ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Τεχνοοικονομική Διοίκηση και Ασφάλεια Ψηφιακών Συστημάτων»

Μεταπτυχιακή Διπλωματική Εργασία

Βασίλειος Α. Μότσιος

ΜΤΕ 1523

Forensics Analysis for e-Wallet

Επιβλέπων: Κωνσταντίνος Λαμπρινουδάκης

Αναπληρωτής Καθηγητής

Πειραιάς, Μάρτιος 2017

Η σελίδα αυτή είναι σκόπιμα κενή

Forensics analysis for e-Wallet

Διπλωματική Εργασία

Επιτροπή Αξιολόγησης

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

Πειραιάς, Μάρτιος 2017

Αφιερώνεται,

Στη σύμβιο μου Σταυρούλα και στα παιδιά μου Αναστάση και Χρήστο

Για την στήριξη και την αγάπη τους, που αποτελεί αστείρευτη πηγή δύναμης και έμπνευσης σε κάθε μου προσπάθεια.

Βασίλειος Α. Μάτσιος

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Κωνσταντίνο Λαμπρινουδάκη για την ανάθεση, καθοδήγηση και την πολύτιμη βοήθεια του στην εκπόνηση αυτής της διπλωματικής εργασίας. Η εργασία αυτή δεν θα είχε ολοκληρωθεί χωρίς την ουσιαστική συμβολή του.

Επιπλέον, θα ήθελα να ευχαριστήσω τον υπηρεσιακό μου Διευθυντή, Σχη (ΕΠ) κ. Κωνσταντίνο Κουβέλη, για την παρότρυνση και την έμπρακτη βοήθειά του, στη προσπάθειά μου να επιλεγώ για την παρακολούθηση του Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων» του Πανεπιστημίου Πειραιά.

Τέλος, θα ήθελα να ευχαριστήσω τη σύζυγό μου, Σταυρούλα, για την υποστήριξή της όλα αυτά τα χρόνια, που είναι πάντα δίπλα μου και με στηρίζει να πετύχω τους στόχους μου.

Περίληψη

Η κοινωνία της πληροφορίας και οι αλματώδεις τεχνολογικές εξελίξεις δεν θα μπορούσαν να αφήσουν αδιάφορο το χρηματοπιστωτικό τομέα, έναν από τους πλέον δραστήριους και δεκτικούς στην καινοτομία χώρο. Την ίδια ώρα η χρήση συσκευών, που βασίζονται σε Android καθώς και η ανάπτυξη ψηφιακών εφαρμογών για την πραγματοποίηση οικονομικών συναλλαγών είναι εκθετικά αυξητική τα τελευταία χρόνια. Πολλές από αυτές τις εφαρμογές είναι κρίσιμες, καθώς υποστηρίζουν συναλλαγές με τράπεζες (mobile banking), πληρωμές σε καταστήματα (e-Wallet) κ.α. Στην παρούσα διπλωματική εργασία γίνεται μία αναλυτική καταγραφή των τεχνολογιών, που χρησιμοποιούνται από εφαρμογές τύπου «ψηφιακό πορτοφόλι» (e-Wallet), σε έξυπνα τηλέφωνα (smartphone) λειτουργικού συστήματος Android με περιγραφή της αρχιτεκτονικής του υλικού και του λειτουργικού συστήματος. Ακόμη, αναλύονται οι αδυναμίες ασφάλειας καθώς και η μεθοδολογία εντοπισμού πειστηρίων του κλάδου της Ψηφιακής Εγκληματολογίας (Digital Forensics). Τέλος, πραγματοποιείται πειραματική υλοποίηση με βάση τα υπάρχοντα δωρεάν εργαλεία ανάλυσης και παρουσιάζονται τα αποτελέσματα που μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία.

Λέξεις κλειδιά: Ψηφιακό Πορτοφόλι, Έξυπνα Κινητά Android, Ψηφιακά Πειστήρια

Abstract

Information society and the immense technological developments could not leave the financial sector, one of the most active and innovation friendly sectors, indifferent. At the same time the use of Android based devices as well as the development of digital applications for business transactions demonstrates an exponential increase. Many of these applications are crucial, since they facilitate transactions with banks (mobile banking), shop purchases (e-Wallet) etc. This thesis monitors in detail the technologies used by applications like the “digital wallet” (e-Wallet) in Android based smart phones describing at the same time their software architecture and operating system. Furthermore, an analysis of the safety deficiencies and the evidence tracking methodology of the Digital Forensics sector shall be presented. Finally, an experimental implementation is carried out based on the existing analysis tools available and the results that can be used as evidence shall be presented.

Keywords: Digital Wallet, Android Operating System Smartphones, Digital Evidence

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Κεφάλαιο 1ο
Εισαγωγή

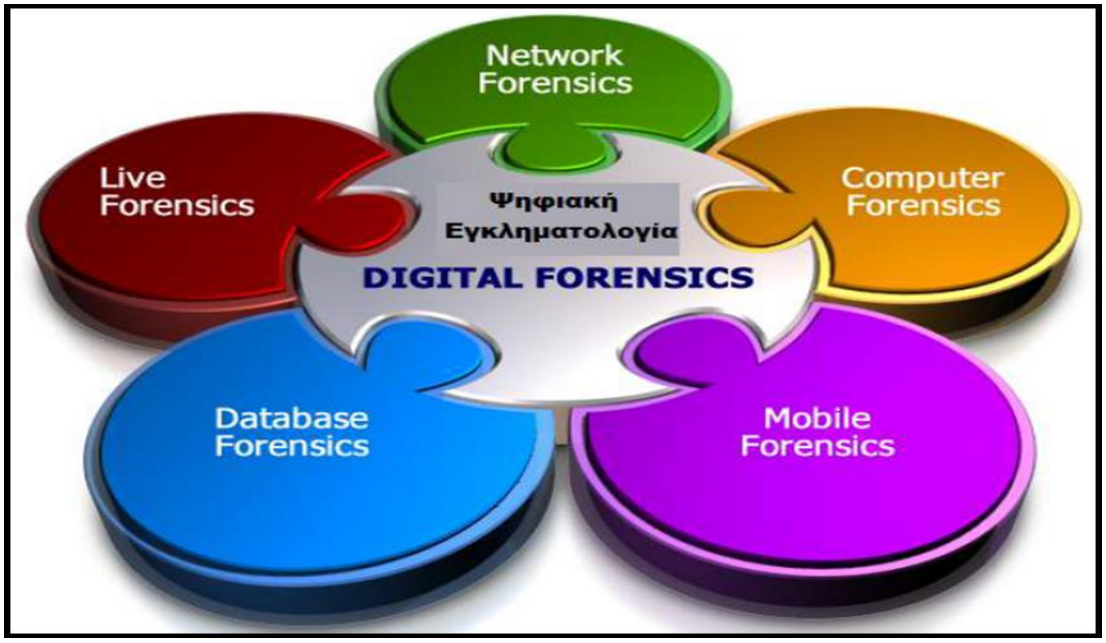
1.1 Αντικείμενο-Πεδίο εφαρμογής

Σήμερα, τα κινητά τηλέφωνα έχουν εξελιχθεί από ένα απλό μέσο επικοινωνίας σε «κινητούς» υπολογιστές με πολύ μεγάλες δυνατότητες. Ειδικότερα, τα έξυπνα τηλέφωνα (smart phones) συγκεντρώνουν λειτουργίες ενός τηλεφώνου και ενός υπολογιστή μαζί. Με την εξάπλωση του διαδικτύου και τις τελευταίες εξελίξεις στον τομέα της ασύρματης επικοινωνίας, τα κινητά τηλέφωνα έχουν αλλάξει ριζικά τη σύγχρονη επικοινωνία και το σημερινό τρόπο ζωής, έτσι ώστε αυτές οι συσκευές να αντικαταστήσουν το συμβατικό πορτοφόλι που διαθέτουν οι άνθρωποι σήμερα, με το αντίστοιχο ψηφιακό «e-Wallet».

Η ραγδαία ανάπτυξη των ψηφιακών συστημάτων και των δικτύων έχει οδηγήσει σε μια νέα εποχή. Άτομα από όλες τις ηλικίες χρησιμοποιούν διαρκώς κάθε είδους ψηφιακή συσκευή, για λόγους είτε επαγγελματικούς, είτε ψυχαγωγίας. Στις μέρες μας, τα παιδιά μαθαίνουν να χειρίζονται υπολογιστικές συσκευές και να πλοηγούνται στο διαδίκτυο από μικρή ηλικία. Ωστόσο, η εξάπλωση του ψηφιακού κόσμου έδωσε την δυνατότητα και την ευκαιρία σε ορισμένους επιτήδειους να διαπράττουν εγκλήματα και άλλες παράνομες δραστηριότητες. Οι κίνδυνοι ελλοχεύουν τόσο για τους απλούς χρήστες, οι οποίοι συχνά πέφτουν θύματα λόγω της ελλιπούς γνώσης τους, με αποτέλεσμα να μην μπορούν να προστατευθούν από κακόβουλες ενέργειες, όσο και για τις μεγάλες εταιρίες, τράπεζες, δημόσιους και ιδιωτικούς οργανισμούς, για τους οποίους, τις περισσότερες φορές, οι επιπτώσεις μιας εγκληματικής ενέργειας μπορεί να είναι καταστροφικές.

Για την αντιμετώπιση της νέας γενιάς εγκλημάτων και των διαφόρων παρανομιών, που διαπράττονται με τη χρήση της ψηφιακής τεχνολογίας, είναι απαραίτητη η ανάπτυξη ενός καινούριου τρόπου έρευνας, που θα καλύπτει τις απαιτήσεις και τις ιδιαιτερότητες του ψηφιακού κόσμου. Η ύπαρξη νομοθετικού πλαισίου με τη θέσπιση νέων νόμων, που θα κολάζει και θα καταπολεμά τη διάπραξη παράνομων δραστηριοτήτων μέσα στο χώρο αυτό είναι επίσης αναγκαία. Απόρροια των παραπάνω, είναι η ανάπτυξη της νέας σχετικά

επιστήμης της «**Ψηφιακής Εγκληματολογίας**» (**Digital Forensics**), η οποία παρέχει νέες, επιστημονικά τεκμηριωμένες, μεθόδους για την απόκτηση, διατήρηση και καταγραφή ψηφιακών αποδεικτικών στοιχείων, κατά τη διάρκεια μιας έρευνας σε υπολογιστικές συσκευές ή συστήματα. Η απόκτηση των στοιχείων αυτών πρέπει να διεξάγεται με τέτοιο τρόπο ώστε να διασφαλίζεται η ακεραιότητά τους και η αποδεικτική τους αξία, και να μπορούν να γίνουν αποδεκτά, ως πειστήρια σε μια νομική διαδικασία.



Εικόνα 1.Συνιστώσες της Ψηφιακής Εγκληματολογίας

1.2 Παρούσα κατάσταση

Στη σημερινή εποχή, η ζωή των ανθρώπων έχει κατακλυστεί από τις νέες ψηφιακές τεχνολογίες, οι οποίες έχουν συντελέσει στη ριζική αλλαγή της καθημερινότητας και έχουν προκαλέσει εξάρτηση από τα ψηφιακά συστήματα και τα δίκτυα. Συσκευές με υπολογιστικές ικανότητες έχουν γίνει απαραίτητες για το μέσο άνθρωπο, ενώ η σύνδεση σε κάποιο δίκτυο αποτελεί συνήθεια αλλά και αναγκαιότητα για μερικούς. Επίσης, η πλειοψηφία των πληροφοριών και υπηρεσιών, που παράγονται κάθε μέρα είναι σε ψηφιακή μορφή και ελάχιστες είναι σε κάποια άλλη, για παράδειγμα έντυπη. Όλα αυτά έχουν ως αποτέλεσμα τη συνεχή μεταφορά πληροφοριών μέσω καλωδίων ή κυμάτων και τη καταγραφή προσωπικών ή και ευαίσθητων δεδομένων των χρηστών ανά πάσα στιγμή.

Όμως, η χρήση των ψηφιακών συσκευών και των δικτύων δε γίνεται πάντα με ευσυνείδητο τρόπο. Η εξέλιξη της τεχνολογίας δημιούργησε ένα νέο περιβάλλον, μέσα στο οποίο κάποιοι βρήκαν πρόσφορο έδαφος για να εξελίξουν τις παράνομες δραστηριότητές τους. Παραδοσιακά εγκλήματα, όπως η κλοπή ή η απάτη, μπορούν να γίνουν και μέσω υπολογιστή, αλλά και νέα εγκλήματα έκαναν την εμφάνισή τους εκμεταλλευόμενα τις νέες ψηφιακές συνθήκες. Οι νέες αυτές απειλές θέτουν σε κίνδυνο και τους απλούς χρήστες αλλά κυρίως τις επιχειρήσεις, τους οργανισμούς, το κράτος και τις κρίσιμες υποδομές του, προκαλώντας οικονομικό, κοινωνικό ή και πολιτικό κόστος.

Η χρήση του διαδικτύου και η καθιέρωσή του ως του κατεξοχήν μέσου για την διεκπεραίωση ποικίλλων δραστηριοτήτων του ανθρώπου, προσφέρουν πολλές ευκαιρίες στους επιτήδειους για την εκτέλεση μη θεμιτών πράξεων. Σε αυτό συντείνουν και η ανωνυμία που προσφέρεται, αλλά και η ευελιξία δράσης ουσιαστικά οπουδήποτε, παρέχοντας ένα πέπλο προστασίας στους κακόβουλους χρήστες. Ένα από τα πιο διαδεδομένα εγκλήματα στον κυβερνοχώρο είναι η υποκλοπή στοιχείων πιστωτικών καρτών. Επίσης, αρκετά συχνό φαινόμενο είναι η παράνομη πρόσβαση στα υπολογιστικά συστήματα, η οποία μπορεί να διαχωριστεί σε «cracking» ή σε «hacking». Η διαφορά τους έγκειται στο ότι στην πρώτη περίπτωση στόχος είναι το οικονομικό όφελος, ενώ στην δεύτερη η περιέργεια και η ευχαρίστηση.

Συνεπώς, η λήψη κατάλληλων μέτρων ασφαλείας είναι κρίσιμη και επιτακτική, για την προφύλαξη των χρηστών από τέτοιου είδους απειλές. Ωστόσο, στην πλειοψηφία των περιπτώσεων που έχει πραγματοποιηθεί ένα περιστατικό ασφαλείας, εκτός από την αποκατάσταση του συστήματος, κρίνεται αναγκαίο και επιτακτικό να εντοπιστούν οι δράστες, προκειμένου να οδηγηθούν στην δικαιοσύνη. Με δεδομένο ότι κάθε πράξη αφήνει πάντα ίχνη, σημασία έχει να μπορούν αυτά να εντοπιστούν και να αναγνωριστούν, ώστε να αποτελέσουν αποδεικτικά στοιχεία εναντίον του δράστη για το έγκλημα που διέπραξε.

Ωστόσο, η συλλογή αποδείξεων, που θα αποτελέσουν τα πειστήρια για τα εγκλήματα που συνδέονται με τις ψηφιακές συσκευές, δεν είναι εύκολη διαδικασία και αποτελεί μια νέα πρόκληση για τις διωκτικές αρχές, τη δικαιοσύνη και τον ακαδημαϊκό τομέα, λόγω των συνεχώς μεταβαλλόμενων

χαρακτηριστικών του ψηφιακού περιβάλλοντος και της διαρκούς εξέλιξής του. Επομένως, η αντιμετώπισή τους με τις γνωστές παραδοσιακές μεθόδους είναι ανέφικτη και λόγω της ιδιαιτερότητας του ψηφιακού κόσμου, αλλά και λόγω της απαίτησης από νομικής πλευράς να διασφαλιστούν η ακεραιότητα και η αξιοπιστία των συλλεχθέντων ηλεκτρονικών στοιχείων. Αυτήν την πρόκληση έρχεται να αντιμετωπίσει και να διεκπεραιώσει η επιστήμη της «Ψηφιακής Εγκληματολογίας» (Digital Forensics).

1.3 Δομή της διπλωματικής εργασίας

Η παρούσα εργασία διαρθρώνεται σε εννέα κεφάλαια, όπου στα πρώτα τέσσερα αναπτύσσονται θέματα που έχουν να κάνουν με τις εφαρμογές ψηφιακού πορτοφολιού στα κινητά και στα επόμενα πέντε αναλύονται θέματα ψηφιακής εγκληματολογίας στα κινητά καθώς και το πρακτικό μέρος της εργασίας. Αναλυτικότερα:

Στο πρώτο κεφάλαιο, δίδεται μια σύντομη εισαγωγή στο θέμα που πραγματεύεται η διπλωματική εργασία, ενώ στο δεύτερο γίνεται μια σύντομη παρουσίαση εφαρμογών e-Wallet σε λειτουργικό σύστημα Android.

Στο τρίτο κεφάλαιο, παρουσιάζεται η καταγραφή των τεχνολογιών που χρησιμοποιεί η υπηρεσία e-Wallet και στο τέταρτο κεφάλαιο μια διεξοδική ανάλυση των αδυναμιών ασφάλειας.

Στο πέμπτο κεφάλαιο, έχουμε την εισαγωγή στη Ψηφιακή Εγκληματολογία σε κινητά τηλέφωνα, ενώ στο έκτο κεφάλαιο αναπτύσσεται η μεθοδολογία για την υλοποίηση πειραμάτων.

Τέλος, τα δύο τελευταία κεφάλαια αναφέρονται στη βιβλιογραφία που χρησιμοποιήθηκε και στο Παράρτημα «Α» απεικονίζονται τα αποτελέσματα της χρήσης των προγραμμάτων.

Κεφάλαιο 2ο
E-Wallet- Android

2.1 Νέα τραπεζικά Προϊόντα

Ο Χρηματοπιστωτικός τομέας υφίσταται τις τελευταίες δεκαετίες, δραστικές διαρθρωτικές, οργανωτικές και τεχνολογικές αλλαγές στη δομή και τη λειτουργία του. Είναι κοινή διαπίστωση ότι το κέντρο βάρους των τραπεζικών εργασιών έχει πλέον μετακινηθεί από γραφειοκρατικές και διοικητικές λειτουργιές, σε εμπορικές δραστηριότητες και σε εξυπηρέτηση και προσέλκυση πελατών.

Ως επακόλουθο, οι νέες τεχνολογίες πληροφορικής και επικοινωνιών να εξελίσσονται σε δομικά συστατικά για την ανάπτυξη πληθώρας νέων τραπεζικών προϊόντων, όπως το **e-Wallet**, web banking, mobile banking, smart cards, με στόχο την ταχύτερη, απλούστερη και αποδοτικότερη ικανοποίηση των ολοένα και αυξανόμενων καταναλωτικών αναγκών.

Χαρακτηριστικό παράδειγμα αποτελούν οι Σκανδιναβικές χώρες και οι ΗΠΑ, όπου συντελείται μια συνεχόμενη αύξηση του αριθμού των εικονικών τραπεζών, οι οποίες δραστηριοποιούνται αποκλειστικά μέσω διαδικτύου [1].

Το ψηφιακό πορτοφόλι είναι μία καινοτόμα τεχνολογικά εφαρμογή (app) προεγκατεστημένη στα περισσότερα σύγχρονα smartphones (Passbook, Google-Wallet, Windows Wallet, PassWallet, Passes). Στόχος του είναι να συγκεντρώνει στο κινητό του καταναλωτή σε ψηφιακή μορφή πλαστικές loyalty cards, χάρτινα κουπόνια, προπληρωμένες κάρτες, δωροεπιταγές, κάρτες μέλους, εισιτήρια, κάρτες επιβίβασης προσφέροντας πρωτοποριακές λειτουργίες. Το κόστος και ο χρόνος δημιουργίας και διανομής των καρτών εκμηδενίζεται και παρέχεται η δυνατότητα διαφοροποίησής τους, ακόμα και μετά τη διανομή τους μέσω ειδικών ειδοποιήσεων (push notifications). Ο χρήστης με αυτό τον τρόπο, γίνεται δέκτης μιας σειράς καινοτόμων υπηρεσιών σε μια μόνο συσκευή, κάτι που στο πρόσφατο παρελθόν όχι μόνο δεν είχε αυτήν τη δυνατότητα, αλλά ενδεχομένως αγνοούσε και την ύπαρξη τους.

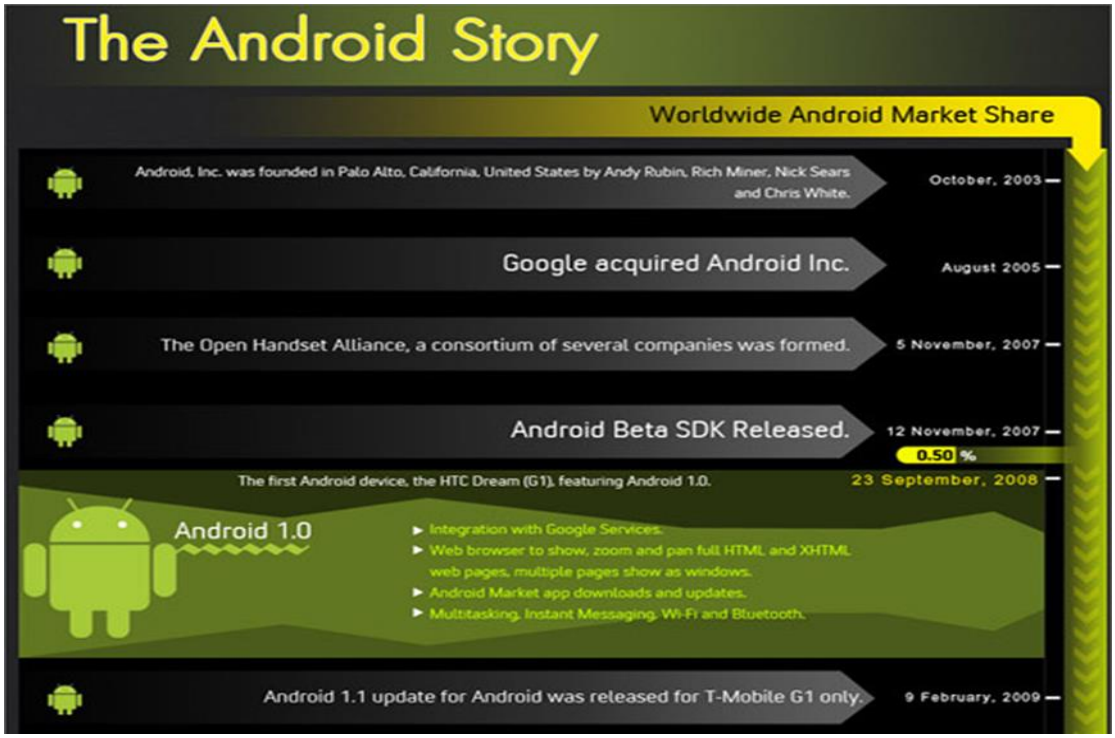
Εικόνα 2. Google-Wallet

Έτσι η επιχείρηση βρίσκεται σε διαρκή επικοινωνία με τον καταναλωτή στέλνοντας στο κινητό του προσφορές και ειδοποιήσεις για υπηρεσίες και προϊόντα. Διανέμονται απλά μέσω web links, email, SMS, IM, Social Media ή ακόμα και σε έντυπη μορφή σαρώνοντας το αντίστοιχο QR code απευθείας από το ψηφιακό πορτοφόλι. Με αυτό τον τρόπο, η κάρτα αποθηκεύεται στο smartphone του καταναλωτή ανεξάρτητα από τον τύπο του [2].

2.2 Λειτουργικό Σύστημα Android

2.2.1 Γενικά

Στο πλαίσιο της παρούσας εργασίας θα επικεντρωθούμε στην εξέταση συσκευής «έξυπνου» κινητού τηλεφώνου, με εγκατεστημένο το λειτουργικό σύστημα Android, το οποίο έκανε την εμφάνισή του το Νοέμβριο του 2007. Πρόκειται για ένα λειτουργικό σύστημα που συναντάται κυρίως σε ενσωματωμένα συστήματα, όπως είναι τα κινητά τηλέφωνα, τα tablet αλλά και άλλες κινητές συσκευές. Είναι σχεδιασμένο να συνυπολογίζει τους περιορισμούς στην τροφοδοσία των συσκευών που το φιλοξενεί, καθώς επίσης και τις εφαρμογές που εκτελούνται σε αυτό.



Εικόνα 3. Android history

Είναι ένα λειτουργικό σύστημα ανοιχτού κώδικα, που επιπροσθέτως διαθέτει και ένα σύνολο εργαλείων ανάπτυξης και διατίθεται δωρεάν. Ο πυρήνας του Android είναι βασισμένος στον πυρήνα του Linux. Αποτελεί ένα αρκετά αξιόπιστο λειτουργικό σύστημα καθώς διαθέτει όλα τα χαρακτηριστικά ασφαλείας του Linux και όλες τις διαχειριστικές τεχνικές μνήμης και επεξεργαστή. Επιπλέον επειδή το Android, αλλά και το Linux, είναι λογισμικά ανοιχτού κώδικα, προσαρμόζεται σχετικά εύκολα στις σημερινές ανάγκες και σε διαφορετικής προέλευσης υλικό. Ενδεικτικό παράδειγμα αποτελούν οι διεπαφές χρήστη που παρέχουν οι πάροχοι συσκευών Android [3].

Ο κυριότερος λόγος που επελέγη το Android για τις ανάγκες της εργασίας είναι ότι αποτελεί μια πλατφόρμα, που συναντάται περισσότερο από οποιαδήποτε άλλη στις κινητές συσκευές. Το μερίδιο του Android στην αγορά κινητών συσκευών αγγίζει, όπως φαίνεται στην Εικόνα 4, το υψηλότατο ποσοστό του 85% έναντι των ανταγωνιστών του. Ανεπιφύλακτα, μπορούμε να πούμε ότι αποτελεί το πιο δημοφιλές λειτουργικό σύστημα κινητών συσκευών σήμερα. Αξίζει να σημειωθεί ότι καθημερινά ενεργοποιούνται περίπου εννιακόσιες χιλιάδες συσκευές Android παγκοσμίως.

Worldwide Smartphone Shipments by OS, Market Share, and Annual Growth (shipments in millions)							
Platform	**2016 Shipment Volume***	**2016 Market Share***	**2016 YoY Growth***	**2020 Shipment Volume***	**2020 Market Share***	**2020 YoY Growth***	**5 Year CAGR***
Android	1,228.8	85.0%	5.2%	1,464.7	85.6%	4.2%	4.6%
iOS	206.1	14.3%	-11.0%	243.6	14.2%	2.5%	1.0%
Windows Phone	6.1	0.4%	-79.1%	1.0	0.1%	-19.3%	-48.6%
Others	4.5	0.3%	-50.0%	1.0	0.1%	-7.3%	-35.3%
Total	**1,445.4**	**100.0%**	**0.6%**	**1,710.3**	**100.0%**	**4.8%**	**3.5%**
Source: IDC Worldwide Quarterly Mobile Phone Tracker, November 29, 2016							

* **Table Note:** All figures are forecast projections.

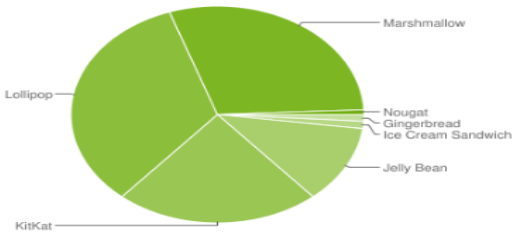
Εικόνα 4.Μερίδιο αγοράς Android συσκευών για το 2016

2.2.2 Εκδόσεις Android

Η πρώτη εμπορική έκδοση του Android χρονολογείται τον Σεπτέμβριο του 2008. Έκτοτε έχει περάσει από πολλές εκδόσεις οι οποίες έχουν διορθώσει ατέλειες και έχουν προσθέσει μια σειρά νέων χαρακτηριστικών. Στην Εικόνα 5 βλέπουμε μια σύντομη ανασκόπηση στις διάφορες εμπορικές εκδόσεις του λειτουργικού συστήματος έως σήμερα.

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	1.1%
4.1.x	Jelly Bean	16	4.0%
4.2.x		17	5.9%
4.3		18	1.7%
4.4	KitKat	19	22.6%
5.0	Lollipop	21	10.1%
5.1		22	23.3%
6.0	Marshmallow	23	29.6%
7.0	Nougat	24	0.5%
7.1		25	0.2%

Data collected during a 7-day period ending on January 9, 2017.
Any versions with less than 0.1% distribution are not shown.



Εικόνα 5. Εκδόσεις του λογισμικού Android

2.2.3 Αρχιτεκτονική

Η αρχιτεκτονική του Android (Εικόνα 6), περιλαμβάνει τα εξής επίπεδα, ξεκινώντας από το ψηλότερο και καταλήγοντας στο χαμηλότερο [4]:

Επίπεδο Εφαρμογών (Applications): Το Android είναι εξαρχής εφοδιασμένο με ένα σύνολο από βασικές εφαρμογές που περιλαμβάνουν ένα email client, ένα πρόγραμμα για SMS μηνύματα, ημερολόγιο, χάρτες (Google Maps), περιηγητή ιστού, πρόγραμμα για δομημένη αποθήκευση των επαφών και άλλα. Όλες οι εφαρμογές είναι γραμμένες στη γλώσσα προγραμματισμού Java.

Επίπεδο Πλαισίου Εφαρμογών (Applications Framework): Παρέχοντας μια ανοικτή πλατφόρμα ανάπτυξης, το Android προσφέρει στους προγραμματιστές την δυνατότητα να κατασκευάσουν νέες και καινοτόμες εφαρμογές. Οι προγραμματιστές αφήνονται ελεύθεροι να εκμεταλλευτούν πλήρως το hardware της συσκευής, να έχουν πρόσβαση σε υπηρεσίες εντοπισμού θέσης, να τρέξουν υπηρεσίες στο background, να θέσουν χρονοδιακόπτες για εμφάνιση ειδοποιήσεων και πολλά άλλα. Επίσης έχουν πλήρη πρόσβαση στο ίδιο πλαίσιο από APIs που έχουν οι βασικές εφαρμογές του Android. Η αρχιτεκτονική είναι διαμορφωμένη με τέτοιο τρόπο που κάθε εφαρμογή μπορεί να χρησιμοποιήσει τις δυνατότητες μιας άλλης και επίσης δίνει την δυνατότητα στον χρήστη να αλλάξει τα συστατικά κάθε εφαρμογής.

Κάτω από το πλαίσιο των εφαρμογών υπάρχει ένα σύστημα από υπηρεσίες και συστήματα τα οποία περιλαμβάνουν:

- Ένα σύνολο από γραφικά στοιχεία (**Views**), για την δημιουργία γραφικού περιβάλλοντος συμπεριλαμβανομένων λιστών (**lists**), πλεγμάτων (**grids**), κουτιών κειμένου (**text boxes**), πλήτρων (**buttons**) και άλλων.

- Ένα διαχειριστή περιεχομένου (**Content Manager**), ο οποίος επιτρέπει στις εφαρμογές την πρόσβαση σε δεδομένα άλλων εφαρμογών ή τον διαμοιρασμό των δικών τους δεδομένων με άλλες εφαρμογές.

• Ένα διαχειριστή πόρων (**Resource Manager**), για την πρόσβαση στους πόρους, όπως strings, εικόνες, layout files.

• Έναν διαχειριστή ειδοποιήσεων (**Notification Manager**), ο οποίος επιτρέπει την προβολή ειδοποιήσεων στην μπάρα κατάστασης (**status bar**).

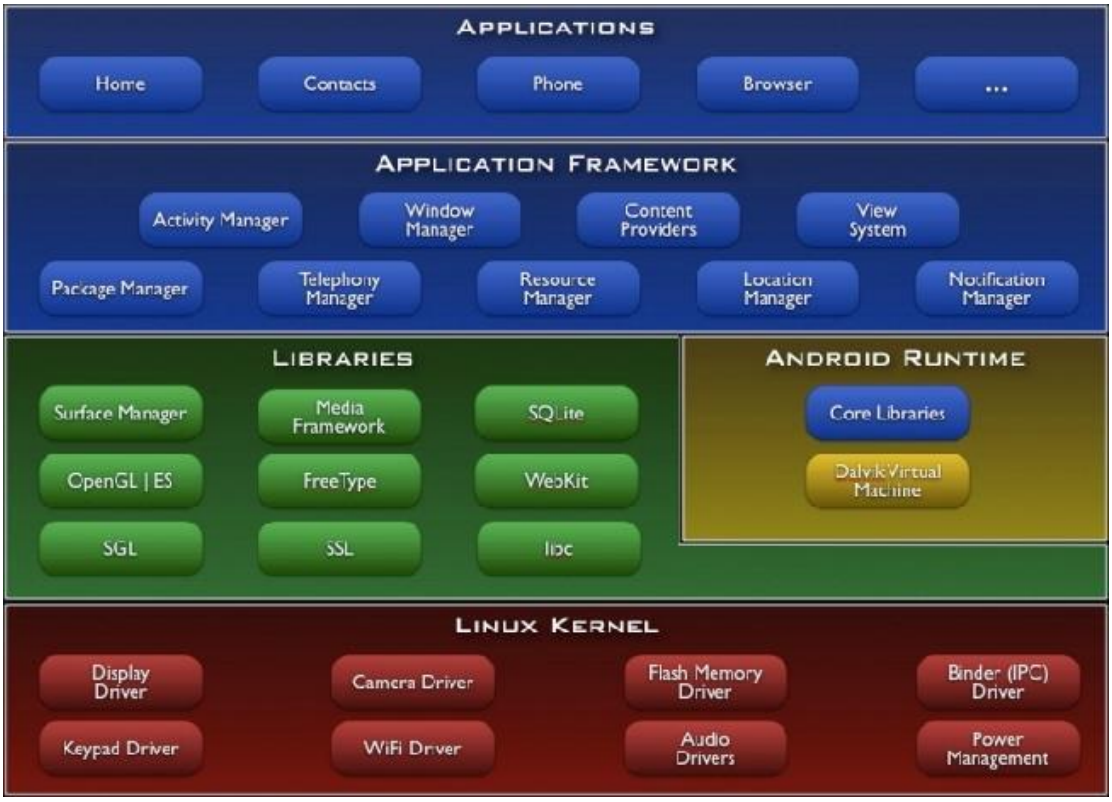
• Έναν διαχειριστή δραστηριοτήτων (**Activity Manager**), ο οποίος διαχειρίζεται τον κύκλο ζωής των εφαρμογών.

Επίπεδο Βιβλιοθηκών (Libraries): Το οποίο περιλαμβάνει ένα σύνολο από βιβλιοθήκες γραμμένες σε C/C++, που χρησιμοποιούνται από διάφορα στοιχεία του συστήματος του Android. Οι δυνατότητες που προσφέρουν αυτές οι βιβλιοθήκες είναι διαθέσιμες στους προγραμματιστές μέσω του επιπέδου πλαισίου εφαρμογής.

Επίπεδο Εκτέλεσης (Android Runtime): Το οποίο αποτελείται από ένα σύνολο από βασικές βιβλιοθήκες και την Dalvik Virtual Machine.

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

Στον πυρήνα της πλατφόρμας Android (Εικόνα 6), βρίσκεται ένας Linux kernel που είναι υπεύθυνος για τη διαχείριση των device drivers, τον έλεγχο πρόσβασης στους πόρους του συστήματος, τη διαχείριση μνήμης και τις λοιπές υπηρεσίες που παρέχει ένα λειτουργικό σύστημα. Σε αυτούς συγκαταλέγονται αυτοί της οθόνης, του WiFi, της κάμερας, του ήχου κ.α. Ένα επίπεδο επάνω βρίσκονται οι προεγκατεστημένες βιβλιοθήκες του συστήματος που είναι γραμμένες σε C++ και περιλαμβάνουν το OpenGL, την SQLite, την Media library κ.α. Οι εφαρμογές που εκτελούνται στο κινητό μπορούν να έχουν πρόσβαση στις βιβλιοθήκες αυτές μέσω της Dalvik JVM.



Εικόνα 6. Αρχιτεκτονική του Android

2.2.4 Αρχεία συστήματος Android

Υπάρχει διαφοροποίηση στον τρόπο με τον οποίο διαμορφώνονται τα αρχεία συστήματος για υπολογιστές και για κινητά τηλέφωνα. Ο χώρος που οργανώνονται αποτελεσματικά τα δεδομένα, καλείται αρχεία συστήματος Android. Η αποδοτικότητα των αρχείων ανάγεται στην ταχύτητα ανάκτησης, εγγραφής και ανάγνωσης των δεδομένων από κάθε εφαρμογή. Το Android έχει ως βάση τα αρχεία του συστήματος Linux πολλά από τα οποία χρησιμοποιούνται τόσο για την εκκίνηση όσο και την λειτουργία της συσκευής.

Χρησιμοποιεί τύπους αρχείων όπως EXT, FAT32 και YAFFS2 για την εκκίνηση και την καταχώρηση των δεδομένων. Τα αρχεία συστήματος FAT και FAT32 είναι γνωστά από το λειτουργικό σύστημα των Windows. Το Android υποστηρίζει αυτόν τον τύπο αρχείων κυρίως στην εξωτερική του μνήμη, παρόλο όμως που χρησιμοποιούνται συχνά δεν θεωρούνται ασφαλή. Τα αρχεία συστήματος τύπου YAFFS2 (Yet Another Flash File System 2) σχεδιάστηκαν για τη μνήμη flash. Το θέμα όμως, που προκύπτει με αυτού του τύπου τα αρχεία είναι ότι τα εργαλεία ψηφιακών πειστηρίων δεν είναι συμβατά μαζί τους [5].

Το Android δημιουργεί ανάλογα με τον κατασκευαστή της συσκευής στην εσωτερική του μνήμη διαφορετικό διαμοιρασμό (partitions) στα αρχεία συστήματος, κάθε ένα από τα οποία χρησιμοποιείται για συγκεκριμένες λειτουργίες. Ο τυπικός διαμοιρασμός είναι:

/boot: περιλαμβάνει τον πυρήνα και το ramdisk και επιτρέπει στη συσκευή να εκκινήσει. Η διαγραφή στοιχείων από αυτό το partition μπορεί να μην επιτρέψει την εκκίνηση της συσκευής.

/system: περιλαμβάνει το λειτουργικό σύστημα της συσκευής και περιέχει τη γραφική διεπαφή χρήστη και τις προεγκατεστημένες εφαρμογές. Χωρίς αυτό δεν είναι δυνατή η χρήση της διεπαφής του λειτουργικού.

/recovery: πρόκειται για εναλλακτικό του διαμερίσματος εκκίνησης (boot) της συσκευής και επιτρέπει την εκκίνηση σε recovery mode.

/data: περιλαμβάνει τα δεδομένα του χρήστη.

/cache: πρόκειται για το partition, όπου το Android αποθηκεύει δεδομένα στα οποία κάνει συχνές προσπελάσεις. Διαγραφή στοιχείων από αυτό το partition δεν επηρεάζει τα δεδομένα του χρήστη.

/misc: περιλαμβάνει διάφορες ρυθμίσεις του συστήματος με τη μορφή διακοπτών on/off, πολλές συσκευές Android ήδη χρησιμοποιούν αρχεία συστήματος της μορφής EXT4. Αυτή η αλλαγή προήλθε από την ανάγκη του συστήματος να υποστηρίζει διπύρηνους επεξεργαστές και πολυεπεξεργαστές καθώς και στη χρήση εξωτερικών καρτών μνήμης [6].

2.2.5 Δομικά Στοιχεία Εφαρμογών

Τα στοιχεία που συνδυάζονται για την υλοποίηση μιας εφαρμογής Android είναι ορισμένα από τα ακόλουθα:

- **Δραστηριότητα**: Η κύρια κλάση Δραστηριότητα (Activity) παρέχει τη γραφική διεπαφή χρήστη, μέσω της οποίας ο χρήστης λαμβάνει και αποστέλλει πληροφορίες στην εφαρμογή. Αποτελεί το πιο κοινό από τα δομικά στοιχεία μιας εφαρμογής. Συνήθως είναι μια μόνο ξεχωριστή οθόνη σε μια

εφαρμογή. Κάθε Δραστηριότητα υλοποιείται μέσα σε μια ξεχωριστή κλάση που επεκτείνει την κλάση Activity.

- **Πάροχος Περιεχομένου**: Ένας Πάροχος Περιεχομένου (Content Provider) επιτρέπει σε μια εφαρμογή να αποθηκεύει και να διαμοιράζεται δεδομένα με άλλες εφαρμογές. Οι εφαρμογές μπορούν να αποθηκεύουν τα δεδομένα τους σε αρχεία, βάσεις δεδομένων SQLite ή με κάποιον άλλον μηχανισμό. Το Android παρέχει τη Βάση SQLite, η οποία συνεργάζεται πολλές φορές με τον Πάροχο Περιεχομένου αποθηκεύοντας τα δεδομένα τα οποία θα προσπελαστούν με τη χρήση του Παρόχου.

- **Δέκτης Εκπεμπόμενων Προθέσεων**: Ένας Δέκτης Εκπεμπόμενων Προθέσεων (Broadcast Receiver) δέχεται και αποκρίνεται σε γεγονότα, τα οποία λαμβάνουν χώρα στη συσκευή. Μπορεί να χρησιμοποιηθεί όταν χρειάζεται να εκτελεστεί κώδικας μιας εφαρμογής από έναν εξωτερικό παράγοντα. Ο receiver μπορεί να χρησιμοποιήσει τον Διαχειριστή Ειδοποιήσεων (Notification Manager) για να ειδοποιήσει τον χρήστη, αν και δεν διαθέτει user interface. Το σύστημα θα ενεργοποιήσει μια εφαρμογή, αν είναι απαραίτητο, όταν ενεργοποιηθεί κάποιος Δέκτης Εκπεμπόμενων Προθέσεων. Κάθε εφαρμογή έχει τη δυνατότητα να στείλει τα δικά της intent broadcasts σε άλλες εφαρμογές.

- **Υπηρεσία**: Υπηρεσία (Service) είναι κώδικας ο οποίος τρέχει στο παρασκήνιο, χωρίς user interface. Συνήθως εκτελεί μία και μόνη εργασία και δεν επιστρέφει κάποιο αποτέλεσμα στον καλούντα. Όταν εκτελεστεί η εργασία αυτή, τότε η Υπηρεσία τερματίζεται μόνη της. Μια εφαρμογή μπορεί να συνδεθεί με μια Υπηρεσία και να διαλειτουργήσει μαζί της με διαπροσωπεία (learning design tool) , που παρέχεται από την Υπηρεσία.

- **Πρόθεση και Φίλτρο Προθέσεως**: Ένα αντικείμενο Πρόθεσης (Intent) είναι ένα μήνυμα το οποίο περιγράφει τι θέλει να κάνει μια εφαρμογή. Απεικονίζει την επιθυμητή ενέργεια (action), τα δεδομένα (data), την κατηγορία των δεδομένων (category) και άλλες εντολές. Τα βασικά στοιχεία μιας Πρόθεσης είναι η ενέργεια που θέλει η εφαρμογή να εκτελεστεί και τα δεδομένα που θα

επηρεαστούν από την εκτέλεση της συγκεκριμένης ενέργειας. Από την άλλη πλευρά, το Φίλτρο Προθέσεως (Intent Filter) αποτελεί μια περιγραφή του τι είδους Προθέσεις είναι δυνατόν να εξυπηρετηθούν [7].

- **Ειδοποίηση**: Ειδοποίηση (Notification) θεωρείται κάθε ενημέρωση νέας κατάστασης και εμφανίζεται με τη μορφή εικονιδίων στο πεδίο ειδοποίησης του χρήστη. Ο χρήστης μπορεί να αλληλεπιδράσει με το εικονίδιο αυτό για να εκκινήσει την εφαρμογή και να λάβει περισσότερες ενημερώσεις.

- **Όψη**: Η Όψη (View) είναι ένα αντικείμενο το οποίο εμφανίζεται στην οθόνη για τα widgets, που χρησιμοποιούνται για τη δημιουργία διαδραστικών στοιχείων UI, όπως πλήκτρα, πεδία κειμένου, κτλ. Το user interface δημιουργείται με χρήση Όψεων. Συμβάλουν στο χειρισμό των events που δημιουργούνται κατά την αλληλεπίδραση του χρήστη με μία εφαρμογή και την αποθήκευση της τρέχουσας κατάστασης.

- **AndroidManifest.xml**: Πρόκειται για το αρχείο ελέγχου , το οποίο υπάρχει στον κεντρικό φάκελο κάθε εφαρμογής (root directory), και μέσα στο οποίο περιγράφονται καθολικές ιδιότητες της εφαρμογής.

2.2.6 Καταχώρηση Δεδομένων

Είναι ουσιώδες να αναφέρουμε τις μεθόδους τις οποίες χρησιμοποιεί το Λειτουργικό Σύστημα Android για την αποθήκευση των δεδομένων [8]. Αυτές είναι:

Internal Storage: τα αρχεία αποθηκεύονται στον υποφάκελο /data/data/ της εφαρμογής. Αυτός ο φάκελος είναι προσπελάσιμος μόνο εφόσον κάποιος έχει δικαιώματα διαχειριστή.

External Storage: τα αρχεία που αποθηκεύονται στην SD Card παρουσιάζουν λιγότερους περιορισμούς πρόσβασης και μπορούν να αναγνωσθούν και να τροποποιηθούν ακόμα και από διαφορετική συσκευή.

SQLite: χρησιμοποιείται για την αποθήκευση δεδομένων με δομημένη μορφή και παρουσιάζει ομοιότητες με τον τρόπο αποθήκευσης στην SD Card.

Network: πρόκειται για δικτυακές βάσεις δεδομένων οι οποίες παρέχουν σημαντικές πληροφορίες στις έρευνες, αλλά δεν χρησιμοποιούνται ευρέως. Τόσο τα συστήματα αρχείων όσο και οι τρόποι αποθήκευσης αποτελούν τα «εργαλεία» που θα μεταχειριστούν το πλέον σημαντικό στοιχείο, που δεν είναι άλλο από τα δεδομένα. Αυτά κατηγοριοποιούνται σε τέσσερις ομάδες:

i) Μεταδεδομένα (metadata): πρόκειται για δεδομένα τα οποία προσδιορίζουν άλλα δεδομένα, όπως ονόματα διαδικασιών, ώρες εκκίνησης ή τερματισμού διεργασιών και ονόματα αρχείων που προσπελάστηκαν. Παρουσιάζουν μεγάλη αξία για την Ψηφιακή Εγκληματολογία.

ii) Αρχεία Δεδομένων (data files): πρόκειται για τα προσωπικά δεδομένα του χρήστη, τα οποία επίσης έχουν μεγάλη αξία για τις έρευνες.

iii) Ευαίσθητα Αρχεία (sensitive data): περιλαμβάνουν κωδικούς πρόσβασης, κλειδιά κρυπτογράφησης ή συνδέσμους που χρησιμοποιήθηκαν και αποτελούν συνήθως παραμέτρους σε άλλες διαδικασίες.

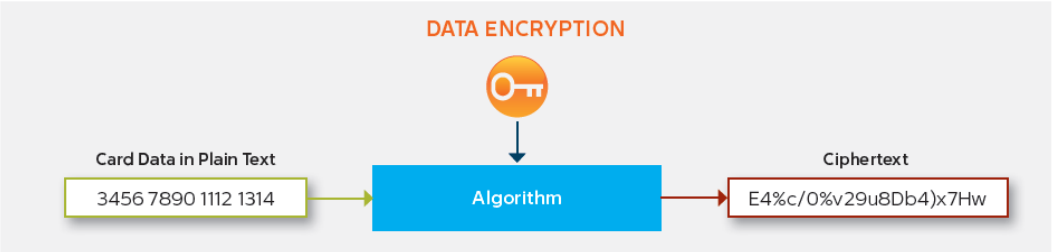
iv) Άσχετα Δεδομένα (case irrelevant data): δεδομένα που δεν παρουσιάζουν περαιτέρω αξία για τις έρευνες.

Κεφάλαιο 3ο
Ανέπαφες Αρχιτεκτονικές Ασφάλειας e-Wallet

3.1 Γενικά

Η ασφάλεια πληρωμών είναι μια πολύπλοκη διαδικασία, με πολλούς κινδύνους και τρωτά σημεία σε κάθε τμήμα των αλυσιδωτών διεργασιών. Ο συνδυασμός του ολοένα αυξανόμενου κόστους συμμόρφωσης στα πρότυπα ασφαλείας και οι συνεχώς αναδυόμενες νέες απειλές για την ασφάλεια των δεδομένων, καθιστούν απαραίτητο για τους παρόχους να εφαρμόσουν αποτελεσματικές τεχνολογίες διαχείρισης του κινδύνου για τον περιορισμό του κόστους και την αποφυγή καταστροφικών συνεπειών από περιπτώσεις διαρροής δεδομένων.

Ο συνδυασμός κρυπτογράφησης και tokenization προσφέρει λύσεις για αλληλοαποκλειόμενες αδυναμίες ασφάλειας κατά τη διαδικασία των πληρωμών, έτσι μπορεί να μειώσει το κόστος συμμόρφωσης ενός παρόχου με τα πρότυπα ασφάλειας. Η κρυπτογράφηση προστατεύει τα δεδομένα, που έχουν συλλεχθεί από τον πάροχο, αλλά δεν έχουν ακόμη χρησιμοποιηθεί για τη διαδικασία έγκρισης της συναλλαγής. Το Tokenization λύνει το πρόβλημα της αποθήκευσης και χρήσης δεδομένων του πραγματικού αριθμού της κάρτας στις επιχειρηματικές διαδικασίες που λαμβάνουν χώρα πριν την έγκριση.



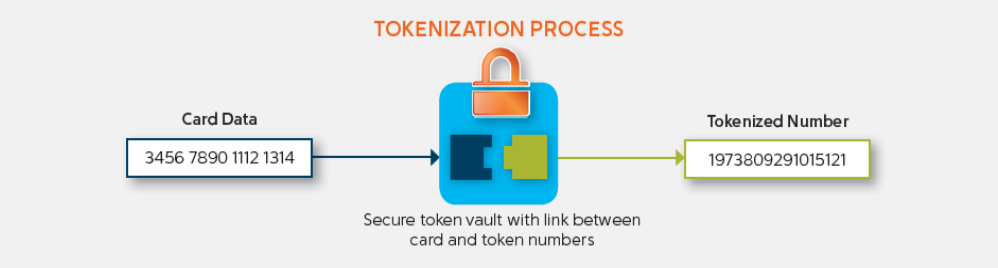
Εικόνα 7. Data Encryption Process

Παρά το γεγονός ότι ούτε η κρυπτογράφηση ούτε το tokenization απαιτούνται σήμερα από τα διεθνή πρότυπα, ο συνδυασμός αυτών των τεχνολογιών είναι ευρέως αναγνωρισμένος, ως ο πιο ισχυρός τρόπος για την προστασία από κλοπή δεδομένων. Σύμφωνα με τις παραινέσεις του προτύπου ασφάλειας,« οι πάροχοι πρέπει να χρησιμοποιούν ισχυρή κρυπτογραφία για να

καταστήσουν τα αποθηκευμένα δεδομένα κατόχου της κάρτας δυσανάγνωστα, και να χρησιμοποιούν άλλες τεχνολογίες πολυεπίπεδης ασφαλείας για την ελαχιστοποίηση του κινδύνου εκμετάλλευσης από κακόβουλους [9].

3.2 Tokenisation

Μια όλο και περισσότερο δημοφιλής προσέγγιση για την προστασία των ευαίσθητων δεδομένων, είναι η χρήση της υποκατάστασης των δεδομένων με ένα token, ως αντικατάσταση για έναν πραγματικό αριθμό κάρτας πληρωμής. Κατά τη διαδικασία του tokenization, τα πραγματικά δεδομένα του κατόχου της κάρτας χρησιμοποιούνται στην πράξη πληρωμής. Μόλις εγκριθεί η συναλλαγή, αυτά τα ευαίσθητα δεδομένα αποστέλλονται σε ένα κεντρικό και ιδιαίτερα ασφαλή διακομιστή που ονομάζεται "θησαυροφυλάκιο", όπου είναι αποθηκευμένα. Την ίδια στιγμή, ένας τυχαίος μοναδικός αριθμός παράγεται και επιστρέφεται στα συστήματα του εμπόρου για χρήση στη θέση των δεδομένων των κατόχων καρτών.



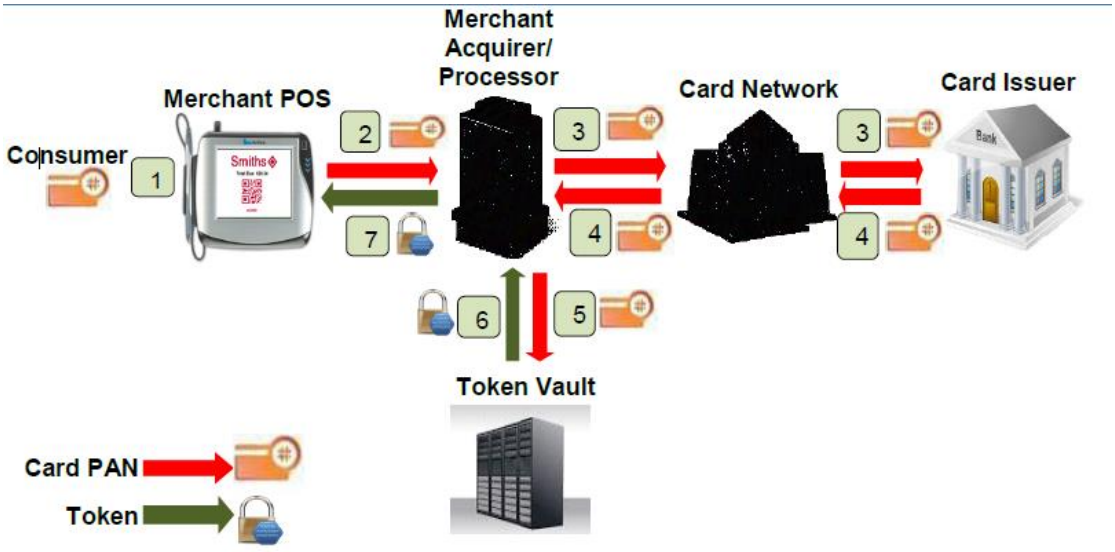
Εικόνα 8. Tokenization Process

Πιο συγκεκριμένα, είναι η διαδικασία αντικατάστασης του Personal Account Number (PAN), το οποίο διαθέτουν όλες οι πλαστικές τραπεζικές κάρτες (χρεωστικές και πιστωτικές), με έναν άλλον λογαριασμό χρήσης, ο οποίος ονομάζεται payment token και διατηρεί όλες τις απαραίτητες πληροφορίες αυξάνοντας όμως την ασφάλεια τόσο των συναλλαγών όσο και των κατόχων του. Εν τω μεταξύ, ο αριθμός payment token, ο οποίος δεν μπορεί να αντιστοιχηθεί από κανέναν με τον πραγματικό, πλήν του παρόχου που ανήκει, μπορεί να χρησιμοποιηθεί σε όλες τις μετέπειτα διαδικασίες πληρωμών μετά τη αρχική έκδοσή του.

Οι βασικές λειτουργίες του tokenization είναι [10]:

- Έκδοση και παροχή token
- Επεξεργασία συναλλαγών
- Διασυνδέσεις με άλλα συστήματα -Application Programming Interfaces (APIs)

Για την υλοποίηση των παραπάνω διαδικασιών καθίσταται αναγκαία η ύπαρξη ενός νέου παρόχου, ο οποίος θα είναι επιφορτισμένος με την εκτέλεση αυτών των υπηρεσιών και ονομάζεται Token Service Provider (TSP). Ο TSP μπορεί να υλοποιείται είτε από τους εκδότες των καρτών (τράπεζες), είτε από τους οργανισμούς των καρτών (Visa, MasterCard, AmEx κ.α.) ή ακόμα και από έναν τρίτο φορέα ο οποίος μπορεί να είναι τελείως ανεξάρτητος.



Εικόνα 9. Security Tokenization Flow

Η χρήση του Tokenization είναι σημαντική για δύο κυρίως λόγους. Πρώτον, μειώνει δραστικά τον κίνδυνο ασφάλειας ενός εμπόρου σε περίπτωση παραβίασης δεδομένων, επειδή η διαδικασία εξαλείφει τα ευαίσθητα δεδομένα του κατόχου της κάρτας από το περιβάλλον του εμπόρου, μετά από μια συναλλαγή που έχει εγκριθεί. Εάν οι αριθμοί token παραβιαστούν, δεν έχουν καμία αξία σε όποιον θα προσπαθούσε να τους χρησιμοποιήσει, επειδή τα token είναι απλά τυχαίοι αριθμοί. Δεύτερον, χρησιμοποιώντας token αντί των

πραγματικών δεδομένων της κάρτας σε επιχειρηματικές εφαρμογές back-end, συρρικνώνεται το εύρος των δεδομένων του κατόχου της κάρτας. Αυτή η μείωση μπορεί να αποφέρει σε έναν έμπορο σημαντικό χρόνο και χρήμα [11].

3.3 Payment Token

Το Payment token είναι ένας αριθμός ο οποίος αντικαθιστά το Personal Account Number (PAN) μιας τραπεζικής κάρτας και χρησιμοποιείται κυρίως σε ηλεκτρονικές πληρωμές μέσω διαδικτύου για την προστασία του φυσικού αριθμού της κάρτας. Το payment token μπορεί να έχει οποιαδήποτε μορφή αλλά για λόγους συμβατότητας και διαλειτουργικότητας των συστημάτων, ακολουθείται η ίδια μορφή που χρησιμοποιείται και από το PAN των τραπεζικών καρτών.

Ο αριθμός λογαριασμού PAN που διαθέτουν όλες οι τραπεζικές κάρτες συμφωνεί με το πρότυπο ISO/IEC 7812 και αποτελείται από 13 έως 19 ψηφία. Η δομή του PAN είναι η ακόλουθη [12]:

- 6 ψηφία: Ένας μοναδικός αριθμός (BIN) ο οποίος εκχωρείται στην εκδότρια τράπεζα. Κάθε εκδότρια τράπεζα μπορεί να διαθέτει παραπάνω από ένα BIN.
- 6 έως 12 ψηφία: Το εύρος των αριθμών καρτών που μπορεί να χρησιμοποιηθεί στο δεδομένο BIN.
- 1 ψηφίο: Είναι το ψηφίο επαλήθευσης (check digit) και υπολογίζεται με την χρήση του αλγορίθμου Luhn.

Τα payment tokens διαθέτουν μια σειρά από χαρακτηριστικά στοιχεία, η ύπαρξη των οποίων μπορεί να είναι είτε υποχρεωτική είτε προαιρετική. Τα χαρακτηριστικά στοιχεία (elements) των payment tokens είναι τα ακόλουθα [12]:

- Token Expiry Date
- Last 4 Digits of PAN
- PAN Product ID
- POS Entry Mode
- Token Requestor ID
- Token Assurance Level

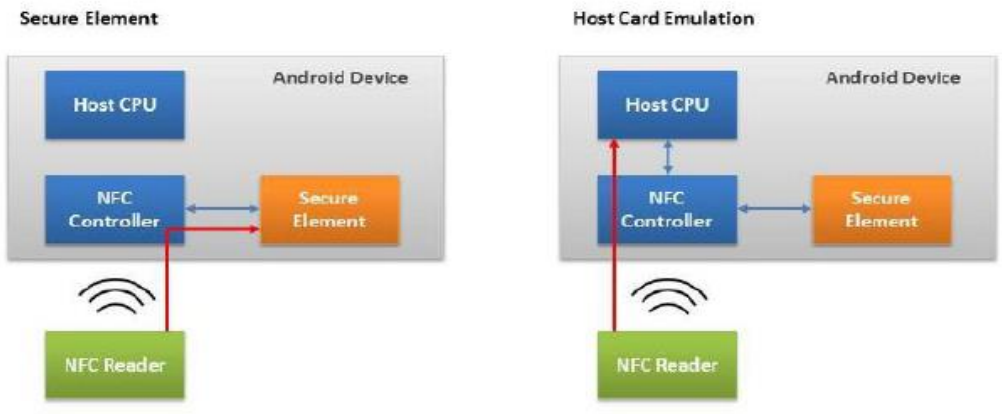
- Token Assurance Data
- Token Cryptogram
- Token Request Indicator

3.4 Εξομοίωση κάρτας υποδοχής (HCE)

3.4.1 Γενικά

Ο όρος «εξομοίωση κάρτας υποδοχής» (HCE) επινοήθηκε το 2012 από τους Doug Yeager και Ted Fifelski, τους ιδρυτές της SimplyTapp Inc, περιγράφοντας τη δυνατότητα να ανοίξει ένα δίαυλο επικοινωνίας ανάμεσα σε ένα τερματικό ανέπαφων πληρωμών και σε ένα εξ'αποστάσεως ασφαλές στοιχείο (Secure Element), που περιέχει οικονομικά δεδομένα της κάρτας πληρωμής και επιτρέπει τις οικονομικές συναλλαγές που θα πραγματοποιούνται σε ένα τερματικό σημείο πώλησης [13].

Είναι ένας μηχανισμός, ο οποίος επιτρέπει σε μια εφαρμογή που τρέχει στον επεξεργαστή «πυρήνα», (κεντρικό επεξεργαστή της κινητής συσκευής -τρέχουν οι περισσότερες εφαρμογές) να πραγματοποιεί συναλλαγές καρτών εξομοίωσης με ένα εξωτερικό αναγνώστη. Είναι αρχιτεκτονική λογισμικού που παρέχει ακριβή εικονική αναπαράσταση των διαφόρων ηλεκτρονικών ταυτοτήτων (πρόσβασης, τραπεζικών), χρησιμοποιώντας μόνο λογισμικό. Πριν από αυτή, οι συναλλαγές μέσω NFC (Near Field Connection), πραγματοποιούνταν κυρίως χρησιμοποιώντας το SE (Secure Element) .



Εικόνα 10. Host Card Emulation

Αυτή η τεχνολογία δίνει τη δυνατότητα σε εμπόρους να προσφέρουν λύσεις πληρωμών με κάρτες πιο εύκολα μέσω του κινητού

τηλεφώνου καθώς επίσης και λύσεις ανέπαφων πληρωμών. Προσφέρει σε πραγματικό χρόνο, τη διανομή των καρτών πληρωμής και, πιο συγκεκριμένα, επιτρέπει την πραγματοποίηση συναλλαγών χωρίς να απαιτεί αλλαγές στο λογισμικό των τερματικών σημείων πληρωμής.

3.4.2 Τεχνολογική Εξέλιξη

Μετά την υιοθέτηση του HCE από το λογισμικό Android, η Google στόχευε, συμπεριλαμβάνοντας το HCE στο πιο εμπορικό λειτουργικό σύστημα στον κόσμο (που μέχρι εκείνη την στιγμή κάλυπτε το 80% της αγοράς), θα είχε την ευκαιρία να αναπτυχθεί περισσότερο γρήγορα, ενώ παράλληλα θα μπορούσε να αναπτύξει το Πορτοφόλι Google-Wallet πιο εύκολα και σε μεγαλύτερο εύρος. Ωστόσο, ακόμη και με την ένταξη της HCE στο Android 4.4, οι τράπεζες εξακολουθούν να χρειάζονται τους παρόχους δικτύων καρτών για την υποστήριξη HCE. Τέσσερις μήνες αργότερα, στο Mobile World Congress 2014, τόσο η Visa όσο και η MasterCard κάνουν δημόσιες ανακοινώσεις, σχετικά με την υποστήριξη της τεχνολογίας HCE. Ως αποτέλεσμα της ευρείας υιοθέτησης του HCE, ορισμένες εταιρείες προσφέρουν τροποποιημένες λύσεις που εστιάζουν συνήθως στην παροχή επιπλέον ασφάλειας για το κανάλι επικοινωνίας του HCE. Μια τέτοια εφαρμογή ονομάζεται HCE +.

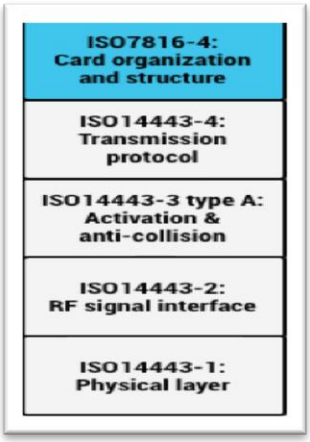
3.4.3 Επιπτώσεις

Η τεχνολογία NFC έχει αντιμετωπίσει ζητήματα αποδοχής, λόγω της έλλειψης υποδομών (τερματικοί σταθμοί) και η προσέγγιση του SE εμποδίζει οργανισμούς με την επιθυμία να συμμετάσχουν στις πληρωμές μέσω κινητού τηλεφώνου, να το πράξουν, λόγω των υψηλών αρχικών δαπανών κεφαλαίου και των πολύπλοκων σχέσεων με τους συμμετέχοντες.

Με την υποστήριξη του HCE στο Android 4.4, η Google έδωσε τη δυνατότητα σε οργανισμούς, να επωφεληθούν από την τεχνολογία NFC, σε σχετικά χαμηλό κόστος. Σε ορισμένους τομείς, η νέα αρχιτεκτονική HCE μπορεί να υποστηρίξει υπηρεσίες που περιλαμβάνουν πληρωμές, προγράμματα επιβράβευσης, κάρτα πρόσβασης και διέλευσης, κ.α.

3.4.4 Εφαρμογή

Τα πρότυπα HCE προσφέρουν υποστήριξη σε πολλά πρωτόκολλα και υπάρχουν διαφορετικά είδη καρτών που μπορούν να υιοθετηθούν. Το Android 4.4 υποστηρίζει διάφορα πρωτόκολλα που είναι κοινά στην αγορά σήμερα. Πολλές από τις υπάρχουσες ανέπαφες κάρτες, βασίζονται ήδη σε αυτά τα πρωτόκολλα, όπως και οι κάρτες ανέπαφων πληρωμών. Τα πρωτόκολλα αυτά υποστηρίζονται επίσης από πολλούς NFC αναγνώστες στην σημερινή αγορά, συμπεριλαμβανομένων των συσκευών Android NFC που λειτουργούν ως αναγνώστες του εαυτούς τους. Αυτό επιτρέπει την δημιουργία και την ανάπτυξη μια λύσης NFC, από άκρη σε άκρη (end-to-end), μέσω της τεχνολογίας HCE, χρησιμοποιώντας μόνο συσκευές βασισμένες στο Android.



Εικόνα 11. Android's HCE protocol stack

Συγκεκριμένα, το Android 4.4 υποστηρίζει κάρτες εξομοίωσης, που βασίζονται στην τεχνολογία NFC-Forum ISO-DEP προδιαγραφή (με βάση το πρότυπο ISO / IEC 14443-4) και της διαδικασίας Application Protocol Data Units (APDUs), όπως ορίζεται στην προδιαγραφή 7816-4 ISO / IEC. Το Android απαιτεί εξομοίωση ISO-DEP μόνο στην κορυφή της NFC-A τεχνολογίας (ISO / IEC 14443 - 3 Τύπος A). Υποστήριξη για την τεχνολογία NFC-B (ISO / IEC 14443-4 Τύπος B) είναι προαιρετική. Η διαστρωμάτωση όλων αυτών των προδιαγραφών φαίνεται στην Εικόνα 11.

3.4.5 Χρήσεις

Η τεχνολογία HCE χρησιμοποιείται για να επιτρέψει τις συναλλαγές μεταξύ των κινητών συσκευών και άλλων συσκευών που απαιτούν διαπιστευτήρια πρόσβασης (π.χ. POS). Ως πλεονεκτήματα, από τη χρήση της, μπορούμε να αναφέρουμε:

- Τη μείωση της πολυπλοκότητας για τους προγραμματιστές εφαρμογών και τις NFC δυνατότητες για νέες εφαρμογές.
- Παρέχει εύκολη και ευέλικτη χρήση κάρτας σε κινητές συσκευές.
- Δεν εξαρτάται από το ασφαλές στοιχειό (SE) του κατόχου.

Οι περιορισμοί από τη χρήση της τεχνολογίας είναι:

- Δεν κατοχυρώνεται η ασφαλής αποθήκευση των δεδομένων και τα πιστοποιητικών στη συσκευή.
- Εξαρτάται από τις δυνατότητες του λειτουργικού συστήματος.
- Εναλλακτικοί τρόποι για την ασφάλεια HCE, μπορεί να αυξήσουν την πολυπλοκότητα μεταξύ ενός διακομιστή (server), μιας εφαρμογής (application) και της βάση δεδομένων (database) (backend complexity).

3.5 Near Field Communication

Το Near Field Communication (NFC), είναι μία τεχνολογία σαν την ασύρματη επικοινωνία, αλλά λειτουργεί σε πολύ μικρότερες αποστάσεις περίπου 4 εκατοστά. Πάντα υπάρχει ένας αποστολέας και ένας δέκτης. Ο αποστολέας δημιουργεί ένα ενεργό πεδίο ραδιοσυχνότητας, όπου μπορεί να τροφοδοτήσει έναν παθητικό στόχο. Επιτρέπει την γρήγορη ανάγνωση και εγγραφή δεδομένων και χρησιμοποιείται σε διάφορες εφαρμογές με κυριότερες τις ηλεκτρονικές πληρωμές και τον έλεγχο πρόσβασης. Εκτός από τα κινητά υπάρχουν και οι NFC κάρτες σε μορφή έξυπνων καρτών με διαφορετική χωρητικότητα ανάλογα με την χρήση [14].

Εικόνα 12. NFC technology

Το NFC μπορεί να βρίσκεται σε 3 διαφορετικές καταστάσεις λειτουργίας.

- Η πρώτη είναι η Read/Write, όπου η μία συσκευή είναι Active και η άλλη Passive και επιτρέπει στις εφαρμογές να μεταδώσουν και να λάβουν δεδομένα.
- Η δεύτερη είναι η Card emulation, όπου επιτρέπει στις NFC συσκευές να συμπεριφέρονται σαν έξυπνη κάρτα.
- Και τέλος, είναι η Peer to Peer (P2P), όπου ορίζεται για επικοινωνία από συσκευή σε συσκευή σε επίπεδο σύνδεσης.

Τα μηνύματα που μεταδίδονται είναι τεχνολογίας NDEF και μπορεί να είναι τύπου Smart Poster (για την ανάγνωση επιπλέον πληροφορίας από διαφημιστικά πόστερ), Handover (για παράδειγμα την άμεση σύνδεση δύο συσκευών Bluetooth με το άγγιγμα τους), vCard (μεταφορά στοιχείων υπό μορφή vCard) και URL (σύνδεσμος σε ιστοσελίδα). Επίσης μια άλλη τεχνολογία είναι και το RTD, όπου χρησιμοποιεί συγκεκριμένο τύπο εγγραφής και όνομα τύπου που μπορούν να μεταφέρονται σε μια εγγραφή NDEF.

Η τεχνολογία της επικοινωνίας κοντινού πεδίου πληροί τις προδιαγραφές των standard ISO/IEC 14443 A&B και Felica (ISO 18092) και προωθήθηκε

κυρίως μέσω του NFC Forum (2004), στο οποίο συμμετέχουν 140 γνωστές εταιρίες και άλλοι οργανισμοί.

Παρόλο που η εμβέλεια επικοινωνίας του NFC είναι περιορισμένη σε κάποια εκατοστά, το NFC από μόνο του δεν μπορεί να εγγυηθεί για την ασφαλή επικοινωνία. Οι εφαρμογές θα πρέπει να χρησιμοποιούν υψηλότερου επιπέδου πρωτόκολλο κρυπτογράφησης για να εδραιώσουν ένα ασφαλές κανάλι. Η διασφάλιση των δεδομένων στο NFC, απαιτεί τη συνεργασία πολλών μελών. Οι πάροχοι συσκευών θα πρέπει να διασφαλίσουν τα τηλέφωνα με ενεργοποιημένο NFC, με ισχυρούς αλγόριθμους κρυπτογράφησης και πρωτόκολλα αυθεντικοποίησης. Οι χρήστες θα πρέπει να προστατεύουν τις προσωπικές τους συσκευές και τα δεδομένα με κωδικούς πρόσβασης, κλείδωμα πληκτρολογίου, και λογισμικά κατά των ιών και οι πάροχοι εφαρμογών θα πρέπει να χρησιμοποιούν συστήματα κατά των ιών και του κακόβουλου λογισμικού για την αποτροπή μόλυνσης των συστημάτων τους.

3.6 Secure Element

Ένα Ασφαλές Στοιχείο (SE), είναι ένα τσιπ μικροεπεξεργαστή που μπορεί να αποθηκεύσει ευαίσθητα δεδομένα και να εκτελέσει ασφαλείς εφαρμογές, όπως αυτές των πληρωμών. Λειτουργεί ως ένα θησαυροφυλάκιο, προστατεύοντας ότι υπάρχει μέσα στο SE (εφαρμογές και δεδομένα), από malware επιθέσεις που είναι τυπικά στον πυρήνα, δηλαδή στο λειτουργικό σύστημα της συσκευής. Είναι συμβατό με το ISO 7816 standard, το οποίο συνήθως ενσωματώνεται στο NFC τσιπ των έξυπνων συσκευών [15].

Τα Ασφαλή Στοιχεία χειρίζονται όλα τα είδη των εφαρμογών που είναι ζωτικής σημασίας για τη σύγχρονη ψηφιακή ζωή μας:

- **Αυθεντικοποίηση**

Αντί για το όνομα χρήστη και τον κωδικό πρόσβασης, η πρόσβαση σε μια ηλεκτρονική υπηρεσία μπορεί να προστατεύεται από ένα ισχυρό μηχανισμό ελέγχου ταυτότητας, με βάση διαπιστευτήρια που αποθηκεύονται και υποβάλλονται σε επεξεργασία στο SE. Έτσι για σύνδεση σε ένα VPN ή στο e-

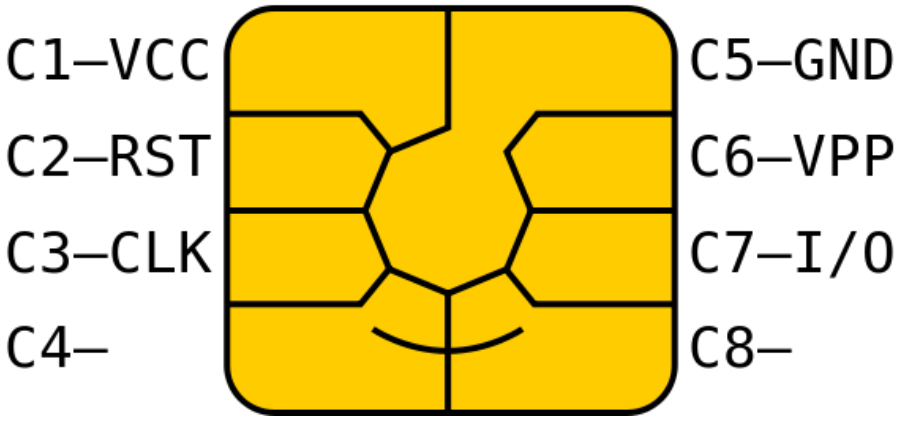
mail , ένα SE θα μπορούσε να ελέγξει και να διασφαλίσει ότι κάποιος είναι αυτός που λέει ότι είναι.

- **Ψηφιακή υπογραφή**

Οι εφαρμογές μπορούν να χρησιμοποιήσουν το SE, για την ψηφιακή υπογραφή ενός εγγράφου ή οποιουδήποτε δεδομένου με ένα κλειδί, που είναι αποθηκευμένο στο ασφαλές στοιχείο. Αυτό το κλειδί βοηθά το ασφαλές στοιχείο να ξεκλειδώσει τα κρυπτογραφημένα δεδομένα, ώστε να μπορεί να τα διαβάσει. Και πάλι αυτό χρησιμοποιείται για να αποδείξει ποιος είναι ο χρήστης. Έτσι, το πρόγραμμα ηλεκτρονικού ταχυδρομείου θα μπορεί να χρησιμοποιήσει τη σύνδεση με το Secure Element και να υπογράψει ψηφιακά τα εξερχόμενα e-mails.

- **Πληρωμές σε κινητά**

Εδώ, το Secure Element αποθηκεύει με ασφάλεια τα στοιχεία της κάρτας και του κατόχου, και διαχειρίζεται την ανάγνωση των κρυπτογραφημένων δεδομένων. Κατά τη διάρκεια μιας συναλλαγής πληρωμής λειτουργεί, όπως μια κάρτα ανέπαφων πληρωμών χρησιμοποιώντας τα αντίστοιχα τεχνολογικά πρότυπα, για να επιτρέψουν μια συναλλαγή. Το Secure Element θα μπορούσε είτε να ενσωματωθεί στο τηλέφωνο ή στην κάρτα SIM.



Εικόνα 13. Smart Card Layout

Το chip διαθέτει οκτώ επαφές (Εικόνα 13), των οποίων οι λειτουργίες περιγράφονται παρακάτω:

C1: Supply Voltage (VCC)
C2: Reset (RST)
C3: Clock (CLK)
C4: AUX1
C5: Ground (GND)
C6: Programming Voltage (Vpp)
C7: Input/Output (I/O)
C8: AUX2

Οι επαφές C4 και C8 χρησιμοποιούνται, σύμφωνα με το πρότυπο ISO/IEC 7816-2:1999/Amd 1:2004, προαιρετικά για τις διεπαφές USB και άλλες χρήσεις.

Κεφάλαιο 4ο
Αδυναμίες Ασφάλειας - Ιδιωτικότητα Χρήστη

4.1 Γενικά

Ένα σημαντικό πρόβλημα για την υιοθέτηση της τεχνολογίας και των υπηρεσιών του e-Wallet στο χώρο του mobile banking, είναι η αίσθηση της ανασφάλειας. Στην έρευνα, που διεξήχθη από την Ομοσπονδιακή Τράπεζα των ΗΠΑ, το 48% των ερωτηθέντων ανέφερε, ότι ο κύριος λόγος για τη μη χρήση mobile banking ήταν: «Είμαι ανήσυχος για την ασφάλεια του mobile banking ». Στην ίδια μελέτη, οι ερωτηθέντες κλήθηκαν να βαθμολογήσουν την ασφάλεια του mobile banking για την προστασία των προσωπικών τους δεδομένων και το 32% τη χαρακτηρίζει ως «κάπως ανασφαλή» και «πολύ ανασφαλή», ενώ το 34% δεν ήταν σίγουρο για την ασφάλεια. Αυτές οι στατιστικές αντιπροσωπεύουν ένα σημαντικό εμπόδιο για τη χρήση των τραπεζικών προϊόντων κινητής τηλεφωνίας και υπηρεσιών [16].

Αναλύοντας τους κινδύνους για την ασφάλεια του κινητού χώρου, πολλά από αυτά τα συναισθήματα δεν είναι απαραιτήτως παράλογα. Η έλλειψη ωριμότητας στο χώρο του mobile banking, φέρνει πολλούς κινδύνους στους τομείς των νέων τεχνολογιών, καθώς νέοι και άπειροι συμμετέχοντες στο σύστημα και σε μια πολύπλοκη αλυσίδα ενεργειών εφοδιασμού αυξάνουν τους κινδύνους της ασφαλούς λειτουργίας ενός πολύπλοκου συστήματος.

Πολλοί από τους νεοεισερχόμενους είναι καινοτόμοι και δυναμικοί, με ελάχιστη όμως εμπειρία ή προσοχή στην ασφάλεια του τομέα. Αυτοί οι κίνδυνοι είναι περισσότερο εμφανείς στον τομέα ανάπτυξης εφαρμογών των κινητών και των δικτύων των κινητών. Νέοι κίνδυνοι παραβίασης της ιδιωτικής ζωής ήρθαν στο φως, όπως τα προσωπικά δεδομένα, που συλλέγονται από τις εφαρμογές, και τις πληροφορίες σχετικά με τη φυσική τοποθεσία του πελάτη. Τέλος, οι πελάτες είναι σε μεγάλο ποσοστό ηλεκτρονικά αναλφάβητοι ή έχουν υψηλή ανοχή στον κίνδυνο και δυστυχώς μπορούν να επιλέξουν υπηρεσίες που θέτουν την ασφάλεια και την προστασία της ιδιωτικής τους ζωής σε κίνδυνο.

Για την άρση των αμφιβολιών, που μοιραία τίθενται στην χρήση των παραπάνω υπηρεσιών, κρίνεται επιτακτική, η ανάλυση των αδυναμιών

ασφαλείας αυτών. Τις αδυναμίες αυτές θα επιχειρήσουμε να τις ταξινομήσουμε σε δύο μεγάλες κατηγορίες. Αυτές που αφορούν τις συσκευές που εμπλέκονται στη χρήση της υπηρεσίας και έχουν να κάνουν με το τρόπο λειτουργίας των τεχνολογιών που αναφέρθηκαν στο προηγούμενο κεφάλαιο. Ενώ στη δεύτερη κατηγορία συγκαταλέγονται αυτές που προέρχονται από τη χρήση της εφαρμογής.

4.2 Σημεία πώλησης (POS)

Τον Δεκέμβριο του 2013, καταγράφηκε ως επίθεση, ότι ένας χάκερ απέκτησε πρόσβαση σε περισσότερα από 70 εκατομμύρια αριθμούς πιστωτικών και χρεωστικών καρτών των πελατών, μέσω του σημείου πώλησης (POS) των συστημάτων της εταιρείας. Μία από τις μεγαλύτερες παραβιάσεις δεδομένων στην ιστορία των ΗΠΑ, η οποία κόστισε τη θέση του Διευθύνων Σύμβουλου και του Υπευθύνου Ασφαλείας της εταιρείας.

Αν και είναι ακόμα ασαφές το πώς ο χάκερ, κατάφερε να μολύνει το δίκτυο-στόχο με κακόβουλο λογισμικό, υπάρχουν πολλοί τρόποι για να εκμεταλλευτεί κάποιος ένα σύστημα POS. Για τις μικρές και μεσαίες επιχειρήσεις (ΜκΜΕ), οι απειλές είναι ακόμη μεγαλύτερες σε σχέση με τις μεγαλύτερες επιχειρήσεις. Αυτό οφείλεται στο γεγονός ότι οι περισσότερες από αυτές, δεν διαθέτουν τους πόρους για να λάβουν τα αναγκαία μέτρα ασφαλείας που θα αποτρέψουν επιθέσεις (ή να αντιληφθούν επιθέσεις, αν οι hackers καταφέρουν να διεισδύσουν στα συστήματά τους). Παρακάτω, θα αναφέρουμε εν συντομία τα οκτώ κορυφαία τρωτά σημεία της ασφάλειας των POS που απειλούν μικρομεσαίες επιχειρήσεις σήμερα [17]. Σε κάθε μια από τις παραπάνω απειλές θα αναφερθούν και ενδεικτικά αντίμετρα :

α. Οι προμηθευτές διαχειρίζονται τα κλειδιά κρυπτογράφησης χωρίς την απαραίτητη ασφάλεια υλικού.

Εδώ καταγράφεται ένα σοβαρό θέμα ασφάλειας: Εάν η εταιρεία αποθηκεύει τις πληροφορίες κρυπτογράφησης στην ίδια θέση, όπου αποθηκεύει τα δεδομένα του χρήστη, είναι σαν να «βάζει όλα τα αυγά σε ένα εύθραυστο καλάθι». Ωστόσο, αν φυσικά κρατήσει το κλειδί κρυπτογράφησης δεδομένων ξεχωριστά από τα δεδομένα του χρήστη, τότε όποιος αποκτά πρόσβαση στα

δεδομένα των χρηστών δεν θα έχει πρόσβαση στις πληροφορίες κρυπτογράφησης. Η απαραίτητη ασφάλεια υλικού, είναι μια φυσική συσκευή (module) που αποθηκεύει τα δεδομένα κρυπτογράφησης και μπορεί να συνδεθεί απευθείας σε υπολογιστές ή διακομιστές που έχουν πρόσβαση στα δεδομένα POS.

Εικόνα 14. Συσκευή POS

β. Δίκτυα επιχειρήσεων με μη διαχωρισμένα δεδομένα των POS

Όταν ένας οργανισμός χρησιμοποιεί το εταιρικό δίκτυο, για να στείλει ενημερώσεις συστήματος και ασφάλειας σε περιφερειακά στοιχεία POS και συσκευές, τότε μπαίνει σε σοβαρό κίνδυνο. Σε αυτή την περίπτωση, εάν κάποιος αποκτά πρόσβαση στο δίκτυο , έχει επίσης αποκτήσει πρόσβαση σε όλα τα δεδομένα POS.

Οργανισμοί με υψηλούς προϋπολογισμούς και ειδικούς της πληροφορικής έχουν διαχωρίσει τα δύο αυτά δίκτυα, προκειμένου να προβούν σε αλλαγές του συστήματος. Αυτή η προσέγγιση ωστόσο, είναι εξαιρετικά δύσκολη και δαπανηρή. Μια πιο εφικτή λύση για περισσότερες επιχειρήσεις είναι η εγκατάσταση ελέγχου πρόσβασης από το δίκτυο της επιχείρησης στα POS, που είναι μια πιο ασφαλής επιλογή διαθέσιμη για μικρομεσαίες εταιρείες.

Μια άλλη σημαντική σημείωση εδώ είναι τα καταστήματα που προσφέρουν Wi-Fi σε πελάτες πρέπει να εξασφαλίζουν, ότι οι συσκευές POS τους δεν είναι συνδεδεμένες στο ίδιο δίκτυο. Σε μια τέτοια περίπτωση η πρόσβαση στο Wi-Fi, μπορεί στη συνέχεια να βάλει σε κίνδυνο τα δεδομένα POS.

γ. Μη αναβάθμιση Λειτουργικού Συστήματος

Κάθε οργανισμός θα πρέπει να φροντίζει να ακολουθεί τις τελευταίες εκδόσεις των λειτουργικών συστημάτων που φέρουν οι τερματικές συσκευές. Η αλλαγή αυτή οφείλει να γίνει επειδή, οι παλιές εκδόσεις δεν υποστηρίζονται με αποτέλεσμα να μην λαμβάνουν ενημερώσεις ασφαλείας. Τέτοιες περιπτώσεις είναι «καλοδεχούμενες» από κακόβουλους χρήστες που βρίσκουν, πρόσφορα σημεία εισόδου στα δίκτυα οργανισμών και κατά επέκταση στα δεδομένα των POS.

δ. Προεπιλεγμένοι κωδικοί ασφαλείας από τον κατασκευαστή

Ακόμα και στην περίπτωση, που ο αρχικός κωδικός συσκευής POS, από τον κατασκευαστή είναι αρκετά περίπλοκος, είναι εξαιρετικά σημαντικό να αλλαχθεί ο κωδικός πρόσβασης, αφού η συσκευή εισάγεται στο λογισμικό του οργανισμού. Αυτό συμβαίνει, επειδή οι χάκερ γνωρίζουν τους καταλόγους αυτών των κωδικών πρόσβασης, από τα δίκτυα των κατασκευαστών και μπορούν στη συνέχεια να εισέλθουν στις συσκευές POS. Έτσι, ακόμα κι αν ένας οργανισμός λάβει όλες τις δυνατές προφυλάξεις για την ασφάλεια των δεδομένων, έχει αφήσει την μπροστινή πόρτα ξεκλείδωτη.

ε. Ύποπτες συσκευές

Η προμήθεια των συσκευών POS πρέπει να γίνεται από γνωστούς και αξιολογημένους παρόχους. Διαφορετικά, η αγορά ενός αμφιβόλου προέλευσης συστήματος POS, θέτει σε κίνδυνο τα δεδομένα των πελατών μιας εταιρείας. Με απευθείας πρόσβαση στην πιστωτική κάρτα του πελάτη, επίδοξοι χάκερ μπορούν να τραβήξουν δεδομένα χωρίς η εταιρία ή ο πελάτης να γνωρίζουν ότι κάτι πήγε στραβά. Τα μηχανήματα αυτά ενημερώνουν ότι η συναλλαγή δεν μπορεί να ολοκληρωθεί, αφήνοντας τον πελάτη να πιστεύει, ότι υπάρχει πρόβλημα με το POS ή την πιστωτική κάρτα ή ότι υπάρχει ένα πρόβλημα με το

back-end συστήματος. Στην πραγματικότητα, το μηχάνημα έχει απλά πλήρη πρόσβαση στα δεδομένα του πελάτη.

στ. Κακόβουλο Λογισμικό μέσω phishing

Είναι σημαντικό, κάθε εταιρία να ενημερώνει και να εκπαιδεύει τους υπαλλήλους της, να μην ανοίγουν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου. Hackers ενσωματώνουν συνδέσεις (links), σε μηνύματα ηλεκτρονικού ταχυδρομείου, που αν πατηθούν μπορεί να τους δώσουν πρόσβαση στον υπολογιστή του υπαλλήλου. Μόλις ο χάκερ πάρει τον έλεγχο της μηχανής, μπορεί να πλοηγηθεί σε όλο το δίκτυο και τους διακομιστές και να αποκτήσει πρόσβαση σε όλα τα δεδομένα. Εάν η εταιρία σταθεί τυχερή ή προσεκτική ώστε να μην αποθηκεύει τα δεδομένα POS στο ίδιο περιβάλλον δικτύου, δεν είναι ακόμα σαφές, κατά πόσο οι χάκερ μπορούν να αποκτήσουν απομακρυσμένη πρόσβαση σε μια συσκευή POS που είναι συνδεδεμένη με τον υπολογιστή που έχει παραβιαστεί.

ζ. RAM Scraping

Είναι μια παλιάς εποχής επίθεση που χρησιμοποιείται ακόμα σε ορισμένες περιπτώσεις. Είναι η τεχνική με την οποία οι εισβολείς υποκλέπτουν τα στοιχεία της πιστωτικής κάρτας, από τη μνήμη της συσκευής POS πριν αυτά κρυπτογραφηθούν στο δίκτυο. Όπως αναφέρθηκε προηγουμένως, διατηρώντας τα συστήματα POS απομονωμένα από το δίκτυο της επιχείρησης, θα περιοριστούν αυτά τα είδη των επιθέσεων (δεδομένου ότι οι χάκερ έχουν λιγότερα σημεία εισόδου σε συσκευές POS από ότι έχουν στο εταιρικό δίκτυο).

Ωστόσο, θα πρέπει με ρυθμισμένες διατάξεις ασφαλείας (π.χ. firewalls), να διασφαλιστεί ότι τα συστήματα POS επικοινωνούν μόνο με γνωστές συσκευές. Αυτό θα περιορίσει τους τρόπους με τους οποίους οι hackers μπορούν να έχουν πρόσβαση στα δεδομένα των συσκευών POS, αναγκάζοντάς τους να επισκιάσουν τους υπολογιστές ή διακομιστές εντός του δικτύου του οργανισμού για να «ξύσει» τη μνήμη RAM.

η. Skimming

Είναι η τεχνική μέσω της οποίας ένας χάκερ προχωράει σε εγκατάσταση κακόβουλου υλικού στη συσκευή POS, το οποίο στη συνέχεια θα τους επιτρέψει να σαρώσουν τα στοιχεία των πιστωτικών καρτών. Αυτό μπορεί να γίνει και μέσω του malware, αν δεν έχουν ακολουθηθεί μερικά από τα βήματα που αναφέρθηκαν νωρίτερα. Αν υπάρχουν πολλαπλά υποκαταστήματα, είναι σημαντικό να παρακολουθείται κεντρικά, με ποιο τρόπο οι συσκευές POS χρησιμοποιούνται και από ποιον.

4.3 Ευπάθειες Κινητών Συσκευών

Οι επιθέσεις στο κινητό τηλέφωνο στοχεύουν συνήθως στην απόκτηση των παρακάτω στοιχείων: το SE, τον επεξεργαστή NFC και το λειτουργικό σύστημα των κινητών. Το λειτουργικό σύστημα στα κινητά έχει αδύναμα σημεία, μέσω της θύρας εντοπισμού σφαλμάτων ή διαχειριστικά σφάλματα, τα οποία μπορούν να δώσουν πρόσβαση στην εφαρμογή πληρωμής στο κινητό. Επιπλέον, μηχανισμοί όπως το καταγραφικό οθόνης, μπορούν να αποκτήσουν πρόσβαση σε σημαντικές πληροφορίες του χρήστη. Προτεινόμενα μέτρα ασφαλείας είναι τα εκτός σύνδεσης PIN, οι έλεγχοι λειτουργικού συστήματος, whitebox κρυπτογραφία και το Trusted Execution Environment (TEE), για την εξασφάλιση του πληκτρολόγιου και της οθόνης.

Οι κίνδυνοι ασφάλειας, που συνδέονται με κινητές συσκευές είναι πολύ παρόμοιοι με οποιαδήποτε άλλη υπολογιστική συσκευή, με μερικές βασικές εξαιρέσεις:

✓ Οι κινητές συσκευές έχουν μικρότερο μέγεθος και ως εκ τούτου είναι πιο ευαίσθητες στην απώλεια ή την κλοπή.

✓ Οι φορητές συσκευές είναι πιο προσωπικές και δημιουργούν την τάση στους χρήστες να τις χρησιμοποιούν με πιο προσωπικό και εμπιστευτικό τρόπο.

✓ Οι έλεγχοι ασφαλείας και τα διαθέσιμα εργαλεία δεν έχουν ωριμάσει για να μπορούν να φιλοξενήσουν τους περιορισμούς λόγω της δεδομένης επεξεργαστικής ισχύος και της περιορισμένης διάρκειας ζωής της μπαταρίας.

Οι βασικοί κίνδυνοι για την κινητή συσκευή περιλαμβάνουν:

- Malware

Το Malware αποτελεί μια αυξανόμενη πρόκληση για φορητές συσκευές. Ενδεικτικά αναφέρεται, ότι σύμφωνα με την έκθεση της Juniper το έτος 2013, το ποσό των κακόβουλων προγραμμάτων που απευθύνονται σε κινητές συσκευές αυξήθηκε κατά 155% από το προηγούμενο έτος. Το ενενήντα εννέα τοις εκατό του κακόβουλου λογισμικού ανάπτυξης συνοψίζεται σε δύο κατηγορίες: spyware και SMS Trojans. Το κακόβουλο λογισμικό Malware στην πλατφόρμα Android αυξάνεται εκθετικά από τα 400 δείγματα που εντοπίστηκαν, τον Ιούνιο του 2011 στα 13000 τον Δεκέμβριο του ίδιου έτους. Σύμφωνα με την έκθεση της Kaspersky Lab, το κακόβουλο λογισμικό που απευθύνεται σε κινητές συσκευές αυξήθηκε 6,4 φορές το 2011, με τη συντριπτική πλειοψηφία των κινητών που ανιχνεύθηκε να στοχεύουν σε συσκευές Android [18].

- Κακόβουλες εφαρμογές

Ένα σημείο κλειδί, μέσω του οποίου το ύποπτο λογισμικό παίρνει πρόσβαση στην κινητή συσκευή είναι μέσα από κακόβουλες εφαρμογές. Η ακεραιότητα των εφαρμογών είναι το τρωτό σημείο σε συνάρτηση με τις κινητές συσκευές. Υπάρχουν διάφορες κακόβουλες εφαρμογές που εμφανίζονται, ως νόμιμες, στην λήψη των οποίων προχωρούν οι χρήστες και έχουν ως αποτέλεσμα στη συνέχεια να μολυνθούν. Τον Απρίλιο του 2012, ανακαλύφθηκε, ότι μια κακόβουλη έκδοση της εφαρμογής Instagram (δωρεάν δημοφιλής εφαρμογή κοινής χρήσης φωτογραφιών) για το Android ήταν να προωθούνται προσφορές σε Ρώσους χρήστες του Android μέσω μιας ιστοσελίδας που φαινόταν να είναι η νόμιμη τοποθεσία λήψης [19].

- Παραβιάσεις της ιδιωτικότητας σε σχέση με τη συλλογή εφαρμογών και τη διανομή των δεδομένων

Ένας καταγεγραμμένος κίνδυνος της ακεραιότητας των εφαρμογών είναι το jail breaking. Πρόκειται για μια μορφή πρόσβασης με προνομιακά δικαιώματα (privileged escalation), που επιτρέπει στον χρήστη να αποκτήσει διακαιώματα διαχειριστή (root) σε μια συσκευή, η οποία επιτρέπει την πρόσβαση σε όλα τα αρχεία, τα κρυφά αρχεία ή τα προστατευμένα αρχεία στη συσκευή. Τη στιγμή,

που μια συσκευή είναι jail broken, ο χρήστης μπορεί να εγκαταστήσει οποιαδήποτε εφαρμογή επιθυμεί στη συσκευή χωρίς να περάσει από τα επίσημα καταστήματα (π.χ. playstore), του κατασκευαστή της συσκευής. Το Jail breaking επιτρέπει επίσης στο χρήστη να χρησιμοποιήσει το τηλέφωνο σε ένα διαφορετικό ασύρματο πάροχο, δεδομένου ότι οι παραπάνω συχνά κλειδώνουν μια συσκευή στο δίκτυό τους. Η συσκευή τίθεται σε αυξημένο κίνδυνο για την ασφάλεια καθώς τα πρότυπα για την προστασία της συσκευής παρακάμπτονται από ενέργειες του χρήστη ή μη επικυρωμένες εφαρμογές. Επιπλέον, οι εγγυήσεις της συσκευής μπορεί να καταλυθούν. Παρά τους κινδύνους αυτούς, οι προσπάθειες για να ξεπεραστούν τα εμπόδια των κατασκευαστών από το Jail breaking, εξακολουθούν να υφίστανται.

- Υποδομή Wireless

Εκτός από το διαδίκτυο, οι κινητές συσκευές έχουν ένα άλλο κλειδί δικτύου που ευθύνεται για την επεξεργασία των κινητών επικοινωνιών. Το ασύρματο δίκτυο είναι η πρωταρχική διεπαφή για την κινητή συσκευή. Το ράδιο κομμάτι της φορητής συσκευής επικοινωνεί με τις τοποθεσίες των κυψελών. Οι κυψέλες, στη συνέχεια, επικοινωνούν μέσω αποκλειστικού κυκλώματος ή μικροκυμάτων με το κινητό κέντρο μεταγωγής (data center), το οποίο περιέχει τόσο τον εξοπλισμό και τα συστήματα επεξεργασίας φωνής όσο και την επεξεργασία των δεδομένων. Το κέντρο μεταγωγής περιέχει την πύλη πρόσβασης στο Internet και στα άλλα δίκτυα μεταφοράς. Εάν υπάρχει αδυναμία ασφαλείας σε οποιοδήποτε τμήμα αυτού του δικτύου, μπορεί να βάλει τα δεδομένα του πελάτη σε κίνδυνο.

- Υποδομή Πληρωμών

Η υποδομή πληρωμών μπορεί να έχει επίσης τρωτά σημεία που οδηγούν σε κίνδυνο της ασφάλειας. Αυτό μπορεί να έρθει με τη μορφή των τρωτών σημείων στα POS που είδαμε προηγούμενα ή στην πραγματικά πολύπλοκη αλυσίδα διαδικασιών που περιλαμβάνει το σύστημα πληρωμών. Όπως έχει ήδη αναφερθεί, το NFC δεν έχει δυνατότητες κρυπτογράφησης και ως εκ τούτου, είναι ευάλωτο στην εκμετάλλευση της ασφάλειας, αν δεν εφαρμοστεί σωστά. Το σήμα RF που λειτουργεί το NFC, έχει τη δυνατότητα να διαβαστεί ή να

υποκλαπεί έως και αρκετά μέτρα μακριά με τον κατάλληλο εξοπλισμό, χωρίς να χρειάζεται οπτική επαφή. Κατάλληλη κρυπτογράφηση, θα παρέχει επαρκή προστασία από υποκλοπές.

- Τρωτά SMS

Η υπηρεσία σύντομων μηνυμάτων (SMS) είναι επιρρεπής σε κακή χρήση, συμπεριλαμβανομένων την ανακατεύθυνση, πειρατεία και πλαστογράφηση. Στις αρχές του 2012, ένας προγραμματιστής ανέπτυξε ένα πρόγραμμα που μπορούσε να επιτρέψει σε κάποιον να εξαπολύσει επιθέσεις social engineering και πλαστογράφησης SMS με σκοπό την λήψη πολύτιμων πληροφοριών και δυνητικά ακόμη και χρημάτων. Το SMS κανάλι μπορεί επίσης να τεθεί σε κίνδυνο από κακόβουλο λογισμικό, όπως ήταν η περίπτωση με μια κακόβουλη εφαρμογή που διατίθεται δωρεάν ως μια πολύ γνωστή εφαρμογή Android. Παράδειγμα αυτών αποτελεί η ψεύτικη εφαρμογή Gmail Android, που ονομάζεται DDSpy και ήταν σε θέση να παρακολουθεί τις αναρτήσεις SMS μηνυμάτων, αρχείων καταγραφής κλήσεων, και φωνητικά αρχεία σε έναν απομακρυσμένο εξυπηρετητή.

- Ευπάθειες Λειτουργικού συστήματος και Υλικού

Υπάρχουν επίσης τρωτά σημεία, που σχετίζονται με συγκεκριμένους κατασκευαστές κινητών συσκευών και τις εκδόσεις του λειτουργικού συστήματος. Παρόμοια με τον παραδοσιακό χώρο των υπολογιστών, τα τρωτά σημεία λειτουργικού συστήματος ανακαλύπτονται αρκετά τακτικά. Η διαφορά στον χώρο των κινητών είναι ότι δεν υπάρχει κυρίαρχο λειτουργικό σύστημα και ως εκ τούτου είναι ένα πιο σύνθετο περιβάλλον για την αντιμετώπιση των αδυναμιών του λειτουργικού. Επιπλέον, οι τελικοί χρήστες έχουν τον έλεγχο της διασύνδεσης των συσκευών τους, και το γεγονός αυτό αφήνει έκθετη την ασφάλεια της συσκευής, δεδομένου ότι ορισμένοι τελικοί χρήστες θα είναι επιμελής και μερικοί όχι, όσον αφορά την ενημέρωση του λειτουργικού τους.

- Τέλος, αδυναμίες μπορεί να προέρθουν από την έλλειψη ανάπτυξης αξιόπιστων εργαλείων ελέγχου ύποπτου λογισμικού, που θα μπορούσαν αποδοτικά, να αποτρέψουν κακόβουλες ενέργειες στη συσκευή.

4.4 Ευπάθειες Εφαρμογών e-Wallet

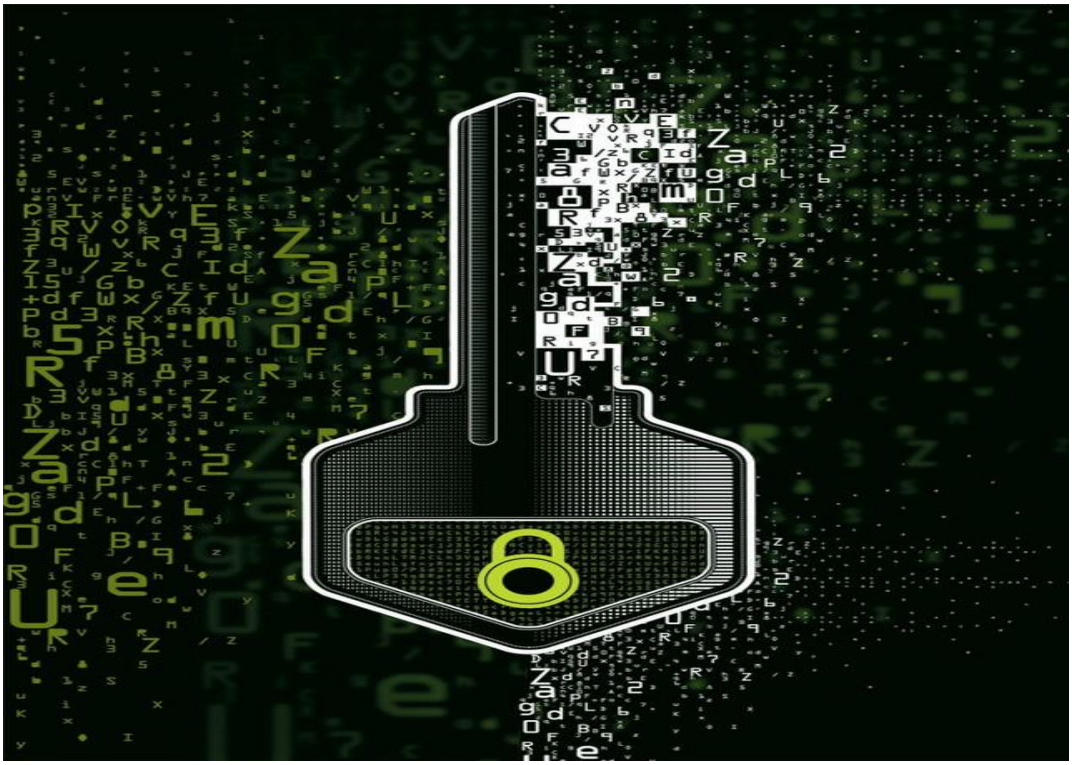
Η Ιδιωτικότητα των πληροφοριών των χρηστών, είναι ένα ιδιαίτερα δύσκολο θέμα, καθώς οι φορητές συσκευές είναι πολύ πιο εξατομικευμένες και συνδέονται με την ταυτότητα του χρήστη, σε σχέση με ένα παραδοσιακό υπολογιστή. Κίνδυνοι που σχετίζονται με νόμιμες εφαρμογές που περνούν δεδομένα χρηστών σε άλλες εφαρμογές ή σε τρίτα μέρη με μη εξουσιοδοτημένο τρόπο κερδίζουν όλο και περισσότερη προσοχή στην αγορά.

Μια πρόσφατη περίπτωση περιλαμβάνει τα προσωπικά δεδομένα πελάτη ΕΕ που αποστέλλονται στη βάση δεδομένων ενός διαφημιστή με έδρα τις ΗΠΑ. Σε αυτήν την περίπτωση συγκαταλέγονται πολλές εφαρμογές Android, που είχαν κατηγορηθεί για παραβίαση της νομοθεσίας περί προστασίας δεδομένων της ΕΕ με την αποστολή προσωπικών πληροφοριών σε μια διαφημιστική εταιρία των ΗΠΑ που ονομάζεται Mobclix χωρίς τη ρητή άδεια του χρήστη [20].

Μπορεί επίσης να υπάρχουν τρωτά σημεία ασφάλειας, που σχετίζονται με το λειτουργικό σύστημα και δίνουν μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες για το χρήστη ή το περιεχόμενο. Στις αρχές του 2012, υπήρχε μια ευπάθεια που ανακαλύφθηκε τόσο στο iOS όσο και στο Android, που έδωσε αιτήσεις πρόσβασης σε βιβλιοθήκες φωτογραφιών του χρήστη χωρίς άδεια [21].

Το Geolocation περιλαμβάνει πρόσθετες πληροφορίες, που μπορούν να συγκεντρωθούν από την εφαρμογή και την κοινή χρήση με μη εξουσιοδοτημένο τρόπο. Αυτό είναι ένα ιδιαίτερα δύσκολο ζήτημα, δεδομένου ότι πολλές εφαρμογές ζητούν την άδεια του χρήστη να χρησιμοποιεί τα δεδομένα θέσης του, χωρίς όμως να είναι σαφές με ποιούς τρόπους η εφαρμογή μπορεί να χρησιμοποιεί τα δεδομένα.

Ένα πιθανό μειονέκτημα στο κινητό πορτοφόλι και στη πρόταση ασφάλειας του ασφαλούς στοιχείου (SE), είναι ότι ένα ενιαίο pin θα ξεκλειδώνει όλους τους λογαριασμούς, που αποθηκεύονται στο πορτοφόλι. Αυτό έρχεται σε αντίθεση με τις πλαστικές κάρτες, όπου μπορεί να ρυθμιστεί κάθε κάρτα να χρησιμοποιεί ένα διαφορετικό pin. Έτσι τα κινητά πορτοφόλια θα παρουσίαζαν μεγαλύτερη έκθεση σε ζημία, σε περίπτωση που μια συσκευή με εφαρμογή e-Wallet και μοναδικό pin τεθεί υπό κακόβουλο έλεγχο.



Εικόνα 15. Διαρροή Δεδομένων

Μια επιτυχημένη επίθεση στο λογισμικό, που βασίζονται οι εφαρμογές πληρωμών σε κινητά, θα μπορούσε να αποτελέσει η τροποποίηση του πηγαίου κώδικα, όπου ο εισβολέας αποκτά πρόσβαση σε όλα τα «κρυμμένα» στοιχεία της εφαρμογής (όπως token και κρυπτογραφικά κλειδιά). Η ακεραιότητα μιας εφαρμογής μπορεί επίσης να τεθεί σε κίνδυνο από αλλοιωμένα δεδομένα και εφαρμογές κλώνους με αποτέλεσμα την υποκλοπή ευαίσθητων δεδομένων. Ένα άλλο σημείο ευπάθειας είναι οι συσκευές POS των εμπόρων (που αναλύσαμε προηγουμένως), μέσω των οποίων θα μπορούσε κάποιος ως κακόβουλος έμπορος να παρέμβει με την εφαρμογή και να ελέγξει το POS.

Με αυτούς τους τρόπους, ένας κακόβουλος μπορεί να αποκτήσει πρόσβαση σε στοιχεία του χρήστη, της κάρτας και στη χρήση κλειδιών. Μηχανισμοί ασφαλείας, όπως whitebox και κρυπτογραφία, μειώνουν την πιθανότητα της κλωνοποίησης και υποκλοπής των εφαρμογών πληρωμής. Τροφοδότηση των δεδομένων ασφαλείας στο SE ή η διανομή του token πληρωμής αποτελούν σημεία ευπάθειας των εφαρμογών πληρωμής στο κινητό.

4.5 Ευπάθειες τεχνολογιών e-Wallet

Η ανάλυση μιας απειλής κατά των εφαρμογών e-Wallet, πρέπει να περιλαμβάνει την ανάλυση των ευπαθειών που σχετίζονται με το περιβάλλον του συστήματος. Ο στόχος αυτού του βήματος είναι να παρουσιαστεί μία λίστα από ευπάθειες του συστήματος (λάθη ή αδυναμίες) που θα μπορούσαν να γίνουν αντικείμενο εκμετάλλευσης από ενδεχόμενες πηγές απειλών. Η λίστα αυτή περιλαμβάνει τις τεχνολογίες που χρησιμοποιούν οι εφαρμογές, καθώς επίσης και το σύστημα που συμμετέχει στην εξυπηρέτηση των διαδικασιών για την ολοκλήρωση μιας συναλλαγής. Συνοπτικά και ανά κατηγορία αναλύονται, ως εξής:

α. Σύστημα που βασίζεται στο σύννεφο (cloud)

Μια επιτυχημένη επίθεση βασισμένη στο cloud συνεπάγεται μια απόπειρα να παραποιηθούν δεδομένα ή να αποκαλυφθούν ευαίσθητες πληροφορίες. Πιθανές απειλές για τις εφαρμογές πληρωμών που βασίζονται στο cloud περιλαμβάνουν την παρακολούθηση των ευαίσθητων δεδομένων από έναν εισβολέα πλαστογραφώντας την ταυτότητας του, την υποκλοπή δεδομένων από κακόβουλο λογισμικό και την ανακατεύθυνση των δεδομένων μιας εφαρμογής σε διαφορετικό κινητό τηλέφωνο.

Με αυτές τις μεθόδους, ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στα στοιχεία χρηστών και καρτών, σε τιμές από μεθόδους επαλήθευσης της κάρτας, χρησιμοποίηση των κλειδιών, και ακόμη και ολόκληρες εφαρμογές κινητής πληρωμής. Οι μεγαλύτερες προκλήσεις είναι η ασφαλή πρόσβαση και ο έλεγχος ταυτότητας του χρήστη στο σύννεφο. Για ένα σύστημα, που βασίζεται σε σύννεφο για να χειριστεί πληρωμές με τεχνολογία tokenization, πρέπει να είναι σε θέση να διαχειριστεί τα token, με κωδικοποίηση και αποκωδικοποίηση των ευαίσθητων δεδομένων.

β. Τεχνολογία Secure element

Η επίπτωση μιας επίθεσης στο SE είναι υψηλή, ωστόσο, η πιθανότητα μιας επιτυχούς επίθεση είναι πολύ χαμηλή λόγω του υψηλού επίπεδου ασφάλειας στο απαραβίαστο του SE. Το πιο κρίσιμο σημείο της ασφάλειας είναι

ο έλεγχος πρόσβασης στο SE, ο οποίος καθορίζει την πρόσβαση για τις εφαρμογές στα κινητά. Η πρόσβαση στο SE βασίζεται σε πιστοποιητικά, που παρέχονται από τον πάροχο της υπηρεσίας, και χρησιμοποιούνται για τον έλεγχο ταυτότητας ή την υπογραφή της παροχής υπηρεσιών της εφαρμογής στο SE.

Στο ασφαλές στοιχείο είναι αποθηκευμένα κλειδιά κρυπτογράφησης, τα οποία είναι ευάλωτα σε κίνδυνο, αν αυτά δεν προστατεύονται κατάλληλα από μη εξουσιοδοτημένη πρόσβαση και χρήση. Οι εφαρμογές πληρωμών στα κινητά χρησιμοποιούν έναν αριθμό PIN ή κωδικό πρόσβασης που απαιτείται για να ξεκλειδώσει τα δεδομένα στο ασφαλές στοιχείο. Η πολυπλοκότητα του PIN, που έχει επιλεγεί από τον χρήστη, είναι ένας παράγοντας στον προσδιορισμό του βαθμού προστασίας των εφαρμογών πληρωμής στα κινητά τηλέφωνα. Τα ασφαλή στοιχεία που είναι ενσωματωμένα στην κάρτα SIM ή τη συσκευή επωφελούνται από επιπλέον προστασία, που παρέχεται από το λειτουργικό σύστημα της κινητής συσκευής, η οποία απαγορεύει τις εφαρμογές να έχουν πρόσβαση στο ασφαλές στοιχείο.

Μόλις ξεκλειδωθεί το ασφαλές στοιχείο, είναι ευάλωτο σε μη εξουσιοδοτημένη πρόσβαση. Οι εφαρμογές πληρωμών στα κινητά μετριάζουν αυτήν την ευπάθεια, με την ανάπτυξη χρονικών ορίων αδράνειας για το αυτόματο εκ νέου κλείδωμα του ασφαλούς στοιχείου. Οι εννοιολογικές μέθοδοι, που έχουν προταθεί, σύμφωνα με τις οποίες ένας εισβολέας θα μπορούσε να εξαπατήσει μια συσκευή διατηρώντας το NFC και το ασφαλές στοιχείο ενεργά μετά από μια συναλλαγή, και ως εκ τούτου ξεκλείδωτα. Μια τέτοια επίθεση θα μπορούσε ακόμα να κερδίσει και φυσική πρόσβαση στη συσκευή, προκειμένου να ολοκληρωθεί μια παράνομη συναλλαγή.

γ. Τεχνολογία tokenization

Δεδομένου ότι η συνάρτηση hash είναι ντετερμινιστική, προκειμένου να αποφευχθεί η επίθεση γνωστή ως λεξικό, θα πρέπει να προστεθεί ποσότητα salt (αλάτι) για την αύξηση της ασφάλειας. Αλλά για πολλαπλών χρήσεων token, πολλοί πάροχοι (π.χ. visa), συνιστούν τη χρήση του ίδιου αλατιού ανά έμπορο. Επαναχρησιμοποίηση της ίδιας ποσότητας αλατιού δεν προσφέρει καμία

υπολογιστική πολυπλοκότητα. Εάν η ποσότητα ενός έμπορου γίνει γνωστή, τότε είναι εφικτό να υπολογιστεί οποιοσδήποτε αριθμός κάρτας πληρωμών με τιμή κατακερματισμού, χρησιμοποιώντας επίθεση λεξικό.

Δεύτερον, μια 64-bit ποσότητα αλατιού, μπορεί να μην είναι επαρκής. Συμφώνα με το NIST [22], ένα ελάχιστο επίπεδο ασφάλειας το 2010 ήταν τα 80 bits . Η ECRYPT II σχολιάζει επίσης ότι ασφάλεια στα 64 bit δεν πρέπει να χρησιμοποιείται για εμπιστευτικότητα δεδομένων σε νέα συστήματα [23]. Δεδομένης της αύξησης της υπολογιστικής ισχύος τα τελευταία χρόνια, θα είναι δυνατόν στο επόμενο διάστημα ασφάλεια στα 64-bit να μπορεί να δεχθεί αποτελεσματική επίθεση σε πραγματικό χρόνο από υψηλής απόδοσης παράλληλα συστήματα.

Μια βασική διαδικασία για πληρωμές μέσω κινητού τηλεφώνου είναι η δυνατότητα ασφαλούς διάταξης καθώς και η εκ νέου παροχή ασφαλών στοιχείων. Θα πρέπει να διατηρηθεί η ασφάλεια σε καθεμιά από αυτές τις διαδικασίες, καθώς αποτελούν μια πιθανή ευκαιρία για τους επιτιθέμενους να υποκλέψουν ευαίσθητες πληροφορίες του λογαριασμού.

Υπάρχουν δύο τύποι μέτρων ασφαλείας για τον περιορισμό του κινδύνου:

• Μείωσης της πιθανότητας επιτυχούς επίθεσης

Η πιθανότητα μιας επιτυχημένης επίθεσης μειώνεται μέσω της εφαρμογής ισχυρών και επαρκών μέτρων ασφάλειας. Αυτό θα μπορούσε να γίνει, για παράδειγμα, με την αποθήκευση ευαίσθητων δεδομένων σε απαραβίαστους κλειστούς χώρους (tamper-proof). Επίσης, κρύβοντας την πληροφορία μέσω κρυπτογράφησης μπορεί να δυσκολέψει ή να αποτρέψει την προσπάθεια κακόβουλης επίθεσης.

• Μείωση της επίπτωσης της επιτυχημένης επίθεσης

Η επίδραση μιας επιτυχημένης επίθεσης μειώνεται με τη μείωση της αξίας των αγαθών, που μπορούν να ληφθούν από έναν εισβολέα. Στο tokenisation, τα ευαίσθητα δεδομένα (αγαθά), αντικαθίσταται από ένα λιγότερο ευαίσθητο ισοδύναμο, το token. Η αξία της πραγματικής πληροφορίας μειώνεται δραστικά και γίνεται λιγότερο ενδιαφέρουσα για έναν εισβολέα. Τα

tokens μπορούν να παράγονται άμεσα και να αντικατασταθούν χωρίς να διακυβεύεται το PAN . Δύο μορφές tokenisation είναι:

• EMVCo tokenisation: Μια tokenised έκδοση του PAN συνδέεται με τον χρήστη και είναι αποθηκευμένη σε μια μοναδική συσκευή.

• Χρησιμοποιώντας το πλήκτρο tokenisation: Ένα token παράγεται για μια μονή ή περιορισμένη χρήση στην οποία ο χρήστης αυθεντικοποιείται πριν από την εγκατάσταση της ασφαλούς σύνδεσης.

4.6 Ιδιωτικότητα χρήστη εφαρμογών e-Wallet

Το 2011, 535 περιστατικά παραβίασης δεδομένων διαπράχθηκαν στις Ηνωμένες Πολιτείες, με αποτέλεσμα την κλοπή πάνω από 30 εκατομμύρια ευαίσθητων αρχείων καταναλωτών (περιλαμβανομένων εκατομμύριων αριθμών από χρεωστικές και πιστωτικές κάρτες) [24]. Παραβιάσεις δεδομένων είναι συνεχώς στην επικαιρότητα, και πρόσφατες δημοφιλής περιπτώσεις δείχνουν ότι κανένας οργανισμός δεν είναι στο απυρόβλητο, ειδικά καθώς οι εγκληματίες αναπτύσσουν ολοένα και πιο εξελιγμένες μεθόδους για να εκμεταλλευτούν τα τρωτά σημεία του συστήματος πληρωμών.

Ορισμένοι πάροχοι κινητής έχουν δώσει μεγάλη βαρύτητα στα ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας. Έχουν φροντίσει κατά την εκτέλεση της υπηρεσίας να μην μεταδίδονται σε κανένα σημείο της διαδρομής μη κρυπτογραφημένα δεδομένα, όπως είναι ο αριθμός της κάρτας, η ημερομηνία λήξης και τα στοιχεία του κατόχου.

Για τους περισσότερους εμπόρους, υπάρχουν δύο σημεία στη διαδικασία πληρωμής, όπου τα ευαίσθητα δεδομένα του κατόχου της κάρτας είναι σε κίνδυνο να εκτεθούν ή να κλαπούν:

α. Πριν την έγκριση

Όταν ο έμπορος έχει συλλέξει τα δεδομένα του καταναλωτή και αποστέλλονται ή είναι σε αναμονή για να σταλούν στον αγοραστή / επεξεργαστή.

β. Μετά την έγκριση

Όταν τα δεδομένα του κατόχου της κάρτας σταλούν πίσω στον έμπορο με την απάντηση της εξουσιοδότησης από τον αγοραστή / επεξεργαστή, και τοποθετούνται σε κάποια μορφή αποθήκευσης στο εμπορικό περιβάλλον και χρησιμοποιούνται για αναλύσεις και άλλες διαδικασίες back-office.

Εικόνα 16.Ασφάλεια Προσωπικών Δεδομένων

Παρόλο που οι υπηρεσίες e-Wallet, χρησιμοποιούν τις πιο εξελιγμένες τεχνολογίες για να προσφέρουν την ασφάλεια και την ιδιωτικότητα των πραγματικών κατόχων, ωστόσο ο τρόπος εγκατάστασης των εφαρμογών στη συσκευή, για τη λήψη της υπηρεσίας παρουσιάζει μια σοβαρή αδυναμία. Η συγκεκριμένη αδυναμία εντοπίστηκε κατά την διάρκεια της παρούσας εργασίας στο πλαίσιο των δοκιμών, που παρουσιάζονται σε επόμενο κεφάλαιο. Αυτή έχει να κάνει με το γεγονός, ότι η εφαρμογή μπορεί να εγκατασταθεί σε συσκευές με διαχειριστικά (root) δικαιώματα παρά τις αντίθετες διαβεβαιώσεις στις οδηγίες από τις τράπεζες. Αύτη η αδυναμία θέτει σε κίνδυνο, τόσο την ασφάλεια της διαδικασίας πληρωμών όσο και των δεδομένων του χρήστη, αφού μπορεί να αποτελέσει αφετηρία πολλαπλών γνωστών και μη επιθέσεων.

Στο σημείο αυτό κρίνεται σκόπιμο, στο πλαίσιο της ιδιωτικότητας του χρήστη, να αναφέρουμε ότι κατά την εγκατάσταση και εκτέλεση της εφαρμογής e-Wallet σε μια κινητή συσκευή λαμβάνουν χώρα, τα κάτωθι:

- Ο αριθμός της πραγματικής κάρτας κρυπτογραφείται και φυλάσσεται σε secure server της Τράπεζας.

- Κατά την διάρκεια προσθήκης μιας κάρτας στο e-Wallet, τα στοιχεία αποστέλλονται κρυπτογραφημένα, αποκρυπτογραφούνται και προωθούνται στο ανάλογο σύστημα, αφού κρυπτογραφηθούν εκ νέου και χωρίς προηγουμένως να αποθηκευτεί οποιαδήποτε πληροφορία στα συστήματα των παρόχων κινητής.

- Η πραγματική φυσική κάρτα αντιστοιχείται με μία ψηφιακή κάρτα, ένα «πλασματικό αριθμό κάρτας» δηλαδή, η οποία φυλάσσεται στο κινητό και θα χρησιμοποιείται σε κάθε πληρωμή. Ο αριθμός συσκευής, πού έχει αντικαταστήσει το PAN, είναι κρυπτογραφημένος και αποθηκευμένος καθώς και εξίσου κρυπτογραφημένος στο SE, στο οποίο η πρόσβαση είναι απόλυτα ελεγχόμενη και περιορισμένη. Επιπλέον, ο αριθμός που αποθηκεύεται στο SE είναι ένας τυχαίος αριθμός και όχι το PAN, με αποτέλεσμα να μην υπάρχει στην συσκευή πλέον καμία σύνδεση με τον πραγματικό αριθμό της κάρτας.

- Ανά τακτά διαστήματα όταν υπάρχει σύνδεση με το internet, κατά τη διενέργεια πληρωμής, οι παράμετροι ασφαλείας της ψηφιακής κάρτας ανανεώνονται με αυτόν τον τρόπο.

- Η αλλαγή mPIN ανά τακτά διαστήματα, ακολουθώντας τις οδηγίες της εφαρμογής, είναι επιβεβλημένη διότι η πληροφορία αυτή δεν κρυπτογραφείται και είναι κρίσιμη η ασφάλεια της.

- Στις συναλλαγές σε φυσικό κατάστημα, με τη χρήση της τεχνολογίας NFC, δεν αποστέλλονται τα πραγματικά στοιχεία της κάρτας, αφού άλλωστε δεν τα γνωρίζει η συσκευή αλλά αντιθέτως αποστέλλεται ένας τυχαίος αριθμός, ο οποίος δεν μπορεί από μόνος του να χρησιμοποιηθεί, αφού δεν συνδέεται με τα πραγματικά στοιχεία της κάρτας. Επιπλέον για την αποστολή των στοιχείων στην τερματική συσκευή PoS, θα πρέπει ο χρήστης να δώσει το mPin. Τα στοιχεία των συναλλαγών δεν είναι προσβάσιμα στους παρόχους κινητής παρά μόνο στις τράπεζες.

- Στις συναλλαγές, που πραγματοποιούνται όλα τα στοιχεία σε όλη την αλυσίδα των διαδικασιών που απαιτούνται, είναι κρυπτογραφημένα για την αποφυγή κακόβουλων επιθέσεων και την ασφάλεια των δεδομένων.

- Κατά την εγκατάσταση των εφαρμογών, e-Wallet, σε μία κινητή συσκευή, ζητείται πρόσβαση σε δεδομένα της συσκευής (όπως π.χ. φωτογραφίες, αρχείο καταγραφής κλήσεων), που δεν έχουν καμία σχέση με την λειτουργία της εφαρμογής και θέτουν σε κίνδυνο τα προσωπικά δεδομένα και την ιδιωτικότητα του χρήστη.

Κεφάλαιο 5ο
Ψηφιακή Εγκληματολογία-Ψηφιακά Πειστήρια

5.1 Γενικά

Η **Εγκληματολογική Επιστήμη** (Forensic Science), είναι η εφαρμογή της επιστήμης στο ποινικό και αστικό δίκαιο, κυρίως, σχετικά με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, κατά τη διάρκεια της ποινικής έρευνας, όπως διέπεται από τις νομικές προδιαγραφές των παραδεκτά αποδεικτικών στοιχείων και την ποινική διαδικασία. Σύγχρονα παραδείγματα της επιστήμης αυτής, αποτελούν η ανάλυση DNA και η εξέταση των δακτυλικών αποτυπωμάτων.

Εικόνα 17. Forensics Science

Η λέξη Forensics προέρχεται από το λατινικό όρο forensis, που σημαίνει «του ή πριν από το φόρουμ» [25]. Η ιστορία του όρου, προέρχεται από τη Ρωμαϊκή εποχή, κατά την οποία ένα ποινικό αδίκημα σήμαινε την παρουσίαση της υπόθεσης ενώπιον μιας ομάδας δημόσιων προσώπων στο φόρουμ. Τόσο το πρόσωπο που κατηγορείται για το έγκλημα όσο και ο κατήγορος θα δώσουν ομιλίες με βάση την προσέγγιση της ιστορίας από την πλευρά τους. Η υπόθεση θα κλείσει υπέρ του ατόμου με το καλύτερο επιχείρημα και την καλύτερη έκφραση. Αυτή η προέλευση αποτελεί την πηγή των δύο σύγχρονων χρήσεων της λέξης Forensics, ως μια μορφή νομικών αποδείξεων και ως μια κατηγορία δημόσιας παρουσίασης. Στη σύγχρονη χρήση, ο όρος εγκληματολογίας στο

χώρο της εγκληματολογικής επιστήμης μπορεί να θεωρηθεί σωστός, καθώς ο όρος Forensics είναι πραγματικά ένα συνώνυμο, που επιτρέπεται ή είναι συναφής με τα δικαστήρια. Ωστόσο, ο όρος είναι σήμερα τόσο στενά συνδεδεμένος με το επιστημονικό πεδίο, που πολλά λεξικά περιλαμβάνουν την έννοια που εξισώνει τη λέξη Forensics με την εγκληματολογική επιστήμη.

Πατέρας της εγκληματολογικής επιστήμης θεωρείται ο Αρχιμήδης. Η πρώτη γνωστή εφαρμογή της εγκληματολογικής επιστήμης πραγματοποιήθηκε από έναν Άραβα μηχανικό, τον 7ο αιώνα, ο οποίος χρησιμοποιούσε τα δαχτυλικά αποτυπώματα για να αποδείξει την ταυτοπροσωπία δανειστών και δανειοληπτών. Συστηματική εφαρμογή της εγκληματολογικής επιστήμης στον ευρωπαϊκό χώρο παρατηρείται αρχικά τον 16ο αιώνα. Στους αιώνες που ακολούθησαν η εγκληματολογική επιστήμη εδραιώθηκε στον τομέα της διερεύνησης του εγκλήματος. Σήμερα η έρευνα του συνόλου των εγκλημάτων, στηρίζεται κατά μεγάλο ποσοστό στην εγκληματολογική επιστήμη. Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα, χρονολογείται το 1820 από τον Γάλλο Joseph-Marie Jacquard.

Η **Ψηφιακή Εγκληματολογία** (Digital Forensics), είναι «η επιστήμη που ασχολείται με την συλλογή, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό». Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε μια συσκευή. Είναι αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις αλλά και να τις συγκεντρώσουμε με τίνι τρόπω 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.

Η Ψηφιακή Εγκληματολογία χωρίζεται σε κατηγορίες ανάλογα με το τεχνολογικό αντικείμενο το οποίο εξετάζεται, περιέχει τα δεδομένα που σχετίζονται με μια υπόθεση και στο οποίο τελικά θα εφαρμοσθούν οι μέθοδοι συλλογής. Οι όροι «Ασφαλής Ανάκτηση και Ανάλυση Ψηφιακών Δεδομένων» και «Συστηματική Διερεύνηση Υπολογιστών», χρησιμοποιούνται ως συνώνυμα

της λέξης «Computer Forensics» και ορίζουν μια σύγχρονη επιστημονική περιοχή, αντικείμενο, της οποίας είναι η έρευνα και ανάλυση των ψηφιακών δεδομένων ενός υπολογιστή με σκοπό την εξαγωγή ακέραιων, αδιάβλητων και νομικά έγκυρων ηλεκτρονικών στοιχείων. Η ανάκτηση και ανάλυση αυτών των στοιχείων γίνονται με βάση αυστηρούς κανόνες και τεχνικές και πραγματοποιούνται με τη βοήθεια ειδικού υλικού και λογισμικού.

Η μεγάλη ανάπτυξη της τεχνολογίας των κινητών «έξυπνων» τηλεφώνων, τα οποία πλέον παρουσιάζουν εφάμιλλες, αν όχι μεγαλύτερες, υπολογιστικές δυνατότητες με τους ηλεκτρονικούς υπολογιστές και η ευρείας κλίμακας είσοδός τους στις ζωές των ανθρώπων παγκοσμίως, καθιστούν σχεδόν απίθανο το γεγονός ότι μία έρευνα ψηφιακών αποδεικτικών στοιχείων, δεν θα περιλαμβάνει έλεγχο ενός κινητού τηλεφώνου ή κινητής συσκευής.

Αντίστοιχα με τον όρο των Computer Forensics, ως «Ψηφιακή Εγκληματολογία Κινητών Τηλεφώνων» (Mobile Forensics), ορίζεται ο κλάδος της Ψηφιακής Εγκληματολογίας, αντικείμενο του οποίου είναι η ανακάλυψη, συλλογή και ανάλυση ψηφιακών αποδεικτικών στοιχείων ή δεδομένων από μια κινητή συσκευή ή συσκευή με δυνατότητες αποθήκευσης και επικοινωνίας ταυτόχρονα όπως ταμπλέτες (tablets) ή Προσωπικοί Ψηφιακοί Οδηγοί (Personal Digital Assistants – PDAs).

5.2 Ψηφιακή Εγκληματολογία σε Κινητές Συσκευές

Η Ψηφιακή Εγκληματολογία σε κινητές συσκευές (mobile forensics) είναι η επιστήμη, που ασχολείται με την ανάκτηση ψηφιακών αποδείξεων ή δεδομένων από μια κινητή συσκευή, υπό συγκεκριμένες τεχνικές και αναλύσεις, χρησιμοποιώντας αποδεκτές μεθόδους. Με τον όρο κινητή συσκευή δεν αναφερόμαστε μόνο σε κινητά τηλέφωνα, αλλά σε όλες εκείνες τις συσκευές, που έχουν εσωτερική μνήμη και δυνατότητες επικοινωνίας, όπως τα PDAs και τα tablets. Η ραγδαία τεχνολογική εξέλιξη των κινητών, καθιστά σχεδόν ακατόρθωτο να δημιουργηθεί ένα ενιαίο εργαλείο ή μια σταθερή ψηφιακή πλατφόρμα για την έρευνα εγκληματικών πράξεων στις οποίες εμπλέκονται κινητές συσκευές.

Τα κινητά τηλέφωνα, σε αντίθεση με τους υπολογιστές, χρησιμοποιούν μνήμη flash για να καταχωρούν δεδομένα και οδήγησαν έτσι στην δημιουργία ενός νέου κλάδου έρευνας, γιατί οι τεχνικές προκλήσεις δεν ικανοποιούνταν με την υπάρχουσα μεθοδολογία. Οι κινητές συσκευές αποθηκεύουν πολλών ειδών προσωπικά στοιχεία, πολλά από τα οποία είναι εν αγνοία του χρήστη, όπως επαφές, φωτογραφίες, βίντεο, SMS, MMS πληροφορίες θέσης και μηνύματα κοινωνικής δικτύωσης. Με δεδομένο ότι σε μία flash μνήμη η δυνατότητα εγγραφής δεδομένων είναι πεπερασμένη, τα δεδομένα μπορούν να διαγραφούν, όταν ένα block είναι γεμάτο. Αυτό αποτελεί σημαντικό πλεονέκτημα, γιατί οι κινητές συσκευές αποτελούν εξαιρετική πηγή ψηφιακών στοιχείων και παρέχουν πληροφορίες που δεν είναι διαθέσιμες σε άλλες συσκευές.

5.3 Ψηφιακά πειστήρια σε κινητά τηλέφωνα

Μεγάλος όγκο πληροφοριών και δεδομένα επικοινωνίας πού είναι αποθηκευμένα σε κινητές συσκευές, μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία. Η αναζήτηση των αποδείξεων στα δεδομένα του κινητού μπορούν να αποκτηθούν κανονικά από την εσωτερική μνήμη, από τη μνήμη της κάρτας SIM, σε αφαιρούμενες κάρτες μνήμης, από τις εξωτερικές κάρτες μνήμης και τους παρόχους υπηρεσιών τηλεπικοινωνιών και διαδικτύου.

Βασικά στοιχεία και πληροφορίες που συνήθως αναζητούνται στη συσκευή κινητού τηλεφώνου και τα οποία μπορούν να αποτελέσουν κατάλληλα αποδεικτικά πειστήρια, είναι τα παρακάτω:

- Τηλεφωνικός κατάλογος με τις επαφές
- Τελευταίες εισερχόμενες/ εξερχόμενες/ αναπάντητες κλήσεις
- Εισερχόμενα και εξερχόμενα γραπτά μηνύματα (SMS) και MMS
- Ηχογραφήσεις/ Φωνητικές σημειώσεις/ Ήχοι κλήσης
- Φωτογραφίες, Video, Γραφικά, Αρχεία ήχου, Επιφάνεια εργασίας
- Ημερολόγιο, Ξυπνητήρια/ Υπενθυμίσεις, Κατάλογος εκκρεμοτήτων
- Γραπτές σημειώσεις
- Ηλεκτρονικό ταχυδρομείο

- Επίσκεψη σε Ιστοσελίδες από το κινητό (ιστορικό περιήγησης)
- Έγγραφα και αρχεία κάθε τύπου
- Αναγνωριστικά χρήστη (π.χ. PIN)
- Αναγνωριστικά συσκευής (π.χ. IMEI)
- Κατάλογος δικτύων
- Γεωγραφικά Δεδομένα

Εικόνα 18. Ψηφιακά Πειστήρια στα Κινητά Τηλέφωνα

Μια σημαντική πληροφορία, που πρέπει να έχει κατά νου ένας ερευνητής, κατά τη διάρκεια αναζήτησης, είναι το γεγονός ότι τα κινητά τηλέφωνα αποτελούν κατά κύριο λόγο πιο περίπλοκα συστήματα, δίνοντας πολύ λιγότερη ενημέρωση, σχετικά με το τι ακριβώς αποθηκεύεται και πού. Ως αποτέλεσμα των παραπάνω είναι η παραμονή στη μνήμη δεδομένων και πληροφοριών τις οποίες ο χρήστης μπορεί να αγνοεί και να μην έχει τα δικαιώματα εκείνα, ώστε να τις διαγράψει. Τονίζεται ότι η διαδικασία της διαγραφής δεν απαλείφει τα δεδομένα από το χώρο της μνήμης, η οποία όπως είδαμε, αν δεν υπερκαλυφθεί με νεότερα, τότε οι πληροφορίες συνεχίζουν να διατηρούνται κανονικά, έστω και αν κάποιος έχει την εντύπωση ότι τα έχει διαγράψει.

Εκτός από την συσκευή του κινητού τηλεφώνου μεγάλος όγκος πληροφοριών είναι αποθηκευμένος και στην κάρτα SIM (Subscriber Identify Module). Η κάρτα SIM είναι μία έξυπνη κάρτα, η οποία πιστοποιεί την ταυτότητα

του χρήστη και παρέχει τη βασική λειτουργικότητα του κινητού. Η δομή της κάρτας SIM οργανώνεται σε καταλόγους και αρχεία, όπου μέσα στους καταλόγους βρίσκονται αρχεία-θέσεις μνήμης, και φυλάσσονται διάφορες πληροφορίες. Σε κάθε ένα από αυτά τα αρχεία υπάρχουν διαφορετικά δικαιώματα πρόσβασης (ανάγνωση, εγγραφή, τροποποίηση ή διαγραφή κ.α.), δηλαδή ορισμένα μπορούν να αναγνωσθούν χωρίς καν να έχει πληκτρολογηθεί το PIN, άλλα απαιτούν την πιστοποίηση του PIN, ενώ στα πιο σημαντικά έχει πρόσβαση μόνον ο πάροχος, μέσω του κατάλληλου κωδικού ADM.

Σύμφωνα με το πρότυπο στην κάρτα SIM, υπάρχουν περίπου 100 αρχεία και κάποια επιπρόσθετα που διατηρεί ο κάθε πάροχος.

Ενδεικτικά κάποια αρχεία βάση του προτύπου περιέχουν:

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

Πολλά από τα αρχεία αυτά, μπορούν να αξιοποιηθούν ως πειστήρια, καθόσον ο κάτοχος δεν έχει άμεση πρόσβαση σε αυτά και συνεπώς δεν γνωρίζει την ύπαρξη τους προκειμένου να τα τροποποιήσει. Σε περίπτωση όμως που η εγκυρότητά τους αμφισβητηθεί, τότε μπορεί να επαληθευτεί βάση των αρχείων, που διατηρεί ο πάροχος [26].

• **Αρχείο ICCID** (Integrated Circuit Card Identifier): είναι ένα μοναδικός σειριακός αριθμός ο οποίος είναι τυπωμένος στο πλαστικό περίβλημα της

κάρτας αλλά και προγραμματισμένος στο αντίστοιχο αρχείο της κάρτας SIM και δηλώνει διεθνώς σε ποια χώρα ανήκει η συγκεκριμένη κάρτα.

• **Αρχείο IMSI** (International Mobile Subscriber Identify): είναι ένας μοναδικός παγκοσμίως 15ψήφιος αριθμός που χρησιμοποιείται για την αναγνώριση του συνδρομητή από το σύστημα και αποτελεί το μυστικό κλειδί για την πιστοποίηση. Μέσω του αριθμού IMSI μπορεί να ταυτοποιηθεί ο αριθμός τηλεφώνου, ακόμα και αν η κάρτα έχει λήξει και δεν είναι πλέον δυνατή η χρήση της στο δίκτυο.

• **Αρχείο Location Information και αρχείο Broadcast Control Channel:** Στο αρχείο πληροφοριών περιοχής (Location Information) βρίσκεται η προσωρινή ταυτότητα του κινητού, που πρόκειται για αριθμό παρόμοιο με τον IMSI και χρησιμοποιείται για λόγους ασφάλειας προκειμένου να μην εκπέμπεται στο δίκτυο η μόνιμη ταυτότητα του χρήστη και ο αριθμός περιοχής που αντιστοιχεί στη χώρα, στο δίκτυο και σε μία ευρύτερη περιοχή, η οποία περιλαμβάνει δεκάδες ή ακόμα και εκατοντάδες κυψέλες. Στο αρχείο πληροφοριών καναλιών ελέγχου εκπομπής αποθηκεύεται η ταυτότητα του τρέχοντος καναλιού ελέγχου επικοινωνίας αλλά και των έξι γειτονικών καναλιών. Από το συνδυασμό των στοιχείων LAI και BCCH μπορεί να εξαχθεί η τελευταία περιοχή στην οποία λειτουργούσε το κινητό. Τα δεδομένα αυτά παραμένουν στη SIM και μετά την απενεργοποίηση της συσκευής και ανανεώνονται καθώς αυτή αλλάζει περιοχές. Συνεπώς εκτός από τη χώρα προέλευσης της κάρτας είναι δυνατή και η εύρεση της τοποθεσίας στην οποία χρησιμοποιήθηκε τελευταία φορά η κάρτα.

• **Αρχείο αποθήκευσης SMS**: Οι σύγχρονες SIM διαθέτουν αρκετές θέσεις αποθήκευσης μηνυμάτων. Συνεπώς σε περίπτωση που ο κατασκευαστής του κινητού δεν έχει προεπιλέξει τη μνήμη του κινητού ως πρωτεύουσα μνήμη αποθήκευσης, μπορεί να βρεθούν τα γραπτά μηνύματα. Σαφώς όμως όταν συμπληρωθεί όλος ο διαθέσιμος χώρος αποθηκεύονται και στη μνήμη του κινητού. Όπως προαναφέρθηκε η απλή διαγραφή ενός SMS δεν οδηγεί σε άμεση διαγραφή του αλλά σε σήμανση της συγκεκριμένης περιοχής μνήμης ως ελεύθερης για περαιτέρω αποθήκευση.

• **Αρχείο ADN** (Abbreviated Dialing Numbers). Οι σύγχρονες SIM διαθέτουν 250 θέσεις για το αρχείο όπου φυλάσσεται ο κατάλογος επαφών. Στην περίπτωση του καταλόγου επαφών κατά τη διαγραφή μιας επαφής ισχύει το γέμισμα της περιοχής με δυαδικά '1', συνεπώς η ανάκτηση είναι και εδώ ανέφικτη. Το μόνο συμπέρασμα που μπορεί ένας πραγματογνώμονας να εξάγει είναι να επιβεβαιώσει την διαδικασία της διαγραφής, καθόσον οι θέσεις μνήμης στο αρχείο αυτό καταλαμβάνονται με τη σειρά και σε περίπτωση διαγραφής η θέση παραμένει κενή.

Γενικότερα οι δυνατότητες εξαγωγής ψηφιακών δεδομένων συνεχώς εξελίσσονται και επεκτείνονται, ενώ υπάρχουν χιλιάδες διαφορετικά μοντέλα, σχετική έλλειψη προτύπων και εξαιρετική πολυπλοκότητα στα δίκτυα των παρόχων. Συνεπώς ο πραγματογνώμονας που ασχολείται με την εξέταση ενός κινητού τηλεφώνου πρέπει να είναι ενημερωμένος για τις τεχνολογικές εξελίξεις σε αυτόν τον τομέα και να ακολουθεί τις εδραιωμένες διαδικασίες εγκληματολογικής και ανάλυσης κινητών τηλεφώνων.

5.4 Διαδικασία Έρευνας

Η ηλεκτρονική έρευνα ενός εγκλήματος διαφέρει σημαντικά από την «παραδοσιακή έρευνα» που αναζητά απτά στοιχεία. Ο ερευνητής δεν αναζητά σε κάποιο συρτάρι τα αποδεικτικά στοιχεία, αλλά σε ηλεκτρονικούς φακέλους, αρχεία, αποθηκευτικά μέσα, υπολογιστικά συστήματα κ.α.

Τα ψηφιακά αποδεικτικά στοιχεία που συλλέγονται θεωρούνται ιδιαιτέρως ευαίσθητα, γι' αυτό σημαντικό κομμάτι της ηλεκτρονικής έρευνας αποτελεί η διατήρησή τους και η διαφύλαξη της μη αλλοίωσής τους. Η έρευνα ψηφιακών πειστηρίων, πρέπει να διεξάγεται σύμφωνα με την ισχύουσα κατά περίπτωση νομοθεσία, καθώς πολλές αμφιβολίες δημιουργούνται για την επάρκεια των γνώσεων ενός ερευνητή και για το αν η ανάλυση και διατήρηση των στοιχείων ακολουθεί τις προβλεπόμενες διαδικασίες. Κατά συνέπεια, πολλές φορές παρατηρείται το φαινόμενο σε μία δίκη να αμφισβητείται είτε η έρευνα, είτε να κατάσχονται οι πληροφορίες, επειδή δεν υφίσταται ειδικό νομοθετικό πλαίσιο στην περίπτωση των ερευνών στον κυβερνοχώρο.

Κατά τη διεξαγωγή μιας έρευνας, είναι σημαντικό να μην παραβιάζεται η ιδιωτικότητα του ατόμου. Κατόπιν τούτου, απαιτείται συνήθως ένταλμα που θα πρέπει να καθορίζει με ακρίβεια τα αντικείμενα που μπορούν να ερευνηθούν. Ακόμα και αν ο ερευνητής θεωρεί ότι μπορεί να αντλήσει στοιχεία και από άλλα εκτός των παραπάνω αντικείμενων, τα στοιχεία αυτά δεν θα έχουν αποδεικτική αξία στη δικαστική αίθουσα.

Οι αναλυτές ψηφιακών πειστηρίων χρησιμοποιούν διάφορες τεχνικές για να εξάγουν τα δεδομένα από μία συσκευή, όπως είναι η φυσική (physical) και η λογική (logical) ανάλυση. Η ψηφιακή εγκληματολογία χρησιμοποιεί τις ίδιες μεθόδους με την βασική εγκληματολογική έρευνα. Υπάρχουν ορισμένες καλές πρακτικές που πρέπει να ακολουθηθούν. Από τη στιγμή όμως που δεν υπάρχει προκαθορισμένη μεθοδολογία αποκλειστικά για κινητά τηλέφωνα, χρησιμοποιούνται οι πρακτικές των ψηφιακών πειστηρίων γενικά. Η διαδικασία της ερευνητικής διαδικασίας που συνήθως ακολουθείται είναι [26] :

- ***Συλλογή:*** Αυτό είναι το πρώτο βήμα που πραγματοποιείται σε μία έρευνα. Ο κύριος σκοπός εδώ είναι να συλλεχθούν όλες οι πιθανές πηγές στοιχείων όπως, η συσκευή του κινητού, η κάρτα SIM και άλλες περιφερειακές συσκευές που υπάρχουν στο σημείο.

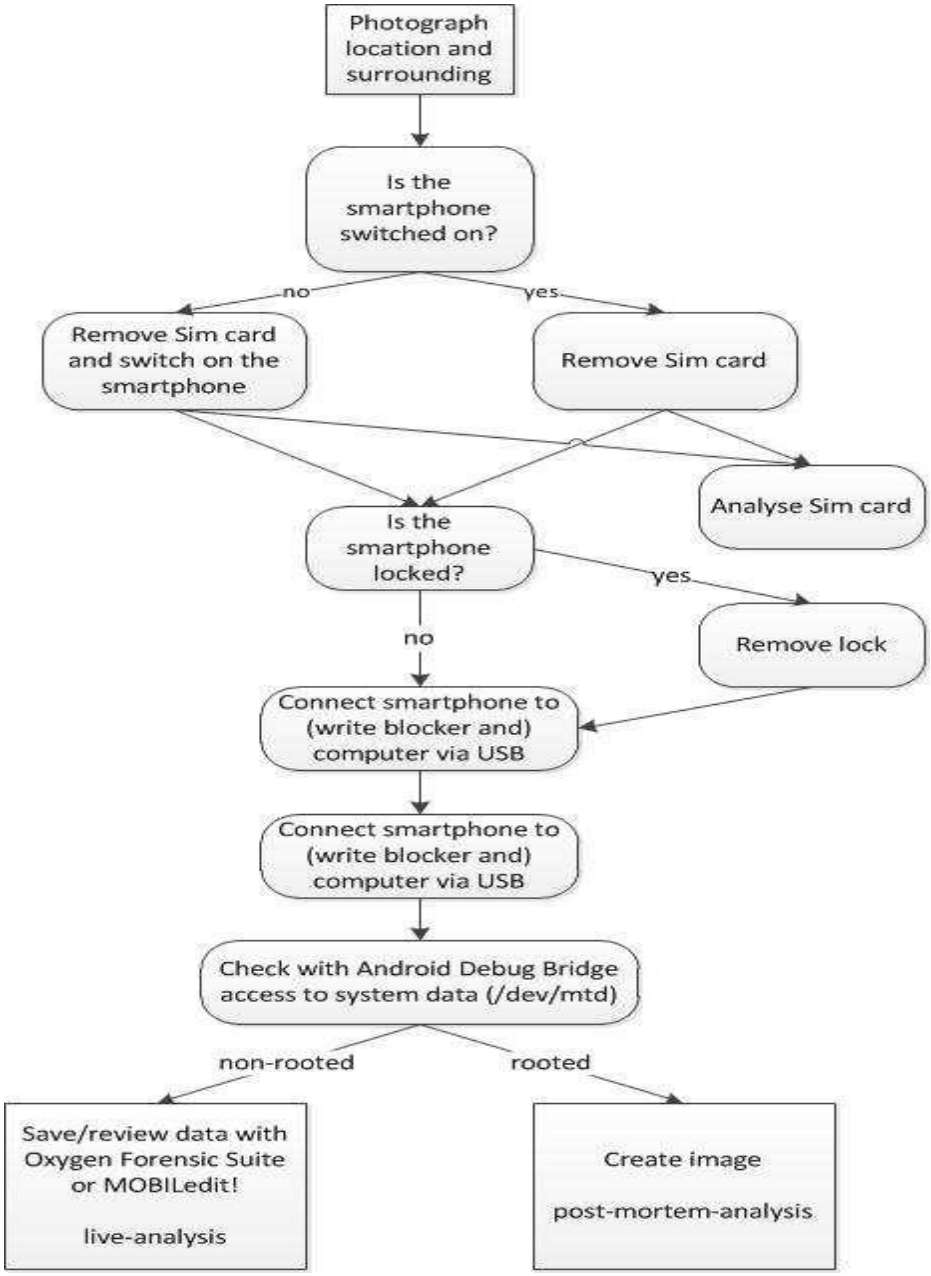
- ***Εξακρίβωση:*** Επικεντρώνεται κυρίως στην αναγνώριση με επισημάνσεις των πιθανών πηγών ψηφιακών στοιχείων.

- ***Απόκτηση στοιχείων:*** Αναφέρεται στην εξαγωγή των δεδομένων ή των πιθανών στοιχείων από διάφορες πηγές που έχουν συλλεχθεί.

- ***Διατήρηση:*** Ένα από τα βασικότερα βήματα που πραγματοποιείται στην έρευνα είναι η διατήρηση των στοιχείων, όπου με αυστηρά μέτρα πρέπει να διαφυλαχθεί η ακεραιότητα των στοιχείων.

- ***Εξέταση και ανάλυση:*** Περιλαμβάνει την αναζήτηση, το φιλτράρισμα, την εξέταση και την εκτίμηση των στοιχείων.

- ***Αναφορά:*** Όπως σε κάθε ψηφιακή έρευνα, η αναφορά είναι το τελικό βήμα που τεκμηριώνονται εγγράφως τα αδιαμφισβήτητα στοιχεία.



Εικόνα 19. Βασικές αρχές εξέτασης κινητού Android

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

- Καμία ενέργεια δε δύναται να μεταβάλει δεδομένα που τηρούνται στη συσκευή ή μέσο αποθήκευσης, τα οποία μπορεί να προσκομισθούν στο δικαστήριο.
- Χρήση αρχέτυπων δεδομένων από τρίτο άτομο, κατόπιν εξουσιοδότησης.
- 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.

Συνοψίζοντας τα παραπάνω [27]:

1) **Συλλογή**: Περιλαμβάνει τις διαδικασίες και τις μεθόδους καταγραφής της φυσικής σκηνής του εγκλήματος καθώς και της απόλυτα πιστής αντιγραφής της πρωτότυπης ψηφιακής απόδειξης χρησιμοποιώντας τυποποιημένες και αποδεκτές πρακτικές.

2) **Διατήρηση**: Περιλαμβάνει ενέργειες απομόνωσης, προστασίας και συντήρησης της κατάστασης της φυσικής και της ψηφιακής απόδειξης, 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.

3) **Ανάλυση**: Σε αυτή τη φάση προσδιορίζεται η σημαντικότητα των συλλεγμένων δεδομένων και βγαίνουν συμπεράσματα που βασίζονται στις αποδείξεις που βρέθηκαν.

4) **Παρουσίαση**: 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 και θα τεκμηριώνει όλα τα συμπεράσματα στα οποία έχει καταλήξει.

5.5 Ψηφιακές Αποδείξεις και Δεδομένα

Οι ψηφιακές αποδείξεις αποτελούν το πιο σπουδαίο αποδεικτικό μέσο, κατά την εξέταση μιας υπόθεσης ηλεκτρονικού εγκλήματος και γενικά κατά την εξέταση οποιουδήποτε στοιχείου έχει ψηφιακή μορφή [28]. Ο SWGDE (Scientific Working Group on Digital Evidence), μια κοινοπραξία διεθνών οργανισμών, που δραστηριοποιείται στον τομέα των ψηφιακών αποδείξεων, τον Οκτώβριο του 1999 προτυποποίησε τις αποδείξεις που έχουν ψηφιακή μορφή, διαχωρίζοντάς τις σε:

Ψηφιακές αποδείξεις (digital evidence): Πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή.

Αντικείμενα δεδομένων (data objects): Αντικείμενα ή πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα.

Φυσικά αντικείμενα (physical items): Τα φυσικά μέσα όπου αποθηκεύονται ή μέσω των οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.

Γνήσιες ψηφιακές αποδείξεις (original digital evidence): Φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.

Διπλότυπες ψηφιακές αποδείξεις (duplicate digital evidence): Ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.

Αντίγραφο (copy): Μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό αντικείμενο, ανεξάρτητα από το αντικείμενο αυτό.

Οι ψηφιακές αποδείξεις μπορεί να είναι αποθηκευμένες σε οποιαδήποτε συσκευή, όπως ηλεκτρονικό υπολογιστή, palmtop, κινητό τηλέφωνο κ.α., καθώς και σε οποιοδήποτε μέσο αποθήκευσης, όπως δισκέτες, CDs, DVDs, κάρτες μνήμης κ.α.

Βασικό χαρακτηριστικό των ψηφιακών αποδείξεων είναι ο μεγάλος βαθμός μεταβλητότητάς τους. Μπορούν πολύ εύκολα να τροποποιηθούν ή να καταστραφούν με τη χρήση διαφόρων εργαλείων και μεθόδων. Ο ερευνητής, λοιπόν, πρέπει να αναζητεί και να μεταχειρίζεται τις πληροφορίες αυτές με ιδιαίτερη δεξιότητα.

Οι ψηφιακές αποδείξεις αποτελούνται από ψηφιακά δεδομένα (digital data). Μια πολύ σημαντική διάκριση των ψηφιακών δεδομένων είναι σε μεταβλητά δεδομένα (volatile data) και σε διαρκή δεδομένα (persistent data). Τα

μεταβλητά, είναι δεδομένα που αποθηκεύονται στην μνήμη του συστήματος (π.χ. μητρώο συστήματος, cache, μνήμη RAM) και χάνονται αν γίνει τερματισμός της λειτουργίας του ή επανεκκίνηση της συσκευής. Τα διαρκή δεδομένα είναι αποθηκευμένα στους δίσκους του συστήματος ή σε άλλες συσκευές μόνιμης αποθήκευσης, όπως οδηγοί USB και κάρτες μνήμης. Τα δεδομένα αυτά δεν χάνονται, όταν τερματιστεί η λειτουργία της συσκευής ή γίνει επανεκκίνηση.

Κεφάλαιο 6ο
Εξαγωγή αποδεικτικών στοιχείων από έξυπνα κινητά τηλέφωνα

6.1 Μεθοδολογία ανάκτησης και εξαγωγής δεδομένων

Στην παρούσα εργασία, θα εξετάσουμε τις δυνατότητες που υποστηρίζουν τα ελεύθερα διαθέσιμα εργαλεία της ψηφιακής εγκληματολογίας για εύρεση ψηφιακών πειστηρίων. Πιο συγκεκριμένα θα αναζητηθούν αποδείξεις, που έχουν να κάνουν με τη χρήση των εφαρμογών του ψηφιακού πορτοφολιού και θα περιέχουν οικονομικά, προσωπικά και στοιχεία προσδιορισμού γεωγραφικής θέσης. Τα στοιχεία αυτά θα μπορούν να χρησιμοποιηθούν, ως αποδεικτικά στοιχεία αποδοχής ή αποποίησης πράξεων για τον κάτοχο του κινητού.

Σε μία εγκληματολογική εξέταση ενός Android κινητού, είναι πολύ σημαντικό να τηρούνται αυστηρά από τον ερευνητή οι κανόνες και οι διαδικασίες που πραγματοποιούνται για τον εντοπισμό σημαντικών στοιχείων. Στην περίπτωση των Android κινητών υπάρχουν τέσσερις τρόποι ώστε να ανιχνευθούν και να διασφαλιστούν τα δεδομένα. Αυτοί οι τρόποι είναι οι εξής [29]:

- **Ανάλυση εξωτερικής κάρτας SD (SD card analysis)**

Η ανάλυση της εξωτερικής κάρτας SD είναι η πιο απλή μέθοδος ανάλυσης δεδομένων, που μπορούν να εξαχθούν από ένα κινητό. Σχεδόν κάθε κινητό Android υποστηρίζει εξωτερική κάρτα μνήμης. Για την ανάλυση της κάρτας SD απαιτείται η δημιουργία ενός αντιγράφου, χρησιμοποιώντας έναν write blocker, ώστε να εξαχθούν με ασφάλεια τα δεδομένα που υπάρχουν μέσα σ' αυτή, είτε τοποθετείται απευθείας σε θύρα του υπολογιστή (στην περίπτωση αυτή χρησιμοποιούμε software write blocker). Η SD κάρτα έχει διαμόρφωση FAT32, που την καθιστά ευάλωτη, όσον αφορά την ακεραιότητα των δεδομένων, ωστόσο δεν είναι το μέσο που θα αποθηκευθούν σημαντικά ή ευαίσθητα δεδομένα. Επιπλέον, όσον αφορά τις εφαρμογές e-Wallet δεν υπάρχει η επιλογή για μεταφορά των εφαρμογών

αυτών στην κάρτα, κάτι που σημαίνει ότι μειώνεται δραστικά το εύρος των εργαλείων που μπορεί να χρησιμοποιηθούν. Η εξωτερική μνήμη χρησιμοποιείται συνήθως για να αποθηκεύει δεδομένα πολυμέσων (εικόνες, ήχοι, video), ενώ μπορεί να περιλαμβάνει και backup του κινητού.

• **Λογική ανάλυση (logical analysis)**

Η λογική ανάλυση ενός κινητού Android πραγματοποιείται κυρίως με την βοήθεια εφαρμογών, που εγκαθίστανται στο υπό εξέταση κινητό και συλλέγουν αυτόματα τα δεδομένα. Στη συνέχεια αφού συλλέξουν με επιτυχία τα δεδομένα, οι εφαρμογές τερματίζονται και διαγράφονται. Σύμφωνα με τις βασικές αρχές των ψηφιακών πειστηρίων, το κινητό δεν θα πρέπει να τροποποιηθεί ή να γίνουν αλλαγές από τη στιγμή που συλλεχθεί για ανάλυση, ωστόσο οι εφαρμογές που χρησιμοποιούνται είναι σχεδιασμένες για αυτόν τον σκοπό, και οι αλλαγές που γίνονται είναι ελάχιστες. Αυτές οι εφαρμογές συνήθως συλλέγουν πληροφορίες από τα κινητά μέσω σύνδεσης καλωδίου, όπου τέτοιες πληροφορίες είναι:

- Βασικά στοιχεία της συσκευής
- Κατάλογος επαφών με φωτογραφίες αυτών και τυχόν ομάδες χρηστών
- Ημερολόγιο και σημειώσεις
- Λίστα κλήσεων
- Μηνύματα sms
- Πολυμέσα (εικόνες, ήχοι, video)
- Λίστα από εγκατεστημένες εφαρμογές
- Πρωτόκολλα τηλεφώνου

Τα αποτελέσματα αυτής της ανάλυσης δίνουν μια πρώτη εικόνα της χρήσης που έγινε στο κινητό, όμως τα δεδομένα, που αποθηκεύονται από εξωτερικές εφαρμογές, όπως e-Wallet, facebook, twitter, viber, δεν μπορούν να διαβαστούν. Για να αποκτήσουμε πρόσβαση σε αυτά τα δεδομένα απαιτείται μία λεπτομερής τεχνική ανάλυση.

• **Τεχνική ανάλυση (technical analysis)**

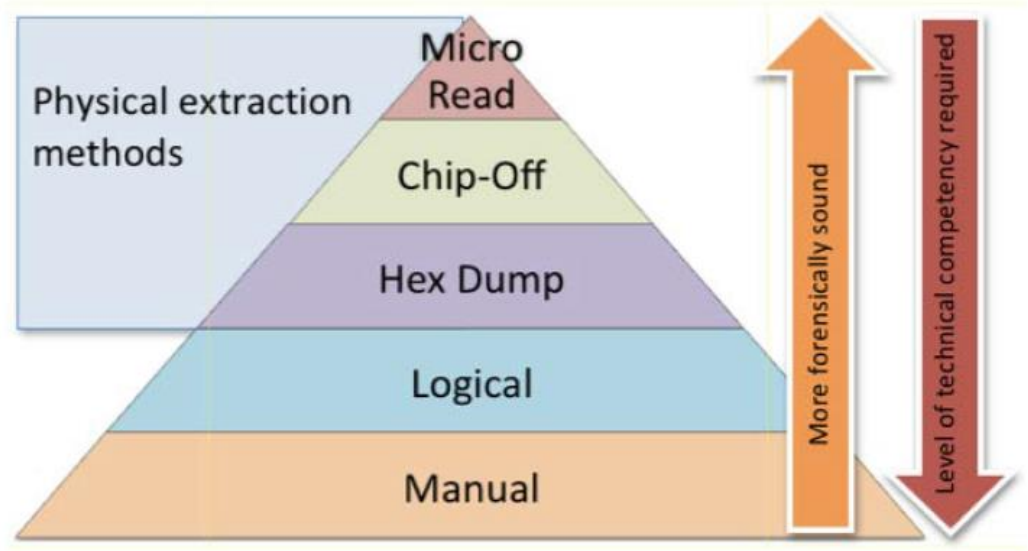
Για πιο λεπτομερή εξέταση των κινητών Android η τεχνική ανάλυση είναι απαραίτητη. Σε αυτό το επίπεδο εξέτασης δημιουργείται ένα είδωλο της εσωτερικής μνήμης flash του κινητού [30]. Η δημιουργία όμως dd-ειδώλων της μνήμης απαιτεί δικαιώματα διαχειριστή, τα οποία εξαρχής ο κάτοχος του κινητού δεν έχει. Πρόκειται για μια εξειδικευμένη διαδικασία που απαιτεί λεπτομερή χειρισμό, καθώς το κινητό πρέπει να τροποποιηθεί μέσω ειδικών μεθόδων. Ο ερευνητής αποκτά πρόσβαση σε όλο το περιεχόμενο του κινητού χωρίς όμως να αλλοιωθούν σημαντικά δεδομένα, αφού τροποποιούνται μόνο οι φάκελοι του συστήματος.

Τα κινητά Android, όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, χρησιμοποιούν αρχεία συστήματος YAFFS2, τα οποία έχουν σχεδιαστεί για μνήμη flash NAND. Τα αρχεία YAFFS2, είναι αρχεία συστήματος βασισμένα σε πρωτόκολλα για χρήση σε κινητά τηλέφωνα, διακρίνονται για την χαμηλή κατανάλωση μνήμης, υψηλές ταχύτητες και καλή διόρθωση σφαλμάτων. Λόγω της περιορισμένης χρήσης αυτών των αρχείων συστημάτων μόνο σε κινητά Android, δεν μπορούν να υποστηριχθούν από τα υπάρχοντα εργαλεία ψηφιακών πειστηρίων. [31]

• **Ανάλυση κυκλώματος του κινητού (chip analysis)**

Η ανάλυση του κυκλώματος του κινητού είναι απαραίτητη στα κινητά με εγκατεστημένες μνήμες flash NAND, όμως είναι δύσκολο να πραγματοποιηθεί, αφού οι επεξεργαστές του κινητού πρέπει να αφαιρεθούν τελείως από το κινητό και να πάνε για περαιτέρω ανάλυση σε εξειδικευμένα εργαστήρια. Τα αποτελέσματα αυτής της ανάλυσης πρέπει να είναι σε συμφωνία των αποτελεσμάτων της τεχνικής ανάλυσης.

Η Brothers (2009) [32], περιγράφει πέντε επίπεδα εξαγωγής από τις συσκευές τηλεφώνου, όπως απεικονίζονται στην Εικόνα 20. Το τελευταίο επίπεδο (Χειρωνακτική Απόκτηση), θεωρείται ότι απαιτεί το μικρότερο ποσό τεχνικής πραγματογνωμοσύνης αλλά, την ίδια στιγμή, είναι η λιγότερη ορθή από εγκληματολογικής άποψης, προσέγγιση, ενώ το πρώτο επίπεδο (Micro Read) είναι το πιο πολύπλοκο και απαιτεί τη μέγιστη τεχνική γνώση για να εκτελεστεί.



Εικόνα 20. Επίπεδα ανάλυσης ψηφιακών πειστηρίων

6.2 Διαδικασίες - Φάσεις εγκληματολογικής έρευνας κινητών τηλεφώνων

6.2.1 Φάση διατήρησης (preservation)

Κατά τη διάρκεια της εγκληματολογικής εξέτασης, όταν το έξυπνο κινητό τηλέφωνο (smartphone) είναι ενεργοποιημένο, είναι πολύ σημαντικό να απομονωθεί, επειδή χαρακτηριστικά απομακρυσμένης διαγραφής δεδομένων υποστηρίζονται σε πολλά smartphones σήμερα. Λογισμικά απομακρυσμένης διαγραφής, όπως το «Mobileme», μπορούν να επιτρέψουν σε έναν χρήστη να διαγράψει όλα τα δεδομένα του απομακρυσμένα μέσω μιας σύνδεσης δικτύου.

Στον οδηγό του NIST υπάρχουν μόνο δύο τρόποι για να απομονωθούν τα ραδιοσήματα, εκ των οποίων ο ένας ήταν να απενεργοποιηθεί το τηλέφωνο. Απενεργοποιώντας το τηλέφωνο θα μπορούσε να θέσει όμως τον κίνδυνο να ζητηθούν οι κωδικοί πρόσβασης για την ενεργοποίηση του κινητού τηλεφώνου. Αυτό επίσης θα μπορούσε να έχει ως αποτέλεσμα την πολυπλοκότητα της απόκτησης και την καθυστέρηση της εξέτασης εξαιτίας των δυσκολιών απόκτησης εισόδου στην συσκευή.

Ο δεύτερος τρόπος είναι να κρατηθεί το κινητό ενεργοποιημένο και να σφραγιστεί σε ένα δοχείο απομόνωσης ακτινοβολίας. Αυτό όμως επίσης θέτει ένα πρόβλημα. Η διάρκεια ζωής της μπαταρίας θα ελαττωνόταν εξαιτίας της αύξησης της ενεργειακής κατανάλωσης του τηλεφώνου διαμέσου της αύξησης

της ισχύος του σήματος του, στην προσπάθεια του να συνδεθεί ανεπιτυχώς σε ένα δίκτυο. Αυτή η αποτυχία σύνδεσης στο δίκτυο μπορεί να προκαλέσει σε ορισμένα τηλέφωνα επαναφορά, ή διαγραφή των δεδομένων δικτύου. Επίσης υπάρχει ο κίνδυνος μη σωστού σφραγίσματος στο δοχείο απομόνωσης ακτινοβολίας και η εν αγνοία σύνδεση του τηλεφώνου σε κινητό δίκτυο.

Η φάση της διατήρησης των πειστηρίων που βρίσκονται στον τόπο του εγκλήματος, εκτελείται στην κύρια περίοδο της εγκληματολογικής έρευνας και περιλαμβάνει την απομόνωση της σκηνής του εγκλήματος και την τεκμηρίωση των ευρεθέντων στοιχείων. Επίσης, προβλέπει, τη συλλογή των κινητών τηλεφώνων, που βρέθηκαν σε αυτή και την αποστολή τους σε εξειδικευμένο εργαστήριο με ορθές διαδικασίες και την αποφυγή οποιασδήποτε τροποποίησης ή αλλοίωσης των κατασχεθέντων τηλεφώνων [33].

6.2.2 Φάση ανάκτησης (acquisition)

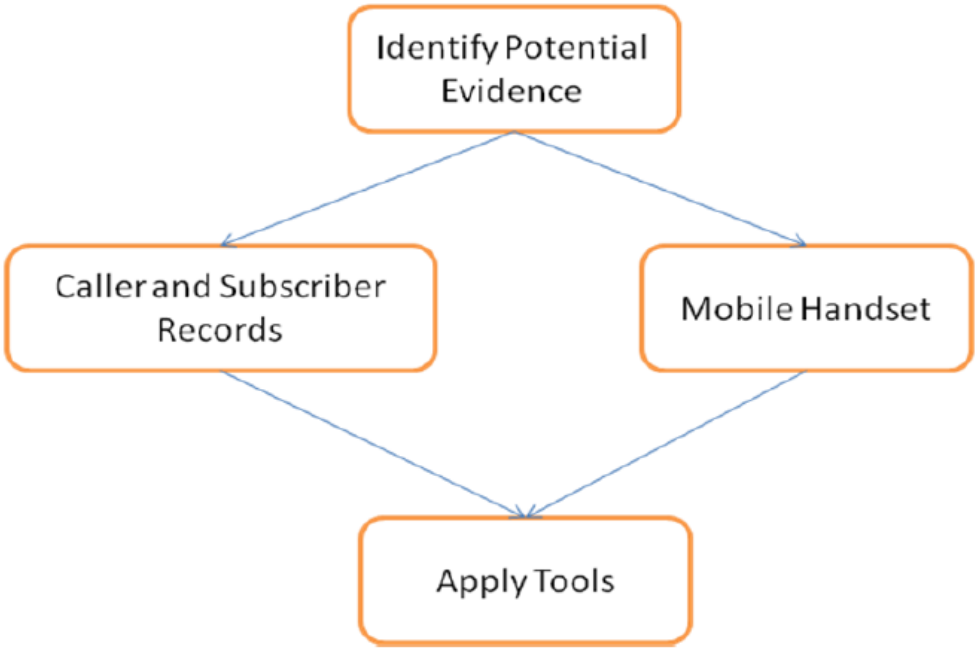
Στη φάση της ανάκτησης, γίνεται η αναγνώριση της τηλεφωνικής συσκευής, η επιλογή των κατάλληλων εργαλείων και η εφαρμογή τους στη συσκευή. Έτσι, ανακτώνται δεδομένα σχετικά με ανταλλαγή μηνυμάτων, επιχειρησιακά δεδομένα, αρχεία καταγραφής κ.α.

Οι ενέργειες που θα γίνουν σε αυτή την φάση δεν πρέπει να τροποποιήσουν τα δεδομένα που περιέχονται στη συσκευή από την οποία θα γίνει η ανάκτηση.

6.2.3 Φάση εξέτασης και ανάλυσης (examination and analysis)

Στη συνέχεια, έπεται η φάση της εξέτασης και ανάλυσης όπου τα πειστήρια εξετάζονται και ερμηνεύονται στο κατάλληλο πλαίσιο από το εγκληματολόγο - δικανικό αναλυτή, για την εξαγωγή συμπερασμάτων.

Οι οδηγοί του NIST, διακρίνουν μόνο δύο σημαντικούς τομείς στη φάση της εξέτασης. Ο ένας είναι ο εντοπισμός της απόδειξης και ο άλλος το εργαλείο εφαρμογής [34]. Ο αναλυτής καλείται να προσδιορίσει τι θα μπορούσε να αποτελεί πιθανή απόδειξη σε σχέση με την υπόθεση και έπειτα μπορούν να επιλεγούν τα εργαλεία που ανταποκρίνονται και εφαρμόζονται για την ανάλυση της (όπως παρακάτω σχήμα).



Εικόνα 21. Διάγραμμα ροής διαδικασιών στην φάση της εξέτασης

Στην τελευταία έκδοση του οδηγού του NIST, τα αρχεία κλήσεων και εγγραφών, προστέθηκαν ως ένας άλλος σημαντικός τομέας στην φάση της εξέτασης. Η τεχνολογία κινητού υπολογιστικού νέφους (Mobile Cloud Computing), η οποία εφαρμόστηκε ευρέως στα κινητά τηλέφωνα, πιθανώς έχει τεράστια ποσά απόδειξης αποθηκευμένα είτε στην εφαρμογή Cloud είτε στο χώρο αποθήκευσης του Cloud. Το πώς να εξεταστεί η πιθανή πληροφορία η οποία βρίσκεται στο υπολογιστικό νέφος (Cloud) είναι μία από τις μεγαλύτερες ανησυχίες αυτή τη στιγμή, καθώς είναι ασαφές τι τύποι δεδομένων μπορούν να ανακτηθούν από το Cloud.

6.2.4 Φάση αναφοράς των αποτελεσμάτων της έρευνας (reporting)

Η διαδικασία καταλήγει, μετά την έρευνα, στο τελικό στάδιο το οποίο σχετίζεται με τη σύνταξη αναλυτικής αναφοράς για τα πειστήρια και την παρουσίασή τους ενώπιων του δικαστηρίου από τον ενάγοντα.

Η αναφορά είναι η διαδικασία προσεκτικής διατήρησης των αρχείων όλων των ενεργειών και παρατηρήσεων από τα βήματα που έγιναν και τα συμπεράσματα που εξήχθησαν από την έρευνα. Οι αναφορές περιγράφουν τα αποτελέσματα των εξετάσεων και εξηγούν τα συμπεράσματα που προέκυψαν από τις αποδείξεις. Η κατάλληλη τεκμηρίωση καθιστά ικανά τα

άτομα να ανακατασκευάσουν και να εξετάσουν την όλη διαδικασία εξέτασης από την αρχή μέχρι το τέλος.

Επισημαίνεται ότι μη ολοκληρωμένες αναφορές ή ανακόλουθες μαρτυρίες μπορούν να ακυρώσουν ακόμα και τις καλύτερες έρευνες.

Γενικότερα, η τελική αναφορά θα περιέχει τις ακόλουθες πληροφορίες:

- Περιεχόμενα που παράχθηκαν από το λογισμικό
- Δεδομένα που συσσωρεύτηκαν κατά τη διάρκεια της έρευνας
- Ανακεφαλαίωση των ενεργειών που έγιναν
- Σχετικές αποδείξεις που αποκαλύφθηκαν
- Αποδεικτικά δεδομένα τύπου αρχείων ήχων ή βίντεο (Αυτά πρέπει να περιλαμβάνονται με την οριστική αναφορά στα αφαιρούμενα μέσα, όπως thumb drive, CD-DVD ROM, μαζί με την κατάλληλη εφαρμογή για σωστή εμφάνιση).

6.3 Εργαλεία ψηφιακών πειστηρίων

Η Ψηφιακή Εγκληματολογία σε κινητά τηλέφωνα είναι ένας σχετικά καινούργιος κλάδος της Εγκληματολογίας, με αποτέλεσμα το λογισμικό και τα εργαλεία που απαιτούνται για την ανίχνευση στοιχείων είναι ακόμα σε αρχικό στάδιο. Επιπρόσθετα, με την εξέλιξη, που παρατηρείται στις κινητές συσκευές, τα εργαλεία είναι σχεδόν αδύνατο να μπορούν άμεσα να εξυπηρετήσουν όλες τις συσκευές. Τα εργαλεία αυτά μπορεί να είναι, εξειδικευμένες συσκευές ή υλικό, βασιζόμενα στο πως μπορούν να ανιχνευθούν δεδομένα στις κινητές συσκευές [35] .

Υπάρχουν αρκετά εργαλεία που κυκλοφορούν στις μέρες μας και υπόσχονται θεαματικά αποτελέσματα, εκ των οποίων αυτά που προσφέρουν φυσική εξαγωγή/ανάλυση δεδομένων, έχουν πολύ υψηλό κόστος. Στο πλαίσιο εκτέλεσης πειραμάτων, στη παρούσας εργασία, θα χρησιμοποιηθούν τα υπάρχοντα δωρεάν εργαλεία ανάλυσης με γνώμονα την ευρύτερη κάλυψη των συσκευών, άρα και υποθέσεων ενός ερευνητή, καθώς επίσης και τη βέλτιστη απόδοση, όσον αφορά τα εξαγόμενα αποτελέσματα-πειστήρια.

Η πληθώρα εργαλείων για ψηφιακά πειστήρια σε Android συσκευές από τη μία, σε συνδυασμό με τους διαφορετικούς τύπους συσκευών από την άλλη, καθιστούν αδύνατη την ύπαρξη μιας κοινής μεθοδολογίας ή προτύπου, που θα κάλυπτε τις περισσότερες των περιπτώσεων. Ως αποτέλεσμα των παραπάνω, είναι το γεγονός ότι οι ερευνητές, που αναζητούν γρήγορα και αποτελεσματικά εργαλεία, αντιμετωπίζουν προβλήματα εγκυρότητας. Παράλληλα, η βιομηχανία παραγωγής εργαλείων δεν ακολουθεί ένα πρότυπο, που θα καλύπτει επαρκώς τις υποθέσεις ψηφιακής εγκληματολογίας [36]. Επίσης λόγω του μεγάλου εύρους κινητών συσκευών Android, τα εργαλεία ψηφιακών πειστηρίων εξάγουν τα δεδομένα αυτά με διαφορετικό τρόπο. Τέλος, παρόλο που πολλοί ερευνητές έχουν ασχοληθεί με τον κλάδο της Εγκληματολογίας σε κινητά τηλέφωνα και ορισμένοι έχουν εκδώσει μεθοδολογίες για τη διαδικασία, δεν υπάρχει μια κοινώς αναγνωρισμένη μέθοδος συγκεκριμένα για κινητά Android.

Με οδηγό τις παραπάνω παρατηρήσεις, τα εργαλεία που επελέγησαν να παρουσιαστούν είναι:

α. Santoku via Forensics

Το Santoku, είναι μια πλατφόρμα για Mobile Forensics, Mobile Malware και Mobile Security. Η ελεύθερη έκδοση της Κοινότητας Santoku , είναι ένα πρόγραμμα συνεργασίας για την παροχή προρυθμισμένου περιβάλλοντος Linux με εργαλεία , οδηγούς (drivers) και οδηγίες χρήσεις για τις περιοχές αυτές. Είναι μια πλατφόρμα με τα πιο σύγχρονα εργαλεία ασφάλειας και βοηθητικά προγράμματα που επικεντρώνεται σε λειτουργικά συστήματα, όπως το Android και iOS. Είναι μια δωρεάν και ανοικτή διανομή που περιέχει τα καλύτερα εργαλεία από το διαδίκτυο, με έμφαση στην Ψηφιακή Εγκληματολογία για κινητά. Έχει πολλά προεγκατεστημένα εργαλεία, το οποίο σημαίνει ότι παρέχει πολλές δυνατότητες, χωρίς την εκ νέου εγκατάσταση κάθε εργαλείου ξεχωριστά.

β. MOBILedit Forensic

Η lite έκδοση του προγράμματος διατίθεται δωρεάν στο διαδίκτυο ενώ δεν απαιτείται κωδικός ενεργοποίησης. Επιτρέπει στους ερευνητές να αποκτήσουν πρόσβαση, να αναζητήσουν δεδομένα και να εξετάσουν το κινητό τηλέφωνο. Χρησιμοποιεί πολλαπλούς μηχανισμούς συνδεσιμότητας από οποιοδήποτε άλλο εργαλείο, ειδικά την ασύρματη σύνδεση του κινητού με το πρόγραμμα. Το πρόγραμμα είναι αρκετά αποτελεσματικό, στο να εξάγει πληροφορίες του συστήματος, όπως επαφές και λίστες μηνυμάτων. Το πρόγραμμα εγκαθιστά μία εφαρμογή στο κινητό (loader), ώστε να εξάγει τα δεδομένα. Πλεονέκτημα του αποτελεί το γεγονός ότι η σύνδεση του κινητού με το πρόγραμμα μπορεί να γίνει και ασύρματα, εκτός από την ενσύρματη.

γ. Paraben's Device Seizure

Το Paraben Devise Seizure διανέμεται δωρεάν στο διαδίκτυο μόνο στην demo έκδοση του και απαιτείται δημιουργία λογαριασμού και κλειδί ενεργοποίησης, ώστε να είναι διαθέσιμο. Το εργαλείο Paraben έχει πολύ χαμηλές απαιτήσεις συστήματος, οπότε μπορεί να εκτελεστεί σε οποιονδήποτε υπολογιστή. Παρέχει συνεχής υποστήριξη και μπορεί να εξετάσει ακόμη και μη υποστηριζόμενα μοντέλα κινητών αρκεί να είναι γνωστός ο κατασκευαστής. Το Paraben μπορεί να αναζητήσει σημαντικά δεδομένα σε όλη τη μνήμη του κινητού. Ωστόσο επικεντρώνεται στο φυσικό επίπεδο παρά στο λογικό γιατί μπορεί να αποκτήσει περισσότερες πληροφορίες.

δ. BitPim

Ένα αρκετά χρήσιμο εργαλείο forensics είναι το BitPim. Είναι ένα δωρεάν πρόγραμμα ανοιχτού κώδικα που επιτρέπει την εξαγωγή δεδομένων από κινητά

Android. Είναι ένα ελαφρύ πρόγραμμα συμβατό με αρκετούς τύπους συσκευών όπως π.χ. LG, Samsung, Sanyo και άλλους κατασκευαστές. Αυτό περιλαμβάνει τον τηλεφωνικό κατάλογο, ημερολόγιο, wallpapers, ringtones (η λειτουργικότητα διαφέρει ανάλογα με το τηλέφωνο) και το σύστημα αρχείων για τα περισσότερα CDMA chipset τηλέφωνα. Είναι ένα εργαλείο που η δημιουργία του είναι καθαρά μόνο για υποθέσεις εγκληματολογίας, το οποίο υποστηρίζεται από τα Windows για αντιμετώπιση περιστατικών. Χρησιμοποιείται από πανεπιστήμια, ερευνητές, επιθεωρητές μέχρι αξιωματικούς και στρατιωτικούς. Γενικά είναι ένα χρήσιμο εργαλείο, αλλά και αποτελεσματικό σε περιπτώσεις διαδικτυακών, και όχι μόνο, εγκλημάτων.

6.4 Σχεδιασμός πειραμάτων

Όπως είδαμε σε προηγούμενο κεφάλαιο, στα κινητά Android, τα δεδομένα καταχωρούνται σε πολλά σημεία, από τα οποία μπορούν να εξαχθούν. Έτσι αποθηκεύονται πολλές πληροφορίες, που σχετίζονται με το σύστημα, τους χρήστες, τις εφαρμογές, τα πολυμέσα κ.α. σε διάφορα μέρη του κινητού, όπως η εσωτερική μνήμη, η εξωτερική μνήμη και η βάση δεδομένων. Τα δεδομένα στα οποία θα εστιαστεί η έρευνα στο πλαίσιο αυτής της εργασίας είναι οικονομικά, προσωπικά και στοιχεία προσδιορισμού γεωγραφικής θέσης, τα οποία μπορούν να ανιχνευθούν σε μια συσκευή, που έχει εγκατεστημένη την εφαρμογή ψηφιακό πορτοφόλι.

Η δωρεάν έκδοση των εργαλείων που επιλέχθηκαν έχουν περιορισμένες δυνατότητες σε σύγκριση με τις αντίστοιχες εμπορικές εκδόσεις, των οποίων το κόστος είναι πολύ υψηλό. Η ανάλυση της SD κάρτας δεν αποτέλεσε αντικείμενο των συγκεκριμένων πειραμάτων, καθώς δεν επιτρέπουν την εγκατάσταση ή μεταφορά εφαρμογών πληρωμών σε αυτές. Επιπλέον από ερευνητική σκοπιά, οι κάρτες αυτές είναι διαμόρφωσης FAT ή FAT32, όπου οι τεχνικές ανάλυσης τους είναι όπως και αυτές των υπολογιστών και απευθύνονται περισσότερο στο τομέα του Computer Forensics.

6.5 Παρουσίαση αποτελεσμάτων- Αξιολόγηση

Στο σημείο αυτό, θα γίνει η παρουσίαση της πρακτικής εξέτασης δυο κινητών συσκευών/τηλέφωνων, η μια με δικαιώματα διαχειριστή και η άλλη

απλού χρήστη από τον κατασκευαστή. Για την εξέταση των συσκευών χρησιμοποιήσαμε τα εργαλεία, που αναφέρθηκαν στην προηγουμένη παράγραφο. Πριν την εφαρμογή των προγραμμάτων έχουν υπολογιστεί τα διαθέσιμα δεδομένα του κινητού, ώστε να συγκριθούν με τα αποτελέσματα που θα προκύψουν από το καθένα.

Τα κινητά τηλέφωνα, που αξιοποιήθηκαν για τα πειράματα είναι το Samsung Galaxy Young II (rooted) και το Samsung Galaxy J1(2016). Η διαδικασία μετατροπής ενός κινητού σε rooted, δεν είναι αποδεκτή από πλευράς ψηφιακής εγκληματολογίας, επειδή παρεμβαίνουμε στο κινητό και ως εκ τούτου, επιλέχθηκε η εξέταση συσκευής για έρευνα να διαθέτει ήδη προνομιακά δικαιώματα πρόσβασης. Ο κύριος λόγος, που επιλέχθηκαν τα συγκεκριμένα κινητά είναι το γεγονός ότι, υποστηρίζονται και από τα τέσσερα εργαλεία ανάλυσης και καλύπτουν τις ελάχιστες απαιτήσεις των εφαρμογών e-Wallet που είναι :

- η ύπαρξη NFC κυκλώματος
- το λογισμικό android έκδοσης τουλάχιστον 4.4.2
- χωρίς σπασμένο (rooted) λογισμικό

Η σύνδεση με τον υπολογιστή γίνεται μέσω του ADB (Android Device Bridge) για να γίνει η ανάλυση και η εξαγωγή των δεδομένων. Τα προγράμματα που έχουν χρησιμοποιηθεί στην παρούσα εργασία είναι:

- ***Santoku via Forensics***
- ***MOBILedit Forensic***
- ***Paraben's Device Seizure***
- ***BitPim***

Η εξέταση των κινητών πραγματοποιήθηκε με τις παρακάτω παραδοχές:

i) τα κινητά δεν είναι κλειδωμένα, διότι όλο και περισσότερα εργαλεία ανάλυσης εφοδιάζονται, με το λογισμικό Screen lock disabler devices based on Android OS και ξεκλειδώνουν όλων των ειδών τα κλειδώματα (Pin, Image, Password & Fingerprint).

ii) η λειτουργία USB Debugging είναι ενεργοποιημένη

iii) οι συσκευές είναι ενεργοποιημένες και

iv) θα εξεταστεί η εφαρμογή winbank wallet [37] της Τράπεζας Πειραιώς, ως η πιο αντιπροσωπευτική εφαρμογή πληρωμών και η πιο κοντινή στα πρότυπα του ψηφιακού πορτοφολιού. Αξίζει να υπενθυμίσουμε, ότι η εν λόγω εφαρμογή εγκαταστάθηκε με επιτυχία και στη συσκευή με δικαιώματα διαχειριστή χωρίς την αναγνώριση του λογισμικού ως «σπασμένο». Πριν ξεκινήσουμε τη διαδικασία για την εξέταση τους, θα πρέπει αρχικά να τα σημάνουμε και έπειτα να τα φωτογραφίσουμε.

Καθώς υπάρχουν πολλών ειδών δεδομένα, που μπορούν να ανιχνευθούν στα κινητά Android, για να μπορέσουμε να αξιολογήσουμε τα αποτελέσματα, θα δώσουμε έμφαση σε αυτά, που είναι κοινά και στα τέσσερα εργαλεία. Αυτά τα δεδομένα είναι:

- Πληροφορίες συστήματος
- Κατάλογος επαφών
- Λίστα κλήσεων (εισερχόμενες, εξερχόμενες, αναπάντητες)
- SMS/MMS
- Εικόνες
- Ήχοι
- Videos
- Ημερολόγιο
- Αρχεία (PDFs, Word, Excel, PowerPoint, αρχεία συστήματος)
- Εφαρμογές
- Σελιδοδείκτες περιηγητή

Η λογική ανάλυση του κινητού Android είναι το βασικότερο στάδιο για την εξαγωγή ψηφιακών πειστηρίων, από το κινητό τηλέφωνο. Η εφαρμογή των προγραμμάτων ανάλυσης, έγινε μετά την εγκατάσταση της εφαρμογής e-Wallet

και στα δυο κινητά , ώστε να έχουμε ένα κοινό μέτρο σύγκρισης. Καθένα από τα εργαλεία χρησιμοποιεί διαφορετικές τεχνικές για να εξάγει τα δεδομένα.

Τα αποτελέσματα της πρακτικής εξέτασης συνοψίζονται στους παρακάτω δύο πίνακες (Πίνακας 1,2), όπου στον πρώτο διακρίνονται τα αποτελέσματα από το κινητό με δικαιώματα διαχειριστή, ενώ στο δεύτερο αυτά της άλλης περίπτωσης που εξετάστηκε. Τα αναλυτικά αποτελέσματα της εκτέλεσης των εργαλείων απεικονίζονται, στο Παράρτημα «Α». Διευκρινίζεται ότι, το κάθε εργαλείο έχει διαφορετική μεθοδολογία και κριτήρια ως προς τα δεδομένα, όπως επίσης και ότι διαφορετικό κινητό Android, ακόμα και της ίδιας εταιρίας, μπορεί να φέρει διαφορετικά αποτελέσματα. Τέλος, πρόκειται για μια διαδικασία αρκετά χρονοβόρα, η οποία δεν είναι εφαρμόσιμη για όλους τους τύπους των συσκευών.

Samsung Galaxy Young II (rooted)	Sandoku Via Forensics	MOBILedit Forensics	Paraben's Device Seizure	BitPim
Πληροφορίες συστήματος	•	✓	•	•
Επαφές	✓	✓	✓	✓
Κλήσεις	✓	✓	•	✓
SMS	✓	✓	•	✓
Εικόνες	✓	✓	•	•
Ήχοι	✓	✓	•	✓
Videos	✓	✓	•	•
Ημερολόγιο	•	•	•	•
Εφαρμογές	•	✓	•	•
Αρχεία	•	•	•	•
Σελιδοδείκτες	•	•	•	•

Πίνακας 1. Αποτελέσματα εγκληματολογικής εξέτασης Ι

Τα αποτελέσματα των εργαλείων δεν είναι τα αναμενόμενα όσον αφορά τα αρχεία των εφαρμογών και συγκεκριμένα του e-Wallet, ειδικά για την πλατφόρμα Linux, που επιλέχθηκε ακριβώς για αυτόν τον σκοπό. Εντύπωση

επίσης προκαλεί το γεγονός ότι η εκτέλεση των εργαλείων δεν οδηγεί σε διαφορετικά αποτελέσματα στην περίπτωση, όπου η συσκευή έχει δικαιώματα διαχειριστή.

Όμως, σε σύγκριση με τα υπόλοιπα δεδομένα της συσκευής, διαπιστώνουμε ότι σχεδόν σε όλες τις κατηγορίες συγκεντρώθηκε ικανοποιητικός αριθμών πειστηρίων, που υπό προϋποθέσεις θα μπορούσε να διαλευκάνει μια υπόθεση ψηφιακής εγκληματολογίας. Τα στοιχεία αυτά που συλλέχθηκαν στο πλαίσιο της λογικής ανάλυσης από τα δωρεάν εργαλεία, αποτελούν σημαντικά στοιχεία σε αναλύσεις κινητών.

Samsung Galaxy J1(2016)	Sandoku Via Forensics	MOBILedit Forensics	Paraben's Device Seizure	BitPim
Πληροφορίες συστήματος	•	✓	•	•
Επαφές	✓	✓	✓	✓
Κλήσεις	✓	✓	•	✓
SMS	✓	✓	•	✓
Εικόνες	✓	✓	•	•
Ήχοι	✓	✓	•	✓
Videos	✓	✓	•	•
Ημερολόγιο	•	•	•	•
Εφαρμογές	•	✓	•	•
Αρχεία	•	•	•	•
Σελιδοδείκτες	•	•	•	•

Πίνακας 2. Αποτελέσματα εγκληματολογικής εξέτασης ΙΙ

Σχολιάζοντας τα αποτελέσματα στην παραπάνω εικόνα μπορούμε να συμπεράνουμε καταρχήν, ότι με τη χρήση των αντίστοιχων εμπορικών εκδόσεων των εργαλείων, που εξετάστηκαν, οι οποίες δεν υπόκεινται σε πολλούς περιορισμούς, η έρευνα μπορεί να είχε οδηγήσει σε τελείως διαφορετικά αποτελέσματα.

Στο κομμάτι της έρευνας των πειστηρίων, που εστίασε η συγκεκριμένη εργασία και αφορά την εφαρμογή e-Wallet που είναι εγκατεστημένη στη συσκευή, τα αποτελέσματα της λογικής ανάλυσης των κινητών συσκευών είναι απογοητευτικά. Από τα εργαλεία που χρησιμοποιήθηκαν μόνο το MOBILedit Forensics κατάφερε να εντοπίσει την εγκατάσταση της εν λόγω εφαρμογής (καθώς επίσης και αυτών που προϋπήρχαν από τον κατασκευαστή), χωρίς όμως να είναι διαθέσιμα περαιτέρω στοιχεία πληρωμών , καρτών ή συναλλαγών που πραγματοποιήθηκαν.

Ωστόσο τα παραπάνω αποτελέσματα δεν μπορούν να είναι καθοριστικά στην χρήση των εργαλείων. Υπάρχουν πολλοί παράγοντες που επηρεάζουν στην αποτελεσματικότητα τους. Έτσι, εκτός από την διαφορετική μεθοδολογία, σαφώς παίζουν ρόλο στα αποτελέσματα της έρευνας παράγοντες, όπως το κινητό τηλέφωνο, το λειτουργικό σύστημα στις διάφορες εκδόσεις του καθώς επίσης και οι οδηγοί που χρησιμοποιεί το κάθε εργαλείο.

Το τελευταίο στάδιο της έρευνας μας είναι να εξετάσουμε τις παραπάνω συσκευές, χωρίς την χρησιμοποίηση ελεύθερων λογισμικών, για τις δύο προαναφερόμενες περιπτώσεις με τεχνική ανάλυση. Μάλιστα, θα αναφερθούμε μόνο στην περίπτωση που το τηλέφωνο είναι rooted, γνωρίζοντας, ότι αν δεν υπάρχουν δικαιώματα διαχειριστή για να μπορέσουμε να πραγματοποιήσουμε την ανάλυση θα πρέπει να εκτελέσουμε μια σειρά εντολών για αντίγραφα ασφαλείας με λειτουργίες, που δεν είναι διαθέσιμες σε όλες τις εκδόσεις Android. Στην περίπτωση αυτή οι εξεταστές ψηφιακών πειστηρίων μπορούν να πάρουν τα δεδομένα από την συσκευή δίχως αυτή να είναι Rooted, αλλά με πολύ περιορισμένες πιθανότητες και χωρίς να έχουν πρόσβαση σε σημαντικούς φακέλους, μέσω του adb shell, καθόσον δεν θα υπάρχουν δικαιώματα διαχειριστή.

Στην περίπτωση αυτή χρησιμοποιήθηκε ένας Η/Υ με επεξεργαστή Intel core 2 Duo 2.27 GHz με Windows 7 Professional, 4GB Μνήμη RAM και σκληρό δίσκο ssd. Στον συγκεκριμένο υπολογιστή έχει εγκατασταθεί το

Android SDK, στο οποίο παρέχεται και το Android ADB, ένα εργαλείο με αρκετές δυνατότητες για τον εξεταστή ψηφιακών πειστηρίων.

Η τεχνική ανάλυση ενός κινητού, όπως αναφέραμε και προηγουμένως, έχει σαν στόχο να δημιουργήσει memory dumps της εσωτερικής μνήμης και στη συνέχεια να τα αξιοποιήσει. Ωστόσο, τα περισσότερα διαθέσιμα δωρεάν εργαλεία, δεν έχουν δυνατότητες για εξαγωγή ψηφιακών πειστήριων. Επίσης, πρόβλημα παρουσιάζεται στα αρχεία του Android τύπου YAFFS2, όπου κανένα εργαλείο ψηφιακών πειστηρίων δεν τα υποστηρίζει. Ο χώρος αυτός στα περισσότερα προγράμματα αναφέρεται, ως μη καταχωρημένος. Για τους λόγους αυτούς, επιλέχθηκε η εξέταση της «σπάνιας» περίπτωσης που το προς ανάλυση κινητό έχει ήδη δικαιώματα διαχειριστή και έχει έρθει προς ανάλυση στο εργαστήριο ενεργοποιημένο και ξεκλείδωτο. Τα αρχεία εφαρμογών του κινητού Android μπορούν να εντοπιστούν στο φάκελο /data και στον υποφάκελο που μας ενδιαφέρει για ανάλυση και είναι ο data/data.

Οι βάσεις δεδομένων του κινητού Android αποθηκεύονται στον φάκελο του συστήματος /data/data/<packageName>/database. Αυτές οι βάσεις μπορούν να αναλυθούν με ειδικά προγράμματα τα οποία παρέχονται από τις δωρεάν πλατφόρμες Sandoku και Deft, όπως το SQLite Database Browser. Ενδιαφέρον παρουσιάζουν από πλευράς των ψηφιακών πειστηρίων, οι παρακάτω βάσεις [38]:

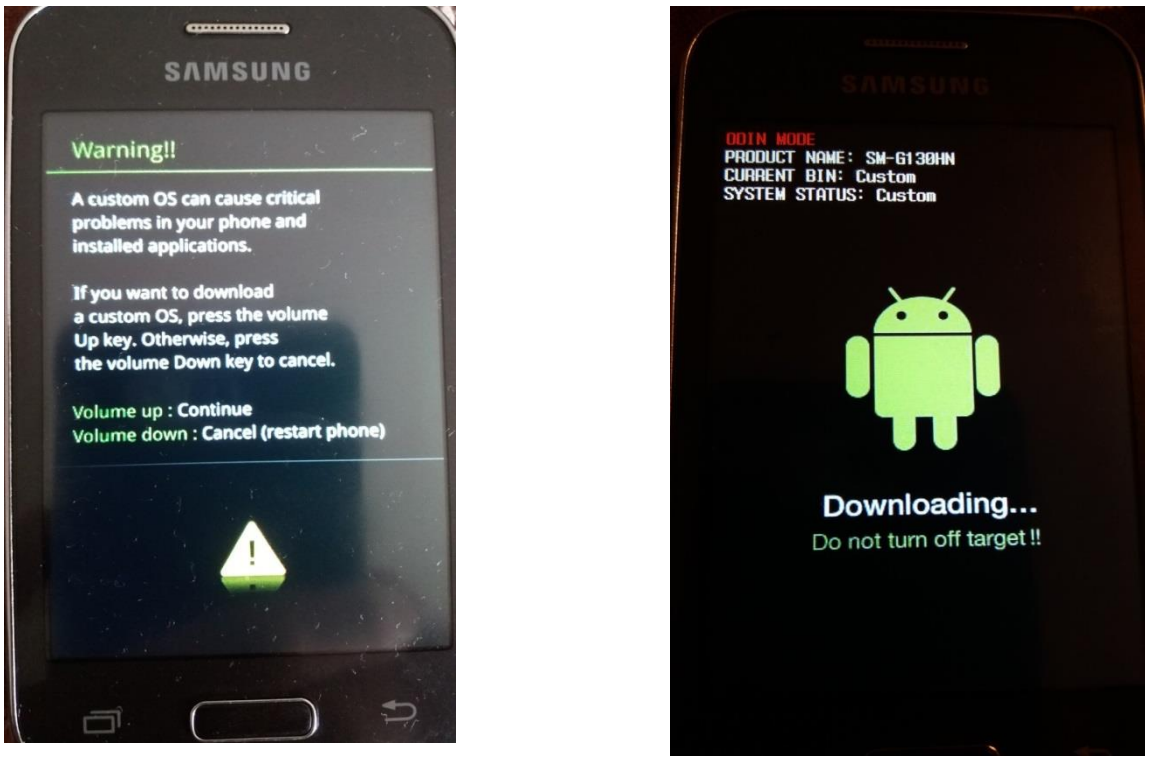
- /com.android.browser/browser.db: Περιλαμβάνει σελιδοδείκτες από το διαδίκτυο
- /com.android.browser/webview.db: Εδώ καταχωρούνται όλες οι ιστοσελίδες που απαιτούν είσοδο με nickname και password
- /com.android.providers.downloads/downloads.db: Περιλαμβάνει πληροφορίες από τις λήψεις που έχουν γίνει από το διαδίκτυο.
- /com.htc.android.mail/: Καταχωρεί όλους τους λογαριασμούς αλληλογραφίας που έχουν συνδεθεί στο κινητό Android.

Παρόλο, που η εν λόγω συσκευή έχει γίνει root πριν τη διαδικασία της ανάλυσης, ο ερευνητής θα διαπιστώσει στο εργαστήριο, ότι το Bootloader είναι

κλειδωμένο και ως εκ τούτου δεν είναι εφικτή η πρόσβαση στον φάκελο /data κατόπιν ελέγχου, που πραγματοποιείται μέσω του adb shell.

Χρησιμοποιούμε, στη συνέχεια, μια σειρά από εργαλεία προκειμένου να δημιουργήσουμε ένα πλήρες αντίγραφο προς ανάλυση με τη χρήση των αρχείων ανάκτησης, που χρησιμοποιούνται για την επαναφορά του συστήματος.

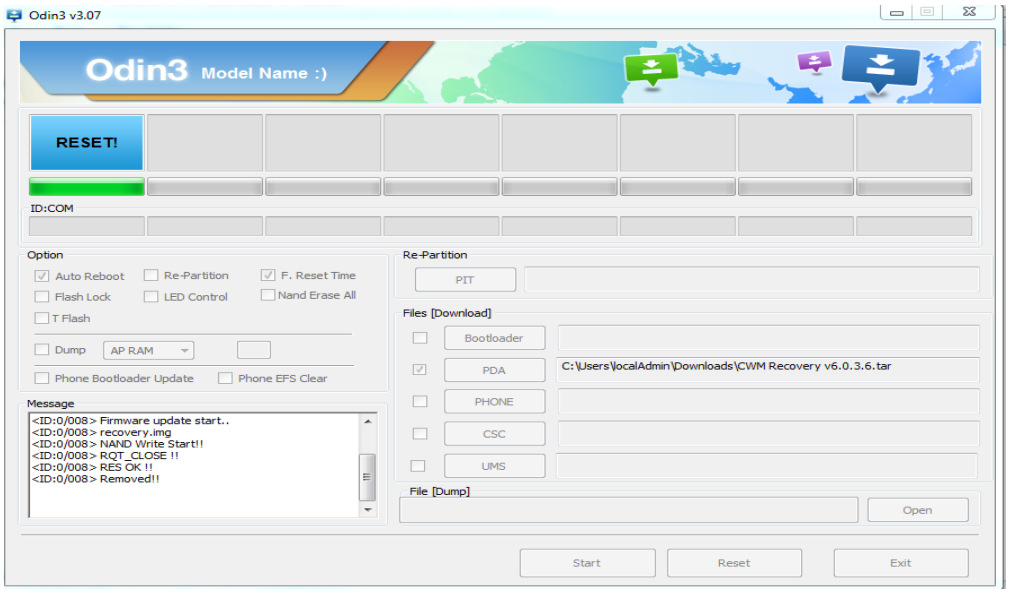
Πιο συγκεκριμένα, χρησιμοποιήθηκε η Clockworkmod (6.0.3.7), ένα προσαρμοσμένο αρχείο ανάκτησης. Για την εγκατάσταση στη συσκευή, πιέζουμε ταυτόχρονα τα πλήκτρα power, volume down, home menu (διαφέρει από τύπο σε τύπο συσκευής), προκειμένου να έρθει στη κατάσταση download mode (Εικόνα 22).



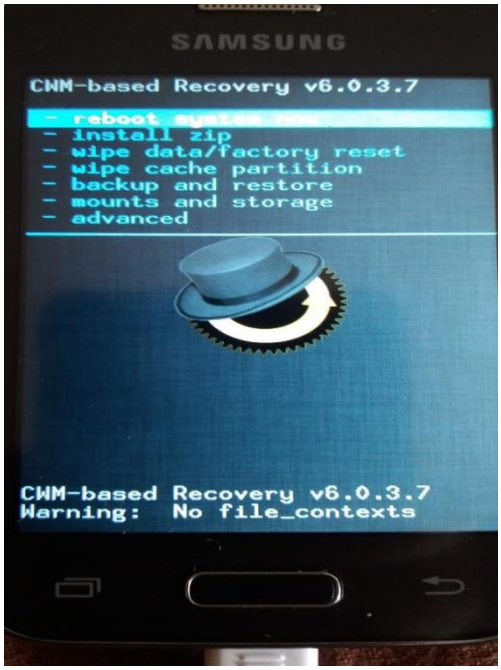
Εικόνα 22. Απεικόνιση συσκευής σε κατάσταση download mode

Έπειτα, χρησιμοποιούμε το εργαλείο Odin3, για εισαγωγή της έκδοσης του Clockworkmod στη συσκευή. Συνδέουμε την συσκευή και διαλέγουμε στο μενού την επιλογή PDA, όπου εισάγουμε το αντίστοιχο αρχείο (Εικόνα 23). Ελέγχουμε τη διαδικασία με τα πλήκτα power, volume

up, home menu, αυτή τη φορά, προκειμένου να μπούμε σε recovery mode και περιμένοντας να εμφανιστεί η custom έκδοση, αντί της προεγκατεστημένης (Εικόνα 24).



Εικόνα 23. Αποτέλεσμα του εργαλείου Odin



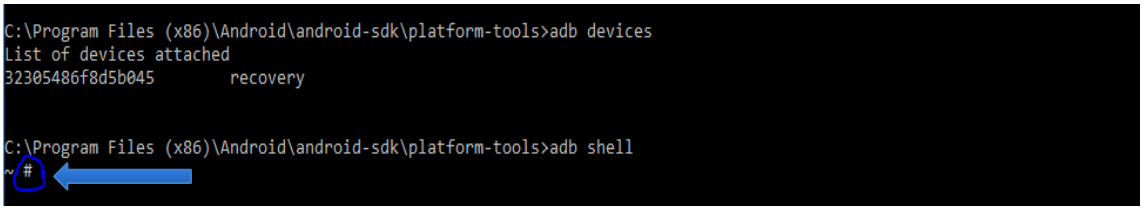
Εικόνα 24. Απεικόνιση της custom recovery image ClockworkMod

Στη συνέχεια, στο menu που εμφανίζεται, επιλέγουμε το /mount and storage και έπειτα κάνουμε mount το φάκελο /data (Εικόνα 25). Επιστρέφουμε στο αρχικό μενού και επιλέγουμε back up and storage, μέσω της οποίας

δημιουργούμε αντίγραφο (Εικόνα 26), το αρχείο που παρουσιάζει εγκληματολογικό ενδιαφέρον, με επιλεγμένο το διαμέρισμα, που περιέχει τα δεδομένα του χρήστη της συσκευής. Ελέγχουμε την διαδικασία χρησιμοποιώντας το adb shell του SDK, όπου διαπιστώνουμε, ότι τώρα αποκτήσαμε πλήρη δικαιώματα πρόσβασης (Εικόνα 27).

Εικόνα 25. mount and storage

Εικόνα 26. Back up



Εικόνα 27. Απεικόνιση των adb devices & adb shell

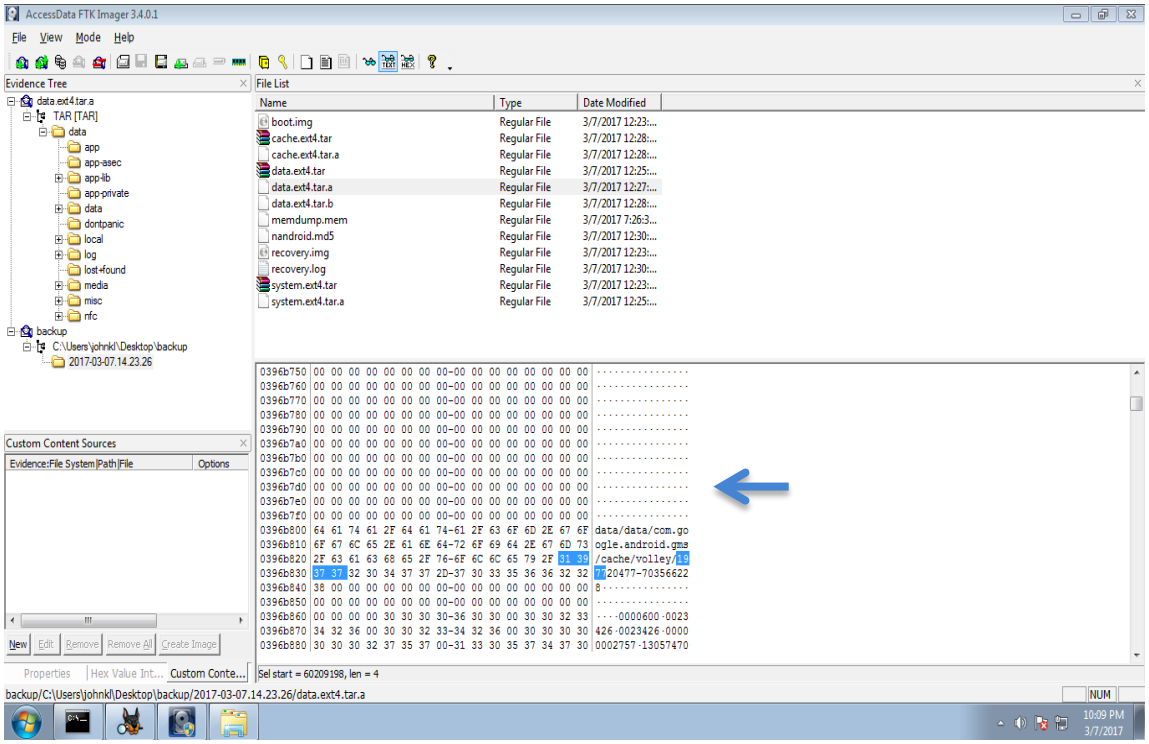
Το αποτέλεσμα της παραπάνω διαδικασίας, μπορεί να αναλυθεί με τη χρήση ελεύθερου λογισμικού, όπως του Autopsy και του FTK Imager. Θα χρησιμοποιήσουμε και τα δύο εργαλεία, τα οποία προσφέρονται δωρεάν για διασταύρωση και έλεγχο αποτελεσμάτων επί των επίμαχων δεδομένων της εφαρμογής e-Wallet.

Σ' αυτό το σημείο, πρέπει να τονιστεί, ότι η αναζήτηση επικεντρώθηκε στον κωδικό πρόσβασης mpin, του πορτοφολιού, για τη χρήση της κάρτας και στα δεδομένα των συναλλαγών μέσω της εφαρμογής. Με δεδομένες τις τεχνολογίες,

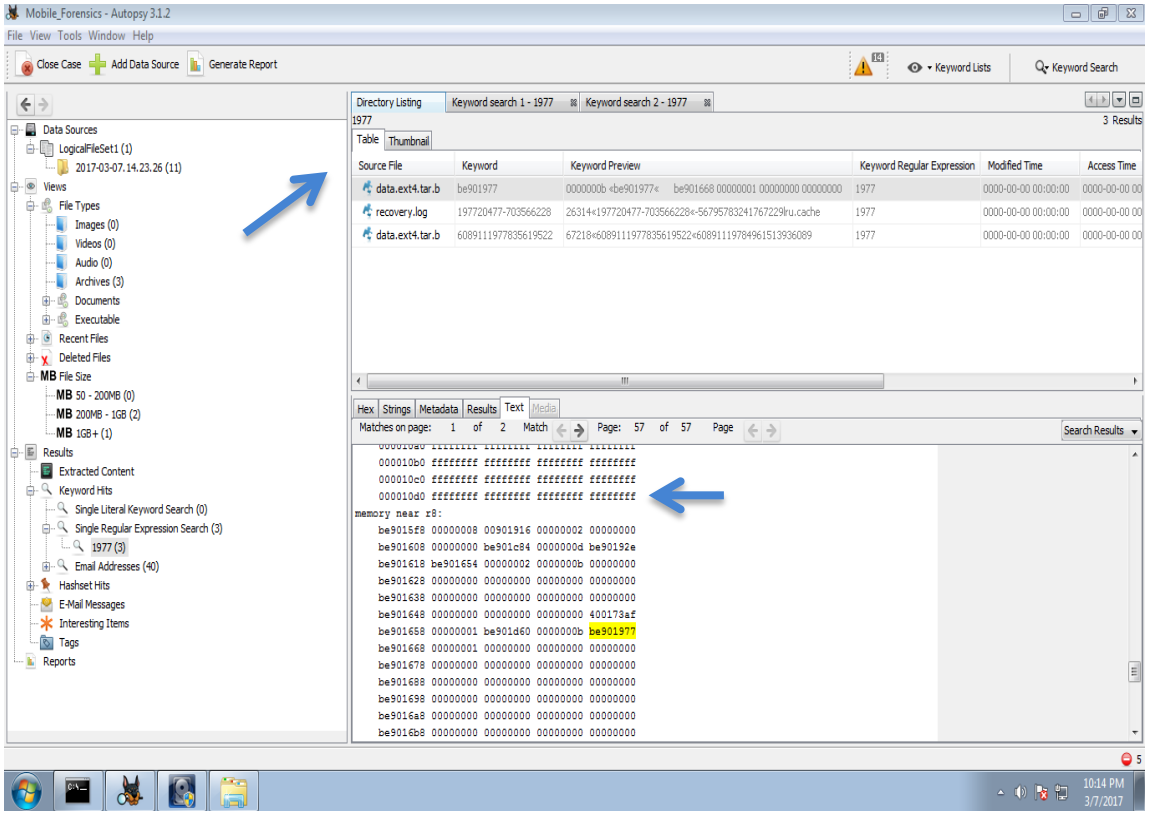
οι οποίες χρησιμοποιούνται από την εφαρμογή και αναλύθηκαν σε προηγούμενο κεφάλαιο, ο κωδικός πρόσβασης είναι το μοναδικό «εκτεθειμένο» στοιχείο, αφού η μοναδική ασφάλειά του είναι η συχνή αλλαγή από το χρήστη. Επίσης, ο αριθμός της κάρτας έχει αντικατασταθεί από άλλον αριθμό χωρίς κάποια σημασία ενώ τα υπόλοιπα στοιχεία μεταφέρονται κρυπτογραφημένα.

Μετά την εκτέλεση των δύο εργαλείων, εντοπίστηκε ο συγκεκριμένος κωδικός έπειτα από στοχευμένη αναζήτηση, προς επιβεβαίωση των όσων λαμβάνουν χώρα κατά την εκτέλεση της εφαρμογής. Αξίζει να σημειωθεί, ότι στο εργαλείο Autopsy εντοπίστηκε μεν στον ίδιο φάκελο, όπως και με το άλλο εργαλείο, αλλά σε τρία διαφορετικά σημεία, γεγονός που καταδεικνύει τον διαφορετικό τρόπο εκτέλεσης και μεθοδολογίας του κάθε εργαλείου. Σημειώνεται επίσης, ότι η παραπάνω διαδικασία εντοπισμού συγκεκριμένων πειστηρίων είναι εξαιρετικά χρονοβόρα και η αποτελεσματικότητά της είναι συνάρτηση πολλών παραγόντων, με κυρίαρχα την εμπειρία του εκάστοτε ερευνητή και τον διαθέσιμο χρόνο.

Στην συνέχεια ακολουθούν απεικονίσεις από την διαδικασία ανάλυσης και εντοπισμού για τα δύο προαναφερόμενα εργαλεία.



Εικόνα 28. Απεικόνιση των αποτελεσμάτων FTK Imager



Εικόνα 29. Απεικόνιση των αποτελεσμάτων Autopsy

Κεφάλαιο 7ο
Επίλογος

7.1 Γενικά

Στη παρούσα διπλωματική εργασία εξετάστηκε ο νεοσύστατος κλάδος της Ψηφιακής Εγκληματολογίας σε κινητά τηλέφωνα λογισμικού Android, και αναλύθηκαν οι εφαρμογές πληρωμών e-Wallet. Εκτός από τις ευπάθειες των εφαρμογών και τις τεχνολογίες τους, παρουσιάστηκαν οι βασικές μεθοδολογίες σχετικά με την ανάλυση κινητών τηλεφώνων και των δεδομένων τους. Ορισμένα από τα κορυφαία υπάρχοντα δωρεάν εργαλεία εξετάστηκαν, ως προς την εξαγωγή των δεδομένων. Τα αποτελέσματα που προέκυψαν από τους ελέγχους αναλύθηκαν και συγκρίθηκαν με βάση τα υπάρχοντα δεδομένα των συσκευών.

7.2 Σύνοψη και συμπεράσματα

Συνοψίζοντας μπορούμε να αναφέρουμε, ότι έγινε προσπάθεια τόσο από θεωρητικής όσο και τεχνικής απόψεως να αναλυθούν οι εφαρμογές ψηφιακού πορτοφολιού στο πλαίσιο της επιστήμη της «Ψηφιακής Εγκληματολογίας σε κινητές συσκευές Android. Αρχικά, παρουσιάστηκαν οι βασικές έννοιες σχετικά με το λειτουργικό σύστημα Android, όπως η αρχιτεκτονική, οι εκδόσεις και η δομή των δεδομένων του, ενώ ακολούθησε μια σύντομη περιγραφή ως προς τις τεχνολογίες και τις μεθόδους εγκληματολογικής εξέτασης μιας κινητής συσκευής Android. Τέλος, επικεντρωθήκαμε στα δωρεάν εργαλεία που χρησιμοποιούνται για την εξέταση των συσκευών αυτών και έγινε προσπάθεια τόσο με λογική όσο και τεχνική ανάλυση να ελεγχθούν τα οικονομικά, προσωπικά και στοιχεία προσδιορισμού γεωγραφικής θέσης που θα μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία αποδοχής ή αποποίησης πράξεων .

Η μαζική εισαγωγή των Τεχνολογιών Πληροφορικής και Επικοινωνιών που παρατηρείται τα τελευταία χρόνια, στον χρηματοπιστωτικό τομέα έχει επιφέρει ραγδαίες αλλαγές και εξελίξεις στην σημερινή οικονομική πραγματικότητα. Η ασφάλεια και η ιδιωτικότητα των οικονομικών

συναλλαγών υπόκεινται διαρκώς σε νέους κινδύνους, που δεν είναι εφικτό να περιοριστούν.

Τα έξυπνα τηλέφωνα (smartphones) είναι αναμφισβήτητο, ότι αποτελούν αναπόσπαστο κομμάτι της σύγχρονης ζωής. Ο κλάδος των έξυπνων κινητών είναι νεοσύστατος στην επιστήμη της ψηφιακής εγκληματολογίας. Με βάση τις παραπάνω επισημάνσεις και με την βοήθεια της θεωρητικής και πρακτικής εξέτασης, που πραγματοποιήθηκε στο πλαίσιο της παρούσας εργασίας εξάγονται μια σειρά από χρήσιμα συμπεράσματα, τα οποία συνοψίζονται στα ακόλουθα:

Από πλευράς ερευνητών απαιτείται σχετικά υψηλό υπόβαθρο και γνώση, τόσο του λειτουργικού συστήματος Android, όσο και των τεχνολογιών πληρωμής στις εφαρμογές για κινητά τηλέφωνα, ώστε να κατανοήσει κάποιος τις μεθοδολογίες και τις τεχνικές που χρησιμοποιούνται στα ψηφιακά πειστήρια. Επίσης, μέχρι στιγμής, δεν έχει αναπτυχθεί κάποια μεθοδολογία κοινώς αποδεκτή από τους ερευνητές που ασχολούνται με τον συγκεκριμένο κλάδο, με αποτέλεσμα να είναι δύσκολη η αξιολόγηση των ευρημάτων που εξάγονται από τη συσκευή σε σύγκριση με τα ευρήματα άλλων εργαλείων, αλλά και της χειρονακτικής-τεχνικής ανάλυσης.

Οι κατασκευαστές των εργαλείων εξέτασης διανέμουν νέες εκδόσεις με αυξημένες δυνατότητες, δίχως όμως να έχουν φτάσει στο επιθυμητό επίπεδο, ώστε όλα τα εργαλεία να είναι το ίδιο αποτελεσματικά σε όλες τις εκδόσεις που κυκλοφορούν. Για αυτό οι εξεταστές, είναι αναγκασμένοι να χρησιμοποιούν περισσότερα του ενός εργαλεία, καθώς και να εφαρμόζουν τεχνικές χειροκίνητης ανάλυσης σε συνδυασμό με τα εργαλεία αυτά, προκειμένου να πετύχουν τα βέλτιστα αποτελέσματα. Τα δωρεάν εργαλεία, που υπάρχουν για την εξέταση ψηφιακών πειστηρίων σε κινητά τηλέφωνα είναι ελάχιστα με τις περισσότερες δυνατότητες τους να παρέχονται μόνο στις εμπορικές εκδόσεις, το κόστος των οποίων είναι αρκετά υψηλό.

Η πληθώρα των τύπων των κινητών συσκευών, με διαφορετικές κατασκευαστικές προσεγγίσεις, η πανσπερμία εφαρμογών, η παροχή ασφάλειας σε διαφορετικά επίπεδα (π.χ. κλείδωμα οθόνης, κάρτας, εφαρμογών)

αποτελούν τροχοπέδη στη διαδικασία για δημιουργία καθολικών εργαλείων που μπορούν να υποστηρίζουν το σύνολο των υποθέσεων σε κινητά, ως προς την φυσική και λογική εξαγωγή/ανάλυση της μνήμης των συσκευών.

Στο πλαίσιο ιδιωτικότητας των δεδομένων και των στοιχείων που αποθηκεύονται γενικά σε ένα έξυπνο κινητό τηλέφωνο διαπιστώνουμε, ότι από τη μια πλευρά είναι πολύ περισσότερα από αυτά που πραγματικά αποθηκεύονται, ενώ από την άλλη ο χρήστης, όχι μόνο δεν μπορεί να ελέγξει που αποθηκεύονται, αλλά αγνοεί ότι έχει εγκρίνει και την αποθήκευση τους.

Οι εφαρμογές ψηφιακού πορτοφολιού (e-Wallet), που εγκαθίστανται στα κινητά τηλέφωνα περιέχουν μεγάλο όγκο προσωπικών δεδομένων, στοιχεία επικοινωνίας, πληροφορίες εντοπισμού τοποθεσίας, τραπεζικές πληροφορίες, συναλλαγές κ.τ.λ. Τα περισσότερα, από αυτά τα δεδομένα, είναι κρυπτογραφημένα και δεν αποθηκεύονται στην συσκευή. Ο κωδικός πρόσβασης στις εφαρμογές αυτές δεν προστατεύεται όμως από κάποια γνωστή μέθοδο και μπορεί σε συνδυασμό με ενδεχόμενη απώλεια να ενέχει κινδύνους απώλειας δεδομένων και πόρων.

Οι έξυπνες συσκευές κινητής τηλεφωνίας και οι ταμπλέτες έχουν μετατραπεί σε προσωπικά αντικείμενα που είναι «δεμένα» με τον κάτοχό τους, λόγω των πληροφοριών που μπορούν να αποκτηθούν από τα δεδομένα που αποθηκεύονται στη συσκευή, καθιστώντας παράλληλα ευάλωτη την ιδιωτική ζωή του χρήστη.

Το υφιστάμενο θεσμικό πλαίσιο που καλύπτει τις υποθέσεις ανάλυσης και εξαγωγής ψηφιακών πειστηρίων από κινητές συσκευές θα πρέπει να αναθεωρηθεί υπό το πρίσμα της διευκόλυνσης του έργου του ερευνητή, πάντα όμως στο πλαίσιο της προστασίας του κατόχου από την αυθαιρεσία της εξεταστικής διαδικασίας. Έτσι θα πρέπει να βρεθεί ο νομικά αποδεκτός τρόπος, που θα δίνει για παράδειγμα, τη δυνατότητα στον ερευνητή πλήρους ελέγχου όλων των διαμερισμάτων της συσκευής-στόχο, χωρίς όμως το δικαίωμα τροποποίησης των αποδεικτικών στοιχείων.

ΒΙΒΛΙΟΓΡΑΦΙΑ-ΑΝΑΦΟΡΕΣ

1. Ένωση Ελλήνων Τραπεζών «E- banking:Νέοι ορίζοντες στο τραπεζικό επιχειρείν», 2000

2. "NTT Docomo to take Japanese mobile-Wallet global". NFC World. Retrieved March 23, 2013.

3. Android for Programmers, An App-Driven Approach. 2st Edition Volume1 Prentice Hall, USA. 2014

4. The Android mobile platform By Benjamin Speckmann,2008

5. Detection of Malicious Applications on Android OS, 2010

6. Android Forensics Investigation, Analysis, and Mobile Security for Google Android,2011

7. Professional Android™ 4 Application Development,2012

8. Android Forensic Capability and Evaluation of Extraction Tools,2012

9.https://www.pcisecuritystandards.org/documents/PCI%20Data%20Storage%20Dos%20and%20Donts.pdf

10. Is Payment Tokenization Ready for Primetime? Marianne Crowe and Susan Pandy,2015

11. PCI Security Standards Council, Information Supplement: PCI DSS Tokenization Guidelines, August 2011

12. EMV®* Payment Tokenisation Specification,2014

13. Wikipedia, Host card emulation

14. http://nfc-forum.org/

15. Secure Element Deployment & Host Card Emulation v1.0, 2014

16. Consumer and Mobile Financial Services, 2012

17. http://www.pcmag.com/article/344192/top-8-security-vulnerabilities-threatening-your-smbs-pos-sy

18. Mobile malware increased six-fold in 2011, 2012

19. Malware disguised as new Instagram Android app, 2012

20. Worth, 2012

21. Chen, 2012

22. NIST. Nist special publication 800-131a

23. ECRYPT II. Ecrypt ii yearly report on algorithms and keysizes, 2009-2010.

24. Privacy Rights Clearinghouse, “Data Breaches: A Year in Review,” December 16, 2011

25. Shorter Oxford English Dictionary

26. ΨΗΦΙΑΚΑ ΠΕΙΣΤΗΡΙΑ ΣΕ ΕΞΥΠΝΑ ΤΗΛΕΦΩΝΑ ANDROID,2014

27. Digital Forensics: Case Studies,2013

28. http://www.e-crime.gr/p/video.html

29. Android Forensics. Investigation, Analysis, and Mobile Security for Google Android. USA: Elsevier

30. Mobile Phone Forensics Challenges, Analysis and Tools Classification,2010

31. Live Memory Forensics of Mobile Phones,2010

32. Brothers, S. Cell Phone and GPS Forensic Tool Classification System. 2009

33. ΑΣΦΑΛΕΙΑ,ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΑΠΟΡΡΗΤΟΥ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ,2014

34. Delegate the smartphone user? Security awareness in smartphone platforms. s.l. : Computers & Security, Vol. 34, 2013.

35. Mobile Device Forensics - Tool Testing. Mobile Device Forensics. NIST,2008

36. A Framework for Designing Benchmarks of Investigating Digital

Forensics Tools for Mobile Devices,2011

37. http://www.piraeusbank.gr/el/idiwtes/trapezikes-ypiresies/e-banking/mobile-apps/winbank-wallet/winbank-wallet-app

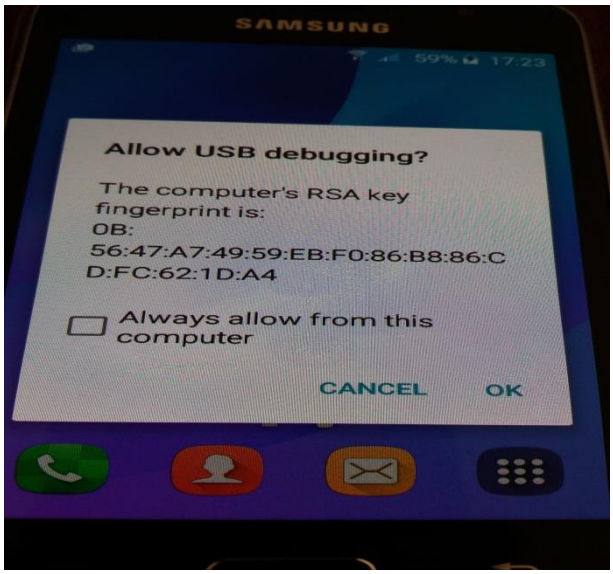
38. Overview of potential forensic analysis of an Android smartphone. Brandenburg University,2012

Παραρτήματα

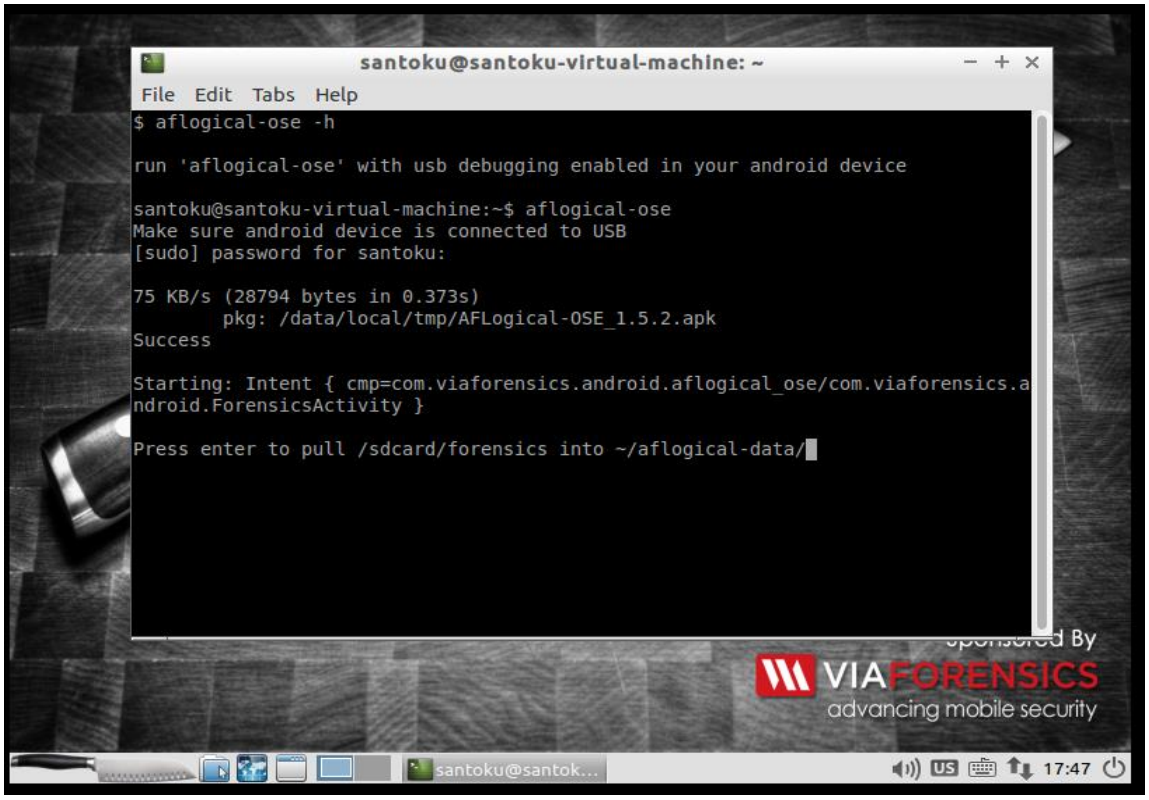
Παράρτημα «Α»

Αποτελέσματα εκτέλεσης εργαλείων εξαγωγής ψηφιακών πειστηρίων

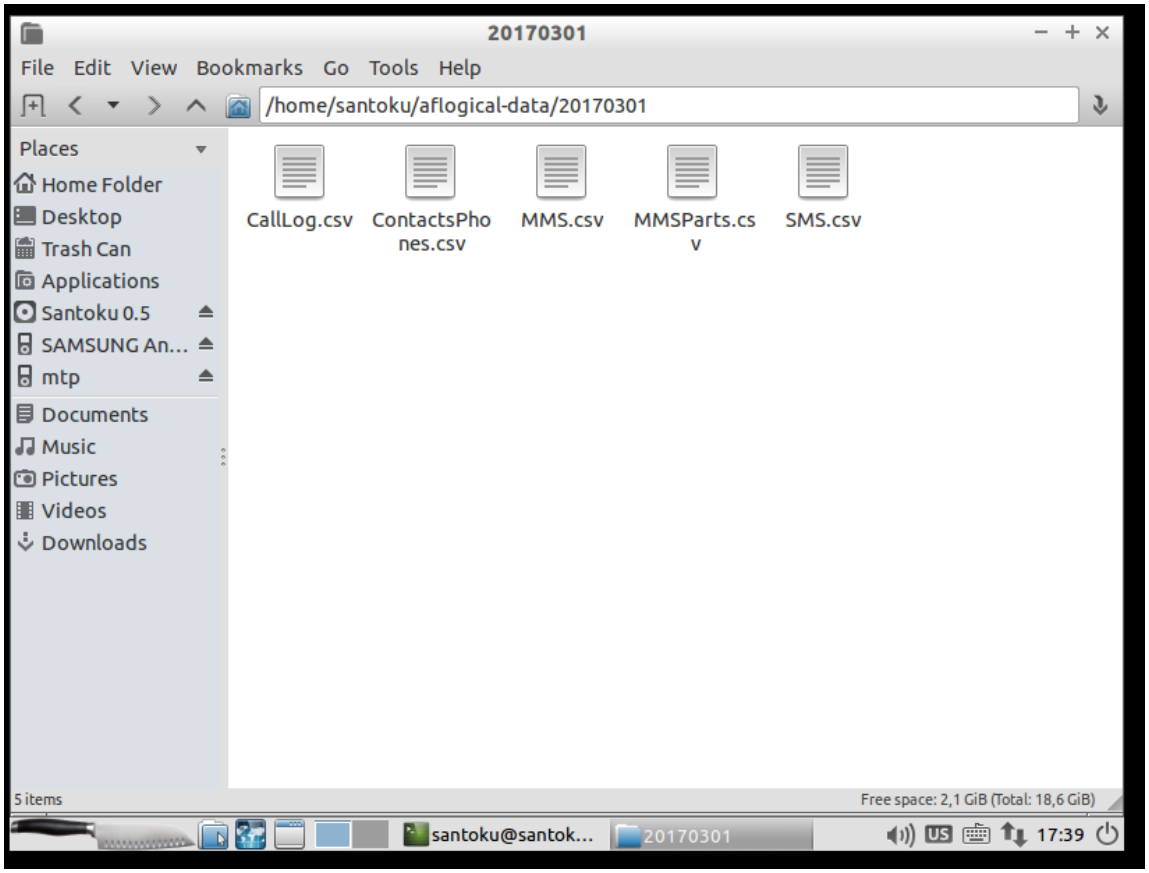
- **Santoku via Forensics**



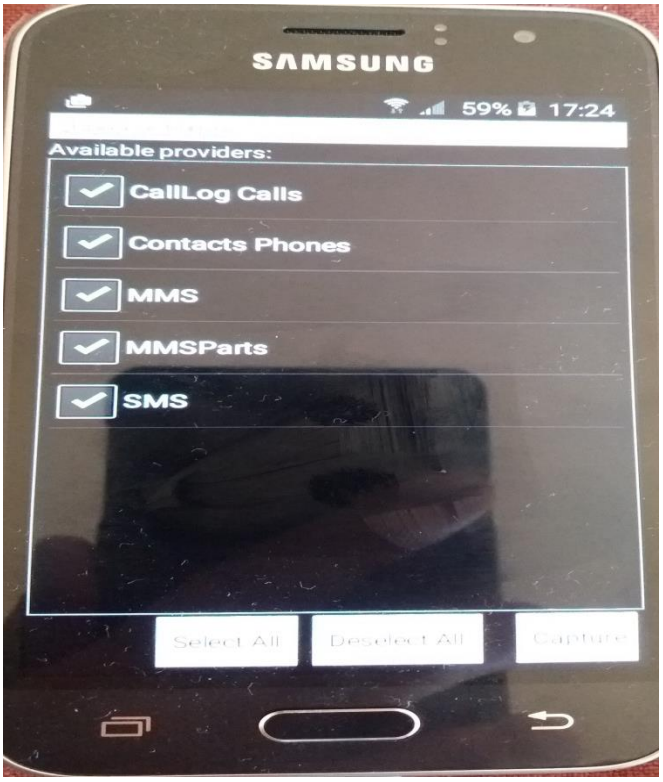
Authorized της συσκευής



Απεικόνιση του εργαλείου AFLogical Sandoku



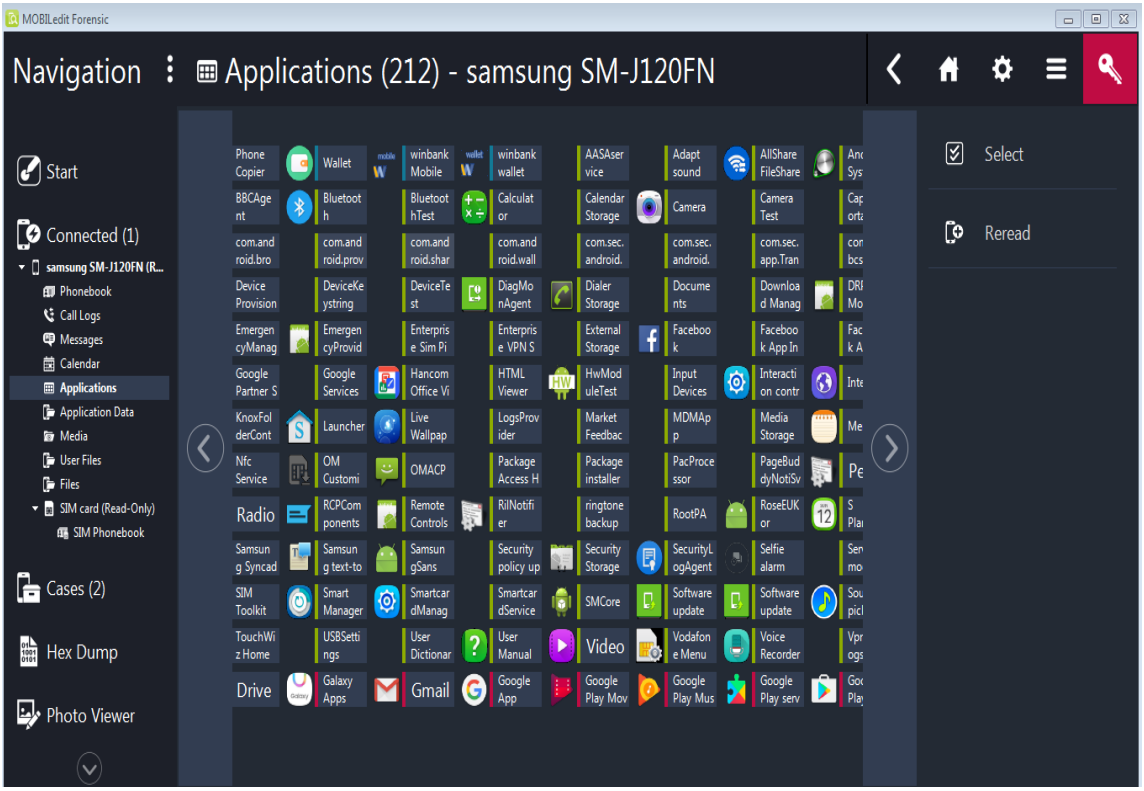
Απεικόνιση των αποτελεσμάτων του AFLogical Sandoku



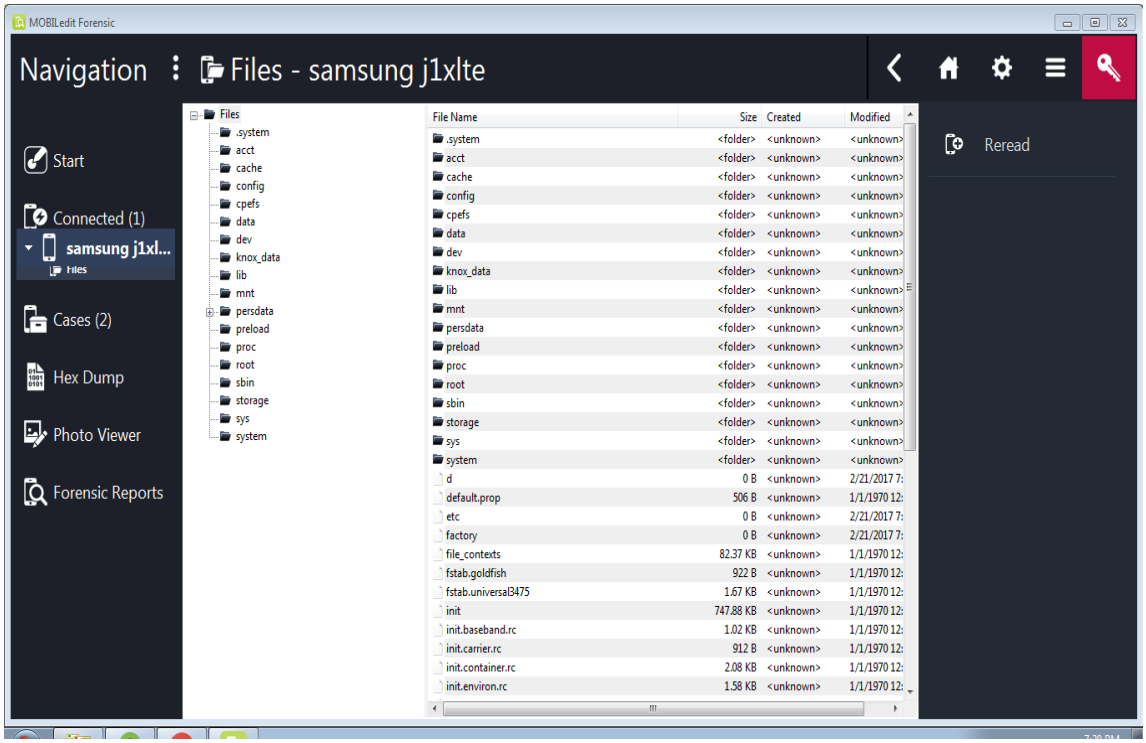
Απεικόνιση της συσκευής

- **MOBILedit Forensic**

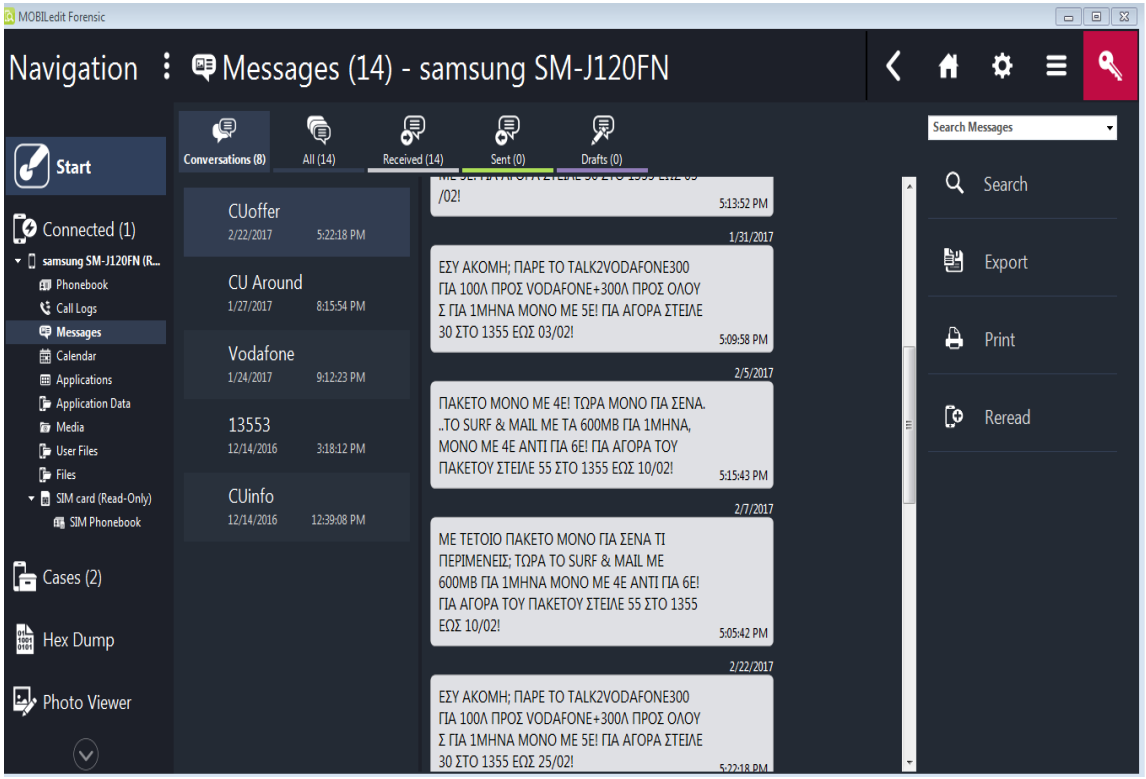
Γραφικό περιβάλλον MOBILedit Forensic



Αποτελέσματα από το εργαλείο MOBILedit Forensic (Εφαρμογές)

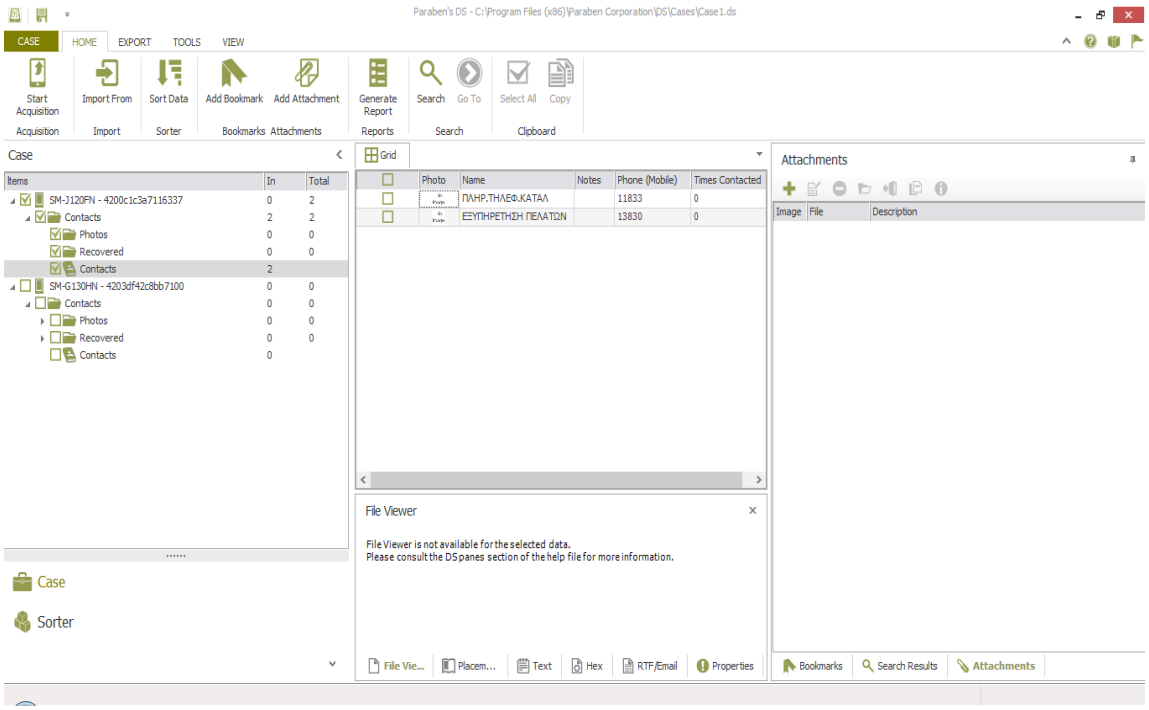


Αποτελέσματα από το εργαλείο MOBILedit Forensic (Αρχεία)



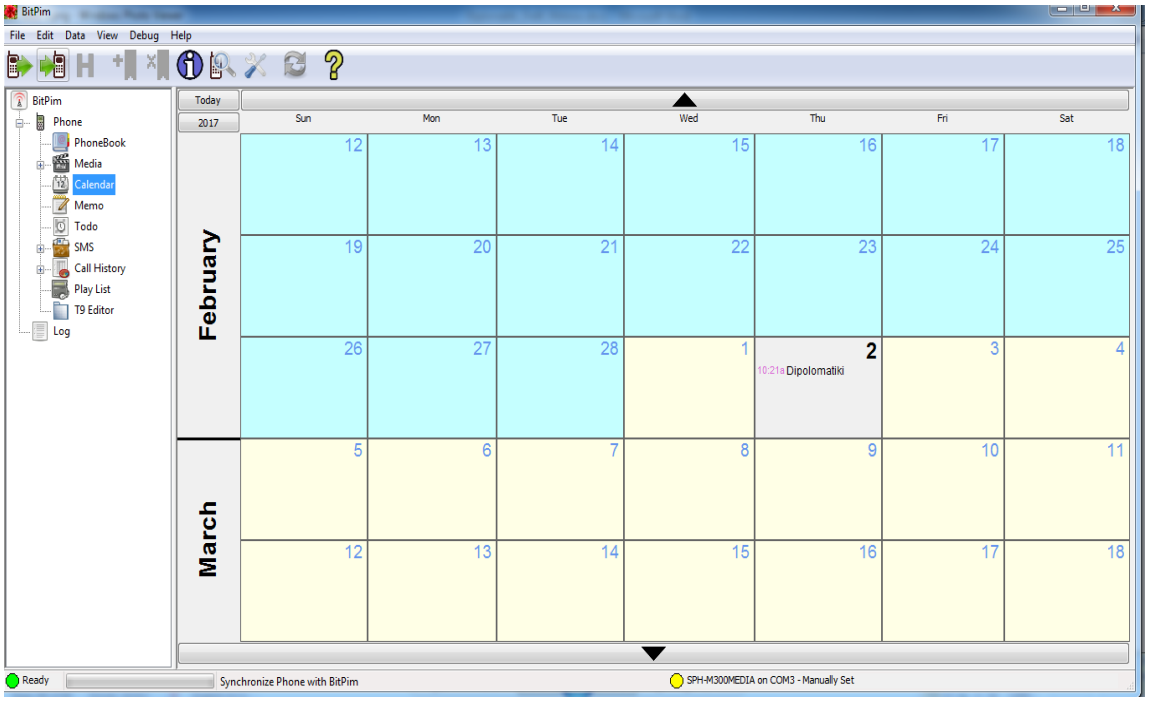
Αποτελέσματα από το εργαλείο MOBILedit Forensic (Μηνύματα)

• Paraben's Device Seizure

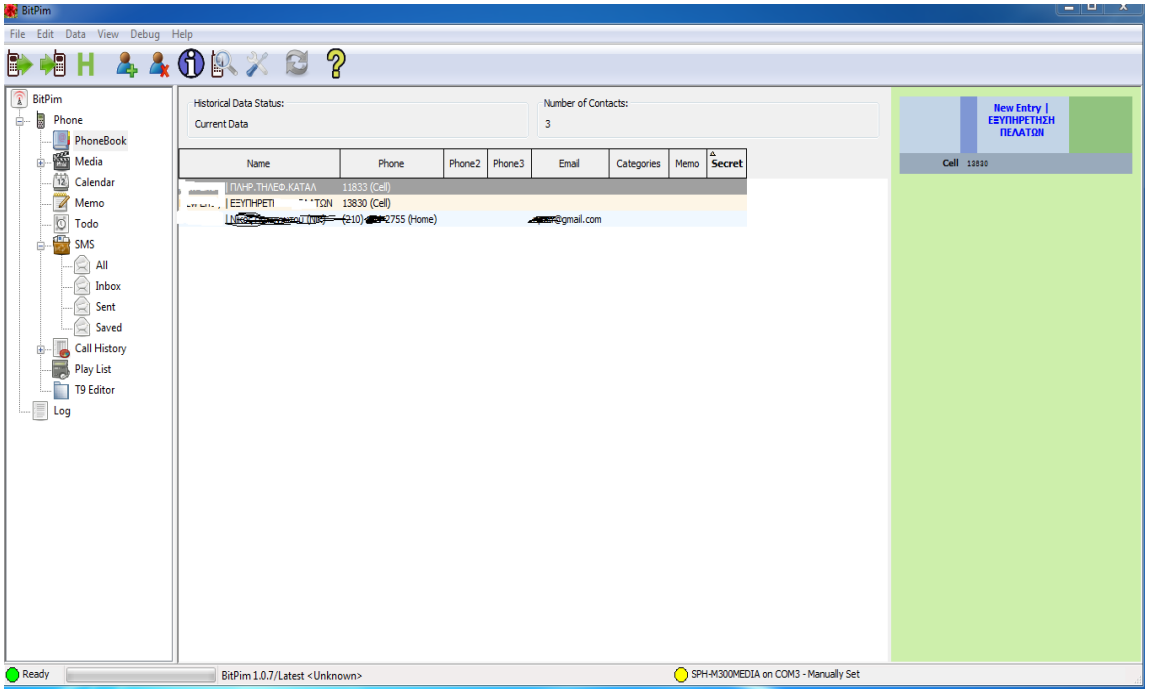


Αποτελέσματα από το εργαλείο Paraben's Device Seizure (Επαφές)

• BitPim



Αποτελέσματα από το εργαλείο BitPim (Ημερολόγιο)



Αποτελέσματα από το εργαλείο BitPim (Επαφές)