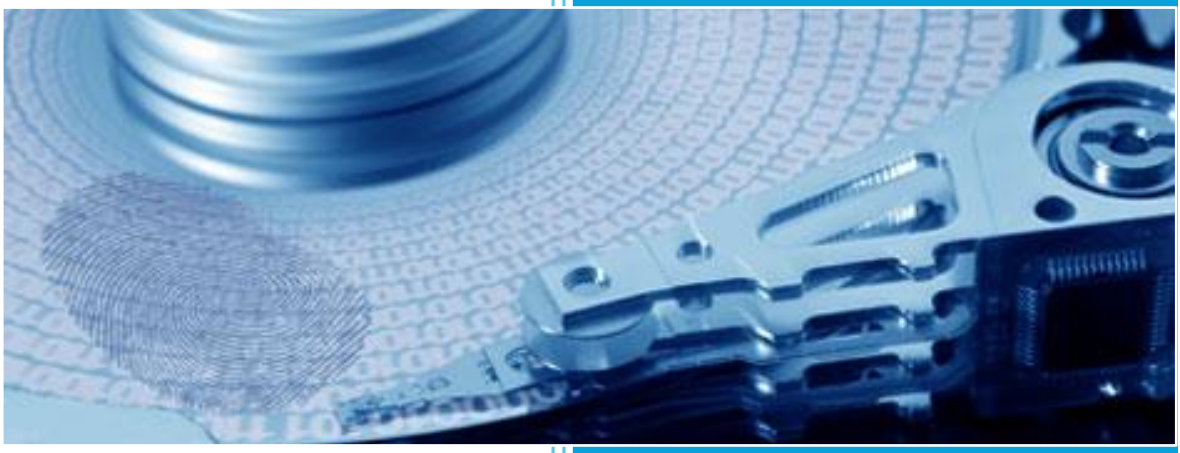
2015

Εγχειρίδιο Digital Forensics



Ψευτέλης Αθανάσιος Δημήτριος

Διπλωματική εργασία

6/7/2015

Πίνακας περιεχομένων

1. Εισαγωγή

Το παρόν κεφάλαιο θα μας εισάγει στις απαραίτητες εντολές Linux . Γίνεται μια αναφορά σε εκείνες που θα χρειαστούμε για την ψηφιακή εγκληματολογία.

1.1 Βασικές Εντολές Τερματικού

1.1.1 Παράθεση αρχείων και καταλόγων

- ls

Η εντολή ls είναι η πιο πολυχρησιμοποιούμενη εντολή . Παραθέτει τα αρχεία και τους καταλόγους που υπάγονται στον κατάλογο .Θα παρουσιάσουμε βασικές επιλογές της.

- ls –F

Η εντολή ls δεν μας αποκαλύπτει και πολλά για ένα αντικείμενο μέσα σε έναν κατάλογο, πέραν του ονόματος του .Από μόνη της δεν μας πληροφορεί αν ένα αντικείμενο είναι αρχείο , κατάλογος ή κάτι άλλο . Ένας απλός τρόπος για να λύσουμε αυτό το πρόβλημα είναι να χρησιμοποιήσουμε την παράμετρο -F .Στον ακόλουθο πίνακα παρουσιάζονται όλες οι πιθανές καταλήξεις.

Πίνακας 1

Σύμβολα και τύποι αρχείων	
*	Εκτελέσιμο
/	Κατάλογος
@	Συμβολικός σύνδεσμος
|	FIFO
=	Υποδοχή

- ls –a

Κάθε κατάλογος περιέχει κρυφά αρχεία και φακέλους που έχουν γίνει αόρατα με την χρήση της . στην αρχή του ονόματός τους . Ένα θέλουμε να δούμε αυτά τα κρυφά αρχεία χρησιμοποιούμε την παράμετρο –a .

- ls -l

Η παράμετρος –l μας παρέχει περισσότερες πληροφορίες για τα περιεχόμενα των καταλόγων.

1.1.2 Μεταφορά σε διαφορετικό κατάλογο

Η εντολή cd μας μεταφέρει σε άλλο κατάλογο . Είναι εύκολη στην χρήση της. Απλά γράφουμε cd και συμπληρώνουμε με τον κατάλογο που θέλουμε να μετακινηθούμε .Μπορούμε να χρησιμοποιήσουμε μια σχετική διαδρομή βασισμένη στο που βρισκόμαστε (π.χ. cd src) ή μια ακριβή διαδρομή αρχείου (π.χ. cd /home/Desktop).

1.1.3 Αντιγραφή αρχείων

Η δημιουργία αντίγραφων αρχείων γίνεται με την εντολή cp . Πληκτρολογούμε την εντολή , ακολούθως το αρχείο που θέλουμε να αντιγράψουμε και μετά το όνομα του νέου αντίγραφου.

- cp sourceFile destinationFile

1.1.4 Καθαρισμός τερματικού

- clear

Το τερματικό με την συγκεκριμένη εντολή μας παρέχει μια οθόνη καθαρή.

1.1.5 Μετακίνηση και μετονομασία αρχείων

- mv sourceFile destinationFile

Η μετακίνηση και μετονομασία αρχείων γίνεται με την εντολή mv .

1.1.6 Διαγραφή αρχείων

- rm fileName

Η εντολή rm διαγράφει αρχεία . Η γραμμή εντολών του Linux δεν έχει κάδο ανακύκλωσης .

1.1.7 Δημιουργία ενός νέου καταλόγου

- mkdir filename

Με την εντολή mkdir δημιουργούμε ένα νέο κατάλογο.

1.1.8 Προβολή αρχείων κειμένου

- less filename

Παρουσιάζουμε την less έναντι των cat και more λόγω του ότι επιτρέπει την ευκολότερη ανάγνωση κειμένων . Είναι ένα πρόγραμμα επισκόπησης αρχείων κειμένου σελίδα προς σελίδα . Με τα βελάκια μπορούμε να ανατρέξουμε τις σελίδες και με q να εξέλθουμε από αυτήν.

1.2 Προχωρημένες Εντολές Τερματικού

1.2.1 Αναζήτηση μοτίβων μέσα σε αρχεία κειμένου

- grep pattern filename

Με την εντολή grep μπορούμε να ψάξουμε αρχεία . Ουσιαστικά της δίνουμε ένα μοτίβο για το οποίο θέλουμε να ψάξει , την καθοδηγούμε προς ένα αρχείο ή μια ομάδα αρχείων ή ακόμα και σε ένα ολόκληρο σκληρό δίσκο , και μετά μας επιστρέφει μια λίστα με γραμμές που ταιριάζουν στο μοτίβο μας .

1.2.2 Εύρεση αρχείων με βάση το όνομα

- find / -name “*pattern*”

Η εντολή find χρησιμοποιείται κυρίως για την αναζήτηση αρχείων με βάση το όνομα η μέρος αυτού (εξού και η παράμετρος –name) . Η / που ακολουθεί μετά την εντολή καθορίζει εάν θα μας επιστρέψει την απόλυτη ή σχετική διαδρομή .

1.2.3 Παρουσίαση της διαδρομής του τρέχοντος καταλόγου

- pwd

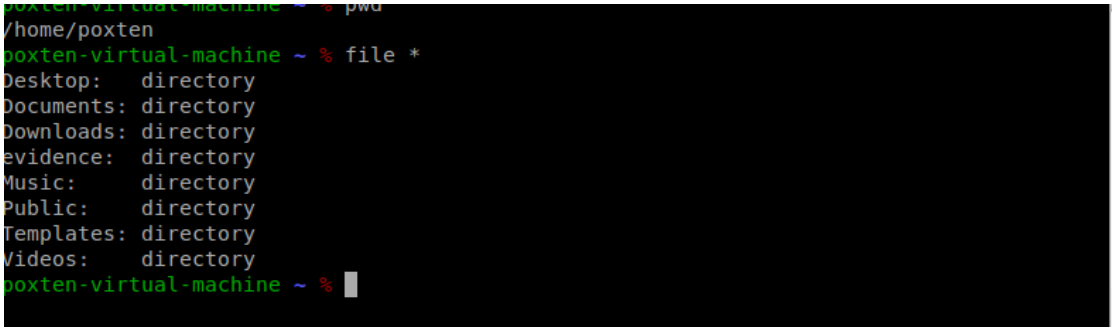
Μας εμφανίζει τον κατάλογο που εργαζόμαστε .

1.2.4 Εύρεση τύπου αρχείων

- file filename

Με την εντολή file μπορούμε να βρούμε τον τύπο του κάθε αρχείου έστω και εάν δεν έχει προέκταση. Συγκεκριμένα αρχεία προγραμμάτων έχουν μαγικούς αριθμούς (magic numbers) που δείχνουν τον τύπο τους.

Εικόνα 1 file



1.2.5 Εμφάνιση όλων των διεργασιών

- ps -aux

Για να δούμε όλες τις διεργασίες που τρέχουν στο σύστημα μας , ακολουθούμε την ps με τις παραμέτρους : a (που σημαίνει όλοι οι χρήστες) , u (για να εμφανίζεται ο χρήστης στον οποίο ανήκει κάθε διεργασία) και x (για να δούμε όλες τις διεργασίες) .

1.2.6 Εκτύπωση αναγνώσιμων χαρακτήρων

- strings filename

Κάποια αρχεία δεν μπορούμε να τα διαβάσουμε όταν δεν τα «ανοίγουμε» με το κατάλληλο πρόγραμμα . Τέτοια είναι τα εκτελέσιμα. Με την εντολή strings μπορούμε να εξάγουμε όλες τις συμβολοσειρές με μήκος 4 και παραπάνω χαρακτήρων .Είναι μια εντολή απαραίτητη για την εξεύρεση ψηφιακών ιχνών .

1.2.7 Αλλαγή δικαιωμάτων σε αρχεία και καταλόγους , με την χρήση αριθμητικών δικαιωμάτων

- chmod [0-7][0-7][0-7]

Το Linux καταλαβαίνει ότι με ένα αρχείο ή κατάλογο μπορούν να εργασθούν τρία σύνολα χρηστών :

- ο πραγματικός χρήστης (u-user)
- μια ομάδα (g-group)
- όλοι οι υπόλοιποι (o-others)

Τα δικαιώματα ορίζουν τι μπορούν να κάνουν οι χρήστες με τα αρχεία και του καταλόγους. Τα δικαιώματα έχουν τα ακόλουθα στοιχεία :

- ανάγνωση (r-read)
- εγγραφή (w-write)
- εκτέλεση (x-execute)

Τα αριθμητικά δικαιώματα (γνωστά και ως οκταδικά δικαιώματα) έχουν φτιαχτεί με βάση το δυαδικό σύστημα. Οι τιμές των δικαιωμάτων είναι ακόλουθες:

- ανάγνωση (r) = 4
- εγγραφή (w) = 2
- εκτέλεση (x) = 1

Πίνακας 2 Δικαιώματα και αριθμητικές αναπαραστάσεις

	Κάτοχος	Ομάδα	Υπόλοιποι
Δικαιώματα	r;w;x	r;w;x	r;w;x
Αριθμητική αναπαράσταση	4;2;1	4;2;1	4;2;1

Έστω ότι το αρχείο filename έχει τιμή 755 ,δηλαδή

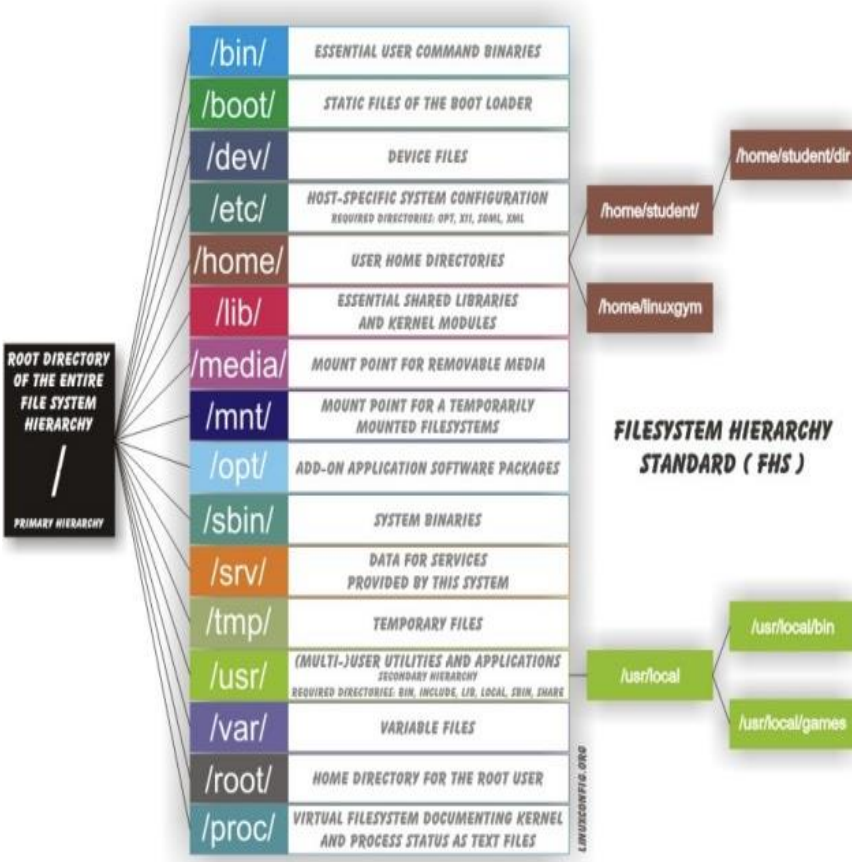
- user rwx =7
- group r-x = 5
- others r-x = 5

Εάν θέλουμε να αλλάξουμε τα δικαιώματα έτσι ώστε οι user & group να έχουν δικαιώματα read,write,execute αλλά οι others να έχουν δικαίωμα μόνο read τότε θα εκτελέσουμε την εντολή chmod 774 filename.

1.3 Οι Χαρακτήρες Μπαλαντέρ

Υπάρχουν τρεις χαρακτήρες μπαλαντέρ:

- * (αστερίσκος) : αντιστοιχεί σε οποιοδήποτε χαρακτήρα, οσεσδήποτε φορές
- ? (αγγλικό ερωτηματικό) : αντιστοιχεί σε οποιοδήποτε χαρακτήρα ,μια φορά
- [] (αγκύλες) : αντιστοιχούν σε ένα στοιχείο από ένα σετ χαρακτήρων (π.χ. [12]) ή σε ένα στοιχείο από μια σειρά χαρακτήρων (π.χ. [1-3])



2. Το Σύστημα Αρχείων

Μια από τις ευθύνες του Λειτουργικού Συστήματος είναι η διαχείριση των αρχείων . Στο παρών κεφάλαιο θα δούμε τις ευκολίες που παρέχει το Linux στον χρήστη για τον χειρισμό τους .

2.1 Γενικά

Το σύστημα αρχείων (file system) του Linux είναι αρκετά αποτελεσματικό και απλό αφού χαρακτηρίζεται από :

- Την ιεραρχική δομή του
- Την δυνατότητα δημιουργίας και διαγραφής αρχείων
- Την δυναμική ανάπτυξη των αρχείων
- Την προστασία των αρχείων
- Την διαχείριση των περιφερειακών συσκευών (δίσκοι , usb stick κ.λπ.) σαν αρχεία

Η οργάνωση του συστήματος αρχείων είναι συνδυασμός των ακολούθων :

- Λογικό σύστημα αρχείων : εικόνα που έχει ο χρήστης για την οργάνωση των αρχείων
- Φυσικό σύστημα αρχείων : πραγματική εικόνα , ο τρόπος που ο πυρήνας βλέπει τα αρχεία

Το Linux διακρίνει μόνο τρία είδη αρχείων :

- Τα κανονικά αρχεία (regular files)
- Τους καταλόγους (directories)
- Τα ειδικά αρχεία (special files)

Κανονικά αρχεία : είναι τα αρχεία που περιέχουν δεδομένα (data) ,κείμενο (text) , κώδικα (code). Ο χρήστης έχει κάθε δυνατότητα χειρισμού , ανάλογα βέβαια με τα δικαιώματα πρόσβασης , σε αυτά τα αρχεία .

Κατάλογοι : είναι εκείνα τα αρχεία που δίνουν πληροφορίες για την θέση όλων των αρχείων στο μέσο αποθήκευσης . Η ενημέρωση αυτών των αρχείων γίνεται από τον ίδιο τον πυρήνα (kernel).

Ειδικά αρχεία : είναι εκείνα τα αρχεία που αντιπροσωπεύουν περιφερειακές συσκευές (δίσκοι , εκτυπωτές κλπ). Για τα Linux όλες οι περιφερειακές συσκευές είναι αρχεία.

- Για να εμφανιστεί το περιεχόμενο ενός κανονικού αρχείου στην οθόνη του τερματικού αρκεί να αντιγραφεί (copy) το κανονικό αρχείο στο ειδικό αρχείο

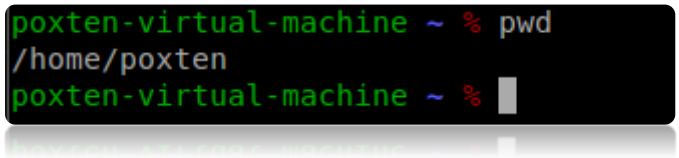
που αντιπροσωπεύει το τερματικό με τον ίδιο τρόπο που θα αντιγραφόταν σε ένα άλλο κανονικό αρχείο .

2.2 Πραγματική Μορφή ενός Καταλόγου

Ένας κατάλογος (directory) είναι ένα αρχείο που περιέχει την λίστα των αρχείων και καταλόγων που ανήκουν σε αυτό τον κατάλογο . Ο χρήστης έχει τη δυνατότητα δημιουργίας ή διαγραφής ενός καταλόγου ,δεν έχει την δυνατότητα ενημέρωσης. Όταν δημιουργείται ή διαγράφεται ένα αρχείο από τον χρήστη , την ενημέρωση της λίστας του καταλόγου αναλαμβάνει ο ίδιος ο πυρήνας(kernel).

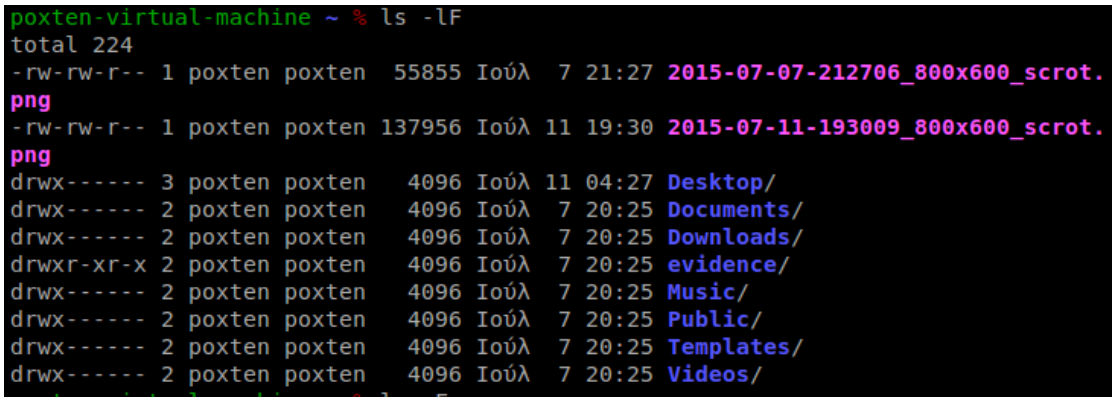
- pwd

Εικόνα 2 pwd



- ls -lF

Εικόνα 3 ls -lF



Ο χρήστης αναγνωρίζει τα αρχεία και τους καταλόγους μέσω των ονομάτων τους.

Το Linux αναγνωρίζει μέσω μοναδικών αριθμών που ονομάζονται αριθμοί κόμβων πληροφοριών **(i –node numbers**).

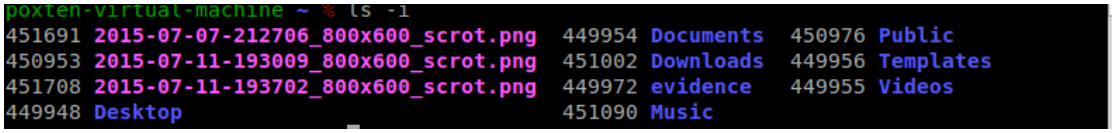
Για κάθε αρχείο υπάρχει ένας μοναδικός **i-node number .** Μέσω αυτού του αριθμού το Linux έχει πρόσβαση στις άλλες πληροφορίες του αρχείου (ιδιοκτήτης ,

δικαιώματα προσπέλασης , ημερομηνίες δημιουργίας-ενημέρωσης-προσπέλασης , είδος αρχείου κλπ).

Ο χρήστης μπορεί να δει το **i-node number** κάθε αρχείου ή καταλόγου εκτελώντας την εντολή ls με την επιλογή -i :

- ls –i

Εικόνα 4 ls -i



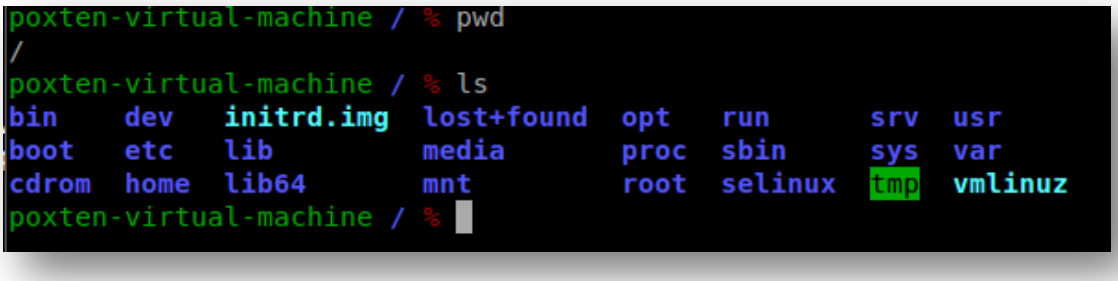
2.3 Φυσικό Σύστημα Αρχείων

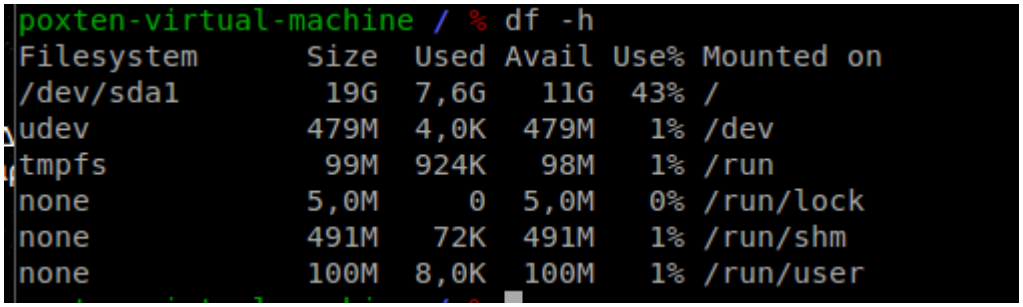
Το λογικό σύστημα αρχείων αποτελείται (συνήθως) από πολλά φυσικά συστήματα αρχείων τα οποία αποθηκεύονται σε διαφορετικές φυσικές συσκευές ή σε διαφορετικές περιοχές του δίσκου (partitions).

Ο κάθε χρήστης βλέπει πάντα ένα σύστημα αρχείων (το λογικό σύστημα αρχείων). Μόνο μέσω της εντολής df μπορεί να διαπιστώσει τα φυσικά συστήματα αρχείων από τα οποία αποτελείται το σύστημα αρχείων .

- df –h

Εικόνα 5 Λογικό Σύστημα Αρχείων





Εικόνα 6 Φυσικό σύστημα αρχείων

2.3.1 Οργάνωση φυσικού συστήματος

Ένα φυσικό σύστημα αρχείων αποτελείται από ένα σύνολο blocks (512 or 1024 bytes) με αριθμημένες διευθύνσεις . Ομάδες αυτών των blocks σχηματίζουν τα τέσσερα εξής τμήματα :

- block φόρτωσης (boot block or block-0)
- Υπέρ-block (super block or block-1)
- Λίστα κόμβων πληροφοριών (i-node list)
- Blocks δεδομένων (data blocks)

2.3.2 Block Φόρτωσης (boot block)

Είναι αποθηκευμένο στο block 0 . Δεν χρησιμοποιείται από το σύστημα των αρχείων ,αλλά μόνο κατά την διάρκεια εκκίνησης του υπολογιστή. Όταν ανοίγουμε τον υπολογιστή , το block φόρτωσης ενεργοποιείται και αναλαμβάνει να φορτώσει στην μνήμη τον πυρήνα (kernel) . Όταν ο πυρήνας φορτωθεί στην μνήμη η διεργασία boot μεταφέρει τον έλεγχο στην αρχική διεύθυνση του πυρήνα , που παραμένει έτσι ενεργοποιημένος στην μνήμη .

2.3.3 Υπέρ-block (super block)

Βρίσκεται στο block 1 και περιγράφει όλες τις παραμέτρους του φυσικού συστήματος αρχείων , όπως :

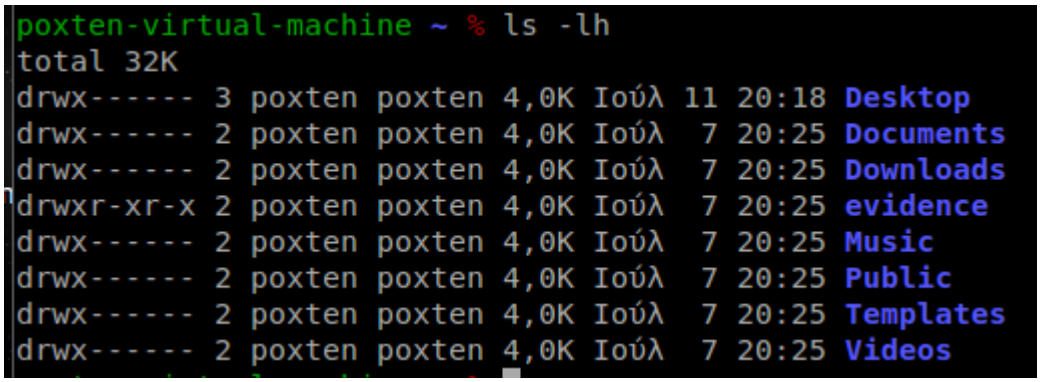
- Όνομα του συστήματος αρχείων
- Μέγεθος του συστήματος αρχείων
- Ημερομηνία και ώρα τελευταίας τροποποίησης
- Αριθμός των ελεύθερων i-nodes
- Συνολικός αριθμός των ελεύθερων blocks
- Πίνακας των 50 ελεύθερων blocks
- Πίνακας των 100 ελεύθερων i-nodes
- Δείκτης στην i-node list

2.3.4 Λίστα κόμβων πληροφοριών (i-node list)

Η λίστα των κόμβων πληροφοριών αποτελείται από όλους τους i-nodes . Για κάθε αρχείο υπάρχει ένας μοναδικός i-node.

Ο i-node ενός αρχείου είναι μια εγγραφή που περιέχει όλες τις πληροφορίες του αρχείου, εκτός από το όνομα του, το οποίο ως γνωστόν διατηρείται στον κατάλογο (directory). Έτσι ενώ ο χρήστης αναφέρεται σε ένα αρχείο με το όνομα του , ο πυρήνας αναφέρεται σε αυτό μέσω του i-node .

Ο i-node περιέχει ουσιαστικά εκείνες τις πληροφορίες για κάθε αρχείο , που εμφανίζονται με την εκτέλεση της εντολής ls –l



Εικόνα 7 ls -lh

Ο i-node περιέχει :

- Τον τύπο του αρχείου
  - – κανονικό αρχείο

  - d κατάλογο
  - b για ειδικό αρχείο blocks (block special file)
  - c για ειδικό αρχείο χαρακτήρων (character special file)
- τα δικαιώματα προσπέλασης
- τον αριθμό συνδέσμων
- ταυτότητα του ιδιοκτήτη του αρχείου(uid)
- ταυτότητα της ομάδας του αρχείου (gid)
- το μέγεθος του αρχείου σε bytes(ls-lh:μας δίνει το μέγεθος του αρχείου σε K,M,G)
- ημερομηνία και ώρα δημιουργίας , τροποποίησης ,προσπέλασης

2.3.4 Blocks δεδομένων (Data blocks)

Τα Blocks δεδομένων περιέχουν όλα τα περιεχόμενα των κανονικών αρχείων (regular files).

2.4 Ειδικά Αρχεία (special files)

Ένα από τα χαρακτηριστικά του Linux είναι ο χειρισμός των περιφερειακών συσκευών (devices) σαν αρχεία που ονομάζονται ειδικά αρχεία (special files)

Σε κάθε περιφερειακή συσκευή αντιστοιχεί ένα ειδικό αρχείο που βρίσκεται στον **κατάλογο /dev** . Κάθε αναφορά σε ειδικό αρχείο μετατρέπεται από τον πυρήνα (kernel) σε διαταγές hardware για την προσπέλαση της αντίστοιχης συσκευής .

Διακρίνουμε δυο είδη ειδικών αρχείων :

- ειδικά αρχεία με δομή block (block special files)
- ειδικά αρχεία με δομή χαρακτήρων (character special files)

Τα ειδικά αρχεία με δομή block (block special files) αντιστοιχούν σε εκείνες τις συσκευές (δίσκους) που μεταφέρουν τα δεδομένα σε blocks (512 or 1024 bytes).

Τα ειδικά αρχεία με δομή χαρακτήρων (character special files) αντιστοιχούν σε εκείνες τις συσκευές (τερματικά ,εκτυπωτές ,δίσκοι) που η μεταφορά δεδομένων γίνεται χαρακτήρα – χαρακτήρα .

Εκτελώντας την ακόλουθη εντολή

```
poxten-virtual-machine ~ % ls -li /dev
```

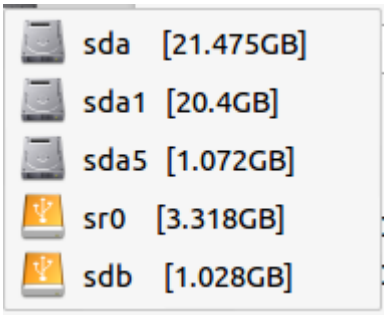
Εικόνα 8 ls –li

Παίρνουμε σαν έξοδο τα ακόλουθα :

```
 7939 brw-rw----  1 root disk      8,   0 Ιούλ 12 16:19 sda
 7944 brw-rw----  1 root disk      8,   1 Ιούλ 12 16:19 sda1
 7945 brw-rw----  1 root disk      8,   2 Ιούλ 12 16:19 sda2
 7946 brw-rw----  1 root disk      8,   5 Ιούλ 12 16:19 sda5
13588 brw-rw----  1 root disk      8,  16 Ιούλ 12 16:27 sdb
 7940 crw-rw----  1 root disk     21,   0 Ιούλ 12 16:19 sg0
 7950 crw-rw----+ 1 root cdrom    21,   1 Ιούλ 12 16:19 sg1
13572 crw-rw----  1 root disk     21,   2 Ιούλ 12 16:27 sg2
 8461 lrwxrwxrwx  1 root root          8 Ιούλ 12 16:19 shm -> /run/shm
 5954 crw-------  1 root root     10, 231 Ιούλ 12 16:19 snapshot
 8552 drwxr-xr-x  3 root root         200 Ιούλ 12 16:19 snd
 7949 brw-rw----+ 1 root cdrom    11,   0 Ιούλ 12 16:19 sr0
```

Εικόνα 9 /dev δίσκοι

Στην εικόνα 9 βλέπουμε τους δίσκους του συστήματος μας σαν ειδικά αρχεία . Στην εικόνα 10 βλέπουμε τους δίσκους μας σε γραφικό περιβάλλον



Εικόνα 10 δίσκοι VM

- sda : Τα ειδικά αρχεία που αρχίζουν από sda* αντιπροσωπεύουν σκληρούς δίσκους
- sdb : Τα ειδικά αρχεία που αρχίζουν από sdb αντιπροσωπεύουν usb sticks

Στην ακόλουθη εικόνα βλέπουμε τα τερματικά του υπολογιστή μας ως ειδικά αρχεία

```
5753 crw-rw-rw-  1 root tty       5,   0 Ιούλ 12 16:19 tty
5755 crw--w----  1 root tty       4,   0 Ιούλ 12 16:19 tty0
5760 crw-rw----  1 root tty       4,   1 Ιούλ 12 16:19 tty1
5769 crw--w----  1 root tty       4,  10 Ιούλ 12 16:19 tty10
5770 crw--w----  1 root tty       4,  11 Ιούλ 12 16:19 tty11
5771 crw--w----  1 root tty       4,  12 Ιούλ 12 16:19 tty12
5772 crw--w----  1 root tty       4,  13 Ιούλ 12 16:19 tty13
5773 crw--w----  1 root tty       4,  14 Ιούλ 12 16:19 tty14
5774 crw--w----  1 root tty       4,  15 Ιούλ 12 16:19 tty15
5775 crw--w----  1 root tty       4,  16 Ιούλ 12 16:19 tty16
5776 crw--w----  1 root tty       4,  17 Ιούλ 12 16:19 tty17
5777 crw--w----  1 root tty       4,  18 Ιούλ 12 16:19 tty18
5778 crw--w----  1 root tty       4,  19 Ιούλ 12 16:19 tty19
5761 crw-rw----  1 root tty       4,   2 Ιούλ 12 16:19 tty2
```

Εικόνα 11 /dev τερματικά

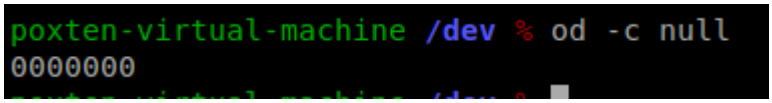
- tty: Τα ειδικά αρχεία που αρχίζουν από tty* αντιπροσωπεύουν τα τερματικά.

Εικόνα 12 ειδικό αρχείο floppy disk

- fd :Τα ειδικά αρχεία που αρχίζουν από fd* αντιπροσωπεύουν δισκέτες(floppy disks)

Εικόνα 13 ειδικό αρχείο null

- null : το ειδικό αρχείο /dev/null αντιπροσωπεύει το κενό αρχείο το οποίο επιβεβαιώνουμε και από την ακόλουθη εικόνα



Εικόνα 14 od -c null

Ανάλυση πεδίων:

- 1 πεδίο : i-node number
- 2 πεδίο : Το πρώτο γράμμα :
  - b :το ειδικό αρχείο είναι με δομή block
  - c :το ειδικό αρχείο είναι δομής χαρακτήρων
- 6 πεδίο : Μείζων αριθμός συσκευής (major device number) καθορίζει τον οδηγό συσκευής (device driver) που θα χρησιμοποιηθεί για τη συσκευή
- 7 πεδίο : Ελάσσων αριθμός συσκευής (minor device number) χρησιμοποιείται για προσδιορίσει τη συγκεκριμένη συσκευή , μεταξύ εκείνων των συσκευών που χρησιμοποιούν τον ίδιο οδηγό συσκευής (δηλαδή έχουν τον ίδιο Μείζονα αριθμό)
- πχ :

βλέπουμε ότι τα τερματικά έχουν τον ίδιο οδηγό συσκευής (χρησιμοποιούν τον ίδιο οδηγό συσκευής) που η τιμή που τον συμβολίζει είναι το 4 , αλλά ξεχωρίζουν μεταξύ τους μέσω του ελάσσων αριθμού , οπού στο μεν πρώτο είναι 0 και στο δεύτερο είναι 1

2.5 Φόρτωση Συστήματος Αρχείων

Ένας υπερχρήστης (root) μπορεί να επεκτείνει το σύστημα αρχείων χρησιμοποιώντας την εντολή mount .Η mount επιτρέπει να ενώσουμε το σύστημα αρχείων μιας συσκευής μέσα στην ιεραρχία του πατρικού καταλόγου root .

- mount -t FileSystemType -o ro deviceName directory

Το πρώτο όρισμα -t στο πεδίο FileSystemType μπορεί να λάβει τις ακόλουθες τιμές :

- auto : αυτόματη επιλογή τύπου συστήματος αρχείων
- ext4 : το πιο πρόσφατο σύστημα αρχείων για Linux
- ext3 : το προηγούμενο ,από το ext4 ,σύστημα αρχείων Linux
- ntfs : σύστημα αρχείων των windows ή μεγάλων σκληρών δίσκων
- vfat : σύστημα αρχείων για μικρότερους σκληρούς δίσκους

Με το όρισμα -o ro διασφαλίζουμε ότι το σύστημα αρχείων που φορτώνουμε θα είναι μόνο για ανάγνωση . Εάν επιθυμούμε να είναι και για εγγραφή θα πρέπει να αντικαταστήσουμε το όρισμα με το –o rw .

Η φόρτωση του συστήματος αρχείων γίνεται σε συγκεκριμένους καταλόγους για λόγους τάξης . Οι κατάλογοι είναι οι ακόλουθοι :

- /mnt : για προσωρινό mount
- /media : στον κατάλογο αυτό γίνονται mount οι αφαιρούμενες συσκευές

Πρέπει να δημιουργούμε για κάθε συσκευή που θέλουμε να φορτώσουμε στον υπολογιστή μας ένα υποκατάλογο , σε ένα εκ των δυο καταλόγων(/mnt or /media) , με όνομα που να μας παραπέμπει στην συσκευή .

Όταν θέλουμε να εκφορτώσουμε ένα σύστημα αρχείων που έχουμε φορτώσει χρησιμοποιούμε την εντολή umount .

- umount deviceName

Θα παρουσιάσουμε ένα παράδειγμα με ένα usb stick προκειμένου να συγκεντρώσουμε τα βήματα που είναι απαραίτητα για την ορθή εφαρμογή της όλης διαδικασίας :

1. Στο πρώτο βήμα μας αλλάζουμε σε χρήστη root :

```
poxten-virtual-machine ~ % whoami
poxten
poxten-virtual-machine ~ % sudo su -
[sudo] password for poxten:
poxten-virtual-machine ~ % whoami
root
```

Εικόνα 15 sudo su –

2. Συνδέουμε το usb stick , ελέγχουμε ότι έχει αναγνωριστεί από τον υπολογιστή μας και τι όνομα έχει λάβει :

```
poxten-virtual-machine ~ % dmesg
```

Η εντολή dmesg μας δίνει την ακόλουθη έξοδο :

```
[ 7643.477318] usb 1-1: new high-speed USB device number 6 using ehci_hcd
[ 7643.994718] usb 1-1: New USB device found, idVendor=8564, idProduct=1000
[ 7643.994730] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[ 7643.994736] usb 1-1: Product: Mass Storage Device
[ 7643.994740] usb 1-1: Manufacturer: JetFlash
[ 7643.994745] usb 1-1: SerialNumber: 157WV9RVIVUFJ0US
[ 7644.013812] scsi37 : usb-storage 1-1:1.0
[ 7645.723757] scsi 37:0:0:0: Direct-Access     JetFlash Transcend 16GB   1100 PQ: 0 AN
SI: 4
[ 7645.732209] sd 37:0:0:0: Attached scsi generic sg2 type 0
[ 7645.786205] sd 37:0:0:0: [sdb] 31703040 512-byte logical blocks: (16.2 GB/15.1 GiB)
[ 7645.833134] sd 37:0:0:0: [sdb] Write Protect is off
[ 7645.833147] sd 37:0:0:0: [sdb] Mode Sense: 43 00 00 00
[ 7645.879879] sd 37:0:0:0: [sdb] No Caching mode page present
[ 7645.879893] sd 37:0:0:0: [sdb] Assuming drive cache: write through
[ 7646.082215] sd 37:0:0:0: [sdb] No Caching mode page present
[ 7646.082228] sd 37:0:0:0: [sdb] Assuming drive cache: write through
[ 7646.128989]  sdb: sdb1
[ 7646.393677] sd 37:0:0:0: [sdb] No Caching mode page present
[ 7646.393691] sd 37:0:0:0: [sdb] Assuming drive cache: write through
[ 7646.393698] sd 37:0:0:0: [sdb] Attached SCSI removable disk
poxten-virtual-machine ~ %
```

Εικόνα 16 dmesg for usb stick

Βλέπουμε ότι το usb stick έχει αναγνωριστεί από τον υπολογιστή και είναι το ειδικό αρχείο /dev/sdb1

```
poxten-virtual-machine ~ % ls -li /dev/sdb1
29906 brw-rw---- 1 root disk 8, 17 Ιούλ 14 20:54 /dev/sdb1
```

3. Δημιουργία του υποκαταλόγου /mnt/usb :

```
poxten-virtual-machine ~ % mkdir /mnt/usb
poxten-virtual-machine ~ % ls /mnt
c  d  e  hgfs  raw1  raw2  raw3  smb  usb
```

Εικόνα 17 /mnt/usb

Ελέγχουμε τα περιεχόμενα του:

```
poxten-virtual-machine ~ % ls /mnt/usb
poxten-virtual-machine ~ % ls -l /mnt/usb
total 0
```

4. Εκτέλεση της mount για να δούμε τα συστήματα που έχουν φορτωθεί:

```
poxten-virtual-machine ~ % mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
none on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
```

Εικόνα 18 mount null

5. Φόρτωση(mount) του usb stick (/dev/sdb1) στον κατάλογο /mnt/usb :

```
poxten-virtual-machine ~ % mount -t auto -o ro /dev/sdb1 /mnt/usb
poxten-virtual-machine ~ % ls -il /mnt/usb
total 3840
1601 -rwxr-xr-x 1 root root   34494 Ιούν 28 23:40 autorun.ico
1600 -rwxr-xr-x 1 root root     204 Ιούν 28 23:40 autorun.inf
1588 drwxr-xr-x 3 root root    8192 Ιούν 28 23:14 boot
1589 drwxr-xr-x 2 root root    8192 Ιούν 28 23:14 casper
1590 drwxr-xr-x 5 root root    8192 Ιούν 28 23:19 dart
1591 -rwxr-xr-x 1 root root 2534400 Ιούν 28 23:40 dart.exe
1592 drwxr-xr-x 3 root root    8192 Ιούν 28 23:40 dists
1585 drwxr-xr-x 3 root root    8192 Ιούν 28 23:14 EFI
1593 drwxr-xr-x 2 root root    8192 Ιούν 28 23:40 install
1594 drwxr-xr-x 2 root root    8192 Ιούν 28 23:40 isolinux
1584 -r-xr-xr-x 1 root root   37512 Ιούν 28 23:14 ldlinux.sys
1595 -rwxr-xr-x 1 root root 1188413 Ιούν 28 23:40 md5sum.txt
1596 drwxr-xr-x 2 root root    8192 Ιούν 28 23:40 pics
1597 drwxr-xr-x 6 root root    8192 Ιούν 28 23:40 pool
1598 drwxr-xr-x 2 root root    8192 Ιούν 28 23:40 preseed
1586 -rwxr-xr-x 1 root root     189 Ιούν 28 23:14 README.diskdefines
1599 -rwxr-xr-x 1 root root      94 Ιούν 28 23:40 syslinux.cfg
1587 -rwxr-xr-x 1 root root    1016 Ιούλ 14 18:18 TO-DO.txt
```

Εικόνα 19 mount /dev/sdb1

6. Επανέλεγχος με την mount :

```
/dev/sdb1 on /mnt/usb type vfat (ro)
```

Εικόνα 20 Επανέλεγχος με την mount

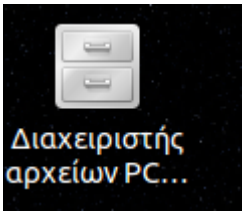
7. Εκφόρτωση (umount) του usb stick :

```
poxten-virtual-machine ~ % umount /dev/sdb1
poxten-virtual-machine ~ % ls -li /mnt/usb
total 0
poxten-virtual-machine ~ %
```

Εικόνα 21 umount usb stick

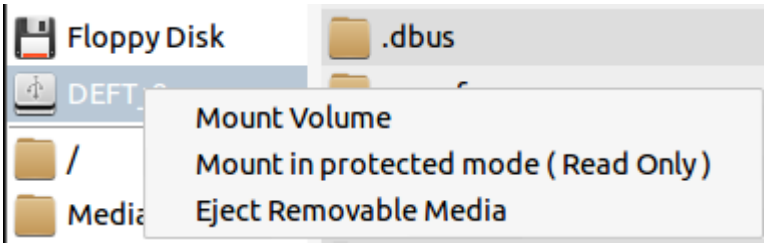
Η διαδικασία της φόρτωσης/εκφόρτωσης μπορεί να γίνει μέσω γραφικού περιβάλλοντος στο DEFT LINUX .Ανοίγοντας τον Διαχειριστή Αρχείων βρίσκουμε όλα τα συστήματα αρχείων που αναγνωρίζει ο υπολογιστής μας .Τις αφαιρούμενες συσκευές (εξωτερικοί σκληροί δίσκοι, usb sticks κλπ) τις αναγνωρίζει, χωρίς όμως να τις έχει φορτώνει .Τα βήματα είναι τα ακόλουθα:

1. Άνοιγμα του διαχειριστή αρχείων :



Εικόνα 22 Διαχειριστής Αρχείων DEFT

2. Φόρτωση του usb stick (το όνομα του usb stick είναι DEFT8):



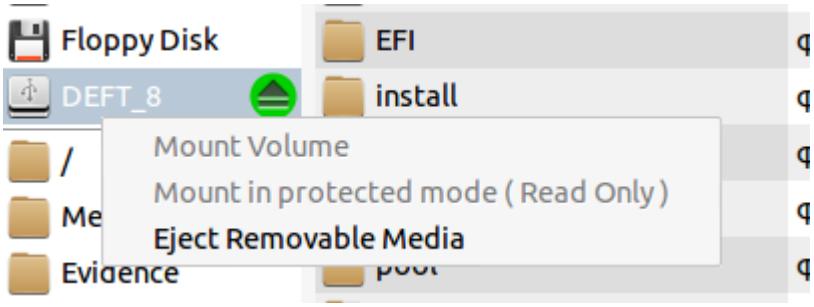
Εικόνα 23 Διαχειριστής Αρχείων GUI-mount

3. Παρουσίαση περιεχομένων του usb stick :

Name	Description	Size	Modified
.disk	φάκελος		28/06/2015 23:14
boot	φάκελος		28/06/2015 23:14
casper	φάκελος		28/06/2015 23:14
dart	φάκελος		28/06/2015 23:19
dists	φάκελος		28/06/2015 23:40
EFI	φάκελος		28/06/2015 23:14
install	φάκελος		28/06/2015 23:40
isolinux	φάκελος		28/06/2015 23:40
pics	φάκελος		28/06/2015 23:40
pool	φάκελος		28/06/2015 23:40
preseed	φάκελος		28/06/2015 23:40
autorun.ico	Microsoft icon	33,7 KiB	28/06/2015 23:40
autorun.inf	έγγραφο απλού κειμένου	204 bytes	28/06/2015 23:40
dart.exe	εκτελέσιμο DOS/Windows	2,4 MiB	28/06/2015 23:40
ldlinux.sys	αγνωστο	36,6 KiB	28/06/2015 23:14
md5sum.txt	έγγραφο απλού κειμένου	1,1 MiB	28/06/2015 23:40

Εικόνα 24 Διαχειριστής Αρχείων περιεχόμενα usb stick

4. Εκφόρτωση (umount) του usb stick :



Εικόνα 25 Διαχειριστής Αρχείων umount DEFT

3.Δημιουργία αντιγράφων-εικόνας συστήματος

Στον κεφάλαιο αυτό θα αναφερθούμε στις μεθόδους που παρέχει το Linux για την δημιουργία αντιγράφου του εκάστοτε υπό εξέταση στοιχείου.

Το κρισιμότερο βήμα για την ψηφιακή εγκληματολογία είναι η λήψη ενός αντιγράφου του υπό εξέταση μέσου αποθήκευσης .**Ποτέ** δεν διεξάγουμε την έρευνα στο μέσο αποθήκευσης , αλλά σε ένα αντίγραφο του. Αυτό το κάνουμε προκειμένου να μην αλλοιώσουμε το αρχικό στοιχείο .

Ο **στόχος μας** είναι η λήψη ενός αντιγράφου χωρίς να μεταβάλουμε το υπό εξέταση στοιχείο.

Η δημιουργία ενός αντίγραφου δεδομένων διακρίνεται σε:

- Απλό αντίγραφο (simple duplication) : ενός αρχείου , ομάδας αρχείων , ενός partition ενός δίσκου , ενός ολόκληρου μέσου αποθήκευσης.
- Εγκληματολογικό αντίγραφο (Forensic duplication) : ένα ακριβές αντίγραφο των δεδομένων , που θα έχει σαν στόχο να είναι αποδεκτό ως αποδεικτικό στοιχείο σε νομικές διαδικασίες . Ορίζουμε ως εγκληματολογικό λογικό αντίγραφο μια εικόνα όπου θα είναι όμοια με το υπό εξέταση στοιχείο και δεν θα διαφέρει ούτε ένα bit.

Άρα θα πρέπει να χρησιμοποιήσουμε μεθόδους για την λήψη αντιγράφων που είναι ευρέως αποδεκτές από τους οργανισμούς που εμπλέκονται στο αντικείμενο της ψηφιακής εγκληματολογίας (Δικαιοσύνη , Κρατικός μηχανισμός κλπ).

Η εκάστοτε μέθοδος θα πρέπει να εξασφαλίζει τα ακόλουθα :

α. Πρέπει να έχει την ικανότητα να αντιγράφει κάθε bit του μέσου αποθήκευσης.
β. Πρέπει να δημιουργεί ένα αντίγραφο εγκληματολογίας (forensic duplication) του πρότυπου μέσου αποθήκευσης .
γ. Πρέπει να χειρίζεται τα λάθη ανάγνωσης (read errors)
δ. Δεν πρέπει να κάνει αλλαγές στο αρχικό μέσο αποθήκευσης .
ε. Πρέπει να παράγει αποτελέσματα τα οποία μπορούν να επαληθεύουν από μια Τρίτη οντότητα .
στ. Πρέπει να παράγει αρχεία καταγραφής που θα περιλαμβάνουν τις ενέργειες που έγιναν και πιθανά σφάλματα που προέκυψαν.

Το αντίγραφο που προκύπτει είναι το πολυτιμότερο στοιχείο στο οποίο θα διεξάγουμε την έρευνα μας . Το επόμενο βήμα μας είναι να αποδείξουμε ότι το πειστήριο δεν έχει αλλοιωθεί κατά οποιοδήποτε τρόπο .Αυτό το εξασφαλίζουμε με την χρήση συναρτήσεων σύνοψης (hash functions).

Οι συναρτήσεις σύνοψης λαμβάνουν μια είσοδο (π.χ. σκληρός δίσκος , usb stick) και παράγουν σαν έξοδο ένα αλφαριθμητικό (hash value) σταθερού μεγέθους.

Σε μερικά μέσα αποθήκευσης υπάρχουν τμήματα τους που φιλοξενούν πληροφορίες οι οποίες δεν είναι προσπελάσιμες από το BIOS και κατ' επέκταση ούτε από τον χρήστη .Συνήθως τα χρησιμοποιούν οι κατασκευαστές για να αποθηκεύουν δεδομένα και πληροφορίες που χρειάζονται για την επαναφορά των συστημάτων τους στις εργοστασιακές ρυθμίσεις (system restore). Τα τμήματα διακρίνονται σε :

- HPA(Host Protected Area)
- DCO(Device configuration Overlay)

Οφείλουμε να ελέγξουμε για την ύπαρξη τους κατά την διάρκεια της έρευνας μας διότι αποτελούν ιδανικό μέρος απόκρυψης δεδομένων.

3.1 Δημιουργία Αντίγραφου μέσω της γραμμής εντολών

Η διανομή DEFT LINUX μας παρέχει μια πληθώρα εργαλείων μέσω των οποίων μπορούμε να δημιουργήσουμε αντίγραφα των μέσων αποθήκευσης .

Οι εντολές που είναι κατάλληλες για αυτό τον σκοπό είναι οι ακόλουθες:

- dd
- bcfldd
- bc3dd
- cyclone

dd

Η εντολή dd υπάρχει σε όλες τις διανομές Linux και Unix . Η χρησιμοποιείται για αντιγραφή και μετατροπή αρχείων .Αντιγράφει το αρχείο που προσδιορίζεται σαν αρχείο εισόδου (input file) στο αρχείο εξόδου (output file).

Η dd διαβάζει και γράφει δεδομένα σε blocks , των οποίων το μέγεθος αρμόζει στην αντίστοιχη συσκευή. Κατά συνέπεια η dd μπορεί να χρησιμοποιηθεί για αντιγραφή αρχείων από μια συσκευή σε διαφορετική συσκευή.

Όπως έχουμε αναφέρει το Linux αντιλαμβάνεται τους σκληρούς δίσκους και οποιοδήποτε υλικό ως ειδικά αρχεία (special files). Άρα μπορούμε να την χρησιμοποιήσουμε για την δημιουργία ενός αντιγράφου μια συσκευής.

- dd [επιλογή =τιμή] …

Πίνακας 3 Επιλογές (options) της εντολής dd

Επιλογές της dd	Ερμηνεία των επιλογών (options)
If = αρχείο	Προσδιορίζεται το αρχείο εισόδου(input file)
of = αρχείο	Προσδιορίζεται το αρχείο εξόδου(output file)
bs = n	Καθορίζεται το μέγεθος των blocks του αρχείου εισόδου/εξόδου σε n bytes (το τυποποιημένο είναι n = 512 bytes)
skip = n	Αγνοούμαι n blocks από το αρχείο εισόδου πριν αρχίσει η αντιγραφή
seek = n	Κατά την αντιγραφή τα πρώτα n blocks από το αρχείο εξόδου μένουν ανέπαφα
count = n	Αντιγράφονται μόνο n blocks από το αρχείο εισόδου

```
poxten-virtual-machine ~ % dd if=/dev/sdb of=/home/poxten/evidence/image.dd
2007040+0 records in
2007040+0 records out
1027604480 bytes (1,0 GB) copied, 231,663 s, 4,4 MB/s
poxten-virtual-machine ~ % file /home/poxten/evidence/image.dd
/home/poxten/evidence/image.dd: DOS floppy 1440k, x86 hard disk boot sector
poxten-virtual-machine ~ % ls -li /home/poxten/evidence/image.dd
396070 -rw-r--r-- 1 root root 1027604480 Ιούλ 27 19:59 /home/poxten/evidence/image.dd
poxten-virtual-machine ~ %
```

Εικόνα 26 dd παράδειγμα

Μετά το τέλος της εκτέλεσης της dd , στην οθόνη εμφανίζεται ο αριθμός των blocks που διαβάστηκαν από το αρχείο εισόδου και ο αριθμός των blocks που γράφτηκαν στο αρχείο εξόδου . Αυτός ο αριθμός εμφανίζεται σαν άθροισμα . Ο πρώτος πρόσθετος δείχνει τον αριθμό των **ολόκληρων blocks** , ενώ ο δεύτερος των αριθμό των **μερικών blocks**.

dcfldd

Αποτελεί παραλλαγή της εντολής dd . Το U.S Department of Defense Computer Laboratory (DFCLdd) την έχει δημιουργήσει .Ο σκοπός της είναι να εκμεταλλευτεί τις δυνατότητες της dd , αλλά με σαφή προσανατολισμό για την ψηφιακή εγκληματολογία .

```
poxten-virtual-machine ~ % whatis dcfldd
dcfldd (1)           - enhanced version of dd for forensics and security
```

Εικόνα 27 whatis dcfldd

- dcfldd [επιλογή = τιμή] …

Μια σημαντική προσθήκη είναι η επιλογή hash η οποία μπορεί να λάβει τις ακόλουθες τιμές :

- md5
- sha1
- sha512

```
poxten-virtual-machine ~ % dcfldd if=/dev/sdb of=/home/poxten/evidence/image.dcfldd has
h=md5
31232 blocks (976Mb) written.Total (md5): 8bed54e1f6238a6d655088b391396416

31360+0 records in
31360+0 records out
```

Εικόνα 28 dcfldd παράδειγμα

Κατά την διάρκεια της δημιουργίας του αντίγραφου η εντολή μας εμφανίζει τον αριθμό των blocks και το μέγεθος του αντίγραφου . Μετά την ολοκλήρωση μας δίνει το md5 του αντίγραφου . (πηγή: http://dcfldd.sourceforge.net/)

Dc3dd

Αποτελεί παραλλαγή της dd. Είναι όμοια με την dcfldd . Έχει αναπτυχθεί από Defense Cyber Crime Center (DC3) . Είναι η πιο πρόσφατη όλων .

```
poxten-virtual-machine ~ % whatis dc3dd
dc3dd (1)            - convert and copy a file
```

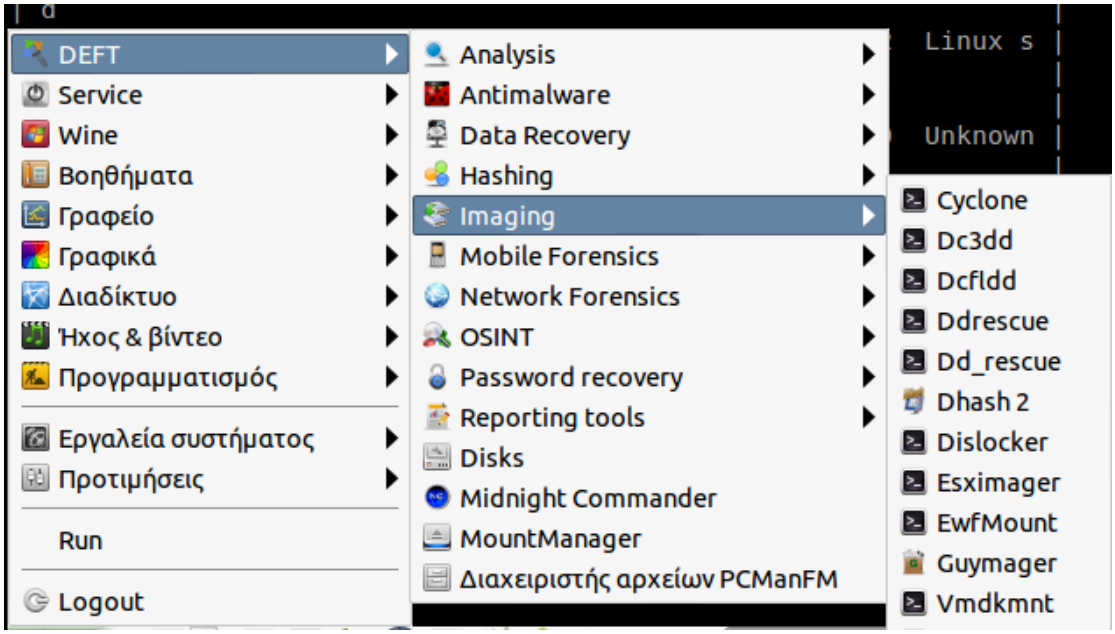
Εικόνα 29 whatis dc3dd

- dc3dd [επιλογή = τιμή] ….

```
poxten-virtual-machine ~ % dc3dd if=/dev/sdb of=/home/poxten/evidence/image.dc3dd hash=
md5 hlog=/home/poxten/evidence/sdb.log

dc3dd 7.1.614 started at 2015-07-27 21:52:31 +0300
compiled options:
command line: dc3dd if=/dev/sdb of=/home/poxten/evidence/image.dc3dd hash=md5 hlog=/hom
e/poxten/evidence/sdb.log
device size: 2007040 sectors (probed)
sector size: 512 bytes (probed)
1027604480 bytes (980 M) copied (100%), 238,182 s, 4,1 M/s

input results for device `/dev/sdb':
   2007040 sectors in
   0 bad sectors replaced by zeros
   8bed54e1f6238a6d655088b391396416 (md5)

output results for file `/home/poxten/evidence/image.dc3dd':
   2007040 sectors out

dc3dd completed at 2015-07-27 21:56:30 +0300
```

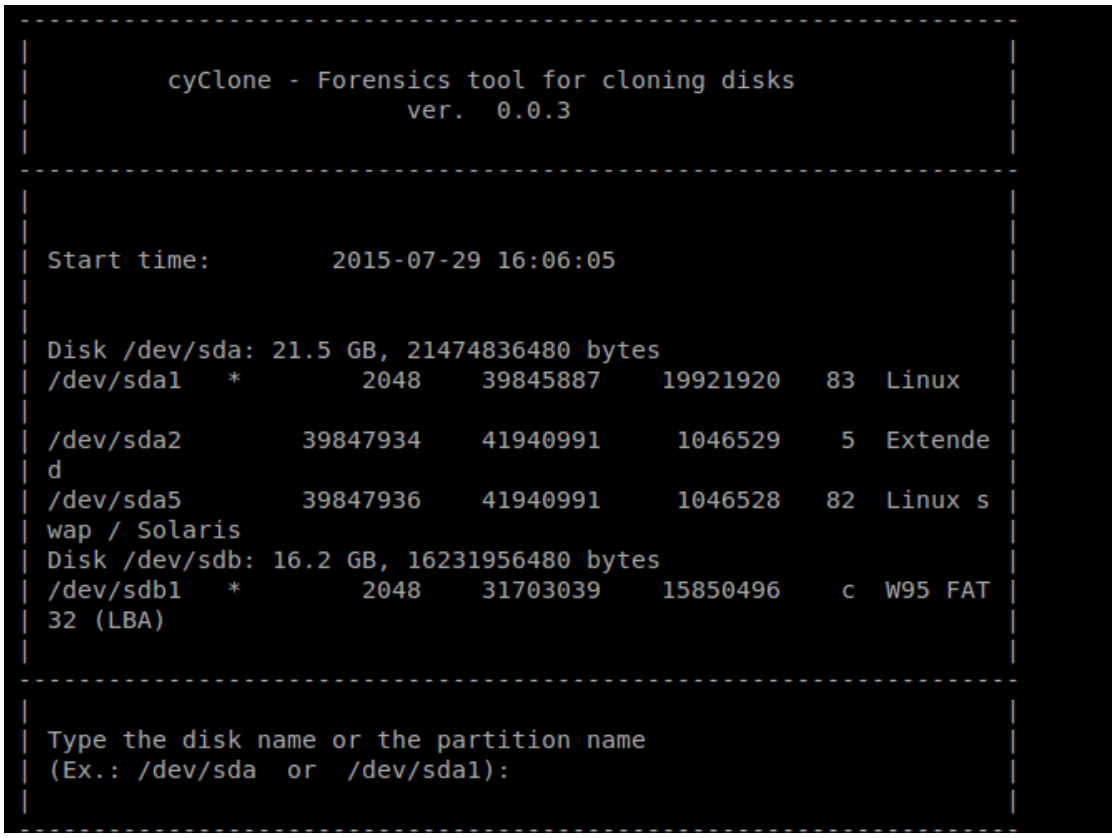
Εικόνα 30 dc3dd παράδειγμα

Cyclone



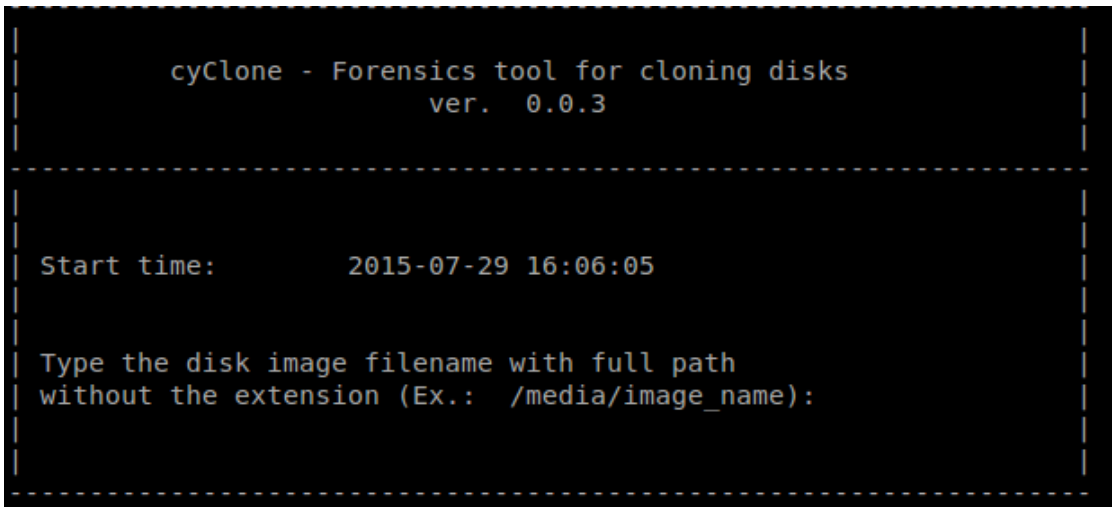
Εικόνα 31 cyclone menu

Ένα εργαλείο που μας παρέχει το DEFT Linux είναι Cyclone . Για την δημιουργία ενός αντιγράφου μας καθοδηγεί βήμα-βήμα , μέσω της γραμμής εντολών .Παρακάτω θα παρουσιάσουμε την διαδικασία λήψης ενός αντιγράφου:



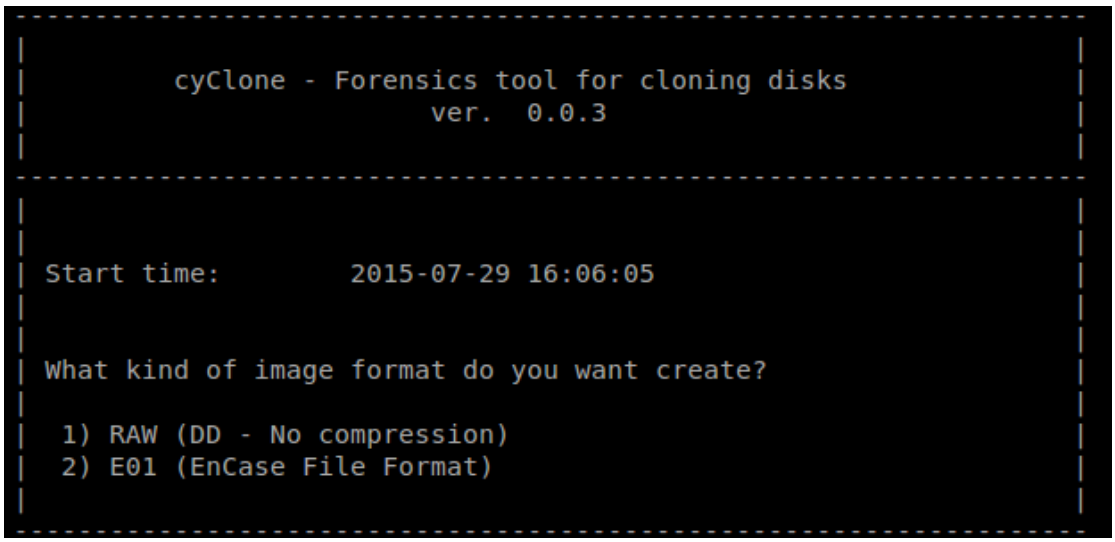
Εικόνα 32 cyclone 1

Με την εκτέλεση της εντολής cyclone μας εμφανίζει όλα τα αποθηκευτικά μέσα που είναι συνδεδεμένα στο σύστημα μας και τις διαμερίσεις τους . Στο σημείο αυτό εισάγουμε το όνομα της συσκευής που επιθυμούμε να αντιγράψουμε. Στο παράδειγμα αυτό θα εισάγουμε το /dev/sdb (είναι ένα usb stick).



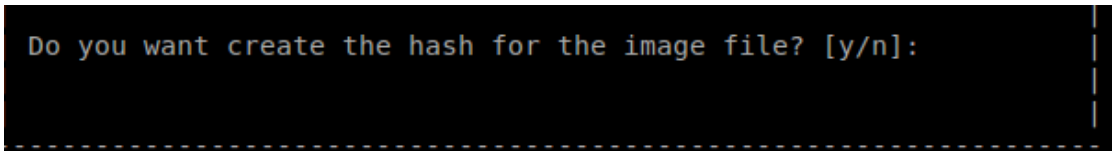
Εικόνα 33 cyclone 2

Στην συνέχεια μας ζητάει να ορίσουμε το όνομα που θέλουμε να δώσουμε και σε ποιο κατάλογο θέλουμε να αποθηκευτεί .Θα δώσουμε σαν είσοδο /home/poxten/evidence/image.cyclone



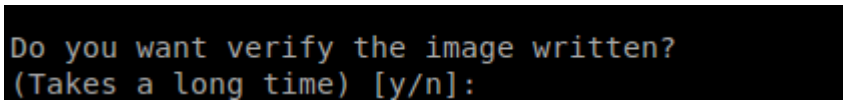
Εικόνα 34 cyclone 3

Στο επόμενο βήμα μας δίνει την δυνατότητα επιλογής της μορφής (format) που θέλουμε να έχει το αντίγραφό μας . Εμείς θα επιλέξουμε το 1 .



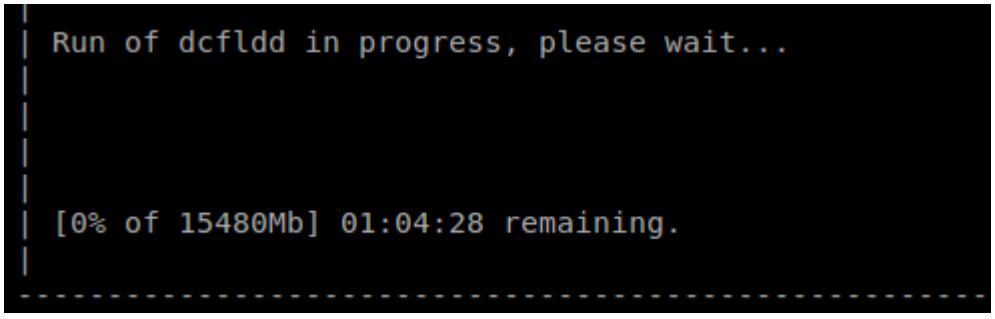
Εικόνα 35 cyclone 4

Ακολούθως μας ρωτάει εάν επιθυμούμε να υπολογίσει το hash value. Με [y] μας το υπολογίζει.



Εικόνα 36 cyclone 5

Μας ρωτάει εάν επιθυμούμε επαλήθευση του αντίγραφου .Μας ενημερώνει ότι η διαδικασία αυτή απαιτεί κάποιο χρονικό διάστημα.



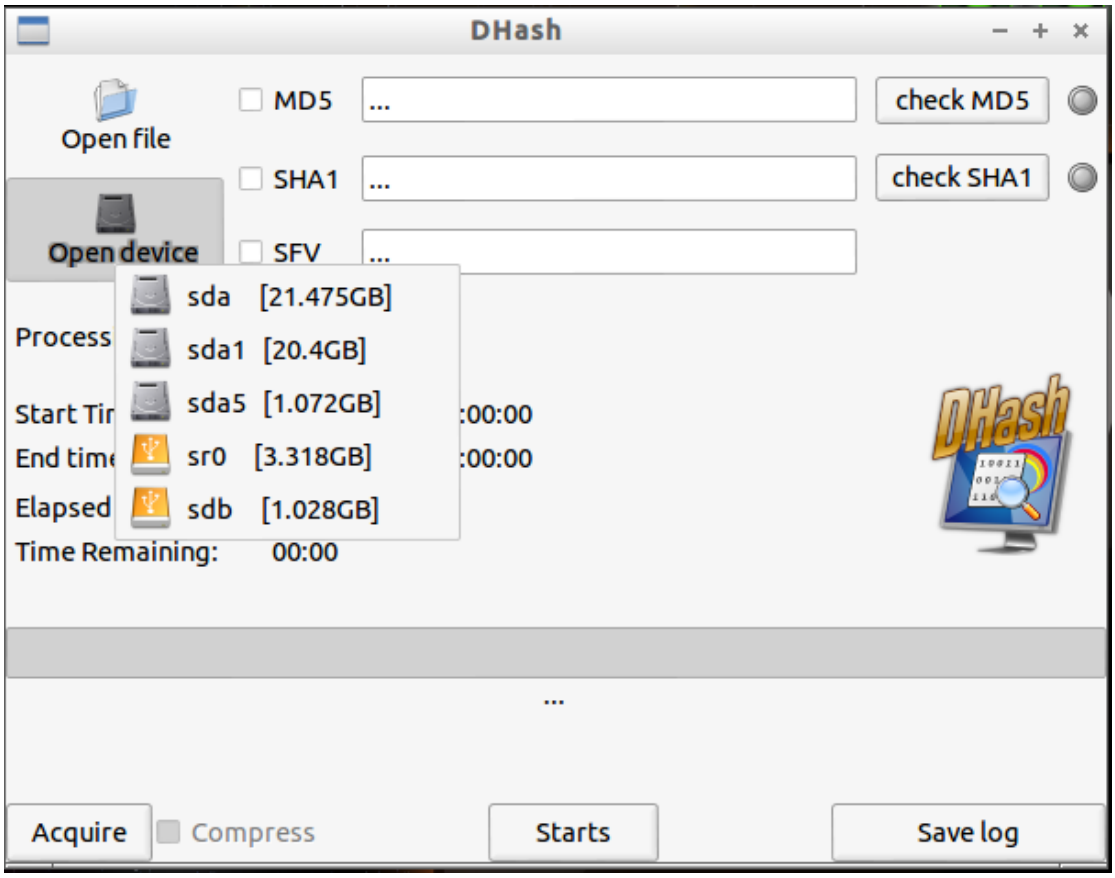
Εικόνα 37 cyclone 6

Ακολούθως ξεκινάει η διαδικασία δημιουργίας αντίγραφου. Βλέπουμε στην παραπάνω εικόνα ότι το αντίγραφο δημιουργείται από το εργαλείο dcfldd που αναλύσαμε .Το μεγάλο όφελος της cyclone είναι ότι μας καθοδηγεί για την δημιουργία αντίγραφου και ότι χρησιμοποιεί αποδεκτές μεθόδους για την δημιουργία ψηφιακών αντίγραφων.

3.2 Δημιουργία αντίγραφου μέσω γραφικού περιβάλλοντος

Με το DEFT Linux μπορούμε να δημιουργήσουμε αντίγραφα μέσω γραφικού περιβάλλοντος χρησιμοποιώντας το DHASH. Η μορφοποίηση του αντίγραφου είναι dd . Πρόσθετα μπορούμε να υπολογίσουμε το hash value της συσκευής .Η μπάρα στην επιφάνειας εργασίας περιλαμβάνει το ακόλουθο εικονίδιο 

.



Εικόνα 38 DHASH GUI

Μπορούμε να διαλέξουμε την συσκευή που θέλουμε να αντιγράψουμε κάνοντας κλικ στο “open device”και στην συνέχεια να κάνουμε κλικ στο“Acquire” .Πατώντας το “Starts” η αντιγραφή ξεκινάει.

Προκειμένου να υπολογίσουμε το hash value πρέπει να επιλέξουμε τον αλγόριθμο βάση του οποίου θα προκύψει η τιμή.

Μετά το τέλος της όλης διαδικασίας μπορούσε να δημιουργήσουμε μια αναφορά σε μορφοποίηση html κάνοντας κλικ στο κουμπί “Save log”.

3.3 Φόρτωση ενός αντιγράφου-εικόνας

Το αντίγραφο (image) πρέπει να φορτωθεί στο σύστημα αρχείων μας .Η διαδικασία φόρτωσης εξαρτάται από το εάν το αντίγραφο(image) είναι αποθηκευμένο σε κάποια συσκευή αποθήκευσης(hard disk or usb stick) ή στον υπολογιστή μας.

Σε κάθε περίπτωση πρέπει να έχουμε δημιουργήσει ένα υποκατάλογο στον οποίο θα φορτώσουμε το υπό εξέταση στοιχείο (πχ mkdir /mnt/analysis).

- **Φόρτωση ενός Restored image**

```
poxten-virtual-machine ~/Desktop % ls -lih /mnt/analysis/
total 0
poxten-virtual-machine ~/Desktop % mount -t auto -o ro,noexec,noatime /dev/sdb /mnt/ana
lysis/
poxten-virtual-machine ~/Desktop % ls -lih /mnt/analysis/
total 107K
12 -rwxr-xr-x 1 root root 20K Αύγ  24  1996 ARP.EXE
10 drwxr-xr-x 3 root root 512 Σεπ  23  2000 Docs
13 -rwxr-xr-x 1 root root 37K Αύγ  24  1996 FTP.EXE
14 -r-xr-xr-x 1 root root 16K Σεπ  21  2000 loveletter.virus
15 -rwxr-xr-x 1 root root 21K Μάρ  19  2000 ouchy.dat
11 drwxr-xr-x 2 root root 512 Σεπ  23  2000 Pics
16 -rwxr-xr-x 1 root root 13K Αύγ   2  2000 snoof.gz
poxten-virtual-machine ~/Desktop %
```

Εικόνα 39 mount restored image

- **Φόρτωση ενός image χρησιμοποιώντας το Device loopback**

Εάν έχουμε το image αποθηκευμένο στον υπολογιστή μας για να το φορτώσουμε θα χρειαστεί να χρησιμοποιήσουμε την διεπαφή loop(loop device). Μας επιτρέπει η διεπαφή loop να φορτώσουμε ένα σύστημα αρχείων που είναι σε μορφή image σε ένα κατάλογο(mount point) για να δούμε τα περιεχόμενα του. Για να μπορέσουμε να κάνουμε κάτι τέτοιο πρέπει να συμπεριλάβουμε την επιλογή (option) loop.

```
poxten-virtual-machine ~/Desktop % ls -lih /mnt/analysis/
total 0
poxten-virtual-machine ~/Desktop % mount -t auto -o ro,noexec,noatime,loop /root/Deskto
p/dhash.dd  /mnt/analysis/
poxten-virtual-machine ~/Desktop % ls -lih /mnt/analysis/
total 107K
40 -rwxr-xr-x 1 root root 20K Αύγ  24  1996 ARP.EXE
38 drwxr-xr-x 3 root root 512 Σεπ  23  2000 Docs
41 -rwxr-xr-x 1 root root 37K Αύγ  24  1996 FTP.EXE
42 -r-xr-xr-x 1 root root 16K Σεπ  21  2000 loveletter.virus
43 -rwxr-xr-x 1 root root 21K Μάρ  19  2000 ouchy.dat
39 drwxr-xr-x 2 root root 512 Σεπ  23  2000 Pics
44 -rwxr-xr-x 1 root root 13K Αύγ   2  2000 snoof.gz
poxten-virtual-machine ~/Desktop %
```

Εικόνα 40 mount loopback

4.Οδηγός Χρήσης του Autopsy

Σε αυτό το κεφάλαιο θα παρουσιάσουμε το εργαλείο ψηφιακής εγκληματολογίας Autopsy 3.0 . Στην τελευταία του έκδοση που απευθύνεται μόνο στο λειτουργικό σύστημα Windows.

4.1 Εισαγωγή

Το Autopsy μας παρέχει την δυνατότητα διενέργειας μιας ψηφιακής εγκληματολογικής έρευνας . Είναι μια γραφική διεπαφή του Sleuth kit και άλλων εργαλείων.

Για να χρησιμοποιήσουμε χρειαζόμαστε τα ακόλουθα:

- Ο υπολογιστής μας να έχει ως λειτουργικό σύστημα Windows XP, Vista ,7 ,8 ή 10
- Το υπό εξέταση στοιχείο (εικόνα δίσκου) που περιέχει την πληροφορία που θέλουμε να αναλύσουμε να είναι μορφοποίησης (format) dd ή E01.
- Το σύστημα αρχείων (file system) του δίσκου πρέπει να έχει μια από τις ακόλουθες μορφοποιήσεις :
    - NTFS
    - FAT12,FAT16,FAT32
    - HFS+
    - ISO9660
    - Ext2,Ext3
    - UFS
- Εάν θέλουμε να εισάγουμε μια βάση δεδομένων hash μόνο οι ακόλουθες μορφοποιήσεις υποστηρίζονται:
    - NIST NSRL
    - Encase
    - MD5
    - HashKeeper

Η ψηφιακή εγκληματολογία έχει ως αντικείμενο την ανάκτηση δεδομένων από ψηφιακές συσκευές . Οι ψηφιακές συσκευές έχουν τα ακόλουθα είδη πληροφοριών:

α. <u>Δεδομένα Διαδικτύου(Internet Data):</u>

- Cookies
- Ιστορικό περιήγησης
- Λήψη αρχείων

β. Μεταδεδομένα(Metadata):

Είναι πληροφορίες που ενσωματώνει το εκάστοτε πρόγραμμα στα αρχεία που παράγει .Οι πληροφορίες αυτές καθορίζουν :

- Πότε το αρχείο δημιουργήθηκε
- Από ποιον χρήστη
- Το μέγεθος του αρχείου

γ. Αρχεία συστήματος και Αρχεία καταγραφής (System files and System logs):

Παρέχουν πληροφορίες για τις δραστηριότητες του συστήματος

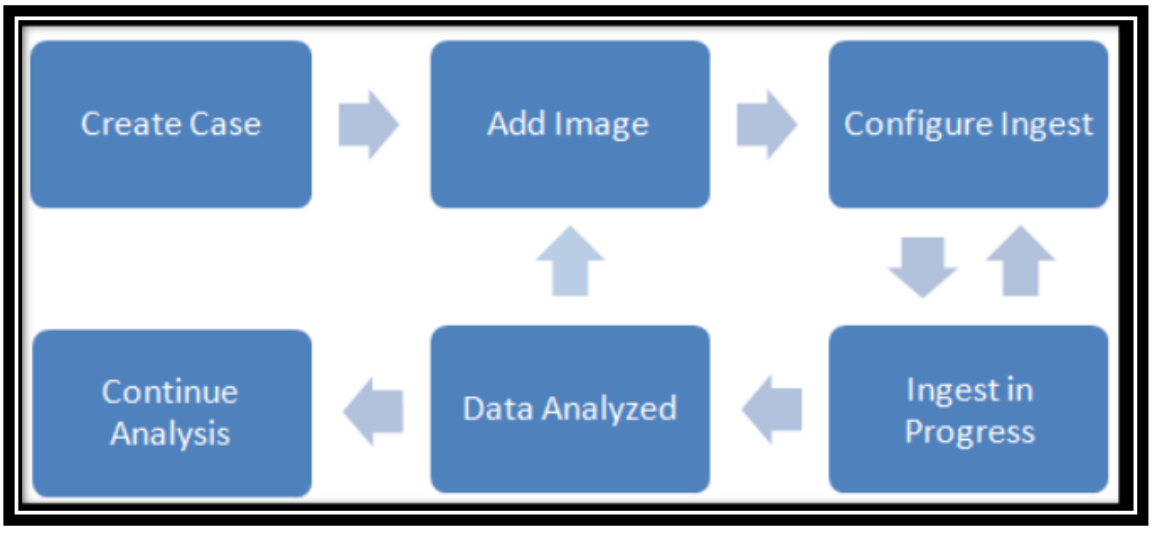
- Προγράμματα που εγκατασταθήκαν
- Συσκευές που φορτώθηκαν
- Το ιστορικό των χρηστών που χρησιμοποίησαν το σύστημα

δ. Διαγραμμένα Αρχεία (Deleted files):

Σαν χρήστες θεωρούμε ότι τα διαγραμμένα αρχεία δεν υπάρχουν στο σύστημα . Όμως γνωρίζουμε ότι κάτι τέτοιο δεν είναι αληθές διότι τα λειτουργικά συστήματα δεν μετακινούν τα αρχεία όταν τα διαγράψουν . Αντίθετα δείχνουν ότι είναι ο χώρος αποθήκευσης διαθέσιμος για χρήση. Δηλαδή μέχρι ότου ξαναγραφτεί ο χώρος αποθήκευσης , τα διαγραμμένα δεδομένα είναι προσβάσιμα από εργαλεία σαν το Autopsy.

4.2 Εκκίνηση του Autopsy

Κατά την εκκίνηση του Autopsy η εφαρμογή θα μας οδηγήσει μέσω της διεργασίας υπόθεσης (case). Θα προσθέσουμε την εικόνα του δίσκου (disk image) και θα εκκινήσουμε την ανάλυση του . Η όλη διαδικασία φαίνεται στην ακόλουθη εικόνα



Εικόνα 41 Διεργασία Autopsy

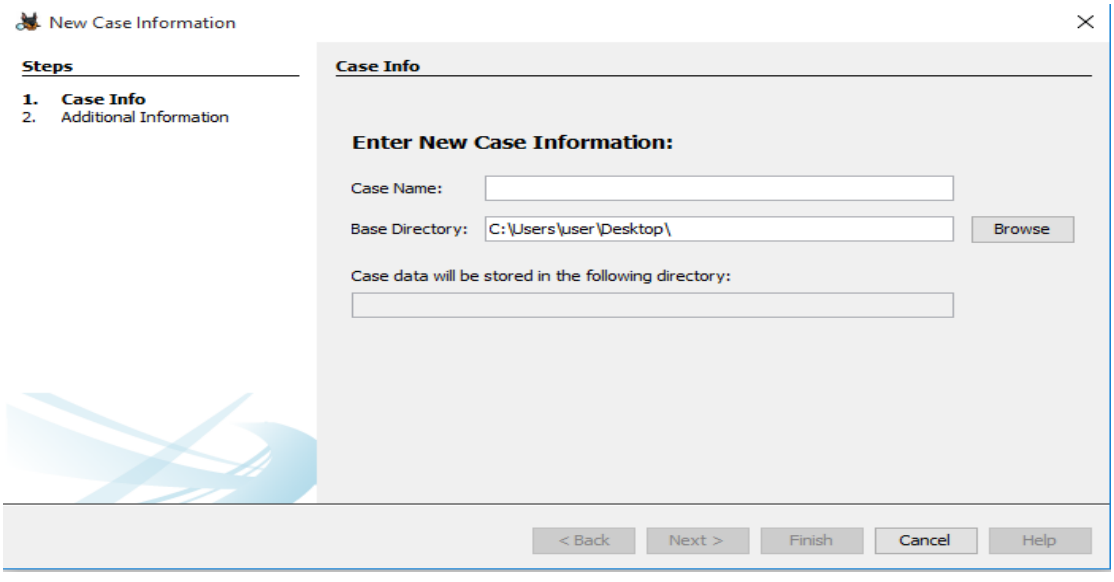
4.2.1 Δημιουργία υπόθεσης

Μια υπόθεση (case) είναι μια συλλογή πληροφοριών (container) . Η υπόθεση πρέπει να περιέχει τουλάχιστον μια εικόνα δίσκου , αλλά μπορούμε στην ίδια υπόθεση να προσθέσουμε όσες εικόνες θέλουμε . Για παράδειγμα εάν έχουμε πολλούς σκληρούς δίσκους μπορούμε την εικόνα του καθενός να την προσθέσουμε στην υπόθεση μας.

Εικόνα 42 Εκκίνηση Autopsy

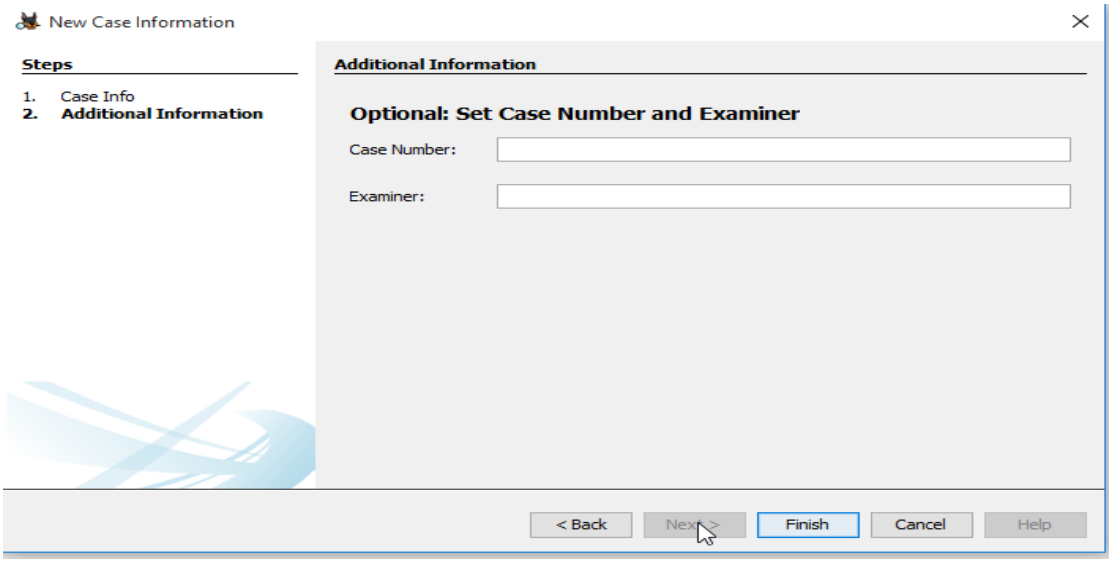
Για να δημιουργήσουμε μια υπόθεση ακολουθούμε τα εξής βήματα:

1. Στο αρχικό παράθυρο (Εικόνα 42) επιλέγουμε **Create New Case** και εμφανίζεται το ακόλουθο παράθυρο:



Εικόνα 43 Πληροφορίες Νέας Υπόθεσης/New Case Information

2. Στο πεδίο **Case Name** γράφουμε το όνομα της υπόθεσης .
3. Στο κουμπί **Browse** μπορούμε να επιλέξουμε που θέλουμε να αποθηκευτεί ο φάκελος της υπόθεσης
4. Επιλέγουμε το κουμπί Next

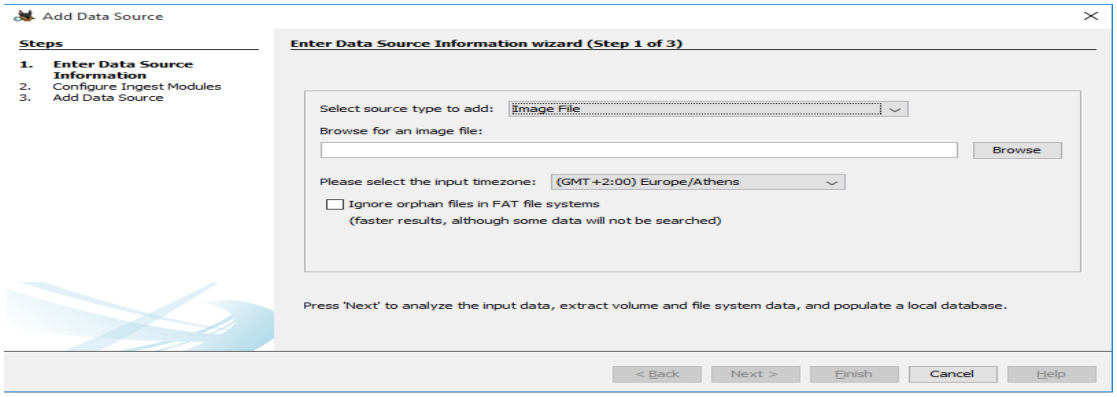


Εικόνα 44 Πρόσθετες Πληροφορίες / Additional Information

5. Στο πεδίο **Case Number** συμπληρώνουμε τον αριθμό της υπόθεσης και στο πεδίο **Examiner** το όνομα του ερευνητή. Αυτές της πληροφορίες δεν μπορούμε να τις συμπληρώσουμε εκ των υστέρων
6. Επιλέγουμε το κουμπί **Finish** και εμφανίζεται το παράθυρο Add Image . Σε αυτό το στάδιο μπορούμε να προσθέσουμε την εικόνα του δίσκου που θέλουμε να εξετάσουμε

4.2.2 Προσθήκη μιας Εικόνας Δίσκου

Μετά την δημιουργία της υπόθεσης , το παράθυρο **Add Data Source** εμφανίζεται και σαν πρώτο βήμα μας ζητάει να εισάγουμε τις πληροφορίες της εικόνας δίσκου .



Εικόνα 45 Παράθυρο Προσθήκης Εικόνας

> Προσοχή!!!
>
> Όταν προσθέσουμε μια εικόνα (image) σε μια υπόθεση δεν μπορούμε να την αφαιρέσουμε

Για να προσθέσουμε εικόνα δίσκου κάνουμε τα εξής :

1. Στο παράθυρο **Add Data Source** επιλέγουμε το κουμπί Browse ,προκειμένου να υποδείξουμε στο Autopsy που είναι αποθηκευμένη η εικόνα
2. Εάν το αντίγραφο έγινε σε διαφορετική ζώνη ώρας επιλέγουμε την κατάλληλη
3. Επιλέγουμε το **Next**. Το παράθυρο ανανεώνεται και μας καθοδηγεί στο επόμενο βήμα **Configure Ingest Modules**

Είμαστε έτοιμοι να επιλέξουν την διαμόρφωση της ανάλυσης του δίσκου. Το Autopsy την καλή αυτή την διαδικασία **Ingest**.

4.2.3 Διαμόρφωση Ανάλυσης Δίσκου

Το Autopsy αναφέρεται στην διαδικασία της αυτοματοποιημένης ανάλυσης δίσκου ως **Ingest** .Η διαδικασία της ανάλυσης εξάγει τους πιο κοινούς τύπους πληροφορίας που μας ενδιαφέρουν από την οπτική της ψηφιακής εγκληματολογίας . Η διαδικασία εκτελείται στο παρασκήνιο.

Η διαδικασία **(ingest process)** χρησιμοποιεί συγκεκριμένες μεθόδους **(modules)** , όπου η κάθε μέθοδος αναλύει συγκεκριμένους τύπους δεδομένων. Ανάλογα των τύπο δεδομένων που αναζητούμε για την ερευνά μας , το Autopsy μας παρέχει τις ακόλουθες μεθόδους :

Πίνακας 4 Μέθοδοι Διαδικασίας Ingest

Μέθοδος	Σκοπός
Αναζήτηση λέξης κλειδί (Key Word Search)	Δημιουργεί ένα ευρετήριο των λέξεων κλειδιών .Μπορούμε να αναζητήσουμε στο ευρετήριο για λέξεις ή να ορίσουμε λίστες λέξεων όπου η διαδικασία τις χρησιμοποιεί για να παράγει αποτελέσματα αναζήτησης
Σύνοψη(Hash)	Υπολογισμός του MD5 hash για κάθε αρχείο
Αναλυτής Thunderbird Parser	Εξάγει τα περιεχόμενα των email από το Outlook και το Thunderbird
Αναλυτής Exif Parser	Αναλύει τα μεταδεδομένα για αρχεία εικόνας (τοποθεσία ,ημέρα ,τύπος μηχανής). Αναγνωρίζει JPG,GIF,PNG.

Πρόσφατη δραστηριότητα (Resent Activity)	Εξάγει την δραστηριότητα του χρήστη .Επικεντρώνεται στο web και στα system settings • Εξάγει την δραστηριότητα του δίσκου για 7 ήμερες • Κατηγοριοποιεί τα αρχεία με βάση τα μεταδεδομένα τους • Εξάγει στοιχεία του Διαδικτύου • Προσδιορίζει τα αναγνωριστικά των συσκευών που συνδέθηκαν στον υπολογιστή Η μέθοδος υποστηρίζει μόνο Windows.

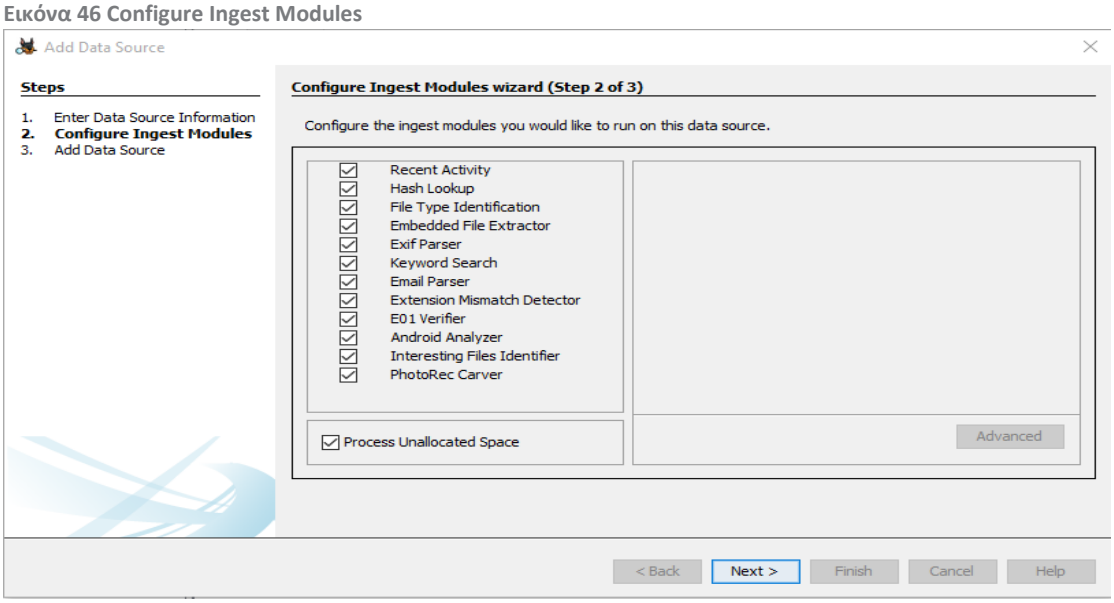
Μπορούμε να επιλέξουμε να αναλύσουμε και τον ελεύθερο χώρο του δίσκου **(Unallocated Disk Space)** . Δηλαδή το κομμάτι του δίσκου όπου το λειτουργικό σύστημα το έχει «σημαδέψει» σαν διαθέσιμο για χρήση αλλά ακόμα δεν έχει γραφτεί σε αυτό νέα δεδομένα . Εάν δεν το επιλέξουμε η διαδικασία μας θα ολοκληρωθεί πιο γρήγορα, αλλά με την πιθανότητα να απολέσουμε χρήσιμη πληροφορία.

Ο χρόνος που απαιτείται για την ανάλυση των περιεχομένων της εικόνας (image) εξαρτάται από δύο παραμέτρους:

- Το μέγεθος της εικόνας
- Ποιες μεθόδους της διαδικασίας Ingest έχουμε επιλέξει

Εάν δεν γνωρίζουμε πια δεδομένα θα χρειαστούμε καλύτερα να επιλέξουμε όλες τις διαθέσιμες μεθόδους. Εάν η διαδικασία διαρκεί πάρα πολύ μπορούμε να την ακυρώσουμε και να μειώσουμε τις μεθόδους .

Εικόνα 46 Configure Ingest Modules



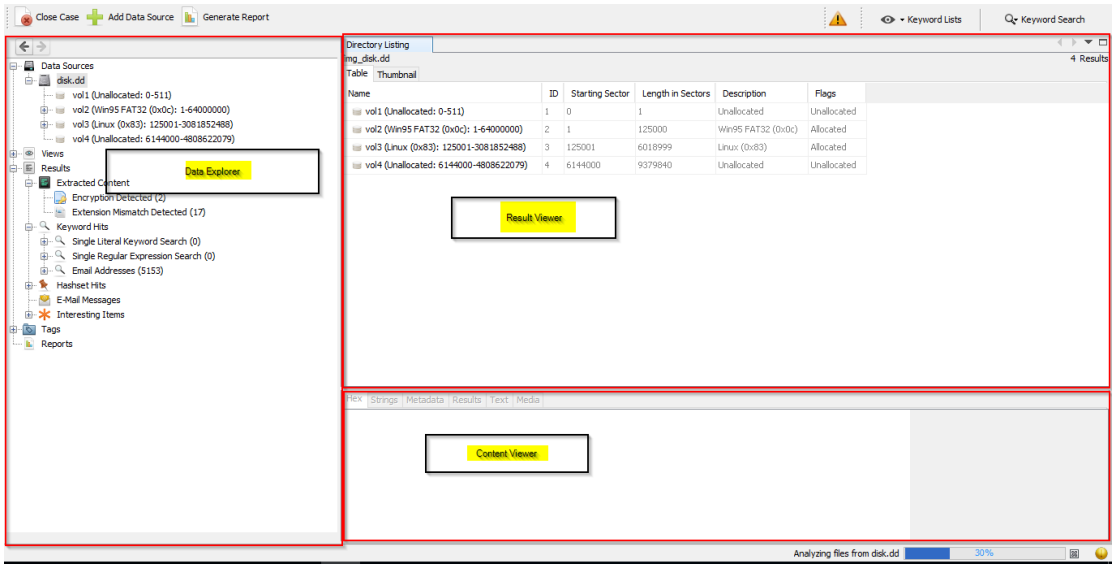
Για να διαμορφώσουμε τις μεθόδους της διαδικασίας Ingest **(Configure Ingest Modules)** κάνουμε τα εξής:

1. Επιλέγουμε τις **μεθόδους (modules)** που χρειαζόμαστε για την ανάλυση των περιεχομένων της εικόνας (image)
2. Επιλέγουμε το **κουμπί Next**. Το παράθυρο Add Data Source ενημερώνεται .Η διαδικασία Ingest ξεκινάει.
3. Επιλέγουμε το **κουμπί Finish**.

Το Autopsy ξεκινάει την ανάλυση των περιεχομένων της εικόνας δίσκου(Disk Image). Μπορούμε να παρακολουθήσουμε την πρόοδο της διαδικασίας από την μπάρα που βρίσκεται κάτω δεξιά στο κύριο παράθυρο .

Εικόνα 47 Πρόοδος της διαδικασίας Ingest

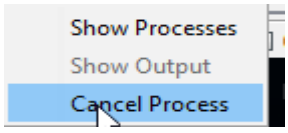
Το **κύριο παράθυρο** του Autopsy έχει χωρίζεται σε τρείς περιοχές:



Εικόνα 48 Κύριο Παράθυρο Autopsy

1. Εξερευνητής δεδομένων -Data Explorer
2. Αποτελέσματα -Result Viewer
3. Περιεχόμενα -Content Viewer

Εάν η διαδικασία Ingest διαρκεί μεγάλο χρονικό διάστημα μπορούμε να την ακυρώσουμε και να την επανεκκινήσουμε με νέα επιλογή μεθόδων.

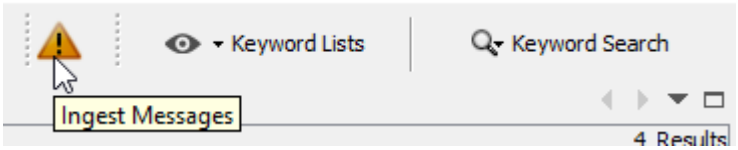


Η **ακύρωση της διαδικασίας Ingest** γίνεται με δεξί κλικ επί της μπάρας προόδου .

Εικόνα 49 Ακύρωση Ingest

Τέλος το Autopsy μας ενημερώνει με **μηνύματα** για την διαδικασία **Ingest.**

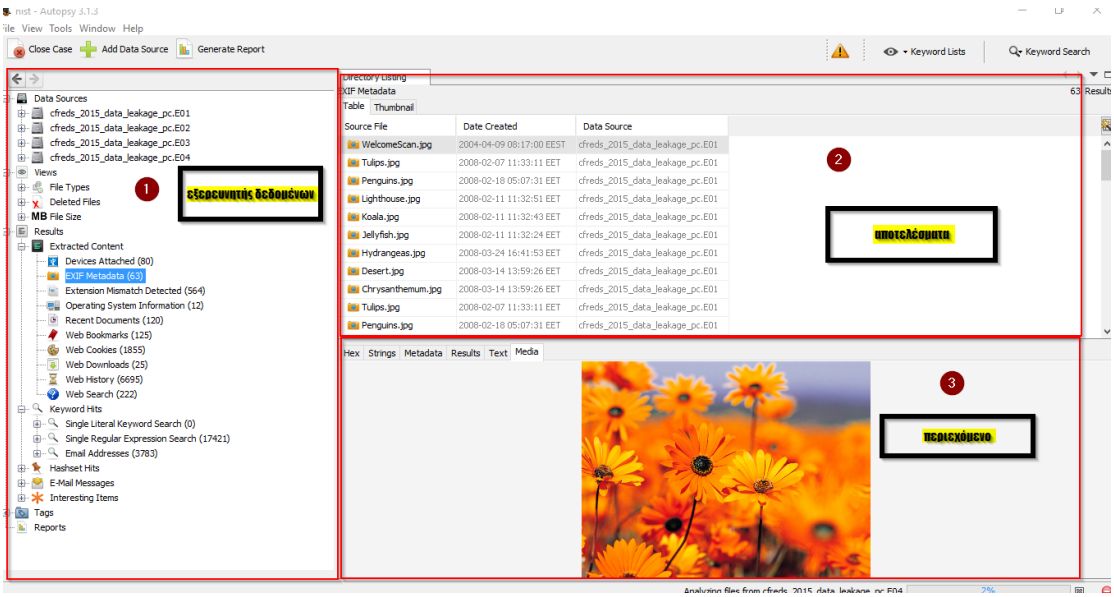
Εικόνα 50 Μηνύματα Ingest



4.3 Περιήγηση στη Ανάλυση Δεδομένων

Αφού ξεκινήσει η διαδικασία Ingest ,μπορούμε να χρησιμοποιήσουμε την διεπαφή του Autopsy ,για να εξερευνήσουμε τα αναλυμένα δεδομένα. Η διεπαφή χωρίζεται στις ακόλουθες «περιοχές» (τομείς):

1. Εξερευνητής Δεδομένων(Data explorer)
2. Αποτελέσματα (Result Viewer)
3. Περιεχόμενα (Content Viewer)



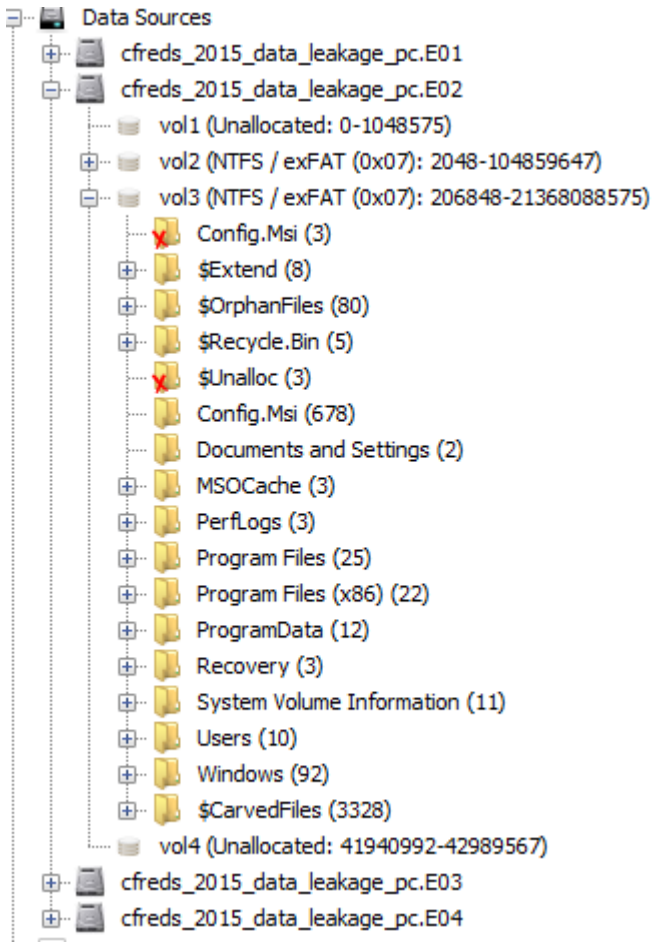
Εικόνα 51 Τριχοτόμηση του Autopsy

4.3.1 Χρήση του Εξερευνητή Δεδομένων

Όπως η διαδικασία Ingest τρέχει , κατηγοριοποιεί τα δεδομένα της εικόνας δίσκου. Ο **εξερευνητής δεδομένων (Data Explorer)** παρουσιάζει τα αποτελέσματα σε δενδρική μορφή .

Ο εξερευνητής δεδομένων χωρίζεται στα ακόλουθα τμήματα:

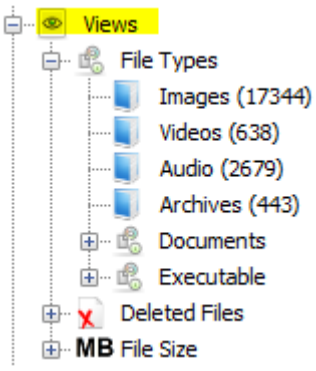
- **Τμήμα Πηγών δεδομένων (Data Sources)**:



Εικόνα 52 Data Sources

Δείχνει τα περιεχόμενα της εικόνας δίσκου (Disk Image) σε μορφοποίηση Windows Explorer.

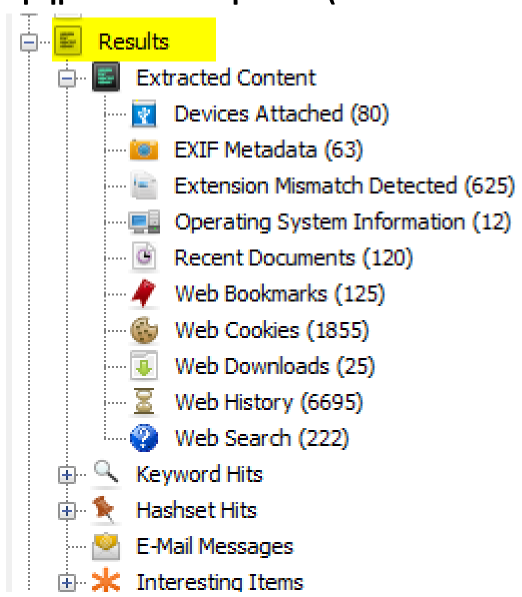
- **Τμήμα «Όψης» (Views section)**:



Εικόνα 53 View Section

Δείχνει τα αρχεία τα οποία το Autopsy τα έχει κατηγοριοποιήσει βάση των μεταδεδομένων (metadata) τους.

- **Τμήμα Αποτελεσμάτων (Results section)** :

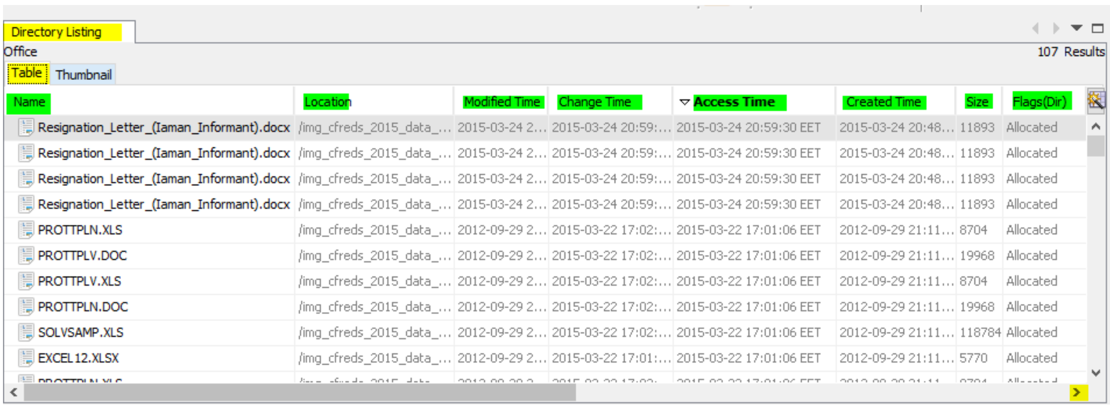


Εικόνα 54 Results Section

Μας παρουσιάζει τα δεδομένα που πρόεκυψαν κατά την διαδικασία Ingest .

4.3.2 Χρήση των Αποτελεσμάτων

Όταν επιλέγουμε ένα αντικείμενο στο εξερευνητή δεδομένων (Data Explorer) τα αποτελέσματα παρουσιάζονται δεξιά στο κύριο παράθυρο του Autopsy.Μπορούμε να παρουσιάσουμε αρχεία διαφορετικών μορφοποιήσεων .



Εικόνα 55 Result Viewer

Οι ιδιότητες που παρουσιάζονται για κάθε αρχείο είναι οι ακόλουθες:

- Όνομα
- Ώρα

- Μέγεθος
- Mode
- UID
- GID
- Μεταδεδομένα

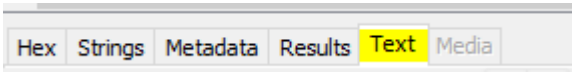
Στην περίπτωση που στο εξερευνητή δεδομένων (Data Explorer) εντοπίσουμε φάκελο με γραφικές εικόνες μπορούμε να δούμε μικρογραφία αυτών μέσω του **Thumbnail view** .Το Autopsy αναγνωρίζει γραφικές εικόνες με μορφοποίηση JPG, PNG ,GIF .

Εικόνα 56 Τμήμα Αποτελεσμάτων Μικρογραφίες

4.3.3 Προβολή των Περιεχομένων Αρχείου

Στον τομέα «Αποτελέσματα» του κύριου παραθύρου του Autopsy μπορούμε να δούμε τα περιεχόμενα του αρχείου σε διάφορες μορφές . Οι επιλογές που έχουμε είναι οι ακόλουθες:

- **Κουμπί Προβολής Κειμένου :**

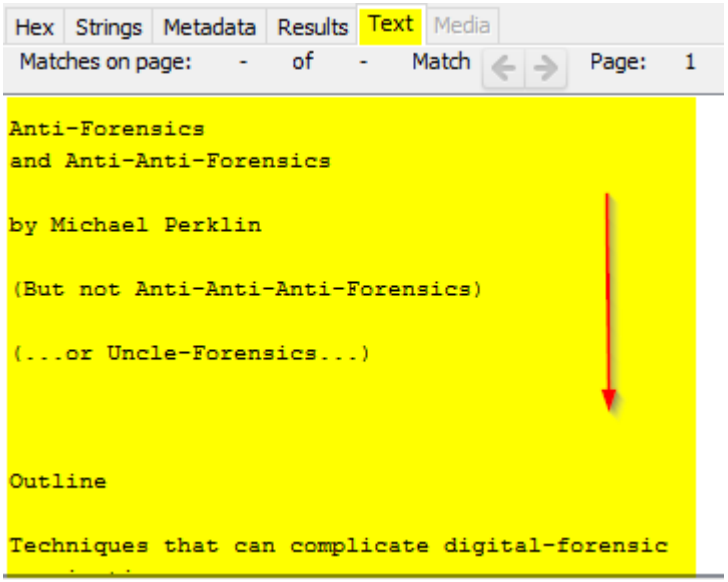


Εικόνα 57 Text View

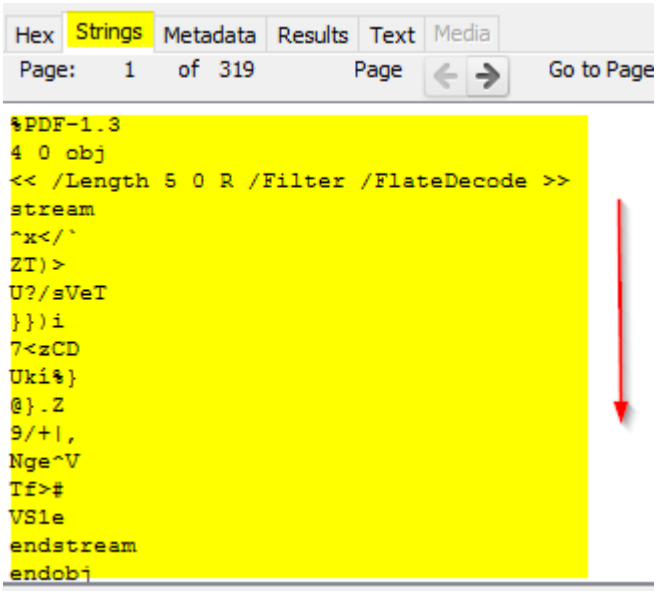
Η μέθοδος της Αναζήτησης Λέξης-Κλειδιού (Keyword Search) της διαδικασίας Ingest δημιουργεί ένα ευρετήριο από λέξεις που αναγνωρίστηκαν στα αρχεία της εικόνας δίσκου . Εάν κατά την διαδικασία Ingest επιλέξαμε την μέθοδο αναζήτησης λέξεων , μπορούμε να δούμε τα αποτελέσματα της για οποιοδήποτε αρχείο επιλέγοντας το κουμπί προβολής κειμένου (Text View).

Η επιλογή ανάμεσα στην προβολή κειμένου (Text View) και την προβολή αλφαριθμητικού (String View) , παρέχει διαφορετικά αποτελέσματα . Διότι η προβολή αλφαριθμητικού (String View) αναζητάει δεδομένα που μπορεί και να μην είναι κείμενο.

Την διαφορά των δύο αυτών επιλογών μπορούμε να την καταλάβουμε με ένα παράδειγμα. Έστω ότι το αρχείο που μας ενδιαφέρει είναι pdf. Η προβολή κειμένου θα μας παρουσιάσει με τρόπο κατανοητό το αρχείο μας , ενώ η προβολή αλφαριθμητικού θα μας παρουσιάσει μόνο συμβολοσειρές.

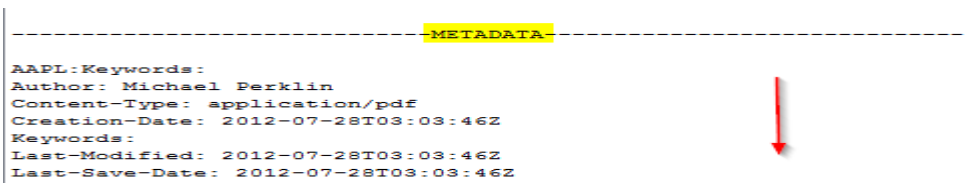


Εικόνα 58 Text View PDF



Εικόνα 59 String View PDF

Η προβολή κειμένου στο τέλος μας παρουσιάζει τα **μεταδεδομένα**:



Εικόνα 60 Metadata Text View PDF

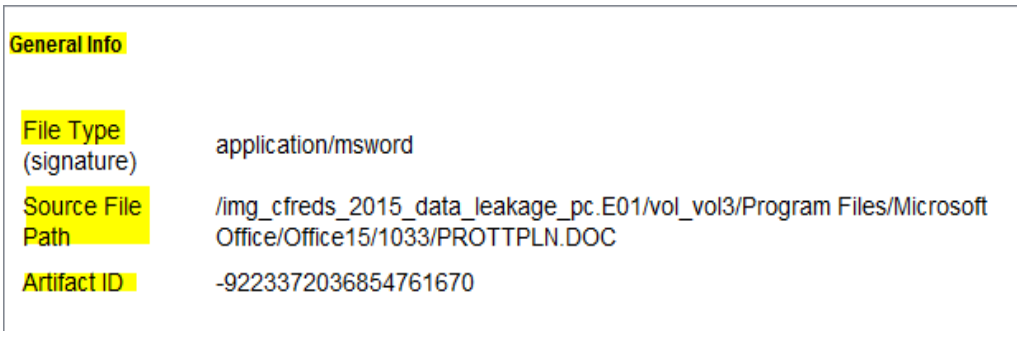
Σε περίπτωση που δεν μπορούμε να επιλέξουμε την προβολή κειμένου (Text View) τότε ισχύουν τα εξής:

- Το αρχείο δεν έχει μορφοποίηση κειμένου
- Δεν επιλέξαμε την μέθοδο αναζήτησης λέξης όταν παραμετροποιήσαμε την διαδικασία Ingest

- **Κουμπί Προβολής Αποτελεσμάτων:**

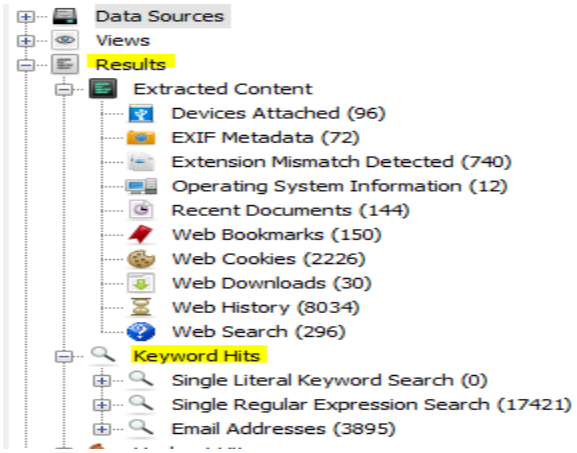
Εικόνα 61 Result View

Η προβολή αποτελεσμάτων μας παρουσιάζει τις ιδιότητες του αρχείου.



Εικόνα 62 Προβολή Αποτελεσμάτων για αρχείο msword

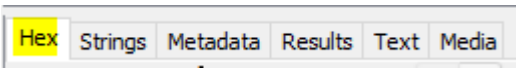
η προβολή αποτελεσμάτων είναι διαθέσιμη για τμήμα αποτελεσμάτων (Results) και για τμήμα λέξεων-κλειδιών (Keyword Hits) του Εξερευνητή Αρχείων (Data Explorer).



Εικόνα 63 Results Keyword Hits

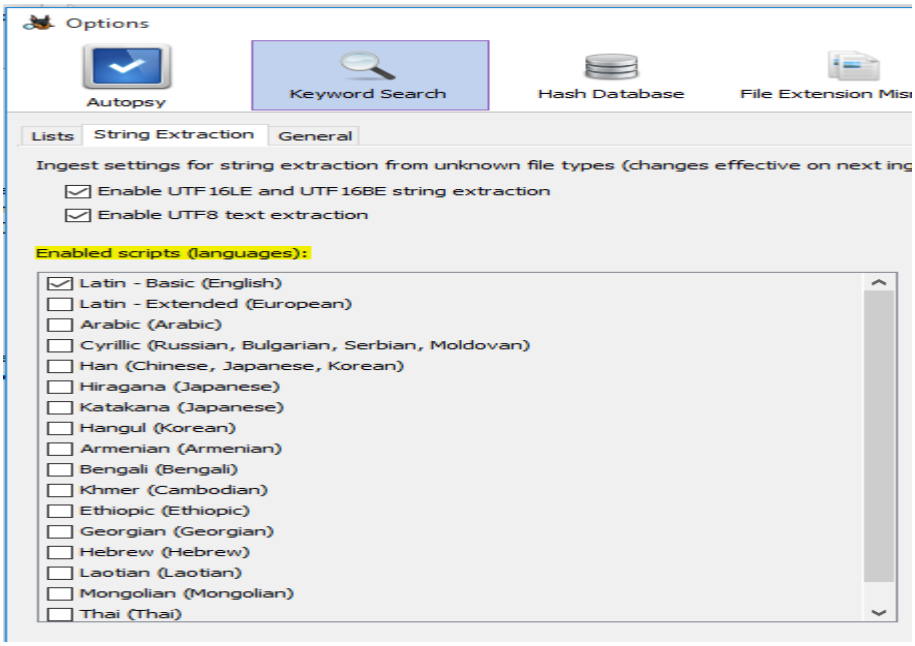
Τέλος για τα **μηνύματα ηλεκτρονικού** ταχυδρομείου είναι η καλύτερη επιλογή.

- **Κουμπί Προβολής Συμβολοσειρών :**



Εικόνα 64 String View

Η προβολή συμβολοσειρών παρουσιάζει όλες τις πιθανές συμβολοσειρές του αρχείου . Οι συμβολοσειρές μπορεί να είναι σε binary format .Η προεπιλεγμένη γλώσσα είναι τα Αγγλικά . Για αλλαγή γλώσσας επιλέγουμε από το μενού Tools (εργαλεία) και μετά το Options (επιλογές).

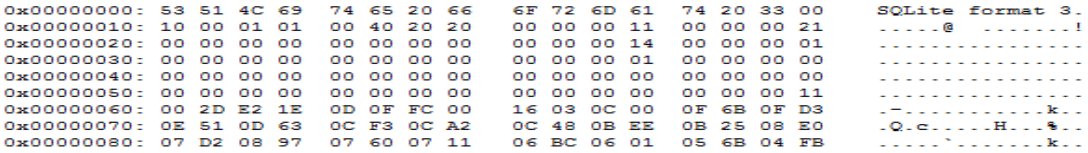


Εικόνα 65 Επιλογή γλώσσας

- **Κουμπί Δεκαεξαδικής Προβολής** :

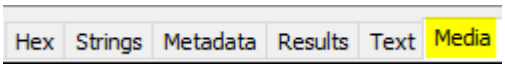
Εικόνα 66 Hex View

Η δεκαεξαδική προβολή παρουσιάζει τα περιεχόμενα ενός αρχείου ακατέργαστα . Τα δεδομένα του αρχείου αναπαρίστανται σε δεκαεξαδικές τιμές . Ομαδοποιούνται σε δυο ομάδες των 8 bytes , που ακολουθείται από μια ομάδα των 16 ASCII χαρακτήρων . Οι χαρακτήρες ASCII απαιτούν παραπάνω από ένα character space αντιπροσωπεύονται από μια (.) τελεία .



Εικόνα 67 Δεκαεξαδική Προβολή Αρχείου

- **Κουμπί Προβολής Εικόνων και Βίντεο :**



Εικόνα 68 Media View

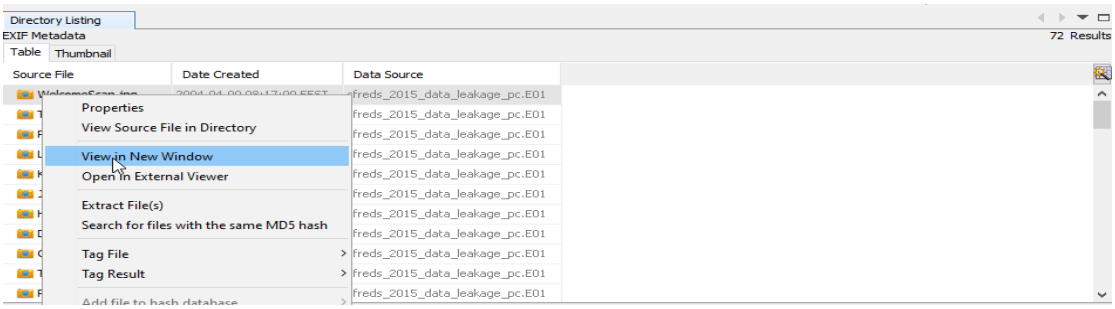
Η επιλογή αύτη είναι διαθέσιμη μόνο για τα ακόλουθα:

- Εικόνες (JPEG, GIF ,PNG)
- Ήχους
- Βίντεο

Εάν το αρχείο δεν υποστηρίζεται από το Autopsy ή εάν επιθυμούμε περεταίρω ανάλυση μπορούμε να εξάγουμε το αρχείο σε πρόγραμμα της αρεσκείας μας.

- **Προβολή Περιεχομένων Αρχείου σε Νέο Παράθυρο** :

Κάνουμε δεξί κλικ στο αρχείο που παρουσιάζεται στο τμήμα Αποτελεσμάτων και επιλέγουμε «Προβολή σε Νέο Παράθυρο»(View in New Window).

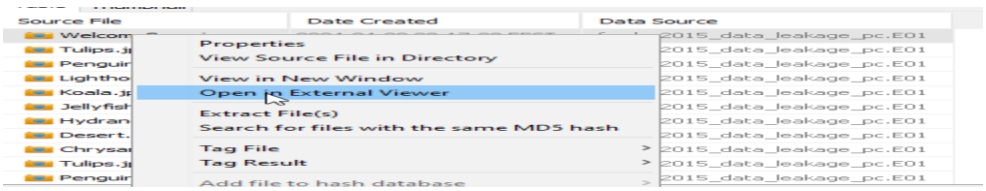


Εικόνα 69 Προβολή σε Νέο Παράθυρο

Το αποτέλεσμα της ενέργειας μας είναι να ανοίξει ένα νέο παράθυρο βάση του οποίου μπορούμε να ερευνήσουμε τα περιεχόμενα του αρχείου .

- **Προβολή του Αρχείου με χρήση Εξωτερικών Προγραμμάτων :**

Κάνουμε δεξί κλικ στο αρχείο και επιλέγουμε «Άνοιγμα σε Εξωτερική Προβολή»(Open in External View) .



Εικόνα 70 Προβολή με Εξωτερικό Πρόγραμμα

Πχ: εάν το αρχείο είναι ένα Word έγγραφο επιλέγουμε να το ανοίξουμε με το Word Office .

4.4 Αναζήτηση Περιεχομένων Αρχείου

Μπορούμε να αναζητήσουμε στα αρχεία της εικόνας δίσκου (disk image) συγκεκριμένες λέξεις κλειδιά (specific keywords) . Οι λέξεις αυτές διακρίνονται σε :

- Συμβολοσειρές(strings)
- Κανονικές εκφράσεις (regular expressions)

Εάν κατά την διάρκεια της αναζήτησης μας προκύψουν χρήσιμα αποτελέσματα για την ερευνά μας μπορούμε να αποθηκεύσουμε την φυσική θέση αυτών των αρχείων.

4.4.1 Αναζήτηση Προκατασκευασμένων Λέξεων Κλειδιών

Το εργαλείο Autopsy συμπεριλαμβάνει λέξεις κλειδιά που μας επιτρέπουν να αναζητήσουμε τα ακόλουθα :

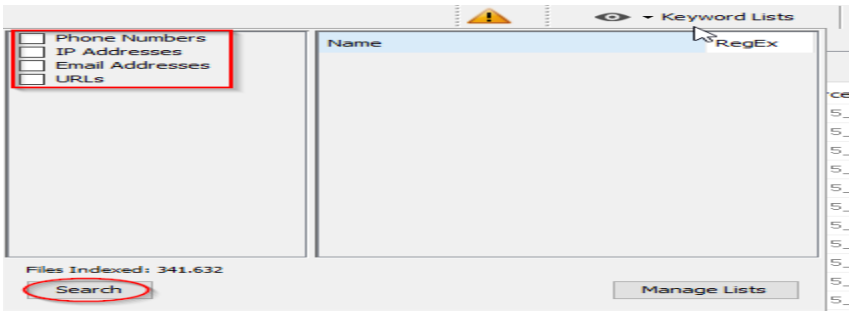
- URLs
- IP Διευθύνσεις
- Email Διευθύνσεις
- Τηλεφωνικούς Αριθμούς(phone numbers)

Για να υλοποιήσουμε μια αναζήτηση βάση των παραπάνω εκφράσεων , πρέπει κατά την διάρκεια εκκίνησης της διαδικασίας Ingest η μέθοδος «Αναζήτηση Λέξεων – Κλειδιών » (Keyword Search) να έχει επιλεγεί . Σε περίπτωση που δεν την επιλέξουμε επανεκκινούμε την διαδικασία Ingest έχοντας επιλέξει την μέθοδο Keyword Search .

Αυτού του είδους η αναζήτηση μπορεί να εξάγει πάρα πολλά αποτελέσματα , μέσα στα οποία να υπάρχουν αρκετά «σκουπίδια».

Αναζήτηση με βάση τις υπάρχουσες λέξεις κλειδιά :

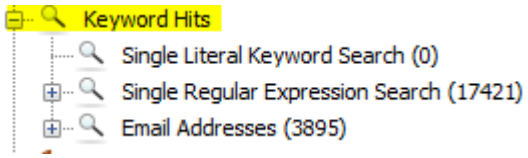
1. Στην μπάρα πάνω δεξιά επιλέγουμε το Keyword Lists και εμφανίζεται το ακόλουθο παράθυρο:



Εικόνα 71 KeyWordList Window

2. Επιλέγουμε τα κουτιά που μας ενδιαφέρουν και κάνουμε κλικ στο κουμπί Search

Τα αποτελέσματα της αναζήτησης εμφανίζονται στον Εξερευνητή Δεδομένων (Data Explorer)



Εικόνα 72 KeyWord Hits

4.4.2 Δημιουργία και Διαχείριση Λίστας Λέξεων Κλειδιών

Η μέθοδος KeyWord Search της διαδικασίας Ingest χρησιμοποιεί την λίστα λέξεων κλειδιών όταν το Autopsy αναλύει τα περιεχόμενα της εικόνας δίσκου .Εάν προσθέσουμε νέες λέξεις κλειδιά στην λίστα , πρέπει να επανεκκινήσουμε την διαδικασία Ingest . Εκ τότε το Autopsy χρησιμοποιεί για όλες τις υποθέσεις τις λέξεις κλειδιά που συμπεριλάβε στην λίστα.

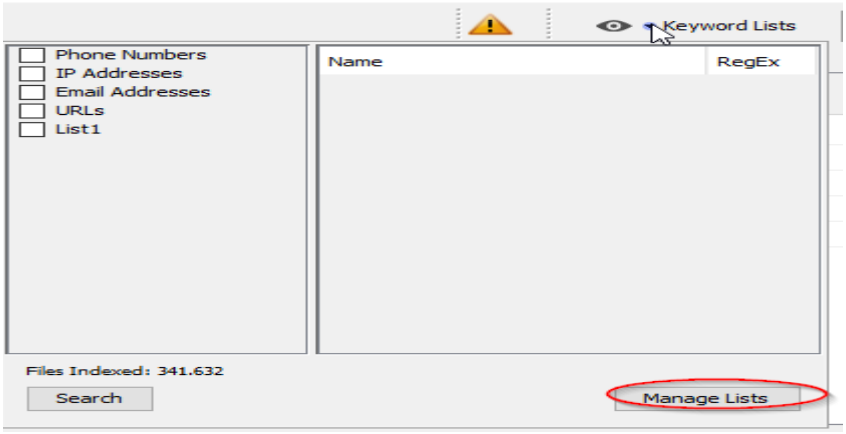
Η λίστα μπορεί να περιέχει τα ακόλουθα:

1. Κανονικές εκφράσεις(regular expressions)
2. Απλά αλφαριθμητικά (strings)

Οι κανονικές εκφράσεις είναι μια συλλογή ειδικών χαρακτήρων που μας επιτρέπουν να τα ταυτίζουμε με ένα σύνολο από αλφαριθμητικά (strings).Παράδειγμα κανονικών εκφράσεων είναι οι υπάρχουσες αναζητήσεις για τις IP και τα URL. Το Autopsy χρησιμοποιεί την σύνταξη της JAVA για τις κανονικές εκφράσεις.

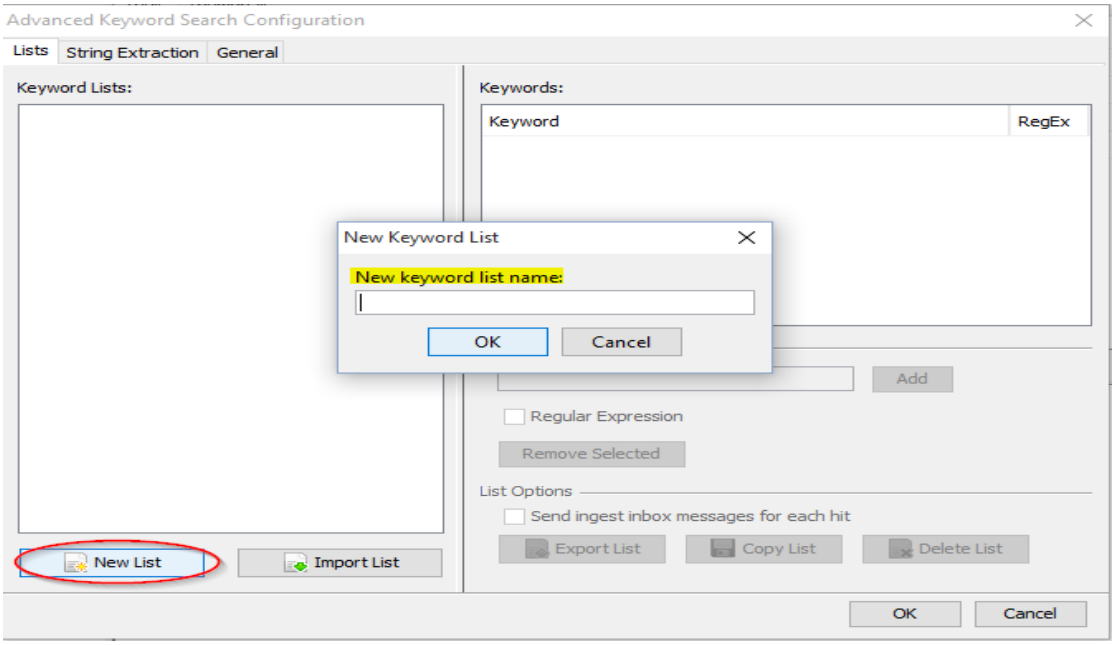
Δημιουργία μιας λίστας λέξεων κλειδιών:

1. Επιλέγουμε δεξιά επάνω το Keyword Lists



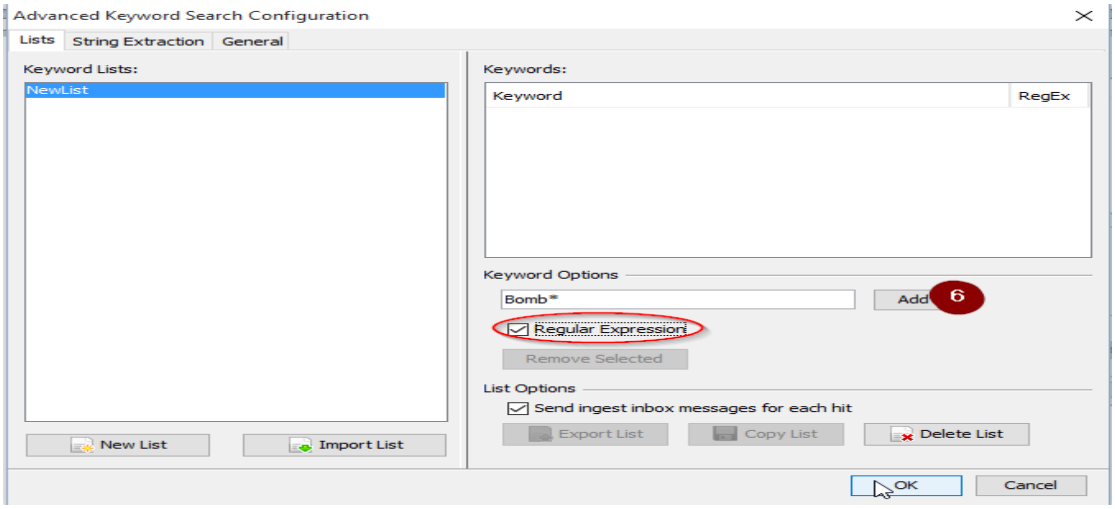
Εικόνα 73 Keyword List Manage Lists

2. Κάνουμε κλικκ στο Manage Lists . Σαν αποτέλεσμα εμφανίζεται το παράθυρο «Διαμόρφωσης Σύνθετης Αναζήτησης Λέξεων Κλειδιών » (Advanced Keyword Search Configuration)



Εικόνα 74 Advanced Keyword Search Configuration

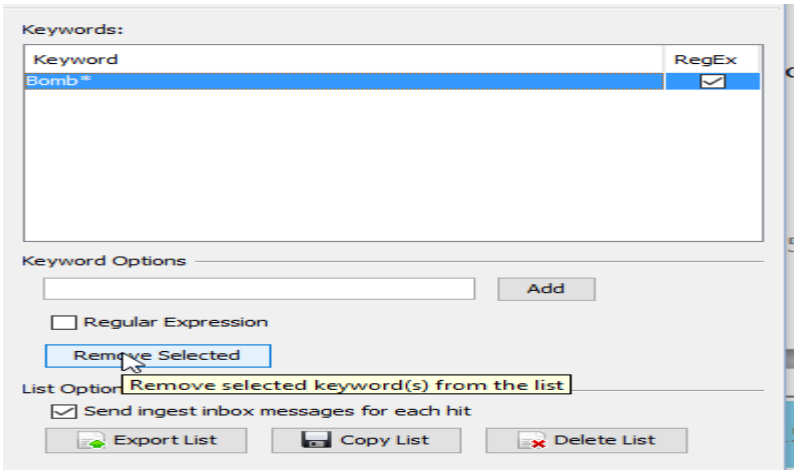
3. Στην αριστερή πλευρά του παραθύρου κάνουμε κλικ στο «New List»
4. Εμφανίζεται ένα κουτί με όνομα «New Keyword List» . Εισάγουμε ένα περιγραφικό όνομα για την λίστα και επιλέγουμε «OK» . Το όνομα της λίστας εμφανίζεται στην αριστερή στήλη Keyword Lists .



Εικόνα 75 Keyword Options

5. Επιλέγουμε στην αριστερή στήλη την λίστα(πχ NewList Εικόνα 75) .Στο πεδίο Keyword Options εισάγουμε την λέξη κλειδί ή την κανονική έκφραση που θέλουμε να αναζητήσουμε . Εάν θέλουμε κανονική έκφραση πρέπει να επιλέξουμε το κουτί «Regular Expression».

6. Επιλέγουμε το «Add» . Η λέξη κλειδί εμφανίζεται στην δεξιά στήλη του παραθύρου

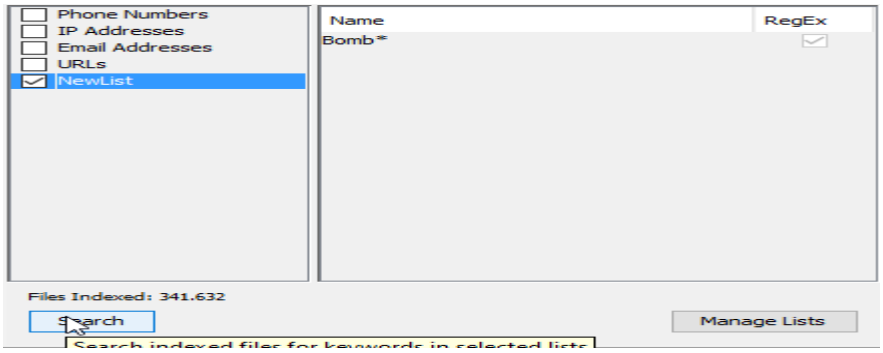


Εικόνα 76 Remove Selected Keyword

7. Μπορούμε να εισάγουμε όσες λέξεις κλειδιά θέλουμε στην λίστα . Όταν τελειώσουμε πατάμε «ΟΚ».

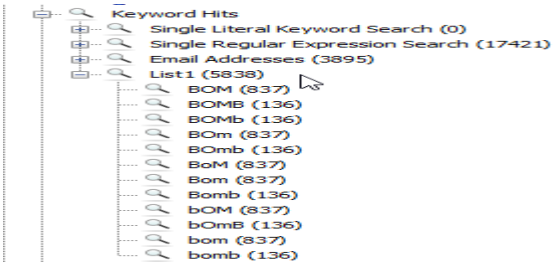
Αναζήτηση λέξης κλειδί με την χρήση λίστας :

1. Επιλέγουμε δεξιά επάνω το Keyword Lists
2. Στο παράθυρο που εμφανίζεται επιλέγουμε το όνομα της λίστας που μας ενδιαφέρει και πατάμε το Search.



Εικόνα 77 Search Keyword List

Τα αποτελέσματα εμφανίζονται στο «Εξερευνητή Δεδομένων» (Data Explorer).



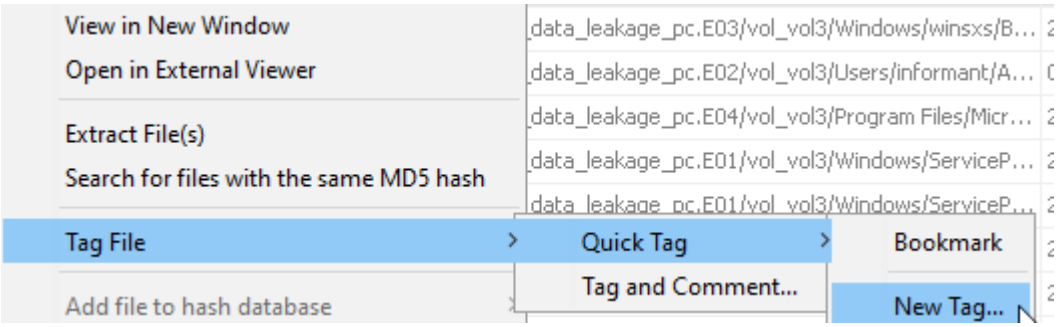
Εικόνα 78 Results NewList

4.4.3 Αποθήκευση Τοποθεσίας Αρχείων

Μπορούμε να αποθηκεύσουμε τις τοποθεσίες αρχείων οποιουδήποτε αρχείου βλέπουμε στο Result Viewer . Αφού κάνουμε μια αναζήτηση μιας λέξης κλειδί , μπορεί να επιθυμούμε να σώσουμε την θέση του αρχείου. Το Autopsy χρησιμοποιεί ετικέτες (tags) .Αφού δημιουργήσουμε την ετικέτα , μπορούμε να την συνδέσουμε με το αρχείο .

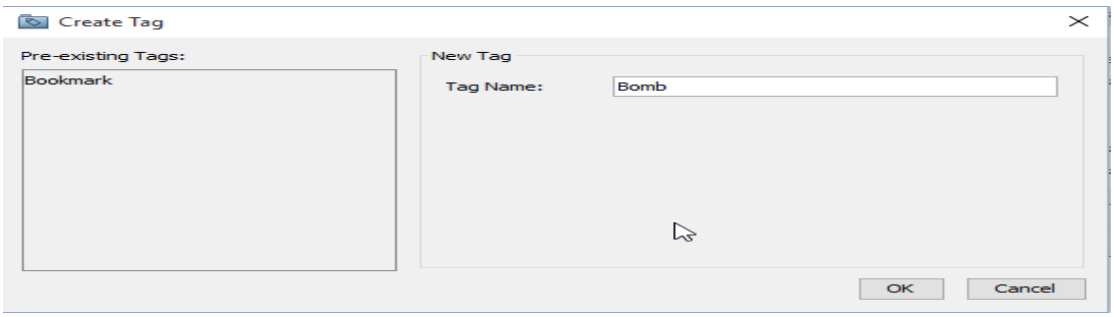
Δημιουργία μιας Λίστας Ετικετών :

1. Στο κεντρικό παράθυρο πάνω δεξιά επιλέγουμε το KeyWord Search.
2. Στο αρχείο που μας ενδιαφέρει κάνουμε δεξί κλικ και επιλέγουμε το «Tag File» και κάνουμε κλικ στο «New Tag»



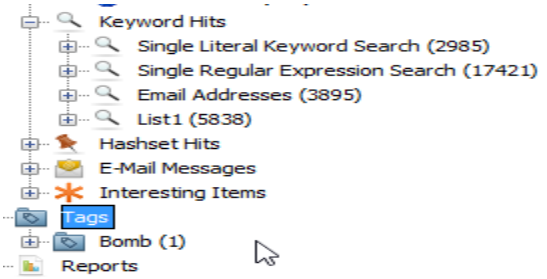
Εικόνα 79 New Tag

Τότε εμφανίζεται το παράθυρο «Δημιουργία Ετικέτας»



Εικόνα 80 Create Tag

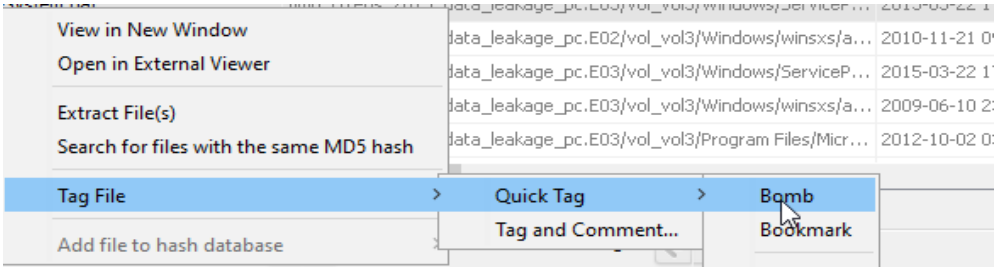
3. Στο πεδίο Tag Name εισάγουμε ένα περιγραφικό όνομα για ετικέτα . Η ετικέτα εμφανίζεται στο Εξερευνητή Δεδομένων.



Εικόνα 81 Data Explorer Tag Name

Προσθήκη ενός αρχείου σε συγκεκριμένη ετικέτα:

1. Στο Result Viewer κάνουμε δεξί κλικ στο αρχείο που θέλουμε να προσθέσουμε σε μια ετικέτα



Εικόνα 82 Add file to the tag

2. Για να δούμε τα αρχεία που προσθέσαμε σε μια ετικέτα επιλέγουμε το όνομα της ετικέτας στον Data Explorer. Η λίστα των αρχείων που έχουν συνδεθεί με την ετικέτα εμφανίζονται και στο Result Viewer.

Εικόνα 83 Result Viewer Tag Files

4.5 Δημιουργία Αναφορών

Το Autopsy μας παρέχει την δυνατότητα δημιουργίας **Αναφορών (Reports)** για τα δεδομένα που έχουμε αναλύσει.

Η αναφορά μπορεί να λάβει μια από τις ακόλουθες μορφοποιήσεις :

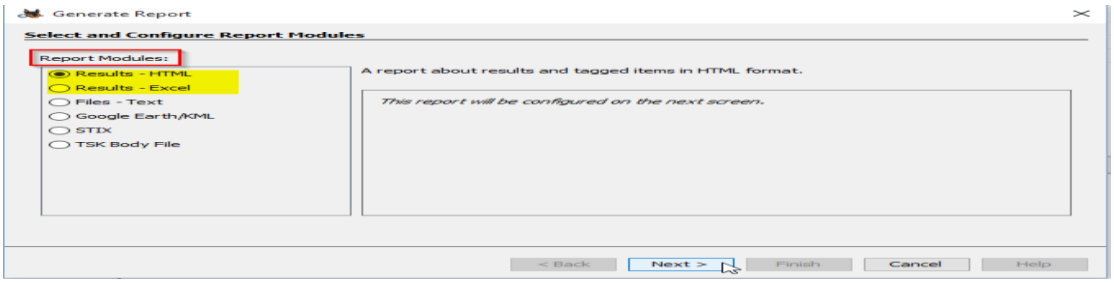
1. HTML Format
2. EXCEL Format

4.5.1 Δημιουργία Βασικής Αναφοράς

Η βασική αναφορά περιλαμβάνει προκαθορισμένες επιλογές .Εμείς καλούμαστε να επιλέξουμε την μορφοποίηση της αναφοράς (HTML or EXCEL).

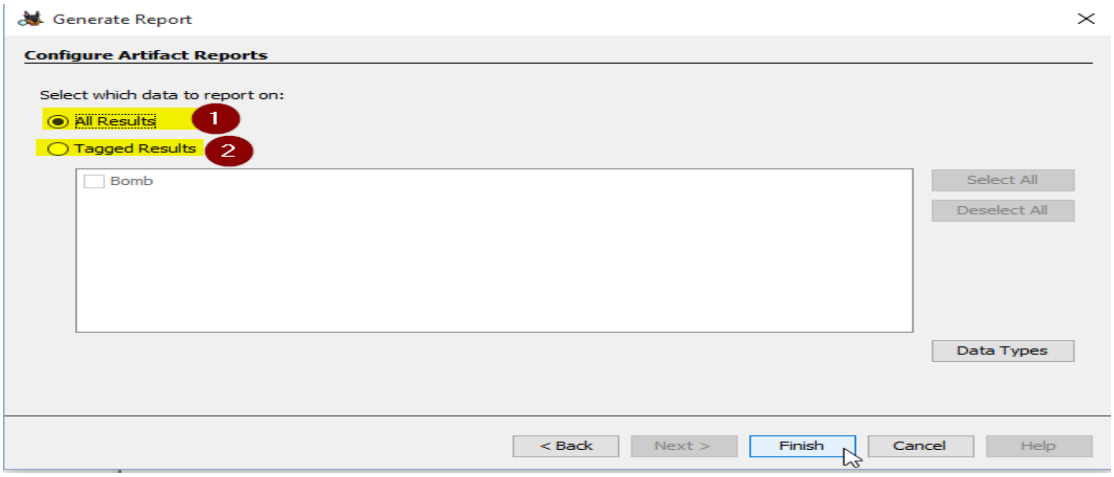
Δημιουργία Βασικής Αναφοράς:

1. Επιλέγουμε από το κεντρικό παράθυρο στην γραμμή εργαλείων το General **Report**



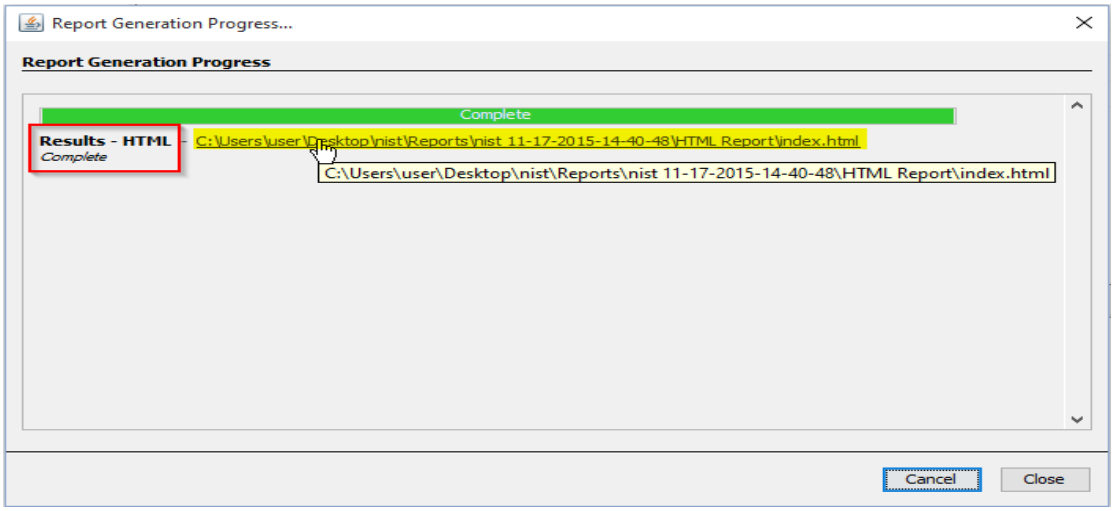
Εικόνα 84 General Report

2. Επιλέγουμε τον τύπο της αναφοράς που επιθυμούμε να παράγουμε και κάνουμε κλικ στο Next . Το παράθυρο ανανεώνεται και μας ζητάει να επιλέξουμε εάν θέλουμε αναφορά για όλα τα δεδομένα ή για κάποια συγκεκριμένα (ετικέτες κλπ)



Εικόνα 85 All results / Tagged Results

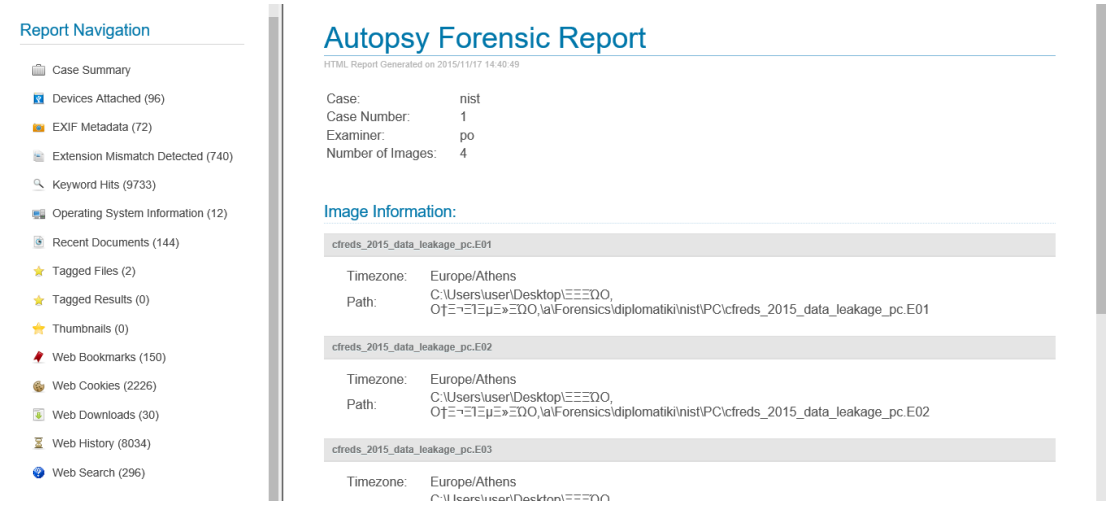
3. Για να ολοκληρώσουμε την δημιουργία αναφοράς επιλέγουμε το Finish . Εμφανίζεται το παράθυρο Report Generation Process που μας δείχνει την διεργασία παραγωγής της αναφοράς.



Εικόνα 86 Report Generation Process

Με την ολοκλήρωση της παραπάνω διαδικασίας το Autopsy μας παρέχει σύνδεσμο (link) για την αναφορά.

4. Για να δούμε την αναφορά κάνουμε κλικ στον σύνδεσμο . Ο περιηγητής διαδικτύου μας παρουσιάζει την αναφορά . Σε περίπτωση που η μορφοποίηση της αναφοράς είναι EXCEL τότε ο σύνδεσμος ανοίγει την αναφορά με MS EXCEL.



Εικόνα 87 HTML Report

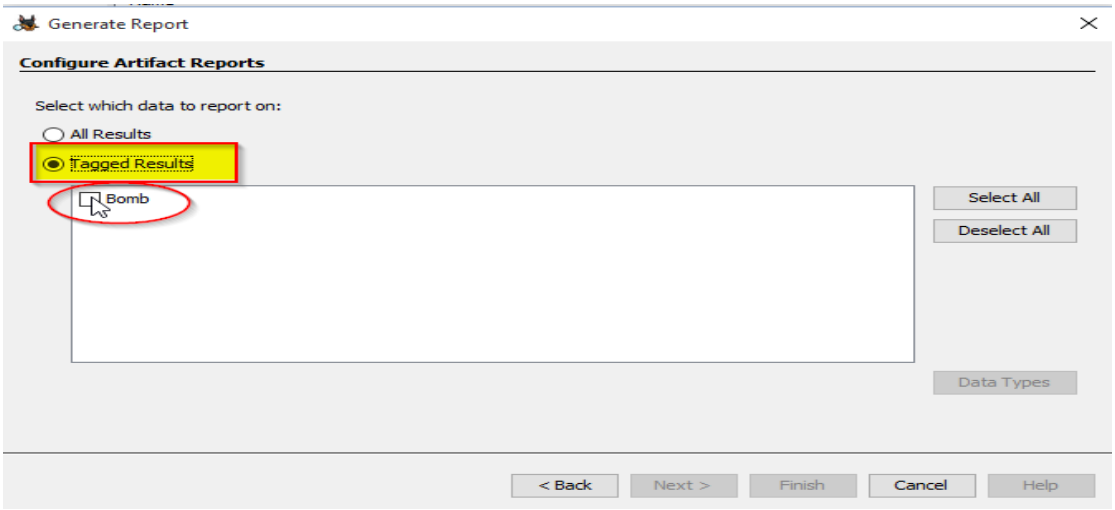
4.5.2 Δημιουργία Στοχευμένης Αναφοράς

Μπορούμε να δημιουργήσουμε δυο τύπους στοχευμένων αναφορών :

1. Αναφορά που περιέχει τα αρχεία που έχουν ετικέτες (tags)
2. Αναφορά που έχουμε επιλέξει τι δεδομένα θα περιέχει

Δημιουργία Αναφοράς για τις Ετικέτες:

1. Στην γραμμή εργαλείων επιλέγουμε το Generate Report
2. Επιλέγουμε το τύπο της αναφοράς και κάνουμε κλικ στο Next



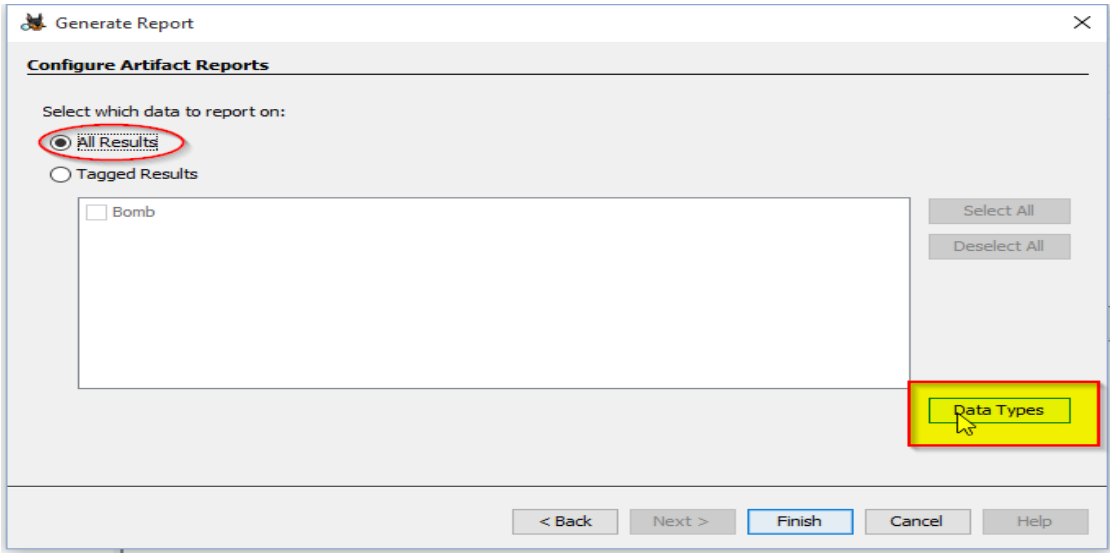
Εικόνα 88 Tagged Results

3. Για να δημιουργήσουμε μια αναφορά που περιέχει τα αρχεία με ετικέτα κάνουμε κλικ στο Tagged Results .Τα ονόματα των ετικετών γίνονται διαθέσιμα.

4. Επιλέγουμε το όνομα της ετικέτας για το οποίο επιθυμούμε να γίνει η αναφορά.

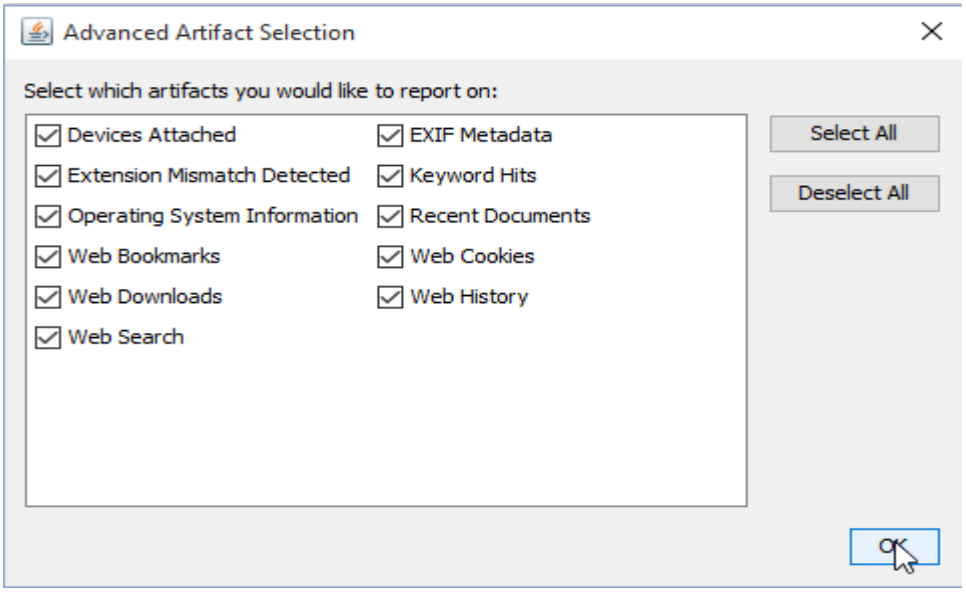
Δημιουργία Αναφοράς για Συγκεκριμένα Δεδομένα:

1. Επιλέγουμε από την γραμμή εργαλείων toGeneral Report
2. Επιλέγουμε τον τύπο της αναφοράς



Εικόνα 89 General Report Data Types

3. Επιλέγουμε το Data Types. Εμφανίζονται οι ακόλουθες επιλογές



Εικόνα 90 Data Types

4. Επιλέγουμε τι θέλουμε να περιέχει η αναφορά. Τα βήματα που ακολουθούν για την αναφορά είναι γνωστά.

4.6 Επιλογή Αρχείων για περαιτέρω Ανάλυση

Μπορούμε να εξάγουμε δεδομένα από την εικόνα ενός δίσκου για εξέταση τους εκτός του Autopsy . Μερικοί λόγοι που αιτιολογούν την παραπάνω δυνατότητα είναι οι ακόλουθοι

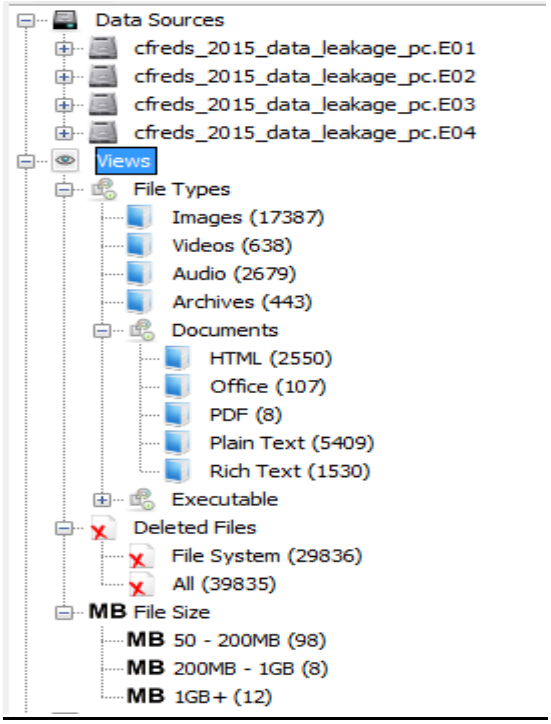
- Για ανάλυση δεδομένων με άλλα εργαλεία
- Επισύναψη δεδομένων σε αναφορά
- Εξέταση του unallocated space με άλλα εργαλεία

4.6.1 Εξαγωγή Αρχείων και Περιεχομένων Καταλόγων

Μπορούμε να εξάγουμε μεμονωμένα αρχεία και καταλόγους . Μπορεί να επιθυμούμε να εξάγουμε αρχεία που έχουν την ίδια ετικέτα (tag) , όπως MS Office ή όλα τα περιεχόμενα του καταλόγου Documents and Settings.

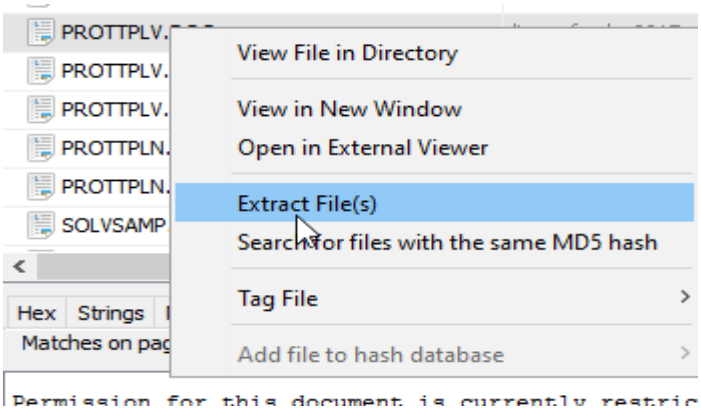
Εξαγωγή Αρχείων/Περιεχομένων καταλόγου:

1. Στον Εξερευνητή Αρχείων (Data Explorer) κάνουμε κλικ στο φάκελο ή το αρχείο που θέλουμε να εξάγουμε π.χ. Views



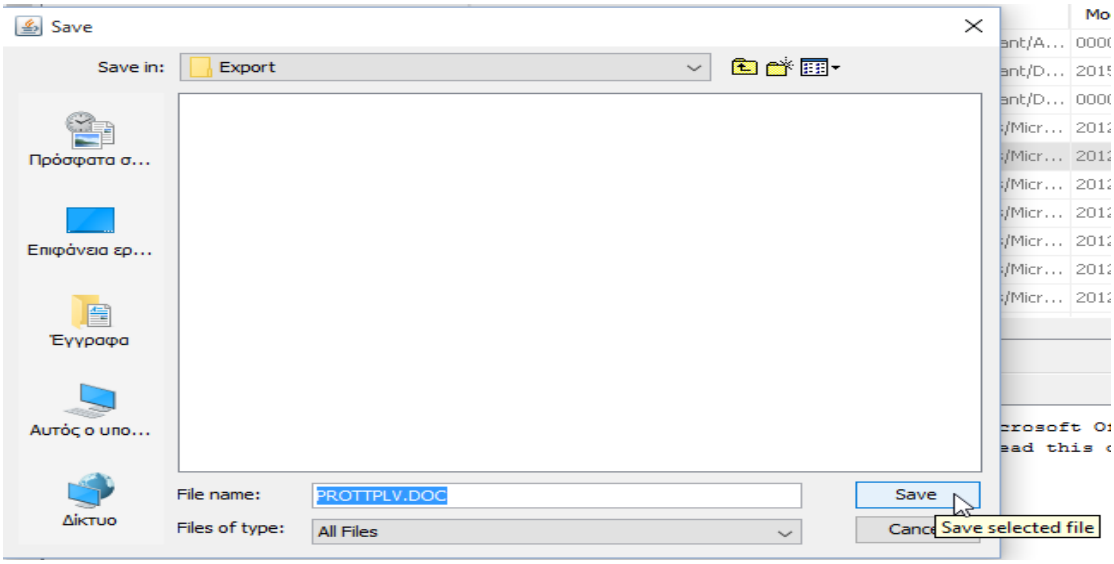
Εικόνα 91 Views

2. Στο παράθυρο Result Viewer , κάνουμε δεξί κλικ στο αρχείο που θέλουμε να εξάγουμε και επιλέγουμε το Extract File



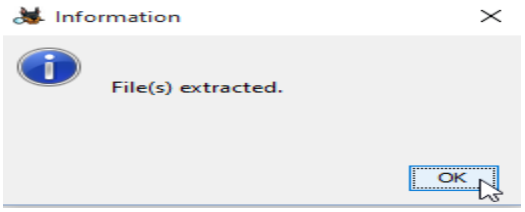
Εικόνα 92 Extract File Result Viewer

Εμφανίζεται ένα νέο παράθυρο που μας κατευθύνει στην αποθήκευση του αρχείου



Εικόνα 93 Save Directory

3. Επιλογή καταλόγου αποθήκευσης αρχείου
4. Στο πεδίο File Name εισάγουμε το όνομα που επιθυμούμε
5. Επιλέγουμε αποθήκευση (Save) και εμφανίζεται το ακόλουθο παράθυρο



Εικόνα 94 File Extracted

Με την επιλογή OK η εξαγωγή αρχείου έχει ολοκληρωθεί.

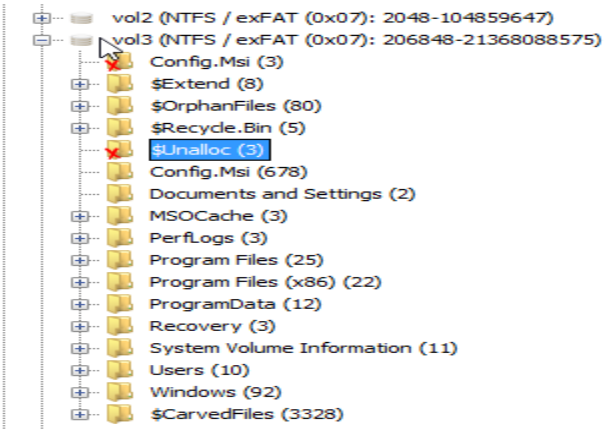
4.6.2 Εξαγωγή Unallocated Space

Ο ελεύθερος χώρος στον δίσκο περιέχει σκουπίδια από το σύστημα αρχείων που δεν χρησιμοποιούνται .Μπορεί να περιέχει διαγραμμένα αρχεία και άλλα σημαντικά στοιχεία για την έρευνα μας .

Η εξαγωγή του ελεύθερου χώρου μπορεί να γίνει με τα βήματα που ακολουθήσαμε πριν για την εξαγωγή ενός αρχείου ή μπορούμε να τον εξάγουμε ενιαίο.

Εξαγωγή ελεύθερου χώρου σαν μεμονωμένα block

1. Στον Εξερευνητή Αρχείων επιλέγουμε το Volume που μας ενδιαφέρει και κάνουμε κλικ στο κατάλογο $Unalloc

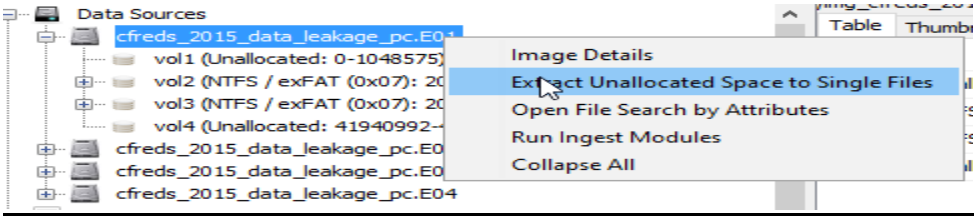


Εικόνα 95 $Unalloc

2. Εμφανίζεται στο Result Viewer η λίστα των αποτελεσμάτων .Μπορούμε να εξάγουμε το κάθε αρχείο μεμονωμένα με δεξί κλικ και επιλέγοντας το Extract File

Εξαγωγή ελεύθερου χώρου σαν ένα αρχείο

1. Στο Data Explorer κάτω από τον κατάλογο Data Sources κάνοντας κλικ στο όνομα της εικόνας επιλέγουμε το **Extract Unallocated to Single Files** .



Εικόνα 96 Image Extract Unallocated Space

2. Στην συνέχεια εμφανίζεται το παράθυρο που μας δίνει την δυνατότητα επιλογής του καταλόγου που θα γίνει η αποθήκευση .