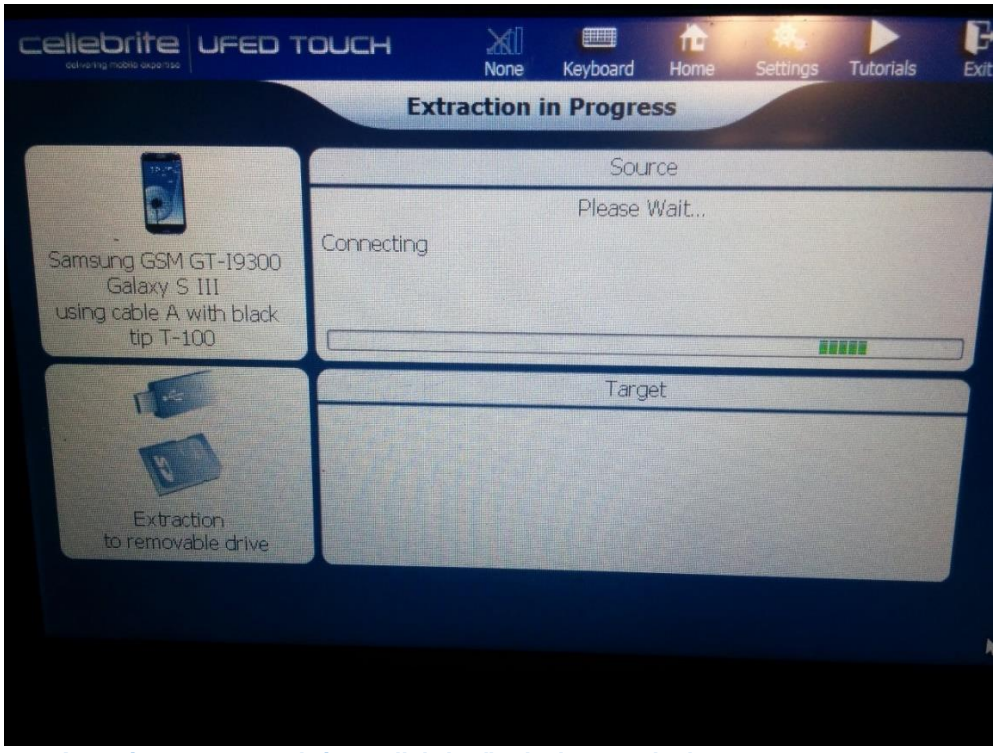
Εικόνα 24. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)



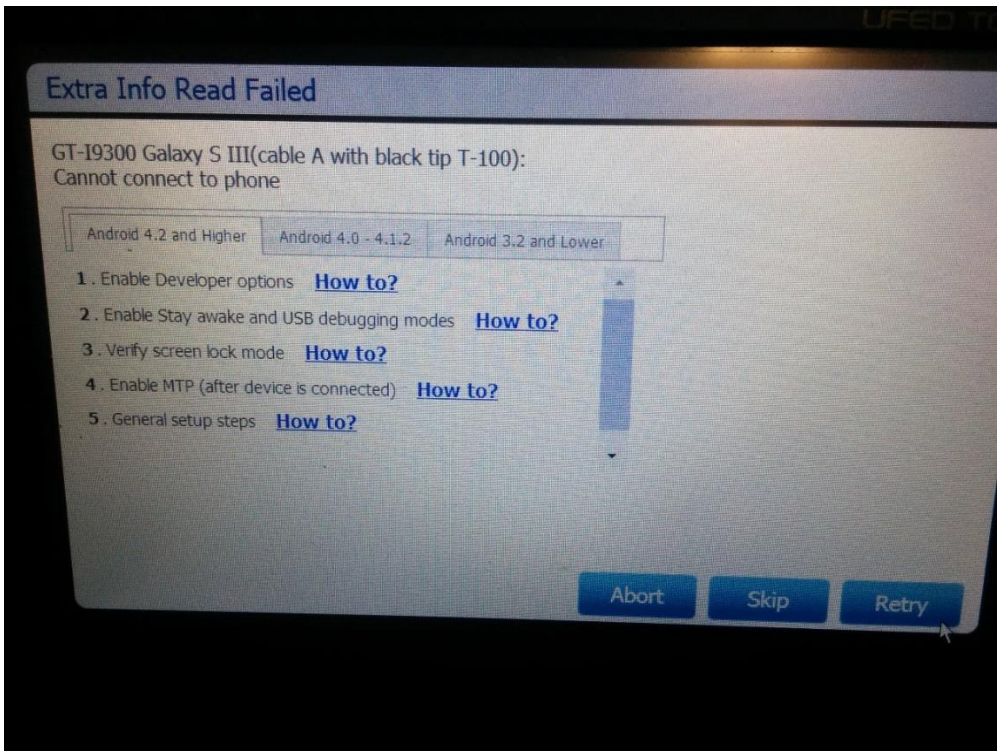
Εικόνα 25. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)



Εικόνα 26. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)



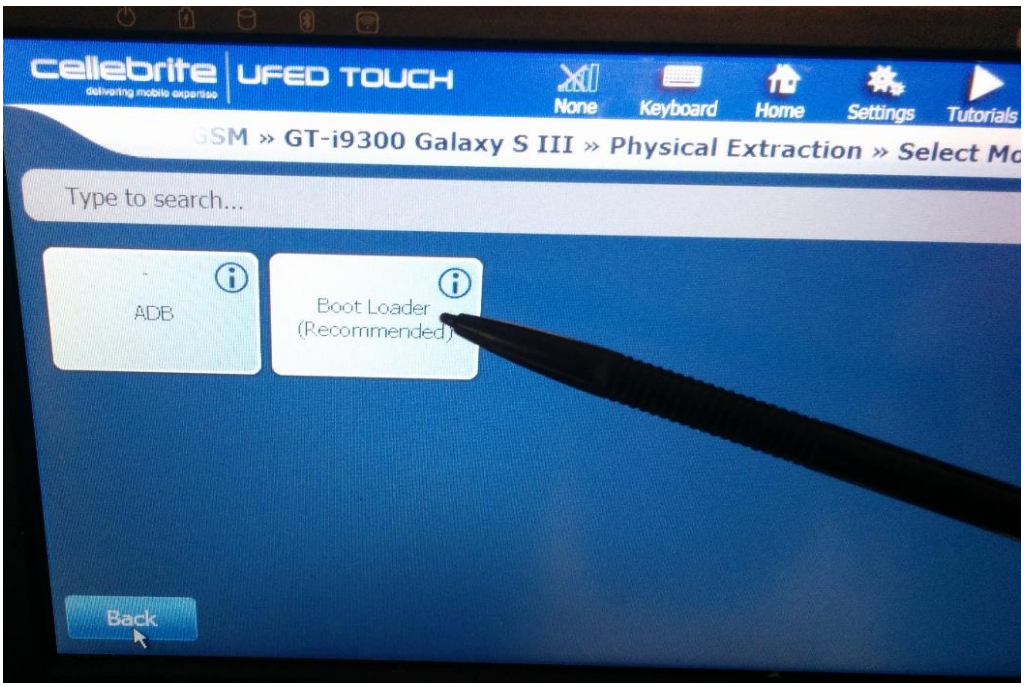
Εικόνα 27. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)



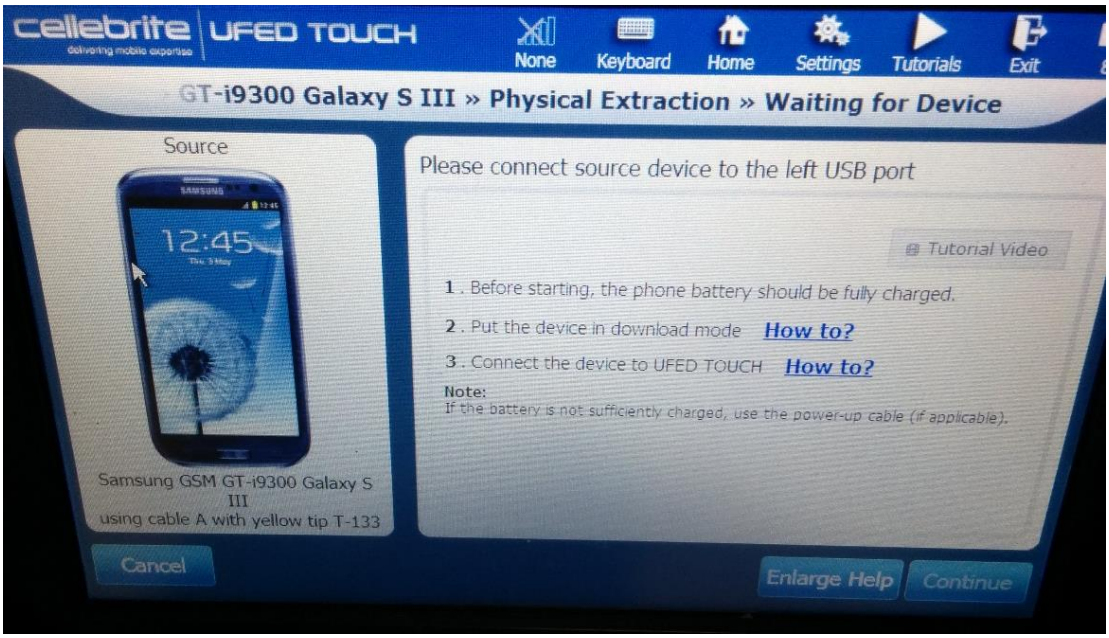
Εικόνα 28. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)

Εδώ, διαπιστώνουμε ότι στην περίπτωσή μας (δηλ. το κινητό είναι κλειδωμένο με μοτίβο), δεν είναι δυνατή η λογική ανάλυση του από το συγκεκριμένο εργαλείο. Συνεχίζουμε την εξέταση δοκιμάζοντας την φυσική ανάλυση της συσκευής. Κατά την φυσική ανάλυση του κινητού, το εργαλείο Cellebrite, προκειμένου να προσπεράσει το κλείδωμα χρησιμοποιηθεί δικό του Bootloader (βλ. Εικόνες 29 έως 36).

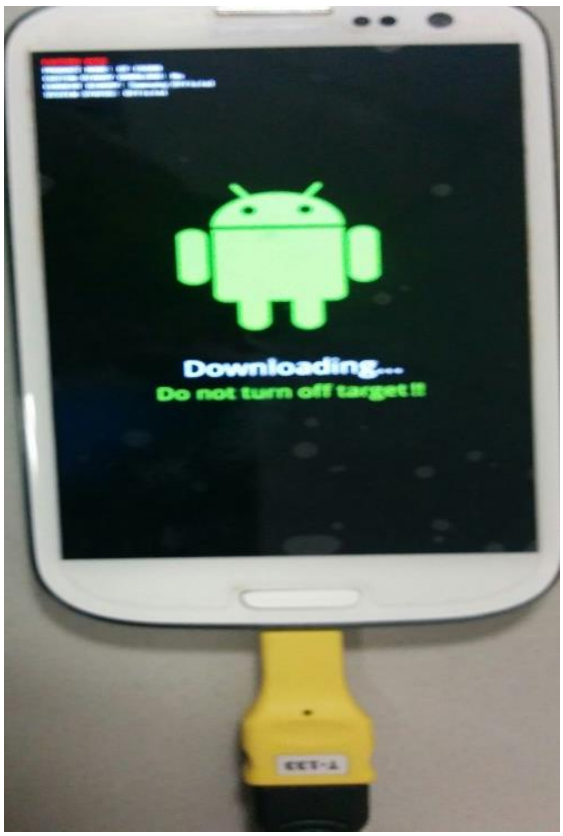
Εικόνα 29. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)



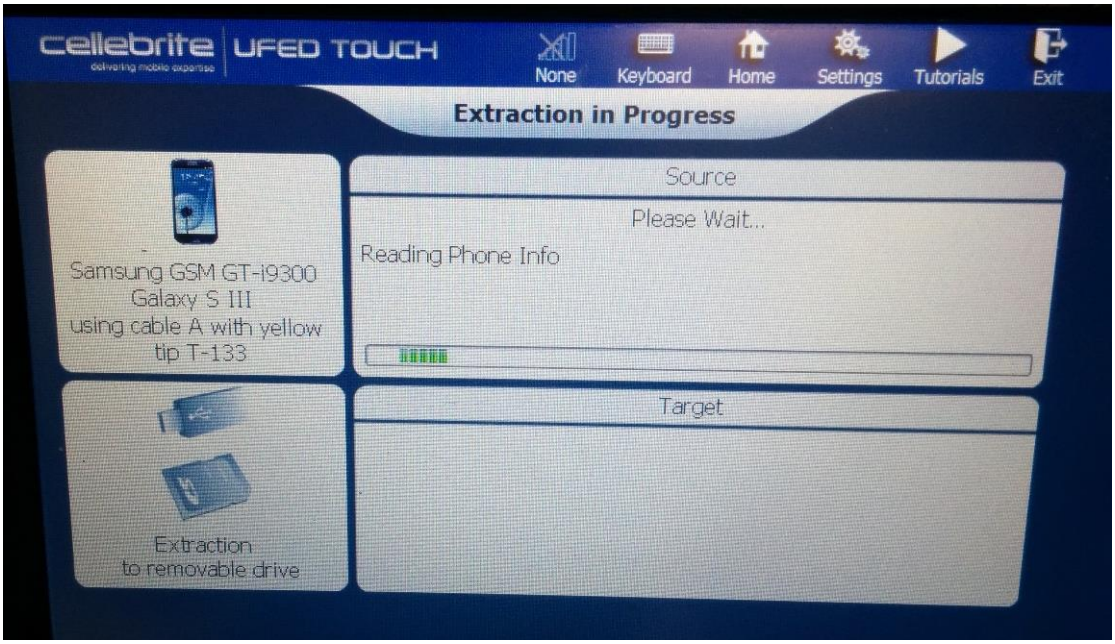
Εικόνα 30. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)



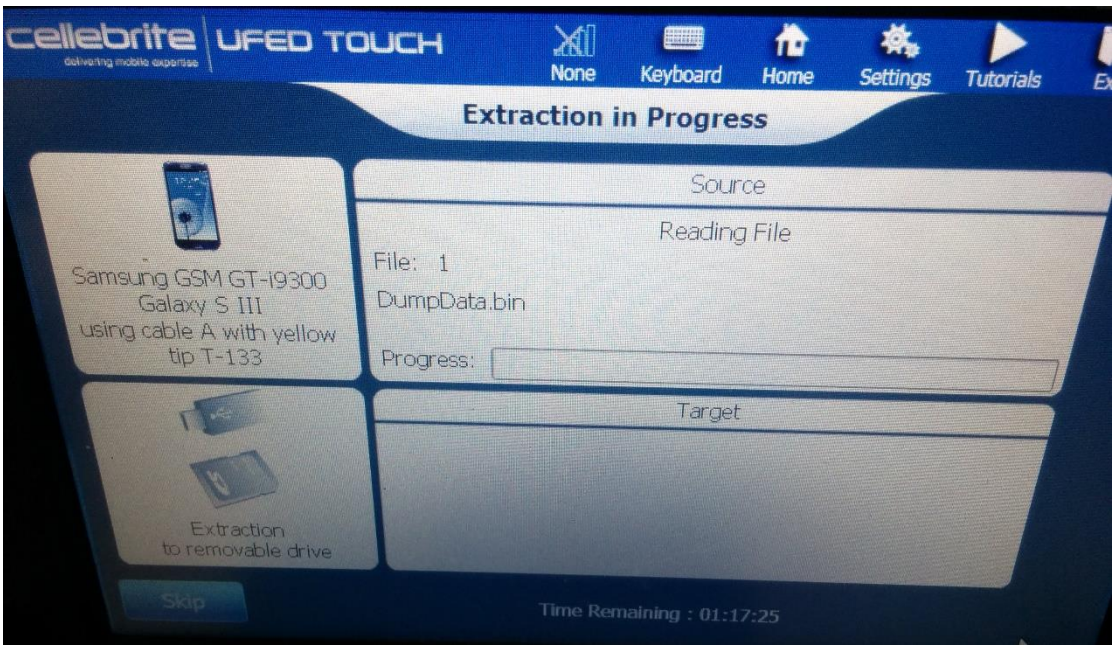
Εικόνα 31. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)



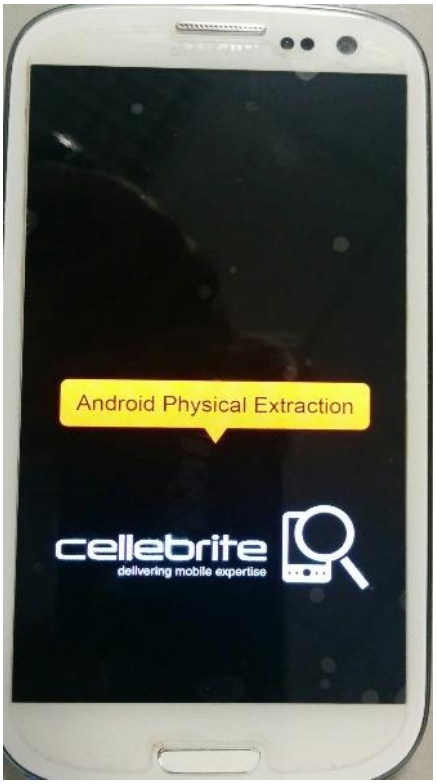
Εικόνα 32. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)



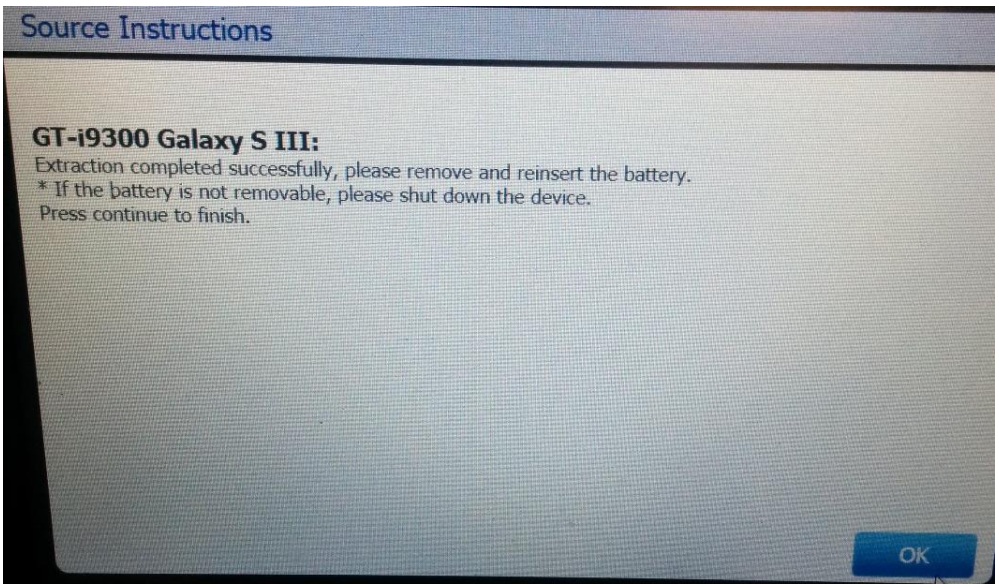
Εικόνα 33. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)



Εικόνα 34. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)

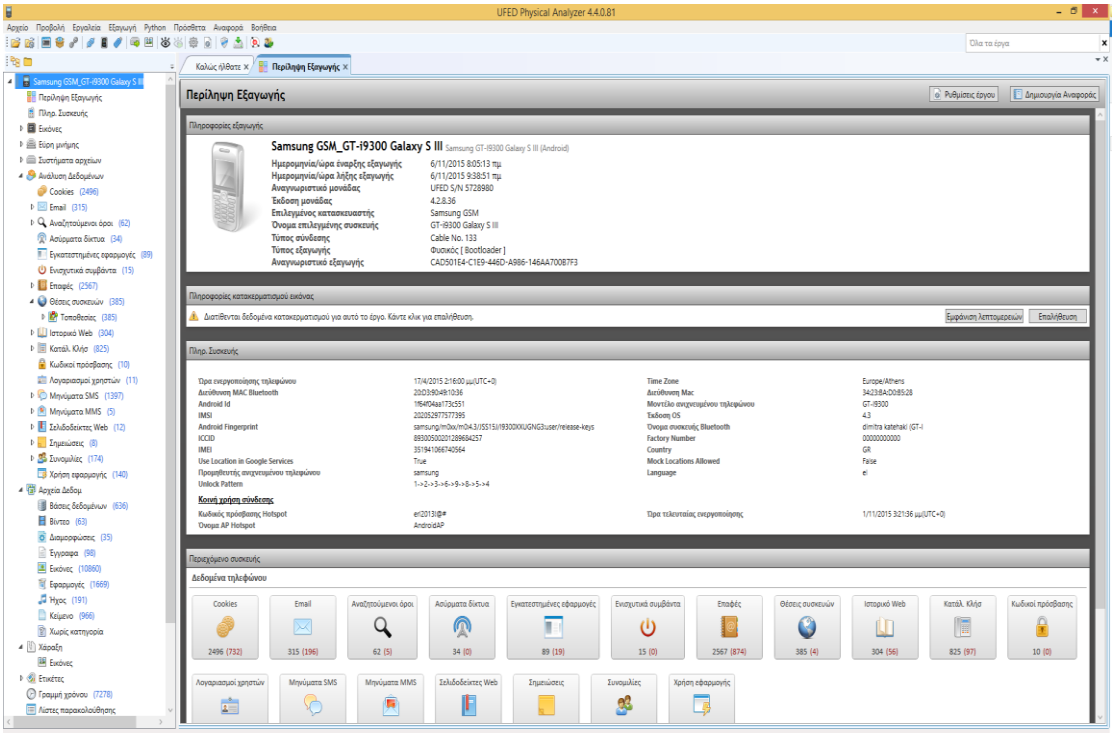


Εικόνα 35. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)

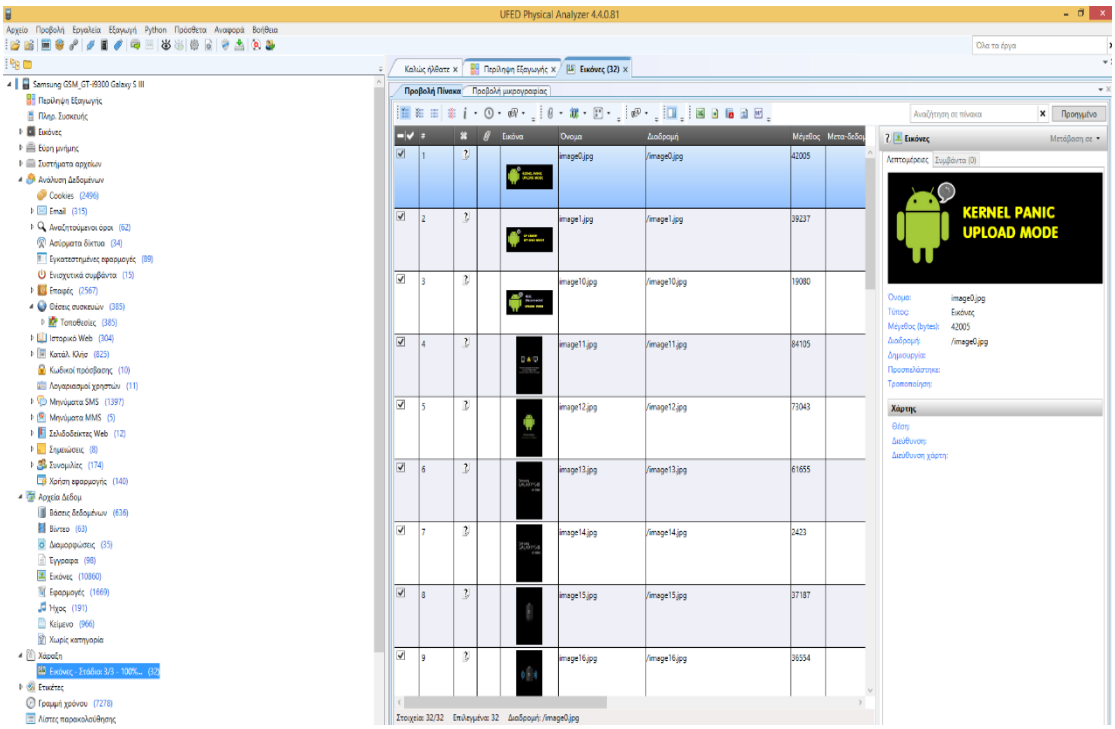


Εικόνα 36. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)

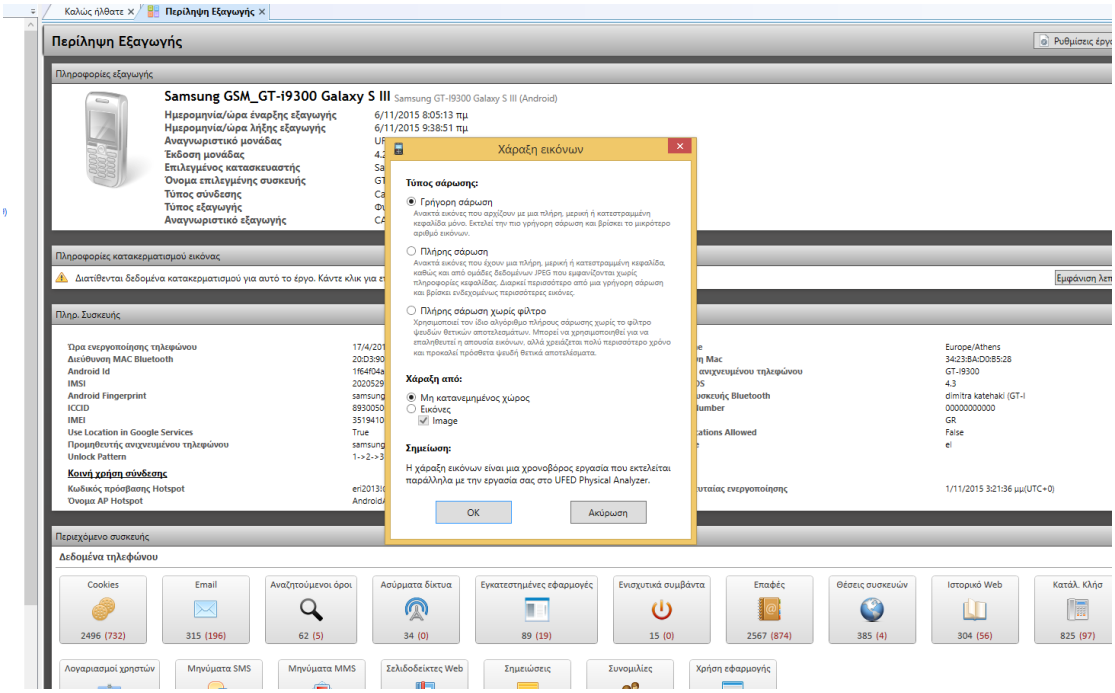
Αφού, ολοκληρωθεί επιτυχώς η φυσική εξαγωγή της μνήμης του κινητού, με το viewer που διαθέτει το εν λόγω εργαλείο, βλέπουμε τα δεδομένα αυτού και εν συνεχεία ακολουθεί η εξαγωγή της αναφοράς ανάλογα με τα ευρήματα που θα δώσουμε. Πριν την τελική εξαγωγή της αναφοράς (βλ. εικόνες 41 & 42), υπάρχει και η δυνατότητα να αναζητήσουμε και περισσότερες εικόνες (π.χ. από τον μη κατανεμημένο χώρο) (βλ. Εικόνες 37 έως 40).



Εικόνα 37. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction)

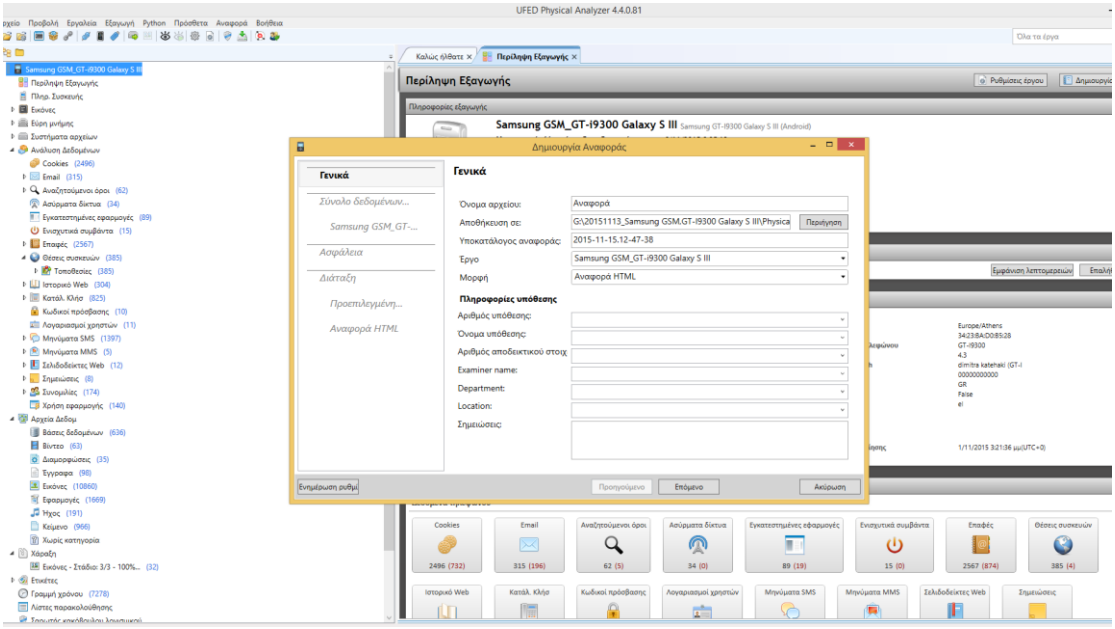


Εικόνα 38. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction) – Διαδικασία αναζήτησης διαγεγραμμένων εικόνων

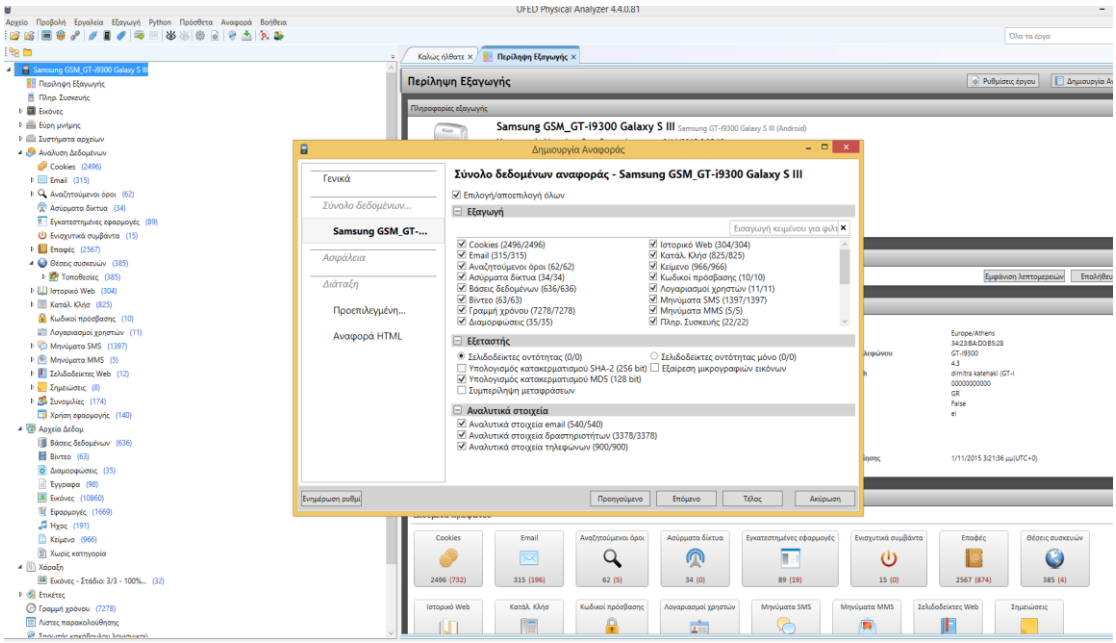


Εικόνα 39. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction) - Διαδικασία αναζήτησης διαγεγραμμένων εικόνων

Εικόνα 40. Απεικόνιση του εργαλείου Cellebrite (Physical Extraction) - Διαδικασία αναζήτησης διαγεγραμμένων εικόνων



Εικόνα 41. Δημιουργία Αναφοράς του εργαλείου Cellebrite (Physical Extraction)

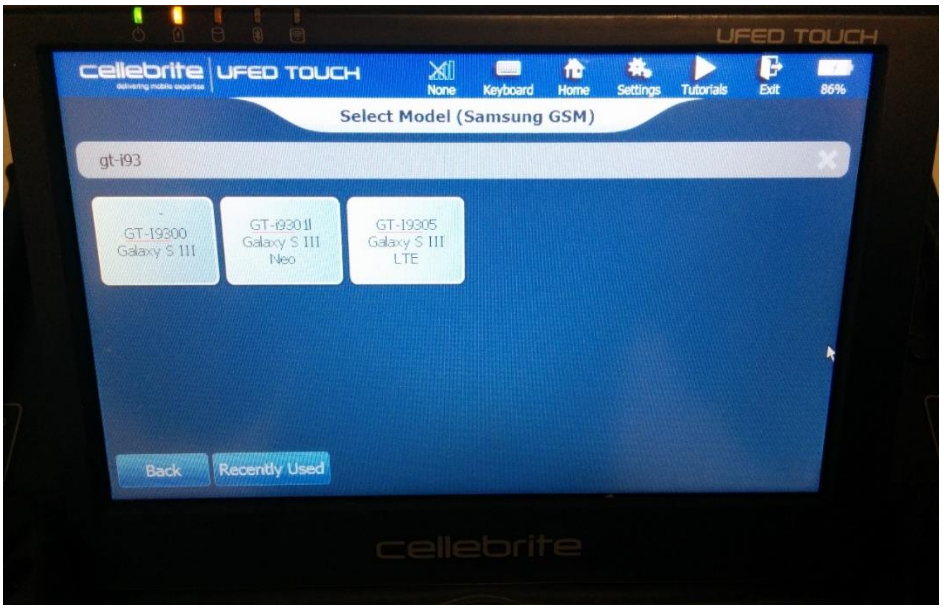


Εικόνα 42. Δημιουργία Αναφοράς του εργαλείου Cellebrite (Physical Extraction)

Εδώ, θα πρέπει να τονιστεί ότι το εργαλείο cellebrite μπορεί να προχωρήσει σε φυσική εξαγωγή και στην περίπτωση που το κινητό δεν έχει ενεργοποιημένο το USB Debugging.

6.2.1 Λογική Εξαγωγή (Logical extraction)

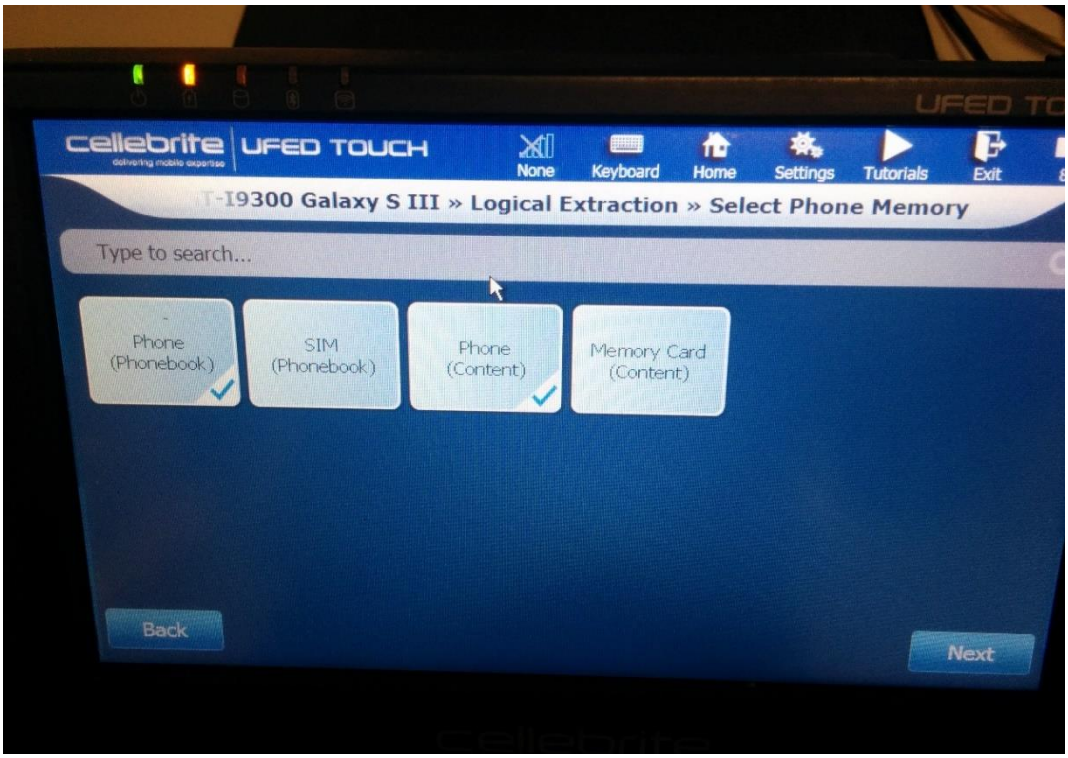
Εδώ θα χρησιμοποιήσουμε εκ νέου το εμπορικό εργαλείο Cellebrite και θα δείξουμε εάν υποστηρίζει την λογική ανάλυση στην ως άνω περίπτωση. Αρχικά, ψάχνουμε το μοντέλο του κινητού προκειμένου να δούμε εάν το συγκεκριμένο εργαλείο το υποστηρίζει (βλ. Εικόνες 43 & 49).



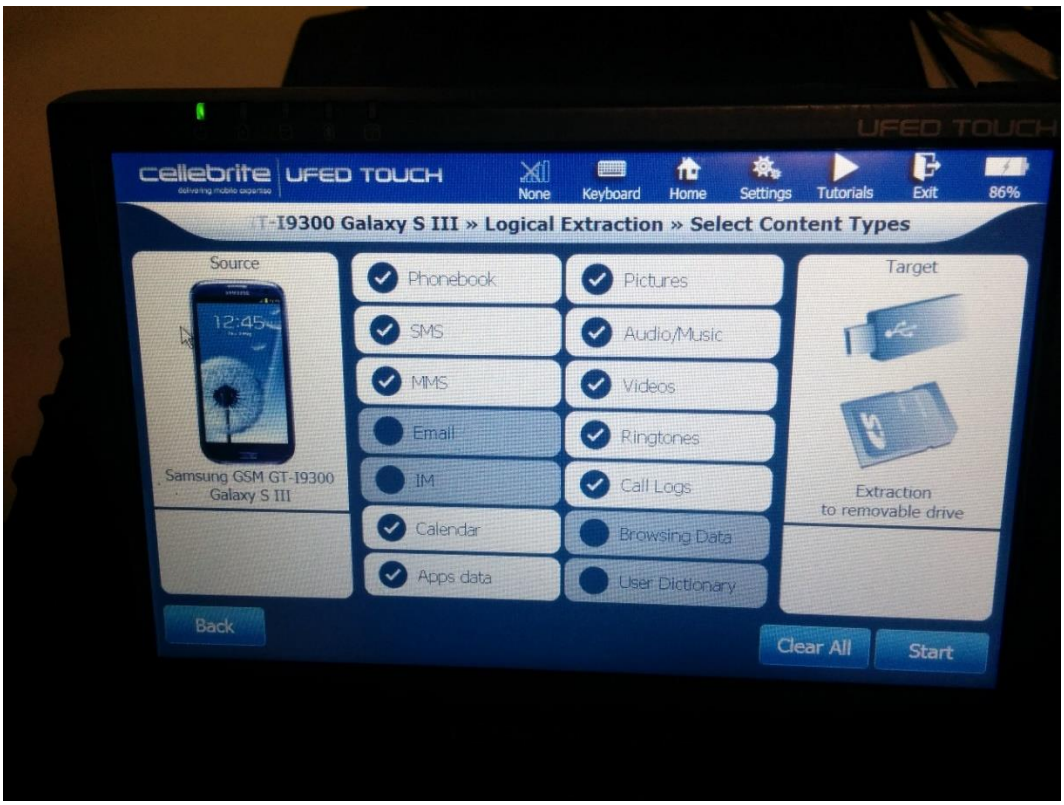
Εικόνα 43. Απεικόνιση του εργαλείου Cellebrite

Εν συνεχεία, επιλέγουμε την λογική εξαγωγή (Logical extraction).

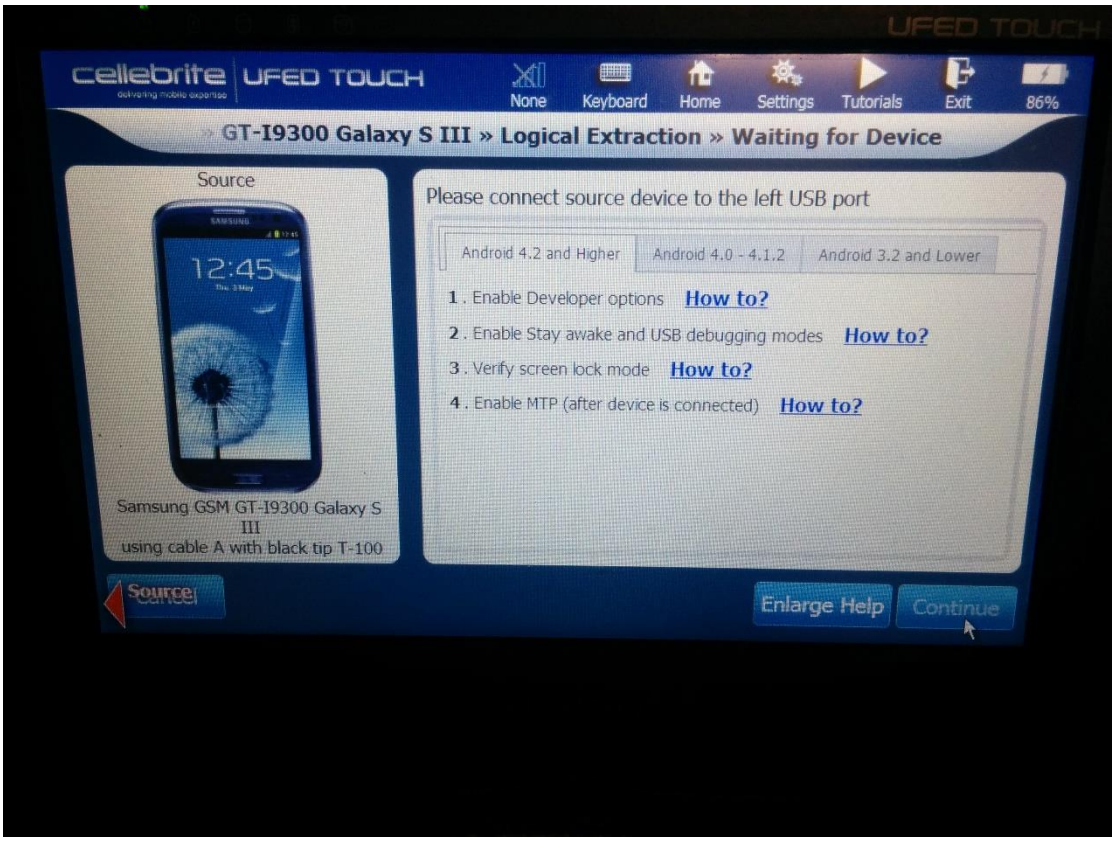
Εικόνα 44. Απεικόνιση του εργαλείου Cellebrite (τύποι εξαγωγής)



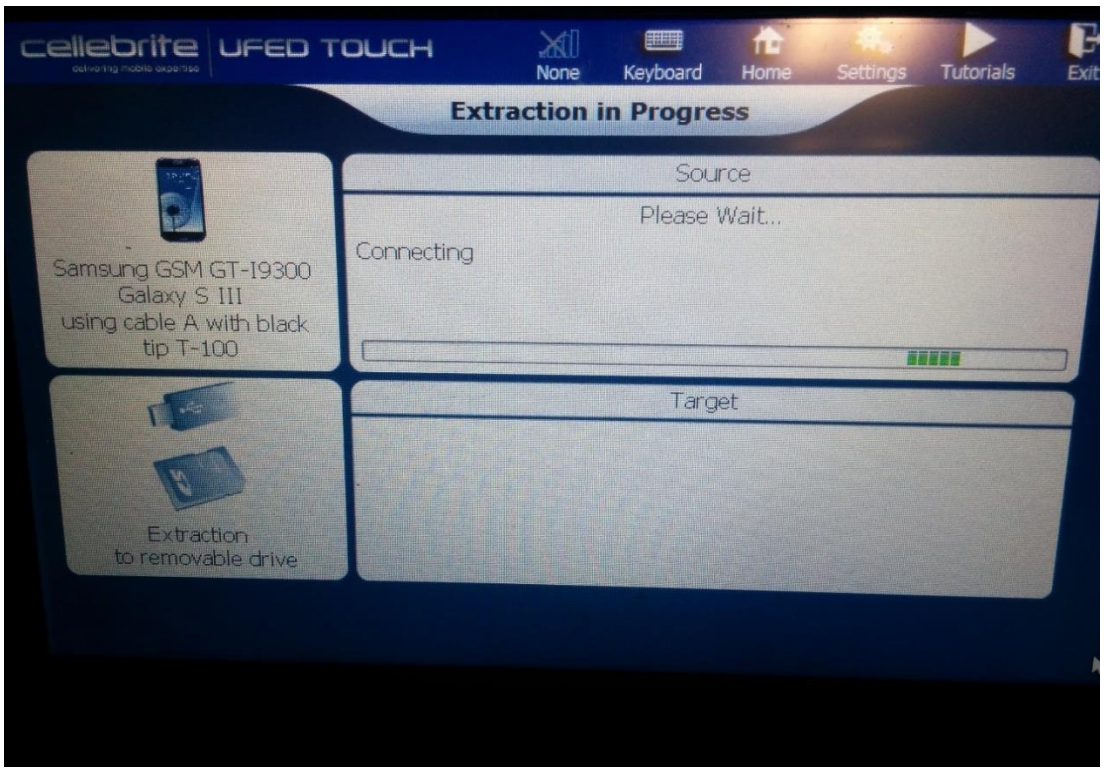
Εικόνα 45. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)



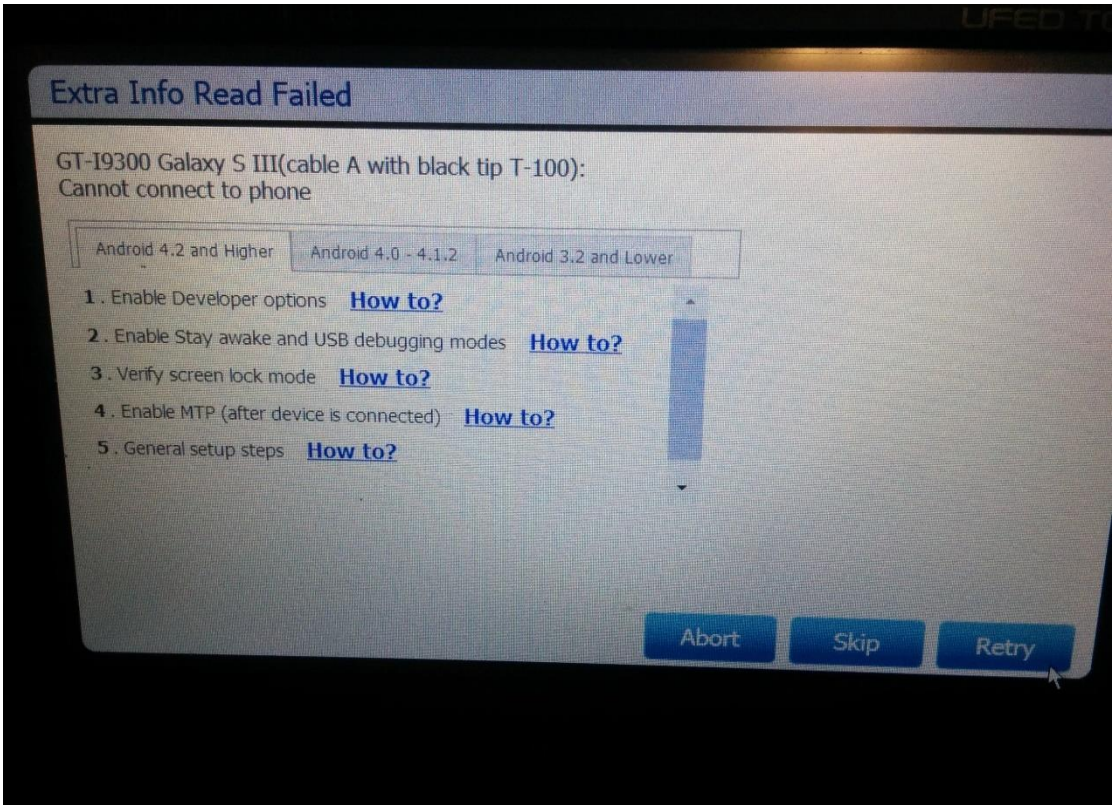
Εικόνα 46. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)



Εικόνα 47. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)



Εικόνα 48. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)

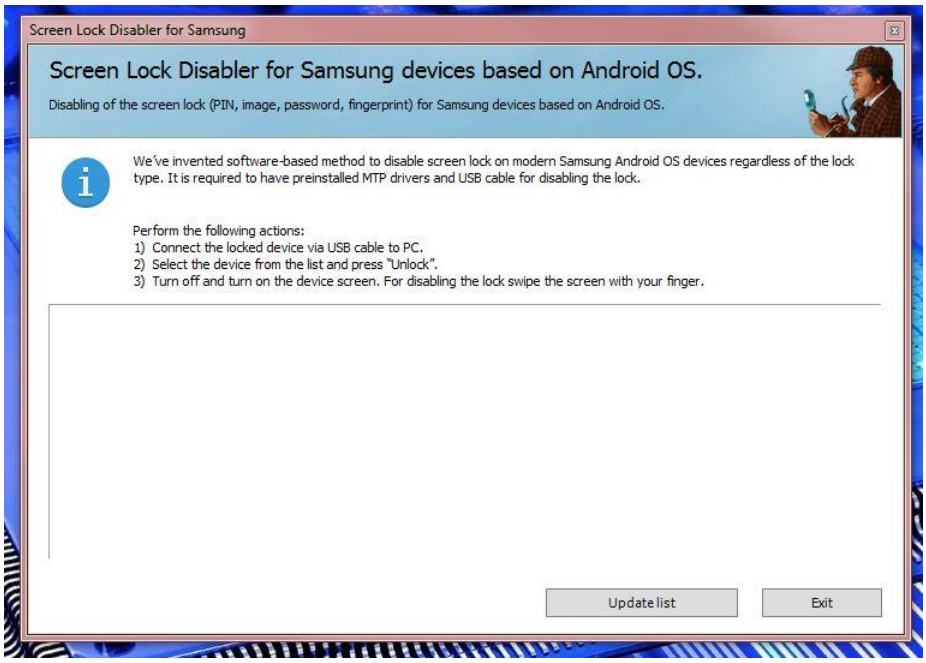


Εικόνα 49. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)

Εδώ, διαπιστώνουμε ότι στην περίπτωσή μας (δηλ. το κινητό είναι κλειδωμένο με μοτίβο), δεν είναι δυνατή η λογική ανάλυση του από το συγκεκριμένο εργαλείο.

6.2.2 Το εργαλείο Oxygen

Αρχικά, θα πρέπει να αναφερθεί ότι το εργαλείο Oxygen παρέχει την δυνατότητα μιας εφαρμογής που ξεκλειδώνει τα κινητά τηλέφωνα κατασκευής Samsung. Ειδικότερα, με το λογισμικό Screen lock disabler devices based on Android OS ξεκλειδώνει όλα τα κλειδώματα (Pin, Image, Password & Fingerprint). Χρησιμοποιώντας το εν λόγω λογισμικό, δοκιμάσαμε να ξεκλειδώσουμε το κινητό της υπόθεσή μας (βλ. Εικόνες 50 & 51).



Εικόνα 50. Απεικόνιση του εργαλείου Oxygen Screen lock disabler

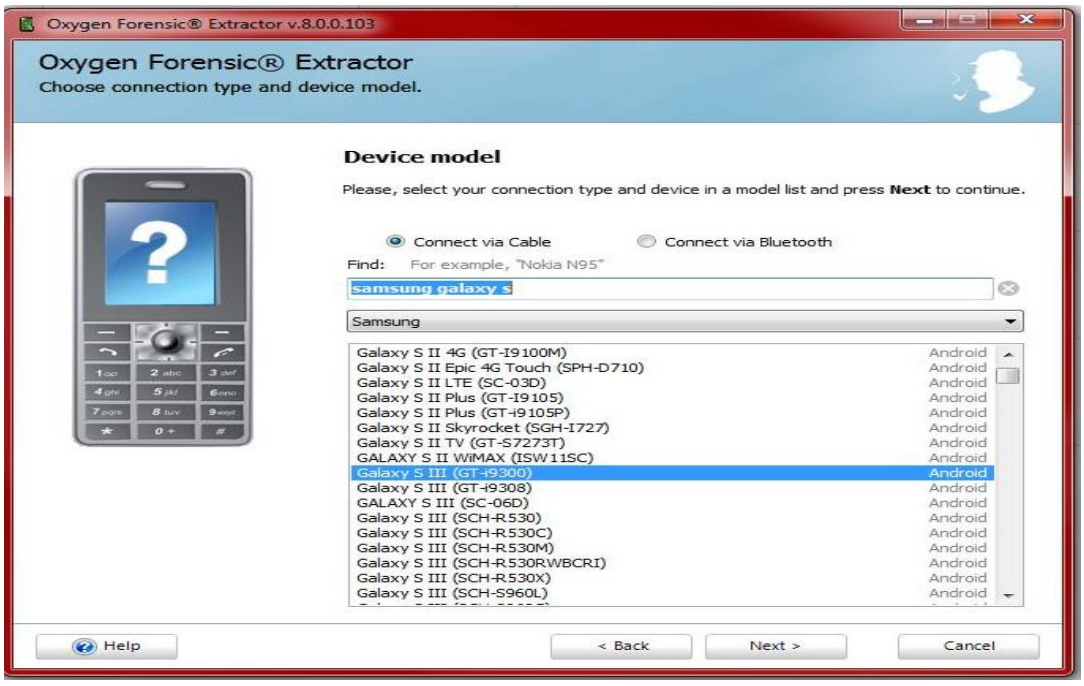
Εικόνα 51. Απεικόνιση του εργαλείου Oxygen Screen lock disabler

Πράγματι, το κινητό ξεκλειδώθηκε και προκειμένου να διαπιστώσουμε εάν όντως αυτό ισχύει και για τα λοιπά κλειδώματα δοκιμάσαμε να βάλουμε ένα (1) κωδικό PIN καθώς και να απενεργοποιήσουμε την δυνατότητα του USB Debugging. Τα αποτελέσματα ήταν εντυπωσιακά εάν αναλογιστούμε ακόμη ότι το κινητό δεν είχε δικαιώματα διαχειριστή. Στην συνέχεια, αφού έχουμε ξεκλειδώσει την συσκευή προβήκαμε στην ανάλυση της.

6.2.2.1 Φυσική Εξαγωγή (Physical extraction)

Προσπαθήσαμε να κάνουμε φυσική ανάλυση πλην όμως αυτό δεν ήταν εφικτό καθώς δεν υπήρχαν δικαιώματα διαχειριστή (βλ. Εικόνες 52 έως 59).

Εικόνα 52. Απεικόνιση του εργαλείου Oxygen

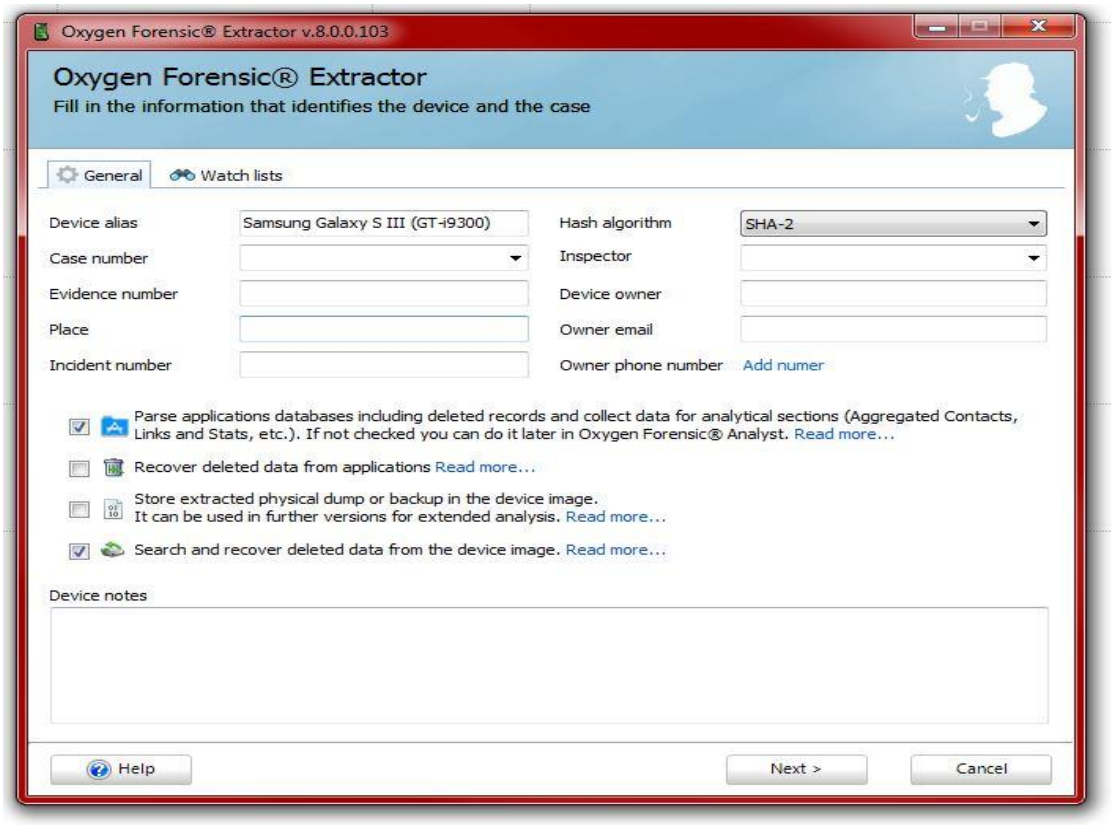


Εικόνα 53. Απεικόνιση του εργαλείου Oxygen

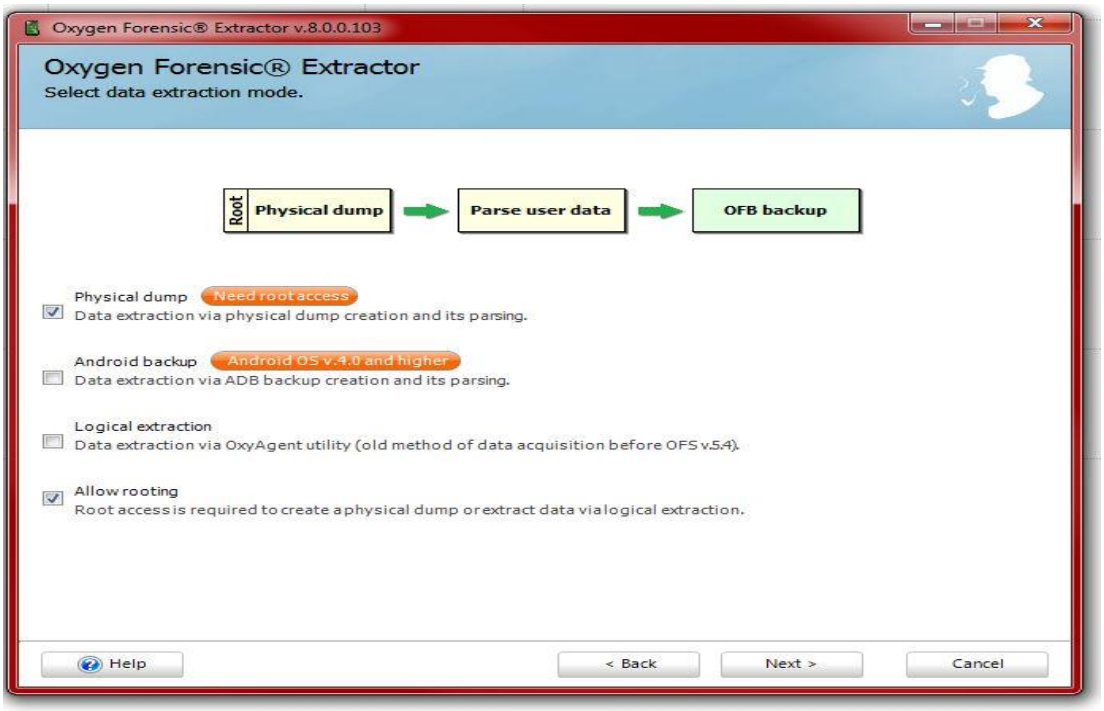
Εικόνα 54. Απεικόνιση του εργαλείου Oxygen

Εικόνα 55. Απεικόνιση του εργαλείου Oxygen (authentication)

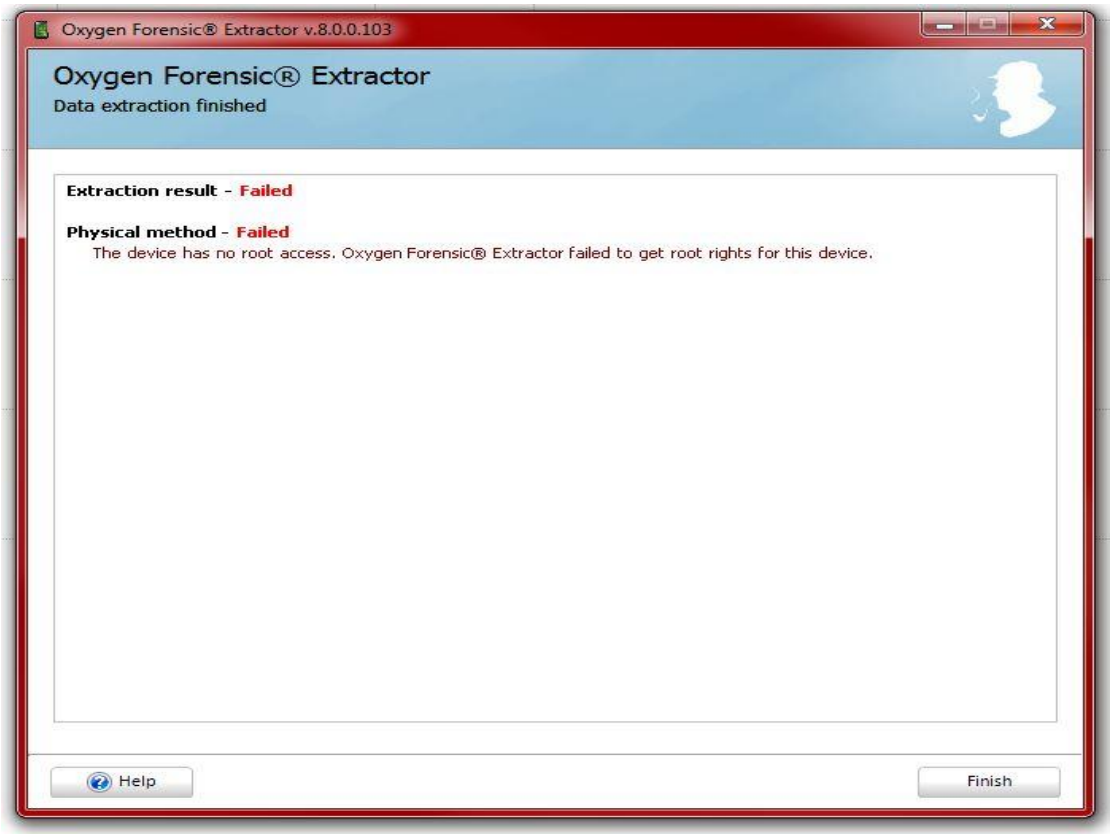
Εικόνα 56. Απεικόνιση του εργαλείου Oxygen (εντοπισμός της συσκευής)



Εικόνα 57. Απεικόνιση του εργαλείου Oxygen (acquisition method)



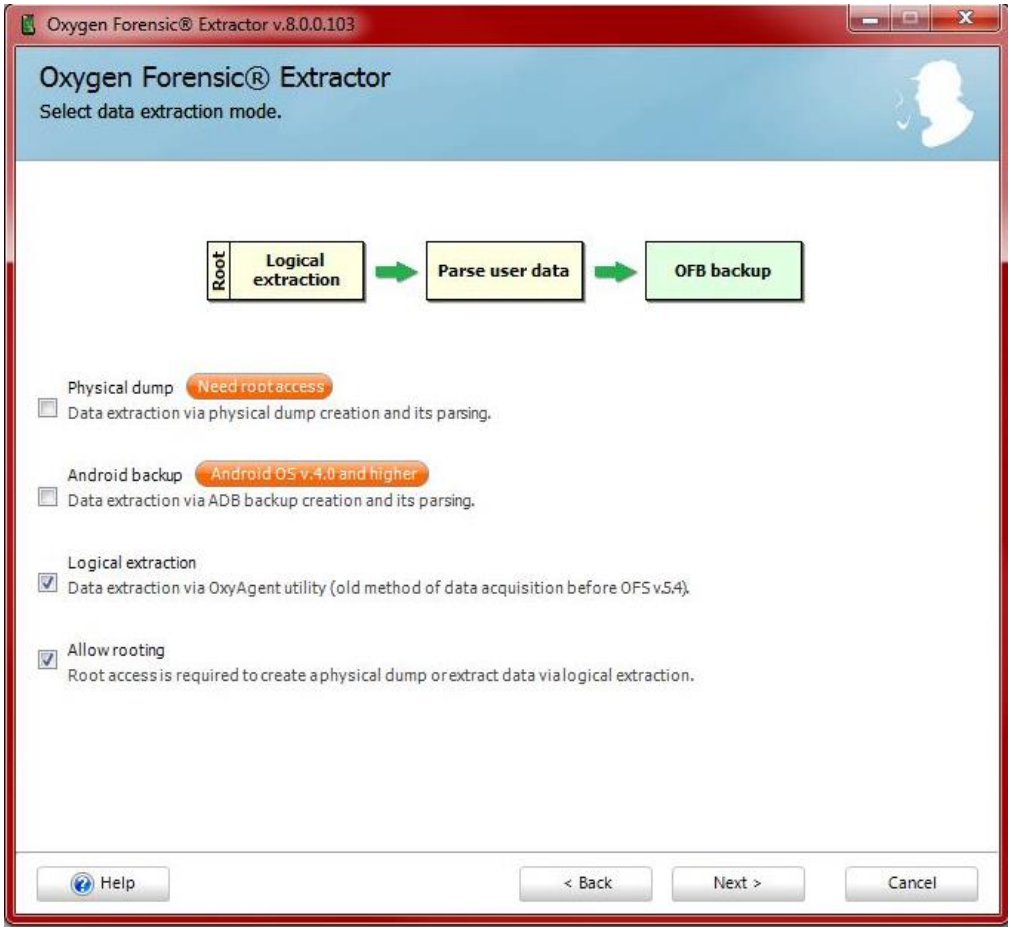
Εικόνα 58. Απεικόνιση του εργαλείου Oxygen (physical extraction)



Εικόνα 59. Απεικόνιση του εργαλείου Oxygen (physical extraction)

6.2.2.2 Λογική Εξαγωγή (Logical extraction)

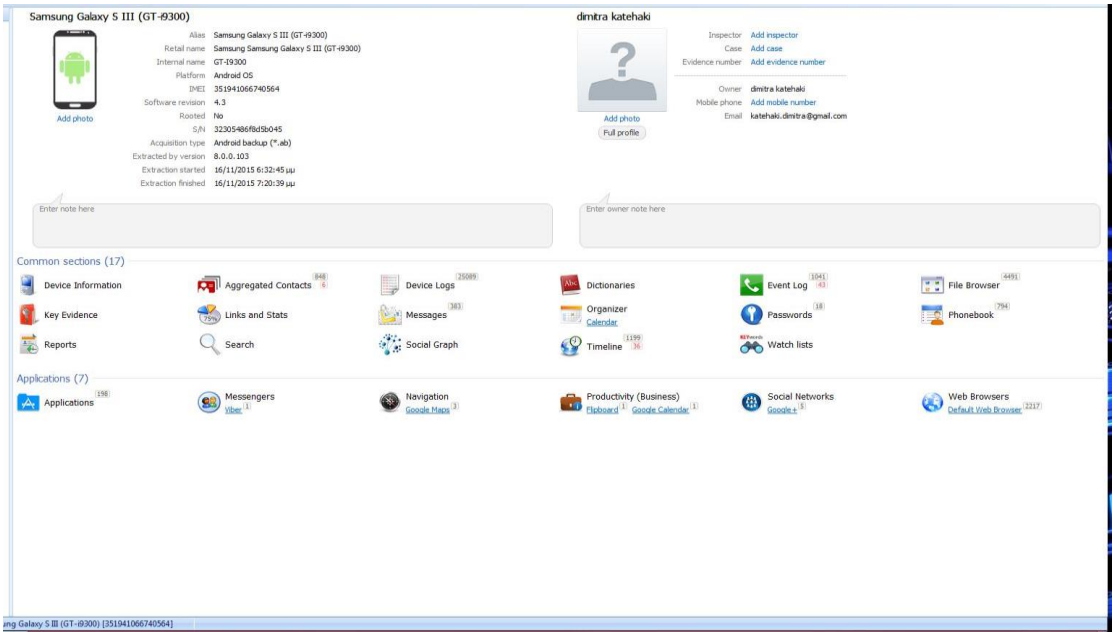
Εδώ θα χρησιμοποιήσουμε εκ νέου το εμπορικό εργαλείο Oxygen και θα δείξουμε εάν υποστηρίζει την λογική ανάλυση στην ως άνω περίπτωση. Ακολουθώντας, τα βήματα που απεικονίζονται στις εικόνες 52 έως 57 φτάνουμε στο βήμα που επιλέγουμε την ανάλυση που θέλουμε να προβούμε (βλ. εικόνα 60).



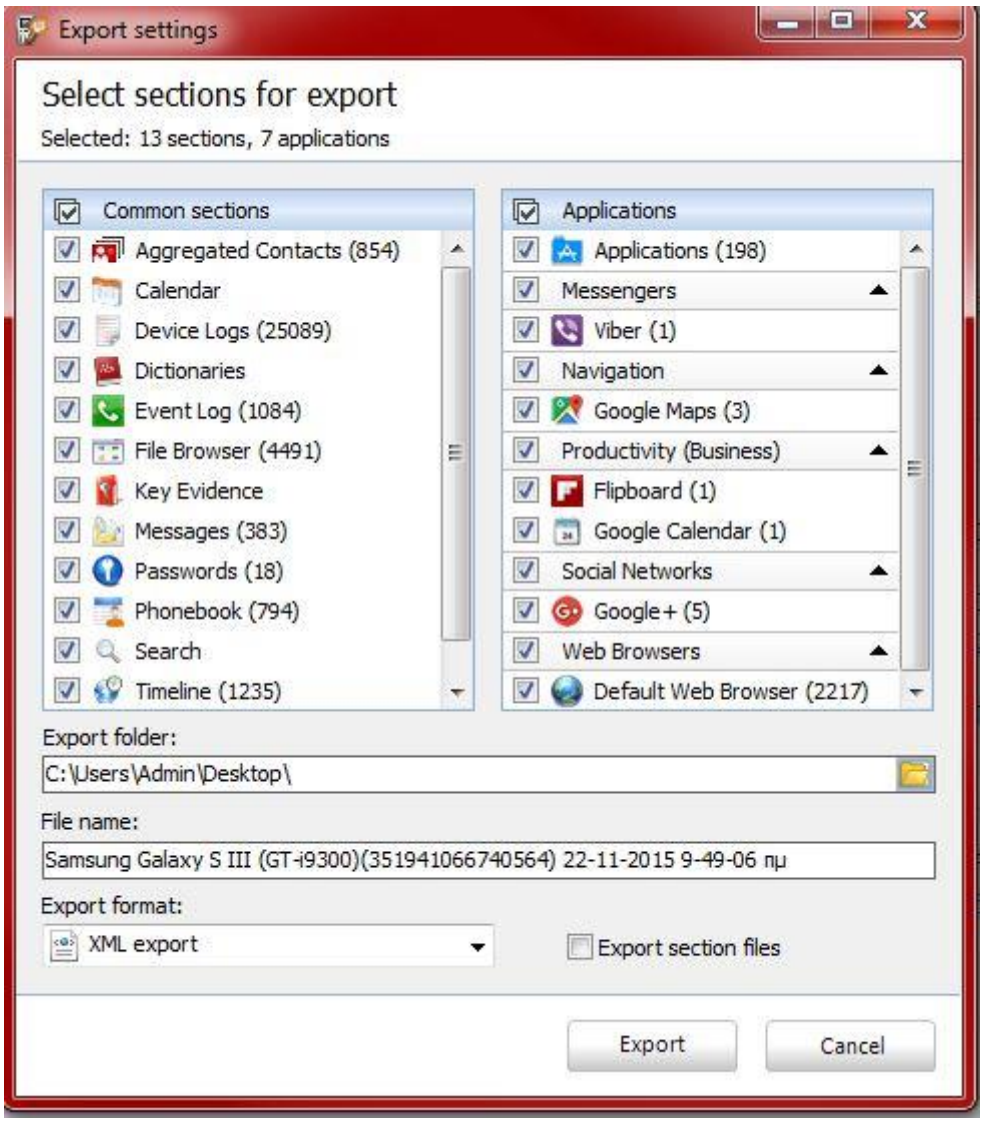
Εικόνα 60. Απεικόνιση του εργαλείου Oxygen (logical extraction)

Ακολουθούμε, τον οδηγό του εργαλείου και επιλέγουμε τα δεδομένα που θέλουμε να πάρουμε (βλ. Εικόνες 61 έως 64)

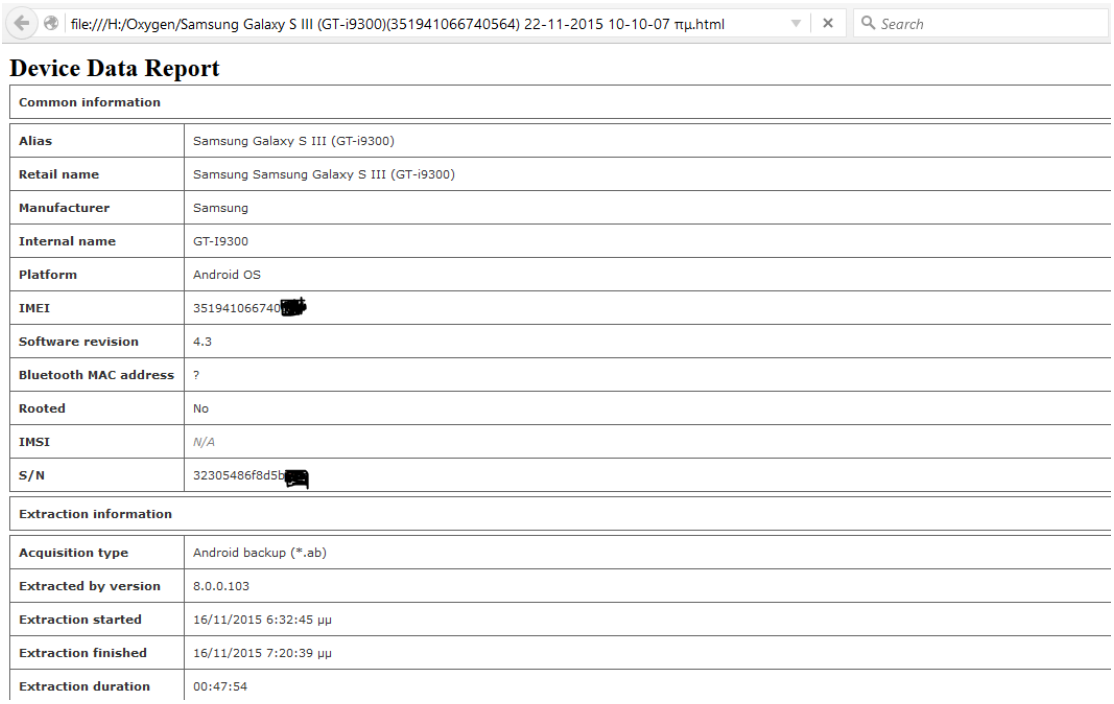
Εικόνα 61. Απεικόνιση του εργαλείου Oxygen (logical extraction)



Εικόνα 62. Απεικόνιση του εργαλείου Oxygen (logical extraction)



Εικόνα 63. Δημιουργία Αναφοράς του εργαλείου Oxygen



file:///H:/Oxygen/Samsung Galaxy S III (GT-i9300)(351941066740564) 22-11-2015 10-10-07 πμ.html

Search

Device Data Report

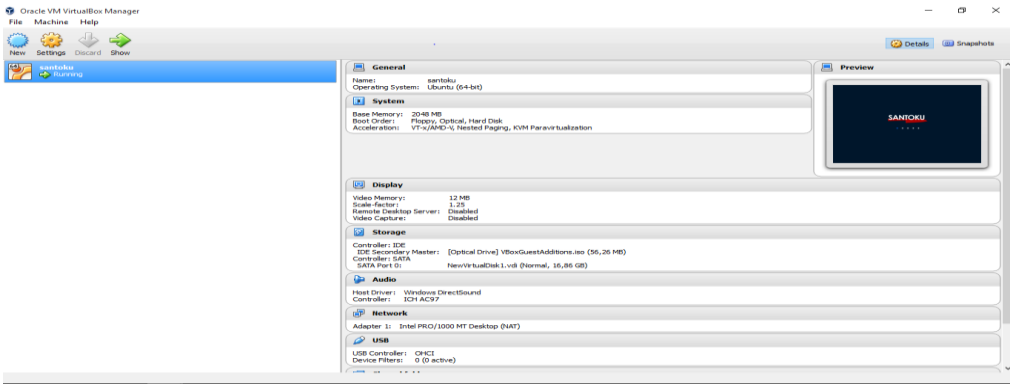
Common information	
Alias	Samsung Galaxy S III (GT-i9300)
Retail name	Samsung Samsung Galaxy S III (GT-i9300)
Manufacturer	Samsung
Internal name	GT-I9300
Platform	Android OS
IMEI	351941066740[redacted]
Software revision	4.3
Bluetooth MAC address	?
Rooted	No
IMSI	*N/A*
S/N	32305486f8d5b[redacted]

Extraction information	
Acquisition type	Android backup (*.ab)
Extracted by version	8.0.0.103
Extraction started	16/11/2015 6:32:45 μμ
Extraction finished	16/11/2015 7:20:39 μμ
Extraction duration	00:47:54

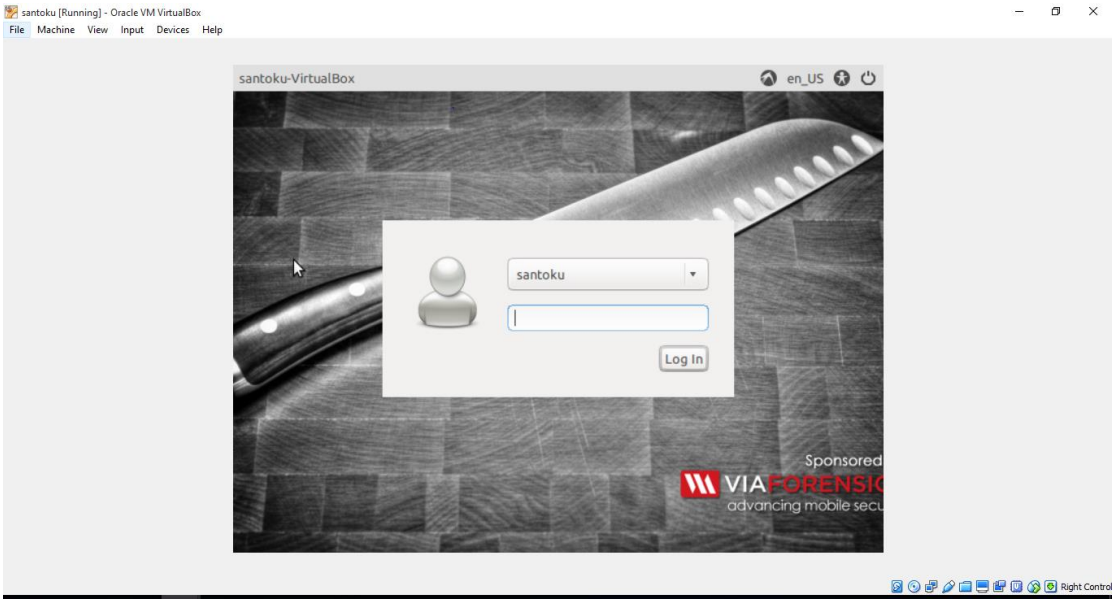
Εικόνα 64. Απεικόνιση του εργαλείου Oxygen - αναφορά

6.2.3 Το ελεύθερο λογισμικό AFlogical viaExtract

Το AFLogical viaExtract είναι το τελευταίο πρόγραμμα που χρησιμοποιήθηκε στην παρούσα εργασία. Διανέμεται δωρεάν στο διαδίκτυο και απαιτείται εγγραφή στο site της εταιρίας ώστε να εκδοθεί το κλειδί ενεργοποίησης. Γίνεται μνεία, ότι προσφέρεται με απεριόριστη άδεια σε περίπτωση που χρησιμοποιείται από αρχές επιβολής του Νόμου. Το πρόγραμμα λειτουργεί μόνο σε εικονικό περιβάλλον (vmware ή virtualbox). Στην περίπτωση μας χρησιμοποιήθηκε το virtualbox μέσω της διανομής Santoku. Συγκεκριμένα, τρέχουμε την εικονική μηχανή και δημιουργούμε ένα (1) μηχάνημα με την διανομή Santoku (βλ. Εικόνα 65).



Εικόνα 65. Απεικόνιση της εικονικής μηχανής VirtualBox



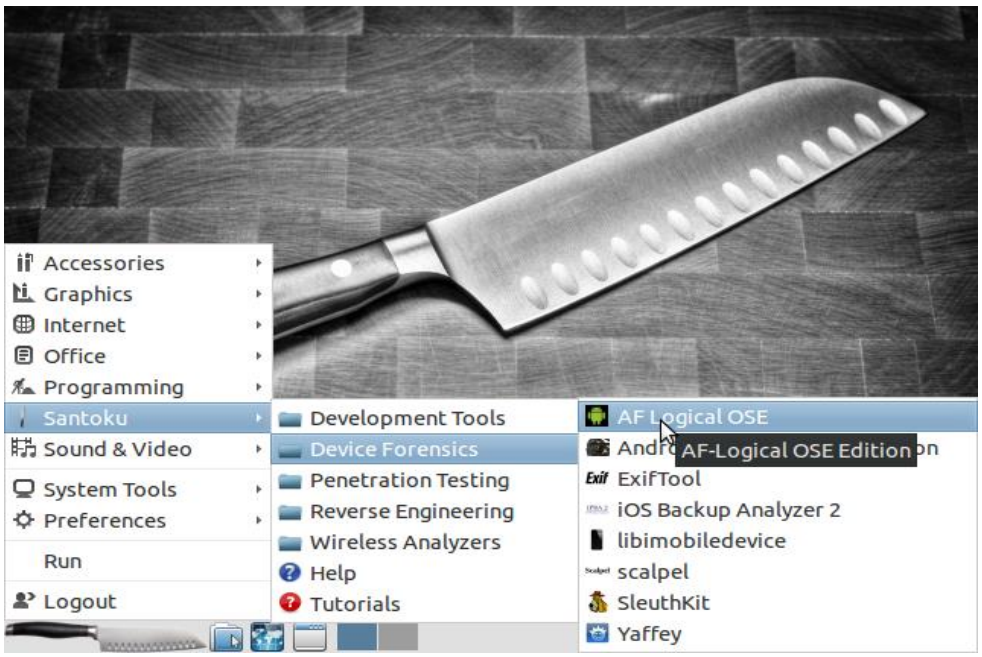
Εικόνα 66. Απεικόνιση του εργαλείου Santoku

6.2.3.1 Φυσική Εξαγωγή (Physical extraction)

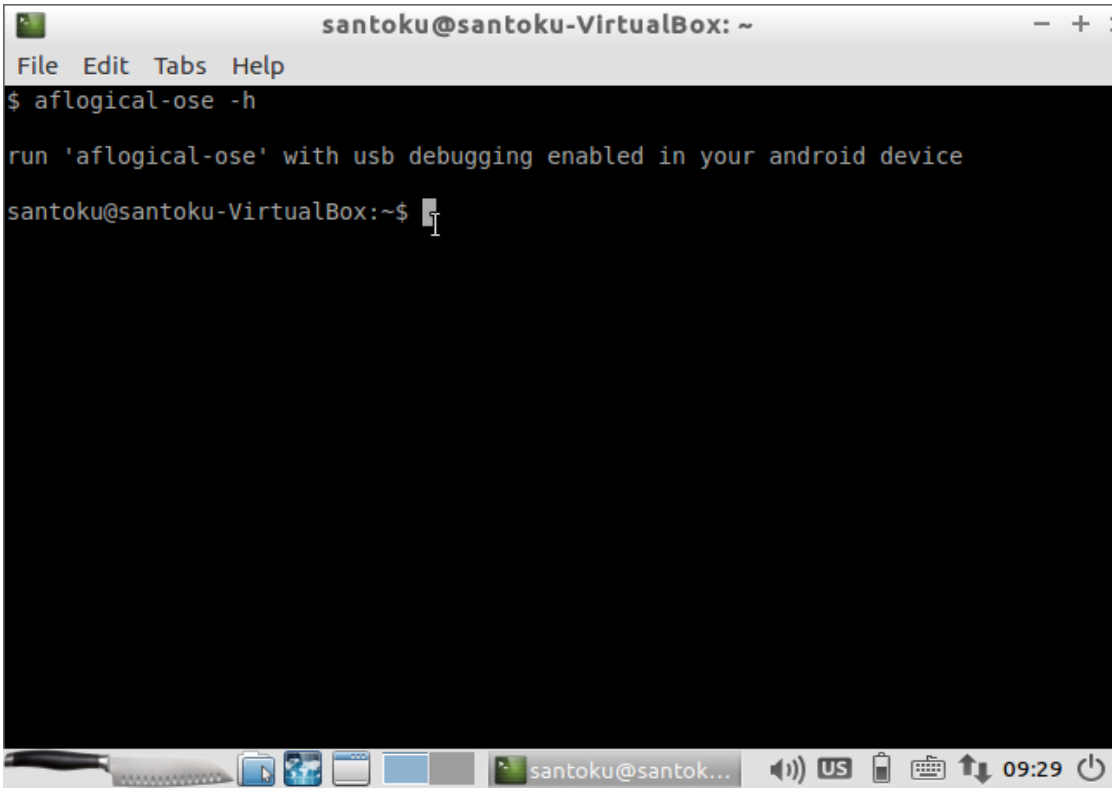
Γίνεται εύκολα κατανοητό (από την ονομασία του) ότι αυτό το εργαλείο προσφέρει μόνο την λογική ανάλυση της συσκευής, οπότε δεν είναι δυνατή η φυσική ανάλυση της συσκευής.

6.2.3.2 Λογική Εξαγωγή (Logical extraction)

Αφού έχουμε ήδη επαναλάβει τα βήματα της παραγράφου 6.2.3, στη συνέχεια, επιλέγουμε το εργαλείο AFLogical (βλ. Εικόνες 67 & 68).

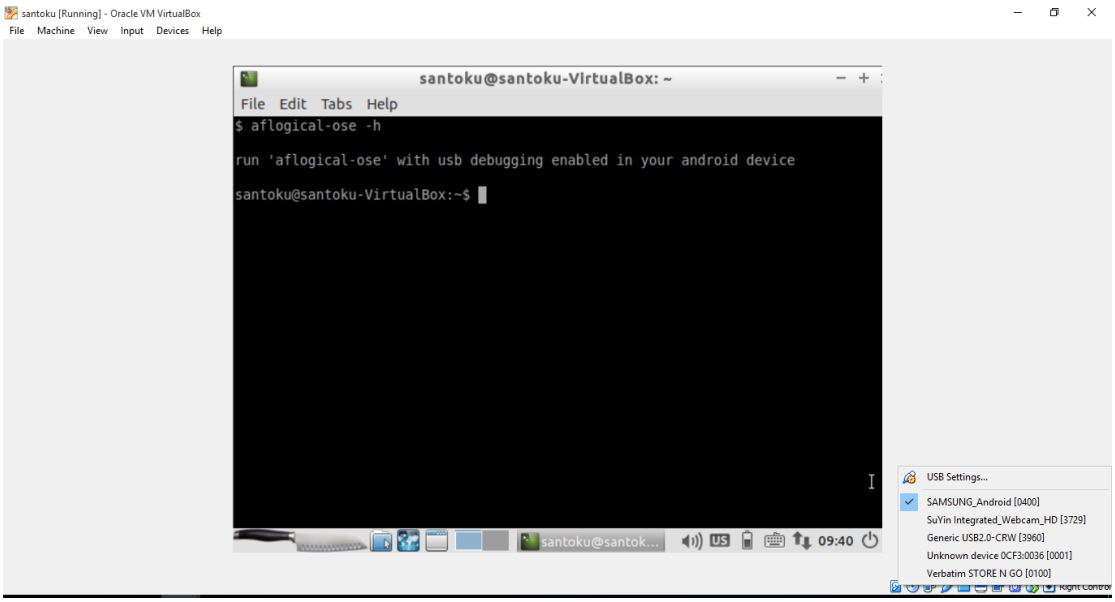


Εικόνα 67. Απεικόνιση του εργαλείου AFLogical

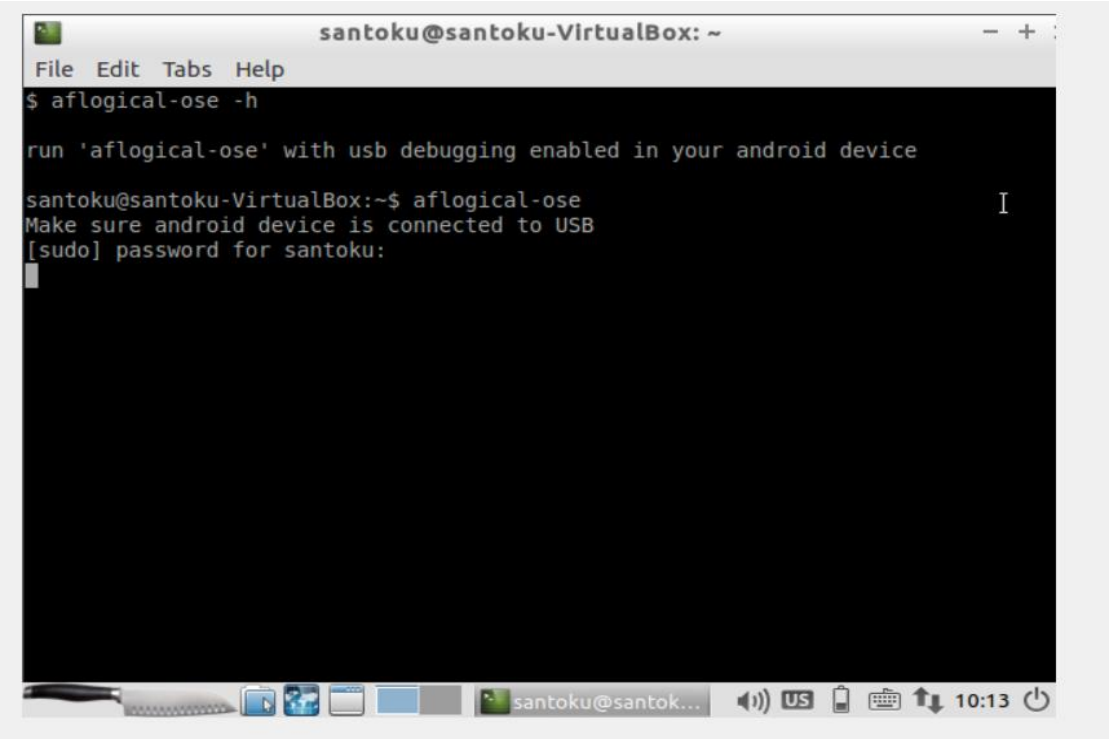


Εικόνα 68. Απεικόνιση του εργαλείου AFLogical

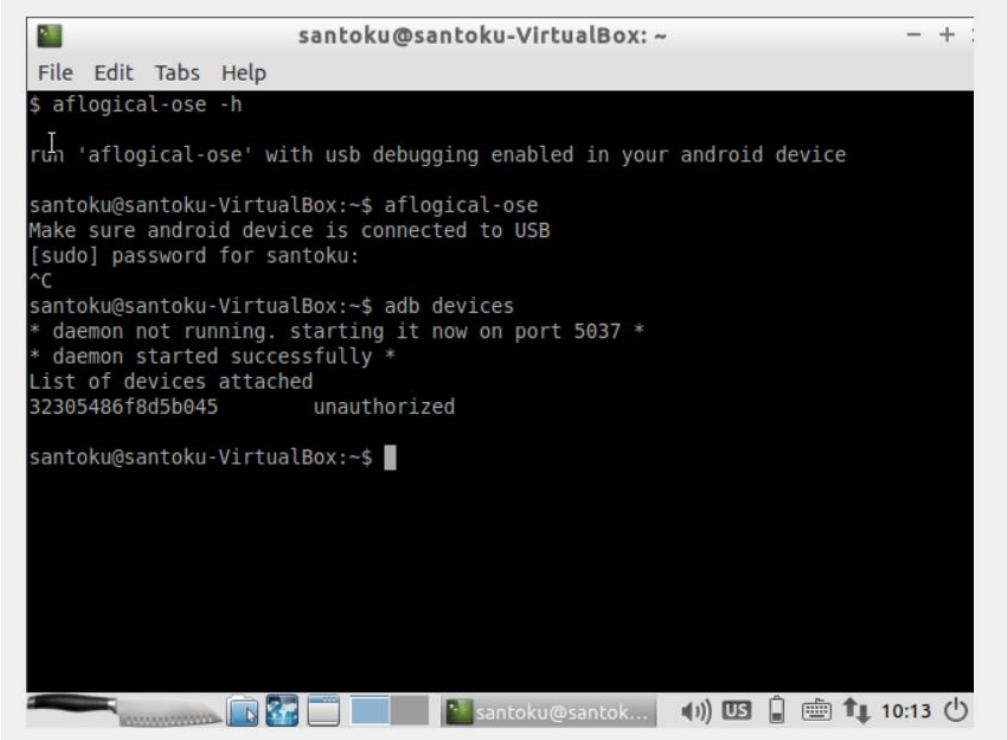
Για να υπάρχει επιτυχημένη σύνδεση του τηλεφώνου με το εργαλείο απαιτείται η ενεργοποίηση του USB Debugging. Συνδέοντας τη συσκευή στον Η/Υ, διαπιστώνουμε ότι εάν και το USB Debugging είναι ενεργοποιημένο, το εργαλείο μας δεν μπορεί να συνδεθεί στο τηλέφωνο, καθόσον αυτό είναι κλειδωμένο (βλ. Εικόνες 69 έως 72).



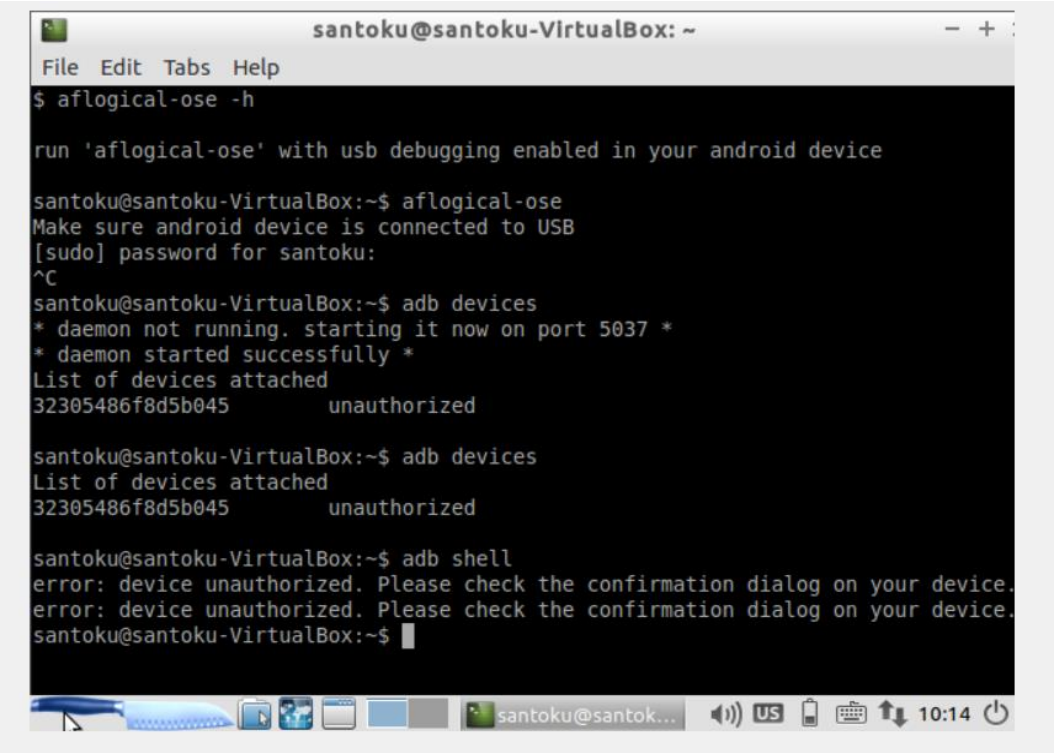
Εικόνα 69. Απεικόνιση του εργαλείου AFLogical



Εικόνα 70. Απεικόνιση του εργαλείου AFLogical



Εικόνα 71. Απεικόνιση του εργαλείου AFLogical – unauthorized device



Εικόνα 72. Απεικόνιση του εργαλείου AFLogical - unauthorized device

6.3 Εξέταση Συσκευής - Δεύτερη Περίπτωση [το κινητό δεν είναι κλειδωμένο & δεν υπάρχουν δικαιώματα διαχειριστή (no root)]

Σ΄ αυτή την περίπτωση θα λέγαμε ότι τα πράγματα είναι πιο εύκολα καθόσον δε υπάρχουν κλειδώματα και έτσι μπορούμε να προβούμε σε περισσότερες ενέργειες.

6.3.1 Το εργαλείο Celebrite

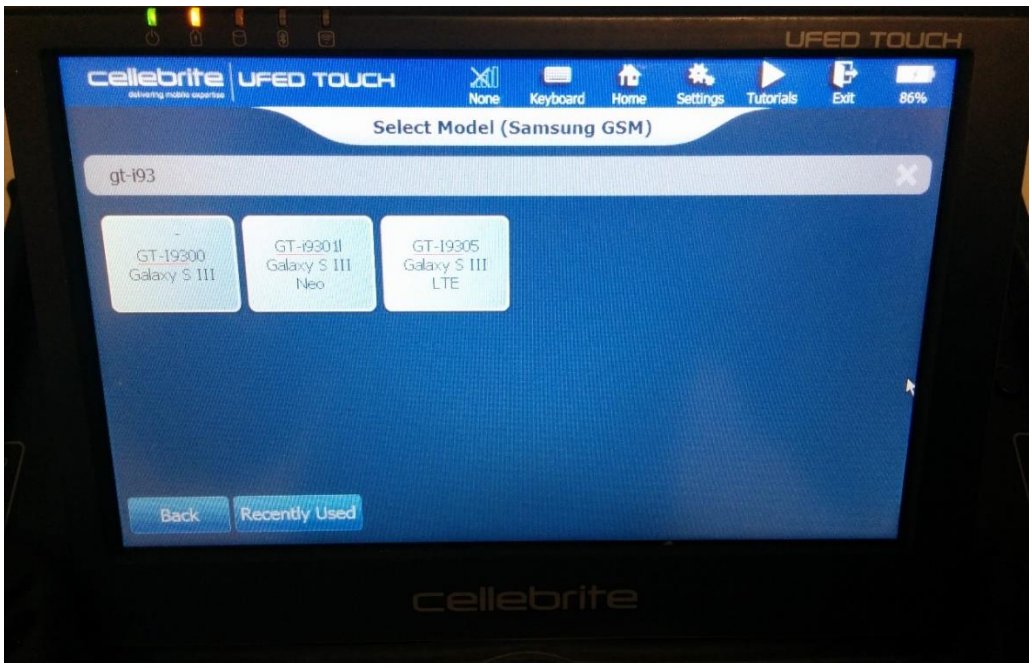
Χρησιμοποιώντας το εργαλείο Cellebrite και έχοντας υπόψη τα αποτελέσματα της προηγούμενης περίπτωσης θα περιμένουμε εδώ να επιτρέπεται η λογική ανάλυση, εφόσον το πρόβλημα μας ήταν το κλείδωμα της συσκευής.

6.3.1.1 Φυσική Εξαγωγή (Physical extraction)

Εδώ, δεν χρειάζεται να αναφέρουμε κάτι καθόσον αφού υποστηριζόταν η δύσκολη διαδικασία, σίγουρα θα υποστηρίζεται και αυτή.

6.3.1.2 Λογική Εξαγωγή (Logical extraction)

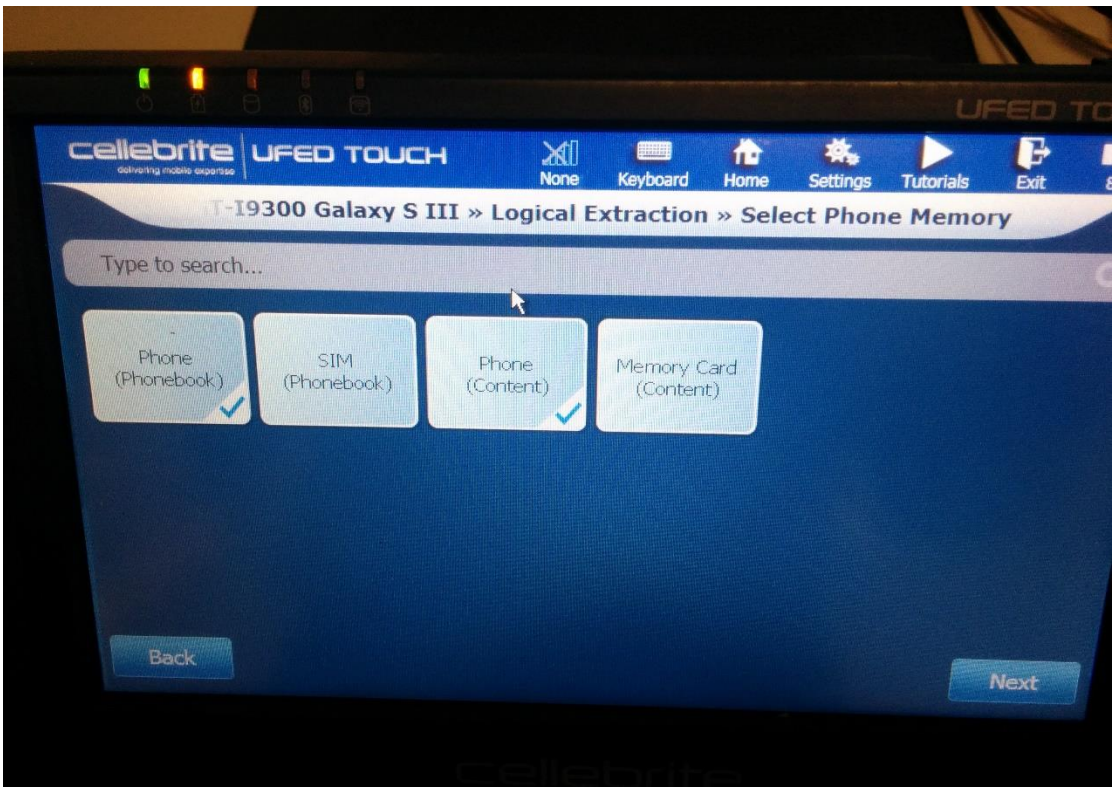
Εδώ θα χρησιμοποιήσουμε εκ νέου το εμπορικό εργαλείο Cellebrite () και θα δείξουμε εάν υποστηρίζει την λογική ανάλυση στην ως άνω περίπτωση. Αρχικά, ψάχνουμε το μοντέλο του κινητού προκειμένου να δούμε εάν το συγκεκριμένο εργαλείο το υποστηρίζει (βλ. Εικόνα 73).



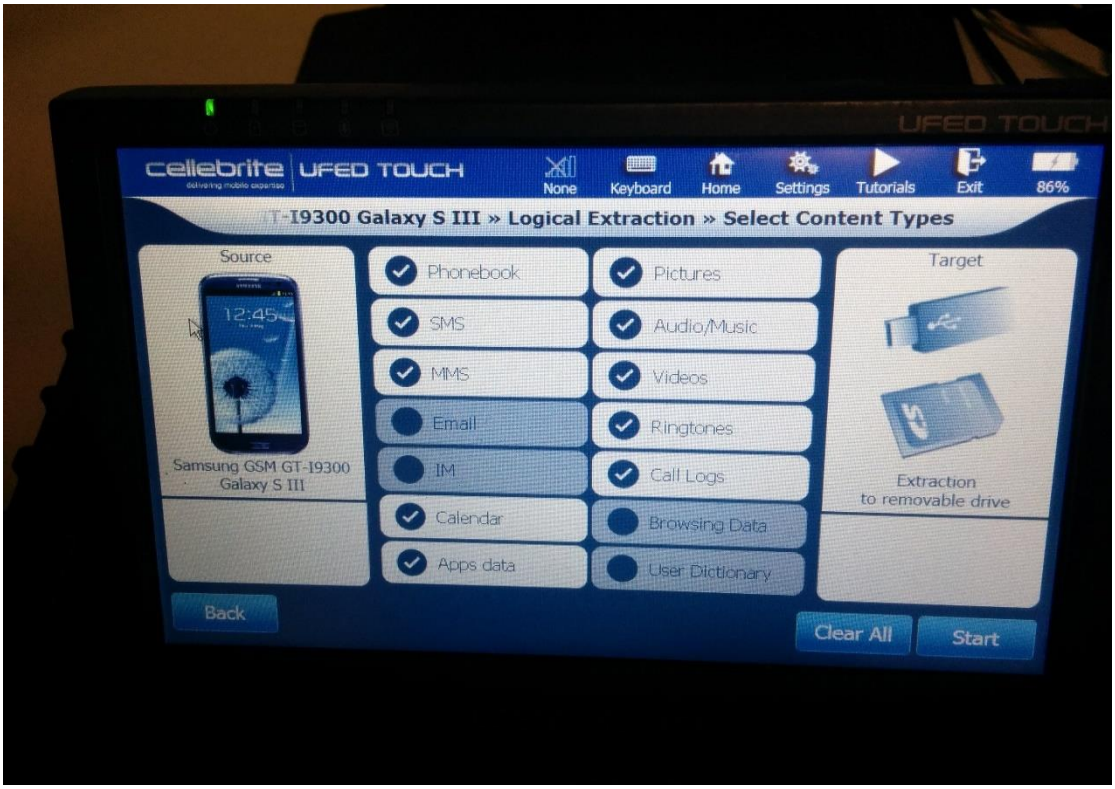
Εικόνα 73. Απεικόνιση του εργαλείου Cellebrite

Εν συνεχεία, επιλέγουμε την λογική εξαγωγή (Logical extraction).

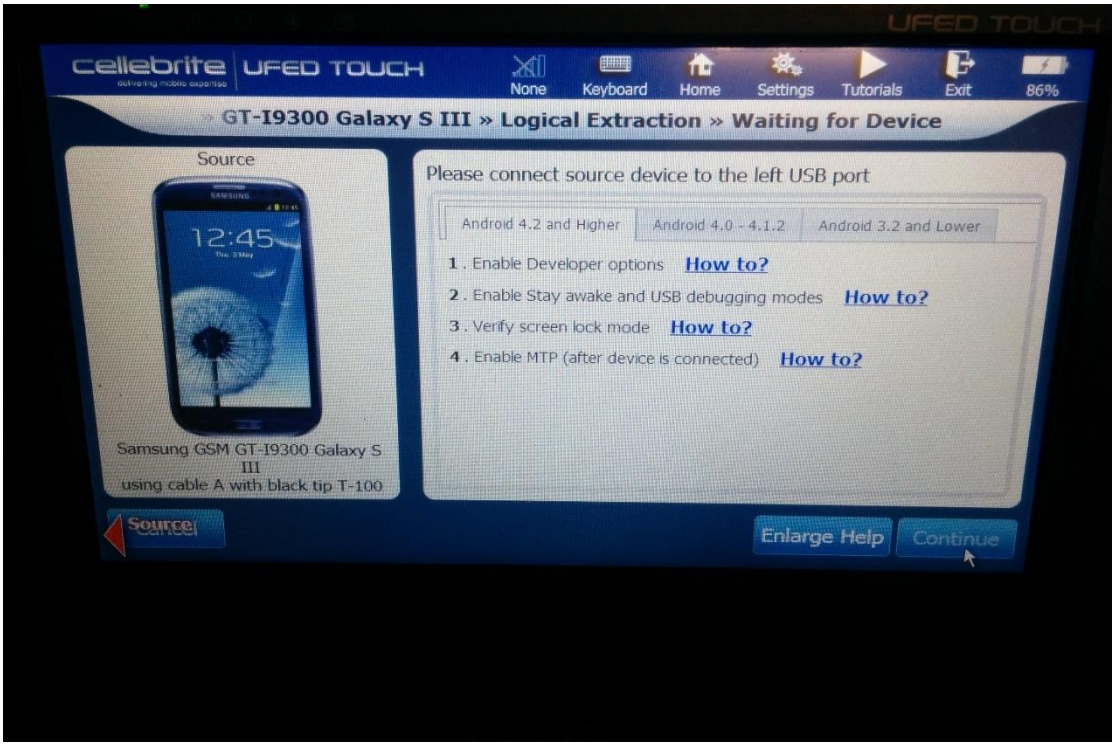
Εικόνα 74. Απεικόνιση του εργαλείου Cellebrite (τύποι εξαγωγής)



Εικόνα 75. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)

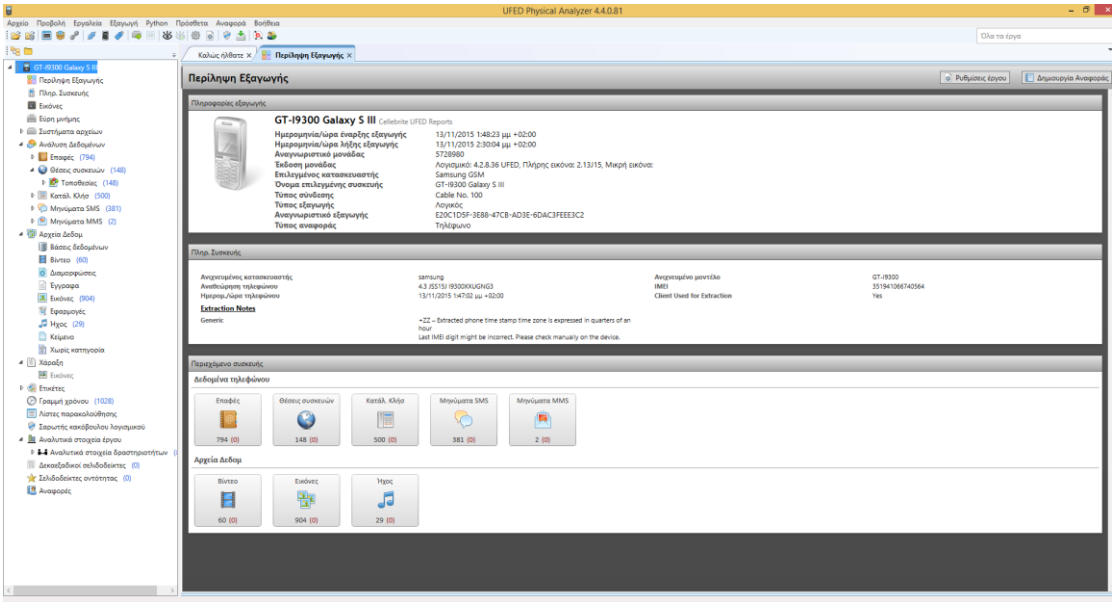


Εικόνα 76. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)

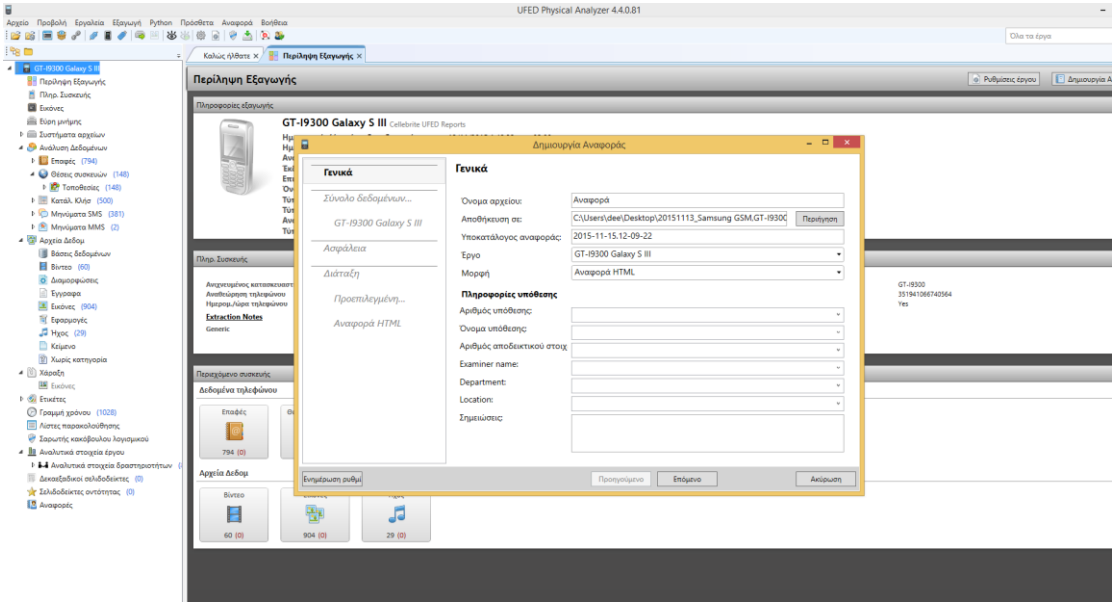


Εικόνα 77. Απεικόνιση του εργαλείου Cellebrite (logical Extraction)

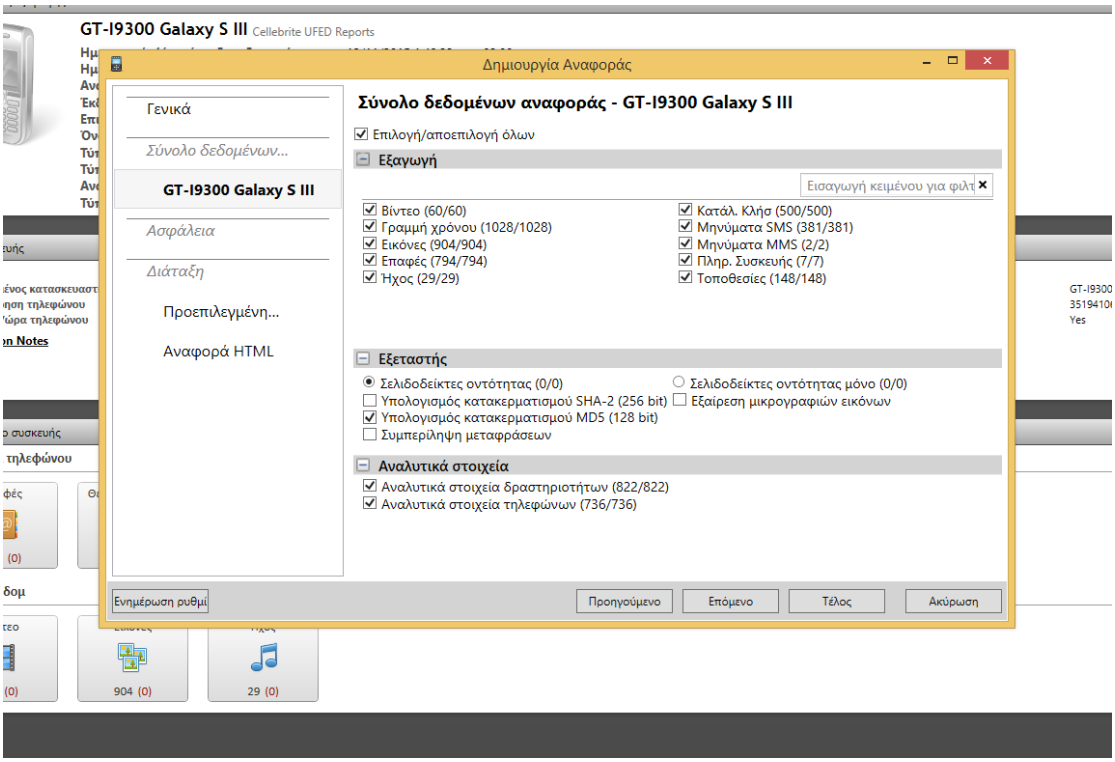
Αυτή, τη φορά η λογική εξαγωγή είναι επιτυχημένη και επομένως ανοίγουμε το εξαγόμενο αρχείο με το εργαλείο UFED Physical Analyzer, προκειμένου να δούμε τα αποτελέσματα και να δημιουργήσουμε την αναφορά μας (βλ. Εικόνες 78 έως 80).



Εικόνα 78. Απεικόνιση του εργαλείου UFED Physical Analyzer (logical Extraction)



Εικόνα 79. Απεικόνιση του εργαλείου UFED Physical Analyzer – Δημιουργία Αναφοράς



Εικόνα 80. Απεικόνιση του εργαλείου UFED Physical Analyzer – Δημιουργία Αναφοράς

6.3.2 Το εργαλείο Oxygen

Σ' αυτή την περίπτωση όπως έχουμε ήδη αναφέρει εάν και τα πράγματα είναι πιο εύκολα αφού δεν υπάρχει κλείδωμα της συσκευής, για το εργαλείο Oxygen πάλι θα σημειώσουμε ότι το πρόβλημα ήταν τα δικαιώματα διαχειριστή προκειμένου να προβούμε σε φυσική ανάλυση. Αξίζει

να τονιστεί όμως ότι σε περίπτωση που εξετάζαμε κάποια άλλη συσκευή διαφορετικής κατασκευάστριας εταιρίας (δηλ. εκτός SAMSUNG), στην περίπτωση μας θα γινόταν λογική ανάλυση ενώ στην προηγούμενη περίπτωση (κλείδωμα συσκευής), αυτή δεν θα ήταν εφικτή.

6.3.2.1 Φυσική Εξαγωγή (Physical extraction)

Προσπαθήσαμε να κάνουμε φυσική ανάλυση, όπως και στην προηγούμενη περίπτωση, πλην όμως αυτό δεν ήταν εφικτό καθώς δεν υπήρχαν δικαιώματα διαχειριστή (βλ. παράγραφο 6.2.2.1).

6.3.2.2 Λογική Εξαγωγή (Logical extraction)

Ακολουθώντας, την διαδικασία που περιγράψαμε (βλ. παράγραφο 6.2.2.2) καταλήγουμε στα ίδια αποτελέσματα.

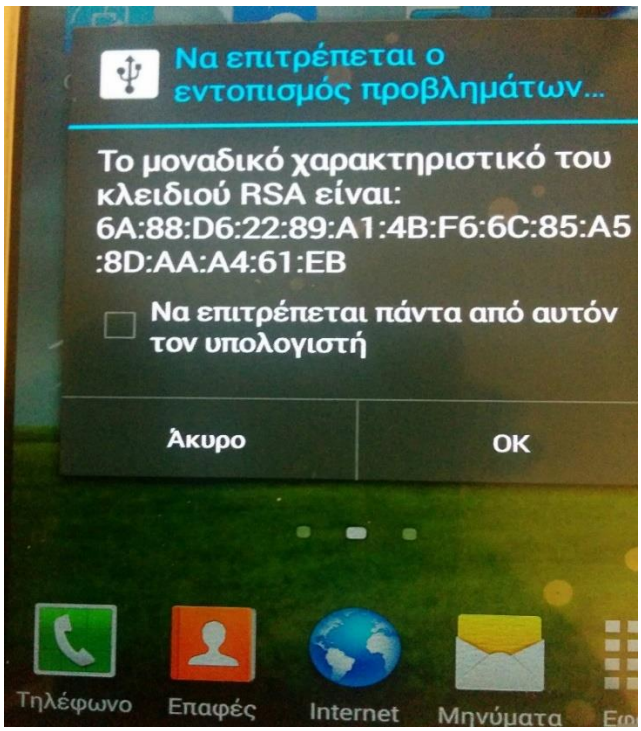
6.3.3 Το ελεύθερο λογισμικό AFlogical viaExtract

6.3.3.1 Φυσική Εξαγωγή (Physical extraction)

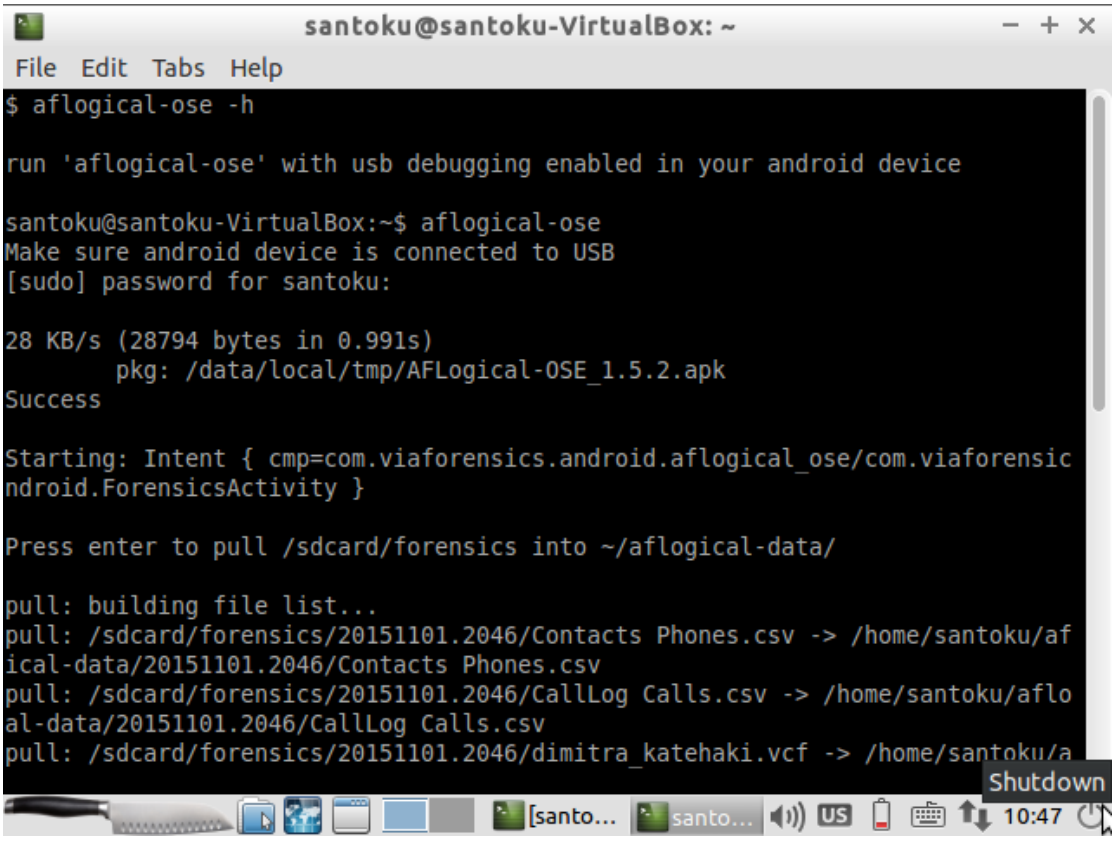
Όπως έχουμε ήδη προαναφέρει δεν είναι δυνατή η φυσική ανάλυση με το δωρεάν αυτό εργαλείο και η δυνατότητα αυτή παρέχεται μόνο στην εμπορική έκδοση του.

6.3.3.2 Λογική Εξαγωγή (Logical extraction)

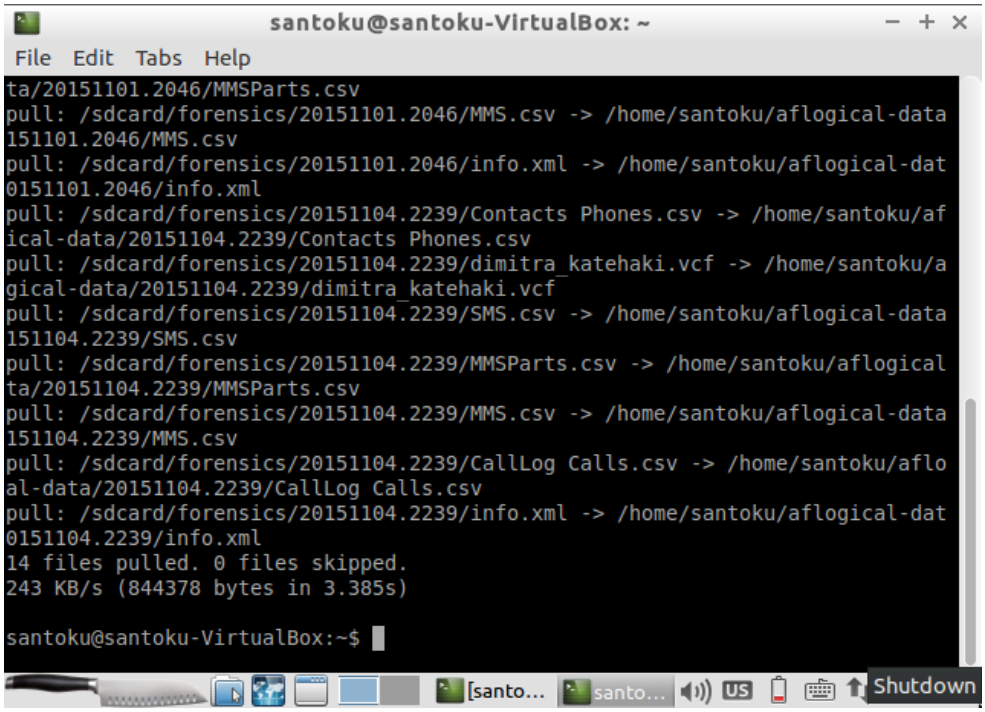
Αντίθετα, με τα αποτελέσματα της πρώτης περίπτωσης (βλ. παράγραφο 6.2.3), εδώ μπορεί να επιτευχθεί η λογική εξαγωγή της συσκευής μας, καθόσον απουσιάζει ο λόγος που μας παρεμπόδιζε προηγουμένως (κλείδωμα συσκευής). Συγκεκριμένα, εδώ μπορεί να γίνει authorized της συσκευής και επομένως να προχωρήσουμε σε λογική εξαγωγή (βλ. Εικόνες 81 έως 85).



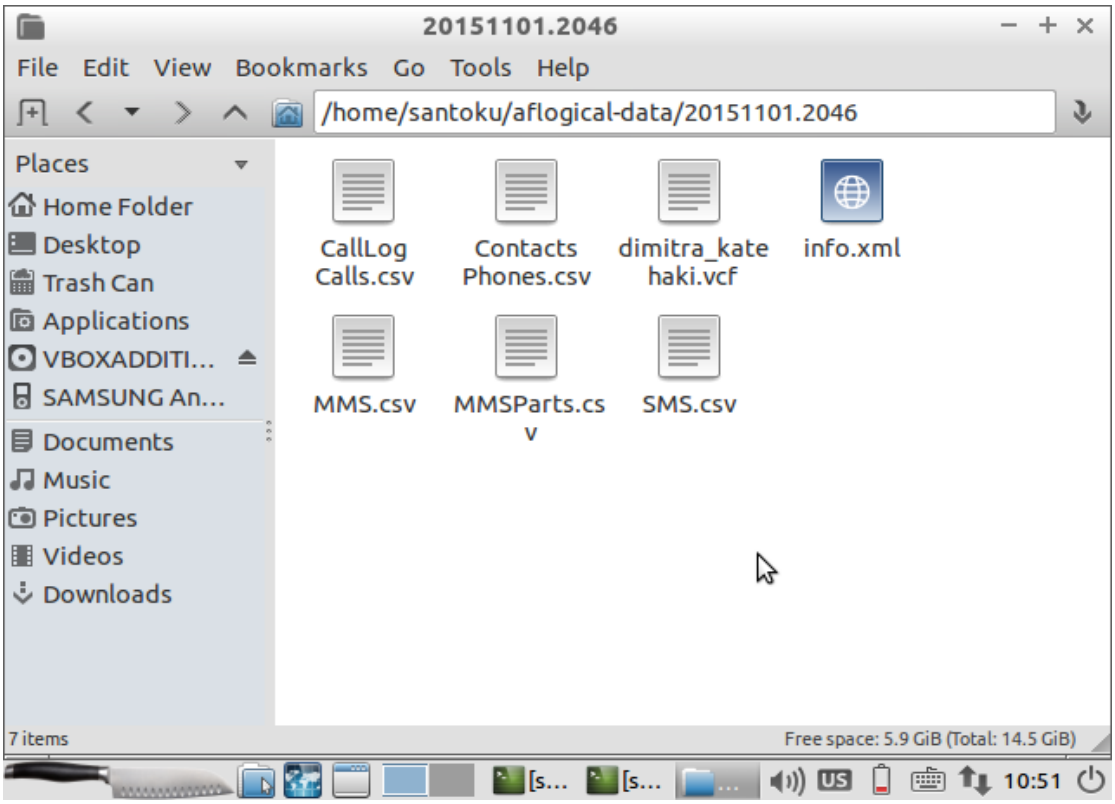
Εικόνα 81. Authorized της συσκευής



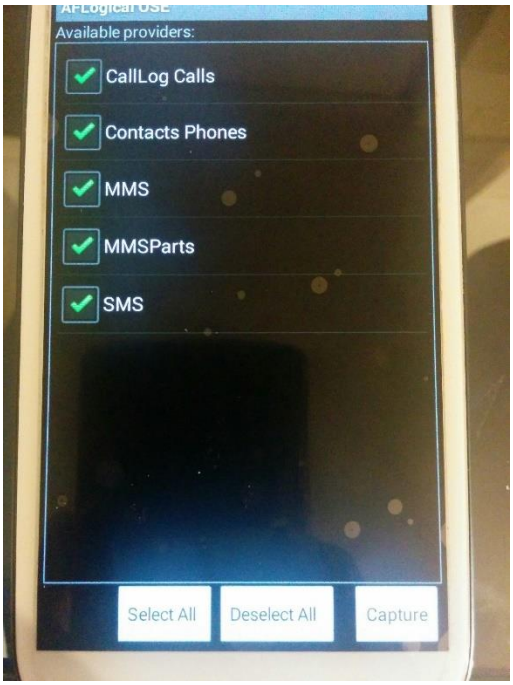
Εικόνα 82. Απεικόνιση του εργαλείου AFLogical



Εικόνα 83. Απεικόνιση του εργαλείου AFLogical



Εικόνα 84. Απεικόνιση των αποτελεσμάτων του AFLogical



Εικόνα 85. Απεικόνιση της συσκευής

Τα δεδομένα εξάγονται από το κινητό, καθώς το πρόγραμμα εγκαθιστά μία εφαρμογή στη συσκευή και στο τέλος δημιουργεί αρχεία .CSV στον ειδικό φάκελο “aflogical-data” στην εικονική μηχανή.

6.4 Εξέταση Συσκευής - Χειροκίνητη ανάλυση της συσκευής

6.4.1 Εισαγωγικά

Στη περίπτωση που θέλουμε να εξετάσουμε την λόγω συσκευή, χωρίς την χρησιμοποίηση είτε εμπορικών είτε ελεύθερων λογισμικών, για τις δύο (2) προαναφερόμενες περιπτώσεις (βλ. παρ. 6.2 & 6.3) θα σημειώναμε ότι τα πράγματα είναι αρκετά δύσκολα και εξαρτώνται από παράγοντες που έχουμε ήδη προαναφέρει όπως κλείδωμα συσκευής, ενεργοποίηση του USB Debugging, δικαιώματα διαχειριστή. Στην χειροκίνητη ανάλυση θα αναφερθούμε πρώτα στην περίπτωση που το τηλέφωνο είναι ξεκλείδωτο και έπειτα στην άλλη περίπτωση.

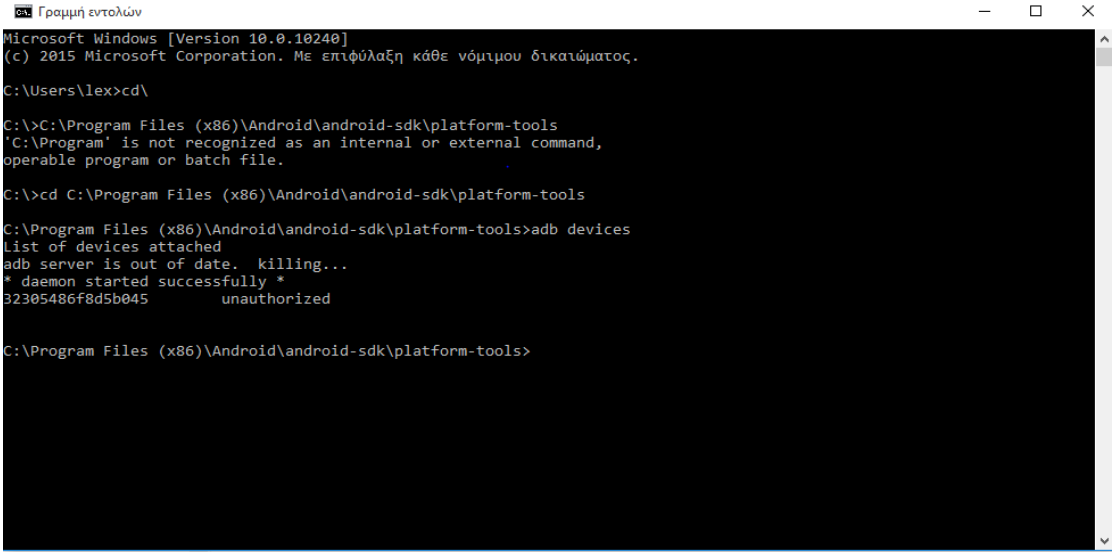
6.4.2 Το κινητό δεν είναι κλειδωμένο & δεν υπάρχουν δικαιώματα διαχειριστή (no root)]

6.4.2.1 Λογική Εξαγωγή (Logical extraction) και Ανάλυση των δεδομένων

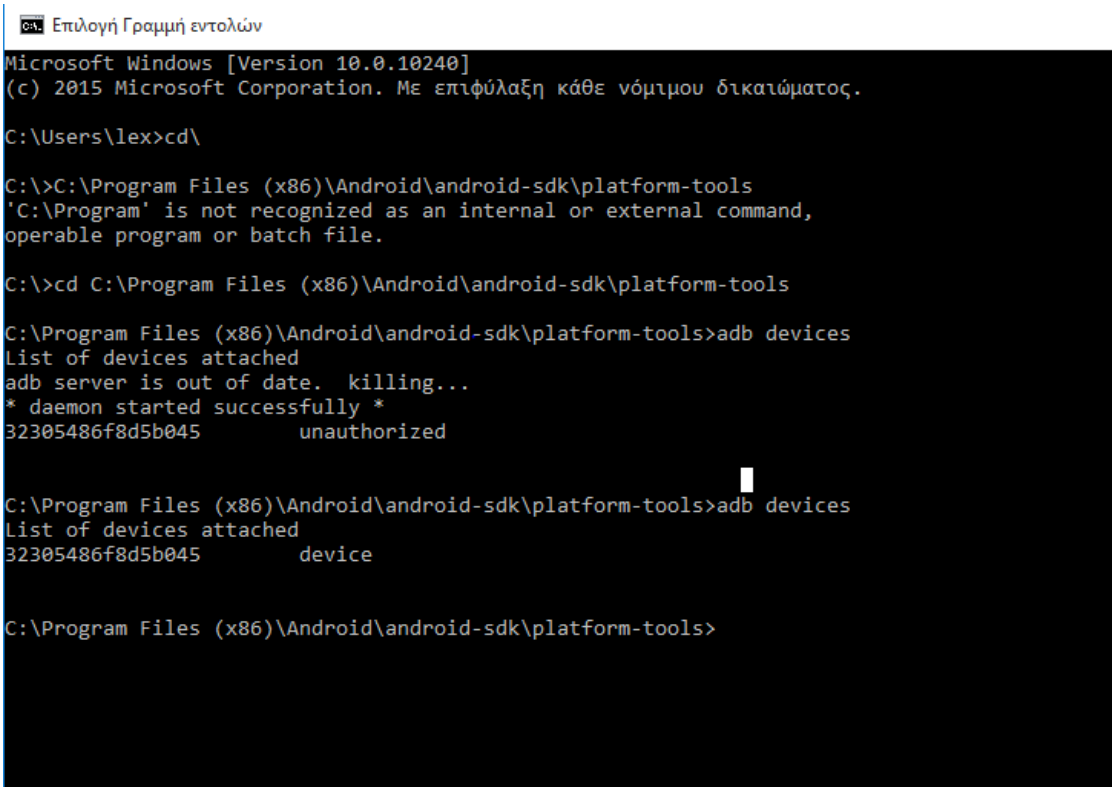
6.4.2.1.1 Λογική Εξαγωγή (Logical extraction)

Ακολουθώντας τα βήματα που έχουμε προαναφέρει (βλ. παρ. 5.2.5.1) πλοηγούμαστε στη διαδρομή που βρίσκεται το εργαλείο Adb. Εκεί, τρέχουμε την εντολή <adb devices> και ότι

αναγνωρίζετε η συσκευή μας καθώς και απαιτείται να γίνει authorized ο Η/Υ από την συσκευή (βλ. Εικόνες 86 & 87).

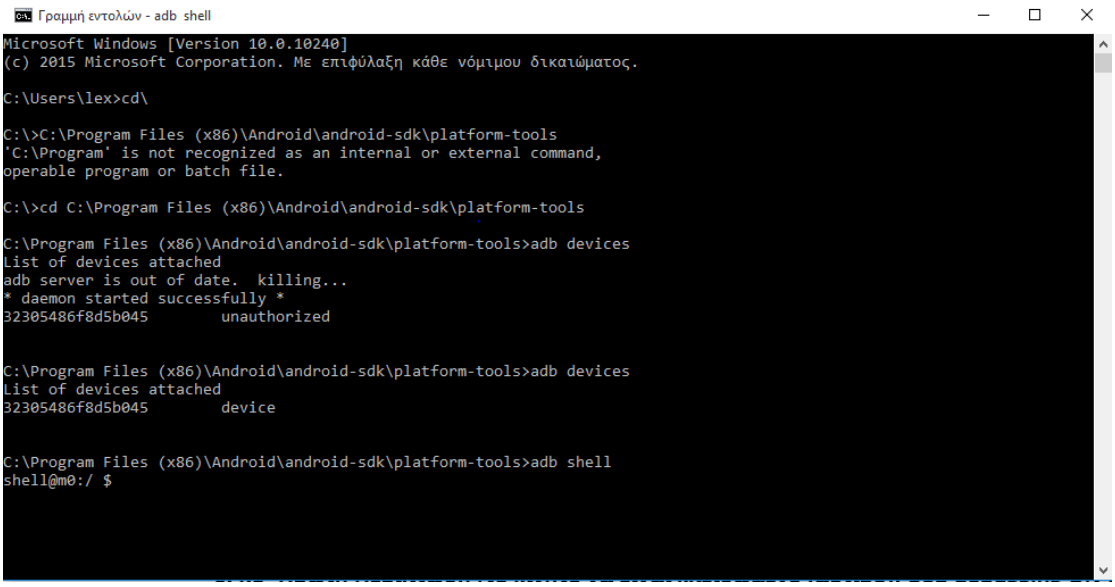


Εικόνα 86. Απεικόνιση της εντολής <adb devices>



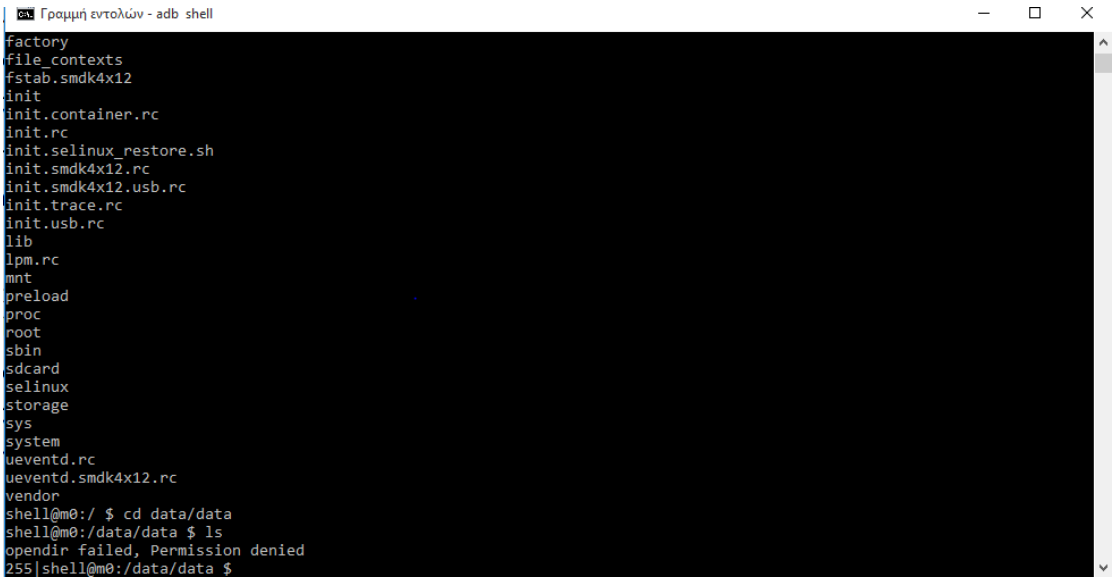
Εικόνα 87. Απεικόνιση των αποτελεσμάτων της εντολής <adb devices>

Σ' αυτό το σημείο τσεκάρουμε εάν υπάρχουν δικαιώματα διαχειριστή με την εντολή <adb shell> και εάν αντί για το σύμβολο $ εμφανίζεται το σύμβολο #, τότε η συσκευή είναι Rooted (βλ. εικόνα 88).



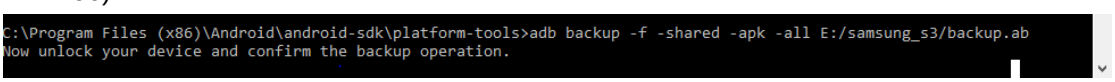
Εικόνα 88. Απεικόνιση των αποτελεσμάτων της εντολής <adb shell>

Ακόμα, μπορούμε να καταλήξουμε στο ίδιο συμπέρασμα και από το γεγονός ότι δεν έχουμε πρόσβαση στο φάκελο: /data/data (βλ. εικόνα 89).



Εικόνα 89. Απεικόνιση των αποτελεσμάτων της εντολής <adb shell>

Γνωρίζοντας, λοιπόν ότι δεν υπάρχουν δικαιώματα διαχειριστή για να μπορέσουμε να προβούμε σε λογική ανάλυση θα πρέπει να εκτελέσουμε την εντολή για αντίγραφα ασφαλείας **<adb backup –f –shared –apk –all E:/samsung_s3/backup.ab >.** Η λειτουργία αυτή προστέθηκε από την Google από την έκδοση Android 4.0 Ice Cream Sandwich και έπειτα (βλ. εικόνα 90).

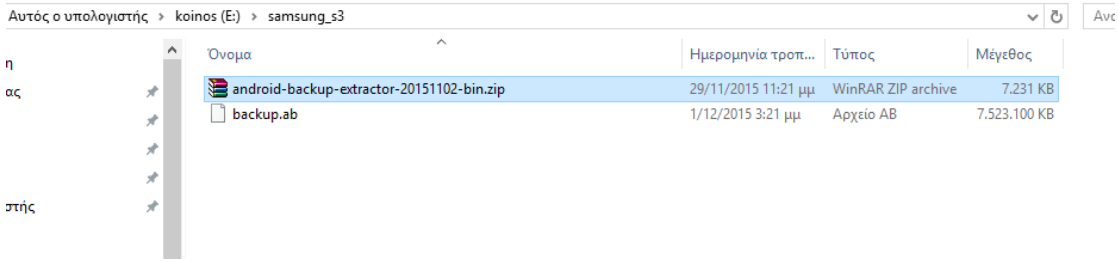


Εικόνα 90. Απεικόνιση των αποτελεσμάτων της εντολής <adb backup>

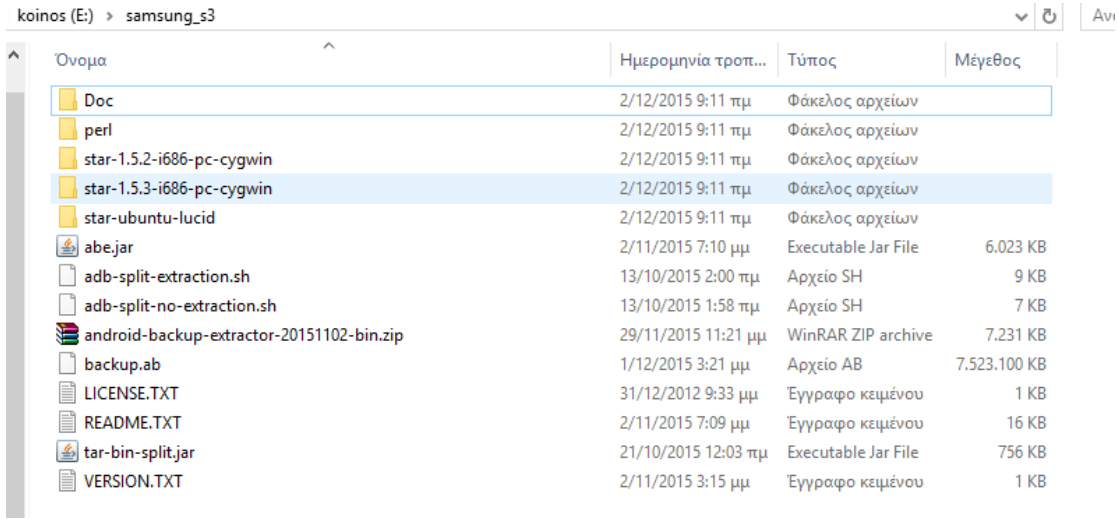
Με αυτό τον τρόπο μπορούν οι χρήστες και οι εξεταστές ψηφιακών πειστηρίων να πάρουν τα δεδομένα από την συσκευή. Όπως ήδη έχουμε τονίσει, δεν χρειάζεται η συσκευή να είναι Root, προκειμένου να αποκτήσουμε πρόσβαση.

6.4.2.1.2 Ανάλυση των δεδομένων από τα αντίγραφα ασφαλείας (Backup)

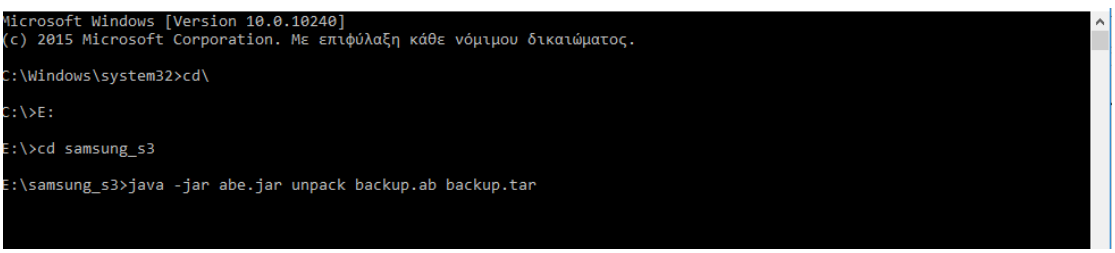
Τα αντίγραφα ασφαλείας αποθηκεύονται σε ένα αρχείο επέκτασης (.ab), το οποίο πραγματικά είναι ένα αρχείο (.tar), που έχει συμπιεστεί. Υπάρχουν αρκετά εργαλεία που μπορούν να διαβάσουν αυτό το αρχείο. Αυτό που θα χρησιμοποιήσουμε εμείς θα είναι το Android Backup Extractor (http://sourceforge.net/projects/adbextractor/). Για να το χρησιμοποιήσουμε θα πρέπει απλά να κάνουμε εξαγωγή των αρχείων του εργαλείου στο ίδιο φάκελο που έχουμε και το backup.ab αρχείο. Έπειτα, τρέχουμε την εντολή <java -jar abe.jar unpack backup.ab backup.tar> (βλ. εικόνες 91 έως 94).



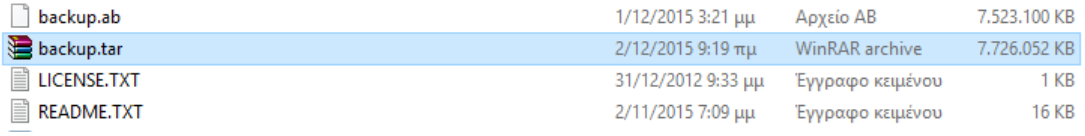
Εικόνα 91. Απεικόνιση των αποτελεσμάτων της εντολής < Android Backup Extractor >



Εικόνα 92. Απεικόνιση των αποτελεσμάτων της εντολής < Android Backup Extractor >

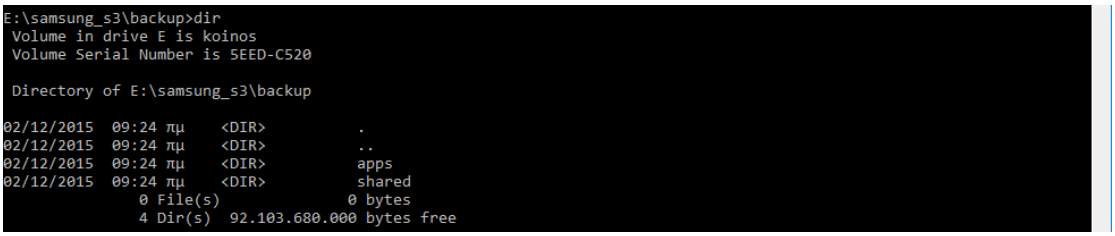


Εικόνα 93. Απεικόνιση των αποτελεσμάτων της εντολής < Android Backup Extractor >



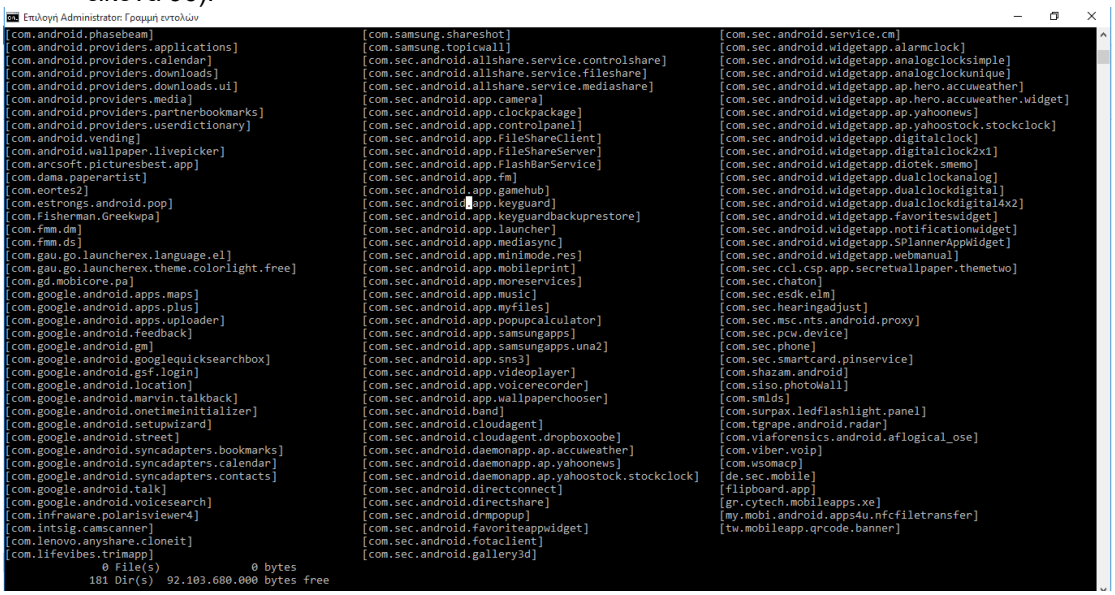
Εικόνα 94. Απεικόνιση των αποτελεσμάτων της εντολής < Android Backup Extractor >

Στη συνέχεια, κάνοντας εξαγωγή το αρχείο backup.tar, βλέπουμε ότι έχουν δημιουργηθεί δύο (2) φάκελοι (apps & shared) (βλ. εικόνα 95).



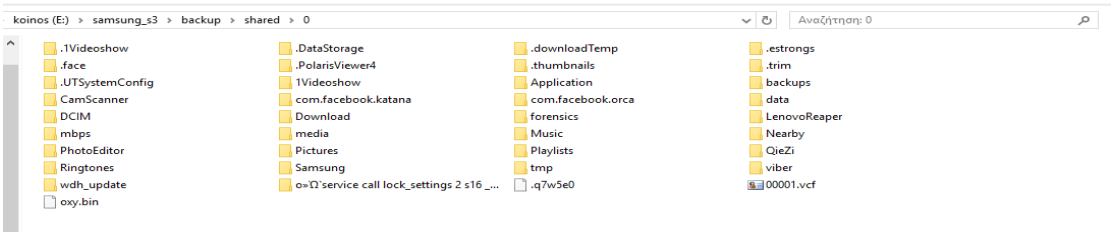
Εικόνα 95. Απεικόνιση των αποτελεσμάτων της εντολής < Android Backup Extractor >

- apps: Αυτός ο φάκελος περιέχει τα δεδομένα από την διαδρομή: /data/data, όπου βρίσκονται οι εγκατεστημένες εφαρμογές (εδώ θα πρέπει να πούμε ότι δεν είχαμε πρόσβαση αρχικά μέσω του adb shell, καθόσον δεν είχαμε δικαιώματα διαχειριστή) (βλ. εικόνα 96).



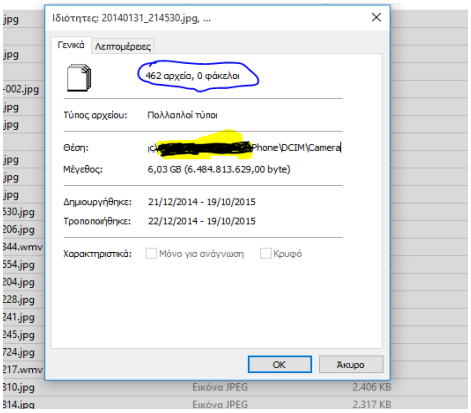
Εικόνα 96. Απεικόνιση των αποτελεσμάτων της εντολής < Android Backup Extractor >

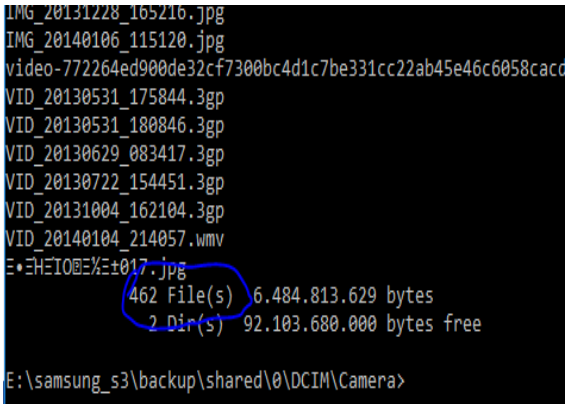
- shared: Αυτός ο φάκελος περιέχει όλα τα δεδομένα της μνήμης (όπως τα βλέπουμε και όταν η συσκευή συνδέεται στο Η/Υ) (βλ. εικόνα 97).



Εικόνα 97. Απεικόνιση των αποτελεσμάτων της εντολής < Android Backup Extractor >

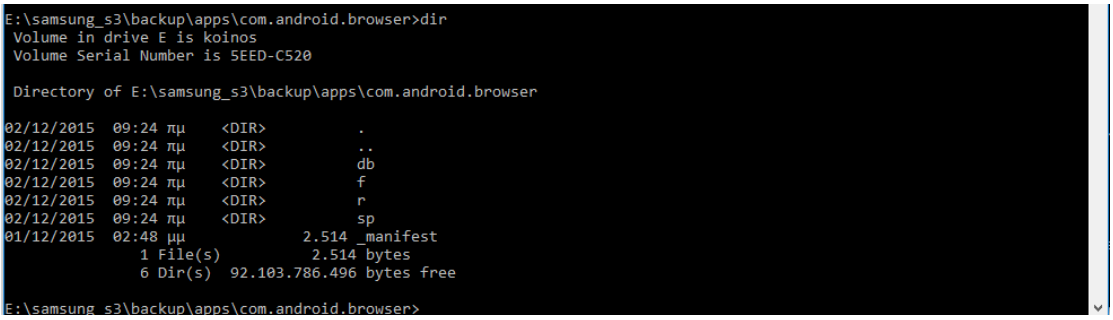
Για παράδειγμα, εδώ μπορούμε να συγκρίνουμε τον αριθμό των φωτογραφιών που είναι τραβηγμένες από την κάμερα και βρίσκονται στη λογική διαδρομή (path): Root\...\DCIM\Camera, όταν συνδέεται το τηλέφωνο με τα δεδομένα που πήραμε από το backup (βλ. εικόνες 98 & 99).





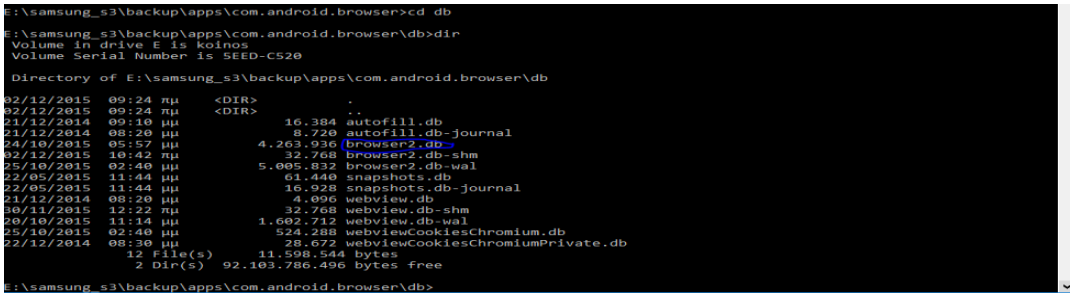
Εικόνες 98 & 99. Απεικόνιση των αποτελεσμάτων

Τώρα, όσον αφορά τα δεδομένα από τις εφαρμογές, θα μπορούσαμε να δείξουμε για μια συγκεκριμένη εφαρμογή πως μπορεί να γίνει η χειροκίνητη ανάλυση. Για παράδειγμα, εάν θελήσουμε να δούμε το ιστορικό περιήγησης (history) του προεγκατεστημένου φυλλομετρητή (default android browser), τότε θα μεταβούμε στο στη διαδρομή (path): Root\..\apps\com.android.browser (βλ. εικόνα 100).



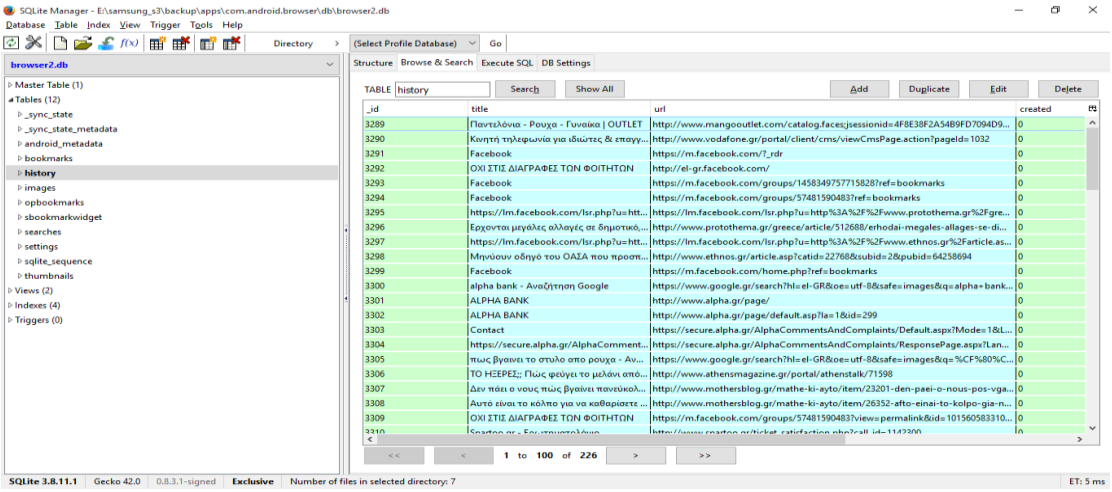
Εικόνα 100. Απεικόνιση του φακέλου μιας εφαρμογής

Εδώ, βλέπουμε την κλασική δομή των αρχείων μιας εφαρμογής Android. Μπαίνοντας στον φάκελο <db>, βλέπουμε την εξής διάρθρωση (βλ. εικόνα 101):



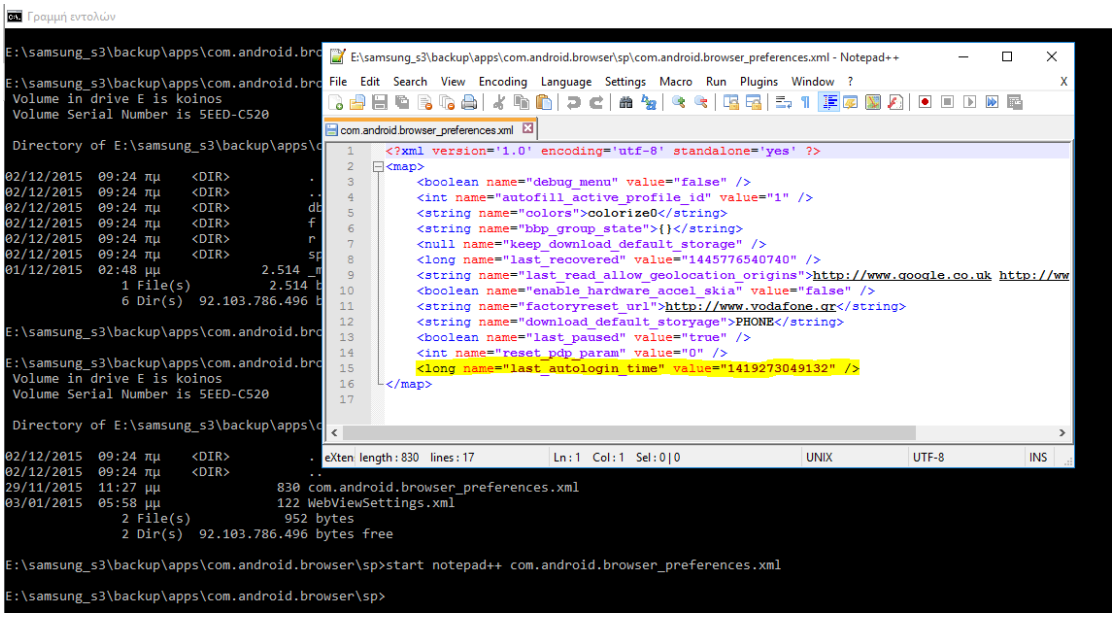
Εικόνα 101. Απεικόνιση του φακέλου db

Με έναν κλασικό viewer βάσεων δεδομένων (στην περίπτωση μας χρησιμοποιούμε τον SQLite Manager, ανοίγουμε το αρχείο που έχουμε μαρκάρει παραπάνω, δηλ. το browser2.db και βλέπουμε το ιστορικό περιήγησης του χρήστη στο διαδίκτυο (βλ. εικόνα 102).



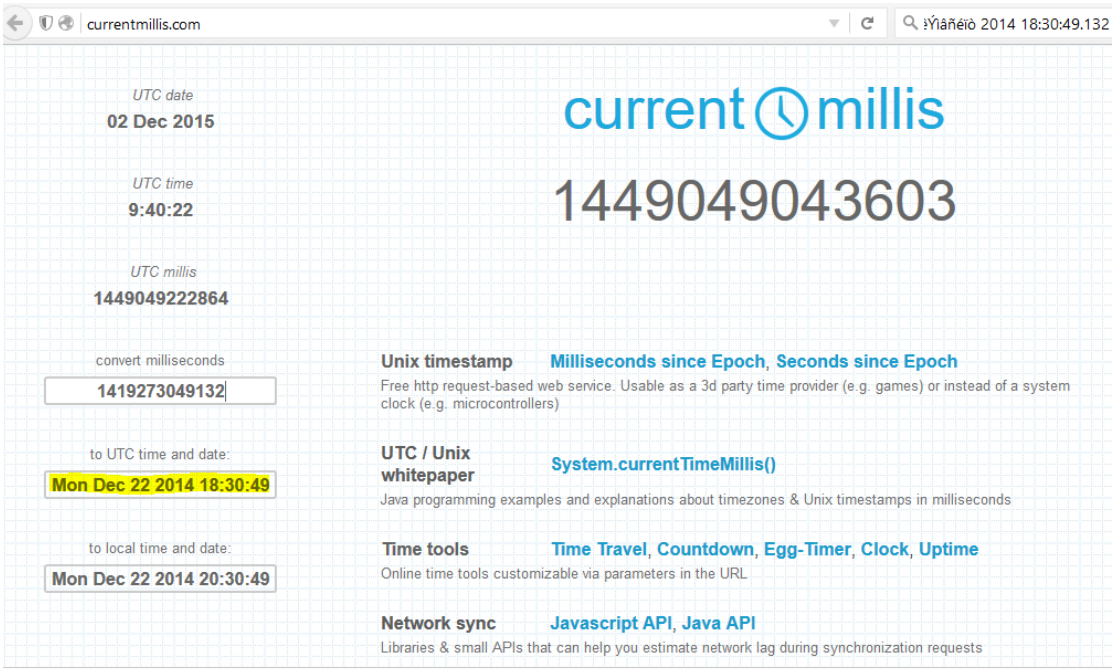
Εικόνα 102. Απεικόνιση της βάσης db

Επιπρόσθετα, κοιτάζοντας το αρχείο xml preferences, μπορούμε να δούμε, για παράδειγμα, την τελευταία ημεροχρονολογία που έγινε είσοδος (login) (βλ. εικόνα 103).



Εικόνα 103. Απεικόνιση της ημέρας που έγινε τελευταία φορά είσοδος

Εδώ θα πρέπει να γίνει μετατροπή της τιμής αυτής σε αναγνωρίσιμη. Υπάρχουν πολλά ελεύθερα εργαλεία, εμείς όμως, θα χρησιμοποιήσουμε ένα online (http://currentmillis.com/) (βλ. εικόνα 104).



Εικόνα 104. Απεικόνιση της μετατροπής της τιμής

Αντίστοιχα, για οποιαδήποτε άλλη εφαρμογή (application) μπορεί να γίνει αυτή η διαδικασία και να πάρουμε τα επιθυμητά αποτελέσματα.

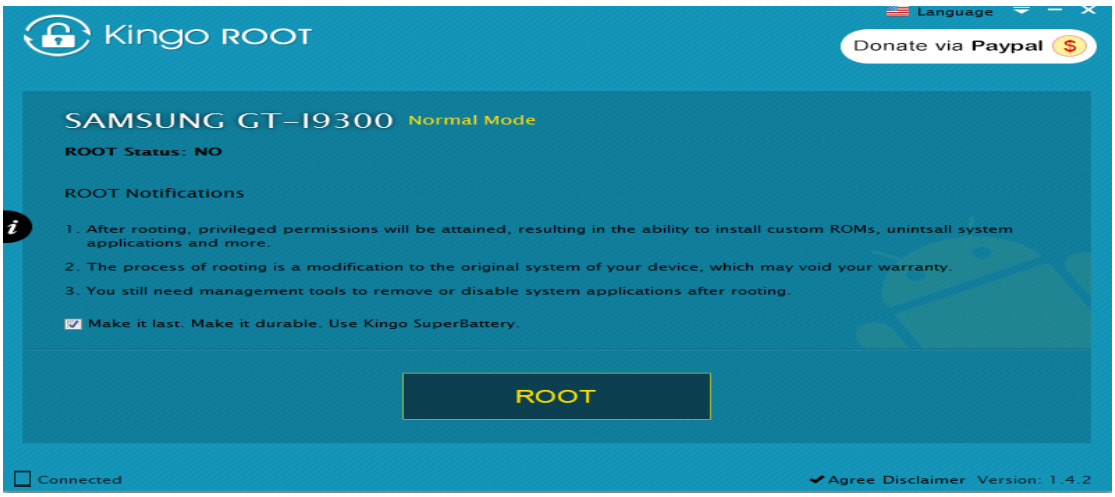
6.4.2.2 Φυσική Εξαγωγή (physical Extraction) και Ανάλυση των δεδομένων με το εργαλείο Autopsy

6.4.2.2.1 Φυσική Εξαγωγή (physical Extraction)

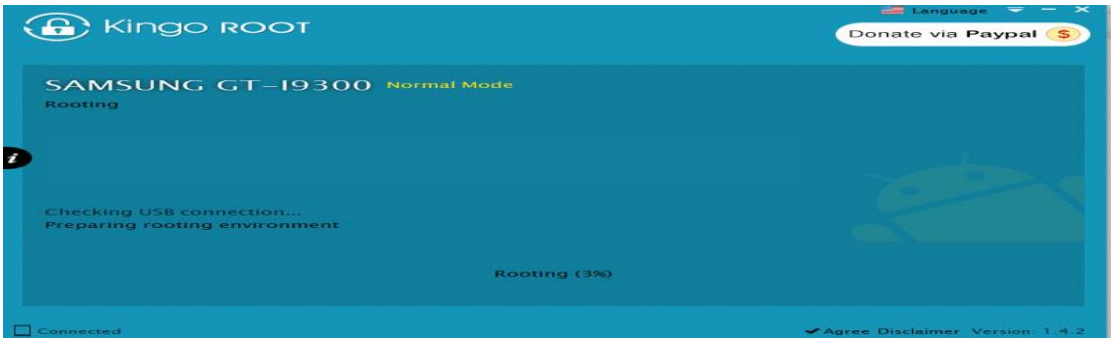
Εφαρμόζοντας την διαδικασία που περιγράφουμε παραπάνω (βλ. παρ. 5.2.5.1.4), εγκαθιστούμε το λογισμικό Kingo Root (https://www.kingoapp.com/) στο Η/Υ που κάνουμε την εξέταση.

Εικόνα 105. Απεικόνιση του λογισμικού Kingo Root

Στη συνέχεια, συνδέουμε τη συσκευή μας και τρέχουμε το συγκεκριμένο λογισμικό (βλ. εικόνα 105 & 106) και περιμένουμε να δούμε τα αποτελέσματα. Παρόλο που το εν λόγω εργαλείο αναφέρει ότι μπορεί να κάνει root την συσκευής μας, αυτό δεν ήταν εφικτό, καθόσον ήταν κλειδωμένο το Bootloader.

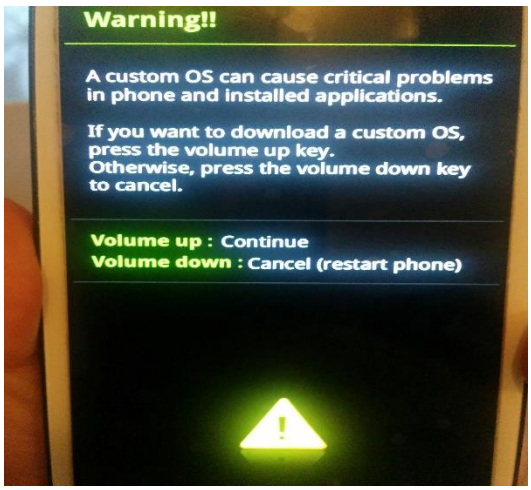


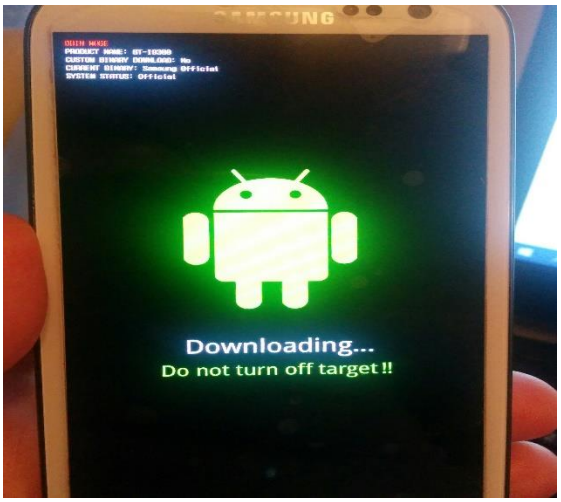
Εικόνα 106. Απεικόνιση του λογισμικού Kingo Root – Διαδικασία Root



Εικόνα 107. Απεικόνιση του λογισμικού Kingo Root – Διαδικασία Root

Προκειμένου να μπορέσουμε να κάνουμε Root τη συσκευή και να παρακάμψουμε το κλειδωμένο Bootloader, θα προσπαθήσουμε να περάσουμε μια custom recovery image. Στην περίπτωση μας θα χρησιμοποιήσουμε την Clockworkmod (6.0.4.7). Για να μπορέσουμε να την εγκαταστήσουμε στη συσκευή, πατάμε ταυτόχρονα τα εξής κουμπιά (power + volume down + home menu), προκειμένου να μπούμε σε κατάσταση download mode (βλ. εικόνες 108 & 109).

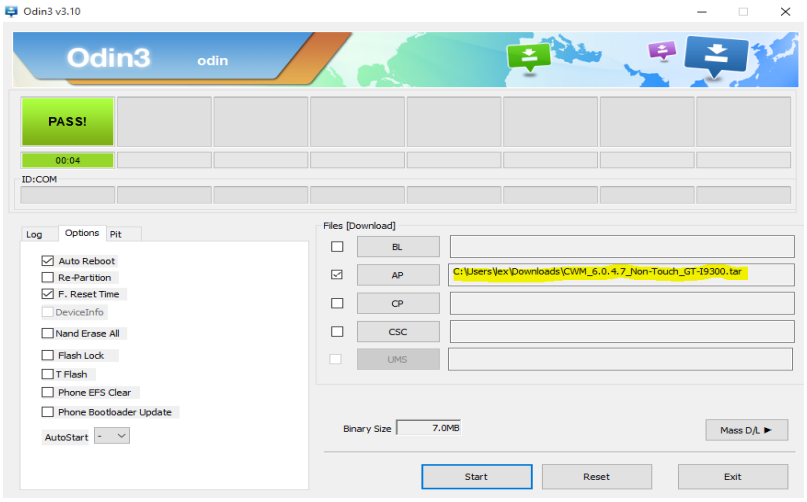




Εικόνες 108 & 109. Απεικόνιση της συσκευής σε κατάσταση download mode

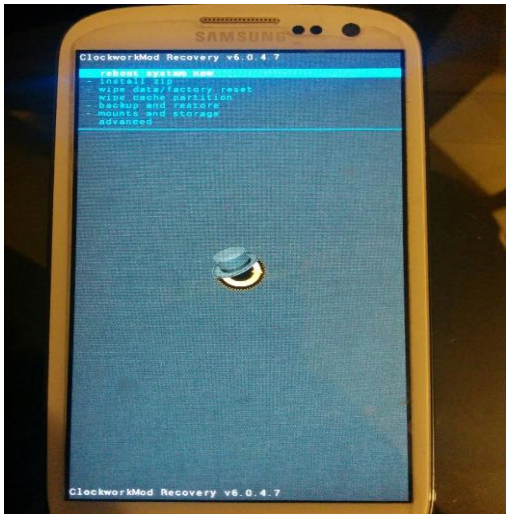
Στην συνέχεια, αφού κατεβάσουμε το λογισμικό Odin3 και συγκεκριμένα την έκδοση 3.10 από την ιστοσελίδα (http://odindownload.com/), το τρέχουμε. Συνδέουμε την συσκευή και

επιλέγουμε στο μενού του Odin την επιλογή AP, όπου εισάγουμε την custom recovery image του Clockworkmod (βλ. εικόνα 110).



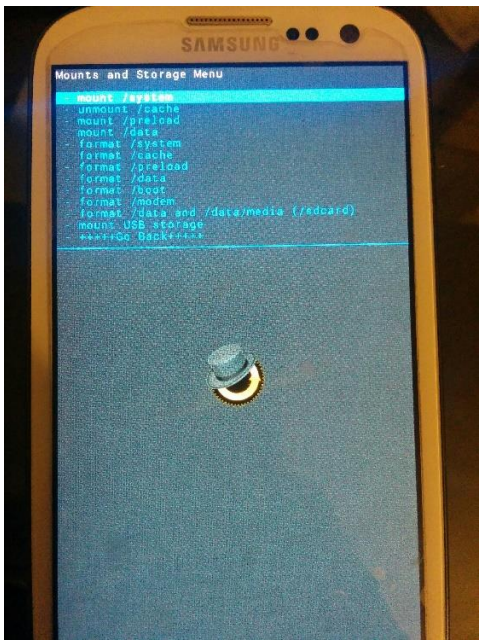
Εικόνα 110. Απεικόνιση του εργαλείου Odin

Προκειμένου να ελέγξουμε εάν έγινε επιτυχής εγκατάσταση της recovery image, κάνουμε επανεκκίνηση την συσκευή μας και πατάμε τα ταυτόχρονα τα κουμπιά (power + volume up + home menu), προκειμένου να μπούμε σε recovery mode και περιμένοντας να δούμε την custom αντί της προεγκατεστημένης (βλ. εικόνα 111).



Εικόνα 111. Απεικόνιση της custom recovery image (ClockworkMod Recovery v.6.0.4.7)

Ακολούθως, μέσω του ως άνω menu επιλέγουμε το /mount and storage και στη συνέχεια κάνουμε mount το φάκελο /data (βλ. εικόνα 112).



Εικόνα 112. Απεικόνιση της custom recovery image (ClockworkMod Recovery v.6.0..1.2)

Τέλος, επιστρέφουμε στην κονσόλα του Η/Υ και τρέχουμε την εντολή <adb devices> και στη συνέχεια την εντολή <adb shell> (βλ. εικόνα 113).

```
C:\Program Files (x86)\Android\android-sdk\platform-tools>adb devices
List of devices attached
32305486f8d5b045        recovery


C:\Program Files (x86)\Android\android-sdk\platform-tools>adb shell
~ #
```

Εικόνα 113. Απεικόνιση των αποτελεσμάτων της εντολών < adb devices & adb shell>

Εδώ, παρατηρούμε ότι αποκτήσαμε δικαιώματα Root και μπορούμε πια να πλοηγηθούμε στο φάκελο /data/data, πράγμα που ήταν αδύνατο προηγουμένως (βλ. εικόνα 114).

```
/data/data # ls |more
android.googleSearch.googleSearchWidget
com.Fisherman.Greekwpa
com.accaci
com.aegean.android
com.android.apps.tag
com.android.backupconfirm
com.android.bluetooth
com.android.browser
com.android.calendar
com.android.certinstaller
com.android.chrome
com.android.contacts
com.android.defcontainer
com.android.dreams.basic
com.android.dreams.phototable
com.android.email
com.android.exchange
com.android.facelock
com.android.htmlviewer
com.android.inputdevices
com.android.keychain
com.android.location.fused
com.android.mms
--More--
```

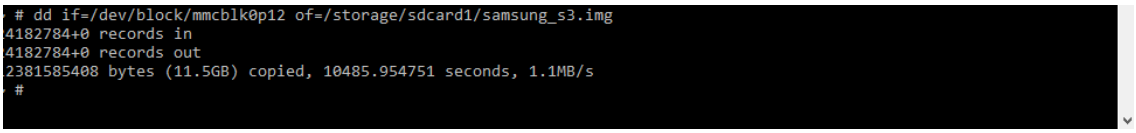
Εικόνα 114. Απεικόνιση της διαδρομής </data/data>

Στη συνέχεια, τρέχουμε την εντολή <cat /proc/partitions>, προκειμένου να εντοπίσουμε το κατάλληλο διαμέρισμα (partition) που θέλουμε να κάνουμε εγκληματολογικό αντίγραφο (image) (βλ. εικόνα 115). Εδώ, παρατηρούμε ότι εάν θέλουμε να πάρουμε αντίγραφο από όλη την μνήμη

της συσκευής πρέπει να επιλέξουμε το πρώτο διαμέρισμα:0 (mmcblk0). Γνωρίζοντας όμως, ότι τα λοιπά διαμερίσματα δεν παρουσιάζουν εγκληματολογικό ενδιαφέρον, επιλέγουμε να πάρουμε αντίγραφο μόνο από το διαμέρισμα που περιέχει τα δεδομένα του χρήστη της συσκευής (user data). Αυτό το διαμέρισμα είναι το 12 (mmcblk12).

Εικόνα 115. Απεικόνιση της διαδρομής </data/data>

Ακολούθως, βάζουμε μία (1) εξωτερική κάρτα (sd), προκειμένου να γράψουμε το εγκληματολογικό αντίγραφο, τρέχοντας την εντολή <dd if=/dev/block/mmcblk0p12 of=/storage/sdcard1/samsung_s3.img. Εδώ, πρέπει να τονιστεί ότι η κάρτα πρέπει να είναι διαμορφωμένη σε σύστημα αρχείων exFat και όχι σε Fat32, προκειμένου να πάρουμε όλο το αντίγραφο, έχοντας υπόψη ότι υπάρχει ο περιορισμός στο Fat32 (4GB).

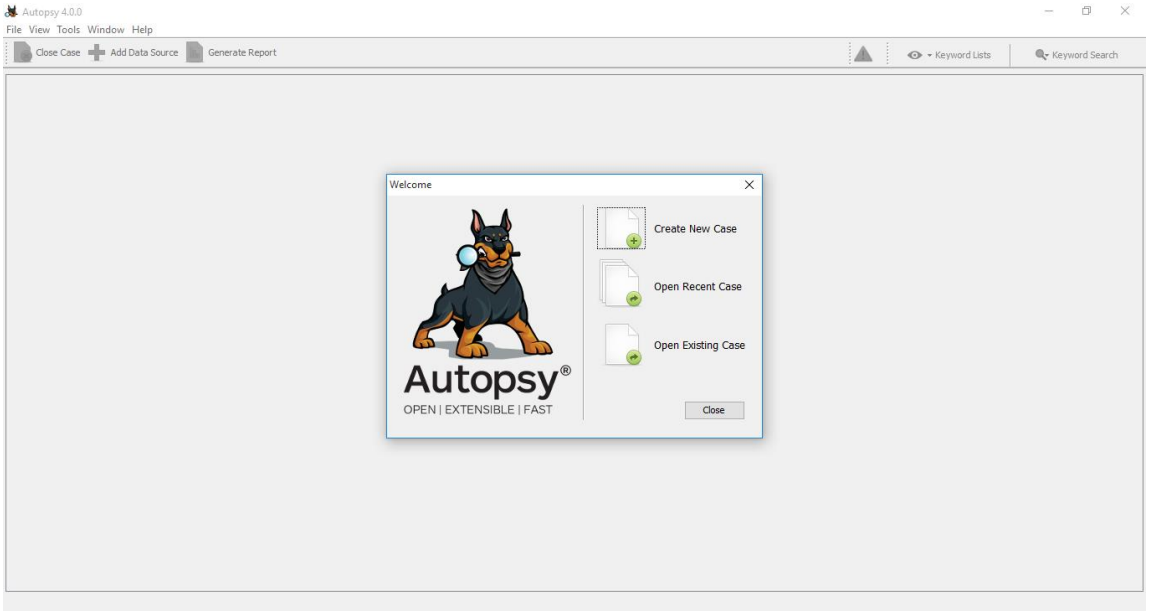


Εικόνα 116. Απεικόνιση της εντολής για απόκτηση εγκληματολογικού αντιγράφου

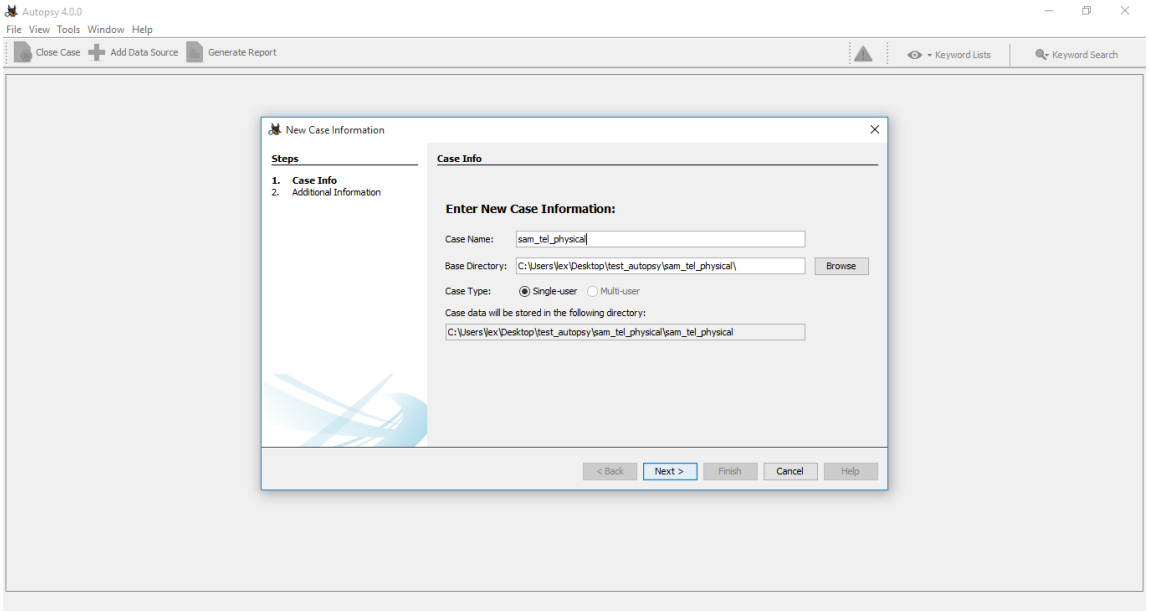
6.4.2.2.2 Ανάλυση των δεδομένων με το εργαλείο Autopsy

Το αρχείο που δημιουργείται από την διαδικασία της φυσικής εξαγωγής μπορεί να αναλυθεί είτε χειροκίνητα όπως δείξαμε προηγουμένως είτε με οποιοδήποτε εμπορικό λογισμικό κινητών (Cellebrite, Oxygen, Xry, Encase, Ftk, κ.α.) είτε ελεύθερου όπως του Autopsy και του FTK Imager. Στην περίπτωση μας, θα χρησιμοποιήσουμε το εργαλείο Autopsy, το οποίο εκτός από Η/Υ, χρησιμοποιείται με τις νέες δυνατότητες του και για ανάλυση συσκευών Android. Το εν λόγω εργαλείο προσφέρεται δωρεάν (http://sleuthkit.org/autopsy) και μπορεί κάποιος να το εγκαταστήσει σε Windows, Linux και OS X περιβάλλον.

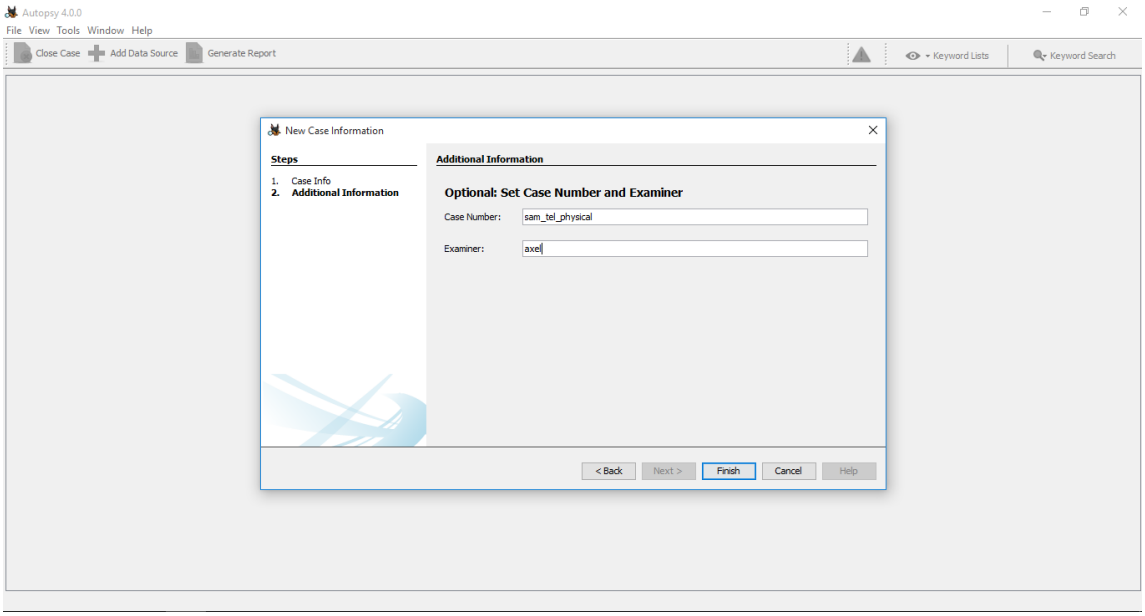
Εγκαθιστώντας αυτό (έκδοση Autopsy 4.0.0) στο περιβάλλον εργασίας μας, ξεκινάμε την διαδικασία ανάλυσης του εγκληματολογικού αντιγράφου μας. Ανοίγουμε το εργαλείο και ακολουθούμε τον οδηγό που μας εμφανίζει (βλ. Εικόνες 117 έως 121).



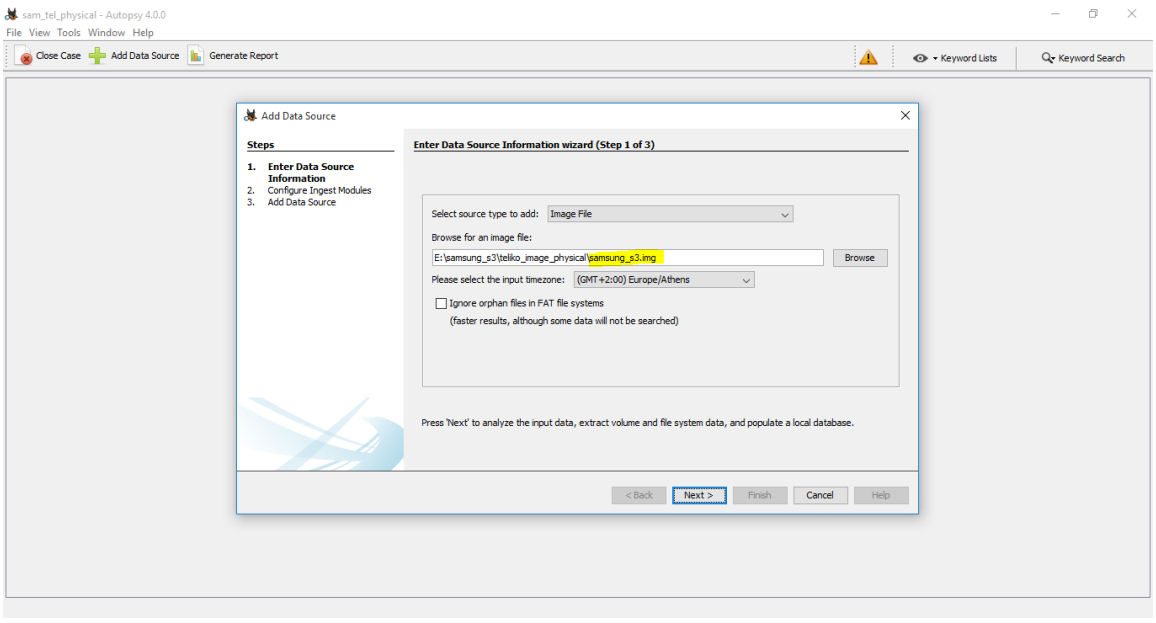
Εικόνα 117. Απεικόνιση της έναρξης του εργαλείου Autopsy



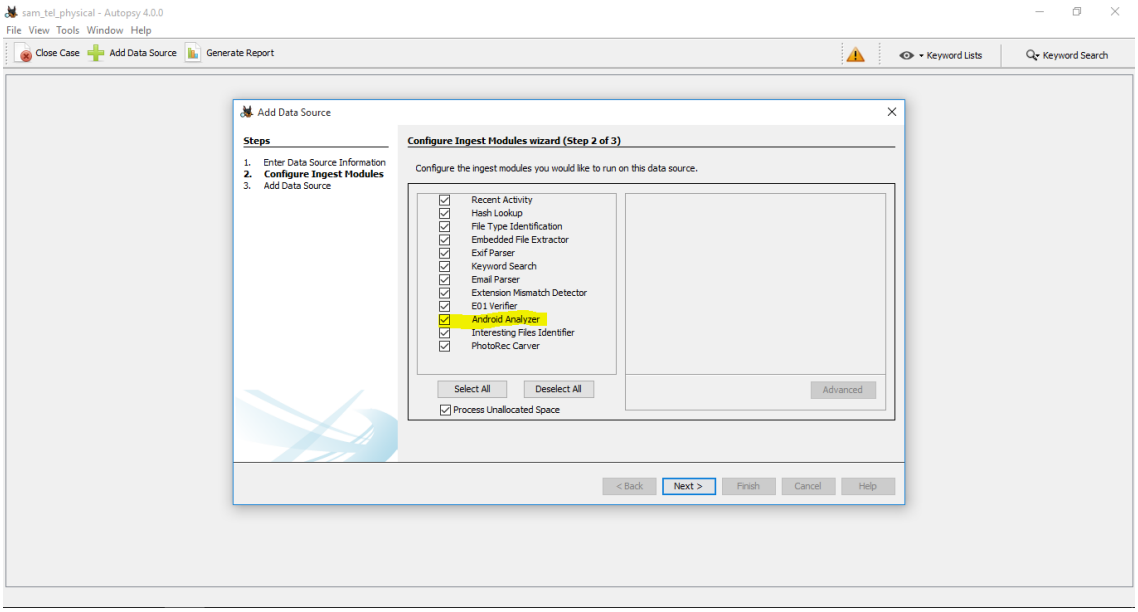
Εικόνα 118. Απεικόνιση της έναρξης του εργαλείου Autopsy



Εικόνα 119. Απεικόνιση του εργαλείου Autopsy

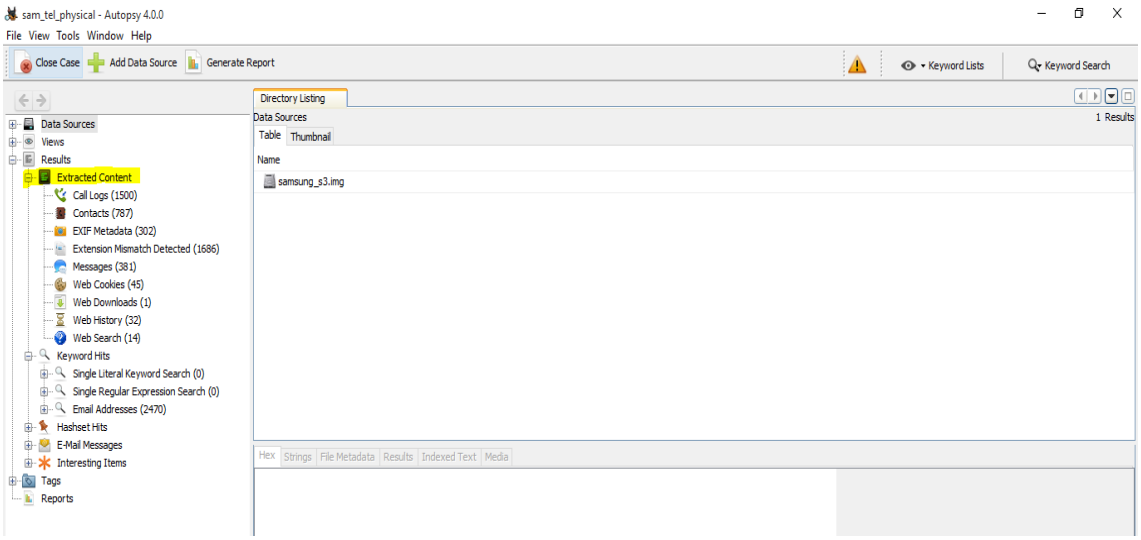


Εικόνα 120. Απεικόνιση του εργαλείου Autopsy (εισαγωγή του αντιγράφου)



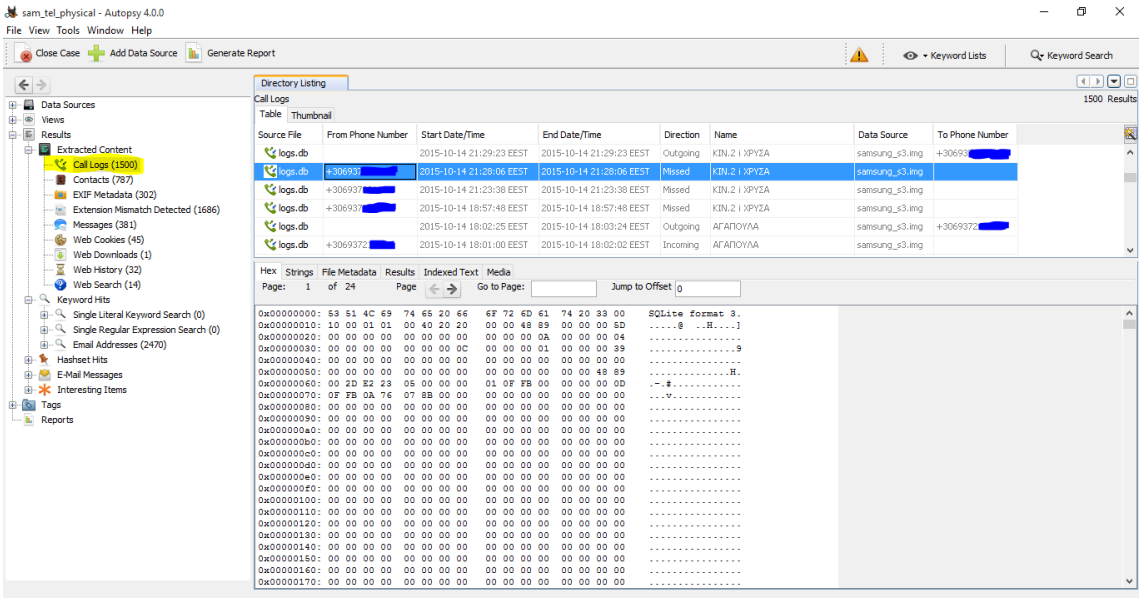
Εικόνα 121. Απεικόνιση του εργαλείου Autopsy (επιλογή αυτοματοποιημένων εργασιών αναζήτησης)

Ακολούθως, βλέπουμε τα αποτελέσματα από την ανάλυση του εγκληματολογικού αντιγράφου της φυσικής εξαγωγής της μνήμης, έχοντας επισημάνει τα αυτοματοποιημένες κατηγορίες από την ανάλυση του Android (βλ. Εικόνα 122).

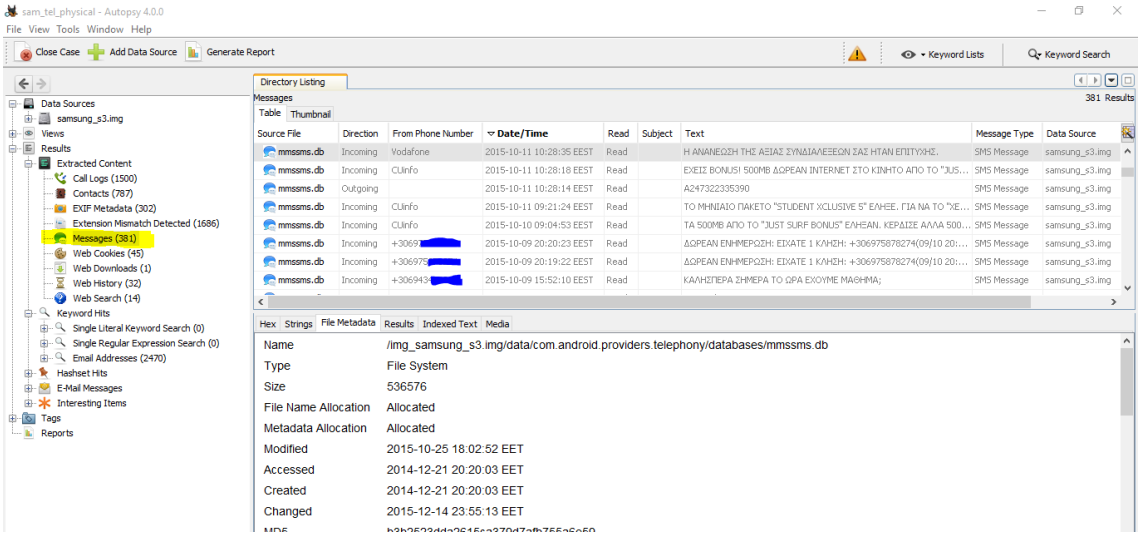


Εικόνα 122. Απεικόνιση του εργαλείου Autopsy (Android Analyzer)

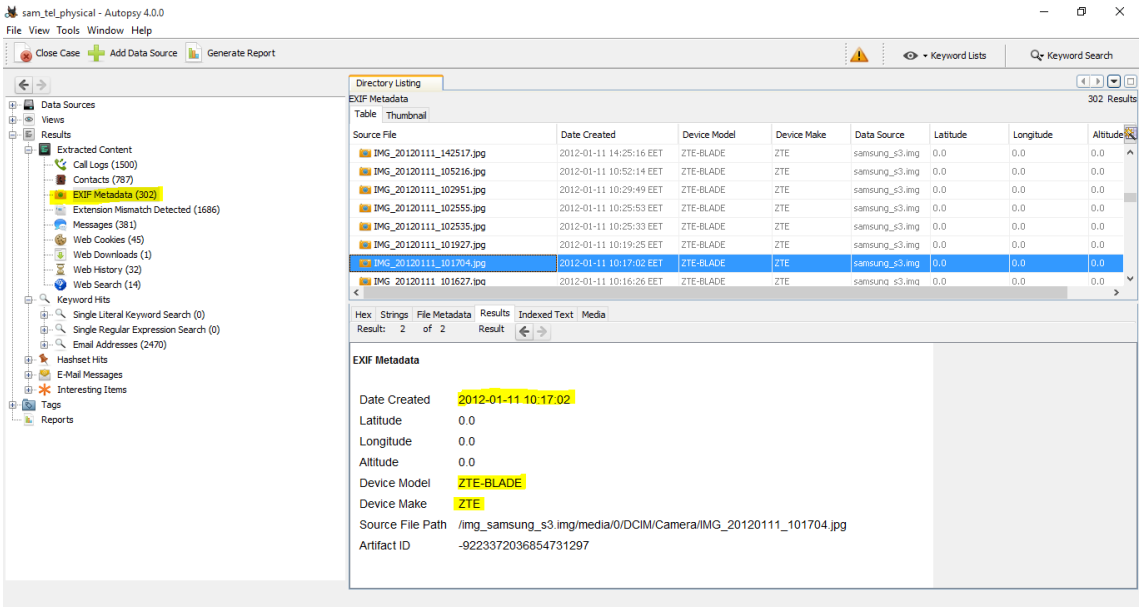
Σ' αυτό το σημείο πρέπει να τονιστεί ότι το εργαλείο Autopsy έχει αυτοματοποιήσει όσον αφορά τις εφαρμογές (applications) της συσκευής μόνο σ' αυτά που βλέπουμε παραπάνω [Κλήσεις (Call logs), Επαφές (contacts), Έξτρα πληροφορίες φωτογραφιών (Exif Metadata), Μηνύματα (Messages) & Πληροφορίες διαδικτύου (Web Cookies, Downloads, History & Search). Για παράδειγμα, κοιτάζοντας επιμέρους κάποιες από αυτές τις κατηγορίες, βλέπουμε πιο αναλυτικά πληροφορίες (βλ. εικόνες 123 έως 126)



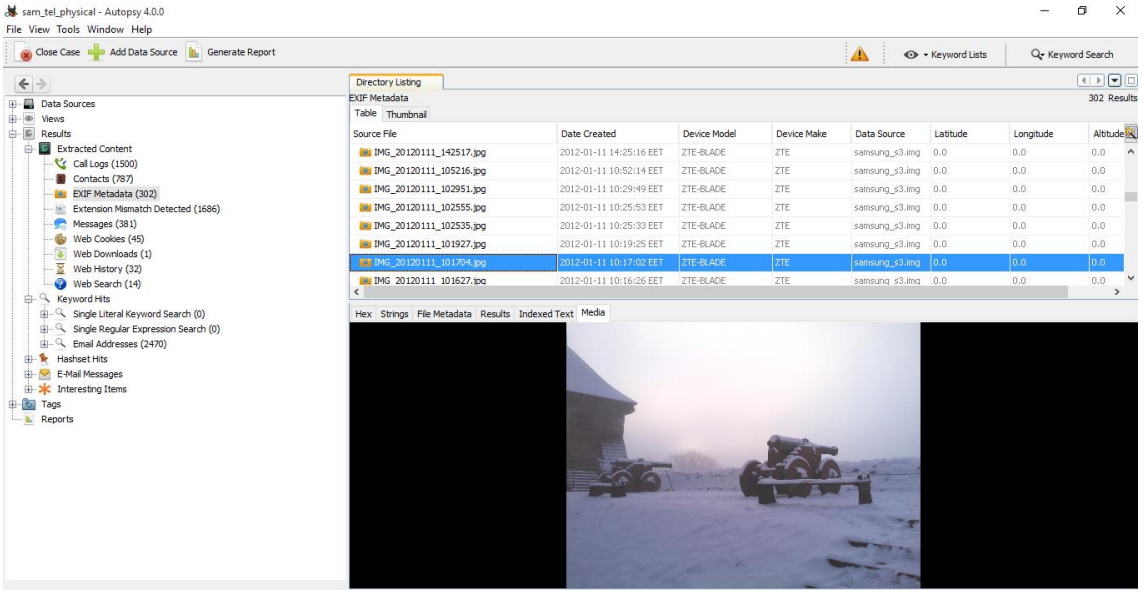
Εικόνα 123. Απεικόνιση του εργαλείου Autopsy (Κατηγορία Κλήσεων)



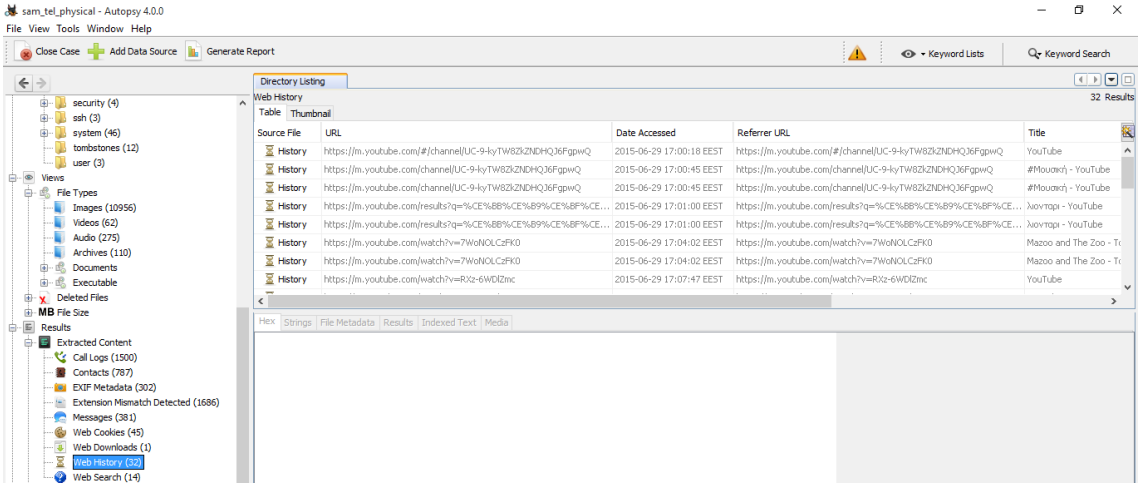
Εικόνα 124. Απεικόνιση του εργαλείου Autopsy (Κατηγορία Μηνυμάτων)



Εικόνα 125. Απεικόνιση του εργαλείου Autopsy (Κατηγορία Exif Metadata)

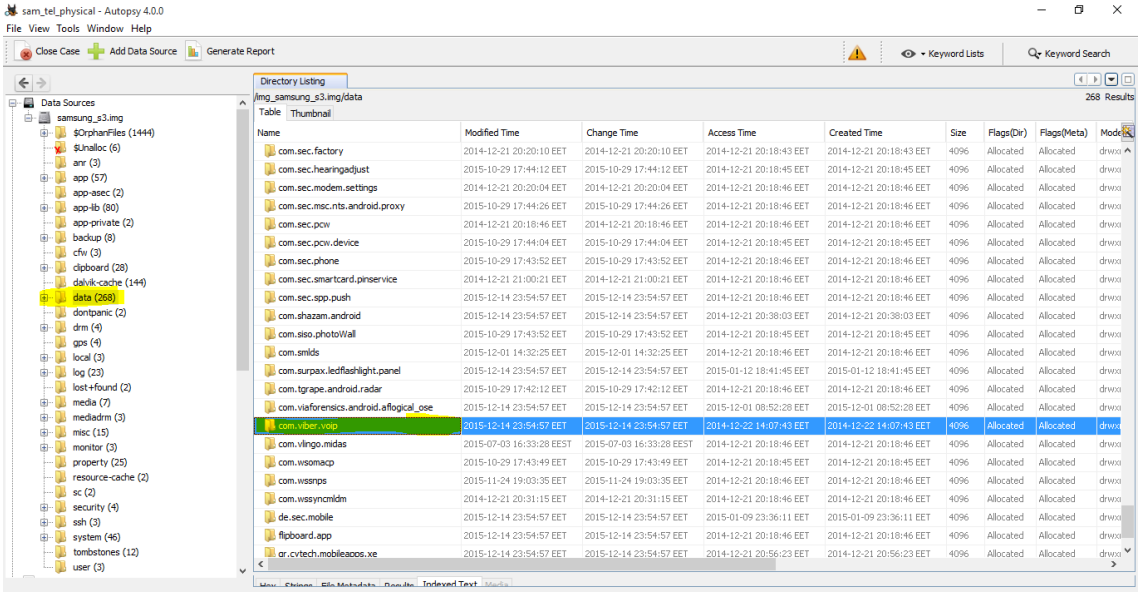


Εικόνα 126. Απεικόνιση του εργαλείου Autopsy (Κατηγορία Exif Metadata)

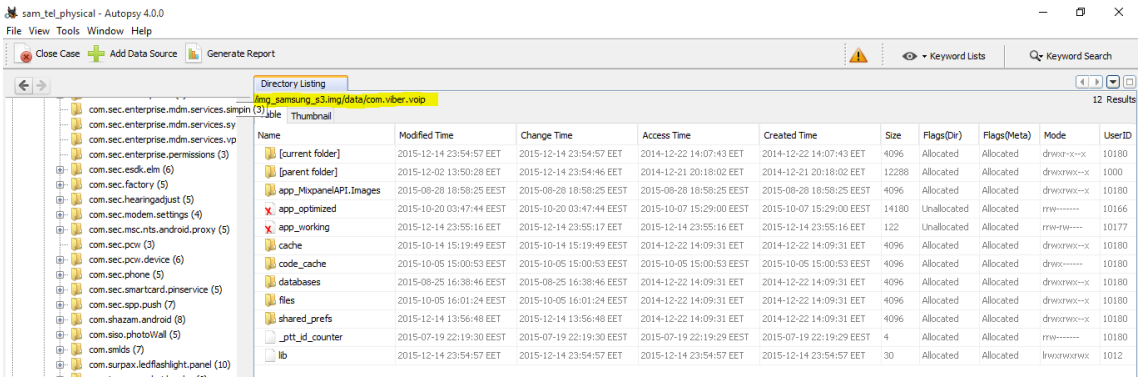


Εικόνα 126. Απεικόνιση του εργαλείου Autopsy (Κατηγορία Ιστορικό Διαδικτύου)

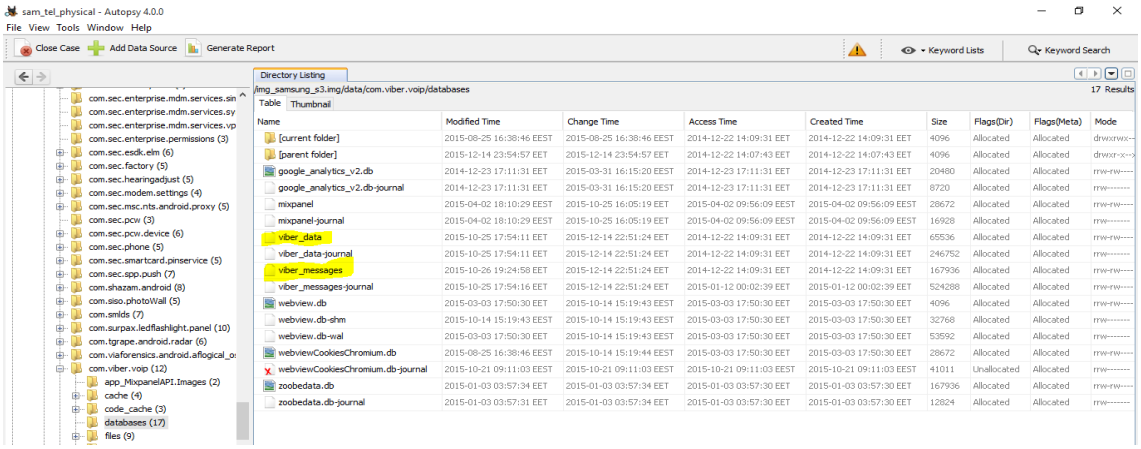
Ακόμα, στις περιπτώσεις που θέλουμε να αναζητήσουμε περαιτέρω πληροφορίες για κάποιες συγκεκριμένες εφαρμογές όπως (viber, whatsup, facebook, κ.α.), θα πρέπει να πλοηγηθούμε στο αντίστοιχο φάκελο και αφού κάνουμε εξαγωγή, να προβούμε σε χειροκίνητη ανάλυση όπως περιγράφουμε στην παράγραφο 6.4.2.1.2. Στην συνέχεια ακολουθούν απεικονίσεις από την διαδικασία ανάλυσης της εφαρμογής Viber (βλ. Εικόνες 127 έως 131).



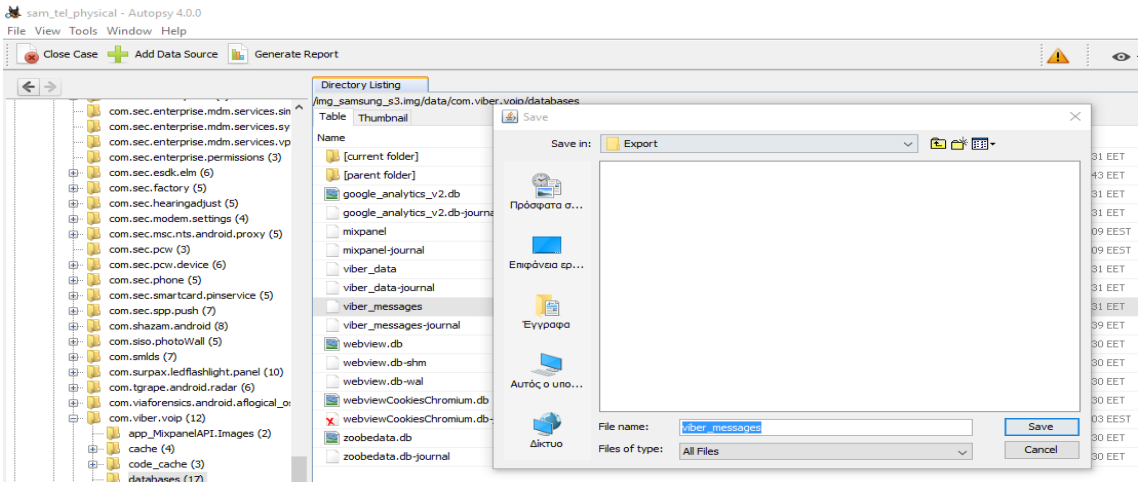
Εικόνα 127. Απεικόνιση του εργαλείου Autopsy (ανάλυση Viber)



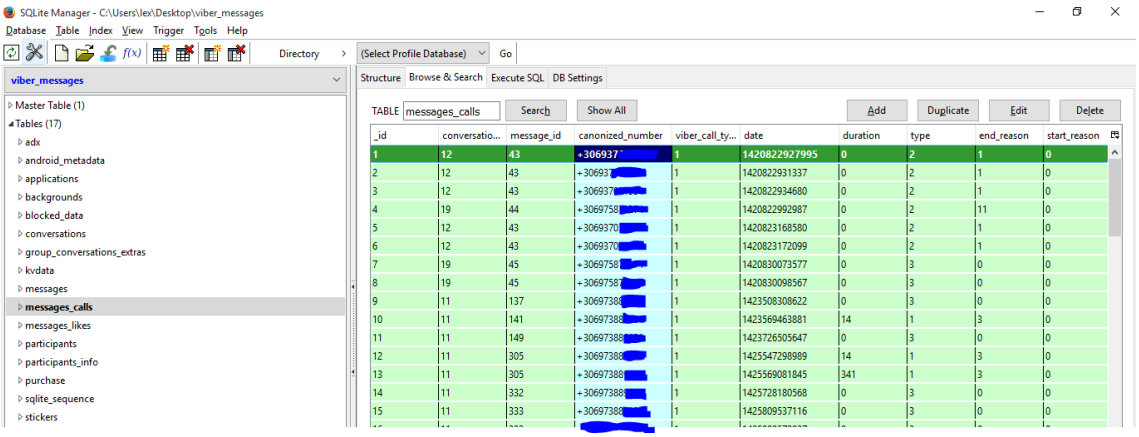
Εικόνα 128. Απεικόνιση του εργαλείου Autopsy (ανάλυση Viber)



Εικόνα 129. Απεικόνιση του εργαλείου Autopsy (ανάλυση Viber)

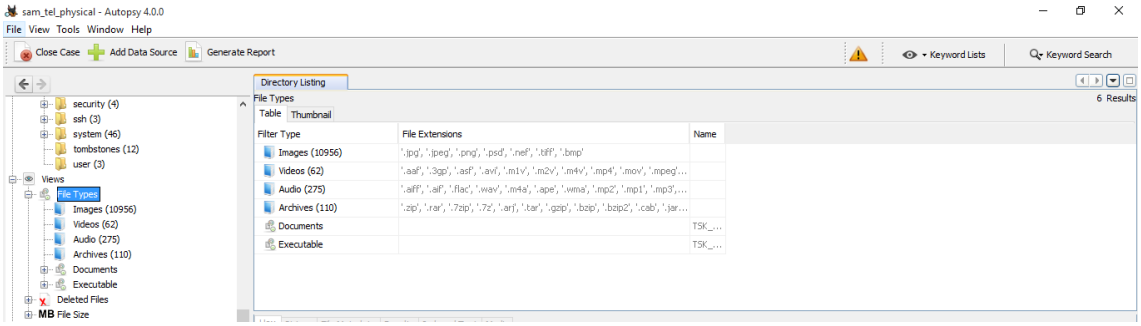


Εικόνα 130. Απεικόνιση του εργαλείου Autopsy (ανάλυση Viber)

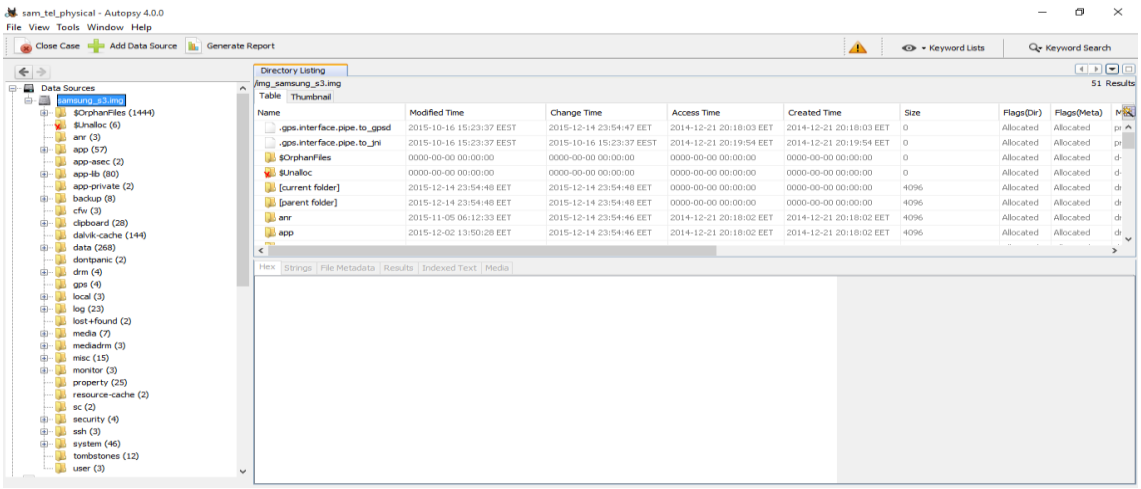


Εικόνα 131. Απεικόνιση του εργαλείου Sql Viewer (ανάλυση Viber)

Τέλος, αξίζει να σημειωθεί ότι μπορούμε να πλοηγηθούμε, να αναζητήσουμε λέξεις κλειδιά, διαγεγραμμένα αρχεία κ.α. (όπως όλα τα λογισμικά ανάλυσης εγκληματολογικών αντιγράφων προσφέρουν) και να πάρουμε χρήσιμες πληροφορίες για την υπόθεση που εξετάζουμε (βλ. εικόνες 132 & 133).



Εικόνα 132. Απεικόνιση του εργαλείου Autopsy



Εικόνα 133. Απεικόνιση του εργαλείου Autopsy

6.4.3 Το κινητό είναι κλειδωμένο & δεν υπάρχουν δικαιώματα διαχειριστή (no root)]

6.4.3.1 Λογική Εξαγωγή (Logical extraction)

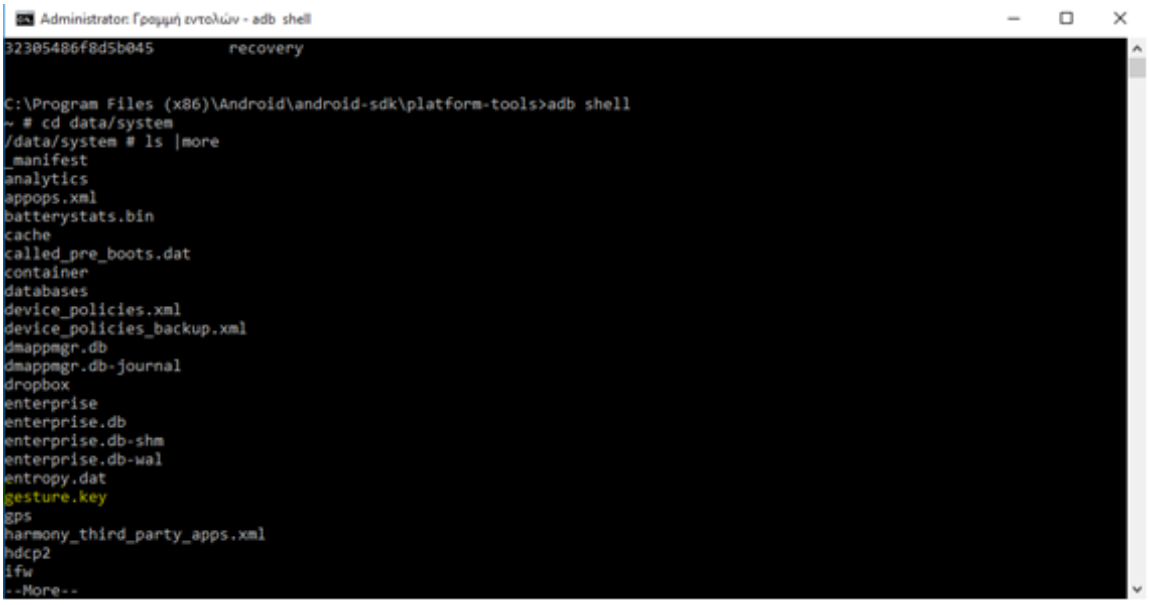
Ακολουθώντας τα βήματα που έχουμε προαναφέρει (βλ. παρ. 5.2.5.1) πλοηγούμαστε στη διαδρομή που βρίσκεται το εργαλείο Adb. Εκεί, τρέχουμε την εντολή <adb devices> και παρατηρούμε ότι δεν αναγνωρίζετε η συσκευή μας καθώς και απαιτείται να γίνει authorized ο H/Y από την συσκευή, πράγμα το οποίο δεν μπορεί να επιτευχθεί καθόσον το κινητό είναι κλειδωμένο. Επομένως, στην εν λόγω περίπτωση δεν μπορούμε να κάνουμε λογική εξαγωγή και ανάλυση της συσκευής.

6.4.3.2 Φυσική Εξαγωγή (Physical extraction)

Ακολουθώντας, τα βήματα της παραγράφου 6.4.2.2, δηλαδή πηγαίνοντας στο Download mode και βάζοντας την διαμορφωμένη έκδοση του clockworkmod (custom recovery image), διαπιστώνουμε ότι οδηγούμαστε στα ίδια αποτελέσματα με πριν και όταν η συσκευή είναι κλειδωμένη και δεν είναι ενεργοποιημένο το Usb Debugging. Επομένως, το να είναι κλειδωμένη η συσκευή μας αποτρέπει μόνο ως προς την λογική και όχι ως προς την φυσική της εξαγωγή.

6.4.3.3 Ξεκλείδωμα της συσκευής μέσω της διαδικασίας της φυσικής εξαγωγής (Physical extraction)

Αρχικά, ακολουθούμε τα βήματα της παραγράφου 6.4.2.2, δηλαδή πηγαίνουμε στο Download mode και βάζουμε την διαμορφωμένη έκδοση του clockworkmod (custom recovery image). Εκεί, μέσω της εντολής <Adb shell>, πλοηγούμαστε στο φάκελο /data/system και εκεί διαγράφουμε το αρχείο: gesture.key, με την εντολή <rm gesture.key> (βλ. εικόνα 134 & 135). Κάνοντας επανεκκίνηση την συσκευή διαπιστώνουμε ότι παραμένει το μοτίβο (pattern), πλην όμως το κινητό ξεκλειδώνει με οποιοδήποτε συνδυασμό.



Εικόνα 133. Απεικόνιση από το φάκελο: /data/system

```
/data/system # ls
_manifest                   hdcp2
analytics                   ifw
appops.xml                  inputmethod
batterystats.bin            locksettings.db
cache                       locksettings.db-shm
called_pre_boots.dat        locksettings.db-wal
container                   ndebugsocket
databases                   netpolicy.xml
device_policies.xml         netstats
device_policies_backup.xml  packages-more-backup.xml
dmappmgr.db                 packages.list
dmappmgr.db-journal         packages.xml
dropbox                     password.key
enterprise                  registered_services
enterprise.db               shared_prefs
enterprise.db-shm           sparepassword.key
enterprise.db-wal           sync
entropy.dat                 uiderrors.txt
gps                         usagestats
harmony_third_party_apps.xml users
/data/system #
```

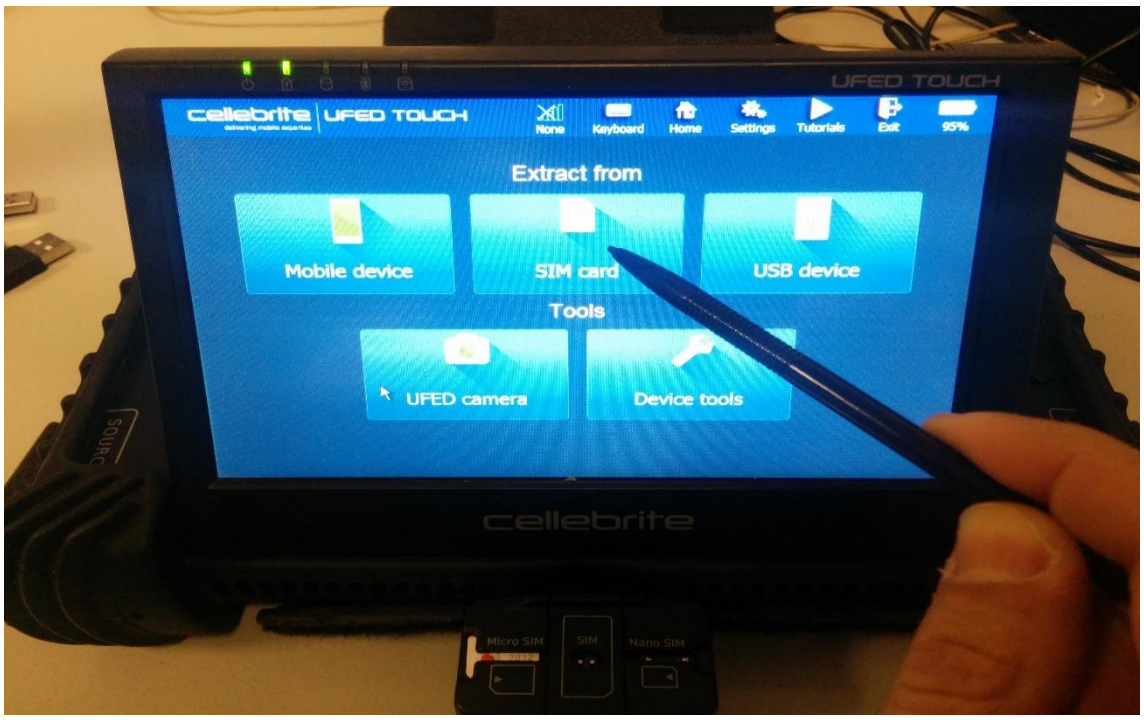
Εικόνα 133. Απεικόνιση από το φάκελο: /data/system μετά από διαγραφή του αρχείου gesture.key

6.5 Εξέταση Κάρτας SIM

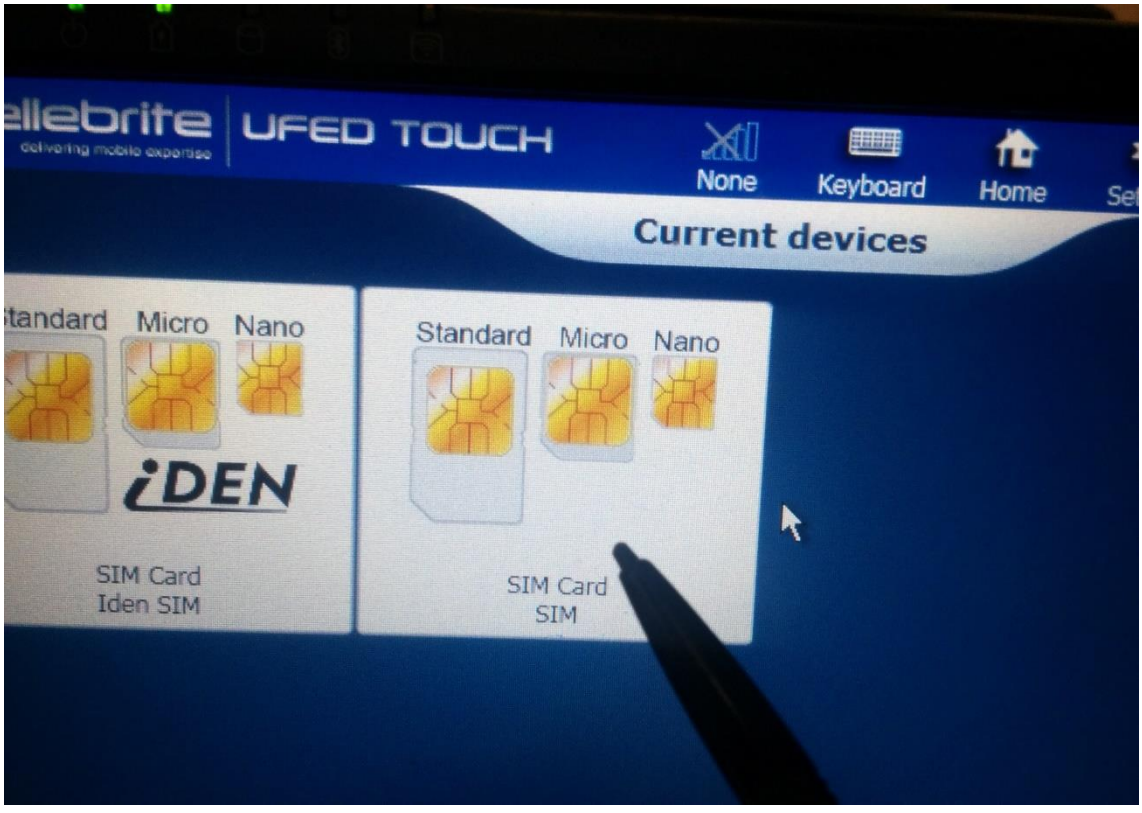
Η εξέταση της κάρτας SIM μπορεί να γίνει είτε με εμπορικό είτε με ελεύθερο εργαλείο. Εδώ, έχουμε επιλέξει το εργαλείο Cellebrite και θα δείξουμε τα βήματα που απαιτούνται για την εξέταση της κάρτας SIM. Αρχικά, αφαιρούμε την κάρτα SIM από την συσκευή και στην συνέχεια, αφού την σημάνουμε και την φωτογραφίσουμε, την βάζοντας στην ειδική θήκη που προσφέρει το εργαλείο Cellebrite (βλ. εικόνες 134 & 135).

Εικόνες 134 & 135. Απεικονίσεις από την κάρτα SIM

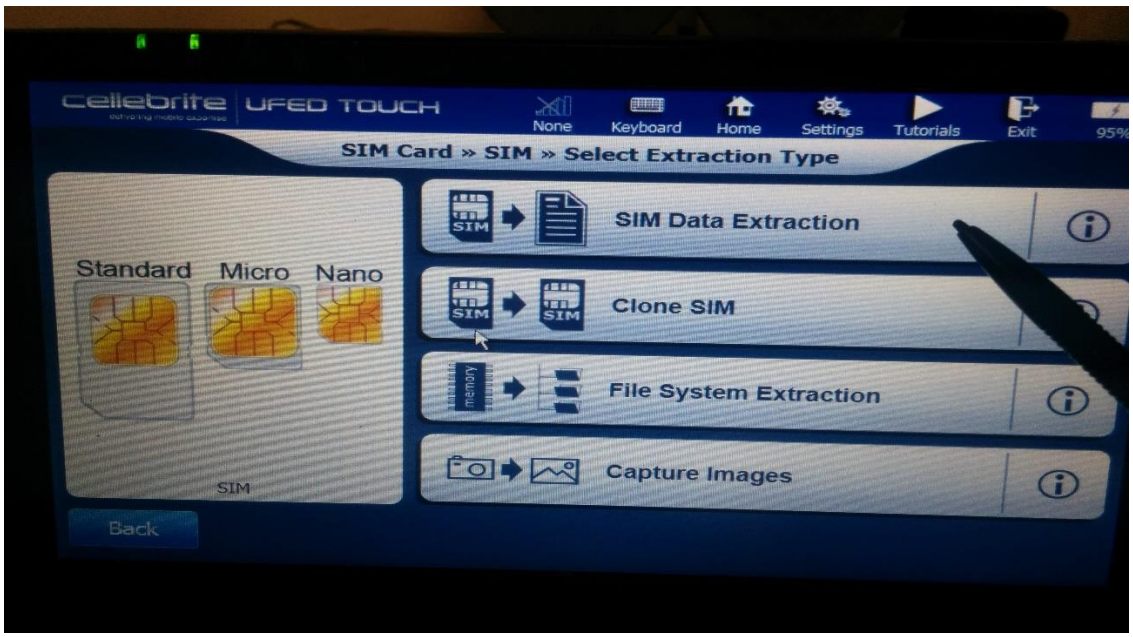
Ακολουθώντας, έπειτα τον οδηγό που προσφέρει το ως άνω εργαλείο παίρνουμε τα στοιχεία της κάρτας SIM (βλ. Εικόνες 136 έως 144).



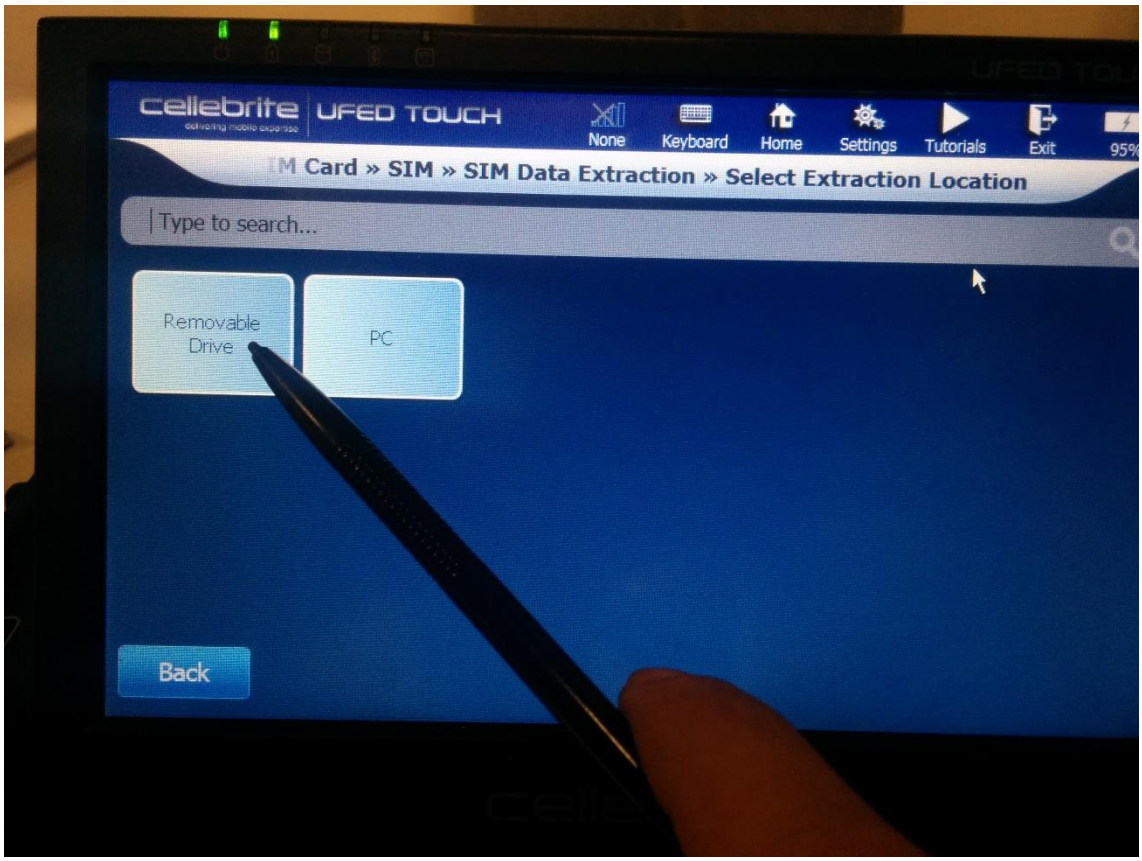
Εικόνα 136. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite



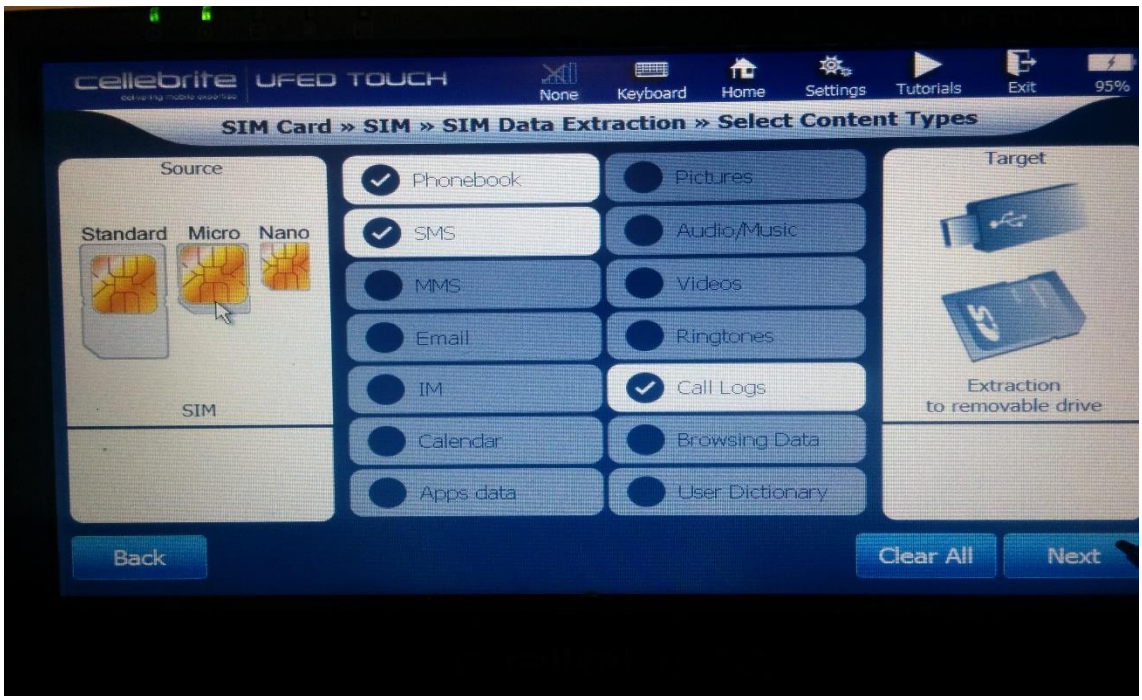
Εικόνα 137. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite



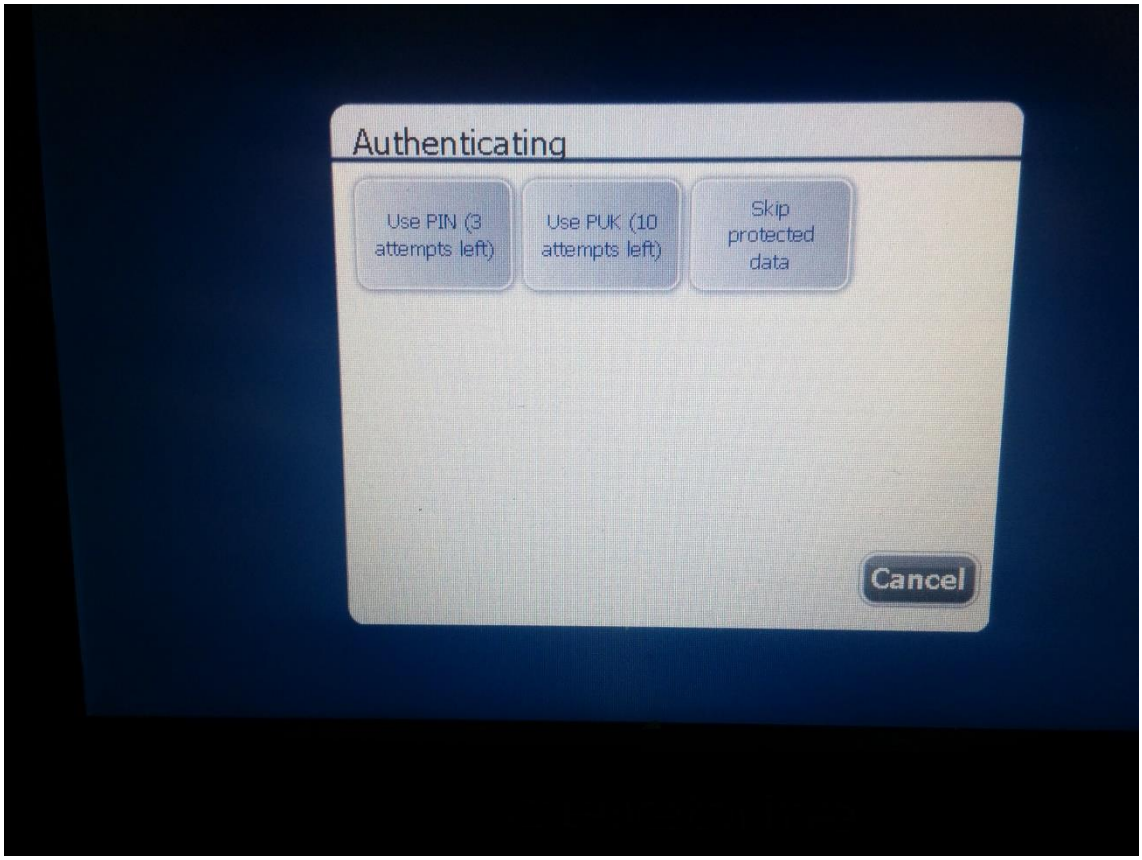
Εικόνα 138. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite



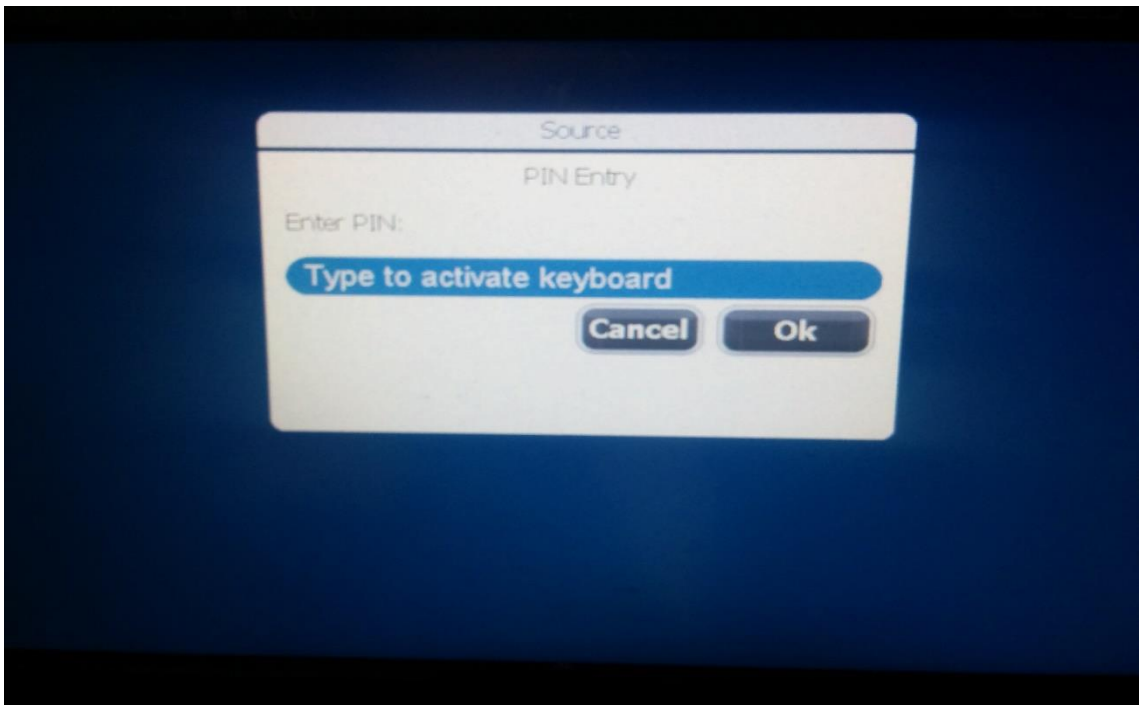
Εικόνα 139. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite



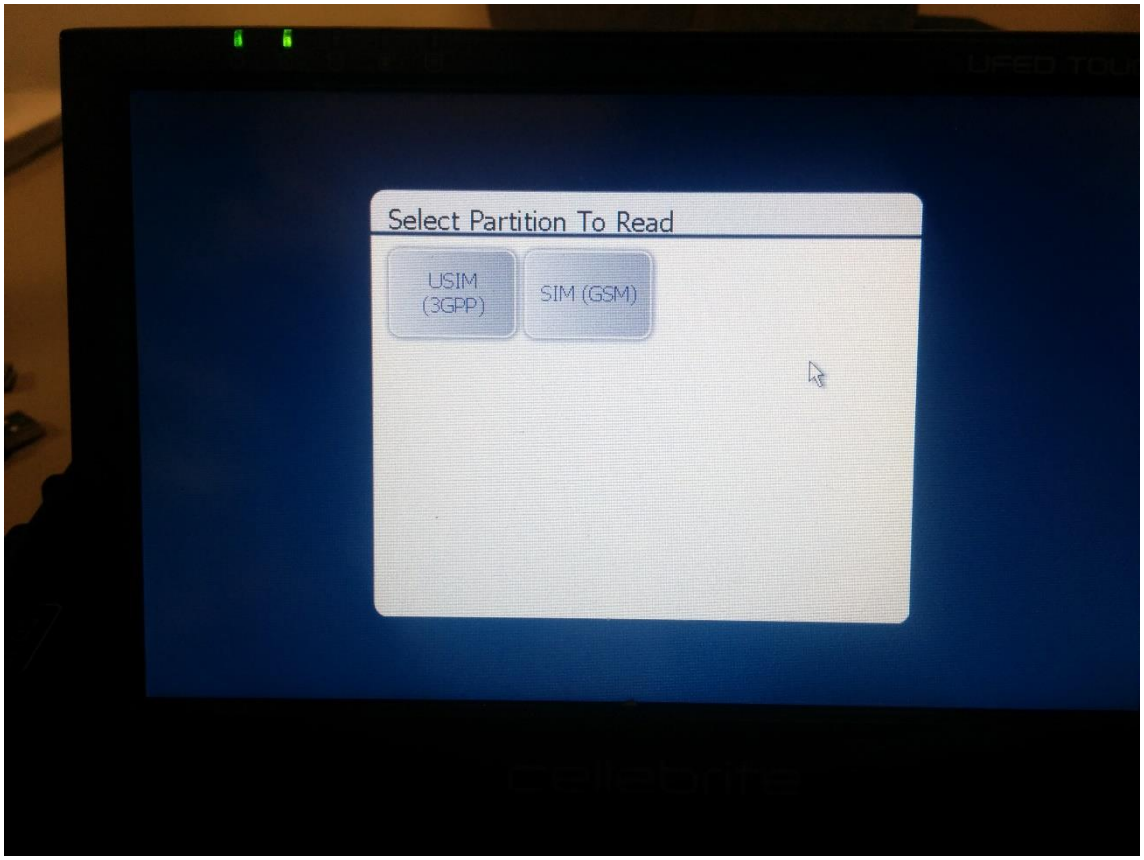
Εικόνα 140. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite



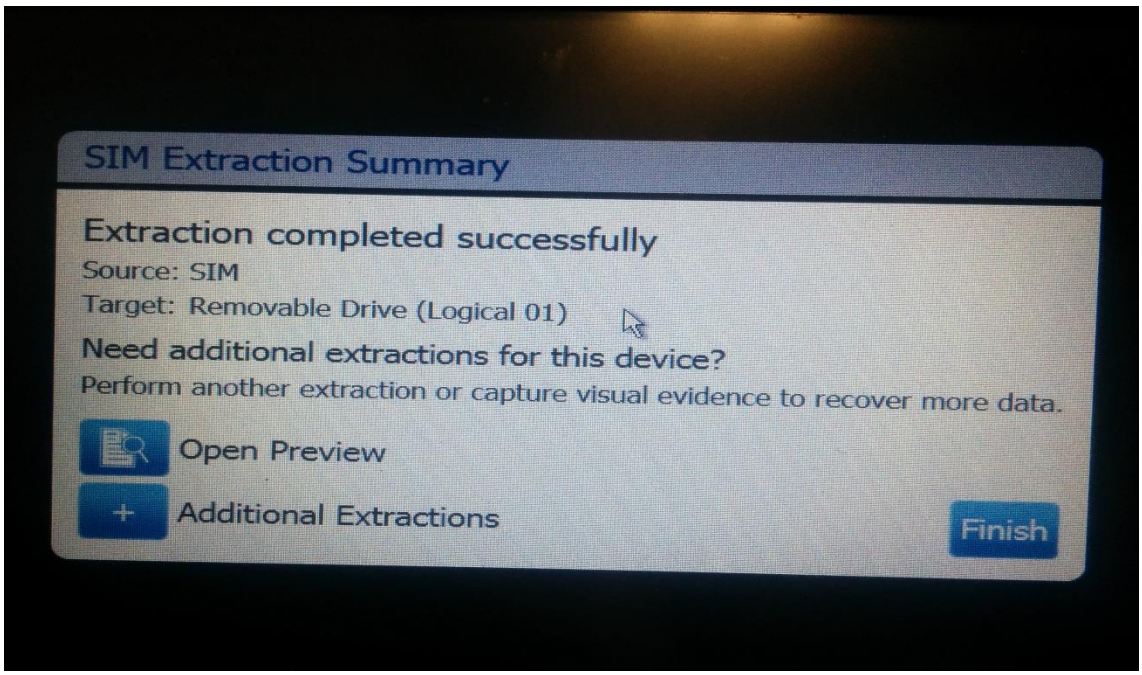
Εικόνα 141. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite



Εικόνα 142. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite

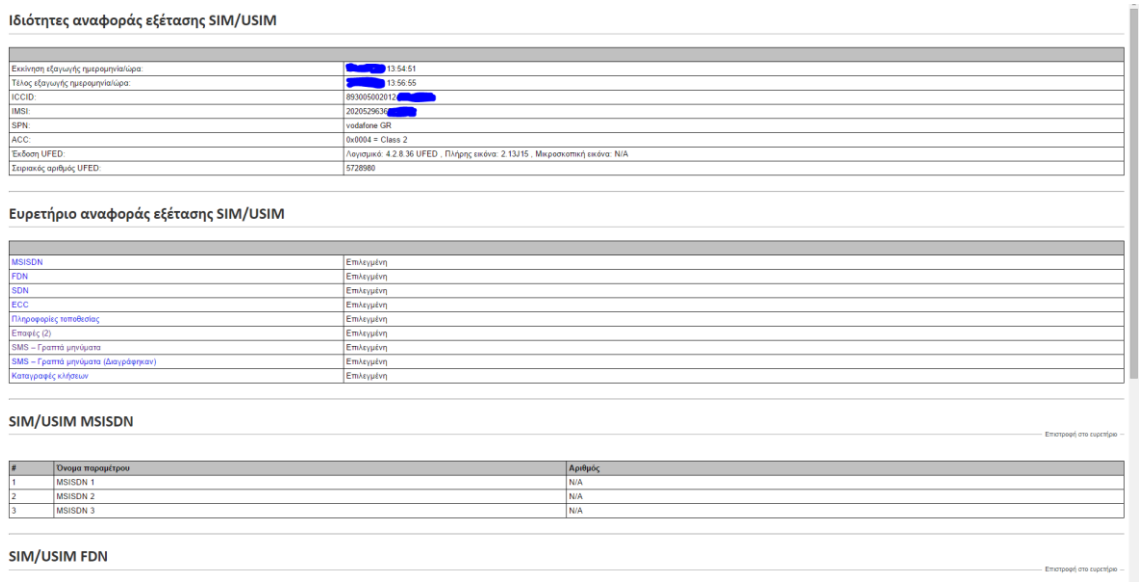


Εικόνα 143. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite



Εικόνα 144. Απεικόνιση από τον οδηγό εξέτασης κάρτας SIM του εργαλείου Cellebrite

Μετά την ολοκλήρωση της διαδικασίας, δημιουργείται ένα (1) αρχείο μορφής (html) όπου παρουσιάζονται τα δεδομένα από την εξέταση της κάρτας SIM (βλ. Εικόνα 145).


Ιδιότητες αναφοράς εξέτασης SIM/USIM

Εκκίνηση εξαγωγής ημερομηνία/ώρα:	[redacted] 13:54:51
Τέλος εξαγωγής ημερομηνία/ώρα:	[redacted] 13:56:55
ICCID:	893005002012[redacted]
IMSI:	202052963[redacted]
SPN:	vodafone GR
ACC:	0x0004 = Class 2
Έκδοση UFED:	Λογισμικό: 4.2.8.36 UFED ; Πλήρης εικόνα: 2.13J15 ; Μικροσκοπική εικόνα: N/A
Σειριακός αριθμός UFED:	5728980

Ευρετήριο αναφοράς εξέτασης SIM/USIM

MSISDN	Επιλεγμένη
FDN	Επιλεγμένη
SDN	Επιλεγμένη
ECC	Επιλεγμένη
Πληροφορίες τοποθεσίας	Επιλεγμένη
Επαφές (2)	Επιλεγμένη
SMS – Γραπτά μηνύματα	Επιλεγμένη
SMS – Γραπτά μηνύματα (Διαγράφηκαν)	Επιλεγμένη
Καταγραφές κλήσεων	Επιλεγμένη

SIM/USIM MSISDN

Επιστροφή στο ευρετήριο

#	Όνομα παραμέτρου	Αριθμός
1	MSISDN 1	N/A
2	MSISDN 2	N/A
3	MSISDN 3	N/A

SIM/USIM FDN

Επιστροφή στο ευρετήριο

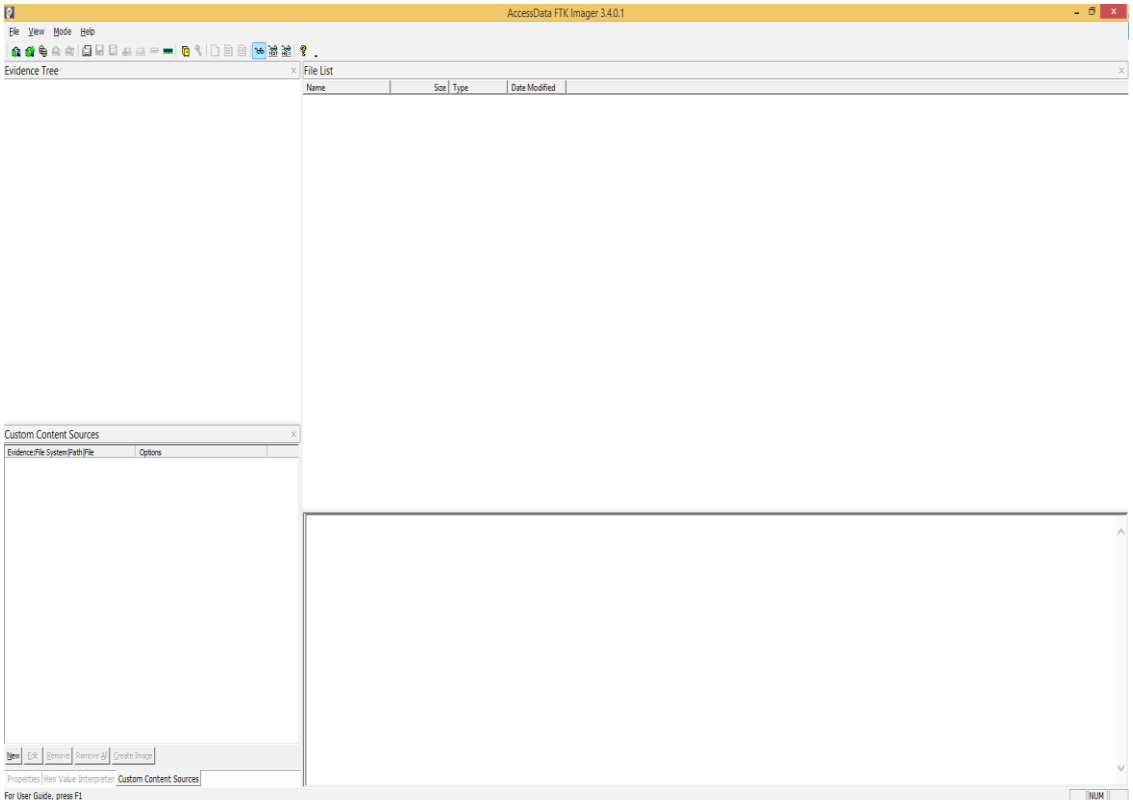
Εικόνα 145. Απεικόνιση από την ανάλυση της κάρτας SIM του εργαλείου Cellebrite

6.6 Εξέταση εξωτερικής κάρτας μνήμης (SD)

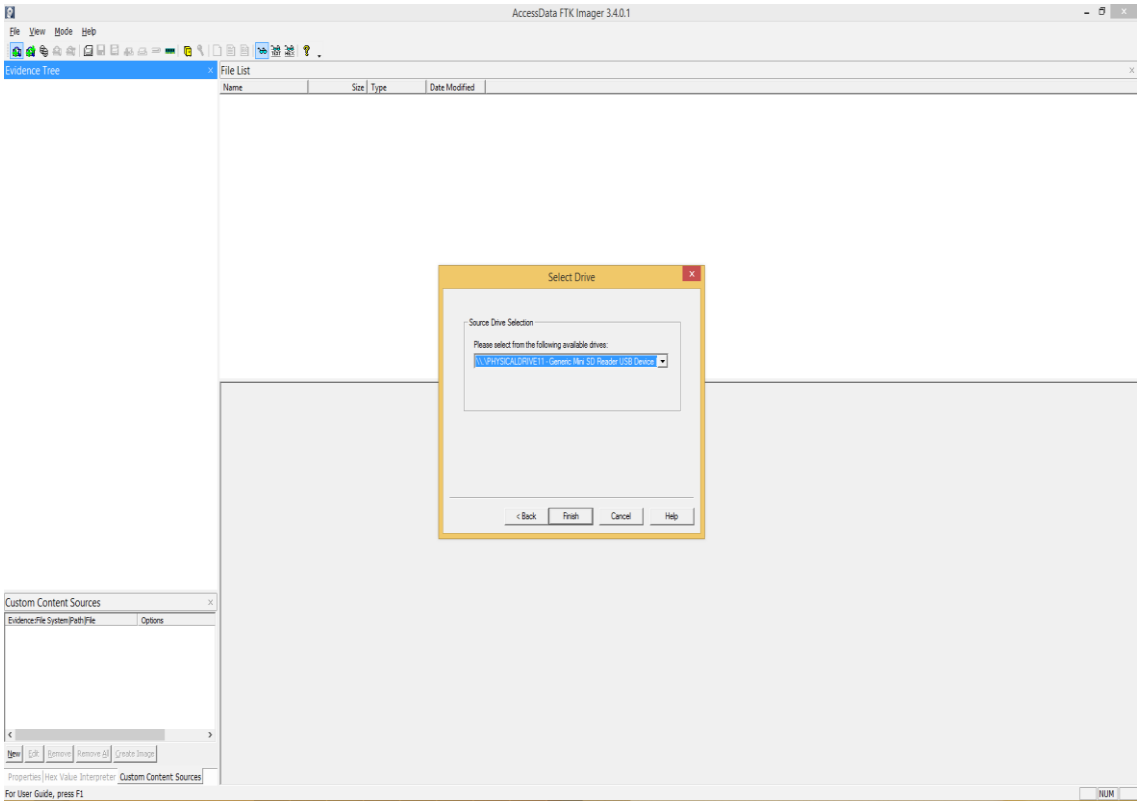
Αφού αφαιρέσουμε την κάρτα από την συσκευή, την σημαίνουμε, την φωτογραφίζουμε (βλ. εικόνες 146 & 147) και εν συνεχεία ακολουθούμε την διαδικασία εξέτασης που περιγράφουμε στην παράγραφο 4.5.

Εικόνες 146 & 147. Απεικονίσεις της κάρτας μνήμης (sd)

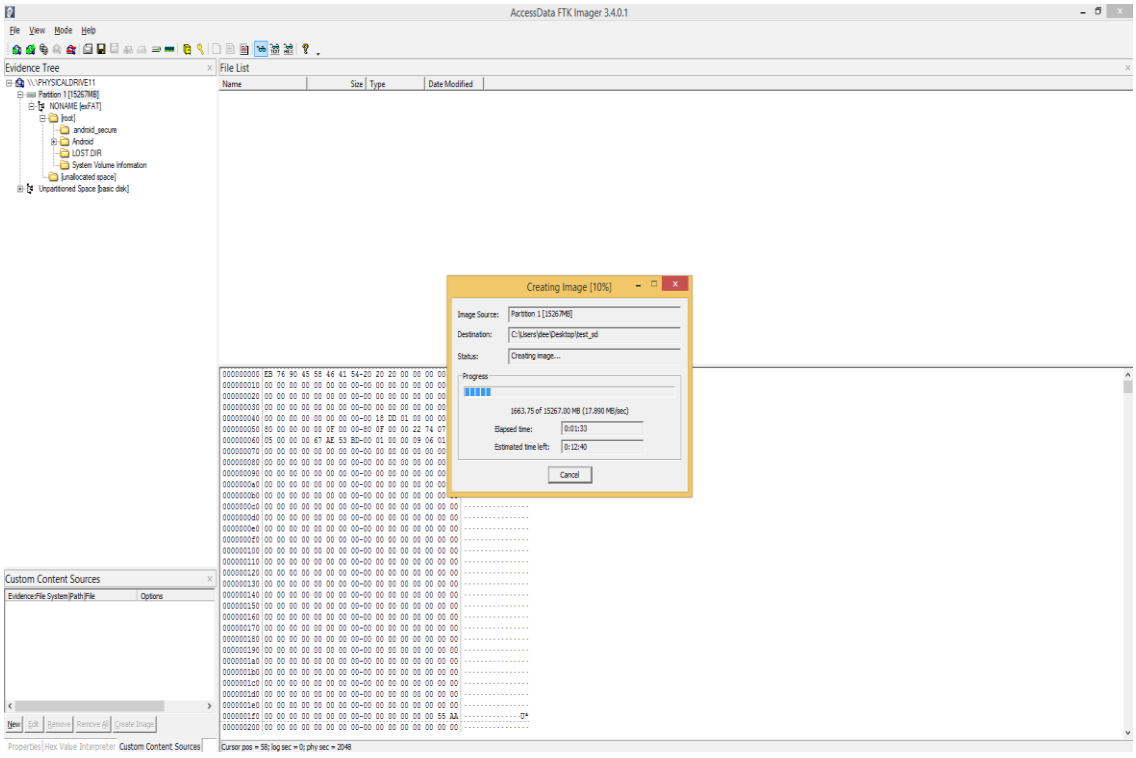
Ειδικότερα, αρχικά δημιουργούμε το εγκληματολογικό αντίγραφο μέσω του εργαλείου FTK Imager (βλ. εικόνες 136 έως 139) και στη συνέχεια κάνουμε ανάλυση με το εργαλείο Autopsy, προκειμένου να δούμε το περιεχόμενο των υπάρχοντων και τυχόν διαγεγραμμένων αρχείων καθώς και να αναζητηθούν ευρήματα, τα οποία θα μας διευκολύνουν ώστε να απαντήθουν τα τιθέντα ερωτήματα (βλ. εικόνες 148 έως 153).



Εικόνα 148. Απεικόνιση του FTK Imager



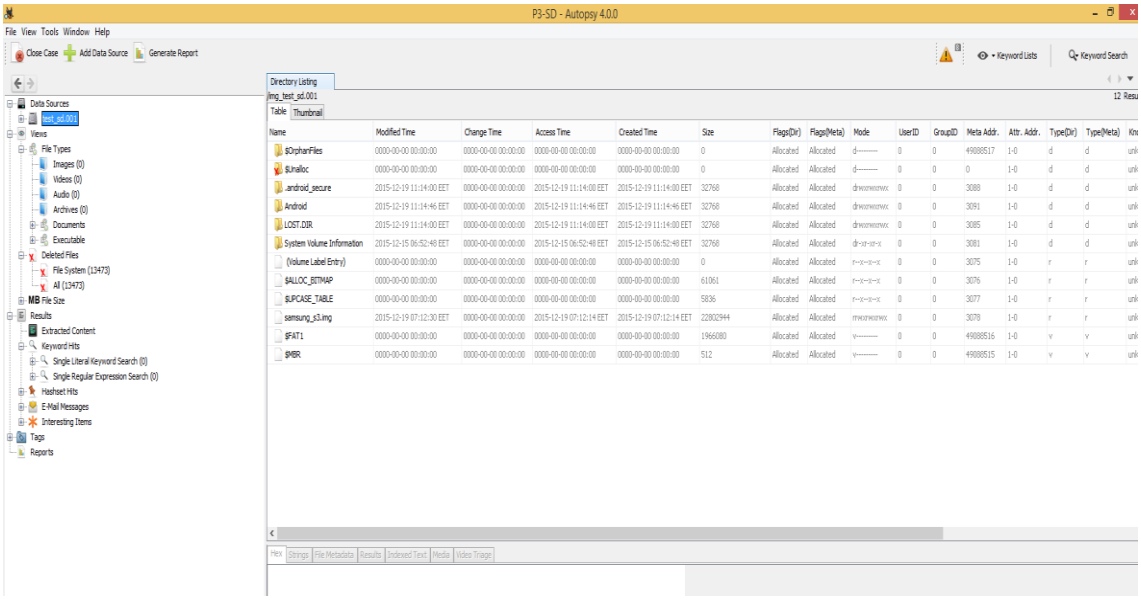
Εικόνα 149. Απεικόνιση του FTK Imager – Εισαγωγή του Φυσικού δίσκου



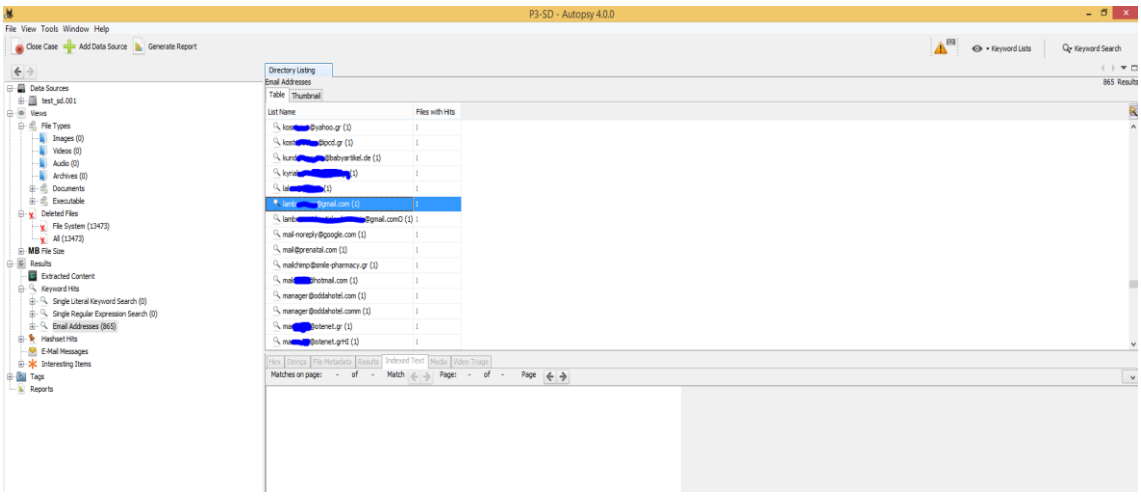
Εικόνα 150. Απεικόνιση του FTK Imager – Δημιουργία του εγκληματολογικού αντιγράφου

```
Created By AccessData® FTK® Imager 3.4.0.1

Case Information:
Acquired using: ADI3.4.0.1
Case Number: test_sd
Evidence Number: test_sd
Unique description: test_sd
Examiner: axel
Notes:

------------------------------------------------------------

Information for C:\Users\dee\Desktop\test_sd:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Partition Information]
 Starting Sector: 2,048
 Sector Count: 31,266,816
 Source data size: 15267 MB
 Sector count:    31266816
[Computed Hashes]
 MD5 checksum:    0c3274b43421c69725fb8550c080fd2c
 SHA1 checksum:   6ce77d064148ce07ad85c6560ccce35c7dc68368

Image Information:
 Acquisition started:   Tue Dec 22 13:25:13 2015
 Acquisition finished:  Tue Dec 22 13:42:57 2015
 Segment list:
  C:\Users\dee\Desktop\test_sd.001
  C:\Users\dee\Desktop\test_sd.002
  C:\Users\dee\Desktop\test_sd.003
  C:\Users\dee\Desktop\test_sd.004
  C:\Users\dee\Desktop\test_sd.005
  C:\Users\dee\Desktop\test_sd.006
  C:\Users\dee\Desktop\test_sd.007
  C:\Users\dee\Desktop\test_sd.008
  C:\Users\dee\Desktop\test_sd.009
  C:\Users\dee\Desktop\test_sd.010
```

Εικόνα 151. Απεικόνιση αναφοράς ύστερα από επιτυχή δημιουργία αντιγράφου με το FTK Imager



Εικόνα 152. Απεικόνιση αναφοράς ύστερα από επιτυχή δημιουργία αντιγράφου με το FTK Imager



Εικόνα 153. Απεικόνιση αναφοράς ύστερα από επιτυχή δημιουργία αντιγράφου με το FTK Imager

7 Επίλογος

7.1 Σύνοψη

Συνοψίζοντας την διπλωματική εργασία θα αναφέραμε ότι έγινε προσπάθεια τόσο από θεωρητικής όσο και τεχνικής απόψεως να τεθούν στοιχεία που απαρτίζουν την επιστήμη της "Ψηφιακής Εγκληματολογίας σε κινητές συσκευές Android". Αρχικά, παρουσιάστηκαν οι βασικές έννοιες σχετικά με το λειτουργικό σύστημα Android όπως η αρχιτεκτονική, οι εκδόσεις και η δομή των δεδομένων του, ενώ ακολούθησε μια σύντομη περιγραφή ως προς τα βήματα και τους μεθόδους εγκληματολογικής εξέτασης μιας κινητής συσκευής Android, καθώς και στα εργαλεία που χρησιμοποιούνται για την εξέταση των συσκευών αυτών.

Ιδιαίτερο βάρος δόθηκε στην πρακτική εξέταση μιας πραγματικής κινητής συσκευής λειτουργικού συστήματος Android, προσδιορίζοντας όλα τα βήματα που απαιτούνται για την εξέταση της από εμπορικά και ελεύθερα λογισμικά. Η εξέταση χωρίστηκε σε δύο (2) περιπτώσεις: α) κλειδωμένη κινητή συσκευή και β) ξεκλείδωτη και για κάθε περίπτωση δοκιμάστηκαν δύο (2) εμπορικά εργαλεία και ένα (1) ελεύθερο ως προς την φυσική και λογική εξαγωγή και εξέταση της συσκευής. Τέλος, αναπτύχθηκε και μια χειροκίνητη διαδικασία εξαγωγής για τις ως άνω περιπτώσεις. Τα αποτελέσματα της πρακτικής εξέτασης συνοψίζονται στον παρακάτω πίνακα (βλ. Πίνακα 3), όπου διαπιστώνουμε ότι με την χειροκίνητη εξέταση της συσκευής (βλ. παράγραφο 6.4) πετύχαμε τα μέγιστα αποτελέσματα. Αξίζει να σημειωθεί όμως, ότι η διαδικασία αυτή είναι αρκετά χρονοβόρα και δεν είναι καθολική για όλους τους τύπους των συσκευών.

Samsung SIII – FORENSIC ANALYSIS	Ξεκλείδωτη Συσκευή		Κλειδωμένη Συσκευή	
	Physical	Logical	Physical	Logical
Cellebrite	x	x	x	-
Oxygen	-	x	-	x
Viaforensics	-	x	-	-
Χειροκίνητη Ανάλυση	x	x	x	x

Πίνακας 3. Πίνακας αποτελεσμάτων εγκληματολογικής εξέτασης της συσκευής Samsung SIII

7.2 Συμπεράσματα

Ο κλάδος της ψηφιακής εγκληματολογίας σε κινητές συσκευές Android είναι σχετικά καινούργιος και λόγω της αυξανόμενης εξέλιξης των κινητών συσκευών, είναι πολύ δύσκολο να υπάρξουν πολύ συγκεκριμένες μεθοδολογίες για την εξέταση τους, εν αντιθέσει με τους Ηλεκτρονικούς Υπολογιστές. Η ευρεία γκάμα των κατασκευαστών κινητών συσκευών, όπου κάθε μία προσαρμόζει τον πυρήνα του Android στα δικά της δεδομένα, η τεράστια γκάμα εφαρμογών και τα κλειδώματα συσκευών αποτελούν τους σημαντικότερους παράγοντες για την μη ύπαρξη

εργαλείων που να υποστηρίζουν όλες τις συσκευές, ως προς την φυσική και λογική εξαγωγή/ανάλυση της μνήμης των συσκευών.

Για τους λόγους αυτούς, ο εξεταστής ψηφιακών πειστηρίων θα πρέπει να χρησιμοποιεί περισσότερα του ενός εργαλεία είτε εμπορικά είτε ελεύθερα, καθώς και να εφαρμόζει τεχνικές χειροκίνητης ανάλυσης σε συνδυασμό με τα εργαλεία αυτά, προκειμένου να πετύχει τα μέγιστα αποτελέσματα, τα οποία καθορίζονται από τα τιθέντα ερωτήματα της κάθε υπόθεσης που καλείται να αντιμετωπίσει.

8 Βιβλιογραφικές Πηγές

1. Aviv, A., κ.α., (2011). Smudge Attacks on Smartphone Touch Screens. University of Pennsylvania
2. Ayers, R., (2008). Mobile Device Forensics - Tool Testing. Mobile Device Forensics. NIST
3. Rick Ayers, Sam Brothers & Wayne Jansen (2014). Guidelines on Mobile Device Forensics. NIST
4. Curran, K., κ.α. (2010). Mobile Phone Forensic Analysis. International Journal of Digital Crime and Forensics
5. Fabio Casadei, A. S. (2005). Forensics and SIM cards: an Overview. International Journal of Digital Evidence
6. Hoog, A. (2011). Android Forensics. Investigation, Analysis, and Mobile Security for Google Android. USA: Elsevier
7. Katz, M., (2013). Android Forensics, Patrick Leahy Center for Digital Investigation (LCDI)
8. Lee, X., κ.α. (2010). Design and implementation of forensic system in Android smartphone. International Forum in Information Technology and Applications
9. Lessard, J., Kessler, G. C. (2010). Android Forensics: Simplifying Cell Phone Examinations. Small Scale Digital Device Forensics Journal.
10. Murphy, Det. Cynthia A. Developing Process for Mobile Device Forensics_v3, Sans Press
11. Simson L. Garfinkel, (2011). Android Forensics
12. Turnbull, E. C. (2011). Digital Evidence on Mobile Devices. Academic Press
13. Καλλέργης, Γ., (2013). Ανάπτυξη εφαρμογών σε περιβάλλον Android, Διπλωματική εργασία του τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πατρών
14. Καρατάσιου, Ε., (2012). Δικανική υπολογιστική: Μέθοδοι, εργαλεία και προοπτικές, Διπλωματική εργασία του τμήματος Πληροφορικής, Πανεπιστήμιο Πειραιώς
15. Μήττα Μ., (2014). Ψηφιακά Πειστήρια σε έξυπνα τηλέφωνα Android, Διπλωματική εργασία του τμήματος Εφαρμοσμένης Πληροφορικής, Πανεπιστήμιο Μακεδονίας
16. Μπαρμπάτσαλου, Κ., (2012). Mobile Device Forensics: A Review to reveal the truth from the bytes, Διπλωματική εργασία του τμήματος Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου
17. Παπαδέας Δ. (2013). Ασφάλεια στο λειτουργικό σύστημα Android, Διπλωματική εργασία του τμήματος Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς
18. Σακκάς Β. (2014). Android Forensics, Διπλωματική εργασία του τμήματος Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς
19. http://en.wikipedia.org/wiki/Mobile_device_forensics
20. http://en.wikipedia.org/wiki/Android_%28operating_system%29
21. https://digital-forensics.sans.org/blog
22. https://www.msab.com/products/xry/
23. http://www.cellebrite.com/Mobile-Forensics/Products/ufed-touch
24. http://www.oxygen-forensic.com/en/
25. https://viaforensics.com/resources/tools/android-forensics-tool/
26. https://www.magnetforensics.com/magnet-acquire/
27. http://www.sleuthkit.org/autopsy/
28. http://www.accessdata.com/support/product-downloads
29. http://www.vmware.com/
30. http://freeandroidforensics.blogspot.gr/