Πανεπιστήμιο Πειραιώς

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Ασφάλεια Ψηφιακών Συστημάτων»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ψηφιακή Εγκληματολογία και Ανάλυση σε Κινητές Συσκευές** **Digital Forensics and Analysis in Mobile Devices**
Ονοματεπώνυμο Φοιτητή	**Αναστασίου Ιωάννης**
Πατρώνυμο	**Βασίλειος**
Αριθμός Μητρώου	**ΜΠΠΛ/ ΜΤΕ1705**
Επιβλέπων	**Αναπληρωτής Καθηγητής, Χρήστος Ξενάκης**

Ημερομηνία Παράδοσης **Ιούνιος 2019**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

Πίνακας Περιεχομένων

Περίληψη

Η ζήτηση στις Κινητές Συσκευές έχει αυξηθεί παγκοσμίως και η λειτουργικότητά τους ενδέχεται να ανταγωνιστεί ακόμη και επιτραπέζιους υπολογιστές παρά τα μικρότερα μεγέθη τους. Γι' αυτό τον λόγο ο εξαιρετικός σχεδιασμός των Κινητών Συσκευών καθιστά εύκολη την χρήση τους στην καθημερινή μας ζωή, εκτελώντας πολλές εργασίες εκτός από την απλή αποστολή και λήψη τηλεφωνικών κλήσεων. Τα κινητά τηλέφωνα είναι πλέον ικανά για την αποστολή γραπτών μηνυμάτων, περιήγηση στο διαδίκτυο, ηλεκτρονικό ταχυδρομείο, φωτογράφηση και άλλα επιχειρηματικά καθήκοντα, γεγονός που αυξάνει τη σημασία των δεδομένων που είναι αποθηκευμένα σε τέτοιες συσκευές. Αυτοί οι φορητοί φορείς μεταφοράς δεδομένων αποτελούν σημαντική πηγή στοιχείων τόσο σε αστικές όσο και σε ποινικές υποθέσεις, εξ' ου και η σημασία της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών.

Για την ανάκτηση δεδομένων από Κινητές Συσκευές κατά τη διάρκεια ψηφιακής έρευνας, απαιτούνται εξειδικευμένα εργαλεία. Διάφοροι τύποι εγκληματολογικών εργαλείων είναι διαθέσιμοι με πλεονεκτήματα και περιορισμούς. Λόγω της μεγάλης ποικιλίας τύπων Κινητών Συσκευών που χρησιμοποιούν αποκλειστικά πρότυπα κατασκευαστών, η Ψηφιακή Εγκληματολογία Κινητών Συσκευών έχει γίνει δυσοίωνη σε σύγκριση με την Ψηφιακή Εγκληματολογία Υπολογιστών.

Η επικείμενη διατριβή περιλαμβάνει μια αναλυτική επισκόπηση Ψηφιακής Εγκληματολογικής Έρευνας και Ανάλυσης σε Κινητές Συσκευές, των διαφόρων τύπων εργαλείων Ψηφιακής Εγκληματολογίας καθώς και διαφορετικών ιατροδικαστικών τεχνικών. Η διπλωματική αυτή εργασία περιλαμβάνει μια πρακτική μελέτη περί του τρόπου χρήσης ποικίλλων διαφορετικών ψηφιακών εργαλείων για την Ψηφιακή 'Ερευνα και Ανάλυση των Κινητών Συσκευών με βάση τις πρότυπες αρχές της Ψηφιακής Εγκληματολογίας.

Abstract

The demand on Mobile Devices has risen globally, and their functionality may even rival desktop computers despite of their smaller sizes. For this reason, this extraordinary design of Mobile Devices makes them easy to use in our daily life performing many tasks other than just sending and receiving phone calls. Mobile Devices are now capable of sending text messages, web browsing, e-mailing, photographing and other business tasks, which increases the importance of data stored on such devices. These portable data carriers represent a significant source of evidence in both civil and criminal cases, hence the importance of Mobile Forensics.

In order to retrieve data from Mobile Devices during a Forensic Investigation, specialized tools are required. Various types of Forensic toolkits are available with both advantages and limitations.
Due to the wide range of Mobile Device types which are using manufacturer proprietary standards, mobile forensic examination has become bleak compared to Computer Forensics.

The forthcoming dissertation includes an overview of Digital Criminal Investigation and Analysis in Mobile Devices, various types of Digital Criminology tools as well as different Forensic techniques. This includes a practical study on the use of a variety of different digital tools for Digital Research and Analysis of Mobile Devices based on the principles of Digital Forensics.

1. Εισαγωγή

Οι Κινητές Συσκευές τα τελευταία χρόνια έχουν γίνει αναπόσπαστο κομμάτι της ζωής των ανθρώπων καθώς μέσω αυτών υλοποιούν τις δραστηριότητες που έχουν μέσα στην καθημερινότητά τους. Αυτό το γεγονός έχει ως αποτέλεσμα,μια Κινητή Συσκευή να είναι πλέον ένα τεράστιο και σημαντικό αποθετήριο που περιέχει ευαίσθητες και χρήσιμες πληροφορίες για τον ιδιοκτήτη της. Όλες αυτές οι αλλαγές που συνέβησαν στο ρόλο της Κινητής Συσκευής στη ζωή του ανθρώπου οδήγησαν στην άνοδο της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών, ενός κλάδου Ψηφιακής Δικανικής που ασχολείται με την ανάκτηση δεδομένων από μια Κινητή Συσκευή. Στόχος της επικείμενης διπλωματικής εργασίας είναι η κατανόηση των τεχνικών ψηφιακής έρευνας στις κύριες πλατφόρμες, Android, iOS, Blackberry και Windows 10 Mobile. Αφού γίνει μια πρώτη θεωρητική ανάλυση των πιο κοινών πλατφόρμων για Κινητές Συσκευές στη συνέχεια θα ακολουθήσουν διάφορες μέθοδοι που μπορούν να συμπεριληφθούν στη συλλογή στοιχείων από διαφορετικές Κινητές Συσκευές.

1.1. Επιστήμη της Εγκληματολογίας

Η Επιστήμη της Εγκληματολογίας (Forensic Science) είναι η μελέτη και η εφαρμογή όλων των φυσικών και εφαρμοσμένων επιστημών με σκοπό την απόδοση της δικαιοσύνης. Πιο συγκεκριμένα η Επιστήμη της Εγκληματολογίας ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο, ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία.

Η ανάλυση του DNA και η εξέταση των δακτυλικών αποτυπωμάτων είναι μερικές από τις δυνατότητες της επιστήμης αυτής. Η Ψηφιακή Εγκληματολογία Υπολογιστών (Computer Forensic Science), «είναι η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό»[1]. Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε έναν υπολογιστή. Είναι αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις, αλλά και να τις συγκεντρώσουμε με τέτοιο τρόπο ώστε να είναι αποδεκτές στο δικαστήριο. Οι διωκτικές αρχές πρέπει να αποδείξουν, ότι τα στοιχεία που συλλέχθηκαν από τη σκηνή διάπραξης του εγκλήματος, διατηρήθηκαν αναλλοίωτα και τεκμηριώνουν την ενοχή του κατηγορουμένου. Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που κατέστρεψε αποδείξεις σχετικές με την αθωότητα του κατηγορουμένου.

1.2. Ψηφιακή Εγκληματολογία ή Δικανική

Η Επιστήμη της Ψηφιακής Εγκληματολογίας (Digital Forensic Science) γνωστή και ως Ψηφιακή Δικανική είναι ένας αναπτυσσόμενος κλάδος της Πληροφορικής, ο οποίος εντάσσεται στο γενικότερο πλαίσιο της Ασφάλειας Πληροφοριών και ειδικότερα σχετίζεται μέσω κοινών πρακτικών και εργαλείων με την απόκριση σε συμβάντα ασφάλειας. Ωστόσο, η ειδοποιός διαφορά εδώ είναι η πρόσθετη ανάγκη για χρήση των εντοπισμένων πειστηρίων προς νομική υπεράσπιση του οργανισμού ο οποίος υπέστη την εισβολή. Δηλαδή, η έμφαση δίνεται στην προσεκτική άντληση των στοιχείων χωρίς να αλλοιωθεί το πρωτογενές υλικό και στη λεπτομερή ανάλυσή τους, προκειμένου να τεκμηριωθούν τα συμπεράσματα με ακλόνητες αποδείξεις που δεν επιτρέπουν διφορούμενες ερμηνείες.

Ως Ψηφιακή Εγκληματολογία ορίζεται η χρήση επιστημονικά αποδεκτών μεθόδων που αποσκοπούν στην διατήρηση, την αναγνώριση, την καταγραφή, την ανάλυση, την ερμηνεία και τη παρουσίαση πειστηρίων προερχόμενων από ψηφιακά μέσα με στόχο την ανακατασκευή, την αναπαράσταση εγκληματικών ενεργειών ή την έγκαιρη πρόληψη και αντιμετώπιση μη εξουσιοδοτημένων ενεργειών οι οποίες αποτελούν κίνδυνο για σχεδιαζόμενες διαδικασίες.

Η Ψηφιακή Εγκληματολογία Υπολογιστών περιλαμβάνει την διατήρηση, ταυτοποίηση, εξαγωγή, τεκμηρίωση και διερμήνευση των υπολογιστικών μέσων για εύρεση αποδεικτικών στοιχείων και ανάλυση των αιτιών του συμβάντος. Ανέκυψε ως αποτέλεσμα του διαρκώς αυξανόμενου προβλήματος του Ηλεκτρονικού Εγκλήματος (Computer Crime). Το Ηλεκτρονικό Έγκλημα διακρίνεται σε δυο κατηγορίες:

- Ο Υπολογιστής είναι ένα εργαλείο που χρησιμοποιείται σε ένα έγκλημα. Η διερεύνηση αυτών των εγκλημάτων συχνά περιλαμβάνει την αναζήτηση των υπολογιστών που εμπλέκονται στο έγκλημα.

- Ο ίδιος ο υπολογιστής είναι το θύμα ενός εγκλήματος. Οι αναφορές που γίνονται απο τους αρμόδιους αστυνομικούς στην «Αντιμετώπιση Περιστατικών» (Incident Response) δείχνουν οτι τα συστημάτα δέχονται συνήθως απομακρυσμένη επίθεση. Οι ειδικοί ερευνητές που αναλαμβάνουν την υπόθεση της Ψηφιακής Εγκληματολογίας ακολουθούν ξεκάθαρες και κατάλληλα ορισμένες διαδικασίες.

Η Ψηφιακή Εγκληματολογία Υπολογιστών ξεκίνησε αρκετά χρόνια πριν, όταν ήταν απλό να συλλεχθούν αποδεικτικά στοιχεία από έναν υπολογιστή. Ενώ οι βασικές μεθοδολογίες της Δικανικής παραμένουν οι ίδιες, η τεχνολογία αλλάζει γρήγορα και αυτό είναι μια πρόκληση για τους ειδικούς. Η βασική μεθοδολογία της Ψηφιακής Έρευνας και Ανάλυσης αποτελείται από τα εξής στοιχεία: Απόκτηση των αποδεικτικών στοιχείων χωρίς την καταστροφή των αυθεντικών, πιστοποίηση ότι τα αποκτηθέντα στοιχεία είναι τα ίδια με τα αυθεντικά και ανάλυση των δεδομένων χωρίς αυτά να τροποποιηθούν καθ' όλη τη διαδικασία ανάλυσης εξασφαλίζοντας έτσι την ακεραιότητα τους κατά τη διάρκεια της δίκης[1].

«Ψηφιακό Πειστήριο» (Digital Evidence) νοείται οποιαδήποτε πληροφορία μπορεί να αποθηκευτεί ή να μεταδοθεί σε δυαδική μορφή και περιλαμβάνει αξιόπιστη πληροφορία που υποστηρίζει ή καταρρίπτει μια υπόθεση.

«Ψηφιακά Μέσα» (Digital Media) νοούνται οποιεσδήποτε συσκευές μπορούν να αποθηκεύσουν, να υφίστανται επεξεργασία και να στείλουν ή να λάβουν ψηφιακή πληροφορία. Τα Ψηφιακά Μέσα δεν αφορούν μόνο υπολογιστές αλλά και Κινητές Συσκευές, δίκτυα, βάσεις δεδομένων, cloud συστήματα, προσωπικά συστήματα PDAs και άλλες ηχητικές συσκευές ή συσκευές βίντεο.

1.3. Στόχος της Ψηφιακής Εγκληματολογίας

Στόχος της Ψηφιακής Εγκληματολογίας είναι η διαμόρφωση μιας υπόθεσης και η αποκάλυψη Ψηφιακών Πειστηρίων που την υποδεικνύουν ως έγκυρη ή λανθασμένη.

Η διαμόρφωση μιας υπόθεσης είναι απαραίτητη διότι τα ψηφιακά γεγονότα και καταστάσεις δεν μπορούν να εντοπιστούν άμεσα συνεπώς, τα γεγονότα δεν είναι γνωστά. Γι' αυτό το λόγο θα πρέπει να χρησιμοποιηθούν ειδικά εργαλεία προκειμένου να προσδιοριστεί η κατάσταση των ψηφιακών δεδομένων. Στα χαρακτηριστικά των ψηφιακών στοιχείων συμπεριλαμβάνεται και η ευθραυστότητα, η μεταβλητότητα και η μη απτή φύση τους που επιβάλλουν ειδική μεταχείριση. Συνεπώς χρειάζεται ιδιαίτερη προσοχή κατά την ανάλυση, συλλογή και εξαγωγή των Ψηφιακών Πειστηρίων ώστε να υπάρχει εμπιστοσύνη της ακεραιότητας τους και να αποφευχθεί κάποιο πιθανό σενάριο απόρριψης τους από κάποια δικαστική αρχή.

Μερικές από τις περιπτώσεις που λαμβάνει χώρα η Ψηφιακή Εγκληματολογία είναι περιπτώσεις παιδικής πορνογραφίας, κλοπής προσωπικών δεδομένων όπως κάποιο στοιχείο ταυτότητας, διαβατηρίου κλπ, πλαστογράφηση δεδομένων, περιπτώσεις παραβίασης ψηφιακής ασφάλειας ,εύρεση κακόβουλου λογισμικού ενσωματωμένο σε ψηφιακές συσκευές και άλλες.

Τέλος αυτός ο κλάδος εγκληματολογίας εφαρμόζεται και σε περιπτώσεις που δεν εμπλέκεται παραβίαση της νομοθεσίας όπως παραβιάσεις κάποιας πολιτικής ή κάποιας διαδικασίας σε μια επιχείρηση στην οποία ο υπεύθυνος της προκειμένου να εξακριβώσει τι συνέβη διεξάγει Ψηφιακή 'Ερευνα και Ανάλυση χωρίς αυτή να περιλαμβάνει κάποια παραβίαση του νόμου.

1.4. Ψηφιακή Εγκληματολογία Κινητών Συσκευών

Η Ψηφιακή Εγκληματολογία Κινητών Συσκευών έχει εξελιχθεί πρόσφατα και είναι πλέον ένας από τους σημαντικότερους τομείς έρευνας, για διάφορους λόγους. Οι δυνατότητες των κινητών τηλεφώνων έχουν ενισχυθεί σημαντικά. Αυτές οι συσκευές είναι αναμφίβολα πιο σημαντικές από τους επιτραπέζιους ή φορητούς υπολογιστές, επειδή συνήθως είναι πάντα ενεργοποιημένοι και συνήθως πάντα φορητοί[2]. Συνεπώς, καταγράφουν συνεχώς τις κινήσεις και τις δραστηριότητές μας και παρέχουν τεράστια εικόνα της συμπεριφοράς μας. Η επικοινωνία σχετικά με τη Κινητή Συσκευή είναι πολύ διαφορετική σε σύγκριση με έναν παραδοσιακό υπολογιστή. Αξίζει να σημειωθεί ότι οι εγκληματίες στέλνουν πολύ πιο συχνά δεδομένα από ένα κινητό τηλέφωνο παρά από έναν παραδοσιακό υπολογιστή.

Τα εγκλήματα δεν συμβαίνουν μεμονωμένα με βάση τις τεχνολογικές τάσεις. Ως εκ τούτου, η Ψηφιακή Εγκληματολογία Κινητών Συσκευών έχει καταστεί σημαντικό μέρος της Επιστήμης της Ψηφιακής Δικανικής.

Οι περισσότεροι άνθρωποι δεν συνειδητοποιούν πόσο πολύπλοκη είναι η διαδικασία της Ψηφιακής ‘Ερευνας και Ανάλυσης των Κινητών Συσκευών στην πραγματικότητα. Καθώς οι Κινητές Συσκευές συνεχίζουν να αυξάνονται όλο και περισσότερο σε προσωπικό αλλά και επαγγελματικό περιβάλλον, τα δεδομένα που εκπέμπονται από αυτά θα συνεχίσουν να αυξάνονται εκθετικά.

Η Ψηφιακή Εγκληματολογία Κινητών Συσκευών δεν λαμβάνεται πάντα σοβαρά υπόψη. Σύμφωνα με τον *Dr.Darren R. Hayes*, μέχρι πρότινος, ο βασικός λόγος χρήσης των λογισμικών Ψηφιακής Εγκληματολογίας Κινητών Συσκευών ήταν ότι μερικοί ύποπτοι σύζυγοι αγόραζαν τα λογισμικά αυτά με σκοπό να ανακαλύψουν αν ο-η σύντροφός τους-τις εξαπάτησε. Οι συσκευές απεικόνισης υλικού έχουν επίσης χρησιμοποιηθεί για αρκετά χρόνια, αλλά δεν χρησιμοποιήθηκαν αρχικά για έρευνες.

Επιπροσθέτως, οι αναλυτές Ψηφιακής Εγκληματολογίας Κινητών Συσκευών ήταν πάντα σημαντικοί, όμως λίγοι μπορούσαν να συνειδητοποιήσουν την πραγματική αξία του έργου τους. Αυτό συνέβαινε γιατί το διαθέσιμο λογισμικό εγκληματολογίας Κινητών Συσκευών δεν μπορούσε να λειτουργήσει στη συντριπτική πλειοψηφία των συσκευών αυτών. Μετά την προσθήκη των δυνατοτήτων του Διαδικτύου στα κινητά τηλέφωνα, η σημασία των λογισμικών Ψηφιακής Εγκληματολογίας Κινητών Συσκευών στις έρευνες αυξήθηκε. Με αυτή τη ζήτηση ήρθε και το καλύτερο κινητό ιατροδικαστικό λογισμικό. Σήμερα, σχεδόν κάθε εργαστήριο Ψηφιακής Εγκληματολογίας Υπολογιστών έχει τις δυνατότητες έρευνας και για Ψηφιακή Εγκληματολογία σε Κινητές Συσκευές. Επιπλέον, σήμερα υπάρχει διαχωρισμός των καθηκόντων. Για παράδειγμα, ένας ερευνητής μπορεί να είναι υπεύθυνος για μεγάλο μέρος των γραφειοκρατικών ενεργειών, συμπεριλαμβανομένων κλητεύσεων στους φορείς κινητής τηλεφωνίας. Ακόμα ένας άλλος ερευνητής μπορεί να είναι υπεύθυνος για τη συλλογή δεδομένων ανάλυσης από σταθμούς βάσης πομποδέκτη (BTS). Ένας σταθμός BTS περιλαμβάνει τον εξοπλισμό που βρίσκεται σε μια κυψέλη που διευκολύνει την επικοινωνία των χρηστών κινητής τηλεφωνίας σε ένα κυψελοειδές δίκτυο.

Οι ερευνητές της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών έχουν τεράστιες προκλήσεις εντούτοις. Ένας τεράστιος αριθμός Κινητών Συσκευών εξακολουθεί να μην μπορεί να απεικονιστεί. Το εγκληματολογικό υλικολογισμικό υποστηρίζεται μόνο από τις πιο δημοφιλείς συσκευές τη στιγμή που πάνω από εκατό νέα κινητά τηλέφωνα έρχονται στην αγορά κάθε χρόνο. Συνήθως τα πιο προβληματικά κινητά τηλέφωνα που εξετάζονται είναι και τα πιο φθηνά. Επίσης, υπάρχουν και ορισμένα κινητά τηλέφωνα από άλλες μικρότερες κυψελοειδείς εταιρείες. Το ζήτημα των κρυπτογραφημένων κινητών πλατφορμών και εφαρμογών για Κινητές Συσκευές που αναπτύσσονται από εταιρείες είναι επίσης σημαντικό.

Όσον αφορά το μέλλον, η εξάρτησή μας από την εγκληματολογία Κινητών Συσκευών τείνει μόνο να αυξάνεται και το πλήθος των Κινητών Συσκευών αλλά και των φορητών όπως είναι τα Tablet, τα GPS, κ.λπ. που υποστηρίζονται από προμηθευτές τείνει να επεκταθεί περισσότερο. Η λογική της αγοράς για συσκευές Android και iOS λέει πως ο ερευνητής πρέπει να κοιτάξει πέρα από τη συσκευή, περισσότερο στα συγχρονισμένα με την εξεταζόμενη συσκευή μέσα, όπως είναι ο υπολογιστής, οι συσκευές στο σπίτι και στην εργασία και στο «Ψηφιακό Νεφος» (cloud). Τα κινητά τηλέφωνα εξακολουθούν να έχουν αυξανόμενη εξάρτηση από το cloud, πράγμα που σημαίνει ότι οι ερευνητές θα βασίζονται όλο και περισσότερο σε αποδεικτικά στοιχεία που υπερβαίνουν το πεδίο του φορέα δικτύου στο μέλλον. Οι ενσωματωμένες εφαρμογές χρηστών που βρίσκονται στο κινητό τηλέφωνο, όπως το Facebook και το Gmail, είναι σημαντικές και θα αποκτήσουν μεγαλύτερη σημασία με τη πάροδο των χρόνων. Επιπλέον, πρέπει να σκεφτόμαστε συνεχώς έξω από αυτό που βλέπουμε, όπως κάνουν οι καλοί ερευνητές ασφάλειας.

Αυτή η διατριβή ονομάζεται Ψηφιακή Έρευνα και Ανάλυση σε Κινητές Συσκευές, αντί Ψηφιακής Εγκληματολογίας Κινητών Τηλεφώνων, διότι αναφέρεται και σε άλλες Κινητές Συσκευές που μπορούν να κατέχουν ενοχοποιητικές αποδείξεις, συμπεριλαμβανομένων των Tablet, των προσωπικών μέσων αναπαραγωγής και των συσκευών GPS. Στη συνέχεια ακολουθεί μια αναλυτική περιγραφή των βασικών χαρακτηριστικών που καθορίζουν μια Κινητή Συσκευή.

2. Χαρακτηριστικά Κινητής Συσκευής

Σε αυτό το κεφάλαιο θα γίνει μια πιο σαφής περιγραφή της διαδικασίας μελέτης του σχεδιασμού και του μοντέλου μιας συσκευής. Είναι σημαντικό σε μια έρευνα να υπάρχει πλήρης ενημέρωση για τις συσκευές που λαμβάνουν χώρα όπως επίσης και για τα περιφερειακά τους εξαρτήματα η συστήματα όπως για παράδειγμα ένας υπολογιστής που βρίσκεται κοντά στη συσκευή ο οποίος μπορεί να ναι συγχρονισμένος ή ένα καλώδιο φόρτισης μιας συσκευής η ακόμα και κάποιο άλλο σύστημα το οποίο θα μπορούσε να παραμένει συγχρονισμένο με τη συσκευή για τη διευκόλυνση του χρήστη (π.χ. Smart Watch). Παράλληλα θα ακολουθήσουν οι τεχνολογίες οι οποίες χρησιμοποιούνται στη κινητή τηλεφωνία και θα αναλυθούν πλήρως τα χαρακτηριστικά τους ώστε να διευκολύνουν τον αναγνώστη στη κατανόηση της υποδομής των κινητών επικοινωνιών. Η έρευνα και η ανάλυση των χαρακτηριστικών της συσκευής γίνονται στο στάδιο εικονικής ανάκτησης της συσκευής (βλ. Κεφάλαιο 3) αφού η συσκευή έχει κατασχεθεί και μεταφερθεί με ασφάλεια, προτού ξεκινήσει η ανάλυση της.

2.1. Μελέτη σχεδιασμού και μοντέλου της συσκευής

Αφού διαπιστώσουμε ότι έχουμε νόμιμη εξουσιοδότηση για να πραγματοποιήσουμε αναζήτηση και να εντοπίσουμε τη συσκευή για το σκοπό αυτό, πρέπει να προσδιορίσουμε με ακρίβεια τον τύπο της συσκευής που ανακτήσαμε, συμπεριλαμβανομένης του σχεδιασμού και του μοντέλου της.

Ο σχεδιασμός και το «μοντέλο της συσκευής» (make and model) μπορούν συχνά να καθορίσουν τις δυνατότητες της συσκευής, την τεχνική απομόνωσης που μπορεί να χρησιμοποιηθεί για να την προστατεύσει από το δίκτυο και τις άλλες πληροφορίες που είναι διαθέσιμες στη συσκευή περισσότερες Κινητές Συσκευές, όπως τα κινητά τηλέφωνα, συνήθως περιλαμβάνουν τον αριθμό του σχεδιασμού και του μοντέλου της συσκευής κάτω από την μπαταρία της συσκευής. Στις περισσότερες περιπτώσεις χρειάζεται αφαίρεση της μπαταρίας για να ληφθούν αυτές οι πληροφορίες. Αυτό μπορεί να απαιτεί απενεργοποίηση της συσκευής, κάτι που μπορεί να προκαλέσει κάποια προβλήματα όταν ενεργοποιηθεί η συσκευή ξανά. Για παράδειγμα, η Κινητή Συσκευή μπορεί να περιέχει έναν κωδικό PIN ή έναν κωδικό πρόσβασης που θα εμποδίζει μετέπειτα τον εξεταστή να έχει πρόσβαση στη συσκευή.

Τέλος, ο σχεδιασμός και το μοντέλο της συσκευής μπορούν να γνωστοποιήσουν εάν το τηλέφωνο λειτουργεί με βάση τη τεχνολογία CDMA ή τη τεχνολογία GSM και εάν η συσκευή μπορεί να περιέχει μια πρόσθετη κάρτα μέσων, για παράδειγμα μια κάρτα SD ή MicroSD. Περισσότερα για τις δύο αυτές τεχνολογίες θα αναλυθούν παρακάτω.

2.2. Τεχνολογίες Κινητών Επικοινωνιών

Υπάρχουν 2 διαφορετικές τεχνολογίες που χρησιμοποιούνται από τα δίκτυα κινητής τηλεφωνίας. Αυτά είναι το «Παγκόσμιο Σύστημα Κινητής Επικοινωνίας» ή αλλιώς GSM (Global System for Mobile Communication), και η «Πολλαπλή Πρόσβαση Διαίρεσης Κώδικα», ή CDMA (Code Division Multiple Access).

2.2.1. CDMA

Η Τεχνολογία CDMA, όπως αναφέρθηκε προηγουμένως, αντιπροσωπεύει την «Πολλαπλή Πρόσβαση Διαίρεσης Κώδικα». Αυτά τα δίκτυα συνδέονται χρησιμοποιώντας διαφορετικές μεθόδους για να επιτρέπουν σε πολλούς καλούντες να έχουν πρόσβαση σε ραδιοκύματα απλής φωνής και επομένως σε διαίρεση κώδικα και ώρας. Τα πραγματικά δίκτυα CDMA δεν κάνουν χρήση της κάρτας SIM σε Κινητές Συσκευές, καθώς το δίκτυο συνδέεται στη συσκευή και τα στοιχεία του συνδρομητή εμπεριέχονται μέσα στη συσκευή και όχι στην κάρτα SIM. Με την εμφάνιση του δικτύου 4G, τα κινητά τηλέφωνα CDMA περιλαμβάνουν συχνά και κάρτα SIM. Αυτό οφείλεται στο γεγονός ότι το 4G είναι πρότυπο της τεχνολογίας GSMA (Group Special Mobile Association) που απαιτεί κάρτα SIM για τη σύνδεση δεδομένων. Η τεχνολογία GSMA αντιπροσωπεύει τα συμφέροντα των περισσότερων φορέων κινητής τηλεφωνίας παγκοσμίως που φτάνουν να συνδέουν περίπου 800 φορείς με σχεδόν 300 εταιρείες.

Η «Ταυτότητα Εξοπλισμού μιας Κινητής Συσκευής» ή MEID (Mobile Equipment Identity) της τεχνολογίας CDMA, είναι το ισοδύναμο για το IMEI για τα κινητά τηλέφωνα τεχνολογίας GSM και

αναφέρεται συχνά ως ο σειριακός αριθμός της φορητής συσκευής. Το MEID αντικατέστησε τον «Ηλεκτρονικό Σειριακό Αριθμό» ή αλλιώς ESN (Electronic Serial Number) επειδή χρησιμοποιήθηκαν όλοι οι διαθέσιμοι αριθμοί ESN το 2005.

Ο αριθμός ID μιας Κινητής Συσκευής ή MIN (Mobile ID Number) συγκρίνονται συχνά με το IMSI που συσχετίζεται με τα κινητά τηλέφωνα GSM. Το MIN είναι ο αριθμός που προσδιορίζει τον συνδρομητή στον πάροχο δικτύου CDMA. Σε ορισμένες περιπτώσεις, ο αριθμός καταλόγου MDN (Mobile Directory Number) διαπιστώνεται ότι είναι ο ίδιος με τον MIN. Το MDN είναι ο αριθμός τηλεφώνου που αντιστοιχεί στη συγκεκριμένη συσκευή CDMA. Κατά την ανάγνωση αναφορών, οι ερευνητές μπορεί να βρουν τα MIN και MDN να διαφέρουν.

Αν κάποιος έχει απρόσκοπτη πρόσβαση στη συσκευή, το MEID για μια συσκευή CDMA μπορεί να εμφανιστεί πληκτρολογώντας * # 06 # ανάλογα με το σχεδιασμό και το μοντέλο της συσκευής. Μερικές φορές αυτή τη δυνατότητα λειτουργεί μόνο αν η ρύθμιση χρήσης δεδομένων LTE ενός φορητού τηλεφώνου έχει οριστεί σε "μόνο δεδομένα". Η τεχνολογία CDMA χρησιμοποιείται ως επί το πλείστον στις Ηνωμένες Πολιτείες της Αμερικής ενώ η τεχνολογία GSM χρησιμοποιείται ως επί το πλείστον στην Ευρώπη όπως εδώ στην Ελλάδα.

2.2.2. GSM

Η τεχνολογία GSM είναι το πιο κοινό σύστημα που χρησιμοποιείται παγκοσμίως. Είναι σπάνιο να βρεθεί συσκευή με τεχνολογία CDMA στην Ευρώπη. Τα δίκτυα GSM συνδέονται με την κάρτα SIM του χρήστη για έλεγχο ταυτοποίησης. Μια συσκευή τεχνολογίας GSM απαιτεί κάρτα SIM και δεν μπορεί να λειτουργήσει χωρίς αυτήν. Η αναγνώριση του συνδρομητή είναι εξίσου σημαντική με το υλικό και σε συσκευές που ακολουθούν το πρότυπο δικτύου GSM, τα δεδομένα συνδρομητών βρίσκονται στη SIM.

Η «Διεθνής Ταυτότητα Κινητού Συνδρομητή» ή IMSI (International Mobile Subscriber Identity) είναι ο σημαντικότερος αριθμός για έναν φορέα κινητής τηλεφωνίας. Χρησιμοποιείται για τον εντοπισμό του συνδρομητή. Μόλις φτάσει μια κλήση στο δίκτυο του συνδρομητή, ο αριθμός τηλεφώνου που είναι γνωστός και ως «Διεθνής Αριθμός Κλήσης Συνδρομητή» ή MSISDN (Mobile Station International Subscriber Dialing Number) είναι χαρτογραφημένος στο IMSI και από εκείνο το σημείο στο IMSI χρησιμοποιείται συνήθως και όχι το MSISDN. Αυτός είναι ο λόγος για τον οποίο μια κάρτα SIM θα καταγράψει το IMSI αλλά όχι το MSISDN του συνδρομητή.

Η ίδια η συσκευή αναγνωρίζεται από τη «Διεθνή Ταυτότητα Κινητού Εξοπλισμού» ή αλλιώς το IMEI. Το IMEI βρίσκεται συνήθως μέσα στη συσκευή και μεταδίδεται μέσω του δικτύου όταν χρησιμοποιείται το ακουστικό. Αν έχουμε ελεύθερη πρόσβαση στη συσκευή, το IMEI για μια συσκευή GSM μπορεί τυπικά να εμφανιστεί πληκτρολογώντας * # 06 #.

Τέλος, το «Αναγνωριστικό Περιοχής Τοποθεσίας» ή αλλιώς LAI (Location Area ID) μπορεί να είναι ανακτήσιμο κατά τη διάρκεια της εξαγωγής των δεδομένων της κάρτας SIM. Το LAI χρησιμοποιείται από το δίκτυο για να εντοπίσει τη συσκευή. Θα αποτελείται από έναν ή περισσότερους σταθμούς BTS και πιθανόν θα χρειαστεί επικοινωνία με τον πάροχο υπηρεσιών προκειμένου να ληφθούν παραπάνω λεπτομέρειες σχετικά με αυτό.

2.2.3. SIM

Οι δύο βασικές λειτουργίες μιας κάρτας SIM είναι να αναγνωρίζουν τον συνδρομητή σε ένα κυψελοειδές δίκτυο και να αποθηκεύουν δεδομένα. Συνήθως μια SIM είναι μια έξυπνη κάρτα που αποτελείται από έναν επεξεργαστή και μια μνήμη.

Οι κάρτες Sim ποικίλλουν στην μορφή τους. Μια μίνι-SIM είναι 25mm x 15mm και μία Micro-SIM είναι 15mm x 12 mm [20]. Αξίζει να σημειωθεί ότι υπάρχουν επίσης και ενσωματωμένες κάρτες SIM. Παρατηρώντας τη κάρτα SIM μπορεί κάποιος να αναγνωρίσει το σειριακό αριθμό ICCID της συσκευής. Το «Αναγνωριστικό Κάρτας Ολοκληρωμένου Κυκλώματος» ή αλλιώς ICCID (Integrated Circuit Card Identifier) είναι ο σειριακός αριθμός της κάρτας SIM. Αυτός ο αριθμός γενικά εκτυπώνεται πάνω στην κάρτα SIM, αλλά μερικές φορές διαφέρει από εκείνον που έχει προγραμματιστεί για το κύκλωμα. Το ICCID ξεκινά με τον αριθμό 89 με το οποίο αναγνωρίζεται η SIM ως κάρτα τηλεπικοινωνίας. Ακολουθεί ο αριθμός διεθνούς κλήσης για τη χώρα έκδοσης.

Συνεχίζοντας, με την ανάλυση του συστήματος αρχείων SIM, η «Ηλεκτρονικά Διαγράψιμη Προγραμματιζόμενη Μνήμη Μόνο για Ανάγνωση» ή EEPROM (Electronically Erasable Programmable Read Only Memory) βρίσκεται στο ιεραρχικό σύστημα αρχείων της συσκευής. Το λειτουργικό σύστημα, ο έλεγχος ταυτότητας χρήστη και οι αλγόριθμοι κρυπτογράφησης βρίσκονται στη Μνήμη που προορίζεται Μόνο για Ανάγνωση ή ROM (Read Only Memory) της κάρτας SIM.

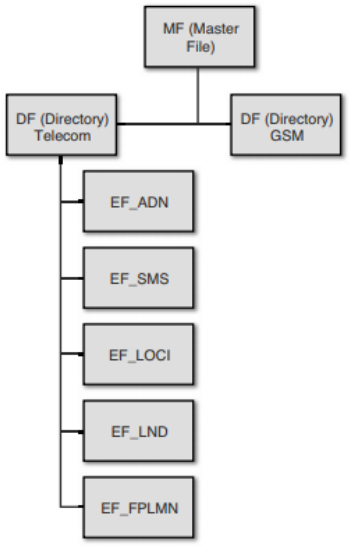
Υπάρχουν τρία βασικά στοιχεία του συστήματος αρχείων:

- Το «Κύριο Αρχείο» ή MF (Master File) που είναι η ρίζα του συστήματος αρχείων.
- Τα «Αποκλειστικά Αρχεία» ή DFs (Dedicated Files,) τα οποία είναι βασικά οι κατάλογοι του συστήματος αρχείων
- Τα «Στοιχειώδη Αρχεία» ή EFs (Elementary Files,) όπου κρατούνται τα δεδομένα του συστήματος αρχείων

Τα τελευταία είναι εκείνα στα οποία οι ερευνητές μπορούν να ανακτήσουν ένα τεράστιο ποσό πληροφοριών που έχουν ανταλλάξει οι συνδρομητές. Αυτές οι πληροφορίες μπορούν να περιέχουν δεδομένα, για παράδειγμα, τη θέση του υπόπτου, ακόμα και αν αυτός δεν κατάφερε να συνδεθεί με ένα δίκτυο. Πιο συγκεκριμένα στα Στοιχειώδη Αρχεία μπορεί κανείς να βρει

- «Συντομευμένους Αριθμούς Κλήσης» ή ADN (Abbreviated Dialing Numbers) που περιέχουν τα ονόματα επαφών και τους αριθμούς που εισήγαγε ο συνδρομητής. Αυτός ο φάκελος υπάρχει κάτω από το όνομα EF_ADN
- «Απαγορευμένα Δημόσια Δίκτυα Κινητής Τηλεφωνίας» ή FPLMN (Forbidden Public And Mobile Network) που αναφέρεται σε κυψελοειδή δίκτυα στα οποία ο συνδρομητής επιχείρησε να συνδεθεί, παρόλο που δεν είχε εξουσιοδοτηθεί να το πράξει. Αυτές οι πληροφορίες υπάρχουν κάτω από το όνομα EF_FPLMN
- «Τελευταίους Αριθμούς Κλήσεων» ή LND (Last Number Dialed) που εμφανίζει μια λίστα όλων των εξερχόμενων κλήσεων που πραγματοποίησε ο συνδρομητής. Αυτές οι πληροφορίες υπάρχουν κάτω από το όνομα EF_LND.

Επίσης ένας ερευνητής μπορεί να λάβει πληροφορίες από την περιοχή EF_LOCI, η οποία περιέχει πληροφορίες σχετικά με το πότε ο χρήστης τερμάτισε τελευταία το τηλέφωνο και την περιοχή EF_SMS που περιέχει τα μηνύματα SMS του συνδρομητή, διαγεγραμμένα και μη. Ένα σχέδιο που απεικονίζει τα πειστήρια που μπορούν να αποκαλυφθούν ερευνώντας το σύστημα αρχείων μιας Κινητής Συσκευής απεικονίζονται στο παρακάτω σχεδιάγραμμα.



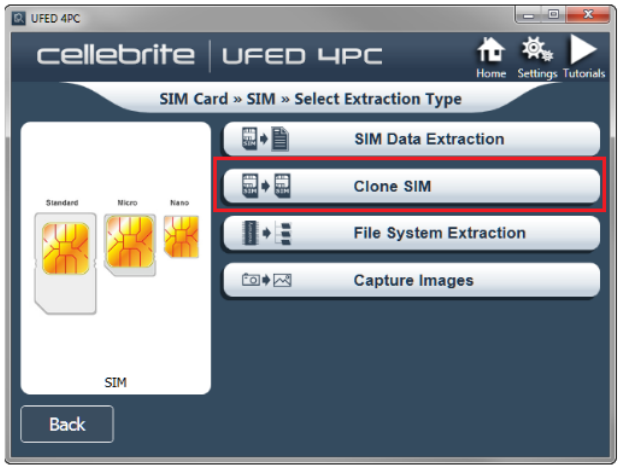
Εικόνα 1: Το σύστημα αρχείων σε μια κάρτα SIM

Συνεχίζοντας, η πρόσβαση στην κάρτα SIM μπορεί να αποτελέσει πρόκληση αν ληφθεί υπόψη ότι η κάρτα μπορεί να προστατευθεί με κάποιο κωδικό PIN. Ένας κωδικός PIN στην κάρτα SIM είναι συνήθως 4 ψηφία, αλλά πολλές φορές μπορεί να φτάνει και τα 8. Ένας ερευνητής έχει τρεις προσπάθειες να πληκτρολογήσει το σωστό PIN πριν κλειδώσει η κάρτα SIM, ενώ αν κλειδώσει στη συνέχεια η συσκευή ζητά ένα PUK (Key Unlock Key) ή PUC (Personal Unblocking Code). Ένας

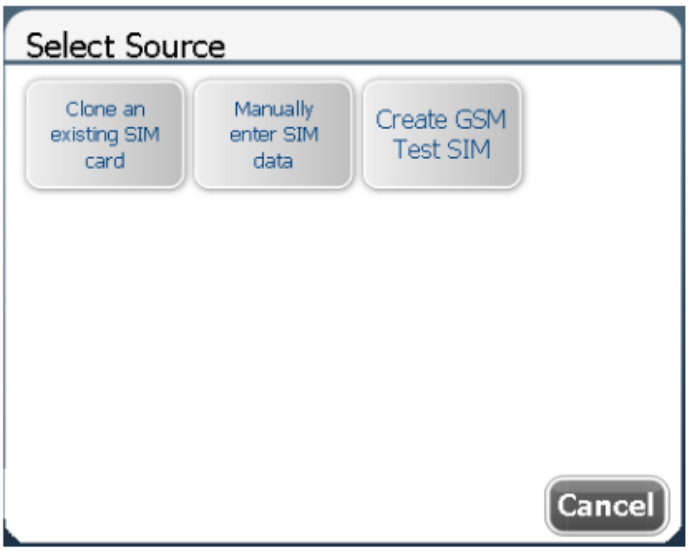
ερευνητής μπορεί να ζητήσει ένα PUC από τον μεταφορέα. Ένα PUC είναι ένας κωδικός που είναι διαθέσιμος από τον μεταφορέα και επιτρέπει σε έναν χρήστη να αφαιρέσει την προστασία PIN από την κάρτα SIM. Θα πρέπει επίσης να σημειωθεί ότι ένας χρήστης μπορεί να συνδεθεί στο διαδίκτυο και να αλλάξει το PUK. Για να το κάνει αυτό θα πρέπει να υπάρχει η άδεια και η συνεργασία του συνδρομητή.

Τέλος παρόμοια με την κλωνοποίηση του σκληρού δίσκου που χρησιμοποιείται στην Ψηφιακή Εγκληματολογία Υπολογιστών, ένας ερευνητής μπορεί συχνά να επιλέξει να κλωνοποιήσει μια κάρτα SIM αντί να εξετάσει την αρχική κάρτα SIM. Αυτή είναι μια καλή πρακτική Ψηφιακής Εγκληματολογίας και μπορεί να γίνει στα πρώτα βήματα του χειρισμού ψηφιακών αποδεικτικών στοιχείων, προκειμένου να αποφευχθεί το κλείδωμα της Κινητής Συσκευής και το πρόβλημα που περιγράφηκε προηγουμένως. Ένα από τα εργαλεία που μπορούν να εκτελέσουν κλωνοποίηση της SIM είναι και το UFED 4PC της Cellebrite. Παρακάτω απεικονίζονται οι κάρτες που χρησιμοποιούνται για την κλωνοποίηση της αυθεντικής SIM καθώς και η διαδικασία κλωνοποίησης στο UFED 4PC.

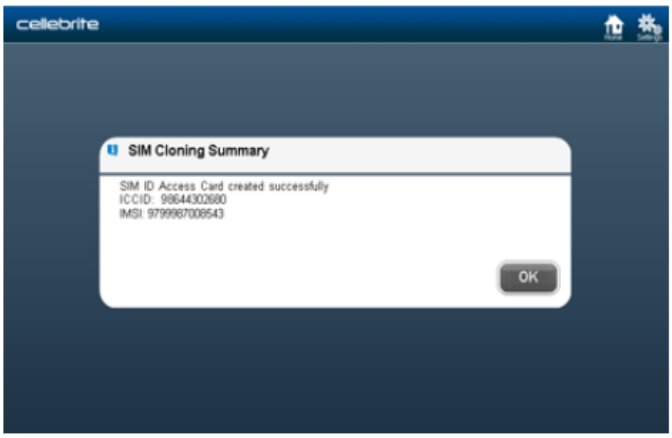
Εικόνα 2: Κάρτες κλωνοποίησης SIM της Cellebrite



Εικόνα 3: Επιλογή κλωνοποίησης με το πρόγραμμα UFED 4PC της Cellebrite



Εικόνα 4: Επιλογές κλωνοποίησης SIM



Εικόνα 5: Ολοκλήρωση κλωνοποίησης SIM

Σε αυτή την ενότητα μελετήθηκαν τα χαρακτηριστικά και η τεχνολογία των Κινητών Συσκευών στοιχεία τα οποία πρέπει να είναι γνωστά στους ερευνητές προκειμένου να γίνει σωστά η ανάκτηση της συσκευής σε μια εικονική μορφή δίσκου που θα αναλυθεί στη συνέχεια στο εργαστήριο. Στην επόμενη ενότητα θα ακολουθήσει μια αναλυτική περιγραφή της διαδικασίας Ψηφιακής 'Ερευνας και Ανάλυσης Κινητών Συσκευών με βάση τις πρότυπες αρχές Ψηφιακής Εγκληματολογίας. Είναι σημαντικό για έναν ερευνητή να κινείται βάση των αρχών ώστε να εξασφαλίζεται η ακεραιότητα των Ψηφιακών Πειστηρίων και η ασφάλεια τους από οποιοδήποτε κίνδυνο που μπορεί να προκύψει είτε στην σκηνή του εγκλήματος είτε κατά τη μεταφορά των πειστηρίων είτε κατά τη διάρκεια ανάλυσης τους στο εργαστήριο.

3. Ψηφιακή Εγκληματολογία Κινητών Συσκευών

Η Ψηφιακή Εγκληματολογία Κινητών Συσκευών (Mobile Forensics) είναι ένας κλάδος της Ψηφιακής Εγκληματολογίας που σχετίζεται με την ανάκτηση Ψηφιακών Δεδομένων από μια Κινητή Συσκευή που αποτελούν Ψηφιακά Πειστήρια. Ο όρος Κινητή Συσκευή δεν περιλαμβάνει μόνο κινητά τηλέφωνα, αλλά όλες εκείνες τις συσκευές που έχουν εσωτερική μνήμη και δυνατότητες επικοινωνίας, όπως τα PDAs και τα Tablets. Αν και η εμπλοκή των Κινητών Συσκευών σε εγκληματικές πράξεις ήταν ευρέως αναγνωρισμένη εδώ και χρόνια, η Ψηφιακή Έρευνα και Ανάλυση Κινητών Συσκευών μετρά μόνο λίγα χρόνια ζωής.

Οι Κινητές Συσκευές μπορούν να αποθηκεύουν πολλών ειδών προσωπικά στοιχεία, όπως επαφές, φωτογραφίες, ηλεκτρονικά μηνύματα e-mail, πληροφορίες περιήγησης στο Διαδίκτυο καθώς και πληροφορίες θέσης και μηνύματα κοινωνικής δικτύωσης.

Η ηλεκτρονική εγκληματολογική έρευνα πρέπει να πραγματοποιείται βάσει των κάτωθι αρχών:

- Καμία ενέργεια δε δύναται να μεταβάλει δεδομένα που τηρούνται σε υπολογιστή ή μέσο αποθήκευσης, τα οποία μπορεί να προσκομισθούν στο δικαστήριο.
- Θα πρέπει να γίνεται χρήση αρχέτυπων δεδομένων από τρίτο άτομο, μόνο ύστερα από εξουσιοδότηση.
- Δημιουργία ιστορικού ελέγχου των διαδικασιών.
- Το άτομο που έχει οριστεί ως υπεύθυνος της έρευνας, επιφορτίζεται με τη γενική ευθύνη για τη διασφάλιση τήρησης της επικείμενης νομοθεσίας και των εν λόγω αρχών.

Ο Οργανισμός «Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας» (NIST) παρέχει τυποποιημένες διαδικασίες λειτουργίας για ποικίλες επιστημονικές πρακτικές, συμπεριλαμβανομένης της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών. Η Ειδική Έκδοση NIST 800-101 Revision 1 [15] εξέδωσε κατευθυντήριες γραμμές σχετικά με την εγκληματολογία Κινητών Συσκευών το 2014. Ο NIST είναι ένας καλά αναγνωρισμένος οργανισμός και οι ερευνητές της επικείμενης Δικανικής πρέπει να είναι εξοικειωμένοι με τις κατευθυντήριες γραμμές του οργανισμού αυτού.

Σύμφωνα με τον NIST[15], τέσσερα βήματα εμπλέκονται σε μια Ψηφιακή Έρευνα.

- **Ανίχνευση και Κατάσχεσης συσκευής** (Identification and Seizure): Περιλαμβάνει τις διαδικασίες και τις μεθόδους καταγραφής της φυσικής σκηνής του εγκλήματος καθώς και της απόλυτα πιστής αντιγραφής των πρωτότυπων Ψηφιακών Αποδεικτικών Στοιχείων (Proof of Digital Evidence) χρησιμοποιώντας τυποποιημένες και αποδεκτές πρακτικές.
- **Ανάκτηση** (Acquisition): Περιλαμβάνει ενέργειες απομόνωσης, προστασίας και συντήρησης της κατάστασης των πρωτότυπων Ψηφιακών Αποδεικτικών Στοιχείων, όπως είναι για παράδειγμα η παρεμπόδιση των ανθρώπων από τη χρήση των ψηφιακών συσκευών και η απαγόρευση άλλων ηλεκτρομαγνητικών συσκευών να χρησιμοποιούνται πέρα από μια συγκεκριμένη ακτίνα.
- **Ανάλυση** (Analysis): Σε αυτή τη φάση προσδιορίζεται η σημαντικότητα των συλλεγμένων δεδομένων και βγαίνουν συμπεράσματα που βασίζονται στις αποδείξεις που βρέθηκαν.
- **Αναφορά και Παρουσίαση** (Reporting): Στο τέλος της έρευνας, τα στοιχεία καταγράφονται και παρουσιάζονται στους εντολείς. Ο ειδικός θα πρέπει να παρουσιάσει τα ευρήματα του σε μια καθαρή, περιεκτική, δομημένη και σαφή αναφορά στην οποία θα εξηγεί όλα τα συμπεράσματα στα οποία έχει καταλήξει.

Στη συνέχεια αυτού του κεφαλαίου ακολουθούν λεπτομερώς τα βήματα καθώς και οι ενέργειες που περιγράφηκαν πιο πάνω.

3.1. Ανίχνευση και Κατάσχεση συσκευής

Η διαδικασία της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών στοχεύει στην ανάκτηση ψηφιακών στοιχείων ή σχετικών δεδομένων από μια συσκευή κατά τρόπο που να διατηρεί τα αποδεικτικά στοιχεία σύμφωνα με τις αρχές Ψηφιακής Εγκληματολογίας. Για να επιτευχθεί αυτό, η διαδικασία έρευνας και ανάλυσης στις Κινητές Συσκευές πρέπει να καθορίσει συγκεκριμένους κανόνες που θα κατασχέσουν, θα απομονώσουν, θα μεταφέρουν, θα αποθηκεύσουν για ανάλυση και θα αποδείξουν τα ψηφιακά στοιχεία που προέρχονται από τις συσκευές αυτές.

Συνήθως, η διαδικασία της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών είναι παρόμοια με αυτή σε άλλους κλάδους της Ψηφιακής Δικανικής. Ωστόσο, πρέπει να γνωρίζουμε ότι η επικείμενη

διαδικασία έχει τις ιδιαιτερότητές της που πρέπει να εξεταστούν. Ακολουθώντας τη σωστή μεθοδολογία και λαμβάνοντας υπόψη σωστά τις κατευθυντήριες γραμμές είναι ζωτικής σημασίας προϋπόθεση για την εξέταση των Κινητών Συσκευών για να αποδώσουν καλά αποτελέσματα.

Σε μια υπόθεση Ψηφιακής Εγκληματολογίας Κινητών Συσκευών εκείνοι που είναι περισσότερο να αναλάβουν την εκτέλεση των ακόλουθων καθηκόντων είναι οι δικαστικοί εξεταστές, οι πρώτοι ανταποκριτές στο περιστατικό και οι εταιρικοί ανακριτές. Κατά την έρευνα για ένα συγκεκριμένο έγκλημα που αφορά την κινητή τεχνολογία, τα άτομα που είναι υπεύθυνα για την διαδικασία Ψηφιακής Έρευνας και Ανάλυσης πρέπει να ανακτήσουν κάθε πληροφορία που μπορεί να τους βοηθήσει αργότερα - για παράδειγμα, κωδικούς πρόσβασης της συσκευής, κλειδαριές προτύπων ή κωδικούς PIN.

Ασφάλιση και Εκτίμηση της τοποθεσίας εγκλήματος (Securing and Evaluating the Scene):
Πριν από την έναρξη της έρευνας, ο ερευνητής θα πρέπει να εξασφαλίσει ότι έχει άδεια από τον ιδιοκτήτη ή ότι υπάρχει η κατάλληλη εξουσιοδότηση. Σε αυτό το στάδιο, ο ερευνητής θα πρέπει να κατανοήσει το εύρος του εγκλήματος και να διασφαλίσει την ασφάλεια του καθενός στη σκηνή και να προστατεύσει την ακεραιότητα των αποδεικτικών στοιχείων. Άλλες παραδοσιακές μέθοδοι εγκληματολογικών ερευνών όπως DNA ή δακτυλικά αποτυπώματα ή οποιαδήποτε βιολογικά ίχνη (σάλιο, μαλλιά και δέρμα) θα μπορούσαν να είναι επωφελείς για τη σύνδεση μεταξύ της Κινητής Συσκευής και του ιδιοκτήτη, γι' αυτό και οποιαδήποτε αλληλεπίδραση με αυτά τα υλικά θα πρέπει να αποφεύγεται. Όλα τα άλλα περιφερειακά εξαρτήματα όπως κάρτες μνήμης, κάρτες SIM, φορτιστής ρεύματος, καλώδια ή προσωπικός υπολογιστής που θα μπορούσαν να χρησιμοποιηθούν σχετικά με τη συσκευή προς ανάλυση θα πρέπει να είναι ένας τόπος ενδιαφέροντος για τον ερευνητή κατά την αξιολόγηση της σκηνής του εγκλήματος.

Ο χρήστης ή ο ιδιοκτήτης του τηλεφώνου δεν πρέπει να επιτρέπεται να χειρίζεται την Κινητή Συσκευή ή οποιαδήποτε άλλη περιφερειακή συσκευή, καθώς μπορεί να αλλάξει το περιεχόμενο του τηλεφώνου ή να εκκαθαρίσει τα δεδομένα χρησιμοποιώντας τον κύριο κωδικό που είναι διαθέσιμος για τα περισσότερα από τα τηλέφωνα. Κατά τη διάρκεια της συνέντευξης με τον χρήστη του τηλεφώνου, ο ερευνητής θα πρέπει να ζητήσει κωδικούς ασφαλείας ή κωδικούς πρόσβασης που απαιτούνται για να αποκτήσουν πρόσβαση στα περιεχόμενα του τηλεφώνου.

Μερικές φορές τα τηλέφωνα μπορεί να βρεθούν σε μια πιθανή επικίνδυνη κατάσταση, για παράδειγμα το κινητό τηλέφωνο ως συστατικό μιας εκρηκτικής συσκευής, το κινητό τηλέφωνο που βρίσκεται σε ένα δοχείο λουλουδιών που καλύπτεται με διαβρωτικό υγρό ή το κινητό τηλέφωνο ενεργοποιημένο σε ένα μέρος όπου υπάρχει πραγματικός κίνδυνος πυρκαγιάς ή κίνδυνος ανάφλεξης. Στην περίπτωση αυτή η ασφάλεια των ανθρώπων έρχεται πρώτη και θα πρέπει να ληφθεί η συμβουλή κάποιου ειδικού.

Τα κινητά τηλέφωνα και οι περιφερειακές συσκευές μπορούν να βρεθούν σε κατάσταση βλάβης και, η ζημιά αυτή μπορεί να αποτρέψει την εξαγωγή επιπρόσθετων δεδομένων. Η μνήμη θα πρέπει να αφαιρεθεί μαζί με όλο τον κατεστραμμένο εξοπλισμό και να μεταφερθεί στο εργαστήριο για να επισκευαστεί και να αποκατασταθεί στην αποδεκτή κατάσταση για την ανάλυση.

Απενεργοποίηση της Κινητής Συσκευής: Θα πρέπει να γίνεται μόνο αν δεν υπάρχει κάποιος κωδικός ασφαλείας για πρόσβαση στα περιεχόμενα που μπορεί να περιπλέξει τη διαδικασία.

Απομόνωση ραδιοσήματος χρησιμοποιώντας ειδικά «κιβώτια» (containers) ή σακούλες: Σε πολλές περιπτώσεις, το τηλέφωνο μπορεί να παραμείνει ενεργό και να συνεχίσει να προσπαθεί να συνδεθεί στο δίκτυο το οποίο μπορεί να ρίξει το επίπεδο μπαταρίας του τηλεφώνου. Ωστόσο, ορισμένα τηλέφωνα μπορούν να επαναφέρουν τα δεδομένα δικτύου, τα οποία μπορεί να είναι χρήσιμα ως Ψηφιακά Πειστήρια, μετά από κάποια περίοδο αποτυχίας σύνδεσης.

Λειτουργία Πτήσης: Ενεργοποίηση της λειτουργίας πτήσης ή απενεργοποίηση όλων των συνδέσεων δικτύου. Αυτή η μέθοδος απαιτεί φυσική αλληλεπίδραση με το τηλέφωνο που μπορεί να προκαλέσει κάποιο κίνδυνο.

Φυσική αποσύνδεση: Όλα τα καλώδια που συνδέουν το τηλέφωνο με τον υπολογιστή για συγχρονισμό πρέπει να αποσυνδεθούν για να αποφευχθούν τυχόν αλλαγές στα περιεχόμενα του τηλεφώνου.

Μπαταρία: Τα επίπεδα των μπαταριών πρέπει να διατηρούνται σε κατάλληλο επίπεδο φόρτισης μέχρι το τέλος της εξέτασης. Μερικές φορές τα δεδομένα χρήστη αποθηκεύονται στην μνήμη, οπότε αν αποφορτιστεί η μπαταρία, τα δεδομένα θα χαθούν.

Κινητές συσκευές με βελτιωμένη ασφάλεια: Ορισμένα τηλέφωνα είναι διαθέσιμα με βελτιωμένους μηχανισμούς ελέγχου ταυτότητας ή ασφαλείας, όπως βιομετρικό έλεγχο ταυτότητας με βάση τα ανθρώπινα χαρακτηριστικά ανίχνευση ίριδος κ.λπ.

Κακόβουλα προγράμματα: Οι ιοί, τα λυτρισμικά και άλλα κακόβουλα λογισμικά ενδέχεται να φορτωθούν στο τηλέφωνο και να εξαπλωθούν μέσω ενσύρματου ή ασύρματου δικτύου. Επίσης, αυτά τα προγράμματα θα μπορούσαν να ενεργοποιηθούν υπό όρους με βάση συγκεκριμένη ενέργεια ή διακοπή κλειδιού για την εκτέλεση κακόβουλων ενεργειών, όπως η εκκαθάριση ή η απενεργοποίηση της συσκευής.

Επαναχαρτογράφηση Κλειδιών (Key Remapping): Ορισμένα πλήκτρα μπορεί να προγραμματιστούν για να εκτελέσουν διαφορετικές ενέργειες από τις προεπιλεγμένες, γεγονός που μπορεί να προκαλέσει κίνδυνο κατά την εξέταση τηλεφώνου.

Τοποθέτηση, μεταφορά και αποθήκευση των πειστηρίων : Όταν το τηλέφωνο είναι έτοιμο για εξέταση, θα πρέπει να τοποθετείται σε ασφαλή σακούλα στατικής απόδειξης, υπογεγραμμένη και χρονολογημένη από τον ερευνητή. Εάν το τηλέφωνο είναι ενεργοποιημένο, ο φορητός φορτιστής πρέπει να είναι συνδεδεμένος στο τηλέφωνο μέσα στην τσάντα, ώστε να διατηρείται το επίπεδο ισχύος κατά τη διάρκεια της μεταφοράς. Κατά τη μεταφορά, η συσκευή θα πρέπει να μεταχειρίζεται απο τους ερευνητές προσεκτικά σε προστατευμένο περιβάλλον.

Τεκμηρίωση της τοποθεσίας του εγκλήματος (Documenting the scene) :
Οι ερευνητές θα πρέπει να καταγράφουν πλήρως τη σκηνή του εγκλήματος, με ακρίβεια τόσο στη καταγραφή ψηφιακών όσο και των συμβατικών αποδεικτικών στοιχείων. Αυτό σημαίνει ότι ακόμη και οι μη ηλεκτρονικές ενδείξεις όπως υλικό συσκευασίας, εγχειρίδια και τιμολόγια μπορεί να είναι χρήσιμες κατά τη διάρκεια της εγκληματολογικής έρευνας. Μπορεί να περιλαμβάνονται κάποιες πληροφορίες σχετικά με τη συσκευή, τον χρήστη, το δίκτυο που χρησιμοποιείται και τους κωδικούς PIN / PUK. Όλα τα αποδεικτικά στοιχεία θα πρέπει να εντοπίζονται προσεκτικά με την επισήμανση, τη σύντομη περιγραφή, την ημερομηνία και ώρα συλλογής και την υπογραφή του ερευνητή / εξεταστή[24].

Όλες οι ψηφιακές συσκευές πρέπει να φωτογραφίζονται μαζί με άλλα περιφερειακά όπως κάρτες πολυμέσων, καλώδια, συνδέσεις ρεύματος και το περιβάλλον όπου βρίσκονται. Εάν το τηλέφωνο είναι ενεργοποιημένο και η οθόνη είναι σε κατάσταση προβολής, θα πρέπει να φωτογραφηθεί η ώρα, τα εικονίδια, η κατάσταση οθόνης LED, το επίπεδο μπαταρίας, η σύνδεση δικτύου και η φυσική κατάσταση[24].Δεν πρέπει να γίνει, καταγραφή ή να προσδιοριστεί τι υπάρχει στο τηλέφωνο σε αυτό το στάδιο. Οποιαδήποτε προσπάθεια προβολής ή εγγραφής μπορεί να επηρεάσει το περιεχόμενο της Κινητής Συσκευής.

Συλλογή Πειστηρίων: Αφού πραγματοποιηθεί ταυτοποίηση των συσκευών, του σχεδιασμού και του μοντέλου κ.λπ., τα επόμενα βήματα είναι να η ανάλυση της κατάστασης της συσκευής, που περιλαμβάνει αν η συσκευή είναι ενεργοποιημένη, απενεργοποιημένη ή σε κατάσταση αναστολής λειτουργίας. Η κατάσταση της συσκευής μπορεί να επηρεάσει τις ενέργειες που έγιναν από τους πρώτους ανταποκριτές σε μια σκηνή του εγκλήματος. Αυτός είναι ο λόγος για τον οποίο η κατάσταση της συσκευής πρέπει να ληφθεί υπόψη με σεβασμό πριν πραγματοποιηθεί οποιαδήποτε περαιτέρω ενέργεια.

Κατάσταση Απενεργοποιημένης συσκευής
Η διαδικασία συλλογής δεδομένων, εάν η συσκευή είναι απενεργοποιημένη, πρέπει να είναι η εξής:

- ✓ Ασφάλεια της συσκευής και αποτροπή από την καταστροφή του DNA: Ο πρώτος ανταποκριτής θα πρέπει να φοράει τον κατάλληλο προστατευτικό εξοπλισμό για να αποτρέψει τυχόν μόλυνση των πρωτότυπων στοιχείων DNA.
- ✓ Καταγραφή των στοιχείων της συσκευής: Προσδιορισμός και τεκμηρίωση του σχεδιασμού και του μοντέλου της συσκευής, του ESN και του φορέα που μπορεί να τοποθετηθεί κάτω από την μπαταρία.
- ✓ Καταγραφή της φυσικής κατάστασης της συσκευής: Σημείωση τυχόν ζημιάς στη συσκευή ή άλλων στοιχείων αναγνώρισης. Ο ερευνητής θα πρέπει να έχει κάνει λήψη φωτογραφιών της συσκευής για να δείξει τυχόν ειδικές συνθήκες που πρέπει να επισημανθούν ή σημάδια.
- ✓ Τεχνικές λεπτομέρειες της συσκευής: Χρήση πόρων Διαδικτύου για αναζήτηση λεπτομερειών για την επικείμενη συσκευή. Ένας καλός πόρος για τις τεχνικές λεπτομέρειες της συσκευής είναι η σελίδα του οργανισμού phonescoop[23].

- ✓ Αφαίρεση κάρτας μνήμης: Όταν και όπου είναι δυνατό και ανεξάρτητα από τις γνώσεις του ερευνητή σχετικά με την Κινητή Συσκευή, θα πρέπει να αφαιρούνται οι κάρτες SIM και η κάρτα μνήμης, εάν υπάρχουν, και μετά από αυτή τη διαδικασία, να αντιγράφονται τα δεδομένα σύμφωνα με τις πρότυπες διαδικασίες Ψηφιακής 'Ερευνας και Ανάλυσης.
- ✓ Θωράκιση από το Δίκτυο: Παρόλο που η συσκευή είναι απενεργοποιημένη, θα πρέπει να προστατεύεται ως μέτρο προφύλαξης από τυχόν αλλοίωση η μόλυνση της συσκευής για την διασφάλιση της ακεραιότητας των πειστηρίων. Σε αυτό το βήμα θα πρέπει να χρησιμοποιούνται είτε κάρτας απομόνωσης ραδιοφώνου, είτε ειδικές «Τσάντες Faraday» (Faraday Bags), «Κουτιά Faraday» κλπ. τα οποία επιτρέπονται κατά τη διάρκεια της δικαιοδοσίας.
- ✓ Πακετάρισμα της ετικέτας και της συσκευής: Θα πρέπει να συμπληρώνονται όλα τα απαραίτητα έγγραφα όπως η δημιουργία μιας «Αλυσίδας Επιμέλειας», η έκθεση συμβάντων και οι ετικέτες των πειστηρίων.
- ✓ Μεταφορά συσκευής: Σε αυτό το βήμα θα πρέπει να προστατεύεται η συσκευή, συμπληρώνοντας εντελώς τις απαιτούμενες φόρμες που έχουν να κάνουν με τη μεταφορά της συσκευής και των πειστηρίων πίσω στο εργαστήριο. Η συσκευή δεν πρέπει να εκτίθεται σε υπερβολική θερμότητα, υγρασία ή άλλους περιβαλλοντικούς παράγοντες που μπορεί να επηρεάσουν την ακεραιότητα της**.**

Κατάσταση Ενεργοποιημένης συσκευής

Η διαδικασία συλλογής δεδομένων, αν η συσκευή είναι ενεργοποιημένη, πρέπει να είναι η εξής:

- ✓ Ασφάλεια της συσκευής και αποτροπή από την καταστροφή του DNA: Όπως και στη κατάσταση Απενεργοποιημένης συσκευής, ο πρώτος ανταποκριτής θα πρέπει να φοράει τον κατάλληλο προστατευτικό εξοπλισμό για να αποτρέψει τυχόν μόλυνση των πρωτότυπων στοιχείων DNA.
- ✓ Καταγραφή των στοιχείων της συσκευής: Προσδιορισμός και τεκμηρίωση του σχεδιασμού και του μοντέλου της συσκευής, του ESN και του φορέα που μπορεί να τοποθετηθεί κάτω από την μπαταρία.
- ✓ Καταγραφή της φυσικής κατάστασης της συσκευής: Σημείωση τυχόν ζημιάς στη συσκευή ή άλλων στοιχείων αναγνώρισης. Ο ερευνητής θα πρέπει να έχει κάνει λήψη φωτογραφιών της συσκευής για να δείξει τυχόν ειδικές συνθήκες που πρέπει να επισημανθούν ή σημάδια.
- ✓ Θωράκιση από το δίκτυο: Είναι κρίσιμο να προστατεύεται η συσκευή από δίκτυα όταν είναι ενεργή. Σε αυτή τη περίπτωση θα πρέπει να χρησιμοποιείται μια κλωνοποιημένη κάρτα ταυτοποίησης SIM, τσάντες Faraday, κουτιά, η συσκευή να μπαίνει σε κατάσταση λειτουργίας πτήσης, και να μπλοκάρεται το σήμα, εάν αυτό είναι αποδεχτό από την αρμόδια αρχή της χώρας.
- ✓ Φόρτιση της συσκευής, αν και όπου χρειαστεί: Θα πρέπει να η συσκευή να εξακολουθεί να διαθέτει επαρκή ισχύ, καθώς μπορεί να προστατεύεται με κωδικό πρόσβασης. Εάν υπάρχει εξωτερική παροχή ρεύματος, θα πρέπει να χρησιμοποιηθεί για τη σωστή φόρτιση του τηλεφώνου.
- ✓ Τεχνικές λεπτομέρειες ακουστικών έρευνας: Χρήση πόρων Διαδικτύου για αναζήτηση λεπτομερειών για την επικείμενη συσκευή. Ένας καλός πόρος για τις τεχνικές λεπτομέρειες του ακουστικού είναι η σελίδα της εταιρείας phonescoop[23].
- ✓ Προσδιορισμός τερματισμού της συσκευής: Αυτή η απάντηση εξαρτάται από την κατάσταση της συσκευής και από το αν η συσκευή διαθέτει κωδικό πρόσβασης ή PIN ενεργοποιημένο. Θα εξαρτηθεί επίσης από το αν τα εργαλεία Ψηφιακής Εγκληματολογίας που διαθέτει ο ερευνητής υποστηρίζουν τη φυσική απεικόνιση για να παρακάμψουν τους κωδικούς πρόσβασης και τους κωδικούς PIN. Περισσότερες λεπτομέρειες σχετικά με τα PIN και τους κωδικούς πρόσβασης θα ακολουθήσουν στο επόμενο κεφάλαιο.
- ✓ Καταγραφή σχετικών πληροφοριών: Καταγραφή της σωστής ημερομηνίας και ώρας, τον επιτραπέζιο υπολογιστή που είναι συγχρονισμένος με τη συσκευή καθώς και τις εφαρμογές, τις ρυθμίσεις και τα ανοιχτά αρχεία.
- ✓ Πακετάρισμα της ετικέτας και της συσκευής: Θα πρέπει να συμπληρώνονται όλα τα απαραίτητα έγγραφα όπως η δημιουργία μιας «Αλυσίδας Επιμέλειας», η έκθεση συμβάντων και οι ετικέτες των πειστηρίων.
- ✓ Μεταφορά συσκευής: Σε αυτό το βήμα θα πρέπει να προστατεύεται η συσκευή, συμπληρώνοντας εντελώς τις απαιτούμενες φόρμες που έχουν να κάνουν με τη μεταφορά της συσκευής και των πειστηρίων πίσω στο εργαστήριο. Η συσκευή δεν πρέπει να εκτίθεται σε υπερβολική θερμότητα, υγρασία ή άλλους περιβαλλοντικούς παράγοντες που μπορεί να επηρεάσουν την ακεραιότητα της**.** Επειδή η συσκευή δεν πρέπει να χάσει την τροφοδοσία και

να απενεργοποιηθεί, συστήνεται για τη διατήρηση της ισχύος η τοποθέτηση της συσκευής σε μια τσάντα Faraday με μια εξωτερική πηγή μπαταρίας. Ακόμα, αν το τηλέφωνο βρίσκεται σε λειτουργία, η απομόνωση του από το ραδιοδίκτυο είναι κάτι πολύ σημαντικό για να αποφευχθεί η αντικατάσταση δεδομένων, για παράδειγμα νέα SMS ή νέες κλήσεις που μπορεί να αντικαταστήσουν τα παλιά αρχεία. Ορισμένα διαθέσιμα προγράμματα, όπως το LockMe, ενεργοποιούν απομακρυσμένο κλείδωμα του τηλεφώνου ενώ άλλα μηνύματα με δυσλειτουργία ενδέχεται να αποστέλλονται στο τηλέφωνο για να το απενεργοποιήσουν πλήρως [24].

3.2. Ανάκτηση Συσκευής

Οι ερευνητές που έχουν αναλάβει να βρίσκονται στο χώρο του εγκλήματος θα πρέπει να τεκμηριώνουν τα πάντα. πριν κάνουν οποιαδήποτε κίνηση που μπορεί να προβεί σε επεξεργασία των πειστηρίων, μαζί με τις φωτογραφίες που ελήφθησαν και οι ερευνητές τεκμηρίωσης βίντεο θα πρέπει να αφιερώσουν χρόνο για να λάβουν λεπτομερείς σημειώσεις για τις ενέργειές τους, συμπεριλαμβανομένων ακριβών ημερομηνιών και χρόνων.

Ανάλογα με την κατάσταση ισχύος της συσκευής, οι ερευνητές θα πρέπει να γνωρίζουν τις ενέργειας που πρέπει να κάνουν σε κάθε κατάσταση. Η κατάσταση κλειδώματος αναγνώρισης συσκευής και η θωράκιση δικτύου είναι όλα παράγοντες που πρέπει να ληφθούν υπόψη πριν από την ασφάλιση και τη μεταφορά της συσκευής. Πρέπει να σημειωθεί ότι ορισμένες δικαιοδοσίες απαιτούν από το προσωπικό επιβολής του νόμου να έχει νομική εξουσία πριν τη χειραγώγηση της συσκευής για πράγματα τόσο απλά όσο μια απογραφή ή ακόμη και μια τοποθέτηση του τηλεφώνου σε λειτουργία πτήσης. Εάν η λειτουργία πτήσης δεν είναι εφικτή ή ο εξεταστής δεν είναι άνετος χειριστής του τηλεφώνου, θα πρέπει να χρησιμοποιήσει μέσα «θωράκισης» (shielding) για να απομονώσει το τηλέφωνο από το δίκτυο. Ο συνιστώμενος τρόπος μεταφοράς των ψηφιακών συσκευών είναι συνήθως στο πάτωμα στην περιοχή των πίσω καθισμάτων του οχήματος, αποφεύγοντας την έκθεση σε μαγνητικά πεδία και άλλα ηλεκτρονικά, όπως είναι για παράδειγμα οι σειρήνες των οχημάτων της αστυνομίας κλπ.

Επιπλέον, οι ερευνητές θα πρέπει να εξασφαλίσουν ότι θα ολοκληρώσουν την κατάλληλη γραφική κατάσχεση, συμπεριλαμβανομένων των εντύπων κατάσχεσης και της «Αλυσίδας Επιμέλειας». Η Ανάκτηση (Acquisition) είναι η διαδικασία απεικόνισης ή απόκτησης πληροφοριών από την ψηφιακή συσκευή και τον περιφερειακό εξοπλισμό της. Μόλις φτάσει το τηλέφωνο στο εργαστήριο, ξεκινάει η διαδικασία ανάκτησης η οποία αποτελείται από τις ακόλουθες διαδικασίες:

- **Αναγνώριση τηλεφώνου:** Το τηλέφωνο πρέπει να αναγνωρίζεται από το σχεδιασμό, το μοντέλο και τον παροχέα υπηρεσιών δικτύου. Με βάση αυτές τις πληροφορίες, ο εξεταστής μπορεί να επιλέξει το κατάλληλο εργαλείο για την ανάκτηση της συσκευής. Ο εξεταστής μπορεί να χρησιμοποιήσει πληροφορίες που λαμβάνονται από την κοιλότητα της μπαταρίας ή την κάρτα SIM για να αναγνωρίσει το τηλέφωνο, όπως είναι το IMEI και το SIM ICCID.

- **Αναγνώριση σύνδεσης:** Ένα τηλέφωνο μπορεί να συνδεθεί με τον ιατροδικαστικό σταθμό είτε μέσω καλωδίου, είτε υπερύθρων είτε μέσω Bluetooth. Η επιλογή του τύπου σύνδεσης εξαρτάται από τη συσκευή, το χρησιμοποιούμενο εργαλείο και τις συνθήκες απόκτησης.

- **Επιλογή εργαλείου:** Οι δυνατότητες του επιλεγμένου εργαλείου διαδραματίζουν σημαντικό ρόλο στο στάδιο της ανάκτησης. Η επιλογή των εργαλείων εξαρτάται κυρίως από τη συσκευή που αποκτάται. Τα ακόλουθα σημεία θα πρέπει να εξεταστούν από τον εξεταστή πριν επιλέξει ένα εγκληματολογικό εργαλείο:

  - ✓ **Ευχρηστία**: Εξετάζει εάν το εργαλείο είναι σε θέση να παρουσιάσει χρήσιμα στοιχεία στον ερευνητή.

  - ✓ **Ολοκληρωμένο**: Το εργαλείο πρέπει να παρουσιάζει όλα τα δεδομένα στον εξεταστή, ώστε να μπορεί να εντοπίσει τα Ψηφιακά Πειστήρια.

  - ✓ **Ακρίβεια**: Το εργαλείο πρέπει να είναι ακριβές και να παρουσιάζει υψηλή ποιότητα παραγωγής.

  - ✓ **Συνθήκες Ντετερμινισμού**: Το εργαλείο πρέπει να παρουσιάζει την ίδια έξοδο όταν δίνεται η ίδια εισαγωγή και οδηγίες.

- ✓ **Επαληθεύσιμο**: Το εργαλείο πρέπει να διασφαλίζει την ακρίβεια της εξόδου.

Συνήθως τα τηλέφωνα υποβάλλονται στο εργαστήριο με αίτημα ανάκτησης συγκεκριμένων στοιχείων, στην περίπτωση αυτή δεν απαιτείται η ανάκτηση των πλήρων δεδομένων. Η ανάκτηση των πλήρων δεδομένων μπορεί να βοηθήσει μόνο στην αποφυγή ξανά της διαδικασίας επαναπλήρωσης εάν υπάρχουν άλλα απαιτούμενα δεδομένα. Η λογική ανάκτηση του κινητού τηλεφώνου, χρησιμοποιώντας τα διαθέσιμα εργαλεία ιατροδικαστικής, απαιτεί την ενεργοποίηση του τηλεφώνου. Η ενεργοποίηση του τηλεφώνου πρέπει να γίνεται σε ραδιοφωνική περιοχή ή όλες οι ασύρματες επικοινωνίες του τηλεφώνου πρέπει να απενεργοποιούνται. Αξίζει να σημειωθεί ότι Τα σημερινά κινητά τηλέφωνα εκτός από ασύρματες δυνατότητες επικοινωνίας έχουν και δυνατότητες κυψελοειδούς επικοινωνίας, ενσωματωμένες δυνατότητες υπέρυθρων (IrDa), Wi-Fi ή Bluetooth. Ορισμένα εργαστήρια Ψηφιακής Εγκληματολογίας χρησιμοποιούν εργαλεία παρεμπόδισης σήματος στα εργαστήρια τους για να εμποδίσουν όλες τις ραδιοφωνικές μεταδόσεις και τις παρεμβολές με άλλες Κινητές Συσκευές. Ένας παρεμποδιστής σήματος μπορεί να χρησιμοποιηθεί εάν μια άδεια αποκτηθεί επίσημα από τη δικαιοδοσία ή το δίκαιο της συγκεκριμένης χώρας. Μπορεί επίσης να υπάρξει επικοινωνία με τον φορέα κινητής τηλεφωνίας για τη διασφάλιση αφαίρεσης της συσκευής από το δίκτυο. Οι εγκληματίες συχνά αναφέρουν ότι ένα κινητό τηλέφωνο χάθηκε για να διαγράψουν τα δεδομένα τους, συνεπώς ένας εξεταστής πρέπει να κινηθεί γρήγορα προκειμένου να αφαιρέσει τη συσκευή από το δίκτυο.

3.3. Ανάλυση Συσκευής

Το στάδιο Ανάλυσης (Analysis) είναι ένα τεχνικό στάδιο που πραγματοποιείται από εξειδικευμένους ερευνητές. Ο αρμόδιος ερευνητής πρέπει να μελετήσει την υπόθεση και να είναι εξοικειωμένος με όλες τις παραμέτρους του εγκλήματος, τους εγκληματίες και τα στοιχεία που μπορεί να βρεθούν. Επίσης συνιστάται ιδιαίτερα στον εξεταστή να διεξάγει την εξέταση του σε συνεννόηση με τον αναλυτή ή τον ερευνητή, έτσι ώστε να μπορεί να του δώσει καλή κατανόηση των διαπιστωμένων αποδεικτικών στοιχείων και μπορεί να τους παράσχει τα μέσα πληροφόρησης που βρέθηκαν.

Η εξέταση μπορεί να αποκαλύψει άμεσα πιθανά αποδεικτικά στοιχεία ή να αποκαλύψει χρήσιμες πληροφορίες, όπως κωδικούς πρόσβασης, σύνδεση στο δίκτυο και σύνδεση στο διαδίκτυο, η οποία μπορεί να οδηγήσει σε άλλες πηγές αποδεικτικών στοιχείων.

Οι έρευνες κατά την Ψηφιακή Εγκληματολογία Κινητών Συσκευών μπορούν να χωριστούν σε δύο τύπους [24].

- ✓ Όταν συνέβη το περιστατικό και η ταυτότητα του παραβάτη είναι άγνωστη (π.χ., συμβάντα hacking)
- ✓ Σε περίπτωση που συνέβη το περιστατικό και η ταυτότητα του παραβάτη είναι γνωστή (π.χ., συμβάντα παιδικής πορνογραφίας).

Χρειάζεται σωστός χειρισμός των αποδεικτικών στοιχείων από τους ερευνητές καθώς σε περίπτωση λάθος χειρισμού όλη η διαδικασία της διερεύνησης θα υπομονευτεί. Για το σωστό χειρισμό των αποδεικτικών στοιχείων θα πρέπει να τηρείται μια αλυσίδα αποδεικτικών στοιχείων που ονομάζεται «Αλυσίδα Επιμέλειας» (Chain of custody). Ο όρος «Αλυσίδα Επιμέλειας» είναι ένας νομικός όρος ο οποίος αναφέρεται στη χρονική παρακολούθηση ενός αποδεικτικού στοιχείου από τη στιγμή κατάσχεσής του και κατά τη διάρκεια ανάλυσής του μέχρι την επιστροφή η την καταστροφή του. Ο στόχος της διατήρησης μιας καλής “Αλυσίδας Επιμέλειας” είναι η εξασφάλιση της ακεραιότητας των αποδεικτικών στοιχείων και η αποτροπή της αλλοίωσης τους. Η αλυσίδα πρέπει να απαντά στα εξής ερωτήματα:

- ❖ Συγκέντρωση πληροφοριών σχετικά με το εμπλεκόμενο άτομο (ΠΟΥ).
- ❖ Προσδιορισμός της φύσης των αποδεικτικών στοιχείων (ΤΙ).
- ❖ Προσδιορισμός των χρονοδιαγράμματα συμβάντων (ΠΟΤΕ)
- ❖ Κατανόηση των πληροφοριών που εξηγούν το κίνητρο του εγκλήματος (ΓΙΑΤΙ)
- ❖ Εύρεση εργαλείων που χρησιμοποιήθηκαν για την πραγματοποίηση του εγκλήματος (ΠΩΣ)

Μία «Αλυσίδα Επιμέλειας» περιλαμβάνει τα εξής χαρακτηριστικά βήματα:

- ➢ **Συλλογή**: Το ζητούμενο σε αυτό το βήμα είναι τα αποδεικτικά στοιχεία να είναι αρκετά ξεκάθαρα ώστε να υποστηρίξουν την υπόθεση.
- ➢ **Ταυτοποίηση**: Τα αποδεικτικά στοιχεία θα πρέπει να ταυτοποιούνται μεθοδικά και να τοποθετείται ετικέτα σε κάθε στοιχείο που εξάγεται από την τοποθεσία του θύματος ή του υπόπτου.

- **Μεταφορά**: Τα αποδεικτικά στοιχεία δεν πρέπει να μετακινούνται και στην περίπτωση που κρίνεται απαραίτητη η μετακίνησή τους θα πρέπει να γίνεται με εξαιρετική προσοχή και από υπεύθυνα άτομα.
- **Αποθήκευση**: Τα αποθηκευτικά στοιχεία θα πρέπει να διατηρούνται σε δροσερό και ξηρό περιβάλλον το οποίο είναι κατάλληλο για εναποθέτηση ηλεκτρονικών μέσων.
- **Τεκμηρίωση της έρευνας**: Αποτελεί το πιο δύσκολο κομμάτι της διαδικασίας. Σε αυτό το βήμα γίνεται λεπτομερέστατη καταγραφή των διαδικασιών που ακολουθήθηκαν κατά την Ψηφιακή Έρευνα και Ανάλυση.
- **Πιστοποίηση της αυθεντικότητας των αποδεικτικών στοιχείων**: Κρίνεται δύσκολο βήμα για την όλη διαδικασία καθώς η τοποθεσία του εγκλήματος μεταβάλλεται με την πάροδο του χρόνου, τα αποδεικτικά στοιχεία συχνά καταστρέφονται από τις περιβαλλοντικές συνθήκες. Το βήμα αυτό περιλαμβάνει τη διατήρηση των αποδεικτικών στοιχείων και της ακεραιότητας των δεδομένων μέσω της κρυπτογράφησης των στοιχείων αυτών.
- **Ανάλυση**: Το βήμα αυτό περιλαμβάνει τη διατήρηση αντιγράφων ασφαλείας των δεδομένων ενώ παράλληλα χρησιμοποιούνται όλα τα γνωστά εργαλεία Ψηφιακής Εγκληματολογίας για να γίνει ανάλυση των αποδεικτικών στοιχείων.

3.4. Δημιουργία Αναφοράς

Η Δημιουργία Αναφοράς (Reporting) είναι το πιο σημαντικό βήμα σε μία έρευνα Ψηφιακής Εγκληματολογίας και τα αποτελέσματα της πρέπει να παρουσιαστούν σε ένα λεπτομερές έντυπο που περιλαμβάνει όλα τα βήματα που έχουν ληφθεί μαζί με το συνολικό συμπέρασμα της έρευνας. Σύμφωνα με τον Dr Darren μια σωστή αναφορά ενός ερευνητή πρέπει να συνοψίζει τα παρακάτω:

- ✓ Τον τόπο κατάσχεσης της συσκευής
- ✓ Πως η συγκεκριμένη συσκευή κατασχέθηκε (αντίγραφα συγκατάθεσης η ένταλμα)
- ✓ Διαδικασίες προετοιμασίας, συμπεριλαμβανομένου τεχνικών αποκοπής της συσκευής από το δίκτυο.
- ✓ Ψηφιακά Εργαλεία που χρησιμοποιήθηκαν για την απόκτηση των Ψηφιακών Πειστηρίων
- ✓ Ψηφιακά Πειστήρια που συλλέχθηκαν (SMS, MMS, εικόνες, video, επαφές, ιστορικό κλήσεων, κ.λπ.)
- ✓ Ψηφιακά Πειστήρια φορέα επικοινωνίας (λεπτομέρειες συνδρομητή και αρχείο καταγραφής κλήσεων)
- ✓ Ψηφιακά Πειστήρια υπηρεσιών εφαρμογών (π.χ. Gmail μηνύματα από τους εξυπηρετητές της Google)

Οι αναφορές μπορούν να δημιουργηθούν από τα εργαλεία της εργαστηριακής ιατροδικαστικής μονάδας εάν υπάρχει ενσωματωμένο εργαλείο αναφοράς, το οποίο επιτρέπει στον εξεταστή να επιλέξει τη μορφή εξόδου και τον τύπο δεδομένων που θα συμπεριληφθούν στην αναφορά. Η τελική έκθεση πρέπει να περιλαμβάνει εκείνη που παράγεται από τα εργαλεία, την ολοκληρωμένη διαδικασία, τις πράξεις των αιτήσεων που πραγματοποιήθηκαν κατά τη διάρκεια των ερευνών και όλα τα δικαιολογητικά, όπως φωτογραφίες, σημειώσεις και υπογραφή ειδικών που είναι υπεύθυνοι για το περιεχόμενο της έκθεσης.

4. Μέθοδοι Ανάκτησης δεδομένων απο μια Κινητή Συσκευή

Οι μέθοδοι που χρησιμοποιούνται για την εξαγωγή δεδομένων από Κινητές Συσκευές εξαρτώνται κυρίως από συνθήκες και χαρακτηριστικά όπως το μοντέλο της συσκευής, το χρόνο, τη φύση της υπόθεσης και τους διαθέσιμους πόρους.

Οι μέθοδοι που χρησιμοποιούνται για την εξαγωγή πληροφοριών από κινητά τηλέφωνα τύπου Smart Phones εστιάζουν στη σύνδεση της συσκευής με υπολογιστή χρησιμοποιώντας καλώδιο, Bluetooth ή υπέρυθρες. Τα δεδομένα αυτά εξάγονται από τη μνήμη της συσκευής χρησιμοποιώντας διαφορετικούς τρόπους απόκτησης. Βασιζόμενες στις παρακάτω μεθόδους, οι τεχνικές ανάλυσης χαρακτηρίζονται από διαφορετικά επίπεδα [20].

Λογική ανάκτηση: Με τον όρο λογική ανάκτηση των πειστηρίων εννοούμε τη λήψη των αρχείων των χρηστών, συνδέοντας το τηλέφωνο και τον υπολογιστή χρησιμοποιώντας καλώδιο δεδομένων ή Bluetooth και αποκτώντας πληροφορίες χρησιμοποιώντας διαθέσιμα εργαλεία Ψηφιακής Εγκληματολογίας. Είναι μια γρήγορη, εύκολη και αξιόπιστη μέθοδος καθώς τα εργαλεία που υπάρχουν υποστηρίζουν πολλές γλώσσες και λειτουργίες και διαθέτουν πολλές φόρμες αναφοράς.

Φυσική ανάκτηση: Η φυσική ανάκτηση γνωστή και ως ανάλυση Hex-dump, περιλαμβάνει τη στατική ανάκτηση του συστήματος αρχείων μιας Κινητής Συσκευής. Σε αυτόν τον τύπο ανάκτησης, η ανάλυση γίνεται είτε συνδέοντας την Κινητή Συσκευή χρησιμοποιώντας καλώδιο είτε αφαιρώντας τις κάρτες από τη συσκευή και εξάγοντας δεδομένα αντιγράφοντας το συνολικό σύστημα αρχείων. Τα δεδομένα που λαμβάνονται με αυτή τη μέθοδο είναι σε ακατέργαστη μορφή και πρέπει να μετατραπούν σε δυαδική μορφή κάτι που γίνεται από το εργαλείο λογισμικού Ψηφιακής Εγκληματολογίας που χρησιμοποιεί ο ερευνητής.

JTAG: Στηριζόμενη στο άρθρο IEEE 1149.1. η ομάδα εξαρτημάτων JTAG (Joint Test Action Group) είναι σχεδιασμένη για χρήση σε επεξεργαστές, μνήμη και πίνακες κυκλωμάτων. Η ομάδα εξαρτημάτων JTAG μπορεί να χρησιμοποιηθεί για την άμεση πρόσβαση στον επεξεργαστή ή το τσιπ μνήμης και όχι ανάλογα με το λειτουργικό σύστημα. Αλλά για να δουλέψει η JTAG πρέπει να υπάρχουν οι οδηγίες του επεξεργαστή και της μνήμης, οι οποίες συνήθως δεν είναι γνωστές στο κοινό, ενώ πρόβλημα αποτελεί και το ότι τα καλώδια JTAG είναι διαθέσιμα συνήθως μόνο για τους κατασκευαστές τηλεφώνων. Υπάρχουν όμως κάποια διαθέσιμα εργαλεία που χρησιμοποιούν JTAG. Τα εργαλεία αυτά ονομάζονται "Flushers".

CHIP-OFF: Η μέθοδος Chip-Off περιλαμβάνει την ανάλυση της μνήμης με την αφαίρεση ενός τσιπ από την Κινητή Συσκευή και την ανάλυση είτε χρησιμοποιώντας το ίδιο τηλέφωνο είτε έναν αναγνώστη μνήμης EEPROM. Αυτή η μέθοδος αποσπά όλα τα δεδομένα από τη μνήμη του κινητού τηλεφώνου, είναι αρκετά δαπανηρή ενώ πολλές φορές μπορεί να αποβεί καταστροφική για τα πειστήρια και γι' αυτό θα πρέπει να συνιστάται η προσοχή της.

MicroRead: Η μέθοδος MicroRead είναι μια μέθοδος που περιλαμβάνει τη διαδικασία χρήσης ενός ηλεκτρονικού μικροσκοπίου υψηλής ισχύος για την παροχή φυσικής απεικόνισης των πυλών εντός των ηλεκτρονικών τσιπ της Κινητής Συσκευής. Αυτή η μέθοδος μπορεί να εξαγάγει δεδομένα από φυσικά κατεστραμμένα τσιπ παρόλα αυτά είναι πολύ ακριβή. Χρησιμοποιείται κυρίως όταν η έρευνα έχει να κάνει με κάποια τρομοκρατική ενέργεια η εμπλοκή της πολιτείας ή του στρατού. Για την πλήρη ανάλυση μιας Κινητής Συσκευής πρέπει να εξάγονται κατάλληλα και τα διαγραμμένα δεδομένα, έτσι ώστε να γίνεται τόσο λογική όσο και φυσική απόκτηση.

Flusher Boxes: Τα Flusher Boxes είναι συσκευές υπηρεσίας που χρησιμοποιούνται από παρόχους υπηρεσιών ή καταστήματα Κινητής τηλεφωνίας για την ανάκτηση δεδομένων από ελαττωματικά τηλέφωνα. Τα Flushers μπορούν να χρησιμοποιηθούν για την ενημέρωση ή την αντικατάσταση του λειτουργικού συστήματος μιας Κινητής Συσκευής, την κατάργηση των ρυθμίσεων του παροχέα υπηρεσιών και το ξεκλείδωμα του φορέα παροχής υπηρεσιών. Μπορεί επίσης να χρησιμοποιηθεί παράνομα για να αλλάξει τον αριθμό IMEI μιας Κινητής Συσκευής.
Τα Εργαλεία αυτά επιτρέπουν στον χρήστη να έχει πρόσβαση στην εσωτερική μνήμη του τηλεφώνου χωρίς να εγκαθιστά οποιοδήποτε λογισμικό στη συσκευή, γεγονός που τα καθιστά ένα καλό εργαλείο

εγκληματολογίας. Παρόλα αυτά δεν υπάρχει εγγύηση ακεραιότητας των δεδομένων της συσκευής και εγγύηση ότι μπορούν να εξασφαλίσουν συνέπεια ή ακόμα και τη καλή διατήρηση τους. Επίσης, αυτές οι συσκευές δεν εγκρίνονται από τους κατασκευαστές Κινητών Συσκευών ούτε εγκρίνονται κατάλληλα για εγκληματολογική έρευνα σύμφωνα με τις πρότυπες αρχές Ψηφιακής Εγκληματολογίας. Έτσι, οι ερευνητές θα πρέπει να είναι πολύ προσεκτικοί σχετικά με τη χρήση αυτών των συσκευών κατά την Ψηφιακή Έρευνα και Ανάλυση των Κινητών Συσκευών. Τα Flushers μπορούν να χρησιμοποιηθούν για την εκτέλεση διαδικασιών ανάγνωσης και εγγραφής (read/write) στην εσωτερική μνήμη του τηλεφώνου και δεν παρέχουν μηχανισμό αποκλεισμού εγγραφής, ώστε να μπορούν να αλλάξουν τα περιεχόμενα του τηλεφώνου ή να αντικαταστήσουν τα αποδεικτικά στοιχεία.

Εικόνα 6: Flasherbox από την εταιρία Octupus

4.1. Τύποι Ψηφιακών Πειστηρίων

Το φάσμα των αποδεικτικών στοιχείων που διατίθενται από ένα κινητό τηλέφωνο είναι αρκετά διαφορετικό από αυτό που μπορεί να ανακτηθεί από ένα φορητό υπολογιστή ή μια επιφάνεια εργασίας. Μία από τις βασικές διαφορές είναι η ύπαρξη μηνυμάτων SMS και MMS, τα οποία θα περιγραφούν λεπτομερώς στην επόμενη ενότητα.

Μηνύματα SMS: Τα SMS είναι μια υπηρεσία επικοινωνίας μηνυμάτων κειμένου που βρίσκεται σε Κινητές Συσκευές. Αυτά τα μηνύματα κειμένου μπορούν να βρεθούν στη μνήμη σε ένα φορητό σύστημα ή σε μια κάρτα SIM της συσκευής. Τα μηνύματα SMS αποθηκεύονται ως επί το πλείστον στη συσκευή ή σε μια κάρτα SIM στο στη συσκευή. Επιπροσθέτως. όταν αποθηκεύονται στην κάρτα SIM μπορούν να βρεθούν στο αρχείο DF_Telecom.

Ένας ερευνητής μπορεί να καθορίσει εάν ένα μήνυμα SMS έχει διαβαστεί, διαγραφεί ή εστάλη με βάση τη τιμή της Σημαίας Κατάστασης (Flag Value). Η μεταβολή της τιμής του byte βασίζεται στην κατάσταση του μηνύματος.

Status Flag Value	Description
00000000	Deleted message
00000001	Read message
00000011	Unread message
00000101	Sent message
00000111	Unsent message

Εικόνα 7: Πίνακας Τιμών Κατάστασης ενός μηνύματος

Κατά την προβολή του μηνύματος κειμένου με ένα hex editor, ένα μη αναγνωσμένο μήνυμα SMS αρχίζει με 11, ένα διαγραμμένο μήνυμα αρχίζει με 00 και ούτω καθεξής.

Μηνύματα MMS: Η υπηρεσία μηνυμάτων πολυμέσων ή MMS είναι μια υπηρεσία ανταλλαγής μηνυμάτων που βρίσκεται στα περισσότερα κινητά τηλέφωνα και επιτρέπει στο χρήστη να στέλνει περιεχόμενο πολυμέσων όπως ηχητικό βίντεο και εικόνες. Χρησιμοποιώντας ένα εγκληματολογικό εργαλείο κινητού τηλεφώνου, ο ερευνητής μπορεί να αποσπάσει αυτό το περιεχόμενο πολυμέσων από

τα μηνύματα του χρήστη. Τα MMS μπορούν να ανακτηθούν απευθείας από μια SIM ή από την Κινητή Συσκευή.

4.1.1. Χαρακτηριστικά στοιχεία συσκευής

Η γνώση του υλικού της συσκευής βοηθά έναν ερευνητή να μάθει πώς να θωρακίσει με ασφάλεια τη συσκευή μετά την κατάσχεσή της.

Μνήμη και Επεξεργαστής: Οι περισσότερες Κινητές Συσκευές περιέχουν ένα μικροεπεξεργαστή, ένα τσιπ ROM και τη μνήμη τυχαίας προσπέλασης RAM. Το λειτουργικό σύστημα βρίσκεται στη ROM. Ασφαλείς ψηφιακές (SD) κάρτες, ιδιαίτερα MicroSD κάρτες, βρίσκονται συχνά σε Smart Phones. Συνολικά οι περισσότερες φορητές συσκευές μπορούν να περιέχουν τα ακόλουθα δεδομένα:

- Φωτογραφίες
- Βίντεο
- Εφαρμογές
- Χάρτες

Μπαταρία: Θα πρέπει να σημειωθεί ότι πολλά Smart Phones σήμερα επιλέγουν να μην χρησιμοποιούν αφαιρούμενη κάρτα SD, αλλά μια εσωτερική ενσωματωμένη κάρτα πολυμέσων (EMMc). Αυτή η μνήμη χρησιμοποιεί σύστημα FAT32. Χρησιμοποιούνται κυρίως τέσσερις τύποι μπαταριών κινητής τηλεφωνίας: Ιόντων Λιθίου (Li-Ion), Πολυμερών Λιθίου (Li-Poly), Νικελίου Καδμίου (NiCd) και Υδριδίου Μετάλλου Νικελίου (NiMH) [20]. Τα περισσότερα iPhone και BlackBerry τηλέφωνα χρησιμοποιούν μπαταρία τύπου Ιόντων Λιθίου, η οποία είναι ελαφριά σε σύγκριση με άλλες μπαταρίες.

Άλλο Υλικό: Οι Κινητές Συσκευές διαφέρουν από μοντέλο σε μοντέλο, αλλά γενικά έχουν ραδιοσυχνική μονάδα, ψηφιακό επεξεργαστή σήματος, «Οθόνη Υγρών Κρυστάλλων» (LCD), μικρόφωνο και ηχείο. Ορισμένα μοντέλα έχουν επίσης ενσωματωμένο πληκτρολόγιο.

Επιταχυνσιόμετρο: Ένα άλλο χαρακτηριστικό που βρίσκεται συχνά στις Κινητές Συσκευές σήμερα είναι ένα επιταχυνσιόμετρο. Ένα επιταχυνσιόμετρο είναι μια συσκευή υλικού που αισθάνεται κίνηση ή βαρύτητα και αντιδρά σε αυτές τις αλλαγές. Για παράδειγμα, ένα επιταχυνσιόμετρο διευκολύνει την αναστροφή της οθόνης όταν η συσκευή γυρίζει προς τα πλάγια ή ανάποδα. Επιπλέον, το επιταχυνσιόμετρο ενισχύει την εμπειρία ενός παίκτη επιτρέποντας του να γυρίσει και να κινήσει την αλλαγή της γωνίας της συσκευής. Το επιταχυνσιόμετρο έχει γίνει δημοφιλές από την ενσωμάτωση του στο iPad και στο iPhone.

Κάμερα :Οι περισσότερες Κινητές Συσκευές έρχονται σήμερα με μια ψηφιακή φωτογραφική μηχανή που έχει ακόμα φωτογραφίες και δυνατότητες βίντεο. Τα περισσότερα Smart Phones διαθέτουν χαρακτηριστικά που επιτρέπουν στο χρήστη να τραβήξει μια φωτογραφία και τη φορτώσει γρήγορα σε Κοινωνικά Μέσα όπως το Facebook. Όσον αφορά το βίντεο, πολλά smartphones επιτρέπουν στο χρήστη να φορτώνει περιεχόμενο απευθείας σε ιστοτόπους όπως το Facebook και το YouTube. Πολλά smartphones ενσωματώνουν επίσης το γεωγραφικό πλάτος και το γεωγραφικό μήκος του τόπου όπου λήφθηκε η φωτογραφία ενώ τα περισσότερα κινητά τηλέφωνα Android κάνουν αυτό από προεπιλογή.

4.2. Συνήθεις Τύποι συσκευών για Mobile Forensics

Η αναγνώριση του λειτουργικού συστήματος μιας Κινητής Συσκευής έχει πρωταρχική σημασία κατά την απόκτηση δεδομένων της. Το λειτουργικό σύστημα κινητής τηλεφωνίας επηρεάζει άμεσα τον τρόπο με τον οποίο ο ερευνητής μπορεί να έχει πρόσβαση στο κινητό τηλέφωνο. Για παράδειγμα, το λειτουργικό σύστημα Android παρέχει πρόσβαση σε επίπεδο «τερματικού» (terminal), ενώ το iOS δεν παρέχει αυτήν την επιλογή.

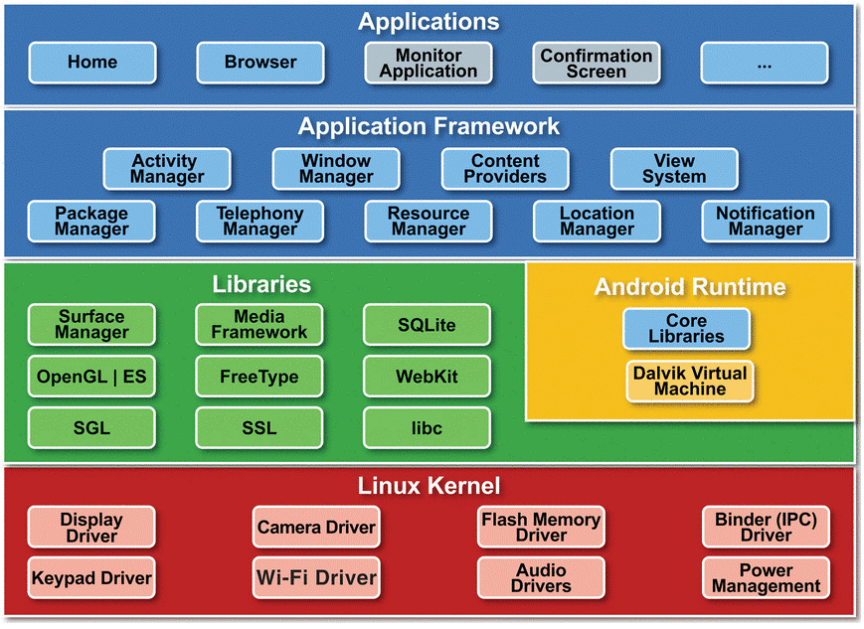
Σήμερα, υπάρχει μια ποικιλία Κινητών Συσκευών με διάφορα λειτουργικά συστήματα κινητής τηλεφωνίας κάτι όμως που καθιστά την Ψηφιακή Έρευνα και Ανάλυση Κινητών Συσκευών πολύπλοκη, επειδή ορισμένες τεχνικές ψηφιακής ανάλυσης μπορεί να είναι αποτελεσματικές για συγκεκριμένες εκδόσεις λειτουργικού συστήματος, αλλά μπορεί να είναι άχρηστες για τους διαδόχους τους. Για

παράδειγμα εάν για ένα εργαλείο Ψηφιακής Εγκληματολογίας υπάρχει μια τεχνική φυσικής ανάκτησης μιας συγκεκριμένης Κινητής Συσκευής iPhone αυτό δε σημαίνει ότι η ίδια τεχνική θα κάνει και σε νεότερα μοντέλα. Τα κυριότερα λειτουργικά συστήματα στη βιομηχανία κινητής τηλεφωνίας περιλαμβάνουν τα Google Android, Blackberry OS, Apple iOS και Windows 10 Mobile. Σε αυτή την ενότητα θα γίνει μια πιο αναλυτική περιγραφή των προαναφερθέντων λειτουργικών συστημάτων Κινητών Συσκευών ενώ παράλληλα θα αναφερθούν και άλλες φορητές συσκευές που χαρακτηρίζονται ως κινητές στο κόσμο της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών όπως είναι τα GPS, και τα Tablet.

4.2.1. Android

Το Android κυκλοφόρησε για πρώτη φορά το 2007 και σε λιγότερο από πέντε χρόνια πέτυχε να είναι το κυρίαρχο λειτουργικό σύστημα στην αγορά Κινητών Συσκευών. Το λειτουργικό σύστημα λειτουργεί με πυρήνα βασισμένο στο Linux 2.6, το οποίο χρησιμεύει για την υποστήριξη βασικών λειτουργιών, όπως προγράμματα οδήγησης συσκευών, δικτυακή υποδομή και διαχείριση ενέργειας. Το επόμενο επίπεδο της αρχιτεκτονικής του Android είναι ο τομέας των βιβλιοθηκών, που χωρίζεται σε εφαρμογές και στο runtime περιβάλλον του Android. Η πρώτη κατηγορία παρέχει την κατάλληλη υποδομή για σωστή λειτουργία των εφαρμογών, όπως τα δυαδικά αρχεία και η υποστήριξη γραφικών, ενώ η τελευταία αποτελείται από την εικονική μηχανή Dalvik, γνωστή και ως DVM, και τις βασικές βιβλιοθήκες που παρέχουν την διαθέσιμη λειτουργικότητα για τις εφαρμογές. Ο κύριος σκοπός του είναι η δημιουργία ενός σταθερού και ασφαλούς περιβάλλοντος για την εκτέλεση των εφαρμογών. Κάθε εφαρμογή εκτελείται στο δικό της εικονικό σύστημα. Επομένως, δεν επηρεάζεται από άλλες εφαρμογές ή λειτουργίες του συστήματος.

Η χρήση ορισμένων πόρων επιτρέπεται μόνο με ειδικά προνόμια. Με αυτόν τον τρόπο διατηρείται ικανοποιητικό επίπεδο ασφάλειας. Ενώ οι βιβλιοθήκες Android Runtime είναι γραμμένες σε γλώσσα προγραμματισμού Java, το DVM μεταφράζει την Java σε γλώσσα που μπορεί να αντιληφθεί το λειτουργικό σύστημα. Η υπόλοιπη αρχιτεκτονική αποτελείται από το πλαίσιο εφαρμογής και το επίπεδο εφαρμογών που διαχειρίζονται τη γενική δομή εφαρμογής, όπως τα containers, οι ειδοποιήσεις και οι εφαρμογές.



Εικόνα 8: Λειτουργικό Σύστημα Android

Λόγω του μικρού μεγέθους τσιπ, της μη μεταβλητότητας της φύσης και της ενεργειακής απόδοσης, η μνήμη NAND επιλέχθηκε για να ενσωματωθεί σε συσκευές Android για λόγους αποθήκευσης. Η μνήμη NAND απαιτούσε ένα σύστημα αρχείων να «συνειδητοποιεί τους γενικούς περιορισμούς της μνήμης Flash και να τη λαμβάνει υπόψη στο επίπεδο του λογισμικού κατά την ανάγνωση και την εγγραφή δεδομένων από και προς το τσιπ». Το σύστημα YAFFS2 ήταν το πρώτο σύστημα αρχείων που εφαρμόστηκε για συσκευές που χρησιμοποιούν το λειτουργικό σύστημα Android. Μετά από μερικά χρόνια πραγματικής χρήσης από την άλλη πλευρά, πολλά ζητήματα σχετικά με την

απόδοση του συστήματος, την ταχύτητα των ενεργειών εισόδου / εξόδου και την κάλυψη μεγάλων αρχείων συνέβησαν.

Καθώς η αρχιτεκτονική των φορητών συσκευών τείνει να ακολουθεί την πορεία των υπολογιστών και να αποκτά επεξεργαστές πολλαπλών πυρήνων, δημιουργείται ένα άλλο εμπόδιο, καθώς το YAFFS2 δεν μπορεί να υποστηρίξει τη συγκεκριμένη τεχνολογία. Λίγο πριν την έκδοση 2.3 του λειτουργικού συστήματος Gingerbread, το σύστημα αρχείων αντικαταστάθηκε από το EXT4. Το συγκεκριμένο σύστημα, πέραν της επιτυχούς αντιμετώπισης των αδύναμων σημείων του προγόνου του, ενισχύεται με τη λειτουργία "journaling event", η οποία παρέχει επιλογές ανάκτησης και διευκολύνει την απόκτηση πειστηρίων κάτι που αποτελεί πολύ σημαντικό εργαλείο για εγκληματολογικούς και γενικούς σκοπούς, χρησιμοποιώντας τη «Γέφυρα Debug Android» (ADB). Η ADB χρησιμοποιεί μια σύνδεση TCP ή USB μεταξύ μιας Κινητής Συσκευής και ενός υπολογιστή. Το κατάλληλο λογισμικό εγκαθίσταται και στις δύο πλευρές για να αποκτήσει πληροφορίες αποσφαλμάτωσης, ξεκινάει μια περίοδο λειτουργίας κελύφους με την παρεχόμενη διεπαφή, ξεκινάει τις συναλλαγές αρχείων και προσθέτει ή αφαιρεί εφαρμογές. Αφού η ADB παρέχει μια διασύνδεση τερματικού, μπορούν να εκτελεστούν εύκολα δράσεις όπως η διαδικασία εξασφάλισης πλήρων δικαιωμάτων στη συσκευή (rooting) και η εξαγωγή της μνήμης. Η μνήμη NAND δεν ήταν συμβατή με τον πυρήνα των Linux. Γι’ αυτό έπρεπε μια νέα τεχνική να εφαρμοστεί προκειμένου να παρασχεθούν στα εξαρτήματα λογισμικού η δυνατότητα πρόσβασης στις περιοχές μνήμης flash. Το σύστημα τεχνολογίας μνήμης (MTD) ήταν μία από τις εγκαταστάσεις που χρησιμεύει ως ενδιάμεσος σύνδεσμος μεταξύ του πυρήνα και του συστήματος αρχείων και υπάρχει σε πολλές συσκευές Android. Τα ακουστικά που δεν υποστηρίζουν το σύστημα MTD χρησιμοποιούν συνήθως το απλό στρώμα συναλλαγών Flash (FTL) που επιτρέπει την επικοινωνία μεταξύ των δύο μερών. Παρόλο που δεν υπάρχουν περιορισμοί σχετικά με τους αριθμούς ή τους τύπους MTD, υιοθετήθηκε ένα συγκεκριμένο πρότυπο από πολλούς κατασκευαστές συσκευών. Τα MTD χωρίζονται σε πολλά «διαμερίσματα δίσκου» (partitions), ανάλογα με τον τύπο των πληροφοριών που αποθηκεύουν. Μπορούν να περιέχουν πληροφορίες σχετικά με την εκκίνηση, την ανάκτηση, τα δεδομένα χρηστών, τις ρυθμίσεις παραμέτρων, την προσωρινή μνήμη και τα αρχεία συστήματος.

Το λειτουργικό σύστημα Android αναπτύχθηκε για Κινητές Συσκευές, αλλά χρησιμοποιεί τον πυρήνα των συστημάτων Linux. Όπως το λειτουργικό σύστημα Linux, έτσι και το Android είναι λειτουργικό ανοικτού κώδικα που επιτρέπει στους προγραμματιστές σε όλο τον κόσμο να τροποποιήσουν και να ενισχύσουν τον κώδικα του.

Το λειτουργικό σύστημα Android μπορεί να αποθηκεύει δεδομένα σε διαφορετικές περιοχές των συσκευών.

- Σε Κοινόχρηστες προτιμήσεις, οι οποίες αφορούν κυρίως το .XML και άλλους τύπους πληροφοριών που προκύπτουν από τα δεδομένα εφαρμογών.
- Στη περιοχή εσωτερικής αποθήκευσης που αναφέρεται σε μνήμη flash ή σε εξωτερικές εικόνες αποθήκευσης. Οι MTD είναι η πιο αντιπροσωπευτική κατηγορία. Βρίσκονται κάτω από το φάκελο / dev / mtd και είναι αυτά που εμπεριέχουν αρχεία συστήματος και δεδομένα χρήστη.
- Στη περιοχή εξωτερικής αποθήκευσης, που σχετίζεται με αφαιρούμενα μέσα. Η κατηγορία αυτή δεν εμπίπτει στο πεδίο εφαρμογής της παρούσας έρευνας και τα στοιχεία της δεν θα αναφερθούν περαιτέρω ούτε θα αναλυθούν.
- Στη περιοχή Βάσεων δεδομένων SQLite: Μπορούν να βρίσκονται σε διαφορετικά σημεία μέσα στην εσωτερική μνήμη και μπορεί να περιέχουν δεδομένα που δημιουργούνται από χρήστη ή εφαρμογή. Ορισμένες από τις σημαντικότερες βάσεις δεδομένων σχετίζονται με επαφές (contacts.db), μηνύματα (mmssms.db), συντεταγμένες GPS (geolocation.db), διαπιστευτήρια λογαριασμών Google (accounts.db).
- Τη περιοχή Δικτύου, το οποίο αλληλεπιδρά με εφαρμογές αποθήκευσης στο διαδίκτυο (Dropbox, Google Drive) ή με πακέτα και τεχνουργήματα.

Έχει δημοσιευθεί ότι υπάρχουν περισσότερα από 1 εκατομμύριο εφαρμογές Android διαθέσιμες από το Google Play, καθώς και πολλά εναλλακτικά αποθετήρια διαθέσιμα σε χρήστες Android.

Ένας εξεταστής πρέπει να γνωρίζει ότι υπάρχουν πολλές παραλλαγές για κάθε έκδοση του Android που μπορεί να βρεθεί κατά την εξέταση μιας συσκευής. Αυτές συνήθως αναφέρονται ως "προσαρμοσμένες ROM".

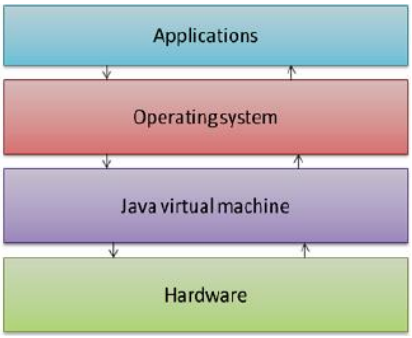
Προστασία Προσωπικών Δεδομένων σε μια Κινητή Συσκευή: Παρακάτω περιγράφονται ορισμένες κοινές επιλογές κλειδώματος συσκευών Android που χρησιμοποιούνται για την ασφάλεια των προσωπικών δεδομένων από τους κατόχους τους.

Κλείδωμα Android: Υπάρχουν 7 επιλογές όταν πρόκειται για το κλείδωμα του Android:

- **Facelock**: Χρησιμοποιεί μια λήψη φωτογραφίας του χρήστη που καταγράφηκε από την μπροστινή κάμερα για να ξεκλειδώσει τη συσκευή
- **Δακτυλικό αποτύπωμα:** Οι νεότερες συσκευές έχουν ενσωματωμένο αισθητήρα δακτυλικών αποτυπωμάτων. Ο χρήστης τοποθετεί το δάχτυλό του πάνω στον αισθητήρα για να αποκτήσει πρόσβαση στη συσκευή.
- **Φωνή:** Ο χρήστης μιλάει ενώ ξεκλειδώνει τη συσκευή και η φωνή του αποκτά πρόσβαση.
- **Iris Scan**: Σαρώνει την ίριδα του ματιού ενός χρήστη για να επιβεβαιώσει την ταυτότητα του
- **Έξυπνη τοποθεσία**: Οι αξιόπιστες τοποθεσίες αφήνουν τη συσκευή ξεκλείδωτη έως και τέσσερις ώρες όταν είναι ενεργοποιημένη και η συσκευή είναι συνδεδεμένη σε ασφαλές σημείο πρόσβασης Wi-Fi, με αξιόπιστο Bluetooth, NFC ή αν η συσκευή εντοπίζει κίνηση του σώματος.
- **Μοτίβο κτυπήματος**: Ο χρήστης πληκτρολογεί συγκεκριμένες θέσεις στην οθόνη με μια συγκεκριμένη σειρά για να αποκτήσει πρόσβαση στη συσκευή.
- **Κωδικός PIN ή Κωδικός και Πρότυπο**: Αυτή είναι η πιο κοινή μέθοδος κλειδώματος οθόνης που εισάγει ένας χρήστης. Το μοτίβο αριθμεί σημεία αναφοράς στα οποία πρέπει να συνδεθεί. Αυτά τα δεδομένα αποθηκεύονται σε ένα αρχείο που ονομάζεται Gesture Key. Αυτό το αρχείο αποθηκεύει το SHA1 hash των σημείων διέλευσης που δημιουργεί ο χρήστης. Αν η συσκευή είναι κλειδωμένη, ενδέχεται να γίνει εξαγωγή της μνήμης flash με εναλλακτικές μεθόδους απόκτησης, για παράδειγμα με μέθοδο JTAG. Εάν αποκωδικοποιήσουμε τον κωδικό κλειδώματος προτύπου από την εξαγωγή, μπορούμε να ξεκλειδώσουμε στη συνέχεια τη συσκευή για συμβατική εκχύλιση χρησιμοποιώντας εργαλεία Ψηφιακής Εγκληματολογίας Κινητών Συσκευών.

4.2.2. Blackberry

Οι συσκευές που λειτουργούν με το Blackberry OS σχεδιάζονται από την εταιρεία RIM και θεωρούνται οι πιο δημοφιλείς μέσα στον επιχειρηματικό κόσμο. Λίγα πράγματα σχετικά με το ίδιο το λειτουργικό σύστημα και τα συστατικά του είναι γνωστά, δεδομένου ότι ο κατασκευαστής δεν παρέχει επαρκή τεκμηρίωση. Σημαντικό χαρακτηριστικό σχετικά με το λειτουργικό σύστημα είναι ότι αποτελείται από δύο χωριστά περιβάλλοντα χρόνου εκτέλεσης, ένα Java ME που προορίζεται για εφαρμογές και ένα MDS που προορίζεται για λειτουργικότητα και λειτουργίες δικτύου. Τα δεδομένα χρήστη, όπως επαφές, μηνύματα, εικόνες και αντικείμενα λειτουργικού συστήματος, αποθηκεύονται σε βάσεις δεδομένων, οι οποίες αποτελούν στόχο απόκτησης κάθε έρευνας.



Εικόνα 9: Λειτουργικό Σύστημα Blackberry

Το βασικό λειτουργικό σύστημα του Blackberry OS είναι χτισμένο γύρω από το QNX.

Το QNX περιγράφεται ως λειτουργικό σύστημα βασισμένο σε μικρο-πυρήνα. Αυτό επιτρέπει στους προγραμματιστές να επιλέξουν τη λειτουργικότητα των συσκευών τους. Πρόσφατα, η Blackberry αποφάσισε να χρησιμοποιήσει το λειτουργικό σύστημα Android για τις συσκευές της που θα πωληθούν στο μέλλον και θα μπορούν να ρυθμιστούν είτε από το χρήστη είτε από τον διαχειριστή του διακομιστή BES (BlackBerry Enterprise Server).

Κλείδωμα Blackberry: Ο μεμονωμένος κωδικός ασφαλείας μπορεί να έχει μήκος μεταξύ τεσσάρων έως δεκατεσσάρων χαρακτήρων. Οι λιγότερο ασφαλείς κωδικοί πρόσβασης απορρίπτονται από το Smart Phone, όπως αυτοί που αποτελούνται από πανομοιότυπους χαρακτήρες ή χαρακτήρες που αποτελούνται από φυσικές ακολουθίες (δηλ. 1234). Από προεπιλογή, επιτρέπονται έως και δέκα προσπάθειες για τη σωστή εισαγωγή των χαρακτήρων του κωδικού πρόσβασης και εάν ένας κωδικός πρόσβασης εισαχθεί εσφαλμένα δέκα συνεχόμενες φορές, αυτό θα σβήσει αυτόματα όλα τα δεδομένα στη συσκευή BlackBerry. Αυτή η προεπιλεγμένη λειτουργία ασφαλείας είναι ενσωματωμένη στη συσκευή. Ένας χρήστης μπορεί επίσης να ρυθμίσει τον αριθμό των επιτρεπόμενων προσπαθειών κωδικού πρόσβασης συσκευής. Επιπλέον, εάν μια συσκευή είναι συνδεδεμένη σε ένα διακομιστή BES, μπορεί να ενεργοποιηθεί μια πολιτική διεύθυνσης ειδοποίησης, η οποία μειώνει κατά το ήμισυ τον αριθμό των προσπαθειών εισαγωγής κωδικού πρόσβασης.

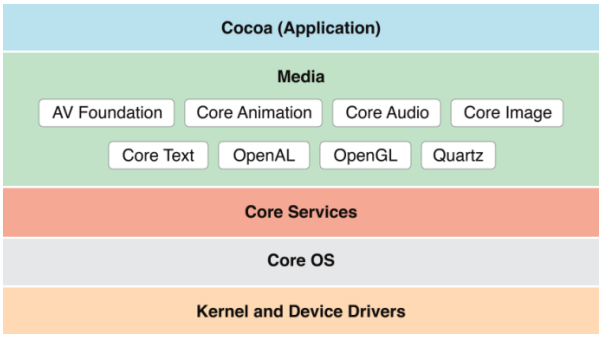
Εάν η πολιτική πληροφόρησης σχετικά με την ειδοποίηση κινδύνου από τον διακομιστή BES και ο ιδιοκτήτης της συσκευής είναι υπό πίεση για την παροχή του κωδικού πρόσβασης της συσκευής, ο χρήστης μπορεί να ειδοποιήσει τον διαχειριστή του διακομιστή BES παρέχοντας έναν τροποποιημένο κωδικό πρόσβασης, ο οποίος είναι ο ίδιος κωδικός πρόσβασης με τον αρχικό κωδικό πρόσβασης του χρήστη της συσκευής BlackBerry[8]. Στη συνέχεια, η συσκευή ξεκλειδώνει κανονικά, αλλά αποστέλλει μήνυμα ηλεκτρονικού ταχυδρομείου στη διεύθυνση ειδοποίησης πίεσης με την οποία ειδοποιεί τον διαχειριστή του διακομιστή BES, ώστε να είναι δυνατή η έναρξη των μέτρων προστασίας δεδομένων. Αντίγραφα αυτού του μηνύματος ηλεκτρονικού ταχυδρομείου δεν αποθηκεύονται στη λίστα Απεσταλμένων στοιχείων. Σε τέτοιες περιπτώσεις, οι πληροφορίες κωδικού πρόσβασης που παρέχονται από έναν ύποπτο / κατηγορούμενο δεν πρέπει να ενεργούν στη συσκευή από τον ερευνητή, αλλά ο κωδικός πρόσβασης θα πρέπει να εμπεριέχεται στις σημειώσεις των ερευνητών και να μεταδίδεται στον εγκληματοδόχο. Εάν εισάγεται λάθος κωδικός πρόσβασης 10 φορές στη συσκευή, η συσκευή θα καθαριστεί πλήρως. Επαναφέρεται σε κατάσταση εργοστασιακών ρυθμίσεων εκτός πλαισίου και ο κωδικός θα επαναφερθεί. Συνέπεια αυτού είναι η ολική καταστροφή όλων των δεδομένων που βρίσκονται στη μνήμη της συσκευής, χωρίς να υπάρχει κάποια δυνατότητα ανάκτησης. Το τηλέφωνο θα εξακολουθεί να είναι χρησιμοποιήσιμο και το λειτουργικό σύστημα θα παραμείνει αμετάβλητο. Επομένως, αυτή η τεχνική δεν μπορεί να χρησιμοποιηθεί για την επιστροφή από ένα πρόβλημα αναβάθμισης του λειτουργικού συστήματος[4, 6].

Προφανώς, αυτό είναι ένα σοβαρό πρόβλημα σε μια Ψηφιακή Έρευνα. Η καλύτερη πρακτική συνιστά την συνεργασία του εξεταστή με τον ιδιοκτήτη της συσκευής ελπίζοντας ότι εκείνος-η θα υπαγορεύσει τον κωδικό πρόσβασης για το ξεκλείδωμα της συσκευής.

4.2.3. iOS

Το iOS κυκλοφόρησε αρχικά το 2007 για το iPhone της Apple και δημιουργήθηκε από την Apple για να είναι αποκλειστικά σε όλες τις Κινητές Συσκευές. Αυτό το λειτουργικό σύστημα έχει σχεδιαστεί γύρω από την οθόνη αφής ως είσοδο αντί για χρήση φυσικού πληκτρολογίου. Η κύρια συσκευή αποθήκευσης ενός κινητού τηλεφώνου που εκτελεί το iOS χωρίζεται σε δύο κατατμήσεις. Η πρώτη περιέχει τη βασική δομή του λειτουργικού συστήματος (OS) και τις εφαρμογές, ενώ η δεύτερη περιέχει όλα τα δεδομένα που χειρίζονται οι χρήστες. Δεδομένα μεγαλύτερης σημασίας βρίσκονται σε διαμερίσματα δίσκου του iOS[14]. Μερικά από αυτά παρουσιάζονται μέσα στις επόμενες γραμμές

- **Dhcpclient**: Αρχείο επέκτασης τύπου plist που περιέχει διευθύνσεις IP
- **Keychains.db**: Βάση δεδομένων με αποθηκευμένους κωδικούς πρόσβασης εφαρμογών
- **Αρχεία καταγραφής (Log)**: πληροφορίες συστήματος όπως Σειριακός Αριθμός (S / N), έκδοση OS και έκδοση Υλικολογισμικού
- **Κινητό**: Δεδομένα χρήστη
- **Προτιμήσεις**: Αντικείμενα συσκευών και δικτύων
- **Φάκελος Root**: Πληροφορίες θέσης GPS, πιστοποιητικά Pairing
- **Εκτέλεση (run)**: Αρχείο καταγραφής συστήματος
- **Tmp**: Εφεδρικό plist



Εικόνα 10: Λειτουργικό Σύστημα iOS

Τα τελευταία χρόνια το λειτουργικό σύστημα έχει εξελιχθεί σε μεγάλες δυνατότητες που προσφέρουν δυνατότητες ψηφιακού βοηθού, βιομετρική αναγνώριση και βελτιωμένα χαρακτηριστικά ασφαλείας.

Οι 5 πιο συνηθισμένοι τύποι κωδικών πρόσβασης στις συσκευές IOS, τους οποίους μπορεί να αντικρίσει ένας ψηφιακός ερευνητής κατά την κατάσχεση μιας Κινητής Συσκευής, είναι οι εξής:

- Κωδικός Πρόσβασης με 4-ψηφία
- Κωδικός Πρόσβασης με 6 ψηφία
- Σύνθετος Κωδικός Πρόσβασης – Μόνο με αριθμούς (Complex –Digits only)
- Σύνθετος Κωδικός Πρόσβασης (Complex)
- Αναγνωριστικό Αφής (Touch ID) - Στις νεότερες εκδόσεις του iPhone

Τις περισσότερες φορές οι χρήστες του iOS επιλέγουν να χρησιμοποιήσουν ένα τετραψήφιο κωδικό πρόσβασης ή ένα αναγνωριστικό αφής, καθώς είναι ο ευκολότερος και ταχύτερος τρόπος να ξεκλειδώσουν τη συσκευή και να την χρησιμοποιήσουν. Η επιτυχία ενός ψηφιακού ερευνητή για την παράκαμψη του τύπου ασφαλείας ποικίλλει ανάλογα με την έκδοση του iOS και του υλικού chipset της συσκευής.

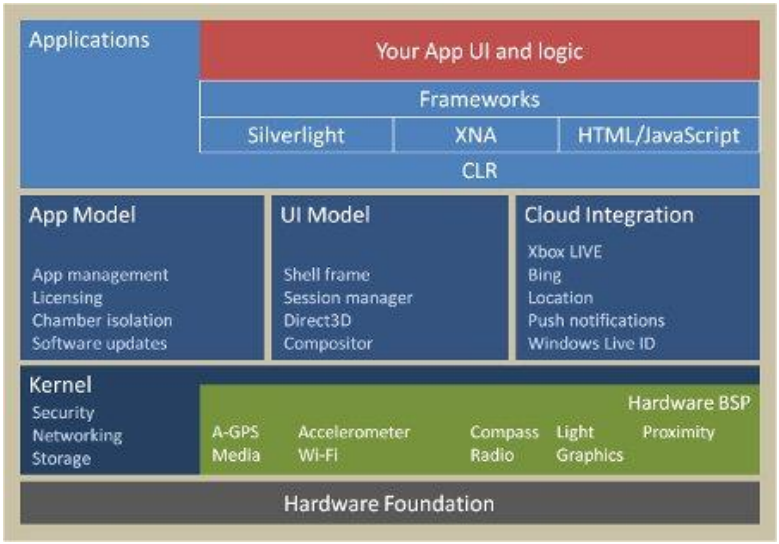
Κλείδωμα iOS: Οι ερευνητές μπορεί να είναι σε θέση να προσδιορίσουν εύκολα τον τύπο του κωδικού πρόσβασης που χρησιμοποιείται στη συσκευή, απλά κοιτάζοντας την οθόνη κλειδώματος που εμφανίζεται.

- **Touch ID**: Μπορεί να ενεργοποιηθεί από κάποιον χρήστη ενός IPhone 5S ή νεότερου καθώς και σε ένα IPAD pro, iPad Air 2 ή iPad mini 3 ή νεότερη έκδοση. Όταν ενεργοποιηθεί, ο χρήστης δεν χρειάζεται να χρησιμοποιεί κωδικό πρόσβασης εάν έχει αποθηκεύσει τα δακτυλικά αποτυπώματα στη συσκευή του και έχει ενεργοποιήσει τη λειτουργία.
- **Τετραψήφιος κωδικός**: ένας τετραψήφιος κωδικός αποτελείται από τέσσερις αριθμητικούς χαρακτήρες που αντιστοιχούν σε 10000 δυνατούς συνδυασμούς. Ανάλογα με την έκδοση iOS που εκτελείται στη συσκευή και το ίδιο το υλικό, ο τετραψήφιος κωδικός πρόσβασης μπορεί να είναι σχετικά εύκολος να νικηθεί. Αρκετές εταιρείες που παρέχουν εργαλεία Ψηφιακής Εγκληματολογίας Κινητών Συσκευών, συμπεριλαμβανομένου του λογισμικού της Cellebrite που περιλαμβάνεται στη παρούσα διατριβή, έχουν δημιουργήσει διάφορα εργαλεία προκειμένου να αποκτήσουν αυτόν τον τύπο κωδικού πρόσβασης.
- **6 ψηφία**: Ένας 6-ψήφιος κωδικός αποτελείται από 6 αριθμητικούς χαρακτήρες που αντιστοιχούν σε 1000000 πιθανούς συνδυασμούς.
- **Συμπληρωματικοί κωδικοί πρόσβασης**: Αυτός ο τύπος κωδικού πρόσβασης, ο οποίος χωρίζεται σε Σύνθετο κωδικό και Σύνθετο κωδικό με ψηφία μόνο, αποτελείται από περισσότερους από έξι χαρακτήρες. Μέχρι τώρα δεν βρέθηκε τεκμηρίωση σχετικά με το μέγιστο μήκος αυτού του τύπου κωδικού πρόσβασης.

4.2.4. Windows 10 Mobile

Η Microsoft, όπως η Apple, διαθέτει το ιδιόκτητο λειτουργικό της σύστημα, το οποίο είναι σήμερα τα Windows 10 για κινητά τηλέφωνα. Το Windows Mobile OS είναι η εξέλιξη του Windows CE, που χρησιμοποιείται κυρίως σε φορητές συσκευές, όπως φορητοί υπολογιστές και PDA. Πρόκειται για ένα σύστημα που βασίζεται στα Windows, με παρόμοιες ιδιότητες ειδικά τροποποιημένες για να εφαρμοστούν στη φύση των Κινητών Συσκευών.

Ένα από τα βασικά παραδείγματα αυτής της κατηγορίας είναι το σύστημα αρχείων του. Το σύστημα αρχείων T-FAT (Transaction Safe File Allocation Table) είναι μια παραλλαγή του συστήματος αρχείων FAT που χρησιμοποιείται σε εκδόσεις υπολογιστών Windows, βελτιωμένες με επιλογές αποκατάστασης. Οι συσκευές υποστηρίζουν τη χρήση τσιπ NOR ή NAND. Η αρχιτεκτονική Windows MobileOS αποτελείται από παρόμοια στρώματα με αυτά των προηγούμενων τύπων συσκευών. Το ανώτερο στρώμα, το Application UI είναι η διάμεσος μεταξύ του χρήστη και των εφαρμογών, ενώ το κάτω επίπεδο πάνω από το υλικό παρέχει την κατάλληλη υποδομή για την ολοκλήρωση συνηθισμένων καθηκόντων ρουτίνας, όπως εκκίνηση, δικτύωση και άλλες λειτουργίες. Εν τω μεταξύ, το Framework και το στρώμα CLR περιέχουν βιβλιοθήκες που εξυπηρετούν την εκτέλεση και απόδοση των εφαρμογών. Οι δύο κύριες πηγές θησαυρού σε ψηφιακές έρευνες που αφορούν συσκευές Windows Mobile είναι οι βάσεις δεδομένων Ce-mail.vol και pim.vol. Το Cemail.vol περιέχει πληροφορίες σχετικά με τις επικοινωνίες, συμπεριλαμβανομένων των μηνυμάτων κειμένου και των τμημάτων των ηλεκτρονικών μηνυμάτων πέρα από τα συνημμένα μηνύματα [15]. Από την άλλη πλευρά, το pim.vol είναι μια συλλογή διαφορετικών βάσεων δεδομένων σχετικά με τα αρχεία καταγραφής κλήσεων (clog.db), τα αρχεία επαφών, τα αρχεία καταχωρήσεων γρήγορων κλήσεων (speed.db) και τις λίστες εργασιών.



Εικόνα 11: Λειτουργικό Σύστημα Windows 10 Mobile

Παλαιότερα γνωστά ως «*τηλέφωνο των Windows*», τα Windows 10 επιτρέπουν στους χρήστες να έχουν την ίδια εμπειρία στις κινητές τους συσκευές όπως έχουν στον προσωπικό υπολογιστή τους. Ορισμένα χαρακτηριστικά που περιλαμβάνονται σε συσκευές Windows 10 Mobile είναι η ψηφιακή οδηγός Cortana, το Ψηφιακό Πορτοφόλι, το OneDrive και τα Office 365.

Κλείδωμα Windows 10 Mobile: Η πιο συνηθισμένη τεχνική κλειδώματος μιας συσκευής Windows 10 mobile είναι η εξής:

- Από το κεντρικό μενού ο χρήστης επιλέγει «Ρυθμίσεις» και στη συνέχεια επιλέγει «Λογαριασμοί» > «Επιλογές Εισόδου»
- Συνεχίζοντας ο χρήστης για να ρυθμίσει το PIN για πρώτη φορά μπορεί να επιλέξει «Προσθήκη» και να πληκτρολογήσει το νέο PIN στο πλαίσιο «Νέο PIN» και στη συνέχεια πληκτρολογεί για μια ακόμα φορά το κωδικό στο πλαίσιο κειμένου «Επιβεβαίωση PIN».[3]
- Εάν ο χρήστης θέλει να αλλάξει το τρέχον PIN της συσκευής επιλέγει «Αλλαγή» και πληκτρολογεί το τρέχον PIN στο πλαίσιο «Τρέχον PIN» και στη συνέχεια πληκτρολογεί και πάλι τον κωδικό πρόσβασής του στο πλαίσιο Επιβεβαίωση PIN.
- Τέλος ο χρήστης επιλέγει OK για την καταχώρηση του κωδικού πρόσβασης.

Παράλληλα ένας χρήστης μπορεί να ενεργοποιήσει και τη κρυπτογράφηση των δεδομένων της συσκευής. Για να το κάνει αυτό τα βήματα είναι τα ακόλουθα[3]:

- Άνοιγμα των «Ρυθμίσεων» και στη συνέχεια επιλογή «Συστήματος»
- Επιλογή «Κρυπτογράφηση Συσκευής»
- Για την κρυπτογράφηση μιας συσκευής Windows 10 Mobile απαιτείται κωδικός PIN ή κωδικός πρόσβασης. Εάν ο χρήστης δεν έχει ήδη ρυθμίσει κάποιον, θα μεταφερθεί στις ρυθμίσεις για τη ρύθμιση κωδικού πρόσβασης / PIN.

Για να ανακτηθεί μια εικονική αναπαράσταση ενός τηλεφώνου συστήματος Windows 10 και να εκτελεστεί μια φυσική εξαγωγή, μερικές φορές η καλύτερη επιλογή είναι να χρησιμοποιηθούν μέθοδοι JTAG ή Chip-Off. Σήμερα υπάρχει ένα εργαλείο Windows Phone με το όνομα WPInternals. Αυτό το εργαλείο μπορεί να ξεκλειδώνει το bootloader και να δίνει πρόσβαση root στο τηλέφωνο. Είναι σημαντικό να σημειωθεί ότι αυτή η τεχνική λειτουργεί ακόμα και με κλειδωμένα τηλέφωνα. Για παράδειγμα, εάν αν σε ένα κλειδωμένο τηλέφωνο υπήρχαν περισσότερα από 1.000.000 δευτερόλεπτα για την επόμενη δοκιμή ξεκλειδώματος, το εργαλείο WPInternals δημιουργεί με επιτυχία μια φυσική εικόνα της συσκευής η οποία μετά μπορεί να αναλυθεί από τον ερευνητή χρησιμοποιώντας το πρόγραμμα Oxygen Forensic Detective.

4.2.5. Άλλοι τύποι Κινητών Συσκευών

Παρακάτω ακολουθούν επιπρόσθετοι τύπο που χαρακτηρίζονται ως Κινητές Συσκευές εκτός των τηλεφωνικών στο χώρο της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών:

Tablet: Όπως και με τα κινητά τηλέφωνα, υπάρχουν πολλοί διαφορετικοί τύποι Tablet στην αγορά. Το λογισμικό και τα λειτουργικά συστήματα που λειτουργούν σε αυτές τις συσκευές είναι πολύ παρόμοια. Τα iOS και το Android είναι τα πιο ευρέως διαδεδομένα λειτουργικά συστήματα που λειτουργούν σε Tablet. Ορισμένα Tablet έρχονται επίσης με ένα σχέδιο δεδομένων που τρέχει σε ένα κυψελοειδές δίκτυο. Εργαλεία Ψηφιακής Εγκληματολογίας όπως αυτά της Cellebrite φέρουν δυνατότητες υποστήριξης Tablet.

Συσκευές GPS: Οι συσκευές GPS μπορούν να χρησιμοποιηθούν για θαλάσσια ναυσιπλοΐα, καθοδήγηση και στην αεροπορία. Ακόμα, φορητές συσκευές GPS χρησιμοποιούνται για ψυχαγωγία, όπως ποδηλασία και πεζοπορία, ή μπορούν να χρησιμοποιηθούν από υπηρεσίες έκτακτης ανάγκης κατά τη διάρκεια καταστροφών. Πολλές από αυτές τις συσκευές μπορούν να υποστηριχθούν από εργαλεία Ψηφιακής Εγκληματολογίας. Πολλές από αυτές τις συσκευές έρχονται επίσης με μια κάρτα SD, η οποία μπορεί να είναι πολύτιμη για έναν ερευνητή. Επίσης στοιχεία μπορούν να βρεθούν και σε έναν υπολογιστή ενός χρήστη που συγχρονίζεται με τη συσκευή GPS.

Τέσσερις κύριες πηγές αποδεικτικών στοιχείων είναι διαθέσιμες από μια συσκευή GPS

- **Σημεία Διαδρομής** (Track Point): Μια γεωγραφική καταγραφή η οποία συλλαμβάνεται και αποθηκεύεται αυτόματα από μια συσκευή GPS.
- **Καταγραφή διαδρομής** (Track Log):Μια λίστα Track Points που μπορούν να χρησιμοποιηθούν για την επαναδημιουργία μιας διαδρομής που ακολούθησε ο χρήστης
- **Σημείο δρόμου** (Waypoint): Ένα γεωγραφικό σημείο ενδιαφέροντος που δημιουργείται από έναν χρήστη και που αποτελεί σημείο ενδιαφέροντος όπως ένα εστιατόριο ή ένα ξενοδοχείο
- **Διαδρομή** (Route): Μια σειρά από σημεία που έχει δημιουργήσει ένας χρήστης σε ένα ταξίδι.

Θα πρέπει επίσης να σημειωθεί ότι οι πιο πρόσφατες συσκευές GPS μπορούν επίσης να περιέχουν δεδομένα σχετικά με Κινητές Συσκευές που συνδέονται μέσω Bluetooth ή ακόμα και αναζητήσεις στο Διαδίκτυο.

4.3. Αντίστροφη Ψηφιακή Εγκληματολογία

Η μέθοδος «Αντίστροφης Ψηφιακής Εγκληματολογίας» (Anti-Forensics) είναι ένα ανώριμο πεδίο της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών, ειδικά αν μιλάμε για κινητά τηλέφωνα που βασίζονται στην Αντίστροφη Ψηφιακή Εγκληματολογία. Οι αντιτρομολόγοι μπορούν να αναγνωρίσουν τον κλάδο της Αντίστροφης Ψηφιακής Εγκληματολογίας ως "Η οποιαδήποτε προσπάθεια που μπορεί να υπονομευθεί για την διακύβευση της διαθεσιμότητας ή της χρησιμότητας των αποδεικτικών στοιχείων στην εγκληματολογική διαδικασία"[22]. Η διαθεσιμότητα Ψηφιακών Πειστηρίων μπορεί να διακυβευτεί παρεμποδίζοντας τη διαδικασία δημιουργίας τους, κρύβοντας ή παραβιάζοντας την ακεραιότητα τους ή διαγράφοντας τα.

Η άμεση πρόσβαση στην εσωτερική μνήμη των κινητών τηλεφώνων είναι ένα από τα κύρια προβλήματα στον τομέα της Ψηφιακής Εγκληματολογίας Κινητών Συσκευών. Ακόμη και αν η αφαιρούμενη μνήμη μπορεί να αφαιρεθεί και να αναλυθεί με άμεσο τρόπο, η εσωτερική μνήμη δεν

μπορεί. Αυτό το σενάριο καθιστά την εσωτερική μνήμη του τηλεφώνου ιδανική για να εφαρμοστεί σε τεχνικές Αντίστροφης Ψηφιακής Εγκληματολογίας.

Υπάρχουν τέσσερις βασικές κατηγορίες τεχνικών Αντίστροφης Ψηφιακής Εγκληματολογίας:

- **Καταστροφή των πειστηρίων**: Υπάρχουν πολλά εργαλεία που χρησιμοποιούνται για την καταστροφή τεκμηρίων, προκειμένου να καταστούν άχρηστα κατά τη διάρκεια της εγκληματολογικής έρευνας. Αυτά τα εργαλεία συνήθως παράγουν αποδείξεις κατά τη χρήση τους, γεγονός που καθιστά τη διαδικασία της ψηφιακής ανάλυσης πιο περίπλοκη.
- **Απόκρυψη των πειστηρίων:** Χρησιμοποιείται για να κρύψει τα αποδεικτικά στοιχεία από τον εγκληματολόγο και όχι από τα εγκληματολογικά εργαλεία, μειώνοντας έτσι την προβολή των αποδεικτικών στοιχείων ή κάνοντάς τα εντελώς αόρατα. Η αποτελεσματικότητα αυτής της τεχνικής εξαρτάται σε μεγάλο βαθμό από τους περιορισμούς των εγκληματολογικών ερευνών ή / και του εργαλείου Ψηφιακής Εγκληματολογίας Κινητών Συσκευών.
- **Εξάλειψη της πηγής των πειστηρίων:** Αυτή η τεχνική χρησιμοποιείται για την αποτροπή της δημιουργίας τεκμηρίων αντί για την απόκρυψη ή καταστροφή των αποδεικτικών στοιχείων.
- **Παραποίηση των πειστηρίων**: Αυτή η τεχνική χρησιμοποιείται προκειμένου να παραπλανηθεί ο ψηφιακός ερευνητής.

5. Πειραματικό μέρος

Σε αυτή την ενότητα θα γίνει μια πειραματική ανάλυση πάνω σε Κινητές Συσκευές χρησιμοποιώντας τα εργαλεία που ακολουθούν παρακάτω. Οι Κινητές Συσκευές που χρησιμοποιήθηκαν σε αυτήν την διπλωματική εργασία ήταν ένα iPhone4 μια Κινητή Συσκευή Huawei P10 Lite και μια Κινητή Συσκευή Android μοντέλου LG-A1000. Τα εργαλεία Ψηφιακής Έρευνας και Ανάλυσης που χρησιμοποιήθηκαν στα πλαίσια της διπλωματικής αυτής εργασίας θα περιγραφούν λεπτομερώς στην επικείμενη ενότητα ενώ θα ακολουθήσουν οδηγίες ανάλυσης καθώς και κάποια σενάρια στα οποία ένας ερευνητής μπορεί να κάνει χρήση τους στα πλαίσια μιας πραγματικής υπόθεσης.

5.1. Το εργαλείο MobSF

Το εργαλείο Mobile Security Framework (MobSF) είναι ένα αυτοματοποιημένο πλαίσιο ελέγχου το οποίο αφορά Κινητές Συσκευές Android, iOS αλλά και Windows και μπορεί να εκτελέσει στατική και Δυναμική Ανάλυση, να ελέγξει τη συσκευή για τυχόν κακόβουλο λογισμικό ενώ παράλληλα δίνεται η δυνατότητα και για έλεγχο διαδικτυακών εφαρμογών. Μπορεί να χρησιμοποιηθεί για την αποτελεσματική και γρήγορη ανάλυση ασφάλειας των εφαρμογών Android, iOS και Windows και φέρει υποστήριξη και για δυαδικά αρχεία τύπου APK, IPA & APPX και ZIP. Επιπροσθέτως το MobSF μπορεί να κάνει δυναμικές Δοκιμές Διείσδυσης (Penetration Testing) στις εφαρμογές Android μιας Κινητής Συσκευής κατά το χρόνο εκτέλεσης τους και διαθέτει δυνατότητες συγχώνευσης API Web που υποστηρίζονται από το ενσωματωμένο εργαλείο CapFuzz, έναν σαρωτή ασφαλείας για το συγκεκριμένο περιβάλλον WebAPI.

Το εργαλείο MobSF έχει σχεδιαστεί από τον Ινδό προγραμματιστή Ajin Abraham, συνεργάτες του οποίου είναι οι Dominik Schlecht, Magaofei, Matan Dobrushin και Vincent Nadal. Όπως αναφέρθηκε διαθέτει 2 επιλογές ανάλυσης την στατική ανάλυση και τη δυναμική.

Στη στατική ανάλυση ένας ερευνητής μπορεί να επιλέξει μια εφαρμογή π.χ. επέκτασης IPA και με το πέρας της διαδικασίας ανάλυσης από το εργαλείο, η οποία γίνεται αυτοματοποιημένα, να λάβει μια λεπτομερής Αναφορά (Report) για την συγκεκριμένη εφαρμογή η οποία στη συνέχεια μπορεί να αποθηκευτεί τοπικά χρησιμοποιώντας τις δυνατότητες του γραφικού περιβάλλοντος MobSF. Για να χρησιμοποιήσει ένας ερευνητής την στατική ανάλυση του εργαλείου θα πρέπει αφού ξεκινήσει το πρόγραμμα (γράφοντας την εντολή "***python3 manage.py runserver***" σε Linux ή πληκτρολογώντας σε cmd "***run.bat***" σε Windows) από το φάκελο του MobSF να μεταβεί στην διεύθυνση 127.0.0.1:8000 όπου και έχει στηθεί το γραφικό περιβάλλον του εργαλείου.

Εικόνα 12: MobSF αρχική σελίδα

Στη Δυναμική Ανάλυση αντιθέτως, παρέχεται η δυνατότητα σε έναν ερευνητή να επιτρέψει στο εργαλείο να συνδεθεί στη Κινητή Συσκευή ή σε μια εικονική συσκευή android (Android VM) και να κάνει εκείνο τον έλεγχο στην εφαρμογή που έχει επιλέξει ο χρήστης προς ανάλυση.

Η Δυναμική Ανάλυση του MobSF για την ορθή λειτουργία της, απαιτεί κάποιες βασικές γνώσεις παραμετροποίησης ρυθμίσεων σε Linux αλλά και Windows λειτουργικά συστήματα και οι οδηγίες για τη παραμετροποίηση αυτή μπορούν να ληφθούν από την επίσημη ιστοσελίδα του MobSF στο Github [25]. Αναλυτική περιγραφή των εντολών που ακολούθησαν για τη παραμετροποίηση της σύνδεσης μεταξύ της εικονικής συσκευής Android και του εργαλείου βγαίνει εκτός θέματος της συγκεκριμένης διπλωματικής εργασίας και για το λόγο αυτό δε θα γίνει περεταίρω περιγραφή. Να σημειωθεί ότι σε αυτή τη διπλωματική εργασία το εργαλείο MobSF λειτούργησε σε περιβάλλον Linux με εγκατεστημένο λειτουργικό σύστημα Xubuntu 18.04.1 LTS [2] ενώ για τη Δυναμική Ανάλυση χρησιμοποιήθηκε η έτοιμη εικονική συσκευή Android "*MobSF Android x86 4.4.2 VM (v0.3)"* κατόπιν λήψης της μέσω της επίσημης ιστοσελίδας του εργαλείου στο GitHub [25].

5.1.1. Ανίχνευση κακόβουλου λογισμικού σε μια APK εφαρμογή

Σε αυτό το σημείο θα γίνει μια πρακτική άσκηση πάνω στην ανάλυση μιας εφαρμογής τύπου APK χρησιμοποιώντας το γραφικό περιβάλλον του εργαλείου MobSF και της εικονικής Android συσκευής που παραμετροποιήθηκε προηγουμένως προς Δυναμική Ανάλυση της αναλυθείσας εφαρμογής.

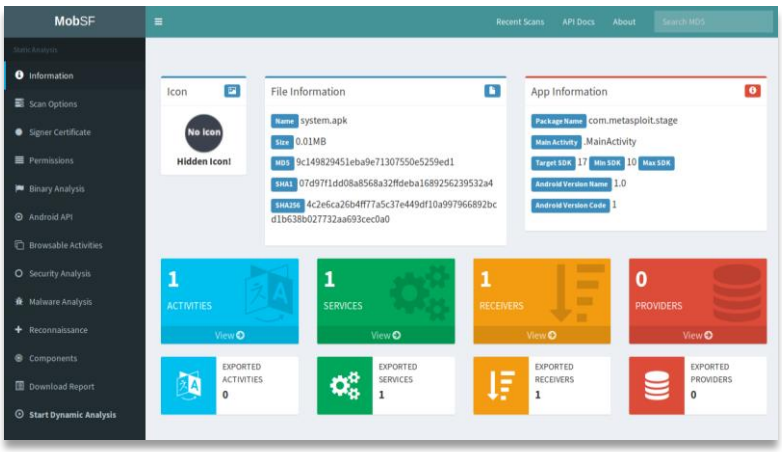
Για την άσκηση αυτή δημιουργήθηκε μια κακόβουλη εφαρμογή με δυνατότητα απομακρυσμένης σύνδεσης χρησιμοποιώντας το εργαλείο ***msfvenom*** το οποίο είναι κομμάτι ενός μεγαλύτερου Framework που είναι γνωστό εργαλείο για Δοκιμές Διείσδυσης και ονομάζεται Metasploit. Το εργαλείο Metasploit μπορεί να ληφθεί είτε στη commercial έκδοση του (Metasploit Pro) είτε στην Open Source από το παρακάτω σύνδεσμο[26].

Η εντολή για τη δημιουργία του συγκεκριμένου αρχείου .APK ήταν η "***msfvenom –p android/meterpreter/reverse_tcp LHOST= [Public IP] LPORT= [PORT] –f android >system.apk*** "

Να σημειωθεί ότι η αρχική ανάλυση από το εργαλείο αποτελεί την ***στατική ανάλυση*** της εφαρμογής system.apk που χρησιμοποιήθηκε στα πλαίσια της συγκεκριμένης διπλωματικής εργασίας. Στη συνέχεια θα ακολουθήσει και η ***Δυναμική Ανάλυση*** της εν λόγω εφαρμογής.

1. **Στατική ανάλυση: Λήψη πληροφοριών της εφαρμογής (*Information Gathering*)**

Με την ολοκλήρωση της ανάλυσης της συγκεκριμένης εφαρμογής APK το MobSF εμφάνισε τα παρακάτω αποτελέσματα μαζί με τις πληροφορίες του πακέτου που δημιουργήθηκε από το Metasploit.



Εικόνα 13: MobSF Dashboard

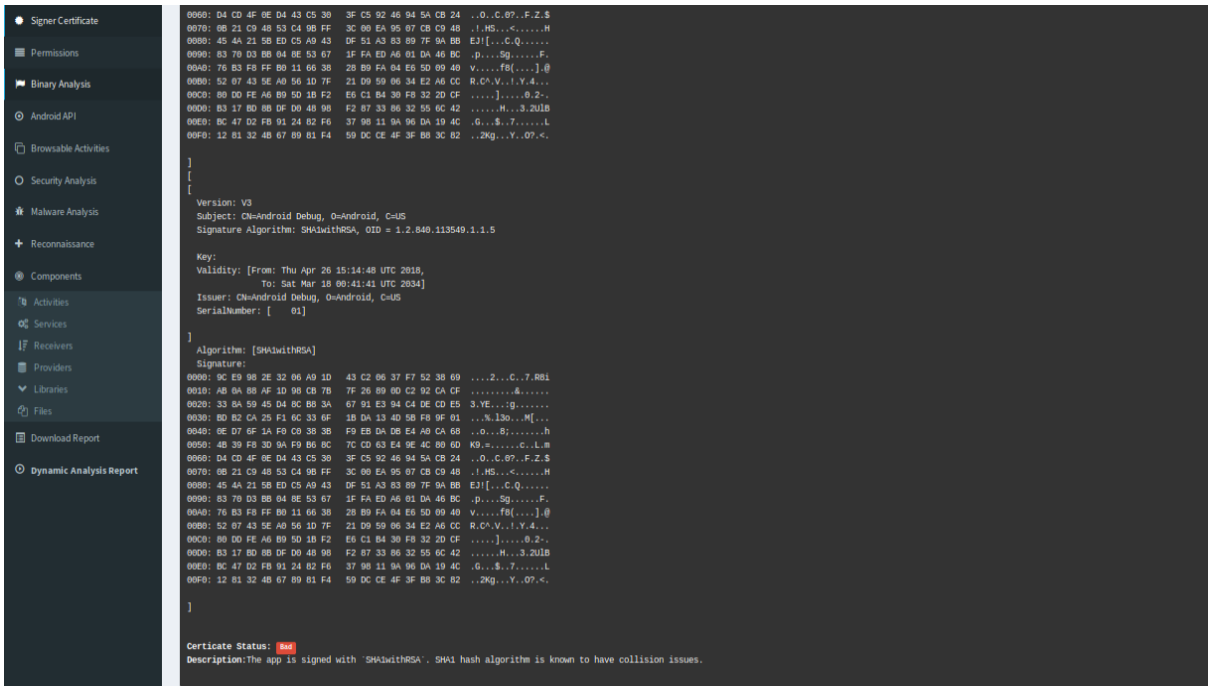
Γίνεται γνωστό, λοιπόν ότι μέσω του MobSF Framework ένας ερευνητής μπορεί να ανακαλύψει εάν ένα αρχείο το οποίο έχει μια default ονομασία στο κινητό έχει εγκατασταθεί για κακόβουλους σκοπούς, ήδη από την αρχική ανάλυση του εκάστοτε APK αρχείου.

Η αρχική ανάλυση του εργαλείου αποτελεί την *στατική ανάλυση* της εφαρμογής που χρησιμοποιήθηκε στα πλαίσια της συγκεκριμένης διπλωματικής εργασίας.

2. **Στατική ανάλυση: Πιστοποιητικό υπογράφοντος (*Signer Certificate*)**

Τα πιστοποιητικά υπογραφόντων εγκαθιδρύουν τη σχέση εμπιστοσύνης πάνω σε πρωτόκολλο επικοινωνίας SSL. Χάρη σε αυτά μπορεί κανείς να αποσπάσει το κομμάτι του υπογράφοντος ενός προσωπικού πιστοποιητικού από μια θυρίδα κλειδιών και στη συνέχεια να προσθέσει το πιστοποιητικό υπογράφοντος σε άλλες θυρίδες.

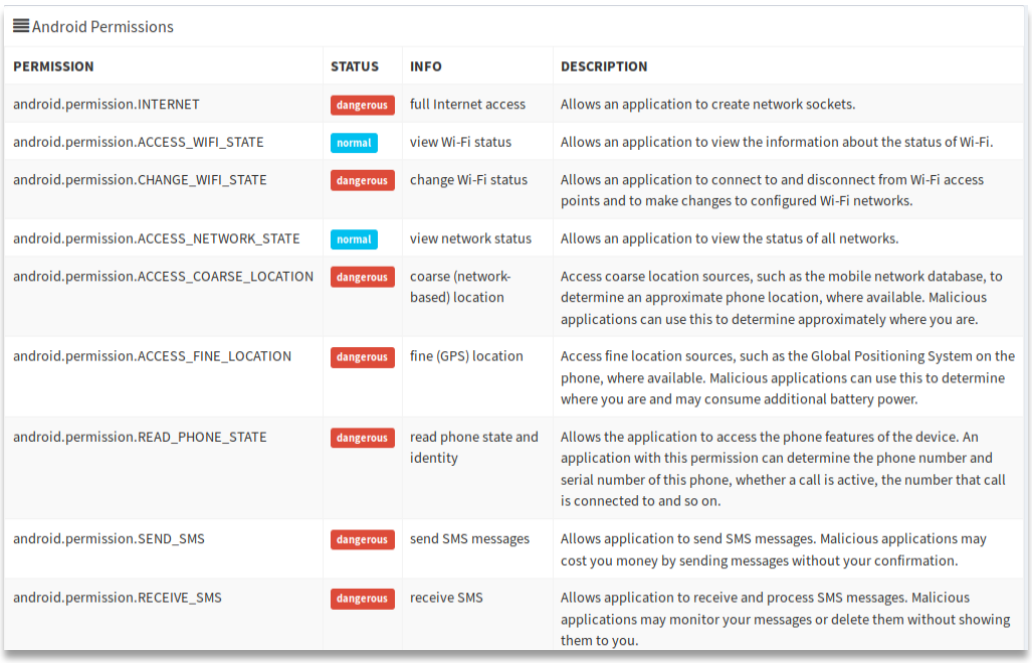
Στο παράδειγμα μας παρατηρείται ότι η εφαρμογή εμπεριέχει πιστοποιητικό στο οποίο ο υπογράφων της εφαρμογής χρησιμοποίησε κρυπτογράφηση SHA1 η οποία είναι γνωστή για τα collisions των συναρτήσεων κατακερματισμού της (*hash functions*).



Εικόνα 14: MOBSF signature analysis

3. **Στατική ανάλυση: Ανάλυση Δικαιωμάτων και αδειών μιας εφαρμογής APK μέσω του MobSF**

Συνεχίζοντας την ανάλυση της παραπάνω εφαρμογής που χρησιμοποιήθηκε για πρακτική άσκηση πάνω στο περιβάλλον του MobSF ένας ερευνητής μπορεί να ανακαλύψει τα δικαιώματα της εφαρμογής και την αντίστοιχη πληροφορία που εξουσιοδοτούνται από τον χρήστη καθώς και την επικινδυνότητα αυτών των δικαιωμάτων. Στο παράδειγμα μας το κακόβουλο αρχείο που έχει δημιουργηθεί για απομακρυσμένη πρόσβαση στη συσκευή μπορεί να παρέχει πλήρη πρόσβαση σε έναν απομακρυσμένο χρήστη, μπορεί να δώσει την άδεια σε οποιοδήποτε να τροποποιήσει το Wi-Fi status, μπορεί να δώσει πληροφορίες τοποθεσίας, να στείλει SMS σε έναν απομακρυσμένο χρήστη κλπ. Φυσικά πολλά από αυτά τα αποτελέσματα μπορεί να είναι αδιάφορα για το σκοπό της δημιουργίας της κάθε εφαρμογής ενώ δεν αποκλείεται κάποια από αυτά να αποτελούν και «λάθος συναγερμό» (false positive).



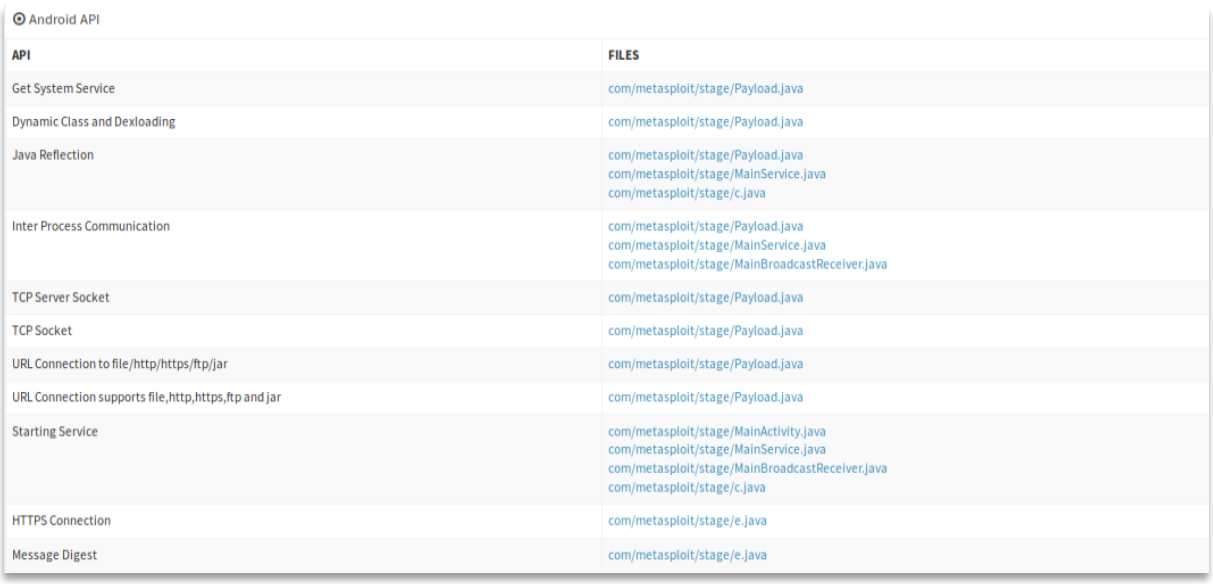
Android Permissions

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	dangerous	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.

Εικόνα 15: Στατική Ανάλυση στο MobSF

4. **Στατική ανάλυση: Περιβάλλον εφαρμογής Android (*Android API*)**

Σε αυτή την ενότητα το εργαλείο MobSF αναλύει όλες τις API υπηρεσίες που αποτελούν την εφαρμογή που αναλύεται. Στο παράδειγμά μας η εφαρμογή system.apk περιλαμβάνει τις ακόλουθες υπηρεσίες API.



Android API

API	FILES
Get System Service	com/metasploit/stage/Payload.java
Dynamic Class and Dexloading	com/metasploit/stage/Payload.java
Java Reflection	com/metasploit/stage/Payload.java com/metasploit/stage/MainService.java com/metasploit/stage/c.java
Inter Process Communication	com/metasploit/stage/Payload.java com/metasploit/stage/MainService.java com/metasploit/stage/MainBroadcastReceiver.java
TCP Server Socket	com/metasploit/stage/Payload.java
TCP Socket	com/metasploit/stage/Payload.java
URL Connection to file/http/https/ftp/jar	com/metasploit/stage/Payload.java
URL Connection supports file,http,https,ftp and jar	com/metasploit/stage/Payload.java
Starting Service	com/metasploit/stage/MainActivity.java com/metasploit/stage/MainService.java com/metasploit/stage/MainBroadcastReceiver.java com/metasploit/stage/c.java
HTTPS Connection	com/metasploit/stage/e.java
Message Digest	com/metasploit/stage/e.java

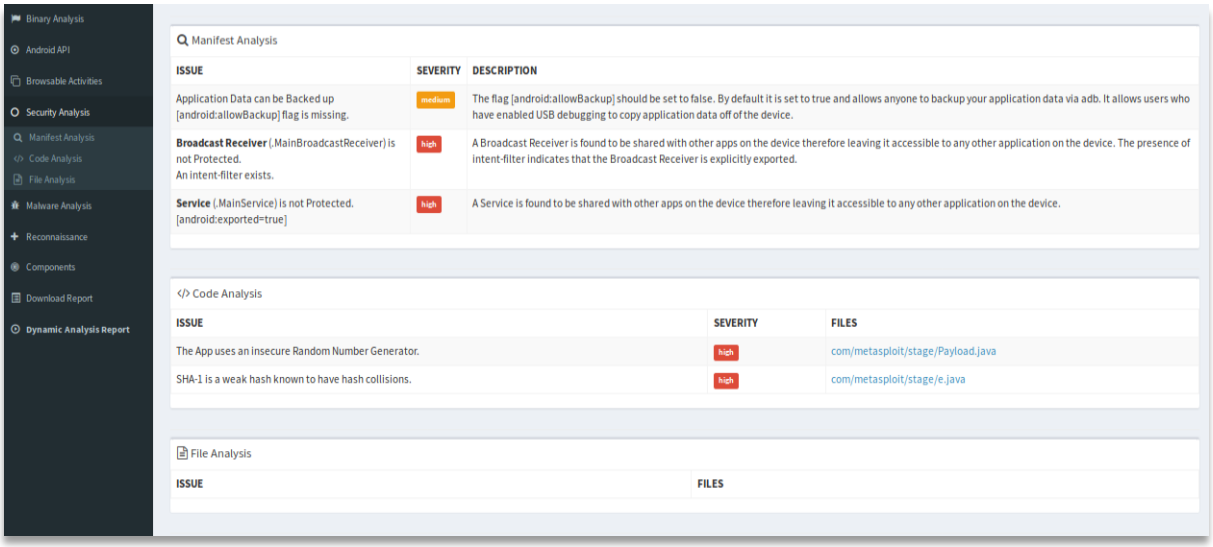
Εικόνα 16: Υπηρεσίες APIτης εφαρμογής

5. **Στατική ανάλυση: Ανάλυση ασφάλειας της εφαρμογής system.apk**

Η ανάλυση μιας εφαρμογής στο εργαλείο MobSF διασπάται σε 3 μέρη την «Προφανή Ανάλυση» (Manifest Analysis), την Ανάλυση Κώδικα (*Code Analysis*) και την Ανάλυση Αρχείου (*File Analysis*).

Στο παράδειγμα της άσκησης η Προφανής Ανάλυση της εφαρμογής system.apk φανέρωσε 3 ζητήματα προς παρακολούθηση τα οποία αφορούσαν την ασφάλεια της εφαρμογής, ενώ η ανάλυση κώδικα φανέρωσε ότι η εν λόγω εφαρμογή χρησιμοποιεί μια ανασφαλής γεννήτρια τυχαίων αριθμών και

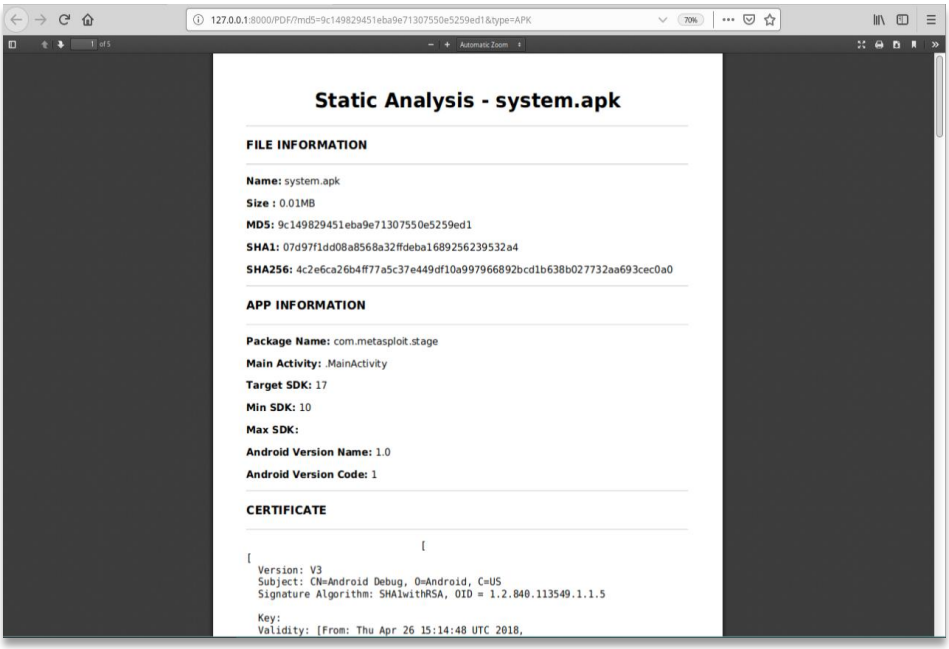
επιβεβαίωσε την επικινδυνότητα της χρήσης SHA1 σε θέματα collision που φανερώθηκαν ήδη από την ανάλυση πιστοποιητικού της εφαρμογής. Τέλος κατά την ανάλυση κώδικα της εφαρμογής γίνονται αντιληπτά και τα java αρχεία που αποτελούν την αιτία των ζητημάτων αυτών. Παρακάτω φαίνονται τα αποτελέσματα ύστερα από την ανάλυση της εφαρμογής system.apk.



Εικόνα 17: Ανάλυσης ασφάλειας του αρχείου

6. **Στατική ανάλυση: Έντυπο αναφοράς (*Reporting*)**

Το περιβάλλον του εργαλείου MobSF παρέχει επίσης την δυνατότητα εξαγωγής ενός επίσημου εγγράφου αναφοράς από τα αποτελέσματα που προέκυψαν κατά την έρευνα. Στο παράδειγμα της παρακάτω εικόνες φαίνεται η εξαγωγή των αποτελεσμάτων από το system.apk σε μορφή PDF. Θα πρέπει να σημειωθεί ότι για τη διεξαγωγή της φόρμας θα πρέπει να έχει εγκατασταθεί το εργαλείο *wkhtmltopdf*. Σε συστήματα windows το εργαλείο wkhtmltopdf μπορεί να ληφθεί από το διαδίκτυο[27] ενώ σε συστήματα Linux μπορεί να ληφθεί χρησιμοποιώντας την εντολή "***sudo apt-get install wkhtmltopdf***".

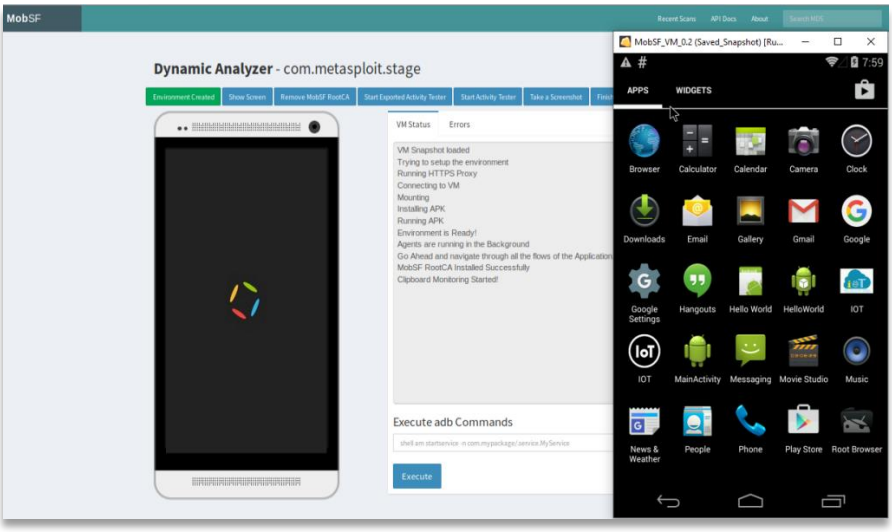


Εικόνα 18: Έντυπο Αναφοράς του MobSF

7. **Δυναμική Ανάλυση του MobSF (*Dynamic Analysis*)**

Παρακάτω μπορεί να γίνει επίσης υναμική ανάλυση είτε μέσω Κινητής Συσκευής είτε μέσω VM περιβάλλοντος Κινητής Συσκευής android την οποία παραχωρεί το εργαλείο στη σελίδα του.

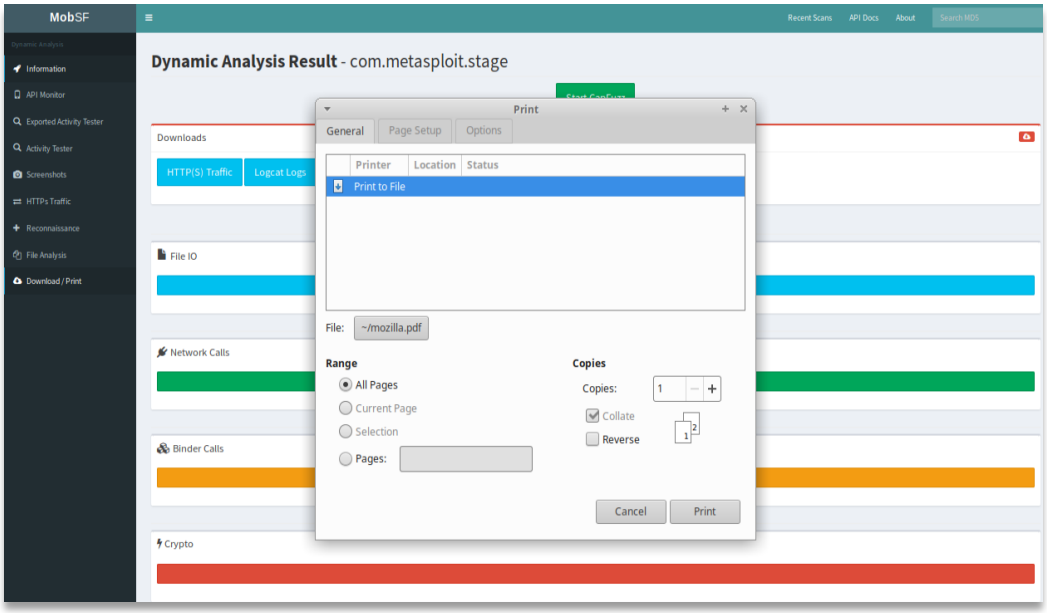
Η Δυναμική Ανάλυση περιλαμβάνει διάφορες επιπλέον δυνατότητες αφού τροποποιηθεί κατάλληλα ακολουθώντας τις οδηγίες συγχρονισμού του VM με το εργαλείο, μεταξύ άλλων την ενεργοποίηση δοκιμής των δραστηριοτήτων της εφαρμογής, την λήψη στιγμιότυπων για την συλλογή πειστηρίων για την αναφορά αργότερα κλπ. Για να ξεκινήσει η Δυναμική Ανάλυση θα πρέπει αν συγχρονιστεί το VM με το εικονικό περιβάλλον του εργαλείου MobSF και στη συνέχεια ο ερευνητής μπορεί να παρατηρήσει ότι στο Android VM δοκιμάζεται η εφαρμογή που χρησιμοποιείται κατά την ανάλυση.



Εικόνα 19: Περιβάλλον Δυναμικής Ανάλυσης στο MobSF

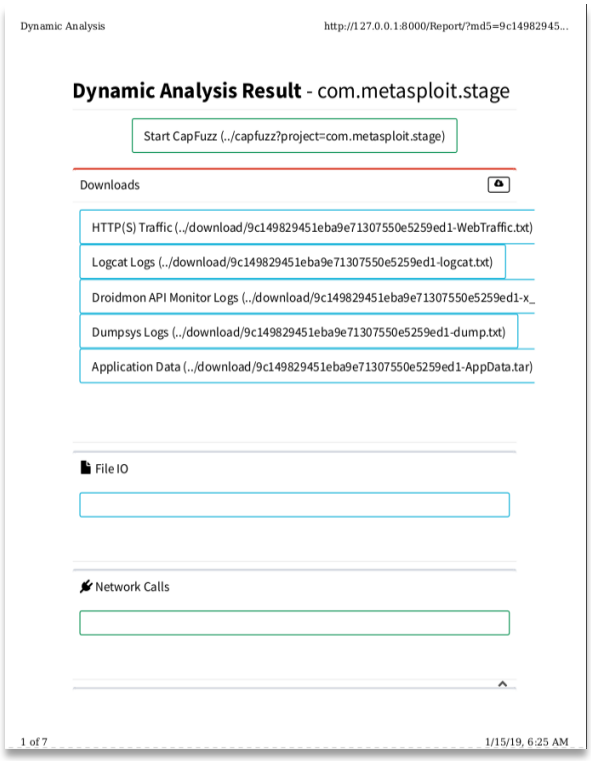
8. **Δυναμική Ανάλυση: Έντυπο αναφοράς (*Reporting*)**

Το εργαλείο MobSF μπορεί να παρέχει και μια λεπτομερή αναφορά τύπου PDF της δυναμικής ανάλυσης που εκτελείται για την εν λόγω εφαρμογή ενώ παράλληλα αποθηκεύει το εν λόγω αρχείο στη τοποθεσία που θα επιλέξει ο χρήστης από το GUI του εργαλείου.



Εικόνα 20: Δημιουργία Αναφοράς σε PDF

Η αναφορά του εργαλείου για τη συγκεκριμένη εφαρμογή φαίνεται στο παρακάτω στιγμιότυπο:

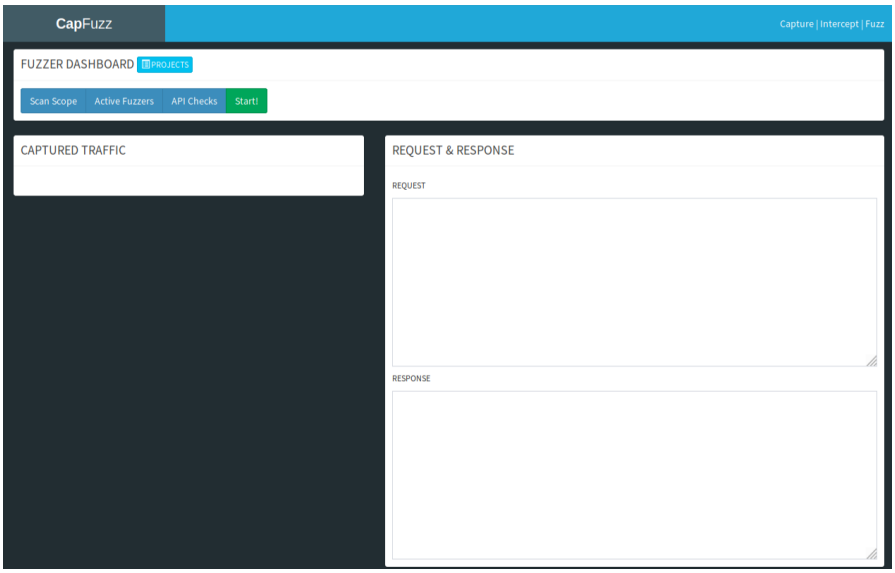


Εικόνα 21: Αναφορά μορφής PDF

9. Άλλες λειτουργίες του MobSF

Το εργαλείο MobSF εκτός από τις δυνατότητες που αναφέρθηκαν παραπάνω μπορεί και να χρησιμοποιηθεί και σε περιπτώσεις Δοκιμών Διείσδυσης καθώς μπορεί να ανιχνεύσει αν μια εφαρμογή είναι ευπαθής σε επιθέσεις SSRFCSRF, XSS κλπ.

Για να εκτελέσει μια τέτοια ενέργεια χρησιμοποιείται το ενσωματωμένο εργαλείο CapFuzz το οποίο έχει τη δυνατότητα ανίχνευσης των συγκεκριμένων επιθέσεων.



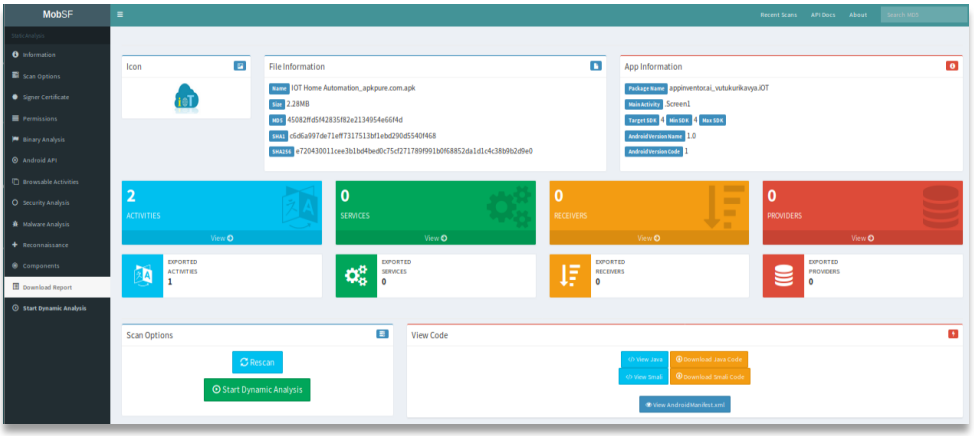
Εικόνα 22: Εργαλείο ανίχνευσης αδυναμιών

5.1.2. Περίληψη Σεναρίου

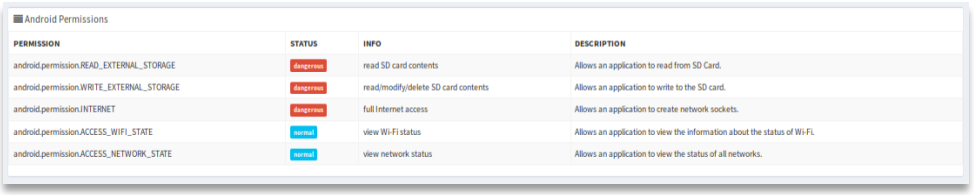
Ο κύριος Α. Δουλεύει ως Senior Developing Manager στην ανώνυμη εταιρία ΧΥ.ΑΕ που στηρίζεται σε 3 εργαζόμενους τον Β τον Γ και τον Δ. Προκειμένου να φέρει εις πέρας ένα μεγάλο έργο πάνω σε συστήματα IoT εμπιστεύθηκε το πλάνο σχεδίου αυτό στον έμπιστο συνάδελφο του κύριο Β ο οποίος δουλεύει εδώ και 15 χρόνια στην εταιρία. 1 μήνα πριν τη δημοσίευση του έργου αυτού στο ευρύ κοινό ο κύριος Α διαπίστωσε ότι η εταιρία Ζ έχει ήδη δημοσιεύσει το έργο αυτό το οποίο και είναι πανομοιότυπο με τα σχέδια της εταιρίας ΧΥ. Ψάχνοντας να βρεθεί μια άκρη με το τι έγινε ο κύριος Α και λαμβάνοντας υπόψη ότι ο χρήστης Γ είναι νέος στην επιχείρηση εδώ και 3 μήνες υποψιάζεται ότι μπορεί να ενέργησε εις βάρος της επιχείρησης ΧΥ για όφελος της ανταγωνίστριας επιχείρησης Ζ. Ζητάει το επιχειρησιακό κινητό του χρήστη Β τον οποίο εμπιστεύεται για να εκτελέσει έρευνα Ψηφιακής Εγκληματολογίας πάνω στη rooted Κινητή Συσκευή του χρήστη Β κατόπιν της συγκατάθεσης του για αυτή την ενέργεια στο Linux μηχάνημα του χρησιμοποιώντας το εργαλείο MobSF.

Διαδικασία που ακολουθήθηκε:

Χρησιμοποιώντας το GUI του εργαλείου τοπικά στο Linux μηχάνημα που έχει για τη διαδικασία Ψηφιακής Έρευνας και Ανάλυσης επισκέπτεται την διεύθυνση 127.0.0.1:8000 στην οποία παρουσιάζεται η παρακάτω επιλογή για ανάλυση εφαρμογών κινητού τύπου APK. Κατά την έρευνα ο κύριος Α διαπίστωσε ότι έχει ληφθεί πρόσφατα μια εφαρμογή που ονομάζεται *IoT.apk*. Η εφαρμογή αυτή έχει ήδη εγκατασταθεί στο κινητό. Ο κύριος Α ρωτώντας τον χρήστη Β για την εφαρμογή διαπιστώνει ότι ο χρήστης Γ έχει προτείνει στον χρήστη Β να κατεβάσει την εν λόγω εφαρμογή από μια σελίδα που εκείνος του πρότεινε με σκοπό να τον βοηθήσει να ρυθμίσει κάποιες συσκευές στο σπίτι του. Ψάχνοντας την εφαρμογή στο Internet ο χρήστης Α ανακαλύπτει πως υπάρχει στη πραγματικότητα αυτή η εφαρμογή και κατεβάζοντας την και εξετάζοντας την ανακαλύπτει πως η εφαρμογή παρέχει 2 σημαντικές δραστηριότητες (Activities) στο χρήστη που μπορεί να αποβούν επικίνδυνες. Αυτές οι υπηρεσίες περιλαμβάνουν άδεια για πλήρη πρόσβαση στο Διαδίκτυο, εγγραφή Δεδομένων της εφαρμογής στην κάρτα SD αλλά και ανάγνωση των περιεχομένων της κάρτας SD.



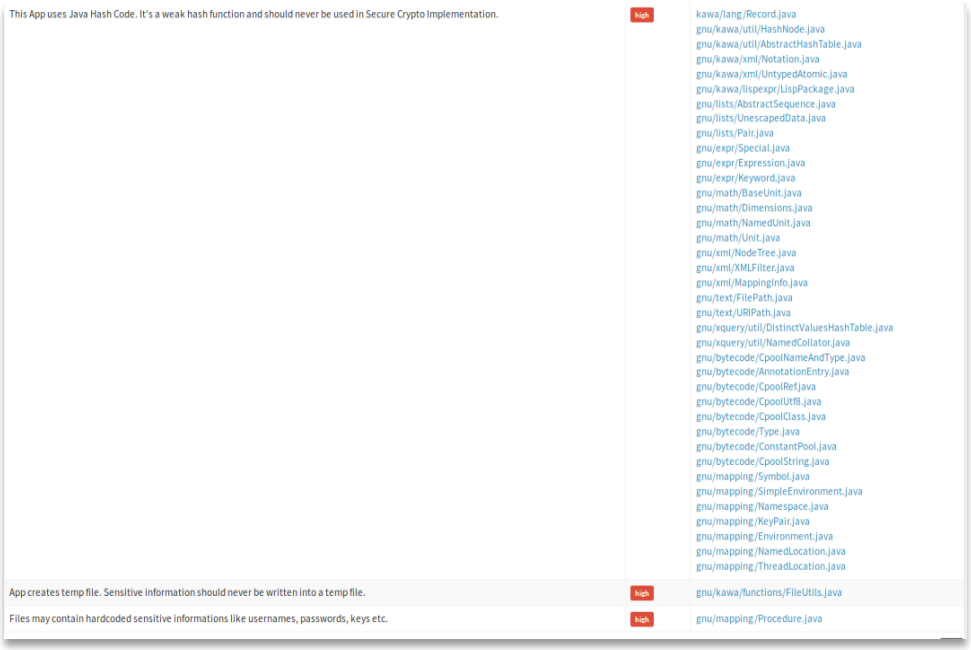
Εικόνα 23: Πληροφορίες της αυθεντικής εφαρμογής



Εικόνα 24: Πληροφορίες δικαιωμάτων χρήστη στην εφαρμογή

Παράλληλα κατά τη διαδικασία εξαγωγής της αναφοράς από το εργαλείο στη καρτέλα «Code Analysis» ο κύριος Α παρατηρεί ότι η συγκεκριμένη εφαρμογή χρησιμοποιεί πολύ χαμηλή ασφάλεια σε ότι αφορά τη κρυπτογράφηση των δεδομένων στην υλοποίηση της ενώ παράλληλα δημιουργεί προσωρινό αρχείο

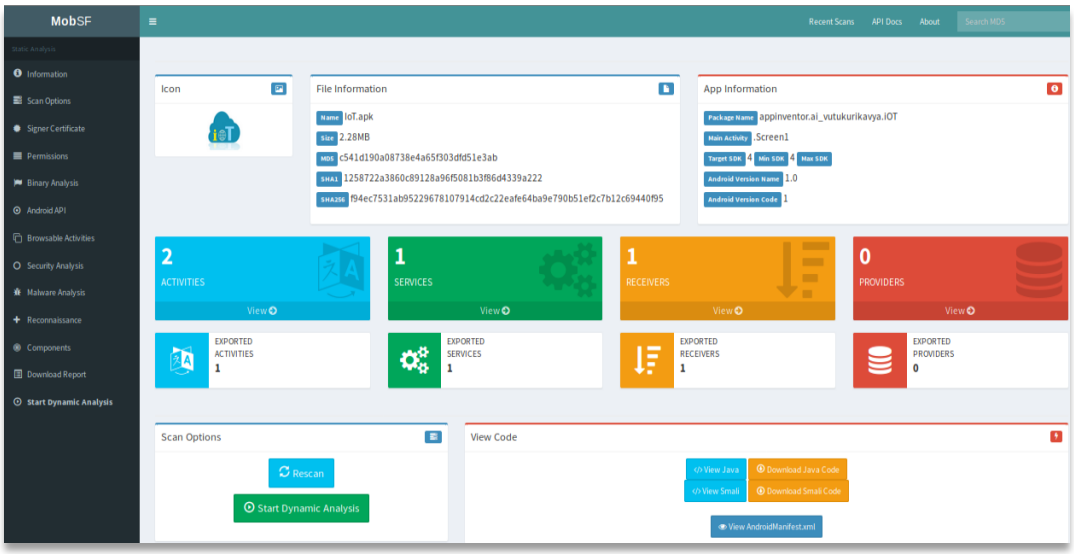
για την εγγραφή των ενεργειών του χρήστη το οποίο μπορεί να περιλαμβάνει κωδικούς πρόσβασης ταυτότητα χρήστη στην εφαρμογή κλπ.



Εικόνα 25: Ανάλυση μερών κώδικα της εφαρμογής

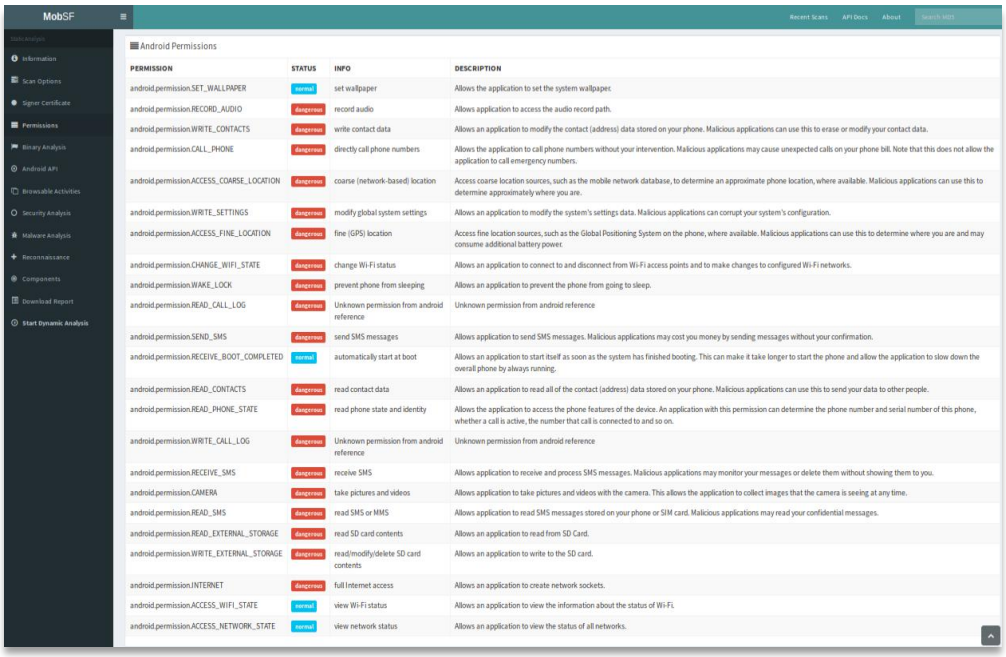
Συνεπώς η συγκεκριμένη εφαρμογή από μόνη της καθίσταται επικίνδυνη σε περιπτώσεις που το κινητό λειτουργεί σε επιχειρησιακό περιβάλλον.

Εξετάζοντας όμως και την εφαρμογή που έχει κατεβάσει ο χρήστης Β ανακαλύπτει μέσω του MobSF ότι η εφαρμογή αυτή διαφέρει από την αυθεντική εφαρμογή του δημιουργού. Το MobSF έδειξε τα παρακάτω αποτελέσματα:



Εικόνα 26: Πληροφορίες κακόβουλης εφαρμογής

Κατά την ανάλυση της ύποπτης εφαρμογής διαπιστώνεται λοιπόν ότι η εφαρμογή αναμφίβολα έχει τροποποιηθεί, λόγω αδύναμης ασφάλειας, με σκοπό την διαρροή κρίσιμων δεδομένων από τη συσκευή του χρήστη.



Εικόνα 27: Δικαιώματα χρήστη στην κακόβουλη εφαρμογή

Με την ολοκλήρωση της δημιουργίας της αναφοράς από το συγκεκριμένο εργαλείο, ο κύριος Α αποθηκεύει τα ευρήματα του, τα οποία πλέον αποτελούν πειστήρια στη συγκεκριμένη υπόθεση.

5.2. Η διανομή Santoku

Η διανομή Ψηφιακής Εγκληματολογίας Santoku είναι μια ελεύθερη διανομή ανοιχτής πηγής αφιερωμένη στην Ψηφιακή Έρευνα, Ανάλυση και Ασφάλεια Κινητών Συσκευών και εφαρμογών. Αποτελείται από ένα Linux γραφικό περιβάλλον με προεγκατεστημένα εργαλεία SDK, προγράμματα οδήγησης, προεγκατεστημένα εργαλεία με έτοιμα γραφικά περιβάλλοντα, όπως το PyGTK, το Autopsy κ.λπ. Παράλληλα εμπεριέχει εργαλεία για την ανάπτυξη και τον έλεγχο των εφαρμογών για Κινητές Συσκευές και για την αυτόματη ανίχνευση και εγκατάσταση τους σε νέες συνδεδεμένες Κινητές Συσκευές.

Το Santoku περιέχει εργαλεία για την Ψηφιακή Ανάκτηση και Ανάλυση δεδομένων, καθώς και εργαλεία που χρησιμοποιούνται για «firmware flashing» (αναβάθμιση λειτουργικού χρησιμοποιώντας ειδική παραμετροποίηση μέσω υπολογιστή) ποικίλλων λειτουργικών, εργαλεία απεικόνισης για NAND, κάρτες πολυμέσων (media cards) και μνήμη RAM, free εκδόσεις ορισμένων εμπορικών εργαλείων εγκληματολογικής ανάλυσης, και σεναρίων και υπηρεσιών κοινής ωφέλειας συγκεκριμένα σχεδιασμένων για Ψηφιακή Έρευνα και Ανάλυση. Επιπλέον, περιλαμβάνει εργαλεία για την εξέταση κακόβουλου λογισμικού για κινητά, εξομοιωτές Κινητής Συσκευής, βοηθητικές εφαρμογές για την προσομοίωση υπηρεσιών δικτύου για Δυναμική Ανάλυση, εργαλεία Αντίστροφης Μηχανικής (Reverse Engineering) και πρόσβαση σε βάσεις δεδομένων κακόβουλου λογισμικού.

Όσον αφορά την Ψηφιακή Έρευνα και Ανάλυση σε Κινητές Συσκευές στην οποία και επικεντρώνεται αυτή η διπλωματική εργασία, το Santoku περιλαμβάνει τα παρακάτω εργαλεία:

- AFLogical Open Source Edition ή AFLogical-OSE
- Android Encryption Brute Force
- BlackBerry Desktop Manager
- iPhone BackupAnalyzer
- ExifTool,
- libimobiledevice
- scalpel
- Autopsy TSK (The Sleuth Kit)
- SQLiteSpy

Στο πρακτικό κομμάτι της επικείμενης διπλωματικής εργασίας θα γίνει χρήση των εργαλείων Ψηφιακής Ανάκτησης και Ανάλυσης AFLogical-OSE, scalpel και Autopsy TSK.

Εκτός από τα εργαλεία Ψηφιακής Εκληματολογίας το Santoku περιλαμβάνει και εργαλεία Ασφαλείας που μπορούν να χρησιμοποιηθούν από αναλυτές ασφάλειας κατά τη διάρκεια μιας Δοκιμής Διείσδυσης. Τα εργαλεία που φαίνονται παρακάτω μπορούν να υποστηρίξουν και δυνατότητες ανάλυσης ασύρματης επικοινωνίας Wi-Fi, Αντίστροφης Μηχανικής και δοκιμών Διείσδυσης.

- nmap
- BurpSuite
- Metasploit
- w3af Console
- Ettercap
- SQLmap
- SSLstrip

Τέλος το Santoku περιλαμβάνει και εργαλεία που χρησιμοποιούνται για Αντίστροφη Μηχανική όπως το APK Tool Flawfinder και το Java Decompiler καθώς και δικτύου όπως το Wireshark και το Kismet για Wi-Fi Penetration Testing και σε επίπεδο πακέτων κινητής τηλεφωνίας το ChaosReader.

Το πειραματικό κομμάτι για τη διανομή Santoku περιλαμβάνει την χρήση των εργαλείων AFLogical-OSE, Scalpel και Autopsy TSK τα οποία χρησιμοποιούνται σε πραγματικό περιβάλλον από ερευνητές Ψηφιακής Εγκληματολογίας για την λογική και φυσική ανάκτηση και απόσπαση δεδομένων με «σωστό και ασφαλή τρόπο Ψηφιακής Έρευνας και Ανάλυσης» (Forensically Sound).

Ξεκινώντας λοιπόν αρχικά έγινε εγκατάσταση του Santoku.iso το οποίο ελήφθη από την επίσημη ιστοσελίδα της Santoku και στη συνέχεια τροποποιώντας τον χρήστη του συστήματος στο να παρέχονται πλήρη δικαιώματα για τυχόν τροποποιήσεις που μπορεί να χρειαστούν έγινε εκκίνηση της διανομής χρησιμοποιώντας το εικονικό περιβάλλον του VirtualBox της Oracle [5].

Εικόνα 28: Το περιβάλλον Santoku

5.2.1. Το εργαλείο AFLogical-OSE

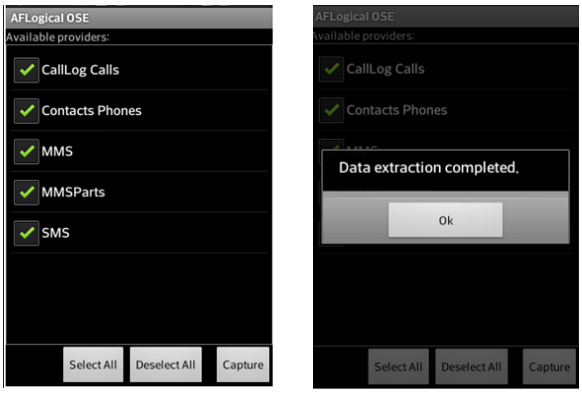
Το εργαλείο AFLogical-OSE επιτρέπει σε έναν ερευνητή Ψηφιακής Εγκληματολογίας να αποσπάσει τις κλήσεις μέσω του αρχείου καταγραφής κλήσεων, τα τηλέφωνα των επαφών και τα μηνύματα MMS και SMS από Κινητές Συσκευές τύπου Android χωρίς να χρειάζεται να υπάρχει πλήρη πρόσβαση με δικαιώματα root στη συσκευή. Το AFLogical-OSE χρησιμοποιείται μόνο για «Λογική Εξαγωγή» (Logical Extraction) πληροφοριών από μια Κινητή Συσκευή και σε καμία περίπτωση δεν μπορεί να ανακτήσει αρχεία συστήματος ή διαγεγραμμένα αρχεία από τη συσκευή. Το πλήρες λογισμικό AFLogical-OSE μπορεί να βρεθεί ενσωματωμένο στη διανομή του Santoku αλλά και διανέμεται δωρεάν από την επίσημη ιστοσελίδα της NowSecure στους ερευνητές και σε αυτούς που επιβάλλουν τον νόμο [16].

Στην επικείμενη διπλωματική εργασία, το AFLogical-OSE χρησιμοποιήθηκε για να αποσπάσει τυχόν ευρήματα, χρησιμοποιώντας τη μέθοδο Λογικής Εξαγωγής, από μια Κινητή Συσκευή Android P10 Lite. Η διαδικασία Λογικής Εξαγωγής στοιχείων από την εικόνα του κινητού μπορεί να συμπτυχθεί στα παρακάτω:

- ✓ Σύνδεση της Κινητής Συσκευής στον υπολογιστή του ερευνητή και στο Santoku
- ✓ Επιλογή σύνδεσης MTP

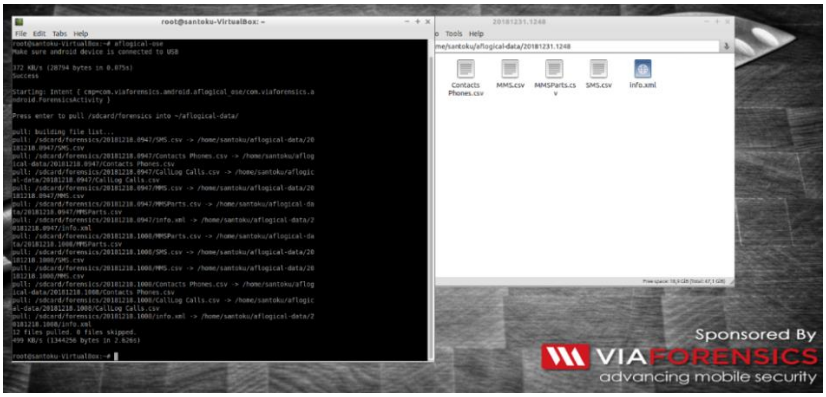
- ✓ Ενεργοποίηση Εντοπισμού σφαλμάτων USB από τις ρυθμίσεις της συσκευής
- ✓ Εκτέλεση της εντολής AFLogical-OSE

Με το που τελειώσει η εγκατάσταση του agent του εργαλείου στη συσκευή εμφανίζεται το παρακάτω παράθυρο επιλογής απόσπασης πληροφοριών από το κινητό τηλέφωνο:

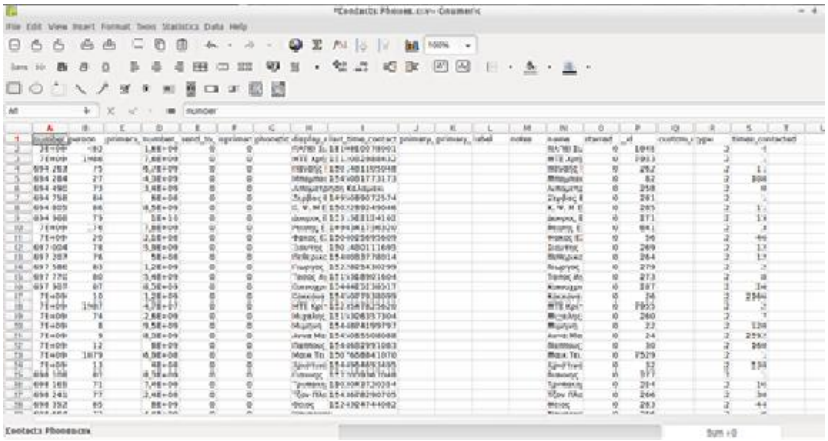


Εικόνα 29: Διαδικασία εξαγωγής δεδομένων χρησιμοποιώντας το εργαλείο AFLogical-OSE

Επιλέγοντας «*Capture*» από τη Κινητή Συσκευή δημιουργείται τοπικά ένας φάκελος που ονομάζεται *aflogical-data* ο οποίος εμπεριέχει τα λογικά ευρήματα σε μορφή CSV (Excel) που αποκτήθηκαν κατά την διαδικασία εκτέλεσης του εργαλείου με χρονική ταξινόμηση. Στο παράδειγμα της άσκησης τα αποτελέσματα και η διαδικασία της απόκτησης των λογικών ευρημάτων φαίνοται στο παρακάτω στιγμιότυπο.



Εικόνα 30: Εκτέλεση του εργαλείου AFLogical-OSEκαι ανάκτηση δεδομένων



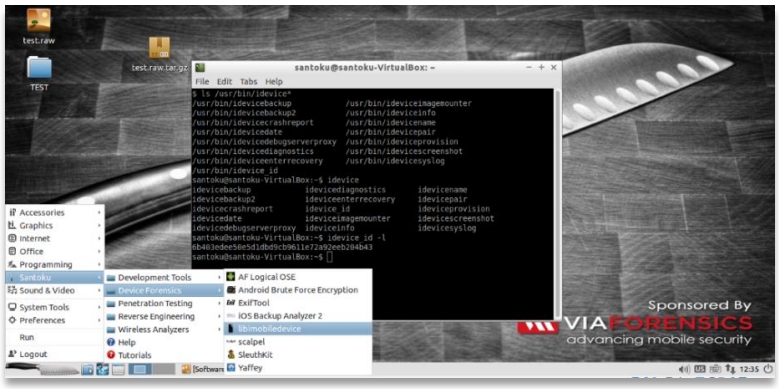
Εικόνα 31: Ανάκτηση τηλεφωνικών αριθμών και δεδομένων τηλεφώνου

5.2.2. Το εργαλείο Libimobiledevice

Ένα άλλο εργαλείο το οποίο βρίσκεται ενσωματωμένο μέσα στη διανομή Santoku και χρησιμοποιείται και αυτό για λογική ανάκτηση δεδομένων αλλά σε iOS Κινητές Συσκευές είναι το εργαλείο libimobiledevice.

Το εργαλείο libimobiledevice είναι μια βιβλιοθήκη λογισμικού πολλαπλών πλατφορμών που αφορά πρωτόκολλα που υποστηρίζουν συσκευές iPhone, iPod Touch, iPad και Apple TV. Σε αντίθεση με άλλα εργαλεία, δεν εξαρτάται από τη χρήση οποιασδήποτε υπάρχουσας ιδιόκτητης βιβλιοθήκης και δεν απαιτεί Jailbreaking. Επιτρέπει σε άλλο λογισμικό να αποκτά εύκολα πρόσβαση στο σύστημα αρχείων της συσκευής, να ανακτά πληροφορίες σχετικά με τη συσκευή και εσωτερικά, να κρατάει backup της συσκευής, να διαχειρίζεται τα εικονίδια SpringBoard, να διαχειρίζεται εγκατεστημένες εφαρμογές, να ανακτά το βιβλίο διευθύνσεων, το ημερολόγιο του χρήστη, τις σημειώσεις του, τους σελιδοδείκτες ιστού και χρησιμοποιώντας τη βιβλιοθήκη libgpod τα βίντεο της συσκευής. Το εργαλείο βρίσκεται σε εξέλιξη από τον Αύγουστο του 2007 με στόχο να υποστηρίξει αυτές τις συσκευές στην επιφάνεια εργασίας Linux λειτουργικών.

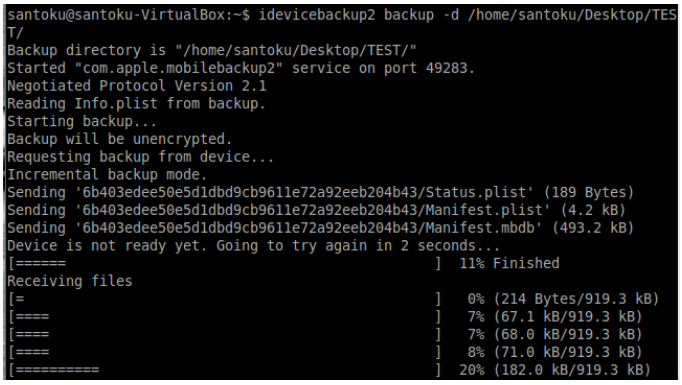
Πρακτικά, επιλέγοντας το libimobiledevice εμφανίζονται στο χρήστη όλες οι εντολές που είναι ενσωματωμένες στο συγκεκριμένο εργαλείο σε νέο παράθυρο τερματικού. Για τη συγκεκριμένη διπλωματική εργασία χρησιμοποιήθηκαν μόνο οι εντολές ***idevice_id*** και ***idevicebackup2***.



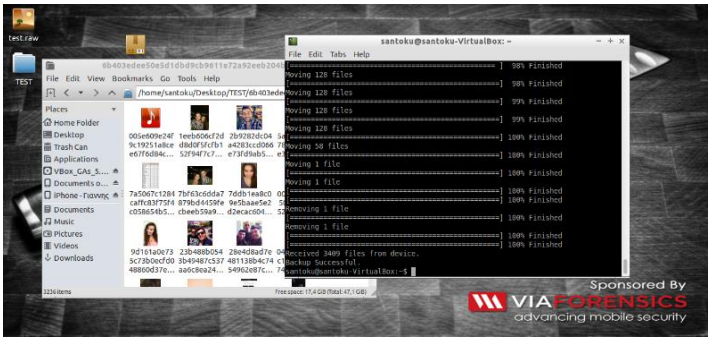
Εικόνα 32: Εκτέλεση εργαλείου libimobiledevice στη διανομή Santoku

Για να ανακτήσει δεδομένα από μια iOS συσκευή χρησιμοποιώντας το συγκεκριμένο πρόγραμμα, ο χρήστης μπορεί να επιλέξει την εντολή idevicebackup ή idevicebackup2 η οποία δημιουργεί σε μια νέα φυσική διεύθυνση του συστήματος ένα φάκελο με τα ανακτημένα αρχεία της Κινητής Συσκευής. Προκειμένου να εκτελεστεί η συγκεκριμένη εντολή θα πρέπει η Κινητή Συσκευή να είναι ορατή στο Santoku και παράλληλα να είναι ξεκλείδωτη στο χρήστη (χωρίς κωδικό, κλειδωμένο pattern κλπ.). Δεν απαιτείται το κινητό να είναι Jailbroken. Μέσω των ρυθμίσεων ο χρήστης μπορεί να απενεργοποιήσει το αυτόματο κλείδωμα για να αποφύγει τυχόν σφάλματα κατά την εκτέλεση της διαδικασίας ανάκτησης δεδομένων από τη Κινητή Συσκευή.

Εκτελώντας λοιπόν την εντολή ***idevice_id -l*** ο χρήστης μπορεί να δει τη ταυτότητα της συνδεδεμένης συσκευής εφόσον η συσκευή έχει συνδεθεί με επιτυχία στο Santoku. Έπειτα εκτελώντας την εντολή ***idevicebackup2*** το εργαλείο εμφανίζει τα παρακάτω αποτελέσματα στην επιθυμητή φυσική διεύθυνση που θα πληκτρολογήσει ο χρήστης.



Εικόνα 33: Ανάκτηση δεδομένων συσκευής



Εικόνα 34: Αποθήκευση δεδομένων συσκευής

Τέλος να σημειωθεί ότι το εργαλείο libimobiledevice χρησιμοποιείται μόνο για λογική ανάκτηση δεδομένων και όχι συστήματος ή φυσική ανάκτηση και μπορεί να ληφθεί από την επίσημη σελίδα[21] του ή από τη σελίδα του δημιουργού του στο GitHub[17].

5.2.3. Το εργαλείο Scalpel

Το Scalpel είναι ένα open source εργαλείο για την ανάκτηση των διαγραμμένων δεδομένων που αρχικά βασίστηκαν κυρίως, αν και σημαντικά πιο αποδοτικά. Αναπτύχθηκε από τον Golden G. Richard και παρουσιάστηκε στο συνέδριο του DFRWS το 2005. Επί του παρόντος, το Scalpel ενσωματώνεται στο Sleuthkit (TSK) και παράλληλα μπορεί κανείς να το βρει στο GitHub [18].

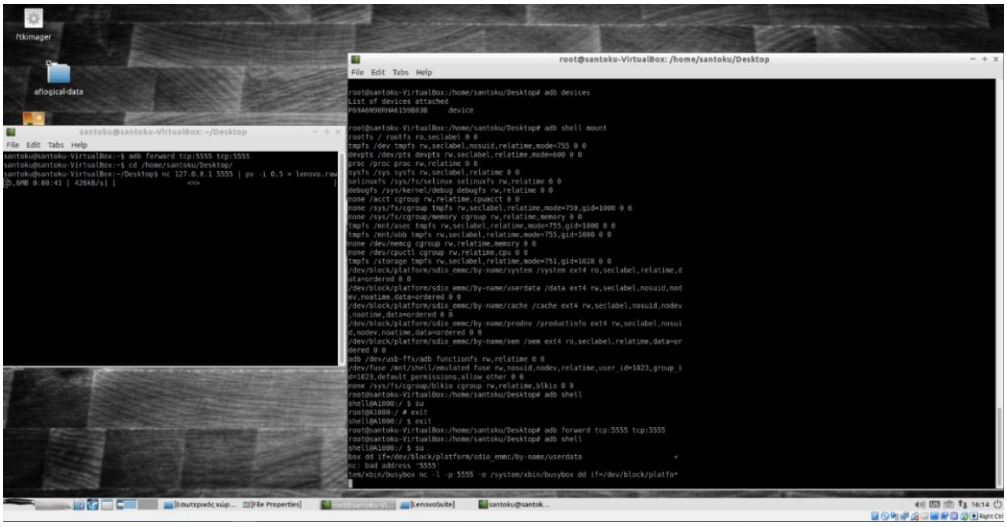
Το Scalpel δίνει τη δυνατότητα σε έναν ερευνητή Ψηφιακής Εγκληματολογίας να καθορίσει εκείνος ποιους τύπους αρχείων θέλει να ανακτήσει από τη συσκευή και για να ανακτήσει τους τύπους των αρχείων αυτών θα πρέπει να τροποποιήσει το αρχείο του προγράμματος που ονομάζεται scalpel.conf. Για να το κάνει αυτό το μόνο που χρειάζεται είναι να ενεργοποιήσει τους τύπους αρχείων που θέλει να εξετάσει αφαιρώντας το σύμβολο της δίεσης από το αρχείο ρύθμισης σε κάθε Header, Footer που χρειάζεται.

Το Scalpel μπορεί να αποσπάσει στοιχεία από μια εικόνα δίσκου μιας Κινητής Συσκευής τύπου raw. Για να αποκτήσει ένας ερευνητής μια τέτοια εικονική αναπαράσταση από ένα κινητό τηλέφωνο υπάρχει η δυνατότητα ανάκτησης αυτής της εικόνας χρησιμοποιώντας το εργαλείο ADB το οποίο είναι ήδη εγκατεστημένο στο Santoku. Η διαδικασία απόκτησης της εικόνας για τη συγκεκριμένη άσκηση μπορεί να συμπτυχθεί στα παρακάτω βήματα που ακολουθούν:

- Παροχή πλήρης πρόσβασης ως root στη Κινητή Συσκευή προς ανάλυση. (Χρήση του KingoRoot και του busybox τα οποία λήφθηκαν από το Playstore της google)
- Επιβεβαίωση σύνδεσης ως διαχειριστής root στη συσκευή μέσω του Santoku και της Κινητής Συσκευής
- Πλήρη Πρόσβαση και φόρτωση της Κινητής Συσκευής χρησιμοποιώντας την εντολή **adb shell mount** και **su**[19]

- Επιλογή του κατάλληλου φακέλου συστήματος για ανάκτηση δεδομένων (Στη περίπτωση της άσκησης λήφθηκε ο φάκελος data που εμπεριέχει όλα τα στοιχεία του χρήστη της συσκευής)
- Προώθηση της δημιουργίας της εικόνας χρησιμοποιώντας την εντολή **adb forward tcp:5555 tcp:5555** στη πόρτα 5555
- Χρήση του προγράμματος **netcat** για την εγκαθίδρυση της επικοινωνίας μεταξύ Κινητής Συσκευής και Santoku στη πόρτα 5555
- Χρήση του εργαλείου **dd** για την αντιγραφή bit προς bit του φακέλου προς ανάλυση

Η διαδικασία φαίνεται και στο παρακάτω στιγμιότυπο:



Εικόνα 35: Αντιγραφή εικόνας συστήματος με το εργαλείο ADB

Στη συνέχεια αφού λήφθηκε η εικόνα έγινε τροποποίηση του αρχείου παραμετροποίησης scalpel.conf ώστε να ανακτηθούν μόνο αρχεία τύπου GIF, JPG, PNG, BMP.

```
#-------------------------------------------------------------------
# GRAPHICS FILES
#-------------------------------------------------------------------
#
#
# AOL ART files
#       art     y       150000  \x4a\x47\x04\x0e        \xcf\xc7\xcb
#       art     y       150000  \x4a\x47\x03\x0e        \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
       gif     y       5000000         \x47\x49\x46\x38\x37\x61        \x00\x3b
       gif     y       5000000         \x47\x49\x46\x38\x39\x61        \x00\x3b
       jpg     y       200000000       \xff\xd8\xff\xe0\x00\x10        \xff\xd9
#
#
# PNG
       png     y       20000000        \x50\x4e\x47?   \xff\xfc\xfd\xfe
#
#
# BMP   (used by MSWindows, use only if you have reason to think there are
#       BMP files worth digging for. This often kicks back a lot of false
#       positives
#
       bmp     y       100000  BM??\x00\x00\x00
#
# TIFF
```

Εικόνα 36: Επεκτάσεις αρχείων που υποστηρίζει το scalpel προς ανάκτηση

Τέλος για να ξεκινήσει η ανάκτηση των αρχείων από αντίγραφο εικόνας της Κινητής Συσκευής εκτελείται η εντολή scalpel ακολουθώντας το πρότυπο "**scalpel -c [**scalpel configuration file**] -o [**output file**] [**input file**]".**

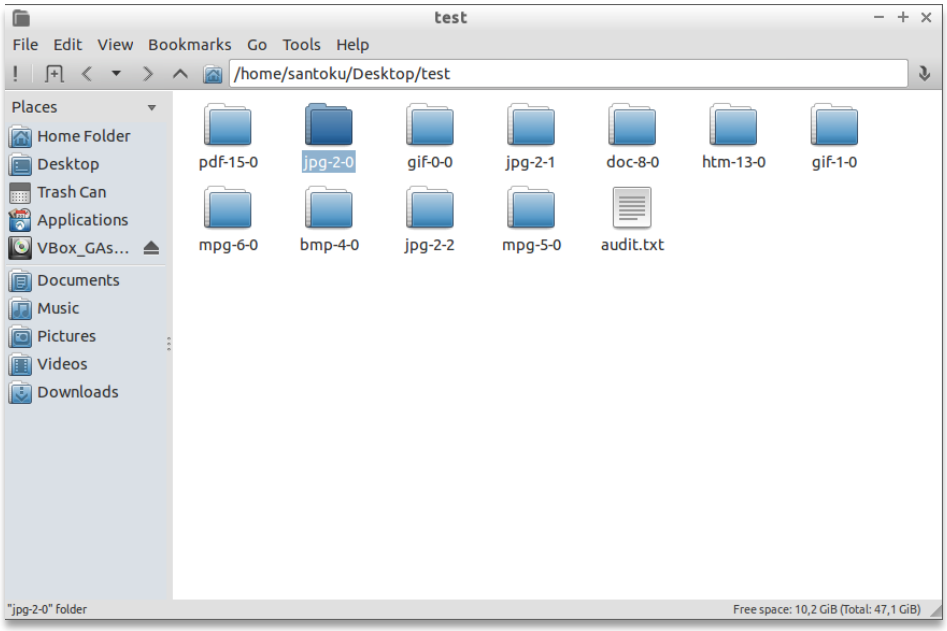
```
root@santoku-VirtualBox:/root/Desktop# nano scalpel.conf
root@santoku-VirtualBox:/root/Desktop# scalpel -c scalpel.conf -o test lenovo.ra
w
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/root/Desktop/lenovo.raw"

Image file pass 1/2.
lenovo.raw: 100.0% |*********************************|    4.7 GB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 3 files
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 530 files
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 2687 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0 files
bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 178 files
mpg with header "\x00\x00\x01\xba" and footer "\x00\x00\x01\xb9" --> 702 files
mpg with header "\x00\x00\x01\xb3" and footer "\x00\x00\x01\xb7" --> 566 files
pst with header "\x21\x42\x4e\xa5\x6f\xb5\xa6" and footer "" --> 0 files
ost with header "\x21\x42\x44\x4e" and footer "" --> 0 files
dbx with header "\xcf\xad\x12\xfe\xc5\xfd\x74\x6f" and footer "" --> 0 files
idx with header "\x4a\x4d\x46\x39" and footer "" --> 0 files
Carving files from image.
Image file pass 2/2.
lenovo.raw: 100.0% |*********************************|    4.7 GB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 4666, elapsed = 246 seconds.
root@santoku-VirtualBox:/root/Desktop#
```

Εικόνα 37: Ανάκτηση αρχείων με τις επιλεγμένες επεκτάσεις

Αφού τελειώσει η ανάκτηση δημιουργείται τοπικά ο φάκελος που έχει ορίσει ο ερευνητής σαν έξοδο από την εκτέλεση του εργαλείου ο οποίος εμπεριέχει πλέον όλα τα ανακτημένα αρχεία από την εικόνα της συσκευής ανά τύπο αρχείου που επιλέχθηκε ρυθμίζοντας το αρχείο scalpel.conf.



Εικόνα 38: Εξαγωγή αρχείων απο το εργαλείο Scalpel

Παρακάτω θα αναπτυχθεί ένα πραγματικό σενάριο χρησιμοποιώντας το εργαλείο Autopsy TSK το οποίο έχει ενσωματωμένο το εργαλείο scalpel για «file carving» από μια εικονική αναπαράσταση της συσκευής.

5.2.4. Περίληψη Σεναρίου

Ο κύριος Χ είναι ιδιοκτήτης ενός ανθοπωλείου στην οδό Πάρου 14, περιοχή Βάρης. Στις 15/01/2018, ώρα 06:32 καθώς πήγαινε να ανοίξει το ανθοπωλείο παρατήρησε ένα δίκυκλο όχημα να κατευθύνεται σε ένα σταματημένο με αλάρμ ΙΧ τύπου Golf VW GTI. Ο κύριος Χ υποστηρίζει ότι ο οδηγός του δίκυκλου

έβγαλε το κινητό τράβηξε φωτογραφία το IX όχημα και στη συνέχεια αφού απομακρύνθηκε το αυτοκίνητο πήρε φωτιά λόγω κάποιου εύφλεκτου υλικού που τοποθέτησε πιθανών ο οδηγός του δίκυκλου. Ο ύποπτος οδηγός του δίκυκλου φωτογράφησε την τοποθεσία μετά την έκρηξη και στη συνέχεια καθώς έφευγε κάνοντας τη κίνηση να βάλει το κινητό στη τσέπη του το κινητό έπεσε από τη μηχανή εν άγνοια του υπόπτου οδηγού. Ο κύριος Χ σύλλεξε τη Κινητή Συσκευή από την σκηνή του εγκλήματος πρώτα και την κράτησε ακέραια μέχρι να έρθει η αστυνομία. Αφού κατέθεσε στη συνέχεια παρέδωσε το κινητό στην αστυνομία η οποία με τη σειρά της έστειλε το κινητό για ανάλυση στο τμήμα εγκληματολογικών ερευνών.

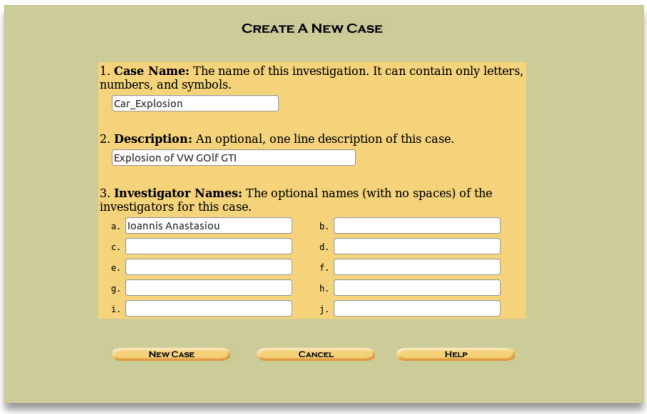
Διαδικασία που ακολουθήθηκε:

Ο ερευνητής Ιωάννης Αναστασίου, στον οποίο ανατέθηκε η ανάλυση της επικείμενης συσκευής αφού έλαβε πλήρη δικαιώματα στην συσκευή του υπόπτου και απόκτησε ένα ακριβές αντίγραφο της συσκευής εφαρμόζοντας τους γενικούς κανόνες της Ψηφιακής Εγκληματολογίας, προχώρησε την ανάλυση του χρησιμοποιώντας το εργαλείο Autopsy στον εργαστηριακό του υπολογιστή ο οποίος έχει εγκατεστημένη τη Linux διανομή Santoku.

Ξεκινώντας λοιπόν, αφού έγινε είσοδος στο Santoku εκτελέστηκε η εντολή autopsy από ένα τερματικό παράθυρο της διανομής. Στη συνέχεια ο ερευνητής μετέβηκε στην loopback διεύθυνση localhost:9999/autopsy στην οποία τρέχει εξαρχής το πρόγραμμα.

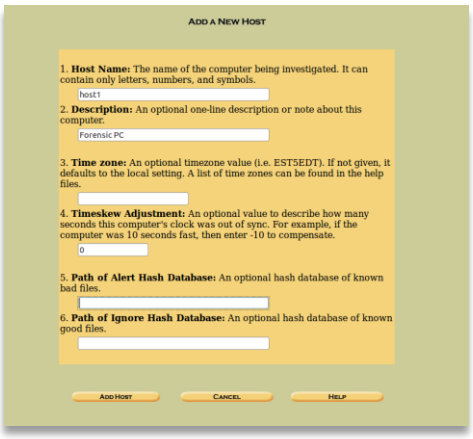
Εικόνα 39: Περιβάλλον Autopsy

Στη συνέχεια το πρόγραμμα δίνει την επιλογή στον ερευνητή να δημιουργήσει μια νέα υπόθεση πληκτρολογώντας τα απαραίτητα στοιχεία για τη περιγραφή της.



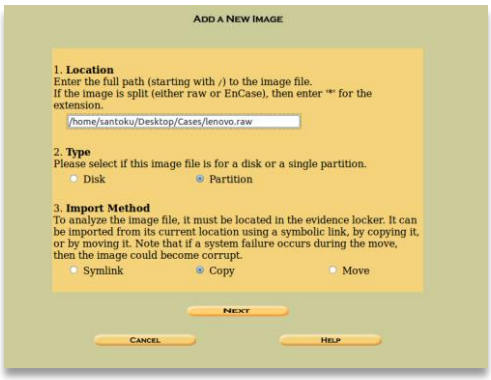
Εικόνα 40: Συμπλήρωση στοιχείων υπόθεσης στο Autopsy

Επιλέγοντας «New Case» εμφανίζεται νέο παράθυρο στο οποίο ο ερευνητής μπορεί εάν θέλει να συμπληρώσει τα στοιχεία του συστήματος στο οποίο τρέχει το πρόγραμμα ή να επιλέξει να ενσωματώσει κάποια έτοιμη βάση hash συναρτήσεων που θα μπορούσαν να τον διευκολύνουν στην έρευνα του σε ότι αφορά τα ευρήματα της υπόθεσης. Επιλέγοντας να προσθέσει μια βάση Hash συναρτήσεων το πρόγραμμα μπορεί να βρει γνωστά αρχεία και να τα επισημάνει κατά το πέρας της ανάλυσης για τον ερευνητή. Αντίθετα επιλέγοντας μια βάση Hash συναρτήσεων απόρριψης στοιχείων το πρόγραμμα μπορεί να αγνοήσει στοιχεία τα οποία είναι “default” και δεν χρειάζονται επιπρόσθετο έλεγχο από τον ερευνητή γεγονός που μπορεί να εξοικονομήσει χρόνο και να μετριάσει τη χρονική διάρκεια της έρευνας. Στη περίπτωση της επικείμενης υπόθεσης δεν θα χρησιμοποιηθούν Hash βάσεις δεδομένων.



Εικόνα 41: Συμπλήρωση περιγραφής υπόθεσης στο Autopsy

Στη συνέχεια με το που προστεθούν οι πληροφορίες για το σύστημα στο οποίο τρέχει το πρόγραμμα εμφανίζεται ένα νέο παράθυρο στο οποίο ζητείται από τον ερευνητή να επιλεχθεί ο δίσκος η το διαμέρισμα δίσκου το οποίο θα υποβληθεί σε ανάλυση. Στη προκειμένη περίπτωση επιλέγεται σαν διαμέρισμα δίσκου το αντίγραφο που δημιουργήθηκε κατά την διαδικασία ανακτήσεως.

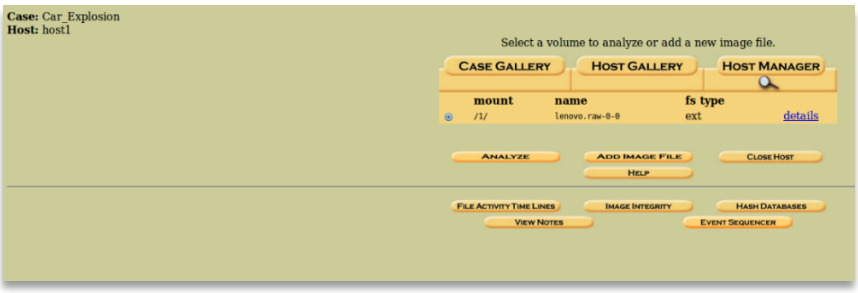


Εικόνα 42: Εισαγωγή εικόνων δίσκου στο Autopsyπρος ανάλυση

Επιλέγοντας “Next” δίνεται από το πρόγραμμα η δυνατότητα υπολογισμού μιας τιμής Hash της εικόνας που θα υποβληθεί σε ανάλυση ώστε να επιβεβαιωθεί η ακεραιότητα της και η ταυτοποίηση των στοιχείων της με αυτών της Κινητής Συσκευής μετά την ανάλυση τους. Παρατηρείται ότι το πρόγραμμα εμφανίζει από μόνο του την επιλογή “ext” για την raw εικόνα που αναλύεται.

Εικόνα 43: Υπολογισμός τιμής hash της εικόνας

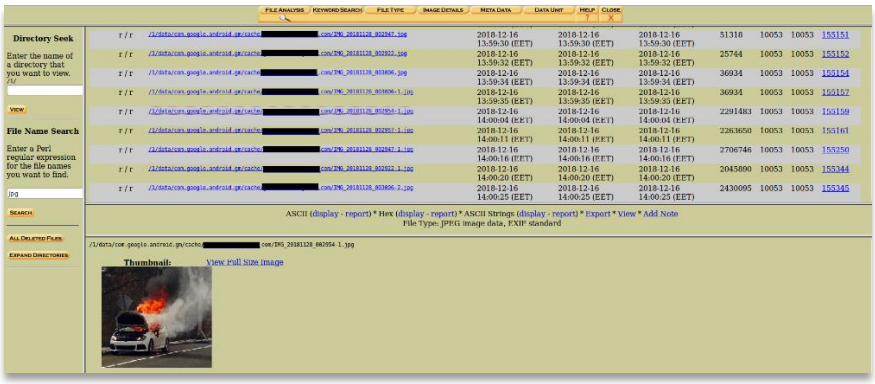
Με το που επιλέξει ο ερευνητής την επιλογή *"ADD"* το πρόγραμμα ξεκινάει τη διαδικασία ανάλυσης και μόλις αυτή τελειώσει εμφανίζεται ένα νέο παράθυρο με ενέργειες για τον ερευνητή, το όνομα και τα στοιχεία τις υπόθεσης.



Εικόνα 44: Ολοκλήρωση εκτέλεσης του εργαλείου

Επιλέγοντας *"ANALYZE"* εμφανίζονται όλα τα αποτελέσματα που προέκυψαν κατά την ανάλυση[19]. Οι επιλογές που δίνονται από το πρόγραμμα περιλαμβάνουν την ανάλυση αρχείου την ανάλυση τύπου αρχείου την έρευνα με βάση κάποια λέξη κλειδί τις λεπτομέρειες του αντιγράφου, τα μεταδεδομένα και τα δεδομένα του αντιγράφου.

Κατά την ανάλυση αρχείων ο ερευνητής λοιπόν διαπιστώνει μια φωτογραφία που απεικονίζει την έκρηξη ενός IX τύπου GOLF VW GTI στη μνήμη cache του φακέλου του ηλεκτρονικού ταχυδρομείου του υπόπτου στη κινητή του συσκευή και επιβεβαιώνει έτσι τη κατάθεση του ιδιοκτήτη του ανθοπωλείου.



Εικόνα 45: Εύρεση πειστήριων χρησιμοποιώντας το autopsy

5.3. Η εργαστηριακή διανομή Androl4b

Το Androl4b είναι μια διανομή ανοιχτής πηγής εικονικού περιβάλλοντος αφιερωμένο στις πτυχές ασφάλειας σε ότι αφορά την Ψηφιακή Εγκληματολογία Κινητών Συσκευών Android και βασίζεται στο λειτουργικό Ubuntu-mate, το οποίο περιλαμβάνει τη συλλογή του τελευταίου Framework, βοηθητικούς οδηγούς εργαστήριων και ασφάλειας, Αντίστροφης Μηχανικής και ανάλυσης κακόβουλου λογισμικού σε εφαρμογές Android.

Εικόνα 46: Το περιβάλλον Androl4b

Τα εργαλεία που περιλαμβάνει το Androl4b Framework είναι τα παρακάτω:

- **APKStudio:** Το APKStudio είναι ένα IDE πολλαπλών πλατφορμών για την αντίστροφη μηχανική και την ανασυγκρότηση δυαδικών αρχείων εφαρμογών Android, μέσα σε ένα περιβάλλον εργασίας χρήστη. Έχει ένα φιλικό σχεδιασμό, με ένα πρόγραμμα επεξεργασίας κώδικα που υποστηρίζει την επισήμανση σύνταξης για τύπους αρχειών κώδικα επέκτασης smali.
- **ByteCodeViewer:** Το ByteCodeViewer, είναι μια σουίτα για Αντίστροφη Μηχανική σε εφαρμογές Android, με πέντε διαφορετικά Java de-Compilers, δύο επεξεργαστές κώδικα byte, έναν μεταγλωττιστή Java και plugins
- **MobSF:** Το MobSF όπως συζητήθηκε και παραπάνω είναι μια εφαρμογή ανοικτού κώδικα για κινητά (Android / iOS). Είναι ένα πλαίσιο ικανό για Στατική και Δυναμική Ανάλυση (Επιτρέπεται μόνο Στατική ανάλυση σε αυτήν την εικονική μηχανή). Μπορεί να χρησιμοποιηθεί για μια αποτελεσματική και γρήγορη ανάλυση ασφάλειας εφαρμογών, είναι συμβατή με δυαδικά αρχεία (APK και IPA) και συμπιεσμένο πηγαίο κώδικα. Το MobSF μπορεί επίσης να εκτελέσει δοκιμές ασφαλείας με το API Fuzzer που μπορεί να κάνει: συλλογή πληροφοριών, ανάλυση κεφαλίδων ασφαλείας, εντοπισμός συγκεκριμένων τρωτών σημείων του API κινητού όπως: XXE, FRSS, δρομολόγηση, IDOR ... και άλλα βασικά ζητήματα ασφάλειας.
- **Drozer:** Το Drozer, είναι ένα Penetration Testing framework που χρησιμοποιείται για εφαρμογές Android. Επιτρέπει την αναζήτηση ευπαθειών ασφαλείας σε εφαρμογές και συσκευές, αναλαμβάνοντας τον ρόλο μιας εφαρμογής, επιτρέποντας την αλληλεπίδραση με την εικονική μηχανή Dalvik, τα τελικά σημεία IPC άλλων εφαρμογών και το υποκείμενο λειτουργικό σύστημα.
- **APKtool:** Το APKtool, είναι ένα εργαλείο για Αντίστροφη Μηχανική σε δυαδικά αρχεία εφαρμογών Android. Μπορεί εκτελέσει αποκωδικοποίηση του πηγαίου κώδικα με έναν σχεδόν πρωτότυπο τρόπο και να ανακατασκευαστεί μετά από κάποιες τροποποιήσεις, πράγμα που καθιστά δυνατό τον βήμα προς βήμα τον εντοπισμό σφαλμάτων κώδικα smali. Επίσης διευκολύνει την εργασία με την εφαρμογή λόγω της δομής των αρχείων σε έργα και με την αυτοματοποίηση ορισμένων επαναλαμβανόμενων εργασιών όπως η κατασκευή του apk.
- **AndroidStudio:** Το AndroidStudio, IDE χρησιμοποιείται για την ανάπτυξη εφαρμογών Android. Πρόκειται για ένα ολοκληρωμένο αναπτυξιακό περιβάλλον (IDE) για την ανάπτυξη εφαρμογών Android, με βάση το IntelliJ IDEA. Το AndroidStudio προσφέρει λειτουργίες που βελτιώνουν την παραγωγικότητα στην κατασκευή εφαρμογών Android.
- **ClassyShark:** Το Classy Shark, είναι ένα εργαλείο για προγραμματιστές Android. Επιτρέπει την αξιόπιστη πλοήγηση μέσω ενός εκτελέσιμου αρχείου Android και την εμφάνιση σημαντικών πληροφοριών όπως: διασυνδέσεις και μέλη κλάσης, count και εξαρτήσεις. Υποστηρίζει πολλαπλές μορφές, όπως: βιβλιοθήκες (.dex, .aar, .so), εκτελέσιμα (.apk, .jar, .class) και όλα τα δυαδικά αρχεία XML Android: Android Manifest, πόρους, σχέδια κ.λπ.
- **BurpSuite**: Το BurpSuite, είναι μια ολοκληρωμένη πλατφόρμα για «Δοκιμές Διεισδύσεων σε Περιβάλλον Διαδικτυακών Εφαρμογών» (Web Application Penetration Testing). Τα διάφορα εργαλεία του λειτουργούν τέλεια για να υποστηρίξουν ολόκληρη τη διαδικασία: Δοκιμών Διείσδυσης, χαρτογράφηση και ανάλυση της επιφάνειας επίθεσης ενός αρχικού αιτήματος, μέσω της αναζήτησης και εκμετάλλευσης των τρωτών σημείων ασφαλείας.
- **Wireshark:** Το Wireshark, είναι ο σημαντικότερος αναλυτής πρωτοκόλλου δικτύου στον κόσμο. Μπορεί να εμφανίσει τι συμβαίνει σε ένα δίκτυο σε μικροσκοπικό επίπεδο ανάλυσης. Είναι το «Defacto» πρότυπο της βιομηχανίας και των εκπαιδευτικών ιδρυμάτων.
- **M.A.R.A framework:** Το M.A.R.A Framework το οποίο θα χρησιμοποιηθεί και στα πλαίσια αυτής της διατριβής, είναι ένα πλαίσιο ανάλυσης ασφάλειας και Αντίστροφης Μηχανικής για εφαρμογές κινητής τηλεφωνίας. Πρόκειται για ένα σύνολο εργαλείων που χρησιμοποιούνται σύμφωνα με τα πρότυπα OWASP.
- **QARK:** Εργαλείο που χρησιμοποιείται για ανάλυση και αξιολόγηση ασφάλειας εφαρμογών Android το οποίο θα χρησιμοποιηθεί και στα πλαίσια της επικείμενης διατριβής.
- **FindBugs-IDEA:** Το FindBugs-IDEA, περιλαμβάνει στατική ανάλυση κώδικα σε byte και ψάχνει για σφάλματα στον κώδικα Java.

- **AndroBugs Framework:** Το AndroBugs Framework, είναι ένας σαρωτής ευπαθειών ασφαλείας για Android που βοηθά τους προγραμματιστές και τους Αναλυτές Ασφάλειας να βρουν πιθανές ευπάθειες ασφαλείας σε εφαρμογές Android.
- **Metasploit Framework:** Το Metasploit Framework είναι ένα μεγάλο πλαίσιο ασφάλειας υπολογιστών ανοιχτού κώδικα που παρέχει πληροφορίες σχετικά με τα τρωτά σημεία της ασφάλειας, στην ανάπτυξη υπογραφών για συστήματα ανίχνευσης εισβολών ενώ παράλληλα μπορεί να βοηθήσει τους Penetration Testers κατά την διαδικασία αξιολόγησης ασφάλειας.

Εργαστήρια:

Εκτός από τα εργαλεία που προσφέρει η διανομή Androl4b παρέχει επίσης και κάποια εργαστήρια στους χρήστες τα οποία σκοπό έχουν την βελτίωση των δυνατοτήτων των χρηστών και δίνουν μια πιο καλή πρακτικά αίσθηση των εργαλείων που συμπεριλαμβάνει η διανομή, ώστε οι χρήστες να εξοικειωθούν με περισσότερο πραγματικές συνθήκες ανάλυσης ασφάλειας. Τα εργαστήρια αυτά αποτυπώνονται παρακάτω περιληπτικά.

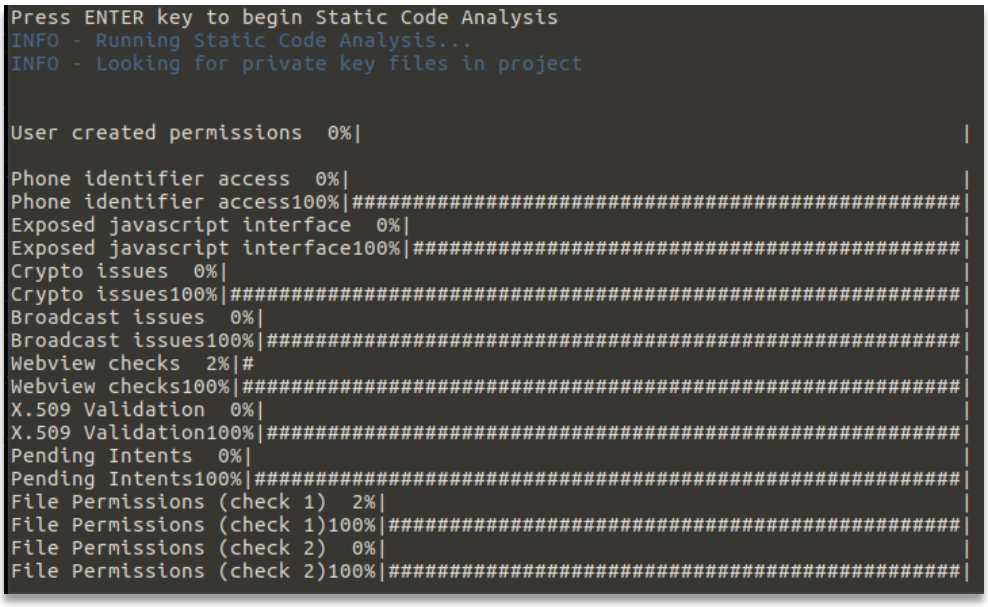
- **DIVA**: Το DIVA Android, είναι μια εφαρμογή που έχει σχεδιαστεί ειδικά για να είναι ανασφαλής. Σκοπός της εφαρμογής είναι να διδάξει επαγγελματίες προγραμματιστές, ελαττώματα που συνήθως υπάρχουν σε εφαρμογές, γενικά λόγω κακής ή μη ασφαλούς πρακτικής κωδικοποίησης.
- **InsecureBankv2**: Το InsecureBankv2, είναι μια εφαρμογή Android η οποία έκανε τους λάτρεις της ασφάλειας υπολογιστών και τους προγραμματιστές να μάθουν τις ανασφάλειες των εφαρμογών Android. Το συστατικό του διακομιστή παρασκηνίου είναι γραμμένο σε Python. Το στοιχείο πελάτη, δηλαδή το InsecureBank.apk για Android, μπορεί να μεταφορτωθεί μαζί με την πηγή.
- **DroidBench**: Συγκεκριμένα, περιέχει ενδιαφέρουσες περιπτώσεις δοκιμών για προβλήματα στατικής ανάλυσης (ευαισθησία πεδίου, ευαισθησία αντικειμένων, πλεονεκτήματα και μειονεκτήματα στα μήκη διαδρομής κλπ.), καθώς και σωστή μοντελοποίηση του κύκλου ζωής μιας εφαρμογής, χειρισμό ασύγχρονων επανακλήσεων και αλληλεπίδραση με το περιβάλλον εργασίας χρήστη.
- **GoatDroid**: Το GoatDroid, είναι ένα πλήρες λειτουργικό και αυτόνομο εκπαιδευτικό περιβάλλον για την εκπαίδευση των προγραμματιστών Android και των Penetration Testers. Το GoatDroid απαιτεί ελάχιστες εξαρτήσεις και είναι ιδανικό τόσο για αρχάριους όσο και για πιο προχωρημένους χρήστες.
- **Sieve:** Το Sieve είναι ένας διαχειριστής κωδικών πρόσβασης εφαρμογών, ο οποίος παρουσιάζει ορισμένες κοινές ευπάθειες εφαρμογών Android.

Σε αυτή την ενότητα λοιπόν, θα χρησιμοποιηθούν κάποια βασικά εργαλεία της διανομής Androl4b για να γίνει πιο κατανοητή η ανάλυση ασφάλειας εφαρμογών Android μέσω του συγκεκριμένου λειτουργικού. Τα εργαλεία αυτά είναι το "**QARK**" και το "***M.A.R.A Framework***".

5.3.1. Το εργαλείο QARK

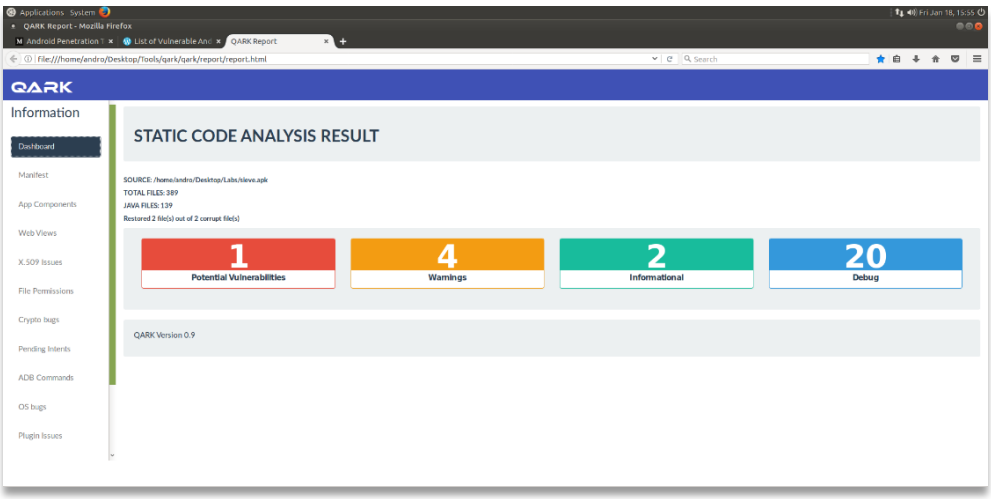
Το εργαλείο QARK έχει σχεδιαστεί για να ερευνά εφαρμογές Android οι οποίες φανερώνουν σχετικές με την ασφάλεια ευπάθειες, είτε σε πηγαίο κώδικα είτε σε ενσωματωμένες εφαρμογές τύπου APK. Το εργαλείο είναι επίσης ικανό να δημιουργήσει αναπτυσσόμενες APK και / ή εντολές ADB, ώστε να εκμεταλλευτεί πολλές από τις ευπάθειες που βρίσκει. Δεν χρειάζεται η συσκευή να λειτουργεί με δικαιώματα διαχειριστή, δηλαδή να είναι rooted καθώς αυτό το εργαλείο επικεντρώνεται στις ευπάθειες που μπορεί να είναι εκμετάλλευσης υπό συνθήκες ασφαλής λειτουργείας.

Για το πρόγραμμα QARK έγινε χρήση της εφαρμογής sieve.apk στο συγκεκριμένο πρόγραμμα. Για να τρέξει η ανάλυση χρειάζεται ο χρήστης να εκτελέσει το python αρχείο "***mainqark.py***" που βρίσκεται εντός του τοπικού φακέλου της εφαρμογής. Στη συνέχεια ζητούνται από το χρήστη να επιλεχθεί η φυσική διεύθυνση του Android SDK εργαλείου καθώς και η τοποθεσία στην οποία θα διεξαχθεί το αποτέλεσμα της ανάλυσης.



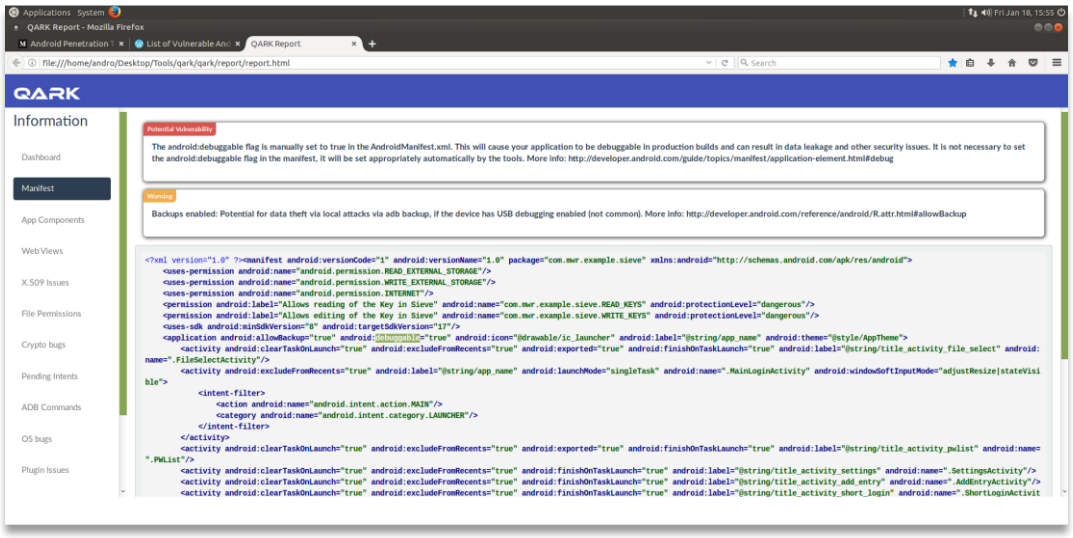
Εικόνα 47: Εκτέλεση στατικής ανάλυσης χρησιμοποιώντας το εργαλείο QARK

Με το πέρας της ανάλυσης δημιουργείται ένας φάκελος ονόματι report μέσα στο φάκελο qark ο οποίος περιέχει τα αποτελέσματα της Ψηφιακής Έρευνας και Ανάλυσης σε μορφή html.



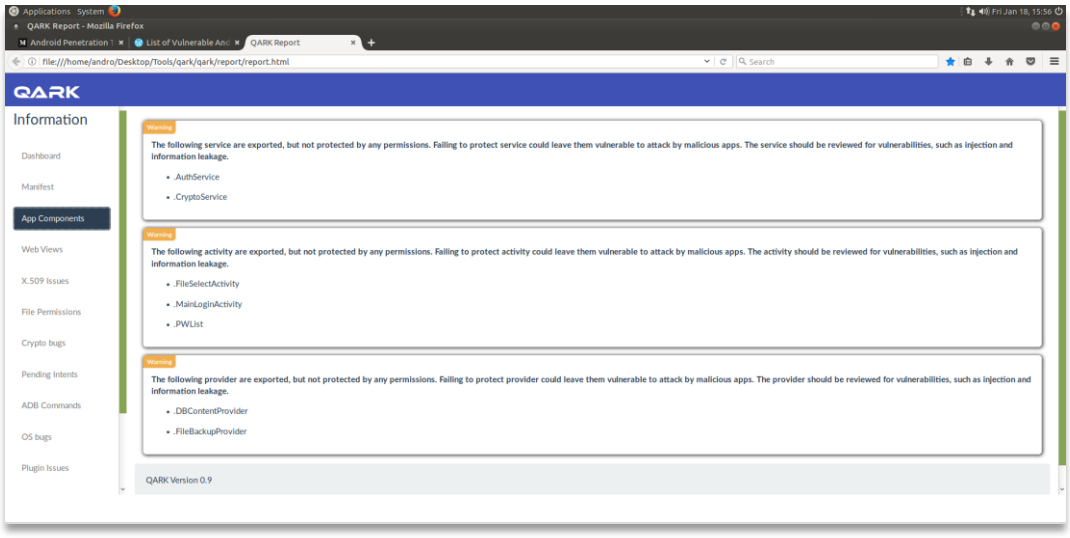
Εικόνα 48: Αποτελέσματα στατικής ανάλυσης της εφαρμογής sieve.apk

Η ανάλυση του αρχείου manifest του sieve.apk έδειξε ότι η δυνατότητα backup της εφαρμογής ήταν ενεργή ενώ παράλληλα η εφαρμογή μπορούσε να αναλυθεί μέσω διαδικασίας debugging κάτι το οποίο μπορεί να αποτελέσει κίνδυνο διαρροής δεδομένων και θέματα ασφάλειας.



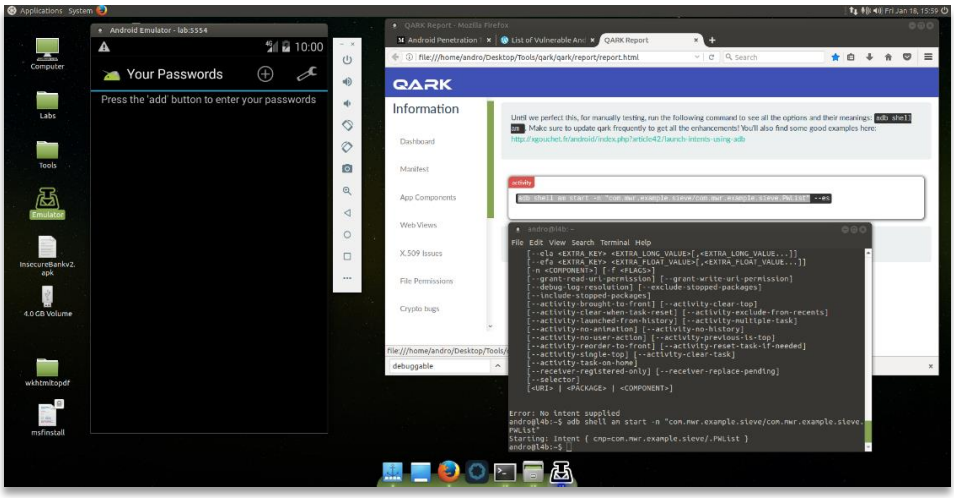
Εικόνα 49: Περιγραφή αποτελεσμάτων

Επιπροσθέτως στη καρτέλα «Τμήματα της εφαρμογής» στην αναφορά του εν λόγω εργαλείου φανερώθηκαν τα παρακάτω τρία θέματα τα οποία χρήζουν προσοχής. Αναλυτικά λοιπόν οι υπηρεσίες, *AuthService*, *CryptoService*, *FileSelectActivity*, *MainLoginActivity*, *PWlist*, *DBContentProvider*, *FireBackupProvider*, λειτουργούνε χωρίς ασφάλεια και χωρίς περιορισμούς δικαιωμάτων κάτι το οποίο μπορεί να αποτελέσει αφορμή για επίθεση τύπου *injection* και διαρροής δεδομένων. Η πληροφορία αυτή από το εργαλείο φαίνεται στο παρακάτω στιγμιότυπο.



Εικόνα 50: Περιγραφή αποτελεσμάτων

Τέλος ο χρήστης έχει τη δυνατότητα χρησιμοποιώντας τον προσομοιωτή Android του Androl4b να εξετάσει την εν λόγω εφαρμογή χρησιμοποιώντας την εντολή που του δίνει το εργαλείο από την αναφορά και ύστερα να την εκτελέσει σε ένα παράθυρο τερματικού.



Εικόνα 51: Δυνατότητες προσομοίωσης του εργαλείου QARK

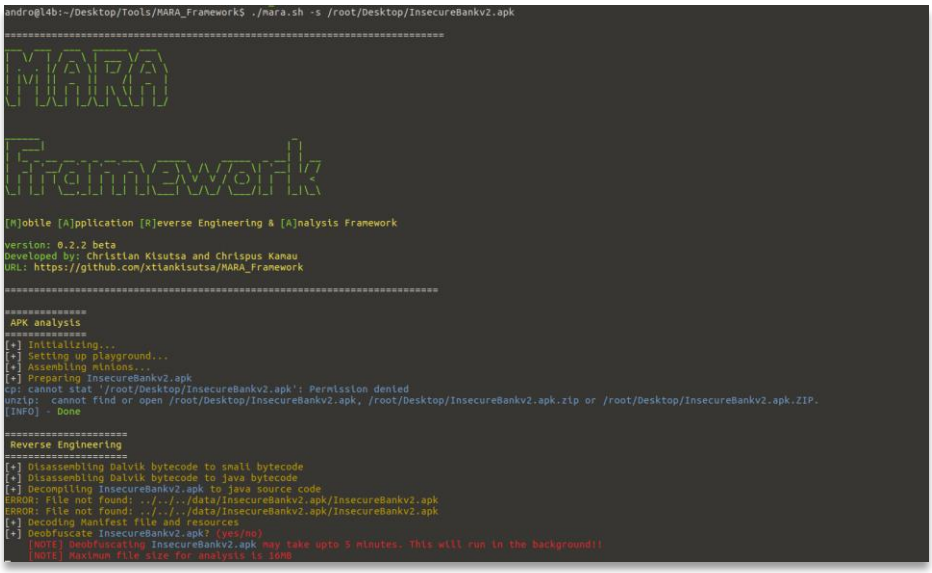
5.3.2. Το Πλαίσιο M.A.R.A Framework:

Το M.A.R.A (*Mobile Application Reverse Engineering & Analysis*) Framework είναι ένα Πλαίσιο Αντίστροφης Μηχανικής και Ανάλυσης εφαρμογών. Πρόκειται για ένα εργαλείο που συνδυάζει κοινά χρησιμοποιούμενα εργαλεία Αντίστροφης Μηχανικής και Ανάλυσης Εφαρμογών για κινητά, για διεξαγωγή Δοκιμών Διείσδυσης σε εφαρμογές κινητών ενάντια στις απειλές ασφάλειας σύμφωνα με τον παγκόσμιο οργανισμό ασφάλειας OWASP. Στόχος του είναι να καταστήσει αυτό το έργο ευκολότερο και πιο φιλικό προς τους προγραμματιστές εφαρμογών για κινητά και τους επαγγελματίες ασφαλείας.

Μερικές δυνατότητες του εργαλείου είναι:

- Αντίστροφη μηχανική σε APK εφαρμογές
  - ✓ Αποσυναρμολόγηση Dalvik bytecode σε smali bytecode μέσω baksmali και apktool
  - ✓ Αποσυναρμολόγηση Dalvik bytecode σε java bytecode μέσω enjarify
  - ✓ Αποσυμπίληση του APK στον πηγαίο κώδικα Java μέσω του jadx
- Αποκάλυψη APK
  - ✓ APK deobfuscation μέσω του apk-deguard.com
- Ανάλυση APK
  - ✓ Ανάλυση αρχείων smali για ανάλυση μέσω smalisca
  - ✓ Κατάργηση των στοιχείων του ενεργητικού, τις βιβλιοθήκες και τους πόρους
  - ✓ Εξαγωγή δεδομένων πιστοποιητικών μέσω του openssl
  - ✓ Εξαγωγή συμβολοσειρών και δικαιωμάτων εφαρμογής μέσω AAPT
  - ✓ Προσδιορισμός μεθόδων και κλάσεων μέσω του ClassyShark
  - ✓ Σάρωση για τα τρωτά σημεία εφαρμογών APK μέσω του androbugs
  - ✓ Ανάλυση APK για πιθανή κακόβουλη συμπεριφορά μέσω του androwarn
  - ✓ Προσδιορισμός τών μεταγλωττιστών, των συσκευαστών και των obfuscators μέσω του APKiD
  - ✓ Εξαγωγή διαδρομών εκτέλεσης, διευθύνσεις IP, URL, URI, ηλεκτρονικά μηνύματα μέσω τεχνικών regex
- Ανάλυση Manifest APK
  - ✓ Προτάσεις εξαγωγής
  - ✓ Ανάκτηση εξαγόμενων δραστηριοτήτων
  - ✓ Απόσπαση τμημάτων
  - ✓ Ανάκτηση εξαγωγικών δεκτών
  - ✓ Υπηρεσίες εξαγωγής
  - ✓ Ανάκτηση εξαγόμενων υπηρεσιών
  - ✓ Ελέγχος αν η εφαρμογή APK είναι debuggable
  - ✓ Ελέγχος αν η εφαρμογή APK επιτρέπει την αποστολή κρυφών κωδικών
  - ✓ Ελέγχος αν η εφαρμογή APK μπορεί να λάβει δυαδικά SMS

- ❖ Ανάλυση Domain
  - ✓ Σάρωση SSL τομέα μέσω pyssltest και testssl
  - ✓ Αποτύπωση δακτυλικών αποτυπωμάτων μέσω δικτυακού τόπου
- ❖ Ανάλυση ασφαλείας
- ✓ Στατική ανάλυση πηγαίου κώδικα βάσει της λίστας «OWASP Mobile Top 10» και της λίστας ελέγχου OWASP για κινητές εφαρμογές



Εικόνα 52: Τοπλαίσιο του εργαλείου M.A.R.A_Framework

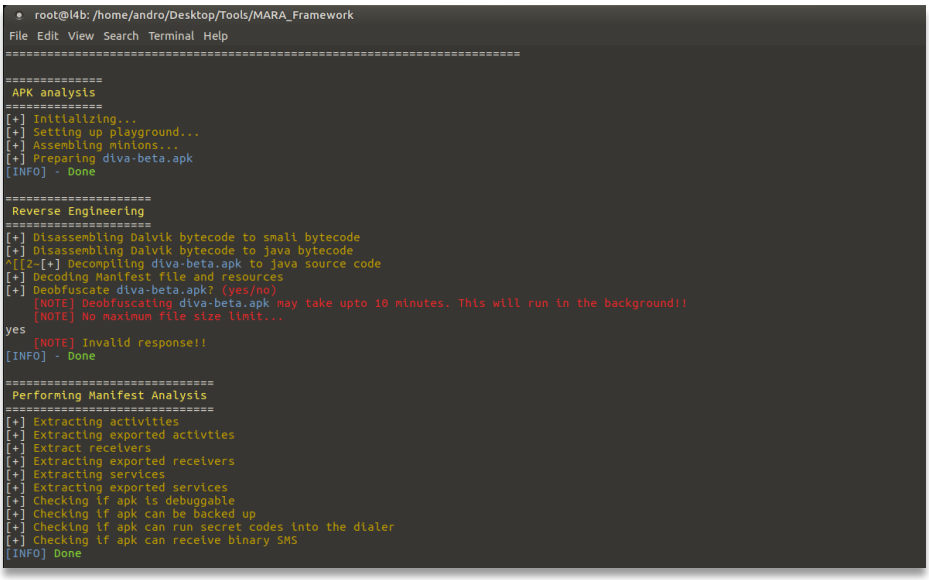
Θα πρέπει να ληφθεί υπόψη ότι για την σωστή εκτέλεση του εν λόγω εργαλείου θα πρέπει οι εφαρμογές να τρέχουν μέσα από το *root* directory του συγκεκριμένου Framework συνεπώς για το σενάριο που ακολουθεί λήφθηκαν και αποθηκεύτηκαν οι εφαρμογές στη φυσική διεύθυνση /home/andro/Desktop/Tools/MARA_Framework ενώ πριν εκτελεστεί το πρόγραμμα δόθηκαν δικαιώματα root για να επιτραπεί η αποθήκευση των αποτελεσμάτων από το εργαλείο.

5.3.3. Περίληψη Σεναρίου

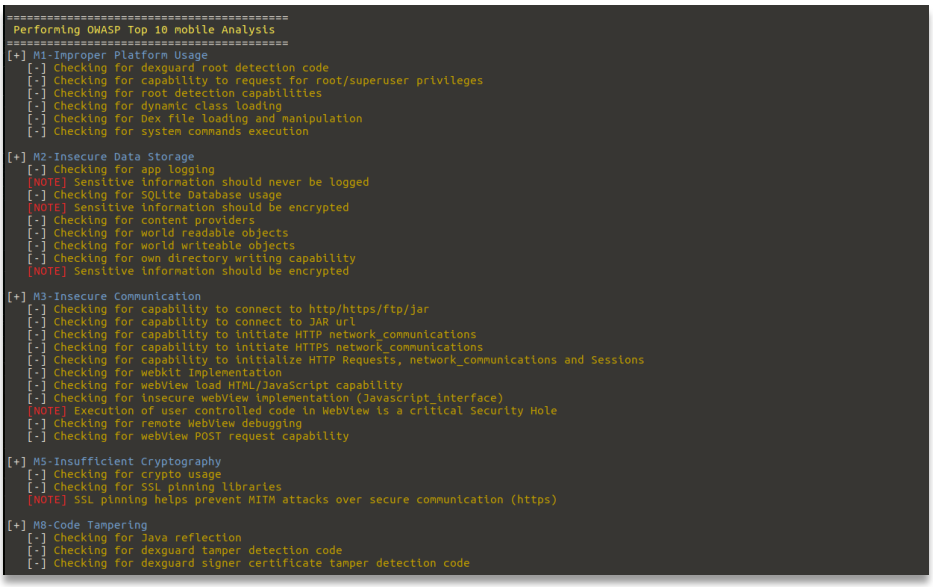
Ο Τζέιμς είναι ένας junior Αναλυτής Ασφάλειας ο οποίος κάνει την πρακτική του στην ανώνυμη εταιρία ψηφιακών ερευνών Χ. Προκειμένου να βελτιώσει την εμπειρία του πάνω στην ανάλυση πηγαίου κώδικα APK εφαρμογών έκανε λήψη διάφορων δημόσιων εφαρμογών APK από το Διαδίκτυο με σκοπό να ανακαλύψει ευπάθειες στον πηγαίο κώδικα και στο manifest της κάθε εφαρμογής χρησιμοποιώντας τεχνικές Αντίστροφης Μηχανικής, χρησιμοποιώντας τη διανομή του Androl4b και του M.A.R.A Framework το οποίο είναι ικανό για εκτύπωση αποτελεσμάτων σε μορφή html. Παρακάτω αποτυπώνεται η διαδικασία ανάλυσης μιας από τις εφαρμογές αυτές, της εφαρμογής diva-beta.apk.

Διαδικασία που ακολουθήθηκε

Για να εκτελέσει το M.A.R.A framework ο Τζέιμς έτρεξε μέσα από τη φυσική διεύθυνση του εργαλείου την εντολή **"./MARA.sh -s [***apkfile***]"** για κάθε μία από τις εφαρμογές που έκανε λήψη**.** Παρακάτω φανερώνονται τα αποτελέσματα της εφαρμογής diva-beta.apk:

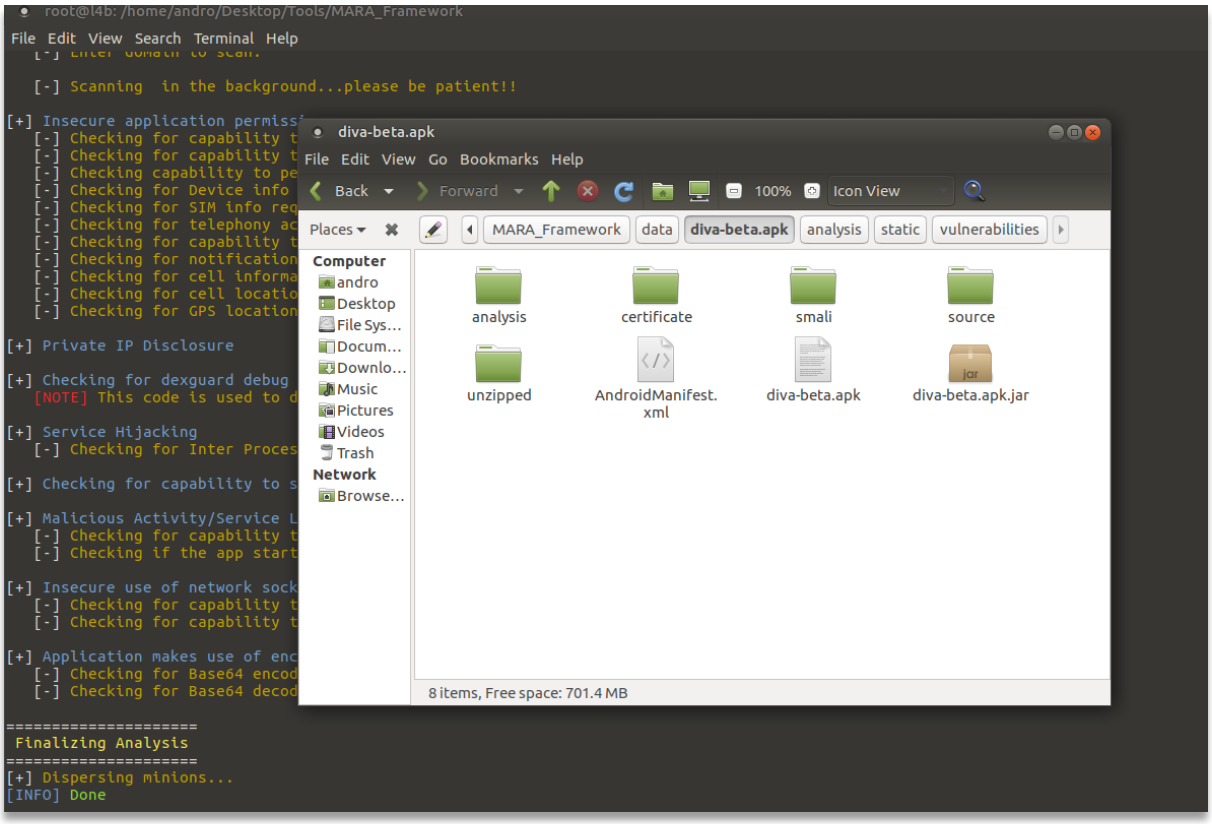


Εικόνα 53: Ανάλυση κώδικα Dalvik της εφαρμογήςdiva-beta.apk στο M.A.R.A Framework



Εικόνα 54: Συνέχεια ανάλυσης του εργαλείου M.A.R.A-framework

Αφού τελειώσει η ανάλυση από το εργαλείο ο Τζέιμς ανέτρεξε στη φυσική διεύθυνση "*home/andro/Desktop/Tools/MARA_framework/data"* όπου και βρήκε σωσμένα τα αποτελέσματα από την ανάλυση του εργαλείου τα οποία φαίνονται παρακάτω:

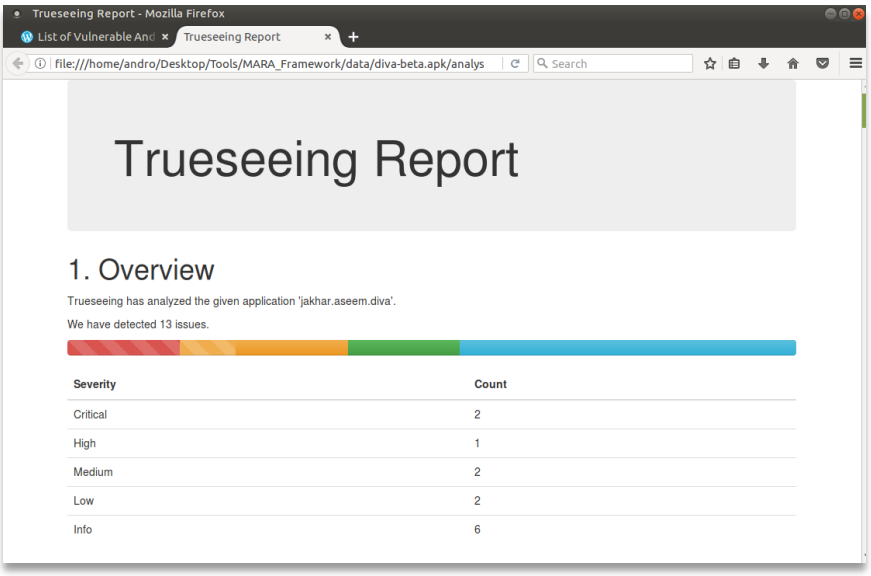


Εικόνα 55: Εξαγωγή αποτελεσμάτων M.A.R.A_Framework

Πιο αναλυτικά οι φάκελοι που δημιουργεί το M.A.R.A Framework είναι οι:

- ✓ **Analysis:** Εμπεριέχει όλα τα στοιχεία της δυναμικής και στατικής ανάλυσης που εξετάζονται από την εφαρμογή
- ✓ **Certificate:** Εμπεριέχει τυχόν πιστοποιητικά και στοιχεία κρυπτογράφησης κλειδιών της εφαρμογής
- ✓ **Smali:** Εμπεριέχει τους κώδικες smali και java της εφαρμογής
- ✓ **Source:** Εμπεριέχει όλα τα στοιχεία που βρίσκονται στον πηγαίο κώδικα της εξεταζόμενης εφαρμογής
- ✓ **Unzipped:** Εμπεριέχει αποσυμπιεσμένα αρχεία που τυχόν προέκυψαν ενώ ήταν ενσωματωμένα στην εν λόγω εφαρμογή**.**
- ✓ **AndroidManifest.xml:** Android κώδικας με όλες τις πληροφορίες που περιγράφουν το λειτουργικό και τις ενέργειες της εφαρμογής
- ✓ **Diva-beta.apk:** Ακριβές αντίγραφο της εφαρμογής
- ✓ **Diva-beta.apk.jar:** Η java επέκταση της εφαρμογής από αποσπάστηκε κατά την εκτέλεση της ανάλυσης

Για μια καλύτερη αναπαράσταση της ανάλυσης το M.A.R.A Framework δημιουργεί μια αναφορά μορφής HTML η οποία ονομάζεται “Trueseeing Report” για κάθε στοιχείο που υπέστη ανάλυση (Στατική, Κακόβουλου λογισμικού, Ευπαθειών) κατά την εκτέλεση του εργαλείου. Τα αποτελέσματα από τις ευπάθειες που ανακαλύφθηκαν φαίνονται στο παρακάτω στιγμιότυπο:

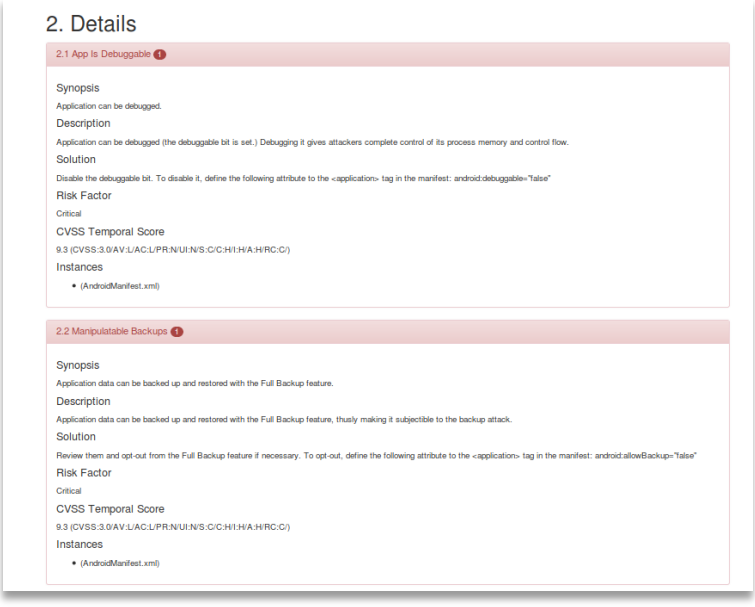


Εικόνα 56: Εξαγωγή αναφοράς του εργαλείου M.A.R.A_Framework

Ο Τζέιμς διαπίστωσε ότι η εφαρμογή diva-beta.apk φανέρωσε τις παρακάτω σοβαρές ευπάθειες:

Η εφαρμογή είναι αναλύσιμη (debuggable): *Αυτό σημαίνει ότι οποιοσδήποτε μπορεί να έχει φυσική πρόσβαση στη συσκευή και παράλληλα μπορεί να εκτελέσει κακόβουλο κώδικα με την άδεια της συγκεκριμένης εφαρμογής. Επιπροσθέτως, εάν η εφαρμογή περιέχει ευαίσθητα δεδομένα, θα είναι αρκετά απλή η εξαγωγή αυτών των ευαίσθητων δεδομένων από την εφαρμογή. Ως αντίμετρο ο προγραμματιστής της εν λόγω εφαρμογής θα πρέπει να απενεργοποιεί το debuggable bit (debuggable=”false”) στο manifest του apk.*

Εκμεταλλεύσιμη λειτουργίαbackup: *Χρησιμοποιώντας το εργαλείο ADB ενώ η εφαρμογή είναι παράλληλα debuggable , ένας επιτήδειος μπορεί να αποσπάσει ευαίσθητα δεδομένα από μια Κινητή Συσκευή κάνοντας backup ακόμη και αν δεν είναι ο ίδιος διαχειριστής στη συσκευή (η επίθεση αυτή είναι γνωστή και ως backup attack). Για να αποφευχθεί μια τέτοια επίθεση θα πρέπει ο προγραμματιστής να απενεργοποιεί τη δυνατότητα allowBackup στο manifest της εφαρμογής.*

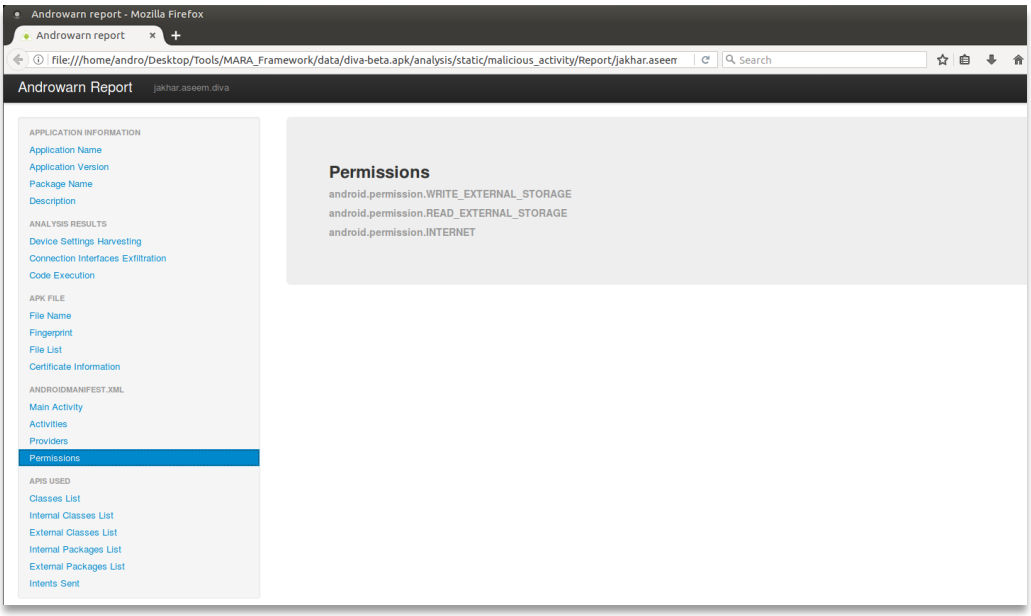


Εικόνα 57: Αποτελέσματα ευπαθειών της εφαρμογής diva-beta.apk

Τέλος το εργαλείο διεξάγει και μια γενική αναφορά μορφής HTML για τη ανάλυση κακόβουλου λογισμικού που υλοποιεί η οποία βρίσκεται στη φυσική διεύθυνση:

MARA_Framework/data/diva-beta.apk/analysis/static/malicious_activity/Report/

Ένα ακόμη σημαντικό κομμάτι που μπορεί να φανερώσει τους σκοπούς μιας εφαρμογής είναι οι άδειες που παρέχονται σε έναν χρήστη και τα δικαιώματα που έχει η εφαρμογή αυτή. Τα αποτελέσματα των δικαιωμάτων για την εφαρμογή του Τζέιμς φαίνονται παρακάτω:



Εικόνα 58: Αδειες χρήστη της εφαρμογής diva-beta.apk

Παρατηρώντας τα παραπάνω φαίνεται πως η συγκεκριμένη εφαρμογή έχει την άδεια να:

- ✓ Συνδέεται στο Διαδίκτυο
- ✓ Διαβάζει εξωτερικές συσκευές που συνδέονται στη Κινητή Συσκευή π.χ. DesktopPC
- ✓ Γράφει δεδομένα σε εξωτερικές συσκευές που συνδέονται στη Κινητή Συσκευή π.χ. Desktop PC

5.4. Το εργαλείο UFED Physical Analyzer

Το εργαλείο Ψηφιακής Εγκληματολογίας UFED Physical Analyzer της Cellebrite[5] είναι μια εμπορική εφαρμογή στο κόσμο της Ψηφιακής Εγκληματολογίας και χρησιμοποιείται για ανάλυση δεδομένων και δυνατοτήτων αναφοράς. Επιπροσθέτως το UFED Physical Analyzer επιτρέπει στον ερευνητή να διεξάγει εις βάθος ανάλυση των εξαγόμενων στοιχείων απο τη συσκευή παρέχοντας τα ακόλουθα βασικά χαρακτηριστικά:

- ❖ Φυσική Ανάκτηση με μια πολυεπίπεδη άποψη του περιεχομένου μνήμης η οποία:
  - ✓ παρέχει λεπτομερή προβολή hexdump
  - ✓ Ανασυγκροτεί το σύστημα αρχείων τηλεφώνου
  - ✓ Αποκωδικοποιεί λίστες επαφών, μηνύματα SMS, αρχεία καταγραφής κλήσεων, πληροφορίες τηλεφώνου (IMSI, ICCID, κωδικοί χρηστών) και πολλά άλλα
  - ✓ Παρέχει μια προβολή αρχείων δεδομένων - εικόνων, βίντεο κ.λπ.
  - ✓ Παρέχει πρόσβαση σε τρέχοντα και διαγραμμένα δεδομένα
  - ✓ Ανάκτηση κωδικών πρόσβασης τηλεφώνου
- ❖ Απλή προβολή και φιλική προς το χρήστη περιήγηση των πληροφοριών
- ❖ Ισχυρά εργαλεία αναζήτησης με δυνατότητες:
  - ✓ Άμεσης αναζήτησης περιεχομένου έργου
  - ✓ Αναζήτησης στο hexdump ή στο σύστημα αρχείων
  - ✓ Αναζήτησης ανά διάφορες παραμέτρους, όπως χορδές, bytes, αριθμούς, ημερομηνίες
  - ✓ Χρήσης της βελτιωμένης αναζήτησης GREP για την έρευνα συγκεκριμένων δεδομένων

- ✓ Σελιδοποίησης θέσεων μνήμης για ευρετηρίαση των τομέων-κλειδιών για μελλοντική αναθεώρηση
- ❖ Δυνατότητα χρήσης εντολών κελύφους Python για ανάλυση δεδομένων
- ❖ Plug-ins με δυνατότητες:
  - ✓ Διαχείρισης εγκατεστημένων plugin
  - ✓ Δημιουργίας plugin χρησιμοποιώντας τη γλώσσα συγγραφής Python αλλά και λήψης πρόσθετων από την επίσημη ιστοσελίδα της Cellebrite[5].
- ❖ Δημιουργία προσαρμοσμένων αναφορών

Σε αυτή την ενότητα θα γίνει μια πρώτη γνωριμία με το εν λόγω εργαλείο της Cellebrite.

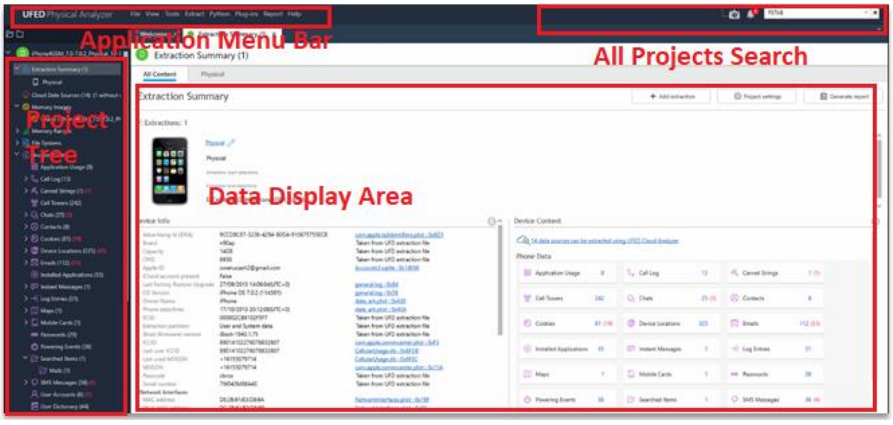
Αρχικά λοιπόν ένας χρήστης μπορεί να επιλέξει ένα αντίγραφο επέκτασης UFD και στη συνέχεια να επιλέξει να αποκωδικοποιήσει την εικόνα για να ξεκινήσει η ανάλυση από το πρόγραμμα. Παρακάτω έχει επιλεχθεί ένα έτοιμο αντίγραφο μίας iOS Κινητής Συσκευής με λειτουργικό 7.0.2.

Στη συνέχεια της ενότητας θα ακολουθήσει ένα πραγματικό σενάριο Ψηφιακής Εγκληματολογίας στο οποίο θα πραγματοποιηθεί Ψηφιακή ‘Ερευνα και Ανάλυση μιας Κινητής Συσκευής iPhone 4 με λειτουργικό iOS 7.1.2 χρησιμοποιώντας τις δυνατότητες του προγράμματος UFED Physical Analyzer.

5.4.1. Το περιβάλλον του εργαλείου UFED Physical Analyzer

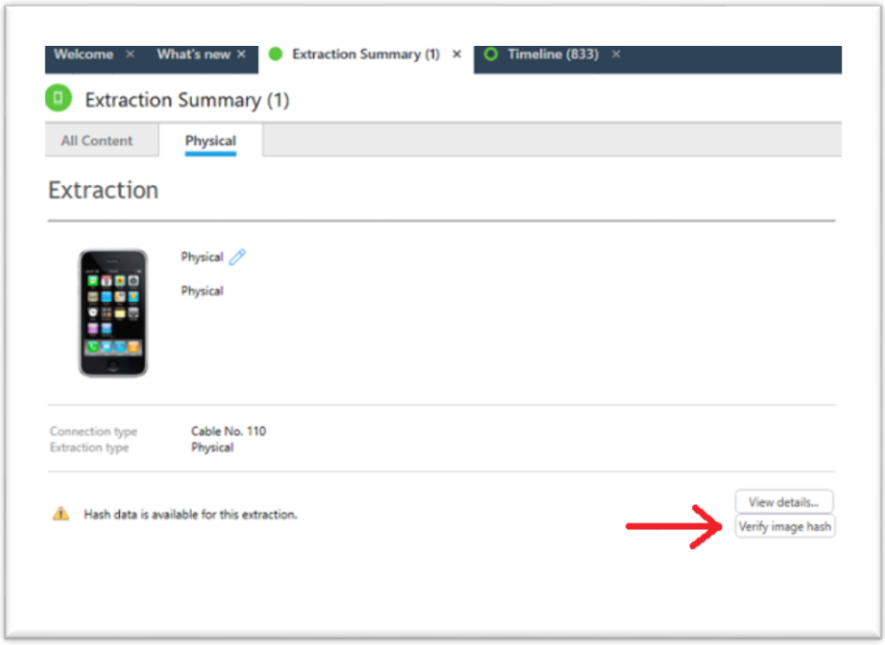
Το περιβάλλον του εργαλείου UFED Physical Analyzer περιλαμβάνει 4 τμήματα αναζήτησης, το κάθε ένα εκ των οποίων δίνει στον χρήστη τις αντίστοιχες πληροφορίες στον ερευνητή. Ξεκινώντας λοιπόν με το πρώτο, στα αριστερά του εργαλείου υπάρχει το «Δέντρο Εργασίας» (Project Tree) το οποίο δίνει μια συνολική κατηγοριοποίηση των ευρημάτων που υπάρχουν μέσα στη συσκευή τα οποία τοποθετούνται στις αντίστοιχες καρτέλες τους για εύκολη πλοήγηση στο εργαλείο. Συνεχίζοντας στο κέντρο του εργαλείου βρίσκεται η «Περιοχή Απεικόνισης Δεδομένων» (Data Display Area) από το UFED Physical Analyzer το περιεχόμενο του οποίου βασίζεται στις επιλεγμένες καρτέλες του Δέντρου εργασιών από τον χρήστη. Παράλληλα, πάνω και δεξιά του εργαλείου υπάρχει η «Καρτέλα Αναζήτησης Όλων των εργασιών» (All Projects Search). Η καρτέλα αυτή μπορεί να χρησιμοποιηθεί από τον ερευνητή για να τον διευκολύνει να αναζητήσει κάποια πληροφορία σε οποιοδήποτε ανάλυση συσκευής έχει αποθηκευτεί προηγουμένως στο εργαλείο. Για παράδειγμα εάν σε μια υπόθεση υπάρχουν 2 Κινητές Συσκευές οι οποίες αναλύθηκαν με το UFED Physical Analyzer και εμπεριέχουν και οι 2 μια συγκεκριμένη πληροφορία (π.χ. ίδιο αριθμό συνδρομητή στο αρχείο κλήσεων), η καρτέλα αναζήτησης όλων των εργασιών διευκολύνει τον ερευνητή να πληκτρολογήσει τον αριθμό αυτό για να γίνει η ταυτοποίηση του και στις 2 συσκευές.

Τέλος, πάνω και αριστερά υπάρχει το «Μενού Εφαρμογών» (Application Menu Bar) του εργαλείου. Ο ερευνητής μπορεί να κάνει επιλογή ανάμεσα σε άνοιγμα κάποιας εργασίας , άνοιγμα πρόσφατης εργασίας, αποθήκευση εργασίας, κλείσιμο παραθύρων άνοιγμα επεκτάσεων για την εργασία κλπ. Παρακάτω φαίνονται επιλεγμένα και τα 4 παράθυρα με τις αντίστοιχες ονομασίες τους στο εργαλείο.



Εικόνα 59: Το πλαίσιο του εργαλείου UFED Physical Analyzer

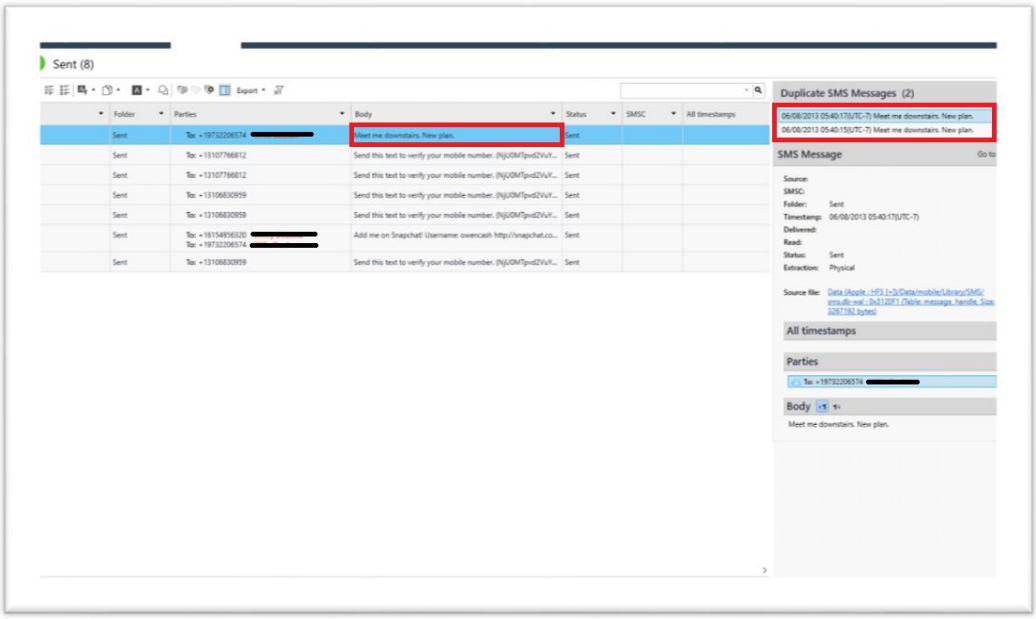
Επιλέγοντας τη καρτέλα Physical από το Δέντρο Εργασίας παρέχονται διάφορες γενικές πληροφορίες στην περιοχή απεικόνισης του εργαλείου ενώ παράλληλα δίνεται η δυνατότητα για επιβεβαίωση της συνάρτησης hash του αντιγράφου ώστε να εξασφαλίσει ο ερευνητής την ακεραιότητα του αντιγράφου του σε σύγκριση με τη πρότυπη συσκευή.



Εικόνα 60: Πληροφορίες συσκευής

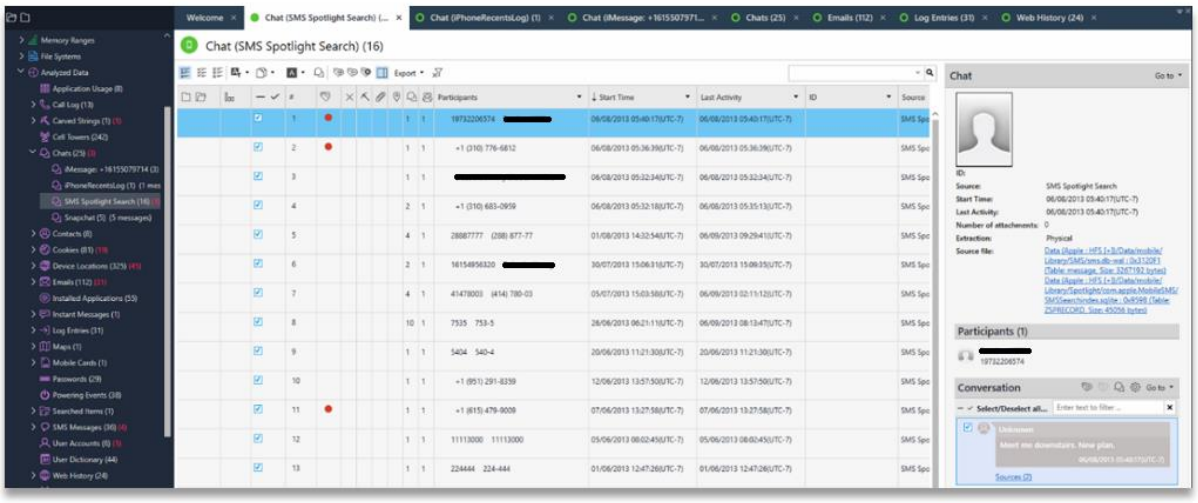
1. Ανάλυση Μηνυμάτων SMS

Το UFED Physical Analyzer μπορεί να βρει όλες τις κλήσεις και όλα τα μηνύματα SMS τα οποία έχει στείλει ένας χρήστης ακόμα και αν εκείνος τα έχει διαγράψει. Επιλέγοντας λοιπόν την καρτέλα SMS Messages, στη παρακάτω εικόνα φαίνεται πως ο χρήστης έχει διαγράψει μηνύματα τα οποία είχε στείλει προηγουμένως και τα οποία αφορούν κάποιο σχέδιο με κάποιον συνεργάτη του.



Εικόνα 61: Καταγραφή μηνυμάτων που εστάλησαν από τη συσκευή με χρήση του εργαλείου UFED Physical Analyzer

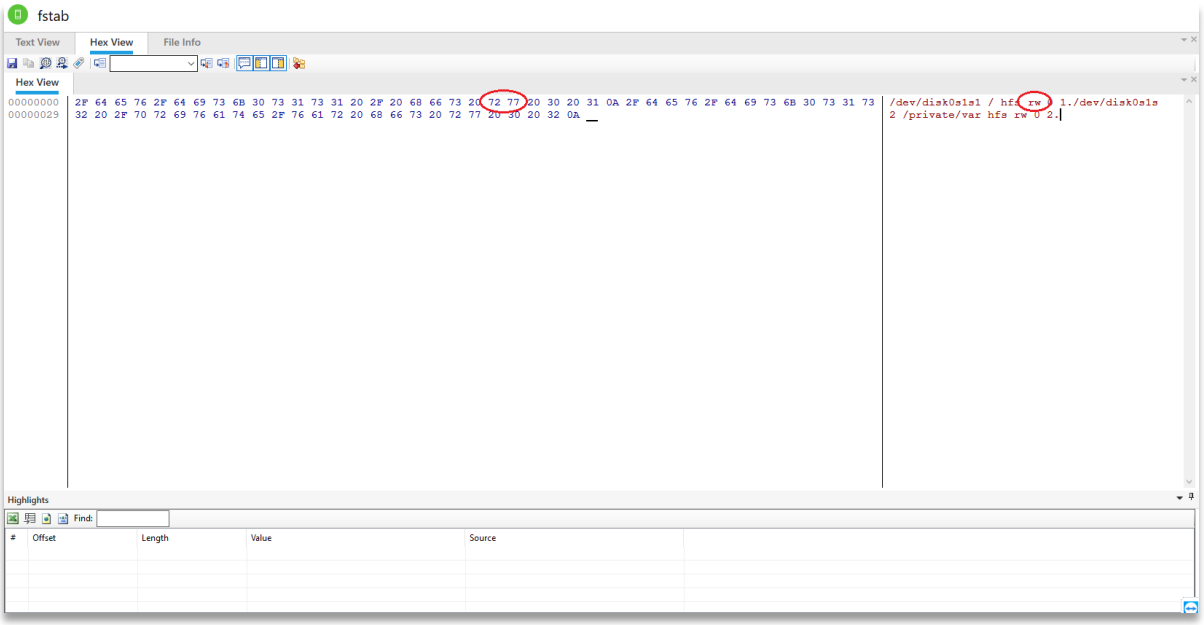
Ωστόσο μια πιο ισχυρή δυνατότητα του εργαλείου UFED Physical Analyzer είναι να μπορεί να φανερώνει σε μια χρονική σειρά όλα τα SMS, διαγεγραμμένα και μη, που έχουν σταλεί από τον χρήστη στη συσκευή.
Η δυνατότητα αυτή του εργαλείου παρέχεται στην καρτέλα «SMS Spotlight Search».



Εικόνα 62: Ανάλυση μηνυμάτων SMS

2. Ανάγνωση αρχείου fstab

Στις δυνατότητες του UFED Physical Analyzer εμπεριέχεται και η δυνατότητα αναγνώρισης μιας συσκευής σε περιπτώσεις που η συσκευή έχει γίνει jailbroken μέσω κάποιου λογισμικού (pangu, ppk κλπ.). Για να το ανακαλύψει ένας ερευνητής αυτό θα πρέπει να μεταβεί στο «Δέντρο Εργασιών» του εργαλείου στην φυσική διεύθυνση /private/etc/fstab. Επιλέγοντας Hex View στο offset 19 θα πρέπει να υπάρχει ο δεκαεξαδικός 72 77 (rw) ο οποίος δηλώνει ότι το σύστημα της συσκευής μπορεί να τροποποιηθεί από οποιονδήποτε χρήστη και άρα η συσκευή λειτουργεί με δικαιώματα root. Τα αποτελέσματα του αρχείου fstab μιας jailbroken συσκευής φαίνονται στο παρακάτω στιγμιότυπο.

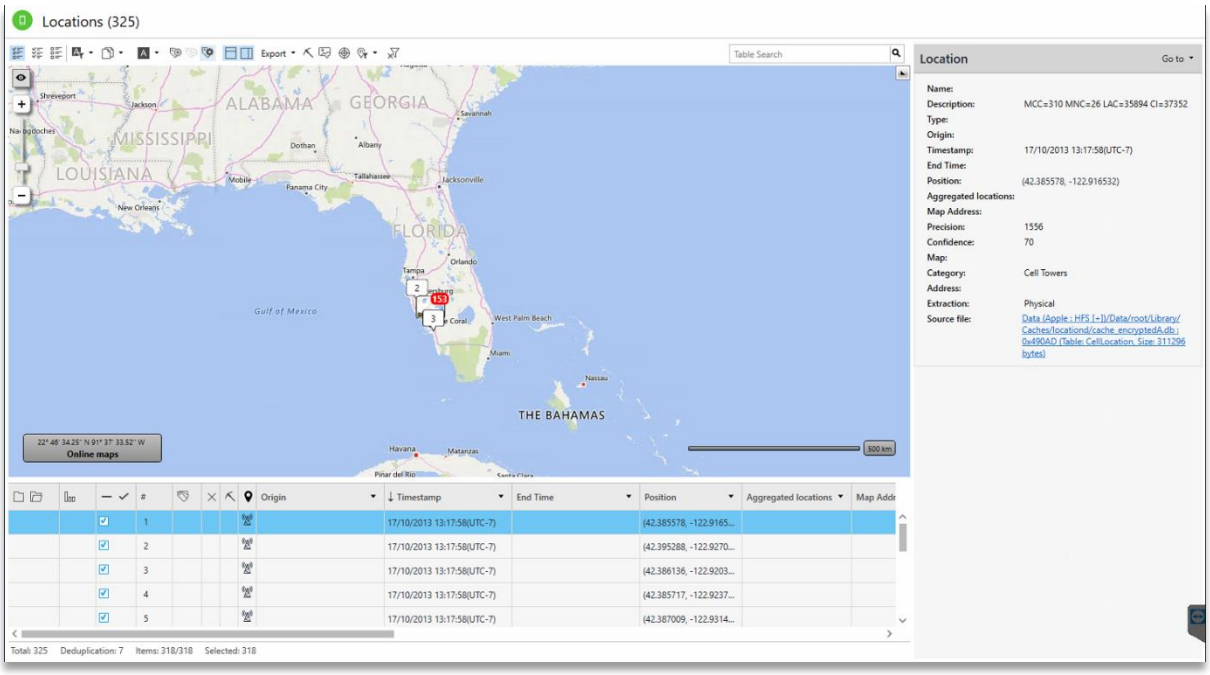


Εικόνα 63: Αναγνώριση Jailbroken συσκευής απο το αρχείο fstab

Αξίζει να σημειωθεί ότι η δυνατότητα αναγνώρισης μιας jailbroken iOS συσκευής μετά την έκδοση iOS 7 δεν είναι δυνατή μέσω του αρχείου fstab ακόμα και αν η συσκευή αυτή είναι Jailbroken. Στο πρακτικό σενάριο που ακολουθεί παρακάτω χρησιμοποιήθηκε Κινητή Συσκευή iOS 7.1.2 η οποία έγινε jailbroken χρησιμοποιώντας το πρόγραμμα Pangu[8].

3. Γεωγραφική Ανάλυση Τοποθεσίας

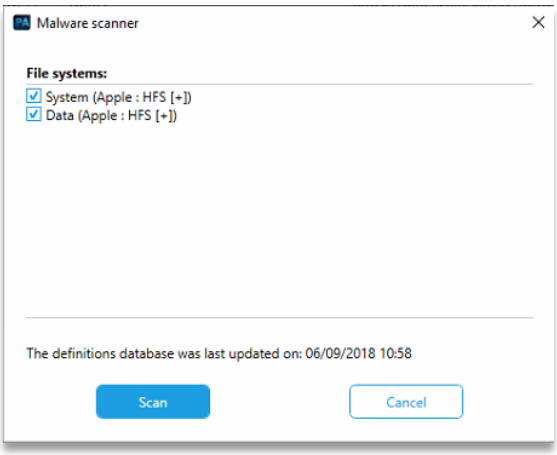
Το UFED Physical Analyzer μπορεί επίσης να δίνει στον ερευνητή μια πιο αναλυτική εικόνα της γεωγραφικής τοποθεσίας όπου χρησιμοποίησε ο αρχικός χρήστης την συσκευή η οποία προκύπτει από τα μεταδεδομένα που γράφηκαν στις εικόνες τις οποίες τράβηξε ο χρήστης κατά την διάρκεια κατοχής της συσκευής. Στο παρακάτω παράδειγμα φαίνεται πως η ανάλυση έχει φανερώσει την τοποθεσία κάποιων φωτογραφιών του χρήστη λόγω χρήσης γεωγραφικής τοποθεσίας τη στιγμή της λήψης τους.



Εικόνα 64: Εύρεση Γεωγραφικής θέσης των λήψεων των φωτογραφιών

4. Σαρωτής Κακόβουλου λογισμικού (Malware Scanner)

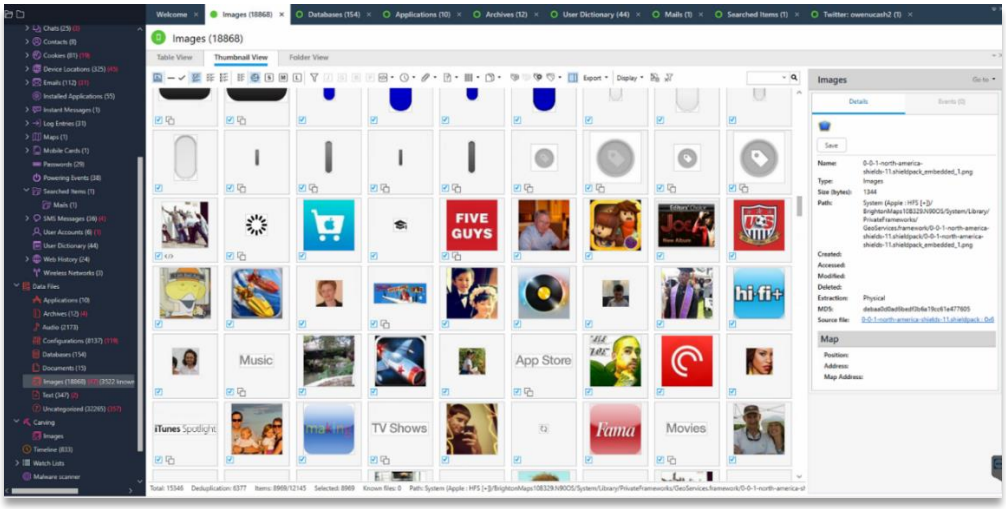
Στα πλεονεκτήματα που προσφέρει το UFED Physical Analyzer είναι και η σάρωση στοιχείων για κακόβουλο λογισμικό. Για να αρχίσει η διαδικασία ο χρήστης απλά πρέπει να επιλέξει την καρτέλα Malware Scanner από το Δέντρο Εργασίας και στη συνέχεια να διαλέξει ποιο σύστημα της Κινητής Συσκευής θέλει να σαρώσει και να πατήσει Scan για να αρχίσει η σάρωση.



Εικόνα 65: Σαρωτής κακόβουλου λογισμικού του εργαλείου Physical Analyzer

5. Ανάκτηση Φωτογραφιών με τεχνική Image Carving

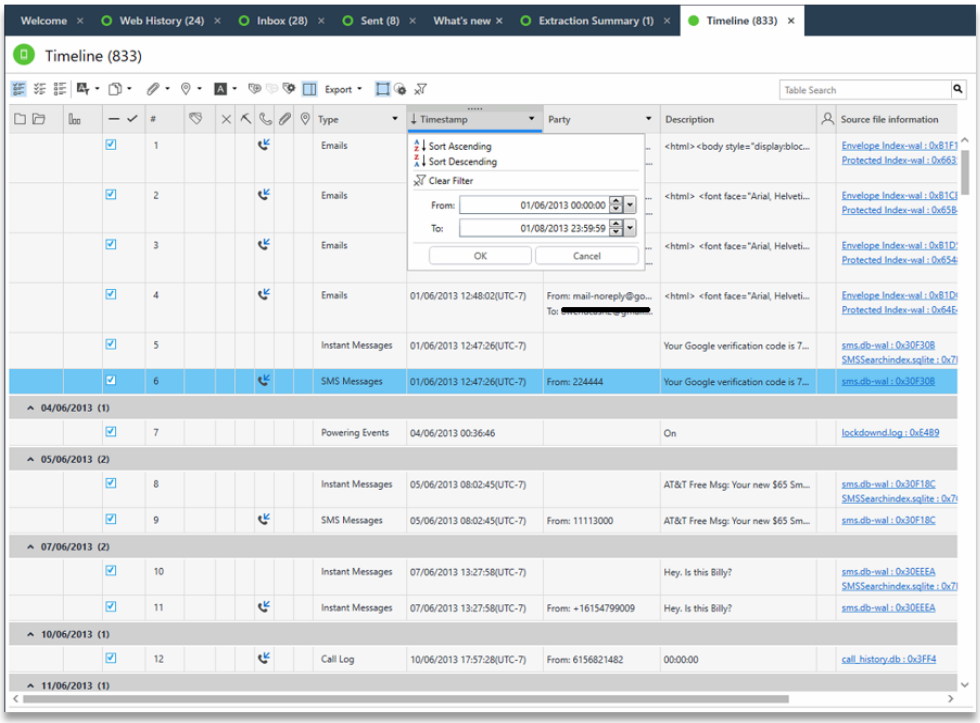
Μια ακόμη δυνατότητα του εργαλείου είναι η ανάλυση και η ανάκτηση φωτογραφιών από δύσκολα ανακτώμενους χώρους της Κινητής Συσκευής όπως είναι οι βάσεις δεδομένων SQLite της Κινητής Συσκευής και η «Μη διευθετημένη περιοχή» δίσκου (Unallocated Space). Επιλέγοντας Carving Images ο χρήστης μπορεί να επιλέξει είτε μια γρήγορη σάρωση είτε μια πλήρη σάρωση η οποία είναι πιο χρονοβόρα ενώ παράλληλα μπορεί να ανακτηθούν ακόμη και μισές φωτογραφίες λόγω κακών «συστάδων» (clusters) του δίσκου στον «Μη διευθετημένο» χώρο της συσκευής.



Εικόνα 66: Ανάκτηση εικόνων χρησιμοποιώντας τις δυνατότητες του εργαλείου

6. Χρονοδιάγραμμα γεγονότων (Timeline)

Άλλη μια ισχυρή δυνατότητα του εργαλείου είναι η ταξινόμηση κατά χρονική στιγμή όλων των γεγονότων που μεσολάβησαν τη χρονική διάρκεια χρήσης της συσκευής από τον κάτοχο της. Στην επόμενη εικόνα παρατηρείται και η δυνατότητα φιλτραρίσματος της ημερομηνίας που συνέβησαν κάποια γεγονότα που πήραν χώρα μεταξύ 1/6/2013 και 1/8/2013.

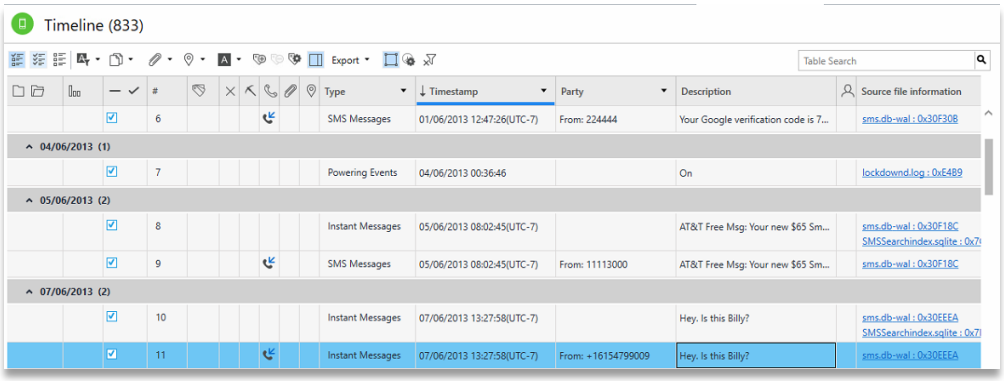


Εικόνα 67: Χρονοδιάγραμμα γεγονότων

Ο πίνακας χρονικής σειράς αποτελείται απο4 βασικές στήλες:

- ✓ Τη στήλη τύπου δεδομένων π.χ. SMS μηνύματα
- ✓ Τη χρονική σφραγίδα που συνέβη το γεγονός
- ✓ Το κύριο μέρος εάν υπάρχει του μηνύματος
- ✓ Η περιγραφή του γεγονότος (στο παράδειγμα μας το περιεχόμενο του μηνύματος)
- ✓ Η τοποθεσία ή η βάση δεδομένων που βρίσκονται τα δεδομένα

Παρακάτω φαίνεται ένα παράδειγμα ενός ευρεθέντος μηνύματος χρησιμοποιώντας τις δυνατότητες του χρονολογίου του εργαλείου:

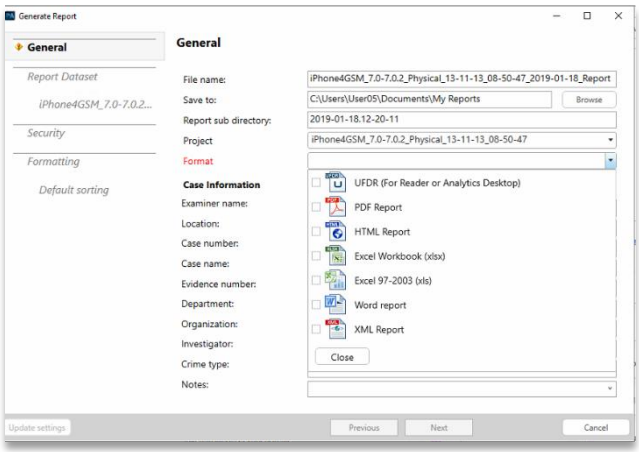


Εικόνα 68: Ανίχνευση μηνυμάτων που εστάλησαν από τη συσκευή

7. Εκτύπωση Αναφοράς

Τέλος στις ισχυρές δυνατότητες του UFED Physical Analyzer περιλαμβάνεται και η δυνατότητα εκτύπωσης όλων των ευρημάτων που αποτέλεσαν πειστήρια κατά την Ψηφιακή Έρευνα σε μια έντυπη αναφορά των μορφών που φαίνονται στο παρακάτω στιγμιότυπο. Να σημειωθεί ότι η δημιουργία αναφοράς από το εργαλείο περιλαμβάνει τα εξής βήματα:

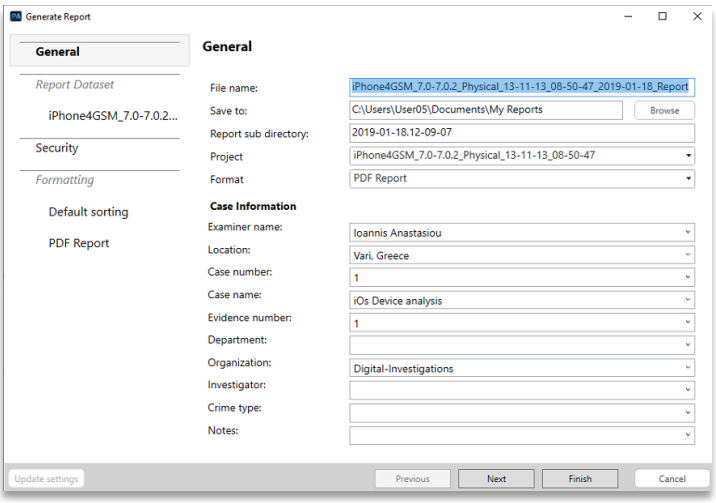
- ❖ Όνομα του αρχείου που θα δημιουργηθεί
  - ✓ Φυσική διεύθυνση στον δίσκο που θα αποθηκευτεί
  - ✓ Όνομα Υποφακέλου
  - ✓ Τίτλος της αναφοράς
- ❖ Μορφή του εντύπου η οποία μπορεί να είναι μια από τις παρακάτω
  - ✓ UFDR
  - ✓ PDF
  - ✓ HTML
  - ✓ XLSX
  - ✓ XLS
  - ✓ DOC
  - ✓ XML
- ❖ Στοιχεία της υπόθεσης όπως:
  - ✓ Όνομα εξεταστή
  - ✓ Τοποθεσία
  - ✓ Αριθμός υπόθεσης
  - ✓ Όνομα Υπόθεσης
  - ✓ Αριθμός πειστηρίου
  - ✓ Τμήμα Εγκληματολογικών Ερευνών
  - ✓ Οργανισμός
  - ✓ Ερευνητής
  - ✓ Τύπος Εγκλήματος



Εικόνα 69: Εξαγωγή αναφοράς απο το εργαλείο

Επιλέγοντας αρχικά τον τύπο του αρχείου μετά εμφανίζεται ένα νέο παράθυρο στο οποίο ο ερευνητής μπορεί να επιλέξει ποια από τα στοιχεία της υπόθεσης που ειπώθηκαν παραπάνω θέλει να

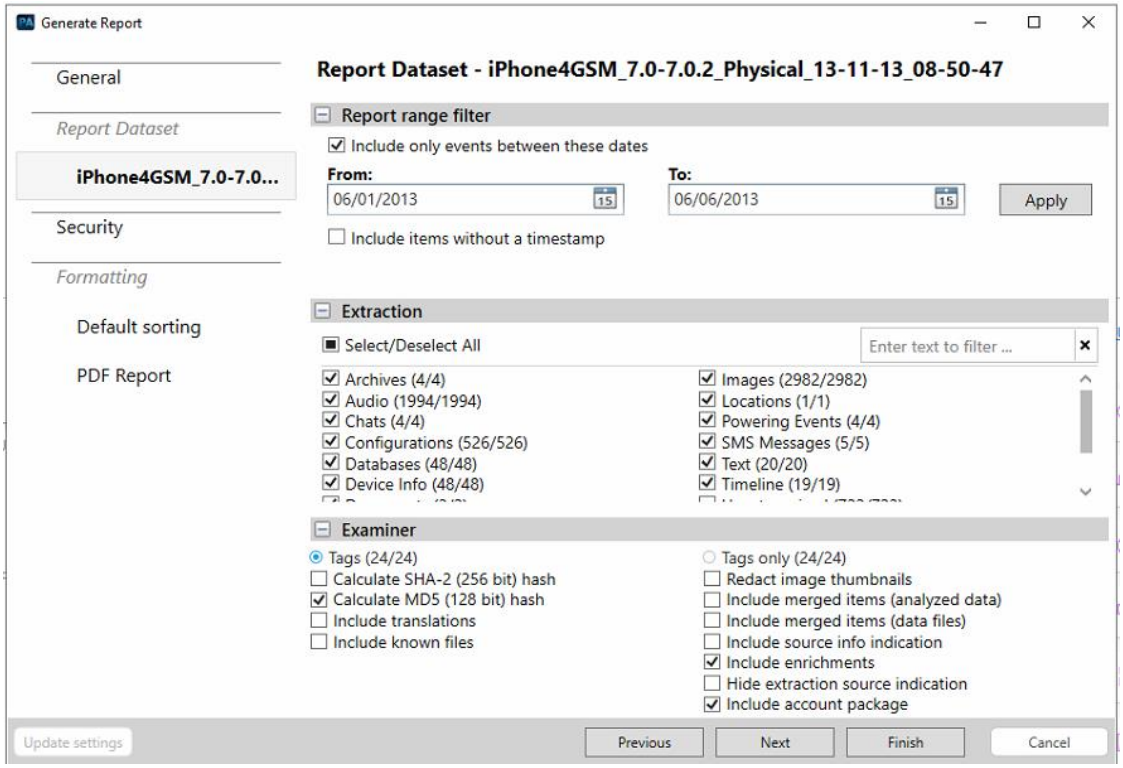
συμπεριλάβει στην αναφορά του. Στο στιγμιότυπο φαίνονται κάποια στοιχεία που συμπληρώθηκαν για την πρακτική άσκηση με το εργαλείο UFED Physical Analyzer της συγκεκριμένης διατριβής.



Εικόνα 70: Συμπλήρωση στοιχείων αναφοράς

Επιλέγοντας "Next" εμφανίζεται νέο παράθυρο στο χρήστη που αποτελείται από το όνομα που έδωσε ο ερευνητής στο προηγούμενο παράθυρο και αφορά το Dataset που θέλει να συμπεριλάβει ο χρήστης στην αναφορά του. Το dataset κυρίως περιλαμβάνει

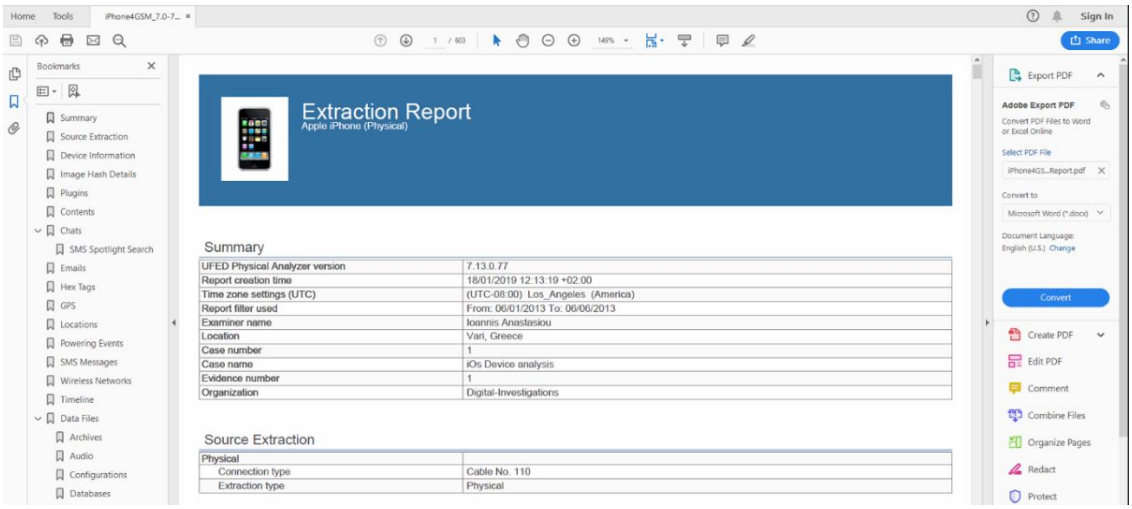
- ✓ Φίλτρο εύρους των ευρημάτων από την ανάλυση
- ✓ Επιλογή των δεδομένων που θέλει να συμπεριλάβει
- ✓ Επιπλέον στοιχεία που θέλει να συμπεριλάβει ο εξεταστής



Εικόνα 71: Επιλογή εισαχθέντων στοιχείων στην αναφορά

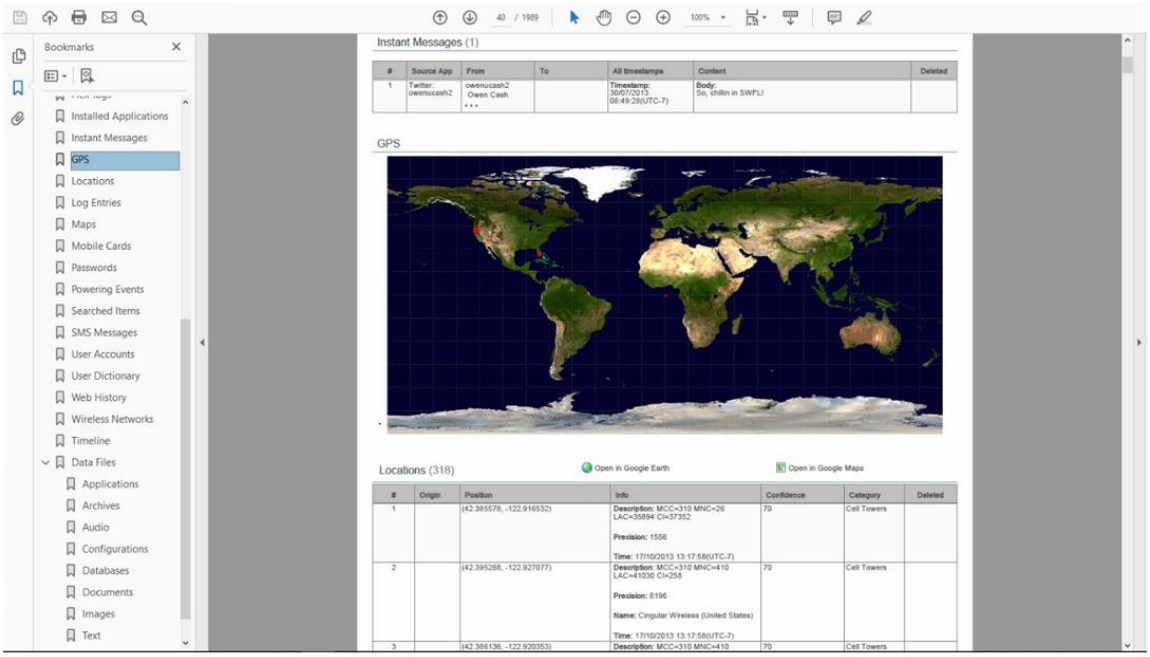
Επιλέγοντας "*Finish*" δημιουργείται η φόρμα αναφοράς στον τύπο που θα επιλέξει ο χρήστης, στη προκειμένη περίπτωση σε PDF και στη συνέχεια ο χρήστης μπορεί να αναγνωρίσει τα στοιχεία που

αποτελούν πειστήρια για την υπόθεση και που επέλεξε να συμπεριλάβει κατά την ανάλυση από το εργαλείο της Cellebrite.
Παρακάτω φαίνεται η φόρμα της αναφοράς που μπορεί να δημιουργήσει για μια υπόθεση το παρόν εργαλείο.



Εικόνα 72: Εκτύπωση Αναφοράς

Τέλος η αναφορά από το εν λόγω εργαλείο εμπεριέχει και στίγματα γεωγραφικής τοποθεσίας υπογραμμισμένα με κόκκινες κουκίδες στην ενότητα “*GPS*” η οποία δίνει μια πιο κατανοητή εικόνα των σημείων που χρησιμοποιήθηκε η συγκεκριμένη Κινητή Συσκευή.



Εικόνα 73: Εκτύπωση γεωγραφικής τοποθεσίας χρήσης της συσκευής

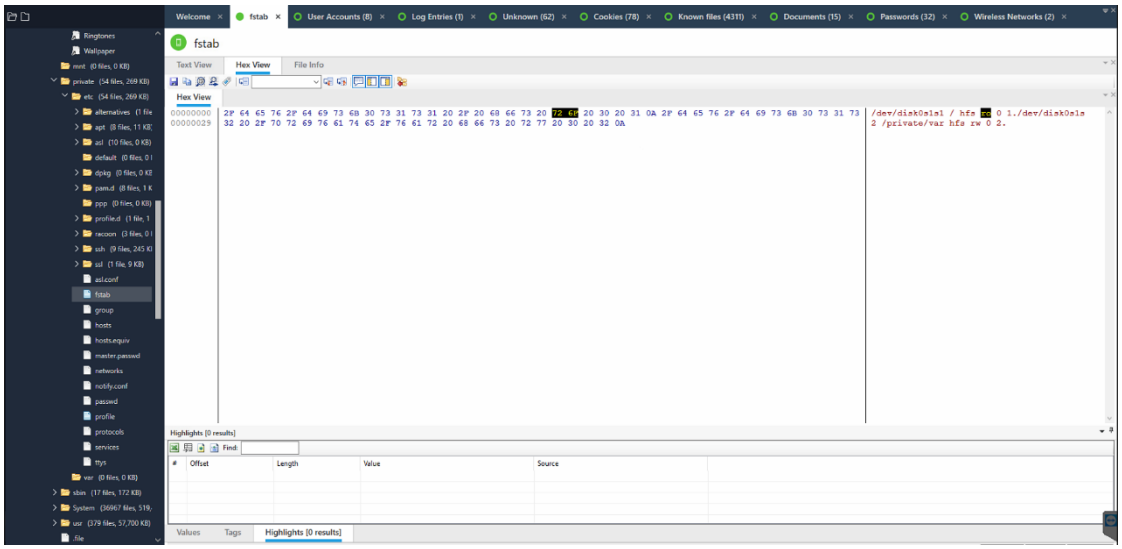
5.4.2. Περίληψη Σεναρίου

Ο Γιάννης ο οποίος μένει μόνιμα στην Κω, εδώ και λίγο καιρό ήθελε να αγοράσει μια φθηνή iOS συσκευή πριν πάει να υπηρετήσει στην Αθήνα την στρατιωτική του θητεία για να την έχει πρόχειρη ώστε να μην του κλέψουν την δική του συσκευή. Έτσι λοιπόν έβαλε τον φίλο του Γιώργο που μένει στον Πειραιά να ψάξει να του βρει μια φθηνή συσκευή. Αυτός με τη σειρά του δοκίμασε τη τύχη του στο Μοναστηράκι όπου και βρήκε έναν πλανόδιο ο οποίος του πούλησε σε τιμή ευκαιρίας ένα iPhone 4. Αφού έστειλε το κινητό στον Γιάννη, εκείνος με τη σειρά του άνοιξε το κινητό να το τσεκάρει αλλά παρατήρησε ότι υπήρχαν προγράμματα όπως το Cydia κλπ. Έτσι λοιπόν απευθύνθηκε στον συνάδελφο του Δημήτρη, ο οποίος ήταν γνώστης Ψηφιακής Εγκληματολογίας και με τη σειρά του αυτός χρησιμοποίησε το πρόγραμμα της Cellebrite UFED Physical Analyzer για να δει αν μπορεί να ανακαλύψει κάτι παραπάνω για την εν λόγω συσκευή.

Διαδικασία που ακολουθήθηκε:

Ξεκινώντας ο Δημήτρης αφού δημιούργησε ένα πιστό αντίγραφο της συσκευής χρησιμοποιώντας την δυνατότητα του UFED Physical Analyzer iOS Advanced Physical Extraction μορφής *UFD* και ακολουθώντας τις οδηγίες που προσφέρει το συγκεκριμένο εργαλείο κατά την ανάκτηση του αντιγράφου, επέλεξε για ανάλυση το εικονικό αντίγραφο της συσκευής επιλέγοντας «Load Evidence» στο αρχικό παράθυρο του εργαλείου. Στη συνέχεια επιλέγοντας το αντίγραφο προς ανάλυση επέλεξε «*Next*» και ένα νέο παράθυρο με τα εργαλεία προς ανάλυση εμφανίστηκε στην οθόνη. Τέλος ο Δημήτρης επιλέγει «*Start Decoding*» για να ξεκινήσει η ανάλυση του αντιγράφου της συσκευής.

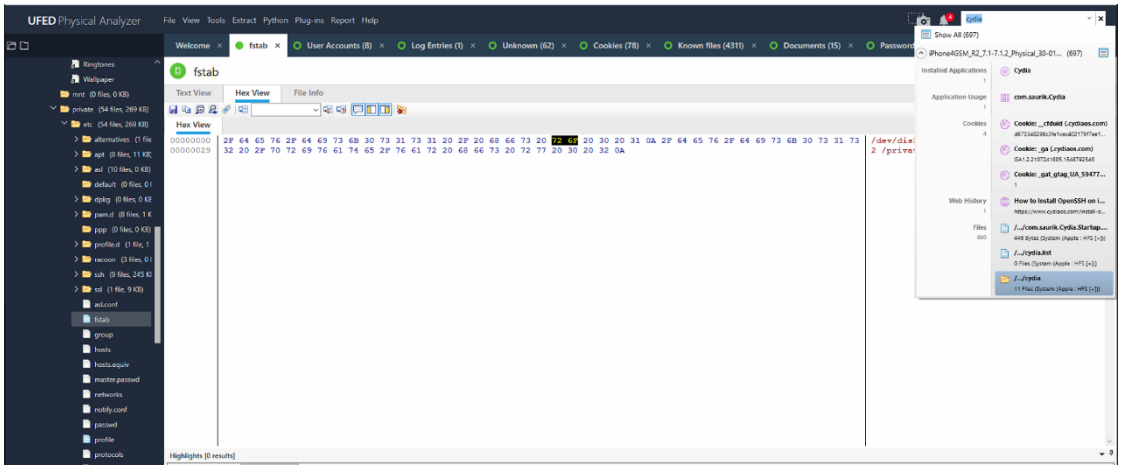
Ένα από τα αρχικά βήματα που ένας ερευνητής μπορεί να κάνει για να ανακαλύψει εάν η συσκευή είναι κλεμμένη και «σπασμένη» δηλαδή Jailbroken είναι να μεταβεί όπως έχει ειπωθεί και προηγουμένως στο αρχείο του συστήματος fstab. Έτσι ο Δημήτρης προκειμένου να ερευνήσει αν το κινητό είναι Jailbroken μετέβηκε στα περιεχόμενα του αρχείου τα οποία φαίνονται στο παρακάτω στιγμιότυπο.



Εικόνα 74: Έλεγχος συσκευής για Jailbreak

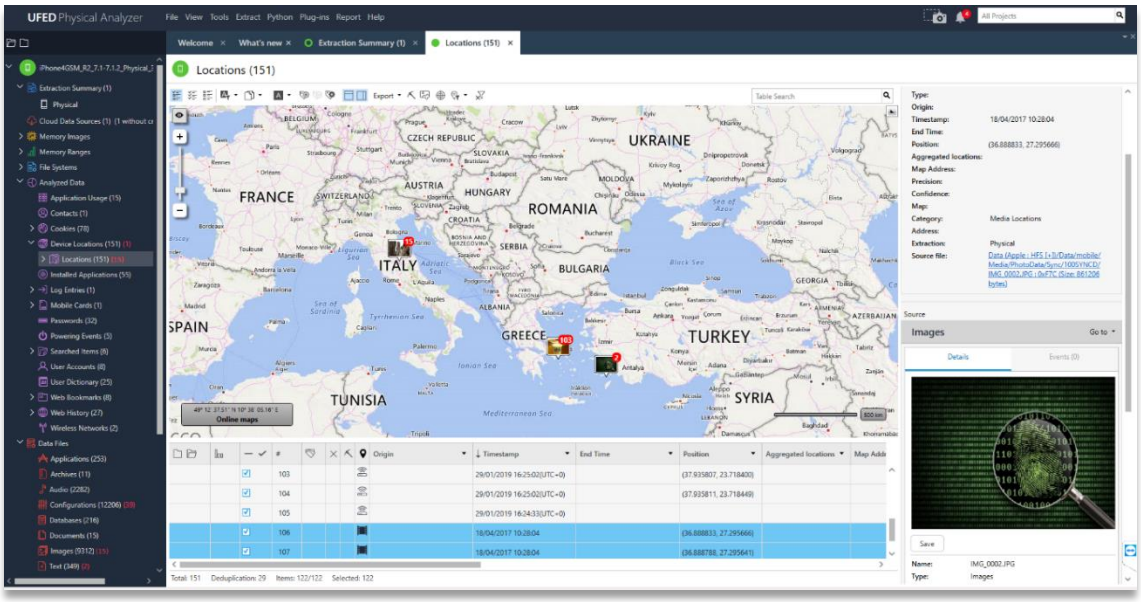
Απο τι παραπάνω πληροφορία φαίνεται στο «Offset 19» πως το σύστημα της συσκευής είναι μορφής «readonly» (ro). Παρολα αυτά η γενική ανάλυση της συσκευής έχει δείξει πως το λειτουργικό της συσκευής ήταν το 7.1.2 κάτι το οποίο επιβεβαιώνει πως πρέπει να γίνει βαθύτερη ανάλυση για να βρεθούν αποδείξεις Jailbreak της συσκευής.

Έτσι ο Δημήτρης χρησιμοποιώντας τη Καρτέλα Αναζήτησης Όλων των εργασιών πληκτρολόγησε την λέξη Cydia η οποία αντιπροσωπεύει τον agent του Pangu που εγκαθίσταται μετά απο Jailbreak μίας συσκευής iOS και πράγματι τα αποτελέσματα απο το εργαλείο φανέρωσαν πως το κινητό δεν είναι αυθεντικό αλλα Jailbroken απο κάποιον επιτήδειο πιθανώς μετά απο κλοπή.



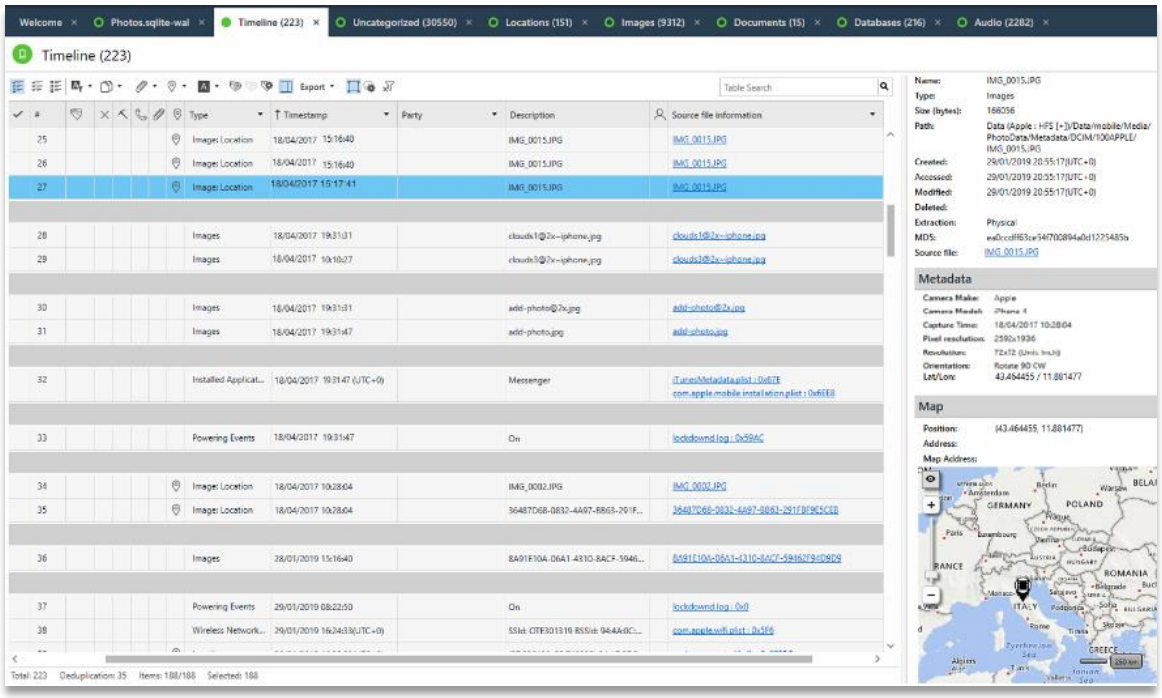
Εικόνα 75 :Εύρεση φακέλου Cydia

Τέλος φως στο τούνελ έριξε και η ανακάλυψη της γεωγραφικής τοποθεσίας των εικόνων που είχαν ληφθεί κατα τη διάρκεια λειτουργίας της συσκευής. Το εργαλείο φανέρωσε τη γεωγραφική τοποθεσία του αρχικού χρήστη της Κινητής Συσκευής η οποία ήταν στην Ιταλία, τη τοποθεσία που αγόρασε το κινητό ο Γιώργος ο φίλος του Γιάννη και τέλος την τοποθεσία του Γιάννη.



Εικόνα 76: Εύρεση τοποθεσίας της συσκευής

Για μια ακόμη πιο ακριβής εικόνα, ο Δημήτρης χρησιμοποίησε τη καρτέλα Timeline του εργαλείου και φιλτράροντας την χρονική σφραγίδα της κάθε φωτογραφίας να δείχνει την ημερομηνία 18/04/2017 το εργαλείο εμφάνισε τα παρακάτω αποτελέσματα.



Εικόνα 77: Χρονοδιάγραμμα Γεγονότων στη συσκευή

6. Επιπρόσθετη Έρευνα και Μελέτη

Σχεδόν κάθε σενάριο που εξετάζεται στο πλαίσιο αυτής της εργασίας καταλήγει ή συνεπάγεται στο ότι μια δικαστική έρευνα ολοκληρώνεται όταν εφαρμόζεται μια σωστή μέθοδος έρευνας και ανάλυσης.

Κατά τη διάρκεια ανάλυσης των παραπάνω εργαλείων διαπιστώθηκε πως τα περισσότερα εργαλεία χρειάζονται να υπάρχει πλήρη πρόσβαση στην συσκευή από τον διοριζόμενο εξεταστή για την υπόθεση. Για παράδειγμα στη συσκευή Android που χρησιμοποιήθηκε για τη πειραματική ανάλυση σε αυτή τη διπλωματική εργασία εγκαταστάθηκε η εφαρμογή KingoRoot και στη συνέχεια χρησιμοποιώντας το εργαλείο ADB έγινε είσοδος στη συσκευή ως χρήστης root και κατόπιν ανάκτηση της εικόνας του συστήματος. Επίσης η συσκευή έπρεπε να λειτουργεί πάλι με δικαιώματα root ώστε να γίνει η σωστή εξαγωγή των δεδομένων χρησιμοποιώντας το εργαλείο Scalpel για φυσική ανάκτηση του συστήματος. Σε ότι αφορά τα εργαλεία Ψηφιακής Εγκληματολογίας για iPhone συσκευές τα περισσότερα εργαλεία ανοιχτής πηγής όπως το εργαλείο Libimobiledevice που χρησιμοποιήθηκε μπορούν να ανακτήσουν μόνο συγκεκριμένη πληροφορία από τις συσκευές όταν το κινητό δεν είναι Jailbroken και είναι ικανά μόνο για λογική ανάκτηση.

Στις προτάσεις για τα παραπάνω εργαλεία με σκοπό τη μελλοντική χρήση τους είναι η επέκταση κώδικα των εργαλείων ώστε αυτά να μπορούν να εκτελούν εκτός από λογική ανάκτηση, και ανάκτηση συστήματος και φυσική όπου χρειάζεται χωρίς να μεταβάλλεται η ακεραιότητα και η κατάσταση της συσκευής από τους ερευνητές. Σε ότι αφορά τα εργαλεία ανοιχτής πηγής όπως το M.A.R.A Framework για τεχνικές Αντίστροφης Μηχανικής σε Κινητές Συσκευές προτείνεται για εξοικονόμηση χρόνου μια πιο αυτοματοποιημένη διαδικασία εκτέλεσης κώδικα χωρίς να χρειάζεται ειδική παραμετροποίηση από τον εξεταστή ώστε να λειτουργούν ορθά κατά τη διαδικασία ανάλυσης κώδικα της συσκευής.

Τέλος, παρόλο που υπάρχουν πολλά που πρέπει να βελτιωθούν, η χρήση εργαλείων ανοικτού κώδικα για την Ψηφιακή Έρευνα και Ανάλυση Κινητών Συσκευών θεωρείται σημαντική. Με το πλεονέκτημα της πρόσβασης στον πηγαίο κώδικα, η χρήση εργαλείων ανοιχτού κώδικα μπορεί να είναι επωφελής για τους ερευνητές Ψηφιακής Εγκληματολογίας στο να χρησιμοποιούν κατάλληλα και άλλα εργαλεία πέρα από τα εμπορικά. Η ανάλυση του πηγαίου κώδικα επιτρέπει στους εξεταστές να γνωρίζουν ακριβώς τι συμβαίνει στη συσκευή προς ανάλυση και πώς, καθώς και να παρουσιάσουν το πρόγραμμα και τον πηγαίο κώδικα στο δικαστήριο κατά τη διάρκεια της δίκης.

7. Επίλογος

Με τις συνεχείς βελτιώσεις στη βιομηχανία των Κινητών Συσκευών, η Ψηφιακή Εγκληματολογία Κινητών Συσκευών έχει εξελιχθεί σε μια ολοένα και πιο αναπτυσσόμενη περιοχή στον τομέα της Ψηφιακής Εγκληματολογίας Υπολογιστών με πολλές προκλήσεις που αντιμετωπίζουν οι εγκληματολόγοι. Όπως αναφέρθηκε παραπάνω, τα πιο αμφισβητήσιμα προβλήματα στη Ψηφιακή 'Ερευνα και Ανάλυση Κινητών Συσκευών είναι η δυνατότητα κάλυψης όλων των τηλεφώνων και συσκευών που είναι διαθέσιμες και η διασφάλιση της ακεραιότητας των αποκτώμενων Ψηφιακών Πειστηρίων. Για την επίλυση αυτών των προβλημάτων απαιτείται μια συμφωνία μεταξύ των εταιρειών και των κατασκευαστών των φορητών συσκευών για την τυποποίηση της διαδικασίας επικοινωνίας μεταξύ Κινητών Συσκευών και εργαλείων Ψηφιακής Εγκληματολογίας καθώς και για την επίλυση ζητημάτων ασφάλειας όπως η ταυτοποίηση ID και η κρυπτογράφηση. Γι' αυτή την περίπτωση, τα εργαλεία που χρησιμοποιούνται για σκοπούς Ψηφιακής Εγκληματολογίας πρέπει να είναι διαθέσιμα μόνο για τις υπηρεσίες επιβολής του νόμου ώστε να αποφευχθεί η κακή χρήση του εργαλείου.

Τα διαθέσιμα σήμερα εργαλεία Ψηφιακής 'Ερευνας και Ανάλυσης μπορούν μεν να λειτουργούν χωρίς σημαντικά προβλήματα και να έχουν επαρκή λειτουργικότητα, ωστόσο, απαιτείται περισσότερη έρευνα για την ανάπτυξη νέων εργαλείων, νέων μεθοδολογιών αλλά και βελτίωση των ήδη διαθέσιμων εργαλείων. Η ταχεία ανάπτυξη της βιομηχανίας κινητής τηλεφωνίας απαιτεί ταχεία ανάπτυξη εργαλείων εγκληματολογικής ανάλυσης για την εκπλήρωση των απαιτήσεων έρευνας, κάλυψης νέων συσκευών και εξασφάλισης της ακεραιότητας των αποδεικτικών στοιχείων. Είναι επίσης σημαντικό οι ερευνητές Ψηφιακής Εγκληματολογίας να κατανοούν τις προδιαγραφές, τις λειτουργίες και τους περιορισμούς των εργαλείων που χρησιμοποιούν.

Στη διπλωματική αυτή εργασία έγινε πειραματική ανάλυση διαφόρων εργαλείων για τη κατανόηση της διαδικασίας Ψηφιακής 'Ερευνας και Ανάλυσης όπως ακριβώς την ακολουθούν οι ψηφιακοί ερευνητές, αναλυτές και εξεταστές σε ένα πραγματικό σενάριο. Τα εργαλεία που χρησιμοποιήθηκαν ήταν το open-source εργαλείο MobSF, τα εργαλεία AFLogical-OSE, libimobiledevice, Scalpel και Autopsy TSK από το περιβάλλον της open-source διανομής Santoku, το εργαλείο M.A.R.A Framework και QARK από το περιβάλλον της εργαστηριακής open-source διανομής Androl4b και τέλος το εμπορικό εργαλείο της Cellebrite UFED Physical Analyzer. Οι συσκευές που χρησιμοποιήθηκαν αντίστοιχα για τους σκοπούς της πειραματικής διαδικασίας της διπλωματικής εργασίας ήταν μια συσκευή Android LG A500 μια συσκευή Android Huawei P10 Lite και μια συσκευή iPhone iOS 4.

Η πειραματική διαδικασία που ακολουθήθηκε είχε ως σκοπό τη κατανόηση της διαδικασίας Ψηφιακής Έρευνας και Ανάλυσης χρησιμοποιώντας τα παραπάνω εργαλεία αλλά και την μελέτη τεσσάρων διαφορετικών σεναρίων Ψηφιακής Εγκληματολογίας τα οποία είχαν ως στόχο να δείξουν τη χρησιμότητα των εργαλείων για κάθε διαφορετική περίπτωση.

Η υπάρχουσα τεχνολογία Κινητών Συσκευών εξελίσσεται με ταχείς ρυθμούς. Ο κλάδος της Ψηφιακής Εγκληματολογίας σχετικά με τις Κινητές Συσκευές θα πρέπει να ενημερώνεται συνέχεια με βάση τα νέα χαρακτηριστικά της κάθε Κινητής Συσκευής που βγαίνει στην αγορά. Για να γίνεται αυτό θα πρέπει τα εργαλεία Ψηφιακής Εγκληματολογίας να αναβαθμίζουν συνέχεια τα χαρακτηριστικά τους με βάση τις νέες απαιτήσεις των Κινητών Συσκευών ακολουθώντας τις πρότυπες μεθόδους Ψηφιακής 'Ερευνας και Ανάλυσης Κινητών Συσκευών.

8. Βιβλιογραφία - Αναφορές

[1] Digital Forensics Research Workshop A Road Map for Digital Forensic Research, 2001

[2] A Practical Guide to Computer Forensics Investigations by DR. DARREN R. HAYES (2015)

[3]Secure your Windows Phone or Windows Mobile device (Knowledge Base of Indiana University https://kb.iu.edu/d/bcja#password)

[4] EPPB: Now Recovering BlackBerry Device Passwords September 29th, 2011 by Andrey Belenko (https://blog.elcomsoft.com/2011/09/recovering-blackberry-device-passwords)

[5]https://www.cellebrite.com/en/home/

[6] Blackberry Forensics NIST Mobile Forensics Workshop (June 2014)

[7] Klaver, C.: Windows mobile advanced forensics. Digital Investigation, 6, Embedded Systems Forensics: Smart Phones, GPS Devices, and Gaming Consoles (2010)

[8] Sasidharan, SatheeshKumar and K.L. Thomas: Blackberry forensics: An agent based approach for database acquisition. In Abraham, Ajith, Jaime Lloret Mauri, JohnF. Buford, Junichi Suzuki, and SabuM. Thampi (editors): Advances in Computing and Communications, volume 190 of CCIS, pages 552-561. Springer Berlin Heidelberg (2011)

[9] Hoog, Andrew and Kyle Ga_aney: iPhone forensics (2009)

[10] Hoog, Andrew: Chapter 6 - android forensic techniques. In Android Forensics Syngress, Boston, (2011)

[11] Yates, Maynard: Practical investigations of digital forensics tools for mobile devices. In 2010 Information Security Curriculum Development Conference, InfoSecCD '10, pages 156-162, New York, NY, USA, 2010. ACM.

[12] Practical Mobile Forensics, Bommisetty, Tamma (2014)

[13] Mobile Device Forensics, Andrew Martin, Joey Niem (2008)

[14] iOS Forensics with OpenSource Tools (2014)

[15] NIST Special Publication 800-101 Revision 1 Guidelines on Mobile Device Forensics (2014)

[16] Santoku 0.5 – Packaged & Delivered (https://santoku-linux.com)

[17] Libimobiledevice Forensic Tool (https://github.com/libimobiledevice)

[18] Scalpel Forensic Tool (https://github.com/sleuthkit/scalpel)

[19] Android Forensic Using Some Open Source Tools by Isaac Mrkaic (2016)

[20] Developing Process for Mobile Device Forensics by Det. Cynthia A. Murphy (2013)

[21]http://www.libimobiledevice.org

[22] Android anti-forensics through a local paradigm by Alessandro Distefano, Gianluigi Me and Francesco Pace (2010)

[23] https://www.phonescoop.com

[24] Jansen, et al., 2007 Guidelines on Cell Phone Forensics

[25] Configuring Dynamic Analyzer with MobSF Android 4.4.2 x86 VirtualBox VM https://github.com/MobSF/Mobile-Security-Framework-MobSF/wiki/11.-Configuring-Dynamic-Analyzer-with-MobSF-Android-4.4.2-x86-VirtualBox-VM

[26] Nightly Installers https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers

[27] wkhtmltopdf converter https://wkhtmltopdf.org