Ιούλιος
2018

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τίτλος Μεταπτυχιακής Εργασίας

«Εγκληματολογική Εξέταση Εφαρμογών Bitcoin σε Σύστημα Android»

Σωτήρης Καραπέτσας

Επιβλέπων Καθηγητής: Νταντογιάν Χριστόφορος

Αυτή η σελίδα είναι σκόπιμα κενή

Περιεχόμενα

Εισαγωγή

Με τις πρόσφατες εξελίξεις στις τεχνολογίες της πληροφορίας και της επικοινωνίας και την διαδεδομένη δημοτικότητα των κινητών τηλεφώνων (π.χ. συσκευών Android και iOS), οι ψηφιακές πληρωμές και τα κρυπτονομίσματα όπως το Bitcoin, το Litecoin, το Ethereum και άλλα, γίνονται ολοένα και πιο δημοφιλή στο ηλεκτρονικό εμπόριο.

Οι εγκληματίες - συχνά πρωτοπόροι των νέων τεχνολογιών - εκτίμησαν γρήγορα ότι το Bitcoin ως πρωτοπόρο, αλλά και τα λοιπά κρυπτονομίσματα στη συνέχεια, έχουν μοναδικές ιδιότητες που θα μπορούσαν ενδεχομένως να εξυπηρετήσουν το ενδιαφέρον τους για αποφυγή της επιβολής του νόμου.

Το Bitcoin εισάγει μια σειρά προκλήσεων στις ψηφιακές έρευνες που οφείλονται κυρίως στα στοιχεία της ψευδωνυμίας που παρέχει σε ένα χρήστη και το αποκεντρωμένο δίκτυο μέσα στο οποίο λειτουργεί, όπου με τη χρήση του μπορεί να μεταφερθεί χωρίς μεσάζοντες ακόμη και σε διεθνή σύνορα τόσο εύκολα όσο και η αποστολή ενός μηνύματος ηλεκτρονικού ταχυδρομείου.

Αυτά τα χαρακτηριστικά το έχουν καταστήσει ελκυστικό μέσο ανταλλαγής για όσους ασχολούνται με εγκληματικές δραστηριότητες στο διαδίκτυο. Κατά το παρελθόν έχει χρησιμοποιηθεί για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες και για φοροαποφυγή, ενώ έχει χρησιμοποιηθεί εκτεταμένα για την αγορά παράνομων προϊόντων, αγαθών και υπηρεσιών μέσω διαδικτυακών αγορών, όπως το Silk Road στο Dark Web.

Χρησιμοποιήθηκε και χρησιμοποιείται επιπλέον από επίδοξους χάκερ ως τρόπος πληρωμής για επιθέσεις ransomware που έχουν σημειώσει τεράστια ανάπτυξη κατά τη διάρκεια των τελευταίων χρόνων από την δημιουργία του.

Παρά το γεγονός ότι το Bitcoin αλλά και τα άλλα εικονικά νομίσματα (κρυπτονομίσματα) αποτελούν πηγή αποδεικτικών στοιχείων, έχει υπάρξει περιορισμένη έρευνα στην εγκληματολογική εξέταση τους. Η υπάρχουσα εγκληματολογική έρευνα σχετικά με το Bitcoin επικεντρώνεται κυρίως στο Blockchain (το καθολικό ledger στο οποίο καταγράφονται οι συναλλαγές) και όχι στο Bitcoin, ως λογισμικό του χρήστη (π.χ. την εφαρμογή πορτοφολιού για κινητά τηλέφωνα) προκειμένου να βρεθούν και να ανακτηθούν δεδομένα σχετικά με τις συναλλαγές που έχει πραγματοποιήσει ένας χρήστης χρησιμοποιώντας την συγκεκριμένη εφαρμογή ή και άλλα στοιχεία που σχετίζονται με την συμπεριφορά του χρήστη κατά την χρήση της εφαρμογής πορτοφολιού Bitcoin. Αυτό είναι το κενό που επιδιώκουμε να αντιμετωπίσουμε σε αυτή την εργασία.

Εγκληματολογική εξέταση κινητών συσκευών (Mobile Forensics)

Η εγκληματολογική εξέταση κινητών συσκευών είναι ένα πεδίο γνώσης και πρακτικής που στοχεύει στην εφαρμογή τεχνικών υγιούς εγκληματολογικής εξέτασης για την παροχή υψηλών προδιαγραφών, ποιοτικών, πραγματικών και αυθεντικών αποδεικτικών στοιχείων για μια νομική υπόθεση. Οι υγιείς τεχνικές εγκληματολογικής ανάλυσης αναφέρονται σε τεχνικές που εξασφαλίζουν τον κατάλληλο κώδικα δεοντολογίας κατά τον εντοπισμό, την κατάσχεση, την αποθήκευση, την εξέταση και την ανάλυση των δεδομένων, με αποτέλεσμα τα αποδεικτικά στοιχεία να μπορούν να χρησιμοποιηθούν με επιτυχία σε νομικές υποθέσεις. Λόγω του γεγονότος ότι οι κινητές συσκευές και οι τεχνολογίες γενικά γίνονται ολοένα και πιο ποικίλες και πολύπλοκες, η κινητή ιατροδικαστική είναι ένας συνεχώς αναπτυσσόμενος τομέας σπουδών με συνεχώς βελτιωμένες μεθόδους, εργαλεία και συσκευές.

Οι εγκληματολογικές έρευνες κινητών (και οι ψηφιακές εγκληματολογικές έρευνες εν γένει) μπορούν να χωριστούν σε διάφορες φάσεις:

- Αναγνώριση της στοχευόμενης κινητής συσκευής
- Κατάσχεση και απόκτηση δεδομένων
- Εξέταση και ανάλυση
- Αιτιολόγηση και αναφορά

Κατά τη διάρκεια της έρευνας, όλες οι δραστηριότητες πρέπει να τεκμηριώνονται και τα συγκεντρωμένα στοιχεία πρέπει να αποθηκεύονται σωστά και με ασφάλεια. Υπάρχουν τρεις διαφορετικές προσεγγίσεις για την εξαγωγή και την απόκτηση δεδομένων από κινητά τηλέφωνα, οι οποίες παρουσιάζονται παρακάτω.

Μέθοδοι εξαγωγής και συλλογής ψηφιακών πειστηρίων από κινητές συσκευές Android

Η συλλογή δεδομένων είναι η διαδικασία της απεικόνισης (imaging) ή άλλης συλλογής πληροφοριών από μια ψηφιακή συσκευή. Η απόκτηση δεδομένων από ένα κινητό τηλέφωνο δεν είναι τόσο απλή όσο μια τυποποιημένη εγκληματολογική εξέταση ενός σκληρού δίσκου. Παρακάτω παρουσιάζονται οι τρείς κυρίαρχοι τύποι μεθόδων

εγκληματολογικής εξέτασης κινητών τηλεφώνων που είναι η φυσική, η λογική και η χειροκίνητη μέθοδος. Η ποσότητα και ο τύπος των δεδομένων που μπορούν να συλλεχθούν ποικίλλει ανάλογα με τον τύπο της μεθόδου απόκτησης που χρησιμοποιείται.

Φυσική απόκτηση (Physical acquisition)

Η μέθοδος της φυσικής απόκτησης πραγματοποιείται με τη χρήση εργαλείων και μεθόδων για την παροχή των εγκληματολογικών δεδομένων. Η φυσική εξαγωγή αποκτά πληροφορίες από τη συσκευή με άμεση πρόσβαση στη μνήμη flash, εξ' ου και είναι ο πιο πολύπλοκος τρόπος απόκτησης δεδομένων. Η μνήμη flash είναι μια μη πτητική μνήμη και χρησιμοποιείται κυρίως σε κάρτες μνήμης και μονάδες flash USB ως αποθήκευση σε στερεά κατάσταση. Η διαδικασία δημιουργεί ένα αντίγραφο bit-for-bit ενός ολόκληρου συστήματος αρχείων, παρόμοιο με την προσέγγιση που ακολουθείται στις εγκληματολογικές έρευνες υπολογιστών. Η φυσική απόκτηση είναι σε θέση να αποκτήσει όλα τα δεδομένα που υπάρχουν σε μια συσκευή, συμπεριλαμβανομένων των διαγραμμένων δεδομένων και της πρόσβασης στον μη κατανεμημένο χώρο στις περισσότερες συσκευές. Οι κατασκευαστές κινητών τηλεφώνων ασφαλίζουν συχνά το υλικό τους από την άμεση πρόσβαση, έτσι οι πωλητές εργαλείων ψηφιακής εξέτασης κινητών τηλεφώνων χρησιμοποιούν διάφορες τεχνικές για να παρακάμψουν τους περιορισμούς π.χ. μεταφορτώνοντας τον πυρήνα του δικού τους λειτουργικού συστήματος στη συσκευή.

Λογική απόκτηση (Logical acquisition)

Η λογική απόκτηση των δεδομένων των κινητών τηλεφώνων πραγματοποιείται χρησιμοποιώντας τη διεπαφή προγραμματισμού εφαρμογών του κατασκευαστή της συσκευής για το συγχρονισμό των περιεχομένων του τηλεφώνου με έναν υπολογιστή. Πολλά από τα εγκληματολογικά εργαλεία που υπάρχουν πραγματοποιούν την λογική απόκτηση. Ωστόσο, ο αναλυτής πρέπει να καταλάβει πώς συμβαίνει η απόκτηση και αν το κινητό τροποποιείται κατά οποιονδήποτε τρόπο κατά τη διάρκεια της διαδικασίας. Ανάλογα με το τηλέφωνο και τα εγκληματολογικά εργαλεία που χρησιμοποιούνται, αποκτώνται όλα ή μερικά από τα δεδομένα. Το πλεονέκτημα της προσέγγισης αυτής είναι η απλότητα: τα λογικά αντικείμενα είναι ευκολότερα κατανοητά και η όλη μέθοδος είναι συνήθως λιγότερο χρονοβόρα. Από την άλλη πλευρά, ο εξεταστής δεν θα είναι σε θέση να ανακτήσει τα διαγραμμένα στοιχεία, ενώ στις περισσότερες περιπτώσεις δεν θα γνωρίζει ακόμη και την ύπαρξή τους.

Μη αυτόματη – χειροκίνητη απόκτηση (Manual acquisition)

Για την εγκληματολογική εξέταση των κινητών τηλεφώνων, η φυσική απόκτηση είναι συνήθως η καλύτερη επιλογή και η λογική απόκτηση είναι η δεύτερη καλύτερη επιλογή. Η χειροκίνητη απόκτηση πρέπει να είναι η τελευταία επιλογή κατά την πραγματοποίηση της εγκληματολογικής ανάλυσης κινητού τηλεφώνου. Τόσο η λογική όσο και η χειροκίνητη απόκτηση μπορούν να χρησιμοποιηθούν για την επικύρωση των ευρημάτων στα φυσικά δεδομένα. Κατά τη χειροκίνητη απόκτηση, ο εξεταστής χρησιμοποιεί τη διεπαφή χρήστη για να ερευνήσει τα περιεχόμενα της μνήμης του τηλεφώνου. Η συσκευή χρησιμοποιείται κανονικά μέσω πληκτρολογίου ή οθόνης αφής και πλοήγησης μενού και ο εξεταστής λαμβάνει φωτογραφίες από τα περιεχόμενα κάθε οθόνης. Η χειροκίνητη απόκτηση εισάγει έναν μεγαλύτερο βαθμό κινδύνου υπό τη μορφή ανθρώπινου σφάλματος και υπάρχει η πιθανότητα να διαγραφούν τα αποδεικτικά στοιχεία. Η χειροκίνητη απόκτηση είναι εύκολη στην εκτέλεση και αποκτά μόνο τα δεδομένα που εμφανίζονται σε ένα κινητό τηλέφωνο.

Ανάλυση εφαρμογών κινητών τηλεφώνων

Υπάρχουν χιλιάδες τρόποι με τους οποίους μια εφαρμογή κινητού τηλεφώνου θα μπορούσε να αποθηκεύσει ή να συσκοτίσει (θολώσει) τα δεδομένα της. Διαφορετικές εκδόσεις της ίδιας εφαρμογής θα μπορούσαν ακόμη να αποθηκεύσουν τα ίδια δεδομένα με διαφορετικό τρόπο. Ένας προγραμματιστής κινητών εφαρμογών περιορίζεται μονάχα από την ίδια του την φαντασία (και τους τυχόν περιορισμούς που θέτει το λειτουργικό σύστημα Android), όσον αφορά τον τρόπο που θα επιλέξει για την αποθήκευση των δεδομένων. Ως αποτέλεσμα αυτών των γεγονότων, η ανάλυση μιας εφαρμογής είναι ένας συνεχώς μεταβαλλόμενος στόχος. Οι μέθοδοι που επιλέγει να χρησιμοποιήσει ένας αναλυτής την μία μέρα, μπορεί να είναι εντελώς άσχετες την επόμενη μέρα. Ο τελικός στόχος της υγιούς ανάλυσης μίας εφαρμογής παραμένει σταθερά ο ίδιος, το να κατανοήσουμε για ποιόν λόγο χρησιμοποιήθηκε η εφαρμογή και να βρούμε τα δεδομένα του χρήστη. Επειδή οι εφαρμογές μπορούν και πράγματι αλλάζουν τον τρόπο με τον οποίο αποθηκεύουν τα δεδομένα μέσα από αναβαθμίσεις, δεν υπάρχει κάποιος οριστικός οδηγός για τον τρόπο που αναλύουμε μια εφαρμογή.

Γιατί πραγματοποιούμε ανάλυση των εφαρμογών κινητών τηλεφώνων;

Ακόμα και οι βασικές λειτουργίες τηλεφώνου, όπως οι επαφές, οι κλήσεις και τα μηνύματα (SMS) πραγματοποιούνται με την χρήση εφαρμογών στις Android συσκευές.

Επομένως, ακόμη και η απόκτηση βασικών δεδομένων απαιτεί την ανάλυση μιας εφαρμογής. Επιπλέον, η χρήση μιας εφαρμογής από κάποιον, μπορεί να μας φανερώσει πολλά στοιχεία σχετικά με αυτό το άτομο: που βρισκόταν κάποια δεδομένη χρονική στιγμή, με ποιόν επικοινώνησε αλλά ακόμη και σχετικά με το τι σχεδιάζει να κάνει στο μέλλον.

Αρκετές συσκευές κινητών τηλεφώνων έρχονται με προ-εγκατεστημένες εφαρμογές που μπορεί να υπερβαίνουν τις 10, ενώ ένας χρήστης μπορεί να έχει κατά μέσο όρο 100 εφαρμογές εγκατεστημένες στο κινητό του τηλέφωνο. Ένας αναλυτής δεν μπορεί με κάποιον τρόπο να γνωρίζει ποιές από αυτές τις εφαρμογές θα μπορούσαν να περιέχουν πληροφορίες χρήσιμες για την έρευνα και επομένως όλες αυτές θα πρέπει να αναλυθούν. Ο αναλυτής ίσως μπει στον πειρασμό να παρακάμψει ορισμένες εφαρμογές που φαίνεται να μην έχουν σημαντικά δεδομένα, όπως είναι τα παιχνίδια, όμως ένα χαρακτηριστικό όπως αυτό της ενσωματωμένης λειτουργίας ανταλλαγής μηνυμάτων που έχουν πολλά παιχνίδια, θα μπορούσε να φανερώσει πολλές χρήσιμες πληροφορίες.

Η ανάλυση που θα πραγματοποιήσουμε στην παρούσα εργασία επικεντρώνεται στις εφαρμογές Bitcoin πορτοφολιών, ενός ηλεκτρονικού συστήματος πληρωμών, που τείνει να αποκτά όλο και περισσότερη απήχηση στο ευρύ κοινό, αλλά και σε εγκληματίες του κυβερνοχώρου ενώ παρουσιάζει ιδιαίτερο ενδιαφέρον από την πλευρά της εγκληματολογικής ανάλυσης.

Bitcoin

Πριν προχωρήσουμε στην ψηφιακή εξέταση ορισμένων εκ των δημοφιλέστερων εφαρμογών πορτοφολιών Bitcoin που υπάρχουν διαθέσιμες στο Play Store της Google, στις παρακάτω παραγράφους θα αναφέρουμε λίγα λόγια για το Bitcoin και για τα είδη πορτοφολιών που υπάρχουν για την αποθήκευσή του.

Τι είναι το Bitcoin

Το Bitcoin, όπως το περιγράφει ο δημιουργός του στην “Λευκή Βίβλο” που εξέδωσε το έτος 2008, είναι ένα peer-to-peer ηλεκτρονικό σύστημα μετρητών (Bitcoin: A Peer-to-peer Electronic Cash System). Σύμφωνα λοιπόν με αυτή την βίβλο, το Bitcoin είναι το πρώτο αποκεντρωμένο ηλεκτρονικό σύστημα μετρητών, καθώς λειτουργεί χωρίς κάποια κεντρική αρχή ελέγχου ή κάποιον διαχειριστή. Το σύστημα σχεδιάστηκε να λειτουργεί ως ένα δίκτυο

μεταξύ ομότιμων (peer-to-peer), στο οποίο οι συναλλαγές λαμβάνουν χώρα απευθείας μεταξύ των χρηστών, χωρίς κανέναν ενδιάμεσο.

Τα bitcoin δημιουργούνται μέσω μιας διαδικασίας που ονομάζεται «εξόρυξη» (mining), η οποία αφορά τον ανταγωνισμό για εύρεση λύσεων σε ένα μαθηματικό πρόβλημα κατά την επεξεργασία των συναλλαγών bitcoin. Κάθε συμμετέχων στο δίκτυο Bitcoin (ο καθένας δηλαδή με τη χρήση μιας συσκευής που τρέχει τη πλήρη στοίβα πρωτοκόλλου Bitcoin) μπορεί να λειτουργήσει ως εξορύκτης (miner), χρησιμοποιώντας την επεξεργαστική ισχύ του υπολογιστή [1] του για να επαληθεύει και να καταγραφεί τις συναλλαγές.

Κάθε 10 λεπτά κατά μέσο ορό, είναι σε θέση κάποιος να επικυρώσει τις συναλλαγές των τελευταίων 10 λεπτών και να ανταμειφτεί με ολοκαίνουργια bitcoin. Το πρωτόκολλο Bitcoin περιλαμβάνει ενσωματωμένους αλγορίθμους που ρυθμίζουν τη λειτουργιά της εξόρυξης σε όλο το δίκτυο. Η δυσκολία του επεξεργαστικού εγχειρήματος που οι εξορυχτείς “miners” πρέπει να εκτελέσουν - με σκοπό την επιτυχή καταγραφή ενός μπλοκ συναλλαγών στο Bitcoin δίκτυο - ρυθμίζεται δυναμικά έτσι ώστε, κατά μέσο ορό, κάποιος να τα καταφέρνει κάθε 10 λεπτά ανεξάρτητα από το πόσο πολλοί εξορυχτείς εργάζονται κάθε στιγμή στη συγκεκριμένη αποστολή. Το πρωτόκολλο επίσης μειώνει στο μισό, κάθε τέσσερα χρόνια, το ρυθμό με τον όποιο τα νέα bitcoin δημιουργούνται, ενώ ταυτόχρονα περιορίζει τον συνολικό αριθμό των bitcoin που θα δημιουργηθούν σε συνολικά 21 εκατομμύρια νομίσματα. Το αποτέλεσμα είναι ότι ο αριθμός των bitcoin σε κυκλοφορία ακόλουθοι πίστα μια εύκολα προβλέψιμη καμπύλη που φτάνει τα 21 εκατομμύρια μέχρι το έτος 2140.

Στην επιστήμη της πληροφορικής, το Bitcoin είναι επίσης το όνομα του πρωτοκόλλου, ένα δίκτυο και μια καινοτομία στα κατανεμημένα υπολογιστικά συστήματα. Είναι ανοιχτού κώδικα (https://github.com/bitcoin/bitcoin), ενώ ο σχεδιασμός του είναι δημόσιος και οποιοσδήποτε προγραμματιστής μπορεί να συνεισφέρει στην ανάπτυξή του.

[1] Η επεξεργαστική ισχύς του υπολογιστή και οι κάρτες γραφικών για mining χρησιμοποιήθηκαν τα πρώτα χρόνια λειτουργίας του Bitcoin. Η αύξηση της δυσκολίας του συστήματος για την παραγωγή καινούριων bitcoin δημιούργησε την ανάγκη για την δημιουργία ολοκληρωμένων κυκλωμάτων εξειδικευμένης χρήσης αποκλειστικά για mining, τα επονομαζόμενα ASIC (Application-Specific Integrated Circuit) και έτσι από το 2013 έως σήμερα το η εξόρυξη νέων bitcoin γίνεται μόνο με ASIC μηχανήματα.

Η ιστορία του Bitcoin

Το Bitcoin επινοήθηκε το 2008 με τη δημοσίευση ενός εγγράφου με τίτλο «Bitcoin: Ένα peer-to-peer ηλεκτρονικό σύστημα μετρητών» (Bitcoin: A Peer-to-Peer Electronic Cash System), γραμμένο με το ψευδώνυμο Σατόσι Νακαμότο (Satoshi Nakamoto). Αποτελεί το

αποκορύφωμα έρευνας στην κρυπτογραφία και τα κατανεμημένα συστήματα, οι οποίες συνδυάστηκαν από τον Satoshi Nakamoto δημιουργώντας ένα σύστημα, με σχεδιασμό πλήρως αποκεντρωμένο, χωρίς καμιά κεντρική αρχή η κεντρικό σημείο έλεγχου που μπορεί να δηχθεί επίθεση η να διαβληθεί.

Η κυρία καινοτομία του ήταν η χρησιμοποίηση ενός κατανεμημένου υπολογιστικού συστήματος (που ονομάζεται αλγόριθμος απόδειξης εργασίας (proof-of-work algorithm)) για να διεξάγεται μια παγκοσμία «εκλογική διαδικασία» κάθε 10 λεπτά, επιτρέποντας το αποκεντρωμένο δίκτυο να καταλήγει σε συναίνεση (consensus) σχετικά με την κατάσταση των συναλλαγών. Αυτό λύνει κομψά το πρόβλημα του διπλό - ξοδέματος (double - spent), όπου μια νομισματική μονάδα μπορεί να δαπανηθεί δύο φορές. Προηγουμένως, το διπλό - ξόδεμα ήταν μια αδυναμία των ψηφιακών νομισμάτων και η επίλυση του γινόταν με την εκκαθάριση όλων των συναλλαγών μέσω ενός κεντρικού γραφείου εκκαθαρίσεως.

Ο Satoshi Nakamoto αποσύρθηκε από τα κοινά τον Απρίλιο του 2011, αφήνοντας την ευθύνη ανάπτυξης του κώδικα και του δικτύου σε μια ακμάζουσα ομάδα εθελοντών. Η ταυτότητα του ατόμου ή των ανθρώπων πίσω από το Bitcoin είναι ακόμα άγνωστη. Ωστόσο, ούτε ο Satoshi Nakamoto ούτε οποιοσδήποτε άλλος ασκεί έλεγχο στο σύστημα του Bitcoin, το όποιο λειτουργεί με βάση απολυτά διαφανείς μαθηματικές αρχές. Η εφεύρεση από μόνη της είναι πρωτοποριακή και έχει ήδη γεννήσει νέα πεδία γνώσης στην επιστήμη των κατανεμημένων συστημάτων πληροφορικής, την οικονομία και την οικονομετρία.

Αποθήκευση των bitcoin - ψηφιακά πορτοφόλια

Σε αντίθεση με τα παραδοσιακά νομίσματα, τα bitcoin είναι εξ' ολόκληρου εικονικά. Δεν υπάρχουν φυσικά κέρματα η ακόμη και τα ψηφιακά νομίσματα αυτά καθαυτά. Τα νομίσματα υπονοείται στις συναλλαγές ότι μεταφέρουν αξία από τον αποστολέα στον παραλήπτη. Οι χρηστές του Bitcoin κατέχουν κλειδιά, με τα οποία τους επιτρέπεται να αποδεικνύουν την κυριότητα των συναλλαγών στο δίκτυο Bitcoin, ξεκλειδώνοντας την αξία για να τη ξοδεύουν και να τη μεταφέρουν σε νέο παραλήπτη. Ως εκ τούτου, ο καθένας με ένα αντίγραφο αυτών των κλειδιών έχει και τον έλεγχο των bitcoin του εν λογγό λογαριασμού. Τα κλειδιά έρχονται σε ζεύγη και αποτελούνται από ένα ιδιωτικό (μυστικό) κλειδί και ένα δημόσιο κλειδί, βρίσκονται σπάνια στη θέα των χρηστών του Bitcoin, ενώ τις περισσότερες φορές αποθηκεύονται μέσα στο αρχείο του πορτοφολιού και η διαχείριση τους γίνεται από το λογισμικό Bitcoin πορτοφόλι. Η κατοχή του ιδιωτικού κλειδιού που ξεκλειδώνει μια συναλλαγή είναι η μόνη προϋπόθεση για το ξόδεμα bitcoin, βάζοντας με αυτό τον τρόπο τον απολυτό έλεγχο στα χέρια του κάθε χρηστή. Με το πέρασμα των χρόνων από τη δημιουργία

του Bitcoin έχουν δημιουργηθεί διαφόρων ειδών εφαρμογές πορτοφόλια για την αποθήκευση των κλειδιών του χρήστη τόσο σε λογισμικό για υπολογιστές, όσο και για κινητά τηλέφωνα ή web εφαρμογές.

Η ανάπτυξη εφαρμογών πορτοφολιών Bitcoin βρίσκεται σε άνθιση, ενώ υπάρχει έντονος ανταγωνισμός από καινούριες εφαρμογές πορτοφόλια που αναπτύσσονται με ταχύτατους ρυθμούς από διάφορες εταιρείες. Πολλά πορτοφόλια επικεντρώνονται σε συγκεκριμένες πλατφόρμες ή συγκεκριμένες χρήσεις και μερικά είναι πιο κατάλληλα για αρχάριους ενώ άλλα είναι γεμάτα με δυνατότητες για προχωρημένους χρήστες. Η επιλογή ενός πορτοφολιού είναι εξαιρετικά υποκειμενική και εξαρτάται από την εμπειρία του χρήστη.

Κατηγοριοποίηση πορτοφολιών με βάση την πλατφόρμα

Τα πορτοφόλια αναλόγως της πλατφόρμας που μπορεί να χρησιμοποιηθεί, μπορούν να κατηγοριοποιηθούν ως εξής:

Επιτραπέζιο πορτοφόλι (Desktop wallet)

Το πορτοφόλι για επιτραπέζιους υπολογιστές ήταν ο πρώτος τύπος πορτοφολιού Bitcoin που δημιουργήθηκε ως εφαρμογή αναφοράς και πολλοί χρήστες τρέχουν τέτοιου είδους πορτοφόλια για τα χαρακτηριστικά, την αυτονομία και τον έλεγχο που προσφέρουν. Η λειτουργία σε λειτουργικά συστήματα γενικής χρήσης, όπως τα Windows και το Mac OS, παρουσιάζει ορισμένα μειονεκτήματα ασφαλείας, καθώς αυτές οι πλατφόρμες είναι συχνά ανασφαλείς και δεν έχουν ρυθμιστεί σωστά.

Κινητό πορτοφόλι (Mobile wallet)

Ένα κινητό πορτοφόλι είναι ο πιο συνηθισμένος τύπος πορτοφολιού Bitcoin. Λειτουργώντας σε λειτουργικά συστήματα έξυπνων τηλεφώνων, όπως το Apple iOS και το Android, αυτά τα πορτοφόλια αποτελούν συχνά μια εξαιρετική επιλογή για νέους χρήστες. Πολλά έχουν σχεδιαστεί για απλότητα και ευκολία στη χρήση, αλλά υπάρχουν επίσης πλήρως εξοπλισμένα πορτοφόλια για τους προχωρημένους χρήστες.

Διαδικτυακό πορτοφόλι (Web wallet)

Τα διαδικτυακά πορτοφόλια έχουν πρόσβαση μέσω ενός προγράμματος περιήγησης ιστού και αποθηκεύουν το πορτοφόλι του χρήστη σε ένα διακομιστή που ανήκει σε τρίτο μέρος.

Υλικό πορτοφόλι (Hardware wallet)

Τα πορτοφόλια υλικού είναι συσκευές που λειτουργούν με ένα ασφαλές αυτόνομο πορτοφόλι Bitcoin σε υλικό ειδικού σκοπού. Διακινούνται μέσω USB με ένα πρόγραμμα περιήγησης ιστού ή μέσω του πρωτοκόλλου επικοινωνίας (NFC) σε μια κινητή συσκευή. Χειρίζοντας όλες τις λειτουργίες που σχετίζονται με το Bitcoin στο εξειδικευμένο υλικό, ενώ θεωρούνται πολύ ασφαλή και κατάλληλα για την αποθήκευση μεγάλων ποσοτήτων bitcoin.

Χάρτινο πορτοφόλι (Paper wallet)

Τα κλειδιά του Bitcoin μπορούν επίσης να εκτυπωθούν για μακροχρόνια αποθήκευση. Αυτός ο τρόπος αποθήκευσης των bitcoin είναι γνωστός ως χάρτινο πορτοφόλι παρόλο που μπορούν να χρησιμοποιηθούν και άλλα υλικά (ξύλο, μέταλλο κ.λπ.). Τα πορτοφόλια χαρτιού προσφέρουν ένα χαμηλής τεχνολογίας, αλλά εξαιρετικά ασφαλές μέσο αποθήκευσης των bitcoin μακροπρόθεσμα.

Κατηγοριοποίηση πορτοφολιών με βάση την αλληλεπίδρασή τους με το δίκτυο

Ένας άλλος τρόπος κατηγοριοποίησης των πορτοφολιών Bitcoin είναι ο βαθμός αυτονομίας τους και ο τρόπος αλληλεπίδρασης τους με το δίκτυο Bitcoin.

Πλήρης - κόμβος πελάτης (Full - node client)

Ο πλήρης πελάτης ή ο "πλήρης κόμβος" είναι ένας πελάτης που αποθηκεύει ολόκληρο το ιστορικό των συναλλαγών Bitcoin (κάθε συναλλαγή από κάθε χρήστη από την αρχή), έχει λειτουργίες για την δημιουργία και διαχείριση του πορτοφολιού για τους χρήστες και μπορεί να πραγματοποιεί συναλλαγές απευθείας στο δίκτυο Bitcoin. Ένας πλήρης κόμβος χειρίζεται όλες τις πτυχές του πρωτοκόλλου και μπορεί ανεξάρτητα να επικυρώσει ολόκληρο το blockchain και κάθε συναλλαγή. [2]

Ελαφρύς πελάτης (Lightweight client)

Ένας ελαφρύς πελάτης, γνωστός και ως πελάτης απλής πληρωμής - επαλήθευσης (SPV | Simple-Payment-Verification), συνδέεται με τους πλήρεις κόμβους Bitcoin για πρόσβαση στις πληροφορίες συναλλαγής Bitcoin, αλλά αποθηκεύει το πορτοφόλι του χρήστη τοπικά και ανεξάρτητα δημιουργεί, επικυρώνει και μεταδίδει συναλλαγές. Οι ελαφροί πελάτες αλληλεπιδρούν άμεσα με το δίκτυο Bitcoin, χωρίς μεσάζοντα.

Πελάτης API τρίτου μέρους (Third - party API client)

Ένας πελάτης API τρίτου μέρους είναι αυτός που αλληλεπιδρά με το Bitcoin μέσω ενός συστήματος τρίτων συμβαλλόμενων μερών (APIs), αντί να συνδεθεί απευθείας στο δίκτυο Bitcoin. Το πορτοφόλι μπορεί να αποθηκευτεί από το χρήστη ή από διακομιστές τρίτων, αλλά όλες οι συναλλαγές περνούν από το τρίτο μέρος.

[2] Ένας πελάτης πλήρους κόμβου καταναλώνει σημαντικούς πόρους υπολογιστή (π.χ. περισσότερα από 165 GB δίσκου, 2 GB μνήμης RAM), αλλά προσφέρει πλήρη αυτονομία και ανεξάρτητη επαλήθευση συναλλαγών.

Είδη Bitcoin πορτοφολιών

Όπως αναφέραμε και προηγουμένως ένα Bitcoin πορτοφόλι δεν περιέχει bitcoin, αλλά περιέχει μόνο τα κλειδιά του χρήστη. Οι χρήστες ελέγχουν τα νομίσματα στο δίκτυο υπογράφοντας συναλλαγές χρησιμοποιώντας τα κλειδιά των πορτοφολιών τους.

Υπάρχουν δύο κυρίαρχοι τύποι πορτοφολιών που διακρίνονται από το αν τα κλειδιά που περιέχουν σχετίζονται μεταξύ τους ή όχι.

Ο πρώτος τύπος είναι ένα μη ντερερμινιστικό πορτοφόλι, όπου το κάθε κλειδί δημιουργείται ανεξάρτητα από έναν τυχαίο αριθμό. Τα κλειδιά σε αυτό τον τύπο πορτοφολιού δεν σχετίζονται μεταξύ τους.

Ο δεύτερος τύπος είναι το ντετερμινιστικό πορτοφόλι, όπου όλα τα κλειδιά προέρχονται από ένα μοναδικό αντικλείδι (master key) γνωστό και ως πηγή (seed). Όλα τα κλειδιά σε αυτό το είδος πορτοφολιού είναι σχετιζόμενα μεταξύ τους και μπορούν να δημιουργηθούν ξανά, αν κάποιος κατέχει την αρχική πηγή (seed).

Μη-ντετερμινιστικά (τυχαία) πορτοφόλια

Αυτός ο τύπος πορτοφολιού έχει το προσωνύμιο «Just a Bunch Of Keys» ή JBOK και έχει αντικατασταθεί από ντετερμινιστικά πορτοφόλια, επειδή είναι δυσκίνητος και δύσχρηστος στη δημιουργία αντιγραφών ασφαλείας και στην εισαγωγή. Το μειονέκτημα των τυχαίων κλειδιών είναι ότι εάν έχετε δημιουργήσει πολλά από αυτά, θα πρέπει να κρατήσετε αντίγραφα από όλα, πράγμα που σημαίνει ότι το πορτοφόλι πρέπει να γίνεται συχνά backup. Πρέπει να γίνεται αντίγραφο ασφαλείας για κάθε ξεχωριστό κλειδί, αλλιώς τα bitcoin που είναι υπό τον έλεγχο του σε περίπτωση που χαθεί με κάποιο τρόπο η πρόσβαση στο πορτοφόλι χάνονται οριστικά.

Ντετερμινιστικά πορτοφόλια - από πηγή (seeded)

Τα ντετερμινιστικά η αλλιώς πορτοφόλια από πηγή (seeded), είναι τα πορτοφόλια που περιέχουν ιδιωτικά κλειδιά, τα οποία προέρχονται όλα από μια κοινή πηγή (seed) μέσω της χρήσης μιας μονόδρομης συνάρτησης κατακερματισμού. Σε ένα ντετερμινιστικό πορτοφόλι, ο αριθμός της πηγής είναι αρκετός για την ανάκτηση όλων των κλειδιών που έχουν παραχθεί από αυτόν και ως εκ τούτου ένα και μονό αντίγραφο ασφαλείας τη στιγμή της δημιουργίας του μας επαρκεί. Η πηγή είναι επίσης αποτελεσματική για εξαγωγή η εισαγωγή πορτοφολιών, επιτρέποντας την εύκολη μετακίνηση όλων των κλειδιών του χρηστή μεταξύ των διάφορων υλοποιήσεων πορτοφολιών.

Μνημονικός κωδικός λέξεων

Οι μνημονικοί κωδικοί (mnemonic codes) είναι ακολουθίες αγγλικών λέξεων που αντιπροσωπεύουν (κωδικοποιούν) έναν τυχαίο αριθμό που χρησιμοποιείται ως πηγή για να δημιουργήσει ένα ντετερμινιστικό πορτοφόλι. Η ακολουθία των λέξεων είναι επαρκής για να δημιουργήσει ξανά την πηγή και από εκεί να δημιουργήσει ξανά το πορτοφόλι και όλα τα παράγωγα κλειδιά. Μια εφαρμογή που υλοποιεί ντετερμινιστικά πορτοφόλια με μνημονικό κωδικό θα δείξει στο χρηστή μια σειρά από 12 έως 24 λέξεις κατά τη πρώτη δημιουργία του πορτοφολιού. Αυτή η ακολουθία των λέξεων είναι το αντίγραφο ασφαλείας του πορτοφολιού και μπορεί να χρησιμοποιηθεί για την ανάκτηση και τη δημιουργία ξανά όλων των κλειδιών στην ιδία η σε οποιαδήποτε άλλη συμβατή εφαρμογή πορτοφολιού. Ο μνημονικός κωδικός λέξεων κάνει πιο εύκολη για τους χρηστές τη δημιουργία αντιγράφου ασφαλείας στα πορτοφόλια, επειδή σε σύγκριση με μια τυχαία ακολουθία αριθμών είναι ευκολότερος να διαβαστεί και να αντιγράφει σωστά.

Ιεραρχικά ντετερμινιστικά πορτοφόλια (hierarchical deterministic wallets)

Τα ντετερμινιστικά πορτοφόλια αναπτυχτήκαν ώστε να είναι εύκολη η άντληση πολλών κλειδιών από μια ενιαία «πηγή» (seed). Η πιο προηγμένη μορφή ντετερμινιστικών πορτοφολιών είναι το ιεραρχικό ντετερμινιστικό πορτοφόλι (hierarchical deterministic wallet) ή πορτοφόλι HD. Τα ιεραρχικά ντετερμινιστικά πορτοφόλια περιέχουν κλειδιά που προκύπτουν σε μια δενδροειδή δομή δεδομένων (tree structure), έτσι ώστε το μητρικό (parent) κλειδί να μπορεί να δημιουργήσει μια ακολουθία κλειδιών παιδικών (children), καθένα από τα οποία μπορεί να δημιουργήσει μια ακολουθία ν-παιδικών (grandchildren) κλειδιών και ούτω καθεξής, σε μια άπειρη κλίμακα.

Χάρτινα πορτοφόλια (paper wallets)

Τα χάρτινα πορτοφόλια είναι η προβολή των ιδιωτικών κλειδιών του Bitcoin σε έντυπη μορφή. Το χάρτινο πορτοφόλι, συχνά, περιλαμβάνει και την αντίστοιχη διεύθυνση bitcoin για λογούς ευκολίας, αλλά αυτό δεν είναι αναγκαίο, καθώς μπορεί να παραχθεί από το ιδιωτικό κλειδί. Τα χάρτινα πορτοφόλια είναι ένας πολύ αποτελεσματικός τρόπος δημιουργίας αντιγράφων ασφαλείας ή αποθήκευσης των bitcoin έκτος σύνδεσης, γνωστό και ως «cold storage» (αποθήκευση έκτος υπολογιστή). Ως ένας μηχανισμός αντιγραφών ασφαλείας, ένα χάρτινο πορτοφόλι μπορεί να παράσχει ασφάλεια έναντι της απώλειας των κλειδιών που μπορεί να οφείλεται σε κάποια δυσλειτουργία του υπολογιστή, όπως καταστροφή σκληρού δίσκου, κλοπή η κατά λάθος διαγράφη. Ως ένας μηχανισμός «αποθήκευσης έκτος υπολογιστή», τα κλειδιά στα χάρτινα πορτοφόλια παράγονται έκτος σύνδεσης και δεν αποθηκεύονται ποτέ σε κάποιο υπολογιστικό σύστημα, είναι πολύ πιο ασφαλή απέναντι σε χάκερ, key-logger και άλλες ηλεκτρονικές απειλές του υπολογιστή.

Εγκληματολογική Ανάλυση Εφαρμογών πορτοφολιών Bitcoin σε κινητό Android με την μέθοδο της λογικής απόκτησης

Δημιουργία του περιβάλλοντος εγκληματολογικής ανάλυσης

Είναι ζωτικής σημασίας να δημιουργηθεί το κατάλληλο περιβάλλον πριν την εγκληματολογική ανάλυση ενός κινητού τηλεφώνου. Με τον όρο κατάλληλο περιβάλλον εννοούμε την επιλογή του κατάλληλου λογισμικού στον υπολογιστή που θα δουλέψουμε καθώς και την εγκατάσταση των προγραμμάτων που θα χρησιμοποιήσουμε κατά την ανάλυσή μας.

Για την εγκληματολογική ανάλυση των εφαρμογών που παρουσιάζονται στη συνέχεια, χρησιμοποιήσαμε μια εικονική μηχανή (virtual machine) με εγκατεστημένο το λογισμικό Linux Ubuntu έκδοσης 16.04 LTS, στο οποίο είχαμε εγκαταστήσει τα απαραίτητα προγράμματα για την εξερεύνηση των αρχείων, όπως θα δούμε στη συνέχεια.

Για την εκτέλεση των δοκιμών χρησιμοποιήσαμε ένα κινητό τηλέφωνο μάρκας OnePlus 3 με εγκατεστημένη την έκδοση Android 6.0.1. Το κινητό τηλέφωνο είχε πλήρη δικαιώματα διαχειριστή (root) ενώ δεν είχε κάποιον κωδικό κλειδώματος της οθόνης. Στο κινητό τηλέφωνο έγινε εγκατάσταση των εφαρμογών που παρουσιάζονται στη συνέχεια και για κάποιο χρονικό διάστημα έγινε χρήση των εφαρμογών πραγματοποιώντας συναλλαγές με Bitcoin.

Όλες οι εφαρμογές που εξετάζονται στη συνέχεια αποτελούν πορτοφόλια ελαφρύ πελάτη ή αλλιώς SPV πορτοφόλια, καθώς η επιλογή του πλήρη κόμβου σε εφαρμογή για κινητά τηλέφωνα δεν υπάρχει (ακόμη τουλάχιστον) διότι απαιτεί μεγάλο αποθηκευτικό χώρο.

Σημείωση: *Παρότι κάναμε προσπάθεια να είμαστε εξονυχιστικοί στην χρήση κάθε εφαρμογής κατά την διαδικασία δημιουργίας δεδομένων από την χρήση τους, είναι πολύ πιθανόν να μην έχει χρησιμοποιηθεί κάθε χαρακτηριστικό της εφαρμογής. Επιπρόσθετα, η ανάλυση των δεδομένων που πραγματοποιήθηκε μπορεί να μην περιλαμβάνει κάθε δυνατό κομμάτι δεδομένων που θα μπορούσε να ανακτηθεί. Στις περισσότερες από τις εφαρμογές που εξετάζουμε στη συνέχεια, κατά την προγενέστερη χρήση τους χρησιμοποιήσαμε τις προεπιλεγμένες ρυθμίσεις ή με ελάχιστες αλλαγές των προεπιλεγμένων ρυθμίσεων.*

Εφαρμογή Copay Bitcoin Wallet

Εγκατάσταση της εφαρμογής Copay Bitcoin Wallet

Η εφαρμογή βρίσκεται στο Play Store και την στιγμή των δοκιμών βρισκόταν στην έκδοση 4.4.0. Σύμφωνα με τους δημιουργούς της, το Copay είναι ελεύθερο και ανοικτού κώδικα λογισμικό και ο πηγαίος κώδικάς του βρίσκεται στο GitHub στον σύνδεσμο https://github.com/bitpay/copay. Υποστηρίζει την δημιουργία και διαχείριση πολλών πορτοφολιών, ενώ ακολουθεί την ντετερμινιστική ιεραρχική δημιουργία διευθύνσεων bitcoin, είναι δηλαδή ένα Hierarchical Deterministic Wallet (HD). Η εφαρμογή είναι αρκετά

δημοφιλής στο Play Store και έχει περίπου 100.000+ λήψεις σύμφωνα με τα στοιχεία της Google.

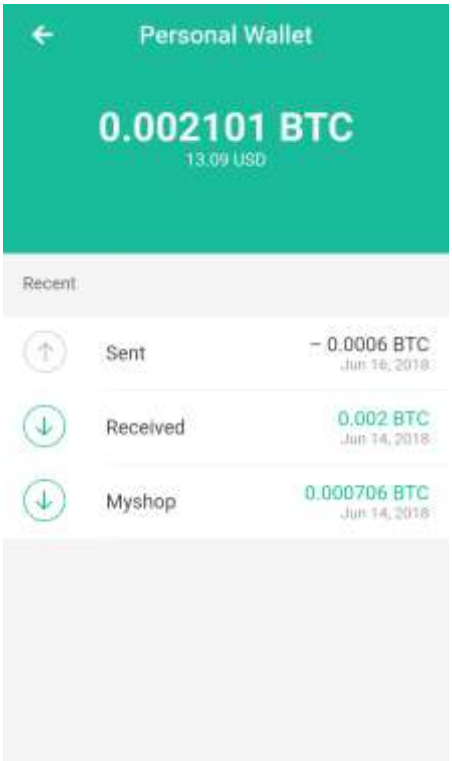
Κατά την είσοδο στην εφαρμογή δίνεται η επιλογή της δημιουργίας καινούριου πορτοφολιού και η επαναφορά πορτοφολιού από backup. Συνεχίζοντας με την δημιουργία νέου πορτοφολιού δίνεται η δυνατότητα κρυπτογράφησης του πορτοφολιού με κωδικό για την προστασία του σε περίπτωση κλοπής ή κακόβουλου λογισμικού. Ωστόσο, υπάρχει η δυνατότητα της μη επιλογής κωδικού, πράγμα που επιλέχθηκε κατά την δοκιμή μας. Η εφαρμογή στη συνέχεια μας προτρέπει να δημιουργήσουμε backup για την προστασία των χρημάτων μας. Επιλέγοντας να κάνουμε backup εμφανίζεται η παρακάτω εικόνα (Στιγμιότυπο 1) από την οποία πρέπει να αντιγράψουμε προσεχτικά τις λέξεις που εμφανίζονται στην οθόνη και να τις φυλάξουμε σε ασφαλές μέρος ώστε να διατηρήσουμε τα χρήματά μας ασφαλή αν χρειαστεί να επαναφέρουμε το πορτοφόλι, σε οποιαδήποτε περίπτωση.

Στιγμιότυπο 1 - Δημιουργία νέου πορτοφολιού και Backup - Copay

Στην επόμενη εικόνα (Στιγμιότυπο 2) παρατηρούμε ότι το πορτοφόλι μας έχει δημιουργηθεί με όνομα “Personal Wallet”, ενώ η εφαρμογή μας εμφανίζει και μια διεύθυνση bitcoin στην οποία μπορούμε να στείλουμε χρήματα.

Στιγμιότυπο 2 - Διεύθυνση λήψης bitcoin - Personal Wallet - Copay

Κάνοντας χρήση της εφαρμογής πραγματοποιούμε δύο λήψεις bitcoin καθώς και μια αποστολή και το πορτοφόλι μας στο τέλος έχει κάποιο υπόλοιπο, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 3).



Στιγμιότυπο 3 - Συναλλαγές και υπόλοιπο πορτοφολιού Personal Wallet - Copay

Εγκληματολογική εξέταση της εφαρμογής - Copay Bitcoin Wallet

Για την εγκληματολογική εξέταση της εφαρμογής, θα χρησιμοποιήσουμε την λογική μέθοδο απόκτησης, κάνοντας χρήση του εργαλείου της γέφυρας εντοπισμού σφαλμάτων του Android (Android Debug Bridge) ή ADB εν συντομία, όπως θα το αποκαλούμε στη συνέχεια.

Το όνομα του πακέτου εγκατάστασης της εφαρμογής είναι το “com.bitpay.copay” και κατά την εγκατάσταση η εφαρμογή δημιουργεί δύο φακέλους με το όνομα του πακέτου, τον πρώτο στην διαδρομή του καταλόγου /data/data και τον δεύτερο στην διαδρομή του καταλόγου /sdcard/Android/data.

Συνδέουμε το κινητό τηλέφωνο με τον υπολογιστή και με την χρήση του ADB εξαγάγουμε τους φακέλους που βρίσκονται στους ανωτέρω καταλόγους.

Ο φάκελος com.bitpay.copay που εξήχθη από την διαδρομή /data/data περιέχει τους φακέλους (app_webview, cache, code_cache, databases, files, no_backup και shared_prefs), ενώ ο φάκελος της διαδρομής /sdcard/Android/data δεν έφερε κανένα δεδομένο στον υπολογιστή μας (προφανώς με την χρήση της εφαρμογής που κάναμε δεν έγινε καμία εγγραφή σε αυτόν τον φάκελο).

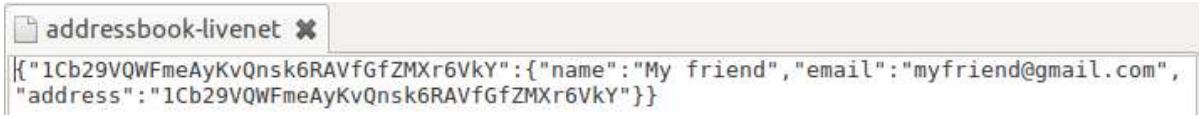
Από τους φακέλους που εξήχθησαν, ενδιαφέρον παρουσιάζουν οι κάτωθι φάκελοι και αρχεία:

- com.bitpay.copay/cache/org.chromium.android_webview
- com.bitpay.copay/files/
  - addressbook-livenet
  - balanceCache-71eca8e9-e4ac-4cec-9ed2-ec1571f09562
  - lastAddress-71eca8e9-e4ac-4cec-9ed2-ec1571f09562
  - txsHistory-71eca8e9-e4ac-4cec-9ed2-ec1571f09562
  - profile

Ο κατάλογος /cache/org.chromium.android_webview περιέχει 1019 αρχεία καταγραφής που περιέχουν ημερομηνίες και ώρες σύνδεσης με τους server της εφαρμογής, για τις ειδοποιήσεις ή για άλλες λειτουργίες της εφαρμογής, ωστόσο δεν μπορεί να

διαπιστωθεί αν περιέχουν και τις εισόδους που πραγματοποίησε ο χρήστης στην εφαρμογή, ενώ πιθανότατα οι περισσότερες από αυτές τις συνδέσεις πραγματοποιήθηκαν στο παρασκήνιο λειτουργίας της εφαρμογής.

Το αρχείο /files/addressbook-livenet, όπως παρατηρούμε στην παρακάτω εικόνα (Στιγμιότυπο 4) περιέχει μία bitcoin διεύθυνση, ένα όνομα και ένα email. Η εφαρμογή επιτρέπει την δημιουργία επαφών (χωρίς διεπαφή με τις επαφές του τηλεφώνου) για την αποθήκευση bitcoin διευθύνσεων που μπορεί να χρησιμοποιούνται συχνότερα από τον χρήστη της εφαρμογής και υποστηρίζει την εισαγωγή ονόματος της επαφής και email. Στο παράδειγμά μας αποθηκεύσαμε μια επαφή, με όνομα “My friend”, email “myfriend@gmail.com” και την διεύθυνση 1Cb29VQWFmeAyKvQnsk6RAVfGfZMXr6VkY.



Στιγμιότυπο 4 - Στοιχεία αποθηκευμένης επαφής στην εφαρμογή Copay

Το αρχείο /files/balanceCache-71eca8e9-e4ac-4cec-9ed2-ec1571f09562, περιέχει το υπόλοιπο του πορτοφολιού εκφρασμένο σε bitcoin, καθώς και την ημερομηνία και ώρα που ενημερώθηκε το πορτοφόλι στη μορφή Linux epoch time. Στην παρακάτω εικόνα (Στιγμιότυπο 5) παρατηρούμε ότι το πορτοφόλι περιέχει υπόλοιπο 0.002101 BTC, με ημερομηνία 1529714752, δηλαδή Σάββατο 23 Ιουνίου 2018, ώρα 3:45:52 AM. Επιπλέον, παρατηρούμε ότι το αλφαριθμητικό “71eca8e9-e4ac-4cec-9ed2-ec1571f09562” που υπάρχει στο τέλος του ονόματος του αρχείου που εξετάσαμε, δηλώνει το id του πορτοφολιού, όπως αυτό έχει δοθεί από την εφαρμογή κατά την δημιουργία του, συνεπώς το υπόλοιπο αφορά το συγκεκριμένο πορτοφόλι και όχι το συνολικό υπόλοιπο που μπορεί να σχηματίζεται κι από άλλα πορτοφόλια που μπορεί να διαχειριζόμασταν με την εφαρμογή.

Στιγμιότυπο 5 - Υπόλοιπο πορτοφολιού Personal Wallet - Copay

Το αρχείο /files/lastAddress-71eca8e9-e4ac-4cec-9ed2-ec1571f09562, περιέχει όπως αναφέρει και το όνομά του, την τελευταία διεύθυνση που δημιουργήθηκε από το πορτοφόλι, προκειμένου να χρησιμοποιηθεί για την λήψη bitcoin. Και πάλι, το αλφαριθμητικό "71eca8e9-e4ac-4cec-9ed2-ec1571f09562" που υπάρχει στο τέλος του ονόματος του αρχείου προσδιορίζει το id του πορτοφολιού από το οποίο δημιουργήθηκε η τελευταία διεύθυνση bitcoin. Στο παράδειγμά μας η διεύθυνση είναι 1DutTnxQDy6a3N9Ua3q2qbwL5zhKsradfn, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 6).

Στιγμιότυπο 6 - Τελευταία διεύθυνση bitcoin που δημιουργήθηκε με αίτηση του χρήστη της εφαρμογής

Το αρχείο /files/txsHistory-71eca8e9-e4ac-4cec-9ed2-ec1571f09562, περιέχει το ιστορικό των συναλλαγών που πραγματοποιήθηκαν στο πορτοφόλι με id "71eca8e9-e4ac-4cec-9ed2-ec1571f09562", όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 7) - στο αρχείο διαχωρίσαμε τις συναλλαγές για καλύτερη απεικόνιση.

*txsHistory-71eca8e9...ec-9ed2-ec1571f09562


```
[{"txid":"07497fb973e951d2397439a553700e53727b494fa40e3cd66020836d9cf82525","action":"sent","amount":60000,
"fees":486,"time":1529175944,"addressTo":"12T6WSasCL6gMctZjUJGs1B8AypkK8FQSw","confirmations":959,"feePerKb
":2160,"outputs":[{"amount":60000,"address":"12T6WSasCL6gMctZjUJGs1B8AypkK8FQSw","message":null,"encryptedM
essage":null,"amountStr":"0.0006 BTC","alternativeAmountStr":"3.74 USD"}],"createdOn":1529175359,"proposalI
d":"3be75549-1422-4d48-84e8-b4ff642e3539","creatorName":"me","message":null,"actions":[{"createdOn":1529175
361,"type":"accept","copayerId":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d309b685d143","copayer
Name":"me","comment":""}],"customData":null,"encryptedMessage":null,"hasUnconfirmedInputs":false,"amountStr
":"0.0006 BTC","alternativeAmountStr":"3.74 USD","feeStr":"0.000004 BTC","amountValueStr":"0.0006","amountU
nitStr":"BTC","safeConfirmed":"6+"},

{"txid":"a6b34ca884f0bbe3bb553b62f7a9a267a6f8c1a841e13edeaf50f26d67820233","action":"received","amount":200
000,"fees":2527,"time":1528936604,"confirmations":1390,"feePerKb":11231,"outputs":[{"amount":200000,"addres
s":"112XRAGBKGmx6Jd5ZgohqyWTC6o4jPzpe7","message":null}],"message":null,"creatorName":"","hasUnconfirmedInp
uts":false,"amountStr":"0.002 BTC","alternativeAmountStr":"12.46 USD","feeStr":"0.000025 BTC","amountValueS
tr":"0.002","amountUnitStr":"BTC","safeConfirmed":"6+"},

{"txid":"798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3","action":"received","amount":706
15,"fees":2112,"time":1528936604,"confirmations":1390,"feePerKb":11058,"outputs":[{"amount":70615,"address
":"1CbnfUrPpakZWe9eJ6FaHd4jrg9864paSS","message":null}],"note":{"version":1,"createdOn":1529691335,"walletI
d":"71eca8e9-e4ac-4cec-9ed2-ec1571f09562",

"txid":"798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3","body":"Myshop","editedOn":152969
1335,"editedBy":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d309b685d143","editedByName":"me","enc
ryptedBody":"{\"iv\":\"j5TiwbAYjbD+xrstya8Qag==\",\"v\":1,\"iter\":1,\"ks\":128,\"ts\":64,\"mode\":\"ccm\",
\"adata\":\"\",\"cipher\":\"aes\",\"ct\":\"koRHAvAPBICVAdW7uyA=\"}","encryptedEditedByName":"{\"iv\":\"TQth
LFIc79ecmlV3Si/VaQ==\",\"v\":1,\"iter\":1,\"ks\":128,\"ts\":64,\"mode\":\"ccm\",\"adata\":\"\",\"cipher\":\
"aes\",\"ct\":\"+36l5KJ0348L0g==\"}"},"message":null,"creatorName":"","hasUnconfirmedInputs":false,"amountS
tr":"0.000706 BTC","alternativeAmountStr":"4.40 USD","feeStr":"0.000021 BTC","amountValueStr":"0.000706","a
mountUnitStr":"BTC","safeConfirmed":"6+"}]
```


Στιγμιότυπο 7 - Ιστορικό συναλλαγών bitcoin που πραγματοποιήθηκαν με την εφαρμογή Copay

Εξερευνώντας προσεχτικά το αρχείο, παρατηρούμε ότι πραγματοποιήθηκαν συνολικά τρεις συναλλαγές, δύο από τις οποίες αφορούν την λήψη bitcoin και μία που αφορά αποστολή bitcoin. Η σειρά με την οποία έγιναν οι συναλλαγές, είναι από κάτω προς τα πάνω,

επομένως η τελευταία συναλλαγή εμφανίζεται στην αρχή του αρχείου. Τα δεδομένα που παρατηρούμε στην κάθε μια είναι τα κάτωθι:

1η συναλλαγή:

Η συναλλαγή έχει αναγνωριστικό (ID) “txid":"798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3” και αφορά την λήψη bitcoin συνολικού ποσού 70615 satoshi (το ποσό είναι εκφρασμένο ως υποδιαίρεση του bitcoin που είναι τα satoshi). Η χρονολογία που πραγματοποιήθηκε η συναλλαγή είναι με την μορφή Linux epoch time* 1528936604, δηλαδή Παρασκευή 14 Ιουνίου 2018, ώρα 3:36:44 AM, ενώ τα bitcoin λήφθηκαν στην διεύθυνση 1CbnfUrPpakZWe9eJ6FaHd4jrg9864paSS. Παρατηρούμε ότι, η χρονοσήμανση της συναλλαγής, αφορά την ώρα που η συναλλαγή συμπεριλήφθηκε στο μπλοκ της αλυσίδας (blockchain) του Bitcoin.

2η συναλλαγή:

Η συναλλαγή έχει αναγνωριστικό (ID) “txid":"a6b34ca884f0bbe3bb553b62f7a9a267a6f8c1a841e13edeaf50f26d67820233" και αφορά την λήψη bitcoin συνολικού ποσού 200000 satoshi (το ποσό είναι εκφρασμένο ως υποδιαίρεση του bitcoin που είναι τα satoshi). Η χρονολογία που πραγματοποιήθηκε η συναλλαγή είναι με την μορφή Linux epoch time* 1528936604, δηλαδή Παρασκευή 14 Ιουνίου 2018, ώρα 3:36:44 AM (η συναλλαγή πραγματοποιήθηκε την ίδια ώρα με την πρώτη), ενώ τα bitcoin λήφθηκαν στην διεύθυνση 112XRAGBKGmx6Jd5ZgohqyWTC6o4jPzpe7. Παρατηρούμε ότι, η χρονοσήμανση της συναλλαγής, αφορά την ώρα που η συναλλαγή συμπεριλήφθηκε στο μπλοκ της αλυσίδας (blockchain) του Bitcoin.

3η συναλλαγή:

Η συναλλαγή έχει αναγνωριστικό (ID) "txid":"07497fb973e951d2397439a553700e53727b494fa40e3cd66020836d9cf82525" και αφορά την αποστολή bitcoin συνολικού ποσού 60000 satoshi (το ποσό είναι εκφρασμένο ως υποδιαίρεση του bitcoin που είναι τα satoshi). Παρατηρούμε ότι, στα δεδομένα της συναλλαγής, αναγράφονται δύο χρονοσημάνσεις σε μορφή Linux epoch time*. Η πρώτη

είναι 1529175944, δηλαδή Σάββατο 16 Ιουνίου 2018, ώρα 10:05:44 PM και η δεύτερη είναι 1529175359, δηλαδή Σάββατο 16 Ιουνίου 2018, ώρα 9:55:59 PM. Η πρώτη χρονοσήμανση αναφέρεται στην ώρα που η συναλλαγή συμπεριλήφθηκε στο μπλοκ της αλυσίδας (blockchain) του Bitcoin, ενώ η δεύτερη χρονοσήμανση αφορά την ώρα που η συναλλαγή λήφθηκε από την ομάδα μνήμης (memory pool) του κόμβου εξόρυξης (miner node). Η διεύθυνση στην οποία στάλθηκαν τα bitcoin είναι η 12T6WSasCL6gMctZjUJGs1B8AypkK8FQSw.

Στο τελευταίο τμήμα του παραπάνω αρχείου, παρατηρούμε ότι για την συναλλαγή “txid":"798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3” που περιγράψαμε προηγουμένως, υπάρχει μια ετικέτα που αναγράφει “Myshop”. Η ετικέτα αυτή δόθηκε από τον χρήστη της εφαρμογής, προκειμένου να χαρακτηρίσει και να αποθηκεύσει την συναλλαγή με αυτό το όνομα.

Στο αρχείο /files/profile που απεικονίζεται στην παρακάτω εικόνα (Στιγμιότυπο 8) - στο αρχείο διαχωρίσαμε κάποια από τα σημαντικότερα δεδομένα για καλύτερη απεικόνιση - , παρατηρούμε ότι περιέχονται αρκετά σημαντικά στοιχεία από την πλευρά της εγκληματολογικής εξέτασης της εφαρμογής. Ένα από τα σημαντικότερα στοιχεία που περιέχονται στο συγκεκριμένο αρχείο είναι η μνημονική ακολουθία λέξεων (mnemonic word sequence) του ιεραρχικά ντετερμινιστικού πορτοφολιού που δημιουργήσαμε με την εφαρμογή, σε μορφή απλού κειμένου: "mnemonic":"toilet valve drop time amateur helmet rude lunch fence impulse jungle narrow". Η κατοχή και μόνο αυτών των λέξεων, μπορεί να μας δώσει την πλήρη πρόσβαση στα bitcoin που είναι αποθηκευμένα στο πορτοφόλι. Παράλληλα με την μνημονική ακολουθία λέξεων παρατηρούμε ότι στο αρχείο εμφανίζεται και το επεκταμένο ιδιωτικό κλειδί ρίζας "xPrivKey":"xprv9s21ZrQH143K3Hrcy2Pwbf2BbHpxiPNYpxrzDz2ZPk4AT5t9y1vsdZLxy qBbe9CcLTFA9mgRRqddKoXTgKjLBz6uUR8E6JTaqX9kKL23uYT", με την χρήση του οποίου μπορεί να δημιουργηθεί όλος ο κλάδος του πορτοφολιού και συνεπώς να μας δώσει πρόσβαση στα παραγόμενα ιδιωτικά και δημόσια κλειδιά του πορτοφολιού και επομένως πλήρη πρόσβαση στα bitcoin του χρήστη. Παρότι με την χρήση του επεκταμένου ιδιωτικού κλειδιού μπορούμε να δημιουργήσουμε και το επεκταμένο δημόσιο κλειδί, όπως αναφέραμε προηγουμένως, ωστόσο παρατηρούμε ότι στα δεδομένα του αρχείου εμφανίζεται σε μορφή απλού κειμένου και το επεκταμένο δημόσιο κλειδί "xPubKey":"xpub6CMUKrbovL9NocA3HVkQ2hLFxs1gL5sCMpDM35UjcqPF94FFS7FiL

c8HKNXc5pUJ1YpqWqBNWSGdFA1shjnVa4kwKx6wYjbmMw6pqFPnDSn". Με την χρήση του επεκταμένου δημοσίου κλειδιού μπορούμε να δημιουργήσουμε όλες τις διευθύνσεις bitcoin του πορτοφολιού, οπότε θα είμαστε σε θέση να γνωρίζουμε τις διευθύνσεις που ανήκουν σε αυτό το πορτοφόλι. Επιπλέον, στο αρχείο εμφανίζεται το id "walletId":"71eca8e9-e4ac-4cec-9ed2-ec1571f09562" του πορτοφολιού στο οποίο ανήκουν τα παραπάνω επεκταμένα ιδιωτικά και δημόσια κλειδιά, καθώς και το όνομα "walletName":"Personal Wallet" του πορτοφολιού, όπως δόθηκε από τον χρήστη της εφαρμογής. Τέλος, παρατηρούμε ότι στο αρχείο εμφανίζονται η έκδοση του λειτουργικού Android και η μάρκα του κινητού τηλεφώνου στο οποίο δημιουργήθηκαν, που στο παράδειγμά μας είναι η έκδοση 6.0.1 του Android και το κινητό τηλέφωνο είναι το ONEPLUS A3003, όπως φαίνεται και στην παρακάτω εικόνα (Στιγμιότυπο 8).

profile


```
{"version":"1.0.0","createdOn":1528401045831,"credentials":[{"coin":"btc","network":"livenet",

"xPrivKey":"xprv9s21ZrQH143K3Hrcy2Pwbf2BbHpxiPNYpxrzDz2ZPk4AT5t9y1vsdZLxyqBbe9CcLTFA9mgRRqddKo
XTgKjLBz6uUR8E6JTaqX9kKL23uYT",

"xPubKey":"xpub6CMUKrbovL9NocA3HVkQ2hLFxs1gL5sCMpDM35UjcqPF94FFS7FiLc8HKNXc5pUJ1YpqWqBNWSGdFA1
shjnVa4kwKx6wYjbmMw6pqFPnDSn",

"requestPrivKey":"b8d872c0ce85899db8eb533a92a916468271571e072d2f51ec6b54dd2bb9848d",
"requestPubKey":"022f81899509307e70b7a30d396f3a08fb11ee13603b0639d8af867c11c7d03a69",

"copayerId":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d309b685d143","publicKeyRing
":[{"xPubKey":"xpub6CMUKrbovL9NocA3HVkQ2hLFxs1gL5sCMpDM35UjcqPF94FFS7FiLc8HKNXc5pUJ1YpqWqBNWSG
dFA1shjnVa4kwKx6wYjbmMw6pqFPnDSn","requestPubKey":"022f81899509307e70b7a30d396f3a08fb11ee13603
b0639d8af867c11c7d03a69"}],

"walletId":"71eca8e9-e4ac-4cec-9ed2-ec1571f09562",

"walletName":"Personal Wallet",

"m":1,"n":1,"walletPrivKey":"fef3bd139218cffa349b32a5736da8e02a7ad4bc9ded64727800719232e95e24
","personalEncryptingKey":"59bspjINhzyUYDoTljB0WA==","sharedEncryptingKey":"9Qk0AccrkbKcehgbEz
v27Q==","copayerName":"me",

"mnemonic":"toilet valve drop time amateur helmet rude lunch fence impulse jungle narrow",

"entropySource":"097d321242660a9abc12b397b133840cb201a8ca863773e3fed8b3252c5eed22",

"mnemonicHasPassphrase":false,"derivationStrategy":"BIP44","account":0,"compliantDerivation":t
rue,"addressType":"P2PKH"}],"disclaimerAccepted":true,"onboardingCompleted":true,"checked":{"7
1eca8e9-e4ac-4cec-9ed2-ec1571f09562":true},"checkedUA":"Mozilla/5.0

(Linux; Android 6.0.1; ONEPLUS A3003 Build/MMB29M; wv)

AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/67.0.3396.87 Mobile Safari/537.36","
dirty":true}
```


Στιγμιότυπο 8 - Μνημονική ακολουθία λέξεων, ιδιωτικό - δημόσιο κλειδί και άλλα ευαίσθητα δεδομένα του πορτοφολιού Copay, σε μορφή απλού κειμένου

* epoch time: Η χρονοσήμανση στα δεδομένα της εφαρμογής αναφέρεται στη ζώνη ώρας που είναι ρυθμισμένο το κινητό μας τηλέφωνο

Επαναφορά πορτοφολιού από Backup - Copay Bitcoin Wallet

Η επόμενη δοκιμή που θα κάνουμε στην εφαρμογή Copay είναι η διαγραφή της από το κινητό μας τηλέφωνο, η επανεγκατάσταση της και η επαναφορά του πορτοφολιού που εξετάσαμε προηγουμένως, από backup που έχουμε κρατήσει.

Χρησιμοποιούμε και πάλι το εργαλείο ADB, προκειμένου να εξάγουμε τα αρχεία που βρίσκονται στο πακέτο εγκατάστασης της εφαρμογής.

Στην διαδρομή του καταλόγου /data/data/com.bitpay.copay περιέχονται οι φάκελοι (app_webview, cache, code_cache, databases, files, no_backup και shared_prefs), όπως και στην προηγούμενη δοκιμή μας, ενώ πάλι ο φάκελος της διαδρομής /sdcard/Android/data δεν έφερε κανένα αρχείο στον υπολογιστή μας.

Από τους φακέλους που εξαγάγαμε, ενδιαφέρον παρουσιάζουν οι φάκελοι με τα αρχεία:

- com.bitpay.copay/cache/org.chromium.android_webview
- com.bitpay.copay/files/
    balanceCache-71eca8e9-e4ac-4cec-9ed2-ec1571f09562
    txsHistory-71eca8e9-e4ac-4cec-9ed2-ec1571f09562
    profile

Παρατηρούμε ότι, συγκριτικά με την προηγούμενη δοκιμή μας, απουσιάζουν τα αρχεία (addressbook-livenet και lastAddress-71eca8e9-e4ac-4cec-9ed2-ec1571f09562). Αυτό σημαίνει ότι το backup του πορτοφολιού μας δεν κρατάει τις επαφές που είχε αποθηκεύσει ο χρήστης, προκειμένου να έχει γρήγορη πρόσβαση στις διευθύνσεις με τις οποίες συναλλάσσεται συχνότερα, καθώς και την τελευταία διεύθυνση που δημιουργήθηκε από το πορτοφόλι. Η τελευταία διεύθυνση δημιουργείται και αποθηκεύεται μόνο όταν ο χρήστης μεταβεί στην καρτέλα λήψης bitcoin μέσα από την εφαρμογή και η διεύθυνση που δημιουργείται είναι μία καινούρια διεύθυνση από τις “άπειρες” διευθύνσεις που μπορούν να δημιουργηθούν από το πορτοφόλι.
Οι διαφορές που εντοπίζονται στα υπόλοιπα αρχεία συγκριτικά με την προηγούμενη ανάλυσή μας είναι οι εξής:

Ο κατάλογος /cache/org.chromium.android_webview περιέχει αυτή την φορά 23 αρχεία καταγραφής αντίθετα με τα 1019 αρχεία που είχαν βρεθεί στην προηγούμενη δοκιμή μας, τα οποία περιέχουν ημερομηνίες και ώρες σύνδεσης με τους server της εφαρμογής, για τις ειδοποιήσεις ή για άλλες λειτουργίες της εφαρμογής, ωστόσο δεν μπορεί να διαπιστωθεί αν περιέχουν και τις εισόδους που πραγματοποίησε ο χρήστης στην εφαρμογή, ενώ πιθανότατα οι περισσότερες από αυτές τις συνδέσεις πραγματοποιήθηκαν στο παρασκήνιο λειτουργίας της εφαρμογής.

Το αρχείο /files/balanceCache-71eca8e9-e4ac-4cec-9ed2-ec1571f09562, που αναγράφει το υπόλοιπο του πορτοφολιού, παρατηρούμε ότι μεταβλήθηκε όσον αφορά την ώρα που ενημερώθηκε το υπόλοιπο του πορτοφολιού μας και έτσι ώρα εμφανίζει τον αριθμό 1530137032, δηλαδή Τρίτη 28 Ιουνίου 2018, ώρα 1:03:52 AM, ενώ αναγράφει και το υπόλοιπο του πορτοφολιού το οποίο αφού πρόκειται για backup του προηγούμενου πορτοφολιού μας παραμένει το ίδιο (Στιγμιότυπο 9).

balanceCache-71eca8...ec-9ed2-ec1571f09562

{"balance":"0.002101 BTC","updatedOn":1530137032}

Στιγμιότυπο 9 - Υπόλοιπο πορτοφολιού Personal Wallet μετά την επαναφορά από backup

Το αρχείο /files/txsHistory-71eca8e9-e4ac-4cec-9ed2-ec1571f09562, μεταβλήθηκε σε κάποιο βαθμό, πλην όμως διατήρησε τις συναλλαγές που πραγματοποιήθηκαν από το πορτοφόλι, ακριβώς όπως τις αναλύσαμε στην προηγούμενη δοκιμή μας (Στιγμιότυπο 10).

*txsHistory-71eca8e9...ec-9ed2-ec1571f09562

[{"txid":"07497fb973e951d2397439a553700e53727b494fa40e3cd66020836d9cf82525","action":"sent","amount":60000,"fees":486,"time":1529175944,"addressTo":"12T6WSasCL6gMctZjUJGs1B8AypkK8FQSw","confirmations":1732,"feePerKb":2160,"outputs":[{"amount":60000,"address":"12T6WSasCL6gMctZjUJGs1B8AypkK8FQSw","message":null,"encryptedMessage":null,"amountStr":"0.0006 BTC","alternativeAmountStr":"3.67 USD"}],"createdOn":1529175359,"proposalId":"3be75549-1422-4d48-84e8-b4ff642e3539","creatorName":"me","message":null,"actions":[{"createdOn":1529175361,"type":"accept","copayerId":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d309b685d143","copayerName":"me","comment":""}],"customData":null,"encryptedMessage":null,"hasUnconfirmedInputs":false,"amountStr":"0.0006 BTC","alternativeAmountStr":"3.67 USD","feeStr":"0.000004 BTC","amountValueStr":"0.0006","amountUnitStr":"BTC","safeConfirmed":"6+"},

{"txid":"a6b34ca884f0bbe3bb553b62f7a9a267a6f8c1a841e13edeaf50f26d67820233","action":"received","amount":200000,"fees":2527,"time":1528936604,"confirmations":2163,"feePerKb":11231,"outputs":[{"amount":200000,"address":"112XRAGBKGmx6Jd5ZgohqyWTC6o4jPzpe7","message":null}],"message":null,"creatorName":"","hasUnconfirmedInputs":false,"amountStr":"0.002 BTC","alternativeAmountStr":"12.24 USD","feeStr":"0.000025 BTC","amountValueStr":"0.002","amountUnitStr":"BTC","safeConfirmed":"6+"},

{"txid":"798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3","action":"received","amount":70615,"fees":2112,"time":1528936604,"confirmations":2163,"feePerKb":11058,"outputs":[{"amount":70615,"address":"1CbnfUrPpakZWe9eJ6FaHd4jrg9864paSS","message":null}],"note":{"body":"Myshop","editedBy":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d309b685d143","editedByName":"me","editedOn":1529691335},"message":null,"creatorName":"","hasUnconfirmedInputs":false,"amountStr":"0.000706 BTC","alternativeAmountStr":"4.32 USD","feeStr":"0.000021 BTC","amountValueStr":"0.000706","amountUnitStr":"BTC","safeConfirmed":"6+"}]

Στιγμιότυπο 10 - Ιστορικό συναλλαγών bitcoin μετά την επαναφορά από backup - Copay

Τέλος, στο αρχείο /files/profile, μπορούμε να εντοπίσουμε και πάλι την μνημονική ακολουθία λέξεων σε μορφή απλού κειμένου, καθώς και όλα τα προηγούμενα ευρήματά μας, χωρίς να έχουν πραγματοποιηθεί ουσιώδης αλλαγές στο αρχείο (Στιγμιότυπο 11).

*profile

{"version":"1.0.0","createdOn":1530136817438,"credentials":[{"coin":"btc","network":"livenet",

"xPrivKey":"xprv9s21ZrQH143K3Hrcy2Pwbf2BbHpxiPNYpxrzDz2ZPk4AT5t9y1vsdZLxyqBbe9CcLTFA9mgRRqddKo
XTgKjLBz6uUR8E6JTaqX9kKL23uYT",

"xPubKey":"xpub6CMUKrbovL9NocA3HVkQ2hLFxs1gL5sCMpDM35UjcqPF94FFS7FiLc8HKNXc5pUJ1YpqWqBNWSGdFA1
shjnVa4kwKx6wYjbmMw6pqFPnDSn",

"requestPrivKey":"b8d872c0ce85899db8eb533a92a916468271571e072d2f51ec6b54dd2bb9848d",
"requestPubKey":"022f81899509307e70b7a30d396f3a08fb11ee13603b0639d8af867c11c7d03a69",

"copayerId":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d309b685d143","publicKeyRing
":[{"xPubKey":"xpub6CMUKrbovL9NocA3HVkQ2hLFxs1gL5sCMpDM35UjcqPF94FFS7FiLc8HKNXc5pUJ1YpqWqBNWSG
dFA1shjnVa4kwKx6wYjbmMw6pqFPnDSn","requestPubKey":"022f81899509307e70b7a30d396f3a08fb11ee13603
b0639d8af867c11c7d03a69","copayerName":"me"}],

"walletId":"71eca8e9-e4ac-4cec-9ed2-ec1571f09562",

"walletName":"Personal Wallet",

"m":1,"n":1,"walletPrivKey":"fef3bd139218cffa349b32a5736da8e02a7ad4bc9ded64727800719232e95e24
","personalEncryptingKey":"59bspjINhzyUYDoTljB0WA==","sharedEncryptingKey":"9Qk0AccrkbKcehgbEz
v27Q==","copayerName":"me",

"mnemonic":"toilet valve drop time amateur helmet rude lunch fence impulse jungle narrow",

"entropySource":"097d321242660a9abc12b397b133840cb201a8ca863773e3fed8b3252c5eed22",

"mnemonicHasPassphrase":false,"derivationStrategy":"BIP44","account":0,"compliantDerivation":t
rue,"addressType":"P2PKH"}],"disclaimerAccepted":false,"onboardingCompleted":true,"checked":{"
71eca8e9-e4ac-4cec-9ed2-ec1571f09562":true},"dirty":true,"checkedUA":"Mozilla/5.0

(Linux; Android 6.0.1; ONEPLUS A3003 Build/MMB29M; wv)

AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/67.0.3396.87 Mobile Safari/537.36"}

Στιγμιότυπο 11 - Μνημονική ακολουθία λέξεων, ιδιωτικό - δημόσιο κλειδί και άλλα ευαίσθητα δεδομένα μετά την επαναφορά του πορτοφολιού Copay από backup

Κρυπτογράφηση του πορτοφολιού που επαναφέραμε μετά το Backup - Copay Bitcoin Wallet

Στην εξέταση που πραγματοποιήσαμε μετά την επαναφορά του πορτοφολιού από backup, συγκριτικά με την αρχική εξέταση της εφαρμογής, δεν βρέθηκαν αρκετές διαφορές. Σε αυτή την δοκιμή θα εξετάσουμε τα δεδομένα της εφαρμογής αφού πρώτα κρυπτογραφήσουμε το πορτοφόλι, καθώς το επαναφέραμε από το backup. Όπως αναφέραμε κατά την διαδικασία εγκατάστασης της εφαρμογής, μας δίνεται η επιλογή κρυπτογράφησης του πορτοφολιού μας για μεγαλύτερη ασφάλεια. Ας δούμε επομένως, τα ευρήματα που μπορούμε να συλλέξουμε, αν ο χρήστης έχει προβεί σε κρυπτογράφηση του πορτοφολιού.

Με το εργαλείο ADB, εξάγουμε τα αρχεία του πακέτου της εφαρμογής που εξετάζουμε, όπως στις προηγούμενες δοκιμές μας. Η διαδρομή του καταλόγου /data/data/com.bitpay.copay περιέχει τους φακέλους (app_webview, cache, code_cache, databases, files, no_backup και shared_prefs), όπως και στην προηγούμενη δοκιμή μας, ενώ ο φάκελος της διαδρομής /sdcard/Android/data δεν επέστρεψε κάποιο αρχείο στον υπολογιστή μας.

Από τους φακέλους που εξαγάγαμε, ενδιαφέρον παρουσιάζουν οι φάκελοι με τα αρχεία:

- com.bitpay.copay/cache/org.chromium.android_webview
- com.bitpay.copay/files/
    - balanceCache-71eca8e9-e4ac-4cec-9ed2-ec1571f09562
    - lastAddress-71eca8e9-e4ac-4cec-9ed2-ec1571f09562
    - txsHistory-71eca8e9-e4ac-4cec-9ed2-ec1571f09562
    - profile

Παρατηρούμε ότι συγκριτικά με την προηγούμενη δοκιμή μας, απουσιάζει το αρχείο addressbook-livenet, όπως ήταν αναμενόμενο, αφού δεν αποθηκεύτηκε με το backup της εφαρμογής όπως εξηγήσαμε προηγουμένως. Η τελευταία διεύθυνση που εμφανίζεται στο αρχείο lastAddress-71eca8e9-e4ac-4cec-9ed2-ec1571f09562 εμφανίζεται, διότι ως χρήστες περιηγηθήκαμε στην καρτέλα λήψης bitcoin μέσα στην εφαρμογή και έτσι δημιουργήσαμε μια καινούρια διεύθυνση που αποθηκεύτηκε ως τελευταία αποθηκευμένη.

Οι υπόλοιπες διαφορές που εντοπίζονται στα αρχεία, συγκριτικά με την προηγούμενη ανάλυσή μας είναι οι εξής:

Ο κατάλογος /cache/org.chromium.android_webview περιέχει αυτή την φορά 9 αρχεία καταγραφής αντίθετα με τα 23 αρχεία που είχαν βρεθεί στην προηγούμενη δοκιμή μας (δεν μπορέσαμε να εξηγήσουμε το λόγο που τα αρχεία ήταν λιγότερα από την προηγούμενη φορά καθώς το μόνο που κάναμε ήταν να κρυπτογραφήσουμε το πορτοφόλι μας).

Το αρχείο /files/balanceCache-71eca8e9-e4ac-4cec-9ed2-ec1571f09562, που αναγράφει το υπόλοιπο του πορτοφολιού, τροποποιήθηκε μόνο όσον αφορά την ώρα

ενημέρωσης του πορτοφολιού μας και εμφανίζει τον αριθμό 1530900585, δηλαδή Παρασκευή 6 Ιουλίου 2018, ώρα 9:09:45 PM, ενώ μπορούμε να δούμε το υπόλοιπο του πορτοφολιού μας, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 12).

balanceCache-71eca8...ec-9ed2-ec1571f09562

{"balance":"0.002101 BTC","updatedOn":1530900585}

Στιγμιότυπο 12 - Υπόλοιπο πορτοφολιού Copay μετά την κρυπτογράφηση του

Το αρχείο /files/txsHistory-71eca8e9-e4ac-4cec-9ed2-ec1571f09562, τροποποιήθηκε μερικώς από τη κρυπτογράφηση του πορτοφολιού μας, πλην όμως διατήρησε τις συναλλαγές που πραγματοποιήθηκαν από το πορτοφόλι ακριβώς όπως τις αναλύσαμε στην προηγούμενη δοκιμή μας, σε μορφή απλού κειμένου (Στιγμιότυπο 13). Δεν πραγματοποιήθηκαν νέες συναλλαγές μετά την κρυπτογράφηση του πορτοφολιού, όποτε δεν γνωρίζουμε αν οι συναλλαγές μετά την κρυπτογράφηση παραμένουν σε μορφή απλού κειμένου ή αν κρυπτογραφούνται κι αυτές.

*txsHistory-71eca8e9...ec-9ed2-ec1571f09562

[{"txid":"07497fb973e951d2397439a553700e53727b494fa40e3cd66020836d9cf82525","action":"sent","amount":60000,"
fees":486,"time":1529175944,"addressTo":"12T6WSasCL6gMctZjUJGs1B8AypkK8FQSw","confirmations":1732,"feePerKb
":2160,"outputs":[{"amount":60000,"address":"12T6WSasCL6gMctZjUJGs1B8AypkK8FQSw","message":null,"encryptedMe
ssage":null,"amountStr":"0.0006 BTC","alternativeAmountStr":"3.67 USD"}],"createdOn":1529175359,"proposalId
":"3be75549-1422-4d48-84e8-b4ff642e3539","creatorName":"me","message":null,"actions":[{"createdOn":152917536
1,"type":"accept","copayerId":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d309b685d143","copayerNam
e":"me","comment":""}],"customData":null,"encryptedMessage":null,"hasUnconfirmedInputs":false,"amountStr":"
0.0006 BTC","alternativeAmountStr":"3.67 USD","feeStr":"0.000004 BTC","amountValueStr":"0.0006","amountUnitS
tr":"BTC","safeConfirmed":"6+"},

{"txid":"a6b34ca884f0bbe3bb553b62f7a9a267a6f8c1a841e13edeaf50f26d67820233","action":"received","amount":2000
00,"fees":2527,"time":1528936604,"confirmations":2163,"feePerKb":11231,"outputs":[{"amount":200000,"address
":"112XRAGBKGmx6Jd5ZgohqyWTC6o4jPzpe7","message":null}],"message":null,"creatorName":"","hasUnconfirmedInput
s":false,"amountStr":"0.002 BTC","alternativeAmountStr":"12.24 USD","feeStr":"0.000025 BTC","amountValueStr
":"0.002","amountUnitStr":"BTC","safeConfirmed":"6+"},

{"txid":"798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3","action":"received","amount":7061
5,"fees":2112,"time":1528936604,"confirmations":2163,"feePerKb":11058,"outputs":[{"amount":70615,"address":"
1CbnfUrPpakZWe9eJ6FaHd4jrg9864paSS","message":null}],"note":{"version":1,"createdOn":1529691335,"walletId":"
71eca8e9-e4ac-4cec-9ed2-ec1571f09562","txid":"798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0
c3","body":"Myshop","editedOn":1529691335,"editedBy":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d3
09b685d143","editedByName":"me",

"encryptedBody":"{\"iv\":\"j5TiwbAYjbD+xrstya8Qag==\",\"v\":1,\"iter\":1,\"ks\":128,\"ts\":64,\"mode\":\"ccm
\",\"adata\":\"\",\"cipher\":\"aes\",\"ct\":\"koRHAvAPBICVAdW7uyA=\"}","encryptedEditedByName":"{\"iv\":\"TQ
thLFIc79ecmlV3Si/VaQ==\",\"v\":1,\"iter\":1,\"ks\":128,\"ts\":64,\"mode\":\"ccm\",\"adata\":\"\",\"cipher\":
\"aes\",\"ct\":\"+36l5KJ0348L0g==\"}"},

"message":null,"creatorName":"","hasUnconfirmedInputs":false,"amountStr":"0.000706 BTC","alternativeAmountSt
r":"4.32 USD","feeStr":"0.000021 BTC","amountValueStr":"0.000706","amountUnitStr":"BTC","safeConfirmed":"6+
"}]

Στιγμιότυπο 13 - Ιστορικό συναλλαγών bitcoin μετά την κρυπτογράφηση του πορτοφολιού Copay

Στο αρχείο /files/profile, όπως ήταν αναμενόμενο μετά την κρυπτογράφηση του πορτοφολιού, η μνημονική ακολουθία λέξεων (mnemonic word sequence) είναι πλέον

κρυπτογραφημένη "mnemonicEncrypted", όπως και το ιδιωτικό κλειδί ρίζας "xPrivKeyEncrypted", συνεπώς δεν μπορούμε να έχουμε πρόσβαση στα bitcoin που είναι αποθηκευμένα στο πορτοφόλι του χρήστη (Στιγμιότυπο 14). Ωστόσο παρατηρούμε ότι το επεκταμένο δημόσιο κλειδί του πορτοφολιού "xPubKey" δεν έχει κρυπτογραφηθεί, οπότε θα μπορούσαμε να το χρησιμοποιήσουμε προκειμένου να δημιουργήσουμε όλες τις διευθύνσεις bitcoin του πορτοφολιού και επομένως να γνωρίζουμε τις διευθύνσεις που ανήκουν σε αυτό το πορτοφόλι.

Άλλα δεδομένα τα οποία δεν έχουν κρυπτογραφηθεί και μπορούν να αντληθούν από το συγκεκριμένο αρχείο είναι το "walletId" του πορτοφολιού, το "walletName", η έκδοση του λειτουργικού Android και η μάρκα του κινητού τηλεφώνου του χρήστη, όπως είδαμε και στις προηγούμενες δοκιμές μας. Αυτά τα ευρήματα θα μας ήταν χρήσιμα αν ο χρήστης χρησιμοποιούσε το ίδιο πορτοφόλι σε δύο συσκευές, όπου θα μπορούσε να εξακριβωθεί ότι είναι το ίδιο πορτοφόλι.

*profile


```
{"version":"1.0.0","createdOn":1530136817438,"credentials":[{"coin":"btc","network":"livenet",

"xPrivKeyEncrypted":"{\"iv\":\"pPWVUfG44d3WGgsYphOAqw==\",\"v\":1,\"iter\":10000,\"ks\":128,\"
ts\":64,\"mode\":\"ccm\",\"adata\":\"\",\"cipher\":\"aes\",\"salt\":\"6ZQqSWJv3sA=\",\"ct\":\"
bmj1d1VK4EdAgqHyCkz34Dnd52uWBkjfzayOuR97K/srxhXsto/KZsmT7/EIPtBIcKNf0ha4ZHS0GuaeCkCPqMBHpeW8AU
TWXcio0YZoy9eUtGnyYXD3V63he7iwnH56L2CpfNjtWJJtF5NQBt/fWzakTp6UbLk=\"}",

"xPubKey":"xpub6CMUKrbovL9NocA3HVkQ2hLFxs1gL5sCMpDM35UjcqPF94FFS7FiLc8HKNXc5pUJ1YpqWqBNWSGdFA1
shjnVa4kwKx6wYjbmMw6pqFPnDSn",

"requestPrivKey":"b8d872c0ce85899db8eb533a92a916468271571e072d2f51ec6b54dd2bb9848d",
"requestPubKey":"022f81899509307e70b7a30d396f3a08fb11ee13603b0639d8af867c11c7d03a69",

"copayerId":"777ec67fbad18c36c4e422af4f13e12fcecf207924950d2b23d4d309b685d143","publicKeyRing
":[{"xPubKey":"xpub6CMUKrbovL9NocA3HVkQ2hLFxs1gL5sCMpDM35UjcqPF94FFS7FiLc8HKNXc5pUJ1YpqWqBNWSG
dFA1shjnVa4kwKx6wYjbmMw6pqFPnDSn","requestPubKey":"022f81899509307e70b7a30d396f3a08fb11ee13603
b0639d8af867c11c7d03a69","copayerName":"me"}],

"walletId":"71eca8e9-e4ac-4cec-9ed2-ec1571f09562",

"walletName":"Personal Wallet",

"m":1,"n":1,"walletPrivKey":"fef3bd139218cffa349b32a5736da8e02a7ad4bc9ded64727800719232e95e24
","personalEncryptingKey":"59bspjINhzyUYDoTljB0WA==","sharedEncryptingKey":"9Qk0AccrkbKcehgbEz
v27Q==","copayerName":"me",

"mnemonicEncrypted":"{\"iv\":\"ElhihrOTNeQIefKSus8mnQ==\",\"v\":1,\"iter\":10000,\"ks\":128,\"
ts\":64,\"mode\":\"ccm\",\"adata\":\"\",\"cipher\":\"aes\",\"salt\":\"6ZQqSWJv3sA=\",\"ct\":\"
SLq1oQtz1xTqJq6S6JCPtlsYOZKF7mlfB6AMky14qPch8bpP6WlrWAziB+MmZEgmoRCNjWImzgHbhgbfuOqhCvbXvhpmoK
HyLs0cIx+UYRcUK5jZ\"}",

"entropySource":"097d321242660a9abc12b397b133840cb201a8ca863773e3fed8b3252c5eed22",

"mnemonicHasPassphrase":false,"derivationStrategy":"BIP44","account":0,"compliantDerivation":t
rue,"addressType":"P2PKH"}],"disclaimerAccepted":true,"onboardingCompleted":true,"checked":{"7
1eca8e9-e4ac-4cec-9ed2-ec1571f09562":true},"checkedUA":"Mozilla/5.0

(Linux; Android 6.0.1; ONEPLUS A3003 Build/MMB29M; wv)

AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/67.0.3396.87 Mobile Safari/537.36","
dirty":true}
```


Στιγμιότυπο 14 - Μνημονική ακολουθία λέξεων και ιδιωτικό κλειδί κρυπτογραφημένα - δημόσιο κλειδί σε μορφή απλού κειμένου - Copay

Εφαρμογή Mycelium Bitcoin Wallet

Εγκατάσταση της εφαρμογής Mycelium Bitcoin Wallet

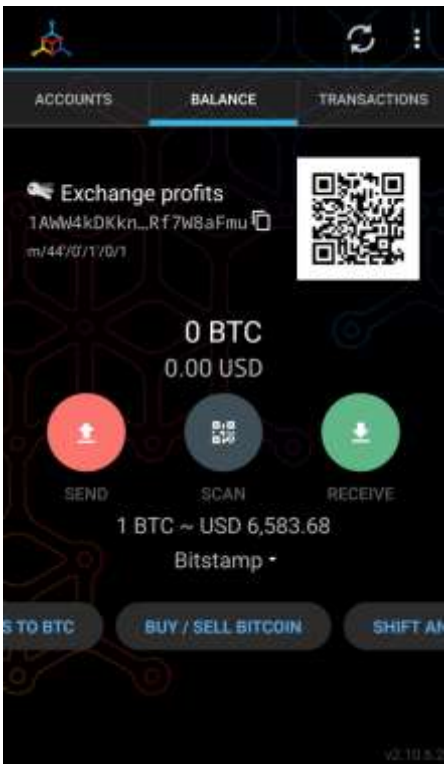
Η εφαρμογή βρίσκεται στο Play Store και την στιγμή των δοκιμών βρισκόταν στην έκδοση 2.10.6.2. Σύμφωνα με τους δημιουργούς της, η εφαρμογή Mycelium είναι ανοικτού κώδικα και ο πηγαίος κώδικάς της βρίσκεται στο GitHub στον σύνδεσμο https://github.com/mycelium-com/wallet. Υποστηρίζει πλήθος λειτουργιών και ακολουθεί την ντετερμινιστική ιεραρχική δημιουργία διευθύνσεων bitcoin, είναι δηλαδή ένα Hierarchical Deterministic Wallet (HD), ενώ μπορεί και διαχειρίζεται διαφορετικούς λογαριασμούς βασιζόμενοι στο ίδιο πρώτο (κύριο) κλειδί γνωστό ως master seed. Η εφαρμογή είναι αρκετά δημοφιλής στο Play Store και έχει περίπου 500.000+ λήψεις σύμφωνα με τα στοιχεία της Google.

Κατά την είσοδο στην εφαρμογή δίνεται η επιλογή της δημιουργίας καινούριου πορτοφολιού και η επαναφορά πορτοφολιού από backup. Συνεχίσαμε με την δημιουργία νέου πορτοφολιού, το οποίο επιλέξαμε να μην κρυπτογραφήσουμε με κάποιον κωδικό (Στιγμιότυπο 15).

Στιγμιότυπο 15 - Δημιουργία νέου πορτοφολιού Mycelium

Κατά την χρήση της εφαρμογής δημιουργήσαμε δύο λογαριασμούς κάτω από το ίδιο κύριο κλειδί, δίνοντάς τους τον πρώτο την ονομασία “Shop1” και τον δεύτερο την ονομασία “Exchange profits”. Τα υπόλοιπα των λογαριασμών παρουσιάζονται στις κάτωθι εικόνες (Στιγμιότυπο 16 και Στιγμιότυπο 17).

Στιγμιότυπο 16 - Υπόλοιπο λογαριασμού Shop1 - Mycelium



Στιγμιότυπο 17 - Υπόλοιπο λογαριασμού Exchange profits - Mycelium

Κάνοντας χρήση των λογαριασμών αυτών, πραγματοποιήσαμε κάποιες συναλλαγές λήψης και αποστολής bitcoin. Ενδεικτικά στις παρακάτω εικόνες (Στιγμιότυπο 18 και Στιγμιότυπο 19) φαίνονται οι συναλλαγές που έγιναν στον λογαριασμό "Shop1" και οι λεπτομέρειες μιας εκ των συναλλαγών στον ίδιο λογαριασμό.

Στιγμιότυπο 18 - Συναλλαγές bitcoin λογαριασμού Shop1 - Mycelium

Στιγμιότυπο 19 - Λεπτομέρειες συναλλαγής όπως εμφανίζεται στο περιβάλλον χρήστη - Mycelium

Εγκληματολογική εξέταση της εφαρμογής Mycelium Bitcoin Wallet

Για την εγκληματολογική εξέταση της εφαρμογής, θα χρησιμοποιήσουμε την λογική μέθοδο απόκτησης, κάνοντας χρήση του εργαλείου της γέφυρας εντοπισμού σφαλμάτων του Android (Android Debug Bridge) ή ADB εν συντομία, όπως θα το αποκαλούμε στη συνέχεια.

Το όνομα του πακέτου εγκατάστασης της εφαρμογής είναι το “com.mycelium.wallet” και κατά την εγκατάσταση η εφαρμογή δημιουργεί τον ομώνυμο φάκελο στην διαδρομή του καταλόγου /data/data.

Συνδέουμε το κινητό τηλέφωνο με τον υπολογιστή και με την χρήση του ADB εξαγάγουμε τους φακέλους που βρίσκονται στους ανωτέρω καταλόγους.

Ο φάκελος com.mycelium.wallet που εξήχθη από την διαδρομή /data/data περιέχει τους φακέλους (code_cache, databases, files και shared_prefs).

Από αυτούς τους φακέλους ενδιαφέρον παρουσιάζουν οι φάκελοι με τα αρχεία:

- com.mycelium.wallet/shared_prefs/
  - settings.xml
  - transaction_fiat_value.xml
- com.mycelium.wallet/databases/
  - mds.db
  - walletbacking.db
  - walletbacking.db-journal

Το αρχείο /shared_prefs/settings.xml μπορεί να μας δώσει στοιχεία σχετικά με τον λογαριασμό που έχει επιλεγμένο ο χρήστης στο πορτοφόλι του, ωστόσο μας το εμφανίζει με την μορφή συμβολοσειράς αντί του ονόματος που είχαμε δώσει στον λογαριασμό. Όπως θα δούμε στη συνέχεια της ανάλυσης μας, ο λογαριασμός "selectedAccount">21dc519d-292f-07cd-851d-4b2c787a9ce8 αντιστοιχεί στον λογαριασμό με όνομα “Shop1”. Τα περιεχόμενα του αρχείου settings.xml φαίνονται στην παρακάτω εικόνα (Στιγμιότυπο 20).

settings.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="selectedAccount">21dc519d-292f-07cd-851d-4b2c787a9ce8</string>
    <string name="MinerFeeEstimationSetting">ECONOMIC</string>
    <string name="tor_mode">ONLY_HTTPS</string>
    <string name="user_language">en</string>
    <set name="selectedFiatCurrencies">
        <string>USD</string>
    </set>
    <string name="ignored_versions">2.10.5.10</string>
</map>
```

Στιγμιότυπο 20 - Ρυθμίσεις - στοιχεία επιλεγμένου λογαριασμού στην εφαρμογή Mycelium

Το αρχείο /shared_prefs/transaction_fiat_value.xml περιέχει το αναγνωριστικό (id) πέντε συναλλαγών συνοδευόμενο από την αξία του ποσού της συναλλαγής σε δολάρια. Ωστόσο δεν μπορεί να προσδιοριστεί αν η συναλλαγή αφορά λήψη ή αποστολή bitcoin, καθώς και το ποσό των bitcoin που συναλλάσσονται. Για να πάρουμε περισσότερα στοιχεία από τις συναλλαγές που εμφανίζονται σε αυτό το αρχείο, θα πρέπει να εισάγουμε το αναγνωριστικό της κάθε συναλλαγής σε κάποιον εξερευνητή της αλυσίδας blockchain του Bitcoin.

Σημείωση: *Εξερευνώντας μία μία τις συναλλαγές που εμφανίζονται στο παραπάνω αρχείο παρατηρούμε ότι δύο από τις συναλλαγές δεν είναι δυνατό να ανευρεθούν στον εξερευνητή γιατί έχουν λανθασμένο αριθμό κατακερματισμού, ενώ δεν περιλαμβάνονται όλες οι συναλλαγές που πραγματοποιήσαμε στο πορτοφόλι, αλλά κάποιες εξ' αυτών. Υποθέτουμε ότι, οι συναλλαγές που δεν βρίσκονται στον εξερευνητή, αποτελούν συναλλαγές που συμπεριλήφθηκαν αρχικά σε κάποιο μπλόκ, το οποίο απορρίφθηκε στη συνέχεια από τους εξορύκτες και δεν συμπεριλήφθηκε στην αλυσίδα των μπλοκ του bitcoin, αλλά δεν μπορεί να δικαιολογηθεί ο λόγος αποθήκευσής τους.*

Τα περιεχόμενα του αρχείου παρουσιάζονται στην επόμενη εικόνα (Στιγμιότυπο 21).

transaction_fiat_value.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f">5.02 USD</string>
    <string name="3b8abfd1de4e07a8bf3638522767acb0ff7032511803c71f48c3d464c4946b87">61.32 USD</string>
    <string name="3a1636d31ff657f317028b8e7fbf925ef1e51c6e532f0a6476285b87039690fb">61.71 USD</string>
    <string name="994cb3b9df4824ca66d140b293134a4b537cb62418e23478c02c5e43440fc726">5.14 USD</string>
    <string name="8f020a1bfb91a7ed5b53e3674f685d1238fb97ecc414ddf3577e502e40a5ed91">5.13 USD</string>
</map>
```

Στιγμιότυπο 21 - Αναγνωριστικά (id) και αξίας σε δολάρια συναλλαγών bitcoin που πραγματοποιήθηκαν με την εφαρμογή Mycelium

Το αρχείο /databases/mds.db, είναι μία βάση δεδομένων SQLite, η οποία περιέχει έναν πίνακα με όνομα keyValueStore. Από τον πίνακα ενδιαφέρον παρουσιάζουν ορισμένα στοιχεία, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 22).

5	52d5249c-ea01-222e-8cea-8928208ca0b2	al	Exchange profits
6	coinsupplyLaA8aiRBha2BcC6PCqMuK8xzZqdA3Lb6VVv41K	exchange_rates	6567.5
7	21dc519d-292f-07cd-851d-4b2c787a9ce8	al	Shop1
8	f7868247f4bdcbe770aaf8c100c807ec21ddf42244c473c8ab05b42d56165da4	tl	Donations
9	coinsupplyLaA8aiRBha2BcC6PCqMuK8xzZqdA3Lb6VVv41K	colu_data	5311.0000000
10	coinsupplyLa4szjzKfJyHQ75qgDEnbzp4qY8GQeDR5Z7h2W	colu_data	1000000000000
11	coinsupplyLa4aGUPuNKZyC393pS2Nb4RJdk2WvmoaAdrRLZ	colu_data	10756.8259
12	lastFull	sync	1530126085609

Στιγμιότυπο 22 - Στοιχεία λογαριασμών του χρήστη και ώρα συγχρονισμού με το δίκτυο - Mycelium

Παρατηρώντας τα στοιχεία του πίνακα μπορούμε να δούμε σε πιο όνομα λογαριασμού αντιστοιχεί η κάθε συμβολοσειρά που του έχει δοθεί από την εφαρμογή, καθώς και την τελευταία φορά που ο χρήστης συγχρόνισε το πορτοφόλι του με το δίκτυο με την μορφή Linux epoch time. Έτσι η συμβολοσείρα "52d5249c-ea01-222e-8cea-8928208ca0b2" ανήκει στον λογαριασμό με όνομα "Exchange profits", ενώ η συμβολοσειρά "21dc519d-292f-07cd-851d-4b2c787a9ce8", στον λογαριασμό με όνομα "Shop1", που όπως είδαμε παραπάνω είναι ο επιλεγμένος λογαριασμός του χρήστη. Η τελευταία φορά που η εφαρμογή συγχρονίστηκε με το δίκτυο είναι 1530126085609, που αντιστοιχεί στην ημερομηνία Τετάρτη 27 Ιουνίου 2018, ώρα 10:01:25 PM.

Το αρχείο /databases/walletbacking.db, είναι μία βάση δεδομένων SQLite, που περιέχει 14 πίνακες όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 23). Εξετάζοντας τους πίνακες παρατηρούμε ότι δεν μπορούμε να διαβάσουμε τα δεδομένα των πινάκων γιατί πιθανόν έχουν κρυπτογραφηθεί με την εγκατάσταση της εφαρμογής.

Στιγμιότυπο 23 - Ονόματα πινάκων που περιέχονται στην βάση δεδομένων walletbacking της εφαρμογής Mycelium

Στις παρακάτω εικόνες θα δούμε κάποια από τα δεδομένα που μπορούμε να εξάγουμε από όσους πίνακες παρουσιάζουν ενδιαφέρον στην δοκιμή μας.

Πίνακας - bip44 -

Από το όνομα του πίνακα καταλαβαίνουμε ότι αφορά την πρόταση βελτίωσης του Bitcoin με αριθμό 44 (Bitcoin Improvement Proposal - bip44), η οποία αναφέρεται στους πολλαπλούς λογαριασμούς που μπορούν να δημιουργηθούν στα Ιεραρχικά Ντετερμινιστικά Πορτοφόλια. Στην κάτωθι εικόνα (Στιγμιότυπο 24) βλέπουμε ότι έχουν δημιουργηθεί δύο λογαριασμοί, βλέπουμε την ημερομηνία που δημιουργήθηκαν με την μορφή Linux epoch time, πλην όμως δεν μπορούμε να δούμε ούτε την συμβολοσειρά τους ούτε τα ονόματά τους.

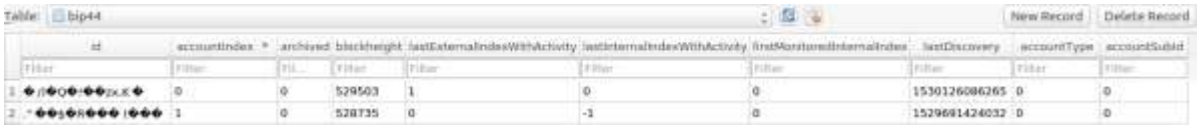


Table: bip44 — New Record — Delete Record

id	accountIndex	archived	blockHeight	lastExternalIndexWithActivity	lastInternalIndexWithActivity	firstMonitoredInternalIndex	lastDiscovery	accountType	accountSubId
1	0	0	529503	1	0	0	1530126086265	0	0
2	1	0	528735	0	-1	0	1529691424032	0	0

Στιγμιότυπο 24 - Δεδομένα του πίνακα bip44

Πίνακας - kv -

Ο πίνακας με το όνομα - kv - περιέχει 191 σειρές με δεδομένα όπως ενδεικτικά φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 25).

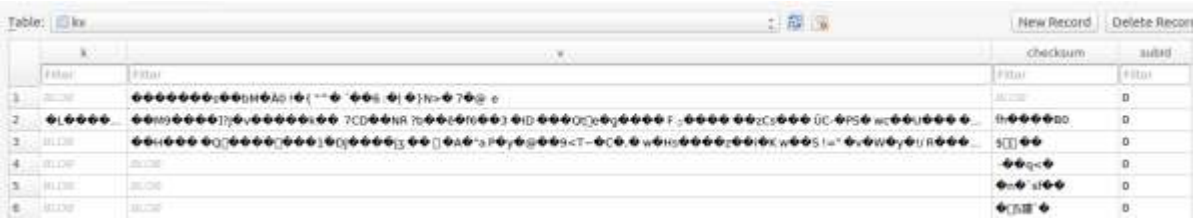


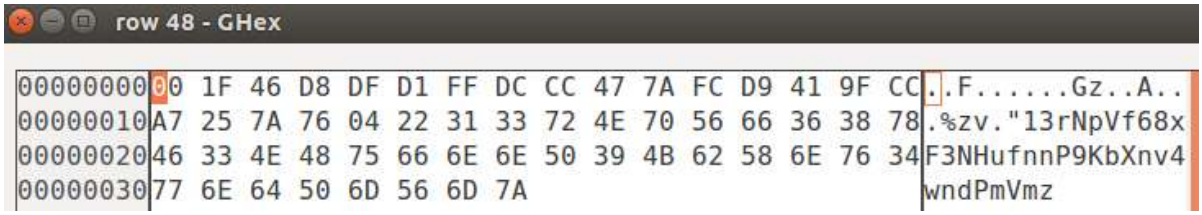
Table: kv — New Record — Delete Record

k	v	checksum	subId
1			0
2			0
3			0
4			0
5			0
6			0

Στιγμιότυπο 25 - Ενδεικτική απεικόνιση δεδομένων του πίνακα kv

Τα περισσότερα από αυτά τα δεδομένα είναι κρυπτογραφημένα και δεν μπορούμε να τα αναγνώσουμε, όμως αν παρατηρήσουμε προσεχτικά, σε κάποια από τα κελιά της στήλης - v- μπορούμε να διακρίνουμε κάποιες bitcoin διευθύνσεις, όπως ενδεικτικά φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 26). Οι διευθύνσεις αυτές αποτελούν κάποιες από τις διευθύνσεις που έχει δημιουργήσει το πορτοφόλι μας και αφορούν και τους δύο λογαριασμούς που είχαμε δημιουργήσει. Ανάμεσα στις διευθύνσεις αυτές βρίσκονται και οι

διευθύνσεις που χρησιμοποιήθηκαν για την αποστολή και τη λήψη bitcoin από το πορτοφόλι μας. Για να δούμε αναλυτικά τις συναλλαγές που πραγματοποιήθηκαν από το πορτοφόλι μας, θα πρέπει να εξερευνήσουμε μία μία τις διευθύνσεις αυτές σε κάποιον εξερευνητή της αλυσίδας blockchain του Bitcoin, που όμως δεν αποτελεί αντικείμενο αυτής της ανάλυσης και δεν θα το παρουσιάσουμε. Ωστόσο, ο συνδυασμός των διευθύνσεων του πορτοφολιού, με τις διευθύνσεις που χρησιμοποιήθηκαν για τις συναλλαγές, μπορούν να μας δώσουν στοιχεία για τις συναλλαγές που έγιναν από τον χρήστη, καθώς και το υπόλοιπο του πορτοφολιού.



Στιγμιότυπο 26 - Στοιχεία bitcoin διεύθυνσης του πορτοφολιού που βρίσκεται αποθηκευμένη στον πίνακα kv

Πίνακας - ptxo_2e2201ea9c24d552b2a08c202889ea8c -

Ο πίνακας αυτός περιλαμβάνει τις συναλλαγές που αφορούν τον λογαριασμό με όνομα "Exchange profits". Αναλύοντας την παρακάτω εικόνα (Στιγμιότυπο 27), όπου μπορούμε να δούμε τα δεδομένα του, βλέπουμε δύο συναλλαγές που συμπεριλήφθηκαν στο ίδιο μπλοκ συναλλαγών στη στήλη "height", καθώς και τα ποσά που συναλλάχθηκαν εκφρασμένα σε satoshi στη στήλη "value". Αν τα δεδομένα αυτά συνδυαστούν με τα δεδομένα του εξερευνητή της αλυσίδας Bitcoin, μπορούμε να εξάγουμε περισσότερα συμπεράσματα για το πορτοφόλι μας.


Table: ptxo_2e2201ea9c24d552b2a08c202889ea8c

	outpoint	height	value	isCoinbase	script
	Filter	Filter	Filter	Filter	Filter
1	BLOB	527114	75093	0	v F Gz A %zv
2	BLOB	527114	74775	0	v bM4w Y<2 P r

Στιγμιότυπο 27 - Απεικόνιση ύψους μπλοκ συναλλαγών και αξία των συναλλαγών σε satoshi του λογαριασμού "Exchange profits"

Πίνακας - ptxo_cd072f299d51dc21e89c7a782c4b1d85 -

Ομοίως, στην παρακάτω εικόνα (Στιγμιότυπο 28) βλέπουμε τις συναλλαγές που έγιναν και αφορούν τον λογαριασμό με όνομα "Shop1" του πορτοφολιού μας. Στην παρακάτω εικόνα μπορούμε να διακρίνουμε το μπλοκ στο οποίο συμπεριλήφθηκαν καθώς και την αξία τους σε satoshi. Για να εξάγουμε περισσότερα συμπεράσματα, θα πρέπει κι εδώ να συνδυάσουμε τα δεδομένα αυτά με τα στοιχεία που μπορούμε να δούμε σε κάποιον εξερευνητή της αλυσίδας Bitcoin.

Table: ptxo_cd072f299d51dc21e89c7a782c4b1d85

	outpoint	height	value	isCoinbase	script
	Filter	Filter	Filter	Filter	Filter
1	BLOB	526900	3644594	0	v\x00 \x00\x00\x00r\x00\x00\x00\x00\x00\x00\x00\x00}!R\x00\x00\x00
2	BLOB	527014	975467	0	v\x00 I\x00 \x00fp \x00\x00pwNb \x00\x00\x00
3	BLOB	-1	75093	0	v\x00 F\x00\x00\x00\x00\x00\x00\x00Gz\x00\x00A\x00%zv \x00\x00
4	BLOB	527216	300000	0	v\x00 kVg5{\x00c,[jK*\x00H\x00z6aA*\x00\x00

Στιγμιότυπο 28 - Απεικόνιση ύψους μπλοκ συναλλαγών και αξία των συναλλαγών σε satoshi του λογαριασμού "Shop1"

Πίνακας - tx_2e2201ea9c24d552b2a08c202889ea8c -

Ο πίνακας αφορά όπως προαναφέραμε τον λογαριασμό με όνομα "Exchange profits". Στον πίνακα αυτόν, φαίνονται σε μορφή απλού κειμένου μόνο το μπλοκ των συναλλαγών και η ώρα σε μορφή Linux epoch time (Στιγμιότυπο 29). Τα στοιχεία αυτά από μόνα τους δεν φαίνονται ιδιαίτερα σημαντικά εκ πρώτης όψεως, όμως θα μπορούσαν να συνδυαστούν με τα υπόλοιπα δεδομένα, καθώς και τα στοιχεία του εξερευνητή της αλυσίδας Bitcoin και να μας δώσουν σημαντικά ευρήματα. Η ανάλυση αυτή δεν αποτελεί κομμάτι αυτής της εργασίας και δεν θα αναλυθεί περαιτέρω η διαδικασία.

Table: tx_2e2201ea9c24d552b2a08c202889ea8c

	id	height	time	binary
	Filter	Filter	Filter	Filter
1	\x00 \x00\x00\x00\x00[S\x00gOh] 8\x00\x00\x00\x00 \x00\x00W~P.@\x00...	527114	1528796020	BLOB
2	h\x00U\x00\x00\x00j(\x00\x00\h Q\x00\x00 \x00 1\x00\x00B5 D\x00\x00\x00 \x00O	527171	1528829070	BLOB

Στιγμιότυπο 29 - Ύψος του μπλοκ συναλλαγών και ώρα συναλλαγών του λογαριασμού Exchange profits

Πίνακας - tx_cd072f299d51dc21e89c7a782c4b1d85 -

Ομοίως με τα παραπάνω, τα δεδομένα αυτού του πίνακα αφορούν τον λογαριασμό με όνομα "Shop1" και φαίνονται στην παρακάτω εικόνα (Στιγμιότυπο 30).

Table: tx_cd072f299d51dc21e89c7a782c4b1d85

	id	height	time	binary
	Filter	Filter	Filter	Filter
1	BLOB	527014	1528738530	BLOB
2	:6 W ^ nS/dv([	527114	1528796020	BLOB
3	[S gOh] 8 W~P.@...	527114	1528796020	BLOB
4	A /8 #W ä\ 9CS*h [Z	527517	1529039779	BLOB

Στιγμιότυπο 30 - Ύψος του μπλοκ συναλλαγών και ώρα συναλλαγών του λογαριασμού "Shop1"

Πίνακας - utxo_cd072f299d51dc21e89c7a782c4b1d85 -

Ο πίνακας αυτός περιέχει, όπως δηλώνει και το όνομά του, τις αξόδευτες εξόδους (unspent outputs) του πορτοφολιού μας και επομένως μπορούμε να δούμε το υπόλοιπο του πορτοφολιού εκφρασμένο σε satoshi στην στήλη value, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 31). Από το όνομα του πίνακα συμπεραίνουμε ότι αφορά τον λογαριασμό με όνομα "Shop1" και το υπόλοιπο βρίσκεται μόνο σε αυτόν τον λογαριασμό, καθόσον ο αντίστοιχος πίνακας που αφορά τον λογαριασμό με όνομα "Exchange profits" είναι κενός.

Table: utxo_cd072f299d51dc21e89c7a782c4b1d85

	outpoint	height	value	isCoinbase	script
	Filter	Filter	Filter	Filter	Filter
1	BLOB	527517	150000	0	v ?[Ν; h=v Ъ

Στιγμιότυπο 31 - Αξία των αξόδευτων εξόδων του λογαριασμού με όνομα Shop1 εκφρασμένες σε satoshi - Υπόλοιπο λογαριασμού

Το αρχείο /databases/walletbacking.db-journal, είναι το journal αρχείο της βάσης δεδομένων walletbacking.db και δεν περιέχει κάποιο επιπλέον δεδομένο άξιο αναφοράς.

Επαναφορά πορτοφολιού από Backup - Mycelium Bitcoin Wallet

Το επόμενο πράγμα που θα εξετάσουμε στην εφαρμογή Mycelium Wallet είναι η διαγραφή της από το κινητό μας τηλέφωνο, η επανεγκατάσταση της και η επαναφορά του πορτοφολιού που εξετάσαμε προηγουμένως, από το backup που έχουμε κρατήσει

Χρησιμοποιώντας και πάλι το εργαλείο ADB, εξάγουμε τα αρχεία που βρίσκονται στο πακέτο εγκατάστασης της εφαρμογής, τα οποία απαρτίζονται από τους φακέλους (code_cache, databases, files και shared_prefs).

Από αυτούς τους φακέλους ενδιαφέρον παρουσιάζουν οι φάκελοι με τα παρακάτω αρχεία:

- com.mycelium.wallet/shared_prefs/
  settings.xml
- com.mycelium.wallet/databases/
  mds.db
  walletbacking.db
  walletbacking.db-journal

Παρατηρούμε ότι, το αρχείο /shared_prefs/transaction_fiat_value.xml που περιείχε το αναγνωριστικό (id) των συναλλαγών του πορτοφολιού μας συνοδευόμενο από την αξία του ποσού της συναλλαγής σε δολάρια, μετά την επαναφορά του backup δεν υπάρχει.

Το αρχείο /shared_prefs/settings.xml, όπως και προηγουμένως μπορεί να μας δώσει στοιχεία σχετικά με τον λογαριασμό που έχει επιλεγμένο ο χρήστης στο πορτοφόλι του και από τα στοιχεία που έχουμε από την προηγούμενη ανάλυσή μας, όπως βλέπουμε στην παρακάτω εικόνα (Στιγμιότυπο 32), είναι ο “21dc519d-292f-07cd-851d-4b2c787a9ce8”, ο οποίος αντιστοιχούσε στον λογαριασμό με όνομα “Shop1”.

settings.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="selectedAccount">21dc519d-292f-07cd-851d-4b2c787a9ce8</string>
    <string name="MinerFeeEstimationSetting">ECONOMIC</string>
    <string name="user_language">en</string>
    <string name="tor_mode">ONLY_HTTPS</string>
    <set name="selectedFiatCurrencies">
        <string>USD</string>
    </set>
</map>
```

Στιγμιότυπο 32 - id επιλεγμένου λογαριασμού χρήστη και οι ρυθμίσεις του μετά την επαναφορά του πορτοφολιού από backup - Mycelium

Το αρχείο /databases/mds.db, είναι μία βάση δεδομένων SQLite, η οποία περιέχει έναν πίνακα με όνομα keyValueStore. Από τον πίνακα, ενδιαφέρον παρουσιάζουν ορισμένα στοιχεία του πίνακα όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 33).

2	seed	backupstate	1
3	21dc519d-292f-07cd-851d-4b2c787a9ce8	al	Λογαριασμός 1
4	lastFull	sync	1531011129020
5	ui	show_bip44_path	1
6	simplex	enable	0
7	glidera	enable	0

Στιγμιότυπο 33 - Στοιχεία λογαριασμών του χρήστη και ώρας συγχρονισμού με το δίκτυο μετά την επαναφορά του backup - Mycelium

Παρατηρώντας τα στοιχεία του πίνακα διαπιστώνουμε ότι μετά την επαναφορά του πορτοφολιού από το backup, επαναφέρθηκε στην εφαρμογή μόνο ο ένας από τους δύο λογαριασμούς που διατηρούσαμε στο πορτοφόλι μας (υποθέτουμε αυτό έγινε γιατί στον δεύτερο λογαριασμό δεν υπήρχε υπόλοιπο bitcoin) και το όνομα του λογαριασμού επανήλθε στον προεπιλεγμένο της εφαρμογής με όνομα “Λογαριασμός 1”. Όπως και προηγουμένως μπορούμε να δούμε την τελευταία φορά που συγχρονίστηκε το πορτοφόλι μας με το δίκτυο, δηλαδή 1531011129020, που αντιστοιχεί στην ημερομηνία Κυριακή 8 Ιουλίου, ώρα 3:52:09.020 AM.

Το αρχείο /databases/walletbacking.db, περιέχει 9 πίνακες αυτή την φορά καθότι δεν έχουν δημιουργηθεί οι πίνακες που αφορούσαν τον δεύτερο λογαριασμό που είχαμε δημιουργήσει, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 34). Εξετάζοντας τους πίνακες παρατηρούμε ότι δεν μπορούμε να διαβάσουμε τα δεδομένα των πινάκων γιατί πιθανόν έχουν κρυπτογραφηθεί με την εγκατάσταση της εφαρμογής.

Στιγμιότυπο 34 - Πίνακες της βάσης δεδομένων walletbacking που δημιουργήθηκαν μετά την επαναφορά του πορτοφολιού από backup - Mycelium

Στις παρακάτω εικόνες θα δούμε κάποια από τα δεδομένα που μπορούμε να εξάγουμε από όσους πίνακες παρουσιάζουν ενδιαφέρον στην δοκιμή μας.

Πίνακας - bip44 -

Από το όνομα του πίνακα καταλαβαίνουμε ότι αφορά την πρόταση βελτίωσης του Bitcoin με αριθμό 44 (Bitcoin Improvement Proposal – bip44), η οποία αναφέρεται στους πολλαπλούς λογαριασμούς που μπορούν να δημιουργηθούν στα Ιεραρχικά Ντετερμινιστικά Πορτοφόλια. Στην κάτωθι εικόνα (Στιγμιότυπο 35) βλέπουμε ότι υπάρχει μόνο ο ένας λογαριασμός (για τον λόγο που αναφέρθηκε παραπάνω) καθώς και την ώρα που επαναφέρθηκε στην εφαρμογή με την μορφή Linux epoch time.

Table: bip44

	id	accountIndex	archived	blockheight	nalIndexWith	nalIndexWith	nitoredInterna	lastDiscovery	accountType	accountSubId
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	◆□)◆Q◆!...	0	0	530961	1	0	0	1531011242356	0	0

Στιγμιότυπο 35 - Δεδομένα του πίνακα bip44 μετά την επαναφορά από backup - Mycelium

Πίνακας - kv -

Ο πίνακας με το όνομα - kv - περιέχει 98 σειρές με δεδομένα όπως ενδεικτικά φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 36).

Table: kv

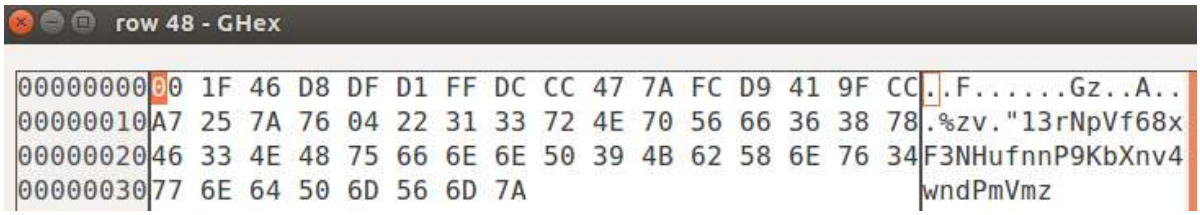
New Record | Delete Recor

	k	v	checksum	subid
	Filter	Filter	Filter	Filter
1		◆◆◆◆◆◆◆◆ε◆◆bM◆A0 !◆(""◆ `◆◆ε .◆[◆)N>◆ 7◆@ e		0
2	◆L◆◆◆◆...	◆◆W◆◆◆◆I]p◆v◆◆◆◆◆ε◆◆ 7CD◆◆NR 7b◆◆◆p◆M◆◆◆)◆ID◆◆◆O□e◆g◆◆◆◆ F ,◆◆◆◆ ◆◆zCs◆◆◆ ÜC◆P5◆ wc◆◆U◆◆◆◆...	th◆◆◆◆B0	0
3		◆◆H◆◆◆ ◆Q□◆◆◆□◆◆◆1◆D◆◆◆◆◆I3◆◆ □◆A◆'a.P◆y◆@◆◆9<T−◆C◆.◆ w◆Ho◆◆◆◆ε◆◆I◆K w◆◆5 !«" ◆.◆W◆y◆U R◆◆◆...	$□◆◆	0
4			-◆◆q<◆	0
5			◆=◆`sI◆◆	0
6			◆□I◆	0

Στιγμιότυπο 36 - Ενδεικτικά δεδομένα του πίνακα kv μετά την επαναφορά του πορτοφολιού από backup - Mycelium

Όπως αναφέραμε και στην προηγούμενη δοκιμή μας, τα περισσότερα από αυτά τα δεδομένα είναι κρυπτογραφημένα και δεν μπορούμε να τα αναγνώσουμε. Όμως, αν παρατηρήσουμε προσεχτικά σε κάποια από τα κελιά της στήλης -v- μπορούμε να διακρίνουμε κάποιες bitcoin διευθύνσεις, όπως ενδεικτικά φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 37). Οι διευθύνσεις αυτές αποτελούν κάποιες από τις διευθύνσεις που έχει

δημιουργήσει το πορτοφόλι μας, απουσιάζουν όμως οι διευθύνσεις του δεύτερου λογαριασμού που είχαμε και υπολείπονται σε αριθμό από πριν. Και πάλι όπως και πριν για να δούμε αναλυτικά τις συναλλαγές που πραγματοποιήθηκαν από το πορτοφόλι μας, θα πρέπει να εξερευνήσουμε μία μία τις διευθύνσεις αυτές σε κάποιον εξερευνητή της αλυσίδας blockchain του Bitcoin, που όμως δεν αποτελεί αντικείμενο αυτής της ανάλυσης και δεν θα το παρουσιάσουμε. Ωστόσο, ο συνδυασμός των διευθύνσεων του πορτοφολιού, με τις διευθύνσεις που χρησιμοποιήθηκαν για τις συναλλαγές, μπορούν να μας δώσουν στοιχεία για τις συναλλαγές που έγιναν από τον χρήστη, καθώς και το υπόλοιπο του πορτοφολιού.



Στιγμιότυπο 37 - Στοιχεία bitcoin διεύθυνσης του πορτοφολιού που βρίσκεται αποθηκευμένη στον πίνακα kv μετά την επαναφορά του πορτοφολιού από backup - Mycelium

Πίνακας - ptxo_cd072f299d51dc21e89c7a782c4b1d85 -

Ο πίνακας αυτός παραμένει σχεδόν ίδιος με πριν, περιλαμβάνοντας τις συναλλαγές που έγιναν από το πορτοφόλι μας και αφορούν τον λογαριασμό που πριν είχε το όνομα “Shop1”, ενώ τώρα έχει επανέλθει στο προεπιλεγμένο “Λογαριασμός 1”. Στην παρακάτω εικόνα (Στιγμιότυπο 38) βλέπουμε το μπλοκ στο οποίο συμπεριλήφθηκαν καθώς και την αξία τους σε satoshi. Για να εξάγουμε περισσότερα συμπεράσματα, θα πρέπει κι εδώ να συνδυάσουμε τα δεδομένα αυτά με τα στοιχεία που μπορούμε να δούμε σε κάποιον εξερευνητή της αλυσίδας Bitcoin.


Table: ptxo_cd072f299d51dc21e89c7a782c4b1d85

	outpoint	height	value	isCoinbase	script
	Filter	Filter	Filter	Filter	Filter
1	BLOB	527216	300000	0	v kVg5{c,[jK*H z6aA*
2	BLOB	527114	75093	0	v F Gz A %zv
3	BLOB	527014	975467	0	v I fp pwNb
4	BLOB	526900	3644594	0	v r !R

Στιγμιότυπο 38 - Απεικόνιση ύψους μπλοκ συναλλαγών και της αξίας τους σε satoshi μετά την επαναφορά του backup - Mycelium

Πίνακας - tx_cd072f299d51dc21e89c7a782c4b1d85 -

Ο πίνακας δεν έχει τροποποιηθεί καθόλου και εμφανίζει το μπλοκ των συναλλαγών και την ώρα σε μορφή Linux epoch time, που πραγματοποιήθηκαν από τον λογαριασμό με όνομα "Λογαριασμός 1" (Στιγμιότυπο 39). Τα στοιχεία αυτά από μόνα τους δεν φαίνονται ιδιαίτερα σημαντικά εκ πρώτης όψεως, όμως θα μπορούσαν να συνδυαστούν με τα υπόλοιπα δεδομένα, καθώς και τα στοιχεία του εξερευνητή της αλυσίδας Bitcoin και να μας δώσουν σημαντικά ευρήματα. Η εργασία αυτή δεν αποτελεί κομμάτι αυτής της ανάλυσης και δεν θα αναλυθεί περαιτέρω η διαδικασία.

Table: tx_cd072f299d51dc21e89c7a782c4b1d85

	id	height	time	binary
	Filter	Filter	Filter	Filter
1	` [S gOh] 8 W~P.@`	527114	1528796020	BLOB
2	`: 6 W  nS/dv([`	527114	1528796020	BLOB
3	BLOB	527014	1528738530	BLOB
4	` A /8 #W ə\ 9CS*h [ Z`	527517	1529039779	BLOB

Στιγμιότυπο 39 - Ύψος του μπλοκ συναλλαγών και ώρα συναλλαγών του λογαριασμού με όνομα Λογαριασμός 1 - Mycelium

Πίνακας - utxo_cd072f299d51dc21e89c7a782c4b1d85 -

Ομοίως, ο πίνακας αυτός δεν έχει τροποποιηθεί καθόλου. Περιέχει, τις αξόδευτες εξόδους (unspent outputs) του πορτοφολιού μας και επομένως μπορούμε να δούμε το υπόλοιπο του πορτοφολιού εκφρασμένο σε satoshi στην στήλη value, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 40). Από το όνομα του πίνακα συμπεραίνουμε ότι αφορά τον λογαριασμό με όνομα "Λογαριασμός 1".

Table: utxo_cd072f299d51dc21e89c7a782c4b1d85

	outpoint	height	value	isCoinbase	script
	Filter	Filter	Filter	Filter	Filter
1	BLOB	527517	150000	0	`v ?[ N; h=v Ъ`

Στιγμιότυπο 40 - Αξία των αξόδευτων εξόδων του λογαριασμού μας εκφρασμένες σε satoshi μετά την επαναφορά από backup - Mycelium

Το αρχείο /databases/walletbacking.db-journal, είναι το journal αρχείο της βάσης δεδομένων walletbacking.db και δεν περιέχει κάποιο επιπλέον δεδομένο άξιο αναφοράς.

Ορισμός κωδικού (pin) στο πορτοφόλι που επαναφέραμε μετά το Backup - Mycelium Bitcoin Wallet

Όπως είδαμε στις προηγούμενες αναλύσεις μας για την εφαρμογή Mycelium Bitcoin Wallet, τα περισσότερα δεδομένα διατηρούνται στο κινητό μας τηλέφωνο κρυπτογραφημένα με την εγκατάσταση της εφαρμογής, ωστόσο η εφαρμογή δίνει την δυνατότητα να ορίσουμε κωδικό, προκειμένου να αποτρέψουμε την πρόσβαση στην αποστολή bitcoin και την εξαγωγή των ιδιωτικών κλειδιών του πορτοφολιού από οποιονδήποτε χρήστη μέσα από το μενού της εφαρμογής.

Αφού ορίσουμε κωδικό στο πορτοφόλι που επαναφέραμε από το backup, εξάγουμε τους φακέλους του πακέτου της εφαρμογής κάνοντας χρήση του εργαλείου ADB. Οι φάκελοι που εξάγονται είναι όπως και προηγουμένως οι (code_cache, databases, files και shared_prefs).

Εξετάζοντας τα αρχεία των φακέλων και συγκρίνοντάς τα με τα αρχεία που εξάγαμε από την επαναφορά του backup, παρατηρούμε ότι τα περισσότερα από αυτά παραμένουν αναλλοίωτα. Επομένως, ο κωδικός που ορίσαμε δεν κρυπτογραφεί κάποια επιπλέον στοιχεία του πορτοφολιού μας.

Αυτό που παρουσιάζει ιδιαίτερο ενδιαφέρον στην εξέταση της εφαρμογής μετά τον ορισμό κωδικού, είναι το αρχείο com.mycelium.wallet/shared_prefs/settings.xml. Το αρχείο αυτό έχει τροποποιηθεί και περιέχει στα δεδομένα του τον κωδικό που ορίσαμε, σε μορφή απλού κειμένου, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 41).

settings.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="MinerFeeEstimationSetting">ECONOMIC</string>
    <string name="tor_mode">ONLY_HTTPS</string>
    <string name="PinResettable">0</string>
    <int name="failedPinCount" value="1" />
    <string name="PIN">123456</string>
    <string name="selectedAccount">21dc519d-292f-07cd-851d-4b2c787a9ce8</string>
    <string name="user_language">en</string>
    <set name="selectedFiatCurrencies">
        <string>USD</string>
    </set>
</map>
```

Στιγμιότυπο 41 - Στοιχεία του κωδικού που εισάγαμε στην εφαρμογή Mycelium σε μορφή απλού κειμένου

Αυτό είναι ιδιαίτερα σημαντικό για την εγκληματολογική εξέταση της εφαρμογής, γιατί μας δίνεται η δυνατότητα να μετακινήσουμε τα bitcoin του χρήστη σε κάποιο άλλο πορτοφόλι, ακόμη και αν ο χρήστης είχε ορίσει κωδικό που θα έπρεπε να απέτρεπε κάτι τέτοιο.

Εφαρμογή Coinomi - Bitcoin Altcoin Wallet

Εγκατάσταση της εφαρμογής Coinomi

Η εφαρμογή βρίσκεται στο Play Store και την στιγμή των δοκιμών βρισκόταν στην έκδοση v1.8.2. Σύμφωνα με τους δημιουργούς του, ο πηγαίος κώδικας του Coinomi είναι ανοικτός και διαθέσιμος στο internet, χωρίς ωστόσο να δίνεται ο σύνδεσμος που παραπέμπει στον κώδικα, τουλάχιστον κατά την περιγραφή της εφαρμογής στο Play Store. Ακολουθεί την ντετερμινιστική ιεραρχική δημιουργία διευθύνσεων bitcoin, είναι δηλαδή ένα Hierarchical Deterministic Wallet (HD). Εκτός από Bitcoin Wallet, είναι και Altcoin Wallet, δηλαδή υποστηρίζει την αποθήκευση και διαχείριση και άλλων κρυπτονομισμάτων, μέσα από το ίδιο πορτοφόλι. Η εφαρμογή είναι αρκετά δημοφιλής στο Play Store και έχει περίπου 500.000+ λήψεις σύμφωνα με τα στοιχεία της Google.

Κατά την είσοδο στην εφαρμογή δίνεται η επιλογή της δημιουργίας καινούριου πορτοφολιού ή η ανάκτηση πορτοφολιού από backup. Συνεχίζοντας με την δημιουργία νέου πορτοφολιού (Στιγμιότυπο 42), η εφαρμογή δημιουργεί την φράση ανάκτησης από την οποία παράγονται τα κλειδιά του πορτοφολιού μας και μας προτρέπει να την αποθηκεύσουμε, προκειμένου να μπορούμε να ανακτήσουμε το πορτοφόλι μας μελλοντικά, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 43). Στη συνέχεια η εφαρμογή ζητάει την εισαγωγή κωδικού για την προστασία του πορτοφολιού από την καθημερινή χρήση, το οποίο μπορεί να παραλειφθεί σαν βήμα (Στιγμιότυπο 44). Για τις ανάγκες της δοκιμής μας επιλέξαμε την παράλειψη της εισαγωγής κωδικού και εισήλθαμε στο μενού της εφαρμογής όπου μας εμφανίστηκε μια διεύθυνση bitcoin για την λήψη χρημάτων στο πορτοφόλι μας (Στιγμιότυπο 45).

Στιγμιότυπο 42 - Δημιουργία νέου πορτοφολιού Coinomi

Στιγμιότυπο 43 - Μνημονική φράση για την ανάκτηση του πορτοφολιού - Coinomi

Στιγμιότυπο 44 - Παράλειψη εισαγωγής κωδικού για την προστασία του πορτοφολιού - Coinomi

Στιγμιότυπο 45 - Προβολή διεύθυνσης για λήψη bitcoin - Coinomi

Μετά την εγκατάστασή της, πραγματοποιήσαμε ορισμένες συναλλαγές, όπως ενδεικτικά φαίνεται στις παρακάτω εικόνες (Στιγμιότυπο 46 και Στιγμιότυπο 47).

Στιγμιότυπο 46 - Συναλλαγές που πραγματοποιήθηκαν με την εφαρμογή Coinomi

Στιγμιότυπο 47 - Λεπτομέρειες συναλλαγής που πραγματοποιήθηκε με την εφαρμογή Coinomi

Εγκληματολογική εξέταση της εφαρμογής Coinomi

Για την εγκληματολογική εξέταση της εφαρμογής, θα χρησιμοποιήσουμε την λογική μέθοδο απόκτησης, κάνοντας χρήση του εργαλείου της γέφυρας εντοπισμού σφαλμάτων του Android (Android Debug Bridge), όπως και στα προηγούμενα παραδείγματά μας.

Το όνομα του πακέτου εγκατάστασης της εφαρμογής είναι το "com.coinomi.wallet" και κατά την εγκατάσταση η εφαρμογή δημιουργεί τον ομώνυμο φάκελο στην διαδρομή του καταλόγου /data/data.

Συνδέουμε το κινητό τηλέφωνο με τον υπολογιστή και με την χρήση του ADB εξαγάγουμε τους φακέλους που βρίσκονται στον ανωτέρω κατάλογο.

Ο φάκελος "com.coinomi.wallet" που εξήχθη από την διαδρομή /data/data περιέχει τους φακέλους (cache, code_cache, databases, files και shared_prefs).

Από αυτούς τους φακέλους ενδιαφέρον παρουσιάζουν οι φάκελοι με τα αρχεία:

- com.coinomi.wallet/cache/http_cache
  54bee67516952cd491c8e8b6d350b3fd.0
- com.coinomi.wallet/databases
  address_book
- com.coinomi.wallet/files/
  wallet

Το αρχείο cache/http_cache/54bee67516952cd491c8e8b6d350b3fd.0, είναι ένα αρχείο καταγραφής που μπορεί να μας δώσει πληροφορίες σχετικά με την τελευταία φορά που ο χρήστης εισήλθε στην εφαρμογή καθώς μας δείχνει την ημερομηνία που η εφαρμογή συνδέθηκε με τους servers της εταιρείας. Η ώρα εμφανίζεται ως GMT, οπότε πρέπει να γίνει η αντίστοιχη μετατροπή για να βρούμε την τοπική ώρα. Στο παράδειγμά μας παρατηρούμε ότι η ημερομηνία σύνδεσης του χρήστη στην εφαρμογή είναι Κυριακή, 8 Ιουλίου 2018, ώρα 19:50:23 GMT, που αντιστοιχεί στην τοπική ώρα 22:50:23. Τα δεδομένα αυτού του αρχείου φαίνονται στην παρακάτω εικόνα (Στιγμιότυπο 48).

Στιγμιότυπο 48 - Αρχείο καταγραφής που εμφανίζει την ώρα σύνδεσης του χρήστη στην εφαρμογή Coinomi

Το αρχείο com.coinomi.wallet/databases/address_book, είναι μια βάση δεδομένων SQLite, η οποία περιέχει 3 πίνακες. Ο ένας εξ' αυτών με όνομα address_book περιέχει τις 3 διευθύνσεις που χρησιμοποιήθηκαν από το πορτοφόλι μας προκειμένου να λάβουμε χρήματα, καθώς και το όνομα ετικέτας που δόθηκε σε κάθε διεύθυνση από το μενού της εφαρμογής, καθαρά με σκοπό την διευκόλυνση του χρήστη κατά την χρήση της εφαρμογής. Στην παρακάτω εικόνα (Στιγμιότυπο 49) παρατηρούμε ότι δύο από τις διευθύνσεις, η "Eshop 2" και η "Eshop 3" εμφανίζονται δύο φορές χωρίς να μπορεί να διευκρινιστεί ο λόγος που συμβαίνει αυτό.

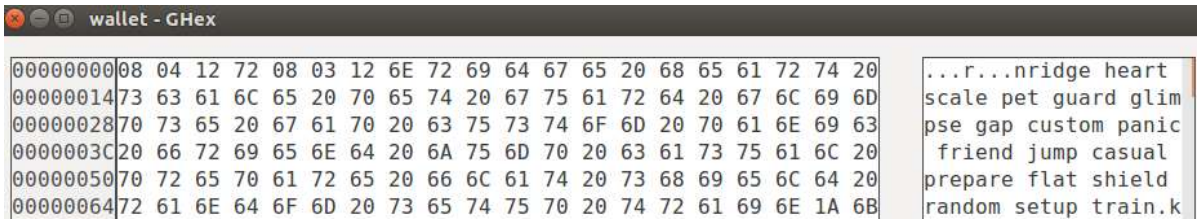
Table: address_book

	_id	coin_id	address	label
	Filter	Filter	Filter	Filter
1	1	bitcoin.main	1AnYovWnbZB5n7CPxntuHPWHZT6WCnmy4a	Eshop 2
2	2	bitcoin.main	17B6bns2tmvH8eTMy9zB89YSP8cYWVTdQa	Eshop 3
3	3	bitcoin.main	1AnYovWnbZB5n7CPxntuHPWHZT6WCnmy4a	Eshop 2
4	4	bitcoin.main	1BHPpNr9ATVgyp6PTUUNGe3zEWpEuw9YFi	Eshop 1
5	5	bitcoin.main	17B6bns2tmvH8eTMy9zB89YSP8cYWVTdQa	Eshop 3

Στιγμιότυπο 49 - Αποθηκευμένες διευθύνσεις bitcoin του πορτοφολιού Coinomi και οι ετικέτες αυτών

Το αρχείο com.coinomi.wallet/files/wallet, είναι ένα αρχείο binary, το οποίο ανοίγοντας το με το κατάλληλο πρόγραμμα παρατηρούμε ότι περιέχει αρκετά σημαντικά

εγκληματολογικά στοιχεία. Πρώτα από όλα περιέχει σε μορφή απλού κειμένου την μνημονική ακολουθία λέξεων (mnemonic word sequence), όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 50). Η μνημονική ακολουθία λέξεων ξεκινάει από την λέξη "ridge" (αφαιρούμε το γράμμα "n" που είναι προσκολλημένο στην λέξη) και τελειώνει στη λέξη "train". Παρατηρώντας όλες τις ενδιάμεσες λέξεις, βλέπουμε ότι είναι αυτές που μας εμφανίστηκαν κατά την διαδικασία δημιουργίας του πορτοφολιού μας. Όπως έχουμε αναφέρει και στα προηγούμενα παραδείγματά μας, η κατοχή αυτών των λέξεων μπορεί να μας δώσει πρόσβαση στα bitcoin του χρήστη, όπως και να αναπαράγει όλες τις διευθύνσεις του πορτοφολιού, αποκαλύπτοντας μας ποιες από αυτές χρησιμοποίησε ο χρήστης, καθώς και τις συναλλαγές που πραγματοποίησε αναλυτικά.



Στιγμιότυπο 50 - Προβολή των δεδομένων του αρχείου wallet - εμφάνιση της μνημονικής ακολουθίας λέξεων του πορτοφολιού Coinomi σε μορφή απλού κειμένου

Παρατηρώντας και τα υπόλοιπα δεδομένα του αρχείου, μπορούμε να διακρίνουμε σε μορφή απλού κειμένου ορισμένες αποθηκευμένες διευθύνσεις bitcoin (Στιγμιότυπο 51). Συγκεκριμένα οι διευθύνσεις που υπάρχουν στα δεδομένα του αρχείου φαίνονται στον παρακάτω πίνακα. Οι τρεις εξ' αυτών είναι οι διευθύνσεις που χρησιμοποιήθηκαν για τη αρχική λήψη των bitcoin στο πορτοφόλι μας, τις οποίες είδαμε προηγουμένως αποθηκευμένες στη βάση address_book με τις ετικέτες που είχαν δοθεί από τον χρήστη, ενώ οι υπόλοιπες τέσσερις διευθύνσεις bitcoin δημιουργήθηκαν προκειμένου να ληφθούν τα ρέστα (change) από τις αποστολές χρημάτων που πραγματοποιήσαμε. Παρόλο λοιπόν που στο αρχείο αυτό βλέπουμε όλες τις διευθύνσεις που χρησιμοποιήθηκαν από το πορτοφόλι μας, δεν είναι εύκολο να εξάγουμε συμπέρασμα σχετικά με τις συναλλαγές του χρήστη. Θα πρέπει σε έτερη αναζήτησή μας να χρησιμοποιήσουμε κάποιον εξερευνητή της αλυσίδας blockchain, προκειμένου να ελέγξουμε μία μία τις διευθύνσεις, ώστε να αντλήσουμε τα ζητούμενα στοιχεία.

Στιγμιότυπο 51 - Προβολή των bitcoin διευθύνσεων που υπάρχουν στα δεδομένα του αρχείου wallet της εφαρμογής Coinomi

Διεύθυνση bitcoin	**Ετικέτα**	**Διεύθυνση bitcoin**	**Ετικέτα**
1BHPpNr9ATVgyp6PTUUNGe3zEWpEuw9YFi	Eshop1	136uNMsuHZKyB5xGDKxhQKYVdz7u3B3QXU	Διεύθυνση ρέστων
1AnYovWnbZB5n7CPxntuHPWHZT6WCnmy4a	Eshop2	18QmgeUY4D67SzCyXCDU4PwmztJXBdsJzh	Διεύθυνση ρέστων
17B6bns2tmvH8eTMy9zB89YSP8cYWVTdQa	Eshop3	1Fk5XHdmsEvBTpDwmEYQ5DYqx9cfXy4CA4	Διεύθυνση ρέστων
		194F8jStmAg2xVEDtf644FkDtVDTcG3uvv	Διεύθυνση ρέστων

Επαναφορά πορτοφολιού από Backup - Coinomi Bitcoin Altcoin Wallet

Χρησιμοποιώντας την μνημονική ακολουθία λέξεων που είχαμε κρατήσει ως backup κατά την εγκατάσταση της εφαρμογής στην επόμενη δοκιμή μας, διαγράφουμε τελείως την εφαρμογή από το κινητό μας τηλέφωνο, την εγκαθιστούμε ξανά και επαναφέρουμε το πορτοφόλι που είχαμε δημιουργήσει.

Όταν πραγματοποιήθηκε αυτή η δοκιμή, η εφαρμογή είχε αναβαθμιστεί στην έκδοση 1.9.3. Επομένως σε αυτή την εξερεύνηση θα εξετάσουμε τυχόν άλλα ενδιαφέροντα αρχεία που μπορεί να αξίζουν την περαιτέρω ανάλυσή τους.

Χρησιμοποιώντας το εργαλείο ADB, εξάγουμε τα αρχεία που βρίσκονται στο πακέτο εγκατάστασης της εφαρμογής. Παρατηρούμε ότι έχει προστεθεί ένας επιπλέον φάκελος με όνομα “no_backup”, επομένως οι φάκελοι είναι τώρα οι εξής (cache, code_cache, databases, files, no_backup και shared_prefs).

Από αυτούς τους φακέλους ενδιαφέρον παρουσιάζουν οι φάκελοι με τα αρχεία:

- com.coinomi.wallet/cache/http_cache
  54bee67516952cd491c8e8b6d350b3fd.0
- com.coinomi.wallet/files/
  wallet

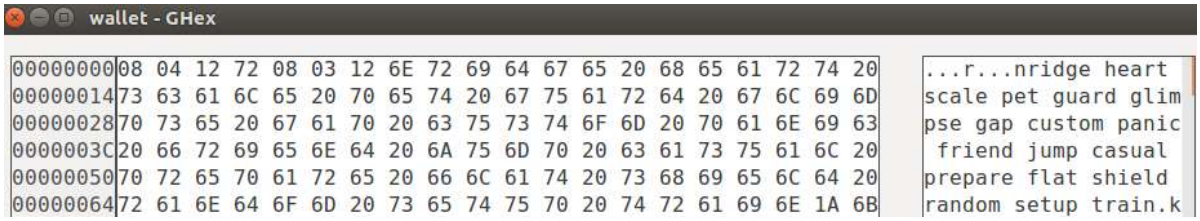
Παρατηρούμε ότι η βάση δεδομένων /databases/address_book που στην αρχική δοκιμή μας περιείχε διευθύνσεις bitcoin με ετικέτες με ονόματα (Eshop1, Eshop2 και Eshop3), μετά την επαναφορά από το backup είναι εντελώς κενή και είναι αδιάφορη από πλευράς εγκληματολογικής εξέτασης.

Το αρχείο cache/http_cache/54bee67516952cd491c8e8b6d350b3fd.0, παραμένει παρά την αναβάθμιση της εφαρμογής και όπως και πριν μπορούμε να δούμε τις καινούριες πληροφορίες σχετικά με την τελευταία είσοδο του χρήστη στην εφαρμογή, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 52).

Στιγμιότυπο 52 - Αρχείο καταγραφής που εμφανίζει την ώρα σύνδεσης του χρήστη στην εφαρμογή Coinomi μετά την επαναφορά από backup

Το αρχείο /files/wallet, έχει τροποποιηθεί σε κάποιον βαθμό συγκριτικά με το προηγούμενο αρχείο, κυρίως στη σειρά που εμφανίζονται οι διευθύνσεις bitcoin του πορτοφολιού μας (Στιγμιότυπο 54). Όπως ήταν αναμενόμενο, η μνημονική ακολουθία

λέξεων (mnemonic word sequence), διατηρείται σε μορφή απλού κειμένου, όπως και στην αρχική δοκιμή μας (Στιγμιότυπο 53).



Στιγμιότυπο 53 - Η μνημονική ακολουθία λέξεων σε μορφή απλού κειμένου μετά την επαναφορά του backup

Στιγμιότυπο 54 - Διευθύνσεις bitcoin του πορτοφολιού Coinomi, όπως είναι αποθηκευμένες στο αρχείο wallet μετά την επαναφορά του από το backup

Επομένως, για το αρχείο /files/wallet, ισχύουν όσα είχαμε προαναφέρει στην αρχική δοκιμή μας και έτσι, για την ανάλυση των συναλλαγών που πραγματοποιήθηκαν, θα πρέπει να ανατρέξουμε σε κάποιον εξερευνητή της blockchain αλυσίδας του Bitcoin και να χρησιμοποιήσουμε τις διευθύνσεις που έχουν αποθηκευτεί στο αρχείο που μόλις εξετάσαμε.

Κρυπτογράφηση του πορτοφολιού που επαναφέραμε μετά το Backup - Coinomi Bitcoin Altcoin Wallet

Κατά την τελευταία δοκιμή θα εξετάσουμε τους φακέλους του πακέτου της εφαρμογής αφού πρώτα κρυπτογραφήσουμε το πορτοφόλι που έχουμε επαναφέρει από το backup. Όπως είδαμε κατά την διαδικασία εγκατάστασης της εφαρμογής, μας δίνεται η δυνατότητα κρυπτογράφησης του πορτοφολιού μας για μεγαλύτερη ασφάλεια. Η ενέργεια αυτή μπορεί να πραγματοποιηθεί και σε μεταγενέστερο χρόνο μέσα από το μενού της εφαρμογής. Παρακάτω θα παρουσιάσουμε όλες τις πληροφορίες που μπορούμε να συλλέξουμε έχοντας προβεί σε κρυπτογράφηση του πορτοφολιού.

Χρησιμοποιώντας το εργαλείο ADB, εξάγουμε τα αρχεία που βρίσκονται στο πακέτο εγκατάστασης της εφαρμογής. Οι φάκελοι εξακολουθούν να είναι οι ίδιοι, όπως και στη δοκιμή μας μετά την επαναφορά του πορτοφολιού από το backup (cache, code_cache, databases, files, no_backup και shared_prefs).

Από αυτούς τους φακέλους, ενδιαφέρον παρουσιάζουν οι φάκελοι με τα αρχεία:

- com.coinomi.wallet/cache/http_cache
  54bee67516952cd491c8e8b6d350b3fd.0
- com.coinomi.wallet/files/
  wallet

Το αρχείο cache/http_cache/54bee67516952cd491c8e8b6d350b3fd.0, έχει μεταβληθεί ως προς την ώρα που εισήλθε ο χρήστης στην εφαρμογή, (προκειμένου στην περίπτωσή μας να πραγματοποιήσει την κρυπτογράφηση του πορτοφολιού) όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 55).

Στιγμιότυπο 55 - Αρχείο καταγραφής που εμφανίζει την ώρα σύνδεσης του χρήστη στην εφαρμογή Coinomi μετά την κρυπτογράφηση του πορτοφολιού

Το αρχείο /files/wallet, έχει πλέον κρυπτογραφηθεί και η μνημονική ακολουθία λέξεων δεν μπορεί να διαβαστεί (Στιγμιότυπο 56). Ωστόσο, παρατηρούμε ότι όλες οι διευθύνσεις του πορτοφολιού που χρησιμοποιήθηκαν για την πραγματοποίηση των

συναλλαγών, παραμένουν ακριβώς όπως εμφανίζονταν μετά την επαναφορά από το backup (Στιγμιότυπο 57). Για να μπορέσουμε να αντλήσουμε περισσότερα δεδομένα των συναλλαγών που έγιναν, θα πρέπει να προβούμε στην εξερεύνηση της αλυσίδας του blockchain του Bitcoin, όπως αναφέραμε και στα προηγούμενα παραδείγματά μας.

Στιγμιότυπο 56 - Η μνημονική ακολουθία λέξεων μετά την εισαγωγή κωδικού στην εφαρμογή, έχει κρυπτογραφηθεί

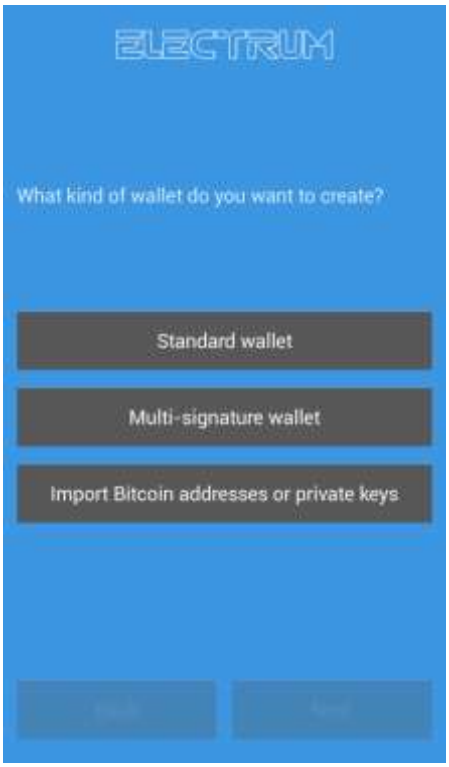
Στιγμιότυπο 57 - Οι διευθύνσεις bitcoin του πορτοφολιού Coinomi συνεχίζουν να εμφανίζονται στο αρχείο wallet όπως και πριν την κρυπτογράφηση του πορτοφολιού

Εφαρμογή Electrum Bitcoin Wallet

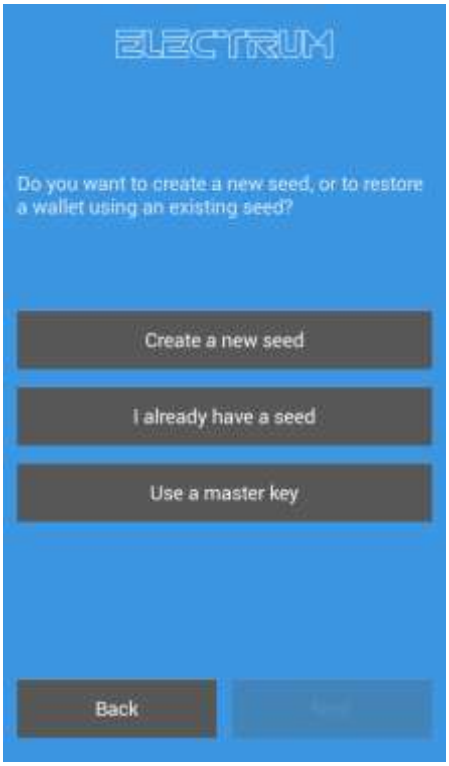
Εγκατάσταση της εφαρμογής Electrum

Η εφαρμογή βρίσκεται στο Play Store και την στιγμή των δοκιμών βρισκόταν στην έκδοση 3.1.1. Σύμφωνα με τους δημιουργούς της, η εφαρμογή Electrum είναι ανοικτού κώδικα και ο πηγαίος κώδικάς της βρίσκεται στο GitHub στον σύνδεσμο https://github.com/spesmilo/electrum . Υποστηρίζει τόσο κανονικά πορτοφόλια, όσο και πορτοφόλια πολλαπλών υπογραφών, καθώς και την δημιουργία περισσότερων του ενός πορτοφολιού, ενώ ακολουθεί την ντετερμινιστική ιεραρχική δημιουργία διευθύνσεων bitcoin, είναι δηλαδή ένα Hierarchical Deterministic Wallet (HD), όπως τα προηγούμενα πορτοφόλια που εξετάσαμε. Η εφαρμογή είναι αρκετά δημοφιλής στο Play Store και έχει περίπου 100.000+ λήψεις σύμφωνα με τα στοιχεία της Google.

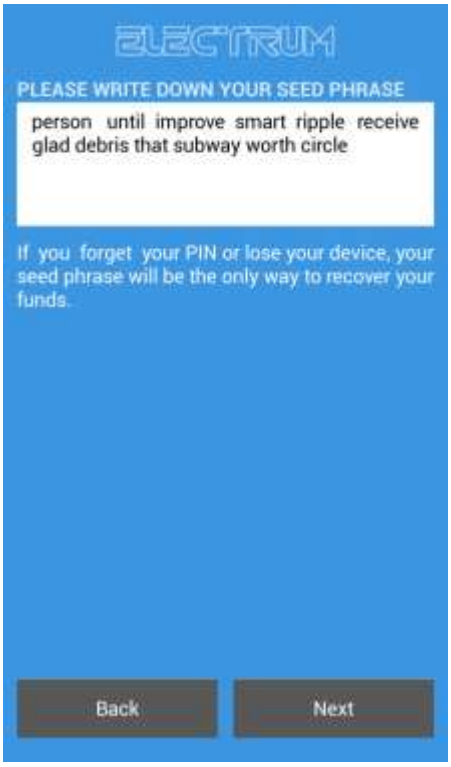
Κατά την είσοδο στην εφαρμογή ερωτόμαστε σχετικά με το είδος του πορτοφολιού που θέλουμε να δημιουργήσουμε (κανονικού ή πολλαπλών υπογραφών) ή αν θέλουμε να εισάγουμε διευθύνσεις Bitcoin ή ιδιωτικά κλειδιά (Στιγμιότυπο 58). Στη δοκιμή μας επιλέγουμε την δημιουργία κανονικού πορτοφολιού, όπου μας δίνεται η επιλογή της δημιουργίας καινούριας μνημονικής ακολουθίας λέξεων ή η επαναφορά πορτοφολιού χρησιμοποιώντας είτε την μνημονική ακολουθία λέξεων είτε το κύριο κλειδί (Στιγμιότυπο 59). Συνεχίσαμε με την δημιουργία νέας μνημονικής ακολουθίας λέξεων, όπου κληθήκαμε να αποθηκεύσουμε την ακολουθία λέξεων για μελλοντική επαναφορά του πορτοφολιού μας (Στιγμιότυπο 60) ενώ επιλέξαμε να μην χρησιμοποιήσουμε κάποιον κωδικό για το πορτοφόλι μας (Στιγμιότυπο 61).



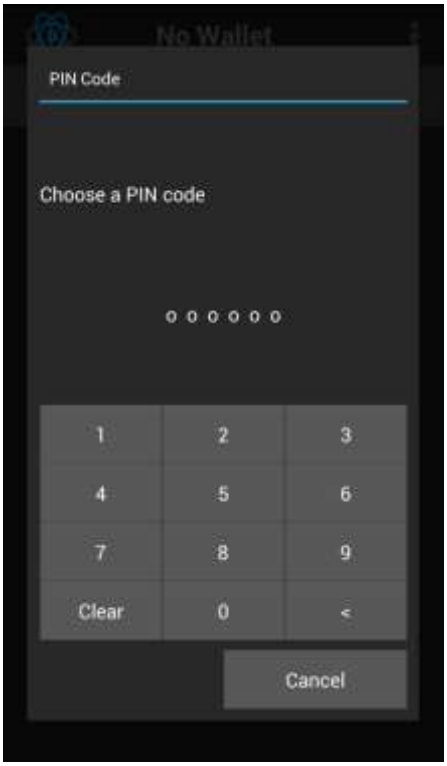
Στιγμιότυπο 58 - Επιλογή είδους νέου πορτοφολιού που θέλουμε να δημιουργήσουμε - Electrum



Στιγμιότυπο 59 - Επιλογή δημιουργίας καινούριας μνημονικής ακολουθίας λέξεων ή εισαγωγής υπάρχουσας

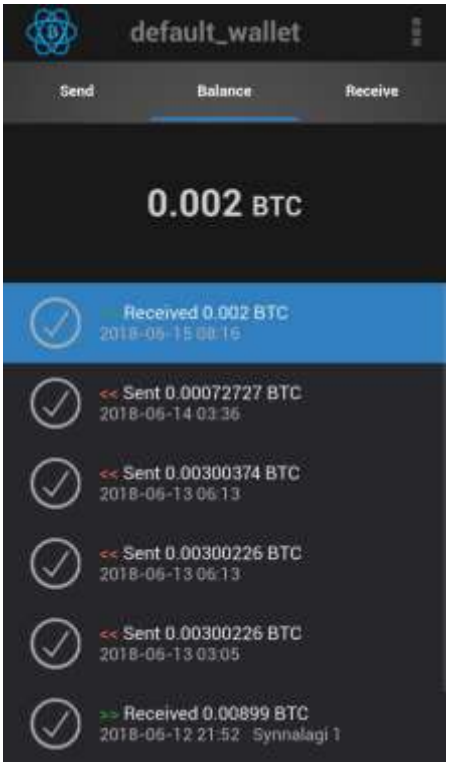


Στιγμιότυπο 60 - Προβολή της καινούριας μνημονικής ακολουθίας λέξεων και δημιουργία backup

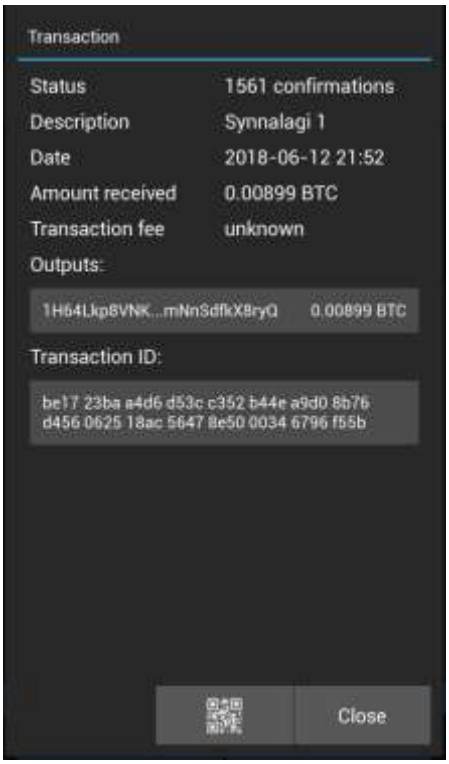


Στιγμιότυπο 61 - Παράλειψη εισαγωγής κωδικού

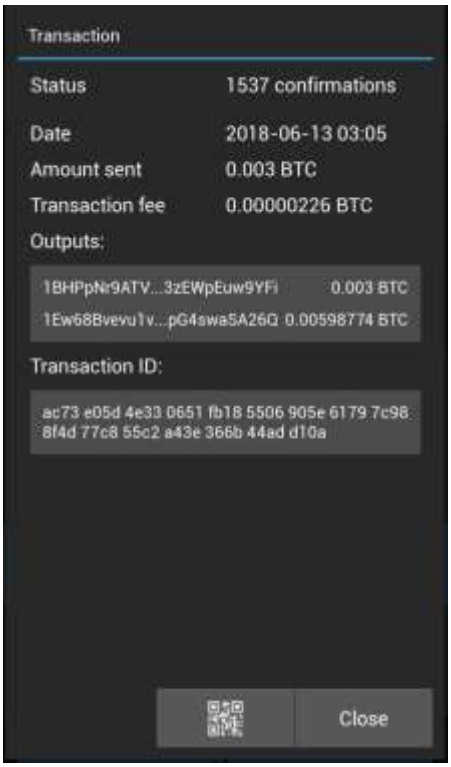
Το πορτοφόλι μας είναι πλέον έτοιμο για την λήψη bitcoin. Χρησιμοποιώντας το πορτοφόλι μας πραγματοποιούμε κάποιες συναλλαγές όπως φαίνεται στις παρακάτω εικόνες (Στιγμιότυπο 62, Στιγμιότυπο 63 και Στιγμιότυπο 64).



Στιγμιότυπο 62 - Ιστορικό συναλλαγών και υπόλοιπο πορτοφολιού Electrum



Στιγμιότυπο 63 - Λεπτομέρειες συναλλαγής λήψης bitcoin



Στιγμιότυπο 64 - Λεπτομέρειες συναλλαγής αποστολής bitcoin

Εγκληματολογική εξέταση της εφαρμογής Electrum Bitcoin Wallet

Για την εγκληματολογική εξέταση της εφαρμογής, θα χρησιμοποιήσουμε την λογική μέθοδο απόκτησης, κάνοντας χρήση του εργαλείου της Γέφυρας Εντοπισμού Σφαλμάτων του Android (Android Debug Bridge – ADB).

Το όνομα του πακέτου εγκατάστασης της εφαρμογής είναι το "org.electrum.electrum" και κατά την εγκατάσταση η εφαρμογή δημιουργεί δύο φακέλους με το όνομα του πακέτου, τον πρώτο στην διαδρομή του καταλόγου /data/data και τον δεύτερο στην διαδρομή του καταλόγου /sdcard.

Συνδέουμε το κινητό τηλέφωνο με τον υπολογιστή και με την χρήση του ADB εξαγάγουμε τους φακέλους που βρίσκονται στους ανωτέρω καταλόγους.

Το πακέτο εγκατάστασης org.electrum.electrum που εξήχθη από την διαδρομή /data/data περιέχει τους φακέλους (code_cache και files) που φαίνονται στην παρακάτω εικόνα, ενώ ο φάκελος της διαδρομής /sdcard περιέχει ένα αρχείο με όνομα blockchain_headers.

Από αυτούς τους φακέλους ενδιαφέρον παρουσιάζει το αρχείο:

- org.electrum.electrum/files/data/wallets/
  default_wallet

Το αρχείο default_wallet περιέχει αρκετά δεδομένα που είναι χρήσιμα κατά την εγκληματολογική εξέταση της εφαρμογής. Λόγω του τρόπου που είναι δομημένο, θα το δούμε τμηματικά μέσα από τα παρακάτω στιγμιότυπα οθόνης.

"addr_history"

Το τμήμα του αρχείου με όνομα "addr_history" περιλαμβάνει όλες τις διευθύνσεις που δημιούργησε το πορτοφόλι μας με ορισμένες από αυτές να αποτελούν τις διευθύνσεις επιστροφής (change addresses) (Στιγμιότυπο 65 και Στιγμιότυπο 66). Κάποιες από αυτές τις διευθύνσεις έχουν χρησιμοποιηθεί σε συναλλαγές και κάποιες όχι. Όσες από αυτές χρησιμοποιήθηκαν σε κάποια συναλλαγή είτε ως είσοδος (input) είτε ως έξοδος (output), περιέχουν μέσα σε αγκύλες το αναγνωριστικό (id) των συναλλαγών. Μέσα στην αγκύλη μπορούμε να ξεχωρίσουμε το αναγνωριστικό (id) της συναλλαγής καθώς και το μπλοκ στο

οποίο αυτή περιλήφθηκε, αλλά δεν μπορούμε να πάρουμε περισσότερες πληροφορίες για την συναλλαγή. Παράδειγμα: Η διεύθυνση "153e1YBYrSgZJ5rLB2UZs3UD1eFtMAg2NP" έχει χρησιμοποιηθεί στην συναλλαγή με αναγνωριστικό "68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f" (που συμπεριλήφθηκε στο μπλοκ 527171), αλλά έχει χρησιμοποιηθεί και στην συναλλαγή "ed4e50792ff4d57f21ca6f770e528f1af4e09f9e1ae6fab87af0c9aa56485c85" (που συμπεριλήφθηκε στο μπλοκ 527171).

Για να αποκτήσουμε περισσότερες πληροφορίες για την συναλλαγή θα πρέπει να εισάγουμε το αναγνωριστικό της συναλλαγής σε κάποιον εξερευνητή της αλυσίδας blockchain του Bitcoin, και να αναλύσουμε την κάθε αλλαγή ξεχωριστά. Ωστόσο, θα δούμε στα παρακάτω τμήματα του αρχείου που εξετάζουμε ότι περιέχονται περισσότερες λεπτομέρειες για τις συναλλαγές αυτές.

default_wallet


```
{
    "addr_history": {
        "126EjL5JF4d7VGnC7hgBBZf3kzZQfgap85": [],
        "12nxmnLjwEogEK3Sp2yAeipLZMUxTTrDPn": [],
        "12pLzhNB7HbyX3aD4maZZHK1F6xUVPFniS": [],
        "12vrYHL2qEmkJuNrDiXm8JFHj5gtHNMiaW": [],
        "13GpJK9fzWrawXcTus74W3EE9w3QU4Duqn": [],
        "13uJW7rXr5wetgauWzAps4tzGrCBTvK2ty": [],
        "14EKEiT39qYxXydLQQhj2NegDyGFHWP1po": [],
        "14NqxMXH3RBjJC4sE1oZs19FxgstK6suqX": [],
        "14P37BcgfYUJ6sP9KtccCqfqNSA5dM4gGB": [],
        "14scK3ZnkbSxkqpoEoZeaWLrQinKGwhJ8v": [],
        "153e1YBYrSgZJ5rLB2UZs3UD1eFtMAg2NP": [
            [
                "68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f",
                527171
            ],
            [
                "ed4e50792ff4d57f21ca6f770e528f1af4e09f9e1ae6fab87af0c9aa56485c85",
                527216
            ]
        ],
        "16KJ8H53NnNwJq1wQsg62XCHasUqSobFyq": [],
        "16n1cVaGNbSJ796A7M9G9asNxdbbL3Zi8S": [],
        "16qrf3VUUaKetANRzTU7ee7DZB12cXbSzD": [],
        "16w6d9Ps3Kz48iYdedVrgYTA66hEsNA2JE": [
            [
                "ed4e50792ff4d57f21ca6f770e528f1af4e09f9e1ae6fab87af0c9aa56485c85",
                527216
            ],
            [
                "798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3",
                527342
            ]
        ],
        "17HsgvN1HNeupaq2baGAQa3SmSTuBCcbLH": [],
        "17veEjaQxUqR8HDczS7E6pmdwAE3Lpve5u": [],
        "18XT48pGNJNpfvWEjESzBgdPdJxnY3cMcU": [],
        "18ifuLzqSieXiMW23j5Gs5hMZ4FxgpCmg5": [],
        "19m6HJ8P4A5i8DD2hGo7PCK5tZ6JAAgWnV": [
            [
                "cc5515271b1111baff26eb44e4d0413610509508 40bf2968a3ebf72f0f0eed90",
                527517
            ]
        ],
        "1AffLqFGfK86mwx1dXrnWt7sie5zkinZYq": [],
        "1BEuVNaVtvXLg3mMzP44WkHFbswhxFKW2S": [],
        "1CRvnjiBdFF7h8H1ByuF71rKfuBL5omwhL": [],
        "1CxpqrdAzH8wLThoYJgXQEKXZHRZCTpd77": [],
```


Στιγμιότυπο 65 - Δημιουργημένες διευθύνσεις bitcoin του πορτοφολιού Electrum και συναλλαγές στις οποίες χρησιμοποιήθηκαν

Στιγμιότυπο 66 - Δημιουργημένες διευθύνσεις bitcoin του πορτοφολιού Electrum και συναλλαγές στις οποίες χρησιμοποιήθηκαν - 2η εικόνα

"addresses"

Το τμήμα του αρχείου με όνομα “addresses” περιλαμβάνει ξανά όλες τις διευθύνσεις που δημιούργησε το πορτοφόλι μας, διαχωρίζοντάς τες όμως σε δύο κατηγορίες: τις διευθύνσεις επιστροφής (change addresses) και τις διευθύνσεις λήψης (receiving addresses). Αρκεί ο έλεγχος των διευθύνσεων αυτών σε κάποιον εξερευνητή blockchain, προκειμένου να δούμε αν κάποια από αυτές τις διευθύνσεις περιέχει bitcoin και έτσι να έχουμε μια εικόνα για το υπόλοιπο του πορτοφολιού του χρήστη (Στιγμιότυπο 67).

default_wallet


```
"addresses": {
    "change": [
        "1Ew68Bvevu1vJdzrLY7nBBwpG4swaSA26Q",
        "1QEKtdFVsaysaEqXwGMGS1EHxQKiLLPNeb",
        "16w6d9Ps3Kz48iYdedVrgYTA66hEsNA2JE",
        "1PEHjHueDPhEcdbjRaKcvTD8FbFGAzLYpz",
        "16n1cVaGNbSJ796A7M9G9asNxdbbL3Zi8S",
        "1BEuVNaVtvXLg3mMzP44WkHFbswhxFKW2S",
        "17veEjaQxUqR8HDczS7E6pmdwAE3Lpve5u",
        "12nxmnLjwEogEK3Sp2yAeipLZMUxTTrDPn",
        "1HEhQiTcUsqbbyRpYikFqLVo4NvivYi2BD"
    ],
    "receiving": [
        "1H64Lkp8VNKrZt54UrQP4wmNnSdfkX8ryQ",
        "19m6HJ8P4A5i8DD2hGo7PCK5tZ6JAAgWnV",
        "13GpJK9fzWrawXcTus74W3EE9w3QU4Duqn",
        "1FdHsqddMztr14TfoeJvoVegSwgAXtpGsR",
        "16qrf3VUUaKetANRzTU7ee7DZB12cXbSzD",
        "126EjL5JF4d7VGnC7hgBBZf3kzZQfgap85",
        "1NXsJ2kBJUByhRyhiYXM2pk2Aq7yJyfAau",
        "1LhXFzKetCzSTPNvLgqVXLvNeyktwo1icV",
        "1GJNEoLgrvCidxhtEpwi3Z5vxExEHcGiGr",
        "1D4g4YhjPkzws6MaYcQQHpvYkVSuhV5DUF",
        "14EKEiT39qYxXydLQQhj2NegDyGFHWP1po",
        "1H22p3uJ6CSEe6f23Yr1ZPUzfGeKYkrRgz",
        "1J1G8pWaz3LqmFJDp8StAJLnQrXqGnh5JV",
        "18ifuLzqSieXiMW23j5Gs5hMZ4FxgpCmg5",
        "1FYZ51SrL6H9yndqBh1mjrbSJ7nKrjVmWA",
        "12pLzhNB7HbyX3aD4maZZHK1F6xUVPFniS",
        "14scK3ZnkbSxkqpoEoZeaWLrQinKGwhJ8v",
        "153e1YBYrSgZJ5rLB2UZs3UD1eFtMAg2NP",
        "1GWsUQ9wBdP84t4snYYEt8F29Tjn3t5ULy",
        "1CRvnjiBdFF7h8H1ByuF71rKfuBL5omwhL",
        "1GUk9qS1z8LjFUX1ywoQcPEPoLfAZnRD5n",
        "14P37BcgfYUJ6sP9KtccCqfqNSA5dM4gGB",
        "1N1g6QotwrLjFc3tXC6vYUqrSunu4WfS7A",
        "16KJ8H53NnNwJq1wQsg62XCHasUqSobFyq",
        "12vrYHL2qEmkJuNrDiXm8JFHj5gtHNMiaW",
        "1JZ2ctSbpB3K2xkaT4qzautZmWnDccV7hL",
        "17HsgvN1HNeupaq2baGAQa3SmSTuBCcbLH",
        "1Nvbq2JYJQhAPPQtG3LgazS8yByKPLUhst",
        "1NQxeR9srxJShAsvfB6ufG3AVgb7w6qwmR",
        "1EWaoz1LSFV7wWGGGhTwLoR8rqZd8SyAWe",
        "18XT48pGNJNpfvWEjESzBgdPdJxnY3cMcU",
        "1HujjQac5yDXPq6n6Q1FLMEGGVsmnrpB15",
        "1AffLqFGfK86mwx1dXrnWt7sie5zkinZYq",
        "13uJW7rXr5wetgauWzAps4tzGrCBTvK2ty",
        "14NqxMXH3RBjJC4sE1oZs19FxgstK6suqX",
        "1LusJvbHNQwz7e2Ccoib7vNREGzPMuG2iN",
        "1MwxRezDcxqw2NDJAupckTc6pvr172cyjr",
        "1CxpqrdAzH8wLThoYJgXQEKXZHRZCTpd77"
    ]
},
```


Στιγμιότυπο 67 - Σύνολο δημιουργημένων διευθύνσεων του πορτοφολιού Electrum κατηγοριοποιημένες σε διευθύνσεις λήψης και διευθύνσεις επιστροφής

"invoices"

Το τμήμα του αρχείου με όνομα "invoices" περιλαμβάνει τα τιμολόγια που έχει λάβει ο χρήστης της εφαρμογής από κάποιον άλλον χρήστη, προκειμένου να πληρώσει ορισμένο ποσό σε συγκεκριμένη διεύθυνση. Στην παρακάτω εικόνα (Στιγμιότυπο 68) βλέπουμε ότι κάποιος χρήστης, ζήτησε να αποσταλούν στην διεύθυνση "1BHPpNr9ATVgyp6PTUUNGe3zEWpEuw9YFi" κάποια bitcoin και η συναλλαγή αυτήν πήρε αναγνωριστικό

"ac73e05d4e330651fb185506905e61797c988f4d77c855c2a43e366b44add10a". Δεν φαίνεται να προκύπτει ωστόσο το ποσό που ζήτησε ο άλλος χρήστης.

Στιγμιότυπο 68 - Τιμολόγιο (invoice) συναλλαγής που πραγματοποίησε ο χρήστης της εφαρμογής έπειτα από αίτηση άλλου χρήστη

"keystore"

Το τμήμα του αρχείου με όνομα "keystore", περιλαμβάνει σε μορφή απλού κειμένου τα εξής: α) την μνημονική ακολουθία λέξεων του πορτοφολιού που δημιουργήσαμε “seed”, β) το επεκταμένο ιδιωτικό κλειδί ρίζας “xprv” και γ) το επεκταμένο δημόσιο κλειδί “xpub” (Στιγμιότυπο 69).

Όπως αναφέραμε και σε προηγούμενες δοκιμές μας, η κατοχή των (α) ή (β) μας παρέχει πλήρη πρόσβαση στα bitcoin του χρήστη, ενώ η κατοχή του (γ) μπορεί να δημιουργήσει όλες τις διευθύνσεις bitcoin του πορτοφολιού του χρήστη και έτσι θα είμαστε σε θέση να γνωρίζουμε τις διευθύνσεις που ανήκουν σε αυτό το πορτοφόλι.

Στιγμιότυπο 69 – Μνημονική ακολουθία λέξεων, ιδιωτικό και δημόσιο κλειδί σε μορφή απλού κειμένου - Electrum

"labels"

Το τμήμα του αρχείου με όνομα "labels", περιέχει ετικέτες (ονόματα) που έδωσε ο χρήστης της εφαρμογής σε κάποιες από τις συναλλαγές του. Είναι μια προαιρετική λειτουργία του πορτοφολιού, ωστόσο θα μπορούσε να μας δώσει κάποια ενδιαφέροντα στοιχεία αν γινόταν χρήση της λειτουργίας αυτής από τον χρήστη του πορτοφολιού. Στην εικόνα που ακολουθεί (Στιγμιότυπο 70) βλέπουμε ότι ο χρήστης ονόμασε την συναλλαγή

"68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f", ως "Synnalagi 2" και την συναλλαγή "be1723baa4d6d53cc352b44ea9d08b76d456062518ac56478e5000346796f55b", ως "Synnalagi 1".

default_wallet

```
    "labels": {
        "68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f": "Synnalagi  2",
        "be1723baa4d6d53cc352b44ea9d08b76d456062518ac56478e5000346796f55b": "Synnalagi 1"
    },
```

Στιγμιότυπο 70 – Ετικέτες συναλλαγών όπως δόθηκαν από τον χρήστη της εφαρμογής Electrum

"payment_requests"

Το τμήμα του αρχείου με όνομα "payment_requests" περιέχει τις διευθύνσεις τις οποίες φαίνεται να χρησιμοποίησε ο χρήστης προκειμένου να ζητήσει από κάποιον άλλον χρήστη να του αποστείλει χρήματα (Στιγμιότυπο 71). Επίσης, σε μορφή Linux epoch time φαίνεται η χρονική στιγμή που έγινε αυτό το αίτημα. Στο δοκιμή μας φαίνεται ότι το ποσό που αιτήθηκε ο χρήστης είναι μηδενικό, οπότε προφανώς ο χρήστης δημιούργησε το αίτημα, πλην όμως δεν το απέστειλε στον άλλον χρήστη. Η δημιουργία αιτήματος και η ακύρωσή του δεν σημαίνει απόλυτα ότι ο χρήστης δεν έλαβε ποτέ χρήματα στην συγκεκριμένη διεύθυνση. Μπορεί να χρησιμοποίησε την διεύθυνση αυτή για λήψη χρημάτων σε μεταγενέστερο χρόνο.

default_wallet

```
    "payment_requests": {
        "153e1YBYrSgZJ5rLB2UZs3UD1eFtMAg2NP": {
            "address": "153e1YBYrSgZJ5rLB2UZs3UD1eFtMAg2NP",
            "amount": 0,
            "exp": null,
            "id": "aec284d5e4",
            "memo": "",
            "time": 1528828654
        },
        "1H64Lkp8VNKrZt54UrQP4wmNnSdfkX8ryQ": {
            "address": "1H64Lkp8VNKrZt54UrQP4wmNnSdfkX8ryQ",
            "amount": 0,
            "exp": null,
            "id": "7db8db4e2f",
            "memo": "",
            "time": 1528402514
        }
    },
    "pruned_txo": {},
    "seed_type": "standard",
    "seed_version": 16,
    "stored_height": 531766,
```

Στιγμιότυπο 71 – Αιτήσεις λήψης χρημάτων από τον χρήστη της εφαρμογής

"transactions"

Το τμήμα του αρχείου με το όνομα "transactions" περιλαμβάνει όλες τις συναλλαγές που πραγματοποιήθηκαν από το πορτοφόλι μας, είτε αυτές αφορούν την λήψη είτε την αποστολή bitcoin, τις οποίες όμως είδαμε και σε προηγούμενα τμήματα του αρχείου που εξετάζουμε. Ένα επιπλέον στοιχείο που περιλαμβάνεται σε αυτό το τμήμα είναι η Raw Hex κωδικοποιημένη μορφή των συναλλαγών (όπως φαίνεται στην παρακάτω εικόνα) (Στιγμιότυπο 72), την οποία αν αποκωδικοποιήσουμε χρησιμοποιώντας κάποιον αποκωδικοποιητή (υπάρχουν αρκετοί online αποκωδικοποιητές), μπορούμε να πάρουμε περισσότερα στοιχεία για την συναλλαγή. Ένα ακόμη στοιχείο που μπορούμε να διακρίνουμε στην παρακάτω εικόνα (Στιγμιότυπο 72), που όμως δεν έχει μεγάλη σημασία για την εγκληματολογική εξέταση είναι τα τέλη που ξοδεύτηκαν για κάθε μια από τις συναλλαγές εκφρασμένα σε satoshi, όπως φαίνονται στην παρακάτω εικόνα στο τμήμα “tx_fees”.

Στιγμιότυπο 72 – id και ιστορικό των συναλλαγών που πραγματοποιήθηκαν από την εφαρμογή Electrum

"txi"

Το τμήμα του αρχείου με όνομα "txi" περιλαμβάνει όλες τις εισόδους (inputs) που χρησιμοποιήθηκαν στις συναλλαγές που πραγματοποιήθηκαν από το πορτοφόλι μας. Το ποσό που αναγράφεται εντός τις αγκύλης (εκφρασμένο σε satoshi) αναφέρεται στην είσοδο (input) του πορτοφολιού μας που δείχνει το ποσό που χρεώθηκε το πορτοφόλι μας πραγματοποιώντας μια συναλλαγή. Συγκεκριμένα, αναλύοντας την πρώτη είσοδο (input) που φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 73), το ποσό των 598774 satoshi δημιουργήθηκε ως έξοδος (output) με την συναλλαγή "ac73e05d4e330651fb185506905e61797c988f4d77c855c2a43e366b44add10a" στη διεύθυνση "1Ew68Bvevu1vJdzrLY7nBBwpG4swaSA26Q" του πορτοφολιού μας και

καταναλώθηκε ως είσοδος (input) στην συναλλαγή "19f126c98bd952ff15ae30033e9277fa5fdb1a39393252fa0efe5aa10c38e0d3", χρεώνοντας το πορτοφόλι μας με το ποσό αυτό. Συνεχίζοντας με τις υπόλοιπες συναλλαγές μπορούμε να δούμε το συνολικό ποσό που χρεώθηκε το πορτοφόλι μας.

default_wallet


```
"txi": {
    "19f126c98bd952ff15ae30033e9277fa5fdb1a39393252fa0efe5aa10c38e0d3": {
        "1Ew68Bvevu1vJdzrLY7nBBwpG4swaSA26Q": [
            [
                "ac73e05d4e330651fb185506905e61797c988f4d77c855c2a43e366b44add10a:1",
                598774
            ]
        ]
    },
    "68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f": {},
    "798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3": {
        "16w6d9Ps3Kz48iYdedVrgYTA66hEsNA2JE": [
            [
                "ed4e50792ff4d57f21ca6f770e528f1af4e09f9e1ae6fab87af0c9aa56485c85:0",
                72727
            ]
        ]
    },
    "ac73e05d4e330651fb185506905e61797c988f4d77c855c2a43e366b44add10a": {
        "1H64Lkp8VNKrZt54UrQP4wmNnSdfkX8ryQ": [
            [
                "be1723baa4d6d53cc352b44ea9d08b76d456062518ac56478e5000346796f55b:0",
                899000
            ]
        ]
    },
    "be1723baa4d6d53cc352b44ea9d08b76d456062518ac56478e5000346796f55b": {},
    "cc5515271b1111baff26eb44e4d0413610509508 40bf2968a3ebf72f0f0eed90": {},
    "ed4e50792ff4d57f21ca6f770e528f1af4e09f9e1ae6fab87af0c9aa56485c85": {
        "153e1YBYrSgZJ5rLB2UZs3UD1eFtMAg2NP": [
            [
                "68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f:0",
                74553
            ]
        ],
        "1QEKtdFVsaysaEqXwGMGS1EHxQKiLLPNeb": [
            [
                "19f126c98bd952ff15ae30033e9277fa5fdb1a39393252fa0efe5aa10c38e0d3:0",
                298548
            ]
        ]
    }
},
```


Στιγμιότυπο 73 – Ιστορικό όλων των εισόδων (inputs) των συναλλαγών που πραγματοποιήθηκαν από το πορτοφόλι Electrum

"txo"

Το τμήμα του αρχείου με όνομα "txo" περιλαμβάνει όλες τις εξόδους (outputs) που χρησιμοποιήθηκαν στις συναλλαγές που πραγματοποιήθηκαν από το πορτοφόλι μας. Το ποσό που αναγράφεται εντός τις αγκύλης (εκφρασμένο σε satoshi) αναφέρεται στην έξοδο (output) που δημιουργήθηκε στο πορτοφόλι μας προσθέτοντας το ποσό αυτό στον

λογαριασμό μας. Συγκεκριμένα, αναλύοντας την πρώτη έξοδο (output) που φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 74), το ποσό των 298548 satoshi, δημιουργήθηκε ως έξοδος (output) με την συναλλαγή "19f126c98bd952ff15ae30033e9277fa5fdb1a39393252fa0efe5aa10c38e0d3" στην διεύθυνση "1QEKtdFVsaysaEqXwGMGS1EHxQKiLLPNeb", προσθέτοντας το ποσό αυτό στον λογαριασμό μας. Συνεχίζοντας με τις υπόλοιπες συναλλαγές μπορούμε να δούμε το συνολικό ποσό που προστέθηκε στο πορτοφόλι μας.

default_wallet


```
"txo": {
    "19f126c98bd952ff15ae30033e9277fa5fdb1a39393252fa0efe5aa10c38e0d3": {
        "1QEKtdFVsaysaEqXwGMGS1EHxQKiLLPNeb": [
            [
                0,
                298548,
                false
            ]
        ]
    },
    "68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f": {
        "153e1YBYrSgZJ5rLB2UZs3UD1eFtMAg2NP": [
            [
                0,
                74553,
                false
            ]
        ]
    },
    "798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3": {},
    "ac73e05d4e330651fb185506905e61797c988f4d77c855c2a43e366b44add10a": {
        "1Ew68Bvevu1vJdzrLY7nBBwpG4swaSA26Q": [
            [
                1,
                598774,
                false
            ]
        ]
    },
    "be1723baa4d6d53cc352b44ea9d08b76d456062518ac56478e5000346796f55b": {
        "1H64Lkp8VNKrZt54UrQP4wmNnSdfkX8ryQ": [
            [
                0,
                899000,
                false
            ]
        ]
    },
    "cc5515271b1111baff26eb44e4d041361050950840bf2968a3ebf72f0f0eed90": {
        "19m6HJ8P4A5i8DD2hGo7PCK5tZ6JAAgWnV": [
            [
                1,
                200000,
                false
            ]
        ]
    },
    "ed4e50792ff4d57f21ca6f770e528f1af4e09f9e1ae6fab87af0c9aa56485c85": {
        "16w6d9Ps3Kz48iYdedVrgYTA66hEsNA2JE": [
            [
                0,
                72727,
                false
            ]
        ]
    }
},
"use_encryption": false,
```


Στιγμιότυπο 74 - Ιστορικό όλων των εξόδων (outputs) των συναλλαγών που πραγματοποιήθηκαν από το πορτοφόλι Electrum

"verified_tx3"

Το τμήμα του αρχείου με όνομα "verified_tx3" περιέχει τις επιβεβαιωμένες συναλλαγές του πορτοφολιού μας, αναφέροντας τον αριθμό του μπλοκ στο οποίο συμπεριλήφθηκαν και την ώρα που περιλήφθηκαν στο μπλοκ εκφρασμένη με την μορφή Linux epoch time. Παράδειγμα, η προτελευταία συναλλαγή που φαίνεται στην εικόνα (Στιγμιότυπο 75), με αναγνωριστικό "cc5515271b1111baff26eb44e4d041361050950840bf2968a3ebf72f0f0eed90", συμπεριλήφθηκε στο μπλοκ 527517 την ώρα 1529039779, δηλαδή Παρασκευή 15 Ιουνίου 2018, ώρα 8:16:19 AM. Τέλος στο παρακάτω τμήμα φαίνεται και το είδος του πορτοφολιού που έχει δημιουργήσει ο χρήστης, το οποίο στην περίπτωσή μας είναι το “standard”.

default_wallet


```
    "verified_tx3": {
        "19f126c98bd952ff15ae30033e9277fa5fdb1a39393252fa0efe5aa10c38e0d3": [
            527216,
            1528859617,
            616
        ],
        "68ab55b4e0af6a28d2f45c68065184901bfe1b31af9642350144a88eb701c04f": [
            527171,
            1528829070,
            250
        ],
        "798423584e4ad541fe8795ae914dc4591c3185469ba4f8a0e6e4b6b0e177f0c3": [
            527342,
            1528936604,
            1686
        ],
        "ac73e05d4e330651fb185506905e61797c988f4d77c855c2a43e366b44add10a": [
            527196,
            1528848316,
            1099
        ],
        "be1723baa4d6d53cc352b44ea9d08b76d456062518ac56478e5000346796f55b": [
            527172,
            1528829551,
            988
        ],
        "cc5515271b1111baff26eb44e4d041361050950840bf2968a3ebf72f0f0eed90": [
            527517,
            1529039779,
            2060
        ],
        "ed4e50792ff4d57f21ca6f770e528f1af4e09f9e1ae6fab87af0c9aa56485c85": [
            527216,
            1528859617,
            617
        ]
    },
    "wallet_type": "standard"
}
```


Στιγμιότυπο 75 – Ιστορικό των επιβεβαιωμένων συναλλαγών του πορτοφολιού Electrum

Επαναφορά πορτοφολιού από Backup - Electrum Bitcoin Wallet

Η επόμενη δοκιμή που θα κάνουμε στην εφαρμογή Electrum είναι η διαγραφή της από το κινητό μας τηλέφωνο, η επανεγκατάσταση της και η επαναφορά του πορτοφολιού που εξετάσαμε προηγουμένως, από backup που έχουμε κρατήσει.

Όταν πραγματοποιήθηκε αυτή η δοκιμή, η εφαρμογή είχε αναβαθμιστεί στην έκδοση 3.2.1.0. Σε αυτή την έκδοση η εφαρμογή δεν επιτρέπει την παράκαμψη εισαγωγής κωδικού τόσο κατά την δημιουργία καινούριου πορτοφολιού, όσο και κατά την επαναφορά πορτοφολιού από backup όπως στην περίπτωσή μας. Με την εισαγωγή του κωδικού, το πορτοφόλι της εφαρμογής κρυπτογραφείται. Παρακάτω θα δούμε τι συμβαίνει κατά την κρυπτογράφηση, ποια δεδομένα κρυπτογραφούνται και τι παραμένει σε "κοινή θέα". Ταυτόχρονα, λόγω της αναβάθμισης θα εξετάσουμε αν υπάρχει κάποιο άλλο στοιχείο που να παρουσιάζει ενδιαφέρον.

Χρησιμοποιούμε και πάλι το εργαλείο ADB, προκειμένου να εξάγουμε τα αρχεία που βρίσκονται στο πακέτο εγκατάστασης της εφαρμογής, όπως φαίνεται στην παρακάτω εικόνα.

Το όνομα του πακέτου εγκατάστασης της εφαρμογής είναι το "org.electrum.electrum" και κατά την εγκατάσταση η εφαρμογή δημιουργεί δύο φακέλους με το όνομα του πακέτου, τον πρώτο στην διαδρομή του καταλόγου /data/data και τον δεύτερο στην διαδρομή του καταλόγου /sdcard. Το πακέτο εγκατάστασης org.electrum.electrum που εξήχθη από την διαδρομή /data/data περιέχει τους φακέλους (code_cache και files) που φαίνονται στην παρακάτω εικόνα, ενώ ο φάκελος της διαδρομής /sdcard περιέχει ένα αρχείο με όνομα blockchain_headers.

Παρά την αναβάθμιση της εφαρμογής και την τροποποίηση ορισμένων αρχείων που εξαγάγαμε, δεν παρατηρήθηκε η ύπαρξη κάποιου νέου αρχείου που να παρουσιάζει ενδιαφέρον συγκριτικά με την προηγούμενη δοκιμή μας, οπότε τα ευρήματα που μας ενδιαφέρουν βρίσκονται και πάλι στο αρχείο:

- org.electrum.electrum/files/data/wallets/
  default_wallet

Τα τμήματα του αρχείου (“addr_history”, "addresses", "transactions", "txi", "txo" & "verified_tx3"), παραμένουν αναλλοίωτα παρά την κρυπτογράφηση του πορτοφολιού και την αναβάθμιση της εφαρμογής και επομένως μπορούμε να αντλήσουμε ακριβώς τα ίδια στοιχεία, όπως τα παρουσιάσαμε στην προηγούμενη ανάλυσή μας.

"invoices"

Το τμήμα του αρχείου με όνομα "invoices" που περιέχονταν στο αρχείο default_wallet και αναλύσαμε παραπάνω, παρατηρούμε ότι κατά την επαναφορά του πορτοφολιού μας από backup δεν υπάρχει πλέον. Το τμήμα αυτό περιελάμβανε τα τιμολόγια που έχει λάβει ο χρήστης της εφαρμογής από κάποιον άλλον χρήστη, προκειμένου να πληρώσει ορισμένο ποσό σε συγκεκριμένη διεύθυνση. Συνεπώς, το πορτοφόλι δεν αποθηκεύει αυτά τα δεδομένα κατά την δημιουργία backup και δεν μπορούμε να τα δούμε σε αυτή την ανάλυσή μας. Ωστόσο η συναλλαγή που περιελάμβανε την δημιουργία του τιμολογίου υπάρχει κανονικά στις συναλλαγές του πορτοφολιού, όποτε κάποια στοιχεία μπορούμε να αντλήσουμε από εκεί.

"keystore"

Το τμήμα του αρχείου με όνομα "keystore", στην προηγούμενη ανάλυσή μας περιείχε τα πιο σημαντικά στοιχεία που θα μπορούσαμε να συλλέξουμε από το πορτοφόλι μας, δηλαδή: α) την μνημονική ακολουθία λέξεων του πορτοφολιού που δημιουργήσαμε “seed”, β) το επεκταμένο ιδιωτικό κλειδί ρίζας “xprv” και γ) το επεκταμένο δημόσιο κλειδί “xpub”, σε μορφή απλού κειμένου. Από την στιγμή που η εφαρμογή μας ανάγκασε να εισάγουμε κωδικό για να κρυπτογραφήσει το πορτοφόλι μας, τα στοιχεία (α) και (β) που μας έδιναν πρόσβαση στα bitcoin του χρήστη, έχουν κρυπτογραφηθεί και δεν μπορούμε να έχουμε πρόσβαση. Ωστόσο, το επεκταμένο δημόσιο κλειδί “xpub” δεν κρυπτογραφήθηκε και θα μπορούσε να χρησιμοποιηθεί για την δημιουργία των bitcoin διευθύνσεων του πορτοφολιού, γνωρίζοντάς μας τις διευθύνσεις που ανήκουν σε αυτό το πορτοφόλι. Στις εικόνες που ακολουθούν φαίνεται το τμήμα "keystore” πριν (Στιγμιότυπο 76) και μετά (Στιγμιότυπο 77) την κρυπτογράφηση του πορτοφολιού.

Στιγμιότυπο 76 – Μνημονική ακολουθία λέξεων, ιδιωτικό και δημόσιο κλειδί σε μορφή απλού κειμένου πριν την κρυπτογράφηση του πορτοφολιού

Στιγμιότυπο 77 – Μνημονική ακολουθία λέξεων και ιδιωτικό κλειδί κρυπτογραφημένα έπειτα από την απαίτηση εισαγωγής κωδικού κατά την επαναφορά του backup. Το δημόσιο κλειδί παραμένει σε μορφή απλού κειμένου όπως προηγουμένως.

"labels"

Στην αρχική δοκιμή μας είχε εντοπιστεί ένα τμήμα του αρχείου “default_wallet” που εξετάσαμε με το όνομα "labels", το οποίο περιείχε ετικέτες (ονόματα) που έδωσε ο χρήστης της εφαρμογής σε κάποιες από τις συναλλαγές του. Όπως παρατηρούμε στο πορτοφόλι που επαναφέραμε, το τμήμα αυτό δεν αποθηκεύεται και συνεπώς δεν μεταφέρεται κατά την επαναφορά του πορτοφολιού μας, οπότε, ότι πληροφορίες είχαμε από αυτό το τμήμα, τώρα δεν υπάρχουν.

"payment_requests"

Ομοίως με το τμήμα “labels”, το τμήμα του αρχείου με όνομα "payment_requests", που περιείχε τις διευθύνσεις τις οποίες φαίνεται να χρησιμοποίησε ο χρήστης προκειμένου να ζητήσει από κάποιον άλλον χρήστη να του αποστείλει χρήματα, δεν επαναφέρεται κατά την επαναφορά του πορτοφολιού μας από το backup και οι πληροφορίες που είχαμε αντλήσει στο προηγούμενο παράδειγμά μας, τώρα δεν υπάρχουν.

Παρά την κρυπτογράφηση του πορτοφολιού μας και την μη επαναφορά ορισμένων εκ των τμημάτων του αρχείου που παρουσίαζε ενδιαφέρον και στις δύο δοκιμές μας, παρατηρούμε ότι τα τμήματα (“addr_history”, "addresses", "transactions", "txi", "txo" & "verified_tx3"), που συνεχίζουν να υπάρχουν και σε αυτή τη δοκιμή, περιέχουν ιδιαίτερα

σημαντικά στοιχεία για τις συναλλαγές που πραγματοποίησε ο χρήστης της εφαρμογής. Τα τμήματα αυτά αναλύθηκαν στο προηγούμενο παράδειγμα, οπότε δεν υπάρχει λόγος να επαναληφθεί η διαδικασία.

Κρυπτογράφηση του πορτοφολιού που επαναφέραμε μετά το Backup - Electrum Bitcoin Wallet

Όπως αναφέραμε παραπάνω, μετά την αναβάθμιση της εφαρμογής ζητείται η εισαγωγή κωδικού για την κρυπτογράφηση του πορτοφολιού. Η εφαρμογή δεν παρέχει κάποιου άλλου είδους κρυπτογράφησης ή εισαγωγής κωδικού, οπότε στην προηγούμενη ανάλυσή μας το πορτοφόλι ήταν ήδη κρυπτογραφημένο. Επομένως, τα ευρήματα αυτής της δοκιμής είναι ακριβώς τα ίδια με αυτά που περιγράφηκαν στην προηγούμενη ανάλυσή μας.

Εφαρμογή Bitcoin Wallet

Εγκατάσταση της εφαρμογής Bitcoin Wallet

Η εφαρμογή βρίσκεται στο Play Store και την στιγμή των δοκιμών βρισκόταν στην έκδοση 6.06. Σύμφωνα με τους δημιουργούς της, η εφαρμογή είναι ανοικτού κώδικα και ο πηγαίος κώδικάς της βρίσκεται στο GitHub στον σύνδεσμο https://github.com/bitcoin-wallet/bitcoin-wallet . Παρέχει απλές αλλά βασικές λειτουργίες του Bitcoin, που είναι κυρίως η αποστολή και λήψη και είναι ένα Hierarchical Deterministic Wallet (HD), όπως τα προηγούμενα πορτοφόλια που εξετάσαμε. Η εφαρμογή είναι πολύ δημοφιλής στο Play Store και έχει περίπου 1.000.000+ λήψεις σύμφωνα με τα στοιχεία της Google.

Η εφαρμογή παρέχει έναν διαφορετικό τρόπο δημιουργίας του πορτοφολιού, συγκριτικά με τις προηγούμενες εφαρμογές που εξετάσαμε. Με την είσοδό μας στην εφαρμογή, έχει ήδη δημιουργηθεί το πορτοφόλι μας και είμαστε έτοιμοι για την αποστολή και την λήψη bitcoin, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 78). Δεν εμφανίζει κάποια μνημονική ακολουθία λέξεων (seed) ζητώντας να την αποθηκεύσουμε για μελλοντική επαναφορά του πορτοφολιού μας, αλλά δίνει την δυνατότητα δημιουργίας backup μέσα από το μενού της εφαρμογής και την επιλογή δημιουργίας αντιγράφου του πορτοφολιού. Κατά την δημιουργία αντιγράφου του πορτοφολιού ζητείται η εισαγωγή κωδικού για την κρυπτογράφηση του (Στιγμιότυπο 79) και δημιουργείται ένα αρχείο το οποίο μπορεί να εξαχθεί από το κινητό μας τηλέφωνο και να αποθηκευτεί οπουδήποτε για

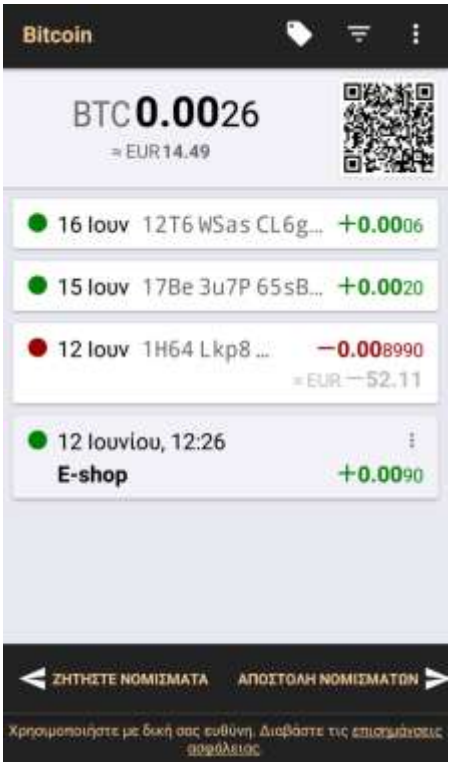
ασφάλεια, ώστε να χρησιμοποιηθεί σε περίπτωση που χρειαστούμε την επαναφορά του (Στιγμιότυπο 80).

Στιγμιότυπο 78 – Δημιουργία νέου πορτοφολιού Bitcoin Wallet

Στιγμιότυπο 79 – Δημιουργία backup του πορτοφολιού Bitcoin Wallet και εισαγωγή κωδικού

Στιγμιότυπο 80 – Αποθήκευση του backup του πορτοφολιού στον εξωτερικό αποθηκευτικό χώρου της συσκευής για μελλοντική χρήση

Αφού ολοκληρώσαμε την εγκατάσταση της εφαρμογής και την δημιουργία αντιγράφου του πορτοφολιού, πραγματοποιήσαμε κάποιες συναλλαγές, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 81), ενώ σε μια διεύθυνση του πορτοφολιού δόθηκε όνομα ετικέτας (Στιγμιότυπο 82).



Στιγμιότυπο 81 – Ιστορικό συναλλαγών που πραγματοποιήθηκαν με την εφαρμογή Bitcoin Wallet

Στιγμιότυπο 82 – Δημιουργημένες διευθύνσεις bitcoin και ετικέτες αυτών

Εγκληματολογική εξέταση της εφαρμογής Bitcoin Wallet

Το όνομα του πακέτου εγκατάστασης της εφαρμογής είναι το “de.schildbach.wallet” και κατά την εγκατάσταση η εφαρμογή δημιουργεί τον ομώνυμο φάκελο στην διαδρομή του καταλόγου /data/data. Κάνοντας χρήση του εργαλείου ADB εξαγάγουμε τους φακέλους που δημιουργήθηκαν κατά την εγκατάσταση.

Οι φάκελοι που περιέχονται στην διαδρομή /data/data και εντός του φακέλου “de.schildbach.wallet”, είναι οι (app_blockstore, cache, code_cache, databases, files και shared_prefs).

Από αυτούς τους φακέλους ενδιαφέρον παρουσιάζουν οι φάκελοι με τα αρχεία:

- de.schildbach.wallet/databases/
  - address_book
  - address_book-journal
- de.schildbach.wallet/files/log/
  - wallet.2018-06-15.log.gz/wallet.2018-06-15.log
  - wallet.2018-06-16.log.gz/wallet.2018-06-16.log

wallet.log

- de.schildbach.wallet/files/log/

wallet-protobuf

key-backup-protobuf

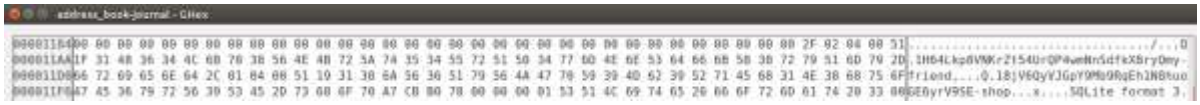
Το αρχείο de.schildbach.wallet/databases/address_book, είναι μία βάση δεδομένων SQLite, που περιέχει τρείς πίνακες. Εγκληματολογικό ενδιαφέρον παρουσιάζει ο πίνακας με όνομα address_book, ο οποίος περιέχει μία διεύθυνση bitcoin συνοδευόμενη από μία ετικέτα με όνομα "E-shop", όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 83). Η διεύθυνση αυτή είναι μια από τις διευθύνσεις του πορτοφολιού που δημιουργήθηκε από την εφαρμογή, στην οποία ο χρήστης έδωσε την ετικέτα με όνομα "E-shop". Το πορτοφόλι δημιούργησε αρκετές διευθύνσεις, όμως στον παρακάτω πίνακα εμφανίζονται μόνο οι διευθύνσεις τις οποίες ο χρήστης χαρακτήρισε με κάποια ετικέτα.

Table: address_book

	_id	address	label
	Filter	Filter	Filter
1	1	18jV6QyVJGpY9Mb9RqEh1N8huoGE6yrV9S	E-shop

Στιγμιότυπο 83 – Πίνακας αποθήκευσης των bitcoin διευθύνσεων που προσδιορίστηκαν με ετικέτα από τον χρήστη της εφαρμογής

Το αρχείο de.schildbach.wallet/databases/address_book-journal, είναι το αρχείο journal της βάσης δεδομένων address_book που εξετάσαμε νωρίτερα. Όπως είναι αναμενόμενο παρατηρούμε την ύπαρξη της διεύθυνσης που υπάρχει στην βάση δεδομένων address_book, συνοδευόμενη από το όνομα "E-shop", ωστόσο παρατηρούμε και την ύπαρξη της διεύθυνσης 1H64Lkp8VNKrZt54UrQP4wmNnSdfkX8ryQ συνοδευόμενη από το όνομα "my-friend", την οποία δεν βρήκαμε αποθηκευμένη στην βάση δεδομένων address_book (Στιγμιότυπο 84). Η διεύθυνση αυτή δεν αποτελεί διεύθυνση του πορτοφολιού του χρήστη, αλλά κάποια διεύθυνση στην οποία ο χρήστης έστειλε χρήματα και στην οποία έδωσε το όνομα "my-friend" ενώ αργότερα την διέγραψε.

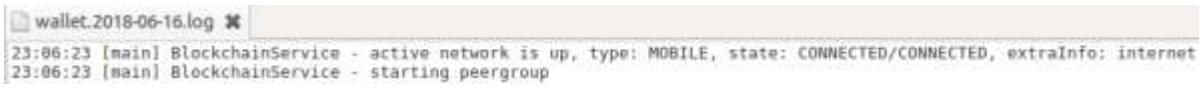


Στιγμιότυπο 84 – Άλλες διευθύνσεις bitcoin με ετικέτα από τον χρήστη

Ο φάκελος de.schildbach.wallet/files/log/ περιέχει ένα αρχείο με όνομα wallet.log και επτά συμπιεσμένα αρχεία με την μορφή "wallet.YEAR-MONTH-DAY.log.gz" που περιέχουν αρχεία καταγραφής (log files) που αφορούν τις ημερομηνίες από 15-06-2018 έως 21-06-2018 όπως δηλώνει και το όνομά τους. Από την χρήση της εφαρμογής παρατηρήθηκε ότι η εφαρμογή διατηρεί και αποθηκεύει τα αρχεία καταγραφής που δημιουργεί για χρονικό διάστημα επτά ημερών. Από τα αρχεία που υπάρχουν στον φάκελο περισσότερο ενδιαφέρον παρουσιάζουν τα αρχεία wallet.2018-06-15.log.gz/wallet.2018-06-15.log, wallet.2018-06-16.log.gz/wallet.2018-06-16.log και το αρχείο wallet.log, όπως θα τα αναλύσουμε στην συνέχεια. Τις υπόλοιπες ημερομηνίες δεν πραγματοποιήθηκε κάποια συναλλαγή, επομένως τα log αρχεία που δημιουργήθηκαν δεν παρουσιάζουν ιδιαίτερο ενδιαφέρον για περισσότερη ανάλυση.

Σε όλα τα προαναφερόμενα αρχεία καταγραφής υπάρχουν τα στοιχεία που αφορούν το δίκτυο στο οποίο συνδέθηκε ο χρήστης της εφαρμογής όπως φαίνεται στις παρακάτω εικόνες. Αν είναι κάποιο δίκτυο wifi εμφανίζεται το όνομα του δικτύου (Στιγμιότυπο 85), ενώ αν είναι μέσω δικτύου κινητής τηλεφωνίας εμφανίζεται η λέξη internet (Στιγμιότυπο 86).

Στιγμιότυπο 85 – Είδος δικτύου και όνομα δικτύου σύνδεσης που χρησιμοποίησε ο χρήστης για πρόσβαση στην εφαρμογή Bitcoin Wallet - WIFI



Στιγμιότυπο 86 - Είδος δικτύου και όνομα δικτύου σύνδεσης που χρησιμοποίησε ο χρήστης για πρόσβαση στην εφαρμογή Bitcoin Wallet - MOBILE

Το αρχείο wallet.2018-06-15.log.gz/wallet.2018-06-15.log περιέχει αρκετά δεδομένα, γι' αυτό θα εξετάσουμε τα πιο σημαντικά από αυτά. Στο αρχείο εμπεριέχεται μια συναλλαγή

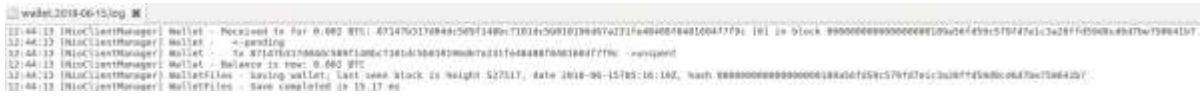
που πραγματοποιήθηκε από το πορτοφόλι μας. Στην επόμενη εικόνα (Στιγμιότυπο 87) φαίνεται το τμήμα του αρχείου όπου ο χρήστης της εφαρμογής κάνει αίτηση για λήψη χρημάτων σε μια από τις διευθύνσεις του πορτοφολιού του (04:59:44 [main] RequestCoinsFragment - request coins started: 17Be3u7P65sBLpArVLmtxpjSzqw8zBSDtd), η αίτηση για αντιγραφή της διεύθυνσης στο πρόχειρο (04:59:47 [main] RequestCoinsFragment - payment request copied to clipboard: bitcoin:17Be3u7P65sBLpArVLmtxpjSzqw8zBSDtd) καθώς και η αίτηση για διαμοιρασμό της διεύθυνσης με άλλον χρήστη (05:00:02 [main] RequestCoinsFragment - payment request shared via intent: bitcoin:17Be3u7P65sBLpArVLmtxpjSzqw8zBSDtd).

Στιγμιότυπο 87 – Καταγεγραμμένη διεύθυνση bitcoin και διαμοιρασμού της για την λήψη χρημάτων

Στη συνέχεια φαίνεται ότι το πορτοφόλι αντιλαμβάνεται την λήψη bitcoin και το καταγράφει όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 88). Αναλυτικά στο αρχείο καταγραφής φαίνεται το ποσό που επρόκειτο να σταλεί στο πορτοφόλι μας, καθώς και το υπολογιζόμενο υπόλοιπο μετά την ολοκλήρωση της συναλλαγής.

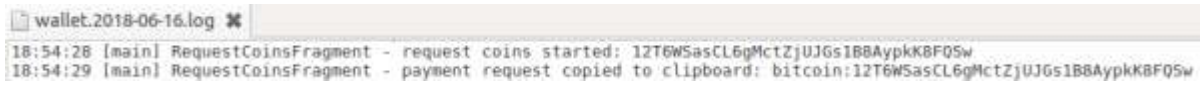
Στιγμιότυπο 88 – Λεπτομέρειες επικείμενης συναλλαγής bitcoin και υπόλοιπο πορτοφολιού Bitcoin Wallet

Με την ολοκλήρωση της συναλλαγής το πορτοφόλι προβαίνει στην καταγραφή της καθώς και στον υπολογισμό του υπολοίπου του πορτοφολιού, όπως φαίνεται παρακάτω (Στιγμιότυπο 89).



Στιγμιότυπο 89 – Λεπτομέρειες επιβεβαιωμένης συναλλαγής bitcoin και υπόλοιπο του πορτοφολιού

Το αρχείο wallet.2018-06-16.log.gz/wallet.2018-06-16.log περιέχει κι αυτό μία συναλλαγή που πραγματοποιήθηκε εκείνη την ημερομηνία. Αρχικά φαίνεται η αίτηση που έκανε ο χρήστης της εφαρμογής για λήψη bitcoin σε κάποια από τις διευθύνσεις του πορτοφολιού του (Στιγμιότυπο 90).



Στιγμιότυπο 90 – Αίτηση λήψης bitcoin σε επιλεγμένη από τον χρήστη διεύθυνση

Στη συνέχεια φαίνεται το ποσό που πρόκειται να ληφθεί από το πορτοφόλι μας καθώς και το νέο υπολογισμένο υπόλοιπο μετά την ολοκλήρωση της συναλλαγής (Στιγμιότυπο 91).

Στιγμιότυπο 91 - Λεπτομέρειες επικείμενης λήψης bitcoin στην επιλεγμένη από τον χρήστη διεύθυνση και υπόλοιπο πορτοφολιού Bitcoin Wallet

Μόλις η συναλλαγή ολοκληρωθεί, το πορτοφόλι καταγράφει την λήψη που πραγματοποιήθηκε και το καινούριο υπόλοιπο (Στιγμιότυπο 92).

Στιγμιότυπο 92 - Λεπτομέρειες επιβεβαιωμένης λήψης bitcoin στην επιλεγμένη από τον χρήστη διεύθυνση και υπόλοιπο πορτοφολιού Bitcoin Wallet

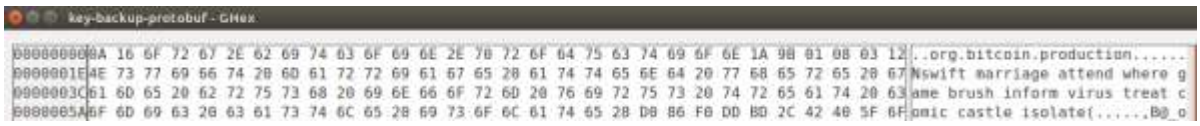
Το αρχείο wallet.log είναι το τελευταίο αρχείο καταγραφής και εμφανίζει την τελευταία αίτηση που έκανε ο χρήστης της εφαρμογής για τη λήψη bitcoin (Στιγμιότυπο 93). Ωστόσο δεν φαίνεται να κατάφερε να ολοκληρώσει την συναλλαγή καθόσον δεν προκύπτουν δεδομένα καταγραφής της.

Στιγμιότυπο 93 – Αίτηση συναλλαγής λήψης bitcoin που όμως δεν πραγματοποιήθηκε

Το αρχείο de.schildbach.wallet/files/log/wallet-protobuf αποτελεί το αρχείο του πορτοφολιού μας και παρατηρούμε ότι περιέχει την μνημονική ακολουθία λέξεων “admit away avocado public stable alter wrist fever worry announce bring club” σε μορφή απλού κειμένου (Στιγμιότυπο 94), παρόλο που δεν μας την εμφάνισε καθόλου κατά την εγκατάσταση της εφαρμογής. Όπως έχουμε αναφέρει, η κατοχή της ακολουθίας αυτής μας παρέχει πλήρη πρόσβαση στα bitcoin του χρήστη. Επιπλέον, μπορούμε να ξανά-παράγουμε τις διευθύνσεις του πορτοφολιού του χρήστη και να εξετάσουμε αυτές που περιέχουν κάποιο υπόλοιπο.

Στιγμιότυπο 94 - Η μνημονική ακολουθία λέξεων του πορτοφολιού Bitcoin Wallet σε μορφή απλού κειμένου

Το αρχείο de.schildbach.wallet/files/log/key-backup-protobuf παρατηρούμε ότι περιέχει κι αυτό μία μνημονική ακολουθία λέξεων “swift marriage attend where game brush inform virus treat comic castle isolate”, η οποία όμως είναι διαφορετική από αυτή που υπάρχει στο αρχείο του πορτοφολιού μας “wallet-protobuf” και υποθέτουμε ότι έχει παραμείνει αποθηκευμένη μετά από κάποια παλαιότερη επαναφορά backup του πορτοφολιού μας (Στιγμιότυπο 95). Όμοια με προηγουμένως θα μπορούσαμε να εξετάσουμε το υπόλοιπο του πορτοφολιού που δημιουργήθηκε από αυτή την ακολουθία λέξεων, αλλά και να αποκτήσουμε πλήρως τα bitcoin του χρήστη.



Στιγμιότυπο 95 – Αποθηκευμένη μνημονική ακολουθία λέξεων από προηγούμενη επαναφορά backup πορτοφολιού

Επαναφορά πορτοφολιού από Backup Bitcoin Wallet

Η επόμενη δοκιμή που θα κάνουμε στην εφαρμογή Bitcoin Wallet είναι η διαγραφή της από το κινητό μας τηλέφωνο, η επανεγκατάσταση της και η επαναφορά του πορτοφολιού από το backup που δημιουργήσαμε μετά την εγκατάστασή της.

Όταν πραγματοποιήθηκε αυτή η δοκιμή, η εφαρμογή είχε αναβαθμιστεί στην έκδοση 6.28. Επομένως, παράλληλα με την εξέταση των δεδομένων που μπορούμε να συλλέξουμε μετά την επαναφορά του backup, θα εξετάσουμε τυχόν μεταβολές σε αρχεία του πακέτου εγκατάστασης και κατά πόσο υπάρχει κάτι άξιο ενδιαφέροντος που προστέθηκε μετά την αναβάθμιση.

Παρά την αναβάθμιση, η εφαρμογή δημιουργεί τους ίδιους φακέλους στο πακέτο εγκατάστασής της στην διαδρομή /data/data και συγκεκριμένα τους εξής: (app_blockstore, cache, code_cache, databases, files και shared_prefs).

Από αυτούς τους φακέλους ενδιαφέρον παρουσιάζουν οι φάκελοι με τα αρχεία:

- de.schildbach.wallet/files/log/
  wallet.2018-07-16.log.gz/wallet.2018-07-16.log
  wallet.2018-07-21.log.gz/wallet.2018-07-21.log
- de.schildbach.wallet/files/log/
  wallet-protobuf
  key-backup-protobuf

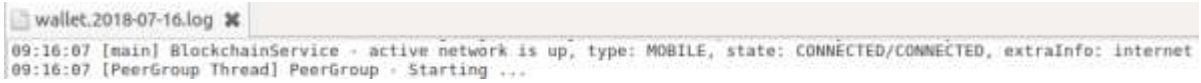
Η βάση δεδομένων de.schildbach.wallet/databases/address_book, που στην προηγούμενη δοκιμή μας είχε αποθηκευμένη μια bitcoin διεύθυνση συνοδευόμενη από την ετικέτα που της είχε προσδώσει ο χρήστης, παρατηρούμε ότι μετά την επαναφορά του πορτοφολιού δεν διατηρεί τα δεδομένα αυτά και πλέον ο πίνακας διευθύνσεων είναι κενός.

Όπως και στην προηγούμενη δοκιμή μας, ο φάκελος de.schildbach.wallet/files/log/ περιέχει ένα αρχείο με όνομα wallet.log και επτά συμπιεσμένα αρχεία με την μορφή wallet.YEAR-MONTH-DAY.log.gz που περιέχουν αρχεία καταγραφής (log files) των τελευταίων επτά ημερών, που αφορούν τις ημερομηνίες από 16-07-2018 έως 22-07-2018 όπως δηλώνει και το όνομά τους.

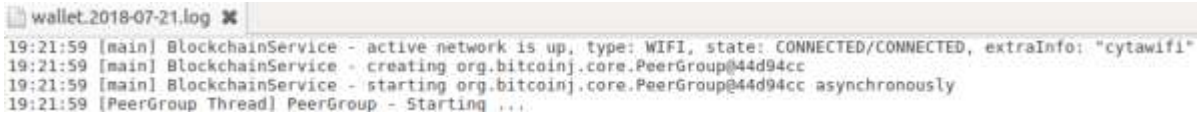
Στα αρχεία καταγραφής των επτά τελευταίων ημερών δεν παρατηρήθηκε η διενέργεια κάποιας συναλλαγής, ωστόσο παρατηρούμε ότι έχει καταγραφεί απόπειρα συναλλαγής του χρήστη που όμως δεν ολοκληρώθηκε. Ενδεικτικά θα δούμε τις συναλλαγές που

αποπειράθηκε να πραγματοποιήσει ο χρήστης, αλλά δεν ολοκλήρωσε σε δύο αρχεία καταγραφής για τις ημερομηνίες 16 και 21-07-2018.

Σε όλα τα προαναφερόμενα αρχεία καταγραφής, όπως και στην προηγούμενη δοκιμή μας, υπάρχουν τα στοιχεία που αφορούν το δίκτυο στο οποίο συνδέθηκε ο χρήστης της εφαρμογής όπως φαίνεται στις παρακάτω εικόνες. Αν είναι κάποιο δίκτυο wifi εμφανίζεται το όνομα του δικτύου (Στιγμιότυπο 96), ενώ αν είναι μέσω δικτύου κινητής τηλεφωνίας εμφανίζεται η λέξη internet (Στιγμιότυπο 97).



Στιγμιότυπο 96 - Είδος δικτύου και όνομα δικτύου σύνδεσης που χρησιμοποίησε ο χρήστης για πρόσβαση στην εφαρμογή Bitcoin Wallet - MOBILE



Στιγμιότυπο 97 - Είδος δικτύου και όνομα δικτύου σύνδεσης που χρησιμοποίησε ο χρήστης για πρόσβαση στην εφαρμογή Bitcoin Wallet - WIFI

Στο αρχείο καταγραφής wallet.2018-07-16.log.gz/wallet.2018-07-16.log υπάρχουν δύο συναλλαγές που φαίνεται να δοκίμασε να κάνει ο χρήστης, πλην όμως δεν προχώρησε στην ολοκλήρωσή τους, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο 98). Και οι δύο αφορούν το άδειασμα του πορτοφολιού με βάση τα στοιχεία που αναφέρονται στις συναλλαγές, ήτοι την αποστολή ποσού 0.0026 bitcoin, ωστόσο δεν αναγράφεται η διεύθυνση bitcoin που θα επέλεγε ο χρήστης για να αποστείλει το αναγραφόμενο ποσό.

09:15:54 [main] Wallet - Completing send tx with 1 outputs totalling 0.0026 BTC and a fee of 0.00055 BTC/kB
09:15:54 [main] Wallet - emptying 0.0026 BTC

Στιγμιότυπο 98 – Ανολοκλήρωτες προσπάθειες πραγματοποίησης συναλλαγών από τον χρήστη της εφαρμογής Bitcoin Wallet

Το αρχείο καταγραφής wallet.2018-07-21.log.gz/wallet.2018-07-21.log περιέχει τις προηγούμενες δύο συναλλαγές, που όπως φαίνεται ξαναδοκίμασε να κάνει ο χρήστης, χωρίς πάλι να έχει συμπληρώσει την διεύθυνση αποστολής των χρημάτων (Στιγμιότυπο 99).

Από την στιγμή που τα αρχεία καταγραφής δεν περιλαμβάνουν ολοκληρωμένες συναλλαγές και η εν λόγο συναλλαγή αφορούσε το άδειασμα του πορτοφολιού, αλλά δεν ολοκληρώθηκε, μπορούμε να συμπεράνουμε ότι το συνολικό ποσό που διαθέτει ο χρήστης είναι 0.0026 bitcoin.

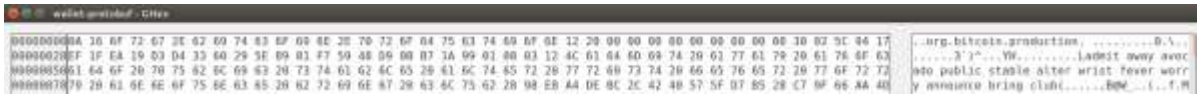
Στιγμιότυπο 99 – Δεύτερη ανολοκλήρωτη προσπάθεια πραγματοποίησης συναλλαγής από τον χρήστη

Στο ίδιο αρχείο καταγραφής, παρατηρούμε και κάτι επιπλέον. Ο χρήστης αιτήθηκε σε μία διεύθυνση του πορτοφολιού του την λήψη bitcoin, την οποία αντέγραψε στο πρόχειρο και φαίνεται να μοίρασε μέσω internet, όπως φαίνεται στην παρακάτω εικόνα (Στιγμιότυπο

100). Παρά το ότι δεν προκύπτει να έλαβε σε αυτή την διεύθυνση bitcoin, θα μπορούσαμε να χρησιμοποιήσουμε κάποιον εξερευνητή της αλυσίδας blockchain του Bitcoin και να δούμε το κατά πόσο η διεύθυνση αυτή χρησιμοποιήθηκε σε κάποια συναλλαγή.

Στιγμιότυπο 100 – Διεύθυνση αίτησης λήψης bitcoin του πορτοφολιού του χρήστη Bitcoin Wallet

Το αρχείο de.schildbach.wallet/files/log/wallet-protobuf αποτελεί το αρχείο του πορτοφολιού που επαναφέραμε και όπως φαίνεται στην παρακάτω εικόνα περιέχει την μνημονική ακολουθία λέξεων “admit away avocado public stable alter wrist fever worry announce bring club” σε μορφή απλού κειμένου (Στιγμιότυπο 101). Όπως έχουμε αναφέρει, η κατοχή της ακολουθίας αυτής μας παρέχει πλήρη πρόσβαση στα bitcoin του χρήστη. Επιπλέον, μπορούμε να ξανά-παράγουμε τις διευθύνσεις του πορτοφολιού του χρήστη και να εξετάσουμε αυτές που περιέχουν κάποιο υπόλοιπο.



Στιγμιότυπο 101 - Η μνημονική ακολουθία λέξεων του πορτοφολιού Bitcoin Wallet σε μορφή απλού κειμένου μετά την επαναφορά από backup

Το αρχείο “de.schildbach.wallet/files/log/key-backup-protobuf” αυτή την φορά παρατηρούμε ότι περιέχει την ίδια μνημονική ακολουθία λέξεων “admit away avocado public stable alter wrist fever worry announce bring club” με το αρχείο wallet-protobuf, που όπως φαίνεται λειτουργεί ως backup του κυρίως πορτοφολιού μας (Στιγμιότυπο 102). Όμοια με προηγουμένως θα μπορούσαμε να εξετάσουμε πορτοφόλι που δημιουργήθηκε από αυτή την ακολουθία λέξεων, αλλά και να αποκτήσουμε πλήρως τα bitcoin του χρήστη.

Στιγμιότυπο 102 – Δεύτερο αρχείο στο οποίο εμπεριέχεται η μνημονική ακολουθία λέξεων του πορτοφολιού Bitcoin Wallet σε μορφή απλού κειμένου μετά την επαναφορά από backup

Κρυπτογράφηση του πορτοφολιού που επαναφέραμε μετά το Backup Bitcoin Wallet

Η εφαρμογή που εξετάζουμε παρόλο που κατά την δημιουργία backup ζητάει κωδικό για την κρυπτογράφηση του πορτοφολιού, με την επαναφορά του backup, το πορτοφόλι μας αποκρυπτογραφείται και αποθηκεύεται με μορφή απλού κειμένου όπως είδαμε στην προηγούμενη δοκιμή μας. Ωστόσο, η εφαρμογή προσφέρει την δυνατότητα εισαγωγής κωδικού για την πραγματοποίηση συναλλαγών ξοδέματος bitcoin. Δεδομένου αυτού του χαρακτηριστικού, θα θέσουμε έναν κωδικό μέσω του μενού της εφαρμογής και θα εξετάσουμε ξανά το πορτοφόλι μας, εξάγοντας τα αρχεία του πακέτου μέσω του εργαλείου ADB.

Από τα αρχεία που εξαγάγαμε, ενδιαφέρον παρουσιάζουν τα κάτωθι:

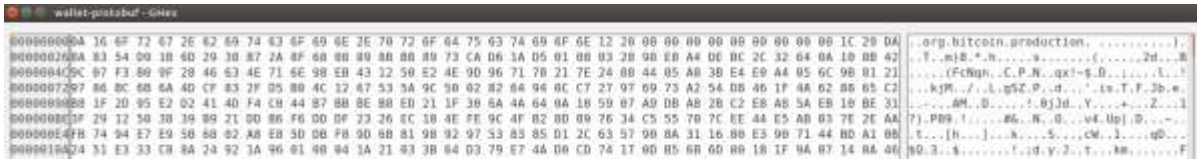
- de.schildbach.wallet/files/log/
  wallet.2018-07-21.log.gz/wallet.2018-07-21.log
- de.schildbach.wallet/files/log/
  wallet-protobuf
  key-backup-protobuf

Τα αρχεία καταγραφής που εξετάσαμε προηγουμένως, δεν μεταβάλλονται καθόλου όταν αφορούν ίδιες ημερομηνίες, επομένως δεν επηρεάζονται από την εισαγωγή του κωδικού. Σε αυτή την δοκιμή μας έχει δημιουργηθεί ένα νέο αρχείο καταγραφής που αφορά την ημερομηνία 23/07/2018 ενώ έχει διαγραφεί το αρχείο που αφορά την ημερομηνία 16/07/2018, καθόσον όπως είπαμε διατηρούνται μόνο τα αρχεία που αφορούν τις τελευταίες επτά ημέρες. Το αρχείο καταγραφής με ημερομηνία 23/07/2018 δεν περιέχει κάτι άξιο αναφοράς από εγκληματολογικής άποψης.

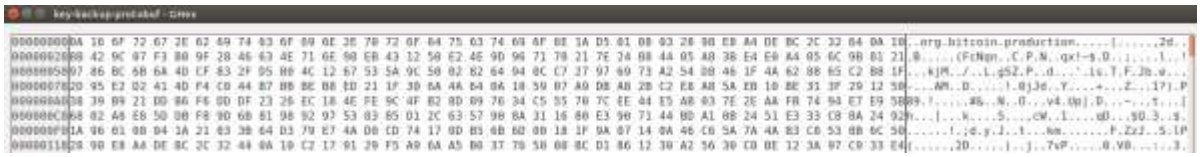
Το αρχείο wallet.2018-07-21.log.gz/wallet.2018-07-21.log, όπως είπαμε δεν μεταβάλλεται, οπότε οι ανολοκλήρωτες συναλλαγές που αναλύσαμε προηγουμένως παραμένουν ως έχουν (Στιγμιότυπο 99).

Η εισαγωγή κωδικού που πραγματοποιήσαμε, παρατηρούμε ότι κρυπτογράφησε τα δύο αρχεία του πορτοφολιού μας, δηλαδή τόσο το αρχείο wallet-protobuf όσο και το αρχείο

key-backup-protobuf, όπως φαίνεται στις παρακάτω εικόνες (Στιγμιότυπο 103 και Στιγμιότυπο 104). Επομένως, ενώ στις προηγούμενες δοκιμές μας μπορούσαμε να δούμε με την μορφή απλού κειμένου την μνημονική ακολουθία λέξεων και να αποκτήσουμε πλήρη πρόσβαση στο πορτοφόλι του χρήστη, αυτό δεν είναι εφικτό σε αυτή την δοκιμή μας.



Στιγμιότυπο 103 – Κρυπτογραφημένη μνημονική ακολουθία λέξεων μετά την εισαγωγή κωδικού ξοδέματος



Στιγμιότυπο 104 – Το δεύτερο αρχείο που εμφάνιζε την μνημονική ακολουθία λέξεων σε μορφή απλού κειμένου, την κρυπτογραφεί και αυτό

Συμπέρασμα

Οι εφαρμογές πορτοφόλια Bitcoin εξελίσσονται με ταχύτατους ρυθμούς. Χαρακτηριστικά καινούρια προστίθενται συνεχώς δίνοντας στον χρήστη περισσότερες επιλογές για τον έλεγχο των χρημάτων του. Τα χαρακτηριστικά αυτά αφορούν την ευκολία χρήσης της εφαρμογής, την ταχύτητα των συναλλαγών, την προσθήκη περισσότερων πληροφοριών στις συναλλαγές του χρήστη, την προστασία της ιδιωτικότητας του χρήστη, την μεγαλύτερη ασφάλεια του χρήστη στην αποθήκευση των χρημάτων του κ.τ.λ. Αυτό έχει ως αποτέλεσμα οι εφαρμογές να αναβαθμίζονται σε σχετικά σύντομα χρονικά διαστήματα για να υποστηρίξουν και να βελτιστοποιήσουν τα όσα αναφέραμε. Όπως αναφέραμε στο κεφάλαιο της «Ανάλυσης εφαρμογών κινητών τηλεφώνων», η μέθοδος που θα πρέπει να χρησιμοποιήσει ένας αναλυτής δεν μπορεί να περιγραφεί με κάποιον οδηγό αλλά θα πρέπει να προσαρμόζεται στις αντίστοιχες συνθήκες έχοντας πάντα ως στόχο την υγιή ανάλυση της εφαρμογής.

Στην ανάλυση που πραγματοποιήσαμε παρατηρήσαμε ότι στις τέσσερις από τις πέντε εφαρμογές, αν ο χρήστης κατά την εγκατάσταση της εφαρμογής επιλέξει να μην εισάγει κάποιον κωδικό που θα κρυπτογραφούσε το πορτοφόλι του, τότε μπορούμε εύκολα σχετικά

να αποκτήσουμε πρόσβαση είτε στην μνημονική ακολουθία λέξεων είτε στα ιδιωτικά κλειδιά του πορτοφολιού και κατ' επέκταση να αποκτήσουμε πρόσβαση στα χρήματα του χρήστη. Η πλήρης πρόσβαση στο πορτοφόλι του χρήστη συνεχίζει να υπάρχει και μετά την επαναφορά του πορτοφολιού από το backup και μόνο όταν επιλεχθεί η εισαγωγή κωδικού δυσκολεύει έως και αδυνατούμε τελείως να αποκτήσουμε πρόσβαση στο πορτοφόλι του χρήστη.

Συγκεκριμένα:

Στην εφαρμογή Copay μπορούμε να αποκτήσουμε εύκολα πρόσβαση στην μνημονική ακολουθία λέξεων αν ο χρήστης δεν επιλέξει την εισαγωγή κωδικού, πράγμα το οποίο συνεχίζει να ισχύει και κατά την επαναφορά του πορτοφολιού από το backup. Η μνημονική ακολουθία λέξεων κρυπτογραφείται όταν επιλεγεί η εισαγωγή κωδικού από τον χρήστη είτε κατά την δημιουργία του πορτοφολιού είτε σε μεταγενέστερο στάδιο. Τα ίδια με την εφαρμογή Copay ισχύουν και για την εφαρμογή Coinomi που αναλύσαμε.

Στην εφαρμογή Mycelium τα πράγματα είναι κάπως διαφορετικά καθόσον η εφαρμογή φαίνεται να κρυπτογραφεί την μνημονική ακολουθία λέξεων με την εγκατάστασή της χωρίς να χρησιμοποιεί κάποιον κωδικό που δίνεται από τον χρήστη, κάτι που ισχύει και κατά την επαναφορά του πορτοφολιού από backup. Ωστόσο, στην επιλογή που δίνεται στον χρήστη για την εισαγωγή κωδικού με σκοπό την αποτροπή αποστολής bitcoin, παρατηρήσαμε ότι ο κωδικός αποθηκεύεται σε μορφή απλού κειμένου και επομένως μπορεί να αποκτηθεί εύκολα.

Η εφαρμογή Electrum στην πρώτη έκδοση που δοκιμάσαμε έδινε την επιλογή παράκαμψης της εισαγωγής κωδικού και η μνημονική ακολουθία λέξεων αποθηκευόταν με την μορφή απλού κειμένου. Με την αναβάθμιση της εφαρμογής, ο χρήστης ήταν αναγκασμένος να εισάγει κωδικό, ο οποίος κρυπτογραφούσε το πορτοφόλι και την μνημονική ακολουθία λέξεων, είτε κατά την δημιουργία του πορτοφολιού είτε κατά την επαναφορά από backup, οπότε δεν μπορούσαμε πλέον να αποκτήσουμε πρόσβαση στα bitcoin του χρήστη.

Η εφαρμογή BitcoinWallet δεν χρησιμοποιούσε κατά την εγκατάστασή της την δυνατότητα δημιουργίας backup μέσω της μνημονικής ακολουθίας λέξεων, αλλά με την εξωτερική αποθήκευση του αρχείου του πορτοφολιού. Ωστόσο, από την εγκληματολογική ανάλυση που πραγματοποιήσαμε, η μνημονική ακολουθία λέξεων υπήρχε στα αρχεία της εφαρμογής σε μορφή απλού κειμένου τόσο κατά την εγκατάστασή της όσο και μετά την επαναφορά του πορτοφολιού από το backup, επομένως μπορούσαμε και πάλι να αποκτήσουμε πρόσβαση στα bitcoin του χρήστη με την χρήση μόνο της μνημονικής

ακολουθίας λέξεων. Ο χρήστης έπρεπε να χρησιμοποιήσει την εισαγωγή κωδικού για την αποτροπή αποστολής χρημάτων, μέσα από το μενού της εφαρμογής, προκειμένου να μην είναι δυνατή η πρόσβαση στην μνημονική ακολουθία λέξεων, η οποία με την εισαγωγή του κωδικού εμφανιζόταν πλέον κρυπτογραφημένη.

Σχεδόν σε όλες τις εφαρμογές που εξετάσαμε, οι επιπρόσθετες λειτουργίες που προσέφεραν, πέραν της απλής αποστολής - λήψης bitcoin και της δημιουργίας πορτοφολιών, δεν διατηρούσαν τα δεδομένα αυτά μετά την επαναφορά του πορτοφολιού από το backup, παρά μόνο στοιχεία που αφορούσαν υπόλοιπα του λογαριασμού, συναλλαγές του χρήστη, χρήση bitcoin διευθύνσεων κ.α. σχετικά με αυτό καθ' αυτό το πορτοφόλι του χρήστη.

Τέλος, παρατηρήθηκε ότι, για κάποια από τα πορτοφόλια δεν ήταν δυνατή η άντληση των δεδομένων που αφορούσαν τις συναλλαγές που είχαν πραγματοποιηθεί γιατί αυτές δεν αποθηκευόταν ξεχωριστά σε κάποιο αρχείο και πιθανόν αντλούσαν τα στοιχεία των συναλλαγών απευθείας από το δίκτυο Bitcoin, επομένως για την περαιτέρω ανάλυση των συναλλαγών έπρεπε να χρησιμοποιηθεί κάποιος εξερευνητής της αλυσίδας blockchain του Bitcoin, το οποίο δεν αποτελούσε αντικείμενο της παρούσας εργασίας και δεν πραγματοποιήθηκε.

Ενδεχομένως, λόγω αυτής της κατάστασης, να ήταν προτιμότερο, κατά την ανάλυση των εφαρμογών αυτών να συνδυαστεί η μέθοδος της λογικής απόκτησης με την μέθοδο της χειροκίνητης απόκτησης προκειμένου να διευκολυνθεί η εργασία του αναλυτή και να εξαχθούν ασφαλέστερα συμπεράσματα.

Στον παρακάτω πίνακα φαίνονται συνοπτικά τα σημαντικότερα ευρήματα που ανευρέθηκαν σε καθεμία εφαρμογή που εξετάστηκε και της κατάστασης που βρισκόταν το πορτοφόλι της εφαρμογής, στην εκάστοτε εξέταση μας.

Πίνακας σύγκρισης των σημαντικότερων ευρημάτων των εφαρμογών που εξετάστηκαν

1η εξέταση: Δημιουργία νέου πορτοφολιού χωρίς εισαγωγή κωδικού (όπου επιτρέπεται από την εφαρμογή).
2η εξέταση: Διαγραφή της εφαρμογής και επαναφορά του αρχικού πορτοφολιού από backup.
3η εξέταση: Κρυπτογράφηση (ή ορισμός κωδικού ξοδέματος) πορτοφολιού που επαναφέρθηκε από το backup.

ΕΦΑΡΜΟΓΕΣ ΣΗΜΑΝΤΙΚΟΤΕΡΑ ΕΥΡΗΜΑΤΑ	Copay	Mycelium	Coinomi	Electrum	BitcoinWallet
Μνημονική ακολουθία λέξεων	**1η εξέταση:** Σε μορφή απλού κειμένου **2η εξέταση:** Σε μορφή απλού κειμένου **3η εξέταση:** Κρυπτογραφημένη	**1η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένη **2η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένη **3η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένη	**1η εξέταση:** Σε μορφή απλού κειμένου **2η εξέταση:** Σε μορφή απλού κειμένου **3η εξέταση:** Κρυπτογραφημένη	**1η εξέταση:** Σε μορφή απλού κειμένου **2η εξέταση:** Κρυπτογραφήθηκε υποχρεωτικά λόγω αναβάθμισης της εφαρμογής μετά από την 1η εξέταση **3η εξέταση:** Κρυπτογραφημένη	**1η εξέταση:** Σε μορφή απλού κειμένου **2η εξέταση:** Σε μορφή απλού κειμένου **3η εξέταση:** Κρυπτογραφημένη
Ιδιωτικό κλειδί ρίζας	**1η εξέταση:** Σε μορφή απλού κειμένου **2η εξέταση:** Σε μορφή απλού κειμένου **3η εξέταση:** Κρυπτογραφημένο	**1η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο **2η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο **3η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο	**1η εξέταση:** Δεν ανευρέθη - θα μπορούσε να προσδιοριστεί με χρήση της μνημονικής ακολουθίας λέξεων **2η εξέταση:** Δεν ανευρέθη - θα μπορούσε να προσδιοριστεί με χρήση της μνημονικής ακολουθίας λέξεων **3η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο	**1η εξέταση:** Σε μορφή απλού κειμένου **2η εξέταση:** Κρυπτογραφήθηκε υποχρεωτικά λόγω αναβάθμισης της εφαρμογής μετά από την 1η εξέταση **3η εξέταση:** Κρυπτογραφημένο	**1η εξέταση:** Δεν ανευρέθη - θα μπορούσε να προσδιοριστεί με χρήση της μνημονικής ακολουθίας λέξεων **2η εξέταση:** Δεν ανευρέθη - θα μπορούσε να προσδιοριστεί με χρήση της μνημονικής ακολουθίας λέξεων **3η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο
Δημόσιο κλειδί ρίζας	**1η εξέταση:** Σε μορφή απλού κειμένου **2η εξέταση:** Σε μορφή απλού κειμένου	**1η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο **2η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο	**1η εξέταση:** Δεν ανευρέθη - θα μπορούσε να προσδιοριστεί με χρήση της μνημονικής ακολουθίας λέξεων	**1η εξέταση:** Σε μορφή απλού κειμένου **2η εξέταση:** Σε μορφή απλού κειμένου	**1η εξέταση:** Δεν ανευρέθη - θα μπορούσε να προσδιοριστεί με χρήση της μνημονικής ακολουθίας λέξεων

	3η εξέταση: Σε μορφή απλού κειμένου	**3η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο	**2η εξέταση:** Δεν ανευρέθη - θα μπορούσε να προσδιοριστεί με χρήση της μνημονικής ακολουθίας λέξεων **3η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο	**3η εξέταση:** Σε μορφή απλού κειμένου	**2η εξέταση:** Δεν ανευρέθη - θα μπορούσε να προσδιοριστεί με χρήση της μνημονικής ακολουθίας λέξεων **3η εξέταση:** Δεν ανευρέθη - πιθανόν κρυπτογραφημένο
Κωδικός ξοδέματος bitcoin	Η κρυπτογράφηση του πορτοφολιού αποτελεί παράλληλα και τον κωδικό ξοδέματος του πορτοφολιού	**1η εξέταση:** Δεν είχε εισαχθεί κωδικός από τον χρήστη **2η εξέταση:** Δεν είχε εισαχθεί κωδικός από τον χρήστη **3η εξέταση:** Σε μορφή απλού κειμένου	Η κρυπτογράφηση του πορτοφολιού αποτελεί παράλληλα και τον κωδικό ξοδέματος του πορτοφολιού	Η κρυπτογράφηση του πορτοφολιού αποτελεί παράλληλα και τον κωδικό ξοδέματος του πορτοφολιού	**1η εξέταση:** Δεν είχε εισαχθεί κωδικός από τον χρήστη **2η εξέταση:** Δεν είχε εισαχθεί κωδικός από τον χρήστη **3η εξέταση:** Δεν ανευρέθη – πιθανόν κρυπτογραφημένος
Υπόλοιπο λογαριασμού	**1η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής **2η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής **3η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής	**1η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής **2η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής **3η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής	**1η εξέταση:** Θα μπορούσε να προσδιοριστεί μόνο με εξέταση των αποθηκευμένων διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain **2η εξέταση:** Θα μπορούσε να προσδιοριστεί μόνο με εξέταση των αποθηκευμένων διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain **3η εξέταση:** Θα μπορούσε να προσδιοριστεί μόνο με εξέταση των αποθηκευμένων διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain	**1η εξέταση:** Μπορεί να προκύψει από τα αρχεία της εφαρμογής **2η εξέταση:** Μπορεί να προκύψει από τα αρχεία της εφαρμογής **3η εξέταση:** Μπορεί να προκύψει από τα αρχεία της εφαρμογής	**1η εξέταση:** Η εφαρμογή διατηρεί αρχείο καταγραφής μόνο για τις τελευταίες επτά ημέρες. Διαφορετικά θα μπορούσε να προσδιοριστεί μόνο με εξέταση των διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain **2η εξέταση:** Η εφαρμογή διατηρεί αρχείο καταγραφής μόνο για τις τελευταίες επτά ημέρες. Διαφορετικά θα μπορούσε να προσδιοριστεί μόνο με εξέταση των διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain **3η εξέταση:** Η εφαρμογή διατηρεί αρχείο καταγραφής

					μόνο για τις τελευταίες επτά ημέρες. Διαφορετικά θα μπορούσε να προσδιοριστεί μόνο με εξέταση των διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain
Ιστορικό συναλλαγών	**1η εξέταση:** Αναλυτική αποθήκευση σε αρχείο **2η εξέταση:** Αναλυτική αποθήκευση σε αρχείο **3η εξέταση:** Αναλυτική αποθήκευση σε αρχείο	**1η εξέταση:** Εμφανίζονται κάποια δεδομένα των συναλλαγών, αλλά θα πρέπει να συγκριθούν με δεδομένα από τον εξερευνητή blockchain **2η εξέταση:** Εμφανίζονται κάποια δεδομένα των συναλλαγών, αλλά θα πρέπει να συγκριθούν με δεδομένα από τον εξερευνητή blockchain **3η εξέταση:** Εμφανίζονται κάποια δεδομένα των συναλλαγών, αλλά θα πρέπει να συγκριθούν με δεδομένα από τον εξερευνητή blockchain	**1η εξέταση:** Θα μπορούσε να προσδιοριστεί μόνο με εξέταση των αποθηκευμένων διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain **2η εξέταση:** Θα μπορούσε να προσδιοριστεί μόνο με εξέταση των αποθηκευμένων διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain **3η εξέταση:** Θα μπορούσε να προσδιοριστεί μόνο με εξέταση των αποθηκευμένων διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain	**1η εξέταση:** Αναλυτική αποθήκευση σε αρχείο **2η εξέταση:** Αναλυτική αποθήκευση σε αρχείο **3η εξέταση:** Αναλυτική αποθήκευση σε αρχείο	**1η εξέταση:** Η εφαρμογή διατηρεί αρχείο καταγραφής των συναλλαγών μόνο για τις τελευταίες επτά ημέρες. Διαφορετικά θα μπορούσε να προσδιοριστεί μόνο με εξέταση των διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain **2η εξέταση:** Η εφαρμογή διατηρεί αρχείο καταγραφής των συναλλαγών μόνο για τις τελευταίες επτά ημέρες. Διαφορετικά θα μπορούσε να προσδιοριστεί μόνο με εξέταση των διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain **3η εξέταση:** Η εφαρμογή διατηρεί αρχείο καταγραφής των συναλλαγών μόνο για τις τελευταίες επτά ημέρες. Διαφορετικά θα μπορούσε να προσδιοριστεί μόνο με εξέταση των διευθύνσεων σε κάποιον εξερευνητή αλυσίδας blockchain
Διευθύνσεις bitcoin που δημιουργήθηκαν	**1η εξέταση:** Εμφάνιση (κατά περίπτωση) της τελευταίας διεύθυνσης που δημιουργήθηκε και	**1η εξέταση:** Εμφανίζονται κάποιες διευθύνσεις σε αρχείο της εφαρμογής	**1η εξέταση:** Εμφάνιση κάποιων διευθύνσεων, κυρίως αυτών που χρησιμοποιήθηκαν στις συναλλαγές. Οι υπόλοιπες	**1η εξέταση:** Εμφάνιση των περισσότερων διευθύνσεων που δημιουργήθηκαν, σε αρχείο	**1η εξέταση:** Εμφάνιση κάποιων διευθύνσεων, διάσπαρτες στα αρχεία καταγραφής. Οι υπόλοιπες μπορούν να εξαχθούν

	όσων χρησιμοποιήθηκαν στις συναλλαγές. Οι υπόλοιπες μπορούν να εξαχθούν με χρήση της μνημονικής ακολουθίας λέξεων **2η εξέταση:** Ομοίως με την πρώτη εξέταση **3η εξέταση:** Εμφάνιση των διευθύνσεων που χρησιμοποιήθηκαν στις συναλλαγές. Οι υπόλοιπες θα μπορούσαν να εξαχθούν με την χρήση του δημοσίου κλειδιού	**2η εξέταση:** Εμφανίζονται κάποιες διευθύνσεις σε αρχείο της εφαρμογής **3η εξέταση:** Εμφανίζονται κάποιες διευθύνσεις σε αρχείο της εφαρμογής	μπορούν να εξαχθούν με χρήση της μνημονικής ακολουθίας λέξεων **2η εξέταση:** Εμφάνιση κάποιων διευθύνσεων, κυρίως αυτών που χρησιμοποιήθηκαν στις συναλλαγές. Οι υπόλοιπες μπορούν να εξαχθούν με χρήση της μνημονικής ακολουθίας λέξεων **3η εξέταση:** Εμφάνιση κάποιων διευθύνσεων, κυρίως αυτών που χρησιμοποιήθηκαν στις συναλλαγές.	**2η εξέταση:** Εμφάνιση των περισσότερων διευθύνσεων που δημιουργήθηκαν, σε αρχείο **3η εξέταση:** Εμφάνιση των περισσότερων διευθύνσεων που δημιουργήθηκαν, σε αρχείο	με χρήση της μνημονικής ακολουθίας λέξεων **2η εξέταση:** Εμφάνιση κάποιων διευθύνσεων, διάσπαρτες στα αρχεία καταγραφής. Οι υπόλοιπες μπορούν να εξαχθούν με χρήση της μνημονικής ακολουθίας λέξεων **3η εξέταση:** Εμφάνιση κάποιων διευθύνσεων, διάσπαρτες στα αρχεία καταγραφής. Από την στιγμή που η μνημονική ακολουθία λέξεων είναι κρυπτογραφημένη, δεν μπορούν να εξαχθούν οι διευθύνσεις του πορτοφολιού
Επιπρόσθετες λειτουργίες της εφαρμογής όπως (επαφές, ετικέτες διευθύνσεων κ.α.)	**1η εξέταση:** Ανεύρεση των περισσότερων δεδομένων σε μορφή απλού κειμένου **2η εξέταση:** Τα δεδομένα δεν διατηρούνται **3η εξέταση:** Τα δεδομένα δεν βρέθηκαν γιατί εξετάστηκε το πορτοφόλι της 2ης εξέτασης (υποθέτουμε αν ο κωδικός κρυπτογράφησης τεθεί σε νέο πορτοφόλι και αποθηκευτούν τέτοιου είδους δεδομένα από τον χρήστη, τα ευρήματα θα είναι αντίστοιχα της 1ης εξέτασης)	**1η εξέταση:** Ανεύρεση των περισσότερων δεδομένων σε μορφή απλού κειμένου **2η εξέταση:** Τα δεδομένα δεν διατηρούνται **3η εξέταση:** Τα δεδομένα δεν βρέθηκαν γιατί εξετάστηκε το πορτοφόλι της 2ης εξέτασης	**1η εξέταση:** Ανεύρεση των περισσότερων δεδομένων σε μορφή απλού κειμένου **2η εξέταση:** Τα δεδομένα δεν διατηρούνται **3η εξέταση:** Τα δεδομένα δεν βρέθηκαν γιατί εξετάστηκε το πορτοφόλι της 2ης εξέτασης	**1η εξέταση:** Ανεύρεση των περισσότερων δεδομένων σε μορφή απλού κειμένου **2η εξέταση:** Τα δεδομένα δεν διατηρούνται **3η εξέταση:** Τα δεδομένα δεν βρέθηκαν γιατί εξετάστηκε το πορτοφόλι της 2ης εξέτασης	**1η εξέταση:** Ανεύρεση των περισσότερων δεδομένων σε μορφή απλού κειμένου **2η εξέταση:** Τα δεδομένα δεν διατηρούνται **3η εξέταση:** Τα δεδομένα δεν βρέθηκαν γιατί εξετάστηκε το πορτοφόλι της 2ης εξέτασης

Ημερομηνία σύνδεσης του χρήστη στην εφαρμογή	Δεν κατέστη δυνατός ο προσδιορισμός σε καμία από τις εξετάσεις που πραγματοποιήσαμε	**1η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής **2η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής **3η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής	**1η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής **2η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής **3η εξέταση:** Εμφανίζεται σε αρχείο της εφαρμογής	Δεν κατέστη δυνατός ο προσδιορισμός σε καμία από τις εξετάσεις που πραγματοποιήσαμε	Δεν κατέστη δυνατός ο προσδιορισμός σε καμία από τις εξετάσεις που πραγματοποιήσαμε
Δίκτυο που χρησιμοποίησε ο χρήστης για να συνδεθεί στην εφαρμογή	Δεν κατέστη δυνατός ο προσδιορισμός σε καμία από τις εξετάσεις που πραγματοποιήσαμε	Δεν κατέστη δυνατός ο προσδιορισμός σε καμία από τις εξετάσεις που πραγματοποιήσαμε	Δεν κατέστη δυνατός ο προσδιορισμός σε καμία από τις εξετάσεις που πραγματοποιήσαμε	Δεν κατέστη δυνατός ο προσδιορισμός σε καμία από τις εξετάσεις που πραγματοποιήσαμε	Εμφανίζεται σε αρχείο καταγραφής, αναλόγως του δικτύου που χρησιμοποιήθηκε (wifi – inetrnet LTE)

Μελλοντική Δουλειά

Όπως προαναφέραμε, οι εφαρμογές που εξετάσαμε αναβαθμίζονται συνεχώς. Συνεπώς, η ανάγκη της εγκληματολογικής εξέτασης των εφαρμογών ακολουθεί αναπόφευκτα την εξέλιξη τους.

Όπως είδαμε, εφαρμογές που μπορεί να μην κρυπτογραφούσαν εξ ορισμού το πορτοφόλι του χρήστη, στην επόμενη αναβάθμιση εισήγαγαν το χαρακτηριστικό αυτό χωρίς την δυνατότητα παράλειψής του από τον χρήστη. Η τακτική αυτή βάζει καινούρια εμπόδια στον αναλυτή, ο οποίος θα πρέπει να διερευνήσει τον τρόπο που γίνεται η κρυπτογράφηση του πορτοφολιού καθώς και τον τρόπο απόκτησης του κλειδιού του χρήστη για να μπορέσει στη συνέχεια να αποκτήσει πρόσβαση στο πορτοφόλι του.

Επειδή όλες οι εφαρμογές χρησιμοποιούν με τον έναν ή τον άλλο τρόπο την δυνατότητα εισαγωγής κωδικού, είτε για την κρυπτογράφηση του πορτοφολιού, είτε μόνο για την δυνατότητα ξοδέματος των bitcoin που περιέχονται στο πορτοφόλι, θα είχε ενδιαφέρον η περαιτέρω ανάλυση του τρόπου κρυπτογράφησης των αρχείων που παρουσιάσαμε και την εύρεση μεθόδων αποκρυπτογράφησής τους αν γνωρίζαμε τον κωδικό που χρησιμοποίησε ο χρήστης.

Ενδιαφέρον επίσης θα παρουσίαζε η ανάλυση της πτητικής μνήμης RAM του τηλεφώνου, μετά την εισαγωγή κωδικού από τον χρήστη της εφαρμογής, προκειμένου να διαπιστώσουμε αν υπάρχει η δυνατότητα εύρεσης του κωδικού στη μνήμη RAM ή όχι.

Τέλος, η ανάγκη των δοκιμών που παρουσιάσαμε σε περισσότερα περιβάλλοντα του λογισμικού Android, θα μπορούσε να μας δώσει αποτελέσματα για το κατά πόσο οι εφαρμογές συμπεριφέρονται με τον ίδιο τρόπο σε αναβαθμίσεις του λειτουργικού συστήματος ή ακόμη και κατά πόσο το λειτουργικό σύστημα έχει μεταβάλλει την λειτουργία του για κάποιες από τις δυνατότητες της εφαρμογής.

Βιβλιογραφία

1) Mobile threats incident handling Toolset, Document for students, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/Mobilethreatsincidenthandlingtoolset.pdf
2) Mobile threats incident handling Handbook, Document for teachers, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/Mobileincidenthandlinghandbook.pdf

3) Mobile Threats Incident Handling (Part II) Toolset, Document for students, 1.0, September 2015 - https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/mobile-threats-incident-handling-part-ii.pdf
4) Mobile Threats Incident Handling (Part II) Handbook, Document for teachers, 1.0, September 2015 - https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/mobile-threats-incident-handling-part-ii-handbook-document-for-teachers
5) David Neilson, Sukhvinder Hara and Ian Mitchell, *Bitcoin Forensics: A Tutorial, January 2016,* http://eprints.mdx.ac.uk/20793/1/Bitcoin%20Forensics%20-%20A%20Tutorial.pdf
6) Yaya J. Fanusie and Tom Robinson, *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*, January 12, 2018, https://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf
7) LUUC VAN DER HORST, KIM-KWANG RAYMOND CHOO, (Senior Member, IEEE), AND NHIEN-AN LE-KHAC, (Member, IEEE), *Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core*, November 7, 2017, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8058429
8) Wikipedia, https://en.wikipedia.org/wiki/Bitcoin
9) Bitcoin - Open source P2P money, https://bitcoin.org
10) S. Nakamoto, "*Bitcoin: A peer-to-peer electronic cash system*." Electronic, 2008. https://bitcoin.org/bitcoin.pdf
11) Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 1st Edition
12) Andrew Hoog, *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*, 1st Edition
13) Rohit Tamma, Donnie Tindall, *Learning Android Forensics Paperback* - April 30, 2015
14) Heather Mahalik, Rohit Tamma, Satish Bommisetty, *Practical Mobile Forensics*, Second Edition Paperback - May 20, 2016
15) Soufiane Tahiri, *Mastering Mobile Forensics Paperback* - May 30, 2016
16) Copay Bitcoin Wallet, https://github.com/bitpay/copay
17) Mycelium Bitcoin Wallet, https://github.com/mycelium-com/wallet

18) Coinomi Bitcoin Altcoin Wallet, https://github.com/Coinomi/coinomi-android

19) Electrum Bitcoin Wallet, https://github.com/spesmilo/electrum

20) Bitcoin Wallet, https://github.com/bitcoin-wallet/bitcoin-wallet