Πανεπιστήμιο Πειραιά

Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. Ασφάλεια Ψηφιακών Συστημάτων

Καθηγητής: Ξενάκης Χρήστος

Διπλωματική Εργασία:

"Ψηφιακή Εγκληματολογία σε Android 10"

Master Thesis:

'Android 10 Forensics'

Χρυσανθακοπούλου Γερασιμίνα Α.Μ.: ΜΤΕ 1831

ΠΕΙΡΑΙΑΣ 2021

Στον εαυτό μου

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Ξενάκη για την εμπιστοσύνη που μου έδειξε, την βοήθειά του ώστε να μπορέσω να ολοκληρώσω την διπλωματική εργασία μου και για το ενδιαφέρον που μου ενέπνευσε για τον τομέα της ασφάλειας υπολογιστών.

Θα ήθελα να ευχαριστήσω τους γονείς μου και τους φίλους μου για την διαρκή υποστήριξη, την υπομονή, την ενθάρρυνση τους και την πίστη τους σε εμένα.

Περιεχόμενα

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ABSTRACT

The purpose of this thesis is to investigate the research field of digital forensics, specifically the scientific branch of mobile forensics. The field of research was limited to mobile phones using the operating system android 10. Throughout the survey a Samsung Galaxy A70 phone was used and not an emulator.

The research began by rooting the device. First we showed the removal of lock screen protections and the process to uninstall Knox which may cause problems in the forensic process of securing a mobile device.

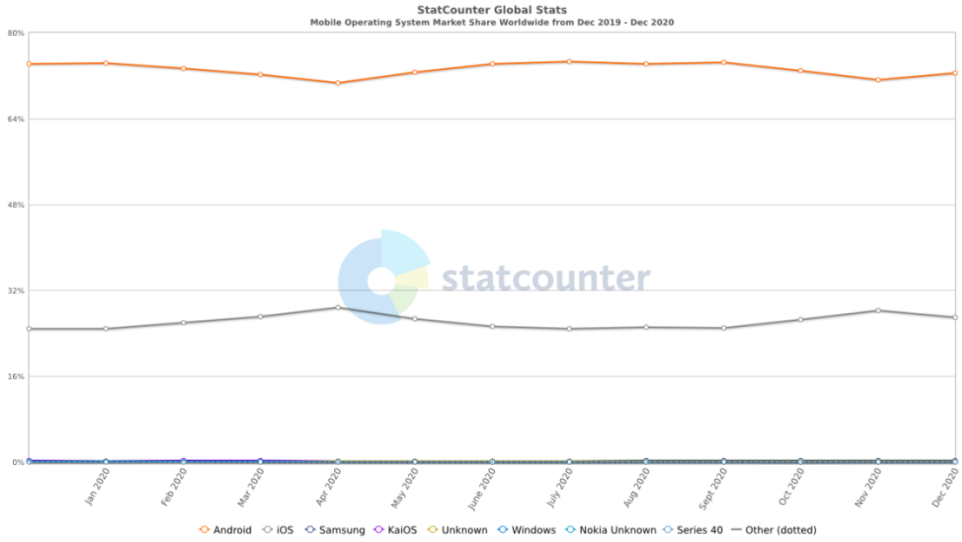
Furthermore, we managed to acquire a logical level image of the device using tools from the Santoku collection and the capabilities provided from the android 10 device, this method wasn't efficient since it provided little to no data. It provided though an interesting finding the IMSI, which is information that shouldn't be this easy to find in a logical extraction. We also managed to get a logical level image of the device using the 30 days free trial version of the program FonePaw, this logical extraction proved more efficient than the one from Santoku and provided more data from the device, it didn't provide the IMSI.

Afterwards we managed to acquire a physical image of the entire device using the tools dd and netcat. We tried to analyze the physical image using Autopsy but didn't manage to do so successfully. We also used andriller which is another open source solution to perform a physical analysis of the device but got only the general information of the device.

We found no open source available programs to the public that can do a successful physical image analysis of android 10.

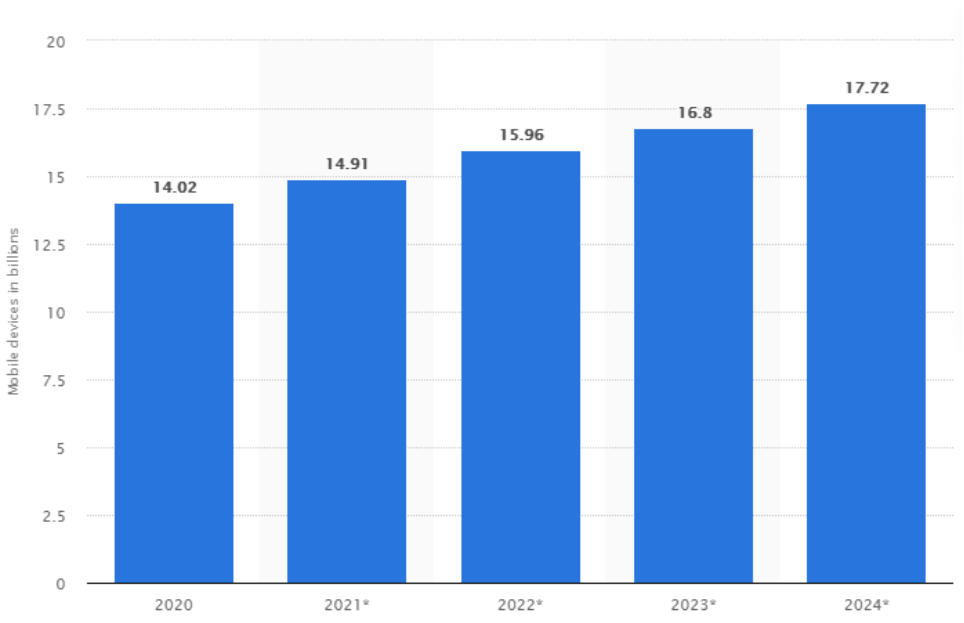
ΕΙΣΑΓΩΓΗ

Το λειτουργικό σύστημα Android είναι το κυρίαρχο λειτουργικό σύστημα στις κινητές συσκευές εφόσον κατέχει το μεγαλύτερο μερίδιο της αγοράς παγκοσμίως (Εικόνα 1) με συντριπτικό ποσοστό της τάξεως του 72.48% (Hazra & Mateti, 2017) (statcounter, 2019 - 2020).



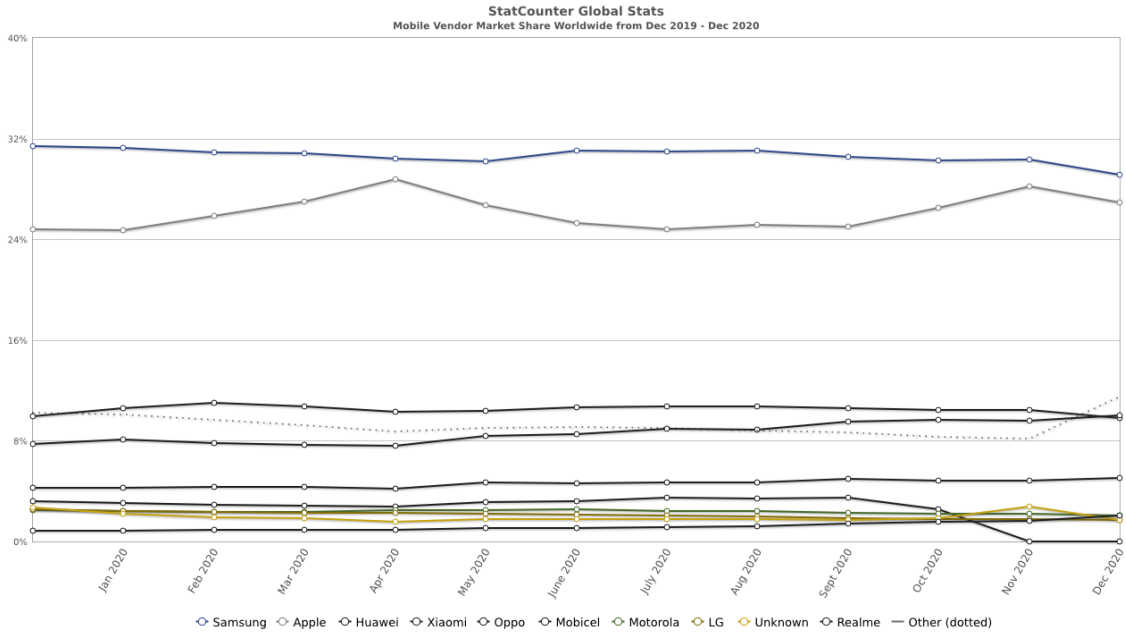
Εικόνα 1 - Κυρίαρχα Λειτουργικά Συστήματα (statcounter, 2019 - 2020)

Ο αριθμός των κινητών συσκευών που λειτουργούσαν παγκοσμίως για το έτος 2020 ανέρχεται στα 14 δισεκατομμύρια (Εικόνα 2) και αναμένεται να αυξηθεί (statista, 2020).



Εικόνα 2 - Ενεργές Κινητές Συσκευές Παγκοσμίως (statista, 2020)

Από τις κινητές συσκευές για το έτος 2020 τις μεγαλύτερες πωλήσεις καταγράφει η Samsung (Εικόνα 3), κατέχοντας σταθερά το μεγαλύτερο μερίδιο της παγκόσμιας αγοράς με τις συσκευές τους κατά κύριο λόγο να έχουν το λειτουργικό σύστημα Android (statcounter, 2019-2020).



Εικόνα 3 - Samsung Market share (statcounter, 2019-2020)

Ο μέσος χρήστης περνάει κατά μέσο όρο 3 ώρες και 15 λεπτά την ημέρα στο κινητό του τηλέφωνο (Spajic, 2020) (Lin, 2020) (Matei, 2019). Οι επιλογές που δίνονται πλέον με ένα κινητό τηλέφωνο είναι απεριόριστες, από ανταλλαγή μηνυμάτων, κλήσεων, λήψη φωτογραφιών, βίντεο, διενέργεια οικονομικών συναλλαγών, διαχείριση αρχείων, web browsing και πολλά ακόμα. Οι κινητές συσκευές καταλήγουν λοιπόν να έχουν μια πληθώρα προσωπικών δεδομένων αποθηκευμένα (Ranjan Roy, et al., 2016) (Nunez, 2020).

Η τεχνολογική εξέλιξη στις κινητές συσκευές έχει προσελκύσει και το ενδιαφέρον τον εγκληματιών δίνοντας τους νέες δυνατότητες για τη διενέργεια παράνομων ενεργειών (Casey, 2011). Από τις κινητές συσκευές συλλέγεται πληθώρα στοιχείων σε έρευνες των διωκτικών αρχών και είναι στατιστικά πιθανό οι κινητές συσκευές προς έρευνα να έχουν λειτουργικό σύστημα android (Hazra & Mateti, 2017).

Πέρα από την χρησιμότητα για τις διωκτικές αρχές η διενέργεια μιας forensics analysis σε κινητές συσκευές μπορεί να ενημερώσει τους χρήστες τι θα πρέπει να αποθηκεύουν τελικά στις συσκευές τους και ποια δεδομένα κρατάνε τελικά οι συσκευές για τους χρήστες (Ranjan Roy, et al., 2016).

Για τους προαναφερθέντες λόγους έγινε η επιλογή να πραγματοποιηθεί η έρευνα σε κινητή συσκευή Samsung (Samsung Galaxy A70) με μοντέλο SM-A705FN/DS) και λειτουργικό σύστημα Android 10. Στην παρούσα διπλωματική εργασία εξετάσθηκαν αναλυτικά οι διαδικασίες:

- Απόκτησης root πρόσβασης στην συσκευή
- Παράκαμψης μηχανισμών ασφάλειας και κλειδώματος οθόνης
- Διαχείρισης permissions, απενεργοποίηση κρυπτογράφησης και απεγκατάστασης Knox
- Logical Level Forensic Image Acquisition and Analysis
- Physical Forensic Image Acquisition
- Physical Forensic Image Analysis

Είδαμε όλες τις πληροφορίες που αποθηκεύει η κινητή συσκευή για την δραστηριότητα και τις επικοινωνίες που έχουν πραγματοποιηθεί καθώς και τα προβλήματα που μπορεί να αντιμετωπίσει ένας ερευνητής με εργαλεία που είναι ελεύθερα διαθέσιμα στο κοινό.

MOBILE FORENSICS – ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

Η εκτέλεση μιας mobile forensics έρευνας έχει ως σκοπό την ανάκτηση δεδομένων από την κινητή συσκευή που ερευνάται τα οποία και θα πρέπει να παραμείνουν αναλλοίωτα, δηλαδή σε μια forensically sound κατάσταση. Αυτό συμβαίνει για να μπορούν να χρησιμοποιηθούν στην συνέχεια της έρευνας ως ψηφιακά πειστήρια (Kostadinov, 2019).

Forensically sound είναι ένας όρος που χρησιμοποιείται εκτενώς στα digital forensics και αφορά την μη αλλοίωση των αρχικών δεδομένων που βρίσκονται στην συσκευή που είναι προς εξέταση από τους ερευνητές. Η βασική αρχή κάθε forensics έρευνας είναι ότι τα δεδομένα δεν πρέπει να υποστούν κανενός είδους επεξεργασία. Αυτό είναι ιδιαιτέρως δύσκολο στην έρευνα των κινητών συσκευών. Ορισμένα εργαλεία απαιτούν επικοινωνία με την κινητή συσκευή που ερευνάται, το γεγονός αυτό αποκλείει τους write protectors. Άλλα εργαλεία προϋποθέτουν την root πρόσβαση στην συσκευή για να παρέχουν αποτελέσματα (Bommisetty, et al., 2014).

Στις περιπτώσεις που η mobile forensics έρευνα απαιτεί την οποιαδήποτε επέμβαση στην συσκευή η διαδικασία που ακολουθείται από τον ερευνητή και οι αλλαγές θα πρέπει να καταγράφονται αναλυτικά και να ακολουθούνται οι προτεινόμενες μεθοδολογίες. Η παράληψη καταγραφής κάποιου βήματος μπορεί να οδηγήσει σε απόρριψη των αποτελεσμάτων της έρευνας στο δικαστήριο (Soufiane, 2016).

Ένα από τα βασικότερα προβλήματα στην forensics έρευνα των κινητών συσκευών αφορά το γεγονός ότι τα δεδομένα που είναι αποθηκευμένα σε αυτές μπορούν να είναι προσβάσιμα από άλλες κινητές συσκευές ή υπολογιστές. Τα δεδομένα που είναι αποθηκευμένα σε κινητές συσκευές χαρακτηρίζονται volatile καθώς μπορούν να τροποποιηθούν και να διαγραφούν μέσα σε σύντομο χρονικό διάστημα απομακρυσμένα. Συνεπώς απαιτείται μεγαλύτερη προσοχή και προσπάθεια από τους ερευνητές προκειμένου να διατηρηθούν ανέπαφα και να μπορεί να αποδειχθεί η μη αλλοίωσή τους κατά την διάρκεια της έρευνας (Bommisetty, et al., 2014).

Κατά την διάρκεια μιας mobile forensics έρευνας μπορούν να προκύψουν διάφορα προβλήματα που αφορούν την απόκτηση των ψηφιακών πειστηρίων από τις κινητές συσκευές. Τα προβλήματα αυτά οφείλονται κυρίως στα ακόλουθα (Bommisetty, et al., 2014):

- Ποικιλία hardware
- Εκδόσεις λειτουργικών συστημάτων κινητών συσκευών
- Μέτρα ασφάλειας
- Έλλειψη υλικού
- Κατάσταση της συσκευής
- Τεχνικές anti-forensics
- Αθέμιτο reset
- Τροποποίηση των δεδομένων της συσκευής
- Παράκαμψη προστασιών οθόνης της συσκευής
- Αποκοπή της επικοινωνίας της συσκευής με το δίκτυο μετά την κατάσχεσή της
- Ύπαρξη malware στην συσκευή
- Νομικά ζητήματα

ΔΙΑΔΙΚΑΣΙΑ ΕΡΕΥΝΑΣ MOBILE FORENSICS

Η διαδικασία μιας mobile forensics έρευνας μπορεί να χωριστεί σε τρία βασικά στάδια (Kostadinov, 2019):

- Seizure: Κατάσχεση της κινητής συσκευής
- Acquisition: Συλλογή στοιχείων
- Examination/Analysis: Εξέταση/Ανάλυση στοιχείων

ΚΑΤΑΣΧΕΣΗ ΚΙΝΗΤΗΣ ΣΥΣΚΕΥΗΣ

Η κατάσχεση μιας κινητής συσκευής θα πρέπει να γίνεται σύμφωνα με κάποιες διαδικασίες που διασφαλίζουν ότι μια συσκευή δεν θα υποστεί τροποποιήσεις μέχρι να φτάσει στο εργαστήριο (Brunty, 2016) (Bommisetty, et al., 2014) (Kostadinov, 2019).

Secure the Phone: Αποτρέπεται η επαφή των ατόμων που υπάρχουν στο σημείο με την συσκευή, είτε η συσκευή είναι ενεργή είτε όχι.

Capture the Information on Display: Γίνεται καταγραφή όλων των πληροφοριών που εμφανίζονται στην οθόνη με την χρήση κάμερας.

Prevent Network Access: Αποτρέπεται η σύνδεση της συσκευής με το τηλεπικοινωνιακό δίκτυο, αυτό γίνεται τοποθετώντας την συσκευή μέσα σε faraday bag.

Seize Relevant Hardware: Ο ερευνητής θα πρέπει να κατασχέσει μαζί με την συσκευή και πιθανό hardware που μπορεί να σχετίζεται με αυτή.

Seize Relevant Documentation: Ο ερευνητής θα πρέπει επιπρόσθετα να κατασχέσει και πιθανά έγγραφα που σχετίζονται με την συσκευή.

Secure Transportation: Πραγματοποίηση ασφαλούς μεταφοράς από τον τόπο κατάσχεσης στο εργαστήριο.

Document Everything: Γίνεται λεπτομερής καταγραφή όλων των ενεργειών που σχετίζονται με την κινητή συσκευή που είναι προς έρευνα από την στιγμή που βρέθηκε μέχρι να φτάσει στο εργαστήριο. Καταγράφονται επιπρόσθετα και τα άτομα που πραγματοποιούν τις συγκεκριμένες ενέργειες.

ΣΥΛΛΟΓΗ ΣΤΟΙΧΕΙΩΝ

Στην συγκεκριμένη φάση μιας mobile forensics έρευνας στόχος του ερευνητή είναι να συλλέξει όσες περισσότερες πληροφορίες μπορεί προκειμένου να πραγματοποιήσει έπειτα την διαδικασία της ανάλυσής τους. Οι πηγές πληροφοριών είναι (Brunty, 2016) :

- Η συσκευή
- Η κάρτα SIM
- Η κάρτα μνήμης SD
- Το Documentation
- Ο πάροχος του δικτύου κινητής τηλεφωνίας
- Οι άνθρωποι
- Οι υπολογιστές

ΕΞΕΤΑΣΗ/ΑΝΑΛΥΣΗ ΣΤΟΙΧΕΙΩΝ

Πρώτο στάδιο στην διαδικασία εξέτασης των στοιχείων είναι η φάση αναγνώρισης/ identification phase. Εδώ ο ερευνητής θα πρέπει να μπορεί να αναγνωρίσει και να καταγράψει (Bommisetty, et al., 2014):

- Νομική Αρχή
- Στόχο Έρευνας
- Βασικές Πληροφορίες για την Κινητή Συσκευή
- Πρόσθετα αποθηκευτικά μέσα (sd/microsd card)
- Πιθανές πηγές άλλων πειστηρίων

Η διαδικασία της ανάλυσης μιας κινητής συσκευής μπορεί να χωριστεί σε πέντε επίπεδα, τα επίπεδα αυτά απαριθμούνται στην συνέχεια ξεκινώντας από αυτό που απαιτεί την μικρότερη επέμβαση στην κινητή συσκευή (Kostadinov, 2019) (Bommisetty, et al., 2014).

Manual/ Scroll Analysis: Η συγκεκριμένη διαδικασία πραγματοποιείται όταν εντοπιστεί η κινητή συσκευή και πριν τοποθετηθεί σε faraday bag. Ο ερευνητής πραγματοποιεί scroll κατευθείαν στην συσκευή και καταγράφει με την χρήση κάμερας όλα τα μενού και τις πληροφορίες που φαίνονται στην συσκευή.

Logical Analysis: Η Logical ανάλυση προϋποθέτει την σύνδεση της κινητής συσκευής και του forensic workstation, δηλαδή του υπολογιστή στον οποίο θα πραγματοποιηθεί όλη η διαδικασία ανάλυσης των δεδομένων που έχουν ανακτηθεί από την συσκευή. Η σύνδεση μεταξύ συσκευής και workstation πραγματοποιείται συνήθως με την χρήση usb καλωδίου. Στην συνέχεια από τον υπολογιστή με την χρήση συγκεκριμένων εντολών ή του κατάλληλου προγράμματος γίνεται η ανάκτηση των δεδομένων. Στο συγκεκριμένο στάδιο σπάνια έχουμε την ανάκτηση διαγραμμένων αρχείων από την συσκευή.

Physical Analysis: Κατά την διαδικασία της physical ανάλυσης μιας συσκευής ο ερευνητής αποκτά physical forensic image της συσκευής και μετά το αναλύει με την βοήθεια λογισμικού.

Η απόκτηση physical forensic image πραγματοποιείται με την βοήθεια εγκατάστασης κάποιου agent στην συσκευή. Ο ερευνητής θα πρέπει να αποθηκεύσει το image σε κάποιον εξωτερικό σκληρό δίσκο και να υπολογίσει τα MD5 και SHA1 hashes του image. Τα συγκεκριμένα hashes θα πρέπει να μείνουν τα ίδια σε όλη την διάρκεια της έρευνας, έτσι ο ερευνητής θα μπορεί να αποδείξει την μη αλλοίωση του image. Αποθηκεύοντας το image σε εξωτερικό σκληρό δίσκο ο ερευνητής μπορεί να διασφαλίσει ότι το image δεν πρόκειται να υποστεί κάποια αλλαγή από το workstation του ερευνητή. Ο ερευνητής συνήθως δουλεύει σε αντίγραφο του image για να διασφαλίσει την ακεραιότητα του.

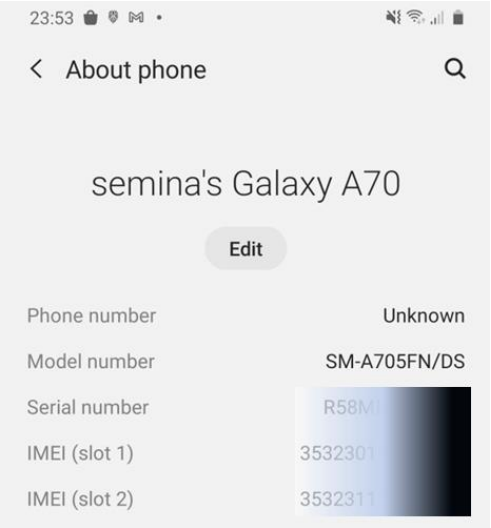
Chip- Off: Κατά την συγκεκριμένη διαδικασία ανάλυσης ο ερευνητής παίρνει δεδομένα κατευθείαν από το memory chip της κινητής συσκευής. Το chip αποσυνδέεται από την κινητή συσκευή και εισάγεται είτε σε έναν chip reader είτε σε άλλη κινητή συσκευή στην οποία και θα γίνει η εξαγωγή των δεδομένων.

Micro Read: Εδώ ο ερευνητής εξετάζει τα δεδομένα που φαίνονται στο memory chip της συσκευής, εξάγοντας το chip από την συσκευή και στην συνέχεια χρησιμοποιώντας ηλεκτρονικό μικροσκόπιο ο ερευνητής μπορεί να αναλύσει τα gates που είναι ορατά στο chip.

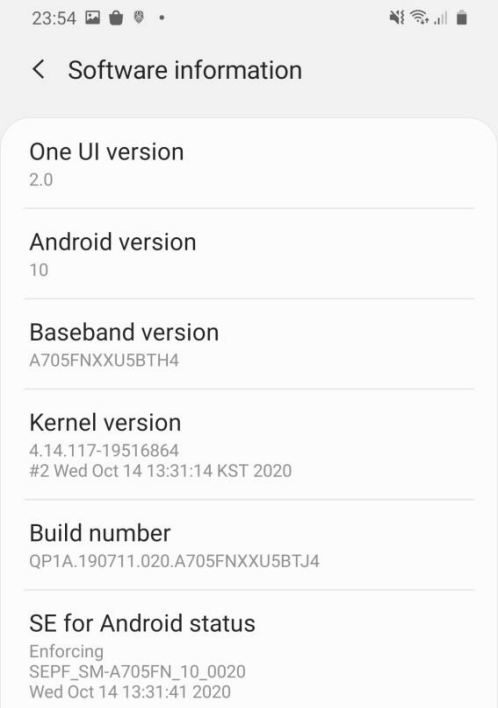
1. ΥΛΙΚΟ ΚΑΙ ΛΟΓΙΣΜΙΚΟ

1.1 Γενικές Πληροφορίες Συσκευής

Στην έρευνα χρησιμοποιήθηκε η κινητή συσκευή SAMSUNG GALAXY A70. Συγκεκριμένα το μοντέλο με κωδικό SM-A705FN/DS (Εικόνα 4). Στην συσκευή υπήρχε η έκδοση Android 10 One UI version 2.0 (Εικόνα 5).

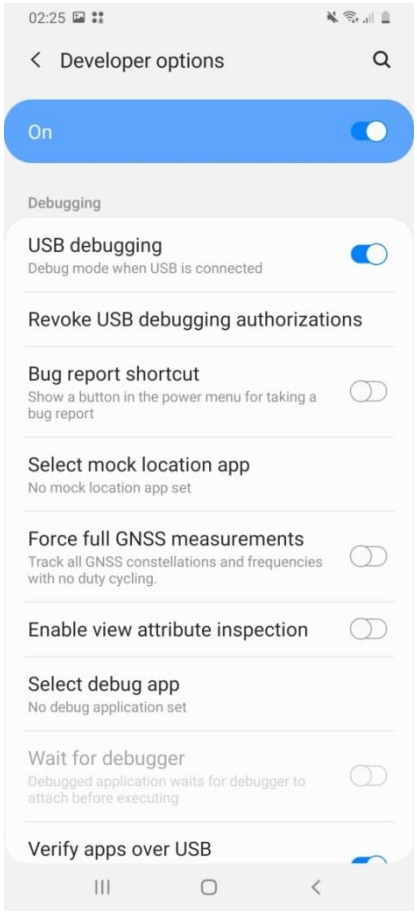


Εικόνα 4 - Γενικές Πληροφορίες Συσκευής 1



Εικόνα 5 - Γενικές Πληροφορίες Συσκευής 2

Η επιλογή του usb debugging από το μενού Developer Options ήταν ενεργοποιημένη (Εικόνα 6). Επιπλέον είχε αποκτηθεί root πρόσβαση στην συσκευή χρησιμοποιώντας το Odin, η συγκεκριμένη διαδικασία θα αναλυθεί στην συνέχεια.



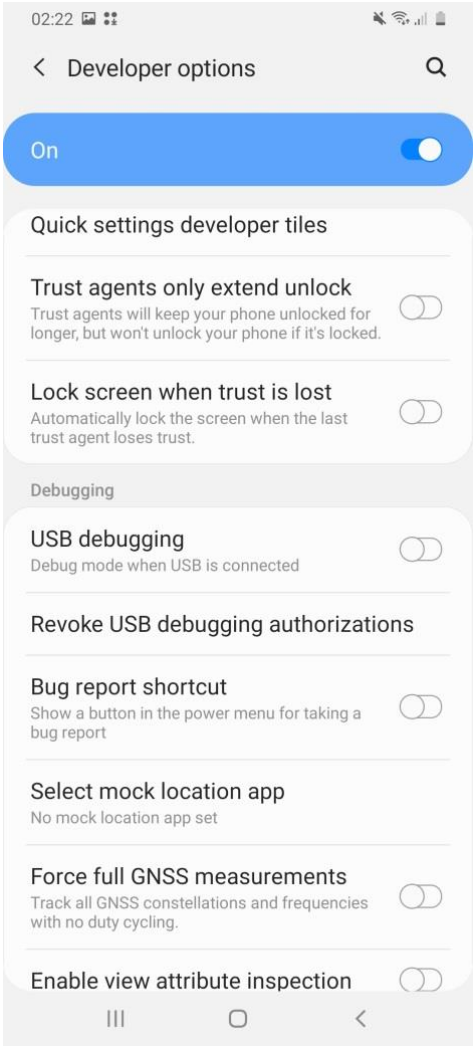
Εικόνα 6 - Γενικές Πληροφορίες Συσκευής 3

1.2 Διαδικασία Απόκτησης Root Πρόσβασης στην Συσκευή

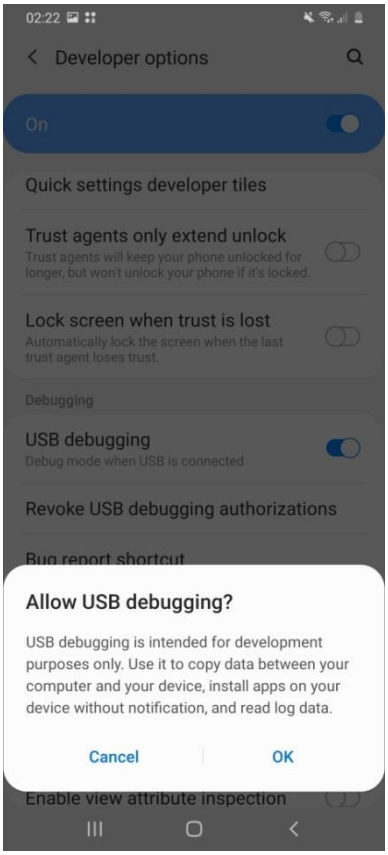
UNLOCKING THE BOOTLOADER

Για να ενεργοποιήσουμε τα Developer Options πηγαίνουμε στα Settings ->About Phone-> Κάνουμε tap 7 φορές το Build Number και ενεργοποιούμε τα Developer Options (Εικόνα 7).

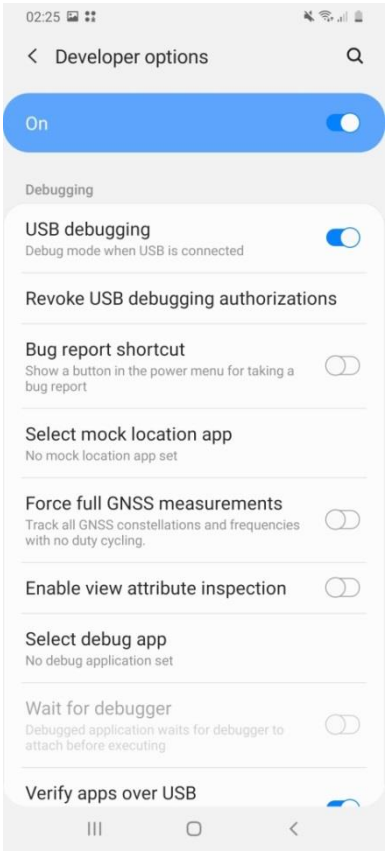
Στα Developer Options ενεργοποιούμε την επιλογή USB debugging (Εικόνα 8, Εικόνα 9) και OEM unlocking (Εικόνα 10).



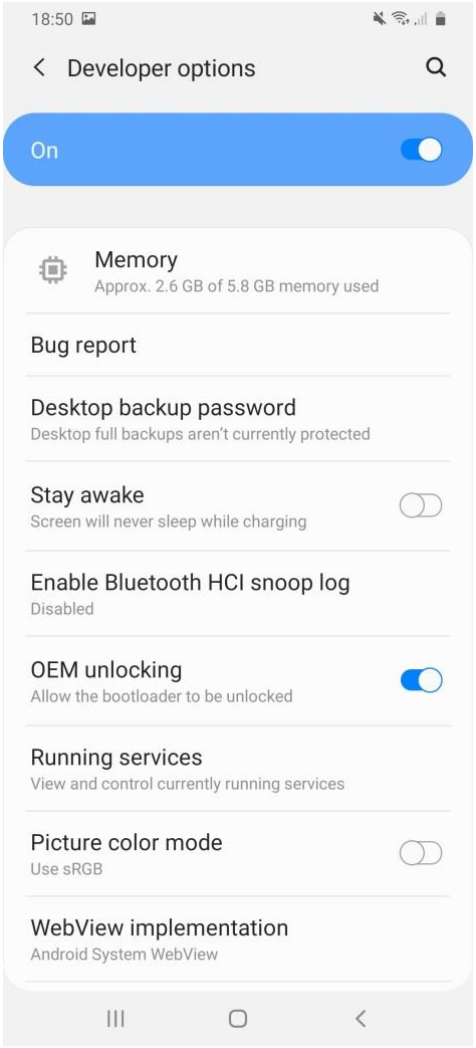
Εικόνα 7 - Developer Options



Εικόνα 8 - Developer Options Allow USB Debugging Question

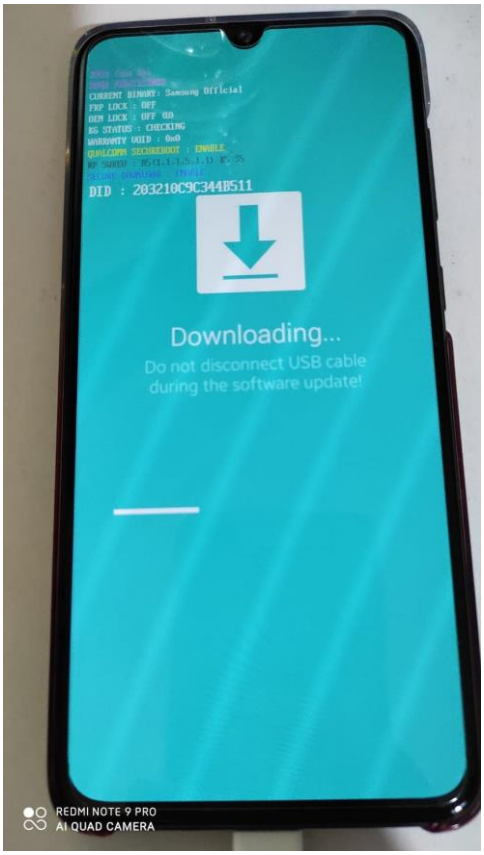


Εικόνα 9 - USB Debugging Ενεργοποιημένο

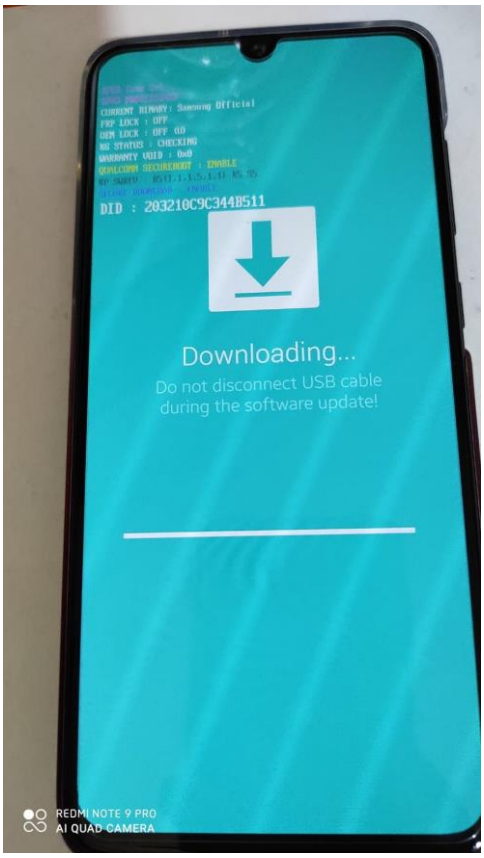


Εικόνα 10 - OEM Unlocking Ενεργοποιημένο

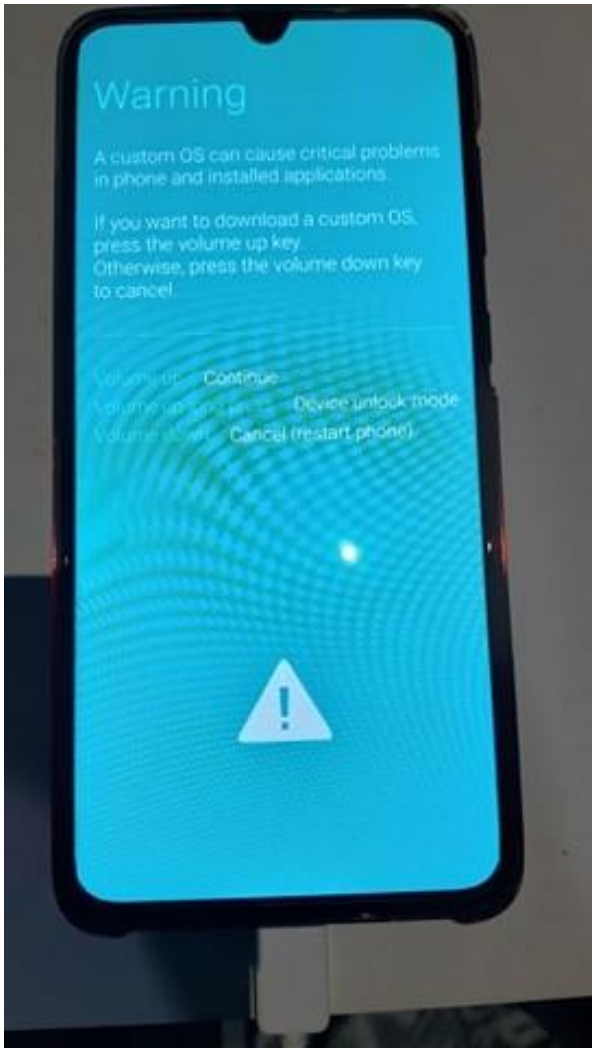
Στην συνέχεια απενεργοποιούμε την συσκευή. Βάζουμε την συσκευή σε Download Mode πατώντας ταυτόχρονα τα κουμπιά volume up και volume down και βάζοντας ταυτόχρονα usb καλώδιο που συνδέεται σε υπολογιστή (Εικόνα 11, Εικόνα 12, Εικόνα 13).



Εικόνα 11 - Download Mode 1

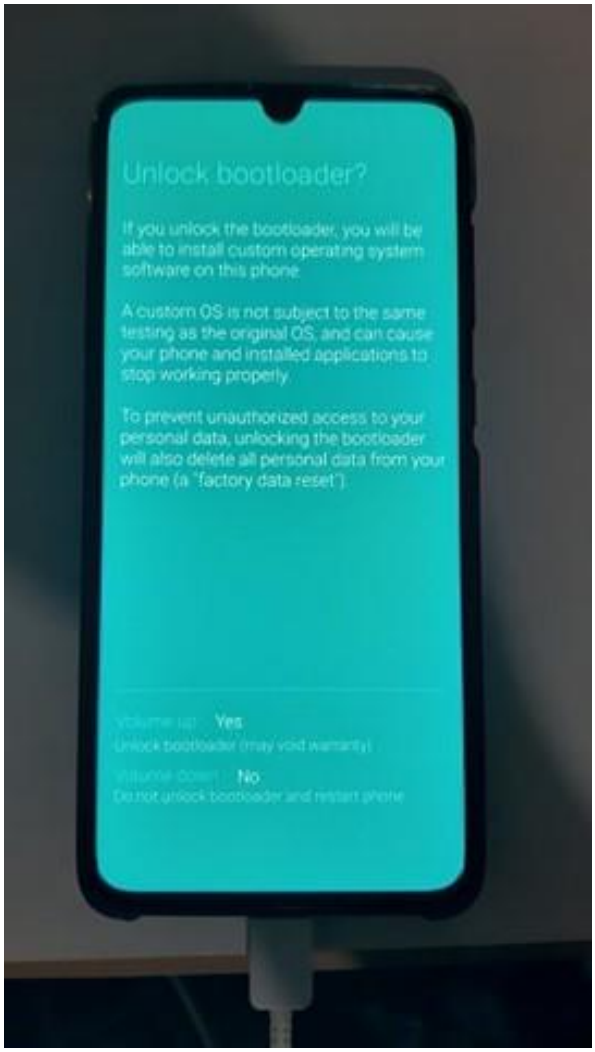


Εικόνα 12 - Download Mode 2

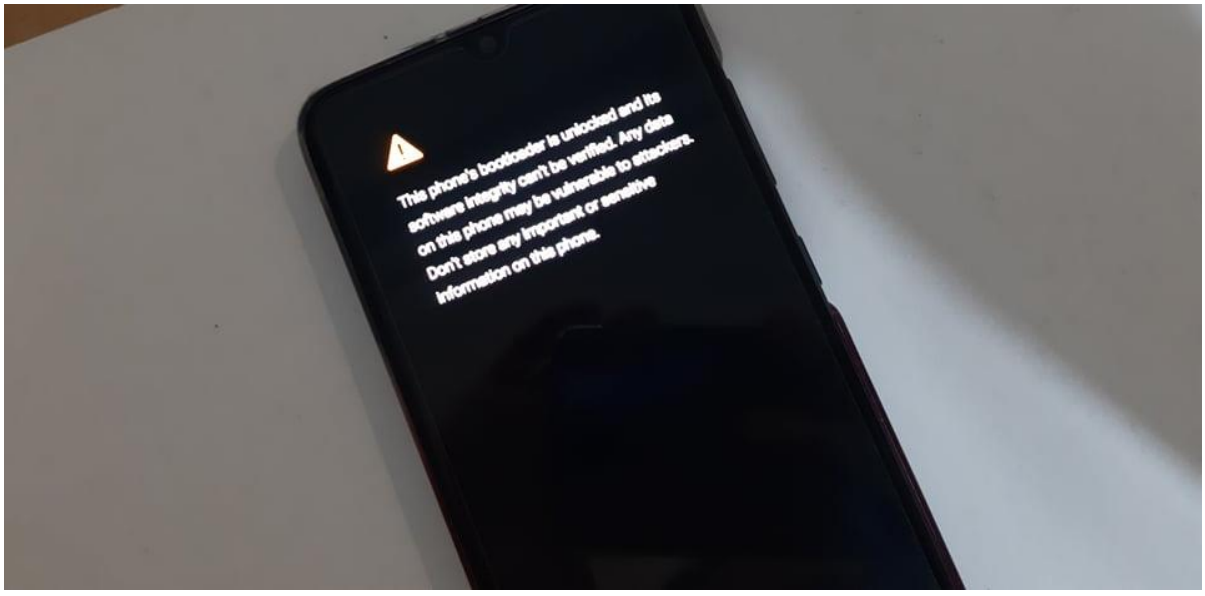


Εικόνα 13 - Download Mode 3

Πατάμε Volume up για να κάνουμε Unlock Bootloader (Εικόνα 14, Εικόνα 15).



Εικόνα 14 - Unlock Bootloader



Εικόνα 15 - Bootloader Unlocked Message

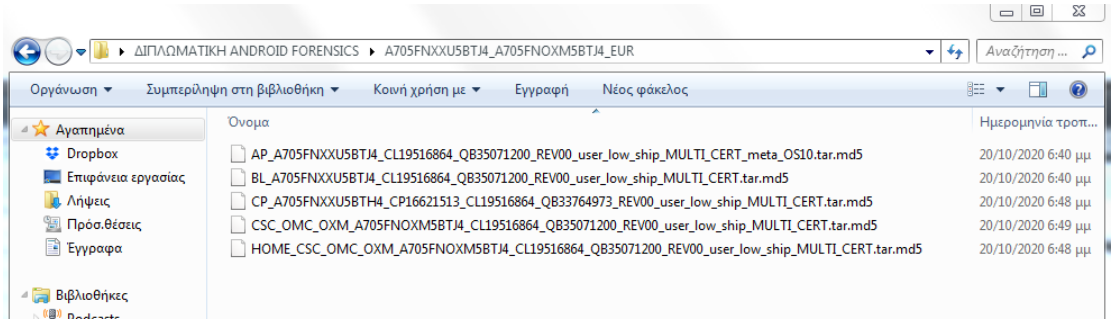
NECESSARY DOWNLOAD FILES

Κατεβάζουμε και εγκαθιστούμε στον υπολογιστή μας τους usb drivers για την κινητή συσκευή μας.

Κατεβάζουμε το λογισμικό Odin3-v3.14.1 που αντιστοιχεί στα android 10.

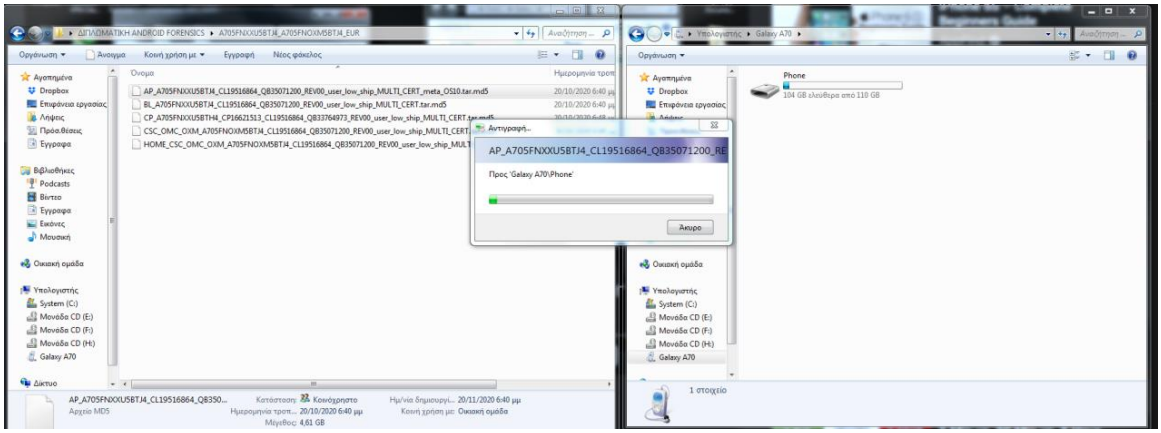
Κατεβάζουμε το κατάλληλο firmware για την συσκευή. Από το Model number της κινητής συσκευής (Εικόνα 16) μπορούμε να αναζητήσουμε στο διαδίκτυο το firmware που αντιστοιχεί σε αυτό (Εικόνα 17).

Εικόνα 16 - Device Model Number



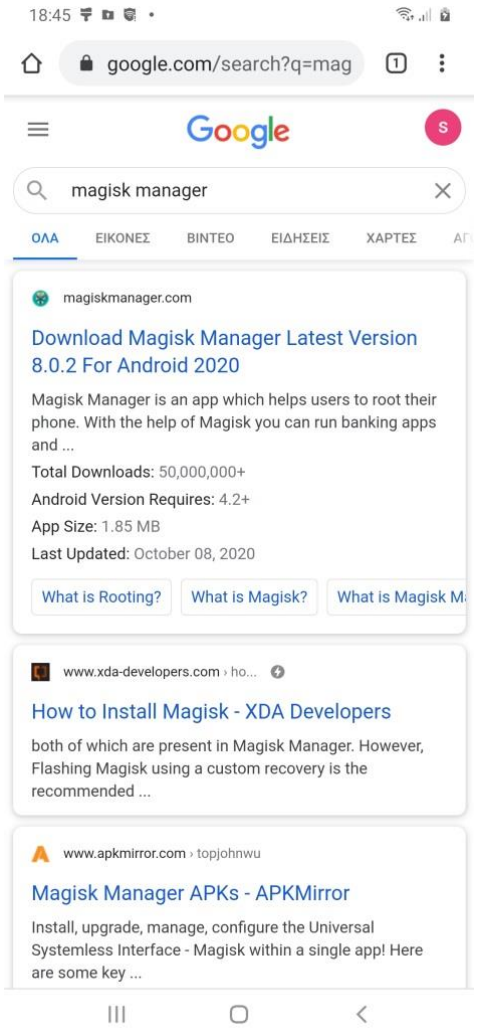
Εικόνα 17 - Firmware Files

Αντιγράφουμε το AP αρχείο στην συσκευή (Εικόνα 18).



Εικόνα 18 - Αντιγραφή AP Αρχείου στην Συσκευή

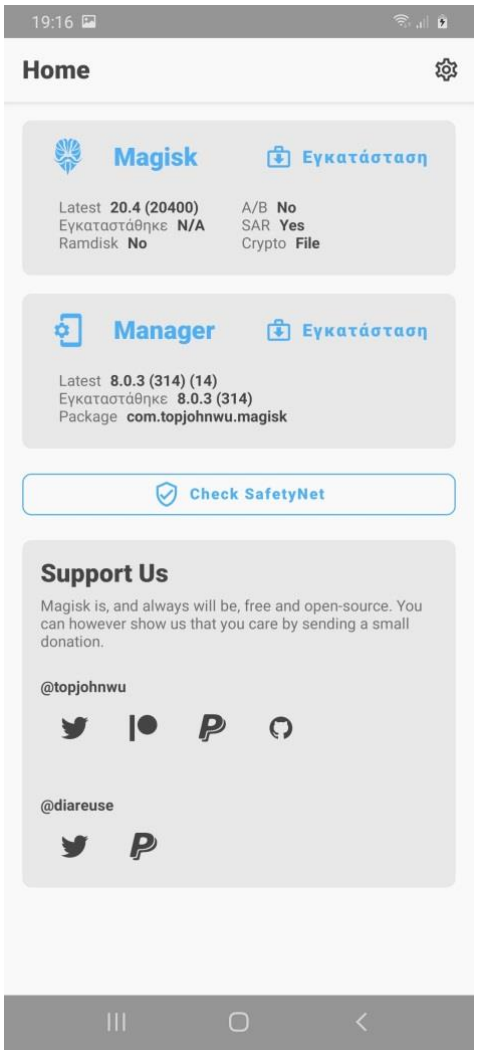
Κατεβάζουμε και εγκαθιστούμε στην συσκευή την εφαρμογή Magisk Manager (Εικόνα 19, Εικόνα 20).



Εικόνα 19 - Magisk Manager Google

Εικόνα 20 - Download Magisk Manager

Εντός της εφαρμογής επιλέγουμε εγκατάσταση για το Magisk (Εικόνα 21).

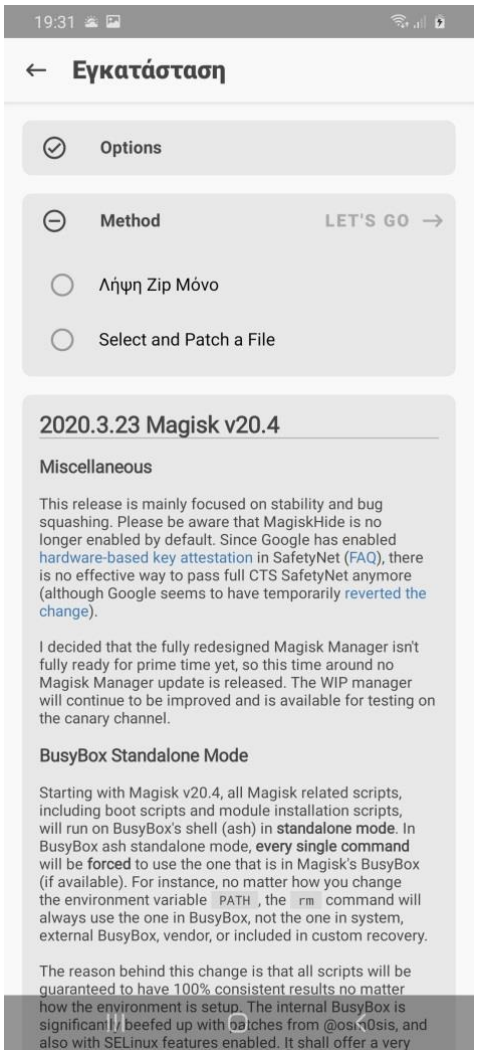


Εικόνα 21 - Magisk Manager Εγκατάσταση (Εντός App)

Επιλέγουμε NEXT (Εικόνα 22).

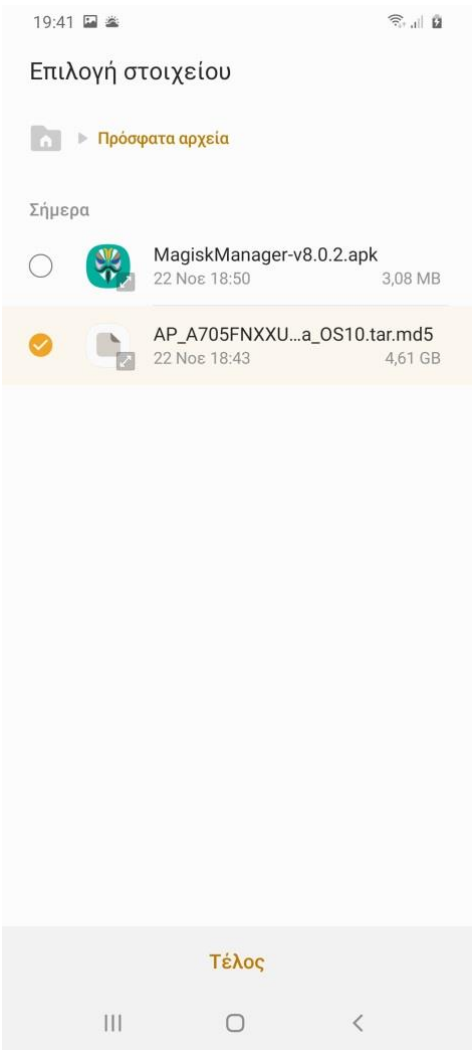
Εικόνα 22 - Magisk Manager NEXT

Στην συνέχεια το Magisk θα ζητήσει ένα αρχείο zip ή ένα patched recovery image. Επιλέγουμε select and patch a file (Εικόνα 23).



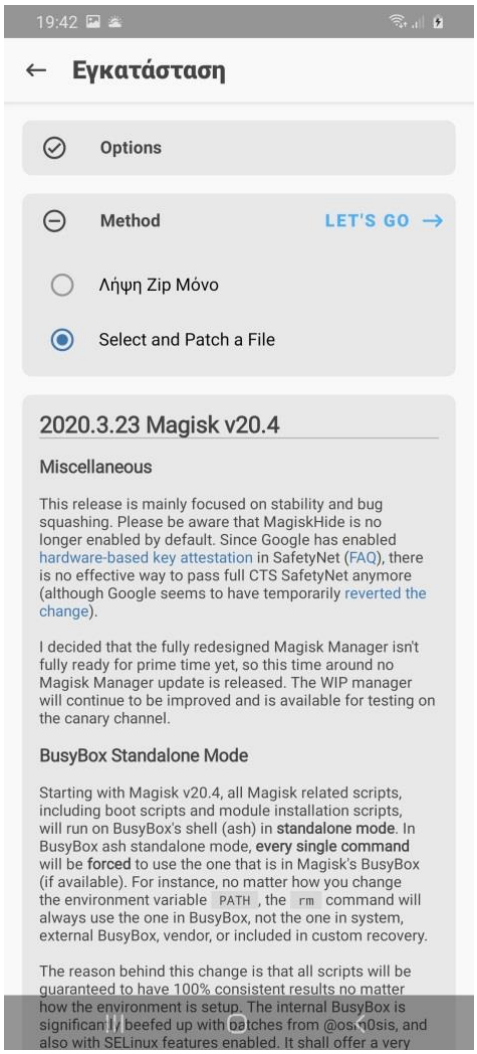
Εικόνα 23 - Magisk Manager Select & Patch a File

Επιλέγουμε το AP αρχείο του firmware που είχαμε αντιγράψει στην συσκευή (Εικόνα 24).



Εικόνα 24 - Magisk Manager Επιλογή AP Αρχείου

Εκκινούμε την διαδικασία (Εικόνα 25, Εικόνα 26).



Εικόνα 25 - Magisk Manager Έναρξη Διαδικασίας Patch

Εικόνα 26 - Magisk Manager Πρόοδος Διαδικασίας

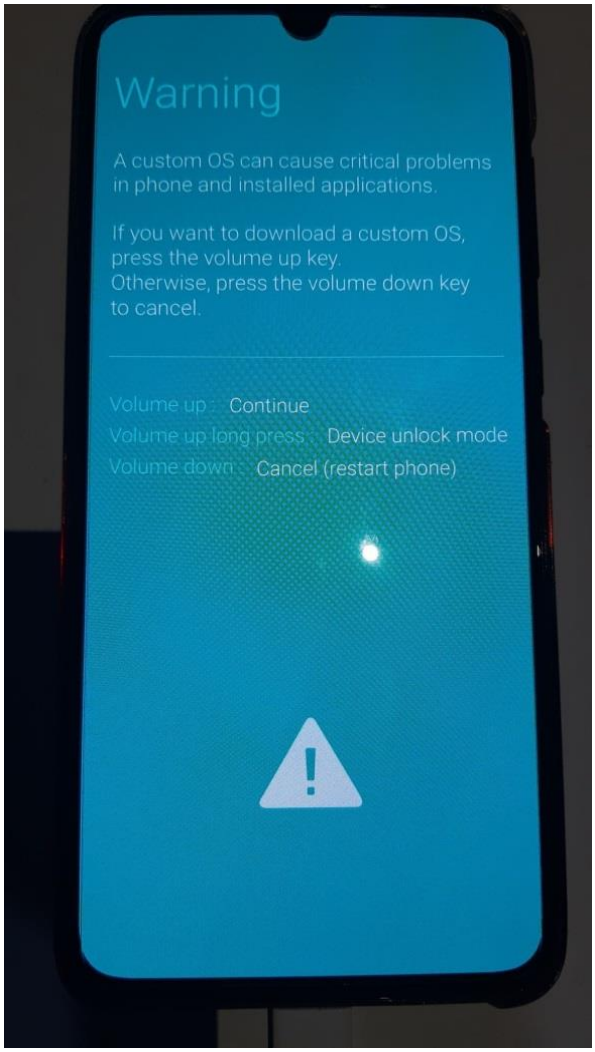
Το αρχείο που προκύπτει το αντιγράφουμε στον υπολογιστή μας από την συσκευή καθώς θα το χρησιμοποιήσουμε στην συνέχεια.

ODIN

Για να κάνουμε flash τα αρχεία στην συσκευή χρησιμοποιήσαμε το Odin3-v3.14.1 που αντιστοιχεί στα android 10. Χρησιμοποιώντας το συγκεκριμένο λογισμικό μπορεί κανείς να εγκαταστήσει επίσημο firmware της Samsung σε κινητές συσκευές, να εγκαταστήσει custom roms, να κατεβάσει τις τελευταίες ενημερώσεις για kernels και να αποκτήσει root πρόσβαση σε κινητές συσκευές.

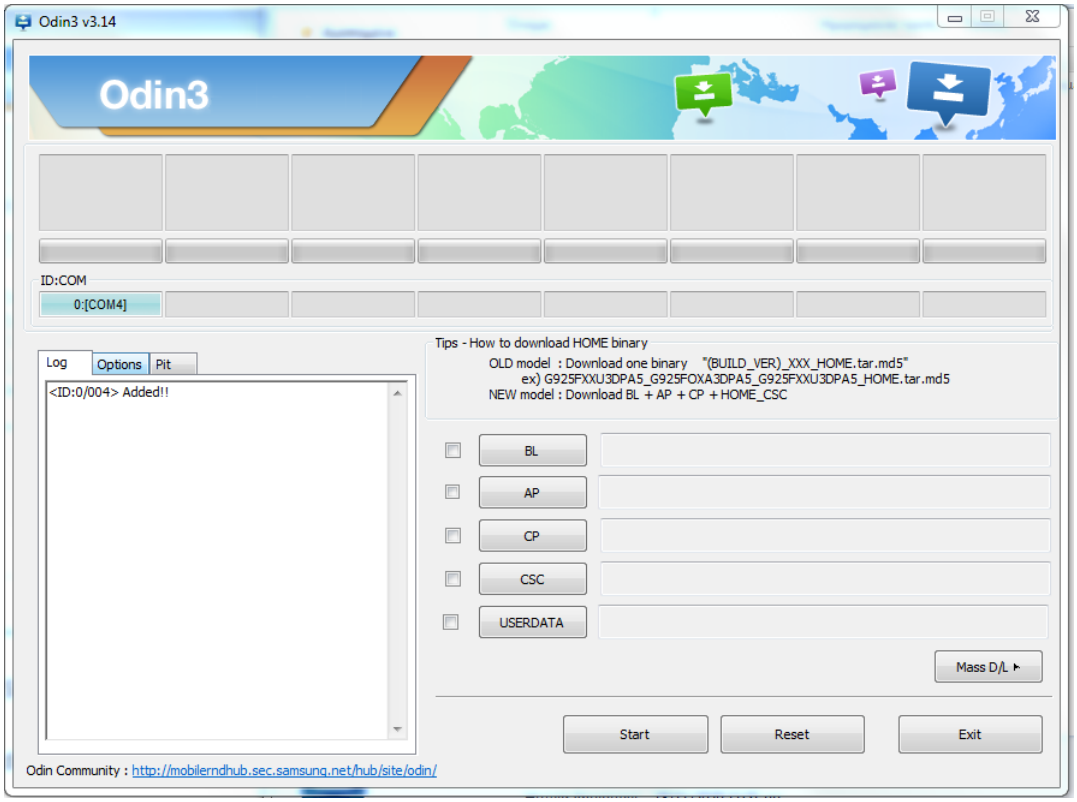
Απενεργοποιούμε την συσκευή και την βάζουμε σε Download mode πατώντας ταυτόχρονα το volume up και volume down και συνδέοντας την συσκευή στον υπολογιστή με usb καλώδιο.

Στο warning που εμφανίζεται (Εικόνα 27) αφού βάλουμε την συσκευή σε Download mode πατάμε volume up για να συνεχίσουμε.



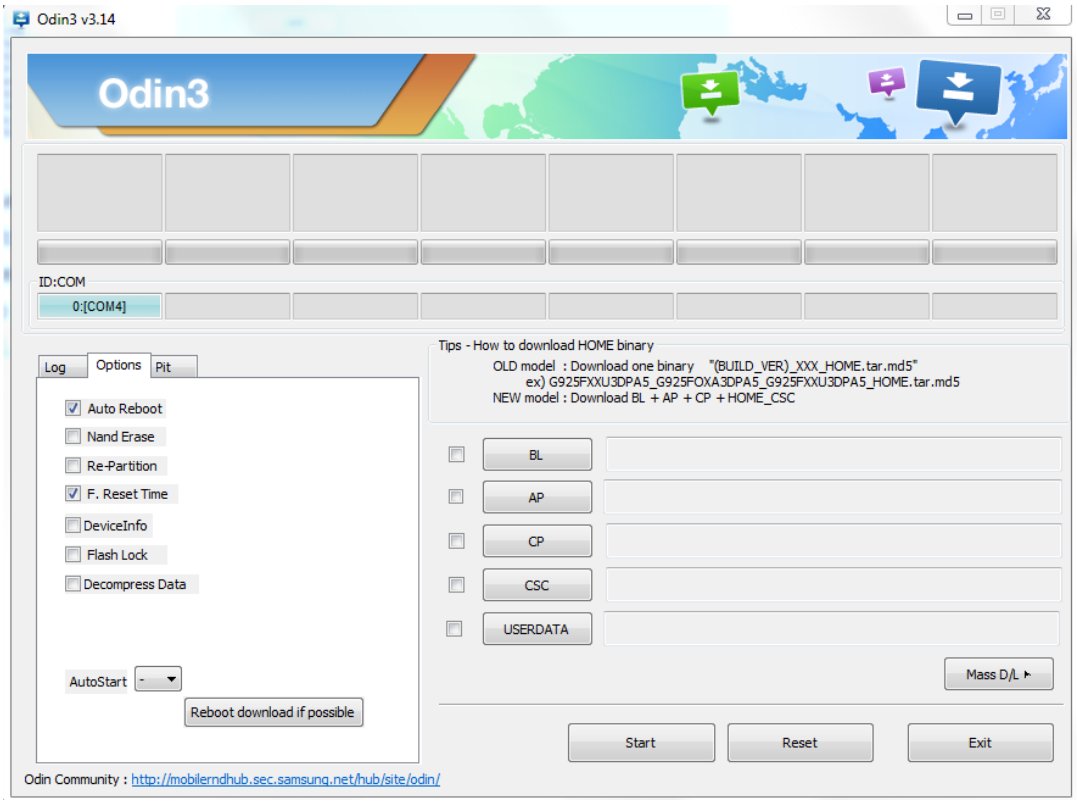
Εικόνα 27 - Download Mode Warning

Ανοίγουμε το Odin που θα πρέπει να εμφανίσει το μήνυμα Added για να έχει αναγνωρίσει σωστά την συσκευή (Εικόνα 28).

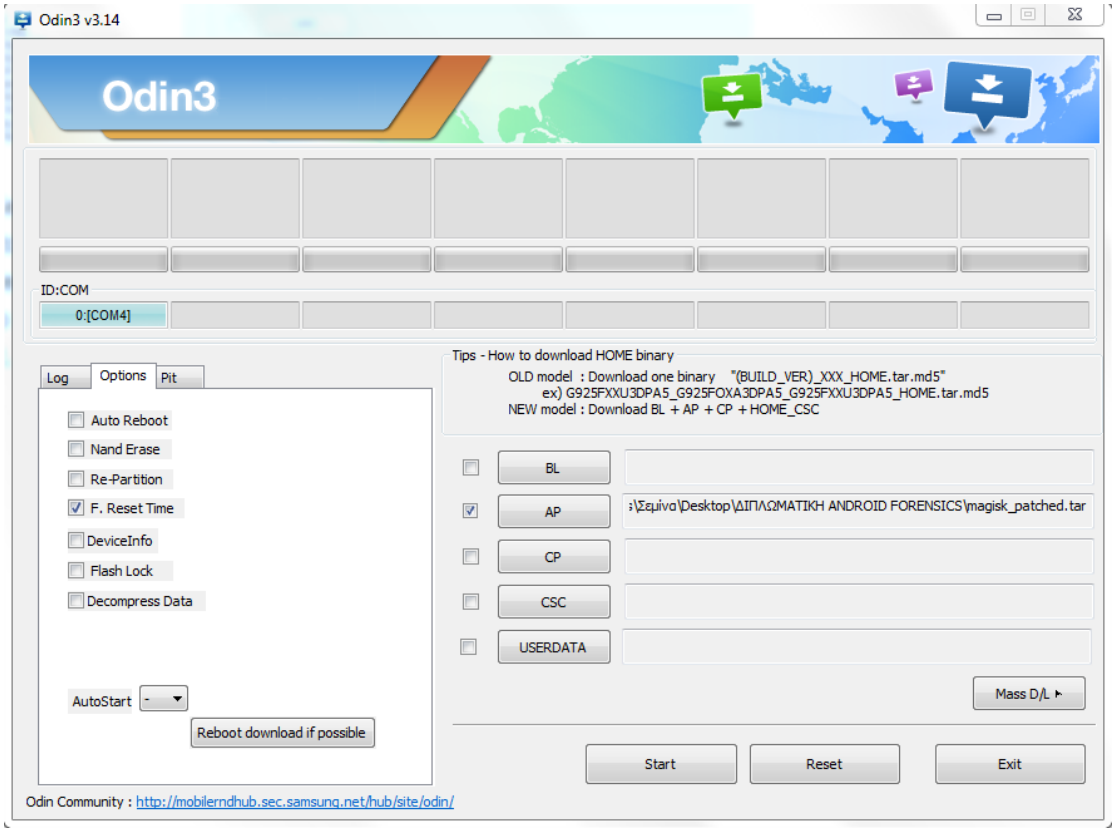


Εικόνα 28 - Odin Added Message

Στην καρτέλα Options αποεπιλέγουμε το Auto Reboot (Εικόνα 29). Πατάμε το κουμπί AP και επιλέγουμε το αρχείο magisk_patched.tar (Εικόνα 30).



Εικόνα 29 - Odin Auto Reboot Αποεπιλογή



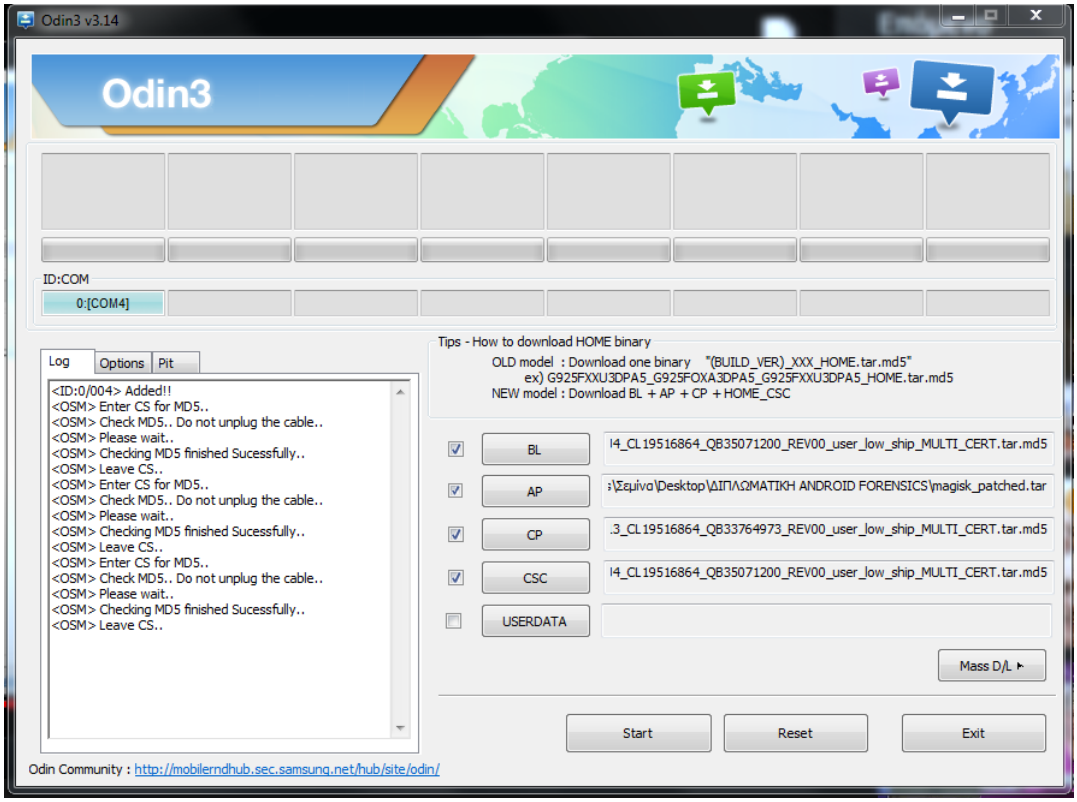
Εικόνα 30 - Odin Επιλογή AP magisk_patched.tar

Στην συνέχεια επιλέγουμε τα αντίστοιχα firmware αρχεία στις υπόλοιπες επιλογές (Εικόνα 31) του Odin από το firmware που είχαμε κάνει download:

BL

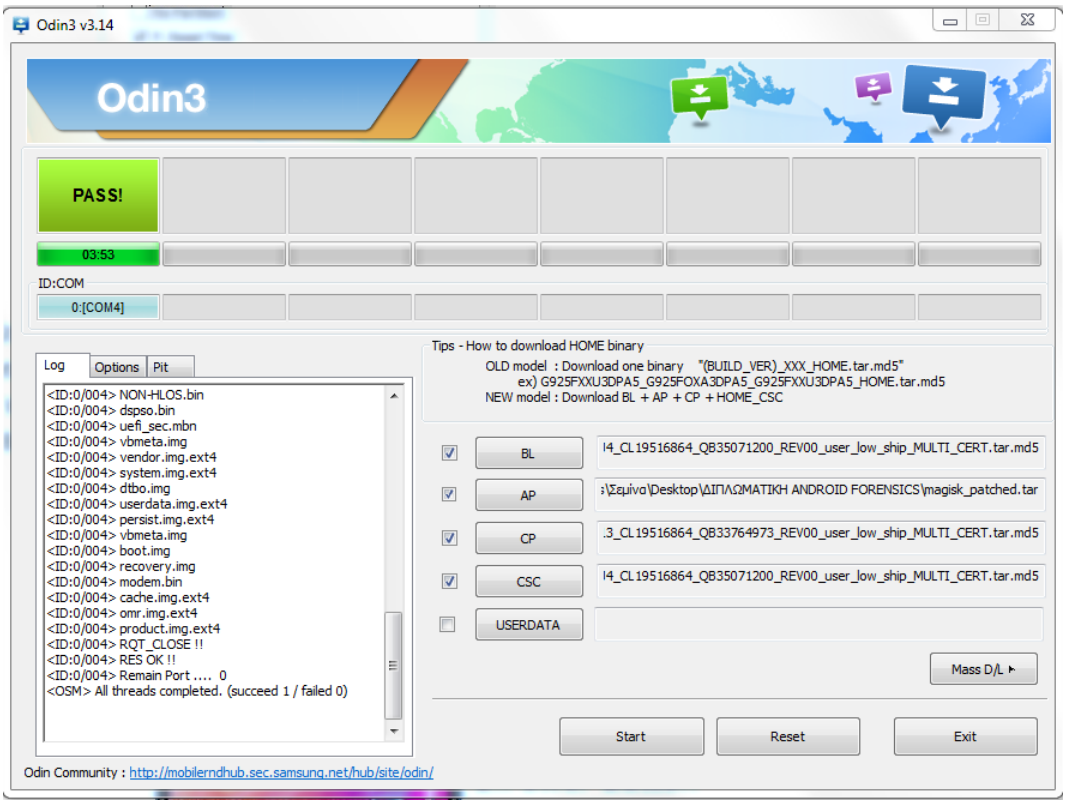
CP

CSC



Εικόνα 31 - Odin Επιλογή Υπόλοιπων Αρχείων Firmware

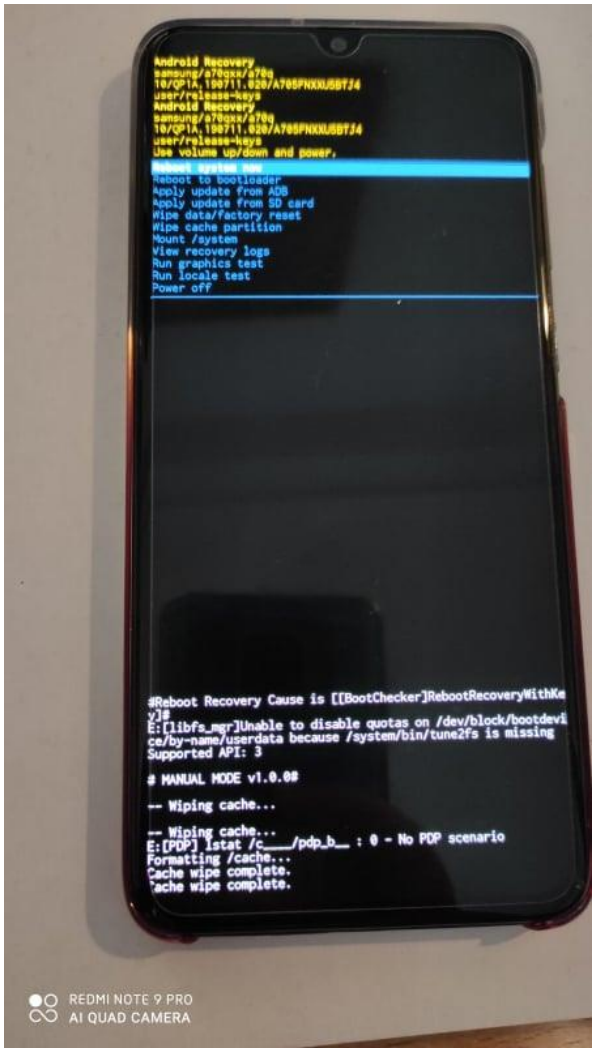
Πατάμε Start για να ξεκινήσει η διαδικασία, μόλις ολοκληρωθεί το Odin θα μας εμφανίσει μήνυμα Pass (Εικόνα 32).



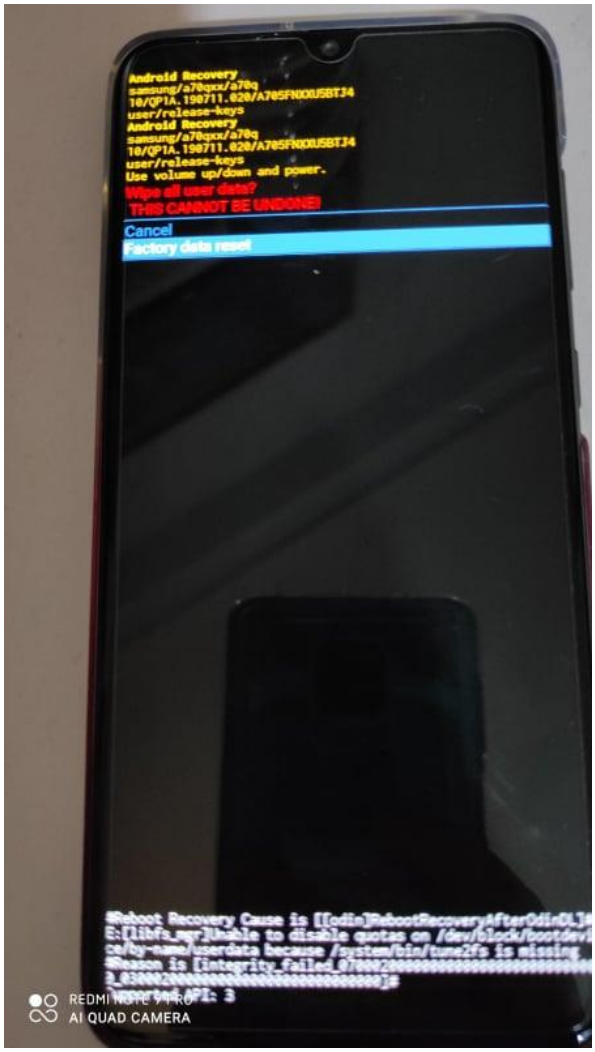
Εικόνα 32 - Odin PASS! Message

Μόλις ολοκληρωθεί η διαδικασία πατάμε το Volume down και το power button για να βγούμε από το Download mode και όταν σβήσει η οθόνη πατάμε κατευθείαν το volume up και το power για να μπούμε στο recovery mode .

Από το μενού που εμφανίζεται επιλέγουμε wipe data/factory reset (Εικόνα 33, Εικόνα 34) έτσι ολοκληρώνουμε την διαδικασία απόκτησης root πρόσβασης στην συσκευή , αυτό θα σβήσει όλα τα δεδομένα στην συσκευή.



Εικόνα 33 - Wipe Data / Factory Reset 1



Εικόνα 34 - Wipe Data / Factory Reset 2

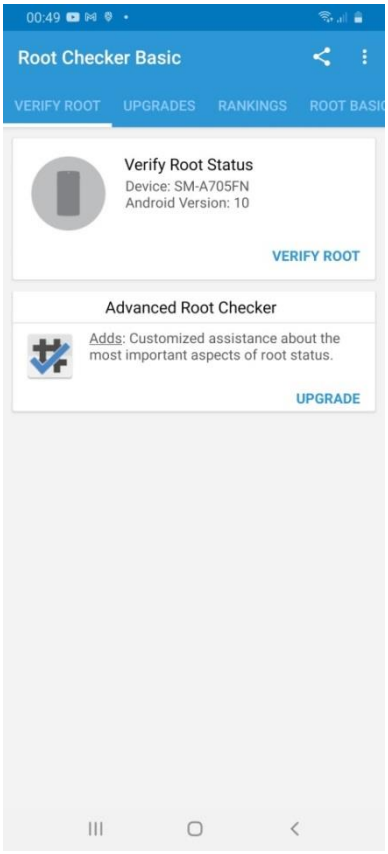
Για να επανεκκινήσουμε την συσκευή σε rooted os πατάμε παρατεταμένα το volume up και το power και τα αφήνουμε όταν εμφανιστεί το bootloader warning.

Η rooted συσκευή πλέον θα πρέπει να σεταριστεί από την αρχή.

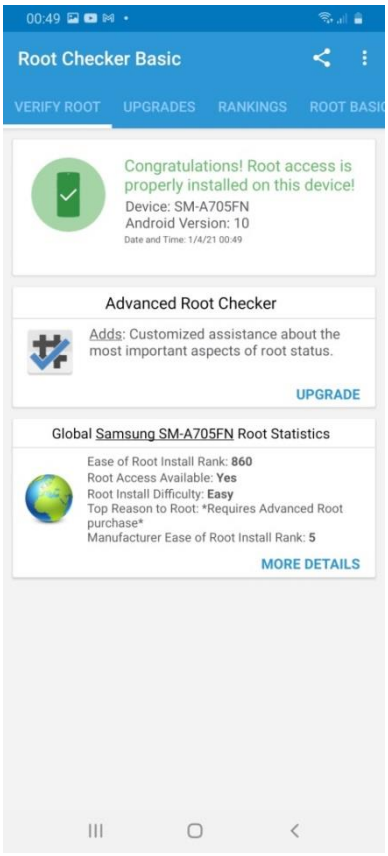
VERIFY ROOT ACCESS

Κατεβάζουμε και εγκαθιστούμε στην συσκευή την εφαρμογή Root Checker από το Play Store για να επαληθεύσουμε εάν πραγματοποιήσαμε με επιτυχία την διαδικασία στην συσκευή.

Στην εφαρμογή Root Checker επιλέγουμε VERIFY ROOT και μας εμφανίζει ότι η διαδικασία της απόκτησης root πρόσβασης στην συσκευή έχει πραγματοποιηθεί με επιτυχία (Εικόνα 35, Εικόνα 36).



Εικόνα 35 - Root Checker App 1

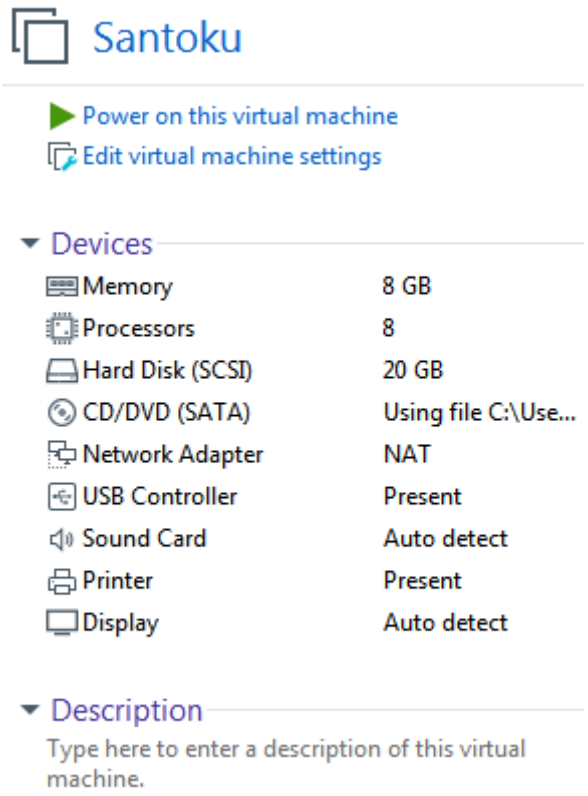


Εικόνα 36 - Root Checker App 2

1.3 Santoku

Για την συνέχεια της έρευνας χρησιμοποιήθηκε το Santoku σαν περιβάλλον workstation, αναλυτικότερα χρησιμοποιήθηκε στις διαδικασίες παράκαμψης ασφάλειας και κλειδώματος οθόνης, στο AFLogical και στο physical image acquisition.

Το Santoku είναι μια open source πλατφόρμα βασισμένη στο Linux. Η έκδοση του Santoku που χρησιμοποιήθηκε για την διενέργεια της έρευνας ήταν η 0.5 εγκατεστημένη σε Virtual Machine που έτρεχε σε περιβάλλον VMware Workstation 15 Pro (Εικόνα 37).



Εικόνα 37 - Santoku VM Settings

Το Santoku παρέχει μια σουίτα εργαλείων στους χρήστες που αφορούν τους τομείς (Hoog, 2013):

- Mobile Forensics

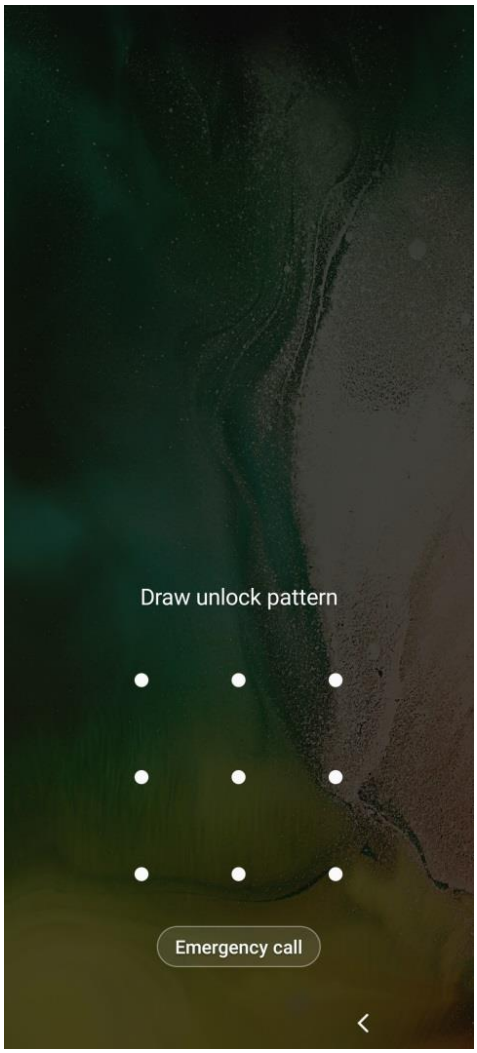
- Mobile Malware Analysis

- Mobile Securtiy Testing

2. ΠΑΡΑΚΑΜΨΗ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΚΛΕΙΔΩΜΑΤΟΣ ΟΘΟΝΗΣ

2.1 Pattern

Έστω ότι η αρχική οθόνη της συσκευής μας είναι κλειδωμένη με pattern (Εικόνα 38).



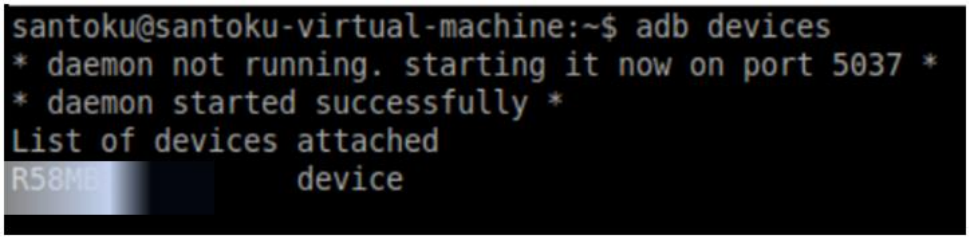
Εικόνα 38 - Pattern Lock Screen

Από το workstation μας συνδεόμαστε στην συσκευή με su shell. Οι εντολές που χρησιμοποιούμε είναι:

adb devices : αναγνώριση της συσκευής (Εικόνα 39)

adb shell : απόκτηση shell στην συσκευή (Εικόνα 40)

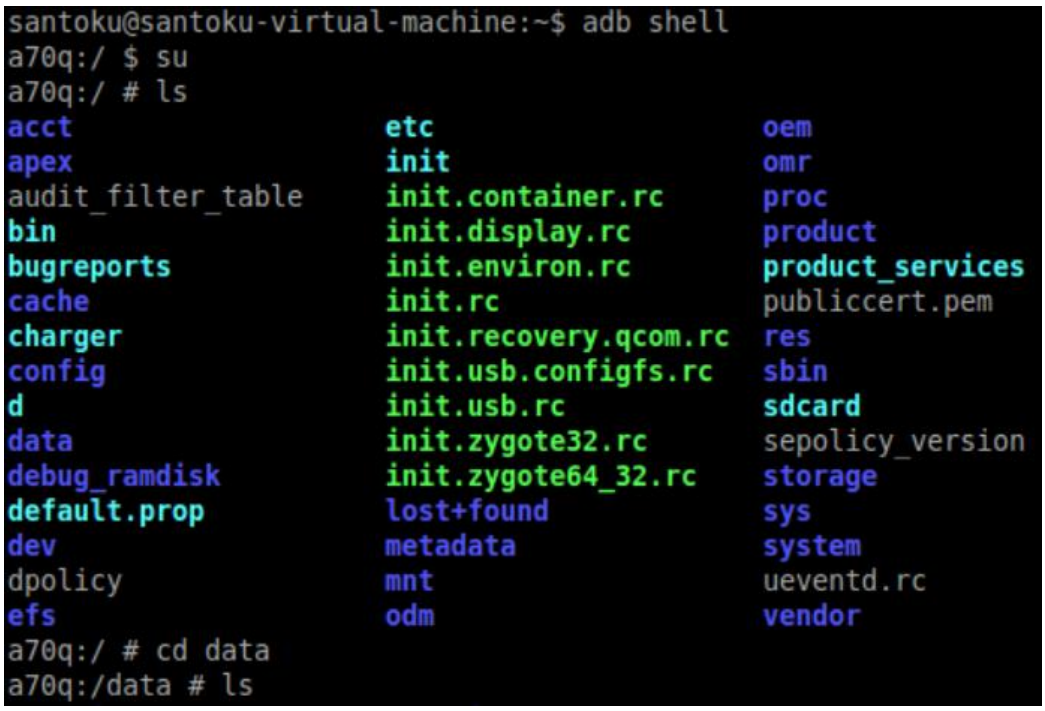
su : απόκτηση su shell στην συσκευή (Εικόνα 40)



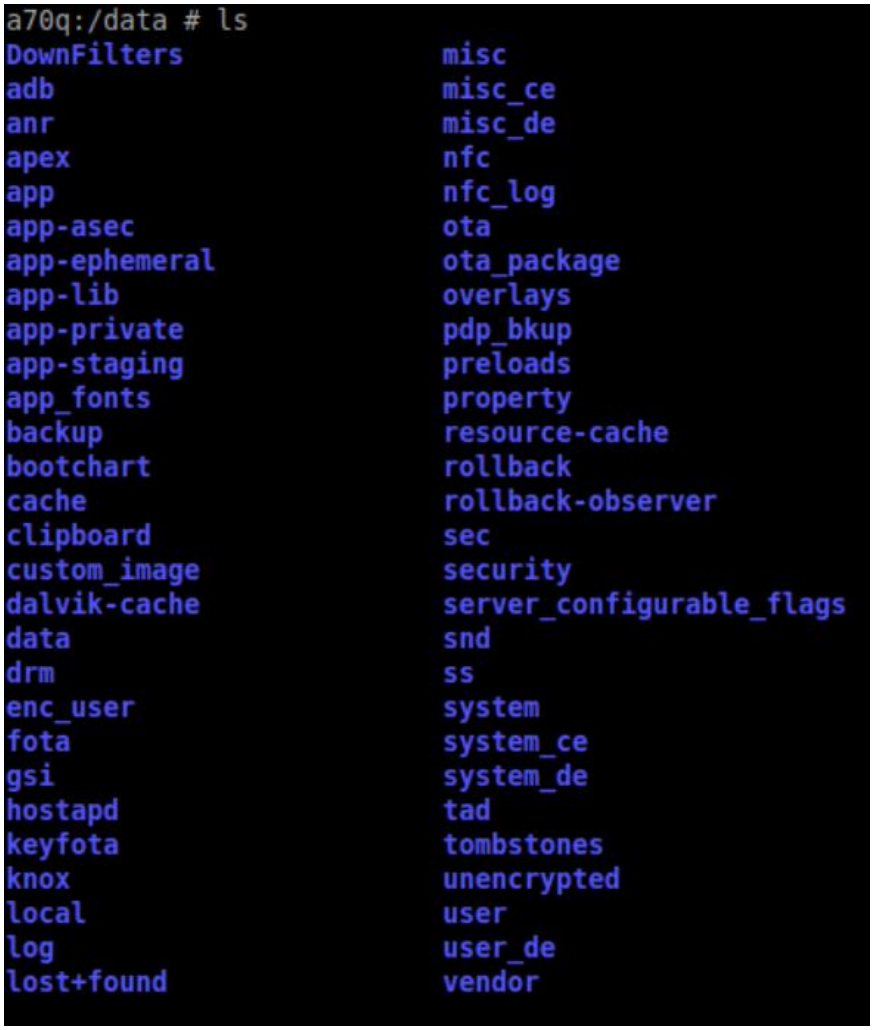
Εικόνα 39 - Pattern Removal - adb devices

Μετακινούμαστε στο directory data (Εικόνα 40):

cd data



Εικόνα 40 – Pattern Removal - cd data



Εικόνα 41 – Pattern Removal - Data Directory ls

Μετακινούμαστε στο directory system (Εικόνα 42):

cd system

Βρισκόμαστε στο directory /data/system , στο συγκεκριμένο directory βρίσκονται τα αρχεία που θα διαγράψουμε.

Διαγράφουμε τα ακόλουθα αρχεία χρησιμοποιώντας την εντολή rm και το όνομα του αρχείου:

gatekeeper.password.key : περιέχει τη σύνοψη του PIN

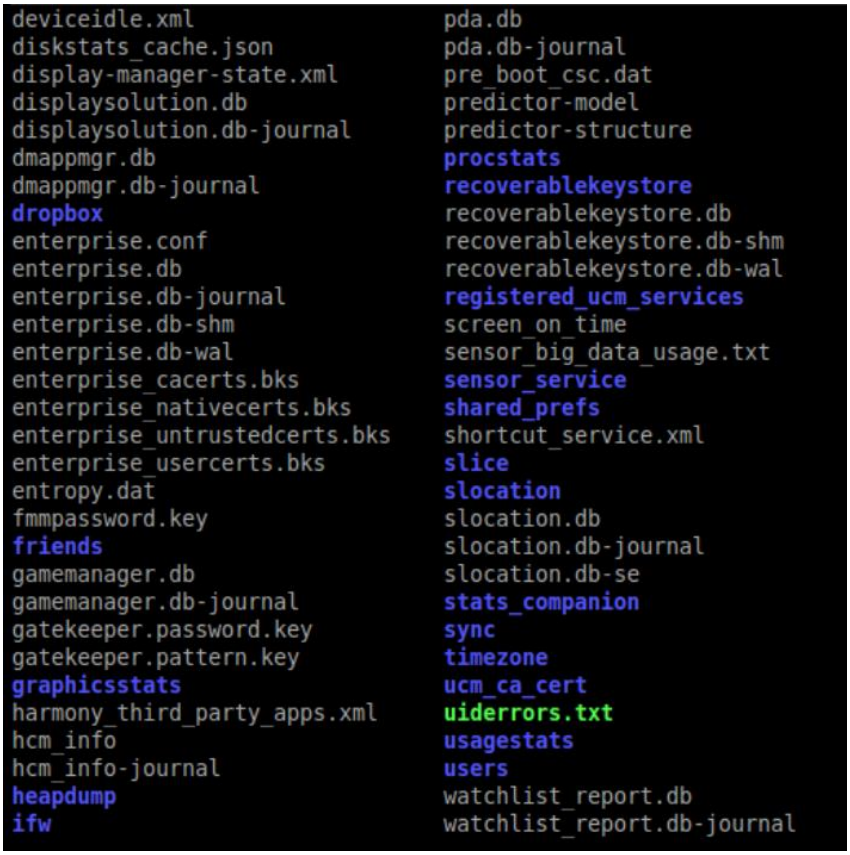
gatekeeper.pattern.key :περιέχει τη σύνοψη του μοτίβου

locksettings.db :αποθηκεύεται το salt

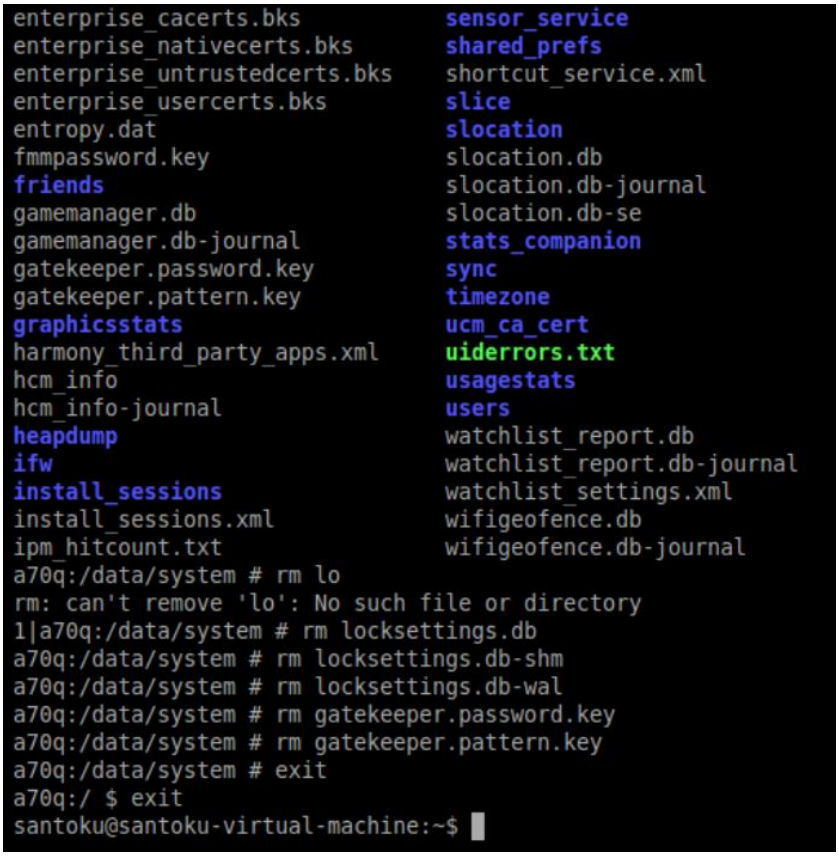
Επιπρόσθετα διαγράφουμε και τα αρχεία locksettings.db-shm και locksettings.db-wal (Εικόνα 42, Εικόνα 43, Εικόνα 44).

```
a70q:/data # cd system
a70q:/data/system # ls
HWParamTime.bin                 ipm_input_data.txt
PkgPredictions.db               job
PkgPredictions.db-journal       last-fstrim
SimCard.dat                     last-header.txt
WifiHistory.db                  locksettings.db
WifiHistory.db-journal          locksettings.db-shm
analytics.db                    locksettings.db-wal
analytics.db-journal            log-files.xml
appops.xml                      ndebugsocket
audioservice_sec.db             netpolicy.xml
audioservice_sec.db-journal     netstats
battery-history                 notification_log.db
battery-saver                   notification_log.db-journal
batterystats-checkin.bin        notification_policy.xml
batterystats-daily.xml          overlays.xml
batterystats.bin                package-cstats.list
big_data_sensor_usage_pkg.txt   package-dcl.list
big_data_usage_call_gesture.txt package-dex-usage.list
bigdata-pkgaccuracy             package-usage.list
cachequota.xml                  package-watchdog.xml
clipboardimage.db               package_cache
clipboardimage.db-journal       packages-warnings.xml
container                       packages.list
conventionalmode                packages.xml
device_policies.xml             packages.xml.mbak
deviceidle.xml                  pda.db
diskstats_cache.json            pda.db-journal
display-manager-state.xml       pre_boot_csc.dat
```

Εικόνα 42 – Pattern Removal - Directory /data/system ls 1



Εικόνα 43 - Pattern Removal - Directory /data/system ls 2



Εικόνα 44 - Pattern Removal - Directory /data/system Delete Files

Κάνουμε επανεκκίνηση της συσκευής (Εικόνα 45).

```
a70q:/data/system # exit
a70q:/ $ exit
santoku@santoku-virtual-machine:~$ adb reboot
santoku@santoku-virtual-machine:~$
```

Εικόνα 45 - Pattern Removal - Reboot Device

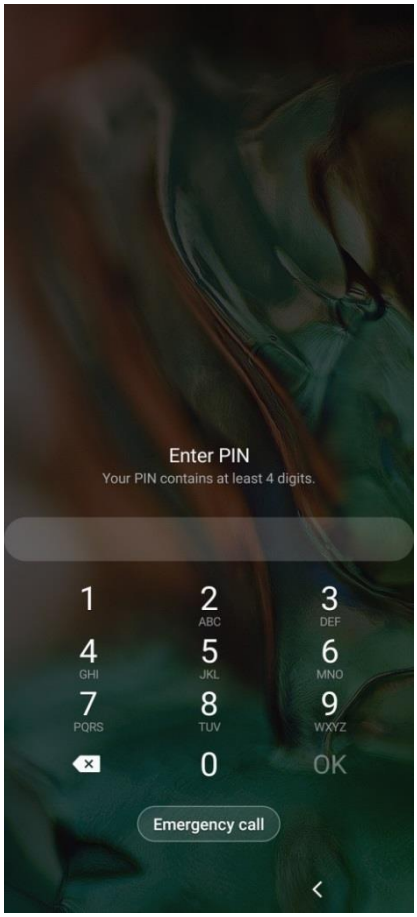
Η διαγραφή του pattern ήταν επιτυχής (Εικόνα 46, Εικόνα 47).

Εικόνα 46 - Pattern Removed Lock Screen 1

Εικόνα 47 - Pattern Removed Lock Screen 2

2.2 Pin

Έστω ότι η αρχική οθόνη της συσκευής μας είναι κλειδωμένη με pin (Εικόνα 48).



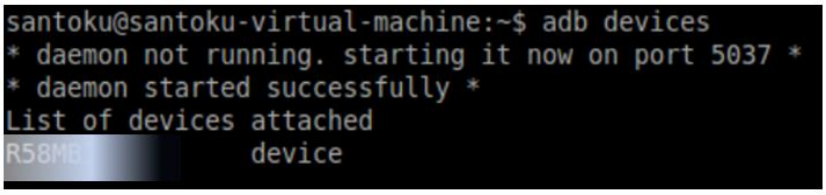
Εικόνα 48 - Pin Lock Screen

Από το workstation μας συνδεόμαστε στην συσκευή με su shell. Οι εντολές που χρησιμοποιούμε είναι (Εικόνα 49, Εικόνα 50):

adb devices

adb shell

su



Εικόνα 49 - Pin Removal - adb devices

```
santoku@santoku-virtual-machine:~$ adb shell
a70q:/ $ su
```

Εικόνα 50 - Pin Removal - su shell

Μετακινούμαστε στο directory /data/system (Εικόνα 51, Εικόνα 52).

Από το συγκεκριμένο directory διαγράφουμε τα αρχεία locksettings.db locksettings.db-shm και locksettings.db-wal (Εικόνα 53).

Τα αρχεία gatekeeper.password.key και gatekeeper.pattern.key δεν υπάρχουν στο directory εφόσον έχει γίνει ήδη διαγραφή κατά την αφαίρεση του pattern, σε περίπτωση που δεν τα είχαμε ήδη διαγράψει προηγουμένως θα υπήρχαν και θα έπρεπε να διαγράψουμε κα αυτά πάλι.

```
a70q:/data # cd system
a70q:/data/system # ls
HWParamTime.bin                 last-fstrim
PkgPredictions.db               last-header.txt
PkgPredictions.db-journal       locksettings.db
SimCard.dat                     locksettings.db-shm
WifiHistory.db                  locksettings.db-wal
WifiHistory.db-journal          log-files.xml
analytics.db                    ndebugsocket
analytics.db-journal            netpolicy.xml
appops.xml                      netstats
audioservice_sec.db             notification_log.db
audioservice_sec.db-journal     notification_log.db-journal
battery-history                 notification_policy.xml
battery-saver                   overlays.xml
batterystats-checkin.bin        package-cstats.list
batterystats-daily.xml          package-dcl.list
batterystats.bin                package-dex-usage.list
big_data_sensor_usage_pkg.txt   package-usage.list
big_data_usage_call_gesture.txt package-watchdog.xml
bigdata-pkgaccuracy             package_cache
cachequota.xml                  packages-warnings.xml
clipboardimage.db               packages.list
clipboardimage.db-journal       packages.xml
container                       packages.xml.mbak
conventionalmode                pda.db
device_policies.xml             pda.db-journal
deviceidle.xml                  pre_boot_csc.dat
diskstats_cache.json            predictor-model
display-manager-state.xml       predictor-structure
```

Εικόνα 51 - Pin Removal - Directory /data/system ls 1

```
displaysolution.db                procstats
displaysolution.db-journal        recoverablekeystore
dmappmgr.db                       recoverablekeystore.db
dmappmgr.db-journal               recoverablekeystore.db-shm
dropbox                           recoverablekeystore.db-wal
enterprise.conf                   registered_ucm_services
enterprise.db                     screen_on_time
enterprise.db-journal             sensor_big_data_usage.txt
enterprise.db-shm                 sensor_service
enterprise.db-wal                 shared_prefs
enterprise_cacerts.bks            shortcut_service.xml
enterprise_nativecerts.bks        slice
enterprise_untrustedcerts.bks     slocation
enterprise_usercerts.bks          slocation.db
entropy.dat                       slocation.db-journal
fmmpassword.key                   slocation.db-se
friends                           stats_companion
gamemanager.db                    storage.xml
gamemanager.db-journal            sync
graphicsstats                     timezone
harmony_third_party_apps.xml      ucm_ca_cert
hcm_info                          uiderrors.txt
hcm_info-journal                  usagestats
heapdump                          users
ifw                               watchlist_report.db
install_sessions                  watchlist_report.db-journal
install_sessions.xml              watchlist_settings.xml
ipm_hitcount.txt                  wifigeofence.db
ipm_input_data.txt                wifigeofence.db-journal
job
```

Εικόνα 52 - Pin Removal - Directory /data/system ls 2

```
a70q:/data/system # rm locksettings.db
a70q:/data/system # rm locksettings.db-wal
a70q:/data/system # rm locksettings.db-shm
a70q:/data/system # exit
a70q:/ $ exit
```

Εικόνα 53 - Pin Removal - Directory /data/system Delete Files

Κάνουμε επανεκκίνηση της συσκευής (Εικόνα 54).

```
a70q:/data/system # exit
a70q:/ $ exit
santoku@santoku-virtual-machine:~$ adb reboot
santoku@santoku-virtual-machine:~$
```

Εικόνα 54 - Pin Removal - Reboot Device

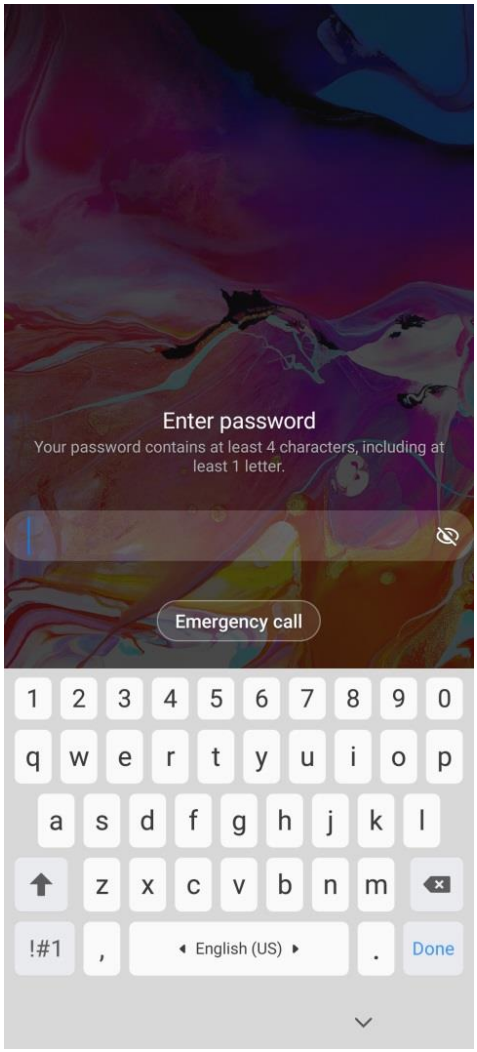
Η διαγραφή του pin ήταν επιτυχής (Εικόνα 55, Εικόνα 56).

Εικόνα 55 - Pin Removed Lock Screen 1

Εικόνα 56 - Pin Removed Lock Screen 2

2.3 Password

Έστω ότι η αρχική οθόνη της συσκευής μας είναι κλειδωμένη με password(Εικόνα 57).



Εικόνα 57 - Password Lock Screen

Από το workstation μας συνδεόμαστε στην συσκευή με su shell (Εικόνα 58).

```
santoku@santoku-virtual-machine:~$ adb devices
List of devices attached
R58MB[redacted]        device

santoku@santoku-virtual-machine:~$ adb shell
a70q:/ $ su
```

Εικόνα 58 - Password Removal - adb devices & su shell

Μετακινούμαστε στο directory /data/system (Εικόνα 59).

```
a70q:/ # cd data
a70q:/data # cd system
```

Εικόνα 59 - Password Removal - cd /data/system

Από το συγκεκριμένο directory διαγράφουμε τα αρχεία locksettings.db locksettings.db-shm και locksettings.db-wal (Εικόνα 60, Εικόνα 61, Εικόνα 62).

Τα αρχεία gatekeeper.password.key και gatekeeper.pattern.key δεν υπάρχουν στο directory εφόσον έχει γίνει ήδη διαγραφή κατά την αφαίρεση του pattern, σε περίπτωση που δεν τα είχαμε ήδη διαγράψει προηγουμένως θα υπήρχαν και θα έπρεπε να διαγράψουμε κα αυτά πάλι.

```
a70q:/data/system # ls
HWParamTime.bin                 last-fstrim
PkgPredictions.db               last-header.txt
PkgPredictions.db-journal       locksettings.db
SimCard.dat                     locksettings.db-shm
WifiHistory.db                  locksettings.db-wal
WifiHistory.db-journal          log-files.xml
analytics.db                    ndebugsocket
analytics.db-journal            netpolicy.xml
appops.xml                      netstats
audioservice_sec.db             notification_log.db
audioservice_sec.db-journal     notification_log.db-journal
battery-history                 notification_policy.xml
battery-saver                   overlays.xml
batterystats-checkin.bin        package-cstats.list
batterystats-daily.xml          package-dcl.list
batterystats.bin                package-dex-usage.list
big_data_sensor_usage_pkg.txt   package-usage.list
big_data_usage_call_gesture.txt package-watchdog.xml
bigdata-pkgaccuracy             package_cache
cachequota.xml                  packages-warnings.xml
clipboardimage.db               packages.list
clipboardimage.db-journal       packages.xml
container                       packages.xml.mbak
conventionalmode                pda.db
device_policies.xml             pda.db-journal
deviceidle.xml                  pre_boot_csc.dat
diskstats_cache.json            predictor-model
display-manager-state.xml       predictor-structure
displaysolution.db              procstats
```

Εικόνα 60 - Password Removal - Directory /data/system ls 1

```
displaysolution.db-journal      recoverablekeystore
dmappmgr.db                     recoverablekeystore.db
dmappmgr.db-journal             recoverablekeystore.db-shm
dropbox                         recoverablekeystore.db-wal
enterprise.conf                 registered_ucm_services
enterprise.db                   screen_on_time
enterprise.db-journal           sensor_big_data_usage.txt
enterprise.db-shm               sensor_service
enterprise.db-wal               shared_prefs
enterprise_cacerts.bks          shortcut_service.xml
enterprise_nativecerts.bks      slice
enterprise_untrustedcerts.bks   slocation
enterprise_usercerts.bks        slocation.db
entropy.dat                     slocation.db-journal
fmmpassword.key                 slocation.db-se
friends                         stats_companion
gamemanager.db                  storage.xml
gamemanager.db-journal          sync
graphicsstats                   timezone
harmony_third_party_apps.xml    ucm_ca_cert
hcm_info                        uiderrors.txt
hcm_info-journal                usagestats
heapdump                        users
ifw                             watchlist_report.db
install_sessions                watchlist_report.db-journal
install_sessions.xml            watchlist_settings.xml
ipm_hitcount.txt                wifigeofence.db
ipm_input_data.txt              wifigeofence.db-journal
job
```

Εικόνα 61 - Password Removal - Directory /data/system ls 2

```
a70q:/data/system # rm locksettings.db
a70q:/data/system # rm locksettings.db-wal
a70q:/data/system # rm locksettings.db-shm
a70q:/data/system # exit
a70q:/ $ exit
```

Εικόνα 62 - Password Removal - Directory /data/system Delete Files

Κάνουμε επανεκκίνηση της συσκευής (Εικόνα 63).

```
santoku@santoku-virtual-machine:~$ adb reboot
santoku@santoku-virtual-machine:~$
```

Εικόνα 63 - Password Removal - Reboot Device

Η διαγραφή του password ήταν επιτυχής (Εικόνα 64, Εικόνα 65).

Εικόνα 64 - Password Removed Lock Screen 1

Εικόνα 65 - Password Removed Lock Screen 2

3. ANDROID 10 SECURITY AND PRIVACY FEATURES

3.1 Android 10 Permissions & Scoped Storage

Το Android σαν λειτουργικό σύστημα έχει κάποια χαρακτηριστικά σε επίπεδο αρχιτεκτονικής τα οποία υπάρχουν για να διασφαλίσουν την ασφάλεια των χρηστών, των εφαρμογών και των δεδομένων που διαχειρίζεται η συσκευή.

Τα συγκεκριμένα security features υπάρχουν στο λειτουργικό σύστημα και έχουν τους ακόλουθους στόχους (Skulkin, et al., 2018) (Android Developers, 2020):

- Την προστασία των δεδομένων του χρήστη.
- Την προστασία των πόρων του συστήματος.
- Την προστασία των δεδομένων των εφαρμογών από μη εγκεκριμένη πρόσβαση από άλλες εφαρμογές.

Το Android 10 εισάγει νέα features που σκοπό έχουν την ασφάλεια των χρηστών και την προστασία της ιδιωτικότητας τους, ένα από αυτά τα features αφορά το scoped storage access που έχουν πλέον οι εφαρμογές. Το scoped storage περιορίζει την πρόσβαση που έχουν οι εφαρμογές στο storage της συσκευής. Οι εφαρμογές δεν έχουν πρόσβαση σε όλο το storage της συσκευής, όπως συνέβαινε σε παλιότερες εκδόσεις android, πλέον η κάθε εφαρμογή έχει πρόσβαση μόνο σε συγκεκριμένο directory (Singh, 2020) (Goyal, 2020) (Solution Analysts, 2020) (Dwivedi, 2020).

Η διαχείριση του σε τι δεδομένα έχει πρόσβαση η κάθε εφαρμογή και τα permissions που παίρνει στην συσκευή περνάνε στην κυριότητα του χρήστη (Android Developers, 2020). Η διαχείριση των permissions για κάθε εφαρμογή έχει γίνει αναλυτικότερη και περισσότερο user friendly προκειμένου ο χρήστης να κατανοεί ευκολότερα τι permissions παρέχει σε κάθε εφαρμογή (Hindy, 2019) (Wallen, 2019) (VisiHow, n.d.). Επιπρόσθετα έχει δοθεί η επιλογή στους χρήστες να μπλοκάρουν εφόσον το επιθυμούν την background πρόσβαση στην τοποθεσία της συσκευής για εφαρμογές (Ansari, 2020) (Davenport, 2020) (Android Developers, 2020).

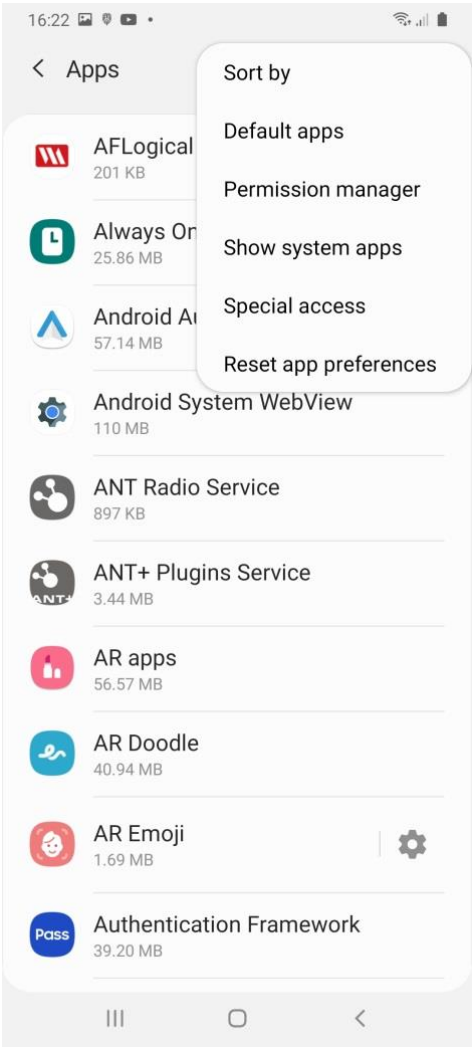
Παρόλο που τα συγκεκριμένα security features έχουν ως σκοπό την προστασία των δεδομένων και της ιδιωτικότητας του χρήστη, πολλές φορές δημιουργούν προβλήματα στους forensic investigators από το να αποκτήσουν πρόσβαση στα δεδομένα της συσκευής (Skulkin, et al., 2018).

Από την σκοπιά μιας forensics έρευνας είναι πολύ σημαντικό η κατανόηση των συγκεκριμένων security features και το πώς αυτά επηρεάζουν το ποια δεδομένα

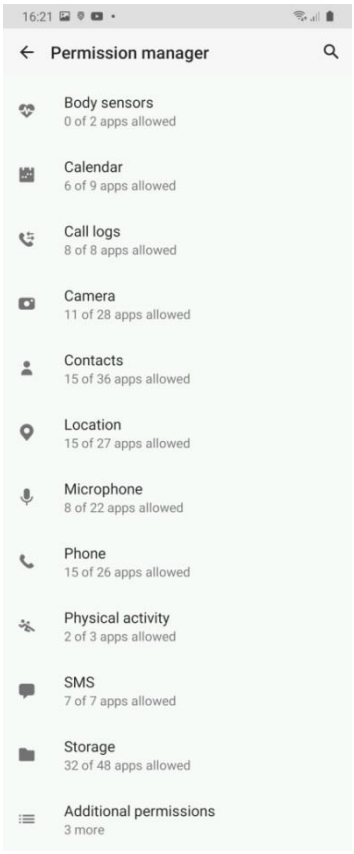
μπορούν να ανακτηθούν από την εκάστοτε συσκευή και κάτω από ποιες συνθήκες (Skulkin, et al., 2018).

Για την συνέχεια της διπλωματικής στην συσκευή μέσω των Settings->Apps θα επιλέξουμε Show System Apps και θα πάμε σε κάθε εφαρμογή ξεχωριστά για να διαχειριστούμε τα permissions. Προκειμένου να μην αντιμετωπίσουμε πρόβλημα με την ανάκτηση δεδομένων από το physical image θα παρέχουμε σε κάθε εφαρμογή όλα τα δυνατά permissions που μπορεί να πάρει.

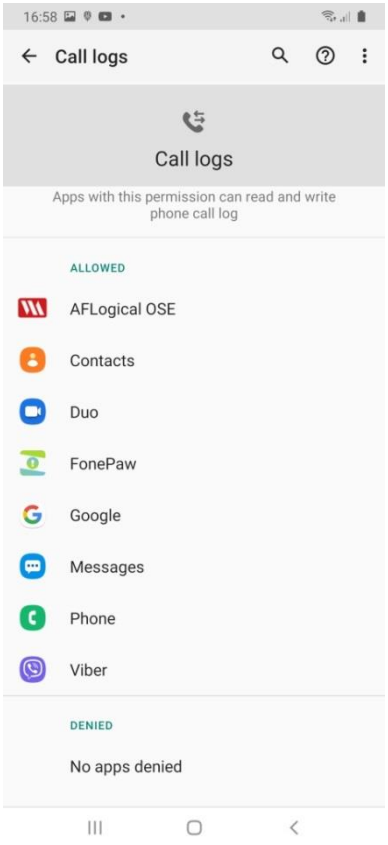
Πηγαίνοντας στα Settings->Apps->Permission Manager (Εικόνα 66) μπορούμε να διαχειριστούμε τα permissions των εφαρμογών (Εικόνα 67). Μέσω του permission manager μπορούμε να δούμε σε τι παρέχεται permission στην συσκευή και ανοίγοντας την κάθε επιλογή μπορούμε να δούμε τις εφαρμογές που έχουν αποκτήσει το συγκεκριμένο permission.



Εικόνα 66 - Device App List



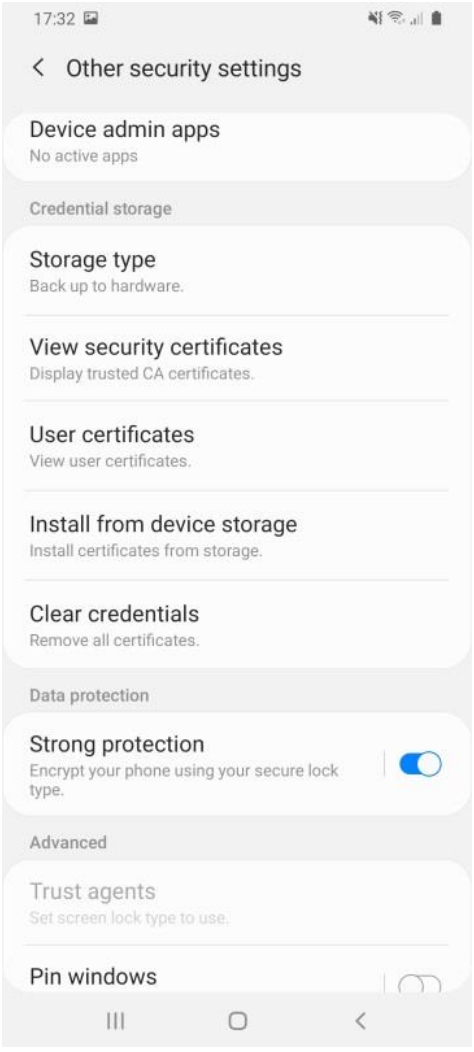
Εικόνα 67 - Permission Manager



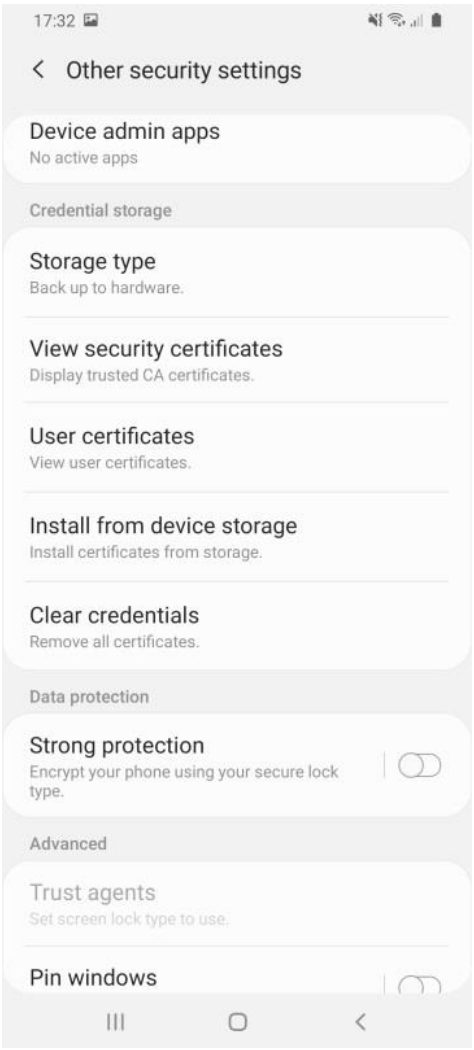
Εικόνα 68 - Call Logs Permissions

3.2 Απενεργοποίηση Κρυπτογράφησης

Τα android 10 έχουν ενεργοποιημένη την κρυπτογράφηση συσκευής ως προεπιλογή (Εικόνα 69). Μέσα από το μενού Settings->Biometrics and security απενεργοποιούμε την επιλογή Strong protection (Εικόνα 70) δηλαδή την κρυπτογράφηση της συσκευής για να μπορούμε να έχουμε πρόσβαση στα δεδομένα της συσκευής σε μορφή plaintext κατά την διαδικασία της forensic analysis (Skulkin, et al., 2018).



Εικόνα 69 - Disable Encryption



Εικόνα 70 - Encryption Disabled

3.3 Απεγκατάσταση Knox

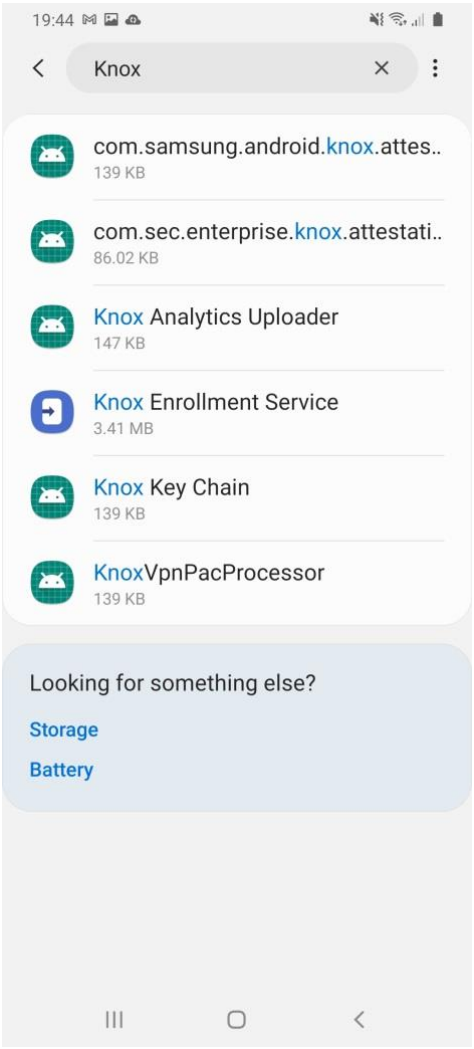
KNOX PROBLEMS

Ένα βασικό χαρακτηριστικό των συσκευών Samsung είναι το σύστημα ασφάλειας που έχουν, Samsung Knox. Το Knox έκανε την εμφάνιση του το 2013 στο Samsung Galaxy S4 με το 4.3 update. Παρέχει πολυεπίπεδη ασφάλεια τόσο σε επίπεδο hardware όσο και σε software και δίνει την δυνατότητα στους χρήστες να απομονώνουν δεδομένα, συνήθως εργασίας, στην συσκευή σε κρυπτογραφημένο περιβάλλον (Samsung, n.d.) (Gillware, n.d.). Το γεγονός αυτό μπορεί να προκαλέσει προβλήματα σε μια forensic analysis συσκευής Samsung που έχει χρησιμοποιηθεί το συγκεκριμένο περιβάλλον, παρόλο που πλέον υπάρχουν εργαλεία που μπορούν να το αντιμετωπίσουν όπως το cellebrite (Cellebrite, 2021).

Ένα άλλο πρόβλημα που προκύπτει με την ύπαρξη του Knox αφορά την απομόνωση της συσκευής. Η σωστή απομόνωση της συσκευής από εξωτερικές παρεμβολές αποτελεί σημαντικό κομμάτι μιας forensics έρευνας (Kostadinov, 2019). Στην περίπτωση που υπάρχει το Knox στην συσκευή είναι ακόμα πιο σημαντικό να πραγματοποιηθεί σωστά η απομόνωση της συσκευής γιατί οι χρήστες με το MyKnox μπορούν να συνδεθούν απομακρυσμένα στην συσκευή και να τροποποιήσουν δεδομένα ακόμα και να διαγράψουν όλα τα δεδομένα της συσκευής, ή να πραγματοποιήσουν remote code injection καταλήγοντας σε κάποια επίθεση μέσω του κινητού. Είναι σημαντικό λοιπόν οι forensic examiners να γνωρίζουν τις δυνατότητες που παρέχει το Knox εάν δουλεύουν σε συσκευές Samsung (Gillware, n.d.) (Samsung, n.d.).

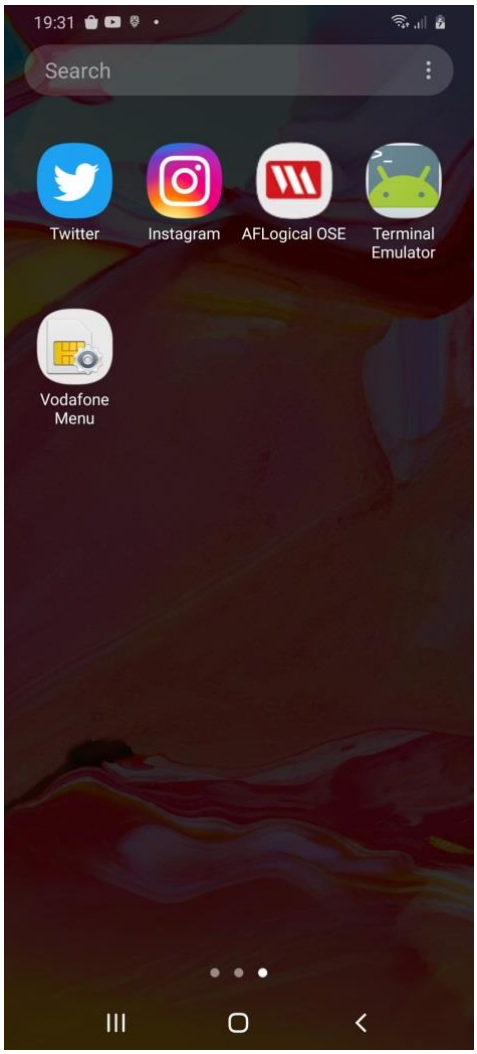
UNINSTALLING KNOX

Στην προκείμενη περίπτωση δεν θα μας απασχολήσει η εφαρμογή Knox συνεπώς προτείνουμε την απεγκατάσταση του Knox και όλων των applications που το αφορούν (Εικόνα 71) (Vivek, 2019).



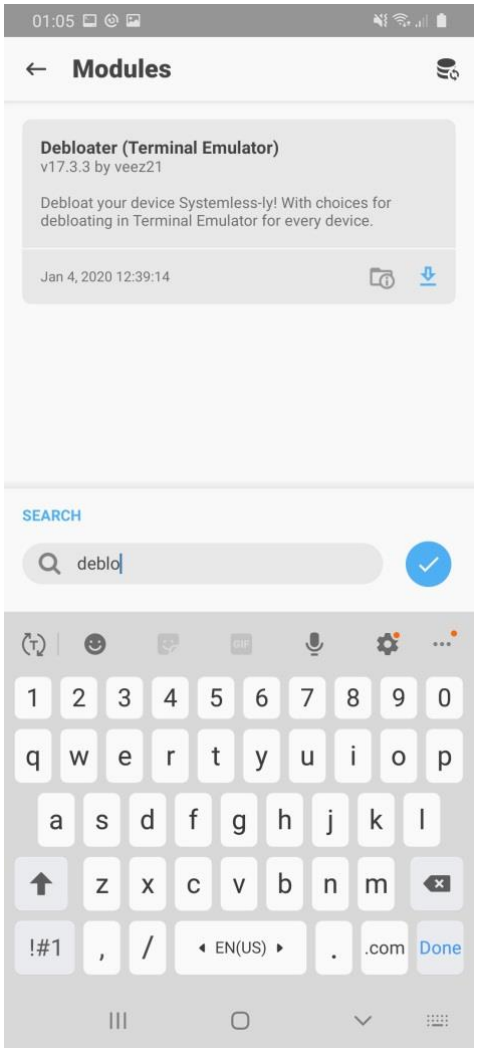
Εικόνα 71 - Knox Apps

Αρχικά μέσω του PlayStore εγκαθιστούμε την εφαρμογή Terminal Emulator (Εικόνα 72).



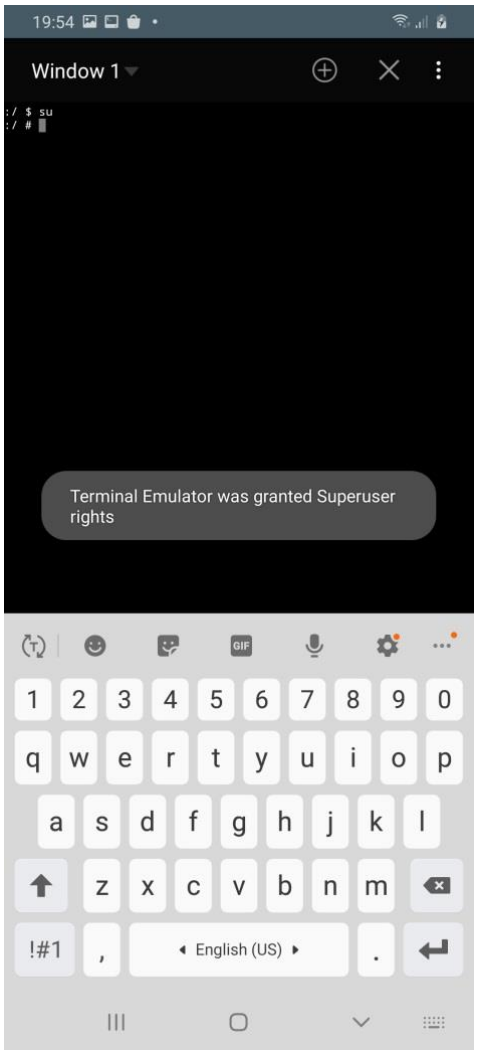
Εικόνα 72 - Terminal Emulator App

Στην συνέχεια μέσα από την εφαρμογή Magisk στην συσκευή και το μενού των Modules επιλέγουμε το Debloater και το εγκαθιστούμε στην συσκευή (Εικόνα 73).



Εικόνα 73 - Magisk Modules - Debloater

Στην συνέχεια επανερχόμαστε στην εφαρμογή Terminal Emulator. Δίνουμε την εντολή su για να μπούμε σε su shell στην συσκευή (Εικόνα 74).

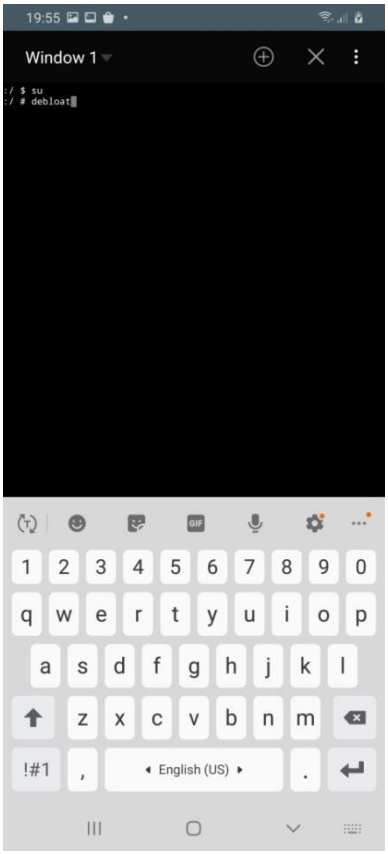


Εικόνα 74 - Terminal Emulator App - su shell

Στην συνέχεια δίνουμε την εντολή:

debloat (Εικόνα 75)

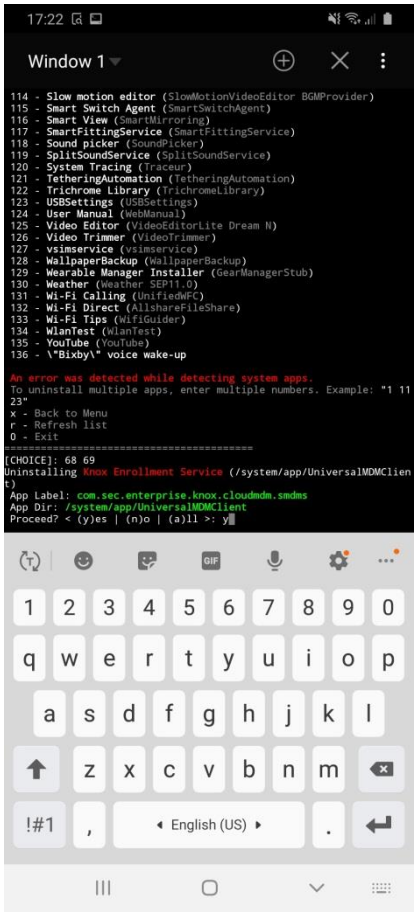
Η συγκεκριμένη εντολή θα ξεκινήσει αυτόματα το Debloater Magisk Module στο terminal (Εικόνα 76).



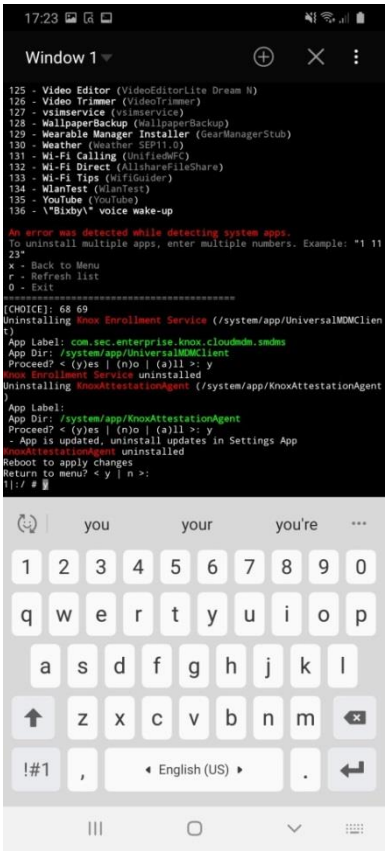
Εικόνα 75 - Terminal Emulator App - debloat

Εικόνα 76 - Debloater Module Menu

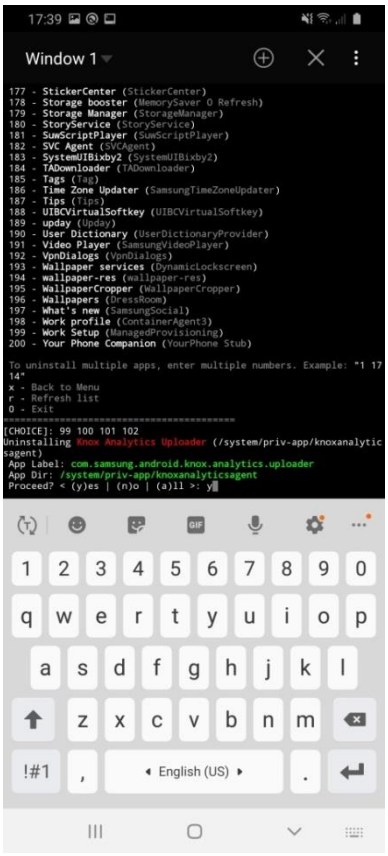
Επιλέγουμε System Apps και System Priv-Apps στο μενού του Debloater και αναζητούμε όλες τις εφαρμογές του Knox στους καταλόγους των εφαρμογών, τις επιλέγουμε χρησιμοποιώντας τον αριθμό τους και δίνουμε y για να γίνει η απεγκατάσταση τους (Εικόνα 77, Εικόνα 78, Εικόνα 79, Εικόνα 80).



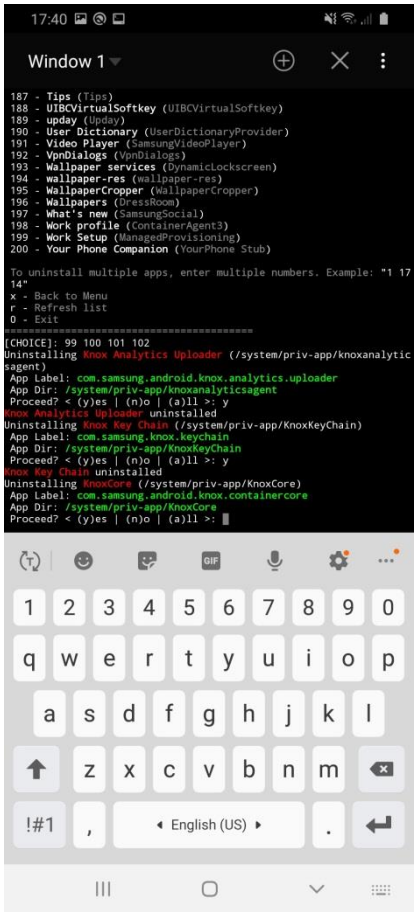
Εικόνα 77 - Uninstalling Knox Apps 1



Εικόνα 78 - Uninstalling Knox Apps 2

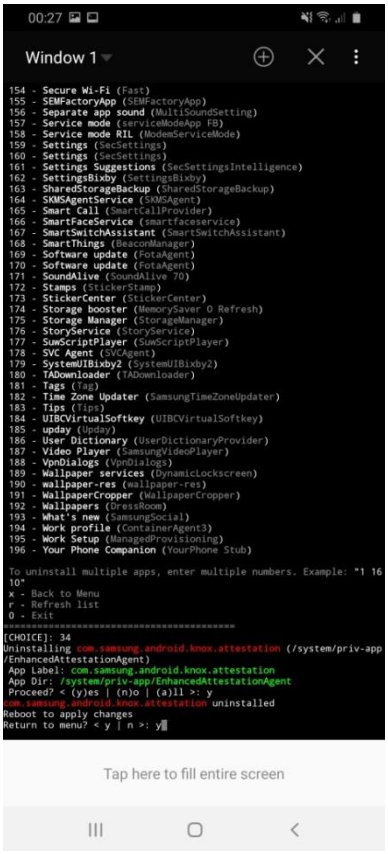


Εικόνα 79 - Uninstalling Knox Apps 3

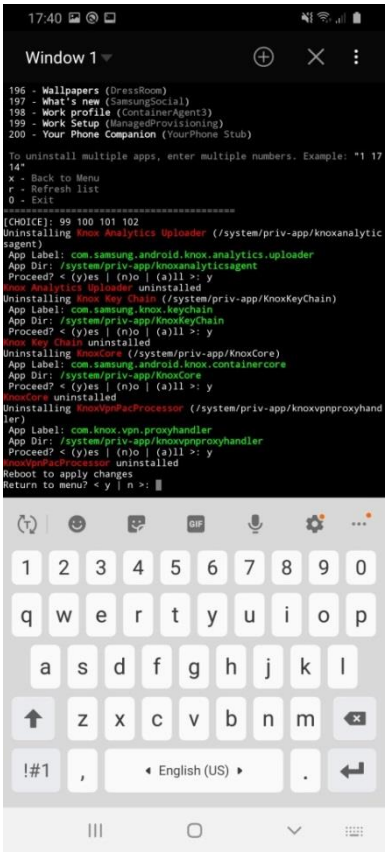


Εικόνα 80 - Uninstalling Knox Apps 4

Όταν τελειώσουμε με την απεγκατάσταση των εφαρμογών το Debloater θα μας προτείνει να κάνουμε reboot την συσκευή (Εικόνα 81, Εικόνα 82) για να γίνουν οι αλλαγές. Πραγματοποιούμε το reboot της συσκευής.

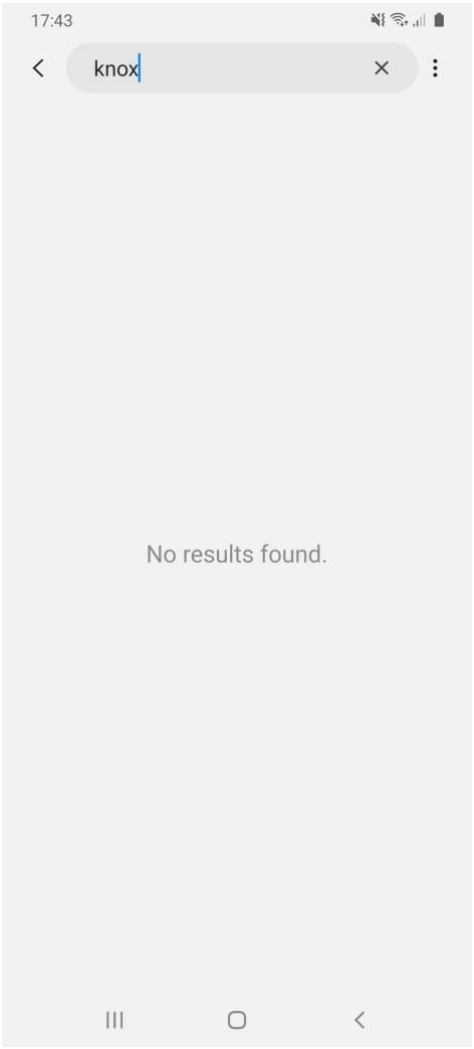


Εικόνα 81 - Uninstalling Knox Apps 5



Εικόνα 82 - Uninstalling Knox Apps 6

Στην συνέχεια από τα Settings της συσκευής επιλέγουμε Apps και ενεργοποιούμε την επιλογή Show System Apps. Πραγματοποιούμε αναζήτηση για Knox και βλέπουμε ότι δεν υπάρχει πλέον στην συσκευή καμία εφαρμογή του Knox (Εικόνα 83), άρα απεγκαταστήσαμε επιτυχώς όλες τις εφαρμογές του Knox από την συσκευή.



Εικόνα 83 - Knox No Results Found

4. LOGICAL ANALYSIS

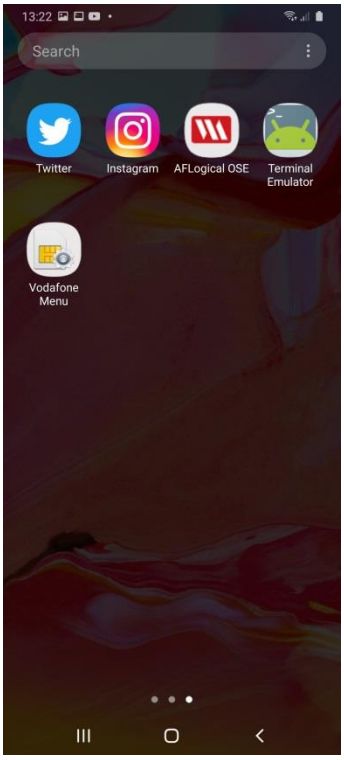
4.1 AFLOGICAL

Η ανάλυση σε logical επίπεδο προϋποθέτει την σύνδεση της συσκευής με τον υπολογιστή, συνήθως με τη χρήση ενός usb καλωδίου. Ο υπολογιστής αναλαμβάνει να στείλει τις ανάλογες εντολές ώστε ο επεξεργαστής της συσκευής να του παρέχει τα δεδομένα που ζήτησε (Bommisetty, et al., 2014).

Στο Santoku υπάρχει η εφαρμογή AFLogical OSE που παρέχει την συγκεκριμένη δυνατότητα. Δίνοντας την εντολή aflogical-ose (Εικόνα 84) (Hoog, 2013) ένα apk δημιουργείται με όνομα AFLogical OSE (Εικόνα 85), το οποίο στη συνέχεια αποστέλλεται στη συσκευή και εγκαθίσταται.

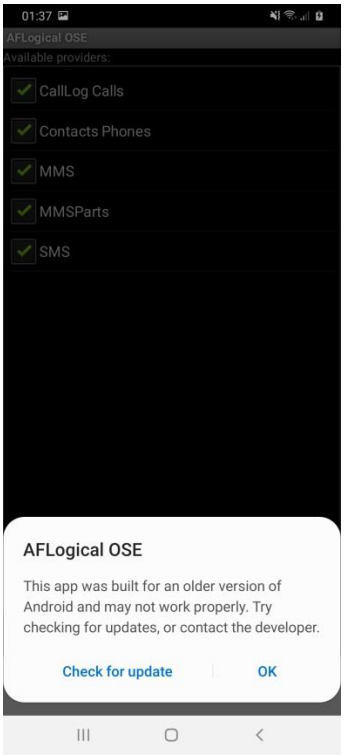
```
$ aflogical-ose -h

run 'aflogical-ose' with usb debugging enabled in your android device

santoku@santoku-virtual-machine:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for santoku:

691 KB/s (28794 bytes in 0.040s)
Success

Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.a
ndroid.ForensicsActivity }

Press enter to pull /sdcard/forensics into ~/aflogical-data/

pull: building file list...
pull: /sdcard/forensics/20201208.0111/info.xml -> /home/santoku/aflogical-data/2
0201208.0111/info.xml
pull: /sdcard/forensics/20201208.0111/Contacts Phones.csv -> /home/santoku/aflog
ical-data/20201208.0111/Contacts Phones.csv
pull: /sdcard/forensics/20201208.0111/CallLog Calls.csv -> /home/santoku/aflogic
al-data/20201208.0111/CallLog Calls.csv
pull: /sdcard/forensics/20201208.0111/MMSParts.csv -> /home/santoku/aflogical-da
```

Εικόνα 84 - aflogical-ose terminal



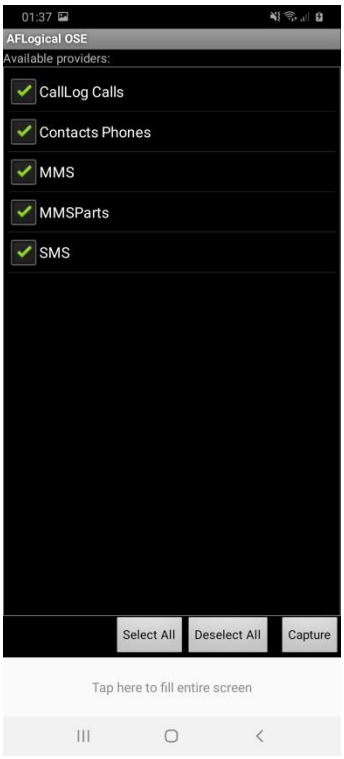
Εικόνα 85 - AFLogical OSE App

Αξίζει να σημειωθεί ότι το συγκεκριμένο apk έχει αναπτυχθεί για παλαιότερες εκδόσεις android (Εικόνα 86) και δεν έχει πραγματοποιηθεί κάποιο update που να αφορά στα android 10. Παρόλα αυτά όμως δίνει αποτελέσματα και σε android 10 συσκευές.



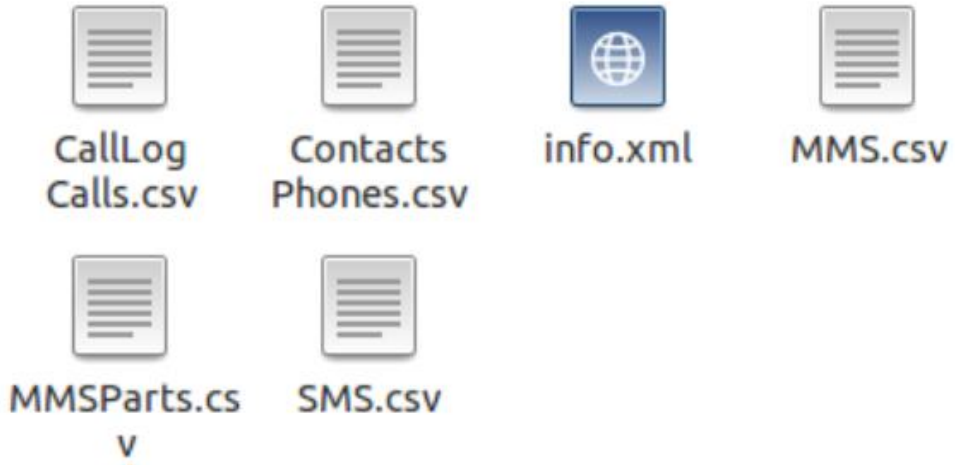
Εικόνα 86 - AFLogical OSE App Message

Μετά την εγκατάστασή της, η εφαρμογή ξεκινάει αυτόματα και εφόσον πατήσουμε την επιλογή Capture (Εικόνα 87), τα δεδομένα που επιθυμούμε συλλέγονται και μεταφέρονται στο Santoku.



Εικόνα 87 - AFLogical OSE App Menu

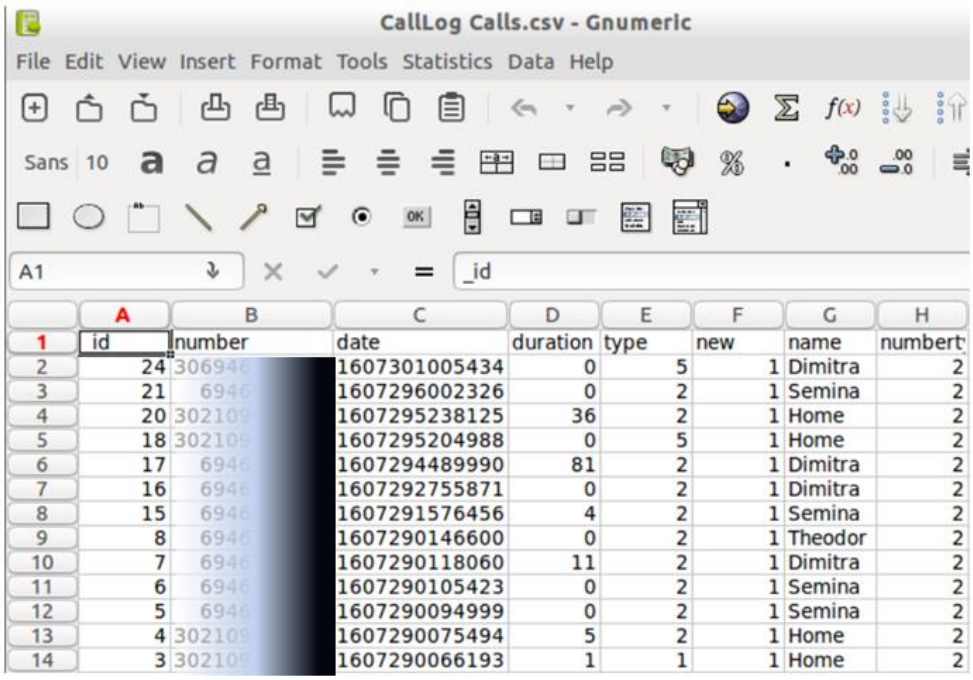
Μετά την ολοκλήρωση της διαδικασίας μπορούμε να δούμε τα δεδομένα που συλλέξαμε, τα οποία είναι σε μορφή csv (Εικόνα 88), με την χρήση οποιουδήποτε προγράμματος spreadsheet.



Εικόνα 88 - Collected Files

Μπορούμε να διαβάσουμε τις κλήσεις από και προς τον χρήστη της συσκευής (Εικόνα 89) αλλά και τα μηνύματα που έχει λάβει και έχει στείλει ο

χρήστης (Εικόνα 90, Εικόνα 91). Μεταξύ άλλων βλέπουμε την ημερομηνία και την ώρα, καθώς και τη διάρκεια της κάθε κλήσης, αλλά και το όνομα με το οποίο είναι αποθηκευμένη η κάθε επαφή στη συσκευή.



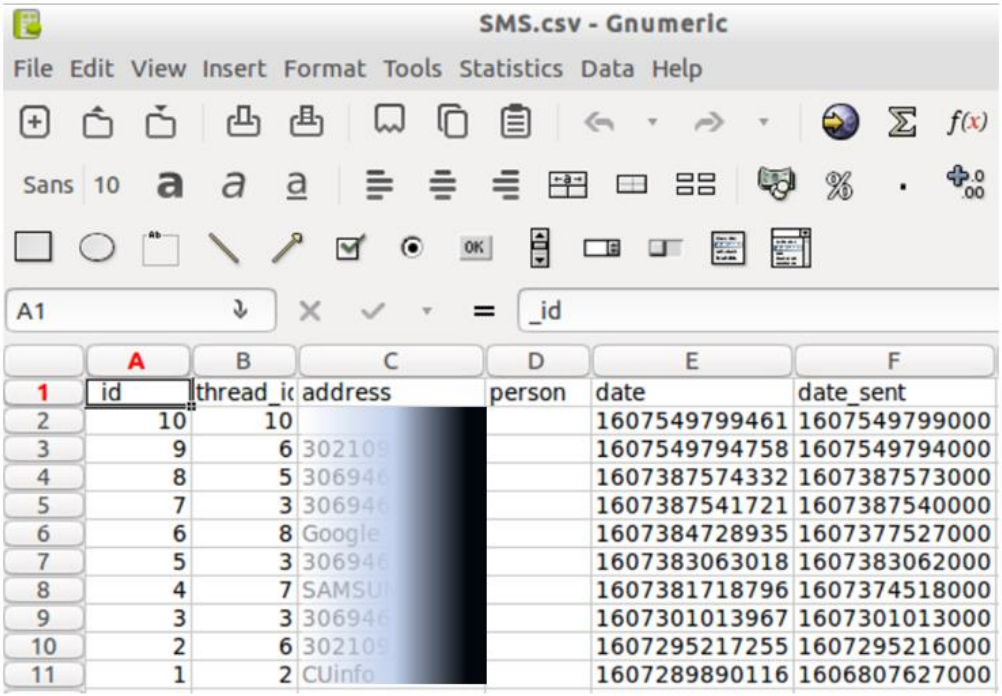
CallLog Calls.csv - Gnumeric

File Edit View Insert Format Tools Statistics Data Help

A1 _id

	A	B	C	D	E	F	G	H
1	id	number	date	duration	type	new	name	numbert
2	24	306946	1607301005434	0	5	1	Dimitra	2
3	21	6946	1607296002326	0	2	1	Semina	2
4	20	302109	1607295238125	36	2	1	Home	2
5	18	302109	1607295204988	0	5	1	Home	2
6	17	6946	1607294489990	81	2	1	Dimitra	2
7	16	6946	1607292755871	0	2	1	Dimitra	2
8	15	6946	1607291576456	4	2	1	Semina	2
9	8	6946	1607290146600	0	2	1	Theodor	2
10	7	6946	1607290118060	11	2	1	Dimitra	2
11	6	6946	1607290105423	0	2	1	Semina	2
12	5	6946	1607290094999	0	2	1	Semina	2
13	4	302109	1607290075494	5	2	1	Home	2
14	3	302109	1607290066193	1	1	1	Home	2

Εικόνα 89 - Call Logs File



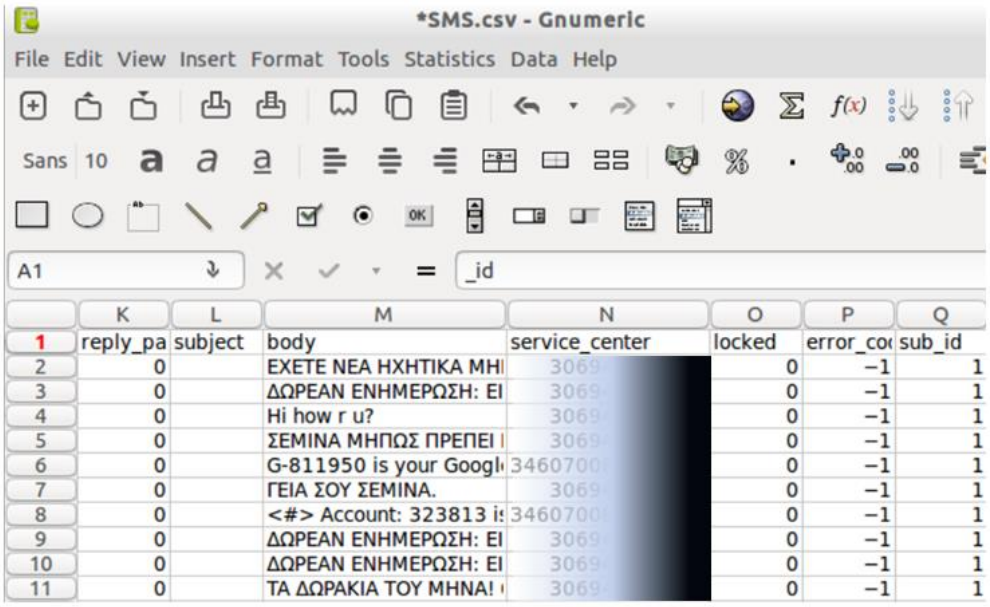
SMS.csv - Gnumeric

File Edit View Insert Format Tools Statistics Data Help

A1 _id

	A	B	C	D	E	F
1	id	thread_ic	address	person	date	date_sent
2	10	10			1607549799461	1607549799000
3	9	6	302109		1607549794758	1607549794000
4	8	5	306946		1607387574332	1607387573000
5	7	3	306946		1607387541721	1607387540000
6	6	8	Google		1607384728935	1607377527000
7	5	3	306946		1607383063018	1607383062000
8	4	7	SAMSU		1607381718796	1607374518000
9	3	3	306946		1607301013967	1607301013000
10	2	6	302109		1607295217255	1607295216000
11	1	2	CUinfo		1607289890116	1606807627000

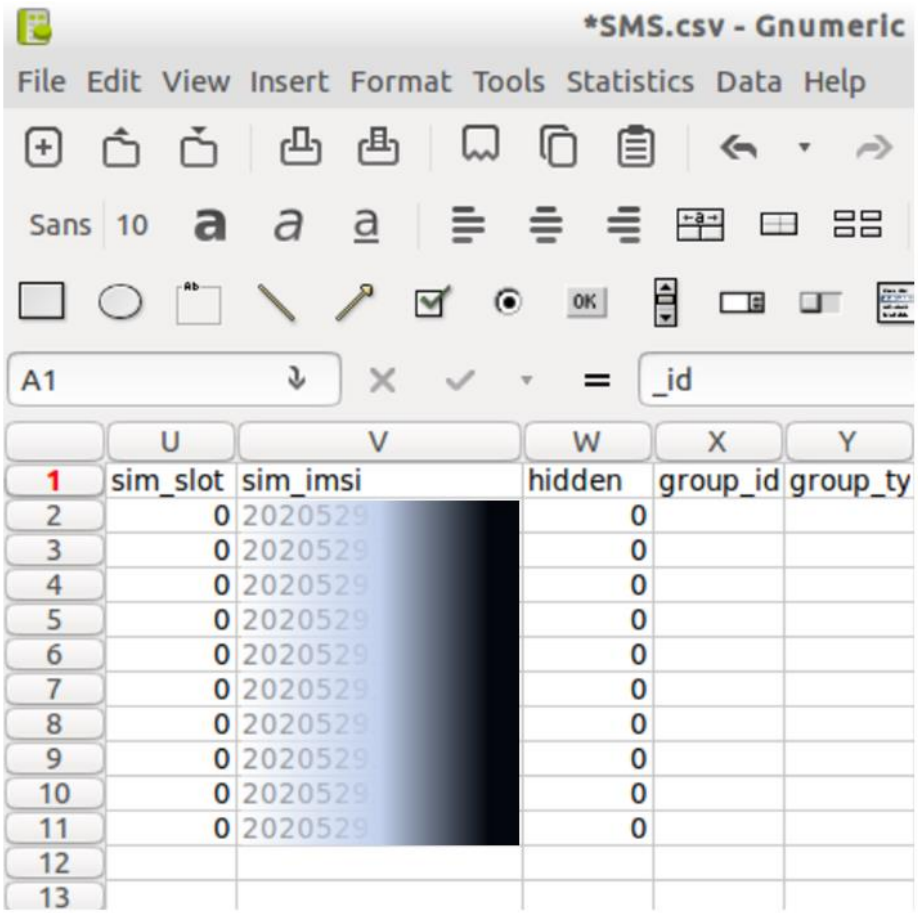
Εικόνα 90 - SMS File 1



	K	L	M	N	O	P	Q
1	reply_pa	subject	body	service_center	locked	error_co	sub_id
2	0		ΕΧΕΤΕ ΝΕΑ ΗΧΗΤΙΚΑ ΜΗ	3069	0	−1	1
3	0		ΔΩΡΕΑΝ ΕΝΗΜΕΡΩΣΗ: ΕΙ	3069	0	−1	1
4	0		Hi how r u?	3069	0	−1	1
5	0		ΣΕΜΙΝΑ ΜΗΠΩΣ ΠΡΕΠΕΙ	3069	0	−1	1
6	0		G-811950 is your Googl	3460700	0	−1	1
7	0		ΓΕΙΑ ΣΟΥ ΣΕΜΙΝΑ.	3069	0	−1	1
8	0		<#> Account: 323813 is	3460700	0	−1	1
9	0		ΔΩΡΕΑΝ ΕΝΗΜΕΡΩΣΗ: ΕΙ	3069	0	−1	1
10	0		ΔΩΡΕΑΝ ΕΝΗΜΕΡΩΣΗ: ΕΙ	3069	0	−1	1
11	0		ΤΑ ΔΩΡΑΚΙΑ ΤΟΥ ΜΗΝΑ!	3069	0	−1	1

Εικόνα 91 - SMS File 2

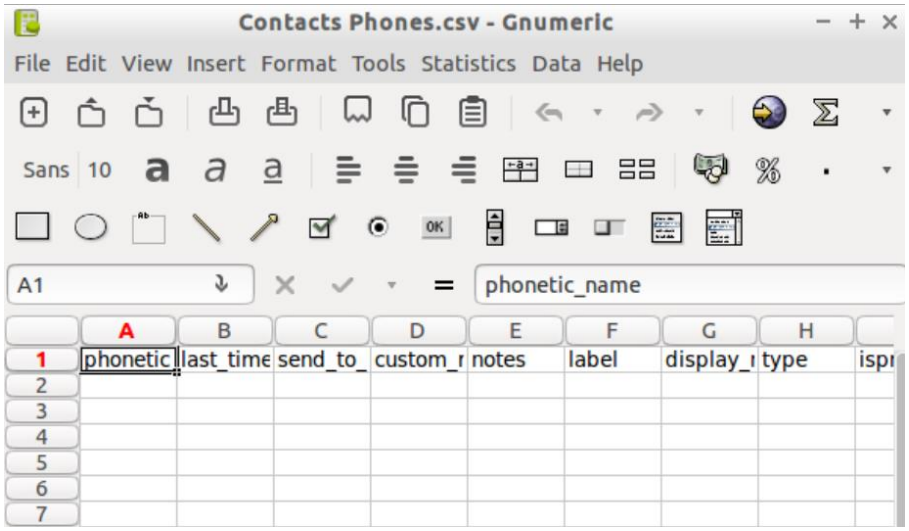
Στο αρχείο μηνυμάτων παρατηρούμε ότι το apk έχει καταφέρει να τραβήξει και το imsi της κάρτας sim της κινητής συσκευής (Εικόνα 92).



	U	V	W	X	Y
1	sim_slot	sim_imsi	hidden	group_id	group_ty
2	0	2020529	0		
3	0	2020529	0		
4	0	2020529	0		
5	0	2020529	0		
6	0	2020529	0		
7	0	2020529	0		
8	0	2020529	0		
9	0	2020529	0		
10	0	2020529	0		
11	0	2020529	0		
12					
13					

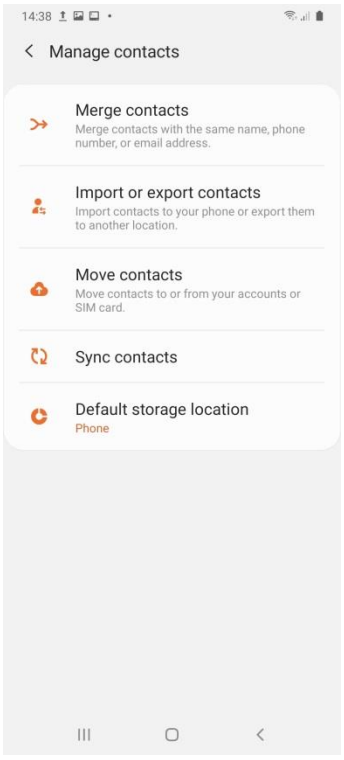
Εικόνα 92 - SMS File 3 - IMSI

Παρόλο που έχουμε δώσει τα κατάλληλα permissions στην εφαρμογή των επαφών παρατηρούμε ότι το AFLogical OSE δεν κατάφερε να τραβήξει τις επαφές που υπάρχουν στην συσκευή (Εικόνα 93).



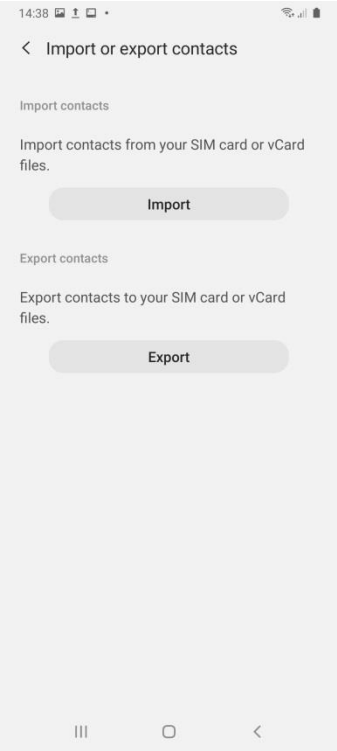
Εικόνα 93 - Contacts File Empty

Από την εφαρμογή των επαφών στην συσκευή και το μενού επιλογών μπορούμε να πάμε στην επιλογή Manage contacts-> Import or export contacts (Εικόνα 94).



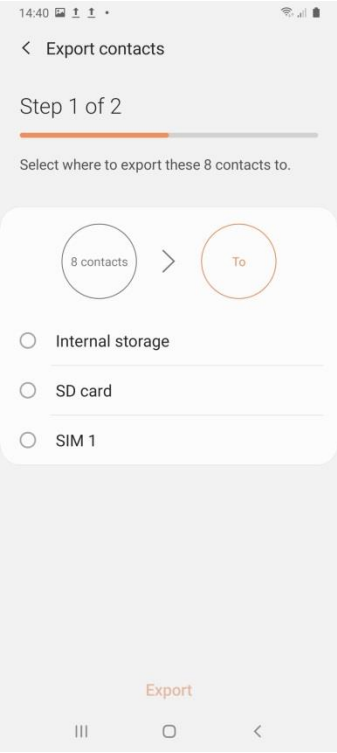
Εικόνα 94 - Manage Contacts Menu

Επιλέγουμε export (Εικόνα 95).

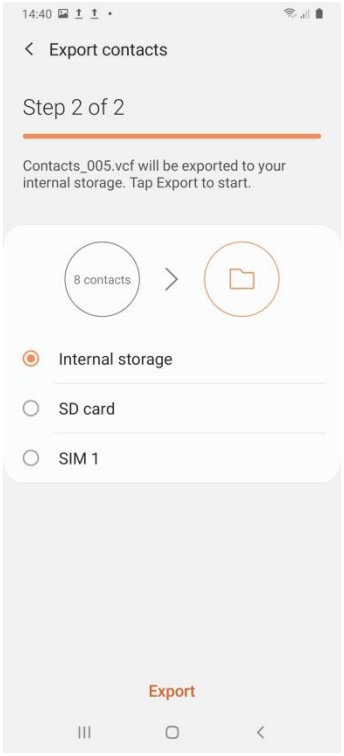


Εικόνα 95 - Import or Export Contacts

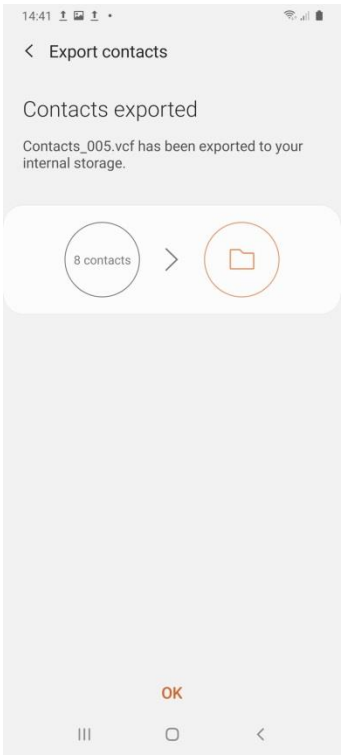
Επιλέγουμε το internal storage για να κάνουμε export το αρχείο των επαφών (Εικόνα 96, Εικόνα 97, Εικόνα 98).



Εικόνα 96 - Internal Storage Export 1/2



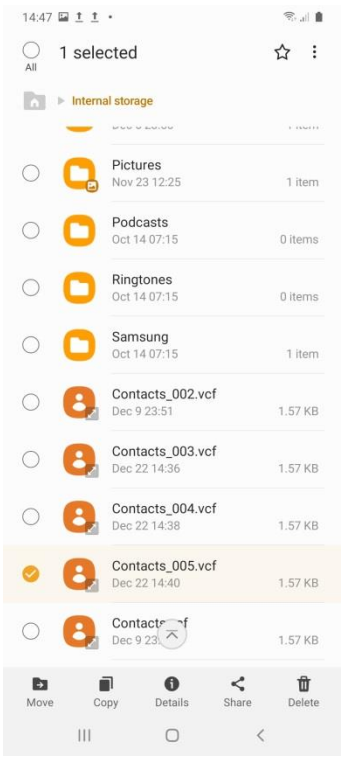
Εικόνα 97 - Internal Storage Export 2/2



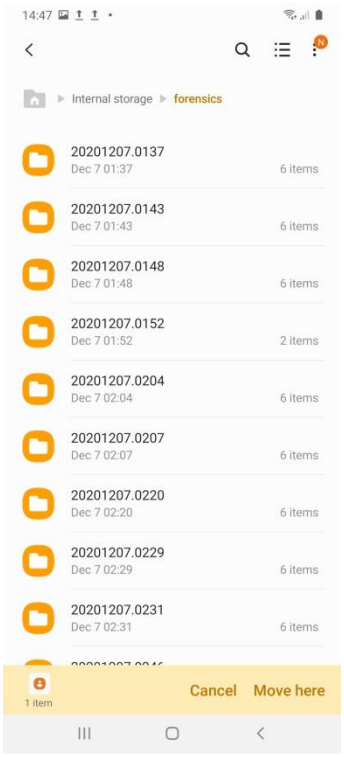
Εικόνα 98 - Contacts Exported

Στην συνέχεια από το internal storage της συσκευής επιλέγουμε το αρχείο που κάναμε export και επιλέγουμε move για να μετακινήσουμε το αρχείο εντός του φακέλου forensics (Εικόνα 99, Εικόνα 100, Εικόνα 101).

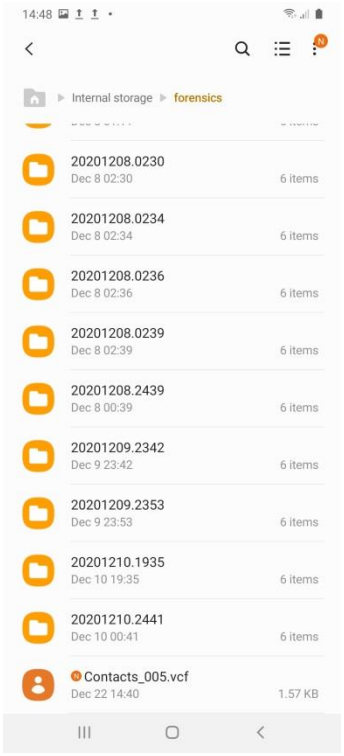
Ο φάκελος forensics έχει δημιουργηθεί από το apk AFLogical OSE στην συσκευή.



Εικόνα 99 - Internal Storage File Selection

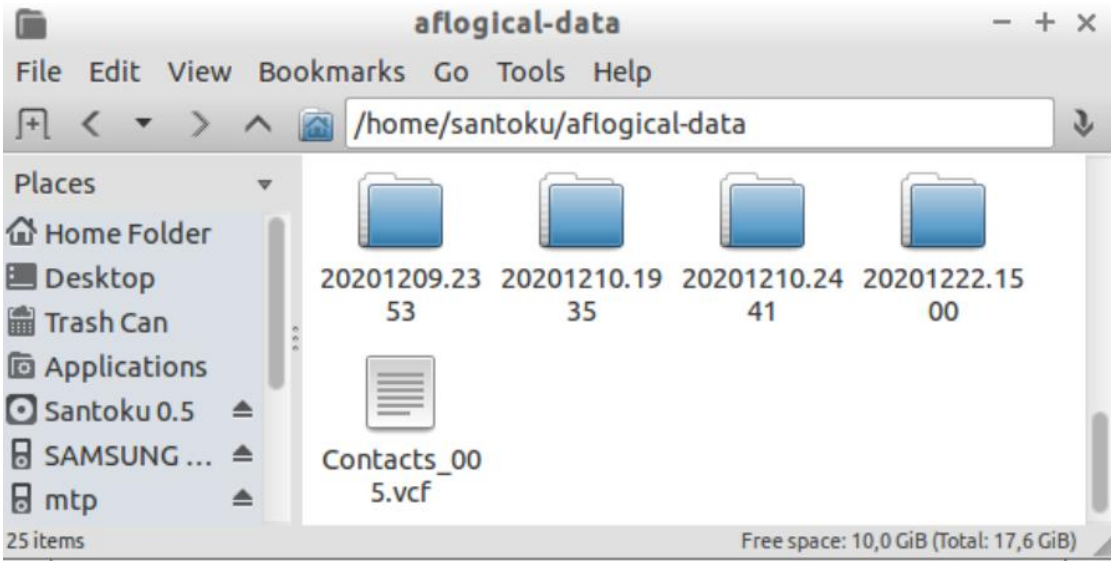


Εικόνα 100 - Move File to Forensics Folder

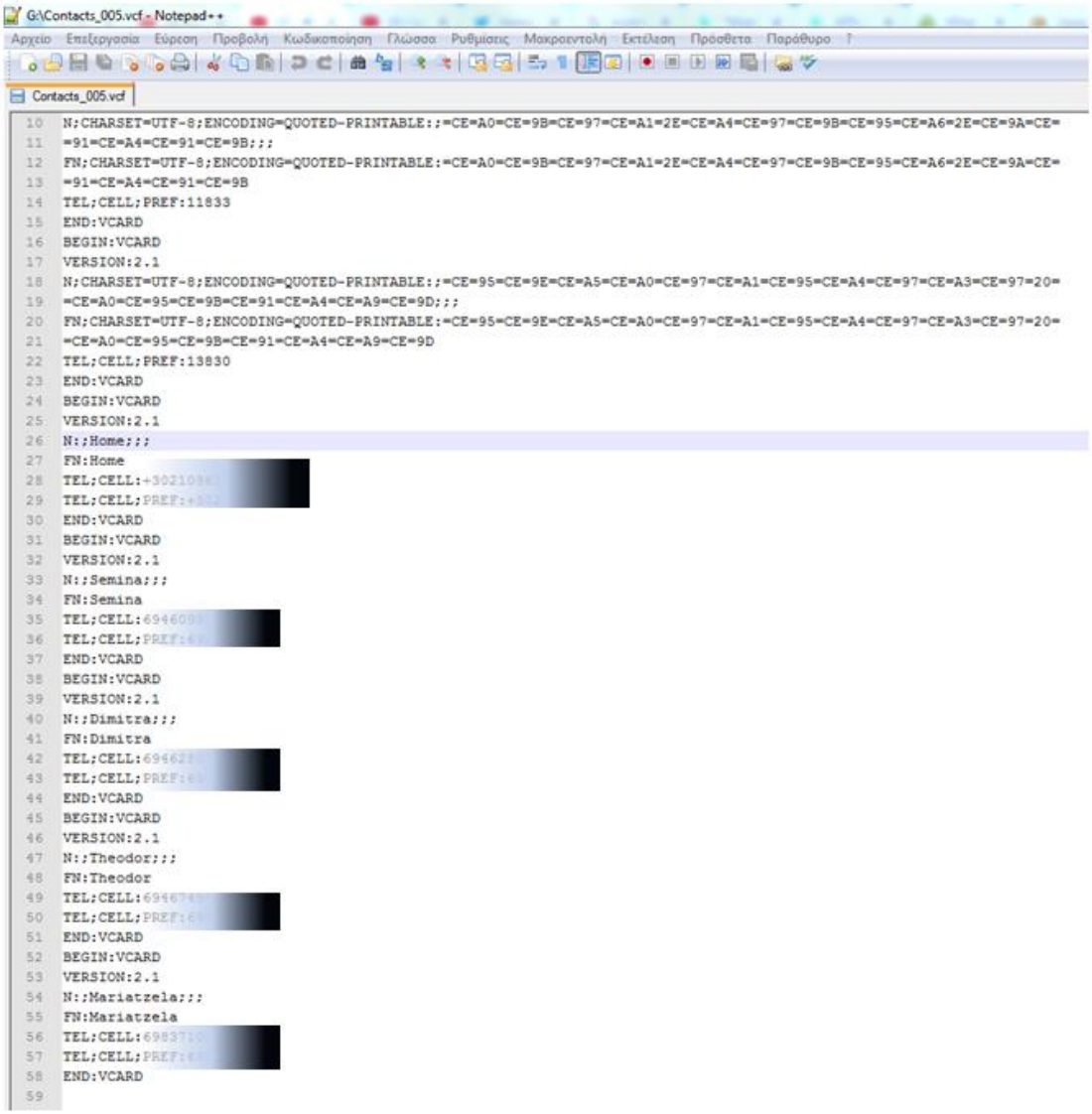


Εικόνα 101 - Forensics Folder Internal Storage

Χρησιμοποιώντας πάλι την εφαρμογή AFLogical OSE από το Santoku με τον ίδιο τρόπο που αναφέρθηκε προηγουμένως, η εφαρμογή θα τραβήξει και το αρχείο με τις επαφές που κάναμε export από την εφαρμογή των επαφών (Εικόνα 102,Εικόνα 103).



Εικόνα 102 - Collected Files with Contacts File

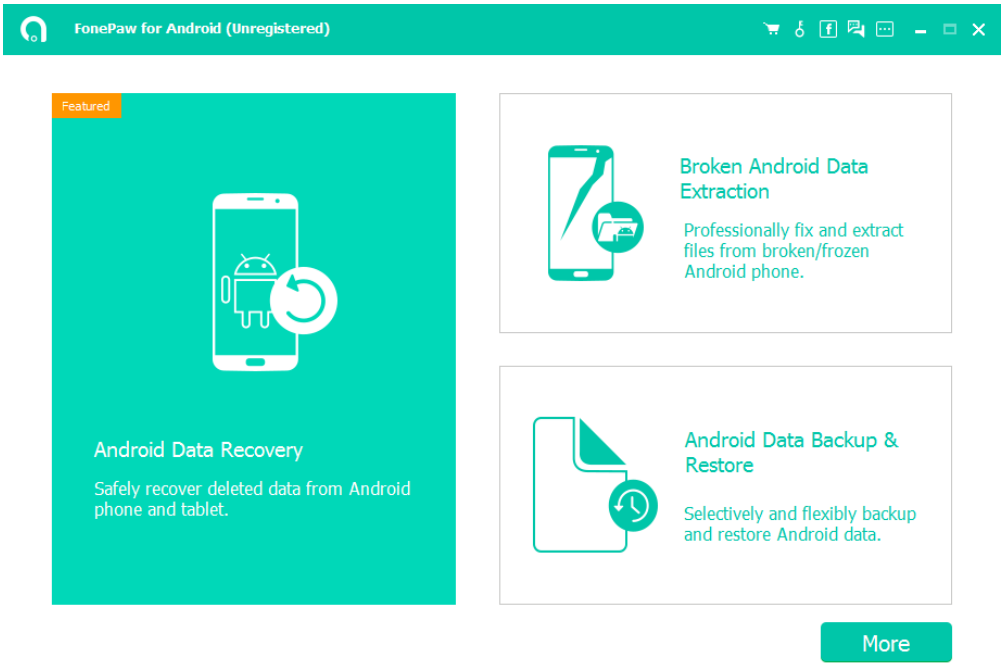


Εικόνα 103 - Exported Contacts File

4.2 FONEPAW

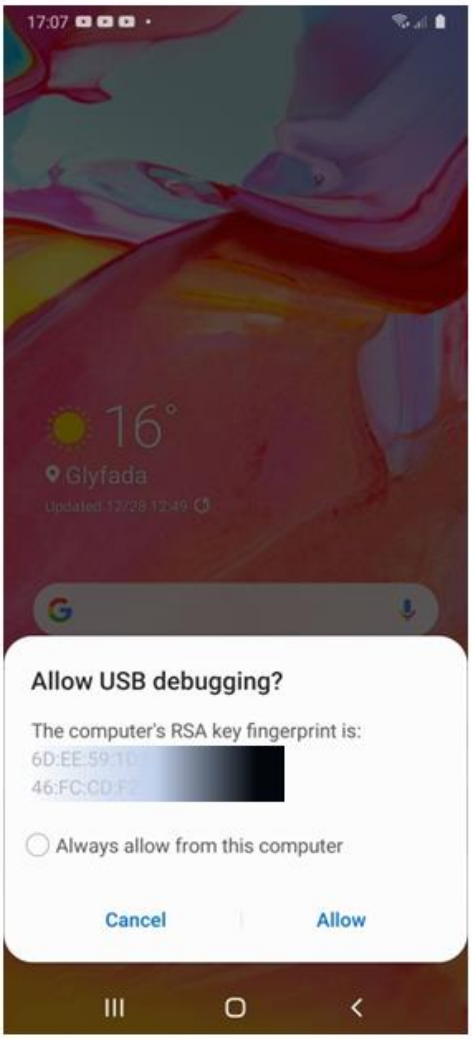
Logical analysis μας παρέχει και το πρόγραμμα FonePaw, έχουμε χρησιμοποιήσει την free trial version που παρέχεται για διάρκεια 30 ημερών.

Ανοίγοντας το πρόγραμμα επιλέγουμε Android Data Recovery (Εικόνα 104).



Εικόνα 104 - FonePaw - Android Data Recovery

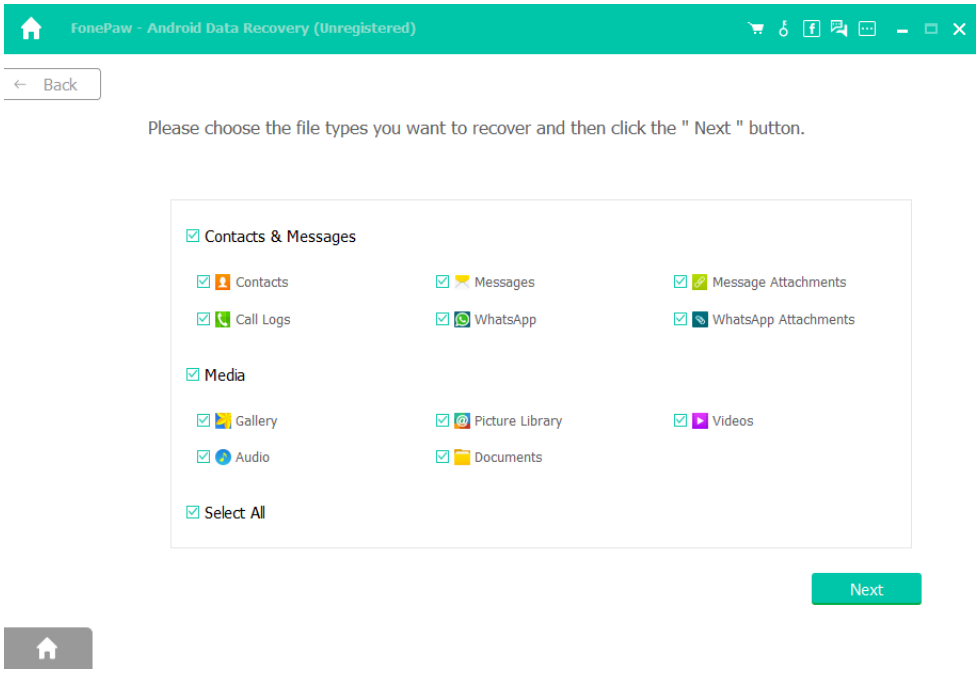
Στο μήνυμα που εμφανίζεται στην συσκευή επιλέγουμε Allow (Εικόνα 105).



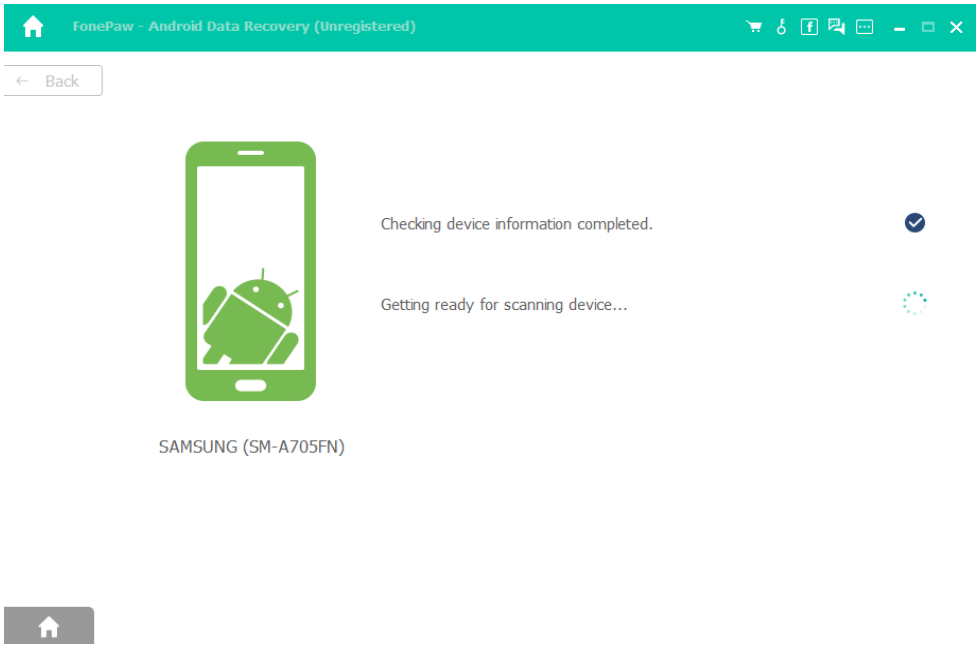
Εικόνα 105 - Allow USB Debugging Message

Στην συνέχεια το FonePaw μας αφήνει να επιλέξουμε τα δεδομένα που θέλουμε να ανακτήσουμε από την συσκευή (Εικόνα 106).

Παρατηρούμε ότι το συγκεκριμένο πρόγραμμα μας δίνει περισσότερες επιλογές ανάκτησης δεδομένων σε logical επίπεδο καθώς μας αφήνει να ανακτήσουμε και εικόνες, βίντεο και αρχεία που υπάρχουν στην συσκευή και δεδομένα από την εφαρμογή what's up αν υπάρχει στην συσκευή, στην προκειμένη περίπτωση εφαρμογή what's up δεν έχει εγκατασταθεί στην συσκευή. Πατάμε Next για να πραγματοποιήσει το πρόγραμμα το logical level extraction (Εικόνα 106, Εικόνα 107).

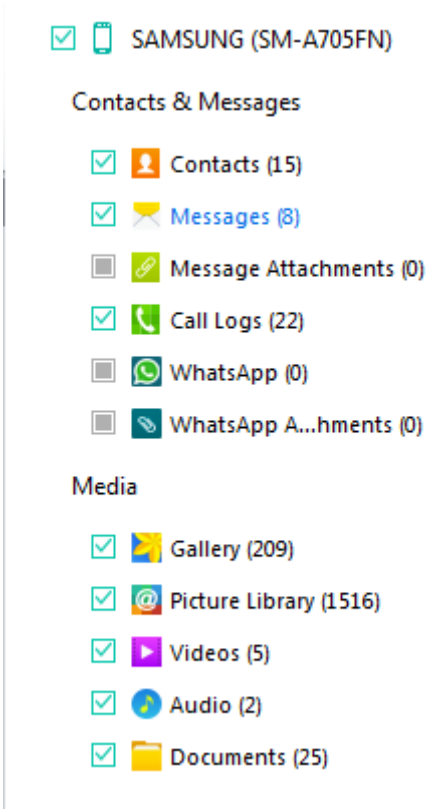


Εικόνα 106 - Choose Files to Recover

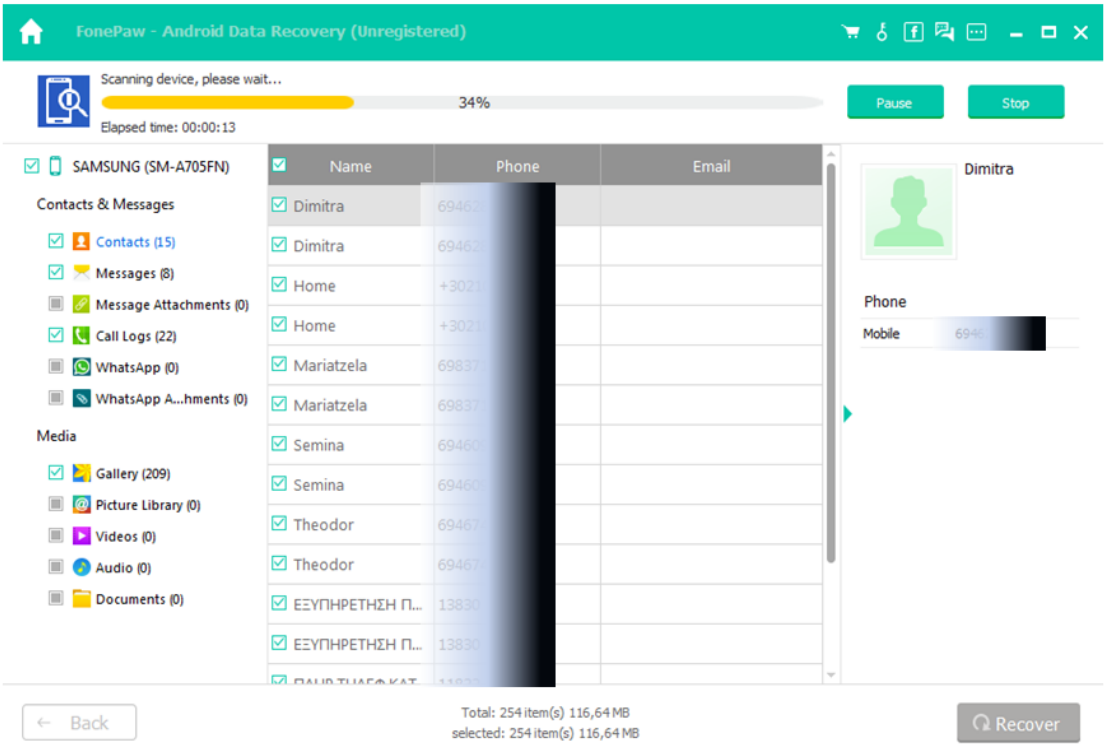


Εικόνα 107 - File Recovery Process

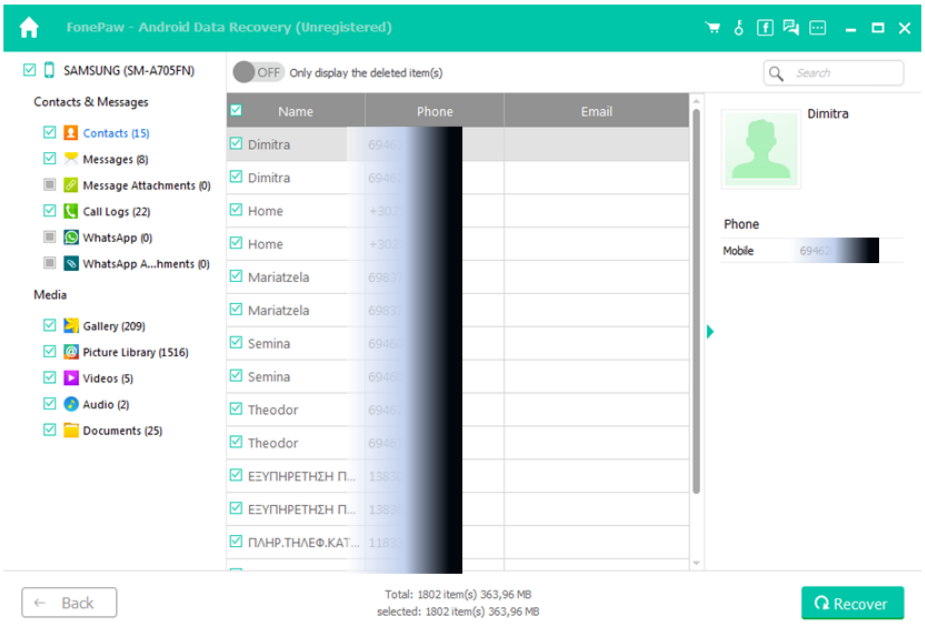
Το πρόγραμμα έχει καταφέρει να αναγνωρίσει σωστά το μοντέλο της συσκευής (Εικόνα 108) και κάτω από αυτό μας εμφανίζει αθροιστικά για κάθε κατηγορία όλα τα δεδομένα που κατάφερε να ανακτήσει (Εικόνα 109).



Εικόνα 108 - FonePaw Collected Evidence 1

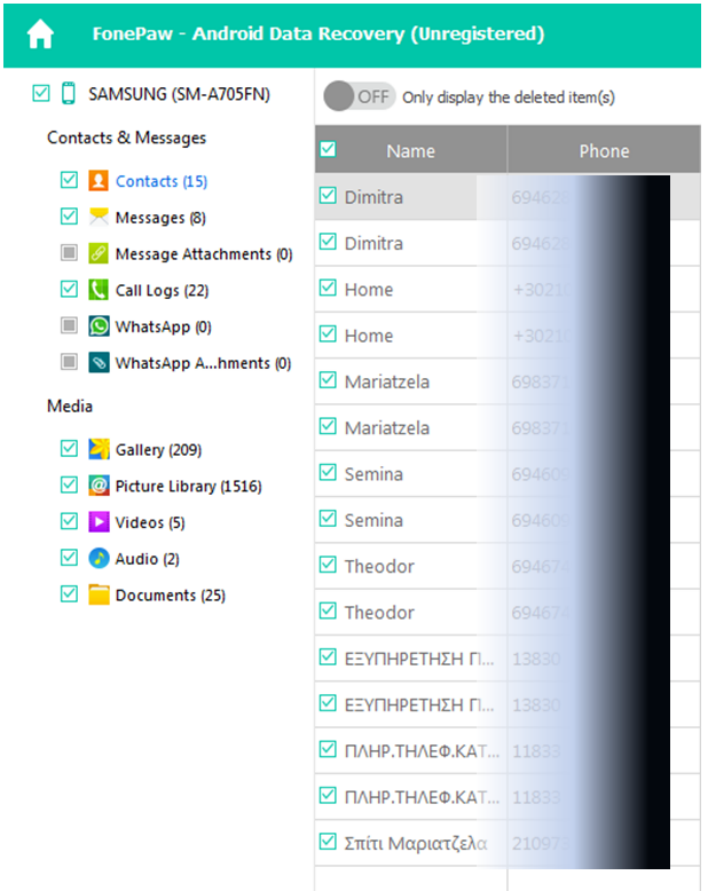


Εικόνα 109 - FonePaw Collected Evidence 2



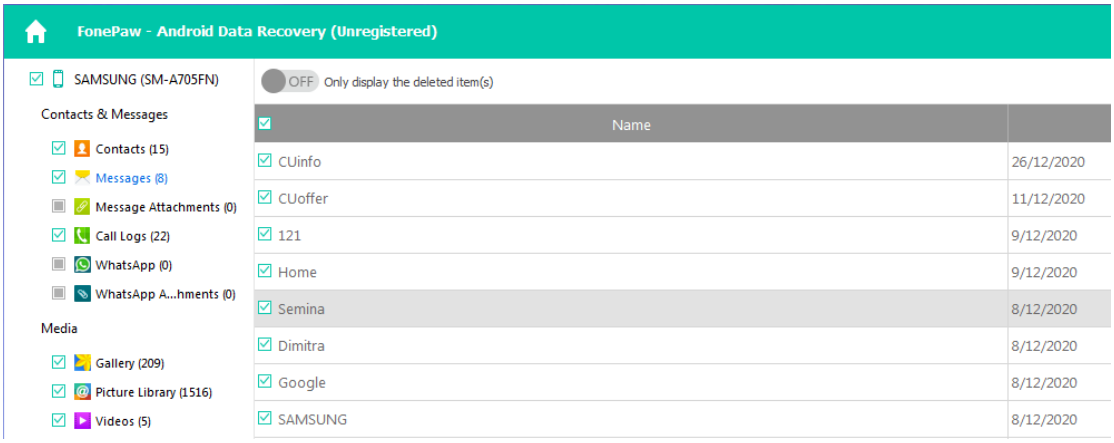
Εικόνα 110 - FonePaw - Contacts 1

Το FonePaw κατάφερε να ανακτήσει επιτυχώς τις επαφές που υπάρχουν στην συσκευή με όνομα επαφής και νούμερο (Εικόνα 110,Εικόνα 111).

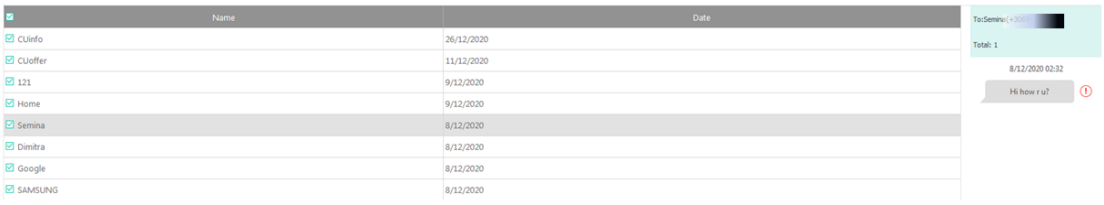


Εικόνα 111 - FonePaw - Contacts 2

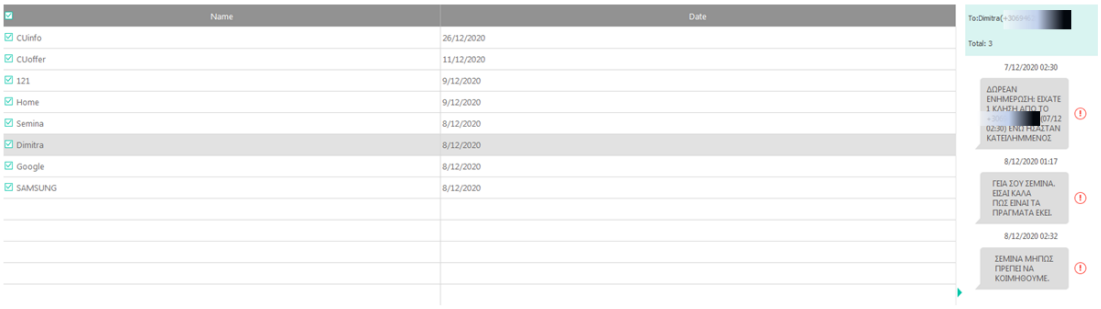
Στην συνέχεια βλέπουμε ότι το πρόγραμμα έχει καταφέρει να ανακτήσει επιτυχώς τα μηνύματα σε μορφή συνομιλίας όπως εμφανίζονται και στην συσκευή (Εικόνα 112, Εικόνα 113, Εικόνα 114).



Εικόνα 112 - FonePaw - SMS 1

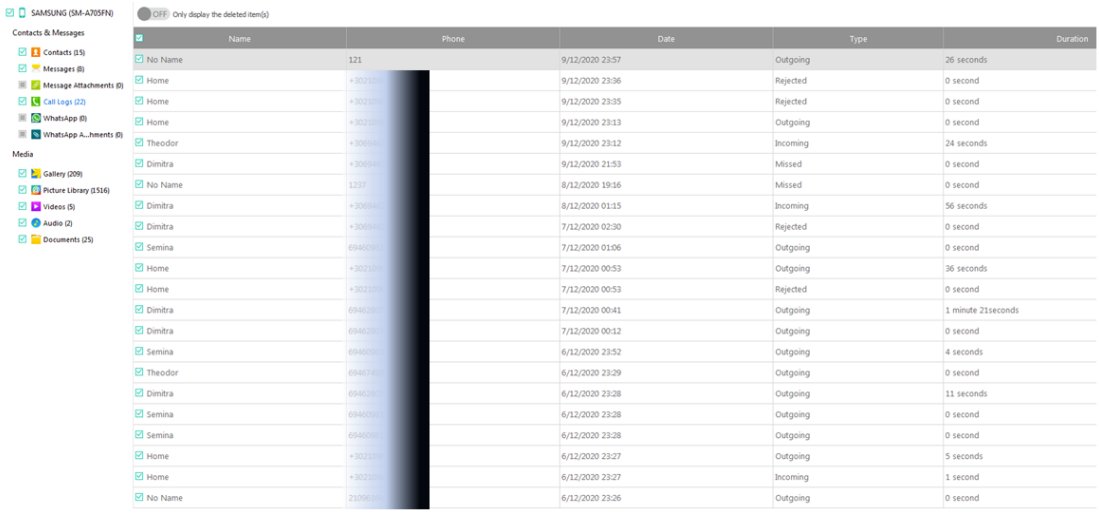


Εικόνα 113 - FonePaw - SMS 2



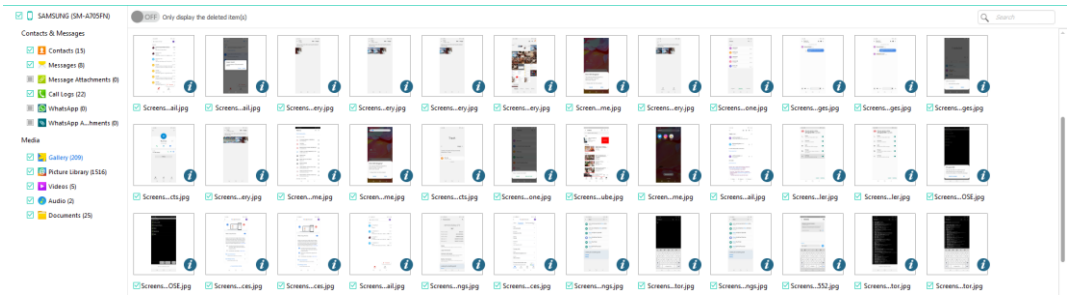
Εικόνα 114 - FonePaw - SMS 3

Όλες οι εισερχόμενες, εξερχόμενες, απορριφθείσες κλήσεις έχουν ανακτηθεί με επιτυχία όπως και η ημερομηνία και ώρα που έχουν πραγματοποιηθεί η διάρκειά τους καθώς και από ποιον έχουν γίνει (Εικόνα 115).



Εικόνα 115 - FonePaw - Call Logs

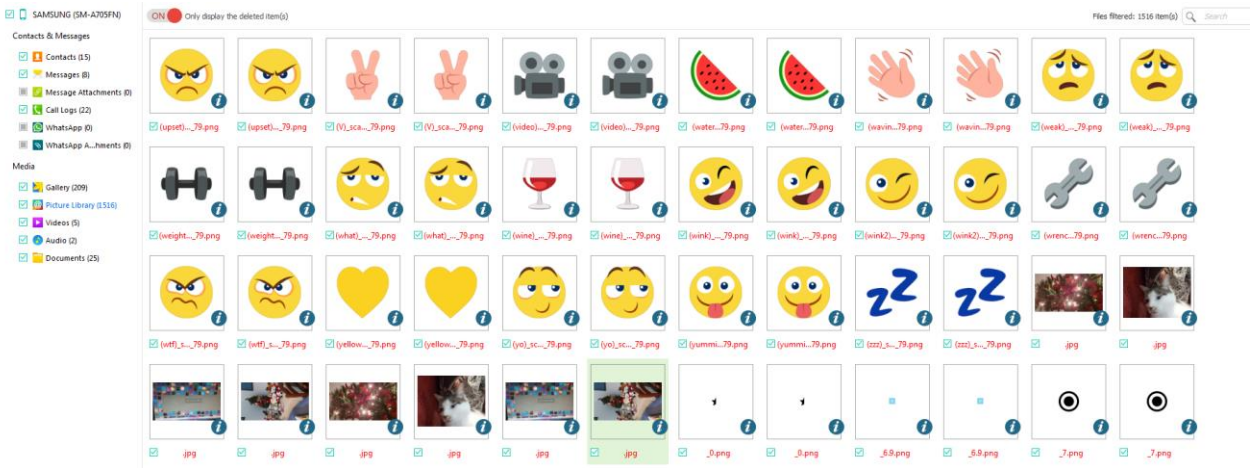
Έχουν ανακτηθεί επιτυχώς και όλες οι εικόνες που υπάρχουν στο Gallery της συσκευής (Εικόνα 116).



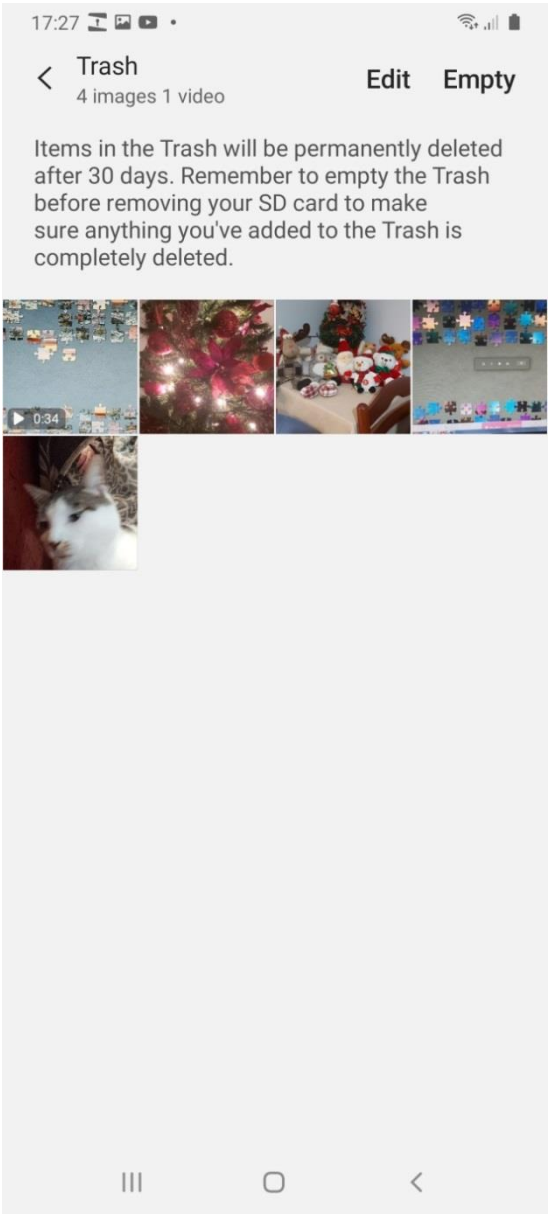
Εικόνα 116 - FonePaw - Pictures 1

Στην καρτέλα Picture Library παρατηρούμε ότι το πρόγραμμα έχει ανακτήσει και φωτογραφίες από το Trash της συσκευής (Εικόνα 117, Εικόνα 118, Εικόνα 119).

Εικόνα 117 - FonePaw - Pictures 2

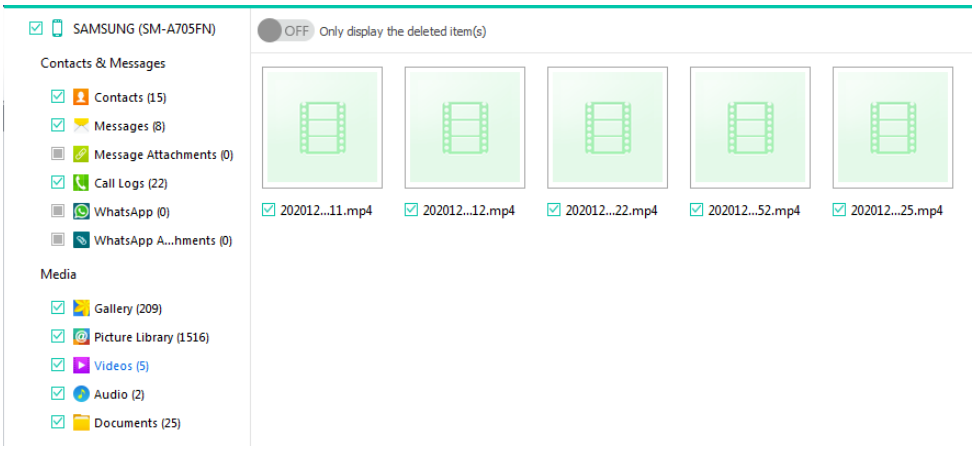


Εικόνα 118 - FonePaw - Pictures 3



Εικόνα 119 - Gallery Trash

Έχουν ανακτηθεί επιτυχώς και πέντε βίντεο από την συσκευή (Εικόνα 120).



Εικόνα 120 - FonePaw - Videos

Τέλος το FonePaw έχει καταφέρει να ανακτήσει και κάποια xml αρχεία από την συσκευή (Εικόνα 121).

Εικόνα 121 - FonePaw - Documents

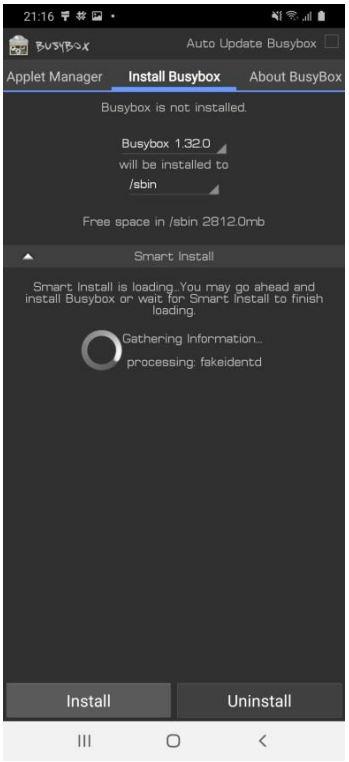
Η free trial εκδοχή που χρησιμοποιούμε δεν μας παρέχει την δυνατότητα να κάνουμε recover κάποιο αρχείο ενδιαφέροντος στον υπολογιστή μας.

Συγκριτικά με το AFLogical OSE που παρέχει το Santoku το FonePaw έχει καλύτερη απόδοση στα android 10 σε logical level εφόσον μπορεί να ανακτήσει επιτυχώς επαφές, κλήσεις, μηνύματα, εικόνες, βίντεο, αρχεία ενώ το AFLogical OSE δεν μπορούσε να ανακτήσει το αρχείο των επαφών και έπρεπε να πραγματοποιήσουμε εμείς το export από την συσκευή και μπορούσε να ανακτήσει μόνο κλήσεις και μηνύματα. Επιπλέον το FonePaw παρέχει αυτές τις δυνατότητες σε ένα φιλικό προς τον χρήστη περιβάλλον.

5. PHYSICAL IMAGE ACQUISITION

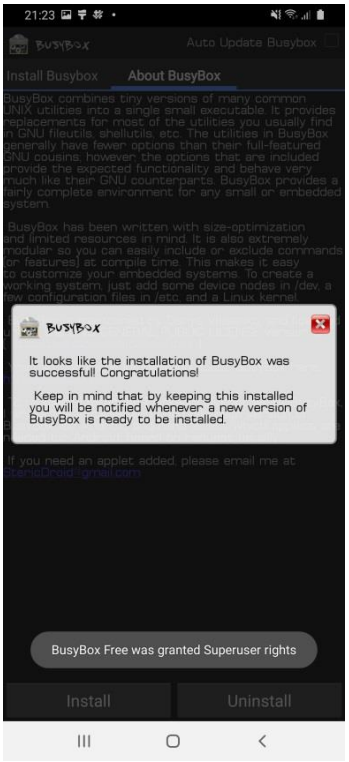
Πριν πραγματοποιήσουμε την διαδικασία της physical image forensics analysis πρέπει πρώτα να πάρουμε ένα image της συσκευής. Για να το πετύχουμε αυτό εγκαθιστούμε στην συσκευή την εφαρμογή BusyBox (Stericson) μέσω Play Store (Εικόνα 122). Η συγκεκριμένη εφαρμογή παρέχει την δυνατότητα να χρησιμοποιηθούν βασικά εργαλεία unix σε κινητές συσκευές.

Εικόνα 122 - BusyBox Welcome Message



Εικόνα 123 - BusyBox App

Μέσα από την εφαρμογή πατάμε install για να εγκαταστήσουμε όλες τις παροχές του BusyBox στην συσκευή (Εικόνα 123, Εικόνα 124).



Εικόνα 124 - BusyBox Installed

Από το adb shell προβάλουμε στο terminal τον πίνακα με τα διαφορετικά partitions της συσκευής, χρησιμοποιώντας την εντολή:

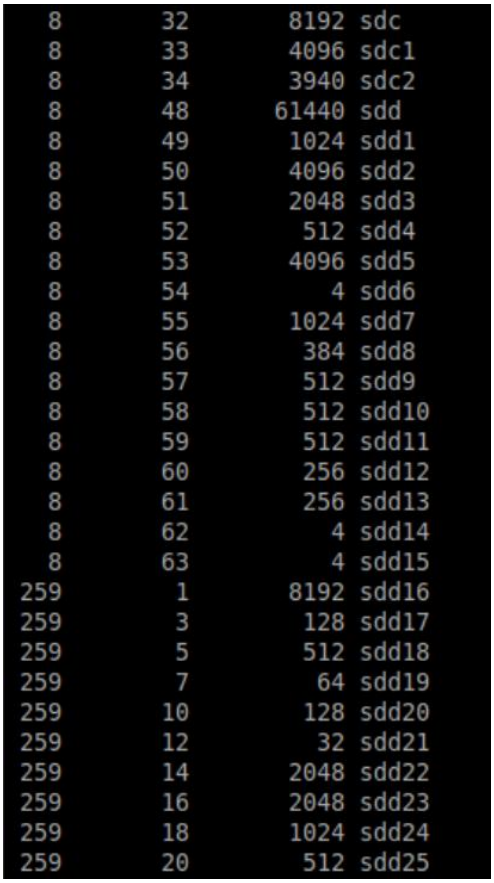
cat /proc/partitions (Εικόνα 125, Εικόνα 126, Εικόνα 127)

```
santoku@santoku-virtual-machine:~$ adb devices
List of devices attached
R58[redacted]          device

santoku@santoku-virtual-machine:~$ adb shell
a70q:/ $ su
a70q:/ # cat /proc/partitions
major minor  #blocks  name

   1        0       8192 ram0
   1        1       8192 ram1
   1        2       8192 ram2
   1        3       8192 ram3
   1        4       8192 ram4
   1        5       8192 ram5
   1        6       8192 ram6
   1        7       8192 ram7
   1        8       8192 ram8
   1        9       8192 ram9
   1       10       8192 ram10
   1       11       8192 ram11
   1       12       8192 ram12
   1       13       8192 ram13
   1       14       8192 ram14
   1       15       8192 ram15
 254        0    2097152 zram0
   8        0  124874752 sda
   8        1       2048 sda1
   8        2       2048 sda2
   8        3          4 sda3
```

Εικόνα 125 - Device Partitions 1

```
   8        4          8 sda4
   8        5      32768 sda5
   8        6      20480 sda6
   8        7      12288 sda7
   8        8      10240 sda8
   8        9      20480 sda9
   8       10       1024 sda10
   8       11        512 sda11
   8       12      40960 sda12
   8       13      21504 sda13
   8       14        512 sda14
   8       15       4096 sda15
 259        0      16384 sda16
 259        2      97280 sda17
 259        4      87040 sda18
 259        6      32768 sda19
 259        8      10240 sda20
 259        9      65536 sda21
 259       11      80884 sda22
 259       13    5632000 sda23
 259       15    1024000 sda24
 259       17     614400 sda25
 259       19     409600 sda26
 259       21      10240 sda27
 259       23      51200 sda28
 259       26  116573020 sda29
   8       16       8192 sdb
   8       17       4096 sdb1
   8       18       3940 sdb2
```

Εικόνα 126 - Device Partitions 2



```
  8       32       8192 sdc
  8       33       4096 sdc1
  8       34       3940 sdc2
  8       48      61440 sdd
  8       49       1024 sdd1
  8       50       4096 sdd2
  8       51       2048 sdd3
  8       52        512 sdd4
  8       53       4096 sdd5
  8       54          4 sdd6
  8       55       1024 sdd7
  8       56        384 sdd8
  8       57        512 sdd9
  8       58        512 sdd10
  8       59        512 sdd11
  8       60        256 sdd12
  8       61        256 sdd13
  8       62          4 sdd14
  8       63          4 sdd15
259        1       8192 sdd16
259        3        128 sdd17
259        5        512 sdd18
259        7         64 sdd19
259       10        128 sdd20
259       12         32 sdd21
259       14       2048 sdd22
259       16       2048 sdd23
259       18       1024 sdd24
259       20        512 sdd25
```

Εικόνα 127 - Device Partitions 3

Το partition που θα κάνουμε physical image είναι το sda.

Χρησιμοποιώντας τα εργαλεία dd και netcat παίρνουμε το physical forensic image της συσκευής.

Το dd είναι προεγκατεστημένο στο Santoku, θα πρέπει όμως να εγκαταστήσουμε το netcat χρησιμοποιώντας την εντολή:

sudo apt-get install netcat

Η διαδικασία του physical image acquisition θα πραγματοποιηθεί με την χρήση δύο terminal, ένα θα είναι su shell στην κινητή συσκευή και ένα θα είναι στον υπολογιστή μας.

Στο terminal που αφορά τον υπολογιστή μας μετακινούμαστε στον φάκελο που θέλουμε να αποθηκεύσουμε το image και εκτελούμε την εντολή (Εικόνα 128):

adb forward tcp:8888 tcp:8888

Η συγκεκριμένη εντολή δημιουργεί μια σύνδεση ανάμεσα στον υπολογιστή μας (στον σκληρό δίσκο που αποθηκεύουμε το image) και στο τηλέφωνο στην tcp port 8888.

Εικόνα 128 - adb forward

Στο terminal που αφορά στην συσκευή βρισκόμαστε σε su shell και εκτελούμε την εντολή (Εικόνα 129):

dd if=/dev/block/sda | busybox nc -l -p 8888

Αναλυτικότερα η συγκεκριμένη εντολή:

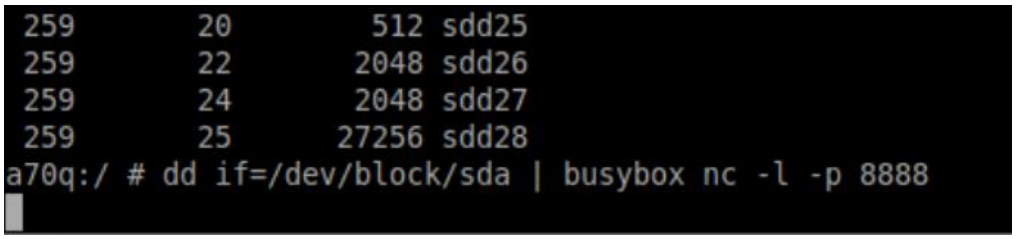
dd if=/dev/block/sda: Δίνει input το sda partition στο dd, το dd λοιπόν θα διαβάσει bit per bit το sda partition.

| busybox nc -l -p 8888: Δίνουμε το output του dd στο busybox το οποίο τρέχει το netcat.

-l -p 8888: Το -l σημαίνει ότι έχουμε ενεργοποιήσει το listen switch, κάνουμε έτσι το τηλέφωνο να ανοίγει μια listen port στο tcp port 8888, κάνοντας το συγκεκριμένο με το –p 8888.

Έτσι λοιπόν όταν έρχεται μια εισερχόμενη σύνδεση στο συγκεκριμένο port το dd θα στέλνει ανά bit όλο το sda partition.

Δεν πατάμε enter στην εντολή και επιστρέφουμε στο terminal που αφορά το workstation μας.



Εικόνα 129 - dd for sda partition

Χρησιμοποιώντας το netcat τώρα από τον υπολογιστή μας θα κάνουμε μια σύνδεση στο localhost στην tcp port 8888 , η οποία γίνεται forward από το adb και το input από εκεί θα το αποθηκεύσουμε στο αρχείο A70F.dd.

Η εντολή (Εικόνα 130):

nc 127.0.0.1 8888 > A70F.dd

Επιστρέφουμε στο terminal της συσκευής και πατάμε enter στην εντολή:

dd if=/dev/block/sda | busybox nc -l -p 8888

Στην συνέχεια πηγαίνουμε στο terminal που αφορά τον υπολογιστή μας και πατάμε enter στην εντολή:

nc 127.0.0.1 8888 > A70F.dd

```
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700$ adb forward tcp:8888 tcp:8888
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700$ nc 127.0.0.1 8888 > A70F.dd
```

Εικόνα 130 - netcat

Μόλις ολοκληρωθεί η διαδικασία στο terminal της συσκευής μπορούμε να δούμε τα αποτελέσματα, τα συνολικά bytes που αντιγράφθηκαν , πόσο διήρκησε η διαδικασία και τον ρυθμό που γινόταν η αντιγραφή σε kb/s (Εικόνα 131).

```
a70q:/ #  dd if=/dev/block/sda | busybox nc -l -p 8888
249749504+0 records in
249749504+0 records out
127871746048 bytes (119.1GB) copied, 143163.145502 seconds, 872.3KB/s
a70q:/ # exit
a70q:/ $ exit
santoku@santoku-virtual-machine:~$
```

Εικόνα 131 - Physical Image Finished 1

Στο terminal στο workstation μας η διαδικασία ολοκληρώνεται εφόσον έχει γίνει exit από την εντολή (Εικόνα 132).

```
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700$ adb forward tcp:8888 tcp:8888
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700$ nc 127.0.0.1 8888 > A70F.dd
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700$
```

Εικόνα 132 - Physical Image Finished 2

Τέλος υπολογίζουμε τις συνόψεις MD5 και SHA1 του physical image (Εικόνα 133) προκειμένου να μπορούμε να επιβεβαιώσουμε και να αποδείξουμε την ακεραιότητά του στο τέλος της διαδικασίας της ανάλυσης. Οι συγκεκριμένες συνόψεις θα πρέπει να παραμείνουν ίδιες σε όλη την διαδικασία της ανάλυσης, σε περίπτωση που στο τέλος της διαδικασίας της ανάλυσης οι συνόψεις διαφέρουν από αυτές που υπολογίσαμε στην αρχή της διαδικασίας σημαίνει ότι συνέβη τροποποίηση στο physical image και τα δεδομένα δεν είναι ίδια με αυτά που εξήχθησαν κατά την διαδικασία του physical image acquisition.

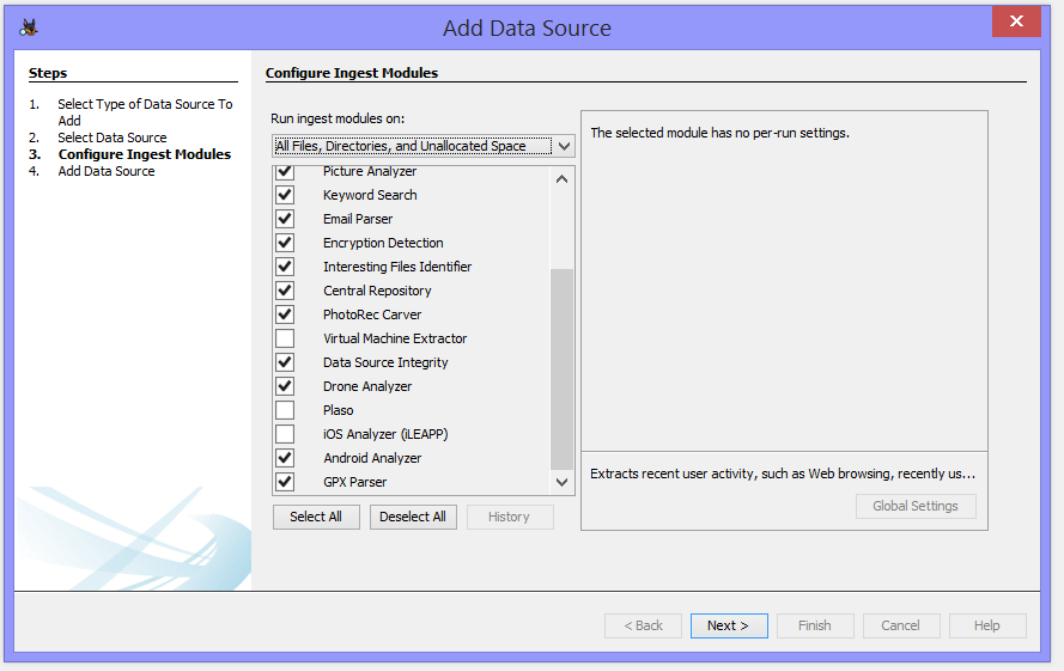
```
C:\Users\Σεμίνα\Desktop>CertUtil -hashfile A70F.dd MD5
Κατακερματισμός MD5 του αρχείου A70F.dd:
c6 9d e8 d8 60 e7 cd f9 75 05 16 25 7e a5 08 22
CertUtil: Η εντολή -hashfile ολοκληρώθηκε με επιτυχία.

C:\Users\Σεμίνα\Desktop>CertUtil -hashfile A70F.dd SHA1
Κατακερματισμός SHA1 του αρχείου A70F.dd:
48 21 b9 11 31 29 f7 2c 3c a0 67 db f2 48 50 52 3f ac 34 5d
CertUtil: Η εντολή -hashfile ολοκληρώθηκε με επιτυχία.
```

Εικόνα 133 - Physical Image MD5 & SHA 1 Hashes

6. PHYSICAL ANALYSIS

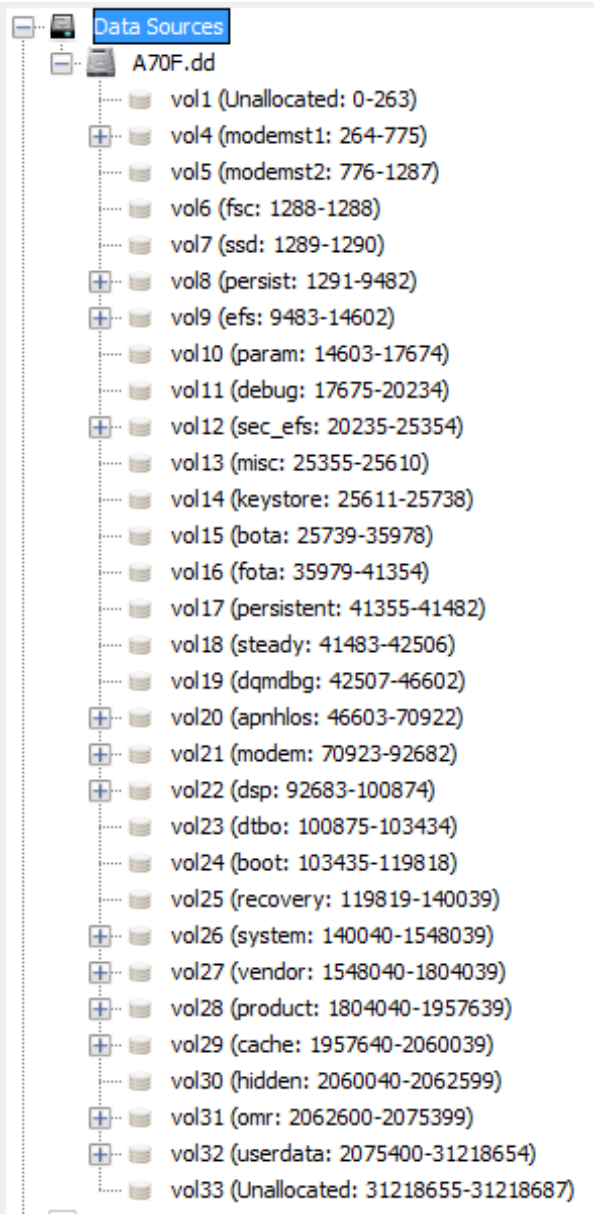
6.1 AUTOPSY

Για την ανάλυση του physical image χρησιμοποιήσαμε το Autopsy version 4.17.0. Το Autopsy παρέχει γραφικό περιβάλλον, ομαδοποίηση των δεδομένων σύμφωνα με συγκεκριμένους τύπους αρχείων, παρέχεται επίσης η δυνατότητα keyword search και δημιουργίας timeline. Επιπρόσθετα με το Android Analyzer Module μπορεί να αναλύσει physical images από android συσκευές (Εικόνα 134).



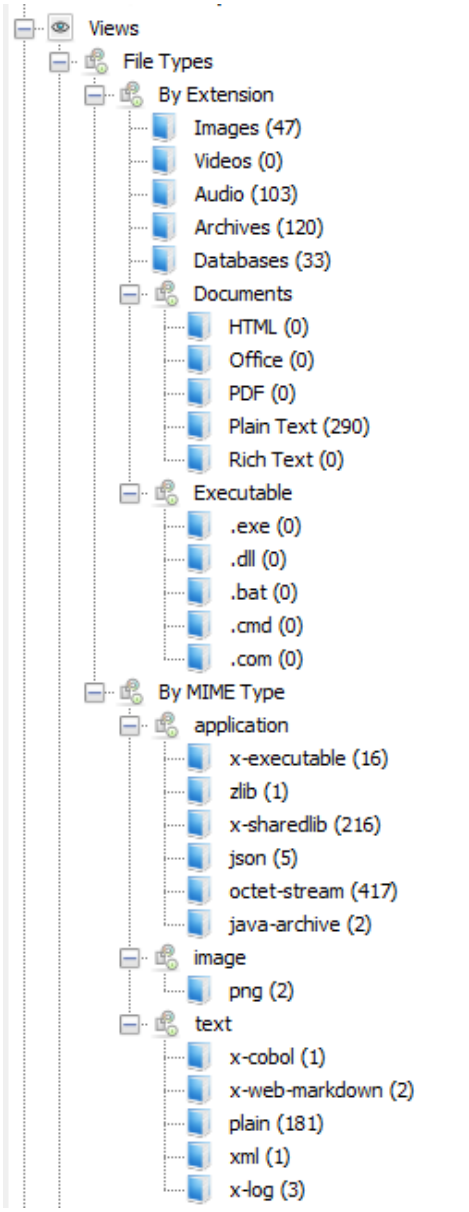
Εικόνα 134 - Autopsy Modules

Το autopsy ανοίγοντας το image δημιουργεί ένα evidence tree (Εικόνα 135). Στην συγκεκριμένη περίπτωση έχουμε ανοίξει το image A70F.dd, το autopsy θα αναλύσει το συγκεκριμένο image σε volumes/partitions όπως ήταν δομημένη και η κινητή συσκευή.

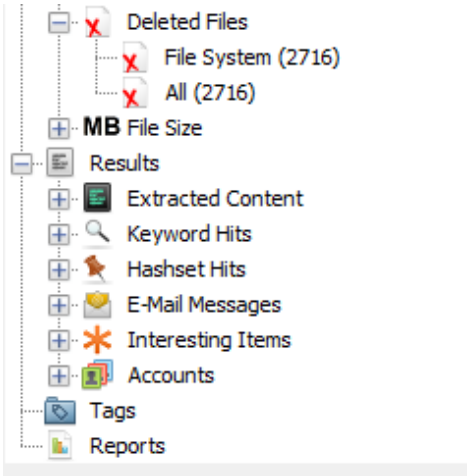


Εικόνα 135 - Evidence Tree - Volumes

Στην συνέχεια του evidence tree το autopsy ομαδοποιεί διάφορα δεδομένα με βάση τον τύπο αρχείου, επιπρόσθετα έχει εντοπίσει όλα τα deleted files (Εικόνα 136, Εικόνα 137).

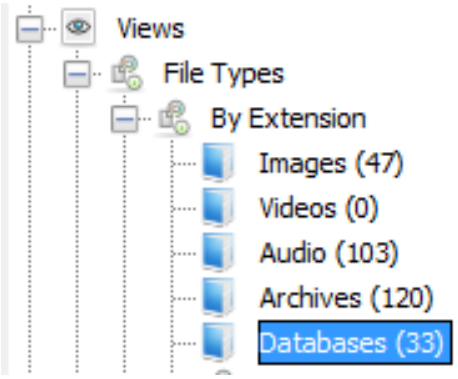


Εικόνα 136 - Evidence Tree - File Types

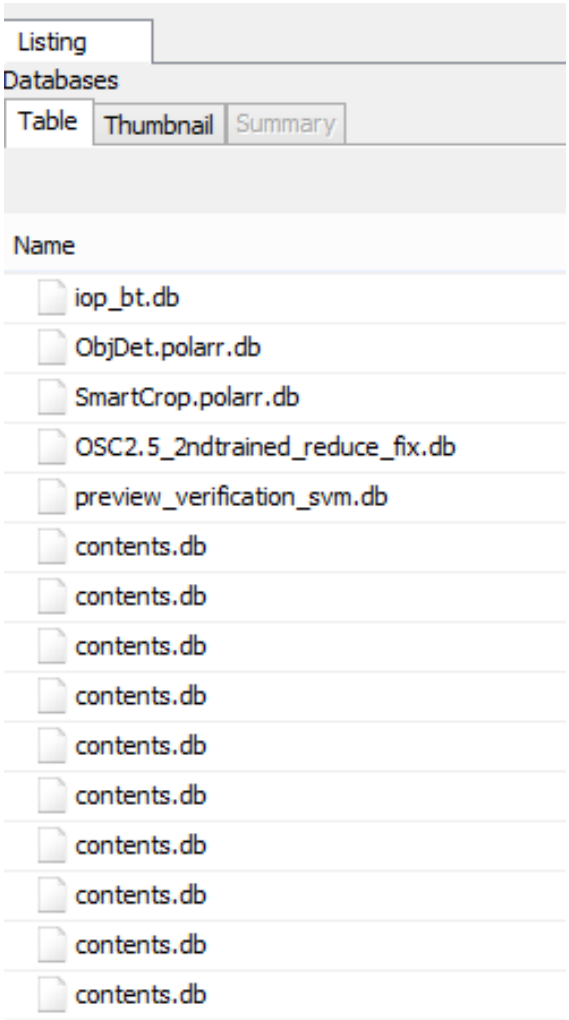


Εικόνα 137 - Evidence Tree - Deleted Files

Πηγαίνοντας όμως να δούμε τις βάσεις δεδομένων (Εικόνα 138) που έχει αναγνωρίσει το autopsy παρατηρούμε ότι πέρα από κάποιες βάσεις που δεν διαθέτουν ιδιαίτερες πληροφορίες το autopsy αναγνωρίζει τις βάσεις ως contents.db (Εικόνα 139) και δεν αναγνωρίζει τις βασικές βάσεις που διαχειρίζεται το android για να αποθηκεύει δεδομένα.

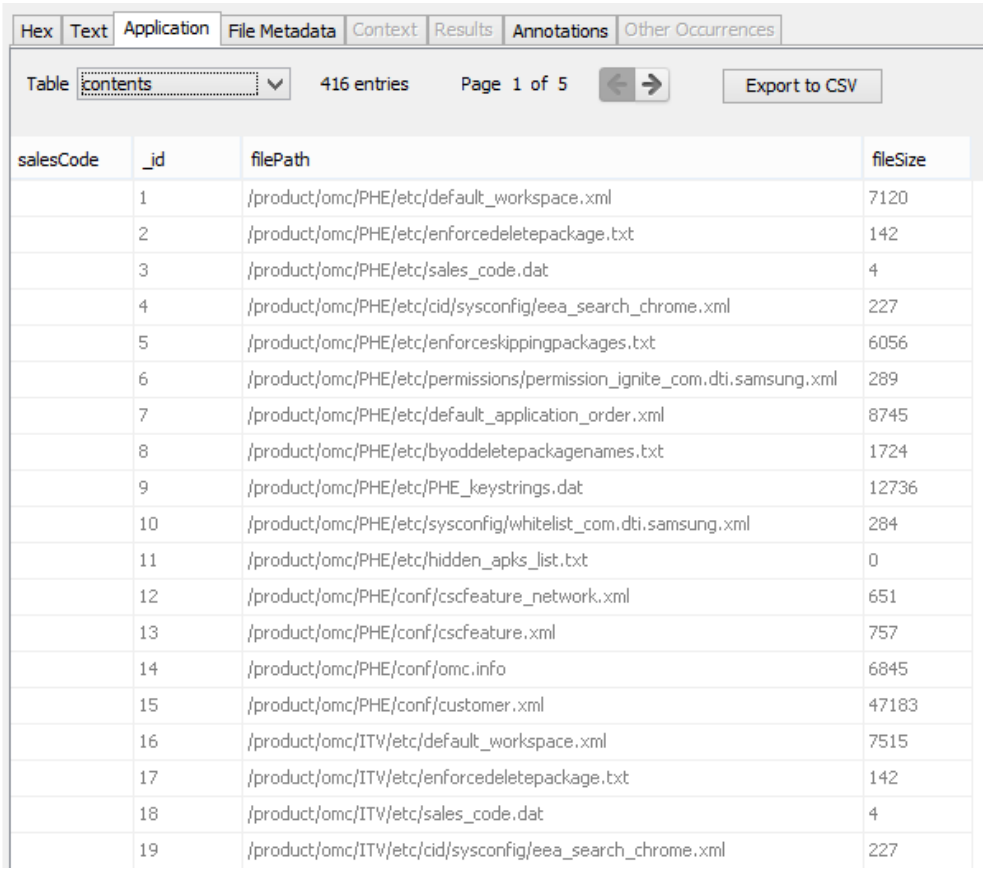


Εικόνα 138 - Databases



Εικόνα 139 - Databases Listing

Οι βάσεις contents.db δεν διαθέτουν δεδομένα από την δραστηριότητα του χρήστη στην συσκευή (Εικόνα 140).



Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Table: contents — 416 entries — Page 1 of 5 — Export to CSV

salesCode	_id	filePath	fileSize
	1	/product/omc/PHE/etc/default_workspace.xml	7120
	2	/product/omc/PHE/etc/enforcedeletepackage.txt	142
	3	/product/omc/PHE/etc/sales_code.dat	4
	4	/product/omc/PHE/etc/cid/sysconfig/eea_search_chrome.xml	227
	5	/product/omc/PHE/etc/enforceskippingpackages.txt	6056
	6	/product/omc/PHE/etc/permissions/permission_ignite_com.dti.samsung.xml	289
	7	/product/omc/PHE/etc/default_application_order.xml	8745
	8	/product/omc/PHE/etc/byoddeletepackagenames.txt	1724
	9	/product/omc/PHE/etc/PHE_keystrings.dat	12736
	10	/product/omc/PHE/etc/sysconfig/whitelist_com.dti.samsung.xml	284
	11	/product/omc/PHE/etc/hidden_apks_list.txt	0
	12	/product/omc/PHE/conf/cscfeature_network.xml	651
	13	/product/omc/PHE/conf/cscfeature.xml	757
	14	/product/omc/PHE/conf/omc.info	6845
	15	/product/omc/PHE/conf/customer.xml	47183
	16	/product/omc/ITV/etc/default_workspace.xml	7515
	17	/product/omc/ITV/etc/enforcedeletepackage.txt	142
	18	/product/omc/ITV/etc/sales_code.dat	4
	19	/product/omc/ITV/etc/cid/sysconfig/eea_search_chrome.xml	227

Εικόνα 140 - Περιεχόμενα Database

Το autopsy συνεπώς μπορεί να ανοίξει το image μόνο σε high level, δηλαδή σε επίπεδο partitions και δεν μπορεί να διαβάσει τα δεδομένα.

Το Autopsy υποστηρίζει τα ακόλουθα file systems:

- NTFS
- FAT 12/16/32
- ExFAT
- HFS+
- Yaffs2
- UFS1/2
- EXT2/3/4
- ISO9660 (CD-ROM)

Σε su shell στην συσκευή δίνουμε την εντολή blkid (Εικόνα 141) για να δούμε τι file systems είναι τα partitions. Παρατηρούμε ότι τα partitions της συσκευής είναι ext4 και vfat , τα partitions που είναι ext4 υποστηρίζονται από το autopsy ενώ το vfat δεν υποστηρίζεται από το autopsy.

```
santoku@santoku-virtual-machine:~$ adb shell
a70q:/ $ su
a70q:/ # blkid
/dev/block/vold/public:179,1: UUID="3701-06FD" TYPE="vfat"
/dev/block/zram0: UUID="2ba2f469-02c6-4e82-94be-556421e6f993" TYPE="swap"
/dev/block/sda18: UUID="00BC-614E" TYPE="vfat"
/dev/block/sda29: LABEL="data" UUID="3eef01a3-9a84-4f67-acc4-f6680cc19154" TYPE=
"ext4"
/dev/block/mmcblk0p1: UUID="3701-06FD" TYPE="vfat"
/dev/block/sda17: UUID="00BC-614E" TYPE="vfat"
/dev/block/sda5: LABEL="persist" UUID="bf85faa3-c647-56cc-bdbb-cc04a4b1cad9" TYP
E="ext4"
/dev/block/sda19: LABEL="dsp" UUID="af32c008-2a39-7e5b-a5dc-201456d93103" TYPE="
ext4"
/dev/block/sda9: LABEL="sec_efs" UUID="736edfa6-0b7c-5264-800a-7bb203039c7d" TYP
E="ext4"
/dev/block/sda26: LABEL="cache" UUID="6e9bd3c2-5ec5-4399-9bf7-c5e23dfebeac" TYPE
="ext4"
/dev/block/sda28: LABEL="omr" UUID="b938e0b2-b515-53a5-9fd5-d72c52a610ba" TYPE="
ext4"
/dev/block/sda6: LABEL="efs" UUID="563d3d87-578d-5542-b8fe-7ffa3ca08c8a" TYPE="e
xt4"
```

Εικόνα 141 - Device Partitions File Systems

Συνεπώς το Autopsy μπορεί να αναγνωρίσει το image και να το ανοίξει σε high level επίπεδο εφόσον αναγνωρίζει μερικώς τα file systems που χρησιμοποιούν τα partitions της συσκευής. Το Autopsy μπορεί και δημιουργεί το evidence tree και την δομή των partitions με τα αρχεία τους , δεν μπορεί όμως να αναλύσει το image σε βαθύτερο επίπεδο. Αυτό συμβαίνει πιθανώς γιατί το Autopsy δεν υποστηρίζει το vfat file system και το scoped storage που έχουν εισάγει τα android 10. Αξίζει να αναφέρουμε ότι στο χρονικό διάστημα που έχει πραγματοποιηθεί η έρευνα της διπλωματικής στο documentation του προγράμματος δεν αναφέρεται κάτι για το συγκεκριμένο πρόβλημα.

Γνωρίζουμε ότι το λειτουργικό σύστημα android απαρτίζεται ουσιαστικά από ένα σύνολο βάσεων δεδομένων, μπορούμε λοιπόν να αποδείξουμε ότι οι βάσεις δεδομένων υπάρχουν στην συσκευή και έχουν καταγράψει δεδομένα απλώς το autopsy δεν μπορεί να τις αναγνωρίσει. Αυτό μπορούμε να το κάνουμε εισάγοντας μια microsd κάρτα στην συσκευή και αντιγράφοντας τις βάσεις δεδομένων εκεί για να εξετάσουμε τα περιεχόμενά τους.

Στόχος μας είναι να πάρουμε και να εξετάσουμε τα περιεχόμενα της βάσης contacts2.db.

Από su shell στην συσκευή μετακινούμαστε στο directory /data/data/com.samsung.android.providers.contacts/databases και δίνουμε την εντολή ls για να δούμε τις βάσεις δεδομένων που υπάρχουν στο directory (Εικόνα 142).

```
a70q:/data/data # cd com.samsung.android.providers.contacts/databases
a70q:/data/data/com.samsung.android.providers.contacts/databases # ls
calllog.db          contacts2.db       profile.db          profile_sa.db
calllog.db-shm      contacts2.db-shm   profile.db-shm      profile_sa.db-shm
calllog.db-wal      contacts2.db-wal   profile.db-wal      profile_sa.db-wal
a70q:/data/data/com.samsung.android.providers.contacts/databases #
```

Εικόνα 142 - /data/data/com.samsung.android.providers.contacts/databases

Δίνουμε την ακόλουθη εντολή για να αντιγράψουμε την βάση δεδομένων contacts2.db με τα περιεχόμενά της στην sd card (Εικόνα 143):

cp contacts2.db /sdcard/contacts2.db

Στην συνέχεια κάνουμε exit από το su shell και στο terminal δίνουμε την εντολή (Εικόνα 143):

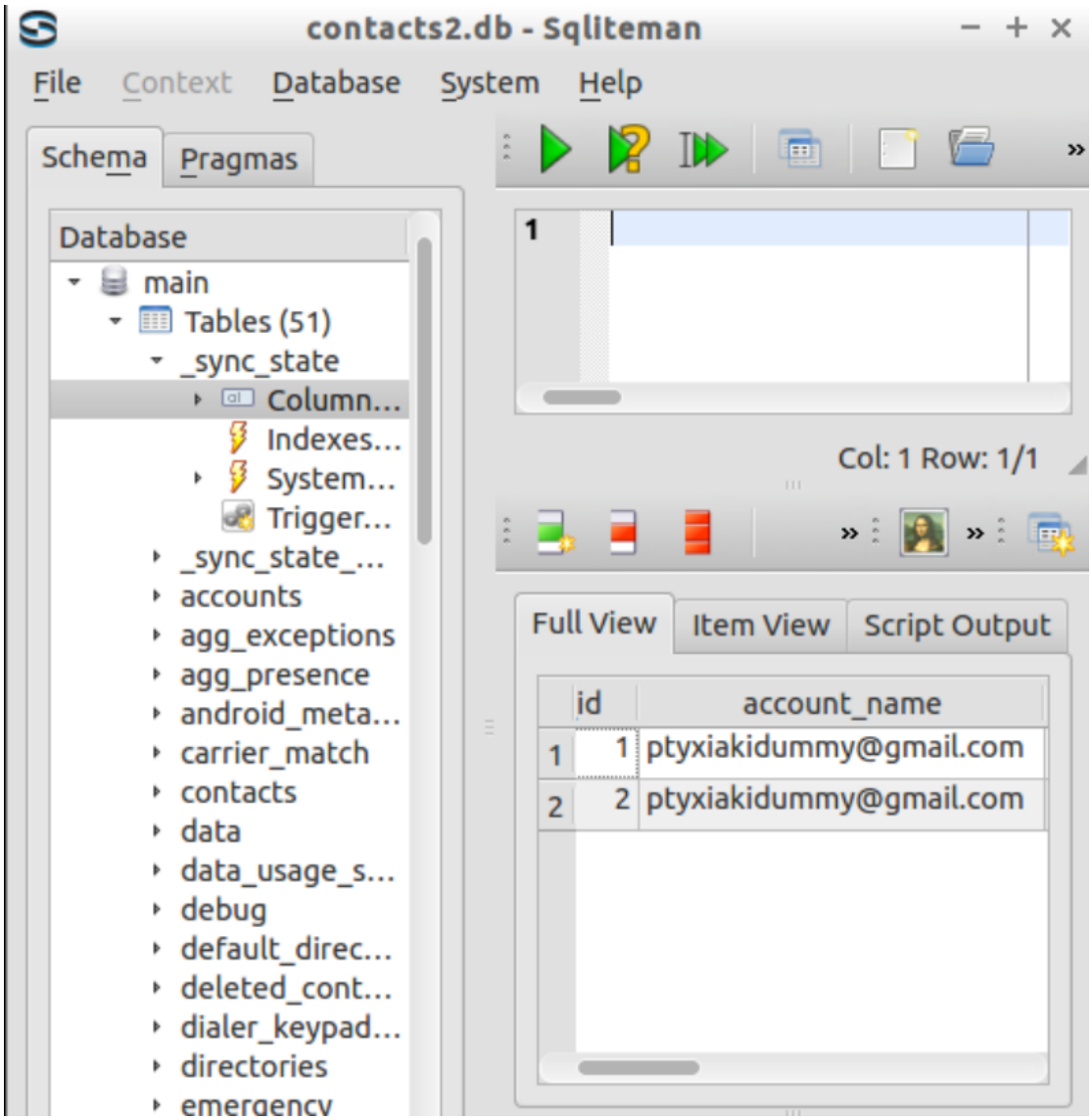
adb pull /sdcard/contacts2.db

Και παίρνουμε την βάση δεδομένων στον υπολογιστή μας.

```
                                  +306[redacted]  '0a70q:/data/data/com.samsung.androi
.providers.contacts/databases # ls
calllog.db          contacts2.db       profile.db          profile_sa.db
calllog.db-shm      contacts2.db-shm   profile.db-shm      profile_sa.db-shm
calllog.db-wal      contacts2.db-wal   profile.db-wal      profile_sa.db-wal
p contacts2.db /sdcard/contacts2.db                                          <
a70q:/data/data/com.samsung.android.providers.contacts/databases # exit
a70q:/ $ exit
santoku@santoku-virtual-machine:~$ adb pull /sdcard/contacts2.db
1629 KB/s (491520 bytes in 0.294s)
santoku@santoku-virtual-machine:~$
```

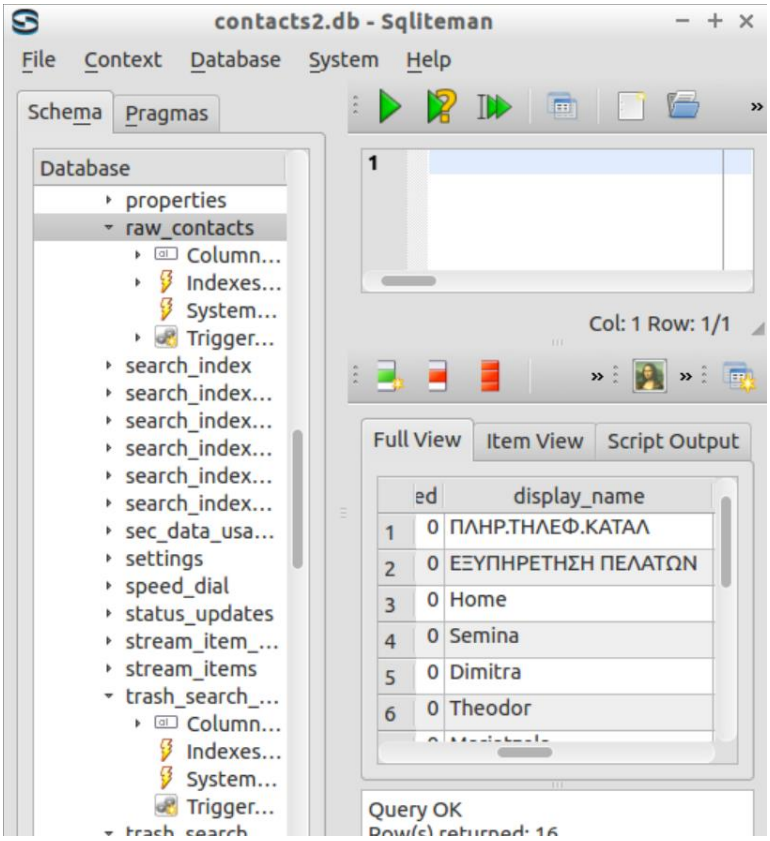
Εικόνα 143 - adb pull database contacts2.db from sdcard

Ανοίγουμε την βάση contacts2.db χρησιμοποιώντας το πρόγραμμα Sqliteman από το Santoku. Το Google Account που βρίσκεται σε synchronization state με την συσκευή είναι το ptyxiakidummy@gmail.com (Εικόνα 144).

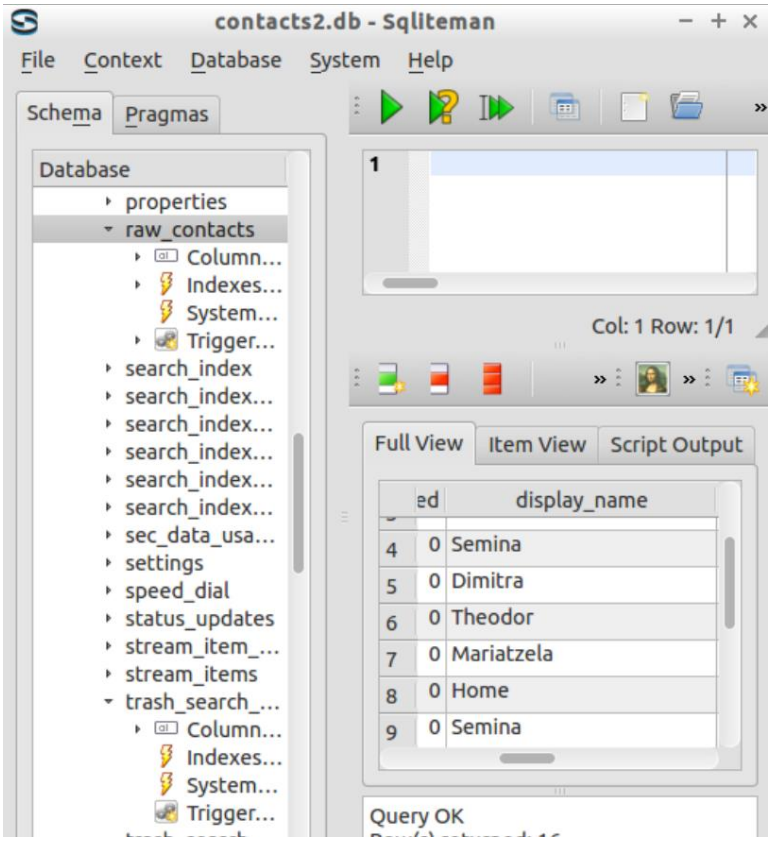


Εικόνα 144 - Gmail on Device

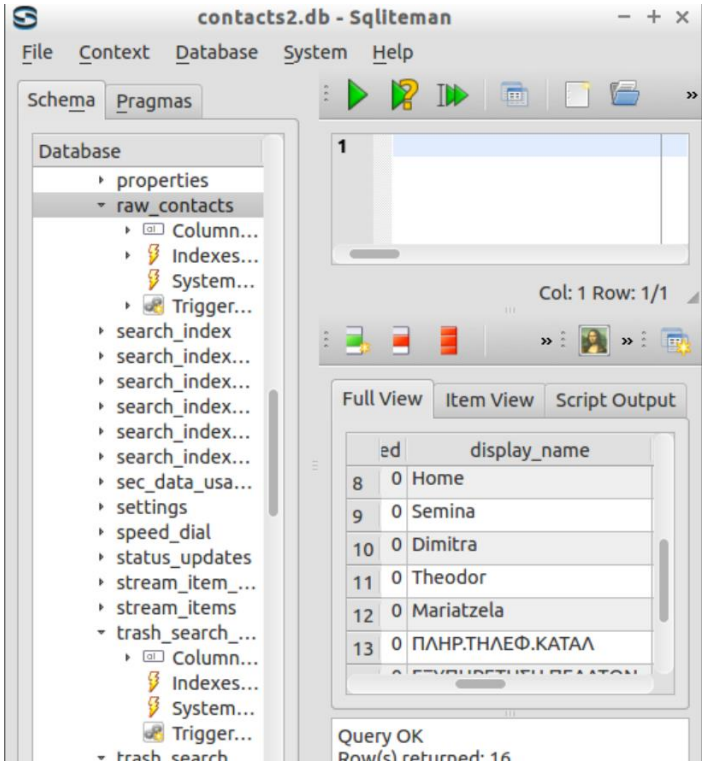
Στην συνέχεια στο table raw_contacts μπορούμε να δούμε όλες τις υπάρχουσες επαφές στην συσκευή (Εικόνα 145, Εικόνα 146, Εικόνα 147, Εικόνα 148).



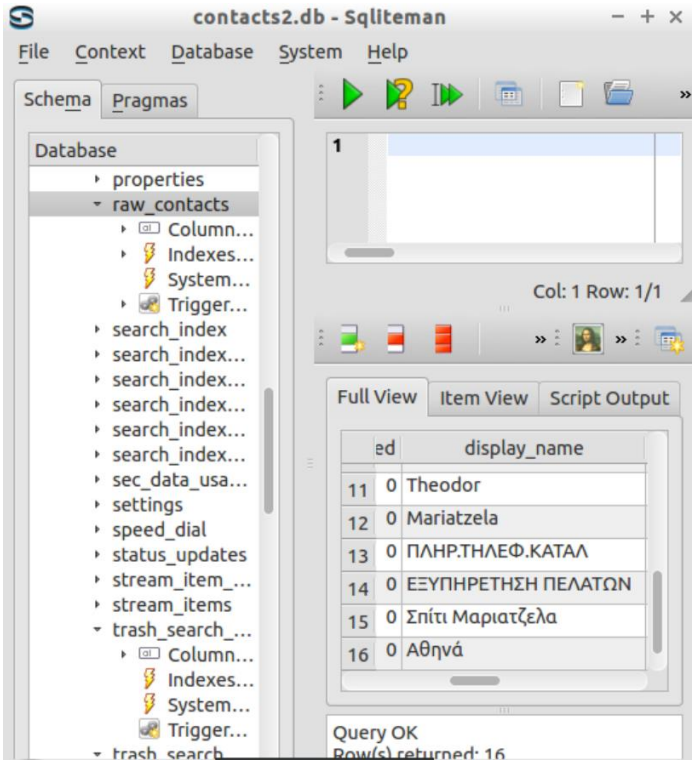
Εικόνα 145 - Raw Contacts on Device 1



Εικόνα 146 - Raw Contacts on Device 2



Εικόνα 147 - Raw Contacts on Device 3



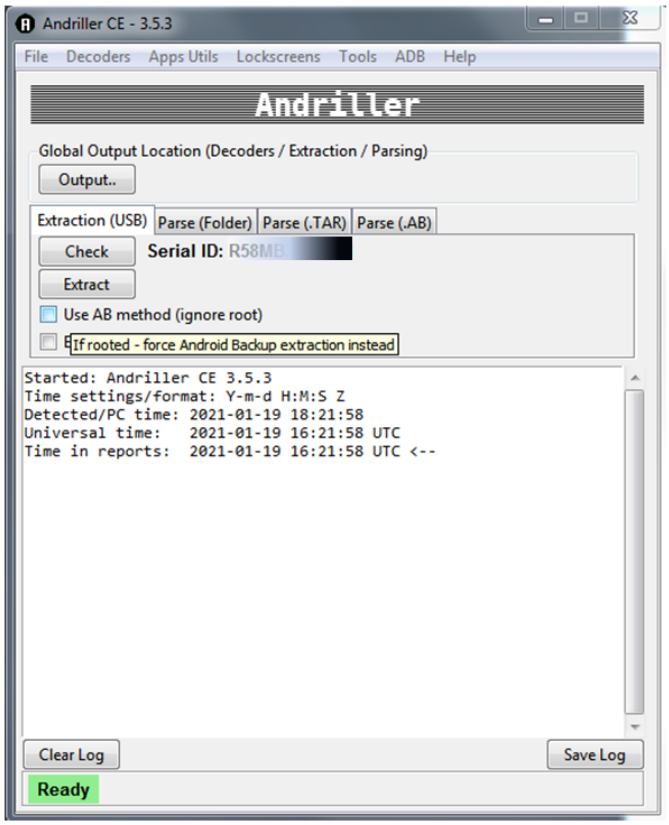
Εικόνα 148 - Raw Contacts on Device 4

Παρατηρούμε λοιπόν ότι τα δεδομένα υπάρχουν στις βάσεις δεδομένων και το autopsy δεν μπορεί να τα ανακτήσει από το physical image.

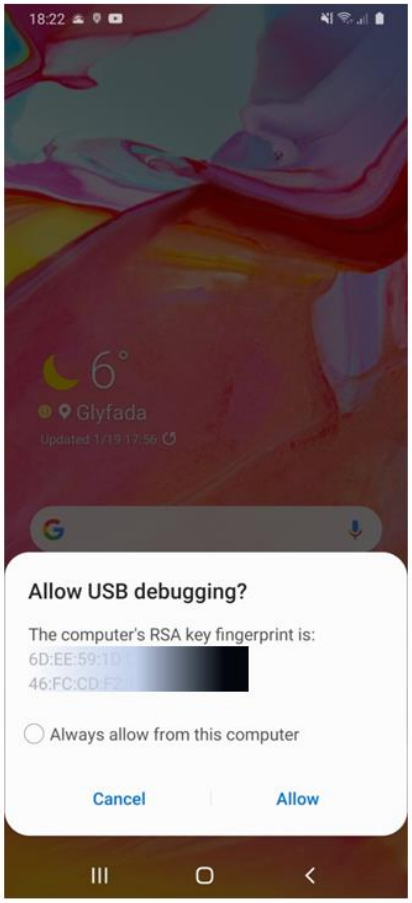
6.2 ANDRILLER

Μία άλλη open source εκδοχή προγράμματος για ανάλυση σε physical level χρησιμοποιώντας σωστές πρακτικές forensics είναι το Andriller. Το πρόγραμμα αυτό απαιτεί root πρόσβαση στο τηλέφωνο και ενεργοποιημένο usb debugging για να λειτουργήσει. Το πρόγραμμα αυτό προσπαθεί να πάρει πρόσβαση στις βάσεις δεδομένων του android που έχουν τις πληροφορίες που μας ενδιαφέρουν.

Στην αρχική οθόνη του Andriller επιλέγουμε Check και στο κινητό επιλέγουμε Allow στο μήνυμα που θα εμφανιστεί (Εικόνα 150). Με αυτό τον τρόπο αναγνωρίζει το andriller την συσκευή. Εάν έχει γίνει επιτυχημένη αναγνώριση συσκευής θα εμφανιστεί το serial number της συσκευής (Εικόνα 149).

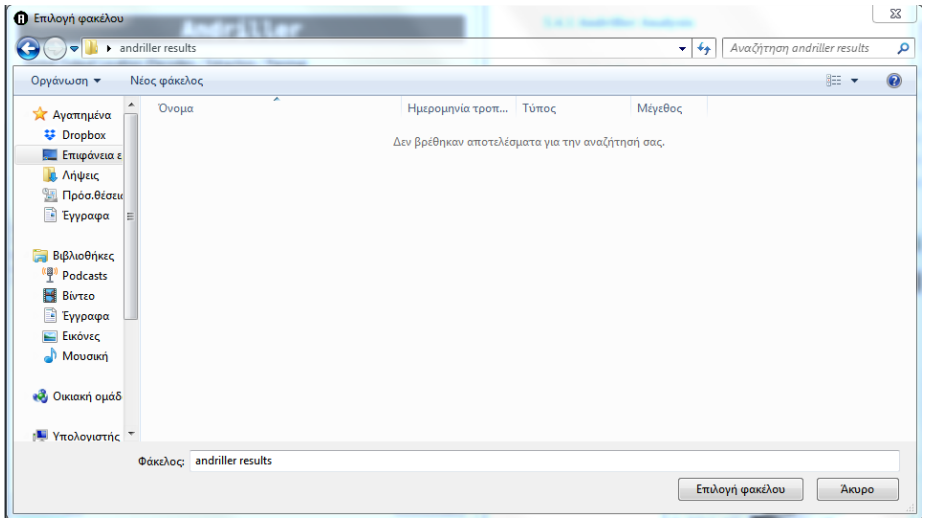


Εικόνα 149 - Andriller



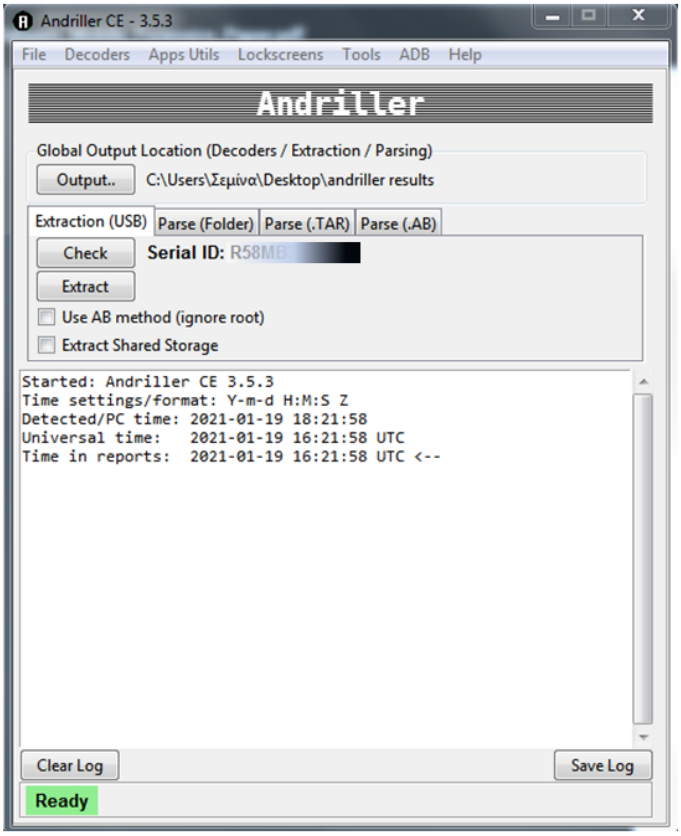
Εικόνα 150 - Andriller - Allow USB debugging?

Στην συνέχεια επιλέγουμε output και επιλέγουμε έναν φάκελο στο workstation μας για να αποθηκεύσει το Andriller τα αποτελέσματα (Εικόνα 151).

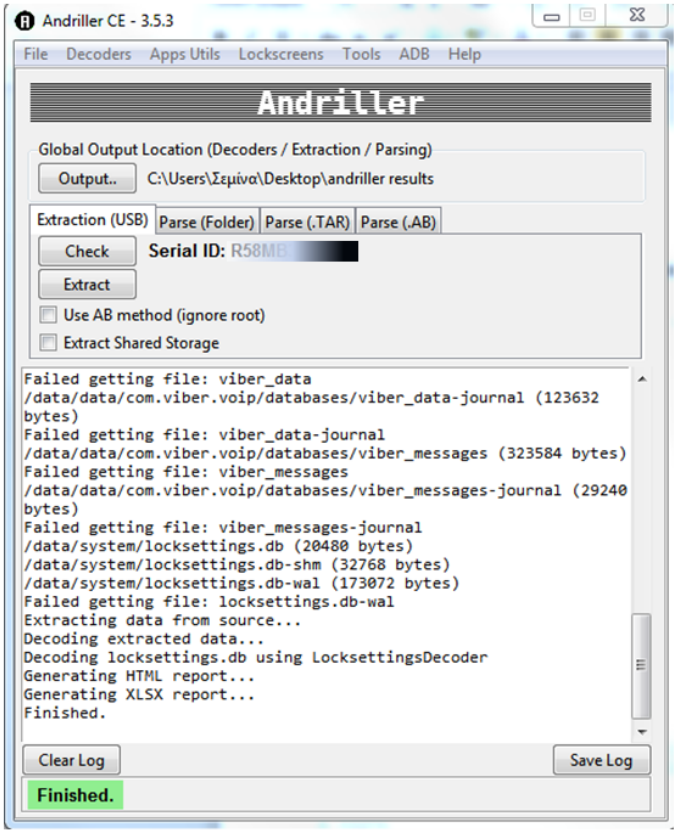


Εικόνα 151 - Andriller Results Folder

Πατάμε Extract για να εκκινήσει η διαδικασία (Εικόνα 152).



Εικόνα 152 - Andriller – Extract



Εικόνα 153 - Andriller - Finished

C:\Users\Σεμίνα\Desktop\andriller results\andriller.log - Notepad++

Αρχείο Επεξεργασία Εύρεση Προβολή Κωδικοποίηση Γλώσσα Ρυθμίσεις Μακροεντολή Εκτέλεση Πρόσθετ

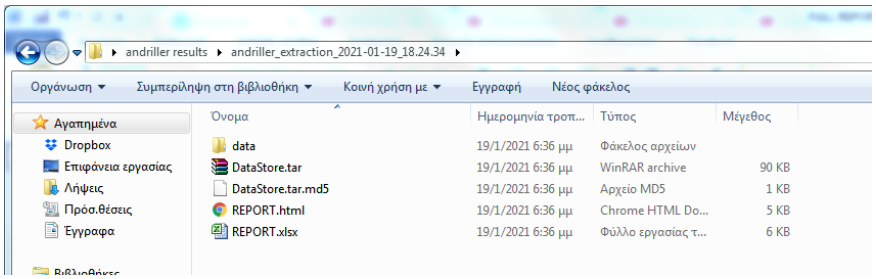
andriller.log

```
1  Started: Andriller CE 3.5.3
2  Time settings/format: Y-m-d H:M:S Z
3  Detected/PC time: 2021-01-19 18:21:58
4  Universal time:   2021-01-19 16:21:58 UTC
5  Time in reports:  2021-01-19 16:21:58 UTC <--
6  Reading information...
7  Acquiring data...
8  Acquiring databases via root...
9  /data/data/com.android.chrome/app_chrome/Default/History (196608 bytes)
10 Failed getting file: History
11 /data/data/com.android.chrome/app_chrome/Default/History-journal (8720 bytes)
12 Failed getting file: History-journal
13 /data/data/com.android.chrome/app_chrome/Default/Login Data (36864 bytes)
14 Failed getting file: Login Data
15 /data/data/com.android.providers.calendar/databases/calendar.db (204800 bytes)
16 Failed getting file: calendar.db
17 /data/data/com.android.providers.calendar/databases/calendar.db-journal (25136 bytes)
18 Failed getting file: calendar.db-journal
19 /data/data/com.android.providers.downloads/databases/downloads.db (24576 bytes)
20 Failed getting file: downloads.db
21 /data/data/com.android.providers.downloads/databases/downloads.db-journal (12824 bytes)
22 Failed getting file: downloads.db-journal
23 /data/data/com.android.providers.telephony/databases/mmssms.db (389120 bytes)
24 Failed getting file: mmssms.db
25 /data/data/com.android.providers.telephony/databases/mmssms.db-shm (32768 bytes)
26 /data/data/com.android.providers.telephony/databases/mmssms.db-wal (362592 bytes)
27 Failed getting file: mmssms.db-wal
28 /data/data/com.facebook.orca/databases/threads_db2 (307200 bytes)
29 Failed getting file: threads_db2
30 /data/data/com.facebook.orca/databases/threads_db2-journal (51200 bytes)
31 Failed getting file: threads_db2-journal
32 /data/data/com.google.android.apps.photos/databases/gphotos-1.db (1589248 bytes)
33 Failed getting file: gphotos-1.db
34 /data/data/com.google.android.apps.photos/databases/gphotos-1.db-shm (32768 bytes)
35 Failed getting file: gphotos-1.db-shm
36 /data/data/com.google.android.apps.photos/databases/gphotos-1.db-wal (524288 bytes)
37 Failed getting file: gphotos-1.db-wal
38 /data/data/com.viber.voip/databases/viber_data (122880 bytes)
39 Failed getting file: viber_data
40 /data/data/com.viber.voip/databases/viber_data-journal (123632 bytes)
41 Failed getting file: viber_data-journal
42 /data/data/com.viber.voip/databases/viber_messages (323584 bytes)
43 Failed getting file: viber_messages
44 /data/data/com.viber.voip/databases/viber_messages-journal (29240 bytes)
45 Failed getting file: viber_messages-journal
46 /data/system/locksettings.db (20480 bytes)
47 /data/system/locksettings.db-shm (32768 bytes)
48 /data/system/locksettings.db-wal (173072 bytes)
49 Failed getting file: locksettings.db-wal
50 Extracting data from source...
51 Decoding extracted data...
52 Decoding locksettings.db using LocksettingsDecoder
53 Generating HTML report...
54 Generating XLSX report...
55 Finished.
```

Εικόνα 154 - Andriller Full Log File

Τελειώνοντας την διαδικασία παρατηρούμε ότι το Andriller έχει αποτύχει να κάνει recover σχεδόν όλες τις βάσεις δεδομένων (Εικόνα 153, Εικόνα 154). Πιθανώς εξαιτίας των αλλαγών που έχουν γίνει στα android 10 με την χρήση του scoped storage και των νέων permissions ή εξαιτίας της μη επαρκούς υποστήριξης των file systems της συσκευής. Αξίζει να αναφέρουμε ότι στο χρονικό διάστημα που έχει πραγματοποιηθεί η έρευνα της διπλωματικής στο documentation του προγράμματος δεν αναφέρεται κάτι για το συγκεκριμένο πρόβλημα.

Στον φάκελο των αποτελεσμάτων βλέπουμε ότι το Andriller έχει φτιάξει ένα report επιπρόσθετα από τον φάκελο data στον οποίο έχουν αποθηκευτεί οι βάσεις και τα αρχεία που κατάφερε να κάνει recover το πρόγραμμα (Εικόνα 155).



Εικόνα 155 - Andriller Results 1

Ανοίγοντας το REPORT αρχείο βλέπουμε ότι το Andriller μας παρέχει κάποιες γενικές αναγνωριστικές πληροφορίες για την συσκευή (Εικόνα 156).

This report was generated using Andriller CE # (This field is editable in Preferences)

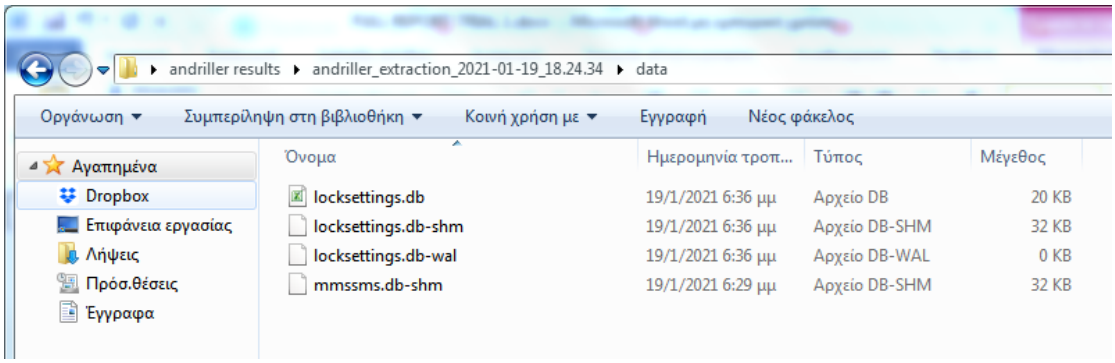
[Andriller Report]

Type	Data
Serial	R58M[redacted]
Status	device
Permisson	root-su
Ro.Build.Version.Release	10
Ro.Build.Display.Id	QP1A.190711.0[redacted]
Wifi Mac	8e:22:0[redacted]
Local_Time	2021-01-19 18:24:34 ◆◆◆◆◆◆◆◆◆◆ ◆◆◆ GTB
Device_Time	2021-01-19 18:24:33 EET
Currentsimserialnumber	8930050[redacted]
Currentsimoperatorname	vodafone GR
Previoussimserialnumber	null
Previoussimphonenumber	null
Accounts	• com.google: ptyxiakidummy@gmail.com • com.microsoft.office: Office • com.osp.app.signin: ptyxiakidummy@gmail.com

 # andriller.com # (This field is editable in Preferences)

Εικόνα 156 - Andriller Report

Πέρα όμως από τις πληροφορίες που παρέχονται στο REPORT αρχείο και το andriller δεν κατάφερε να κάνει recover τις βάσεις δεδομένων με τις πληροφορίες που μας ενδιαφέρουν (Εικόνα 157).



Εικόνα 157 - Andriller Recovered Files

7. ΣΥΜΠΕΡΑΣΜΑΤΑ-ΕΠΙΛΟΓΟΣ

Τα android 10 έχουν εισαγάγει νέα security features. Αναλυτικότερα έχει υιοθετηθεί νέος τρόπος διαχείρισης των permissions που παίρνουν οι εφαρμογές πάνω στην συσκευή και το scoped storage που δίνει νέο τρόπο αποθήκευσης δεδομένων στην συσκευή. Οι συγκεκριμένες αλλαγές έχουν ως σκοπό την προστασία της ιδιωτικότητας των χρηστών.

Μεγάλο ενδιαφέρον παρουσιάζει το γεγονός ότι τα open source εργαλεία για mobile forensics που είναι διαθέσιμα δεν έχουν καταφέρει ακόμα να προσαρμοστούν στις συγκεκριμένες αλλαγές και στον τρόπο αποθήκευσης και διαχείρισης των δεδομένων στην συσκευή που χρησιμοποιεί android 10. Επιπρόσθετα παρουσιάζουν ανεπαρκή στήριξη σε ό,τι αφορά τα file systems.

Μέσα από την έρευνα παρατηρήσαμε πως σε ό,τι αφορά το logical επίπεδο το AFLogical δεν είναι αποδοτικό καθώς δεν είναι προσαρμοσμένο στα android 10 και πρέπει να πραγματοποιήσουμε επιπρόσθετο export πληροφοριών κατευθείαν από την συσκευή.

Το free trial του FonePaw είναι αποδοτικότερο συγκριτικά με το AFLogical σε σχέση με τις πληροφορίες που μπορεί να κάνει recover από την συσκευή όμως δεν μας δίνει την δυνατότητα να κάνουμε export κάποιες από αυτές τις πληροφορίες στο workstation μας.

Επομένως οι λύσεις που εξετάσαμε για ανάλυση σε logical επίπεδο μας παρέχουν ικανοποιητικά αποτελέσματα. Για να έχουμε την μέγιστη απόδοση σε logical επίπεδο χωρίς να πρέπει να κάνουμε manual export από την συσκευή που ερευνάται και να μπορούμε να κάνουμε export πληροφορίες ενδιαφέροντος στο workstation μας θα πρέπει να στραφούμε σε κάποια επί πληρωμή λύση.

Η ανάλυση σε physical επίπεδο του image του κινητού δεν ήταν επιτυχής καθώς το autopsy δεν μπορεί να φτάσει στα δεδομένα που είναι αποθηκευμένα στις βάσεις εφόσον δεν είναι προσαρμοσμένο στις αλλαγές που έχουν συμβεί στα android 10 και δεν παρέχει ικανοποιητική υποστήριξη των file systems της συσκευής. Το andriller παρουσιάζει και αυτό το ίδιο πρόβλημα.

Συνεπώς κάποιος για να επιτύχει forensics ανάλυση σε physical επίπεδο, χρησιμοποιώντας ελεύθερα διαθέσιμες λύσεις στο κοινό, θα πρέπει να κάνει export των βάσεων δεδομένων κατευθείαν από την κινητή συσκευή σε micro sd card και στην συνέχεια να πάρει τις βάσεις στο workstation του. Η συγκεκριμένη διαδικασία δεν θεωρείται δόκιμη σε ό,τι αφορά τις σωστές πρακτικές forensics και δεν είναι αποδοτική καθώς το android χρησιμοποιεί πολλές βάσεις για να αποθηκεύσει δεδομένα.

Εναλλακτικά για μια επιτυχημένη ανάλυση σε physical επίπεδο κάποιος θα πρέπει να στραφεί σε επί πληρωμή λύση, μέχρι τα open source εργαλεία να προσαρμοστούν στις αλλαγές των android 10 και να παρέχουν επαρκή στήριξη των file systems που μπορεί κανείς να συναντήσει σε κινητές συσκευές.

Με τα android 11 να υπάρχουν ήδη από τις 19 Φεβρουαρίου 2020 στην αγορά είναι πολύ σημαντική η προσαρμογή των open source εργαλείων για mobile forensics στις αλλαγές που έχουν φέρει τα android 10 καθώς πρέπει να παρέχεται και στο ευρύ κοινό γνώση για το τι αποθηκεύεται πραγματικά στις κινητές συσκευές που χρησιμοποιεί.

ΧΡΗΣΙΜΑ LINKS

https://play.google.com/store/apps/details?id=com.joeykrim.rootcheck&hl=en

https://www.androidinfotech.com/root-samsung-galaxy-sm-a705-a70-android-10/

https://www.androidinfotech.com/download-odin-all-versions/

https://www.sammobile.com/samsung/galaxy-a70/firmware/SM-A705FN/EUR/download/A705FNXXU5BTJ4/536942/?__cf_chl_jschl_tk__=e06ec8c054be38463512e18b89437a22b7931f1e-1609857939-0-AcZKhGcLJognsRLRQfUu04LNf3g6h5llZJIx3bqfT8pNgkfDi_nKo3VrI8i_75muTOeCU1y68KXQpg7_CS8el29YxXhJo3CIRp3_qKP7RJ8GCqLQ-wCuqKbwK1hKAeCPKagD_Msm-8I9YM6dDgnAPfjnvSV7s48kHfaUIizWUpBgoPqa3ulJsf-hkE7ZD5fOicbZEe4q8voF4UU0Q9gxL5YADxfT07DOEV9Sje3jT-x2t1qVdKKalfqRsCHlJfN5bXsrwv9aRnoD6vdMLCbWviURml__JGSAphyJTNZyArkBByTnINmarMxMwI0TObjtChiy9_hMmcKQx9MjG3r-GxV1FdCZBQnb80MZ0fPJdOpzSuAHloIPZWVZjpZuBTC1MQ-Fd4eU4LdaG49ULvPmV6A

https://www.androidinfotech.com/samsung-galaxy-usb-driver-all-versions/

https://www.androidinfotech.com/magisk-versions-download/

https://magiskmanager.com/

https://www.samsungknox.com/en/about-knox

https://www.cellebrite.com/en/cas-supported-devices/

https://santoku-linux.com/

https://www.fonepaw.com/

https://play.google.com/store/apps/details?id=stericson.busybox&hl=en

https://www.unixmen.com/play-with-netcat-in-ubuntu/

https://www.youtube.com/watch?v=UQYuaOC5v0I&list=PL3dfduuyhbBcFrg7-TPKis1RExcYWrXd0&index=5&t=977s

https://www.sleuthkit.org/autopsy/

https://www.sleuthkit.org/autopsy/desc.php

https://www.sleuthkit.org/autopsy/features.php

https://github.com/den4uk/andriller

https://sleuthkit.discourse.group/t/android-image-cannot-define-file-system-type/1709

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Android Developers, 2020. *Android Developers.* [Ηλεκτρονικό]
Available at: https://developer.android.com/about/versions/10/privacy/changes
[Πρόσβαση January 2021].

Ansari, M., 2020. *Medium.* [Ηλεκτρονικό]
Available at: https://medium.com/codixlab/what-is-the-difference-between-android-9-and-android-10-500b6e5bb991
[Πρόσβαση January 2021].

Bommisetty, S., Tamma, R. & Mahalik, H., 2014. *Practical Mobile Forensics.* s.l.:s.n.

Brunty, J., 2016. *Mobile Forensics: An Introduction.* Virginia, s.n.

Casey, E., 2011. *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet.* 3η Έκδοση επιμ. s.l.:s.n.

Cellebrite, 2021. *Cellebrite.* [Ηλεκτρονικό]
Available at: https://www.cellebrite.com/en/cas-supported-devices/
[Πρόσβαση January 2021].

Davenport, C., 2020. *Android Police.* [Ηλεκτρονικό]
Available at: https://www.androidpolice.com/2020/05/12/10-android-10-features-to-look-for-when-your-phone-gets-updated/
[Πρόσβαση January 2021].

Dwivedi, H., 2020. *Heartbeat.* [Ηλεκτρονικό]
Available at: https://heartbeat.fritz.ai/implementing-scoped-storage-in-android-10-4b657280c066
[Πρόσβαση January 2021].

Gillware, n.d. *Gillware.* [Ηλεκτρονικό]
Available at: https://www.gillware.com/phone-data-recovery-services/samsung-forensics/
[Πρόσβαση January 2021].

Goyal, G., 2020. *Medium.* [Ηλεκτρονικό]
Available at: https://medium.com/microsoft-mobile-engineering/scoped-storage-in-android-10-android-11-28d58d989f3c
[Πρόσβαση January 2021].

Hazra, S. & Mateti, P., 2017. *ResearchGate.* [Ηλεκτρονικό]
Available at:
https://www.researchgate.net/publication/320952681_Challenges_in_Android_Forensics
[Πρόσβαση January 2021].

Hindy, J., 2019. *Android Authority.* [Ηλεκτρονικό]
Available at: https://www.androidauthority.com/android-10-permissions-1040121/
[Πρόσβαση January 2021].

Hoog, A., 2013. *APPSEC USA.* [Ηλεκτρονικό]
Available at: https://2013.appsecusa.org/2013/wp-content/uploads/2013/12/viaForensics-AppSecUSA-Nov-2013.pdf
[Πρόσβαση January 2021].

Kostadinov, D., 2019. *INFOSEC.* [Ηλεκτρονικό]
Available at:
https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref
[Πρόσβαση January 2021].

Lin, Y., 2020. *OBERLO.* [Ηλεκτρονικό]
Available at: https://www.oberlo.com/blog/mobile-usage-statistics
[Πρόσβαση January 2021].

Matei, A., 2019. *The Guardian.* [Ηλεκτρονικό]
Available at: https://www.theguardian.com/lifeandstyle/2019/aug/21/cellphone-screen-time-average-habits
[Πρόσβαση January 2021].

Nunez, S., 2020. *INSIGHTS - SAMSUNG.* [Ηλεκτρονικό]
Available at: https://insights.samsung.com/2020/08/07/your-phone-is-now-more-powerful-than-your-pc-2/
[Πρόσβαση January 2021].

Ranjan Roy, N., Kanchan Khanna, A. & Aneja, L., 2016. *ResearchGate.* [Ηλεκτρονικό]
Available at:
https://www.researchgate.net/publication/312559420_Android_phone_forensic_Tools_and_techniques
[Πρόσβαση January 2021].

Samsung, n.d. *Samsung Knox.* [Ηλεκτρονικό]
Available at: https://docs.samsungknox.com/admin/whitepaper/kpe/remote-control.htm
[Πρόσβαση January 2021].

Singh, A., 2020. *raywenderlich.* [Ηλεκτρονικό]
Available at: https://www.raywenderlich.com/9577211-scoped-storage-in-android-10-getting-started
[Πρόσβαση January 2021].

Skulkin, O., Tindall, D. & Tamma, R., 2018. *Learning Android Forensics.* s.l.:s.n.

Solution Analysts, 2020. *Solution Analysts.* [Ηλεκτρονικό]
Available at: https://www.solutionanalysts.com/blog/scoped-storage-in-android-10/
[Πρόσβαση January 2021].

Soufiane, T., 2016. *Mastering Mobile Forensics.* s.l.:s.n.

Spajic, D. J., 2020. *Kommando Tech.* [Ηλεκτρονικό]
Available at: https://kommandotech.com/statistics/how-much-time-does-the-average-person-spend-on-their-phone/
[Πρόσβαση January 2021].

statcounter, 2019 - 2020. *statcounter.* [Ηλεκτρονικό]
Available at: https://gs.statcounter.com/os-market-share/mobile/worldwide
[Πρόσβαση January 2021].

statcounter, 2019-2020. *statcounter.* [Ηλεκτρονικό]
Available at: https://gs.statcounter.com/vendor-market-share/mobile
[Πρόσβαση January 2021].

statista, 2020. *statista.* [Ηλεκτρονικό]
Available at: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/
[Πρόσβαση January 2021].

VisiHow, n.d. *VisiHow.* [Ηλεκτρονικό]
Available at: https://visihow.com/Use_the_Permission_Manager_in_Android_10
[Πρόσβαση January 2021].

Vivek, 2019. *DroidViews.* [Ηλεκτρονικό]
Available at: https://www.droidviews.com/debloater-magisk-module-uninstall-system-apps-android/
[Πρόσβαση January 2021].

Wallen, J., 2019. *TechRepublic.* [Ηλεκτρονικό]
Available at: https://www.techrepublic.com/article/how-to-use-the-new-app-permissions-in-android-10/
[Πρόσβαση January 2021].