# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών


## Μεταπτυχιακή Διατριβή
## Στην Ασφάλεια Υπολογιστών και Δικτύων

# Επισκόπηση Εργαλείων Οριστικής Διαγραφής Δεδομένων ως Αντι-Δικανική Μέθοδος


**Βασίλειος Βασιλείου**

**Επιβλέπων Καθηγητής**
**Δρ. Δημήτριος Μανιαδάκης**



**Μάιος 2023**

# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών


# Επισκόπηση Εργαλείων Οριστικής Διαγραφής Δεδομένων ως Αντι-Δικανική Μέθοδος


**Βασίλειος Βασιλείου**

**Επιβλέπων Καθηγητής**
**Δρ. Δημήτριος Μανιαδάκης**



Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

**Μάιος 2023**

# Περίληψη

Στη σύγχρονη ψηφιακή εποχή, το απόρρητο και η ασφάλεια των δεδομένων έχουν γίνει πιο κρίσιμα από ποτέ. Με την αύξηση των απειλών στον διαδίκτυο, των χάκερ και άλλων κακόβουλων παραγόντων, η ανάγκη για προστασία των ευαίσθητων πληροφοριών κρίνεται επιτακτική. Στο σημείο αυτό εισάγεται η έννοια των εργαλείων οριστικής διαγραφής που μπορούν να βοηθήσουν στην διαχείριση των δεδομένων που κρίνονται περιττά. Όπως λίγοι γνωρίζουν τα αρχεία που "διαγράφονται" παραμένουν στο μέσο αποθήκευσης μέχρι να αντικατασταθούν. Αυτό μπορεί να πάρει μέρες, μήνες ή ακόμη και χρόνια. Η διαγραφή αυτών των αρχείων απλώς καθιστά τον αποδεσμευμένο χώρο διαθέσιμο για χρήση. Ένα εργαλείο οριστικής διαγραφής αρχείων είναι ένα πρόγραμμα λογισμικού που έχει σχεδιαστεί για τη μόνιμη διαγραφή αρχείων από τον υπολογιστή ή άλλα μέσα αποθήκευσης. Σε αντίθεση με τις παραδοσιακές μεθόδους διαγραφής αρχείων, οι οποίες αφαιρούν μόνο την αναφορά στο αρχείο, αφήνοντας τα δεδομένα άθικτα στο δίσκο, τα εργαλεία οριστικής διαγραφής δεδομένων χρησιμοποιούν προηγμένους αλγόριθμους για να αντικαταστήσουν τα δεδομένα πολλές φορές, καθιστώντας ουσιαστικά αδύνατη την ανάκτηση τους.

Στόχος της παρούσας μεταπτυχιακής διατριβής είναι η διερεύνηση διαφόρων δημοφιλών εργαλείων οριστικής διαγραφής ως προς την ικανότητα τους για οριστική και αμετάκλητη διαγραφή αρχείων. Στο πλαίσιο αυτό εξετάζονται οι αλγόριθμοι που χρησιμοποιούν και κατά πόσο τα εργαλεία αυτά μπορούν να ανταπεξέλθουν σε σειρά δοκιμασιών που ετοιμάσαμε.

Για την επίτευξη των στόχων σχεδιάστηκε και υλοποιήθηκε κατάλληλη πειραματική διάταξη για να εξεταστούν σενάρια διαγραφής συγκεκριμένων αρχείων από το δίσκο ή ολόκληρου του δίσκου.

Τα αποτελέσματα που προκύπτουν είναι ποικίλα και δίνουν μια πρώτη αποτίμηση των δυνατοτήτων τους, καθώς αρκετά από τα εργαλεία αποδείχτηκαν αρκετά ικανά και διέγραψαν οριστικά τα δεδομένα. Συνεπώς, η χρήση εργαλείων οριστικής διαγραφής δεδομένων μπορεί να επηρεάσει σημαντικά μια δικανική εγκληματολογική έρευνα φέρνοντας τους ερευνητές σε αδιέξοδα. Ταυτόχρονα άλλα εργαλεία υπό εξέταση άφησαν τα δεδομένα άθικτα.

Σε κάθε περίπτωση, λόγω των πολλών μεταβλητών που υπάρχουν, η παρούσα διατριβή καταδεικνύει την ανάγκη για περεταίρω έρευνα με χρήση νέων παραμέτρων για εμπλουτισμό της υφιστάμενης γνώσης.

# Summary

In today's digital age, data privacy and security have become more critical than ever before. With the rise of cyber threats, hackers, and other malicious actors, it is essential to protect sensitive information from falling into the wrong hands. This is where a file shredder tool comes in handy. As few may know, the files that are "deleted" remain on the storage device until they are replaced. This action can take days, months or even years. Deleting these files simply makes the free space available for use. A permanent file shredder tool is a software program designed to permanently delete files from computers or other storage devices. Unlike traditional file deletion methods, which only remove the reference to the file, leaving the data still intact on the disk, file shredders use advanced algorithms to overwrite the data multiple times, making it virtually impossible to recover.

The aim of this master's dissertation is to investigate various popular permanent deletion tools in terms of their ability to delete files permanently and irreversibly. In this context, the algorithms they use are examined and whether these tools can cope with a series of tests that we have prepared.

To achieve the objectives, a suitable experimental setup was designed and implemented to examine scenarios of deleting specific files from a disk or the entire disk.

The results are varied and give a first assessment of their capabilities, as several of the tools proved to be quite capable of permanently erasing data. Therefore, the use of data erasure tools can significantly affect a forensic investigation by leading investigators to dead ends. At the same time, other tools under review left the data intact.

In any case, due to the many variables that exist, this dissertation demonstrates the need for further research using new parameters to enrich existing knowledge.

# Ευχαριστίες

Θερμές ευχαριστίες στον επιβλέποντα καθηγητή μου Δρ. Δημήτριο Μανιαδάκη για την αμέριστη βοήθεια και καθοδήγηση, καθώς και για την άψογη συνεργασία μεταξύ μας και το ενδιαφέρον του που έπαιξαν καθοριστικό ρόλο για την εκπόνηση της παρούσας μεταπτυχιακής διατριβής.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου για την υποστήριξη και την υπομονή τους καθ' όλη τη διάρκεια των σπουδών μου και κυρίως κατά το χρόνο συγγραφής της παρούσας διατριβής.

# Περιεχόμενα

# Κατάλογος Εικόνων

# Κατάλογος Πινάκων

# Κεφάλαιο 1
# Εισαγωγή

Στις μέρες μας η μαζική χρήση των υπολογιστών τόσο σε προσωπικό όσο και σε επαγγελματικό επίπεδο αποτελεί αδιαμφισβήτητο γεγονός. Η εκ σχεδιασμού λειτουργία των υπολογιστών και ευρύτερα των σύγχρονων υπολογιστικών συστημάτων προϋποθέτει την ύπαρξη αποθηκευτικών μέσων όπως σκληροί δίσκοι στους οποίους αποθηκεύεται τεράστιος όγκος δεδομένων και πληροφοριών. Τα δεδομένα αυτά συσσωρεύονται, επεξεργάζονται, τροποποιούνται διαμοιράζονται και εν τέλει αποθηκεύονται. Η αποθήκευση των δεδομένων αυτών έχει σκοπό να διασφαλίσει την απρόσκοπτή λειτουργία του υπολογιστή και την ευχάριστη εμπειρία του χρήστη.

Παράλληλα όμως η παρουσία στα αποθηκευτικά μέσα των δεδομένων αυτών εγείρει σημαντικά ζητήματα διαχείρισής τους στις περιπτώσεις όπου τα δεδομένα αυτά κρίνονται ευαίσθητα και κατάλληλα προς διαγραφή. Οι ενέργειες που εκτελούνται από το λειτουργικό σύστημα για την διαγραφή των δεδομένων περιορίζονται στην απελευθέρωση χώρου στο δίσκο, χωρίς να διασφαλίζεται ότι τα δεδομένα δεν μπορούν πλέον να ανακτηθούν αφού αυτό που συμβαίνει είναι το λειτουργικό σύστημα διαγράφει τους δείκτες προς τα διαγραμμένα αρχεία και ο χώρος που καταλαμβάνουν γίνεται πλέον διαθέσιμος για εγγραφή νέων δεδομένων. Μέχρι όμως να γίνει αυτό, τα δεδομένα παραμένουν αποθηκευμένα αναλλοίωτα και με τη χρήση συγκεκριμένων τεχνικών και τα κατάλληλα εργαλεία μπορούν να ανακτηθούν. Στο παρελθόν υπήρξαν πολλές

περιπτώσεις όπου σκληροί δίσκοι που περιείχαν ευαίσθητες πληροφορίες έπεσαν σε λάθος χέρια, οδηγώντας σε σοβαρές συνέπειες άτομα και οργανισμούς. Μερικές από τις σημαντικότερες περιπτώσεις διαρροής δεδομένων λόγω μη ασφαλούς διαγραφής σκληρών δίσκων είναι οι ακόλουθες:

1. National Health Service (NHS) England(Pinsent Masons, 2016)- Το 2016, επιβλήθηκε πρόστιμο 325.000 λιρών στο Εθνικό Σύστημα Υγείας της Αγγλίας μετά την κλοπή 74 μη κρυπτογραφημένων σκληρών δίσκων από τις εγκαταστάσεις μιας εταιρείας διαχείρισης δεδομένων. Οι σκληροί δίσκοι περιείχαν ευαίσθητα προσωπικά δεδομένα ασθενών, συμπεριλαμβανομένων των ιατρικών τους αρχείων, τα οποία δεν είχαν διαγραφεί με ασφάλεια πριν από την απόρριψή τους.

2. California State University(Weiss, 2004)– Το 2004, η διοίκηση του Πανεπιστημίου σε ανακοίνωσή της γνωστοποίησε ότι ένας πρώην υπάλληλος απέρριψε χωρίς να ακολουθήσει κανένα πρωτόκολλο διαχείρισης, σκληρούς δίσκους που περιείχαν τα προσωπικά στοιχεία περισσότερων από 23.000 φοιτητών, καθηγητών και μελών του προσωπικού. Οι σκληροί δίσκοι δεν διαγράφηκαν με ασφάλεια πριν από την απόρριψή τους και τα δεδομένα ήταν πιθανώς προσβάσιμα σε μη εξουσιοδοτημένα μέρη.

3. UK Ministry of Defense(Tim Wilson, 2008)- Το 2008, το υπουργείο Άμυνας του ΗΒ επικρίθηκε για την απόρριψη σκληρού δίσκου που περιείχε απόρρητα δεδομένα χωρίς να τα διαγράψει όπως προβλεπόταν. Ο σκληρός δίσκος περιείχε πληροφορίες για πάνω από 700 000 άτομα και περιείχε περίπου 1,5 εκατομμύριο πληροφορίες, συμπεριλαμβανομένων ορισμένων στοιχείων τράπεζας, άδειας οδήγησης, αριθμούς διαβατηρίων, διευθύνσεις, ημερομηνίες γέννησης και αριθμούς τηλεφώνου.

Η οριστική διαγραφή δεδομένων από σκληρούς δίσκους είναι μια υποσχόμενη πρακτική που εξασφαλίζει την ασφαλή διαχείριση εμπιστευτικών πληροφοριών και προσωπικών δεδομένων. Καθώς η τεχνολογία εξελίσσεται και η ανάγκη αποθήκευσης δεδομένων αυξάνεται, η απαίτηση για ασφαλή διαγραφή δεδομένων από τους σκληρούς δίσκους είναι επίσης καίριας σημασίας και επιβάλλεται.

Τα λογισμικά οριστικής διαγραφής δεδομένων παρέχουν μια αποτελεσματική λύση στο πρόβλημα της διαγραφής δεδομένων από τους σκληρούς δίσκους και παράλληλα διασφαλίζουν την ασφάλεια των προσωπικών δεδομένων και της ιδιωτικότητας.

Η ανάγκη αυτή φαίνεται να υιοθετείται τα τελευταία χρόνια από όλο και περισσότερους χρήστες και οργανισμούς αφού η ανησυχία για τη διασφάλιση της ιδιωτικότητας και την ασφάλεια των προσωπικών δεδομένων είναι πιο έντονη και η χρήση εργαλείων μόνιμης διαγραφής δεδομένων έχει γίνει πιο κοινή. Πολλά άτομα και οργανισμοί έχουν συνειδητοποιήσει τους πιθανούς κινδύνους που ελλοχεύουν και σχετίζονται με διαρροή δεδομένων και λαμβάνουν μέτρα για να προστατεύσουν τις πληροφορίες τους διαγράφοντας με ασφάλεια δεδομένα από τις συσκευές τους πριν από την απόρριψη ή την επαναχρησιμοποίηση. Ως αποτέλεσμα, η ζήτηση για προγράμματα διαγραφής δεδομένων έχει αυξηθεί και πολλοί κατασκευαστές λογισμικού έχουν αναπτύξει νέες και βελτιωμένες λύσεις για να καλύψουν αυτή την ανάγκη.

Στον αντίποδα όμως, η χρήση τέτοιων εργαλείων μπορεί να αποτελέσει σημαντική τροχοπέδη στην διεξαγωγή μιας δικανικής έρευνας αφού η εφαρμογή τους από άτομα που εμπίπτουν εκτός νομικών πλαισίων πιθανόν να οδηγήσει σε καταστροφή διαφόρων αποδεικτικών στοιχείων που σχετίζονται με τις παράνομες δραστηριότητες τους.

Στο παρελθόν υπήρξαν αρκετές υποθέσεις όπου διαφαίνεται πώς τα εργαλεία μόνιμης διαγραφής δεδομένων έχουν επηρεάσει σε μεγάλο βαθμό τις εγκληματολογικές έρευνες:

1. Silk Road (2015) - Στην υπόθεση Silk Road, της πιο γνωστής διαδικτυακής αγοράς για παράνομα αγαθά και υπηρεσίες στο Dark Web, ο τότε κατηγορούμενος Ross Ulbricht, δημιουργός του site είχε χρησιμοποιήσει ένα εργαλείο μόνιμης διαγραφής δίσκων για να καταστρέψει οριστικά αρχεία στον φορητό υπολογιστή του πριν από τη σύλληψή του. Αν και οι δικανικοί ερευνητές μπόρεσαν να ανακτήσουν ορισμένα στοιχεία, η χρήση του εργαλείου διαγραφής δεδομένων κατέστησε δύσκολη την σύνθεση μιας ολοκληρωμένης εικόνας των δραστηριοτήτων του Ulbricht.

2. Martha Stewart (2004)(Ferrell, 2011) – Σε αυτή την υπόθεση η Stewart κατηγορήθηκε για αθέμιτη χρηματιστηριακή εκμετάλλευση εμπιστευτικών πληροφοριών, αφού πούλησε όλο το μερίδιο των μετοχών που κατείχε της εταιρείας ImClone Systems ακριβώς πριν αυτή καταρρεύσει. Οι ερευνητές προσπάθησαν να ανακτήσουν τα διαγραμμένα email που θα μπορούσαν να παρέχουν στοιχεία για τη γνώση της Stewart περί πτώσης της μετοχής, αλλά ο βοηθός της είχε χρησιμοποιήσει ένα εργαλείο μόνιμης διαγραφής δεδομένων για να διαγράψει οριστικά τα email. Εν τέλει η Stewart κατηγορήθηκε για παρακώλυση της δικαιοσύνης και ψευδείς δηλώσεις στους ανακριτές και καταδικάστηκε σε φυλάκιση πέντε μηνών και σε περίοδο αποφυλάκισης υπό επιτήρηση.

3. Enron Corporation (2000)(Paul Festa, 2002) - Η Enron Corporation, μια από τις μεγαλύτερες εταιρείες ενέργειας στον κόσμο, ενεπλάκη σε ένα μεγάλο οικονομικό σκάνδαλο λογιστικής απάτης. Κατά τη διάρκεια της έρευνας, ανακαλύφθηκε ότι πολλά στελέχη είχαν χρησιμοποιήσει εργαλεία μόνιμης διαγραφής δεδομένων για να διαγράψουν ενοχοποιητικά email και έγγραφα από τους υπολογιστές τους. Αυτό κατέστησε πιο δύσκολο για τους ανακριτές να δημιουργήσουν δικογραφία εναντίον της εταιρείας και των στελεχών της.

4. Βομβιστική επίθεση στη Βοστώνη (2013)(Bob Sullivan & Rosa Golijan, 2013) – Κατά τη διάρκεια του Μαραθωνίου στη Βοστώνη το 2013, δύο αδέρφια πυροδότησαν βόμβες σκοτώνοντας τρία άτομα και τραυματίζοντας εκατοντάδες άλλους. Στις έρευνες που ακολούθησαν, ανακαλύφθηκε ότι ο μεγαλύτερος αδερφός είχε χρησιμοποιήσει ένα εργαλείο μόνιμης διαγραφής δεδομένων για να διαγράψει αρχεία από τον υπολογιστή και το τηλέφωνό του, συμπεριλαμβανομένης της τζιχαντιστικής προπαγάνδας και των οδηγιών κατασκευής βομβών. Αυτό κατέστησε πιο δύσκολο για τους ερευνητές να κατανοήσουν τα κίνητρα πίσω από την επίθεση και να εντοπίσουν πιθανούς συνεργάτες.

5. Volkswagen (2015)(Shepardson, 2016) - Το 2015, αποκαλύφθηκε το σκάνδαλο εκπομπών ρύπων της Volkswagen, όπου η εταιρεία είχε εγκαταστήσει λογισμικό στα πετρελαιοκίνητά της αυτοκίνητα, που της επέτρεπε να εξαπατήσουν στις δοκιμές εκπομπών ρύπων και να παραποιήσουν τα αποτελέσματα. Κατά τη διάρκεια της έρευνας, ανακαλύφθηκε ότι ορισμένοι υπάλληλοι είχαν χρησιμοποιήσει εργαλεία οριστικής διαγραφής δεδομένων για να διαγράψουν email και άλλες επικοινωνίες που σχετίζονται με το σκάνδαλο. Αυτό παρεμπόδισε τους ερευνητές να προσδιορίσουν την έκταση της παρανομίας της εταιρείας και να εντοπίσουν τους πραγματικά υπεύθυνους.

Τα παραδείγματα αυτά καταδεικνύουν τον σημαντικό αντίκτυπο που μπορεί να έχει η χρήση εργαλείων μόνιμης διαγραφής δεδομένων στις εγκληματολογικές έρευνες, ειδικά σε κρίσιμες εταιρικές ή ποινικές υποθέσεις.

## 1.1 Σκοπός Διατριβής

Σκοπός της διατριβής είναι να εξετάσει διεξοδικά ένα αριθμό από συγκεκριμένα διαθέσιμα εργαλεία οριστικής διαγραφής δεδομένων και να προσδιορίσει πόσο αποτελεσματικά λειτουργούν και εάν λειτουργούν έχοντας υπόψη τα ακόλουθα χαρακτηριστικά:

1. Ασφαλής διαγραφή: Το λογισμικό χρησιμοποιεί ασφαλείς, αναγνωρισμένες και αποτελεσματικές μεθόδους διαγραφής που αποτρέπουν κάθε πιθανότητα ανάκτησης δεδομένων. Αυτό μπορεί να περιλαμβάνει την αντικατάσταση των δεδομένων πολλαπλές φορές χρησιμοποιώντας τυχαία μοτίβα δεδομένων ή μια προκαθορισμένη ακολουθία από bits.

2. Φιλικό προς το χρήστη: Το λογισμικό έχει μια εύχρηστη διεπαφή με γραφικό περιβάλλον που θα επιτρέπει στους χρήστες να χειρίζονται το εργαλείο και να επιλέγουν τα αρχεία ή τις μονάδες δίσκου που θέλουν να διαγράψουν χωρίς κάποια ιδιαίτερη τεχνική γνώση.

3. Υποστήριξη Σκληρών Δίσκων: Το λογισμικό μπορεί να λειτουργεί με μια ποικιλία συσκευών αποθήκευσης, συμπεριλαμβανομένων των σκληρών δίσκων.

4. Συμμόρφωση με Πρότυπα Προστασίας Δεδομένων: Το λογισμικό συμμορφώνεται με τα σχετικά πρότυπα και κανονισμούς προστασίας δεδομένων, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)(*General Data Protection Regulation (GDPR) – Official Legal Text*, 2023) ή του NIST (National Institute of Standards and Technology , US)('NIST Standards', 2016).

5. Επαλήθευση: Το λογισμικό παρέχει μια διαδικασία επαλήθευσης που διασφαλίζεται ότι τα δεδομένα έχουν διαγραφεί πλήρως και δεν μπορούν να ανακτηθούν.

6. Ευελιξία: Το λογισμικό εργαλείο προσφέρει ευέλικτες επιλογές για τη διαγραφή δεδομένων, όπως τη δυνατότητα διαγραφής μεμονωμένων αρχείων, φακέλων, τμήματος δίσκου ή ολόκληρου του δίσκου.

7. Αναφορά: Το λογισμικό εργαλείο παρέχει μια λεπτομερή αναφορά της διαδικασίας διαγραφής, συμπεριλαμβανομένης της συσκευής ή των αρχείων που διαγράφηκαν και της μεθόδου που χρησιμοποιήθηκε.

Η διατριβή θα διεξαχθεί μέσω προκαθορισμένης, καλά σχεδιασμένης πειραματικής διαδικασίας κατά την οποία εκτός από τα πιο πάνω χαρακτηριστικά θα εξεταστούν και επιμέρους στόχοι σχετικά με την απόδοση τους σε κατανάλωση πόρων του συστήματος, υπολογιστική ισχύ και χρόνο αποπεράτωσης των εργασιών.

Αξιολογώντας τα αποτελέσματα από την εξέταση των εργαλείων θα μπορούμε να γνωρίζουμε εάν μπορούν να χρησιμοποιηθούν μεταξύ άλλων στην εξάλειψη αποδεικτικών στοιχείων διαγράφοντας ανεπανόρθωτα αρχεία και εγγραφές δραστηριότητας του υπολογιστή δυσχεραίνοντας έτσι το έργο των ψηφιακών δικανικών αναλυτών.

## 1.2 Βασικά Ερευνητικά Ερωτήματα

Τα ερωτήματα εστιάζονται κυρίως στη λειτουργία των εργαλείων μόνιμης διαγραφής που θα εξεταστούν και συγκεκριμένα στις ιδιότητες τους με βάση τις παραμέτρους που θα τεθούν και των αποτελεσμάτων που θα προκύψουν από την πειραματική διαδικασία.

Με βάση τα πιο πάνω η διατριβή θα επικεντρωθεί στα ακόλουθα ερευνητικά ερωτήματα:

1. Ποιο/Ποια από τα εργαλεία υπό εξέταση κρίνεται πιο αποτελεσματικό σύμφωνα με τις προϋποθέσεις που έχουμε θέσει στις πιο κάτω περιπτώσεις:
   α. Οριστική διαγραφή δεδομένων συγκεκριμένων αρχείων από το δίσκο.
   β. Οριστική διαγραφή δεδομένων ολόκληρου του δίσκου.

2. Υπάρχουν περιθώρια επαναφοράς κάποιων από τα δεδομένα που διαγράφηκαν με τη χρήση των εργαλείων; Αν ναι, σε τι ποσοστό;

3. Ποιο εργαλείο είναι ταχύτερο στην διεκπεραίωση της οριστικής διαγραφής συγκεκριμένου μεγέθους και πλήθους αρχείων;

4. Ποιο εργαλείο είναι το λιγότερο απαιτητικό σε υπολογιστικούς πόρους και αντίθετα ποιο εργαλείο είναι το πιο δαπανηρό;

5. Επηρεάζει την αποτελεσματικότητα του εργαλείου η ποσότητα των δεδομένων που βρίσκονται αποθηκευμένα στο δίσκο. Δηλαδή, αν παίζει ρόλο για τα αποτελέσματα το αν π.χ. θα σβήσουν 10GB/250GB ή 200GB/250GB.

## 1.3 Αναγκαιότητα και Σπουδαιότητα της Διατριβής

Στις μέρες μας η ραγδαία αύξηση των ψηφιακών συσκευών και η ανάγκη για ασφαλή διαχείριση των δεδομένων οδήγησε στη δημιουργία και διάθεση πληθώρας εργαλείων που υπόσχονται οριστική διαγραφή δεδομένων από τα μέσα αποθήκευσης. Αρκετά από αυτά διατίθενται είτε δωρεάν είτε επι πληρωμή. Στο σύνολο λοιπόν αυτών των εργαλείων που υπάρχουν διαθέσιμα και διαφημίζονται από τους κατασκευαστές τους για τις εξαιρετικές επιδόσεις τους θα πρέπει να γίνει μια αξιολόγηση ώστε να διαπιστωθεί ποσοτικά ποια από αυτά είναι αποτελεσματικά και ποια όχι.

Η απόδοση λειτουργίας των εργαλείων μόνιμης διαγραφής δεδομένων είναι ένα εξαιρετικό θέμα για έρευνα και πειραματισμό, αφού σχετίζεται άμεσα με την σωστή διαχείριση των προσωπικών αρχείων και δεδομένων τόσο από άτομα όσο και από οργανισμούς.

Η έρευνα και ο πειραματισμός μπορούν να βοηθήσουν στην αξιολόγηση της απόδοσης των εργαλείων οριστικής διαγραφής δεδομένων αναλύοντας την αποτελεσματικότητά τους σε διαφορετικά σενάρια, όπως η χωρητικότητα του μέσου αποθήκευσης, το επίπεδο ευαισθησίας των δεδομένων και η φύση των ίδιων των δεδομένων. Μπορεί επίσης να βοηθήσει στον εντοπισμό πιθανών αδυναμιών σε αυτά τα εργαλεία, όπως η δυνατότητα ανάκτησης διαγραμμένων δεδομένων χρησιμοποιώντας προηγμένες τεχνικές ανάκτησης δεδομένων.

Η αποτελεσματικότητα των εργαλείων αυτών είναι κρίσιμη για να διασφαλιστεί ότι οι εμπιστευτικές πληροφορίες δεν είναι ανακτήσιμες και προσβάσιμες από μη εξουσιοδοτημένα άτομα.

Τέλος, η μελέτη απόδοσης των εργαλείων οριστικής διαγραφής δεδομένων, κύριο αντικείμενο της παρούσας διατριβής αποτελεί σήμερα ανοικτό ερευνητικό πεδίο από διάφορους δικανικούς ερευνητές που προσπαθούν να εντοπίσουν τα όρια κατά τη χρήση τους ως αντί δικανικά εργαλεία και το βαθμό που μπορεί να επηρεάσουν την έρευνα σε ένα σύστημα στο οποίο έγινε χρήση τέτοιων εργαλείων.

## 1.4 Σημεία Καινοτομίας Διατριβής

Παρόλο που το συγκεκριμένο αντικείμενο λόγω της σημαντικότητάς του έχει απασχολήσει τους ερευνητές και στο παρελθόν, εντούτοις η παρούσα διατριβή φέρει αρκετά σημεία καινοτομίας

που δεν υιοθετήθηκαν σε προηγούμενες μελέτες. Μερικά από τα σημεία που παρουσιάζουν διαφοροποίηση είναι τα εξής:

1. Τα εργαλεία που θα εξεταστούν δεν έχουν αξιολογηθεί στο παρελθόν ως προς την ικανότητα τους για οριστική διαγραφή αρχείων. Εργαλεία που μελετήθηκαν στο παρελθόν από άλλους ερευνητές και δεν έχουν αναβαθμιστεί θα παρουσιάσουν λογικά τα ίδια αποτελέσματα.

2. Τα εργαλεία θα αξιολογηθούν ως προς:
   α. Τη δυνατότητα οριστικής διαγραφής ολόκληρου του δίσκου.
   β. Τη δυνατότητα οριστικής διαγραφής συγκεκριμένων αρχείων στο δίσκο.

3. Η καταγραφή σχετικά με την απόδοση των εργαλείων σε κατανάλωση πόρων του συστήματος, υπολογιστική ισχύ και χρόνο αποπεράτωσης των εργασιών θα γίνει με τη χρήση εξειδικευμένου εργαλείου (SysGauge Utility)(*SysGauge - System Monitor*, 2023) .

4. Θα αξιολογηθεί η αποτελεσματικότητα του εργαλείου κατά πόσο παρουσιάζει διαφοροποιήσεις σε σχέση με την ποσότητα των δεδομένων που βρίσκονται αποθηκευμένα στο δίσκο.

Εκτός από τα πιο πάνω σημεία, η συγκεκριμένη διατριβή παρουσιάζει σημαντικά σημεία καινοτομίας από προηγούμενες μελέτες που έχουν εκπονηθεί αφού γενικά η διαδικασία και η μεθοδολογία που θα ακολουθηθεί και θα εξηγηθεί πιο κάτω είναι σε πολλά σημεία διαφορετική.

## 1.5 Περιγραφή Δομής Διατριβής

Η παρούσα μεταπτυχιακή διατριβή αποτελείται από επτά κεφάλαια στα οποία παρουσιάζεται και αναλύεται το αντικείμενο της μελέτης με τρόπο ώστε να καλυφθούν όλες οι επιμέρους πτυχές του.

Στο 2ο Κεφάλαιο που ακολουθεί γίνεται μια γενική αναφορά στη θεωρία και τις βασικές έννοιες που έχουν άμεση σχέση με το αντικείμενο και εμφανίζονται συχνά στα επόμενα κεφάλαια.

Στο 3ο Κεφάλαιο γίνεται μια ανασκόπηση στην υπάρχουσα ερευνητική βιβλιογραφία καθώς επίσης και μια ιστορική αναδρομή σε προηγούμενες σχετικές μελέτες που έχουν εκπονηθεί για το ίδιο θέμα.

Στο 4ο Κεφάλαιο εξετάζεται η μεθοδολογία που θα ακολουθηθεί κατά την πειραματική διαδικασία όπως επίσης παρουσίαση και αναφορά στα εργαλεία οριστικής διαγραφής που θα αξιολογηθούν.

Στο 5ο Κεφάλαιο εκτελούνται τα σενάρια για κάθε εργαλείο οριστικής διαγραφής και παρουσιάζονται τα εργαλεία αξιολόγησης-ανάλυσης που θα χρησιμοποιηθούν.

Στο 6ο Κεφάλαιο παρουσιάζεται μια σύνοψη των αποτελεσμάτων της πειραματικής μελέτης και σύγκριση των μεταξύ τους ευρημάτων.

Τέλος, στο Κεφάλαιο 7 ως επίλογο εξάγουμε τα γενικά συμπεράσματα της όλης διαδικασίας καθώς επίσης και εισηγήσεις για μελλοντικές έρευνες.

# Κεφάλαιο 2
# Θεωρία – Βασικοί Εννοιολογικοί Ορισμοί

Πιο κάτω παρουσιάζονται μερικοί βασικοί εννοιολογικοί ορισμοί σχετικά με το θέμα που πραγματεύεται η παρούσα μεταπτυχιακή διατριβή.

## 2.1 Ψηφιακή Δικανική ως Επιστήμη

Η Δικανική υπολογιστών ή ευρύτερα ψηφιακή δικανική είναι η επιστήμη που έχει σαν αντικείμενο της, τον εντοπισμό, ανάλυση και διατήρηση των ψηφιακών δεδομένων που συλλέγονται από διάφορα μέσα αποθήκευσης δεδομένων όπως ηλεκτρονικοί υπολογιστές, κινητές συσκευές, εξωτερικοί δίσκοι κτλ., με σκοπό την ανασύνθεση και τον εντοπισμό συγκεκριμένων λεπτομερειών, στοιχείων και γεγονότων που σχετίζονται με ένα έγκλημα και την παρουσίαση τους στο δικαστήριο.

Η βασική μεθοδολογία της ψηφιακής δικανικής είναι:

1. (Acquire)-Απόκτηση τεκμηρίων χωρίς τροποποίηση ή αλλοίωση των αυθεντικών στοιχείων.
2. (Authenticate)-Πιστοποίηση της αυθεντικότητας των ανακτημένων αποδεικτικών στοιχείων και η επιβεβαίωση της σχέσης τους με τα πρωτότυπα αυθεντικά στοιχεία.
3. (Analyse)-Ανάλυση δεδομένων χωρίς αυτά να παραποιηθούν.

Η πιο πάνω μεθοδολογία θεωρείται κρίσιμη καθώς οποιαδήποτε παρατυπία στη διαχείριση των αποδεικτικών στοιχείων η διαδικασία διερεύνησης θα καταστεί αναξιόπιστη. Αυτό μπορεί να οδηγήσει σε αδυναμία απόδειξης ή στην ακύρωση τους από το δικαστήριο. Έτσι κατά την ανάκτηση δεδομένων σε μια ψηφιακή δικανική έρευνα, χρησιμοποιούνται ειδικά εργαλεία και τεχνικές που επιτρέπουν την ανάκτηση των δεδομένων χωρίς να τα καταστρέψουν ή να τα τροποποιήσουν. Αυτό περιλαμβάνει χρήση ειδικών εργαλείων για την ανάκτηση των δεδομένων από το αρχικό μέσο και την αντιγραφή των δεδομένων σε άλλο μέσο αποθήκευσης. Έχοντας υπόψη τα πιο πάνω αντιλαμβανόμαστε τη σημασία της ακεραιότητας των δεδομένων σε ένα σύστημα προς διερεύνηση πράγμα το οποίο έχουν σαν στόχο να πλήξουν οι τεχνικές Αντι-δικανικής.

## 2.2 Αντι-δικανική και Μέθοδοι Αντι-δικανικής

Ως Αντι-δικανική ορίζεται η χρήση τεχνικών, μεθόδων ή εργαλείων που έχουν σαν στόχο την παρεμπόδιση ή την παραπλάνηση ενός ψηφιακού δικανικού αναλυτή κατά την διενέργεια μιας δικανικής έρευνας. Η εφαρμογή των μεθόδων αυτών, έχει σαν απώτερο σκοπό να καταστήσει δύσκολη ή αδύνατη την ανάκτηση αποδεικτικών στοιχείων από μια συσκευή ή μέσο αποθήκευσης ώστε με αυτό τον τρόπο να πληγεί το πρώτο σημείο της βασικής μεθοδολογίας της ψηφιακής δικανικής. Οι αντι-δικανικές μέθοδοι χρησιμοποιούνται κατά κόρον από εγκληματίες για να καλύψουν τα ίχνη τους και να αποφύγουν τον εντοπισμό από τις υπηρεσίες επιβολής του νόμου. Ωστόσο, μπορούν επίσης να χρησιμοποιηθούν για νόμιμους σκοπούς, όπως η προστασία ευαίσθητων δεδομένων από μη εξουσιοδοτημένη πρόσβαση ή η ασφαλής διαγραφή δεδομένων από μια συσκευή ή μέσο αποθήκευσης προτού απορριφθούν ή επαναχρησιμοποιηθούν. Ένας ικανός εμπειρογνώμονας δικανικής θα πρέπει να είναι γνώστης των αντι-δικανικών τεχνικών και μεθόδων που μπορεί να χρησιμοποιηθούν και να είναι σε θέση να τις αντιμετωπίσει.

### 2.2.1 Τεχνικές Αντι-δικανικής

Μερικές από τις πιο συνηθισμένες τεχνικές Αντι-δικανικής είναι:

1. Κρυπτογράφηση (Encryption) - Η κρυπτογράφηση είναι μια από τις πιο διαδεδομένες αντι-δικανικές τεχνικές που μετατρέπει ένα μήνυμα σε ένα κωδικοποιημένο μήνυμα για να το κάνει αναγνώσιμο μόνο από όσους έχουν το αντίστοιχο κλειδί αποκωδικοποίησης. Τα κρυπτογραφημένα δεδομένα μπορεί να είναι δύσκολο ή αδύνατο να αποκρυπτογραφηθούν χωρίς το κατάλληλο κλειδί. Η κρυπτογράφηση χρησιμοποιείται συχνά για την προστασία απόρρητων δεδομένων, αλλά μπορεί επίσης να χρησιμοποιηθεί από επιτιθέμενους για να κρύψουν τις δραστηριότητές τους από τους ερευνητές.

2. Στεγανογραφία (Steganography) - Η Στεγανογραφία είναι μια άλλη αντι-δικανική τεχνική που περιλαμβάνει την απόκρυψη ενός μηνύματος ή ενός αρχείου μέσα σε ένα άλλο αρχείο, όπως ένα αρχείο εικόνας ή ήχου. Το κρυφό μήνυμα μπορεί να εξαχθεί χρησιμοποιώντας ένα συγκεκριμένο εργαλείο ή κλειδί. Η στεγανογραφία χρησιμοποιείται συνήθως από εγκληματίες για να κρύψουν την επικοινωνία τους ή για να κρύψουν κάποιο κακόβουλο λογισμικό.

3. Παραλλαγή Αρχείων (File Obfuscation) – Κατά την εφαρμογή της τεχνικής αυτής η δομή του αρχείου αλλάζει με τρόπο ώστε να παριστάνει κάποιο άλλου είδους αρχείο. Αυτό καθιστά το αρχείο δύσκολο να διαβαστεί και να αναλυθεί από τους ερευνητές.

4. Αλλαγή Χρονοσήμανσης (Changing Timestamps) - Στην ψηφιακή δικανική, η χρονική σήμανση αφορά μια πληροφορία που καταγράφει την ημερομηνία και την ώρα που συνέβη ένα συγκεκριμένο γεγονός ή δραστηριότητα σε ένα σύστημα υπολογιστή. Επίσης καταγράφει το χρόνο δημιουργίας ενός αρχείου (creation time), το χρόνο τροποποίησης (modification time) και το χρόνο προσπέλασης του (access time). Οι χρονικές σημάνσεις χρησιμοποιούνται σε ψηφιακές έρευνες για τον καθορισμό του ιστορικού των γεγονότων και για την παρακολούθηση των δραστηριοτήτων πιθανών υπόπτων. Η αλλαγή χρονικών σφραγίδων είναι μια αντι-δικανική τεχνική που χρησιμοποιείται για να χειραγωγηθούν ή να παραποιηθούν τα δεδομένα χρονικής σφραγίδας που σχετίζονται με αρχεία ή αρχεία καταγραφής συστήματος προκειμένου να παραπλανήσουν τους ερευνητές. Αυτό μπορεί να γίνει με διάφορους τρόπους, όπως η τροποποίηση του ρολογιού του συστήματος, η

προσαρμογή των ρυθμίσεων ζώνης ώρας ή η επεξεργασία των αρχείων με ειδικά εργαλεία.

5. Διαγραφή δεδομένων (Data Wiping) - Η διαγραφή δεδομένων είναι η διαδικασία καταστροφής δεδομένων σε μια συσκευή αποθήκευσης ώστε να μην είναι δυνατή η ανάκτησή τους. Αυτή η τεχνική χρησιμοποιείται συνήθως από εγκληματίες για να διαγράψουν στοιχεία των δραστηριοτήτων τους σε μια συσκευή. Τα εργαλεία οριστικής διαγραφής δεδομένων αντικαθιστούν τα υφιστάμενα δεδομένα στη συσκευή αποθήκευσης πολλές φορές για να διασφαλίσουν ότι δεν μπορούν να ανακτηθούν.

## 2.3 Φυσικά Μέσα Αποθήκευσης

Η χρήση των υπολογιστών και ψηφιακών συσκευών σε μια ποικιλία εφαρμογών οδήγησε στην δημιουργία πολλαπλών μέσων αποθήκευσης με ξεχωριστά χαρακτηριστικά, σχεδιασμένα να εξυπηρετούν διαφορετικές ανάγκες. Η επιλογή του κατάλληλου φυσικού μέσου αποθήκευσης εξαρτάται από τις ανάγκες του χρήστη, την ποσότητα των δεδομένων που πρέπει να αποθηκεύονται, τη συχνότητα της πρόσβασης στα αποθηκευμένα δεδομένα και το επίπεδο ασφαλείας που απαιτείται. Τα κοινά φυσικά μέσα αποθήκευσης που είναι διαθέσιμα σήμερα χωρίζονται γενικά σε τρείς μεγάλες κατηγορίες ανάλογα με την τεχνολογία που χρησιμοποιούν:

1. Μαγνητικές συσκευές αποθήκευσης (πχ Floppy disk, HDD, Magnetic Tape κτλ)
2. Συσκευές μνήμης flash (πχ USB Drives, SSD, SD Cards, κτλ )
3. Συσκευές οπτικής αποθήκευσης (πχ CD , DVD κτλ)

Για τους σκοπούς αυτής της διατριβής θα επικεντρωθούμε στα αποθηκευτικά μέσα που χρησιμοποιούνται σήμερα, κυρίως για αποθήκευση δεδομένων στους υπολογιστές.

### 2.3.1 Σκληροί Δίσκοι (HDD)

Ο σκληρός δίσκος είναι η πιο συνηθισμένη συσκευή αποθήκευσης δεδομένων που χρησιμοποιείται κυρίως σε υπολογιστές, διακομιστές και άλλες συσκευές τήρησης αρχείων πληροφορίας. Αποτελείται από μία ή περισσότερες περιστρεφόμενες πλάκες επικαλυμμένες με μαγνητικό υλικό και μια κεφαλή ανάγνωσης/εγγραφής που κινείται κατά μήκος των πλακών για ανάγνωση και εγγραφή δεδομένων. Οι σκληροί δίσκοι είναι ένα κρίσιμο στοιχείο στη σύγχρονη

πληροφορική, καθώς μας επιτρέπουν να αποθηκεύουμε μεγάλες ποσότητες δεδομένων και να έχουμε πρόσβαση σε αυτά γρήγορα και αποτελεσματικά.

## Ιστορία και εξέλιξη του σκληρού δίσκου

Ο πρώτος σκληρός δίσκος αναπτύχθηκε το 1956 από την IBM('History of Hard Disk Drives', 2023). Είχε χωρητικότητα μόλις 5 megabyte (MB), κάτι που θεωρήθηκε σημαντική ανακάλυψη εκείνη την εποχή. Με τα χρόνια, οι σκληροί δίσκοι συνέχισαν να εξελίσσονται και να γίνονται μικρότεροι, ταχύτεροι και πιο αποτελεσματικοί. Μία από τις πιο σημαντικές εξελίξεις στην τεχνολογία του σκληρού δίσκου ήταν η ανάπτυξη της κεφαλής λεπτής μεμβράνης τη δεκαετία του 1970. Αυτό επέτρεψε την αποθήκευση πολύ μεγαλύτερης πυκνότητας δεδομένων σε κάθε δίσκο. Στη δεκαετία του 1980, η εισαγωγή του δίσκου Winchester επέτρεψε ακόμη μεγαλύτερες χωρητικότητες, με το πρώτο μοντέλο να προσφέρει 10 MB αποθηκευτικού χώρου. Από τότε, οι σκληροί δίσκοι συνέχισαν να γίνονται μικρότεροι σε μέγεθος και πιο μεγάλοι σε χωρητικότητα. Σήμερα, υπάρχουν σκληροί δίσκοι με χωρητικότητα πολλαπλών terabyte (TB), η οποία είναι εκατομμύρια φορές μεγαλύτερη από την αρχική μονάδα σκληρού δίσκου 5 MB που αναπτύχθηκε από την IBM.

## Τρόπος λειτουργίας

Η βασική αρχή πίσω από τους σκληρούς δίσκους είναι η χρήση του μαγνητισμού για την αποθήκευση και την ανάκτηση δεδομένων. Οι πλάκες στο εσωτερικό του σκληρού δίσκου είναι επικαλυμμένες με μαγνητικό υλικό και η κεφαλή ανάγνωσης/εγγραφής κινείται κατά μήκος των πλακών για ανάγνωση και εγγραφή δεδομένων. Όταν τα δεδομένα εγγράφονται στον σκληρό δίσκο, η κεφαλή ανάγνωσης/εγγραφής δημιουργεί ένα μαγνητικό πεδίο που ευθυγραμμίζει τα μαγνητικά σωματίδια στα τμήματα του δίσκου με ένα συγκεκριμένο μοτίβο. Αυτό το μοτίβο αντιπροσωπεύει τα δεδομένα που έχουν εγγραφεί στον σκληρό δίσκο. Όταν διαβάζονται δεδομένα από τον σκληρό δίσκο, η κεφαλή ανάγνωσης/εγγραφής μετακινείται κατά μήκος της πλάκας και ανιχνεύει το μαγνητικό πεδίο που δημιουργείται από τα ευθυγραμμισμένα σωματίδια. Η φορά αυτών των ευθυγραμμισμένων σωματιδίων καθορίζει το είδος της δυαδικής πληροφορίας σε 0 και 1. Αυτά τα ψηφιακά δεδομένα στη συνέχεια μετατρέπονται σε πληροφορίες που μπορούν να χρησιμοποιηθούν από τον υπολογιστή.

### 2.3.2 Solid State Drive (SSD)

Ο δίσκος Solid State (SSD)('Solid-State Drive', 2023) είναι ένας άλλος σύγχρονος τύπος συσκευής αποθήκευσης που ουσιαστικά εκτελεί τις ίδιες λειτουργίες (αποθηκεύει δεδομένα σε μορφή 0 και 1) με τους παραδοσιακούς σκληρούς δίσκους αλλά χρησιμοποιεί διαφορετικές τεχνολογίες. Αποτελείται από πολλές μνήμες flash, δηλαδή συστοιχίες από chips πυριτίου που σε αυτά αποθηκεύονται μόνιμα οι πληροφορίες. Αυτά τα chips αποτελούνται από (floating gate transistors) FGTs, ημιαγωγούς που έχουν την ικανότητα να διατηρούν το ηλεκτρικό φορτίο. Έτσι κάθε FGT θεωρείται ένα κελί και περιέχει ένα bit δεδομένων. Όταν δηλαδή το κελί είναι φορτισμένο τότε το bit θεωρείται 0 ενώ όταν δεν υπάρχει φορτίο η τιμή του είναι 1.

Ο πρώτος εμπορικά διαθέσιμος SSD κατασκευάστηκε από τη SanDisk Corporation το 1991 και είχε χωρητικότητα μόλις 20MB. Ωστόσο λόγω του υψηλού κόστους, η χρήση του περιορίστηκε σε κρίσιμους τεχνολογικούς τομείς όπως στρατιωτικές και αεροδιαστημικές εφαρμογές. Μερικά χρόνια αργότερα όταν πλέον η τεχνολογία των SSDs ωρίμασε και οι τιμές έγιναν πιο προσιτές οι δίσκοι γίνονται εμπορικά ευρέως διαθέσιμοι και σε προσωπικούς υπολογιστές.

Οι δίσκοι SSDs έχουν συγκεκριμένη διάρκεια ζωής, που καθορίζεται από ένα πεπερασμένο κύκλο εγγραφών στις μνήμες flash του δίσκου. Όταν ο αριθμός αυτός ξεπεραστεί η απόδοση του δίσκου γίνεται απρόβλεπτη αφού τα floating gate transistors παύουν να είναι σε θέση να διατηρήσουν το φορτίο τους. Για να μειωθεί λοιπόν η φθορά του δίσκου από τις συνεχείς εγγραφές, οι κατασκευαστές υιοθέτησαν διάφορες τεχνικές για επέκταση της διάρκειας ζωής του. Η κυριότερη τεχνική ονομάζεται wear leveling κατά την οποία ο ελεγκτής του δίσκου ανεξάρτητα από το λειτουργικό σύστημα κανονίζει ώστε τα δεδομένα να κατανέμονται ομοιόμορφα στις μνήμες και οι κύκλοι εγγραφών / διαγραφών να είναι παρόμοιοι σε όλα τα block μνήμης. Πέραν από το wear leveling στους δίσκους SSDs εφαρμόζονται και άλλες λειτουργίες όπως το Garbage Collection και TRIM όπου σκοπό έχουν την καλύτερη απόδοση του δίσκου αφού αυτές καθορίζουν με ποια σειρά τα δεδομένα θα διαγραφούν οριστικά από το δίσκο.

### 2.3.3 Διαφορές HDD σε σχέση με τους SSDs

Οι SSDs προσφέρουν μεγαλύτερες ταχύτητες ανάγνωσης και εγγραφής από τους σκληρούς δίσκους, γεγονός που μεταφράζεται σε πιο γρήγορη πρόσβαση και μεταφορά δεδομένων. Αυτό παρατηρείται επειδή οι SSD δεν έχουν κινούμενα μηχανικά μέρη και χρησιμοποιούν μνήμες flash για την αποθήκευση δεδομένων, ενώ οι σκληροί δίσκοι χρησιμοποιούν περιστρεφόμενους

δίσκους και κεφαλές ανάγνωσης/εγγραφής για πρόσβαση σε πληροφορίες. Ως αποτέλεσμα, οι SSD έχουν ταχύτερη πρόσβαση στις πληροφορίες, η καθυστέρηση μειώνεται επίσης σημαντικά και οι χρήστες συνήθως βιώνουν μειωμένους χρόνους εκκίνησης εφαρμογών και βελτιωμένη συνολική απόδοση του συστήματος. Επιπλέον, οι SSDs είναι πιο αξιόπιστοι από τους σκληρούς δίσκους, καθώς είναι σαφώς λιγότερο επιρρεπείς σε μηχανικές βλάβες. Λόγω της λειτουργίας και του τρόπου κατασκευής τους οι σκληροί δίσκοι μπορεί να καταστραφούν εάν πέσουν ή εκτεθούν σε υψηλά επίπεδα κραδασμών, καθώς οι περιστρεφόμενοι δίσκοι τους μπορεί να τεθούν εκτός ευθυγράμμισης ή να χτυπηθούν από τις κεφαλές ανάγνωσης. Αντίθετα, οι SSDs που δεν έχουν κινούμενα μέρη είναι λιγότερο επιρρεπείς σε βλάβες από χτυπήματα και κραδασμούς. Τέλος οι SSDs αντέχουν καλύτερα τις ακραίες θερμοκρασίες και δεν επηρεάζονται από μαγνητικά πεδία. Όσο αφορά το θέμα της κατανάλωσης ενέργειας και εδώ οι SSD πλεονεκτούν καθώς η απουσία κινούμενων μερών από την κατασκευή τους, τους καθιστά λιγότερο ενεργοβόρους σε σχέση με τους μηχανικούς σκληρούς δίσκους. Αυτό σημαίνει ότι οι φορητοί υπολογιστές και άλλες κινητές συσκευές μπορούν να επωφεληθούν, για μεγαλύτερη διάρκεια ζωής της μπαταρίας και τα κέντρα δεδομένων μπορούν να μειώσουν την κατανάλωση ενέργειας και το σχετικό οικονομικό κόστος. Παρόλα αυτά οι παραδοσιακοί σκληροί δίσκοι αποτελούν το βασικό μέρος της αγοράς αποθηκευτικών μέσων ακόμα και σήμερα αφού προσφέρουν μεγαλύτερες χωρητικότητες σε σχέση με το οικονομικό κόστος.

Σε αυτή τη διατριβή θα μελετήσουμε την επίδραση που έχουν τα εργαλεία οριστικής διαγραφής στους σκληρούς δίσκους (HDD). Η επιλογή αυτή βασίστηκε στο γεγονός ότι η λειτουργία διαγραφής στους δίσκους SSD όπως είδαμε και πιο πάνω παρουσιάζει αρκετές διαφορές σε σχέση με τους συμβατικούς δίσκους έτσι τα εργαλεία αυτά δεν θεωρούνται αποτελεσματικά στις περιπτώσεις αυτές. Αντίθετα η χρήση τέτοιων εργαλείων σε μονάδες SSD πιθανόν να οδηγήσει σε φθορά των μνημών και να μειώσει τη συνολική διάρκεια ζωής του δίσκου. Για οριστική διαγραφή δεδομένων από τις μονάδες SSD συνίσταται η χρήση της ενσωματωμένης λειτουργίας διαγραφής που παρέχεται από τον κατασκευαστή του SSD. Αυτές οι μέθοδοι διασφαλίζουν ότι τα δεδομένα διαγράφονται σωστά χωρίς να διακυβεύεται η διάρκεια ζωής ή η απόδοση της μονάδας.

## 2.4 Τύποι Συστημάτων Αρχείων (File Systems)

Το σύστημα αρχείων (File system) αποτελεί μια αποθηκευτική δομή σε ένα σύστημα υπολογιστή που οργανώνει τον τρόπο με τον οποίο αποθηκεύονται τα δεδομένα. Ουσιαστικά λειτουργεί σαν ένα είδος πίνακα περιεχομένων με τις φυσικές θέσεις όλων των δεδομένων που βρίσκονται

αποθηκευμένα στο αποθηκευτικό μέσο. Τα συστήματα αρχείων αποτελούν αναπόσπαστο τμήμα κάθε λειτουργικού συστήματος αφού καθορίζουν που υπάρχει ελεύθερος χώρος για να αποθηκευτούν νέα δεδομένα, επιτρέπουν στους χρήστες να δημιουργούν και να αποθηκεύουν αρχεία, παρέχουν πρόσβαση σε δεδομένα, και φυσικά αξιοποιούν τις δυνατότητες στους σκληρούς δίσκους. Τέλος καθορίζουν περιορισμούς στις ονομασίες αρχείων, το μέγιστο αριθμό χαρακτήρων στην ονομασία του αρχείου , περιορισμούς στους χαρακτήρες που μπορούν να χρησιμοποιηθούν κτλ. Συνήθως υπάρχουν διαφορετικά συστήματα αρχείων σε διαφορετικά λειτουργικά συστήματα το καθένα με τα δικά του χαρακτηριστικά, πλεονεκτήματα και μειονεκτήματα. Στο λειτουργικό σύστημα Windows υπάρχουν 3 είδη file Systems (NTFS, FAT32 και exFAT ).

1. NTFS - Το NTFS (New Technology File System) είναι το προεπιλεγμένο σύστημα αρχείων που χρησιμοποιείται από τις τελευταίες εκδόσεις των Windows, συμπεριλαμβανομένων των Windows 10 και Windows 11. Εισήχθη από τη Microsoft το 1993 ως διάδοχος του συστήματος αρχείων FAT (File Allocation Table), το οποίο χρησιμοποιούσε σε προηγούμενες εκδόσεις των Windows. Η μετάβαση αυτή χαρακτηρίστηκε ως σημαντική αναβάθμιση αφού το προηγούμενο σύστημα υστερούσε σε αρκετά σημεία. Μερικά από τα βασικά πλεονεκτήματα του NTFS έναντι του FAT είναι η υποστήριξη σε λειτουργίες όπως η συμπίεση αρχείων και η κρυπτογράφηση. Επίσης παρέχει καλύτερη απόδοση και αξιοπιστία από το σύστημα FAT ειδικά για χρήση σε μεγάλα αρχεία. Αξιοσημείωτο χαρακτηριστικό του NTFS είναι η υποστήριξη που παρέχει για δικαιώματα αρχείων και έλεγχο πρόσβασης. Το NTFS επιτρέπει στους διαχειριστές να ορίζουν λεπτομερή δικαιώματα σε αρχεία και καταλόγους, συμπεριλαμβανομένης της πρόσβασης ανάγνωσης, εγγραφής και εκτέλεσης για διαφορετικούς χρήστες και ομάδες. Αυτό καθιστά απλό τον έλεγχο ποιος μπορεί να έχει πρόσβαση για να τροποποιεί συγκεκριμένα δεδομένα σε ένα σύστημα Windows. Αναμφίβολα το NTFS είναι ένα ισχυρό αρχείο συστήματος με αρκετά χαρακτηριστικά και πολλά πλεονεκτήματα σε σύγκριση με παλαιότερα συστήματα αρχείων καθιστώντας το δημοφιλή επιλογή για χρήστες Windows.

2. FAT32 - Το FAT32 (File Allocation Table) είναι ένα ευρέως γνωστό και διαδεδομένο σύστημα αρχείων το οποίο συναντάται κυρίως σε συσκευές όπως μονάδες USB, κάρτες μνήμης, και άλλες εξωτερικές μονάδες αποθήκευσης. Πρωτοεμφανίστηκε το 1996 ως μια επέκταση του προκατόχου του FAT16, το οποίο έφερε αρκετούς περιορισμούς όπως το μέγιστο μέγεθος partition το οποίο ήταν καθορισμένο στα 2GB. Το βελτιωμένο σύστημα

αρχείων FAT32 σχεδιάστηκε με τρόπο ώστε να ξεπερνά τους προηγούμενους περιορισμούς και να παρέχει υποστήριξη για μεγαλύτερα αρχεία. Το σημαντικότερο πλεονέκτημα του FAT32 είναι η συμβατότητα του με διαφορετικά λειτουργικά συστήματα όπως Mac, Linux και Android. Το γεγονός αυτό καθιστά το FAT32 ιδανικό για χρήση σε φορητές μονάδες αποθήκευσης αφού μπορεί να χρησιμοποιηθεί σε διαφορετικές συσκευές με ποικίλα λειτουργικά συστήματα. Το FAT32 ωστόσο φέρει και κάποιους περιορισμούς. Ο πιο σημαντικός αφορά το μέγιστο μέγεθος αρχείου που μπορεί να αποθηκευτεί, το οποίο δεν ξεπερνά τα 4GB ενώ το συνολικό μέγεθος του αποθηκευτικού μέσου δεν πρέπει να είναι μεγαλύτερο από 2TB. Επιπλέον δεν προσφέρει το ίδιο επίπεδο ασφάλειας και ελέγχου δικαιωμάτων όπως το εξελιγμένο σύστημα αρχείου NTFS. Συνολικά όμως το FAT32 είναι ένα αξιόπιστο σύστημα αρχείων του οποίου η απλότητα και η συμβατότητά, το καθιστούν εξαιρετική επιλογή για φορητή αποθήκευση ακόμα και σήμερα.

3. ExFAT – Το ExFAT (Extended File Allocation Table) αποτελεί ένα σύστημα αρχείων το οποίο σχεδιάστηκε και αναπτύχθηκε από τη Microsoft το 2006, με σκοπό να αντικαταστήσει το ξεπερασμένο FAT32 το οποίο παρουσίαζε τις αδυναμίες που καταγράφηκαν πιο πάνω. Χρησιμοποιείται επί το πλείστον σε συσκευές εξωτερικής αποθήκευσης όπως USB drives και SD cards. Το σημαντικότερο πλεονέκτημα του exFAT είναι η υποστήριξη του για μεγάλα μεγέθη αρχείων και συσκευές αποθήκευσης. Σε αντίθεση με το προκάτοχο του FAT32, το οποίο έχει μέγιστο μέγεθος αρχείου 4 GB και μέγιστο μέγεθος συσκευής αποθήκευσης 2 TB, το exFAT μπορεί να χειριστεί αρχεία έως 16 exabyte και συσκευές αποθήκευσης έως 128 PB. Επίσης το exFAT έχει συμβατότητα τόσο με λειτουργικά συστήματα Windows όσο και με Mac. Το χαρακτηριστικό αυτό το καθιστά ιδανικό για μεταφορά αρχείων μεταξύ διαφορετικών υπολογιστών με διαφορετικά λειτουργικά. Το exFAT υποστηρίζει επίσης ονόματα αρχείων και φακέλων έως 255 χαρακτήρες, το οποίο είναι σημαντικά μεγαλύτερο από το όριο του FAT32. Όσο αφορά τα μειονεκτήματα του το exFAT δεν υποστηρίζεται από παλαιότερα λειτουργικά συστήματα.

## 2.5 Μέθοδοι Μόνιμης Διαγραφής Δεδομένων

Για τις περιπτώσεις μόνιμης διαγραφής δεδομένων από σκληρούς δίσκους μπορούν να εφαρμοστούν οι ακόλουθες μέθοδοι.

1. Η επανεγγραφή είναι μια μέθοδος που χρησιμοποιείται για τη μόνιμη διαγραφή δεδομένων από μια συσκευή αποθήκευσης με εγγραφή πάνω στα υπάρχοντα δεδομένα με νέα δεδομένα. Σε αυτό το επίπεδο τα δεδομένα στο δίσκο θα πρέπει να τύχουν επανεγγραφής με τη χρήση αξιόπιστων, επικυρωμένων τεχνολογιών, μεθόδων ή εργαλείων. Αυτό περιλαμβάνει τη χρήση λογισμικού που έχει σχεδιαστεί για την αντικατάσταση ολόκληρου του σκληρού δίσκου ή συγκεκριμένων αρχείων με τυχαία δεδομένα ή μηδενικά, καθιστώντας αδύνατη την ανάκτηση των αρχικών δεδομένων. Η όλη διαδικασία θα πρέπει να περιλαμβάνει τουλάχιστο ένα πέρασμα εγγραφής δεδομένων όπως μηδενικά. Μπορούν ωστόσο να χρησιμοποιηθούν εάν απαιτείται από την πολιτική διαχείρισης δεδομένων του οργανισμού και πολλαπλά περάσματα με πολύπλοκα μοτίβα επανάληψης εγγραφών. Η επανεγγραφή θεωρείται μια αποτελεσματική μέθοδος για τη μόνιμη διαγραφή δεδομένων, αλλά μπορεί να είναι χρονοβόρα και μπορεί να μειώσει τη διάρκεια ζωής της συσκευής αποθήκευσης λόγω του μεγάλου αριθμού κύκλων εγγραφής που απαιτούνται. Επιπλέον, είναι σημαντικό να γίνεται χρήση αξιόπιστου λογισμικού που μπορεί να αντικαταστήσει πλήρως τα δεδομένα για να διασφαλιστεί ότι τα δεδομένα έχουν πραγματικά καταστραφεί.

2. Μια αποτελεσματική μέθοδος μόνιμης διαγραφής δεδομένων είναι ο απομαγνητισμός (Degaussing) όπου με τη χρήση ειδικών συσκευών, τα αποθηκευτικά μέσα εκτίθενται σε ισχυρό μαγνητικό πεδίο με αποτέλεσμα να διαταράσσονται οι καταγεγραμμένες μαγνητικές περιοχές έτσι τα δεδομένα στον δίσκο να διαγράφονται μόνιμα. Η τεχνική του απομαγνητισμού είναι αποτελεσματική και συστήνεται σε περιπτώσεις όπου υπάρχουν δίσκοι με εξαιρετικά μεγάλη χωρητικότητα και η διαδικασία της επανεγγραφής ακόμα και με ένα πέρασμα θα ήταν ιδιαίτερα χρονοβόρα. Ωστόσο, είναι σημαντικό να σημειωθεί ότι λειτουργεί μόνο σε μαγνητικά μέσα και δεν μπορεί να χρησιμοποιηθεί για τη διαγραφή δεδομένων από μονάδες SSD ή άλλες μη μαγνητικές συσκευές αποθήκευσης. Μετά τον απομαγνητισμό, η μονάδα σκληρού δίσκου (HDD) δεν μπορεί να χρησιμοποιηθεί ξανά, επειδή η όλη διαδικασία καταστρέφει το μαγνητικό πεδίο στις πλάκες των δίσκων, καθιστώντας αδύνατη την αποθήκευση νέων δεδομένων.

3. Η φυσική καταστροφή του αποθηκευτικού μέσου εφαρμόζεται όταν οι δύο προηγούμενες μέθοδοι δεν θεωρούνται επαρκείς για την οριστική διαγραφή των δεδομένων στο δίσκο. Το επίπεδο αυτό προνοεί την αμετάκλητη διαγραφή των δεδομένων μαζί με την καταστροφή του μέσου που τα φιλοξενεί. Η φυσική καταστροφή μπορεί να γίνει με διάφορους τρόπους, συμπεριλαμβανομένου του τεμαχισμού, της σύνθλιψης ή της τήξης των μέσων αποθήκευσης.

## 2.6 Παγκόσμια πρότυπα διαγραφής δεδομένων

Για την διαχείριση των δεδομένων και την ορθή χρήση των εργαλείων οριστικής διαγραφής συντάχθηκαν διάφορα παγκόσμια πρότυπα που περιγράφουν τις απαιτήσεις και τις προϋποθέσεις για την εφαρμογή τους. Τα πρότυπα αυτά έχουν αναπτυχθεί από διάφορους οργανισμούς και κυβερνητικές υπηρεσίες για να διασφαλίσουν ότι τα δεδομένα διαγράφονται με ασφάλεια και μόνιμα από τα μέσα αποθήκευσης και ότι η διαδικασία διαγραφής είναι διαφανής, ελεγχόμενη και επαληθεύσιμη. Μερικά από τα πιο ευρέως αναγνωρισμένα παγκόσμια πρότυπα για τη διαγραφή δεδομένων είναι:

1. National Institute of Standards and Technology (NIST) – Δημοσίευση 800-88 rev.1, Guidelines for Media Sanitization.(Kissel et al., 2014)
2. International Organization for Standardization (ISO) 27001(*ISO/IEC 27001 Standard – Information Security Management Systems*, n.d.)
3. Department of Defense (DoD) 5220.22-M(*DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM)* , 1995)
4. Payment Card Industry Data Security Standard (PCI DSS)('Payment Card Industry Data Security Standard', 2023)
5. General Data Protection Regulation (GDPR)

Είναι σημαντικό να αναφερθεί ότι τα διάφορα πρότυπα πιθανόν να έχουν διαφορετικές απαιτήσεις για την οριστική διαγραφή δεδομένων όπως τον αριθμό των επανεγγραφών ή τη χρήση συγκεκριμένων μεθόδων διαγραφής που θα δούμε πιο κάτω.

## 2.7 Μέθοδοι Επανεγγραφής Δεδομένων

Πρόκειται ουσιαστικά για αλγόριθμους που εφαρμόζονται από τα διάφορα εργαλεία οριστικής διαγραφής για να διασφαλίσουν ότι τα υφιστάμενα δεδομένα έχουν πλήρως αντικατασταθεί με νέα. Η κάθε μέθοδος ξεχωρίζει ως προς τον αριθμό των επαναλήψεων και το είδος των νέων εγγραφών που εκτελεί. Υπάρχει μεγάλη ποικιλία και η χρήση τους καθορίζεται ανάλογα με τις ειδικές απαιτήσεις και τους κανονισμούς που διέπουν τη διαγραφή δεδομένων για έναν συγκεκριμένο οργανισμό σύμφωνα με το πρότυπο που ακολουθεί. Είναι σημαντικό να επιλεγεί ένα εργαλείο διαγραφής που χρησιμοποιεί μεθόδους διαγραφής που πληρούν τα απαραίτητα πρότυπα για τη διαγραφή δεδομένων και παρέχουν το επίπεδο ασφάλειας που απαιτείται για τα δεδομένα που διαγράφονται. Ακολουθεί καταγραφή των σημαντικότερων μεθόδων/ αλγορίθμων μαζί με τα χαρακτηριστικά τους.

1. US - DoD 5220.22-M – Υλοποιήθηκε από το Αμερικάνικο υπουργείο άμυνας. Η μέθοδος αυτή πραγματοποιεί συνολικά τρείς διαδοχικές εγγραφές. Κατά την πρώτη επανάληψη εγγράφονται στο δίσκο δυαδικά μηδενικά (0), στην δεύτερη επανάληψη δυαδικά ένα (1) και στη τρίτη τυχαίοι χαρακτήρες. Ακολουθεί ένα τελευταίο πέρασμα ανάγνωσης του δίσκου για να επιβεβαιωθεί ότι σε αυτό βρίσκονται τυχαία δεδομένα και τα αρχικά έχουν αντικατασταθεί.

2. US DoD 5220.22-M (ECE) – Όμοιος αλγόριθμος με τον προηγούμενο, με τη διαφορά ότι επαναλαμβάνει τις εγγραφές συνολικά επτά φορές. Κατά την πρώτη εγγραφή στο δίσκο καταχωρούνται δυαδικά μηδενικά (0), στο δεύτερο πέρασμα δυαδικά ένα (1) , στη τρίτη επανάληψη τυχαίοι χαρακτήρες ενώ στην τέταρτη επανάληψη εγγράφεται σε όλους τους τομείς του δίσκου ο χαρακτήρας 0x96 (δυαδικό 10010110). Οι τρείς τελευταίες εγγραφές αποτελούν επαναλήψεις των πρώτων τριών.

3. US - DoD 5200.28-STD – Ακόμα ένας αλγόριθμός επτά επαναλήψεων του Αμερικάνικου υπουργείου άμυνας. Σε αυτή τη μέθοδο στο δίσκο εγγράφονται κατά την πρώτη επανάληψη διαδοχικά 01010101 ενώ στη δεύτερη επανάληψη διαδοχικά 10101010 . Το μοτίβο αυτό εκτελείται συνολικά 6 φορές ενώ κατά το τελευταίο πέρασμα στο δίσκο εγγράφονται τυχαίοι χαρακτήρες.

4. Russian GOST-50739-95 – Η μέθοδος αυτή δημιουργήθηκε από τη κρατική ρωσική τεχνική επιτροπή για προστασία από μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες.

Αποτελείται από δύο μόνο επαναλήψεις. Στη πρώτη επανάληψη εγγράφονται στο δίσκο δυαδικά μηδενικά (0) ενώ στην δεύτερη και τελευταία επανάληψη τυχαίοι χαρακτήρες.

5. German Standard VSITR – Η μέθοδος αυτή αναπτύχθηκε από το Γερμανικό ομοσπονδιακό γραφείο ασφάλειας πληροφοριών το 2000. Η κεφαλή εγγραφής περνά πάνω από κάθε τομέα συνολικά επτά φορές. Κάθε πέρασμα εγγράφει τους παρακάτω χαρακτήρες διαδοχικά : 0x00 (binary 00000000), 0xFF (binary 11111111), 0x00 (binary 00000000), 0xFF (binary 11111111), 0x00 (binary 00000000), 0xFF (binary 11111111), 0xAA (binary 10101010).

6. Canadian OPS-II – Η μέθοδος αυτή χρησιμοποιείται από την ομοσπονδιακή και εθνική υπηρεσία αστυνομίας του Καναδά. . Η κεφαλή εγγραφής περνά πάνω από κάθε τομέα συνολικά επτά φορές. Κάθε πέρασμα εγγράφει τους παρακάτω χαρακτήρες διαδοχικά : 0x00 (binary 00000000), 0xFF (binary 11111111), 0x00 (binary 00000000), 0xFF (binary 11111111), 0x00 (binary 00000000), 0xFF (binary 11111111), τυχαίοι χαρακτήρες.

7. British HMG IS5 Baseline – Η μέθοδος αυτή χρησιμοποιείται από την Βρετανική κυβέρνηση για τη διαχείριση των ευαίσθητων πληροφοριών. Ο αλγόριθμος περιλαμβάνει ένα πέρασμα κατά το οποίο ο δίσκος εγγράφεται με μηδενικά (0). Στη συνέχεια ακολουθεί ακόμα ένα πέρασμα ανάγνωσης για σκοπούς επιβεβαίωσης της αντικατάστασης των δεδομένων.

8. British HMG IS5 (Enhanced) – Πρόκειται για την βελτιωμένη και πιο ασφαλή έκδοση της πιο πάνω μεθόδου. Στην περίπτωση αυτή ο αλγόριθμος εκτελείται τρεις φορές. Κατά την πρώτη εγγραφή καταχωρούνται δυαδικά μηδενικά (0), στο δεύτερο πέρασμα δυαδικά ένα (1) και στη τρίτη επανάληψη τυχαίοι χαρακτήρες. Ακολουθεί επιβεβαίωση για τα αποτελέσματα των εγγραφών.

9. US Army AR 380-19 – Η μέθοδος αυτή ορίστηκε και δημοσιεύτηκε από τον Αμερικάνικο στρατό στον κανονισμό 380-19 το 1998. Σύμφωνα με αυτό για την πλήρη καταστροφή των δεδομένων προβλέπεται να γίνουν τρεις διαδοχικές εγγραφές στο δίσκο. Στο πρώτο πέρασμα εγγράφονται τυχαίοι χαρακτήρες, στη δεύτερη επανάληψη με μηδενικά (0) και στην τρίτη επανάληψη με ένα (1).

10. Peter Gutmann – Η μέθοδος αυτή αναπτύχθηκε το 1996 από τον Peter Gutmann, ακαδημαϊκό επιστήμονα υπολογιστών και προνοεί συνολικά 35 επαναλήψεις εγγραφών στο δίσκο. Ο αλγόριθμος Gutmann χρησιμοποιεί τυχαίες τιμές για τα πρώτα και τα τελευταία 4 περάσματα, ενώ για τις υπόλοιπες επαναλήψεις χρησιμοποιεί ένα σύνθετο μοτίβο. Είναι μια από τις πιο αποτελεσματικές μεθόδους διαγραφής δεδομένων, αν και πολύ χρονοβόρα.

11. Bruce Schneier – Ο αλγόριθμος Schneier αναπτύχθηκε από τον Bruce Schneier και παρουσιάστηκε στο βιβλίο του Applied Cryptography το έτος 1994. Η μεθοδολογία που ακολουθεί αποτελείται από επτά διαδοχικά περάσματα εγγραφών στο δίσκο. Η αντικατάσταση γίνεται με ένα (1) και μηδέν (0) στις πρώτες δύο επαναλήψεις ενώ οι υπόλοιπες πέντε εγγραφές γίνονται με τυχαίους χαρακτήρες.

12. NCSC-TG-025 – Η μέθοδος αυτή αναπτύχθηκε από την Υπηρεσία Εθνικής Ασφάλειας της Αμερικής. Περιλαμβάνει τρεις εγγραφές με επαλήθευση μετά το πέρας κάθε εγγραφής. Κατά την πρώτη εγγραφή γίνεται αντικατάσταση των δεδομένων με μηδέν (0) , κατά την δεύτερη με ένα (1) ενώ στο τελευταίο πέρασμα γίνεται εγγραφή με τυχαίο χαρακτήρα.

13. One Pass Zeros – Αποτελεί τη ταχύτερη μέθοδο οριστικής διαγραφής δεδομένων αφού περιλαμβάνει ένα πέρασμα κατά το οποίο γίνεται εγγραφή ολόκληρου του δίσκου με μηδενικά (0). Η μέθοδος αυτή λόγω της απλότητας και της ευχρηστίας της υποστηρίζεται σχεδόν από όλα τα εργαλεία οριστικής διαγραφής. Η μέθοδος αυτή θα χρησιμοποιηθεί και για τους σκοπούς της πειραματικής μελέτης σε αυτή τη διατριβή.

Πέραν των πιο πάνω μεθόδων υπάρχουν και αρκετές άλλες με παρόμοια γνωρίσματα τις οποίες θα αναφέρω απλώς ονομαστικά:

- US Air Force 5020
- German BSI
- Navso P-5329-26 RL
- Navso P-5329-26 MFM
- NATO standard
- Pfitzner Method
- NSA 130-1
- Pseudo-Random

# Κεφάλαιο 3
# Ιστορική Αναδρομή και Βιβλιογραφική Ανασκόπηση

Πιο κάτω πραγματοποιείται ιστορική αναδρομή και βιβλιογραφική ανασκόπηση σχετικά με τη μεταπτυχιακή διατριβή.

## 3.1 Ιστορική Αναδρομή Προηγούμενων Σχετικών Ερευνών

Στα προηγούμενα χρόνια εκτελέστηκαν πολυάριθμες μελέτες και πειραματικές έρευνες για τα εργαλεία οριστικής διαγραφής δεδομένων. Το γεγονός αυτό αποτελεί ακόμα ένα δείκτη της σημαντικότητας του συγκεκριμένου ερευνητικού πεδίου στην δικανική επιστήμη. Η ιστορική αναδρομή στις προηγούμενες σχετικές έρευνες στοχεύει στην επισκόπηση της εξέλιξης αυτών των εργαλείων, των μεθόδων και τεχνικών που χρησιμοποιούνται για την αξιολόγηση της αποτελεσματικότητας τους όπως επίσης και τις προκλήσεις που κλήθηκαν να αντιμετωπίσουν οι ερευνητές κατά τον έλεγχο της αξιοπιστίας τους. Η καταγραφή, μελέτη και κατανόηση του ιστορικού πλαισίου των προηγούμενων ερευνών μπορεί να βοηθήσει στην παρούσα διατριβή παρέχοντας χρήσιμες πληροφορίες για σημεία στα οποία υπάρχουν παραλήψεις και πρόσφορο

έδαφος για νέα έρευνα. Επίσης μπορεί να βοηθήσει σε μελλοντική έρευνα για ανάπτυξη πιο ισχυρών και ασφαλών εργαλείων οριστικής διαγραφής. Παρακάτω παρατίθενται κατά χρονολογική σειρά οι προηγούμενες σχετικές έρευνες που διεξήχθησαν σχετικά με τα εργαλεία μόνιμης διαγραφής.

| A/A | Research Paper Title | Authors | Year |
|---|---|---|---|
| **1** | Secure Deletion of Data from Magnetic and Solid-State Memory | Peter Gutmann | 1996 |
| **2** | Evaluating Commercial Counter-Forensic Tools | Matthew Geiger | 2005 |
| **3** | Overwriting Hard Drive Data: The Great Wiping Controversy | Craig Wright, Dave Kleiman, Shyaam Sundhar R.S | 2008 |
| **4** | Disposal of Disk and Tape Data by Secure Sanitization | Gordon Hughes, Tom Coughlin, Daniel M. Commins | 2009 |
| **5** | An Evaluation of Data Erasing Tools | Thomas Martin, Andrew Jones | 2011 |
| **6** | Identifying Trace Evidence from Target-Specific Data Wiping Application Software | Gregory H. Carlton, Gary C. Kessler | 2012 |
| **7** | Wiping techniques and anti-forensics methods | Miroslav Ölvecký, Darja Gabriška | 2018 |
| **8** | The Efficiency of Wiping Tools in Media Sanitization | M. Sahri, Siti Norul Huda Sheikh Abdulah, Mohd. Firham Efendy Md. Senan, Nooreen A. Yusof, Nor Z. Binti Zainal Abidin, N. Syahiran Bin Shaiful Azam, T. J. B. T. Ariffin | 2018 |
| **9** | Digital tool marks (DTMs): a forensic analysis of file wiping software | Graeme Horsman | 2019 |
| **10** | An Evaluation of Data Erasing Tools | Andrew Jones, Isaac Afrifa | 2020 |
| **11** | Forensic analysis of anti-forensic file-wiping tools on Windows | Rayed AlHarbi, Ali AlZahrani , Wasim Ahmad Bhat | 2021 |

**Πίνακας 3-1: Προηγούμενες σχετικές έρευνες κατά χρονολογική σειρά που διεξήχθησαν σχετικά με τα εργαλεία μόνιμης διαγραφής.**

Αξίζει να σημειωθεί ότι τα αποτελέσματα από τις πρώτες έρευνες που έχουν γίνει σε σχέση με τις πιο πρόσφατες διαφέρουν, αφού σύμφωνα με την πρωτοπόρο έρευνα του Peter Gutmann το

1996, Secure Deletion of Data from Magnetic and Solid-State Memory τα δεδομένα που έχουν αντικατασταθεί μία ή δύο φορές μπορούν να ανακτηθούν. Εξού και η ομώνυμη μέθοδος Peter Gutmann που υλοποιήθηκε από τον ίδιο περιλαμβάνει 35 συνολικά επαναλαμβανόμενες εγγραφές ώστε να διασφαλίσει την οριστική διαγραφή των δεδομένων. Αντίθετα σύμφωνα με τις τελευταίες μελέτες η απλή εφαρμογή της μεθόδου One Pass Zeros είναι αρκετή για διαγράψει μόνιμα τα δεδομένα. Αυτό οφείλεται στο γεγονός ότι η τεχνολογία των σκληρών δίσκων τα τελευταία χρόνια έχει αλλάξει με πιο σημαντικό επίτευγμα την αυξημένη πυκνότητα χωρητικότητας δεδομένων ανά περιοχή η οποία αναφέρεται στην ποσότητα δεδομένων που μπορούν να αποθηκευτούν σε μια μονάδα επιφάνειας των πλακών δίσκου μέσα στον σκληρό δίσκο. Η πυκνότητα έχει αυξηθεί δραματικά με τα χρόνια, από μερικές εκατοντάδες kilobits ανά τετραγωνική ίντσα τη δεκαετία του 1980 σε πολλαπλά terabit ανά τετραγωνική ίντσα στους σύγχρονους σκληρούς δίσκους (HDD). Αυτή η αυξημένη πυκνότητα κατέστη δυνατή μέσω των εξελίξεων στην επιστήμη των υλικών, στις διαδικασίες κατασκευής και στην τεχνολογία καταγραφής δεδομένων, όπως η χρήση κάθετης μαγνητικής εγγραφής (PMR), shingled magnetic recording (SMR) και μαγνητικής καταγραφής με θερμότητα (HAMR). Η αυξημένη πυκνότητα δεδομένων στους μοντέρνους δίσκους καθιστά τη μέθοδο ανάκτησης δεδομένων που χρησιμοποίησε ο Gutmann, MFM (Magnetic Force Microscopy) στα πειράματα του αναποτελεσματική. Αξιοσημείωτο επίσης είναι το γεγονός ότι στις προηγούμενες έρευνες που έχουν γίνει έχουν αξιολογηθεί πέραν των είκοσι (20) διαφορετικών εργαλείων οριστικής διαγραφής σε διαφορετικές εκδόσεις του λειτουργικού Windows.

## 3.2 Βιβλιογραφική Ανασκόπηση

Κατά τη βιβλιογραφική ανασκόπηση διεξήχθη μια εκτενής μελέτη σχετικά με τα εργαλεία οριστικής διαγραφής, το ιστορικό προηγούμενων παρόμοιων ερευνών και γενικά το τι κατάφερε να πετύχει και να παρουσιάσει μέχρι σήμερα η παγκόσμια επιστημονική κοινότητα. Ως κεντρικό άξονα μελέτης αποτέλεσαν άρθρα δημοσιευμένα σε διεθνή αναγνωρισμένα επιστημονικά περιοδικά, ιστοσελίδες οργανισμών, κεφάλαια από συναφή βιβλία και οδηγοί σχετικά με τη θεματολογία της διατριβής. Το κάθε επιμέρους άρθρο από αυτά παρουσιάζει ιδιαίτερο ενδιαφέρον αφού σε αυτά εκτελούνταν και παρουσιάζονταν ενναλακτικά σενάρια με χρήση ποικίλων εργαλείων και μεθόδων. Η μελέτη αυτών των ερευνών μου επέτρεψε να προσανατολιστώ ως προς την κατεύθυνση που θα έχει αυτή η διατριβή, όπως επίσης να εντοπίσω κάποιες παραλήψεις και αδυναμίες και απώτερο στόχο να αποφευχθούν. Γενικά στη μέχρι τώρα

βιβλιογραφία που μελετήθηκε, εκπονήθηκαν αρκετές σχετικές μελέτες οι οποίες εστιάζουν στα εργαλεία οριστικής διαγραφής, ποιες μεθόδους χρησιμοποιούν και πόσο αποτελεσματικά είναι.

Η βιβλιογραφία που μελετήθηκε συνοψίζεται στα ακόλουθα:

- Στο άρθρο "An Evaluation Of Data Erasing Tools"(Jones, 2020) των Andrew Jones και Isaac Afrifa γίνεται μια συνοπτική ονομαστική αναφορά στα διάφορα διεθνή πρότυπα διαγραφής δεδομένων χωρίς όμως να διευκρινίζει πώς ακριβώς οι αλγόριθμοι αυτοί λειτουργούν για την επανεγγραφή των δεδομένων. Ωστόσο κάνει λεπτομερή αναφορά και επεξηγεί τις μεθόδους επαναφοράς δεδομένων από σκληρούς δίσκους μέσω τριών άλλων εργαστηριακών μεθόδων που στις μέρες μας λόγω της πυκνότητας εγγραφής των δεδομένων στο δίσκο δεν είναι εφικτό να χρησιμοποιηθούν. Στη συνέχεια εστιάζει στην περιγραφή της πειραματικής διαδικασίας η οποία μέσα από τα αποτελέσματα διαφαίνεται να είναι αξιόπιστη και να ακολουθεί όλα τα πρωτόκολλα συλλογής, διαχείρισης και επεξεργασίας δεδομένων της δικανικής επιστήμης. Σημασία επίσης δίνεται και στην επεξήγηση της χρήσης των βοηθητικών μέσων που χρησιμοποιήθηκαν για την ανάλυση και αξιολόγηση των εργαλείων. Οι ερευνητές για τους σκοπούς της μελέτης επέλεξαν να αναλύσουν συνολικά 8 εργαλεία με ποικίλα και ενδιαφέροντα αποτελέσματα.

- Στο ομότιτλο άρθρο "An Evaluation Of Data Erasing Tools"(Martin & Jones, 2011) των Thomas Martin και Andrew Jones το οποίο έχει εκδοθεί μερικά χρόνια νωρίτερα, γίνεται μια παρόμοια επισκόπηση με το προηγούμενο άρθρο αλλά σε αυτή την περίπτωση τα εργαλεία που αξιολογούνται είναι διαφορετικά. Διαφορετική είναι επίσης και η πειραματική μεθοδολογία που ακολουθείται, όπως επίσης και τα εργαλεία ανάλυσης και αξιολόγησης που επέλεξαν να κάνουν χρήση. Η εργασία τους συνολικά είναι αρκετά καλά δομημένη και αυτό διαφαίνεται και στα αποτελέσματα των 12 εργαλείων που επέλεξαν να αξιολογήσουν.

- Μια διαφορετική προσέγγιση επέλεξε να ακολουθήσει ο ερευνητής Graeme Horsman στο άρθρο του "Digital tool marks (DTMs): a forensic analysis of file wiping software"(Horsman, 2021) . Η έρευνα του εστιάζεται στον αντίκτυπο που έχει η χρήση των εργαλείων οριστικής διαγραφής στα αρχεία συστήματος (file system) σε FAT32 και NTFS. Απώτερος στόχος της μελέτης είναι να εξετάσει την δυνατότητα εντοπισμού της χρήσης εργαλείων οριστικής διαγραφής και ταυτοποίηση πιθανών ιχνών μετά από χρήση τους.

Για την εκτέλεση του πειράματος και την εξαγωγή συμπερασμάτων χρησιμοποίησε συνολικά 8 εργαλεία οριστικής διαγραφής.

- Παρόμοια έρευνα με την πιο πάνω παρουσιάζεται στο άρθρο των Gregory H. Carlton και Gary C. Kessler με τίτλο "Identifying Trace Evidence from Target-Specific Data Wiping Application Software"(Carlton & Kessler, 2012) . Η μελέτη διεξήχθη σε 5 εργαλεία οριστικής διαγραφής και εστιάζει στον εντοπισμό ιχνών που παραμένουν στο σύστημα κατά την εκτέλεση αυτών των εφαρμογών. Στο άρθρο γίνεται ενδελεχής περιγραφή της μεθοδολογίας που ακολουθήθηκε, τα κριτήρια που τέθηκαν για την επιλογή των υποψήφιων προς ανάλυση εργαλείων καθώς επίσης και παρουσίαση των ευρημάτων και η σημασία αυτών στη αντί-δικανική έρευνα γενικότερα.

- Στο άρθρο "Forensic analysis of anti-forensic file-wiping tools on Windows"(*AlHarbi* , 2021) των Rayed AlHarbi, Ali AlZahrani και Wasim Ahmad παρουσιάζεται μια δικανική ανάλυση σε 4 αντι-δικανικά εργαλεία οριστικής διαγραφής σε περιβάλλον λειτουργικού συστήματος Windows. Η διαγραφή των αρχείων έγινε στα τρία αρχεία συστήματος (file systems) FAT32 , exFat και NTFS. Στόχος της ήταν να καταδείξει εάν η ανάλυση σε συστήματα όπου έγινε η χρήση των εργαλείων έχει την δυνατότητα να παρέχει στοιχεία σχετικά με το εργαλείο που χρησιμοποιήθηκε και τα δεδομένα που διαγράφηκαν.

- Το άρθρο των Miroslav Ölvecký και Darja Gabriška με τίτλο "Wiping techniques and anti-forensics methods"(Olvecky & Gabriska, 2018) εξετάζει καθαρά το θεωρητικό υπόβαθρο των εργαλείων οριστικής διαγραφής και εστιάζει στην ορολογία, τις τεχνικές και τα πρότυπα που ακολουθούνται κατά την διαδικασία της ασφαλούς διαγραφής πληροφοριών. Παρέχει επίσης υπόδειγμα μεθοδολογίας επισκόπησης των εργαλείων οριστικής διαγραφής που συστήνεται να ακολουθηθεί σε σχετικές αξιολογήσεις.

- Το άρθρο των Craig Wright, Dave Kleiman και Shyaam Sundhar με τίτλο "Overwriting Hard Drive Data: The Great Wiping Controversy "(Wright et al., 2008) μετά από μια σειρά δοκιμών και υποθέσεων εξετάζει κατά πόσο τα δεδομένα μπορούν να ανακτηθούν μετά από μια πετυχημένη διαδικασία οριστικής διαγραφής ακόμα και με τη χρήση MFM ( Magnetic Force Microscopy) ή άλλων γνωστών μεθόδων ανάκτησης δεδομένων.

- Το άρθρο του Matthew Geiger με θέμα "Evaluating Commercial Counter-Forensic Tools" (Geiger, 2005) αξιολογεί την απόδοση 6 εργαλείων οριστικής διαγραφής και εστιάζει σε

διάφορες λειτουργικές αδυναμίες τους που έχουν σαν αποτέλεσμα την δυνατότητα επαναφοράς σημαντικού αριθμού διαγραμμένων δεδομένων.

- Στο βιβλίο του George Kostopoulos με θέμα "Cyberspace and Cybersecurity"(Kostopoulos, 2017) γίνεται εκτενής αναφορά στους αλγόριθμους οριστικής διαγραφής που χρησιμοποιούν οι συγκεκριμένες εφαρμογές. Ο συγγραφέας απαριθμεί συνολικά 16 αλγορίθμους και περιγράφει αναλυτικά τον τρόπο που εφαρμόζονται. Η κάθε μέθοδος ξεχωρίζει ως προς τον αριθμό των επαναλήψεων στις εγγραφές bit στον δίσκο καθώς επίσης και στο είδος του χαρακτήρα που επιλέγει να γράψει. Σε άλλες πηγές από το διαδίκτυο οι αλγόριθμοι / μέθοδοι παρουσιάζονται να είναι περισσότεροι ωστόσο η φιλοσοφία πίσω από τη λειτουργία τους παραμένει η ίδια.

- Σύμφωνα με τον οδηγό που δημοσίευσε ο NIST, Special Publication 800-88 rev.1 , "Guidelines for Media Sanitization" σχετικά με την διαδικασία διαχείρισης των δεδομένων σε μονάδες αποθήκευσης, μεταξύ άλλων περιγράφονται και τα τρία επίπεδα διαγραφής δεδομένων από σκληρούς δίσκους. Το κάθε επίπεδο από αυτά χαρακτηρίζεται από πλεονεκτήματα και μειονεκτήματα ανάλογα πάντοτε από τη διαβάθμιση των δεδομένων που βρίσκονται αποθηκευμένα και από την πολιτική που διέπει τον κάθε οργανισμό. Τα 3 επίπεδα που εφαρμόζονται στις περιπτώσεις σκληρών δίσκων είναι τα ακόλουθα:
  1. Clear
  2. Purge
  3. Destroy

  Σε συνέχεια των πιο πάνω ο NIST (National Institute of Standards and Technology , US) χαρακτηρίζει μη αποδεκτές μεθόδους οριστικής διαγραφής δεδομένων τις ακόλουθες.

  1. Διαγραφή αρχείου - Το λειτουργικό σύστημα διαγράφει τους δείκτες προς τα διαγραμμένα αρχεία και ο χώρος που καταλαμβάνουν γίνεται πλέον διαθέσιμος για εγγραφή νέων δεδομένων. Μέχρι όμως να γίνει αυτό, τα δεδομένα παραμένουν αποθηκευμένα αναλλοίωτα και με τα κατάλληλα εργαλεία μπορούν να ανακτηθούν.

  2. Μορφοποίηση (Format) Δίσκου – Η πεποίθηση ότι κατά την μορφοποίηση αφαιρούνται τα δεδομένα ενός δίσκου είναι εσφαλμένη. Στην πραγματικότητα αυτό που συμβαίνει είναι το καθάρισμα ή διαφορετικά η αρχικοποίηση του συστήματος αρχείων (file system) του δίσκου. Τα δεδομένα συνεχίζουν να βρίσκονται ορφανά

στα διάφορα τμήματα (sectors) του δίσκου και σχετικά εύκολα μπορούν να ανακτηθούν.

3. Διαμερισματοποίηση Δίσκου ( Disk Partitioning ) – Κατά την διαδικασία του disk partitioning καθορίζονται τα στοιχεία που αφορούν τη κατανομή του μεγέθους και οι περιοχές που καταλαμβάνουν τα διάφορα τμήματα ενός δίσκου. Η διαδικασία αυτή είναι σημαντική καθώς με αυτό το τρόπο ο δίσκος αναγνωρίζεται από το λειτουργικό σύστημα. Ωστόσο η διαδικασία καθορισμού της νέας δομής απαιτεί μόνο μερικές επανεγγραφές στο δίσκο αφήνοντας έτσι τα προηγούμενα δεδομένα που ήταν ήδη γραμμένα άθικτα άρα και ανακτήσιμα.

4. Κρυπτογράφηση – Οι τεχνικές κρυπτογράφησης αποτελούν ιδανικό εργαλείο για διασφάλιση της ασφάλειας των δεδομένων. Δεν μπορούν όμως να χαρακτηριστούν ως μια αποδεκτή μέθοδος διαγραφής δεδομένων από τη στιγμή που τα δεδομένα διατηρούνται έστω και κρυπτογραφημένα.

- Στο άρθρο των Robert Winter και Kroll Ontrack με τίτλο SSD vs HDD(Winter, 2013) – data recovery and destruction γίνεται μια σύγκριση μεταξύ των δύο δημοφιλών μέσων αποθήκευσης και παρουσιάζεται ο τρόπος με τον οποίο λειτουργεί η κάθε τεχνολογία. Σκοπός του είναι να τονίσει τις προκλήσεις που προκύπτουν σχετικά με την μόνιμη διαγραφή αρχείων σε δίσκους SSDs . Αυτό οφείλεται στο γεγονός ότι αντίθετα με τους συμβατικούς μαγνητικούς δίσκους (HDD) τα εργαλεία οριστικής διαγραφής στους SSD δεν ελέγχουν σε πιο μέρος του δίσκου θα γραφτεί η νέα πληροφορία. Έτσι πιθανόν μέρη του δίσκου όπου βρίσκονται γραμμένα δεδομένα να προσπεραστούν χωρίς να γίνει καμία νέα εγγραφή σε αυτά. Αυτό οφείλεται στον τρόπο με τον οποίο λειτουργούν οι SSDs ώστε να αυξηθεί η διάρκεια ζωής τους. Επίσης να αναφέρουμε ότι αρκετοί κατασκευαστές SSDs παρέχουν τις δικές τους λύσεις για την διαγραφή των δεδομένων από τους δίσκους τους χωρίς να ακολουθείται μια ενιαία κοινή αποδεκτή από όλους μεθοδολογία.

## 3.3 Συνοπτικός πίνακας σύγκρισης προηγούμενων σχετικών άρθρων

Πιο κάτω παρουσιάζονται οι προηγούμενες σχετικές έρευνες που έχουν γίνει για Εργαλεία Οριστικής Διαγραφής Δεδομένων και μελετήθηκαν στα πλαίσια αυτής της Διατριβής.

| Α/Α | Τίτλος Άρθρου | Συγγραφέας | Έτος | Μέθοδος | Αριθμός Εργαλείων | Μέθοδος Διαγραφής | Κύρια Ευρήματα | Περιορισμοί | Προβήματα που Διαπιστώθηκαν |
|---|---|---|---|---|---|---|---|---|---|
| **1** | Evaluating Commercial Counter-Forensic Tools | Matthew Geiger | 2005 | Πειραματική | 6 | One Time Pass (Zero or Random Not specified) | Όλα τα εργαλεία που δοκιμάστηκαν άφησαν πίσω ίχνη δεδομένων σημαντικής αξίας για ένα δικανικό ερευνητή | Περιορισμένος αριθμός δεδομένων για διαγραφή | Το άρθρο δεν παρέχει μια λεπτομερή περιγραφή της μεθοδολογίας για την αξιολόγηση αυτών των εργαλείων, η οποία μπορεί να περιορίσει την ικανότητα αναπαραγωγής ή γενίκευσης των ευρημάτων. |
| **2** | An evaluation of data erasing tools | Thomas Martin, Andrew Jones | 2011 | Πειραματική | 12 | DoD 5220.22, Single pass | Από τα 12 εργαλεία που δοκιμάστηκαν, 7 από αυτά έχουν αποτύχει να διαγράψουν πλήρως τα δεδομένα | Κάποια από τα εργαλεία μπορούν να διαγράψουν αρχεία, ενώ άλλα ολόκληρο το δίσκο | Ασυνέπεια στον αλγόριθμο που έγινε χρήση για την επανεγγραφή των δεδομένων. |
| **3** | Identifying Trace Evidence from Target-Specific Data Wiping Application Software | Gregory H. Carlton Gary C. Kessler | 2012 | Πειραματική | 5 | Δεν προσδιορίζεται | Διαπιστώθηκε ότι όλα τα εργαλεία οριστικής διαγραφής δεδομένων αφήνουν κάποια ίχνη που μπορεί να είναι πολύτιμα για τους ψηφιακούς δικανικούς ερευνητές. | Περιορισμένοι πόροι, περιορισμένος αριθμός δεδομένων για διαγραφή, χρονικοί περιορισμοί. Αξιολόγηση εργαλείων μόνο για διαγραφή αρχείων και όχι ολόκληρου του δίσκου. | Απροσδιόριστος τρόπος διαγραφής των δεδομένων. |

| Α/Α | Τίτλος Άρθρου | Συγγραφέας | Έτος | Μέθοδος | Αριθμός Εργαλείων | Μέθοδος Διαγραφής | Κύρια Ευρήματα | Περιορισμοί | Προβήματα που Διαπιστώθηκαν |
|---|---|---|---|---|---|---|---|---|---|
| **4** | Digital tool marks (DTMs): a forensic analysis of file wiping software | Graeme Horsman | 2019 | Πειραματική | 8 | Single pass, two pass, DoD 5220-22.M, Gutman | Επτά εργαλεία παρουσίασαν αξιοσημείωτα ευρήματα μετά τη διαγραφή τα οποία μπορούν να χρησιμοποιηθούν για να διαπιστωθεί ότι πραγματοποιήθηκε διαγραφή και να γίνει σύνδεση με συγκεκριμένο εργαλείο. | Περιορισμένος αριθμός δεδομένων για διαγραφή (6 αρχεία), Αξιολόγηση εργαλείων μόνο για διαγραφή αρχείων και όχι ολόκληρου του δίσκου. | Ασυνέπεια στον αλγόριθμο που έγινε χρήση για την επανεγγραφή των δεδομένων. |
| **5** | An Evaluation Of Data Erasing Tools | Andrew Jones Isaac Afrifa | 2020 | Πειραματική | 8 | One Pass Zero | Μερικά εργαλεία διάγραψαν εντελώς ολόκληρο το δίσκο, συμπεριλαμβανομένου του boot sector. Άλλα εργαλεία επίσης διάγραψαν το δίσκο εξαιρουμένου του boot sector, ενώ ένα εργαλείο απέτυχε να διαγράψει τα ονόματα των αρχείων. | Περιορισμένος αριθμός δεδομένων για διαγραφή(9GB), Αξιολογήθηκε η ικανότητα των εργαλείων μόνο στην οριστική διαγραφή ολόκληρου του δίσκου. | - |

**Πίνακας 3-2: Συνοπτικός πίνακας σύγκρισης εργαλείων, που μελετήθηκαν στα άρθρα**

# Κεφάλαιο 4
# Μεθοδολογία

Για τους σκοπούς αξιολόγησης των εργαλείων οριστικής διαγραφής υλοποιήθηκε προσεκτικά η πειραματική διαδικασία που περιγράφεται πιο κάτω. Κατά το στάδιο του σχεδιασμού της λήφθηκαν υπόψη τα βασικά ερευνητικά ερωτήματα καθώς επίσης και διάφοροι περιορισμοί που προέκυψαν από τα συμπεράσματα μελέτης της βιβλιογραφίας. Σύμφωνα λοιπόν με αυτά:

1. Η πειραματική διαδικασία θα επικεντρωθεί στο πρώτο επίπεδο διαγραφής δεδομένων από σκληρούς δίσκους κατά το NIST (Clear). Αυτό συνεπάγεται χρήση εργαλείων τα οποία έχουν ως βασική αρχή λειτουργίας τους την επανεγγραφή δεδομένων στα ως προς διαγραφή τμήματα του δίσκου ώστε να καταστεί αδύνατη η ανάκτηση τους. Σύμφωνα λοιπόν με αυτή τη παράμετρο οδηγούμαστε σε αυτόματο αποκλεισμό εργαλείων οριστικής διαγραφής που χρησιμοποιούν εντολές που βρίσκονται στο firmware του εκάστοτε δίσκου, σε τεχνικές απομαγνητισμού του δίσκου ή στη φυσική καταστροφή του υλικού του δίσκου. Αυτό γίνεται ώστε τα συμπεράσματα που θα εξάγουμε να είναι γενικευμένα για το σύνολο των δίσκων και όχι συγκεκριμένα για συσκευές συγκεκριμένου κατασκευαστή.

2. Θα χρησιμοποιηθεί καινούργιος συμβατικός μαγνητικός σκληρός δίσκος (HDD) μεγέθους 250GB του οποίου η "υγεία" θα εξετάζεται πριν από κάθε επανάληψη με κατάλληλο εργαλείο (CrystalDiskInfo). Σκοπός του είναι ο εντοπισμός bad sectors που θα οδηγήσουν σε λανθασμένες εγγραφές και εσφαλμένα αποτελέσματα στην αξιολόγηση τους. Η διαδικασία αυτή θεωρείται αναγκαία υπό τις περιστάσεις, αφού οι συνεχόμενες και επαναλαμβανόμενές εγγραφές μεγάλου όγκου δεδομένων σε όλα τα τμήματα του δίσκου πιθανόν να δημιουργήσουν φθορά και αλλοίωση του. Η επιλογή του HDD ως μέσο διεξαγωγής των πειραμάτων αξιολόγησης είναι μονόδρομος αφού μελετώντας τη βιβλιογραφία και συγκεκριμένα το άρθρο 11, "SSD vs HDD – data recovery and destruction " συμπεραίνουμε ότι η οριστική διαγραφή δεδομένων από μονάδες SSD παρουσιάζει ιδιαίτερες προκλήσεις που θα πρέπει να εξεταστούν με διαφορετική προσέγγιση. Τα κλασικά εργαλεία οριστικής διαγραφής – αντικείμενο μελέτης αυτής της διατριβής- που έχουν ως αρχή τους την επανεγγραφή δεδομένων στο δίσκο, στις περιπτώσεις των SSD κρίνονται μη αποτελεσματικά. Αντίθετα ο συγκεκριμένος τρόπος λειτουργίας τους μειώνει δραματικά το χρόνο ζωής τους.

3. Η χρήση εικονικής μηχανής (virtual machine), παρόλο που θα χρησιμοποιηθεί, περιορίζεται μόνο κατά την φάση της ανάλυσης. Δηλαδή η εικόνα που θα ληφθεί από το φυσικό δίσκο (HDD) με τη βοήθεια του AccessData FTK Imager θα μεταφερθεί σε εικονικό μηχάνημα που θα τρέχει λειτουργικό Kali Linux για ανάλυση με συγκεκριμένα εργαλεία δικανικής. Η διεξαγωγή της διαδικασίας διαγραφής των δεδομένων θα γίνεται απευθείας στο φυσικό μέσο. Η απόφαση αυτή λήφθηκε για τους πιο κάτω λόγους:

    α. Να περιοριστούν στο μέγιστο βαθμό οι παράμετροι που πιθανόν να επηρεάσουν τα αποτελέσματα της αξιολόγησης. Σύμφωνα με το άρθρο 13, The Forensic Effectiveness of Virtual Disk Sanitization,(Sablatura & Karabiyik, 2016) οι ερευνητές εντόπισαν σε εικονικές μηχανές ίχνη δεδομένων που ανήκουν στο host machine. Ένα τέτοιο ενδεχόμενο σίγουρα θα επηρεάσει σε κάποιο βαθμό τα αποτελέσματα της αξιολόγησης και ο τρόπος αντιμετώπισής του είναι να εκτελεστεί η διαγραφή απευθείας στο φυσικό μέσο.

    β. Κατά τη δημιουργία μιας εικονικής μηχανής δημιουργείται ταυτόχρονα ένας εικονικός δίσκος (virtual hard disk) ο οποίος ουσιαστικά καταλαμβάνει ένα χώρο από το φυσικό δίσκο που εμείς του ορίσαμε. Ο χώρος αυτός χρησιμοποιείται από την εικονική μηχανή για αποθήκευση των δεδομένων που κάνει χρήση. Σε αυτή την περίπτωση δεν έχουμε

έλεγχο στο χώρο εκτός της περιοχής αυτής έτσι τα εργαλεία που θα εκτελούνται θα διαγράφουν δεδομένα μόνο στην περιοχή αυτή. Το υπόλοιπο μέρος του φυσικού δίσκου θα μένει ανέπαφο έτσι στη συνέχεια κατά την ανάλυση του δίσκου να εμφανίζονται δεδομένα που πιθανόν να βρίσκονταν εκτός της περιοχής του εικονικού δίσκου και δεν έτυχαν οποιασδήποτε επεξεργασίας από τα εργαλεία οριστικής διαγραφής που εκτελέστηκαν.

γ. Επιμέρους στόχοι έχουν επίσης τεθεί σχετικά με την απόδοση των εργαλείων σε κατανάλωση πόρων του συστήματος, υπολογιστική ισχύ και χρόνο αποπεράτωσης των εργασιών. Μια εικονική μηχανή μοιράζεται τους πόρους της με τον υπολογιστή που την φιλοξενεί. Έτσι με τους περιορισμένους πόρους που θα έχει στη διάθεση της η εικονική μηχανή, τα εργαλεία οριστικής διαγραφής που θα αξιολογούνται να μην ανταποκρίνεται όπως πραγματικά θα έπρεπε.

δ. Η ανάλυση εικονικών δίσκων για εύρεση δεδομένων σχετιζόμενων με τον host υπολογιστή και γενικότερα εικονικών μηχανών θα μπορούσε να αποτελέσει ξεχωριστό θέμα για μεταπτυχιακή διατριβή.

Κύριο μέλημα μας ήταν η δημιουργία μιας πειραματικής αξιολόγησης που να εξετάζει όλα τα σενάρια που συντάχθηκαν αρχικά και να καλύπτει επαρκώς όλους τους στόχους που τέθηκαν. Όλα τα βήματα της διαδικασίας που προσεκτικά επιλέγηκαν αποσκοπούν στο σχεδιασμό μιας διαδικασίας που να είναι αξιόπιστη, μη αμφισβητήσιμη και να ακολουθεί όλα τα πρότυπα συλλογής και επεξεργασίας δεδομένων της δικανικής επιστήμης.

## 4.1 Παρουσίαση Εξοπλισμού και Εργαλείων που Χρησιμοποιήθηκαν

Τα πειράματα θα εκτελούνται σε υπολογιστή Desktop με τα ακόλουθα τεχνικά χαρακτηριστικά:

1. Λειτουργικό σύστημα

| | |
|---|---|
| **Edition** | Windows 10 Pro |
| **Version** | 21H2 |
| **OS build** | 19044.2251 |

2. Hardware

| **Επεξεργαστής** | Intel(R) Core (TM) i5-6600K CPU @ 3.50GHz |
|---|---|
| **Μνήμη RAM** | 16.0 GB |
| **Κάρτα Γραφικών** | NVIDIA GeForce GTX 1060 6GB |
| **System Drive** | XPG GAMMIX S50 Lite SSD (1TB) |
| **Storage Drive** | Seagate Barracuda ST250DM000 (250GB) |
| **Τύπος Συστήματος** | 64-bit operating system, x64-based processor |

Ο σκληρός δίσκος (HDD) που θα διεξάγονται οι δοκιμές διαγραφής δεδομένων είναι ο Seagate Barracuda ST250DM000 μεγέθους 250GB σε απευθείας σύνδεση με τη μητρική χρησιμοποιώντας καλώδιο SATA. Ο δίσκος αγοράστηκε καινούργιος για τους σκοπούς των πειραματικών δοκιμών. Η επιλογή του συγκεκριμένου μεγέθους δίσκου έγινε ώστε να εξυπηρετεί τους σκοπούς των δοκιμών ενώ παράλληλα να μην καθιστά ιδιαίτερα χρονοβόρα τη όλη διαδικασία δεδομένου ότι η διαγραφές των δεδομένων θα επαναληφθούν αρκετές φορές. Σε περίπτωση επιλογής δίσκου μεγαλύτερης χωρητικότητας πχ >1TB θα απαιτείτο ακόμα και με την μέθοδο επανεγγραφής one pass zero τεράστιος χρόνος αναμονής, χωρίς ωστόσο κάποιο ιδιαίτερο όφελος στα συνολικά αποτελέσματα.

**Εικόνα 4-1: Seagate Barracuda ST250DM000**

| **General** | |
|---|---|
| Model Number | ST250DM0002 |
| Capacity | 250GB |
| Interface | SATA 6Gb/s NCQ |

| **Performance** | |
|---|---|
| Spindle Speed (RPM) | 7200 |
| Cache, Multisegmented (MB) | 16 |
| SATA Transfer Rates (Gb/s) | 6.0/3.0/1.5 |
| Seek Average, Read (ms) | <11 |
| Seek Average, Write (ms) | <12 |
| Average Data Rate, Read/Write (MB/s) | 125 |
| Max Sustained Data Rate, OD Read (MB/s) | 144 |
| **Configuration/Organization** | |
| Heads/Disks | 1/1 |
| Bytes per Sector | 512 |
| **Voltage** | |
| Voltage Tolerance, Including Noise (5V) | +10%/–5.0% |
| Voltage Tolerance, Including Noise (12V) | +10%/–7.5% |
| **Reliability/Data Integrity** | |
| Contact Start/Stop Cycles | 50,000 |
| Nonrecoverable Read Errors per Bits Read, Max | 1 per 10E14 |
| Annualized Failure Rate (AFR) | <1% |
| Power-On Hours | 2400 |
| **Power Management** | |
| Startup Power (A) | 2.0 |
| Operating Mode, Typical (W) | 6.19 |
| Idle Average (W) | 4.60 |
| Standby Mode (W) | 0.79 |
| Sleep Mode (W) | 0.79 |
| **Temperature** | |
| Operating (ambient min °C) | 0 |
| Operating (drive case max °C) | 60 |
| Nonoperating (ambient °C) | –40 to 70 |
| **Physical** | |
| Height (mm) | 19.98 |
| Width (mm) | 101.6 |
| Weight (g) | 415/ |

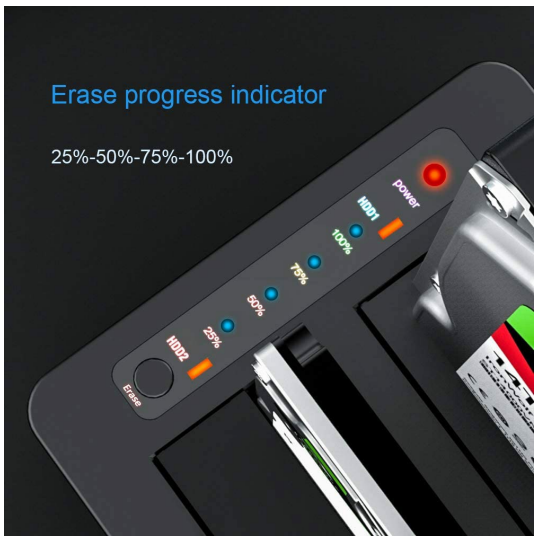
**Πίνακας 4-1: Χαρακτηριστικά Σκληρού Δίσκου(*Seagate Barracuda Data Sheet.Pdf*, n.d.)**

Παράλληλα με το σκληρό δίσκο για τη διεξαγωγή των πειραμάτων θα χρησιμοποιηθεί και η συσκευή GLOTRENDS 2-in-1 SATA Hard Drive Eraser and USB 3.0 HDD Docking Station .


**Εικόνα 4-2: GLOTRENDS 2-in-1 SATA Hard Drive Eraser and USB 3.0 HDD Docking Station**

Πρόκειται για μια συσκευή με αρκετές δυνατότητες, οι οποίες θα φανούν ιδιαίτερά χρήσιμες κατά την εκτέλεση των δοκιμών. Καταρχάς μπορεί να λειτουργήσει ως βάση για να συνδέσεις τον προς εξέταση σκληρό δίσκο στον υπολογιστή μέσω διεπαφής USB 3.0. Το γεγονός αυτό μας δίνει την ευχέρεια για γρήγορη προσθήκη και αφαίρεση του εξεταζόμενου δίσκου από το σύστημα εξοικονομώντας έτσι αρκετό χρόνο μιας και η διαδικασία απαιτεί αρκετές επαναλήψεις. Ακόμα ένα σημαντικό πλεονέκτημα της χρήσης της συσκευής είναι ότι η κατά την σύνδεση της με τον υπολογιστή διαμέσου θύρας USB θα διαμεσολαβήσει εφαρμογή Write Blocking USB ώστε να διασφαλιστεί ότι τα δεδομένα που βρίσκονται σε αυτόν δεν θα τύχουν οποιασδήποτε τροποποίησης. Αυτή η ενέργεια μας θα ενισχύσει την αξιοπιστία της πειραματικής διάταξης αφού θα διασφαλιστεί ότι τα δεδομένα από το δίσκο παραμένουν ανέπαφα.

Η δεύτερη σημαντική δυνατότητα που μας παρέχει η συσκευή είναι η ικανότητα της να λειτουργήσει ανεξάρτητα από οποιανδήποτε εφαρμογή, εργαλείο ή λειτουργικό σύστημα και να διαγράψει τα δεδομένα του δίσκου.




**Εικόνα 4-3: Standalone Eraser**

Η διαγραφή υλοποιείται δια μέσου του hardware της συσκευής και για αυτό ακριβώς το λόγο κατά την διαδικασία αυτή δεν χρειάζεται το καλώδιο USB να είναι συνδεδεμένο με τον υπολογιστή. Σύμφωνα με τον κατασκευαστή έχει ικανότητα διαγραφής 6Gbps και η μέθοδος διαγραφής που κάνει χρήση είναι το ένα πέρασμα με μηδενικά (one-time overwriting of "0"). Η χρήση της δυνατότητας αυτής θα περιοριστεί κατά την φάση της αρχικοποίησης του δίσκου. Δηλαδή στην αρχή κάθε πειραματικής δοκιμής όπου απαιτείται να έχουμε ένα πραγματικά κενό δίσκο ώστε να του μεταφορτώσουμε τα δεδομένα προς διαγραφή. Θα ήταν οξύμωρο να βασιζόμαστε στη ολική διαγραφή και αρχικοποίηση του δίσκου για ετοιμασία τοποθέτησης των αρχείων σε κάποιο λογισμικό εργαλείο ολικής διαγραφής δεδομένων από τη στιγμή που το πεδίο έρευνας της διατριβής είναι η εξέταση αξιοπιστίας αυτών των εργαλείων.

| **General** | |
|---|---|
| Brand | GLOTRENDS |
| Model | BE2 |
| Number of Drives | 2 |
| Drive Size | 2.5 in & 3.5in |
| Interface | USB 3.0 |
| Compatible Drive Types | SATA |
| Drive Installation | Removable |
| Fan(s) | No |
| **Performance** | |
| Maximum Data Transfer Rate | 3Gbps |
| Type and Rate | USB 3.0 - 5 Gbit/s |

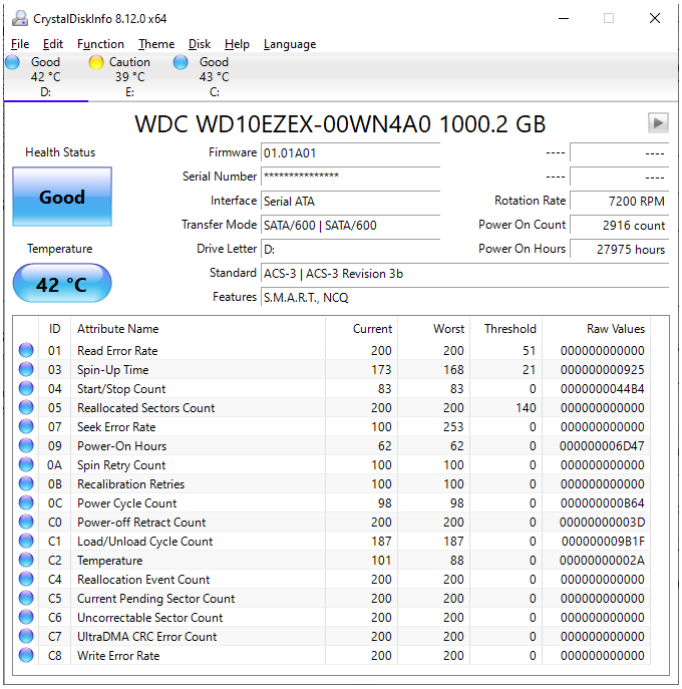
| | |
|---|---|
| Duplication Modes | Sector by Sector |
| Duplication Speed | 11GBpm |
| Erase Modes | 1-Pass Zero Overwrite |
| **Connector(s)** | |
| Drive Connectors | 2 - SATA Data & Power (7+15 pin) |
| Host Connectors | 1 - USB 3.0 |
| **Software** | |
| OS Compatibility | OS independent.<br>No software or drivers required |
| **Power** | |
| Power Source | AC Adapter |
| Input Voltage | 12V DC |
| Input Current | 1.2A |
| Output Voltage | 12V DC |
| Output Current | 3000mA |
| Power Consumption (Watts) | 36 |
| **Environmental** | |
| Operating Temperature | 0°C to 85°C |
| Storage Temperature | -10°C to 95°C |
| Humidity | 5-90% |
| **Physical** | |
| Color | Black |
| Length(cm) | 12.8 |
| Width(cm) | 10.3 |
| Height(cm) | 6.2 |
| Weight(g) | 424.0 |

**Πίνακας 4-2: Χαρακτηριστικά συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser and USB 3.0 HDD Docking Station**

Κατά την διαδικασία των πειραματικών δοκιμών θα γίνει χρήση των ακόλουθων εργαλείων, των οποίων η χρήση περιγράφεται πιο κάτω.

1. CrystalDiskInfo (*CrystalDiskInfo - Website [En]*, 2018) – Είναι ένα ισχυρό εργαλείο που διανέμετε δωρεάν και επιτρέπει στους χρήστες να παρακολουθούν την κατάσταση και την απόδοση των διαφόρων αποθηκευτικών μέσων που βρίσκονται ανά πάσα στιγμή

συνδεδεμένα στον υπολογιστή τους. Υποστηρίζει ένα ευρύ φάσμα τύπων διεπαφής, συμπεριλαμβανομένων των SATA, SAS, USB και NVMe καθώς και όλους τους τύπους αποθηκευτικών μέσων συμπεριλαμβανομένων των δίσκων HDD και SSD. Παρέχει λεπτομερή ανάλυση των λειτουργιών τους και παρουσιάζει μέσω του εύχρηστου γραφικού περιβάλλοντος διάφορες μετρήσεις και στατιστικά στοιχεία με τη χρήση S.M.A.R.T ((Self-Monitoring, Analysis, and Reporting Technology) δεδομένων.




**Εικόνα 4-4: CrystalDiskInfo**

Εκτός από την παρακολούθηση της υγείας των συσκευών αποθήκευσης, το CrystalDiskInfo παρέχει επίσης πληροφορίες σχετικά με την έκδοση firmware, τον σειριακό αριθμό, τον τύπο διεπαφής της συσκευής καθώς επίσης πληροφορίες όπως της θερμοκρασίας, του χρόνου χρήσης του και του συνολικού αριθμού κατεστραμμένων τομέων(bad sectors). Μία από τις βασικές δυνατότητες του CrystalDiskInfo είναι η ικανότητά του να εντοπίζει πιθανά προβλήματα στις συσκευές αποθήκευσης προτού γίνουν κρίσιμα. Το περιβάλλον εργασίας χρήστη του CrystalDiskInfo είναι απλό και εύκολο στην πλοήγηση, καθιστώντας το ακόμη και σε χρήστες με ελάχιστες τεχνικές γνώσεις προσβάσιμο. Η γενική κατάσταση υγείας του δίσκου αντιπροσωπεύεται με βάση τα αντίστοιχα χρώματα που παρουσιάζονται πιο κάτω.

| Health Status | Color | Description |
|---|---|---|
| Good | Blue |   |
| Caution | Yellow |   |
| Bad | Red |   |
| Unknown | Gray |   |

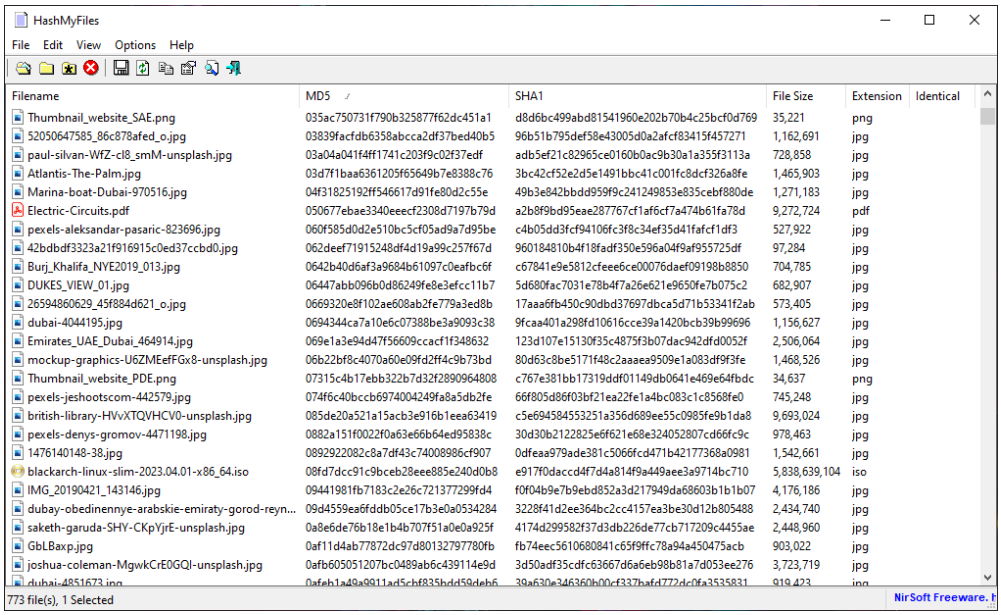
**Πίνακας 4-3: Ενδείξεις κατάστασης υγείας σκληρών δίσκων (HDD)**

Το εργαλείο παρέχει επίσης προσαρμογή, επιτρέποντας στους χρήστες να προγραμματίζουν ειδοποιήσεις για συγκεκριμένα συμβάντα, όπως μια απότομη αύξηση της θερμοκρασίας ή κατά τον εντοπισμό κατεστραμμένων τομέων.

Στην περίπτωση των δοκιμών που θα πραγματοποιήσουμε λόγω των πολλαπλών εγγραφών και επαναλήψεων που θα γίνονται στο δίσκο πιθανόν να δημιουργηθούν bad sectors τα οποία να αλλοιώσουν τα αποτελέσματα και τις αξιολογήσεις των εργαλείων. Σε περίπτωση που μέσω του CrystalDiskInfo έχουμε ενδείξεις ότι ο δίσκος βρίσκεται σε κακή κατάσταση πιθανόν να χρειαστεί αντικατάσταση.

2. HashMyFiles (*HashMyFiles*, 2023) - Το HashMyFiles είναι ένα δωρεάν, ελαφρύ και εύχρηστο εργαλείο που επιτρέπει τη δημιουργία και επαλήθευση της ακεραιότητας των αρχείων χρησιμοποιώντας διάφορους αλγόριθμους κατακερματισμού. Αναπτύχθηκε από τη NirSoft, το HashMyFiles προσφέρει μια ποικιλία από χρήσιμες λειτουργίες μεταξύ των οποίων η δημιουργία τιμών κατακερματισμού ενός ή περισσοτέρων αρχείων ταυτόχρονα. Το εργαλείο υποστηρίζει αρκετούς δημοφιλείς αλγόριθμους κατακερματισμού, συμπεριλαμβανομένων των MD5, SHA-1, SHA-256, SHA-384 και SHA-512, μεταξύ άλλων. Οι κατακερματισμένες τιμές μπορούν να παρουσιαστούν σε δεκαεξαδική μορφή ή σε base64. Μία από τις πιο σημαντικές λειτουργίες του HashMyFiles είναι η δυνατότητα σύγκρισης των τιμών κατακερματισμού δύο ή περισσοτέρων αρχείων για να

προσδιοριστεί εάν είναι πανομοιότυπα ή όχι. Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη για την επαλήθευση της ακεραιότητας των ληφθέντων αρχείων, διασφαλίζοντας ότι δεν έχουν καταστραφεί ή τροποποιηθεί με οποιονδήποτε τρόπο κατά τη διαδικασία λήψης. Επίσης επιτρέπει στους χρήστες να αποθηκεύουν τις παραγόμενες τιμές κατακερματισμού σε ένα αρχείο, το οποίο μπορεί να είναι χρήσιμο για μελλοντική αναφορά ή για κοινή χρήση με άλλους. Για τους πιο προχωρημένους χρήστες υπάρχει και η δυνατότητα χρήσης του προγράμματος μέσω γραμμής εντολών.




**Εικόνα 4-5: HashMyFiles**

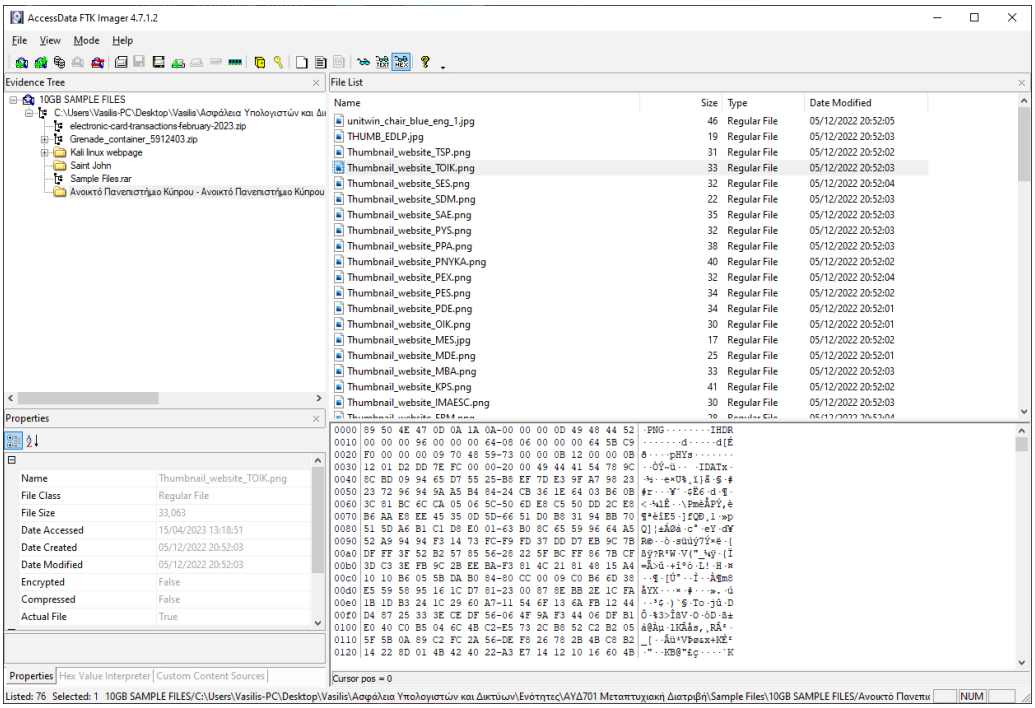
Τις δυνατότητες του εργαλείου θα τις αξιοποιήσουμε κατά την διεξαγωγή της αξιολόγησης των εργαλείων διαγραφής στις πιο κάτω περιπτώσεις:

α. Μετά την εισαγωγή των προς διαγραφή δεδομένων στο δίσκο, θα δημιουργήσουμε την κατακερματισμένη τιμή ολόκληρου του δίσκου η οποία θα χρησιμοποιηθεί σαν τιμή αναφοράς και στις επόμενες επαναλήψεις ώστε να διασφαλιστεί ότι σε κάθε δοκιμή τα δεδομένα που χρησιμοποιούνται για διαγραφή είναι τα ίδια.

β. Θα δημιουργήσουμε τις κατακερματισμένες τιμές του κάθε αρχείου ξεχωριστά και με το πέρας της διαδικασίας διαγραφής θα συγκρίνουμε τυχόν εναπομείναντα αρχεία ώστε να εξακριβώσουμε σε τι ποσοστό τα αρχεία διαγράφηκαν ή τροποποιήθηκαν.

3. AccessData FTK Imager (*FTK Imager*, 2023) – Το AccessData FTK Imager είναι ένα ισχυρό εργαλείο ψηφιακής δικανικής που χρησιμοποιείται ευρέως από τους αναλυτές

υπολογιστών για την απόκτηση και ανάλυση ψηφιακών στοιχείων. Παρόλο που αποτελεί μέρος του εμπορικού πακέτου δικανικών εργαλείων FTK® Forensic Toolkit, το FTK Imager λειτουργεί αυτόνομα και προσφέρεται δωρεάν. Μπορεί να χρησιμοποιηθεί για τη λήψη δεδομένων από ένα ευρύ φάσμα ψηφιακών συσκευών αποθήκευσης, συμπεριλαμβανομένων σκληρών δίσκων, μονάδων flash και καρτών μνήμης. Μία από τις βασικές δυνατότητες του εκτός από την απόκτηση δεδομένων, είναι η δημιουργία μιας εικόνας (image) της συσκευής. Αυτή η εικόνα μπορεί στη συνέχεια να αναλυθεί χρησιμοποιώντας άλλα ψηφιακά δικανικά εργαλεία για την αποκάλυψη κρυμμένων ή διαγραμμένων δεδομένων, την ανάκτηση των διαγραμμένων αρχείων και την εξαγωγή metadata από αυτά. Επίσης, το FTK Imager παρέχει πολλές άλλες χρήσιμες λειτουργίες, όπως η προεπισκόπηση αρχείων και φακέλων, η οποία επιτρέπει στους δικανικούς αναλυτές να κάνουν προεπισκόπηση του περιεχομένου ενός αρχείου ή φακέλου χωρίς να το ανοίξουν πραγματικά. Το FTK Imager περιλαμβάνει επίσης δυνατότητες, όπως η αναζήτηση λέξεων-κλειδιών, η οποία επιτρέπει στους χρήστες να αναζητούν συγκεκριμένες λέξεις-κλειδιά ή φράσεις σε μια εικόνα ενός αποθηκευτικού μέσου. Μπορεί επίσης να δημιουργήσει τιμές κατακερματισμού των δεδομένων που αποκτήθηκαν, οι οποίες μπορούν να χρησιμοποιηθούν για την επαλήθευση της ακεραιότητας των δεδομένων και τη διασφάλιση ότι δεν έχουν τροποποιηθεί.




**Εικόνα 4-6: AccessData FTK Imager**

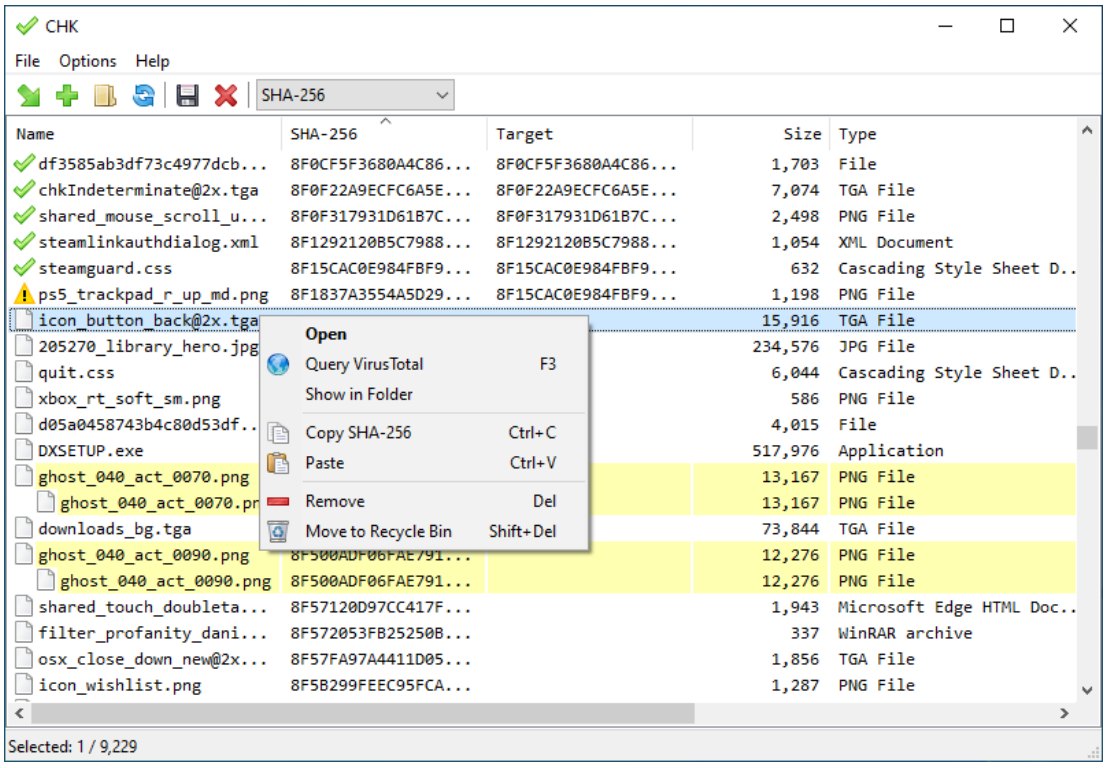
Στις δοκιμές αξιολόγησης των εργαλείων οριστικής διαγραφής θα χρησιμοποιήσουμε το AccessData FTK Imager στις πιο κάτω περιπτώσεις:

α. Κατά την αρχικοποίηση του δίσκου και μετά την διαγραφή του με τη συσκευή GLOTRENDS SATA Hard Drive Eraser θα επιβεβαιώσουμε ότι στο δίσκο είναι γραμμένα μόνο μηδενικά.

β. Μετά την εισαγωγή των δεδομένων που θα διαγραφούν θα εξάγουμε με τη βοήθεια του εργαλείου την εικόνα του δίσκου και την κατακερματισμένη τιμή της ώστε να μπορούμε να την συγκρίνουμε στις επόμενες επαναλήψεις και να επιβεβαιώσουμε ότι ξεκινούμε με κοινή βάση.

γ. Μετά τη χρήση των εργαλείων οριστικής διαγραφής θα δημιουργήσουμε την εικόνα του δίσκου ώστε να μπορούμε να την αναλύσουμε με άλλα εργαλεία δικανικής και να διαπιστώσουμε αν τα δεδομένα έχουν διαγραφεί.

4. CHK Checksum Utility (*CHK Checksum Utility*,2023) – Δωρεάν εργαλείο δημιουργίας κατακερματισμένων τιμών (hash values) και σύγκριση μεταξύ τους για έλεγχο ακεραιότητας των αρχείων.




**Εικόνα 4-7: CHK Checksum Utility**

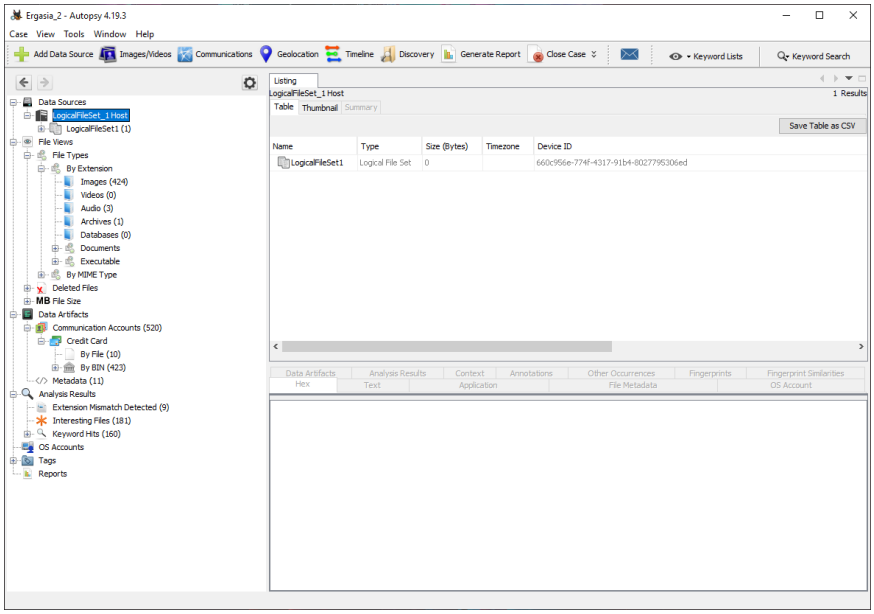
5. USBWriteBlocker (‘Orion USB Write Blocker -Orion Forensics LAB’, 2023) – Είναι ένα εργαλείο που λειτουργεί παρεμποδίζοντας τις εντολές εγγραφής που αποστέλλονται στις θύρες USB του υπολογιστή αποκλείοντας έτσι την εγγραφή δεδομένων, ενώ παράλληλα επιτρέπει την πρόσβαση ανάγνωσης στα δεδομένα της μονάδας που βρίσκεται συνδεδεμένη. Χρησιμοποιείται για να διασφαλιστεί η ακεραιότητα των δεδομένων στις προς εξέταση συσκευές από τυχόν τροποποιήσεις.


**Εικόνα 4-8: Orion USB Write Blocker**

Το συγκεκριμένο εργαλείο θα χρησιμοποιηθεί σε συνδυασμό με τη συσκευή GLOTRENDS SATA Hard Drive Eraser όπου αφού ενεργοποιηθεί η προστασία εγγραφής στις συσκευές USB θα γίνει εξαγωγή της εικόνας του δίσκου για ανάλυση.

6. Autopsy 4.19.3 (*Autopsy | Digital Forensics*, 2023) - Πρόκειται για ένα λογισμικό εργαλείο με γραφικό περιβάλλον που χρησιμοποιείται στην ανάλυση μονάδων αποθήκευσης δεδομένων , υπολογιστών και κινητών συσκευών. Μπορεί επίσης να χρησιμοποιηθεί σε ανεξάρτητα αρχεία και εικόνες (images) αποθηκευτικών μέσων . Οι δυνατότητες του βρίσκουν εφαρμογή στην δικανική υπολογιστών αφού μπορεί να χρησιμοποιηθεί για ανάκτηση δεδομένων, συσχέτιση πληροφοριών , εύρεση δεδομένων σε αρχεία καθώς και χρονική ή γεωγραφική αναπαράσταση υποθέσεων. Σημαντικό πλεονέκτημα του Autopsy είναι τα διάφορα plugins που μπορούν να προστεθούν σε αυτό δίνοντας του ακόμη

περισσότερες δυνατότητες ή να αυτοματοποιήσουν εργασίες κάνοντας το πιο αποτελεσματικό και αποδοτικό.




**Εικόνα 4-9: Autopsy 4.19.3**

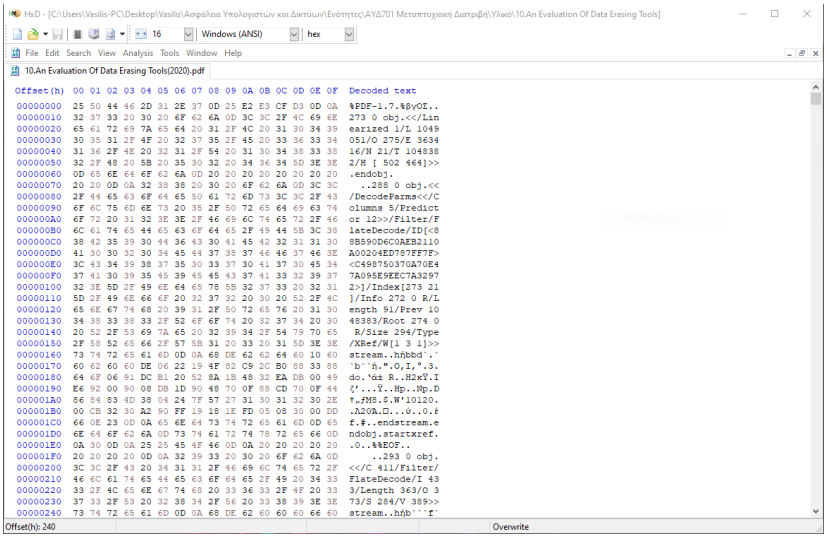
Το Autopsy 4.19.3 θα χρησιμοποιηθεί κατά το στάδιο της ανάλυσης της εικόνας από το διαγραμμένο σκληρό δίσκο ώστε να εντοπιστούν πιθανά αρχεία που παρέμειναν στο δίσκο ακόμα και μετά την διαγραφή.

7. Bulk Extractor (*Bulk-Extractor | Kali Linux Tools*, 2023) - Το Bulk Extractor είναι ένα χρήσιμο εργαλείο ψηφιακής δικανικής ανοιχτού κώδικα που χρησιμοποιείται ευρέως από ερευνητές για την εξαγωγή πληροφοριών από διάφορα ψηφιακά μέσα. Το εργαλείο είναι ειδικά σχεδιασμένο για να σαρώνει μεγάλους όγκους δεδομένων και να εξάγει συγκεκριμένες πληροφορίες με βάση προκαθορισμένα μοτίβα αναζήτησης. Το Bulk Extractor τρέχει σε περιβάλλον Kali Linux και είναι γραμμένο σε γλώσσα προγραμματισμού C++ και το οποίο σου δίνει τη δυνατότητα να αναλύει τα αρχεία, ενώ παράλληλα ετοιμάζει αυτόματα καταλόγους όπου ταξινομεί ανάλογα με το τύπο τους όλα τα ευρήματα. Μία από τις βασικές δυνατότητες του Bulk Extractor είναι η ικανότητά του να αναγνωρίζει και να εξάγει αρχεία και αντικείμενα που συνήθως παραβλέπονται από άλλα εργαλεία ψηφιακής δικανικής. Μπορεί να εξαγάγει ένα ευρύ φάσμα πληροφοριών, όπως διευθύνσεις email, αριθμούς πιστωτικών καρτών, αριθμούς τηλεφώνου, διευθύνσεις URL και άλλες πληροφορίες προσωπικής ταυτοποίησης από διαφορετικούς τύπους αρχείων. Το Bulk extractor δεν διαθέτει γραφικό περιβάλλον, τρέχει με εντολές στο

terminal σε Linux και βρίσκεται προ εγκατεστημένο στην έκδοση Kali κάτω από την κατηγορία Forensics.

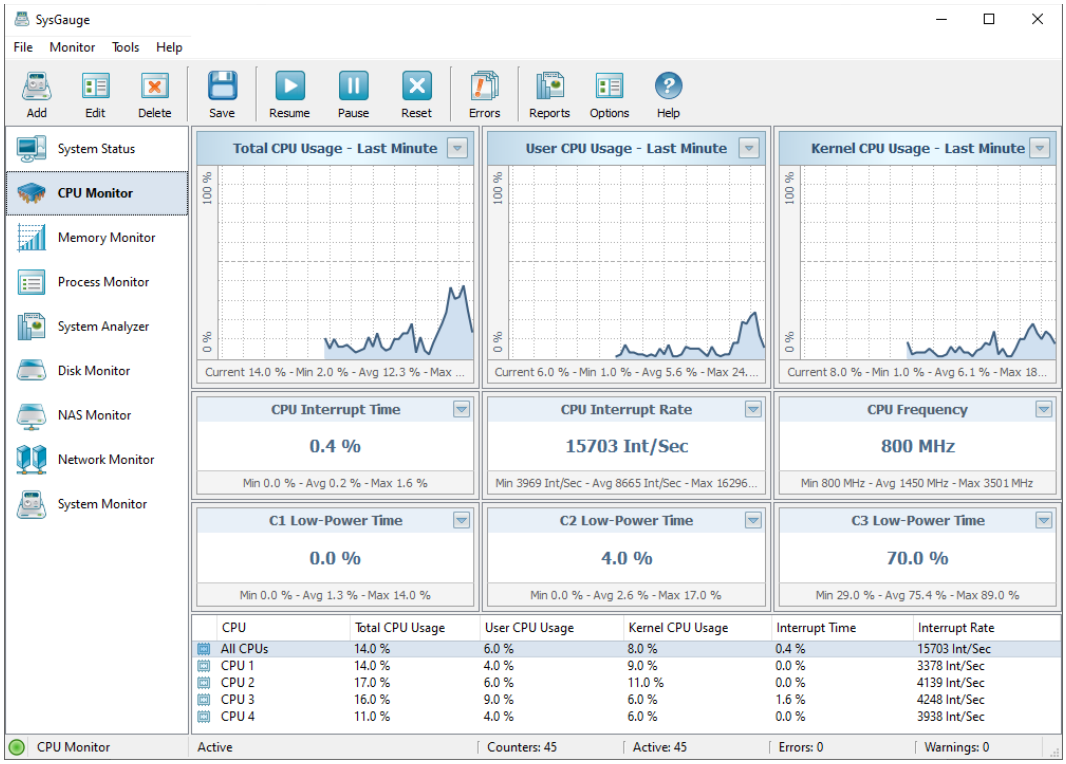

**Εικόνα 4-10: Bulk Extractor**

8. HxD – Hex Editor και Disk Editor (*HxD - Freeware Hex Editor and Disk Editor*, 2023) - Το HxD είναι ένα δωρεάν, πολυδύναμο εργαλείο επεξεργασίας που επιτρέπει στους χρήστες να προβάλλουν και να επεξεργάζονται ακατέργαστα δυαδικά δεδομένα αρχείων, σκληρών δίσκων και άλλων συσκευών αποθήκευσης. Επίσης δίνει τη δυνατότητα να ανοίξουν οποιοδήποτε αρχείο και να δουν τις δεκαεξαδικές, δεκαδικές και ASCII αναπαραστάσεις του. Μπορούν να μεταβούν σε συγκεκριμένες θέσεις του δίσκου, να αναζητήσουν κείμενο ή δυαδικά μοτίβα και να επεξεργαστούν απευθείας τα δεδομένα.




**Εικόνα 4-11: HxD - Hex Editor and Disk Editor**

9. SysGauge (*SysGauge - System Monitor*, 2023) - Το SysGauge είναι ένα ολοκληρωμένο και ισχυρό εργαλείο παρακολούθησης συστήματος με αρκετές λειτουργίες που μπορεί να χρησιμοποιηθεί για την εποπτεία και τη διαχείριση διαφόρων συστημάτων. Με το SysGauge, οι χρήστες μπορούν να παρακολουθούν διάφορους πόρους συστήματος, συμπεριλαμβανομένης της χρήσης της CPU, της χρήσης μνήμης, της δραστηριότητας του δίσκου, της δραστηριότητας δικτύου και των διεργασιών του συστήματος.




**Εικόνα 4-12: SysGauge System Monitoring Tool**

Το SysGauge θα χρησιμοποιηθεί κατά τη διάρκεια των πειραματικών δοκιμών για να καταγράψει τη χρήση του επεξεργαστή και της μνήμης κατά την εκτέλεση των εργαλείων οριστικής διαγραφής ώστε να εξάγουμε συμπεράσματα σχετικά με την επίδοση τους.

## 4.2 Δημιουργία Συνόλων Δεδομένων

Σημαντικό κομμάτι της πειραματικής δοκιμής των εργαλείων αποτελεί η δημιουργία προκαθορισμένου όγκου δεδομένων, δηλαδή αρχείων που θα τοποθετηθούν στον δίσκο για διαγραφή. Τα δεδομένα αυτά θα αποτελούν την κοινή βάση στην οποία θα πραγματοποιούνται οι αξιολογήσεις. Περιλαμβάνονται διάφοροι τύποι αρχείων με διαφορετικά μεγέθη. Μεταξύ των αρχείων θα τοποθετηθούν κάποια με ευαίσθητες πληροφορίες όπως κωδικοί, αριθμοί

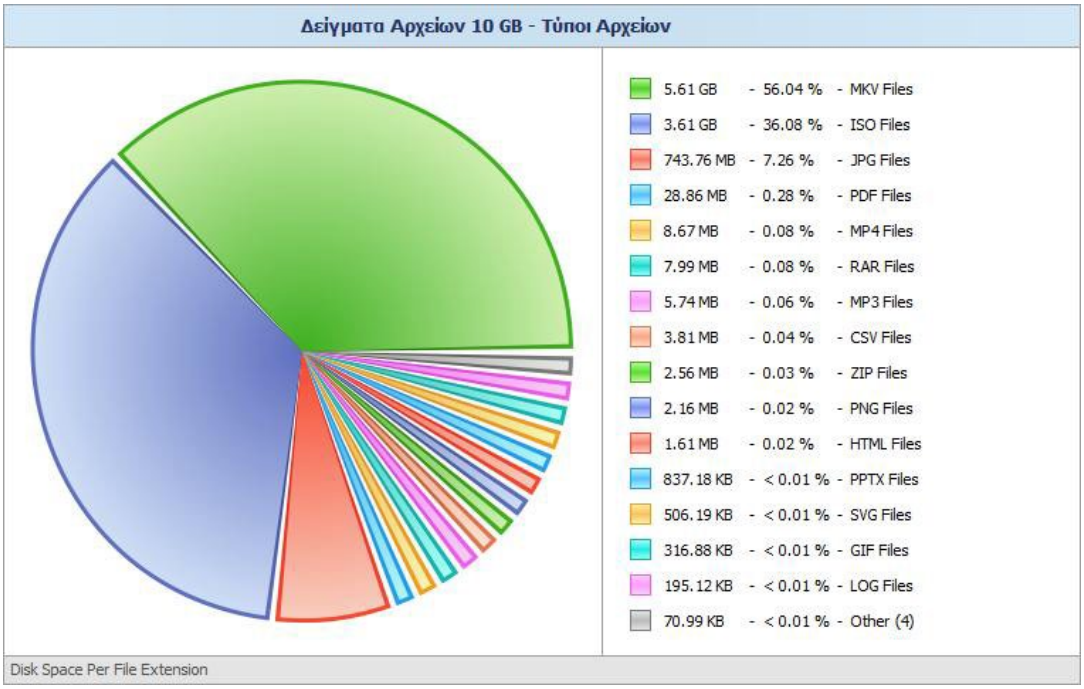
πιστωτικών καρτών κτλ για να διαπιστωθεί αν κάποια από αυτά μετά την διαγραφή μπορούν να ανακτηθούν κατά την διαδικασία της ανάλυσης. Το Autopsy όπως επίσης και το εργαλείο bulk extractor που αναφέρθηκαν πιο πάνω έχουν τη δυνατότητα να αναγνωρίσουν τέτοιες ευαίσθητες πληροφορίες και να τις καταγράψουν. Επίσης αρκετά από τα αρχεία περιέχουν πληροφορίες metadata που επίσης θα προσπαθήσουμε να ανακτήσουμε. Δημιουργήθηκαν δύο σύνολα δεδομένων με διαφορετικά μεγέθη. Το πρώτο έχει μέγεθος 10GB ενώ το δεύτερο έχει μέγεθος 200GB. Με αυτό τον τρόπο θα μπορέσουμε να καθορίσουμε εάν το συνολικό μέγεθος των αρχείων προς διαγραφή επηρεάζει την απόδοση του εργαλείου οριστικής διαγραφής.

Τα αρχεία που επιλέχτηκαν περιλαμβάνουν διάφορους γνωστούς τύπους αρχείων που χρησιμοποιούνται ευρέως και συλλέχθηκαν από το διαδίκτυο. Συγκεκριμένα:

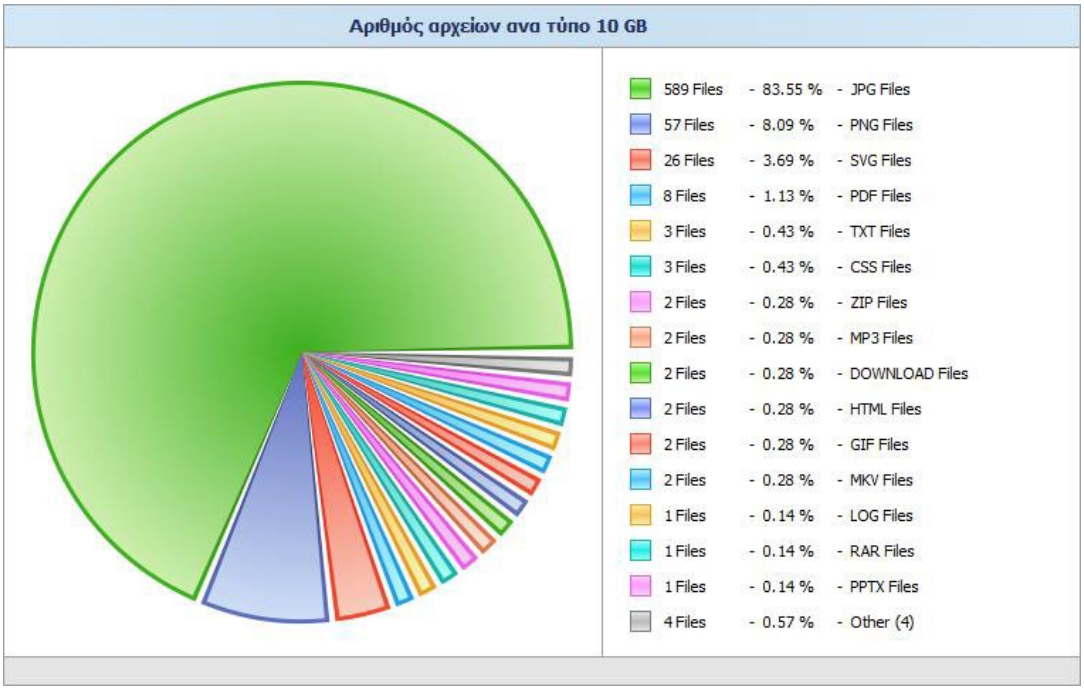
- Σετ αρχείων μεγέθους 10 GB

| Τύπος Αρχείου | Αριθμός Αρχείων | Μέγεθος |
|---|---|---|
| MKV Files | 2 | 5.61 GB |
| ISO Files | 1 | 3.61 GB |
| JPG Files | 589 | 743.76 MB |
| PDF Files | 8 | 28.86 MB |
| MP4 Files | 1 | 8.67 MB |
| RAR Files | 1 | 7.99 MB |
| MP3 Files | 2 | 5.74 MB |
| CSV Files | 1 | 3.81 MB |
| ZIP Files | 2 | 2.56 MB |
| PNG Files | 57 | 2.16 MB |
| HTML Files | 2 | 1.61 MB |
| PPTX Files | 1 | 837.18 KB |
| SVG Files | 26 | 506.19 KB |
| GIF Files | 2 | 316.88 KB |
| LOG Files | 1 | 195.12 KB |
| CSS Files | 3 | 38.86 KB |
| TXT Files | 3 | 25.18 KB |
| NOEXT Files | 1 | 4.99 KB |
| DOWNLOAD Files | 2 | 1.96 KB |

**Πίνακας 4-4: Σετ αρχείων μεγέθους 10 GB**




**Εικόνα 4-13: Τύποι αρχείων - 10 GB**




**Εικόνα 4-14: Αριθμός αρχείων ανά τύπο - 10 GB**

Συνολικά για το δείγμα των αρχείων μεγέθους 10 GB συγκεντρώθηκαν 705 διαφορετικά αρχεία. Μέρος τους καταγράφεται στην παρακάτω λίστα.

| A/A | Filename | MD5 | File Size | Extension |
|---|---|---|---|---|
| 1 | pexels-ivan-siarbolin-3015864.jpg | 001f2ba421834224e73d5aa716486a8a | 999,027 | jpg |
| 2 | 46782678564_f16bd553f4_o.jpg | 0037ead9d8a9e98dd5ca1067ad523a2e | 1,739,364 | jpg |
| 3 | dubai-4516584.jpg | 014413990127b96dc7b384ec38bfd6d4 | 1,023,627 | jpg |
| 4 | cd8a0b8f957965f06f3d71bb.jpg | 014462f0a2bd3f7bce90f4735225c070 | 1,747,352 | jpg |
| 5 | play.png | 014940b979824ab02f0b8ed0c8a26227 | 883 | png |
| 6 | Rail-57382392.jpg | 024710e12e650f2d47455bd889dac19f | 1,209,946 | jpg |
| 7 | sreehari-devadas--WQI3xmytv8-unsplash.jpg | 0267d179869a77eb820b278e0d153079 | 920,005 | jpg |
| 8 | i-47n9bGd.jpg | 027b083df4e816a5dd5f7bc2f66672f9 | 1,386,380 | jpg |
| 9 | dubay-obedinennye-arabskie-emiraty-gorod-kxlo.jpg | 02b3fa54ab6f83e13b830781324760ac | 769,567 | jpg |
| 10 | i-QCsX8zX.jpg | 030e31bc977e3dc1af0e1fc1370d5bc1 | 1,817,044 | jpg |
| 11 | tom-chen-577408-unsplash.jpg | 0348a8b42997e0e347a780ef052f0709 | 1,349,435 | jpg |
| 12 | Thumbnail_website_SAE.png | 035ac750731f790b325877f62dc451a1 | 35,221 | png |
| 13 | 52050647585_86c878afed_o.jpg | 03839facfdb6358abcca2df37bed40b5 | 1,162,691 | jpg |
| 14 | paul-silvan-WfZ-cl8_smM-unsplash.jpg | 03a04a041f4ff1741c203f9c02f37edf | 728,858 | jpg |
| 15 | kali-everywhere-cloud.svg | 03cad759f65d47c85df039bb84118f2b | 38,574 | svg |
| 16 | Atlantis-The-Palm.jpg | 03d7f1baa6361205f65649b7e8388c76 | 1,465,903 | jpg |
| 17 | Marina-boat-Dubai-970516.jpg | 04f31825192ff546617d91fe80d2c55e | 1,271,183 | jpg |
| 18 | Electric-Circuits.pdf | 050677ebae3340eeecf2308d7197b79d | 9,272,724 | pdf |
| 19 | pexels-aleksandar-pasaric-823696.jpg | 060f585d0d2e510bc5cf05ad9a7d95be | 527,922 | jpg |
| 20 | Burj_Khalifa_NYE2019_013.jpg | 0642b40d6af3a9684b61097c0eafbc6f | 704,785 | jpg |
| 21 | DUKES_VIEW_01.jpg | 06447abb096b0d86249fe8e3efcc11b7 | 682,907 | jpg |
| 22 | 26594860629_45f884d621_o.jpg | 0669320e8f102ae608ab2fe779a3ed8b | 573,405 | jpg |
| 23 | dubai-4044195.jpg | 0694344ca7a10e6c07388be3a9093c38 | 1,156,627 | jpg |
| 24 | Emirates_UAE_Dubai_464914.jpg | 069e1a3e94d47f56609ccacf1f348632 | 2,506,064 | jpg |
| 25 | mockup-graphics-U6ZMEefFGx8-unsplash.jpg | 06b22bf8c4070a60e09fd2ff4c9b73bd | 1,468,526 | jpg |
| 26 | Thumbnail_website_PDE.png | 07315c4b17ebb322b7d32f2890964808 | 34,637 | png |
| 27 | pexels-jeshootscom-442579.jpg | 074f6c40bccb6974004249fa8a5db2fe | 745,248 | jpg |
| 28 | british-library-HVvXTQVHCV0-unsplash.jpg | 085de20a521a15acb3e916b1eea63419 | 9,693,024 | jpg |

**Εικόνα 4-15: Κατάλογος αρχείων 10 GB**

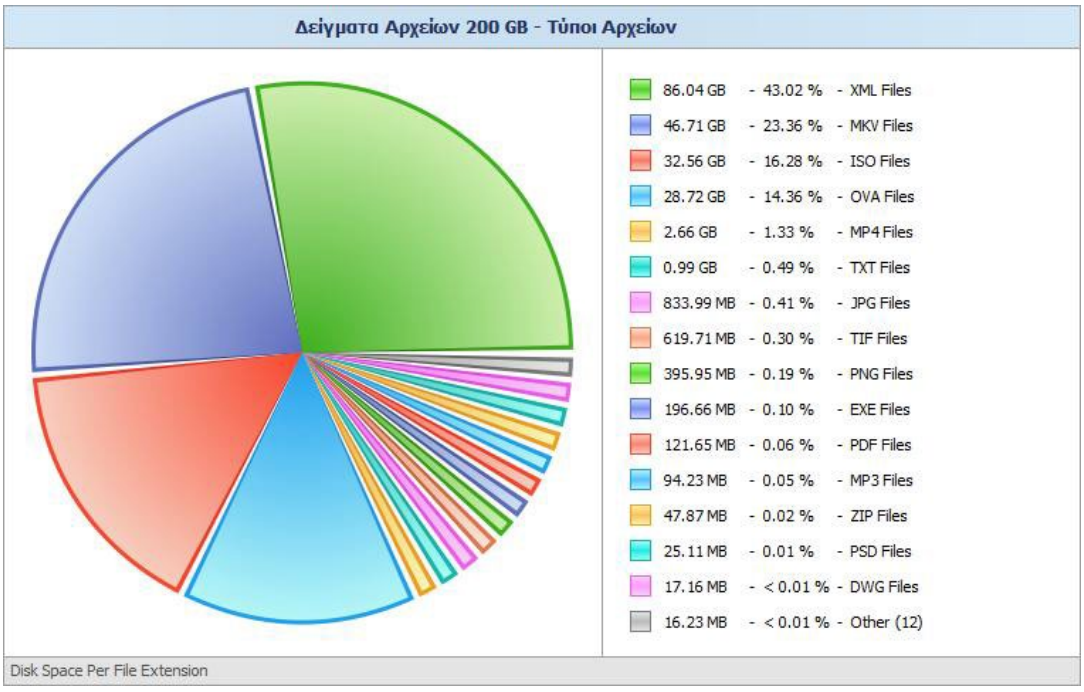
Ο αναλυτικός κατάλογος των αρχείων αυτών μαζί με το ακριβές μέγεθος τους και την hash τιμή MD5 η οποία θα χρησιμοποιηθεί αργότερα κατά την σύγκριση τους με τα ευρήματα στο δίσκο βρίσκεται στο τέλος (Παράρτημα Α).

- Σετ αρχείων μεγέθους 200 GB

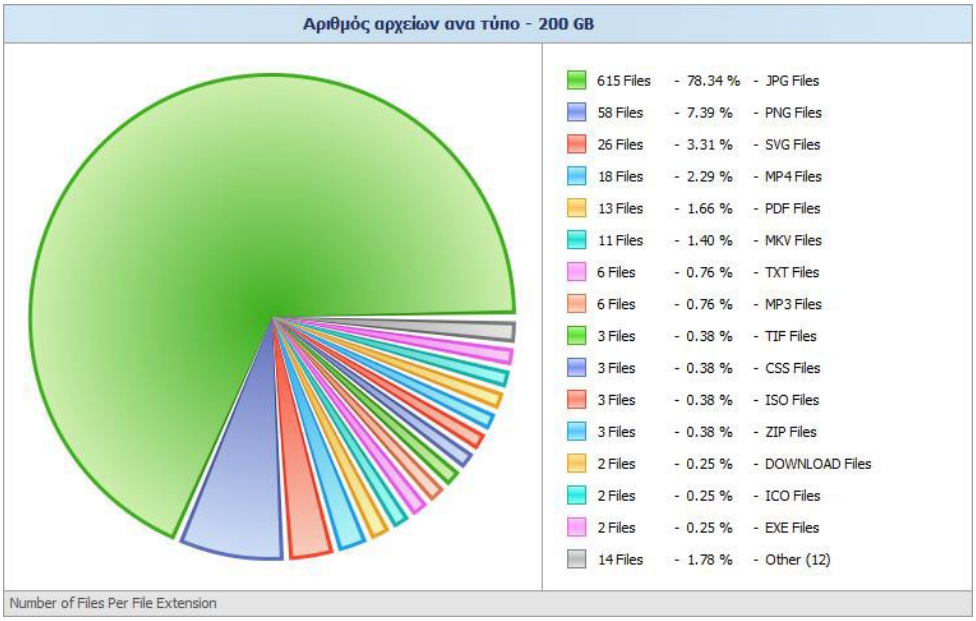
| Τύπος Αρχείου | Αριθμός Αρχείων | Μέγεθος |
|---|---|---|
| XML Files | 1 | 86.04 GB |
| MKV Files | 11 | 46.71 GB |
| ISO Files | 3 | 32.56 GB |
| OVA Files | 1 | 28.72 GB |
| MP4 Files | 18 | 2.66 GB |
| TXT Files | 6 | 0.99 GB |
| JPG Files | 615 | 833.99 MB |
| TIF Files | 3 | 619.71 MB |
| PNG Files | 58 | 395.95 MB |
| EXE Files | 2 | 196.66 MB |

| Τύπος Αρχείου | Αριθμός Αρχείων | Μέγεθος |
|---|---|---|
| PDF Files | 13 | 94.23 MB |
| MP3 Files | 6 | 47.87 MB |
| ZIP Files | 3 | 25.11 MB |
| PSD Files | 1 | 17.16 MB |
| DWG Files | 1 | 7.99 MB |
| RAR Files | 1 | 3.81 MB |
| CSV Files | 1 | 1.61 MB |
| HTML Files | 2 | 853.38 KB |
| DOCX Files | 1 | 837.18 KB |
| PPTX Files | 1 | 506.19 KB |
| SVG Files | 26 | 316.88 KB |
| GIF Files | 2 | 195.12 KB |
| LOG Files | 1 | 132.12 KB |
| ICO Files | 2 | 38.86 KB |
| CSS Files | 3 | 4.99 KB |
| NOEXT Files | 1 | 1.96 KB |
| DOWNLOAD Files | 2 | 86.04 GB |

**Πίνακας 4-5: Σετ αρχείων μεγέθους 200 GB**




**Εικόνα 4-16: Τύποι αρχείων - 200 GB**




**Εικόνα 4-17: Αριθμός αρχείων ανά τύπο - 200 GB**

Για το δείγμα των αρχείων συνολικού μεγέθους 200 GB συγκεντρώθηκαν 785 διαφορετικά αρχεία αποτελούμενα από 27 διαφορετικούς τύπους. Μέρος των αρχείων αυτών είναι και τα αρχεία από το προηγούμενο δείγμα των 10 GB. Τα υπόλοιπα 190 GB αποτελούν καινούργια αρχεία όλα διαφορετικά μεταξύ τους . Στην πιο κάτω λίστα απαριθμείται μέρος τους. Ο αναλυτικός κατάλογος των αρχείων αυτών μαζί με το ακριβές μέγεθος τους και την hash τιμή MD5 η οποία θα χρησιμοποιηθεί αργότερα κατά την σύγκριση τους με τα ευρήματα στο δίσκο βρίσκεται στο τέλος (Παράρτημα Α).

| A/A | Filename | MD5 | File Size | Extension |
|---|---|---|---|---|
| 1 | 014a.jpg | 635c5d89a764edfe93d1594a2cf664ef | 612,809 | jpg |
| 2 | 14-30mm_F4_S_10_JM_0001.jpg | fe110a0e5ddb542d60f2eaa52abf5b3b | 1,304,219 | jpg |
| 3 | 18da517618031157d05b66a017cb39d1.jpg | a60e6e88bee2a1e5474817a69e1b1252 | 426,613 | jpg |
| 4 | 2019-10-19_11-52-51_down-town-staycaejpg.jpg | dc8ed547681335fe9ba402a328b390a5 | 1,217,765 | jpg |
| 5 | 2021-05-01_123359.jpg | cc53126b67f6ec9c3b1f8f3a9c743b0a | 1,158,716 | jpg |
| 6 | 4K Ultra HD Video of Wild Animals.mkv | ae35b814a43ea4c258d9851b11e17649 | 3,411,969,751 | mkv |
| 7 | 4K Video Unbelievable Beauty.mkv | 64e83573405f11c619c8b0dbe27d632b | 4,003,893,219 | mkv |
| 8 | Administration_propaganda.tif | a3102eb747714c555de6560be1ec7e4a | 165,706,080 | tif |
| 9 | Altered Carbon.mkv | f776bf9e405b1044c2060aa39342bf16 | 2,960,899,264 | mkv |
| 10 | An Awesome Tool to Prevent Corruption Of Your Most Important Files.mp4 | b853c56a8ea958519093c505a72963f8 | 122,833,116 | mp4 |
| 11 | artist-designer-at-work.jpg | 3c2aa0c9a10417b8897b69b1f9f6c2f2 | 1,016,749 | jpg |
| 12 | augustine-wong-T0BYurbDK_M-unsplash.jpg | dd32494a3aa65ca45a5c12921b8d2599 | 5,258,388 | jpg |
| 13 | austin-distel-21GWwco-JBQ-unsplash.jpg | 5f7b6b157176aa184857c43074f42cce | 4,758,054 | jpg |
| 14 | austin-distel-744oGeqpxPQ-unsplash.jpg | f0ab969cd1661a0dd3be10006ced6071 | 5,820,331 | jpg |
| 15 | austin-distel-Jn1csk3lWDA-unsplash.jpg | 606fa66cdc2f329530623978cdb8b5db | 3,708,970 | jpg |
| 16 | austin-distel-nGc5RT2HmF0-unsplash.jpg | 5fdb186472ef98f10a1a4ba5e9c1c018 | 4,120,280 | jpg |
| 17 | bernard-hermant-_THpp4Hs8LU-unsplash.jpg | 7d3df0dc6bf9ba1c6bc06dbabc95c403 | 3,780,686 | jpg |
| 18 | blackarch-linux-2023.04.01.ova | ce041f01e0ce2ebfd5d09179b6df10f6 | 30,840,756,736 | ova |
| 19 | Blow_fight!__General_August_Willich_at_the_Battle_of_Liberty_Gap,_Tennessee,_June_1863_L | 6cd05e6aad6e63433df9dd776cca1639 | 321,636,638 | tif |
| 20 | Bon Jovi - You Give Love A Bad Name.mp3 | 65078ed0922a6e8a630ac493a80f7632 | 3,602,603 | mp3 |
| 21 | cdc-_XLJy3h77cw-unsplash.jpg | 0ecbf61c0adb9ed7b1ceff53613ea1d7 | 5,588,600 | jpg |
| 22 | ChatGPT For Cybersecurity.mp4 | 2939bdd5a8e7040b95d808c4ecc26da3 | 166,827,440 | mp4 |

**Εικόνα 4-18: Κατάλογος αρχείων 200 GB**

## 4.3 Εργαλεία Οριστικής Διαγραφής Δεδομένων

Λαμβάνοντας υπόψη τους περιορισμούς που τέθηκαν πιο πάνω, συγκεντρώσαμε όλα τα εργαλεία που πληρούν τα κριτήρια και είναι σήμερα διαθέσιμα για χρήση. Ως βασικό κριτήριο τέθηκε η δυνατότητα τους να διαγράφουν οριστικά δεδομένα σύμφωνα με το πρώτο επίπεδο διαγραφής δεδομένων σκληρών δίσκων από το NIST. Εργαλεία οριστικής διαγραφής που έκαναν χρήση εντολών που βρίσκονται στο firmware συγκεκριμένων δίσκων απορρίφθηκαν αφού η συγκεκριμένη μέθοδος δεν εμπίπτει στα πλαίσια μελέτης αυτής της διατριβής. Με βάση λοιπόν αυτό, τα εργαλεία οριστικής διαγραφής που καταγράφηκαν έχουν σαν αρχή λειτουργίας τους την επανεγγραφή δεδομένων με ένα ή περισσότερα περάσματα στα τμήματα του δίσκου που ορίστηκαν για μη αναστρέψιμη διαγραφή σύμφωνα με τις μεθόδους επανεγγραφής δεδομένων που είδαμε στο κεφάλαιο 2 . Στον πιο κάτω πίνακα απαριθμούνται όλα τα εργαλεία οριστικής διαγραφής που είναι σήμερα διαθέσιμα για χρήση και είναι συμβατά με το λειτουργικό σύστημα των Windows 10.

| Α/Α | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη Αξιολόγηση | Άρθρο Αναφοράς |
|---|---|---|---|---|---|
| **1** | DBAN (Darik's Boot and Nuke) | 2.3.0 | Free / Open Source | Ναι | (Martin & Jones, 2011), (Olvecky & Gabriska, 2018) |
| **2** | CBL Data Shredder | 1.0.0 | Free | Ναι | (Jones, 2020), (Olvecky & Gabriska, 2018) |
| **3** | HDD LLF Low Level Format Tool | 4.4 | Free & commercial version | Όχι | - |
| **4** | Active@ KillDisk | 15.0 | Free & commercial version | Ναι | (Martin & Jones, 2011), (Jones, 2020), (Olvecky & Gabriska, 2018) |
| **5** | Macrorit Data Wiper | 6.3.8 | Free & commercial version | Ναι | (Jones, 2020) |
| **6** | Eraser | 6.2.0.2993 | Free / Open Source | Ναι | (Martin & Jones, 2011), (Jones, 2020), |

| Α/Α | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη Αξιολόγηση | Άρθρο Αναφοράς |
|---|---|---|---|---|---|
| | | | | | (Horsman, 2021), (Carlton & Kessler, 2012), (Olvecky & Gabriska, 2018) |
| **7** | Freeraser | 1.0.0.23 | Free | Ναι | (Martin & Jones, 2011),(Horsman, 2021),(Olvecky & Gabriska, 2018) |
| **8** | Disk Wipe | 1.7 | Free | Ναι | (Jones, 2020), (Olvecky & Gabriska, 2018) |
| **9** | Hardwipe | 5.2.1 | Free | Ναι | (Jones, 2020) |
| **10** | ASCOMP Secure Eraser | 6.001 | Free & commercial version | Όχι | - |
| **11** | PrivaZer | 4.0.58 | Free & Donated Version | Όχι | - |
| **12** | PC Shredder | 1.1 | Free | Ναι | (*AlHarbi*, 2021) |
| **13** | AOMEI Partition Assistant Standard Edition | 9.13.0 | Free & commercial version | Όχι | |
| **14** | Remo Drive Wipe | 2.0.0 | Free & commercial version | Ναι | (Martin & Jones, 2011), |
| **15** | CCleaner | 6.06.10144 | Free & commercial version | Ναι | (Horsman, 2021) |
| **16** | File Shredder | 2.5 | Free | Ναι | (Martin & Jones, 2011),(Horsman, 2021) |

| Α/Α | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη Αξιολόγηση | Άρθρο Αναφοράς |
|---|---|---|---|---|---|
| **17** | Hard Drive Eraser | 2.0 | Free | Ναι | (Martin & Jones, 2011) |
| **18** | Super File Shredder | 4.1.2 | Free | Ναι | (Jones, 2020) |
| **19** | TweakNow SecureDelete | 1.0.0 | Free | Όχι | - |
| **20** | MiniTool Drive Wipe | 5.0 | Free | Όχι | - |
| **21** | XT File Shredder Lizard | 2.1 | Free | Όχι | - |
| **22** | WipeFile | 3.6 | Free | Ναι | (Horsman, 2021) |
| **23** | Puran Wipe Disk | 1.2 | Free | Ναι | (Jones, 2020) |
| **24** | BitKiller | 2.0 | Free | Ναι | (Horsman, 2021) |
| **25** | Simple File Shredder | 3.2 | Free | Όχι | - |
| **26** | Ashampoo WinOptimizer Free | 17.00.33 | Free | Όχι | - |
| **27** | AbsoluteShield File Shredder | 1.41 | Free | Όχι | - |
| **28** | DeleteOnClick | 2.6.5.0 | Free | Όχι | - |
| **29** | CopyWipe | 1.14 | Free | Όχι | - |
| **30** | SDelete | 2.04 | Free | Ναι | (Oh et al., 2020) |
| **31** | Wise Care 365 | 6.3.9 | Free & commercial version | Όχι | - |
| **32** | ProtectStar Data Shredder | 2.2 | Free & commercial version | Όχι | - |
| **33** | HDShredder Free Edition | 6 | Free & commercial version | Όχι | - |
| **34** | Moo0 Disk Wiper | 1.14 | Free | Όχι | - |
| **35** | BCWipe Total WipeOut | 5.02.5 | Trial & Commercial Version | Ναι | (Martin & Jones, 2011) |
| **36** | O&O SafeErase | 17 | Trial & Commercial Version | Όχι | - |

| Α/Α | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη Αξιολόγηση | Άρθρο Αναφοράς |
|---|---|---|---|---|---|
| **37** | Donemax Data Eraser | 1.2 | Trial & Commercial Version | Όχι | - |
| **38** | Iolo DriveScrubber | - | Commercial Version | Όχι | - |
| **39** | Abylon Shredder | 23.10.3 | Trial & Commercial Version | Όχι | - |
| **40** | TS DataWiper | 2.2 | Trial & Commercial Version | Όχι | - |
| **41** | Easy File Shredder | 2.0.2018.1209 | Trial & Commercial Version | Όχι | - |
| **42** | Zer0 | 0.6.0.6 | Free | Όχι | - |
| **43** | Kernel File Shredder | 11.04.01 | Trial & Commercial Version | Όχι | - |
| **44** | BitRaser Data Eraser | - | Paid | Όχι | - |

**Πίνακας 4-6: Εργαλεία οριστικής διαγραφής, συμβατά με το λειτουργικό σύστημα των Windows 10**

Συνολικά καταγράφηκαν σαράντα τέσσερα (44) εργαλεία οριστικής διαγραφής δεδομένων να είναι διαθέσιμα για χρήση. Αρκετά από αυτά οι δημιουργοί τους σταμάτησαν να τα υποστηρίζουν ενώ σε άλλα δεν υπάρχει επίσημη ιστοσελίδα. Σε αυτές τις περιπτώσεις τα αρχεία εγκατάστασής τους διατηρούνται και είναι διαθέσιμα από ιστοσελίδες γενικού διαμοιρασμού εφαρμογών. Λόγω του μεγάλου αριθμού τους η υποβολή του καθενός από αυτά σε πειραματική δοκιμασία και διαδικασία αξιολόγησης κρίνεται ανέφικτη. Με βάση λοιπόν κριτηρίων θα γίνει επιλογή πέντε (5) εξ αυτών.

Τα κριτήρια που τέθηκαν για την επιλογή των εργαλείων οριστικής διαγραφής δεδομένων είναι:

1. Να μην έχει γίνει μέχρι σήμερα καμιά αντίστοιχη αξιολόγηση ως προς την ικανότητά του για οριστική διαγραφή αρχείων.

2. Να έχουν την δυνατότητα επιλογής ως μεθόδου διαγραφής την One Pass Zeros η οποία θεωρείται σύμφωνα με τις συστάσεις του NIST η ελάχιστη εφαρμόσιμη επιτρεπτή

μέθοδος. Οι αλγόριθμοι / μέθοδοι διαγραφής που μπορεί να εκτελέσει το κάθε εργαλείο καταγράφονται στο Παράρτημα Α.

3. Να έχει τη δυνατότητα να διαγράψει συγκεκριμένο αριθμό αρχείων που θα επιλεγούν όπως επίσης και διαγραφή ολόκληρου του δίσκου.

4. Να μπορούν να εκτελεστούν σε περιβάλλον λειτουργικού συστήματος Windows 10.

5. Να μην έχει περιορισμούς ως προς το συνολικό αριθμό των αρχείων που μπορεί να διαγράψει ή το συνολικό μέγεθος των δεδομένων.

Τα πιο πάνω κριτήρια τέθηκαν για τους ακόλουθους λόγους:

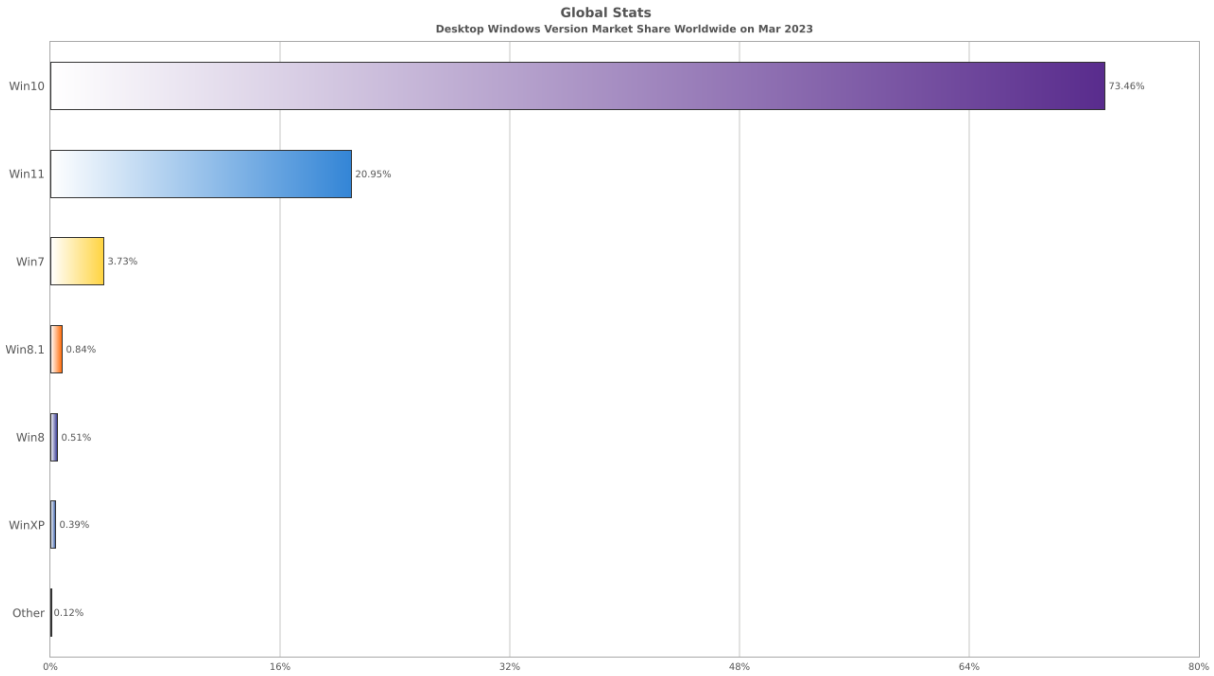
1. Η επιλογή των προς εξέταση εργαλείων οριστικής διαγραφής δεδομένων να παρουσιάζει κάποια καινοτομία σε σχέση με τις προηγούμενες μελέτες που διενεργήθηκαν. Εργαλεία που μελετήθηκαν στο παρελθόν από άλλους ερευνητές και δεν έχουν αναβαθμιστεί θα παρουσιάσουν λογικά τα ίδια αποτελέσματα.

2. Η μέθοδος "one pass zero" που επιλέχτηκε εκτός από γρήγορη, είναι ιδανική ώστε να μπορέσουμε να εξετάσουμε τα αποτελέσματα του διαγραμμένου δίσκου με ένα απλό hex editor πρόγραμμα όπως το AccessData FTK Imager ή το HxD σε πρώτο στάδιο. Σε περίπτωση επιλογής κάποιας άλλης μεθόδου επανεγγραφής δεδομένων όπως πχ τυχαία δεδομένα (random data), η χρήση τέτοιων εργαλείων δεν θα ήταν ιδιαίτερα αποτελεσματική αφού δεν θα ήμασταν σε θέση να διακρίνουμε εάν τα δεδομένα που βρίσκονται στο δίσκο είναι νέες εγγραφές ή πρόκειται για τις αρχικές.

3. Η ανάγκη για εφαρμογή του τρίτου κριτηρίου για ολική και επιλεκτική διαγραφή αρχείων του δίσκου τέθηκε αφού με αυτό τον τρόπο θα εξεταστεί κατά πόσο οι δυνατότητες των εργαλείων δεν επηρεάζονται από τη θέση των αρχείων στο δίσκο. Πχ ένα εργαλείο μπορεί να είναι αποτελεσματικό στην πλήρη διαγραφή του δίσκου, αλλά για οριστική διαγραφή συγκεκριμένων αρχείων που βρίσκονται σε αυτόν να μειονεκτεί.

4. Το Workstation για την διεξαγωγή των αξιολογήσεων και στο οποίο θα εγκαθίστανται τα εργαλεία οριστικής διαγραφής διαθέτει λειτουργικό Windows 10. Η επιλογή του συγκεκριμένου λειτουργικού συστήματος έγινε αφού ακόμα και σήμερα το συγκεκριμένο

λειτουργικό κατέχει την πρώτη θέση ανάμεσα στις προτιμήσεις των χρηστών παρόλο που η τελευταία έκδοση του είναι τα Windows 11.




**Εικόνα 4-19: Παγκόσμιο μερίδιο αγοράς λειτουργικού συστήματος Windows**

5. Τυχόν περιορισμοί στον αριθμό αρχείων ή του συνολικού μεγέθους των αρχείων, πιθανόν να μην μας επέτρεπε να εκτελέσουμε πλήρως τα σενάρια δοκιμών. Ειδικά στην περίπτωση όπου το εργαλείο οριστικής διαγραφής θα πρέπει να διαχειριστεί την διαγραφή 200 GB δεδομένων και 785 διαφορετικών αρχείων.

Στο Παράρτημα Α σημειώνονται τα πιο πάνω εργαλεία του πίνακα μαζί με επιπρόσθετες πληροφορίες όπως :

- Μέθοδοι επανεγγραφής δεδομένων που υποστηρίζουν.
- Ιστοσελίδα Εταιρείας / Δημιουργού ή link για λήψη αρχείου εγκατάστασης εργαλείου.
- Άλλες σχετικές πληροφορίες
- Δυνατότητα εργαλείων για διαγραφή αρχείων , όλου του δίσκου ή και τα δύο.

Έχοντας υπόψη τις πιο πάνω προϋποθέσεις, κατέληξα στην επιλογή των ακόλουθων εργαλείων οριστικής διαγραφής δεδομένων :

1. AOMEI Partition Assistant
2. O&O SafeErase
3. Easy File Shredder

4. TS DataWiper
5. Abylon Shredder

Τα εργαλεία αυτά ελέγχθηκαν ότι πληρούν όλα τα κριτήρια που τέθηκαν, και μπορούν να αξιολογηθούν ως προς την απόδοση τους.

## 4.4 Ανάλυση / Παρουσίαση Εργαλείων Οριστικής Διαγραφής Δεδομένων

Ακολουθεί ανάλυση και παρουσίαση των πέντε εργαλείων οριστικής διαγραφής δεδομένων που πληρούν τις προδιαγραφές που τέθηκαν.

### 4.4.1 Εργαλείο 1 - AOMEI Partition Assistant


**Εικόνα 4-20: AOMEI Partition assistant 9.13.1**

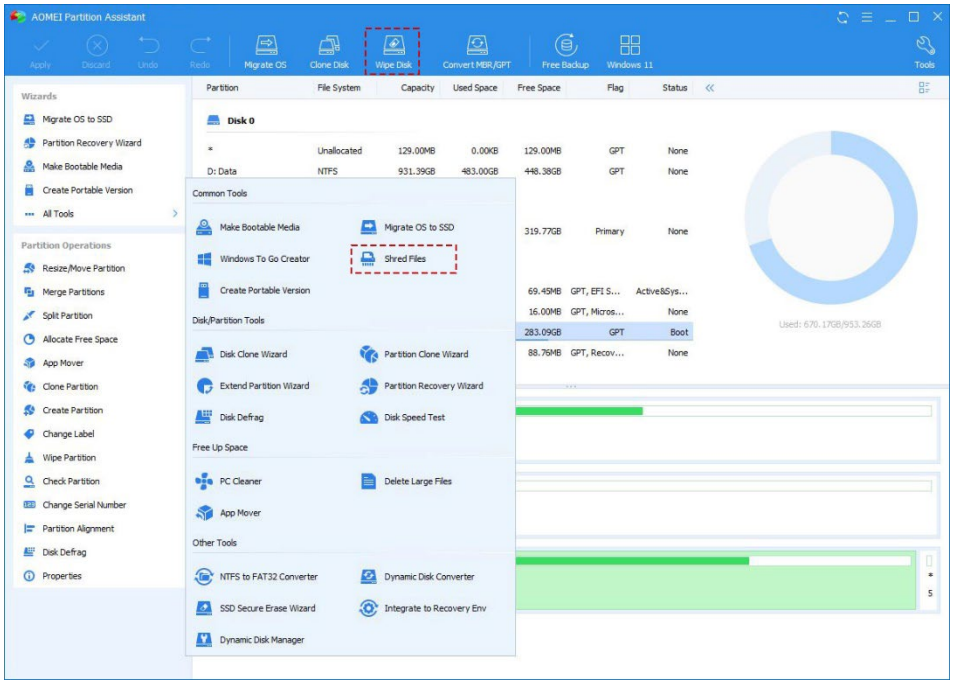
Το AOMEI Partition Assistant είναι ένα ισχυρό, πολυδύναμο και φιλικό προς το χρήστη εργαλείο διαχείρισης partitions για το λειτουργικό σύστημα Windows. Επιτρέπει στους χρήστες να διαχειρίζονται τα partitions του σκληρού τους δίσκου με αλλαγή μεγέθους (resizing), μετακίνηση, δημιουργία, διαγραφή, μορφοποίηση (formatting) , συγχώνευση (merging) και διαχωρισμό (splitting) τους. Επιπλέον με το AOMEI Partition Assistant, οι χρήστες μπορούν να αντιγράψουν, να κλωνοποιήσουν ή να μετεγκαταστήσουν ολόκληρο τον δίσκο ή τα διαμερίσματα τους σε ένα νέο, κάτι που είναι χρήσιμο κατά την αναβάθμιση σε μεγαλύτερο σκληρό δίσκο ή τη μεταφορά δεδομένων από έναν υπολογιστή σε άλλο. Περιλαμβάνει επίσης διάφορα εργαλεία για τη διόρθωση σφαλμάτων του συστήματος αρχείων, τη σάρωση για κατεστραμμένους τομείς (bad sectors) και την ασφαλή οριστική διαγραφή δεδομένων από έναν δίσκο.

| | |
|---|---|
| **Developer** | AOMEI Technology Co., Ltd.(*AOMEI | Windows & IPhone Backup Software, Partition Manager and Cloud Backup Service*, n.d.) |
| **Έκδοση** | 9.13.1 |
| **Έτος δημιουργίας** | 2010 |
| **Λειτουργικό Σύστημα** | Windows 11,10, 8.1, 8, 7, Vista, and XP (32/64-bit) |
| **Ελάχιστες απαιτήσεις συστήματος** | 500 MHz x86 or compatible CPU \| 256MB RAM |
| **Άδεια Χρήσης** | Δωρεάν και εκδόσεις επί πληρωμή |
| **Γλώσσες** | Αγγλικά, Γερμανικά, Γαλλικά, Ισπανικά, Ιταλικά, Ιαπωνικά, Κινέζικα και άλλες 12 γλώσσες. |
| **Ιστοσελίδα** | https://www.diskpart.com/ |

| **Βασικές λειτουργίες / δυνατότητες** | |
|---|---|
| Resize/Move Partition | Create Partition |
| Extend Partition Wizard | Delete Partition |
| Allocate Free Space | Format Partition |
| Merge Partitions | System Migration |
| Split Partitions | Clone Disk |
| Clone Partition | Move Application |
| Dynamic to Basic Disk Conversion | MBR and GPT Conversion |
| NTFS and FAT32 Conversion | Primary and Logical Conversion |
| Create Bootable Disk | Windows to Go Creator |
| Quick Partition | Partition Alignment |
| Partition Recovery | Wipe Disk / Partition |

| | |
|---|---|
| Change Drive Letter | Hide / Unhide Partition |
| Bad Sector Check | Shred Files |
| Schedule Disk Defragmentation | Disk Health Status Check |
| Check Partition | Command Line Partitioning |
| Rebuild MBR | Initialize Disk |
| Change Serial Number | Create Portable Version |

Στις πειραματικές δοκιμές που θα εκτελέσουμε, θα εξετάσουμε τις δυνατότητες του εργαλείου μόνο ως προς την ικανότητα του για οριστική διαγραφή όλων των δεδομένων από το σκληρό δίσκο όσο και για συγκεκριμένα αρχεία που βρίσκονται σε αυτόν. Οι υπόλοιπες λειτουργίες του εργαλείου δεν εμπίπτουν στο πεδίο εφαρμογής αυτής της μελέτης και δεν θα αξιολογηθούν.



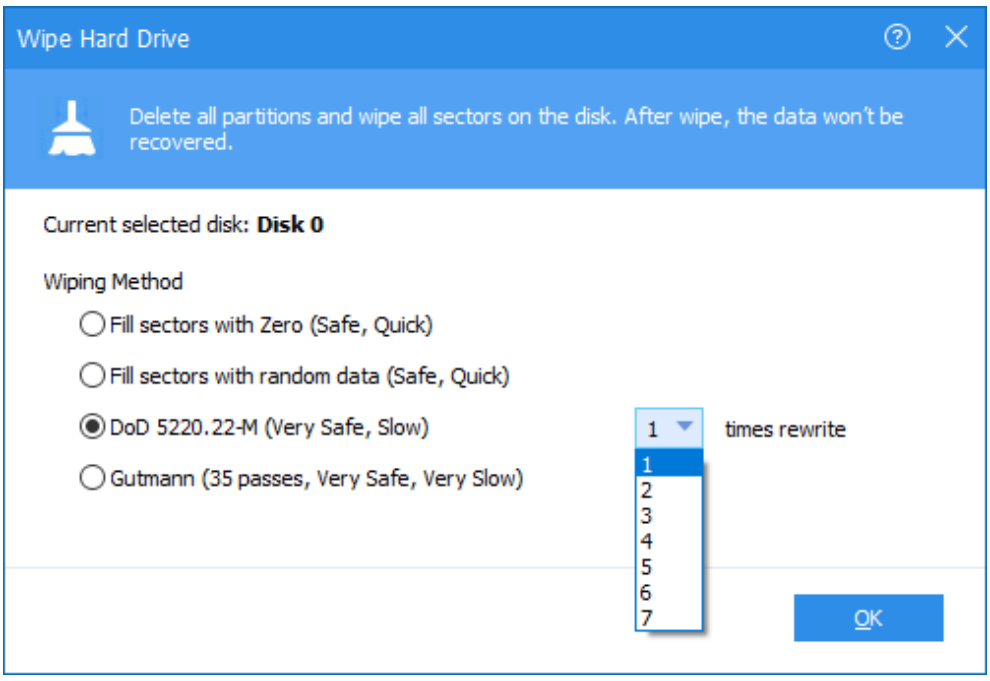

**Εικόνα 4-21: Στιγμιότυπο από το AOMEI Partition Assistant. Μπορούμε να δούμε τις επιλογές για οριστική διαγραφή του δίσκου ή συγκεκριμένων αρχείων.**

Το AOMEI Partition Assistant υποστηρίζει συνολικά τέσσερεις (4) μεθόδους επανεγγραφής δεδομένων στο δίσκο διαφορετικών επαναλήψεων και επιπέδων ασφαλείας. Μεταξύ τους είναι και η μέθοδος one pass zero που θα χρησιμοποιήσουμε στις πειραματικές δοκιμασίες. Ανάλογα με τον αριθμό επαναλήψεων των εγγραφών στο δίσκο αυξάνεται και ο συνολικός χρόνος οριστικής διαγραφής του.

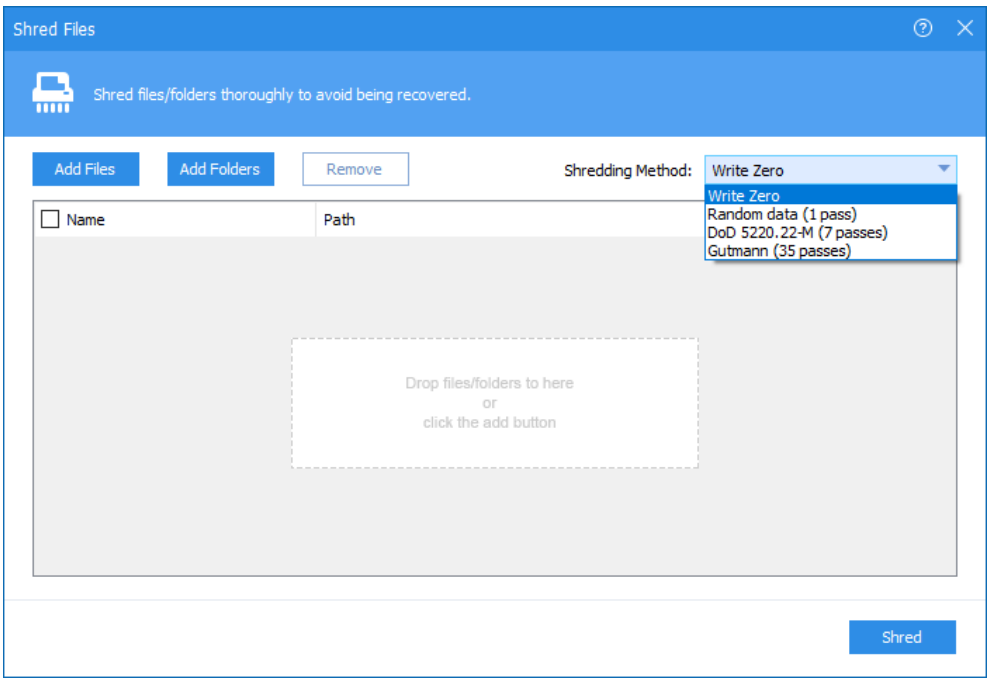
Συνολικά οι μέθοδοι επανεγγραφής που κάνει χρήση είναι:

1. One pass zero (1 επανάληψη)
2. Random Data (1 επανάληψη)
3. DoD 5220.22M (1-7 επαναλήψεις)
4. Gutmann (35 επαναλήψεις)

Να σημειώσουμε ότι για οριστική διαγραφή δεδομένων ολόκληρου του δίσκου με τη μέθοδο DoD 5220.22M το εργαλείο σου δίνει την δυνατότητα να επιλέξεις τον αριθμό των επαναλήψεων από 1 - 7 φορές. Αντίθετα για την διαγραφή συγκεκριμένων αρχείων η προκαθορισμένη επιλογή για τη μέθοδο DoD 5220.22M είναι 7 επαναλήψεις χωρίς δυνατότητα αλλαγής.




**Εικόνα 4-22: Στιγμιότυπο απο το AOMEI Partion Assistant. Μέθοδοι επανεγγραφής δεδομένων για διαγραφή ολόκληρου του δίσκου**




**Εικόνα 4-23: Στιγμιότυπο απο το AOMEI Partion Assistant. Μέθοδοι επανεγγραφής δεδομένων για διαγραφή συγκεκριμένων αρχείων στο δίσκο**

Το AOMEI Partition Assistant έχει επιλεγεί να είναι ένα από τα εργαλεία που θα αξιολογηθούν αφού ανταποκρίνεται σε όλα τα κριτήρια που έχουν τεθεί πιο πάνω, ενώ παράλληλα αποτελεί ένα δημοφιλές εργαλείο με πάνω από 50 εκατομμύρια χρήστες παγκόσμιος σύμφωνα με στοιχεία από τη σελίδα τους (*AOMEI Partition Assistant | Partition Manager Software for Windows PC and Server*, n.d.). Το γεγονός αυτό καθιστά ιδανική επιλογή το συγκεκριμένο εργαλείο για αξιολόγηση.

### 4.4.2 Εργαλείο 2 - O&O SafeEraser

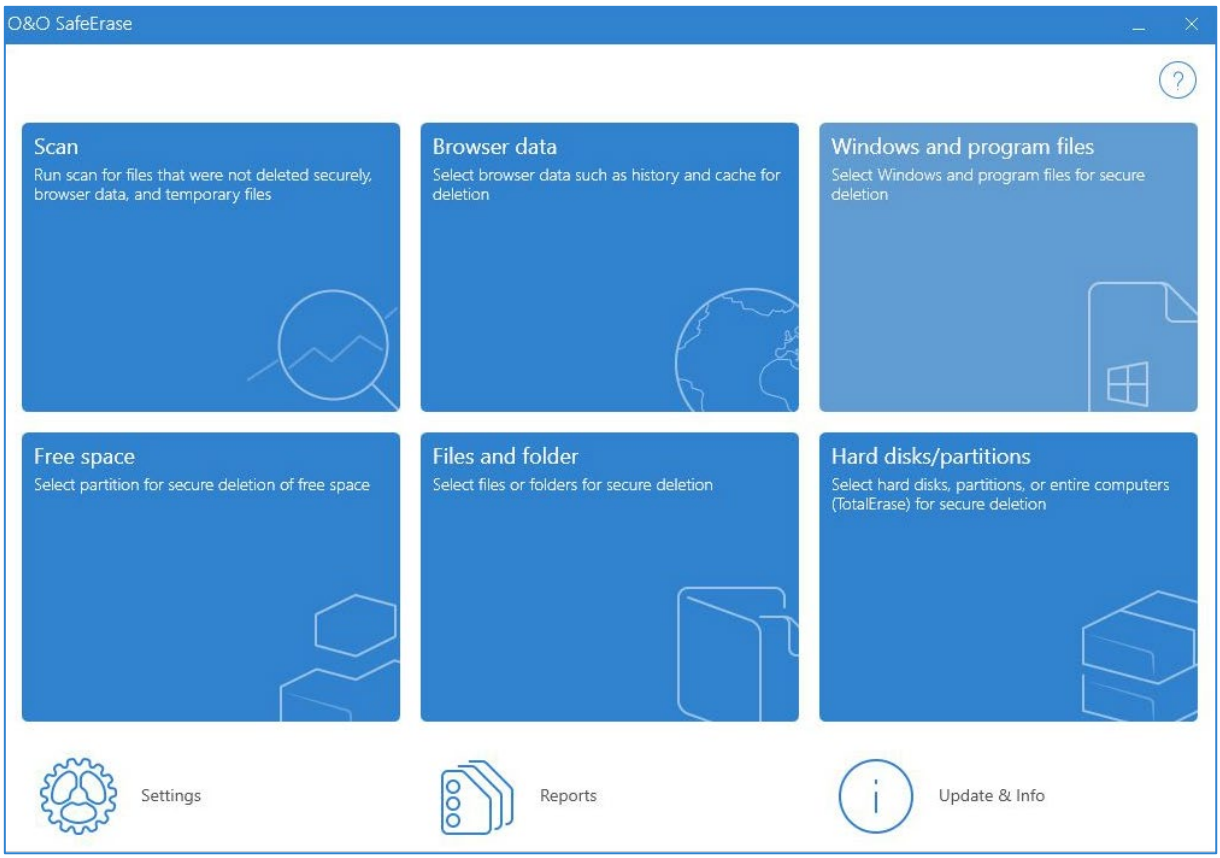

**Εικόνα 4-24: O&O SafeErase 15**

Το O&O SafeErase είναι ένα εργαλείο οριστικής διαγραφής δεδομένων που έχει σχεδιαστεί για να διαγράφει με ασφάλεια δεδομένα από υπολογιστές και συσκευές ψηφιακής αποθήκευσης. Το λογισμικό αναπτύσσεται από την γερμανική O&O Software GmbH, κορυφαίο πάροχο βοηθητικών προγραμμάτων συστήματος και λύσεων ασφάλειας δεδομένων για λειτουργικά συστήματα Windows. Το εργαλείο O&O SafeErase υπόσχεται στους χρήστες την προστασία των εμπιστευτικών πληροφορίων τους διαγράφοντας πλήρως και μόνιμα όλα τα ίχνη δεδομένων από τους σκληρούς δίσκους, τις μονάδες SSD, τις μονάδες USB και άλλους τύπους μέσων αποθήκευσης. Το λογισμικό χρησιμοποιεί προηγμένους αλγόριθμους για την αντικατάσταση των διαγραμμένων δεδομένων με τυχαίους χαρακτήρες και μηδενικά, καθιστώντας ουσιαστικά αδύνατη την ανάκτηση. Επιπλέον, το O&O SafeErase μπορεί επίσης να διαγράψει με ασφάλεια ολόκληρους σκληρούς δίσκους, διαμερίσματα και ελεύθερο χώρο, διασφαλίζοντας ότι δεν θα μείνουν υπολειπόμενα δεδομένα. Το εργαλείο O&O SafeErase έχει σχεδιαστεί να προσφέρει ευκολία χρήσης, καθιστώντας το προσβάσιμο τόσο σε αρχάριους όσο και σε προχωρημένους χρήστες. Το λογισμικό διαθέτει μια φιλική προς το χρήστη διεπαφή που επιτρέπει στους χρήστες να επιλέξουν τα αρχεία, τους φακέλους ή τις μονάδες δίσκου που θέλουν να διαγράψουν και στη συνέχεια να επιλέξουν από μια ποικιλία μεθόδων ασφαλούς διαγραφής. Οι χρήστες μπορούν επίσης να ρυθμίσουν προγραμματισμένες εργασίες διαγραφής για αυτόματη διαγραφή ευαίσθητων δεδομένων σε καθορισμένα χρονικά διαστήματα που οι ίδιοι επιθυμούν.

| | |
|---|---|
| **Developer** | O&O Software GmbH(*About O&O*, n.d.) |
| **Έκδοση** | 15 |
| **Έτος δημιουργίας** | 2004 |
| **Λειτουργικό Σύστημα** | Windows 11,10, 8.1, 8, 7, Vista, and XP (32/64-bit) |
| **Ελάχιστες απαιτήσεις συστήματος** | 50 MB free disk space \| 1 GHz processor \| 512 MB RAM |
| **Άδεια Χρήσης** | Δωρεάν δοκιμαστική έκδοση και εκδόσεις επί πληρωμή |
| **Γλώσσες** | Αγγλικά & Γερμανικά |
| **Ιστοσελίδα** | https://www.oo-software.com/en/safeerase-hard-drive-data-secure-deletion |

| Βασικές λειτουργίες / δυνατότητες | |
|---|---|
| | Σάρωση δίσκου για εύρεση προσωρινών αρχείων και διαγραφή τους |
| | Διαγραφή δεδομένων ιστορικού από browsers |
| | Διαγραφή προγραμμάτων και περιεχομένου κάδου ανακύκλωσης |
| | Οριστική διαγραφή αρχείων και φακέλων |
| | Οριστική διαγραφή ολόκληρου του δίσκου ή partitions |

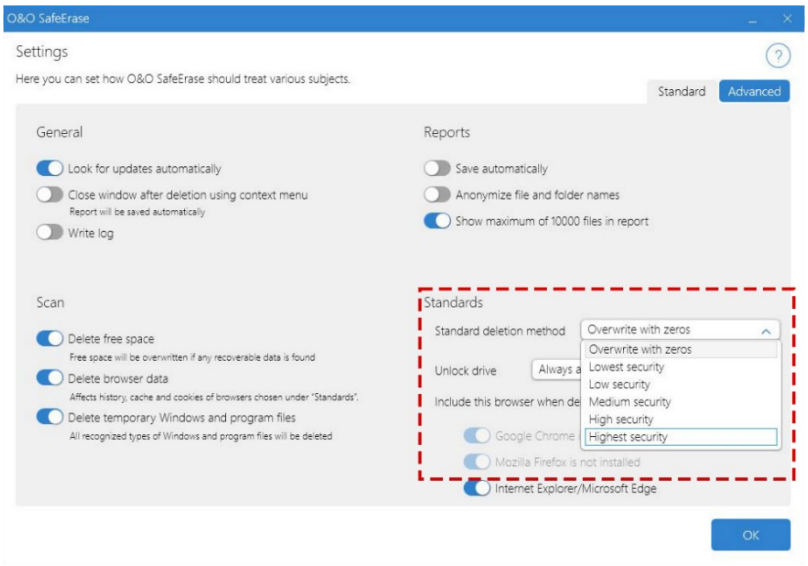
Στις πειραματικές δοκιμές που θα εκτελέσουμε, θα εξετάσουμε τις δύο τελευταίες δυνατότητες του εργαλείου, δηλαδή μόνο ως προς την ικανότητα του για οριστική διαγραφή όλων των δεδομένων από το σκληρό δίσκο και για συγκεκριμένα αρχεία που βρίσκονται σε αυτόν. Οι υπόλοιπες λειτουργίες του εργαλείου δεν εμπίπτουν στο πεδίο εφαρμογής αυτής της μελέτης και δεν θα αξιολογηθούν.



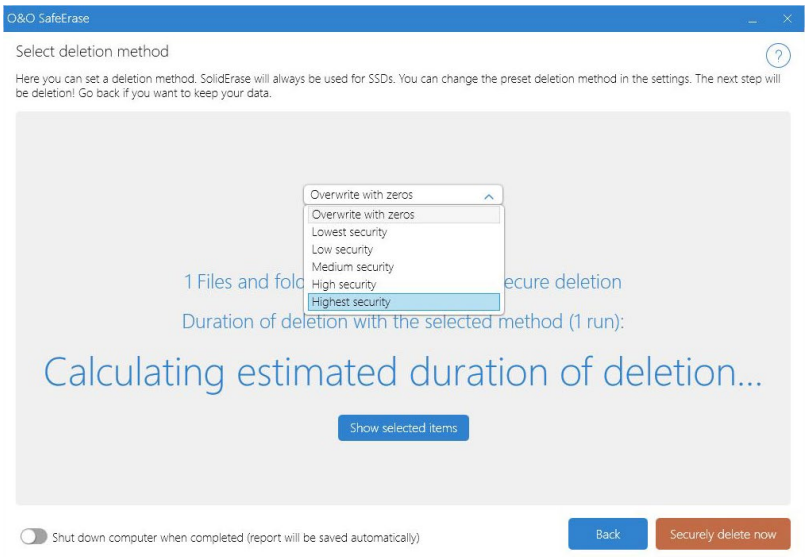

**Εικόνα 4-25: Στιγμιότυπο από το κεντρικό μενού του O&O SafeErase**

Το O&O SafeErase υποστηρίζει συνολικά έξι (6) μεθόδους επανεγγραφής δεδομένων διαφορετικών επιπέδων ασφαλείας. Στις ρυθμίσεις του εργαλείου οι έξι μέθοδοι αναφέρονται ως εξής:

1. Overwrite with zeros
2. Lowest Security
3. Low Security
4. Medium Security
5. High Security
6. Highest Security




**Εικόνα 4-26: Στιγμιότυπο από το O&O SafeErase. Μέθοδοι επανεγγραφής δεδομένων**




**Εικόνα 4-27: Στιγμιότυπο από το O&O SafeErase. Μέθοδοι επανεγγραφής δεδομένων για διαγραφή συγκεκριμένων αρχείων στο δίσκο**

Τα ονόματα που δίνονται στις μεθόδους από τον κατασκευαστή δεν περιγράφουν ακριβώς τον αλγόριθμο που χρησιμοποιείται αντίστοιχα σε κάθε περίπτωση. Αντίθετα είναι γενικά και προφανώς επιλέχτηκαν ώστε να μην προκαλούν σύγχυση στους αρχάριους χρήστες. Για να εντοπίσουμε τις αντιπροσωπευτικές μεθόδους ανατρέξαμε στην επίσημη ιστοσελίδα(*Method of Deletion O&O Software,* n.d.) του εργαλείου όπου σύμφωνα με αυτή οι πιο πάνω μέθοδοι αντιστοιχούν στους ακόλουθους αλγόριθμους.

1. Overwrite with zeros – Η μέθοδος αυτή περιλαμβάνει μια εγγραφή του δίσκου με μηδενικά. Παρέχει την γρηγορότερη διαγραφή δεδομένων και αυτή θα υλοποιήσουμε κατά τη διάρκεια των πειραματικών δοκιμών.

2. Lowest Security – Η μέθοδος αυτή απαιτεί μια επανεγγραφή του δίσκου με τυχαία δεδομένα. Είναι επίσης γρήγορη μέθοδος.

3. Low Security – Η μέθοδος αυτή είναι η αντίστοιχη DoD 5220.22-M E που περιλαμβάνει συνολικά 3 επαναλήψεις εγγραφών δεδομένων στο δίσκο.

4. Medium Security – Η μέθοδος αυτή είναι σύμφωνη με τα πρότυπα του German BSI όπως περιγράφεται μέσα από το BSI IT Baseline Protection Manual. Συνολικά γίνονται 6 επανεγγραφές δεδομένων στο δίσκο.

5. High Security – Η μέθοδος αυτή είναι η αντίστοιχη DoD 5220.22-M ECE. Συνολικά γίνονται 7 επανεγγραφές στο δίσκο.

6. Highest Security – Η μέθοδος αυτή αντιστοιχεί στην αλγόριθμο που αναπτύχθηκε από τον Peter Gutmann και απαιτεί 35 επανεγγραφές δεδομένων. Λόγω των πολλών επαναλήψεων η μέθοδος αυτή είναι και η πιο χρονοβόρα.

Το O&O SafeErase έχει επιλεγεί να είναι ένα από τα εργαλεία που θα αξιολογηθούν αφού ανταποκρίνεται σε όλα τα κριτήρια που έχουν τεθεί πιο πάνω. Επίσης πρόκειται για ένα εργαλείο το οποίο βρίσκεται στην αγορά με τακτικές αναβαθμίσεις και νέες εκδόσεις για σχεδόν μια εικοσαετία χωρίς να έχει μέχρι σήμερα αξιολογηθεί η αποτελεσματικότητα του. Το γεγονός αυτό καθιστά ιδανική επιλογή το συγκεκριμένο εργαλείο για δοκιμή.

### 4.4.3 Εργαλείο 3 - Easy File Shredder


**Εικόνα 4-28: Easy File Shredder**

Το Easy File Shredder είναι ακόμα ένα εργαλείο που επιτρέπει στους χρήστες να διαγράφουν με ασφάλεια ανεπιθύμητα αρχεία από τον υπολογιστή τους. Αναπτύχθηκε από την αμερικάνικη εταιρεία λογισμικού WebMinds, που ειδικεύεται στην ανάπτυξη εφαρμογών, σε λύσεις ασφάλειας δεδομένων και υπηρεσίες Διαδικτύου. Η λειτουργία του βασίζεται στην κλασική αντικατάσταση των ήδη γραμμένων δεδομένων στο δίσκο με νέα. Η διαδικασία αυτή διασφαλίζει την οριστική και αμετάκλητη διαγραφή των δεδομένων από τα μέσα αποθήκευσης. Αυτό που ξεχωρίζει το συγκεκριμένο εργαλείο από τους ανταγωνιστές του είναι το απλό και εύχρηστο γραφικό περιβάλλον αλλά και η ποικιλία σε επιλογές όσο αφορά την μέθοδο διαγραφής. Συγκεκριμένα το εργαλείο περιλαμβάνει 13 μεθόδους διαγραφής ενώ παράλληλα δίνει την δυνατότητα στο χρήστη να δημιουργήσει το δικό του αλγόριθμο επανεγγραφής δεδομένων στο δίσκο.

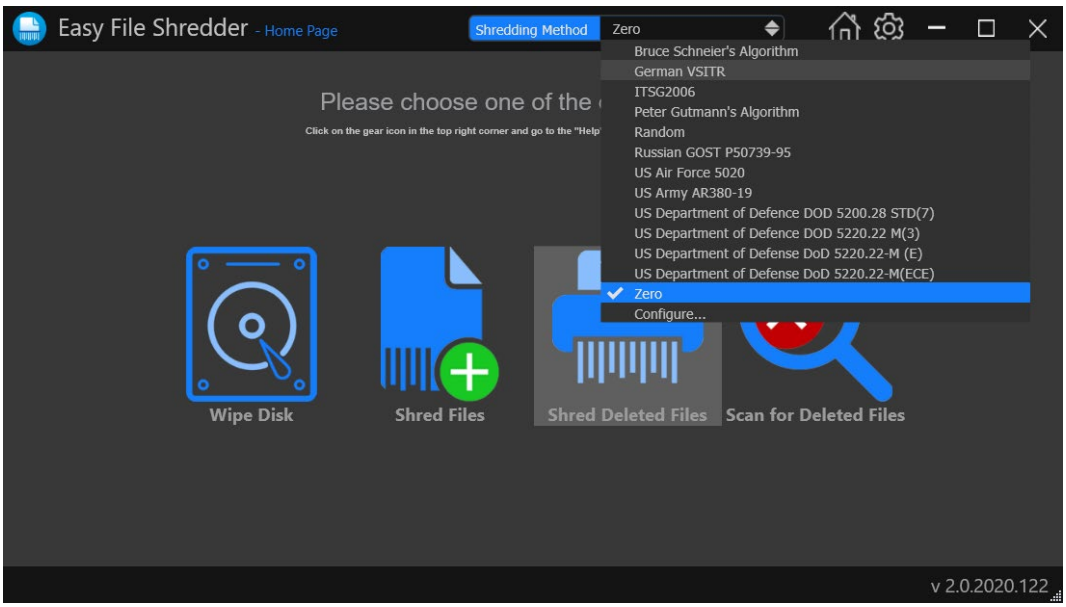
| | |
|---|---|
| **Developer** | WebMinds, Inc.(*WebMinds*, n.d.) |
| **Έκδοση** | 2.0.2020.122 |
| **Έτος δημιουργίας** | 2007 |
| **Λειτουργικό Σύστημα** | Windows XP, Vista ,7, 8 ,10 & 11 (32/64-bit versions) |
| **Ελάχιστες απαιτήσεις συστήματος** | - |
| **Άδεια Χρήσης** | Δωρεάν δοκιμαστική έκδοση με περιορισμούς και έκδοση επί πληρωμή |
| **Γλώσσες** | Αγγλικά |
| **Ιστοσελίδα** | https://www.easyfileshredder.com/ |

| Βασικές λειτουργίες / δυνατότητες | |
|---|---|
|  | Οριστική διαγραφή αρχείων και φακέλων |
|  | Οριστική διαγραφή ολόκληρου του δίσκου |
|  | Διαγραφή ελεύθερου χώρου στο δίσκο |
|  | Αναζήτηση διαγραμμένων αρχείων στο δίσκο |

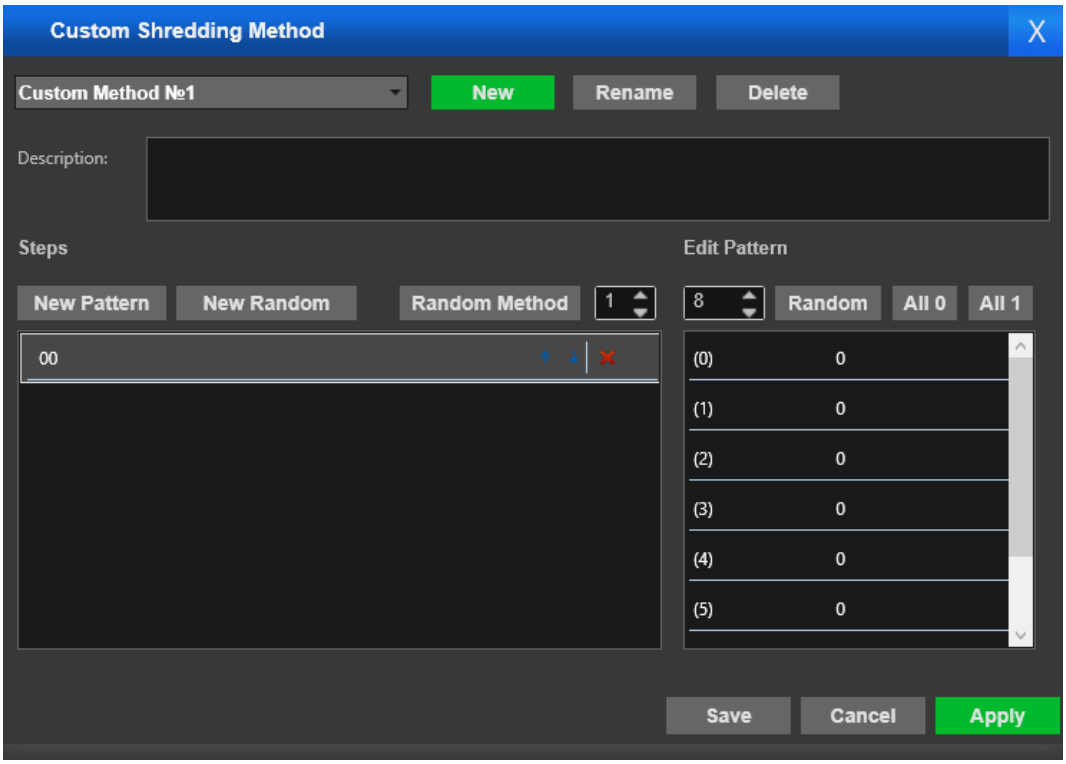
Το Easy File Shredder υποστηρίζει συνολικά δεκατρείς (13) μεθόδους διαγραφής δεδομένων διαφορετικών επιπέδων ασφαλείας. Στις ρυθμίσεις του εργαλείου οι μέθοδοι είναι:

1. Zero Algorithm (1 επανάληψη)
2. US Department of Defense DOD 5220.22-M (ECE) (3 επαναλήψεις)
3. US Department of Defense DOD 5220.22-M (E) (3 επαναλήψεις)
4. US Department of Defense DOD 5220.22 M(3) (3 επαναλήψεις)
5. US Department of Defense DOD 5200.28 STD(7) (7 επαναλήψεις)
6. US Army AR380-19 (3 επαναλήψεις)
7. US Air Force 5020 (3 επαναλήψεις)
8. Russian GOST P50739-95 (2 επαναλήψεις)
9. Random algorithm (1 επανάληψη)
10. Peter Gutmann's Algorithm (35 επαναλήψεις)
11. ITSG2006 (3 επαναλήψεις)
12. German VSITR (7 επαναλήψεις)
13. Bruce Schneier's Algorithm (7 επαναλήψεις)

Επίσης το εργαλείο δίνει τη δυνατότητα στο χρήστη να δημιουργήσει το δικό του μοτίβο διαγραφής δεδομένων με όσες επαναλήψεις επιθυμεί.




**Εικόνα 4-29: Στιγμιότυπο από το Easy File Shredder. Μέθοδοι επανεγγραφής δεδομένων**




**Εικόνα 4-30: Στιγμιότυπο από το Easy File Shredder. Δημιουργία προσαρμοσμένης μεθόδου διαγραφής**

Το Easy File Shredder έχει επιλεγεί να είναι ένα από τα εργαλεία που θα αξιολογηθούν αφού ανταποκρίνεται σε όλα τα κριτήρια που έχουν τεθεί. Επίσης πρόκειται για ένα εργαλείο το οποίο βρίσκεται αρκετά χρόνια στην αγορά και εμφανίζεται στις πρώτες θέσεις κατά την αναζήτηση εργαλείων οριστικής διαγραφής στο διαδίκτυο. Το εργαλείο δεν έχει μέχρι σήμερα αξιολογηθεί η αποτελεσματικότητα του και αυτό το γεγονός το καθιστά ιδανική επιλογή για δοκιμή.

### 4.4.4 Εργαλείο 4 - TS DataWiper

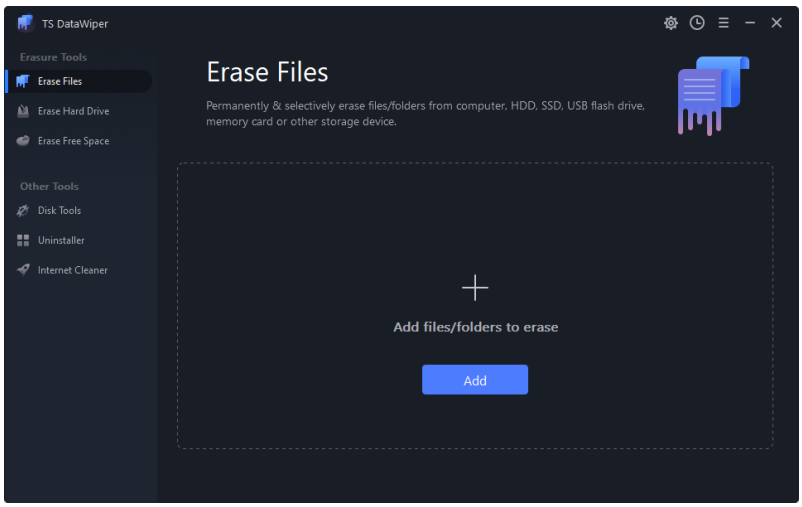

**Εικόνα 4-31: TS DataWiper**

Το TS DataWiper είναι ένα ισχυρό και ευέλικτο εργαλείο διαγραφής δεδομένων που παρέχει μια ασφαλή και αξιόπιστη λύση για τη μόνιμη διαγραφή ευαίσθητων δεδομένων από διάφορα μέσα αποθήκευσης. Το εργαλείο αναπτύχθηκε από την TS Software, ένα αξιόπιστο όνομα στον τομέα των λύσεων ασφάλειας δεδομένων και ανάκτησης. Το TS DataWiper έχει σχεδιαστεί για να ανταποκρίνεται στις ανάγκες ατόμων, επιχειρήσεων και οργανισμών που απαιτούν μια ασφαλή και αποτελεσματική μέθοδο για τη διαγραφή δεδομένων από διαφορετικούς τύπους συσκευών, συμπεριλαμβανομένων σκληρών δίσκων, δίσκων SSD, μονάδων flash USB, καρτών μνήμης και άλλων αποθηκευτικών συσκευών. Με τους προηγμένους αλγόριθμους οριστικής διαγραφής δεδομένων, το TS DataWiper μπορεί να διαγράψει δεδομένα πέρα από την ανάκτηση, διασφαλίζοντας ότι οι ευαίσθητες πληροφορίες παραμένουν εμπιστευτικές και δεν μπορούν να ανακτηθούν από μη εξουσιοδοτημένα άτομα. Επιπλέον, το εργαλείο διαθέτει μια φιλική προς το χρήστη διεπαφή που το καθιστά εύκολο στη λειτουργία ακόμη και για αρχάριους χρήστες. Το TS DataWiper είναι επίσης συμβατό με διαφορετικά λειτουργικά συστήματα, συμπεριλαμβανομένων των Windows και Mac OS. Τέλος το λογισμικό εργαλείο μπορεί να δημιουργήσει αναφορές ολοκλήρωσης διαγραφής για σκοπούς συμμόρφωσης, επιτρέποντας στους οργανισμούς να αποδείξουν τη συμφωνία τους με τους κανονισμούς προστασίας δεδομένων και τα διεθνή πρότυπα.

| | |
|---|---|
| **Developer** | TS Technologies(*About TogetherShare | Learn More about TogetherShare*, n.d.) |
| **Έκδοση** | 2.2 |
| **Έτος δημιουργίας** | 2018 |
| **Λειτουργικό Σύστημα** | Windows 10/8/7/Vista/XP, Windows Server 2019/2016/2012 \| macOS 10.7 ~ macOS Ventura |
| **Ελάχιστες απαιτήσεις συστήματος** | 60 MB free disk space \| 1 GHz or faster processor \| 512 MB RAM or more |
| **Άδεια Χρήσης** | Δωρεάν δοκιμαστική έκδοση και έκδοση επί πληρωμή |
| **Γλώσσες** | Αγγλικά |
| **Ιστοσελίδα** | https://www.togethershare.com/data-eraser/datawiper-for-windows.html |

| **Βασικές λειτουργίες / δυνατότητες** | |
|---|---|
|  | Οριστική διαγραφή αρχείων και φακέλων |
|  | Οριστική διαγραφή ολόκληρου του δίσκου / διαμερίσματος |
|  | Διαγραφή ελεύθερου χώρου στο δίσκο |
|  | Διαχείριση δίσκων (μορφοποίηση, μετονομασία, επισκευή) |
|  | Δημιουργία αναφορών διαγραφής |
|  | Απεγκατάσταση εφαρμογών |

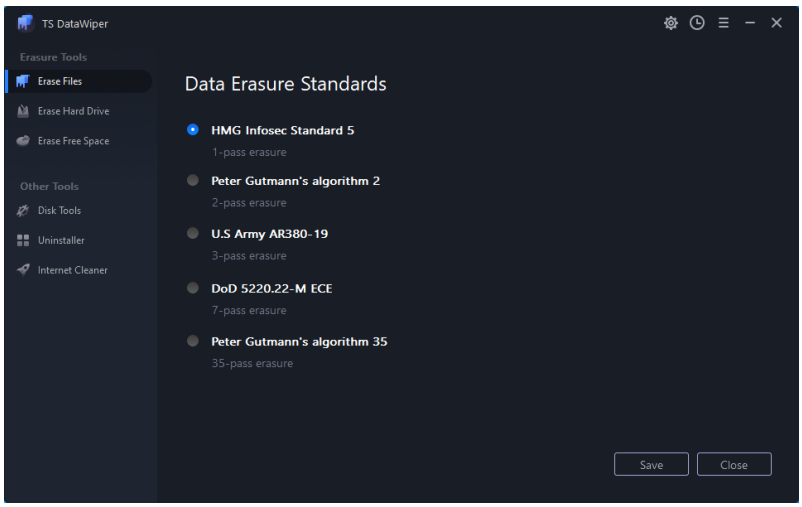
Στις πειραματικές δοκιμές που θα εκτελέσουμε, θα εξετάσουμε τις δύο πρώτες λειτουργίες του εργαλείου, δηλαδή μόνο ως προς την ικανότητα του για οριστική διαγραφή όλων των δεδομένων από το σκληρό δίσκο και για αρχεία που εμείς θα επιλέξουμε. Επίσης θα συγκρίνουμε αν οι αναφορές διαγραφής που δημιουργούνται από την εφαρμογή συμφωνούν με τα πραγματικά αποτελέσματα στο δίσκο. Οι υπόλοιπες λειτουργίες του εργαλείου δεν εμπίπτουν στο πεδίο εφαρμογής αυτής της μελέτης και δεν θα αξιολογηθούν.




**Εικόνα 4-32: Στιγμιότυπο απο το κεντρικό μενού του TS DataWiper**

Το TS DataWiper υποστηρίζει συνολικά πέντε (5) μεθόδους διαγραφής δεδομένων διαφορετικών επιπέδων ασφαλείας. Στις ρυθμίσεις του εργαλείου οι πέντε μέθοδοι αναφέρονται ως εξής:

1. HMG Infosec Standard 5 (1 επανάληψη)
2. Peter Gutmann's algorithm 2 (2 επαναλήψεις)
3. U.S Army AR380-19 (3 επαναλήψεις)
4. DoD 5220.22-M ECE (7 επαναλήψεις)
5. Peter Gutmann's algorithm 35 (35 επαναλήψεις)




**Εικόνα 4-33: Στιγμιότυπο απο το TS DataWiper. Μέθοδοι επανεγγραφής δεδομένων**

Το TS DataWiper έχει επιλεγεί να είναι ένα από τα εργαλεία που θα αξιολογηθούν αφού ανταποκρίνεται σε όλα τα κριτήρια που έχουν τεθεί. Επίσης πρόκειται για ένα σχετικά καινούργιο εργαλείο με αρκετή δημοτικότητα ωστόσο χωρίς να αξιολογηθεί η αποτελεσματικότητα του μέχρι σήμερα. Το γεγονός αυτό καθιστά ιδανική επιλογή το συγκεκριμένο εργαλείο για δοκιμή.

### 4.4.5 Εργαλείο 5 - Abylon Shredder

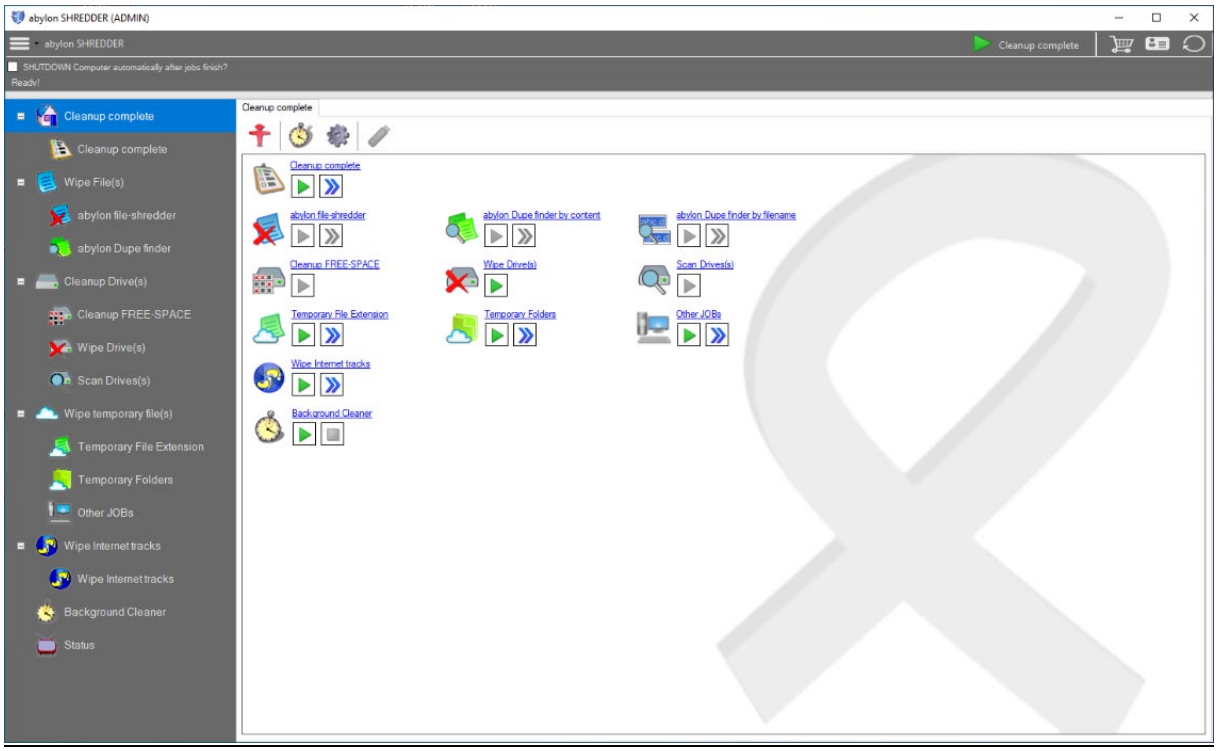

**Εικόνα 4-34: Abylon Shredder**

Το Abylon Shredder είναι ένα εργαλείο που έχει σχεδιαστεί για να διασφαλίζει την ασφαλή διαγραφή δεδομένων από συστήματα υπολογιστών ή εξωτερικές συσκευές αποθήκευσης. Αναπτύχθηκε από την abylonsoft, μια γερμανική εταιρεία λογισμικού που ειδικεύεται σε λύσεις ασφάλειας δεδομένων και κρυπτογράφησης. Το Abylon Shredder χρησιμοποιεί αλγόριθμους που αντικαθιστούν τα αρχεία με νέα δεδομένα, καθιστώντας αδύνατο για οποιοδήποτε λογισμικό ανάκτησης να επαναφέρει τα διαγραμμένα αρχεία. Το Abylon Shredder μπορεί να διαγράψει οριστικά μεμονωμένα αρχεία, πλήρεις φακέλους, ακόμη και ελεύθερο χώρο σε έναν δίσκο, διασφαλίζοντας ότι τυχόν ίχνος διαγραμμένων δεδομένων αφαιρείται από το σύστημα. Επιπλέον, το εργαλείο περιλαμβάνει τη δυνατότητα να επιτρέπει στους χρήστες να διαγράφουν με ασφάλεια ίχνη περιήγησης στο Διαδίκτυο, προσωρινά αρχεία και cookies, διασφαλίζοντας ότι το ιστορικό περιήγησής τους δεν είναι ανιχνεύσιμο.

| | |
|---|---|
| **Developer** | abylonsoft GmbH(Germany, n.d.) |
| **Έκδοση** | 23.10.12.3 |
| **Έτος δημιουργίας** | 2001 |
| **Λειτουργικό Σύστημα** | Windows 11/10/8/7/Vista/XP 32-Bit, 64-Bit |
| **Ελάχιστες απαιτήσεις συστήματος** | 40 MB free disk space \| screen resolution min. 1024x600p \| 512 MB RAM or more \| Processor: Pentium (or comparable) |
| **Άδεια Χρήσης** | Δωρεάν δοκιμαστική έκδοση 30 ημερών και έκδοση επί πληρωμή |
| **Γλώσσες** | Αγγλικά και Γερμανικά |
| **Ιστοσελίδα** | https://www.abylonsoft.com/shredder/ |

| Βασικές λειτουργίες / δυνατότητες | |
|---|---|
|  | Οριστική διαγραφή αρχείων και φακέλων |
|  | Οριστική διαγραφή ολόκληρου του δίσκου / διαμερίσματος |
|  | Διαγραφή ελεύθερου χώρου στο δίσκο |
|  | Διαγραφή ιχνών περιήγησης στο Διαδίκτυο |
|  | Διαγραφή προσωρινών αρχείων |
|  | Ρύθμιση προγραμματισμένων εργασιών διαγραφής για αυτόματη διαγραφή ευαίσθητων δεδομένων σε καθορισμένα χρονικά διαστήματα |

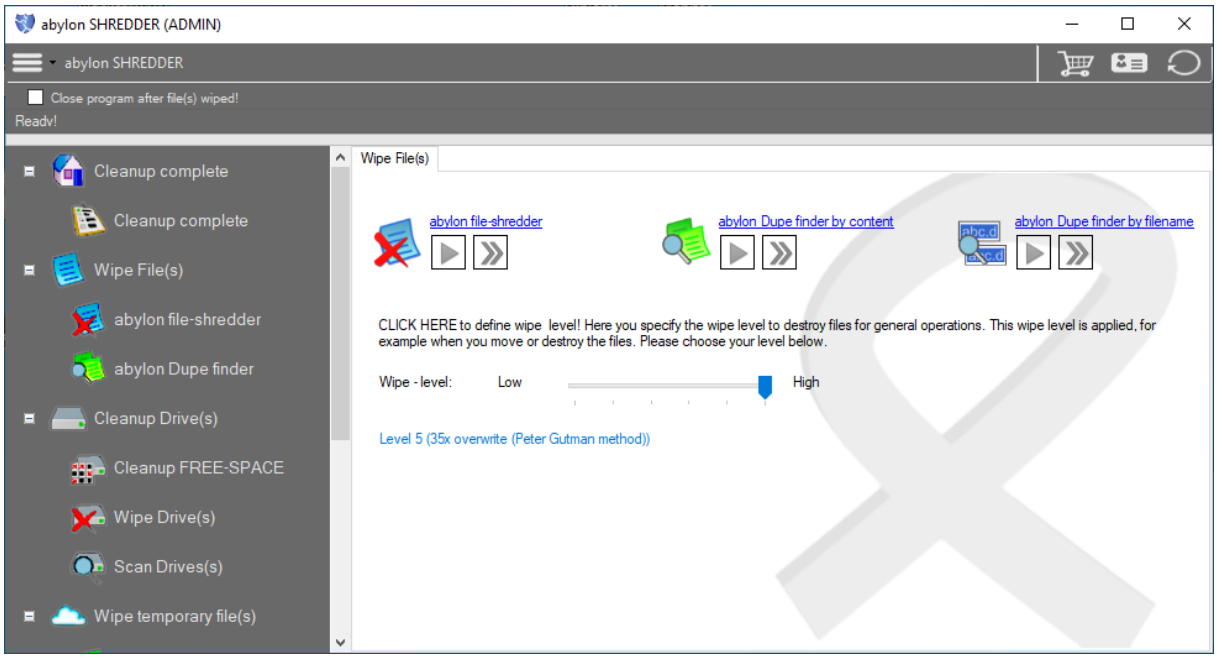
Στην πειραματική αξιολόγηση που θα εκτελέσουμε, θα εξετάσουμε τις δύο πρώτες λειτουργίες του εργαλείου, δηλαδή την ικανότητα του για οριστική διαγραφή ολόκληρου του σκληρού δίσκου και την ικανότητα του για διαγραφή συγκεκριμένων αρχείων που βρίσκονται σε αυτόν. Οι υπόλοιπες λειτουργίες του εργαλείου δεν εμπίπτουν στο πεδίο εφαρμογής αυτής της μελέτης και δεν θα αξιολογηθούν.




**Εικόνα 4-35: Στιγμιότυπο από το κεντρικό μενού του Abylon Shredder**

Το Abylon Shredder υποστηρίζει συνολικά πέντε (5) μεθόδους διαγραφής δεδομένων διαφορετικών επιπέδων ασφαλείας. Στις ρυθμίσεις του εργαλείου οι πέντε μέθοδοι αναφέρονται ως εξής:

1. Επίπεδο 1 – Εγγραφή με μηδενικά (1 επανάληψη)
2. Επίπεδο 2 – Εγγραφή με μηδενικά και τυχαία δεδομένα (3 επαναλήψεις)
3. Επίπεδο 3 – Μέθοδος DoD II (7 επαναλήψεις)
4. Επίπεδο 4 – Μέθοδος DoD II και τυχαία δεδομένα (13 επαναλήψεις)
5. Επίπεδο 5 – Peter Gutmann's algorithm (35 επαναλήψεις)




**Εικόνα 4-36: Στιγμιότυπο από το Abylon Shredder. Μέθοδοι επανεγγραφής δεδομένων**

Το Abylon Shredder έχει επιλεγεί να είναι ένα από τα εργαλεία που θα αξιολογηθούν αφού ανταποκρίνεται σε όλα τα κριτήρια που έχουν τεθεί πιο πάνω. Επίσης πρόκειται για ένα εργαλείο το οποίο βρίσκεται στην αγορά από το 2001 με συνεχόμενες αναβαθμίσεις και αρκετά βραβεία χωρίς να έχει μέχρι σήμερα αξιολογηθεί η αποτελεσματικότητα του. Το γεγονός αυτό καθιστά ιδανική επιλογή το συγκεκριμένο εργαλείο για δοκιμή.

# Κεφάλαιο 5
# Πειραματική διαδικασία

Η υλοποίηση της πειραματικής διαδικασίας προϋποθέτει εμπεριστατωμένο αρχικό σχεδιασμό, ώστε να διασφαλιστεί η ακρίβεια και αξιοπιστία των αποτελεσμάτων. Ο κακός πειραματικός σχεδιασμός μπορεί να οδηγήσει σε σπατάλη χρόνου και πόρων, καθώς τα πειράματα μπορεί να χρειαστεί να επαναληφθούν ή μπορεί να αποφέρουν ασαφή αποτελέσματα. Ο προσεκτικός πειραματικός σχεδιασμός είναι κρίσιμος για την επιτυχία οποιουδήποτε ερευνητικού έργου και διασφαλίζει ότι τα αποτελέσματα που λαμβάνονται είναι έγκυρα και χρήσιμα για την επιβεβαίωση της θεωρίας και της πρακτικής στο σχετικό πεδίο. Σχεδιάζοντας τις πειραματικές δοκιμές για αξιολόγηση των εργαλείων οριστικής διαγραφής προσεκτικά από την αρχή, μπορούμε να διασφαλίσουμε ότι τα τελικά συμπεράσματα που εξάγονται είναι ορθά. Για αυτό ακριβώς το λόγο προχωρήσαμε με τον καθορισμό σαφών βημάτων τα οποία θα ακολουθηθούν κατά την αξιολόγηση όλων των εργαλείων προς εξέταση.

## 5.1 Περιγραφή Πειραματικής Διαδικασίας

Βήματα:

1. Εύρεση, συλλογή δειγμάτων αρχείων από το διαδίκτυο και δημιουργία λίστας με αρχεία που θα τοποθετηθούν στο δίσκο για διαγραφή. Συνολικά δημιουργήθηκαν τρείς (3) ομάδες αρχείων, μιας και οι πειραματικές δοκιμές θα εξετάσουν τρία διαφορετικά σενάρια για κάθε εργαλείο.

    α. Ομάδα 1 - Αποτελείται από 20 συγκεκριμένα αρχεία διαφόρων τύπων που θα επιλεγούν κατά την εξέταση του εργαλείου ως προς την ικανότητα του για οριστική διαγραφή επιλεγμένων αρχείων και φακέλων.

    β. Ομάδα 2 - Συλλογή από διάφορους τύπους αρχείων συνολικού μεγέθους 10 GB. Τα αρχεία αυτά θα αντιγραφούν στο δίσκο και θα διαγραφούν κατά την εξέταση του εργαλείου σχετικά με την ικανότητα του για οριστική διαγραφή του δίσκου.

    γ. Ομάδα 3 – Συλλογή από διάφορους τύπους αρχείων συνολικού μεγέθους 200 GB. Τα αρχεία αυτά θα αντιγραφούν στο δίσκο και θα διαγραφούν κατά την εξέταση του εργαλείου σχετικά με την ικανότητα του για οριστική διαγραφή του δίσκου όπως επίσης εξέταση της μεταβλητής αν το συνολικό μέγεθος των δεδομένων παίζει ρόλο στα αποτελέσματα.

    Ο αναλυτικός κατάλογος των αρχείων αυτών μαζί με το ακριβές μέγεθος τους, τον τύπο τους και την hash τιμή MD5 η οποία θα χρησιμοποιηθεί αργότερα κατά την σύγκριση τους με τα ευρήματα στο δίσκο βρίσκεται στο τέλος (Παράρτημα Α).

2. Αρχικοποίηση – Με τη χρήση της συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser για την οποία αναφορά έγινε πιο πάνω, διαγράφουμε το δίσκο ώστε σε αυτό να υπάρχουν μόνο μηδενικά. Η διαδικασία της διαγραφής/ αρχικοποίησης του δίσκου είναι ανεξάρτητη και δεν απαιτεί οποιανδήποτε σύνδεση της συσκευής με τον υπολογιστή. Με την ολοκλήρωση της διαδικασίας αναμένουμε να έχουμε σε όλους τους τομείς του σκληρού δίσκου γραμμένα μόνο binary μηδενικά.

3. Αφού ολοκληρωθεί η διαδικασία διαγραφής συνδέουμε τη συσκευή στην οποία βρίσκεται ο δίσκος, με τον υπολογιστή διαμέσου της διεπαφής USB 3.0 που διαθέτει. Με τη χρήση του εργαλείου USB Write Blocker διασφαλίζουμε ότι ο δίσκος βρίσκεται σε READ ONLY κατάσταση και καμιά πληροφορία δεν θα μεταφερθεί σε αυτό.

4. Εκτελούμε το λογισμικό HxD με δικαιώματα διαχειριστή και στη συνέχεια επιλέγουμε από το μενού την επιλογή για να εμφανιστούν όλοι οι φυσικοί δίσκοι που βρίσκονται συνδεδεμένοι στον υπολογιστή. Αφού εντοπίσουμε τον διαγραμμένο δίσκο, τον επιλέγουμε για να έχουμε μια αναπαράσταση των περιεχομένων του δίσκου ώστε να βεβαιωθούμε ότι όλα τα bit που βρίσκονται σε αυτόν είναι 0.

5. Έχοντας επαληθεύσει ότι ο δίσκος έχει διαγραφεί, απενεργοποιούμε τη ρύθμιση από το USB Write Blocker και αποσυνδέουμε το δίσκο και την συσκευή.

6. Συνδέουμε το δίσκο κατευθείαν στη μητρική πλακέτα του υπολογιστή μέσω διεπαφής SATA. Με αυτό τον τρόπο θα πετύχουμε καλύτερες ταχύτητες εγγραφής και διαγραφής σε σχέση με την εξωτερική σύνδεση με USB.

7. Από το Disk Management των Windows αρχικοποιούμε το δίσκο επιλέγοντας στο Partition Style το MBR και δημιουργούμε ένα νέο ενιαίο partition NTFS. Με αυτό το τρόπο ο δίσκος αναγνωρίζεται από το λειτουργικό και εμφανίζεται στα Windows.

8. Εξετάζουμε την κατάσταση του δίσκου με το εργαλείο CrystalDiskInfo , ώστε να διαπιστώσουμε ότι η "υγεία" του είναι καλή.

9. Αντιγράφουμε στο δίσκο τα αρχεία που έχουμε καταγράψει στο βήμα 1 και με το εργαλείο HashMyFiles συγκρίνουμε τις MD5 Hash τιμές ώστε να βεβαιωθούμε ότι έχουμε ακριβώς τα ίδια αρχεία στο δίσκο.

10. Εκτελούμε το προς εξέταση εργαλείο οριστικής διαγραφής και διαγράφουμε τα 20 συγκεκριμένα αρχεία από το δίσκο τα οποία έχουμε επιλέξει με τη μέθοδο One Pass Zero.

11. Με το AccessData FTK Imager εξάγουμε την εικόνα του δίσκου.

12. Εκτελούμε ξανά το εργαλείο οριστικής διαγραφής αλλά αυτή τη φορά επιλέγουμε τη διαγραφή ολόκληρου του δίσκου.

13. Παράλληλα εκτελούμε το εργαλείο SysGauge για να καταγράψουμε τη χρήση του επεξεργαστή και της μνήμης που κάνει χρήση το συγκεκριμένο εργαλείο.

14. Με το AccessData FTK Imager εξάγουμε δεύτερη φορά την εικόνα του διαγραμμένου δίσκου.

15. Επαναλαμβάνουμε τα βήματα 2 – 9 αλλά αυτή τη φορά στο δίσκο αντιγράφουμε τα αρχεία μεγέθους 200 GB.

16. Εκτελούμε για τρίτη φορά το εργαλείο οριστικής διαγραφής επίσης με επιλογή διαγραφής ολόκληρου του δίσκου.

17. Παράλληλα εκτελούμε το εργαλείο SysGauge για να καταγράψουμε τη χρήση του επεξεργαστή και της μνήμης που κάνει χρήση το συγκεκριμένο εργαλείο.

18. Με το AccessData FTK Imager εξάγουμε τρίτη φορά την εικόνα του διαγραμμένου δίσκου.

19. Εισάγουμε τις τρεις εικόνες που δημιουργήσαμε στο Autopsy και σε άλλα εργαλεία δικανικής ανάλυσης ώστε να βρούμε μοτίβα από μηδενικά , εναπομείναντα δεδομένα , αρχεία ή άλλα ασυνήθιστα ευρήματα.

20. Από τα ανακτηθέντα αρχεία δημιουργούμε τις hash MD5 τιμές τους και τις συγκρίνουμε με τα αρχικά αρχεία που τοποθετήσαμε στο δίσκο.

21. Επαναλαμβάνουμε τη διαδικασία και με τα υπόλοιπα εργαλεία οριστικής διαγραφής.

Για σκοπούς οργάνωσης, καταγραφής και ταξινόμησης των πειραματικών δοκιμών, ορίσθηκε η πιο κάτω κωδικοποίηση, η οποία χρησιμοποιείται ως αναφορά για κάθε αντίστοιχο σενάριο.

| A/A | FTK IMAGER CASE NUMBER | FTK IMAGE NAME | SCENARIO | AUTOPSY CASE NAME |
|---|---|---|---|---|
| **1** | 001-T1-20FILES | Image001 | AOMEI Partition Assistant - 20 FILES ERASE IMAGE | Autopsy T1-20FILES |
| **2** | 002-T1-10GB | Image002 | AOMEI Partition Assistant - 10GB DATA HARD DISK ERASE IMAGE | Autopsy T1-10GB |
| **3** | 003-T1-200GB | Image 003 | AOMEI Partition Assistant - 200GB DATA HARD DISK ERASE IMAGE | Autopsy T1-200GB |
| **4** | 004-T2-20FILES | Image004 | O&O SafeErase - 20 FILES ERASE IMAGE | Autopsy T2-20FILES |

| A/A | FTK IMAGER CASE NUMBER | FTK IMAGE NAME | SCENARIO | AUTOPSY CASE NAME |
|---|---|---|---|---|
| **5** | 005-T2-10GB | Image005 | O&O SafeErase - 10GB DATA HARD DISK ERASE IMAGE | Autopsy T2-10GB |
| **6** | 006-T2-200GB | Image006 | O&O SafeErase - 200GB DATA HARD DISK ERASE IMAGE | Autopsy T2-200GB |
| **7** | 007-T3-20FILES | Image007 | Easy File Shredder - 20 FILES ERASE IMAGE | Autopsy T3-20FILES |
| **8** | 008-T3-10GB | Image008 | Easy File Shredder - 10GB DATA HARD DISK ERASE IMAGE | Autopsy T3-10GB |
| **9** | 009-T3-200GB | Image009 | Easy File Shredder - 200GB DATA HARD DISK ERASE IMAGE | Autopsy T3-200GB |
| **10** | 010-T4-20FILES | Image010 | TS DataWiper - 20 FILES ERASE IMAGE | Autopsy T4-20FILES |
| **11** | 011-T4-10GB | Image011 | TS DataWiper - 10GB DATA HARD DISK ERASE IMAGE | Autopsy T4-10GB |
| **12** | 012-T4-200GB | Image012 | TS DataWiper - 200GB DATA HARD DISK ERASE IMAGE | Autopsy T4-200GB |
| **13** | 013-T5-20FILES | Image013 | Abylon Shredder - 20 FILES ERASE IMAGE | Autopsy T5-20FILES |
| **14** | 014-T5-10GB | Image014 | Abylon Shredder - 10GB DATA HARD DISK ERASE IMAGE | Autopsy T5-10GB |
| **15** | 015-T5-200GB | Image015 | Abylon Shredder - 200GB DATA HARD DISK ERASE IMAGE | Autopsy T5-200GB |

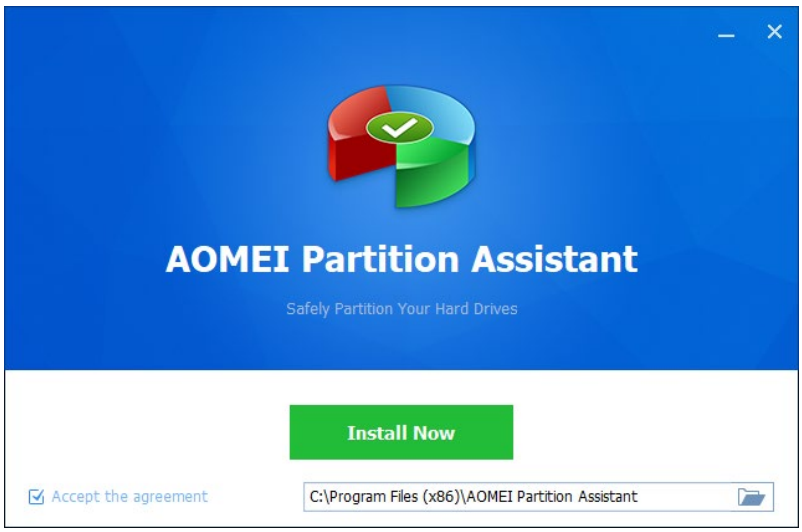
**Πίνακας 5-1: Πίνακας κωδικοποίησης σεναρίων**

## 5.2 Εφαρμογή/ Επανάληψη Διαδικασίας

Η πειραματική διαδικασία που περιεγράφηκε πιο πάνω, εφαρμόζεται ομοίως σε όλα τα επιλεγμένα εργαλεία, ώστε να δημιουργηθεί μια κοινή βάση σύγκρισης.

### 5.2.1 Εργαλείο 1 - AOMEI Partition Assistant

Εγκατάσταση εργαλείου

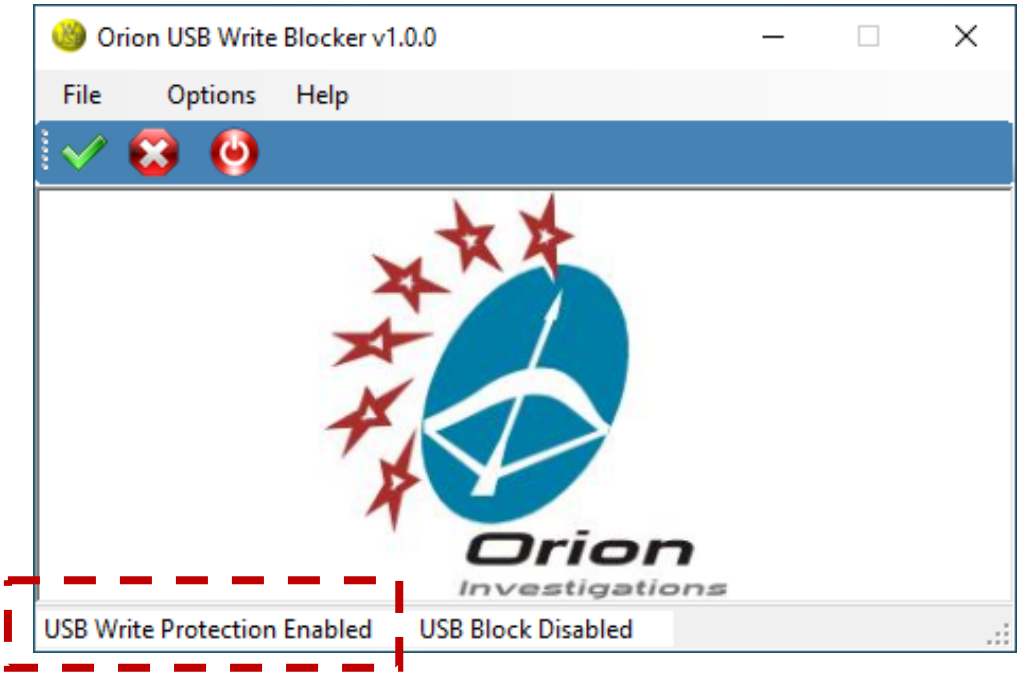



**Εικόνα 5-1: Εργαλείο 1 - Εγκατάσταση AOMEI Partition Assistant**

Αρχικοποίηση δίσκου

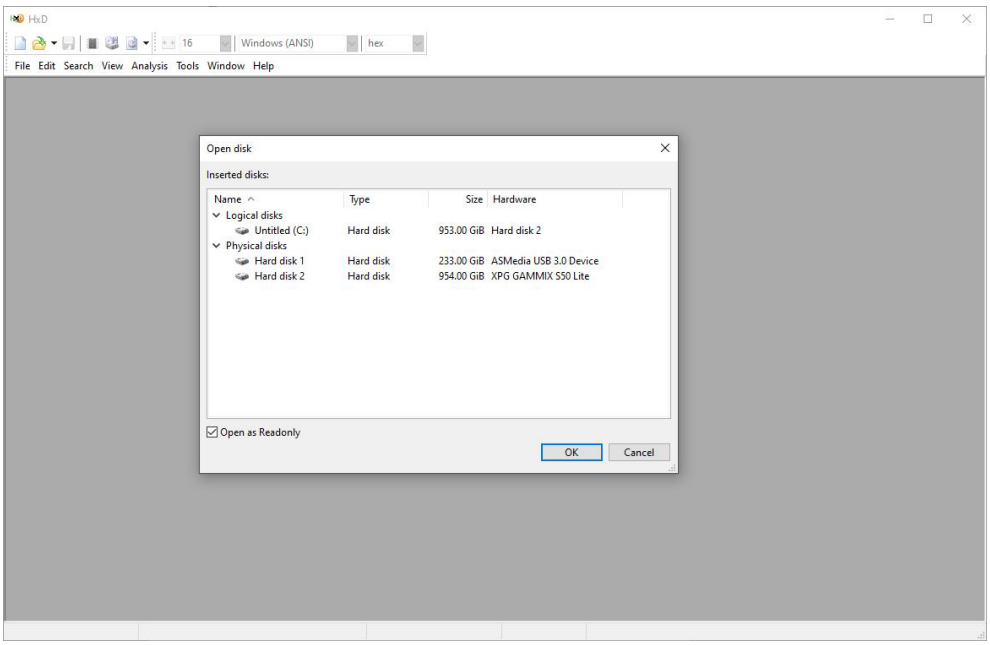
**Εικόνα 5-2: Εργαλείο 1 - Διαγραφή δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser**

Ενεργοποίηση USB Write Blocker

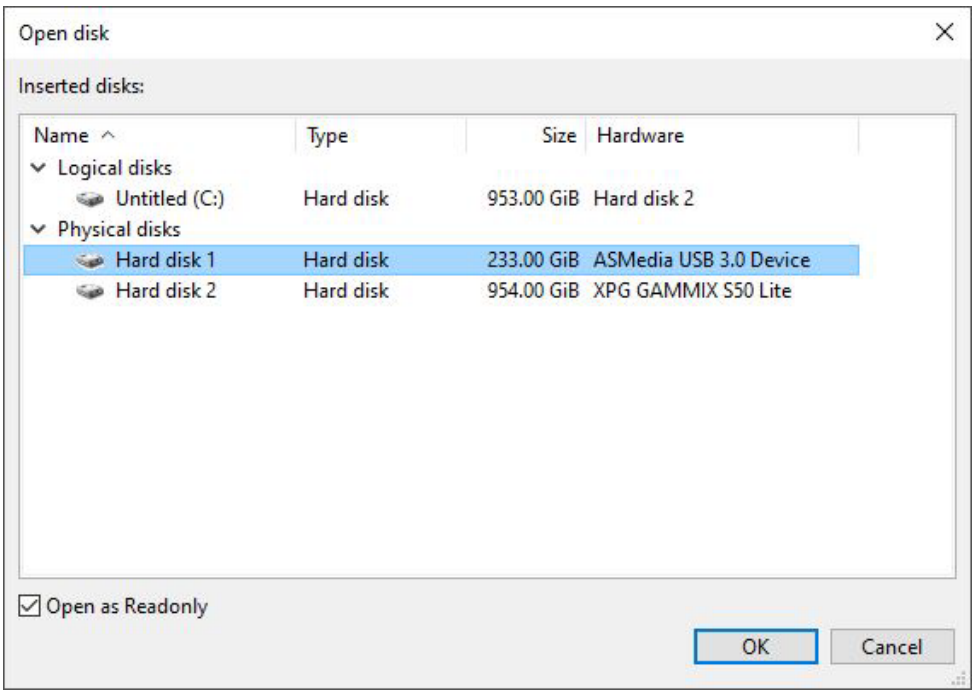



**Εικόνα 5-3: Εργαλείο 1 - Ενεργοποίηση USB Write Blocker για αποτροπή εγγραφής δεδομένων στο δίσκο**

Σύνδεση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser με υπολογιστή μέσω USB 3.0 και επιβεβαίωση με το εργαλείο HxD - Hex Editor και Disk Editor ότι όλα τα bit που βρίσκονται σε αυτόν είναι 0.

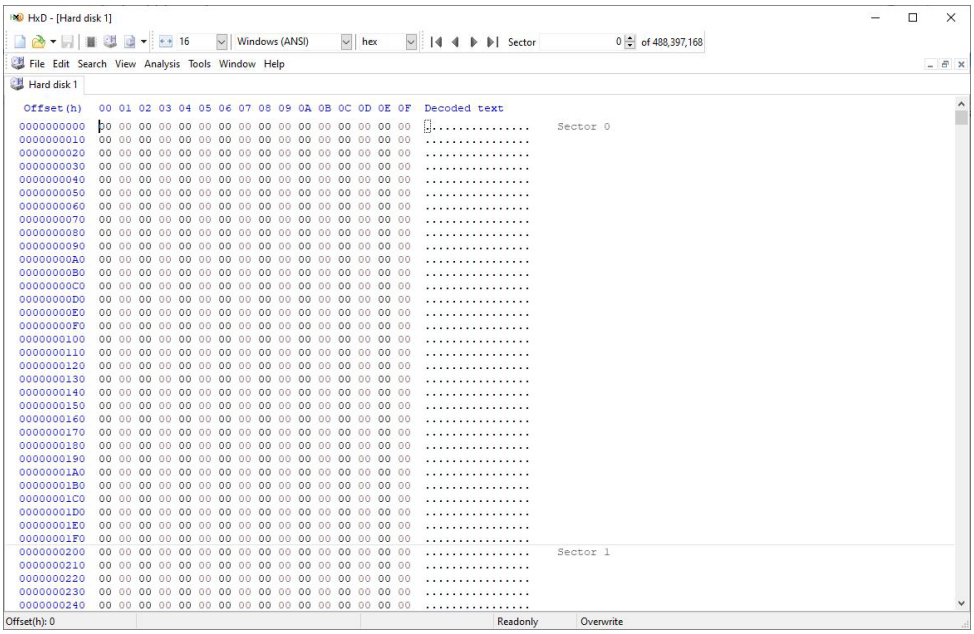



**Εικόνα 5-4: Εργαλείο 1 - HxD - Άνοιγμα δίσκου για επισκόπηση**



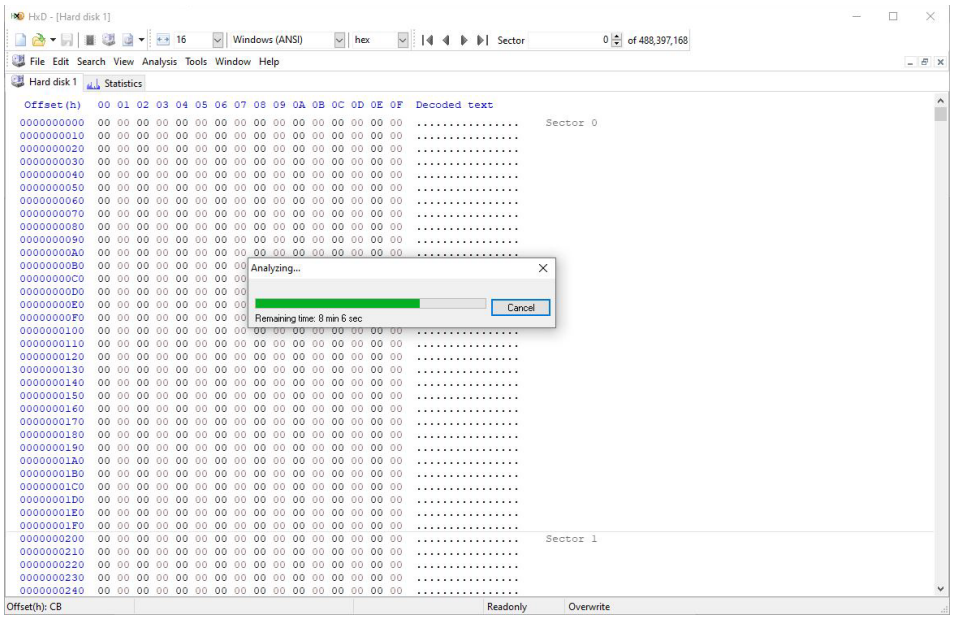

**Εικόνα 5-5: Εργαλείο 1 - HxD - Επιλογή δίσκου συνδεδεμένου σε συσκευή USB**

Στο νέο παράθυρο που εμφανίζεται, παρουσιάζονται όλοι οι δίσκοι που βρίσκονται συνδεδεμένοι με τον υπολογιστή. Ο δίσκος (Hard disk 2) αφορά το δίσκο C: στον οποίο βρίσκεται και το λειτουργικό σύστημα του υπολογιστή μεγέθους 1 TB, ενώ ο Hard disk 1 αποτελεί το δίσκο που έχουμε συνδέσει και στον οποίο θα γίνουν οι δοκιμές. Να σημειώσουμε ότι ο hard disk 1 δεν εμφανίζει Logical disk αφού στο σημείο αυτό ακόμη δεν έχει μορφοποιηθεί.



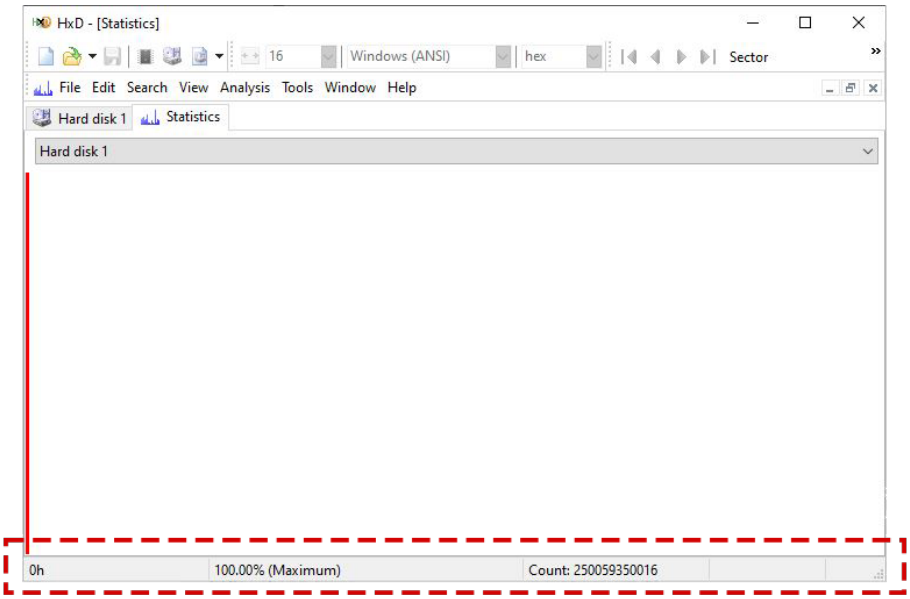

**Εικόνα 5-6: Εργαλείο 1 - Hxd - Επισκόπηση δεδομένων δίσκου**

Με μια πρώτη ματιά, από την επισκόπηση του δίσκου φαίνεται ότι η συσκευή διαγραφής λειτούργησε όπως θα έπρεπε. Τα περιεχόμενα όλων των τμημάτων του δίσκου έχουν εγγραφεί με μηδενικά. Ωστόσο λόγω του μεγάλου αριθμού τομέων (sectors) στο δίσκο, οπτικά μπορεί να μας διέφυγε κάποια άλλη τιμή εκτός από το μηδέν. Για να βεβαιωθούμε ότι πράγματι στο δίσκο δεν υπάρχουν άλλες εγγραφές προχωρήσαμε σε ανάλυση των περιεχομένων του δίσκου χρησιμοποιώντας τη δυνατότητα statistics analysis που προσφέρει το εργαλείο.




**Εικόνα 5-7: Εργαλείο 1 - HxD - Ανάλυση δίσκου**

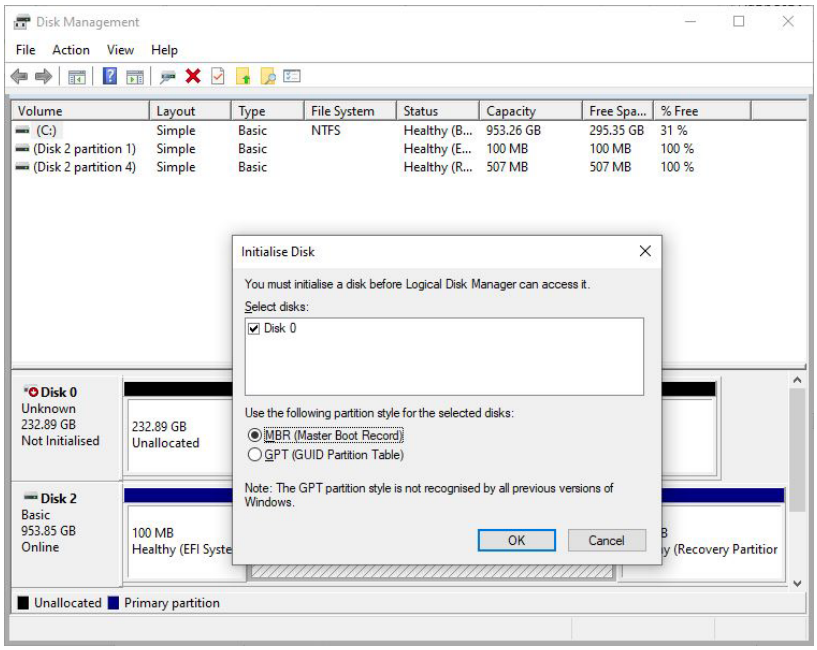
Η δυνατότητα αυτή είναι ιδιαίτερα χρήσιμη αφού καταμετρά και καταγράφει όλες τις διαφορετικές τιμές που υπάρχουν στο δίσκο, όπως επίσης και τη συχνότητα εμφάνισης τους.




**Εικόνα 5-8: Εργαλείο 1 - HxD - Αποτελέσματα στατιστικής ανάλυσης**

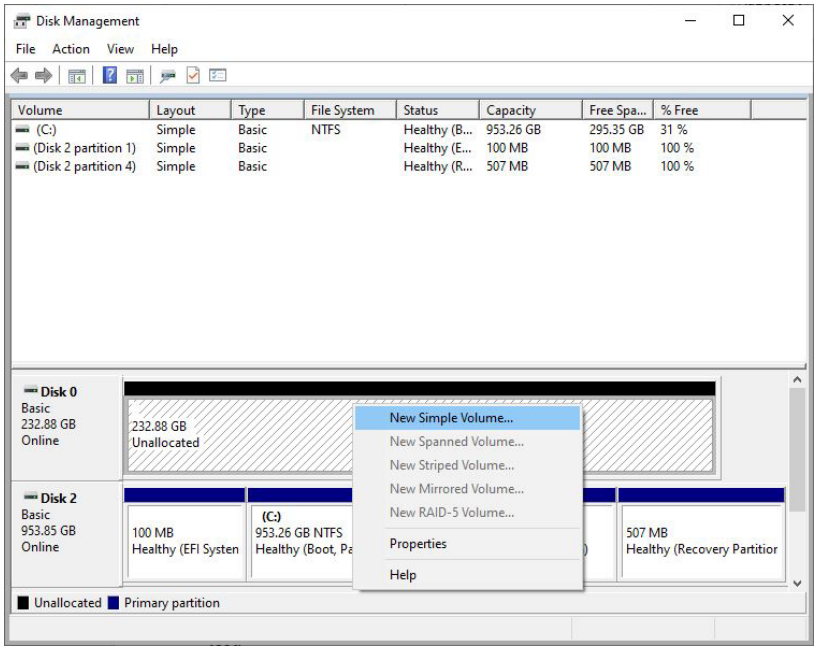
Σύμφωνα με τα αποτελέσματα της ανάλυσης του δίσκου το 100% των περιεχομένων του έχει την τιμή 0. Σε αυτό το σημείο μπορούμε με βεβαιότητα να πούμε ότι έχουμε ένα κενό δίσκο τον οποίο θα μορφοποιήσουμε και στον οποίο θα αντιγράψουμε τα αρχεία για διαγραφή.

Αρχικοποίηση και μορφοποίηση σκληρού δίσκου

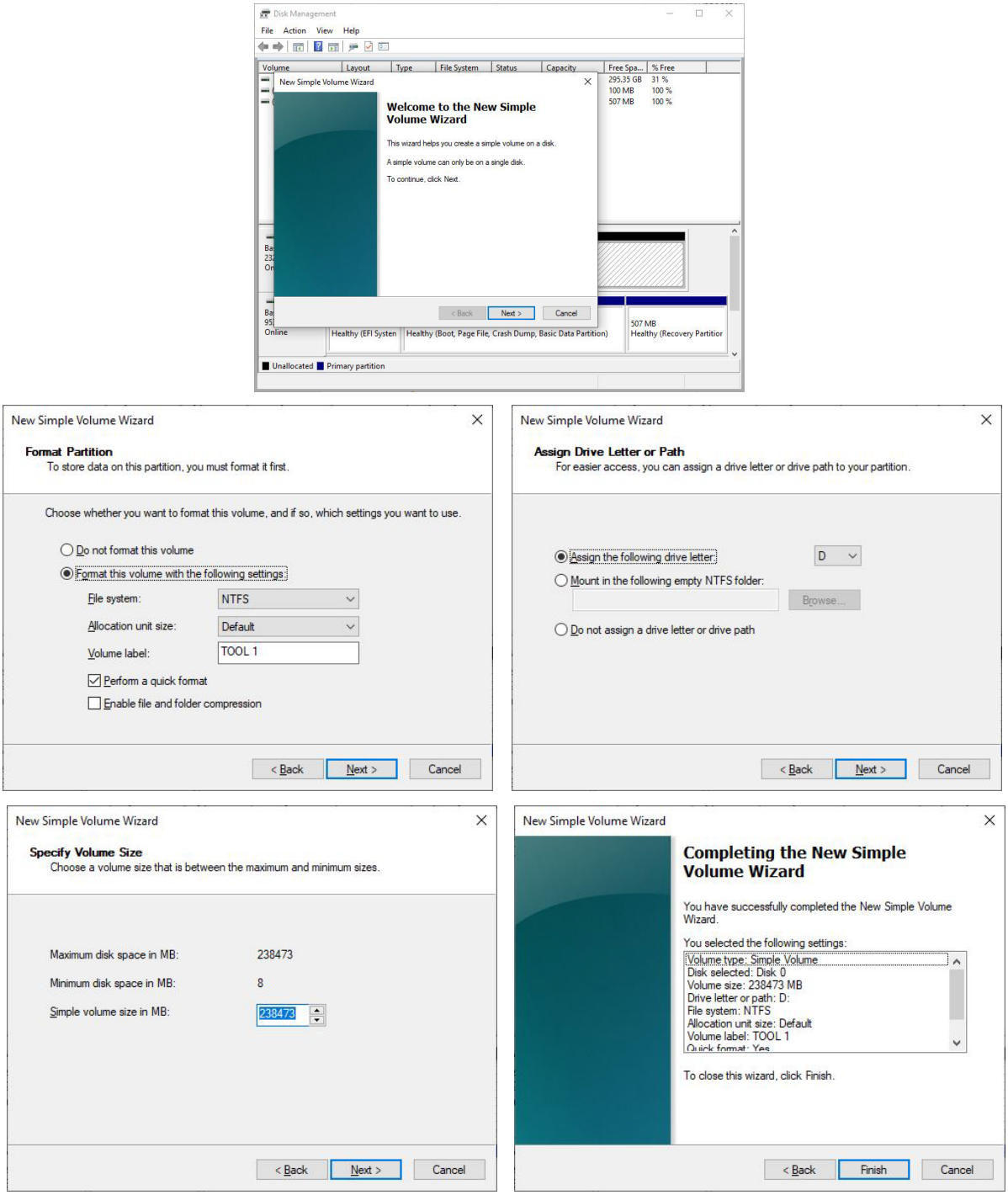



**Εικόνα 5-9: Εργαλείο 1 - Windows Disk Management**

Μέσα από το Disk Management των windows προχωρούμε σε αρχικοποίηση και μορφοποίηση του δίσκου. Γίνεται επιλογή του partition style σε MBR ( Master Boot Record).

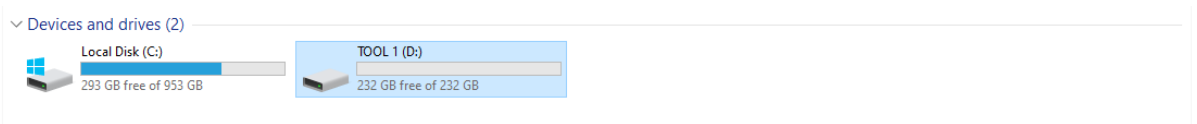



**Εικόνα 5-10: Εργαλείο 1 - Διαδικασία μορφοποίησης δίσκου**

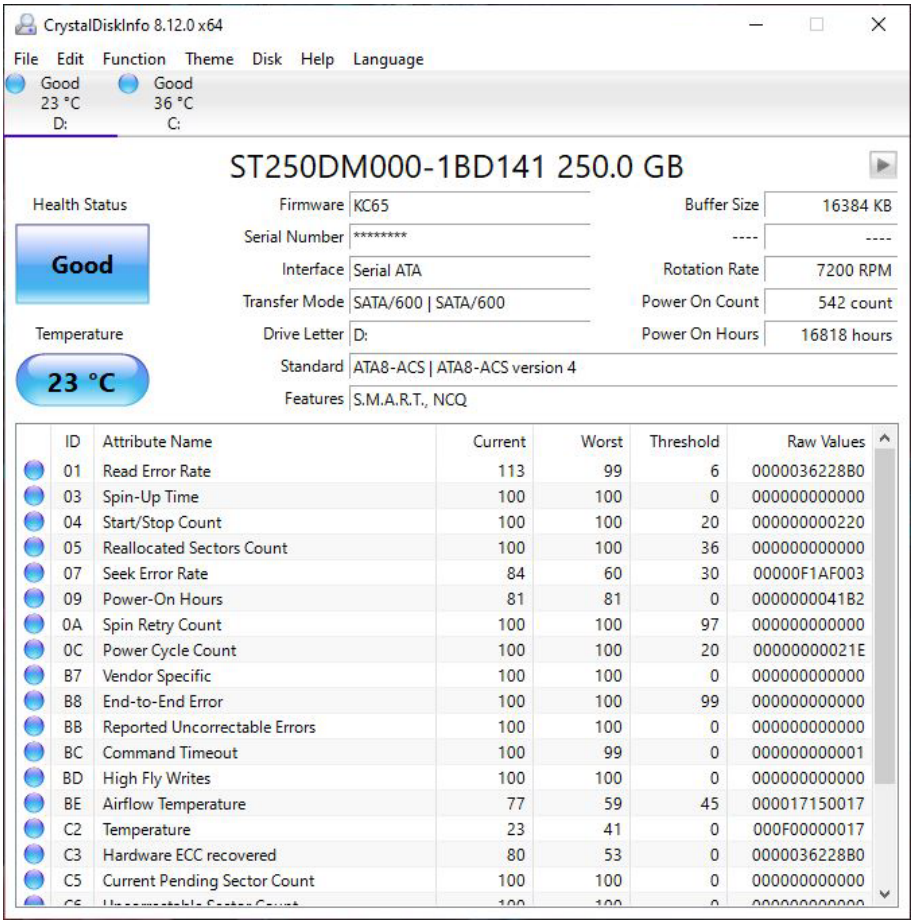



**Εικόνα 5-11: Εργαλείο 1 - Διαδικασία μορφοποίησης δίσκου για αξιολόγηση**

Τα πιο πάνω βήματα αποτελούν τη διαδικασία για τη μορφοποίηση του σκληρού δίσκου ώστε να μπορεί να χρησιμοποιηθεί από το λειτουργικό σύστημα. Μετά το πέρας της διαδικασίας ο δίσκος με την ονομασία TOOL 1 είναι ορατός και μπορεί να χρησιμοποιηθεί κανονικά από τα windows.

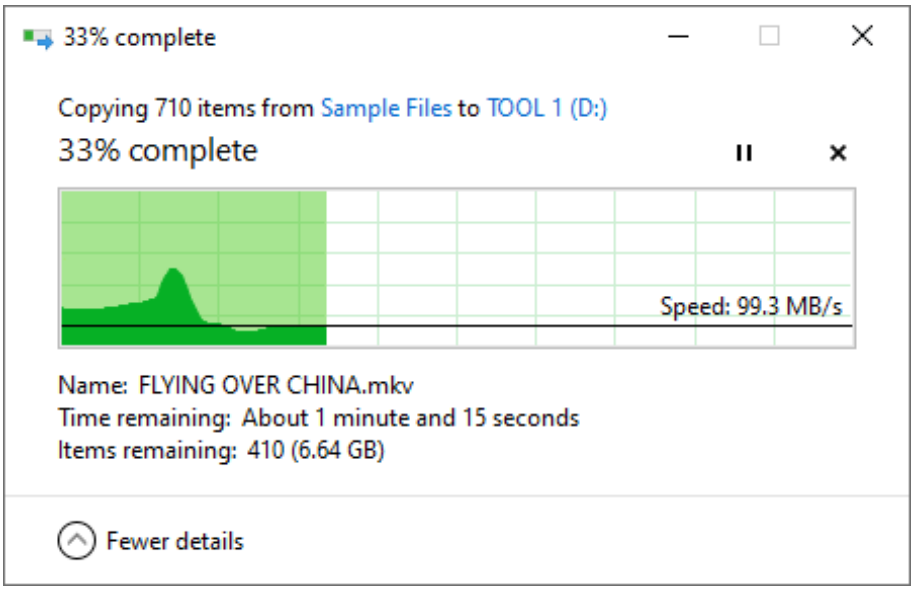


Εξέταση κατάστασης υγείας δίσκου με το CrystalDiskInfo



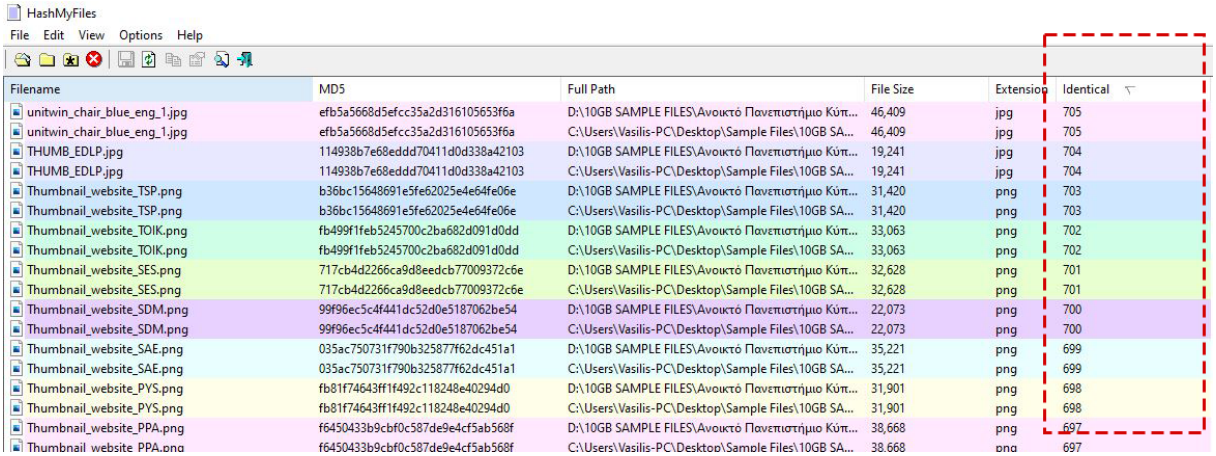

**Εικόνα 5-12: Εργαλείο 1 - CrystalDiskInfo - Αναφορά κατάστασης δίσκου**

Σύμφωνα με την αναφορά του εργαλείου, ο δίσκος βρίσκεται σε καλή κατάσταση έτσι μπορούμε να αντιγράψουμε σε αυτόν τα αρχικά δεδομένα των 10 GB (705 αρχεία) .




**Εικόνα 5-13: Εργαλείο 1 - Αντιγραφή 10 GB δεδομένων στο δίσκο**

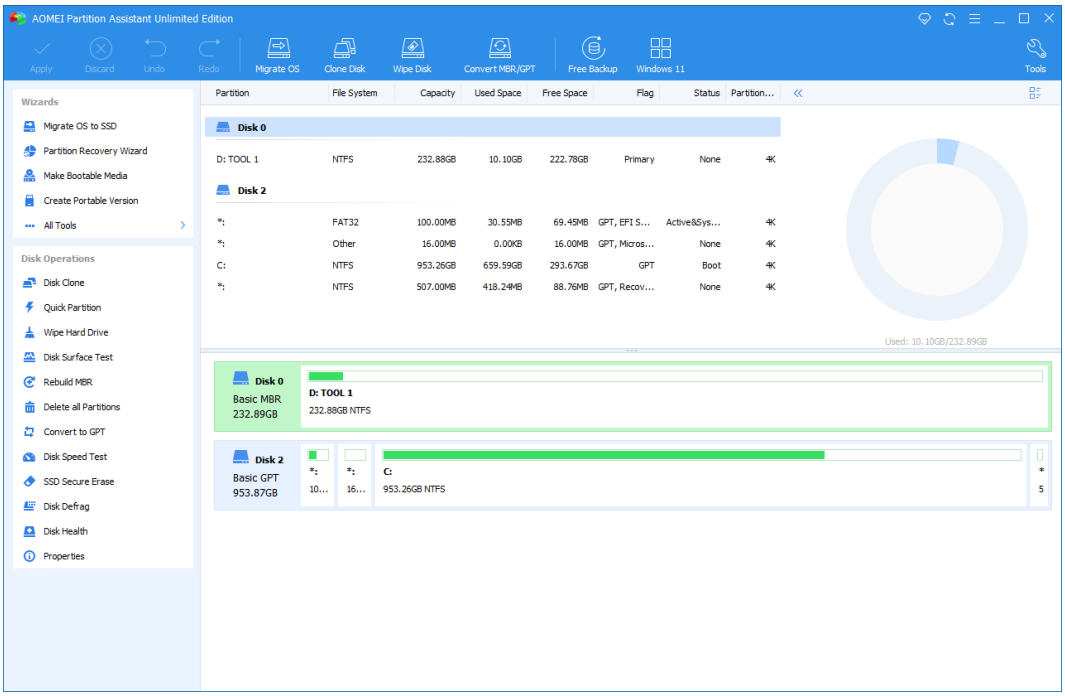
Με το εργαλείο HashMyFiles συγκρίνουμε τις MD5 Hash τιμές ώστε να βεβαιωθούμε ότι η αντιγραφή έχει ολοκληρωθεί πλήρως και έχουμε ακριβώς τα ίδια αρχεία στο δίσκο.




**Εικόνα 5-14: Εργαλείο 1 - HashMyFiles - Σύγκριση αρχείων**

Το εργαλείο HashMyFiles αφού του εισάγουμε τα δύο directories με τα αρχεία, δημιουργεί τις κατακερματισμένες τιμές τους σε MD5 και στη συνέχεια τις συγκρίνει για να εντοπίσει όμοια αρχεία. Στην τελευταία στήλη παρουσιάζονται τα αρχεία που έχουν τις ίδιες hash τιμές. Παρατηρούμε ότι και τα 705 αρχεία που αντιγράψαμε στο δίσκο έχουν ένα αντίγραφο, αυτό του αρχικού φακέλου που βρίσκονταν τα αρχεία δείγματα. Με αυτό το τρόπο επιβεβαιώσαμε ότι στο δίσκο αντιγράφηκαν όλα τα αρχεία και δεν έγινε καμία παράληψη.

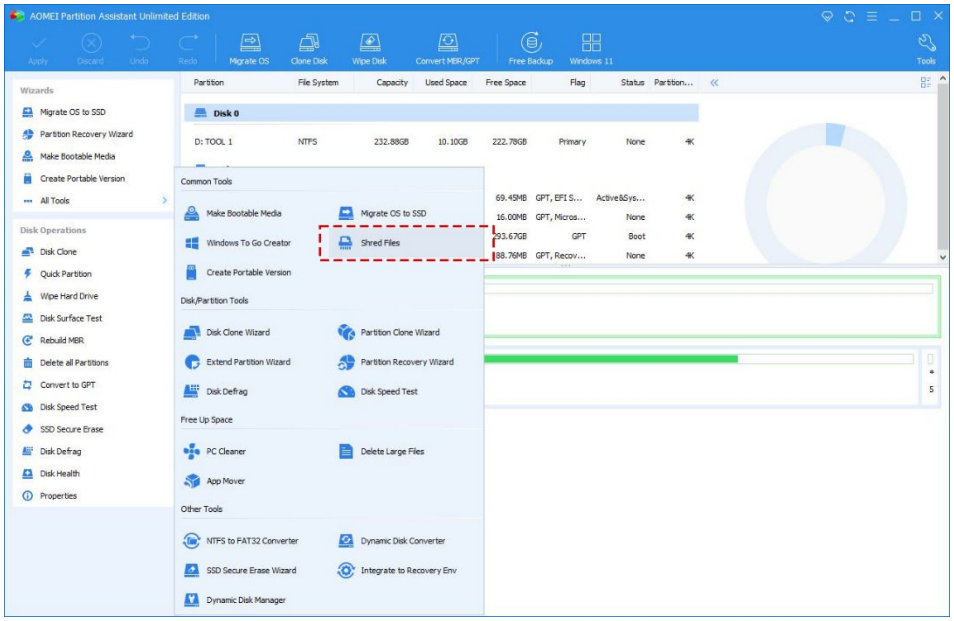
Εκτελούμε το 1ο εργαλείο οριστικής διαγραφής AOMEI Partition Assistant.




**Εικόνα 5-15: Εργαλείο 1 - AOMEI Partition Assistant - Εμφάνιση δίσκων**

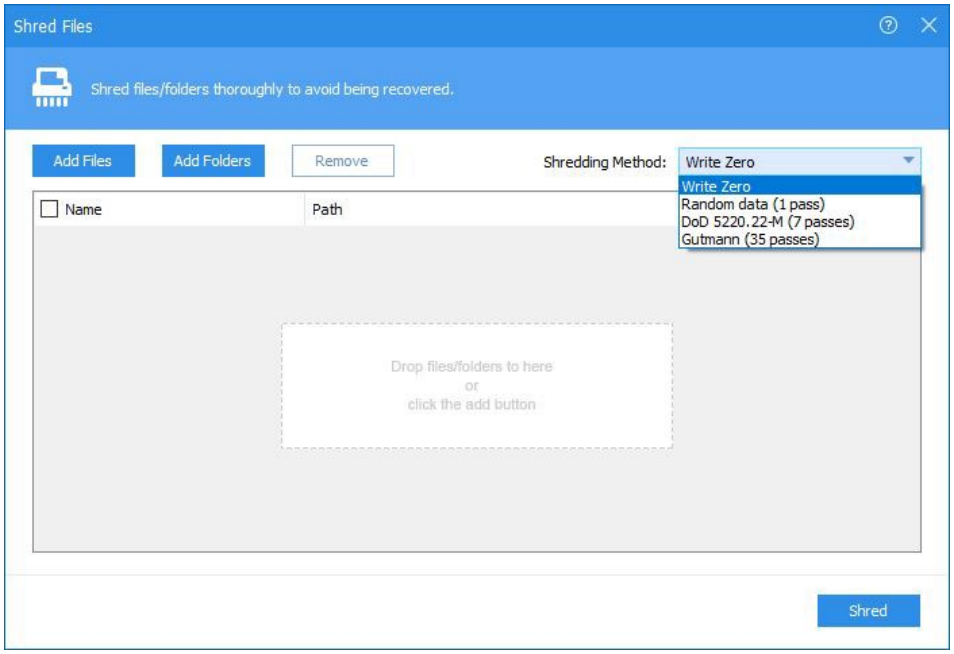
- **<u>Εκτέλεση πρώτου σεναρίου</u>** – Διαγραφή 20 συγκεκριμένων αρχείων από το δίσκο

Από τα εργαλεία επιλέγουμε την διαγραφή αρχείων (Shred Files)




**Εικόνα 5-16: Εργαλείο 1 - AOMEI Partition Assistant - Επιλογή διαγραφής αρχείων**

Στο νέο παράθυρο που εμφανίζεται επιλέγουμε τα 20 αρχεία που θέλουμε να διαγράψουμε ενώ παράλληλα καθορίζουμε και τη μέθοδο διαγραφής σε write zero.



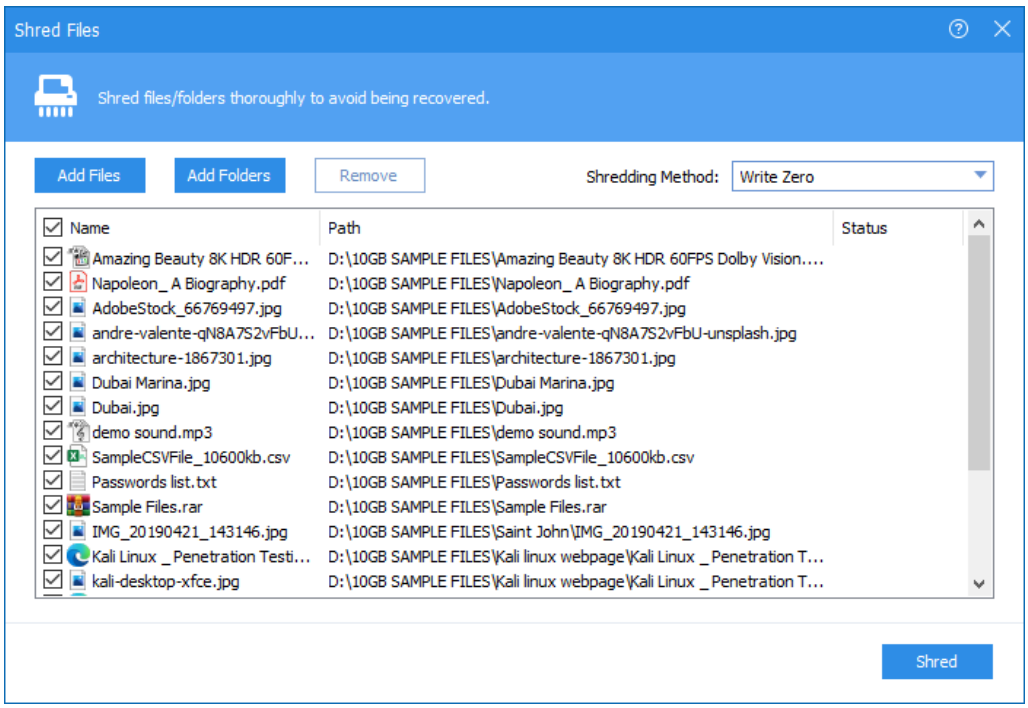

**Εικόνα 5-17: Εργαλείο 1 - AOMEI Partition Assistant - Επιλογή αρχείων και μεθόδου διαγραφής**

Τα 20 αρχεία που επιλέξαμε για διαγραφή είναι τα ακόλουθα:

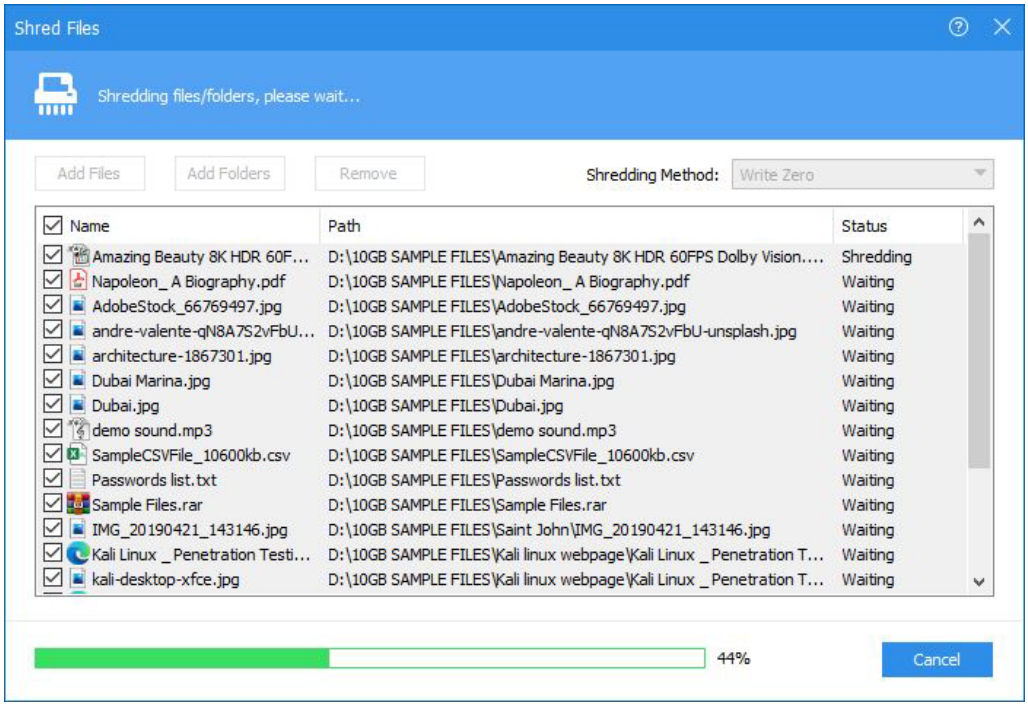
| A/A | Filename | Type |
|---|---|---|
| 1 | Amazing Beauty 8K HDR 60FPS Dolby Vision.mkv | mkv |
| 2 | Napoleon_ A Biography.pdf | pdf |
| 3 | AdobeStock_66769497.jpg | jpg |
| 4 | andre-valente-qN8A7S2vFbU-unsplash.jpg | jpg |
| 5 | architecture-1867301.jpg | jpg |
| 6 | Dubai Marina.jpg | jpg |
| 7 | Dubai.jpg | jpg |
| 8 | demo sound.mp3 | mp3 |
| 9 | SampleCSVFile_10600kb.csv | csv |
| 10 | Passwords list.txt | txt |
| 11 | Sample Files.rar | rar |
| 12 | IMG_20190421_143146.jpg | jpg |
| 13 | Kali Linux _ Penetration Testing and Ethical Hacking Linux Distribution.html | html |
| 14 | kali-desktop-xfce.jpg | jpg |
| 15 | logo-gnome.svg | svg |
| 16 | sake.jpg | jpg |
| 17 | Electric-Circuits.pdf | pdf |
| 18 | AdobeStock_94572528.jpg | jpg |
| 19 | Atlantis-hotel.jpg | jpg |
| 20 | Atlantis-The-Palm.jpg | jpg |

**Πίνακας 5-2: Ονόματα και τύπος επιλεγμένων αρχείων για διαγραφή**

Τα αρχεία που έχουν επιλεγεί είναι διαφόρων τύπων και μεγεθών. Ο αναλυτικός κατάλογος των αρχείων αυτών μαζί με το ακριβές μέγεθος τους, τον τύπο τους και την hash τιμή MD5 η οποία θα χρησιμοποιηθεί αργότερα κατά την σύγκριση τους με τα ευρήματα στο δίσκο βρίσκεται στο τέλος (Παράρτημα Α).

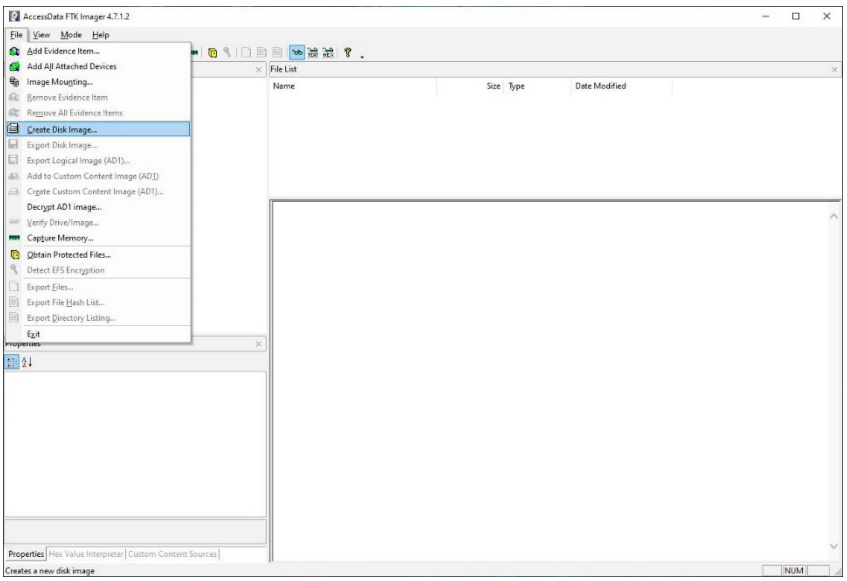



**Εικόνα 5-18: Εργαλείο 1 - AOMEI Partition Assistant - Αρχεία προς διαγραφή**

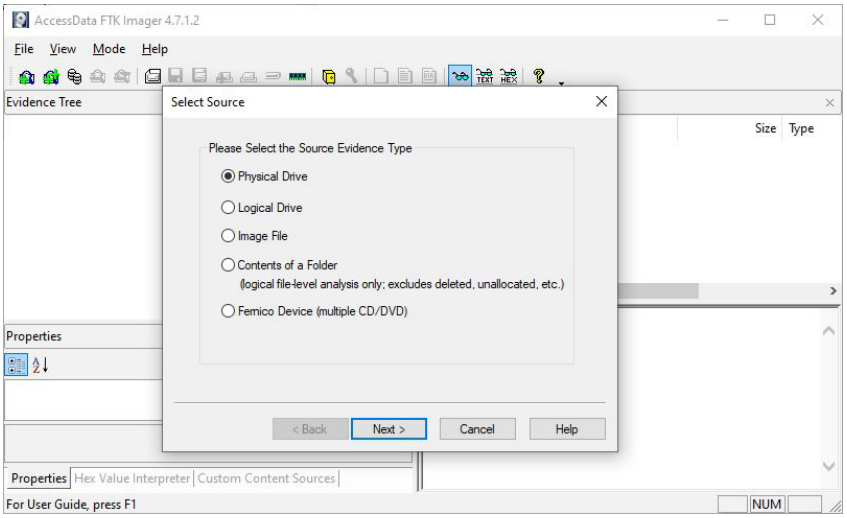



**Εικόνα 5-19: Εργαλείο 1 - AOMEI Partition Assistant - Διαδικασία Διαγραφής**

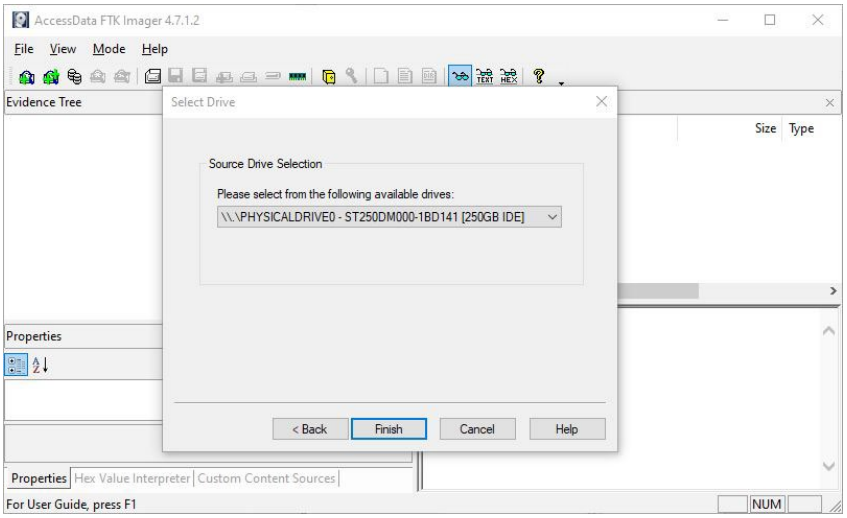
Με το πέρας της διαδικασίας διαγραφής των αρχείων προχωρούμε σε εξαγωγή της εικόνας του δίσκου με το εργαλείο AccessData FTK Imager. Με αυτό τον τρόπο θα μπορέσουμε να εισάγουμε την εικόνα στο Autopsy και να εντοπίσουμε τυχόν ίχνη από τα αρχεία.



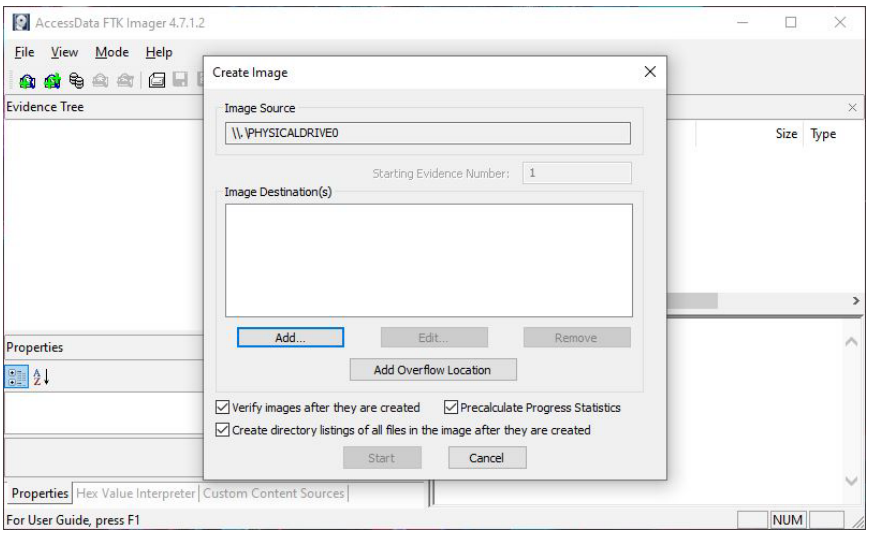

**Εικόνα 5-20: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 1**



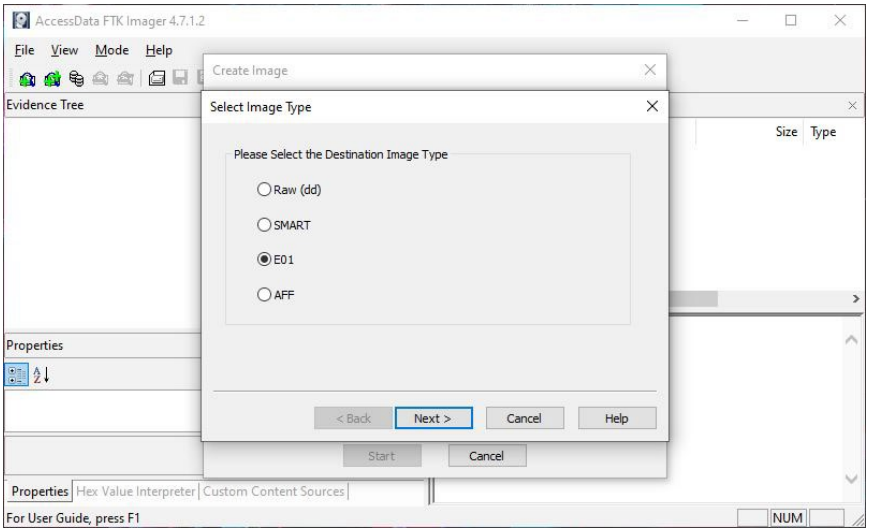

**Εικόνα 5-21: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 2**



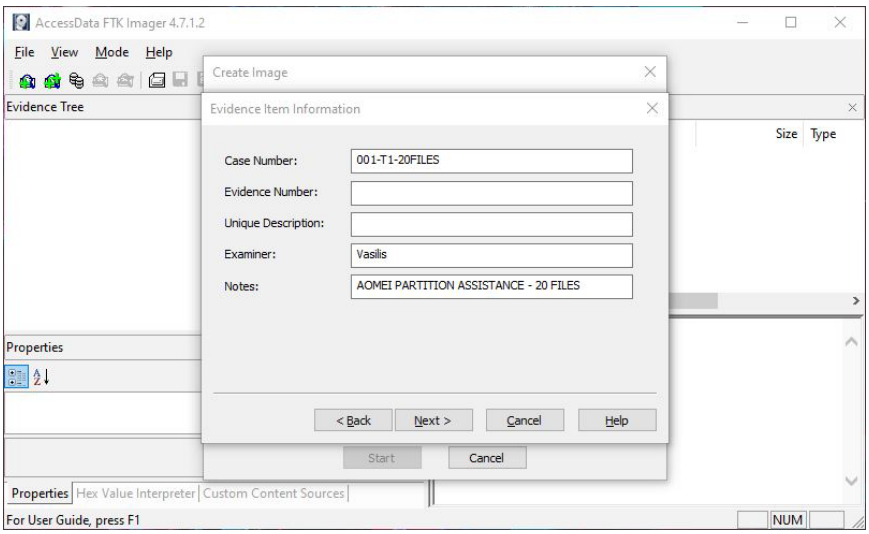

**Εικόνα 5-22: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 3**



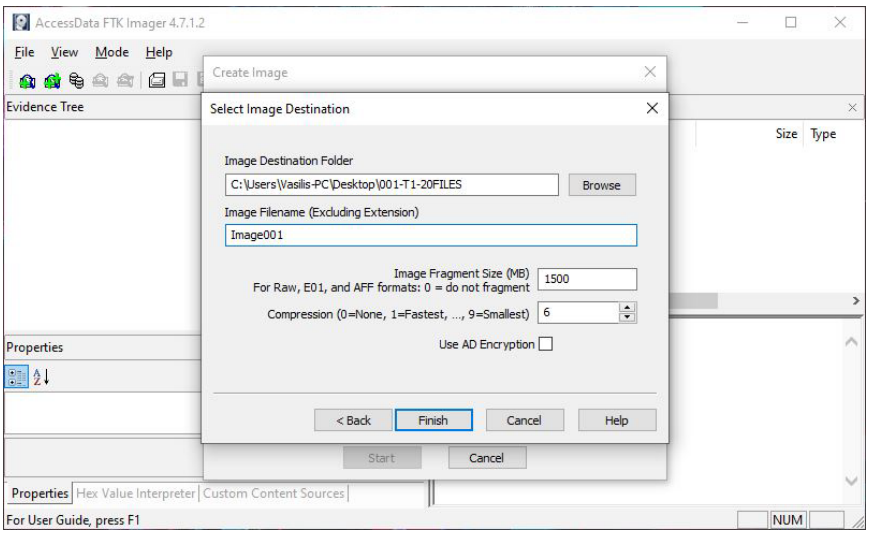

**Εικόνα 5-23: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 4**



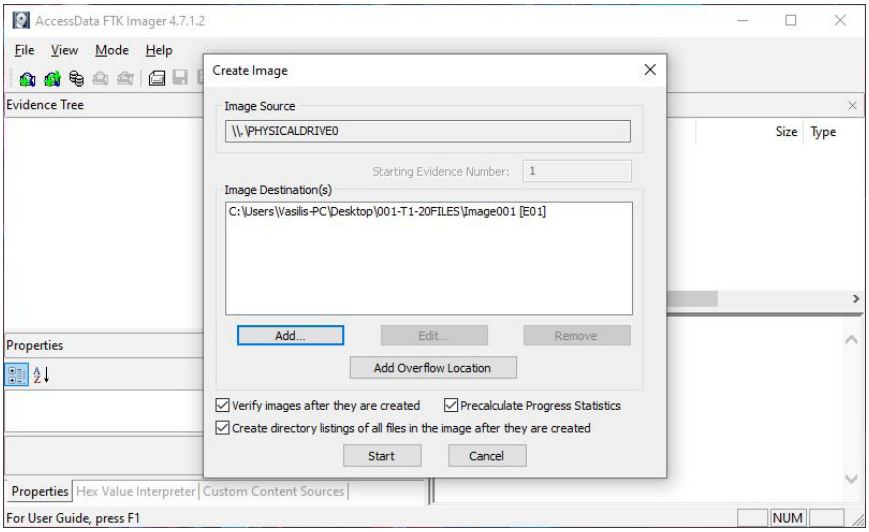

**Εικόνα 5-24: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 5**



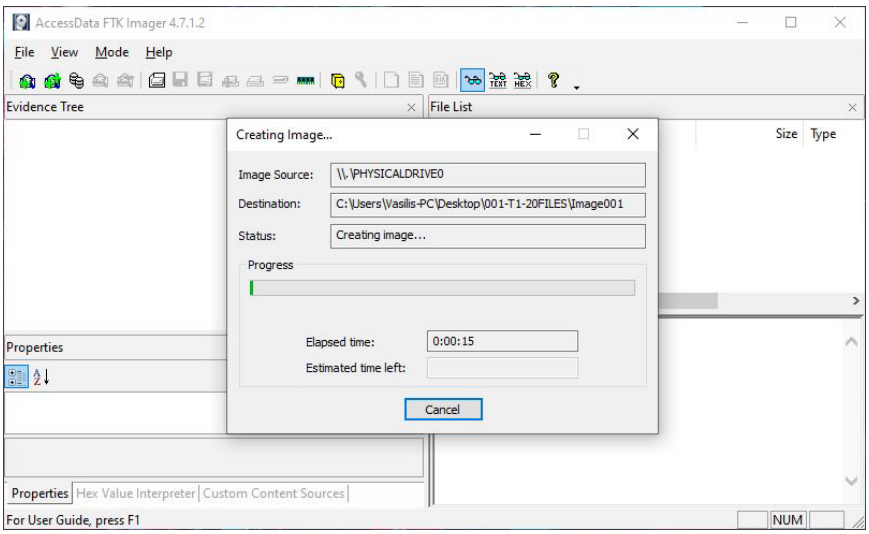

**Εικόνα 5-25: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 6**



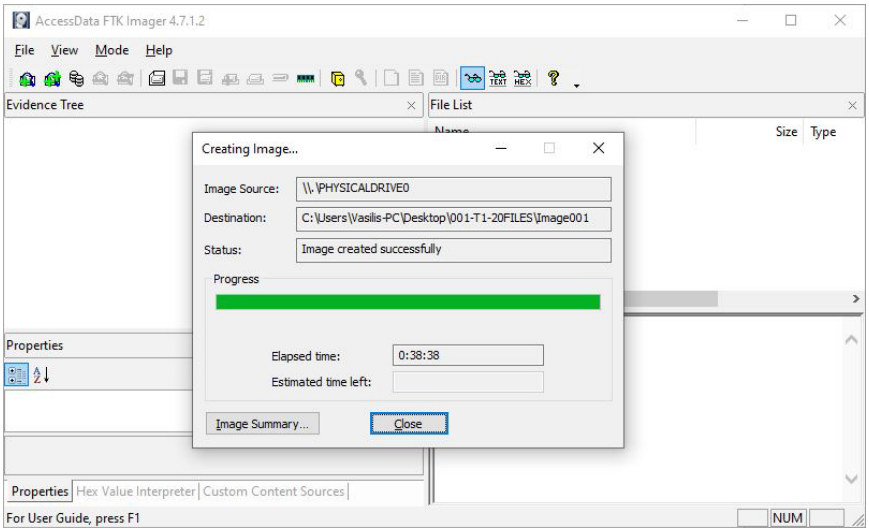

**Εικόνα 5-26: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 7**




**Εικόνα 5-27: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 8**




**Εικόνα 5-28: Εργαλείο 1 - AccessData FTK Imager - Δημιουργία εικόνας δίσκου - Βήμα 9**

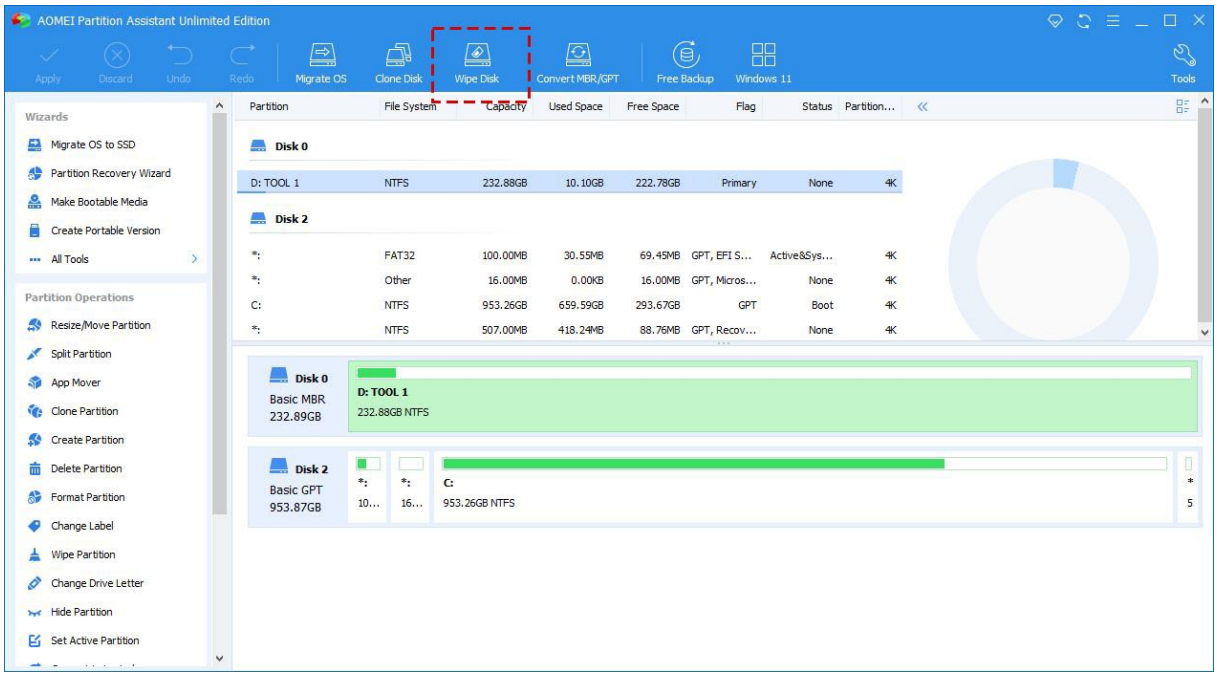



**Εικόνα 5-29: Εργαλείο 1 - AccessData FTK Imager - Ολοκλήρωση δημιουργίας εικόνας δίσκου**

Η εικόνα του δίσκου θα χρησιμοποιηθεί αργότερα για εισαγωγή της στο Autopsy και ανάλυση της για την εύρεση των 20 διαγραμμένων αρχείων.

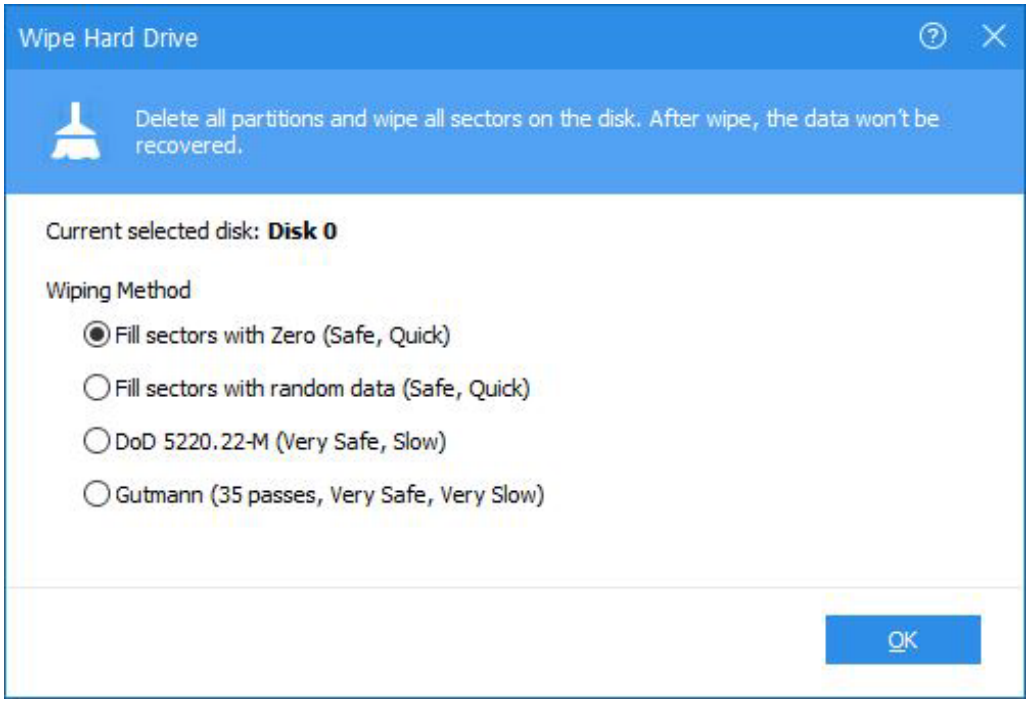
- **<u>Εκτέλεση δεύτερου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 10 GB**

Αφού διαλέξουμε τον δίσκο που θέλουμε να διαγράψουμε οριστικά, επιλέγουμε από το μενού εργαλείων την επιλογή Wipe Disk.

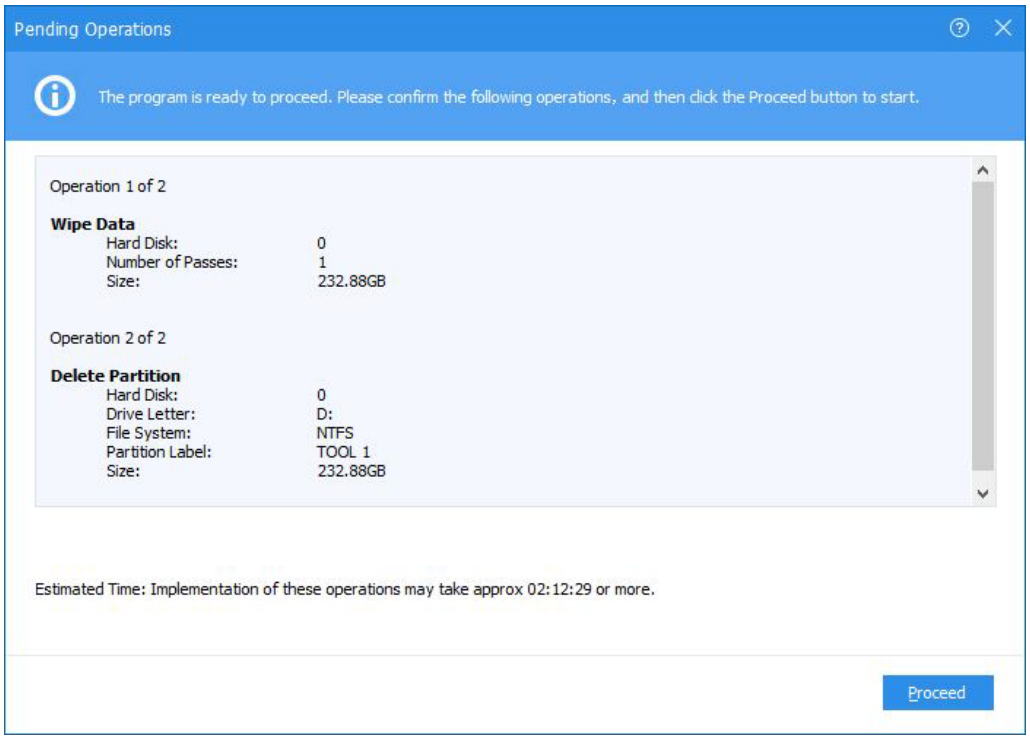



**Εικόνα 5-30: Εργαλείο 1 - AOMEI Partition Assistant - Επιλογή διαγραφής ολόκληρου του δίσκου**

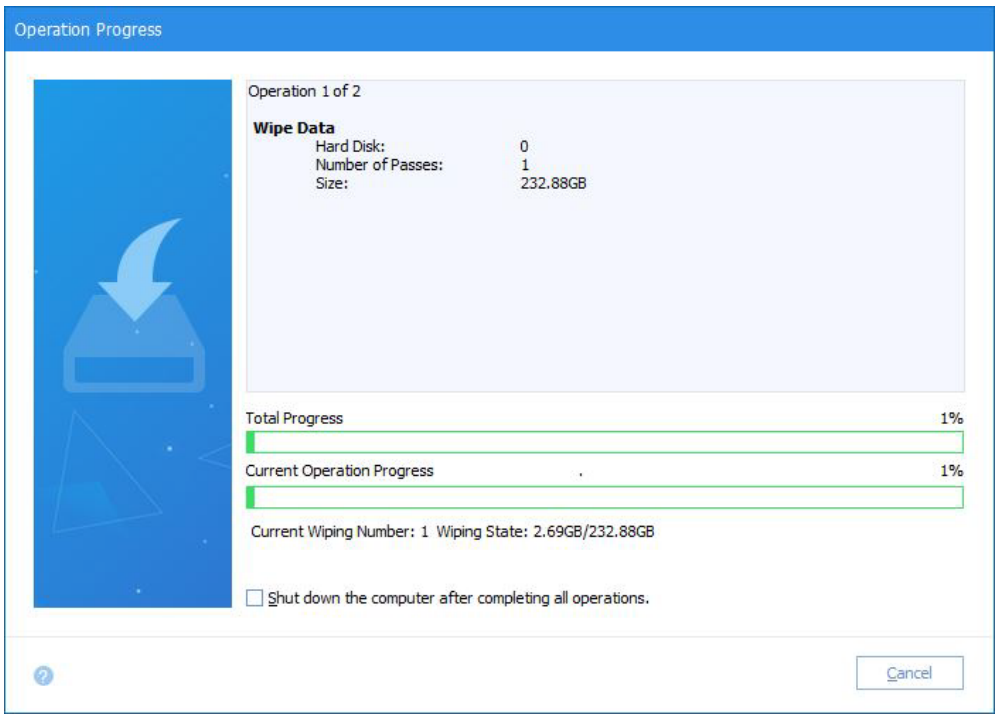
Από το παράθυρο με τις μεθόδους οριστικής διαγραφής που εμφανίζεται επιλέγουμε την πρώτη (Fill sectors with Zero(Safe, Quick)).




**Εικόνα 5-31: Εργαλείο 1 - AOMEI Partition Assistant - Επιλογές για μέθοδο διαγραφής**

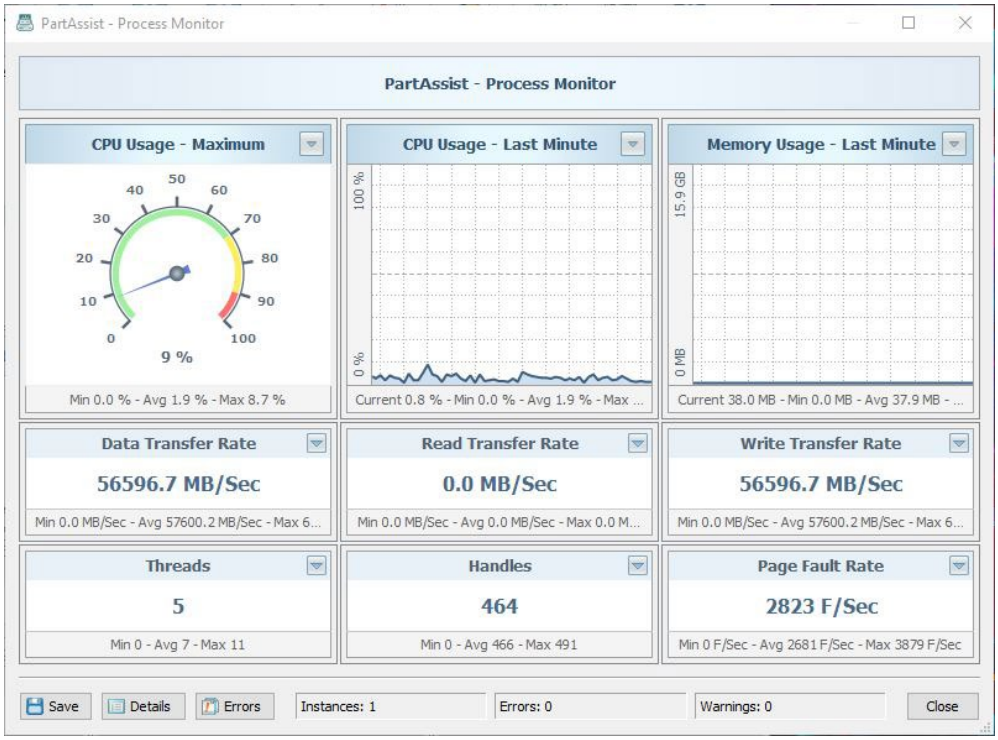



**Εικόνα 5-32: Εργαλείο 1 - AOMEI Partition Assistant - Επιβεβαίωση οριστικής διαγραφής ολόκληρου του δίσκου**

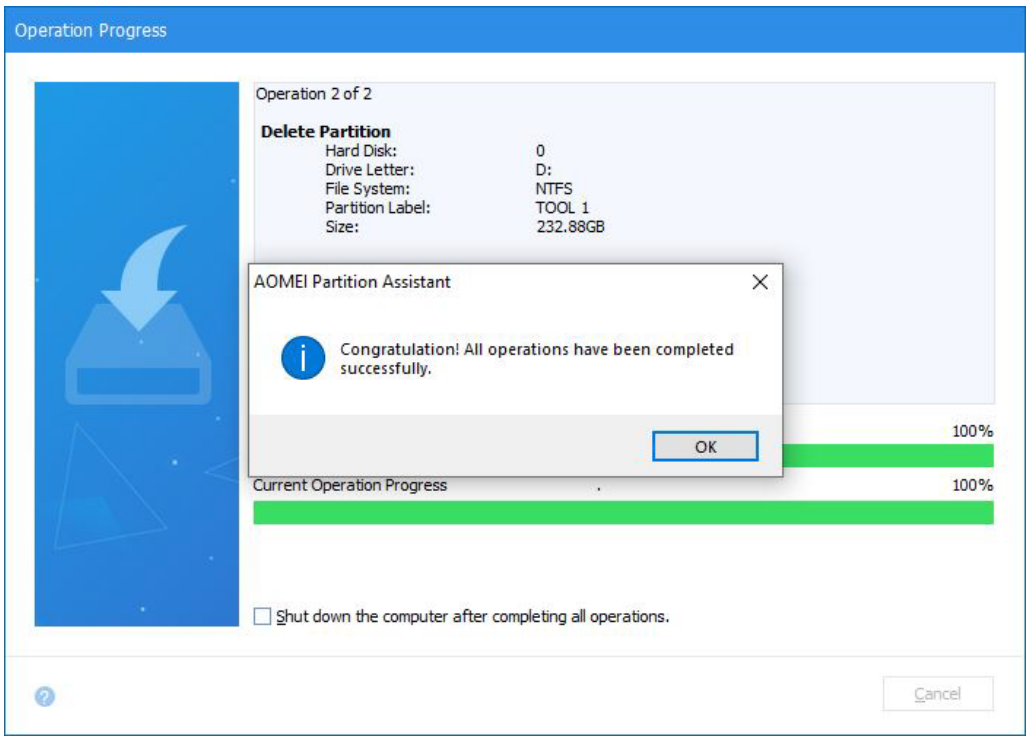



**Εικόνα 5-33: Εργαλείο 1 - AOMEI Partition Assistant - Έναρξη διαδικασίας οριστικής διαγραφής**

Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.

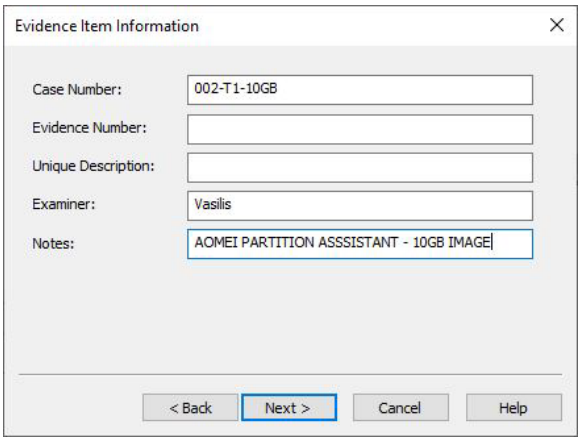


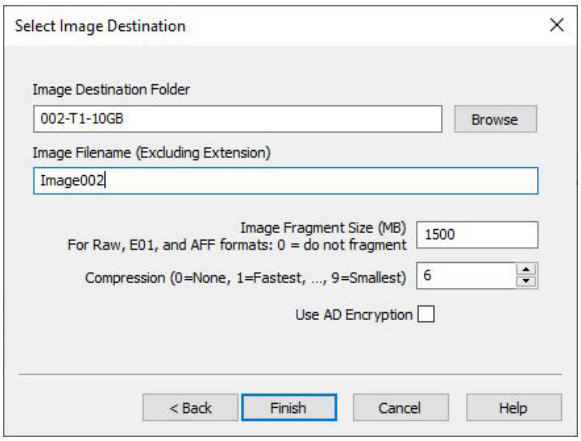

**Εικόνα 5-34: Εργαλείο 1 - SysGauge - Καταγραφή CPU, Memory που καταναλώνει το εργαλείο**

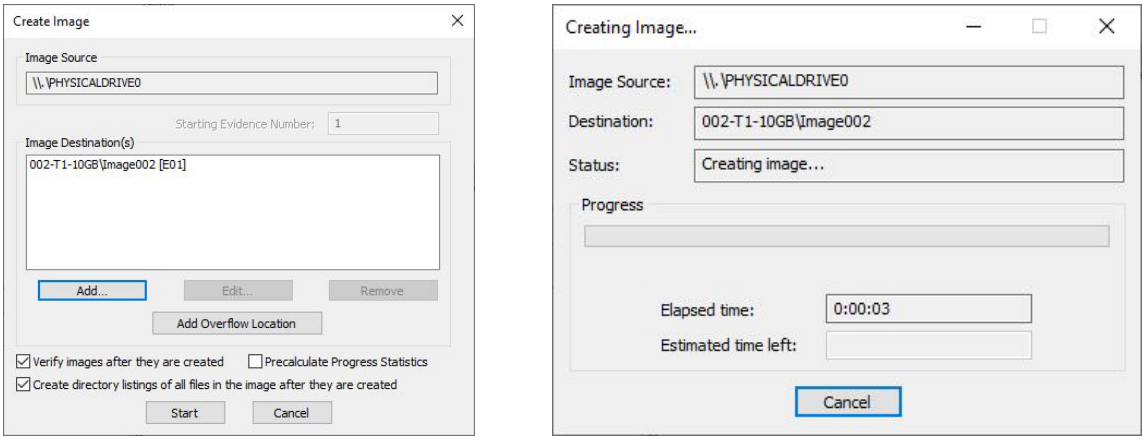



**Εικόνα 5-35: Εργαλείο 1 - AOMEI Partition Assistant - Ολοκλήρωση διαδικασίας οριστικής διαγραφής δίσκου**

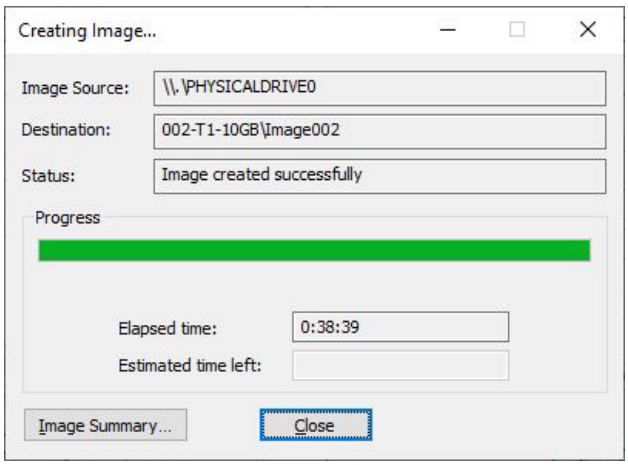
Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 10 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για δεύτερη φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που ακολουθήσαμε και στην πιο πάνω περίπτωση με μόνη διαφορά στην ονομασία της εικόνας του δίσκου ώστε να υπάρχει διαχωρισμός των δοκιμών σύμφωνα με το πίνακα κωδικοποίησης σεναρίων που ορίσαμε.






**Εικόνα 5-36: Εργαλείο 1 - AccessData FTK Imager - Διαδικασία δημιουργίας 2ης εικόνας δίσκου μετά την διαγραφή**



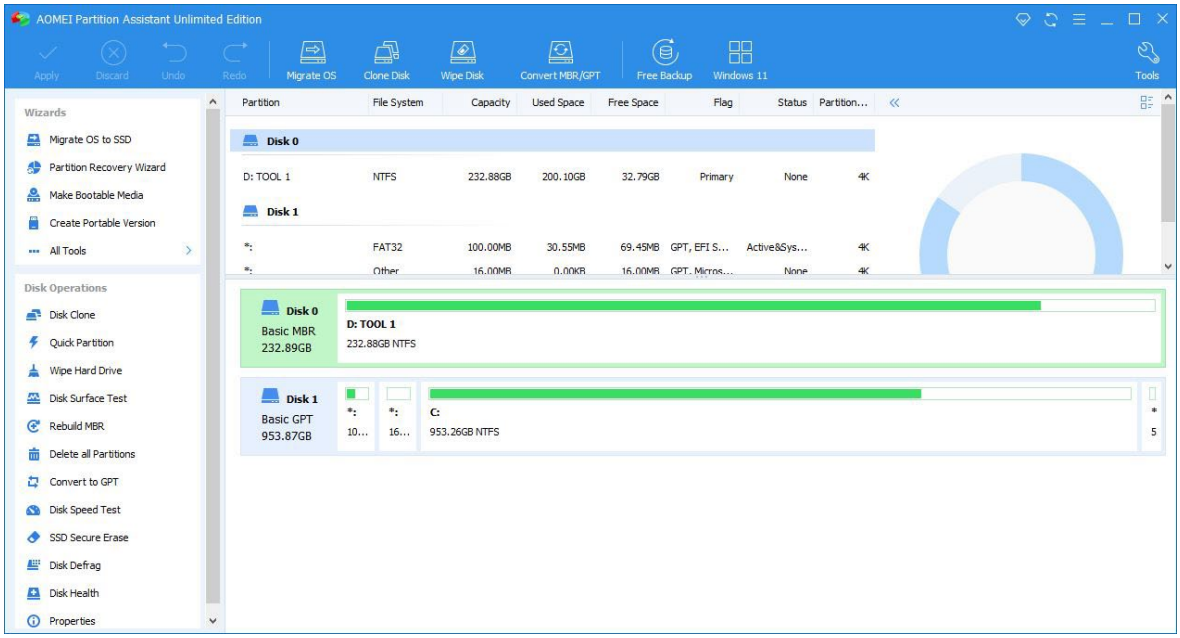

**Εικόνα 5-37: Εργαλείο 1 - AccessData FTK Imager - Ολοκλήρωση δημιουργίας 2ης εικόνας δίσκου**

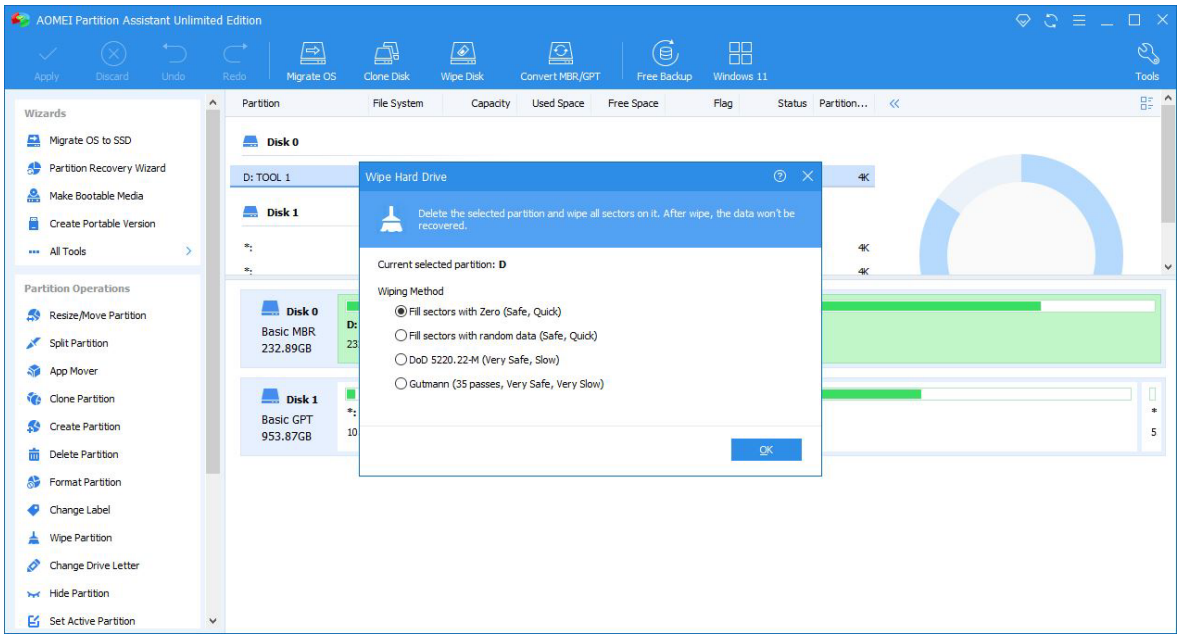
- **<u>Εκτέλεση τρίτου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 200 GB**

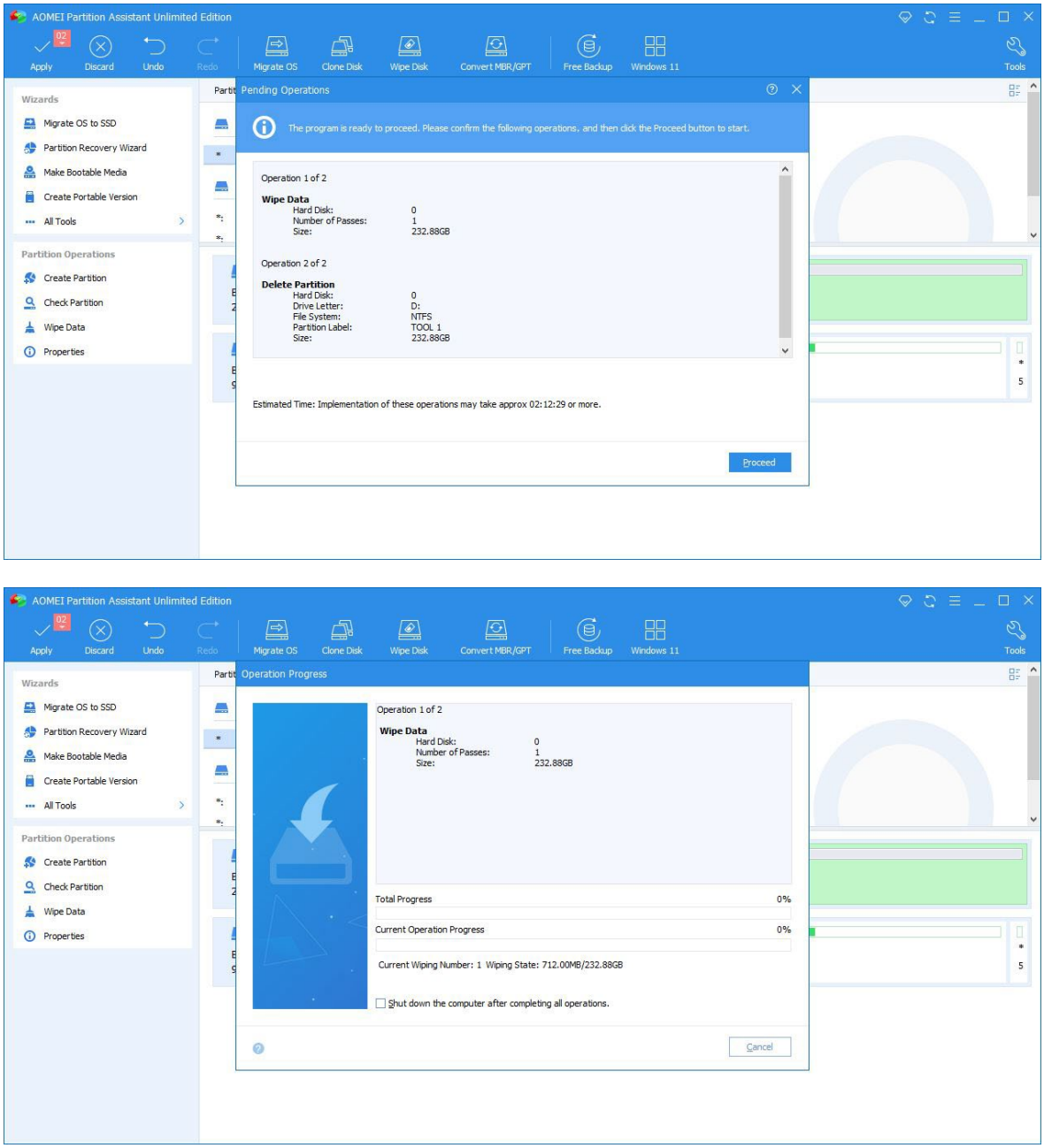
Για σκοπούς αποφυγής επανάληψης τα βήματα αρχικοποίησης και μορφοποίησης του δίσκου για το τρίτο σενάριο, αυτό της διαγραφής ολόκληρου του δίσκου με τα 200GB δεδομένων σε αυτόν, δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια πιο πάνω. Θα αναφερθούμε μόνο επιγραμματικά ως βήματα.

1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser.
2. Ενεργοποίηση εργαλείου USB Write Blocker
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.

4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.
5. Αρχικοποίηση MBR και μορφοποίηση του δίσκου σε NTFS Format.
6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.
7. Αντιγραφή 200GB στο δίσκο για διαγραφή.
8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.
9. Έναρξη διαδικασίας διαγραφής ολόκληρου του δίσκου με το εργαλείο οριστικής διαγραφής .

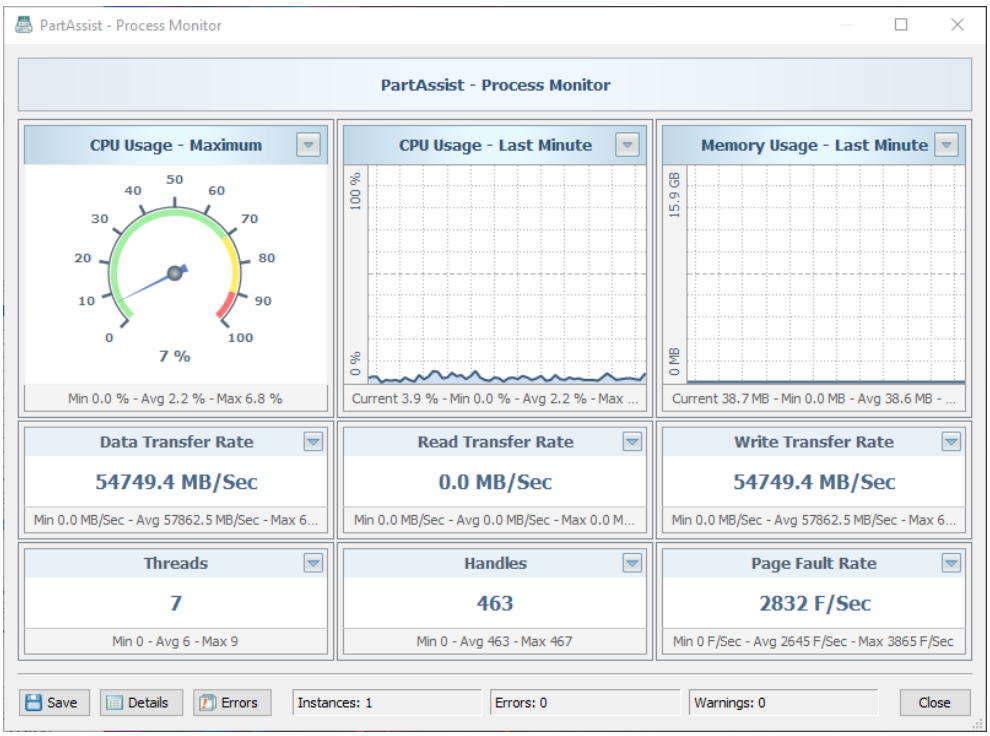


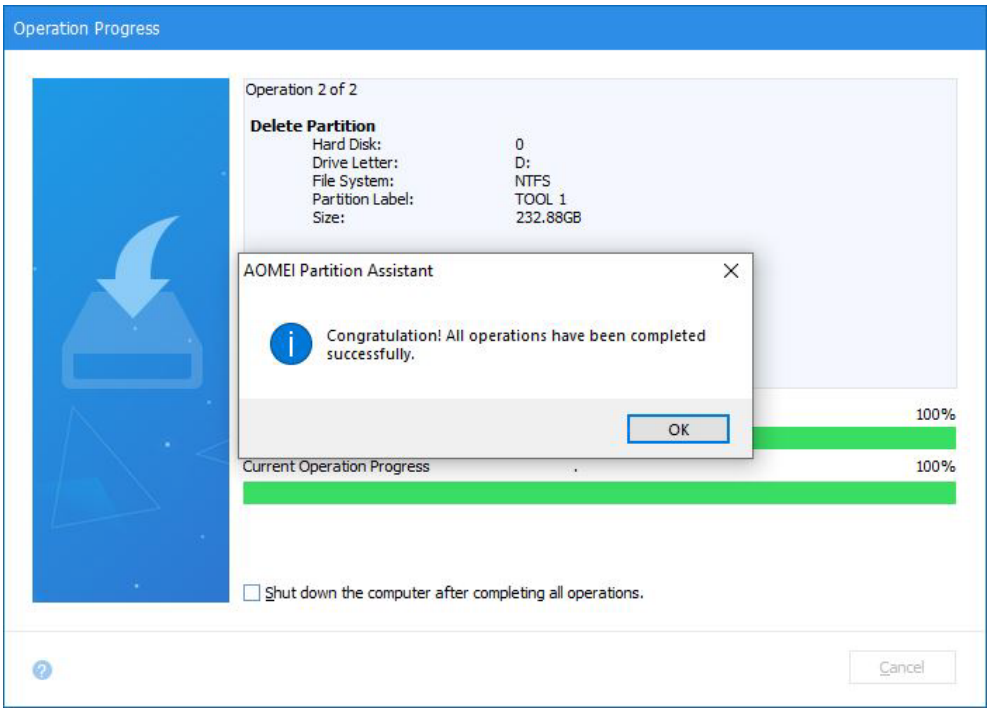



**Εικόνα 5-38: Εργαλείο 1 - AOMEI Partition Assistant - Διαδικασία οριστικής διαγραφής ολόκληρου του δίσκου**

Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.



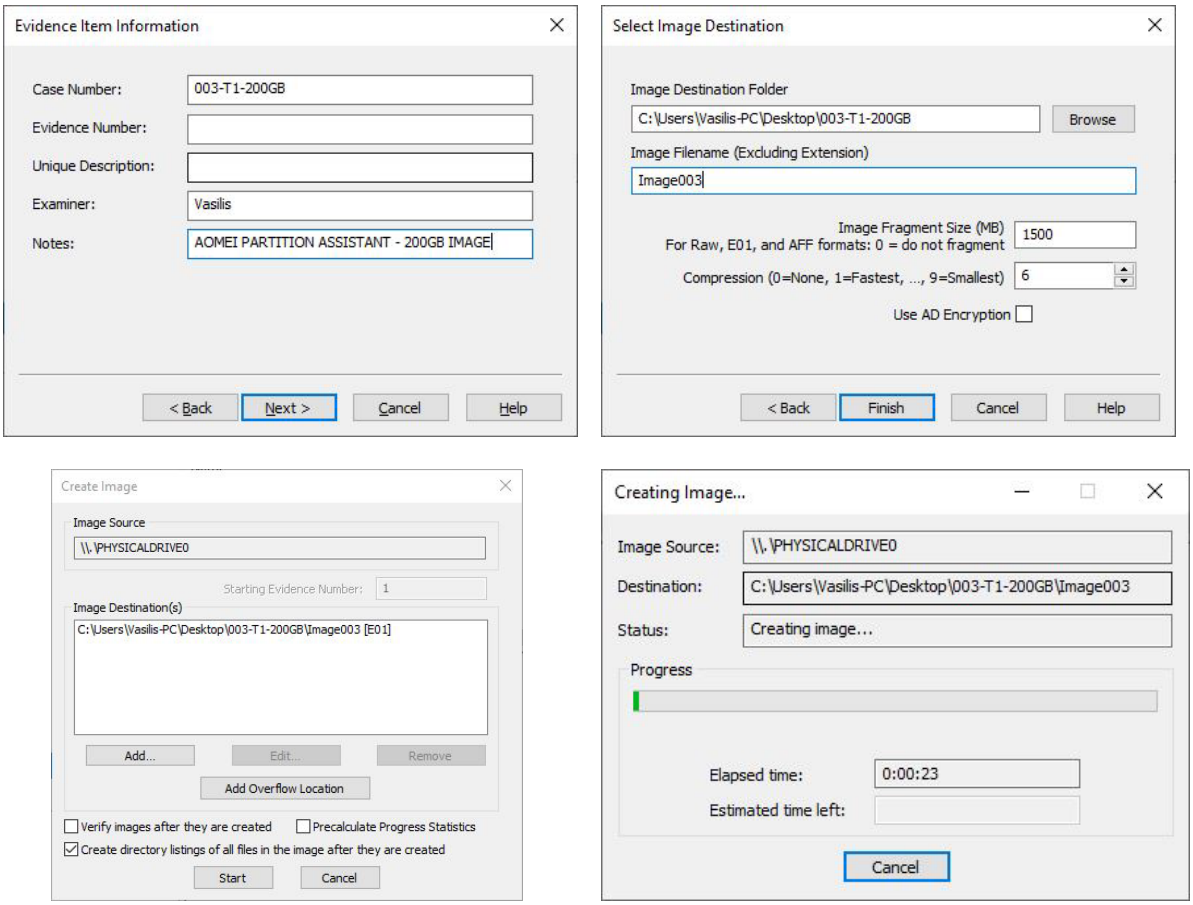

**Εικόνα 5-39: Εργαλείο 1 - SysGauge - Καταγραφή CPU και Memory κατά την διαγραφή του δίσκου**



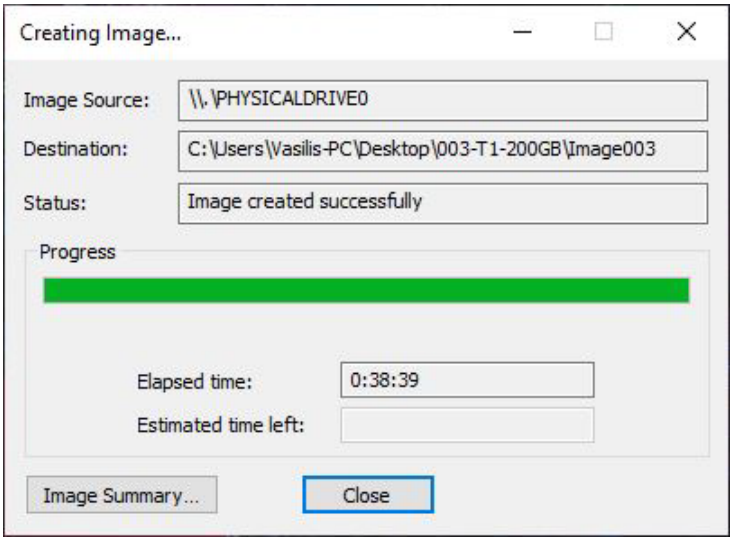

**Εικόνα 5-40: Εργαλείο 1 - AOMEI Partition Assistant - Ολοκλήρωση διαδικασίας διαγραφής δίσκου με 200GB**

Μετά την ολοκλήρωση της διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 200 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για τελευταία φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που

ακολουθήσαμε και στην πιο πάνω περίπτωση με μόνη διαφορά στην ονομασία της εικόνας του δίσκου ώστε να υπάρχει διαχωρισμός των δοκιμών σύμφωνα με τον πίνακα κωδικοποίησης σεναρίων που ορίσαμε.




**Εικόνα 5-41: Εργαλείο 1 - AccessData FTK Imager - Διαδικασία δημιουργίας 3ης εικόνας δίσκου μετά την διαγραφή**

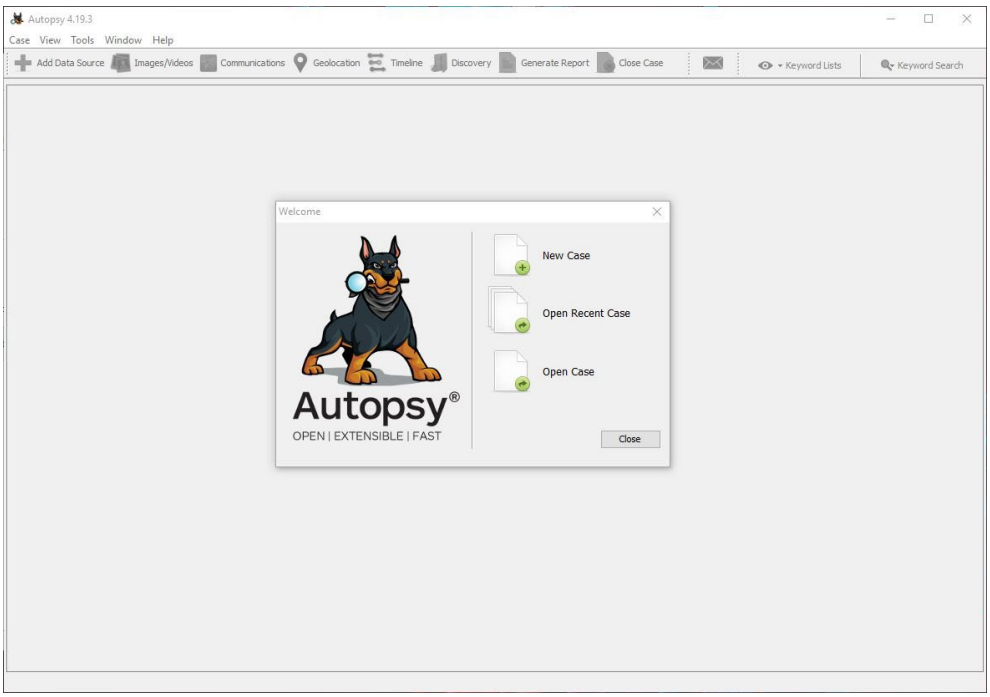



**Εικόνα 5-42: Εργαλείο 1 - AccessData FTK Imager - Ολοκλήρωση δημιουργίας 3ης εικόνας δίσκου**

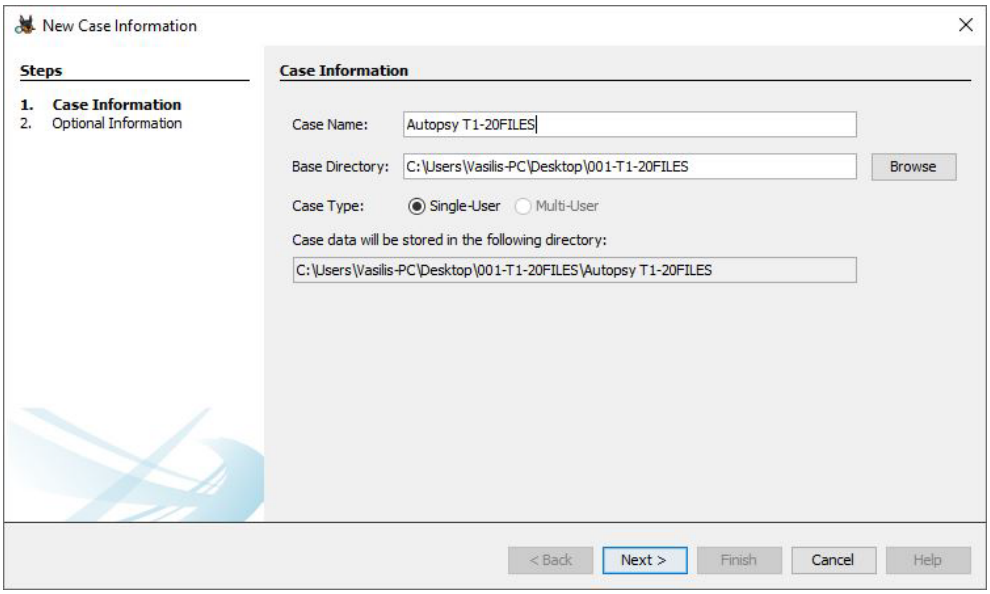
Μετά την ολοκλήρωση των τριών σεναρίων προχωρούμε με τη χρήση δικανικών εργαλείων σε διερεύνηση των εικόνων των δίσκων ώστε να εντοπίσουμε ίχνη από τα αρχικά δεδομένα.

Εισαγωγή εικόνων δίσκων στο Autopsy

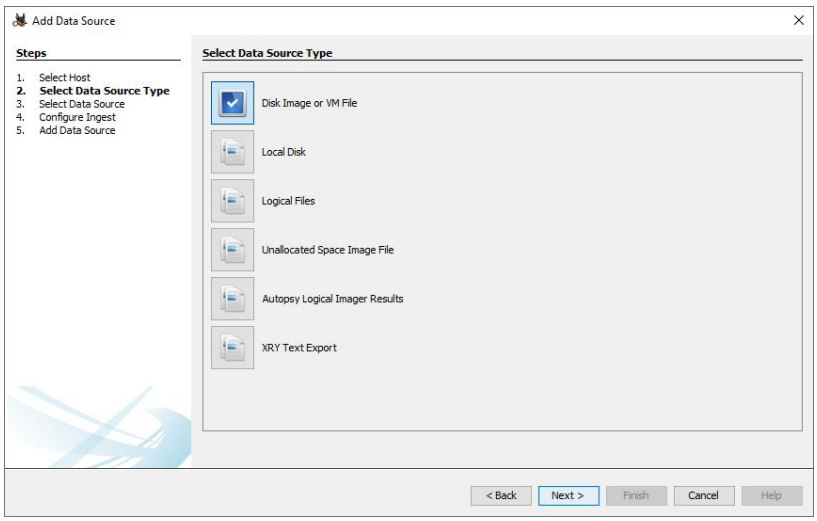
1. Εικόνα δίσκου με τα 20 διαγραμμένα αρχεία



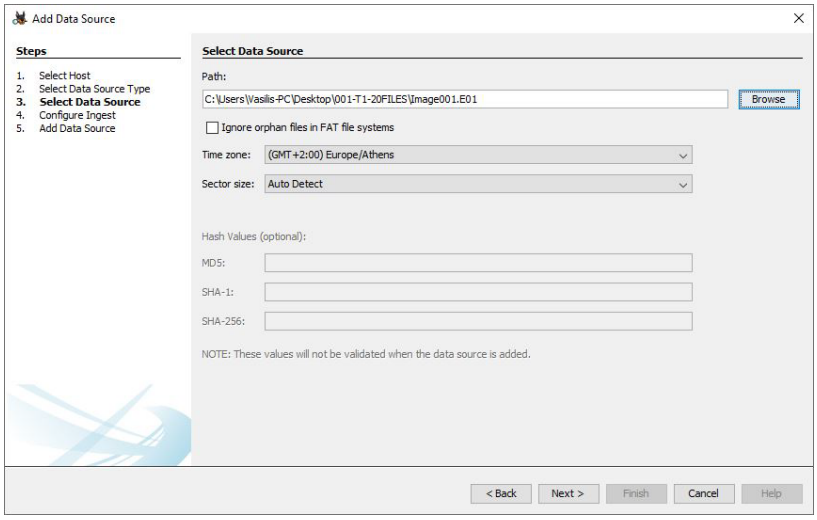

**Εικόνα 5-43: Εργαλείο 1 - Autopsy - Εισαγωγή εικόνας δίσκου - Βήμα 1**



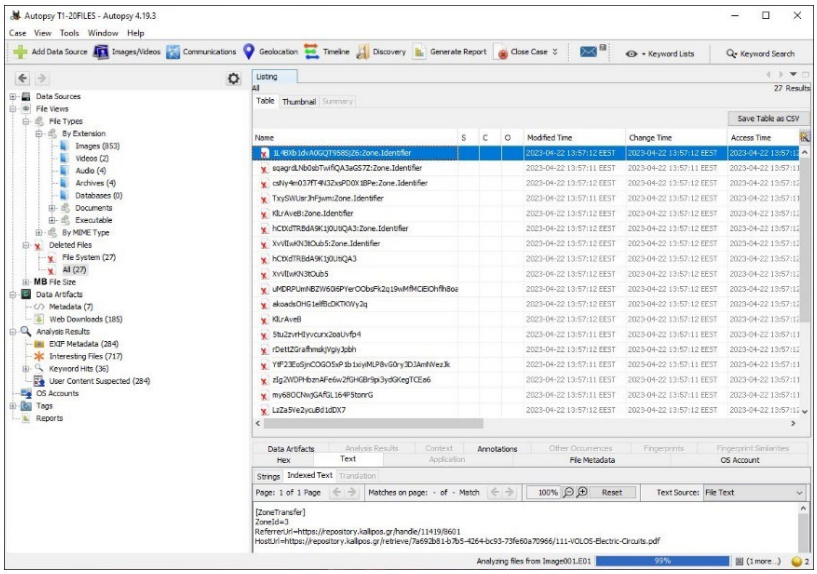

**Εικόνα 5-44: Εργαλείο 1 - Autopsy - Εισαγωγή εικόνας δίσκου - Βήμα 2**




**Εικόνα 5-45: Εργαλείο 1 - Autopsy - Εισαγωγή εικόνας δίσκου - Βήμα 3**

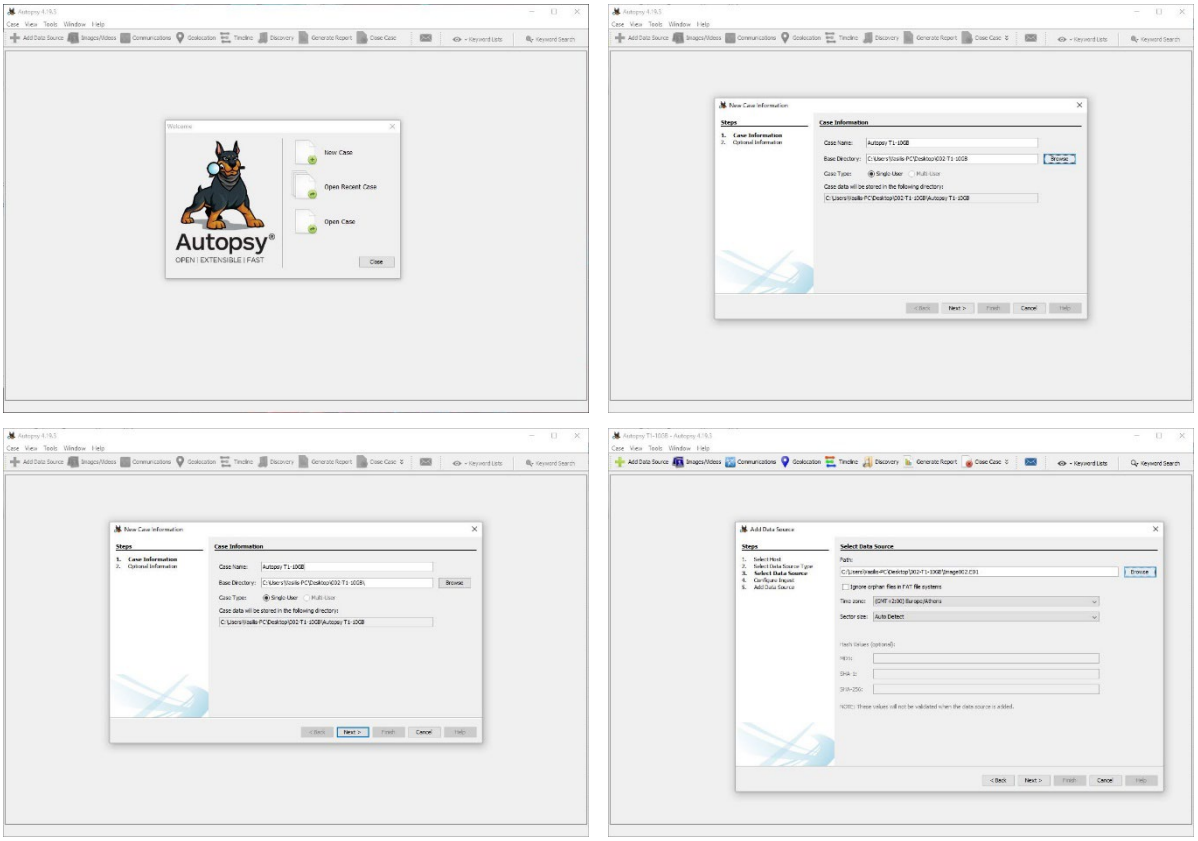



**Εικόνα 5-46: Εργαλείο 1 - Autopsy - Εισαγωγή εικόνας δίσκου - Βήμα 4**



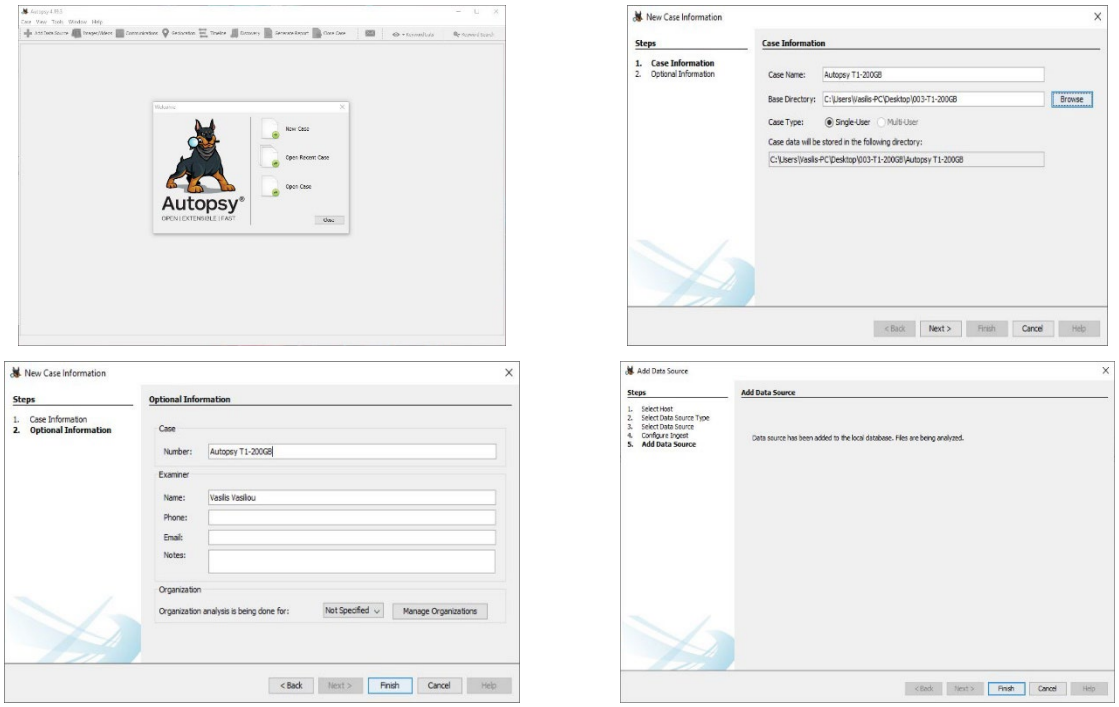

**Εικόνα 5-47: Εργαλείο 1 - Autopsy - Αναζήτηση δεδομένων**

2. Εικόνα δίσκου με 10GB δεδομένων διαγραμμένος ολόκληρος



**Εικόνα 5-48: Εργαλείο 1 - Autopsy - Διαδικασία εισαγωγής 2ης εικόνας δίσκου**

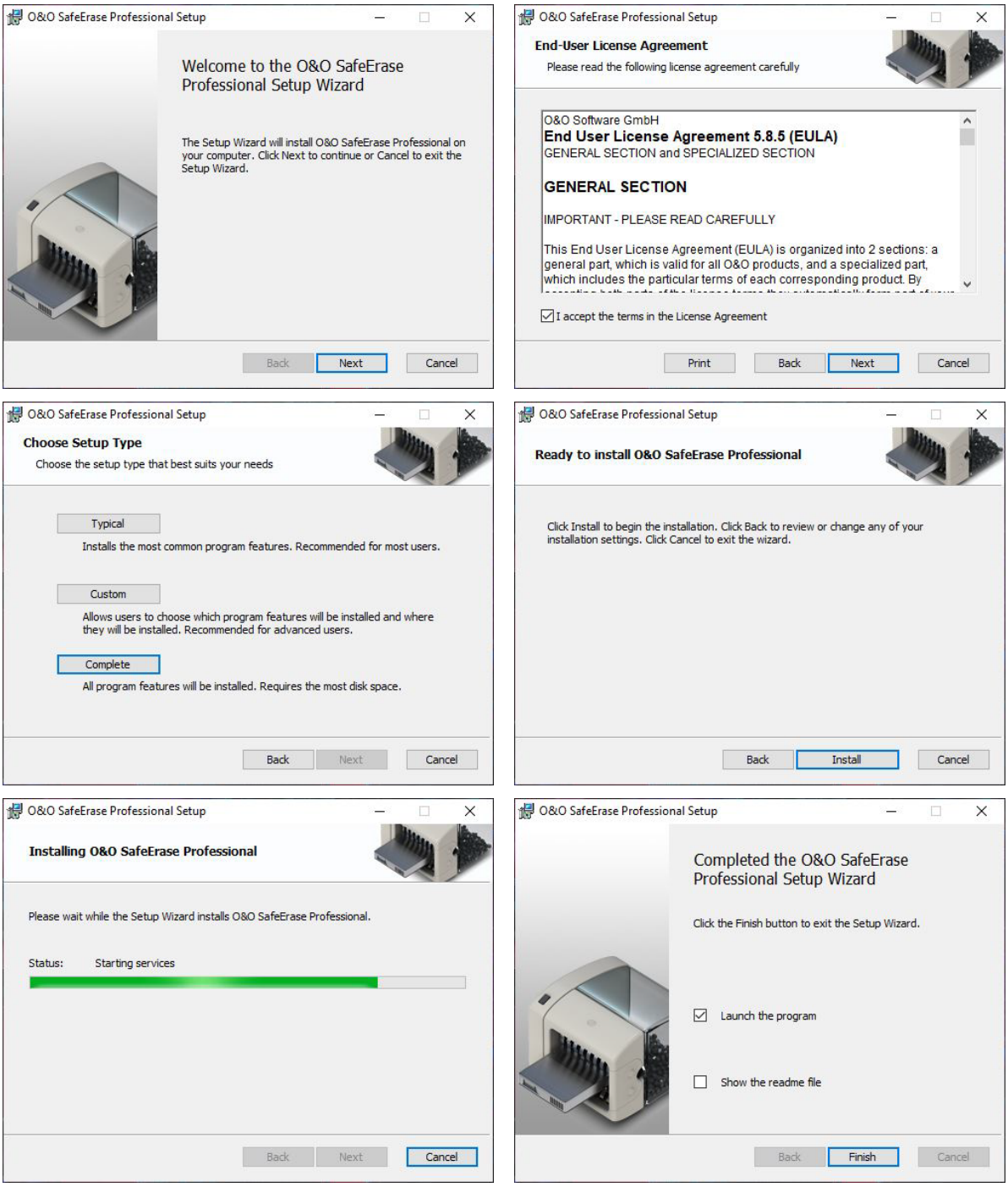
3. Εικόνα δίσκου με 200GB δεδομένων διαγραμμένος ολόκληρος



**Εικόνα 5-49: Εργαλείο 1 - Autopsy - Διαδικασία εισαγωγής 3ης εικόνας δίσκου**

### 5.2.2 Εργαλείο 2 - O&O SafeEraser

Εγκατάσταση εργαλείου

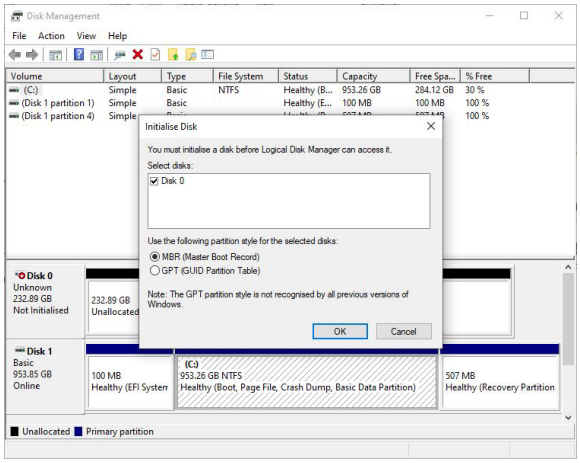


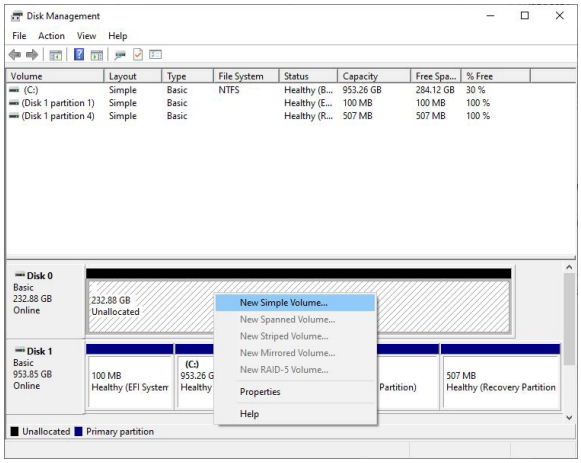

**Εικόνα 5-50: Εργαλείο 2 - Διαδικασία εγκατάστασης O&O SafeErase**

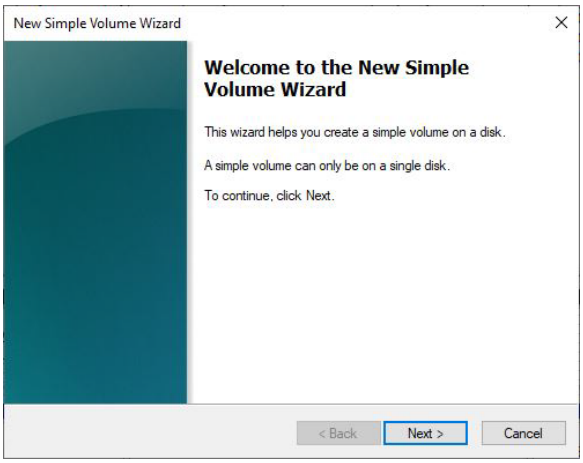
Για σκοπούς αποφυγής επανάληψης, τα βήματα προετοιμασίας του δίσκου για την αξιολόγηση του δεύτερου εργαλείου οριστικής διαγραφής δεδομένων δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια κατά την εξέταση του πρώτου εργαλείου.

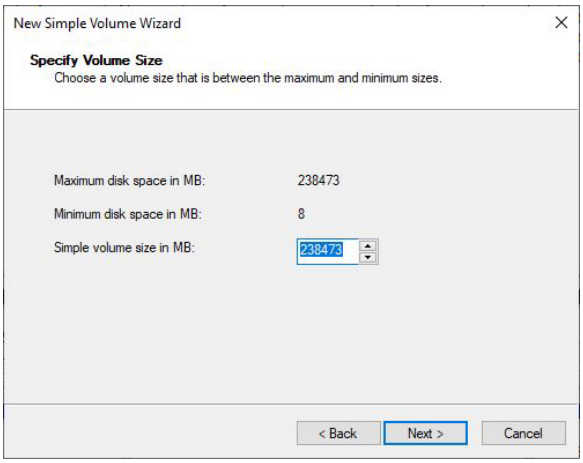
Θα αναφερθούμε μόνο επιγραμματικά στα βήματα.

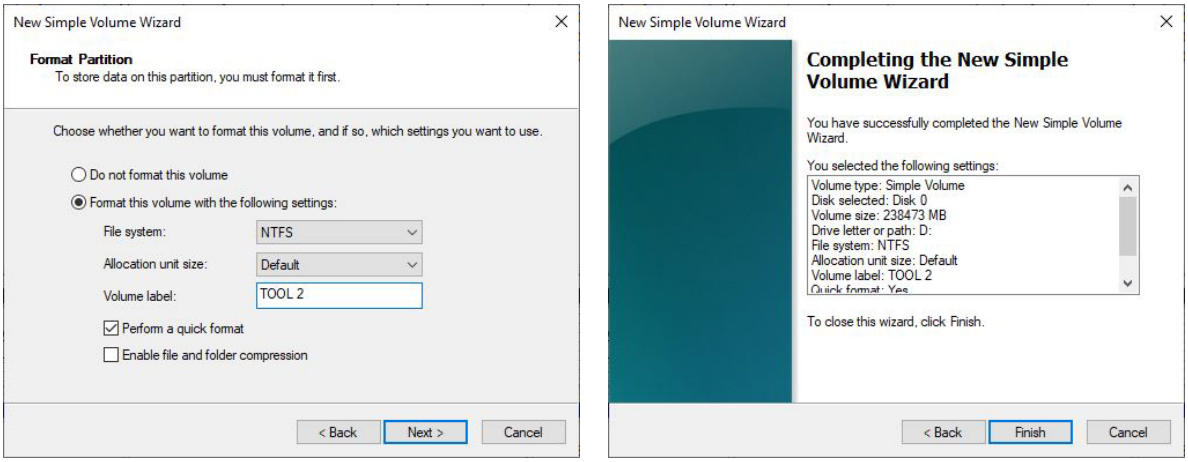
1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser.
2. Ενεργοποίηση εργαλείου USB Write Blocker.
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.
4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.
5. Αρχικοποίηση MBR, μορφοποίηση του δίσκου σε NTFS Format και ονομασία του δίσκου σε TOOL 2.



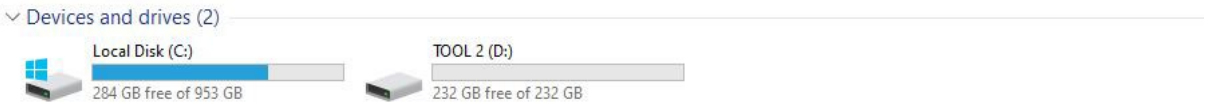



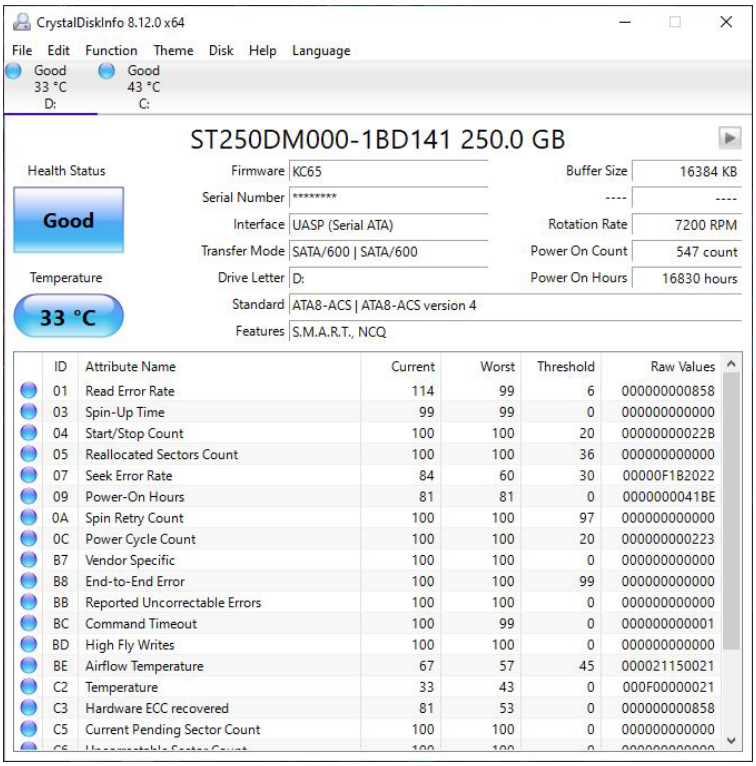



**Εικόνα 5-51: Εργαλείο 2 - Βήματα διαδικασίας μορφοποίησης δίσκου**

Τα πιο πάνω βήματα αποτελούν τη διαδικασία για τη μορφοποίηση του σκληρού δίσκου ώστε να μπορεί να χρησιμοποιηθεί από το λειτουργικό σύστημα. Μετά το πέρας της διαδικασίας ο δίσκος με την ονομασία TOOL 2 είναι ορατός και μπορεί να χρησιμοποιηθεί κανονικά από τα windows.



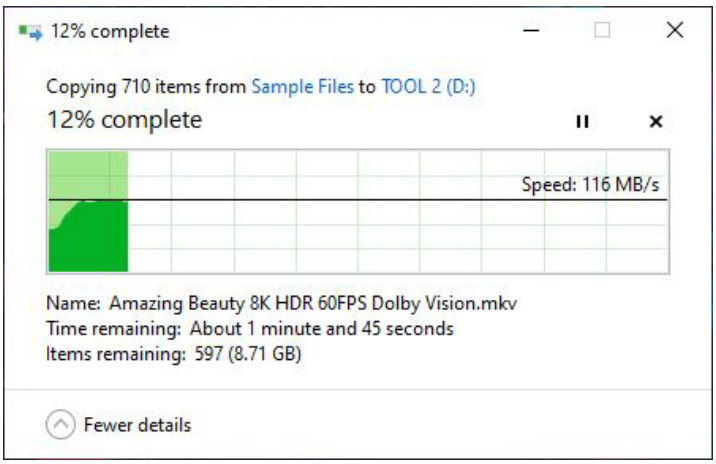

6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.




**Εικόνα 5-52: Εργαλείο 2 - CrystalDiskInfo - Αναφορά κατάστασης δίσκου**

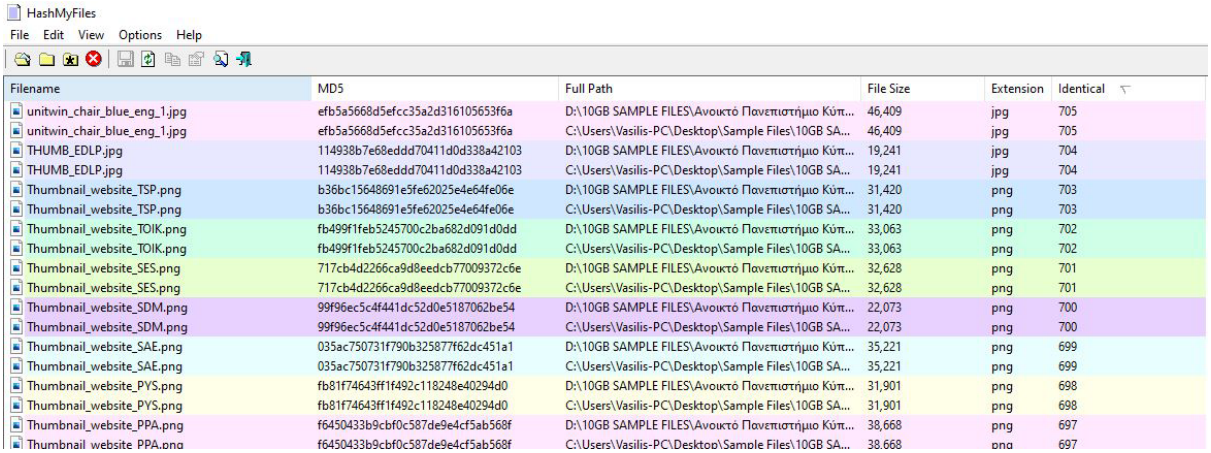
Σύμφωνα με την αναφορά του εργαλείου, ο δίσκος βρίσκεται σε καλή κατάσταση έτσι μπορούμε να αντιγράψουμε σε αυτόν τα αρχικά δεδομένα των 10 GB (705 αρχεία).

7. Αντιγραφή 10GB στο δίσκο




**Εικόνα 5-53: Εργαλείο 2 - Αντιγραφή 10GB δεδομένων στο δίσκο**

8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.



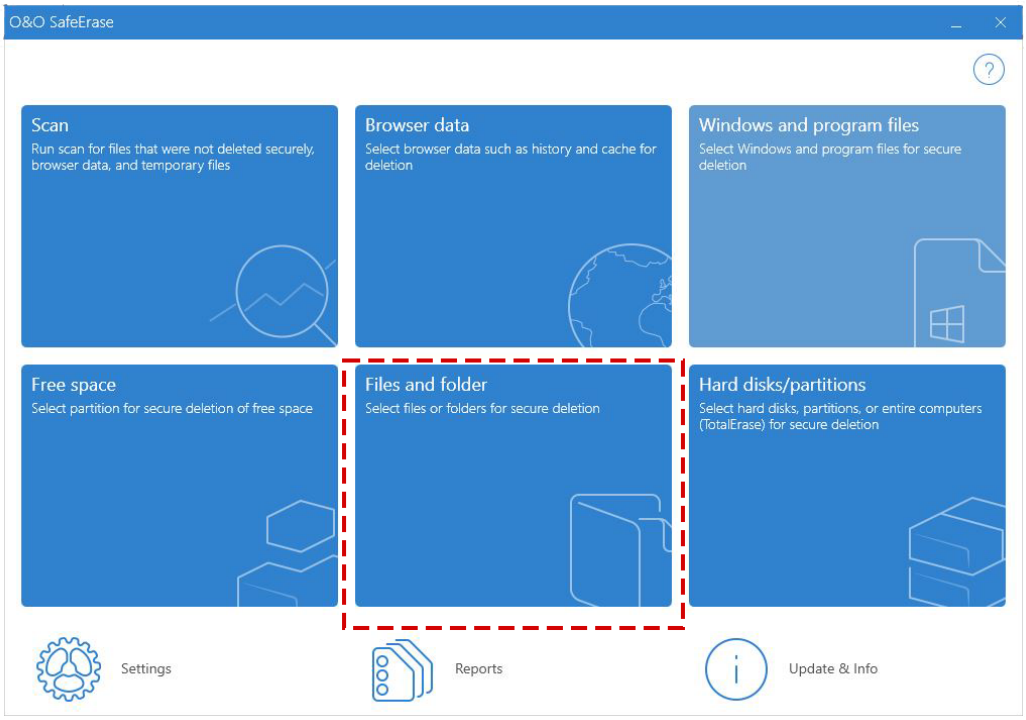

| Filename | MD5 | Full Path | File Size | Extension | Identical |
|---|---|---|---|---|---|
| unitwin_chair_blue_eng_1.jpg | efb5a5668d5efcc35a2d316105653f6a | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 46,409 | jpg | 705 |
| unitwin_chair_blue_eng_1.jpg | efb5a5668d5efcc35a2d316105653f6a | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 46,409 | jpg | 705 |
| THUMB_EDLP.jpg | 114938b7e68eddd70411d0d338a42103 | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 19,241 | jpg | 704 |
| THUMB_EDLP.jpg | 114938b7e68eddd70411d0d338a42103 | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 19,241 | jpg | 704 |
| Thumbnail_website_TSP.png | b36bc15648691e5fe62025e4e64fe06e | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 31,420 | png | 703 |
| Thumbnail_website_TSP.png | b36bc15648691e5fe62025e4e64fe06e | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 31,420 | png | 703 |
| Thumbnail_website_TOIK.png | fb499f1feb5245700c2ba682d091d0dd | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 33,063 | png | 702 |
| Thumbnail_website_TOIK.png | fb499f1feb5245700c2ba682d091d0dd | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 33,063 | png | 702 |
| Thumbnail_website_SES.png | 717cb4d2266ca9d8eedcb77009372c6e | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 32,628 | png | 701 |
| Thumbnail_website_SES.png | 717cb4d2266ca9d8eedcb77009372c6e | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 32,628 | png | 701 |
| Thumbnail_website_SDM.png | 99f96ec5c4f441dc52d0e5187062be54 | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 22,073 | png | 700 |
| Thumbnail_website_SDM.png | 99f96ec5c4f441dc52d0e5187062be54 | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 22,073 | png | 700 |
| Thumbnail_website_SAE.png | 035ac750731f790b325877f62dc451a1 | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 35,221 | png | 699 |
| Thumbnail_website_SAE.png | 035ac750731f790b325877f62dc451a1 | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 35,221 | png | 699 |
| Thumbnail_website_PYS.png | fb81f74643ff1f492c118248e40294d0 | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 31,901 | png | 698 |
| Thumbnail_website_PYS.png | fb81f74643ff1f492c118248e40294d0 | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 31,901 | png | 698 |
| Thumbnail_website_PPA.png | f6450433b9cbf0c587de9e4cf5ab568f | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 38,668 | png | 697 |
| Thumbnail_website_PPA.png | f6450433b9cbf0c587de9e4cf5ab568f | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 38,668 | png | 697 |

**Εικόνα 5-54: Εργαλείο 2 - HashMyFiles - Επιβεβαίωση αντιγραφής αρχείων στο δίσκο**

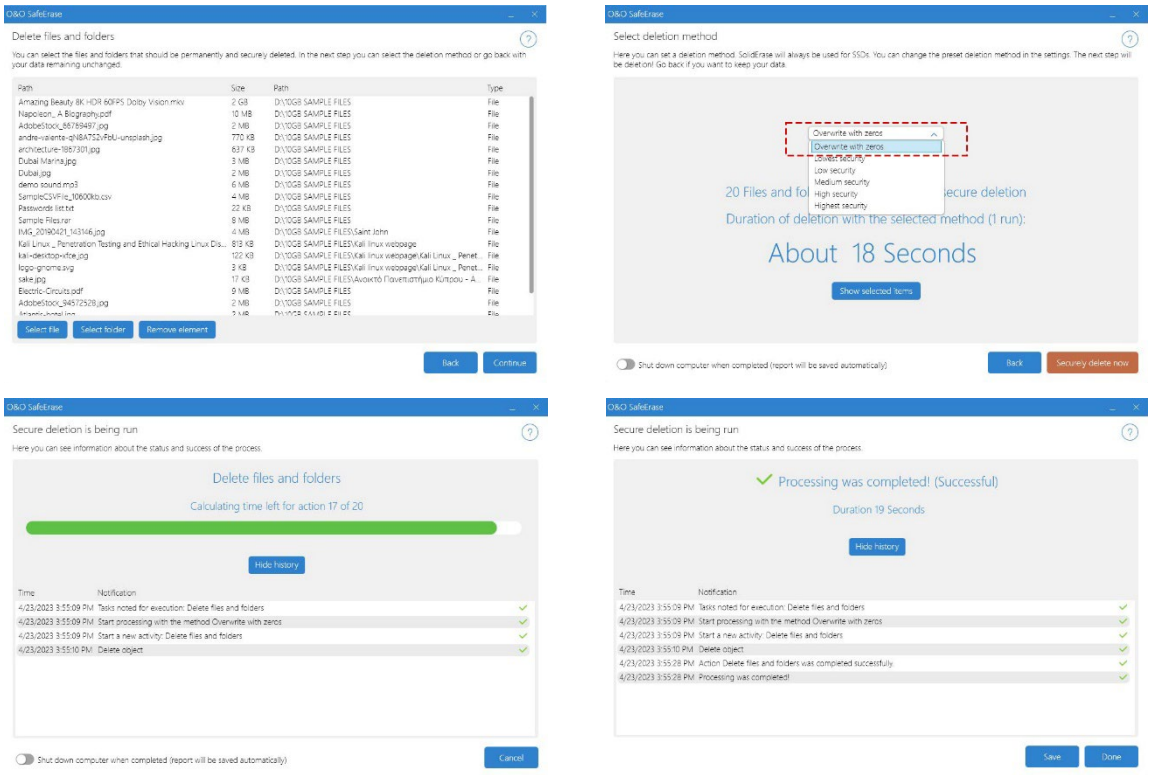
- **<u>Εκτέλεση πρώτου σεναρίου</u>** – Διαγραφή 20 συγκεκριμένων αρχείων από το δίσκο

Από το κεντρικό μενού επιλέγουμε Αρχεία και Φάκελοι (Files and Folder). Στη συνέχεια επιλέγουμε τα 20 αρχεία που έχουμε καθορίσει από την αρχή για τη διεξαγωγή αυτού του σεναρίου για όλα τα εργαλεία οριστικής διαγραφής δεδομένων. Τα αρχεία που έχουν επιλεγεί είναι διαφόρων τύπων και μεγεθών. Ο αναλυτικός κατάλογος των αρχείων αυτών μαζί με το ακριβές μέγεθος τους και την hash τιμή MD5 η οποία θα χρησιμοποιηθεί αργότερα κατά την σύγκριση τους με τα ευρήματα στο δίσκο, βρίσκεται στο τέλος (Παράρτημα Α). Επίσης καθορίζουμε τη μέθοδο

διαγραφής σε Overwrite with Zeros. Η μέθοδος αυτή είναι η αντίστοιχη μέθοδος One Pass Zero κατά την οποία τα δεδομένα του δίσκου εγγράφονται σε μια επανάληψη με μηδενικά.

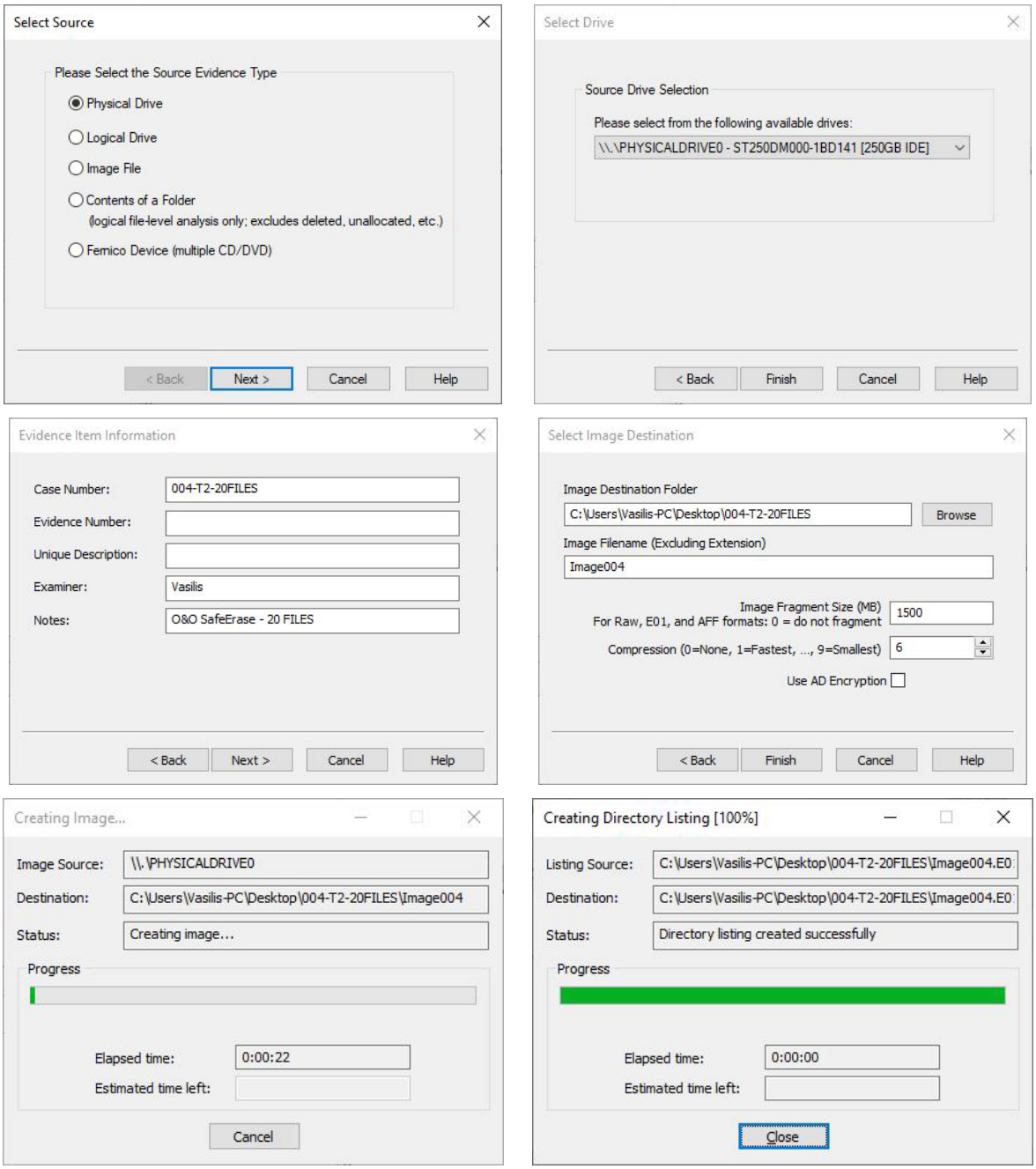



**Εικόνα 5-55: Εργαλείο 2 - O&O SafeErase – Κεντρικό μενού**




**Εικόνα 5-56: Εργαλείο 2 - O&O SafeErase - Διαδικασία διαγραφής των 20 αρχείων**

Με το πέρας της διαδικασίας διαγραφής των αρχείων προχωρούμε σε εξαγωγή της εικόνας του δίσκου με το εργαλείο AccessData FTK Imager. Με αυτό τον τρόπο θα μπορέσουμε να εισάγουμε την εικόνα στο Autopsy και να εντοπίσουμε τυχόν ίχνη από τα αρχεία.

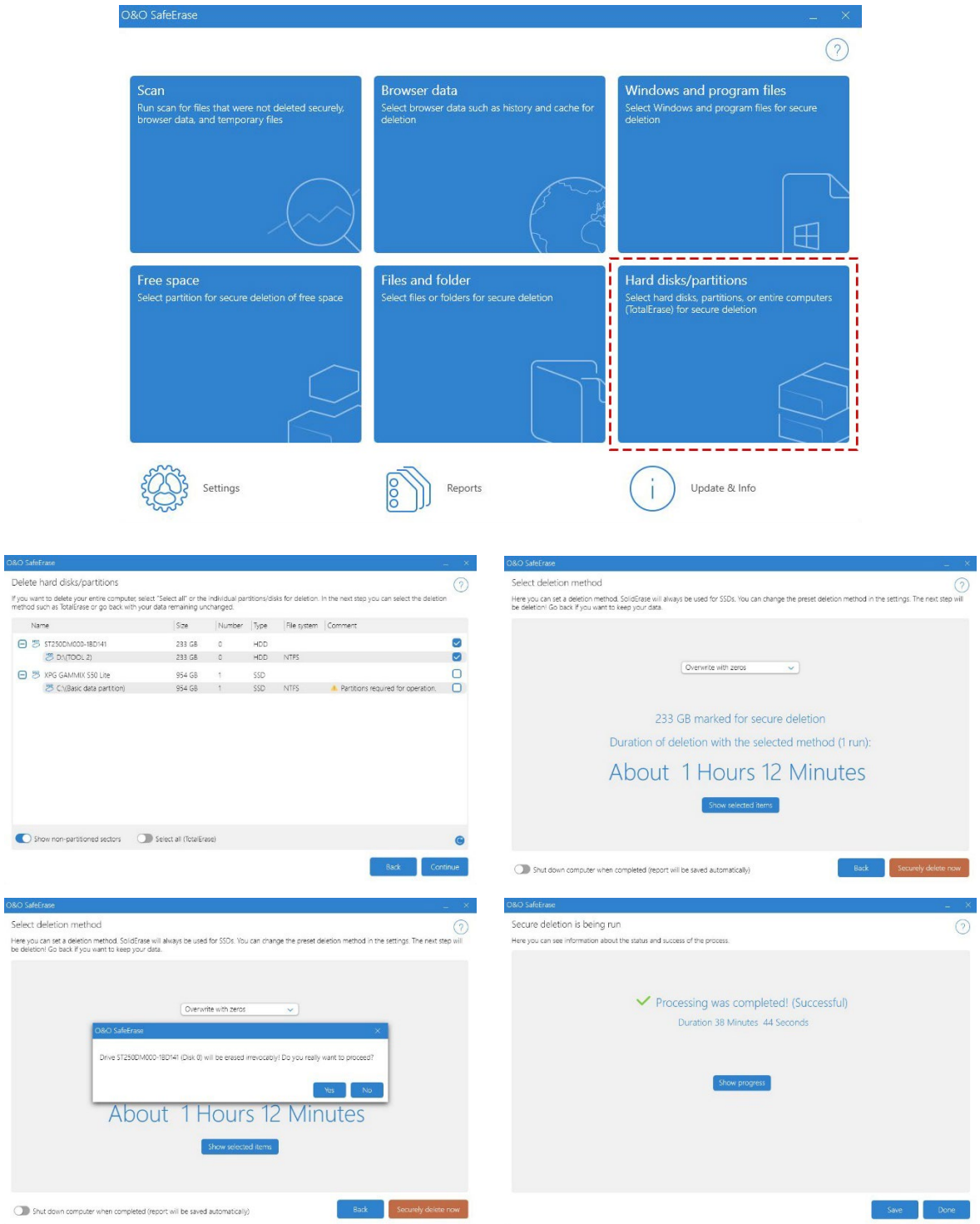



**Εικόνα 5-57: Εργαλείο 2 - AccessData FTK Imager - Διαδικασία δημιουργίας 1ης εικόνας δίσκου μετά την διαγραφή**

Η εικόνα του δίσκου θα χρησιμοποιηθεί αργότερα για εισαγωγή της στο Autopsy και ανάλυση της για την εύρεση ιχνών από τα 20 διαγραμμένα αρχεία.

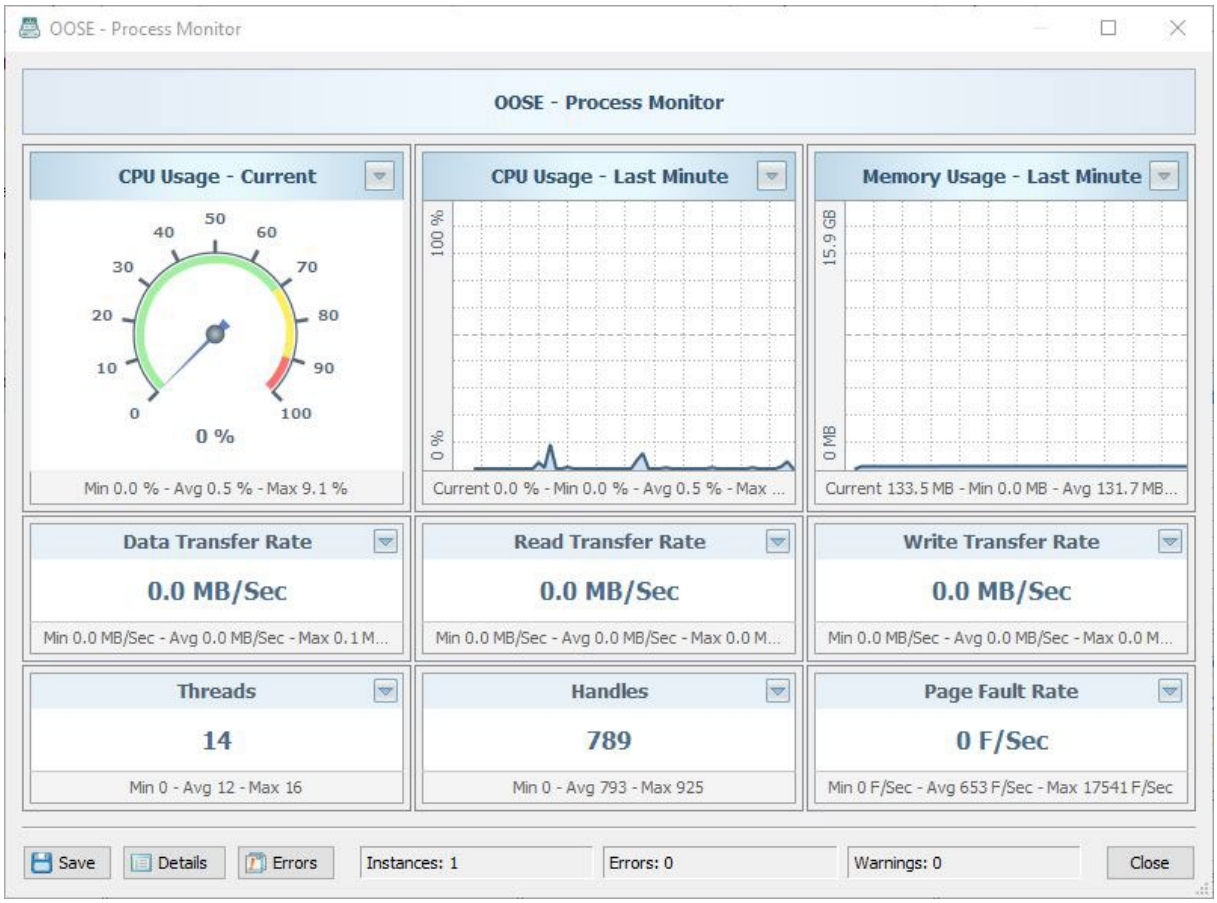
- **<u>Εκτέλεση δεύτερου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 10 GB**

Από το κεντρικό μενού επιλέγουμε Σκληροί δίσκοι / διαμερίσματα (Hard disks / partitions). Στη λίστα με τους διαθέσιμους δίσκους για διαγραφή, εντοπίζουμε το προς διαγραφή δίσκο και τον επιλέγουμε. Καθορίζουμε την τη μέθοδο διαγραφής σε Overwrite with Zeros όπως και στις προηγούμενες περιπτώσεις. Τέλος το εργαλείο μας προτρέπει να επιβεβαιώσουμε την πρόθεση μας για οριστική διαγραφή δεδομένων του δίσκου.



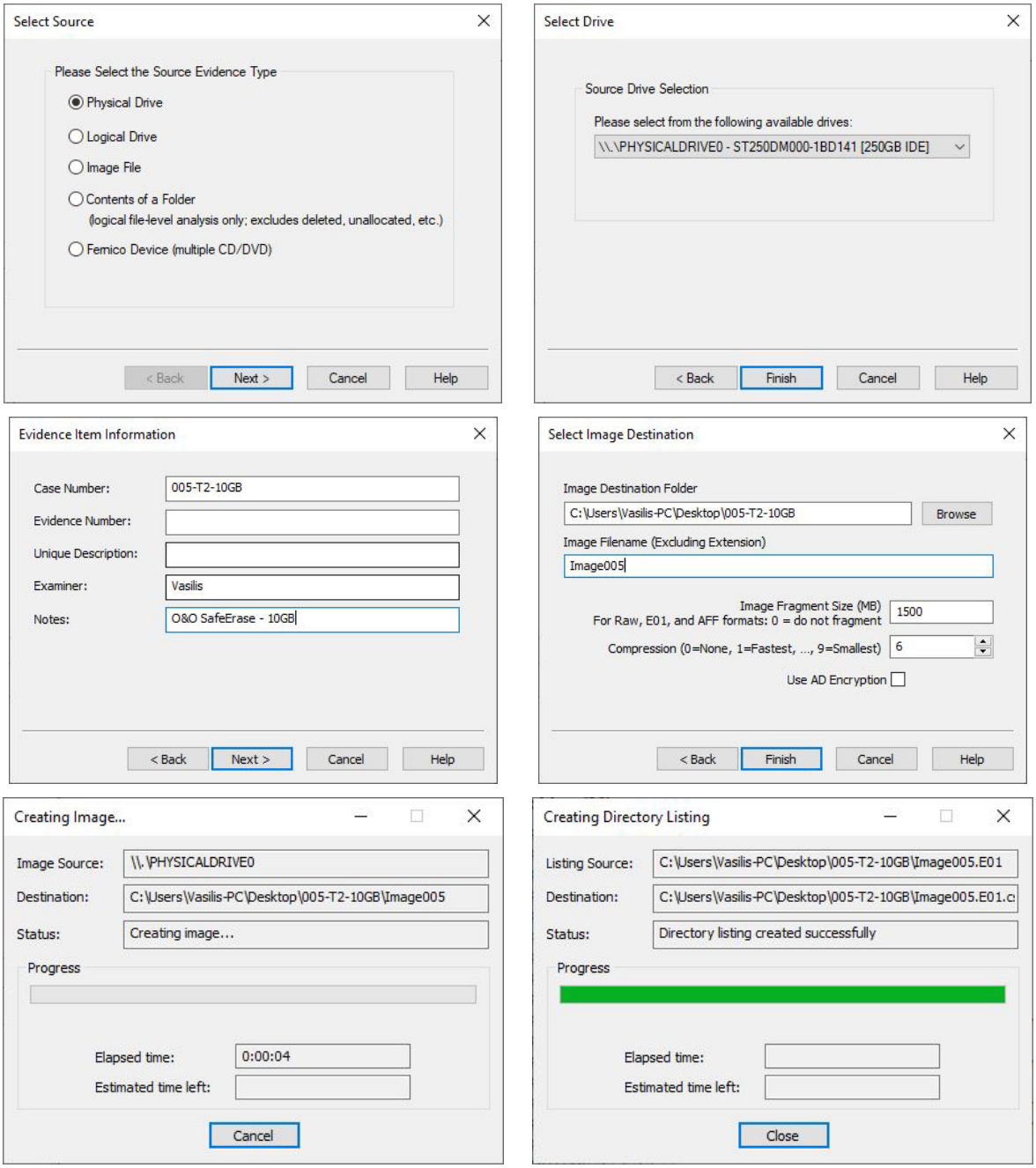

**Εικόνα 5-58: Εργαλείο 2 - O&O SafeErase - Διαδικασία διαγραφής δίσκου – Αρχεία 10GB**

Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.




**Εικόνα 5-59: Εργαλείο 2 - SysGauge - Καταγραφή πόρων συστήματος κατα την διαγραφή ολόκληρου του δίσκου - 10GB**

Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 10 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για δεύτερη φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που ακολουθήσαμε και στην πιο πάνω περίπτωση με διαφορά την ονομασία της εικόνας του δίσκου ώστε να υπάρχει αρχειοθέτηση και καταγραφή των δοκιμών σύμφωνα με το πίνακα κωδικοποίησης σεναρίων που ορίσαμε.



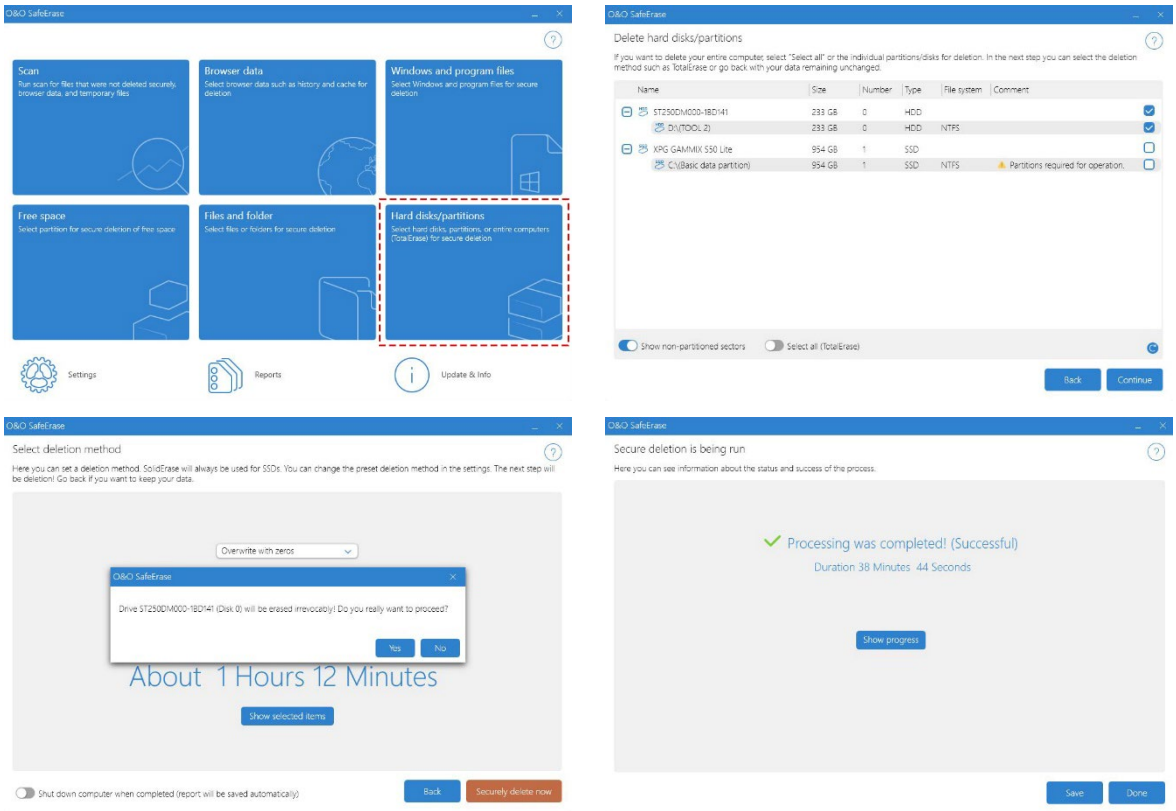

**Εικόνα 5-60: Εργαλείο 2 - AccessData FTK Imager - Διαδικασία δημιουργίας 2ης εικόνας δίσκου μετά την διαγραφή**

- **<u>Εκτέλεση τρίτου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 200 GB**

Για σκοπούς αποφυγής επανάληψης τα βήματα αρχικοποίησης και μορφοποίησης του δίσκου για το τρίτο σενάριο, αυτό της διαγραφής ολόκληρου του δίσκου με τα 200GB δεδομένων σε αυτόν, δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια πιο πάνω. Θα αναφερθούμε μόνο επιγραμματικά ως βήματα.

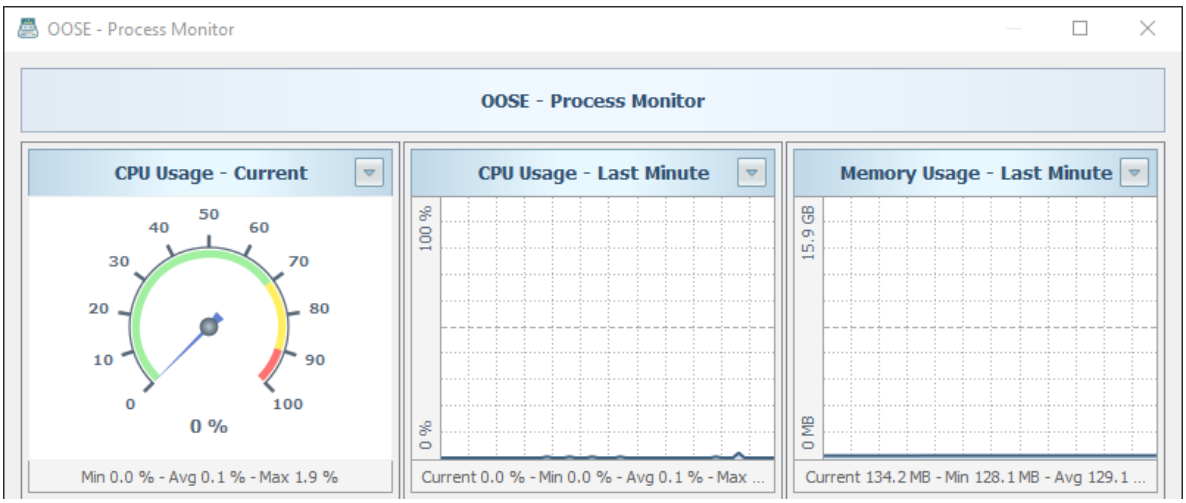
1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser.

2. Ενεργοποίηση εργαλείου USB Write Blocker
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.
4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.
5. Αρχικοποίηση MBR και μορφοποίηση του δίσκου σε NTFS Format.
6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.
7. Αντιγραφή 200GB στο δίσκο για διαγραφή.
8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.
9. Έναρξη διαδικασίας διαγραφής ολόκληρου του δίσκου με το εργαλείο οριστικής διαγραφής .



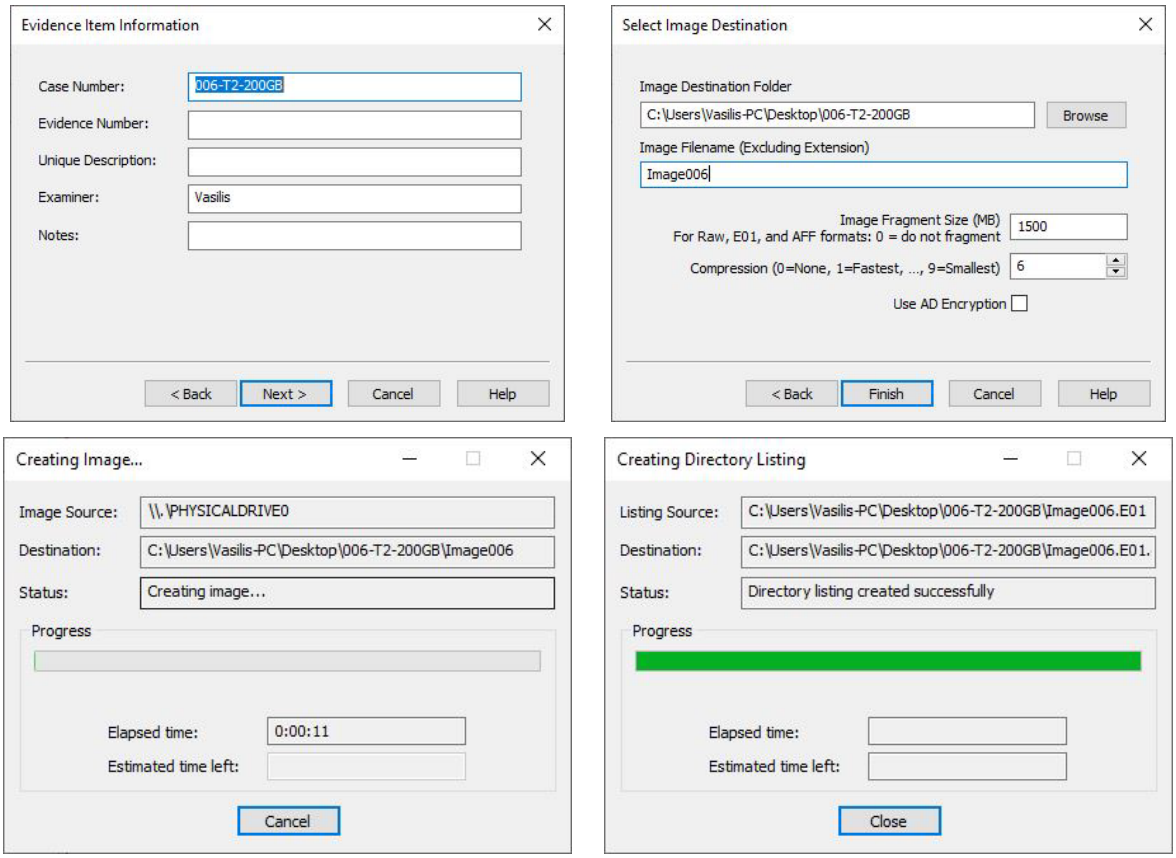

**Εικόνα 5-61: Εργαλείο 2 - O&O SafeErase - Διαδικασία διαγραφής δίσκου – Αρχεία 200GB**

Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.




**Εικόνα 5-62: Εργαλείο 2 - SysGauge - Καταγραφή πόρων συστήματος κατα την διαγραφή ολόκληρου του δίσκου - 200GB**

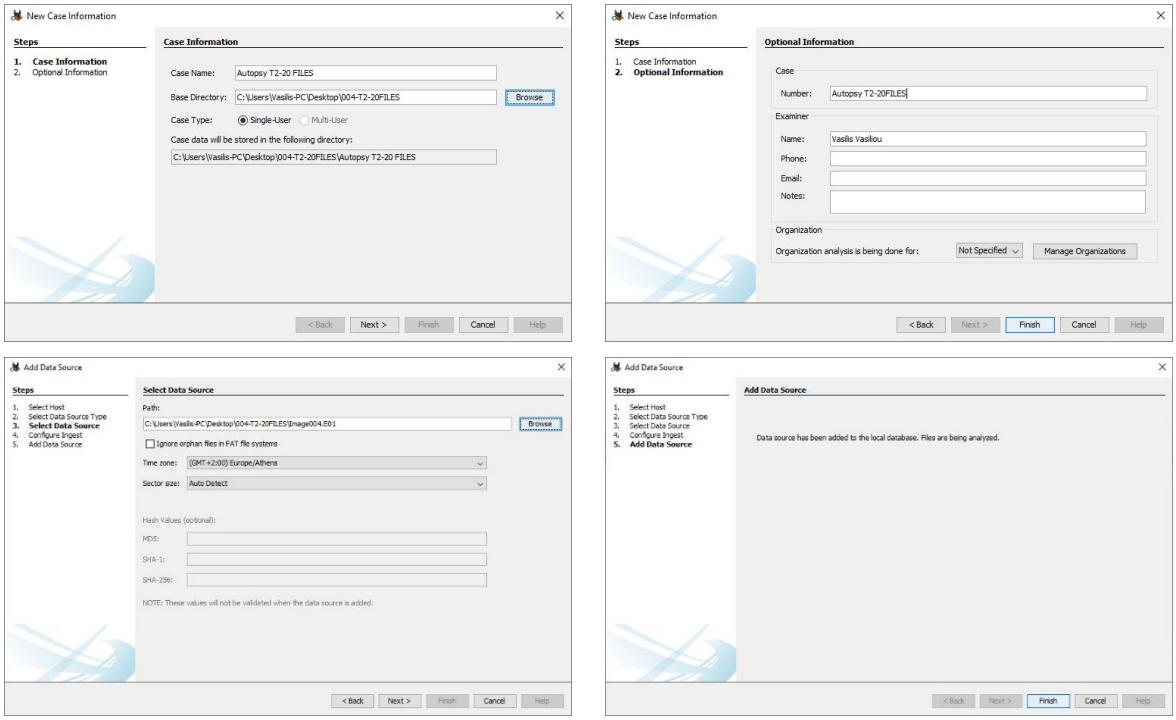
Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 200 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για τρίτη φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που ακολουθήσαμε και στην πιο πάνω περίπτωση με διαφορά την ονομασία της εικόνας του δίσκου ώστε να υπάρχει αρχειοθέτηση και καταγραφή των σεναρίων .




**Εικόνα 5-63: Εργαλείο 2 - AccessData FTK Imager - Διαδικασία δημιουργίας 3ης εικόνας δίσκου μετά την διαγραφή**

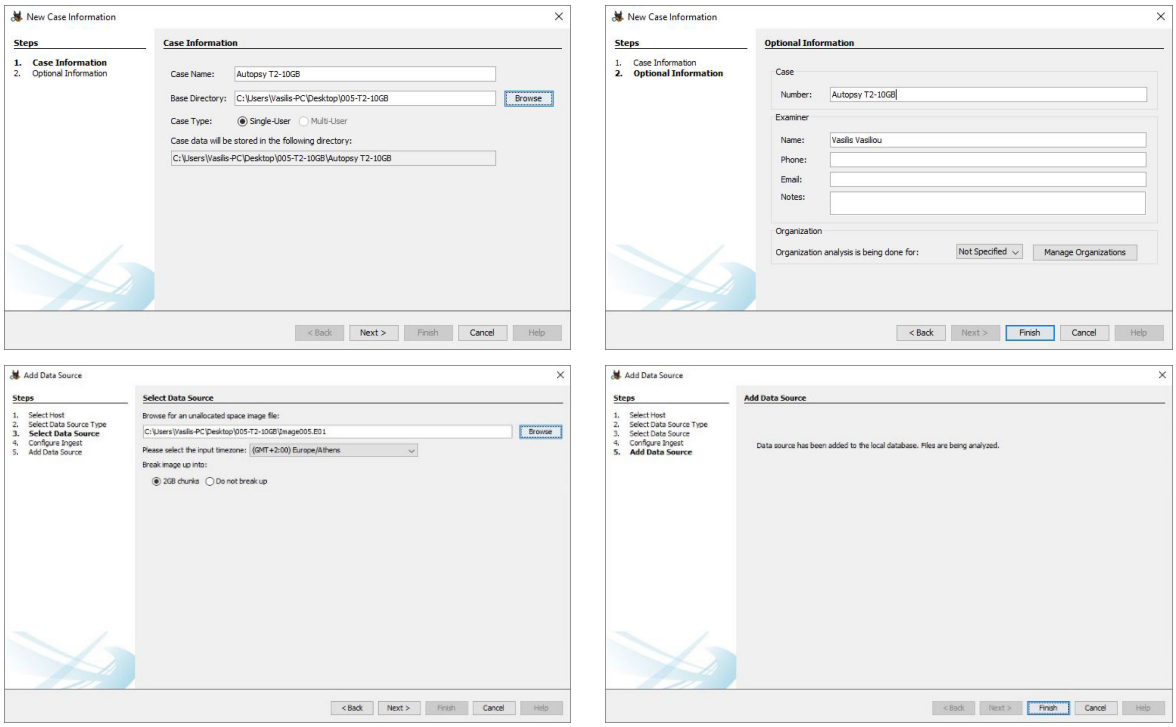
Εισαγωγή εικόνων δίσκων στο Autopsy

1. Εικόνα δίσκου με τα 20 διαγραμμένα αρχεία



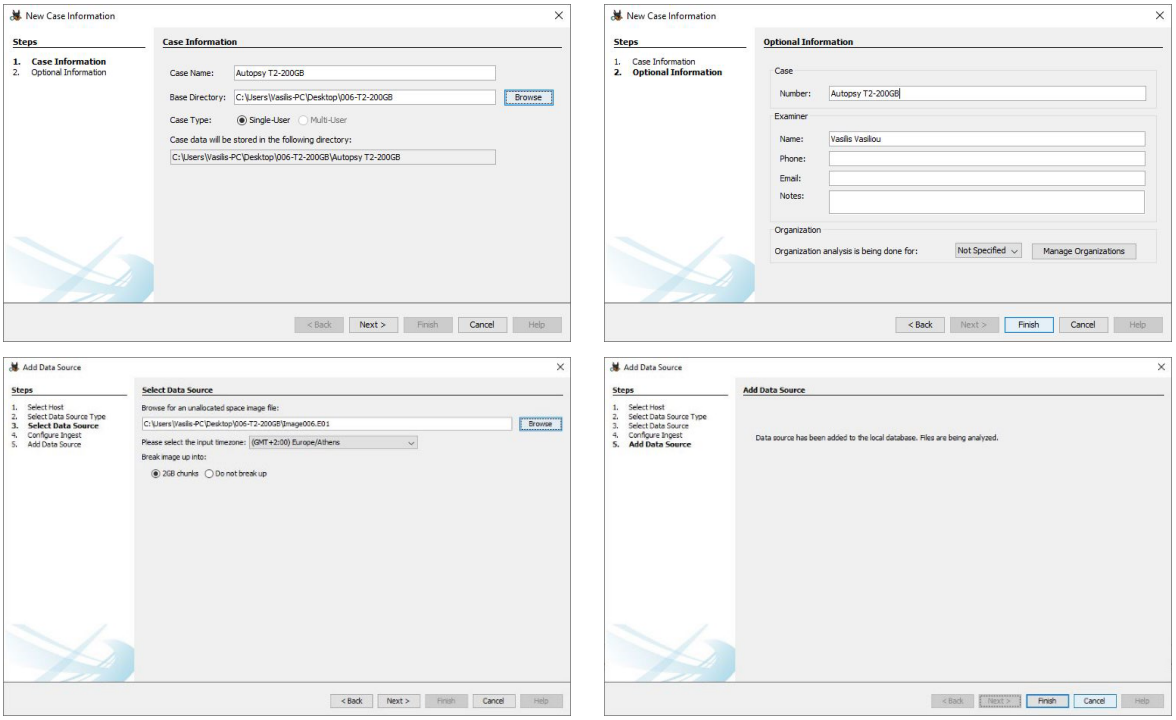

**Εικόνα 5-64: Εργαλείο 2 - Autopsy - Βήματα εισαγωγής 1ης εικόνας δίσκου**

2. Εικόνα δίσκου με 10GB δεδομένων διαγραμμένος ολόκληρος




**Εικόνα 5-65: Εργαλείο 2 - Autopsy - Βήματα εισαγωγής 2ης εικόνας δίσκου**

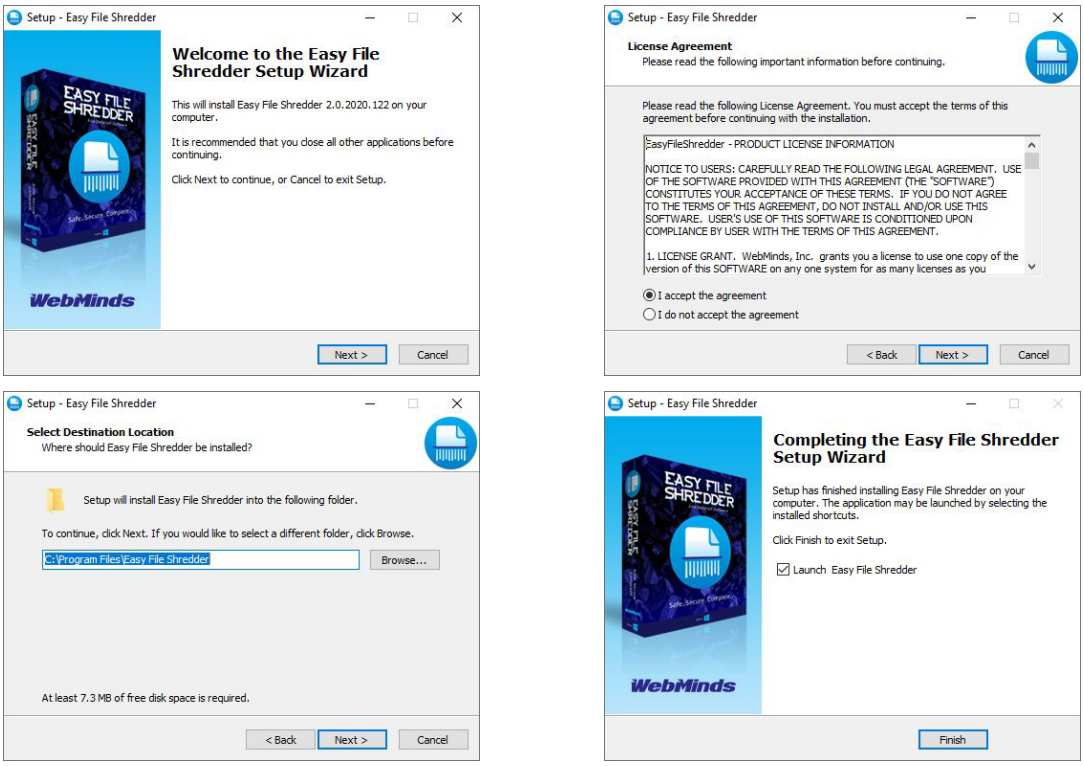
3. Εικόνα δίσκου με 200GB δεδομένων διαγραμμένος ολόκληρος




**Εικόνα 5-66: Εργαλείο 2 - Autopsy - Βήματα εισαγωγής 3ης εικόνας δίσκου**

## 5.2.3 Εργαλείο 3 - Easy File Shredder

Εγκατάσταση εργαλείου

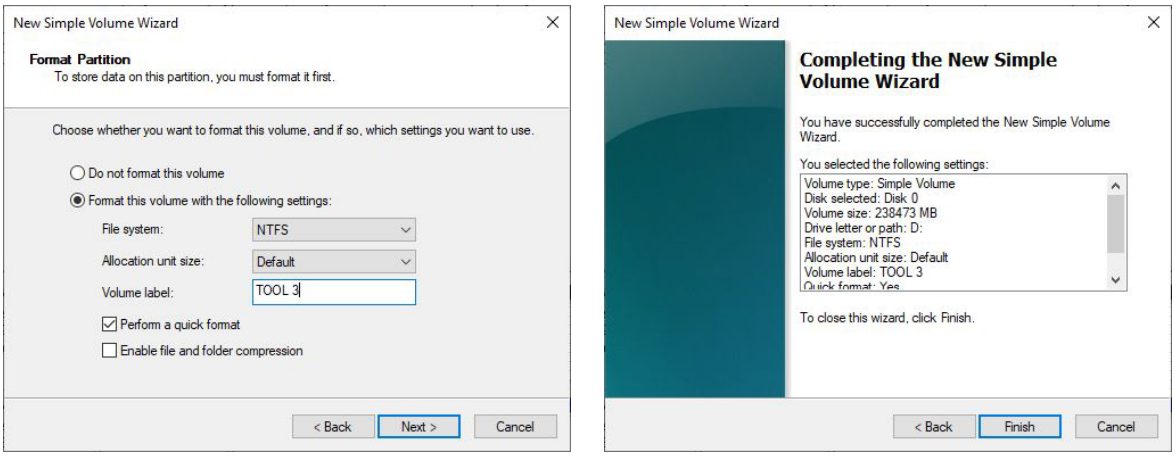



**Εικόνα 5-67: Εργαλείο 3 - Διαδικασία εγκατάστασης Easy File Shredder**

Για σκοπούς αποφυγής επανάληψης, τα βήματα προετοιμασίας του δίσκου για την αξιολόγηση του τρίτου εργαλείου οριστικής διαγραφής δεδομένων δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια κατά την εξέταση του πρώτου εργαλείου.

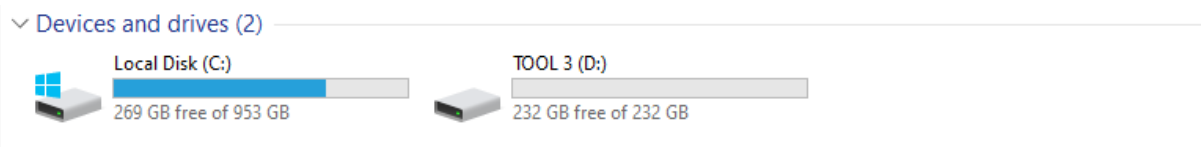
Θα αναφερθούμε μόνο επιγραμματικά στα βήματα.

1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser.
2. Ενεργοποίηση εργαλείου USB Write Blocker.
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.
4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.
5. Αρχικοποίηση MBR, μορφοποίηση του δίσκου σε NTFS Format και ονομασία του δίσκου σε TOOL 3.

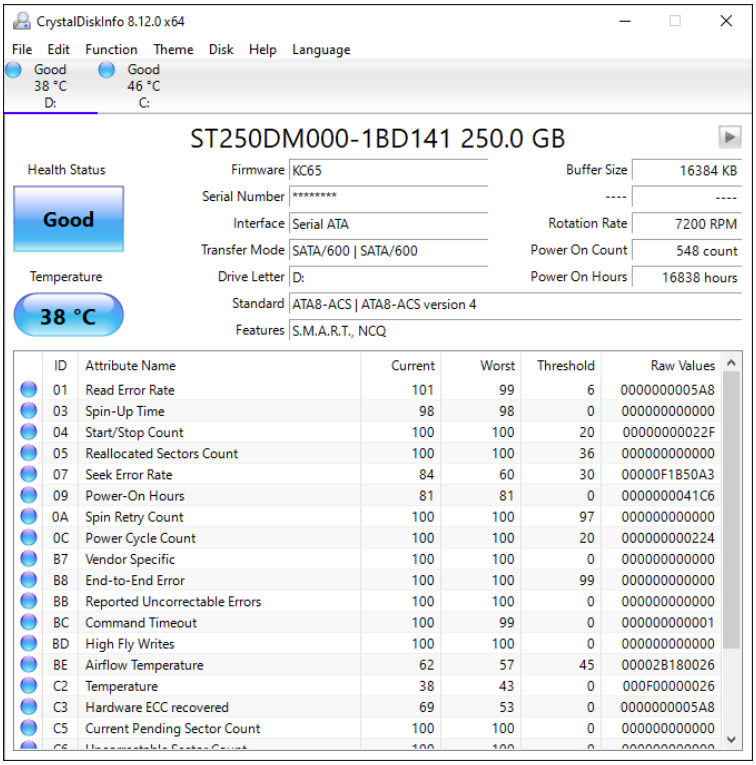



**Εικόνα 5-68: Εργαλείο 3 - Διαδικασία μορφοποίησης δίσκου για αξιολόγηση**

Τα πιο πάνω βήματα αποτελούν τη διαδικασία για τη μορφοποίηση του σκληρού δίσκου ώστε να μπορεί να χρησιμοποιηθεί από το λειτουργικό σύστημα. Μετά το πέρας της διαδικασίας ο δίσκος με την ονομασία TOOL 3 είναι ορατός και μπορεί να χρησιμοποιηθεί κανονικά από τα Windows.



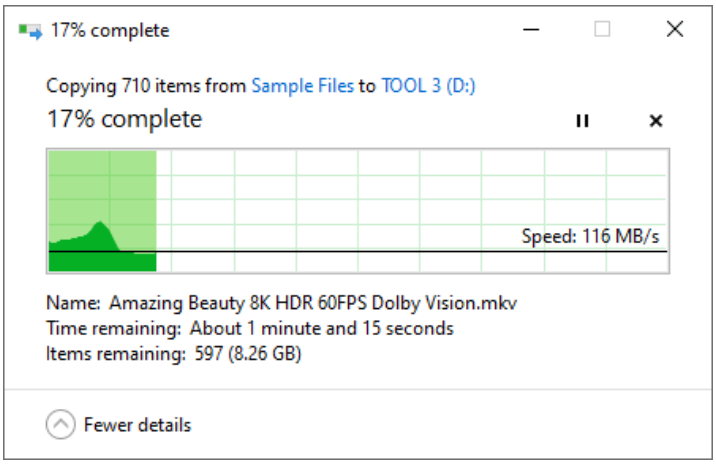
6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.




**Εικόνα 5-69: Εργαλείο 3 - CrystalDiskInfo - Αναφορά κατάστασης δίσκου**

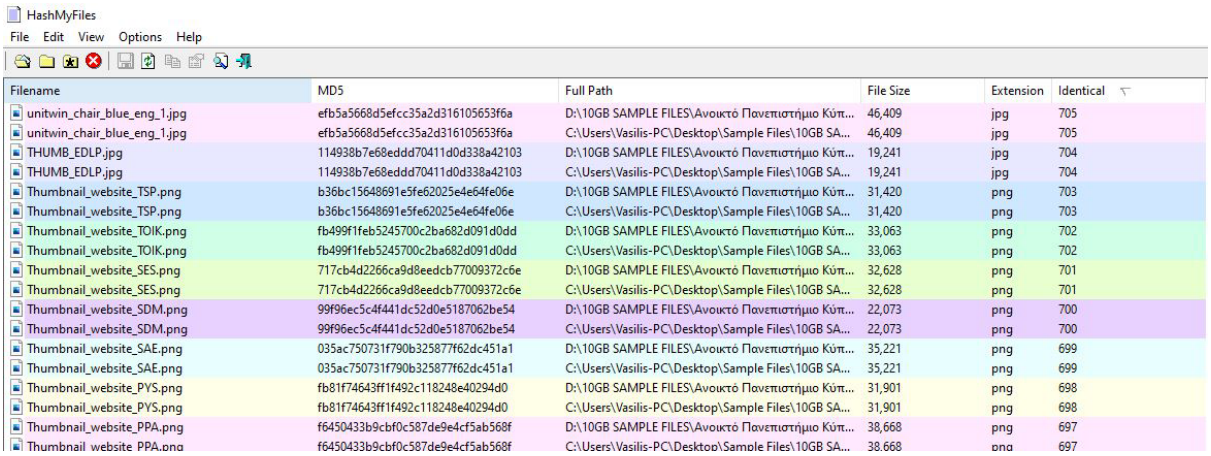
Σύμφωνα με την αναφορά του εργαλείου, ο δίσκος βρίσκεται σε καλή κατάσταση έτσι μπορούμε να αντιγράψουμε σε αυτόν τα αρχικά δεδομένα των 10 GB (705 αρχεία) .

7. Αντιγραφή 10GB στο δίσκο




**Εικόνα 5-70: Εργαλείο 3 - Αντιγραφή 10 GB δεδομένων στο δίσκο**

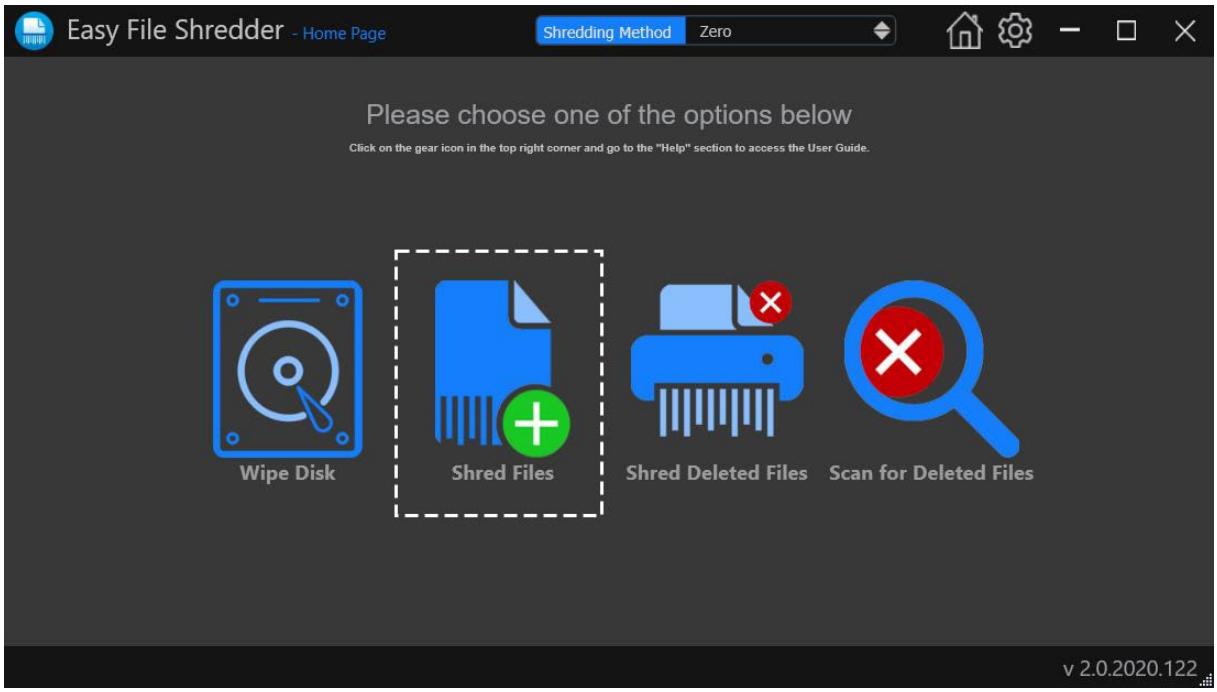
8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.



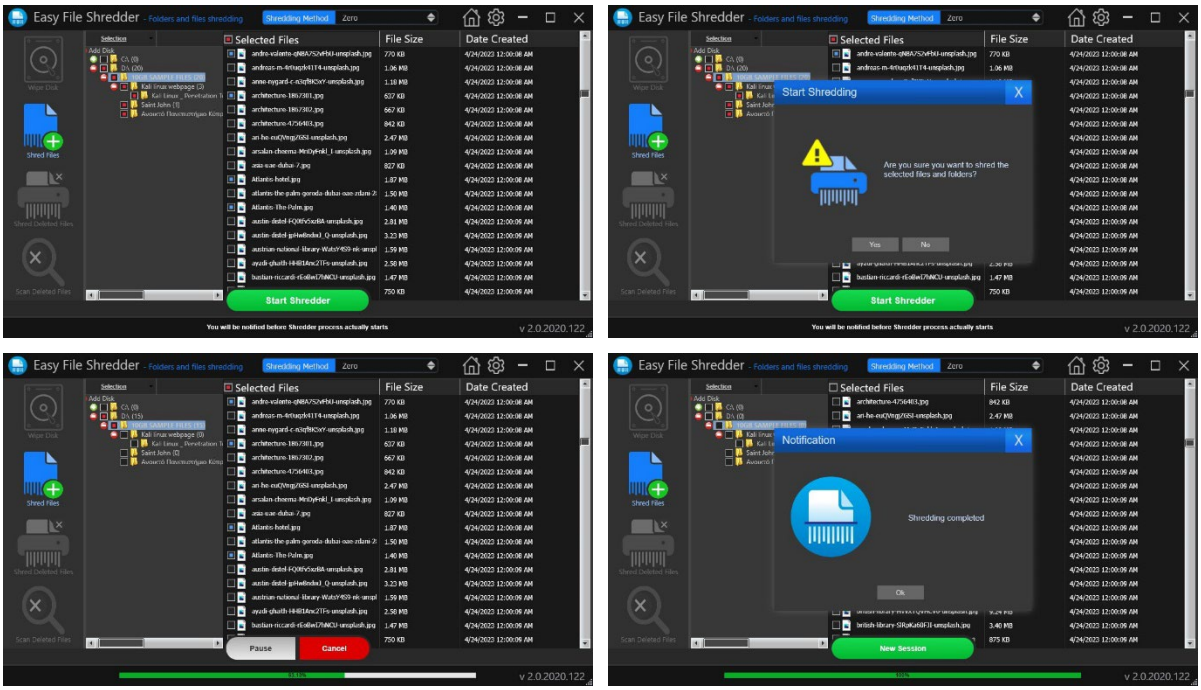

**Εικόνα 5-71: Εργαλείο 3 - HashMyFiles - Σύγκριση αρχείων**

- **<u>Εκτέλεση πρώτου σεναρίου</u> – Διαγραφή 20 συγκεκριμένων αρχείων από το δίσκο**

Από το κεντρικό μενού επιλέγουμε Διαγραφή Αρχείων (Shred Files). Στη συνέχεια επιλέγουμε τα 20 αρχεία που έχουμε καθορίσει από την αρχή για τη διεξαγωγή αυτού του σεναρίου για όλα τα εργαλεία οριστικής διαγραφής δεδομένων. Επίσης καθορίζουμε τη μέθοδο διαγραφής σε Zero. Η μέθοδος αυτή είναι η αντίστοιχη μέθοδος one pass zero κατά την οποία τα δεδομένα του δίσκου εγγράφονται σε μια επανάληψη με μηδενικά. Επιβεβαιώνουμε την πρόθεση μας για οριστική διαγραφή των 20 αρχείων που επιλέξαμε και το εργαλείο ξεκινά την διαγραφή. Στο τέλος της διαδικασίας το εργαλείο ενημερώνει για την επιτυχή διαγραφή των αρχείων.

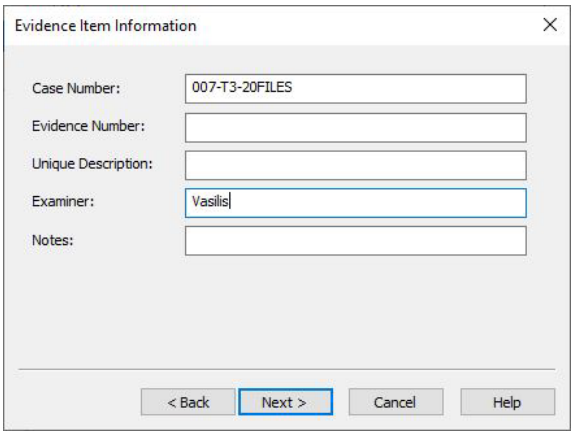


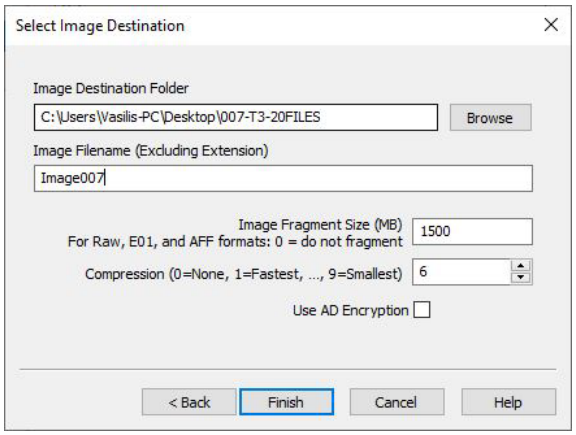

**Εικόνα 5-72: Εργαλείο 3 - Easy File Shredder – Κεντρικό μενού**

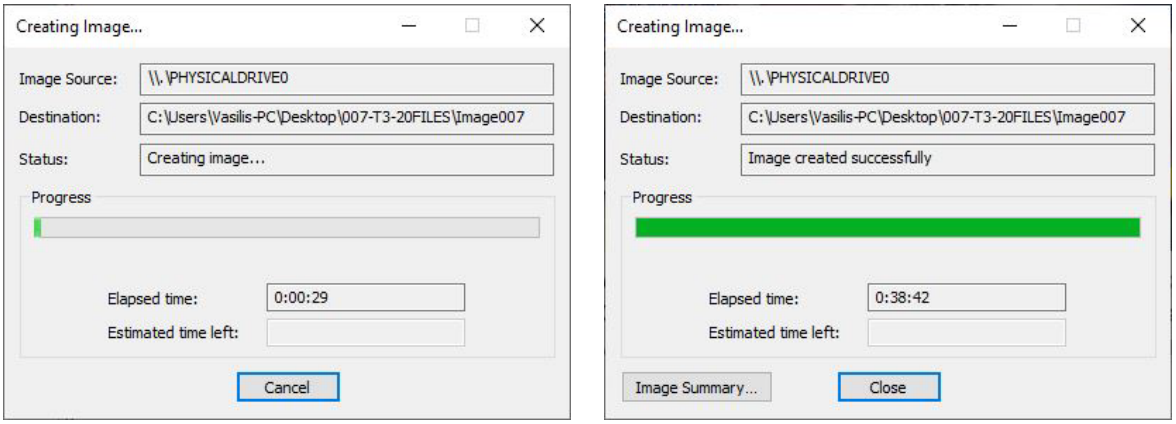



**Εικόνα 5-73: Εργαλείο 3 - Easy File Shredder - Διαδικασία διαγραφής των 20 αρχείων**

Με το πέρας της διαδικασίας διαγραφής των αρχείων προχωρούμε σε εξαγωγή της εικόνας του δίσκου με το εργαλείο AccessData FTK Imager. Με αυτό τον τρόπο θα μπορέσουμε να εισάγουμε την εικόνα στο δικανικό εργαλείο Autopsy και να εντοπίσουμε ίχνη από τα αρχεία που πιθανόν να έχουν μείνει.



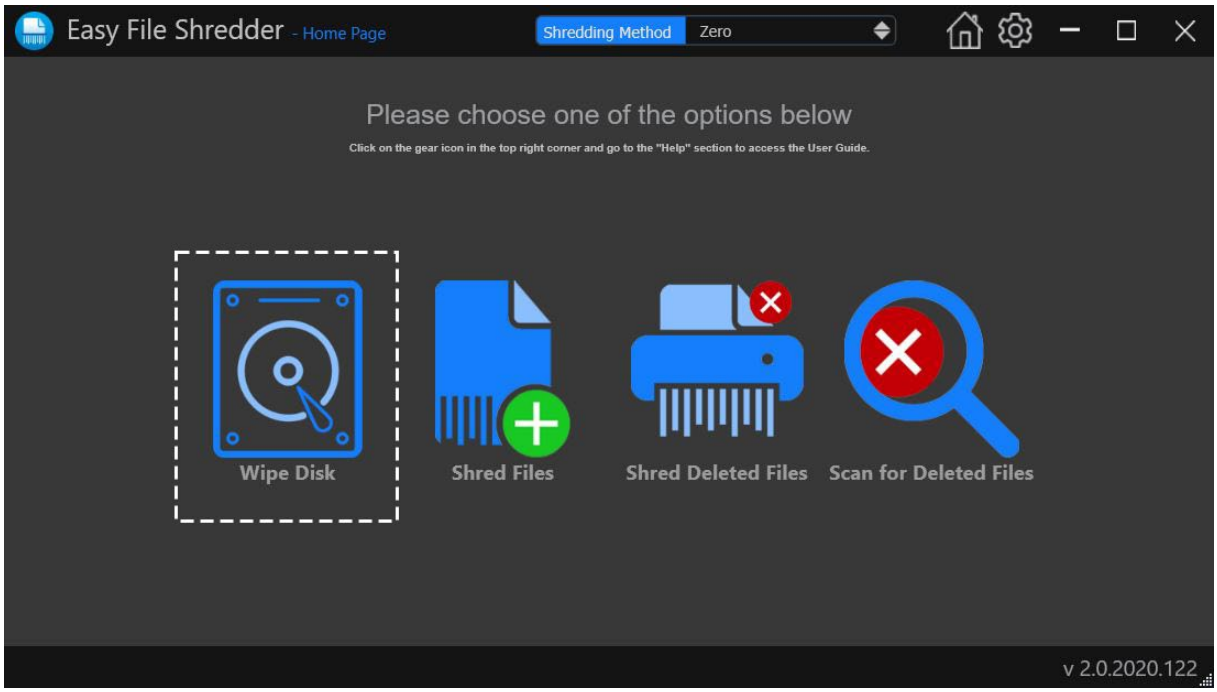



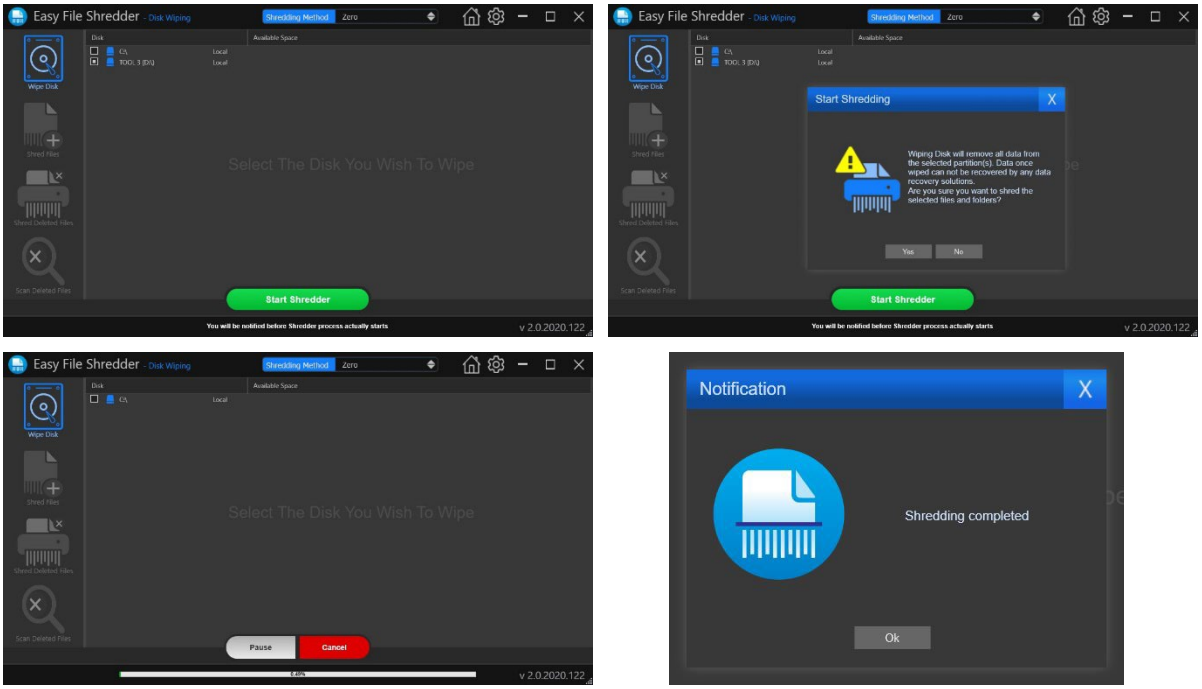



**Εικόνα 5-74: Εργαλείο 3 - AccessData FTK Imager - Διαδικασία δημιουργίας 1ης εικόνας δίσκου μετά την διαγραφή**

- **<u>Εκτέλεση δεύτερου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 10 GB**

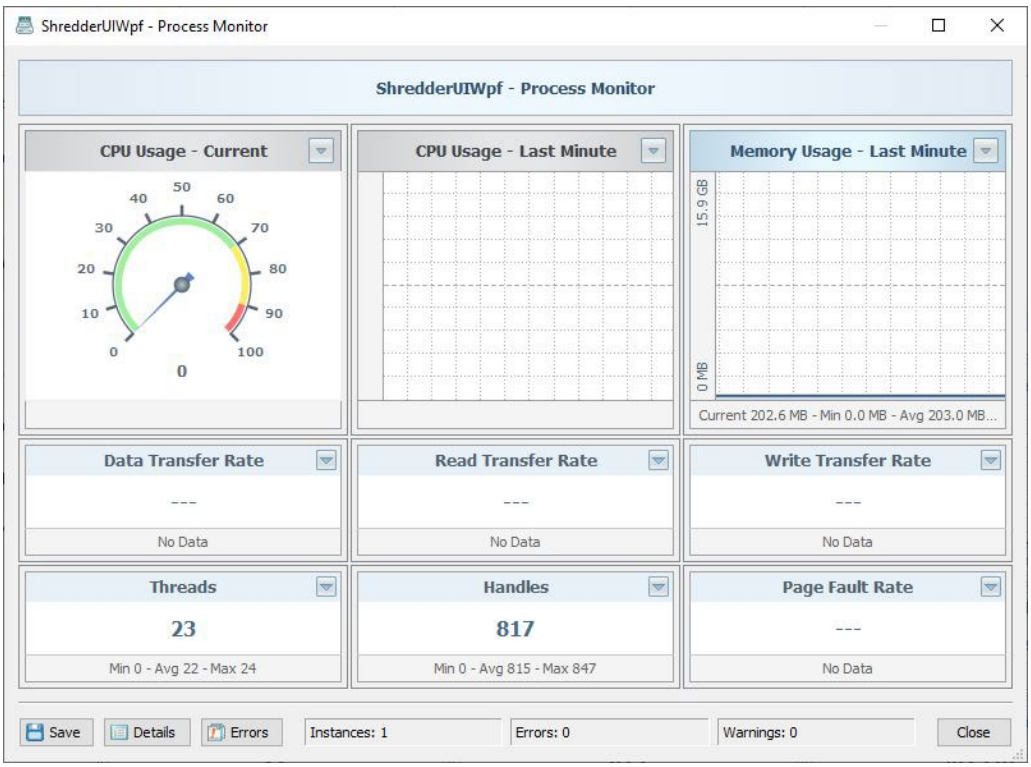
Από το κεντρικό μενού επιλέγουμε τη πρώτη επιλογή, διαγραφή δίσκου (Wipe Disk). Στη λίστα με τους διαθέσιμους δίσκους για διαγραφή, εντοπίζουμε το προς διαγραφή δίσκο και τον επιλέγουμε. Καθορίζουμε την τη μέθοδο διαγραφής σε Zero όπως και στις προηγούμενες περιπτώσεις. Τέλος το εργαλείο μας προτρέπει να επιβεβαιώσουμε την πρόθεση μας για οριστική διαγραφή του δίσκου.





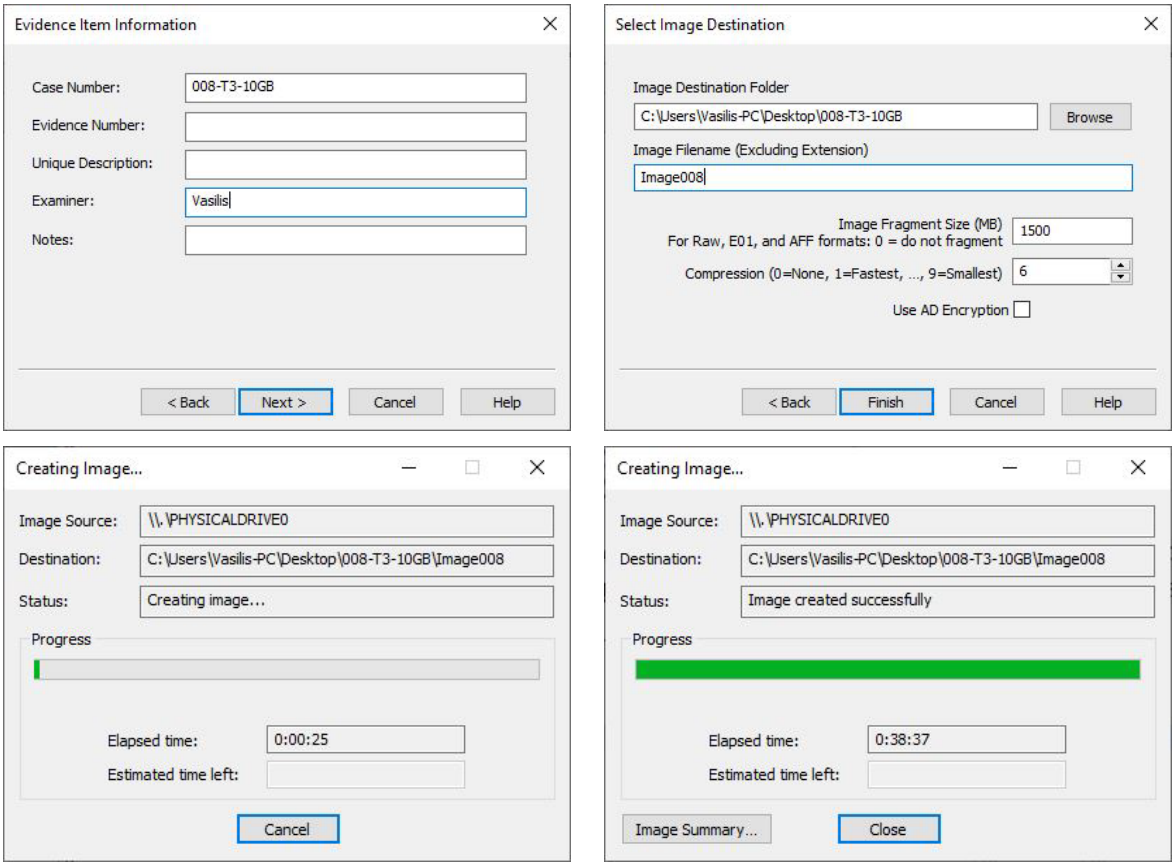

**Εικόνα 5-75: Εργαλείο 3 - Easy File Shredder - Διαδικασία διαγραφής δίσκου – Αρχεία 10GB**

Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.




**Εικόνα 5-76: Εργαλείο 3 - SysGauge - Καταγραφή πόρων συστήματος κατά την διαγραφή ολόκληρου του δίσκου - 10GB**

Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 10 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για δεύτερη φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που ακολουθήσαμε και στην πιο πάνω περίπτωση με διαφορά την ονομασία της εικόνας του δίσκου ώστε να υπάρχει αρχειοθέτηση και καταγραφή των σεναρίων .



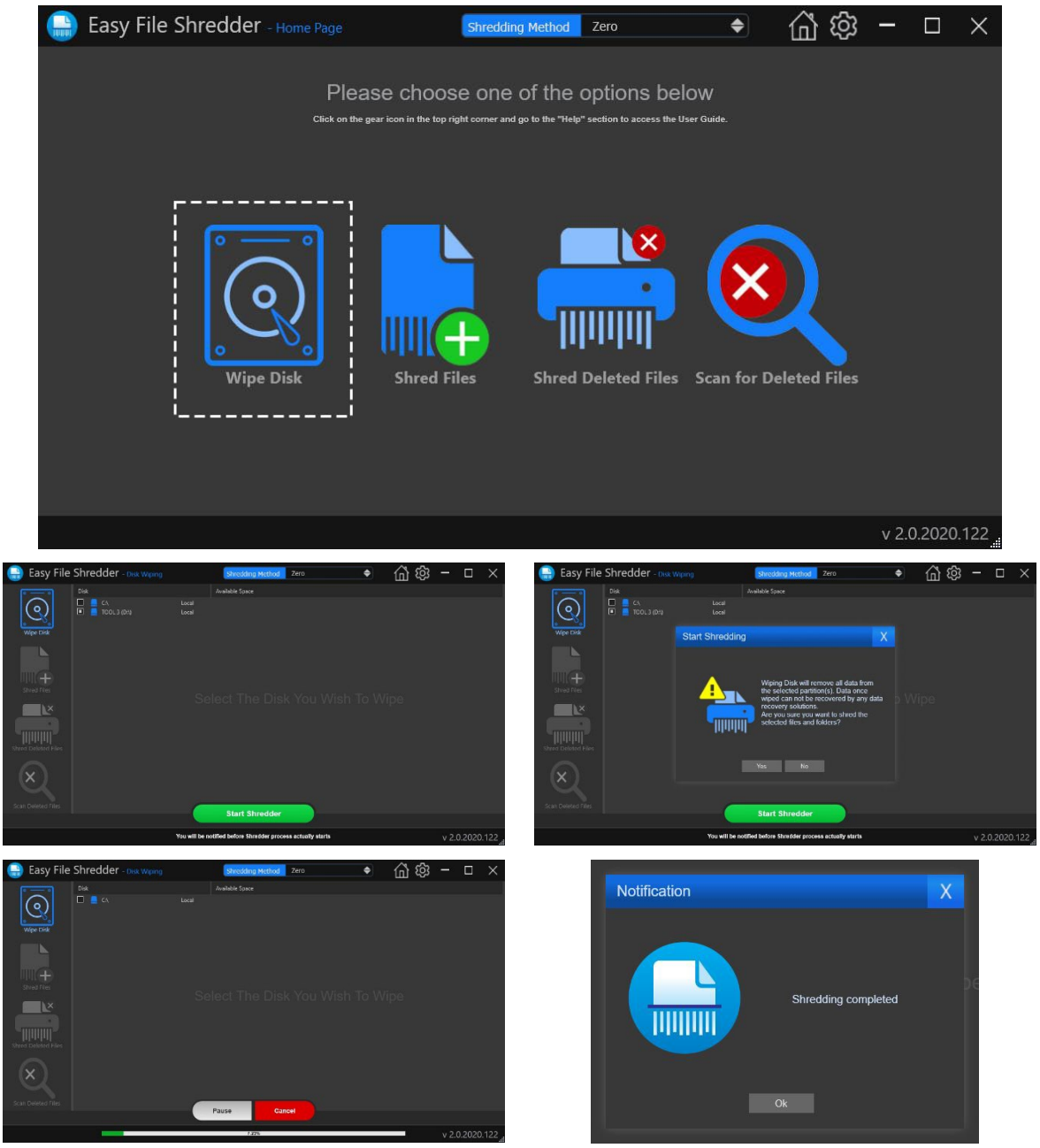

**Εικόνα 5-77: Εργαλείο 3 - AccessData FTK Imager - Διαδικασία δημιουργίας 2ης εικόνας δίσκου μετά την διαγραφή**

- **<u>Εκτέλεση τρίτου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 200 GB**

Για σκοπούς αποφυγής επανάληψης τα βήματα αρχικοποίησης και μορφοποίησης του δίσκου για το τρίτο σενάριο, αυτό της διαγραφής ολόκληρου του δίσκου με τα 200GB δεδομένων σε αυτόν, δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια πιο πάνω. Θα αναφερθούμε μόνο επιγραμματικά ως βήματα.

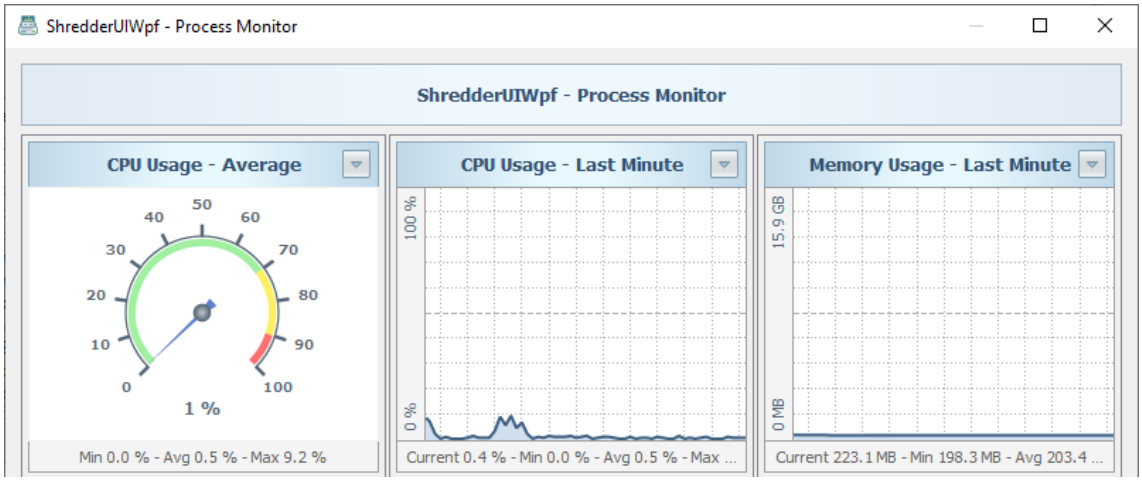
1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser .
2. Ενεργοποίηση εργαλείου USB Write Blocker
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.

4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.
5. Αρχικοποίηση MBR και μορφοποίηση του δίσκου σε NTFS Format.
6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.
7. Αντιγραφή 200GB στο δίσκο για διαγραφή.
8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.
9. Έναρξη διαδικασίας διαγραφής ολόκληρου του δίσκου με το εργαλείο οριστικής διαγραφής .



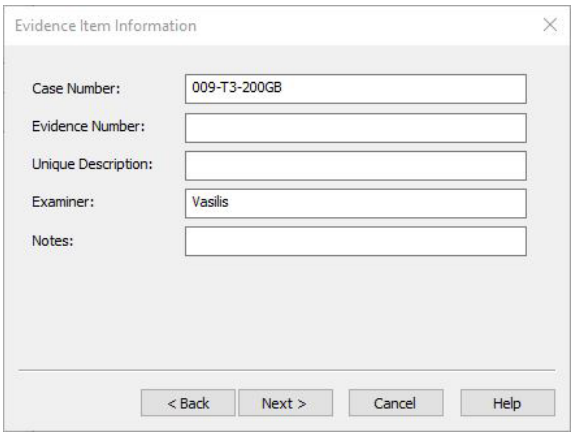

**Εικόνα 5-78: Εργαλείο 3 - Easy File Shredder - Διαδικασία διαγραφής δίσκου – Αρχεία 200GB**

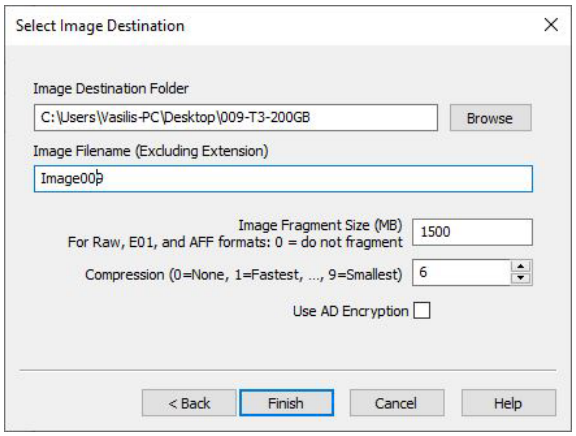
Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο

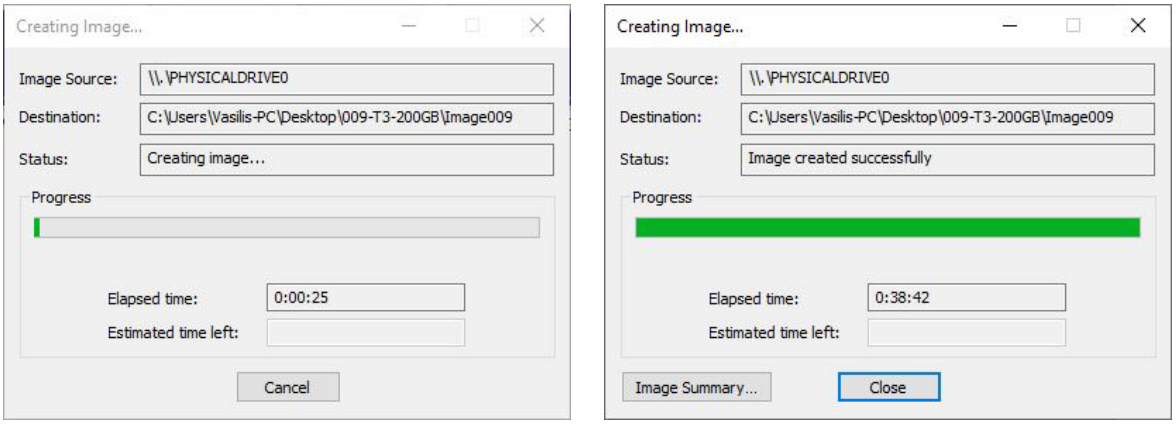



**Εικόνα 5-79: Εργαλείο 3 - SysGauge - Καταγραφή πόρων συστήματος κατά την διαγραφή ολόκληρου του δίσκου - 200GB**

Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 200 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για τρίτη φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που ακολουθήσαμε και στην πιο πάνω περίπτωση με διαφορά την ονομασία της εικόνας του δίσκου ώστε να υπάρχει αρχειοθέτηση και καταγραφή των σεναρίων .



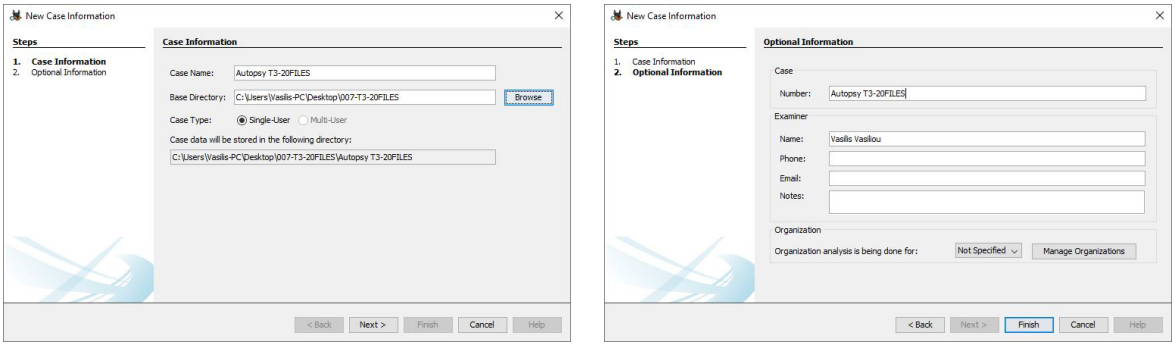






**Εικόνα 5-80: Εργαλείο 3 - AccessData FTK Imager - Διαδικασία δημιουργίας 3ης εικόνας δίσκου μετά την διαγραφή**

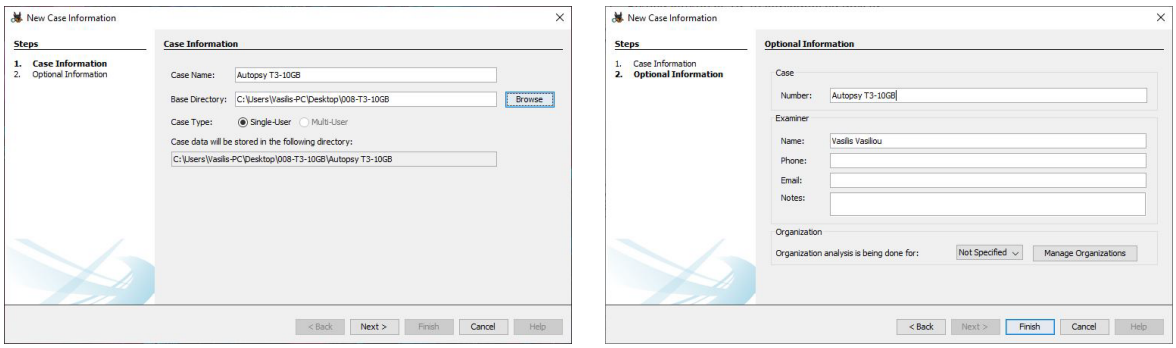
Εισαγωγή εικόνων δίσκων στο Autopsy

1. Εικόνα δίσκου με τα 20 διαγραμμένα αρχεία



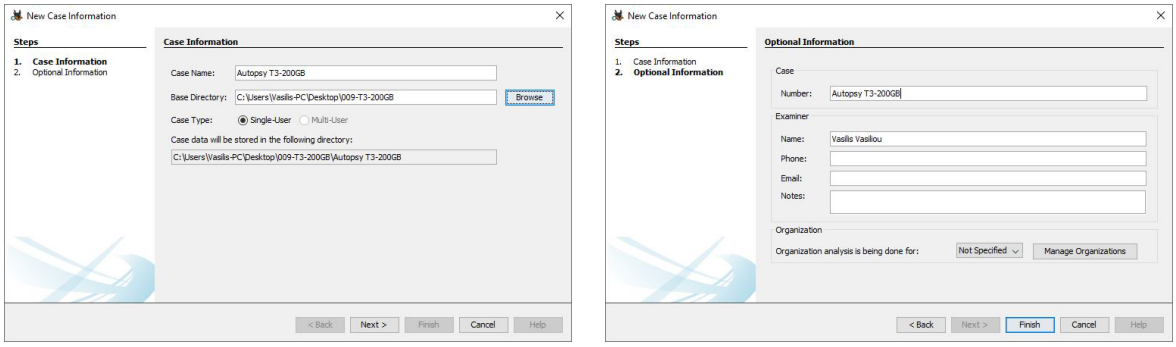

**Εικόνα 5-81: Εργαλείο 3 - Autopsy - Βήματα εισαγωγής 1ης εικόνας δίσκου**

2. Εικόνα δίσκου με 10GB δεδομένων διαγραμμένος ολόκληρος




**Εικόνα 5-82: Εργαλείο 3 - Autopsy - Βήματα εισαγωγής 2ης εικόνας δίσκου**

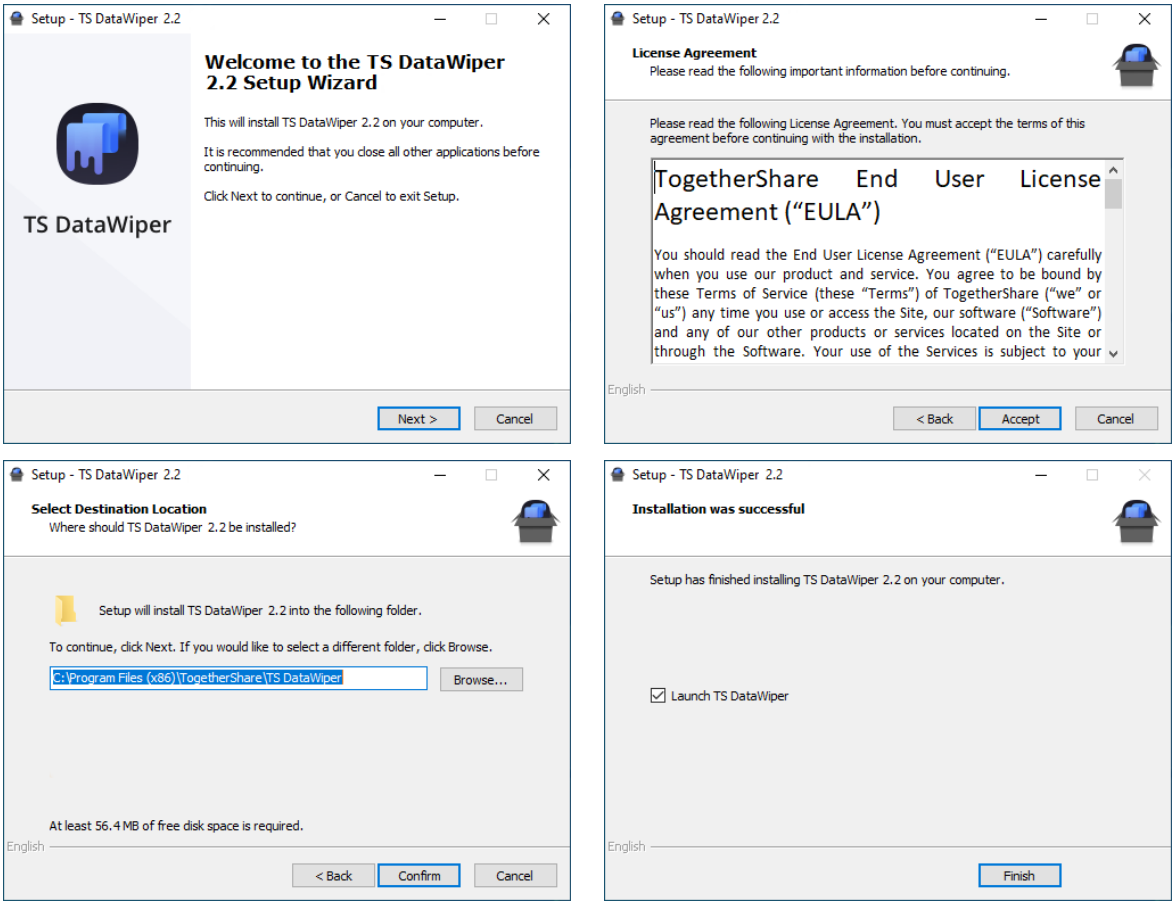
3. Εικόνα δίσκου με 200GB δεδομένων διαγραμμένος ολόκληρος




**Εικόνα 5-83: Εργαλείο 3 - Autopsy - Βήματα εισαγωγής 3ης εικόνας δίσκου**

## 5.2.4 Εργαλείο 4 - TS DataWiper

Εγκατάσταση εργαλείου

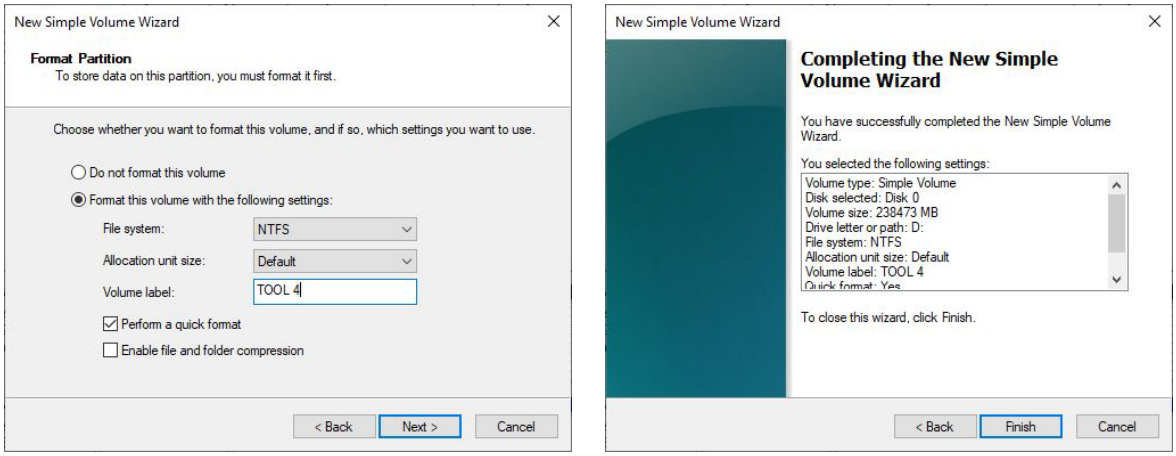



**Εικόνα 5-84: Εργαλείο 4 - Διαδικασία εγκατάστασης TS DataWiper**

Για σκοπούς αποφυγής επανάληψης, τα βήματα προετοιμασίας του δίσκου για την αξιολόγηση του τέταρτου εργαλείου οριστικής διαγραφής δεδομένων δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια κατά την εξέταση του πρώτου εργαλείου.

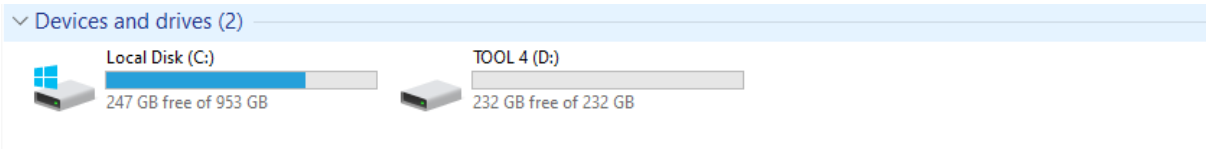
Θα αναφερθούμε μόνο επιγραμματικά στα βήματα.

1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser.
2. Ενεργοποίηση εργαλείου USB Write Blocker.
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.
4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.
5. Αρχικοποίηση MBR, μορφοποίηση του δίσκου σε NTFS Format και ονομασία του δίσκου σε TOOL 4.

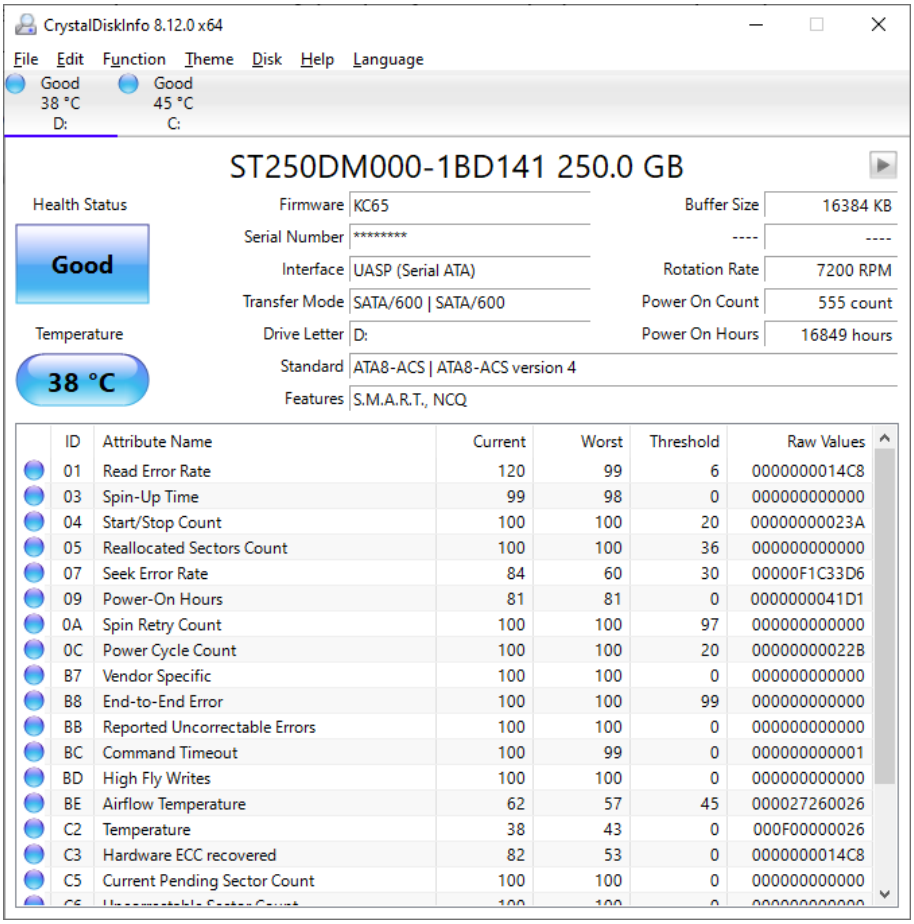



**Εικόνα 5-85: Εργαλείο 4 - Διαδικασία μορφοποίησης δίσκου για αξιολόγηση**

Τα πιο πάνω βήματα αποτελούν τη διαδικασία για τη μορφοποίηση του σκληρού δίσκου ώστε να μπορεί να χρησιμοποιηθεί από το λειτουργικό σύστημα. Μετά το πέρας της διαδικασίας ο δίσκος με την ονομασία TOOL 4 είναι ορατός και μπορεί να χρησιμοποιηθεί κανονικά από τα windows.



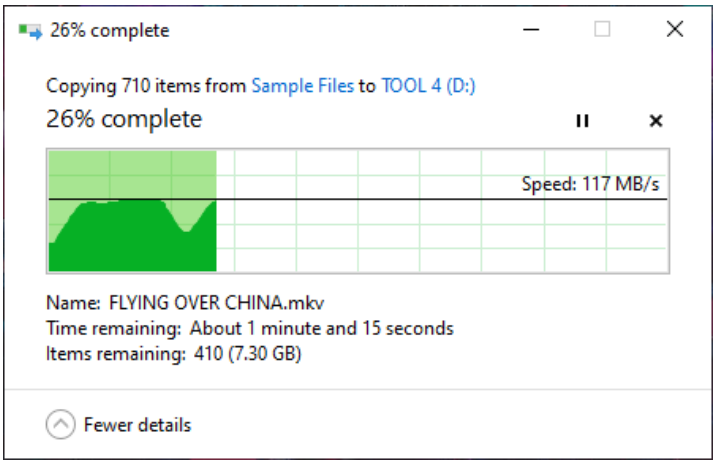
6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.




**Εικόνα 5-86: Εργαλείο 4 - CrystalDiskInfo - Αναφορά κατάστασης δίσκου**

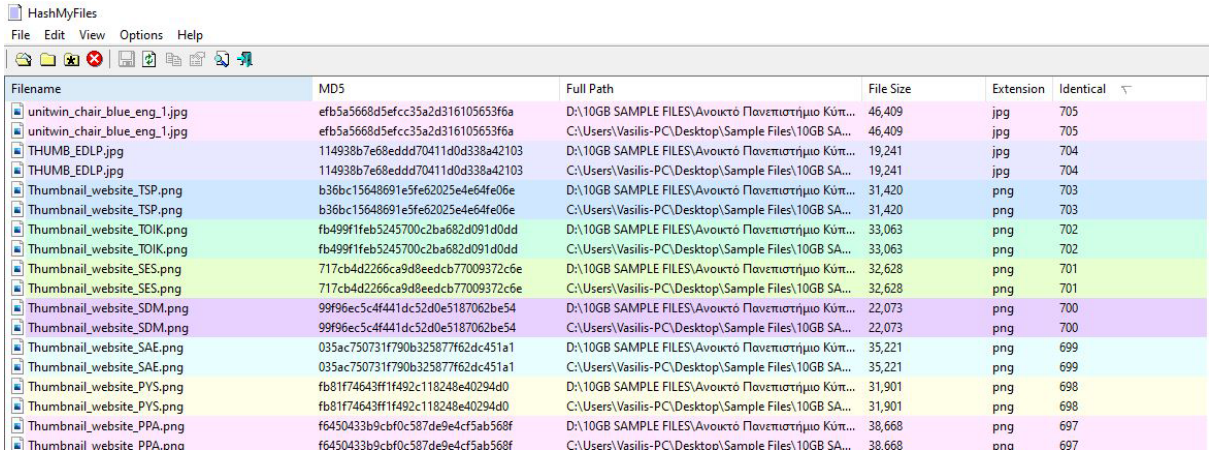
Σύμφωνα με την αναφορά του εργαλείου, ο δίσκος βρίσκεται σε καλή κατάσταση έτσι μπορούμε να αντιγράψουμε σε αυτόν τα αρχικά δεδομένα των 10 GB (705 αρχεία) .

7. Αντιγραφή 10GB στο δίσκο




**Εικόνα 5-87: Εργαλείο 4 - Αντιγραφή 10 GB δεδομένων στο δίσκο**

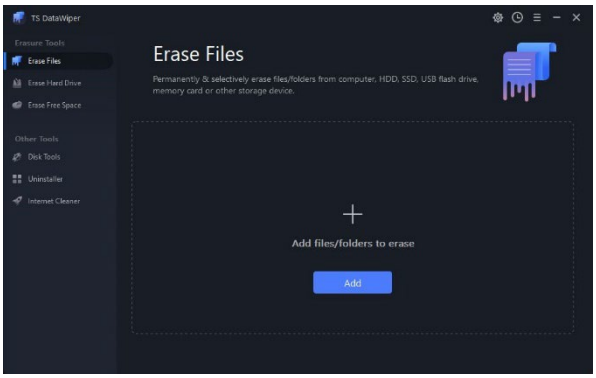
8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.

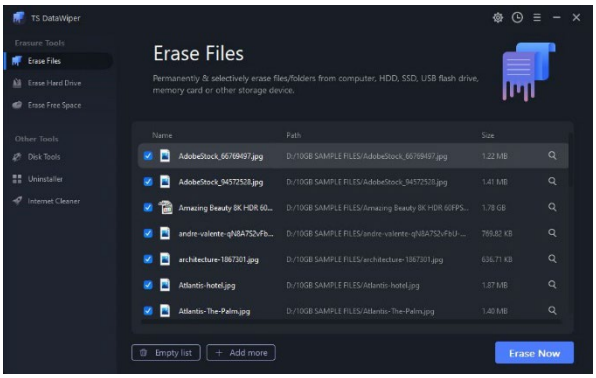


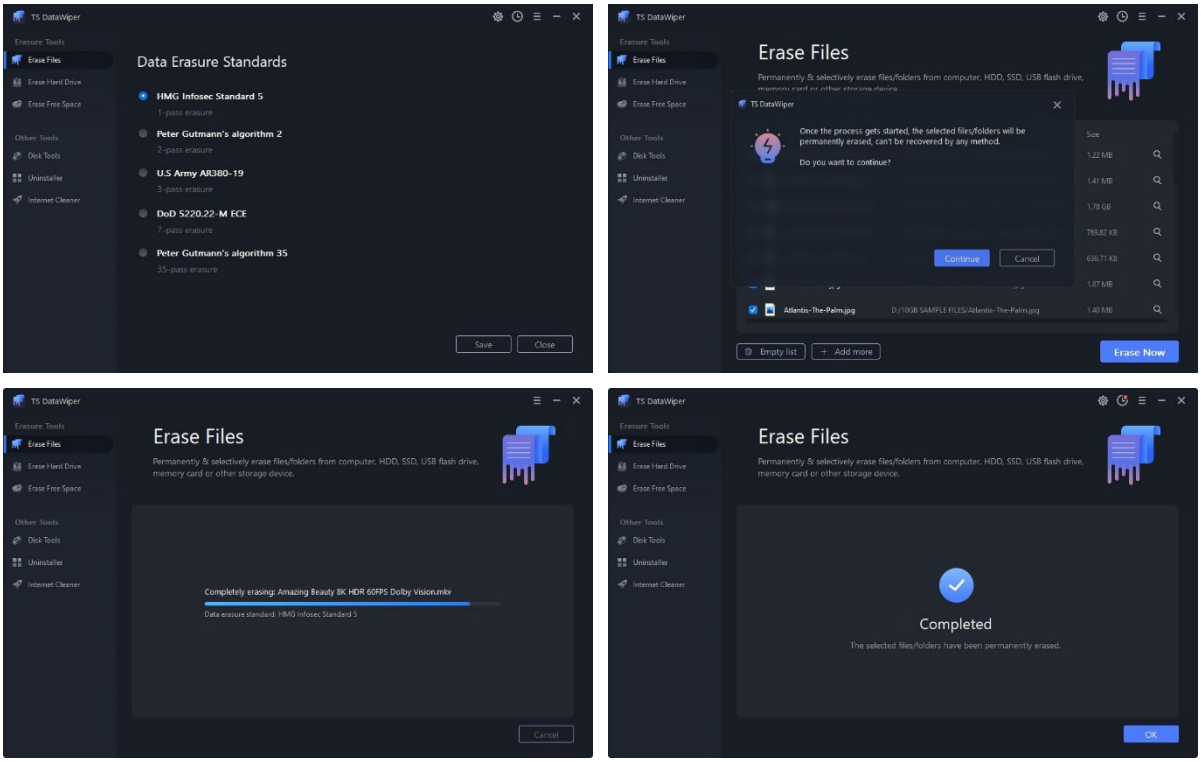

**Εικόνα 5-88: Εργαλείο 4 - HashMyFiles - Σύγκριση αρχείων**

- **<u>Εκτέλεση πρώτου σεναρίου</u> – Διαγραφή 20 συγκεκριμένων αρχείων από το δίσκο**

Από το κεντρικό μενού επιλέγουμε Διαγραφή Αρχείων (Erase Files). Στη συνέχεια επιλέγουμε τα 20 αρχεία που έχουμε καθορίσει από την αρχή για τη διεξαγωγή αυτού του σεναρίου για όλα τα εργαλεία οριστικής διαγραφής δεδομένων. Επίσης καθορίζουμε τη μέθοδο διαγραφής σε HMG Infosec Standard 5. Η μέθοδος αυτή είναι η αντίστοιχη μέθοδος one pass zero κατά την οποία τα δεδομένα του δίσκου εγγράφονται σε μια επανάληψη με μηδενικά. Επιβεβαιώνουμε την πρόθεση μας για οριστική διαγραφή των 20 αρχείων που επιλέξαμε και το εργαλείο ξεκινά την διαγραφή. Στο τέλος της διαδικασίας το εργαλείο ενημερώνει για την επιτυχή διαγραφή των αρχείων.

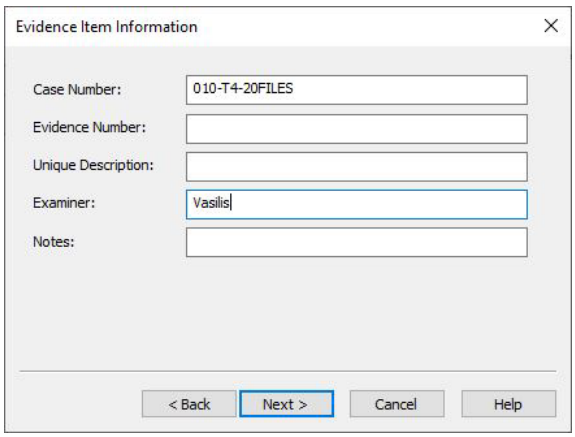


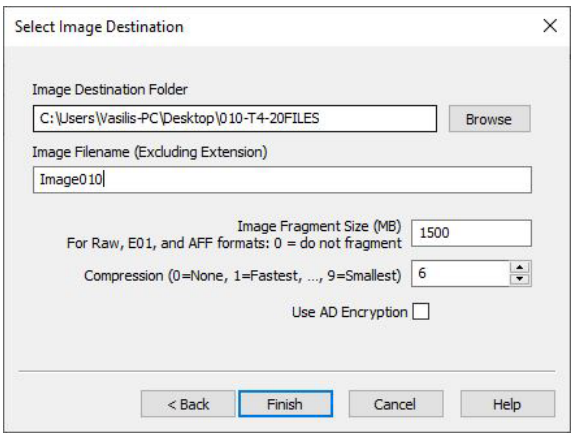



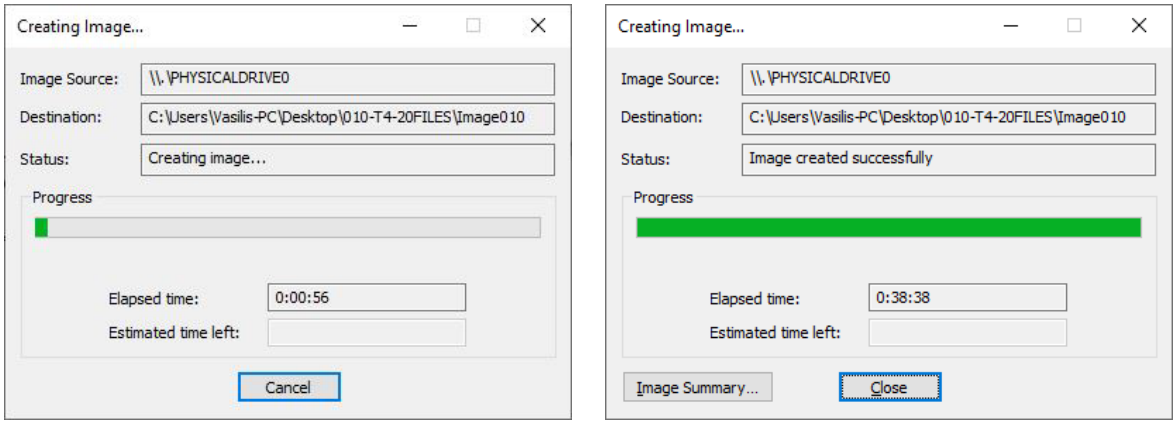



**Εικόνα 5-89: Εργαλείο 4 - TS DataWiper - Διαδικασία διαγραφής των 20 αρχείων**

Με το πέρας της διαδικασίας διαγραφής των αρχείων προχωρούμε σε εξαγωγή της εικόνας του δίσκου με το εργαλείο AccessData FTK Imager. Με αυτό τον τρόπο θα μπορέσουμε να εισάγουμε την εικόνα στο δικανικό εργαλείο Autopsy και να εντοπίσουμε ίχνη από τα αρχεία που πιθανόν να έχουν μείνει.



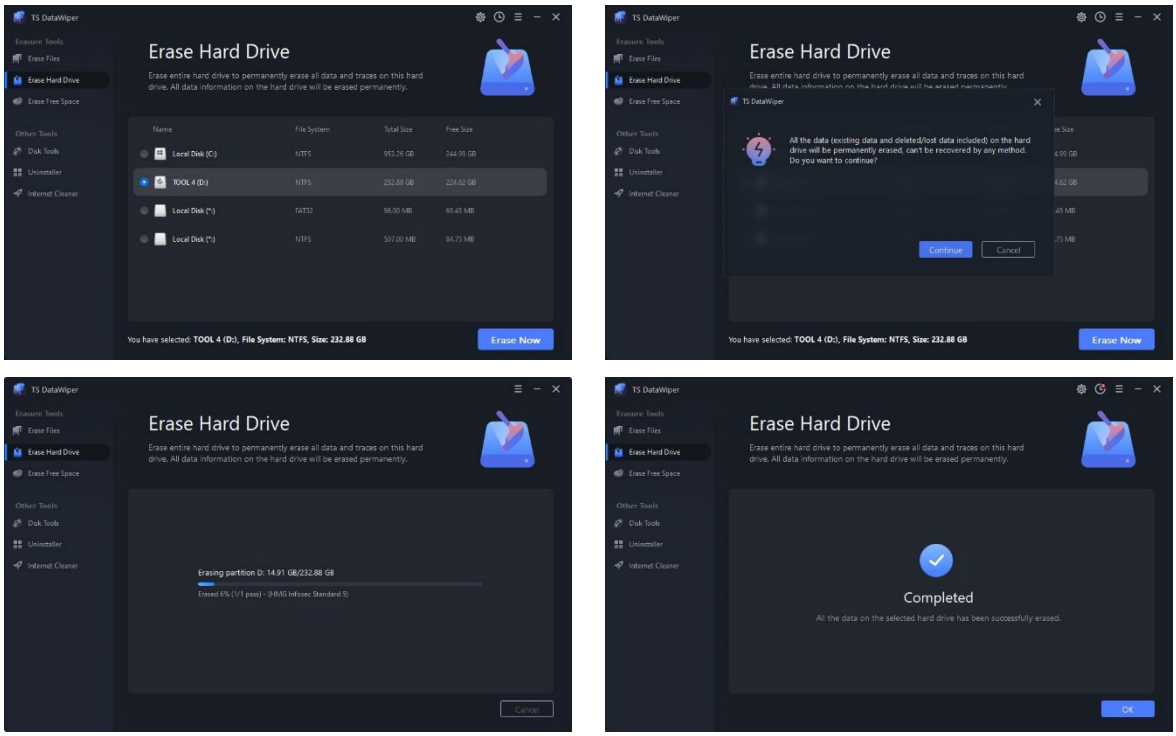






**Εικόνα 5-90: Εργαλείο 4 - AccessData FTK Imager - Διαδικασία δημιουργίας 1ης εικόνας δίσκου μετά την διαγραφή**

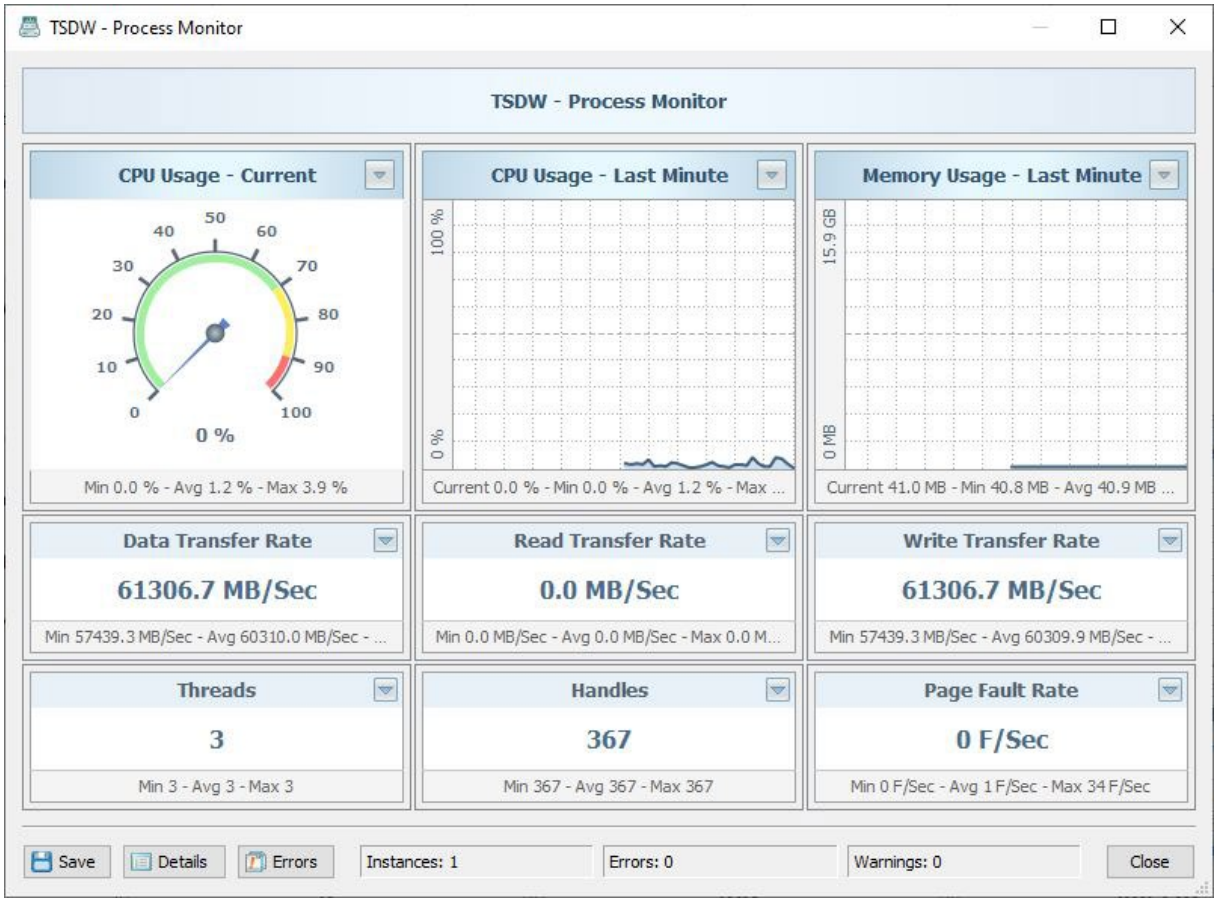
- **<u>Εκτέλεση δεύτερου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 10 GB**

Από το κεντρικό μενού επιλέγουμε τη δεύτερη επιλογή, διαγραφή σκληρού δίσκου (Erase Hard Drive). Στη λίστα με τους διαθέσιμους δίσκους για διαγραφή, εντοπίζουμε το προς διαγραφή δίσκο και τον επιλέγουμε. Τέλος το εργαλείο μας προτρέπει να επιβεβαιώσουμε την πρόθεση μας για οριστική διαγραφή του δίσκου.



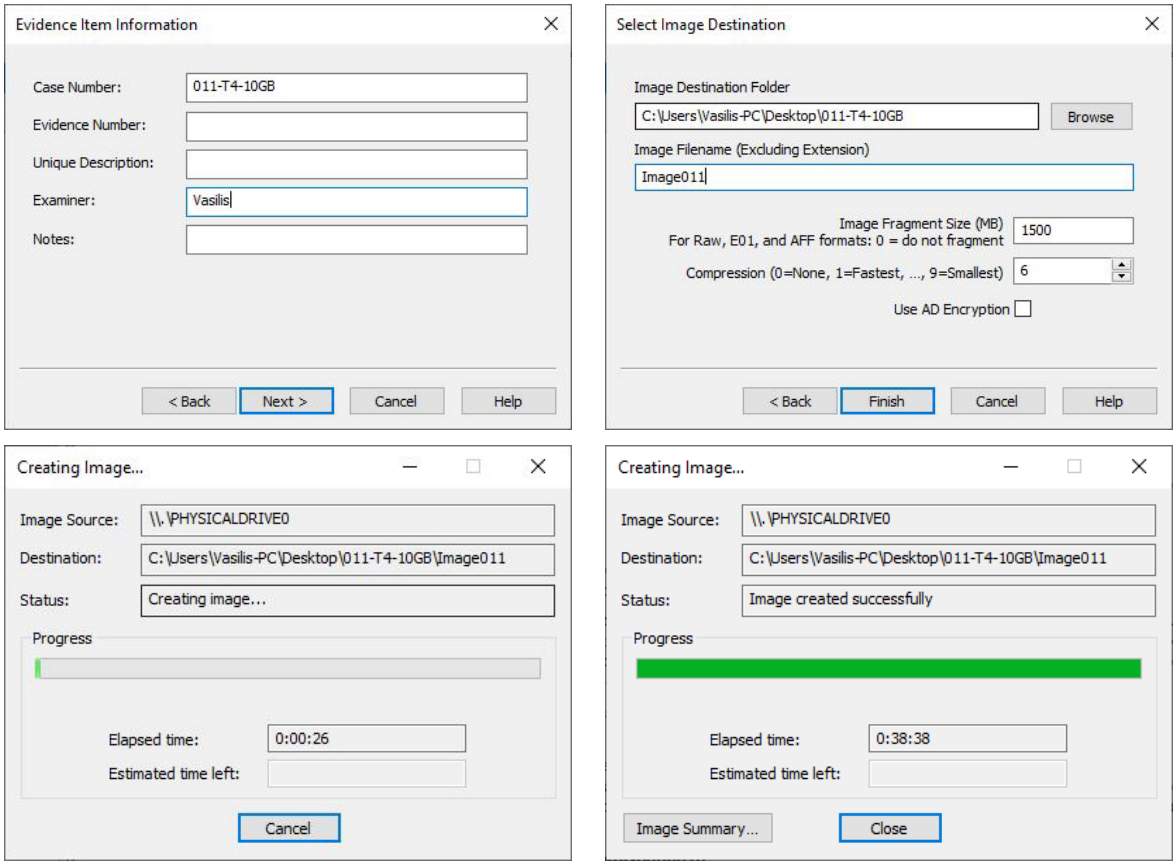

**Εικόνα 5-91: Εργαλείο 4 - TS DataWiper - Διαδικασία διαγραφής δίσκου – Αρχεία 10GB**

Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.




**Εικόνα 5-92: Εργαλείο 4 - SysGauge - Καταγραφή πόρων συστήματος κατά την διαγραφή ολόκληρου του δίσκου - 10GB**

Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 10 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για δεύτερη φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που ακολουθήσαμε και στην πιο πάνω περίπτωση με διαφορά την ονομασία της εικόνας του δίσκου ώστε να υπάρχει αρχειοθέτηση και καταγραφή των σεναρίων .



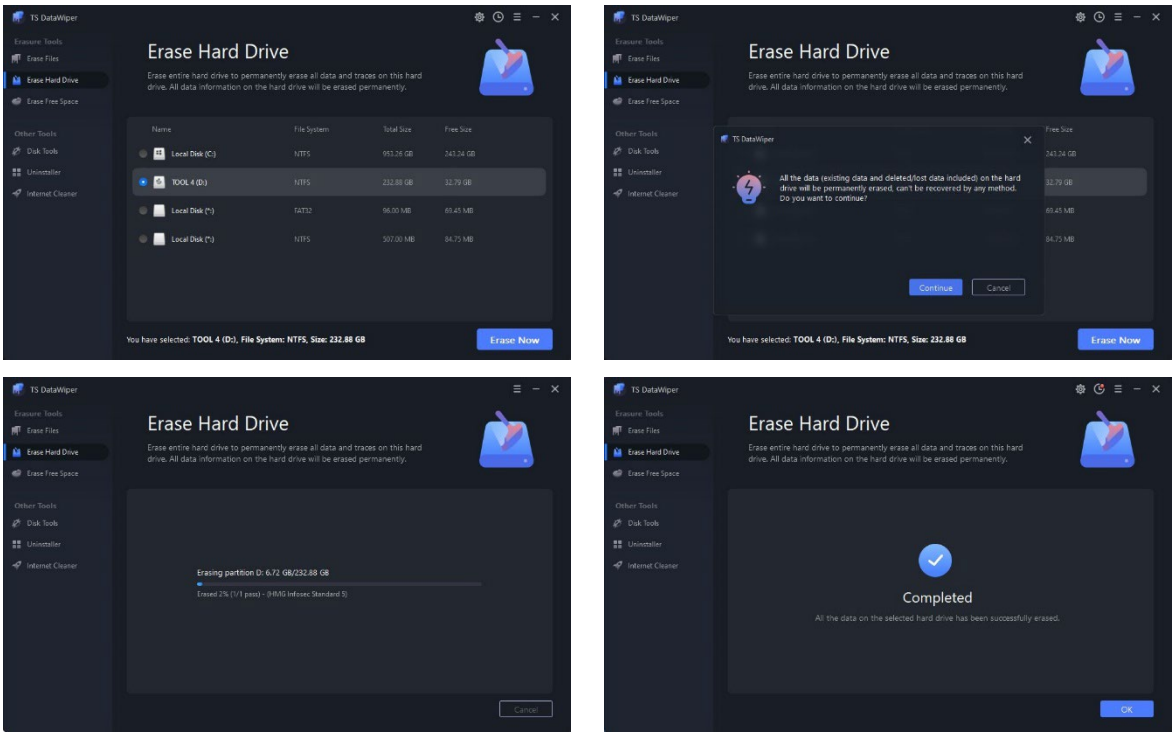

**Εικόνα 5-93: Εργαλείο 4 - AccessData FTK Imager - Διαδικασία δημιουργίας 2ης εικόνας δίσκου μετά την διαγραφή**

- **<u>Εκτέλεση τρίτου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 200 GB**

Για σκοπούς αποφυγής επανάληψης τα βήματα αρχικοποίησης και μορφοποίησης του δίσκου για το τρίτο σενάριο, αυτό της διαγραφής ολόκληρου του δίσκου με τα 200GB δεδομένων σε αυτόν, δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια πιο πάνω. Θα αναφερθούμε μόνο επιγραμματικά ως βήματα.

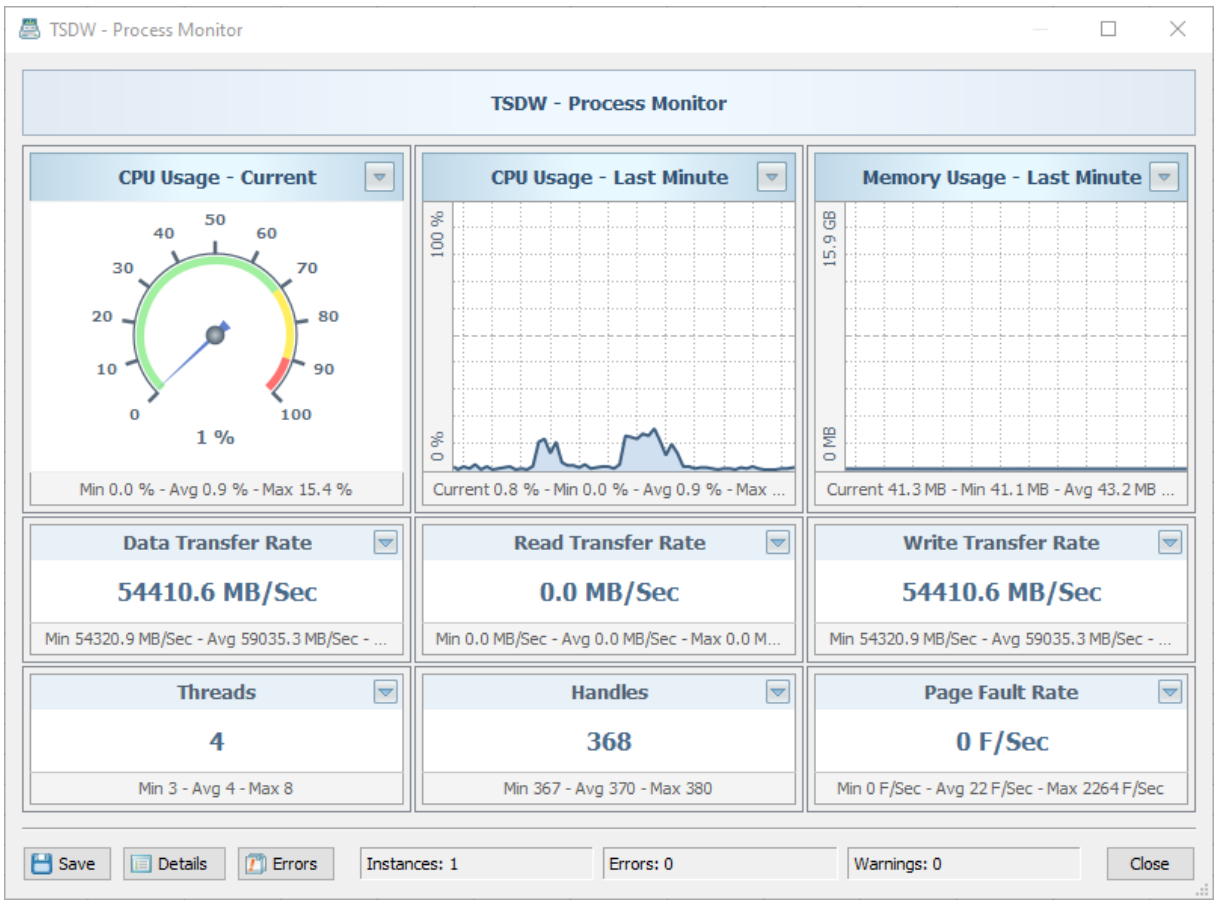
1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser.
2. Ενεργοποίηση εργαλείου USB Write Blocker
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.
4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.
5. Αρχικοποίηση MBR και μορφοποίηση του δίσκου σε NTFS Format.
6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.
7. Αντιγραφή 200GB στο δίσκο για διαγραφή.

8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.
9. Έναρξη διαδικασίας διαγραφής ολόκληρου του δίσκου με το εργαλείο οριστικής διαγραφής.



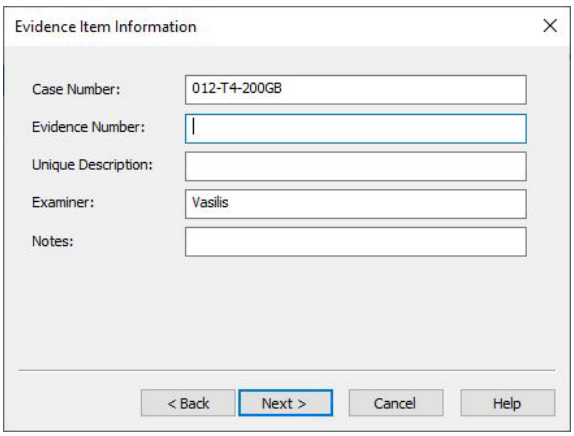

**Εικόνα 5-94: Εργαλείο 4 - TS DataWiper - Διαδικασία διαγραφής δίσκου – Αρχεία 200GB**

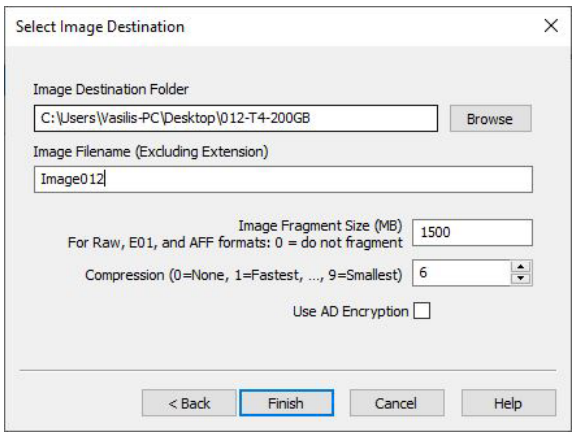
Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.

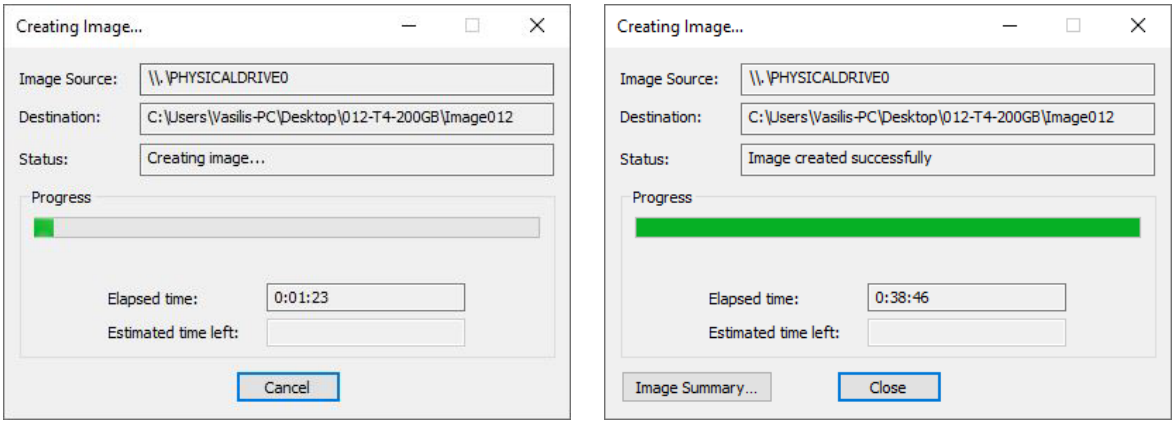



**Εικόνα 5-95: Εργαλείο 4 - SysGauge - Καταγραφή πόρων συστήματος κατά την διαγραφή ολόκληρου του δίσκου - 200GB**

Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 200 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για τρίτη φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που ακολουθήσαμε και στην πιο πάνω περίπτωση με διαφορά την ονομασία της εικόνας του δίσκου ώστε να υπάρχει αρχειοθέτηση και καταγραφή των σεναρίων .



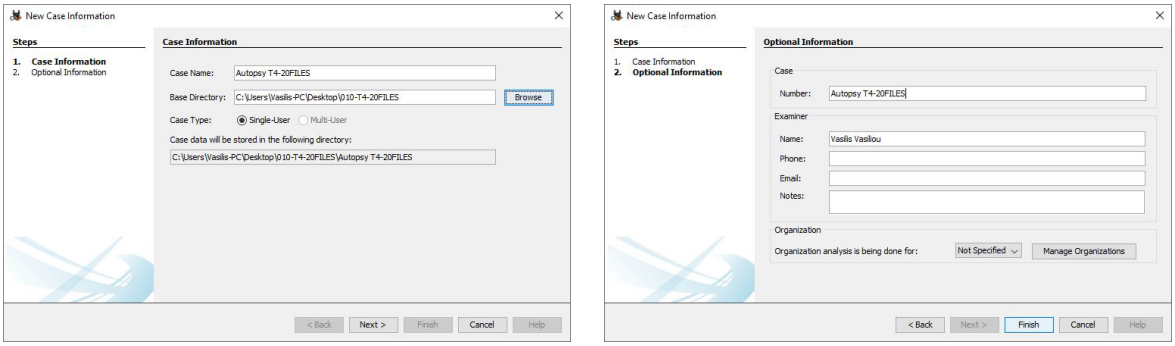






**Εικόνα 5-96: Εργαλείο 4 - AccessData FTK Imager - Διαδικασία δημιουργίας 3ης εικόνας δίσκου μετά την διαγραφή**

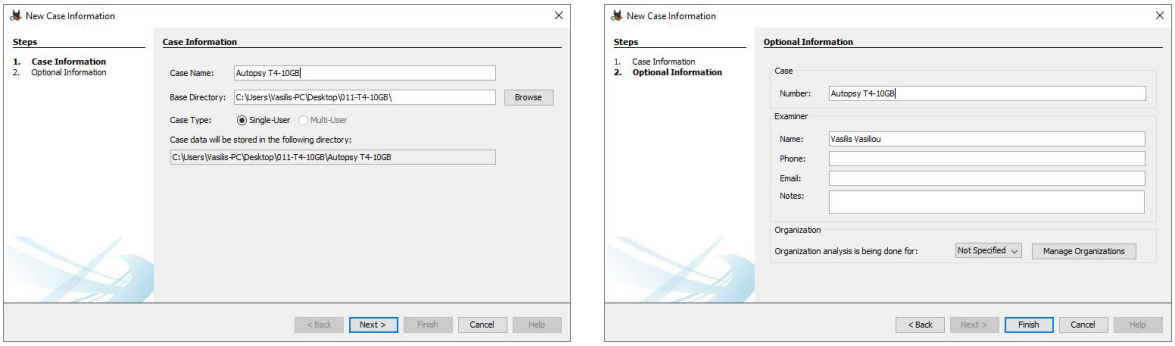
Εισαγωγή εικόνων δίσκων στο Autopsy

1. Εικόνα δίσκου με τα 20 διαγραμμένα αρχεία



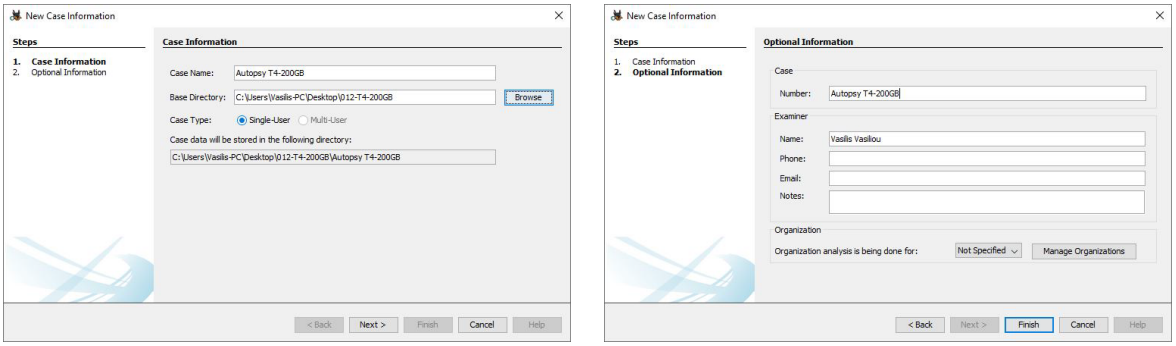

**Εικόνα 5-97: Εργαλείο 4 - Autopsy - Διαδικασία εισαγωγής 1ης εικόνας δίσκου**

2. Εικόνα δίσκου με 10GB δεδομένων διαγραμμένος ολόκληρος




**Εικόνα 5-98: Εργαλείο 4 - Autopsy - Διαδικασία εισαγωγής 2ης εικόνας δίσκου**

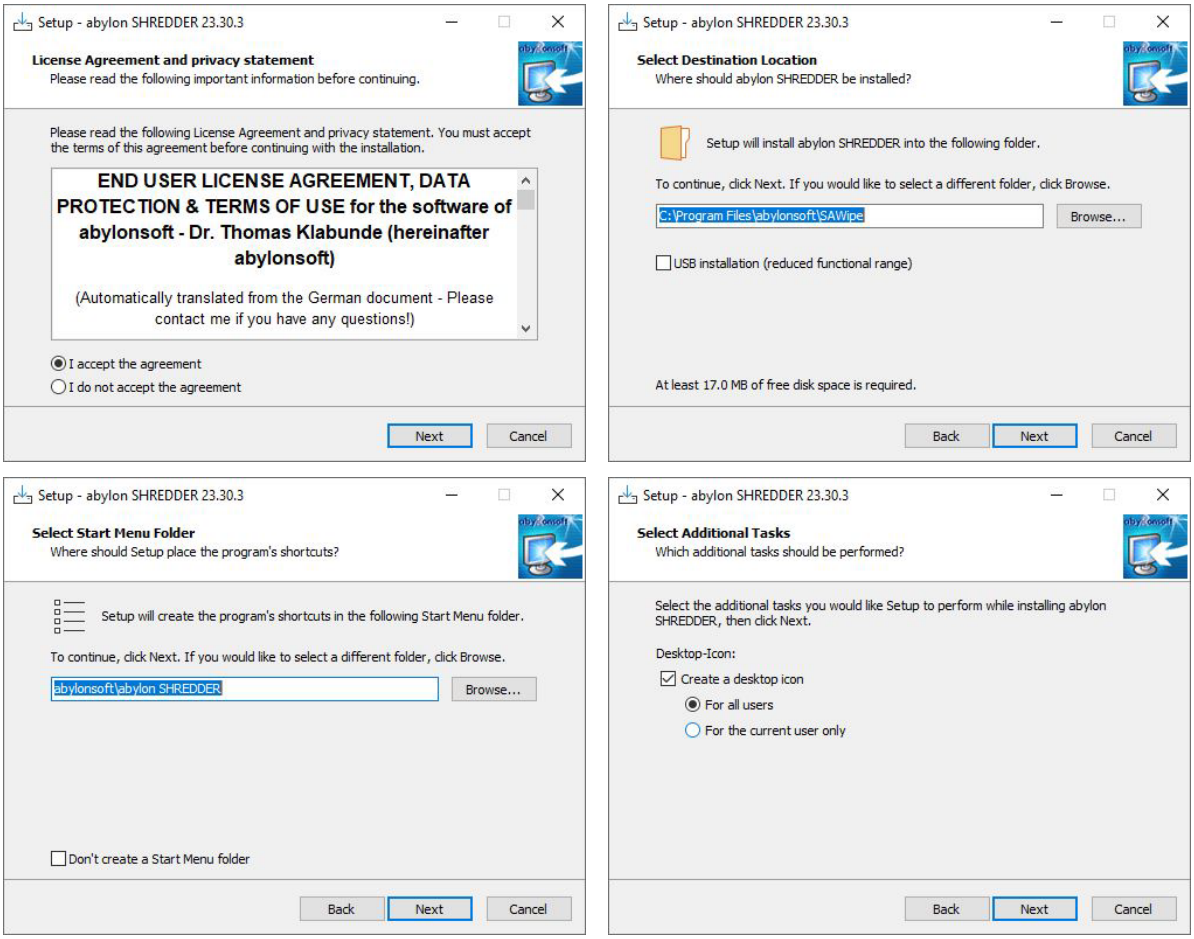
3. Εικόνα δίσκου με 200GB δεδομένων διαγραμμένος ολόκληρος

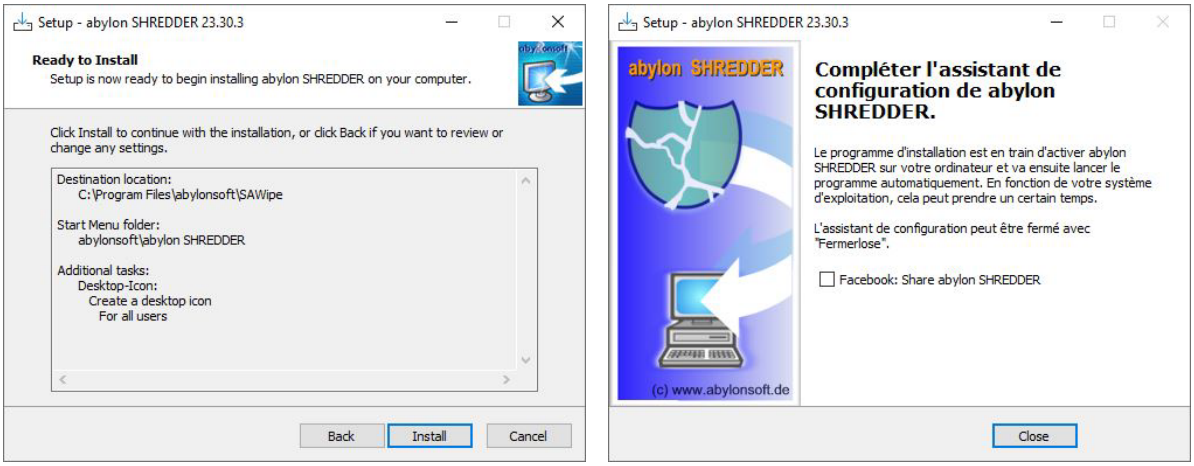



**Εικόνα 5-99: Εργαλείο 4 - Autopsy - Διαδικασία εισαγωγής 3ης εικόνας δίσκου**

### 5.2.5 Εργαλείο 5 - Abylon Shredder

Εγκατάσταση εργαλείου



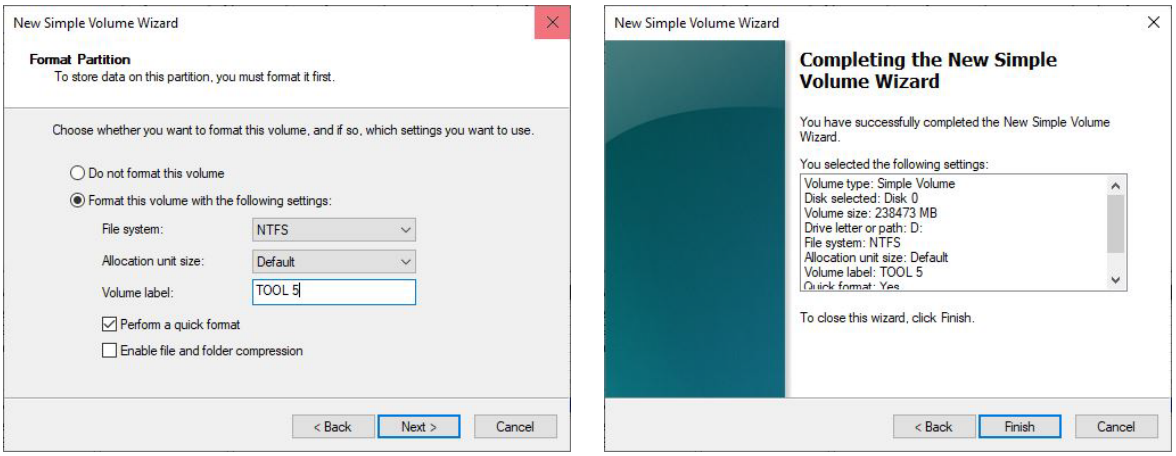



**Εικόνα 5-100: Εργαλείο 5 - Διαδικασία εγκατάστασης TS DataWiper**

Για σκοπούς αποφυγής επανάληψης, τα βήματα προετοιμασίας του δίσκου για την αξιολόγηση του τέταρτου εργαλείου οριστικής διαγραφής δεδομένων δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια κατά την εξέταση του πρώτου εργαλείου.

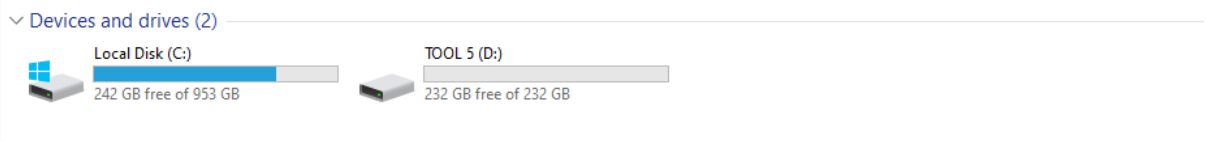
Θα αναφερθούμε μόνο επιγραμματικά στα βήματα.

1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser.
2. Ενεργοποίηση εργαλείου USB Write Blocker.
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.
4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.
5. Αρχικοποίηση MBR, μορφοποίηση του δίσκου σε NTFS Format και ονομασία του δίσκου σε TOOL 5.

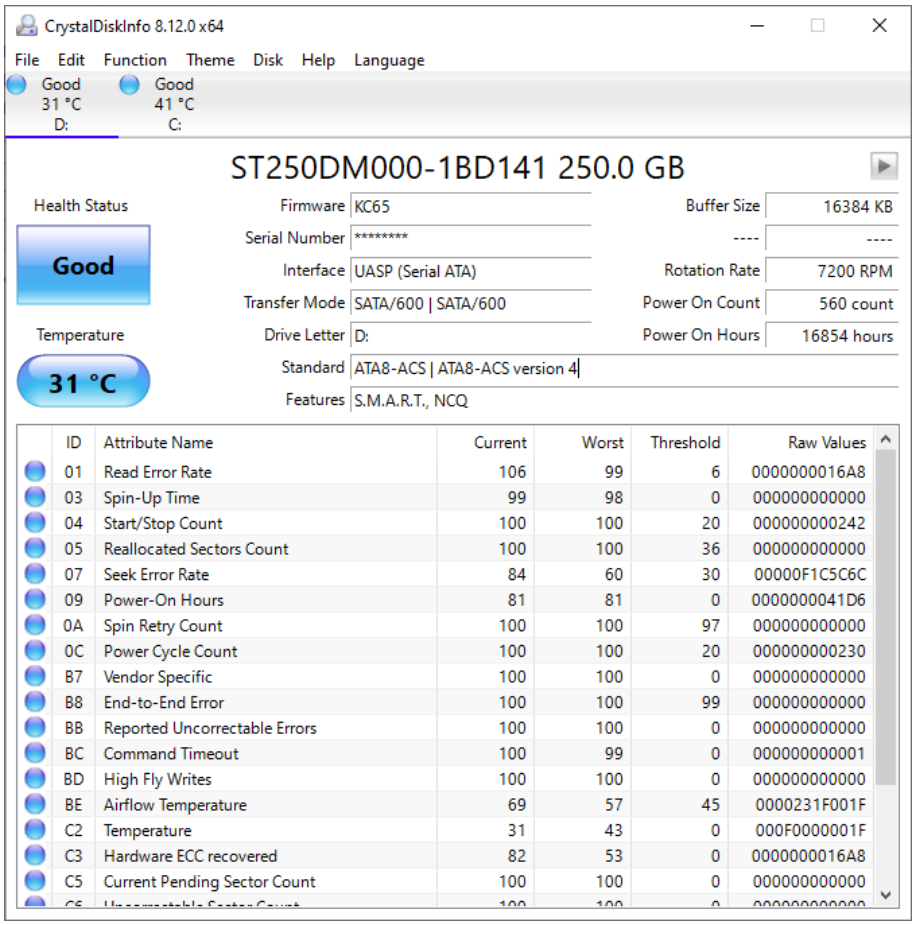



**Εικόνα 5-101: Εργαλείο 5 - Διαδικασία μορφοποίησης δίσκου για αξιολόγηση**

Τα πιο πάνω βήματα αποτελούν τη διαδικασία για τη μορφοποίηση του σκληρού δίσκου ώστε να μπορεί να χρησιμοποιηθεί από το λειτουργικό σύστημα. Μετά το πέρας της διαδικασίας ο δίσκος με την ονομασία TOOL 5 είναι ορατός και μπορούν να αντιγραφούν σε αυτόν τα δεδομένα για την διεξαγωγή των διαγραφών.



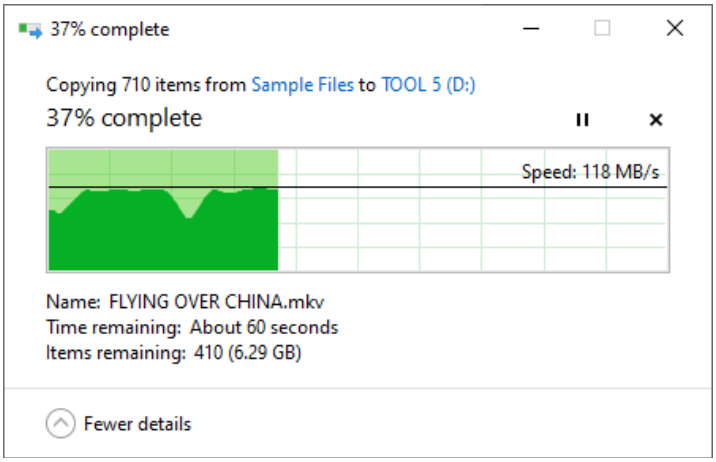

6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.




**Εικόνα 5-102: Εργαλείο 5 - CrystalDiskInfo - Αναφορά κατάστασης δίσκου**

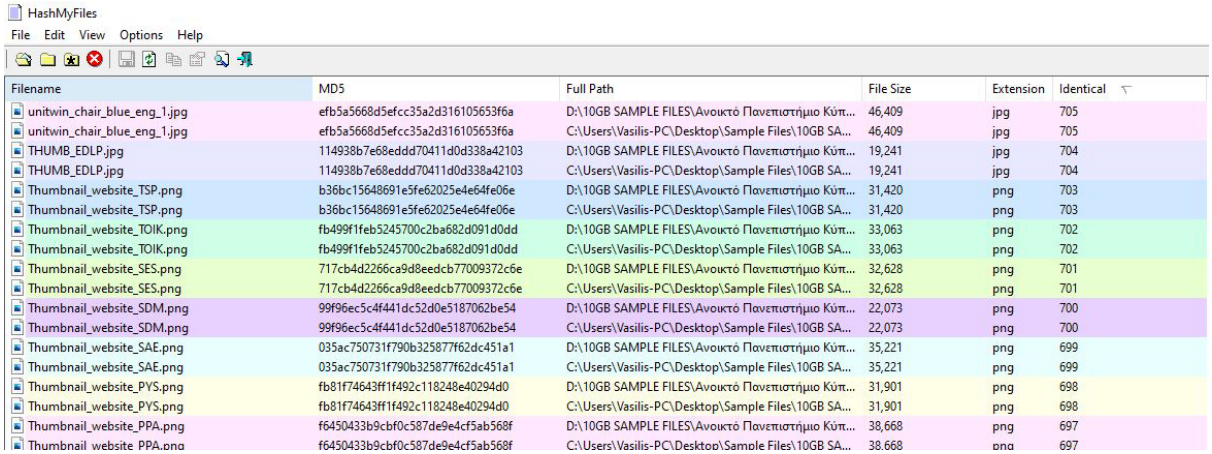
Σύμφωνα με την αναφορά του εργαλείου, ο δίσκος βρίσκεται σε καλή κατάσταση έτσι μπορούμε να αντιγράψουμε σε αυτόν τα αρχικά δεδομένα των 10 GB (705 αρχεία).

7. Αντιγραφή 10GB στο δίσκο




**Εικόνα 5-103: Εργαλείο 5 - Αντιγραφή 10 GB δεδομένων στο δίσκο**

8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.

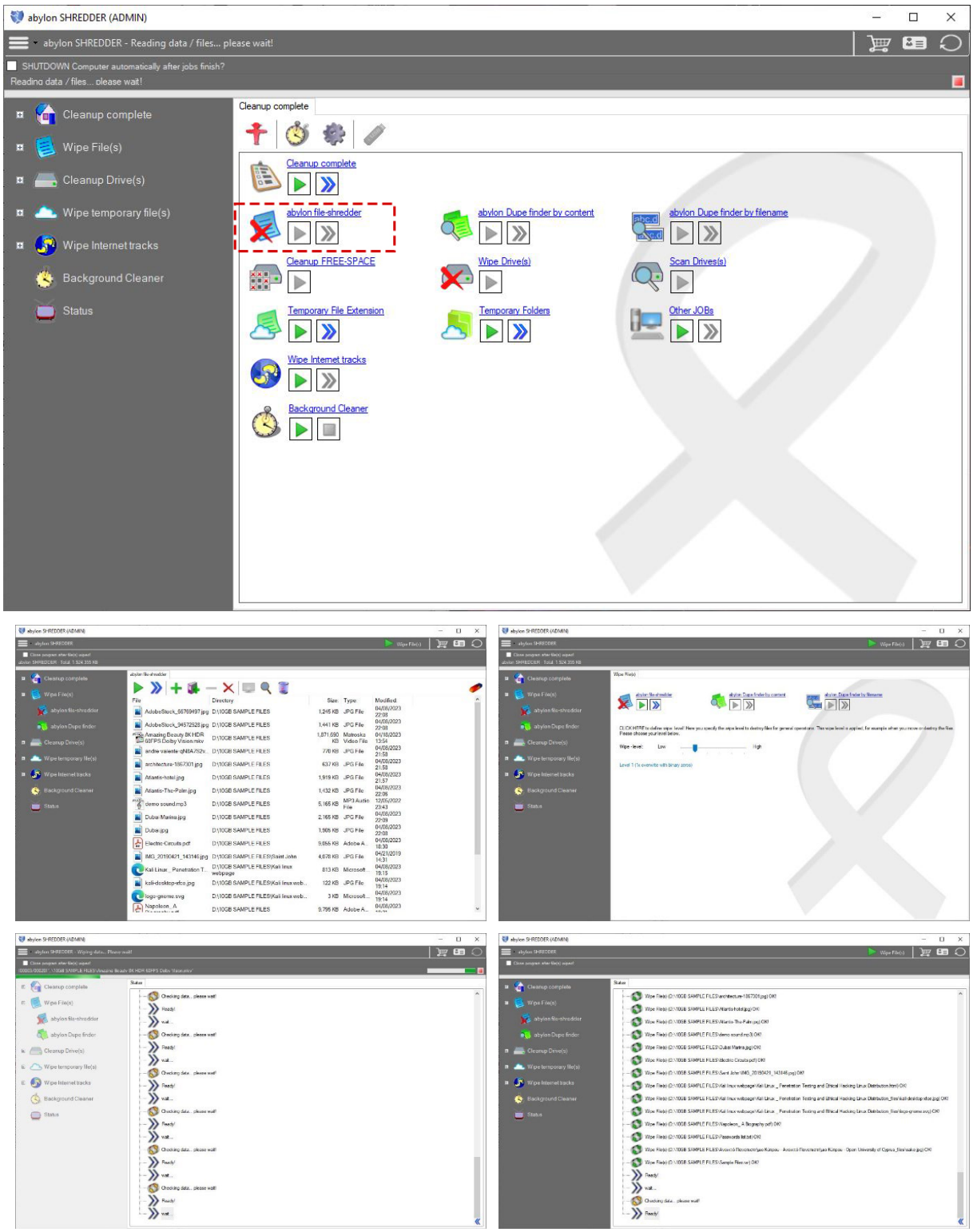



| Filename | MD5 | Full Path | File Size | Extension | Identical |
|---|---|---|---|---|---|
| unitwin_chair_blue_eng_1.jpg | efb5a5668d5efcc35a2d316105653f6a | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 46,409 | jpg | 705 |
| unitwin_chair_blue_eng_1.jpg | efb5a5668d5efcc35a2d316105653f6a | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 46,409 | jpg | 705 |
| THUMB_EDLP.jpg | 114938b7e68eddd70411d0d338a42103 | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 19,241 | jpg | 704 |
| THUMB_EDLP.jpg | 114938b7e68eddd70411d0d338a42103 | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 19,241 | jpg | 704 |
| Thumbnail_website_TSP.png | b36bc15648691e5fe62025e4e64fe06e | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 31,420 | png | 703 |
| Thumbnail_website_TSP.png | b36bc15648691e5fe62025e4e64fe06e | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 31,420 | png | 703 |
| Thumbnail_website_TOIK.png | fb499f1feb5245700c2ba682d091d0dd | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 33,063 | png | 702 |
| Thumbnail_website_TOIK.png | fb499f1feb5245700c2ba682d091d0dd | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 33,063 | png | 702 |
| Thumbnail_website_SES.png | 717cb4d2266ca9d8eedcb77009372c6e | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 32,628 | png | 701 |
| Thumbnail_website_SES.png | 717cb4d2266ca9d8eedcb77009372c6e | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 32,628 | png | 701 |
| Thumbnail_website_SDM.png | 99f96ec5c4f441dc52d0e5187062be54 | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 22,073 | png | 700 |
| Thumbnail_website_SDM.png | 99f96ec5c4f441dc52d0e5187062be54 | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 22,073 | png | 700 |
| Thumbnail_website_SAE.png | 035ac750731f790b325877f62dc451a1 | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 35,221 | png | 699 |
| Thumbnail_website_SAE.png | 035ac750731f790b325877f62dc451a1 | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 35,221 | png | 699 |
| Thumbnail_website_PYS.png | fb81f74643ff1f492c118248e40294d0 | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 31,901 | png | 698 |
| Thumbnail_website_PYS.png | fb81f74643ff1f492c118248e40294d0 | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 31,901 | png | 698 |
| Thumbnail_website_PPA.png | f6450433b9cbf0c587de9e4cf5ab568f | D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπ... | 38,668 | png | 697 |
| Thumbnail_website_PPA.png | f6450433b9cbf0c587de9e4cf5ab568f | C:\Users\Vasilis-PC\Desktop\Sample Files\10GB SA... | 38,668 | png | 697 |

**Εικόνα 5-104: Εργαλείο 5 - HashMyFiles - Σύγκριση αρχείων**

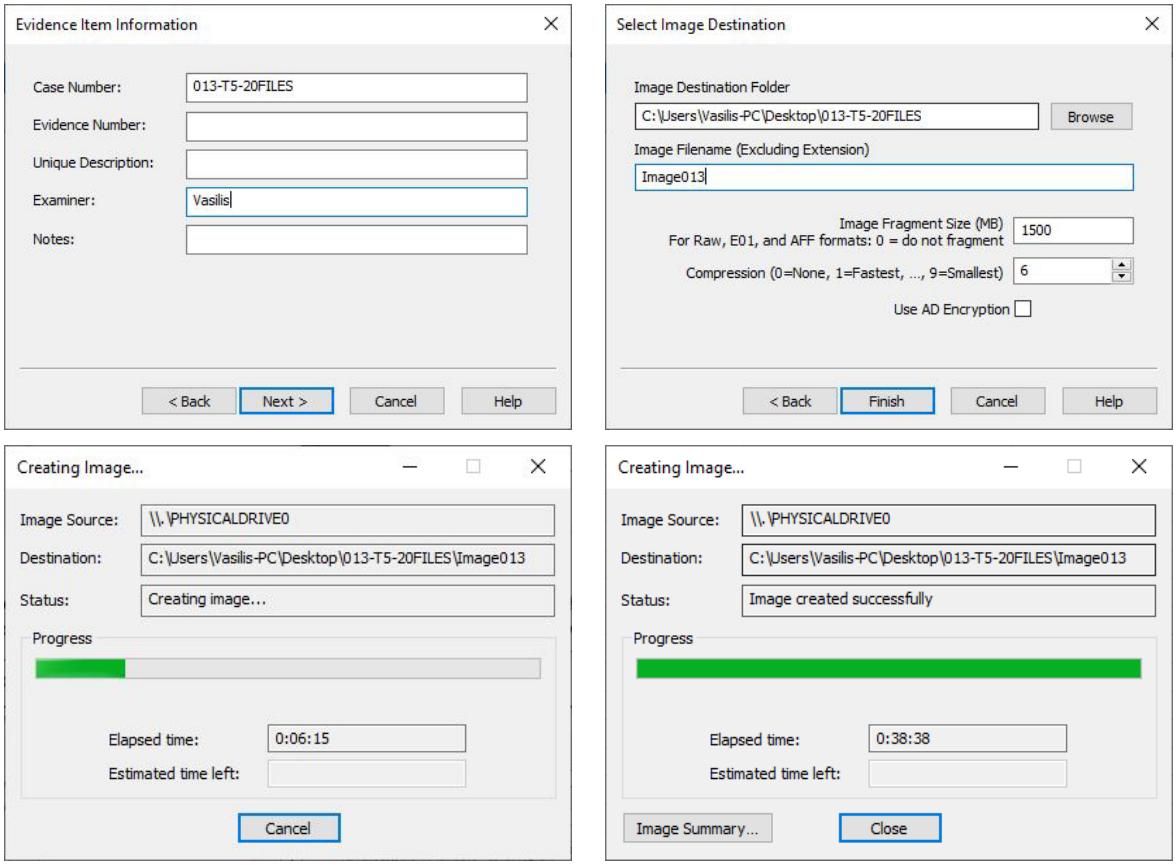
- **<u>Εκτέλεση πρώτου σεναρίου</u> – Διαγραφή 20 συγκεκριμένων αρχείων από το δίσκο**

Από το κεντρικό μενού επιλέγουμε Διαγραφή Αρχείων (Wipe Files). Στη συνέχεια επιλέγουμε τα 20 αρχεία που έχουμε καθορίσει από την αρχή για τη διεξαγωγή αυτού του σεναρίου για όλα τα εργαλεία οριστικής διαγραφής δεδομένων. Επίσης καθορίζουμε τη μέθοδο διαγραφής σε Level 1 (1x overwrite with binary zeros). Η μέθοδος αυτή είναι η αντίστοιχη μέθοδος one pass zero κατά την οποία τα δεδομένα του δίσκου εγγράφονται σε μια επανάληψη με μηδενικά. Πατάμε Wipe και το εργαλείο ξεκινά την διαγραφή. Στο τέλος της διαδικασίας το εργαλείο ενημερώνει για την επιτυχή διαγραφή των αρχείων.




**Εικόνα 5-105: Εργαλείο 5 - Abylon Shredder - Διαδικασία διαγραφής των 20 αρχείων**

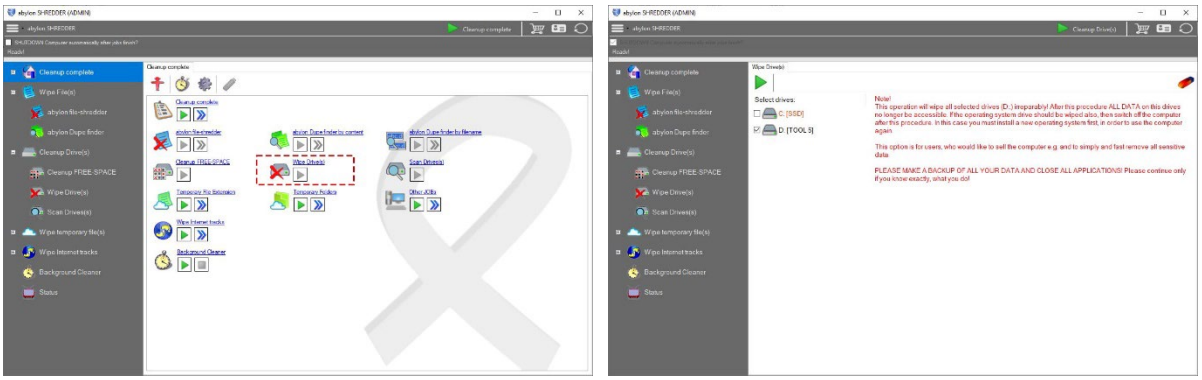
Με το πέρας της διαδικασίας διαγραφής των αρχείων προχωρούμε σε εξαγωγή της εικόνας του δίσκου με το εργαλείο AccessData FTK Imager. Με αυτό τον τρόπο θα μπορέσουμε να εισάγουμε την εικόνα στο δικανικό εργαλείο Autopsy και να εντοπίσουμε ίχνη από τα αρχεία που πιθανόν να μην έχουν διαγραφεί.

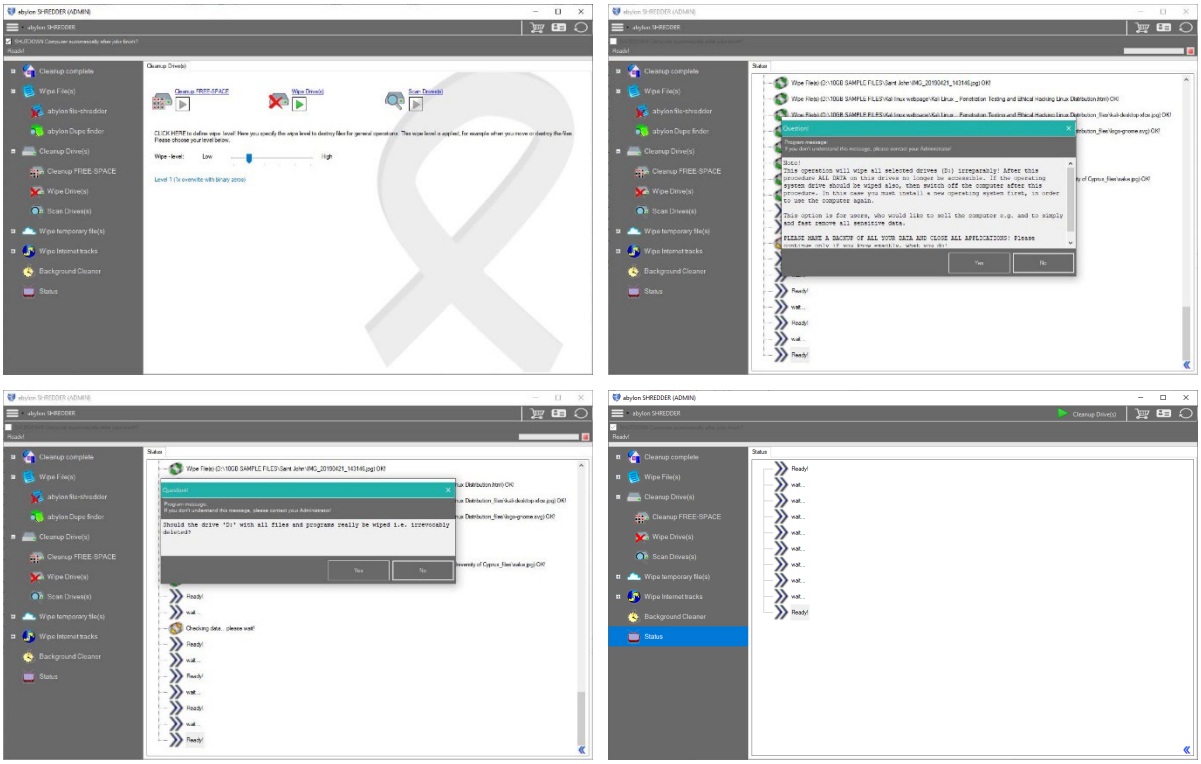



**Εικόνα 5-106: Εργαλείο 5 - AccessData FTK Imager - Διαδικασία δημιουργίας 1ης εικόνας δίσκου μετά την διαγραφή**

- **<u>Εκτέλεση δεύτερου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 10 GB**

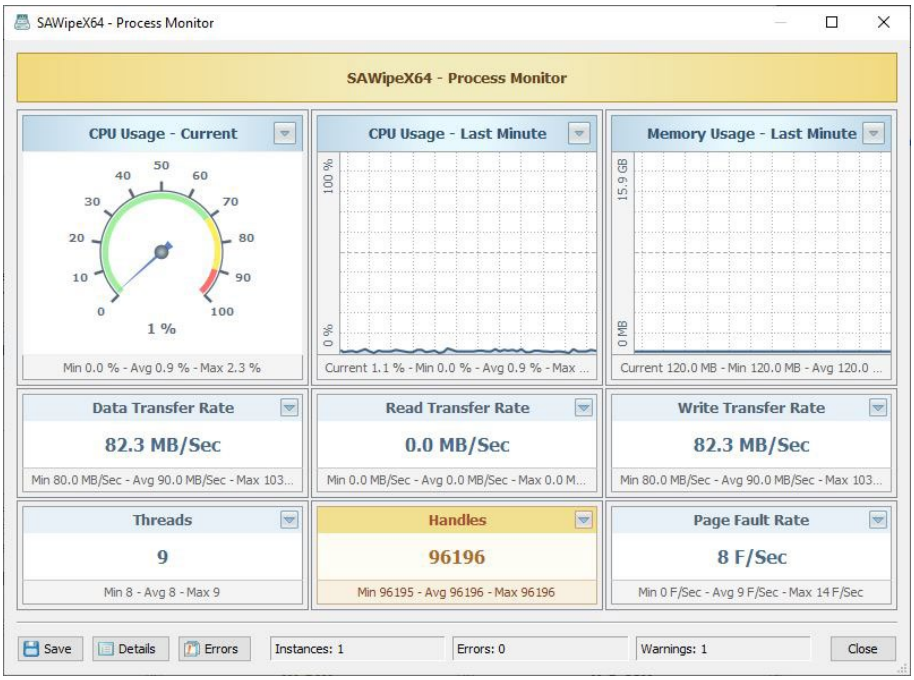
Από το κεντρικό μενού επιλέγουμε την επιλογή, διαγραφή σκληρού δίσκου (Wipe Drive). Στη λίστα με τους διαθέσιμους δίσκους για διαγραφή, εντοπίζουμε το προς διαγραφή δίσκο και τον επιλέγουμε. Στο επόμενο βήμα καθορίζουμε τη μέθοδο διαγραφής σε Level 1 (1x overwrite with binary zeros). Η μέθοδος αυτή είναι η αντίστοιχη μέθοδος one pass zero κατά την οποία τα δεδομένα του δίσκου εγγράφονται σε μια επανάληψη με μηδενικά. Τέλος το εργαλείο μας προτρέπει να επιβεβαιώσουμε την πρόθεση μας για οριστική διαγραφή του δίσκου 2 φορές.





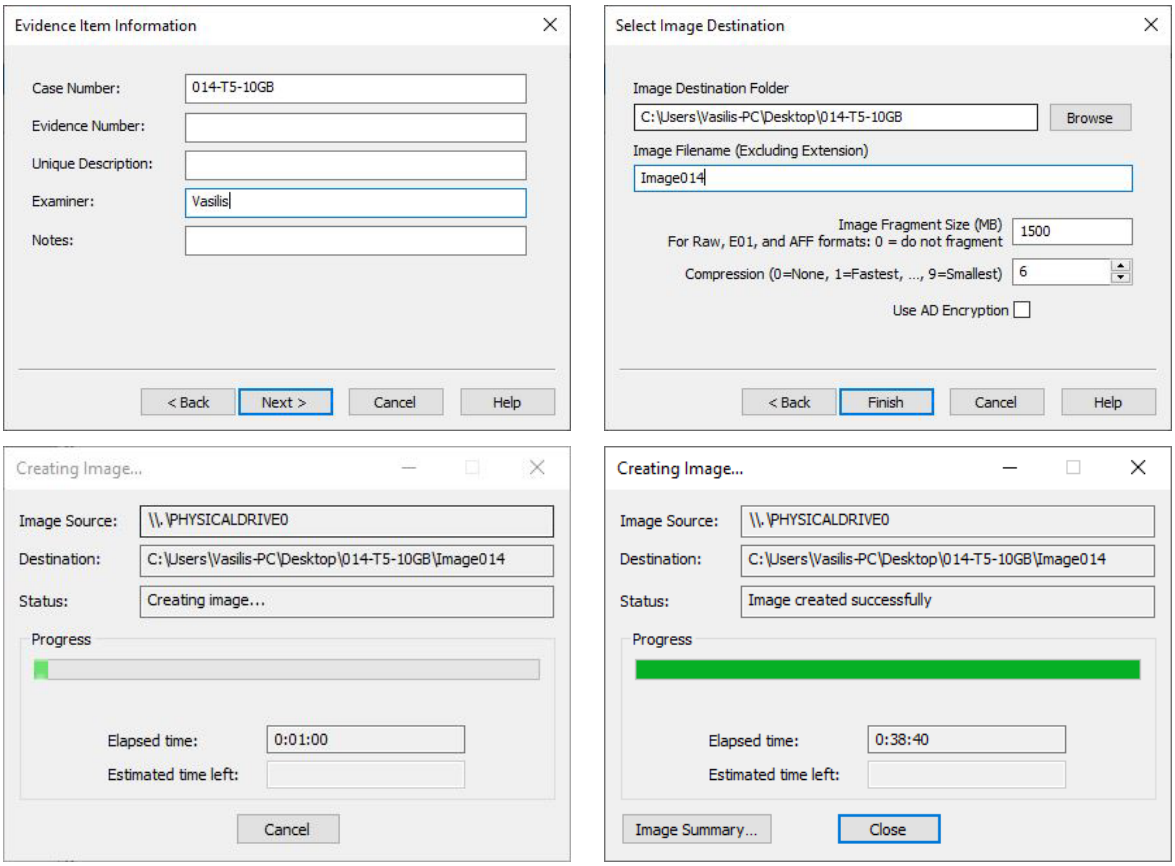
**Εικόνα 5-107: Εργαλείο 5 - Abylon Shredder - Διαδικασία διαγραφής δίσκου – Αρχεία 10GB**

Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.




**Εικόνα 5-108: Εργαλείο 5 - SysGauge - Καταγραφή πόρων συστήματος κατά την διαγραφή ολόκληρου του δίσκου - 10GB**

Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 10 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για δεύτερη φορά με το εργαλείο AccessData FTK Imager.



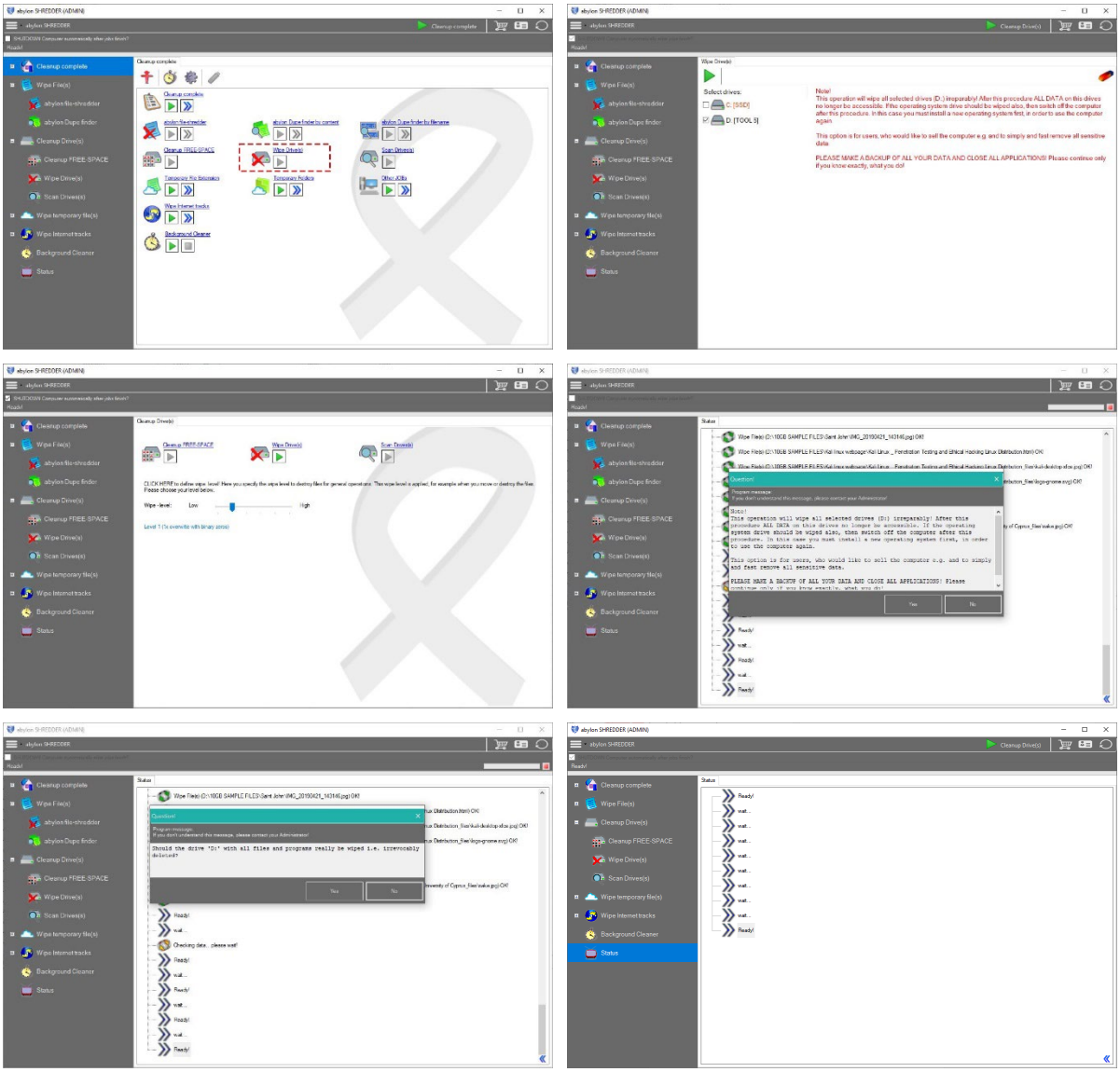

**Εικόνα 5-109: Εργαλείο 5 - AccessData FTK Imager - Διαδικασία δημιουργίας 2ης εικόνας δίσκου μετά την διαγραφή**

- **<u>Εκτέλεση τρίτου σεναρίου</u> – Διαγραφή ολόκληρου του δίσκου – 200 GB**

Για σκοπούς αποφυγής επανάληψης τα βήματα αρχικοποίησης και μορφοποίησης του δίσκου για το τρίτο σενάριο, αυτό της διαγραφής ολόκληρου του δίσκου με τα 200GB δεδομένων σε αυτόν, δεν θα παρουσιαστούν με στιγμιότυπα αφού έχουν αναλυθεί με λεπτομέρεια πιο πάνω. Θα αναφερθούμε μόνο επιγραμματικά ως βήματα.

1. Αρχικοποίηση του δίσκου με χρήση συσκευής GLOTRENDS 2-in-1 SATA Hard Drive Eraser.
2. Ενεργοποίηση εργαλείου USB Write Blocker
3. Σύνδεση του δίσκου στον υπολογιστή μέσω σύνδεσης USB 3.0 και επιβεβαίωση με το εργαλείο HxD ότι όλα τα bit που βρίσκονται γραμμένα σε αυτό είναι 0.
4. Σύνδεση του σκληρού δίσκου στη μητρική του υπολογιστή μέσω σύνδεσης SATA.

5. Αρχικοποίηση MBR και μορφοποίηση του δίσκου σε NTFS Format.
6. Έλεγχος της υγείας του δίσκου με το εργαλείο CrystalDiskInfo.
7. Αντιγραφή 200GB στο δίσκο για διαγραφή.
8. Έλεγχος κατακερματισμένων τιμών MD5 των αρχείων του δίσκου σε σύγκριση με τα αρχικά αρχεία για να διαπιστωθεί ότι έχουν τοποθετηθεί όλα τα αρχεία στο δίσκο.
9. Έναρξη διαδικασίας διαγραφής ολόκληρου του δίσκου με το εργαλείο οριστικής διαγραφής .

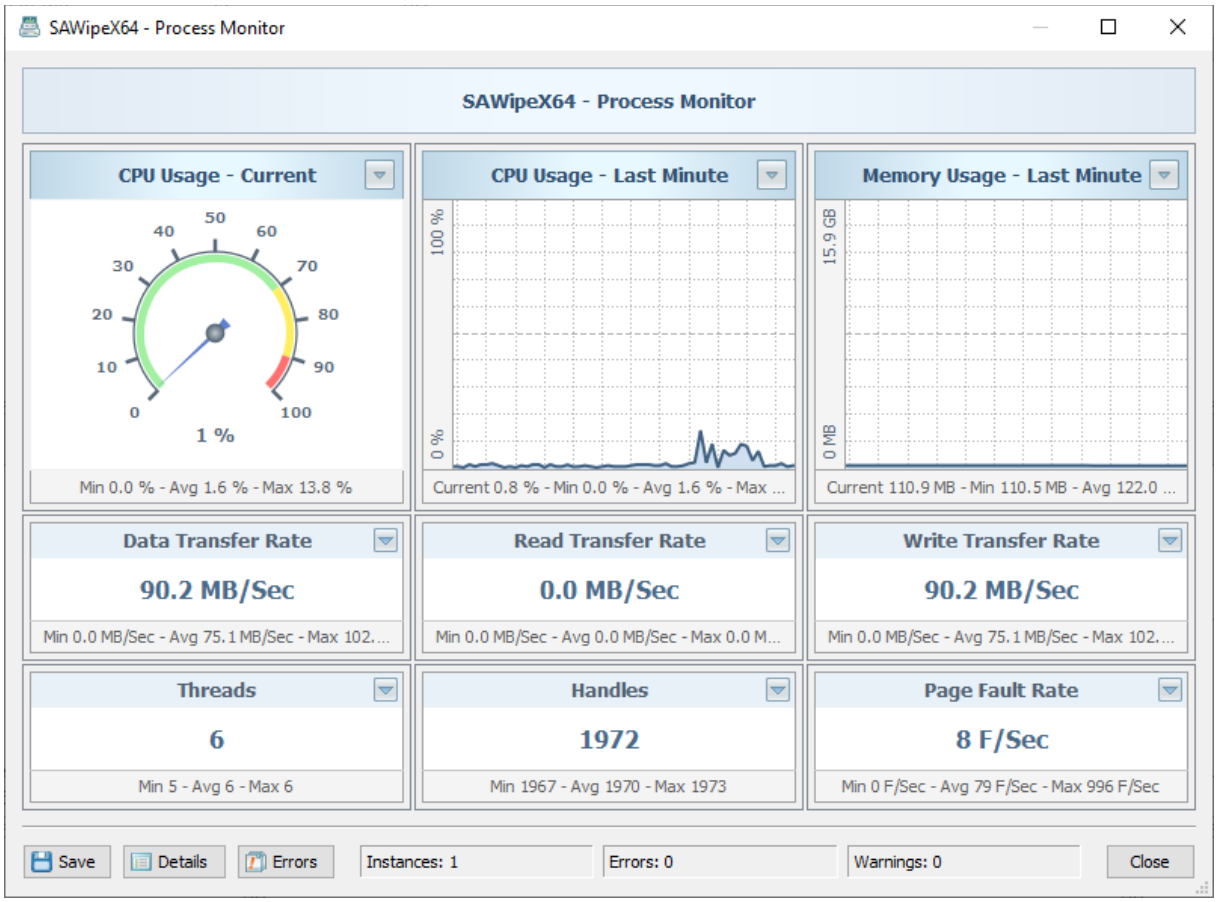


**Εικόνα 5-110: Εργαλείο 5 - Abylon Shredder - Διαδικασία διαγραφής δίσκου – Αρχεία 200GB**

Να αναφέρουμε ότι κατά την διάρκεια της διαγραφής το εργαλείο σταμάτησε να ανταποκρίνεται έτσι χρειάστηκε να επαναλάβουμε την διαδικασία από την αρχή. Το ίδιο πρόβλημα προέκυψε και

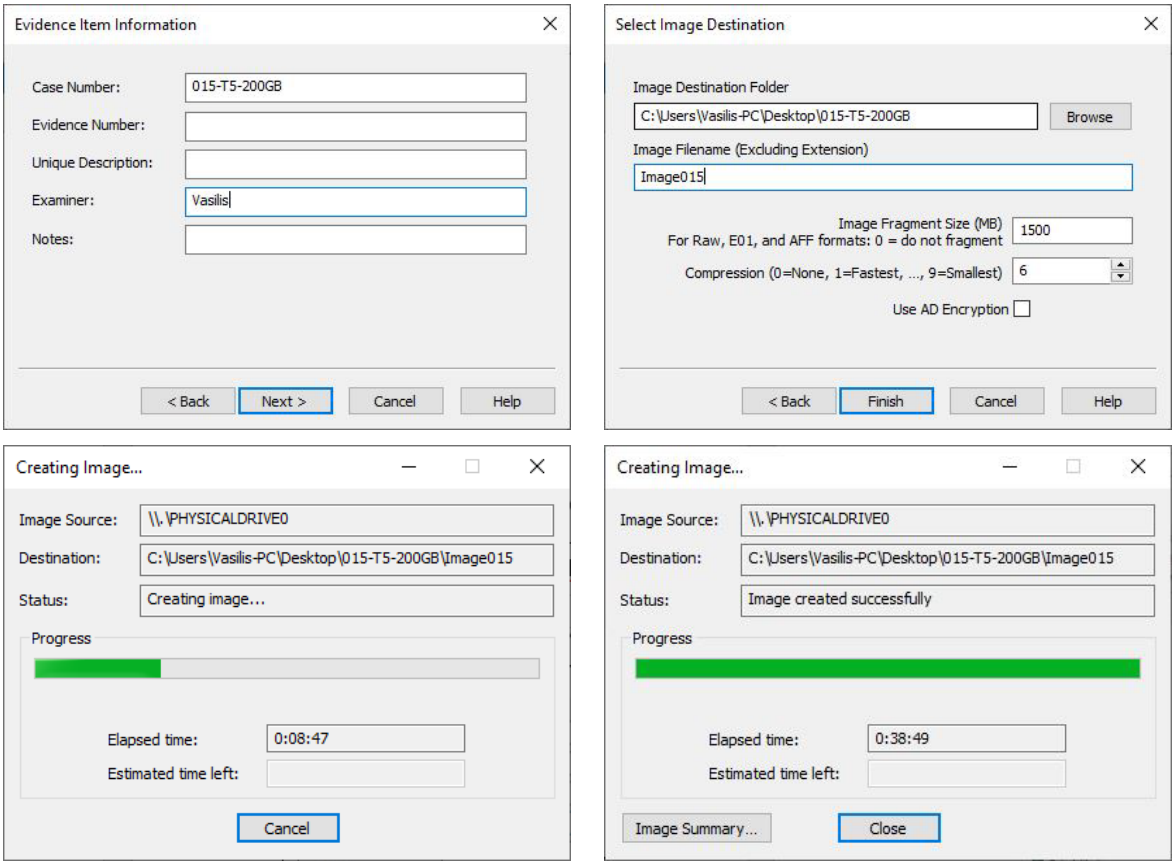
στην δοκιμή οριστικής διαγραφής ολόκληρου του δίσκου με τα 10GB δεδομένων σε αυτό. Η συστηματικότητα εμφάνισης του συγκεκριμένου προβλήματος μας οδηγεί στο συμπέρασμα ότι πρόκειται για σφάλμα υλοποίησης του εργαλείου και όχι κάποιο τυχαίο γεγονός.

Παράλληλα με την έναρξη της διαδικασίας διαγραφής του δίσκου, εκτελούμε το εργαλείο SysGauge το οποίο καταγράφει σε πραγματικό χρόνο τη χρήση του επεξεργαστή, της μνήμης και των εγγραφών δεδομένων στο δίσκο που κάνει το συγκεκριμένο εργαλείο.




**Εικόνα 5-111: Εργαλείο 5 - Abylon Shredder - Καταγραφή πόρων συστήματος κατά την διαγραφή ολόκληρου του δίσκου - 200GB**

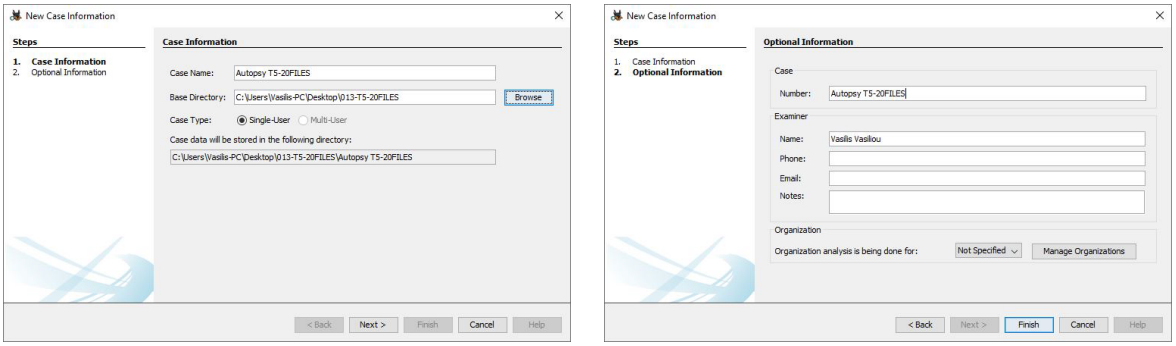
Με το πέρας της διαδικασίας διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε τα 200 GB δεδομένων προχωρούμε σε εξαγωγή της εικόνας του δίσκου για τρίτη φορά με το εργαλείο AccessData FTK Imager. Η διαδικασία εξαγωγής της εικόνας του δίσκου είναι η ίδια που ακολουθήσαμε και στην πιο πάνω περίπτωση με διαφορά την ονομασία της εικόνας του δίσκου ώστε να υπάρχει αρχειοθέτηση και καταγραφή των σεναρίων .




**Εικόνα 5-112: Εργαλείο 5 - AccessData FTK Imager - Διαδικασία δημιουργίας 3ης εικόνας δίσκου μετά την διαγραφή**

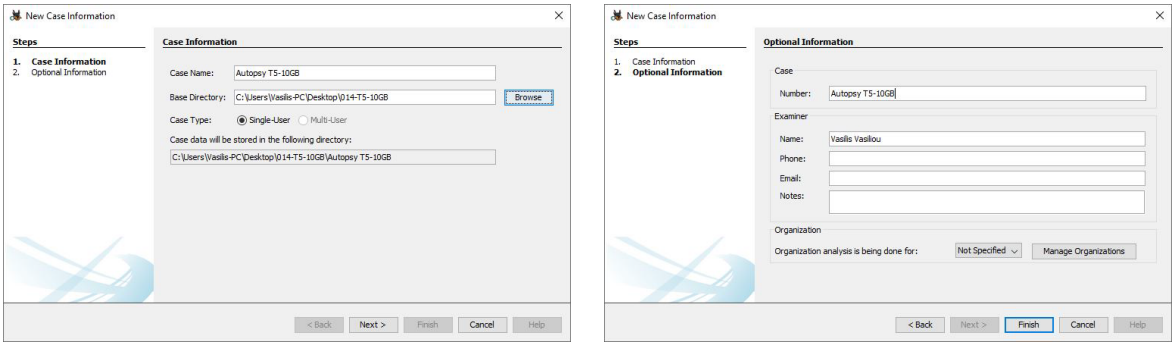
## Εισαγωγή εικόνων δίσκων στο Autopsy

1. Εικόνα δίσκου με τα 20 διαγραμμένα αρχεία



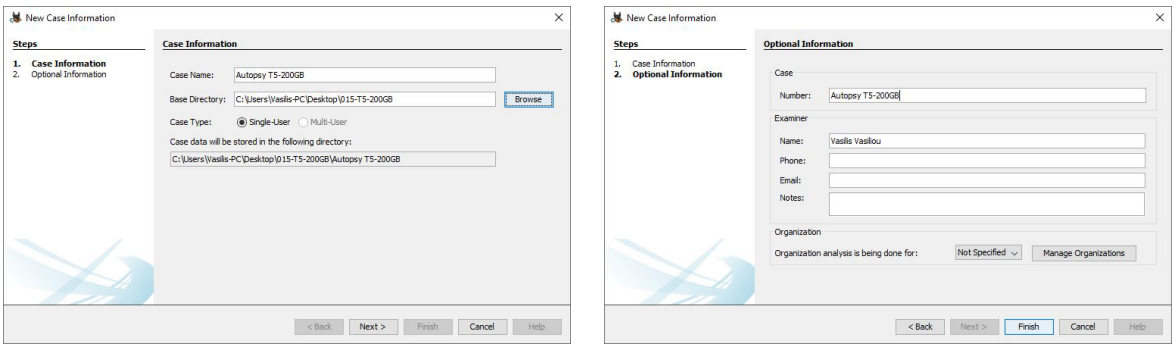

**Εικόνα 5-113: Εργαλείο 5 - Autopsy - Διαδικασία εισαγωγής 1ης εικόνας δίσκου**

2. Εικόνα δίσκου με 10GB δεδομένων διαγραμμένος ολόκληρος




**Εικόνα 5-114: Εργαλείο 5 - Autopsy - Διαδικασία εισαγωγής 2ης εικόνας δίσκου**

3. Εικόνα δίσκου με 200GB δεδομένων διαγραμμένος ολόκληρος




**Εικόνα 5-115: Εργαλείο 5 - Autopsy - Διαδικασία εισαγωγής 3ης εικόνας δίσκου**

# Κεφάλαιο 6
# Αποτελέσματα Μελέτης Εργαλείων Οριστικής Διαγραφής

Στο παρόν κεφάλαιο παρουσιάζονται τα αποτελέσματα των πειραματικών δοκιμών στα εργαλεία οριστικής διαγραφής δεδομένων που αναλύθηκαν στα προηγούμενα κεφάλαια.

## 6.1 Παρουσίαση Αποτελεσμάτων

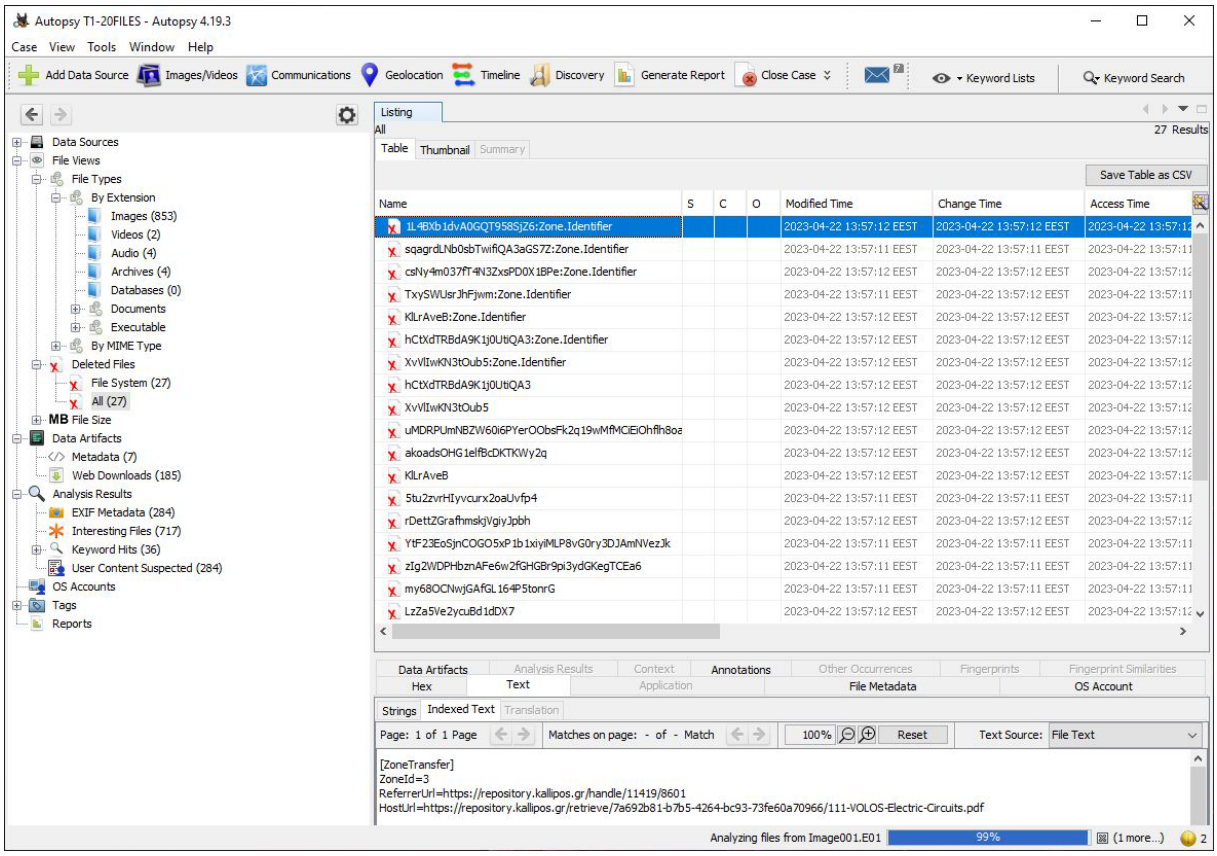
Τα αποτελέσματα παρουσιάζονται ανά εργαλείο και ανά σενάριο αξιολόγησης, ενώ στο τέλος του κεφαλαίου παρουσιάζεται συνοπτικός πίνακας με την ικανότητα διαγραφής όλων των εργαλείων.

### 6.1.1 Εργαλείο 1 - AOMEI Partition Assistant

Για το εργαλείο αυτό εκτελέστηκαν συνολικά τρία διαφορετικά σενάρια κατά τα οποία αξιολογήθηκαν οι δυνατότητες του εργαλείου όσο αφορά την οριστική διαγραφή συγκεκριμένων αρχείων όσο και ολόκληρου του δίσκου.

- Αξιολόγηση 1 (A1) – Οριστική διαγραφή 20 προκαθορισμένων αρχείων από το δίσκο

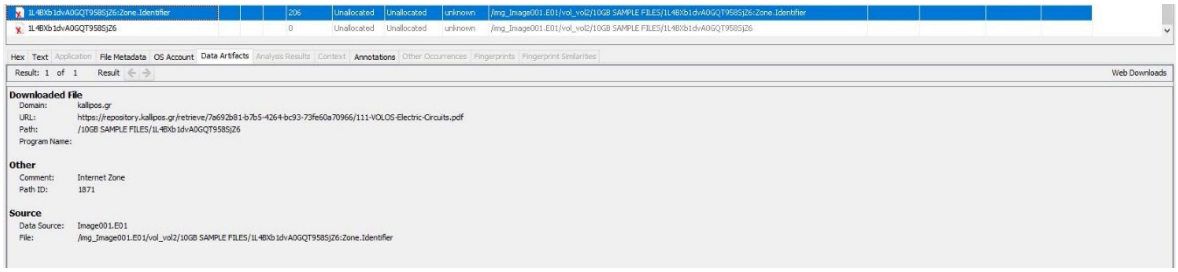
Από την εξέταση της εικόνας του δίσκου η οποία λήφθηκε αμέσως μετά την διαγραφή των συγκεκριμένων αρχείων με τη χρήση του δικανικού εργαλείου Autopsy διαφαίνεται ότι τα αρχεία έχουν μόνιμα διαγραφεί. Δεν κατέστη δυνατή οποιαδήποτε επαναφορά σε κανένα από τα αρχεία ανεξαρτήτου μεγέθους. Ωστόσο θα πρέπει να αναφερθεί ότι παρόλο που τα ίδια τα αρχεία έχουν εξαφανιστεί, στο αρχείο συστήματος του δίσκου παρέμειναν καταχωρήσεις που μαρτυρούσαν την παρουσία των συγκεκριμένων αρχείων στο δίσκο πριν την διαγραφή τους. Οι καταχωρήσεις αυτές εντοπίζονται στην κατηγορία Deleted files στο Autopsy.



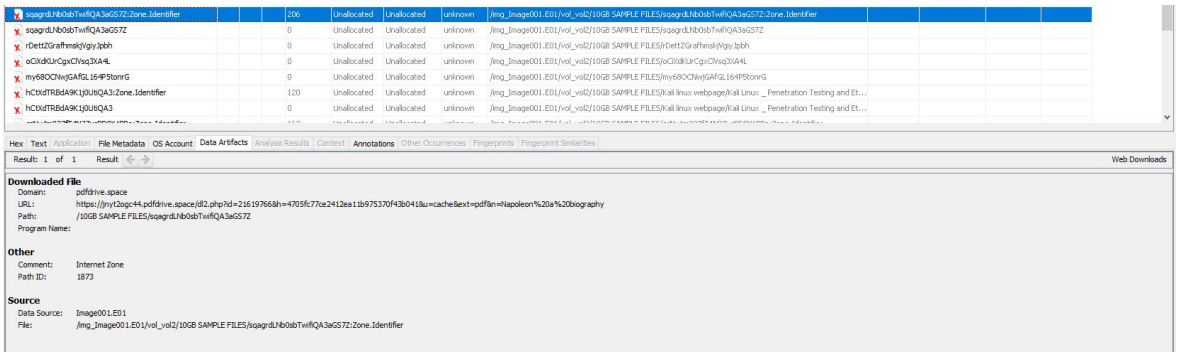

**Εικόνα 6-1: Εργαλείο 1 (A1) - Autopsy - Καταχωρήσεις διαγραμμένων αρχείων**

Συγκεκριμένα οι καταχωρίσεις που εντοπίστηκαν περιέχουν πληροφορίες για το ίδιο το αρχείο όπως ο φάκελος στον οποίο βρισκόταν, το όνομα του ή κάποιο σχετικό url που σχετίζεται με το αρχείο. Παρακάτω παρουσιάζονται κάποια παραδείγματα από τα ευρήματα.

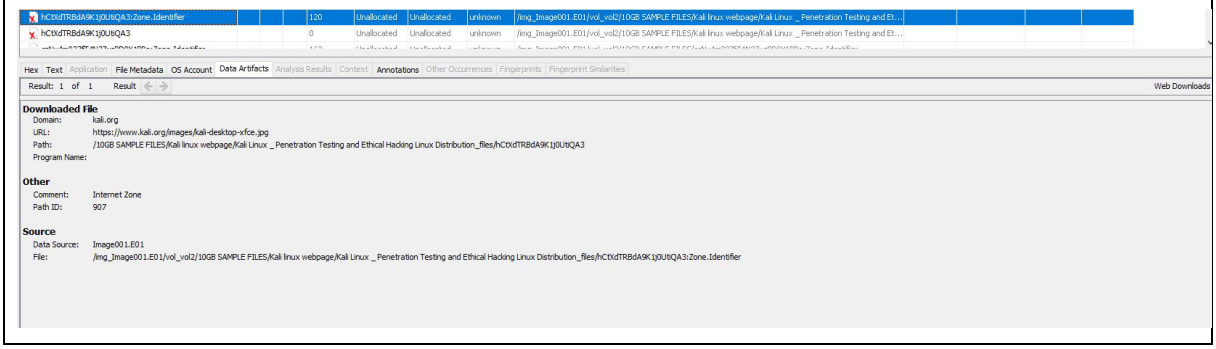
Αρχείο : Electric-Circuits.pdf



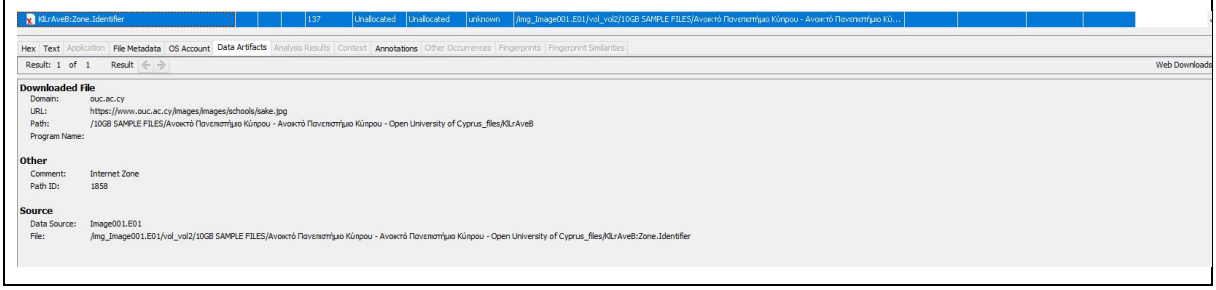

Αρχείο : Napoleon_ A Biography.pdf




Αρχείο : kali-desktop-xfce.jpg




Αρχείο : sake.jpg

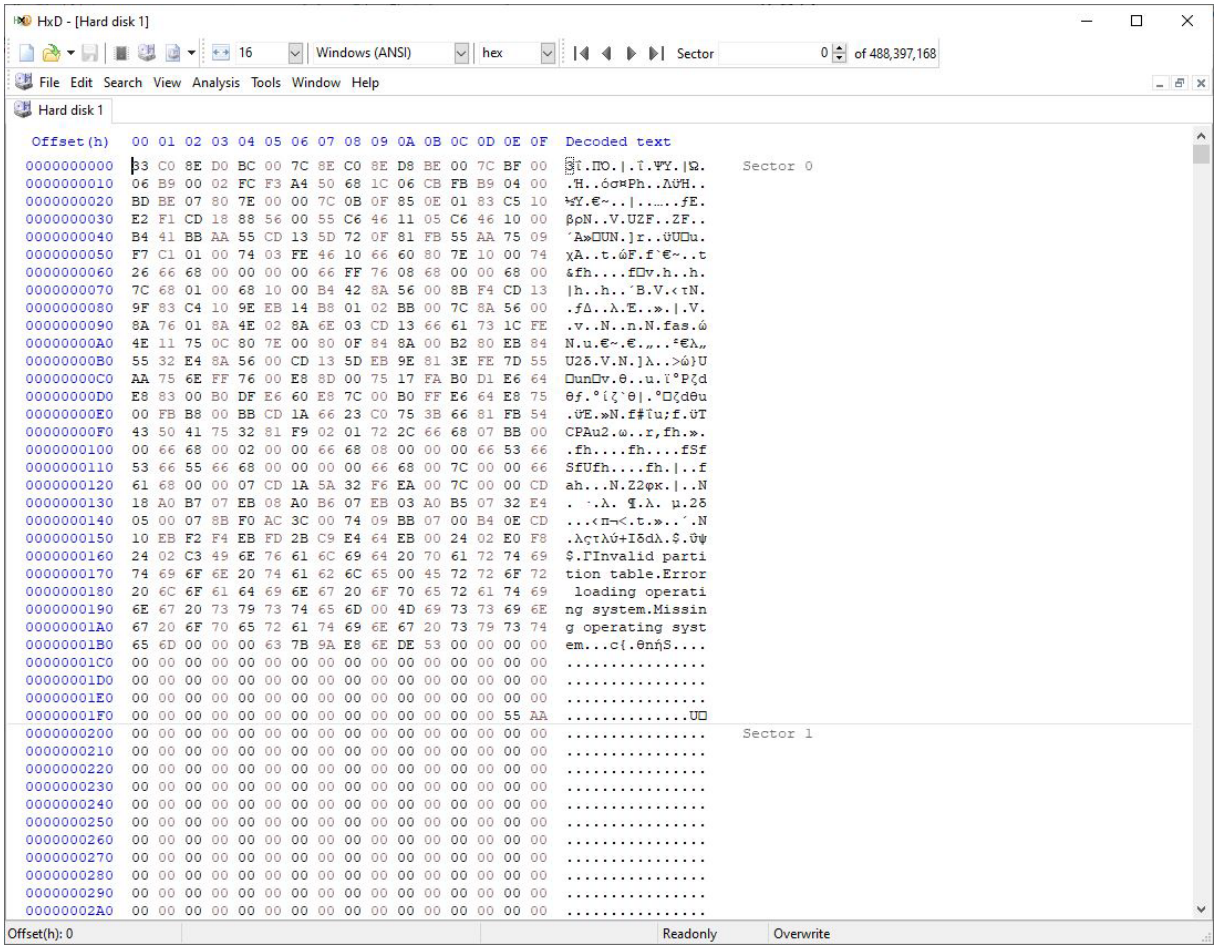



**Εικόνα 6-2: Εργαλείο 1 (Α1) – Ευρήματα από τα διαγραμμένα αρχεία**

Από τα ίχνη που εντοπίστηκαν μπορεί κάποιος να εντοπίσει το όνομα του αρχείου, τον τύπο, την πηγή λήψης του αρχείου καθώς επίσης και τον φάκελο στο οποίο ήταν αποθηκευμένο.

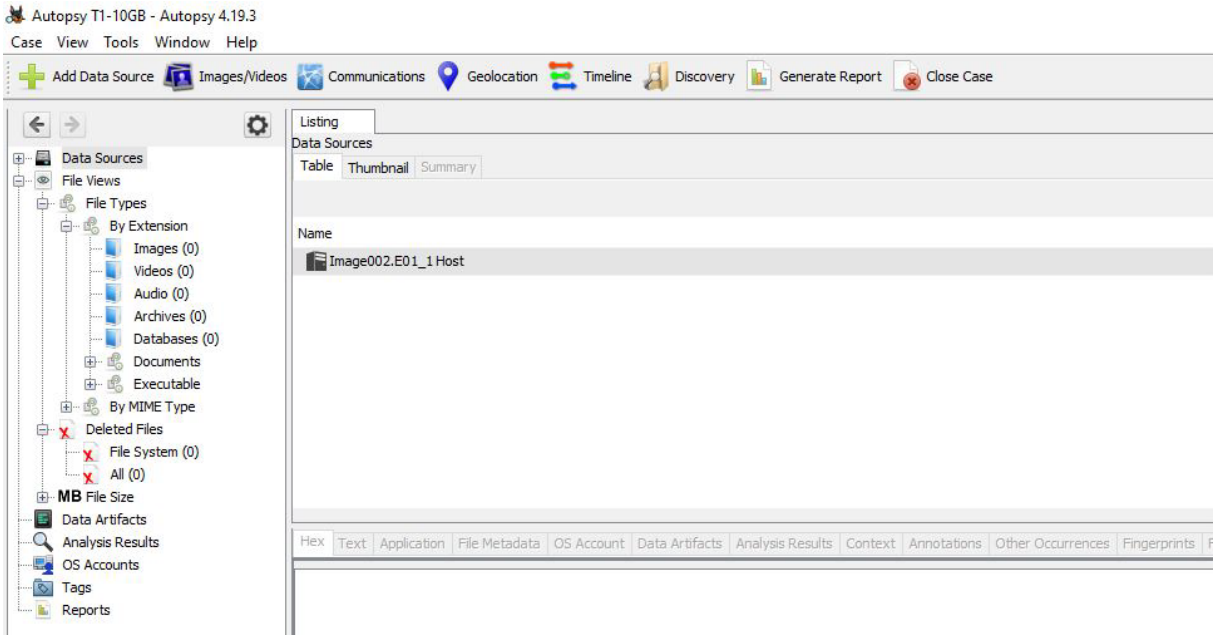
- Αξιολόγηση 2 (Α2) – Οριστική διαγραφή ολόκληρου του δίσκου με 10GB δεδομένα

Μετά την διαγραφή ολόκληρου του δίσκου και την εξαγωγή της εικόνας του, προχωρήσαμε σε ανάλυση της με το εργαλείο δικανικής Autopsy. Παράλληλα ανοίξαμε το δίσκο με το εργαλείο HxD για να έχουμε οπτική απεικόνισή των περιεχομένων του. Έχοντας κάνει χρήση του αλγόριθμού διαγραφής One Pass Zero κατά την διαγραφή του δίσκου αναμένουμε για μια πετυχημένη οριστική διαγραφή όλα τα bits στον δίσκο να είναι γραμμένα με μηδενικά.




**Εικόνα 6-3: Εργαλείο 1 (Α2) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Από την απεικόνιση των περιεχομένων παρατηρούμε ότι όλοι οι τομείς (sectors), εκτός από τον πρώτο είναι διαγραμμένοι. Αυτό οφείλεται στο γεγονός ότι στον πρώτο τομέα του δίσκου βρίσκεται ο MBR (Master Boot Record) στον οποίο το εργαλείο οριστικής διαγραφής δεν έχει πρόσβαση. Οι υπόλοιποι τομείς του δίσκου ωστόσο έχουν επιτυχώς εγγραφεί με μηδενικά, διαγράφοντας έτσι κάθε ίχνος δεδομένων από το δίσκο. Τα πιο πάνω επιβεβαίωσε και η ανάλυση της εικόνας του δίσκου που πραγματοποιήθηκε με την βοήθεια του εργαλείου Autopsy. Σύμφωνα λοιπόν με αυτή στον δίσκο δεν παρέμεινε κανένα αρχείο. Η περεταίρω ανάλυση της εικόνας με το εργαλείο δικανικής Bulk Extractor εκ του αποτελεσμάτος κρίνεται περιττή.




**Εικόνα 6-4: Εργαλείο 1 (Α2) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

PartAssist - Process Counters

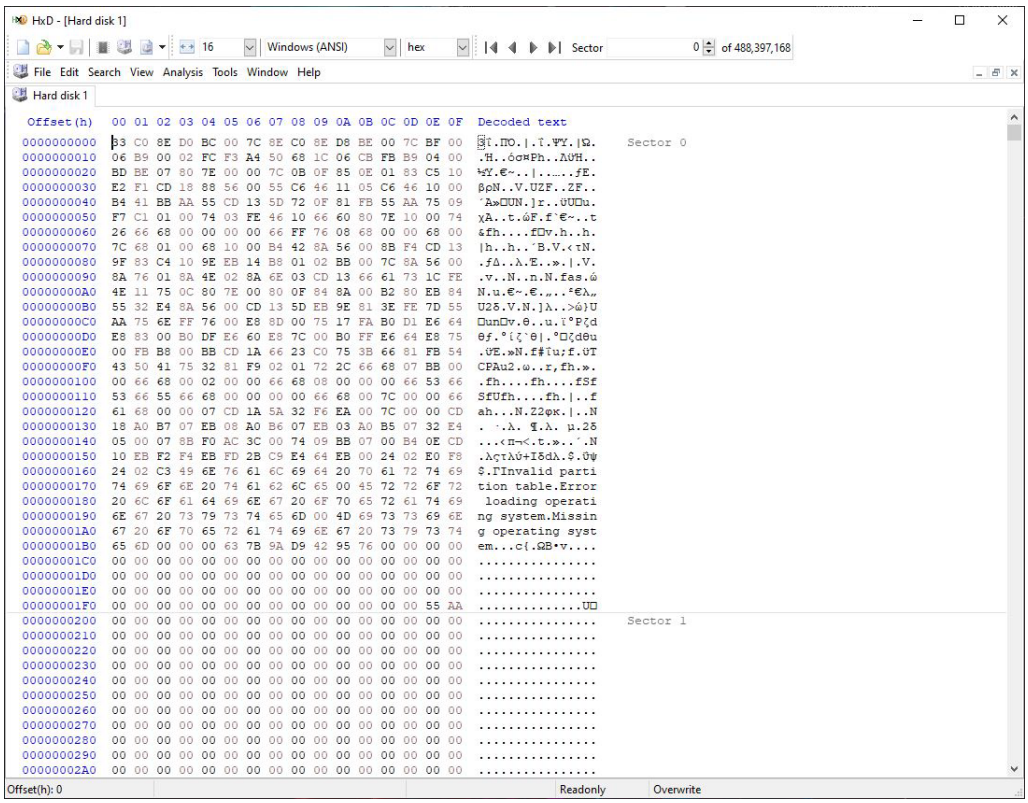
| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 1.6 % | 0.0 % | 8.7 % | --- |
| Process Memory Used | 37.9 MB | 0.0 MB | 38.8 MB | --- |
| Process Thread Count | 6 | 0 | 11 | --- |
| Process Handle Count | 464 | 0 | 491 | --- |
| Process Data Rate | 44939.6 MB/Sec | 0.0 MB/Sec | 62637.2 MB/Sec | 29359.94 GB |
| Process Read Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.1 MB/Sec | 0.1 MB |
| Process Write Rate | 44939.6 MB/Sec | 0.0 MB/Sec | 62637.2 MB/Sec | 29359.94 GB |
| Process Page Fault Rate | 2719 F/Sec | 0 F/Sec | 3879 F/Sec | 1818766 F/Sec |
| Process Nonpaged Pool Used | 0.0 MB | 0.0 MB | 0.0 MB | --- |

**Εικόνα 6-5: Εργαλείο 1 (Α2) – Απαιτήσεις σε υπολογιστικούς πόρους**

Χρόνος αποπεράτωσης διαγραφής: 42 λεπτά

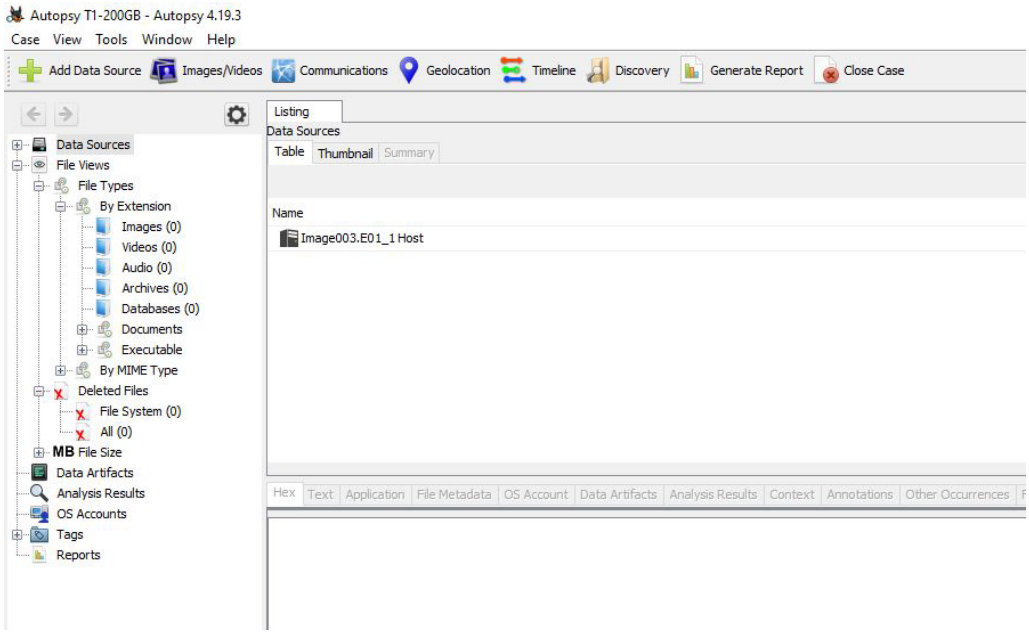
- Αξιολόγηση 3 (Α3) – Οριστική διαγραφή ολόκληρου του δίσκου με 200GB δεδομένα

Τα αποτελέσματα από την ολική διαγραφή του δίσκου με τα 200GB δεδομένων είναι όμοια με το προηγούμενο σενάριο του δίσκου στον οποίο περιέχονταν μόνο 10GB δεδομένων. Από την επισκόπηση του διαγραμμένου δίσκου με το εργαλείο HxD φαίνεται να έχουμε επίσης όλους τους τομείς πλην του πρώτου γραμμένους με μηδενικά.




**Εικόνα 6-6: Εργαλείο 1 (Α3) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Τα ίδια αποτελέσματα καταδεικνύει και η ανάλυση της εικόνας του δίσκου με το εργαλείο Autopsy.




**Εικόνα 6-7 Εργαλείο 1 (Α3) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

PartAssist - Process Counters

| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 2.2 % | 0.0 % | 7.5 % | --- |
| Process Memory Used | 38.6 MB | 0.0 MB | 38.7 MB | --- |
| Process Thread Count | 6 | 0 | 9 | --- |
| Process Handle Count | 464 | 0 | 467 | --- |
| Process Data Rate | 45531.6 MB/Sec | 0.0 MB/Sec | 62952.8 MB/Sec | 30947.23 GB |
| Process Read Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.2 MB/Sec | 0.2 MB |
| Process Write Rate | 45531.5 MB/Sec | 0.0 MB/Sec | 62952.8 MB/Sec | 30947.23 GB |
| Process Page Fault Rate | 2643 F/Sec | 0 F/Sec | 3865 F/Sec | 1839866 F/Sec |
| Process Nonpaged Pool Used | 0.0 MB | 0.0 MB | 0.0 MB | --- |

**Εικόνα 6-8: Εργαλείο 1 (A3) – Απαιτήσεις σε υπολογιστικούς πόρους**

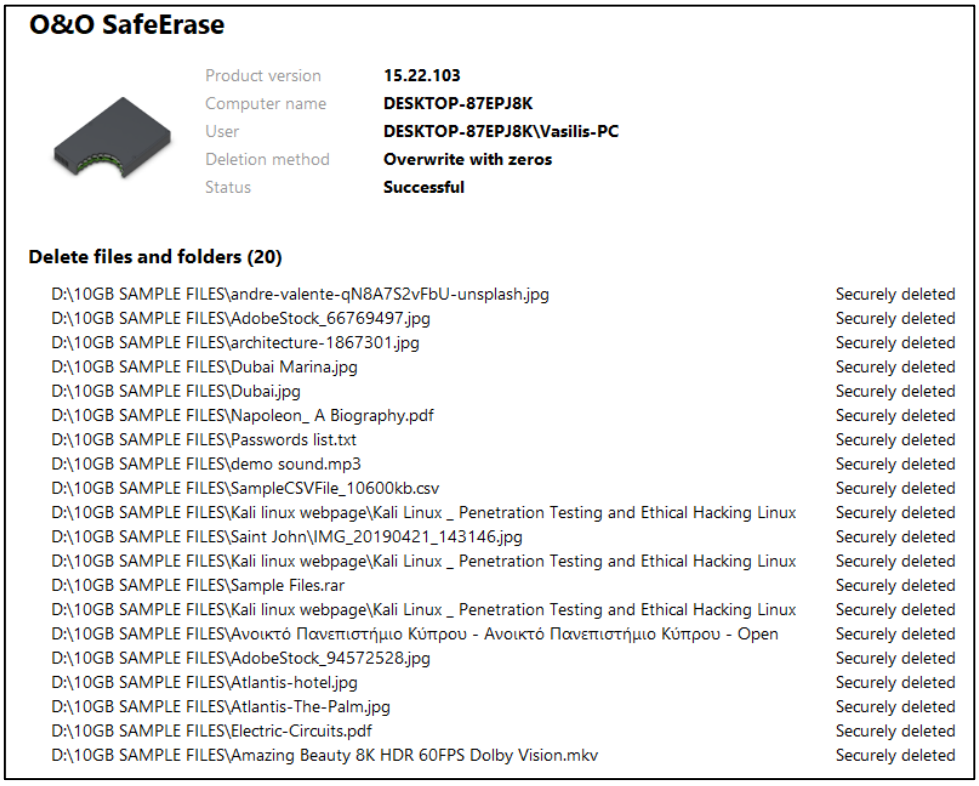
Χρόνος αποπεράτωσης διαγραφής : 42 λεπτά

### 6.1.2 Εργαλείο 2 - O&O SafeErase

Στο εργαλείο εκτελέστηκαν συνολικά τρία διαφορετικά σενάρια κατά τα οποία αξιολογήθηκαν οι δυνατότητες του για τις πιο κάτω περιπτώσεις:

- Αξιολόγηση 1 (A1) – Οριστική διαγραφή 20 προκαθορισμένων αρχείων από το δίσκο

Η διαδικασία οριστικής διαγραφής των αρχείων ολοκληρώθηκε επιτυχώς σύμφωνα με την αναφορά που δημιουργήθηκε από το εργαλείο με το πέρας της εργασίας.


O&O SafeErase

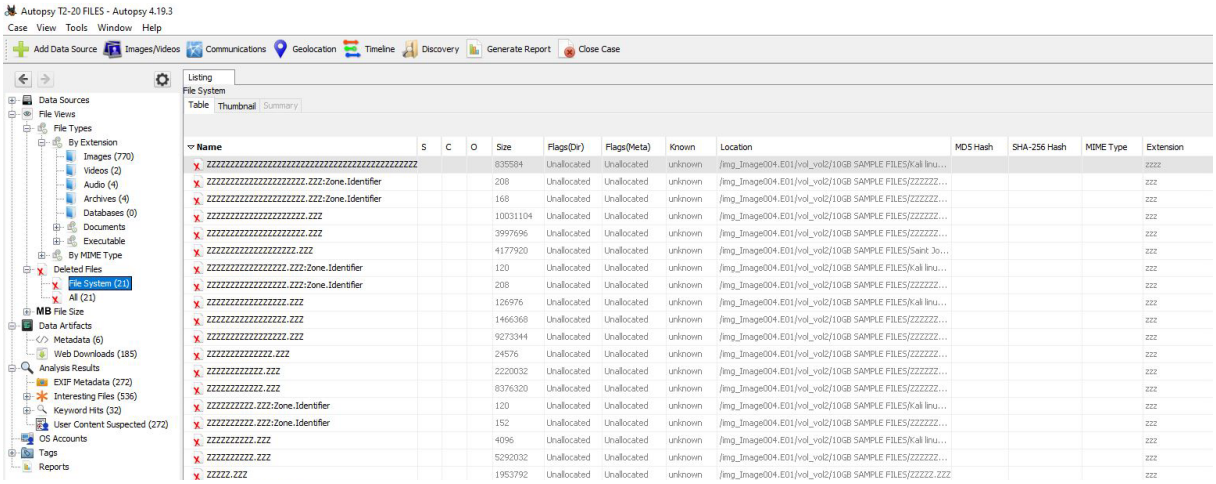
Product version 15.22.103
Computer name DESKTOP-87EPJ8K
User DESKTOP-87EPJ8K\Vasilis-PC
Deletion method Overwrite with zeros
Status Successful

Delete files and folders (20)

| | |
|---|---|
| D:\10GB SAMPLE FILES\andre-valente-qN8A7S2vFbU-unsplash.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\AdobeStock_66769497.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\architecture-1867301.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\Dubai Marina.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\Dubai.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\Napoleon_ A Biography.pdf | Securely deleted |
| D:\10GB SAMPLE FILES\Passwords list.txt | Securely deleted |
| D:\10GB SAMPLE FILES\demo sound.mp3 | Securely deleted |
| D:\10GB SAMPLE FILES\SampleCSVFile_10600kb.csv | Securely deleted |
| D:\10GB SAMPLE FILES\Kali linux webpage\Kali Linux _ Penetration Testing and Ethical Hacking Linux | Securely deleted |
| D:\10GB SAMPLE FILES\Saint John\IMG_20190421_143146.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\Kali linux webpage\Kali Linux _ Penetration Testing and Ethical Hacking Linux | Securely deleted |
| D:\10GB SAMPLE FILES\Sample Files.rar | Securely deleted |
| D:\10GB SAMPLE FILES\Kali linux webpage\Kali Linux _ Penetration Testing and Ethical Hacking Linux | Securely deleted |
| D:\10GB SAMPLE FILES\Ανοικτό Πανεπιστήμιο Κύπρου - Ανοικτό Πανεπιστήμιο Κύπρου - Open | Securely deleted |
| D:\10GB SAMPLE FILES\AdobeStock_94572528.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\Atlantis-hotel.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\Atlantis-The-Palm.jpg | Securely deleted |
| D:\10GB SAMPLE FILES\Electric-Circuits.pdf | Securely deleted |
| D:\10GB SAMPLE FILES\Amazing Beauty 8K HDR 60FPS Dolby Vision.mkv | Securely deleted |

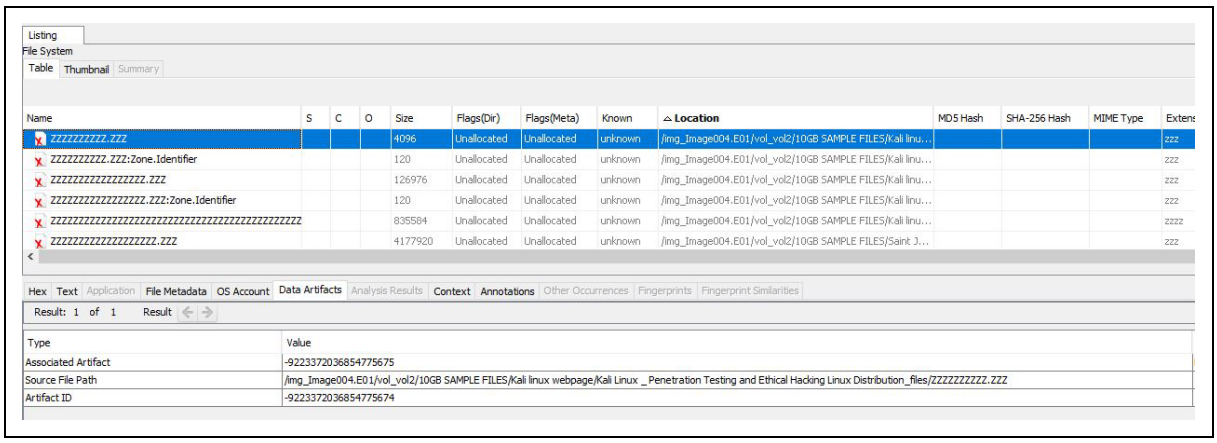
**Εικόνα 6-9: Εργαλείο 2 (A1) - O&O SafeErase - Αναφορά επιτυχημένης διαγραφής αρχείων**

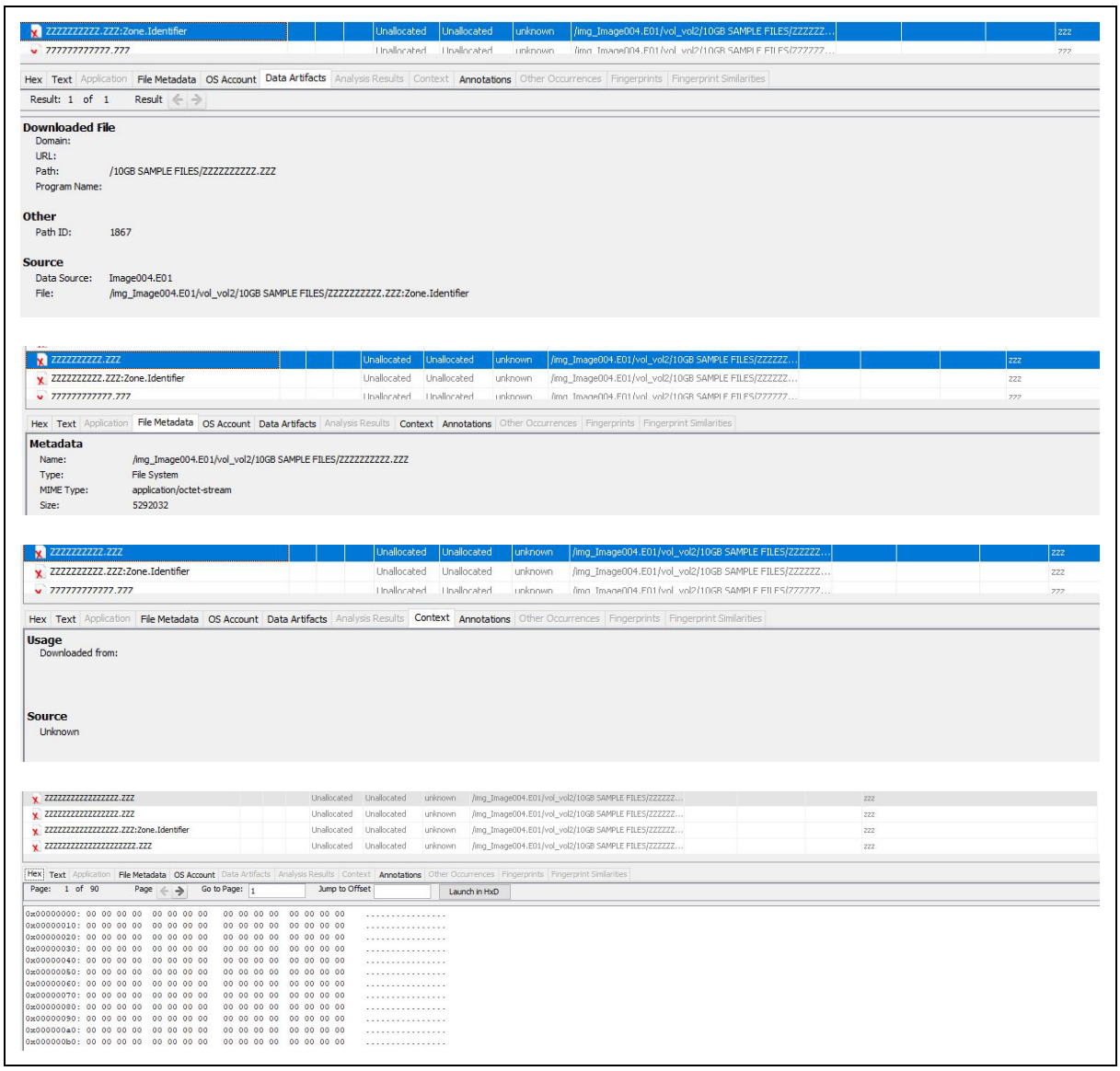
Από την ανάλυση της εικόνας του δίσκου η οποία λήφθηκε αμέσως μετά την διαγραφή των συγκεκριμένων αρχείων κάνοντας χρήση του δικανικού εργαλείου Autopsy διαφαίνεται ότι τα αρχεία έχουν οριστικά διαγραφεί. Δεν κατέστη δυνατή οποιαδήποτε επαναφορά σε κανένα από τα αρχεία ανεξαρτήτου μεγέθους. Το Autopsy ωστόσο εντόπισε διαγραφές αρχείων, τα οποία όμως δεν έφεραν καμιά πληροφορία σχετικά με τη ταυτότητα του αρχικού αρχείου. Οι καταχωρήσεις αυτές εντοπίζονται στην κατηγορία Deleted files στο Autopsy.




**Εικόνα 6-10: Εργαλείο 2 (Α1) - Autopsy - Καταχωρήσεις διαγραμμένων αρχείων**

Οι καταχωρίσεις των διαγραμμένων αρχείων που εντοπίστηκαν όπως φαίνεται και από το στιγμιότυπο πιο πάνω έχουν για όνομα αριθμό χαρακτήρων Z, ενώ καμιά άλλη πληροφορία δεν τα συνοδεύει. Αυτό φανερώνει ότι το εργαλείο στην περίπτωση διαγραφής αρχείων από το δίσκο έκανε εξαιρετική δουλεία. Παρακάτω παρουσιάζονται κάποια παραδείγματα από τα ευρήματα.

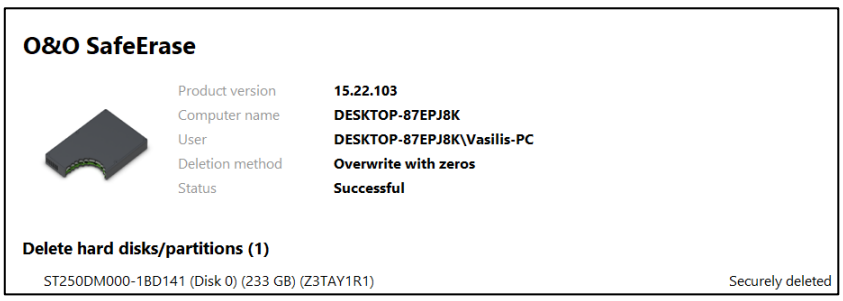





**Εικόνα 6-11: Εργαλείο 2 (A1) – Ευρήματα από τα διαγραμμένα αρχεία**

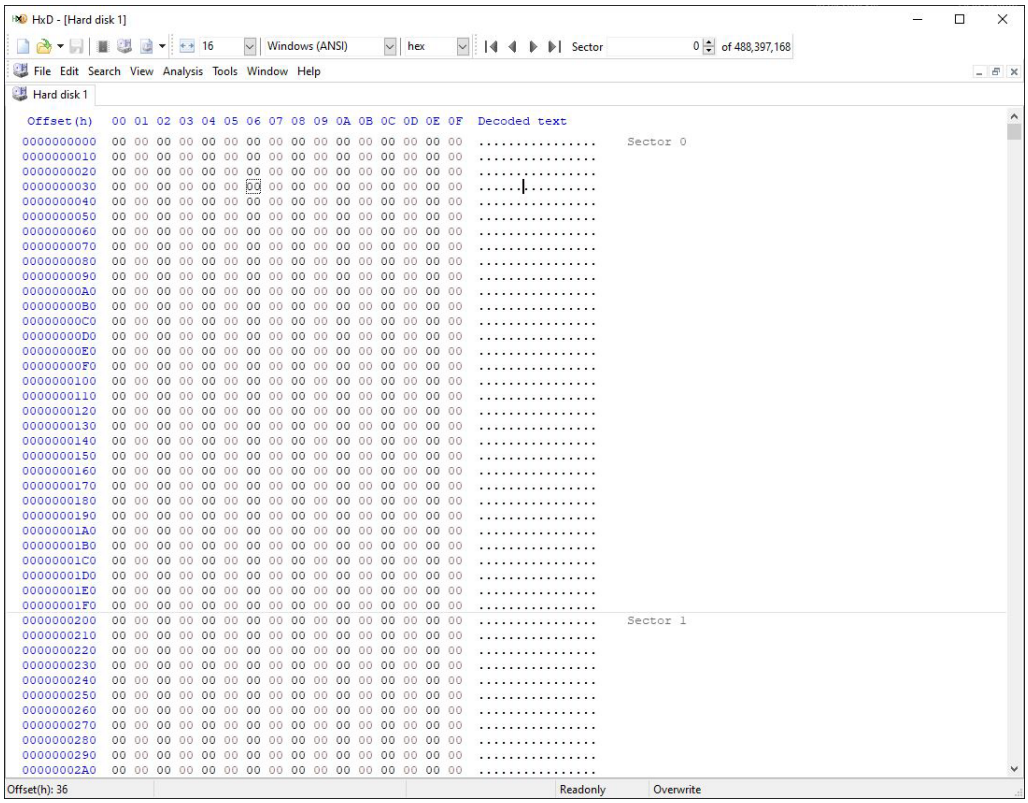
- Αξιολόγηση 2 (A2) – Οριστική διαγραφή ολόκληρου του δίσκου με 10GB δεδομένα

Η διαδικασία οριστικής διαγραφής ολόκληρου του δίσκου ολοκληρώθηκε επιτυχώς σύμφωνα με την αναφορά που δημιουργήθηκε από το εργαλείο με το πέρας της εργασίας.




**Εικόνα 6-12: Εργαλείο 2 (A2) – O&O SafeErase - Αναφορά επιτυχημένης διαγραφής δίσκου - 10GB δεδομένων**

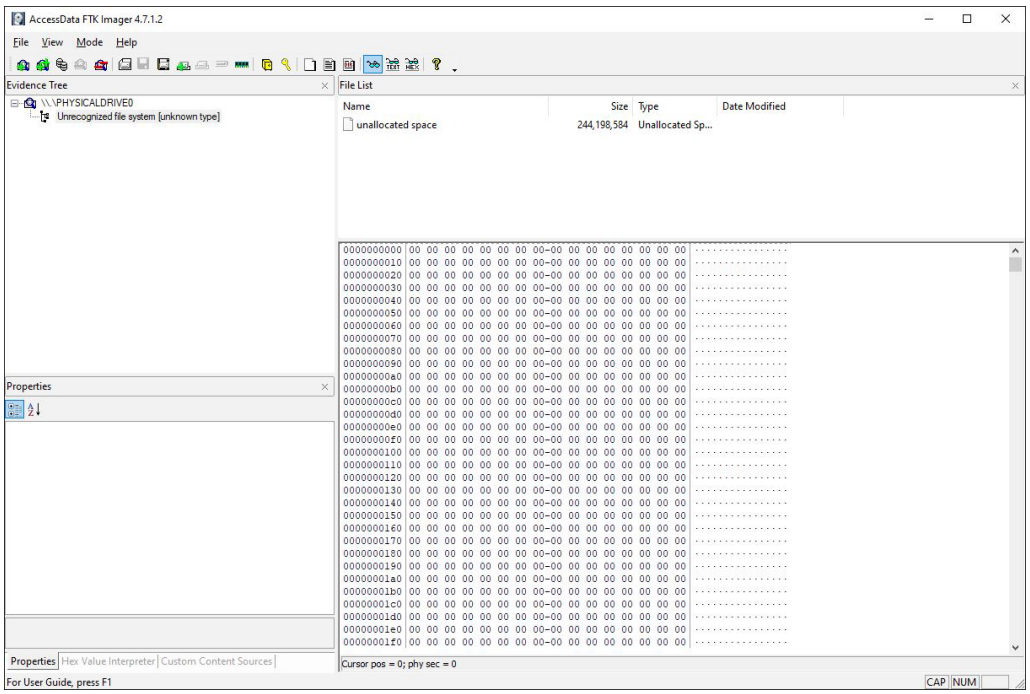
Μετά την διαγραφή ολόκληρου του δίσκου και την εξαγωγή της εικόνας του, προχωρήσαμε σε ανάλυση της με το εργαλείο δικανικής Autopsy. Παράλληλα ανοίξαμε το δίσκο με το εργαλείο HxD για να έχουμε οπτική απεικόνισή των περιεχομένων του. Έχοντας κάνει χρήση του αλγόριθμού διαγραφής One Pass Zero κατά την διαγραφή του δίσκου αναμένουμε για μια πετυχημένη οριστική διαγραφή όλα τα bits στον δίσκο να είναι γραμμένα με μηδέν.




**Εικόνα 6-13: Εργαλείο 2 (A2) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

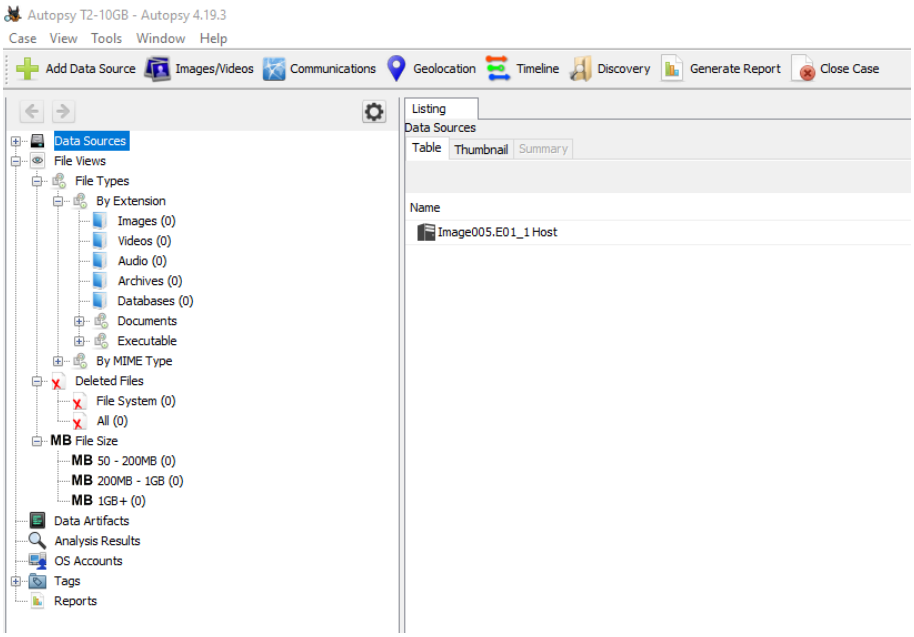
Από την απεικόνιση των περιεχομένων παρατηρούμε ότι όλοι οι τομείς (sectors) είναι διαγραμμένοι. Επίσης θα πρέπει να αναφερθεί ότι ακόμα και ο MBR (Master Boot Sector) που βρισκόταν στο αρχικό τομέα του δίσκου έχει επίσης διαγραφεί με επιτυχία.

Τον διαγραμμένο δίσκο ανοίξαμε επίσης και με το AccessData FTK Imager για να εξετάσουμε το περιεχόμενο του. Τα αποτελέσματα είναι όμοια με το προηγούμενο εργαλείο HxD .




**Εικόνα 6-14: Εργαλείο 2 (Α2) – AccessData FTK Imager – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Τα πιο πάνω επιβεβαίωσε και η ανάλυση της εικόνας του δίσκου που πραγματοποιήθηκε με την βοήθεια του εργαλείου Autopsy. Σύμφωνα λοιπόν με αυτή στον δίσκο δεν παρέμεινε κανένα αρχείο. . Η περεταίρω ανάλυση της εικόνας με το εργαλείο δικανικής Bulk Extractor εκ του αποτελέσματος κρίνεται αχρείαστη.




**Εικόνα 6-15: Εργαλείο 2 (Α2) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

OOSE - Process Counters

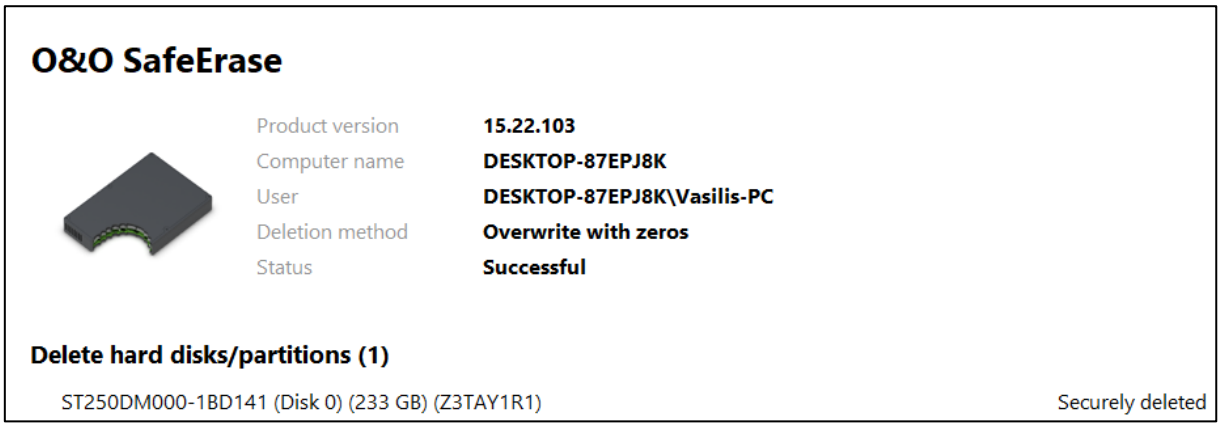
| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 3.1 % | 0.0 % | 8.9 % | --- |
| Process Memory Used | 60.28 MB | 0.00 MB | 60.29 MB | --- |
| Process Thread Count | 8 | 0 | 11 | --- |
| Process Handle Count | 624 | 0 | 624 | --- |
| Process Data Rate | 47533.2 MB/Sec | 0.1 MB/Sec | 68475.9 MB/Sec | 31116.17 GB |
| Process Read Rate | 0.1 MB/Sec | 0.0 MB/Sec | 0.5 MB/Sec | 31.6 MB |
| Process Write Rate | 47533.1 MB/Sec | 0.0 MB/Sec | 68475.9 MB/Sec | 31116.17 GB |
| Process Page Fault Rate | 19 F/Sec | 0 F/Sec | 543 F/Sec | 8717 F/Sec |
| Process Nonpaged Pool Used | 0.1 MB | 0.1 MB | 0.1 MB | --- |

**Εικόνα 6-16: Εργαλείο 2 (A2) – Απαιτήσεις σε υπολογιστικούς πόρους**

Χρόνος αποπεράτωσης διαγραφής: 38 λεπτά , 44 δευτερόλεπτα

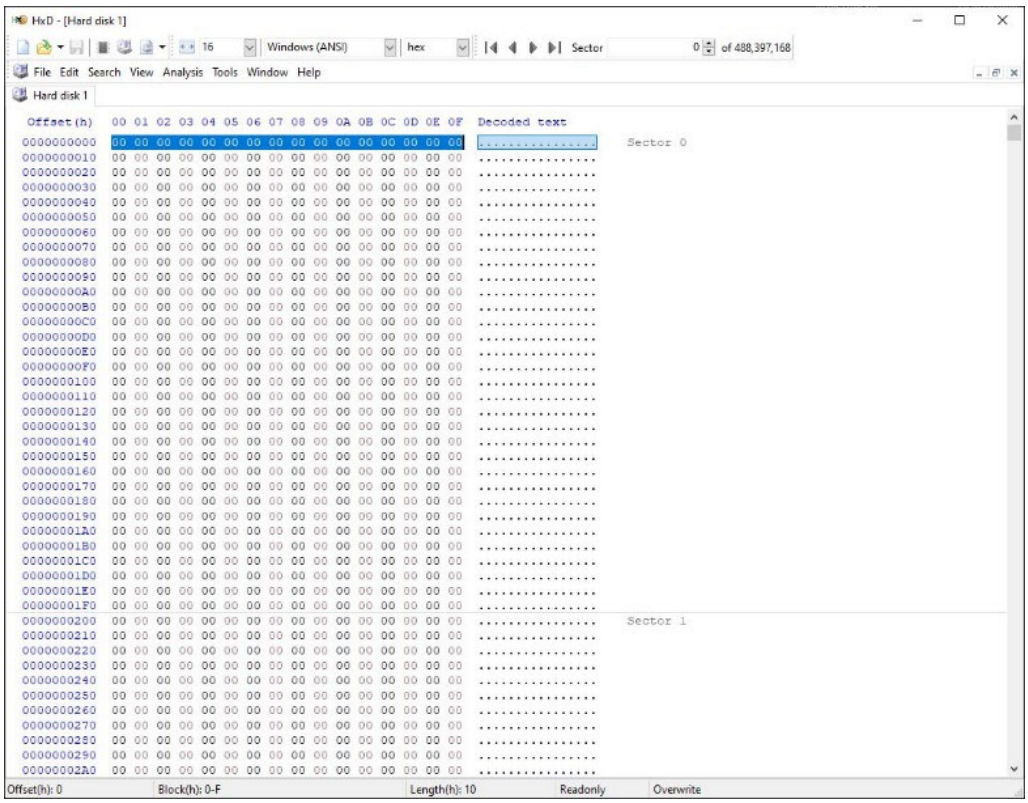
- Αξιολόγηση 3 (A3) – Οριστική διαγραφή ολόκληρου του δίσκου με 200GB δεδομένα

Η διαδικασία οριστικής διαγραφής ολόκληρου του δίσκου ο οποίος περιείχε 200GB δεδομένων ολοκληρώθηκε επιτυχώς σύμφωνα με την αναφορά που δημιουργήθηκε από το εργαλείο με το πέρας της εργασίας.



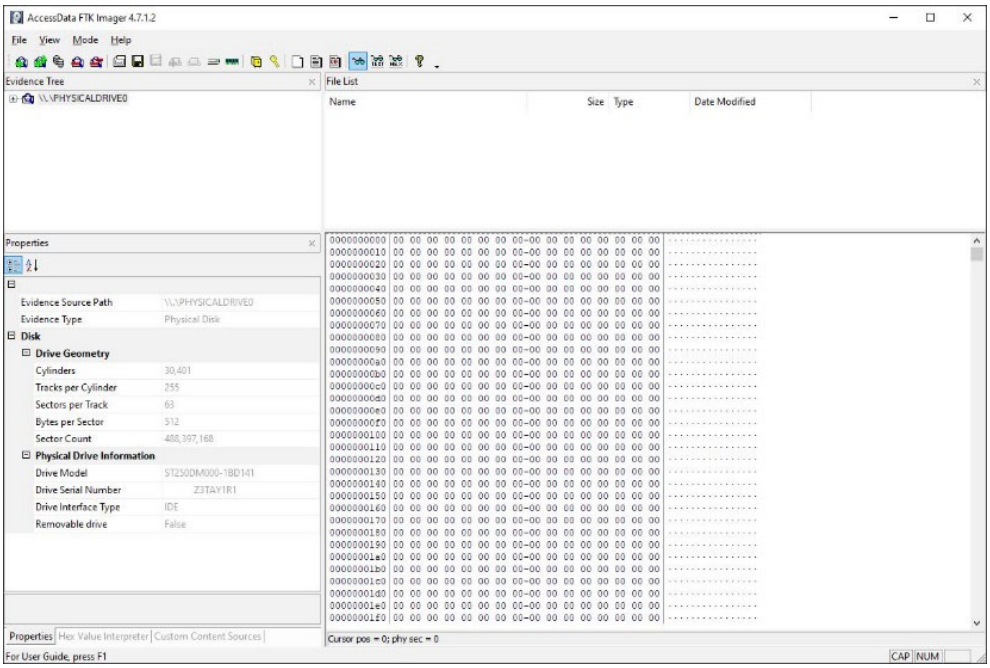

**Εικόνα 6-17: Εργαλείο 2 (A3) – O&O SafeErase - Αναφορά επιτυχημένης διαγραφής δίσκου - 200GB δεδομένων**

Τα αποτελέσματα από την ολική διαγραφή του δίσκου με τα 200GB δεδομένων είναι όμοια με το προηγούμενο σενάριο του δίσκου στον οποίο περιέχονταν μόνο 10GB δεδομένων. Από την επισκόπηση του διαγραμμένου δίσκου με το εργαλείο HxD φαίνεται να έχουμε σε όλους τους τομείς ανεξαιρέτως γραμμένους με μηδενικά.



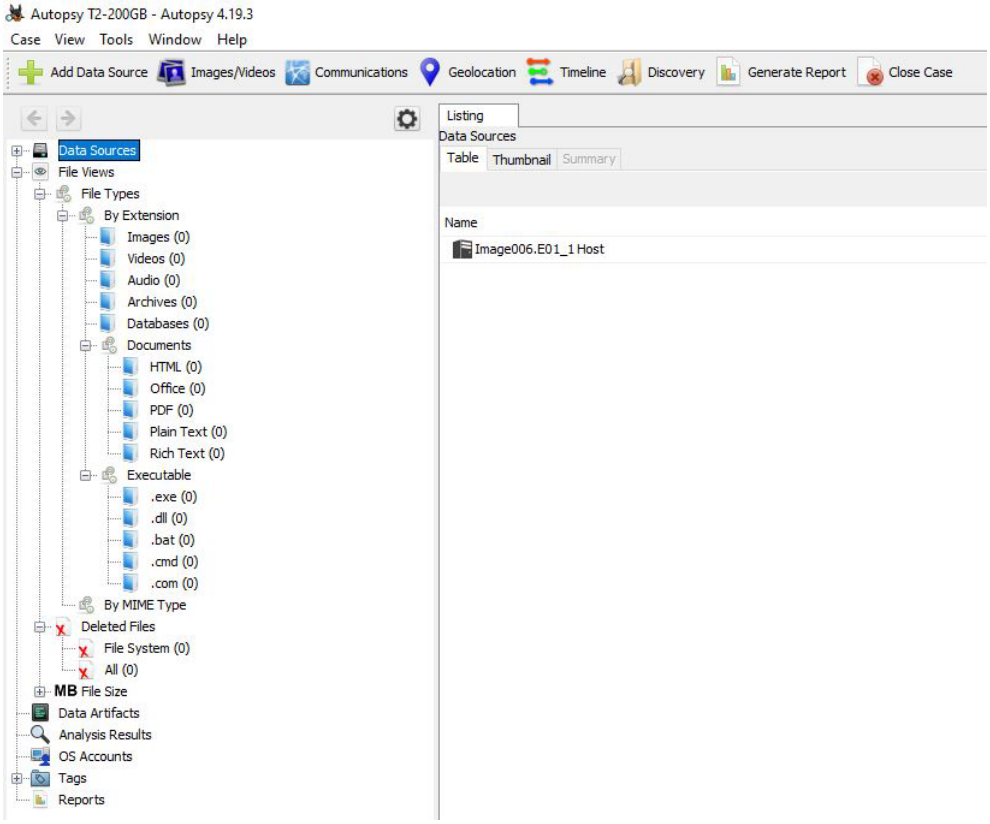

**Εικόνα 6-18: Εργαλείο 2 (A3) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Τα ίδια αποτελέσματα φανερώνει και το άνοιγμα του διαγραμμένου δίσκου με το AccessData FTK Imager.




**Εικόνα 6-19: Εργαλείο 2 (A3) – AccessData FTK Imager – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Τα πιο πάνω επιβεβαίωσε και η ανάλυση της εικόνας του δίσκου που πραγματοποιήθηκε με την βοήθεια του εργαλείου Autopsy. Σύμφωνα λοιπόν με αυτή στον δίσκο δεν παρέμεινε κανένα αρχείο.




**Εικόνα 6-20 Εργαλείο 2 (A3) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

Ο χρόνος αποπεράτωσης διαγραφής του δίσκου και οι απαιτήσεις σε υπολογιστικούς πόρους είναι τα ίδια με την ολική διαγραφή του δίσκου με 10GB δεδομένα σε αυτόν.

OOSE - Process Counters

| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 3.1 % | 0.0 % | 8.9 % | --- |
| Process Memory Used | 60.28 MB | 0.00 MB | 60.29 MB | --- |
| Process Thread Count | 8 | 0 | 11 | --- |
| Process Handle Count | 624 | 0 | 624 | --- |
| Process Data Rate | 47533.2 MB/Sec | 0.1 MB/Sec | 68475.9 MB/Sec | 31116.17 GB |
| Process Read Rate | 0.1 MB/Sec | 0.0 MB/Sec | 0.5 MB/Sec | 31.6 MB |
| Process Write Rate | 47533.1 MB/Sec | 0.0 MB/Sec | 68475.9 MB/Sec | 31116.17 GB |
| Process Page Fault Rate | 19 F/Sec | 0 F/Sec | 543 F/Sec | 8717 F/Sec |
| Process Nonpaged Pool Used | 0.1 MB | 0.1 MB | 0.1 MB | --- |

**Εικόνα 6-21: Εργαλείο 2 (A3) – Απαιτήσεις σε υπολογιστικούς πόρους**

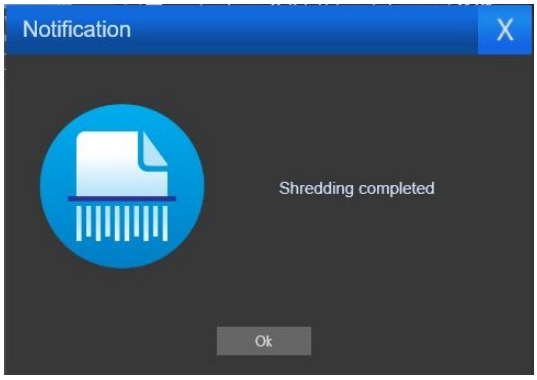
Χρόνος αποπεράτωσης διαγραφής : 38 λεπτά , 44 δευτερόλεπτα

### 6.1.3 Εργαλείο 3 – Easy File Shredder

Στο εργαλείο εκτελέστηκαν συνολικά τρία διαφορετικά σενάρια κατά τα οποία αξιολογήθηκαν οι δυνατότητες του για τις πιο κάτω περιπτώσεις:

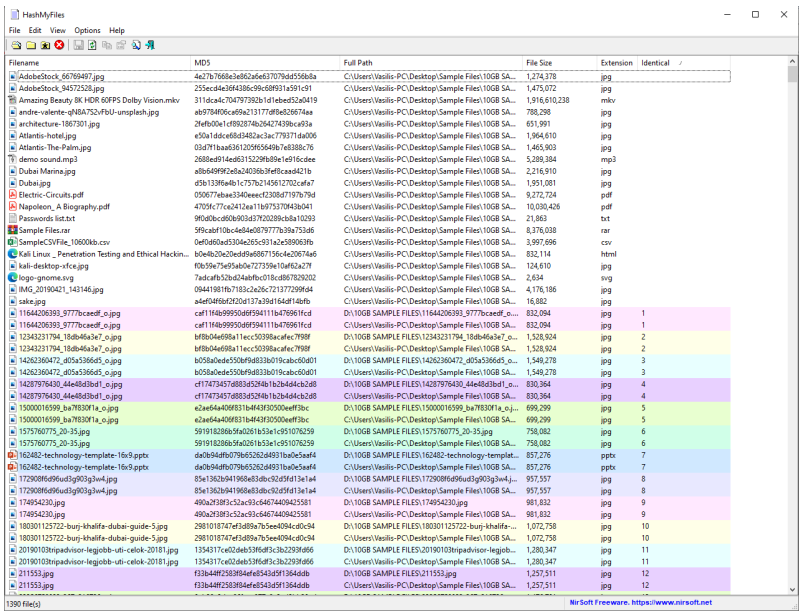
- Αξιολόγηση 1 (A1) – Οριστική διαγραφή 20 προκαθορισμένων αρχείων από το δίσκο

Η διαδικασία οριστικής διαγραφής των αρχείων ολοκληρώθηκε επιτυχώς σύμφωνα με την αναφορά που δημιουργήθηκε από το εργαλείο με το πέρας της εργασίας.



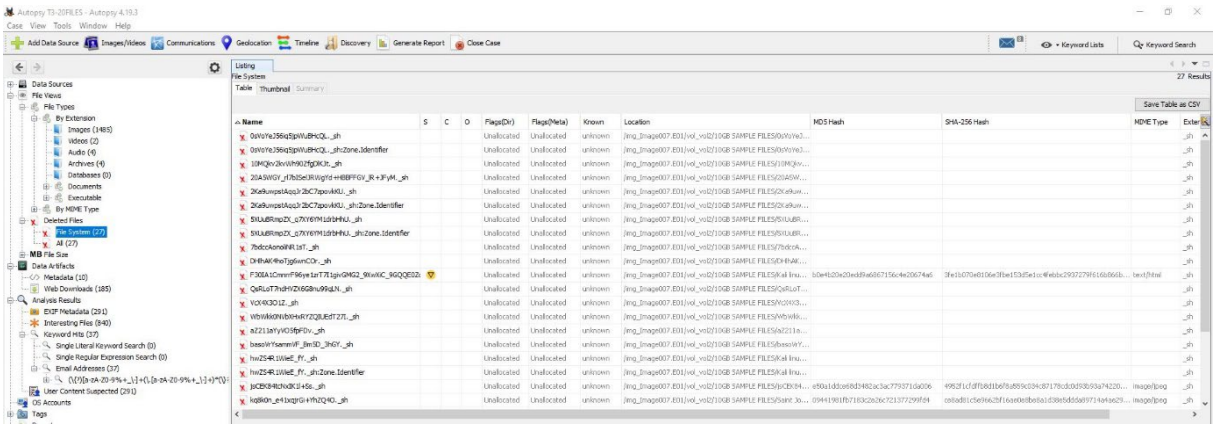

**Εικόνα 6-22: Εργαλείο 3 (A1) - Αναφορά επιτυχημένης διαγραφής αρχείων**

Με μια πρώτη εξέταση στα περιεχόμενα του δίσκου μέσω των Windows, τα 20 αρχεία που επιλέξαμε για διαγραφή δεν βρίσκονται στο δίσκο. Το ίδιο κατέδειξε και η εισαγωγή των εναπομεινάντων αρχείων του δίσκου μαζί με τα αρχικά στο εργαλείο HashMyFiles όπου η σύγκριση έδειξε ότι από το δίσκο έλειπαν τα 20 αρχεία.




**Εικόνα 6-23: Εργαλείο 3 (A1) - HashMyFiles - Σύγκριση αρχείων**

Ωστόσο από την ανάλυση της εικόνας του δίσκου η οποία λήφθηκε αμέσως μετά την διαγραφή των συγκεκριμένων αρχείων κάνοντας χρήση του δικανικού εργαλείου Autopsy διαφαίνεται ότι τα πλείστα από τα αρχεία ΔΕΝ έχουν οριστικά διαγραφεί. Συγκεκριμένα το Autopsy εντόπισε και κατέγραψε 27 αρχεία τα οποία και κατηγοριοποίησε ως διαγραμμένα αρχεία (Deleted Files).

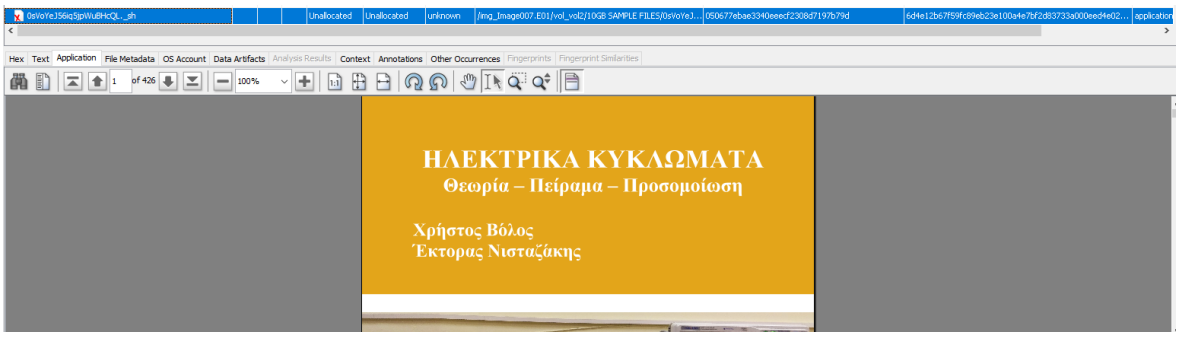


**Εικόνα 6-24: Εργαλείο 3 (Α1) - Autopsy - Καταχωρήσεις διαγραμμένων αρχείων**

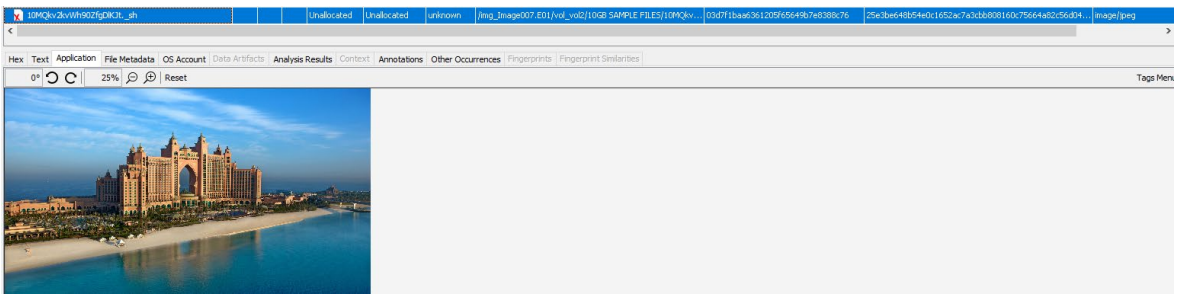
Τα αρχεία αυτά παρόλο που τα ονόματα τους έχουν εντελώς αλλοιωθεί, εντούτοις διατηρούν ανέπαφα όλα τα δεδομένα σε αυτά.

Μερικά από τα ευρήματα παρουσιάζονται πιο κάτω:

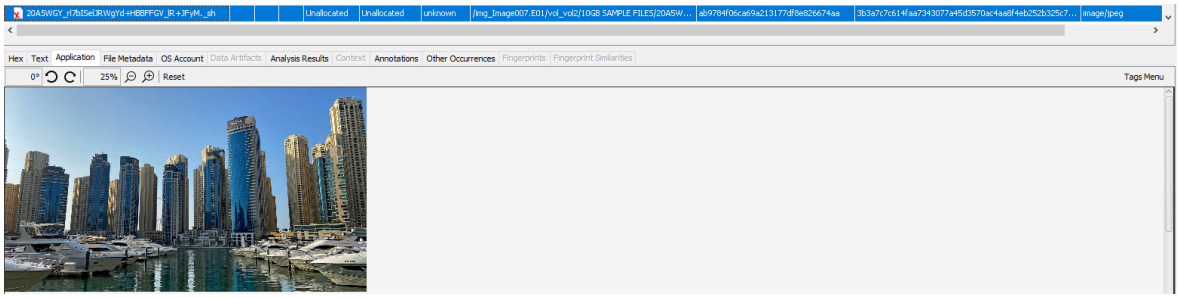
Αρχείο : Electric-Circuits.pdf / MD5: 050677ebae3340eeecf2308d7197b79d



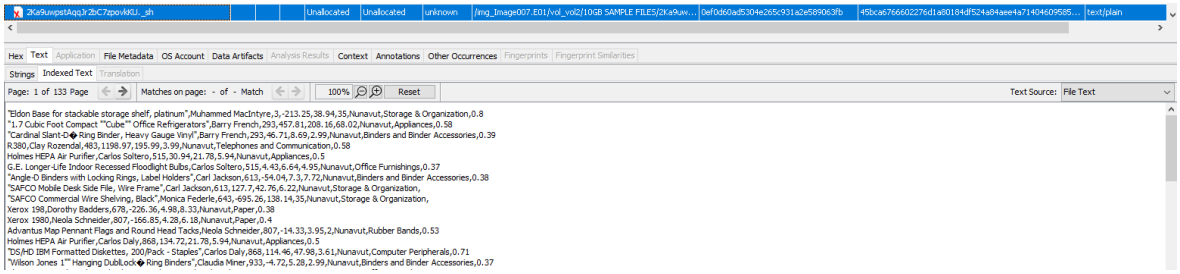

Αρχείο : Atlantis-The-Palm.jpg / MD5: 03d7f1baa6361205f65649b7e8388c76



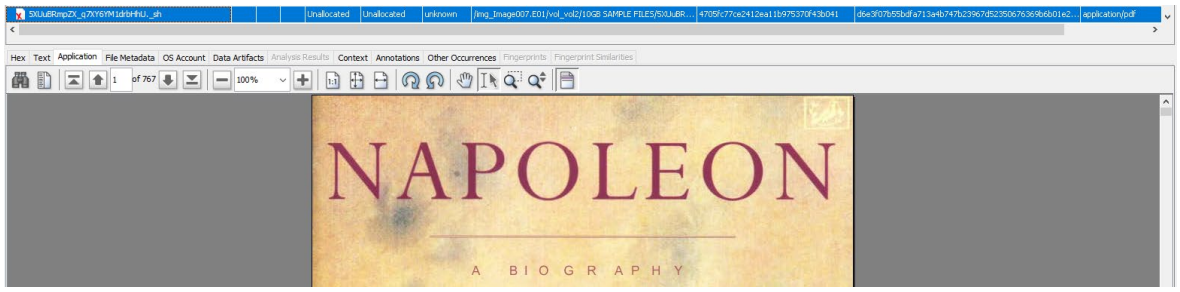
Αρχείο : andre-valente-qN8A7S2vFbU-unsplash.jpg / MD5: ab9784f06ca69a213177df8e826674aa



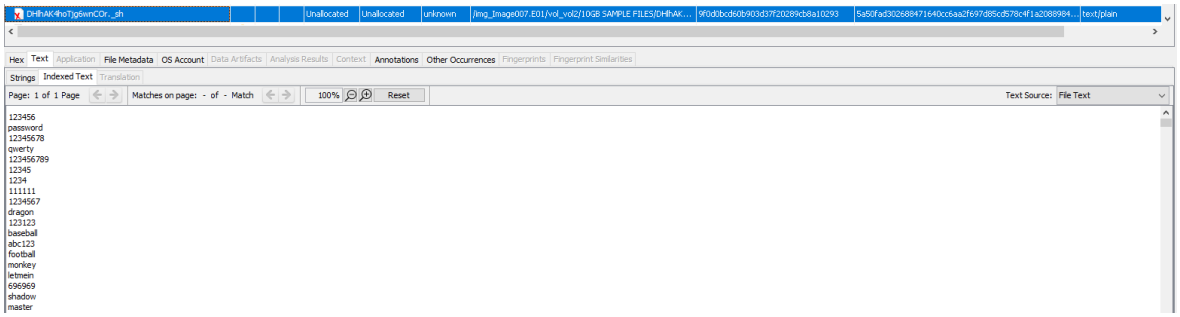
Αρχείο : SampleCSVFile_10600kb.csv / MD5: 0ef0d60ad5304e265c931a2e589063fb



Αρχείο : Napoleon_ A Biography.pdf / MD5: 4705fc77ce2412ea11b975370f43b041




Αρχείο : Passwords list.txt / MD5: 9f0d0bcd60b903d37f20289cb8a10293



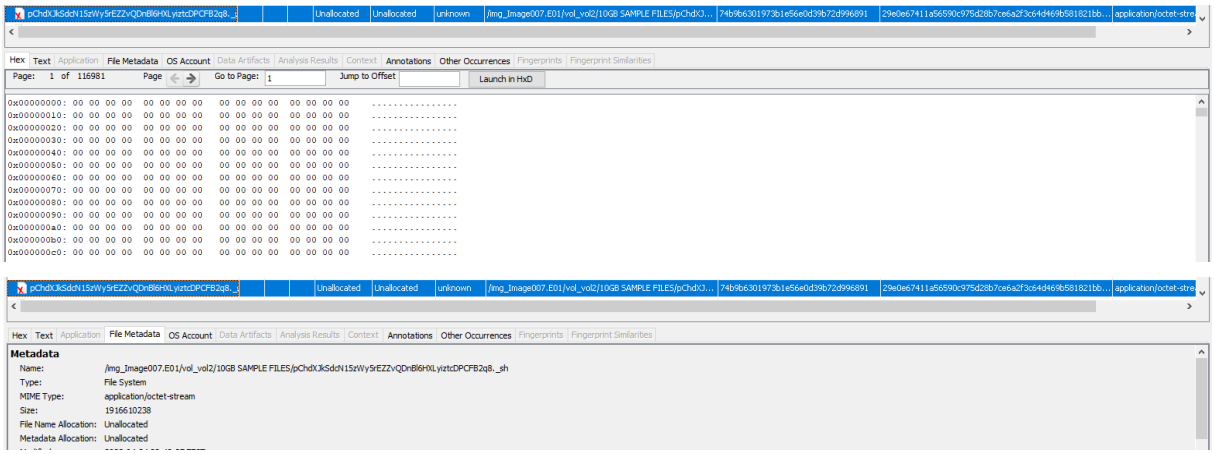
**Εικόνα 6-25: Εργαλείο 3 (A1) – Ευρήματα από τα διαγραμμένα αρχεία**

Εκτός από τα πιο πάνω εντοπίστηκαν επίσης τα ακόλουθα αρχεία:

| Αρχείο | MD5 |
|---|---|
| Atlantis-hotel.jpg | e50a1ddce68d3482ac3ac779371da006 |
| kali-desktop-xfce.jpg | f0b59e75e95ab0e727359e10af62a27f |
| Dubai Marina.jpg | a8b649f9f2e8a24036b3fef8caad421b |
| architecture-1867301.jpg | 2fefb00e1cf892874b26427439bca93a |
| Dubai.jpg | d5b133f6a4b1c757b2145612702cafa7 |
| IMG_20190421_143146.jpg | 09441981fb7183c2e26c721377299fd4 |
| AdobeStock_94572528.jpg | 255ecd4e36f4386c99c68f931a591c91 |
| AdobeStock_66769497.jpg | 4e27b7668e3e862a6e637079dd556b8a |
| sake.jpg | a4ef04f6bf2f20d137a39d164df14bfb |
| Kali Linux _ Penetration Testing and Ethical Hacking Linux Distribution.html | b0e4b20e20edd9a6867156c4e20674a6 |
| demo sound.mp3 | 2688ed914ed6315229fb89e1e916cdee |

**Πίνακας 6-1: Εργαλείο 3 (A1) – Επιπλέον ευρήματα από τα διαγραμμένα αρχεία**

Να αναφέρουμε ότι το αρχείο βίντεο "Amazing Beauty 8K HDR 60FPS Dolby Vision.mkv" το οποίο είχε μέγεθος 1,91GB διαγράφηκε με επιτυχία, αφού όπως φαίνεται και από το Autopsy ολόκληρο το περιεχόμενο του ξαναγράφτηκε με μηδέν.

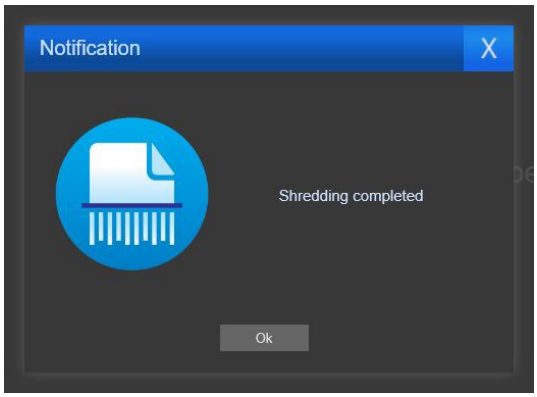



**Εικόνα 6-26: Εργαλείο 3 (A1) - Autopsy – Απόδειξη πλήρους διαγραφής συγκεκριμένου αρχείου**

Από τα συνολικά αποτελέσματα το εργαλείο απέτυχε στην επιλεκτική διαγραφή αρχείων, αφού περισσότερα από τα μισά αρχεία έχουν πλήρως ανακτηθεί με εξαίρεση τα αρχικά τους ονόματα.

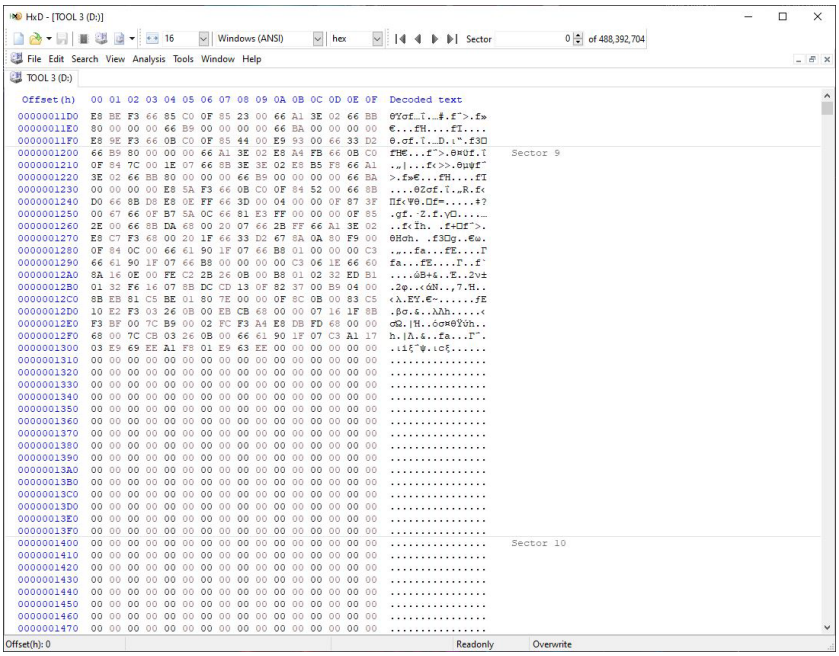
- Αξιολόγηση 2 (A2) – Οριστική διαγραφή ολόκληρου του δίσκου με 10GB δεδομένα

Έχοντας ολοκληρωθεί η διαδικασία οριστικής διαγραφής ολόκληρου του δίσκου, το εργαλείο μας ενημέρωσε εμφανίζοντας την πιο κάτω ειδοποίηση.



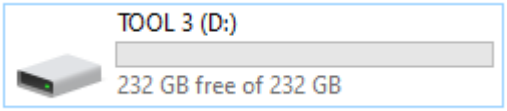

**Εικόνα 6-27: Εργαλείο 3 (A2) – Αναφορά επιτυχημένης διαγραφής δίσκου - 10GB δεδομένων**

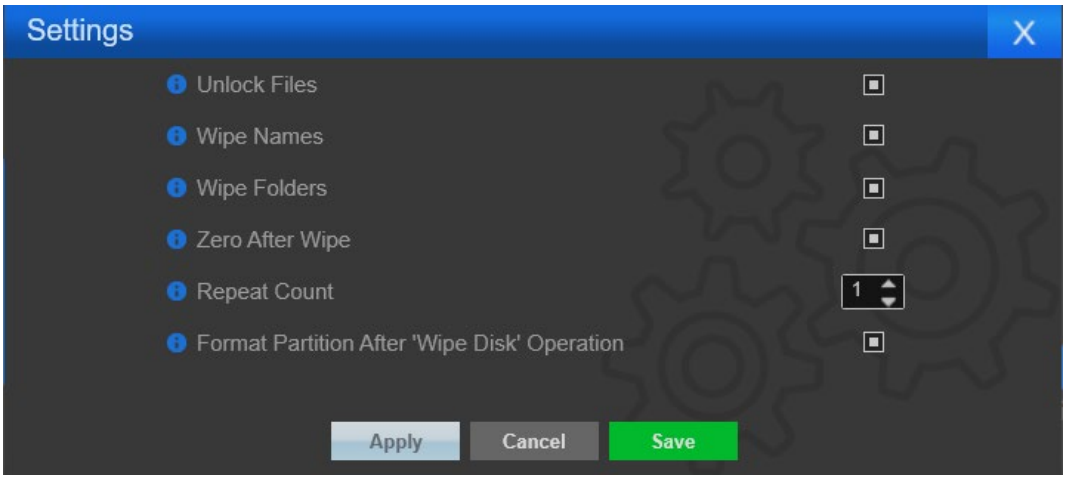
Προχωρήσαμε με ανάλυση της εικόνας του δίσκου, όπως επίσης επισκόπηση των περιεχομένων του δίσκου με το εργαλείο HxD. Σύμφωνα με αυτό οι πρώτοι εννέα sectors του δίσκου ήταν γραμμένοι με δεδομένα, ενώ ο υπόλοιπος δίσκος ήταν διαγραμμένος.




**Εικόνα 6-28: Εργαλείο 3 (A2) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

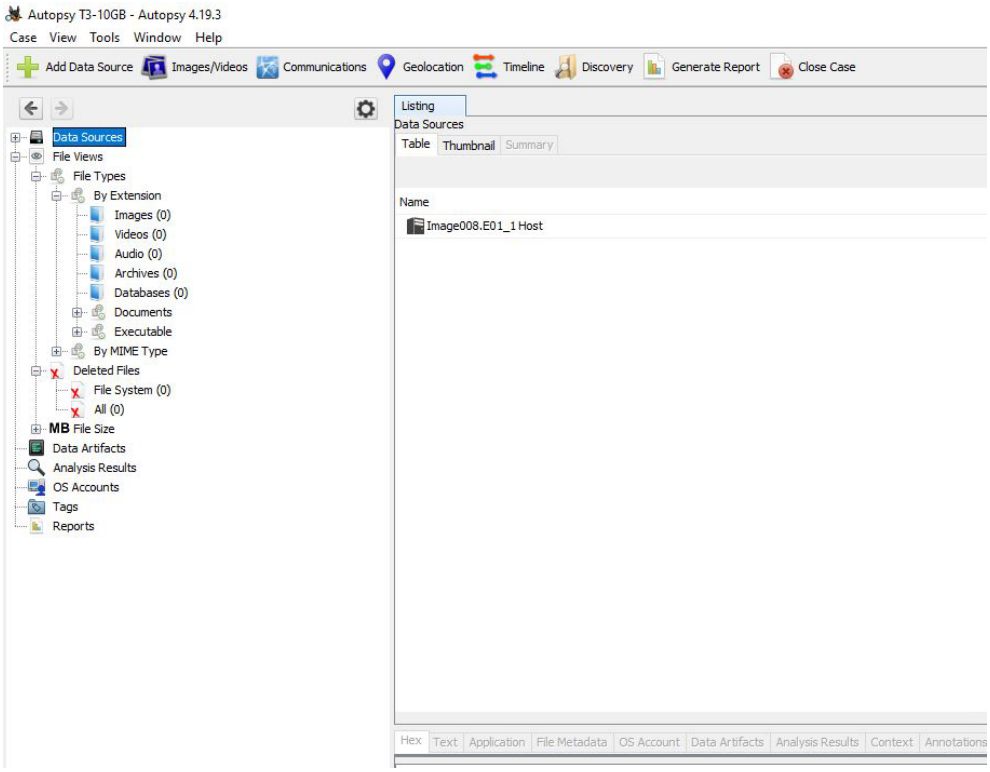
Αυτό οφείλεται στο γεγονός ότι το εργαλείο με το πέρας της διαδικασίας διαγραφής του, μορφοποιεί (formatting) το δίσκο, σύμφωνα με τις ρυθμίσεις που είχε πριν διαγραφεί. Έτσι τα δεδομένα στα αρχικά sectors αφορούν το MBR και το NTFS. Για αυτό το λόγο ο δίσκος διατήρησε και το όνομα του που είχε πριν την διαγραφή.




**Εικόνα 6-29: Εργαλείο 3 (A2) – Επιλογή μορφοποίησης δίσκου μετά την διαγραφή**

Προχωρήσαμε επίσης σε ανάλυση της με το εργαλείο δικανικής Autopsy, όπου σύμφωνα με αυτό δεν βρέθηκε κανένα αρχείο στο δίσκο.




**Εικόνα 6-30: Εργαλείο 3 (A2) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

ShredderUIWpf - Process Counters

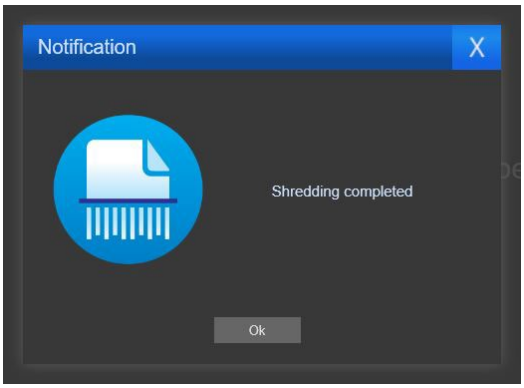
| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 0.6 % | 0.0 % | 14.5 % | --- |
| Process Memory Used | 203.1 MB | 0.0 MB | 208.3 MB | --- |
| Process Thread Count | 23 | 0 | 29 | --- |
| Process Handle Count | 833 | 0 | 871 | --- |
| Process Data Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.5 MB/Sec | 0.7 MB |
| Process Read Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.4 MB/Sec | 0.7 MB |
| Process Write Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB |
| Process Page Fault Rate | 178 F/Sec | 0 F/Sec | 59908 F/Sec | 126619 F/Sec |
| Process Nonpaged Pool Used | 0.1 MB | 0.0 MB | 0.1 MB | --- |

**Εικόνα 6-31: Εργαλείο 3 (A2) – Απαιτήσεις σε υπολογιστικούς πόρους**

Χρόνος αποπεράτωσης διαγραφής: 1ώρα, 20 λεπτά, 34 δευτερόλεπτα

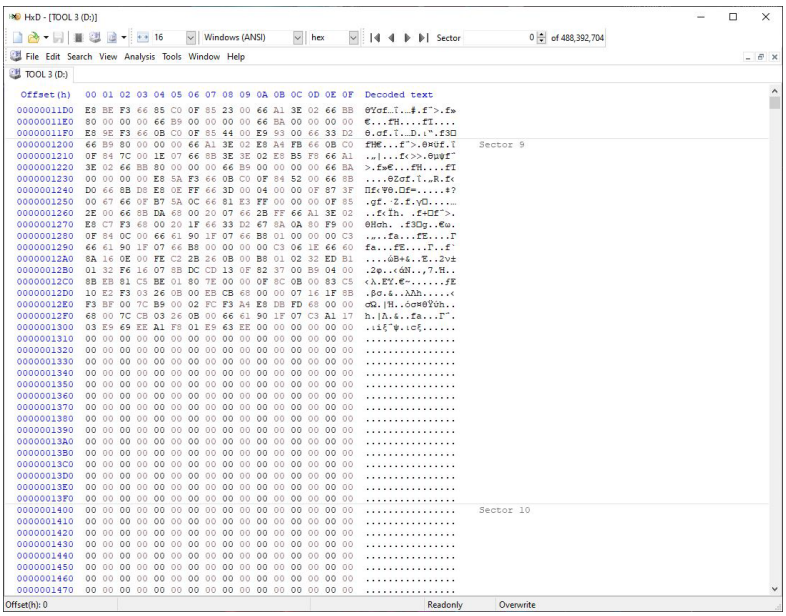
- Αξιολόγηση 3 (A3) – Οριστική διαγραφή ολόκληρου του δίσκου με 200GB δεδομένα

Με το πέρας της διαδικασίας οριστικής διαγραφής ολόκληρου του δίσκου, το εργαλείο μας ενημέρωσε για την ολοκλήρωση της εμφανίζοντας την πιο κάτω ειδοποίηση.



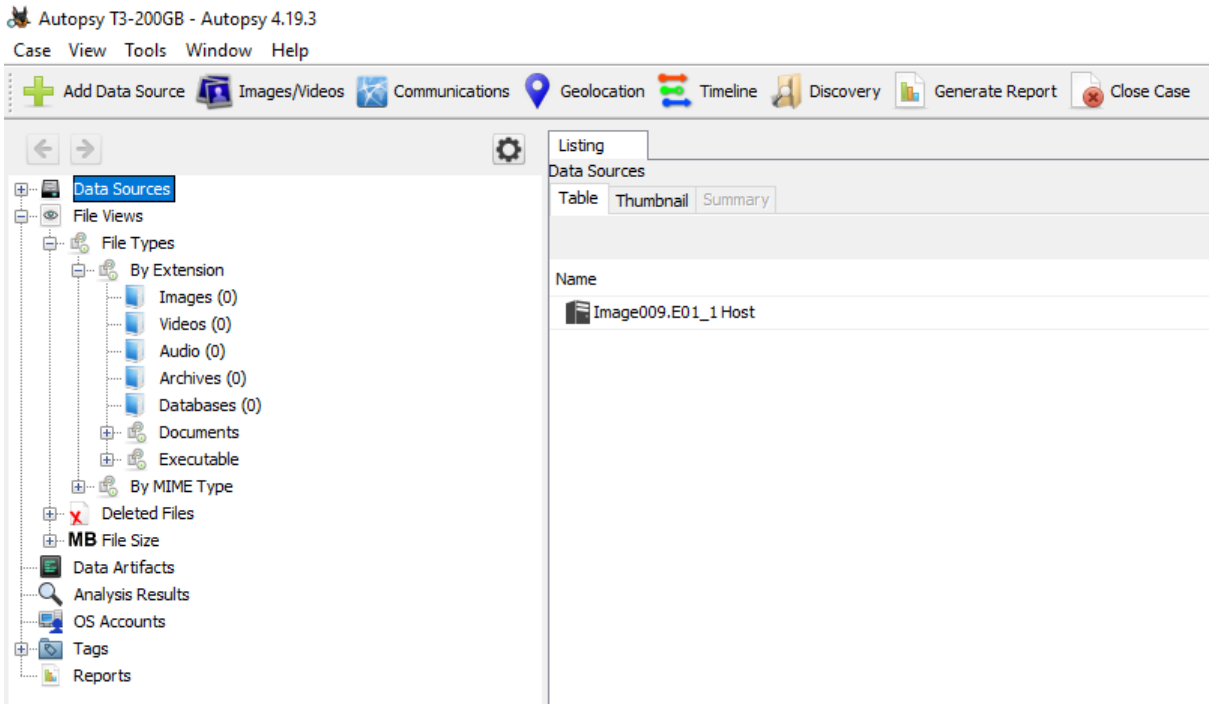

**Εικόνα 6-32: Εργαλείο 3 (A3) – Αναφορά επιτυχημένης διαγραφής δίσκου - 200GB δεδομένων**

Προχωρήσαμε με δημιουργία της εικόνας του δίσκου, όπως επίσης επισκόπηση των περιεχομένων του δίσκου με το εργαλείο HxD και Autopsy. Τα αποτελέσματα είναι όμοια με το προηγούμενο σενάριο όπου είχαμε τη ολική διαγραφή ολόκληρου του δίσκου ο οποίος περιείχε 10GB δεδομένων. Οι πρώτοι εννέα sectors του δίσκου, οι οποίοι αποτελούν το MBR και το NTFS ήταν γραμμένοι με δεδομένα, ενώ ο υπόλοιπος δίσκος ήταν διαγραμμένος.



**Εικόνα 6-33: Εργαλείο 3 (Α3) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Πέραν αυτών, οι υπόλοιποι sectors παρουσιάζονται να είναι όλοι μηδενικά. Έτσι και τα αποτελέσματα από την ανάλυση της εικόνας με το δικανικό εργαλείο Autopsy δεν αποκάλυψε κανένα αρχείο.




**Εικόνα 6-34: Εργαλείο 3 (Α3) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

ShredderUIWpf - Process Counters

| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 0.7 % | 0.0 % | 11.9 % | --- |
| Process Memory Used | 218.1 MB | 198.3 MB | 254.9 MB | --- |
| Process Thread Count | 21 | 19 | 24 | --- |
| Process Handle Count | 809 | 775 | 849 | --- |
| Process Data Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB/Sec | 0.7 MB |
| Process Read Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB/Sec | 0.7 MB |
| Process Write Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB |
| Process Page Fault Rate | 122 F/Sec | 0 F/Sec | 7765 F/Sec | 81159 F/Sec |
| Process Nonpaged Pool Used | 0.1 MB | 0.1 MB | 0.1 MB | --- |

**Εικόνα 6-35: Εργαλείο 3 (A3) – Απαιτήσεις σε υπολογιστικούς πόρους**

Χρόνος αποπεράτωσης διαγραφής : 1ώρα, 20 λεπτά, 34 δευτερόλεπτα

### 6.1.4 Εργαλείο 4 – TS DataWiper

Στο εργαλείο εκτελέστηκαν συνολικά τρία διαφορετικά σενάρια κατά τα οποία αξιολογήθηκαν οι δυνατότητες του για τις πιο κάτω περιπτώσεις:

- Αξιολόγηση 1 (A1) – Οριστική διαγραφή 20 προκαθορισμένων αρχείων από το δίσκο

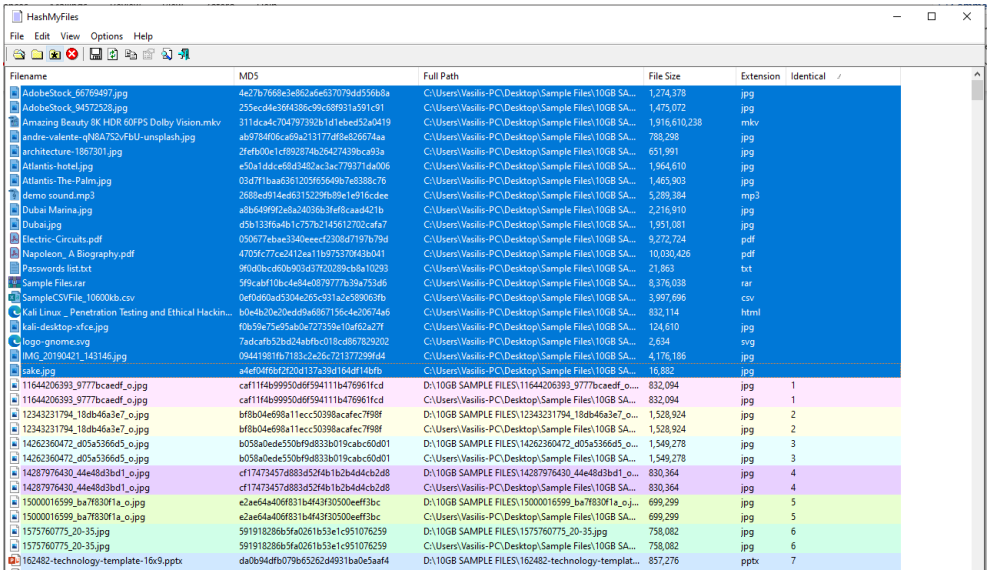
Η διαδικασία οριστικής διαγραφής των αρχείων σύμφωνα με το εργαλείο ολοκληρώθηκε επιτυχώς. Το ίδιο επιβεβαιώνει και η αναφορά που δημιουργήθηκε από το εργαλείο με το πέρας της εργασίας.

| | | |
|---|---|---|
| D:/10GB SAMPLE FILES/SampleCSVFile_10600kb.csv | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Sample Files.rar | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Ανοικτό Πανεπιστήμιο Κύπρου - Ανοικτό Πανεπιστήμιο Κύπρου - Open University of Cyprus_files/sake.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Passwords list.txt | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Napoleon_ A Biography.pdf | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Kali linux webpage/Kali Linux _ Penetration Testing and Ethical Hacking Linux Distribution_files/logo-gnome.svg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Kali linux webpage/Kali Linux _ Penetration Testing and Ethical Hacking Linux Distribution_files/kali-desktop-xfce.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Kali linux webpage/Kali Linux _ Penetration Testing and Ethical Hacking Linux Distribution.html | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Saint John/IMG_20190421_143146.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Electric-Circuits.pdf | HMG Infosec Standard 5 | Erased |

| | | |
|---|---|---|
| D:/10GB SAMPLE FILES/Dubai.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Dubai Marina.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/demo sound.mp3 | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Atlantis-The-Palm.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Atlantis-hotel.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/architecture-1867301.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/andre-valente-qN8A7S2vFbU-unsplash.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/Amazing Beauty 8K HDR 60FPS Dolby Vision.mkv | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/AdobeStock_94572528.jpg | HMG Infosec Standard 5 | Erased |
| D:/10GB SAMPLE FILES/AdobeStock_66769497.jpg | HMG Infosec Standard 5 | Erased |

**Εικόνα 6-36: Εργαλείο 4 (A1) - Αναφορά επιτυχημένης διαγραφής αρχείων**

Ως πρώτο βήμα εξετάσαμε τα περιεχόμενα του δίσκου μέσω Windows, όπου διαπιστώσαμε ότι τα 20 αρχεία που διαγράψαμε απουσίαζαν. Το ίδιο κατέδειξε και η εισαγωγή των εναπομεινάντων αρχείων του δίσκου μαζί με τα αρχικά στο εργαλείο HashMyFiles όπου η σύγκριση έδειξε ότι από το δίσκο έλειπαν τα 20 αρχεία.

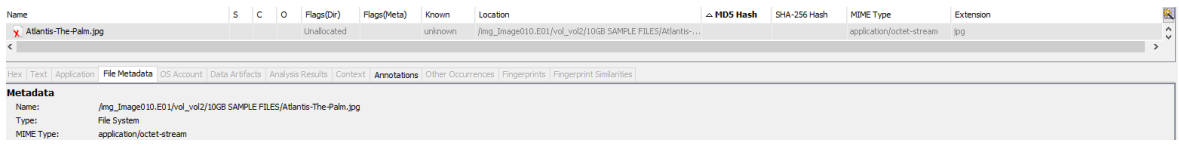



**Εικόνα 6-37: Εργαλείο 4 (A1) - HashMyFiles - Σύγκριση αρχείων**

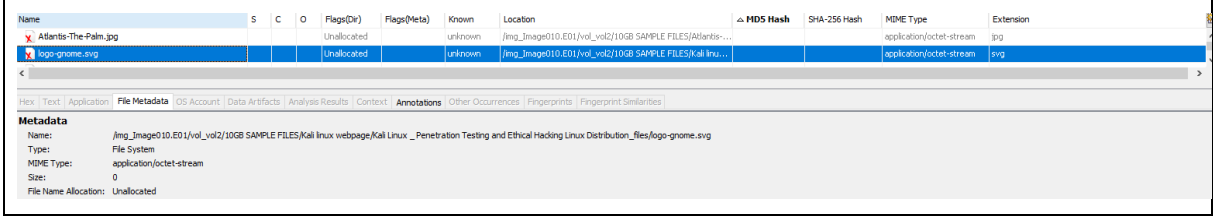
Από την ανάλυση της εικόνας του δίσκου, η οποία λήφθηκε αμέσως μετά την διαγραφή των συγκεκριμένων αρχείων κάνοντας χρήση του δικανικού εργαλείου Autopsy διαφαίνεται ότι το περιεχόμενο των αρχείων έχει οριστικά διαγραφεί αλλά σε κάποια από τα αρχεία διατηρήθηκαν σχετικές πληροφορίες με αυτά. Δύο από τα αρχεία διατήρησαν ακέραια τα αρχικά ονόματα τους και τον τύπο τους χωρίς ωστόσο να είναι δυνατή η ανάκτηση τους. Τα υπόλοιπα αρχεία που διαγράφηκαν, μετονομάστηκαν τόσο τα ονόματα τους όσο και ο τύπος τους σε togethershare. (Developer του εργαλείου TS DataWiper). Σε μερικά αρχεία διατηρήθηκαν πληροφορίες metadata οι οποίες φανέρωναν πληροφορίες για το αρχείο. Σε όλες τις περιπτώσεις όμως τα αρχεία καθαυτά είχαν διαγραφεί και καμιά πληροφορία για το περιεχόμενο τους δεν ήταν δυνατό να αποκτηθεί.

Μερικά από τα ευρήματα παρουσιάζονται πιο κάτω:

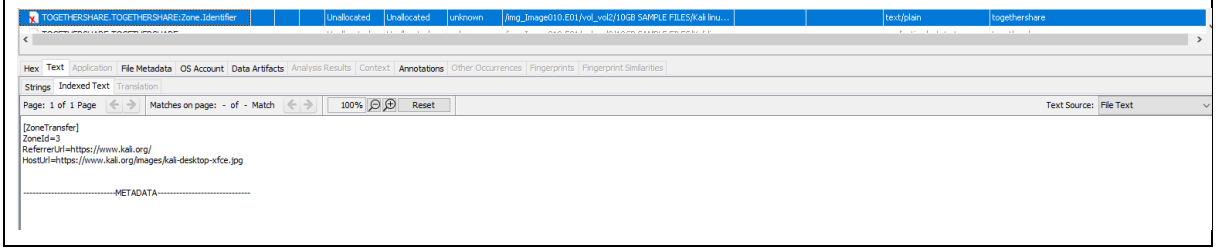
Αρχείο : Atlantis-The-Palm.jpg / MD5: 03d7f1baa6361205f65649b7e8388c76



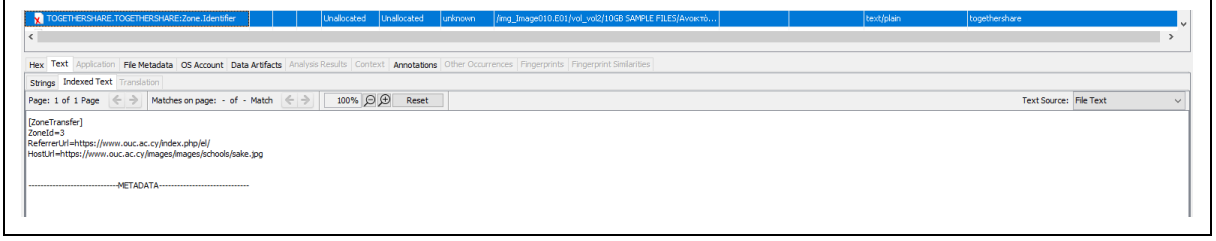

Αρχείο : logo-gnome.svg / MD5: 7adcafb52bd24abfbc018cd867829202



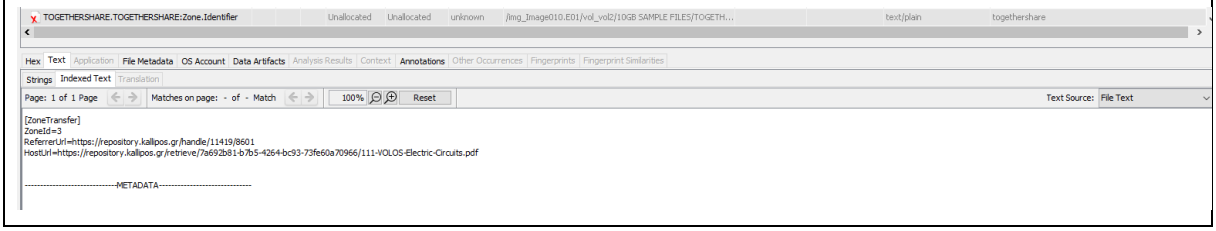
Αρχείο : kali-desktop-xfce.jpg / MD5: f0b59e75e95ab0e727359e10af62a27f



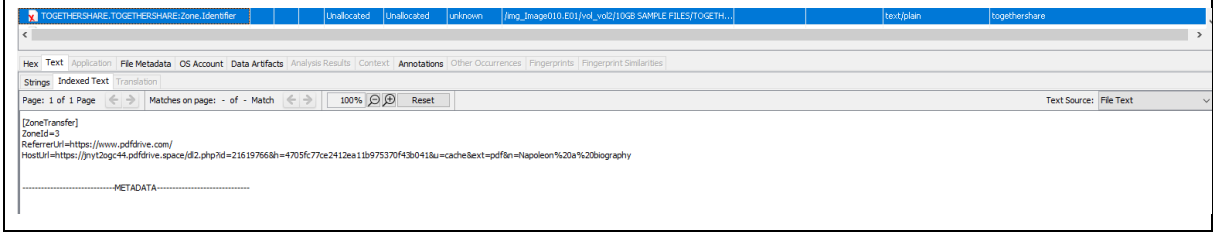

Αρχείο : sake.jpg / MD5: a4ef04f6bf2f20d137a39d164df14bfb




Αρχείο : Electric-Circuits.pdf / MD5: 050677ebae3340eeecf2308d7197b79d




Αρχείο : Napoleon_ A Biography.pdf / MD5: 4705fc77ce2412ea11b975370f43b041




**Εικόνα 6-38: Εργαλείο 4 (A1) – Ευρήματα από τα διαγραμμένα αρχεία**

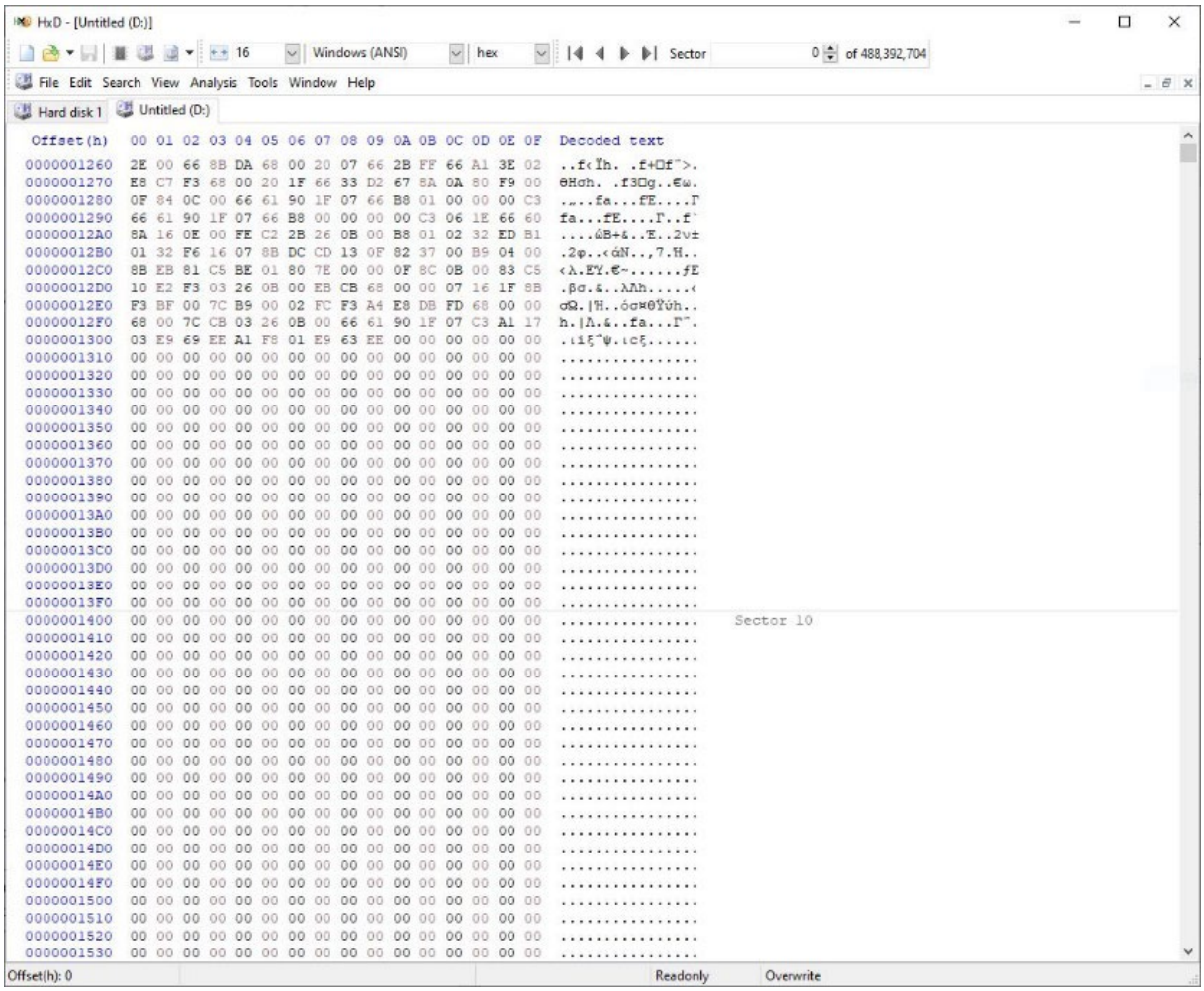
- Αξιολόγηση 2 (A2) – Οριστική διαγραφή ολόκληρου του δίσκου με 10GB δεδομένα

Η διαδικασία οριστικής διαγραφής του δίσκου σύμφωνα με το εργαλείο ολοκληρώθηκε επιτυχώς. Το ίδιο επιβεβαιώνει και η αναφορά που δημιουργήθηκε από το εργαλείο με το πέρας της εργασίας.

| | | |
|---|---|---|
| wipe partition D | HMG Infosec Standard 5 | Erased |

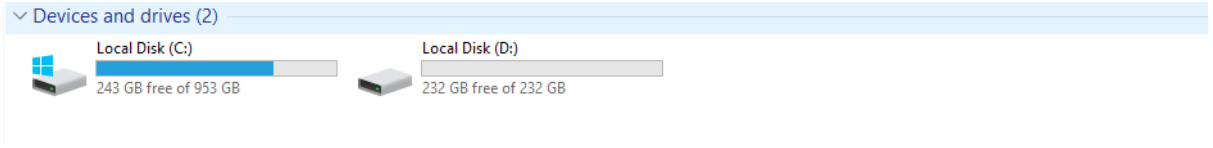
**Εικόνα 6-39: Εργαλείο 4 (A2) – Αναφορά επιτυχημένης διαγραφής δίσκου - 10GB δεδομένων**

Προχωρήσαμε σε ανάλυση της εικόνας του δίσκου, όπως επίσης επισκόπηση των περιεχομένων του δίσκου με το εργαλείο HxD. Σύμφωνα με αυτό οι πρώτοι εννέα sectors του δίσκου ήταν γραμμένοι με δεδομένα, ενώ ο υπόλοιπος δίσκος ήταν διαγραμμένος.

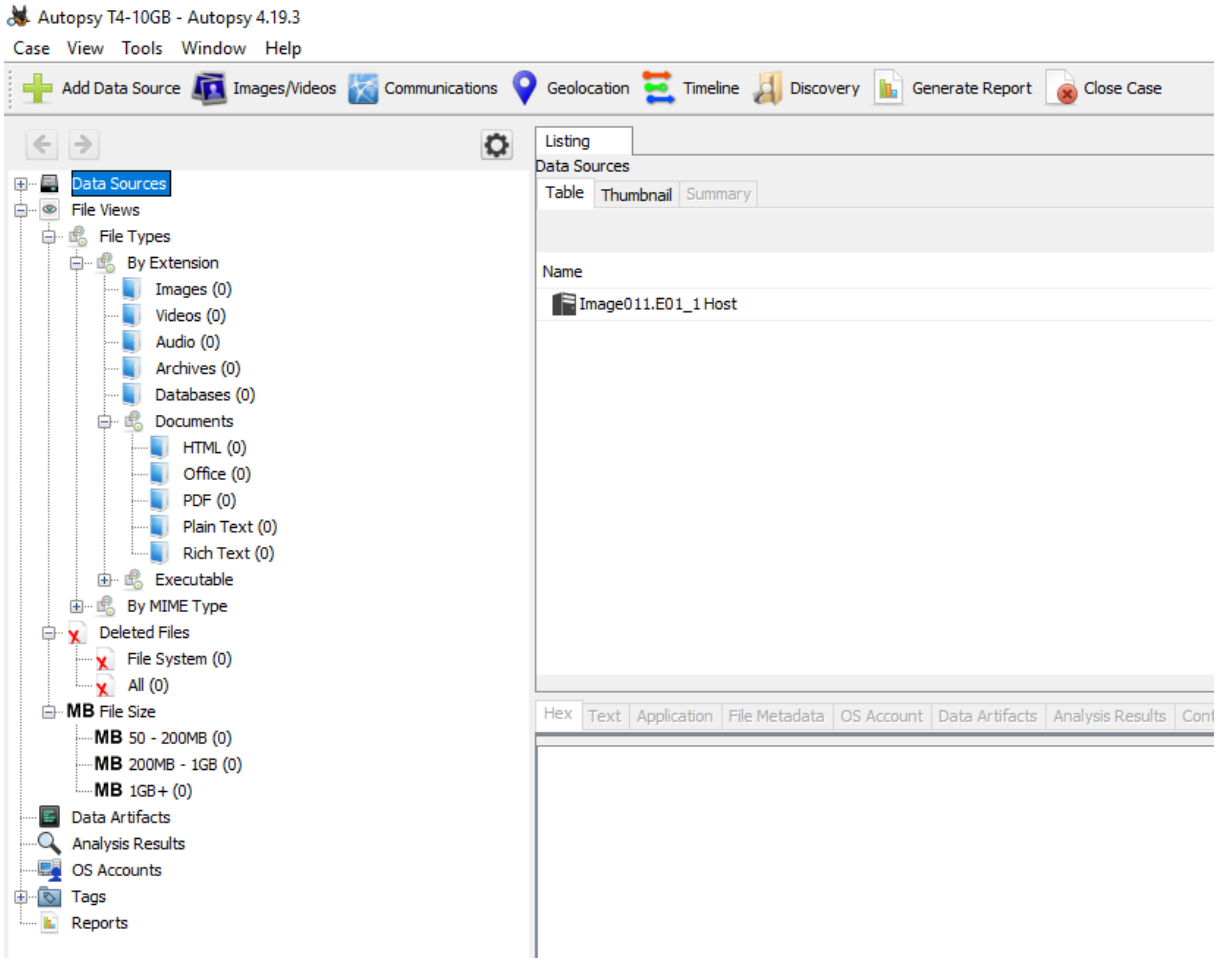



**Εικόνα 6-40: Εργαλείο 4 (A2) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Αυτό οφείλεται στο γεγονός ότι το εργαλείο με το πέρας της διαδικασίας διαγραφής του μορφοποιεί (formatting) το δίσκο και τα δεδομένα στα αρχικά sectors αφορούν το MBR και το NTFS. Ο δίσκος μετονομάζεται με το πέρας της μορφοποίησης του σε Local Disk και είναι έτοιμος να χρησιμοποιηθεί χωρίς περεταίρω ενέργειες από το χρήστη. Η επιλογή για μορφοποίηση του δίσκου μετά την διαγραφή είναι προεπιλογή του εργαλείου και στην παρούσα έκδοση δεν μπορεί να τροποποιηθεί.



Προχωρήσαμε επίσης σε ανάλυση της με το εργαλείο δικανικής Autopsy.




**Εικόνα 6-41: Εργαλείο 4 (Α2) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

TSDW - Process Counters

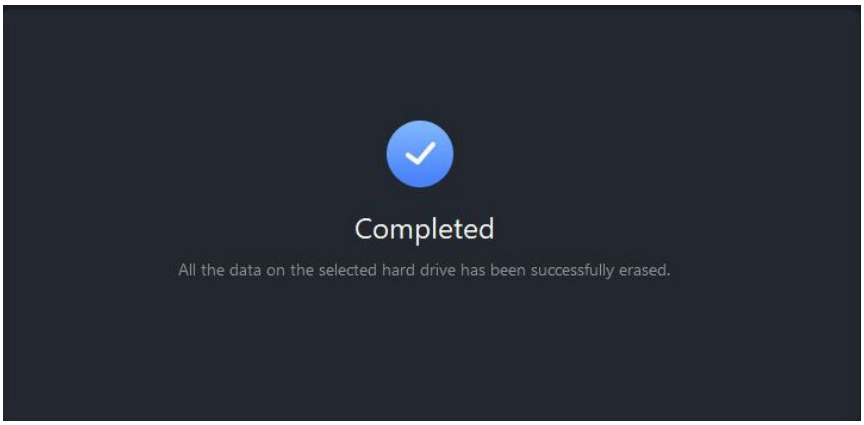
| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 0.9 % | 0.0 % | 6.8 % | --- |
| Process Memory Used | 42.1 MB | 40.2 MB | 43.0 MB | --- |
| Process Thread Count | 4 | 3 | 7 | --- |
| Process Handle Count | 369 | 367 | 377 | --- |
| Process Data Rate | 58307.9 MB/Sec | 52996.7 MB/Sec | 63330.0 MB/Sec | 39118.71 GB |
| Process Read Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB/Sec | 11.5 MB |
| Process Write Rate | 58307.9 MB/Sec | 52996.7 MB/Sec | 63330.0 MB/Sec | 39118.70 GB |
| Process Page Fault Rate | 19 F/Sec | 0 F/Sec | 2954 F/Sec | 13263 F/Sec |
| Process Nonpaged Pool Used | 0.0 MB | 0.0 MB | 0.0 MB | --- |

**Εικόνα 6-42: Εργαλείο 4 (Α2) – Απαιτήσεις σε υπολογιστικούς πόρους**

Χρόνος αποπεράτωσης διαγραφής: 39 λεπτά, 25 δευτερόλεπτα

- Αξιολόγηση 3 (A3) – Οριστική διαγραφή ολόκληρου του δίσκου με 200GB δεδομένα

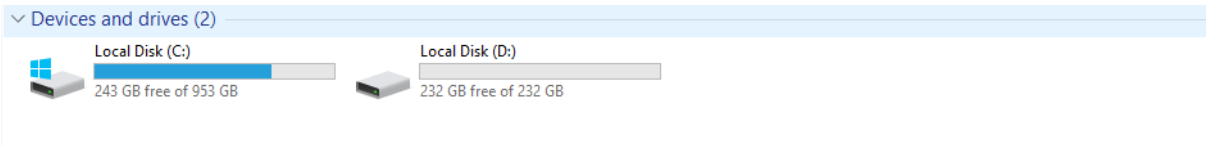
Με το πέρας της διαδικασίας οριστικής διαγραφής ολόκληρου του δίσκου, το εργαλείο μας ενημέρωσε για την ολοκλήρωση της εμφανίζοντας την πιο κάτω ειδοποίηση και δημιουργώντας την σχετική αναφορά.



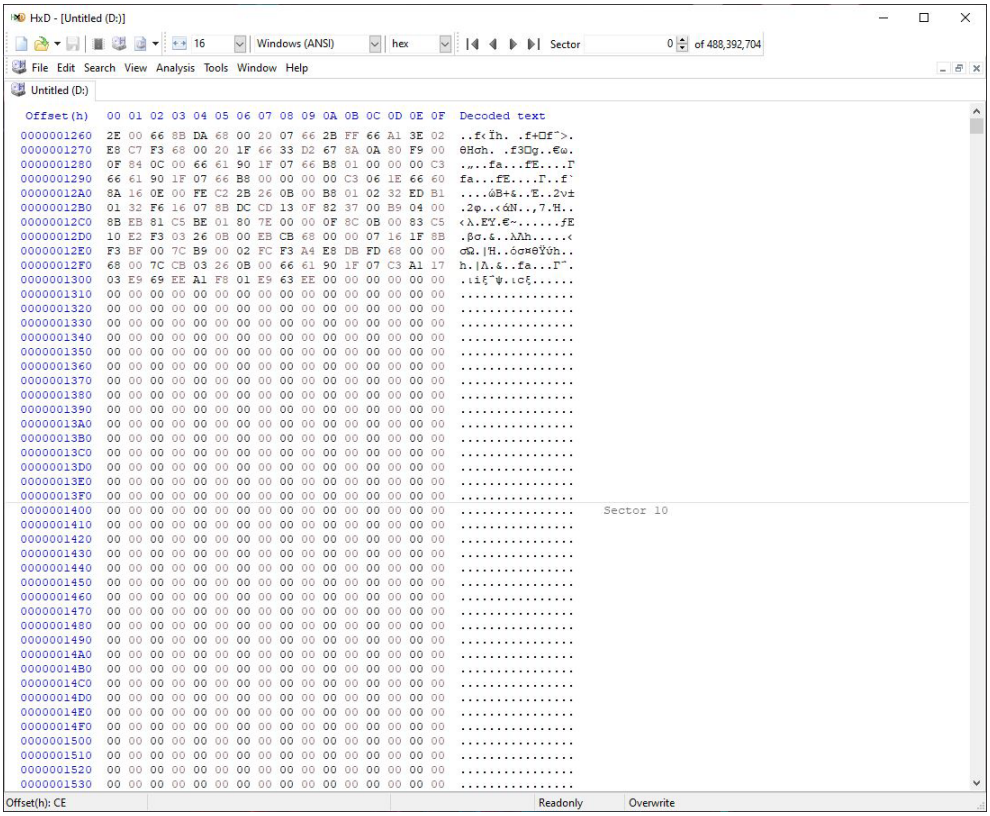

| | | |
|---|---|---|
| wipe partition D | HMG Infosec Standard 5 | Erased |

**Εικόνα 6-43: Εργαλείο 4 (A3) – Αναφορά επιτυχημένης διαγραφής δίσκου - 200GB δεδομένων**

Προχωρήσαμε σε ανάλυση της εικόνας του δίσκου, όπως επίσης επισκόπηση των περιεχομένων του δίσκου με το εργαλείο HxD. Τα αποτελέσματα είναι όμοια με το προηγούμενο σενάριο όπου είχαμε τη ολική διαγραφή ολόκληρου του δίσκου ο οποίος περιείχε 10GB δεδομένων. Οι πρώτοι εννέα sectors του δίσκου, οι οποίοι αποτελούν το MBR και το NTFS ήταν γραμμένοι με δεδομένα, ενώ ο υπόλοιπος δίσκος ήταν διαγραμμένος. Ο δίσκος μετονομάζεται με το πέρας της μορφοποίησης του σε Local Disk και είναι έτοιμος να χρησιμοποιηθεί χωρίς περεταίρω ενέργειες από το χρήστη. Η επιλογή για μορφοποίηση του δίσκου μετά την διαγραφή είναι προεπιλογή του εργαλείου και στην παρούσα έκδοση δεν μπορεί να τροποποιηθεί.

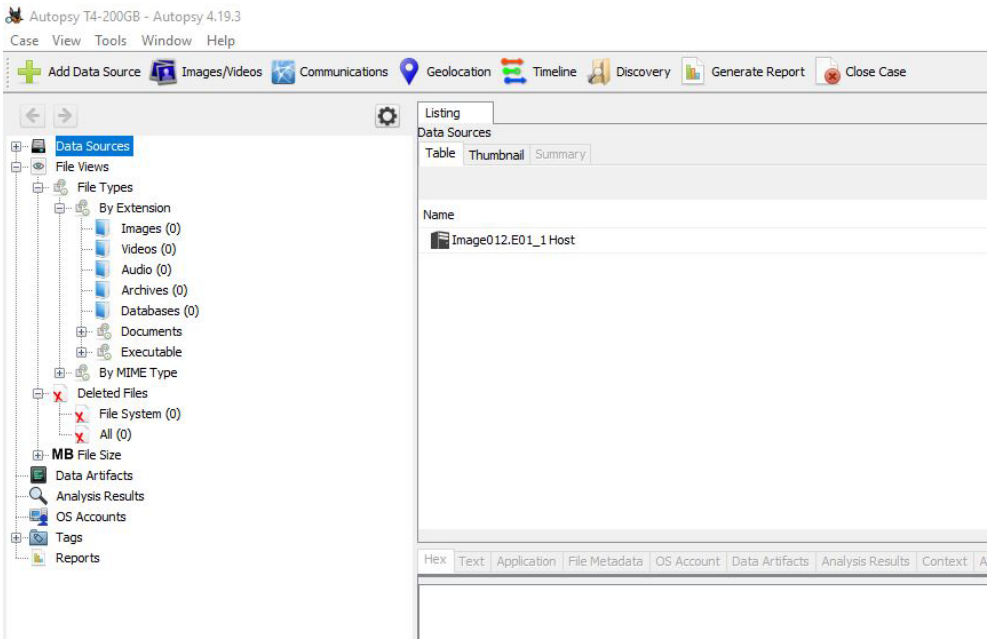


Πέραν αυτών, οι υπόλοιποι sectors παρουσιάζονται να είναι όλοι μηδενικά.




**Εικόνα 6-44: Εργαλείο 4 (Α3) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Έτσι και τα αποτελέσματα από την ανάλυση της εικόνας με το δικανικό εργαλείο Autopsy δεν αποκάλυψε κανένα αρχείο.




**Εικόνα 6-45: Εργαλείο 4 (Α3) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

TSDW - Process Counters

| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 0.6 % | 0.0 % | 6.8 % | --- |
| Process Memory Used | 42.5 MB | 40.2 MB | 43.0 MB | --- |
| Process Thread Count | 3 | 3 | 7 | --- |
| Process Handle Count | 367 | 367 | 377 | --- |
| Process Data Rate | 52197.1 MB/Sec | 44277.1 MB/Sec | 63330.0 MB/Sec | 36599.13 GB |
| Process Read Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB/Sec | 11.9 MB |
| Process Write Rate | 52197.1 MB/Sec | 44277.1 MB/Sec | 63330.0 MB/Sec | 36599.12 GB |
| Process Page Fault Rate | 0 F/Sec | 0 F/Sec | 2954 F/Sec | 98 F/Sec |
| Process Nonpaged Pool Used | 0.0 MB | 0.0 MB | 0.0 MB | --- |

**Εικόνα 6-46: Εργαλείο 4 (A3) – Απαιτήσεις σε υπολογιστικούς πόρους**

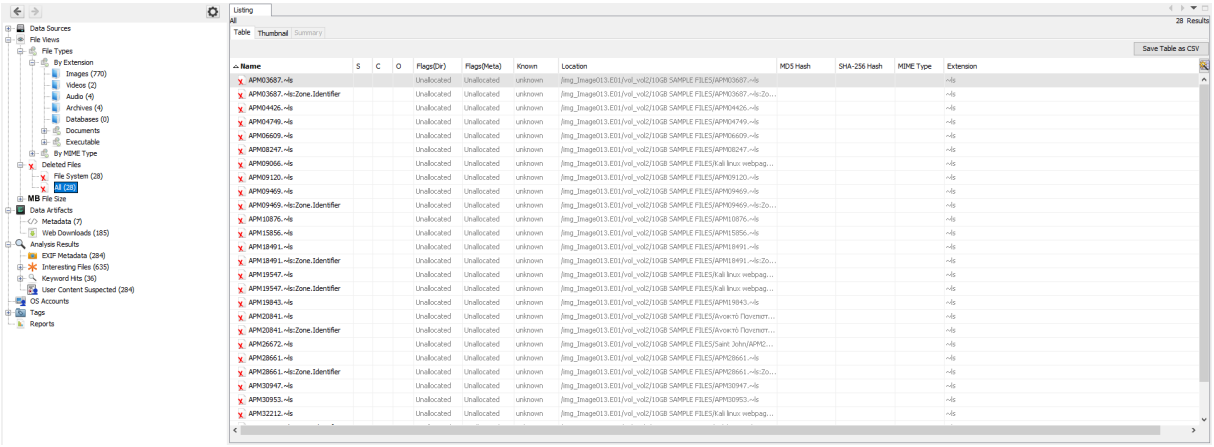
Χρόνος αποπεράτωσης διαγραφής : 41 λεπτά, 38 δευτερόλεπτα

### 6.1.5 Εργαλείο 5 – Abylon Shredder

Για το εργαλείο αυτό εκτελέστηκαν συνολικά τρία διαφορετικά σενάρια κατά τα οποία αξιολογήθηκαν οι δυνατότητες του εργαλείου όσο αφορά την οριστική διαγραφή συγκεκριμένων αρχείων όσο και ολόκληρου του δίσκου.

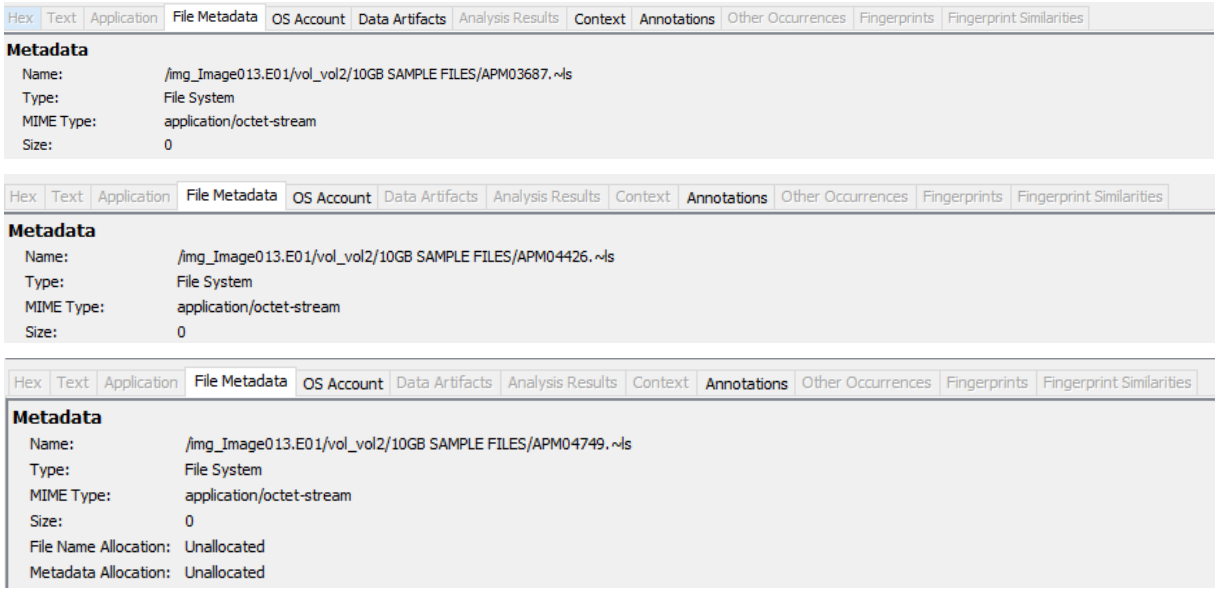
- Αξιολόγηση 1 (A1) – Οριστική διαγραφή 20 προκαθορισμένων αρχείων από το δίσκο

Η ανάλυση της εικόνας του δίσκου η οποία λήφθηκε αμέσως μετά την διαγραφή των συγκεκριμένων αρχείων, κάνοντας χρήση του δικανικού εργαλείου Autopsy διαφαίνεται ότι τα αρχεία έχουν οριστικά διαγραφεί. Δεν κατέστη δυνατή καμιά ανάκτηση σε κανένα από τα αρχεία ανεξαρτήτου μεγέθους. Το Autopsy εντόπισε τις διαγραφές αρχείων, τα οποία όμως δεν έφεραν καμιά πληροφορία σχετικά με τη ταυτότητα του αρχικού αρχείου. Οι καταχωρήσεις αυτές εντοπίζονται στην κατηγορία Deleted files στο Autopsy.



**Εικόνα 6-47: Εργαλείο 5 (A1) - Autopsy - Καταχωρήσεις διαγραμμένων αρχείων**

Οι καταχωρίσεις των διαγραμμένων αρχείων που εντοπίστηκαν όπως φαίνεται και από το στιγμιότυπο πιο πάνω έχουν για όνομα APMXXXX και κατάληξη ~ls, ενώ καμιά άλλη πληροφορία δεν τα συνοδεύει. Επίσης κατάφερε επιτυχώς να διαγράψει και όλα τα metadata που τα συνόδευαν. Αυτό φανερώνει ότι το εργαλείο στην περίπτωση διαγραφής αρχείων από το δίσκο έκανε εξαιρετική δουλεία. Παρακάτω παρουσιάζονται κάποια παραδείγματα από τα ευρήματα.

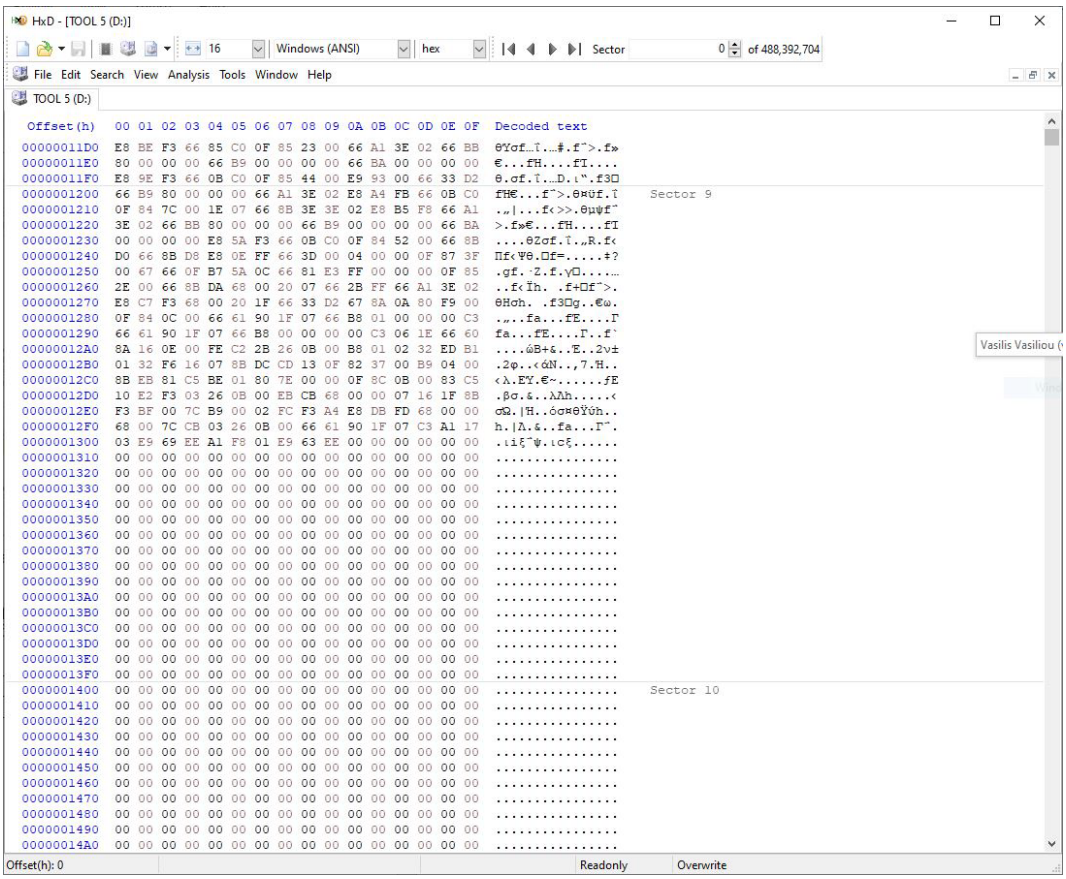



**Εικόνα 6-48: Εργαλείο 5 (Α1) – Ευρήματα από τα διαγραμμένα αρχεία**

- Αξιολόγηση 2 (Α2) – Οριστική διαγραφή ολόκληρου του δίσκου με 10GB δεδομένα

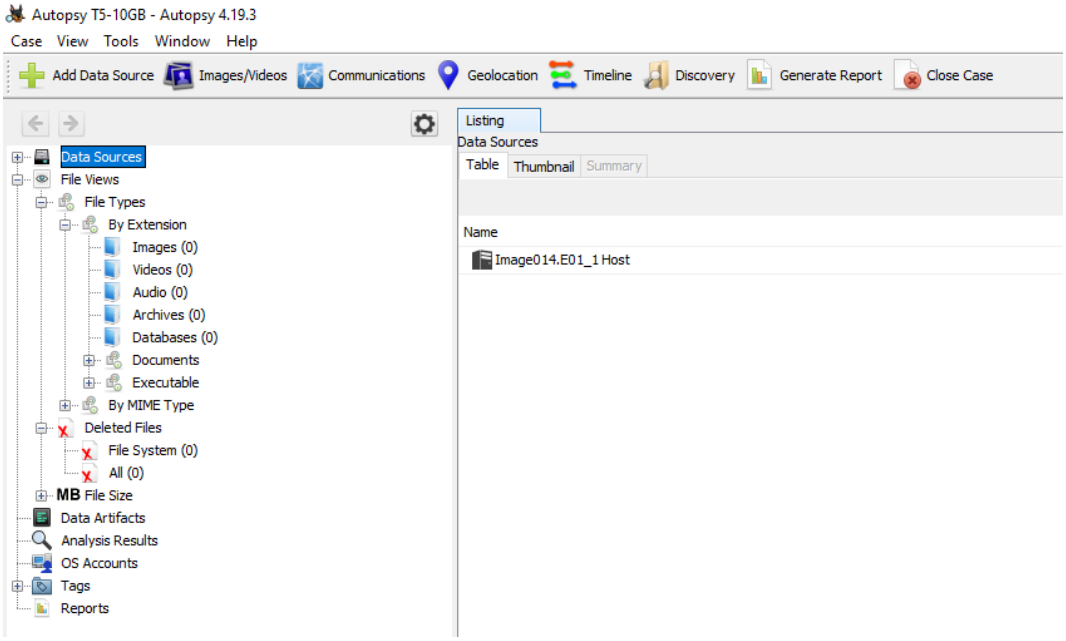
Η διαδικασία οριστικής διαγραφής του δίσκου σύμφωνα με το εργαλείο ολοκληρώθηκε επιτυχώς. Προχωρήσαμε σε ανάλυση της εικόνας του δίσκου, όπως επίσης επισκόπηση των περιεχομένων του δίσκου με το εργαλείο HxD. Σύμφωνα με αυτό οι πρώτοι εννέα sectors του δίσκου ήταν γραμμένοι με δεδομένα, ενώ ο υπόλοιπος δίσκος ήταν διαγραμμένος.

Αυτό οφείλεται στο γεγονός ότι το εργαλείο με το πέρας της διαδικασίας διαγραφής του μορφοποιεί (formatting) το δίσκο και τα δεδομένα στα αρχικά sectors αφορούν το MBR και το NTFS. Ο δίσκος μετονομάζεται με το πέρας της μορφοποίησης του σε TOOL 5, όπως δηλαδή ήταν η αρχική του ονομασία και είναι έτοιμος να χρησιμοποιηθεί χωρίς περεταίρω ενέργειες από το χρήστη. Η επιλογή για μορφοποίηση του δίσκου μετά την διαγραφή είναι προεπιλογή του εργαλείου και δεν μπορεί να τροποποιηθεί μέσα από τις ρυθμίσεις του εργαλείου.




**Εικόνα 6-49: Εργαλείο 5 (A2) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Όπως αναμενόταν η ανάλυση της εικόνας με το δικανικό εργαλείο Autopsy δεν αποκάλυψε κανένα αρχείο.




**Εικόνα 6-50: Εργαλείο 5 (A2) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

SAWipeX64 - Process Counters

| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 1.6 % | 0.0 % | 5.3 % | --- |
| Process Memory Used | 102.3 MB | 92.3 MB | 120.0 MB | --- |
| Process Thread Count | 8 | 6 | 10 | --- |
| Process Handle Count | 96194 | 96191 | 96197 | --- |
| Process Data Rate | 27.5 MB/Sec | 0.0 MB/Sec | 103.1 MB/Sec | 19.26 GB |
| Process Read Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB/Sec | 0.0 MB |
| Process Write Rate | 27.5 MB/Sec | 0.0 MB/Sec | 103.1 MB/Sec | 19.26 GB |
| Process Page Fault Rate | 3 F/Sec | 0 F/Sec | 79 F/Sec | 2170 F/Sec |
| Process Nonpaged Pool Used | 0.1 MB | 0.1 MB | 0.1 MB | --- |

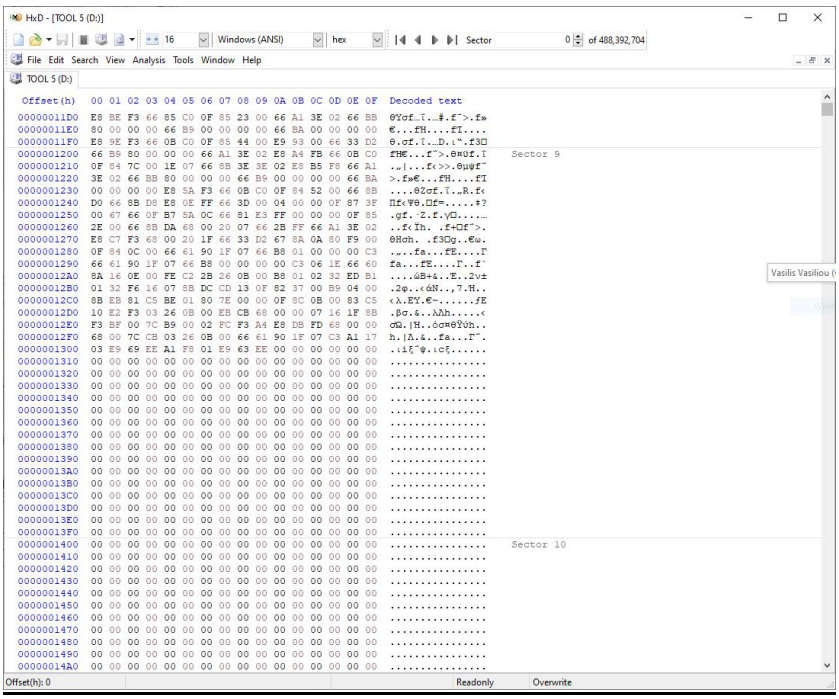
**Εικόνα 6-51: Εργαλείο 5 (A2) – Απαιτήσεις σε υπολογιστικούς πόρους**

Χρόνος αποπεράτωσης διαγραφής: 1 ώρα, 17 λεπτά, 25 δευτερόλεπτα

- Αξιολόγηση 3 (A3) – Οριστική διαγραφή ολόκληρου του δίσκου με 200GB δεδομένα

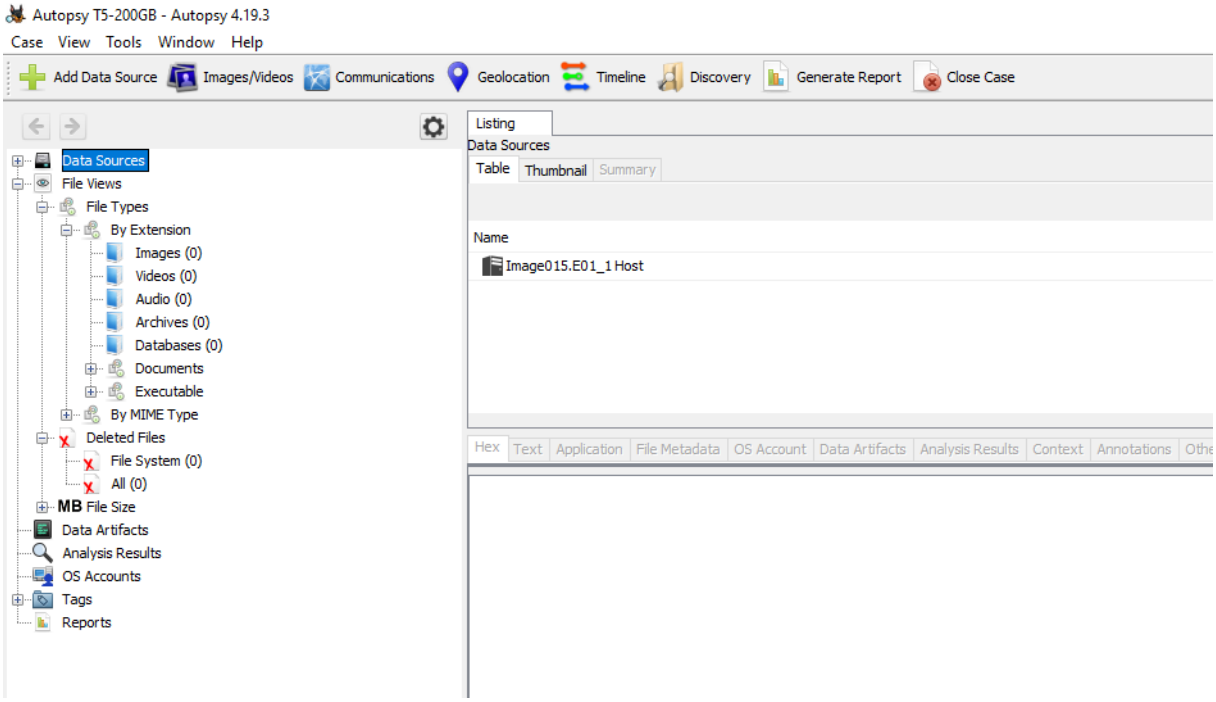
Προχωρήσαμε σε ανάλυση της εικόνας του δίσκου, όπως επίσης επισκόπηση των περιεχομένων του δίσκου με το εργαλείο HxD. Τα αποτελέσματα είναι όμοια με το προηγούμενο σενάριο όπου είχαμε τη ολική διαγραφή ολόκληρου του δίσκου ο οποίος περιείχε 10GB δεδομένων. Οι πρώτοι εννέα sectors του δίσκου, οι οποίοι αποτελούν το MBR και το NTFS ήταν γραμμένοι με δεδομένα, ενώ ο υπόλοιπος δίσκος ήταν διαγραμμένος. Ο δίσκος μετονομάζεται με το πέρας της μορφοποίησης του σε TOOL 5. Η επιλογή για μορφοποίηση του δίσκου μετά την διαγραφή είναι προεπιλογή του εργαλείου και στην παρούσα έκδοση δεν μπορεί να τροποποιηθεί

Πέραν αυτών, οι υπόλοιποι sectors παρουσιάζονται να είναι όλοι μηδενικά.




**Εικόνα 6-52: Εργαλείο 5 (A3) – HxD – Επισκόπηση περιεχομένου διαγραμμένου δίσκου**

Έτσι και τα αποτελέσματα από την ανάλυση της εικόνας με το δικανικό εργαλείο Autopsy δεν αποκάλυψε κανένα αρχείο.




**Εικόνα 6-53: Εργαλείο 5 (Α3) – Autopsy – Επιβεβαίωση διαγραφής δίσκου**

SAWipeX64 - Process Counters

| Counter | Average | Minimum | Maximum | Total |
|---|---|---|---|---|
| Process CPU Usage | 1.6 % | 0.0 % | 21.8 % | --- |
| Process Memory Used | 94.1 MB | 93.5 MB | 126.1 MB | --- |
| Process Thread Count | 9 | 6 | 12 | --- |
| Process Handle Count | 137566 | 6201 | 137644 | --- |
| Process Data Rate | 0.0 MB/Sec | 0.0 MB/Sec | 82.7 MB/Sec | 0.0 MB |
| Process Read Rate | 0.0 MB/Sec | 0.0 MB/Sec | 0.2 MB/Sec | 0.0 MB |
| Process Write Rate | -0.0 MB/Sec | 0.0 MB/Sec | 82.7 MB/Sec | -0.0 MB |
| Process Page Fault Rate | 183 F/Sec | 0 F/Sec | 15072 F/Sec | 125229 F/Sec |
| Process Nonpaged Pool Used | 0.0 MB | 0.0 MB | 0.0 MB | --- |

**Εικόνα 6-54: Εργαλείο 5 (Α3) – Απαιτήσεις σε υπολογιστικούς πόρους**

Χρόνος αποπεράτωσης διαγραφής : 1 ώρα, 18 λεπτά, 5 δευτερόλεπτα

### 6.1.6 Συνοπτική παρουσίαση αποτελεσμάτων

| Εργαλείο | Ικανότητα διαγραφής αρχείων | | | Ικανότητα διαγραφής ολόκληρου δίσκου - 10GB δεδομένων | | Ικανότητα διαγραφής ολόκληρου δίσκου - 200GB δεδομένων | | ΜΟΡΦΟΠΟΙΗΣΗ ΔΙΣΚΟΥ ΜΕΤΑ ΤΗΝ ΔΙΑΓΡΑΦΗ |
|---|---|---|---|---|---|---|---|---|
| | Διαγραφή περιεχομένων | Διαγραφή ονόματος | Διαγραφή Metadata | Διαγραφή ολόκληρου δίσκου | Διαγραφή MBR | Διαγραφή ολόκληρου δίσκου | Διαγραφή MBR | |
| **AOMEI Partition Assistant** | PASS | PASS | FAIL | PASS | FAIL | PASS | FAIL | ΟΧΙ |
| **O&O SafeErase** | PASS | PASS | PASS | PASS | PASS | PASS | PASS | ΟΧΙ |
| **Easy File Shredder** | FAIL | PASS | FAIL | PASS | FAIL | PASS | FAIL | ΝΑΙ |
| **TS DataWipe** | PASS | PASS | FAIL | PASS | FAIL | PASS | FAIL | ΝΑΙ |
| **Aabylon SHREDDER** | PASS | PASS | PASS | PASS | FAIL | PASS | FAIL | ΝΑΙ |

| Εργαλείο | 10GB DATA | | | 200GB DATA | | |
|---|---|---|---|---|---|---|
| | Average CPU | Average Memory | Time | Average CPU | Average Memory | Time |
| **AOMEI Partition Assistant** | 1.60% | 37.90 MB | 00:42:00 | 2.20% | 38.60 MB | 00:42:00 |
| **O&O SafeErase** | 3.10% | 60.28 MB | 00:38:44 | 3.10% | 60.28 MB | 00:38:44 |
| **Easy File Shredder** | 0.60% | 203.10 MB | 01:20:34 | 0.70% | 218.10 MB | 01:20:34 |
| **TS DataWipe** | 0.90% | 42.10 MB | 00:39:25 | 0.60% | 42.50 MB | 00:41:38 |
| **Aabylon SHREDDER** | 1.60% | 102.30 MB | 01:17:29 | 1.60% | 94.10 MB | 01:18:05 |

**Πίνακας 6-2: Συνοπτική παρουσίαση αποτελεσμάτων**

# Κεφάλαιο 7
# Συμπεράσματα

Η διεξαγωγή των πειραματικών αξιολογήσεων στα διάφορα εργαλεία οριστικής διαγραφής οδήγησε σε σαφή αποτελέσματα τα οποία αξιολογώντας τα μπορούμε να εξάγουμε ποικίλα συμπεράσματα, τόσο γενικά για την χρήση των εργαλείων όσο και ειδικά για κάθε εργαλείο ανεξάρτητα.

Καταρχάς οι πειραματικές δοκιμές έδωσαν μια συλλογή αποτελεσμάτων σχετικά με την ικανότητα των εργαλείων οριστικής διαγραφής, στο να διαγράφουν συγκεκριμένα αρχεία από το δίσκο, όσο και τη διαγραφή ολόκληρου του δίσκου.

Σύμφωνα λοιπόν με αυτά, υπάρχουν εργαλεία οριστικής διαγραφής όπου στο σενάριο οριστικής διαγραφής συγκεκριμένων αρχείων από το δίσκο κατάφεραν με επιτυχία να διαγράψουν οριστικά τόσο το ίδιο το αρχείο όσο και τις πληροφορίες που μαρτυρούσαν την ύπαρξη του. Σε άλλες περιπτώσεις εργαλεία κατάφεραν να διαγράψουν με επιτυχία το περιεχόμενο του αρχείου ωστόσο άφησαν άθικτες πληροφορίες που αφορούσαν το αρχείο και σχετιζόταν με αυτό. Τέλος υπήρξαν εργαλεία το οποία δεν κατάφεραν να διαγράψουν τα αρχεία και κατέστη δυνατή η πλήρης επαναφορά τους. Αβίαστα συμπεραίνουμε ότι η οριστική διαγραφή συγκεκριμένων αρχείων από το δίσκο παρουσιάζει ιδιαιτερότητες που καθιστά την όλη διαδικασία πιο

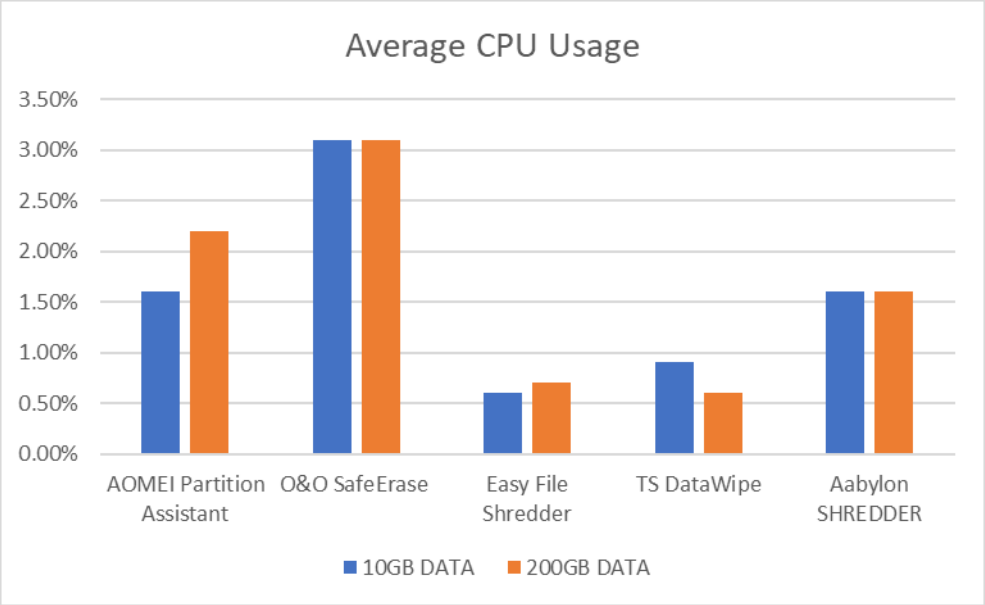
πολύπλοκη αλλά όχι ακατόρθωτη. Αυτό οφείλεται κυρίως στο αρχείο συστήματος NTFS που περιλαμβάνει πληροφορίες για τα αρχεία που βρίσκονται στο δίσκο και πιθανόν τα εργαλεία οριστικής διαγραφής να αποτυγχάνουν να προβαίνουν στις κατάλληλες τροποποιήσεις του.

Όσο αφορά το σενάριο διαγραφής ολόκληρου του δίσκου τα αποτελέσματα έχουν μεγαλύτερη συνοχή αφού σε αυτό υπήρξαν δύο περιπτώσεις. Η πρώτη αφορά την επιτυχή διαγραφή ολόκληρου του δίσκου ενώ η δεύτερη αφορά επίσης την διαγραφή ολόκληρου του δίσκου εξαιρουμένου του MBR (Master Boot Sector). Και στις δύο περιπτώσεις τα δεδομένα από το δίσκο δεν ήταν ανακτήσιμα άρα θεωρούμε τα εργαλεία οριστικής διαγραφής σε αυτό το σενάριο είναι αποτελεσματικά. Τα ίδια αποτελέσματα προέκυψαν τόσο στην διαγραφή ολόκληρου του δίσκου που περιείχε 10GB δεδομένων όσο και στη διαγραφή ολόκληρου του δίσκου που περιείχε 200GB δεδομένων. Το γεγονός αυτό μας οδηγεί στο συμπέρασμα ότι η ποσότητα δεδομένων που βρίσκονται σε ένα δίσκο δεν επηρεάζει την αποτελεσματικότητα του εργαλείου όταν πρόκειται για την ολική διαγραφή του.

Η ύπαρξη εργαλείου που κατάφερε να διαγράψει οριστικά τόσο τα 20 συγκεκριμένα αρχεία από το δίσκο, όσο και ολόκληρο το δίσκο επιβεβαιώνει ότι η μέθοδος διαγραφής One Pass Zero που χρησιμοποιήθηκε είναι επαρκείς για την οριστική διαγραφή δεδομένων και μπορεί να χρησιμοποιηθεί ως μια πετυχημένη αντι-δικανική μέθοδος. Επίσης, ένα μόνο πέρασμα αντικατάστασης για τη διαγραφή του δίσκου είναι αρκετό για να καταστήσει τα δεδομένα από το δίσκο μη ανακτήσιμα.

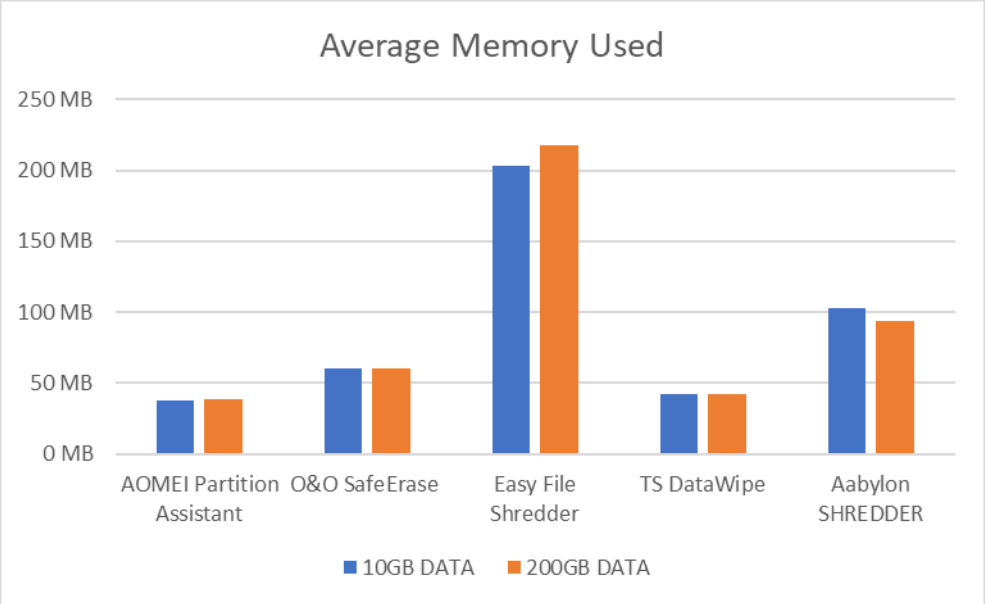
Η σωστή εφαρμογή των αλγορίθμων οριστικής διαγραφής εξαρτάται καθαρά από την υλοποίηση του εργαλείου από τον δημιουργό του. Να αναφέρουμε ότι η υλοποίηση του κάθε εργαλείου επηρεάζει την ικανότητα του στην οριστική διαγραφή δεδομένων.

Ένα άλλο συμπέρασμα που προέκυψε από την ανάλυση και αξιολόγηση των εργαλείων οριστικής διαγραφής σχετίζεται με τους πόρους του συστήματος που καταναλώνονται κατά την εφαρμογή τους. Με βάση τα πειράματα που εκτελέστηκαν και τις καταγεγραμμένες μετρήσεις, μπορεί να εξαχθεί το συμπέρασμα ότι δεν υπάρχει άμεση συσχέτιση μεταξύ των πόρων του συστήματος (χρήση CPU και χρήση μνήμης) και την αποτελεσματικότητα του εργαλείου διαγραφής.



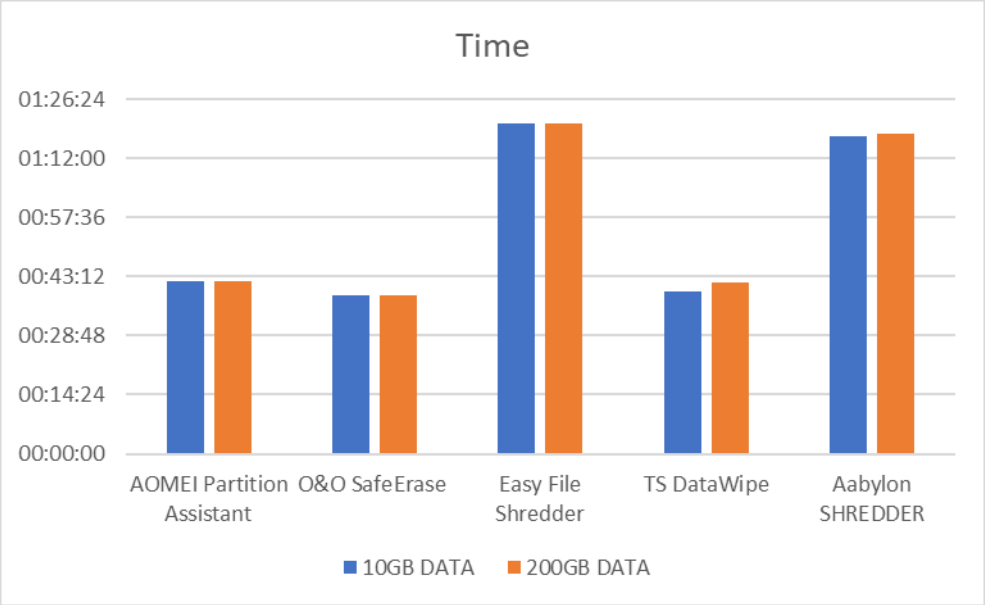

**Εικόνα 7-1: Συγκριτική χρήση επεξεργαστή (CPU)**

Η χρήση του επεξεργαστή του συστήματος δεν σχετίζεται με την ικανότητα οριστικής διαγραφής των εργαλείων. Το ποσοστό χρήσης του επεξεργαστή είναι θέμα βελτιστοποίησης του κώδικα του εργαλείου από τον κατασκευαστή του.




**Εικόνα 7-2: Συγκριτική κατανάλωση μνήμης**

Η χρήση μνήμης συστήματος από το εργαλείο κατά την διάρκεια της διαδικασίας διαγραφής δεν συνδέεται με την ικανότητα του για οριστική διαγραφή. Υπήρχαν περιπτώσεις όπου εργαλεία απέδωσαν καλύτερα στην οριστική διαγραφή δεδομένων και έκαναν χρήση λιγότερης μνήμης συστήματος ενώ άλλα που δεν ήταν τόσο αποτελεσματικά χρειάστηκαν περισσότερη μνήμη.




**Εικόνα 7-3: Σύγκριση χρόνου διαγραφής εργαλείων**

Ο συνολικός χρόνος που απαιτείται για την διαγραφή ολόκληρου του δίσκου δεν εξαρτάται από το μέγεθος ή το σύνολο των αρχείων που βρίσκονται σε αυτόν. Εξαρτάται από τη συνολική χωρητικότητα του δίσκου και το εργαλείο που χρησιμοποιήθηκε. Για αυτό το λόγο οι χρόνοι που καταγράφηκαν κατά την διαγραφή του δίσκου με τα 10GB δεδομένων είναι πανομοιότυποι με τους χρόνους κατά την διαγραφή του δίσκου με τα 200GB δεδομένων. Αυτό ήταν κάτι που αναμέναμε αφού η φιλοσοφία λειτουργίας των εργαλείων οριστικής διαγραφής κατά τη διαγραφή ολόκληρου του δίσκου, είναι η επανεγγραφή όλων των sectors του δίσκου ανεξάρτητα από το ποιοι περιέχουν δεδομένα.

Συμπερασματικά, η χρήση εργαλείων οριστικής διαγραφής δεδομένων μπορεί να επηρεάσει σημαντικά μια δικανική εγκληματολογική έρευνα. Αυτά τα εργαλεία έχουν σχεδιαστεί για να διαγράφουν πλήρως δεδομένα, και εφόσον έχουν υλοποιηθεί και σωστά μπορεί να καταστήσει δύσκολο, αν όχι αδύνατο, για τους ερευνητές να ανακτήσουν σχετικές πληροφορίες. Καθώς οι ψηφιακές συσκευές και οι μέθοδοι αποθήκευσης συνεχίζουν να εξελίσσονται, γίνεται όλο και πιο σημαντικό για τους δικανικούς ερευνητές να παραμένουν ενημερωμένοι σχετικά με τις μεθόδους αντι-δικανικής που πιθανόν να αντιμετωπίσουν. Ενώ τα εργαλεία μόνιμης διαγραφής δεδομένων μπορεί να είναι ένα χρήσιμο εργαλείο για την προστασία ευαίσθητων δεδομένων, η χρήση τους πρέπει να σταθμίζεται προσεκτικά έναντι των πιθανών επιπτώσεων στις ψηφιακές δικανικές έρευνες.

Τέλος να αναφέρουμε ότι τα αποτελέσματα της διατριβής παρουσιάζουν εξαιρετικό ενδιαφέρον όχι μόνο για την ακαδημαϊκή ερευνητική κοινότητα αλλά και για τους απλούς χρήστες μιας η μελέτη αφορά την σύγκριση πέντε από τα πιο δημοφιλή εργαλεία οριστικής διαγραφής με χιλιάδες λήψεις καθημερινά.

## 7.1 Απαντήσεις στα Ερευνητικά Ερωτήματα

Ολοκληρώνοντας τις πειραματικές δοκιμές και έχοντας μελετήσει εμπεριστατωμένα τα αποτελέσματα των εργαλείων οριστικής διαγραφής δεδομένων μπορούμε να απαντήσουμε με σαφήνεια τα ερευνητικά ερωτήματα που τέθηκαν στην αρχή της διατριβής.

1. **Ποιο/Ποια από τα εργαλεία υπό εξέταση κρίνεται πιο αποτελεσματικό σύμφωνα με τις προϋποθέσεις που έχουμε θέσει στις πιο κάτω περιπτώσεις:**

   **α. Οριστική διαγραφή συγκεκριμένου αρχείου από το δίσκο.**

   Τα εργαλεία οριστικής διαγραφής που κατάφεραν με επιτυχία να διαγράψουν τα αρχεία που έχουμε επιλέξει χωρίς να αφήσουν κανένα ίχνος τους είναι:

   i. O&O SafeErase
   ii. Aabylon SHREDDER

   Τα υπόλοιπα εργαλεία αστόχησαν στη συγκεκριμένη δοκιμασία αφού με τη ολοκλήρωση της διαγραφής ήταν δυνατή η ανάκτηση ολόκληρων των αρχείων είτε διατήρησαν πληροφορίες για τα αρχεία.

   **β. Οριστική διαγραφή ολόκληρου του δίσκου.**

   Όλα ανεξαιρέτως τα εργαλεία κατάφεραν να διαγράψουν το περιεχόμενο ολόκληρου του δίσκου σε σημείο που κανένα αρχείο δεν ήταν ανακτήσιμο. Το O&O SafeErase κατάφερε επιπρόσθετα να διαγράψει και τη περιοχή του MBR.

2. **Υπάρχουν περιθώρια επαναφοράς κάποιων από τα δεδομένα που διαγράφηκαν με τη χρήση των εργαλείων; Αν ναι, σε τι ποσοστό;**

   Στην περίπτωση διαγραφής συγκεκριμένων αρχείων υπήρχε περίπτωση όπου ήταν δυνατή η επαναφορά ολόκληρων των αρχείων (Easy File Shredder). Στην περίπτωση οριστικής διαγραφής του δίσκου δεν κατέστη για κανένα εργαλείο δυνατή η ανάκτηση δεδομένων.

3. **Ποιο εργαλείο είναι ταχύτερο στην διεκπεραίωση της οριστικής διαγραφής συγκεκριμένου μεγέθους και πλήθους αρχείων;**

   Το ταχύτερο εργαλείο στην διεκπεραίωση της οριστικής διαγραφής είναι το O&O SafeErase όπου σε χρόνο 38 λεπτών και 44 δευτερολέπτων κατάφερε να επαναγράψει το δίσκο των 250GB με μηδενικά .

4. **Ποιο εργαλείο είναι το λιγότερο απαιτητικό σε υπολογιστικούς πόρους και αντίθετα ποιο εργαλείο είναι το πιο δαπανηρό;**

   Λιγότερο απαιτητικό σε επεξεργαστική ισχυ είναι το Easy File Shredder, το οποίο έκανε χρήση μόλις το 0.6% της δυνατότητας του επεξεργαστή. Σε μνήμη συστήματος το λιγότερο απαιτητικό είναι το AOMEI Partition Assistant το οποίο χρειάστηκε μόνο 37.9MB μνήμης για να διεκπεραιώσει την εργασία.

   Αντίθετα το πιο δαπανηρό σε επεξεργαστική ισχυ είναι το O&O SafeErase με 3.10% χρήση του επεξεργαστή και σε χρήση μνήμης το Easy File Shredder που χρειάστηκε 203.1MB μνήμης.

   Σε γενικές γραμμές όμως τα εργαλεία οριστικής διαγραφής που εξετάστηκαν δεν έχουν υπερβολικές απαιτήσεις σε σχέση με τις δυνατότητες των σημερινών υπολογιστικών συστημάτων έτσι δεν θεωρείται σημαντικό κριτήριο για την επιλογή κατάλληλου εργαλείου οριστικής διαγραφής.

5. **Επηρεάζει την αποτελεσματικότητα του εργαλείου η ποσότητα των δεδομένων που βρίσκονται αποθηκευμένα στο δίσκο. Δηλαδή, αν παίζει ρόλο για τα αποτελέσματα το αν π.χ. θα σβήσουν 10GB/250GB ή 200GB/250GB.**

Σύμφωνα με τα αποτελέσματα η ποσότητα των δεδομένων που βρίσκονται στο δίσκο δεν επηρεάζει την αποτελεσματικότητα του εργαλείου. Αυτό οφείλεται στο γεγονός ότι η λειτουργία των εργαλείων οριστικής διαγραφής βασίζεται στην επανεγγραφή ολόκληρου του δίσκου bit με bit ασχέτως αν σε αυτά βρίσκονται γραμμένα δεδομένα ή όχι.

## 7.2 Προοπτική για Μελλοντική Έρευνα

Η παρούσα μεταπτυχιακή διατριβή εξέτασε εκτεταμένα ένα μέρος από το πλήθος εργαλείων οριστικής διαγραφής που είναι σήμερα διαθέσιμα για χρήση. Μελλοντικές πειραματικές δοκιμές θα ήταν χρήσιμο να διεξαχθούν για διεύρυνση της γνώσης γύρω από το αντικείμενο. Μερικές παράμετροι που δεν εξετάστηκαν στην παρούσα διατριβή και θα μπορούσαν να αποτελέσουν τη βάση για εκπόνηση σχετικών μελετών και εμπλουτισμό της υφιστάμενης γνώσης είναι:

α. Προσαρμογές στην πειραματική διαδικασία όπως χρήση άλλων δημοφιλών πρότυπων διαγραφής πέραν από το One Pass Zero. (πχ US - DoD 5220.22-M , British HMG IS5 (Enhanced), NCSC-TG-025).

β. Αύξηση των εργαλείων που θα αξιολογηθούν.

γ. Χρήση του GPT σαν Partition Style .

δ. Χρήση άλλου συστήματος αρχείων εκτός από το NTFS.

ε. Διεξαγωγή πειραματικών δοκιμών σε δίσκους SSD.

στ. Μεγαλύτερο μέγεθος αποθηκευτικών μέσω της τάξεως των TB.

ζ. Οριστική διαγραφή δεδομένων σε δίσκους τοποθετημένους σε εικονικές μηχανές.

η. Εξέταση εργαλείων οριστικής διαγραφής σε λειτουργικά Linux ή macOS.

# Βιβλιογραφία


Journal of Forensic Sciences—2021—AlHarbi—Forensic analysis of anti-forensic file-wiping tools on Windows(2021).pdf. (n.d.).

About O&O. (n.d.). Retrieved 20 April 2023, from https://www.oo-software.com/en/company

About TogetherShare | Learn More about TogetherShare. (n.d.). Retrieved 21 April 2023, from https://www.togethershare.com/company/

AOMEI | Windows & iPhone Backup Software, Partition Manager and Cloud Backup Service. (n.d.). Retrieved 19 April 2023, from https://www.aomeitech.com/

AOMEI Partition Assistant | Partition Manager Software for Windows PC and Server. (n.d.). Retrieved 20 April 2023, from https://www.diskpart.com/

Autopsy | Digital Forensics. (n.d.). Autopsy. Retrieved 15 April 2023, from https://www.autopsy.com/

Bob Sullivan, & Rosa Golijan. (2013, April 22). Terrorists may leave 'digital breadcrumbs' for investigators. NBC News. http://www.nbcnews.com/news/us-news/terrorists-may-leave-digital-breadcrumbs-investigators-flna6C9538422

Bulk-extractor | Kali Linux Tools. (n.d.). Kali Linux. Retrieved 15 April 2023, from https://www.kali.org/tools/bulk-extractor/

Carlton, G., & Kessler, G. (2012). Identifying Trace Evidence from Target-Specific Data Wiping Application Software. Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2012.1122

CHK Checksum Utility. Retrieved 15 April 2023, from https://compressme.net/

CrystalDiskInfo—Website [en]. (2018, January 12). https://crystalmark.info/en/software/crystaldiskinfo/, https://crystalmark.info/en/software/crystaldiskinfo/

DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) January 1995. (n.d.).

Ferrell. (2011). Martha Stewart's Insider Trading Scandal.

FTK Imager. (n.d.). Exterro. Retrieved 15 April 2023, from https://www.exterro.com/ftk-imager

Geiger, M. (2005). Evaluating Commercial Counter-Forensic Tools.

General Data Protection Regulation (GDPR) – Official Legal Text. (2023). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Germany, abylonsoft-S. and C. S. /. (n.d.). Software and Development by abylonsoft | Made in Germany. Retrieved 21 April 2023, from https://www.abylonsoft.com/

HashMyFiles: Calculate MD5/SHA1/CRC32 hash of files. (n.d.). NirSoft. Retrieved 15 April 2023, from https://www.nirsoft.net/utils/hash_my_files.html

History of hard disk drives. (2023). In Wikipedia. https://en.wikipedia.org/w/index.php?title=History_of_hard_disk_drives&oldid=1150677180

Horsman, G. (2021). Digital tool marks (DTMs): A forensic analysis of file wiping software. Australian Journal of Forensic Sciences, 53(1), 96–111. https://doi.org/10.1080/00450618.2019.1640793

HxD - Freeware Hex Editor and Disk Editor. (n.d.). Retrieved 16 April 2023, from https://mh-nexus.de/en/hxd/

ISO/IEC 27001 Standard – Information Security Management Systems. (n.d.). ISO. Retrieved 30 April 2023, from https://www.iso.org/standard/27001

Jones, A. (2020). An Evaluation Of Data Erasing Tools. The Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2020.1615

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). Guidelines for Media Sanitization (NIST SP 800-88r1; p. NIST SP 800-88r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1

Kostopoulos, G. K. (2017). Cyberspace and cybersecurity (Second edition). CRC Press, Taylor & Francis Group.

Martin, T., & Jones, A. (2011). An evaluation of data erasing tools [PDF]. 9th Australian Digital Forensics Conference, Edith Cowan University, 5th7th December 2011. https://doi.org/10.4225/75/57B2C01440CEF

Method of deletion O&O Software. (n.d.). Retrieved 20 April 2023, from https://docs.oo-software.com/en/oosafeerase-15/method-of-deletion-oose15

NIST Standards. (2016). NIST. https://www.nist.gov/standards

Oh, D. B., Park, K. H., & Kim, H. K. (2020). De-Wipimization: Detection of data wiping traces for investigating NTFS file system. Computers & Security, 99, 102034. https://doi.org/10.1016/j.cose.2020.102034

Olvecky, M., & Gabriska, D. (2018). Wiping Techniques and Anti-Forensics Methods. 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), 000127–000132. https://doi.org/10.1109/SISY.2018.8524756

Orion USB Write Blocker -Orion Forensics LAB. (n.d.). Orion Forensics Thailand. Retrieved 15 April 2023, from http://www.orionforensics.com/forensics-tools/orion-usb-write-blocker/

Paul Festa. (2002). Can PC sleuths undo Enron shredding? ZDNET. https://www.zdnet.com/article/can-pc-sleuths-undo-enron-shredding/

Payment Card Industry Data Security Standard. (2023). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Payment_Card_Industry_Data_Security_Standard&oldid=1146553256

Pinsent Masons. (2016). NHS Trust to appeal against £325k patient data breach fine. Pinsent Masons. https://www.pinsentmasons.com/out-law/news/nhs-trust-to-appeal-against-325k-patient-data-breach-fine

Sablatura, J., & Karabiyik, U. (2016). The forensic effectiveness of virtual disk sanitization. 2016 4th International Symposium on Digital Forensic and Security (ISDFS), 126–131. https://doi.org/10.1109/ISDFS.2016.7473530

Seagate Barracuda Data Sheet.pdf. (n.d.). Retrieved 15 April 2023, from https://www.seagate.com/files/staticfiles/docs/pdf/datasheet/disc/barracuda-ds1737-1-1111us.pdf

Shepardson, D. (2016). The FTC is trying to figure out whether Volkswagen intentionally destroyed documents related to emissions scandal. Business Insider. https://www.businessinsider.com/volkswagen-investigation-destroy-documents-emissions-scandal-2016-11

Solid-state drive. (2023). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Solid-state_drive&oldid=1149314927

SysGauge—System Monitor. (2023). https://www.sysgauge.com/index.html

Tim Wilson. (2008, October 10). UK Ministry of Defense Loses Hard Drive Containing Data on 700,000. Dark Reading. https://www.darkreading.com/vulnerabilities-threats/uk-ministry-of-defense-loses-hard-drive-containing-data-on-700-000

WebMinds. (n.d.). WebMinds. Retrieved 21 April 2023, from https://www.webminds.com/

Weiss, T. R. (2004, September 3). Hard drive with 23,000 Social Security numbers disappears. Computerworld. https://www.computerworld.com/article/2566748/hard-drive-with-23-000-social-security-numbers-disappears.html

Winter, R. (2013). SSD vs HDD – data recovery and destruction. Network Security, 2013(3), 12–14. https://doi.org/10.1016/S1353-4858(13)70041-2

Wright, C., Kleiman, D., & Sundhar R.S., S. (2008). Overwriting Hard Drive Data: The Great Wiping Controversy. In R. Sekar & A. K. Pujari (Eds.), Information Systems Security (Vol. 5352, pp. 243–257). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-89862-7_21

# Παράρτημα Α
# Κατάλογος Αρχείων και Εργαλείων

Στο παρόν παράρτημα καταγράφονται, ο κατάλογος των αρχείων που χρησιμοποιήθηκαν στις πειραματικές δοκιμές, μαζί με τις κατακερματισμένες τιμές τους και τα εργαλεία οριστικής διαγραφής που είναι σήμερα διαθέσιμα για χρήση.

## Α.1 Κατάλογος Αρχείων

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 1 | 014a.jpg | 635c5d89a764edfe93d1594a2cf664ef | 0.58 | jpg |
| 2 | 14-30mm_F4_S_10_JM_0001.jpg | fe110a0e5ddb542d60f2eaa52abf5b3b | 1.24 | jpg |
| 3 | 18da517618031157d05b66a017cb39d1.jpg | a60e6e88bee2a1e5474817a69e1b1252 | 0.41 | jpg |
| 4 | 2019-10-19_11-52-51_down-town-staycaejpg.jpg | dc8ed547681335fe9ba402a328b390a5 | 1.16 | jpg |
| 5 | 2021-05-01_123359.jpg | cc53126b67f6ec9c3b1f8f3a9c743b0a | 1.11 | jpg |
| 6 | 4K Ultra HD Video of Wild Animals.mkv | ae35b814a43ea4c258d9851b11e17649 | 3,253.91 | mkv |
| 7 | 4K Video Unbelievable Beauty.mkv | 64e83573405f11c619c8b0dbe27d632b | 3,818.41 | mkv |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 8 | Administration_propaganda.tif | a3102eb747714c555de6560be1ec7e4a | 158.03 | tif |
| 9 | Altered Carbon.mkv | f776bf9e405b1044c2060aa39342bf16 | 2,823.73 | mkv |
| 10 | An Awesome Tool to Prevent Corruption Of Your Most Important Files.mp4 | b853c56a8ea958519093c505a72963f8 | 117.14 | mp4 |
| 11 | artist-designer-at-work.jpg | 3c2aa0c9a10417b8897b69b1f9f6c2f2 | 0.97 | jpg |
| 12 | augustine-wong-T0BYurbDK_M-unsplash.jpg | dd32494a3aa65ca45a5c12921b8d2599 | 5.01 | jpg |
| 13 | austin-distel-21GWwco-JBQ-unsplash.jpg | 5f7b6b157176aa184857c43074f42cce | 4.54 | jpg |
| 14 | austin-distel-744oGeqpxPQ-unsplash.jpg | f0ab969cd1661a0dd3be10006ced6071 | 5.55 | jpg |
| 15 | austin-distel-Jn1csk3lWDA-unsplash.jpg | 606fa66cdc2f329530623978cdb8b5db | 3.54 | jpg |
| 16 | austin-distel-nGc5RT2HmF0-unsplash.jpg | 5fdb186472ef98f10a1a4ba5e9c1c018 | 3.93 | jpg |
| 17 | bernard-hermant-_THpp4Hs8LU-unsplash.jpg | 7d3df0dc6bf9ba1c6bc06dbabc95c403 | 3.61 | jpg |
| 18 | blackarch-linux-2023.04.01.ova | ce041f01e0ce2ebfd5d09179b6df10f6 | 29,412.04 | ova |
| 19 | Blow_fight!__General_August_Willich_at_the_Battle_of_Liberty_Gap,_Tennessee,_June_1863_LCCN2017647020.tif | 6cd05e6aad6e63433df9dd776cca1639 | 306.74 | tif |
| 20 | Bon Jovi - You Give Love A Bad Name.mp3 | 65078ed0922a6e8a630ac493a80f7632 | 3.44 | mp3 |
| 21 | cdc-_XLJy3h77cw-unsplash.jpg | 0ecbf61c0adb9ed7b1ceff53613ea1d7 | 5.33 | jpg |
| 22 | ChatGPT For Cybersecurity.mp4 | 2939bdd5a8e7040b95d808c4ecc26da3 | 159.10 | mp4 |
| 23 | cod4.iso | cc9c7c0734193d581b3a4f2e30203dcd | 6,472.28 | iso |
| 24 | Cooperativa_de_fluido.jpg | dc8584d977b660863d4cb91419d93c52 | 10.47 | jpg |
| 25 | CYBER CRIME INVESTIGATORS FIELD GUIDE.pdf | ce7a2f4be81f18de5c3267a0434a3dd8 | 19.94 | pdf |
| 26 | Cyberspace and Cybersecurity .pdf | 30070247573144d0025e908432688b85 | 15.97 | pdf |
| 27 | Das_Lagerregal_Gottes Menger.png | 0973b0362f134bc52b39462fef4522a2 | 393.78 | png |
| 28 | Data Analysis with Microsoft Excel.pdf | bb155cc35a5bb2aa4c28c733055cf0b0 | 10.55 | pdf |
| 29 | EARTH in 8K ULTRA HD .mkv | a32710d19f88f7bc5e328c8b7d7ac436 | 3,470.87 | mkv |
| 30 | easter_egg.psd | d7b3a1f2a541ce9db58de04374e12683 | 25.11 | psd |
| 31 | enwiki-pages-articles-multistream-index.txt | be809e8e087abfb93743c39fd1f63a6b | 1,013.12 | txt |
| 32 | Ethical Hacking in 15 Hours - 2023 Edition.mp4 | c3280985715154cee35de2f521f0bf23 | 597.37 | mp4 |
| 33 | Evenescence - My Immortal.mp3 | 6a39f3dc37ba33a5c4d548cd8b41feee | 4.07 | mp3 |
| 34 | Ferry_Corsten_Corsten_s_Countdown.mp3 | b44642c61f2abeeb57b30caaf8aaba82 | 76.70 | mp3 |
| 35 | HitMan.2.Gold.Edition-ZAZIX.iso | caf4aea597b4686ba7360ffab9a9d74c | 23,174.78 | iso |
| 36 | jack-b-l55ioqdp474-unsplash.jpg | a975d86c171ea93b9e6876bdfdb69333 | 4.30 | jpg |
| 37 | John Bon Jovi - It's My Life.mp3 | ecf1797cd554cb21c09d842ff2ee3f87 | 4.30 | mp3 |
| 38 | JurassicWorldDominion.mkv | 1c167ae7db2ba52bc71d787991026da4 | 2,746.52 | mkv |
| 39 | korani-greek.pdf | fe26ae1f1d148c73bfd9208b5680a01f | 24.81 | pdf |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 40 | Linux Privilege Escalation for Beginners.mp4 | e0a89bcb31652b720bc8f4793b67c652 | 560.00 | mp4 |
| 41 | Maldives 12K HDR 60fps Dolby Vision.mkv | 86ab117635b945760d03f22bc30597c8 | 1,005.06 | mkv |
| 42 | MALWARE ANALYSIS - VBScript Decoding & Deobfuscating.mp4 | 9ce50af1fdb684e7aa8da10e347c92fb | 161.73 | mp4 |
| 43 | martin-bennie.jpg | 9a673277ba7e1ca8c9505093362306ce | 5.07 | jpg |
| 44 | mixkit-waves-coming-to-the-beach-5016-4k.mp4 | 151220e60ab826d9d1dc48ccc6b54448 | 36.81 | mp4 |
| 45 | Most Popular Operating Systems 1999 - 2022.mp4 | 2de1cdb1408be8d707f16a961ce4ece6 | 10.20 | mp4 |
| 46 | Most Popular Websites 1995 - 2023.mp4 | 58b36dedee81f7ff81cf43b8d3560703 | 41.46 | mp4 |
| 47 | mostafa-meraji.jpg | 47912f5e649799ed31a637fc8411638e | 5.48 | jpg |
| 48 | my SUPER secure Raspberry Pi Router (wifi VPN travel router).mp4 | c8d85f508ec4513ba52aa0779cd521ec | 81.22 | mp4 |
| 49 | NATURAL BEAUTY 8K ULTRA HD.mkv | a75bed26bb568b44a19e984798426063 | 12,586.56 | mkv |
| 50 | nature-tall-pine-tree-forest.mp4 | b418d841164b5f2697bb1f72e3d70efb | 117.02 | mp4 |
| 51 | NEW MOVIE TRAILERS 2023 4K ULTRA HD.mkv | 6b28eb92b14fe88d567a1b29c68af79f | 9,660.31 | mkv |
| 52 | NOPE.mkv | f77fc454a40f551e6a86b04a0e867d08 | 2,729.00 | mkv |
| 53 | ocean_with_audio.mp4 | 14b631184bb5eecdd8c08a078fe3a3d4 | 16.71 | mp4 |
| 54 | oil_painting_realistic_portrait_smoke_effect.zip | 9f83252df19db145db5cdfad8e3f1223 | 45.31 | zip |
| 55 | pexels-charles-parker-24fps.mp4 | 87ee241dd34a8e3682b28c346db233ed | 28.28 | mp4 |
| 56 | pexels-mikhail-nilov-7441154-1920x1080-25fps.mp4 | 47c14612aa597954cea8bb3d74e63e32 | 14.99 | mp4 |
| 57 | piggybank-1pJSWFdyJ98-unsplash.jpg | bb6ec4aee5eaedd97599f31f5e67c507 | 5.02 | jpg |
| 58 | piggybank-RR4SnaM7Dqw-unsplash.jpg | 3fd6c46708c15ae7bc6a1e963b17e47a | 4.24 | jpg |
| 59 | rhamely.jpg | 64b49514cff87f83c6ba37d57212dd01 | 1.85 | jpg |
| 60 | rodion-kutsaiev-0VGG7cqTwCo-unsplash.jpg | 9956731b6f021779ee358de5d27a5208 | 5.38 | jpg |
| 61 | sampe text file.txt | e65891d5b7df76ab6a1761073e774359 | 0.00 | txt |
| 62 | sample text file 2.txt | abffe85bd7f1dd990ab4f8d1a8e05879 | 0.00 | txt |
| 63 | Sample video-AZ-LAGOA.mp4 | feaa9b797568d9b076c67b8fb61be15c | 110.01 | mp4 |
| 64 | Sample word document.docx | 9fb58da8785cc2ad4a9f4815109d3795 | 0.83 | docx |
| 65 | sangga-rima-roman-selia-rDH2ND9Ajjo-unsplash.jpg | 13db06b7a8283da317306a1839d4cd05 | 3.71 | jpg |
| 66 | seat_office_furniture_chair_sofa_icon.ico | 4e1c4511130aa2feb6aac231a993037c | 0.06 | ico |
| 67 | Service,_Inc.tif | 966c61882b54385aff2d4cd64f687f04 | 154.94 | tif |
| 68 | sixteen-miles-out.jpg | 92edab624890b34317af0f8e71b203f4 | 1.41 | jpg |
| 69 | SnapSave.io-OSINT_ Gathering Intelligence with Spiderfoot and Kali(720p).mp4 | 0cb1d1d6d8bb7f79b4e8b99dbe4b349e | 324.90 | mp4 |
| 70 | sobhan-joodi-VaH8Q1BU024-unsplash.jpg | 96f92d9508cb5d68c95cf6f48a872131 | 3.45 | jpg |
| 71 | sofa_table_furniture_seat.ico | b0d4d20b9fb890505544a6a961b67b29 | 0.06 | ico |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 72 | spin earth.mp4 | d7a3decdb6280eb0ef3a059ac35ea0ee | 17.01 | mp4 |
| 73 | Sunset plan.dwg | fb6332e0133a1ad256e962f5392dfab5 | 17.16 | dwg |
| 74 | The Whole History of the Earth and Life.mp4 | f1006f7ae92f98cf224b0cabd6fb9f4e | 318.20 | mp4 |
| 75 | torbrowser-install-win64-12.0.4_ALL.exe | c516a833ca713c1ea4e84e7f505f9435 | 91.48 | exe |
| 76 | VirtualBox-7.0.4-154605-Win.exe | bf83a6171e669d9cbfc3fd353c5ba8db | 105.18 | exe |
| 77 | wikipidia-pages-articles.xml | 28c49835614fba639b682e654c61eb61 | 88,103.42 | xml |
| 78 | woman-edits-images-on-her-laptop.jpg | 5bc1d6c451fbfa1d13bbb14e345cddbf | 1.16 | jpg |
| 79 | working-late.jpg | a8fc039aae249cc31ed5856c727d484c | 1.73 | jpg |
| 80 | Η Αγία Γραφή.pdf | ad3e13d6d8a739d8d537337bfbbd71fa | 21.52 | pdf |
| 81 | 11644206393_9777bcaedf_o.jpg | caf11f4b99950d6f594111b476961fcd | 0.79 | jpg |
| 82 | 12343231794_18db46a3e7_o.jpg | bf8b04e698a11ecc50398acafec7f98f | 1.46 | jpg |
| 83 | 14262360472_d05a5366d5_o.jpg | b058a0ede550bf9d833b019cabc60d01 | 1.48 | jpg |
| 84 | 14287976430_44e48d3bd1_o.jpg | cf17473457d883d52f4b1b2b4d4cb2d8 | 0.79 | jpg |
| 85 | 15000016599_ba7f830f1a_o.jpg | e2ae64a406f831b4f43f30500eeff3bc | 0.67 | jpg |
| 86 | 1575760775_20-35.jpg | 591918286b5fa0261b53e1c951076259 | 0.72 | jpg |
| 87 | 162482-technology-template-16x9.pptx | da0b94dfb079b65262d4931ba0e5aaf4 | 0.82 | pptx |
| 88 | 172908f6d96ud3g903g3w4.jpg | 85e1362b941968e83dbc92d5fd13e1a4 | 0.91 | jpg |
| 89 | 174954230.jpg | 490a2f38f3c52ac93c64674409425581 | 0.94 | jpg |
| 90 | 180301125722-burj-khalifa-dubai-guide-5.jpg | 2981018747ef3d89a7b5ee4094cd0c94 | 1.02 | jpg |
| 91 | 20190103tripadvisor-legjobb-uti-celok-20181.jpg | 1354317ce02deb53f6df3c3b2293fd66 | 1.22 | jpg |
| 92 | 211553.jpg | f33b44ff2583f84efe8543d5f1364ddb | 1.20 | jpg |
| 93 | 23356759823_367c216726_o.jpg | 8ab30c3dea06feaa977c9e3cd2bb38ad | 1.41 | jpg |
| 94 | 24518474097_5be5b66ddb_o.jpg | 4dca70c5a1e5bff39d865eeba9d63c79 | 1.25 | jpg |
| 95 | 24935671220_08e30244fa_o.jpg | 7d6098d7c734a51a3ada0e46a36b8e44 | 0.54 | jpg |
| 96 | 25299715274_dba19dc953_o.jpg | 42846ceafc00d40fbbe572debce23dbe | 1.26 | jpg |
| 97 | 26594860629_45f884d621_o.jpg | 0669320e8f102ae608ab2fe779a3ed8b | 0.55 | jpg |
| 98 | 26594864009_1380ee7bd5_o.jpg | 1e7ea4776a4a0559926985b935a5c8f0 | 1.08 | jpg |
| 99 | 27027973158_966d1934e5_o.jpg | 3975ac53fec9b6d52bbcf06ab4acc3c2 | 0.91 | jpg |
| 100 | 27632067869_f9c9a3db80_o.jpg | dc9f0f2ace6a579795a6f8867dde6cc5 | 0.96 | jpg |
| 101 | 29095872020_722b7e5671_o.jpg | ccb92852efc46e5acb0ec3d1d4198579 | 1.18 | jpg |
| 102 | 29483948964_cef2222b89_o.jpg | efc0c05dfb8de98ecbd884d4bad98331 | 1.35 | jpg |
| 103 | 29707533051_ae26459b7b_o.jpg | c76d8d4af80bd989d94850a9aa9879a8 | 1.82 | jpg |
| 104 | 29776422193_4a89a16f7d_o.jpg | 69bac92cd102490fd4bf6ddcf7d13213 | 1.64 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 105 | 29803379066_4e23e0f7e0_o.jpg | 5ac7e1d6f2b09b0d5a090031a43f678c | 1.61 | jpg |
| 106 | 30081677473_8c8e09c478_o.jpg | 4e0c3874af70f0d782c7f255ebd04cb4 | 1.25 | jpg |
| 107 | 30199416351_ba6d611ed9_o.jpg | bef0dfeba3da3df873d24af639211f4b | 1.54 | jpg |
| 108 | 31049557664_c38340da28_o.jpg | 428145c18956fc3daee0c4f1fdd76bb7 | 0.36 | jpg |
| 109 | 31176746853_a36f51a36e_o.jpg | e3373e6ffc63df6ba1d75509c3811e34 | 0.98 | jpg |
| 110 | 31215843072_a1fcba4850_o.jpg | 83ef5216ac7d9cee8d9cab3ec9024145 | 0.89 | jpg |
| 111 | 31270122883_445de899c6_o.jpg | 4f8e904e123922a2c2c8dd66c70f969c | 0.45 | jpg |
| 112 | 31611820357_0a5ef5335e_o.jpg | 783d33e9632f7f63aae84f9ca9c2413e | 1.53 | jpg |
| 113 | 31611822167_3a07d7a823_o.jpg | 3370196ba6810f8b368bb36e89466c56 | 1.63 | jpg |
| 114 | 31705078450_59796c19dd_o.jpg | c059ed03067225d8e8b0d78440a22b08 | 0.75 | jpg |
| 115 | 31809500946_ae02a380ff_o.jpg | 0d6116983471374d462b977e01de547b | 0.87 | jpg |
| 116 | 31932142592_26d2c30535_o.jpg | 379756eeaf035c0b7605323b45f25648 | 0.96 | jpg |
| 117 | 31932151792_f76edf0b7e_o.jpg | c1022fa5c51a2695aafcae7d6070a544 | 0.87 | jpg |
| 118 | 31962759751_3a5b83248e_o.jpg | 6ac53b23c06b710236a018b511db9353 | 0.85 | jpg |
| 119 | 31985981015_7843e267dc_o.jpg | bfb5e491df5821475bd4360af946e090 | 0.99 | jpg |
| 120 | 32605570867_abd136d001_o.jpg | 979599fe6470bd1755bf5ffc12849e31 | 1.52 | jpg |
| 121 | 32749801330_02912e66bc_o.jpg | b72eecca029f93e05e37c09464b1ced2 | 0.84 | jpg |
| 122 | 32791566858_0e8907f70d_o.jpg | f008781f140db07a49e17a0857a92c06 | 0.76 | jpg |
| 123 | 33022868261_c6669ecd9f_o.jpg | 272a7b4e3b5f3129566156e495620b2a | 0.95 | jpg |
| 124 | 33108698636_4780c4ffea_o.jpg | ca15169ad5a1da4d63d89036e0265878 | 0.90 | jpg |
| 125 | 33671450728_58be8fe167_o.jpg | 10049320c55e14edf017b62597282add | 1.70 | jpg |
| 126 | 33753233180_61af970655_o.jpg | 62c7e862b2c9d1d06001088bac918839 | 1.34 | jpg |
| 127 | 34080101726_6d8b61e705_o.jpg | 8af84b0126df4a854f3156bf54f021b7 | 1.12 | jpg |
| 128 | 36470361916_1d52bf54e6_o.jpg | 658ab7ef12d7a9a38b0feba384493cdd | 0.59 | jpg |
| 129 | 38460416570_87defac692_o.jpg | fb80a0dc5a89aa4c198e5b954b16bd8b | 1.81 | jpg |
| 130 | 38478514360_ab0ca13bfc_o.jpg | 90238c1e08fd66ecbc5979dfcdf667c4 | 1.07 | jpg |
| 131 | 38478663680_78fe02c4df_o.jpg | fbf9f5b60752854e822516213da0c189 | 1.72 | jpg |
| 132 | 38701089584_cffe5041d7_o.jpg | 84813082e62f8f0d0a2e255dfbc2846d | 1.03 | jpg |
| 133 | 39365259735_0dc026e7ab_o.jpg | a74f299ca185fbee6bfac11ea9da5c76 | 1.55 | jpg |
| 134 | 39714948323_c6f1e0feb7_o.jpg | 4ee7848440188a2ccd8d471dbe0ae32b | 0.85 | jpg |
| 135 | 39884887263_f781fd6cfe_o.jpg | 84fa11061978fd85d61fd978fc6fa2bb | 1.38 | jpg |
| 136 | 39941940585_d057ab382c_o.jpg | e2b39739a6bb3e7039d55373cba745e9 | 0.91 | jpg |
| 137 | 40249365381_c8da6373e6_o.jpg | 4914e563f563079ea6c37063d263c766 | 1.87 | jpg |
| 138 | 40249371581_3fea2fb9c0_o.jpg | a16c903e95bf2966751bbf08b3b2aa01 | 1.66 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 139 | 40943374852_8dd861f417_o.jpg | c4b9b1bb2938ce38f5f1da28fb8dc957 | 0.90 | jpg |
| 140 | 44734893310_28dd505b0d_o.jpg | 5f788d9157f683de23bb2a858fc59e30 | 1.31 | jpg |
| 141 | 45647484805_5b9f1e0e8b_o.jpg | 0ff0fb2eaf3bb178b1ae880204bec1e8 | 0.95 | jpg |
| 142 | 45829179764_a4582b16b5_o.jpg | 71ca3b72891cdb69a6cbba1c2a404c8d | 0.78 | jpg |
| 143 | 45829179764_a4582b16b6_o.jpg | b6d60e75a621913a78c09f56a453fbd2 | 0.81 | jpg |
| 144 | 45829179764_a4582b16b7_o.jpg | fd09ce202f5ed3cf7743d7e58b95bcc4 | 0.87 | jpg |
| 145 | 45935621735_f2519f541d_o.jpg | a3ecbef4bc94d3dd7fac8b3f67e14967 | 1.42 | jpg |
| 146 | 46782678224_d42c1f79ed_o.jpg | 5805db193efb3a9add3f31b8dee80dd1 | 1.60 | jpg |
| 147 | 46782678564_f16bd553f4_o.jpg | 0037ead9d8a9e98dd5ca1067ad523a2e | 1.66 | jpg |
| 148 | 49080329543_b3caa23870_o.jpg | ce6af157bcbc490f4f375456f44da92f | 0.92 | jpg |
| 149 | 49237894107_f4a29b5246_o.jpg | f4d53dcc373363291665d4cd32d85889 | 1.66 | jpg |
| 150 | 50398808981_822aae282f_o.jpg | a2fe2745c7a8137fef6f609f0b6ed439 | 0.78 | jpg |
| 151 | 50548231746_e56d2e021b_o.jpg | 7ee6b81aa107d0daa5e2847bf172cc2d | 1.55 | jpg |
| 152 | 50682617956_18177166e9_o.jpg | b479a712717248539714d70cdfa70821 | 1.55 | jpg |
| 153 | 50682682337_d54c92ef77_o.jpg | 89f36ccf29103244968bc75a1216f0f0 | 1.56 | jpg |
| 154 | 50723068896_1a013a9a5a_o.jpg | 485f8070ed69b486346ead18e9773c50 | 1.11 | jpg |
| 155 | 50732543798_e8b6470eb1_o.jpg | e3aa4e0f6e9e3ddb3b3e1c2d9f8f1a85 | 1.25 | jpg |
| 156 | 51301521816_63f84249f3_o.jpg | b8e0a6bb1d3cade373444f27039596c3 | 1.37 | jpg |
| 157 | 51302236799_2ffe36fcac_o.jpg | 65ca6cc9bbc8dc6caebcc3a859278158 | 1.22 | jpg |
| 158 | 51735889901_06954ae821_o.jpg | 663234ba1ac7c1c2cefb42dde131c889 | 1.04 | jpg |
| 159 | 51736127573_8cfd49a453_o.jpg | c8f09c175cefd65127d583ae9a150309 | 1.20 | jpg |
| 160 | 51783617574_a24e4f4f68_o.jpg | 3c432aa4ee49d9f03f4e9d94ffae28bf | 0.85 | jpg |
| 161 | 51801943658_2307f01cb6_o.jpg | c351af6ddcdba63488da1e24fffe5721 | 1.31 | jpg |
| 162 | 51818599064_5258c90cc0_o.jpg | b1fcccd76808cc41bab154386988c737 | 0.90 | jpg |
| 163 | 51850400510_756ae0507c_o.jpg | cf6f118b928bfd6fe765268247119ec6 | 1.07 | jpg |
| 164 | 51861735688_02e9bc93fb_o.jpg | 63b56861652cbafa977c45a973e3133f | 1.13 | jpg |
| 165 | 51864736147_990c96b8f8_o.jpg | e3d6fcbe9d0dcb400f1c472f29109385 | 0.98 | jpg |
| 166 | 51864792117_e47ce8f522_o.jpg | 94aeb2dbc170f0ecd51d05ec0e088616 | 0.76 | jpg |
| 167 | 51888311182_9cbe0c4828_o.jpg | 4f49cca5e136bc2f93107eb0b592ebd3 | 0.73 | jpg |
| 168 | 51948462676_caf64fdb04_o.jpg | 82d400345a53733a971a19392b66e3e0 | 1.30 | jpg |
| 169 | 52050647585_86c878afed_o.jpg | 03839facfdb6358abcca2df37bed40b5 | 1.11 | jpg |
| 170 | 69541677_l.jpg | c01b7327d421e7926ed742d147d9c22e | 1.41 | jpg |
| 171 | 7184668167_62d7d127a6_o.jpg | a53671c5e84a9ead34dbca7e8d04528d | 0.82 | jpg |
| 172 | 7243876768_cbf00d63cc_o.jpg | 6a1ef823785ffb911ff1f3be0438b0ee | 0.62 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 173 | 7243876768_cbf00d63cc_p.jpg | 85e72927ba773e4bf6db611265f18978 | 0.61 | jpg |
| 174 | 8171221407_d836c1af19_o.jpg | 61bc57af1a7aea2bf3f8a156c5b91049 | 0.61 | jpg |
| 175 | 8339124554_288deb986e_o.jpg | 3412fc7775dedf191eecf53c0ead36d2 | 0.83 | jpg |
| 176 | 9290508575_3bdcff306a_o.jpg | 326e58a5c7c2796832fc4d2144d371fb | 0.84 | jpg |
| 177 | 9290508575_3bdcff306b_o.jpg | 5be503cdff85754e9096eb1d8cee7608 | 0.83 | jpg |
| 178 | 9290508575_3bdcff306c_o.jpg | be4dbb590277abc59ad9fa5d76497a54 | 0.76 | jpg |
| 179 | ADH_ADBOH_EXTERIOR-DAY_AMBIENT_HR_03.jpg | 721524a895c935f9d9f71f2780cc94ee | 1.24 | jpg |
| 180 | ADH_ADSVH_EXTERIOR_AMBIENT_HR_04.jpg | c32856d6d216727d49c96bbc2a469bfc | 0.74 | jpg |
| 181 | AdobeStock_66769497.jpg | 4e27b7668e3e862a6e637079dd556b8a | 1.22 | jpg |
| 182 | AdobeStock_94572528.jpg | 255ecd4e36f4386c99c68f931a591c91 | 1.41 | jpg |
| 183 | adrien-olichon-WVOh2Z6eGV0-unsplash.jpg | e7c4d54581ccf688cd37ea8d3592745b | 0.59 | jpg |
| 184 | Agence-ASD-DUBAI.jpg | c2db5677d8e9d4491bdfe3a8d416f4d6 | 1.29 | jpg |
| 185 | ahmed-galal-5-2FD8DCfB0-unsplash.jpg | bdaa07a36297a6aa061f3708f8ce9d8b | 0.61 | jpg |
| 186 | ahmed-galal-F5crZVukKMo-unsplash.jpg | 6d429fc62aa0c02c17878394fa7548bb | 0.66 | jpg |
| 187 | al-mars-tower-jumeirah-lake-dubaii-a.jpg | 95f732b766ceefe00ee38f8b92f7f4a7 | 1.87 | jpg |
| 188 | al-mars-tower-jumeirah-lake-dubaii-b.jpg | 557335a6d3e5649da7c0981c99178cc1 | 1.84 | jpg |
| 189 | al-mars-tower-jumeirah-lake-dubaii-c.jpg | 276a7a3d4d306f1b2e79ed59555f1f72 | 1.83 | jpg |
| 190 | albert-s-YpQYuKd-z8k-unsplash.jpg | e5af1558388093041e266cf66135f565 | 0.91 | jpg |
| 191 | alessandro-bianchi-_kdTyfnUFAc-unsplash.jpg | eca223dff66032136d4bdbe79fb3a8c8 | 2.07 | jpg |
| 192 | alexander-grey-uk-no6Yv91g-unsplash.jpg | 84292ac591351746262a0fcb0a98b0d4 | 1.52 | jpg |
| 193 | Amazing Beauty 8K HDR 60FPS Dolby Vision.mkv | 311dca4c704797392b1d1ebed52a0419 | 1,827.82 | mkv |
| 194 | An Evaluation Of Data Erasing Tools.pdf | 37b03377837ec9d6fbd4b5b64bcbdd1a | 1.00 | pdf |
| 195 | andre-valente-qN8A7S2vFbU-unsplash.jpg | ab9784f06ca69a213177df8e826674aa | 0.75 | jpg |
| 196 | andreas-m-4r0uqzk41T4-unsplash.jpg | d29c9dd9d4b973f3a91e4a1c3b1e09b0 | 1.06 | jpg |
| 197 | anne-nygard-c-n3qf8K5xY-unsplash.jpg | 99f4e0ea75a1c0cc6efdac17ba63426b | 1.18 | jpg |
| 198 | architecture-1867301.jpg | 2fefb00e1cf892874b26427439bca93a | 0.62 | jpg |
| 199 | architecture-1867302.jpg | a2501a54b3e194d75c5a145cf8fdc6a8 | 0.65 | jpg |
| 200 | architecture-4756403.jpg | 8c8d42fbb985d8f8aaf135f291c96c85 | 0.82 | jpg |
| 201 | ari-he-euQVngjZGSI-unsplash.jpg | 1870a314f595d8d708099c77c8b335ac | 2.47 | jpg |
| 202 | arsalan-cheema-MriDyFnkl_I-unsplash.jpg | 2eb33c108e1413da217934924feece39 | 1.09 | jpg |
| 203 | asia-uae-dubai-7.jpg | 733998f19b64722b84e0885dc55c1de5 | 0.81 | jpg |
| 204 | Atlantis-hotel.jpg | e50a1ddce68d3482ac3ac779371da006 | 1.87 | jpg |
| 205 | atlantis-the-palm-goroda-dubai-oae-zdani-285918.jpg | 71847eba15fad49290016ddc64c823cd | 1.50 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 206 | Atlantis-The-Palm.jpg | 03d7f1baa6361205f65649b7e8388c76 | 1.40 | jpg |
| 207 | austin-distel-FQ0tfv5xzBA-unsplash.jpg | 6282c3ac89425c669bcb3fab3d36b558 | 2.81 | jpg |
| 208 | austin-distel-jpHw8ndwJ_Q-unsplash.jpg | 2684fafe09b7955d0a0dc43a16d65cc6 | 3.23 | jpg |
| 209 | austrian-national-library-WatsY4S9-nk-unsplash.jpg | dd072bd76f8c3c98fbae62530198f9c5 | 1.59 | jpg |
| 210 | ayadi-ghaith-HHB1Anc2TFs-unsplash.jpg | 5966ec51a6463f02ae924ef0533bab29 | 2.58 | jpg |
| 211 | bastian-riccardi-rEoBwI7hNCU-unsplash.jpg | 414461e529437a6230987d345010b3dc | 1.47 | jpg |
| 212 | bc0d311b.jpg | 5b904535bfcdc74b0ed4bbcdfc2fb1b6 | 0.73 | jpg |
| 213 | Beautiful_night_view_of_Dubai._UAE_135229.jpg | 2fa434a067545358a4faf8d8ad3651fd | 1.52 | jpg |
| 214 | benjamin-brank-NRLu2zOYesw-unsplash.jpg | 873c3e935f9e5f81493a0b0f7f75e517 | 0.90 | jpg |
| 215 | blogging-guide-mMBxumIfuSo-unsplash.jpg | 84312b14f6e5f14ec6627ed0efcb6012 | 3.24 | jpg |
| 216 | board.jpg | 37ca14866812327e1776d8cbb250501c | 0.87 | jpg |
| 217 | british-library-HVvXTQVHCV0-unsplash.jpg | 085de20a521a15acb3e916b1eea63419 | 9.24 | jpg |
| 218 | british-library-SlRpKa60FJI-unsplash.jpg | f0500efbc0672b372cb996fc26ce4848 | 3.40 | jpg |
| 219 | bruce-kamm-O1ulT7On0WQ-unsplash.jpg | 3ae63f2376519f9b3e39e79828f8e1fb | 0.85 | jpg |
| 220 | buri-al-arab-1026866.jpg | be6c62dd7d96f2b28bd1e86bb16247b4 | 0.78 | jpg |
| 221 | Burj Al Arab 3.jpg | b703cfa6ca061039e90bb4d4c06cdd14 | 1.10 | jpg |
| 222 | burj-al-arab-hotel-Dubai-uae-sky-sea-653539.jpg | a672681bbb6d29a9f50a5e3a6c039d7c | 1.12 | jpg |
| 223 | Burj-Khalifa-Dubai-Wallpapers-Pictures-Images.jpg | 38030a2c9b1323cb95e3b703b097eaef | 1.02 | jpg |
| 224 | burj-khalifa-in-dubai-burdzh-halifa-dubae.jpg | fa0e3bc9f29735f5dc79885ba142b917 | 1.65 | jpg |
| 225 | burj-khalifa_4200x2800_98o8f.jpg | 319351d278fbb336354e65fa11faffcf | 0.90 | jpg |
| 226 | Burj.al.Arab.original.6350.jpg | 218d878946ee9e45fb6e52cd7da00018 | 1.04 | jpg |
| 227 | burj_dubai___landscape_by_keyszers.jpg | c9f8fe8672787e018c667dc1b15d4380 | 0.79 | jpg |
| 228 | Burj_Khalifa_NYE2019_013.jpg | 0642b40d6af3a9684b61097c0eafbc6f | 0.67 | jpg |
| 229 | business-bay-bridge-at-dubai_15416743753_o.jpg | 1f3bb2ab8e95bc41d1b71d51656aac8f | 0.82 | jpg |
| 230 | business-bay-dubai-downtown-dubay.jpg | 72b47d6925ab5391e15e1182c4997503 | 1.03 | jpg |
| 231 | business-flatlay-in-india.jpg | 3df970da19e3226165cacf8569b64778 | 2.56 | jpg |
| 232 | c1833068c9547fdb8d040db1bee98312.jpg | 1af17e40a3210e4852094e0414b29424 | 0.82 | jpg |
| 233 | c73612d9d87be7ec9b67966f.jpg | 5c02be4438eefd61e17dba8ca66f0039 | 1.23 | jpg |
| 234 | cd8a0b8f957965f06f3d71bb.jpg | 014462f0a2bd3f7bce90f4735225c070 | 1.67 | jpg |
| 235 | cem-ersozlu-g_F7fPaUDl8-unsplash.jpg | f16052fd761a2644286f26364860f849 | 0.67 | jpg |
| 236 | chris-liu-R0mWlPiK1hw-unsplash.jpg | d5d07ddfb050d073f2a702f8966b2cf9 | 0.53 | jpg |
| 237 | christopher-burns-dzejyfCAzIA-unsplash.jpg | 5323ce1b5c7ef034921c7ee814aa8731 | 2.79 | jpg |
| 238 | city-5366132.jpg | 10d0a92ff989d2bb97e3056de69c6630 | 1.32 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 239 | city-5366133.jpg | c69254ef5c8b61042ac1682ede2458a7 | 1.30 | jpg |
| 240 | city-5366134.jpg | 61629d25f2dea9099429c71957a96da7 | 1.30 | jpg |
| 241 | city-night-lights-skyscraper-1566751.jpg | 9347bd6715a69d84328a71e7f3319e20 | 1.04 | jpg |
| 242 | city-sight-seeing_31809522086_o.jpg | bb5d6d8b4807915569dbfb88468385be | 1.05 | jpg |
| 243 | cityscape_dubai_panorama_skyscraper_4k.jpg | d71850902e2ba4807cbaf98dfb786e22 | 1.69 | jpg |
| 244 | codioful-formerly-gradienta-7E5kq_sW0Ew-unsplash.jpg | 12c09bba00f39838e6c6028a889977b1 | 0.31 | jpg |
| 245 | Credit Cards.txt | 2e75a3ffdb3427e2a4fa8320f3a7184b | 0.00 | txt |
| 246 | Critical Concepts, Standards, and Techniques in Cyber Forensics.pdf | 6377127277a5fb0b5a8b277acad8a621 | 6.19 | pdf |
| 247 | cropped.16_to_9.jpg | ec4e9b7e73067eae8e2e666625f84c73 | 1.34 | jpg |
| 248 | darcey-beau-q8D7WZc40eA-unsplash.jpg | 73db672a5f2f3127b819f569a67f2048 | 0.77 | jpg |
| 249 | dblringexcellence-tplringexcellence-970561.jpg | a7b8f281b52cb1d9352f32188865126c | 1.58 | jpg |
| 250 | dcf220f3296c480affaf5a35.jpg | 33be671254118799fc678245b81a1683 | 1.63 | jpg |
| 251 | demo sound.mp3 | 2688ed914ed6315229fb89e1e916cdee | 5.04 | mp3 |
| 252 | depositphotos_57797419_original.jpg | daaa0b14100e62f5e596335ff2038476 | 1.93 | jpg |
| 253 | deva-darshan-v0zwX1aPlHI-unsplash.jpg | 3c0053f6ff04585e68eb82b83b611320 | 1.83 | jpg |
| 254 | di-A3hODd0s6uI-unsplash.jpg | 404925a99289f0f142568c94ab4117d1 | 0.76 | jpg |
| 255 | di-BN79L6Uqyfk-unsplash.jpg | 14de47a562c18d8816f5cc14aba0a83d | 0.91 | jpg |
| 256 | dovi-o5GIrbrgy3I-unsplash.jpg | 9d0bf128a87b0de112bca22ad6eec5b5 | 0.96 | jpg |
| 257 | dovi-PE6oXZoNPIY-unsplash.jpg | fbacf06db14ddf1ffe83f7493882f8d1 | 0.84 | jpg |
| 258 | downtown-dubai-1.jpg | de01c8274fd332452255f166682e5563 | 1.25 | jpg |
| 259 | downtown-Dubai-burj-burjkhalifah-dubaidowntown-970583.jpg | 978101deb37cb5b5ff2064d2504b3073 | 1.34 | jpg |
| 260 | downtown-dubai.jpg | d2d185973c13a6d7083bd103872da6d2 | 1.48 | jpg |
| 261 | dsc_8581.jpg | 2d509ba9be66451db30952ce28eee303 | 1.08 | jpg |
| 262 | Dubai Marina (2).jpg | cfbfb544044af0a3ae592ccc2879b482 | 1.33 | jpg |
| 263 | Dubai Marina.jpg | a8b649f9f2e8a24036b3fef8caad421b | 2.11 | jpg |
| 264 | dubai-1141567.jpg | c6631c91330f98fefeca54f841713342 | 0.90 | jpg |
| 265 | dubai-1227538.jpg | 789933ca736c9a6ba09d9c66768420f8 | 1.02 | jpg |
| 266 | dubai-1908485.jpg | 82353424370fb679d5fc6ad7fe44cf99 | 1.25 | jpg |
| 267 | dubai-2367021.jpg | 7cdc49aa5b5992ad9a4cc979605ff40f | 1.05 | jpg |
| 268 | dubai-326543.jpg | 6ce5d61961a2d2742046d26eca76418d | 0.47 | jpg |
| 269 | dubai-4-2103073.jpg | 83eb8ff5d5a78087b04b2ae159882a03 | 1.22 | jpg |
| 270 | dubai-4044195.jpg | 0694344ca7a10e6c07388be3a9093c38 | 1.10 | jpg |
| 271 | dubai-4516584.jpg | 014413990127b96dc7b384ec38bfd6d4 | 0.98 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 272 | dubai-4748856.jpg | bfd4cb58423034370e057ef39849d817 | 1.31 | jpg |
| 273 | dubai-4851673.jpg | 0afeb1a49a9911ad5cbf835bdd59deb6 | 0.88 | jpg |
| 274 | dubai-4940303.jpg | 1c74fe0f71604f125252dbf19e9afdc2 | 0.98 | jpg |
| 275 | dubai-4k-wallpapers-desktop-As-Wallpape.jpg | 7863a1cfaf17677fab3acb70aa0eff67 | 1.03 | jpg |
| 276 | dubai-4k-wallpapers-desktop-As-Wallpaper-HD.jpg | 2e336e8abdfe96e75887f3760d586200 | 0.94 | jpg |
| 277 | dubai-5082317.jpg | 7d70cd1b2ddb9196a288be93878b9a79 | 0.77 | jpg |
| 278 | dubai-5082318.jpg | a1914af6874d22427214530bba91c144 | 0.88 | jpg |
| 279 | dubai-5082334.jpg | 270f9c2d0291b66867fac41e08e4a3d7 | 0.97 | jpg |
| 280 | dubai-5082335.jpg | cc1ea3b6e52f7fe6f41ec9e3541e2cf6 | 0.91 | jpg |
| 281 | dubai-5269851.jpg | dc96312f3f71fb4eb937cb7e78c69666 | 1.19 | jpg |
| 282 | dubai-5269852.jpg | b01b6d3c5fbc02c572d03037318c1d53 | 1.79 | jpg |
| 283 | dubai-5293950.jpg | 9da010afde3c9e16893df335aa2ef9fb | 1.03 | jpg |
| 284 | dubai-5293953.jpg | e8ac67aa42cae990bf4c030e668c8363 | 1.10 | jpg |
| 285 | dubai-5911191.jpg | 1a4fefe1bac1035d4bdc3509f2930e64 | 0.44 | jpg |
| 286 | Dubai-burjarab-madinatjumerah-mydubai-970485.jpg | b4ea1d68b21829d5e18422c2ac7fe7b8 | 1.28 | jpg |
| 287 | dubai-creek-4602838.jpg | 8d7a8aa15e9a9a36ccf6322d34b69023 | 1.08 | jpg |
| 288 | dubai-downtown-night-scene.jpg | ed35c1b687b1f7fe7166c8386f552d82 | 2.02 | jpg |
| 289 | dubai-dubay-oae-6ody.jpg | 901a7d9de35ceb27e954b2b792800870 | 0.79 | jpg |
| 290 | dubai-dubay-oae-gghp.jpg | d5dc7f4142cd036f873a44a57f3972ec | 0.72 | jpg |
| 291 | dubai-dubay-oae-ndve.jpg | 3c42af2b141d38ec78a4508c820c8ce9 | 0.79 | jpg |
| 292 | dubai-dubay-oae-ufqy.jpg | 1d5c1b810f72150ae40c349efe222315 | 0.50 | jpg |
| 293 | dubai-dubay-oae-xzld.jpg | d53c679ef3e73d34a75648eb8e30fa79 | 0.40 | jpg |
| 294 | dubai-dubay-oae-yvuo.jpg | 943df8da9b477df6b78f51ab81acbd91 | 0.71 | jpg |
| 295 | dubai-dubay-oae-zrhb.jpg | 82c0c63c5b345661893b8908b1613721 | 0.60 | jpg |
| 296 | dubai-dubay-obedinennye-arabskie-emiraty.jpg | b90a24e7f837adc405f226a5e273edac | 2.52 | jpg |
| 297 | dubai-fountain-burj-khalifa-dubai-mall-cityscape.jpg | cf3d51208970725fe3b9ab48a360781d | 0.88 | jpg |
| 298 | dubai-gorod-dubay-oae.jpg | 7e42fe9767d457dcbc7c1c8994dae126 | 1.02 | jpg |
| 299 | dubai-gorod-noch.jpg | 0e77b5fccd1b8911e5142247a3eb2212 | 1.91 | jpg |
| 300 | dubai-marina-by-night-dubay-obedinennye-arabskie-emiraty-icdp.jpg | 848f24b3a81a42812914d0640ce80fa0 | 1.11 | jpg |
| 301 | dubai-marina-by-night-dubay-obedinennye-arabskie-emiraty.jpg | dfc5feca20b4e603d86258337b9adced | 1.06 | jpg |
| 302 | dubai-marina_2500x1693_ylrhy(1).jpg | 5cb661bd0842556e661862ce1d860176 | 1.11 | jpg |
| 303 | dubai-marina_39394937870_o.jpg | 8309939b138235d0243c31b456f97a5e | 1.98 | jpg |
| 304 | dubai-marina_39839401022_o.jpg | 4d9c9bc22a6464da389b3f5d10440572 | 1.40 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 305 | dubai-marina_41492397631_o.jpg | 6d04f873a0d7db3b2c0d3fb82e1ebe71 | 1.98 | jpg |
| 306 | dubai-marina_44476985262_o.jpg | cff710e6c7d0dc1d3881602a3ad59f34 | 1.78 | jpg |
| 307 | Dubai-metropolis-downtown-landmark-metropolitan.jpg | 4a7ee4b13510563cbe2620f0d1108203 | 1.21 | jpg |
| 308 | dubai-obedinennye-arabskie-emiraty-dubay-cfht.jpg | 2e58f8608acd4db206647f3d02070375 | 0.87 | jpg |
| 309 | dubai-obedinennye-arabskie-emiraty-dubay-iuri.jpg | e0411900ae68fb1258de6e5fefc01cba | 0.90 | jpg |
| 310 | dubai-obedinennye-arabskie-emiraty-dubay-kjzr.jpg | 7c086b5b55869b0a5df4325c579ee46b | 0.98 | jpg |
| 311 | dubai-obedinennye-arabskie-emiraty-dubay-wvun.jpg | 35bbb45baea50fd0fec86126b23b7a35 | 2.08 | jpg |
| 312 | dubai-reflection-water-lights-colorful-city-8F2Q.jpg | c89887d03929c4f6fe12d32fe8e0ad02 | 1.06 | jpg |
| 313 | dubai-skyline-1070127800.jpg | 9394acbba2716d389ab582a52b5c6de7 | 1.43 | jpg |
| 314 | dubai-skyscrapers-battista-supercar.jpg | 1c6f4834dfad6e554729b58af52b5e2a | 0.77 | jpg |
| 315 | Dubai-uae-bluehour-archticture-eos5dii-cayantwisttower-970314.jpg | 7a6a8b45506ff4a4c15a91c19ba26da3 | 1.12 | jpg |
| 316 | dubai-united-arab-emirates-city-awat.jpg | 28589fd4e7cfdd2ba0d4b4eef23ce364 | 1.17 | jpg |
| 317 | dubai-united-arab-emirates-city-rega.jpg | a470fd0e723a246cc6b4c475143e0972 | 1.09 | jpg |
| 318 | dubai-united-arab-emirates-city.jpg | e3b2e60321e7325b63131f96a69041ae | 1.12 | jpg |
| 319 | Dubai-United-Arab-Emirates-Skyline.jpg | 0f078a8699b9b0487fb1aae1111dfd1f | 1.27 | jpg |
| 320 | dubai-united-arab-emirates-sunset-hdwc.jpg | f7c3cd7a5261b0f7bd655bc7208c530e | 0.65 | jpg |
| 321 | dubai-united-arab-emirates-sunset.jpg | b970dd025d3ad94e3ae8783909967084 | 0.98 | jpg |
| 322 | Dubai-urlaub-ereignisse-2015.jpg | fcb153cfb8f5909570cdf189a646391f | 0.83 | jpg |
| 323 | Dubai.jpg | d5b133f6a4b1c757b2145612702cafa7 | 1.86 | jpg |
| 324 | dubaii.jpg | 52dd03a86428cec8394da27884433711 | 0.99 | jpg |
| 325 | Dubai_0.jpg | 5cd83e14714e42ae4b0dd73e70718330 | 1.69 | jpg |
| 326 | dubai_26408308538_o.jpg | 693f117a5d5280a2bcf78417f4a0273d | 2.06 | jpg |
| 327 | dubai_28241577519_o.jpg | 28e4b7061aa604cf2d7e4f664aa73f83 | 1.56 | jpg |
| 328 | dubai_41503586155_o.jpg | ffef4684157e1fdfbd63aab2bc6087f0 | 1.39 | jpg |
| 329 | Dubai_Emirates_UAE_464817.jpg | 1a041e57c2352d5e803fd9c3b3935130 | 2.52 | jpg |
| 330 | Dubai_Emirates_UAE_465326.jpg | 930c7a887aeaf2991d7354b20bb83bd5 | 1.51 | jpg |
| 331 | Dubai_Emirates_UAE_465777.jpg | 1920596bfe9c6947ff4db123950af133 | 2.58 | jpg |
| 332 | Dubai_Emirates_UAE_Coast_Sea_Jumeirah_Al_Naseem.jpg | acbc2c8f38f1b31a9c6da0f6e4559e22 | 0.99 | jpg |
| 333 | Dubai_Emirates_UAE_Houses_Skyscrapers_Roads.jpg | 9aa473c0f0649a52143cda1468323214 | 1.72 | jpg |
| 334 | Dubai_Emirates_UAE_Skyscrapers_Megapolis.jpg | a22ff1f9b36f3b004e671755f094b0bd | 1.55 | jpg |
| 335 | Dubai_Emirates_UAE_Skyscrapers_Motorboat_Houses_599810.jpg | cd4a7e1d2a99cfdd79f4594d831d5b7a | 1.22 | jpg |
| 336 | Dubai_Houses_Night_472520.jpg | 0dc3d702ba59fffc531ef9fcd6a21d1c | 1.34 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 337 | Dubai_Island_Palm_Jumeirah_From_above_592728_4944x3253.jpg | f95bbb6f8089b24b36ba0ca2e6986041 | 1.21 | jpg |
| 338 | dubay-oae-doma-sduo.jpg | 6f55c841f66edeeb0db231074f34ef8c | 1.61 | jpg |
| 339 | dubay-oae-dubai.jpg | f51b1a470ff1a5868819b574904bcf5b | 0.75 | jpg |
| 340 | dubay-obedinennye-arabskie-emiraty-dubai-drso.jpg | 4198328e2ce779be2f14c212dc20478e | 1.13 | jpg |
| 341 | dubay-obedinennye-arabskie-emiraty-dubai-suov.jpg | 5280571ec5fb789efc46bb3cca0da990 | 2.22 | jpg |
| 342 | dubay-obedinennye-arabskie-emiraty-dubai-uuad.jpg | a29a6331735732c4b0a60a4de9991761 | 1.26 | jpg |
| 343 | dubay-obedinennye-arabskie-emiraty-dubai-vdss.jpg | 22e527c02865047fbf8763b8431e7d78 | 2.11 | jpg |
| 344 | dubay-obedinennye-arabskie-emiraty-dubai-ywcb.jpg | bf1342f0daeaebb49e0763b1ad756b87 | 1.57 | jpg |
| 345 | dubay-obedinennye-arabskie-emiraty-dubai.jpg | 0b733a281b915acde307afb9b2e21324 | 1.90 | jpg |
| 346 | dubay-obedinennye-arabskie-emiraty-gorod-dete.jpg | fc7c27486058300ed41afea2a3a7d718 | 1.68 | jpg |
| 347 | dubay-obedinennye-arabskie-emiraty-gorod-glko.jpg | 27557ecaab0c4412ceb1ff842db7c752 | 0.55 | jpg |
| 348 | dubay-obedinennye-arabskie-emiraty-gorod-icfa.jpg | 5c5a144303e37c200f7bc6aa6ec19cbc | 1.22 | jpg |
| 349 | dubay-obedinennye-arabskie-emiraty-gorod-ipsv.jpg | 5ad907291eed3d6381e7be64a44919f4 | 0.68 | jpg |
| 350 | dubay-obedinennye-arabskie-emiraty-gorod-kqyo.jpg | d1c2270f4ec354c291cb71c0bf223cf3 | 1.77 | jpg |
| 351 | dubay-obedinennye-arabskie-emiraty-gorod-kxlo.jpg | 02b3fa54ab6f83e13b830781324760ac | 0.73 | jpg |
| 352 | dubay-obedinennye-arabskie-emiraty-gorod-linw.jpg | baeb68b2f334183685aad12b1f543366 | 0.31 | jpg |
| 353 | dubay-obedinennye-arabskie-emiraty-gorod-reyn.jpg | 09d4559ea6fddb05ce17b3e0a0534284 | 2.32 | jpg |
| 354 | dubay-obedinennye-arabskie-emiraty-gorod-tjbz.jpg | 467bdcb02c25c0bcd6aec98f34848caf | 1.93 | jpg |
| 355 | dubay-obedinennye-arabskie-emiraty-gorod-xvil.jpg | 227c3157b7f8e59017d689469f5186a0 | 0.63 | jpg |
| 356 | dubay-obedinennye-arabskie-emiraty-gorod-yrzr.jpg | 1350dc2171f42fa5779c75d461bd5408 | 0.77 | jpg |
| 357 | dubay-otel-plyaj-yahtyi.jpg | 6213ed2f96faec42846521b44d7ea2a9 | 1.92 | jpg |
| 358 | DUKES_VIEW_01.jpg | 06447abb096b0d86249fe8e3efcc11b7 | 0.65 | jpg |
| 359 | dxbjw-exterior-0210-hor-clsc.jpg | 9b30bee224f4dcad4b387676048f6569 | 0.66 | jpg |
| 360 | Electric-Circuits.pdf | 050677ebae3340eeecf2308d7197b79d | 8.84 | pdf |
| 361 | electronic-card-transactions-february-2023.zip | e538736aa7414baba8b07a80e091c73b | 0.13 | zip |
| 362 | emaar-nye-1.jpg | 6b1ad1941014b52449b7282ee04ecda1 | 0.75 | jpg |
| 363 | emirates-towers_5818941736_o.jpg | 86acf46adce1df9750d81c1b20050c07 | 1.19 | jpg |
| 364 | Emirates_Dubai.jpg | e87839d9075e53b61b1d048e4a0029ce | 1.08 | jpg |
| 365 | Emirates_UAE_Dubai_443252.jpg | 0e71e44891e6d726342978fee36e6799 | 1.62 | jpg |
| 366 | Emirates_UAE_Dubai_464616.jpg | 57ff0a24a5b0e77b4f37097eebf9afcf | 2.64 | jpg |
| 367 | Emirates_UAE_Dubai_464914.jpg | 069e1a3e94d47f56609ccacf1f348632 | 2.39 | jpg |
| 368 | Emirates_UAE_Dubai_466413.jpg | 61ea4212620208f49fe11d160b5eb6e4 | 1.83 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 369 | Emirates_UAE_Dubai_Houses_Marinas_Night_Bay_558258_5668x3322.jpg | 974b80b6da2a0e7794698f74f844d254 | 1.87 | jpg |
| 370 | Emirates_UAE_Dubai_Houses_Skyscrapers_Business_Bay.jpg | a30fa251ff2dd130b786364fa795e535 | 0.85 | jpg |
| 371 | Emirates_UAE_Dubai_Houses_Skyscrapers_Jumeirah_589441_4500x3000.jpg | 7a7abaed523b9a0e9b5751bb62deaa77 | 1.13 | jpg |
| 372 | Emirates_UAE_Dubai_Houses_Skyscrapers_Marinas_587017_5120x3413.jpg | c4b9ee10719731d20b3c56d818f2f106 | 1.17 | jpg |
| 373 | Emirates_UAE_Dubai_Houses_Skyscrapers_Yacht_Marina_598181.jpg | 73d4110d44b20786b173bf1209953467 | 0.93 | jpg |
| 374 | Emirates_UAE_Dubai_Umm_Suqeim_Waterfront_587064_5120x3413.jpg | 1858f970ac07cdb24d88381607c646e3 | 0.95 | jpg |
| 375 | entrances-and-exits-from-dubai-mall_51241649504_o.jpg | 7ceaf998808a9a86219b86748ebaf8f9 | 1.26 | jpg |
| 376 | ewan-kennedy-S8ZzjfWwer4-unsplash.jpg | 90d9a64186ade903a3f1590b9f68b556 | 1.34 | jpg |
| 377 | fabio-oyXis2kALVg-unsplash.jpg | 16b7e02535028fd21c1fda4acfe24cc6 | 0.21 | jpg |
| 378 | faizan-rao-7rpCd9BjpqQ-unsplash.jpg | 504e6ab816ae99c29cc504f9ff0997e8 | 0.51 | jpg |
| 379 | ferris-wheel-4792152.jpg | 59aedf2967cd700304dd06316c4f2ccc | 0.59 | jpg |
| 380 | FLYING OVER CHINA.mkv | a3915fdc55a6c7e2446ab0f0899062e8 | 3,912.56 | mkv |
| 381 | fog-clouds-Nikon-cityscape-skylines-1034117.jpg | df58a649b9fccd71366d86e91460219b | 0.68 | jpg |
| 382 | fogy-night-over-dubai-dubay-obedinennye-arabskie-emiraty-ghyr.jpg | b3c9e9b78fd1a38899474c39790fe448 | 1.99 | jpg |
| 383 | fogy-night-over-dubai-dubay-obedinennye-arabskie-emiraty.jpg | 29cc67a3ab71dca81a3a64d1c9c80d38 | 0.81 | jpg |
| 384 | GbLBaxp.jpg | 0af11d4ab77872dc97d80132797780fb | 0.86 | jpg |
| 385 | GettyImages-1002325104-1.jpg | 66a0833c00ed7cfcb3555db897c3e896 | 2.14 | jpg |
| 386 | GettyImages-479832494.jpg | 871ce863fd96320e1fed4ee82f8cb452 | 1.14 | jpg |
| 387 | GettyImages-487696283.jpg | f264321ec864c6002880e43b0dd4b735 | 2.70 | jpg |
| 388 | GettyImages-531431765.jpg | cf17d84ba1befa42dbbbab0d03d6ab52 | 1.60 | jpg |
| 389 | GettyImages-911190496.jpg | b3a299a2969355a81d6cfd0c6cbc8cdf | 0.98 | jpg |
| 390 | gorod-dubai-noch-nochnye-ogni-neboskreb-reka.jpg | c961c21e4e27f6264df3b3e37970055d | 0.84 | jpg |
| 391 | grand_canyon_panorama_samsung_sample.jpg | da86fd83a233f7f9be7b23333c1fbfa5 | 1.80 | jpg |
| 392 | Grenade_container_5912403.zip | 70ffdd86fe65bd0faa48eebe04da75ec | 2.43 | zip |
| 393 | harbor-6084470dea314.jpg | e8341261fc15524eec638ecc376ca98f | 0.86 | jpg |
| 394 | hilman-luthfi-4Zjzhs6BPZM-unsplash.jpg | 674ba7066cc2de4e0ff2c9d959ae7a0c | 1.46 | jpg |
| 395 | hochhau-theaddressdowntowndubai-970540.jpg | 8a41df2394893e206e15045829e2b338 | 0.74 | jpg |
| 396 | Houses_Skyscrapers_Marinas_Dubai_Emirates_UAE_553087_7639x5376.jpg | cc68d88bebe8ca53fac81bd9e7f942fc | 1.13 | jpg |
| 397 | https __www.lifeofpix.com_wp-content_uploads_2018_04_Dubai-view.jpg | a16b77841e3b9ace4399b3226de02659 | 1.32 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 398 | i-2Bw4vkz.jpg | dc6ee9901f3e0ec654dd68f34e71fa2b | 2.12 | jpg |
| 399 | i-3tf2LpF.jpg | 51470449ba660e903254d13e34ddedaa | 1.32 | jpg |
| 400 | i-466r3vv-5K.jpg | 46d2f1cc1a5e87ffa9c2d851679a40b5 | 1.15 | jpg |
| 401 | i-47n9bGd.jpg | 027b083df4e816a5dd5f7bc2f66672f9 | 1.32 | jpg |
| 402 | i-8KLjRVp.jpg | ecf21fc43a22e2b9d7e4336fa6caf4bb | 1.72 | jpg |
| 403 | i-9WmrDn4.jpg | f2d3a184ba9fe52992c2f5da328a7ce9 | 1.07 | jpg |
| 404 | i-CTtP9TP.jpg | 2396245f9ec72cd0870494ec61e2a365 | 0.99 | jpg |
| 405 | i-DLbLkHx.jpg | 33e84ae7eec672480388932adbbacb65 | 1.00 | jpg |
| 406 | i-dNVHSzd.jpg | 853c111e424db1c4b3fcbca29e0c19af | 2.07 | jpg |
| 407 | i-f3bk55n.jpg | 128053b594f1f5a45bf4887233116f44 | 0.56 | jpg |
| 408 | i-GnKfrC5-a.jpg | c35b5c28ff2308bf0ea2618478cd6c99 | 0.62 | jpg |
| 409 | i-GnKfrC5.jpg | 34dd161d292e4cc5d09050ff4e407f8a | 1.36 | jpg |
| 410 | i-gQMWpqQ.jpg | a365fe7b4a9770090ee4c1f3b94e9edf | 1.45 | jpg |
| 411 | i-GqNqcPK.jpg | 3cb2be8ef6e46788ba1e9db7ed6d73c1 | 1.29 | jpg |
| 412 | i-hBqcFTN.jpg | e2bb0097afbc7184ded639f548acbaf5 | 2.21 | jpg |
| 413 | i-k6RG6hS.jpg | 913b4cde789dec338385bdbe1488826f | 2.34 | jpg |
| 414 | i-KX6pF36.jpg | 424b26315d742def9d797b49064e1740 | 1.61 | jpg |
| 415 | i-MPV4K34.jpg | 26c91d71e4cef3cedf230e648dc3ce93 | 1.61 | jpg |
| 416 | i-PFZnxSR.jpg | 435954a88bf3b9a8fe1baf94b6fa6779 | 2.26 | jpg |
| 417 | i-pWNMr4D.jpg | a94d36cdfd6ea66d53900c96d8b02019 | 1.59 | jpg |
| 418 | i-pXhncjM.jpg | 848a3598689117e6aa66b74798a5463c | 1.35 | jpg |
| 419 | i-QCrjVkT.jpg | 620c5c03abe16f0129f73bf833c33474 | 1.71 | jpg |
| 420 | i-QCsX8zX.jpg | 030e31bc977e3dc1af0e1fc1370d5bc1 | 1.73 | jpg |
| 421 | i-qLv49Lt-5K.jpg | f629ebe5265b4d135892d4e972dad4f9 | 1.00 | jpg |
| 422 | i-RhgtNcf.jpg | 3d0731657e69ee80be793d2c32d7a6bf | 1.57 | jpg |
| 423 | i-rR8smRH.jpg | 3a35df32f9b8fcec93698359677ce2c6 | 2.31 | jpg |
| 424 | i-Spjt7xc.jpg | ad70a045a6f78ababdbe9591b8d984cb | 1.39 | jpg |
| 425 | i-Tk4td92-5K.jpg | 4f31a227f926f9cd2437d6c7f60d76bf | 1.02 | jpg |
| 426 | i-x2B6nJv.jpg | 915fc0ed5bf834e4550a4cc65ab1c009 | 1.67 | jpg |
| 427 | i-XhrVjtd.jpg | eaf08d08cc4fc90ddc7488ac4de5045c | 2.23 | jpg |
| 428 | i-z4t4Jzn.jpg | 2c8210086c1ced3f4391d80e410c902d | 1.97 | jpg |
| 429 | i-ZFqxSPk.jpg | 8b52c86475f2fc629bcbba2939ea25b8 | 2.06 | jpg |
| 430 | i-zHqtZxG.jpg | 34637161c713cc51ff95cb2b809daab5 | 1.89 | jpg |
| 431 | image-20170203-14027-plmo90.jpg | e786a10f4fbb614b84c1aaa9ba7a5f20 | 1.12 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 432 | intercontinental-dubai-4930171844-4x3.jpg | f3fdb053e8d4b390119762d4ae34445b | 1.27 | jpg |
| 433 | iStock_000040552480.jpg | 9febbc8bda0eabd21e65dcd1518eb9cb | 1.29 | jpg |
| 434 | jeroen-den-otter.jpg | 87b4045a9063cad6109f962bfe22df8f | 3.13 | jpg |
| 435 | JMz1w7.jpg | 177ab388c0306c1832eaeb91b83629d0 | 0.88 | jpg |
| 436 | joel-abraham-8RRYJg26Wr4-unsplash.jpg | 5b97fe764b76a059e2139ae867c8adc6 | 0.43 | jpg |
| 437 | johann-siemen.jpg | ec47c1b6b9cb063d138b68736b2ceba6 | 2.87 | jpg |
| 438 | jon-tang-DHVk542D9rQ-unsplash.jpg | de2d904e7742f5203487bd21f396791a | 1.94 | jpg |
| 439 | jonathan-j-castellon-kUg-z_i5arU-unsplash.jpg | afc8eeb026006e0ae0a51344756f4424 | 2.27 | jpg |
| 440 | jonathan-sanchez-_C6nNIZ-PVA-unsplash.jpg | d30b73bf1cb7a450fb8ddbe43e095378 | 2.09 | jpg |
| 441 | josef-ivan-jimenea--mP3-QqJLKU-unsplash.jpg | c7c8c639b3600f9b1f507347cf9defe7 | 0.81 | jpg |
| 442 | josef-ivan-jimenea-XVwjO89bxiI-unsplash.jpg | d240d30d6c125a0414764f451754b337 | 0.75 | jpg |
| 443 | juliana-vkKpmzdDuDg-unsplash.jpg | 577b4124f12cb25b26a37a62dbe1e320 | 0.72 | jpg |
| 444 | Jumeirah-Mina-A-Salam-Fireworks-Madinat-View.jpg | c8921ee6bca71125cb55ea033fcde8bc | 0.86 | jpg |
| 445 | jw_marriott_marquis_Emirates.jpg | 1bd525260512cfd0d3d5a4db26c3611a | 1.50 | jpg |
| 446 | kali-linux-2023.1-installer-amd64.iso | dd2d18cf94853f9adbe12500f31bb788 | 3,696.00 | iso |
| 447 | kel-avelino-Ge5h2W7d9_k-unsplash.jpg | 4c874be877f5df9175473b69c49b0218 | 0.51 | jpg |
| 448 | kenny-eliason-JW6r_0CPYec-unsplash.jpg | 6bf388e937a8448c28f2b04c3cf36d62 | 0.57 | jpg |
| 449 | kent-tupas-BJ6Yfrv93R8-unsplash.jpg | 3bb9526fd3eb477ac558af5b43f325cd | 0.55 | jpg |
| 450 | kent-tupas-Eo6jKTIjIyY-unsplash.jpg | a3f0cf02a885656fe3f83b13ee0f8ab1 | 0.67 | jpg |
| 451 | ktivtunp_lw.jpg | 825ea252ef3ca1c3d460e327acc62be7 | 0.92 | jpg |
| 452 | leone-venter-pVt9j3iWtPM-unsplash.jpg | e30d8d5747199f80fc16690c7ac0411a | 1.13 | jpg |
| 453 | Lisistrati.pdf | db53b97e3be366657c005540499f566f | 0.14 | pdf |
| 454 | longexposure-nightphotography-dubai-marina_3840x2360_vx0sb.jpg | 1b5ba7cc2e95628155337231f7cad281 | 0.78 | jpg |
| 455 | longexposure-sky-water-Marina-boat-Nikon-exposure-Dubai.jpg | 647857feb9eb1bafb4f5e842e26bdc2d | 1.62 | jpg |
| 456 | Lorem Ipsum.pdf | ee7ac8084eeab08035fdcb47bfa81931 | 0.99 | pdf |
| 457 | M0b6CN.jpg | 7d0e2b881dd1e5dbd7f89af3e20a7e1d | 1.18 | jpg |
| 458 | M0b6CO.jpg | fc4b39f25fee1355c657f44e082085c0 | 1.13 | jpg |
| 459 | M0b6CP.jpg | 986a8cbbd268733fa65bc647ed04d848 | 1.01 | jpg |
| 460 | Madinat-Jumeirah-06.jpg | 7e9eeb78d80e76ff93594a7caeb837af | 1.40 | jpg |
| 461 | mahdis-mousavi-hJ5uMIRNg5k-unsplash.jpg | ee3e83eb8bdeffd773666c9c3d7b7574 | 7.73 | jpg |
| 462 | Marina-boat-Dubai-970516.jpg | 04f31825192ff546617d91fe80d2c55e | 1.21 | jpg |
| 463 | Marina-Dubai-relection-dubaimarina-939225.jpg | ab52d01bd8f02305d5993d2a13ed1cbf | 2.21 | jpg |
| 464 | Marina-landscape-high-Nikon-Dubai.jpg | 7aec1a931c5c3871a912a815a51650ac | 0.77 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 465 | markus-spiske-jgOkEjVw-KM-unsplash.jpg | e3544a7dbdb88a819c6cdcc782b28898 | 1.41 | jpg |
| 466 | marra-m7fT6OreZfI-unsplash.jpg | e1649eb3257c90ec2f8acb48a21ada1c | 1.38 | jpg |
| 467 | metro-rail-and-office-towers-dubai_50896039487_o.jpg | bf3aa807f10084f23c9bbdb8e6bc2eee | 1.13 | jpg |
| 468 | metro-station-dubai-united-arab-emirates_51110507253_o.jpg | 0c75a302ee46366920477cff885285c2 | 1.46 | jpg |
| 469 | metropolitan-area-tower-block-colorco.jpg | d0d59304c6e457a70d9e902696c69556 | 1.08 | jpg |
| 470 | mike-kienle-OVn4TjlihFI-unsplash.jpg | 35adc3ec930e392408c7f62b476be285 | 2.56 | jpg |
| 471 | mingwei-lim-yvaWgD12YcA-unsplash.jpg | 10c92b6971645df444f653e10397398f | 1.80 | jpg |
| 472 | miriam-eh-SfsqLqgdI04-unsplash.jpg | a2e9d6b06549621b767fd46bca585b1e | 0.68 | jpg |
| 473 | mo-tj86_D4rK2Q-unsplash.jpg | 8f8dea85c5d7aa415776675f52786b42 | 0.70 | jpg |
| 474 | mockup-graphics-U6ZMEefFGx8-unsplash.jpg | 06b22bf8c4070a60e09fd2ff4c9b73bd | 1.40 | jpg |
| 475 | mohsin-Ru5DQBpgl-w-unsplash.jpg | c22973e725dede973353cc0489c47dfe | 0.99 | jpg |
| 476 | most-tolerantnosti-dubae-gorod.jpg | fdf98c91a0b29924bc1c974714628f09 | 1.38 | jpg |
| 477 | Mother Teresa - A Biography.pdf | bfebd0853043921dabd7a053288d2a47 | 1.08 | pdf |
| 478 | museum-of-the-future_killa-design1.jpg | f1c6b9eefcb39718db9148b2eddb8ce7 | 0.83 | jpg |
| 479 | mydubai-nikon1424-f.jpg | ba4ada0dd916867ae67b5cadb696eb8f | 1.16 | jpg |
| 480 | Napoleon_ A Biography.pdf | 4705fc77ce2412ea11b975370f43b041 | 9.57 | pdf |
| 481 | neutraldensity-nikon1424-nikond800-1011141.jpg | 9d82ea11e824dd222ab14e417ed52b54 | 1.42 | jpg |
| 482 | new-year-post-party.jpg | bb4738c1a20b1678fdee69ef77bffe9d | 1.23 | jpg |
| 483 | niko-photos.jpg | feac6456f08b877e55506e2e0eecac0d | 2.51 | jpg |
| 484 | nintchdbpict000284676210-WEB.jpg | 9e9c8b77c0a8125c2e21ad314c98d606 | 1.43 | jpg |
| 485 | nintchdbpict000306788396.jpg | 9a5f43355351d520f9f46d9ad65e8366 | 1.21 | jpg |
| 486 | nintchdbpict000398497436.jpg | c1b66c57288ce8e87691b16f8039bd0e | 1.14 | jpg |
| 487 | nintchdbpict000410004997.jpg | 44175aac8bbc7aef57ace95b7d4620bc | 0.99 | jpg |
| 488 | NINTCHDBPICT000417796991.jpg | 0c3732f646c83137763c9ccd41899bcb | 0.89 | jpg |
| 489 | NINTCHDBPICT000551804068.jpg | e7a9dfac3422e2cbde5940341f50aeb7 | 1.43 | jpg |
| 490 | nm-dubai-0101.jpg | 4d90c9977c92c465cce1e1237a6b0b2f | 0.79 | jpg |
| 491 | nochnoy-gorod-dubay-oae-noch-neboskreby-dnlo.jpg | cdadcb7332a22454daea745db9369115 | 0.72 | jpg |
| 492 | nochnoy-gorod-dubay-oae-noch-neboskreby-dwfh.jpg | aa8077e2ba599e6df08a854ca1328d83 | 0.87 | jpg |
| 493 | nochnoy-gorod-dubay-oae-noch-neboskreby-kdei.jpg | 59e38768ef745028f3e47275fe9cc58c | 0.67 | jpg |
| 494 | nochnoy-gorod-dubay-oae-noch-neboskreby-quec.jpg | 50147b3c8370851738ad692a3f6f981a | 1.51 | jpg |
| 495 | nochnoy-gorod-dubay-oae-noch-neboskreby-ruug.jpg | 3a8a710e26b3eb4952ecd16f860f62d1 | 2.31 | jpg |
| 496 | nochnoy-gorod-dubay-oae-noch-neboskreby-tkzw.jpg | 98fcc12de1e645da579e36c2ea125b12 | 2.05 | jpg |
| 497 | nochnoy-gorod-dubay-oae-noch-neboskreby-uezj.jpg | 66558b367c51facf049fe328b5dae7c9 | 1.13 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 498 | nochnoy-gorod-dubay-oae-noch-neboskreby-wdpn.jpg | ae8a3649a314c970c408709ca6be06b5 | 1.55 | jpg |
| 499 | nochnoy-gorod-dubay-oae-noch-neboskreby-zvzr.jpg | e3a2351468a8182deb0b5ac6182ca06c | 1.12 | jpg |
| 500 | Now-see-another-over-the-top-building.jpg | e23a86e8de7d127f6c449984509e3228 | 1.23 | jpg |
| 501 | office-towers-along-the-city-highway-and-metro-rail-dubai_50895175553_o.jpg | ed8ce579cb4104aa0eaf11fd6bb6df46 | 1.27 | jpg |
| 502 | omar-bakri-5MtiChVjZGM-unsplash.jpg | dd4d4d56d2351015954bbbb7c6d8ec26 | 0.60 | jpg |
| 503 | panagia2.jpg | 55ea5ef6c7361df3aa0f3dfa71f4eb02 | 0.30 | jpg |
| 504 | Passwords list.txt | 9f0d0bcd60b903d37f20289cb8a10293 | 0.02 | txt |
| 505 | pat-whelen-MIGILwnvEh0-unsplash.jpg | 3d2d576eeb689515aa7d6aaafd1ddaa6 | 3.31 | jpg |
| 506 | paul-silvan-WfZ-cl8_smM-unsplash.jpg | 03a04a041f4ff1741c203f9c02f37edf | 0.70 | jpg |
| 507 | paweldotio-7RrnOq4AR6Q-unsplash.jpg | e3402ebb7953a7ed522b88c3a366da36 | 1.17 | jpg |
| 508 | pedestrian-overpass-dubai-united-arab-emirates_51213505041_o.jpg | 219c1f36e18a2ba4f458235c46acf1c3 | 1.35 | jpg |
| 509 | pedestrian-tunnel-from-convention-center-dubai_51111375490_o.jpg | 2a9994c26bde158baad331a2fd56cbbc | 1.61 | jpg |
| 510 | pexels-aleksandar-pasaric-1079850.jpg | cc190c133083e9e67ecf5ca8eb8092f4 | 0.89 | jpg |
| 511 | pexels-aleksandar-pasaric-1415794.jpg | 84a9483f0879a694504f92b8a59dc27a | 0.67 | jpg |
| 512 | pexels-aleksandar-pasaric-1436119.jpg | d9f58542e04c3cb7e58a2f3c77a6f6c8 | 0.72 | jpg |
| 513 | pexels-aleksandar-pasaric-1497417.jpg | 9879a4139a42aa14061547bace588cef | 0.90 | jpg |
| 514 | pexels-aleksandar-pasaric-1530829.jpg | 56a2cad15c0a5eac233e51884f59d995 | 0.77 | jpg |
| 515 | pexels-aleksandar-pasaric-1692681.jpg | 88654529e04cdeba4250f037cb218b48 | 0.54 | jpg |
| 516 | pexels-aleksandar-pasaric-2025069.jpg | c830d6b7dd02661b6d41561cdcb37ed2 | 0.83 | jpg |
| 517 | pexels-aleksandar-pasaric-2044434.jpg | 629cbe2fbe7749d16965bbb1630823d2 | 0.51 | jpg |
| 518 | pexels-aleksandar-pasaric-2115367.jpg | ed65e721dc50ec4eae1dfd7efb419d80 | 0.56 | jpg |
| 519 | pexels-aleksandar-pasaric-325185.jpg | f66f349c55b7edb33df01f688a068ae7 | 0.68 | jpg |
| 520 | pexels-aleksandar-pasaric-325193.jpg | 37600d2831f6531b449995d2b68d38ff | 0.87 | jpg |
| 521 | pexels-aleksandar-pasaric-3317535.jpg | 75848cfef928fae56e875baa16b5ca6d | 0.54 | jpg |
| 522 | pexels-aleksandar-pasaric-4201659.jpg | 0c1a2b61b9585e8dfeaa291c7768bb4f | 0.79 | jpg |
| 523 | pexels-aleksandar-pasaric-5686514.jpg | 4a7b01cc303d3a38dab8143cdf87c106 | 0.56 | jpg |
| 524 | pexels-aleksandar-pasaric-618079.jpg | 6a461c0628d792da2543b30f093c05d0 | 1.20 | jpg |
| 525 | pexels-aleksandar-pasaric-692102.jpg | 107c306720c8405f0a735115d4ea75b2 | 0.63 | jpg |
| 526 | pexels-aleksandar-pasaric-692103.jpg | 56dd42859844c05d2a744a0d385410da | 0.91 | jpg |
| 527 | pexels-aleksandar-pasaric-752688.jpg | f5fc35189ed4c058361130cf5d5a07a4 | 0.69 | jpg |
| 528 | pexels-aleksandar-pasaric-823696.jpg | 060f585d0d2e510bc5cf05ad9a7d95be | 0.50 | jpg |
| 529 | pexels-asha-sebastian-4986111-1920x1080-30fps.mp4 | c60fcc2bceaf14b42fa10fe3867526f1 | 8.67 | mp4 |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 530 | pexels-asifgraphy-4348305.jpg | 948d515f6b5fb7dae996670a200270df | 1.00 | jpg |
| 531 | pexels-asifgraphy-4348473.jpg | 2588929193d6639383abfca59d91e92f | 0.34 | jpg |
| 532 | pexels-baluc-photography-6598291.jpg | 87af0b3c9c0855fcf65885a617e21a29 | 0.89 | jpg |
| 533 | pexels-baluc-photography-6598294.jpg | 16952b9e480bb935083a89ca87ef0cf9 | 0.98 | jpg |
| 534 | pexels-denys-gromov-4471198.jpg | 0882a151f0022f0a63e66b64ed95838c | 0.93 | jpg |
| 535 | pexels-denys-gromov-4471199.jpg | 57b22fd5b838c89327395ec255b7c54e | 0.84 | jpg |
| 536 | pexels-denys-gromov-4471200.jpg | 8495420085ad8b133a14dd7a1e7f709e | 0.85 | jpg |
| 537 | pexels-denys-gromov-4471207.jpg | e70e94354b3d4281f3549e0672fa2942 | 0.77 | jpg |
| 538 | pexels-denys-gromov-4471209.jpg | 9aa135119a5c8960075cf21e3d23e586 | 0.84 | jpg |
| 539 | pexels-denys-gromov-4491944.jpg | c2b37b896c83916fea4160c379cbe805 | 0.79 | jpg |
| 540 | pexels-denys-gromov-4502690.jpg | 71d6dd2c8562736a17027a65d60e3f80 | 0.96 | jpg |
| 541 | pexels-denys-gromov-4502694.jpg | 26ba3ed1e5be8a2a5a6ab268f377462f | 1.04 | jpg |
| 542 | pexels-denys-gromov-4502720.jpg | 5b46f7c335b54f2706dce47bc5d20c72 | 0.70 | jpg |
| 543 | pexels-denys-gromov-4560325.jpg | 5dd33adeeeb6082559dea12a4c5d4fc7 | 0.63 | jpg |
| 544 | pexels-denys-gromov-4561219.jpg | 95c424d6197d02baef5392bd53534dab | 0.83 | jpg |
| 545 | pexels-denys-gromov-4612748.jpg | 84706ba2cf9c06019d19adcd02bc836e | 1.01 | jpg |
| 546 | pexels-denys-gromov-4624570.jpg | c1c2dc85c7a5ea7249925524639fbf28 | 1.00 | jpg |
| 547 | pexels-denys-gromov-4624577.jpg | 415b09f53428aa87d3131432323cd2c7 | 1.19 | jpg |
| 548 | pexels-denys-gromov-4857611.jpg | 855a6e99dc16a305f05361a960a9eacc | 0.78 | jpg |
| 549 | pexels-denys-gromov-7199830.jpg | 8ce07a294f4fdf95670782715b38c986 | 1.12 | jpg |
| 550 | pexels-denys-gromov-7662956.jpg | 462807febf49a4b9fd439557c570e9fc | 0.80 | jpg |
| 551 | pexels-denys-gromov-7662957.jpg | 1d503f525cb80fa520020af73de0c554 | 1.20 | jpg |
| 552 | pexels-denys-gromov-7974825.jpg | 2e9dd508d668842db5e2baeb8105fdfe | 0.64 | jpg |
| 553 | pexels-denys-gromov-7974826.jpg | 45c2217f1e664bd761ead8e71b1b15b8 | 1.01 | jpg |
| 554 | pexels-denys-gromov-7974827.jpg | 8f96a9e85f091287448f4de485dc96e1 | 0.91 | jpg |
| 555 | pexels-ivan-siarbolin-3015863.jpg | db1ee77a2dda9acaf644da7213621c52 | 0.86 | jpg |
| 556 | pexels-ivan-siarbolin-3015864.jpg | 001f2ba421834224e73d5aa716486a8a | 0.95 | jpg |
| 557 | pexels-ivan-siarbolin-3015865.jpg | 8ac2a1532457f2c0c8e5c0892bb51946 | 0.90 | jpg |
| 558 | pexels-ivan-siarbolin-3015874.jpg | bc6ca469ae86d57f18805f50c6e35cd7 | 1.04 | jpg |
| 559 | pexels-ivan-siarbolin-3787843.jpg | 2798978ec02f04f1d813f4ab2e0fd851 | 0.59 | jpg |
| 560 | pexels-jeshootscom-442579.jpg | 074f6c40bccb6974004249fa8a5db2fe | 0.71 | jpg |
| 561 | pexels-marcus-herzberg-1381722.jpg | e7e7357fb5c7195956d863775d1fc18a | 0.70 | jpg |
| 562 | pexels-marcus-herzberg-1745554.jpg | 30037829e3fd24ab2a27e1d2b7a584ed | 0.95 | jpg |
| 563 | pexels-marcus-herzberg-2086765.jpg | c390eaf030adb8366588d6404f9b2a49 | 0.72 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 564 | pexels-maria-charizani-5577693.jpg | 505a56deeb1ece77b37c3ca0cc2460d5 | 0.80 | jpg |
| 565 | pexels-marit-sukk-402433.jpg | 51b0c56c3b819746e624988a961cd0f0 | 0.74 | jpg |
| 566 | pexels-mo-3462514.jpg | 2bab321c5b491e5ca1474b26da7a9517 | 1.09 | jpg |
| 567 | pexels-mo-eid-9454915.jpg | 251c47614cb9ad46ec8773793c621fef | 0.55 | jpg |
| 568 | pexels-mo-ismail-3763191.jpg | 551e041379391a7791f62391178c7647 | 0.93 | jpg |
| 569 | pexels-nextvoyage-5879262.jpg | 78eff5d96ef252ccfa3527e22fdb7e19 | 0.90 | jpg |
| 570 | pexels-nixon-johnson-7703869.jpg | 534441d52675af397d3b8a9194129242 | 0.94 | jpg |
| 571 | pexels-photo-91628.jpg | 9e3de2009b5e440fa24570568fbe3efc | 1.15 | jpg |
| 572 | pexels-pixabay-417267.jpg | 28ebd5a128199b01f0c7566d9deffff9 | 0.72 | jpg |
| 573 | pexels-pixabay-460683.jpg | aaf8b09ea886298a9f9a8c659a94195a | 0.61 | jpg |
| 574 | pexels-san-photography-6260815.jpg | 5d303131dac9532e9535cadcf47e4c2e | 0.94 | jpg |
| 575 | pexels-san-photography-6435224.jpg | 6fb0a0ef1f7151ba6170614327c0cb2c | 1.09 | jpg |
| 576 | pexels-san-photography-6526440.jpg | 3b4f47431c083119419e777c8bb7d71b | 0.89 | jpg |
| 577 | pexels-san-photography-6526442.jpg | f3db31fce711adb2ef05d0b7064b9336 | 0.92 | jpg |
| 578 | pexels-san-photography-6526443.jpg | 97774c9ef3a36ad04a3ad691f920bf0f | 0.87 | jpg |
| 579 | pexels-san-photography-6526445.jpg | fa49dccf87763235aff4ca0218e79902 | 0.85 | jpg |
| 580 | pexels-san-photography-6895999.jpg | 8739db015ffd3ca89d6255e97a64af1b | 0.71 | jpg |
| 581 | pexels-walid-ahmad-1717301.jpg | 973db014c990d58c5718187be8620548 | 0.80 | jpg |
| 582 | pic04031.jpg | 43bf82bef42134353c055501b7c42d89 | 0.81 | jpg |
| 583 | piggybank-DnJK8sEZWbk-unsplash.jpg | 8227b90559dad1747b651b7199b880f2 | 1.50 | jpg |
| 584 | piggybank-uUMzuD71BJw-unsplash.jpg | da0a3d7c462ef21e88a791ea5f5b2ce7 | 1.52 | jpg |
| 585 | piotr-chrobot-6oUsyeYXgTg-unsplash.jpg | 8010d92801b93278230002fb31b4a4a0 | 0.58 | jpg |
| 586 | prateek-kochar-au1s8PEBAtE-unsplash.jpg | 0b669c27a5351ad4ec1a77fb9907ece7 | 0.51 | jpg |
| 587 | radu-florin-V8H6hXhmoqI-unsplash.jpg | 8f2501afab35ea062b08a4e47a6508c0 | 0.84 | jpg |
| 588 | Rail-57382392.jpg | 024710e12e650f2d47455bd889dac19f | 1.15 | jpg |
| 589 | raimond-klavins---e5pn5yzYU-unsplash.jpg | 804e1cd018a69214f6447705d5dc564d | 0.93 | jpg |
| 590 | raphael-renter-VO_c55zvyrk-unsplash.jpg | 13987f2c5b45ee5a05d488d7572f448e | 1.46 | jpg |
| 591 | region_2b5586ac29.jpg | e4c110b7b3db168798fb0c8267e706fc | 1.04 | jpg |
| 592 | resource-database-fnZRST1xIUA-unsplash.jpg | 63c47b5a86efa8913015e24b4776832f | 1.75 | jpg |
| 593 | resource-database-F_z2cHsOXnM-unsplash.jpg | ae08003ba625e0f58055316002849371 | 0.71 | jpg |
| 594 | resource-database-mocQyiFsgtM-unsplash.jpg | 8d77aeb4f3ffe7dbf445b7adf4b46e5a | 0.71 | jpg |
| 595 | resource-database-XaVNix5mpDQ-unsplash.jpg | ff60ef048f8cecb75e0af31d4ac75786 | 0.43 | jpg |
| 596 | ricardo-l-2bCEHNTW324-unsplash.jpg | 24c007767b80c5ec141bd28d75b2d593 | 1.50 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 597 | rodeo-project-management-software-iqLVxrHp46k-unsplash.jpg | 5664b85c4f30791a611a45635d9c8f71 | 2.80 | jpg |
| 598 | saketh-garuda-SHY-CKpYjrE-unsplash.jpg | 0a8e6de76b18e1b4b707f51a0e0a925f | 2.34 | jpg |
| 599 | Sample Files.rar | 5f9cabf10bc4e84e0879777b39a753d6 | 7.99 | rar |
| 600 | sample-animated-400x300.gif | c0a72897dae4a00b80652bffc22d899b | 0.00 | gif |
| 601 | SampleAudio_0.7mb.mp3 | 71e5cb4f2f80f10e6e6c1c071896b6f3 | 0.69 | mp3 |
| 602 | SampleCSVFile_10600kb.csv | 0ef0d60ad5304e265c931a2e589063fb | 3.81 | csv |
| 603 | SampleJPGImage_2mbmb.jpg | ea5efc10c2873f1713fdb368e4d25dd7 | 2.00 | jpg |
| 604 | Scyscrapers.jpg | 560c8ed13278d8725dd31399b547e598 | 1.64 | jpg |
| 605 | shaun-jones-9aO3871uVlc-unsplash.jpg | a63be2d56eb18575cabda32174b8b480 | 1.31 | jpg |
| 606 | shutterstock_132104546.jpg | 58a5ed14e3facdec2007cf383743db43 | 1.06 | jpg |
| 607 | shutterstock_233682652.jpg | 1ce4a0d9415bf4651ebd1ddacc5b3392 | 1.04 | jpg |
| 608 | shutterstock_246106153-copy.jpg | 8a6646a61e345b7b5cde5a0656ecbfb1 | 1.07 | jpg |
| 609 | shutterstock_552820438.jpg | d20426ad4aed33efb497c81b0df87222 | 1.48 | jpg |
| 610 | shutterstock_700446010.jpg | a67c9e0ebb9c1751fc320642251a0423 | 1.03 | jpg |
| 611 | shutterstock_786266752.jpg | 610f32cc7046cba4158ff05c39431479 | 1.35 | jpg |
| 612 | simon-lee-xRVnUhe0fss-unsplash.jpg | 459e6c89747eb556e35e72b853ef3c2c | 1.98 | jpg |
| 613 | skyline-night-Marina-buildings-Dubai-skyscrapers-2013.jpg | 67a5b13de75bdc1556f00ae4fcf64d1e | 1.32 | jpg |
| 614 | skyscrapers-dubai_32041540986_o.jpg | c6ac3de27499a038c4c0e9f38284b3ff | 0.86 | jpg |
| 615 | Smart-city-2.jpg | c9119662d952a28f7523ebec7eeac459 | 1.72 | jpg |
| 616 | Smart-city.jpg | dc4a29e3faabad83f3cbcd43b00b0b8d | 1.86 | jpg |
| 617 | sreehari-devadas--WQI3xmytv8-unsplash.jpg | 0267d179869a77eb820b278e0d153079 | 0.88 | jpg |
| 618 | sumaid-pal-singh-bakshi-MZAsMHUcwhY-unsplash.jpg | 831bd40e5af8e04c378c8e1bb957f9a3 | 1.26 | jpg |
| 619 | sunrise-Dubai-uae-cityscapes-d750-970424.jpg | 6feb89a1a5f067bc95473211e6c19012 | 0.79 | jpg |
| 620 | SWPR168a_24291116.jpg | 1047de7e007edfa7cc228431eaeb2ad6 | 1.59 | jpg |
| 621 | szz20Ukgc-FN4JhhEI0CUZBzwF3B_7S8wX9Zkqfq4UM.jpg | 2b1fccd284c068ec3574653800dd3c45 | 0.93 | jpg |
| 622 | the-address-residence-sky-view-under-construction-dubai_51293301698_o.jpg | 25d8fb1c87efffd0484a907ca5f1494d | 1.55 | jpg |
| 623 | the-atlantis-resort-the-palm-dubai-dubay.jpg | b8d9ca453d237a13f19a7698c54c8993 | 0.96 | jpg |
| 624 | the-dubai-ferris-wheel-under-construction-dubai_51293281938_o.jpg | 67a64b35aa905efafd58681fd41f88bd | 1.22 | jpg |
| 625 | the-fairmont-the-palm-jumeirah-dubai-united-arab-emirates_51267447595_o.jpg | 3bb7687d0e8e5a8eb9b811ed16b728a2 | 1.64 | jpg |
| 626 | the-metro-the-palm-jumeirah-dubai-united-arab-emirates_51267143389_o.jpg | f0e918e59e76376966e6b8e5f4f616fc | 1.33 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 627 | thom-milkovic-qGQIOLke2kE-unsplash.jpg | 9c4cdc42da33d770e4369170db1493e7 | 2.04 | jpg |
| 628 | thomas-winkler-qIOCsS2TYvA-unsplash.jpg | dd7bbb7bc266e739c6a4a51aec8db646 | 0.84 | jpg |
| 629 | thomas-winkler-TgWiS7h3ioE-unsplash.jpg | a76badb6980dcd8e8ce0fef33b2df1f9 | 0.80 | jpg |
| 630 | tobias-reich-5h6VXw9h-VA-unsplash.jpg | 3fd474b4f493fec2e923beaf4c333501 | 0.62 | jpg |
| 631 | tom-chen-577408-unsplash.jpg | 0348a8b42997e0e347a780ef052f0709 | 1.29 | jpg |
| 632 | train-in-the-metro-station-dubai-united-arab-emirates_51232929428_o.jpg | e0510a0c07d2a84b299b69b226f5ceea | 1.66 | jpg |
| 633 | train-operators-cab--metro-station-dubai_51232006582_o.jpg | a44a4a899c6d89ed0e3a4d2f18c686a8 | 1.21 | jpg |
| 634 | TUI_dubai.jpg | da25ec7c2bf7722bb387ac0e54d69dc4 | 1.60 | jpg |
| 635 | typerium-app-hbfBIs_Q67g-unsplash.jpg | 61044b337bad5b623ea7f9afafb78d27 | 3.35 | jpg |
| 636 | u-a-e-1154532.jpg | f8e441a20602f3f2c8cef076c7761e01 | 1.16 | jpg |
| 637 | u-a-e-1154544.jpg | 2abe323ea68ee1597b359c305fcdd342 | 0.95 | jpg |
| 638 | u-a-e-5453673.jpg | 2e466b97a49148e724c79012a87d09ec | 0.53 | jpg |
| 639 | u-a-e-5475247.jpg | f09972d6e68033bfdca3e87538c95659 | 0.80 | jpg |
| 640 | unnamed (2).jpg | a19dd7b4b98a6704e6050bdd9229a6ec | 0.96 | jpg |
| 641 | unnamed.jpg | df17fac35a6a148c6e84f24d9374f5b4 | 1.02 | jpg |
| 642 | valentine-mytchyk-XXU3Uw0yvBg-unsplash.jpg | 110a82cacf0147b08cf76c25086df8fa | 2.60 | jpg |
| 643 | VBox.log | ec8b34ed82b7ed119fa4aafc60a61e53 | 0.19 | log |
| 644 | vereinigtearabischeemirate-970300.jpg | 79121dff34462ad53c6c83be1705a4f6 | 0.92 | jpg |
| 645 | VeXx27.jpg | e13b87176d86d375bb3ab12c3e0cebbc | 1.09 | jpg |
| 646 | View from the top 2.jpg | 4074227592a9a5b54767cf2abe272390 | 2.47 | jpg |
| 647 | view-of-burj-khalifia-the-address-and-another-emaar-property-dubai_51241901720_o.jpg | 7c14d9a9624b01f49d7ad0b042d2a2ad | 1.72 | jpg |
| 648 | views-from-the-river-cruise_33023021701_o.jpg | 34af203adef31f1bfb1565fa243e12a8 | 0.94 | jpg |
| 649 | views-from-the-river-cruise_33108546496_o.jpg | 5f8995dbd90aac3373513d62f8522a36 | 0.94 | jpg |
| 650 | visitdubai.com-2021-05-19_203646.jpg | bbe209afbee0fab10e9009bd3ff230b2 | 0.97 | jpg |
| 651 | vitalii-ustymenko-2WMuWzIE73E-unsplash.jpg | 9eaa3e1f560123ea505e1f00529655cc | 0.87 | jpg |
| 652 | wallpapersden.com_dubai-burj-khalifa-cityscape-in-night_5120x2880.jpg | 1962745f0e409d75bacb561a2a9d0913 | 1.08 | jpg |
| 653 | wallpapersden.com_dubai-united-arab-emirates-sea_7680x4320.jpg | ea1967104351cc6602bd91094b0df5be | 1.17 | jpg |
| 654 | water-horizon-sky-skyline-night-city-skyscraper.jpg | f2d4d1fe056bb1bb5cceabbec05f2af5 | 1.31 | jpg |
| 655 | white-9CmBwMycqFQ-unsplash.jpg | b00a98a2e8541c6a2162c8f90c1bb2b2 | 0.37 | jpg |
| 656 | Wiping Techniques and Anti-Forensics Methods.pdf | 366bef8561877b8a2acffaadbd14f90a | 1.04 | pdf |
| 657 | zack-walker-GM-FgNYBuo0-unsplash.jpg | 3393ae54873b7a87b02669e2c6f1f376 | 0.71 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 658 | Ανοικτό Πανεπιστήμιο Κύπρου - Open University of Cyprus.html | ed88b24a9ddf2bce15c58bbb5066296d | 0.82 | html |
| 659 | Kali Linux _ Penetration Testing and Ethical Hacking Linux Distribution.html | b0e4b20e20edd9a6867156c4e20674a6 | 0.79 | html |
| 660 | css | 56c6a382b59bed3ecb342ee0e5ecd8b3 | 0.00 | |
| 661 | index.min.css | 76b50bef7fea6f7f064462013b07b7a4 | 0.01 | css |
| 662 | index.min.js.download | d085bb2cb86503aef159eebf835468ab | 0.00 | download |
| 663 | kali-desktop-gnome.jpg | 171721fcb4e986aacf7a4eb84bc4c010 | 0.13 | jpg |
| 664 | kali-desktop-kde.jpg | 153ff319135c6442c562d6aff16776f1 | 0.11 | jpg |
| 665 | kali-desktop-xfce.jpg | f0b59e75e95ab0e727359e10af62a27f | 0.12 | jpg |
| 666 | kali-everywhere-arm.svg | 77078749d3d44b3e40f4036dacd1d3bb | 0.02 | svg |
| 667 | kali-everywhere-cloud.svg | 03cad759f65d47c85df039bb84118f2b | 0.04 | svg |
| 668 | kali-everywhere-container.svg | 2c4df2a2d98bef8c4e92d07fc930427a | 0.01 | svg |
| 669 | kali-everywhere-installerimages.svg | 9f549a60c02837ec9254fbbbced67758 | 0.02 | svg |
| 670 | kali-everywhere-mobile.svg | 85e2a07a8d9096a4d485a9f36a914f50 | 0.02 | svg |
| 671 | kali-everywhere-usb.svg | ed85d6d88495eb66f8cd5e403c7685d5 | 0.01 | svg |
| 672 | kali-everywhere-vm.svg | c9a04cf0601a1015e2bf881f598b2374 | 0.00 | svg |
| 673 | kali-everywhere-wsl.svg | 264698e0093ecd00ee6413b82b01fbd4 | 0.00 | svg |
| 674 | logo-gnome.svg | 7adcafb52bd24abfbc018cd867829202 | 0.00 | svg |
| 675 | logo-kde.svg | b432b11a5a27f19c1454ee1778dfdd28 | 0.00 | svg |
| 676 | logo-xfce.svg | 1d3e7f50ded37475bb4a3a6e6ec27e80 | 0.00 | svg |
| 677 | notebook-kali-2022.1.jpg | 19d0dc53aa2380272e45b689b83fe032 | 0.24 | jpg |
| 678 | notebook.svg | 2718149ecea0cf2e7a33242309669b60 | 0.00 | svg |
| 679 | script.min.js.download | 518bb3b113c4f82beb1538c816718a7f | 0.00 | download |
| 680 | style.min.css | 7db07c74284fe194c756e856bd870184 | 0.02 | css |
| 681 | themify-icons.css | 3255e5391f906a3b6e0353f27c90da48 | 0.01 | css |
| 682 | tool-logo-aircrack-ng.svg | dc10538b3029bc4836629d1488ddf607 | 0.01 | svg |
| 683 | tool-logo-burp.svg | 78ed0910199882afb0d30e4249308915 | 0.00 | svg |
| 684 | tool-logo-crackmapexec.svg | dee7bf8d1755ec33e9ece9e7fbd1826f | 0.02 | svg |
| 685 | tool-logo-ffuf.svg | 69bbdf88a3268a852d92afc54b9592c4 | 0.01 | svg |
| 686 | tool-logo-hydra.svg | 222731453ce456201dc30146917cfef2 | 0.17 | svg |
| 687 | tool-logo-john.svg | e05ce2ef105bea1125d063cc43c073d3 | 0.02 | svg |
| 688 | tool-logo-maltego.svg | 32daadd8b4e2c1c3a1940fc0a4151265 | 0.01 | svg |
| 689 | tool-logo-metasploit.svg | 893cb3959a58dadb23e005424d7c8c21 | 0.00 | svg |
| 690 | tool-logo-nmap.svg | 918188b1f2adeb464de1db354343ff20 | 0.01 | svg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 691 | tool-logo-powershell-empire.svg | 3c3016c431284ada4cb5e29640acb1f3 | 0.01 | svg |
| 692 | tool-logo-responder.svg | c796417d1c5987d2aa0a6800f2d7045d | 0.01 | svg |
| 693 | tool-logo-sqlmap.svg | e2233dfdfd63f677bfa3a0ec0333a3b8 | 0.00 | svg |
| 694 | tool-logo-starkiller.svg | be8dbe32a431f1757d4a8a16adbea1d3 | 0.09 | svg |
| 695 | tool-logo-wireshark.svg | f952d63c9738033e4555451a629b8dbe | 0.01 | svg |
| 696 | IMG_20190421_143146.jpg | 09441981fb7183c2e26c721377299fd4 | 3.98 | jpg |
| 697 | IMG_20190421_143149.jpg | f11bc18eddcbfd3da649a38cdad52f43 | 3.95 | jpg |
| 698 | IMG_20190421_143201.jpg | 56d81046e75f0dec381b598ba227ee18 | 4.67 | jpg |
| 699 | IMG_20190421_143217.jpg | 2cc1073e09b799188c31a5d8a5502d58 | 4.88 | jpg |
| 700 | IMG_20190421_143241.jpg | 5ce5d773f3968acc6798300685be4404 | 2.14 | jpg |
| 701 | IMG_20190421_143348.jpg | ea57d521df400e60b27308db65145fc2 | 3.98 | jpg |
| 702 | IMG_20190421_143351.jpg | b90b6d291d5bf672e1da2911a795bbaa | 4.08 | jpg |
| 703 | IMG_20190421_143357.jpg | 21813b4bf7bd1ff6efc7b28e7b84bf06 | 4.24 | jpg |
| 704 | IMG_20190421_143402.jpg | 8a0e1f759aa1a2d65181cdc34ec4cee7 | 4.63 | jpg |
| 705 | IMG_20190421_143408.jpg | 2d486ac3471ae5bf6956c4c8158a2e42 | 4.71 | jpg |
| 706 | IMG_20190421_143557.jpg | c390a511dc20054ea9dcbcb0e8645d6c | 6.21 | jpg |
| 707 | IMG_20190421_143958.jpg | e1488d1ba987742766cdd6525a9c2008 | 3.87 | jpg |
| 708 | IMG_20190421_144000.jpg | 67ed83ba499f4344ae59ca83024f639c | 4.52 | jpg |
| 709 | IMG_20190421_144059.jpg | e755721c443663dc69c3229cee76e94d | 2.10 | jpg |
| 710 | 1200x600px_GR.gif | 7c5b65dbd7e0e6ee5b6ed9b8442c4b3f | 0.31 | gif |
| 711 | 2022-10-05_14-31-52.png | b617e0e81650e545e761126b46293d15 | 0.27 | png |
| 712 | 2022-10-10_16-16-37_new2.png | 9a9350db22546e3ed95871fca102dee3 | 0.05 | png |
| 713 | 260x100-01-WHY-OUC-EL.png | ddc903ddf2227ec95bea666c90b6046a | 0.02 | png |
| 714 | 260x100-01_applications_2022-2023_EL.png | eef20f4563cf7f91d974b17d07577a1b | 0.02 | png |
| 715 | aftoteleis_150.png | e2de8d19b959a123eb36281981dd3f11 | 0.03 | png |
| 716 | canyon-g0fa67900d_1280.jpg | 46a4b3574c8d581eae467666f379356b | 0.17 | jpg |
| 717 | CYCAT_sm_150png.png | dcd10830980dedfb5318dfebeb102a56 | 0.01 | png |
| 718 | Cyprus_Education_Awawrds_100.png | ff56cd54705cb301db5ffa4f5818db9c | 0.00 | png |
| 719 | EADTU_100.png | 829825d2d2562a30da8eb1a153dbe1ad | 0.01 | png |
| 720 | erasmus_logo_new.png | 8f72913707849d3a5f4449029b23b821 | 0.12 | png |
| 721 | eua_100.png | d8fdd286060a70fe2ca8056c7c5f1b44 | 0.02 | png |
| 722 | f.txt | 2233e1fcf074c626c0976a265ded8515 | 0.00 | txt |
| 723 | FB_cover_greek.jpg | a7e7223ad21794e23ff34cd73a0c74d5 | 1.58 | jpg |
| 724 | hiring.jpg | a5a7246c7801b5fba56a58bb62ed8ac6 | 0.15 | jpg |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 725 | icde_100.jpg | 310b84aef4b3a052520414d771a97ada | 0.01 | jpg |
| 726 | KChrysantis_4.jpg | d18f27a7a150aff53e15132370bfee11 | 0.94 | jpg |
| 727 | lab-chem-mechanic-150.png | 6644b52172fc2d3c4c69613d5ae537e1 | 0.03 | png |
| 728 | lab-edutech-150.png | e86c3fccc5a1cbb44c77d95c00f6b360 | 0.03 | png |
| 729 | lab-kivernoasfalia-150.png | 8365589df2957ce28def4fc2ce9a8588 | 0.02 | png |
| 730 | lab-noisis-150.png | da1c98fa08f571e170ee6eb73083f9d3 | 0.02 | png |
| 731 | lab-xerseon-150.png | 4683b5832a1e19511c07b3183bd4697d | 0.03 | png |
| 732 | logo_96_gr_new.png | a601d46daa88c9445f17c099bc9f474e | 0.01 | png |
| 733 | logo_ouc_30.png | 7fef27ed89315b929b93eaac7f695196 | 0.00 | png |
| 734 | logo_white.png | 181c18df38ab7239b3553be0f81d9a43 | 0.00 | png |
| 735 | MoU_ΑΠΚΥ_ΣΑΛΑ(1).jpg | 2795baea17bd3dbd8f5dd0cc2a201f06 | 0.22 | jpg |
| 736 | MoU_ΑΠΚΥ_ΣΑΛΑ.jpg | 8fc8fe23da82ab9db2c8b88f94f54862 | 0.00 | jpg |
| 737 | next.png | e321b7d0dd091cb9d307ea1eaf729ced | 0.00 | png |
| 738 | OUC-UNESCOCHAIR-LAUNCHEVENT-Banner-12(1).png | 771501e2f826e23871e0252a862b0a83 | 0.31 | png |
| 739 | OUC-UNESCOCHAIR-LAUNCHEVENT-Banner-1200x628.png | 147bcef9aed259a418ea592d52bca25b | 0.01 | png |
| 740 | OUCDEP_List_small_new.png | f7cee5eb89c28ed0b070ec7e6fa84d64 | 0.13 | png |
| 741 | OUCEvents_Programme(1).png | 74ac42fe373b95d93e2a77bfbe544607 | 0.13 | png |
| 742 | OUCEvents_Programme.png | b39347b8bd48d73ff3c42808ba0c3dfa | 0.00 | png |
| 743 | pause.png | 4de88363007b9d9a2482b55beebab9fa | 0.00 | png |
| 744 | play.png | 014940b979824ab02f0b8ed0c8a26227 | 0.00 | png |
| 745 | prev.png | 6da2410fb7545ce8f404bece4c727871 | 0.00 | png |
| 746 | Researcher.jpg | 997f625c0f29449a86f1355ca23b6a5e | 0.05 | jpg |
| 747 | sake.jpg | a4ef04f6bf2f20d137a39d164df14bfb | 0.02 | jpg |
| 748 | SDSN_logo_100.jpg | d57a4c7a8d9315953c64d2a7d6caca1c | 0.01 | jpg |
| 749 | SLR-SIR_2014_100.jpg | e89e0f8d76146f7af7391f515290adff | 0.03 | jpg |
| 750 | soed.jpg | 5f4a59342d726009efe93469a7dfa1c0 | 0.03 | jpg |
| 751 | sthee.jpg | 12adb4bb4836bea51b3c4c781655c879 | 0.01 | jpg |
| 752 | Thumbnail_website_ASP.png | 22648914510ff08966eaf76af3ccd0f1 | 0.03 | png |
| 753 | Thumbnail_website_AYD.png | a80a232d10d4ab90979b8967e6f8817a | 0.03 | png |
| 754 | Thumbnail_website_BIH.jpg | 40626c2b8409824ce6da2f2f33167d33 | 0.02 | jpg |
| 755 | Thumbnail_website_CHD.png | ccf686183ad3a7f7b83ec7bd77a85f25 | 0.04 | png |
| 756 | Thumbnail_website_COS.png | 1e634ed2c7637dfb8b2dff6dbe300f7d | 0.03 | png |
| 757 | Thumbnail_website_DEE.png | e5c5443e72107059f8b10cbe9c4d236c | 0.03 | png |

| A/A | Filename | MD5 | File Size (MB) | Type |
|---|---|---|---|---|
| 758 | Thumbnail_website_DMY.png | 2a5dba5637fc701b0c747bfadc6bf58b | 0.03 | png |
| 759 | Thumbnail_website_DPP.png | ad8a2f31c5031d987bdefe4659d3dac6 | 0.03 | png |
| 760 | Thumbnail_website_DTP.png | 6f9a5b3bf0f8d7bd53d3719d693c2654 | 0.03 | png |
| 761 | Thumbnail_website_EDM.png | e2b9366092326f869f266b5547c1aa2a | 0.01 | png |
| 762 | Thumbnail_website_EGL.png | f0fe848a0e4e0ccc775ed12d513d810e | 0.03 | png |
| 763 | Thumbnail_website_ELL.png | 6efac98038662692ba5ba051e8183cf1 | 0.02 | png |
| 764 | Thumbnail_website_EPA.png | bf786784d8cce7e385a74a91c037cf65 | 0.03 | png |
| 765 | Thumbnail_website_EPT.png | a3166f1376ef2777e70c4422caaee664 | 0.03 | png |
| 766 | Thumbnail_website_ERM.png | 6626b4f54cf1f70dbe4adae47c09abbf | 0.03 | png |
| 767 | Thumbnail_website_IMAESC.png | 17876c7df144582d85e8915f864e9be3 | 0.03 | png |
| 768 | Thumbnail_website_KPS.png | 991ad990585cf914b81ec964813a786e | 0.04 | png |
| 769 | Thumbnail_website_MBA.png | 0b1faedcd2452351caa16cddb5e7010d | 0.03 | png |
| 770 | Thumbnail_website_MDE.png | 38ad3c8972876acc5af46c347b33511a | 0.02 | png |
| 771 | Thumbnail_website_MES.jpg | fcd6828d461cb10eda564adbaf250341 | 0.02 | jpg |
| 772 | Thumbnail_website_OIK.png | f82a5ae4490a682eee5e1c3ded2b2ef9 | 0.03 | png |
| 773 | Thumbnail_website_PDE.png | 07315c4b17ebb322b7d32f2890964808 | 0.03 | png |
| 774 | Thumbnail_website_PES.png | 9d1caac3deacf4d72544073dab5cd2b1 | 0.03 | png |
| 775 | Thumbnail_website_PEX.png | d819ccc7b3d2e87486d00b3d48d33796 | 0.03 | png |
| 776 | Thumbnail_website_PNYKA.png | 89ee1e830c1cdec7e298b420afe79c13 | 0.04 | png |
| 777 | Thumbnail_website_PPA.png | f6450433b9cbf0c587de9e4cf5ab568f | 0.04 | png |
| 778 | Thumbnail_website_PYS.png | fb81f74643ff1f492c118248e40294d0 | 0.03 | png |
| 779 | Thumbnail_website_SAE.png | 035ac750731f790b325877f62dc451a1 | 0.03 | png |
| 780 | Thumbnail_website_SDM.png | 99f96ec5c4f441dc52d0e5187062be54 | 0.02 | png |
| 781 | Thumbnail_website_SES.png | 717cb4d2266ca9d8eedcb77009372c6e | 0.03 | png |
| 782 | Thumbnail_website_TOIK.png | fb499f1feb5245700c2ba682d091d0dd | 0.03 | png |
| 783 | Thumbnail_website_TSP.png | b36bc15648691e5fe62025e4e64fe06e | 0.03 | png |
| 784 | THUMB_EDLP.jpg | 114938b7e68eddd70411d0d338a42103 | 0.02 | jpg |
| 785 | unitwin_chair_blue_eng_1.jpg | efb5a5668d5efcc35a2d316105653f6a | 0.04 | jpg |

Υπόμνημα:

| |
|---|
| Αρχεία που περιλαμβάνονται στο σετ 200 GB δεδομένων |
| Αρχεία που περιλαμβάνονται στο σετ 10 GB δεδομένων |
| Είκοσι (20) Αρχεία που επιλέχθηκαν |

## A.2 Κατάλογος Εργαλείων

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **1** | DBAN (Darik's Boot and Nuke) | 2.3.0 | Free / Open Source | Ναι | An evaluation of data erasing tools<br>Wiping techniques and anti-forensics methods | Quick Erase<br>RCMP TSSIT OPS-II<br>DoD Short<br>DoD 5220.22-M<br>Peter Gutmann<br>PRNG Stream wipe | https://dban.org/ | DISK |
| **2** | CBL Data Shredder | 1.0.0 | Free | Ναι | An evaluation of data erasing tools<br>Wiping techniques and anti-forensics methods | DoD 5220.22-M<br>Peter Gutmann<br>Bruce Schneier's (VSITR) Standard<br>RMCP DSX<br>Custom Algorith | https://www.cbldatarecovery.com/data-shredder/ | DISK |
| **3** | HDD LLF Low Level Format Tool | 4.4 | Free for personal / home use commercial or professional use | Όχι | - | One pass zeroes | https://hddguru.com/software/HDD-LLF-Low-Level-Format-Tool/ | DISK |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **4** | Active@ KillDisk | 15.0 | Free and commercial version | Ναι | An evaluation of data erasing tools<br>An evaluation of data erasing tools<br>Wiping techniques and anti-forensics methods | One pass zeros | https://www.killdisk.com/killdisk-freeware.htm | DISK |
| **5** | Macrorit Data Wiper | 6.3.8 | Free and commercial version | Ναι | An evaluation of data erasing tools | One pass zeros<br>Pseudo-Random<br>Zero and one (2 passes)<br>DoD 5220.22-M<br>DoD 5220.28-STD<br>Peter Gutmann | https://macrorit.com/free-data-wiper.html | DISK |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **6** | Eraser | 6.2.0.2993 | Free / Open Source | Ναι | An evaluation of data erasing tools<br>An evaluation of data erasing tools<br>Digital tool marks (DTMs): a forensic analysis of file wiping software<br>Identifying Trace Evidence from Target-Specific Data Wiping Application Software<br>Wiping techniques and anti-forensics methods | Peter Gutmann<br>DoD 5220.22-M(ECE)<br>Canadian RCMP TSSIT OPS-II<br>Bruce Schneier's<br>German VSITR<br>DoD 5220.22-M (E)<br>British HMG IS5 (Enhanced)<br>US Air Force 5020<br>US Army AR380-19<br>Russian GOST P50739-95<br>British HMG IS5 (Baseline)<br>Pseudorandom data<br>First/Last 16KB<br>Erasure | https://eraser.heidi.ie/download/ | BOTH |

| Α/Α | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **7** | Freeraser | 1.0.0.23 | Free | Ναι | An evaluation of data erasing tools<br>Digital tool marks (DTMs): a forensic analysis of file wiping software<br>Wiping techniques and anti-forensics methods | DoD 5220.22-M<br>Peter Gutmann<br>Pseudorandom data | https://freeraser.en.uptodown.com/windows | FILE |
| **8** | Disk Wipe | 1.7 | Free | Ναι | An evaluation of data erasing tools<br>Wiping techniques and anti-forensics methods | DoD 5220.22-M<br>US Army AR380-19<br>Peter Gutmann | https://www.diskwipe.org/ | DISK |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **9** | Hardwipe | 5.2.1 | Free | Ναι | An evaluation of data erasing tools. | DoD 5220.22-M<br>Russian GOST P50739-95<br>Peter Gutmann<br>Bruce Schneier's<br>German Standard VSITR<br>Pseudorandom data<br>One pass zeros | https://hardwipe.en.uptodown.com/windows/download | BOTH |
| **10** | ASCOMP Secure Eraser | 6.001 | Free and commercial version | Όχι | - | DoD 5220.22-M (E)<br>DoD 5220.22-M(ECE)<br>German VSITR<br>Peter Gutmann<br>Random Data | https://www.ascompsoftware.com/en/products/secureeraser | BOTH |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **11** | PrivaZer | 4.0.58 | Free and Donated Version | Όχι | - | Peter Gutmann<br>DoD 5220.22-M(ECE)<br>Canadian RCMP TSSIT OPS-II<br>Bruce Schneier's<br>German VSITR<br>DoD 5220.22-M (E)<br>British HMG IS5 (Enhanced)<br>US Air Force 5020<br>US Army AR380-19<br>Russian GOST P50739-95<br>British HMG IS5 (Baseline)<br>Pseudorandom data<br>One pass zeroes | https://privazer.com/en/ | BOTH |
| **12** | PC Shredder | 1.1 | Free | Ναι | Forensic analysis of anti-forensic file-wiping tools on Windows. | DoD 5220.22-M<br>Peter Gutmann<br>Random Data | http://www.softsea.com/review/PC-Shredder.html | FILE |
| **13** | AOMEI Partition Assistant Standard Edition | 9.13.0 | Free and commercial version | Όχι | | One pass zeros<br>Random Data<br>DoD 5220.22-M<br>Peter Gutmann | https://www.diskpart.com/free-partition-manager.html | BOTH |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **14** | Remo Drive Wipe | 2.0.0 | Free and commercial version | Ναι | An evaluation of data erasing tools<br>Forensic analysis of anti-forensic file-wiping tools on Windows | One pass zeros<br>Random Data<br>DoD 5220.22-M | https://www.remosoftware.com/free-drive-wipe | DISK |
| **15** | CCleaner | 6.06.10144 | Free and commercial version | Ναι | Digital tool marks (DTMs): a forensic analysis of file wiping software. | One pass zeroes<br>DoD 5220.22-M<br>Peter Gutmann<br>Bruce Schneier's | https://www.ccleaner.com/ccleaner/download | DISK |
| **16** | File Shredder | 2.5 | Free | Ναι | An evaluation of data erasing tools<br>Digital tool marks (DTMs): a forensic analysis of file wiping software. | DoD 5220.22-M<br>Peter Gutmann<br>One pass zeroes<br>Two pass zeroes | https://fileshredder.org/ | FILE |
| **17** | Hard Drive Eraser | 2.0 | Free | Ναι | An evaluation of data erasing tools. | One pass zeros<br>DoD 5220.22-M<br>US Army AR380-19<br>Peter Gutmann | https://www.harddriveeraser.org/download.php | DISK |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **18** | Super File Shredder | 4.1.2 | Free | Ναι | An Evaluation Of Data Erasing Tools. | One pass zeros<br>DoD 5220.22-M<br>Peter Gutmann | https://www.kakasoft.com/file-shredder/ | BOTH |
| **19** | TweakNow SecureDelete | 1.0.0 | Free | Όχι | - | Peter Gutmann<br>DoD 5220.22-M<br>Random Data | https://www.tweaknow.com/SecureDeleteFiles.php | FILE |
| **20** | MiniTool Drive Wipe | 5.0 | Free | Όχι | - | One pass zeros<br>One pass one<br>One pass zeros & one<br>DoD 5220.22-M<br>DOD 5220.28-STD | https://www.minitool.com/free-tools/minitool-drivewipe.html | DISK |
| **21** | XT File Shredder Lizard | 2.1 | Free | Όχι | - | One pass zeros<br>DoD 5220.22-M<br>Random Data | https://www.softpedia.com/get/System/File-Management/XT-File-Shredder-Lizard.shtml | FILE |
| **22** | WipeFile | 3.6 | Free | Ναι | Digital tool marks (DTMs): a forensic analysis of file wiping software. | Supports 14 different wipe methods | https://www.gaijin.at/en/software/wipefile | FILE |
| **23** | Puran Wipe Disk | 1.2 | Free | Ναι | An Evaluation Of Data Erasing Tools. | One pass zeros<br>DoD 5220.22-M<br>Bruce Schneier's | https://www.puransoftware.com/Wipe-Disk.html | DISK |

| Α/Α | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **24** | BitKiller | 2.0 | Free | Ναι | Digital tool marks (DTMs): a forensic analysis of file wiping software. | One pass zeros<br>Random Data<br>DoD 5220.22-M<br>DOD 5220.28-STD<br>Peter Gutmann | https://sourceforge.net/projects/bitkiller/ | - |
| **25** | Simple File Shredder | 3.2 | Free | Όχι | - | DoD 5220.22-M<br>Peter Gutmann<br>Random Data | https://simple-file-shredder.en.softonic.com/ | FILE |
| **26** | Ashampoo WinOptimizer Free | 17.00.33 | Free | Όχι | - | One pass zeros<br>DoD 5220.22-M<br>Peter Gutmann | https://www.ashampoo.com/en-us/winoptimizer-free | FILE |
| **27** | AbsoluteShield File Shredder | 1.41 | Free | Όχι | - | Two pass zeros<br>DoD 5220.22-M | https://www.softpedia.com/get/Security/Secure-cleaning/AbsoluteShield-File-Shredder.shtml | FILE |
| **28** | DeleteOnClick | 2.6.5.0 | Free | Όχι | - | DoD 5220.22-M | https://www.2brightsparks.com/onclick/help/ | FILE |
| **29** | CopyWipe | 1.14 | Free | Όχι | - | Supports 9 different wipe methods | https://www.techspot.com/downloads/415-copywipe.html | - |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **30** | SDelete | 2.04 | Free | Ναι | De-Wipimization: Detection of data wiping traces for investigating NTFS file system. | DOD 5220.22-M | https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete | - |
| **31** | Wise Care 365 | 6.3.9 | Free and commercial version | Όχι | - | Random Data<br>DoD 5220.22-M<br>Bruce Schneier's<br>Peter Gutmann | https://www.wiseccleaner.com/wise-care-365.html | BOTH |
| **32** | ProtectStar Data Shredder | 2.2 | Free and commercial version | Όχι | - | Random Data | https://download.cnet.com/ProtectStar-Data-Shredder/3000-2144_4-10637320.html | BOTH |
| **33** | HDShredder Free Edition | 6 | Free and commercial version | Όχι | - | One pass zeros | https://www.miray-software.com/download/hdshredder.html | DISK |
| **34** | Moo0 Disk Wiper | 1.14 | Free | Όχι | - | unknown | https://www.moo0.com/?top=https://www.moo0.com/software/AntiRecovery/ | DISK |
| **35** | BCWipe Total WipeOut | 5.02.5 | Trial & Commercial Version | Ναι | An evaluation of data erasing tools. | One pass zeros | https://www.jetico.com/downloads/data-wiping | FILE |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **36** | O&O SafeErase | 17 | Trial & Commercial Version | Όχι | - | Peter Gutmann<br>DoD 5220.22-M<br>German BSI<br>One pass zeros | https://www.oo-software.com/en/safeerase-hard-drive-data-secure-deletion | BOTH |
| **37** | Donemax Data Eraser | 1.2 | Trial & Commercial Version | Όχι | - | Peter Gutmann<br>U.S. Army AR380-19<br>DoD 5220.22-M ECE<br>One pass zeros | https://www.donemax.com/data-erasure-software/data-eraser.html | BOTH |
| **38** | Iolo DriveScrubber | - | Commercial Version | Όχι | - | NIST.SP.800-88 r1<br>Custom | https://www.iolo.com/products/drivescrubber/ | DISK |
| **39** | Abylon Shredder | 23.10.3 | Trial & Commercial Version | Όχι | - | Peter Gutmann<br>DoD 5220.22-M<br>One pass zeros | https://www.abylonsoft.com/shredder/ | BOTH |
| **40** | TS DataWiper | 2.2 | Trial & Commercial Version | Όχι | - | Peter Gutmann<br>U.S. Army AR380-19<br>DoD 5220.22-M ECE<br>One pass zeros | https://www.togethershare.com/data-eraser/datawiper-for-windows.html | BOTH |

| A/A | Όνομα | Τελευταία Έκδοση | Άδεια Χρήσης | Άλλη δοκιμή | Τίτλος δοκίμιου Αναφοράς | Μεθόδοι Sanitization | Ιστοσελίδα | File / Disk |
|---|---|---|---|---|---|---|---|---|
| **41** | Easy File Shredder | 2.0.2018.1209 | Trial & Commercial Version | Όχι | - | one pass zeroes<br>DoD 5220.22-M<br>Peter Gutmann<br>Bruce Schneier's<br>German VSITR<br>ITSG2006<br>Russian GOST P50739-95<br>US Air Force 5020<br>US Army AR380-19 | https://www.easyfileshredder.com/ | BOTH |
| **42** | Zer0 | 0.6.0.6 | Free | Όχι | - | One pass zeros | https://www.kcsoftwares.com/?zero | FILE |
| **43** | Kernel File Shredder | 11.04.01 | Trial & Commercial Version | Όχι | - | One pass zeros<br>DoD 5220.22-M<br>Peter Gutmann | https://www.nucleustechnologies.com/file-shredder.html | FILE |
| **44** | BitRaser Data Eraser | - | Paid | Όχι | - | 18 Global Standards | https://www.bitraser.com/bitraser-file-eraser.php | FILE |