ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εγκληματολογική πληροφορική (Digital forensics) στα Λειτουργικά Συστήματα Android

Του φοιτητή
Μανώλη Στυλιανού
Αρ. Μητρώου: 154416

Επιβλέπων
Ηλιούδης Χρήστος
Καθηγητής

Ημερομηνία 12/6/21

Εγκληματολογική πληροφορική (Digital forensics) στα Λειτουργικά Σύστηματα Android

Κωδικός Π.Ε. 20225

Ονοματεπώνυμο φοιτητή: Στυλιανός Μανώλη

Ονοματεπώνυμο εισηγητή: Ηλιούδης Χρήστος

Ημερομηνία ανάληψης: Π.Ε. 1/11/20

Ημερομηνία περάτωσης Π.Ε. 12/6/21

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

«Αφιέρωση»

Ένα μεγάλο ευχαριστώ σε όλους τους καθηγητές μου. Ήταν για μένα πολύτιμη η καθοδήγηση και η βοήθεια που μου πρόσφερε ο κ.Ηλιούδης για τη δημιουργία της πτυχιακής εργασίας. Επίσης οφείλω ευχαριστίες τόσο στην οικογένεια μου αλλά και σε φίλους, που με τον τρόπο τους και την στήριξη τους με βοήθησαν να είμαι στο τελικό στάδιο για τη λήψη του πτυχίου μου.

ΠΡΟΛΟΓΟΣ

Η τεχνολογία των κινητών συσκευών έχει αλλάξει ριζικά τον τρόπο ζωής του σύγχρονου ανθρώπου. Ως αποτέλεσμα, οι κινητές συσκευές χρησιμοποιούνται σε όλους τους τομείς δραστηριοποίησης του ανθρώπου, περιλαμβάνοντας καθημερινές υποχρεώσεις όπως το επάγγελμα, αλλά και την ψυχαγωγία. Από την άλλη όμως οι κινητές συσκευές μπορούν να χρησιμοποιηθούν κακόβουλα, με αποτέλεσμα να παραβιάζονται ηθικοί και κοινωνικοί κανόνες, όπως η ιδιωτικότητα και τα προσωπικά δεδομένα [1]. Βέβαια, τέτοιες ενέργειες δεν μπορούν να γίνουν ανεξέλεγκτα, αφού η τεχνολογία αφήνει επίσης ίχνη μετά από κάθε κίνηση, όπως είναι για παράδειγμα τα ψηφιακά αποτυπώματα. Παρόλα αυτά, η ανίχνευση κακόβουλων ενεργειών δεν είναι πάντα εύκολη, αφού λόγω της συνεχούς ανάπτυξης των καινούργιων τεχνολογιών και εφαρμογών, η αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί μια συνεχή πρόκληση που επιβάλλει ανανεωμένη μάθηση [2].

ΠΕΡΙΛΗΨΗ

Στην παρούσα εργασία μελετήθηκε η εγκληματολογική πληροφορική (Digital forensics), η οποία ασχολείται με τα λειτουργικά σύστημα κινητών συσκευών android. Αφόρμηση για την εκπόνηση της παρούσας μελέτης ήταν η παρατήρηση ότι στη σύγχρονη εποχή οι κινητές συσκευές χρησιμοποιούνται όχι μόνο για αποθήκευση προσωπικών δεδομένων, αλλά και για εκτέλεση διαφόρων ενεργειών που μπορεί να είναι και εγκληματικές. Στα πλαίσια αυτά, έγινε συγκριτική αξιολόγηση των φάσεων για την ανάλυση των δεδομένων καθώς και του τρόπου διεκπεραίωσής τους. Επίσης έγινε εκτενής αναφορά στα ανοικτού κώδικα προγράμματα που ασχολούνται με την ανάλυση και εξαγωγή ευαίσθητων δεδομένων. Τέλος, πραγματοποιήθηκε μελέτη περίπτωσης εξαγωγής και ανάλυσης δεδομένων από μια κινητή συσκευή.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΠΛΗΡΟΦΟΡΙΚΗ

1.1. Εισαγωγή

Τις τελευταίες δεκαετίες παρουσιάζεται ένα αυξανόμενο ενδιαφέρον για την ψηφιακή εγκληματολογία τόσο σε ακαδημαϊκό επίπεδο, αλλά και σε νομικό επίπεδο ακόμη και σε επίπεδο επιχειρήσεων. Το αυξημένο αυτό ενδιαφέρον θεωρείται ότι εκπηγάζει από το φαινόμενο των κυβερνοεπιθέσεων που παρουσιάζονται καθημερινά σε οργανισμούς και εταιρίες, ακόμη και σε δημόσια πρόσωπα [3]. Το ηλεκτρονικό έγκλημα εμφανίστηκε γύρω στη δεκαετία του 1980, όταν οι υπολογιστές άρχισαν να γίνονται πιο προσιτοί στο ευρύ κοινό, κυρίως λόγω χαμηλότερου κόστους, διευκόλυνσης της χρήσης τους και ευρύτερης διασύνδεσης μέσω ψηφιακών δικτύων [4]. Επομένως, σκοπός της παρούσας είναι η διερεύνηση του φαινομένου του ψηφιακού εγκλήματος και των τρόπων αντιμέτωπισής του, καθώς και η παρουσίαση προγραμμάτων ανοικτού κώδικα αλλά και προγραμμάτων με συνδρομή, τα οποία θεωρούνται απαραίτητα εργαλεία για την αντιμετώπιση του ψηφιακού εγκλήματος. Απώτερος στόχος είναι η καλύτερη κατανόηση των επιμέρους πτυχών του προβλήματος και η αξιολόγηση της εξέλιξης που έχει σημειωθεί όσον αφορά τόσο το ψηφιακό έγκλημα όσο και τις τεχνικές που χρησιμοποιούνται για την αντιμετώπισή του.

1.2. Νομοθετικά πλαίσια

Αν και υπάρχει νομοθεσία σχετικά με το έγκλημα, η νομοθεσία αυτή μπορεί να θεωρηθεί ανεπαρκής όσον αφορά τα ψηφιακά εγκλήματα. Για παράδειγμα, η κλοπή ενός ηλεκτρονικού υπολογιστή σε σχέση με την κλοπή άυλων πληροφοριών που χρησιμοποιήθηκαν από μη εξουσιοδοτημένα πρόσωπα πιθανόν να τυγχάνει πιο εύκολα νομοθετικής διαχείρισης, αφού υπάρχει πρόνοια για νομικές κυρώσεις, σε αντίθεση με τα εγκλήματα ψηφιακής μορφής [5]. Γι' αυτό τον λόγο διαφάνηκε η ανάγκη για κατοχύρωση των νομοθετικών πλαισίων που αφορούν το ηλεκτρονικό έγκλημα, αν και οι προσπάθειες αυτές βρίσκονται ακόμα σε αρχικά στάδια. Έτσι, τα νομοθετικά πλαίσια για τις ψηφιακές παραβιάσεις έχουν κενά, με αποτέλεσμα το ψηφιακό έγκλημα να παρουσιάζει αυξημένη συχνότητα, αφού σύμφωνα με πηγές μόνο στην Αμερική προκύπτουν καθημερινά 4000 επιθέσεις [6].

1.3 Οργανισμοί και Επιχειρήσεις στην εποχή των πρώτων ψηφιακών εγκλημάτων

Πολλές επιχειρήσεις αλλά και οργανισμοί που χρησιμοποιούν την ηλεκτρονική πληροφορία είναι ιδιαίτερα ευάλωτοι για κάποια ψηφιακή εγκληματική ενέργεια, με αποτέλεσμα να αναγκάζονται να παίρνουν κάποια μέτρα ασφαλείας για την πρόληψη και αντιμετώπιση τέτοιων ενεργειών, πράγμα που συνέτεινε στην εμφάνιση των πρώτων πολιτικών ασφαλείας [7]. Βέβαια, σε πρακτικό επίπεδο η διαχείριση του ηλεκτρονικού εγκλήματος δεν είναι τόσο απλή, ιδιαίτερα τα πρώτα χρόνια της εμφάνισης της ψηφιακής τεχνολογίας. Έτσι οι προγραμματιστές αναγκάστηκαν να δημιουργήσουν δικές τους πλατφόρμες βασισμένες στα MS-DOS. Από αυτές που δημιουργήθηκαν κάποιες παραμένουν μέχρι και σήμερα, εννοείται με αναβαθμίσεις για να μπορούν να ανταπεξέλθουν στην σημερινή εποχή. Μερικές από αυτές είναι [8]:

- Norton's Utilities
- Central Point Software
- Mace Utilities

1.4. Η εποχή της ψηφιακής εγκληματολογίας

Η ψηφιακή εγκληματολογία και το ψηφιακό έγκλημα επηρεάζουν πλέον ευρέως τη ζωή ακόμα και σε προσωπικό επίπεδο αφού πλέον θύματα δεν είναι μόνο μεγάλες εταιρίες αλλά και πρόσωπα, συχνά με σκοπό την απόσπαση κάποιου χρηματικού ποσού [9]. Για να εκπαιδευτεί κάποιος στην εγκληματολογική πληροφορική χρειάζεται η γνώση και η τεχνική κατάρτιση στην διαφύλαξη της πληροφορίας και γενικά στην ασφάλεια. Περισσότερο η γνώση της εγκληματολογικής πληροφορικής συναντάται σε μεταπτυχιακά προγράμματα και διπλώματα που είναι πιο στοχευμένα. Πέραν του να υπάρχουν εξαιρετικές γνώσεις στην εγκληματολογία στον χώρο της πληροφορικής, η ενασχόληση με την καταπολέμηση του ηλεκτρονικού εγκλήματος χρειάζεται να υπάρχουν και γνώσεις σε ερευνητικό επίπεδο και αυτά να συνδυάζονται μαζί. Γι' αυτό συνήθως στις δημόσιες υπηρεσίες καταπολέμησης ηλεκτρονικού εγκλήματος θεωρείται ότι πρέπει πρώτα κάποιος να έχει περάσει την αστυνομική σχολή [10].

1.5. Εξέλιξη

Από το 1999 μέχρι και το 2007 θεωρείται η περίοδος ανάπτυξης για την εγκληματολογική πληροφορική αφού πλέον είναι δυνατόν να γίνει έρευνα για το παρελθόν ενός υπόπτου, να ανακτηθούν δεδομένα που έχουν διαγραφεί και γενικά να εντοπιστούν αποτυπώματα που έχουν μείνει από κάποιο έγκλημα. Έτσι, η εγκληματολογική πληροφορική θεωρείται πλέον σαν μια επιστήμη όπως η παραδοσιακή εγκληματολογία χωρίς να θεωρείται υποδεέστερη ή αναξιόπιστη. Από το 2005 έχουν αρχίσει να δημιουργούνται και κάποιες τυποποιημένες διαδικασίες για την ανάλυση ενός ηλεκτρονικού υπολογιστή, πράγμα που θεωρείται ένα μεγάλο βήμα στον χώρο, αν και με μεγάλα κενά, αφού σχεδόν οι περισσότερες διαδικασίες είχαν σαν περιορισμό το λειτουργικό σύστημα της Microsoft και τα Windows [11].

1.6. Κατηγορίες Ψηφιακής Εγκληματολογίας

Γενικά η εγκληματολογική πληροφορική χωρίζεται σε 3 κατηγορίες [12]:

- Δημόσιες διερευνήσεις (Public Investigations): Είναι οι δημόσιες έρευνές που διεξάγονται από τις δημόσιες αρχές

2) Ιδιωτικές διερευνήσεις (Private Investigations): Είναι οι ιδιωτικές έρευνες που διεξάγονται από το αρμόδιο τμήμα της εταιρίας για δικές τις υποθέσεις
3) Ατομικές (Individual): Ατομικές μορφή ηλεκτρονικής έρευνας και ανακάλυψης στοιχείων

1.7. Ψηφιακά και Μη ψηφιακά Εγκλήματα

Όποιο μη ψηφιακό έγκλημα γίνεται κατά κάποιο τρόπο υποδεικνύει το είδος των σχετικών αποδεικτικών στοιχείων που μπορούν να ανακτηθούν. Για παράδειγμα σε μια ανθρωποκτονία θα ήταν χρήσιμο να προσδιοριστεί η ώρα, η τοποθεσία και η αιτία θανάτου. Κατά παρόμοιο τρόπο, η ψηφιακή εγκληματολογική εξέταση πρέπει να θεωρείται εξίσου σημαντική αφού οι κινήσεις πρέπει να είναι στοχευμένες και ο εξεταστής το ίδιο προσεκτικός και αποτελεσματικός όπως με το μη ψηφιακό έγκλημα. Σε ένα ψηφιακό περιβάλλον γίνεται επίσης έρευνα για το "όπλο" του δράστη, το οποίο μπορεί να είναι της μορφής ενός ηλεκτρονικού μηνύματος με απειλητικό περιεχόμενο, πράγμα που απαιτεί να διαπιστωθεί η ακριβής χρονικής σήμανση της αποστολής και η ζώνη ώρας χρησιμοποιήθηκε, καθώς και ο υπολογιστής από τον οποίο εστάλη το μήνυμα, όπως και το άτομο πίσω από αυτό. Η θεμελιώδης πρόκληση που υπάρχει λοιπόν στα ψηφιακά εγκλήματα είναι να συνδεθούν τα δεδομένα που

ανακτώνται κατά την έρευνα με τον δράστη, πράγμα που δεν είναι πάντα εύκολο, αφού ο έλεγχος πρόσβασης δεν είναι αλάνθαστος και δεν είναι πάντα αξιόπιστος [13].

1.8. Παράδειγμα σύνδεσης αποδεικτικών στοιχείων με το χρήστη

Ένα παράδειγμα διασύνδεσης των αποδεικτικών στοιχείων με τον χρήστη αποτελεί η περίπτωση ψηφιακού εγκλήματος που έγινε το 2006 στην Αμερική, όταν σε ένα κατάστημα επισκευής ηλεκτρονικών υπολογιστών ο υπάλληλος που ασχολείτο με την επισκευή ενός υπολογιστή εντόπισε μια συλλογή από φωτογραφίες και βίντεο παιδικής πορνογραφίας. Ο υπάλληλος κατάγγειλε το συμβάν στην αστυνομία με αποτέλεσμα να κατασχεθεί ο υπολογιστής σαν τεκμήριο. Μετά από δύο χρόνια απαγγέλθηκαν κατηγορίες παιδικής πορνογραφίας στον ιδιοκτήτη του υπολογιστή, αν και είχαν περάσει δυο ολόκληρα χρόνια. Μέσα στην καταγγελία αναφέρθηκε ότι τα αρχεία είχαν κατεβεί στον υπολογιστή μέσω του προγράμματος LimeWire, μερικά το 2004 και τα υπόλοιπα το 2005. Βρέθηκαν επίσης εγκατεστημένα προγράμματα αναπαραγωγής βίντεο το Real Player και το Windows Media Player, τα οποία έχουν και τα δύο την δυνατότητα καταγραφής των αρχείων βίντεο και ήχου που είχαν αναπαραχθεί πρόσφατα, με τα παράνομα βίντεο να είναι στη λίστα. Στην επανεξέταση των δεδομένων είχε διαφανεί ότι μερικά είχαν αναπαραχθεί αρκετές φορές. Εκτός από τον κατηγορούμενο στην ανάκριση ειπώθηκε ότι δεν είχε μόνο αυτός πρόσβαση στον υπολογιστή αλλά και το ανήλικο παιδί του, καθώς και ένα νεαρό ζευγάρι που ζούσε στην ίδια κατοικία με αυτόν εκείνη την περίοδο, ενώ γενικά ήταν σύνηθες ο κατηγορούμενος να κουβαλάει τον φορητό υπολογιστή του σε διάφορα μέρη. Τελικά φάνηκε ότι οι τελευταίες ημερομηνίες πρόσβασης στα αρχεία ήταν λανθασμένες, αφού τροποποιήθηκαν κατά λάθος από πρόγραμμα ανίχνευσης ιών, συγκαλύπτοντας τις σωστές ημερομηνίες. Σαν άλλοθι ο κατηγορούμενος παρουσίασε ότι δεν μπορούσε να έχει πρόσβαση εκείνη την περίοδο αναπαραγωγής των αρχείων αφού απουσίαζε στο εξωτερικό. Αντιθέτως, το ανήλικο παιδί του είχε πρόσβαση, όπως και οι φίλοι του, αφού ο κωδικός πρόσβασης στον υπολογιστή ήταν γνωστός σε όλους αυτούς. Η παρουσία επίσης κακόβουλου λογισμικού Trojan ήταν εμφανής στον υπολογιστή ωστόσο δεν αποδείχθηκε ότι το λογισμικό αυτό είχε μολύνει τον υπολογιστή καθιστώντας τον διαχειρίσιμο μέσω του συγκεκριμένου λογισμικού. Λόγω ελλιπών στοιχείων, αστοχιών και ανεπαρκούς ανάλυσης της ερευνητικής επιτροπής καθώς οι ημερομηνίες ήταν λανθασμένες, θεωρήθηκε ότι η ακεραιότητα των δεδομένων δεν είχε διασφαλιστεί και η υπόθεση απορρίφθηκε [14].

ΚΕΦΑΛΑΙΟ 2: ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΗ ΠΛΗΡΟΦΟΡΙΚΗ

2.1. Ανάλυση σταδίων εκτέλεσης σε μια κυβερνοεπίθεση

Συνήθως τα υποψήφια θύματα μιας κυβερνοεπίθεσης είναι μεγάλες εταιρίες και οργανισμοί, οι οποίες αντιμετωπίζουν ιδιαίτερα σοβαρές ψηφιακές προκλήσεις. Όπως γίνεται και με τα μη ψηφιακά εγκλήματα, όταν παρουσιαστεί κάποιο ψηφιακό έγκλημα γίνονται κάποιες σταθερές διαδικασίες, οι οποίες περιλαμβάνουν συγκεκριμένες ενέργειες που γίνονται από την στιγμή που θα εμφανιστεί ένα περιστατικό και αναφερθεί στους εκάστοτε αρμόδιους μέχρι και την στιγμή που θα καταλήξει στα δικαστήρια [15]. Αν και υπάρχουν αρκετά θεωρητικά σχήματα διαδικασιών, για τους σκοπούς της παρούσας εργασίας θα αναλυθεί το σχήμα Digital Forensics Research Workshop (Εικόνα 2.1), το οποίο αποτελείται από τα ακόλουθα έξι πλαίσια [16]:

- Ταυτοποίηση (Identification)

  Μια αρχή που συζητιέται συχνά στον κόσμο της εγκληματολογίας είναι ο νομός ανταλλαγής του Locard's. Αυτός ο νόμος λέει ότι όταν δυο αντικείμενα έρθουν σε επαφή αφήνουν πάντα ίχνη το ένα στο άλλο, τόσο στον φυσικό όσο και στον ψηφιακό κόσμο. Για παράδειγμα, όταν κάποιος σερφάρει στο διαδίκτυο και έχει επισκεφτεί κάποιες σελίδες, είναι πολύ πιθανόν ο διακομιστής να κρατάει ιστορικό από τις διευθύνσεις που μπήκαν στην ιστοσελίδα. Αντίστοιχα και η σελίδα αφήνει κάποιο cookie στον υπολογιστή απ' όπου ζητήθηκε πρόσβαση. Όπως και στον φυσικό έτσι και στον ψηφιακό κόσμο, αυτά τα αποτυπώματα όμως δεν παραμένουν για πάντα. Επομένως η υπεύθυνη ομάδα πρέπει να εντοπίζει γρήγορα δεδομένα που μπορούν εύκολα να προσδιορίσουν την πηγή του ψηφιακού εγκλήματος.

- Διατήρηση (Preservation)

  Κατά τη διαδικασία εύρεσης των δεδομένων είναι σημαντικό αυτά να παραμείνουν ακέραια και να προστατευθούν από οποιαδήποτε αλλαγή ή διαγραφή. Για παράδειγμα για τεκμήρια όπως log files είναι σημαντικό να ενεργοποιηθούν έλεγχοι από λογισμικά που προστατεύουν οποιαδήποτε αλλαγή, ενώ οι υπολογιστές που θεωρούνται τεκμήρια πρέπει να απομονώνονται από άλλα συστήματα και να βγαίνουν εκτός δικτύου. Εκτός από ψηφιακή προφύλαξη βέβαια πρέπει να υπάρχει και φυσική προφύλαξη έτσι ώστε μόνο εξουσιοδοτημένα άτομα να έχουν πρόσβαση στα δεδομένα.

- Συγκέντρωση (Collection)

  Η συγκέντρωση των δεδομένων είναι σημαντική κατά την διάρκεια καταγραφής ενός συμβάντος, ειδικά αν αυτά τα δεδομένα είναι αποθηκευμένα σε πτητικές μνήμες δηλαδή σε αυτές που χρειάζονται ηλεκτρική ενέργεια για να λειτουργούν, ενώ όταν σταματήσει η ηλεκτροδότηση τους χάνουν όλα τα δεδομένα. Για παράδειγμα από τις συσκευές δικτύου μπορεί κανείς να δει log files, rooting table και arp cache, ενώ από τις μνήμες ram προσωρινά δεδομένα. Σε αυτές τις περιπτώσεις πρέπει να υπάρχει πρόνοια ούτως ώστε να μην χαθεί η ηλεκτροδότηση μέχρι να ληφθούν τα δεδομένα και να αποθηκευτούν σε μη πτητικές μνήμες όπου τα δεδομένα δεν χάνονται με την διακοπή παροχής ρεύματος.

- Εξέταση (Examination)

  Σε αυτή την φάση εξετάζονται τα δεδομένα μέσω τον ειδικών εργαλείων που μπορούν να εξάγουν τα δεδομένα που χρειάζονται. Επειδή συχνά υπάρχει η πιθανότητα ενός κακόβουλου λογισμικού, γι'αυτό εδώ εμπλέκεται και το βήμα της συντήρησης, γιατί αν δεν προφυλαχτούν

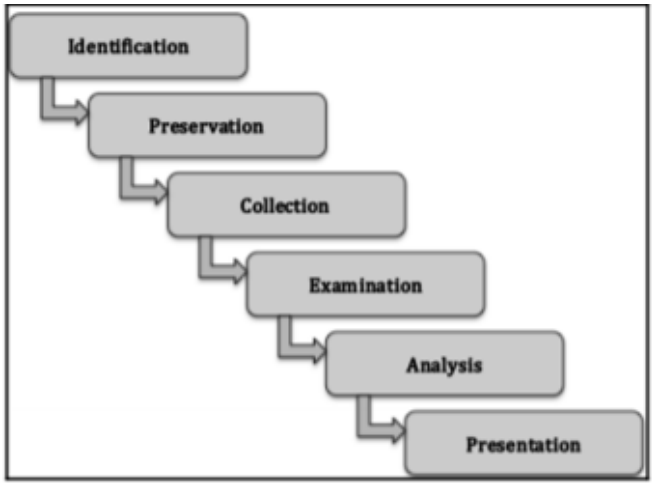
σωστά τα δεδομένα μπορεί να αποβούν μη επαρκή στοιχεία για το δικαστήριο λόγω μη βέβαιης ακεραιότητας.

- Ανάλυση (Analysis)

  Αφού εξεταστούν τα δεδομένα γίνεται μια σχετική ομαδοποίηση ανάλογα με τα ευρήματα. Αν δηλαδή βρέθηκαν ίχνη κακόβουλου λογισμικού αυτά μπαίνουν σε μια στήλη, αν υπήρχαν τεκμήρια που μπορούν να βοηθήσουν στην υπόθεση κατατάσσονται σε άλλη στήλη, όπως επίσης και αν έχει βρεθεί κάποια αδυναμία για ανάκτηση ενός αρχείου, ή ακόμα και τα κατεστραμμένα αρχεία που πιθανόν να μπορούσαν να βοηθήσουν στη σωστή τεκμηρίωση της υπόθεσης.

- Παρουσίαση (Presentation)

  Σε αυτή την φάση ο υπεύθυνος της υπόθεσης πρέπει να έχει καταγράψει με λεπτομέρεια και σαφήνεια στην αναφορά του την κάθε ενέργεια που έχει γίνει για την εξαγωγή τον δεδομένων χωρίς να εκφέρει κάποια προσωπική άποψη. Πρέπει επίσης να κατατεθούν όλα τα δεδομένα με την σειρά κατά την οποία έχουν βρεθεί καθώς και την χρονική στιγμή. Σημαντικό στην κατάθεση στοιχείων είναι τα δεδομένα να μιλούν από μόνα τους χωρίς να πλαισιώνονται από μεροληπτικά λόγια.



Εικόνα 2.1 Στάδια εκτέλεσης αντιμετώπισης μιας κυβερνοεπίθεσης

2.1.1 Ανάλυση μοντέλου Systematic Digital Forensic Investigation

Στην προηγούμενη ενότητα αναλύθηκε το σχήμα/μοντέλο Digital Forensics Research Workshop, το οποίο φαίνεται να είναι χρήσιμο για την ανάλυση μιας κυβερνοεπίθεσης. Στη συνέχεια θα αναλυθεί ένα άλλο μοντέλο, το μοντέλο Systematic Digital Forensic Investigation Model (SRDFIM), το οποίο έχει ώς στόχο να αντιμετωπίσει αδυναμίες που προκύπτουν από άλλα μοντέλα της ψηφιακής εγκληματολογικής πληροφορικής. Είναι εμπνευσμένο από το μοντέλο του μη κερδοσκοπικού οργανισμού DFRWS που ασχολείται με την πάταξη του ψηφιακού εγκλήματος και τις αναδυόμενες προκλήσεις. Σύμφωνα με τους Kruse και Heiser, η εγκληματολογια στην επιστημη των υπολογιστων και δικτυων περιλαμβάνει τρεις βασικούς άξονες για τη δικανική διευρεύνηση [17]:

- Ανάκτηση των αποδεικτικών στοιχείων διασφαλίζοντας παράλληλα τη διατήρηση της ακεραιότητας.
- Έλεγχος ταυτότητας της εγκυρότητας των ανακτημένων δεδομένων, ότι δηλαδή είναι ίδια με τα πρότυπα

- Ανάλυση των δεδομένων διατηρώντας παράλληλα την ακεραιότητά τους.

Η ανάλυση πλαισίων του μοντέλου Systematic Digital Forensic Investigation Model (SRDFIM) περιλαμβάνει τα ακόλουθα [18]:

1) Προπαρασκευή (Preparation)

   Σε αυτό το πρώτο πλαίσιο γίνεται η προετοιμασία πριν από την διεξαγωγή της έρευνας, η οποία συμπεριλαμβάνει την κατανοήση της φύσης του εγκλήματος και των ενεργειών που έχουν προκύψει, καθώς και την ετοιμασία εξοπλισμού για την περισυλλογή των αποδεικτικών στοιχείων. Γενικά προτείνεται να γίνεται η καλυτερη δυνατή προμετοιμασία πριν την μετάβαση στο χώρο του εγκλήματος.

- Διασφάλιση του χώρου (Secure the Scene)

  Το δευτερο πλαίσιο ασχολείται κυριως με την διασφάλιση του χώρου του εγκλήματος και τη μετατροπή του σε έναν ασφαλή χώρο όπου μόνο εξουσιοδοτημένα άτομα μπορούν να έχουν προσβαση. Επίσης χρειάζεται να αποκλειστεί περιμετρικά ο χώρος που υπάρχουν πιθανά τεκμήρια. Αξιοσημείωτο είναι ότι όσο περισσότεροι έχουν εξουσιοδότηση για πρόσβαση στο χώρο τόσο μεγαλύτερος κίνδυνος υπάρχει να χαθούν ή να καταστραφούν πιθανά τεκμήρια.

- Έλεγχος και αναγνώριση (Survey and Recognition)

  Αυτό το πλαίσιο περιλαμβάνει τον προσδιορισμό πιθανών αποδεικτικών στοιχείων καθώς και το πλάνο εξατομικευμένων αναζητήσεων βάσει των στοιχείων που έχουν βρεθέι. Για παράδειγμα σε περίπτωση που βρεθεί μια έξυπνη κινητή συσκευή, πηγή δεν είναι μόνο η ίδια η συσκευή αλλά και περιφεριακά αντικείμενα όπως κάρτες μνήμης, καλώδια. Δεδομένου μάλιστα ότι αυτές οι συσκευές συγχρονίζονται εύκολα με τους υπολογιστές, μπορούν να βρεθούν και στοιχεία στους υπολογιστές. Ακόμη, αν βρεθεί ηλεκτρονικός εξοπλισμός που δεν μπορεί να εξεταστεί με τον υπάρχοντα εξοπλισμό, μπορεί να ζητηθεί εξιδεικευμένη βοήθεια για τον έλεγχο της. Ακολούθως χρειάζεται οι κάτοχοι των ύποπτων συσκευών να ανακριθούν για να δώσουν περαιτέρω πληροφορίες για την ανάλυση των συσκευών. Τέλος πρέπει να εκδοθούν εντάλματα για την περισυλλογή συσκευών/τεκμηρίων.

- Τεκμηρίωση (Documenting the Scene)

  Μετά τον προσδιορισμό των πιθανών αποδεικτικών στοιχείων, δημιουργείται ένα σύνολο εγγράφων για την τεκμηρίωση, την περιγραφή και χαρτογράφηση της σκηνής του εγκλήματος. Όλες οι ηλεκτρονικές συσκευές που περισυλλέχθηκαν πρέπει να φωτογραφίζονται μαζί με τροφοδοτικά καλώδια και ότι άλλα αξεσουάρ βρέθηκαν. Αν η συσκευή βρέθηκε αναμμένη αυτό πρέπει να αναφερθεί. Γενικώς πρέπει όλα τα δεδομένα που έχουν μαζευτεί να περιγράφονται και να αναλύονται επαρκώς καθώς θα παρουσιαστούν στο δικαστήριο αρκετούς μήνες μετά. Επίσης είναι απαραίτητο να διατηρείται ιστορικό όσων ήταν παρόντες στη σκηνή, με λεπτομέρειες όπως ώρα και μέρα. Ακόμη, συστήνεται η δημιουργία ενός πίνακα όπου εμφανίζονται οι κατηγορίες των ατόμων που ενεπλάκησαν στην υπόθεση, όπως θύματα, ύποπτοι παρευρισκόμενοι μάρτυρες και ερευνητές.

- Ασπίδα επικοινωνίας (Communication Shielding)

  Το πέμπτο πλαίσιο πραγματοποιείται πριν από τη συλλογή αποδεικτικών στοιχείων. Σε αυτό το στάδιο κάθε επικοινωνία που μπορεί να πραγματοποιηθεί από τη συσκευή τερματίζεται. Ακόμη και αν μια συσκευή βρίσκεται σε ανενεργή φάση, εφαρμογές όπως wifi και Bluetooth μπορεί

να είναι ενεργοποιημένες. Αυτό μπορεί να προκαλέσει την εγγραφή άλλων πληροφορίων ή ακόμα και παραποίηση των ήδη υπαρχόντων. Σε περίπτωση που μια συσκευή είναι συνδεδεμένη με των υπολογιστή πιθανόν να συγχρονίζει με τον υπολογιστή αυτό, κάτι που πάλι μπορεί να αλλοιώσει τα αποδεικτικά στοιχεία. Επομένως η καλύτερη επιλογή μετά την κατάσχεση μιας συσκευής είναι η απομόνωση της.

2) Συλλογή τεκμηρίων (Evidence Collection)

Η συλλογή αποδεικτικών στοιχείων από τις ηλεκτρονικές συσκευες είναι ένα από τα σημαντικότερα σημεία και απαιτεί συγκεκριμένες διαδικασίες για υπάρχει εγκυρότητα. Η συλλογή των αποδεικτικών στοιχείων χωρίζεται σε δύο κατηγορίες: α) Συλλογή πτητικών στοιχείων και β) Συλλογή μη πτητικών στοιχείων

6.1 Συλλογή πτητικών στοιχείων (Volatile Evidence Collection): Η πλειονότητα των αποδεικτικών στοιχείων συνήθως είναι πτητικής φύσεως. Γι' αυτό τον λόγο υπάρχει και το δίλημμα κατά πόσον πρέπει η συλλογή των δεδομένων να γίνει στη σκηνή του εγκλήματος την ίδια ώρα ή πιο μετά σε ασφαλές εργαστήριο, με τον κίνδυνο να χαθούν δεδομένα, αφου η τρέχουσα κατάσταση του υπολογιστή θα έχει αλλάξει.

6.2 Συλλογή μη πτητικών στοιχείων (Non-Volatile Evidence Collection): Αυτής της μορφής αποδεικτικά στοιχεία συλλέγονται από εξωτερικά μέσα αποθήκευσης που υποστηρίζονται από αυτές τις συσκευές, όπως για παράδειγμα οι ασφαλείς ψηφιακές καρτες αποθηκευσης SD. Για τη συλλογή αυτών των δεδομένων χρειάζονται τα κατάλληλα εργαλεία, ούτως ώστε να διασφαλιστεί η ακεραιότητα τους και να γίνονται αποδεκτά στο δικαστήριο.

- Διατήρηση (Preservation):

Στο έβδομο πλαίσιο περιλαμβάνεται η συσκευασία, η μεταφορά και η αποθήκευση. Η διαδικασία που ακολουθείται πρέπει να τεκμηριώνεται σωστά και να καταγράφεται για την εξασφάλιση ότι οι ηλεκτρονικές αποδείξεις δεν έχουν τροποποιηθεί ή καταστραφεί. Για την συσκευασία και μεταφορά χρησιμοποιούνται πάντα αντιστατικές σακούλες για την αποφυγή δημιουργίας στατικού ηλεκτρισμού. Ακόμη οι αντιστατικές σακούλες σφραγίζονται και τοποθετούνται μέσα σε ένα ειδικό φάκελο με σύντομη περιγραφή του τι περιέχει η κάθε σακούλα. Η αποθήκευση τους γίνεται σε σημείο που προστατεύεται από ακτινοβολίες, σκόνη, θερμότητα και υγρασία, ενώ σε αυτό τον χώρο έχουν πρόσβαση μόνο άτομα με εξουσιοδότηση.

- Εξέταση (Examination):

Σε αυτή το πλαίσιο πραγματοποιείται η εξέταση του περιεχομένου των αποδεικτικών στοιχείων που έχουν περισυλλεχθεί από την εκάστοτε εγκληματολογική ομάδα. Πριν την εξέταση όμως των αποδεικτικών στοιχείων πρέπει να έχει ήδη δημιουργηθεί ένα αντίγραφο ασφαλείας. Σημασία κατά την εξέταση έχει τα στοιχεία να μπορούν να βοηθήσουν στην εξιχνίαση της υπόθεσης. Συνήθως πριν την εξέταση των δεδομένων γίνεται ένα φιλτράρισμα από τον τεράστιο όγκο που συνήθως συλλέγεται από τα πτητικά και μη πτητικά μέσα αποθήκευσης. Στόχος του φλιταρίσματος είναι ο εντοπισμός ύποπτων στοιχείων. Συνήθως ύποπτα στοιχεία εντοπίζονται στα γραπτά και φωνητικά μηνύματα, καθώς και στα έγγραφα ηλεκτρονικού ταχυδρομείου. Στην εύρεση αυτών των δεδομένων σημαντικό ρόλο παίζουν και οι εφαρμογές που χρησιμοποιούνται, αφού οι σύγχρονες εφαρμογές καταγράφουν δεδομένα όπως χρονολογία, ώρα και ημερομηνία, ενώ εγγυούνται και εγκυρότητα δεδομένων, καθώς και το ότι δεν έχουν τύχει τροποποιήσεων.

3) Ανάλυση (Analysis):

   Μετά την εξέταση των αποδεικτικών στοιχείων γίνεται μια τεχνική ανασκόπηση που διενεργείται με βάση τα αποτελέσματα της εξέτασης των στοιχείων και με στόχο την εύρεση και κατανόηση της συνοχής μεταξύ των δεδομένων. Ακόμα ένας από τους στόχους αυτού του πλαισίου είναι η δημιουργία ενός χρονολογίου των συμβάντων. Μετά βέβαια μπορεί να προκύψει η ανάγκη για περισσότερα στοιχεία που πιθανόν να χρειαστούν για να κατανοηθούν καλύτερα τα ήδη υπάρχοντα.

- Παρουσίαση (Presentation):

  Τα αποτελέσματα πολύ πιθανόν να παρουσιαστούν σε ένα ευρύ κοινό, όπως λειτουργούς του νόμου, εμπειρογνώμονες, νομικούς και απλούς πολίτες. Ανάλογα με το έγκλημα που έχει διαπραχθεί το πόρισμα θα δημοσιοποιηθεί στο δικαστήριο ή στη διοίκηση της εταιρίας, αν επρόκειτο για εσωτερική έρευνα. Στόχος σε αυτό το πλαίσιο είναι η επιβεβαίωση ή η απόρριψη ισχυρισμών και καταγγελιών. Συχνά τα αποτελέσματα μπορεί να μην εξάγονται με απόλυτη βεβαιότητα ή να μην μπορούν να σχηματίσουν την πλήρη εικόνα, αλλά να δίνουν ένα πιθανό σενάριο. Επίσης πρέπει να δημιουργηθεί και μια πλήρης περιγραφική έκθεση που να υποδεικνύει από την αρχή μέχρι το τέλος τις διαδικασίες που έχουν γίνει.

- Αποτελέσματα και επανεξέταση (Result and Review):

  Το τελικό στάδιο περιλαμβάνει μια αναθεώρηση που επαναλαμβάνει όλα τα βήματα που έχουν γίνει στην έρευνα και το τι έχει εντοπιστεί σε αυτή, καθώς και πού θα μπορούσε να υπάρξει καλύτερη διαχείριση. Στόχος είναι αυτές οι πληροφορίες να συμβάλουν στην καθιέρωση καλύτερων πρακτικών και διαδικασιών για μελλοντικές υποθέσεις.

2.1.2 Ανάλυση Μοντέλου Abstract Digital Forensic

Ένα άλλο μοντέλο είναι το μοντέλο Abstract Digital Forensic, το οποίο αποτελείται από τα ακόλουθα εννιά βήματα τυποποιημένων διαδικασιών [19]:

1) Αναγνώριση (Identification):

   Στο πρώτο βήμα γίνεται μια αναγνωριστική έρευνα για καθορισμό του είδους του εγκλήματος.

2) Προπαρασκευή (Preparation):

   Στην δεύτερη φάση γίνεται μια προετοιμάσια εξοπλισμού, ειδικών μονάδων και ενταλμάτων αν κριθεί αναγκαίο, αφού έχει γινει η αναγνωριστική έρευνα.

3) Προσέγγιση (Approach strategy):

   Σε αυτό το σημείο δημιουργείται μια στρατηγική για τον τρόπο με τον οποίο θα γίνει συλλογή των δεδομένων, επιδιώκοντας τη μέγιστη πιθανότητα συλλογής όσο το δυνατόν περισσότερων ύποπτων δεδομένων και την εγγύηση της εγκυρότητάς τους.

4) Διατήρηση (Preservation):

   Το τέταρτο βήμα περιλαμβάνει την απομόνωση ,διασφάλιση και διατήρηση της ακεραιότητας των δεδομένων.

5) Συλλογή (Collection):

Με αποδεδειγμένες διαδικασίες διασφάλισης της ακεραιότητας των στοιχείων, γίνεται δημιουργία ασφαλούς αντιγράφου και λεπτομερής καταγραφή όλων διαδικασιών.

6) Εξέταση (Examination):

Μετά και τη δημιουργία των ασφαλών αντιγράφων, γίνεται μια ενδελεχής έρευνα για αναζήτηση αποδεικτικών στοιχείων που σχετίζονται με την υπόθεση.

7) Ανάλυση (Analysis):

Αφού έχουν γίνει οι έρευνες για τα αποδεικτικά στοιχεία με βάση τα ευρήματα, εξάγονται συμπεράσματα σχετικά με την υπόθεση.

8) Παρουσίαση (Presentation):

Παρουσίαση των συμπερασμάτων μαζί με λεπτομερή επεξήγηση.

9) Επιστροφή τεκμηρίων (Returning evidence):

Επιστροφή του εξοπλισμού του στον ιδιοκτήτη μετά την έρευνα της υπόθεσης.

2.1.3 Ανάλυση μοντέλου Integrated Digital Investigation(IDIP)

Οι Brian Carrier και Eugene Spafford [20] διαμόρφωσαν ένα ακόμη μοντέλο για την καταπολέμηση του ψηφιακού εγκλήματος, το οποίο αποτελείτε από τα ακόλουθα πεδία:

1) Ετοιμότητα (Readiness):

Στόχος του πρώτου πεδίου είναι η διασφάλιση ότι τόσο ο εξοπλισμός αλλα και οι υποδομές και το προσωπικό είναι απόλυτα έτοιμο και λειτουργικό για διεκπεραίωση μιας έρευνας.

2) Ανάπτυξη (Deployment):

Το δεύτερο πεδίο χωρίζεται σε δύο φάσεις

i. Πρώτο βήμα: όταν συμβεί ένα περιστατικό ειδοποιείται το εκάστοτε ειδικό κλιμάκιο
ii. Δεύτερο βήμα: γίνεται επιβεβαίωση του περιστατικού και διασφαλίζεται εξουσιοδότηση για εκκίνηση της έρευνας

- Διερεύνηση της σκηνής του εγκλήματος (Physical Crime Scene Investigation):

Το τρίτο πεδίο έχει ως στόχο την συλλογή και ανάλυση των τεκμηρίων και χωρίζεται σε έξι φάσεις:

- Οριοθέτηση της σκηνής του εγκλήματος για την συλλογή και εντοπισμό τεκμηρίων
  i. Έρευνα και εντοπισμός από εξιδεικευμένο προσωπικό για εντοπισμό και συλλογή των φυσικών αποδεικτικών στοιχείων
  ii. Λήψη φωτογραφικού υλικού, βίντεο και γενικά καταγραφή όσο το δυνατόν περισσότερων πληροφορίων που σχετίζονται για την υπόθεση
  iii. Σε βάθος έρευνα για οποιαδήποτε φυσική συσκευή η τεκμήριο
  iv. Οργάνωση και ανάλυση των αποτελεσμάτων για την ανάπτυξη μιας θεωρίας για το περιστατικό.
- Παρουσίαση ψηφιακών και φυσικών στοιχείων στο δικαστήριο ή στην εταιρία, αν επρόκειτο για εσωτερική έρευνα.
- Αντίστοιχα αν πρόκειται για ψηφιακά δεδομένα χρησιμοποιείται η πιο κάτω ακολουθία σε έξι φάσεις:
  i. Συντήρηση της ψηφιακής εγκληματικής σκηνής για συγχρονισμό και αργότερα για περαιτέρω ανάλυση και εντοπισμό αποδείξεων

ii. Μεταφορά των σχετικών ύποπτων δεδομένων σε ένα ελεγχόμενο και ασφαλές χώρο για ανάλυση
iii. Ανάλυση των ψηφιακών στοιχείων και καταγραφή τους.
iv. Μια εις βάθος ανάλυση των ψηφιακών ευρημάτων μέσω ειδικών προγραμμάτων που έχουν δυνατότητες όπως αποκάλυψη κρυφών, διαγραμμένων, κατεστραμμένων αρχείων, συμπεριλαμβανομένου και δεδομένων όπως ημερομηνία δημιουργίας και εκτέλεσης.
v. Σε αυτή τη φάση γίνεται μια ένωση των ευρημάτων στην προσπάθεια να προχωρήσει η έρευνα

- Παρουσίαση των ευρημάτων στο δικαστήριο ή στην εταιρία, αν επρόκειτο για εσωτερική έρευνα

2.2. Παράδειγμα περίπτωσης προσέγγισης δεδομένων

Ένα παράδειγμα προσέγγισης δεδομένων από προσωπικό ηλεκτρονικό υπολογιστή περιλαμβάνει τα ακόλουθα [21]:

Αν είναι σε σύνδεση με router/modem γίνονται τα εξής:

- Δεν γίνεται ξεκίνημα του υπολογιστή με στόχο να εντοπιστούν αποδείξεις, αλλά φωτογράφηση του υπολογιστή από όλες τις πλευρές καθώς και με όλες τις συνδεδεμένες συσκευές
- Αν η οθόνη του υπολογιστή δείχνει οτιδήποτε το φωτογραφίζουμε
- Αν είναι σε κατάσταση αδράνειας κουνάμε το ποντίκι ή πατάμε το κουμπί space για αλλαγή της κατάστασης και φωτογραφίζουμε αυτό που θα μας δείξει
- Αφαιρούμε το καλώδιο παροχής ηλεκτροδότησης στον υπολογιστή, ενώ αν είναι φορητός υπολογιστής αφαιρούμε την μπαταρία
- Αφαίρεση όλων τον καλωδίων και αναφορά για το καθένα
- Καταγραφή όλων των βημάτων λεπτομερώς
- Κατά την μεταφορά σε ασφαλή χώρο ανάλυσης, ο υπολογιστής πρέπει να είναι μακριά από μαγνήτες, συσκευές που εκπέμπουν ραδιοκύματα και άλλα πιθανά αντικείμενα που μπορεί να προκαλέσουν ζημιά

Προσέγγιση δεδομένων από Κινητές Έξυπνες Συσκευές

- Καταγραφή των διαθέσιμων συσκευών
- Αναγνώριση αν η συσκευή είναι σε λειτουργία ή απενεργοποιημένη (λαμπτήρες ένδειξης ειδοποιήσεων, δονήσεις, ήχοι, θερμοκρασία)
- Αν η συσκευή είναι απενεργοποιημένη να μην μπει σε λειτουργία
- Αν είναι σε λειτουργία πράττουμε τα εξής με προσοχή:
    - Απομόνωση από τηλεφωνικά και τοπικά δίκτυα
    - Ανάκτηση κωδικών ασφαλείας για την διεκπεραίωση ψηφιακής ανάλυσης
- Το καλύτερο είναι η συσκευή να παραμείνει ανοικτή χωρίς να κλείνει η οθόνη, με απενεργοποιημένη ασφάλεια και σε λειτουργία πτήσης, μέχρι να φτάσει στα εργαστήρια για περαιτέρω ανάλυση
- Συνήθως στις κινητές συσκευές γίνεται συλλογή από δακτυλικά αποτυπώματα, γι' αυτό πρέπει να αποφεύγεται η παραμόρφωση ή αλλοίωση αυτών των στοιχείων

2.3. Αποδεικτικά στοιχεία

Αποδεικτικά στοιχεία θεωρούνται τα δεδομένα που αναπαριστούν οτιδήποτε μπορεί να υποδείξει μια κατάσταση ή μια ενέργεια που έχει γίνει ή συμβαίνει. Η καταγραφή αυτών μπορεί να γίνει και

χειρόγραφα και ηλεκτρονικά. Η χειρόγραφη μορφή είναι πολύ πιο μικρή σε κόστος σε σύγκριση με την ψηφιακή. Αναπαρίσταται σε ένα ειδικά διαμορφωμένο χαρτί που είναι χωρισμένο σε πεδία για την καλύτερη διατύπωση. Αν και το κόστος στην περίπτωση αυτή είναι χαμηλότερο, χαμηλότερος είναι και ο δείκτης εμπιστευτικότητας, αφού ο εκάστοτε υπεύθυνος που πρέπει να γράψει την αναφορά μπορεί να κάνει λάθη που μπορεί να καταστήσουν τα στοιχεία μη έγκυρα [22]. Η ηλεκτρονική μορφή από την άλλη χωρίζεται σε δυο υποκατηγορίες: την υλική καταγραφή και τη λογισμική καταγραφή. Στην υλική καταγραφή χρειάζεται κάποιος εξοπλισμός από ειδικές συσκευές και ηλεκτρονικούς υπολογιστές με κύρια χαρακτηριστικά μεγάλη RAM(32GB+) και αρκετό αποθηκευτικό χώρο(2TB+). Επίσης χρειάζεται ειδικά διαμορφωμένος χώρος για το εργαστήριο, με πρόσβαση μόνο στα εξουσιοδοτημένα άτομα. Τέλος απαιτείται ένα Physical write blocker (Εικόνα 2.2). Αυτή η συσκευή επιτρέπει την σύνδεση μεταξύ του σκληρού δίσκου που θεωρείται ως αποδεικτικό στοιχείο και της συσκευής. Η συσκευή αυτή εγγυάται ότι υπάρχει καθαρός χώρος αποθήκευσης χωρίς οτιδήποτε επιπλέον, όπως για παράδειγμα μια συσκευή usb η οποία μπορεί να έχει διάφορα αρχεία [23].

Εικόνα 2.2 Physical Write Blocker

Η λογισμική καταγραφή προσφέρει μια πληθώρα από επιλογές προγραμμάτων για τη διεκπεραίωση της ανάκτησης των δεδομένων. Τέτοια προγράμματα που προσφέρουν δωρεάν αυτές τις λειτουργίες είναι τα ακόλουθα:

Paladin (Εικόνα 2.3):

Διαθέσιμο για τα λειτουργικά Linux, είναι σουίτα που προσφέρει αρκετά εργαλεία βοηθητικά για το ψηφιακό έγκλημα, όπως ανάλυση κακόβουλου λογισμικού για εντοπισμό επικίνδυνων αρχείων, κρυπτογράφηση για διασφάλιση της ακεραιότητας των δεδομένων, και imaging για ασφαλές αντίγραφο δεδομένων της συσκευής [24].

Εικόνα 2.3 Στιγμιότυπο από την σουίτα Paladin v.7

SANS SIFT (Εικόνα 2.4):

Ακόμα μια σουίτα διαθέσιμη στα λειτουργικά συστήματα Linux, η οποία προσφέρει ανάλυση μνήμης για εντοπισμό ύποπτων δεδομένων, καταγραφές, imaging για ασφαλές αντίγραφο δεδομένων της συσκευής. Προσφέρεται σαν μια αυτόνομη virtual machine στον πιο κάτω σύνδεσμο δωρεάν και αποδικνύει ότι προηγμένες δυνατότητες για ανταπόκριση σε ένα περαστατικό μπορούν να υπάρξουν και στα προγράμματα ανοικτού κώδικα: https://digital-forensics.sans.org/community/downloads Προσφέρεται και στα λειτουργικά linux, ενώ μπορεί να αποκτηθεί από το τερματικό με την παρακάτω εντολή: wget –quiet -O – https://raw.github.com/sans-dfir/sift-bootstrap/master/bootstrap.sh | sudo bash -s -- -I -s -y[25].

Εικόνα 2.4 Στιγμιότυπο από την σουίτα SANS SIFT

2.4. Προβλεπόμενη εργαλειοθήκη κατά την αντιμετώπιση ενός συμβάντος

Στις περισσότερες περιπτώσεις όταν σε μια εταιρία προκύψει ένα περιστατικό, η ομάδα ανταπόκρισης ενεργεί μέσα στον χώρο της εταιρίας, εκτός αν κριθεί αναγκαίο να γίνει μεταφορά της ομάδας σε άλλο χώρο. Συνήθως τέτοιες περιπτώσεις είναι πιο συχνές στην περίπτωση της δίωξης ηλεκτρονικού εγκλήματος. Γι' αυτό το κιτ που προτείνετε να κουβαλάει το προσωπικό για την εκτέλεση των απαραίτητων ενεργειών κατά την διάρκεια ενός συμβάντος πρέπει να περιέχει τα ακόλουθα εργαλεία:

- Δικανικός υπολογιστής: Ένας φορητός υπολογιστής με μεγάλη RAM για την δημιουργία imaging γρήγορα. Επίσης ο υπολογιστής πρέπει να έχει τουλάχιστον μια σουίτα από εγκληματολογικά εργαλεία
- Διαδικτυακά Καλώδια: Να υπάρχουν διαθέσιμα καλώδια τύπου CAT5 με διάφορα μήκη, για την πραγματοποίηση μιας ενημέρωσης σε οποιοδήποτε router, switch
- Physical Write Blocker: Κάθε προβλεπόμενη εργαλειοθήκη πρέπει να έχει έναν Physical write Blocker για την μεταφορά και μετέπειτα ανάλυση των δεδομένων
- Bootable USB: Αν και σπάνια μπορεί να χρησιμοποιηθεί, καλό είναι να υπάρχει για την εκκίνηση Linux για εκτέλεση εγκληματολογικών εφαρμογών
- Anti-static bags: Σε περίπτωση κατάσχεσης σκληρών δίσκων, οι μεταφορά τους πρέπει να γίνεται σε αντιστατικούς σάκους [26].

2.5. Διαδικτυακές συσκευές και τεκμήρια

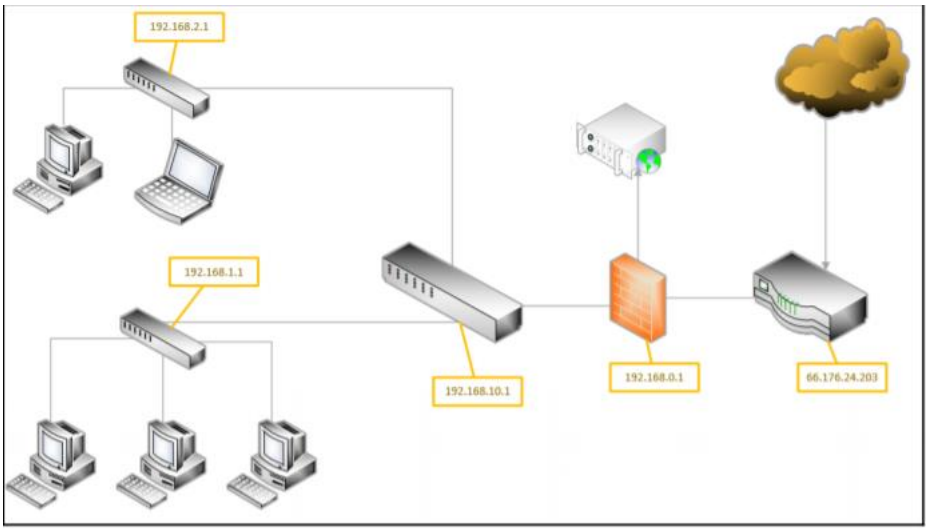
Ένας γνώστης της εγκληματολογικής πληροφορικής γνωρίζει καλά ότι σε ένα εμπλεκόμενο υπολογιστή υπάρχουν συγκεκριμένοι χώροι στο λογισμικό όπου εντοπίζονται αποτυπώματα. Πέραν όμως από το

περιβάλλον του υπολογιστή υπάρχουν και τεκμήρια στις διαδικτυακές συσκευές όπως routers και switches. Επομένως, η ομάδα που ανταποκρίνεται σε αυτά τα περιστατικά πρέπει να γνωρίζει πώς να εντοπίζει αυτές τις χρήσιμες πληροφορίες, σε διαδικτυακές συσκευές όπως τις ακόλουθες:

- Switches: Συσκευές που λειτουργούν κυρίως στο εσωτερικό του δικτύου. Δεδομένα υπάρχουν στον πίνακα CAM (Content addressable memmory). Εδώ εντοπίζεται η αντιστοίχιση των ports του switch στην αντίστοιχη άλλη πλευρά του καλωδίου που βρίσκεται η NIC (Network Interface Card) της αντίστοιχης συσκευής που είναι συνδεδεμένη.
- Routers: Οι Δρομολογητές επιτρέπουν τα LAN να διασυνδέονται μεταξύ τους, με αποτέλεσμα να χειρίζονται μεγάλα ποσοστά κίνησης του διαδικτύου. Το βασικό πεδίο που μπορεί κάποιος να εντοπίσει χρήσιμες πληροφορίες είναι στο rooting table. Αυτός ο πίνακας κρατάει πληροφορίες σχετικά με φυσικές θύρες που έχει και σε ποια δίκτυα ανήκουν, καθώς και πού δρομολογούνται τα πακέτα ανάλογα με τον προορισμό.
- Firewalls: Τα Firewalls άλλαξαν πάρα πολύ από τον καιρό που απλά θεωρούνταν ως διαφορετικού τύπου routers. Τα Firewalls νέας γενιάς προσφέρουν μια μεγάλη ποικιλία χαρακτηριστικών όπως ανίχνευση και πρόληψη μιας επίθεσης, φιλτράρισμα στο διαδίκτυο από μη έμπιστες σελίδες, πρόληψη απώλειας δεδομένων και απαγόρευση σελίδων που είναι αναγνωρισμένες ως επικίνδυνες. Επίσης κρατούν λεπτομερές αρχείο καταγραφών όλων των συμβάντων.

2.6. Packet Capture

Η Δυνατότητα καταγραφής της κίνησης του δικτύου είναι ζωτικής σημασίας για την πλήρη καταγραφή και κατανόηση ενός περιστατικού. Με την παρακολούθηση μπορούν να συγκεντρωθούν περισσότερες λεπτομέρειες σχετικά με τον τύπο του κακόβουλου λογισμικού που ενδέχεται να έχει μολύνει τον χρήστη. Σε άλλες περιπτώσεις μπορεί να εντοπιστεί η κινητικότητα των ύποπτων χρηστών και να γίνει παρακολούθηση πακέτων που στέλνονταν και λαμβάνονταν. Ένας τρόπος για την καταγραφή της κίνησης είναι με την επιλογή network tap. Είναι ένα σύστημα ανάμεσα στο χρήστη και το swtich. Σύμφωνα με την Εικόνα 2.5, αν ο host που έχει παραβιαστεί βρίσκεται στο υποδίκτυο 192.168.1.0/24 το tap (υπολογιστής που κάνει καταγραφή της κίνησης) πρέπει να τοποθετηθεί μεταξύ του host και του switch. Η δεύτερη επιλογή είναι να ρυθμιστεί μια θύρα SPAN (Switch Port Analyzer). Η θύρα που βλέπει στον παραβιασμένο host θα τεθεί σε αυτό το Mode και θα στέλνει όλα τα δεδομένα που πηγαινοέρχονται στην θύρα που έχει οριστεί. Τέλος, μερικές διαδικτυακές συσκευές έχουν ενσωματωμένες εφαρμογές ειδικά γι’ αυτή την ενέργεια. Μια από αυτές τις εφαρμογές είναι και το tcpdump που μπορεί να καταγράφει κίνηση για περισσότερη ανάλυση. Αυτή θεωρείται και η γρηγορότερη τεχνική αφού δεν χρειάζεται η φυσική πρόσβαση στον εξοπλισμό [27].



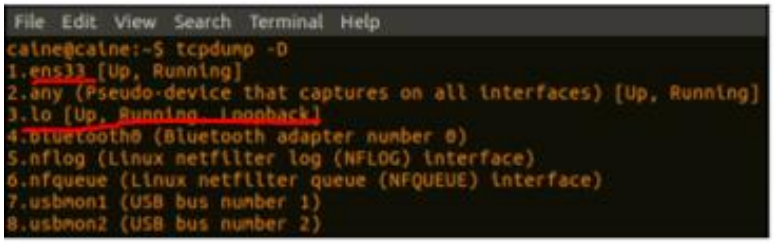
Εικόνα 2.5 Υπόδειγμα δικτύου

2.6.1 TCPDUMP

Το TCPDUMP είναι μια command-line εφαρμογή ειδικά σχεδιασμένη για καταγραφή κίνησης. Συχνά το βρίσκουμε προεγκατεστημένο στα λειτουργικά Linux αλλά υπάρχει και σε πολλές διαδικτυακές συσκευές. Παρακάτω αναφέρονται μερικές από τις πιο σημαντικές εντολές που μπορούν να εκτελεστούν [28]:

Εντολή tcpdump -D

Με αυτή την εντολή φαίνονται οι διαθέσιμες θύρες καταγραφής της κίνησης (Εικόνα 2.6).



Εικόνα 2.6 Εντολές tcpdump

Εντολή sudotcpdump -I ens33

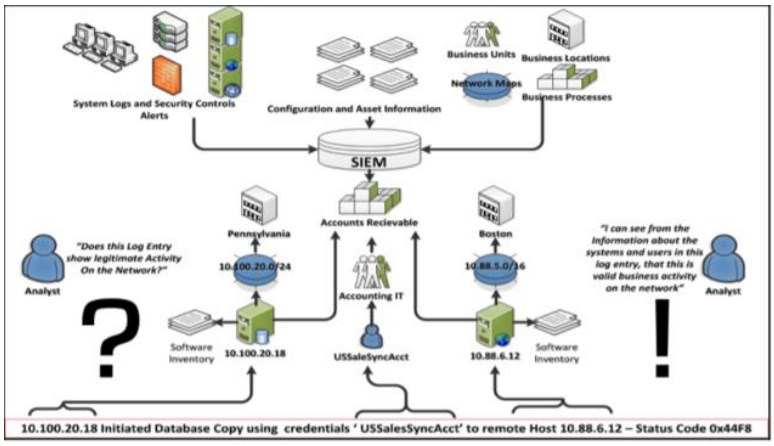
Με αυτή την εντολή ξεκινάει η καταγραφή κίνησης στη θύρα ens33, ενώ με την παράμετρο -i υποδεικνύεται η θύρα. Η καταγραφή των πακέτων είναι ένα βοηθητικό όπλο για την ανακάλυψη των δεδομένων που χρειάζονται. Μια καλή πρακτική είναι να τα δεδομένα να αποθηκεύονται για την ανάλυση τους πιο μετά. Αν υπάρχουν βάσιμες υποψίες για την προέλευση ή άφιξη των κακόβουλων δεδομένων, μπορεί να γίνει παρακολούθηση συγκεκριμένων διευθύνσεων με τις πιο κάτω εντολές, αφού κάποιες φορές άτομα παρέχουν δεδομένα σε άλλα άτομα χωρίς εξουσιοδότηση.

- Sudotcpdump -I ens33 src host 192.168.10.54 (για πακέτα που παραλαμβάνονται)
- Sudotcpdump -I ens33 dst host 192.168.10.54 (για πακέτα που στέλνονται)

2.7. SIEM (Security Information and Event Management)

Οι τεχνικές που αναφέρθηκαν πιο πάνω περιλαμβάνουν και ένα μεγάλο μειονέκτημα που έχουν οι διαδικτυακές συσκευές. Ο μεγάλος όγκος των log files πολλές φορές γίνεται roll over. Έτσι γράφονται από πάνω τα καινούργια log files, αφού είναι πάρα πολλά, με αποτέλεσμα αν η εταιρία είναι μεγάλη να

μπορεί να κρατάει δεδομένα μόνο των προηγουμένων ημερών ή ακόμη και μόνο των προηγουμένων ωρών. Γι' αυτό το λόγο δημιουργήθηκε το SIEM. Αυτά τα συστήματα έχουν την δυνατότητα να δέχονται όλα τα log files και να τα αποθηκεύουν σε μια συγκεκριμένη τοποθεσία, πράγμα που τους δίνει περισσότερο χώρο αλλά και ευελιξία, αφού κατά την έρευνα δεν χρειάζεται να ελεγχθούν ξεχωριστά ένα-ένα τα συστήματα αλλά μόνο ο χώρος αποθήκευσης που μπαίνουν τα log files. επίσης, δεν περιορίζονται μόνο στα Log files των διαδικτυακών συσκευών, αφού όπως φαίνεται στην Εικόνα 2.7, λαμβάνονται και log files από βάσεις δεδομένων, όπως είναι για παράδειγμα αλλαγές και προσθήκες/αφαιρέσεις που συμβαίνουν. Έτσι αν για παράδειγμα παραβιάστηκε μια βάση δεδομένων με το SIEM είναι δυνατό να βρεθεί εύκολα από πού δόθηκαν οι εντολές για εκτέλεση οποιασδήποτε ενέργειας [29].



Εικόνα 2.7 Υπόδειγμα ενός ολοκληρωμένου συστήματος SIEM

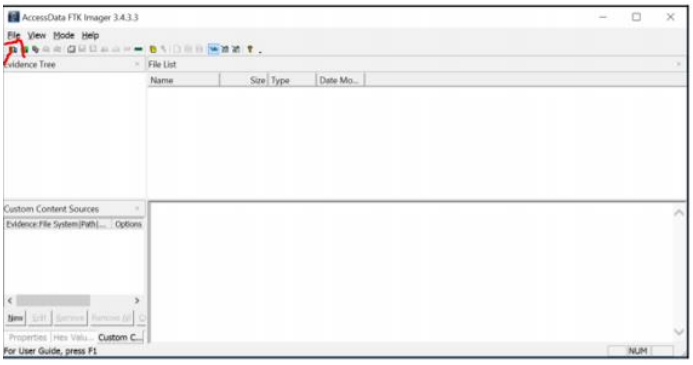
Συνήθως η υλοποίηση ενός τέτοιου συστήματος είναι πολύ ακριβή τόσο στην αγορά όσο και στην εγκατάσταση και την συντήρηση. Παρόλα αυτά, υπάρχουν και υλοποιήσεις ανοιχτού κώδικα όπως αυτή του Security Onion, η οποία καλύπτει ένα μεγάλο φάσμα υπηρεσιών που χρειάζονται αυτά τα συστήματα όπως ανάλυση log files καθώς και πίνακα ελέγχου των διαδικτυακών δραστηριοτήτων [30]. Για εταιρίες που δεν μπορούν να προβούν σε μια πλήρη έκδοση ενός τέτοιου συστήματος αυτή η επιλογή μοιάζει ιδανική, ενώ μπορεί να βρεθεί στον παρακάτω σύνδεσμο https://securityonion.net/

2.8. Ανάκτηση δεδομένων από χρήστες

Αν και δεν είναι συχνό φαινόμενο οι χρήστες να πέφτουν θύματα κακόβουλης επιθέσεις για ανάκτηση δεδομένων, πρέπει ο υπεύθυνος για την περισυλλογή των τεκμηρίων να είναι έτοιμος για την περισυλλογή δεδομένων σε τέτοιες περιπτώσεις. Τέτοιες καταστάσεις συνήθως εμπλέκουν λειτουργικά συστήματα Windows, ενώ στις σύγχρονες εκδόσεις δίνεται η δυνατότητα να εντοπιστεί το ιστορικό των δραστηριοτήτων που έγιναν. Η περισυλλογή δεδομένων μπορεί να γίνει τοπικά αλλά και απομακρυσμένα με τους ακόλουθους τρόπους [31]:

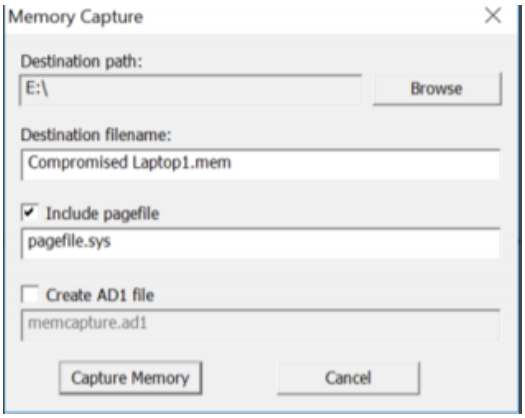
Συλλογή δεδομένων για ανάλυση τοπικά:

Για την συλλογή δεδομένων τοπικά από ένα υπολογιστή που θεωρείται ότι εμπλέκεται, θα πρέπει να χρησιμοποιηθεί USB που έχει προεγκατεστημένα ειδικά προγράμματα όπως το FTK Imager. Αρχικά γίνεται άνοιγμα του προγράμματος, όπως φαίνεται στην Εικόνα 2.8.



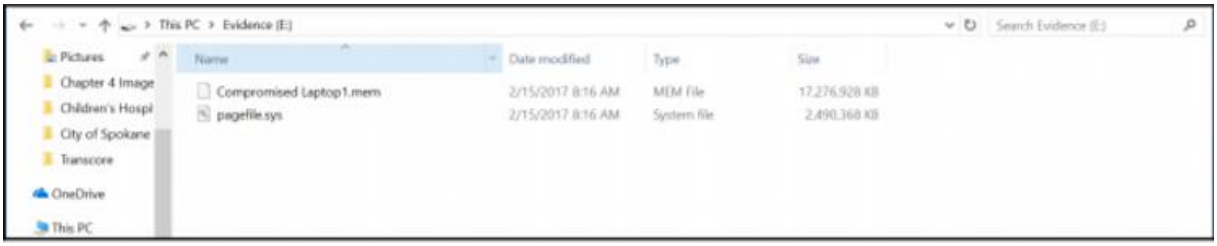
Εικόνα 2.8 Στιγμιότυπο από το πρόγραμμα FTK Manager

Από την επιλογή File επιλέγεται το Capture Memory (Εικόνα 2.9).



Εικόνα 2.9 Επιλογή χώρου αποθήκευσης των αποτελεσμάτων

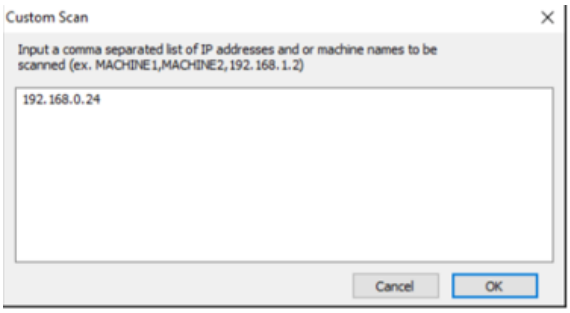
Μόλις τελειώσει η περισυλλογή των δεδομένων, μέσα στον φάκελο προορισμού φαίνεται ότι προστέθηκε ένα αρχείο τύπου .mem (Εικόνα 2.10).



Εικόνα 2.10 Φάκελος προορισμού των αποτελεσμάτων

Συλλογή δεδομένων απομακρυσμένα:

Όταν δεν είναι εφικτή η τοπική μέθοδος, μπορεί να εφαρμοστεί η απομακρυσμένη μέθοδος, η οποία μάλιστα μπορεί να προσφέρει και γρηγορότερη ανταπόκριση παρά της τοπικής. Υπάρχουν βέβαια κάποιες προϋποθέσεις, όπως η προεγκατάσταση του προγράμματος ανάκτησης των δεδομένων της μνήμης. Η απομακρυσμένη συλλογή γίνεται με την χρήση του διαδικτύου. Στο πιο κάτω παράδειγμα έχει χρησιμοποιηθεί το πρόγραμμα F-Response. Κατά την εκκίνηση επιλέγεται η επιλογή Custom Scan. Εδώ προστίθεται η IP του υπολογιστή από τον οποίο πρέπει να ληφθούν τα δεδομένα (Εικόνα 2.11).

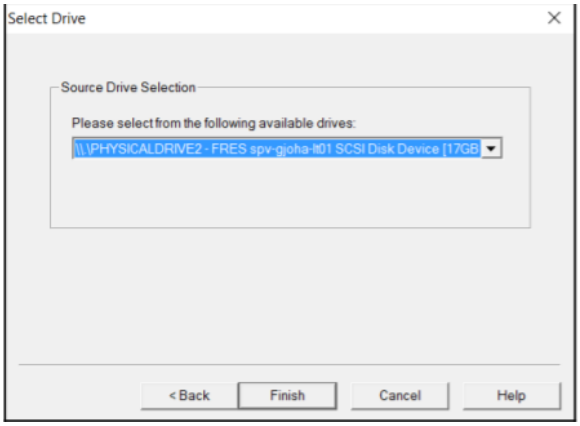


Εικόνα 2.11 Εισαγωγή διευθύνσεις IP για εξαγωγή δεδομένων

Κατά τον εντοπισμό του υπολογιστή, φαίνονται οι διαθέσιμοι αποθηκευτικοί χώροι απ' όπου μπορούν να ανακτηθούν τα δεδομένα, τα οποία στην παρούσα περίπτωση έχουν κατάληξη .pmem

Εικόνα 2.12 Διαθέσιμοι αποθηκευτικοί χώροι που έχουν εντοπιστεί

Στην συνέχεια πρέπει να χρησιμοποιηθεί το πρόγραμμα FTK Imager που χρησιμοποιήθηκε και πριν. Αυτή την φορά θα επιλεγεί από το file η εντολή Create Disk Image και ο δίσκος που αναφέρθηκε πριν (Εικόνα 2.13).



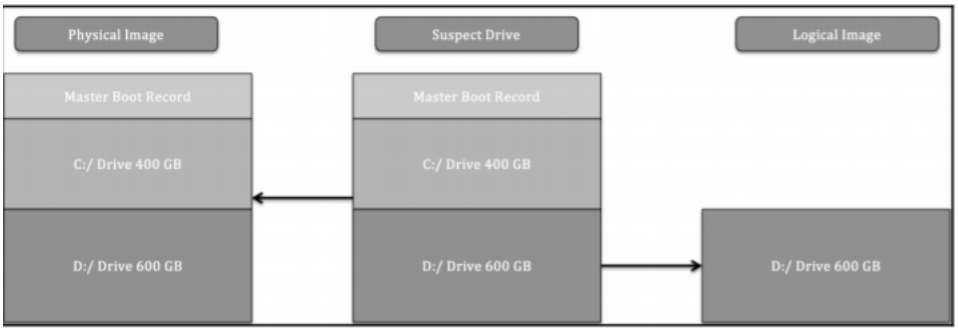
Εικόνα 2.13 Επιλογή δίσκου που θα δημιουργηθεί το image

Κατά το τέλος της ανάκτησης, η εφαρμογή FTK Imager παρέχει και το hash code για το αρχείο που δημιουργηθηκε με τις κρυπτογραφήσεις MD5 και SHA1.

2.9. Imaging

Η καλή κατανόηση των καταστάσεων ενός συμβάντος και τα σωστά βήματα που πρέπει να γίνει για να διασφαλιστεί ότι ο χειρισμός των αποδεικτικών στοιχείων γίνεται σωστά αποτελούν βασικές αρχές της εγκληματολογικές πληροφορικής. Γι' αυτό και στη συνέχεια εξηγείται η διαφορά της αντιγραφής των δεδομένων με το imaging. Η αντιγραφή αρχείων από ένα σκληρό δίσκο σε ένα USB παρέχει μόνο τα δεδομένα που σχετίζονται με αυτά τα αρχεία. Το imaging από την άλλη επιτρέπει τη συλλογή ολόκληρου του σκληρού δίσκου, συμπεριλαμβανομένου και του unlocated space, καθώς και πιθανή πρόσβαση σε διαγραμμένα αρχεία. Επίσης με το imaging επιτρέπεται στην μετέπειτα ανάλυση η διατήρηση των δεδομένων και τα μεταδεδομένα, όπως οι χρονικές σημάνσεις για το πότε

άνοιξε/δημιουργήθηκε/διαγράφηκε ένα αρχείο. Σημαντικό επίσης είναι να εξηγηθεί η διαφορά του logical volume και του Physical Volume. Στην Εικόνα 2.14 φαίνεται ότι με το Logical volume μπορεί να ανακτηθεί μέρος του δίσκου ενώ με το physical volume μπορούν να ανακητθούν όλα τα μέρη του δίσκου.



Εικόνα 2.14 Διαφορές Logical image εναντί Physical image

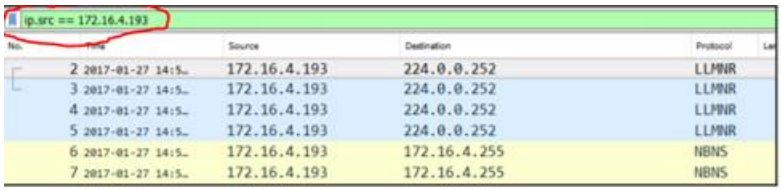
Υπάρχουν δυο διαφορετικές τεχνικές για την δημιουργία imaging. Με την τεχνική του Dead Imaging η συσκευή δεν πρέπει να βρίσκεται σε λειτουργία. Όταν είναι κλειστή αφαιρούνται τα αποθηκευτικά μέσα και παραπέμπονται σε ειδικά διαμορφωμένα εργαστήρια για περαιτέρω ανάλυση και δημιουργία εικόνας του τι συνέβηκε. Όπως προαναφέρθηκε, είναι κρίσιμο να διατηρείται η ακεραιότητα των αποδεικτικών στοιχείων. Η δεύτερη τεχνική είναι το Live Imaging με την οποία ο ανακριτής πηγαίνει στον χώρο του υπολογιστή και ανακτά τα δεδομένα εκείνη την στιγμή [31].

2.10. Ανάλυση αποδεικτικών στοιχείων

Αφού γίνει σωστή συλλογή των δεδομένων και ακολουθεί η ανάλυση, όπως περιγράφεται στη συνέχεια [32].

Ανάλυση διαδικτυακών πακέτων

Για την ανάλυση των πακέτων χρησιμοποιήθηκε το πρόγραμμα WireShark ένα από τα πιο διάσημα προγράμματα για ανάλυση διαδικτυακών πακέτων. Όπως φαίνεται στην Εικόνα 2.15, αν είναι γνωστές κάποιες διευθύνσεις IP που θεωρούνται κακόβουλες είναι δυνατόν μέσω φίλτρου να φανεί τι πακέτα έχουν αποσταλεί από αυτές τις διευθύνσεις



Εικόνα 2.15 Στιγμιότυπο του προγράμματος WireShark με φίλτρο μια συγκεκριμένη IP

Επίσης μπορεί να φανεί η κίνηση βάσει της ώρας που έχει συμβεί ένα περιστατικό, ενώ ανάλογα με τον τύπο τον πακέτων μπορεί να μπει διαφορετικό φόντο, για παράδειγμα τα πακέτα τύπου ICMP να έχουν μπλε φόντο. Για τις ανάγκες του παραδείγματος, θεωρείται ότι την ώρα που συνέβηκε το περιστατικό υπήρχαν πολλά πακέτα πρωτοκόλλου HTTP άρα πολύ πιθανόν να έγινε εκεί η μετάδοση του κακόβουλου λογισμικού. Μπορούμε να βλέπουμε μόνο τα πακέτα με πρωτόκολλο που θέλουμε. Στην συνέχεια εντοπίστηκε μια πηγή με πολύ παράξενο url

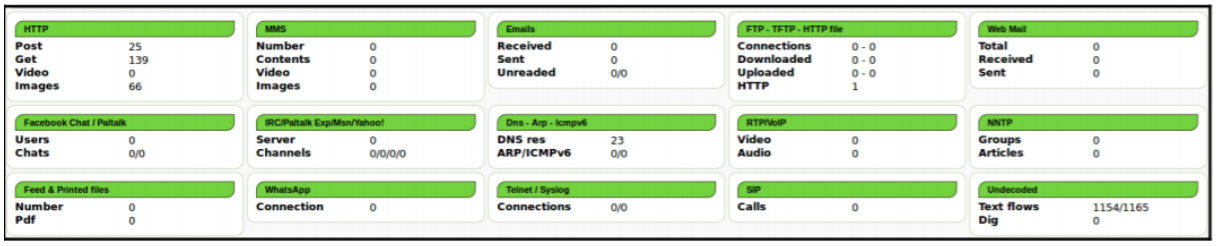
p27dokhpz2n7nvgr.1jw21x.top

Μπορεί να γίνει περισσότερη ανάλυση με την επιλογή του και μετά να επιλεχθεί να φανεί το HTTP Stream, με αποτέλεσμα να εμφανιστεί το παράθυρο της Εικόνας 2.16.

Εικόνα 2.16 HTTP Stream

Κατά την ανάλυση του συγκεκριμένου stream φαίνεται ότι έχει ληφθεί μια εικόνα με το όνομα bitcoin.png.

Η επόμενη εφαρμογή είναι ανοιχτού κώδικα και είναι διαθέσιμη μόνο στα λειτουργικά linux. Ονομάζεται XPLICO και επιτρέπει την εξαγωγή δεδομένων από πακέτα που παραλαμβάνονται από το δίκτυο. Προϋποθέτει να υπάρχουν δεδομένα και απλά να εισαχθούν για ανάλυση. Δεν μπορεί να παράξει Packet capture όπως στο wireshark κατά την εισαγωγή τους και αφού τα επεξεργαστεί εμφανίζει την ανάλυση όπως στην Εικόνα 2.17.



Εικόνα 2.17 Ομαδοποίηση που μας παρέχει η εφαρμογή XPLICO με το packet capture που του δώσαμε

Για κάθε πρωτόκολλο εμφανίζει και διαφορετική καρτέλα. Μπορούν να υπάρχουν παραπάνω επιλογές στην καρτέλα με το να επιλεγεί. Παρακάτω που έχει επιλεχθεί η καρτέλα HTTP εμφανίζει τα url όπου έγινε η ανταλλαγή των πακέτων (Εικόνα 2.18).

Εικόνα 2.18 Περισσότερές πληροφορίες που μας δίνει από την καρτέλα του HTTP

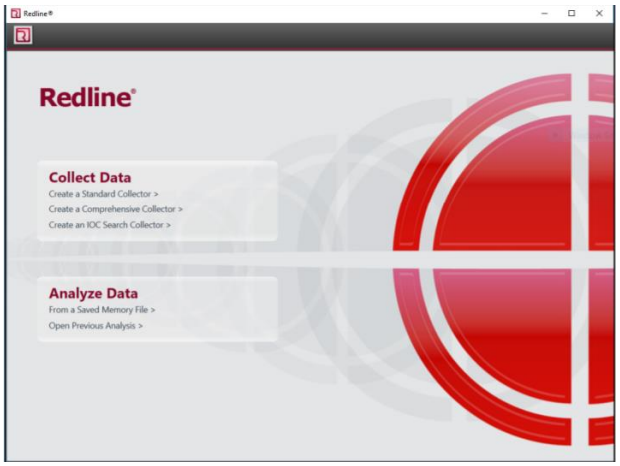
2.11. RAM Evidence

Από την αρχή που μπήκαν οι βάσεις και τα πλαίσια για το πώς διεξάγεται μια ψηφιακή εγκληματολογική έρευνα, οι πλείστες ερευνητικές αρχές είτε ιδιωτικές είτε δημόσιες είχαν ως πρωταρχικό στόχο να πάρουν τεκμήρια που βρίσκονται μέσα στο σκληρό δίσκο, με τεχνικές dead imaging όπου αφαιρείτο ο σκληρός δίσκος, το σύστημα παρέμενε κλειστό και πήγαινε σε ειδικό εργαστήριο για ανάλυση. Αυτό είχε ως αποτέλεσμα να θεωρείται μονόδρομος για την ανάλυση, με αποτέλεσμα να χάνονται κρίσιμα τεκμήρια που βρίσκονταν στην μνήμη RAM. Ακόμα και μετέπειτα ανάλυση της RAM ήταν περίπλοκη αφού έπρεπε να αποδεικτεί ότι τα δεδομένα θεωρούνταν αξιόπιστα, χωρίς να έχει υποβαθμιστεί η ακεραιότητα. Στη συνέχεια αναφέρονται οι μεθοδολογίες που είναι καλό να χρησιμοποιούνται αν θα γίνει ανάλυση της μνήμης RAM.

SANS six-part methodology: Είναι μια μεθοδολογία που αποτελείται από τα εξής 6 βήματα:

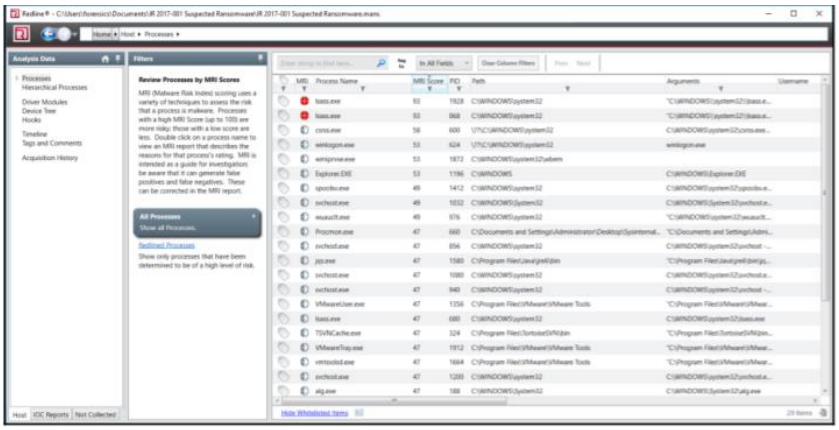
- Identify rogue processes: Συνήθως κακόβουλα λογισμικά είναι κρυμμένα πίσω από διεργασίες που δεν δείχνουν κάποια παράνομη λειτουργία. Με τον εντοπισμό τους μπορεί να γίνει κατανοητός ο χώρος όπου βρίσκονται στο λειτουργικό, τι συμβαίνει αλλά και αν είναι εν τέλει ένα κακόβουλο λογισμικό. Συχνό φαινόμενο είναι οι λειτουργίες να επωνομάζονται ως μια κανονική λειτουργία με αλλαγή ενός γράμματος.
- Analyze process DLLs and handles: Αν έχουν εντοπιστεί κακόβουλες διεργασίες το επόμενο βήμα είναι η ανάλυση των DLL files καθώς και κάτω από ποιο λογαριασμό γινόταν η εκτέλεση.
- Review network artifacts: Για να φτάσει ένα κακόβουλο λογισμικό στο σύστημα μια κύρια πηγή εισόδου είναι μέσω του δικτύου. Με την ανάλυση των ανοιχτών συνδέσεων μπορεί να εντοπιστεί και η πηγή απ’ όπου λήφθηκε το κακόβουλο λογισμικό.
- Look for evidence of code injection: Συνήθως οι δημιουργοί των κακόβουλων λογισμικών χρησιμοποιούν χώρους στη μνήμη που δεν έχουν διευθύνσεις, τα οποία μπορούν να εντοπιστούν με προγράμματα ανάλυσης μνήμης.
- Check for signs of a rootkit: Συνήθως ένα κακόβουλο λογισμικό όπως είπαμε και πιο πάνω κρύβεται πίσω από διεργασίες που φαίνονται φυσιολογικές, όσο δεν ανιχνεύονται δίνουν στους εγκληματίες την ευκαιρία για απομακρυσμένη διαχείριση του υπολογιστή-θύματος.
- Dump suspicious process and drivers: Μετά τον εντοπισμό και την απομάκρυνση του κακόβουλου λογισμικού η συλλογή και περαιτέρω ανάλυση με πρόσθετα εργαλεία είναι μια διαδικασία που δεν πρέπει να αποφεύγεται καθώς μπορούμε να πάρουμε περισσότερες πληροφορίες και εμπειρία για μελλοντικές επιθέσεις [33].

Σήμερα υπάρχουν αρκετά εργαλεία για ανάλυση των δεδομένων μνήμης. Παρακάτω αναφέρεται ένα δωρεάν εργαλείο που παρέχεται από το MandiantRedline (Εικόνα 2.19). Είναι διαθέσιμο για τα λειτουργικά Windows στον σύνδεσμο https://www.fireeye.com/MandiantRedline/FireEyeRedline. Μετά την εγκατάσταση, κατά την εκκίνηση δίνει διάφορες επιλογές που χωρίζονται σε δύο κατηγορίες: Collect Data και Analyze Data [34].



Εικόνα 2.19 Αρχική οθόνη του προγράμματας RedLine

Μετά την εισαγωγή, εμφανίζει τις διεργασίες που έτρεχαν (Εικόνα 2.20).



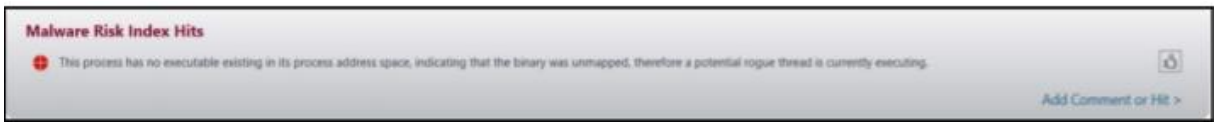
Εικόνα 2.20 Διεργασίες που έχουν εντοπιστεί

Ένα δυνατό χαρακτηριστικό αυτής της εφαρμογής είναι το MRI (Malware Risk Inticator) score για κάθε διεργασία που έτρεχε. Ανάλογα με το αν είναι συνηθισμένο μια τέτοια διεργασία να τρέχει στα λειτουργικά windows και αν διαθέτει ψηφιακή υπογραφή υπολογίζεται η πιθανότητα να είναι κακόβουλη διεργασία. Στην δική μας περίπτωση βλέπουμε ότι οι διεργασίες με PID 1928,868 και με όνομα lsaas.exe έχουν score 93 που υποδεικνύει μεγάλη πιθανότητα να είναι κακόβουλο το λογισμικό.

Αν επιλεχθεί μια από αυτές τις διεργασίες μπορούν να φανούν περισσότερες λεπτομέρειες.

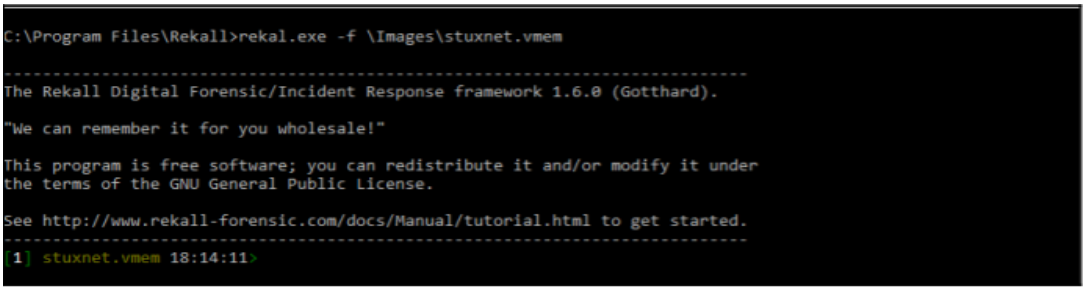
Εικόνα 2.21 Ανάλυση διεργασιών

Στην Εικόνα 2.22 μπορούμε να διακρίνουμε το πεδίο MRI Report, το οποίο δίνει την αιτιολόγηση γιατί θεωρείται κακόβουλο λογισμικό.



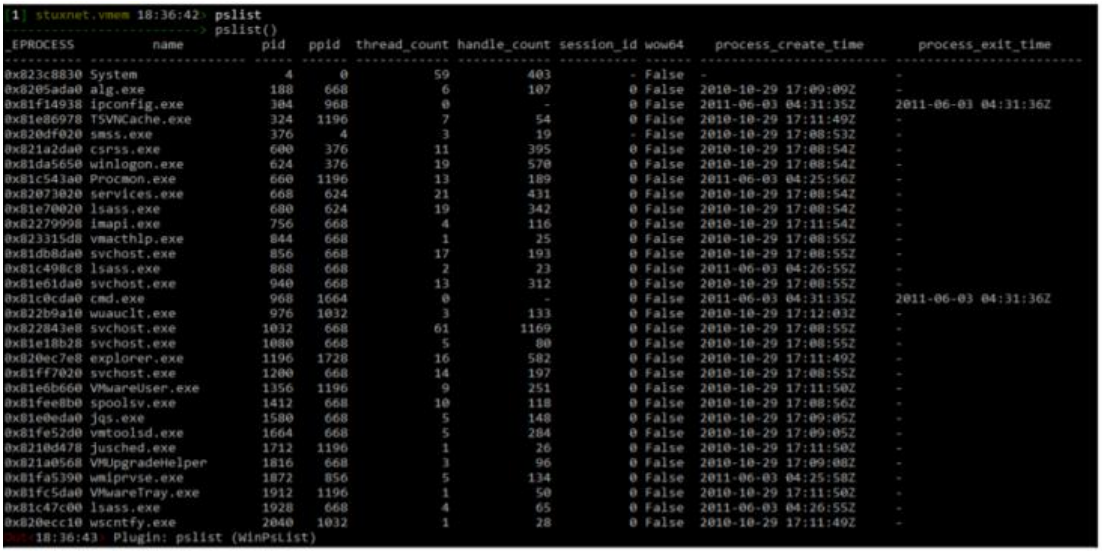
Εικόνα 2.22 Λεπτομέρειες σχετικά με την ένδειξη γιατί θεωρείτε κακόβουλη διεργασία

Στην συνέχεια εξετάζεται ακόμα ένα πρόγραμμα Rekall που δημιουργήθηκε από την Google. Είναι ανοικτού κώδικα και είναι διαθέσιμο σε όλα τα λειτουργικά MacOs, Linux, Windows. Μπορεί να αποκτηθεί στο Link https://github.com/google/rekall/releases. Η λειτουργία του βασίζεται σε command-line, ενώ δεν παρέχει GUI. Στη συνέχεια επεξηγείται πώς λειτουργεί και αναφέρονται μερικές βασικές εντολές. Για αρχή πρέπει να φορτωθεί στην εφαρμογή το image. Κατευθυνόμαστε στην τοποθεσία της εφαρμογής μέσα στον σκληρό δίσκο από το cmd των Windows και εκτελούμε την εντολή: C:\Program Files\Rekall>rekal.exe -f \<Path of Image.vmem>. Αν έχει γίνει σωστά θα φανεί το αποτέλεσμα της Εικόνας 2.23.



Εικόνα 2.23 Επιτυχής φόρτωση στο πρόγραμμα το image

Με την εντολή **pslist** εμφανίζει τις διεργασίες που έτρεχαν καθώς και το processID, parentID (Εικόνα 2.24).



```
1] stuxnet.vmem 18:36:42> pslist
                        > pslist()
_EPROCESS          name          pid   ppid  thread_count handle_count session_id wow64    process_create_time       process_exit_time
---------- -------------------- ----- ------ ------------ ------------ ---------- ------ ------------------------ ------------------------
0x823c8830 System                 4      0           59          403          - False  -                        -
0x8205ada0 alg.exe              188    668            6          107          0 False  2010-10-29 17:09:09Z     -
0x81f14938 ipconfig.exe         304    968            0            -          0 False  2011-06-03 04:31:35Z     2011-06-03 04:31:36Z
0x81e86978 TSVNCache.exe        324   1196            7           54          0 False  2010-10-29 17:11:49Z     -
0x820df020 smss.exe             376      4            3           19          - False  2010-10-29 17:08:53Z     -
0x821a2da0 csrss.exe            600    376           11          395          0 False  2010-10-29 17:08:54Z     -
0x81da5650 winlogon.exe         624    376           19          570          0 False  2010-10-29 17:08:54Z     -
0x81c543a0 Procmon.exe          660   1196           13          189          0 False  2011-06-03 04:25:56Z     -
0x82073020 services.exe         668    624           21          431          0 False  2010-10-29 17:08:54Z     -
0x81e70020 lsass.exe            680    624           19          342          0 False  2010-10-29 17:08:54Z     -
0x8227998 imapi.exe             756    668            4          116          0 False  2010-10-29 17:11:54Z     -
0x823315d8 vmacthlp.exe         844    668            1           25          0 False  2010-10-29 17:08:55Z     -
0x81db8da0 svchost.exe          856    668           17          193          0 False  2010-10-29 17:08:55Z     -
0x81c498c8 lsass.exe            868    668            2           23          0 False  2011-06-03 04:26:55Z     -
0x81e61da0 svchost.exe          940    668           13          312          0 False  2010-10-29 17:08:55Z     -
0x81c0cda0 cmd.exe              968   1664            0            -          0 False  2011-06-03 04:31:35Z     2011-06-03 04:31:36Z
0x822b9a10 wuauclt.exe          976   1032            3          133          0 False  2010-10-29 17:12:03Z     -
0x822843e8 svchost.exe         1032    668           61         1169          0 False  2010-10-29 17:08:55Z     -
0x81e18b28 svchost.exe         1080    668            5           80          0 False  2010-10-29 17:08:55Z     -
0x820ec7e8 explorer.exe        1196   1728           16          582          0 False  2010-10-29 17:11:49Z     -
0x81ff7020 svchost.exe         1200    668           14          197          0 False  2010-10-29 17:08:55Z     -
0x81e6b660 VMwareUser.exe      1356   1196            9          251          0 False  2010-10-29 17:11:50Z     -
0x81fee8b0 spoolsv.exe         1412    668           10          118          0 False  2010-10-29 17:08:56Z     -
0x81e0eda0 jqs.exe             1580    668            5          148          0 False  2010-10-29 17:09:05Z     -
0x81fe52d0 vmtoolsd.exe        1664    668            5          284          0 False  2010-10-29 17:09:05Z     -
0x8210d478 jusched.exe         1712   1196            1           26          0 False  2010-10-29 17:11:50Z     -
0x821a0568 VMUpgradeHelper     1816    668            3           96          0 False  2010-10-29 17:09:08Z     -
0x81fa5390 wmiprvse.exe        1872    856            5          134          0 False  2011-06-03 04:25:58Z     -
0x81fc5da0 VMwareTray.exe      1912   1196            1           50          0 False  2010-10-29 17:11:50Z     -
0x81c47c00 lsass.exe           1928    668            4           65          0 False  2011-06-03 04:26:55Z     -
0x820ecc10 wscntfy.exe         2040   1032            1           28          0 False  2010-10-29 17:11:49Z     -
[1] 18:36:43> Plugin: pslist (WinPsList)
```

Εικόνα 2.24 Εκτέλεση εντολής pslist

Με την εντολή sockets μπορούν να φανούν οι διαθέσιμες ανοικτές συνδέσεις που ήταν ανοικτές.

ΚΕΦΑΛΑΙΟ 3: ANDROID FORENSICS

Η εγκληματολογική πληροφορική στις κινητές συσκευές είναι ένας κλάδος που εξελίσσεται μαζί με την εξέλιξη της τεχνολογίας των τελευταίων χρόνων και των κινητών συσκευών, ενώ μεγάλο μέρος του πληθυσμού σήμερα έχει μια έξυπνη κινητή συσκευή στην κατοχή του με λειτουργικό σύστημα έτοιμο να πράξει ακόμα και απαιτητικές διεργασίες. Το Android Forensics ασχολείται με το λειτουργικό σύστημα Android και τον τρόπο με τον οποίο μπορεί να γίνει εξαγωγή, ανάκτηση και ανάλυση δεδομένων που υπάρχουν σε μια κινητή συσκευή μέσω διαφόρων τεχνικών. Λόγω της ανοιχτής φύσης του λειτουργικού συστήματος android, όλες οι μέθοδοι που αναφέρονται μπορούν να εφαρμοστούν και στις τηλεοράσεις και στα ρολόγια και στα συστήματα πολυμέσων αυτοκινήτου που έχουν τέτοιο λειτουργικό [35].

Οι κινητές συσκευές επιτρέπουν να εκτελεστεί ένα ευρύ φάσμα δραστηριοτήτων πέραν των συνηθισμένων, όπως σερφάρισμα στο Διαδίκτυο, εγγραφή με υψηλής ευκρίνειας βίντεο, αποθήκευση εγγράφων, προσδιορισμός τοποθεσίας μέσω GPS, καθιστώντας την κινητή συσκευή μια αποθήκη προσωπικών δεδομένων και πληροφοριών. Σε βάθος χρόνου, τα δεδομένα που έχει μια κινητή συσκευή μπορεί να είναι πιο πολύτιμα και από την ίδια την συσκευή. Ένα μεγάλο μέρος αυτών των δεδομένων είναι διαθέσιμα από τους φορείς παροχής τηλεφωνικών υπηρεσιών αλλά συχνά για την πρόσβαση χρειάζεται ένταλμα και διαδικασίες που χρονοτριβούν, με αποτέλεσμα στο τέλος τα δεδομένα να χάσουν την αξία τους [36].

3.1. The Mobile Forensics process

Οι διαδικασίες που αναφέρθηκαν στα πιο πάνω μοντέλα που χρησιμοποιούνται για την πάταξη της ψηφιακής εγκληματολογίας είναι πολύ παρόμοιες με αυτές που χρησιμοποιούνται και στην ψηφιακή εγκληματολογία στις κινητές συσκευές. Παρόλα αυτά υπάρχουν και κάποιες ιδιαιτερότητες που πρέπει να ληφθούν υπόψη. Ακολουθώντας τη σωστή μεθοδολογία και τις οδηγίες για την εξέταση των κινητών συσκευών μπορούν να επιτευχθούν τα επιθυμητά αποτελέσματα [37].

- Seizure

  Η ψηφιακή εγκληματολογία βασίζεται στο γεγονός ότι τα αποδεικτικά στοιχεία πρέπει πάντα να διατηρούνται επαρκώς σε ασφαλές περιβάλλον, για να μπορούν να τύχουν επεξεργασίας μετέπειτα και να είναι αποδεκτά στο δικαστήριο. Υπάρχουν όμως κάποια σημεία που οι ερευνητές πρέπει να λαμβάνουν υπόψη, όπως ότι η κινητή συσκευή μπορεί να κλειδώσει είτε από τον χρήστη είτε από εφαρμογές που μπορούν να ενεργοποιηθούν απομακρυσμένα. Γι' αυτό και συστήνεται πάντα η απομόνωση της συσκευής μέσω λειτουργίας πτήσης και απενεργοποίηση του WIFI. Συχνά όταν μια συσκευή κατάσχεται παραμένει ενεργοποιημένη με στόχο τη διατήρηση των δεδομένων και των πιθανών αποδεικτικών στοιχείων. Γι' αυτό και όταν μεταφέρετε πρέπει να παραμένει ενεργοποιημένη, αλλιώς υπάρχει μεγάλη πιθανότητα να τροποποιηθούν ή να χαθούν αρχεία. Η μεταφορά γίνεται σε ειδικές σακούλες (faraday) που εγγυούνται ασφαλή μεταφορά αποδεικτικών στοιχείων και απομόνωση από οποιαδήποτε προσπάθεια για εξωτερική επικοινωνία με την συσκευή.

- Acquisition

  Στόχος αυτής της φάσης είναι η ανάκτηση των δεδομένων από την κινητή συσκευή. Μια συσκευή όμως αν έχει κωδικό κλειδώματος, είτε μοτίβο, είτε βιομετρικά στοιχεία, χρειάζεται τον κατάλληλο κωδικό για να έχει κάποιος πρόσβαση στην συσκευή και στα δεδομένα, χωρίς

την παρέμβαση άλλων τεχνικών που μπορεί να θέσουν σε κίνδυνο την ακεραιότητα των δεδομένων. Ακόμα και αν δεν έχει η συσκευή κάποιο κλείδωμα, μπορεί να είναι δύσκολο να υπάρξει πρόσβαση στα δεδομένα, αφού ο συνεχόμενος συγχρονισμός των δεδομένων με υπηρεσίες cloud για ασφαλή αποθήκευση μπορεί να αλλοιώσει τα δεδομένα. Για παράδειγμα στα κινητά Android, η εφαρμογή google photos καθιστά την συσκευή τοπικά να μην έχει κάποιες αποδείξεις, ενώ στον λογαριασμό google photos να υπάρχουν πάρα πολλές αποδείξεις. Γι' αυτό πρέπει να είναι γνωστές και αυτές οι εφαρμογές, όπως και άλλες εφαρμογές που είναι εγκατεστημένες στην εφαρμογή και μπορεί να κρύβουν δεδομένα. Επομένως, πρέπει να καταγράφονται όλα όσα είναι εγκατεστημένα στην κινητή συσκευή. Δεν μπορεί όμως να μην σταθεί και εμπόδιο η συνεχής μεταβολή και αναβάθμιση του λογισμικού αφού κάθε αναβάθμιση φέρνει και καινούργιες ρυθμίσεις.

- Examination and analysis

  Κατά την εξέταση της συσκευής ίσως να χρειαστεί να χρησιμοποιηθούν πολλά εγκληματολογικά εργαλεία για να αποκτηθούν και να αναλυθούν τα δεδομένα που βρίσκονται στην συσκευή. Λόγω της ποικιλομορφίας των κινητών συσκευών(κινητά.ταμπλέτ) δεν υπάρχει μια καθολική εφαρμογή που μπορεί να εξάγει τα δεδομένα, αλλά επιβάλλεται η χρήση διαφόρων εφαρμογών, ανάλογα με την συσκευή. Τέλος όλα τα αποδεικτικά στοιχεία και ευρήματα που βρέθηκαν καθ' όλη την διάρκεια της έρευνας θα πρέπει να παρουσιαστούν στο δικαστήριο ή στον εκάστοτε υπεύθυνη αρχή.

3.2. Android Forensic Setup

Στο προηγούμενο κεφάλαιο αναφέρθηκε πως μπορούν να ληφξουν τα αποδεικτικά στοιχεία είτε από κινητές συσκευές, η άλλη συσκευή. Εδώ εξετάζεται η διαφορετική διαδικασία που ακολουθείται στις κινητές συσκευές. Αρχικά, η ύπαρξη ενός καλά ελεγχόμενου σύγχρονου εργαστηρίου είναι απαραίτητη, καθώς και ένας υπολογιστής "αποστειρωμένος" από εξωτερικές εφαρμογές που μπορεί να βλάψουν τα τεκμήρια και με εγκατεστημένες στο λογισμικό μόνο τις εξής εφαρμογές [38]:

- Android SDK
- Drivers for mobile phones
- Tools used for analysis

3.3. Android SDK

Σημαντικά προγράμματα για έρευνα στις κινητές συσκευές είναι τα Android Studio και το Android SDK. Το Android Studio είναι ένα πλήρως ολοκληρωμένο περιβάλλον ανάπτυξης (IDE) και περιέχει όλα όσα χρειάζονται για να δημιουργηθεί μια πλήρης εφαρμογή από την αρχή που τρέχει στα λειτουργικά Android. Το Android SDK είναι ένα υποσύνολο του Android Studio που συμπεριλαμβάνει τα απαραίτητα εργαλεία για την επικοινωνία του υπολογιστή με την κινητή συσκευή μέσω του cmd. Επίσης περιλαμβάνει βιβλιοθήκες λογισμικού API, εξομοιωτή κινητών συσκευών με πληθώρα εκδόσεων του λειτουργικού Android και άλλα εργαλεία που βοηθούν στην δημιουργία μιας εφαρμογής. Το SDK υποστηρίζεται σε πληθώρα λειτουργικών(Windows,Linux,OS X,) και κατά την διενέργεια της έρευνας βοηθά να αποκτηθεί πρόσβαση στα δεδομένα. Μπορεί να αποκτηθεί δωρεάν από τον σύνδεσμο https://developer.android.com/studio [39].

Τα πιο σημαντικά εργαλεία που παρέχονται στο SDK είναι τα ακόλουθα [40]:

- Apkanalyzer: Επιτρέπει να αναλυθούν τα περιεχόμενα ενός αρχείου APK (εκτελέσιμο αρχείο στα λειτουργικά Android) όπως applicationID, version code, version name.
- Avdmanager: Δίνει την δυνατότητα δημιουργίας και διαχείρισης εικονικών συσκευών Android, χρησιμοποιώντας command-line εντολές. Αυτή η δυνατότητα βοηθάει όταν πρόκειται να αναλυθεί ένα κακόβουλο λογισμικό. Επίσης μπορεί να χρησιμοποιηθεί για δοκιμές εφαρμογών αν δεν υπάρχει πρόσβαση σε φυσική συσκευή.
- Sdkmanager: Εργαλείο για να εξοπλίζονται με τις τελευταίες αναβαθμίσεις τα εργαλεία του SDK.
- Adb (Android Debug Bridge): Εργαλείο γραμμής εντολών που επιτρέπει την επικοινωνία με μια κινητή συσκευή. Μπορεί να χρησιμοποιηθεί για εγκατάσταση εφαρμογών, αντιγραφή δεδομένων, διαγραφή εφαρμογών. Ακόμη έχει την δυνατότητα να παρέχει Unix κέλυφος.

3.4. Android Virtual Device

Με το Android SDK εγκατεστημένο μπορεί να δημιουργηθεί μια εικονική συσκευή που θα την διαχειριζόμαστε από τον εξομοιωτή. Αυτή η τακτική χρησιμοποιείται συχνά από προγραμματιστές κατά τη δημιουργία νέων εφαρμογών όταν δοκιμάζονται οι λειτουργίες. Όμως βοηθάει και τους ψηφιακούς εγκληματολόγους που θέλουν να κατανοήσουν πώς συμπεριφέρονται οι κακόβουλες εφαρμογές. Επίσης πολύ χρήσιμο είναι το ότι η εικονική συσκευή που δημιουργείται έρχεται με δικαιώματα root όπου εξηγείται στη συνέχεια [41].

Εικόνα 3.1 Εικόνα εικονικής συσκευής android 9(Pie)

3.5. Accesing the Device with ADB

Στην εγκληματολογική πληροφορική, το ADB παίζει πολύ σημαντικό ρόλο στα λειτουργικά συστήματα Android. Για την λειτουργία του όμως χρειάζεται η ενεργοποίηση της επιλογής USB Debugging που βρίσκεται μέσα στις ρυθμίσεις της συσκευής. Μόλις ενεργοποιηθεί η επιλογή USB debugging, η συσκευή θα εκτελέσει το ADB και θα ψάχνει για μια σύνδεση μέσω USB. Συσκευές που δεν έχουν πλήρη δικαιώματα δεν θα έχουν πρόσβαση στα εσωτερικά δεδομένα της συσκευής. Τηλέφωνα που έχουν πλήρη δικαιώματα μπορούν να έχουν πρόσβαση σε όλα τα δεδομένα. Κατά την εκτέλεση του adb στην κινητή συσκευή όλες οι λειτουργίες δουλεύουν στο παρασκήνιο. Στη συνέχεια παρουσιάζονται μερικές εντολές και δυνατότητες του adb μέσω των εντολών Unix [42].

adb devices: με αυτή την εντολή βλέπουμε τις συσκευές που είναι ενωμένες. Αν είναι παραπάνω από μια συσκευή, τότε μπορούμε να απευθυνθούμε στην συγκεκριμένη με τον εξής τρόπο:

```
adb devices
List of devices attached
4df16ac5115e4e04       device
7f1c864544456o6e        device
```

```
adb shell -s 4df16ac5115e4e04
```

Εικόνα 3.2 Επιλογή συγκεκριμένης συσκευής με τον κωδικό που της έχε ανατεθεί

3.6. Shell commands

Αφού έχει συνδεθεί η συσκευή με την εντολή adb shell ενεργοποιείται το shell και μπορούν να χρησιμοποιηθούν οι εντολές unix. Όπως φαίνεται και στην Εικόνα 3.3, αλλάζει και το prompt μετά την εκτέλεση της εντολής [43].

```
adb shell
shell@android:/ $
```

Εικόνα 3.3 Σύνδεση συσκευής με τον υπολογιστή μέσω adb

LS Command

Με την εκτέλεση της εντολή ls εμφανίζονται οι υποφακέλοι που υπάρχουν στην περιοχή που είμαστε. Υπάρχουν αρκετοί παράμετροι στην εντολή ls, όπως για παράδειγμα με την παράμετρο -l φαίνονται οι φάκελοι, τα αρχεία, το μέγεθος, η ημερομηνία δημιουργίας, τα δικαιώματα. Στην Εικόνα 3.4 φαίνεται τι κάνουν κι άλλοι παράμετροι.

Option	Description
a	Lists hidden files
c	Displays files by timestamp
d	Displays only directories
n	Displays the long format listing, with GID and UID numbers
R	Displays subdirectories as well
t	Displays files based on timestamp
u	Displays the file access time

Εικόνα 3.4 Λίστα με της παραμέτρους που δέχεται η εντολή ls

Cat Command

Με την εντολή cat μπορούν να εμφανιστούν τα δεδομένα ενός αρχείου κειμένου (Εικόνα 3.5).

```
shell@android:/ $ cat adb_keys
QAAAADeVcId5z+6WTzB5Qtyj4RMBmP3IsbHsiLC2Q8EpmIRDAHywZ45jjUENg+2NF4T
UnXlBAU0LyycR/ER7/EZBUjTaLE09gWJuMbZQ4RcwFjM9nnhHquctYFNB4MzobWNDeZ
xdYXaDEqzycEij50ae3zZ3H5F7eVSoCvwaulOWf3oxwxaeWQsDBNt0EX0yqznfxO2GI
PQhwzOdtYQsAxJye16OaazCHCsXLwMNcuZLDYpH37em71S/mUfz8hwDrDlnN0CqnpQc
vXW6Q0dE1RdkJZP+FCmbYCMautkEJR5vx70Xrfv1PE+2rXzXw582h8i8Ctq8V567l7D
DRLaoyO4FtST4Lw/toV3KgTcVmHo7FHhhuml5ZNUwAMtBxkw8sDOTaoU9o5LjcPZdxK
+0Iik/XFFZz2IxlNxQsmn9zErA7mJghkEjuZ2L4ZxPPB38HuCiCBXjTNecX2S4QPeOT
VSq+VTHi9tHwN+9fKcYIwhczMg7JSNIxHDVOlLudjwzISSmWfp2/0i9J8nUHHH8jmXO
e+bHv6QvFvzUl/8wtyV+prS5EcJ6sAqoCqu1Xr+9FdKqmjyNyYK3K6fZTkAetjLFuTJ
at/lkqUfiIL1B3chQyRP09mEk8EklWpugo0chec17ZL3Vv0CPPJIy/2rTITZDj7MKwd
Zi7kEAo6Rgcg/ypAESuHlMWQEAAQA= android-eng@google
```

Εικόνα 3.5 Εκτέλεση της εντολής cat adb_keys

Cd Command

Με την εντολή cd μπορεί να γίνει μετάβαση από τον ένα φάκελο στον άλλο (Εικόνα 3.6).

```
shell@android:/ $ cd /data
shell@android:/data $
```

Εικόνα 3.6 Εκτέλεση εντολής cd

Rm command

Με την εντολή rm μπορούν να διαγραφούν αρχεία και φάκελοι.

Chmod command

Με την εντολή chmod μπορούν να αλλαχθούν τα δικαιώματα που μπορεί να έχει ο χρήστης στο αρχείο/φάκελο. Για παράδειγμα το chmod 777 δίνει άδεια σε όλους τους χρήστες να μπορούν να το διαβάσουν, να το ανοίξουν και να κάνουν αλλαγές.

3.7. Εξαγωγή Δεδομένων από κινητή συσκευή

Με την χρήση του adb μπορούν να εξαχθούν δεδομένα που υπάρχουν στην κινητή συσκευή στην συνδεδεμένη συσκευή όπου βρισκόμαστε με την εντολή:

Adb pull <remote> <local> *remote είναι το path στην κινητή συσκευή
Local το path στον συνδεδεμένο υπολογιστή

Σε μια συσκευή που δεν έχει ξεκλειδώσει όλα τα δικαιώματα, δεν μπορούν να εξαχθούν όλα τα αρχεία με αυτή την εντολή λόγω του ότι το λογισμικό δεν δίνει πρόσβαση σε όλους τους φακέλους, για παράδειγμα δεν υπάρχει πρόσβαση σε αρχεία από τον φάκελο/data/data αν δεν υπάρχουν root permisions [44].

3.8. Εισαγωγή Δεδομένων στην κινητή συσκευή

Με το abd μπορούν να γίνουν αρκετές ενέργειες για εξασφάλιση τεκμηρίων από τις κινητές συσκευές. Ακόμα ένα χαρακτηριστικό του adb είναι και η εισαγωγή δεδομένων στην συσκευή με την εντολή:

Adb push <local> <remote>

Εδώ ο περιορισμός που υπάρχει αν η συσκευή δεν είναι ξεκλειδωμένη είναι ότι επιτρέπει την εισαγωγή μόνο σε συγκεκριμένους φακέλους [45].

3.9. Rooting

Το root είναι μια λέξη που ακούγεται συχνά σε σχέση με τις συσκευές Android. Με την λεπτομερή κατανόηση του αποκτάται η γνώση που απαιτείται για την αντιμετώπιση ζητημάτων κατά την διάρκεια μιας έρευνας. Το rooting έχει γίνει ένα συχνό φαινόμενο, αφού πολλές φορές οι συσκευές όπου πρέπει να διενεργηθεί έρευνα είναι ήδη root. Για την κατανόηση όμως είναι σημαντικό να υπάρχουν οι βασικές γνώσεις για το πώς λειτουργούν τα λειτουργικά συστήματα Unix (λειτουργικό όπου βασίζονται τα λειτουργικά Linux). Επειδή ήταν σχεδιασμένο από την αρχή ως σύστημα για πολλαπλούς χρήστες. αφού τις προηγούμενες δεκαετίες δεν είχε ο καθένας τον δικό του υπολογιστή, ήταν απαραίτητος ένας μηχανισμός διαχωρισμού για την προστασία των δεδομένων των χρηστών και των πόρων. Για την εκτέλεση όμως εργασιών που μόνο εξουσιοδοτημένοι χρήστες μπορούσαν να διενεργήσουν όπως παραχώρηση και ανάκληση πρόσβασης σε δεδομένα από απλούς χρήστες, πρόσβαση σε κρίσιμα αρχεία για επισκευή ή αναβάθμιση του συστήματος, σχηματίζονται οι απλοί χρήστες και οι χρήστες

(superusers) με ξεκλειδωμένα όλα τα προνόμια. Η λέξη root είναι το όνομα χρήστη η ο λογαριασμός που από προεπιλογή έχει πρόσβαση σε όλες τις εντολές και τα αρχεία Linux. Αγοράζοντας όμως ένα τηλέφωνο Android θεωρούμαστε απλοί χρήστες και όχι root αφού δεν έχουμε πρόσβαση σε όλα τα αρχεία και σε όλες τις ενέργειες [46].

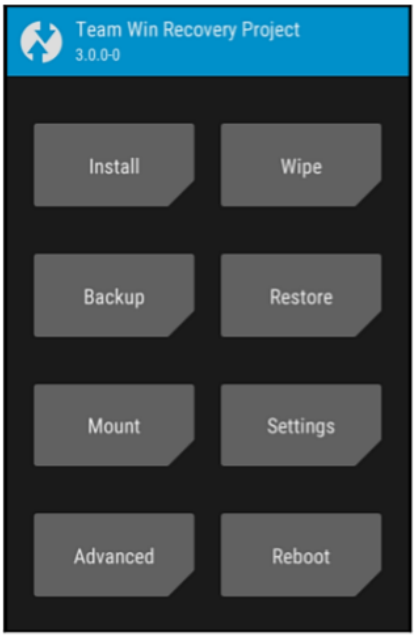
Είναι επίσης σημαντικό να γίνει κατανοητή η διαφορά rootin με jailbreaking καθώς θεωρούνται ίδια. Jailbreaking συμβαίνει σε συσκευές Apple με λειτουργικό iOS που επιτρέπει να καταργηθούν μερικοί περιορισμοί που έχουν τεθεί από το λογισμικό. Για παράδειγμα δεν επιτρέπεται η εγκατάσταση μη υπογεγραμμένων εφαρμογών στη συσκευή δηλαδή εφαρμογές που δεν έχουν εγκριθεί από την εταιρία Apple, κάτι που το Android επιτρέπει. Αν και για να αποκτηθεί root πρόσβαση στην συσκευή υπάρχει ο κίνδυνος κατά την μετατροπή η συσκευή να πάθει βλάβη, πολλές φορές εκτελείται με στόχο να ξεπεραστούν οι περιορισμοί που βάζουν οι εταιρίες κινητής τηλεφωνίας και οι κατασκευαστές, αφού με την αλλαγή μπορούν να αντικατασταθούν εφαρμογές που οι απλοί χρήστες δεν έχουν το δικαίωμα να κάνουν. Στην ψηφιακή εγκληματολογία ο κύριος λόγος που μια συσκευή γίνεται root είναι για να αποκτηθεί πρόσβαση σε αυτά τα μέρη του συστήματος που συνήθως δεν είναι προσβάσιμα. Μπορούν να εντοπιστούν δυο διαφορετικοί τύποι root: ο μόνιμος και ο προσωρινός. Ο προσωρινός χρησιμοποιείται στην εγκληματολογική πληροφορική για να δώσει η συσκευή όλα τα δικαιώματα μέχρι να ξαναγίνει επανεκκίνησή της. Με τον μόνιμο η συσκευή παραμένει με όλα τα δικαιώματα. Πέραν των θετικών, υπάρχουν βέβαια και τα αρνητικά, όπως η βλάβη του τηλεφώνου, ενώ οι πλείστες τηλεφωνικές εταιρίες επισημαίνουν ότι αν η συσκευή υποστεί αλλαγή δεν είναι πλέον στην εγγύηση που προσφέρεται. Στην ψηφιακή εγκληματολογία, αν και μπορεί να δώσει πολλά δεδομένα, δεν προτείνεται σαν τακτική πάρα μόνο αν είναι απόλυτη ανάγκη [47].

3.10. Recovery Mode

Ένα τηλέφωνο Android μπορεί να θεωρηθεί ως μια συσκευή που είναι χωρισμένη στα τρία: boot loader, Android ROM, και Recovery. Το bootloader είναι το πρώτο πρόγραμμα που εκτελείται όταν το τηλέφωνο ενεργοποιείται. Η δουλειά του είναι η αρχικοποίηση χαμηλού επιπέδου hardware και η εκκίνηση, η φόρτωση στο δεύτερο μέρος όπου βρίσκεται η ROM που περιέχει όλα τα αρχεία για την εκκίνηση του λειτουργικού συστήματος και γενικά όλα τα απαραίτητα αρχεία για την σωστή λειτουργία του λογισμικού. Το τρίτο μέρος είναι αυτό που διενεργεί τις αναβαθμίσεις και τη διαγραφή όλων των αρχείων. Για παράδειγμα όταν γίνεται επαναφορά εργοστασιακών ρυθμίσεων αυτό που τρέχει είναι το recovery, ενώ όταν αναβαθμίζεται το λογισμικό, το recovery είναι αυτό που είναι υπεύθυνο για εγγραφή της αναβάθμισης στην ROM. Υπάρχουν και οι custom recovery που παρέχονται από τρίτες εταιρίες με σκοπό την αλλαγή από την εργοστασιακή, αφού προσφερθούν επιπρόσθετα εργαλεία όπως [48]:

- Παρέχει πλήρη άδεια στο adb να τρέχει σαν root
- Παρέχει πλήρη χρήση και εξαγωγή δεδομένων σε εξωτερική μονάδα αποθήκευσης

Υπάρχουν αρκετά custom recovery δωρεάν όπως τα ClockworkMod recovery και TeamWin Recovery Project.



Εικόνα 3.7 Στιγμιότυπο από το custom recovery TWRP (TeamWin Project)

3.11. Fastboot Mode

Μπορεί να αναφερθεί και σαν ένα πρωτόκολλο το οποίο μπορεί να χρησιμοποιηθεί για την επαναφορά των partition στην κινητή συσκευή. Συνοδεύεται μαζί με το Android SDK και είναι μια εναλλακτική λύση για την εγκατάσταση ενημερώσεων και ξεκλείδωμα της κινητής συσκευής, αλλά σε συγκεκριμένες περιπτώσεις. Μπορούμε επίσης να διαχειριστούμε και να κάνουμε μετατροπές στα αρχεία του συστήματος μέσω φορητού υπολογιστή [49].

3.12. ADB and Rooted device

Σε ένα κανονικό κινητό τηλέφωνο android, ορισμένοι φάκελοι δεν είναι διαθέσιμη για προσπέλαση όπως για παράδειγμα ο φάκελος/data/data που περιέχει όλα τα δεδομένα των εφαρμογών που εγκατασταθήκαν στην κινητή συσκευή (Εικόνα 3.8). Ως εκ τούτου με μια συσκευή που είναι root αυτά τα δεδομένα καθίσταται διαθέσιμα [50].

```
adb shell
shell@android:/ $ cd /data/data
cd /data/data
shell@android:/data/data $ ls
ls: .: Permission denied
```

```
adb shell
shell@android:/ $ su
shell@android:/ # ls /data/data
android
 com.android.backupconfirm
 com.android.bips
 com.android.bluetooth
 com.android.bluetoothmidiservice
 com.android.calllogbackup
 com.android.camera2
 com.android.captiveportallogin
 com.android.carrierconfig
```

Εικόνα 3.8 Αριστερά παρατηρούμε ότι δεν επιτρέπετε η είσοδος επειδή η συσκευή δεν είναι root και δεξιά μας δείχνει τα περιεχόμενα του φακέλου

3.13. Android Common Directories

Cache directory:

Σε αυτό τον φάκελο στα λειτουργικά Android αποθηκεύονται συχνά προσπελάσιμα δεδομένα και εφαρμογές. Με την διαγραφή του περιεχομένου αυτού του φακέλου δεν επηρεάζονται τα προσωπικά δεδομένα αλλά απλώς διαγράφονται τα δεδομένα που βρίσκονται εκεί. Φαίνεται ακόμα ένας φάκελος με το όνομα lost+found που διατηρεί ανακτημένα αρχεία που έχουν βρεθεί από την οποιαδήποτε καταστροφή αρχείων είτε λόγω κάποιας βλάβης ή εσφαλμένη αφαίρεση της κάρτας SD. Από εγκληματολογικής πλευράς περιέχει δεδομένα που μπορεί να φανούν αρκετά χρήσιμα όπως ιστορικά περιήγησης, δεδομένα εφαρμογών και εικόνες.

mnt directory:

Αυτός ο φάκελος χρησιμεύει ως σημείο αναφοράς για όλα τα συστήματα αρχείων εσωτερικού και εξωτερικού αποθηκευτικού χώρου.

System directory:

Φάκελος που περιέχει βιβλιοθήκες, αρχεία που σχετίζονται με το σύστημα μιας κινητής συσκευής. Οι προεγκατεστημένες εφαρμογές που συνοδεύουν την κινητή συσκευή βρίσκονται σε αυτό τον κατάλογο.

Data directory:

Σε αυτό τον φάκελο υπάρχουν όλα τα ιδιωτικά δεδομένα όλων των εφαρμογών. Τα περισσότερα δεδομένα ανήκουν στο χρήστη. Από εγκληματολογικής πλευράς αυτός ο φάκελος περιέχει πολύτιμα δεδομένα αφού εμπεριέχει χρήσιμα στοιχεία [51].

3.14. Logical extraction

Στην εγκληματολογική πληροφορική ο όρος logical extraction χρησιμοποιείται συνήθως για την εξαγωγή δεδομένων που δεν παρέχει ανάκτηση διαγραμμένων δεδομένων ή που δεν παρέχεται ένα πλήρες αντίγραφο των αποδεικτικών στοιχείων bit by bit. Η εγκληματολογία του android στην ουσία είναι οποιαδήποτε μέθοδος επικοινωνίας με το λειτουργικό σύστημα για εύρεση τεκμηρίων, αρά λοιπόν αφού η αλληλεπίδραση γίνεται μόνο με το λειτουργικό δεν είναι βέβαιη η ανάκτηση όλων των πιθανών δεδομένων. Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, υπάρχει και η φυσική εξαγωγή δεδομένων στους υπολογιστές κάτι που υπάρχει επίσης και στις κινητές συσκευές με μικρές διαφορές. Με τη λογική εξαγωγή δεδομένων στα κινητά, υπάρχει μια πιθανότητα να ληφθούν και διαγραμμένα δεδομένα λόγω του τρόπου που αποθηκεύει μια κινητή συσκευή τα δεδομένα. Όμως δεν μπορούν να ληφθούν δεδομένα όπως γίνεται στον υπολογιστή όπου μπορεί να αφαιρεθεί ο σκληρός δίσκος χωρίς κάποια αλληλεπίδραση με το λειτουργικό. Στα λειτουργικά android, η ανάκτηση δεδομένων επηρεάζει το λειτουργικό Android. Με λογική εξαγωγή μπορούν να εξαχθούν:

- Επαφές
- Αρχείο κλήσεων
- SMS/MMS
- Δεδομένα εφαρμογών

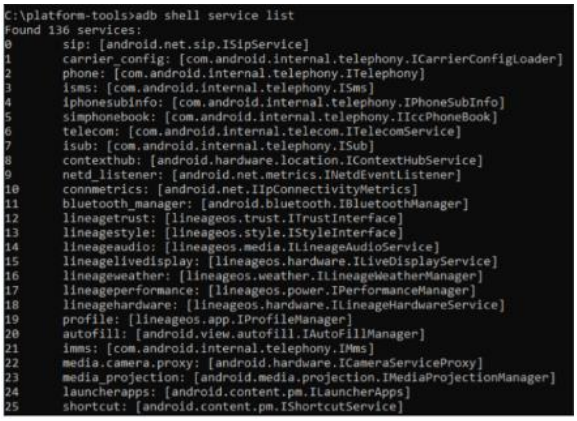
Αυτά τα δεδομένα αποθηκεύονται μέσα σε βάσεις SQLite [52].

Κατά την εγκληματολογική ανάλυση στις κινητές συσκευές, ο περιοριστικός παράγοντας είναι αν μπορεί ο εκάστοτε υπεύθυνος για την ανάκτηση των δεδομένων να έχει η όχι πρόσβαση στα δεδομένα.

Όπως αναφέρθηκε στις προηγούμενες ενότητες, όποια δεδομένα αποθηκεύονται στην εσωτερική μνήμη προστατεύονται και απαιτείται πρόσβαση root για την προσπέλαση τους. Αν η περίπτωση ακολουθήσει την οδό του νόμου μέσω της έρευνας, ο εξεταστής έχει το δικαίωμα να ζητήσει πρόσβαση στην συσκευή από τον χρήστη με τα συνθηματικά. Χωρίς τα απαραίτητα συνθηματικά και τη σωστή μέθοδο εξαγωγής δεδομένων υπάρχει μεγάλη πιθανότητα να καταστραφούν και τα δεδομένα και η συσκευή. Επειδή βέβαια η μέθοδος πρόσβασης είναι συχνά διαφορετική στις συσκευές κάθε εταιρίας, δεν υπάρχει μια καθολική μέθοδος για όλες τις συσκευές [53].

3.15. ADB DumpSys

Το εργαλείο αυτό βρίσκεται ενσωματωμένο στο λειτουργικό σύστημα Android, το όποιο χρησιμοποιείται συνήθως για σκοπούς ανάπτυξης εφαρμογών, αφού εμφανίζει την κατάσταση που βρίσκονται οι εφαρμογές που εκτελούνται στην συσκευή. Ωστόσο μπορεί να περιέχει σημαντικές πληροφορίες εγκληματολογικού χαρακτήρα. Δεν απαιτεί η κινητή συσκευή να έχει πρόσβαση root, και ενεργοποιείται με την εξής εντολή: **adb shell service list** [54]. Με την ενεργοποίηση της εντολής εμφανίζεται κάτι όπως στην Εικόνα 3.9:



Εικόνα 3.9 Στιγμιότυπο από την εκτέλεση της εντολής

3.16. ADB DumpSys

Batterystats

Δείχνει τις εφαρμογές που εκτελούνται.

Procstats

Παρόμοια εντολή με την batterystats, η οποία δείχνει την χρήση που έχει ο επεξεργαστής και από ποιες εφαρμογές.

App Ops

Ίσως μια από τις πιο ενδιαφέρουσες υπηρεσίες του dumpsys. Παρουσιάζει πότε χρησιμοποιήθηκε τελευταία φορά η εφαρμογή και τι άδεια πρόσβασης είχε.

Wi-Fi

Εμφανίζει μια λίστα με όλα τα SSID για τα οποία έχει αποθηκευτεί μια σύνδεση. Αυτό μπορεί να φανεί αρκετά χρήσιμο για προσδιορισμό τοποθεσιών του υπόπτου.

Notification

Παρέχει πληροφορίες σχετικά με τις τρέχουσες ενεργές ειδοποιήσεις [55].

3.17. Παράκαμψη Οθόνης κλειδώματος

Μια από τις πιο δύσκολες πτυχές της πρόσβασης σε δεδομένα μιας κινητής συσκευής είναι η παράκαμψη της οθόνης κλειδώματος. Ενώ υπάρχουν μέθοδοι για την παράκαμψη τους, κάθε έκδοση ενός λειτουργικού μπορεί να χρειάζεται διαφορετική μέθοδο. Οι τύποι κλειδώματος είναι οι ακόλουθοι [56]:

- None/slide
- Pattern
- PIN
- Password
- Smart Lock: Trusted Face, Trusted Voice, Trusted Location, Trusted Device, Onbody Detection

None/Slide lock screens

Αποτελεί την προεπιλεγμένη ρύθμιση των περισσότερων android συσκευών. Δεν παρέχει κανένα επίπεδο ασφαλείας και παρακάμπτεται σύροντας ένα δάκτυλο στην οθόνη με υποδεικνυόμενη κατεύθυνση.

Pattern lock screens

Μοτίβο όπου πρέπει ο χρήστης να σαρώσει με το δάκτυλο του μια διαδρομή στην οθόνη για το ξεκλείδωμα. Ο τύπος κλειδώματος Pattern αποθηκεύει τις πληροφορίες στο εξής αρχείο **/data/system/gesture.key**

Password/Pin

Χρήστες που είναι εξοικειωμένοι με το iOS της Apple θα αναγνωρίσουν αυτή την επιλογή. Απαιτεί από ένα χρήστη να πληκτρολογήσει ένα κωδικό πρόσβασης ή σε δεύτερο χρόνο εναλλακτικά ένα κωδικό PIN. Ο τύπος κλειδώματος PIN/Password αποθηκεύετε στο εξής αρχείο **/data/system/password.key**

Smart Lock

Πρωτοεμφανίστηκε στην έκδοση Android Lollipop. Απαιτεί μια συνθήκη για να ξεκλειδώσει η συσκευή όπως: το πρόσωπο ενός χρήστη, ο χρήστης να βρίσκεται σε μια συγκεκριμένη τοποθεσία ή κοντά σε κάποια άλλη συσκευή.

Σε όλες σχεδόν τις περιπτώσεις η παράκαμψη της οθόνης κλειδώματος θα απαιτήσει την ανάκτηση ενός αρχείου από την συσκευή.

Μετά την έκδοση Android 6.0 τις αποθηκευμένες πληροφορίες τόσο για το pattern αλλά και για το Pin/password στα αρχεία **gatekeeper.pattern.key & gatekeeper.password.key**

3.18. Αφαίρεση οθόνης κλειδώματος

Ανάλογα με τη συσκευή που εξετάζεται και την έκδοση του λειτουργικού συστήματος μπορεί να αφαιρεθεί η οθόνη κλειδώματος. Με την χρήση του adb και τις εντολές της Εικόνας 3.10 γίνεται η αφαίρεση.

```
adb shell
su
cd /data/system
rm *.key
```

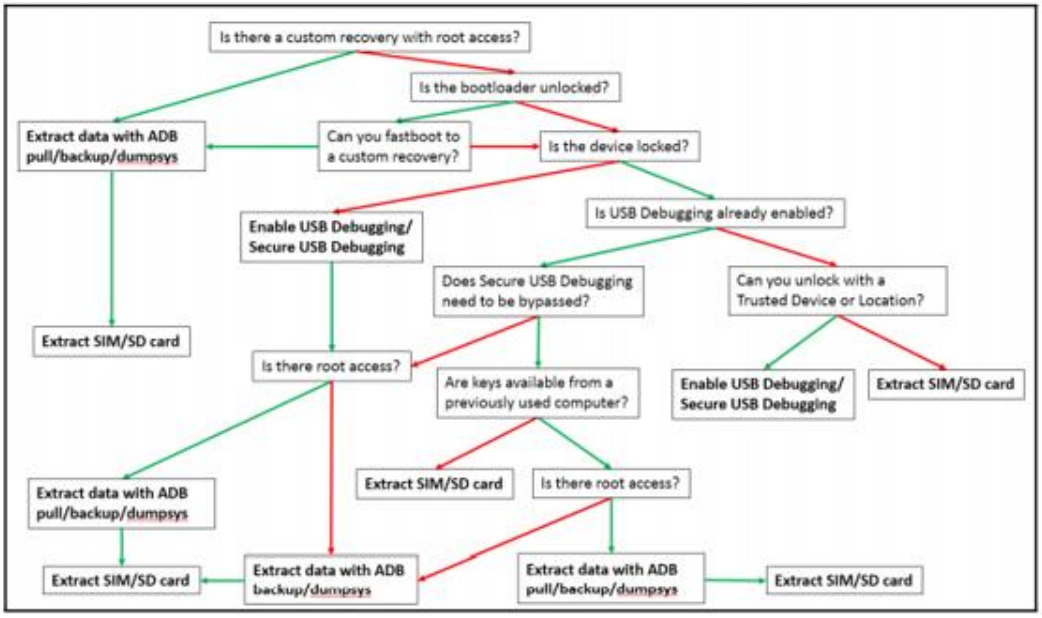
Εικόνα 3.10 Αφαίρεση κωδικού ξεκλειδώματος

Μετά την επανεκκίνηση της συσκευής δεν θα χρειαστεί να προστεθεί κάποιος κωδικός. Η αφαίρεση PIN/Password με ADB και SQL γίνεται όπως στην Εικόνα 3.11:

```
adb shell
su
cd /data/system
sqlite3 locksettings.db
update locksettings set value=0 where name='lockscreen.password_salt';
update locksettings set value=0 where name='sp-handle';
.quit
```

Εικόνα 3.11 Αφαίρεση κωδικού με εντολές SQL

Στην Εικόνα 3.12 ξεκαθαρίζονται τα βήματα που πρέπει να ακολουθούνται ανάλογα με την κατάσταση της συσκευής [57].



Εικόνα 3.12 Σχεδιάγραμμα για την πορεία που συνιστάτε να ακολουθήσουμε ανάλογα με την κατάσταση της συσκευής

3.19. Φυσική εξαγωγή Δεδομένων

Στην εγκληματολογική πληροφορική η φυσική εξαγωγή θεωρείται μια ακριβής αντιγραφή bit by bit. Στον παραδοσιακό υπολογιστή, αυτό συνήθως περιλαμβάνει την αφαίρεση της μονάδας αποδεικτικών στοιχείων από τον υπολογιστή του υπόπτου και την απεικόνισή του μέσω ενός προγράμματος. Στην κινητή εγκληματολογία διαφέρει η μέθοδος, για παράδειγμα η αφαίρεση της εσωτερικής μνήμης από

την συσκευή μπορεί να είναι χρονοβόρα, ακριβή και να απαιτεί εξειδικευμένη γνώση αλλά και πάλι θα πρέπει να λειτουργήσει το λογισμικό της συσκευής για την εξαγωγή.

JOIN TEST ACTION GROUP (JTAG)

Το πρότυπο JTAG αναπτύχθηκε από την IEEE. Κατά την παραγωγή της συσκευής χρησιμοποιείται για την επικοινωνία με τον επεξεργαστή μέσω μιας εξειδικευμένης διεπαφής για σκοπούς δοκιμών. Έτσι με τον ίδιο τρόπο ένας τεχνικός μπορεί να επικοινωνεί απευθείας με τον επεξεργαστή και να ανακτήσει τα δεδομένα της μνήμης. Για την εξαγωγή δεδομένων με αυτήν την τεχνική χρειάζεται η αποσυναρμολόγησή της συσκευής τελείως μέχρι την μητρική όπως φαίνεται στην Εικόνα 3.13.

Εικόνα 3.13 JTAG

Αν και αποτελεί κάτι πολύ δύσκολο και χρονοβόρο, ενώ χρειάζονται άτομα με μεγάλη εμπειρία, με αυτό τον τρόπο μπορούν να επιτευχθούν τα εξής:

- Ανάκτηση δεδομένων χωρίς την ενεργοποίηση της συσκευής
- Ανάκτηση δεδομένων ακόμα και αν η συσκευή υπέστη ζημιά
- Μπορεί να χρησιμοποιηθεί για παράκαμψη οθόνης ασφάλειας
- Μπορεί να γίνει φυσική εξαγωγή δεδομένα [58]

3.20. Ανάκτηση διαγραμμένων δεδομένων

Η ανάκτηση διαγραμμένων δεδομένων είναι η διαδικασία που ανακτούνται δεδομένα είτε από εξωτερική κάρτα αποθήκευσης είτε από την εσωτερική μνήμη, όταν δεν είναι δυνατή η φυσική πρόσβαση. Η ανάκτηση τους βοηθάει συχνά στην επίλυση αστικών ή ποινικών υποθέσεων επειδή συνήθως πολλοί κατηγορούμενοι απλά διαγράφουν τα δεδομένα από τη συσκευή, ελπίζοντας ότι τα στοιχεία καταστρέφονται. Έτσι στις πλείστες περιπτώσεις τα διαγραμμένα δεδομένα περιέχουν κρίσιμες πληροφορίες. Από την οπτική πλευρά ενός απλού χρήστη, ο όρος ανάκτηση διαγραμμένων αρχείων σημαίνει λύση, όπως μεταφορά στον κάδο ανακύκλωσης του λειτουργικού και επαναφορά των δεδομένων, πράγμα βέβαια που λειτουργεί στα λειτουργικά Windows. Στα λειτουργικά Android είναι πολύ πιθανόν να γίνει ανάκτηση των δεδομένων των περισσότερων διαγραμμένων αρχείων αν και προτείνεται να γίνεται με συγκεκριμένες τεχνικές και μεθόδους αλλιώς μπορεί άθελα να διαγραφούν δεδομένα που δεν πρέπει. Έτσι όταν γίνεται ανάκτηση δεδομένων πρέπει να έχουμε υπόψη μερικούς κανόνες όπως [59]:

- Να μην χρησιμοποιείται το τηλέφωνο για οποιαδήποτε δραστηριότητα μετά την κατάσχεση του.
- Τα διαγραμμένα δεδομένα, για παράδειγμα μηνύματα κειμένου, υπάρχουν στην συσκευή μέχρι να χρειαστεί ο χώρος για επόμενα εισερχόμενα.
- Ακόμα και όταν το κινητό δεν χρησιμοποιείται, τα εισερχόμενα μηνύματα καταλαμβάνουν απευθείας τον χώρο που χρειάζονται, με αποτέλεσμα ο χώρος όπου υπήρχαν τα διαγραμμένα να κινδυνεύει να γεμίσει με τα καινούργια μηνύματα.

Όταν ένας χρήστης διαγράφει τα δεδομένα, αυτό που διαγράφεται είναι ο δείκτης που δείχνει σε ποια θέση μνήμης βρίσκονται αυτά τα δεδομένα. Όλα τα συστήματα αρχείων περιέχουν μεταταδεδομένα τα οποία διατηρούν πληροφορίες σχετικά με την ιεραρχία αρχείων. Η διαγραφή δεν θα διαγράψει πραγματικά τα δεδομένα αλλά καταργεί τα μεταδεδομένα. Έτσι πλέον τα δεδομένα γίνονται αόρατα μόνο από τον χρήστη αλλά εξακολουθούν να υπάρχουν στην συσκευή εφόσον δεν έχουν αντικατασταθεί ακόμα από καινούργια δεδομένα [60].

3.21. Ανάκτηση διαγραμμένων μηνυμάτων παράδειγμα

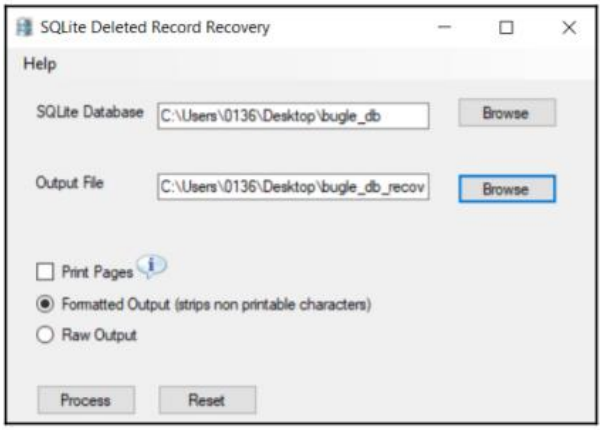
Τα πλείστα δεδομένα εφαρμογών του Android που σχετίζονται με κείμενο όπως μηνύματα και email αποθηκεύονται σε βάσεις δεδομένων SQLite. Εγγραφές στη βάση δεδομένων που επισημαίνονται ως διαγραμμένες υπάρχουν σε δύο περιοχές [61]:

1) Στην περιοχή των μη κατανεμημένων μπλοκ (unallocated blocks)

2) Στην περιοχή των ελεύθερων μπλοκ (free blocks)

Οι περισσότερες εφαρμογές εγκληματολογικών εργαλείων σαρώνουν τα μη κατανεμημένα μπλοκ και τα ελεύθερα μπλοκ. Στο παράδειγμα που θα δούμε θα ανακτήσουμε διαγραμμένα SMS από μια συσκευή Android. Το αρχείο bungle_db είναι μια βάση δεδομένων SQLite που περιέχει μηνύματα SMS που αποστέλλονται ή λαμβάνονται χρησιμοποιώντας την εφαρμογή Messages .Το αρχείο αυτό μπορεί να εντοπιστεί στη διαδρομή: **/data/data/com.android.messaging/databases**. Εάν έχει ήδη δημιουργηθεί ένα image μπορεί να εξαχθεί το συγκεκριμένο αρχείο με το FTK Imager, το οποίο αναφέρθηκε σε προηγούμενα κεφάλαια. Εάν πάλι πρέπει να εξαχθεί από την ίδια την συσκευή, αυτό μπορεί να πραγματοποιήθεί μέσω του **adb pull** (μόνο με root συσκευές). Δωρεάν προγράμματα για την βοήθεια της εξαγωγής είναι στην εφαρμογή SQLite Deleted Records Parser by Mari DeGrazia. https://github.com/mdegrazia/

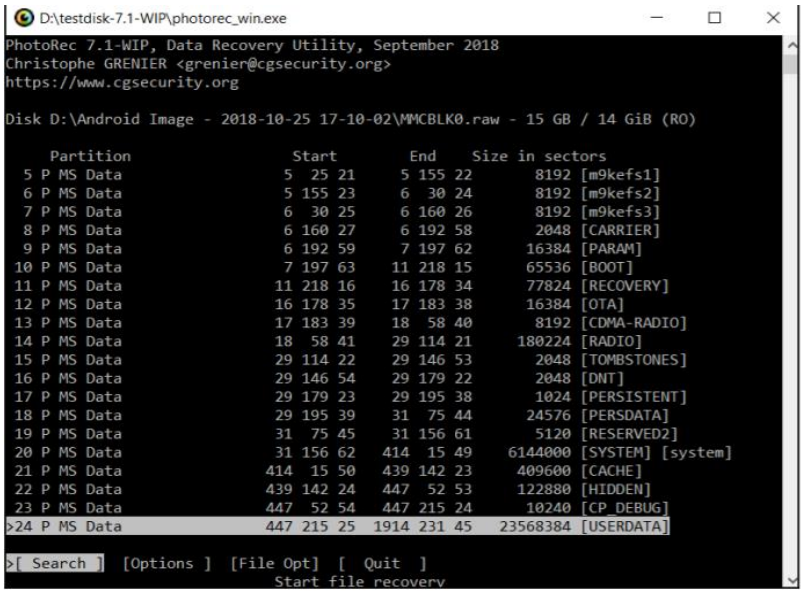
Υπάρχουν τρείς παραλλαγές του προγράμματος (Python script,command line version, GUI version). Στο παράδειγμα θα δούμε την GUI έκδοση. Στην εικόνα 3.14 φαίνεται ότι είναι πολύ εύκολη η χρήση του εργαλείου. Ως αποτέλεσμα θα δοθεί ένα αρχείο .tsv όπου με ένα πρόγραμμα αναγνώσεων βάσεων δεδομένων θα φανούν τα αποτελέσματα.



Εικόνα 3.14 Στιγμιότυπο από την μετατροπή για την εξαγωγή αρχείο .tsv

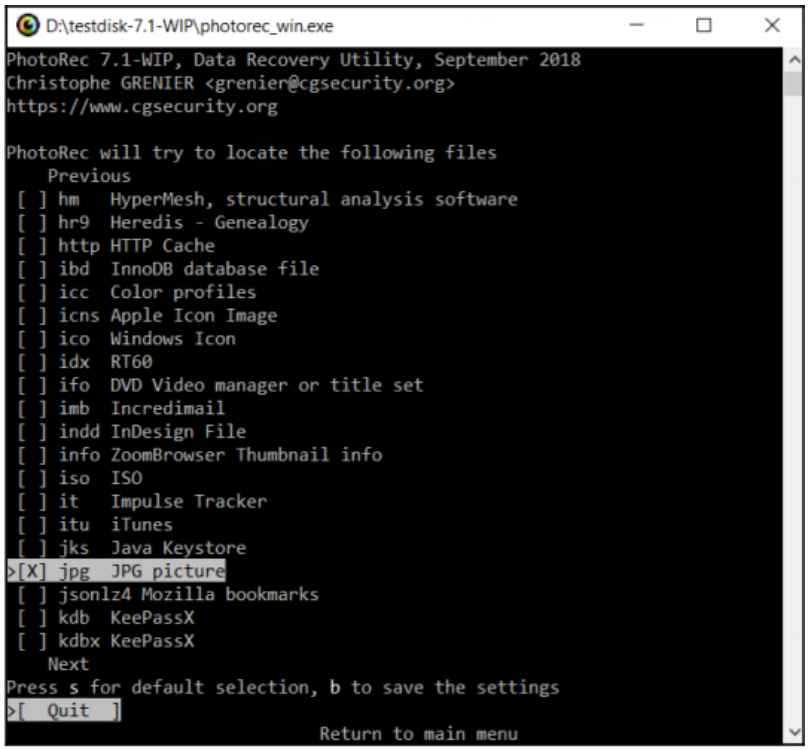
3.22. Ανάκτηση δεδομένων με την χρήση file carving

Η μέθοδος file carving είναι μια εξαιρετικά χρήσιμη μέθοδος στην εγκληματολογία επειδή επιτρέπει την ανάκτηση για ανάλυση των δεδομένων που έχουν διαγραφεί (Εικόνα 3.15). Με απλά λόγια με αυτή την τεχνική μπορούν να μαζευτούν κομμάτια ενός που βρίσκεται σε μη κατανεμημένους χώρους (unallocated memmory space) της μνήμης του συστήματος, δηλαδή χώρους που δεν υπάρχουν πληροφορίες για δεδομένα αρχείων, αφού δεν υπάρχουν δείκτες πλέον που δείχνουν σε αυτό τον χώρο μνήμης. Η επανασυναρμολόγηση των δεδομένων γίνεται με την σάρωση των bytes του δίσκου εξετάζοντας τα πρώτα και τελευταία bytes του αρχείου, για παράδειγμα για μια εικόνα αρχείου jpeg τα πρώτα bytes ξεκινούν με 0xffd8 και τελειώνουν με 0xffd9. Μια δωρεάν εφαρμογή που χρησιμοποιεί αυτή τη μέθοδο για ανάκτηση δεδομένων βρίσκεται στον σύνδεσμο https://www.cgsecurity.org/wiki/TestDisk_ Download. Με την εγκατάσταση και εκκίνηση του προγράμματος φαίνονται τα διαθέσιμα partitions που υπάρχουν για ανάλυση. Μπορεί να επιλεγεί να γίνει ανάλυση μόνο σε συγκεκριμένους τύπους αρχείων αν διερευνάται κάτι συγκεκριμένο όπως για παράδειγμα μια εικόνα ή ένα αρχείο κειμένου.



Εικόνα 3.15 Εικόνα περιβάλλοντος προγράμματος file carving

Με το τέλος της αναζήτησης και τις ενοποιήσεις των δεδομένων τα ευρήματα τοποθετούνται σε έναν υποφάκελο μέσα στον φάκελο που βρίσκεται η εφαρμογή με όνομα recup_dir [62].



Εικόνα 3.16 Επιλογή τύπων αρχείων που θέλουμε να εξάγουμε

3.23. Ανάλυση δεδομένων από βασικές εφαρμογές του λειτουργικού συστήματος Android

Wi-Fi Analysis

Το Wi-Fi τεχνικά δεν είναι μια εφαρμογή αλλά μια πολύτιμη πηγή δεδομένων. Τα δεδομένα που μπορούν να μας φανούν χρήσιμα βρίσκονται στο αρχείο **/data/misc/wifi/wpa_supplicant.conf** (Εικόνα 3.17). Το αρχείο αυτό περιέχει μια λίστα με τα σημεία πρόσβασης στα οποία έχει συνδεθεί ο χρήστης μαζί με τους κωδικούς πρόσβασης.

```
network={
    ssid="NETGEAR60"
    psk="ancientshoe601"
    key_mgmt=WPA-PSK
    priority=22
}

network={
    ssid="hhonors"
    key_mgmt=NONE
    priority=50
}
```

Εικόνα 3.17 Στιγμιότυπο από την ανάλυση του αρχείο wpa_supplicant.conf

Contact/Call Analysis

Τα αρχεία κλήσεων και επαφών αποθηκεύονται στην ίδια βάση δεδομένων. Δεδομένα βρίσκουμε στα αρχεία **com.android.providers.contacts/file/photos** και **com.android.providers.contacts/file/profile** όπως και στα αρχεία **com.android.providers.contacts/databases/contacts2.db** και **callog.db**. Στα αρχεία που βρίσκονται μέσα στο φάκελο file μπορούν να εντοπιστούν φωτογραφίες της επαφής, και περαιτέρω πληροφορίες για την επαφή. Στο αρχείο **contacts2.db** μπορούν να εντοπιστούν όλες οι

πληροφορίες για τις επαφές του χρήστη. Στο αρχείο **calllog.db** εντοπίζονται όλες οι πληροφορίες για τις εισερχόμενες/εξερχόμενες και χαμένες κλήσεις.

SMS/MMS Analysis

Τα μηνυματα SMS και MMS αποθηκεύονται στην ίδια βάση δεδομένων. Στο φάκελο **com.android.providers.telephony/files** βρίσκονται αρχεία που έχουν σταλεί με MMS. Στο αρχείο **com.android.providers.telephony/databases/mmssms.db** και στο αρχείο **com.android.providers. contacts.telephony** παρέχονται επιπλέον πληροφορίες για τα μηνύματα.

Gmail Analysis

Η Gmail είναι υπηρεσία ηλεκτρονικού ταχυδρομείου που παρέχεται από την εταιρία Google. Στις κινητές συσκευές android, για την εκκίνηση της συσκευής και την σωστή λειτουργία της, χρειάζεται να δημιουργηθεί ένα ηλεκτρονικό ταχυδρομείο ή να γίνει σύνδεση με το υπάρχον. Στον φάκελο **/com.google.android.gm/cache** περιέχονται πρόσφατα αρχεία τα οποία είτε έχουν σταλεί είτε είναι εισερχόμενα.

Google Chrome Analysis

Το Google Chrome είναι ένα γνωστό πρόγραμμα περιήγησης ιστού και πλέον είναι η προεπιλογή σε πάρα πολλές συσκευές. Τα δεδομένα που μπορούν να βρεθούν είναι πιθανόν δεδομένα στα οποία έχει περιηγηθεί ο χρήστης όχι μόνο στην συγκεκριμένη συσκευή αλλά σε όποια άλλη συσκευή έχει συνδεθεί με το ίδιο λογαριασμό. Αυτό δημιουργεί ένα μικρό αλλά πρόβλημα, το οποίο όμως είναι επιλύσιμο, αφού δίνεται αρκετά μεγάλος όγκος δεδομένων στον εξεταστή. Όλα τα δεδομένα που βρίσκονται μέσα στον φάκελο **com.android.chrome/app_chrome/Default/** είναι αποθηκευμένα σε αρχεία στη βάση δεδομένων SQLite. Στο αρχείο **com.android.chrome/app_chrome/Default/SyncData.sqlite3** περιέχεται μια λίστα με δεδομένα όπως ιστορικό, αυτόματη συμπλήρωση, αγαπημένες ιστοσελίδες, κωδικοί.

Facebook Analysis

Η γνωστή πλατφόρμα κοινωνικού δικτύου facebook μετράει πάνω από 1,000,000,000 λήψεις μόνο από το google play. Στον φάκελο **com.facebook.katana/files/video-cache** μπορούν να εντοπιστούν από την αρχική σελίδα εικόνες και βίντεο που ανέβασαν άλλοι χρήστες. Στον φάκελο **com.facebook.katana/cache/images** μπορούν να εντοπιστούν εικόνες από την αρχική σελίδα του χρήστη καθώς επίσης και φωτογραφίες χρηστών. Στο αρχείο **com.facebook.katana/databases/ bookmarks_db2** εμφανίζονται λίστες με ομάδες και εφαρμογές που συμμετέχει ο χρήστης. Στο αρχείο **com.facebook.katana/databases/contacts_db2** εμφανίζονται όλες οι πληροφορίες για τα άτομα τα όποια είναι φίλοι με τον χρήστη.

Facebook Messenger Analysis

Το Facebook Messenger είναι μια εφαρμογή ανταλλαγής μηνυμάτων ξεχωριστή πλέον από την εφαρμογή Facebook έχει πάνω από 500.000.000 λήψεις μόνο από το google play. Στον φάκελο **com.facebook.orca/cache/audio** περιέχονται ηχητικά μηνύματα τα οποία έχουν αποσταλεί από την εφαρμογή. Τα αρχεία έχουν επέκταση .cnt αλλά στην πραγματικότητα είναι αρχεία RIFF που μπορούν να αναπαραχθούν μέσω προγραμμάτων Windows Media Player,Vlc. Στον φάκελο **com.facebook.orca/cache/fb_temp** περιέχει αρχεία temp για εικόνες και βίντεο που αποστέλλονται μέσω της εφαρμογής. Δεν είναι σαφές για πόσο καιρό παραμένουν τα αρχεία σε αυτό τον φάκελο. Στον φάκελο **com.facebook.orca/databases/call_log.sqlite** περιέχονται αρχεία καταγραφής των κλήσεων που έχουν γίνει μέσω της εφαρμογής.

Viber Analysis

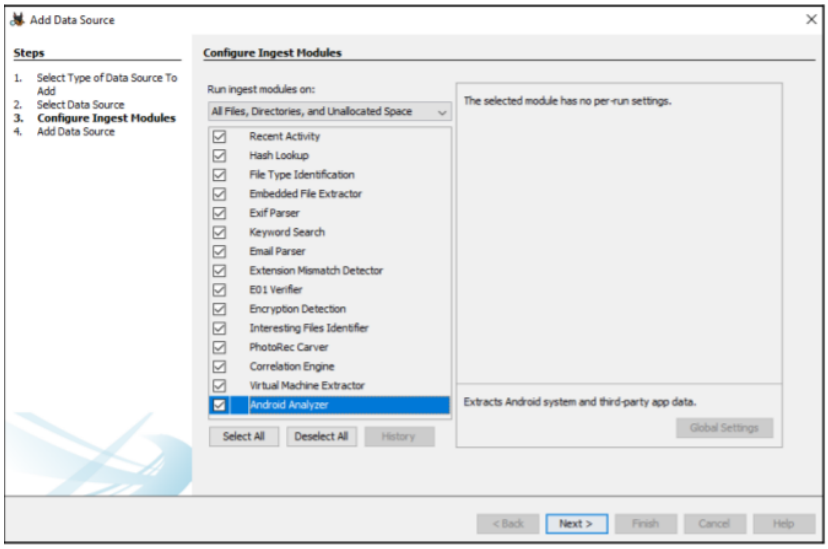
Παρομοίως με το viber, αποτελεί εφαρμογή ανταλλαγής μηνυμάτων και κλήσεων με πάνω από 100,000,000 λήψεις. Στον φάκελο **com.viber.voip/files/preferences** περιέχεται το ICCID της κάρτας Sim, το όνομα του χρήστη και ο αριθμός τηλεφώνου που χρησιμοποιήθηκε για την εγγραφή στην εφαρμογή. Στον φάκελο **com.viber.voip/sdcard/viber/media** αποθηκεύονται φωτογραφίες προφίλ τον επαφών του χρήστη καθώς και όλες οι εικόνες/βίντεο που έχουν σταλεί μέσω της εφαρμογής [63].

3.24. AutoSpy

Το πρόγραμμα AutoSpy είναι ένα δωρεάν ανοικτού κώδικα πρόγραμμα που δημιουργήθηκε από τον Brian Carrier (Εικόνα 3.18). Η πρώτη έκδοση της εφαρμογής υποστηριζόταν μόνο στα λειτουργικά Linux αλλά πιο μετά στην 3η έκδοση της εφαρμογής μπορούσε να τρέξει πλέον και στα λειτουργικά Windows. Η εφαρμογή υπάρχει διαθέσιμη στον σύνδεσμο http://www.sleuthkit.org/autospy/. Παρακάτω παρουσιάζεται ένα παράδειγμα όπου αναλύεται ένα image από μια συσκευή android.

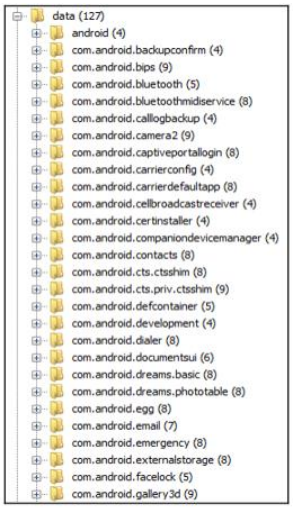
Πριν την εκκίνηση της σάρωσης και της εξαγωγής, εμφανίζεται ένας πίνακας των ingest modules όπου υπάρχουν ενσωματωμένα εργαλεία που βοηθούν να γίνει μια πιο εξιδεικευμένη έρευνα. Για παράδειγμα μπορεί να επιλεγεί:

- Recent activity: Πρόσφατες δραστηριότητες που έχει κάνει ο χρήστης στην κινητή συσκευή όπως ιστορικό περιήγησης, πρόχειρα μηνύματα, εγκατάσταση προγραμμάτων.
- Keyword Search: Σαρώνει για λέξεις κλειδιά που έχουν ανατεθεί.
- PhotoRec Carver: Σάρωση σε μη κατανεμημένους χώρους για δεδομένα.



Εικόνα 3.18 Στιγμιότυπο από το πρόγραμμα AutoSpy πριν τη σάρωση

Με το τέλος της σάρωσης φαίνεται ότι εντοπίστηκαν 28 partitions στην συσκευή (Εικόνα 3.19). Για την περαιτέρω διερεύνησή τους μπορεί απλά να επιλεγεί το partition που θέλει ο ερευνητής και θα φανούν οι υποφακέλοι. Για παράδειγμα αν επιλεγεί ο φάκελος data πολύ πιθανόν να εντοπιστούν υποφακέλοι που αναλύθηκαν σε προηγούμενη ενότητα



Εικόνα 3.19 Αποτελέσματα του προγράμματος AutoSpy

Αν ο ερευνητής γνωρίζει καλά την ιεραρχία τον android και πού να ψάξει για συγκεκριμένα δεδομένα, με τη χρήση του AutoSpy μπορεί εύκολα να εντοπίσει πιθανά τεκμήρια [64].

ΚΕΦΑΛΑΙΟ 4. ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ

Στη συνέχεια εξετάζεται πώς μπορεί να γίνει μια εξαγωγή από μια κινητή συσκευή με δικαιώματα root δεδομένα μέσω των διάφορων τεχνικών που εξηγήθηκαν πιο πάνω.

Τεχνικά Χαρακτηριστικά:

- Συσκευή – Motorola
- Μοντέλο – Nexus 6
- Χωρητικότητα – 32 GB
- Μνήμη – 2 GB
- Λειτουργικό Σύστημα – Android 10
- Δικαιώματα χρήστη : Root

1ο Παράδειγμα

Στο πρώτο παράδειγμα παρουσιάζεται ένα σενάριο όπου η συσκευή θεωρείται ότι περιέχει κρίσιμα δεδομένα για τη διευκόλυνση μιας έρευνας σχετικά με μια υπόθεση κατοχής απαγορευμένου περιεχομένου. Ο χρήστης υπέστη σοβαρό ατύχημα και δεν είναι σε θέση να δώσει πληροφορίες για το ξεκλείδωμα της συσκευής, η οποία είναι ασφαλισμένη με μια σειρά από χαρακτήρες για κωδικό. Οι ερευνητές θέλουν να διατηρήσουν την ακεραιότητα των δεδομένων για να μπορούν να γίνουν αποδεκτά στο δικαστήριο. Ανάλογα με την έκδοση του λειτουργικού Android ο τρόπος χειρισμού της συσκευής είναι διαφορετικός. Στη συγκεκριμένη περίπτωση θα δημιουργηθεί επικοινωνία μεταξύ υπολογιστή συσκευής μέσω του adb shell και με εντολές sql θα διαγραφούν οι καταχωρήσεις του κωδικού κλειδώματος. Η συσκευή διαθέτει την έκδοση Android 10 του λειτουργικού συστήματος Android που είναι σχετικά καινούργια. Γενικά από την έκδοση Android Oreo και μετά χρησιμοποιείται άλλη τεχνική για να ξεπεραστεί μια οθόνη κλειδώματος ενώ πριν την έκδοση χρησιμοποιείτο άλλη. Στην παρούσα περίπτωση γίνεται είσοδος στο τερματικό του υπολογιστή και γράφεται η εντολή adb shell, η οποία δίνει την πρόσβαση για περιήγηση μέσα στα αρχεία της κινητής συσκευής. Γίνεται μεταφορά στον φάκελο /data/system. Για τη μετάβαση στο συγκεκριμένο φάκελο ο χρήστης πρέπει να έχει δικαιώματα root. Αφού γίνει είσοδος μέσα στο φάκελο /data/system πρέπει να εντοπιστεί το αρχείο με όνομα locksettings.db. Μέσα στο αρχείο αυτό είναι αποθηκευμένος ο κωδικός ασφαλείας της οθόνης κλειδώματος. Για την επεξεργασία του αρχείου με την βοήθεια εντολών sql γίνεται αλλαγή της καταχώρησης στο αρχείο locksettings.db. Μετά την επανεκκίνηση της κινητής συσκευής φαίνεται ότι πλέον δεν χρειάζεται κωδικός για να ξεκλειδώσει η συσκευή. Αν το λειτουργικό είχε παλαιότερη έκδοση λογισμικού πάλι θα γινόταν μεταφορά στον φάκελο /data/system αλλά θα διαγραφόταν όποιο αρχείο είχε κατάληξη .key.

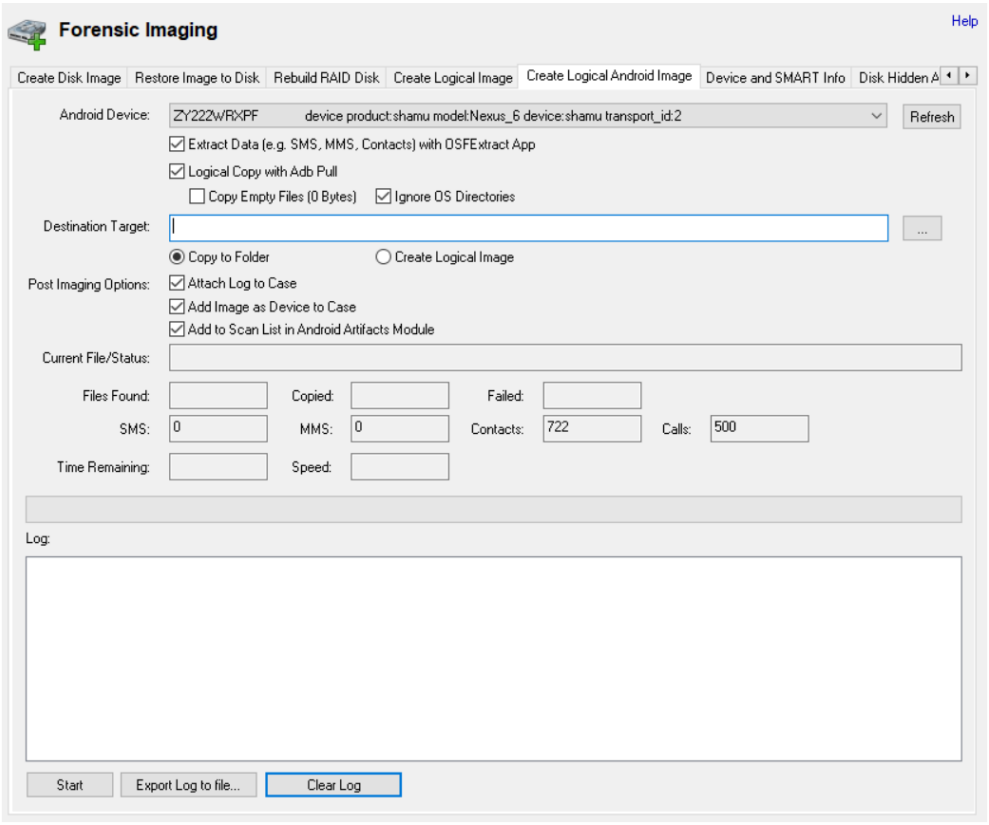
2ο Παράδειγμα

Στο δεύτερο παράδειγμα χρειάστηκε να δημιουργηθεί ένα logical image της κινητής συσκευής για εύρεση και ανάλυση των αποδεικτικών στοιχείων. Το σενάριο σε αυτή την περίπτωση είναι η ανάγνωση μηνυμάτων αρχείων κλήσεων διαγραμμένων δεδομένων για περισσότερες πληροφορίες σχετικά με μια υπόθεση υποκλοπής προσωπικών δεδομένων. Για την δημιουργία του logical image χρησιμοποιήθηκε το λογισμικό OSForensics και για ανάλυση των δεδομένων το AutoSpy. Η εφαρμογή OSForensics παρέχει την υπηρεσία για την δημιουργία ενός logical virtual image file δηλαδή επιτρέπει στον εκάστοτε ερευνητή να αντιγράψει αρχεία και καταλόγους από μια συσκευή Android σε ένα αρχείο, στην περίπτωση αυτή σε ένα αρχείο τύπου .vhd (virtual hard disk), διατηρώντας όσο γίνεται περισσότερα μεταδεδομένα των αρχείων όπως ημερομηνία, χαρακτηριστικά, επεξεργασία. Η εφαρμογή για την

δημιουργία του image βασίζεται στην λειτουργία adb pull που αναφέρθηκε και πιο πάνω. Η διαδικασία ξεκινάει με την σύνδεση του υπολογιστή με την κινητή συσκευή. Στον υπολογιστή επιλέγεται η δημιουργία ενός Logical Android Image και αφού το πρόγραμμα εντοπίσει τη συσκευή ξεκινάει η μεταφορά των δεδομένων.

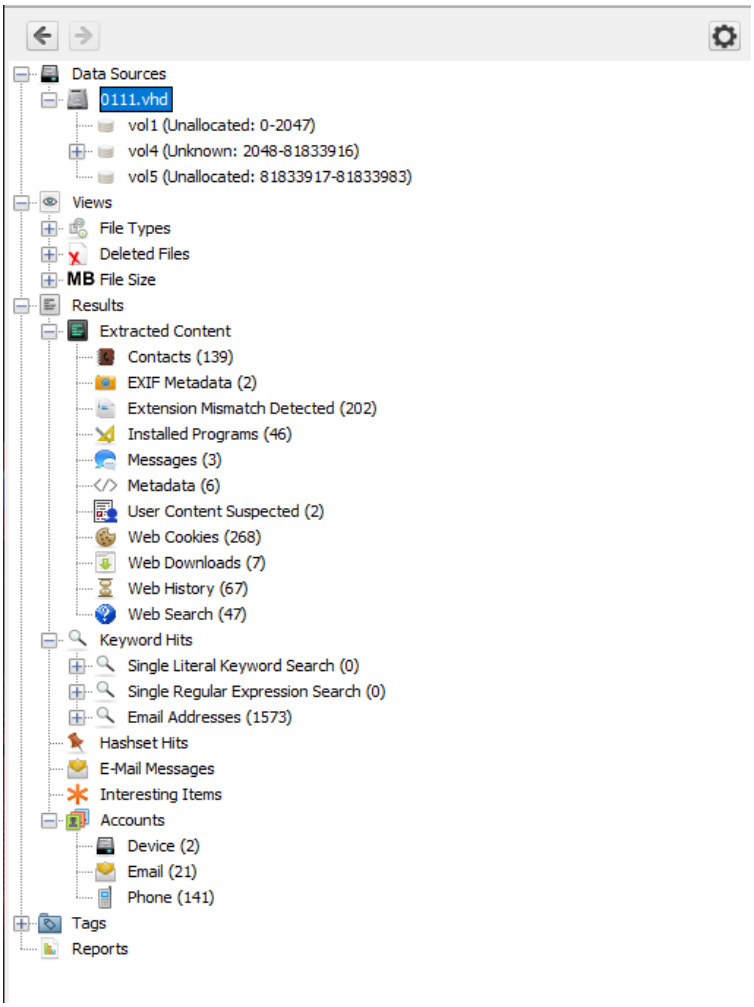
- Αρχικά συνδέεται η συσκευή με τον υπολογιστή όπου υπάρχει εγκατεστημένη η εφαρμογή OSForensics (Εικόνα 3.20)

- Επόμενο βήμα είναι να επιλεχθεί η δημιουργία ενός Forensic Image και να κατευθυνθεί ο ερευνητής στο πεδίο Create Logical Android Image.
- Τέλος ο ερευνητής επιλέγει πού θα αποθηκεύσει το αρχείο που θα δημιουργηθεί, πατά το Start.
- Μετά την δημιουργία ανοίγεται το αρχείο από το AutoSpy όπως αναφέρθηκε και στην προηγούμενη ενότητα και γίνεται η ανάλυση των δεδομένων που θα ληφθούν από το αρχείο.



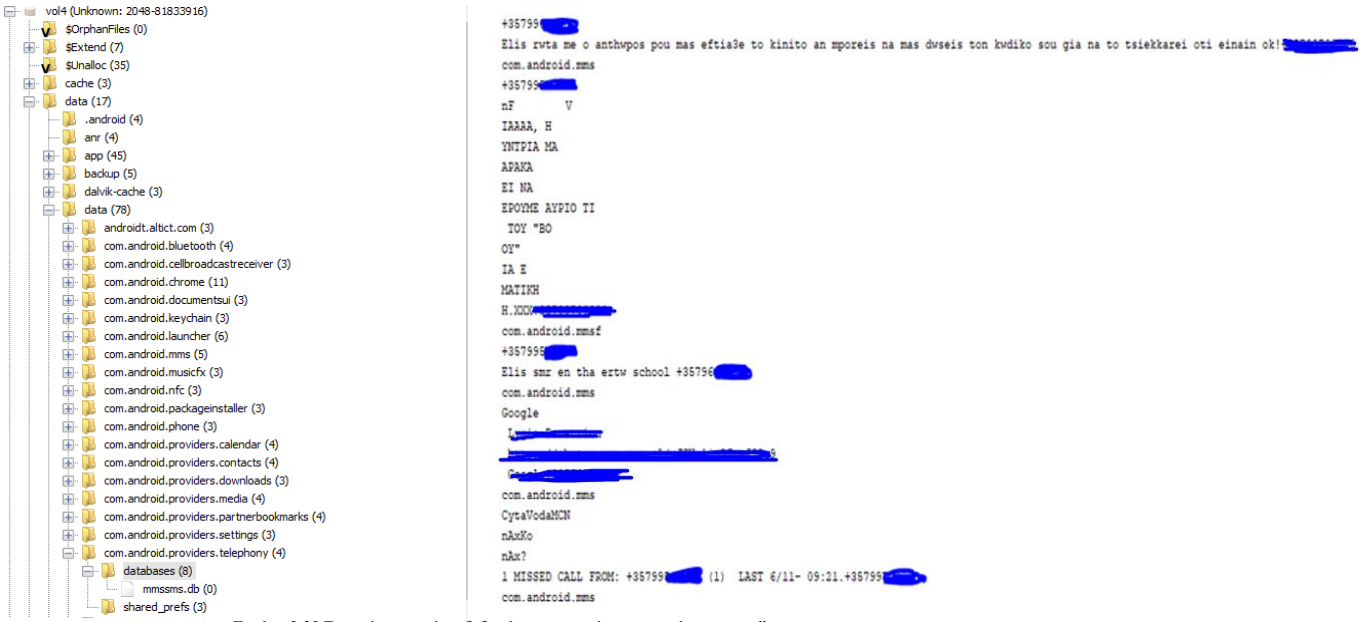
Εικόνα 3.20 Στιγμιότυπο από την εφαρμογή OSForensics

- Για να αναλυθούν τα δεδομένα πρέπει πρώτα να δημιουργηθεί μια υπόθεση στην εφαρμογή AutoSpy και να ονομαστεί η υπόθεση που θέλουμε να αποθηκευτούν τα δεδομένα και από πού να αντληθεί το αρχείο.
- Για επίσημες υποθέσεις μπορούν να προστεθούν τα στοιχεία του οργανισμού στον οποίο εργάζεται ο ερευνητής, καθώς και περαιτέρω λεπτομέρειες όπως τηλέφωνα επικοινωνίας.
- Με την ολοκλήρωση της φόρτωσης στα αποτελέσματα φαίνεται ότι το image της κινητής συσκευής είναι χωρισμένο σε τρία partition. Αυτό που μας ενδιαφέρει είναι το vol4 που περιέχει και τα δεδομένα (συνήθως υπάρχουν περισσότερα partition).



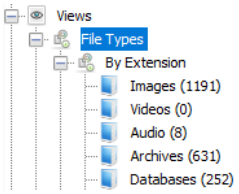
Εικόνα 3.21 Αποτελέσματα από την επεξεργασία του image της κινητής συσκευής

Με την επιλογή της επέκτασης των δεδομένων του vol4 θα φανεί το αρχείο φακέλων της κινητής συσκευής. Μέσα στον φάκελο data/app μπορούν να εντοπιστούν οι εφαρμογές που είναι εγκατεστημένες. Τα δεδομένα των εφαρμογών που αναφέρθηκαν και πιο πάνω στην ενότητα βρίσκονται στον φάκελο data/data. Για παράδειγμα, με τη μεταφορά στον φάκελο data/data/com.android.providers.telephony μπορούν να φανούν τα μηνύματα που έχουν αποσταλεί από την συσκευή. Στη συσκευή φαίνεται ότι ο χρήστης έλαβε μήνυμα για αποστολή του κωδικού πρόσβασης άρα πιθανόν να έχει γίνει από εκεί η υποκλοπή των δεδομένων.



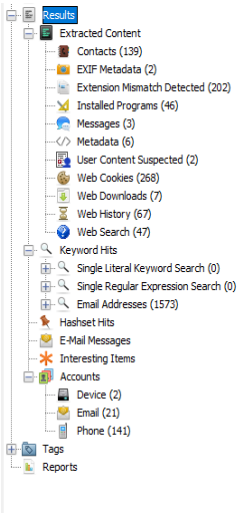
Εικόνα 3.22 Στιγμιότυπο από τα δεδομένα που περιέχει το αρχείο mmsms.db

Παρακάτω με την επέκταση του πεδίου Views φαίνονται αρχεία δεδομένων ανάλογα με τον τύπο τους, δηλαδή για παράδειγμα όλες οι εικόνες μαζί, όλα τα βίντεο, όλοι οι ήχοι (Εικόνα 3.23). Στη συνέχεια εξετάζονται τα πιο σημαντικά πεδία που μπορούν να βοηθήσουν στην υπόθεση.



Εικόνα 3.23 Στιγμιοτύπο από το πεδίο Views

Πιο κάτω βρίσκεται και το πιο σημαντικό πεδίο Result που δίνει η εφαρμογή μετά την ανάλυση του Image (Εικόνα 3.24). Σημαντικό να αναφερθεί είναι το υποπεδίο Extension Mismatch Detected που περιέχει όλα τα αρχεία τύπου .cnt, τα οποία είναι αρχεία εικόνων που εντοπίστηκαν από το AutoSpy από διάφορες τοποθεσίες στο αρχείο φακέλων της κινητής συσκευής.



Εικόνα 3.24 Στιγμιότυπο από το πεδίο Results

Στο πεδίο contacts βρίσκονται όλες οι επαφές που είχε αποθηκεύσει ο χρήστης στην κινητή συσκευή (Εικόνα 3.25)

Source File	S	C	O	Name	Phone Number	Data Source	Email
contacts2.db			2	202	[redacted]	0111.vhd	
contacts2.db			2	Aggelos [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Aggelos [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Alexis [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antonio [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antonis [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antonis [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	[redacted]
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	[redacted]@hotmail.com
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	
contacts2.db			2	Antreas [redacted]	[redacted]	0111.vhd	

Εικόνα 3.25 Στιγμιότυπο από το πεδίο contacts

Στο πεδίο Web Downloads φαίνεται το ιστορικό λήψεων καθώς και περαιτέρω χρήσιμες πληροφορίες (Εικόνα 3.26).

Source File	S	C	O	Path	URL	Date Accessed	Domain	Program Name	Data Source
History			2	/storage/emulated/0/Download/[redacted]	https://repository.kallipos.gr/bitstream/11419/3480/1/02_...	2019-11-06 19:37:03 EET	repository.kallipos.gr	Google Chrome	0111.vhd
History			2	/storage/emulated/0/Download/[redacted]	https://eclass.upatras.gr/modules/document/file.php/CMN...	2019-11-06 19:38:52 EET	eclass.upatras.gr	Google Chrome	0111.vhd
History			2	/storage/emulated/0/Download/[redacted]	https://forum.xda-developers.com/attachment.php?attach...	2020-11-17 18:15:50 EET	forum.xda-developers.com	Google Chrome	0111.vhd
History			2	/storage/emulated/0/Download/[redacted]	https://dl.xda-cdn.com/3/0/0/8/5/2/7/adbd-Insecure-v2.0...	2020-11-17 18:15:50 EET	dl.xda-cdn.com	Google Chrome	0111.vhd
History			2	/storage/emulated/0/Download/[redacted]	ftp://ftp.netbsd.org/pub/pkgsrc/current/pkgsrc//net/netca...	2020-11-18 18:15:06 EET	ftp.netbsd.org	Google Chrome	0111.vhd
History			2	/storage/emulated/0/Download/[redacted]	http://supersuroot.org/downloads/supersu-2-82.apk	2020-11-20 15:13:14 EET	supersuroot.org	Google Chrome	0111.vhd
History			2	/storage/emulated/0/Download/[redacted]	https://supersuroot.org/downloads/supersu-2-82.apk	2020-11-20 15:13:14 EET	supersuroot.org	Google Chrome	0111.vhd

3.26 Στιγμιότυπο από το πεδίο Web Downloads

Στο πεδίο Web Search φαίνονται οι αναζητήσεις που έχει κάνει ο χρήστης (Εικόνα 3.27).

Source File	S	C	O	Domain	Text	Program Name	Date Accessed
History				www.google.com	[redacted]	Google Chrome	2020-11-11 17:11:33 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-11 17:11:38 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-11 17:11:38 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:13:46 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:13:46 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:13:46 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:15:25 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:15:25 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:15:25 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:15:12 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:15:25 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:15:27 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-17 18:15:27 EET
History				www.google.com	[redacted]	Google Chrome	2020-11-18 18:13:49 EET

3.27 Στιγμιότυπο Web Search

Στο πεδίο Phone φαίνεται σε ποιους αριθμούς έχουν γίνει κλήσεις είτε εξερχόμενες είτε εισερχόμενες (Εικόνα 3.28).

Source File	S	C	O	Account Type	ID
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]
contacts2.db			2	PHONE	[redacted]

Εικόνα 3.28 Στιγμιότυπο από το πεδίο Phone

ΚΕΦΑΛΑΙΟ 5. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ

Η εγκληματολογική Πληροφορική ακόμη και σήμερα δεν θεωρείται σαν μια επιστήμη ισάξια με την ανθρώπινη εγκληματολογία. Παρόλα αυτά και σύμφωνα με τον υπεύθυνο του τμήματος ηλεκτρονικού εγκλήματος Κύπρου, σχεδόν σε κάθε ποινικό έγκλημα, προσωπικές κινητές συσκευές αλλά και υπολογιστές κατάσχονται για ανάλυση και για εντοπισμό ευρύτερων αποδεικτικών στοιχείων. Μόνο από αυτή την αναφορά γίνεται αντιληπτό ότι η εγκληματολογική πληροφορική αποτελεί πλέον σημαντικό εργαλείο στην επίλυση εγκλημάτων αλλά και στην σωστή κατανομή ευθυνών και ποινών στα άτομα που εμπλέκονται. Περισσότερο όμως διαφαίνεται ότι αν τα άτομα με καίριες θέσεις δεν έχουν τις βασικές γνώσεις γύρω από τον τομέα της πληροφορικής δεν μπορούν να συμπεράνουν και να εξάγουν σωστά συμπεράσματα με βάση τα ηλεκτρονικά τεκμήρια. Επομένως πρέπει να καταβληθεί προσπάθεια για να αναδειχθεί η σημασία που έχει η εγκληματολογική πληροφορική [65].

5.1. Εγκληματολογική Πληροφορική

Ο ψηφιακός κόσμος σήμερα είναι μια πηγή από πληροφορίες σε μέγεθος που δεν μπορεί κατ' ακρίβεια να προσδιοριστεί. Καθημερινά μέσα από το διαδίκτυο διακινούνται προσωπικά δεδομένα, εμπιστευτικά μηνύματα, κρυπτογραφημένες αλληλογραφίες, τραπεζικές συναλλαγές, αγορές. Από την άλλη, η χρήση της ψηφιακής τεχνολογίας για παράνομες ενέργειες, υποκλοπές και παρακολουθήσεις αποτελεί πλέον δεδομένο. Δισεκατομμύρια χάνονται καθημερινά στον επιχειρηματικό κόσμο λόγω διαρροής πληροφορίων ή μολύνσεις του δικτύου τις εταιρίας με σκοπό την καταστροφή ολόκληρου του συστήματος. Από πλευράς των αρχών αυτή η απότομη ανάπτυξη του ψηφιακού εγκλήματος θεωρείται μια τεράστια πρόκληση, αφού για να θεωρηθεί στο δικαστήριο ένα τεκμήριο αποδεκτό πρέπει να πληροί συγκεκριμένες προϋποθέσεις, κάτι που καθιστά δύσκολο το έργο των αρχών. Πέρα όμως από τα τεκμήρια, πιο γενικά οι υποθέσεις που έχουν να κάνουν με το ψηφιακό έγκλημα χρήζουν ειδικής μεταχείρισης από άτομα με γνώσεις, αφού η τόσο ραγδαία ανάπτυξη του ψηφιακού κόσμου παρέχει ένα σημαντικό όπλο για τις αρχές. Η συλλογή των ψηφιακών δεδομένων ενός υπόπτου μπορεί να βοηθήσει στη διαλεύκανση μιας υπόθεσης, αφού υπάρχουν τόσα πολλά δεδομένα που μπορεί να βρει κάποιος, ακόμα και ο πιο προσεκτικός εγκληματίας κάπου αφήνει τα ψηφιακά του αποτυπώματα. Επομένως, μπορεί οι ψηφιακές υποθέσεις να αποτελούν ιδιαίτερες περιπτώσεις αλλά η όλη εικόνα δείχνει ότι ο ψηφιακός κόσμος μπορεί και να αποτελέσει ένα σημαντικό βοηθητικό εργαλείο για τον ερευνητή [66].

5.2. Εργαλεία Εγκληματολογικής Πληροφορικής

Η ανάπτυξη έφερε και καινούργια εργαλεία που είναι ένας βασικός πυλώνας για την αποφυγή αμφισβήτησης των δεδομένων που θεωρείται ο μεγαλύτερος αντίπαλος της ψηφιακής εγκληματολογίας. Μέχρι και πρόσφατα, στοιχεία από τους κατηγόρους εύκολα μπορούσαν να διαψευσθούν είτε γιατί δεν υπήρχε επαρκής γνώση στο προσωπικό, αλλά και λογισμικά που με διάφορες τεχνικές εγγυούνται την ακεραιότητα των δεδομένων. Αφού όμως η ανάπτυξη της ψηφιακής τεχνολογίας είναι κατακόρυφη, η κοινωνία χρειάζεται αρκετό χρόνο να εκπαιδευτεί και να είναι έτοιμη να αντιμετωπίσει τέτοιες προκλήσεις, ενώ σε επίπεδο εκπαίδευσης λίγες είναι οι εκπαιδευτικές μονάδες που μπορούν να παρέχουν τέτοια εκπαίδευση στον συγκεκριμένο χώρο της πληροφορικής. Η ανάγκη όμως για άτομα με γνωστικό πεδίο την εγκληματολογική πληροφορική υπάρχει γιατί αν προχωρήσει το ψηφιακό έγκλημα, χωρίς άτομα με γνώσεις δεν θα μπορεί να αντιμετωπιστεί αποτελεσματικά [67].

5.3. Μοντέλα και η εφαρμογή τους

Ένα επιπλέον βοήθημα στην αντιμετώπιση του ψηφιακού εγκλήματος είναι και τα διάφορα μοντέλα που δείχνουν ότι ανάλογα βέβαια και με την φύση του εγκλήματος μπορούν να γίνουν κάποια βήματα για την σωστή έρευνα, ανάλυση, και επίλυση μιας υπόθεσης. Βέβαια, πάντα πρέπει να λαμβάνονται υπόψη οι τυπικές διαδικασίες για την αντιμετώπιση ενός συμβάντος, καθώς και ότι η τεχνολογία αναπτύσσεται, οι συσκευές αλλάζουν, τα λειτουργικά συστήματα αναβαθμίζονται και τα μοντέλα προσφέρονται για τις υφιστάμενες συσκευές, χωρίς να εγγυούνται κάλυψη για μεταγενέστερες συσκευές. Επομένως, πρέπει να γίνουν κατανοητές οι βασικές αρχές, όπως για παράδειγμα ότι πρέπει να ελέγχεται ο χώρος όπου διενεργείται μια έρευνα, τα δεδομένα πρέπει πάντα να είναι ασφαλή, η ακεραιότητα τους να μην αμφισβητείται, η ανάλυση να γίνεται σε ασφαλές περιβάλλον και τα τεκμήρια να παρουσιάζονται σωστά με λεπτομέρειες [68].

5.4. Εγκληματολογική Πληροφορική στις κινητές συσκευές

Υπολογίζεται ότι υπάρχουν γύρω στις 3.8 εκατομμύρια έξυπνες κινητές συσκευές ανά τον κόσμο, ενώ στις ανεπτυγμένες χώρες σχεδόν όλοι έχουν στην κατοχή τους μια τέτοια συσκευή. Εκτός από την επικοινωνία με άλλα άτομα, οι κινητές συσκευές εξυπηρετούν και άλλους σκοπούς όπως ψυχαγωγία, διεκπεραίωση υποχρεώσεων, αποστολή ηλεκτρικονικών μηνυμάτων μέσω email, πλοήγηση και άλλες καθημερινές δραστηριότητες. Έτσι με όλες αυτές τις διαθέσιμες λειτουργίες που παρέχουν, οι σύγχρονες κινητές συσκευές είναι πηγές δεδομένων του εκάστοτε χρήστη. Συνομιλίες, ιστορικά κλήσεων, φωτογραφίες, ιστορικό περιήγησης μπορούν να προσδιορίσουν τόσο το προφίλ του χρήστη αλλά και τις ενέργειες που έχει διαπράξει στο παρελθόν [69]. Όπως αναφέρθηκε από το ειδικό προσωπικό της πάταξης του ηλεκτρονικού εγκλήματος της Αστυνομίας Κύπρου, ακόμη και αν μια υπόθεση δεν είναι ψηφιακής φύσεως έγκλημα, οι προσωπικές κινητές συσκευές του χρήστη κατάσχονται για διερεύνηση αφού μπορεί να περιέχουν πληροφορίες που να εξιχνιάσουν την υπόθεση. Αυτό συμβαίνει γιατί αν σε μια κινητή συσκευή δεν έχει υποστεί κάποια διαγραφή δεδομένων ή ζημιά, εύκολα μπορεί να αποκτηθεί πρόσβαση σε χρήσιμα δεδομένα.

5.5. Προτάσεις βελτίωσης

Ο ψηφιακός κόσμος μπήκε για τα καλά στην καθημερινότητα μας. Η πλειονότητα οργανισμών και επιχειρήσεων βασίζεται σε ψηφιακές συσκευές για την σωστή λειτουργία και ανάπτυξη. Μεγάλες ποσότητες δεδομένων παράγονται και διαδίδονται καθημερινά πράγμα που πολλές εταιρίες θεωρούν ακίνδυνο, με αποτέλεσμα να μην επενδύουν σε λύσεις προστασίας τους από επιθέσεις. Πρέπει να υπάρξει μια σωστή ενημέρωση σχετικά με τους σύγχρονους κινδύνους και τις απώλειες που μπορεί να προκύψουν από αυτούς. Είναι επίσης απαραίτητη η ανάπτυξη των ικανοτήτων των ανθρώπων που είναι στο χώρο της ψηφιακής εγκληματολογίας.

Η εγκληματολογική πληροφορική σε σύγκριση με της προηγούμενες δεκαετίες έχει φτάσει σε σημείο που μπορεί να αντιμετωπίζει και να διαλευκάνει τις πλείστες υποθέσεις. Υπάρχουν αρκετές εφαρμογές που βοηθάνε σε αυτό το έργο. Όμως καθώς εξελίσσεται η τεχνολογία, τα δεδομένα είναι πολύ περισσότερα. Άρα είναι απαραίτητες οι πιο κάτω προϋποθέσεις: μια πιο έξυπνη αναλυτική προσέγγιση στα δεδομένα, μια πιο ομαλή πρόσβαση στην εξαγωγή των δεδομένων χωρίς τους περιορισμούς δικαιωμάτων, εύρεση μιας καθολικής διαδικασίας εξαγωγής χωρίς δυσκολίες που προκύπτουν αν μια συσκευή είναι άλλο μοντέλο ή μάρκα ή λογισμικό και η ανάπτυξη εργαλείων με ταχύτερους χρόνους διαχείρισης και δημιουργίας αντίγραφου της συσκευής.

Θα πρέπει επίσης ό κάθε χρήστης να γνωρίζει ότι η συσκευή κρατάει πολύ περισσότερα δεδομένα απ' ότι έχει στο μυαλό του, ενώ η μη ασφαλής χρήση μιας κινητής συσκευής εύκολα μπορεί να την μετατρέψει σε στόχο για υποκλοπή προσωπικών δεδομένων και κάποιου χρηματικού ποσού. Μια γενική ενημέρωση σχετικά με απλούς τρόπους προφύλαξης της συσκευής διαγραφής δεδομένων που προδίδουν ευαίσθητα προσωπικά δεδομένα είναι ένας τρόπος ευαισθητοποίησης και εξοικείωσης των χρηστών σχετικά με τους κινδύνους που υπάρχουν. Έτσι η χρήση των μέσων κοινωνικής δικτύωσης που ως επί το πλείστο γίνεται από κινητές συσκευές και οι πληροφορίες που δημοσιεύουν οι χρήστες καθημερινά μπορούν εύκολα να τους κάνουν στόχους για διαφορές κακόβουλες ενέργειες.

Επομένως, πρέπει η πανεπιστημιακή κοινότητα να συνεργαστεί με τους ειδικούς στην επιστήμη της εγκληματολογικής πληροφορικής σε ερευνητικό επίπεδο για τον εμπλουτισμό των γνώσεων, τη δημιουργία περισσότερων μοντέλων και καινούργιων ιδεών για την πάταξη του ψηφιακού εγκλήματος και την προσθήκη σεμιναρίων και μαθημάτων σχετικά με αυτό τον τομέα.

5.6 Μελλοντικές επεκτάσεις

Με την διεκπεραίωση της πτυχιακής εργασίας στο μέλλον θα ήθελα να ασχοληθώ με την έρευνα και καταπολέμηση υποθέσεων στον επιχειρηματικό κόσμο. Εκεί συναντώνται οι μεγαλύτερες υποθέσεις, οι πιο συχνές επιθέσεις, ενώ υπάρχει καθημερινή τριβή με καινούργιες προκλήσεις, κάτι που καθιστά έναν άτομο καλύτερο γνώστη στα θέματα καινούργιων τεχνολογιών και επιθέσεων, και πιο έτοιμο για σωστή αντιμετώπιση των κρίσεων. Ακόμη πιο ενδιαφέρουσα είναι μια θέση στην ομάδα καταπολέμησης ηλεκτρονικού εγκλήματος του κράτους, η οποία περιλαμβάνει περιπτώσεις με διαφορετικές υποθέσεις πιο ανθρωποκεντρικής φύσεως, όπως απειλές για δημοσίευση προσωπικών δεδομένων που αποτελεί ένα εξίσου ενδιαφέρον πεδίο. Αν και η θέση αυτή ενέχει τεράστιες ευθύνες, επιτρέπει να εφαρμοστούν οι γνώσεις για το κοινό καλό, κάτι που δίνει κίνητρο για περισσότερη γνώση.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Διαδικτυακές Πηγές

[6]39 Worrying Cyber Crime Statistics [Updated for 2020] (legaljobsite.net)

[17]https://www.researchgate.net/profile/Yatendra-Gupta/publication/228410430_Systematic_Digital_Forensic_Investigation_Model/links/56ea8cd208ae95bddc2bcc6b/Systematic-Digital-Forensic-Investigation-Model.pdf

[20]https://www.researchgate.net/profile/Yatendra-Gupta/publication/228410430_Systematic_Digital_Forensic_Investigation_Model/links/56ea8cd208ae95bddc2bcc6b/Systematic-Digital-Forensic-Investigation-Model.pdf

[21] https://info.publicintelligence.net/usssbestpractices.pdf

[24] PALADIN | The World's Most Popular Linux Forensic Suite (sumuri.com)

[25] SANS Digital Forensics and Incident Response Blog | Investigate and fight cyberattacks with SIFT Workstation | SANS Institute

[26] https://truxtonforensics.com/product/portable-forensics-lab-w-xry/

[34] Forensic Investigation with Redline - Infosec Resources (infosecinstitute.com)

[35]https://www.gartner.com/en/newsroom/press-releases/2018-01-29-gartner-says-worldwide-device-shipments-will-increase-2-point-1-percent-in-2018

[39] https://developer.android.com/studio/command-line

[42] https://developer.android.com/studio/command-line/adb

[43] An A-Z Index of the Linux command line - SS64.com

[58] http://lowcostwin4n6.blogspot.com/

[62] https://resources.infosecinstitute.com/topic/file-carving/

Βιβλία

[8] Practical Digital Forensics By Richard Boddington Chapter 1 The Role of Digital Forensic and its Enviroment.

[12] Practical Digital Forensics By Richard Boddington Chapter 3 The Nature and Special Properties of Digital Evidence

[14] Practical Digital Forensics By Richard Boddington Chapter 2 Hardware and Software Enviroments

[27] Digital Forensics and Incident Response By Gerard Johansen Chapter 3 Network Evidence Collection

[33] Digital Forensics and Incident Response By Gerard Johansen Chapter 7 Analyze System Memmory

[63] Learning Android Forensics Second Edition By Oleg Skulkin, Donnie Tindall, Rohit Tamma Chapter 7 Forensics Analysis of Android Applications

[64] Learning Android Forensics Second Edition By Oleg Skulkin, Donnie Tindall, Rohit Tamma Chapter 8 Android Forensics Tools Overview

Άρθρα σε περιοδικά

[1] Akkaladevi S, Keesara H & Luo X (2011) Efficient forensic tools for handheld device: a comprehensive perspective. *Softw Eng Res Manag Appl Stud Comput Intell 377*:349–359

[2] Andriotis P, Oikonomou G, Tryfonas T (2012) Forensic analysis of wireless networking evidence of android smartphones. *2012 I.E. International Workshop on Information Forensics and Security*, pp. 109–114

[3] Choi J, Jang B, & Kim GJ (2011) Organizing and presenting geospatial tags in location-based augmented reality. *Pers Ubiquit Comput 15*(6):641–647

[4] Dearman D, Inkpen M, & Truong N (2010) Mobile map interactions during a rendezvous: exploring the implications of automation. *Pers Ubiquit Comput 14*(1):1–13

[5] Iqbal B, Iqbal A, & Obaidli HA (2012) A novel method of iDevice (iPhone, iPad, iPod) forensics without jailbreaking. *2012 International Conference on Innovations in Information Technology*, pp. 238–243

[7] Kim GH, Kim YG, & Chung KY (2013) Towards virtualized and automated software performance test architecture. *Multimed Tools Appl*. doi:10.1007/s11042-013-1536-3

[9] Kim H, Reitmayr G, & Woo W (2013) IMAF: in situ indoor modeling and annotation frame-work on mobile phones. *Pers Ubiquit Comput 17*(3):571–582

[10] Ko JW, Chung KY, & Han JS (2013) Model transformation verification using similarity and graph comparison algorithm. *Multimed Tools Appl.* doi:10.1007/s11042-013-1581-y

[11] Kubi AK, Saleem S, & Popov O (2011) Evaluation of some tools for extracting e-evidence from mobile devices. *Proc. of the International Conference on Application of Information and Communication Technologies*, pp. 1–6

[12] Kuntze N, & Rudolph C (2011) Secure digital chains of evidence. *Proc. of the IEEE Inter-national Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 1–8

[13] Lim JH, Song CW, Chung KY, Rim KW, & Lee JH (2012) Forensic evidence collection procedures of smartphone in crime scene. *Proc. of the 2th International Conference IT Convergence and Security 2012, LNEE 215*, pp. 711–718

[15] Lin IL, Chao HC, & Peng SH (2011) Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone. *Proc. of the International Conference on Broadband and Wireless Computing, Communication and Applications*, pp. 386–391

[16] Lopez P, Orfila A, Palomar E, & Castro H (2012) A secure distance-based RFID identification protocol with an off-line back-end database. *Pers Ubiquit Comput 16*(3):351–365

[18] Kubi AK, Saleem S, & Popov O (2011) Evaluation of some tools for extracting e-evidence from mobile devices. *Proc. of the International Conference on Application of Information and Communication Technologies*, pp. 1–6

[19] Kuntze N, & Rudolph C (2011) Secure digital chains of evidence. *Proc. of the IEEE Inter-national Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 1–8

[22] Moreland D, Nepal S, & Hwang H, Zic J (2010) A snapshot of trusted personal devices applicable to transaction processing. *Pers Ubiquit Comput 14*(4):347–361

[23] Song CW, Lim JH, Chung KY, Rim KW, & Lee JH (2012) Fast data acquisition with mobile device in digital crime. *Proc. of the 2th International Conference IT Convergence and Security 2012, LNEE 215*, pp. 711–718

[28] Cahyani NDW, Martini B, Choo KKR, & Muhammad Nuh Al-Azhar AKBP (2016) Forensic data acquisition from cloud-of-things devices: Windows smartphones as a case study. *Concurrency and Computation: Practice and Experience 29*(14): e3855

[29] Lee KD, Nam MY, Chung KY, Lee YH, & Kang UG (2013) Context and profile based cascade classifier for efficient people detection and safety care system. *Multimed Tools Appl 63*(1):27–44

[30] Said H, Yousif A, & Humaid H (2011) IPhone forensics techniques and crime investigation. *Proc. of the International Conference and Workshop on Current Trends in Information Technology*, pp. 120–125

[31] Song CW, Lim JH, Chung KY, Rim KW, & Lee JH (2012) Fast data acquisition with mobile device in digital crime. *Proc. of the 2th International Conference IT Convergence and Security 2012, LNEE 215*, pp. 711–718

[32] Casey E, Back G, & Barnum S (2014) Leveraging CybOX to standardize representation and exchange of digital information. *Digital Investig. 12*: S102–S110

[36] Moreland D, Nepal S, & Hwang H, Zic J (2010) A snapshot of trusted personal devices applicable to transaction processing. *Pers Ubiquit Comput 14*(4):347–361

[37] Akkaladevi S, Keesara H & Luo X (2011) Efficient forensic tools for handheld device: a comprehensive perspective. *Softw Eng Res Manag Appl Stud Comput Intell 377*:349–359

[38] Lim JH, Song CW, Chung KY, Rim KW, & Lee JH (2012) Forensic evidence collection procedures of smartphone in crime scene. *Proc. of the 2th International Conference IT Convergence and Security 2012, LNEE 215*, pp. 711–718

[40] Cheng Y (2011) Cybercrime forensic system in cloud computing. *Proceedings of the 2011 International Conference on Image Analysis and Signal Processing (IASP'11)*, pp. 612–615

[41] Song CW, Lim JH, Chung KY, Rim KW, & Lee JH (2012) Fast data acquisition with mobile device in digital crime. *Proc. of the 2th International Conference IT Convergence and Security 2012, LNEE 215*, pp. 711–718

[44] Kuntze N, & Rudolph C (2011) Secure digital chains of evidence. *Proc. of the IEEE Inter-national Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 1–8

[45] Barmpatsalou K, Sousa B, Monteiro E, & Simoes P (2015) Mobile forensics for PPDR communications: How and why. *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS'15)*, pp. 30-32

[46] Casey E, Back G, & Barnum S (2014) Leveraging CybOX to standardize representation and exchange of digital information. *Digital Investig. 12*: S102–S110

[47] Lin IL, Chao HC, & Peng SH (2011) Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone. *Proc. of the International Conference on Broadband and Wireless Computing, Communication and Applications*, pp. 386–391

[48] Cahyani NDW, Martini B, Choo KKR, & Muhammad Nuh Al-Azhar AKBP (2016) Forensic data acquisition from cloud-of-things devices: Windows smartphones as a case study. *Concurrency and Computation: Practice and Experience 29*(14): e3855

[49] Song CW, Lim JH, Chung KY, Rim KW, & Lee JH (2012) Fast data acquisition with mobile device in digital crime. *Proc. of the 2th International Conference IT Convergence and Security 2012, LNEE 215*, pp. 711–718

[50] Said H, Yousif A, & Humaid H (2011) IPhone forensics techniques and crime investigation. *Proc. of the International Conference and Workshop on Current Trends in Information Technology*, pp. 120–125

[51] Zareen A, & Baig S (2010) Mobile phone forensics: challenges, analysis and tools classification. *Proc. of the IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 47–55

[52] Kubi AK, Saleem S, & Popov O (2011) Evaluation of some tools for extracting e-evidence from mobile devices. *Proc. of the International Conference on Application of Information and Communication Technologie*s, pp. 1–6

[53] Cahyani NDW, Martini B, Choo KKR, & Muhammad Nuh Al-Azhar AKBP (2016) Forensic data acquisition from cloud-of-things devices: Windows smartphones as a case study. *Concurrency and Computation: Practice and Experience 29*(14): e3855

[54] Moreland D, Nepal S, & Hwang H, Zic J (2010) A snapshot of trusted personal devices applicable to transaction processing. *Pers Ubiquit Comput 14*(4):347–361

[55] Lee KD, Nam MY, Chung KY, Lee YH, & Kang UG (2013) Context and profile based cascade classifier for efficient people detection and safety care system. *Multimed Tools Appl 63*(1):27–44

[56] Lin IL, Chao HC, & Peng SH (2011) Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone. *Proc. of the International Conference on Broadband and Wireless Computing, Communication and Applications*, pp. 386–391

[57] Song CW, Lim JH, Chung KY, Rim KW, & Lee JH (2012) Fast data acquisition with mobile device in digital crime. *Proc. of the 2th International Conference IT Convergence and Security 2012, LNEE 215*, pp. 711–718

[59] Lim JH, Song CW, Chung KY, Rim KW, & Lee JH (2012) Forensic evidence collection procedures of smartphone in crime scene. *Proc. of the 2th International Conference IT Convergence and Security 2012, LNEE 215*, pp. 711–718

[60] Said H, Yousif A, & Humaid H (2011) IPhone forensics techniques and crime investigation. *Proc. of the International Conference and Workshop on Current Trends in Information Technology*, pp. 120–125

[61] Raghav S, & Saxena AK (2009) Mobile forensics: guidelines and challenges in data preservation and acquisition. *2009 I.E. Student Conference on Research and Development*, pp. 5–8

[65] Lee KD, Nam MY, Chung KY, Lee YH, & Kang UG (2013) Context and profile based cascade classifier for efficient people detection and safety care system. *Multimed Tools Appl 63*(1):27–44

[66] Kubi AK, Saleem S, & Popov O (2011) Evaluation of some tools for extracting e-evidence from mobile devices. *Proc. of the International Conference on Application of Information and Communication Technologies*, pp. 1–6

[67] Barmpatsalou K, Sousa B, Monteiro E, & Simoes P (2015) Mobile forensics for PPDR communications: How and why. *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS'15)*, pp. 30-32

[68] Zareen A, & Baig S (2010) Mobile phone forensics: challenges, analysis and tools classification. *Proc. of the IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 47–55

[69] Cheng Y (2011) Cybercrime forensic system in cloud computing. *Proceedings of the 2011 International Conference on Image Analysis and Signal Processing (IASP'11)*, pp. 612–615