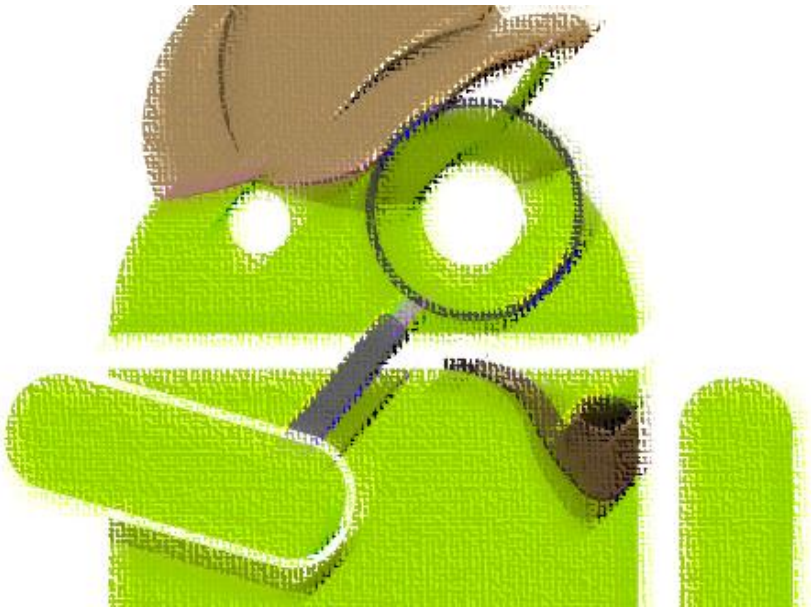
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Ψηφιακών Συστημάτων

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



Διπλωματική εργασία

"Android forensics with open source tools"

Νάτσιος Μιλτιάδης
Αρ. Μ. ΜΤΕ 1215

Επιβλέπον καθηγητής
Σωκράτης Κάτσικας

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω όλους όσους με στήριξαν κατά τη διάρκεια εκπόνησης της διπλωματικής μου εργασίας και δεν είναι άλλοι από την οικογένεια και τους φίλους μου. Επίσης δεν θα μπορούσα να παραλείψω τους επιβλέποντες καθηγητές μου, Σωκράτη Κάτσικα και Κωνσταντίνο Λαμπρινουδάκη, που με την κατάλληλη καθοδήγηση και τις συμβουλές που μου παρείχαν με βοήθησαν στην ολοκλήρωση του στόχου που είχα θέσει.

Table of Contents

1. Εισαγωγή

Τα έξυπνα κινητά τηλέφωνα αποτελούν πλέον αναπόσπαστο κομμάτι της καθημερινότητάς. Πρόκειται για μικρές ως επί το πλείστο, πανίσχυρες ηλεκτρονικές συσκευές, που ενσωματώνουν κάθε σύγχρονη τεχνολογία που αναπτύσσεται στον κλάδο της πληροφορικής και των τηλεπικοινωνιών, με σκοπό την βελτίωση της επικοινωνίας και του καθημερινού τρόπου ζωής. Οι δυνατότητες που διαθέτουν, μπορούν να συγκριθούν άμεσα με αυτές την σύγχρονων προσωπικών υπολογιστών και να υπερτερήσουν αυτών σε συχνές και απλές επαναλαμβανόμενες λειτουργίες, όπως αυτές της ανταλλαγής άμεσων μηνυμάτων, λήψης φωτογραφιών και βίντεο, διαχείρισης του ηλεκτρονικού ταχυδρομείου, καθώς και της συμμετοχής σε μέσα κοινωνικής δικτύωσης. Παράλληλα, η χρήση των έξυπνων κινητών συσκευών συνδυάζεται και με άλλες λειτουργίες, όπως είναι οι ηλεκτρονικές συναλλαγές, το ηλεκτρονικό εμπόριο, η πλοήγηση στο διαδίκτυο, καθώς και η αποθήκευση πλήθους δεδομένων, γεγονός που τα καθιστούν μία πραγματικά τεράστια τράπεζα πληροφοριών, που μπορεί αφενός να αποτελέσει δυνητικά στόχο επιτηδείων και αφετέρου ένα πολύτιμο εργαλείο στα χέρια ερευνητών.

Η δυναμική που έχει παρατηρηθεί στην χρήση των smartphones και η σημαντική διείσδυσή τους στην καθημερινότητα, αναδεικνύουν την ανάγκη ύπαρξης ερευνητικού ενδιαφέροντος στον τομέα των mobile forensics. Όσο οι συσκευές αυτές αποκτούν ισχυρότερη θέση στην ζωή κάθε ανθρώπου και όσο οι τελευταίοι εξαρτώνται από αυτές σε μεγάλο βαθμό, δίνουν το κίνητρο σε εγκληματίες να τις χρησιμοποιήσουν. Απάτες μέσω e-mail, διακίνηση μη νόμιμου υλικού, απόκτηση και γνωστοποίηση προσωπικών δεδομένων σε τρίτους, είναι μερικές μόνο από τις παράνομες πράξεις που μπορεί να διαπραχθούν.

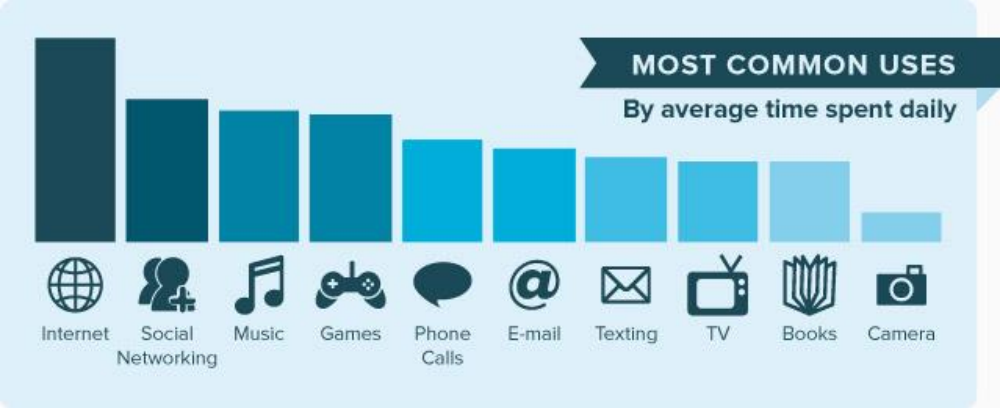
Ο κλάδος λοιπόν της ψηφιακής εγκληματολογίας σε έξυπνα τηλέφωνα, είναι αυτός που αναλαμβάνει να ανακτήσει πειστήρια των εγκληματικών δραστηριοτήτων, που πραγματοποιούνται με την χρήση των παραπάνω συσκευών. Τα δεδομένα που αποθηκεύονται τόσο κατά τη διάρκεια λειτουργίας τους, όσο και κατά τη διάπραξη παράτυπων ενεργειών, αποτελούν πολύτιμα στοιχεία για έναν αναλυτή,

προκειμένου να πραγματοποιήσει την έρευνά του. Αρχεία καταγραφής κλήσεων, μηνύματα κειμένου, emails, αποθηκευμένες πληροφορίες λογαριασμών, ιστορικό περιήγησης, ακόμα και αρχεία συζητήσεων, είναι μερικά βασικά από αυτά. Υπάρχουν επίσης και αρκετά άλλα δεδομένα, τα οποία χρήζουν διαφορετικής προσέγγισης, για να μπορέσουν να αξιοποιηθούν, όπως για παράδειγμα στοιχεία από εφαρμογές που βρίσκονται εγκατεστημένες, δεδομένα θέσης (GPS), ακόμα και διεγραμμένα αρχεία.

Σκοπός της παρούσας εκπόνησης είναι η παρουσίαση της βασικής μεθοδολογίας απόκτησης πειστηρίων από μια έξυπνη κινητή συσκευή με λειτουργικό Android, καθώς και η διερεύνηση της αποτελεσματικότητας των εργαλείων ελεύθερου λογισμικού, που είναι διαθέσιμα στην κοινότητα. Πιο συγκεκριμένα αρχικά θα γίνει αναφορά στα πέντε βασικά βήματα μιας κοινά αποδεκτής διαδικασίας, που ακολουθούνται για την απόκτηση και την εξέταση των δεδομένων στα πλαίσια μιας ερευνητικής δραστηριότητας, ενώ στη συνέχεια θα γίνει σύντομη παρουσίαση του λειτουργικού συστήματος Android και των εσωτερικών του δομών, όπως τα partitions, τα filesystems που υποστηρίζονται και η αρχιτεκτονική του γενικότερα. Τέλος, θα γίνει εκτενή αναφορά σε υλοποιήσεις λογισμικών ανοιχτού κώδικα και θα κριθεί, έπειτα από δοκιμαστική χρήση τους, η δυνατότητα υποστήριξης μιας εγκληματολογικής έρευνας με απώτερο στόχο την αντικατάσταση εταιρικών προϊόντων υψηλού κόστους.

2. Έξυπνες συσκευές και καθημερινότητα

Όλα εκείνα τα στοιχεία που κάνουν τα smartphones μοναδικές συσκευές με απεριόριστες δυνατότητες, όπως για παράδειγμα το μικρό τους μέγεθος, η υπολογιστική τους ισχύς, οι αισθητήρες που διαθέτουν, καθώς και η δυνατότητα να βρίσκονται σε απόσταση μερικών εκατοστών από τον ιδιοκτήτη τους καθ' όλη τη διάρκεια της ημέρας, είναι και αυτά που τα εκθέτουν σε επιπρόσθετους κινδύνους από έναν απλό προσωπικό υπολογιστή. Οι παραπάνω δυνατότητες, όπως γίνεται αντιληπτό μπορούν να αποκαλύψουν, από την ταυτότητα του χρήστη και τις συνήθειες περιήγησής του, μέχρι τα πρόσωπα που επικοινωνεί συχνά και τα μέρη που επισκέπτεται.



Οι έξυπνες κινητές συσκευές αντιπροσωπεύουν το μέλλον της επικοινωνίας και του νέου τρόπου ζωής. Μία έρευνα που δημοσιεύθηκε για λογαριασμό του μεγαλύτερου μέσου κοινωνικής δικτύωσης (Facebook), παρουσιάζει το ρόλο που έχουν οι συγκεκριμένες συσκευές στην καθημερινότητα και αναφέρει χαρακτηριστικά, πως το 80% των χρηστών της πλατφόρμας την επισκέπτεται σε διάστημα 15 λεπτών από την στιγμή που θα ξυπνήσει. Ταυτόχρονα επισημαίνεται πως η κύρια και παραδοσιακή λειτουργία τους έχει παραγκωνιστεί, καθώς η ποιότητα των εξαρτημάτων που διαθέτουν, συμβάλλει στη σταδιακή αντικατάσταση του παραδοσιακού τρόπου επικοινωνίας με πιο σύνθετους, όπως η χρήση διάφορων εφαρμογών κοινωνικών δικτύων (Facebook, whatsapp, etc.). Συνεπώς, ο νέος αυτός τρόπος χρήσης των smartphones έχει αυξήσει το ποσοστό συγκέντρωσης προσωπικών δεδομένων στις συσκευές.

3. Mobile forensics

Τα τελευταία χρόνια ο κλάδος της ψηφιακής εγκληματολογίας έχει αρχίσει να δέχεται μεγάλο αριθμό αιτήσεων για εξέταση δεδομένων από έξυπνες κινητές συσκευές. Η αποθήκευση όλο και περισσότερων προσωπικών δεδομένων και η γενικότερη αύξηση της online δραστηριότητας με την χρήση των smartphones, οδηγούν στη δημιουργία του τομέα της ψηφιακής εγκληματολογίας για κινητές συσκευές που στοχεύει στην απόκτηση, ανάκτηση και ανάλυση στοιχείων από αυτές, χρησιμοποιώντας ευρέως αποδεκτές μεθόδους. Πιο συγκεκριμένα, στοχεύει στην προσπέλαση και εξέταση δεδομένων, που βρίσκονται αποθηκευμένα σε κάθε συσκευή με συγκεκριμένη μεθοδική προσέγγιση. Η διαδικασία αυτή περιλαμβάνει από μηνύματα sms, δεδομένα κλήσεων και φωτογραφίες μέχρι ψηφιακά ίχνη σε μέσα κοινωνικής δικτύωσης, ιστορικό περιήγησης στο διαδίκτυο, καθώς και κάθε είδους πληροφορίες που προκύπτουν από την χρήση των αισθητήρων, που βρίσκονται εγκατεστημένοι στα smartphones. Αξίζει να σημειωθεί, πως η διαδικασία απόκτησης των παραπάνω δεδομένων θα πρέπει να γίνεται με σαφή και προκαθορισμένο τρόπο, καθώς ενδέχεται τα στοιχεία της έρευνας να χρησιμοποιηθούν για την εξιχνίαση μιας νομικής υπόθεσης και ως εκ τούτου θα πρέπει να διέπονται από την έννοια της ακεραιότητας.

Η φορμαλιστική προσέγγιση στον τομέα της ψηφιακής εγκληματολογίας είναι η έννοια που παίζει το σημαντικότερο ρόλο για την διερεύνηση μιας υπόθεσης. Η διασφάλιση της ακεραιότητας που αναφέρθηκε προηγούμενα, δεν αποτελεί τον μοναδικό στόχο ενός ερευνητή. Αυτό που θα πρέπει να τον απασχολεί περισσότερο είναι η ακριβής καταγραφή των γεγονότων (documentation). Η διαδικασία αυτή παρουσιάζει με συγκεκριμένο και ακριβή τρόπο, πώς έχει χειριστεί την κάθε συσκευή από την στιγμή της απόκτησής της. Έτσι η διαδικασία μπορεί να ελεγχθεί ως προς την ορθότητά της και τα δεδομένα που έχουν ανακτηθεί μπορούν να επιβεβαιωθούν ως προς την ακεραιότητά τους, καθώς μπορούν να συγκριθούν με αυτά, κατά την στιγμή απόκτησης της συσκευής.

4. Challenges in mobile forensics

Η ολοένα και αυξανόμενη ζήτηση για διερεύνηση υποθέσεων, που αφορούν έξυπνα κινητά τηλέφωνα, οδηγεί τους ερευνητές μπροστά σε διάφορες προκλήσεις που θα πρέπει να αντιμετωπίσουν.

Αρχικά, ο μεγάλος πλέον αριθμός συσκευών και λειτουργικών συστημάτων είναι μια από αυτές. Μπορεί η πλειοψηφία των smartphones να χρησιμοποιεί λειτουργικό Android, ωστόσο μεγάλο μερίδιο στην αγορά κατέχει το iOS, ενώ ακολουθεί το blackberry και τέλος το λειτουργικό των Windows. Παράλληλα για κάθε ένα από τα λειτουργικά αυτά, υπάρχουν χιλιάδες συσκευές που μπορούν να τα υποστηρίξουν και διαθέτουν ταυτόχρονα διαφορετικό hardware, έκδοση, όπως και διαφορετικές δυνατότητες. Για παράδειγμα, στο λειτουργικό σύστημα Android υπάρχουν 10 περίπου διαφορετικές εκδόσεις, που κάθε μία από αυτές χρησιμοποιείται από διαφορετικούς κατασκευαστές, κάνοντας με την σειρά τους και αυτοί διαφορετικές τροποποιήσεις. Με αποτέλεσμα πολλές φορές στο ίδιο λειτουργικό τα δεδομένα να αποθηκεύονται με διαφορετικό τρόπο, ενώ και η γενικότερη ιεραρχία (file structure) μπορεί να διαφέρει.

Μια ακόμα πρόκληση που κάθε αναλυτής θα πρέπει να αντιμετωπίσει είναι τα διάφορα χαρακτηριστικά ασφάλειας, που ο κάθε κατασκευαστής έχει προσθέσει. Καθώς η έννοια της ασφάλειας των προσωπικών δεδομένων βρίσκεται ολοένα και περισσότερο στο επίκεντρο, υλοποιούνται ισχυροί μηχανισμοί που να αποτρέπουν την εύκολη πρόσβαση σε αυτά. Από την απλή χρήση ενός passcode μέχρι και την χρήση full disk encryption, ένας forensic expert θα πρέπει να ανακαλύψει τρόπους για να τα ξεπεράσει.

Θα πρέπει επίσης να λαμβάνεται υπόψη η φύση ενός έξυπνου τηλεφώνου, πράγμα που σημαίνει, ότι η ευκολία μετακίνησής του και η δυνατότητά του να βρίσκεται πάντα δίπλα στον χρήστη χωρίς να γνωρίζει γεωγραφικά όρια, μπορεί να παρέχει δεδομένα και στοιχεία, όπου ανάλογα με τους νόμους που ισχύουν, μπορούν να στοιχειοθετήσουν ένα αδίκημα σε κάποια χώρα, ενώ σε κάποια άλλη όχι.

Τέλος η σημαντικότερη και παράλληλα θεμελιώδη πρόκληση για έναν ερευνητή είναι η διατήρηση της ακεραιότητας των δεδομένων. Από τη μία, ο ίδιος θα πρέπει να διασφαλίσει, ότι οποιαδήποτε τεχνική και να χρησιμοποιηθεί για την απόκτηση και την ανάκτηση πληροφοριών, δεν θα έχει αντίκτυπο στα ίδια τα δεδομένα και από την άλλη θα πρέπει να κάνει όλες τις απαραίτητες ενέργειες, ώστε κανείς να μη μπορέσει να πάρει πρόσβαση απομακρυσμένα και να τροποποιήσει ή να διαγράψει δεδομένα.

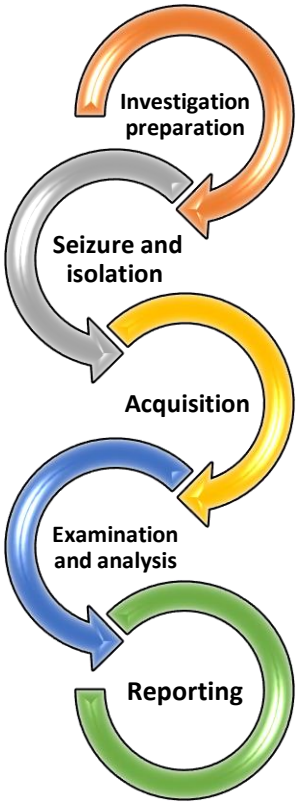
Για όλους τους παραπάνω λόγους γίνεται αντιληπτό, πως η σχεδίαση και υιοθέτηση μιας συγκεκριμένης μεθοδολογίας, που διαθέτει σαφείς οδηγίες και κατευθύνσεις, αποτελεί τον πιο κρίσιμο παράγοντα στη διαδικασία εξέτασης μιας κινητής έξυπνης συσκευής με στόχο τη διασφάλιση της ακεραιότητας των δεδομένων.

5. Cellular Phone Evidence Extraction Process

Η διαδικασία ανάκτησης και εξέτασης δεδομένων μπορεί να πραγματοποιηθεί χρησιμοποιώντας διάφορες μεθόδους. Ωστόσο, όπως αναφέρθηκε και προηγουμένως, υπάρχει η ανάγκη για μία συγκεκριμένη μεθοδολογία, που θα βοηθήσει τον ερευνητή να διαβεβαιώσει, ότι κάθε απόδειξη είναι καλά τεκμηριωμένη και τα αποτελέσματα μπορούν να είναι επαναλαμβανόμενα και ικανά να υποστηριχθούν σε δικαστικές διαδικασίες.

Μια τυπική μεθοδολογία μπορεί να χωριστεί σε πέντε επιμέρους φάσεις:

- Investigation preparation
- Seizure and isolation
- Acquisition
- Examination and analysis
- Reporting



5.1. Investigation preparation

Η πρώτη φάση ξεκινά αμέσως μόλις ληφθεί το αίτημα για διενέργεια έρευνας για μία συγκεκριμένη υπόθεση. Περιλαμβάνει όλες εκείνες τις γραφειοκρατικές διαδικασίες, που είναι ωστόσο απαραίτητες για την ακριβή καταγραφή τόσο της διαδικασίας που θα ακολουθηθεί και τον σκοπό αυτής, όσο και γενικών πληροφοριών για την συσκευή και τον τύπο των δεδομένων που αναζητούνται.

Κρίσιμο στην φάση αυτή είναι η οικοδόμηση συγκεκριμένων επιμέρους στόχων, που θα βοηθήσει στο να αποσαφηνιστεί περαιτέρω ο σκοπός της έρευνας.

5.2. Seizure and isolation

Ο τρόπος που θα χειριστεί ένας ερευνητής την συσκευή που θα κατάσχει, αποτελεί κρίσιμο παράγοντα για την επιτυχή έκβαση της ερευνητικής διαδικασίας. Τα αποδεικτικά στοιχεία συνήθως μεταφέρονται με την χρήση anti-static bags, που είναι σχεδιασμένες για να προστατεύουν τα ηλεκτρονικά εξαρτήματα από τον στατικό ηλεκτρισμό, ώστε να μην προκληθεί καμία βλάβη σε αυτά. Γίνεται αντιληπτό, ότι στην φάση της κατάσχεσης πρέπει να γίνει ό,τι είναι δυνατό, ώστε οι χειρισμοί που θα εφαρμοσθούν να μην αποφέρουν καμία αλλαγή στα δεδομένα, που βρίσκονται στη συσκευή. Ένας ακόμη παράγοντας, που πρέπει να διασφαλιστεί στην συγκεκριμένη φάση είναι η απόλυτη απομόνωση από κάθε δίκτυο, ώστε να μην υπάρχει η δυνατότητα έστω και απομακρυσμένα κάποιος να αλλάξει ή ακόμα και να διαγράψει δεδομένα.

Η δυνατότητα απομακρυσμένης πρόσβασης υπάρχει και μπορεί να χρησιμοποιηθεί εύκολα, χωρίς να απαιτεί εξιδεικευμένες γνώσεις. Η εφαρμογή Android device manager (ADM) δίνει την δυνατότητα μέσω του Google account, που είναι εγκατεστημένος στο smartphone, να το εντοπίσει, να το κλειδώσει, ακόμα και να διαγράψει τις πληροφορίες που περιέχει. Η ίδια διαδικασία μπορεί να πραγματοποιηθεί και χωρίς να υπάρχει πρόσβαση στο διαδίκτυο, μέσω ενός διαφορετικού λογισμικού, το mobile device management (MDM) που έχει τις ίδιες δυνατότητες με την αποστολή ενός sms.

Γίνεται λοιπόν αντιληπτό, ότι οποιαδήποτε επικοινωνία του κινητού τηλεφώνου με τα δίκτυα που μπορεί να αλληλοεπιδράσει, θα πρέπει να αποτραπεί. Αυτό μπορεί να γίνει είτε με την επιλογή airplane mode που υπάρχει σε κάθε συσκευή είτε με την χρήση faraday bag ή RF isolation box, που μπλοκάρει αποτελεσματικά κάθε μετάδοση σήματος.

ΤΕΧΝΙΚΗ	ΠΛΕΟΝΕΚΤΗΜΑ	ΜΕΙΟΝΕΚΤΗΜΑ
Ενεργοποίηση του Airplane mode	Η συσκευή συνεχίζει να λειτουργεί αφήνοντας τα δεδομένα άθικτα καθώς απενεργοποιεί την κάλυψη από το δίκτυο	Επέμβαση στις ρυθμίσεις της συσκευής
Αν η συσκευή διαθέτει λειτουργία GSM αφαιρείται η κάρτα SIM	Αποτελεσματικό μέσο για απομόνωση από το δίκτυο κινητής	Δεν απενεργοποιείται η προσβασιμότητα στην συσκευή μέσω WIFI
Αποκλεισμός της συσκευής από τον τηλεπικοινωνιακό πάροχο	Κάθε αλληλεπίδραση με το δίκτυο αποκλείεται	Απαιτείται δικαστική παρέμβαση που μπορεί να είναι χρονοβόρα
Τοποθέτηση της συσκευής σε τσάντα απομόνωσης ή τέντα faraday	Αρκετά αποτελεσματικό μέσο που αποτρέπει οποιαδήποτε μετάδοση δεδομένων	Το τηλέφωνο προσπαθεί συνεχώς να συνδεθεί με το δίκτυο με αποτέλεσμα να καταναλώνει την μπαταρία του γρήγορα.
Απενεργοποίηση συσκευής	Άμεσο και αποτελεσματικό μέσο για την αποτροπή αλληλεπίδρασης με οποιοδήποτε δίκτυο	Σημαντική μεταβολή της κατάστασης της συσκευής και πιθανή απώλεια δεδομένων που βρίσκονταν στην μνήμη την ώρα της απόκτησης.

Παράλληλα, στο σημείο αυτό εμφανίζονται κάποιες ευκαιρίες, που μπορούν να βοηθήσουν στην ερευνητική διαδικασία και καλό είναι ο ερευνητής να τις λάβει υπόψη του και να τις εκμεταλλευθεί.

Εάν η συσκευή είναι ξεκλείδωτη πρέπει να γίνουν αμέσως όλες οι απαραίτητες αρχικά ενέργειες, ώστε να του δώσουν την δυνατότητα να έχει την απαραίτητη πρόσβαση σε αυτή.

- Ενεργοποίηση της επιλογής **usb debugging**

  Με την ενεργοποίηση της επιλογής αυτής, δίνεται αρκετά καλή πρόσβαση στην συσκευή μέσω μιας λειτουργείας, που διαθέτει το περιβάλλον του λειτουργικού Android και ονομάζεται adb (Android debug bridge). Η συγκεκριμένη λειτουργία παίζει καθοριστικό ρόλο στην διαδικασία ανάκτησης των δεδομένων της κινητής συσκευής.

- Ενεργοποίηση της επιλογής **stay awake**

  Η επιλογή αυτή είναι αρκετά σημαντική, καθώς δεν αφήνει την συσκευή να μπει σε κατάσταση sleep mode

- Αύξηση του **screen timeout**

  Με την αύξηση του χρόνου αναμονής διασφαλίζεται, ότι το τηλέφωνο θα μένει ενεργό για περισσότερο χρονικό διάστημα, πράγμα που σημαίνει, ότι δεν μπορεί να κλειδώσει αυτόματα μετά την πάροδο κάποιων λεπτών που έχει ορισθεί στην εργοστασιακή ρύθμιση.

5.3. Acquisition

Η συγκεκριμένη φάση αναφέρεται στην διαδικασία απόκτησης των δεδομένων από την συσκευή. Λόγω των ενσωματωμένων λειτουργειών ασφάλειας που υπάρχουν, η παραπάνω διαδικασία τις περισσότερες φορές δεν είναι απλή, καθώς η επιλογή της κατάλληλης εξαρτάται τόσο από το λειτουργικό σύστημα, όσο και από το μοντέλο της συσκευής. Οι διαθέσιμοι τρόποι απόκτησης δεδομένων είναι οι ακόλουθοι:

5.3.1. Manual acquisition:

Αυτή θεωρείται η πιο απλοϊκή προσέγγιση. Ο ερευνητής χρησιμοποιεί τις βασικές λειτουργίες του τηλεφώνου, περιηγείται και εξερευνά χωρίς τη χρήση ειδικών εργαλείων και τεχνικών. Στην περίπτωση αυτή, υπάρχουν κάποιοι περιορισμοί ως προς τον όγκο των δεδομένων που είναι διαθέσιμα και απαιτείται για την αύξηση της αποτελεσματικότητας η εφαρμογή της διαδικασίας rooting που αναλύεται σε επόμενο κεφάλαιο.

5.3.2. Logical acquisition:

Η μέθοδος αυτή είναι γνωστή και ως logical extraction και αναφέρεται στην απόκτηση δεδομένων, που είναι αποθηκευμένα σε ένα τμήμα του λειτουργικού. Με τη συγκεκριμένη διαδικασία μπορούν να ανακτηθούν δεδομένα, όπως:

- Call Logs
- SMS
- MMS
- Ιστορικό περιήγησης
- Contacts groups
- Contacts phones
- External image media (metadata)
- External image thumbnail media (metadata)
- External media, audio, and misc. (metadata)
- External videos (meta data)
- Δεδομένα θέσης (GPS data)
- Internet activity
- Λίστα όλων των εγκατεστημένων εφαρμογών, συμπεριλαμβανομένης της έκδοσής τους
- Εφαρμογές κοινωνικής δικτύωσης, όπως το WhatsApp, Skype, Facebook, και άλλα.

5.3.3. Physical acquisition:

Η μέθοδος αυτή αποτελεί την πιο αποτελεσματική και πλήρη διαδικασία, καθώς δημιουργεί ένα αντίγραφο bit-by-bit όλης της μνήμης. Επί της ουσίας, δημιουργείται ένα αντίγραφο ολόκληρου του λειτουργικού, όπου συμπεριλαμβάνεται το σύνολο των δεδομένων της συσκευής. Κύριο χαρακτηριστικό της είναι η δυνατότητα ανάκτησης διαγεγραμμένων πληροφοριών και στοιχείων, που βρίσκονται ακόμα αποθηκευμένα στις βάσεις δεδομένων της.

5.3.4. Logical vs physical acquisition

Οι πιο συνηθισμένες μέθοδοι που χρησιμοποιούνται για την απόκτηση των προς ανάλυση δεδομένων είναι οι προηγούμενες δύο. Στην πρώτη τεχνική (logical acquisition) τα δεδομένα που συλλέγονται είναι αυτά που δεν έχουν διαγραφεί και είναι προσπελάσιμα στο filesystem. Εξαίρεση αποτελούν ίσως κάποια αρχεία, όπως για παράδειγμα μια βάση δεδομένων SQL, η οποία μπορεί να περιλαμβάνει και εγγραφές διαγραμμένων στοιχείων. Από την άλλη, στην τεχνική physical acquisition η απόκτηση των δεδομένων γίνεται με την απευθείας πρόσβαση στο φυσικό μέσο αποθήκευσής τους και όχι μέσω του filesystem, με αποτέλεσμα σημαντικός όγκος πληροφοριών και αρχείων που μαρκάρονται ως διαγραμμένα να γίνονται προσβάσιμα.

5.4. Examination and analysis

Στην φάση αυτή ο ερευνητής χρησιμοποιεί διάφορα εργαλεία και τις μεθοδολογίες που αναφέρθηκαν, για να ανακτήσει τα δεδομένα από την κινητή συσκευή, να εξετάσει τα μέσα αποθήκευσής της ή ακόμα και την ram μνήμη της, με σκοπό την στοιχειοθέτηση ενός αδικήματος. Σχηματικά η διαδικασία που ακολουθείται είναι η εξής :

- Ανάκτηση των δεδομένων που χρειάζονται και έχουν τεθεί ως στόχος
- Στοιχειοθέτηση της παραβατικής δραστηριότητας
- Εξακρίβωση και επανέλεγχος στοιχείων
- Προστασία πειστηρίων

5.5. Reporting

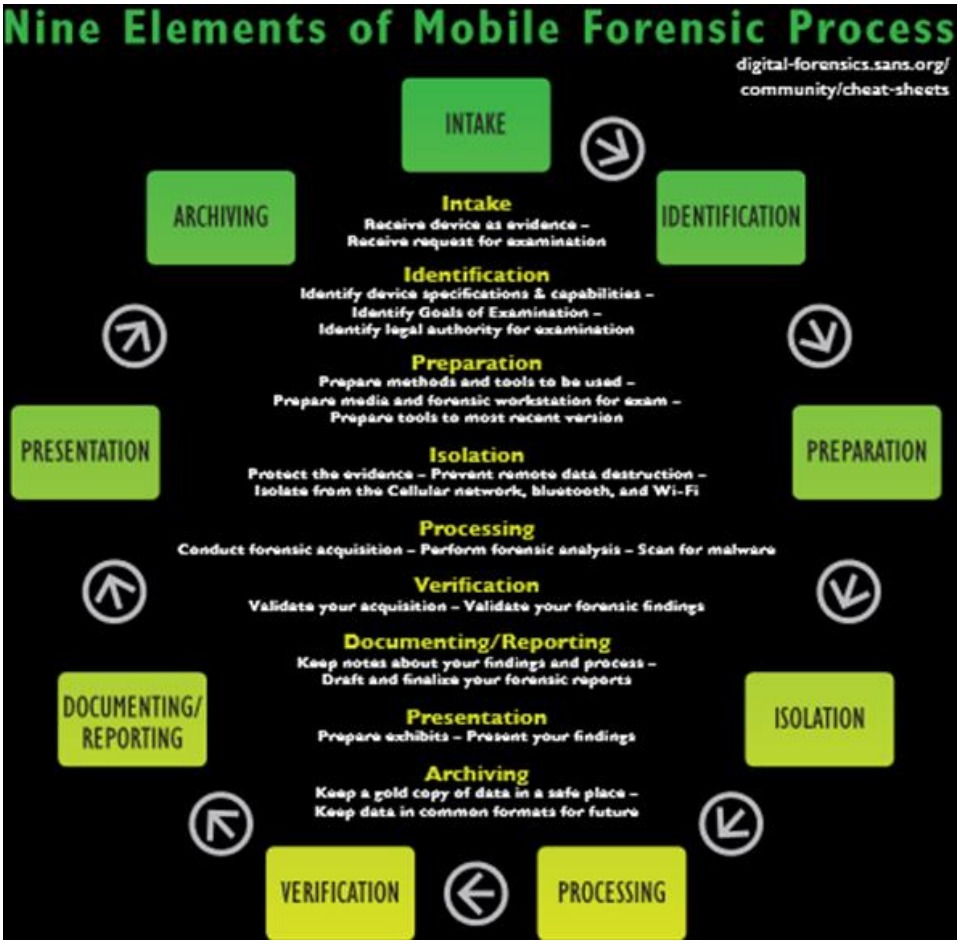
Το τελικό στάδιο στη διαδικασία διερεύνησης μιας υπόθεσης, είναι η παρουσίαση ενός καλά τεκμηριωμένου εγγράφου, όπου θα καταγράφονται με λεπτομέρεια όλες οι διαδικασίες που ακολουθήθηκαν και τα εργαλεία που χρησιμοποιήθηκαν καθιστώντας το παράλληλα, κατανοητό ακόμη και σε άτομα, που δεν διαθέτουν την κατάλληλη τεχνογνωσία.

Σχηματικά θα πρέπει να καταγραφούν :

- Ημερομηνία που ξεκίνησε η έρευνα
- Κατάσταση συσκευής κατά την κατάσχεση
- Μοντέλο smartphone, λειτουργικό σύστημα
- Φωτογραφίες του κινητού τηλεφώνου και των εξαρτημάτων του
- Εργαλεία που χρησιμοποιήθηκαν στην έρευνα
- Τα δεδομένα που ανακτήθηκαν κατά την έρευνα

Τέλος, θεμιτό είναι να υπάρχει και ένα κεφάλαιο, όπου θα αναφέρεται στα συμπεράσματα της έρευνας. Σε αυτό το κεφάλαιο, ο υπεύθυνος αναλυτής θα αναφέρεται συμπερασματικά σε γεγονότα και ευρήματα που αξιολογούνται ως σημαντικά και χρίζουν προσοχής.

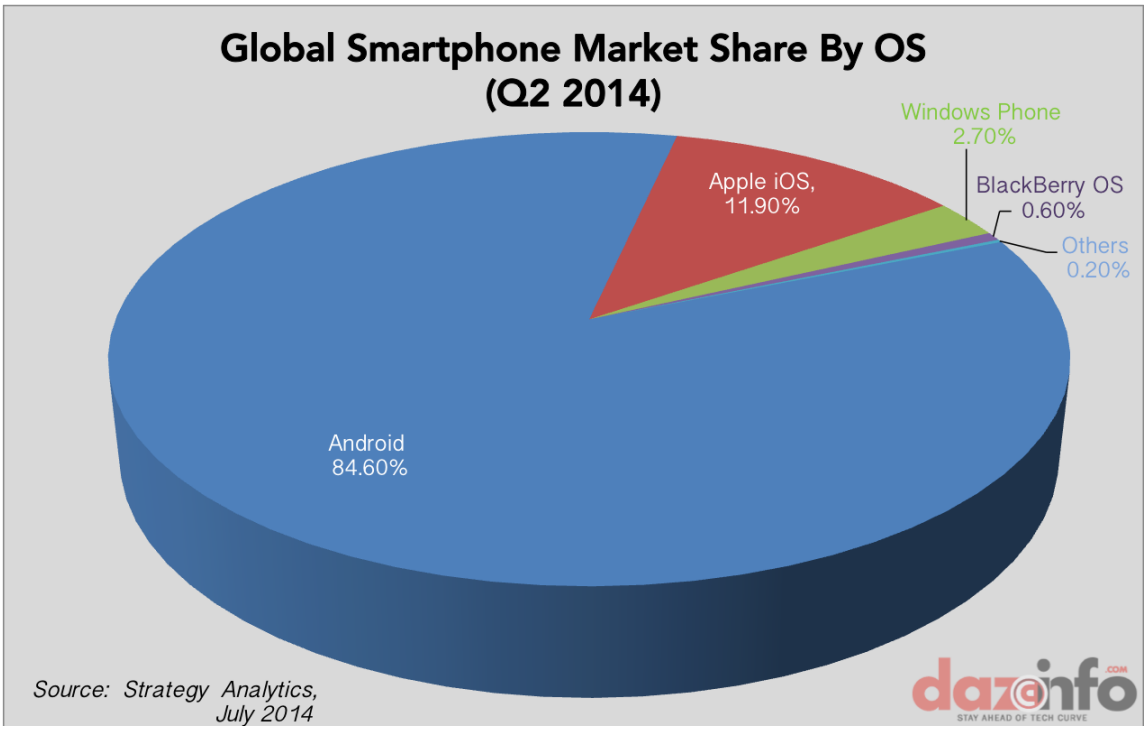
Όπως αναφέρθηκε στην αρχή του κεφαλαίου, υπάρχουν αρκετές μεθοδολογίες που μπορεί να ακολουθήσει ένας mobile forensic analyst για την διερεύνηση μιας υπόθεσης. Ωστόσο, αυτό που γίνεται αντιληπτό είναι ότι τα βήματα που αναλύθηκαν προηγουμένως αποτελούν τον θεμέλιο λίθο πάνω στον οποίο νέοι ερευνητές δομούν νέες μεθοδολογίες με περισσότερη έμφαση στην λεπτομέρεια. Αξιοσημείωτη και καλά τεκμηριωμένη είναι διαδικασία που παρουσιάζεται από την Detective Cynthia A. Murphy και σχηματοποιείται στην ιστοσελίδα της SANS.



Στην συγκεκριμένη δημοσίευση η Det. Murphy αναγνωρίζοντας την αυξημένη ανάγκη για την ύπαρξη μιας διαδικασίας, η οποία θα χαράξει κατευθυντήριες γραμμές στην διερεύνηση υποθέσεων, που ασχολούνται με την εύρεση ηλεκτρονικών πειστηρίων σε έξυπνα κινητά τηλέφωνα, καταγράφει και παρουσιάζει μια συνολική διαδικασία. Όπως αναφέρει και η ίδια, ακόμα και αν οι συσκευές που τίθενται υπό έρευνα διαφέρουν η μία από την άλλη, η διαδικασία που αναλύεται είναι σε θέση να προσφέρει στον κάθε ερευνητή έναν ασφαλή και σίγουρο δρόμο, που του εξασφαλίζει πως τα στοιχεία που θα εξαχθούν από τη συσκευή, θα είναι καλά τεκμηριωμένα και τα αποτελέσματα της έρευνας θα μπορούν να υποστηριχθούν στην δικαστική αίθουσα.

6. Android operating system

Ο ρόλος κάθε λειτουργικού είναι να χρησιμοποιεί και να διαχειρίζεται τους πόρους που διαθέτει ένα υπολογιστικό σύστημα, με σκοπό να προσφέρει ένα δίαυλο επικοινωνίας μεταξύ των εφαρμογών και των φυσικών εξαρτημάτων του για την ολοκλήρωση συγκεκριμένων εργασιών. Το λειτουργικό σύστημα Android ακολουθεί την ίδια λογική και εξοπλίζει σχεδόν όλα τα σύγχρονα κινητά τηλέφωνα, tablet αλλά και άλλες κινητές συσκευές. Η λειτουργία του είναι βασισμένη στον γνωστό και δοκιμασμένο πυρήνα του Linux κληρονομώντας έτσι όλα τα χαρακτηριστικά ασφαλείας, που το τελευταίο διαθέτει, καθώς και την ευελιξία που προσδίδει ένα λογισμικό ανοιχτού κώδικα. Το μερίδιο αγοράς που κατείχε την χρονιά 2014 ήταν κοντά στο 85%, με δεύτερο το iOS της Apple με μόλις 12% παγκοσμίως, τρίτο το λειτουργικό Windows για κινητά και τέλος το blackBerry OS.



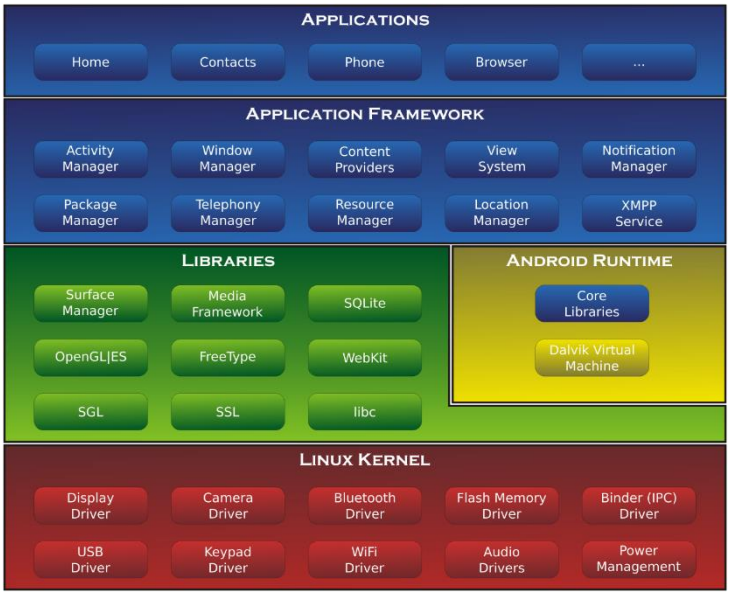
Η αλματώδης ανάπτυξή του από το 2007 και έπειτα, , οφείλεται κατά κύριο λόγο στην δυνατότητα που προσφέρει σε προγραμματιστές και εταιρίες να χρησιμοποιούν ελεύθερα τον ανοιχτό κώδικα λειτουργίας του, ώστε να

δημιουργούν εφαρμογές με μηδενικό κόστος, που μπορούν να χρησιμοποιηθούν σε πλήθος ηλεκτρονικών συσκευών.

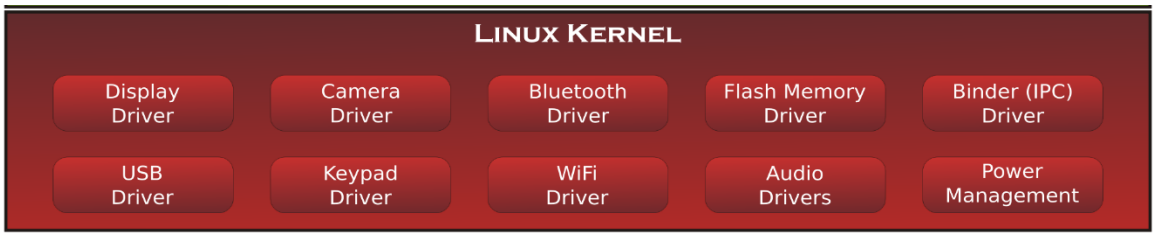
Η συνεχής ενασχόληση σχεδόν ολόκληρης της κοινότητας του ανοιχτού λογισμικού με το συγκεκριμένο λειτουργικό, οδήγησε τόσο στην ανακάλυψη αδυναμιών, όσο και στην προσθήκη νέων χαρακτηριστικών. Αποτέλεσμα αυτού είναι, σχεδόν κάθε ένα με δύο έτη να εμφανίζεται και μια νέα έκδοση, που καλύπτει τις αδυναμίες της προηγούμενης και προσφέρει νέες δυνατότητες που μπορούν να εκμεταλλευθούν οι κατασκευαστές έξυπνων κινητών συσκευών, για να δημιουργήσουν δυναμικά προϊόντα με εντυπωσιακές δυνατότητες λειτουργίας.

6.1. Android architecture

Όλες οι βασικές δυνατότητες του λειτουργικού Android, όπως η διαχείριση μνήμης, η δικτύωση (Wi-Fi, Bluetooth), καθώς και η ασφάλεια, διαχειρίζονται από τον πυρήνα του Linux. Η αρχιτεκτονική λοιπόν του συστήματος είναι ο τρόπος με τον οποίο τα παραπάνω μέρη του αλληλοεπιδρούν, ώστε να δουλέψει αποτελεσματικά όλο το οικοδόμημα.



6.2. Linux kernel

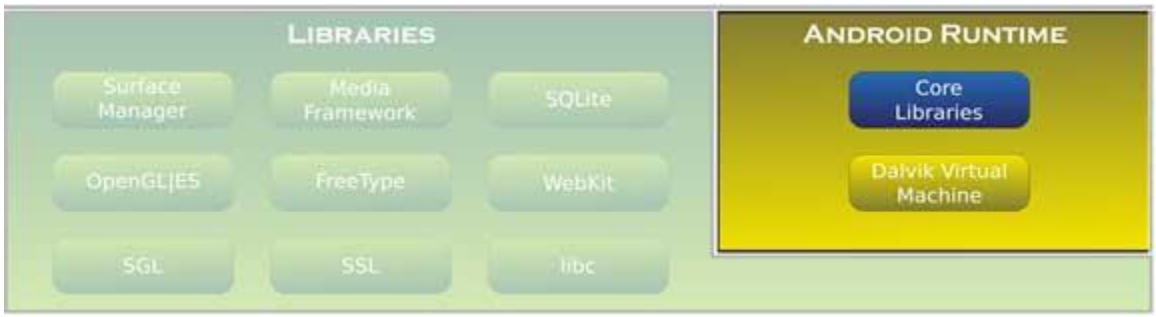


Πιο συγκεκριμένα, ο πυρήνας του linux είναι αυτός που αναλαμβάνει να μεταφράσει τις εντολές, που δίνει ο χρήστης πατώντας ένα κουμπί σε επίπεδο software. Όταν για παράδειγμα ο χρήστης πατάει το κουμπί, για να ενεργοποιήσει την λειτουργεία του Bluetooth στο κινητό του, μία εντολή κατευθύνεται προς τον συγκεκριμένο οδηγό που υπάρχει στον πυρήνα του λειτουργικού και εκείνος με την σειρά του στέλνει τις απαραίτητες εντολές στο Bluetooth hardware, ώστε να το ενεργοποιήσει. Με παρόμοια διαδικασία γίνονται και όλες οι υπόλοιπες λειτουργίες, όπως πχ. η λήψη φωτογραφιών, η ενεργοποίηση του GPS ή του Wi-Fi.

6.3. Libraries

Στο αμέσως επόμενο επίπεδο από τον πυρήνα του Linux βρίσκονται οι βιβλιοθήκες του συστήματος, οι οποίες είναι υπεύθυνες για να διαχειρίζονται διάφορους τύπους δεδομένων, όπως για παράδειγμα η SQL που χρησιμοποιείται για τις βάσεις δεδομένων και το media framework, που υποστηρίζει τις λειτουργίες βίντεο και φωτογραφίας.

6.4. Επίπεδο Android run time



Στο συγκεκριμένο επίπεδο, περιλαμβάνονται οι βασικές βιβλιοθήκες της java που χρησιμοποιούνται κατά την ανάπτυξη των εφαρμογών, καθώς και ο διερμηνευτής Dalvik. Οι εφαρμογές που δημιουργούνται στο περιβάλλον του Android υλοποιούνται με την γλώσσα προγραμματισμού της java. Για την εκτέλεση των εφαρμογών στην συγκεκριμένη γλώσσα γίνεται πάντα χρήση ενός διερμηνευτή, που στην περίπτωση του λειτουργικού Android έχει βελτιστοποιηθεί για χρήση σε μικρά ενσωματωμένα συστήματα με περιορισμένους πόρους. Το όνομα του συγκεκριμένου διερμηνευτή είναι Dalvik και έχει προκύψει από τον προγραμματιστή που τον ανέπτυξε. Κάθε εφαρμογή εκτελείται σε διαφορετικό στιγμιότυπο και απομονωμένη από τις υπόλοιπες, με αποτέλεσμα να διασφαλίζεται τόσο η ευστάθεια, όσο και η ασφάλεια του λειτουργικού.

6.5. Application framework

Το προτελευταίο επίπεδο της στοίβας ονομάζεται application framework. Στο συγκεκριμένο, υπάρχει πληθώρα APIs, τα οποία προσφέρουν στον προγραμματιστή των εφαρμογών την δυνατότητα να ενσωματώσει λειτουργίες, όπως συνδεσιμότητα στο διαδίκτυο, πρόσβαση σε αποθηκευτικά μέσα, κλπ. Για κάθε υπηρεσία που παρέχεται στις εφαρμογές, υπάρχουν και διαχειριστές οι οποίοι καλούνται για να υλοποιήσουν την συγκεκριμένη λειτουργεία.

- Activity manager - η υπηρεσία αυτή ελέγχει όλο τον κύκλο ζωής μιας εφαρμογής καθώς και την λειτουργικότητα της
- Content providers – η συγκεκριμένη υπηρεσία βοηθάει τις εφαρμογές στο να μοιράζονται δεδομένα μεταξύ τους.
- Notifications manager – αυτή η υπηρεσία χρησιμοποιείται από τις εφαρμογές για να εμφανίζουν alerts και ειδοποιήσεις
- Telephony manager – παρέχει στις εφαρμογές πληροφορίες για τις τηλεφωνικές υπηρεσίες που είναι διαθέσιμες.
- Location manager – δίνει τις απαραίτητες πληροφορίες θέσης σε κάθε εφαρμογή.

6.6. Application layer

Στο ανώτερο επίπεδο της αρχιτεκτονικής του λειτουργικού Android, βρίσκονται οι εφαρμογές που ο χρήστης αλληλοεπιδρά. Είναι υλοποιημένες με την γλώσσα προγραμματισμού java και μπορούν να χωριστούν σχηματικά σε δύο κατηγορίες, τις προ-εγκατεστημένες εφαρμογές συστήματος και αυτές, που ο χρήστης εγκαθιστά.

Στις πρώτες περιλαμβάνεται ο προεπιλεγμένος φυλλομετρητής (default browser), ένας email client, η εφαρμογή για τις επαφές, η εφαρμογή για τη λήψη φωτογραφιών, το εικονικό πληκτρολόγιο, κλπ. Οι εφαρμογές αυτές συνήθως υπάρχουν στον φάκελο /system και δεν μπορούν να διαγραφούν.

Η άλλη κατηγορία περιλαμβάνει τις εφαρμογές, που εγκαθιστά ο ίδιος ο χρήστης μέσα από πλατφόρμες, όπως το Google play, που αποτελεί και το επίσημο app-Store για το λογισμικό Android. Αυτή τη στιγμή υπάρχουν διαθέσιμες πάνω από 2 εκατομμύρια πιστοποιημένες εφαρμογές, που ένας χρήστης μπορεί να πλοηγηθεί και να επιλέξει. Οι δυνατότητες δημιουργίας ακόμα και μη πιστοποιημένων, μέσω του Google play, εφαρμογών είναι απεριόριστες. Όποιος επιθυμεί μπορεί να

υλοποιήσει και να διαμοιράσει οποιαδήποτε εφαρμογή εκμεταλλευόμενος όλες τις δυνατότητες, που το λογισμικό ανοιχτού κώδικα του παρέχει.

7. Filesystem overview

Όπως αναφέρθηκε και νωρίτερα το λειτουργικό σύστημα Android βασίζεται σε κάποιον πυρήνα Linux, που ως γνωστόν υποστηρίζει μεγάλη ποικιλία file systems. Από την οπτική ενός αναλυτή είναι σημαντικό να γνωρίζει πόσα και ποια filesystems χρησιμοποιούνται, με σκοπό να καταλήξει στην επιλογή στοχευμένων εργαλείων, που θα τον βοηθήσουν στην εκπόνηση της έρευνας. Η συνύπαρξη ταυτόχρονα πολλών filesystems επιβάλει την ύπαρξη μιας λειτουργίας, που ονομάζεται VFS (Virtual File System) και αναλαμβάνει να δίνει την πρόσβαση που χρειάζεται κάθε εφαρμογή σε όποιο από αυτά την εξυπηρετεί. Επιγραμματικά θα μπορούσαν να κατηγοριοποιηθούν ως εξής:

7.1. Flash memory filesystems

Λόγω των ιδιαίτερων χαρακτηριστικών που διαθέτουν οι μνήμες Flash απαιτούνται συγκεκριμένα filesystems, προκειμένου να λειτουργήσουν αποτελεσματικά. Οι πιο συνηθισμένες μορφές που συναντώνται σε συσκευές Android είναι οι εξής :

- **ExFAT** (extended file allocation table) το συγκεκριμένο file system έχει αναπτυχθεί από την Microsoft και υποστηρίζεται από ορισμένους κατασκευαστές, καθώς δεν αποτελεί, λόγω περιορισμών στην άδεια χρήσης, κομμάτι του πυρήνα του Linux.
- **F2FS** (Flash Friendly File System) πρόκειται για ένα file system ανοιχτού λογισμικού, που δημιουργήθηκε από την Samsung το 2012.
- **JFFS2** (Journal Flash File System version 2) χρησιμοποιείται ως προεπιλεγμένο flash file system για το Android Open Source Project από την έκδοση Ice Cream Sandwich και έπειτα.

- **YAFFS2** (Yet Another File System version 2) το συγκεκριμένο file system είναι ένα από τα πιο δημοφιλή στο οικοσύστημα των συσκευών Android. Υιοθετήθηκε το 2002 από τους περισσότερους κατασκευαστές, είναι προϊόν ανοιχτού λογισμικού, ωστόσο αφήνει σιγά σιγά τη θέση του σε μια καινούρια μορφή την EXT4 που υποστηρίζει και καλύπτει την ανάγκη για χρήση πολυεπεξεργαστών.

7.2. Media-based filesystems

Εκτός από τα filesystems που αναφέρθηκαν και αφορούν στις μνήμες flash, υπάρχουν και τα media-based, που παρουσιάζονται στην συνέχεια.

- **EXT2/EXT3/EXT4** (EXTended file system) το συγκεκριμένο filesystem εμφανίστηκε το 1992 και δημιουργήθηκε για πυρήνες linux. Η τελευταία του έκδοση το EXT4 γίνεται όλο και πιο δημοφιλής από την στιγμή που η Google ανακοίνωσε, ότι οι περισσότερες συσκευές από την έκδοση Gingerbread και έπειτα θα χρησιμοποιούν το συγκεκριμένο, καθώς οι υπολογιστικές ανάγκες των επεξεργαστών αυξάνονται.
- **FAT** (File allocation table) Το συγκεκριμένα filesystem το συναντάμε σε εξωτερικές κάρτες μνήμης με τις μορφές FAT12,FAT16,FAT32
- **VFAT** (Virtual File Allocation Table) πρόκειται για μια επέκταση του προηγούμενου filesystem. Το Συγκεκριμένο βοηθά τις συσκευές με λειτουργικό Android να επεξεργάζονται δεδομένα αποθηκευμένα σε FAT32 και προέρχονται από άλλα λειτουργικά, όπως τα Windows και τα Mac OS.

8. Android partition layout

Η κατανόηση της διάρθρωσης των filesystems στις συσκευές που χρησιμοποιούν λειτουργικό Android αποτελεί σημαντικό παράγοντα για την επιτυχή εξέταση μιας υπόθεσης από έναν ερευνητή. Ο τρόπος με τον οποίο τα δεδομένα αποθηκεύονται ανακτώνται και γενικότερα οργανώνονται, αποτελεί επίσης μία πολύτιμη γνώση, καθώς μπορεί να καθοδηγήσει την ερευνητική διαδικασία υποδεικνύοντας τα μέρη του συστήματος, που υπάρχουν σημαντικές πληροφορίες.

Τα partitions αποτελούν λογικές μονάδες αποθήκευσης δεδομένων, οι οποίες μπορούν να προσπελαστούν ξεχωριστά και κάθε μία από αυτές περιέχει ξεχωριστές πληροφορίες. Ο αριθμός των partitions μπορεί να διαφέρει από κατασκευαστή σε κατασκευαστή, ωστόσο κάποια από αυτά συναντώνται στο σύνολο σχεδόν των συσκευών, που χρησιμοποιούν λειτουργικό Android.

8.1. Boot loader partition

Το συγκεκριμένο partition είναι υπεύθυνο για την εκκίνηση του πυρήνα Android και για την επιλογή διαδικασίας εκκίνησης σε διάφορες λειτουργίες, όπως download mode ή update mode για manual ή αυτόματη αναβάθμιση πυρήνα (kernel), recovery mode για εκκίνηση της κονσόλας recovery, κλπ. Διαθέτει δηλαδή το κατάλληλο πρόγραμμα, που φροντίζει την εκκίνηση του τηλεφώνου σε πολύ χαμηλό επίπεδο λειτουργικότητάς του.

8.2. Boot partition

Στην συγκεκριμένη λογική μονάδα βρίσκεται η μνήμη RAM, καθώς και ο πυρήνας του λογισμικού Android που χρησιμοποιείται. Περιέχονται λοιπόν όλες οι απαραίτητες πληροφορίες και αρχεία που χρειάζονται για να εκκινήσει το κινητό τηλέφωνο στο απαραίτητο επίπεδο λειτουργικότητας του.

8.3. Recovery partition

Το partition αυτό χρησιμοποιείται για λειτουργίες συντήρησης του τηλεφώνου. Μέσω της κονσόλας recovery, ο χρήστης μπορεί να πραγματοποιήσει εργασίες όπως αναβάθμιση, λήψη backup των δεδομένων του, κλπ.

8.4. User data partition

Στον τομέα αυτόν είναι αποθηκευμένο σχεδόν το σύνολο των δεδομένων του χρήστη, με αποτέλεσμα το συγκεκριμένο partition να αποτελεί πρωτεύον στόχο για ανάλυση από τον εκάστοτε ερευνητή. Πιο συγκεκριμένα, περιέχει τα δεδομένα των εφαρμογών που έχουν εγκατασταθεί, τα δεδομένα των επικοινωνιών, όπως οι επαφές, η διάρκεια κλήσης, τα SMS, καθώς και δεδομένα θέσης (GPS).

8.5. System partition

Στο system partition περιλαμβάνεται το user interface που εμφανίζεται στον χρήστη, καθώς και κάποιες προεγκατεστημένες εφαρμογές.

8.6. Cache partition

Το partition αυτό περιλαμβάνει όλα εκείνες τις πληροφορίες δεδομένα, τις οποίες αναζητούν συχνά οι εφαρμογές. Η χρήση του συγκεκριμένου τομέα γίνεται για λόγους βελτιστοποίησης της ταχύτητας προσπέλασης των δεδομένων.

8.7. Radio partition

Στο Radio partition περιλαμβάνονται πληροφορίες και δεδομένα που χρησιμεύουν στην πραγματοποίηση τηλεφωνικών λειτουργιών.

8.8. Misc Partition

Το συγκεκριμένο partition αποτελεί μια αξιοσημείωτη πηγή δεδομένων, καθώς περιλαμβάνει πληροφορίες και logs που αφορούν στην χρήση λειτουργιών, όπως του Wi-Fi, του Bluetooth και άλλων. Τα στοιχεία που μπορούν να αξιοποιηθούν είναι σημαντικά, καθώς μπορεί να συνδέσουν άμεσα σχεδόν τον χρήστη του κινητού τηλεφώνου με μια συγκεκριμένη τοποθεσία σε μια συγκεκριμένη χρονική στιγμή.

9. Rooting Android

Η έννοια Rooting στο περιβάλλον του Android παρατηρείται όλα και ποιο συχνά. Το συγκεκριμένο λειτουργικό ως multiuser, όπως και το Linux από το οποίο και προέρχεται, υιοθετεί την ίδια λογική στα δικαιώματα χρήσης των αρχείων που περιέχει. Πιο συγκεκριμένα, διαχωρίζει τους χρήστες σε απλούς και super-users, με σκοπό να προστατεύσει τους πόρους ολόκληρου του συστήματος. Κάθε απλός χρήστης είναι σε θέση να διαχειρίζεται ένα μεγάλο πεδίο δυνατοτήτων της συσκευής, ωστόσο υπάρχουν περιορισμοί ως προς την πρόσβαση σε σημεία του λειτουργικού, που απαιτούν αυξημένα δικαιώματα.

Η έκφραση “rooting” λοιπόν αναφέρεται στην απομάκρυνση των περιορισμών που θέτουν τόσο οι πάροχοι, όσο και οι κατασκευαστές. Ένας απλός χρήστης ακολουθώντας μία συγκεκριμένη και πλέον σχεδόν αυτοματοποιημένη διαδικασία, καταφέρνει να πάρει root access σε όλα τα αρχεία του συστήματος. Μπορεί δηλαδή να τρέξει εφαρμογές, που απαιτούν αυξημένα δικαιώματα επιπέδου root, να παραμετροποιήσει ρυθμίσεις του συστήματος και να έχει πρόσβαση σε δεδομένα των εφαρμογών, που προηγουμένως δεν είχε, να απεγκαταστήσει προεγκατεστημένες εφαρμογές, ακόμα και να αλλάξει όλο το interface του λειτουργικού Android εγκαθιστώντας μια custom ROM.

Από την μεριά του ερευνητή, ένα “rooted smartphone” αποτελεί έναν ισχυρό σύμμαχο για την διερεύνηση μια υπόθεσης. Χωρίς περιορισμούς πλέον μπορεί να πλοηγείται σε βάθος και να χρησιμοποιεί εργαλεία ανάκτησης και εξέτασης δεδομένων με την μέγιστη αποτελεσματικότητα. Στο σημείο αυτό, θα πρέπει να σημειωθεί πως τα περισσότερα εργαλεία που χρησιμοποιούνται για τον παραπάνω σκοπό, απαιτούν την ύπαρξη αυξημένων δικαιωμάτων χρήσης, ώστε να επιτρέπεται η πρόσβαση σε σημεία του λειτουργικού, όπου υπάρχουν χρήσιμες προς αξιολόγηση και περαιτέρω ανάλυση, πληροφορίες.

10. Opensource tools in mobile forensics

Για πολλά χρόνια, ο τομέας των “digital forensics” αποτελούσε έργο αποκλειστικά των κυβερνητικών υπηρεσιών. Ωστόσο, τα τελευταία χρόνια αναπτύσσονται αρκετές εταιρικές πρωτοβουλίες, που κινούνται προς την ίδια κατεύθυνση, προωθώντας ορθολογικές πρακτικές απόκτησης και ανάλυσης δεδομένων. Σαν συνέπεια αυτού εμφανίζονται στην αγορά εργαλεία, που στόχο έχουν την ανάλυση δεδομένων με σκοπό την ανακάλυψη πειστηρίων και την χρήση τους στις δικαστικές αίθουσες για την στοιχειοθέτηση μίας υπόθεσης.

Τα λογισμικά που αποτελούν εταιρικά προϊόντα συνήθως χαρακτηρίζονται από υψηλή αποτελεσματικότητα, άρτια γραφική σχεδίαση, καθώς και αξιοπιστία. Ωστόσο, τα περισσότερα από αυτά στο παρελθόν, δημιουργούνταν αποκλειστικά και μόνο με την λογική του ιδιόκτητου λογισμικού κλειστού κώδικα, κρίνοντας πως με αυτόν τον τρόπο οι δυνατότητες και η ασφάλεια των διαδικασιών λειτουργίας των εργαλείων θα είναι διασφαλισμένες. Αποτέλεσμα της συγκεκριμένης πρακτικής ήταν η δημιουργία λογισμικών, που χαρακτηρίζονται από την αυξημένη εξάρτηση τους από την εταιρία που τα δημιούργησε, καθώς και από αυξημένα κόστη απόκτησης και αναβάθμισής τους.

Η απάντηση στο συγκεκριμένο πρόβλημα προέρχεται από την κοινότητα του ελεύθερου λογισμικού. Για παράδειγμα, η εισβολή του λειτουργικού Android στην καθημερινότητα των χρηστών τεχνολογικών προϊόντων αναδεικνύει την δυναμική και τις δυνατότητες που μπορεί να προσδώσει ένα προϊόν ανοιχτού κώδικα χωρίς στενά πλαίσια υλοποίησης και περιορισμών.

Έτσι λοιπόν τόσο κάποιες εταιρίες, όσο και μεμονωμένοι ερευνητές, παρατηρώντας την τάση αυτή, αρχίζουν να δίνουν περισσότερη έμφαση στην υλοποίηση εργαλείων, που εκμεταλλεύονται τις δυνατότητες που τους παρέχει ένα λογισμικό ανοιχτού κώδικα. Με τον τρόπο αυτό ουσιαστικά μειώνουν τα κόστη λειτουργίας και υποστήριξης, καθώς η ύπαρξη κοινότητας ελεύθερου λογισμικού μπορεί να βοηθήσει σε αυτό. Ο πηγαίος κώδικας είναι ελεύθερα διαθέσιμος,

πράγμα το οποίο σημαίνει πως ελέγχεται από ένα μεγάλο μέρος χρηστών που παρατηρούν την λειτουργία του, τον διορθώνουν και τον εξελίσσουν.

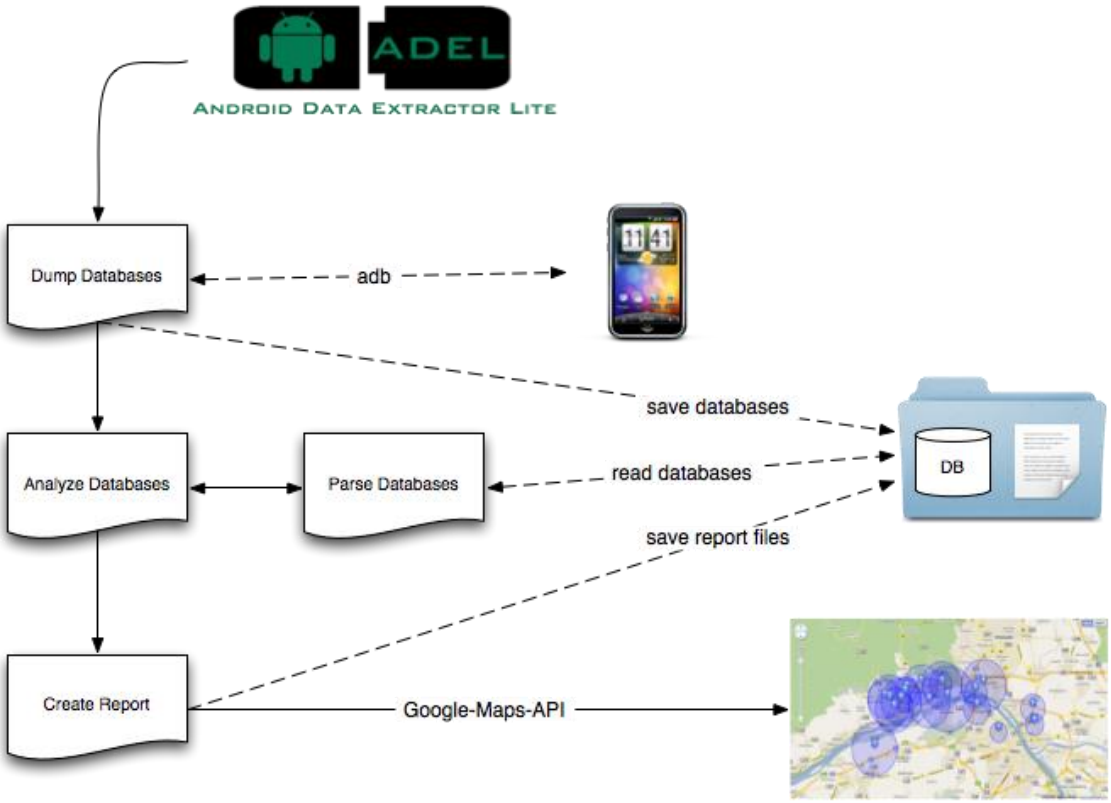
Στον τομέα των mobile forensics, η λογική που ακολουθείται είναι παρόμοια. Υπάρχουν αρκετά αξιόλογα εργαλεία κλειστού κώδικα, όπως το Device seizure της Paraben's, το Oxygen forensics, το Cellebrite, το XRY, το Mobile phone Examiner, κλπ. Τα λογισμικά αυτά προέρχονται από αρκετά σημαντικές εταιρίες στον χώρο των Forensics και αποτελούν αξιόπιστες εμπορικές λύσεις για την περάτωση μιας έρευνας. Η αλήθεια είναι πως τα συγκεκριμένα λογισμικά λειτουργούν εξαιρετικά όσο αφορά την υποστήριξη λειτουργικών, όπως το iOS και το Android και ειδικά σε περιπτώσεις κλειδωμένων συσκευών ή "not-rooted". Πρέπει ωστόσο να αναφερθεί πως εκτός από το υψηλό κόστος απόκτησης των παραπάνω εργαλείων, υπάρχουν και άλλοι παράγοντες που δρουν αποτρεπτικά στην τυφλή υιοθέτησή τους. Η μη υποστήριξη του συνόλου των συσκευών που κυκλοφορεί στην αγορά και το γεγονός, ότι κατά την διαδικασία εξαγωγής των δεδομένων, κάποιες πληροφορίες που χρησιμοποιούνται από τρίτες εφαρμογές δεν μπορούν να προσπελαστούν με επιτυχία και οδηγούν τον ερευνητή να χρησιμοποιήσει και μη αυτοματοποιημένες μεθόδους εξέτασης των στοιχείων. Εκτός από τα παραπάνω λογισμικά κλειστού κώδικα, παρατηρούνται και αξιόλογες προσπάθειες στην υλοποίηση εργαλείων ελεύθερου λογισμικού.

10.1. AFlogical

Η εταιρία VIAFORENSICS έχει παρουσιάσει την open source edition του AFlogical. Ουσιαστικά πρόκειται για μία μικρή εύχρηστη εφαρμογή, που εγκαθίσταται στην μνήμη ενός smartphone με λειτουργικό Android μέσω του

Android debug bridge (adb). Σκοπός της είναι η απόκτηση δεδομένων σε μορφή .csv, όπως για παράδειγμα η λίστα επαφών με όλες τις πληροφορίες που είναι αποθηκευμένες για κάθε μία από αυτές, πότε πραγματοποιήθηκε η τελευταία συνομιλία, sms με πληροφορίες αποστολέα-παραλήπτη, αρχείο κλήσεων με την διάρκεια αυτών και τη χρονική στιγμή που αυτές έγιναν, καθώς και κάποιες πληροφορίες για την ίδια τη συσκευή, όπως το IMSI, το IMEI-MEID,την έκδοση του λειτουργικού, κλπ.

10.2. ADEL



Η εφαρμογή ADEL (Android Data Extractor Lite) αποτελεί μια ακόμα υλοποίηση ανοιχτού κώδικα και η λειτουργία της βασίζεται στην απόκτηση βάσεων δεδομένων, που βρίσκονται στην συσκευή με απώτερο σκοπό την ανάλυση και παρουσίαση των δεδομένων που περιέχονται. Ένα μεγάλο πλεονέκτημα που τονίζεται στο συγκεκριμένο εργαλείο είναι ότι όλες οι ενέργειες γίνονται αυτοματοποιημένα μέσω της γλώσσας python και δίνοντας έμφαση στην αποφυγή

οποιασδήποτε αλλαγής στα αρχικά δεδομένα. Για τον λόγο αυτό, η εφαρμογή δημιουργεί ένα αντίγραφο των βάσεων, όπου γίνεται όλη η έρευνα και ταυτόχρονα υπολογίζει τις τιμές Hash πριν και μετά από αυτήν, ώστε να επιβεβαιωθεί ότι καμία αλλαγή δεν έγινε στα αρχικά δεδομένα. Το συγκεκριμένο λογισμικό εγκαθίσταται μέσω adb (Android debug bridge) και απαιτεί για την λειτουργία του αρχικά η συσκευή να είναι Rooted και στην συνέχεια ένα προκαθορισμένο αρχείο ρυθμίσεων .xml για αυτή. Δυστυχώς μέχρι σήμερα υπάρχει μόνο ένα τέτοιο αρχείο διαθέσιμο και αναφέρεται στο Samsung Galaxy S2 με έκδοση Android 2.3.3

10.3. DroidSpotter

Το εργαλείο DroidSpotter δημιουργήθηκε το 2013 στα πλαίσια ακαδημαϊκής έρευνας στο πανεπιστήμιο της Iowa. Πρόκειται για μια υλοποίηση, η οποία εκμεταλλεύεται την αυξανόμενη χρήση δεδομένων θέσης από τις εφαρμογές. Πιο συγκεκριμένα, η λειτουργία της βασίζεται στην παρακολούθηση του location API του Android. Όταν μια εφαρμογή το καλέσει, τότε τα δεδομένα της τίθενται υπό έρευνα για τυχόν πληροφορίες θέσης.

10.4. Aytopsy

Ένα πολύ γνωστό εργαλείο ανάλυσης δεδομένων είναι το Aytopsy. Το συγκεκριμένο αποτελεί την γραφική απεικόνιση της πλατφόρμας SleuthKit, που συναντάται στο λογισμικό linux και περιλαμβάνει αρκετές λειτουργίες, που είναι χρήσιμες για την εξέταση των πιο κοινών μορφών filesystems, που συναντώνται στις συσκευές Android. Μερικές από αυτές είναι, η παρουσίαση των πρόσφατων ενεργειών του χρήστη, όπως οι τελευταίες ιστοσελίδες που επισκέφθηκε και τα πιο πρόσφατα αρχεία που προσπέλασε, η ανάκτηση μεταδεδομένων από τις φωτογραφίες που κατέχει, καθώς και η δυνατότητα εξέτασης των δεδομένων των εφαρμογών που έχει εγκατεστημένες στη συσκευή.

10.5. LiME

Το εργαλείο LiME παρουσιάστηκε το 2012 και είναι από τα πιο χαρακτηριστικά παραδείγματα υλοποίησης ανοιχτού κώδικα. Πρόκειται ουσιαστικά για ένα kernel module, που στοχεύει στην απόκτηση της πτητικής μνήμης από συσκευές με λειτουργικό Linux ή βασισμένες σε αυτό, όπως το Android. Συγκριτικό πλεονέκτημά του σε σχέση με άλλα παρόμοια εργαλεία είναι το γεγονός, ότι μπορεί να καταγράψει το σύνολο της μνήμης μιας συσκευής με εγκληματολογικά αποδεκτό τρόπο, καθώς η χρήση του μειώνει την αλληλεπίδραση ερευνητή -

συσκευής κατά την διάρκεια της έρευνας με αποτέλεσμα να παρατηρείται και πολύ μικρό αποτύπωμα στις διεργασίες του συστήματος.

10.6. Scalpel / Foremost

Και τα δύο αυτά εργαλεία είναι αρκετά γνώριμα στην κοινότητα των digital forensics, καθώς αποτελούν δυο ισχυρές υλοποιήσεις ανοιχτού κώδικα με δυνατότητες αναζήτησης και ανάκτησης αρχείων. Τόσο το Foremost όσο και το Scalpel βασίζουν την λειτουργία τους στην αναζήτηση των headers και footers των αρχείων, που βρίσκονται σε κάποιο μέσο αποθήκευσης, κάποιο directory ή ένα image αρχείο. Η διαδικασία αυτή είναι γνωστή ως file carving. Μία πλήρης λίστα των αρχείων που υποστηρίζονται είναι διαθέσιμη στις *man pages,* ωστόσο σημαντικό θεωρείται το γεγονός, ότι μέσω των αρχείων .conf (scalpel.conf , foremost.conf) των δυο εργαλείων είναι δυνατό να προστεθούν και άλλοι τύποι αρχείων, που δεν περιλαμβάνονται εξ' αρχής. Στον τομέα των mobile forensics και ειδικά στο περιβάλλον του λειτουργικού Android αποδίδουν το ίδιο καλά, με αποτέλεσμα να αποτελούν δύο εύχρηστες υλοποιήσεις που συμβάλουν θετικά στην πορεία διερεύνησης μιας υπόθεσης.

10.7. Androphsy

Το συγκεκριμένο εργαλείο παρουσιάζεται ως η μοναδική έως τώρα συνολική προσπάθεια ελεύθερου λογισμικού, που μπορεί να υποστηρίξει έναν ερευνητή σε όλη τη διάρκεια της εγκληματολογικής διαδικασίας. Οι δημιουργοί του Androphsy φιλοδοξούν να εκμεταλλευτούν τον κενό χώρο, που υπάρχει μεταξύ των ακριβών εταιρικών προϊόντων και αυτόν των δωρεάν λύσεων με τις ελάχιστες δυνατότητες που προσφέρουν, εγκαθιδρύοντας μία πλατφόρμα διερεύνησης συσκευών με λειτουργικό Android. Η πλατφόρμα αυτή έχει σκοπόνα προσφέρει διαχείριση των υποθέσεων και μεγιστοποίηση του αριθμού των στοιχείων, που αποκτώνται διατηρώντας παράλληλα την εγκυρότητα των δεδομένων. Η λεπτομερής σχεδίαση και κατά συνέπεια η αποτελεσματικότητα πάνω στην οποία βασίζεται το οικοδόμημα της συγκεκριμένης υλοποίησης, έγκειται σε δύο γεγονότα. Αρχικά στο ότι δεν γίνεται χρήση κάποιας custom recovery image για την εξαγωγή των

δεδομένων, καθώς όπως αναφέρεται δεν υπάρχει κάποια κοινά αποδεκτή για χρήση σε εγκληματολογική έρευνα, αλλά χρησιμοποιεί χαμηλού επιπέδου ήδη υπάρχουσες λειτουργίες, όπως η *DD* και οι εντολές μέσω *ADB.* Και στην συνέχεια για την διαδικασία της πρόσβασης με αυξημένα δικαιώματα χρήσης (Root) γίνεται χρήση ενός script που εκμεταλλεύεται συγκεκριμένες αδυναμίες του συστήματος (exploits) και προσφέρει εγγυημένα καμία αλλαγή στα δεδομένα του χρήστη.

Η συγκεκριμένη πολλά υποσχόμενη εκπόνηση πραγματοποιήθηκε στα πλαίσια ακαδημαϊκής έρευνας στο Πανεπιστήμιο Colombo και είναι διαθέσιμη στην κοινότητα του ελεύθερου λογισμικού μέσω της δημοσίευσης του πηγαίου κώδικα στο GitHUB.

Σχηματικά το Androphsy framework υποστηρίζει

- Αποτελεσματική διαχείριση υποθέσεων και στοιχείων
- Απόκτηση δεδομένων σε physical – logical - filesystem επίπεδο
- Ανάλυση δεδομένων που αποκτήθηκαν
- Παρουσίαση πειστηρίων και στοιχείων

10.8. Osaf toolkit / Santoku linux

Πρόκειται ουσιαστικά για δύο δημοφιλείς διανομές Linux με προεγκατεστημένες εφαρμογές απόκτησης και ανάλυσης δεδομένων, τόσο από κινητές συσκευές, όσο και από άλλα υπολογιστικά συστήματα.

Η υλοποίηση του Open source Android forensics toolkit γίνεται από μια ομάδα φοιτητών στο πανεπιστήμιο του Cincinnati με σκοπό την δημιουργία και προτυποποίηση μιας διαδικασίας ανάλυσης εφαρμογών και πιθανών κακόβουλων λογισμικών, που υπάρχουν στο περιβάλλον του λειτουργικού Android. Η διανομή αυτή βασίζεται στην έκδοση Ubuntu 11.10 και περιέχει πληθώρα εργαλείων για τους σκοπούς που αναφέρθηκαν.

Παρόμοια περίπτωση είναι και η διανομή Santoku Linux. Η συγκεκριμένη έκδοση παρουσιάζεται ως η πλέον ενδεδειγμένη για την εγκληματολογική διερεύνηση κινητών συσκευών, για την εξέταση κακόβουλων λογισμικών, καθώς και για την συνολική επισκόπηση της ασφάλειας μιας έξυπνης κινητής συσκευής.

Τα εργαλεία που περιέχει είναι αρκετά και μπορούν δειγματοληπτικά να κατηγοριοποιηθούν ως εξής:

- Development tools : Android sdk manager / Heimdall
- Penetration testing : Burp suite / nmap / Ettercap
- Wireless analyzers : Wireshark / DSniff
- Device forensics : AFLogical OSE / ExifTool / Scapel / Sleuthkit
- Reverse engineering : Androguard / APK tool / Dex2jar

Κοινή συνισταμένη και των δύο προηγούμενων είναι η επιθυμία για την δημιουργία μιας ανοιχτής κοινότητας, όπου ειδικοί της ασφάλειας, αναλυτές, ερευνητές, καθώς και προγραμματιστές ή ακόμα και μη ειδικοί, θα μπορούν να μαθαίνουν να συζητούν και να μοιράζονται μεταξύ τους τεχνικές και μεθοδολογίες.

11. Dive into the data

Η απόκτηση και η ανάλυση των δεδομένων αποτελεί τον ακρογωνιαίο λίθο μιας ερευνητικής διαδικασίας. Ο τρόπος με τον οποίο ένας ερευνητής καταφέρνει να μετατρέψει απλές πληροφορίες σε πολύτιμα στοιχεία, απαιτεί συγκεκριμένη και καλά τεκμηριωμένη μεθοδολογία σε συνδυασμό πάντα με τα κατάλληλα εργαλεία και αποτελεσματικές τεχνικές. Στο συγκεκριμένο κεφάλαιο θα παρουσιαστεί η δυνατότητα, που υπάρχει για την πραγματοποίηση της παραπάνω δραστηριότητας με την αποκλειστική χρήση προϊόντων ανοιχτού κώδικα.

Στο σημείο αυτό θεωρείται χρήσιμη μια αναφορά στο Android software development kit (SDK) και σε ένα από τα εργαλεία του, το Android debug bridge (ADB), που αποδεικνύεται πολύτιμος συνεργάτης στα χέρια ενός Android forensics examiner.

Android software development kit (SDK)

Η συγκεκριμένη υλοποίηση είναι αυτή που ουσιαστικά βοηθά τους προγραμματιστές στο περιβάλλον του Android να δημιουργούν και να ελέγχουν τις εφαρμογές, που οι ίδιοι αναπτύσσουν. Πρόκειται για ένα σύνολο εργαλείων, που προσφέρουν από χρήσιμες βιβλιοθήκες (που είναι απαραίτητες κατά την υλοποίηση αυτών) έως και εικονικές συσκευές με διάφορες εκδόσεις του παραπάνω λειτουργικού. Η χρησιμότητα των εργαλείων αυτών παρατηρείται και κατά την ερευνητική διαδικασία αναζήτησης στοιχείων από κάποιον αναλυτή.

Android debug bridge (ADB)

Η χρήση του συγκεκριμένου εργαλείου κρίνεται απαραίτητη για οποιαδήποτε διαδικασία απόκτησης δεδομένων από κινητές συσκευές με λειτουργικό Android. Χαρακτηρίζεται ως client-server πρόγραμμα και λειτουργεί μέσω command line προσφέροντας επικοινωνία του ερευνητή με την φυσική ή κάποια εικονική συσκευή. Σχηματικά για την επίτευξή της περιλαμβάνει τρείς επιμέρους λειτουργίες: τον client, τον server και έναν deamon. Οι δύο πρώτοι τρέχουν στο υπολογιστικό σύστημα που έχει εγκατεστημένο το SDK, ενώ ο deamon ως

background process στην συσκευή. Οι εντολές που μπορεί να δεχθεί σαν παράμετρος το εργαλείο ADB είναι αρκετές και μερικές από αυτές θα παρουσιαστούν στην συνέχεια.

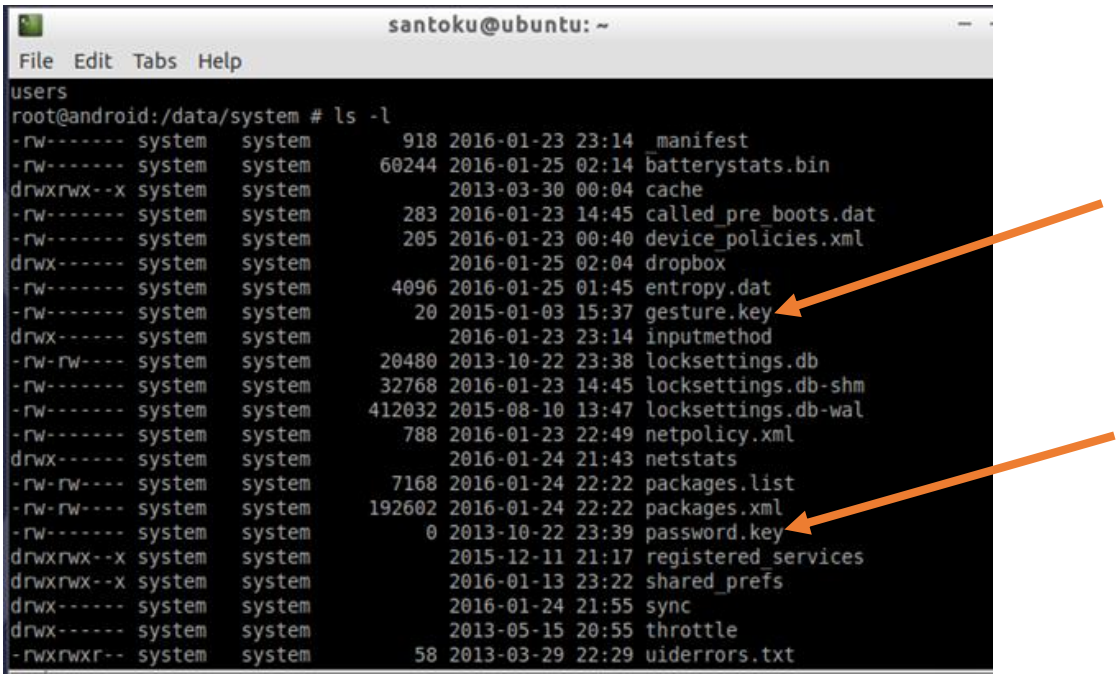
12. Access to the device

Η πρώτη διαδικασία που πρέπει να πραγματοποιήσει ένας ερευνητής μόλις αποκτήσει μια έξυπνη κινητή συσκευή στα χέρια του και ενώ αρχικά έχει φροντίσει να απομονωθεί αποτελεσματικά από κάθε επικοινωνία με το δίκτυο είναι να απομακρύνει οποιοδήποτε υποτυπώδες μέσο ασφάλειας έχει χρησιμοποιήσει ο χρήστης ώστε να πάρει πρόσβαση στο περιβάλλον του τηλεφώνου. Οι μηχανισμοί αυτοί προσφέρονται συνήθως από το ίδιο το λειτουργικό ή τον κατασκευαστή και εμφανίζονται ως κλείδωμα οθόνης. Ένας χρήστης έχει την δυνατότητα να διαλέξει ανάμεσα σε τρείς συνήθως λειτουργίες και αυτές είναι το κλείδωμα με την χρήση ενός τετραψήφιου κωδικού PIN, ενός αλφαριθμητικού κωδικού ή ενός δημιουργικού μοτίβου.

Όλες οι παραπάνω λειτουργίες απαιτούν παρόμοιες τεχνικές για την αντιμετώπιση τους. Αυτό πάντως που πρέπει να τονιστεί είναι ότι σε καμία από τις τρείς περιπτώσεις ένας ερευνητής δεν θα πρέπει να μπει στην διαδικασία να μαντέψει καθώς αρκετοί κατασκευαστές προσφέρουν την επιλογή ολικής διαγραφής των δεδομένων έπειτα από έναν αριθμό αποτυχημένων προσπαθειών.

Η τεχνική απομάκρυνσης όπως αναφέρθηκε και πριν είναι παρόμοια και για τους τρείς μηχανισμούς και μπορεί να εφαρμοστεί με την χρήση του ADB και με την προϋπόθεση ότι η συσκευή παρέχει ROOT πρόσβαση στα δεδομένα. Στην περίπτωση του αλφαριθμητικού κωδικού και του PIN αρκεί η απόκτηση δύο αρχείων από την συσκευή, του *password.key* που βρίσκεται αποθηκευμένο σε μορφή hash στην διεύθυνση */data/system/* και της έξτρα ποσότητας που προστηθετε στον κωδικό και ονομάζεται salt που βρίσκεται στην διεύθυνση */data/data/com.Android.providers.settings/databases/setting.db.* Στην περίπτωση του μοτίβου αρκεί η απόκτηση μόνο του *gesture.key* που βρίσκεται στην διεύθυνση

data/system/gesture.key. Σε μια επίσημη εγκληματολογική έρευνα ίσως απαιτείται η διαδικασία να καταλήξει στο να αποκαλύψει τους κωδικούς και την μορφή του μοτίβου και αυτό μπορεί να γίνει με την χρήση του εργαλείου ανοιχτού κώδικα Android pattern lock cracker που εκμεταλλεύεται την δυναμική της Python ή του δωρεάν Andriller. Ωστόσο υπάρχει και μια ακόμη επιλογή αυτή του να διαγραφούν τα συγκεκριμένα αρχεία.



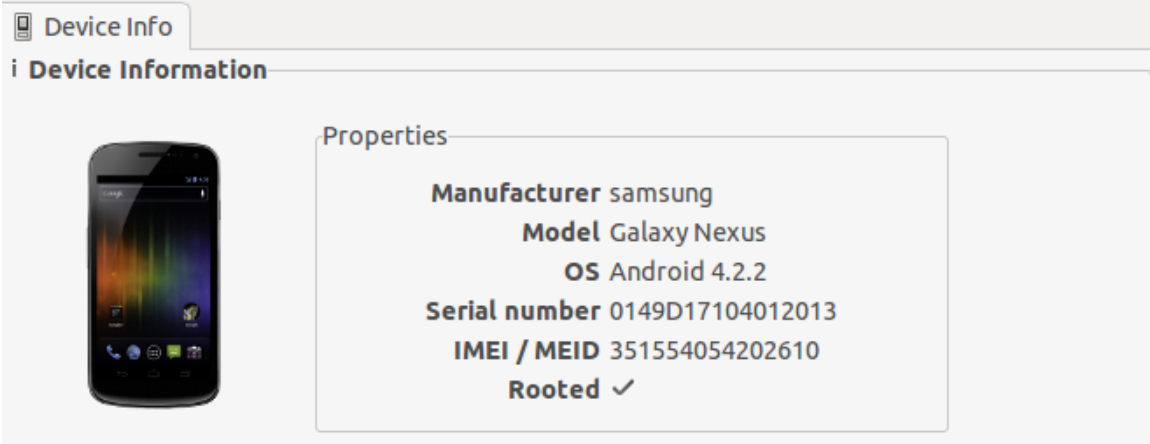
13. Logical acquisition

Η μέθοδος της λογικής απόκτησης δεδομένων, αναφέρεται συνήθως στην συλλογή συγκεκριμένων πληροφοριών αυτοματοποιημένα από μια συσκευή με την εγκατάσταση σε αυτή, μιας μικρής εφαρμογής. Οι εφαρμογές αυτές είναι σχεδιασμένες στο να τοποθετούνται αρχικά σε σημεία του λειτουργικού που δεν θα επιφέρουν καμία τροποποίηση στα δεδομένα, ενώ μόλις ολοκληρώσουν την λειτουργία τους απομακρύνονται από το σύστημα. Ουσιαστικά το αποτέλεσμα της λειτουργίας τους αναφέρεται σε σχετική βιβλιογραφία ως η πρώτη εικόνα που σχηματίζει ένας ερευνητής για την χρήση του κινητού τηλεφώνου.

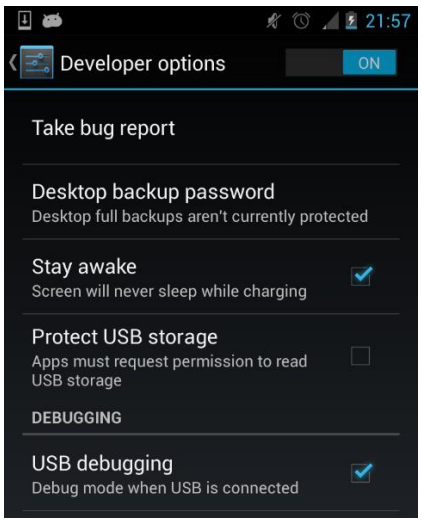
Οι δυνατότητες τις συγκεκριμένης πρακτικής είναι καθορισμένες και περιορίζονται στην απόκτηση δεδομένων όπως για παράδειγμα το αρχείο κλήσεων της συσκευής, ο κατάλογος επαφών, τα μηνύματα κειμένου, το ιστορικό δραστηριότητας στο διαδίκτυο καθώς και κάποιες άλλες βασικές πληροφορίες για την συσκευή. Όσο αφορά την ανάκτηση διαγραμμένων πληροφοριών η πρακτική αυτή δεν μπορεί να αποφέρει τα μέγιστα αποτελέσματα καθώς περιορίζεται η δυναμική της μόνο στην πιθανή εύρεση αρχείων βάσης SQL που έχουν μαρκαριστεί από το λειτουργικό ως διαγραμμένα και παράλληλα δεν έχουν επαναχρησιμοποιηθεί.

Υπάρχουν αρκετά εργαλεία διαθέσιμα στην αγορά των mobile forensics. Η εφαρμογή ανοιχτού κώδικα AFLogical της NowSecure αποτελεί μια αξιόπιστη λύση για την απόκτηση αρχείων από έξυπνες κινητές συσκευές που χρησιμοποιούν λειτουργικό Android από την έκδοση 1.5 και έπειτα. Η διαδικασία αρχικά απαιτεί την σύνδεση του κινητού τηλεφώνου μέσω usb καλωδίου με έναν υπολογιστή που διαθέτει το εργαλείο ADB (Android debug bridge). Στο επόμενο στάδιο δημιουργείται η διασύνδεση μεταξύ τους και στην συνέχεια το ίδιο εργαλείο αναλαμβάνει να προωθήσει την εφαρμογή στην μνήμη του κινητού. Εκεί τα δεδομένα καταγράφονται και αποθηκεύονται σε μορφή .csv που αργότερα θα μπορούν να αναγνωστούν από διάφορα λογισμικά υπολογιστικών φύλλων. Τέλος μια άλλη λειτουργία του ADB χρησιμοποιείται για να εξάγει τα δεδομένα στον υπολογιστή και να απεγκαταστήσει την εφαρμογή.

Για την καλύτερη κατανόηση της παραπάνω τεχνικής απόκτησης δεδομένων παρουσιάζεται στην συνέχεια η διαδικασία με τις απαραίτητες λεπτομέρειες. Το περιβάλλον εργασίας αποτελείται από έναν ηλεκτρονικό υπολογιστή με λειτουργικό Windows 8, ένα εικονικό μηχάνημα Santoku Linux με τις απαραίτητες εφαρμογές προεγκατεστημένες και ένα Smartphone Samsung με λειτουργικό Android 4.2.2.

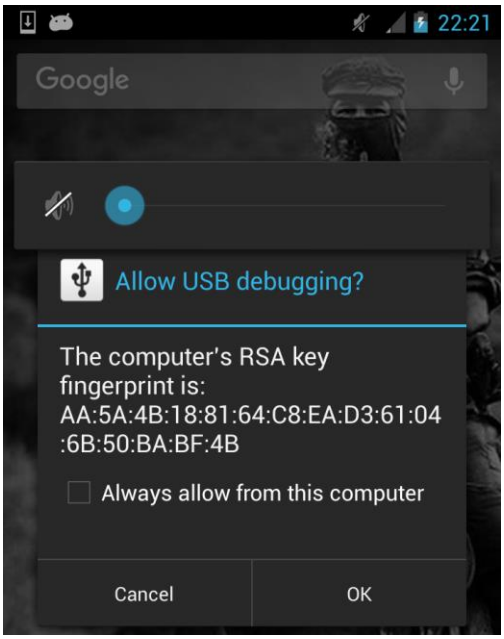


Πρώτο βήμα της διαδικασίας αποτελεί η σύνδεση του smartphone με τον Η/Υ και στην συνέχεια με το εικονικό περιβάλλον που έχει εγκατασταθεί το λειτουργικό Santoku με τα απαραίτητα για την εξόρυξη δεδομένων εργαλεία. Η σύνδεση αυτή πραγματοποιείται μέσω του καλωδίου usb 2.0 που διαθέτει η συσκευή και έπειτα από την ενεργοποίηση των Developer Options που εμφανίζονται στις ρυθμίσεις, ο ερευνητής επιλέγει την λειτουργία του usb debugging.

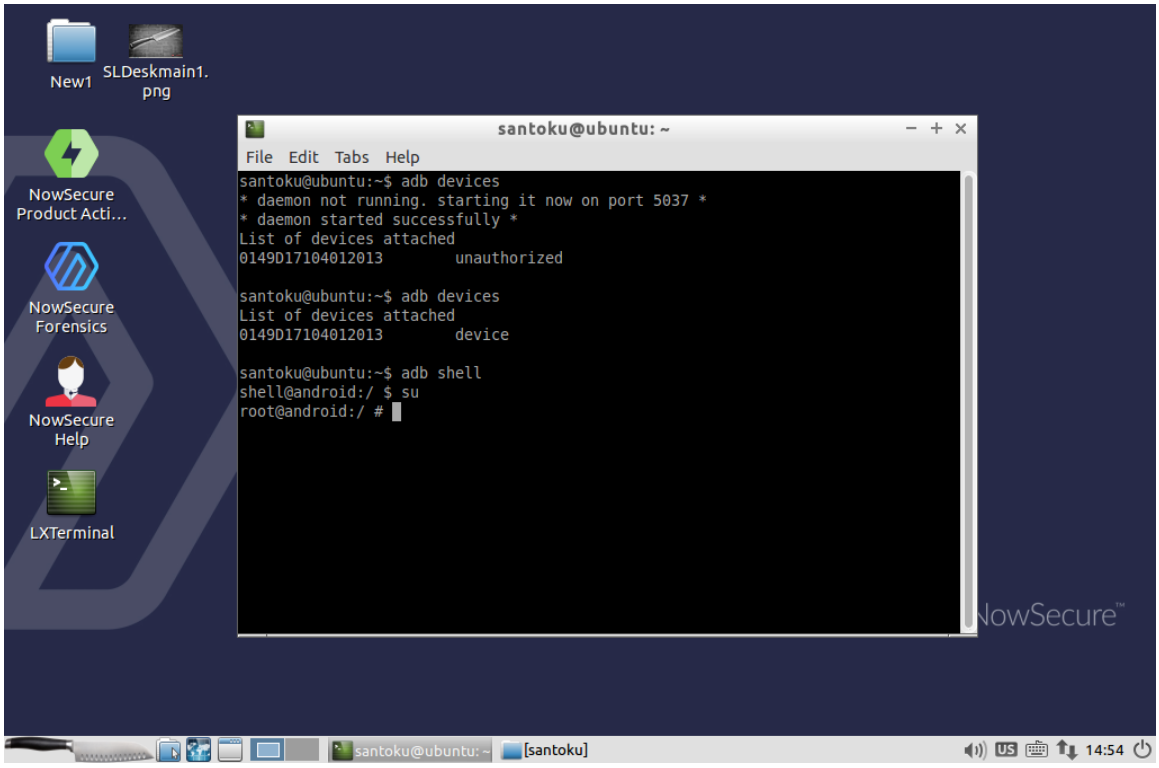


Έπειτα από την επιλογή αυτή το τηλέφωνο αναγνωρίζεται από το σύστημα που είναι συνδεδεμένο, εγκαθιστά κάποια προγράμματα οδήγησης και είναι έτοιμο πλέον να δεχθεί εντολές και να αλληλεπιδράσει.

Το λειτουργικό Santoku που χρησιμοποιείται στην συγκεκριμένη περίπτωση έχει προεγκατεστημένο το εργαλείο adb που παρέχει την δυνατότητα επικοινωνίας ενός χρήστη με την συσκευή μέσω γραμμής εντολών. Ανοίγοντας λοιπόν ένα terminal και πληκτρολογώντας την εντολή adb εμφανίζονται οι τρόποι χρήσης του εργαλείου αυτού, τα ορίσματα που δέχεται και γενικότερα η σύνταξη των εντολών λειτουργίας του. Επιλέγοντας την εντολή adb devices παρατηρείται πως ενεργοποιείται μια διεργασία στην πόρτα 5037 και ψάχνει για τυχόν συνδεδεμένες συσκευές. Αρχικά αυτό που εμφανίζεται είναι μια συσκευή με τον χαρακτηρισμό unauthorized, κοιτώντας όμως την οθόνη του κινητού τηλεφώνου διακρίνεται ένα μήνυμα με την αποτύπωση ενός κλειδιού RSA που έχει δημιουργηθεί από τον Η/Υ και προτρέπει στην επιλογή, του εάν επιτέπεται ο τελευταίος να εκτελέσει λειτουργίες debugging στην συσκευή.

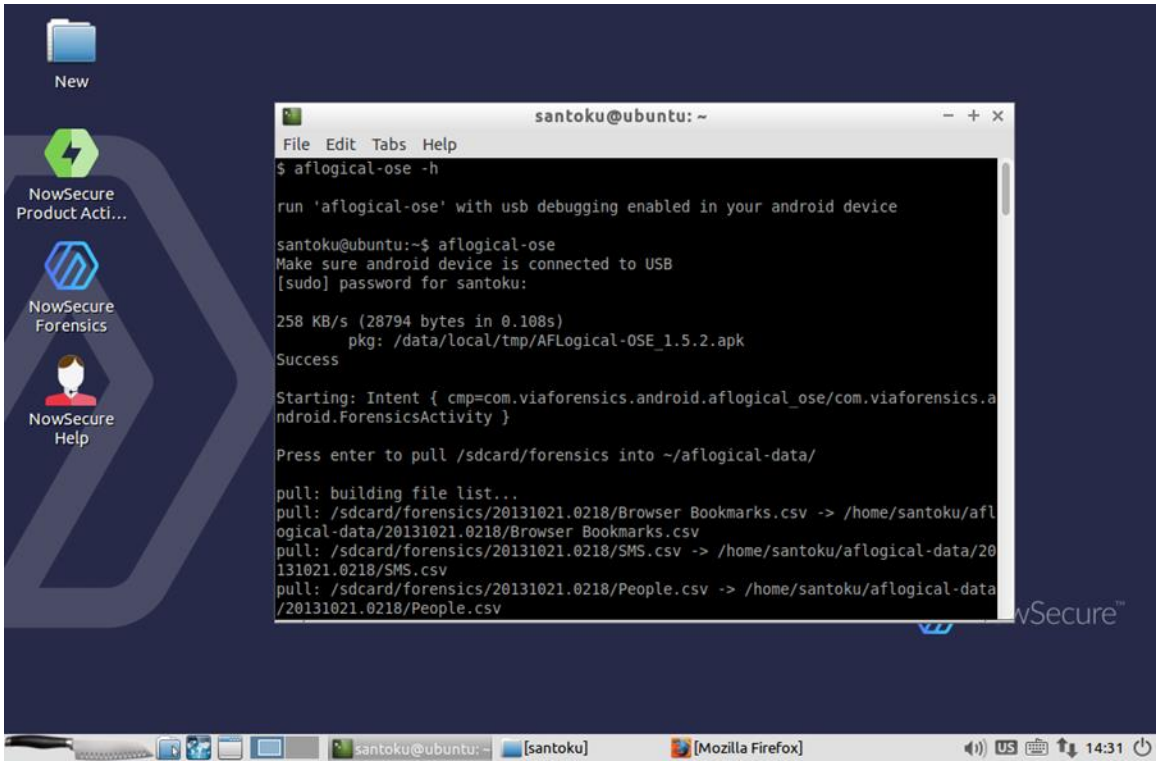


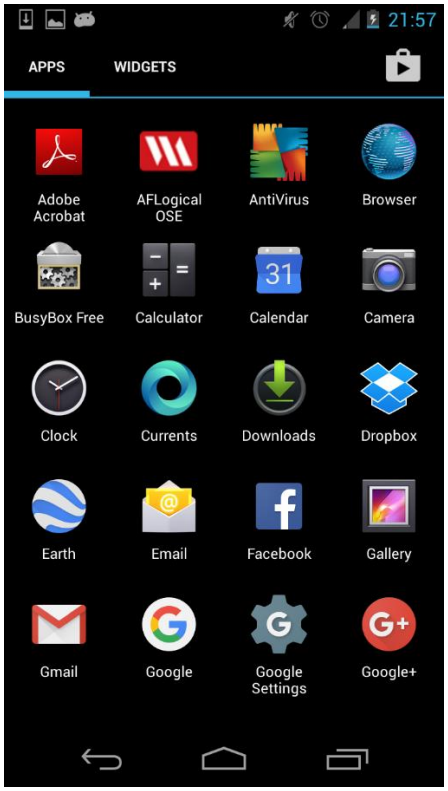
Έπειτα από την θετική απόκριση στο μήνυμα που παρουσιάστηκε εκτελείται ξανά η εντολή adb devices και διακρίνεται πως η συσκευή πλέον αναγνωρίστηκε επιτυχώς και επιτρέπει διεργασίες debugging.

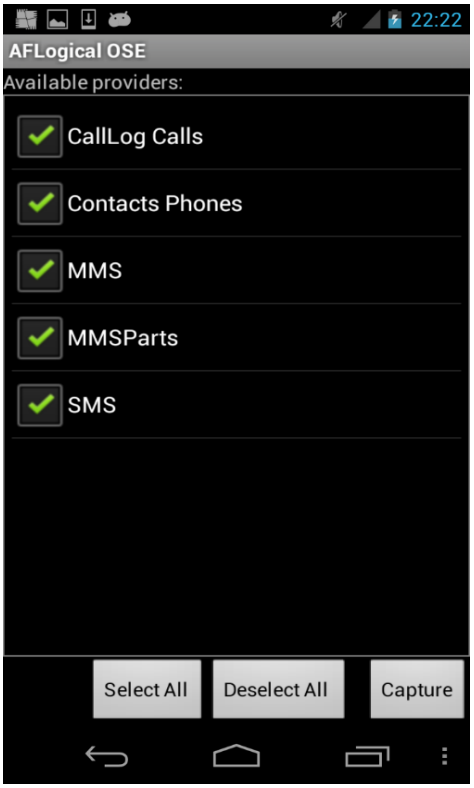


Η συσκευή που χρησιμοποιείται είναι Rooted με αποτέλεσμα να παρέχει αυξημένα δικαιώματα πρόσβασης σε αυτόν που την περιεργάζεται. Για να μπορέσει ο ερευνητής να εκμεταλλευθεί την δυνατότητα αυτή εκτελεί στην συνέχεια την εντολή adb shell και με τον τρόπο αυτόν δημιουργεί ένα session επικοινωνίας που ουσιαστικά του επιτρέπει να εισέλθει στο filesystem με δικαιώματα υπερχρήστη. Στο σημείο αυτό έχει πλέον αποκτήσει πρόσβαση στο σύνολο των δεδομένων που υπάρχουν στην συσκευή και συνεχίζει στην διαδικασία απόκτησης τους.

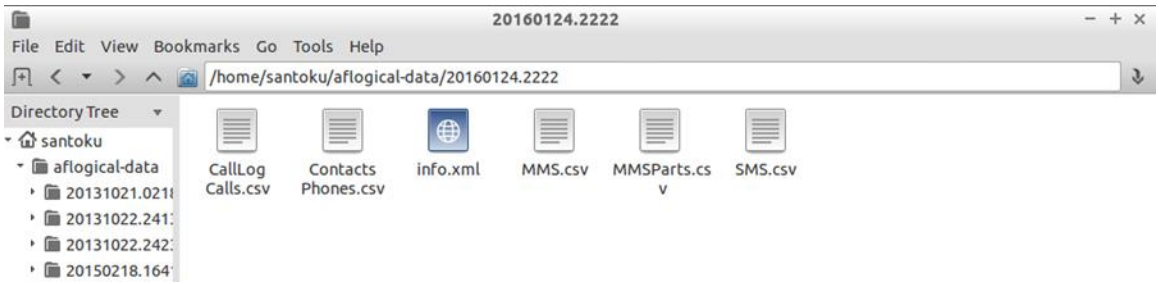
Για την απόκτηση των δεδομένων αυτών θα χρησιμοποιηθεί ένα από τα εργαλεία ανοιχτού κώδικα που αναφέρθηκαν προηγούμενα και ονομάζεται AFLogical OSE. Πρόκειται για μία από τις εφαρμογές που βρίσκονται ήδη προεγκατεστημένες στο περιβάλλον εργασίας που χρησιμοποιείται και το πλεονέκτημα της είναι η απλοποιημένη λειτουργία της καθώς και το ελάχιστο μέγεθος της (80kb). Αρχικά στην συσκευή μεταφέρεται το αρχείο .apk και τοποθετείται σε έναν προσωρινό φάκελο του filesystem στην συνέχεια εκτελείτε και αντλεί τα αποτελέσματα σε έναν άλλο φάκελο με την ονομασία forensics που και αυτός με την σειρά του μεταφέρετε με την εντολή adb pull στο εικονικό μηχάνημα.


New
NowSecure Product Acti...
NowSecure Forensics
NowSecure Help
santoku@ubuntu: ~
File Edit Tabs Help
$ aflogical-ose -h
run 'aflogical-ose' with usb debugging enabled in your android device
santoku@ubuntu:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for santoku:
258 KB/s (28794 bytes in 0.108s)
pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success
Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.android.ForensicsActivity }
Press enter to pull /sdcard/forensics into ~/aflogical-data/
pull: building file list...
pull: /sdcard/forensics/20131021.0218/Browser Bookmarks.csv -> /home/santoku/aflogical-data/20131021.0218/Browser Bookmarks.csv
pull: /sdcard/forensics/20131021.0218/SMS.csv -> /home/santoku/aflogical-data/20131021.0218/SMS.csv
pull: /sdcard/forensics/20131021.0218/People.csv -> /home/santoku/aflogical-data/20131021.0218/People.csv
[santoku]
[Mozilla Firefox]
14:31

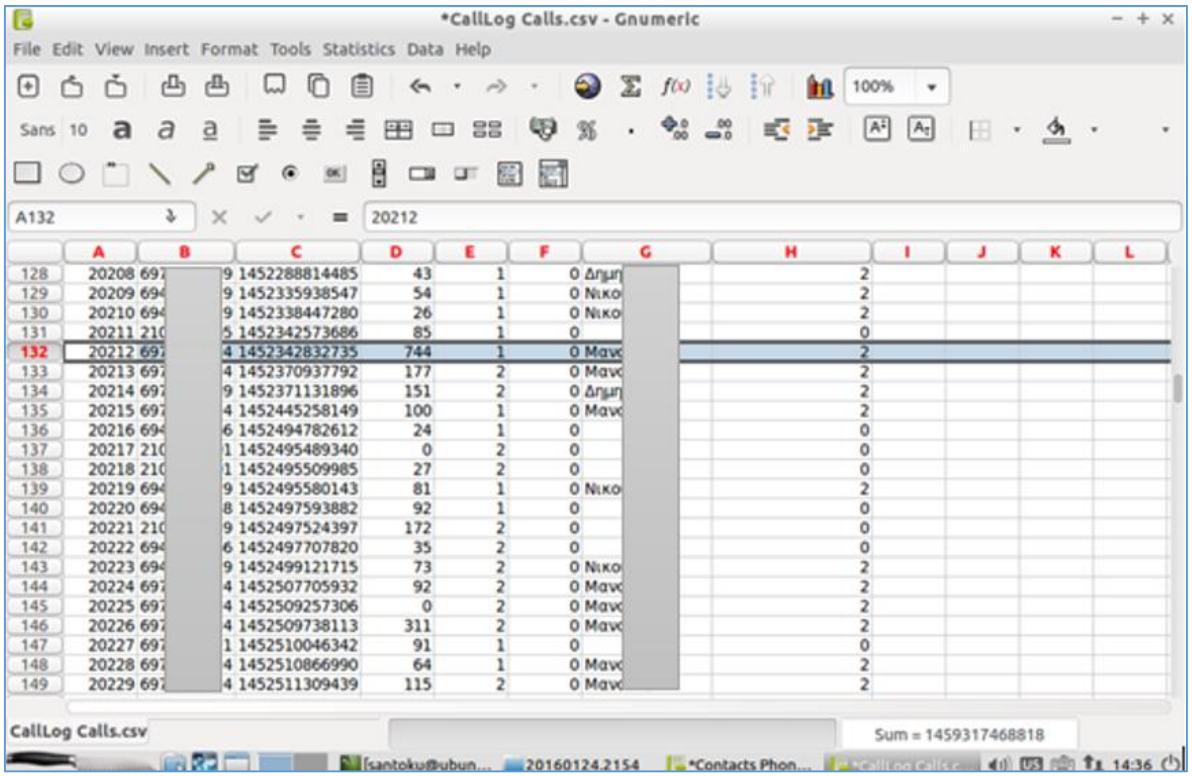

21:57
APPS
WIDGETS
Adobe Acrobat
AFLogical OSE
AntiVirus
Browser
BusyBox Free
Calculator
Calendar
Camera
Clock
Currents
Downloads
Dropbox
Earth
Email
Facebook
Gallery
Gmail
Google
Google Settings
Google+


22:22
AFLogical OSE
Available providers:
CallLog Calls
Contacts Phones
MMS
MMSParts
SMS
Select All
Deselect All
Capture

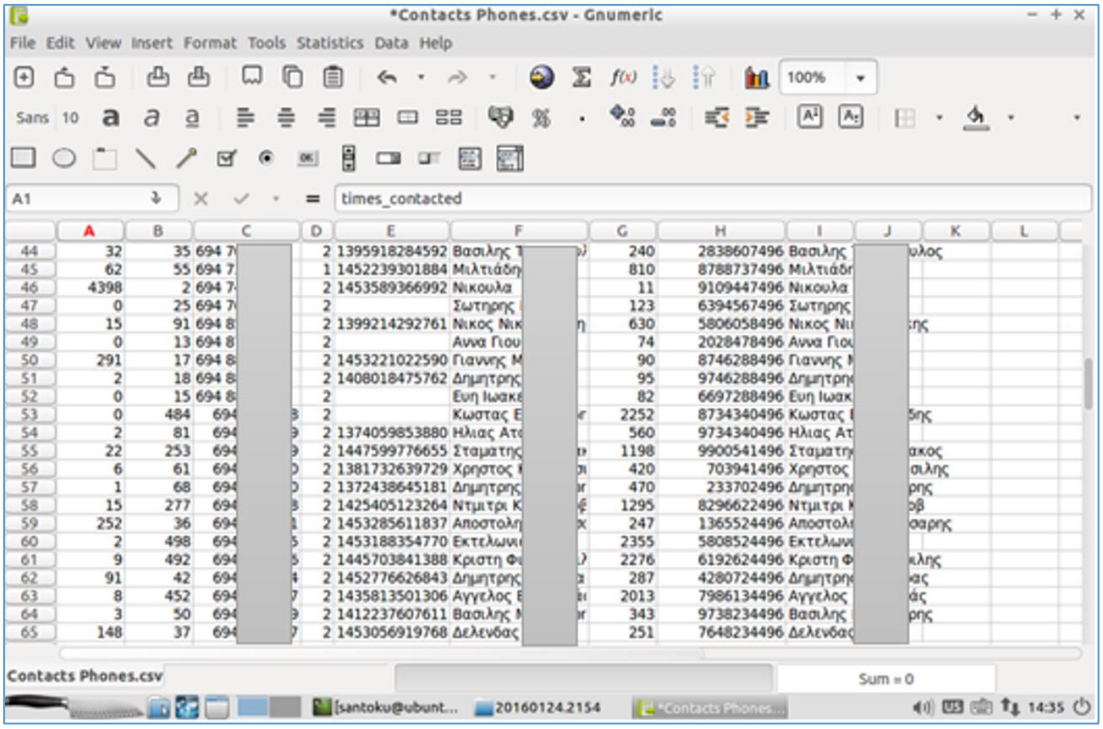
Τα δεδομένα πλέον περνάνε από το στάδιο της απόκτησης σε αυτό της ανάλυσης και παρουσίασης τους. Ανοίγοντας τον φάκελο forensics που δημιουργήθηκε εμφανίζονται τα αρχεία που αποκτήθηκαν, πιο συγκεκριμένα η λίστα επαφών, τα μηνύματα sms/mms, η λίστα με τα δεδομένα κλήσεων και τέλος ένα αρχείο info.xml με πληροφορίες της συσκευής.



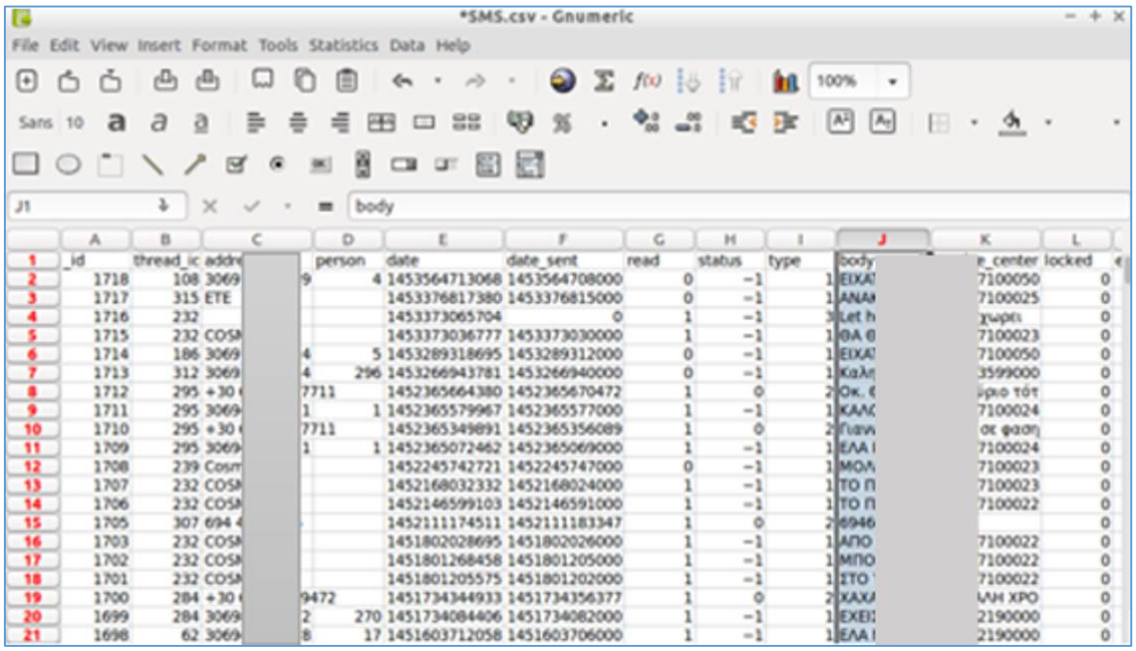
Πιο συγκεκριμένα ανοίγοντας το πρώτο αρχείο ο αναλυτής λαμβάνει γνώση για το σύνολο των κλήσεων που έγιναν στο τηλέφωνο, το όνομα και τον αριθμό που πραγματοποίησε τις κλήσεις αυτές καθώς και την χρονική στιγμή που έγινε η τελευταία συνομιλία.



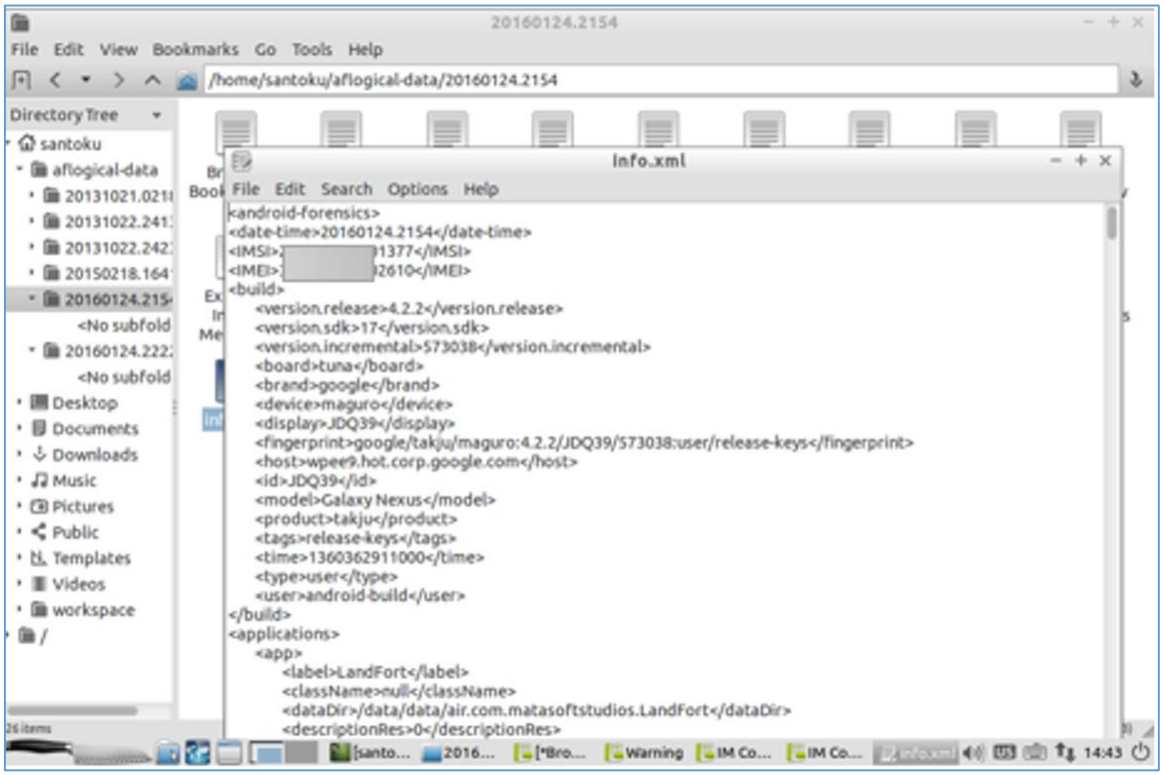
Τα ίδια σχεδόν στοιχεία προσφέρονται και στο επόμενο αρχείο με την ονομασία contacts.csv



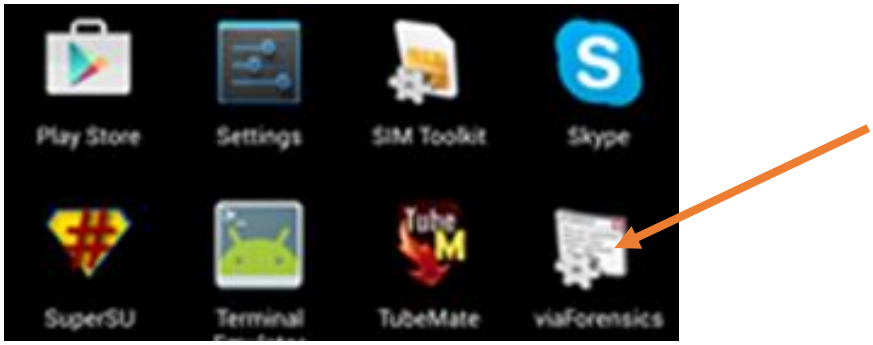
Το αρχείο των sms παρουσιάζει μεγάλο ενδιαφέρον καθώς περιλαμβάνει πληροφορίες όπως, τα δεδομένα των μηνυμάτων, τον αριθμό από τον οποίο εστάλησαν και την ημερομηνία που πραγματοποιήθηκε η επικοινωνία αυτή.

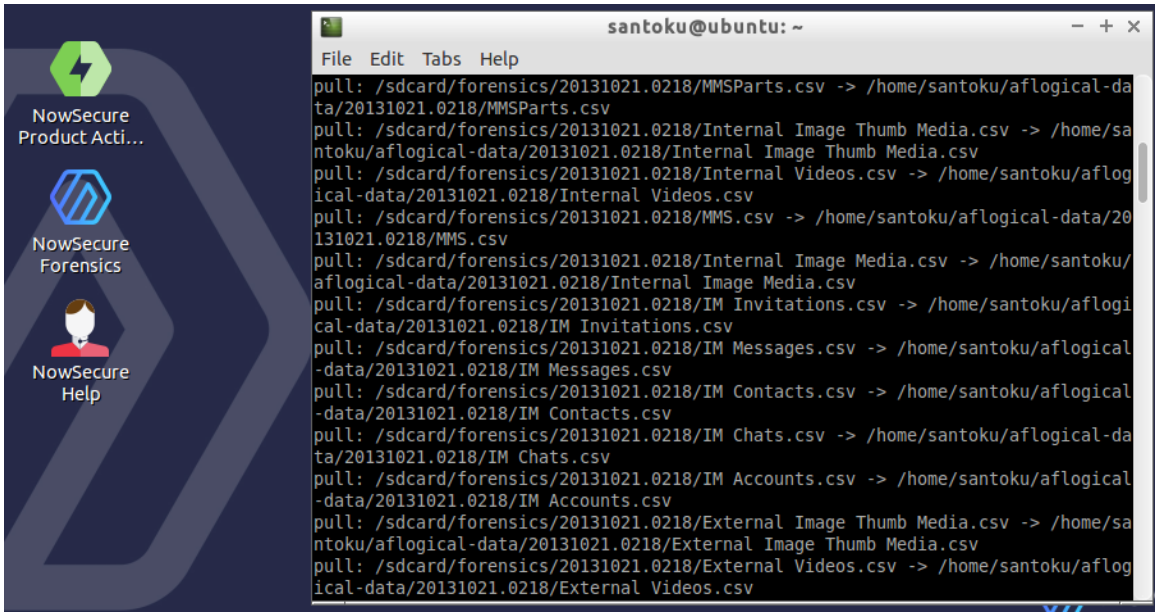


Τέλος στο αρχείο info.xml παρουσιάζονται χαρακτηριστικά γνωρίσματα της συγκεκριμένης συσκευής, όπως οι αριθμοί IMSI και IMEI, το μοντέλο της, η έκδοση του λειτουργικού και άλλα.

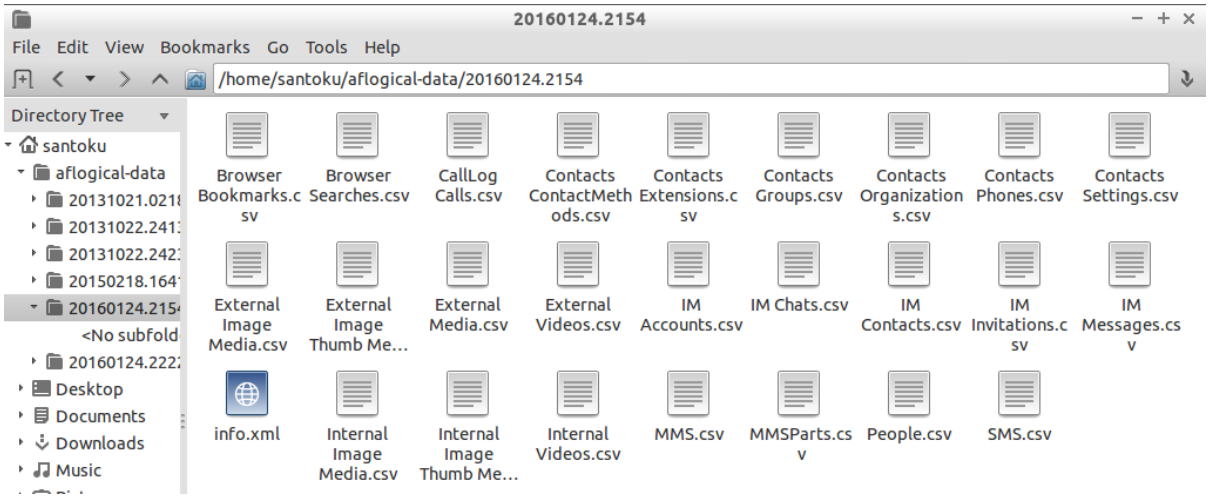


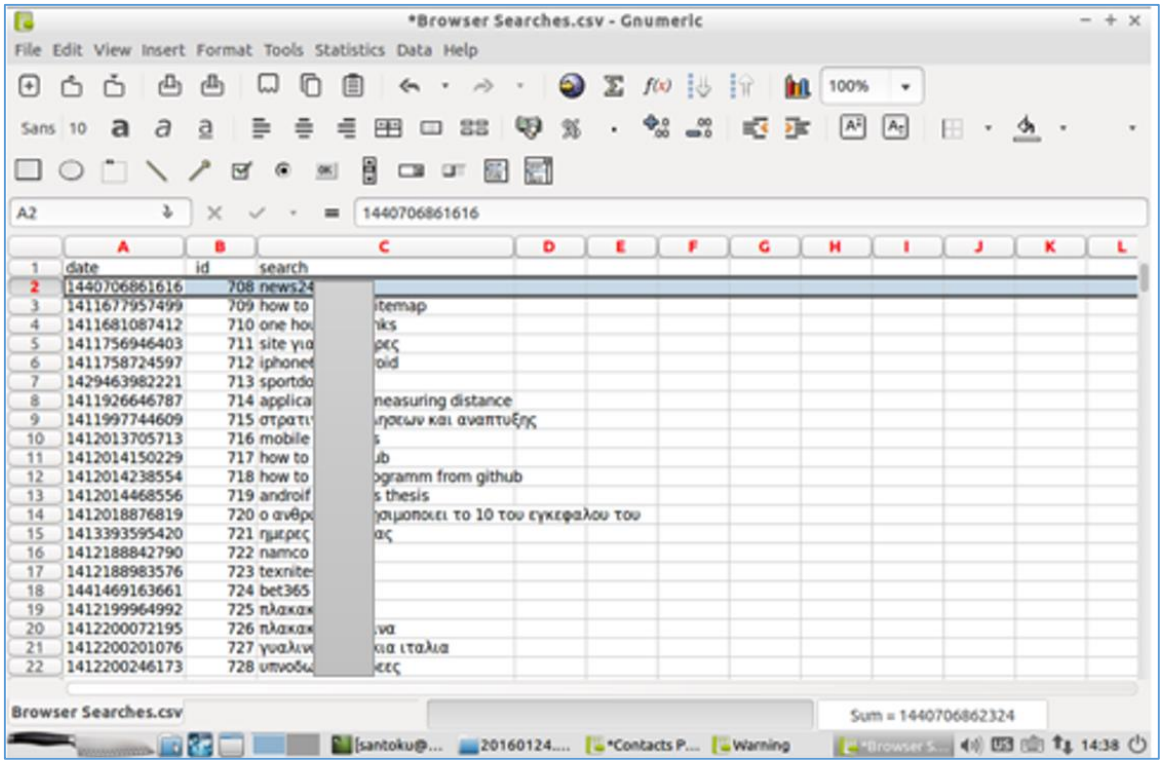
Για να τονιστεί η δυναμική που χαρακτηρίζει το συγκεκριμένο εργαλείο κρίνεται θεμιτό να παρουσιαστεί και μια ακόμη έκδοση του. Η έκδοση AFLogical for law enforcement ακολουθεί την ίδια λογική όσο αφορά την πολιτική ανοιχτού κώδικα ωστόσο διατίθεται αποκλειστικά σε κυβερνητικές υπηρεσίες. Η διαδικασία εγκατάστασης της εφαρμογής, ο τρόπος με τον οποίο συλλέγονται τα δεδομένα και η παρουσίαση τους γίνονται με την ίδια ακριβώς μεθοδολογία. Η διαφορά ωστόσο παρατηρείται στον αριθμό των αρχείων που αποκτώνται και στον όγκο των δεδομένων.

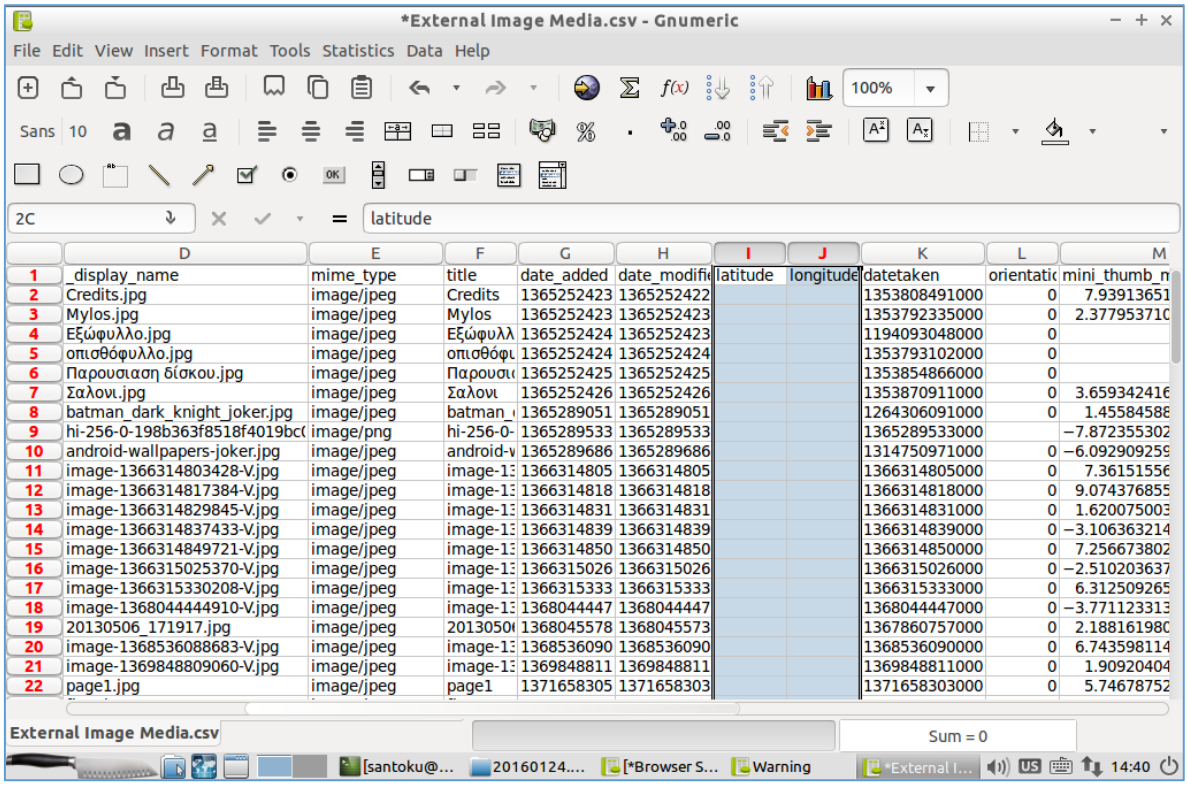




Με την εφαρμογή αυτή ένας ερευνητής είναι σε θέση να αποκτήσει το σύνολο σχεδόν των πληροφοριών που μπορούν να προκύψουν από την διαδικασία της λογικής απόκτησης δεδομένων. Δεδομένα ιστορικού αναζήτησης, στοιχεία για την περιήγηση στο διαδίκτυο, καθώς και φωτογραφίες ή βίντεο που είναι αποθηκευμένα στην συσκευή προστίθενται επιπλέον στα προηγούμενα αρχεία δίνοντας μια πιο σαφή εικόνα για τις δραστηριότητες που έχουν πραγματοποιηθεί στην συσκευή που διερευνάτε.







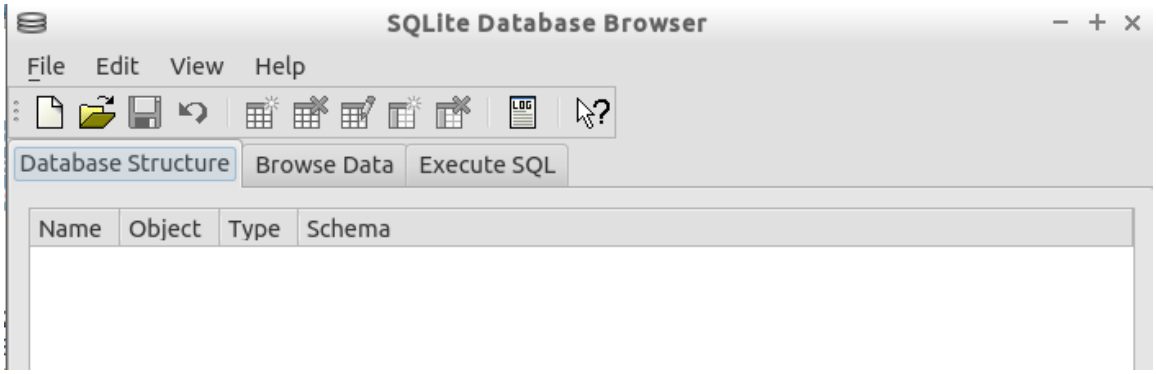
Κλείνοντας την αναφορά στα συγκεκριμένα εργαλεία θα πρέπει να τονιστεί ότι για την διασφάλιση της ακεραιότητας της διαδικασίας, η λειτουργία των εφαρμογών θα

πρέπει να τερματίζεται, να απομακρύνονται τα αρχεία εγκατάστασης .apk και η συσκευή να επανέρχεται στην κατάσταση που βρισκόταν κατά την κατάσχεση της.

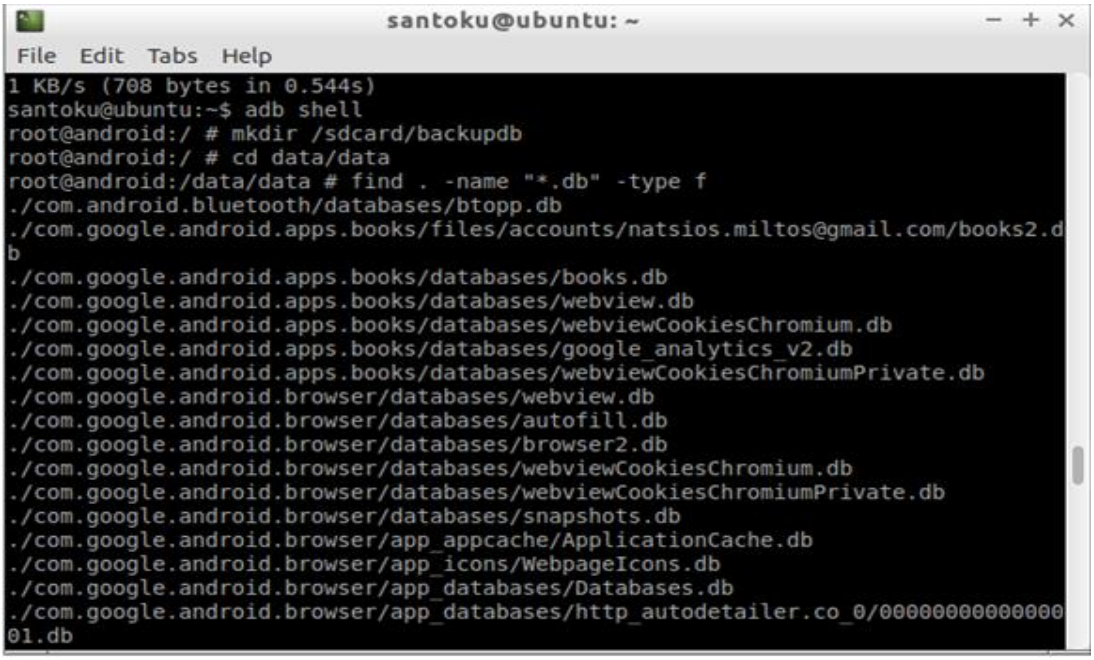
14. Manual acquisition

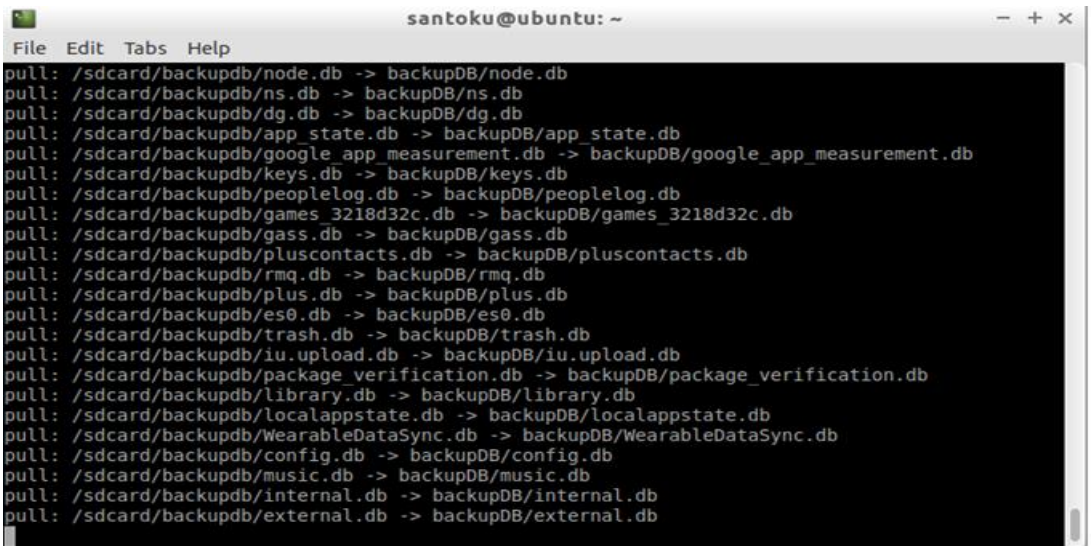
Τα αυξημένα δικαιώματα πρόσβασης που παρέχει η συσκευή δίνουν επιπλέον την δυνατότητα στον ερευνητή να αναζητά και να συλλέγει πληροφορίες και στοιχεία χωρίς την χρήση κάποιας αυτοματοποιημένης διεργασίας. Με άλλα λόγια η χρήση της εφαρμογής ADB (Android Debug Bridge) αρκεί στο να συγκεντρωθούν δεδομένα από σημεία του filesystem που θα βοηθήσουν στην διερεύνηση μιας υπόθεσης.

Οι βάσεις δεδομένων (SQL) αποτελούν σημαντικό στοιχείο ελέγχου τόσο στην περίπτωση των παραδοσιακών διαδικασιών εξέτασης στον κλάδο της εγκληματολογικής έρευνας ηλεκτρονικών υπολογιστών όσο και σε αυτόν της διερεύνησης έξυπνων κινητών συσκευών. Στο περιβάλλον εργασίας που αναφέρθηκε προηγούμενα, σημαντική πηγή πληροφοριών αποτελούν οι βάσεις δεδομένων που βρίσκονται αποθηκευμένες στην μνήμη του Smartphone. Πιο συγκεκριμένα τόσο το λειτουργικό σύστημα Android όσο και οι εφαρμογές που είναι εγκατεστημένες σε αυτό χρησιμοποιούν υλοποιήσεις SQL για την οργάνωση και αποθήκευση των δεδομένων. Τα συγκεκριμένα στοιχεία αποθηκεύονται συνήθως στην διεύθυνση */data/data/*application_name** με την μορφή *όνομα_αρχείου.db* και μπορούν να προσπελαστούν με την χρήση ενός SQL browser.

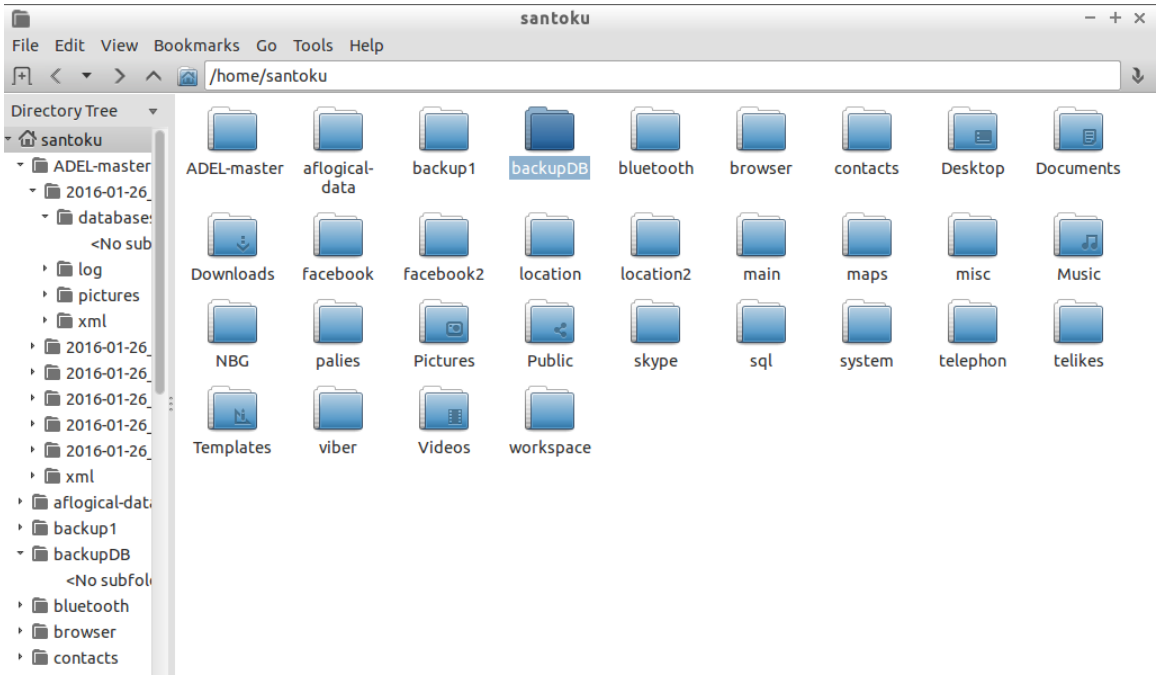


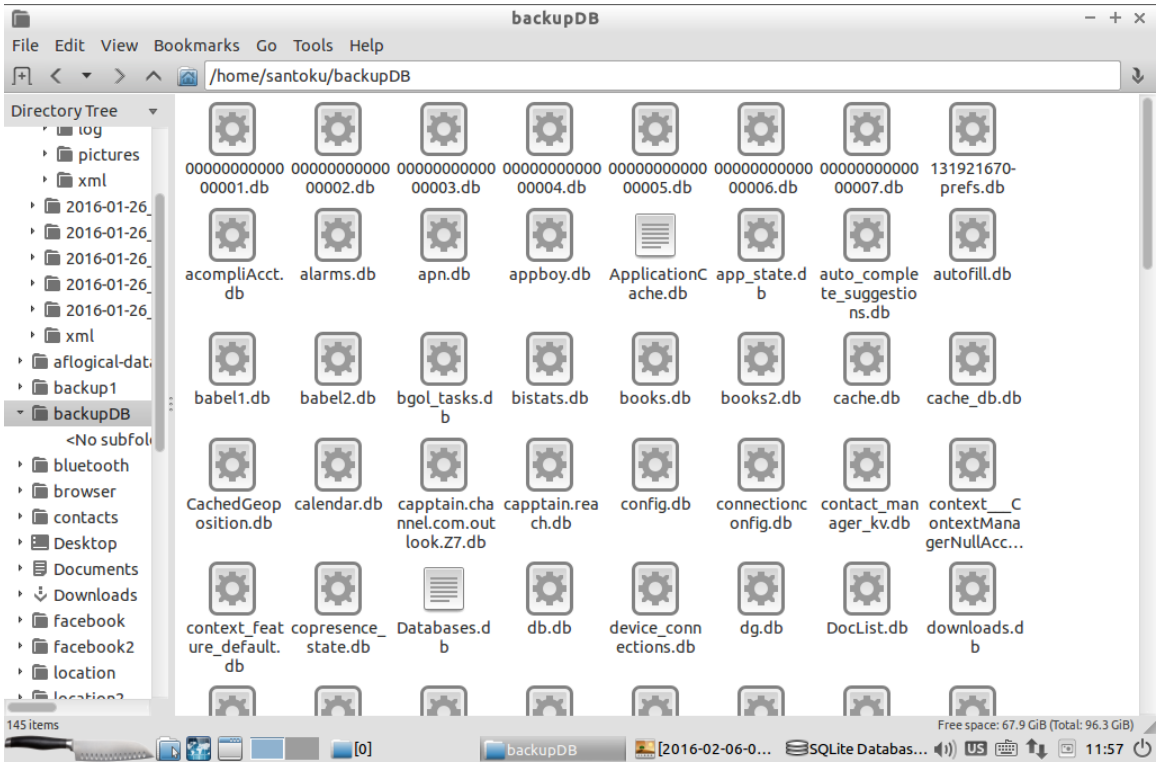
Η διαδικασία εξερεύνησης και απόκτησης των συγκεκριμένων πληροφοριών απαιτεί μεθοδική προσέγγιση και επαναλαμβανόμενες χειροκίνητες ενέργειες. Για την συντόμευση ωστόσο της διαδικασίας και για την διασφάλιση ενός πιο οργανωμένου αποτελέσματος προτείνεται η παρακάτω μεθοδολογία που δημιουργεί έναν φάκελο *backupdb* στην μονάδα αποθήκευσης (sdcard) αναζητά όλα τα αρχεία με κατάληξη .db τα αντιγράφει, στην συνέχεια τα αποθηκεύει και τέλος τα στέλνει με την χρήση της λειτουργίας adb pull στον υπολογιστή του αναλυτή.





Το αποτέλεσμα της παραπάνω διαδικασίας είναι η δημιουργία ενός φακέλου με όνομα *backupDB* στο μονοπάτι */home/santoku* και περιέχει το σύνολο των αρχείων .db που υπάρχουν αποθηκευμένα στην μνήμη του κινητού τηλεφώνου και συγκεκριμένα στην διεύθυνση *data/data*.

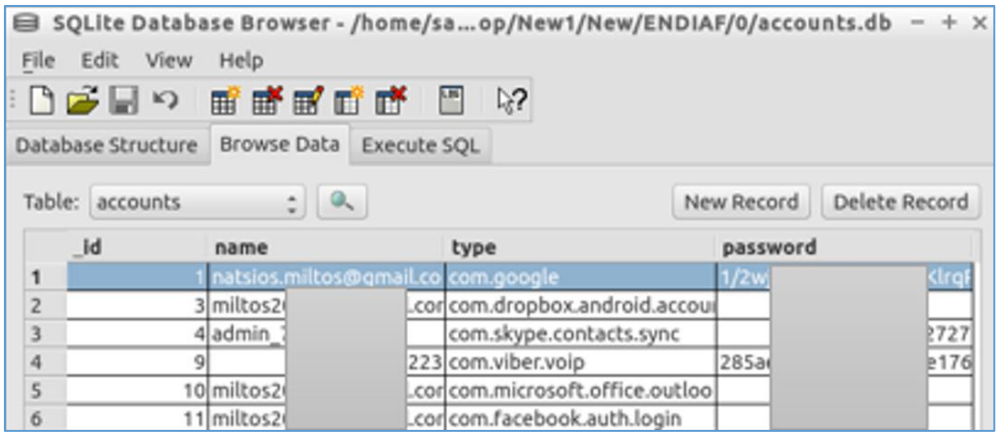




Από τα αρχεία που αποκτήθηκαν, αρκετά είναι αυτά που παρουσιάζουν ενδιαφέρον σχετικά με τις πληροφορίες που περιλαμβάνουν.

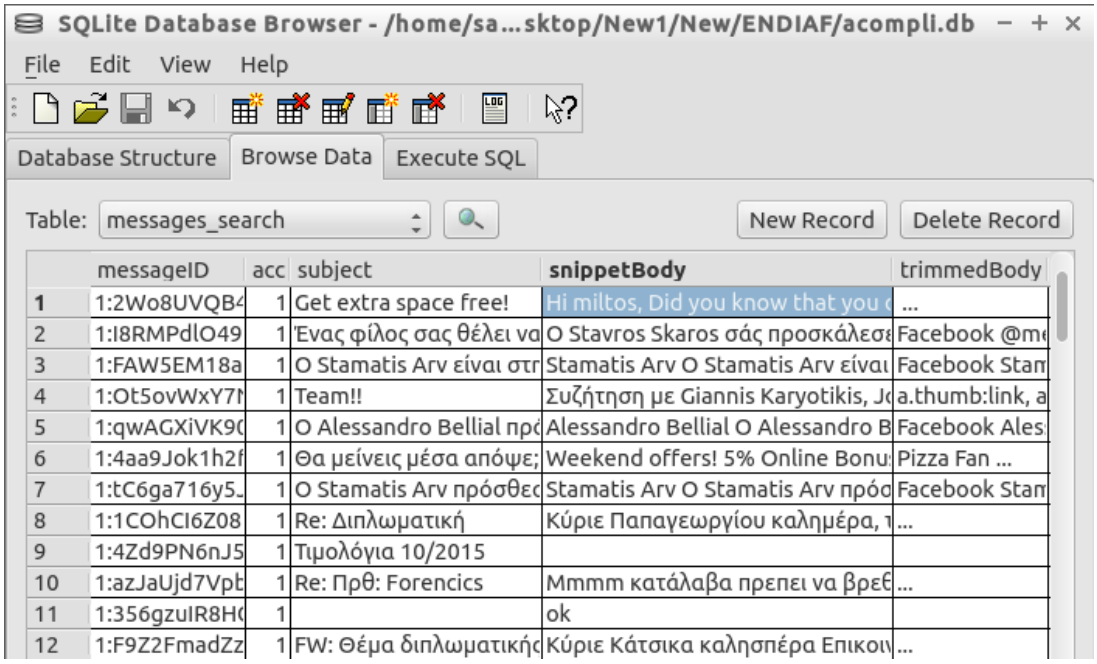
Accounts.db

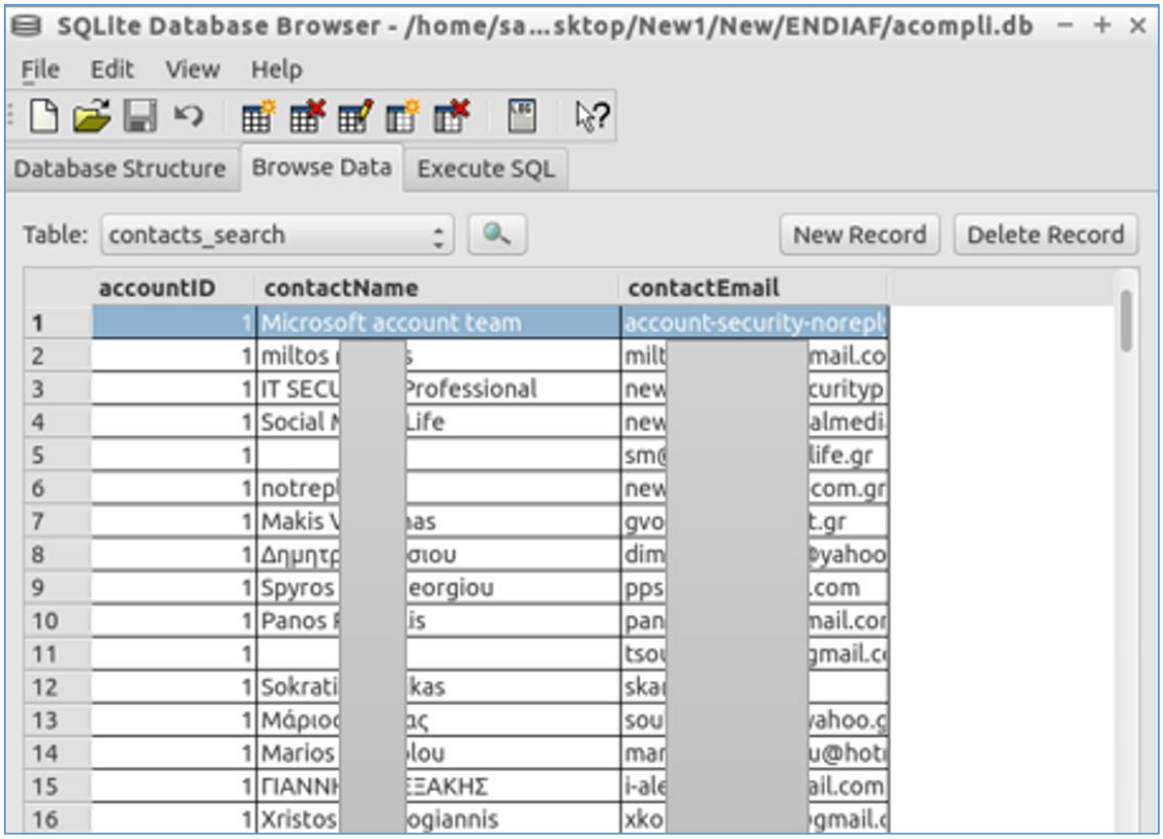
Περιλαμβάνει πληροφορίες σχετικά με τους λογαριασμούς που είναι αποθηκευμένοι στην συσκευή.

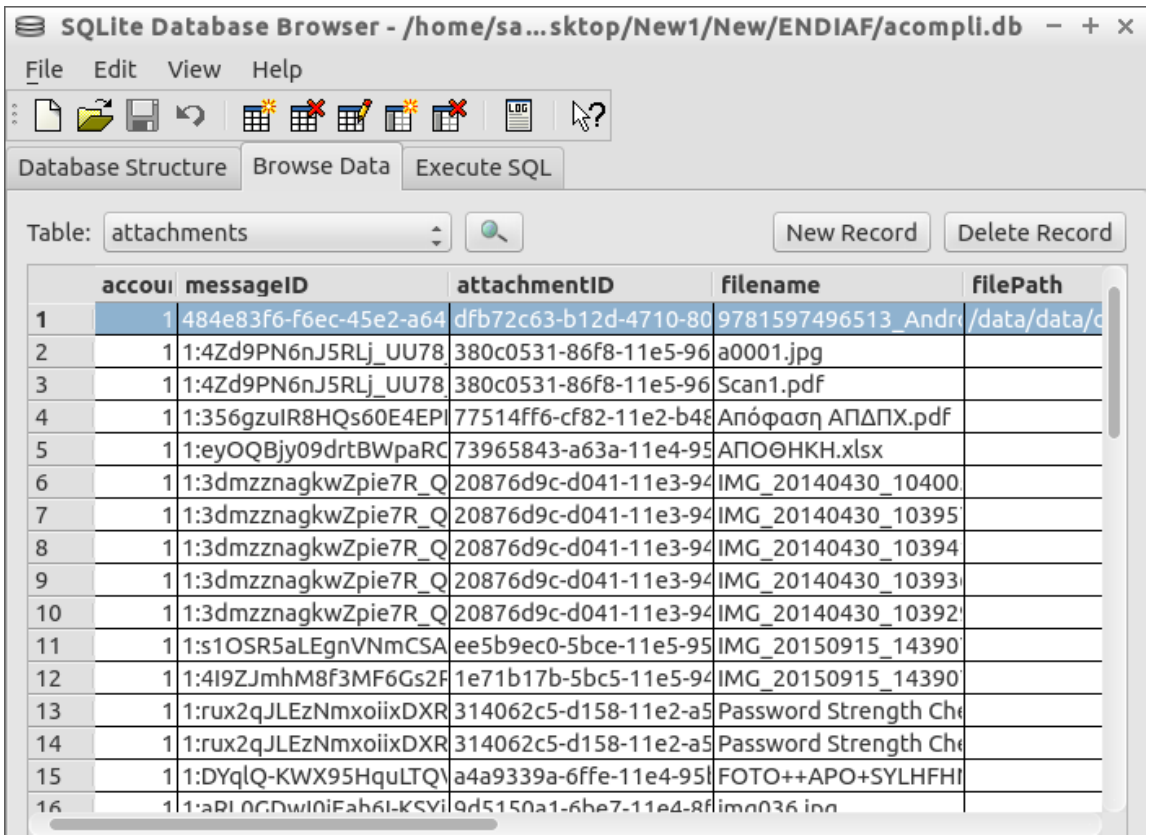


Accompli.db

Περιλαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου, τους λογαριασμούς άλλων χρηστών που επικοινώνησαν, τα αρχεία που εστάλησαν και το όνομα τους, καθώς και την ημ/νια που πραγματοποιήθηκε η κάθε ενέργεια.

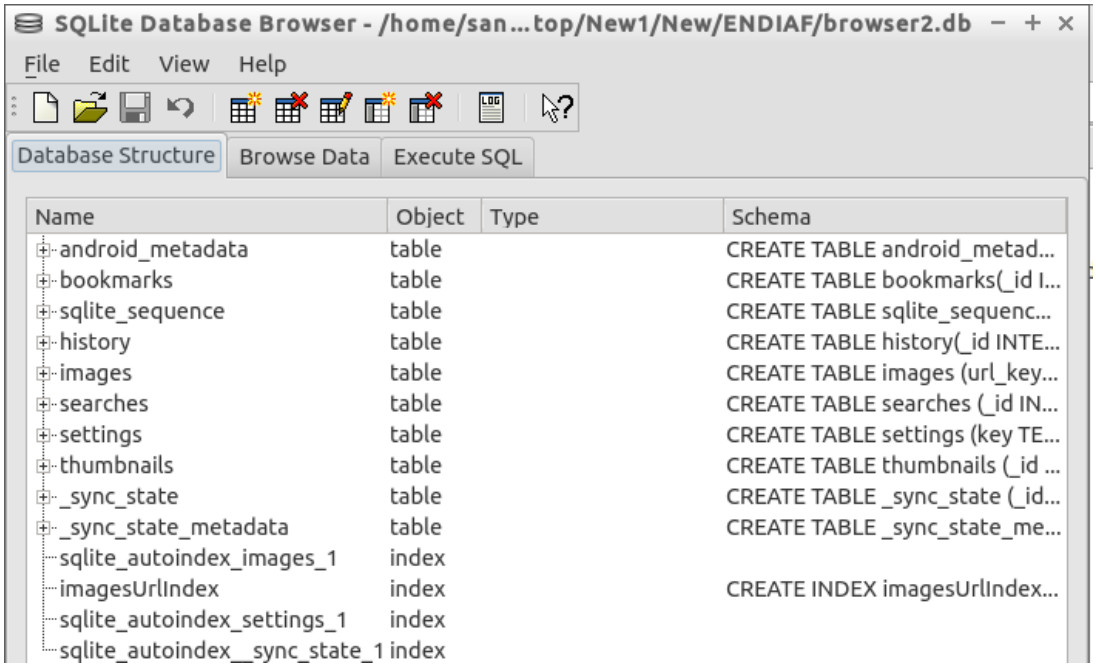


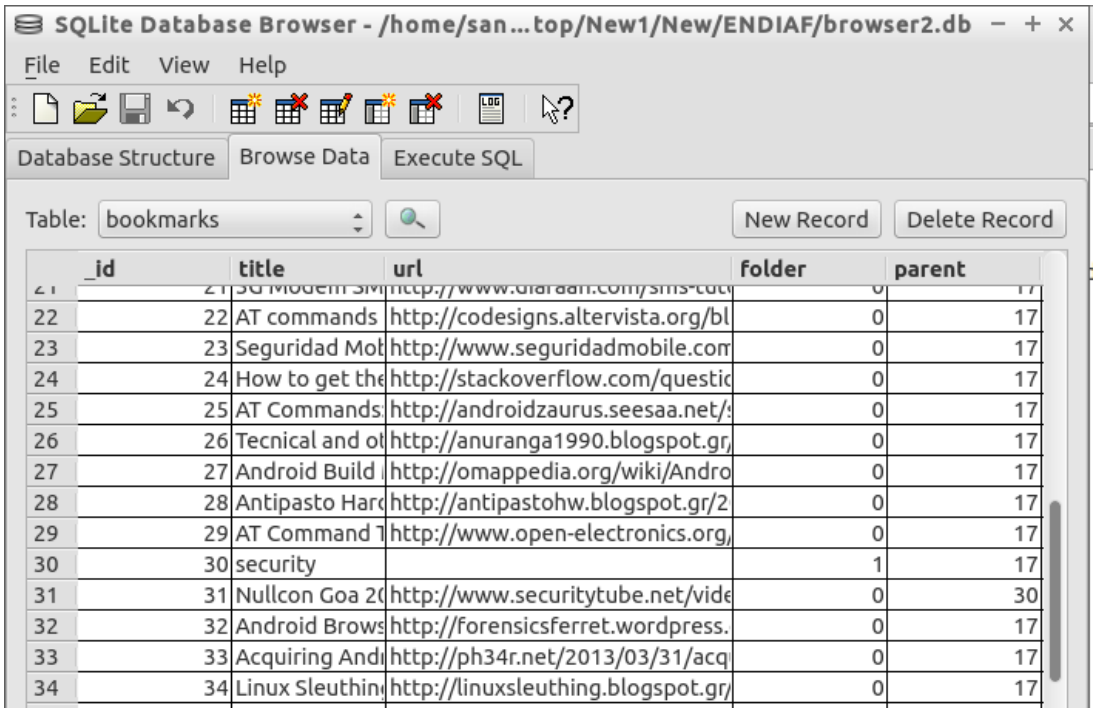

SQLite Database Browser - /home/sa...sktop/New1/New/ENDIAF/acompli.db
File Edit View Help
Database Structure Browse Data Execute SQL
Table: contacts_search
New Record Delete Record
accountID contactName contactEmail
1 1 Microsoft account team account-security-norepl
2 1 miltos mail.co
3 1 IT SECU Professional curityp
4 1 Social Life almedi
5 1 life.gr
6 1 notrepl com.gr
7 1 Makis V t.gr
8 1 Δημητρ yahoo
9 1 Spyros .com
10 1 Panos nail.cor
11 1 gmail.c
12 1 Sokrati kas
13 1 Μάριος vahoo.g
14 1 Marios u@hot
15 1 ΓΙΑΝΝΗ ΞΑΚΗΣ ail.com
16 1 Xristos ogiannis gmail.c

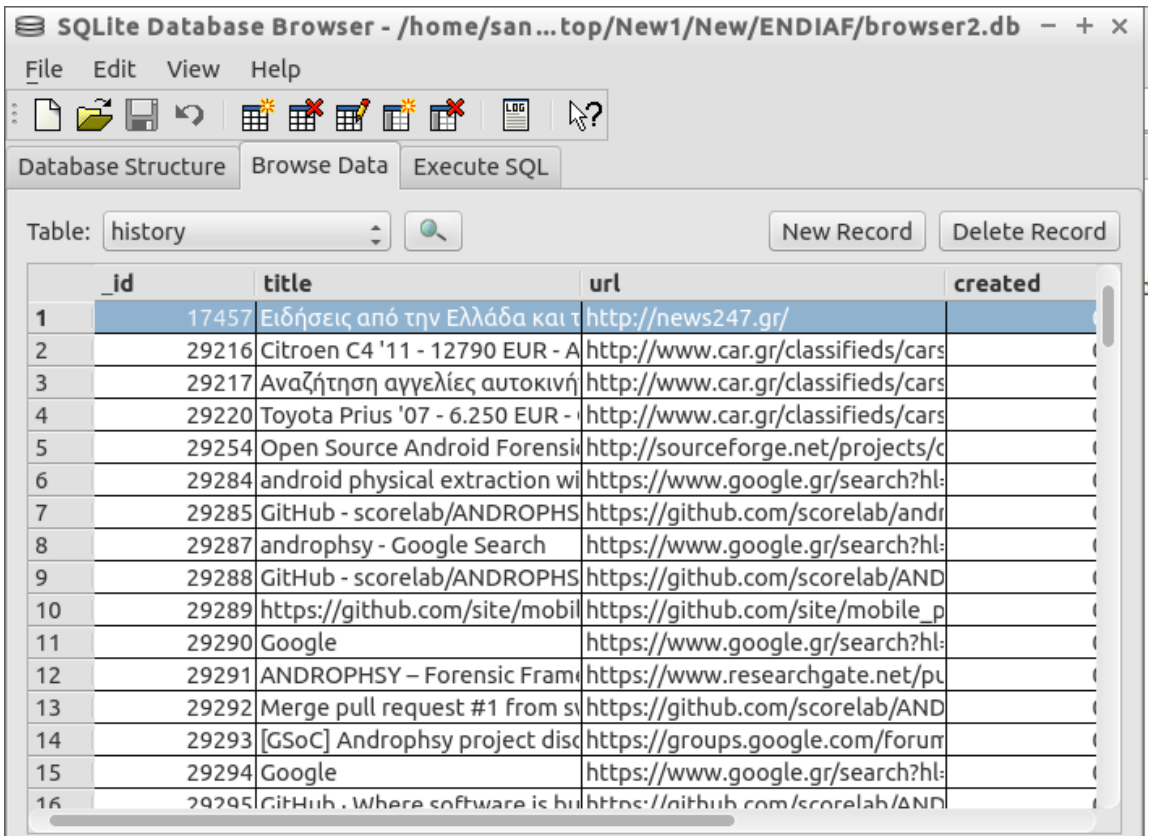

SQLite Database Browser - /home/sa...sktop/New1/New/ENDIAF/acompli.db
File Edit View Help
Database Structure Browse Data Execute SQL
Table: attachments
New Record Delete Record
accou messageID attachmentID filename filePath
1 1 484e83f6-f6ec-45e2-a64 dfb72c63-b12d-4710-80 9781597496513_Andr /data/data/c
2 1 1:4Zd9PN6nJ5RLj_UU78 380c0531-86f8-11e5-96 a0001.jpg
3 1 1:4Zd9PN6nJ5RLj_UU78 380c0531-86f8-11e5-96 Scan1.pdf
4 1 1:356gzuIR8HQs60E4EPI 77514ff6-cf82-11e2-b48 Απόφαση ΑΠΔΠΧ.pdf
5 1 1:eyOQBjy09drtBWpaRC 73965843-a63a-11e4-95 ΑΠΟΘΗΚΗ.xlsx
6 1 1:3dmzznagkwZpie7R_Q 20876d9c-d041-11e3-94 IMG_20140430_10400
7 1 1:3dmzznagkwZpie7R_Q 20876d9c-d041-11e3-94 IMG_20140430_10395
8 1 1:3dmzznagkwZpie7R_Q 20876d9c-d041-11e3-94 IMG_20140430_10394
9 1 1:3dmzznagkwZpie7R_Q 20876d9c-d041-11e3-94 IMG_20140430_10393
10 1 1:3dmzznagkwZpie7R_Q 20876d9c-d041-11e3-94 IMG_20140430_10392
11 1 1:s1OSR5aLEgnVNmCSA ee5b9ec0-5bce-11e5-95 IMG_20150915_14390
12 1 1:4I9ZJmhM8f3MF6Gs2F 1e71b17b-5bc5-11e5-94 IMG_20150915_14390
13 1 1:rux2qJLEzNmxoiixDXR 314062c5-d158-11e2-a5 Password Strength Che
14 1 1:rux2qJLEzNmxoiixDXR 314062c5-d158-11e2-a5 Password Strength Che
15 1 1:DYqlQ-KWX95HquLTQ\ a4a9339a-6ffe-11e4-95l FOTO++APO+SYLHFHI
16 1 1:aRL0GDwl0iEab6I-KSYi 9d5150a1-6be7-11e4-8f img036.jpg

Browser2.db

Η συγκεκριμένη βάση δεδομένων περιλαμβάνει πληροφορίες σχετικά με την πλοήγηση του χρήστη στο διαδίκτυο. Πιο συγκεκριμένα παρουσιάζονται τα αποθηκευμένα bookmarks, οι αναζητήσεις που έχει κάνει, το ιστορικό χρήσης του φυλλομετρητή και οι ημερομηνίες κάθε ενέργειας.

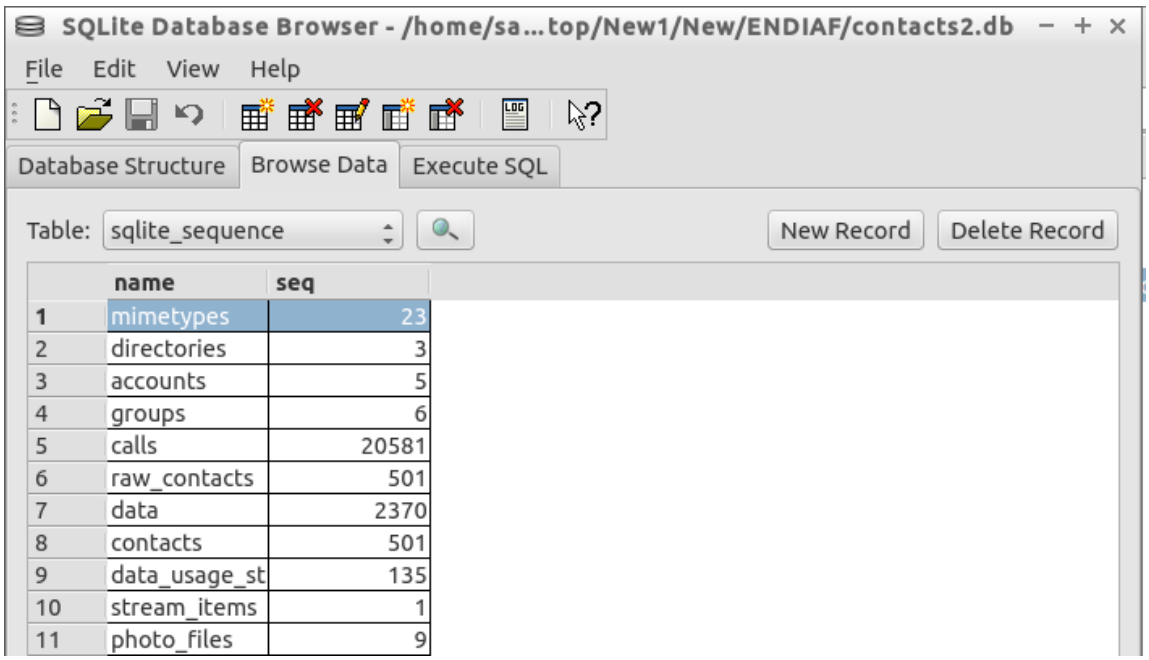






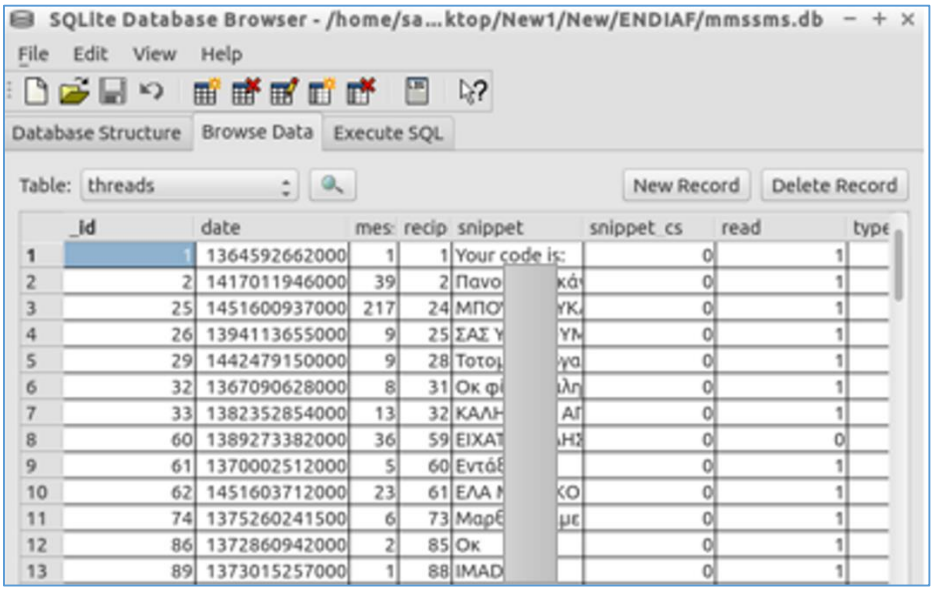
Contacts2.db

Η βάση αυτή παρέχει πληροφορίες σχετικά με τις επαφές του χρήστη, όπως ονόματα και κλήσεις που έχουν πραγματοποιηθεί.



Mmssms.db

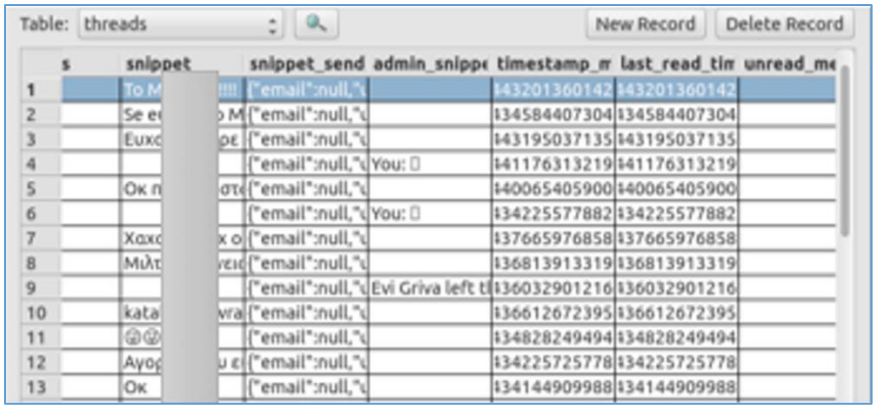
Το αρχείο αυτό αποτελεί σημαντική πηγή δεδομένων καθώς περιλαμβάνει το σύνολο των γραπτών μηνυμάτων που βρίσκονται αποθηκευμένα στην μνήμη της συσκευής, την ημερομηνία που εστάλησαν καθώς και πληροφορίες που αποκαλύπτουν αν αυτά αναγνώστηκαν ή όχι.



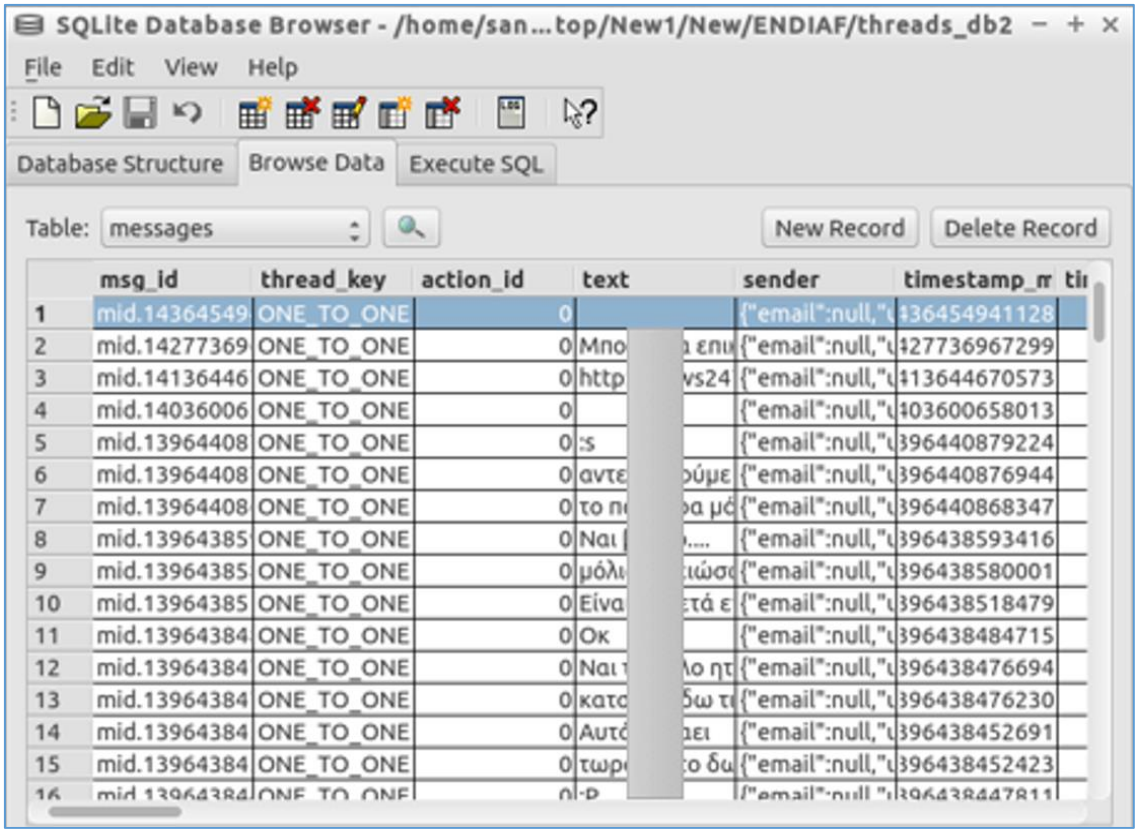
	_id	date	mes	recip	snippet	snippet_cs	read	type
1	1	1364592662000	1	1	Your code is:	0	1	
2	2	1417011946000	39	2	Πανο	0	1	
3	25	1451600937000	217	24	ΜΠΟ	0	1	
4	26	1394113655000	9	25	ΣΑΣ Υ	0	1	
5	29	1442479150000	9	28	Τοτο	0	1	
6	32	1367090628000	8	31	Οκ φ	0	1	
7	33	1382352854000	13	32	ΚΑΛΗ	0	1	
8	60	1389273382000	36	59	ΕΙΧΑΤ	0	0	
9	61	1370002512000	5	60	Εντάξ	0	1	
10	62	1451603712000	23	61	ΕΛΑ Ν	0	1	
11	74	1375260241500	6	73	Μαρξ	0	1	
12	86	1372860942000	2	85	Οκ	0	1	
13	89	1373015257000	1	88	IMAD	0	1	

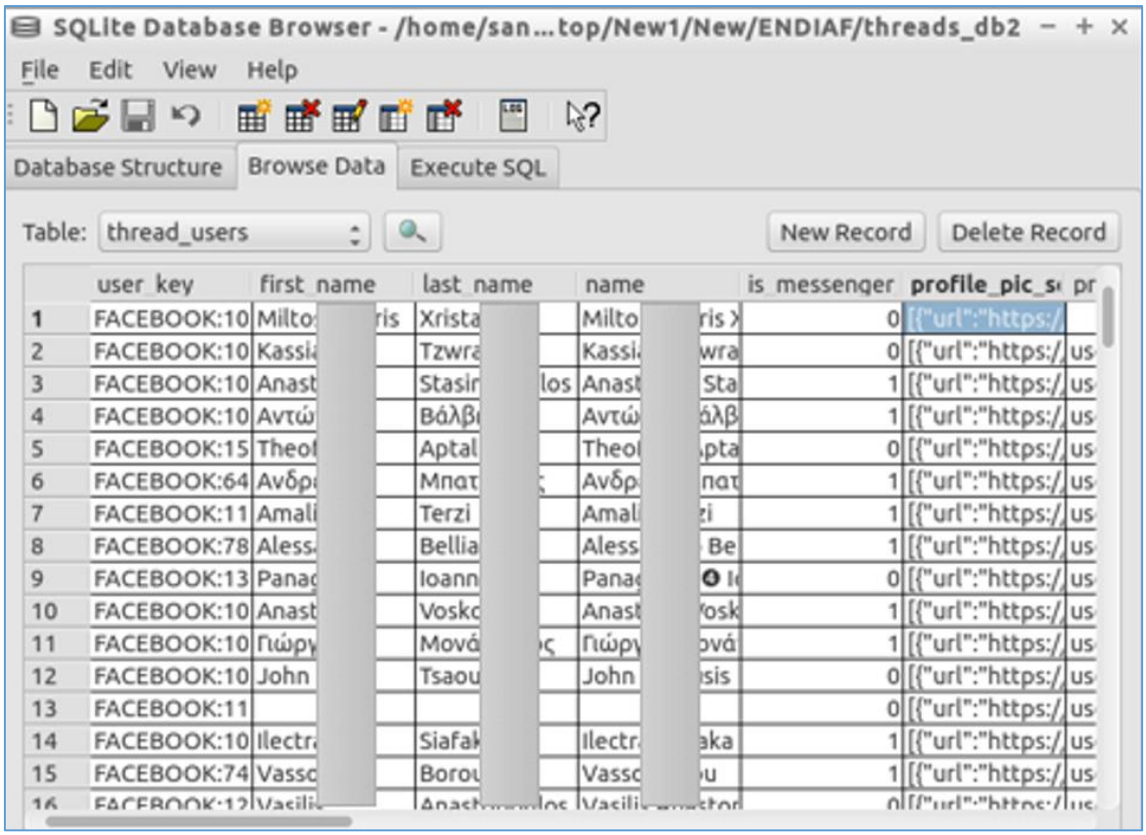
Threads_db2

Η συγκεκριμένη βάση δεδομένων αποκτήθηκε από την εφαρμογή του μέσου κοινωνικής δικτύωσης Facebook που είναι εγκατεστημένη στο smartphone. Παρουσιάζει τα ονόματα των φίλων, τα άμεσα μηνύματα που έχουν ανταλλαχθεί εκατέρωθεν, τα μηνύματα του λογαριασμού καθώς και σχόλια χρηστών και φωτογραφίες από τα προφίλ τους.



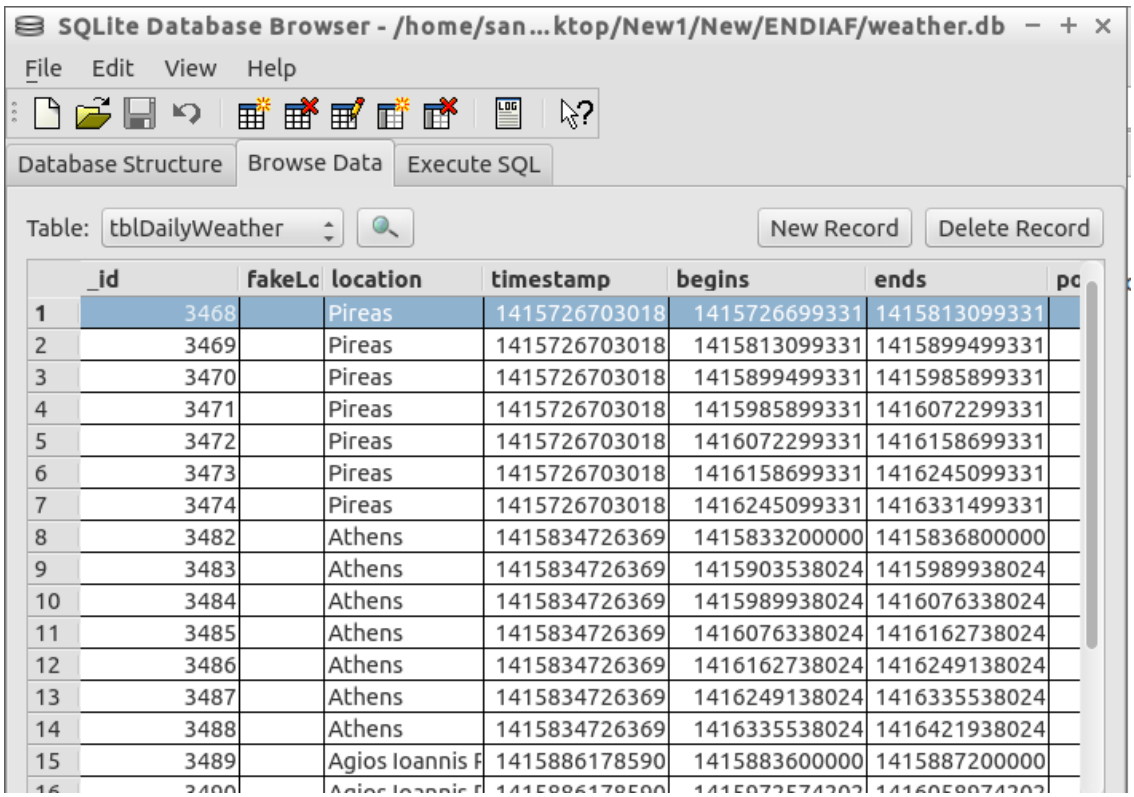
	s	snippet	snippet_send	admin_snippe	timestamp_m	last_read_tim	unread_me
1		To M	{"email":null,"u		143201360142	143201360142	
2		Se e	{"email":null,"u		134584407304	134584407304	
3		Ευχο	{"email":null,"u		143195037135	143195037135	
4			{"email":null,"u	You:	141176313219	141176313219	
5		Οκ π	{"email":null,"u		140065405900	140065405900	
6			{"email":null,"u	You:	134225577882	134225577882	
7		Χαχο	{"email":null,"u		137665976858	137665976858	
8		Μιλτ	{"email":null,"u		136813913319	136813913319	
9			{"email":null,"u	Evi Griva left t	136032901216	136032901216	
10		kata	{"email":null,"u		136612672395	136612672395	
11			{"email":null,"u		134828249494	134828249494	
12		Αγορ	{"email":null,"u		134225725778	134225725778	
13		Οκ	{"email":null,"u		134144909988	134144909988	


SQLite Database Browser - /home/san...top/New1/New/ENDIAF/threads_db2
File Edit View Help
Database Structure Browse Data Execute SQL
Table: messages
New Record Delete Record
msg_id thread_key action_id text sender timestamp_m ti
1 mid.14364549 ONE_TO_ONE 0 {"email":null,"u 1436454941128
2 mid.14277369 ONE_TO_ONE 0 Μπο {"email":null,"u 1427736967299
3 mid.14136446 ONE_TO_ONE 0 http vs24 {"email":null,"u 1413644670573
4 mid.14036006 ONE_TO_ONE 0 {"email":null,"u 1403600658013
5 mid.13964408 ONE_TO_ONE 0 :s {"email":null,"u 1396440879224
6 mid.13964408 ONE_TO_ONE 0 αντε ούμε {"email":null,"u 1396440876944
7 mid.13964408 ONE_TO_ONE 0 το π α μό {"email":null,"u 1396440868347
8 mid.13964385 ONE_TO_ONE 0 Ναι .... {"email":null,"u 1396438593416
9 mid.13964385 ONE_TO_ONE 0 μόλι ιώσο {"email":null,"u 1396438580001
10 mid.13964385 ONE_TO_ONE 0 Είνα τά ε {"email":null,"u 1396438518479
11 mid.13964384 ONE_TO_ONE 0 Οκ {"email":null,"u 1396438484715
12 mid.13964384 ONE_TO_ONE 0 Ναι λο ητ {"email":null,"u 1396438476694
13 mid.13964384 ONE_TO_ONE 0 κατο δω τ {"email":null,"u 1396438476230
14 mid.13964384 ONE_TO_ONE 0 Αυτό ει {"email":null,"u 1396438452691
15 mid.13964384 ONE_TO_ONE 0 τωρ ο δω {"email":null,"u 1396438452423


SQLite Database Browser - /home/san...top/New1/New/ENDIAF/threads_db2
File Edit View Help
Database Structure Browse Data Execute SQL
Table: thread_users
New Record Delete Record
user_key first_name last_name name is_messenger profile_pic_s pr
1 FACEBOOK:10 Milto ris Xrista Milto ris 0 [{"url":"https:/
2 FACEBOOK:10 Kassi Tzwra Kassi wra 0 [{"url":"https:/ us
3 FACEBOOK:10 Anast Stasi los Anast Sta 1 [{"url":"https:/ us
4 FACEBOOK:10 Αντώ Βάλβ Αντώ άλβ 1 [{"url":"https:/ us
5 FACEBOOK:15 Theo Aptal Theo pta 0 [{"url":"https:/ us
6 FACEBOOK:64 Ανδρ Μπατ Ανδρ πατ 1 [{"url":"https:/ us
7 FACEBOOK:11 Amali Terzi Amal zi 1 [{"url":"https:/ us
8 FACEBOOK:78 Aless Bellia Aless Be 1 [{"url":"https:/ us
9 FACEBOOK:13 Panac Ioann Panac 0 [{"url":"https:/ us
10 FACEBOOK:10 Anast Vosk Anast osk 1 [{"url":"https:/ us
11 FACEBOOK:10 Γιώργ Μονά Γιώργ ονά 1 [{"url":"https:/ us
12 FACEBOOK:10 John Tsaou John sis 0 [{"url":"https:/ us
13 FACEBOOK:11 0 [{"url":"https:/ us
14 FACEBOOK:10 Ilectra Siafak Ilectr aka 1 [{"url":"https:/ us
15 FACEBOOK:74 Vasso Borou Vasso u 1 [{"url":"https:/ us

Weather.db

Η συγκεκριμένη βάση προκύπτει από την εφαρμογή καιρού που υπάρχει εγκατεστημένη στο τηλέφωνο. Όσο περίεργη και να φαντάζει η ανάλυση της μπορεί να προσφέρει πληροφορίες που συνδέουν τον χρήστη του smartphone μια συγκεκριμένη χρονική στιγμή με μια καθορισμένη περιοχή.



	_id	fakeLo	location	timestamp	begins	ends	pc
1	3468		Pireas	1415726703018	1415726699331	1415813099331	
2	3469		Pireas	1415726703018	1415813099331	1415899499331	
3	3470		Pireas	1415726703018	1415899499331	1415985899331	
4	3471		Pireas	1415726703018	1415985899331	1416072299331	
5	3472		Pireas	1415726703018	1416072299331	1416158699331	
6	3473		Pireas	1415726703018	1416158699331	1416245099331	
7	3474		Pireas	1415726703018	1416245099331	1416331499331	
8	3482		Athens	1415834726369	1415833200000	1415836800000	
9	3483		Athens	1415834726369	1415903538024	1415989938024	
10	3484		Athens	1415834726369	1415989938024	1416076338024	
11	3485		Athens	1415834726369	1416076338024	1416162738024	
12	3486		Athens	1415834726369	1416162738024	1416249138024	
13	3487		Athens	1415834726369	1416249138024	1416335538024	
14	3488		Athens	1415834726369	1416335538024	1416421938024	
15	3489		Agios Ioannis F	1415886178590	1415883600000	1415887200000	

Btopp.db

Πρόκειται για την βάση δεδομένων που υπάρχει στον φάκελο Bluetooth της συσκευής και περιλαμβάνει πληροφορίες για τα αρχεία που έχουν μοιραστεί μέσω της λειτουργίας αυτής. Πιο συγκεκριμένα παρουσιάζει τη mac address αποστολέα και παραλήπτη, το όνομα, το είδος του αρχείου και την ημερομηνία που πραγματοποιήθηκε η συναλλαγή.

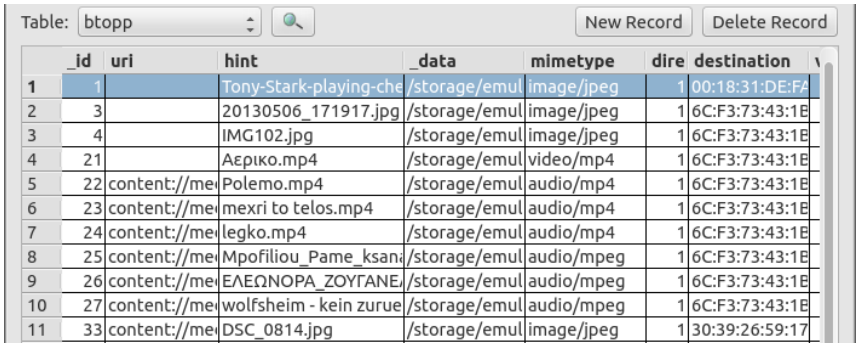


Table: btopp

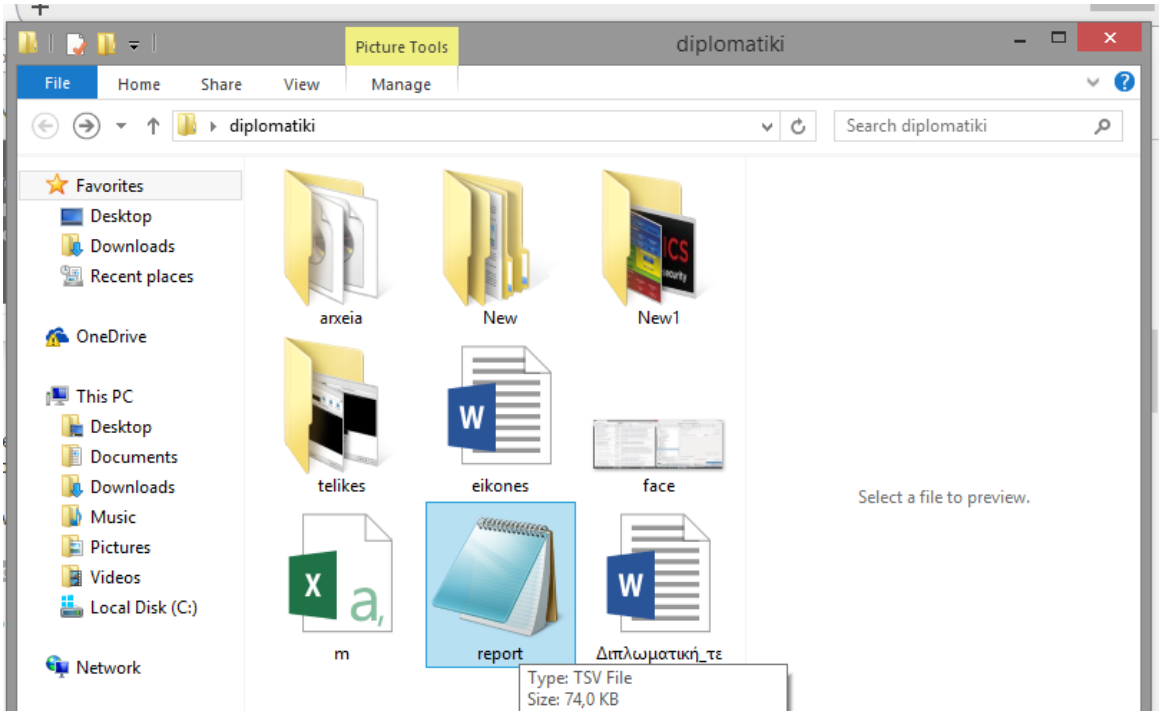
New Record | Delete Record

	_id	uri	hint	_data	mimetype	dire	destination
1	1		Tony-Stark-playing-che	/storage/emul	image/jpeg	1	00:18:31:DE:FA
2	3		20130506_171917.jpg	/storage/emul	image/jpeg	1	6C:F3:73:43:1E
3	4		IMG102.jpg	/storage/emul	image/jpeg	1	6C:F3:73:43:1E
4	21		Αερικο.mp4	/storage/emul	video/mp4	1	6C:F3:73:43:1E
5	22	content://me	Polemo.mp4	/storage/emul	audio/mp4	1	6C:F3:73:43:1E
6	23	content://me	mexri to telos.mp4	/storage/emul	audio/mp4	1	6C:F3:73:43:1E
7	24	content://me	legko.mp4	/storage/emul	audio/mp4	1	6C:F3:73:43:1E
8	25	content://me	Mpofiliou_Pame_ksan	/storage/emul	audio/mpeg	1	6C:F3:73:43:1E
9	26	content://me	ΕΛΕΩΝΟΡΑ_ΖΟΥΓΑΝΕ	/storage/emul	audio/mpeg	1	6C:F3:73:43:1E
10	27	content://me	wolfsheim - kein zurue	/storage/emul	audio/mpeg	1	6C:F3:73:43:1E
11	33	content://me	DSC_0814.jpg	/storage/emul	image/jpeg	1	30:39:26:59:17

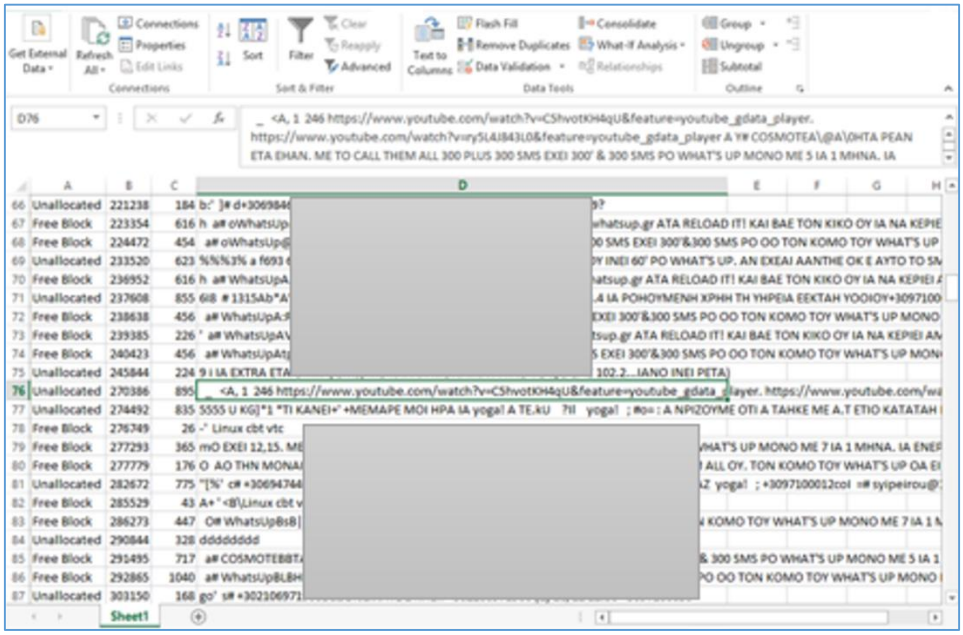
Συνοψίζοντας την συγκεκριμένη τεχνική μη αυτοματοποιημένης απόκτησης δεδομένων (manual acquisition) σημαντικό θεωρείται να αναφερθούν δύο ακόμη δυνατότητες που παρέχονται στον ερευνητή. Η πρώτη αναφέρεται στην εξαγωγή διεγραμμένων πληροφοριών που υπάρχουν ακόμη αποθηκευμένες στις βάσεις δεδομένων που αποκτήθηκαν και η δεύτερη στην ανακάλυψη αρχείων που συγκρατούν κωδικούς και στοιχεία χρήσιμα για την έρευνα, σε μορφή μη κρυπτογραφημένη.

Η python όπως είναι κοινά γνωστό αναφέρεται ως μια από τις ισχυρότερες γλώσσες προγραμματισμού για την δημιουργία μικρών και ευέλικτων εφαρμογών για την εκπλήρωση συγκεκριμένων διεργασιών. Για τον λόγο λοιπόν αυτό, χρησιμοποιείται και για την ανακάλυψη διεγραμμένων πληροφοριών από βάσεις δεδομένων. Η υλοποίηση sqlparse.py στοχεύει στην προσπέλαση ενός αρχείου βάσης και εν συνεχεία στην παρουσίαση στοιχείων που περιέχονται είτε σε unallocated space είτε σε free blocks. Χρησιμοποιώντας το αρχείο βάσης μηνυμάτων που αποκτήθηκε προηγούμενα, ως είσοδο στο συγκεκριμένο πρόγραμμα, παράγεται στην έξοδο ένα αρχείο .tsv, το οποίο παρουσιάζει όλες τις απαραίτητες πληροφορίες.

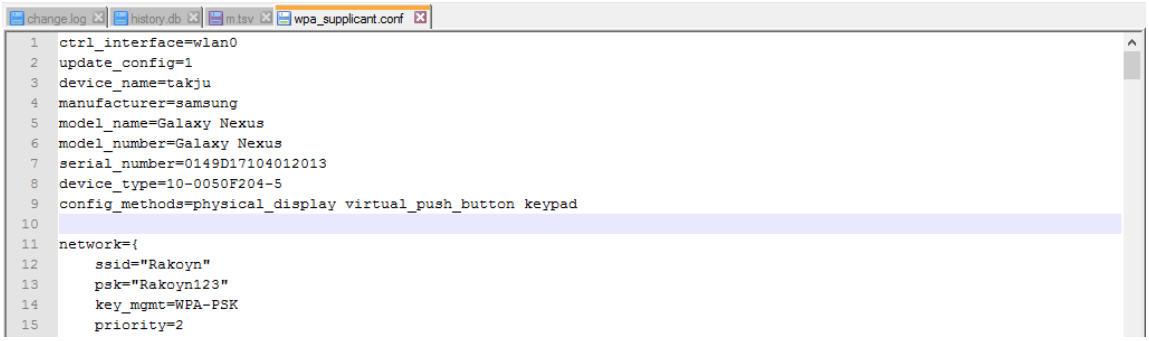
sqlparse.py -f mmssms.db -r -o report.txt

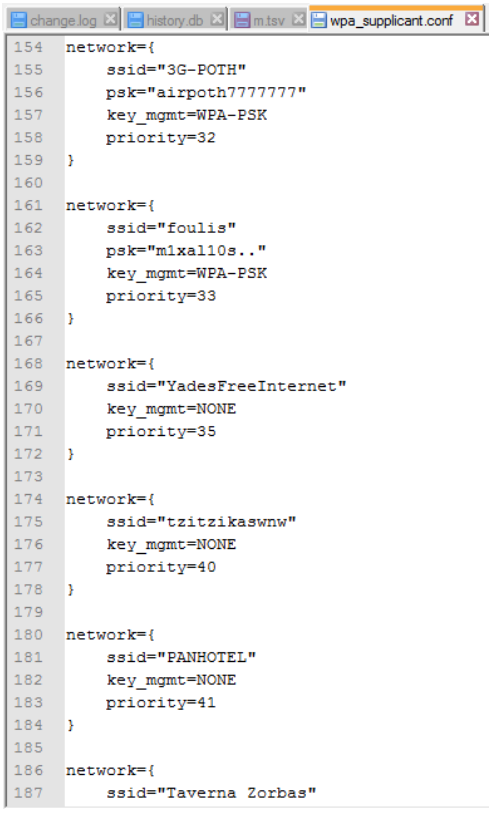


Το report που παρήχθη πράγματι περιλαμβάνει έναν αρκετά ικανοποιητικό αριθμό διεγραμμένων μηνυμάτων όμως λόγω των ελληνικών χαρακτήρων η παρουσίαση και ανάγνωσή τους είναι κάπως δύσκολη. Με τους λατινικούς χαρακτήρες ωστόσο και με το κατάλληλο encoding τα αποτελέσματα είναι πιο ευανάγνωστα. Για παράδειγμα στο block 270386 εμφανίζεται ένα διεγραμμένο μήνυμα του 2013 και περιλαμβάνει ένα ενδιαφέρον βίντεο από το YouTube.



Μια ακόμη ενδιαφέρουσα ανακάλυψη που προέκυψε από την χειροκίνητη διαδικασία απόκτησης δεδομένων ήταν ο εντοπισμός κωδικών ασύρματων δικτύων που έχει χρησιμοποιήσει η έξυπνη κινητή συσκευή. Πιο συγκεκριμένα στο μονοπάτι ***misc/wifi/*** στο filesystem της, εμφανίζεται ένα αρχείο με ονομασία wpa_supplicant.conf και περιέχει το σύνολο των ασύρματων δικτύων καθώς και τους κωδικούς πρόσβασης στο καθένα από αυτά.



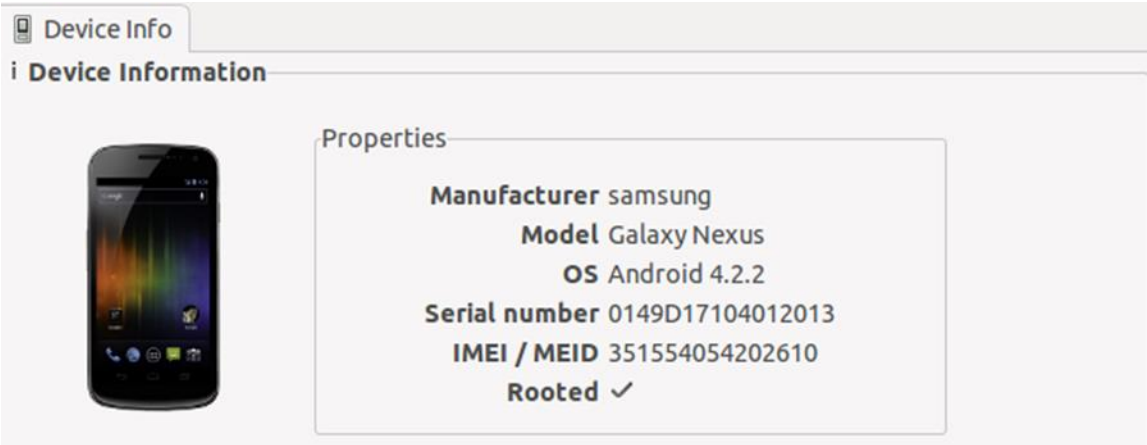


15. Physical acquisition

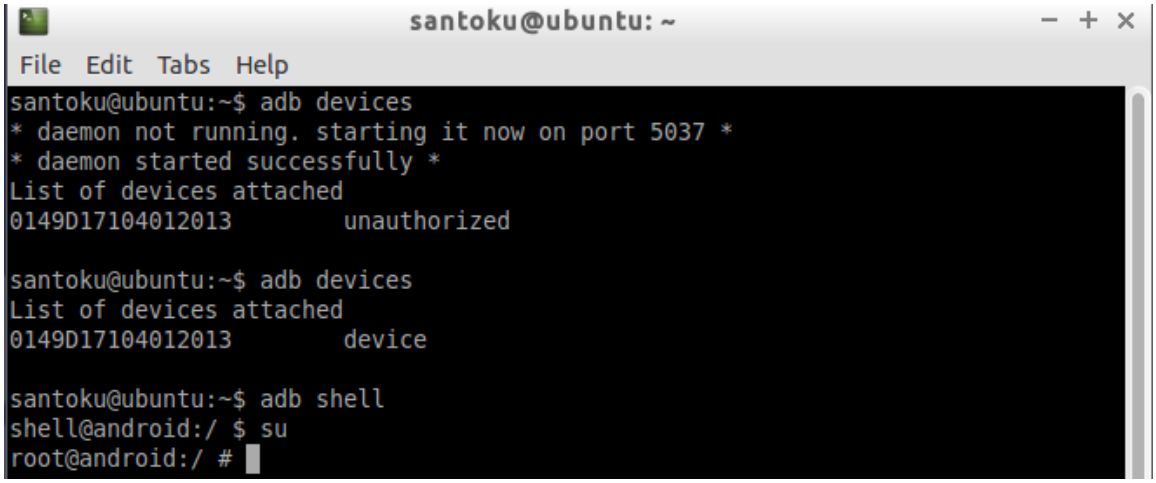
Στον κλάδο της εγκληματολογικής έρευνας ηλεκτρονικών μέσων, η τεχνική της φυσικής απόκτησης δεδομένων αναφέρεται στην δημιουργία και εξαγωγή ενός ιδανικού αντίγραφου, του συνόλου της μνήμης μιας συσκευής. Αυτό σημαίνει πως κάθε κομμάτι δεδομένων που περιέχεται, ακόμα και αρχεία που έχουν απομακρυνθεί από αυτή, ανακτώνται και είναι διαθέσιμα για εξέταση. Η ίδια λογική ακολουθείται και στην περίπτωση των έξυπνων κινητών συσκευών πράγμα το οποίο σημαίνει πως μοναδικός περιορισμός ενός ερευνητή είναι η δυνατότητα του, να ξεχωρίσει από το σύνολο, τις πληροφορίες που του είναι απαραίτητες για την στοιχειοθέτηση μιας υπόθεσης.

Η διαδικασία που ακολουθεί στην συνέχεια παρουσιάζει αναλυτικά την μεθοδολογία που χρησιμοποιείται για την επίτευξη του στόχου της δημιουργίας και εξέτασης ενός bit-by-bit image της συσκευής.

Το περιβάλλον εργασίας παραμένει το ίδιο με αυτό που αναφέρθηκε στο κεφάλαιο logical acquisition και αποτελείται από έναν ηλεκτρονικό υπολογιστή με λειτουργικό Windows 8, ένα εικονικό μηχάνημα Santoku Linux με τις απαραίτητες εφαρμογές προεγκατεστημένες και ένα Smartphone Samsung με λειτουργικό Android 4.2.2.

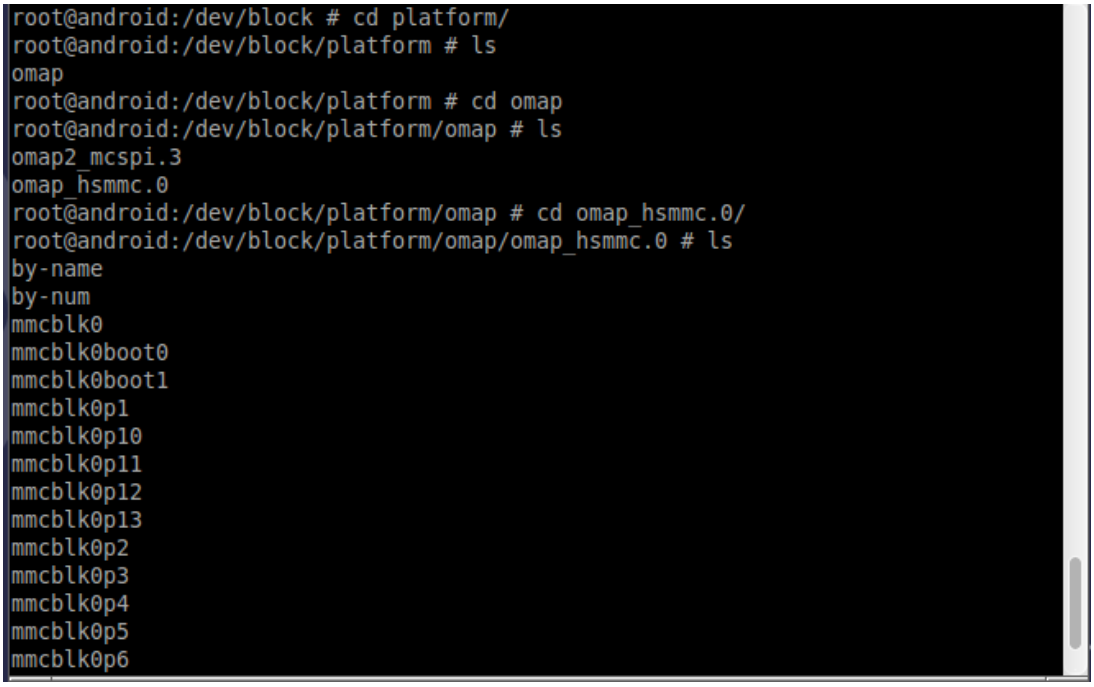


Αρχικός στόχος αποτελεί η διερεύνηση του filesystem της συσκευής και ο εντοπισμός των partitions που διαθέτει. Για τον λόγο αυτό η χρήση του adb με αυξημένα δικαιώματα χρήσης, κρίνεται απαραίτητη.



Από την στιγμή που ο ερευνητής έχει root access στο σύνολο του filesystem περιηγείται και προσπελά φακέλους μέχρι να εντοπίσει αυτόν που ονομάζεται /dev/block. Στην συγκεκριμένη διαδρομή, το λειτουργικό Android, συνήθως αποθηκεύει τα partitions χωρίς ωστόσο αυτό να αποτελεί κανόνα, καθώς αυτό μπορεί να διαφέρει από κατασκευαστή σε κατασκευαστή ή από τη μια έκδοση λειτουργικού στην άλλη.

Στο περιβάλλον που εξετάζεται εδώ τα partitions βρίσκονται στο μονοπάτι ***/dev/block/platform/omap/omap_hsmmc.0.***



Στην συνέχεια επιλέγοντας τον φάκελο by-name, εμφανίζονται οι λογικές μονάδες αποθήκευσης με τα ονόματα τους.

```
root@android:/dev/block/platform/omap/omap_hsmmc.0/by-name # ls -l
lrwxrwxrwx root     root              2016-01-25 08:50 boot -> /dev/block/mmcblk0p7
lrwxrwxrwx root     root              2016-01-25 08:50 cache -> /dev/block/mmcblk0p11
lrwxrwxrwx root     root              2016-01-25 08:50 dgs -> /dev/block/mmcblk0p6
lrwxrwxrwx root     root              2016-01-25 08:50 efs -> /dev/block/mmcblk0p3
lrwxrwxrwx root     root              2016-01-25 08:50 metadata -> /dev/block/mmcblk0p13
lrwxrwxrwx root     root              2016-01-25 08:50 misc -> /dev/block/mmcblk0p5
lrwxrwxrwx root     root              2016-01-25 08:50 param -> /dev/block/mmcblk0p4
lrwxrwxrwx root     root              2016-01-25 08:50 radio -> /dev/block/mmcblk0p9
lrwxrwxrwx root     root              2016-01-25 08:50 recovery -> /dev/block/mmcblk0p8
lrwxrwxrwx root     root              2016-01-25 08:50 sbl -> /dev/block/mmcblk0p2
lrwxrwxrwx root     root              2016-01-25 08:50 system -> /dev/block/mmcblk0p10
lrwxrwxrwx root     root              2016-01-25 08:50 userdata -> /dev/block/mmcblk0p12
lrwxrwxrwx root     root              2016-01-25 08:50 xloader -> /dev/block/mmcblk0p1
```

Κάθε ένα από τα partition περιλαμβάνει και διαφορετικά δεδομένα. Το είδος των πληροφοριών που περιέχεται σε κάθε ένα από αυτά, αναφέρεται σε προγενέστερο κεφάλαιο. Για τον σκοπό ωστόσο της απόκτησης σημαντικών πληροφοριών ένας ερευνητής, θα πρέπει να στρέψει αρχικά την προσοχή του σε συγκεκριμένα από αυτά. Πλήθος αξιοποιήσιμων στοιχείων περιέχεται στο /userdata στο /system και στο /cache. Η διαδικασία δημιουργίας ενός image για κάθε ένα από αυτά απαιτεί αρκετή προσοχή ώστε να διασφαλιστεί η ακεραιότητα των δεδομένων, μεθοδική προσέγγιση και ευχέρεια χρόνου καθώς αποδεικνύεται αρκετά χρονοβόρα.

Το συγκεκριμένο Samsung Smartphone που αναλύεται στην συνέχεια, παρουσιάζει ιδιαιτερότητες οι οποίες πρέπει ξεπεραστούν για να επιτευχθεί ο στόχος της απόκτησης των δεδομένων. Η πρώτη εντοπίζεται στην απουσία αφαιρούμενης εξωτερικής κάρτας μνήμης, με αποτέλεσμα οι ενέργειες που πρέπει να γίνουν, να πραγματοποιούνται με πολύ προσοχή, στην εσωτερική μνήμη του τηλεφώνου καθώς τίθενται σε κίνδυνο το σύνολο των στοιχείων με μια άστοχη ενέργεια. Η επόμενη ιδιαιτερότητα αναφέρεται στο πεπερασμένο μέγεθος αυτής της μνήμης και ως εκτούτου στην δυνατότητα να αποθηκευτούν εκεί, τα images που θα παραχθούν.

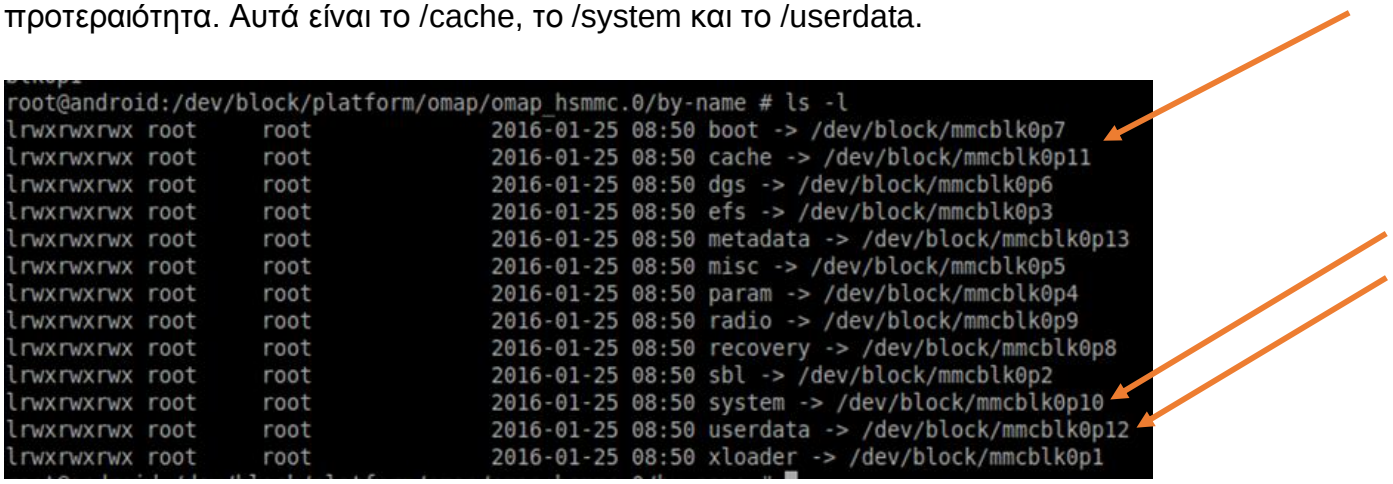
Η διαδικασία που ακολουθεί περιλαμβάνει την δημιουργία ενός φακέλου /images στην εικονική sdcard της συσκευής, την μετατροπή και εξαγωγή των partitions σε αρχεία .img με την βοήθεια της λειτουργίας dd του λειτουργικού linux και τέλος της

εισαγωγή των αρχείων αυτών, στο λογισμικό ανάκτησης και εξέτασης δεδομένων Sleuthkit. Ενώ παράλληλα θα αντιμετωπιστούν και οι παραπάνω ιδιαιτερότητες.

Εφόσον υπάρχει root access στην συσκευή, υπάρχει η δυνατότητα δημιουργίας ενός φακέλου που θα αποθηκευτούν οι εικόνες των partitions. Με την παρακάτω εντολή δημιουργείται ένας φάκελος με όνομα images στο μονοπάτι */sdcard/* .

```
File  Edit  Tabs  Help
255|root@android:/sdcard # mkdir images
root@android:/sdcard # cd images
root@android:/sdcard/images #
```

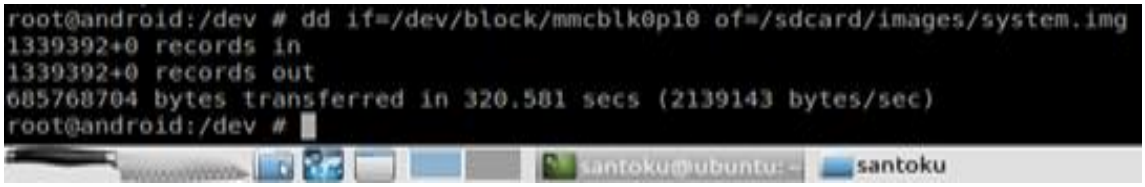
Στην συνέχεια, από το σύνολο των partitions που εμφανίζονται, επιλέγονται αυτά που κρίνονται ως πιο σημαντικά, με αποτέλεσμα να εξετάζονται κατά προτεραιότητα. Αυτά είναι το /cache, το /system και το /userdata.



Η διαδικασία μετατροπής και αντιγραφής των παραπάνω λογικών μονάδων αποθήκευσης γίνεται με την χρήση μιας εξαιρετικά χρήσιμης υλοποίησης που ονομάζεται dd και υπάρχει προεγκατεστημένη στο σύνολο σχεδόν των λειτουργικών που βασίζονται στον πυρήνα Linux. Στην συσκευή που εξετάζεται υπάρχει εγκατεστημένη η εφαρμογή BusyBox που περιλαμβάνει τόσο την συγκεκριμένη λειτουργία όσο και πολλές άλλες.

Η χρήση της συγκεκριμένης υλοποίησης γίνεται ως εξής:
 # dd if=(partition_path) of=(output_path_.img)

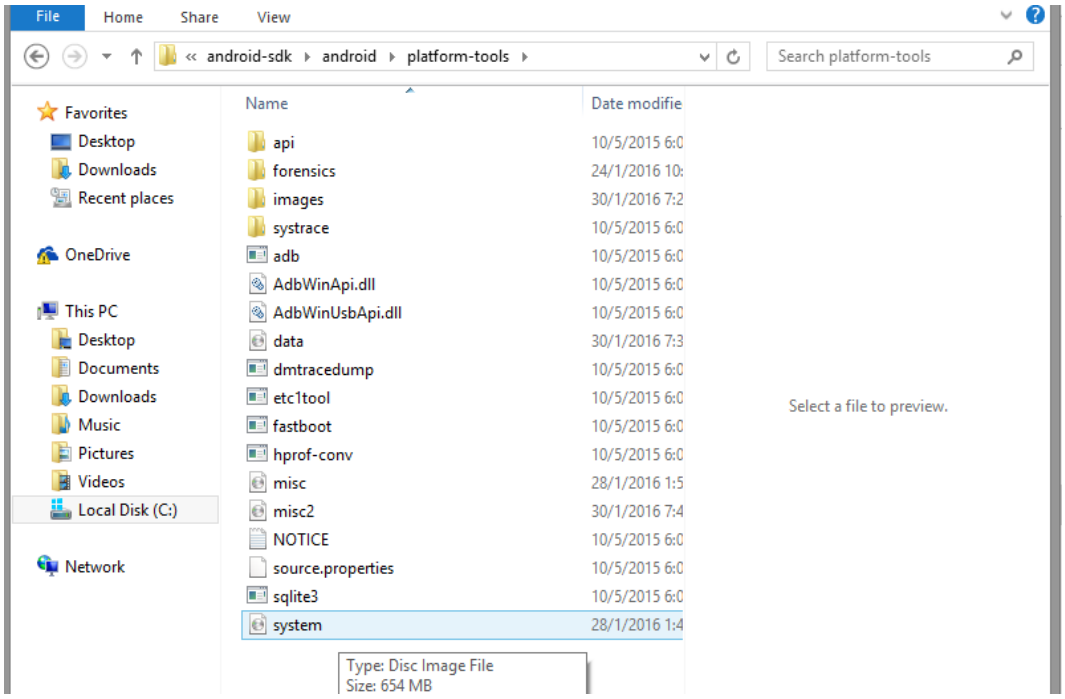
Έτσι λοιπόν για την δημιουργία ενός image του system partition, δίνεται η εντολή **dd if=dev/block/mmcblk0p10 of=/sdcard/images/system.img** αποτέλεσμα της εντολής αυτής είναι η δημιουργία του αρχείου **system.img** και η αποθήκευση του στον φάκελο που δημιουργήθηκε προηγούμενα.

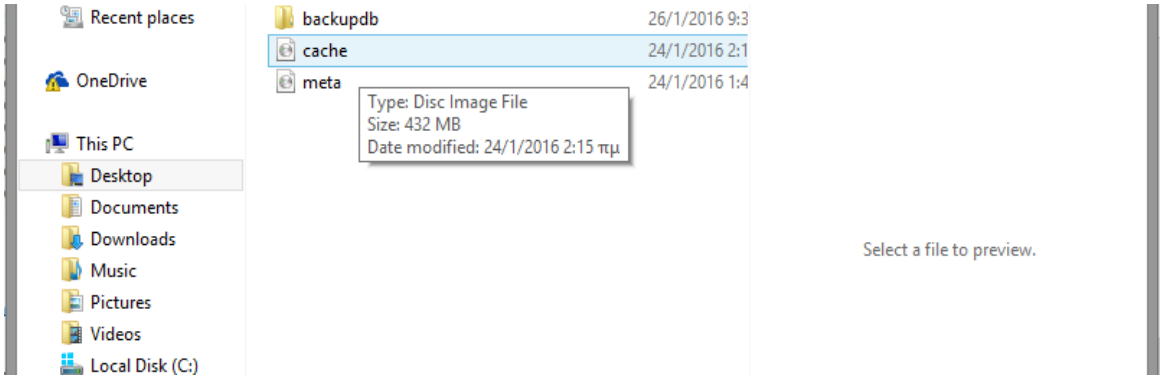


Με τον ίδιο σχεδόν τρόπο δημιουργείται και το αρχείο **cache.img**. Η σύνταξη της εντολής είναι : **dd if=dev/block/mmcblk0p11 of=/sdcard/images/cache.img.**

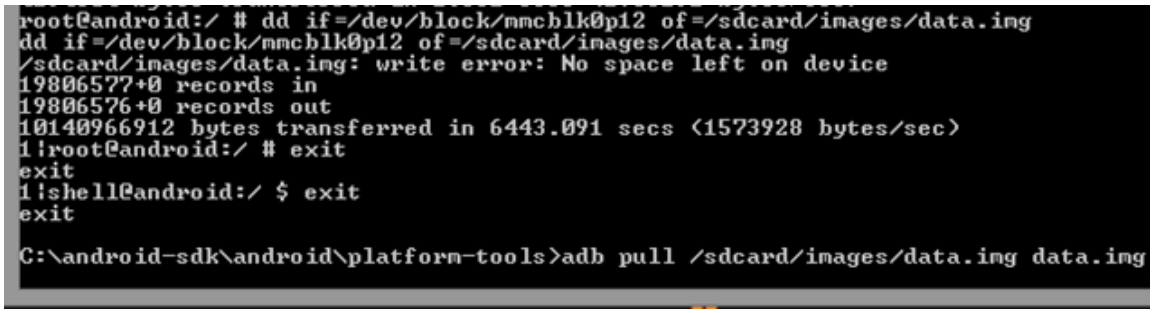
Τα δύο αρχεία με συνολικό μέγεθος 1gb βρίσκονται πλέον αποθηκευμένα στην μνήμη της συσκευής και συγκεκριμένα στον φάκελο με την ονομασία images. Για να εξαχθούν από εκεί και να μεταφερθούν στον υπολογιστή χρησιμοποιείται το εργαλείο adb με την παράμετρο pull σε καινούργιο terminal.

adb pull /sdcard/images/cache.img cache.img
adb pull /sdcard/images/system.img system.img





Στο επόμενο και πιο βασικό partition image, που περιέχει τα δεδομένα του χρήστη, αντιμετωπίζεται η ιδιαιτερότητα του πεπερασμένου χώρου αποθήκευσης που αναφέρθηκε πριν. Προσπαθώντας με την ίδια διαδικασία που δημιουργήθηκαν τα προηγούμενα, να δημιουργηθεί το image του /userdata partition, εμφανίζεται ένα μήνυμα λάθους που αναφέρει πως δεν υπάρχει διαθέσιμος ελεύθερος χώρος στην συσκευή.



Έτσι η διαδικασία σταματά και τα δεδομένα που προκύπτουν από την απόκτηση είναι ελλιπή. Για να αντιμετωπιστεί η δυσκολία αυτή γίνεται χρήση της υλοποίησης Netcat που περιλαμβάνεται και στην εφαρμογή Busybox που είναι ήδη εγκατεστημένη στην συσκευή.

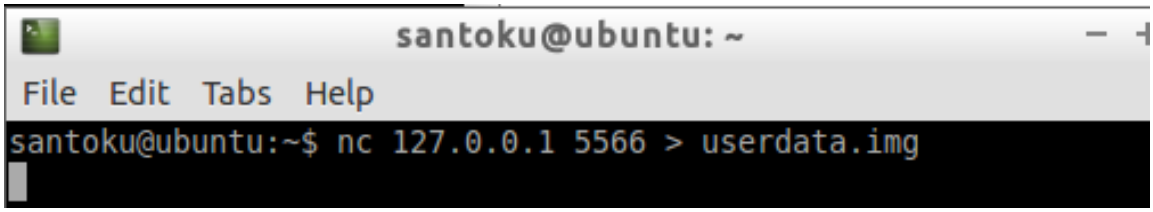
Βήμα πρώτο είναι η προώθηση μιας πόρτας tcp από την συσκευή στον υπολογιστή. Αυτό υλοποιείται με το εργαλείο adb και την παράμετρο forward.

adb forward tcp:5566 tcp:5566

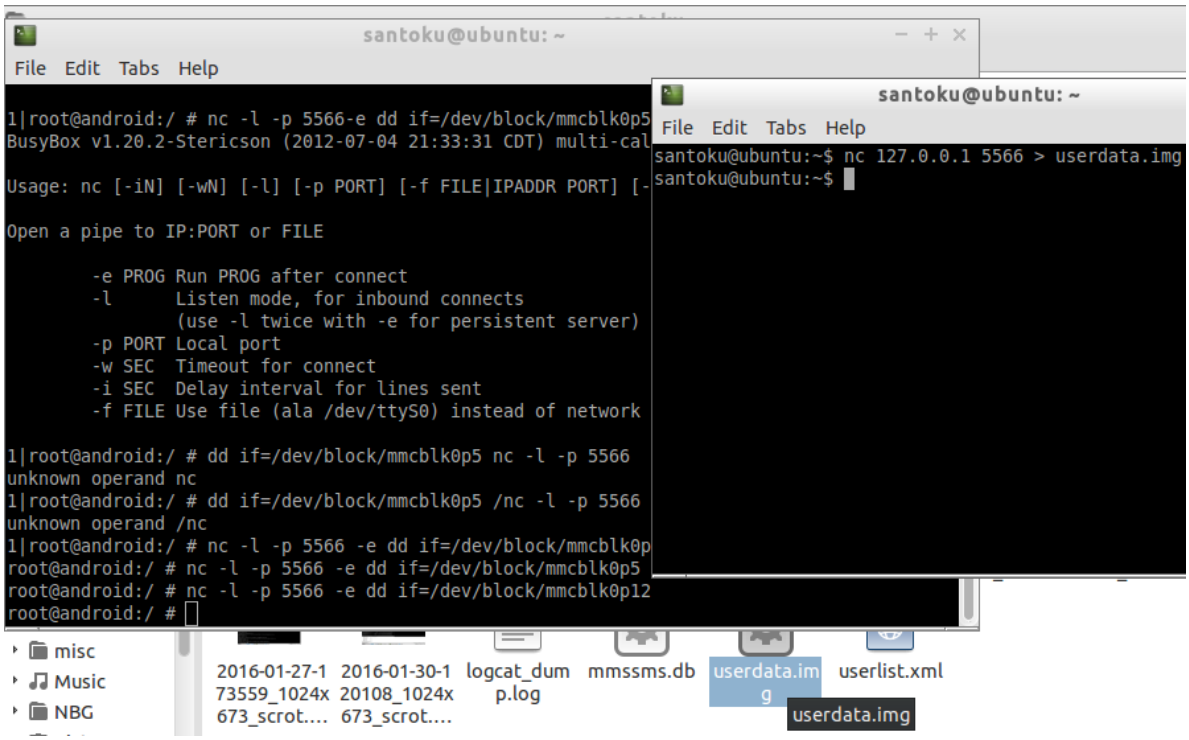
Έπειτα απαιτείται η χρήση της λειτουργίας adb shell ώστε ο ερευνητής να εισέλθει στο περιβάλλον της συσκευής και να χρησιμοποιήσει τις υλοποιήσεις dd και Netcat για να δημιουργήσει το image του /userdata partition και να το μεταφέρει στον υπολογιστή αντίστοιχα.

```
root@android:/ # nc -l -p 5566 -e dd if=/dev/block/mmcblk0p12
```

Παράλληλα και για να ολοκληρωθεί η διαδικασία της μεταφοράς, απαραίτητη είναι και η εκκίνηση της λειτουργίας Netcat στην έκδοση του Santoku Linux που χρησιμοποιείται. Στην εντολή αυτή περιλαμβάνεται η ip της πηγής, η πόρτα επικοινωνίας που έχει ορισθεί καθώς και η ονομασία του αρχείου image που θα προκύψει.



Με την τεχνική αυτή ο ερευνητής αποφεύγει να αποθηκεύσει τις εικόνες των partition που δημιουργεί, στην συσκευή αλλά τις αποθηκεύει κατευθείαν στον ηλεκτρονικό υπολογιστή του, αποφεύγοντας έτσι κάθε πιθανότητα τροποποίησης των δεδομένων της μνήμης λόγω του περιορισμένου χώρου.

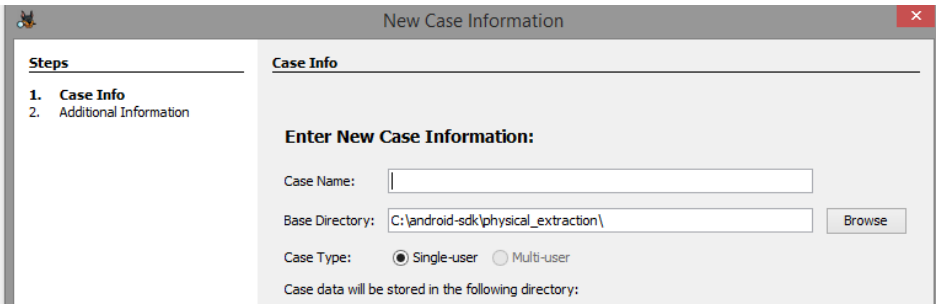


Από την στιγμή που τα δεδομένα των λογικών μονάδων αποθήκευσης που παρουσιάζουν ενδιαφέρον (/userdata,/cache,/system) έχουν αποκτηθεί, το επόμενο βήμα περιλαμβάνει την ανάλυσή τους, με τα κατάλληλα εργαλεία. Τα εργαλεία αυτά θα πρέπει να διαθέτουν την δυνατότητα εξερεύνησης αρχείων image και να είναι σε θέση να εντοπίζουν αρχεία του συστήματος που έχουν διαγραφεί από αυτό. Αυτό είναι και το βασικό πλεονέκτημα της τεχνικής απόκτησης που αναλύθηκε νωρίτερα.

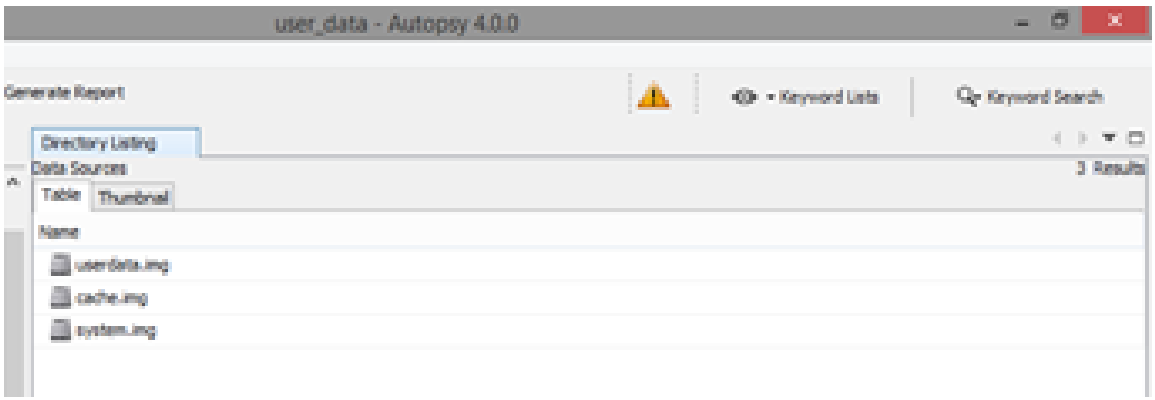
Για την ανάλυση των δεδομένων που αποκτήθηκαν και πιο συγκεκριμένα των τριών partition που παρουσιάζουν ενδιαφέρον, θα χρησιμοποιηθεί το λογισμικό Autopsy. Η τελευταία του έκδοση εκτός από την δυνατότητα να αναλύει ext4 file systems, διαθέτει και μια λειτουργία αποκλειστικά για διερεύνηση πληροφοριών που προκύπτουν από Android smartphones.

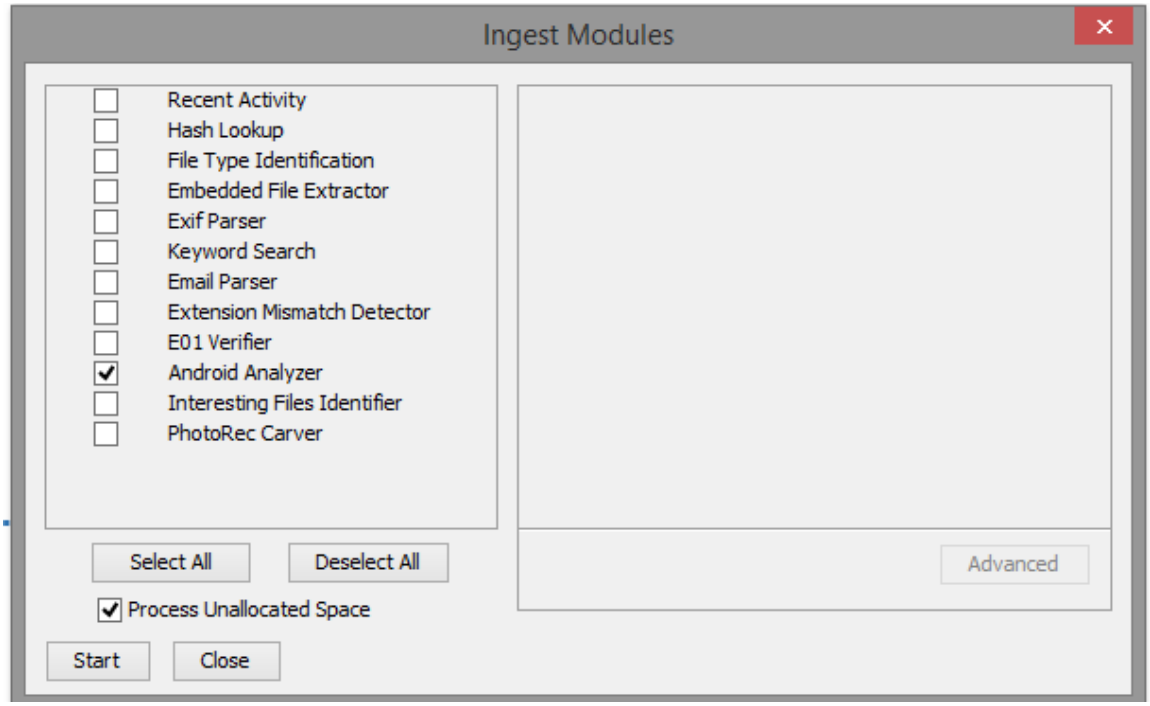
Η διαδικασία ξεκινά με την ενεργοποίηση του προγράμματος και την επιλογή create new case.

Στο επόμενο βήμα ο ερευνητής καλείται να συμπληρώσει βασικές πληροφορίες για την υπόθεση, όπως το όνομα της και το πού αυτή θα αποθηκευτεί.

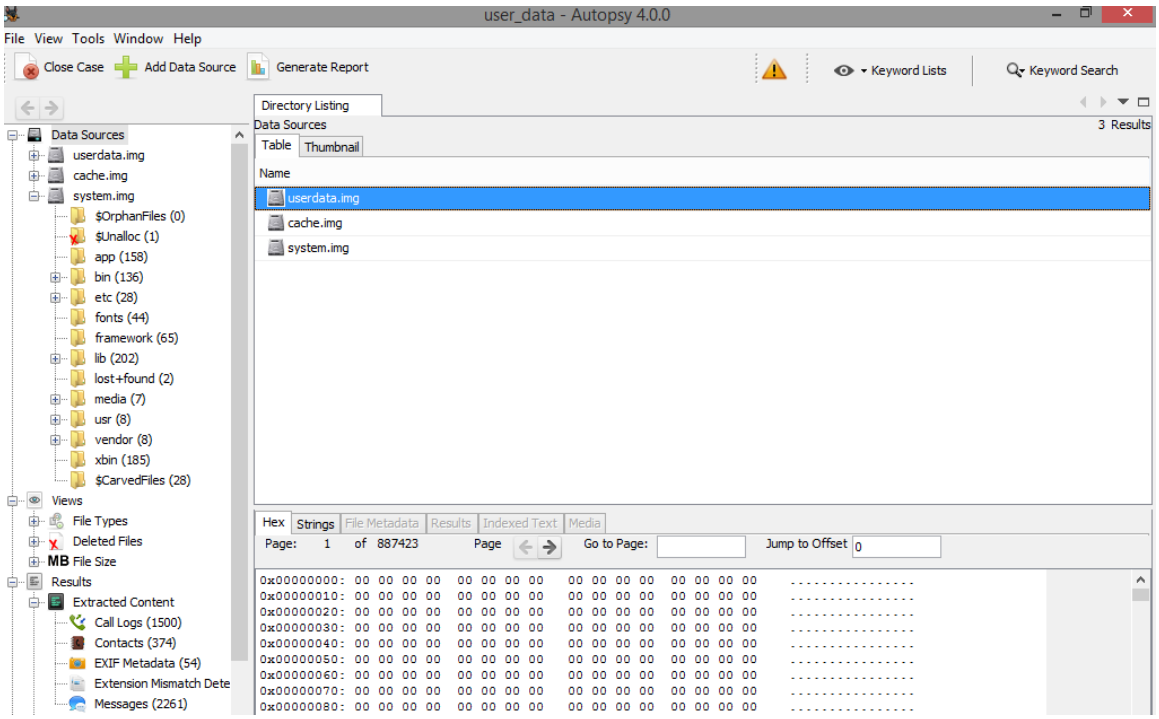


Στην συνέχεια σημειώνει κάποιες πληροφορίες για τον ίδιο και επιλέγει τα αρχεία που θέλει να αναλύσει. Στο υπόθεση εργασίας που εξετάζεται εδώ αυτά είναι το userdata.img το cache.img και το system.img. Μόλις επιλεχθούν ξεκινάει η αυτοματοποιημένη διαδικασία ανάλυσης, μέσω κάποιων ενσωματωμένων λειτουργιών. Ανάμεσα τους ξεχωρίζει αυτή που ονομάζεται Android Analyzer, και είναι αυτή που παρέχει εξειδικευμένες διεργασίες που αφορούν filesystems που προέρχονται από το λειτουργικό Android.

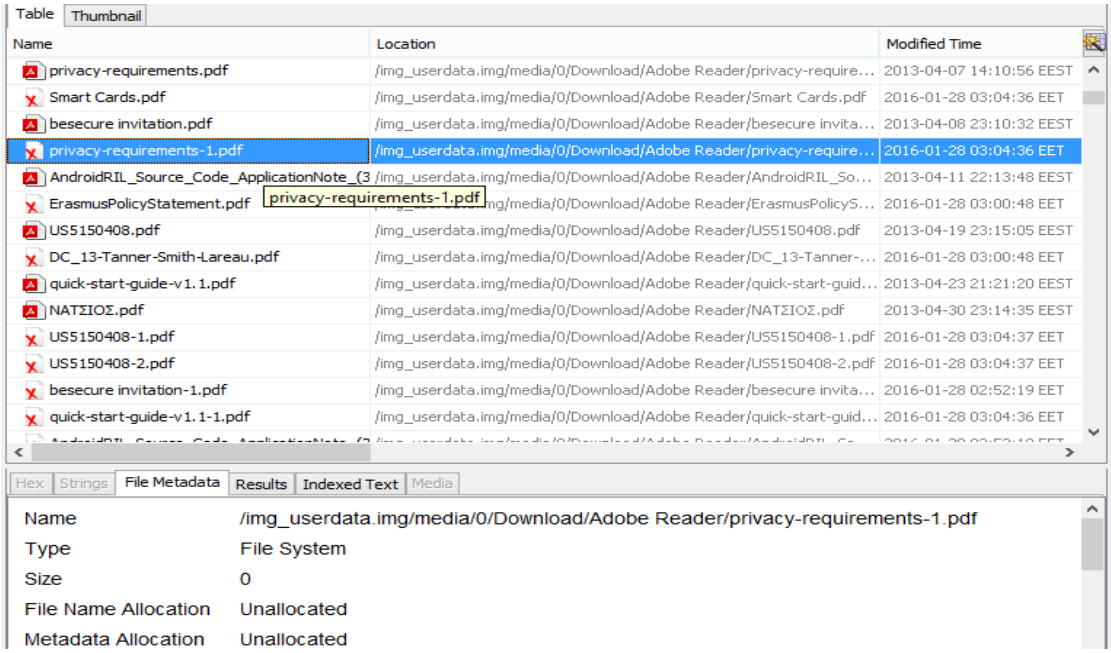


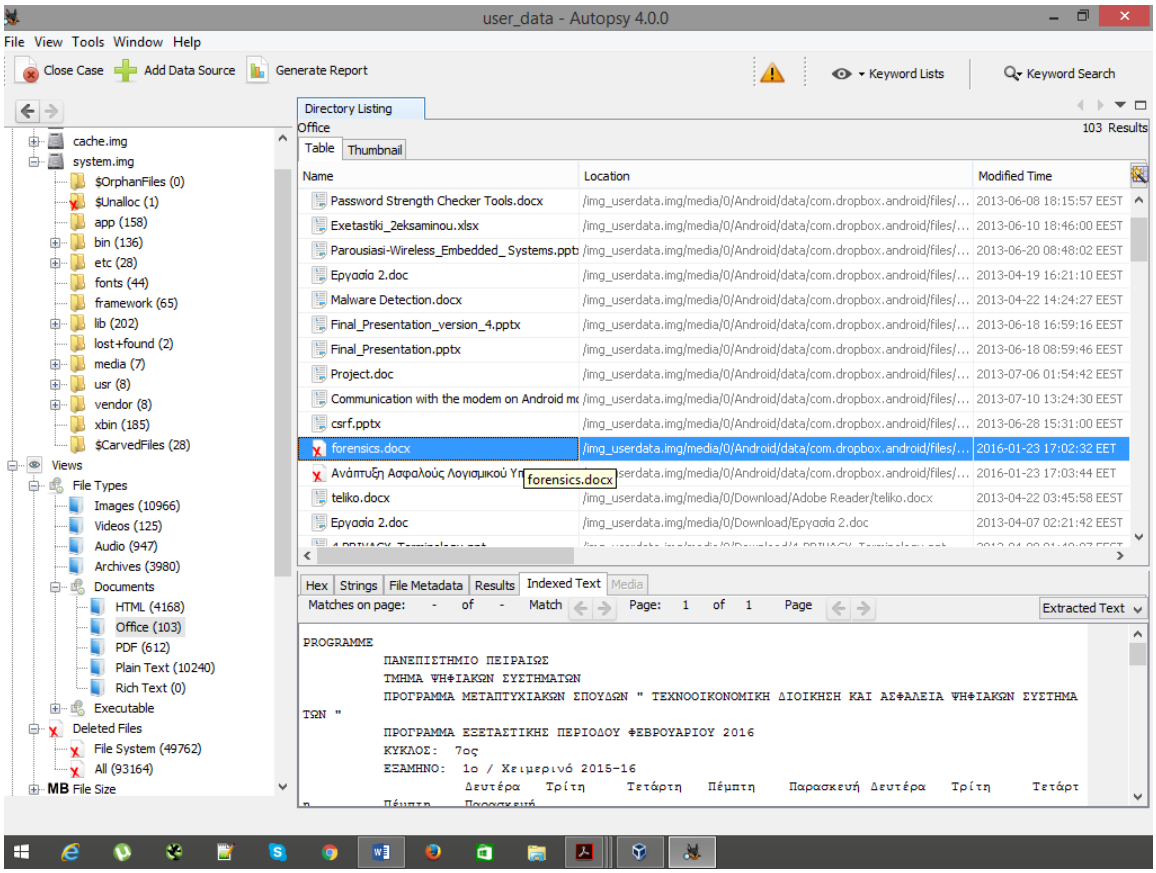


Η εισαγωγή και ανάλυση των δεδομένων διαρκεί αρκετή ώρα, μόλις ωστόσο ολοκληρωθεί, το σύνολο των πληροφοριών που υπάρχει στα partitions που αποκτήθηκαν, είναι διαθέσιμο προς αξιολόγηση.

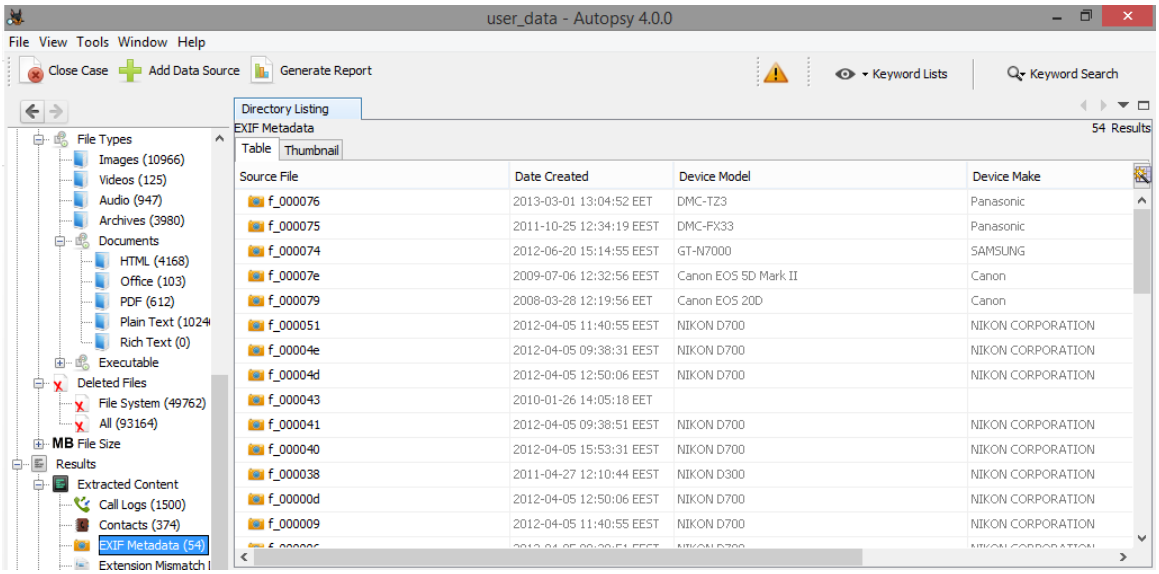


Για να διασφαλιστεί η αποτελεσματικότητα της ερευνητικής διαδικασίας απαιτείται μεθοδικότητα καθώς ο όγκος των προς ανάλυση δεδομένων είναι τεράστιος. Οι δυνατότητες του συγκεκριμένου εργαλείου ανοιχτού κώδικα είναι αξιόλογες, καθώς εκτός από την συγκέντρωση των πληροφοριών που βρίσκονται ακόμα αποθηκευμένες στην μνήμη της συσκευής, έχει την δυνατότητα να ανακτά και διεγραμμένα αρχεία.

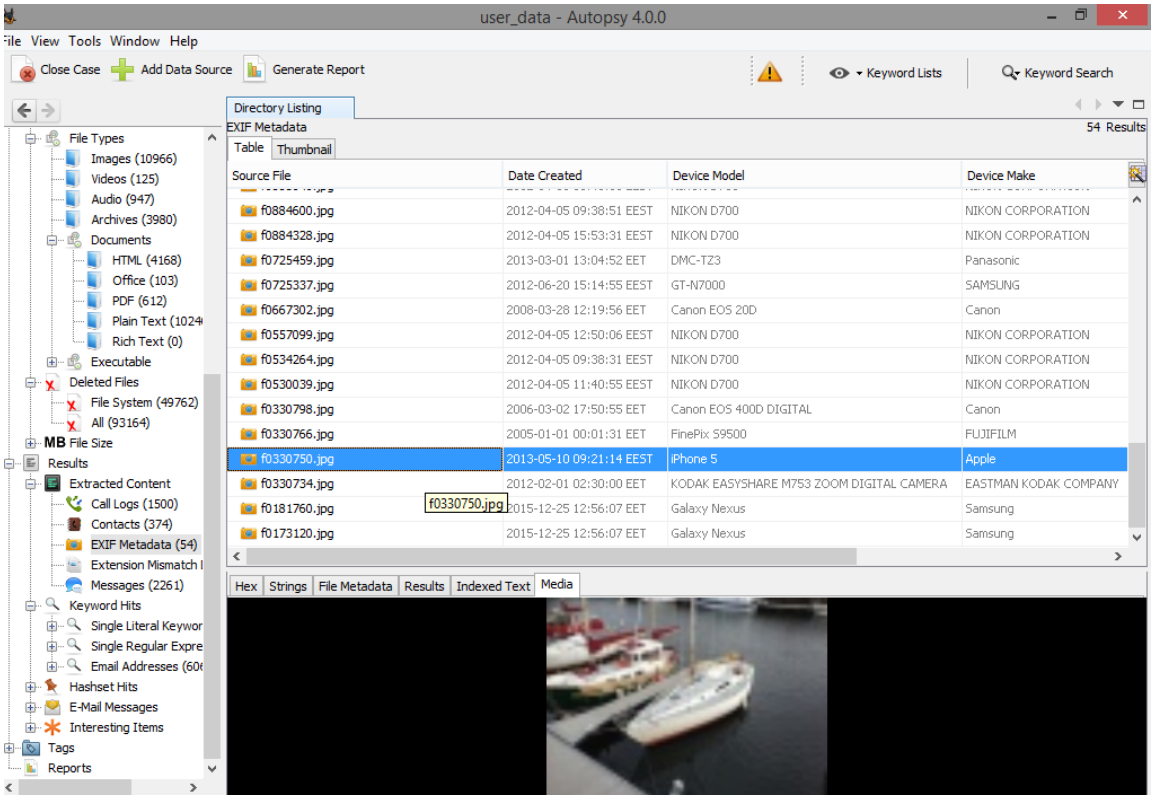


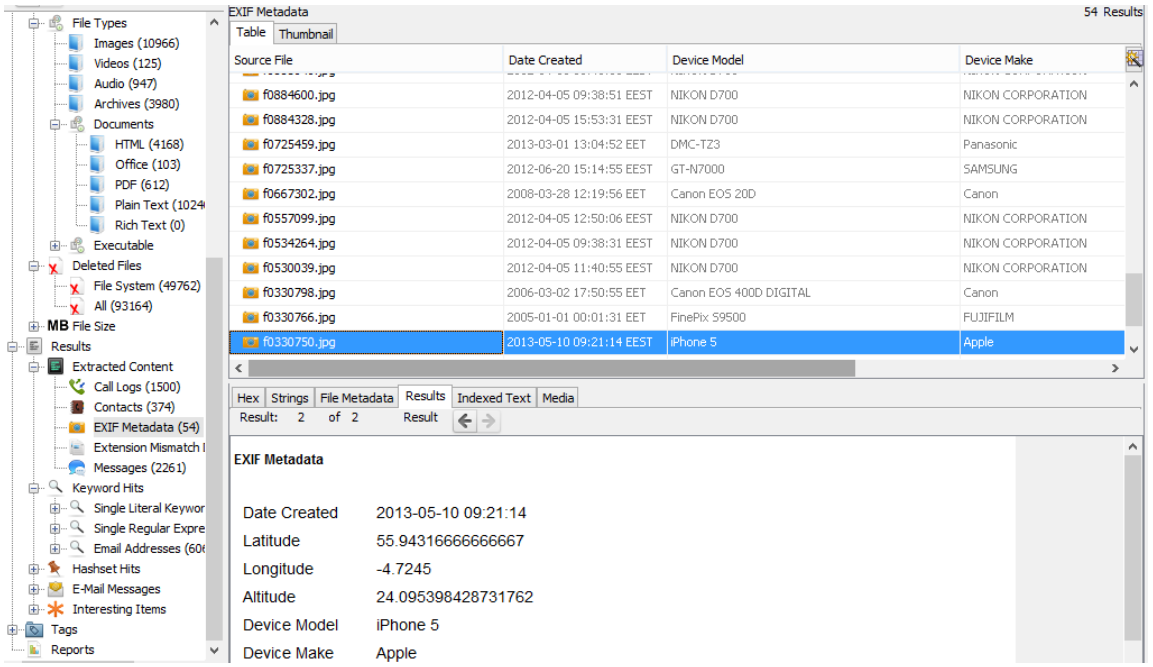


Μια ακόμα σημαντική λειτουργία που ενσωματώνει το εργαλείο αυτό, παρουσιάζεται με το όνομα EXIF Metadata. Πρόκειται ουσιαστικά για μια εφαρμογή απόκτησης μεταδεδομένων από εικόνες που έχουν ανακτηθεί ή υπάρχουν ακόμη.

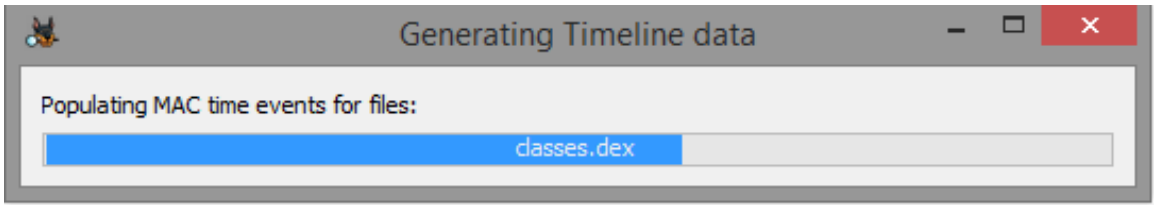


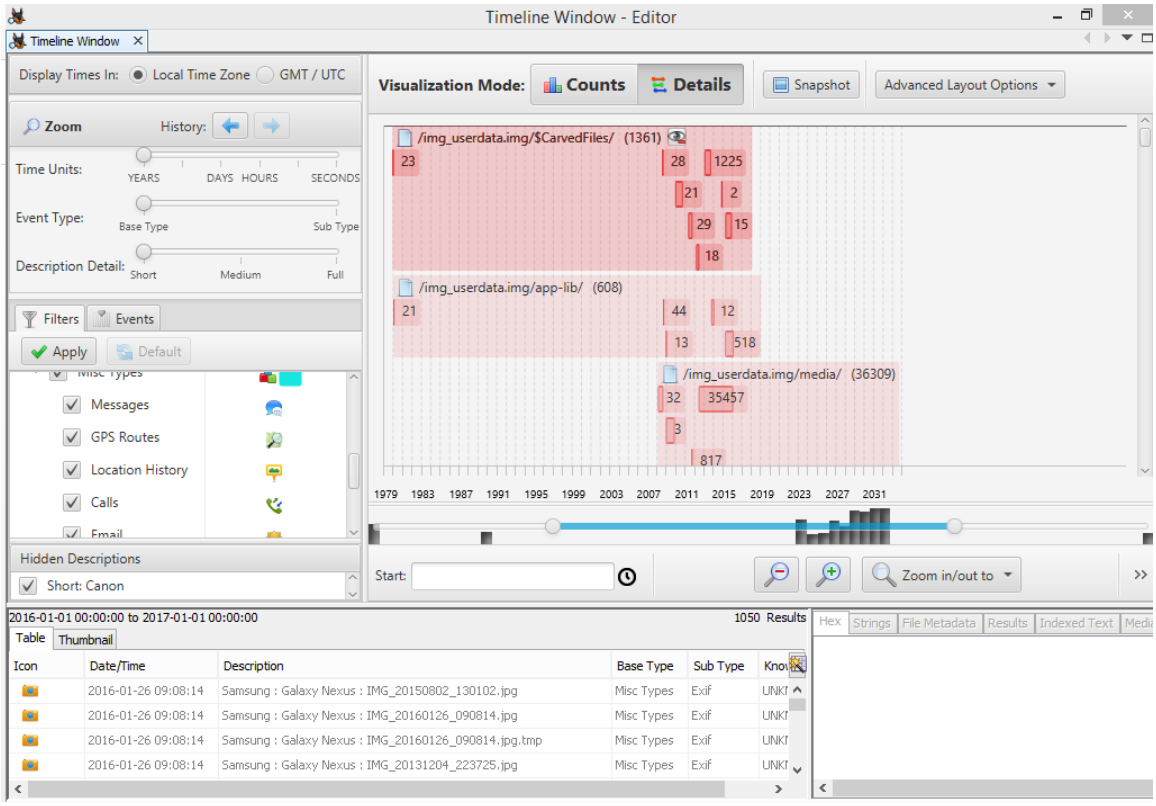
Ενδιαφέρον παρουσιάζει η περίπτωση του αρχείου JPG με όνομα f0330750, καθώς εκτός από την ίδια την εικόνα και κάποιες βασικές πληροφορίες για το πότε δημιουργήθηκε και το μοντέλο του τηλεφώνου που χρησιμοποιήθηκε, περιλαμβάνει και κάποια στοιχεία θέσης (γεωγραφικό μήκος και πλάτος).





Τέλος το εργαλείο Autopsy διαθέτει και μια εντυπωσιακή λειτουργία που ονομάζεται Timeline data. Η υλοποίηση αυτή, αντλεί πληροφορίες από το σύνολο των δεδομένων και τα κατηγοριοποιεί σύμφωνα με την ημερομηνία και τη φύση τους, με αποτέλεσμα ο ερευνητής να δημιουργεί μια συνολική εικόνα για την χρήση της συσκευής





16. File carving

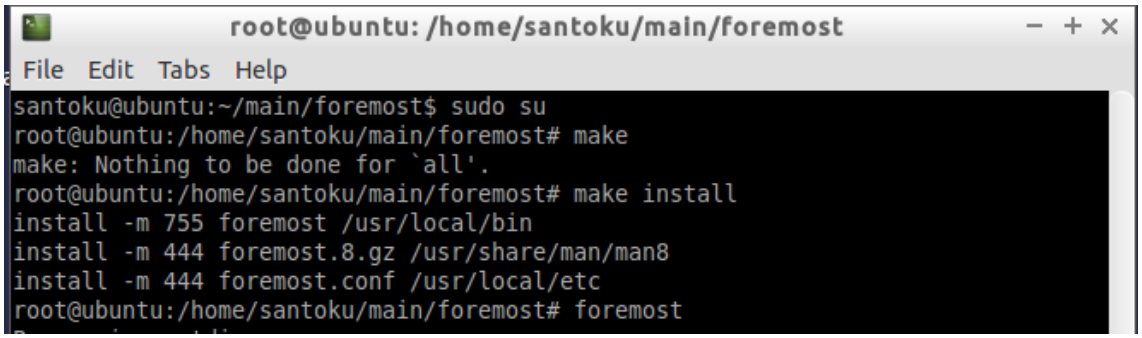
Η διαδικασία ανάκτησης διεγραμμένων αρχείων αποδεικνύεται σημαντικός και αναπόσπαστος παράγοντας για την επιτυχή ολοκλήρωση της ερευνητικής δραστηριότητας. Στο περιβάλλον του λειτουργικού linux, έχουν αναπτυχθεί αρκετές υλοποιήσεις που στοχεύουν στην αναζήτηση και απόκτηση καθορισμένων τύπων αρχείων μέσα από κάποια λογική μονάδα αποθήκευσης. Η μέθοδος αυτή ορίζεται ως file carving και βασίζεται στον εντοπισμό συγκεκριμένων ακολουθιών που ονομάζονται headers και footers.

Δυο από τα πιο γνωστά εργαλεία ανοιχτού κώδικα που χρησιμοποιούνται για την συγκεκριμένη λειτουργία, είναι το Scalpel και το Foremost. Η χρήση και των δύο γίνεται με τον ίδιο ακριβώς τρόπο, αρχικά γίνεται παραμετροποίηση του .conf file που περιλαμβάνει τους τύπους των αρχείων που αναζητούνται και έπειτα μέσω γραμμής εντολών, εκτελούνται και ανακτούν τα δεδομένα.

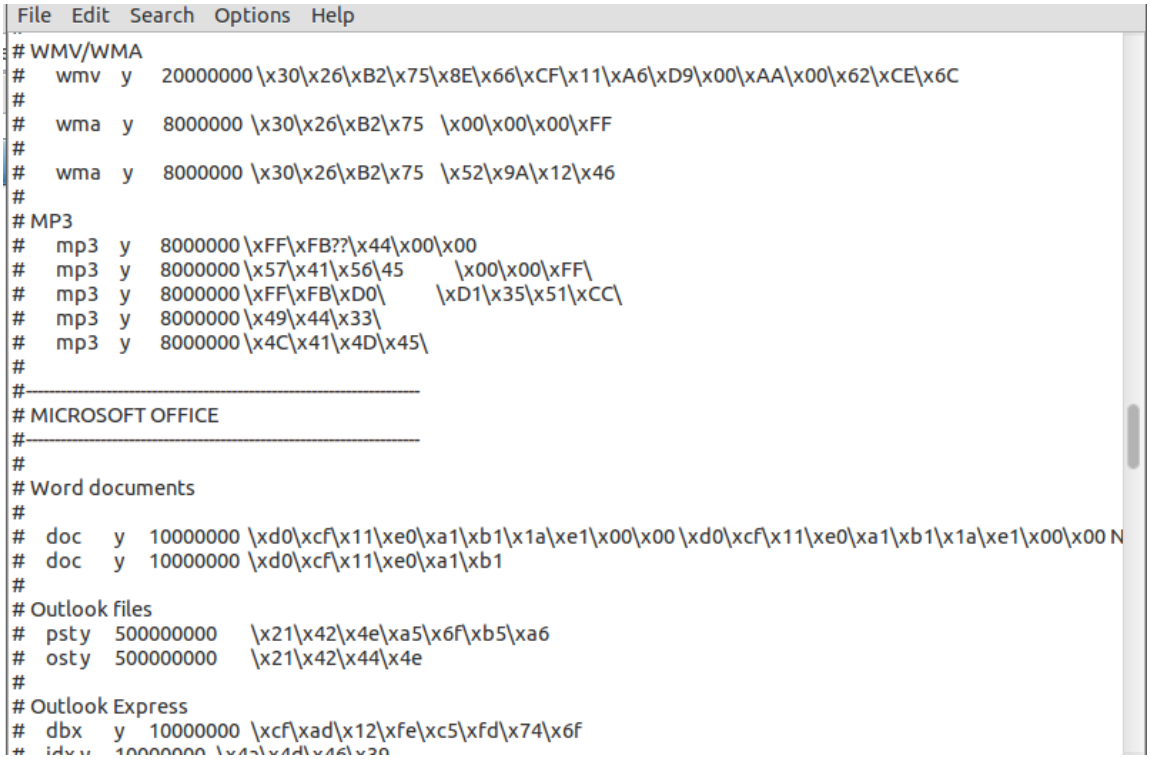
Πιο συγκεκριμένα και για την καλύτερη κατανόηση της λειτουργίας τους, θα χρησιμοποιηθεί το αρχείο userdata.img από την υπόθεση εργασίας του προηγούμενου κεφαλαίου.

Εργαλείο Foremost

Στο περιβάλλον εργασίας του Santoku Linux που χρησιμοποιήθηκε, το εργαλείο Foremost, δεν ήταν προεγκατεστημένο με αποτέλεσμα πρώτη κίνηση να αποτελεί η απόκτηση και εγκατάσταση του.



Επόμενη κίνηση είναι η τροποποίηση του αρχείου foremost.conf με σκοπό την επιλογή του τύπου των αρχείων που θα τεθούν προς αναζήτηση. Στο ίδιο αρχείο περιλαμβάνονται και σαφής οδηγίες για την σωστή παραμετροποίηση του.

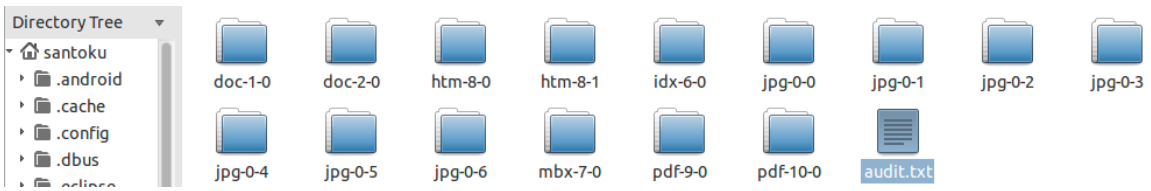


Στην συνέχεια το πρόγραμμα καλείται από την γραμμή εντολών και με την κατάλληλη σύνταξη ξεκινά η λειτουργία του. Οι βασικές παράμετροι που τίθενται, είναι απλά το μονοπάτι στο οποίο βρίσκεται η εικόνα του δίσκου που θα υποστεί την ανάλυση και ο φάκελος συγκέντρωσης των αποτελεσμάτων.

Foremost – i (αρχείο_image) – o (φάκελος αποτελεσμάτων)

```
foremost version 1.5.5 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
root@ubuntu:/home/santoku/main/foremost# foremost -i /home/santoku/main/userdata
.img -o /home/santoku/main
ERROR: /home/santoku/main is not empty
        Please specify another directory or run with -T.
root@ubuntu:/home/santoku/main/foremost# foremost -i /home/santoku/main/userdata
.img -o /home/santoku/main/e
Processing: /home/santoku/main/userdata.img
|*****************************
```

Μόλις η λειτουργία του προγράμματος ολοκληρωθεί εμφανίζεται ο φάκελος που έχει οριστεί για να δεχθεί τα αποτελέσματα της διαδικασίας carving. Εκτός από τα διάφορα αρχεία που περιέχονται, υπάρχει και ένα που συνοψίζει τα αποτελέσματα της ανάλυσης και ονομάζεται audit.txt



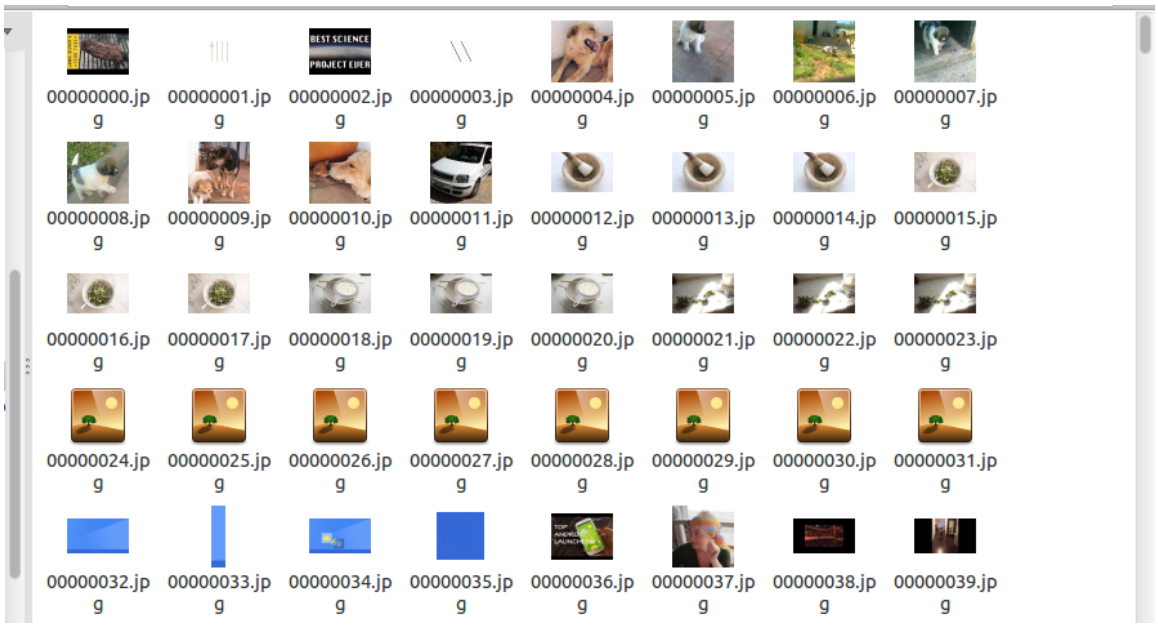

```
audit.txt
File  Edit  Search  Options  Help
Foremost version 1.5.5 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Mon Feb  8 14:02:27 2016
Invocation: foremost -i /home/santoku/main/userdata.img -o /home/santoku/main/e
Output directory: /home/santoku/main/e
Configuration file: /home/santoku/main/foremost/foremost.conf
------------------------------------------------------------------
File: /home/santoku/main/userdata.img
Start: Mon Feb  8 14:02:27 2016
Length: 13 GB (14539537520 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00105128.png           1 KB        53825812       (144 x 144)
```

```
258251 FILES EXTRACTED

jpg:= 34727
gif:= 1714
bmp:= 26
mov:= 309
rif:= 86
htm:= 1107
ole:= 104
zip:= 2894
exe:= 63
png:= 216845
pdf:= 376
-----------------------------------------------------------------

Foremost finished at Mon Feb  8 14:36:32 2016
```

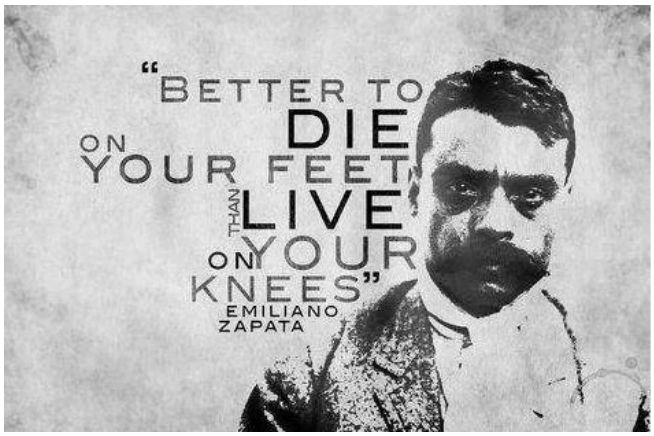
Ο όγκος των δεδομένων που ανακτήθηκε είναι αρκετά σημαντικός και περιλαμβάνει τα αρχεία των οποίων τα headers και footers που εντοπίστηκαν μέσα στο userdata.img

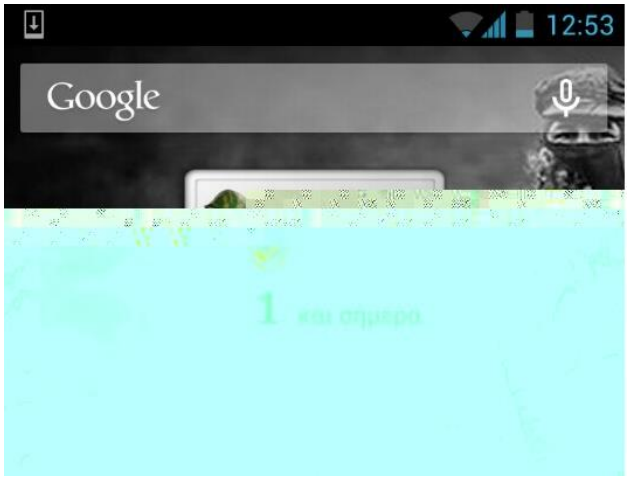
Εικόνες

Οι εικόνες που προέκυψαν από την διαδικασία του carving προέρχονται από το σύνολο των δραστηριοτήτων που πραγματοποιήθηκαν με την συσκευή. Αναλυτικότερα περιλαμβάνονται φωτογραφίες επαφών, wallpaper του τηλεφώνου, φωτογραφίες από τα αρχεία μουσικής που είναι αποθηκευμένα, εικόνες από την περιήγηση στο διαδίκτυο καθώς και αποθηκευμένα screenshots που έχουν διαγραφεί.



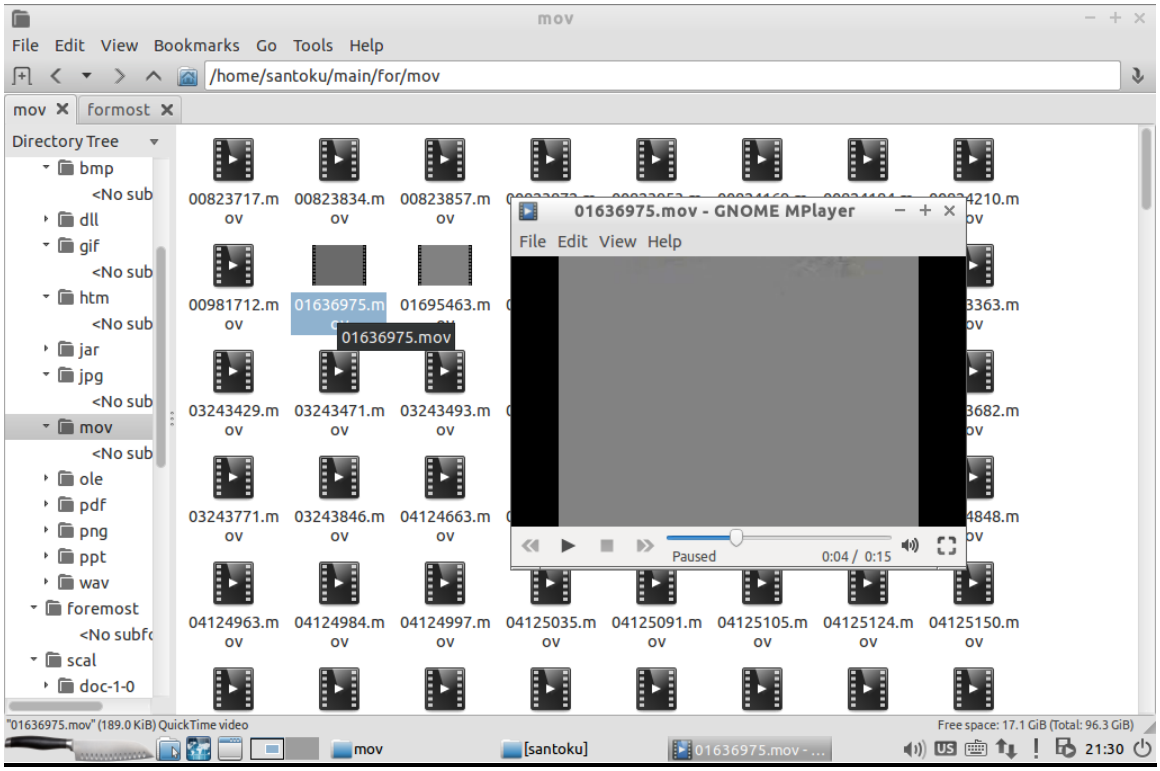

VILLAGERS OF
IOANNINA CITY
ZVARA/KARAKOLIA


"BETTER TO
DIE
ON
YOUR FEET
THAN
LIVE
ON
YOUR
KNEES"
EMILIANO
ZAPATA


12:53
Google

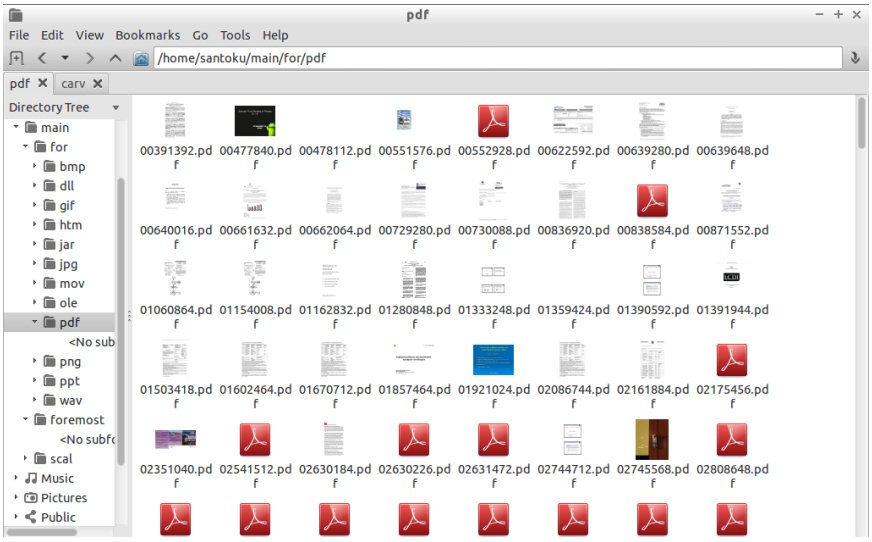
Αρχεία βίντεο

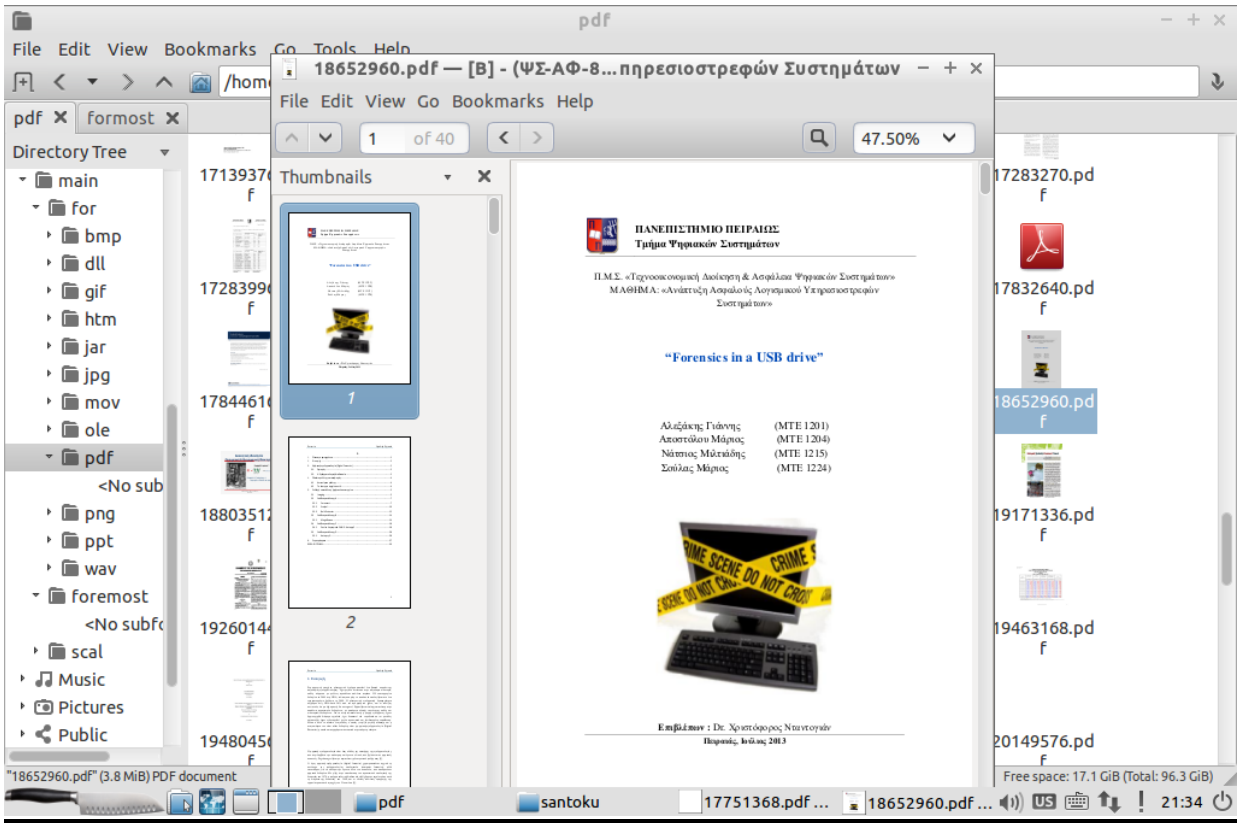
Επίσης ανακτήθηκε και μέρος των βίντεο αρχείων που υπήρχαν στην συσκευή. Κάποια από αυτά μάλιστα διατηρούσαν ακέραια και την δυνατότητα αναπαραγωγής τους.

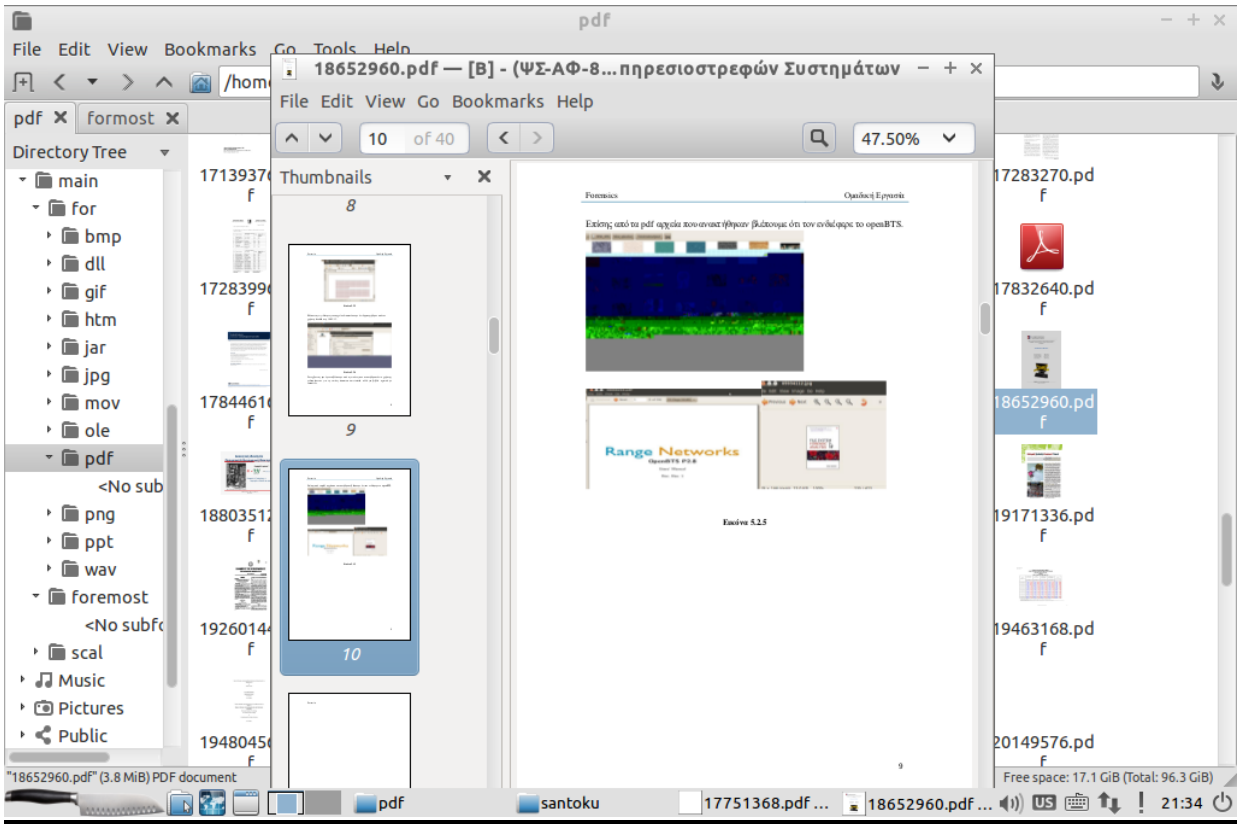


Αρχεία pdf

Το αρχείο με τα δεδομένα .pdf είναι από τα πιο πλούσια σε πληροφορίες και η ανάκτησή τους έχει γίνει διατηρώντας την πλήρη λειτουργικότητα τους.




pdf
File Edit View Bookmarks Go Tools Help
18652960.pdf — [B] - (ΨΣ-ΑΦ-8...πηρεσιοστρεφών Συστημάτων
File Edit View Go Bookmarks Help
1 of 40
47.50%
Thumbnails
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Ψηφιακών Συστημάτων
"Forensics in a USB drive"
Αλεξάκης Γιάννης (MTE 1201)
Αποστόλου Μάριος (MTE 1204)
Νάτσιος Μιλτιάδης (MTE 1215)
Σούλας Μάριος (MTE 1224)
Επιβλέπων : Δρ. Χριστόφορος Ντεντογιάν
Directory Tree
main
for
bmp
dll
gif
htm
jar
jpg
mov
ole
pdf
png
ppt
wav
foremost
scal
Music
Pictures
Public
"18652960.pdf" (3.8 MiB) PDF document
Free space: 17.1 GiB (Total: 96.3 GiB)
21:34


pdf
File Edit View Bookmarks Go Tools Help
18652960.pdf — [B] - (ΨΣ-ΑΦ-8...πηρεσιοστρεφών Συστημάτων
File Edit View Go Bookmarks Help
10 of 40
47.50%
Thumbnails
Forensics
Ομαδική Εργασία
Range Networks
Εικόνα 5.2.5
Directory Tree
"18652960.pdf" (3.8 MiB) PDF document
Free space: 17.1 GiB (Total: 96.3 GiB)
21:34

Εργαλείο scalpel

Η λειτουργία του συγκεκριμένου εργαλείου είναι παρόμοια με αυτή του Foremost. Για την ακρίβεια το scalpel αποτελεί φυσική συνέχεια του, καθώς η ανάπτυξή του βασίστηκε σε μεγάλο βαθμό στην βελτίωση του ήδη υπάρχοντα κώδικα από το προηγούμενο. Συγκριτικό του πλεονέκτημα παρουσιάζεται η βελτιστοποίηση της διαδικασίας αναζήτησης των αρχείων, με αποτέλεσμα την ταχύτερη εκτέλεση και εύρεση των δεδομένων.

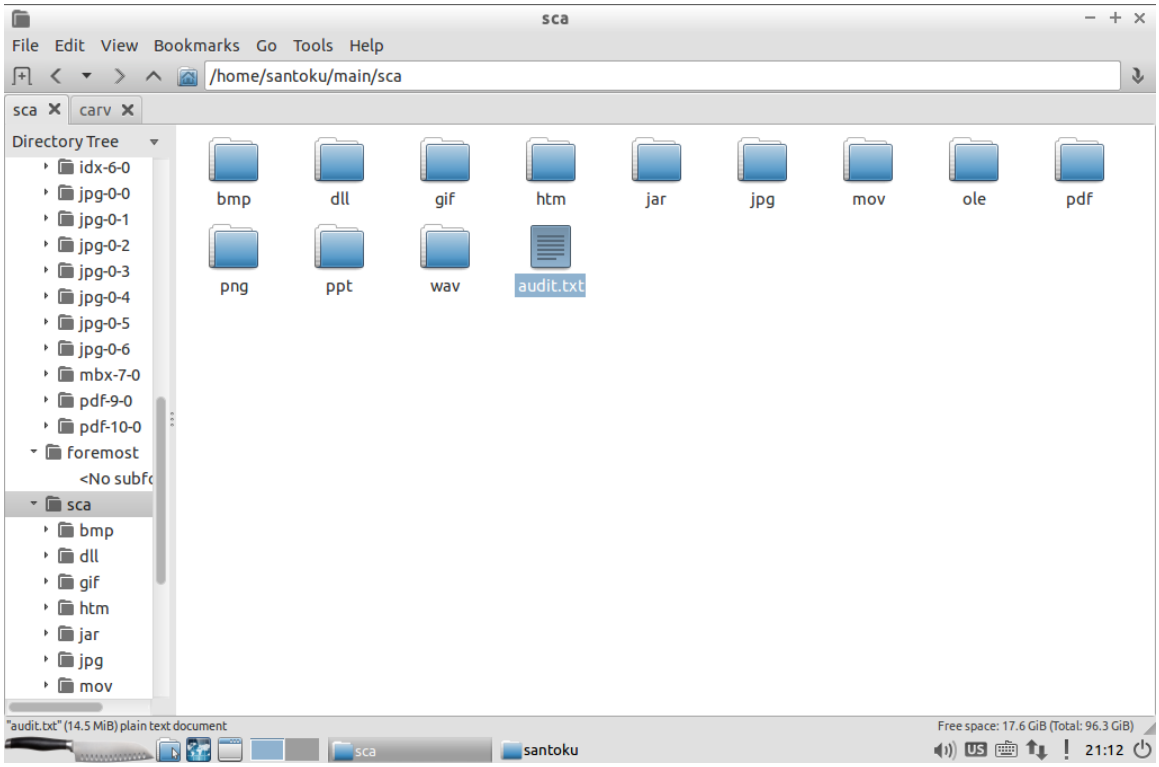
Στο περιβάλλον εργασίας που χρησιμοποιήθηκε η εφαρμογή βρίσκεται ήδη εγκατεστημένη, με αποτέλεσμα αυτό που χρειάζεται να είναι μόνο η παραμετροποίηση του αρχείου scalpel.conf, για να ξεκινήσει η διαδικασία ανάκτησης των αρχείων που δηλώθηκαν.

Η βασική σύνταξη της εντολής λειτουργίας του είναι η εξής:

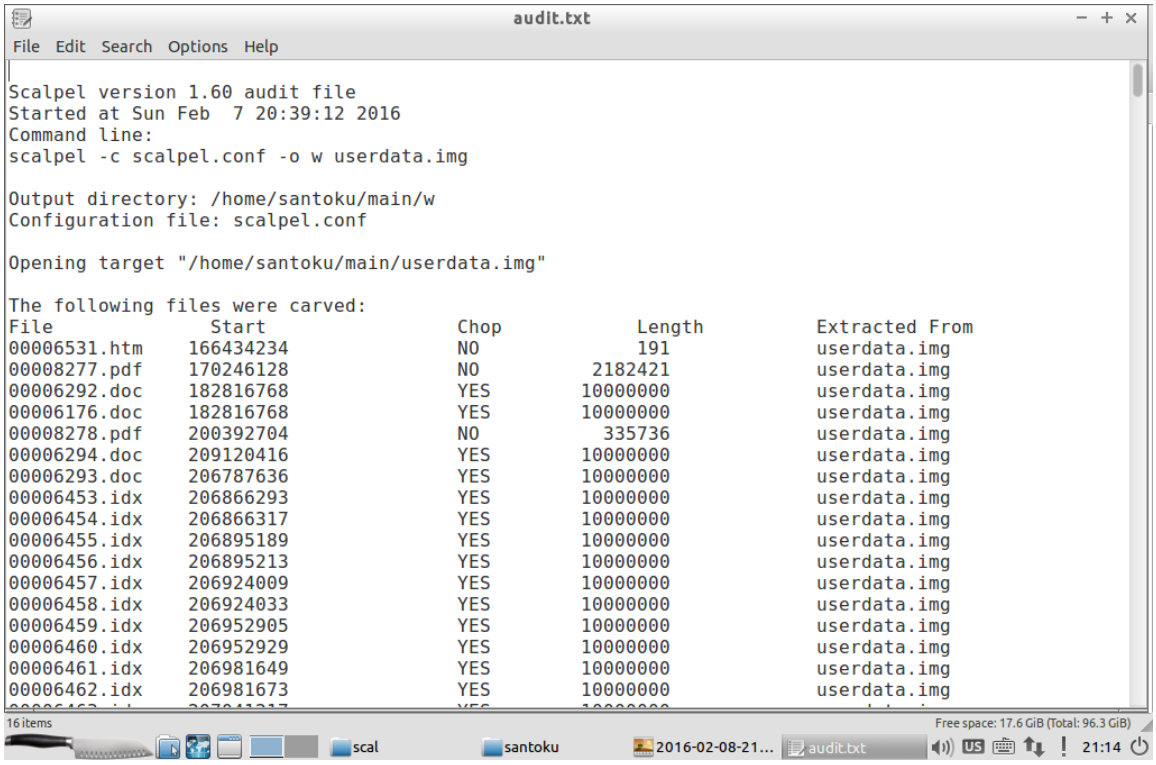
Scalpel –c scalpel.conf –o (φάκελος_εξαγωγής) (αρχείο_image)

```
santoku@ubuntu:~/main$ scalpel -c scalpel.conf -o sca userdata.img
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/santoku/main/userdata.img"

Image file pass 1/2.
userdata.img: 100.0% |*********************************|   13.5 GB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 6176 files
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 44 files
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x00\x3b" --> 1693 fi
les
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 33729 files
jpg with header "\xff\xd8\xff\xe1" and footer "\xff\xd9" --> 2322 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 62212 files
bmp with header "\x42\x4d\x3f\x3f\x00\x00\x00" and footer "" --> 1075 files
tif with header "\x49\x49\x2a\x00" and footer "" --> 2383 files
tif with header "\x4d\x4d\x00\x2a" and footer "" --> 1740 files
Carving files from image.
Image file pass 2/2.
userdata.img:   2.8% |                                 |  390.0 MB  6:43:57 ETA
```

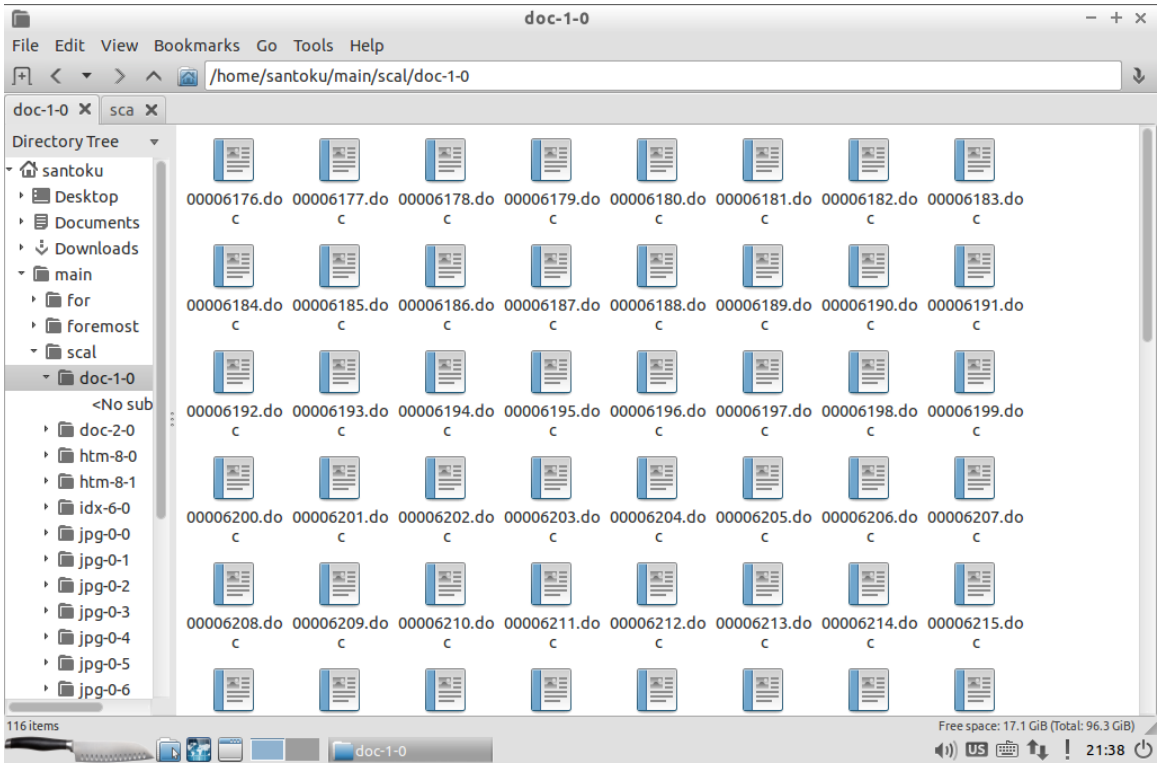
Ο φάκελος που δημιουργήθηκε περιλαμβάνει τα εξής αρχεία:

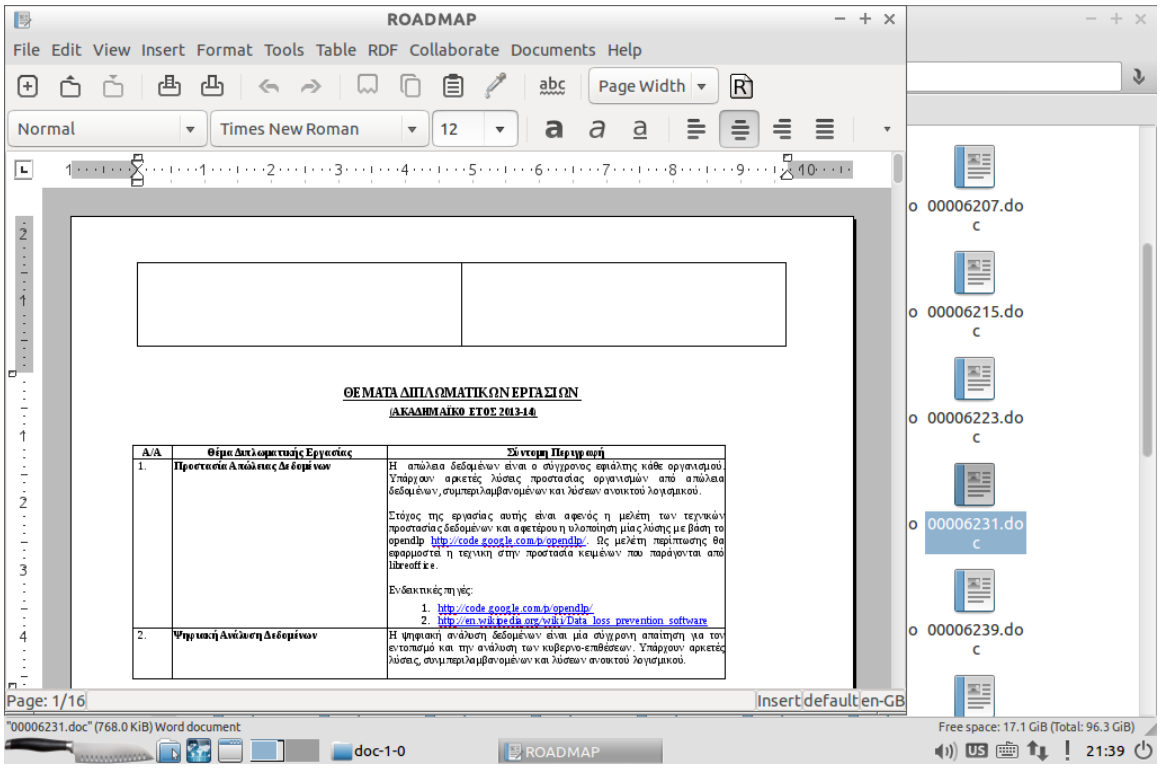


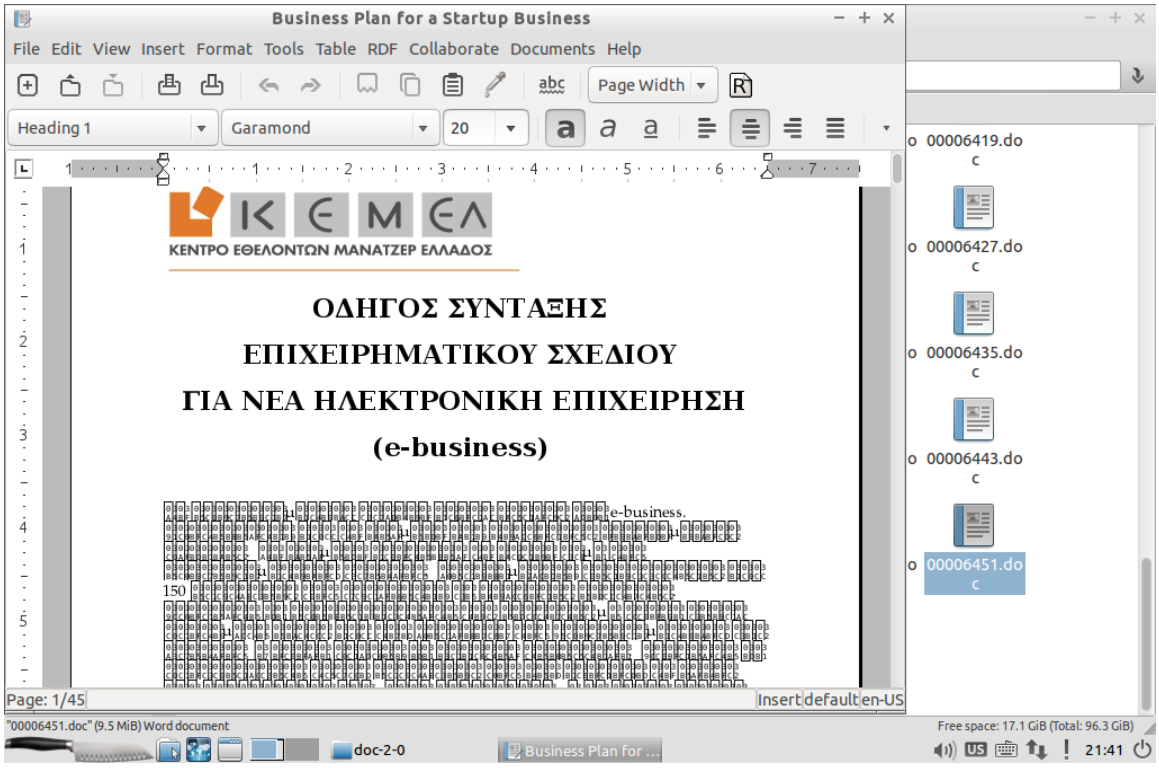
Στο αρχείο audit.txt περιλαμβάνεται μια συγκεντρωτική κατάσταση των αρχείων που ανακτήθηκαν, καθώς και κάποιες βασικές πληροφορίες της διαδικασίας.



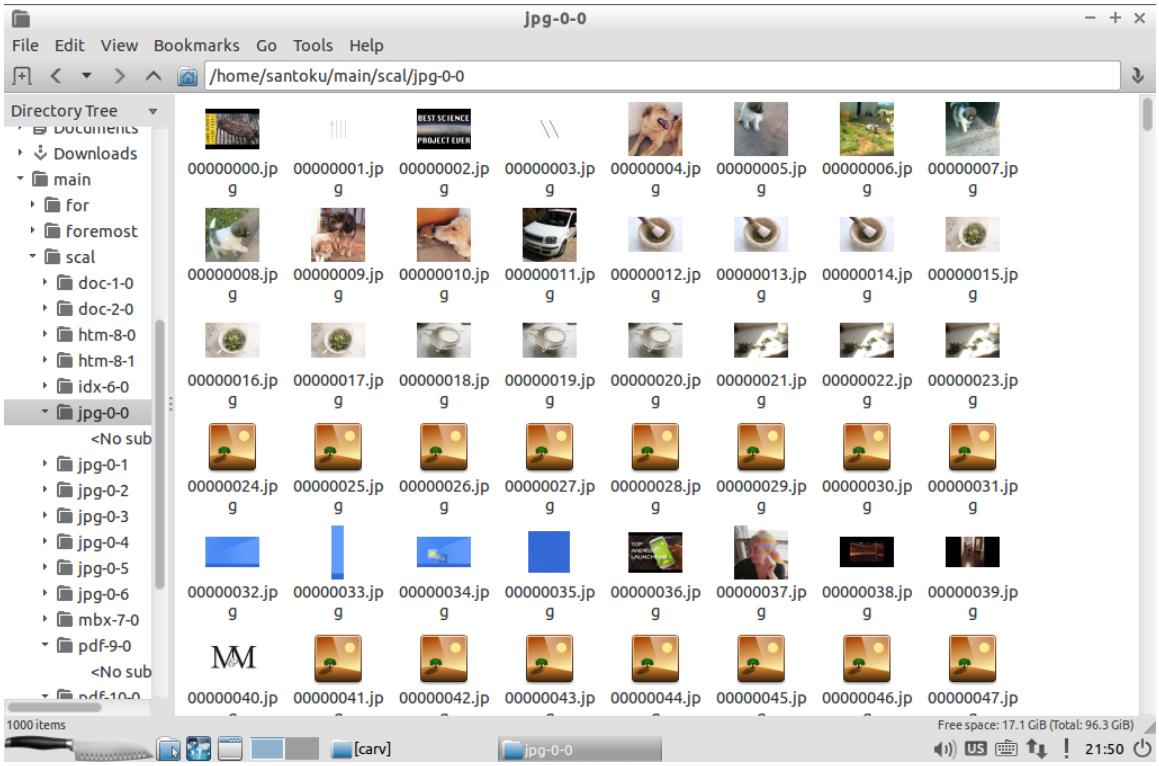
Από τα αποτελέσματα, ενδιαφέρον παρουσιάζει ο φάκελος των αρχείων Word που περιέχει διεγραμμένα δεδομένα κειμένων.







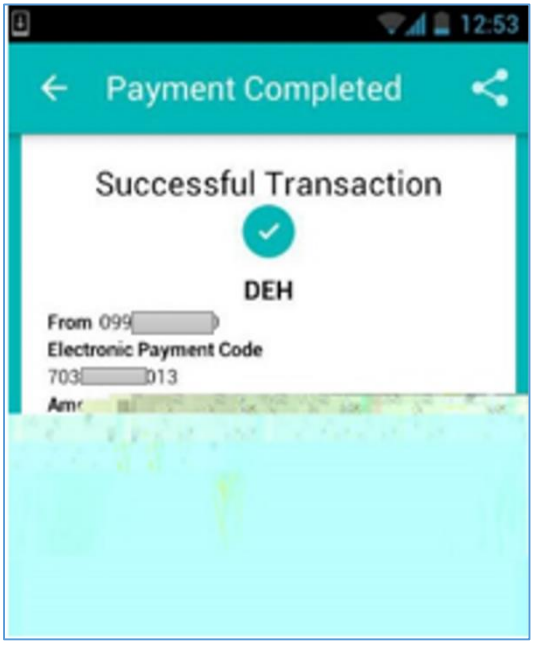
Στον φάκελο των εικόνων το αποτέλεσμα είναι ίδιο με αυτό του προηγούμενου εργαλείου.



Περιλαμβάνει εικόνες από εφαρμογές, που είναι εγκατεστημένες στην συσκευή, πχ. viber, facebook, καθώς και εικόνες από την περιήγηση στο διαδίκτυο.

Και στους επόμενους φακέλους (pdf,htm,ppt,wav κλπ), τα αρχεία που ανακτήθηκαν είναι σε μεγάλο βαθμό ίδια, με αποτέλεσμα να μην κρίνεται απαραίτητη η λεπτομερής παρουσίασή τους.

Κλείνοντας το κεφάλαιο του file carving θα πρέπει να τονιστεί η σημαντικότητα που έχει η προσεκτική ανάλυση κάθε στοιχείου που προκύπτει. Ο μεγάλος όγκος των αποτελεσμάτων, που προέρχονται από μια συσκευή με μεγάλο αποθηκευτικό χώρο, μπορεί να δημιουργήσει σύγχυση στον ερευνητή. Ωστόσο η μεθοδική ανάγνωσή τους μπορεί να αποφέρει σημαντικά στοιχεία για την στοιχειοθέτηση μιας υπόθεσης. Χαρακτηριστικό παράδειγμα αποτελεί μια εικόνα screenshot, που ανακτήθηκε από διεγραμμένο φάκελο του λειτουργικού και περιείχε κάποια αποδεικτικά πληρωμών μέσω ebanking.



17. Σύνοψη και συμπεράσματα

Ο κλάδος των digital forensics την τελευταία δεκαετία αρχίζει να περιλαμβάνει στις διαδικασίες διερεύνησης μιας υπόθεσης, πειστήρια, τα οποία προκύπτουν από την χρήση και άλλων ηλεκτρονικών συσκευών πέρα από τον προσωπικό υπολογιστή. Η πληθώρα των συσκευών που χρησιμοποιεί ένας άνθρωπος στην καθημερινότητά του, σε συνδυασμό με τις υπολογιστικές δυνατότητες που αυτές προσφέρουν, έχουν σαν αποτέλεσμα την συγκέντρωση μεγάλου αριθμού δεδομένων, που κάτω από συνθήκες ελέγχου, μπορούν να στοιχειοθετήσουν μια παραβατική δραστηριότητα ή αντίθετα να αθωώσουν κάποιον στις αίθουσες των δικαστηρίων.

Χαρακτηριστικό παράδειγμα μιας τέτοιας συσκευής αποτελεί το smartphone. Οι έξυπνες αυτές τηλεφωνικές συσκευές αποτελούν πλέον αναπόσπαστο κομμάτι κάθε δραστηριότητας ελέγχου, καθώς οι πληροφορίες που αποκτώνται από την μεθοδική ανάλυσή τους, περιλαμβάνουν στοιχεία από την καθημερινές δραστηριότητες του χρήστη. Προς το παρόν καμία κοινά αποδεκτή μεθοδολογία ανάλυσης δεν έχει εδραιωθεί επαρκώς, με αποτέλεσμα οι διαδικασίες που χρησιμοποιούνται να βασίζονται στις αρχές της ψηφιακής εγκληματολογίας γενικά, σε συνδυασμό με τεχνικές ελέγχου που αναπτύσσονται από μεμονωμένους ερευνητές ή ομάδες αυτών.

Στην παρούσα διπλωματική εκπόνηση έγινε παρουσίαση μιας βασικής μεθοδολογίας εγκληματολογικής ανάλυσης ενός έξυπνου κινητού τηλεφώνου με λειτουργικό Android και δόθηκε έμφαση στις τεχνικές απόκτησης και ανάκτησης των δεδομένων, που αυτό περιείχε. Μοναδικός περιορισμός αποτέλεσε το γεγονός, πως η παραπάνω διαδικασία έπρεπε να πραγματοποιηθεί με την αποκλειστική και μόνο χρήση εργαλείων ανοιχτού κώδικα, με απώτερο σκοπό την αξιολόγηση της αποτελεσματικότητάς τους.

Η ζήτηση των συγκεκριμένων εργαλείων τα τελευταία χρόνια τείνει να αυξάνεται, καθώς η ύπαρξη κοινοτήτων που βοηθούν τόσο στην δημιουργία τους, όσο και στην επέκτασή τους, τα καθιστά εφάμιλλα των ακριβών εμπορικών λύσεων με

παρόμοια αποτελεσματικότητα. Από την άλλη μεριά, το γεγονός ότι ο κώδικάς τους είναι δημόσια διαθέσιμος και κατά συνέπεια, η λειτουργία τους γνωστή στο ευρύ κοινό, μπορεί να τα καταστήσει αναποτελεσματικά όσο αφορά στην εξαγωγή στοιχείων από έμπειρους χρήστες, που λαμβάνουν αντίμετρα προστασίας.

Συνοψίζοντας, αυτό που πρέπει να τονιστεί είναι πως ο κλάδος των mobile forensics είναι σχετικά νέος και ως εκ τούτου η προοπτική ανάπτυξής του φαίνεται αρκετά υποσχόμενη. Οι σχετικές βιβλιογραφίες, που είναι διαθέσιμες, παρουσιάζουν μεμονωμένες λύσεις διαχείρισης συγκεκριμένων συσκευών, χωρίς να εξετάζουν μία πιο φορμαλιστική διαδικασία. Η υιοθέτηση μιας συγκεκριμένης και καλά τεκμηριωμένης μεθοδολογικής προσέγγισης, που σέβεται την αξία της ακεραιότητας των δεδομένων και ο συνδυασμός της με την χρήση εργαλείων, που κοινοποιούνται και αξιολογούνται από την ευρύτερη ερευνητική κοινότητα, αποτελούν ουσιαστικά τους δύο βασικούς πυλώνες, πάνω στους οποίους θα χτιστεί στέρεο το οικοδόμημα της εγκληματολογικής έρευνας έξυπνων κινητών συσκευών.

18. Βιβλιογραφία

1. Android Forensics : simplifying cell phone examinations, Jeff Lessard, Gary C. Kessler, September 2010
2. Learning Pentesting for Android Devices. A practical guide to learning penetration testing for Android devices and application, Packt Learning, March 2014
3. Learning Android Forensics. A hands on guide to Android forensics, Packt Learning 2015
4. Developing Process for Mobile Device Forensics , Det. Cynthia A. Murphy
5. Sushi-grade Smartphone Forensics on a Ramen Noodle Budget, Heather Mahalik
6. Open Source Digital Forensics Tools The Legal Argument, Brian Carrier
7. Forensic Analysis of Wireless Networking Evidence of Android Smartphones, Panagiotis Andriotis, George Oikonomou, Theo Tryfonas
8. Dissecting the Droid: Forensic Analysis of Android and its malicious Applications, Michael Spreitzenbarth Erlangen – 2013
9. Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool, Muhammad Faheem, N.-A. Le-Khac, Tahar Kechadi
10. DroidSpotter: A Forensic Tool for Android Location Data Collection and Analysis , Jeffrey Alan Kramer
11. An evidence - based Android cache forensics model, Felix Jeyareuben Chandrakumar 2014
12. Android Forensics: A Case Study of the “HTC Incredible” Phone, C. Racioppo and N. Murthy Seidenberg School of CSIS, Pace University, New York
13. Android Forensics Investigation, Analysis, and Mobile Security for Google Android, Andrew Hoog, 2011 Elsevier, Inc
14. Practical Mobile Forensics, Satish Bommisetty, Rohit Tamma, May 2014
15. Forensic analysis of mobile phone internal memory, Svein Y. Willassen, Norwegian University of Science and Technology
16. Mobile Device Forensics, Wikipedia, 2013
17. Foremost Tool, http://foremost.sourceforge.net
18. Android Forensics: Cracking the Pattern Lock Protection, http://resources.infosecinstitute.com